厚生労働科学研究費補助金
（食品の安全確保推進研究事業）

新型コロナ感染症拡大収束後の
食品等事業者の新たな営業形態にも対応した
食品防御の推進のための研究

令和７年度　総括・分担研究報告書

研究代表者　今村　知明

（奈良県立医科大学　公衆衛生学講座）

令和８（２０２６）年３月

目　次

厚生労働科学研究費補助金（食品の安全確保推進研究事業）
総括研究報告書（令和７年度）

新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究

研究代表者　今村知明（奈良県立医科大学 公衆衛生学講座・教授）

研究要旨

本研究は、新型コロナ感染症収束後の食品提供形態の多様化を踏まえ、食品防御の課題整理と対策検討を目的として実施した。大阪・関西万博の調査により食品提供環境の対策状況を把握し、店頭販売品を含むガイドライン改訂の必要性を検討した。小売、飲食、製造施設の現地調査では監視体制や運用面の課題を整理し、感染症対策との調和および店頭販売品やデリバリー対応を踏まえガイドライン改訂とチェックリスト整備・英訳を行った。ロボット配膳では無人搬送による食品防御構造の変化と人的関与低下の影響、監視カメラ映像流出ではサイバーと物理の連鎖による供給停止リスクの波及性、地方自治体では相談対応による未然防止の実態と所管の不明確さを把握し、海外動向調査では食品不正、IA 規則、Codex における食品偽装ガイドライン、PAS96 改訂の動向を整理した。これらを踏まえ、サイバー攻撃を含む食品テロ対策、実践コストを踏まえたガイドライン改訂・普及を含む対策の方向性を整理した。

本研究における研究体制は以下の通り。

・今村 知明（奈良県立医科大学　公衆衛生学講座 教授）

・岡部信彦（川崎市健康安全研究所　参与）

・赤羽学（国立保健医療科学院 医療・福祉サービス研究部 部長）

・加藤礼識（茨城キリスト教大学　生活科学部 食物健康学科　講師）

・入江 芙美（九州大学医学研究院 医療経営・管理学講座 准教授）

A．研究目的

我々はこれまで、食品産業の内部及び外部環境の変化に対応した食品防御対策の検討を進め、多様なガイドラインの作成を行ってきた。しかしながら、新型コロナ感染症の収束後、食品販売業界においては自動レジや無人店舗等の自動化技術の進展により、非接触型のサービス形態が拡大している。さらに、ゴーストキッチンや食品配信プラットフォーム等の新たなビジネスモデルの発達により、食品提供形態は多様化している。このような背景のもと、従来の食品防御対策では十分に対応できない新たなリスクが顕在化している。

特に、新たな業態におけるサイバー攻撃を含む食品テロへの対応、地方自治体食品衛生行政における食品防御対策の在り方、さらに物価高や人件費高騰に対応した実効性の高い対策の構築が課題となっている。また、大阪・関西万博のような大規模イベントでは、多様な提供形態や複雑な動線への対応が求められ、従来ガイドラインの適用が困難である。

以上を踏まえ、本研究では新たな営業形態を含む広範な業種における食品防御上の課題を整理し、サイバーリスク及び行政対応を含めた総合的対策を検討するとともに、サイバー攻撃を

含む食品テロ対策や、事業者の実践コストを考慮したガイドラインの改訂及び普及を目指し、これを目的として研究を行った。具体的には、以下を明らかにするための研究を実施した。

- 大阪・関西万博などに向けて食品提供に関する食品防御対策の検討と提案（赤羽、入江、岡部、神奈川）
- フードチェーン全体の安全性向上に向けてのコロナ対策を踏まえた調査と食品防御対策ガイドライン等の改善と、同ガイドラインの普及（赤羽、入江、神奈川）
- 多様化した飲食物の販路（デリバリー等）における食品防御上の課題、特にロボット配膳システムへの食品防御対策の必要性に関する調査（加藤）
- 地方自治体食品衛生行政における食品防御対策の課題検討（岡部、赤星）
- 海外における食品防御政策、規格等の動向調査（今村）

B．研究方法

1．全体概要

研究は、A. に示した大きく 5 つの項目について、国内外の政府機関ウェブサイト・公表情報の収集整理、実地調査、検討会における専門家・実務家らとの討議を通じて実施した。

検討会の参加メンバーと開催状況は以下の通りである。（以下敬称略、順不同）

- 今村 知明（奈良県立医科大学 公衆衛生学講座 教授）
- 岡部 信彦（川崎市健康安全研究所 参与）
- 赤羽 学（国立保健医療科学院 医療・福祉サービス研究部 部長）
- 鬼武 一夫（日本生活協同組合連合会 品質保証本部 総合品質保証担当（Senior Scientist））
- 高畑 能久（大阪成蹊大学経営学部 経営学科 食ビジネスコース フードシステム研究室 教授）
- 神奈川 芳行（奈良県立医科大学 公衆衛生学講座 非常勤講師）
- 島﨑 眞人（一般社団法人日本農林規格協会 専務理事）
- 赤星 千絵（川崎市健康安全研究所 ウイルス・衛生動物担当）
- 温井 健司（厚生労働省 健康・生活衛生局食品監視安全課 課長補佐）
- 藤田 佳代（農林水産省消費・安全局食品安全政策課 食品安全危機管理官）
- 加藤 礼識（茨城キリスト教大学 生活科学部 食物健康学科 講師）
- 入江 芙美（九州大学医学研究院 医療経営・管理学講座 准教授）
- 亀本 啓子（大阪市健康局健康推進部生活衛生課 課長）
- 田中 昭次（大阪市保健所 保健主幹）
- 浅井 威一郎（川崎市健康安全研究所呼吸器・環境細菌担当課長補佐）
- 相原 俊介（川崎市健康福祉局保健医療政策部生活衛生課食品安全担当係長）
- 三亀 美津穂（川崎市健康安全研究所残留農薬・放射能担当）
- 名倉 卓（一般社団法人 日本能率協会 審査登録センター ＣＳ・マーケティング部）
- 平野 展代（一般社団法人 日本食品安全支援機構）
- 山口 健太郎（社会構想大学院大学コミュニケーションデザイン研究科 客員教授）
- 長田 瑞花（奈良県立医科大学公衆衛生学講座 大学院生）
- 一蝶 茂人（BSI グループジャパン株式会社）
- 河井 宏介（BSI グループジャパン株式会）
- 北條 健一（BSI グループジャパン株式会社）

（検討会の開催状況）

令和 7 年 5 月 27 日（火）（オンライン）

令和 8 年 1 月 27 日（水）（オンライン）

◆倫理面への配慮

本研究で得られた成果は厚生労働省に報告をしているが、一部意図的な食品汚染実行の企てに悪用される恐れのある情報・知識については、本報告書には記載せず、非公開としている。

２．分担研究について

２．１．１　大阪・関西万博などに向けて食品提供に関する食品防御対策の検討と提案

大阪・関西万博会場における現地視察調査を主たる方法として実施した。調査は 2025 年 7 月 3 日に実施され、入場ゲート、フードコート、キッチンカー、パビリオン等の複数の飲食提供形態を対象に観察・記録を行った。具体的には、①入場時の X 線検査・金属探知機・監視カメラによるセキュリティ体制、②厨房配置や提供動線、調味料配置等の物理的管理、③従業員の衛生行動やマスク着用状況等の人的管理、④廃棄物管理や施錠状況、⑤監視カメラ配置によるトレーサビリティ確保状況を評価項目とした。加えて、各施設における共通点および差異を整理し、食品防御上の脆弱性の有無を分析した。さらに、既存の食品防御対策ガイドライン（運搬・保管施設向け、調理・提供施設向け（令和 5 年度版））の枠組みと照合し、現場実態との整合性および改善点を抽出することで、実務的示唆の導出を行った。

２．１．２　食品防御対策のための現地調査

以下の３施設を対象に、研究班メンバーが直接訪問し、施設担当者の案内のもとで見学調査を実施するとともに、ヒアリングを通じて食品防御体制に関する情報を収集・整理した。

・小売店（某スーパーマーケット店舗）：2025 年 11 月 21 日

・飲食チェーン店舗（某回転寿司チェーン　店舗）：2025 年 11 月 14 日

・食品製造工場（某食品製造工場）：2026 年 2 月 2 日

２．２　フードチェーン全体の安全性向上に向けてのコロナ対策を踏まえた調査と食品防御対策ガイドライン等の改善と、同ガイドラインの普及

食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）（令和 5 年度版）の修正のため、令和 5 年度版に、新型コロナウィルス感染症対策及び第 3 者認証の要素および店舗販売品に関する要素および店舗販売品を加味した見直しを行った。加えて、近年、監視カメラの映像が海外サイトを経由または直接外部から閲覧可能となっている事例が報道されていることを踏まえ、監視カメラの管理方法についても検討し、必要な追記を行った。

２．３．１　新型コロナ感染症収束後におけるロボット配膳システムと食品防御の課題

ロボット配膳システムにおける食品防御上の課題を把握するため、文献調査および質的調査を組み合わせた研究方法を採用した。

まず、文献調査として、厚生労働科学研究報告書、食品防御に関する国内外ガイドライン、学術論文および行政資料を収集・整理し、基本概念や従来の対策枠組み、飲食店への適用可能性を検討した。これにより、導入以前の食品防御対策の構造を整理し、本研究の分析視点を明確化した。

次に、質的調査として、販売代理店 2 社および導入飲食店 1 社に対し半構造化インタビューを実施した。調査項目は導入目的、運用体制、食品防御対策の状況、接触行動の発生、トラブル対応主体、仕様変更の可能性、情報共有体制である。

インタビュー内容は整理・分析し、「人的監視体制」「物理的防御措置」「情報共有構造」の三側面から構造的課題を抽出した。なお、調査対象は匿名化し倫理的配慮を行った。

２．３．２　食品工場における監視カメラ映像流出リスクの検討―　サイバー時代の食品防御の課題 ―

研究方法の基本的枠組みとして、①文献・制度分析、②海外基準との比較、③事例分析、④事業者ヒアリング、⑤リスク構造モデル構築の五段階で実施した。食品工場における監視カメラ映像流出の影響を把握するため、制度分析および事例分析を中心に検討した。

1. 制度および規格の分析

食品防御およびサイバーセキュリティに関する国内外の制度・規格を対象に横断的分析を実施し、監視カメラ管理の制度上の位置づけに着目した。対象は国内指針、サイバー関連政策、IFS Food、NIS2、米国指針等とし、情報資産の扱い、事故報告義務、経営責任、IT・OT 分離、監視設備管理の観点から比較整理を行った。

2. 海外事例の系統的検索

食品産業におけるサイバー攻撃および IoT 機器関連事例の把握を目的として、政府資料、国際機関文書、学術論文、報道等を対象に系統的検索を実施した。対象期間は直近 10 年を基本とし、特に 2018 年以降の事例を重点的に収集した。

検索は英語を中心に、攻撃類型、対象産業、技術領域（OT、IoT 等）の観点からキーワードを組み合わせて実施し、複数情報源で照合した。検索条件および手順は記録し、再現性を確保した。

抽出事例は、食品供給への影響に着目して選定し、小規模事例や情報不足事例を除外した。分析は統一的枠組みに基づき、侵入経路、権限拡大、被害拡大要因、操業停止および供給影響、政策対応の観点から整理した。

２．４　地方自治体食品衛生行政における食品防御対策の課題検討

本研究における検討のため、研究協力者間の対面での打ち合わせを 3 回及びメール会議を随時実施し、昨年度に引き続き以下の 2 点を実施した。

１．実態調査

(調査 1) 他自治体における食品防御対策の状況調査

以下のアンケート調査を実施した。

・対象：関東甲信越静ブロックに属する各都県市・特別区の食品衛生主管課

・実施時期：2025 年 11 月

・方法：対象にメールで案内を送付し、設問内容（別添 1）に回答を記載するか、同様の設問内容について LoGo フォームに回答を入力するよう依頼した。

・結果還元：対象に集計結果をメールで送付した。

(調査 2) 食品防御に関連する相談の実態調査

保健所の食品衛生監視員が受けた相談のうち、事業者からの対策相談や食品への意図的な混入事例相談の割合を調べるため、2020 年～2024 年に川崎市の保健情報システムに記録された苦情相談対応のデータベースを解析した。

２．教育訓練や食品防御対策の内容検討

昨年度確認した以下の検討スタンスを念頭に、取り入れやすい教育訓練や対策について、今年度から来年度にかけて具体的に検討する。

【検討スタンス】食品衛生対策とのバランスや保健所の状況を踏まえ、食品防御の視点に偏らないように、かつ、防御的案件が懸念される場合に適切な対応が取れるように、食品衛生対策の中に食品防御の視点を適度に加えていく。

２．５　海外における食品防御政策、規格等の動向調査

米国 FDA（Food and Drug Administration）が施行・管理する FSMA 法に関する更新事項のうち、特にフードディフェンスおよびフードフラウドに関連する内容について、その最新の動向を整理

した。あわせて、コーデックス委員会（Codex Alimentarius Commission）総会およびCCFICS（食品輸出入検査・認証制度部会）におけるフードディフェンスに関する検討議題と、その進捗状況について整理した。
さらに、英国 BSI を中心として進められているPAS96（第5版）の改訂作業については、開発担当者への聞き取り調査を実施し、その進捗状況を整理した。

C．研究結果

本年度研究によって以下の成果を得た。詳細については、それぞれの分担研究報告書を参照されたい。

１．１.大阪・関西万博などに向けて食品提供に関する食品防御対策の検討と提案

現地視察調査による各施設における意図的な食品汚染に関する脆弱性分析の結果を以下に示す。パビリオンAは日本の食文化を発信する施設であり、体験プログラムや複数のテイクアウト中心の販売ブース、期間限定ブースが設置され、1日1万人以上が来場していた。脆弱性については、直接接触可能食材、洗浄・加熱工程の有無、薬品等の管理、混入・すり替えリスク等の観点から確認を行った結果、該当するリスクは確認されなかった。薬剤は外部業者が管理し、アルコールは従業員の目が届く位置に配置されていた。食材搬入は営業前に限定され対面受取とし、来場者動線と交差しない構造で、裏口は施錠可能であった。また、各ブースに冷蔵・冷凍設備が設置され、監視カメラは死角なく配置されていた。

B 国パビリオンは文化・技術等を紹介する展示施設で、1 階のレストランにおいて各種料理が提供されていた。同様の観点で確認した結果、接触可能食材、未加熱食品、薬品放置、混入リスクはいずれも確認されなかった。アルコールは入口に設置され、調理場は奥に配置されカウンター受取方式であり、テーブルに調味料は設置されていなかった。退席後のアルコール消毒も実施されていた。
万博会場ではフードコート、キッチンカー、店舗販売など多様な形態で飲食提供が行われていた。東ゲートではX線検査および金属探知機による入場管理が実施され、屋外には多数の監視カメラが設置されていたが、一部店舗では未設置箇所が確認された。飲食提供エリアでは調理場を奥に配置したカウンター受取方式が採用され、調味料は従業員管理下に置かれていた。キッチンカーでは食材管理が徹底され、発電機は使用されておらず、ゴミ箱や灰皿は施錠管理されていた。一方、一部で顎マスク着用や衛生管理のばらつきが見られ、当日未確認ではあるが販売ルール違反の可能性に関する情報もあった。

結果の詳細については分担研究報告書を参照されたい。

１．２.食品防御対策のための現地調査

2025 年 11 月 21 日、某スーパーマーケットにおいて複数機関の研究者が参加し見学調査を実施した。搬入エリアは区画され夜間施錠可能で、搬入時間は 05:00～22:00 に制限されていた。搬入車両は 1 日約 10 台で時間帯により集中が見られた。勤怠はタイムカード方式で、代理打刻は指導により是正されており、帽子着用により顔識別が困難なため名札確認を徹底し、外部者はストラップ付き名札で区分していた。バックヤード間の往来は限定的で、消毒用アルコールの配置および一体型刃物の使用が確認された。商品不良は年間約 11,000 件で、異物混入は約 3,200 件（約 30%）、

うち店舗起因は約 500 件であり、主な非意図的混入は残骨、フィルム片、機械部品、毛髪・虫等であった。意図的混入が疑われる事例は過去にバナナへの縫い針混入 1 件のみ（警察届出済み、未解決）であった。要員への教育は年 1 回の研修とテスト、月次点検、年次監査が実施されていた。課題として、バックヤードに監視の死角がありカメラ増設の必要性、設備や作業ルールの不統一、整理整頓の徹底不足、外国人採用増加への対応や労働環境改善の必要性が示された。

また、2025 年 11 月 14 日には某回転寿司チェーン店舗にて見学およびヒアリングを実施した。アルバイト比率は約 10%、外国人は 20～25%で、指導および記録管理が行われていた。客テロ対策として禁止事項の表示、卓上設置物の削減、オーダー制導入が行われていたが、客席はカメラ監視下にある一方で背もたれにより死角が存在した。店内はキッチンとホールが区分されカメラと目視で管理されており、接客が客テロ防止に重要であることが確認された。対策として同意画面の導入、卓上食品の撤去、セルフコーナー化、カトラリー管理の集約が提案された。

さらに、2026 年 2 月 2 日には某食品製造工場にて見学調査を実施した。ゾーニングや IC タグによる入室管理、ロボット清掃、粘着ローラーおよび手洗い工程により衛生管理が行われていた。原材料は QR コードで管理され、開封時のカメラ確認や製造工程におけるふるい、専用開封、X 線検査が実施されていた。課題として共連れ対策の困難、照明や死角の把握、工具管理の必要性が指摘され、録画保存期間の見直し、薬品管理の複数人対応、廃棄物管理の徹底が必要とされた。落下物管理、相談体制、新人ケア等の運用も確認され、異常対応については初期段階からのアラート運用の必要性が示された。

結果の詳細については分担研究報告書を参照されたい。

２．フードチェーン全体の安全性向上に向けてのコロナ対策を踏まえた調査と食品防御対策ガイドライン等の改善と、同ガイドラインの普及

食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）（令和 5 年度版）について、店頭販売品を「営業許可や製造許可を受けた実店舗で調理された料理等を容器に入れ、店舗の敷地内で販売される商品」と定義し見直しを行った。優先的に実施すべき対策では、大規模イベント時における店頭販売品の増加を踏まえ「調理・提供」に店頭販売品を含める旨を追記し、人的要素では私物持込み確認の対象を販売現場へ拡張した。部外者対応では業者の持ち物確認に店舗を追加し、施設管理では受渡し場所、無人時間帯の店舗、飲食料品保管庫、洗剤・殺虫剤の保管、監視カメラ管理（映像流出への注意を含む）等を追加・修正した。入出荷等の管理では容器や店頭販売品を対象に含め、保管中の数量管理にも反映した。また、可能な範囲での対策および大規模イベント時対応においても同様に店頭販売品の位置づけを明確化し、監視カメラ設置では受渡し場所を対象に追加した。

中小規模向けガイドラインについても同様に「調理・提供」に店頭販売品を含める旨を追記し、危機管理体制、私物持込み確認、無人時間帯の店舗管理、監視カメラ管理の新設等を行った。入出荷等の管理では積み下ろし監視や数量管理に店頭販売品を含め、対応体制に購入者を追加した。さらに大規模イベント時対応では、販売場所での異物混入防止、監視カメラ設置における受渡し場所の追加、厨房の防犯・監視体制の強化および共有キッチン使用前後の異常確認を追加した。

フードデリバリーサービス提供事業者及び利用事業者向けチェックリストについては、施設管理に監視カメラ管理の項目を新設した以外に変更はなかった。配達員向けチェックリストについては現時点で大きな修正は行われなかった。これらフードデリバリーサービス提供事業者及び利用事業者向けチェックリスト、ならびに配達員向けチェックリストの英訳版を作成した。

結果の詳細については分担研究報告書を参照されたい。

３．１.新型コロナ感染症収束後におけるロボット配膳システムと食品防御の課題

文献調査、および販売代理店 2 社および導入飲食店 1 社への聞き取り調査により、ロボット配膳システムの普及背景、運用実態、食品防御上の課題を整理した。ロボット配膳は、労働力不足、人件費上昇、感染症対策に伴う非接触需要、顧客体験向上等を背景に導入が進んでおり、単なる業務効率化にとどまらず、店舗内のリスク構造を変化させる要素であることが確認された。

食品防御上は、親しみやすいデザインや食品を載せた無人搬送により、顧客の接触行動や意図的・偶発的接触の余地が生じる可能性が示された。また、触知部と食品部の物理的分離不足、搬送中の監視の空白、人的監視による心理的抑止力の低下が課題として整理された。カバー等の物理的対策は有効と考えられる一方、利便性、作業効率、デザイン性への影響から採用が進みにくい状況も確認された。

販売代理店では、ロボットを食品を運ぶ機器として捉え、食品の安全管理は導入店舗の責任範囲と認識する傾向があり、いたずらや過度な接触等のトラブル情報も体系的に収集されていなかった。また、多くが海外メーカー製であるため、国内の改善要望を設計へ反映させるには制約があり、設計・販売・運用の各段階で責任が分散する構造が確認された。

導入店舗では、ロボット配膳により従業員を客席巡回、顧客対応、不審行動の観察、トラブル初期対応に再配置する運用が確認された。現場では接触、走行妨害、下膳時の不衛生化、意図的行為の潜在性がリスクとして挙げられた一方、ロボットが重量物運搬や定型ルート移動を担い、人が最終確認、監視、異常対応を担う補助的自動化の役割分担も確認された。以上より、ロボット配膳は運用次第で食品防御上のリスクを高める可能性がある一方、人的資源の再配置により監視体制を強化する契機にもなり得ることが示された。

結果の詳細については分担研究報告書を参照されたい。

３．２.食品工場における監視カメラ映像流出リスクの検討― サイバー時代の食品防御の課題―

国内外の制度・規格比較により、食品防御におけるサイバーリスクの位置づけには国ごとの差異が確認された。米国では食品産業が重要インフラとして位置づけられ、FSMA や CISA の枠組みにより食品防御とサイバーセキュリティが一体的に扱われ、ネットワーク接続機器や IoT 機器もリスク対象とされている。EU では NIS2 指令によりリスク管理、経営層責任、24 時間以内の報告義務が制度化され、IFS Food 規格においても監視設備やアクセス管理を含むリスク評価が求められているなど、サプライチェーン全体を対象とした管理が行われている。

これに対し日本では、食品防御は主として物理的対策中心であり、サイバーセキュリティは別分野として扱われる傾向がある。そのため、監視カメ

ラ等のネットワーク接続機器について、食品防御の枠組み内での位置づけが必ずしも明確ではない。海外では監視カメラやIoT機器は侵入経路や情報資産としてリスク評価対象に含まれるのに対し、日本では主に防犯設備や個人情報管理の観点で扱われる傾向が確認された。

以上の比較から、日本における制度上の課題として、①食品防御における情報資産の位置づけの不明確さ、②サイバー事故と食品防御を結びつけた報告・共有制度の不足、③経営層責任やBCPとの連動の弱さが整理された。これにより、監視カメラ映像流出等の事案が食品防御の課題として体系的に整理されにくい構造が示された。

４.地方自治体食品衛生行政における食品防御対策の課題検討

食品防御対策の実態把握として自治体調査および相談データ分析を実施した。自治体調査では、食品防御対策を事務分掌に含むと回答した自治体は56自治体中8自治体（14%）であったが、明文化は確認されなかった。また、明文化されていないが対応している自治体を含めると 18 自治体（32%）であり、多くは制度として明確に位置づけられていない状況であった。イベント時の普及啓発の実施は1自治体にとどまり、食品防御的助言の経験がある自治体も18自治体(32%)であった。一方で、約9割の自治体は相談対応経験がない状況であった。意図的混入および化学物質混入に関する食中毒事例はいずれも 2 自治体で報告され、原因特定や対応に課題が見られた。

川崎市の苦情相談データ（2020～2024 年、総数11,689 件）から、14 キーワードにより 1,268 件を抽出し､そのうち食品防御的視点を有する69件を整理した。内訳は意図的混入が否定できない事案39件、未然防止関連30件であった。意図的混入疑い事案は特定年度に増加が見られ、相談者は消費者が多く、対象は異物が中心であった。未然防止関連は近年増加傾向を示し、営業者からの相談が多く、保健所からの助言により食品防御対策が付加される事例が多かった。対策内容としては、営業者の目が行き届かない場所の食品管理が最も多く、営業中の管理監視、調理場管理、共用食品管理が確認された。

以上の結果から、食品防御対策は制度としての明確な位置づけが限定的である一方、現場においては相談対応や助言を通じて対応が進められており、特に未然防止の観点は近年重要性が高まっていることが示された。

また、本研究の内容を踏まえ、令和８年３月５日に川崎市において食品防御対策研修会が開催され、事業者および食品衛生監視員を対象に講演およびグループワークが実施された。

結果の詳細については分担研究報告書を参照されたい。

５.海外における食品防御政策、規格等の動向調査

FDAは2025年9月2日、輸入冷凍シーフード28検体の正味重量表示を調査し、10 検体（36%）に短量(short-weighting)違反（2.3～9.9%）を確認し、当該貨物を輸入拒否とした。本調査は2022～2024年のEMA対策の一環であり、氷衣重量の不適切算入が要因とされ、当該行為は経済的動機による不正（Economically Motivated Adulteration：EMA）および食品不正に位置づけられる。対象はエビ25、イカ2、ティラピア1で、4か国12社由来であった。違反は規制措置や刑事調査の対象となり得るほか、Import Alert 99-47等により監視されている。

CPGM 7303.842（2025年9月30日）では、EMAお

よび食品不正に関する特別指示として、受入記録と表示の照合および必要に応じた Form 483 への記録が示され、魚種置換等が毒素・アレルゲン・ヒスタミン中毒と関連し得ることが示された。食品不正および EMA は査察対象として実務上取り扱われている。

FDA は 2025 年 8 月 28 日、EMA を食品中成分の除去・置換・添加等による価値操作と定義し、これを食品不正と位置づけた。対象は食品、飼料、化粧品に及び、誤表示に該当し得る。シーフードにおける魚種置換や氷による重量増加、はちみつ等の例が示され、健康被害の可能性も指摘されている。

FSMA の IA 規則では、極小規模事業者の基準額が 1,000 万ドルから 13,318,941 ドルへ更新され、適用日は事業規模別に設定されている。対象施設は脆弱性評価および防御計画の策定・実施が求められる。EMA とは区別され、2025 年時点で要求事項の改正は確認されなかった。

Codex では食品偽装ガイドラインが 2024 年 11 月に Step5 採択され、2025 年以降も EWG で検討継続中である。本年度内の本会合開催や新規文書公表は確認されなかった。

PAS96 第 5 版改訂は 2023 年開始後遅延し、2025 年 12 月にドラフトが公開され、2026 年 2 月 1 日までパブリックコンサルテーションが実施された。本規格は意図的攻撃（不正混入、恐喝、サイバー攻撃等）を対象とするガイダンスであり、TACCP を含むリスク評価体系が示されているが、最終版は未公表であり、最終的な内容は未だ確定していない状況であった。

結果の詳細については分担研究報告書を参照されたい。

D．考察

１．１．大阪・関西万博などに向けて食品提供に関する食品防御対策の検討と提案については、会場内に多数の飲食提供施設が出展される中で、食品衛生に加えて食品防御への対応の重要性が増していると考えられた。本調査結果から、物理的対策（ハード）および運用的対策（ソフト）の両面において高水準で整備されていることが確認され、特に入場ゲートにおける空港レベルのセキュリティ、会場全体の監視カメラ配置、受け渡しカウンター方式の採用は、外部からの意図的混入リスク低減に有効な措置であった。今後の食品防御ガイドラインへの反映に関しては、「運搬・保管施設向け」では新たな追加項目は認められなかった一方、「調理・提供施設向け」では店頭販売品への対応を踏まえた修正を行い、タイトルを「調理・提供（店頭販売品を含む）」へ変更することが望ましいと考えられる。また、「大規模イベント時に必要な対応」として、「監視カメラの設置」に店頭販売品の受渡し場所を追加することが望ましいと考えられる。

１．２.食品防御対策のための現地調査については、小売店、飲食チェーン店舗および食品製造工場の３施設において食品防御上の課題が確認された。小売店では、監視カメラの死角（特にバックヤード、水産、ベーカリー作業室）、作業環境やルールの不統一（蛍光灯カバー、エプロンのポケット等）、外国人労働者増加への対応が主要な課題であった。飲食チェーン店舗では、オーダー制の導入や卓上食品の管理見直し等、業態特有のリスク低減策が具体化され、特に顧客との衛生意識の共有（同意ボタン等）が客テロ抑止に有効であることが示唆された。食品製造工場では、IC タグや多数のカメラ活用などの先進的な取り組み

が見られた一方で、共連れ対策、薬品庫の複数人管理、廃棄物の即時搬出等、運用面における改善余地が明らかとなった。いずれの施設においても、従業員教育および管理体制の整備が食品防御強化の鍵であり、物理的対策（ハード）とルール・教育（ソフト）の両面から継続的な改善が求められる。

２．フードチェーン全体の安全性向上に向けてのコロナ対策を踏まえた調査と食品防御対策ガイドライン等の改善と、同ガイドラインの普及については、食品防御対策ガイドライン（令和５年度版）の多くの項目が新型コロナウィルス感染症対策としての有用性も併せ持つことが確認されており、感染症対策と食品防御対策は相互に関連し得るものと考えられた。また、感染症対策は「新たな日常」として定着しつつある一方で、人々のリスク意識に応じて変化するものであることから、今後新たな感染症が流行した際には、本ガイドラインを参考に食品防御対策との調和を考慮した具体的対策を検討する必要がある。さらに、長期間にわたる大規模イベントにおいては、店頭販売品を購入し会場内で飲食する形態が想定されるため、従来の施設内での調理・提供に加え、店頭販売時の対応にも留意が必要であり、複数事業者の関与や施設の共用といった特性を踏まえ、共有部分への対策やスタッフ教育の重要性が示唆された。加えて、フードデリバリーサービスにおいては、配達員が単独で行動するという特性から、従業員間の相互監視に依存していた従来の管理とは異なる課題が存在し、スマートフォンのGPS 機能等の活用は既に一定程度実施されているものの、配達員の契約形態や就労実態により、身元確認や教育の実効性確保には制約があることが明らかとなった。このため、チェックリストの英訳版を作成し、海外出身者にも対応可能な形とすることで汎用性の向上が図られており、今後は多言語化の進展と活用が期待される。また、各ステークホルダーが実施可能な対策を組み合わせることにより、フードデリバリーサービスのサプライチェーン全体として食品防御対策の実効性を高める必要がある。なお、本ガイドラインにおける「監視カメラ」という表現については他の呼称の適否も含め、今後検討が必要である。

３．１．新型コロナ感染症収束後におけるロボット配膳システムと食品防御の課題については、ロボット配膳が業務効率化や労務負担軽減に寄与する一方で、食品防御の観点から従来の管理構造を変容させる要素を有していると考えられる。特に、人が担っていた物理的管理、視覚的監視、心理的抑止の機能が分離され、食品が無人状態で搬送される構造が生じることにより、従来の前提が変化し、構造的脆弱性が形成され得ることが示唆される。この変化は、多層防御の観点から見ると、従来の防御層の一部が弱体化する一方で、人的配置や運用設計により再構築が可能であり、さらに技術的手段による新たな防御層の導入余地も存在することを意味すると考えられる。具体的には、物理的防御については食品が露出した状態で搬送されることから完全な遮断ではなく接触機会低減を前提とした設計が求められると考えられ、人的防御については省人化のみを進めた場合には弱体化する可能性があるが、業務再配分により巡回や監視を強化することで補完可能であると考えられる。また、心理的防御は機械化により低下する可能性がある一方、人の目を意識的に配置することで維持され得ることが示唆される。さらに、トラブル情報の共有や蓄積といった情報防御層は未整備であり、体系的な報告・共有の仕組み

の必要性があると考えられる。一方で、ロボット自体にはカメラやセンサー等を活用した新たな監視・検知機能を付加できる可能性があり、従来にはない技術的防御層の構築余地も存在すると考えられる。以上より、ロボット配膳環境における食品防御は、防御層が減少したのではなく構成が変化したものと捉えることが適切であり、その再配置と再設計を前提とした対応が必要であると考えられる。

３．２．食品工場における監視カメラ映像流出リスクの検討―サイバー時代の食品防御の課題―については、食品防御の考え方が従来の物理的対策中心から、サイバーと現場が結びついた統合的なリスク管理へ変化しつつあることが示唆された。スマート化やIoT機器の普及により、監視カメラや製造設備がネットワーク接続される中、防御設備自体が不正アクセスの対象となり得る構造が生じており、映像流出は単なる情報漏えいにとどまらず、工場内部の構造や管理状況の把握を通じて、物理的侵入や妨害行為のリスクを高める可能性があると考えられる。このことは、防御設備が攻撃を支援する情報源となり得る新たな課題を示している。

また、食品防御とサイバーセキュリティが制度および組織上分断されていることにより、監視カメラ等の責任所在が不明確となり、事故時の統合的対応や再発防止が困難となる可能性が示唆された。特に経営層の関与が限定的な場合、リスクが部門単位に分散し、供給停止リスクとして十分に評価されない構造が存在すると考えられる。

さらに、映像流出は、不正アクセス、情報取得、物理的妨害、操業停止、サプライチェーンへの影響という連鎖を通じて、食品供給全体に影響を及ぼす可能性がある。特にセントラルキッチン等の集約型施設では、単一拠点の停止が広範な供給停止につながる可能性があり、その影響は社会的基盤にも及ぶと考えられる。

加えて、現場では高度な技術不足よりも、パスワード管理、アクセス権限、ログ確認、機器更新等の日常運用の不備がリスク要因となる傾向が見られ、対策は技術導入だけでなく運用体制や責任の明確化に依存することが示唆された。特に中小規模事業者では人材やコスト制約により対策が限定的となる可能性があり、ガイドラインが実務に十分反映されない課題も確認された。

以上より、監視カメラ映像流出は単なる情報管理問題ではなく、供給停止リスクの前段階として位置づける必要があり、食品防御はサイバーと物理を統合した視点で再構築されるべきであると考えられる。また、この課題は個別企業にとどまらず、食品供給の安定性や経済安全保障とも関係し、組織横断的かつ制度的対応が求められると考えられる。

４．地方自治体食品衛生行政における食品防御対策の課題検討については、食品衛生行政機関の現状把握を目的として実施したアンケート調査および苦情相談データの解析結果を踏まえ、有事対応と未然防止の観点から整理した結果が示唆された。

有事対応については、56自治体の保健所において過去3年間に意図的混入と把握された食中毒事例は1事例のみであり、混入原因不明の化学物質事例を含めても計3事例と少ない傾向にあると考えられた。一方で、対応においては助言内容の検討や警察との連携に苦慮する状況がみられ、特に相談者が意図的混入を疑う場合に警察への相談を促しても理解が得られないなど、所管の不明確さが課題である可能性が示唆された。また、意図的

混入が否定できない相談は 5 年間で 39 件確認され、同様に警察相談を助言する事例が含まれていたことから、各自治体に一定程度存在する事象であると考えられた。監視カメラにより確認された事例がある一方で原因不明の事例も多いと推察され、重大事案の早期探知や未然防止に向けた対応の整理が今後の課題であると考えられる。

未然防止については、食品防御の所管が関係法令上明確でない中で、56 自治体中 32%が業務として可能な範囲で対応していることが確認され、その多くは事業者からの相談対応における助言を通じて対策を推進している実態があると考えられた。また、イベント時に食品防御対策の普及啓発を行っている自治体もみられた。さらに、未然防止に関わる相談件数は 2022 年以降増加しており、過去のアンケート調査や研修会の実施により保健所側の助言機会が増加した影響である可能性が示唆された。

今後は実態のさらなる把握を進めるとともに、負担が少なく効果的な対策の検討および教育訓練内容の整理が必要であると考えられる。

５．海外における食品防御政策、規格等の動向調査については、食品不正および食品防御に関する考え方が、定義、規制、運用の各レベルで体系的に整理されていることが示唆された。

FDA による輸入冷凍シーフードの調査では、正味重量の不適合が一定割合で確認され、特に氷衣を含めた重量表示が問題とされていることから、冷凍製品特有の表示管理の重要性が示された。また、違反製品が輸入拒否の対象とされていることから、当該不適合は規制措置に直結する事項として扱われており、EMA および食品不正の一形態として整理されていることが示唆された。

さらに、FDA の査察プログラムでは食品不正および EMA が確認事項として明示され、受入記録と製品ラベルの照合等により実務上運用されていることが確認された。また、これらがアレルゲンや毒素等の危害要因と関連し得ることから、食品安全の観点を含めて管理対象とされていることが示唆された。加えて、EMA と食品不正が同一概念として整理され、魚種の置換や重量の水増しといった事例と整合していることから、定義と運用の一貫性が確認された。

IA 規則については、2025 年時点で大きな変更はなく、基準更新や情報提供が継続されており、EMA とは区別された制度として運用が維持されていると考えられる。また、脆弱性評価およびフードディフェンス計画の策定が引き続き求められていることが確認された。

Codex における食品偽装ガイドラインは、ステップ 5 到達後も電子作業部会による検討が継続されている一方で、本会合の開催や新規文書の公表は確認されておらず、大きな進展は見られていない状況にあると考えられる。

PAS96 の改訂については、遅延を経てドラフトが公開されパブリックコンサルテーションが実施されたことから公開段階に移行したが、最終版は未公表であり、現時点では確定していない段階にあると考えられる。

Ｅ．結論

１．１．大阪・関西万博などに向けて食品提供に関する食品防御対策の検討と提案については、大阪・関西万博における食品防御対策が国際的大規模イベントとして高い水準で構築されており、入場管理、監視体制、厨房設計、提供方式において、食品への意図的混入リスクを低減する実践的な対策が講じられていた。一方で、食品防御対策ガイドラインの「運搬・保管施設向け」および「調

理・提供施設向け」の改訂案等も踏まえ、脆弱な部分への対応が必要であると考えられた。

１．２．食品防御対策のための現地調査については、3 施設の調査を通じて各業態における食品防御上の脆弱性と改善課題が把握され、小売店・飲食チェーン・製造工場に共通して、監視体制の強化、作業環境の整備、従業員教育の充実が必要であることが示された。また、本調査の知見は食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け等）の改訂および普及活動に活用される予定である。

２．フードチェーン全体の安全性向上に向けてのコロナ対策を踏まえた調査と食品防御対策ガイドライン等の改善と、同ガイドラインの普及については、食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）および中小規模事業者向けガイドラインの双方について、新型コロナウィルス感染症対策との調和および大規模イベントにおける店頭販売品への活用を踏まえた修正を行った。また、フードデリバリーサービス提供事業者および利用事業者向けチェックリストについては、事業者の実態を踏まえた確認を行い、海外出身の配達員による活用を考慮した英訳版を試作した。

３．１．新型コロナ感染症収束後におけるロボット配膳システムと食品防御の課題については、ロボット配膳が食品搬送を無人搬送を含む形態へ転換させることにより、食品防御の前提条件を変化させることが示された。これに伴い、運用によって防御機能が弱体化する場合と強化される場合があること、また食品防御は多層防御として再設計する必要があることが明らかとなった。さらに、設計・販売・運用間の責任分散や情報共有体制の未整備が課題として示された。今後は、ロボット配膳に対応したガイドライン整備、情報共有体制の構築、責任の明確化を通じ、人的監視を前提とした適切な運用モデルの確立が必要であると考えられる。

３．２．食品工場における監視カメラ映像流出リスクの検討―サイバー時代の食品防御の課題―については、監視カメラ映像の流出が単なる情報漏えいにとどまらず、供給停止につながる可能性を有する前段階の事象であることが示された。従来の食品防御は物理的対策を中心として構築されてきたが、工場のネットワーク化により情報流出が物理的脅威と結びつく可能性が明らかとなった。制度面では、海外が統合的に扱うのに対し、日本では分断され、監視カメラ等の情報資産に関する責任の所在が不明確となる課題が示された。また、監視カメラ映像流出は不正アクセス等を起点として操業停止やサプライチェーンへの影響に至る可能性があり、重要な出発点となり得ることが確認された。さらに、課題は技術面に加え、日常運用や部門間連携、責任体制といった組織的要因に依存することが示された。以上より、食品防御はサイバー領域を含めた統合的視点で再構築する必要があり、今後は情報資産の位置づけの明確化、責任体制の整理、制度的枠組みの統合が求められると考えられる。

４．地方自治体食品衛生行政における食品防御対策の課題検討については、行政機関において食品衛生対策の中に食品防御の視点を適切に組み込み、食品衛生監視員による苦情相談対応を通じた発生予防対策を検討する必要があることが示された。また、未然防止に関する所管が不明瞭な自

治体が多い状況を踏まえ、食品事業者等の相談窓口として食品衛生行政機関の役割を明確化する必要があると考えられる。

５．海外における食品防御政策、規格等の動向調査については、FDA において食品不正 (Food Fraud) および EMA への対応が、short-weighting を含め規制措置および査察運用の中で一貫して実施されていることが確認された。FSMA に基づく IA 規則については、新たな改正は確認されず、既存制度の運用が継続されている状況であった。コーデックス委員会の食品偽装ガイドラインは検討段階が継続しており、PAS 96（第 5 版）についてはドラフト公開およびパブリックコンサルテーションの実施により改訂プロセスが進行中であることが確認された。以上より、食品防御および食品不正に関する国際動向は、FDA において実務運用が継続的に進められる一方、国際規格は検討・改訂段階にあることが示されており、今後もその進展状況を継続的に把握する必要があると考えられる。

F．健康危険情報

なし

G．研究発表

１.論文発表

甲斐剛志、葛西伶乃凛、古澤魁世、菊島優菜、岩崎雄介、伊藤里恵、田口貴章、堤智昭、今村知明、穐山浩．食品テロ対策のためのヒト血液中のシアン化物イオン及びチオシアン酸イオンの同時分析法の確立．日本食品科学学会誌．32 (1) :10-14, 2025. 島津賞受賞

畠山理沙、佐々木国玄、赤星千絵、小河内麻衣、駒根綾子、清水英明、渡辺麻衣子、工藤由起子、岡部信彦． 流通食品表面における SARS-CoV-2 汚染実態調査について．食品衛生学雑誌　66(5): 106-111, 2025.

長田瑞花, 多川優也 , 田崎ひなた, 藤内琉成 , 今村知明, 加藤礼識．飲食店における食品防御対策の新たな課題「ロボット配膳システム」における食品防御対策の検討．食品衛生研究 (Food Sanitation Research),76 巻　1 号, 9-19 , 2026 年 01 月.

２．学会発表

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その①～販売代理店への聞き取り調査．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その②～飲食店への聞き取り～．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

加藤礼識、長田瑞花、多川優也．飲食物販売が多様化する中で食品防御対策はどのように変化したのか～大規模食品工場から小規模飲食店での対策への変化．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

加藤礼識、長田瑞花、多川優也．小規模な飲食店舗における食品防御対策 「バイトテロ」・「客テロ」をどう防ぐべきなのか？．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

田口貴章、小川亮介、穐山浩、今村知明 、堤智昭．意図的混入対策としての加工食品中の界面活性剤分析法の検討．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

加藤礼識、長田瑞花、多川優也、平子ほほみ、神奈川芳行、今村知明．多様化した飲食物販売における食品防御対策～これまでの食品防御対策の流れ～．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

平子ほほみ、多川優也、長田瑞花、加藤礼識、高畑能久、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　飲食店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡

長田瑞花、加藤礼識、多川優也、平子ほほみ、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　販売代理店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡

神奈川芳行、赤羽学、高畑能久、加藤礼識、入江芙美、山口健太郎、今村知明．大規模イベントでの食品防御対策と食品防御対策ガイドライン英訳の意義．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

H．知的財産権の出願・登録状況

１．特許取得　なし

２．実用新案登録　なし

３．その他　なし

厚生労働科学研究費補助金（食品の安全確保推進研究事業）
「新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究」分担研究報告書（令和７年度）

大阪・関西万博などに向けて食品提供に関する食品防御対策の検討と提案

研究分担者 赤羽 学（国立保健医療科学院 医療・福祉サービス研究部 部長）
研究分担者 入江 芙美（九州大学医学研究院 医療経営・管理学講座 准教授）
研究協力者 神奈川芳行（奈良県立医科大学 公衆衛生学講座 非常勤講師）

研究要旨

大規模イベントでは、多様な食品提供形態が存在し、物流の複雑化や来場者の集中により、食品の意図的な汚染や異物混入のリスクが高まる。近年、食品への意図的混入リスクは、テロのみならず内部不正を含む多様な脅威として認識されており、特に多数の来場者を受け入れるイベントでは、その影響は極めて大きい。本研究では、大阪・関西万博という国際的大規模イベントにおける食品提供環境を対象に、食品防御の観点から現場実態を把握し、その有効性および課題を明らかにすることを目的に、入場ゲートの高度なセキュリティ、監視カメラの配置、厨房構造、提供オペレーション、廃棄物管理等に着目し、食品防御対策の実装状況を実地で確認した。その結果、全体として多層的かつ高度な管理体制が構築されている一方で、運用のばらつきや人的要因に起因する改善余地も確認された。これを踏まえ、別の分担研究「フードチェーン全体の安全性向上に向けてのコロナ対策を踏まえた調査と食品防御対策ガイドライン等の改善と、同ガイドラインの普及」において、食品防御対策ガイドライン運搬・保管施設向け（令和５年度版）及び調理・提供（店頭販売品を含む）施設向け（令和５年度版）の改訂を行う予定となっている。

本分担研究においては、これらの実地調査と過去の大規模イベント時の事例を踏まえ、大規模イベントに適用可能な食品防御対策を検討した。

A. 研究目的

大阪・関西万博会場における飲食提供環境を対象に、食品防御の実装状況を体系的に評価し、実効性のある対策モデルを抽出することである。具体的には、①入場管理・監視体制・厨房設計・提供オペレーションなどのハード・ソフト両面の対策状況を整理すること、②フードコート、キッチンカー、パビリオン等の異なる提供形態におけるリスク差異を明確化すること、③現場運用におけるばらつきや人的要因の影響を分析することを目的とする。さらに、得られた知見を既存の食品防御ガイドラインと照合し、大規模イベントに適した実践的かつ標準化可能な対策の提示を目指す。

B. 研究方法

大阪・関西万博会場における現地視察調査を主たる方法として実施した。調査は 2025 年 7 月 3 日に実施され、入場ゲート、フードコート、キッチンカー、パビリオン等の複数の飲食提供形態を対象に観察・記録を行った。具体的には、①入場時の X 線検査・金属探知機・監視カメラによるセキュリティ体制、②厨房配置や提供動線、調味料配置等の物理的管理、③従業員の衛生行動やマスク着用状

況等の人的管理、④廃棄物管理や施錠状況、⑤監視カメラ配置によるトレーサビリティ確保状況を評価項目とした。加えて、各施設における共通点および差異を整理し、食品防御上の脆弱性の有無を分析した。さらに、既存の食品防御対策ガイドライン（運搬・保管施設向け、調理・提供施設向け（令和 5 年度版））の枠組みと照合し、現場実態との整合性および改善点を抽出することで、実務的示唆の導出を行った。

◆倫理面への配慮

本研究で得られた成果は厚生労働省に報告をしているが、一部意図的な食品汚染実行の企てに悪用される恐れのある情報・知識については、本報告書には記載せず、非公開としている。

C. 研究結果

１．パビリオン A（飲食販売および飲食体験ブース）における意図的な食品汚染に関する脆弱性

１．１　訪問先の概要

2025 年の国際博覧会に出展されたパビリオン A は、日本の食文化の魅力を発信する場として設計されており、体験プログラムや営業販売ブースが配置され、来場者が食の背景や調理技術に触れられる工夫が施されており、毎日 1 万人以上が来場している。営業販売ブースは複数ありテイクアウトの食品（日本の飲料及びアルコール飲料を含む）を中心に販売していた、通期出展者に加えて、週ごとまたは月ごとの期間限定ブースが設置され、食を通じた多彩な交流の場を提供していた。

１．２　意図的な食品汚染に関する脆弱性についての情報収集

当研究班におけるこれまでの研究成果の中から、脆弱性の視点として「直接手を触れることができる食材の販売の有無」、「その後の工程に洗浄や加熱がない食材の販売の有無」、「洗剤、薬品、不要物等の放置の有無」、「混入やすり替えのリスクの有無」、「その他」の 5 点を取り上げたうえで、大規模イベントにおける食品防御に対する脆弱性の確認を行った。

１．２．１　直接手を触れることができる食材の販売の有無

訪問時において、そのような食材の販売は確認できなかった。

１．２．２　その後の工程に洗浄や加熱がない食材の販売の有無

販売物は蓋付きのパッケージでそのまま飲食可能なものが販売される予定であり、そのような食材の販売は確認できなかった。

１．２．３　洗剤、薬品、不要物等の放置の有無

害虫駆除については外部業者に委託し、薬剤は使用時に持参し、持ち帰る。消毒用のアルコールはブース毎に従業員の目が届く、受け渡しカウンター前に置かれていた。その他、訪問時において、そのような状況は確認できなかった。

１．２．４　混入やすり替えのリスクの有無

訪問時において、そのような状況は確認できなかった。

１．２．５　その他

食材の搬入は営業前のみに行われ、訪問時では食材を途中搬入することはできないルールとなっている。配送の受け取りは対面のみで行われる。搬入は各ブースの裏口から行われ、来場者および他のブースの食材と交差することはない。

裏口は施錠する事ができる。各ブースには、それぞれに冷蔵、冷凍庫が設置さ

れている。各所（外周、入口、各ブース裏口および屋内）に死角無くカメラが設置されており、高性能のものを取り付けるように指定がある。カメラ映像の管理は警備会社、大阪府警およびパビリオンAで管理されている。

２．B 国パビリオンにおける意図的な食品汚染に関する脆弱性

２．１ 訪問先の概要

2025 年日本国際博覧会協会の大阪・関西万博に出展された B 国パビリオンは、「ともに未来を創ろう」をテーマに、B 国の創造性・革新性・多様性を体感できる展示空間として構成されている。来場者は、B 国の科学技術、サステナビリティ、文化、教育などの分野における先進的な取組を、映像や体験型展示を通じて学ぶことができる。また、１階に常設されているレストランでは、B 国各地の料理を提供、B 国の伝統料理から、一風変わった料理もあった。

２．２ 意図的な食品汚染に関する脆弱性についての情報収集

パビリオンAのケースと同様の方法により食品防御に対する脆弱性の確認を行った。

２．２．１　直接手を触れることができる食材の販売の有無

訪問時において、そのような食材の販売は確認できなかった。

２．２．２　その後の工程に洗浄や加熱がない食材の販売の有無

訪問時において、そのような食材の販売は確認できなかった。

２．２．３　洗剤、薬品、不要物等の放置の有無

訪問時において、そのような状況は確認できなかった。消毒用のアルコールは、従業員の目が届く、レストラン入口に設置されていた。

２．２．４　混入やすり替えのリスクの有無

訪問時において、そのような食材の販売は確認できなかった。

２．２．５　その他

レストランは、テーブル席が１０席程設置されており、卓上には調味料等は、置かれていない。調理場は、店舗の奥側にあり、注文をして受け渡しカウンターで受け取る方式を取っていた。また、顧客退席後にホールスタッフがテーブルをアルコールで消毒を行っていることが確認できた。

３．フードコート、キッチンカーおよび店舗販売品における意図的な食品汚染に関する脆弱性

３．１　訪問先の概要

2025 年の大阪・関西万博会場は複数のゾーンに分けられており、フードコート、キッチンカー、パビリオン内店舗など多様な形態で飲食販売が展開されていた。2025 年 7 月 3 日に実施した見学調査では、東ゲートから会場内のセキュリティ体制、フードコート、キッチンカーおよび店舗販売品の運用状況を視察した。(別添資料)

３．２ セキュリティおよび監視体制

東ゲートにはX線検査機と金属探知機を備えた空港の保安検査場と同等のセキュリティが設置されており、外部からの危険物持ち込みは困難な状況であった。会場屋外には多数の監視カメラが設置され、大屋根リングでは約 50 メートル間隔でカメラが配置されていた。一方、長屋造りの店舗販売店では構造上の関係で一部カメラのないエリアが確認された。

３．３ 飲食提供エリアにおける管理状況

フードコート、キッチンカーのいずれにおいても、調理場は店舗奥側に配置され、受け渡しカウンターで商品を受け取る形式が採用されていた。調味料やポーションは従業員の目が届く受け渡しカウンター付近に置かれており、食卓テーブルには基本的に調味料は設置されていなかった（一部ラーメン店を除く）。キッチンカーは通常のイベントと比較して食材保管や整理整頓が徹底されており、すべての配置場所に分電盤が設けられ発電機（ガソリン）の使用はなかった。ゴミ箱はカテゴリー別に分別され、すべて施錠されていた。喫煙所の灰皿も施錠されており、吸い殻浸出液の持ち出しは困難であった。

３．４ その他

一部店舗では従業員の顎マスクでの調理が散見され、手洗い場へのハンドソープ設置やアルコール消毒の配置にばらつきが見られた。また、パビリオン内での飲食物販売は最大 20%までというルールが設けられているが、無許可で販売を行うパビリオンがあるとの情報もあった(当日は未確認)。大阪･関西万博では、厨房の構造、監視体制、衛生管理、販売ルールのいずれにおいてもフードディフェンスの観点から適切な対応が確認された。一部にルール運用上のばらつきや改善余地が見られたものの、全体として統一的かつ高い管理意識のもとで運営されており、食品の安全性・信頼性を確保する上での良好な事例と評価できる。

D. 考察

大阪・関西万博の会場では 100 を超える飲食を提供するパビリオンや店舗が出展されており、食品衛生の確保だけでなく、食品防御への取り組みが、重要性を増すものと考えられる。

本調査結果から、物理的対策（ハード）と運用的対策（ソフト）の両面において高水準で整備されていることが確認された。特に、入場ゲートにおける空港レベルのセキュリティ、会場全体に配置された監視カメラ、また、食品提供においては､受け渡しカウンター方式の採用など、外部からの意図的混入リスクを大幅に低減する有効な措置であった。

今後、食品防御ガイドラインに新たに反映できる可能性のある脆弱性の内容として、以下のような項目が考えられた。

(「運搬・保管施設向け」について)

現時点では、追加が必要と考えられた項目は見られなかった。

(「調理・提供施設向け」について)

店頭販売品への対応を踏まえた修正を行うと共に。タイトルを「調理・提供（店頭販売品を含む）に変更することが望ましいと考えられた。

「大規模イベント時に必要な対応」に係る変更点について

「監視カメラの設置」の項目に店頭販売品の受渡し場所を追加することが望ましい。

E. 結論

本研究の結果、大阪・関西万博における食品防御対策は、国際的大規模イベントとして極めて高い水準で構築されており、外部脅威に対しては有効に機能していると評価できる。特に、入場管理、監視体制､厨房設計､提供方式においては、食品への意図的混入リスクを低減するための合理的かつ実践的な対策が講じられていた。食品防御対策ガイドラインの「運搬・保管施設向け（令和 5 年度版)」や、「調理・提供施設向け」（令和 5 年度版）

の改訂案等も参考に、脆弱な部分への対応が必要と考えられた。

F. 健康危険情報

なし

G. 研究発表

１．論文発表

なし

２．学会発表

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その①～販売代理店への聞き取り調査．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その②～飲食店への聞き取り～．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

加藤礼識、長田瑞花、多川優也．飲食物販売が多様化する中で食品防御対策はどのように変化したのか～大規模食品工場から小規模飲食店での対策への変化．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

加藤礼識、長田瑞花、多川優也．小規模な飲食店舗における食品防御対策 「バイトテロ」・「客テロ」をどう防ぐべきなのか？．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

加藤礼識、長田瑞花、多川優也、平子ほほみ、神奈川芳行、今村知明．多様化した飲食物販売における食品防御対策～これまでの食品防御対策の流れ～．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

平子ほほみ、多川優也、長田瑞花、加藤礼識、高畑能久、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　飲食店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

長田瑞花、加藤礼識、多川優也、平子ほほみ、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　販売代理店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

神奈川芳行、赤羽学、高畑能久、加藤礼識、入江芙美、山口健太郎、今村知明．大規模イベントでの食品防御対策と食品防御対策ガイドライン英訳の意義．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

H. 知的財産権の出願・登録状況

１．特許取得

なし

２．実用新案登録

なし

２．その他

なし

別添資料

会場全体図

*出典：EXPO 2025　大阪・関西万博公式Webサイト

会場は、5つのゾーンに分けられており、2025年日本国際博覧会協会（以下、万博協会）は、それぞれのエリアに飲食販売店舗を展開する。

フューチャーライフゾーン・風の広場・西ゲート広場エリア

開催地である日本・関西・大阪の食や品物を広域からの来場者を中心にPRするエリア

【立地特性】
・ゲート、交通ターミナルなどのゲート機能近接
・屋外イベント広場近接
・未来を感じるフューチャーライフパーク近接

【業態イメージ】
・日本、関西、大阪の店舗を中心に集約
・大阪の食集積や日本を代表する品物の物販店舗を配置

ウォータープラザエリア

水辺に近いロケーションを活かした
ゆったりとした時間を過ごすエリア

【立地特性】
・ウォータープラザに隣接のロケーションであり、水上ショーの実施エリア
・海外パビリオン、シグネチャーパビリオンが近接

【業態イメージ】
・水辺のロケーションとグルメを楽しめる飲食・物販店舗

静けさの森エリア

会場中心の「静けさの森」や海外パビリオンに近接する未来を感じる食のエリア

【立地特性】
・会場中心の「静けさの森」近接
・海外パビリオン、シグネチャーパビリオンが近接

【業態イメージ】
・静けさの森隣接の立地で食の未来へ導く飲食店舗
・他エリアにはない未来の食を感じられる飲食店舗の集積

空の広場エリア

海外パビリオンと近接の立地を活かした
これからのダイバーシティを楽しむことができるエリア

【立地特性】
・海外パビリオン・民間パビリオン・静けさの森近接
・会場を形成するリングに沿った建築

【業態イメージ】
・海外パビリオン近接の周辺の雰囲気を取り込み、世界各国の飲食も楽しめる店舗の集積
・SDGsを意識した未来社会の実現に取り組む飲食・物販店舗

東ゲート広場エリア

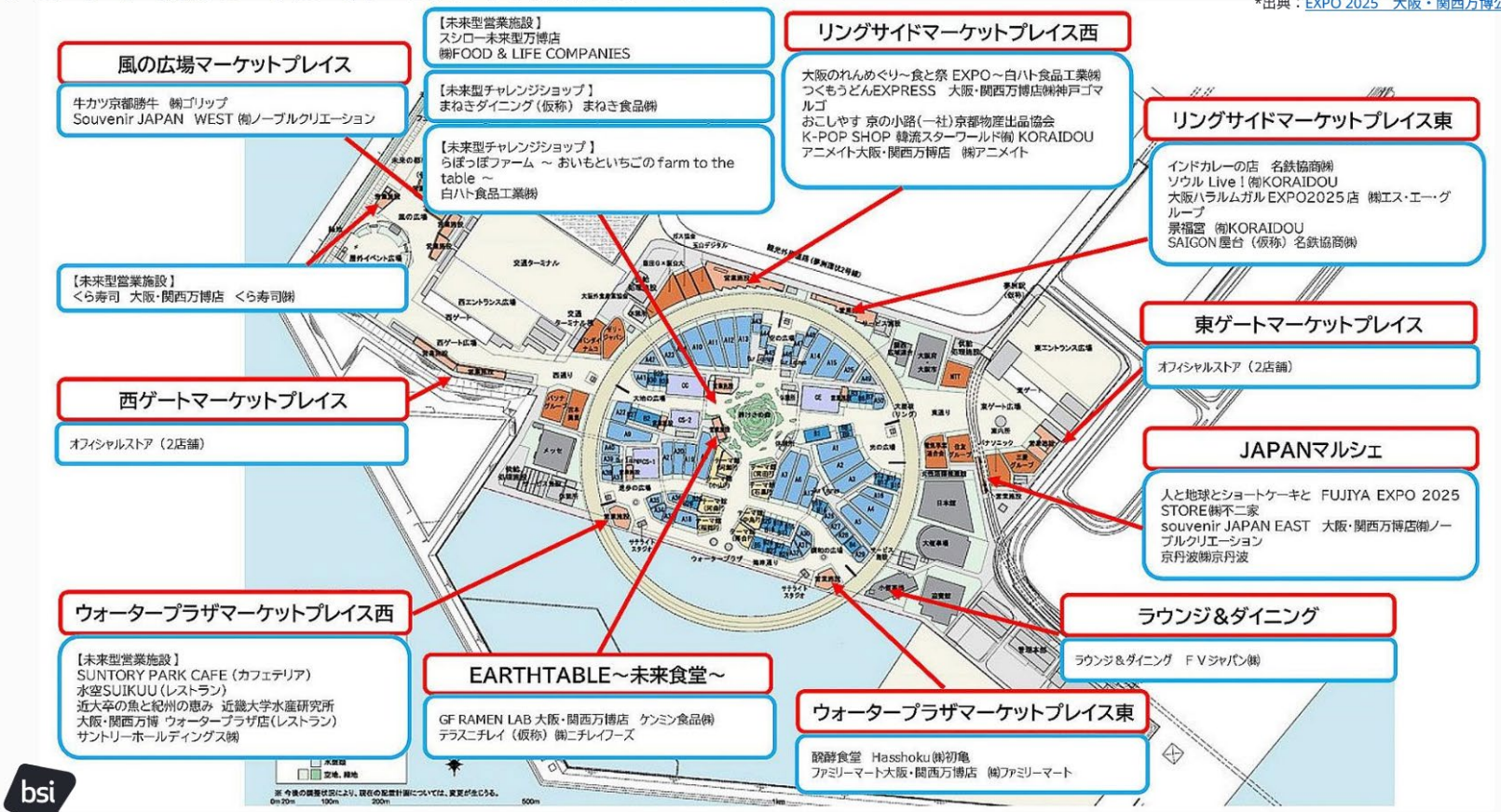
万博に訪れる日本全国・各国の人々を招き入れる
日本のゲート機能を持つエリア

【立地特性】
・来場者の多くが利用することが予想される大阪メトロ夢洲駅直結の東ゲート近接
・日本政府館、大阪ヘルスケアパビリオン、民間パビリオン近接

【業態イメージ】
・JAPANマルシェを中心としたおもてなし感やウェルカム感のある物販・飲食店舗が集積
・東ゲート近接で入退場来場者のお土産需要を獲得

万博協会委託店舗分布図

*出典：EXPO 2025　大阪・関西万博公式Webサイト



厚生労働科学研究費補助金（食品の安全確保推進研究事業）
「新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究」分担研究報告書（令和 7 年度）

食品防御対策のための現地調査

研究分担者 赤羽 学（国立保健医療科学院 医療・福祉サービス研究部 部長）
研究分担者 入江 芙美（九州大学医学研究院 医療経営・管理学講座 准教授）
研究分担者 加藤 礼識（茨城キリスト教大学 生活科学科 食物健康科学科 講師）
研究協力者 神奈川芳行（奈良県立医科大学 公衆衛生学講座 非常勤講師）
研究協力者 長田 瑞花（奈良県立医科大学 公衆衛生学講座）

研究要旨

本研究では、食品防御対策の実態を把握することを目的に、小売店（スーパーマーケット）、飲食チェーン店舗（回転寿司）、食品製造工場の 3 施設を対象に現地調査（見学・ヒアリング）を実施した。

小売店では、監視カメラの死角や作業環境の不統一、人材管理の課題が確認された。飲食チェーン店舗では、回転寿司業態特有の客テロ・バイトテロリスクへの対応として、オーダー制導入や卓上食品の管理見直しが有効であることが示唆された。食品製造工場では、IC タグ・カメラ等を活用した入室管理や工程管理が進んでいる一方、共連れ対策・薬品庫管理・廃棄物管理等に改善の余地が認められた。

これらの調査結果を踏まえ、各施設類型における食品防御対策上の脆弱性と推奨対策を取りまとめた。食品防御対策ガイドラインの改訂および普及活動に活用される予定である。

A. 研究目的

食品事業者における食品防御対策の実施状況および脆弱性を把握するため、小売店舗、飲食チェーン店舗、食品製造工場の 3 施設における現地見学調査およびヒアリング調査を実施した。各施設における食品防御上の課題と推奨対策を整理し、食品防御対策ガイドラインの改訂・普及に資することを目的とする。

B. 研究方法

以下の 3 施設を対象に、研究班メンバーが直接訪問し、施設担当者の案内のもとで見学調査を実施するとともに、ヒアリングを通じて食品防御体制に関する情報を収集・整理した。

・小売店（某スーパーマーケット店舗）：2025 年 11 月 21 日
・飲食チェーン店舗（某回転寿司チェーン店舗）：2025 年 11 月 14 日
・食品製造工場（某食品製造工場）：2026 年 2 月 2 日

倫理面への配慮として、意図的な食品汚染実行の企てに悪用される恐れのある情報・知識については本報告書には記載せず、非公開としている。

C. 研究結果

小売店（某スーパーマーケット店舗）の見学調査

2025年11月21日（9時～11時30分）、某スーパーマーケット店舗において、神奈川芳行（奈良県立医科大学）、島崎眞人（日本農林規格協会）、加藤礼識（茨城キリスト教大学）、井之上仁・鬼武一夫（日本生活協同組合連合会）、赤星千絵・相原俊介・浅井威一郎（川崎市）、長田瑞花（奈良県立医科大学院生）、一蝶茂人・河井宏介（BSIグループジャパン）が参加して見学調査を実施した。

（1）セキュリティ・アクセス管理

物理的セキュリティおよび搬入・勤怠の管理状況について以下を確認した。

搬入エリア管理

- トラックヤードは防音壁およびカーテン式仕切りで区画され、外部からの視認性を遮断している。
- 夜間は施錠可能な構造となっており、物理的セキュリティは確保されている。
- 近隣協定により搬入時間は 05:00～22:00 に制限されており、時間外搬入に対する近隣住民からの抑止力となっている。
- 搬入車両は1日あたり約10台（パン配送含む）。特定時間帯に集中し待機が発生するケースが見られる。

入退館・勤怠管理

- タイムカード方式を採用。稀に代理打刻の事例が発生するが、都度教育指導を行い是正している。
- 帽子着用により顔の識別が困難なため、名札による本人確認を徹底している。
- 本部スタッフ等の外部者はストラップ付き名札で明確に区分している。
- バックヤード間での従業員の往来は限定的であり、担当外エリアへの不必要な立ち入りは少ない。

店舗内の対策

- 消毒用アルコール等がバックヤード各所に配置されている。
- 混入防止・衛生上の観点から、一部を除いて刃と柄が一体型の刃物類を使用している。

（2）異物混入の実績と傾向

商品不良の申し出総数は年間約 11,000 件（宅配・店舗合計）であり、うち異物混入は約 3,200 件（全体の約 30%）を占める。そのうち店舗業態に起因するものは約 500 件（混入全体の約 15%）であった。非意図的な主な混入事例（インストア製造外の仕入れ商品）：残骨（精肉処理工場での骨除去不足）、青いフィルム片、稀に機械部品の脱落、毛髪・虫など。過去にバナナへの縫い針混入申し出が1件あり（警察届出済み、未解決）、意図的混入が疑われる事例はこの1件のみである。

（3）教育・研修体制

- 年1回、全職員に対しDVD教材を用いた「食品衛生・フードディフェンス教育」を実施し、テストによる効果測定・記録保管を行っている。
- 月次：副店長による衛生点検（私物持ち込みチェック等）
- 年次：品質保証部職員による監査

（4）課題と提言

視察を通じて明らかになった脆弱性および推奨対策は以下の通り。

監視体制の死角

- 店舗全体で36台のカメラが稼働しているが、バックヤード内の監視が手薄であり、特に水産・ベーカリー作業室にカメラが設置されていない。（農産・水産・畜産・惣菜・ベーカリー調理場全体にカメラ未設置）
- ワンオペ（単独）作業が発生するエリアでの監視強化が重要。
- 【推奨】監視カメラの増設・配置見直し。増設時は「スタッフを守るため」という趣旨の説明が必要。

作業環境・ルールの不統一

- 蛍光灯カバーが改装エリアと未改装エ

リアで統一されておらず、破損時の飛散リスクに差がある。【推奨：全域統一】
・ポケット付きエプロンの使用が見られ、私物混入・脱落リスクがある。【推奨：ポケット無しエプロンへの切り替え検討】
・薬剤・納品物の定位置管理（整理整頓）の徹底が必要。

人材面の変化への対応

・今後外国人技能実習生の採用増加が見込まれるため、多言語対応や視覚的にわかりやすい教育ツールの開発が急務。
・労働環境の改善（休憩室の充実）および職員相互の信頼関係の構築も重要。

飲食チェーン店舗（某回転寿司チェーン店舗）の見学調査

2025年11月14日(9時30分～11時)、某回転寿司チェーンの店舗において、加藤礼識（茨城キリスト教大学)、長田瑞花（奈良県立医科大学院生)、一蝶茂人・河井宏介(BSIグループジャパン､アテンド)が参加して見学調査・ヒアリングを実施した。

（1）バイトテロ対策

・アルバイト採用率は約 10%程度（視察店舗に限る）と低く､採用時の言葉遣いやルール順守に特に注意している。
・外国人労働者比率は 20～25%。定期的な指導および指導記録の活用を実施している。

（2）客テロ対策

・オーダーシステム上に禁止事項を表示し、客テロ抑止を図っている。
・詰め替え醤油を廃止し､ガリ・粉茶以外は卓上に置かない運用としている。
・「オーダー制」(寿司を回さない）の導入により食品ロスや乾燥によるクレームを削減。
・客席側は 2 台のカメラで対応しているが、個室感を出すために背もたれが高く、死角が生じている。

（3）店内視察の所見

・キッチンエリアとホールエリアの明確な区分けがあり、エリア間にはアクリルボード製の壁が設けられ、キッチンからホールを観察できる構造となっている。商品配膳の便宜上､エリア間の施錠は行っていないが、スタッフの目と監視カメラで補完している。
・背もたれの高い間仕切りが死角を生んでいる。個室感の維持と死角排除の両立できる最適値の模索が必要。
・ホールエリアの給仕スタッフは客テロ防止に重要な役割を担う。顧客満足度の高い飲食店では客テロ発生が少ないことが示唆されており、十分な人員配置と接客品質の維持が重要。

（4）推奨対策

オーダーパネルへの同意ボタンの導入

入店時のタッチパネル操作において「衛生的な環境維持へのご協力」をお願いする確認画面（同意ボタン）を設けることが有効と考えられる。「マナーを守って楽しく食事をする」という意識を最初に共有していただくことで、迷惑行為に対する心理的な抑制効果が働き、リスクの大幅な低減が期待できる。

テーブルからの常設食品の撤去

ガリについては、タッチパネルで注文後に配膳する形式にすることで、常に管理された安全な提供が可能となり、死角を減らすことができる。粉茶については、セルフコーナー（給茶機）でのご提供に切り替えることで、循環式給湯設備の衛生管理リスクを解消できる。

カトラリーのセルフコーナー化

テーブル上の箸立て等のカトラリー類もセルフコーナーからの持参スタイルへの変更が望ましい。最終的には卓上に置くものを「真空ボトルの醤油」のみに絞ることで、清潔で管理の行き届いた食事環境が実現できると考える。

食品製造工場（某食品製造工場）の見学調査

2026 年 2 月 2 日（13 時 00 分～16 時 30 分）、某食品製造工場において、赤羽学（国立保健医療科学院）、神奈川芳行（奈良県立医科大学）、名倉卓（日本能率協会）、河井宏介・一蝶茂人（BSI グループジャパン）が参加して見学調査を実施した。

（1）衛生管理・入室管理

更衣室・入室フロー

- ゾーニング：私服エリアと作業服エリアの間に仕切りがあり、交差汚染を防止する構造となっている。
- ロッカー設備：ロッカー上部に傾斜をつけることで、異物の秘匿や私物の置き忘れ等の危害を物理的に低減している。
- セキュリティ：IC タグをスキャンしなければエリア内に入れない仕組み（インターロック等）が導入されている。
- 清掃・異物除去：ロボット掃除機による自動清掃を実施。入室時は粘着ローラー掛けの後、ローラー自体への毛髪等の付着確認工程がある（眉毛・まつ毛等の人毛混入対策）。

手洗い場

以下の厳格な洗浄プロセスが規定されている：①粘着ローラー（40 秒）→②手洗い（40 秒）→③エアドライヤー

（2）製造・原材料管理

- 原材料トレーサビリティ：バルク等の原材料は QR コードでパレット・袋単位管理。原材料（餡）は袋ごと洗浄し、開封時カメラ（2 台）で確認している。
- 生地工程：小麦粉・砂糖等をふるいにかけて使用。
- 中具工程：外注品を専用カッターで開封し、温めて注入機へ投入。
- 焼成・包装・検査：就業前および各タイミングで手袋の確認を実施し、破損・欠落を管理。手袋ステーションと象の鼻型ごみ箱を設置。目視確認・包装後に X 線検査を通している。

（3）食品防御・セキュリティに関する課題と提言

物理的セキュリティの課題

- 「共連れ（テールゲーティング）」に対する物理的な制御が困難な状況にある。
- 照明設備：犯罪心理の観点から、現状より照度を明るく保つ、または人感センサーによる照度調整等の対策が有効と考えられる。
- フードディフェンスの弱点が見つけにくいという課題があり、セキュリティ会社の協力のもと死角の把握が必要。工具がラインの近くに置かれており、工具破片の混入リスクに留意が必要。

運用ルールの改善

- カメラ録画保存期間：製品の賞味期限だけでなく、消費者が実際に喫食するまでの日数を考慮した保存期間の設定が必要。
- 薬品庫の持ち出し管理：1 名での作業を廃し、2 名での対応とする。また、固定の 2 名組ではなく、適宜組み合わせを変えることで癒着・慣れによる不正を防止する。
- 薬品・廃棄物管理：廃棄物は発生後すぐに工場の外へ出すルールの徹底が必要。廃棄物が死角になりやすい場所に置かれており、工場設計時の留意事項として考慮すべきである。

（4）その他の運用ルール

- 落下物管理：機械部品等の落下物はカラー半透明袋に入れ、マネージャー管理下の「落下物拾得 Box」へ投入するルールを運用している。
- 通報・相談体制：工場長・製造グループ・本社へ直通の「相談ボックス」が設置されており、風通しの良い組織作りがなされている。
- 採用時の対応：アルバイト社員については業務内容によって確認事項が異なる。
- 新入社員ケア：「一人にしません」と掲示し、新入社員に対するケアを周知し

ている。
・異常事象への対応:今回の事象では１件目をラインの通常トラブルとして処理し２件目から調査を実施したが､1 件目からアラートを上げる運用が予防の観点から望ましい。

D. 考察

本調査では、小売店・飲食チェーン店舗・食品製造工場の３施設において食品防御上の課題が確認された。

小売店では､監視カメラの死角（特にバックヤード・水産・ベーカリー作業室)、作業環境・ルールの不統一（蛍光灯カバー・エプロンのポケット等)、外国人労働者増加への対応が主要課題であった。飲食チェーン店舗では、オーダー制の導入や卓上食品の管理見直し等、業態特有のリスク低減策が具体化された。特に、顧客との「衛生意識の共有」（同意ボタン等）が客テロ抑止に有効であることが示唆された。食品製造工場では、IC タグや多数のカメラ活用など先進的な取り組みが見られた一方､共連れ対策･薬品庫の複数人管理･廃棄物の即時搬出等、ソフト面の運用改善余地が明らかになった。

いずれの施設においても､従業員教育･管理体制の整備が食品防御強化の鍵であり、物理的対策（ハード）とルール・教育（ソフト）の両面から継続的な改善が求められる。

E. 結論

３施設の現地調査を通じて、各業態における食品防御上の脆弱性と改善すべき課題を具体的に把握した。小売店･飲食チェーン･製造工場のいずれにおいても､監視体制の強化、作業環境の統一・整備、従業員教育の充実が共通した推奨事項として挙げられる。本調査の知見は食品防御対策ガイドライン（「食品製造工場向け」「運搬・保管施設向け」「調理・提供施設向け」等（令和 5 年度版））の改訂および普及活動に活用される予定である。

F. 健康危険情報

なし

G. 研究発表

論文発表

なし

学会発表

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その①～販売代理店への聞き取り調査．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その②～飲食店への聞き取り～．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

加藤礼識、長田瑞花、多川優也．飲食物販売が多様化する中で食品防御対策はどのように変化したのか～大規模食品工場から小規模飲食店での対策への変化．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

加藤礼識、長田瑞花、多川優也．小規模な飲食店舗における食品防御対策 「バイトテロ」･「客テロ」をどう防ぐべきなのか？．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京.

加藤礼識、長田瑞花、多川優也、平子ほ

ほみ、神奈川芳行、今村知明．多様化した飲食物販売における食品防御対策～これまでの食品防御対策の流れ～．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

平子ほほみ、多川優也、長田瑞花、加藤礼識、高畑能久、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　飲食店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

長田瑞花、加藤礼識、多川優也、平子ほほみ、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　販売代理店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

神奈川芳行、赤羽学、高畑能久、加藤礼識、入江芙美、山口健太郎、今村知明．大規模イベントでの食品防御対策と食品防御対策ガイドライン英訳の意義．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

H．知的財産権の出願・登録状況

１．特許取得

なし

２．実用新案登録

なし

３．その他

なし

厚生労働科学研究費補助金（食品の安全確保推進研究事業）
「新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した
食品防御の推進のための研究」分担研究報告書（令和７年度）

フードチェーン全体の安全性向上に向けてのコロナ対策を踏まえた調査と食品防御対策ガイドライン等の改善と、同ガイドラインの普及

研究分担者 赤羽 学（国立保健医療科学院 医療・福祉サービス研究部 部長）
研究協力者 神奈川芳行（奈良県立医科大 公衆衛生学講座 非常勤講師）

研究要旨

近年、食品への意図的な毒物や異物の混入事件が頻発したことも相まって、大規模・中小規模の食品製造施設や物流施設、調理提供施設に関しての食品防御対策ガイドラインやチェックリストの作成が進んできている。しかし、その後の新型コロナウィルス感染症の流行や、終息後の５類指定等の変化を経て、食品提供に関する社会情勢は大きく変化し、日常の感染症対策として消毒用アルコールの常設など、コロナ前には見られなかった光景が定着している。また、外食産業ではテイクアウトやデリバリーなどの割合が増す等の大きな変化が起きた。さらに、令和７年度には、大阪・関西万博が開催され、改めて大規模イベント時の食品防御対策の確認も必要となった。これらの業界構造の変化や大規模イベントに対しては、法的な規制や枠組みが未整備で、今後何らかのルールの設定が求められる。

以上の観点から今年度の本分担研究では、新型コロナウィルス感染症の流行を経て新たに日常生活に定着した対策や、フードデリバリーやテイクアウトなど新たな業態における食品防御対策と感染症対策の両立についての検討を深度化させ、また、令和７年度に実施される大規模イベント等での対策も想定して、食品防御対策ガイドラインや、チェックリストの改訂を行った。また、フードデリバリーの配達担当者や利用企業向けのチェックリストについては、従事者の特性等を考慮し、多言語化にも取り組んだ。

A. 研究目的

食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）（令和５年度版）を基に、新型コロナウィルス感染症の収束を経た現在において、また、本年度開催された大阪・関西万博での対応を念頭に、店頭販売品における対策を含め、フードチェーン全体の安全性を向上させるための食品防御対策ガイドラインの見直しと改善を行う。

また、新型コロナウィルス感染症の流行時に急速に普及し、現在では一般化したフードデリバリーサービスにおける食品防御対策についても重点的に検討する。フードデリバリーサービス提供事業者および利用事業者向けの食品防御対策チェックリスト（令和５年度版）、フードデリバリーサービス配達員向けの食品防御対策チェックリスト（令和５年度版）を基に、実施の容易さを考慮したツールの開発を進める。特に、外国人労働者の増加に対応するため、チェックリストの英訳版を作成し、多様な現場での運用を検討する。

B. 研究方法

１．食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）（令和 5 年度版）の修正

令和 5 年度版に、新型コロナウィルス感染症対策及び第 3 者認証の要素および店舗販売品に関する要素および店舗販売品を加味した見直しを行った。加えて、近年、監視カメラの映像が海外サイトを経由または直接外部から閲覧可能となっている事例が報道されていることを踏まえ、監視カメラの管理方法についても検討し、必要な追記を行った。

◆倫理面への配慮

本研究で得られた成果は厚生労働省に報告をしているが、一部意図的な食品汚染実行の企てに悪用される恐れのある情報・知識については、本報告書には記載せず、非公開としている。

C. 研究結果

１．食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）（令和 5 年度版）の修正

店頭販売品の範囲を、「営業許可や製造許可を受けた実店舗で調理された料理等を容器に入れ、店舗の敷地内で販売される商品とする。」と定義した。検討経過を（資料：別添１－１）に示す。併せて

既存ガイドラインからの主な変更点は以下のとおりである。

１．１　「優先的に実施すべき対策」に係る変更点について

大規模イベント時の食品の提供教法として、「店頭販売品」が大きなウエートを占めることが想定されたことから、「調理・提供」に（店頭販売品を含む）を追記。

１．１．１　組織マネジメント

- 変更点はない。

１．１．２　人的要素（従業員等）

- 「私物の持込みと確認」の項目の保管庫を飲食料品保管庫に修正し、解説でも、販売の現場への私物の持ち込みを追加。（No.11）

１．１．３　人的要素（部外者）

- 「業者の持ち物確認」の項目に店舗等を追加。（No.19）

１．１．４　施設管理

- 「調理器具等の定数管理」の項目の解説に店舗および受渡し場所を追加。（No.22）
- 「脆弱性の高い場所の把握と対策」の項目に店頭販売品の受渡し場所を追加。（No.23）
- 「無人の時間帯の対策」の項目に店舗を追加。（No.24）
- 「外部からの侵入防止策」の項目の食品保管庫を店頭販売品を含む飲食料品保管庫に修正。（No.26）
- 「確実な施錠」の項目の食品保管庫を店頭販売品を含む飲食料品保管庫に修正。（No.27）
- 「洗剤等の保管場所」の項目に店舗を追加し、解説の保管場所として、店頭販売品の受け渡し場所を追加。（No.28）
- 「殺虫剤等の保管」の解説に、店舗を追加。（No.30）
- 監視カメラの管理について新たに項目を追加し、特に映像流出に注意するよう追記。（No.34）

１．１．５　入出荷等の管理

- 「ラベル・包装・数量の確認」の項目の解説に、容器を追加。（No.35）
- 「積み下ろしの監視」の項目に店頭販売品を追加。（No.36）
- 「保管中の食材や料理数の増減や汚染行為の徴候への対応」を「保管中の食材や料理数・店頭販売品の増減

や汚染行為の徴候への対応」に修正。（No.38）

・ 「対応体制･連絡先等の確認」(No.40)の項目の解説に、店舗をも追加。

１．２ 「可能な範囲での実施が望まれる対策」に係る変更点について

「調理･提供」に(店頭販売品を含む)を追記。

１．２．１ 人的要素（従業員等）

・ 「従業員の所在把握」の項目の解説に店舗内を追加。(No.41)

１．２．２ 施設管理

・ 「扉の施錠等の設置」の項目の解説に店舗内を追加。(No.42)

・ 「監視カメラの設置」の項目の解説に店舗を追加。(No.43)

・ 「継続的な監視」の項目の解説に店頭販売品を追加。(No.44)

１．３ 「大規模イベント時に必要な対応」に係る変更点について

・ 「調理･提供」に(店頭販売品を含む)を追記。

・ 「監視カメラの設置」の項目に店頭販売品の受渡し場所を追加。(No.48)

２．食品防御対策ガイドライン（中小規模：食品製造工場向け・運搬・保管施設向け・調理・提供施設向け）（令和５年度版）の修正

検討経過を（資料：別添１－２）に示す。既存ガイドラインからの主な変更点は以下のとおりである。

２．１「優先的に実施すべき対策」に係る変更点について

「調理･提供」に(店頭販売品を含む)を追記。

２．１．１ 組織マネジメント

・ 調理・提供（店頭販売品を含む）の「危機管理体制の構築」の項目に飲食料品(店頭販売品を含む)を追加。（No.1）

２．１．２ 人的要素（従業員等）

・ 調理・提供（店頭販売品を含む）の「私物の持込みと確認」の項目に店頭販売の現場を追加。(No.12)

２．１．３ 人的要素（部外者）

・ 変更点はない。

２．１．４ 施設管理

・ 調理・提供（店頭販売品を含む）の「無人の時間帯の対策」の項目に販売店舗を追加。(No.22)

・ 製造、運搬・保管、調理・提供（店頭販売品を含む）に新たに監視カメラの管理についての項目を追加。（No.32）

２．１．５ 入出荷等の管理

・ 調理・提供（店頭販売品を含む）の「積み下ろしの監視」の項目に店頭販売品を追加。(No.34)

・ 調理・提供（店頭販売品を含む）の「保管中の食材や料理数の増減や汚染行為の徴候への対応」を「保管中の食材や料理数・店頭販売品の増減や汚染行為の徴候への対応」に修正。（No.36）

・ 調理・提供（店頭販売品を含む）の「対応体制・連絡先等の確認」の項目に購入者を追加。(No.38)

２．２「大規模イベント時に必要な対応」に係る変更点について

・ 「調理･提供」に(店頭販売品を含む)を追記。

・ 調理・提供（店頭販売品を含む）の「お客様対策」の項目に「店頭販売品においても、販売場所での異物の混入防止に注意する。」を追加。（No.40）

・ 調理・提供（店頭販売品を含む）の「監視カメラの設置」の項目に店頭販売品の受け渡し場所を追加。（No.42）

・ 調理・提供（店頭販売品を含む）の「厨房の防犯・監視体制の強化」の

項目に店頭販売品を追加。併せて、「共有で使用するキッチン等は、使用前後に異常の有無を確認する。」を追加。（No.43）

３．食品防御対策チェックリスト（フードデリバリーサービス提供事業者及び利用事業者向け）（令和５年度版）の時点修正の必要性の確認

検討経過を（資料：別添２－１）に示す。既存ガイドラインからの主な変更点は以下のとおりである。

３．１「優先的に実施すべき対策」に係る変更点について

３．１．１　組織マネジメント

・ 変更点はない。

３．１．２　人的要素（従業員等）

・ 変更点はない。

３．１．３　人的要素（部外者）

・ 変更点はない。

３．１．４　施設管理

・ 監視カメラの管理について新たに項目を追加。（No.26）

３．１．５　入出荷等の管理

・ 変更点はない。

３．２　「可能な範囲での実施が望まれる対策」に係る変更点について

・ 変更点はない。

４．フードデリバリーサービス配達員向けの食品防御対策チェックリスト（令和５年度版）の時点修正の必要性の確認

検討経過を（資料：別添２－２）に示す。チェックリスト自体には、現時点では大きな修正は行われなかった。

５．食品防御対策チェックリスト（フードデリバリーサービス提供事業者及び利用事業者向け）（令和５年度版）、フードデリバリーサービス配達員向けの食品防御対策チェックリスト（令和５年度版）の英訳版の作成

検討経過を（資料：別添２－３）に示す。既存ガイドラインからの主な変更点は以下のとおりである。フードデリバリーサービス配達員向けの食品防御対策チェックリスト自体には、現時点では大きな修正は行われなかった。（資料：別添２－４）

５．１　「優先的に実施すべき対策」に係る変更点について

５．１．１　組織マネジメント

・ 変更点はない。

５．１．２　人的要素（従業員等）

・ 変更点はない。

５．１．３　人的要素（部外者）

・ 変更点はない。

５．１．４　施設管理

・ 監視カメラの管理について新たに項目を追加（No.26）

５．１．５　入出荷等の管理

・ 変更点はない。

５．２　「可能な範囲での実施が望まれる対策」に係る変更点について

・ 変更点はない。

D. 考察

1. 新型コロナウィルス感染症対策と調和した食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）の作成

食品防御対策ガイドライン（令和５年度版）は、多くの項目において、新型コロナウィルス感染症対策としての有用性も併せ持っていることが確認できた（別添１－１・２参照）。また、新型コロナウィルス感染症の経験を経て、「新たな日常」として定着した種々の感染症対策があるが、これらの対策は、人々のリスク意識に合わせてこれらも変化するものと思われる。

今後、新たな感染症が流行した際には、

本ガイドラインを参考に、食品防御対策との調和を考慮した具体的な対策を検討する必要がある。

また、長期間にわたる大規模イベントにおいては、店頭販売品をイベント会場内で購入し、休憩スペース等で飲食することが想定されることから、従来の施設内での調理・提供だけでなく、それらの食品を店頭販売する際にも注意が必要と考えられた。さらに、イベント期間中に多くの食品提供事業者が関与することや、期間内に同じ施設を複数の事業者が使用することから、共有部分等に対する対策や、スタッフ教育等にも留意が必要と考えられた。

２．食品防御対策チェックリスト（フードデリバリーサービス提供事業者及び利用事業者向け）（令和５年度版）、フードデリバリーサービス配達員向けの食品防御対策チェックリスト（令和５年度版）の確認と英訳版の作成

従来の食品製造工場や調理・提供施設等では、複数の従業員が一緒に業務を行っているため、従業員同士の相互監視が重要な役割を担っていた。しかし、フードデリバリーサービスでは、配達員が単独で行動する事が一番の特徴である。過年度の調査では、スマートフォン等のGPS 機能等は既に有効に活用されていたが、それらの内容は、チェックリストには既に含まれていた。

また、配達員も、アルバイトや個人事業主としての請負契約が多いことから、身元の確認、食品衛生管理や食品防御対策に関する教育等に実効性や強制力を担保させることは困難である。さらに、海外出身者が従事するケースも多いことから、より汎用性を高めるために、英訳版を試作した。今後、英訳版がさらに多言語にも翻訳され、活用されることが期待されている。

今後、各ステークホルダーがそれぞれ可能な範囲で実施可能な対策を整理し、それぞれの掛け合わせにより、フードデリバリーサービスのサプライチェーン全体として食品防御対策の実効性が向上するシステムを構築する必要がある。

尚、本ガイドライン等では、監視カメラとの表現を使用しているが、他の呼称の方が望ましいとの意見もあることから、次年度以降、その呼称についても検討する予定である。

E. 結論

食品防御対策ガイドライン（食品製造工場向け、運搬・保管施設向け、調理・提供施設向け）（令和５年度版）及び食品防御対策ガイドライン（中小規模：食品製造工場向け・運搬・保管施設向け・調理・提供施設向け）（令和５年度版）について、新型コロナウィルス感染症対策との調和と、大規模イベントでの特に店頭販売品への活用を加味した修正を行った。（別添１－１・２）

フードデリバリーサービス提供事業者及び利用事業者向けの食品防御対策チェックリスト（令和５年度版）について事業者の実態を踏まえた確認を行った。（別添２－１・２）

さらに、フードデリバリーサービス提供事業者および利用事業者向けの食品防御対策チェックリスト（令和５年度版）について、海外出身の配達員における活用を考慮した、英訳版を試作した。（別添２－３・４）

F. 健康危険情報

なし

G. 研究発表

１．論文発表

なし

２．学会発表

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その①～販売代理店への聞き取り調査．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

長田瑞花、加藤礼識、多川優也．食品防御上の新たな問題（ロボット配膳システム）その②～飲食店への聞き取り～．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

加藤礼識、長田瑞花、多川優也．飲食物販売が多様化する中で食品防御対策はどのように変化したのか～大規模食品工場から小規模飲食店での対策への変化．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

加藤礼識、長田瑞花、多川優也．小規模な飲食店舗における食品防御対策 「バイトテロ」・「客テロ」をどう防ぐべきなのか？．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

田口貴章、小川亮介、穐山浩、今村知明 、堤智昭．意図的混入対策としての加工食品中の界面活性剤分析法の検討．第 121 回日本食品衛生学会・学術講演会．2025 年 10 月．東京．

加藤礼識、長田瑞花、多川優也、平子ほほみ、神奈川芳行、今村知明．多様化した飲食物販売における食品防御対策～これまでの食品防御対策の流れ～．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

平子ほほみ、多川優也、長田瑞花、加藤礼識、高畑能久、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　飲食店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

長田瑞花、加藤礼識、多川優也、平子ほほみ、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　販売代理店への聞き取り調査．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

神奈川芳行、赤羽学、高畑能久、加藤礼識、入江芙美、山口健太郎、今村知明．大規模イベントでの食品防御対策と食品防御対策ガイドライン英訳の意義．第 84 回日本公衆衛生学会総会．2025 年 10 月．静岡．

H．知的財産権の出願・登録状況

１．特許取得

なし

２．実用新案登録

なし

３．その他

なし

『食品防御対策ガイドライン（食品製造工場向け）』[1]および「運搬・保管」向け、「調理・提供」向けガイドライン（案）[2]

※2020 年度改訂案に、新型コロナウィルス感染症対策及び第 3 者認証の要素および店舗販売品*を加味したもの。

*店頭販売品の範囲は、営業許可や製造許可を受けた実店舗で調理された料理等を容器に入れ、店舗の敷地内で販売される商品とする。

令和 5 年度版→20250210 確認⇒20250303 修正案→万博を踏まえて再修正予定⇒20260127 班会議版

1．優先的に実施すべき対策

■組織マネジメント

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
1	○製品の異常を早い段階で探知するため苦情や健康危害情報等を集約・解析する仕組みを構築するとともに、万一、意図的な食品汚染が発生した際に迅速に対処できるよう、自社製品に意図的な食品汚染が疑われた場合の保健所等への通報・相談や社内外への報告、製品の回収、保管、廃棄等の手続きを定めておく。	・苦情、健康危害情報等については、販売店経由で寄せられる情報についても把握に努め、これらの情報等について企業内での共有化を図る。 ・意図的な食品汚染が判明した場合や疑われる場合の社内の連絡フロー、保健所・警察等関係機関への連絡先等をマニュアル等に明記しておく。 ・異物混入が発生した際には、原因物質に関わらず、責任者に報告し、報告を受けた責任者は故意による混入の可能性を排除せずに対策を検討する。	○（危機管理体制の構築） 製品の異常を早い段階で探知するため苦情や健康危害情報等を集約・解析する仕組みを構築すると共に、リスク情報に関するモニタリングを実施しましょう。 万一、意図的な食品汚染が発生した際に迅速に対処できるよう、自社製品に意図的な食品汚染が疑われた場合の保健所等への通報・相談や社内外への報告、製品の回収、保管、廃棄等の手続きを定めておきましょう。	・社内の連絡網、保健所・警察等関係機関への連絡先等をマニュアル等に明記しておくことは、万が一、製品に意図的な食品汚染が判明した場合や疑われた場合の関係部署への情報提供を円滑に行うために有用です。 ・苦情、健康危害情報等については、販売店経由で寄せられる情報についても把握に努め、これらの情報等についても企業内で共有しましょう。 ・異物混入が発生した際には、原因物質に関わらず、責任者に報告し、報告を受けた責任者は故意による混入の可能性を排除せずに対策を検討しましょう。	○（危機管理体制の構築） 製品の異常を早い段階で探知するため苦情や健康危害情報等を集約・解析する仕組みを構築すると共に、リスク情報に関するモニタリングを実施しましょう。 万一、意図的な食品汚染が発生した際に迅速に対処できるよう、自社の取扱商品に意図的な食品汚染が疑われた場合の保健所等への通報・相談や社内外への報告、製品の回収、保管、廃棄等の手続きを定めておきましょう。	・社内の連絡網、保健所・警察等関係機関への連絡先等をマニュアル等に明記しておくことは、万が一、取扱商品に意図的な食品汚染が判明した場合や疑われた場合の関係部署への情報提供を円滑に行うために有用です。 ・苦情、健康危害情報等については、販売店経由で寄せられる情報についても把握に努め、これらの情報等についても企業内で共有しましょう。 ・異物混入が発生した際には、原因物質に関わらず、責任者に報告し、報告を受けた責任者は故意による混入の可能性を排除せずに対策を検討しましょう。	○（危機管理体制の構築） 提供した飲食料品の異常を早い段階で探知するため、苦情や健康危害情報等を集約・解析する仕組みを構築すると共に、リスク情報に関するモニタリングを実施しましょう。 万一、意図的な食品汚染が発生した際に迅速に対処できるよう、自施設で提供した飲食料品に意図的な食品汚染が疑われた場合の保健所等への通報・相談や社内外への報告、飲食料品の回収、保管、廃棄等の手続きを定めておきましょう。	・社内の連絡網、保健所・警察等関係機関への連絡先等をマニュアル等に明記しておくことは、万が一、提供した飲食料品に意図的な食品汚染が判明した場合や疑われた場合の関係部署への情報提供を円滑に行うために有用です。 ・苦情、健康危害情報等については、販売店経由で寄せられる情報についても把握に努め、これらの情報等についても企業内で共有しましょう。 ・異物混入が発生した際には、原因物質に関わらず、責任者に報告し、報告を受けた責任者は故意による混入の可能性を排除せずに対策を検討しましょう。 ・施設内での情報伝達の際には警備班や、外部の関係機関等（警察・消防・関係省庁・自治体・保健所等）と連携して行いましょう。 ・事前に決めたルールに通りに対応できない場合の対応者と責任者を決めておきましょう。	○有り 食品防御も感染症対策も企業の危機管理の一環として必要。	○無し
2	○従業員等や警備員は、敷地内での器物の破損、不用物、異臭等に気が付いた時には、すぐに工場長や責任者に報告する。	・警備や巡回時に確認する項目をチェックリスト化し、警備の質を確保しておくことが望ましい。 ・故意による器物の破損や悪意の落書きなどの予兆を見	○（異常発見時の報告） 従業員等や警備員は、施設内や敷地内での器物の破損、不用物、異臭等に気が付いた時には、すぐに施設責任者や調理責任者に報告しましょう。	・警備や巡回時に確認する項目をチェックリスト化し、警備の質を確保しましょう。 ・故意による器物の破損や悪意の落書きなどの予兆を見つけた場合は、早急に責任者に報告しましょう。	○（異常発見時の報告）従業員等や警備員は、施設内や敷地内での器物の破損、不用物、異臭等に気が付いた時には、すぐに施設責任者に報告しましょう。	・警備や巡回時に確認する項目をチェックリスト化し、警備の質を確保しましょう。 ・故意による器物の破損や悪意の落書きなどの予兆を見つけた場合は、早急に責任者に報告しましょう。	○（異常発見時の報告） 従業員等や警備員は、施設内や敷地内での器物の破損、不用物、異臭等に気が付いた時には、すぐに施設責任者や調理責任者に報告しましょう。	・警備や巡回時に確認する項目をチェックリスト化し、警備の質を確保しましょう。 ・故意による器物の破損や悪意の落書きなどの予兆を見つけた場合は、早急に責任者に報告しましょう。	○無し	○無し

[1] 奈良県立医科大学, 食品防御対策ガイドライン（食品製造工場向け）（平成 25 年度改訂版）, http://www.naramed-u.ac.jp/~hpm/pdf/fd_guideline/h25_fd_guideline.pdf

[2] 参考資料：日本中央競馬会畜産振興事業「オリンピック・パラリンピック東京大会における食品テロ防止対策事業」（主任研究者 今村知明）報告書（平成 28 年度）

No.	食品防御対策ガイドライン （食品製造工場向け） 【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供 （店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
		逃さないことが重要である。								
3			○（感染症対策） 従業員が感染症に罹患した場合、工場閉鎖や食品汚染の原因となることがあります。地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の対応策を事前に検討しておきましょう。	・食品企業における感染症対策の意義を理解しましょう。 ・普段から地域の感染症の流行状況に注意を払い、従業員等が感染した場合には、出勤させないようにしましょう。 ・世界的な感染症の流行が発生した際に備えて BCP を作成し、出勤禁止や職場復帰可能の基準を予め定めておき、従業員に周知しましょう。	○（感染症対策） 従業員が感染症に罹患した場合、工場閉鎖や食品汚染の原因となることがあります。 地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の対応策を事前に検討しておきましょう。	・食品企業における感染症対策の意義を理解しましょう。 ・普段から地域の感染症の流行状況に注意を払い、従業員等が感染した場合には、出勤させないようにしましょう。 ・世界的な感染症の流行が発生した際に備えて BCP を作成し、出勤禁止や職場復帰可能の基準を予め定めておき、従業員に周知しましょう。	○（感染症対策） 従業員が感染症に罹患した場合、工場閉鎖や食品汚染の原因となることがあります。地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の対応策を事前に検討しておきましょう。	・食品企業における感染症対策の意義を理解しましょう。 ・普段から地域の感染症の流行状況に注意を払い、従業員等が感染した場合には、出勤させないようにしましょう。 ・世界的な感染症の流行が発生した際に備えて BCP を作成し、出勤禁止や職場復帰可能の基準を予め定めておき、従業員に周知しましょう。	○有り 感染症対策は、食品企業にとっても必要。	☆有り 出退勤の管理が複雑になる。 消毒薬等を配置した場合は、異物混入のリスクが高まる。
4	○食品工場の責任者は、従業員等が働きやすい職場環境づくりに努め､従業員等が自社製品の品質と安全確保について高い責任感を感じながら働くことができるように留意する。	・従業員等の監視を強化するのではなく、従業員等自らが、自社製品の安全を担っているという高い責任感を感じながら働くことができる職場環境づくりを行う。	○（職場環境づくり） 従業員等が働きやすい職場環境づくりに努めましょう。 ○（教育） 従業員等が自社の製品・サービスの品質と安全確保について高い責任感を感じながら働くことができるように、適切な教育を実施しましょう。	・働きやすい快適な職場環境は、職場に対する不満等を抱かせないためにも、重要なものです。労働安全衛生法に基づき、毎月 1 回開催されている安全衛生委員会がある職場では、その場も有効に活用しましょう。 ・食品工場の責任者は従業員が職場への不平・不満から犯行を行う可能性があることを認識し、対応可能な食品防御対策の検討や、従業員教育を行いましょう。 ・従業員の多様な背景を十分に理解して対応できるようにしましょう。 ・従業員の不満を早期に把握し対応するため、定期的なサーベイランスの実施、第三者相談窓口や社長へ直接メール等の通報制度を活用しましょう。 ・従業員の人間関係を良好に保つため、普段からのコミュニケーションを心掛けましょう。	○（職場環境づくり） 従業員等が働きやすい職場環境づくりに努めましょう。 ○（教育） 従業員等が自社の製品・サービスの品質と安全確保について高い責任感を感じながら働くことができるように、適切な教育を実施しましょう。	・働きやすい快適な職場環境は、職場に対する不満等を抱かせないためにも、重要なものです。労働安全衛生法に基づき、毎月 1 回開催されている安全衛生委員会がある職場では、その場も有効に活用しましょう。 ・物流・保管施設の責任者は従業員が職場への不平・不満から犯行を行う可能性があることを認識し、対応可能な食品防御対策の検討や、従業員教育を行いましょう。 ・従業員の不満を早期に把握し対応するため、定期的なサーベイランスの実施、第三者相談窓口や社長へ直接メール等の通報制度を活用しましょう。 ・従業員の人間関係を良好に保つため、普段からのコミュニケーションを心掛けましょう。	○（職場環境づくり） 従業員等が働きやすい職場環境づくりに努めましょう。 ○（教育） 従業員等が自社の製品・サービスの品質と安全確保について高い責任感を感じながら働くことができるように、適切な教育を実施しましょう。	・働きやすい快適な職場環境は、職場に対する不満等を抱かせないためにも、重要なものです。労働安全衛生法に基づき、毎月 1 回開催されている安全衛生委員会がある職場では、その場も有効に活用しましょう。 ・接客施設の責任者は従業員が職場への不平・不満から犯行を行う可能性があることを認識し、対応可能な食品防御対策の検討や、従業員教育を行いましょう。 ・様々な地域からの来訪者が想定されます。多様性を十分に理解して対応できるようにしましょう。 ・従業員の不満を早期に把握し対応するため、定期的なサーベイランスの実施、第三者相談窓口や社長へ直接メール等の通報制度を活用しましょう。 ・従業員の人間関係を良好に保つため、普段からのコミュニケーションを心掛けましょう。	○有り	☆有り 安全衛生委員会では、職場内での感染予防対策について議論される。 様々な地域からの来訪者は、感染源となりうる。 感染拡大期には、コミュニケーションの取り方に注意が必要
5	○食品工場の責任者は、自社製品に意図的な食品汚染が	・従業員等に対して、意図的な食品汚染に関する脅威	○（教育内容） 定期的な従業員教育の中に、	・食品防御の教育の目的は、食品防御に対する意識を持っ	○（教育内容） 定期的な従業員教育の中に、	・食品防御の教育の目的は、食品防御に対する意識を持っ	○（教育内容） 定期的な従業員教育の中に、	・食品防御の教育の目的は、食品防御に対する意識を持っ	○有り 食品防御・感染	☆有り 食品防御・感染予

No.	食品防御対策ガイドライン （食品製造工場向け） 【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供 （店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
	発生した場合、お客様はまず工場の従業員等に疑いの目を向けるということを、従業員等に意識付けておく。	や、予防措置の重要性に関して定期的に教育を行い、従業員自らが自社製品の安全を担っているという責任感を認識させる。	意図的な食品汚染に関する脅威や、予防措置に関する内容を含め、その重要性を認識してもらいましょう。 世界的な感染症が流行している時期には、その感染症に対する内容も含めましょう。	てもらうことであり、従業員等の監視を強化することではないことに留意しましょう。 ・食品防御対策は、食品衛生対策とは異なる視点が必要であることを理解してもらいましょう。 ・採用時や定期的な従業員教育の中に、意図的な食品汚染に関する脅威や、予防措置に関する内容を含め、その重要性を認識してもらいましょう。 ・自社で製造した飲食料品に意図的な食品汚染が発生した場合、顧客や行政はまず製造工場の従業員等に疑いの目を向ける可能性があるということを、従業員等に認識してもらいましょう。 ・従業員等には、自施設のサービスの品質と安全を担っているという強い責任感を認識してもらいましょう。 ・臨時スタッフについても同様の教育を行いましょう。 ・従業員教育の際には、内部による犯行を誘発させないよう、部署ごとに応じた内容に限定する等の工夫や留意が必要です。 ・従業員への教育では、具体的な事例や手口を伝えないように注意することが重要です。教育用媒体を有効に活用しましょう。 ・万が一犯行に及んだ場合には、刑事罰を受けることも教育しておきましょう。 ・SNS の利用に関する注意を行いましょう。 ・感染症に関する内容も適宜取り入れましょう。	意図的な食品汚染に関する脅威や、予防措置に関する内容を含め、その重要性を認識してもらいましょう。 世界的な感染症が流行している時期には、その感染症に対する内容も含めましょう。	てもらうことであり、従業員等の監視を強化することではないことに留意しましょう。 ・食品防御対策は、食品衛生対策とは異なる視点が必要であることを理解してもらいましょう。 ・採用時や定期的な従業員教育の中に、意図的な食品汚染に関する脅威や、予防措置に関する内容を含め、その重要性を認識してもらいましょう。 ・取扱商品で意図的な食品汚染が発生した場合、顧客や行政はまず当該施設内の従業員等に疑いの目を向ける可能性があるということを、従業員等に認識してもらいましょう。 ・従業員等には、自施設のサービスの品質と安全を担っているという強い責任感を認識してもらいましょう。 ・臨時スタッフについても同様の教育を行いましょう。 ・従業員教育の際には、内部による犯行を誘発させないよう、部署ごとに応じた内容に限定する等の工夫や留意が必要です。 ・従業員への教育では、具体的な事例や手口を伝えないように注意することが重要です。教育用媒体を有効に活用しましょう。 ・万が一犯行に及んだ場合には、刑事罰を受けることも教育しておきましょう。 ・SNS の利用に関する注意を行いましょう。 ・感染症に関する内容も適宜取り入れましょう。	意図的な食品汚染に関する脅威や、予防措置に関する内容を含め、その重要性を認識してもらいましょう。 世界的な感染症が流行している時期には、その感染症に対する内容も含めましょう。	てもらうことであり、従業員等の監視を強化することではないことに留意しましょう。 ・食品防御対策は、食品衛生対策とは異なる視点が必要であることを理解してもらいましょう。 ・採用時や定期的な従業員教育の中に、意図的な食品汚染に関する脅威や、予防措置に関する内容を含め、その重要性を認識してもらいましょう。 ・施設内で提供した飲食料品に意図的な食品汚染が発生した場合、顧客や行政はまず接客施設内の従業員等に疑いの目を向ける可能性があるということを、従業員等に認識してもらいましょう。 ・従業員等には、自施設のサービスの品質と安全を担っているという強い責任感を認識してもらいましょう。 ・臨時スタッフについても同様の教育を行いましょう。 ・従業員教育の際には、内部による犯行を誘発させないよう、部署ごとに応じた内容に限定する等の工夫や留意が必要です。 ・従業員への教育では、具体的な事例や手口を伝えないように注意することが重要です。教育用媒体を有効に活用しましょう。 ・万が一犯行に及んだ場合には、刑事罰を受けることも教育しておきましょう。 ・SNS の利用に関する注意を行いましょう。 ・感染症に関する内容も適宜取り入れましょう。	予防の両方において、適切な教育内容が求められる。	防の教育内容に留意が必要。（内部犯行を誘発させないように）

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
6	○自社製品に意図的な食品汚染が疑われた場合に備え、普段から従業員の勤務状況、業務内容について正確に把握しておく。	・意図的な食品汚染が発生した場合においても、各方面への情報提供を円滑に行うことができるよう、平時から、従業員の勤務状況、業務内容について正確に記録する仕組みを構築しておく。	○（勤務状況等の把握） 従業員の勤務状況、業務内容、役割分担等を正確に把握しましょう。	・平時から、従業員の勤務状況や業務内容、役割分担について正確に記録する仕組みを構築しておくことは、自社製品に意図的な食品汚染が疑われた場合の調査に有用です。	○（勤務状況等の把握） 従業員の勤務状況、業務内容、役割分担等を正確に把握しましょう。	・平時から、従業員の勤務状況や業務内容、役割分担について正確に記録する仕組みを構築しておくことは、自社の取扱商品に意図的な食品汚染が疑われた場合の調査に有用です。	○（勤務状況等の把握） 従業員の勤務状況、業務内容、役割分担等を正確に把握しましょう。	・平時から、従業員の勤務状況や業務内容、役割分担について正確に記録する仕組みを構築しておくことは、自施設で提供した飲食料品に意図的な食品汚染が疑われた場合の調査に有用です。	○有り 感染症罹患時も把握しやすい。	○無し

■人的要素（従業員等）

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
7	○従業員等の採用面接時には、可能な範囲で身元を確認する。身分証、免許証、各種証明書等は、可能な限り原本を確認し、面接時には、記載内容の虚偽の有無を確認する。		○従業員採用時の留意点（身元の確認等） 従業員等の採用面接時には、可能な範囲で身元を確認しましょう。	・記載内容の虚偽の有無を確認するため、従業員等の採用面接時には、可能な範囲で身元を確認しましょう。 ・確認時に用いる身分証、免許証、マイナンバーカード、各種証明書等は、可能な限り原本を確認しましょう。 ・外国籍の人に対しては「在留証明書」の原本を確認しましょう。 ・イベント期間中のみの臨時スタッフや派遣スタッフ等についても、同様となるように、派遣元等に依頼しておきましょう。 ・応募の動機や、自社に対するイメージ等も確認しましょう。 ・採用後も、住所や電話番号が変更されていないかを定期的に確認しましょう。	○従業員採用時の留意点（身元の確認等） 従業員等の採用面接時には、可能な範囲で身元を確認しましょう。	・記載内容の虚偽の有無を確認するため、従業員等の採用面接時には、可能な範囲で身元を確認しましょう。 ・確認時に用いる身分証、免許証、マイナンバーカード、各種証明書等は、可能な限り原本を確認しましょう。 ・外国籍の人に対しては「在留証明書」の原本を確認しましょう。 ・イベント期間中のみの臨時スタッフや派遣スタッフ等についても、同様となるように、派遣元等に依頼しておきましょう。 ・応募の動機や、自社に対するイメージ等も確認しましょう。 ・採用後も、住所や電話番号が変更されていないかを定期的に確認しましょう。	○従業員採用時の留意点（身元の確認等） 従業員等の採用面接時には、可能な範囲で身元を確認しましょう。	・記載内容の虚偽の有無を確認するため、従業員等の採用面接時には、可能な範囲で身元を確認しましょう。 ・確認時に用いる身分証、免許証、マイナンバーカード、各種証明書等は、可能な限り原本を確認しましょう。 ・外国籍の人に対しては「在留証明書」の原本を確認しましょう。 ・イベント期間中のみの臨時スタッフや派遣スタッフ等についても、同様となるように、派遣元等に依頼しておきましょう。 ・応募の動機や、自社に対するイメージ等も確認しましょう。 ・採用後も、住所や電話番号が変更されていないかを定期的に確認しましょう。	○有り 感染症発生時には従業員の居住地の保健所や医療機関との連携に有用	○無し
8			○従業員の配置 フードディフェンスに関する理解・経験の深い職員を重要箇所に配置しましょう。	・経験と信頼感のある従業員を重要な箇所に配置し、混入事故の事前防止や、同僚の不審な行動等の有無を見守りましょう。 ・脆弱性が高いと判断された工程や場所に配置する従業員は、事前に面談を行い、不平・不満を抱えていないかを確認しましょう。	○従業員の配置 フードディフェンスに関する理解・経験の深い職員を重要箇所に配置しましょう。	・経験と信頼感のある従業員を重要な箇所に配置し、混入事故の事前防止や、同僚の不審な行動等の有無を見守りましょう。 ・脆弱性が高いと判断された工程や場所に配置する従業員は、事前に面談を行い、不平・不満を抱えていないかを確認しましょう。 ・倉庫側の管理が及ばない外部	○従業員の配置 フードディフェンスに関する理解・経験の深い職員を重要箇所に配置しましょう。	・経験と信頼感のある従業員を重要な箇所に配置し、混入事故の事前防止や、同僚の不審な行動等の有無を見守りましょう。 ・脆弱性が高いと判断された工程や場所に配置する従業員は、事前に面談を行い、不平・不満を抱えていないかを確認しましょう。	○有り 感染症発生時には感染を受けた可能性のある者の特定に有用	☆有り 対面での面接は感染拡大の要因になるため注意が必要

No.	食品防御対策ガイドライン（食品製造工場向け）【平成25年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
						組織の従業員が荷揚げや搬入を行っている場合には、外部組織とも十分に連携した管理を行いましょう。				
9			○（従業員の健康管理） 日々、従業員の健康管理を適切に行いましょう。 飛沫や濃厚接触で感染拡大を起こりやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意しましょう。	・自身の健康管理の重要性について理解させましょう。 ・感染拡大が心配される感染症に罹患した際に無理に出勤した場合、同僚への感染拡大や、食品中への混入による食中毒の原因となります。 ・感染症に罹患した場合（同居の家族を含む）や、体調が優れない場合の出勤停止の考え方を予め整理し、従業員等の理解を得ておきましょう。 ・パンデミック等が発生した際には、通常の健康管理に加えて、勤務シフトの厳格化や、共有部分の小まめな清掃により、感染拡大予防に努めましょう。	○（従業員の健康管理） 日々、従業員の健康管理を適切に行いましょう。 飛沫や濃厚接触で感染拡大を起こりやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意しましょう。	・自身の健康管理の重要性について理解させましょう。 ・感染拡大が心配される感染症に罹患した際に無理に出勤した場合、同僚への感染拡大や、食品中への混入による食中毒の原因となります。 ・感染症に罹患した場合（同居の家族を含む）や、体調が優れない場合の出勤停止の考え方を予め整理し、従業員等の理解を得ておきましょう。 ・パンデミック等が発生した際には、通常の健康管理に加えて、勤務シフトの厳格化や、共有部分の小まめな清掃により、感染拡大予防に努めましょう。	○（従業員の健康管理） 日々、従業員の健康管理を適切に行いましょう。 飛沫や濃厚接触で感染拡大を起こりやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意しましょう。	・自身の健康管理の重要性について理解させましょう。 ・感染拡大が心配される感染症に罹患した際に無理に出勤した場合、同僚への感染拡大や、食品中への混入による食中毒の原因となります。 ・感染症に罹患した場合（同居の家族を含む）や、体調が優れない場合の出勤停止の考え方を予め整理し、従業員等の理解を得ておきましょう。 ・パンデミック等が発生した際には、通常の健康管理に加えて、勤務シフトの厳格化や、共有部分の小まめな清掃により、感染拡大予防に努めましょう。	○有り 日常からの感染予防、発生時の早期発見、感染拡大防止に有用。	☆有り 感染拡大時には、食品防御に必要なスタッフの確保が困難になる可能性があり、BCPの作成が必要となる。
10	○従業員等の異動・退職時等には制服や名札、IDバッジ、鍵（キーカード）を返却させる。		○（制服・名札等の管理） 従業員等の制服や名札、IDバッジ、鍵（キーカード）を適切に管理しましょう。	・製造施設への立ち入りや、従業員を見分けるために重要な制服や名札、IDバッジ、鍵（キーカード）等は厳重に管理しましょう。 ・名札や社員証等は、可能な限り顔写真付きのものにしましょう。 ・退職や異動の際には制服や名札、IDバッジ、鍵（キーカード）を確実に返却してもらいましょう。	○（制服・名札等の管理） 従業員等の制服や名札、IDバッジ、鍵（キーカード）を適切に管理しましょう。	・保管施設や仕分け現場への立ち入りや、従業員を見分けるために重要な制服や名札、IDバッジ、鍵（キーカード）等は厳重に管理しましょう。 ・名札や社員証等は、可能な限り顔写真付きのものにしましょう。 ・退職や異動の際には制服や名札、IDバッジ、鍵（キーカード）を確実に返却してもらいましょう。	○（制服・名札等の管理） 従業員等の制服や名札、IDバッジ、鍵（キーカード）を適切に管理しましょう。	・接客（食事提供）施設への立ち入りや、従業員を見分けるために重要な制服や名札、IDバッジ、鍵（キーカード）等は厳重に管理しましょう。 ・名札や社員証等は、可能な限り顔写真付きのものにしましょう。 ・退職や異動の際には制服や名札等を確実に返却してもらいましょう。	○有り 従業員の適切な管理は感染防止にも有用	○無し
11	○製造現場内へは原則として私物は持ち込まないこととし、これが遵守されていることを確認する。持ち込む必要がある場合は、個別に許可を得るようにする。	・製造現場内への持ち込み禁止品の指定は際限がないため、持ち込まないことを原則として、持ち込み可能品はリスト化すると共に、持ち込む場合は、個別に許可を得る方が管理しやすいと考えられる。 ・また、更衣室やロッカールームなども相互にチェックする体制を構築しておく。	○（私物の持込みと確認） 私物を製造現場内へは原則として持ち込まないこととし、これが遵守されていることを確認かを定期的に確認しましょう。	・私物は、異物混入や感染源となる可能性及び感染症の発生・拡大の予防のため、原則として製造現場内へは、持ち込まないようにしましょう。 ・私物（財布などの貴重品）は金庫などの鍵のかかる貴重品保管場所に保管し、作業場には原則として持ち込まないようにしましょう。 ・持ち込み可能品はリスト化しましょう。	○（私物の持込みと確認） 私物を仕分け現場へは原則として持ち込まないこととし、これが遵守されているかを定期的に確認しましょう。	・私物は、異物混入や感染源となる可能性及び感染症の発生・拡大の予防のため、原則として仕分け現場内へは持ち込まないようにしましょう。 ・私物（財布などの貴重品）は金庫などの鍵のかかる貴重品保管場所に保管し、作業場には原則として持ち込まないようにしましょう。 ・持ち込み可能品はリスト化しましょう。	○（私物の持込みと確認） 私物を食材や飲食料品保管庫・厨房・配膳の現場へは原則として持ち込まないこととし、これが遵守されているかを定期的に確認しましょう。	・私物は、異物混入や感染源となる可能性及び感染症の発生・拡大の予防のため、原則として食材保管庫や厨房、配膳、販売の現場内へは持ち込まないようにしましょう。 ・私物（財布などの貴重品）は金庫などの鍵のかかる貴重品保管場所に保管し、作業場には原則として持ち込まないようにしましょう。 ・持ち込み可能品はリスト化し	○有り 無制限な私物の持ち込みは、感染源となる可能性及び感染症の発生。拡大の要因となりうる。	☆有り

No.	食品防御対策ガイドライン （食品製造工場向け） 【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供 （店頭販売品を含む）	解説	感染症対策 としての 有用性	食品防御対策と 感染症対策の 並立時の課題
				・持ち込む場合には、個別に許可を得るなど、適切に管理しましょう。 ・更衣室やロッカールームなどでも相互にチェックできる体制を構築しておきましょう。 ・従業員立会いの下、不定期でロッカーを点検し、不審物の持込の未然防止に努めましょう。 ・換気で窓等を開ける際には、外部からの侵入に注意しましょう。		・持ち込む場合には、個別に許可を得るなど、適切に管理しましょう。 ・更衣室やロッカールームなどでも相互にチェックできる体制を構築しておきましょう。 ・従業員立会いの下、不定期でロッカーを点検し、不審物の持込の未然防止に努めましょう。 ・換気で窓等を開ける際には、外部からの侵入に注意しましょう。		ましょう。 ・持ち込む場合には、個別に許可を得るなど、適切に管理しましょう。 ・更衣室やロッカールームがある場合には、相互にチェックできる体制を構築しておきましょう。 ・共用のロッカー等を利用している場合、不審な荷物に気が付いた時には、ただちに責任者に報告しましょう。 ・換気で窓等を開ける際には、外部からの侵入に注意しましょう。		更衣室やロッカールームでの感染拡大防止に注意が必要（窓開け・換気等） 共用ロッカーも適切な消毒等が必要 換気のための窓開けには、防犯上の課題有。
12			○（休憩室・トイレ等の 5S の徹底） 休憩室やトイレ等も普段から 5S を心がけましょう。	・休憩室やトイレ等の 5S を普段から推奨しましょう。 ・感染症流行時には、感染源になることが指摘されている多くの人が触れるドアノブ・スイッチ類や休憩室等は入念に清掃・消毒をしましょう。 ・消毒用薬剤を利用する際には、その管理に注意しましょう。	○（休憩室・トイレ等の 5S の徹底） 休憩室やトイレ等も普段から 5S を心がけましょう。	・休憩室やトイレ等の 5S を普段から推奨しましょう。 ・感染症流行時には、感染源になることが指摘されている多くの人が触れるドアノブ・スイッチ類や休憩室等は入念に清掃・消毒をしましょう。 ・消毒用薬剤を利用する際には、その管理に注意しましょう。	○（休憩室・トイレ等の 5S の徹底） 休憩室やトイレ等も普段から 5S を心がけましょう。	・休憩室やトイレ等の 5S を普段から推奨しましょう。 ・感染症流行時には、感染源になることが指摘されている多くの人が触れるドアノブ・スイッチ類や休憩室等は入念に清掃・消毒をしましょう。 ・消毒用薬剤を利用する際には、その管理に注意しましょう。	○有り	☆有り 消毒用薬剤が異物混入に繋がる可能性があり、管理方法に留意が必要。
13	○従業員等の従来とは異なる言動、出退勤時間の著しい変化等を把握する。	・従業員等が犯行に及んだ場合の動機は、採用前から抱いていたものとは限らず、採用後の職場への不平・不満等も犯行動機となることも考えられる。 ・製造現場の責任者等は、作業前の朝礼、定期的なミーティング、個別面談等を通じて、従業員の心身の状態について確認するとともに、日常の言動や出退勤時刻の変化が見られる場合には、その理由についても確認する。	○（出勤時間･言動の変化等の把握） 従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握しましょう。	・従業員等が意図的な異物混入等を行う動機は、勤務開始後の職場への不平・不満等だけでなく、採用前の事柄が原因となることも考えられます。 ・製造現場の責任者等は、作業前の朝礼、定期的なミーティング、個別面談等を通じて、従業員の心身の状態や、職場への不満等について確認しましょう。 ・感染症が拡大している場合には、社員の健康状態にも十分に留意し、必要に応じて出勤時の検温等を実施しましょう。 ・日常の言動や出退勤時刻の変化が見られる場合には、その理由についても確認しましょう。 ・深夜の時間帯での勤務のみを	○（出勤時間･言動の変化等の把握） 従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握しましょう。	・従業員等が意図的な異物混入等を行う動機は、勤務開始後の職場への不平・不満等だけでなく、採用前の事柄が原因となることも考えられます。 ・物流・保管施設の責任者等は、作業前の朝礼、定期的なミーティング、個別面談等を通じて、従業員の心身の状態や、職場への不満等について確認しましょう。 ・感染症が拡大している場合には、社員の健康状態にも十分に留意し、必要に応じて出勤時の検温等を実施しましょう。 ・日常の言動や出退勤時刻の変化が見られる場合には、その理由についても確認しましょう。 ・深夜の時間帯での勤務のみを	○（出勤時間･言動の変化等の把握） 従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握しましょう。	・従業員等が意図的な異物混入等を行う動機は、勤務開始後の職場への不平・不満等だけでなく、採用前の事柄が原因となることも考えられます。 ・調理・提供施設の責任者等は、作業前の朝礼、定期的なミーティング、個別面談等を通じて、従業員の心身の状態や、職場への不満等について確認しましょう。 ・感染症が拡大している場合には、社員の健康状態にも十分に留意し、必要に応じて出勤時の検温等を実施しましょう。 ・日常の言動や出退勤時刻の変化が見られる場合には、その理由についても確認しましょう。 ・深夜の時間帯での勤務のみを	○有り 出退勤時間の変更の理由が体調不良の可能性があり、予兆として把握することが出来る。	○無し

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
				希望する者についても、同様にその理由を確認し、出退勤時間を管理しましょう。 ・他人への成りすましを防ぐため、指紋認証システムを出退勤のチェックに導入している企業もあります。		希望する者についても、同様にその理由を確認し、出退勤時間を管理しましょう。 ・他人への成りすましを防ぐため、指紋認証システムを出退勤のチェックに導入している企業もあります。		希望する者についても、同様にその理由を確認し、出退勤時間を管理しましょう。 ・他人への成りすましを防ぐため、指紋認証システムを出退勤のチェックに導入している企業もあります。		
14	○就業中の全従業員等の移動範囲を明確化する（全従業員等が、移動を認められた範囲の中で働いているようにする）。	・他部署への理由のない移動を制限し、異物が混入された場合の混入箇所を同定しやすくする。 ・制服や名札、帽子の色、IDバッジ等によって、全従業員の「移動可能範囲」や「持ち場」等を明確に識別できるようにする。	○（移動可能範囲の明確化） ○　就業中の全従業員等の移動範囲を明確化にし、全従業員等が、移動を認められた範囲の中で働いているようにしましょう。	・製品に異物が混入された場合の混入箇所を同定しやすくするために、施設の規模に応じて他部署への理由のない移動を制限しましょう。 ・感染症が疑われる場合には、原則自宅での療養を推奨し、やむを得ず勤務する場合は、感染による影響の大きい箇所での勤務は禁止しましょう。 ・制服や名札、帽子の色、IDバッジ等によって、全従業員の「移動可能範囲」や「持ち場」等を明確に識別できるようにしましょう。 ・倉庫内での荷物の運搬に利用するフォークリフト等にも運転者の氏名を表示するなど、使用者が分かりやすい状況を作りましょう。	○（移動可能範囲の明確化） 就業中の全従業員等の移動範囲を明確化にし、全従業員等が、移動を認められた範囲の中で働いているようにしましょう。	・取扱商品に異物が混入された場合の混入箇所を同定しやすくするために、施設の規模に応じて他部署への理由のない移動を制限しましょう。 ・感染症が疑われる場合には、原則自宅での療養を推奨し、やむを得ず勤務する場合は、感染による影響の大きい箇所での勤務は禁止しましょう。 ・制服や名札、帽子の色、IDバッジ等によって、全従業員の「移動可能範囲」や「持ち場」等を明確に識別できるようにしましょう。 ・倉庫内での荷物の運搬に利用するフォークリフト等にも運転者の氏名を表示するなど、使用者が分かりやすい状況を作りましょう。	○（移動可能範囲の明確化 規模の大きな施設では、就業中の全従業員等の移動範囲を明確化にし、全従業員等が、移動を認められた範囲の中で働いているようにしましょう。	・提供した飲食料品に異物が混入された場合の混入箇所を同定しやすくするために、施設の規模に応じて他部署への理由のない移動を制限しましょう。 ・感染症が疑われる場合には、自宅での待機・療養を原則とし、やむを得ず勤務する場合は、感染による影響の大きい箇所での勤務は禁止しましょう。 ・規模の大きな施設で、職制等により「移動可能範囲」を決めている場合には、制服や名札、帽子の色等によって、その従業員の「移動可能範囲」や「持ち場」等が明確に識別できるようにしましょう。	○有り 感染を受けた可能性のある者や消毒等が必要な場所の特定に有用	○無し
15	○新規採用者は、朝礼等の機会に紹介し、従業員に認知させ、従業員同士の識別度を高める。	・新規採用者を識別しやすくするとともに、従業員が見慣れない人の存在に疑問を持つ習慣を意識づける。	○（新規採用者の紹介） 新規採用者は、朝礼等の機会に紹介し、見慣れない人への対応力を高めましょう。	・新規採用者は朝礼等の機会に紹介し、皆さんに識別してもらいましょう。 ・見慣れない人の存在に従業員が疑問を持ち、一声かける習慣を身につけてもらいましょう。 ・日々の挨拶や態度で異変を感じたら直ぐに上司に報告しましょう。	○（新規採用者の紹介） 新規採用者は、朝礼等の機会に紹介し、見慣れない人への対応力を高めましょう。	・新規採用者は朝礼等の機会に紹介し、皆さんに識別してもらいましょう。 ・見慣れない人の存在に従業員が疑問を持ち、一声かける習慣を身につけてもらいましょう。 ・日々の挨拶や態度で異変を感じたら直ぐに上司に報告しましょう。	○（従業員の自己紹介） 新たな店舗等がスタートする際には、ミーティング等で自己紹介し、スタッフ同士の認識力を高め、見慣れない人への対応力を高めましょう。	・新たな店舗等での業務がスタートする際には、自己紹介等を行い、スタッフ同士の認識力を高めましょう。 ・応援スタッフや新規採用者は、その日の打合せ等の機会に紹介し、皆さんに識別してもらいましょう。 ・見慣れない人の存在に従業員が疑問を持ち、一声かける習慣を身につけてもらいましょう。 ・日々の挨拶や態度で異変を感じたら直ぐに上司に報告しましょう。	○有り 感染を受けた可能性のある者の早期の認識に有用	○無し

■人的要素（部外者）

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
16	○事前に訪問の連絡があった訪問者については、身元・訪問理由・訪問先（部署・担当者等）を確認し、可能な限り従業員が訪問場所まで同行する。	・訪問者の身元を、社員証等で確認する。訪問理由を確認した上で、従業員が訪問場所まで同行する。	○（訪問者への対応） ①　事前予約がある場合 身元・訪問理由・訪問先（部署・担当者等）を確認し、可能な限り従業員が訪問場所まで同行しましょう。 感染症の流行時は、直接の訪問は極力避けて頂く様にしましょう。	・訪問者の身元を、社員証等で確認しましょう（顔写真付が望ましい）。 ・感染症が流行している時期においては、体調確認に対する協力も要請しましょう。 ・訪問理由を確認した上で、従業員が訪問場所まで同行しましょう。	○（訪問者への対応） ①　事前予約がある場合 身元・訪問理由・訪問先（部署・担当者等）を確認し、可能な限り従業員が訪問場所まで同行しましょう。 感染症の流行時は、従業員との接触を極力避ける工夫を行いましょう。	・訪問者の身元を、社員証等で確認しましょう（顔写真付が望ましい）。 ・感染症が流行している時期においては、体調確認に対する協力も要請しましょう。 ・訪問理由を確認した上で、従業員が訪問場所まで同行しましょう。	○（訪問者への対応） ①　事前予約がある場合 身元・訪問理由・訪問先（部署・担当者等）を確認し、従業員が訪問場所まで同行しましょう。 感染症の流行時は、直接の訪問は極力避けて頂く様にしましょう。	・訪問者の身元を、社員証等で確認しましょう（顔写真付が望ましい）。 ・感染症が流行している時期においては、体調確認に対する協力も要請しましょう。 ・訪問理由を確認した上で、従業員が訪問場所まで同行しましょう。	○有り 事前予約は、感染判明後の対応に有用。	☆有り 同行の際には、濃厚接触に留意が必要。
17	○事前に訪問の連絡がなかった訪問者、かつ初めての訪問者は、原則として工場の製造現場への入構を認めない。	・「飛び込み」の訪問者については原則として製造現場への入構を認めない。 ・なお、訪問希望先の従業員に対して面識の有無や面会の可否等について確認が取れた場合は、事前に訪問の連絡があった訪問者と同様の対応を行う。	②事前予約がない場合や初めての訪問者 原則として事務所等で対応し、工場の製造現場への入構を認めないようにしましょう。 特に感染症の流行時は、注意しましょう。	・「飛び込み」の訪問者は、原則として製造現場には入構させず、事務所等で対応しましょう。 ・訪問希望先の従業員から、面識の有無や面会の可否等について確認が取れた場合は、事前予約がある場合と同様に対応しましょう。	②事前予約がない場合や初めての訪問者 原則として事務所等で対応し、仕分け現場を認めないようにしましょう。 特に感染症の流行時は、注意しましょう。	・「飛び込み」の訪問者は、原則として仕分け現場には入構させず、事務所等で対応しましょう。 ・訪問希望先の従業員から、面識の有無や面会の可否等について確認が取れた場合は、事前予約がある場合と同様に対応しましょう。	②事前予約がない場合や初めての訪問者 立ち入りを認めないようにしましょう。 特に感染症の流行時は、注意しましょう。	・「飛び込み」の訪問者は、原則として立ち入りは認めないようにしましょう。 ・訪問希望先の従業員から、面識の有無や面会の可否等について確認が取れた場合は、事前予約がある場合と同様に、従業員が訪問場所まで同行しましょう。	○有り 感染拡大期の飛び込みの訪問者には、特に注意が必要。	○無し
18	○訪問者（業者）用の駐車場を設定する。この際、製造棟とできるだけ離れていることが望ましい。	・全ての訪問者について車両のアクセスエリア、荷物の持ち込み等を一律に制限することは現実的ではない。 ・特定の訪問者（例：施設メンテナンス、防虫防鼠業者等）については、それらの車両であることが明確になるように、駐車エリアを設定しておく。	○（駐車エリアの設定や駐車許可証の発行） 訪問者（業者）用の駐車場を設定したり、駐車許可証を発行する等、無許可での駐車を防止しましょう。	・全ての訪問者について車両のアクセスエリア、荷物の持ち込み等を一律に制限することは現実的ではありません。 ・駐車エリアは、原材料や商品の保管庫やゴミ搬出場所等、直接食品に手を触れることができるような場所とはできるだけ離れていることが望ましいでしょう。 ・繰り返し定期的に訪問する特定の訪問者（例：施設メンテナンス、防虫防鼠業者等）については、それらの車両であることが明確になるように、駐車エリアを設定しておきましょう。	○（駐車エリアの設定や駐車許可証の発行） 訪問者（業者）用の駐車場を設定したり、駐車許可証を発行する等、無許可での駐車を防止しましょう。	・全ての訪問者について車両のアクセスエリア、荷物の持ち込み等を一律に制限することは現実的ではありません。 ・駐車エリアは、取扱商品保管庫やゴミの搬出場所等、直接商品に手を触れることができるような場所とはできるだけ離れていることが望ましいでしょう。 ・繰り返し定期的に訪問する特定の訪問者（例：施設メンテナンス、防虫防鼠業者等）については、それらの車両であることが明確になるように、駐車エリアを設定しておきましょう。	○（駐車エリアの設定や駐車許可証の発行） 規模の大きな施設では、納入業者用や廃棄物収集車の駐車場を設定したり、駐車許可証を発行する等、無許可での進入や駐車を防止しましょう。	・全ての訪問者について車両のアクセスエリア、荷物の持ち込み等を一律に制限することは現実的ではありません。 ・専用の駐車エリアがある場合には、食材保管庫やゴミ搬出場所等、直接食品に手を触れることができるような場所とはできるだけ離れていることが望ましいでしょう。 ・繰り返し定期的に訪問する特定の訪問者（例：施設メンテナンス、防虫防鼠業者等）については、それらの車両であることが明確になるように、可能な範囲で駐車エリアを設定しておきましょう。	○有り 接触場所等の把握に有用	○無し
19	○食品工場の施設・設備のメンテナンスや防虫・防鼠作業等のため、工場内を単独で行動する可能性のある訪問者（業者）には、持ち物を十分確認し、不要なものを持ち込ませないようにする。	・食品工場の施設・設備のメンテナンスや防虫・防鼠等に関する作業員は、長時間にわたり多人数で作業することもあるため、従業員が全ての作業員の作業に同行することは困難である。 ・作業開始前に、持ち物の確認を実施し、不要な持ち込み品の管理を徹底する。	○（業者の持ち物確認） 食品工場内を単独で行動する可能性のある訪問者（業者）の持ち物は十分確認し、不要なものを持ち込ませないようにしましょう。	・施設・設備のメンテナンスや防虫・防鼠等のために、長時間にわたり施設内で作業することもある業者については、全ての作業に同行することは困難です。 ・立入り業者については、制服・顔写真付き社員証等を確認しましょう。 ・作業開始前には、持ち物の確認を実施し、不要な持ち込み	○（業者の持ち物確認） 物流・保管施設内を単独で行動する可能性のある訪問者（業者）の持ち物は十分確認し、不要なものを持ち込ませないようにしましょう。	・施設・設備のメンテナンスや防虫・防鼠等のために、長時間にわたり施設内で作業することもある業者については、全ての作業に同行することは困難です。 ・立入り業者については、制服・顔写真付き社員証等を確認しましょう。 ・作業開始前には、持ち物の確認を実施し、不要な持ち込み	○（業者の持ち物確認） 厨房や店舗等の施設・設備内を単独で行動する可能性のある訪問者（業者：報道関係・警備関係を含む）の持ち物は十分確認し、不要なものを持ち込ませないようにしましょう。	・施設・設備のメンテナンスや防虫・防鼠等、取材・警備等のために、長時間にわたり施設内で作業することもある業者については、全ての作業に同行することは困難です。 ・立入り業者については、制服・顔写真付き社員証等を確認しましょう。 ・作業開始前には、持ち物の確認を実施し、不要な持ち込み	や感染を受けた可能性のある者の特定に有用。	○無し

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
				品を持ち込ませないようにしましょう。 ・可能であれば、入場時と退場時に業者の同意を得て、鞄を開けた状態でデジタルカメラによる写真撮影により、証拠を残しましょう。		品を持ち込ませないようにしましょう。 ・可能であれば、入場時と退場時に業者の同意を得て、鞄を開けた状態でデジタルカメラによる写真撮影により、証拠を残しましょう。		品を持ち込ませないようにしましょう。 ・可能であれば、持込み可能品リストを作成し、それ以外のものを持ち込む場合には、申告してもらいましょう。		
20	―	―	―	―	―	―	○（悪意を持った来客対策） 来客の中には悪意を持っている者がいる可能性も考慮しましょう。	・来店するお客の中には、店舗等に悪意を持っている人がいる可能性も否定できません。 ・お客によるいたずら等を防ぐために、大規模イベント時に必要な対応を参考にした対策を採りましょう。	○有り 感染を受けた可能性のある者の特定に有用	☆有り 悪意を持った来客は、感染予防にも非協力的と考えられる。
21	○郵便、宅配便の受け入れ先（守衛所、事務所等）を定めておく。また配達員の敷地内の移動は、事前に設定した立ち入り可能なエリア内のみとする。	・信書と信書以外の郵便物、また宅配物等の届け物や受取人の違いにより、配達員は比較的自由に食品工場の敷地内を移動できる状況にあるため、郵便、宅配物等の受け入れ先は数箇所の定められた場所に限定する。 ・また、郵便局員や宅配業者が、食品工場の建屋内に無闇に立ち入ることや、建屋外に置かれている資材・原材料や製品に近づくことができないよう留意する。	○（郵便・宅配物の受取場所） 郵便、宅配物等の受け入れ先（守衛所、事務所等）を定めておきましょう。	・郵便局員や宅配業者が、食品工場の建屋内に無闇に立ち入ることや、施設内に置かれている食材等に近づくことは、異物混入の危険性を高めます。 ・郵便、宅配物等の受け入れ先は、守衛所、事務所等の数箇所の定められた場所に限定しておきましょう。 ・郵便局員や宅配業者が、食品工場内に無闇に立ち入ることや、建屋外に置かれている資材・原材料や製品に近づけないように、立ち入り可能なエリアを事前に設定しておきましょう。	○（郵便・宅配物の受取場所） 郵便、宅配物等の受け入れ先（守衛所、事務所等）を定めておきましょう。	・郵便局員や宅配業者が、物流・保管施設の建屋内に無闇に立ち入ることや、施設内に置かれている商品等に近づくことは、異物混入の危険性を高めます。 ・郵便、宅配物等の受け入れ先は、守衛所、事務所等の数箇所の定められた場所に限定しておきましょう。 ・郵便局員や宅配業者が、物流・保管施設内に無闇に立ち入ることや、取扱商品等に近づけないように、立ち入り可能なエリアを事前に設定しておきましょう。	―	―	○有り 接触した場所や感染を受けた可能性のある者の限定にも繋がる。	○無し

■施設管理

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
22	○不要な物、利用者・所有者が不明な物の放置の有無を定常的に確認する。	・食品工場で使用する原材料や工具等について、定数・定位置管理を行い、過不足や紛失に気づきやすい環境を整える。 ・また、食品に直接手を触れることができる製造工程や従事者が少ない場所等、意図的に有害物質を混入	○（調理器具等の定数管理） 使用する原材料や調理器具、洗剤等について、定位置・定数管理を行いましょう。	・食品工場で使用する原材料や工具等について、定位置・定数管理を行い、過不足や紛失に気づきやすい環境を整えましょう。 ・不要な物、利用者・所有者が不明な物の放置の有無を定常的に確認しましょう。 ・食品に直接手を触れることが	○（仕分け用具等の定数管理） 使用する仕分け作業用の器具や工具等について、定位置・定数管理を行いましょう。	・物流施設で使用する機器や工具等について、定位置・定数管理を行い、過不足や紛失に気づきやすい環境を整えましょう。 ・不要な物、利用者・所有者が不明な物の放置の有無を定常的に確認しましょう。 ・取扱商品に直接手を触れるこ	○（調理器具等の定数管理） 使用する原材料や調理器具、洗剤等について、定位置・定数管理を行いましょう。	・厨房や店舗で使用する原材料や調理器具、洗剤等について、定位置・定数管理を行うことで、過不足や紛失に気づきやすい環境を整えましょう。 ・不要な物、利用者・所有者が不明な物の放置の有無を定常的に確認しましょう。	○有り 感染者が利用した機器等の特定に有用	○無し

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
		し易い箇所については特に重点的に確認する。		できる製造工程や従事者が少ない場所等、意図的に有害物質を混入し易い箇所については特に重点的に確認しましょう。 ・配電盤等不要な物を隠せる場所には、施錠等の対応を行いましょう。		とができる分別工程や従事者が少ない場所等、意図的に有害物質を混入し易い箇所については特に重点的に確認しましょう。 ・配電盤等不要な物を隠せる場所には、施錠等の対応を行いましょう。		・食品に直接手を触れることができる調理・盛り付け・配膳・受渡し場所や従事者が少ない場所等、意図的に有害物質を混入し易い箇所については特に重点的に確認しましょう。 ・配電盤等不要な物を隠せる場所には、施錠等の対応を行いましょう。 ・医薬品が保管されている医務室等については、医師・患者等関係者以外の立入の禁止、無人となる時間帯の施錠、薬剤の数量管理を徹底する。		
23	○食品に直接手を触れることができる仕込みやや袋詰めの工程や、従事者が少ない場所等、意図的に有害物質を混入しやすい箇所を把握し、可能な限り手を触れない様にカバーなどの防御対策を検討する。	・仕込みや包装前の製品等に直接手を触れることが可能な状況が見受けられる。 ・特に脆弱性が高いと判断された箇所は、見回りの実施、従業員同士による相互監視、監視カメラの設置等を行うと共に、可能な限り手を触れられない構造に改修する。	○（脆弱性の高い場所の把握と対策） 食品に直接手を触れることができる仕込みや袋詰めの工程や、従事者が少ない場所等、意図的に有害物質を混入しやすい箇所を把握し、可能な限り手を触れない様にカバーなどの防御対策を検討しましょう。	・仕込みや包装前の製品等に直接手を触れることが可能な状況が見受けられる。 ・特に脆弱性が高いと判断された箇所は、見回りの実施、従業員同士による相互監視、監視カメラの設置等を行うと共に、可能な限り手を触れられない構造に改修しましょう。	○（脆弱性の高い場所の把握と対策） 食品に直接手を触れることができる仕分けや袋詰め工程や、従事者が少ない場所等、意図的に有害物質を混入しやすい箇所を把握し、可能な限り手を触れない様にカバーなどの防御対策を検討しましょう。	・仕分けや梱包前の製品等に直接手を触れることが可能な状況が見受けられる。 ・特に脆弱性が高い箇所は、見回りの実施、従業員同士による相互監視、監視カメラの設置等を行うと共に、可能な限り手を触れられない構造に改修しましょう。	○（脆弱性の高い場所の把握と対策） 食品に直接手を触れることができる調理や配膳の工程や店頭販売品の受渡し場所、従事者が少ない場所等、意図的に有害物質を混入しやすい箇所を把握しましょう。	・調理や配膳・受渡し場所では、飲食料等に直接手を触れないことは不可能です。 ・特に脆弱性が高いと考えられる人目の少ない箇所（配膳準備室・厨房から宴会場までのルート）等は、見回りの実施、従業員同士による相互監視、監視カメラの設置等を行うと共に、可能な限り手を触れられない構造への改修や、配膳方法に工夫をしましょう。・レストランや食堂等の客席に備え付けの飲料水や調味料、バイキング形式のサラダバーなどでは、従業員以外の人物による意図的な有害物質の混入にも注意を払いましょう。 ・屋外の販売用の屋台等でも注意しましょう。 ・店舗の設計に際しては、食品防御を意識した作業動線や人の流れを考慮しましょう。	○有り 感染の可能性がある場所の特定に有用 感染の予防に有用 利用客用の動線を考慮した手洗い場等の設置も有用	○無し
24	○工場が無人となる時間帯についての防犯対策を講じる。	—	○（無人の時間帯の対策） 工場が無人となる時間帯についての防犯対策を講じましょう。	・工場が無人となる時間帯は、万が一、混入が行われた場合の対応が遅れます。 ・終業後は必ず施錠し、確認する習慣を身につけましょう。	○（無人の時間帯の対策） 物流・保管施設が無人となる時間帯についての防犯対策を講じましょう。	・物流・保管施設が無人となる時間帯は、万が一、混入が行われた場合の対応が遅れます。 ・終業後は必ず施錠し、確認す	○（無人の時間帯の対策） 厨房・食事提供施設・店舗が無人となる時間帯（閉店後を含む）についての防犯対策を講じましょう。	・食品保管庫や厨房等が無人となる時間帯は、万が一、混入が行われた場合の対応が遅れます。 ・終業後は必ず施錠し、確認す	○有り 無人の時間帯の防犯対策は、時間外に施設に入った者の	○無し

No.	食品防御対策ガイドライン（食品製造工場向け）【平成25年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
				・製造棟が無人となる時間帯は必ず施錠し、人が侵入できないようにしましょう。 ・施錠以外にも、無人の時間帯の防犯対策を講じましょう。		る習慣を身につけましょう。 ・物流・保管施設が無人となる時間帯は必ず施錠し、人が侵入できないようにしましょう。 ・施錠以外にも、無人の時間帯の防犯対策を講じましょう。		る習慣を身につけましょう。 ・食品保管庫や厨房・店舗が無人となる時間帯は必ず施錠し、人が侵入できないようにしましょう。 ・施錠以外にも、監視（品質向上）カメラ等、無人の時間帯の防犯対策を講じましょう。	確認に有用	
25	○鍵の管理方法を策定し、定期的に確認する。	・最低限、誰でも自由に鍵を持ち出せるような状態にならないよう管理方法を定め、徹底する。	○（鍵の管理） 鍵の管理方法を策定し、定期的に確認しましょう。	・鍵の使用権を設定し、誰でも自由に鍵を持ち出せないようにしましょう。 ・鍵の管理方法を定め、順守されているかどうかを確認しましょう。	○（鍵の管理） 鍵の管理方法を策定し、定期的に確認しましょう。	・鍵の使用権を設定し、誰でも自由に鍵を持ち出せないようにしましょう。 ・鍵の管理方法を定め、順守されているかどうかを確認しましょう。	○（鍵の管理） 鍵の管理方法を策定し、定期的に確認しましょう。	・鍵の使用権を設定し、誰でも自由に鍵を持ち出せないようにしましょう。 ・鍵の管理方法を定め、順守されているかどうかを確認しましょう。	○有り 鍵の使用権は行動範囲にも影響するため有用 感染者が鍵を利用した場合の消毒にも有用	☆有り 使用権の設定が厳しすぎると、対応者の負担が大きい。
26	○製造棟、保管庫は、外部からの侵入防止のため、機械警備、定期的な鍵の取り換え、補助鍵の設置、格子窓の設置等の対策を行う。	・食品工場内の全ての鍵を定期的に交換することは現実的ではない。 ・異物が混入された場合の被害が大きいと考えられる製造棟や保管庫については、補助鍵の設置や定期的な点検を行うなどの侵入防止対策を採ることが重要である。	○（外部からの侵入防止策） 製造棟、保管庫への外部からの侵入防止対策を行いましょう。	・異物が混入された場合の被害が大きいと考えられる製造棟、保管庫は、機械警備、補助鍵の設置や、格子窓の設置、定期的な点検を行い、侵入防止対策を採りましょう。	○（外部からの侵入防止策） 物流・保管施設への外部からの侵入防止対策を行いましょう。	・異物が混入された場合の被害が大きいと考えられる物流・保管施設は、機械警備、補助鍵の設置や、格子窓の設置、定期的な点検を行い、侵入防止対策を採りましょう。	○（外部からの侵入防止策） 店頭販売品を含む飲食料品の保管庫や厨房への外部からの侵入防止対策を行いましょう。	・異物が混入された場合の被害が大きいと考えられる食品保管庫や厨房・店舗は、機械警備、補助鍵の設置や、格子窓の設置、定期的な点検を行い、侵入防止対策を採りましょう。 ・店舗外のプレハブ倉庫等に食材を保管している場合も、適切に施錠しましょう。 ・通常施錠されているところが開錠されている等、定常状態と異なる状態を発見した時には、速やかに責任者に報告しましょう。	○有り 外部からの病原菌等の持ち込み防止に有用	○無し
27	○製造棟の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を採る。	・製造棟が無人となる時間帯は必ず施錠し、人が侵入できないようにする。全ての出入り口・窓に対して直ちに対策を講じることが困難な場合は、優先度を設定し、施設の改築等のタイミングで順次改善策を講じるように計画する。	○（確実な施錠） 製造棟の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を採りましょう。	・全ての出入り口・窓に対して直ちに対策を講じることが困難な場合は、優先度を設定し、施設の改築等のタイミングで順次改善策を講じるように計画しましょう。	○（確実な施錠） 物流・保管施設の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を採りましょう。	・全ての出入り口・窓に対して直ちに対策を講じることが困難な場合は、優先度を設定し、施設の改築等のタイミングで順次改善策を講じるように計画しましょう。	○（確実な施錠） 店頭販売品を含む飲食料品の保管庫や厨房の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を採りましょう。	・全ての出入り口・窓に対して直ちに対策を講じることが困難な場合は、優先度を設定し、施設の改築等のタイミングで順次改善策を講じるように計画しましょう。	○有り 外部からの感染者の侵入防止に有用	○無し
28	○食品工場内の試験材料（検査用試薬・陽性試料等）や有害物質については保管場所を定めた上で、当該場所への人の出入り管理を行うと共	・試験材料（検査用試薬・陽性試料等）の保管場所は検査・試験室内等に制限する。無断で持ち出されることの無いよう定期的に保	○（試験材料等の管理） 食品工場内の試験材料（検査用試薬・陽性試料等）や有害物質の保管場所を定め、当該場所への人の出入りを管理	・試験材料（検査用試薬・陽性試料等）の保管場所は検査・試験室内等に制限しましょう。 ・無断で持ち出されることの無	—	—	○（洗剤等の保管場所） 厨房や店舗の洗剤等、有害物質の保管場所を定め、当該場所への人の出入りを管理しましょう。また、使用日時や	・日常的に使用している洗剤等についても、作業動線等も考慮した管理方法等を定め、在庫量を定期的に確認しましょう。 ・保管は、食材保管庫や調理・料	○有り 洗剤は汚染された食器や機器等の洗浄に不可欠。	☆有り 洗剤や手指消毒用薬剤等は使いやすい場所への設置が必要。設

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
	に、使用日時及び使用量の記録、施錠管理を行う。	管数量の確認を行う。可能であれば警備員の巡回やカメラ等の設置を行う。	しましょう。また、使用日時や使用量の記録、施錠管理を行いましょう。	いよう定期的に保管数量を確認しましょう。 ・可能であれば警備員の巡回やカメラ等の設置を行いましょう。			使用量の記録、施錠管理を行いましょう。	理の保管エリア、店頭販売品の受渡し場所から離れた場所とし、栓のシーリング等により、妥当な理由無く使用することが無いよう、十分に配慮しましょう。		置場所の検討が必要。
29	○食品工場内の試験材料（検査用試薬・陽性試料等）や有害物質を紛失した場合は、工場長や責任者に報告し、工場長や責任者はその対応を決定する。	・法令等に基づき管理方法等が定められているものについては、それに従い管理を行う。 ・それ以外のものについては、管理方法等を定め、在庫量の定期的な確認、食品の取扱いエリアや食品の保管エリアから離れた場所での保管、栓のシーリング等により、妥当な理由無く有害物質を使用することの無いよう、十分に配慮した管理を行う。また試験材料や有害物質の紛失が発覚した場合の通報体制や確認方法を構築する。	○（紛失時の対応） 食品工場内の試験材料（検査用試薬・陽性試料等）や有害物質を紛失した場合は、工場長や責任者に報告し、工場長や責任者はその対応を決定しましょう。	・法令等に基づき管理方法等が定められているものについては、それに従い管理しましょう。 ・それ以外のものについても管理方法等を定め、在庫量の定期的な確認、食品の取扱いエリアや食品の保管エリアから離れた場所での保管、栓のシーリング等により、妥当な理由無く有害物質を使用することの無いよう、十分に配慮した管理を行いましょう。 ・試験材料や有害物質の紛失が発覚した場合の通報体制や確認方法を構築しておきましょう。	―	―	○（洗剤等の紛失時の対応） 厨房の洗剤等、有害物質を紛失した場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定しましょう。	―	○有り	○無し
30	○殺虫剤の保管場所を定め、施錠による管理を徹底する。	・食品工場の従業員等が自ら殺虫・防鼠等を行う場合は、使用する殺虫剤の成分について事前に確認しておくことが重要である。 ・殺虫剤を保管する場合は鍵付きの保管庫等に保管し、使用場所、使用方法、使用量等に関する記録を作成する。 ・防虫・防鼠作業の委託する場合は、信頼できる業者を選定し、殺虫対象、殺虫を行う場所を勘案して、委託業者とよく相談の上、殺虫剤（成分）を選定する。 ・殺虫・防鼠等を委託する場合、殺虫剤は委託業者が持参することになるが、工場長等が知らないうちに、委託業者から従業員等が殺虫剤を譲り受けたり、工場内に保管したりするよう	○（殺虫剤の管理） 殺虫剤の使用目的や保管場所を定め、施錠による管理を徹底しましょう。	・食品工場の従業員等が自ら殺虫・防鼠等を行う場合は、使用する殺虫剤の成分について事前に確認しておくことが重要です。 ・殺虫剤を施設内で保管する場合は、鍵付きの保管庫等に保管し、使用場所、使用方法、使用量等に関する記録を作成しましょう。 ・防虫・防鼠作業を委託する場合は、信頼できる業者を選定し、殺虫対象、殺虫を行う場所を勘案して、委託業者とよく相談の上、殺虫剤（成分）を選定しましょう。 ・殺虫・防鼠等を委託する場合、殺虫剤は委託業者が持参することになりますが、施設責任者等が知らないうちに、委託業者から従業員等が殺虫剤を譲り受けたり、施設内に保管したりするようなことがない	○（殺虫剤の管理） 殺虫剤の使用目的や保管場所を定め、施錠による管理を徹底しましょう。	・物流施設の従業員等が自ら殺虫・防鼠等を行う場合は、使用する殺虫剤の成分について事前に確認しておくことが重要です。 ・殺虫剤を施設内で保管する場合は、鍵付きの保管庫等に保管し、使用場所、使用方法、使用量等に関する記録を作成しましょう。 ・防虫・防鼠作業を委託する場合は、信頼できる業者を選定し、殺虫対象、殺虫を行う場所を勘案して、委託業者とよく相談の上、殺虫剤（成分）を選定しましょう。 ・殺虫・防鼠等を委託する場合、殺虫剤は委託業者が持参することになりますが、施設責任者等が知らないうちに、委託業者から従業員等が殺虫剤を譲り受けたり、施設内に保管したりするようなことがない	○（殺虫剤の管理） 殺虫剤の使用目的や保管場所を定め、施錠による管理を徹底しましょう。	・調理・提供施設・店舗の従業員等が自ら殺虫・防鼠等を行う場合は、使用する殺虫剤の成分について事前に確認しておくことが重要です。 ・殺虫剤を施設内で保管する場合は、鍵付きの保管庫等に保管し、使用場所、使用方法、使用量等に関する記録を作成しましょう。 ・防虫作業を委託する場合は、信頼できる業者を選定し、殺虫対象、殺虫を行う場所を勘案して、委託業者とよく相談の上、殺虫剤（成分）を選定しましょう。 ・殺虫・防鼠等を委託する場合、殺虫剤は委託業者が持参することになりますが、施設責任者等が知らないうちに、委託業者から従業員等が殺虫剤を譲り受けたり、施設内に保管したりするようなこと	○有り 媒介動物による感染症防止に有用	○無し

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
		なことがないよう、管理を徹底する。		よう、管理を徹底しましょう。		よう、管理を徹底しましょう。		がないよう、管理を徹底しましょう。 ・24 時間営業等で営業時間帯に店舗内の清掃を行う場合には、店員の目の届く範囲で作業を行うなど、異物混入に留意しましょう。		
31	○井戸、貯水、配水施設への侵入防止措置を講じる。	・井戸、貯水、配水施設への出入り可能な従業員を決め、鍵等による物理的な安全対策、防御対策を講じる。	○（給水施設の管理） 井戸、貯水、配水施設への侵入防止措置を講じましょう。	・井戸、貯水、配水施設への出入り可能な従業員を決めましょう。 ・井戸、貯水、配水施設への立入防止のため、鍵等による物理的な安全対策、防御対策を講じましょう。 ・貯水槽等の試験用水取出し口や塩素投入口、空気抜き等からの異物混入防止対策を講じましょう。 ・浄水器のフィルターについても定期的に確認しましょう。	—	—	○（給水施設の管理） 井戸、貯水、配水施設への侵入防止措置を講じましょう。	・井戸、貯水、配水施設への出入り可能な従業員を決めましょう。 ・井戸、貯水、配水施設への立入防止のため、鍵等による物理的な安全対策、防御対策を講じましょう。 ・貯水槽等の試験用水取出し口や塩素投入口、空気抜き等からの異物混入防止対策を講じましょう。 ・浄水器のフィルターについても定期的に確認しましょう。	○有り 水系感染症の予防に有用	○無し
32	○井戸水を利用している場合、確実な施錠を行い、塩素消毒等浄化関連設備へのアクセスを防止すると共に、可能であれば監視カメラ等で監視する。	・井戸水に毒物を混入された場合の被害は、工場全体に及ぶため、厳重な管理が必要である。	○（井戸水の管理） 井戸水に毒物を混入された場合の被害は、工場全体に及ぶため、厳重な管理が必要です。	・井戸水を利用している場合は、確実に施錠し、塩素消毒等浄化関連設備へのアクセスを防止しましょう。 ・可能であれば監視カメラ等で監視しましょう。	—	—	○（井戸水の管理） 井戸水に毒物を混入された場合の被害は、接客（食事提供）施設全体に及ぶため、厳重な管理が必要です。	・井戸水を利用している場合は確実に施錠し、塩素消毒等浄化関連設備へのアクセスを防止しましょう。 ・可能であれば監視カメラ等で監視しましょう。	○有り 水系感染症の予防に有用	○無し
33	○コンピューター処理制御システムや重要なデータシステムについて、従業員の異動・退職時等に併せてアクセス権を更新する。アクセス許可者は極力制限し、データ処理に関する履歴を保存する。	・コンピューター処理制御システムや重要なデータシステムにアクセス可能な従業員をリスト化し、かつシステムの設置箇所に鍵を設ける、ログインパスワードを設ける等の物理的なセキュリティ措置を講じる。	○（コンピューターの管理） コンピューター処理制御システムや重要なデータシステムへのアクセス許可者は極力制限し、不正なアクセスを防止しましょう。	・コンピューター処理制御システムや重要なデータシステムにアクセス可能な従業員をリスト化し、従業員の異動・退職時等に併せてアクセス権を更新しましょう。 ・アクセス許可者は極力制限し、データ処理に関する履歴を保存しましょう。 ・システムの設置箇所に鍵を設ける、ログインパスワードを設ける等の物理的なセキュリティ措置を講じましょう。	○（コンピューターの管理） コンピューター処理制御システムや重要なデータシステムへのアクセス許可者は極力制限し、不正なアクセスを防止しましょう。	・コンピューター処理制御システムや重要なデータシステムにアクセス可能な従業員をリスト化し、従業員の異動・退職時等に併せてアクセス権を更新しましょう。 ・アクセス許可者は極力制限し、データ処理に関する履歴を保存しましょう。 ・システムの設置箇所に鍵を設ける、ログインパスワードを設ける等の物理的なセキュリティ措置を講じましょう。	○顧客情報の管理 喫食予定の VIP の行動や食事内容に関する情報へのアクセス可能者は、接客の責任者などに限定しましょう。	—	○有り 感染を受けた可能性のある者が疑われる場合の連絡に不可欠	○無し
34			○（監視カメラの管理） 監視カメラの映像の外部流出に注意しましょう。	・監視カメラの映像は、外部に流出しないよう、適切に管理しましょう。 ・特にクラウド型の監視カメラのパスワードは、初期設定のまま使用せず、定期的に変更し、部外者に見られない対策を取りまし	○（監視カメラの管理） 監視カメラの映像の外部流出に注意しましょう。	・監視カメラの映像は、外部に流出しないよう、適切に管理しましょう。 ・特にクラウド型の監視カメラのパスワードは、初期設定のまま使用せず、定期的に変更し、部外者に見られない対策	○（監視カメラの管理） 監視カメラの映像の外部流出に注意しましょう。	・監視カメラの映像は、外部に流出しないよう、適切に管理しましょう。 ・特にクラウド型の監視カメラのパスワードは、初期設定のまま使用せず、定期的に変更し、部外者に見られない対策を取		

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
				ょう。		を取りましょう。		りましょう。		

■入出荷等の管理

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
35	○資材や原材料等の受け入れ時及び使用前に、ラベルや包装を確認する。異常を発見した場合は、工場長や責任者に報告し、工場長や責任者はその対応を決定する。	―	○（ラベル・包装・数量の確認） 資材や原材料等の受け入れ時及び使用前に、ラベルや包装の異常の有無、納入製品・数量と、発注製品・数量との整合性を確認しましょう。 異常を発見した場合は、工場長や責任者に報告し、工場長や責任者はその対応を決定しましょう。	・資材や原材料等の受け入れ時や使用前には、必ずラベルや包装を確認しましょう。 ・異常が発見された場合は、異物混入の可能性も念頭に、責任者に報告し、施設責任者はその対応を決定しましょう。 ・数量が一致しない場合は、その原因を確認しましょう。 ・納入数量が増加している場合は特に慎重に確認し、通常とは異なるルートから商品等が紛れ込んでいないかに注意を払いましょう。 ・運搬時のコンテナ等の封印など、混入しづらく、混入が分かりやすい対策も検討しましょう。	○（ラベル・包装・数量の確認） 取扱商品等の受け入れ時及び仕分け前に、ラベルや包装の異常の有無、納入製品・数量と、発注製品・数量との整合性を確認しましょう。 異常を発見した場合は、施設責任者に報告し、責任者はその対応を決定しましょう。 ・入荷時には、事前に発送元から通知のあったシリアルナンバーと製品・数量に間違いがないかを確認しましょう。 ・出荷時には、シリアルナンバーの付いた封印を行い、製品・数量とともに荷受け側に予め通知をする。事前通知には、車両のナンバーやドライバーの名前なども通知することが望ましい。	・取扱商品等の受け入れ時や仕分け前には、必ずラベルや包装、数量を確認しましょう。 ・異常が発見された場合は、異物混入の可能性も念頭に、施設責任者に報告し、施設責任者はその対応を決定しましょう。 ・数量が一致しない場合は、その原因を確認しましょう。 ・納入数量が増加している場合は特に慎重に確認し、通常とは異なるルートから商品等が紛れ込んでいないかに注意を払いましょう。 ・運搬時のコンテナ等の封印など、混入しづらく、混入が分かりやすい対策も検討しましょう。	○（ラベル・包装・数量の確認） 食材や食器等の受け入れ時及び使用前に、ラベルや包装の異常の有無、納入製品・数量と、発注製品・数量との整合性を確認しましょう。 異常を発見した場合は、料理長や責任者に報告し、料理長や責任者はその対応を決定しましょう。	・食材だけでなく食器や容器等の受け入れ時や使用前には、必ず数量やラベル・包装を確認しましょう。 ・異常が発見された場合は、異物混入の可能性も念頭に、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定しましょう。 ・数量が一致しない場合は、その原因を確認しましょう。 ・納入数量が増加している場合は特に慎重に確認し、通常とは異なるルートから商品等が紛れ込んでいないかに注意を払いましょう。 ・加工センターで調理された食材の配送は、契約した配送業者に依頼しましょう。 ・食材等は定期的な棚卸しの実施や売上との乖離の確認により、定期的に点検しましょう。	○有り 適切な包装は感染予防にも有用	○無し
36	○資材や原材料等の納入時の積み下ろし作業や製品の出荷時の積み込み作業を監視する。	・積み下ろし、積み込み作業は食品防御上脆弱な箇所である。実務上困難な点はあるが、相互監視や、可能な範囲でのカメラ等による監視を行う。	○（積み下ろしや積み込み作業の監視） 資材や原材料等の納入時の積み下ろし作業や製品の出荷時の積み込み作業を監視しましょう。	・資材や原材料等積み下ろし、積み込み作業は、人目が少なかったり、外部の運送業者等が行うことがあるため、食品防御上脆弱な箇所と考えられます。 ・実務上困難な点もありますが、相互監視や可能な範囲でのカメラ等による監視を行う等、何からの対策が望まれています。 ・感染症拡大時には、感染予防に注意して監視作業を行いましょう。	○（積み下ろしや積み込み作業の監視） 取扱商品等の納入時の積み下ろし作業や出荷時の積み込み作業にも気を配りましょう。	・積み下ろし、積み込み作業は、人目が少なかったり、外部の運送業者等が行うことがあるため、食品防御上脆弱な箇所と考えられます。 ・実務上困難な点もありますが、相互監視や可能な範囲でのカメラ等による監視を行う等、何からの対策が望まれています。 ・感染症拡大時には、感染予防に注意して監視作業を行いましょう。	○（積み下ろしの監視） 食材や食器・店頭販売品等の納入時の積み下ろし作業は確認しましょう。	・食材や食器・店頭販売品等の納入作業は、食品防御上脆弱な箇所と考えられます。 ・実務上困難な点はありますが、従業員や警備スタッフの立会や、可能な範囲でのカメラ等による確認を行いましょう。 ・無人の時間帯に食材等が搬入される場合は、カメラ等による確認を行いましょう。 ・感染症拡大時には、感染予防に注意して監視作業を行いましょう。	○有り	☆有り 監視の際には濃厚接触にならないよう注意が必要。

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
					○（製品等の混在防止対策） ハイセキュリティ製品と一般製品が混ざる事の無いように動線を確保し、物理的に分離して保管しましょう。また監視カメラを設置するなどの対策が望ましい。	・運搬・保管施設では、大規模イベント用の商品と一緒に一般の商品を取り扱う場合があるため、枠で囲う、ラインを分けるなどの対策が必要です。	○（調理や配膳作業・店頭販売品の保管庫の監視） 調理や料理等の配膳時の作業を確認しましょう。	・調理や料理の配膳作業・品出し作業は、食品防御上脆弱な箇所と考えられます。 ・従業員同士の相互監視や、作業動線の工夫、可能な範囲でのカメラ等による確認を行いましょう。	○有り	☆有り 監視の際には濃厚接触にならないよう注意が必要。
37	○納入製品・数量と、発注製品・数量との整合性を確認する。	・数量が一致しない場合は、その原因を確認する。納入数量が増加している場合は特に慎重に確認を行い、通常とは異なるルートとから製品が紛れ込んでいないかに注意を払う。	（28→33 に統合）	（28→33 に統合）	（28→33 に統合）	（28→33 に統合）	（28→33 に統合）	（28→33 に統合）		
38	○保管中の在庫の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、工場長や責任者に報告し、工場長や責任者はその対応を決定する。	・数量が一致しない場合は、その原因を確認する。在庫量が増加している場合は特に慎重に確認し、外部から製品が紛れ込んでいないかに注意を払う。	○（在庫数の増減や汚染行為の徴候への対応） 保管中の在庫の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定しましょう。	・数量が一致しない場合は、その原因を確認しましょう。 ・在庫量が増加している場合は特に慎重に確認し、外部から食材等が紛れ込んでいないかに注意を払いましょう。	○（在庫数の増減や汚染行為の徴候への対応） 保管中の商品の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定しましょう。	・数量が一致しない場合は、その原因を確認しましょう。 ・食材等の在庫量が増加している場合は特に慎重に確認し、外部から食材等が紛れ込んでいないかに注意を払いましょう。	○（保管中の食材や料理数・店頭販売品の増減や汚染行為の徴候への対応） 保管中の食材や料理の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定しましょう。	・保管中の食材や料理・店頭販売品の数量が一致しない場合は、その原因を確認しましょう。 ・食材や食器、料理の保管数量が増加している場合は特に慎重に確認し、外部から食材等が紛れ込んでいないか、慎重に確認しましょう。	○有り	○無し
39	○製品の納入先から、納入量の過不足（紛失や増加）についての連絡があった場合、工場長や責任者に報告し、工場長や責任者はその対応を決定する。	・過不足の原因について、妥当な説明がつくように確認する。特に納入量が増加している場合は慎重に確認し、外部から製品が紛れ込んでいないかに注意を払う。	○（過不足への対応） 製品の納入先から、納入量の過不足（紛失や増加）についての連絡があった場合、工場長や責任者に報告し、工場長や責任者はその対応を決定しましょう。	・過不足の原因について、妥当な説明がつくように確認しましょう。 ・特に納入量が増加している場合は慎重に確認し、外部から製品が紛れ込んでいないかに注意を払いましょう。	○（過不足への対応） 取扱商品の納入先から、納入量の過不足（紛失や増加）についての連絡があった場合、施設責任者に報告し、施設責任者はその対応を決定しましょう。	・過不足の原因について、妥当な説明がつくように確認しましょう。 ・特に納入量が増加している場合は慎重に確認し、外部から商品が紛れ込んでいないかに注意を払いましょう。	○（過不足への対応） お客様から、提供量の過不足（特に増加）についての連絡があった場合、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定しましょう。	・過不足の原因について、妥当な説明がつくように確認しましょう。 ・特に提供量が増加している場合は慎重に確認し、外部から飲食料品が紛れ込んでいないかに注意を払いましょう。	○有り 特に増加していた場合は、感染源となる食品が紛れ込んでいる可能性がある。	○無し
40	○製品納入先の荷受担当者の連絡先を、誰でもすぐに確認できるようにしておく。	・食品工場内で意図的な食品汚染行為等の兆候や形跡が認められた場合は、被害の拡大を防ぐため、至急納入先と情報を共有する必要がある。納入担当者が不在の場合でも、代理の従業員が至急連絡できるように、予め手順・方法を定めておくこと。	○（対応体制・連絡先等の確認） 製品納入先の荷受担当者の連絡先を、誰でもすぐに確認できるようにしておきましょう。	・食品工場内で意図的な食品汚染行為等の兆候や形跡が認められた場合は、被害の拡大を防ぐため、至急納入先と情報を共有しましょう。 ・納入担当者が不在の場合でも、代理の従業員が至急連絡できるように、予め手順・方法を定めておきましょう。	○（対応体制・連絡先等の確認） 取扱商品納入先の荷受担当者の連絡先を、誰でもすぐに確認できるようにしておきましょう。	・物流・保管施設内で意図的な食品汚染行為等の兆候や形跡が認められた場合は、被害の拡大を防ぐため、至急発注元や納入先と情報を共有しましょう。 ・発注・納入担当者が不在の場合でも、代理の従業員が至急連絡できるように、予め手順・方法を定めておきましょう。	○（対応体制・連絡先等の確認） 喫食者に異変が見られた場合の対応体制・連絡先等を、誰でもすぐに確認できるようにしておきましょう。	・調理・提供施設・店舗内で意図的な食品汚染行為等の兆候や形跡が認められた場合は、被害の拡大を防ぐため、至急施設内で情報を共有しましょう。 ・責任者が不在の場合でも、代理の従業員が至急連絡できるように、予め手順・方法を定めておきましょう。	○有り 感染症発生時の連絡にも有用	○無し

2. 可能な範囲での実施が望まれる対策

■人的要素(従業員等)

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
41	○敷地内の従業員等の所在を把握する。	・従業員の敷地内への出入りや所在をリアルタイムでの把握や、記録保存のために、カードキーやカードキーに対応した入退構システム等を導入する。	○（従業員の所在把握） 施設内・敷地内の従業員等の所在を把握しましょう。	・従業員の施設内・敷地内への出入りや所在をリアルタイムでの把握や、記録保存のために、カードキーやカードキーに対応した入退構システム等の導入を検討しましょう。	○（従業員の所在把握） 施設内・敷地内の従業員等の所在を把握しましょう。	・従業員の施設内・敷地内への出入りや所在をリアルタイムでの把握や、記録保存のために、カードキーやカードキーに対応した入退構システム等の導入を検討しましょう。	○（従業員の所在把握） 施設内・敷地内の従業員等の所在を把握しましょう。	・従業員の施設内・敷地内・店舗内への出入りや所在をリアルタイムでの把握や、記録保存のために、カードキーやカードキーに対応した入退構システム等の導入を検討しましょう。	○有り 感染を受けた可能性のある者の把握にも有用	○無し

■施設管理

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
42	○敷地内への侵入防止のため、フェンス等を設ける。	・食品工場の敷地内への出入りしやすい環境が多いため、敷地内への立ち入りを防止することが望ましい。	○（フェンス等の設置） 敷地内への侵入防止のため、フェンス等を設けましましょう。	・食品工場の敷敷地内への出入りしやすい環境が多いため、敷地内への立ち入りを防止するための対策（フェンス等の設置）を検討しましょう。	○（フェンス等の設置） 敷地内への侵入防止のため、フェンス等を設けましょう。	・物流・保管施設の敷地内への出入りしやすい環境が多いため、敷地内への立ち入りを防止するための対策（フェンス等の設置）を検討しましょう。	○（扉の施錠等の設置） 接客（食事提供）施設内での作業空間への侵入防止のため、扉への施錠等を検討しましょう。	・接客（食事提供）施設や店舗の敷地内へは、常に利用客が出入りしています。作業用スペースへのお客様の立ち入りを防止するため、死角となるような個所では、扉の施錠等の対策を検討しましょう ・食材や原材料等が保管されているバックヤードは、無人になることがあるため、確実に施錠しましょう。	○有り 外部者の進入防止に有用	○無し
43	○カメラ等により工場建屋外の監視を行う。	・カメラ等による工場建屋への出入りを監視することによる抑止効果が期待でき、また、有事の際の確認に有用である。	○（監視カメラの設置） カメラ等により工場建屋外の監視を検討しましょう。	・カメラ等による工場建屋への出入りを監視することは、抑止効果が期待できると共に、有事の際の確認に有用です。	○（監視カメラの設置） カメラ等により物流・保管施設建屋外の監視を検討しましょう。	・カメラ等による物流・保管施設建屋への出入りを監視することは、抑止効果が期待できると共に、有事の際の確認に有用です。	○（監視カメラの設置） カメラ等により接客（食事提供）施設建屋内外の監視を検討しましょう。	・カメラ等による接客（食事提供）施設・店舗の建屋内外を監視することは、抑止効果が期待できると共に、有事の際の確認に有用です。	○有り 感染を受けた可能性のある者の確認等に有用	○無し
44	○警備員の巡回やカメラ等により敷地内に保管中／使用中の資材や原材料の継続的な監視、施錠管理等を行う。	・資材・原料保管庫は人が常駐していないことが多く、かつアクセスが容易な場合が多い。可能な範囲で警備員の巡回やカメラ等の設置、施錠確認等を行う。	○（継続的な監視） 警備員の巡回やカメラ等により敷地内に保管中／使用中の資材や原材料の継続的な監視、施錠管理等を行いましょう。	・人が常駐していないことが多く、アクセスが容易な場合が多い資材・原料保管庫は、可能な範囲で警備員の巡回やカメラ等の設置、施錠確認等を行いましょう。	○（継続的な監視） 警備員の巡回やカメラ等により敷地内に保管中の商品の継続的な監視、施錠管理等を行いましょう。	・人が常駐していないことが多く、アクセスが容易な場合が多い取扱商品の保管庫は、可能な範囲で警備員の巡回やカメラ等の設置、施錠確認等を行いましょう。	○（継続的な監視） 警備員の巡回やカメラ等により敷地内に保管中／使用中の食材や食器等の継続的な監視、施錠管理等を行いましょう。	・人が常駐していないことが多く、アクセスが容易な場合が多い食材・店頭販売品の保管庫は、カメラ等の設置、施錠確認等を行いましょう。 ・警備員が配置されている規模の大きな施設で、定期的な巡回経路に組み込みましょう。	○有り 感染を受けた可能性のある者の確認等に有用	○無し

3. 大規模イベント時に必要な対応

大規模イベント時には、ケータリング等、外部の食品工場等で調理された商品が搬入されることがあるため、配送用トラック等でも必要な対策。

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
45	—	—	—	—	○（感染症流行期の対策）	・従業員の健康管理と感染予防	○（感染症流行期の対策）	・従業員の健康管理と感染予防	○有り	○無し

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
					世界的なす感染症の拡大が見られる場合には、運搬中の感染防止のため、国等が推奨する感染予防策を積極的に取り入れましょう。	対策を定め、職場内での感染拡大防止を徹底しましょう。 ・感染症の拡大時期には、国等のガイドラインに従って感染防止対策を講じましょう。 ・搬送用トラックへの同乗時は、マスク直用・会話を控える等の感染予防策を徹底しましょう。	世界的な感染症の拡大が見られる場合には、施設内での感染防止のため、国等が推奨する感染予防策を積極的に取り入れましょう。	対策を定め、職場内での感染拡大防止を徹底しましょう。 ・感染症の拡大時期には、国等のガイドラインに従って感染防止対策を講じましょう。 ・また、利用者にも体調確認を依頼し、体調不良者には、施設の利用を控えて頂きましょう。	感染症対策であるため	
46	—	—	—	—	—	—	○（お客様対策） 不特定多数の利用客が出入りする接客（食事提供）施設では、利用客に交じって意図的に有害物質を混入することも考えられますので対策を行いましょう。	・接客（食事提供）施設・店舗では、不特定多数の人の出入りがあるため、利用客に交じって意図的に有害物質を混入することも考えられます。利用客の行動可能範囲を予め定めておきましょう。 ・入口等に消毒用薬剤を設置する際には、その管理に注意しましょう。	○有り 感染者の入場制限にも有用	☆有り 感染者が正確に申告してくれるのかが課題。 手指消毒薬の食品中への混入や、消毒薬に細菌等が混入される可能性がある。
47	—	—	—	—	—	—	○（客席等の対策） 客席等には、お冷や調味料、食器などは置かないようにしましょう。 また、セルフサービスのサラダバーやドリンクバー等での混入や感染防止対策も必要です。 感染拡大時には、換気や客席の間隔をとる等、動線上の手洗い場を設ける等の有効な対策も検討しましょう。	・客席テーブル上のお冷や調味料、食器等に異物が混入されると可能性も否定できず、また、食器、共有のトング等は、感染拡大の原因にもなります。食品防御及び感染拡大防止の両方の観点から、それらを客席に備え付けることは控え、その都度渡す、封をする等の対策を行いましょう。 ・利用客に交じっての異物混入や、共有のトング等による感染を予防する観点から、ビュッフェ形式は避け、小分けにした状態で個別に提供することを検討しましょう。	○有り 接触感染防止に有用	☆有り スタッフが利用客と接触機会が増えないような対策が必要。
48	—	—	—	—	—	—	○（監視カメラの設置） 利用者が直接、食品に触れる様なカフェテリア形式の配膳場所、サラダバー等や店頭販売品の受渡し場所には、カメラ等による監視を検討しましょう。	・不特定多数のお客様が出入りする飲食店等の配膳場所やサラダバー・ドリンクバー等や店頭販売品の受渡し場所をカメラ等により監視することは、抑止効果が期待できると共に、有事の際の確認に有用です。	○有り 感染者の立入りの有無の確認や。感染を受けた可能性のある者の特定に有用	☆有り 録画画像を確認するための人が必要。
49	—	—	—	—	—	—	○（厨房の防犯・監視体制の強化） 厨房内には、作り置きの料	—	○有り 感染者の立入りの有無の確	○無し

No.	食品防御対策ガイドライン（食品製造工場向け）【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供（店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
							理等が保管される場合があります。保管の際には、冷蔵庫等にカギをかける等の異物混入対策が必要です。		認に有用。	
50			—	—	—	—	○（報道陣対応） 大規模なイベント時には、報道陣に紛れての不審者の侵入にも注意しましょう。	・報道関係者の駐車エリアも設定しておきましょう。 ・報道関係者も施設内に立ち入る際には、適切な許可を受けた者のみにしましょう。	○有り 感染者の立入りの有無の確認に有用。	○無し
51			—	—	—	—	○（関係機関との連携強化） 大規模なイベント時には、多くの関係機関との連携を密にし、迅速な情報の共有化に努めましょう。	・大規模イベント時には、開催主体・食品事業者・保健所等、多くの組織が運営に関与します。どのような組織が関与しているのか十分に把握しておきましょう。 ・事故等発生時、感染者が利用した際の連絡体制及び対応方法を定め、情報の共有と適切・迅速な対応に努めましょう。	○有り 感染拡大の防止にも関係機関等の連携は有用	○無し
52	—	—	—	—	（荷台等への私物の持込み禁止） ・配送用トラック等の車輌の荷台には、私物等は持ち込ませない。また定期的に持ち込んでいないかを確認しましょう。	・荷台への私物の持ち込みは、異物混入のリスクを高めるだけでなく、従業員への疑いも掛かります。	—	—	○有り 私物が感染源となることや感染拡大予防に有用	○無し
53	—	—	—	—	（無関係者の同乗禁止） ・配送用トラック等の車輌には、運転手及び助手以外の配送作業に関係しない人間は同乗させない。	・たとえ同じ会社の同僚・上司であっても配送車輌への同乗は異物混入のリスクを高めます。	—	—	○有り 密な状況での感染拡大防止に有用	○無し
54	—	—	—	—	（荷台ドアの施錠） ・配送用トラック等の荷台ドアに施錠が出来る車輌での配送を行い、荷積み、荷卸し以外は荷台ドアに施錠をしましょう。車輌を離れる際は、荷台ドアの施錠を確認しましょう。	—	—	—	○有り 感染力のある食品の積み込み防止に有用	○無し
55	—	—	—	—	・配送作業が無い場合でたとえ施設内に駐車した配送用トラック等の車輌でも必ず、運転席や荷台ドアの施錠を行いましょう。	・夜間や駐車中の車輌に行われる意図的な行為に対いてのリスクを低減しましょう。 ・閉めると自動で鍵がかかる機能を持つ荷台の扉などを積極的に導入し、駐車時等の盗難防止に努めましょう。	—	—	○有り 感染力のある食品の積み込み防止に有用	○無し

No.	食品防御対策ガイドライン （食品製造工場向け） 【平成 25 年度版】	解説	製造	解説	運搬・保管	解説	調理・提供 （店頭販売品を含む）	解説	感染症対策としての有用性	食品防御対策と感染症対策の並立時の課題
56	―	―	―	―	（GPS 等による位置確認） ・不測の事態が起こった場合などに備え、GPS が搭載された車輌が望ましい。	―	―	―	○有り	○無し

別添１－２

中小規模事業所向け『食品防御対策ガイドライン（案）』

令和５年度版→20250210 確認⇒20250303 修正案→万博を踏まえて再修正予定⇒20260127 班会議版

*店頭販売品の範囲は、営業許可や製造許可を受けた実店舗で調理された料理等を容器に入れ、店舗の敷地内で販売される商品とする。

１．優先的に実施すべき対策

■組織マネジメント

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
1 □	○（危機管理体制の構築） 異常の早期発見するための苦情等集約する仕組みを構築している。 保健所等への相談、社内外への報告、製品の回収、保管、廃棄等の手続き定めている。	○（危機管理体制の構築） 異常の早期発見のための苦情等を集約する仕組みを構築している。 保健所等への相談、社内外への報告、製品の回収、保管、廃棄等の手続きを定めている。	○（危機管理体制の構築） 異常の早期発見のための苦情等を集約する仕組みを構築している。 保健所等への相談、社内外への報告、飲食料品（店頭販売品を含む）の回収、保管、廃棄等の手続きを定めている。
2 □	○（異常発見時の報告） 施設内や敷地内での器物の破損、不用物、異臭等に気が付いた時には、すぐに施設責任者や調理責任者に報告させている。	○（異常発見時の報告） 施設内や敷地内での器物の破損、不用物、異臭等に気が付いた時には、すぐに施設責任者に報告させている。	○（異常発見時の報告） 施設内や敷地内での器物の破損、不用物、異臭等に気が付いた時には、すぐに施設責任者や調理責任者に報告させている。
3 □	○（感染症対策） 従業員の感染症への罹患状況を確認している。 地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の対応策を事前に検討している。	○（感染症対策） 従業員の感染症への罹患状況を確認している。 地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の対応策を事前に検討している。	○（感染症対策） 従業員の感染症への罹患状況を確認している。 地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の対応策を事前に検討している。
4 □	○（職場環境づくり） 従業員等が働きやすい職場環境づくりに努めている。	○（職場環境づくり） 従業員等が働きやすい職場環境づくりに努めている。	○（職場環境づくり） 従業員等が働きやすい職場環境づくりに努めている。
5 □	○（教育） 自社の製品・サービスの品質と安全確保について高い責任感を持ちながら働けように、適切な教育を行っている。	○（教育） 取扱い製品の品質と安全確保について高い責任感を持ちながら働けるように、適切な教育を行っている。	○（教育） 自社の製品・サービスの品質と安全確保について高い責任感を持ちながら働けるように、適切な教育を行っている。
6	○（教育内容）	○（教育内容）	○（教育内容）

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
□	定期的に食品防御に関する教育を行い、その重要性を認識してもらっている。	定期的に食品防御に関する教育を行い、その重要性を認識してもらっている。	定期的に食品防御に関する教育を行い、予防措置に関する内容を含め、その重要性を認識してもらっている。
7 □	○（勤務状況等の把握） 従業員の勤務状況、業務内容、役割分担等を正確に把握している。	○（勤務状況等の把握） 従業員の勤務状況、業務内容、役割分担等を正確に把握している。	○（勤務状況等の把握） 従業員の勤務状況、業務内容、役割分担等を正確に把握している。

■人的要素（従業員等）

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
8 □	○従業員採用時の留意点（身元の確認等） 従業員等の採用面接時には、可能な範囲で身元を確認している。	○従業員採用時の留意点（身元の確認等） 従業員等の採用面接時には、可能な範囲で身元を確認している。	○従業員採用時の留意点（身元の確認等） 従業員等の採用面接時には、可能な範囲で身元を確認している。
9 □	○（従業員の配置） フードディフェンスに関する理解・経験の深い職員を重要箇所に配置している。	○（従業員の配置） フードディフェンスに関する理解・経験の深い職員を重要箇所に配置している。	○　（従業員の配置） フードディフェンスに関する理解・経験の深い職員を重要箇所に配置している。
10 □	○（従業員の健康管理） 日々、従業員の健康管理を適切に行っている。 飛沫や濃厚接触で感染拡大を起こしやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意している。	○（従業員の健康管理） 日々、従業員の健康管理を適切に行っている。 飛沫や濃厚接触で感染拡大を起こしやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意している。	○（従業員の健康管理） 日々、従業員の健康管理を適切に行っている。 飛沫や濃厚接触で感染拡大を起こしやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意している。
11 □	○（制服・名札等の管理） 従業員等の制服や名札、ID バッジ、鍵（キーカード）を適切に管理している。	○（制服・名札等の管理） 従業員等の制服や名札、ID バッジ、鍵（キーカード）を適切に管理している。	○（制服・名札等の管理） 従業員等の制服や名札、ID バッジ、鍵（キーカード）を適切に管理している。
12 □	○（私物の持込みと確認） 私物を製造現場内へは原則として持ち込まないこととし、これが遵守されていることを確認かを定期的に確認している。	○（私物の持込みと確認） 私物を仕分け現場へは原則として持ち込まないこととし、これが遵守されているかを定期的に確認している。	○（私物の持込みと確認） 私物を食材保管庫・厨房・配膳・店頭販売の現場へは原則として持ち込まないこととし、これが遵守されているかを定期的に確認している。
13 □	○（休憩室・トイレ等の 5S の徹底） 休憩室やトイレ等も普段から 5S を心がけている。	○（休憩室・トイレ等の 5S の徹底） 休憩室やトイレ等も普段から 5S を心がけている。	○（休憩室・トイレ等の 5S の徹底） 休憩室やトイレ等も普段から 5S を心がけている。

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
14 □	○（出勤時間・言動の変化等の把握） 従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握している。	○（出勤時間・言動の変化等の把握） 従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握している。	○（出勤時間・言動の変化等の把握） 従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握している。
15 □	○（新規採用者の紹介） 新規採用者は、朝礼等の機会に紹介し、見慣れない人への対応力を高めている。	○（新規採用者の紹介） 新規採用者は、朝礼等の機会に紹介し、見慣れない人への対応力を高めている。	○（従業員の自己紹介） 新たな店舗等がスタートする際には、ミーティング等で自己紹介し、スタッフ同士の認識力を高め、見慣れない人への対応力を高めている。

■人的要素（部外者）

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
16 □	○（訪問者への対応） 1_事前予約がある場合 身元・訪問理由・訪問先（部署・担当者等）を確認し、可能な限り従業員が訪問場所まで同行している。 感染症の流行時は、直接の訪問は極力避ける様にしている。 2_事前予約がない場合や初めての訪問者 原則として事務所等で対応し、工場の製造現場への入構を認めないようにしている。 特に感染症の流行時は、注意している。	○（訪問者への対応） 1_事前予約がある場合 身元・訪問理由・訪問先（部署・担当者等）を確認し、可能な限り従業員が訪問場所まで同行している。 感染症の流行時は、直接の訪問は極力避ける様にしている。 2_事前予約がない場合や初めての訪問者 原則として事務所等で対応し、工場の製造現場への入構を認めないようにしている。 特に感染症の流行時は、注意している。	○（訪問者への対応） 1_事前予約がある場合 身元・訪問理由・訪問先（部署・担当者等）を確認し、可能な限り従業員が訪問場所まで同行している。 感染症の流行時は、直接の訪問は極力避ける様にしている。 2_事前予約がない場合や初めての訪問者 立ち入りを認めないようにしている。 特に感染症の流行時は、注意している。
17 □	○（業者の持ち物確認） 食品工場内を単独で行動する可能性のある訪問者（業者）の持ち物は十分確認し、不要なものを持ち込ませないようにしている。	○（業者の持ち物確認） 物流・保管施設内を単独で行動する可能性のある訪問者（業者）の持ち物は十分確認し、不要なものを持ち込ませないようにしている。	○（業者の持ち物確認） 厨房等施設・設備内を単独で行動する可能性のある訪問者（業者：報道関係・警備関係を含む）の持ち物は十分確認し、不要なものを持ち込ませないようにしている。
18 □	—	—	○（悪意を持った来客対策） 来客の中には悪意を持っている者がいる可能性も考慮している。
19 □	○（郵便・宅配物の受取場所） 郵便、宅配物等の受け入れ先（守衛所、事務所等）を定めている。	○（郵便・宅配物の受取場所） 郵便、宅配物等の受け入れ先（守衛所、事務所等）を定めている。	—

■施設管理

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
20 □	○（調理器具等の定数管理） 使用する原材料や調理器具、洗剤等について、定数・定位置管理を行っている。	○（仕分け用具等の定数管理） 使用する仕分け作業用の器具や工具等について、定数・定位置管理を行っている。	○（調理器具等の定数管理） 使用する原材料や調理器具、洗剤等について、定数・定位置管理を行っている。
21 □	○（脆弱性の高い場所の把握と対策） 食品に直接手を触れることができる仕込みや袋詰めの工程や、従事者が少ない場所等、意図的に有害物質を混入しやすい箇所を把握し、可能な限り手を触れない様にカバーなどの防御対策を検討している。	○（脆弱性の高い場所の把握） 食品に直接手を触れることができる仕分けや袋詰め工程や、従事者が少ない場所等、意図的に有害物質を混入しやすい箇所を把握し、可能な限り手を触れない様にカバーなどの防御対策を検討している。	○（脆弱性の高い場所の把握） 食品に直接手を触れることができる調理や配膳の工程や、従事者が少ない場所等、意図的に有害物質を混入しやすい箇所を把握している。
22 □	○（無人の時間帯の対策） 工場が無人となる時間帯についての防犯対策を講じている。	○（無人の時間帯の対策） 物流・保管施設が無人となる時間帯についての防犯対策を講じている。	○（無人の時間帯の対策） 厨房・食事提供施設・販売店舗が無人となる時間帯（閉店後を含む）についての防犯対策を講じている。
23 □	○（鍵の管理） 鍵の管理方法を策定し、定期的に確認している。	○（鍵の管理） 鍵の管理方法を策定し、定期的に確認している。	○（鍵の管理） 鍵の管理方法を策定し、定期的に確認している。
24 □	○（外部からの侵入防止策） 製造棟、保管庫への外部からの侵入防止対策を行っている。	○（外部からの侵入防止策） 物流・保管施設への外部からの侵入防止対策を行っている。	○（外部からの侵入防止策） 食品保管庫や厨房への外部からの侵入防止対策を行っている。
25 □	○（確実な施錠） 製造棟の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を採っている。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。	○（確実な施錠） 物流・保管施設の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を採っている。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。	○（確実な施錠） 食品保管庫や厨房の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を採っている。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。
26 □	○（試験材料等の管理） 食品工場内の試験材料（検査用試薬・陽性試料等）や有害物質の保管場所を定め、当該場所への人の出入りを管理する。また、使用日時や使用量の記録、施錠管理を行っている。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。	―	○（洗剤等の保管場所） 厨房の洗剤等、有害物質の保管場所を定め、当該場所への人の出入りを管理する。また、使用日時や使用量の記録、施錠管理を行っている。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。
27 □	○（紛失時の対応） 食品工場内の試験材料（検査用試薬・陽性試料等）	―	○（洗剤等の紛失時の対応） 厨房の洗剤等、有害物質を紛失した場合は、施設責

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
	や有害物質を紛失した場合は、工場長や責任者に報告し、工場長や責任者はその対応を決定している。		任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定している。
28 □	○（殺虫剤の管理） 殺虫剤の使用目的や保管場所を定め、施錠による管理を徹底している。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。	○（殺虫剤の管理） 殺虫剤の使用目的や保管場所を定め、施錠による管理を徹底している。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。	○（殺虫剤の管理） 殺虫剤の使用目的や保管場所を定め、施錠による管理を徹底している。 この項目は、コストをかけず対応可能な部分であり、中小規模事業所において徹底を図ること。
29 □	○（給水施設の管理） 井戸、貯水、配水施設への侵入防止措置を講じている。	—	○（給水施設の管理） 井戸、貯水、配水施設への侵入防止措置を講じている。
30 □	○（井戸水の管理） 井戸水に毒物を混入された場合の被害は、工場全体に及ぶため、厳重に管理している。	—	○（井戸水の管理） 井戸水に毒物を混入された場合の被害は、接客（食事提供）施設全体に及ぶため、厳重に管理している。
31 □	○（コンピューターの管理） コンピューター処理制御システムや重要なデータシステムへのアクセス許可者は極力制限し、不正なアクセスを防止している。	○（コンピューターの管理） コンピューター処理制御システムや重要なデータシステムへのアクセス許可者は極力制限し、不正なアクセスを防止している。	◯（顧客情報の管理） 喫食予定のVIPの行動や食事内容に関する情報へのアクセス可能者は、接客の責任者などに限定している。
32 □	○（監視カメラの管理） 監視カメラの映像は外部に流出しないように注意し、特にクラウド型の監視カメラのパスワードは、初期設定のまま使用せず、定期的に変更し、部外者に見られない対策を取っている。	○（監視カメラの管理） 監視カメラの映像は外部に流出しないように注意し、特にクラウド型の監視カメラのパスワードは、初期設定のまま使用せず、定期的に変更し、部外者に見られない対策を取っている。	○（監視カメラの管理） 監視カメラの映像は外部に流出しないように注意し、特にクラウド型の監視カメラのパスワードは、初期設定のまま使用せず、定期的に変更し、部外者に見られない対策を取っている。

■入出荷等の管理

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
33 □	○（ラベル・包装・数量の確認） 資材や原材料等の受け入れ時及び使用前に、ラベルや包装の異常の有無、納入製品・数量と、発注製品・数量との整合性を確認している。 異常を発見した場合は、工場長や責任者に報告し、工場長や責任者はその対応を決定している。	○（ラベル・包装・数量の確認） 取扱商品等の受け入れ時及び仕分け前に、ラベルや包装の異常の有無、納入製品・数量と、発注製品・数量との整合性を確認している。 異常を発見した場合は、施設責任者に報告し、責任者はその対応を決定している。 入荷時には、事前に発送元から通知のあったシリア	○（ラベル・包装・数量の確認） 食材や食器等の受け入れ時及び使用前に、ラベルや包装の異常の有無、納入製品・数量と、発注製品・数量との整合性を確認している。 異常を発見した場合は、料理長や責任者に報告し、料理長や責任者はその対応を決定している。

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
		ルナンバーと製品・数量に間違いがないかを確認している。 出荷時には、シリアルナンバーの付いた封印を行い、製品・数量とともに荷受け側に予め通知している。事前通知には、車両のナンバーやドライバーの名前なども通知している。	
34 □	○（積み下ろしや積み込み作業の監視） 資材や原材料等の納入時の積み下ろし作業や製品の出荷時の積み込み作業を監視している。 中小規模事業所においては、原材料仕入先との信頼関係や、重量での発注に基づく「納入品の外置き」等の習慣が見られるので、これら習慣の撤廃の徹底を図ること。	○（積み下ろしや積み込み作業の監視） 取扱商品等の納入時の積み下ろし作業や出荷時の積み込み作業にも気を配る。 中小規模事業所においては、原材料仕入先との信頼関係や、重量での発注に基づく「納入品の外置き」等の習慣が見られるので、これら習慣の撤廃の徹底を図ること。	○（積み下ろしの監視） 食材や食器等・店頭販売品の納入時の積み下ろし作業は確認している。 中小規模事業所においては、原材料仕入先との信頼関係や、重量での発注に基づく「納入品の外置き」等の習慣が見られるので、これら習慣の撤廃の徹底を図ること。
35 □	―	○（製品等の混在防止対策） ハイセキュリティ製品と一般製品が混ざる事の無いように動線を確保し、物理的に分離して保管している。また監視カメラを設置するなどの対策を行っている。	○（調理や配膳作業の監視） 調理や料理等の配膳時の作業を確認している。
36 □	○（在庫数の増減や汚染行為の徴候への対応） 保管中の在庫の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定している。	○（在庫数の増減や汚染行為の徴候への対応） 保管中の商品の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定している。	○（保管中の食材や料理数・店頭販売品の増減や汚染行為の徴候への対応） 保管中の食材や料理の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定している。
37 □	○（過不足への対応） 製品の納入先から、納入量の過不足（紛失や増加）についての連絡があった場合、工場長や責任者に報告し、工場長や責任者はその対応を決定している。 中小規模事業所においては、原材料仕入先との信頼関係や、重量での発注に基づく「納入品の内容をよく確認しない」等の習慣が見られるので、これら習慣の撤廃の徹底を図ること。	○（過不足への対応） 取扱商品の納入先から、納入量の過不足（紛失や増加）についての連絡があった場合、施設責任者に報告し、施設責任者はその対応を決定している。 中小規模事業所においては、原材料仕入先との信頼関係や、重量での発注に基づく「納入品の内容をよく確認しない」等の習慣が見られるので、これら習慣の撤廃の徹底を図ること。	○（過不足への対応） お客様から、提供量の過不足（特に増加）についての連絡があった場合、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を決定している。 中小規模事業所においては、原材料仕入先との信頼関係や、重量での発注に基づく「納入品の内容をよく確認しない」等の習慣が見られるので、これら習慣の撤廃の徹底を図ること。

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
38 □	○（対応体制・連絡先等の確認） 　製品納入先の荷受担当者の連絡先を、誰でもすぐに確認できるようにしている。	○（対応体制・連絡先等の確認） 　取扱商品納入先の荷受担当者の連絡先を、誰でもすぐに確認できるようにしている。	○（対応体制・連絡先等の確認） 　喫食者や購入者に異変が見られた場合の対応体制・連絡先等を、誰でもすぐに確認できるようにしている。

2. 大規模イベント時に必要な対応

大規模イベント時には、ケータリング等、外部の食品工場等で調理された商品が搬入されることがあるため、配送用トラック等でも必要な対策。

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
39 □	―	○（感染症流行期の対策） 　世界的な感染症の拡大が見られる場合には、運搬中の感染防止のため、国等が推奨する感染予防策を積極的に取り入れている。	○（感染症流行期の対策） 　世界的な感染症の拡大が見られる場合には、施設内での感染防止のため、国等が推奨する感染予防策を積極的に取り入れている。
40 □	―	―	○（お客様対策） 　不特定多数のお客様が出入りする接客（食事提供）施設では、利用客に交じって意図的に有害物質を混入することも考えられるため、対策を検討している。 　店頭販売品においても、販売場所での異物の混入防止に注意する。
41 □	―	―	○（客席等の対策） 　客席等には、お冷や調味料、食器などは置かない。また、セルフサービスのサラダバーやドリンクバー等での混入や感染防止対策も検討している。 　感染拡大時には、換気や客席の間隔をとる等、動線上の手洗い場を設ける等の有効な対策も検討している。
42 □	―	―	○（監視カメラの設置） 　利用者が直接、食品に触れる様なカフェテリア形式の配膳場所、サラダバー、店頭販売品の受け渡し場所等には、カメラ等による監視を検討している。

No.	製造	運搬・保管	調理・提供（店頭販売品を含む）
43 □	—	—	○（厨房の防犯・監視体制の強化） 厨房内には、作り置きの料理や店頭販売品等を保管する場合には、冷蔵庫等にカギをかける等の異物混入対策を行っている。 共有で使用するキッチン等は、使用前後に異常の有無を確認する。
44 □	—	—	○（報道陣対応） 大規模なイベント時には、報道陣に紛れての不審者の侵入にも注意している。
45 □	—	—	○（関係機関との連携強化） 大規模なイベント時には、多くの関係機関との連携を密にし、迅速な情報の共有化に努めている。
46 □	—	○（荷台等への私物の持込み禁止） 配送用トラック等の車輌の荷台には、私物等は持ち込ませない。また、定期的に持ち込んでいないかを確認している。	—
47 □	—	○（無関係者の同乗禁止） 配送用トラック等の車輌には、運転手及び助手以外の配送作業に関係しない人間は同乗させない。	—
48 □	—	○（荷台ドアの施錠） 配送用トラック等の荷台ドアに施錠が出来る車輌での配送を行い、荷積み、荷卸し以外は荷台ドアに施錠し、車輌を離れる際は、荷台ドアの施錠を確認している。 配送作業が無い場合でたとえ施設内に駐車した配送用トラック等の車輌でも必ず、運転席や荷台ドアの施錠を行っている。	—
49 □	—	○（GPS 等による位置確認） 不測の事態が起こった場合などに備え、車輌には GPS を搭載している。	—

別添２－１

食品防御対策ガイドライン
（フードデリバリーサービス提供事業者及び利用事業者向けチェックリスト）
（令和５年度版）→20250205 確認（修正なし）→万博等を踏まえて再修正予定⇒20260127 班会議版

【本チェックリストの対象】

食品の宅配を担当するフードデリバリーサービス提供事業者（以下「デリバリー事業者」という。自社配達、プラットフォーム運営事業者及び個人事業主、タクシー運転手等の兼業者を含む）と、同事業者に食品の宅配を依頼する食品事業者（ファーストフード店・レストラン・食品工場等）において活用されることを念頭に作成したものである。

デリバリー事業者においては食品防御対策ガイドラインの「運搬・保管向け」の内容を、デリバリー事業者を利用する食品事業者においては、「調理・提供施設向け」及び「食品製造工場向け」に記載された内容を参考に、当チェックリストを作成している。

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと
１．優先的に実施すべき対策		
	■組織マネジメント	■組織マネジメント
１ □	○（危機管理体制の構築） ・配達中に、配達員が異物等を混入しない体制を構築している。	○（危機管理体制の構築） ・配達中に従業員が異物等を混入しづらい体制を構築している信頼できる事業者に委託している。 ・配達員から異常等の連絡があった場合、利用客への連絡、保健所等への相談、社内外への報告、飲食料品の回収、保管、廃棄等の手続きを定めている。
２□	○（異常発見時等の報告） ・配達中に商品の破損や異常・異臭等を発見した場合や、苦情等を受けた場合の報告体制を整備し、速やかに委託を受けた運営事業者や食品事業者等の責任者に報告している。	○（異常発見時等の報告） ・配達中に商品の破損や異常・異臭等が発見された場合や、苦情等を受けた場合の報告体制を整備し、速やかに配達員や運営事業者から報告を受けている。
３□	○（感染症対策） ・地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時のBCP 等を事前に検討している。 ・世界的な感染症の拡大が見られる場合には、配達員の感染防止のため、国等が推奨する感染予防策を積極的に取り入れている。	○（感染症対策） ・地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時のBCP 等を事前に検討している。 ・世界的な感染症の拡大が見られる場合には、従業員の感染防止のため、国等が推奨する感染予防策を積極的に取り入れている。
４□	○（職場環境づくり） ・配達員等の安全対策を実施し、働きやすい職場環境づくりに努めている。	○（職場環境づくり） ・委託先及びその配達員との良好な関係を構築し、配達員等が働きやすい職場環境づくりに協力している。
５ □	○（教育） ・配達員等に対して、取扱う商品の品質と安全確保に関して適切な教育を行っている。 ・配達員等に対する教育内容には、万が一、不適切な行動があった場合は、刑事罰だけでなく、賠償責任が発生することも含めている。 ・業務委託契約の場合には、契約事項で食品防御対策	○（教育） ・デリバリー事業者を利用する際に発生する自社の商品・サービスの品質と安全確保、食品防御に関するリスク等について、適切な教育を行っている。 ・従業員に対する教育内容には、万が一、不適切な行動があった場合は、刑事罰だけでなく、賠償責任が発生することも含めている。

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと
	の実施について触れている。業務仲介の場合は、食品防御対策ガイドライン等について情報提供を行っている。	
	■人的要素（従業員・委託契約者等）	■人的要素（従業員等）
6□	○ （配達員登録・契約・採用時の身元の確認等） ・配達員の登録・契約・採用時には、可能な範囲で身元を確認している。 ・運転免許証の原本は、契約時及び定期的に確認している。 ・契約・採用時には、配達員向けチェックリスト等を用いて、食品防御に関する知識の確認や情報提供を行っている。	○ （従業員採用時の身元の確認等） ・従業員等の採用面接時には、可能な範囲で身元を確認している。
7□	○（従業員の配置） ・運営事業者の食品安全等を担当する部署には、可能な限りフードディフェンスに関する理解・経験の深い職員を重要箇所に配置している。	○ （従業員の配置） ・デリバリーに関係する部署にも、可能な限りフードディフェンスに関する理解・経験の深い職員を配置している。
8□	○ （配達員の健康管理） ・日々、配達員の健康状態を適切に確認するよう注意喚起している。 ・飛沫や濃厚接触で感染拡大を起こしやすい感染症に罹患した場合は、速やかに上司等に相談し、取引先・配達先を含む周囲への感染拡大防止や、食品中への混入防止に留意している。	○ （従業員の健康管理） ・日々、従業員の健康状態を適切に確認している。 ・飛沫や濃厚接触で感染拡大を起こしやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意している。
9□	○（用具等の管理） ・配達員等に対して運搬用ボックス等を適切に管理するよう注意喚起している。	○（制服・名札等の管理） ・従業員等の制服や名札、ID バッジ、鍵（キーカード）を適切に管理している。
10□	—	○（私物の持込みと確認） ・私物を食材保管庫・厨房・商品受け渡し口等の現場へは原則として持ち込まないこととし、これが遵守されているかを定期的に確認している。
11□	—	○（休憩室・トイレ等の 5S の徹底） ・休憩室やトイレ等も普段から 5S を心がけている。
12□	○（配達員の勤務状況・稼働時間・配達範囲の変化等の把握） ・契約状況に応じて、配達員等の稼働時間や配達範囲を把握し、著しい変化や、従来とは異なる稼働時間や配達範囲・稼働頻度の変化等に注意を払っている。	○（勤務状況・出勤時間・言動の変化等の把握） ・従業員の勤務状況、業務内容、役割分担等を正確に把握している。 ・従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握している。
13□	—	○（移動可能範囲の明確化） ・規模の大きな施設では、就業中の全従業員等の移動可能範囲を明確化にし、認められた範囲内で働かせている。

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと
１４ □	○（新規採用者・契約者の紹介） ・新たに採用・契約した配達員は、依頼元事業者等に適切に紹介し、成りすましを防ぐ工夫を行っている。	
	■人的要素（部外者）	■人的要素（部外者）
１５ □	○（依頼元での対応） ・配達員には、正規の契約であることを証明するために、依頼元事業者に対して注文番号等の電子記録を提示させている。 ・感染症の流行時は、依頼元の店舗等の商品の受渡しの際には、配達員と受渡し担当者との接触を極力避ける工夫を行うよう、利用事業者にも注意喚起している。	○（配達員への対応） ・注文番号が確認できない配達員には配達を依頼しない。 ・感染症の流行時は、感染防止策を取った上で商品の受渡しを行っている。
１６ □	○（駐車エリアの設定や駐車許可証の発行） ・配達用車両は、指定された場所に駐車・駐輪している。駐車・駐輪許可証が発行されている場合は、適切に使用するように注意喚起している。	○（駐車エリアの設定や駐車許可証の発行） ・規模の大きな施設では、配達用車両の駐車・駐輪場の設定や、駐車・駐輪許可証の発行等、無許可での敷地内への進入や駐車・駐輪を防止している。
１７ □	○（商品の受渡しと配達員の持ち物確認） ・商品の受取りは、定められた受渡し窓口で行い、不用意に厨房内へは立入らないように注意喚起している。 ・配達用車両の荷台や配達用バック内に、不要な私物等を一緒に収納しないよう、注意喚起している。	○（商品の受渡しと配達員の持ち物確認） ・商品の受渡しは、定められた受渡し窓口で行い、配達員が厨房等施設・設備内への立入らなくてもよいようにしている。 ・配達用車両の荷台や配達用バック内に、不要な私物等を一緒に収納しないように、注意喚起している。
１８ □	○（悪意を持った配達員対策） ・配達員の中には悪意を持っている者がいる可能性も考慮している。	○（悪意を持った配達員対策） ・配達員の中には悪意を持っている者がいる可能性も考慮している。
	■施設管理	■施設管理
１９ □	○（配達用の用具等の定数管理） ・配達に使用する用具（配達用バック等）等について、定期的に定数管理を行うよう注意喚起している。	○（宅配用資材等の定数管理） ・宅配に使用する容器・包装材料等について、定期的に定数管理を行っている。
２０ □	○（脆弱性の高い配達中の対策） ・意図的に有害物質を混入しやすい環境が出現した場合に備えて、商品にカバーや封印を行う等の防御対策を行うよう、利用事業者に対して注意喚起している。	○（脆弱性の高い配達中の対策） ・意図的に有害物質を混入しやすい環境が出現した場合に備えて、商品にカバーや封印を行い、混入されにくい、混入に気づきやすい対策を取っている。
２１ □	○（車両を離れる際の対策） ・荷台に施錠が出来る配達用車両での配達を行い、走行中や配達で車両を離れる際には、荷台の施錠を確認し、自転車やバイクの場合には、配達用バックを持ち歩くように注意喚起している。 ・たとえ施設内に駐車した配達用車両でも、必ず運転席や荷台の施錠を行うよう注意喚起している。	○（無人の時間帯の対策） ・施設が無人となる時間帯（閉店後を含む）について防犯対策を講じている。
２２ □	―	○（鍵の管理） ・鍵の管理方法を策定し、定期的に確認している。

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと
		・配達員には鍵へのアクセス権を設定しない。
２３ □	―	○（外部からの侵入防止策） ・食品保管庫・厨房への外部からの侵入防止対策を行っている。
２４ □	―	○（確実な施錠） ・施設全体、食品保管庫や厨房の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を取っている。
２５ □	○（顧客情報の管理） ・顧客情報（取引業者・利用客）等の重要なデータシステムへのアクセス許可者は極力制限し、不正なアクセスを防止している。	○（顧客情報の管理） ・顧客情報（取引業者・利用客等）の重要なデータシステムへのアクセス可能者は、接客の責任者などに限定している。
２６ □	―	○（監視カメラの管理） ・監視カメラの映像は外部に流出しないように注意し、特にクラウド型の監視カメラのパスワードは、初期設定のまま使用せず、定期的に変更している。
	■入出荷等の管理	■入出荷等の管理
２７ □	○（ラベル・包装・数量の確認） ・商品等の受取り時に、ラベルや包装の異常の有無、注文番号、発注商品と数量の整合性を確認し、異常があれば施設責任者に連絡している。 ・異常を発見した場合は、施設責任者に報告し、施設責任者はその対応を予め決めている。	○（ラベル・包装・数量の確認） ・商品等の受渡し時に、ラベルや包装の異常の有無、注文番号、発注商品と数量の整合性を確認し、異常があれば施設責任者に連絡している。 ・異常を発見した場合は、店長や責任者に報告し、店長や責任者はその対応を予め決めている。
２８ □	○（配達中の商品の増減や汚染行為の徴候への対応） ・配達中に商品の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者に報告し、施設責任者はその対応を予め決めている。	○（配達中の商品の増減や汚染行為の徴候への対応） ・配達中に商品の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を予め決めている。
２９ □	○（対応体制・連絡先等の確認） ・配達した商品の依頼元や配達先の連絡先を、すぐに確認できるようにしている。	○（対応体制・連絡先等の確認） ・配達した商品により喫食者に異変が見られた場合の対応体制・連絡先等を、誰でもすぐに確認できるようにしている。
２．可能な範囲での実施が望まれる対策		
３０ □	○（ドライブレコーダー・GPS 等の活用） ・不測の事態が起こった場合などに備えドライブレコーダーや GPS 等により配達中の位置の確認や記録を検討している。	○（ドライブレコーダー等・GPS の活用） ・不測の事態が起こった場合などに備え、ドライブレコーダーや GPS 等を活用し、配達中の安全性の確保が可能な事業者を選定し委託している。

別添２－２

食品防御対策ガイドライン
（フードデリバリーサービス配達員向けチェックリスト）

（令和 5 年度版）→20250125 確認（修正なし）→万博等を踏まえて再修正予定⇒20260127 班会議版

【本チェックリストの対象】

食品の配達を担当するフードデリバリーサービス提供事業者（以下「デリバリー事業者」という。自社配達、フードデリバリー・デジタル・プラットフォーム運営事業者及び個人事業主、タクシー運転手等の兼業者を含む）において、配達員が日々の配達において活用されることを念頭に作成したものである。

事業者においては、食品防御対策ガイドライン（フードデリバリーサービス提供事業者及び利用事業者向けチェックリスト（案））と併せて使用されることを想定している。

No.	内容	デリバリー向けチェックリスト対応項目
１ □	○（新規登録・契約・採用時の身元の確認等） ・配達員として新たに登録・契約・採用される際には、事業者の求めに応じて運転免許証の原本等、身元を証明する書類を提示している。 ・運転免許証の原本は、事業者の求めに応じて定期的に提示している。	６、１４
２□	○（契約者の確認） ・配達員として契約された場合には、成りすまし等を防ぐために、依頼元事業者等に適切に発注時の注文番号等で確認してもらっている。	１４
３□	○（食品防御に関する知識と認識） ・配達員として事業者に登録する際には、事業者が推奨する、取扱う商品の品質と安全確保、食品防御に関する適切な知識を持っている。 ・不適切な行動があった場合、刑事罰や賠償責任等が発生することを正しく認識している。 ・登録・契約・採用時には、本チェックリスト等を用いて、食品防御に関する知識を確認している。	５
４□	○（健康管理） ・日々、健康状態を適切に確認し、体調不良があった場合は、速やかに契約先・取引先等に相談している。	８
	○（感染症対策） ・地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、国等が推奨する感染予防策を適切に実践している。 ・感染の恐れがある場合は、速やかに契約先・取引先等に相談している。	３
５ □	○（用具等の管理） ・配達員等は、注文番号、運搬用ボックスを適切に管理し、自分以外の者には貸与しない。	９、１９
６□	○（商品の受渡し） ・商品の受取りは、定められた受渡し窓口で行い、不用意に厨房内へは立入らないようにしている。 ・商品等の受取り時に、ラベルや包装の異常の有無、発注商品と数量の整合性を確認し、記録に残している。	１７、２６
７□	○（配達中の対策） ・配達中に、第三者が意図的に有害物質を食品へ混入することがないよう、商品にカバーや封印等が施されていることを確認している。	２０

No.	内容	デリバリー向けチェックリスト対応項目
８□	○（異常発見時等の報告） ・配達中に商品の破損や異常・異臭等を発見、または苦情等を受けた場合は、速やかに委託を受けた運営事業者や食品事業者等の責任者に報告している。	２、２７、２８
９ □	○（配達員の私物等） ・配達中は不要な私物は携行せず、また、配達用車両の荷台や配達用バック内では、私物と食品（商品）との接触を避ける様にしている。	１７
１０ □	○（駐車・駐輪） ・配達用車両は、指定された場所に駐車・駐輪している。駐車・駐輪許可証が発行されている場合は、適切に使用している。	１６
１１ □	○（車両を離れる際の対策） ・荷台に施錠が出来る配達用車両での配達を行い、走行中や配達で車両を離れる際には、荷台の施錠を確認している。 ・自転車やバイクで配達する場合は、配達用バックを自転車等に置いたままにしない。 ・自動車で配達する場合は、車両の施錠を確実に実施する。 ・不測の事態が起こった場合等に備え、ドライブレコーダーや GPS 等を活用している。	２１、２９
１２ □	○（顧客情報の管理） ・プラットフォーム運営事業者が保管する重要な顧客情報（取引業者・利用客）等のデータシステムには、不正・にアクセスしないようにしている。	２５

＼食品防御対策／

フードデリバリーサービス配達員向け チェックリスト

CHECK

1 ☐
- 配達員として新たに登録・契約・採用される際には、事業者の求めに応じて運転免許証の原本等、身元を証明する書類を提示している。
- 運転免許証の原本は、事業者の求めに応じて定期的に提示している。

2 ☐
- 配達員として契約された場合には、成りすまし等を防ぐために、依頼元事業者等に適切に発注時の注文番号等で確認してもらっている。

3 ☐
- 配達員として事業者に登録する際には、事業者が推奨する、取扱う商品の品質と安全確保、食品防御に関する適切な知識を持っている。
- 不適切な行動があった場合、刑事罰や賠償責任等が発生することを正しく認識している。
- 登録・契約・採用時には、本チェックリスト等を用いて、食品防御に関する知識を確認している。

4 ☐
- 日々、健康状態を適切に確認し、体調不良があった場合は、速やかに契約先・取引先等に相談している。
- 地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、国等が推奨する感染予防策を適切に実践している。
- 感染の恐れがある場合は、速やかに契約先・取引先等に相談している。

5 ☐
- 配達員等は、注文番号、運搬用ボックスを適切に管理し、自分以外の者には貸与しない。

6 ☐
- 商品の受取りは、定められた受渡し窓口で行い、不用意に厨房内へは立入らないようにしている。
- 商品等の受取り時に、ラベルや包装の異常の有無、発注商品と数量の整合性を確認し、記録に残している。

7 ☐
- 配達中に、第三者が意図的に有害物質を食品へ混入することがないよう、商品にカバーや封印等が施されていることを確認している。

8 ☐
- 配達中に商品の破損や異常・異臭等を発見、または苦情等を受けた場合は、速やかに委託を受けた運営事業者や食品事業者等の責任者に報告している。

9 ☐
- 配達中は不要な私物は携行せず、また、配達用車両の荷台や配達用バック内では、私物と食品（商品）との接触を避ける様にしている。

10 ☐
- 配達用車両は、指定された場所に駐車・駐輪している。駐車・駐輪許可証が発行されている場合は、適切に使用している。

11 ☐
- 荷台に施錠が出来る配達用車両での配達を行い、走行中や配達で車両を離れる際には、荷台の施錠を確認している。
- 自転車やバイクで配達する場合は、配達用バックを自転車等に置いたままにしない。
- 自動車で配達する場合は、車両の施錠を確実に実施する。
- 不測の事態が起こった場合等に備え、ドライブレコーダーやGPS等を活用している。

12 ☐
- プラットフォーム運営事業者が保管する重要な顧客情報（取引業者・利用客）等のデータシステムには、不正にアクセスしないようにしている。

MEMO

本チェックリストの対象

食品の配達を担当するフードデリバリーサービス提供事業者（以下「デリバリー事業者」という。自社配達、フードデリバリー・デジタル・プラットフォーム運営事業者及び個人事業主、タクシー運転手等の兼業者を含む）の配達員の方々が、日々の配達において活用されることを念頭に作成したものです。
事業者においては、食品防御対策ガイドライン（フードデリバリーサービス提供事業者及び利用事業者向けチェックリスト）と併せて使用されることを想定しています。

別添２－３

食品防御対策ガイドライン
（フードデリバリーサービス提供事業者及び利用事業者向けチェックリスト）
（令和５年度版）→20250210 確認（修正なし）英訳対比表（案）→万博等を踏まえて再修正後作成予定⇒20260127 班会議版

【本チェックリストの対象】
食品の宅配を担当するフードデリバリーサービス提供事業者（以下「デリバリー事業者」という。自社配達、プラットフォーム運営事業者及び個人事業主、タクシー運転手等の兼業者を含む）と、同事業者に食品の宅配を依頼する食品事業者（ファーストフード店・レストラン・食品工場等）において活用されることを念頭に作成したものである。
デリバリー事業者においては食品防御対策ガイドラインの「運搬・保管向け」の内容を、デリバリー事業者を利用する食品事業者においては、「調理・提供施設向け」及び「食品製造工場向け」に記載された内容を参考に、当チェックリストを作成している。

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	Food Defense Measures Guidelines: Checklist for Food Delivery Services (For food delivery service providers responsible for home delivery)	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと	Food Defense Measures Guidelines - Checklist for Food Delivery Services (For businesses using food delivery service providers: cooking and serving facilities and food manufacturing plants) For details, refer to the Food Defense Measures Guideline
	１．優先的に実施すべき対策	1. Measures to be Implemented as a Priority	１．優先的に実施すべき対策	1. Measures to be Implemented as a Priority
	■組織マネジメント	Organizational Management	■組織マネジメント	Organizational Management
1 □	○（危機管理体制の構築） ・配達中に、配達員が異物等を混入しない体制を構築している。	(Establishment of Crisis Management System) ● A system has been established to ensure that delivery personnel do not mix foreign objects, etc., during delivery.	○（危機管理体制の構築） ・配達中に従業員が異物等を混入しづらい体制を構築している信頼できる事業者に委託している。 ・配達員から異常等の連絡があった場合、利用客への連絡、保健所等への相談、社内外への報告、飲食料品の回収、保管、廃棄等の手続きを定めている。	(Establishment of a Crisis Management System) ● When outsourcing delivery services, select reliable providers that have established systems to prevent employees from contaminating products during delivery. ● Establishing procedures for notifying customers, consulting with public health authorities, reporting internally and externally, and retrieving, storing, and disposing of food and beverages in the event that delivery personnel report any irregularities.”
2□	○（異常発見時等の報告） ・配達中に商品の破損や異常・異臭等を発見した場合や、苦情等を受けた場合の報告体制を整備し、速やかに委託を受けた運営事業者や食品事業者等の責任者に報告している。	(Reporting in Case of Abnormalities, etc.) ● A reporting system has been established to ensure that any damage, abnormalities, or unusual odors found in products during delivery, as well as any complaints received, are promptly reported to the responsible parties of the contracted operating company or food business operator.	○（異常発見時等の報告） ・配達中に商品の破損や異常・異臭等が発見された場合や、苦情等を受けた場合の報告体制を整備し、速やかに配達員や運営事業者から報告を受けている。	(Reporting in Case of Abnormalities, etc.) ● A reporting system has been established to ensure that any damage, abnormalities, or unusual odors found in products during delivery, as well as any complaints received, are promptly reported to the responsible parties of the contracted operating company or food business operator.
3□	○（感染症対策） ・地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の BCP 等を事前に検討している。 ・世界的な感染症の拡大が見られる場合には、配達員の感染防止のため、国等が推奨する感染予防策を積極的に取り入れている。	(Infection Control Measures) ● We consistently pay attention to local infection information and global infectious disease outbreaks, and we proactively consider BCP (Business Continuity Plans) in the event of an infection spread. ● In the case of a global infectious disease outbreak, we actively adopt infection prevention measures recommended by the government and other authorities to protect delivery personnel from infection.	○（感染症対策） ・地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、感染拡大時の BCP 等を事前に検討している。 ・世界的な感染症の拡大が見られる場合には、従業員の感染防止のため、国等が推奨する感染予防策を積極的に取り入れている。	(Infection Control Measures) ● We consistently pay attention to local infection information and global infectious disease outbreaks, and we proactively consider BCP (Business Continuity Plans) in the event of an infection spread. ● In the case of a global infectious disease outbreak, we actively adopt infection prevention measures recommended by the government and other authorities to protect delivery personnel from infection.
4□	○（職場環境づくり） ・配達員等の安全対策を実施し、働きやすい職場環境づくりに努めている。	(Creating a Positive Work Environment) ● We implement safety measures for delivery personnel and strive to create a comfortable and conducive work environment.	○（職場環境づくり） ・委託先及びその配達員との良好な関係を構築し、配達員等が働きやすい職場環境づくりに協力している。	(Creating a Positive Work Environment) ● Building good relationships with subcontractors and their delivery personnel, and cooperating to create a work environment where delivery personnel can work

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	Food Defense Measures Guidelines: Checklist for Food Delivery Services (For food delivery service providers responsible for home delivery)	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと	Food Defense Measures Guidelines - Checklist for Food Delivery Services (For businesses using food delivery service providers: cooking and serving facilities and food manufacturing plants) For details, refer to the Food Defense Measures Guideline
				comfortably.
5 □	○（教育） ・配達員等に対して、取扱う商品の品質と安全確保に関して適切な教育を行っている。 ・配達員等に対する教育内容には、万が一、不適切な行動があった場合は、刑事罰だけでなく、賠償責任が発生することも含めている。 ・業務委託契約の場合には、契約事項で食品防御対策の実施について触れている。業務仲介の場合は、食品防御対策ガイドライン等について情報提供を行っている。	(Education) ● We provide appropriate education to delivery personnel regarding the quality and safety assurance of the products they handle. ● The education for delivery personnel includes information on the potential for criminal penalties and liability for damages in the event of inappropriate behavior. ● In the case of business outsourcing contracts, the contract terms address the implementation of food defense measures. For business intermediaries, we provide information on food defense measures guidelines and other relevant materials.	○（教育） ・デリバリー事業者を利用する際に発生する自社の商品・サービスの品質と安全確保、食品防御に関するリスク等について、適切な教育を行っている。 ・従業員に対する教育内容には、万が一、不適切な行動があった場合は、刑事罰だけでなく、賠償責任が発生することも含めている。	(Education) ● We provide appropriate education on the risks related to ensuring the quality and safety of the company's products and services, as well as food defense, when using delivery service providers. ● The education for employees includes information on the potential for criminal penalties and liability for damages in the event of inappropriate behavior.
	■人的要素（従業員・委託契約者等）	**Human Factors (Employees and Contractors, etc.)**	■人的要素（従業員等）	**Human Factors (Employees, etc.)**
6 □	○ （配達員登録・契約・採用時の身元の確認等） ・配達員の登録・契約・採用時には、可能な範囲で身元を確認している。 ・運転免許証の原本は、契約時及び定期的に確認している。 ・契約・採用時には、配達員向けチェックリスト等を用いて、食品防御に関する知識の確認や情報提供を行っている。	(Verification of Identity During Registration, Contracting, and Hiring of Delivery Personnel) ● We verify the identity of delivery personnel to the extent possible during registration, contracting, and hiring as possible. ● The original driver's license is checked at the time of contracting and periodically thereafter. ● During contracting and hiring, we use checklists for delivery personnel to confirm their knowledge of food defense and provide relevant information.	○ （従業員採用時の身元の確認等） ・従業員等の採用面接時には、可能な範囲で身元を確認している。	(Verification of Identity During Employee Recruitment) ● We verify the identity of delivery personnel to the extent possible during employee recruitment interviews as much as possible.
7 □	○（従業員の配置） ・運営事業者の食品安全等を担当する部署には、可能な限り食品防御に関する理解・経験の深い職員を重要箇所に配置している。	(Employee Placement) ● In the departments responsible for food safety and related areas within the operating company, we place personnel with a deep understanding and experience in food defense in key positions whenever possible.	○ （従業員の配置） ・デリバリーに関係する部署にも、可能な限り食品防御に関する理解・経験の深い職員を配置している。	(Employee Placement) ● In the departments related to delivery, we place personnel with a deep understanding and experience in food defense in key positions whenever possible.
8 □	○ （配達員の健康管理） ・配達員に対して、日々の健康状態を適切に確認するよう定期的に注意喚起している。 ・飛沫や濃厚接触で感染拡大を起こしやすい感染症に罹患した場合は、速やかに上司等に相談し、取引先・配達先を含む周囲への感染拡大防止や、食品中への混入防止に留意している。	(Health Management of Delivery Personnel) ● We regularly remind delivery personnel to appropriately monitor their health condition daily. ● If they contract an infectious disease that can easily spread through droplets or close contact, they are advised to promptly consult with their supervisor and take measures to prevent the spread of infection to clients, delivery destinations, and to prevent contamination of food.	○ （従業員の健康管理） ・従業員に対して、日々の健康状態を適切に確認している。 ・飛沫や濃厚接触で感染拡大を起こしやすい感染症に罹患した場合は、速やかに上司等に相談し、周囲への感染拡大防止や、食品中への混入防止に留意している。	(Employee Health Management) ● We regularly remind employees to appropriately monitor their health condition daily. ● If they contract an infectious disease that can easily spread through droplets or close contact, they are advised to promptly consult with their supervisor and take measures to prevent the spread of infection to others and contamination of food.
9 □	○（用具等の管理） ・配達員等に対して運搬用ボックス等を適切に管理するよう注意喚起している。	(Management of Equipment, etc.) ● Delivery personnel are regularly reminded to properly manage transportation boxes and other equipment.	○（制服・名札等の管理） ・従業員等の制服や名札、ID バッジ、鍵（キーカード）を適切に管理している。	(Management of Uniforms and Name Tags) ● Properly managing employees' uniforms, name tags, ID badges, and keys (key cards).

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	Food Defense Measures Guidelines: Checklist for Food Delivery Services (For food delivery service providers responsible for home delivery)	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと	Food Defense Measures Guidelines - Checklist for Food Delivery Services (For businesses using food delivery service providers: cooking and serving facilities and food manufacturing plants) For details, refer to the Food Defense Measures Guideline
１０ □	―		○（私物の持込みと確認） ・私物を食材保管庫・厨房・商品受け渡し口等の現場へは原則として持ち込まないこととし、これが遵守されているかを定期的に確認している。	(Bringing and Checking Personal Belongings) ● As a general rule, personal belongings are not to be brought into food storage areas, kitchens, or product handover points, and compliance with this rule is regularly checked.
１１ □	―		○（休憩室・トイレ等の 5S の徹底） ・休憩室やトイレ等も普段から 5S を心がけている。	(Ensuring 5S in Stuff Lounges Break Rooms and Toilets) ● Always practicing the 5S principles in stuff lounges break rooms and toilets.
１２ □	○（配達員の勤務状況・稼働時間・配達範囲の変化等の把握） ・契約状況に応じて、配達員等の稼働時間や配達範囲を把握し、著しい変化や、従来とは異なる稼働時間や配達範囲・稼働頻度の変化等に注意を払っている。	(Monitoring of Delivery Personnel's Work Conditions, Working Hours, and Delivery Area Changes) ● Depending on the contract situation, we monitor the working hours and delivery areas of delivery personnel, paying attention to significant changes, as well as any deviations from usual working hours, delivery areas, or frequency of operations.	○（勤務状況・出勤時間・言動の変化等の把握） ・従業員の勤務状況、業務内容、役割分担等を正確に把握している。 ・従業員等の出退勤時間を把握し、著しい変化や、従来とは異なる言動の変化等を把握している。	(Monitoring Work Conditions, Attendance, and Behavioral Changes) ● Accurately tracking employees' work conditions, job content, and role assignments. ● Monitoring employees' attendance times and noting any significant changes or deviations in behavior from the norm.
１３ □	―		○（移動可能範囲の明確化） ・規模の大きな施設では、就業中の全従業員等の移動可能範囲を明確化にし、認められた範囲内で働かせている。	(Clarification of Permissible Movement Areas) ● In large facilities, clearly defining the permissible movement areas for all employees during working hours and ensuring they work within the approved areas.
１４ □	○（新規採用者・契約者の紹介） ・新たに採用・契約した配達員は、依頼元事業者等に適切に紹介し、成りすましを防ぐ工夫を行っている。	(Introduction of New Hires and Contractors) ● Newly hired or contracted delivery personnel are appropriately introduced to the client companies to prevent impersonation.		
	■人的要素（部外者）	**Human Factors (Outsiders)**	■人的要素（部外者）	**■ Human Factors (Outsiders)**
１５ □	○（依頼元での対応） ・配達員には、正規の契約であることを証明するために、依頼元事業者に対して注文番号等の電子記録を提示させている。 ・感染症の流行時は、依頼元の店舗等の商品の受渡しの際には、配達員と受渡し担当者との接触を極力避ける工夫を行うよう、利用事業者にも注意喚起している。	(Response at the Client's End) ● Delivery personnel are required to present electronic records such as order numbers to the client companies to prove that they are under a legitimate contract. ● During infectious disease outbreaks, client companies are reminded to take measures to minimize contact between delivery personnel and the staff responsible for handing over the products.	○（配達員への対応） ・注文番号が確認できない配達員には配達を依頼しない。 ・感染症の流行時は、感染防止策を取った上で商品の受渡しを行っている。	(Handling Delivery Personnel) ● We do not request deliveries from delivery personnel who cannot confirm the order number. ● During infectious disease outbreaks, ensure that products are handed over while taking infection prevention measures.
１６ □	○（駐車エリアの設定や駐車許可証の発行） ・配達用車両は、指定された場所に駐車・駐輪している。駐車・駐輪許可証が発行されている場合は、適切に使用するように注意喚起している。	(Setting Parking Areas and Issuing Parking Permits) ● Delivery vehicles are parked or stationed in designated areas. ● When parking or bicycle parking permits are issued, delivery personnel are reminded to use them appropriately.	○（駐車エリアの設定や駐車許可証の発行） ・規模の大きな施設では、配達用車両の駐車・駐輪場の設定や、駐車・駐輪許可証の発行等、無許可での敷地内への進入や駐車・駐輪を防止している。	(Setting Parking Areas and Issuing Parking Permits) ● In large facilities, setting up parking and bicycle parking areas for delivery vehicles and issuing parking/bicycle parking permits to prevent unauthorized entry and parking within the premises.

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	Food Defense Measures Guidelines: Checklist for Food Delivery Services (For food delivery service providers responsible for home delivery)	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと	Food Defense Measures Guidelines - Checklist for Food Delivery Services (For businesses using food delivery service providers: cooking and serving facilities and food manufacturing plants) For details, refer to the Food Defense Measures Guideline
１７ □	○（商品の受渡しと配達員の持ち物確認） ・商品の受取りは、定められた受渡し窓口で行い、不用意に厨房内へは立入らないように注意喚起している。 ・配達用車両の荷台や配達用バック内に、不要な私物等を一緒に収納しないよう、注意喚起している。	(Product Handover and Checking Delivery Personnel's Belongings) ● Products are received at the designated handover window, and delivery personnel are reminded not to enter the kitchen area unnecessarily. ● Delivery personnel are reminded not to store unnecessary personal items together with the products in the delivery vehicle's cargo area or delivery bags.	○（商品の受渡しと配達員の持ち物確認） ・商品の受渡しは、定められた受渡し窓口で行い、配達員が厨房等施設・設備内への立入らなくてもよいようにしている。 ・配達用車両の荷台や配達用バック内に、不要な私物等を一緒に収納しないように、注意喚起している。	(Product Handover and Checking Delivery Personnel's Belongings) ● Conducting product handovers at designated handover points to ensure delivery personnel do not need to enter kitchens or other facility areas. ● Advising delivery personnel not to store unnecessary personal items together with delivery items in the vehicle's cargo area or delivery bags.
１８ □	○（悪意を持った配達員対策） ・配達員の中には悪意を持っている者がいる可能性も考慮している。	(Measures Against Malicious Delivery Personnel) ● We consider the possibility that some delivery personnel may have malicious intent.	○（悪意を持った配達員対策） ・配達員の中には悪意を持っている者がいる可能性も考慮している。	(Measures Against Malicious Delivery Personnel) ● We consider the possibility that some delivery personnel may have malicious intent
	■施設管理	**Facility Management**	■施設管理	**■ Facility Management**
１９ □	○（配達用の用具等の定数管理） ・配達に使用する用具（配達用バック等）等について、定期的に定数管理を行うよう注意喚起している。	(Inventory Management of Delivery Equipment) ● Delivery personnel are regularly reminded to conduct periodic inventory management of the equipment used for deliveries (such as delivery bags).	○（宅配用資材等の定数管理） ・宅配に使用する容器・包装材料等について、定期的に定数管理を行っている。	**(Inventory Management of Delivery Materials)** ● Regularly conducting inventory management of containers and packaging materials used for delivery.
２０ □	○（脆弱性の高い配達中の対策） ・意図的に有害物質を混入しやすい環境が出現した場合に備えて、商品にカバーや封印を行う等の防御対策を行うよう、利用事業者に対して注意喚起している。	(Measures for High-Risk Deliveries) ● Client companies are reminded to implement protective measures, such as covering or sealing products, to prepare for environments where harmful substances could be intentionally introduced.	○（脆弱性の高い配達中の対策） ・意図的に有害物質を混入しやすい環境が出現した場合に備えて、商品にカバーや封印を行い、混入されにくい、混入に気づきやすい対策を取っている。	(Measures for High-Risk Deliveries) ● Taking precautions such as covering or sealing products to prevent and detect the intentional contamination of harmful substances in environments where such risks may arise.
２１ □	○（車両を離れる際の対策） ・荷台に施錠が出来る配達用車両での配達を行い、走行中や配達で車両を離れる際には、荷台の施錠を確認し、自転車やバイクの場合には、配達用バックを持ち歩くように注意喚起している。 ・たとえ施設内に駐車した配達用車両でも、必ず運転席や荷台の施錠を行うよう注意喚起している。	(Measures When Leaving the Vehicle) ● Delivery personnel are reminded to use delivery vehicles with lockable cargo areas and to ensure the cargo area is locked when driving or leaving the vehicle. In the case of bicycles or motorcycles, they are reminded to carry the delivery bag with them. ● Even when the delivery vehicle is parked within a facility, delivery personnel are reminded to always lock the driver's seat and cargo area.	○（無人の時間帯の対策） ・施設が無人となる時間帯（閉店後を含む）について防犯対策を講じている。	(Measures for Unattended Hours) ● Implementing security measures for times when the facility is unattended, including after closing hours.
２２ □	—		○（鍵の管理） ・鍵の管理方法を策定し、定期的に確認している。 ・配達員には鍵へのアクセス権を設定しない。	(Key Management) ● Establishing and regularly reviewing key management procedures. ● Not granting delivery personnel access to keys.
２３ □	—		○（外部からの侵入防止策） ・食品保管庫・厨房への外部からの侵入防止対策を行っている。	(Measures to Prevent External Intrusion) ● Implementing measures to prevent external intrusion into food storage areas and kitchens.
２４ □	—		○（確実な施錠） ・施設全体、食品保管庫や厨房の出入り口や窓など外部から侵入可能な場所を特定し、確実に施錠する等の対策を	(Ensuring Secure Locking) ● Measures are taken to identify and securely lock all potential entry points from the outside, including the entire facility,

No.	宅配を担当するフードデリバリー事業者向け （運搬・保管）	Food Defense Measures Guidelines: Checklist for Food Delivery Services (For food delivery service providers responsible for home delivery)	フードデリバリー事業者を利用する食品事業者向け （調理・提供施設及び食品製造工場を想定） ※詳細は食品防御対策ガイドラインを参照のこと	Food Defense Measures Guidelines - Checklist for Food Delivery Services (For businesses using food delivery service providers: cooking and serving facilities and food manufacturing plants) For details, refer to the Food Defense Measures Guideline
			取っている。	food storage areas, and entrances and windows of the kitchen.
２５ □	○（顧客情報の管理） ・顧客情報（取引業者・利用客）等の重要なデータシステムへのアクセス許可者は極力制限し、不正なアクセスを防止している。	(Management of Customer Information) ● Access to important data systems containing customer information (such as business partners and clients) is highly restricted to prevent unauthorized access.	○（顧客情報の管理） ・顧客情報（取引業者・利用客等）の重要なデータシステムへのアクセス可能者は、接客の責任者などに限定している。	(Management of Customer Information) ● Access to important data systems containing customer information (such as business partners and clients) is restricted to responsible personnel, such as those in charge of customer service.
２６ □	―		○（監視カメラの管理） ・監視カメラの映像は外部に流出しないように注意し、特にクラウド型のパスワードは、初期設定のまま使用せず、定期的に変更している。	(Surveillance Camera Management) ● Ensure that camera footage does not leak externally. For cloud-based systems, do not use default passwords and change them regularly.
	■入出荷等の管理	**Management of Shipments and Deliveries**	■入出荷等の管理	■ Management of Shipping and Receiving
２７ □	○（ラベル・包装・数量の確認） ・商品等の受取り時に、ラベルや包装の異常の有無、注文番号、発注商品と数量の整合性を確認し、異常があれば施設責任者に連絡している。 ・異常を発見した場合は、施設責任者に報告し、施設責任者はその対応を予め決めている。	(Verification of Labels, Packaging, and Quantity) ● Upon receiving products, we check the order number, any abnormalities in labels or packaging, and the consistency between the ordered products and quantities. If any abnormalities are found, we contact the facility manager. ● When an abnormality is discovered, it is reported to the facility manager, who has predetermined procedures for handling such issues.	○（ラベル・包装・数量の確認） ・商品等の受渡し時に、ラベルや包装の異常の有無、注文番号、発注商品と数量の整合性を確認し、異常があれば施設責任者に連絡している。 ・異常を発見した場合は、店長や責任者に報告し、店長や責任者はその対応を予め決めている。	(Verification of Labels, Packaging, and Quantity) ● Upon receiving or delivering products, we check the order number, any abnormalities in labels or packaging, and the consistency between the ordered products and quantities. If any abnormalities are found, we contact the facility manager. ● When an abnormality is discovered, it is reported to the store manager or responsible personnel, who have predetermined procedures for handling such issues.
２８ □	○（配達中の商品の増減や汚染行為の徴候への対応） ・配達中に商品の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者に報告し、施設責任者はその対応を予め決めている。	(Response to Signs of Product Loss, Increase, or Contamination During Delivery) ● If any signs or evidence of product loss, increase, or intentional food contamination are observed during delivery, it is reported to the facility manager, who has predetermined procedures for handling such issues.	○（配達中の商品の増減や汚染行為の徴候への対応） ・配達中に商品の紛失や増加、意図的な食品汚染行為の兆候・形跡等が認められた場合は、施設責任者や調理責任者に報告し、施設責任者や調理責任者はその対応を予め決めている。	(Response to Signs of Product Loss, Increase, or Contamination During Delivery) ● If any signs or evidence of product loss, increase, or intentional food contamination are observed during delivery, it is reported to the facility manager or the person in charge of cooking., who has predetermined procedures for handling such issues.
２９ □	○（対応体制・連絡先等の確認） ・配達した商品の依頼元や配達先の連絡先を、すぐに確認できるようにしている。	(Verification of Response System and Contact Information) ● We ensure that the contact information for the client and the delivery destination of the delivered products can be quickly verified.	○（対応体制・連絡先等の確認） ・配達した商品により喫食者に異変が見られた場合の対応体制・連絡先等を、誰でもすぐに確認できるようにしている。	(Verification of Response System and Contact Information) ● The response system and contact information for cases where consumers experience any adverse effects from delivered products are made readily accessible to everyone.
	２．可能な範囲での実施が望まれる対策	**2. Measures Recommended to be Implemented as Far as Possible**	**２．可能な範囲での実施が望まれる対策**	**2. Measures Recommended to be Implemented as Much as Possible**
３０ □	○（ドライブレコーダー・GPS 等の活用） ・不測の事態が起こった場合などに備えドライブレコーダーや GPS 等により配達中の位置の確認や記録を検討している。	(Utilization of Dashcams and GPS) ● Considering the use of dashcams and GPS to monitor and record the location during deliveries in case of unforeseen circumstances.	○（ドライブレコーダー等・GPS の活用） ・不測の事態が起こった場合などに備え、ドライブレコーダーや GPS 等を活用し、配達中の安全性の確保が可能な事業者を選定し委託している。	(Utilization of Dashcams and GPS) ● To prepare for unforeseen circumstances, businesses that can ensure safety during delivery by utilizing dashcams and GPS are selected and entrusted with the task.

別添２－４

食品防御対策ガイドライン
（フードデリバリーサービス配達員向けチェックリスト）
（令和 5 年度版）→20250210 確認（修正なし）英訳対比表（案）→万博等を踏まえて再修正後作成予定⇒20260127 班会議版

【本チェックリストの対象】 食品の配達を担当するフードデリバリーサービス提供事業者（以下「デリバリー事業者」という。自社配達、フードデリバリー・デジタル・プラットフォーム運営事業者及び個人事業主、タクシー運転手等の兼業者を含む）において、配達員が日々の配達において活用されることを念頭に作成したものである。 事業者においては、食品防御対策ガイドライン（フードデリバリーサービス提供事業者及び利用事業者向けチェックリスト（案））と併せて使用されることを想定している。	**[Scope of This Checklist]** This checklist is intended for food delivery service providers (hereinafter referred to as "delivery providers") responsible for delivering food. This includes in-house delivery, food delivery digital platform operators, sole proprietors, and those with secondary jobs such as taxi drivers. It is designed to be used by delivery personnel in their daily deliveries. It is assumed that businesses will use this checklist in conjunction with the Food Defense Measures Guidelines (Checklist for Food Delivery Service Providers and Users (Draft)).

No.	内容	
1 □	○ （新規登録・契約・採用時の身元の確認等） ・配達員として新たに登録・契約・採用される際には、事業者の求めに応じて運転免許証の原本等、身元を証明する書類を提示している。 ・運転免許証の原本は、事業者の求めに応じて定期的に提示している。	**(Verification of Identity at the Time of New Registration, Contract, or Employment)** ● When newly registering, contracting, or being employed as a delivery person, Ipresent documents providing myidentity, such as the original driver's license, upon the request of the business. ● The original driver's license is periodically presented upon the request of the business.
2 □	○（契約者の確認） ・配達員として契約された場合には、成りすまし等を防ぐために、依頼元事業者等に適切に発注時の注文番号等で確認してもらっている。	**(Verification of the Contractor)** ● When contracted as a delivery person, to prevent impersonation, the ordering business should verify the order number, etc., at the time of order placement.
3 □	○（食品防御に関する知識と認識） ・配達員として事業者に登録する際には、事業者が推奨する、取扱う商品の品質と安全確保、食品防御に関する適切な知識を持っている。 ・不適切な行動があった場合、刑事罰や賠償責任等が発生することを正しく認識している。 ・登録・契約・採用時には、本チェックリスト等を用いて、食品防御に関する知識を確認している。	**(Knowledge and Awareness of Food Defense)** ● When registering as a delivery person with the business, I possess appropriate knowledge recommended by the business regarding the quality and safety assurance of the products handled, as well as food defense. ● I correctly recognize that inappropriate actions may result in criminal penalties or liability for damages. ● At the time of registration, contracting, or employment, my knowledge of food defense is confirmed using this checklist, etc.

No.	内容	
4 □	○ （健康管理） ・日々、健康状態を適切に確認し、体調不良があった場合は、速やかに契約先・取引先等に相談している。	**(Health Management)** ● Appropriately check my health condition daily, and if I experience any illness, promptly consult with my contractor or business partner.
	○（感染症対策） ・地域の感染症情報や、世界的な感染症の流行等に関する情報にも普段から注意を払い、国等が推奨する感染予防策を適切に実践している。 ・感染の恐れがある場合は、速やかに契約先・取引先等に相談している。	**(Infection Control Measures)** ● I regularly pay attention to local infection information and global infection outbreaks, and appropriately implement infection prevention measures recommended by the government and other authorities. ● If there is a risk of infection, I promptly consult with my contractor or client. (Refer to section 3 for food delivery service providers)
5 □	○（用具等の管理） ・配達員等は、注文番号、運搬用ボックスを適切に管理し、自分以外の者には貸与しない。	**(Management of Equipment, etc.)** ● Delivery personnel appropriately manage order numbers and transport boxes, and do not lend them to others.
6 □	○（商品の受渡し） ・商品の受取りは、定められた受渡し窓口で行い、不用意に厨房内へは立入らないようにしている。 ・商品等の受取り時に、ラベルや包装の異常の有無、発注商品と数量の整合性を確認し、記録に残している。	**(Product Handover)** ● Products are received at the designated handover counter, and unnecessary entry into the kitchen is avoided. ● Upon receiving products, any abnormalities in labels or packaging, as well as the consistency of ordered products and quantities, are checked and recorded.
7 □	○（配達中の対策） ・配達中に、第三者が意図的に有害物質を食品へ混入することがないよう、商品にカバーや封印等が施されていることを確認している。	(Measures During Delivery) ● During delivery, it is ensured that products are covered or sealed to prevent any third party from intentionally contaminating the food with harmful substances.
8 □	○（異常発見時等の報告） ・配達中に商品の破損や異常・異臭等を発見、または苦情等を受けた場合は、速やかに委託を受けた運営事業者や食品事業者等の責任者に報告している。	(Reporting Upon Discovery of Abnormalities, etc.) ● If damage, abnormalities, or unusual odors are discovered in products during delivery, or if complaints are received, I promptly report to the responsible party of the contracted operating company or food business.
9 □	○（配達員の私物等） ・配達中は不要な私物は携行せず、また、配達用車両の荷台や配達用バック内では、私物と食品（商品）との接触を避ける様にしている。	(Personal Belongings, etc. of Delivery Personnel) ● During delivery, unnecessary personal belongings are not carried, and contact between personal belongings and food (products) is avoided in the cargo area of the delivery vehicle or inside the delivery bag.
１０ □	○（駐車・駐輪） ・配達用車両は、指定された場所に駐車・駐輪している。駐車・駐輪許可証が発行されている場合は、適切に使用している。	(Parking and Bicycle Parking) ● Delivery vehicles are parked or parked in designated areas. If parking or bicycle parking permits are issued, they are used appropriately.

No.	内容	
１１ □	○（車両を離れる際の対策） ・荷台に施錠が出来る配達用車両での配達を行い、走行中や配達で車両を離れる際には、荷台の施錠を確認している。 ・自転車やバイクで配達する場合は、配達用バックを自転車等に置いたままにしない。 ・自動車で配達する場合は、車両の施錠を確実に実施する。 ・不測の事態が起こった場合等に備え、ドライブレコーダーや GPS 等を活用している。	(Measures When Leaving the Vehicle) ● Deliveries are made using delivery vehicles with lockable cargo areas, and the locks are checked when leaving the vehicle during deliveries or while driving. ● When delivering by bicycle or motorcycle, the delivery bag is not left on the bicycle or motorcycle. ● When delivering by car, the vehicle is securely locked. ● In preparation for unforeseen circumstances, devices such as dashcams and GPS are utilized.
１２ □	○（顧客情報の管理） ・配達員は、プラットフォーム運営事業者が保管する重要な顧客情報（取引業者・利用客）等のデータシステムには、不正・にアクセスしないようにしている。	(Customer Information Management) ● Delivery Personnel make sure that there is no unauthorized access to important customer information (such as business partners and clients) stored by platform operator.

厚生労働科学研究費補助金（食品の安全確保推進事業）
分担報告書

新型コロナ感染症収束後におけるロボット配膳システムと食品防御の課題

研究分担者　加藤　礼識　（茨城キリスト教大学　生活科学科　食物健康科学科　講師）
研究協力者　田崎ひなた　（茨城キリスト教大学　生活科学部　食物健康科学科）
研究協力者　平子ほほみ　（茨城キリスト教大学　生活科学部　食物健康科学科）
研究協力者　永野　衣祝　（別府大学　食物栄養科学部　発酵食品学科）
研究協力者　多川　優也　（別府大学　大学院　食物栄養科学研究科）
研究協力者　長田　瑞花　（奈良県立医科大学　公衆衛生学講座）

研究要旨
本研究は、飲食店において普及が進むロボット配膳システムについて、食品防御（Food Defense）の観点から課題を整理し、安全確保の方向性を検討することを目的とした。人手不足や人件費高騰、感染症対策を背景に導入が進む一方で、食品搬送中の監視体制の希薄化や、親和的デザインによる接触行動の誘発など、新たな脆弱性が生じている可能性が示された。販売代理店および導入店舗への聞き取り調査の結果、食品防御は店舗責任と認識され情報共有体制が未整備である実態が明らかとなった。一方で、配膳業務の自動化により人的余力を監視やサービス向上に再配分することで、安全性強化につながる可能性も示唆された。今後は人的監視の維持、物理的防御策の導入、情報共有体制の構築を柱としたガイドライン策定が必要である。

A. 研究目的

近年、飲食業界では慢性的な人手不足や人件費の高騰、新型コロナウイルス感染症流行下における非接触化ニーズの高まりを背景として、ロボット配膳システムの導入が急速に進展している。配膳業務の自動化は、省人化や業務効率化、感染リスク低減といった点で一定の効果を上げている一方、食品を搬送する主体が人から機械へと移行することにより、従来の運用体制では想定されていなかった新たなリスクが生じている可能性がある。

食品防御（Food Defense）は、故意による汚染や悪意ある行為から食品を守るための概念であり、衛生管理や HACCP とは異なる視点からの対策を必要とする。しかし、現在普及しているロボット配膳システムは、省人化や顧客サービス向上を主目的として設計されており、食品防御の観点が十分に組み込まれているとは言い難い状況にある。また、導入店舗、販売代理店、メーカー間における情報共有体制も必ずしも整備されていない。

本研究の目的は、ロボット配膳システム

導入に伴う食品防御上の脆弱性を明らかにするとともに、人的監視体制、物理的防御措置、情報共有体制の三側面から課題を整理し、実効性のある対策の方向性を提示することである。さらに、将来的なロボット配膳システムに特化した食品防御対策ガイドライン策定に資する基礎資料を得ることを最終的な目的とする。

B．研究方法

本研究では、ロボット配膳システムにおける食品防御上の課題を多角的に把握するため、文献調査および質的調査を組み合わせた研究方法を採用した。

まず、文献調査として、厚生労働科学研究報告書、食品防御に関する国内外のガイドライン、関連する学術論文および行政資料を収集・整理し、食品防御の基本概念、従来の対策枠組み、および飲食店における適用可能性について検討した。これにより、ロボット配膳システム導入以前の食品防御対策の構造を整理し、本研究における分析視点を明確化した。

次に、質的調査として、ロボット配膳システム販売代理店 2 社および導入飲食店 1 社に対し、半構造化インタビューを実施した。主な調査項目は、①導入目的および運用体制、②食品防御対策の実施状況、③いたずら・過激接触等の発生状況、④トラブル発生時の対応主体、⑤製品仕様変更の可能性、⑥情報共有体制の有無、である。

インタビュー内容は記録・整理し、逐語録を作成した上で、テーマ別に分類・分析を行った。分析にあたっては、食品防御の観点から「人的監視体制」「物理的防御措置」「情報共有構造」の三側面に着目し、構造的課題の抽出を試みた。
なお、調査協力企業および店舗の名称は匿名化し、倫理的配慮を行った。

C. 研究結果

本研究では、文献調査および販売代理店 2 社、導入飲食店 1 社への聞き取り調査を通じて、ロボット配膳システムの普及背景、運用実態、ならびに食品防御上の課題構造を多面的に整理した。その結果、ロボット配膳は単なる業務効率化ツールではなく、店舗内のリスク構造そのものを変化させる存在であることが明らかとなった。以下に、得られた知見を詳細に示す。

1. ロボット配膳システム普及の多層的背景

ロボット配膳システムの普及は、一過性の流行や技術的興味に基づくものではなく、飲食業界を取り巻く構造的課題の蓄積に対応する中で進展してきたものである。本研究の聞き取り調査および関連資料の整理から、普及の背景には大きく分けて「労働構造の変化」「経営環境の圧迫」「感染症対策の社会的要請」「サービス価値の再定義」という四つの要素が相互に作用していることが明らかとなった。

第一に、労働構造の変化である。少子高齢化の進行により生産年齢人口は減少を続けており、飲食業界は他業種と比べても人材確保が困難な状況にある。特に飲食店は、土日祝日や夜間勤務を含む不規則な労働形態であることから、若年層の就労選択肢として敬遠される傾向がある。また、外国人労働者に依存してきた店舗では、国際移動の制限等による労働供給の不安定化も経験している。このような状況下で、安定

的に配膳業務を担う代替手段としてロボットが注目されることとなった。

第二に、経営環境の圧迫である。最低賃金の継続的上昇は、労働集約型産業である外食産業に直接的な影響を与えている。人件費の上昇に対し、価格転嫁が十分に行えない中小規模店舗では、利益率の低下が顕在化している。そのため、固定費削減の一環として業務の自動化・機械化が検討されるようになった。ロボット配膳は初期投資を要するものの、長期的には人件費削減効果が見込まれるとの認識が広がっている。

第三に、感染症対策という社会的要請である。新型コロナウイルス感染症の流行は、飲食店の営業形態に大きな変化をもたらした。非接触型注文システムやセルフレジの導入が進む中、配膳業務においても対面機会を減少させる手段としてロボットが導入された。この経験により、ロボット配膳は単なる効率化装置ではなく、「安全・安心」を可視化する存在としても機能するようになった。感染症収束後も、衛生意識の高まりは継続しており、非接触型サービスへの需要は一定程度維持されている。

第四に、サービス価値の再定義である。近年の外食産業では、単に料理を提供するだけでなく、体験価値を提供することが重視されている。ロボット配膳は、その視覚的インパクトやエンターテインメント性により、顧客体験を向上させるツールとしても評価されている。実際に、ロボットを「客寄せ」の要素として活用しているとの回答も得られた。このように、経営合理性だけでなく、ブランドイメージや差別化戦略の一環として導入されている側面も存在する。

以上のように、ロボット配膳システムの普及は、労働力不足への対応という消極的要因と、サービス価値向上という積極的要因の双方によって推進されていることが明らかとなった。この多層的背景を理解することは、食品防御対策を検討する上で重要である。なぜなら、導入目的が省人化のみである場合と、サービス強化を含む場合とでは、店舗内の人的配置や監視体制の構築方法が大きく異なるためである。

したがって、ロボット配膳の普及は単なる技術導入ではなく、飲食業界における労働構造・経営戦略・社会的価値観の変化を反映した現象であり、その全体像を踏まえた上で食品防御の課題を整理する必要がある。

2. 食品防御上の新たなリスク構造

ロボット配膳システムの導入は、配膳工程の自動化という業務効率上の利点をもたらす一方で、食品防御の観点からは従来とは異なるリスク構造を形成している。本研究の聞き取り調査および現状分析から、これらのリスクは単発的な問題ではなく、「設計思想」「運用体制」「心理的要因」「情報構造」の複数要素が重なり合うことで生じていることが明らかとなった。

(1) 新奇性・親和性が誘発する接触リスク

現在国内で広く普及しているロボット配膳システムは、ネコ型をはじめとする親しみやすいデザインを採用し、音声や表情表示などのインタラクティブ機能を備えているものが多い。これらは顧客体験の向上や集客効果を目的とした設計であるが、食品防御の観点からは接触行動を誘発する要因となり得る。

特に児童や若年層では、移動するロボットに触れる、撫でる、ボタンを押すといった行為が自然発生的に起こりやすい。食品を搭載した状態で顧客の近傍を通過する構造は、意図的行為のみならず偶発的接触の可能性も高める。また、写真撮影や動画撮影を目的とした接近行動も見受けられるとの指摘があった。

従来の人による配膳では、配膳者自身が食品を保持しており、顧客が直接接触する機会は限定的であった。ロボット配膳では食品が一定時間無人状態で移動するため、第三者が介入可能な空間が生じる点が構造的な違いである。

(2) 触知部と食品部の物理的分離不足

ロボット配膳システムの多くは、顧客とのコミュニケーション機能を重視した設計となっており、タッチパネルや外装部分への接触を前提としている。一方で、食品を載せるトレイ部分が物理的に十分保護されていない場合があり、触知部と食品部の明確な分離がなされていない事例が確認された。

食品防御の基本原則の一つは「物理的バリアの構築」であるが、現行の配膳ロボットでは、食品が開放空間に露出したまま搬送される構造が一般的である。カバーや蓋の装着は理論上有効な対策であるが、利便性や作業効率の低下、デザイン性の毀損を理由に採用されていない例が多い。

このように、顧客満足度向上を優先した設計思想が、食品防御の多層防御構造を十分に確保していない可能性が示唆された。

(3) 無人搬送時間帯と監視の空白

人による配膳では、配膳者が移動中も食品を直接管理しており、監視機能を自然に担っていた。しかしロボット配膳では、食品が自律的に店内を移動するため、搬送中に従業員の視線が必ずしも届かない時間帯が生じる。

省人化が進んだ店舗では、フロアスタッフの配置人数が少なく、全経路を常時視認することは困難である。特に混雑時やピークタイムでは、監視密度が低下する傾向があると指摘された。

この「監視の空白時間」は、意図的な異物混入や悪戯行為が発生し得る環境を構成する可能性がある。また、実際に重大事例が発生していなくとも、構造的脆弱性が存在すること自体がリスク評価上の課題となる。

(4) 心理的抑止力の変化

人の存在はそれ自体が抑止力となる。従業員が近くにいる環境では、不適切行動をとる心理的ハードルが高くなる。一方、ロボット配膳では、人の直接的視線が感じられにくく、心理的抑止力が低下する可能性がある。

特に集団心理が働く環境では、「機械相手である」という認識が行動規範を緩和させる可能性も否定できない。これは食品防御に限らず、機械化が進むサービス環境全般に共通する課題である。

(5) トラブル情報の未集約と制度的空白

販売代理店への聞き取りでは、いたずらや過度な接触の件数について体系的なデータ収集は行われていないとの回答が得られ

た。店舗内で発生した問題は個別に対応され、販売代理店や製造元へ詳細が共有される仕組みは整備されていない。

この情報分断構造は、設計改善や予防的対策の蓄積を困難にする。食品防御は過去事例の分析と共有によって強化されるが、現状ではその基盤が十分とは言えない。

(6) 海外製造構造による設計改善の困難性

国内で導入されているロボット配膳システムの多くは海外メーカー製である。したがって、日本国内で生じた課題や改善要望が設計段階に反映されるまでには時間的・制度的障壁が存在する。

販売代理店は技術的改修の権限を持たない場合が多く、構造的問題が放置される可能性もある。この点は、食品防御対策を制度化する上で重要な検討課題である。

〔総括〕

以上の分析から、ロボット配膳システムにおける食品防御上のリスクは、単一の技術的欠陥に起因するものではなく、設計思想、運用体制、心理的要因、情報共有構造が相互に影響し合う複合的構造であることが明らかとなった。

すなわち、ロボット配膳は効率化を実現する一方で、食品防御の観点からは「無人搬送」「接触誘発設計」「監視の希薄化」「情報分断」という新たな課題を内包している。しかし同時に、これらは運用設計と制度整備によって改善可能な要素でもある。したがって、今後の対策検討においては、単なる技術的修正にとどまらず、人的配置、情報共有体制、設計ガイドラインを含む包括的アプローチが求められる。

3. 販売代理店における認識と構造的課題

本研究において実施した販売代理店 2 社への聞き取り調査から、ロボット配膳システムの食品防御に関する認識および制度的課題が明らかとなった。両社に共通していたのは、ロボット配膳システムを「飲食物を運搬する機器」として位置づけ、食品そのものの安全管理は基本的に導入店舗の責任範囲であるとの認識であった。

(1) 食品防御に対する位置づけ

販売代理店への聞き取り調査において最も特徴的であったのは、ロボット配膳システムを「食品を運ぶ機械」として位置づける認識であった。すなわち、ロボットは配膳という労務を代替する存在であり、食品そのものの安全管理や防御対策は、基本的に飲食店側の業務範囲であるとの立場である。この認識は、契約上および法的責任の整理という観点では一定の合理性を有する。しかしながら、食品防御の観点からは、食品を運搬する構造そのものが変化している以上、単なる運搬機器としての位置づけでは十分とは言い難い。従来の配膳では、人が常に食品を保持し、監視機能を担っていた。ロボット配膳では、食品が無人状態で移動する時間帯が生じるため、設計段階で食品防御を考慮する必要性が高まる。

それにもかかわらず、販売代理店側では「食品防御は導入店舗の管理責任である」との前提が強く、設計仕様の中に食品防御を組み込むという発想は現段階では限定的であった。このことは、ロボット配膳がもたらすリスク構造の変化が、製品設計思想

に十分反映されていない可能性を示している。

さらに、食品防御という概念自体が、販売現場ではまだ一般化していない可能性も示唆された。衛生管理や事故防止とは異なり、意図的混入という視点は、製品開発段階で体系的に議論されているとは言い難い状況である。

(2) トラブル実態の把握不足

販売代理店は、いたずらや過度な接触、妨害行為といった事例について体系的なデータ収集を行っていないとの回答であった。修理依頼があった場合でも、機械的故障として処理されることが多く、その原因が顧客行為に起因するものかどうかまで詳細に分析される仕組みは整備されていない。

このことは、食品防御の観点から重大な課題である。食品防御は過去事例の分析と情報共有によって強化される概念であり、トラブルの発生状況を把握しなければ、予防的対策の立案は困難である。にもかかわらず、現状では店舗単位で問題が完結し、販売代理店や製造元に体系的に報告される仕組みが存在しない。

さらに、店舗側もブランドイメージへの影響を懸念し、軽微なトラブルを積極的に外部へ報告しない可能性がある。この情報の非対称性は、構造的脆弱性を可視化しにくくしている。

したがって、現状の情報収集体制は受動的かつ断片的であり、食品防御対策を制度化する基盤としては不十分であることが明らかとなった。

(3) 海外製造構造による改善の困難性

現在日本国内で導入されているロボット配膳システムの多くは海外メーカー製であり、国内販売代理店は基本設計の変更権限を持たない。この構造は、食品防御対策を迅速に製品仕様へ反映させる上で大きな制約となっている。

販売代理店からは、「設計変更は製造元の判断事項であり、国内の要望のみで大幅な改修は困難である」との意見が示された。また、製造元にとっては世界市場全体が対象であり、日本国内特有のリスクや社会的要請が優先順位の上位に位置づけられるとは限らない。

さらに、文化的背景や法制度の違いも影響する可能性がある。食品防御に対する社会的感度や規制水準が異なる場合、日本国内で求められる安全水準が設計段階に十分反映されない恐れがある。

このように、製造拠点が海外にあることは、食品防御対策を国内主導で制度化する際の構造的障壁となり得る。

(4) 利便性と安全性の優先順位

一部店舗では、食品トレイにカバーを設置するなどの対策が試みられた事例が確認された。しかし、視認性の低下や料理の取り出しにくさ、作業効率の悪化などの理由により、最終的に撤去されたとの報告があった。

この事例は、現場において利便性や顧客体験が強く重視されていることを示している。ロボット配膳は省人化と同時にエンターテインメント性を持つ装置として位置づけられており、デザイン性や操作性を損なう改修は導入効果を減殺する可能性がある

と認識されている。

また、重大事故が顕在化していない段階では、安全対策への投資優先度が低くなる傾向もみられる。これは食品防御全般に共通する課題であり、「問題が起きていないから対策しない」という受動的姿勢が構造的リスクを温存する可能性がある。

利便性と安全性のバランスをどのように設計段階で確保するかは、今後の重要な検討課題である。

(5) 責任分散構造の存在

本研究で明らかとなった最も重要な構造的課題の一つが、責任の分散である。販売代理店は「食品管理は店舗責任」とし、店舗は「製品構造はメーカー責任」と捉える傾向がある。このような構図は、食品防御対策の主体を曖昧にする。

食品防御は多層防御（multiple barrier）の概念に基づき、設計段階・販売段階・運用段階が連携して初めて機能する。しかし現状では、各段階が独立しており、横断的なガイドラインや統一基準は存在しない。

さらに、法的義務として明確に規定されていない分野であることも、責任の所在を不明確にしている要因である。結果として、重大事例が発生しない限り、包括的対策が進みにくい構造となっている。

この責任分散構造を是正し、設計・販売・運用の各段階を統合する枠組みを構築することが、食品防御強化の前提条件であると考えられる。

〔総括〕

販売代理店における認識は、ロボット配膳を「運搬機器」として捉える技術中心的視点が強く、食品防御を設計要素として積極的に組み込む段階には至っていないことが明らかとなった。また、トラブル情報の未集約、海外製造構造、責任分散といった制度的課題が、食品防御対策の体系化を阻害している可能性が示唆された。

この結果は、食品防御対策を店舗単位の努力に委ねるのではなく、販売代理店や製造元を含めた制度的枠組みの再構築が必要であることを示している。

4. 導入店舗における運用実態

本研究において聞き取りを行った導入飲食店では、ロボット配膳システムの活用方法は単なる人員削減策にとどまらず、店舗運営全体の再設計と密接に関連していることが明らかとなった。すなわち、ロボット導入の効果は「どの業務を代替させ、どの業務に人を再配置するか」という運用設計によって大きく異なる。

(1) 導入目的の実態 ― 経営合理性と労務構造改革

導入店舗では、ロボット配膳の導入目的として表面的には「人手不足対策」が挙げられたが、実際にはより複合的な意図が存在していた。

第一に、慢性的労働力不足の緩和である。特にピークタイムにおける配膳業務は往復回数が多く、身体的負担が大きい。重い鉄板料理や複数皿の同時運搬は従業員に相当な負担を与えており、離職要因の一つとなっていた。ロボット導入により、体力負担の軽減が図られ、従業員定着率向上への期待も示された。

第二に、業務標準化である。ロボットは

設定されたルートを一定速度で移動するため、配膳品質のばらつきが少ない。新人教育の負担軽減という副次的効果も確認された。

第三に、サービス価値の向上である。ロボットが話題性を持つことで集客効果が生まれ、顧客体験の差別化が図られている。これは経営戦略上の意図も含まれている。

このように、導入は単なるコスト削減ではなく、労務構造改革とサービス戦略の両面を持つものであった。

(2) 人的再配置と監視機能の再構築

配膳業務が軽減された結果、従業員の業務内容は変化している。具体的には、

- 客席巡回頻度の増加
- 顧客の食事状況の確認
- 不審行動の観察
- トラブル初期対応

などが強化されている。

導入初期には、ロボットに対する接触や妨害行為が散見されたが、フロアスタッフが積極的に巡回する体制を整えたことで、問題行動は減少したとの報告があった。

この結果は、「人の目」が依然として食品防御における最も強力な抑止装置であることを示している。すなわち、ロボット導入は監視機能を弱体化させるのではなく、人的資源の再配置次第でむしろ強化し得る。

(3) 顧客満足度と抑止メカニズム

導入店舗では、ロボット配膳により従業員が顧客との対話時間を確保できるようになり、サービスの質が向上したとの評価が得られた。

食品防御の観点では、店舗の雰囲気や顧客満足度は重要な要素である。不満やストレスは逸脱行動の誘因となることが過去事例から示唆されている。満足度が高い環境では、意図的行為の発生確率が低減する可能性がある。

さらに、従業員が顧客と積極的にコミュニケーションをとることで、「見られている感覚」が維持され、心理的抑止力が働く構造が形成されている。

(4) 現場が認識する具体的リスクの類型化

導入店舗では、以下のようなリスク類型が挙げられた。

① 物理的接触リスク
子どもが触れる、写真撮影時に接触する、荷物が引っかかる等。

② 走行妨害リスク
顧客が意図せず経路を塞ぐ、椅子やベビーカーが障害となる。

③ 下膳時リスク
残飯が露出し、不衛生状態になる可能性。

④ 意図的行為の潜在性
重大事例はないが、構造的に介入可能な状態であること。

これらは重大事故には至っていないが、「発生可能性の存在」自体がリスク評価上重要である。

(5) 物理的対策の現実的限界

食品トレイへのカバー装着や囲い込み構造は理論上有効であるが、以下の課題が挙げられた。

- 提供スピードの低下
- 顧客が料理を取りづらい

- 視認性の低下
- デザイン性の毀損

特に回転率を重視する業態では、わずかな遅延が売上に影響する。したがって、安全性を高める設計は、業態特性を踏まえたバランス設計が不可欠である。

(6) ロボットと人の役割分担モデル

導入店舗では、以下の役割分担が明確化されていた。

ロボット：

・重量物運搬
・定型ルート移動
・ピークタイム補助

人：

・最終確認
・顧客対応
・監視
・異常対応

この協働モデルは、「完全自動化」ではなく「補助的自動化」である。食品防御の観点からは、この補助型モデルの方が安全性を確保しやすい可能性がある。

(7) 総合評価 ― 二面性と運用依存性

導入店舗の実態から導かれた最も重要な示唆は、ロボット配膳は食品防御を弱体化させる技術でもあり、強化する契機にもなり得るという二面性である。

省人化のみを目的とし監視人員を削減すればリスクは増大する。一方で、業務再配分により監視体制を再構築すれば、従来より強固な体制を構築することも可能である。

すなわち、食品防御の強度は技術そのものではなく、「導入目的」「人的配置」「店舗文化」「管理意識」によって決定される。この運用依存性を踏まえた制度設計が今後の課題である。

D. 考察

本研究の結果から、ロボット配膳システムは飲食店の業務効率化および労務負担軽減に寄与する一方で、食品防御（Food Defense）の観点からは従来の管理構造を変容させる要素を内包していることが明らかとなった。本考察では、①リスク構造の再編、②多層防御理論との関係、③運用依存性の構造分析、④責任分散と制度的空白、⑤技術と人間の協働モデル、⑥政策的・制度的含意の六側面から詳細に検討する。

1. リスク構造の再編 ― 無人搬送という構造的転換

従来の飲食店における配膳は、人が食品を直接保持しながら移動するという形式をとっていた。この構造では、配膳者の存在が以下の三機能を同時に担っていた。

- 物理的管理機能（食品を直接保持する）
- 視覚的監視機能（周囲を確認する）
- 心理的抑止機能（顧客に見られている感覚を与える）

ロボット配膳では、この三機能が分離される。ロボットは物理的運搬機能を担うが、監視機能や抑止機能は自動的には付随しない。結果として、食品が一定時間「無人状態」で移動するという新たな状況が生じる。

この無人搬送構造は、食品防御上の前提

条件を大きく変化させる。すなわち、食品は常に人の直接的監視下にあるという従来の暗黙の前提が崩れる。この構造変化を認識せずに従来型の管理を継続した場合、リスクは潜在化する。

重要なのは、実際に重大事例が発生していないことと、構造的脆弱性が存在しないことは同義ではないという点である。食品防御は「発生後対応」ではなく「発生可能性の低減」を目的とする概念であり、構造的評価が不可欠である。

2. 多層防御理論との整合性 ― ロボット配膳環境における防御層の再設計

食品防御は、単一の対策によって成立するものではなく、複数の防御層を重ね合わせることでリスクを低減する「多層防御（multiple barrier）」の考え方に基づいて構築される。これは、いずれか一つの防御が破られた場合でも、次の層が機能することで全体として安全性を確保するという発想である。

本研究の結果をこの理論枠組みに照らして整理すると、ロボット配膳システム導入環境では、既存の防御層の一部が弱体化し、新たな層の設計が十分に行われていない可能性が明らかとなった。

（1）物理的防御層の再評価

従来の飲食店においては、厨房と客席の分離、調理場への立入制限、食品保管エリアの管理など、空間的分離が物理的防御層として機能していた。一方、客席内での配膳工程については、配膳者が直接食品を保持すること自体が物理的管理を担っていた。

ロボット配膳では、食品がトレイ上に露出した状態で客席間を移動するため、物理的バリアは限定的となる。特に、トレイが開放構造である場合、食品は第三者が容易に接触可能な位置に存在する。

理論上は、以下のような物理的強化策が考えられる。

- 半透明カバーによる囲い込み
- ワンタッチ開閉式保護構造
- 食品収納部の高さ制限
- トレイ縁部の立ち上げ設計

しかし現場では、提供速度の低下や視認性の悪化を理由に全面的な採用には至っていない。ここに、物理的防御層とサービス効率とのトレードオフが存在する。

したがって、ロボット配膳環境では「完全封鎖型バリア」ではなく、「接触機会を減少させる合理的設計」という新たな物理的防御概念の導入が求められる。

（2）人的防御層の変動性と再構築

多層防御の中核となるのは人的監視である。従来は、配膳者が食品を監視しながら移動することで、自然に人的防御層が形成されていた。ロボット導入後、この層は二つの方向に分岐する。

① 省人化のみを追求する場合：人的防御層が薄くなる
② 業務再配分を行う場合：人的防御層が強化される

本研究で確認された導入店舗では、後者のモデルが機能していた。すなわち、配膳業務削減により生じた人的余力をフロア巡回や顧客観察に充てることで、人的防御層が再構築されていた。この結果は、人的防御層が固定的ではなく、経営判断と運用設

計によって強度が変化する可変層であることを示している。したがって、ガイドライン策定においては「ロボット 1 台あたりの最低巡回頻度」など、具体的な運用指標を提示する必要がある。

(3) 心理的防御層の再考

食品防御において見落とされがちなのが、心理的抑止層である。人が食品を運搬する環境では、「従業員に見られている」という感覚が不適切行為を抑止する。ロボット配膳では、移動主体が機械であるため、この心理的抑止効果が低減する可能性がある。特に混雑時には、無人搬送時間が延び、抑止力が弱まる。

一方で、導入店舗ではフロアスタッフが積極的に巡回することで「人の目」を可視化し、心理的抑止層を維持していた。これは、物理的監視と心理的監視が重なり合うことで抑止効果が強化されることを示している。したがって、ロボット配膳環境では心理的防御層を意識的に設計する必要がある。

(4) 情報防御層の制度化不足

多層防御において極めて重要なのが情報層である。トラブルやヒヤリハット事例の共有は、次の防御強化につながる。
しかし本研究では、

- トラブル件数の体系的把握がない
- 販売代理店への報告制度がない
- 製造元へのフィードバック経路が限定的

という状況が確認された。

これは、防御層としての情報システムが未成熟であることを意味する。食品防御を強化するためには、

- 統一的報告様式
- データベース化
- 定期的情報共有会議

などの制度的枠組みが必要である。

(5) 技術的防御層の可能性

ロボット配膳は、逆に新たな防御層を創出する可能性も持つ。例として、

- カメラ搭載による録画監視
- AI による異常行動検知
- 接触感知センサー
- 走行ログ記録

などが考えられる。

これらは従来の人配膳では実現しにくかった防御層である。ただし、プライバシー保護、コスト、デザイン性との均衡が必要である。

(6) 総合評価 ― 防御層の再設計が鍵

以上を総合すると、ロボット配膳環境では、

- 一部防御層が弱体化し
- 一部防御層が再設計可能であり
- 新たな防御層の導入余地がある

という三重構造が存在する。

重要なのは、「防御層が減った」のではなく、「防御層の構成が変わった」という認識である。問題は、この再構成が意図的に設計されていない点にある。したがって、ロボット配膳における食品防御は、従来型の管理発想をそのまま適用するのではなく、防御層の再配置・再設計を前提とした新たな理論枠組みを必要とする。

E. 結論

本研究は、飲食店において急速に普及しているロボット配膳システムについて、食品防御（Food Defense）の観点から現状の課題構造を整理し、安全確保に向けた方向性を検討したものである。

その結果、ロボット配膳システムは単なる業務効率化装置ではなく、食品搬送構造を「人が直接管理する形態」から「無人搬送を含む形態」へと転換させる技術であり、食品防御の前提条件を変化させる存在であることが明らかとなった。特に、以下の点が重要な知見として抽出された。

第一に、ロボット配膳は食品防御を弱体化させる可能性と、強化する可能性の両面を有するという二面性である。省人化のみを目的とし監視体制を縮小した場合には、無人搬送時間の増加や心理的抑止力の低下を招き、構造的脆弱性が生じる。一方で、配膳業務を自動化し人的資源を監視や顧客対応へ再配置する運用モデルを採用した場合には、むしろ防御機能を強化し得ることが確認された。

第二に、食品防御は単一対策では成立せず、多層防御構造として再設計する必要があることである。ロボット配膳環境においては、物理的防御層、人的防御層、心理的防御層、情報共有層を統合的に構築しなければならない。現状では、情報共有体制や設計段階での防御要件が十分に制度化されていない。

第三に、責任分散構造の存在である。販売代理店は食品管理を店舗責任と捉え、店舗は設計をメーカー責任と捉える傾向がある。この構造は食品防御対策の主体を曖昧にし、予防的対策の制度化を阻害する要因となっている。

以上を踏まえ、今後必要とされるのは以下の三つの方向性である。

1. ロボット配膳システムに特化した食品防御対策ガイドラインの策定
2. トラブル情報の体系的収集・共有プラットフォームの構築
3. 設計・販売・運用を横断した統合的責任枠組みの明確化

特に、導入店舗向けには「人的監視を前提とした運用モデル」を明示し、省人化と監視削減を同一視しない原則を提示する必要がある。また、海外メーカーを含めた設計段階への食品防御要件の反映も中長期的課題である。

ロボット配膳は今後さらに普及することが予想される。その普及を前提とすれば、問題発生後の対症療法ではなく、予防的・構造的対策の構築が不可欠である。本研究が示した最も重要な結論は、「ロボットはリスクではない。無設計な運用がリスクである。」という点である。

技術の進展とともに、食品防御もまた進化しなければならない。人とロボットの協働を前提とした新たな安全モデルの構築こそが、今後の飲食業界に求められる課題である。

F. 健康危機情報

なし

G. 研究発表

1. 論文発表

長田瑞花，多川優也，田崎ひなた，藤内琉成，今村知明，加藤礼識．飲食店における

食品防御対策の新たな課題「ロボット配膳システム」における食品防御対策の検討. 食品衛生研究（Food Sanitation Research),76 巻 1 号, 9-19 , 2026 年 01 月.

２. 学会発表

長田瑞花、加藤礼識、多川優也. 食品防御上の新たな問題（ロボット配膳システム）その①～販売代理店への聞き取り調査. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

長田瑞花、加藤礼識、多川優也. 食品防御上の新たな問題（ロボット配膳システム）その②～飲食店への聞き取り～. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

加藤礼識、長田瑞花、多川優也. 飲食物販売が多様化する中で食品防御対策はどのように変化したのか～大規模食品工場から小規模飲食店での対策への変化. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

加藤礼識、長田瑞花、多川優也. 小規模な飲食店舗における食品防御対策 「バイトテロ」・「客テロ」をどう防ぐべきなのか？. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

加藤礼識、長田瑞花、多川優也、平子ほほみ、神奈川芳行、今村知明. 多様化した飲食物販売における食品防御対策～これまでの食品防御対策の流れ～. 第 84 回日本公衆衛生学会総会. 2025 年 10 月. 静岡.

平子ほほみ、多川優也、長田瑞花、加藤礼識、高畑能久、神奈川芳行、今村知明. ロボット配膳システムにおける食品防御対策飲食店への聞き取り調査. 第 84 回日本公衆衛生学会総会. 2025 年 10 月. 静岡.

長田瑞花、加藤礼識、多川優也、平子ほほみ、神奈川芳行、今村知明. ロボット配膳システムにおける食品防御対策　販売代理店への聞き取り調査. 第 84 回日本公衆衛生学会総会. 2025 年 10 月. 静岡.

神奈川芳行、赤羽学、高畑能久、加藤礼識、入江芙美、山口健太郎、今村知明. 大規模イベントでの食品防御対策と食品防御対策ガイドライン英訳の意義. 第 84 回日本公衆衛生学会総会. 2025 年 10 月. 静岡.

H. 知的財産権の出願・登録状況

1.特許所得

なし

2.実用新案登録

なし

3.その他

なし

厚生労働科学研究費補助金（食品の安全確保推進研究事業）
「新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した
食品防御の推進のための研究」分担研究報告書（令和７年度）

食品工場における監視カメラ映像流出リスクの検討
― サイバー時代の食品防御の課題 ―

研究分担者　加藤　礼識　（茨城キリスト教大学　生活科学科　食物健康科学科　講師）
研究協力者　長田　瑞花　（奈良県立医科大学　公衆衛生学講座）
研究協力者　田崎ひなた　（茨城キリスト教大学　生活科学部　食物健康科学科）
研究協力者　藤内　琉成　（同志社大学 文学部 文化史学科）
研究協力者　永野　衣祝　（別府大学　食物栄養科学部　発酵食品学科）
研究協力者　多川　優也　（別府大学　大学院　食物栄養科学研究科）

研究要旨
本研究は、食品工場における監視カメラ映像データの流出を、単なる情報漏えいではなく、食品供給停止に連鎖し得る前段階リスクとして再定義することを目的とした。スマート化や生産集約の進展により、食品工場はネットワークと常時接続された環境へと変化し、映像の不正取得が内部構造の可視化を通じて物理的妨害や操業停止につながる可能性がある。国内外制度の比較、海外事例の整理、実務者ヒアリングを通じて、米国・EU では食品分野を重要インフラとして位置づけサイバー管理を制度に組み込む一方、日本では両者が分離して整理される傾向が確認された。監視カメラ映像データ流出は直ちに供給停止を招くものではないが、不正アクセスから操業停止、サプライチェーン波及へと連鎖する出発点となり得る。以上より、映像流出を軽微な情報問題ではなく戦略的リスクとして再評価し、食品防御を情報資産を含む統合的リスク管理へ再構築する必要性を提示した。

A．研究目的

近年、食品産業ではセントラルキッチン方式の広がりやスマート工場化の進展によって、生産の仕組みが大きく変化している状況にある。多くの工場で、生産が一か所に集められ、自動化が進み、効率よく大量に作る体制が整えられている。IoT 機器や遠隔監視システム、クラウド型の管理ソフト等が導入され、製造工程、温度管理、在庫管理、品質管理、そして監視カメラの映像までが、常にネットワークに常時接続された状態で管理されている。その結果、食品工場は単なる「物理的な作業の場」ではなく、現場とインターネット空間が結びついた新しい形のインフラへと変化している。

このような変化の中で、これまでの食品防御ではあまり考えられてこなかった問題として、本来、異物混入や不審者の侵入を防ぐための「守るための設備」として設置されている監視カメラの映像が不正に見られたり、外部に流出したりするリスクがあることが明らかになってきた。

しかし、現在の食品防御制度やガイドラインでは、監視カメラ映像のサイバー管理を食品防御の中心的な課題として整理したものは明確な位置づけがなされていない。特に中小規模の事業者では、サイバー対策が情報担当者に任され、食品防御とのつながりが弱いまま運用されている場合もある。

本分担研究では、監視カメラ映像の流出を食品防御上の重要なリスクとしてとらえ直し、サイバー食品防御の課題を明らかにすることを目的としている。具体的には、①流出が物理的な妨害や供給停止につながる流れの整理、②セントラルキッチン型施設におけるリスクの集中の検討、③サプライチェーン全体への影響の仕組みの整理、④実際に取り入れやすい技術的・制度的対策の提案を行う。

さらに、食品防御をこれまでの「物理的に守る対策」だけで考えるのではなく、ネットワーク上のリスクも含めて一体的に考える視点を示し、最終的には、食品の安定供給を守り、国民生活の安心につなげるための提案を行うことを目標とする。

B．研究方法

研究方法の基本的枠組み

研究全体は、①文献・制度分析、②海外基準との比較、③具体的事例の分析、④事業者へのヒアリング調査、⑤リスク構造モデルの構築、の五段階の流れで進めた。本研究では、食品工場における監視カメラ映像の流出が、食品防御にどのような影響を及ぼす可能性があるのかの問題を多角的に検討するため、制度分析

1．制度および規格の企画分析

本研究ではまず、食品防御およびサイバーセキュリティに関する国内外の制度や規格について、全体像を把握するための横断的な分析を行った。単に関連文献を整理するのではなく、「監視カメラの管理が制度の中でどのように位置づけられているのか」という具体的な視点から検討することを重視した。特に、監視カメラが食品防御の枠組みの中で明確に扱われているのか、それとも別の分野として分けて考えられているのかを確認することを目的とした。

分析対象としたのは、次のような国内外の制度・規格である。

- 国内の食品防御に関する通知や指針
- サイバーセキュリティに関する基本方針や関連文書
- IFS Food 規格
- 欧州の NIS2 指令
- 米国における食品関連のセキュリティ指針

これらを比較しながら、食品防御とサイバー対策がどのように整理されているのかを検討した。

分析にあたっては、いくつかの観点をあらかじめ設定した。具体的には、

- 食品防御の対象資産の中に、情報資産が含まれているか
- サイバー事故が発生した場合の報告義務が明確に定められているか
- 経営層の責任が制度上明文化されているか
- 工場内の制御系（OT）と事務系（IT）の分離が求められているか
- 監視カメラなどの監視設備について、具体的な管理要求が示されているか

等の点である。これらの観点をもとに比較することで、制度の中で監視カメラ管理がどのように扱われているのかを整理した。

その結果、海外の制度や規格では、監視設備や IoT 機器がリスク評価の対象として明確に含まれている場合が多く、サイバー対策と食品防御が一定程度結びつ

いていることが分かった。一方で、日本では依然として物理的な対策が中心となっており、監視カメラのサイバー管理については情報部門に任される傾向が強いことが確認された。このように、食品防御とサイバー対策の統合の程度には、国内外で差があることが明らかとなった。

2．海外事例の系統的検索

本研究では、食品産業におけるサイバー攻撃の事例や、監視カメラ等の IoT 機器に関連する問題を体系的に把握するため、海外で公開されている情報を対象とした系統的検索（systematic case review）を実施した。単に印象的な事例を集めるのではなく、同じ条件で再度検索すればおおよそ同様の結果が得られるように、あらかじめ検索範囲、選定基準、分析の視点を設定したうえで進めた。研究としての客観性と再確認可能性を確保することを意識した点が、本節の特徴である。

（1）検索対象

検索対象は、信頼性および検証可能性を確保する観点から、以下の情報源に限定した。

- 各国政府機関および規制当局の公式発表資料
- サイバーセキュリティ関連の公的機関による報告書
- 国際機関および標準化団体の公開文書
- 学術論文データベース（主に英語文献）
- 主要報道機関の記事（複数の報道で内容が確認できるもの）

一方で、個人ブログ、未確認の SNS 投稿、出所が明確でない技術フォーラムの情報については、信頼性を担保できないため除外した。食品防御は社会的影響の大きいテーマであり、政策的議論にも関わる内容であることから、情報の正確性を重視する必要があると判断したためである。

また、検索対象期間は直近 10 年間を基本とし、とくにランサムウェア被害が急増した 2018 年以降の事例を重点的に収集した。これは、食品工場のデジタル化やスマート工場化が進展した時期と重なるためであり、現代の製造環境に即した事例を中心に整理することを目的とした。こうした期間設定により、従来型の IT 障害ではなく、ネットワーク化が進んだ環境下での被害事例を把握することを目指した。

（2）検索キーワードおよび検索式

検索は主に英語で実施し、食品産業におけるサイバー攻撃や監視カメラ関連の事例を幅広く抽出できるよう、複数のキーワードを組み合わせて用いた。具体的には、以下の語を中心に検索を行った。

・“Food industry ransomware”
・“Food factory cyber attack”
・“Food manufacturing OT breach”
・“CCTV breach food plant”
・“Food supply chain disruption cyber”
・“IoT camera vulnerability factory”
・“SCADA attack food processing”

これらのキーワードは、単なる IT システムへの侵入事例だけに限定しないように設計した。食品工場では、事務系システムだけでなく、製造設備や制御系（OT）もネットワークに接続されている場合が多い。そのため、OT（Operational Technology）や SCADA、IoT カメラ、監視システムといった、食品工場特有の設備や技術に関連する語も含めることで、より実態に近い事例を把握できるように工夫した。

また、検索語は単独で使用するのではなく、いくつかを組み合わせることで、異なる視点から事例を抽出できるように

した。具体的には、

- 攻撃の種類（ransomware, breach, attack）
- 対象となる産業（food industry, food plant, food processing）
- 関係する技術領域（OT, SCADA, CCTV, IoT）

の三つの軸を意識して組み合わせた。これにより、食品産業におけるサイバー攻撃を、技術面・産業面・攻撃類型のそれぞれから網羅的に確認できるようにした。

検索は複数のデータベースや情報源を用いて実施し、同一の事例が異なる媒体で報告されている場合には内容を照合した上で統合した。さらに、使用した検索語や検索手順は記録し、研究の透明性と再現性を確保するよう努めた。

（3）選定基準および除外基準

検索によって抽出された事例の中から、本研究の目的に沿ったものを選ぶため、あらかじめ選定基準および除外基準を設定した。単に被害が大きい事例を取り上げるのではなく、「監視カメラを含むサイバーリスクが供給停止につながる可能性」という視点から整理することを重視した。

まず、分析対象として含める基準は以下のとおりである。

① 含める基準

- 食品の製造、加工、流通に直接関係している事案であること
- サイバー侵入により操業停止、出荷停止、物流の混乱などが実際に発生していること
- 侵入経路や被害の広がりについて、一定程度の情報が公開されていること
- 公的機関の発表、または複数の報道機関によって内容が確認できること

これらの条件を満たす事例を対象とすることで、単なる IT トラブルではなく、食品供給に影響を与えた事例に焦点を当てた。

一方で、以下のような事例は分析対象から除外した。

② 除外基準

- 小規模な店舗単独の被害であり、サプライチェーンへの波及が認められないもの
- 情報が不足しており、被害範囲や経過を十分に把握できないもの
- サイバー要因が明確ではなく、機器故障や自然災害など別の要因による障害の可能性が高いもの

これらを除外することで、本研究の中心課題である「供給停止リスク」との関連が明確な事例のみを抽出した。

以上のように、選定基準と除外基準をあらかじめ設定することで、分析対象の範囲を明確にし、研究の一貫性を保つようにした。

（4）分析枠組みおよび評価項目

抽出した各事例については、個別にばらばらに見るのではなく、同じ視点で比較できるように、あらかじめ設定した統一的な枠組みに基づいて分析を行った。これにより、食品産業におけるサイバー攻撃の共通点や特徴を整理し、監視カメラ流出との関連を検討できるようにした。主な分析項目は以下のとおりである。

① 初期侵入経路

まず、攻撃がどのような経路から始まったのかを整理した。具体的には、

・フィッシングメール
・VPN の脆弱性
・リモートデスクトップ設定の不備
・IoT 機器を経由した侵入
・サプライチェーンを通じた侵入

等の可能性を確認した。特に、本研究

のテーマである監視カメラやIoT機器が侵入口となった可能性があるかどうかを重点的に検討した。これにより、ネットワークにつながった設備がどの程度リスク要因となっているのかを把握しようとした。

② 権限拡大および横展開

次に、侵入後に攻撃者がどのように権限を拡大し、事務系システム（IT）から工場の制御系（OT）へと影響を広げたのかを整理した。食品工場では、製造制御系に影響が及ぶと操業停止に直結する場合が多いため、この段階は特に重要であると考えた。IT領域の問題がどのように現場の生産活動へつながったのかを意識しながら分析を行った。

③ 被害拡大要因

さらに、被害が広がった要因についても整理した。具体的には、

- 異常の発見が遅れたこと
- ログ監視体制が十分でなかったこと
- ネットワークが適切に分離されていなかったこと
- 更新プログラム（パッチ）が適用されていなかったこと
- サポートが終了した機器が使われ続けていたこと

等を確認した。これらの点については、ヒアリングで得られた現場の実態とも照らし合わせ、共通する弱点があるかどうかを検討した。

④ 操業停止および供給への波及

被害が操業停止や供給にどのように影響したのかも重要な分析項目とした。具体的には、

- 停止期間の長さ
- 影響を受けた拠点の数
- 出荷停止の範囲
- 学校給食、医療機関、外食産業などへの社会的影響

といった点を整理した。ここでは、単なるITトラブルとしてではなく、社会機能への波及という観点から事例を検討した。

⑤ 政策的対応

最後に、事案発生後に当該国で制度改正や報告義務の強化、ガイドラインの見直し等が行われたかを確認した。これにより、個別のインシデントが政策にどのような影響を与えたのかを把握し、今後の制度設計への示唆を検討した。

ここでの整理の意味

ここで行った海外事例の整理は、単に事例を紹介することが目的ではない。

- 監視カメラ映像の流出が、攻撃の準備に使われる可能性があるのかどうかを確認すること
- サイバー侵入から操業停止、さらに供給停止へと広がる流れを整理すること
- 日本の制度と比べたときに、どのような課題や空白があるのかを明らかにすること

を目的として実施した。

このように整理することで、監視カメラ映像データの流出を単なる情報漏えいの問題としてとらえるのではなく、食品供給の停止につながる可能性のあるリスクの出発点として考えるための土台をつくることを目指した。

C．研究結果

1．制度・規格分析の結果

本研究で行った国内外の制度および規格の比較分析から、食品防御の中でサイバーリスクがどのように位置づけられているかについて、国ごとに違いがあることが分かった。特に、「監視カメラなどの情報資産を食品防御の対象として明確に扱っているかどうか」という点で、大きな差が見られた。

（1）米国における位置づけ

米国では、食品産業は重要インフラの一つとして明確に位置づけられている。U.S. Food and Drug Administration（FDA）が所管する食品安全強化法（FSMA）では、意図的な混入を防ぐための対策（Food Defense Rule）が義務化されており、事業者には脆弱性評価の実施や防御計画の策定が求められている。

さらに、Cybersecurity and Infrastructure Security Agency（CISA）は、食品・農業分野を重要インフラ部門の一つとして位置づけ、OT セキュリティやランサムウェア対策に関するガイドラインを公表している。これらの文書では、ネットワークに接続された機器や遠隔監視装置、IoT 機器が攻撃経路となる可能性についても言及されており、製造現場のデジタル機器がリスク要因となり得ることが示されている。

このように、米国では食品防御とサイバーセキュリティが別々に扱われるのではなく、重要インフラを守るという大きな枠組みの中で一体的に考えられている点が特徴である。

（2）欧州連合（EU）における位置づけ

EU では、NIS2 Directive の施行により、重要分野に対するサイバーリスク管理と重大インシデントの報告義務が強化された。食品の製造や加工もその対象分野に含まれており、事業者にはリスク管理措置の実施が求められている。また、経営層の責任を明確にすることや、重大な事故が発生した場合には原則として 24 時間以内に報告することなども定められている。

さらに、International Featured Standards（IFS）の Food 規格においては、フードディフェンスに関するリスク評価の実施が求められている。この中では、アクセス管理や監視設備の適切な運用も監査の対象となっている。IFS は法律ではないものの、欧州の流通市場では事実上の取引条件となる場合が多く、実質的な拘束力を持つ基準として機能している。

特に、監視カメラなどの設備についてもリスク評価の対象に含めることが求められており、映像データの管理やアクセス制御の仕組みも確認事項となっている点が特徴である。つまり、単に物理的な防御だけでなく、情報の管理も含めて食品防御を考える姿勢が制度の中に組み込まれている。

EU の大きな特徴は、個別の企業対策だけでなく、サプライチェーン全体を視野に入れたリスク管理を制度として求めている点にある。これにより、食品産業におけるサイバーリスクが、より広い社会的視点から位置づけられていると考えられる。

（3）制度構造の比較

以上の分析結果を表 1 に整理した。表 1 では、日本、米国、EU における食品防御とサイバーセキュリティの制度上の位置づけを、複数の視点から比較している。

表 1 から明らかなように、米国および EU では、食品産業を重要分野として明確に位置づけ、その枠組みの中にサイバーリスク管理を組み込んでいる。サイバー事故の報告義務や経営層責任が制度上明確に示されており、ネットワーク接続機器や OT 機器もリスク管理の対象として整理されている。これに対し、日本では食品防御は主として物理的対策を中心に構成されており、サイバーセキュリティは情報分野の政策として別に扱われる傾向がある。その結果、監視カメラのように物理設備でありながらネットワークに接続されている機器について、食品防御の枠組みの中でどのように管理するのかが必ずしも明確ではない。

また、EU ではサプライチェーン全体を視野に入れたリスク管理が制度として求められているのに対し、日本では個別事業者単位の対策にとどまる傾向が存在することも、比較から読み取ることができる。

以上のことから、日本では食品防御とサイバーセキュリティが制度上十分に統合されているとは言い難く、両者が分かれて運用されている構造があると考えられる。表 1 は、その構造的な違いを整理したものである。

表 1　食品防御とサイバーリスク管理に関する制度比較（米国・EU・日本）

比較項目	米国	EU	日本
食品産業の制度的位置づけ	重要インフラ部門（Food and Agriculture Sector）として明示	NIS2 により essential entities として指定	重要インフラとしての明確な法的指定はなし
サイバー事故の報告義務	CIRCIA 等に基づく報告義務あり	NIS2 により原則 24 時間以内の報告義務	分野横断的な報告制度は存在するが、食品防御と直接結びついた義務規定は限定的
経営層の責任	重要インフラ保護政策の枠組みで明示	NIS2 により経営層責任を法令上明確化	食品防御分野での経営層責任の明文化は限定的
OT・制御系管理	OT セキュリティ指針を公表し管理対象として明示	リスク管理措置義務に OT を含む	OT を食品防御対象として明示的に整理した規定は少ない
監視設備・IoT 機器の位置づけ	リスク評価対象として位置づけ	監査・リスク評価対象に含まれる	主に防犯設備・個人情報管理の文脈で扱われる傾向

また、EU ではサプライチェーン全体を視野に入れたリスク管理が制度として求められているのに対し、日本では個別事業者単位の対策にとどまる傾向があることも、比較から読み取ることができる。

以上のことから、日本では食品防御とサイバーセキュリティが制度上十分に統合されているとは言い難く、両者が分かれて運用されている構造があると考えられる。表 1 は、その構造的な違いを整理したものである。

（4）監視カメラの制度的位置づけ

制度分析の結果、海外の制度では、監視カメラや IoT 機器が「侵入経路」や「重要な情報資産」として明示的にリスク評価の対象に含まれている傾向が存在することが分かった。つまり、これらの機器は単なる設備ではなく、攻撃の入り口になり得るものとして位置づけられている。

一方で、日本では監視カメラは主に防犯設備として扱われることが多く、食品

防御計画の中で「情報資産」として明確に整理されている例はあまり多くない。ネットワークにつながっている場合であっても、その管理は情報部門の業務とされ、食品防御の枠組みの中で十分に検討されていない可能性が存在する。

この違いは、監視カメラ映像の流出をどのように捉えるかという考え方の違いに関係していると考えられる。海外では、映像の流出を将来的な攻撃や妨害の準備につながるリスクとして捉える視点が確認されるのに対し、日本では個人情報の問題として整理される傾向が強い。

つまり、監視カメラ映像流出を「単なる情報漏えい」として扱うのか、それとも「供給停止につながる可能性のある前段階のリスク」として位置づけるのかという概念上の違いが、制度の整理の仕方にも表れていると考えられる。

(5) 制度的空白の抽出

以上の制度比較の結果から、日本における制度上の課題、いわば「空白」と考えられる点は、主に三つに整理することができた。

第一に、食品防御の中で「情報資産」がどのように位置づけられるのかが明確ではない点である。現在の制度では、物理的な設備や人の出入りに関する対策は比較的整理されているが、監視カメラの映像データやネットワーク機器といった情報に関わる資産について、食品防御の対象として明確に定義されているとは言い難い。

第二に、サイバー事故に関する統一的な報告制度が十分に整備されていない点である。サイバーセキュリティに関する報告の仕組みは存在するものの、それが食品防御の文脈と結びついているわけではなく、食品供給への影響という観点から整理されているとは限らない。そのため、事案が起きた場合でも、食品防御の課題として横断的に共有されにくい可能性が存在する。

第三に、経営層の責任やBCP（事業継続計画）との連動が制度上十分に明示されていない点である。海外では、経営層がリスク管理に直接責任を持つことや、重大事故の報告義務が明確に示されている場合が多いが、日本ではその位置づけが比較的弱いと考えられる。

これらの要素が重なることで、たとえ監視カメラ映像の流出事案が発生したとしても、それが食品防御の問題として体系的に整理され、再発防止策が制度的に議論される仕組みが十分に機能しにくい構造が生まれている可能性が指摘される。

D. 考察

1. 食品防御の考え方は変わりつつある — 物理防御からサイバー・フィジカル統合防御へ

本研究の結果から、食品防御の考え方は今まさに転換点にあると考えられる。これまで食品防御は、意図的な異物混入や不審者の侵入、内部不正といった物理的な脅威を中心に想定してきた。そのため、入退室管理、施錠管理、監視カメラの設置、重要区域へのアクセス制限などの対策が主な柱となっていた。これらの取り組みは一定の抑止効果を持ち、食品安全の維持に貢献してきたことは間違い

ない。

しかし現在では、スマート工場化の進展やIoT機器の普及、クラウド型管理システムの導入により、食品工場の環境は大きく変化している。監視カメラ、温度管理装置、在庫管理システム、製造制御系（OT）等がネットワークを通じて接続され、情報と現場が常時つながっている状態が一般的になっている。このような状況では、物理的防御と情報セキュリティを分けてとらえる枠組みでは十分に対応できず、新たなリスクの把握と評価が求められる。

特に監視カメラは、その変化を象徴する存在である。本来は工場を守るための設備として設置されてきたが、ネットワーク接続型のIPカメラが普及したことで、外部からの不正アクセスの対象にもなり得るようになった。もし映像が流出した場合、それは単なるプライバシー侵害や企業秘密の漏えいにとどまらない可能性が存在する。工場内部のレイアウト、重要管理点（CCP）の位置、警備の死角、従業員の動き方等が外部に知られてしまえば、それらは物理的侵入や妨害行為の成功率を高める情報となり得る。

ここに、食品防御の大きな矛盾がある。守るために設置された設備が、管理の不備によっては攻撃を助ける情報源になってしまう可能性があるという点である。これまで暗黙のうちに前提とされてきた「防御設備は安全側に働く」という考え方は、ネットワーク化が進んだ現在では必ずしも成り立たない。この認識の変化は、食品防御の考え方そのものを見直す必要があることを示している。

さらに、セントラルキッチン型施設や集約型の生産拠点では、一つの工場が停止することの影響が非常に大きい。サイバー侵入によって得られた情報が物理的な妨害と結びつけば、製造停止から出荷停止へと影響が広がり、学校給食や医療機関、外食産業など、社会の基盤となる分野にまで波及する可能性が存在する。その意味で、監視カメラ映像の流出は単なる情報管理の問題ではなく、食品供給全体の安定性に関わる問題として考える必要がある。

以上のことから、食品防御は単なる「物理的侵入を防ぐ対策の集まり」ではなく、情報資産を含めた統合的なリスク管理の考え方へと再構築されるべきであると考えられる。物理的対策、サイバー対策、日常的な運用管理、そして経営レベルでの責任体制を一体として捉える「サイバー・フィジカル統合防御」の視点が求められている。

この統合的な考え方のもとでは、①情報資産を明確に定義すること、②ITとOTを適切に分けて管理すること、③ログ管理や異常検知体制を整えること、④経営層がリスクを把握し責任を持つこと、⑤事業継続計画（BCP）と連動させること、などが重要になる。とくに重要なのは、食品防御を情報部門だけの課題とせず、経営全体の問題として位置づけることである。

本研究の最大の示唆は、監視カメラ映像の流出という一見周辺的に見える出来事が、食品供給停止という重大なリスクの出発点になり得るという点である。このような認識の転換こそが、食品防御の

考え方を次の段階へ進めるための第一歩になると考えられる。

今後は、物理空間とサイバー空間を切り離して考えるのではなく、両者がつながっていることを前提とした防御設計が必要になる。食品産業が高度にデジタル化している現在、食品防御の再定義は避けて通れない課題である。

2. 制度分断と責任のあいまいさ

本研究の制度分析およびヒアリング結果から見えてきた大きな課題の一つは、食品防御とサイバーセキュリティが制度上、また組織上で分かれて扱われていることである。日本では、食品防御は主に品質管理部門や安全管理部門が担当し、異物混入対策や入退室管理など、物理的な対策が中心となっている。一方で、サイバーセキュリティは情報システム部門の業務とされ、ネットワーク管理や情報漏えい対策として整理されることが多い。

このような分かれ方は、監視カメラの管理において特に分かりやすく表れている。監視カメラは防犯設備として導入されることが多く、設置や保守は設備管理部門や外部の警備会社が担当する場合がある。しかし実際には、映像データはネットワークを通じて保存・閲覧されるため、情報資産としての性質も持っている。このような二つの側面を持つにもかかわらず、食品防御計画の中で監視カメラ映像が「重要な情報資産」として明確に位置づけられていない場合、誰が最終的に責任を持つのかがあいまいになりやすい。

責任のあいまいさは、実際に事故が発生したときに表面化する。たとえば、監視カメラ映像が外部に流出した場合、それを情報漏えい事故として扱うのか、食品防御上の重大な問題として扱うのか、あるいは設備管理上の不備として整理するのかがはっきりしないことがある。その結果、原因の分析や再発防止策が部門ごとに分かれてしまい、組織全体としての見直しにつながらない可能性が存在する。

さらに、現行制度では経営層の責任が明確に示されていない場合も多く、リスク管理が現場レベルに任されやすい傾向が確認された。サイバー対策は「IT 部門の問題」、食品防御は「現場の問題」と受け止められ、経営レベルで統合的に議論されない構造が問題として指摘される。このような状況では、セントラルキッチンのように一拠点の停止が広い範囲に影響を及ぼす施設において、供給停止リスクを全体として評価することは難しい。

海外では、重要インフラを守るという枠組みの中でサイバーリスクが経営課題として位置づけられ、インシデントの報告義務や経営層の責任が明確に示されている例が多い。それに比べると、日本では食品防御とサイバーセキュリティを統合して考える仕組みがまだ十分に整っていない可能性があることが、本研究から示唆された。

したがって、食品防御を実効性のあるものとするためには、監視カメラを含む情報資産を明確に食品防御の対象として位置づけ、責任の所在を経営レベルまで引き上げる制度設計が必要である。部門

ごとに分かれた構造を見直すことが、サイバーと物理の両面を含めた統合的な防御へ進むための第一歩になると考えられる。

3. 監視カメラ流出と供給停止リスクのつながり

本研究で整理したリスクの流れから分かったのは、監視カメラ映像の流出がそれだけで直ちに大きな被害を生むというよりも、段階を経て供給停止につながる可能性があるという点である。つまり、流出は単独の出来事ではなく、その後の事態を引き起こす出発点になり得る。

第一段階は、不正アクセスの発生である。初期パスワードが変更されていない、推測しやすい認証情報が使われている、ネットワークが十分に分けられていないといった基本的な管理の不備が侵入口となる。この段階では、まだ大きな被害が表面化していないことも多い。

第二段階では、攻撃者が監視カメラの映像データを取得し、工場内部の状況を把握する。ここで得られる情報には、製造ラインの配置、原材料の保管場所、重要管理点（CCP）の位置、警備体制の死角、従業員の動き方などが含まれる可能性がある。これらは、物理的な侵入や妨害を計画する際の基礎情報になり得る。

第三段階では、取得された情報をもとに、実際の物理的妨害や意図的な侵入が試みられる可能性が出てくる。必ずしもすぐに攻撃が行われるとは限らないが、成功の可能性は高まると考えられる。特に、警備体制の弱点が明らかになっている場合には、抑止効果が弱まるおそれがある。

第四段階では、製造ラインの停止や操業停止が発生する可能性が確認された。たとえ実際に異物混入や設備破壊が起きなくても、脅威の存在が明らかになった場合や風評が広がった場合には、自主的に操業を停止する判断が取られることもある。食品産業では信頼が非常に重要であるため、少しでも疑いが生じれば出荷停止措置が選択される可能性が高い。

最終段階では、その影響がサプライチェーン全体へと拡大する。セントラルキッチン型の施設では、一つの拠点が多数の施設に供給していることが多いため、学校給食、医療機関、外食チェーンなどに広い範囲で影響が及ぶ。供給の遅れや代替調達の難しさは、地域社会の機能にも直接的な影響を与える可能性がある。

この連鎖の重要な点は、監視カメラ映像の流出そのものが直ちに供給停止を引き起こすわけではないということである。しかし、それが供給停止リスクの前段階として位置づけられることで、問題の見え方は大きく変わる。これまで「情報漏えい問題」として比較的限定的に扱われてきた事象が、実際にはサイバーと物理が結びついた複合的なリスクの出発点となる可能性が確認された。

もしこうした弱点から監視カメラの映像が外部に流出した場合、その問題は単なる個人情報の流出では終わらない可能性がある。工場内の映像には、

- 製造ラインの配置
- 原材料の保管場所
- 重要管理点（CCP）の位置
- 警備の死角

・従業員の動き方
・出入口の施錠の様子

など、食品防御にとってとても重要な情報が映っている。これらの情報が第三者に知られてしまえば、工場に侵入したり、わざと妨害をしたりする際に役立つ情報となってしまう。つまり、守るために設置した監視カメラが流出してしまえば「攻撃を支援する情報資産」になってしまうなど、矛盾した状況が起こり得る。

さらに、監視映像がSNSやインターネット上に拡散した場合、企業の信用は大きく傷つく可能性がある。取引先からの信頼を失い、出荷が止まり、行政からの指導を受け、消費者の不安が拡大することも考えられる。特にセントラルキッチンや大規模な製造拠点では、一つの工場が停止すると、多くの学校給食、医療機関、外食チェーン等の食品供給体制に影響が生じる。風評と実際の操業停止が重なれば、供給そのものが止まってしまう可能性もある。これは企業だけの問題ではなく、地域社会全体に関わる問題である。

したがって、監視カメラの流出は軽いセキュリティ事案として扱うべきではなく、食品供給の安定性に影響し得る潜在的な危機として評価する必要がある。このような認識の変化が、統合的な食品防御の考え方を進めるための重要な一歩になると考えられる。

実際に、2025年にはアサヒグループホールディングスがランサムウェア攻撃を受け、受注や出荷のシステムが止まり、出荷業務及び供給体制に混乱が生じた。また2021年にはJBSが攻撃を受け、複数の工場が操業停止に追い込まれた。これらは主に基幹システムへの攻撃であったが、もし事前に工場内部の映像や情報が漏れていれば、サイバー攻撃と物理的な妨害が組み合わさる可能性もあったと考えられる。今後は、ネット上の攻撃と現場での妨害が同時に起こるような事態も現実的になっていくと予想される。

4. 現場で見えてきた弱点と運用の課題

ヒアリングや事例分析を通して感じたのは、食品工場におけるサイバーリスクの多くが、必ずしも高度な技術不足によるものではなく、日々の運用の積み重ねに関わる問題である。監視カメラの導入時には、仮パスワードの設定や基本的なセキュリティ対策が行われていることが多い。しかし、その後の運用の中で、パスワードが変更されないまま使われ続けたり、アクセス権限の見直しが行われなかったり、ログの確認が習慣化していなかったりする状況が見られた。

このように、最初は整えられていた対策が、時間の経過とともに形だけになってしまう構造があると感じられた。特に監視カメラは、防犯設備として導入されることが多いため、情報セキュリティの枠組みの中で継続的に管理されない場合が存在する。設備管理部門と情報システム部門の連携が十分でない場合には、ネットワーク機器としてのリスク評価が後回しになり、ソフトウェアの更新や脆弱性への対応が遅れる可能性が指摘される。

また、サポートが終了した機器がその

まま使われ続けている例も確認された。これはすぐに問題が起こるわけではないが、長い目で見るとリスクが積み重なっていく可能性がある。現場では「今は問題が起きていないから大丈夫」等の感覚が働きやすいが、その状態が続くこと自体が弱点になることもあると考えられる。

さらに、侵入検知システムの導入やネットワークを分けるといった高度な対策は、技術的には可能であっても、最終的な判断は事業者に委ねられている。特に中小規模の事業者では、専門人材の不足やコスト面の負担が大きく、最低限の対策にとどまる場合も多い。その結果、ガイドラインで示されている対策が「理想」として理解されるにとどまり、実際の運用に十分に反映されないこともある。

こうした状況から、本研究では食品防御の課題は単に技術の問題ではなく、組織としてどのように管理し続けるか等の運用の問題でもあると考えた。新しい機器を導入することよりも、それをどう使い続け、どう見直し、誰が責任を持つのかを明確にすることの方が重要な場合もある。

特に、監視カメラを含む IoT 機器を食品防御の重要な資産として明確に位置づけ、組織の中で管理責任をはっきりさせることが必要であると感じた。責任があいまいなままでは、問題が起きたときに「どこが対応すべきか」が分からず、対策が後手に回る可能性が存在する。

運用体制を強化するためには、①誰が最終的に責任を持つのかを明確にすること、②定期的に見直しや点検を行う仕組みをつくること、③従業員への教育や訓練を継続すること、④事業継続計画（BCP）と結びつけて考えること、などが重要になると考えられる。

監視カメラの流出を単なる情報漏えいとして扱うのではなく、供給停止につながる可能性のある出来事として認識することが、組織全体の意識を変えるきっかけになるのではないかと思われる。

このように、実務上の弱点は高度な技術を導入するだけで解決するものではなく、日々の運用と組織全体の考え方の見直しによって、はじめて改善されていくものだと考えられる。

5. 経済安全保障とのつながり

食品の安定供給は、日常生活を支える基本的な条件であり、その意味で経済安全保障とも深く関わっている。近年では、サプライチェーンの強化や重要物資の安定供給が政策課題として取り上げられているが、サイバー攻撃によって供給が止まる可能性についても、同じように考える必要があるのではないかと示唆される。

食品工場のスマート化や集約化は、生産効率を高めるという点で大きな利点がある。しかしその一方で、生産拠点が集まることで、ひとつの工場が止まった場合の影響が大きくなるという側面もある。セントラルキッチン型の施設では、一つの拠点が多数の学校や医療機関、外食チェーンなどに供給していることも少なくない。そのため、操業停止が起きた場合、企業内部の問題にとどまらず、地

域社会全体に影響が及ぶ可能性がある。

監視カメラの映像が流出し、攻撃の準備情報として利用された場合、被害は単なる情報漏えいでは終わらない可能性がある。操業停止や出荷停止が起きれば、学校給食が提供できなくなる、医療機関への食事供給が滞るといった事態も想定される。このような影響は、特に子どもや高齢者など、支援を必要とする人々に直接的に及ぶ可能性があるため、その社会的な影響は小さくない。

また、サイバー攻撃は国境を越えて実行されることが多く、個別企業だけで対応するには限界がある。監視カメラやIoT機器の弱点は、一つの企業の問題というよりも、社会全体の仕組みに関わる課題とも言える。供給停止が広がれば、消費者の不安や価格の変動、流通の混乱など、経済全体にも波及する可能性が存在する。

こうした点を考えると、食品防御は企業の内部管理の問題にとどまらず、より広い政策的視点ともつながっていると考えられる。監視カメラ映像データ流出のように一見限定的に見える出来事も、サイバーと物理が結びついた複合的なリスクの前段階として捉えることで、その重要性がよりはっきりする。

食品防御を見直すことは、単に技術を強化することではなく、社会全体の安定性をどう守るかという問いにもつながっている。経済安全保障という視点と結びつけて考えることによって、食品供給のレジリエンスを高めるための議論がより具体的になるのではないかと考えられる。

E. 結論

本研究では、食品工場における監視カメラ映像の流出という事象を手がかりに、サイバーリスクが食品防御にどのような影響を与え得るのかを検討した。制度分析、海外事例の整理、ヒアリング調査、リスク連鎖の検討を通して、監視カメラ流出は単なる情報漏えいにとどまらず、供給停止につながる可能性を持つ前段階の出来事として位置づけられることが明らかとなった。

従来の食品防御は、物理的な侵入や意図的な混入を防ぐことを中心に構築されてきた。しかし、食品工場がネットワークと密接につながる現在では、情報の流出が物理的な脅威へと結びつく可能性がある。監視カメラはその象徴的な例であり、本来は守るための設備であるにもかかわらず、管理が不十分な場合には工場内部の情報を外部に伝えてしまう可能性が指摘される。この点は、食品防御の考え方を見直す必要性を示している。

制度比較の結果からは、海外では食品防御とサイバーセキュリティを統合的に扱う傾向が見られる一方、日本では両者が分かれて整理されている側面があることが分かった。特に、監視カメラのように物理設備でありながら情報資産でもあるものについて、責任の所在があいまいになりやすい構造が存在している可能性が示唆された。

また、リスク連鎖の整理からは、監視カメラ映像データ流出が直ちに供給停止を引き起こすわけではないものの、不正アクセス、情報取得、物理的妨害、操業停止、そしてサプライチェーンへの波及

という流れの中で、重要な出発点になり得ることが確認された。とくにセントラルキッチン型施設では、その影響が広範囲に及ぶ可能性がある。

さらに、ヒアリング結果からは、技術そのものよりも、日常的な運用や部門間の連携、責任の明確化といった組織的な課題が大きいことが分かった。食品防御は単なる技術対策ではなく、組織全体でどのようにリスクを管理するかという問題でもある。

以上のことから、本研究は、食品防御を物理的対策に限定せず、サイバー領域を含めた統合的な視点で再構築する必要性を示した。監視カメラ映像流出という一見限定的な問題も、食品供給の安定性というより大きな課題と結びついている可能性が指摘される。

今後は、情報資産の明確な位置づけ、責任体制の整理、制度面での統合的な枠組みの検討などが求められる。本研究はその基礎的な整理を行った段階にとどまるが、食品防御の新しい方向性を考えるための一つの視点を提示できたのではないかと考えられる。

F. 健康危機情報

なし

G. 研究発表

1. 論文発表

長田瑞花, 多川優也 , 田崎ひなた, 藤内琉成 , 今村知明, 加藤礼識. 飲食店における食品防御対策の新たな課題「ロボット配膳システム」における食品防御対策の検討. 食品衛生研究（Food Sanitation Research),76 巻 1 号, 9-19 , 2026 年 01 月.

2. 学会発表

長田瑞花、加藤礼識、多川優也. 食品防御上の新たな問題（ロボット配膳システム）その①～販売代理店への聞き取り調査. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

長田瑞花、加藤礼識、多川優也. 食品防御上の新たな問題（ロボット配膳システム）その②～飲食店への聞き取り～. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

加藤礼識、長田瑞花、多川優也. 飲食物販売が多様化する中で食品防御対策はどのように変化したのか～大規模食品工場から小規模飲食店での対策への変化. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

加藤礼識、長田瑞花、多川優也. 小規模な飲食店舗における食品防御対策 「バイトテロ」・「客テロ」をどう防ぐべきなのか？. 第 121 回日本食品衛生学会・学術講演会. 2025 年 10 月. 東京.

加藤礼識、長田瑞花、多川優也、平子ほほみ、神奈川芳行、今村知明. 多様化した飲食物販売における食品防御対策～これまでの食品防御対策の流れ～. 第 84 回日本公衆衛生学会総会. 2025 年 10 月. 静岡.

平子ほほみ、多川優也、長田瑞花、加藤礼識、高畑能久、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　飲食店への聞き取り調査．第84回日本公衆衛生学会総会．2025年10月. 静岡.

長田瑞花、加藤礼識、多川優也、平子ほほみ、神奈川芳行、今村知明．ロボット配膳システムにおける食品防御対策　販売代理店への聞き取り調査．第84回日本公衆衛生学会総会．2025年10月. 静岡.

神奈川芳行、赤羽学、高畑能久、加藤礼識、入江芙美、山口健太郎、今村知明．大規模イベントでの食品防御対策と食品防御対策ガイドライン英訳の意義．第84回日本公衆衛生学会総会．2025年10月. 静岡.

H．知的財産権の出願・登録状況

1.特許所得

　なし

2.実用新案登録

　なし

3.その他

　なし

厚生労働科学研究費補助金(食品の安全確保推進研究事業)
「新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した
食品防御の推進のための研究」
分担研究報告書（令和 7 年度）

地方自治体食品衛生行政における食品防御対策の課題検討

研究分担者　岡部　信彦　（川崎市健康安全研究所）
協力研究者　赤星　千絵　（川崎市健康安全研究所）
相原　俊介　（川崎市健康福祉局保健医療政策部生活衛生課）
浅井　威一郎　（川崎市健康安全研究所）
三亀　美津穂　（川崎市健康安全研究所）

研究要旨
地方自治体食品衛生行政では、市民の食の安全・安心を確保するため食品関係法に基づき行政機関による指導・監督等が行われている。食品防御対策については、事案発生後（発覚後）の危害拡大防止や食中毒の原因究明等は既存の規定で対応可能と考えられるが、意図的な異物混入の防止等、食品防御で必要となる意図的な行為に対しての未然防止策の規定はない。そこで、食品衛生行政機関が担うべき役割と適度で効果的な対策方法を検討するため、以下の 2 種類の実態調査を行った。
・他自治体における食品防御対策の状況調査（アンケート調査）
・食品防御に関連する相談の実態調査（苦情相談対応データベースの解析）
実態調査から、有事対応の状況や未然防止対応の状況が推察できた。実態調査結果から推察された地方自治体食品衛生行政における状況を踏まえ、食品防御対策につながる対応を取り入れやすいよう教育訓練の内容について次年度検討する予定である。

A．研究目的

食品テロ等の意図的な毒物等混入による食中毒事件は、食品衛生上の問題による食中毒事件に比べ発生頻度は非常に少ないが、食の安全・安心に与える悪影響は大きい。食品防御対策はこれまで主に国とフードチェーンにおける事業者等の自主的な取り組みにより進められてきているが、フードチェーンと地方自治体の保健所等の行政機関との連携も重要であり、連携して対策を強化することで事件発生の抑止及び発生後の拡大防止につながる。

平成 27-29 年度厚生労働科学研究「行政機関や食品企業における食品防御の具体的な対策に関する研究」（研究代表者：今村知明）分担研究「食品への毒物等混入事件時における保健所や行政機関における円滑な事件処理に向けての検討」（研究分担者：高谷幸）において、行政機関における食品防御対策として、発生後の対応については各自治体で体制整備が進められている一方で、未然防止に係る対応については、事業者の自主的な取組みを推進するため、具体的な対応方法をわかりやすく提示していくことが必要とされていた。この対策に関する現状について、令和 3-5 年度厚生労働科学研究「新型コロナウィルス感染症対策に取組む食品事業者における食品防御の推進のための研

究」（研究代表者：今村知明）分担研究「新興感染症流行時における地方自治体の食品防御対策の検討」（以下、先行研究）において実態調査を行った結果、未然防止の食品防御対策に関しては所管が不明瞭な自治体が多いと考えられ、そのような中でも食品衛生監視員は、食品事業者等からの食品防御対策に関する相談に対応することがあることがわかった。そのため、食品事業者等の身近な相談窓口として食品衛生行政機関が担うべき役割が明確化され、食品衛生監視員の知識向上を図る必要があると思われた。そこで、本研究では先行研究を踏まえ、食品衛生行政機関の食品防御対策への関わり方をさらに具体的に検討し、担うべき役割を検討することを目的とした。

B．研究方法

本研究における検討のため、研究協力者間の対面での打ち合わせを 3 回及びメール会議を随時実施し、昨年度に引き続き以下の 2 点を実施した。

１．実態調査

（調査 1）他自治体における食品防御対策の状況調査

以下のアンケート調査を実施した。

- 対象：関東甲信越静ブロックに属する各都県市・特別区の食品衛生主管課
- 実施時期：2025 年 11 月
- 方法：対象にメールで案内を送付し、設問内容（別添 1）に回答を記載するか、同様の設問内容について LoGo フォームに回答を入力するよう依頼した。
- 結果還元：対象に集計結果をメールで送付した。

（調査 2）食品防御に関連する相談の実態調査

保健所の食品衛生監視員が受けた相談のうち、事業者からの対策相談や食品への意図的な混入事例相談の割合を調べるため、2020 年～2024 年に川崎市の保健情報システムに記録された苦情相談対応のデータベースを解析した。

２．教育訓練や食品防御対策の内容検討

昨年度確認した以下の検討スタンスを念頭に、取り入れやすい教育訓練や対策について、今年度から来年度にかけて具体的に検討する。

【検討スタンス】食品衛生対策とのバランスや保健所の状況を踏まえ、食品防御の視点に偏らないように、かつ、防御的案件が懸念される場合に適切な対応が取れるように、食品衛生対策の中に食品防御の視点を適度に加えていく。

（倫理面への配慮）

本研究において、特定の研究対象者は存在せず、倫理面への配慮は不要である。

C．研究結果

１．実態調査

（調査 1）他自治体における食品防御対策の状況調査

食品衛生行政における食品防御対策の実態調査のため、アンケート調査を実施し集計結果（別添 2）から判明したことを以下に示す。

- 食品防御対策について事務分掌に「含む」と回答した自治体は 56 自治体中 8 自治体（14%）であったが、その自治体の公表されている事務分掌を調べたところ明文化はされてはいなかったため、含むと解釈している状況と思われた。また、「その他」と回答した自治体のうち 10 自治体は”明文化されていないが可能な範囲で対応している”状況であった。以上のことから、56 自治体中 18 自治体（32%）の食品衛生所管課は、食品防御対策についても業務上可能な範囲で対応していると思われた。
- イベント開催における予防的な対応として、1 自治体から食品防御対策について普及啓発しているとの記載があった。
- 2024 年度に事業者等からの相談対応の中で、食品防御的な視点から助言を行った経験あり（「ある」「あると思う」の回答を集計）の自治体は、56 自治体中 18 自治体（32%）

であり、事業者等から食品防御対策に関する相談は約 9 割が対応経験なし（「ない」「ないと思う」の回答を集計）の状況の中、助言を通して食品防御対策を推進している自治体があることがわかった。

・2022～2024 年の意図的な混入による汚染食品が原因と考えられる食中毒事例の経験については、2 自治体から経験「あり」と回答があった。うち 1 事例は意図的な混入が確認されていた事例であり、指導内容に苦慮していた。もう 1 事例は「意図的な混入の不安がある相談があり警察の管轄であると説明しているが理解を得るのが困難」と苦慮していた。

・2022～2024 年の混入原因が不明な化学物質による汚染食品が原因と考えられる食中毒事例の経験については、2 自治体が経験「あり」と回答があった。1 事例は混入経路が不明で再発防止策の助言に苦慮していた。もう 1 事例では保健所より先に事情聴取していた警察と情報共有しており、警察が証拠品を押収して残品で検査ができなかったこと及び同様事例の際に地方衛生研究所での検査対応不可の可能性に苦慮していた。

（調査 2）食品防御に関連する相談の実態調査

川崎市の保健情報システム WEL-MOTHER の苦情相談対応のデータベースは、川崎市保健所の食品衛生監視員が苦情相談を受けた際に記録するために備えられている様式であるが、記録すべき内容の明確な基準がないため、各所属の食品衛生担当係長への聞き取り調査によると、以下の 2 点の制限がある。①市民・営業者・後任の職員にとって有益な記録は必ず残すようにしているが、一般的な質問及び回答は記録しないことが多い。②一部の食中毒を疑う案件では、別の様式で記録し、このデータベースに記録していない所属もある。

本データベースを解析した結果を表 1 に示す。2020 年～2024 年に 11,689 件の相談内容が登録されていた。この中から食品防御対策

表1. 川崎市保健所の苦情相談記録件数

受付日（年）	2020	2021	2022	2023	2024	計
苦情相談記録件数	1994	2201	2160	2724	2610	11689
キーワード入り苦情件数※	245	198	239	293	293	1268

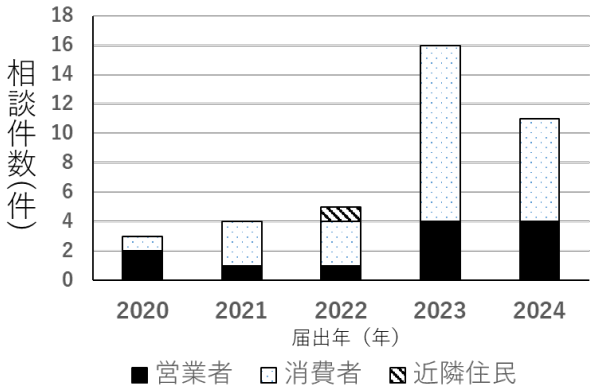
※キーワード：経緯が別記録で不明のものを含む。キーワード内訳は表2参照。

表2. 検索に使用したキーワードと該当件数

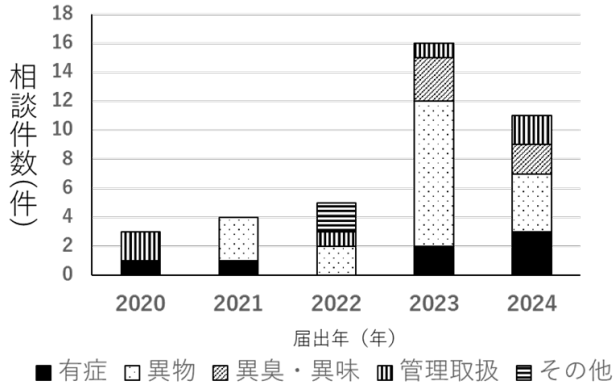
キーワード	該当件数
混入	499
意図的	0
警察	121
事件性	2
犯罪	0
悪意	2
特異	1
毒物	6
化学物質	8
劇物	0
検査	760
食品防御	1
フードディフェンス	7
いたずら	34

表3. 意図的混入が否定できない事案相談の年別推移

(A) 相談者別



(B) 苦情対象別



に関連する案件を抽出するため、14 のキーワード（「混入」「意図的」「警察」「事件性」「犯罪」「悪意」「特異」「毒物」「化学物質」「劇物」「検査」「食品防御」「フードディフェンス」「いたずら」）を含む内容の案件 1,268 件を抽出した（各キーワードの該当件数は表 2 に示す）。抽出した案件について内容から食品防御的視点のあるものを仕分けし、69 件の食品防御的視点を含む苦情相談を得た。69 件の苦情相談を大別すると、意図的混入が否定できない事案相談が 39 件、未然防止が関わる相談は 30 件であった。

a. 意図的混入が否定できない事案相談

意図的混入が否定できない事案相談は、例えば異物の混入原因が不明である事例や相談者が疑っている事例などが含まれる。相談者別、苦情対象別の年別推移を表 3 に示す。相談件数は 2023 年の 16 件が最も多く、次いで 2024 年の 11 件であった。相談者別では消費者が多く、苦情対象別では異物が多い傾向にあった。

b. 未然防止が関わる相談

未然防止が関わる相談は、相談者又は食品衛生監視員に未然防止の視点が含まれていると記載内容から判断した相談であり、年別件数を表 4 に示す。2020-2022 年の各年より 2023、2024 年の各年の件数が増加していた。

表4. 未然防止が関わる相談の件数

受付年	2020	2021	2022	2023	2024	計
相談件数	3	3	5	9	10	30

相談者の内訳は、営業者（営業予定者を含む）が 27 件、行事主催者が 2 件、店舗設計者が 1 件であり、いずれも相談の主旨は食品防御対策ではなかったが、保健所からの回答や助言に食品防御対策を含めていた（保健所からの積極的助言）ものが 26 件、相談時に相談者側において対策済み（又は対策予定）である説明があったものが 4 件であった。各案件に含まれていた対策内容（表 5 参照）は、営業者の目が行き届かない場所の食品等の管理が多かった。

表5. 相談に含まれた未然防止対策の内容と該当件数

対策内容	該当件数
不在時の食品等保管	19
営業中の食品等の管理監視	7
調理場の管理	5
客の共通利用食品等の管理監視	3

２．教育訓練の内容検討

今年度は本研究での検討内容を活かして、川崎市健康福祉局生活衛生課が主催の研修会が開催された。

・食品防御対策研修会開催概要

日時：令和 8 年 3 月 5 日（木）15 時～17 時

場所：川崎市役所　復元棟２階ホール

対象者:川崎市内食品関係事業者、食品衛生監視員（川崎市）

内容：奈良県立医科大学公衆衛生学講座非常勤講師　神奈川芳行先生による食品防御対策に関する講演、事業者からの取組に関する講演、グループワーク

D．考察

食品衛生行政機関における食品防御対策の現状を知るため、二種類（調査 1、2）の実態調査を行った。調査 1 は、関東甲信越静ブロックに属する各都県市・特別区の保健所における食品防御対策に関わる業務の状況について、アンケート調査により把握を試みた。調査 2 は、川崎市の苦情相談データベースを用いて食品防御に関する相談対応の実態の把握を試みた。食品衛生行政機関における食品防御対策として、有事対応と未然防止に分けて検討した。

(1) 有事対応

調査 1 の結果から、56 自治体の保健所において 3 年間での意図的な混入と把握した食中毒事例の経験は 1 事例のみであり、非常にまれであることが確認された。また、混入原因不明の化学物質による食中毒事例の経験を含めても 3 事例と

少なく、対策の助言等に苦慮していた。また、警察との連携において、相談者が意図的な混入を疑っている場合に警察に相談するよう伝えても理解が得られないという所管不明瞭な事例の対応に苦慮していた。調査2の解析結果においても意図的混入が否定できない事案相談は5年間で39件が該当し、中には同様に警察に相談するよう助言していた事例もあり、どの自治体にも一定数ある事例と考えられた。調査1の回答で記載のあった意図的混入事例は監視カメラにより確認されていたが、原因不明のままの事例も多いと考えられ、その中で重大事案などの早期探知や未然防止に向けて保健所が可能な範囲でできることを次年度に検討していきたい。

(2) 未然防止

地方自治体における食品防御対策は関係法令からは所管が不明瞭であったが、調査1の回答内容から回答自治体の 32%が業務として可能な範囲で対応していることが判明した。その対応内容は、事業者等からの相談対応で助言を通して食品防御対策を推進しているものが多く、なかにはイベント開催において食品防御対策の普及啓発を行っている自治体もあった。調査2の解析結果においても、保健所からの積極的助言を通して食品防御対策を推進しており、このような推進方法は取り入れやすいのではないかと考えられた。

表 4 の結果から、2022 年から未然防止が関わる相談の件数が増加していた。これは、先行研究において川崎市の食品衛生監視員を対象に 2022 年に食品防御に関するアンケート調査を実施し、また 2024 年 1 月に食品防御に関する研修会を開催したことが影響して、保健所からの積極的助言が増えたのではないかと推察された。

調査 1、調査 2 について次年度にさらに解析することで保健所の状況を把握し、負担は少なく、かつ適度で効果的な対策を検討し、併せて教育訓練の内容についても検討する予定である。

E．結論

行政機関における食品防御対策として、食品衛生対策の中に食品防御の視点を適度に加え、食品衛生監視員の苦情相談対応を通した発生予防対策を検討する必要がある。また、未然防止の食品防御対策に関しては所管が不明瞭な自治体が多いと考えられ、食品事業者等の身近な相談窓口として食品衛生行政機関が担うべき役割が明確化されるべきである。

F．健康危険情報

なし

G．研究発表

1．論文発表

畠山理沙、佐々木国玄、赤星千絵、小河内麻衣、駒根綾子、清水英明、渡辺麻衣子、工藤由起子、岡部信彦：流通食品表面における SARS-CoV-2 汚染実態調査について．食品衛生学雑誌　66(5)：106-111，2025.

2．学会発表

なし

H．知的財産権の出願・登録状況

1．特許取得　なし

2．実用新案登録　なし

3．その他　なし

別添１：アンケート設問

【自治体食品衛生担当対象】

食品防御に関するアンケート

自治体名			
所属		回答者名	

回答については、該当の箇所を□で囲み（例：あり）、回答欄に内容を御記入ください。
貴所属の対応について評価するものではなく実態調査で、自治体名を伏せて集計し、結果報告を行います。

１　食品防御対策（フードディフェンス）は、悪意を持った者による意図的な食品の汚染に対する対策のことですが、この対策に関することについて貴部署の事務分掌に含まれていますか。

含む・含まない・その他

その他の概要

２　昨年度（2024 年度）に、以下について食品衛生法所管部局で対応したことがありますか。
(3)については、対応がある場合は業務内容も教えてください。

(1) 管轄食品事業者等の食品防御対策に関する相談対応

ある・あると思う・ないと思う・ない・その他

その他欄

(2) イベントにおける飲食提供の際の主催者や出店事業者の食品防御対策に関する相談対応

ある・あると思う・ないと思う・ない・その他

その他欄

(3) 自治体主催（又は関連）の大規模イベントにおける食品防御対策につながる予防的な対応（対策強化の案内や依頼、監視の実施、対策に対する補助等で、衛生対策の中に盛り込まれている場合を含む）

ある・あると思う・ないと思う・ない・その他

（ある場合）担当課が実施した業務内容：

回答欄

3　昨年度（2024 年度）に、食品衛生法所管部局において管轄食品事業者等や市民からの相談対応の中で、食品防御的な視点から助言を行ったことはありますか。

ある・あると思う・ないと思う・ない・その他

（ある場合）助言の例：

回答欄
（例）例えば防災用備蓄食品の保管場所の相談について、部外者にいたずらされないよう施錠できる場所で保管した方が良い等の食品防御的な観点からの助言をしたことがある。

4　2、3に関して、相談を受けた際に案内するホームページや資料はありますか。

(1) ホームページ：　　ある　・　ない

（ある場合）URL を記載ください。

回答欄

(2) 資料等：　ある　・　ない

（ある場合）差し支えなければ提供をお願いしたく、実施概要に記載の担当宛てに添付して送っていただくか、返送用の封筒を送りますので、資料の大きさと郵送先を以下に記載してください。

回答欄

5　2022~2024 年の 3 年間で、意図的な混入による汚染食品が原因と考えられる食中毒事例（有症苦情含む）について（警察との連携も含め）対応したことがありますか。

ある　・　ない

（ある場合）対応などの概要：

回答欄

6　2022~2024 年の 3 年間で、化学物質による汚染食品が原因と考えられ、かつ混入原因が不明だった食中毒事例（有症苦情含む）はありましたか。（5 で回答いただいた事例を除く）

ある　・　ない

（ある場合）概要と件数：

回答欄
（例）飲食店で有症苦情があり、店が提供する水のボトルから洗浄剤成分が検出されたが、混入原因は不明だった例が１件あった。警察にも情報提供を行った。

7　2、3、5、6 のいずれかで「ある」の場合、その際に困ったことはありましたか。

回答欄

8　食品防御対策に関する食品衛生監視員の対応について、国（厚生労働省又は農林水産省）に御要望があればお書きください。

回答欄

御協力ありがとうございました。

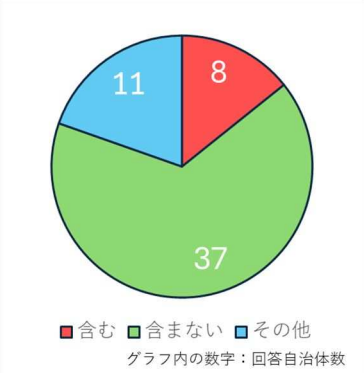
別添２：アンケート集計結果

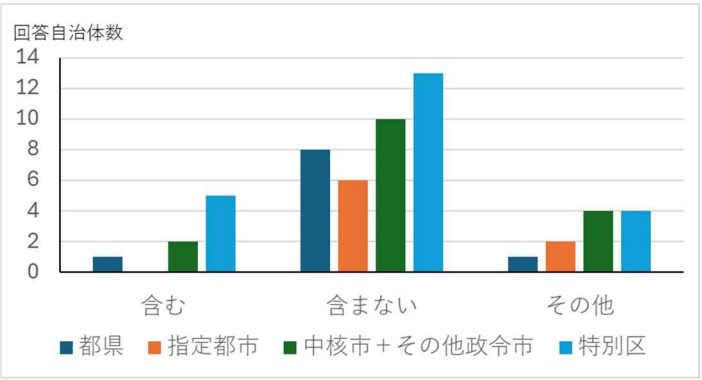
【自治体食品衛生担当対象】

食品防御に関するアンケートの集計結果

対象：関東甲信越静ブロックに属する各都県市・特別区の食品衛生所管課
実施：2025 年 11 月
回答率：95%（56/59 自治体）、
都県：10/11、指定都市：8/8、中核市・その他政令市：16/17、特別区：22/23

１　食品防御対策（フードディフェンス）は、悪意を持った者による意図的な食品の汚染に対する対策のことですが、この対策に関することについて貴部署の事務分掌に含まれていますか。

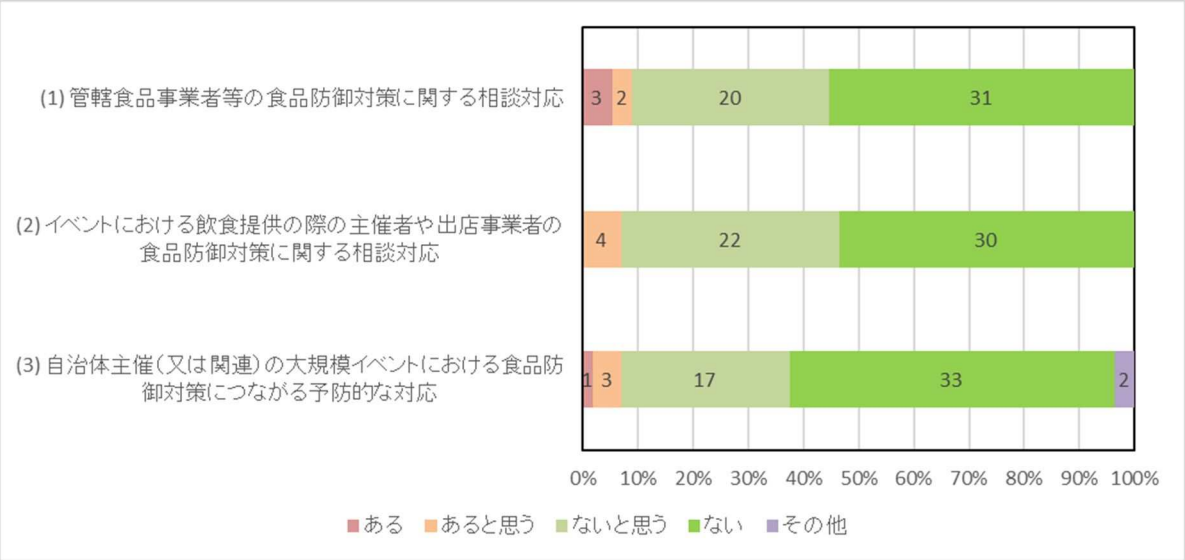




以下、その他の内容：

「食品防御対策」という直接的な文言はない。しかしながら、食品による健康被害という点で、気づいた点については助言を行っているが、積極的に行っているものではない。
明文化されていないが、食品衛生に関することの一部、健康危機管理の異物混入対策として含まれると考える。
事務分掌に明記していないが、事前相談時や申請受理時など必要に応じて事業者に対して助言等を行っている。
食品防御対策について直接の事務分掌には含まれていないが、これに関連する事故が発生した場合の衛生上の危害防止や被害拡大防止については、通常業務の一環として対応する。
発生時対応については含まれている。
内容により判断する。
食品衛生の観点から対応は行いますが、必要に応じて関係機関と連携することを想定しております。
食品を介して被害が発生することから、一概に当職が関与しないとは言い切れないが、基本的に悪意を持った意図的な混入の場合は、警察が所管する案件（刑事事件案件）であると解する。
当課の所掌事務は「食品衛生に関すること」となっており、食品防御対策については具体的に明文化されていない。
事務分掌には含まれないが、相談があった場合は応じ、事例が発生した場合は悪意があるか否かがわからない時点では食品衛生法第6条各項違反（疑い）で保健所が対応することになるが、明らかに悪意があるとなった場合は警察と対応を協議するものと思料される。
事務分掌上、フードディフェンスについて明記はされていないが、食中毒予防の防止の観点から、事業者に対して食品の適切な保管方法について、指導することがある。

2　昨年度（2024 年度）に、以下について食品衛生法所管部局で対応したことがありますか。



(1) の対応事例紹介：

・2025 年度に開催された世界陸上大会やデフリンピック大会などのイベントを運営する部署の担当者に対して、大会における飲食物提供時の助言の際に食品衛生のほか、食品防御対策についても普及啓発した。

(2) の「あると思う」の補足：

・相談窓口である各保健所の対応の詳細は不明であるが、(1)のような世界大会規模のイベント開催の際には適宜、管内に出店する食品事業者等からの問い合わせ時に普及啓発していることが想定される。

・地域行事に該当する場合、行事における食品提供の取扱指導要領に該当項目あり

(3) のその他：

・当課では実施していないが、イベント主催課が実施している対応は把握していない。

・自治体による大規模イベントではないですが、一般的な縁日祭礼に関する配布リーフレット（「行事における食品の提供について」）の中に、「毒物・異物混入の防止対策」として「調理の作業場所や食品の保管場所を離れる際には、必ず関係者を残すようにすること。」「容器包装に入れられた食品は、仕入れ時と販売時に容器包装に異常がないか確認すること。」という文言を入れております。

(3) の「あると思う」の補足：

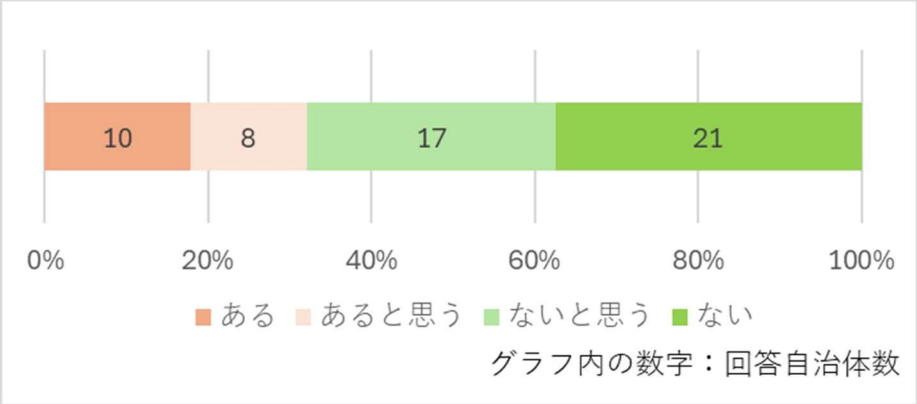
・自治体主催の行事に該当する場合、行事における食品提供の取扱指導要領に該当項目あり

・相談窓口である各保健所の対応の詳細は不明であるが、大規模イベント開催の際には自治体等のイベント主催者等からの問い合わせ時に衛生対策とは別に普及啓発していることが想定される。

(3) の「ある」の業務内容：

・出店者向けの講習会やイベント当日の監視の実施

3　昨年度（2024 年度）に、食品衛生法所管部局において管轄食品事業者等や市民からの相談対応の中で、食品防御的な視点から助言を行ったことはありますか。



以下、助言内容：

・シェアキッチンの施設では、複数の営業者が同じ冷蔵庫を使用するため、次の営業者が施設を使用する時は、原則食材も撤去することになっている。しかし、食材を撤去しない事例があったため、冷蔵庫内の保管場所に施錠するよう助言した。 ・許可調査に行った時に、屋外に食品保管用の冷凍冷蔵庫が置かれており、部外者が開けられないよう施錠等の措置をした方がよいと助言した。
・通常監視時に屋外で設置した冷蔵庫等について、いたずら防止に鍵を掛けるように指導している。 ・セルフサービスの水、ドリンクバー、サラダバー等の設置場所をスタッフから死角にならない場所にすること。 ・テーブル調味料は補充するだけでなく、監視・管理を行うこと。 ・消毒液や洗剤等は、客から見え、容易に持ち出すことができない場所に保管すること。 ・厨房からの死角に、未開封の食品保管棚があったため、客がいたずらできないような対策（鍵付の戸付き棚にする、区画をつける等）を行うこと。
・　・客席部分に不特定多数が出入り可能なオープンキッチンの調理場において、そ族昆虫防除の観点と合わせて区画や施錠が望ましい ・　・複合施設内の飲食店について、飲食店閉店後の従業員がいない時間帯にも客席部分に人の出入りが想定されることから、部外者にいたずらされないようにカウンター部分に窓のはめ込みが可能な一室構造がよい ・　・調理場、製造所内への監視カメラの設置
地域行事における食品提供の相談を受けた際、「行事における食品提供の取扱指導要領」にもとづいた指導内容のひとつとして「いたずら防止の観点から、食材を保管した場所には関係者が常駐すること」を助言しているケースは少なからずあると思われる。
飲食店において、厨房外にストッカーやショーケースを設置している場合、厨房内に移動するか、施錠して管理するよう助言している。客が自ら行うドリンクバーや調理機等について、従業員の目が届くよう指導している。
各事業所における対応の詳細は不明であるが、施設基準に反する事業者（例：調理場外に営業用冷蔵庫が置かれており、施錠もされていないなど）を発見した際には食品衛生法に基づく指導のほかに食品防御の視点からも注意喚起し改善させることはある。
大規模なイベントにキッチンカーが出店し、使用する食材が車内に納まりきらず、主催者が用意した出店者が共同で使える冷凍冷蔵庫に保管していた。出店場所から離れた場所に設置していたため、施錠するよう助言したことがある。
屋外でのイベントにおいて、従事者の目の届く範囲に食品を保管するよう助言した。
薬品庫には施錠し管理者以外の持ち出しを禁止するような措置をとる、施設の外に冷蔵庫等がある場合は施錠するよう助言したことがある。
厨房外（客席）にある食品庫の施錠について助言
食品の保管場所が屋外の場合、部外者にいたずらされないよう施錠する等の助言をしたことがある。
食品事業者に対し、施設外に食品保管設備を設置する場合は、施錠するように指導している。
飲食店で裏口を出た屋外の誰でも立ち入れそうな所に冷蔵冷凍庫がある場合は、部外者にいたずらをされないように鍵をかけた方がよいという助言をしています。
屋外の冷蔵庫等に食品を保管している場合、部外者にいたずらされないよう施錠できる場所で保管した方が良い等の食品防御的な観点からの助言をしたことがある。

4　２、３に関して、相談を受けた際に案内するホームページや資料はありますか。

・自治体独自ホームページ
https://www.hokeniryo1.metro.tokyo.lg.jp/shokuhin/bougyo.html
・自治体独自ホームページ（※地域行事における食品提供に関する相談のみ。）
https://www.city.yokohama.lg.jp/kenko-iryo-fukushi/kenkoiryo/shoku/yokohamaWEB/gyomu/tetuduki/gyouji.html
・農林水産省パンフレット「食品製造事業者、外食事業者の皆さまへ　取り組みましょう食品防御」
・国や東京都のホームページ

5　2022~2024 年の 3 年間で、意図的な混入による汚染食品が原因と考えられる食中毒事例（有症苦情含む）について（警察との連携も含め）対応したことがありますか。

あり：２例、以下概要。

(1) 飲食店において、客席に置かれたピッチャーの水を飲んだところ、体調不良（悪心等）となる有症苦情があった。監視カメラの確認により、先客が飲み残したアルコール飲料をピッチャーに入れていたことがわかった。店には、従業員が客席の飲食物に目が届くようにし、見回るよう指導した。

困った点：対象が水で、厨房外でサービスで提供しているものであり、管理強化の方法などの指導内容に苦慮した。

(2) 実際に意図的な混入があったかどうかは不明ですが、本人申立てで飲食店で異物や薬剤を意図的に混入されているのではないか、との相談はあります。食品の衛生的な取扱いについてのみ当該施設に立ち入り状況を確認することもありますが、原則的には異物の意図的な混入については、警察の管轄である旨説明しています。

困った点：薬物等であれば事件であるため警察の管轄である旨説明するが、他に相談した際に保健所に伝える様に言われたとして、なかなか理解が得られない。

6　2022~2024 年の 3 年間で、化学物質による汚染食品が原因と考えられ、かつ混入原因が不明だった食中毒事例（有症苦情含む）はありましたか。（5 で回答いただいた事例を除く）

あり：２例、以下概要。

(1) 学童クラブで提供する麦茶に洗剤が混入した事例があったが、混入経路が不明であった例が１件あった。

困った点：当時の状況を聞くが、原因を特定できず再発防止策に関する助言に苦慮した。

(2) 社会福祉施設で発生した「塩素系消毒剤が混入（疑い）したほうじ茶」による有症苦情において、保健所より先に事情聴取等していた警察と情報共有した事例が１件あった。

困った点：

・社会福祉施設が残品を廃棄しており、先に通報を受けた警察がその他証拠品を押収していたため、地方衛生研究所で検査することができなかったこと

・地方衛生研究所では、検査できる項目に限りがあり、化学物質を特定するための検査手法は整えていないこと（混入された化学物質をある程度推定できない状況では、地方衛生研究所で対応することができない可能性があること）

８　食品防御対策に関する食品衛生監視員の対応について、国（厚生労働省又は農林水産省）に御要望があればお書きください。

・悪意を持って意図的になされる行為に対する食品防御対策について、その予防は事業者責任において自主管理されるものであり、発生後の対応は警察案件と考える。食品衛生監視員には知識も経験もなく、現時点で対応することは困難と考える。 ・事業者から相談があった場合に、食品防御対策が案内ができるような、ウェブサイトを作成し、教育素材や、リーフレット、事業者向けの動画、チェックリスト等があれば、御供与願いたい。
・食品防御対策について、食品衛生行政における明確な役割を国に示して欲しい。 ・2022年以前に、事業者より何者かにより商品を偽物にすり替えられた事例があるという事例を聞いたことがある。その事業者は警察に対応を依頼し対処したと聞いているが、食品による事故が発生した場合などの警察との連携等、マニュアル等の整備や、連携フロー、研修などがあるとよい。 ・発生した際は、警察案件である。食品防御対策については気づいた点については助言程度で行っているが、正式に保健所の業務として扱われるのはいかがなものかと思う。事業者へのパンフレット配布程度であれば可能と考える。
実際の事例をもとに対応指針などを示してもらえるとありがたいです。
監視員の対応ではなく、事業者に対する依頼になるが、飲食店等食品取扱事業者のフードディフェンスに対する考えが非常に乏しいと感じている。各店舗が個別に閉鎖空間にできない厨房となっているフードコート型店舗において、フードディフェンスの観点から冷蔵庫等に鍵の設置等を提案しても、必要性が全く響かない（対策を講じない）。また、路面店でも営業前に路上に食材が放置されている（店員不在時に納品されたものと思われる）店舗も少なくない。食品衛生責任者養成講習会における必須履修科目にするなど、飲食店等食品等取扱事業者に対し、フードディフェンスの啓発、意識向上を図ってほしい。
基本的に警察の所管と思われるが、今後食品防御対策を国として積極的に進めるのであれば、まずは所管を明確にしたうえで、自治体向けの対応指針等を整備する必要があると思われる。また、故意によるに食品危害事案発生時の対応については、自治体向けの対応マニュアル等があれば事例発生時には有効であると思われる。
故意に混入された可能性がある場合は警察事案となることから、再発防止に向けた原因の究明に当たっては警察との連携が必要となるため、国として警察との調整を図ってもらいたい。
上記４(2)にて農林水産省より提供いただいて使用しているパンフレットの内容が以前は農林水産省のHPに掲載されていたが、現在、パンフレットとしては閲覧することができなくなっており、各事業所において紙のパンフレットがなくなった場合にご案内ができない。農林水産省に問い合わせたところ担当部署が変更されたとのことであるが、部署名・問い合わせ先を変更のうえ再度HP掲載を希望する。
食品衛生法第28条③で食品衛生監視員の職務において「第一項の規定による権限は、犯罪捜査のために認められたものと解釈してはならない。」と明記されているため、食品防御（food defense）の定義が「悪意からの毒物等による食品汚染を防ぐこと」であるなら、原則的に我々自治体の食品衛生監視員では食品防御対策は対応できません（改めての確認です。法改正は望みません）。 ただし、これまでの経緯（清涼飲料水等への薬物混入・冷凍食品への農薬の混入事件、伊勢志摩サミット・東京オリンピック　等）を考えると、食品防御が重要であることは重々承知しております。当自治体での講習会や監視等の際には、食品衛生の考え方と合わせて状況に応じて食品防御に関する説明・対応のお願いをしたことはあります。
ガイドラインの作成
不特定多数を殺傷等しようとして、食品等に有害物質を混入し発生する健康被害について、事後の事件捜査は傷害事件として警察の対応となることはゆるぎないが、事業者自身が食品防御対策をしっかり構築すること及び警察との連携を視野に入れた国による法令及び実施体制の整備等の対策を望む。
本件に関する対応について、統一的な見解を示していただけるとありがたいです。
各企業においては場内へのカメラ設置等抑止力を整えつつあるが、その総てを防止するには困難な状況である。実際に発生した場合は威力業務妨害、傷害等の刑法犯が成立すると思料され、この場合は食品防御対策について食品衛生監視員だけでは対応困難となる。警察庁等とも連携が取れるような仕組みを予め構築願いたい。
過去にあった意図的に食品が汚染された事例やその対応策などがあれば知りたい。また、どういった点から意図的に食品が汚染されたと判断したのかが知りたい。
「食べ残しの持ち帰りガイドライン」と同様、必要に応じて食品衛生部局が取り組むべき方向性を示していただきたい。

厚生労働科学研究費補助金（食品の安全確保推進研究事業）
「新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した
食品防御の推進のための研究」分担研究報告書（令和 7 年度）

海外における食品防御政策、規格等の動向調査

研究代表者　今村 知明（公立大学法人奈良県立医科大学　公衆衛生学講座　教授）

研究要旨

本調査は、海外における食品防御政策および食品不正（Food Fraud）対策の動向を把握し、我が国の食品防御対策の基礎資料とすることを目的として実施した。米国 FDA では、輸入冷凍シーフードの short-weighting（短量）が経済的動機による不正（EMA）および食品不正として扱われ、輸入拒否等の規制措置の対象となっていることを確認した。また、査察において食品不正が確認事項として位置付けられていることを整理した。FSMA の意図的混入（IA）規則については大きな改正はなく、運用が継続されている。CODEX/CCFICS では食品偽装ガイドラインが Step5 到達後も検討継続中である。PAS96 改訂はドラフト公開およびコンサルテーションが実施されたが、最終版は未公表であった。以上より、食品防御および食品不正に関する国際動向は、各制度において運用継続または検討段階にあり、規制運用の実務化と国際基準整備が進展している状況が確認された。

A．研究目的

令和 7 年度における海外での食品防御政策に関わる最新情報の把握を通じて、我が国におけるフードディフェンス対策の検討を行っていくうえでの基礎的資料とすることを目的とする。

B．研究方法

米国 FDA（Food and Drug Administration）が施行・管理する FSMA 法[1]に関する更新事項のうち、特にフードディフェンスおよびフードフラウドに関連する内容について、その最新の動向を整理した。あわせて、コーデックス委員会（Codex Alimentarius Commission）総会および CCFICS（食品輸出入検査・認証制度部会）におけるフードディフェンスに関する検討議題と、その進捗状況について整理した。

さらに、英国 BSI を中心として進められている PAS96（第 5 版）の改訂作業については、開発担当者への聞き取り調査を実施し、その進捗状況を整理した。

（倫理面への配慮）

本研究において、特定の研究対象者は存在せず、倫理面への配慮は不要である。

C．研究結果

1. FDA による輸入冷凍シーフードの EMA（short-weighting）調査の動向

FDA は、輸入冷凍シーフードにおける正味重量の不正表示、即ち short-weighting（短量）に関する調査結果を 2025 年 9 月 2 日付で公表

[1] FDA, FSMA Rules,2024.2.5 https://www.fda.gov/food/guidance-regulation-food-and-die-tary-supplements/food-safety-modernization-act-fsma 最終閲覧日 2026 年年 3 月 22 日

した 。FDA の「Constituent Update」では、同庁が 4 か国から輸入された小売包装済み冷凍シーフード製品 28 検体を収集し、製品ラベル上の正味重量表示への適合性を調査したこと、その結果として 10 検体（36%）が違反であり、短量の程度は 2.3%から 9.9%であったこと、さらに違反検体に係るすべての貨物は米国への輸入を拒否されたことが記載されている。

同日付で公表された詳細ページでは、本調査が FDA の経済的動機による不正（Economically Motivated Adulteration：EMA）に対処する継続的取組の一環として、2022 年から 2024 年にかけて輸入冷凍の生および加熱済みシーフード製品を収集・試験したものであることが示されている。また、short-weighting（短量）とは、包装に表示された正味重量より少ない量の製品が販売されることであり、その一因として、水グレーズ又は氷の許容されない重量が正味重量に含まれていることが説明されている [2]。

さらに、当該ページでは、氷衣（glaze）は冷凍シーフード製品を冷凍焼け（freezer burn）から保護する目的で一般的に用いられるものの、その重量を含めて正味重量を過大表示することは認められていないこと、及びこのような行為は食品不正（Food Fraud）の一種であり、消費者に対して重量に基づく製品価値について誤解を与えるものであることが記載されている。

調査対象の内訳については、28 検体の内訳がエビ 25、イカ 2、ティラピア 1 であり、対象製品が 4 か国の 12 社由来であったこと、さらに各検体は同一製造ロットの包装済み冷凍シーフード 48 ユニットで構成されていたことが示されている [3]。

また、FDA の「Constituent Update」及び詳細ページでは、氷衣を含めて内容量を過大表示する行為が、食品のかさ（見かけ量）又は重量を増やすために物質を加える EMA の一形態であることが明示されている。 さらに、氷衣重量を含めた過大表示は食品不正の一種としても位置付けられている。これにより、short-weighting（短量）は表示不適合にとどまらず、経済的利益を目的とする不正行為として、EMA および食品不正の枠組みで扱われていることが示されている。

行政措置との関係では、違反貨物は輸入拒否（refused entry）の対象となることが示されており、さらに違反検体は規制措置（regulatory actions）の対象となり、適切な場合には刑事調査（criminal investigations）の検討対象となることが記載されている。また、FDA は輸入製品に関連する EMA を検出し対処するため、国際的な当局間連携を行っていることも示されている。

なお、Import Alert 99-47 については、FDA 関連公式サイトにおいて、EMA に関連する輸入監視措置として位置付けられている [4]。

以上より、2025 年 9 月 2 日に公表された一

[2] FDA: Sample Collection and Analysis of Imported Frozen Seafood for Economically Motivated Adulteration: Year 2022-24
URL:https://www.fda.gov/food/economically-motivated-adulteration-food-fraud/sample-collection-and-analysis-imported-frozen-seafood-economically-motivated-adulteration-year-2022 最終閲覧日 2026 年年 3 月 22 日

[3] FDA companion data table: Sample # Firm Country of Frozen Product % Short Weight
URL: https://www.fda.gov/media/188499/download
最終閲覧日 2026 年年 3 月 22 日

[4] FDA Access Data search result for Import Alert 99-47
URL:

連の FDA 情報は、輸入冷凍シーフード分野において、氷衣を利用した short-weighting（短量）が EMA および食品不正として継続的に問題視されており、FDA がこれをサンプリング調査、輸入拒否、規制措置の対象として監視していることを示すものである。

2. CPGM 7303.842 における食品不正（Food Fraud）対応指示の明確化

FDA の「Compliance Program Guidance Manual（CPGM）7303.842 : Seafood Processor, Products, and Importer Inspection Program」は、2025 年 9 月 30 日付で公表されている。本文書は、シーフード加工業者、製品及び輸入者に対する査察・検査プログラムを規定するものである。

当該文書には、「経済的動機による不正又は食品不正に関する特別指示（Special Instructions for Economically Motivated Adulteration or Food Fraud）」と題する節が設けられており、査察時には受入記録（購買記録等）と最終製品ラベルを比較すること、及び必要に応じて誤表示（misbranding）に関する事項を FDA Form 483 に記録することが示されている [5]。

また、同文書には、魚種の置換や誤表示といった食品不正が、海洋毒素（marine toxins）、アレルゲン（allergens）、ヒスタミン中毒（scombrotoxin）等の食品安全上の危害要因と関連し得ることが示されている。

さらに、当該プログラムにおいては、食品不正及び EMA が検査・記録・観察・指摘の対象として位置付けられており、査察の現場において文書照合や表示確認を通じて具体的に取り扱われることが示されている。

これらの内容は、2025 年 9 月 2 日に公表された short-weighting 調査結果と整合しており、FDA がシーフード分野における食品不正及び EMA を、調査のみならず、実際の査察・検査の運用枠組みにおいて取り扱っていることを示している。

3. FDA における食品不正（Food Fraud）の定義整理とシーフード事例との関係

2025 年 8 月 28 日、FDA は「Economically Motivated Adulteration（Food Fraud）」に関するページを公表している [6]。

当該ページでは、EMA は、食品中の価値のある成分や一部を意図的に除く、取り除く、置換する、又は食品を高価に見せるために物質を加える行為として説明されている。また、FDA はこの種の EMA を食品不正（Food Fraud）と呼ぶことを明示している。

同ページでは、食品不正は一般的な EMA の一形態として位置付けられており、対象は食品に限らず動物用飼料（animal food）や化粧品（cosmetics）にも及び得ることが示されている。さらに、一部の EMA は誤表示違反（misbranding violations）に該当する可能性があることも記載されている。

具体例として、はちみつ（Honey）、メープルシロップ（Maple Syrup）、シーフード（Seafood）

https://www.accessdata.fda.gov/cms_ia/importalert_1178.html 最終閲覧日 2026 年年 3 月 22 日

[5] FDA: Food Compliance Program Guidance Manual 7303.842: Seafood Processor, Products, and Importer Inspection Program
URL: https://www.fda.gov/media/71302/download
最終閲覧日 2026 年年 3 月 22 日

[6] FDA: Economically Motivated Adulteration (Food Fraud)
URL:https://www.fda.gov/food/compliance-enforcement-food/economically-motivated-adulteration-food-fraud
最終閲覧日 2026 年年 3 月 22 日

が挙げられており、シーフードでは、高価な魚種の代わりに安価な魚種を販売する行為や、氷を加えて重量を増やして見せる行為が示されている。また、食品不正は経済的な問題にとどまらず、添加・置換・除去された物質によっては重大な健康被害につながる可能性があることが示されており、香辛料の不正混入（adulterated spices）による鉛中毒や、アレルゲンの混入による健康影響が例示されている。

以上の内容と、2025 年 9 月の short-weighting 調査及び CPGM の運用指示をあわせて整理すると、FDA は食品不正及び EMA を、定義、具体例、調査、査察運用の各レベルで一貫して取り扱っていることが示されている。

4. FSMA に基づく意図的混入（Intentional Adulteration：IA）規則に関する動向

2025 年時点の FDA の公開情報において示されている IA 関連の主な動向としては、食品安全強化法（FSMA）に基づく基準額のインフレ調整の更新及び、適用範囲並びに適用日を示す FAQ の継続掲載が挙げられる [7,8]。

基準額のインフレ調整においては、「意図的混入から食品を保護するための緩和戦略」に関する極小規模事業者（Very Small Business）の基準額が、2011 年の 1,000 万ドルから、2022 年から 2024 年の平均値に基づくインフレ調整後の 13,318,941 ドルに更新されている。

また、FDA の FAQ においては、IA 規則の適用日として、極小規模事業者は 2021 年 7 月 26 日、小規模事業者は 2020 年 7 月 27 日、それ以外の事業者は 2019 年 7 月 26 日とされている。さらに、極小規模事業者は規則の全要件から免除される一方、当局から求められた場合には当該区分に該当することを示す文書の提示が必要とされている。

同 FAQ では、対象施設は脆弱性評価（vulnerability assessment）を実施し、重要工程（actionable process steps）を特定し、緩和戦略、監視、是正、検証を含むフードディフェンス計画（food defense plan）を作成・実施する必要があることが示されている。

さらに、水産物（seafood）、果汁（juice）、低酸性缶詰（LACF）、栄養補助食品（dietary supplements）については、他の FSMA 規則において一部免除が存在するものの、IA 規則においてはこれらに対する包括的な免除規定が存在しないことが示されている。

また、IA 規則は広範な公衆衛生被害を意図した行為への対応を目的としており、経済的利益を目的とする EMA とは区別されている [9]。以上より、2025 年時点における IA 規則の動向は、主として事業規模基準の更新及び既存制度の運用継続に関するものであり、IA 規則そのものの要求事項に関する新たな改正は確認されていない。

5. Codex（CCFICS）における食品偽装ガイドラインの動向

Codex における「食品偽装の防止及び管理に

[7] FDA: FSMA Inflation Adjusted Cut Offs
URL:https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-inflation-adjusted-cut-offs
最終閲覧日 2026 年年 3 月 22 日

[8] FDA: Frequently Asked Questions on FSMA
URL:https://www.fda.gov/food/food-safety-modernization-act-fsma/frequently-asked-questions-fsma
最終閲覧日 2026 年年 3 月 22 日

[9] FDA: Draft Guidance for Industry: Mitigation Strategies to Protect Food Against Intentional Adulteration
URL:https://www.fda.gov/regulatory-information/search-fda-guidance-documents/draft-guidance-industry-mitigation-strategies-protect-food-against-intentional-adulteration
最終閲覧日 2026 年年 3 月 22 日

関するガイドライン（Guidelines on the prevention and control of food fraud）」については、2024年11月のCodex Alimentarius Commission第47回総会（CAC47）において、Step 5として採択されている[10]。

2025年1月以降のCodex公開情報では、当該ガイドラインに関する電子作業部会（EWG）が継続して掲載されており、作業が継続していることが示されている[11]。また、当該EWGの参加登録締切が2025年1月15日とされていることが確認できる。

一方で、Codexの会合情報によれば、2025年1月から2026年3月までの期間において、CCFICSの本会合は開催されていない[12]。また、同期間において、食品偽装ガイドラインに関する新たなドラフト文書又は新たなコメント募集回章が公開された事実は確認されていない[13]。

さらに、2025年11月時点のCodex公開文書において、当該ガイドラインがCCFICSにおいて開発中の文書として言及されている[14]。

以上より、2025年1月から2026年3月までの期間におけるCodex/CCFICSの食品偽装ガイドラインに関する動向は、CAC47におけるStep 5採択後、電子作業部会による検討が継続している一方で、本会合の開催や新規文書の公開といった進展は確認されていない。

6.PAS 96（第5版）改訂作業の動向

PAS 96（Publicly Available Specification 96）の第5版改訂は、2023年11月に開始されたことが確認されている[15]。その後、2025年4月時点では、Technical Authorとの契約締結およ

[10] Codex Alimentarius Commission (CAC47) Final Report (REP24/CAC)
URL:https://www.fao.org/fao-who-codexalimentarius/sh-proxy/en/?lnk=1&url=https%3A%2F%2Fwork-space.fao.org%2Fsites%2Fcodex%2FMeetings%2FCX-701-47%2FFINAL%2520REPORT%2FREP24_CACe.pdf
最終閲覧日 2026年年3月22日

[11] Codex Committee on Food Import and Export Inspection and Certification Systems (CCFICS) – Related Electronic Working Groups
URL:https://www.fao.org/fao-who-codexalimentarius/committees/committee/related-ewgs/en/?committee=CCFICS
最終閲覧日 2026年年3月22日

[12] Codex Committee on Food Import and Export Inspection and Certification Systems (CCFICS) – Related Meetings
URL:https://www.fao.org/fao-who-codexalimentarius/committees/committee/related-meetings/en/?committee=CCFICS
最終閲覧日 2026年年3月22日

[13] Codex Committee on Food Import and Export Inspection and Certification Systems (CCFICS) – Related Circular Letters
URL:https://www.fao.org/fao-who-codexalimentarius/committees/committee/related-circular-letters/en/?committee=CCFICS
最終閲覧日 2026年年3月22日

[14] Codex Alimentarius Commission (CAC48) Final Report (REP25/CAC)
URL:https://www.fao.org/fao-who-codexalimentarius/sh-proxy/en/?lnk=1&url=https%3A%2F%2Fwork-space.fao.org%2Fsites%2Fcodex%2FMeetings%2FCX-701-48%2FFINAL%2520REPORT%2FREP25_CACe.pdf
最終閲覧日 2026年年3月22日

[15] BSI Standards Development Portal（PAS 96 Project Page）
URL: https://standardsdevelopment.bsigroup.com/projects/2023-02427
最終閲覧日 2026年年3月22日

び契約後に BSI の起草ルールに関するトレーニングを実施する計画が想定されていた。

しかしながら、2025 年 9 月時点において、スポンサー側との契約調整が継続しており、Technical Author による文書作成作業が開始されていない状況であることが関係者間で共有されている。このため、当初想定されていたドラフト作成およびレビュー工程は遅延した。その後、2025 年 12 月初旬の時点で、担当者より文書は内部レビュー段階にあり、スポンサー承認後にパブリックコンサルテーションを開始する予定であることが示された[16,17]。そして、2025 年 12 月 17 日に Draft PAS 96 が公開され、パブリックコンサルテーションが開始された。本コンサルテーションは、BSI Standards Development Portal 上で実施され、コメント提出は同ポータルを通じて行われた[15]。

当初の案内ではコンサルテーション期間は 2026 年 1 月中旬までとされていたが、その後延長され、最終的に 2026 年 2 月 1 日まで実施されたことが確認されている[18]。

PAS の改訂プロセスにおいて、ドラフト文書が外部に公開されるのはパブリックコンサルテーション開始時点のみであり、それ以前の Technical Author 作業、内部レビュー、Steering Group レビュー等の段階では公開ドラフトは存在しない。したがって、本改訂におけるパブリックコンサルテーションは、内部検討を経た文書が初めて外部ステークホルダーに提示される段階であり、外部からの評価および意見収集を行う正式なプロセスとして位置づけられる。

公開された Draft PAS 96 においては、本規格が食品および飲料に対する意図的攻撃への対応を目的としたガイダンスであることが明示されている。対象は、破壊行為、不正混入、恐喝、スパイ行為、サイバー攻撃等の意図的行為であり、偶発的汚染や自然由来ハザード、通常の食品安全リスクは対象外とされている。また、本規格は要求事項ではなくガイダンスであり、組織の状況に応じた対応を前提とする点が示されている。

さらに、ドラフト本文から、食品防御におけるリスク評価の枠組みとして TACCP の体系的整理が図られていること、サイバー領域を含む多様な脅威への対応が考慮されていることが確認できる[16,19]。

以上より、2025 年から 2026 年初頭にかけての PAS 96（第 5 版）改訂の動向は、改訂作業の遅延を経て 2025 年 12 月に公開フェーズへ移行し、パブリックコンサルテーションの実施に至ったことが確認される段階にある。一方、最終版は現時点で未公表であり、最終的な内容は確定していない。

D．考察

1. FDA による輸入冷凍シーフードの EMA（short-weighting）調査の動向

本調査結果から、輸入冷凍シーフードにおいて正味重量の不適合が一定割合で確認されていることが示された。特に、氷衣を含めた重量表示が問題となっている点は、冷凍製品特有の

16 海外における食品防御政策、規格等の動向調査（添付資料 1）

17 英国 BSIPAS96 開発担当者からのメール(添付資料 2)

18 PAS 96 Draft Public Consultation に関する案内メール（添付資料 3）

19 PAS 96:2026 Draft – Protecting and defending food and drink from deliberate attack – Guide（添付資料 4）

工程に起因する表示管理の重要性を示している。また、違反製品が輸入拒否の対象となっていることから、当該不適合は単なる表示の問題にとどまらず、規制上の措置に直結する事項として扱われていることが確認できる。さらに、当該行為がEMAおよび食品不正として位置付けられている点から、FDA は重量表示の不適合を経済的動機による不正の一形態として整理していることが明らかである**エラー! ブックマークが定義されていません。**。

2. CPGM 7303.842 における食品不正（Food Fraud）対応指示の明確化

本プログラムにおいて、食品不正およびEMA が査察時の確認事項として明示されていることから、これらは単なる概念的整理にとどまらず、実務上の検査項目として運用されていることが確認できる。特に、受入記録と製品ラベルの照合が求められている点は、表示の適正性を検証するための基本的な手法として位置付けられている。また、食品不正がアレルゲンや毒素等の危害要因と関連し得ることが示されていることから、食品不正は品質・表示の問題に加え、食品安全上のリスクとも関連付けて扱われていることが確認される[5]。

3. FDA における食品不正（Food Fraud）の定義整理とシーフード事例との関係

FDA において、EMA と食品不正（Food Fraud）が同一概念として整理されていることにより、食品不正の範囲が明確化されている。具体例として示されたシーフードにおける魚種の置換や重量の水増しは、前述の short-weighting の事例とも整合しており、定義と実際の事例が一貫していることが確認できる。また、食品不正が場合によっては健康被害につながる可能性が示されている点から、経済的問題に限定されず、食品安全の観点からも管理対象とされていることが分かる。これらより、FDA は食品不正を定義、事例、規制運用の各レベルで整理しているといえる[6]。

4. FSMA に基づく意図的混入（Intentional Adulteration：IA）規則に関する動向

2025 年時点において、IA 規則そのものの要求事項に大きな変更は確認されていない一方で、事業規模に関する基準額の更新や適用範囲に関する情報提供が継続されていることが示された。また、IA 規則が EMA とは区別され、広範な公衆衛生被害を意図した行為への対応を目的としていることが改めて整理されている。さらに、対象事業者に対して脆弱性評価およびフードディフェンス計画の策定が求められている点から、既存の制度の運用が継続している状況にあるといえる[7,8]。

5. Codex（CCFICS）における食品偽装ガイドラインの動向

本ガイドラインは CAC47 においてステップ 5 に到達した後、電子作業部会による検討が継続されているが、当該期間において本会合の開催や新たな文書の公表は確認されていない。このことから、ガイドライン策定は進行中ではあるものの、一定期間においては大きな進展が見られていない状況にあるといえる。また、電子作業部会による検討が継続していることから、未解決の論点について引き続き調整が行われている段階であることが示されている[10,11]。

6. PAS 96（第 5 版）改訂作業の動向

PAS 96 の改訂作業は、契約手続きの遅延により当初のスケジュールから遅延したものの、2025 年 12 月にドラフトが公開され、パブリックコンサルテーションが実施されたことから、改訂プロセスが公開段階に移行したことが確認できる。また、コンサルテーション期間が延長されたことから、外部ステークホルダーから

の意見収集が一定期間確保されたことが示されている。一方で、最終版は公表されておらず、現時点では内容が確定していない段階にある。したがって、本改訂は進行中のプロセスにあり、今後の結果を確認する必要がある状況である[19]。

E．結論

本調査により、米国 FDA における食品不正（Food Fraud）および経済的動機による不正（EMA）への対応、FSMA に基づく意図的混入（IA）規則の運用状況、コーデックス委員会における食品偽装ガイドラインの検討状況、ならびに英国 PAS 96 の改訂動向について、最新の状況を整理した。

FDA においては、輸入冷凍シーフードにおける short-weighting（短量）が EMA および食品不正として取り扱われ、サンプリング調査および輸入拒否等の規制措置の対象となっていることが確認された。また、CPGM において食品不正が査察時の確認事項として明確に位置付けられていることから、食品不正への対応が調査のみならず査察運用でも実施されていることが示された。さらに、食品不正に関する定義および具体例が整理されており、定義、調査、査察の各段階で一貫した枠組みで取り扱われている状況が確認された。

FSMA に基づく IA 規則については、2025 年時点において新たな要求事項の追加や大きな改正は確認されておらず、事業規模基準の更新および既存制度の運用が継続されている状況であった。また、IA 規則が EMA とは区別され、広範な公衆衛生被害を意図した行為への対応として位置付けられていることが改めて整理された。

コーデックス委員会においては、食品偽装の防止及び管理に関するガイドラインが CAC47 にてステップ 5 に到達した後、電子作業部会による検討が継続されているものの、本会合の開催や新たな文書の公表といった進展は確認されていない。したがって、当該ガイドラインは引き続き検討段階にあることが示された。

PAS 96（第 5 版）の改訂については、契約手続きの遅延により当初計画から遅延が生じたものの、2025 年 12 月にドラフトが公開され、パブリックコンサルテーションが実施されたことから、改訂プロセスが公開段階に移行したことが確認された。一方で、最終版は現時点で公表されておらず、内容は確定していない状況にある。

以上より、2025 年から 2026 年初頭にかけての食品防御および食品不正に関する国際的動向は、FDA においては食品不正対応の実務運用が継続的に強化されている一方、IA 規則は既存制度の運用段階にあり、コーデックスおよび PAS 96 については検討・改訂が進行中である段階にあることが確認された。今後は、これらの制度およびガイドラインの進展状況を継続的に把握することが重要である。

F．健康危険情報

なし

G．研究発表

１．論文発表　　なし

２．学会発表　　なし

H．知的財産権の出願・登録状況

１．特許取得　なし

２．実用新案登録　なし

３．その他　なし

（添付資料 1）

海外における食品防御政策、規格等の動向調査

BSIグループジャパン株式会社
2026年3月22日

FDA Food Fraud（EMA）対策に関する最新動向

2025年 FDAにおける Food Fraud（EMA）の定義整理

(August 28, 2025)

◆ FDAにおける Food Fraud（EMA）の定義

・EMAは、価値のある成分の除去・置換・追加等を指す

・FDAはこの種のEMAをFood Fraudと呼んでいる

・Food Fraudは一般的なEMAの一形態とされている

◆ FDAが示す具体例

・Honey、Maple Syrup、Seafood などが例示されている

・Seafoodでは魚種すり替えや氷による重量増加が示されている

◆ Food Defense（IA）との関係

・EMAは経済的利益を目的とする行為

・IA (Intentional Adulteration) は広範な健康被害を目的とする行為に対応

・両者はFDA上で区別されている

⇒ 次頁：short-weightingはEMA（Food Fraud）の具体例

https://www.fda.gov/food/compliance-enforcement-food/economically-motivated-adulteration-food-fraud

2025年 FDA Food Fraud（EMA）対策に関する最新動向
― 輸入冷凍シーフードのEMA（short-weighting）調査結果 ―

(September 2, 2025)

◆調査の概要
調査対象サンプル：2022–2024に収集された輸入冷凍シーフード
28 サンプル（エビ 25／イカ 2／ティラピア 1）
目的：正味重量の不正表示（short-weighting）の有無を確認
試験方法：AOAC 963.18(*) に基づく重量検証
判定基準：平均 1% を超える正味重量不足 → 違反
(*)：冷凍シーフード製品の「正味重量（Net Weight）」を測定するための公式分析法

■ 調査結果
10/28 サンプル（36%）が違反（short-weighting）
違反サンプルが含まれる出荷はすべて輸入拒否（Refusal of Entry）

■ EMA（Economically Motivated Adulteration）
経済的利益を目的とした意図的な食品偽装行為
FDA は short-weighting を EMA＝Food Fraud と明確に分類
国際的な食品偽装リスクとして取り扱われる主要カテゴリー

■ Import Alert 99-47
経済的動機による不正の疑いがある食品を「物理検査なしで拘留できる制度（DWPE）」
違反した製品（shipments）はImport Alert 99-47の対象に登録
以後の同製品は、追加証明がない限り自動的に拘留対象

https://www.fda.gov/food/hfp-constituent-updates/fda-releases-results-economically-motivated-adulteration-short-weighting-seafood

https://www.fda.gov/food/economically-motivated-adulteration-food-fraud/sample-collection-and-analysis-imported-frozen-seafood-economically-motivated-adulteration-year-2022

2025年 FDA Food Fraud（EMA）調査の政策的意義

なぜこの FDA 調査が食品防御政策として重要か？

【1】short-weighting を“公式にEMA＝Food Fraud”と位置づけた事例

- FDAが食品偽装の定義と分類を明確に表明
- 政策カテゴリとしてのEMAへの対応が可

【2】国際サプライチェーン上の不正リスクを示す根拠

- 対象製品は4か国由来
- 冷凍水産物の食品偽装リスクが依然として高いことを示す

【3】行政措置の適用まで公開された事例

- 違反製品は輸入拒否
- Import Alert 99-47（DWPE）が適用
- FDAのFood Fraud対策プロセスが実際に機能していることを示す資料

【4】FDAが「監視継続」を明言（政策方向性の確認）

- 冷凍シーフードはEMAの対象になりやすいカテゴリ
- FDAは今後もサンプリングと監視を継続する方針を表明

EMAとは

経済的利益を目的とした意図的な食品偽装行為であり、short-weighting はFDAがEMAとして扱うカテゴリー。

Import Alert 99-47とは

Food Fraudの疑いがある製品を、追加証明がない限り「物理検査なしで拘留できる措置（DWPE）

https://www.fda.gov/food/hfp-constituent-updates/fda-releases-results-economically-motivated-adulteration-short-weighting-seafood

https://www.fda.gov/food/economically-motivated-adulteration-food-fraud/sample-collection-and-analysis-imported-frozen-seafood-economically-motivated-adulteration-year-2022

2025年 FDAシーフード検査プログラム（CPGM 7303.842）における Food Fraud（EMA）対応指示の明確化

(September 30, 2025)

◆ 現行文書（CPGM 7303.842）の概要

- **文書名**：*Seafood Processor, Products, and Importer Inspection Program*
- **位置づけ**：FDA検査官向けの **HACCP／GMP 検査マニュアル（運用指示文書）**

- 最新版は FDAで公開されており、「Food Fraud／EMA」に関する指示が文書内に明記
- 検査実施の手順・記録照合・報告方法が規定されている

◆ Food Fraud（EMA）に関する主な確認事項

- **受入記録と最終製品ラベルの照合**
- **種類のすり替え（species substitution）やミスブランディングの確認**
- **問題があれば Form 483 に記載することが指示**
- 食品偽装は海洋毒素・アレルゲン等の**安全性リスクにつながる可能性**があることを明示
- 検査データは **Food Fraud 関連コード（PAF等）で分類整理**

⇒現行の検査手順の中でFood Fraudが明確に扱われている点が重要

◆ 政策動向としての意義

- FDAは **Food Fraud（EMA）を既存のシーフード検査枠組みに組み込んで運用**
- 2025年1月に公表された EMA 調査（輸入冷凍シーフード short-weighting）とも整合

→ Food Fraudの重要性が確認され、検査マニュアルでも確認事項が明確

- **安全性ハザードを伴うFood Fraud** に対し、*“記録照合・ラベル確認・公式指摘書（Form 483）での記録化・統計分類”* という一連の運用が文書上で体系化
- これは **食品安全・食品防御・食品偽装の交差領域**としての政策動向を示す

【用語補足】

- **CPGM（Compliance Program Guidance Manual）**： FDA検査官向けの運用マニュアル（法令ではなく検査手順を示す文書）
- **FDA Form 483**： 検査官が企業に提示する **公式の指摘書（観察事項）**
- **PAF／sub-PAFコード**： FDAラボ検査の分類コード。Food Fraud関連検査が **統計カテゴリとして識別** される

https://www.fda.gov/food/compliance-enforcement-food/food-compliance-programs

https://www.fda.gov/media/71302/download

FSMA法関連動向、新業態に関する国外Food Defenseに係る論点整理

FSMA法関連動向（2025年1月）

【今年の更新：IA Cut Offs】

- 2025年7月17日、FDAはFSMA Intentional Adulteration（IA）規則における事業者区分（Very Small / Small / Other）の基準額を、インフレ調整により更新した。
- 今回の更新は事業規模判定額のみであり、IA規則の要求事項や施行要件に変更はない。

※IA Cut Offs：IA規則における事業者区分（Very Small / Small / Other）の判定に用いる基準額のインフレ調整。

【ガイダンス動向】

- 関連ガイダンスの更新なし

【過去報告内容】

- FSMAに関わる更新事項として、特定の食品に対する追加的なトレーサビリティ記録要件に関する最終規則が策定された。この最終規則は、2023年1月20日に発効し、2026年1月20日から施行される予定。
- 2022年3月に新たなガイダンス、「Guidance for Industry: Current Good Manufacturing Practice and Preventive Controls, Foreign Supplier Verification Programs, Intentional Adulteration, and Produce Safety Regulations: Enforcement Policy Regarding Certain Provisions　MARCH 2022 /（現行の適正製造基準及び予防的管理、外国供給者確認プログラム、意図的不純物混入、及び農産物安全規制。特定の条項に関する施行方針 産業界向けガイダンス　2022年3月）」が公表された。
- 事業規模によって段階的に設定されていた規則の遵守日が、2021年7月26日に最後に残っていた零細企業の遵守日を迎えたことにより、すべての規模の事業主体が遵守対象となる。
- 新しく発表されたガイダンス(2022年3月）では施行裁量に関する方針が示された。

・FDA (2025). FSMA IA Rule — Inflation-Adjusted Cut Offs. https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-final-rule-preventing-intentional-adulteration

・FDA (2023). FSMA Section 204 Traceability Rule. https://www.fda.gov/food/food-safety-modernization-act-fsma/requirements-additional-traceability-records-certain-foods

2025年 FSMA Intentional Adulteration（IA）規則に関する最新更新―
Inflation-Adjusted Cut Offs（インフレ調整後の基準額）の改定 ―

(July 17, 2025)

FDA は 2025 年 7 月 17 日付で、FSMA（Food Safety Modernization Act）に関する「Inflation-Adjusted Cut Offs（インフレ調整後の基準額）」を更新した。

本更新は、FSMA の各規則で適用される事業者区分（Very Small / Small / Other） を判定するための年間総売上額の基準を、物価指数に基づき改定するもの。

Intentional Adulteration（IA：意図的混入防止）規則では、事業者規模により適用要件・準備期間等が異なるため、**この基準額の更新は、IA 規則に関連する適用区分（Very Small Business）の金額基準の更新であり、IA 規則の施行要件・要求事項の変更ではない。**。
※ IA 規則の要件内容・施行要件に変更はない。

「FSMA Inflation-Adjusted Cut Offs（FDA, 2025）」

Baseline Value for Cut-offs (2011)	Value in 2020	Value in 2021	Value in 2022	Value in 2023	Value in 2024	Average 3 Year Value for 2022 - 2024
$10,000,000	$11,519,441	$12,047,638	$12,901,695	$13,365,945	$13,689,181	$13,318,941

- 本更新は FSMA 年次見直しによる金額基準の調整であり、Food Defense／IA に特化した新規ガイダンスや規制改訂ではない。
- 2025 年時点で FDA は IA 規則に関する施行・要求事項の変更を公表していない。

FSMA Inflation-Adjusted Cut Offs（最新）https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-inflation-adjusted-cut-offs

Intentional Adulteration Final Rulehttps://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-final-rule-mitigation-strategies-protect-food-against-intentional-adulteration

特定の食品に対する追加的なトレーサビリティ記録要件に関する最終規則

最終規則は2023年1月20日に発効し、2026年1月20日から施行される予定です。この情報は、FDAの公式ウェブサイトで確認できます。

最終規則の概要

この最終規則は、食品トレーサビリティリスト（FTL）に掲載された特定の食品を製造、加工、包装、または保管する事業者に対し、追加的なトレーサビリティ記録の保持を求めるものです。これにより、食中毒の発生時などにおいて、汚染された可能性のある食品を迅速に特定し、市場から速やかに除去することが可能となり、食源性疾患の発生や死亡を減少させることが期待されています。

主な要件

- **食品トレーサビリティリスト（FTL）**: FTLには、追加的なトレーサビリティ記録が必要とされる食品が一覧化されています。具体的な食品のリストは、FDAの公式サイトで公開されています。
- **重要追跡イベント（CTEs）と主要データ要素（KDEs）**: 事業者は、FTLに掲載された食品に関連する特定のCTEs（例: 収穫、冷却、初回包装、輸送、受領、変換）に対して、対応するKDEs（例: 追跡ロットコード、出荷日、受領者情報）を記録し、保存する必要があります。
- **追跡ロットコードの割り当て**: 事業者は、FTLに掲載された食品に対して一意の追跡ロットコードを割り当て、サプライチェーン全体でこのコードを使用して食品の追跡を行います。
- **トレーサビリティ計画**: 事業者は、自社のトレーサビリティ計画を策定し、記録の保存方法、担当者、手順などを明確にする必要があります。

施行スケジュール

すべての対象事業者は、2026年1月20日までにこの最終規則の要件を遵守する必要があります。これは、サプライチェーン全体で一貫したトレーサビリティ情報の共有を確保するためです。

https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-final-rule-requirements-additional-traceability-records-certain-foods?utm_source=chatgpt.com

https://www.fda.gov/media/171414/download

QAページでのIA規則関連情報（1/2）（2025年1月）

- 「意図的な偽和規則の遵守日はいつですか?」
  - この規則は、米国で消費する食品を製造/加工、梱包、または保管する国内または外国の食品施設を担当する所有者、運営者、または代理人に適用され、免除の対象とならない限り、連邦食品医薬品化粧品法(21 USC 350d)のセクション415に基づいて登録する必要があります。IA ルールのコンプライアンス日は、ビジネスの規模によってずらされます。
    - Very small （これまでまとめた報告書中の訳「零細企業」）: 2021年7月26日
    - Small （同じく、「小規模企業」）: 2020 年7月27日
    - All others（同じく、「小規模企業または零細企業でない企業で、免除対象とならない企業」） その他すべて:2019年7月26日

- 「FD.9 “A Very small Business“の定義は何ですか?私がそれに該当する場合、私は何をしなければなりませんか、そしていつ従わなければなりませんか?」
  - “A Very small Business“は、該当する暦年の前の3年間に、人間の食品の売上高に、製造、加工、梱包、または販売なしで保持されている(たとえば、有料で保持されている)人間の食品の市場価値を加えた、インフレ調整後の年間平均10,000,000ドル未満の企業(子会社および関連会社を含む)です。非常に中小企業は規則の全要件から免除されますが、2021年7月26日以降、要求に応じて、会社が“A Very small Business“であることを示すのに十分な公式レビュー文書を提供する必要があります。
  - IA規則の対象とならない、または免除される可能性のある施設の証明フォームはありません。
  - あなたが“A Very small Business“であるかどうかを計算する方法の詳細については、IAドラフトガイダンスの付録3「パート121に基づく非常に中小企業または中小企業としてのステータスの決定:意図的な偽和から食品を保護するための緩和戦略」を参照してください。

(参照)https://www.fda.gov/food/food-safety-modernization-act-fsma/frequently-asked-questions-fsma FDAホームページの「FSMAによくある質問と回答」より

※FDA Website構成変更によりURLが昨年より変更

QAページでのIA規則関連情報（2/2）（2025年1月）

- 「第117.5条(b)(シーフード)、第117.5条(c)(ジュース)、第117.5条(d)(LACF)、第117.5条(e)(栄養補助食品)に基づく人間の食品予防管理規則の要件から免除された場合、IA規則も免除されますか?食品防御計画を立てる必要がありますか?」
  - IA規則には、シーフード、ジュース、LACF、または栄養補助食品の免除は含まれていません。IA規則は、米国で消費する食品を製造/加工、梱包、または保持する国内または外国の食品施設を担当する所有者、運営者、または代理人に適用され、免除の対象とならない限り、連邦食品医薬品化粧品法のセクション415に基づいて登録する必要があります(21 CFR 121.5を参照)。この規則は、対象となる施設が書面による食品防御計画を準備するか、準備し、実施することを要求しています。

    - 重大な脆弱性と実行可能なプロセスステップを特定するための、必要な説明を含む脆弱性評価
    - 必要な説明を含む緩和戦略
    - 緩和戦略の実施に関する食品防御監視の手順
    - 食品防御是正措置の手順そして
    - 食品防御検証の手順(21 CFR 121.126を参照)

(参照)https://www.fda.gov/food/food-safety-modernization-act-fsma/frequently-asked-questions-fsma FDAホームページの「FSMAによくある質問と回答」より

※FDA Website構成変更によりURLが昨年より変更

2022年3月公表のガイダンスについて（2025年1月）

- 「Guidance for Industry: Current Good Manufacturing Practice and Preventive Controls, Foreign Supplier Verification Programs, Intentional Adulteration, and Produce Safety Regulations: Enforcement Policy Regarding Certain Provisions　MARCH 2022 /（現行の適正製造基準及び予防的管理、外国供給者確認プログラム、意図的な不純物混入、及び農産物安全規制：特定の条項に関する施行方針 産業界向けガイダンス　2022年3月）」
  - 米国食品医薬品局（FDA）は、FDA食品安全近代化法（FSMA）を実施する5つの規則のうち、特定の条項を施行しない意向を示すガイダンスを公表しました。5つの規則の対象となる特定の事業体および/または活動に対して特定の規制要件を強制しないことを明らかにしています。
  - 公表された施行裁量方針は、以下の５規則に関するものです。
    - ✓ 人間の食品の現在の適正製造慣行とハザード分析とリスクベースの予防管理
    - ✓ 動物性食品の現在の適正製造基準とハザード分析とリスクベースの予防管理
    - ✓ 人間と動物のための食品の輸入者のための外国サプライヤー検証プログラム(FSVP)
    - ✓ 人間の消費するための農産物の栽培、収穫、梱包、および保持に関する基準(PSR)
    - ✓ 意図的な異物混入から食品を保護するための緩和戦略(IA)
- IA規則関する施行裁量方針（セクションIII.Bに記載）
  - 特定の事業体に対する執行方針：2018年1月のFSMAガイダンスで、FDAは、特定の農場関連活動を行っているが、「農場」の定義の下では農場とは見なされない特定の施設に対して、執行裁量ポリシーを確立しました。この新しいガイダンスでは、FDAはIA規則に関連する執行措置を同じ施設や活動に適用するつもりはないことを明確にしています。（しかしながら、FDAは「農場」の定義を変更する可能性のある規則作成を発行しているので、これらは今後IAの規定がこれらの事業体に適用されるかどうかに影響します。）
  - 特定の状況におけるIA規則の執行方針：特定の状況（たとえば、是正措置手順の実装によって対処される単一の障害がある場合など）で再分析の要件を強制しないとした。

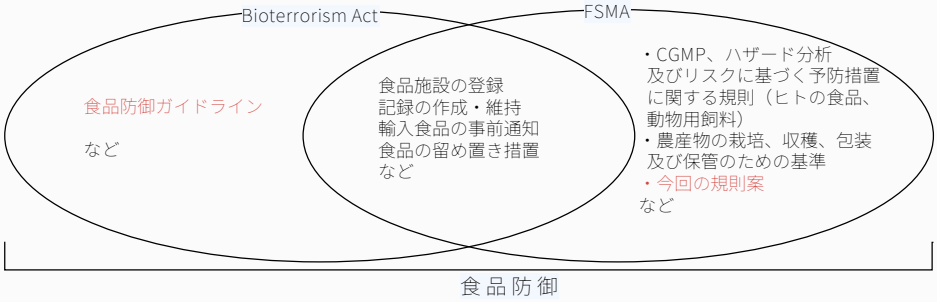
✓IA規則は、緩和戦略、戦略の組み合わせ、またはFDP全体が適切に実施されていない場合など、特定の状況において、食糧防衛計画(FDP)の再分析を要求しています。

✓IA規則はまた、対象となる事業体が、緩和戦略が適切に実施されていない場合に取らなければならない食品防御是正措置手順を確立し、実施することを要求しています。

重複を減らすために、FDAは、欠陥を修正し、欠陥が再び発生する可能性を減らす行動を通じて緩和戦略の不適切な実施が対処された場合には、再分析の要件については裁量をもって判断するとしています。

(参考) FDA食品防御ガイドラインとFSMAとの関係

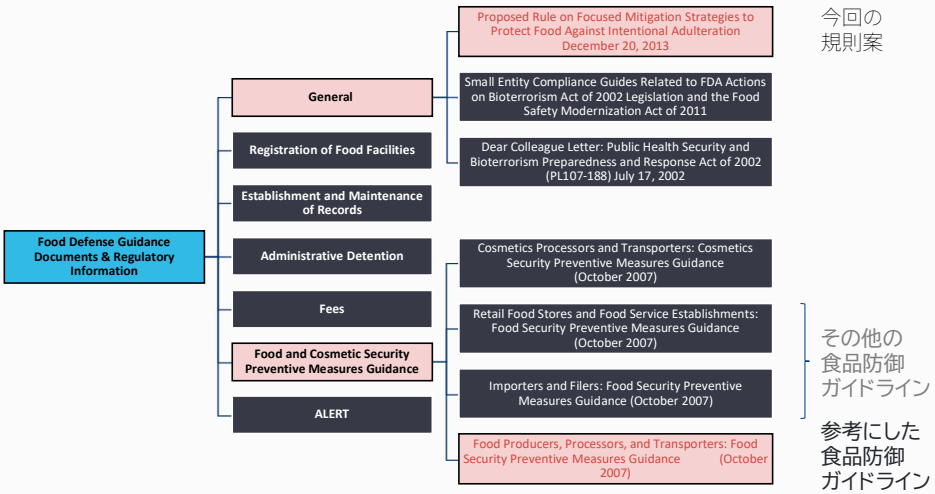
- FDA食品防御ガイドラインは、Bioterrorism Act(2002)を踏まえ、非拘束的な食品テロ予防措置として作成(*1)
  - 現在も2007.10ver.を最新版として公開(*2)
- FSMA(2011)は、食品安全・防御強化の一環として食品防御対策を検討・策定
  - Bioterrorism Actの関係規則・施策の一部を充実・強化
  - 追加的な規則・施策を作成・運用⇒今回の規則案 など



*1: Food Engineering “The Bioterrorism Act: Essential Facts”, 2004.9.2 (https://www.foodengineeringmag.com/articles/82392-the-bioterrorism-act-essential-facts)
*2: Guidance for Industry: Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance, 2007.10 (https://www.fda.gov/regulatory-information/search-fda-(https://www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-industry-food-security-preventive-measures-guidance-food-producers-processors-and)

（参考）食品防御における規則案とガイドラインの位置づけ

- 両者とも、FDAの「食品防御ガイダンス資料・規則情報」のページに掲載（*）



- http://www.fda.gov/Food/GuidanceRegulation/GuidanceDocumentsRegulatoryInformation/FoodDefense/default.htm
- ※FDA Website構成変更によりURLが昨年より変更

15

CCFICS　New Work on the development of Guidance on the prevention and　control of food fraudについての調査 (2026年1月までの進捗)

2025年12月時点

- **近年の「食品偽装の防止及び管理に関するガイドライン」関連の主な動向　（2025年12月2日確認）**

- 第26回食品輸出入検査・認証制度部会（CCFICS26）
  2023年5月1日～5日開催 @オーストラリア ホバート
  CCFICS26th session （2023May1-5）
- 第107回コーデックス連絡協議会
  2023年9月8日開催　@東京AP虎ノ門（ハイブリッド開催）
  （CCFICS26について確認・議論）
  第107回コーデックス連絡協議会：農林水産省（maff.go.jp）
  第107回コーデックス連絡協議会の概要について（caa.go.jp）
- 第46回　コーデックス総会（CAC46）
  2023年１１月２７日～１２月２日開催 @イタリア ローマ＆Web
  CAC46 | CODEXALIMENTARIUS FAO-WHO
  meeting-detail | CODEXALIMENTARIUS FAO-WHO
- 第27回食品輸出入検査・認証制度部会（CCFICS27）
  2024/9/16～20開催@オーストラリア ケアンズ
  https://gforss.org/wp-content/uploads/2024/10/EN_CCFICS27_GFoRSS_vf.pdf?utm_source=chatgpt.com
  https://www.fao.org/fao-who-codexalimentarius/committees/committee/related-meetings/en/?committee=CCFICS
- 第47回コーデックス総会（CAC47）
  2024/11/25~30開催@スイス ジュネーブ
  https://www.fao.org/fao-who-codexalimentarius/news-and-events/news-details/en/c/1727810/?utm_source=chatgpt.com

CCFICS電子作業部会（EWG）による
「食品偽装の防止及び管理に関するガイドライン」草案作成作業

EWG議長国：米国、共同議長国：英国、中国、EU、イラン

CCFICS電子作業部会の作業計画（タイムテーブル）
- 2023年10月 EWGへの初回草案
- 2023年11月 コメント提出期限
- 2024年2月初旬 ドラフト2をEWGに提出
- 2024年3月中旬 コメント提出期限
- 2024年5月 会議用文書案をEWGに提出
- 2024年6月 会議用文書提出
- 2024年9月 CCFICS 27

CCFICS27 での検討のため、CCFICS26 で提出された全ての議論とコメント（角括弧内の文章を含む）を考慮し、食品偽装の防止と規制に関するCCFICS26 総会の編集版を使用し、ステップ２ガイドラインの改訂草案を作成する。

Microsoft Word - FoodFraud_EWG_invitation_e_062023 (fao.org)
https://www.fao.org/fao-who-codexalimentarius/committees/ewg/detail/en/c/1644731/

【2025年12月に追加で確認された事項（一般公開情報）】
・EWG は 2025 年も継続して活動実施（Codex 公開資料により確認）
https://www.fao.org/fao-who-codexalimentarius/committees/ewg/detail/en/c/1644731/
・EWG 参加国登録案内（2025/1/15 締切）が公開
https://www.fao.org/fao-who-codexalimentarius/committees/ewg/detail/en/c/1644731/
【2025年時点の最新公開状況】
・最新公開ドラフトは 2024 年 CAC47（Step 5採択）版であり、2025 年には新たな公開版は確認されていない
https://www.fao.org/fao-who-codexalimentarius/committees/cac/meetings/en/

https://www.fao.org/fao-who-codexalimentarius/committees/committee/related-meetings/en/?committee=CCFICS
https://www.fao.org/fao-who-codexalimentarius/committees/committee/related-meetings/en/?committee=CAC

2023年以降の見通し

- 食品偽装に関するガイダンスの完成目標　→　2024年または2025年・・・Codex委員会
  ➢2025年の完成までに開発中の複数の草案が出される見込み

- 電子作業部会（議長国：米国、共同議長国：中国、EU、イラン、および英国）が設置され、次回のCCFICS26部会（2023年5月開催予定）での議論に向け食品偽装に関するガイダンス草案を検討中
  ➢電子作業部会キックオフ時の計画書によると、次回のCCFICS26部会（2023年5月開催予定）の3か月前の2023年2月頃に草案が出る見込みことが予想される。
  ➢それに伴い、電子作業部会の会合が開催される可能性がある。（EWG は、未解決の問題に対処するために CCFICS26 の前に会合することができ、CCFICS26 の 3 か月前に EWG の報告書を提出し、他の関連するコーデックス委員会に 新しい作業の進捗状況を通知し続ける。）

2025年1月時点(1/2)

2025年1月現在、「食品偽装の防止及び管理に関するガイドライン」の策定は、コーデックス委員会の下で引き続き進行中です。このガイドラインは、食品偽装の防止と管理を目的としており、消費者の健康保護と食品貿易の公正性を確保することを目指しています。

進捗状況（2025年1月時点）:

- **第27回食品輸出入検査・認証制度部会（CCFICS27）の開催**: 2024年9月にオーストラリアのケアンズで開催され、食品偽装の防止及び管理に関するガイドライン原案がステップ4として検討されました。この会合では、電子的作業部会およびバーチャルワークショップを経て作成された討議文書を基にガイドラインの目的、範囲、定義、食品偽装の種類、原則、役割と責務、当局による関連活動、当局間の協力及び情報共有などが議論されました。
- **ガイドラインの進捗:** CCFICS27では、食品偽装の防止及び管理に関するガイドラインの草案が詳細に検討され、いくつかの修正提案が行われました。これらの提案は、ガイドラインの明確化と実効性の向上を目的としています。
- **第47回コーデックス委員会（CAC47）**: 2024年11月に開催され、CCFICS27での議論を踏まえ、ガイドライン原案がステップ5として採択されました。これにより、ガイドライン策定プロセスは次の段階へと進み、最終的な承認に向けた準備が進められています。
- **今後のステップ:** 電子作業部会（EWG）がステップ6でのコメントおよび未解決事項を検討し、必要に応じて会合を開催のうえ、2026年開催予定のCCFICS28の3か月前までに報告書を提出することが合意されています。
- **主な重要ポイント:**

1. **目的と適用範囲**: ガイドラインは、食品偽装の防止、検出、緩和、および管理に関する指針を提供し、消費者の健康保護と食品貿易の公正性を確保することを目的としています。適用範囲は、食品および飼料の生産、輸送、輸出入、販売を含むサプライチェーン全体に及びます。
2. **食品偽装の定義と分類**: ガイドラインでは、食品偽装を以下のように分類しています。
    1. 添加（Addition）: 未申告の物質を食品に加える行為。
    2. 代替（Substitution）: 高価な成分を低価な別の成分で置き換える行為。
    3. 虚偽表示（Misrepresentation）: 製品の内容や品質について誤解を招く表示を行う行為。
    4. 隠蔽（Concealment）: 製品の欠陥や品質低下を隠す行為。

https://www.fao.org/fao-who-codexalimentarius/news-and-events/news-details/en/c/1710359/?utm_source=chatgpt.com
https://www.fao.org/fao-who-codexalimentarius/news-and-events/news-details/en/c/1710762/?utm_source=chatgpt.com
https://www.fao.org/fao-who-codexalimentarius/sh-proxy/jp/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-27%252FFinal%252520report%252FREP24_FICSe.pdf&utm_source=chatgpt.com

2025年1月時点(2/2)

3.予防的アプローチの推進: ガイドラインは、食品偽装を未然に防ぐため、リスク評価を重視しています。また、サプライチェーン全体にわたるモニタリング体制の強化を推奨しています。

4.政府と業界の役割:

1. 政府機関: 食品偽装に関連する基準の策定、執行、監督を担います。
2. 事業者: リスクに応じた対策を導入し、予防策を講じることが求められています。

国際的な取り組み:

欧州連合（EU）では、食品偽装防止のための取り組みが強化されています。例えば、2024年9月には、消費者が食品の原産地情報を明確に知ることができるよう、新たなラベル表示の導入が提案されました。この取り組みは、消費者の権利保護と食品偽装の撲滅を目的としています。

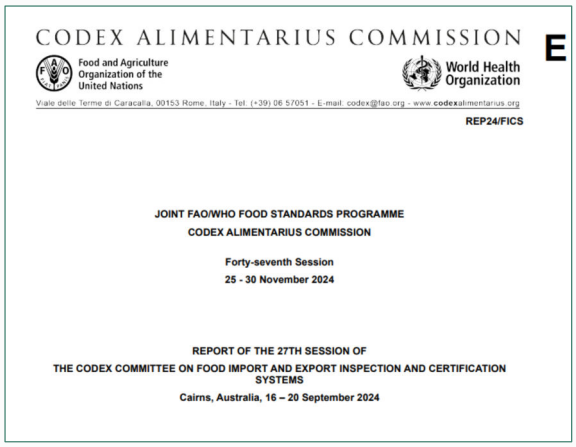
今後の展望:

本ガイドラインは、2024年のCAC47においてステップ5として採択されました。現在、未解決事項の整理や各国から提出された意見の検討が電子作業部会により進められており、その結果は2026年10月に開催予定のCCFICS28に報告され、ステップ7として再審議される見通しです。今後は、同部会での検討結果を踏まえ、Codex委員会において最終採択（ステップ8）が行われる予定です。

https://www.caa.go.jp/policies/policy/consumer_safety/meeting_materials/assets/consumer_safety_cms203_240926_01.pdf?utm_source=chatgpt.com
https://www.fao.org/fao-who-codexalimentarius/committees/committee/related-meetings/en/?committee=CCFICS&utm_source=chatgpt.com
https://www.huffingtonpost.es/life/consumo/basta-comida-falsa-nueva-etiqueta-supermercado-acaba-10-alimentos-mas-falsificados.html?utm_source=chatgpt.com
https://www.fao.org/fao-who-codexalimentarius/sh-proxy/jp/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-27%252FFinal%252520report%252FREP24_FICSe.pdf&utm_source=chatgpt.com

2025年1月時点　第27回食品輸出入検査・認証制度部会（CCFICS27）公式報告書

CCFICS27では、食品偽装の防止及び管理に関するガイドラインの草案が詳細に検討され、(1)知的財産に関する記載の除外,(2)電子的作業部会の設置などの修正提案が行われました。



CODEX ALIMENTARIUS COMMISSION

E

Food and Agriculture Organization of the United Nations

World Health Organization

Viale delle Terme di Caracalla, 00153 Rome, Italy - Tel: (+39) 06 57051 - E-mail: codex@fao.org - www.codexalimentarius.org

REP24/FICS

JOINT FAO/WHO FOOD STANDARDS PROGRAMME

CODEX ALIMENTARIUS COMMISSION

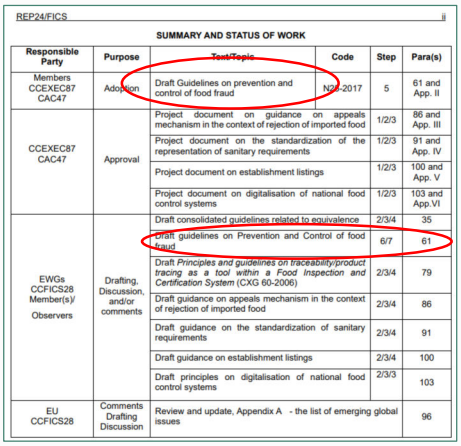
Forty-seventh Session

25 - 30 November 2024

REPORT OF THE 27TH SESSION OF

THE CODEX COMMITTEE ON FOOD IMPORT AND EXPORT INSPECTION AND CERTIFICATION SYSTEMS

Cairns, Australia, 16 – 20 September 2024



REP24/FICS

SUMMARY AND STATUS OF WORK

Responsible Party	Purpose	Text/Topic	Code	Step	Para(s)
Members CCEXEC87 CAC47	Adoption	Draft Guidelines on prevention and control of food fraud	N06-2017	5	61 and App. II
CCEXEC87 CAC47	Approval	Project document on guidance on appeals mechanism in the context of rejection of imported food		1/2/3	86 and App. III
		Project document on the standardization of the representation of sanitary requirements		1/2/3	91 and App. IV
		Project document on establishment listings		1/2/3	100 and App. V
		Project document on digitalisation of national food control systems		1/2/3	103 and App.VI
EWGs CCFICS28 Member(s)/ Observers	Drafting, Discussion, and/or comments	Draft consolidated guidelines related to equivalence		2/3/4	35
		Draft guidelines on Prevention and Control of food fraud		6/7	61
		Draft *Principles and guidelines on traceability/product tracing as a tool within a Food Inspection and Certification System* (CXG 60-2006)		2/3/4	79
		Draft guidance on appeals mechanism in the context of rejection of imported food		2/3/4	86
		Draft guidance on the standardization of sanitary requirements		2/3/4	91
		Draft guidance on establishment listings		2/3/4	100
		Draft principles on digitalisation of national food control systems		2/3/3	103
EU CCFICS28	Comments Drafting Discussion	Review and update, Appendix A - the list of emerging global issues			96

(1)知的財産に関する記載の除外: ガイドラインの対象範囲から、地理的表示（GI）などの知的財産に関連する事項を除外することが合意されました。

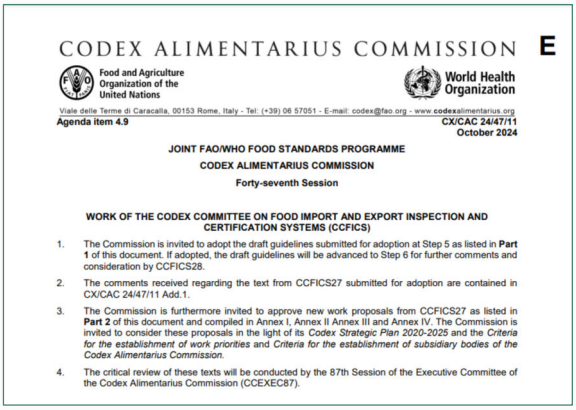
(2)電子的作業部会の設置: ガイドライン原案の改訂を進めるため、電子的作業部会（EWG）が設置されることが決定されました。この作業部会は、米国が議長国を務め、英国、中国、EU、イラン、パナマが共同議長国として参加します。

https://www.fao.org/fao-who-codexalimentarius/sh-proxy/jp/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-27%252FFinal%252520report%252FREP24_FICSe.pdf&utm_source=chatgpt.com

2025年1月時点　第47回コーデックス委員会報告書 CAC47　Report of CCFICS27

CCFICS27（第27回食品輸入・輸出検査認証システムに関するコーデックス委員会）で策定された食品防御に関するガイドライン原案がステップ5としてCAC47（第47回コーデックス委員会）で採択されました。具体的には、食品不正の予防と管理に関するガイドラインがCCFICS27で大幅に進展し、CAC47での採択に向けて送付されました。

https://www.fao.org/fao-who-codexalimentarius/news-and-events/news-details/en/c/1710762/?utm_source=chatgpt.com



CODEX ALIMENTARIUS COMMISSION

E

Food and Agriculture Organization of the United Nations

World Health Organization

Viale delle Terme di Caracalla, 00153 Rome, Italy - Tel: (+39) 06 57051 - E-mail: codex@fao.org - www.codexalimentarius.org

Agenda item 4.9

CX/CAC 24/47/11

October 2024

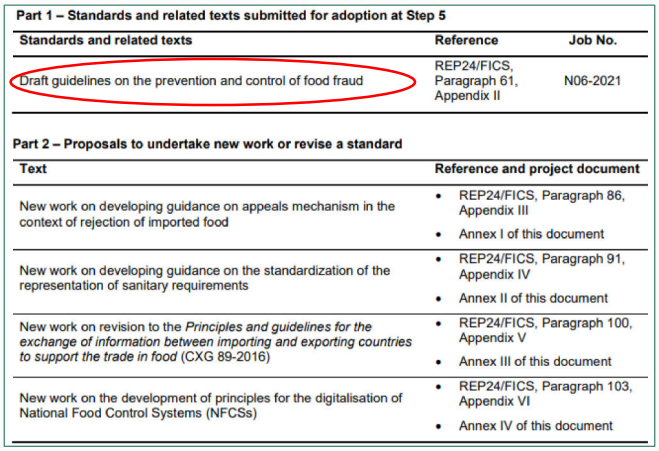
JOINT FAO/WHO FOOD STANDARDS PROGRAMME

CODEX ALIMENTARIUS COMMISSION

Forty-seventh Session

WORK OF THE CODEX COMMITTEE ON FOOD IMPORT AND EXPORT INSPECTION AND CERTIFICATION SYSTEMS (CCFICS)

1. The Commission is invited to adopt the draft guidelines submitted for adoption at Step 5 as listed in **Part 1** of this document. If adopted, the draft guidelines will be advanced to Step 6 for further comments and consideration by CCFICS28.
2. The comments received regarding the text from CCFICS27 submitted for adoption are contained in CX/CAC 24/47/11 Add.1.
3. The Commission is furthermore invited to approve new work proposals from CCFICS27 as listed in **Part 2** of this document and compiled in Annex I, Annex II Annex III and Annex IV. The Commission is invited to consider these proposals in the light of its *Codex Strategic Plan 2020-2025* and the *Criteria for the establishment of work priorities and Criteria for the establishment of subsidiary bodies of the Codex Alimentarius Commission*.
4. The critical review of these texts will be conducted by the 87th Session of the Executive Committee of the Codex Alimentarius Commission (CCEXEC87).



Part 1 – Standards and related texts submitted for adoption at Step 5

Standards and related texts	Reference	Job No.
Draft guidelines on the prevention and control of food fraud	REP24/FICS, Paragraph 61, Appendix II	N06-2021

Part 2 – Proposals to undertake new work or revise a standard

Text	Reference and project document
New work on developing guidance on appeals mechanism in the context of rejection of imported food	• REP24/FICS, Paragraph 86, Appendix III • Annex I of this document
New work on developing guidance on the standardization of the representation of sanitary requirements	• REP24/FICS, Paragraph 91, Appendix IV • Annex II of this document
New work on revision to the *Principles and guidelines for the exchange of information between importing and exporting countries to support the trade in food* (CXG 89-2016)	• REP24/FICS, Paragraph 100, Appendix V • Annex III of this document
New work on the development of principles for the digitalisation of National Food Control Systems (NFCSs)	• REP24/FICS, Paragraph 103, Appendix VI • Annex IV of this document

https://www.fao.org/fao-who-codexalimentarius/sh-proxy/en/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-701-47%252FWorking%2BDocuments%252Fcac47_11e.pdf

【参考】第27回食品輸出入検査・認証制度部会（CCFICS27）の主な検討議題

第27回コーデックス食品輸出入検査・認証制度部会（CCFICS27）で検討された主な議題と、それぞれに関連する情報ソースは以下の通りです：

（１）食品偽装の防止と管理に関するガイドラインの策定
- •食品偽装（Food Fraud）の防止と管理に関する新たなガイドラインの策定が議論されました。
(参考)Tomorrow's Food and Feed

（２）輸出入食品の検査・認証システムにおけるデジタル技術の活用
- •食品貿易におけるデジタル技術の導入に関する議論が行われました。
(参考)食品規制科学協会

（３）食品安全のための緊急措置に関するガイドラインの更新
- •食品安全問題への迅速な対応を確保するためのプロトコル改訂が検討されました。
(参考)食品規制科学協会

（４）コンプライアンスと透明性の確保
- •輸出入食品検査制度におけるコンプライアンス基準と透明性向上のための提案が議論されました。
(参考)食品規制科学協会

（５）政府間の協力と情報共有の強化
- •食品の安全性と公正な貿易を確保するための各国政府間での情報共有と協力体制の拡大が推進されました。
(参考)食品規制科学協会

（６）食品の追跡可能性（トレーサビリティ）に関する要件
- •食品のトレーサビリティに関する新たな基準や要求事項の検討が行われました。
(参考)食品規制科学協会

【参考】第26回食品輸出入検査・認証制度部会（CCFICS）の主な検討議題より

仮議題6
食品偽装の防止及び管理に関するガイダンス原案（ステップ4）

食品システムの複雑化と食品の世界的な貿易取引により、食品サプライチェーンは食品偽装に対して脆弱になっており、食品安全当局、関係機関及び食品事業者に対して食品偽装の探知、防止、緩和及び管理に関する実用的なガイダンスを提供する。

主な論点

・ガイダンス原案は①序論、②目的／範囲、③定義、④食品偽装の種類、⑤原則、⑥役割と責務、⑦当局による関連活動、⑧当局間の協力及び情報共有の構成となっており、⑤～⑦のセクションは、作業部会では概ねコンセンサスが得られている。
・目的／範囲に知的財産及び危害を加えること目的とした食品への意図的混入に関する記載を含めるか。
・定義及び食品偽装の種類に含めるべきは何か。

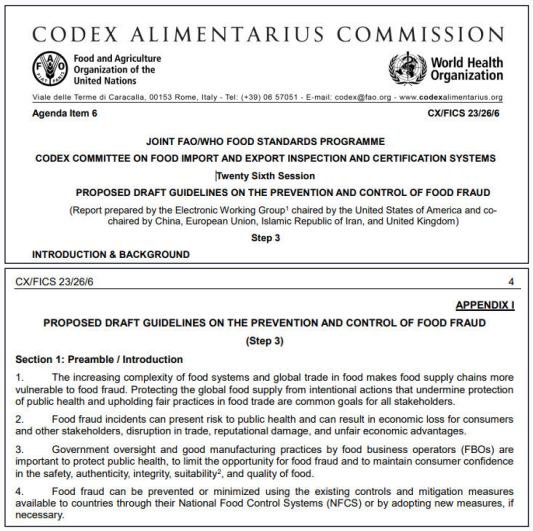
対処方針

・食品偽装が関連する分野は広いことから、本部会の所掌範囲である消費者の健康保護及び食品貿易の公正な取引の保証のために、必要な範囲を本ガイダンスの対象とすべきとの立場で対処したい。

13

第 105 回コーデックス連絡協議会（2023年4月26日、資料１より）（https://www.maff.go.jp/j/syouan/kijun/codex/attach/pdf/105-4.pdf ）

【参考】ガイドライン案の公表（未定稿）



CODEX ALIMENTARIUS COMMISSION

Food and Agriculture Organization of the United Nations

World Health Organization

Viale delle Terme di Caracalla, 00153 Rome, Italy - Tel: (+39) 06 57051 - E-mail: codex@fao.org - www.codexalimentarius.org

Agenda Item 6 CX/FICS 23/26/6

JOINT FAO/WHO FOOD STANDARDS PROGRAMME

CODEX COMMITTEE ON FOOD IMPORT AND EXPORT INSPECTION AND CERTIFICATION SYSTEMS

Twenty Sixth Session

PROPOSED DRAFT GUIDELINES ON THE PREVENTION AND CONTROL OF FOOD FRAUD

(Report prepared by the Electronic Working Group[1] chaired by the United States of America and co-chaired by China, European Union, Islamic Republic of Iran, and United Kingdom)

Step 3

INTRODUCTION & BACKGROUND

CX/FICS 23/26/6 4

APPENDIX I

PROPOSED DRAFT GUIDELINES ON THE PREVENTION AND CONTROL OF FOOD FRAUD

(Step 3)

Section 1: Preamble / Introduction

1. The increasing complexity of food systems and global trade in food makes food supply chains more vulnerable to food fraud. Protecting the global food supply from intentional actions that undermine protection of public health and upholding fair practices in food trade are common goals for all stakeholders.

2. Food fraud incidents can present risk to public health and can result in economic loss for consumers and other stakeholders, disruption in trade, reputational damage, and unfair economic advantages.

3. Government oversight and good manufacturing practices by food business operators (FBOs) are important to protect public health, to limit the opportunity for food fraud and to maintain consumer confidence in the safety, authenticity, integrity, suitability[2], and quality of food.

4. Food fraud can be prevented or minimized using the existing controls and mitigation measures available to countries through their National Food Control Systems (NFCS) or by adopting new measures, if necessary.

ガイドライン案の構成

Section 1: Preamble / Introduction
Section 2: Purpose / Scope
Section 3: Definitions
Section 4: Types of food fraud:
Section 5: Principles
Section 6: Roles and Responsibilities
Section 7: Relevant Activities for Competent Authorities
Section 8: [Cooperation] [Collaboration] and exchange of information between competent authorities

https://www.fao.org/fao-who-codexalimentarius/sh-proxy/en/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-26%252FWorking%2BDocuments%252Ffc26_06e.pdf

鬼武先生からご紹介いただいた資料

CCFICS New Work on the development of Guidance on the prevention and control of food fraudについての調査
昨年度(R3年度)鬼武委員よりご紹介。今村委員より、調査の指示あり。

- CODEX ALIMENTARIUS 委員会 第25回
- https://www.fao.org/fao-who-codexalimentarius/sh-proxy/jp/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-25%252FFinal%252520Report%252FREP21_FICSe.pdf
- JOINT FAO/WHO FOOD STANDARDS PROGRAMME CODEX ALIMENTARIUS COMMISSION
- Forty-fourth Session 8-13 November 2021（CAC44）
- REPORT OF THE 25TH SESSION OF
- THE CODEX COMMITTEE ON FOOD IMPORT AND EXPORT INSPECTION AND CERTIFICATION SYSTEMS（CCFICS25）
- Virtual, 31 May – 8 June 2021

CODEX ALIMENTARIUS COMMISSION E

2024年1月時点

- 現状確認された「食品偽装の防止及び管理に関するガイドライン」についての主な重要ポイント（2024年1月時点）

■地理的表示保護制度（GI）を含む知的財産の扱いについて

- 「食品偽装の防止及び管理に関するガイドライン」について、地理的表示保護制度（GI）を含む知的財産に関する記載をコーデックス及びCCFICSの所掌範囲とすべきか否か、各国認識の違いから意見が分かれ、議論の余地があることが明らかになった。これについてはCAC執行部に助言を求めるとともに電子作業部会（EWG）で継続検討となった。
- この背景にはGIの保護を拡充したい国々（EU）と、 これに反対し従来通りWTO の「知的所有権の貿易関連の側面に関する協定（TRIPS）」の範囲とすべきとする国々（米国）の対立構造がある。
- 我が国はGI に関する議論はコーデックスの所掌範囲外の立場（これまで通りTRIPS等で議論すべきとの立場）。
- 仮に GI が当ガイドラインの対象となった場合にも、 直ちに日本に影響はないと思われるが、日本の制度や食品貿易に影響を及ぼすガイドラインとならないよう、引き続き注視する必要がある。

■食品偽装の議論の進め方、対象範囲について

- 食品偽装はCCFICSだけでなく部門横断的で広範な課題であるが、議論の進め方について、まずはCCFICSで消費者の健康保護と食品の輸出入における公正な取引の保証に必要な範囲を対象として検討し、検討状況を関連他部門（CCFLやCCMAS等）に情報共有する、ということが確認された（CCGP31でも確認）。

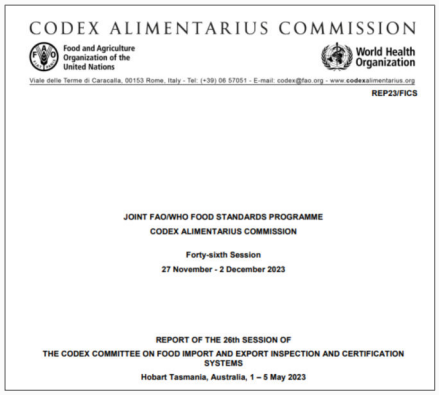
■「食品偽装の防止及び管理に関するガイドライン」の今後

- ガイドライン原案をステップ2/3に戻し、CCFICS26 で提出された全ての議論とコメント（角括弧内の文章を含む）を考慮し、次回CCFICS27会合（2024年9月16日～20日開催予定）までに改訂草案を作成することとなった。
- 改訂版の作成は電子作業部会（EWG議長国：米国、共同議長国：英国、中国、EU、イラン）が作業を進める。

出所） 第107回コーデックス連絡協議会：農林水産省（maff.go.jp)、第107回コーデックス連絡協議会の概要について（caa.go.jp) 105-4.pdf (maff.go.jp)

2024年1月時点　第46回コーデックス委員会報告書 CAC46　Report of CCFICS26

- 第46回コーデックス委員会(CAC46)が2023年11月27日～12月2日に開催され、そこで第26回 食品輸入管理・認証制度部会(CCFICS26)の提案についての採択と承認がなされた。



CODEX ALIMENTARIUS COMMISSION

Food and Agriculture Organization of the United Nations

World Health Organization

Viale delle Terme di Caracalla, 00153 Rome, Italy - Tel: (+39) 06 57051 - E-mail: codex@fao.org - www.codexalimentarius.org

REP23/FICS

JOINT FAO/WHO FOOD STANDARDS PROGRAMME

CODEX ALIMENTARIUS COMMISSION

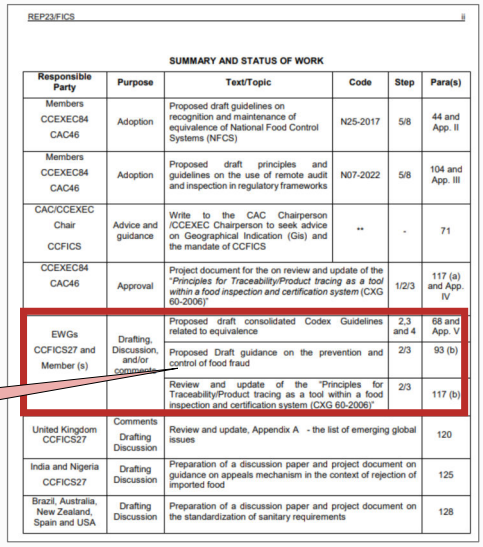
Forty-sixth Session

27 November - 2 December 2023

REPORT OF THE 26th SESSION OF THE CODEX COMMITTEE ON FOOD IMPORT AND EXPORT INSPECTION AND CERTIFICATION SYSTEMS

Hobart Tasmania, Australia, 1 – 5 May 2023

食品偽装の防止と管理に関するガイドライン草案の提出　ステップ2/3



REP23/FICS ii

SUMMARY AND STATUS OF WORK

Responsible Party	Purpose	Text/Topic	Code	Step	Para(s)
Members CCEXEC84 CAC46	Adoption	Proposed draft guidelines on recognition and maintenance of equivalence of National Food Control Systems (NFCS)	N25-2017	5/8	44 and App. II
Members CCEXEC84 CAC46	Adoption	Proposed draft principles and guidelines on the use of remote audit and inspection in regulatory frameworks	N07-2022	5/8	104 and App. III
CAC/CCEXEC Chair CCFICS	Advice and guidance	Write to the CAC Chairperson /CCEXEC Chairperson to seek advice on Geographical Indication (GIs) and the mandate of CCFICS	**	-	71
CCEXEC84 CAC46	Approval	Project document for the on review and update of the "*Principles for Traceability/Product tracing as a tool within a food inspection and certification system* (CXG 60-2006)"		1/2/3	117 (a) and App. IV
EWGs CCFICS27 and Member (s)	Drafting, Discussion, and/or comments	Proposed draft consolidated Codex Guidelines related to equivalence		2,3 and 4	68 and App. V
		Proposed Draft guidance on the prevention and control of food fraud		2/3	93 (b)
		Review and update of the "Principles for Traceability/Product tracing as a tool within a food inspection and certification system (CXG 60-2006)"		2/3	117 (b)
United Kingdom CCFICS27	Comments Drafting Discussion	Review and update, Appendix A - the list of emerging global issues			120
India and Nigeria CCFICS27	Drafting Discussion	Preparation of a discussion paper and project document on guidance on appeals mechanism in the context of rejection of imported food			125
Brazil, Australia, New Zealand, Spain and USA	Drafting Discussion	Preparation of a discussion paper and project document on the standardization of sanitary requirements			128

https://www.fao.org/fao-who-codexalimentarius/sh-proxy/pt/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-26%252FFinal%252520Report%252FREP23_FICSe.pdf

2024年1月時点　第46回コーデックス委員会報告書
CAC46　Report of CCFICS26

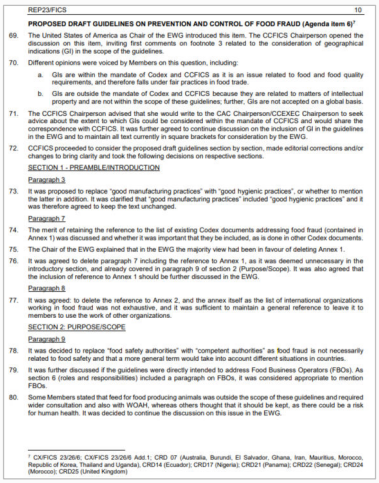
TABLE OF CONTENTS

- 報告書目次「食品偽装の防止と管理に関するガイドライン」に関する記載箇所はパラグラフ69-93。

https://www.fao.org/fao-who-codexalimentarius/sh-proxy/pt/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-26%252FFinal%252520Report%252FREP23_FICSe.pdf

2024年1月時点　第46回コーデックス委員会報告書
CAC46　Report of CCFICS26

- 報告書内「食品偽装の防止と管理に関するガイドライン」に関する記載箇所、パラグラフ69-93 。



REP23/FICS 10

PROPOSED DRAFT GUIDELINES ON PREVENTION AND CONTROL OF FOOD FRAUD (Agenda item 6)[7]

69. The United States of America as Chair of the EWG introduced this item. The CCFICS Chairperson opened the discussion on this item, inviting first comments on footnote 3 related to the consideration of geographical indications (GI) in the scope of the guidelines.

70. Different opinions were voiced by Members on this question, including:

a. GIs are within the mandate of Codex and CCFICS as it is an issue related to food and food quality requirements, and therefore falls under fair practices in food trade.

b. GIs are outside the mandate of Codex and CCFICS because they are related to matters of intellectual property and are not within the scope of these guidelines; further, GIs are not accepted on a global basis.

71. The CCFICS Chairperson advised that she would write to the CAC Chairperson/CCEXEC Chairperson to seek advice about the extent to which GIs could be considered within the mandate of CCFICS and would share the correspondence with CCFICS. It was further agreed to continue discussion on the inclusion of GI in the guidelines in the EWG and to maintain all text currently in square brackets for consideration by the EWG.

72. CCFICS proceeded to consider the proposed draft guidelines section by section, made editorial corrections and/or changes to bring clarity and took the following decisions on respective sections.

SECTION 1 - PREAMBLE/INTRODUCTION

Paragraph 3

73. It was proposed to replace "good manufacturing practices" with "good hygienic practices", or whether to mention the latter in addition. It was clarified that "good manufacturing practices" included "good hygienic practices" and it was therefore agreed to keep the text unchanged.

Paragraph 7

74. The merit of retaining the reference to the list of existing Codex documents addressing food fraud (contained in Annex 1) was discussed and whether it was important that they be included, as is done in other Codex documents.

75. The Chair of the EWG explained that in the EWG the majority view had been in favour of deleting Annex 1.

76. It was agreed to delete paragraph 7 including the reference to Annex 1, as it was deemed unnecessary in the introductory section, and already covered in paragraph 9 of section 2 (Purpose/Scope). It was also agreed that the inclusion of reference to Annex 1 should be further discussed in the EWG.

Paragraph 8

77. It was agreed: to delete the reference to Annex 2, and the annex itself as the list of international organizations working in food fraud was not exhaustive, and it was sufficient to maintain a general reference to leave it to members to use the work of other organizations.

SECTION 2: PURPOSE/SCOPE

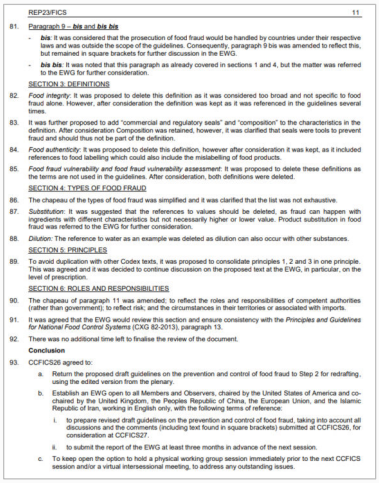
Paragraph 9

78. It was decided to replace "food safety authorities" with "competent authorities" as food fraud is not necessarily related to food safety and that a more general term would take into account different situations in countries.

79. It was further discussed if the guidelines were directly intended to address Food Business Operators (FBOs). As section 6 (roles and responsibilities) included a paragraph on FBOs, it was considered appropriate to mention FBOs.

80. Some Members stated that feed for food producing animals was outside the scope of these guidelines and required wider consultation and also with WOAH, whereas others thought that it should be kept, as there could be a risk for human health. It was decided to continue the discussion on this issue in the EWG.

[7] CX/FICS 23/26/6; CX/FICS 23/26/6 Add.1; CRD 07 (Australia, Burundi, El Salvador, Ghana, Iran, Mauritius, Morocco, Republic of Korea, Thailand and Uganda); CRD14 (Ecuador); CRD17 (Nigeria); CRD21 (Panama); CRD22 (Senegal); CRD24 (Morocco); CRD25 (United Kingdom)



REP23/FICS 11

81. Paragraph 9 – ***bis*** and ***bis bis***

- ***bis***: It was considered that the prosecution of food fraud would be handled by countries under their respective laws and was outside the scope of the guidelines. Consequently, paragraph 9 bis was amended to reflect this, but remained in square brackets for further discussion in the EWG.
- ***bis bis***: It was noted that this paragraph as already covered in sections 1 and 4, but the matter was referred to the EWG for further consideration.

SECTION 3: DEFINITIONS

82. *Food integrity*: It was proposed to delete this definition as it was considered too broad and not specific to food fraud alone. However, after consideration the definition was kept as it was referenced in the guidelines several times.

83. It was further proposed to add "commercial and regulatory seals" and "composition" to the characteristics in the definition. After consideration Composition was retained, however, it was clarified that seals were tools to prevent fraud and should thus not be part of the definition.

84. *Food authenticity*: It was proposed to delete this definition, however after consideration it was kept, as it included references to food labelling which could also include the mislabelling of food products.

85. *Food fraud vulnerability and food fraud vulnerability assessment*: It was proposed to delete these definitions as the terms are not used in the guidelines. After consideration, both definitions were deleted.

SECTION 4: TYPES OF FOOD FRAUD

86. The chapeau of the types of food fraud was simplified and it was clarified that the list was not exhaustive.

87. *Substitution*: It was suggested that the references to values should be deleted, as fraud can happen with ingredients with different characteristics but not necessarily higher or lower value. Product substitution in food fraud was referred to the EWG for further consideration.

88. *Dilution*: The reference to water as an example was deleted as dilution can also occur with other substances.

SECTION 5: PRINCIPLES

89. To avoid duplication with other Codex texts, it was proposed to consolidate principles 1, 2 and 3 in one principle. This was agreed and it was decided to continue discussion on the proposed text at the EWG, in particular, on the level of prescription.

SECTION 6: ROLES AND RESPONSIBILITIES

90. The chapeau of paragraph 11 was amended, to reflect the roles and responsibilities of competent authorities (rather than government), to reflect risk, and the circumstances in their territories or associated with imports.

91. It was agreed that the EWG would review this section and ensure consistency with the *Principles and Guidelines for National Food Control Systems* (CXG 82-2013), paragraph 13.

92. There was no additional time left to finalise the review of the document.

Conclusion

93. CCFICS26 agreed to:

a. Return the proposed draft guidelines on the prevention and control of food fraud to Step 2 for redrafting, using the edited version from the plenary.

b. Establish an EWG open to all Members and Observers, chaired by the United States of America and co-chaired by the United Kingdom, the Peoples Republic of China, the European Union, and the Islamic Republic of Iran, working in English only, with the following terms of reference:

i. to prepare revised draft guidelines on the prevention and control of food fraud, taking into account all discussions and the comments (including text found in square brackets) submitted at CCFICS26, for consideration at CCFICS27.

ii. to submit the report of the EWG at least three months in advance of the next session.

c. To keep open the option to hold a physical working group session immediately prior to the next CCFICS session and/or a virtual intersessional meeting, to address any outstanding issues.

https://www.fao.org/fao-who-codexalimentarius/sh-proxy/pt/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-733-26%252FFinal%252520Report%252FREP23_FICSe.pdf

2024年1月時点 第107回コーデックス連絡協議会における、第２６回食品輸出入検査・認証制度部会（CCFICS）に関する記載

第107回コーデックス連絡協議会（2023年9月8日開催）において、第２６回食品輸出入検査・認証制度部会（ CCFICS26、2023年5月1日～5日開催）について確認された。「食品偽装の防止と管理に関するガイドライン」に関する記載を以下抜粋。

食品輸出入検査・認証制度部会（CCFICS）の今後の作業

事項	今後のアクション
国の食品管理システムの同等性の承認及び維持に関するガイドライン原案	CAC46（ステップ５/８）
規制枠組みにおける適領監査及び監視利用に関する原則及びガイドライン原案	CAC46（ステップ５/８）
「食品検査・認証制度におけるツールとしてのトレーサビリティ/製品トレーシングの原則(CXG 60-2006)」の更新及び改訂に関する討議文書	ステップ１ CAC46（新規作業の提案）
同等性に係るガイドラインの統合原案	ステップ２/３ 電子的作業部会（議長国：ニュージーランド、共同議長国：米国及びケニア）
食品偽装の防止及び管理に関するガイドライン原案	ステップ２/３ 電子的作業部会（議長国：米国、共同議長国：英国、中国、EU 及びイラン） CCFICS 議長は CAC 及び執行委員会の議長宛に GI は CCFICS の所掌範囲に含まれるか助言を要請。
付属書 A（CCFICS をとりまく新たな世界規模の問題）の見直し及び更新	文書管理国：英国 ○輸入食品の却下に関する不服申し立てメカニズムに関する討議文書及びプロジェクト文書の策定（提案国：インド、協力国：ナイジェリア） ○衛生要件の標準化に関する討議文書及びプロジェクト文書の策定（提案国：ブラジル、協力国：オーストラリア、ニュージーランド、スペイン、米国）

食品偽装の防止と管理に関するガイドライン草案 ステップ2/3

https://www.maff.go.jp/j/syouan/kijun/codex/attach/pdf/107-1.pdf

議題６：食品偽装の防止及び管理に関するガイドライン原案（ステップ４）

電子的作業部会の議長国である米国から、ガイドライン原案について説明がなされ、セクションごとに検討された。

［主な議論］

・脚注３の地理的表示保護制度（GI）を含む知的財産に関する記載について、EU をはじめとするいくつかの国からは GI は食品及び食品の品質に関わることからコーデックス及び CCFICS の所掌範囲とする意見があった。

一方で、GI は一部地域に適用されるもので、国際的に承認されたものではなく、知的財産に関してはコーデックス及び CCFICS 所掌範囲外のため、本ガイドラインからも対象外であるという意見もあった。

CCFICS 議長は CAC 及び執行委員会の議長宛に GI は CCFICS の所掌範囲に含まれるか助言を求めることとなった。また、本ガイドラインにおける GI の取扱いについては引き続き電子的作業部会でも検討することとなった。

セクション１：序論／はじめに

・食品偽装に関連する国際機関の取り組みについては、一般的な参照として残しておくこととし、パラ８の Annex ２の reference（国際機関のリスト）は削除することで合意した。

・Annex １を引用しているパラ７はセクション２のパラ９でカバーされているので不要ということで削除した。食品偽装に関するコーデックス既存の文書リスト（Annex １）の要否については、引き続き電子的作業部会で検討することとなった。

2024年1月追加分 第107回コーデックス連絡協議会における、第２６回食品輸出入検査・認証制度部会（CCFICS）に関する記載

（つづき）第107回コーデックス連絡協議会（2023年9月8日開催）において、第２６回食品輸出入検査・認証制度部会（CCFICS26、2023年5月1日～5日開催）について確認された。「食品偽装の防止と管理に関するガイドライン」に関する記載を以下抜粋。

セクション２：目的／範囲

・食品偽装に対応する機関については国の体制によって必ずしも「food safety authorities（食品安全担当局）」とは限らないため、「competent authority（当局）」に修正した。

・このガイドラインは食品事業者（FBO）を対象にしているか議論したが、セクション６（役割及び責任）に FBO に関するパラが含まれているので、ここで FBO について記述するのは適切であると考えられた。

・本ガイドラインの対象に「feed for food producing animals（食用動物のための飼料）」を含むか否か異なる意見があったが、引き続き議論することとなった。

・パラ９bis 及び bis bis についても、他のセクションとの重複などで、削除提案等があったが、電子的作業部会においてその削除意見も含め、引き続き議論することとなった。

セクション３：定義

・「Food fraud vulnerability」及び「food fraud vulnerability assessment」は本ガイドラインの中で使用されていないことから、削除することで合意された。その他の定義は、削除提案等もあったが、維持することに賛同多数だったため、軽微な修正を行った上で、維持することとなった。

セクション４：食品偽装の種類

・リストはこれに限定されるものではなく、例示であることを明確化した。

・「Substitution（置き換え）」については、異なる性質の原料などでも起こり、必ずしも価値の低いものとの置き換えとは限らないことから、「lower value」は削除した。「Dilution（希釈）」についても、必ずしも水での希釈に限らないことから、水の例示は削除した。

セクション５：原則

・重複を削除するため、原則１、２及び３を統合して、一つの原則とし、原則４と合わせて２つとした。

［結論］

本ガイドライン原案をステップ２/３に戻し、今次会合で議論された点とコメントを踏まえ、ガイドライン原案を改訂することが合意された。改訂作業は電子的作業部会を設置（議長国：米国、共同議長国：英国、中国、EU、イラン）し、次回第 27 回会合に向けて作業することが合意された。

https://www.maff.go.jp/j/syouan/kijun/codex/attach/pdf/107-1.pdf

2024年1月時点 第107回コーデックス連絡協議会における、第２６回食品輸出入検査・認証制度部会（CCFICS）に関する記載

- 第107回コーデックス連絡協議会（2023年9月8日開催）で、第２６回食品輸出入検査・認証制度部会（CCFICS）で示された「食品偽装の防止及び管理に関するガイドライン」に関して確認と議論がなされた。以下、該当箇所の文章抜粋。

・議題 6「食品偽装の防止及び管理に関するガイドライン原案」について、菅沼修 委員、森田満樹委員、山口隆司委員から、地理的表示保護制度（GI）を含む知的財産に関する記載に関して、日本は本ガイドライン原案の所掌範囲外であるとのコメントを提出しているが、その理由について質問がありました。これについて、GI に関する議論はコーデックスの所掌範囲外であり、本ガイダンスの目的には馴染まないと考えていること、仮に GI がもしこのガイドラインの対象となった場合にも、直ちに日本に影響は出ないと考えているが、日本の制度や食品貿易に影響を及ぼすガイドラインとならないよう、引き続き対応していきたい旨回答しました。

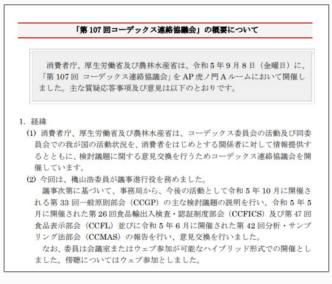
・同じく議題 6 について、菅沼修委員から、GI に関する議論に関して、本ガイドラインの所掌範囲内とすべきというEUと、所掌範囲外とすべきという米国で対立構造になっているのか、また、この議論については今後も電子的作業部会（EWG）において継続されるようだが、打開策はあるのか、質問がありました。これについ て、GI については WTO の「知的所有権の貿易関連の側面に関する協定（TRIPS）」など、他の会議体での議論においても、GI の保護を拡充しようとする国々とそれに反対する国々との間で対立構造ができており、本ガイドラインの議論でも同様の構造が見られていること、我が国としては GI についてはコーデックスではなく、これまで通り TRIPS 等で議論すべきであると考えている旨回答しました。

・同じく議題 6 について、森田満樹委員から、食品の偽装に関しては、様々な部会でバラバラに議論されている印象があるが、CCFICS のガイドラインは、今後こうした問題を包括する形で所掌していくのか、質問がありました。これについて、食品偽装については部会横断的な課題であるため、他部会からの付託事項として CCGP31 において検討の必要性について議論されたが、その際には CCGP では議論せず、まずは CCFICS において食品の輸出入における食品偽装の防止及び管理について議論することとなったこと、CCFICS の今後の検討の状況については、CCFL や CCMAS 等関連する部会に対して情報共有をすることになっている旨回答しました。

出所） 第107回コーデックス連絡協議会：農林水産省 (maff.go.jp)、第107回コーデックス連絡協議会の概要について (caa.go.jp)

2024年1月時点 第107回コーデックス連絡協議会における、第２６回食品輸出入検査・認証制度部会（CCFICS）に関する記載

（つづき）第107回コーデックス連絡協議会（2023年9月8日開催）で、第２６回食品輸出入検査・認証制度部会（CCFICS）で示された「食品偽装の防止及び管理に関するガイドライン」に関して確認と議論がなされた。以下、報告書の該当箇所。



「第 107 回コーデックス連絡協議会」の概要について

消費者庁、厚生労働省及び農林水産省は、令和５年９月８日（金曜日）に、「第 107 回 コーデックス連絡協議会」を AP 虎ノ門Ａルームにおいて開催しました。主な質疑応答事項及び意見は以下のとおりです。

1. 経緯

(1) 消費者庁、厚生労働省及び農林水産省は、コーデックス委員会の活動及び同委員会での我が国の活動状況を、消費者をはじめとする関係者に対して情報提供するとともに、検討課題に関する意見交換を行うためコーデックス連絡協議会を開催しています。

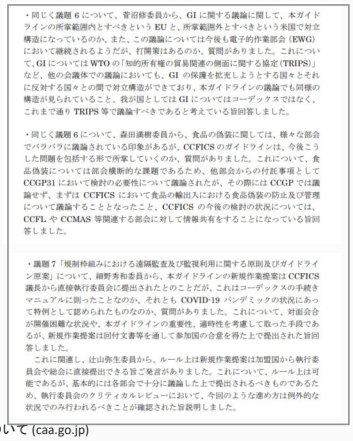
(2) 今回は、穐山浩委員が議事進行役を務めました。

議事次第に基づいて、事務局から、今後の活動として令和５年 10 月に開催される第 33 回一般原則部会（CCGP）の主な検討議題の説明を行い、令和５年５月に開催された第 26 回食品輸出入検査・認証制度部会（CCFICS）及び第 47 回食品表示部会（CCFL）並びに令和５年６月に開催された第 42 回分析・サンプリング法部会（CCMAS）の報告を行い、意見交換を行いました。

なお、委員は会議室またはウェブ参加が可能なハイブリッド形式での開催としました。傍聴についてはウェブ参加としました。

中略

・議題６「食品偽装の防止及び管理に関するガイドライン原案」について、菅沼修委員、森田満樹委員、山口隆司委員から、地理的表示保護制度（GI）を含む知的財産に関する記載に関して、日本は本ガイドライン原案の所掌範囲外であるとのコメントを提出しているが、その理由について質問がありました。これについて、GI に関する議論はコーデックスの所掌範囲外であり、本ガイダンスの目的には馴染まないと考えていること、仮に GI がもしこのガイドラインの対象となった場合にも、直ちに日本に影響は出ないと考えているが、日本の制度や食品貿易に影響を及ぼすガイドラインとならないよう、引き続き対応していきたい旨回答しました。



・同じく議題 6 について、菅沼修委員から、GI に関する議論に関して、本ガイドラインの所掌範囲内とすべきという EU と、所掌範囲外とすべきという米国で対立構造になっているのか、また、この議論については今後も電子的作業部会（EWG）において継続されるようだが、打開策はあるのか、質問がありました。これについて、GI については WTO の「知的所有権の貿易関連の側面に関する協定（TRIPS）」など、他の会議体での議論においても、GI の保護を拡充しようとする国々とそれに反対する国々との間で対立構造ができており、本ガイドラインの議論でも同様の構造が見られていること、我が国としては GI についてはコーデックスではなく、これまで通り TRIPS 等で議論すべきであると考えている旨回答しました。

・同じく議題６について、森田満樹委員から、食品の偽装に関しては、様々な部会でバラバラに議論されている印象があるが、CCFICS のガイドラインは、今後こうした問題を包括する形で所掌していくのか、質問がありました。これについて、食品偽装については部会横断的な課題であるため、他部会からの付託事項として CCGP31 において検討の必要性について議論されたが、その際には CCGP では議論せず、まずは CCFICS において食品の輸出入における食品偽装の防止及び管理について議論することとなったこと、CCFICS の今後の検討の状況については、CCFL や CCMAS 等関連する部会に対して情報共有をすることになっている旨回答しました。

・議題７「規制枠組みにおける遠隔監査及び監視利用に関する原則及びガイドライン原案」について、細野秀和委員から、本ガイドラインの新規作業提案は CCFICS 議長から直接執行委員会に提出されたとのことだが、これはコーデックスの手続きマニュアルに則ったことなのか、それとも COVID-19 パンデミックの状況にあって特例として認められたものなのか、質問がありました。これについて、対面会合が開催困難な状況や、本ガイドラインの重要性、適時性を考慮して取った手段であるが、新規作業提案は回付文書等を通して参加国の合意を得た上で提出された旨回答しました。

これに関連し、辻山弥生委員から、ルールⅡは新規作業提案は加盟国から執行委員会や総会に直接提出できる旨ご発言がありました。これについて、ルールⅡは可能であるが、基本的には各部会で十分に議論した上で提出されるべきものであるため、執行委員会のクリティカルレビューにおいて、今回のような進め方は例外的な状況でのみ行われるべきことが確認された旨説明しました。

出所） 第107回コーデックス連絡協議会：農林水産省 (maff.go.jp)、第107回コーデックス連絡協議会の概要について (caa.go.jp)

PAS 96（第5版）改訂の経緯

PAS 96（第5版）改訂の経緯と2025年の進捗

改訂の経緯

- 2023年11月：改訂作業開始
- 2025年4月：Technical Author との契約および、契約後の BSI 起草ルールに関するトレーニング実施が想定されていた
- 2025年5月末：改訂ドラフト作成（当初の暫定計画）
- 2025年秋：Steering Group による編集レビュー（当初の暫定計画）

2025年の進捗

- 2025年9月：スポンサー側との契約調整が継続しており、作業開始に至っていない旨が関係者間で共有された
- 2025年12月上旬：文書は内部レビュー段階にあると説明
- 2025年12月17日：Draft PAS 96 が公開され、パブリックコンサルテーションが開始
- Review Panel への通知は、パブリックコンサルテーション開始に合わせて実施

本スライドの内容は、BSI Standards Development Portal に掲載された公開情報および、BSI Standards 関係者との公式な連絡により確認された事実に基づく（2025年12月時点）。

出典：https://standardsdevelopment.bsigroup.com/projects/2023-02427

PAS 96（第5版）改訂とパブリックコンサルテーションの位置づけ

• パブリックコンサルテーションの制度的位置づけ

- PAS（Publicly Available Specification）は、英国規格協会（BSI）が策定する迅速な合意形成を目的としたガイド文書である
- PAS の改訂プロセスにおいて、ドラフト文書が外部公開されるのは、パブリックコンサルテーション開始時のみである
- それ以前の段階（Technical Author 作業、内部レビュー、Steering Group レビュー等）では、公開ドラフトは存在しない
- パブリックコンサルテーションは、外部ステークホルダーからの意見を収集し、最終文書に反映可否を判断する正式工程である

• 第5版改訂における今回のパブリックコンサルテーションの意味

- PAS 改訂プロセスにおいて、パブリックコンサルテーションはドラフト文書が初めて外部に提示される段階である
- 今回の第5版改訂では、内部検討を経た文書が初めて外部ステークホルダーによる検証に付される工程として実施されている
- したがって本パブリックコンサルテーションは、改訂内容の妥当性・実効性が初めて外部から評価される重要な節目に位置づけられる

本スライドの内容は、BSI Standards Development Portal に掲載された公開情報および、BSI Standards 関係者との公式な連絡により確認された事実に基づく（2025年12月時点）。

出典：https://standardsdevelopment.bsigroup.com/projects/2023-02427

PAS 96（第5版）改訂の目的と主な改訂点

• 改訂の目的（第5版）

- PAS 96 を、意図的攻撃（deliberate attack）に対する実践的な食品防御ガイドとして再整理すること
- 従来の TACCP の枠組みを維持しつつ、現代の脅威環境（デジタル化・サイバー化・複雑化したサプライチェーン）を反映すること
- 中小事業者を含む幅広い事業者が、自組織のリスクに応じて“過不足のない対策”を検討できるようにすること

• 主な改訂点・注目点（ドラフトより）

１） TACCP の実務適用を重視した構成複数のケーススタディ（Annex E）により、脅威識別・評価・対応・見直しの一連の流れを具体的に提示「文書作成」ではなく、リスクマネジメントプロセスとしての TACCP を強調（論拠：Annex E, Tables E.2–E.8）

２）サイバー・IT・遠隔操作由来の脅威の明確化デリバリー、遠隔制御、オンライン受注等を想定したケースを提示物理的混入に限らない食品防御の対象範囲を明確化（論拠：Case study（FryByNite 等）、Annex G）

３） 比例的管理（proportionate controls）の強調すべての脅威に一律対応するのではなく、影響度・発生可能性に応じた合理的な対応を推奨特に中小事業者を念頭に、過剰対策を求めない設計思想を明確化（論拠：Case study conclusions, TACCP outcomes）

本スライドの内容は、BSI Standards Development Portal に掲載された公開情報および、BSI Standards 関係者との公式な連絡により確認された事実に基づく（2025年12月時点）。

出典：PAS96　Draft（https://standardsdevelopment.bsigroup.com/projects/2023-02427）

（添付資料 2）

RE: PAS 96 - Brief update on progress

要約

返信 | 全員に返信 | 転送

Philippa Morrell
宛先 Kenichi Hojo （北條 健一）
ＣＣ Todd Redwood; Titi Susanti; Gary Wills; Kosuke Kawai （河井 宏介）; Shigeto Iccho （一蝶 茂人）; Neil Coole; Kevin Laverty; Yoshio Izumi （泉 佳夫）

2025/12/02 (火) 17:41

Public¥Public - Unmarked

フラグを設定します:
2025/12/02 19:16 にこのメッセージに返信しました。
フラグ処理などが設定されたスレッドに含まれているメッセージです。関連するすべてのメッセージを検索したり、元のフラグ付きメッセージを開くには、ここをクリックしてください。

メッセージを日本語に翻訳する | 翻訳に関する設定

Dear Hojo san

Thank you for your email.

I am pleased to confirm that we are on track to start the public consultation for PAS 96 in mid-December before the festive break. It is currently undergoing some internal reviews, before it is then sent to the sponsor for their approval.

You will be advised once it is released.

Kind regards,
Philippa

Tel: +44 (0) 1442 276262

My working hours are 0800 – 1645
Please note that I work compressed hours, with a non-working day every other week. This month, my non-working Mondays are on the 10 and 24 November.

（添付資料 3）

PAS 96 - Final reminder - Public consultation ends 1 February

Philippa Morrell
宛先

返信 | 全員に返信 | 転送 | ...

2026/01/29 (木) 18:56

Restricted¥Restricted - Marked

このメッセージは "重要度 - 高" で送信されました。

Restricted

Please be reminded that if you are planning to comment on the draft of PAS 96 **the public consultation will close on 1 February.**

If you have not already done so, to review and provide comments on the draft, please go to: https://standardsdevelopment.bsigroup.com/projects/2023-02427 New users will need to register (it is free to do so) and then log in.

If you are experiencing problems understanding how to leave feedback via the SDP, here is a help guide on how to submit comments: https://standardsdevelopment.bsigroup.com/Home/Help

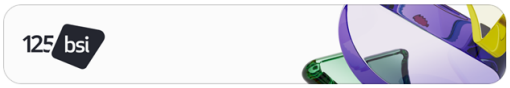
When making a comment please also provide a proposal for how your comment could be resolved.

Many thanks and kind regards,
Philippa

Philippa J.K. Morrell (she/her)
Editorial Project Manager
Tel: +44 (0) 1442 276262
philippa.morrell@bsigroup.com

My working hours are 0800 – 1645
Please note that I work compressed hours, with a non-working day every other week. This month, my non-working day is 23 January.

BSI, The Acre, 90 Long Acre, London, WC2E 9RA
bsigroup.com | LinkedIn



（添付資料4）

PAS 96:2026, Protecting and defending food and drink from deliberate attack – Guide

Foreword

Add/View comments (0)

Publishing information

This PAS jointly sponsored by Department for Environment, Food & Rural Affairs (Defra) and the Food Standards Agency (FSA). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on XX Month 202X .

Acknowledgement is given to Leanne Singleton, FoodSure as the technical author, and the following organizations that were involved in the development of this PAS as members of the Steering Group:

[SG member organization]

[SG member organization]

[SG member organization]

This PAS is not to be regarded as a British Standard. It will be withdrawn in the event it is superseded by a British Standard.

The PAS process enables a standard to be rapidly developed in order to fulfil an immediate stakeholder need. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or international standard.

Supersession

This PAS supersedes PAS 96:2017, which is withdrawn

Information about this document

This is a full revision of the document, and introduces the following principal changes:

a) recognize current UK Government guidance on the increasing risk of cyberattack;

b) address the evolving threat landscape post Covid-19, which exposed global supply chain fragility and vulnerabilities in international food trade;

c) recognize the potential impact of climate change on threats to food and supply chains due to disruptions in primary production leading to ingredient scarcity; and

d) anticipate the effect of food sector developments driven by policies such as "go-green", "carbon neutral", "net-zero" and food waste reduction.

It is also an opportunity to align definitions and integrate the collective learnings from the global food community. Key updates include:

a) recent food defence cases;

b) updated cybercrime threat information;

c) alignment of the Threat Assessment Critical Control Points (TACCP) process diagram to the application guidance;

d) an expansion of food protection arrangements; and

e) further information on other approaches to food and drink protection.

The document format has been restructured with question prompts and checklists being relocated to Annex D to provide a dedicated set of tools to guide the TACCP approach.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Presentational conventions

The provisions of this document are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is "shall".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the *Shorter Oxford English Dictionary* is used (e.g. "organization" rather than "organisation").

Contractual and legal considerations

Compliance with a PAS cannot confer immunity from legal obligations.

Introduction

Add/View comments (0)

0. 1 Rationale

Add/View comments (0)

PAS 96 provides broad guidelines to food business operators to help them assess and reduce the risk of threats to their businesses and mitigate the impact of an attack.

This is a guidance document, not a set of requirements as a key feature of this PAS is proportionality. The risk is different for different organizations, for different operations and for different products. It is therefore implicit that different threat assessments result in different controls, proportionate to a business context.

PAS 96 is not an external audit tool as it provides guidance, not requirements, to demonstrate conformance.

0 . 2 Focus

Add/View comments (0)

The focus of this PAS is on protecting the authenticity and safety of food and drinks from malicious and ideological motivated attacks leading to contamination, supply disruption or financial harm. There are numerous threats that continue to evolve, making it impractical to identify all threats. However, by assessing risk and prioritizing the most likely threats, the business can focus their attention and resources to where they are most needed.

This guide describes the Threat Assessment Critical Control Points (TACCP) approach, a risk management methodology aligned with Codex Alimentarius General Principles of Food Hygiene , Hazard Analysis Critical Control Point, (HACCP) [1] but with a distinct focus on food defence. It assumes business operators have established preventative food safety systems (such as HACCP), supported by robust crisis management and business continuity procedures. It builds on existing food safety controls to strengthen food protection arrangements and defend food and drink from attack, as many measures implemented for food safety also deter or detect deliberate acts of harm.

Information sharing and industry collaboration are critical to proactively address emerging and evolving threats. Since the initial publication of PAS 96 in 2008, numerous food defence incidents have provided valuable insights into threats and their impacts on food businesses. This highlights the importance of analysing past events to better predict and prevent similar incidents in the future [2].

Any intending attacker, whether internal to the food business or its supply chain, or external to both, is likely to attempt to evade or bypass routine procedures that could lead to detection. A primary factor is the attacker's motivation, which may be to cause harm to human health or business reputation, or to seek financial gain. The common factor behind these attacks is people who can be:

a) within a food business, (insiders);

b) employees of a supply chain partner or customer; and

c) complete outsiders with no connection to the food business.

Key concepts include the distinction between a food defence risk, a threat and a vulnerability. For example; the *risk* of malicious contamination can arise from the *threat* of insider action or an external extremist, prompting monitoring of potentially vulnerable steps in a production process.

TACCP encourages business operators to think like attackers, to anticipate their motivations, capabilities and opportunity to carry out an attack, and to implement proportionate controls and protective arrangements. As threats are continually evolving, food business operators should adopt a proactive approach to food protection.

1) Who might want to attack us?

2) How might they do it?

3) Where are we vulnerable?

4) How can we stop them?

No approach or process can guarantee that food and food supply remain free from criminal activity.

The use of PAS 96 can help businesses to manage risk by implementing protective arrangements, reducing their vulnerability as targets and enhancing detection of potential attacks.

1 Scope

Add/View comments (0)

This PAS provides guidance on preventing and mitigating deliberate (intentional) threats to food and drink and their supply chains, using the Threat Assessment Critical Control Points (TACCP) risk management approach.

It applies to organizations of all sizes and at all point in the food and drink supply chain, from primary production through manufacturing, distribution, retailing and foodservice. The guidance is particularly valuable for small and medium sized enterprises (SMEs) who might not have access to specialist risk management expertise.

The scope is limited to intentional acts, (e.g. sabotage, adulteration, extortion, espionage, or cyberattack carried out for ideological, financial gain or malicious reasons). Unintentional incidents, (e.g. accidental contamination or naturally occurring hazards) and routine food safety or quality issues fall outside the scope of this PAS and are addressed by other standards such as HACCP-based food safety management systems.

2 Normative references

Add/View comments (0)

There are no normative references in this document.

3 Terms and definitions

Add/View comments (0)

For the purposes of this PAS, the following terms and definitions apply.

3 . 1 adulteration

Add/View comments (0)

reducing the quality of a food product through the inclusion of another substance, with the intention either to make production costs lower, or apparent quality higher

{SOURCE: Food Crime Strategic Assessment 2024 [3] }

3 . 2 attack

Add/View comments (0)

intentional act aimed at causing harm, disruption, or loss to a food business, including acts motivated by economic gain, ideological causes, sabotage or terrorism

3 . 3 authenticity

Add/View comments (0)

quality of being authentic

[SOURCE: BS EN 17972:2024. 3.6]

NOTE In the context of food defence, authenticity means of genuine origin and not copied or falsified.

3 . 4 cyber security

Add/View comments (0)

protection of devices, services and networks, and the information on them, from theft or damage

{ SOURCE: NCSC Advice and Guidance - Glossary [4]}

3 . 5 food defence

Add/View comments (0)

procedures adopted to assure the protection of food and drink and their supply chains from malicious and ideologically motivated attack leading to contamination or supply disruption

NOTE Food security is distinct from food defence. Food security is when all people have physical, social, and economic access to sufficient, safe, and nutritious food that meets their dietary needs and food preferences [6]. Except in the limited sense that a successful attack can affect the availability of food, food security is not used and is outside the scope of this PAS.

3 . 6 food fraud deliberate misrepresentation Add/View comments (0)

<misdescription > intentionally causing or allowing a mismatch between food product claims and food product characteristics

[SOURCE: BS EN 17972:2024, **3.13**]

NOTE 1 Food fraud can happen either when the implicit claims that are relevant in the given context for the food product in question are violated, when the explicit claims related to the food product are deliberately changed (record tampering), or when the characteristics of the food are deliberately changed (product tampering). Food fraud in practice often involves a combination of these violations.

NOTE 2 Fraud is a covert act of adulteration for economic gain. There are many kinds of food fraud:

a) the sale of food which is unfit and potentially harmful;

1) recycling animal by-products back into the food chain;

2) packing and selling beef and poultry with an unknown origin;

3) knowingly selling goods which are past their "use by" date; and

4) knowingly selling foods that have been contaminated;

b) the deliberate misrepresentation of food;

1) products substituted with a cheaper alternative, for example, farmed salmon sold as wild, and Basmati rice adulterated with cheaper varieties; and

2) making false statements about the source of ingredients, i.e. their geographic, plant or animal origin; and

c) unlawful processing; the slaughter, preparation or processing of products of animal origin outside of the relevant regulatory framework [3]

.

3 . 7 food protection Add/View comments (0)

procedures adopted to deter and detect fraudulent attacks on food

3 . 8 food supply Add/View comments (0)

elements of what is commonly called a food supply chain

NOTE An example of a food supply chain is given in Annex A, A.1 .

3 . 9 hazard Add/View comments (0)

something that can cause loss or harm which arises from a naturally occurring or accidental event or results from lack of necessary competence on the part of the people involved

3 . 10 hazard analysis critical control point (HACCP) Add/View comments (0)

system which identifies, evaluates, and controls hazards which are significant for food safety

{ SOURCE: Codex Alimentarius, General Principles of Food Hygiene [1]}

3 . 11 insider Add/View comments (0)

person who has, or previously had, authorised acoess to or knowledge of the organization's resources, including people, prooesses, information, technology and facilities

{SOURCE: National Protective Security Authority NPSA [5]}

3 . 12 insider threat Add/View comments (0)

insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organization

{SOURCE: National Protective Security Authority NPSA [5]}

3 . 13 personnel security Add/View comments (0)

protecting organizations from the risks associated with the people it employs

{SOURCE: NCSC Advice and Guidance - Glossary [4]}

NOTE Personnel security principles are used to assure the trustworthiness of employees or contractors inside an organization but may be applied to the employees and contractors of suppliers within processes for vendor accreditation. Not to be confused with "personal security".

3 . 14 product tampering Add/View comments (0)

<food fraud> type of food fraud which includes the deliberate changing of food characteristics so that they no longer match the implicit or explicit claims associated with the product

[SOURCE: BS EN 17972:2024, **3.16**]

NOTE 1 Product tampering can happen either by subjecting the food product to an unapproved or undeclared process, by removing a substance which should have been present in the product (removal), or by adding or replacing a substance (adulteration).

NOTE 2 Product tampering includes tampering with the food product packaging.

NOTE 3 Malicious tampering is a term used to refer to the deliberate tampering of food products with the intent of sabotage or extortion; this is not primarily a food fraud issue.

3 . 15 protective arrangements Add/View comments (0)

overall, integrated set of policies, procedures and systems that form a business's food defence strategy

NOTE Protective arrangements encompass a broad range of practices and procedures, including proportionate controls.

3 . 16 risk Add/View comments (0)

possible future outcomes that we can describe in terms of their chances of occurrence, and the impact they would have if realised

{SOURCE: NCSC Advice and Guidance - Glossary [4]}

3 . 17 seal numbers Add/View comments (0)

unique alphanumeric identifier printed or embossed on tamper-evident security seals applied to containers, pallets, packaging or vehicles in food supply chains

3 . 18 threat Add/View comments (0)

something that can cause loss or harm which arises from the ill intent of a person or group of people

NOTE Threat is not used in the sense of threatening behaviour or promise of unpleasant consequence of a failure to comply with a malicious demand.

3 . 19 threat assessment critical control point (TACCP) Add/View comments (0)

systematic approach to identify perceived threats, assess vulnerabilities and mitigate risks from intentional acts aimed at harming the organization, its operations, or products

3 . 20 vulnerability Add/View comments (0)

weakness, or flaw, in software, a system or process

NOTE An attacker exploits these to, for example gain unauthorised access to a computer system.

{SOURCE: NCSC Advice and Guidance – Glossary; revised the second sentence, changed to a note [4]}

4 Types of threat Add/View comments (0)

4 . 1 General Add/View comments (0)

Deliberate acts targeting food and drink, and the supply chain can take various forms, from cybercrime to economically motivated adulteration (EMA) and malicious contamination. Threats are listed in order of likelihood, with cybercrime being the most significant type of threat. Cases are included to provide a context to the nature of different threats and their impact.

4 . 2 Cybercrime Add/View comments (0)

4 . 2 . 1 Advancing technology Add/View comments (0)

Rapidly advancing information and communication technologies provide new and increasing opportunities for malpractice that could target networks or operational technology.

NOTE In total in England and Wales for the year to March 2022, the Office for National Statistics [6] reported approximately 4.5 million frauds, of which 61% were cyber-related, and 1.6 million cases of computer misuse. The Scottish Crime and Justice Survey (SCJS) 2023/24 report indicates there were approximately 456 000 fraud related crimes and 68 000 crimes of computer misuse [7].

The increasing use of artificial intelligence (AI) in precision agriculture technologies to enhance crop management and productivity has led to alerts warning primary producers of their heightened vulnerability to cyberattacks [8].

A successful cyberattack could compromise an organization's proprietary data, such as financial or employees' details, confidential recipes, processes, marketing strategies or supplier and customer details. In some cases, the attacker might seek to defraud both business and consumer. A fraudster might try to exploit an individuals' ignorance of the technologies involved. This type of fraud is cyber-enabled, where technology is used to enhance another crime such as a scam made easier by electronic communications.

Identity theft is more commonly associated with individuals, but organizations can also have their identity stolen to facilitate procurement fraud. Goods are ordered in the name of the customer but diverted to the fraudsters' premises, leaving the duped supplier and supposed purchaser to carry the cost and litigation.

4 . 2 . 2 Cyber-enabled industrial espionage or hacking Add/View comments (0)

Another type of attack is cyber-enabled industrial espionage or hacking, a form of cybercrime involving unauthorized access to computer systems, potentially with malicious intent .

Example case: In 2024 a former Disney employee hacked Disney World's servers falsifying allergen information to falsely mark certain items as peanut free , altering prices, adding profanity and redirecting QR codes to a boycott website. The cyberattacks followed the employee's termination for misconduct. Although Disney intercepted the altered menus before distribution, preventing consumer harm, the attacks disrupted the menu system for up to two weeks costing $150 000 USD [9].

4 . 2 . 3 Distributed Denial of Service (DDoS) Add/View comments (0)

A business can be impacted by a Distributed Denial of Service (DDoS), which occurs when multiple sources overload a website or network to degrade its performance or render it inaccessible [10]. This can cause disruption and financial loss, especially for businesses reliant on online platforms. The growing presence of the Internet of Things (IoT) increases vulnerability, as everyday connected devices might be compromised and exploited by attackers.

Example case: In 2020 the German food delivery service Takeaway.com reported cybercriminals had conducted a DDoS attack against its website, resulting in orders not being processed. The attackers requested payment through cryptocurrency to stop the attack [11].

4 . 2 . 4 Ransomware attacks Add/View comments (0)

Ransomware attacks use malicious software that prevents an individual or organization from accessing their computer or the data that is stored on it. These types of attack have become a favoured technique of organized criminals who operate globally, requesting payment in cryptocurrency and are often based in countries where governments tolerate their existence on the proviso that they themselves are not targeted [12].

Example case: In 2021, the world's biggest meat processor, JBS paid a £7.8m ransom after a cyber-attack on its system shut down operations, including abattoirs and feedlots in the US, Australia and Canada . Cattle slaughter was halted at US facilities, causing disruption in a food supply chain already strained by Covid 19 impacts [13] .

4 . 2 . 5 Misinformation and disinformation Add/View comments (0)

The rise in misinformation and disinformation which has coincided with the growth of social media, has the potential to undermine public confidence in the authenticity, safety and reliability of food. The rise in food-related fake news and misleading information can significantly influence consumer perceptions and behaviour [14].

Example case: Despite no evidence of widespread plastic rice, social media rumours originating in China around 2010 claimed rice is made from plastic and mixed into real supplies. Then again in 2016, Nigerian customs seized 2.5 tonnes of rice, initially calling it plastic; later retracted after tests found high bacteria but no plastic. Persistent online myths continue in Africa and beyond, fuelled by misinformation [15].

4 . 3 Economically motivated adulteration (EMA) Add/View comments (0)

4 . 3 . 1 Motivation Add/View comments (0)

The motivation of EMA is financial and can cause multiple impacts from serious public health risks through the introduction of harmful substances; financial losses to businesses through reputational damage and supply chain disruptions; and erosion of consumer confidence.

A successful adulteration, from the attacker's perspective, is one which remains undetected. If involving an insider, it could be revealed through audits or detected through routine product testing and process verification activities, for example:

a) an audit of procurement and incoming materials could reveal purchases which are unexplained by recipes, such as Sudan dyes which have no place in spice manufacture; or

b) differences between the quantities sold and quantities purchased, for example, the amount of beef sold compared to beef purchased, with horse meat used to make up the difference.

4 . 3 . 2 Substitution Add/View comments (0)

Substitution is a common form of EMA for example by either passing off a cheaper product as a more expensive one (or replacing or extending a high-value ingredient with a lower-cost alternative.

Example case: In 2017, Italian authorities disrupted an organized crime ring which was exporting fake olive oil to the United States. Similarly, Brazilian officials reported that a very high proportion of olive oils tested did not meet the quality standards required by their labelling [16] .

4 . 3 . 3 Adulteration Add/View comments (0)

The common factor in many cases of EMA is that the adulterant is neither a food safety hazard, nor readily identifiable as this would defeat the attack. Common adulterants can include water, sugar, starch and other ingredients that would normally be declared on the label but are not disclosed or are added in different proportions to the product or that stated on the label.

Example case: In 2024, Delhi police in India seized 15 tonnes of fraudulent spices from two factories, arresting three individuals involved in the production and supply of adulterated spices. The suspects were found using banned substances and non-edible items in the manufacturing process, endangering public health and safety [17].

4 . 3 . 4 Economic gain Add/View comments (0)

The avoidance of loss can also be an incentive for adulteration where limited supply of a key product can encourage a producer to improvise to meet an order rather than declare short delivery to the customer.

Example case: In 2016, the Kenyan Dairy Board claimed that hawkers were putting lives at risk by adding preservatives (hydrogen peroxide) in an attempt to extend the shelf life of milk [18].

The intention of EMA is not generally to cause illness or death, although this could be an unintended outcome, as was the case in 2008 when melamine was used as a nitrogen source to fraudulently increase the protein content of milk, resulting in more than 50 000 infants hospitalized and 6 deaths after having consumed contaminated infant formula [19].

4 . 4 Counterfeiting Add/View comments (0)

4 . 4 . 1 Motivation Add/View comments (0)

Counterfeiting is motivated by financial gain through fraudulently substituting inferior foods, drinks or packaging for reputable brands. While both petty criminals and organized crime groups engage in this activity, it is predominately perpetrated by organized crime groups operating across international supply chains. Petty criminals may seek opportunistic quick wins, whereas organised groups exploit scale and complexity.

4 . 4 . 2 Counterfeit food and drink Add/View comments (0)

Counterfeit products, often produced in unsanitary conditions, can be contaminated or otherwise unsafe for consumption.

Example case: Operation OPSON IX [20] reported in 2021 the seizure by its global network of enforcement bodies of 1 613 tonnes of illicit alcohol, much of it violating intellectual property rights.

4 . 4 . 3 Counterfeit packaging Add/View comments (0)

Sophisticated printing technologies can be used by organized crime groups to create fake product labels that are indistinguishable from the genuine ones. Petty criminals might steal genuine packaging or even refill single use containers for resale.

Example case: An investigation in 2018 uncovered a fraud in Italy involving the reuse of authentic primary (empty wine bottles) and secondary (wooden boxes) packaging. Two individuals in the food industry collected empties from restaurants, refilled them with cheap wines bought online or from discount stores, and sealed them with corks and counterfeit capsules. Packaging films and fake guarantee seals concealed the tampering. Counterfeiters contacted buyers via a major e-commerce platform, offering prices far below market rates. The fake wines were sold as genuine in Italy and abroad, creating a completely uncontrolled market with no traceability [20].

4 . 5 Malicious contamination Add/View comments (0)

The motivation for malicious contamination can be to cause localized or widespread illness or death. In certain scenarios, attackers may use contaminants that are not normally present or readily accessible.

Example case: In 2014, when a worker at Aqlifoods' Oizumi facility in Japan was arrested for contaminating frozen foods with malathion (an organophosphate insecticide), causing over 2 800 illnesses. Maruha Nichiro recalled 6.4 million packages and issued public apologies [21]. The worker, dissatisfied with pay and conditions, denied the charges.

Example case: In 2018, an incident in Queensland Australia [22] led to extensive public concern and a dramatic drop in retail sales when retail customers found sewing needles inserted into fresh strawberries.

In most instances, the materials that an attacker could use to gain publicity or to extort money, are likely to be those that are readily available, rather than those required to cause widespread harm.

Example case: A factory worker in Worcestershire, UK in 2022 was jailed for three years after knowingly and maliciously contaminating hummus and salad dressings destined for Nando's with plastic bags, rubber gloves and metal ring pulls. The company detected the contamination via metal detectors post-production, confirming that the product tampering occurred in the storage area. An internal investigation identified multiple tampered boxes, leading to police involvement [23] . No contaminated products reached end customers.

4 . 6 Ideologically motivated malicious contamination Add/View comments (0)

Ideologically motivated malicious contamination refers to deliberate acts to advance political, religious or extremist agendas, often aiming to cause public harm, disruption or influence events like elections. The motivation can be to disrupt the supply chain by undermining public confidence.

Example case: In 2017, an anarchist group called Green-Black Commando published online threats to contaminate food products in Greece. They claimed to have injected hydrochloric acid into soft drinks, milk, sausages and sauces from multinational companies. The group warned that poisoned items would soon appear on supermarket shelves. Similar anarchist threats of food contamination targeting major corporations occurred in Greece in 2013 and 2016, typically aimed at forcing product withdrawals and causing significant revenue loss, especially during peak seasons [24].

Support for religious extremism can also be a motivation, with the harm intended to maximize publicity for the cause .

Example case: In 2018, the Derby Plot led to the conviction of a UK couple for preparing a terrorist attack, which could have targeted Derby or involved contaminating supermarket food with ricin (a toxin derived from castor beans) [25] .

4 . 7 Extortion Add/View comments (0)

The motivation for extortion by an individual or group, is driven by financial motives, seeking to obtain money from the targeted organization or individual. A small number of samples can be used to demonstrate an attacker's intent, their capability and opportunity, sufficient to cause public concern and draw media attention. Such actions appeal to criminals when the product is a sensitive food such as an infant food, or the target is perceived as wealthy.

Example case: In 2020, a farmer in the UK was jailed for 14 years after being found guilty of extortion and contaminating infant food with metal shards [26].

4.8 Espionage Add/View comments (0)

The primary motivation of espionage is for competitors seeking commercial advantage to access intellectual property. Criminals or organized crime groups, often state sponsored and protected, may attempt to extract confidential information from executives and employees through blackmail, extortion (see **4.5**) or threats. Tactics can include obtaining information on employees in compromising situations to threaten exposure, infiltration using insiders or by targeting IT systems remotely.

Example case: In January 2022, a Chinese national pleaded guilty to participating in a plot to steal a proprietary algorithm from Monsanto. The software enabled farmers to increase agricultural productivity [27].

5 Understanding the attacke r Add/View comments (0)

5 . 1 General Add/View comments (0)

The success of an attack on food or food supply can depend on the following.

a) Does the attacker have the motivation and drive to overcome the barriers to their actions? When barriers appear robust and success seems unlikely, many would-be attackers seek easier targets.

b) Does the attacker have the capability to carry out the attack? A group is likely to have more resources available to them and potentially have the required skills for an attack.

c) Does the attacker have the opportunity to carry out the attack? A physical attack needs physical access to the target, however a cyberattack might only need access to a computer.

d) Would the attacker be deterred by the chance of detection or potential penalties?

Subclauses **5.2** to **5.8** describe the characteristics of different types of attackers. It is possible that individuals might represent more than one type of attacker.

5 . 2 Cyber criminals and other malicious digital actors Add/View comments (0)

Cyber criminals aim to subvert controls on computerized information and communication systems:

a) to stop them working effectively;

b) to steal or to corrupt data which they hold; and/or

c) to disrupt internet business.

These malicious actors might also align with other type of attackers. Their approaches can be opportunistic rather than targeted, finding value in broad scale phishing campaigns sent to thousands, where even a single response can yield rewards.

Their motivation can be criminal, political, financial or even mischievous to demonstrate their expertise and ability to outsmart a protective system devised to stop them. An attraction of cybercrime is anonymity or deniability where the perpetrator can disguise their role and protest innocence, while proving guilt can be highly burdensome. Another attraction is remote access where interconnectivity enables attacks from distant jurisdictions which can condone or even encourage their actions.

This type of aggressor is known to have the expertise to cause commercial harm, as warned by the National Cyber Security Centre (NCSC), "With attackers able to achieve many of their aims by using techniques that are not particularly advanced, the distinction between nation states and cyber criminals has blurred, making attribution all the more difficult" [10].

The rapid increase in cybercrime, in particular ransomware attacks, has made many businesses conclude that an attack is inevitable and that they need to plan accordingly.

5 . 3 The opportunist Add/View comments (0)

The opportunist can hold an influential position within an operation and be able to evade internal controls. They might have some technical expertise, but their primary advantage is access. They are likely to be discouraged by the chance of detection. Their actions might be deterred by the knowledge that unannounced customer visits, audits or ad hoc product sampling for analysis could occur at any time.

A supplier unable to risk non-delivery of a product might occasionally adulterate products, hoping it goes undetected. This opportunist could even persuade themselves that the adulteration is legitimate. For example, chicken in a pork sausage would still be considered meat.

5 . 4 The extremist Add/View comments (0)

Extremists take their cause so seriously that they distort its context and disregard broader implications. Their dedication might have no limits and their determination to advance the cause could be unlimited.

Extremists might want to cause harm and are likely to enjoy publicity after the event. They might view personal harm as irrelevant, or even beneficial to their cause. They have a higher level of motivation and while failure is a potential deterrent, the risk of capture after the event is not. They are typically resourceful and innovative in devising ways to attack.

A single-issue or terrorist group might aim to disrupt business operations and reputation but avoid mass harm to maintain support for their cause.

5 . 5 The irrational individual Add/View comments (0)

Some individuals have no rational motive for their actions but believe they are acting with purpose. Their distorted priorities and preoccupations prevent them from maintaining a balanced view. They might have clinically diagnosed mental health conditions.

These individuals can be deterred by making access to their targets more difficult or by increasing the likelihood of detecting contamination.

5 . 6 The disgruntled individual Add/View comments (0)

The disgruntled individual believes that an organization has been unfair to them and seeks revenge. They could be an aggrieved employee, former employee or supply chain partner. They could have expert knowledge of the operation and access to it.

This type of aggressor is likely to be an individual rather than part of a group. If an insider, they could pose a serious threat but are more likely to aim for embarrassment and financial loss than harm to the public. An individual external to the business is more likely to falsely claim an attack than to actually execute one or possess the capability to do so.

5 . 7 The professional criminal Add/View comments (0)

Organized crime groups might view food fraud as a low-risk, high-reward opportunity that is relatively easy to execute, offering substantial profits with a minimal chance of detection and lenient penalties if convicted. The global food trade, where materials move relatively freely across enforcement borders, appears to encourage professional criminals.

The anonymity of the internet and the opportunity for remote access into electronic systems makes cybercrime increasingly attractive to professional criminals.

Professional criminals can be deterred through close collaboration between food businesses, and national and international law enforcement authorities.

5 . 8 The extortionist Add/View comments (0)

The extortionist seeks financial gain from an attack and concentrates on avoiding detection. Their target is more likely to be a high-profile business with much to lose from negative publicity. They can work alone and be resourceful, secretive and self-interested. Individuals might claim to be able to act against a business while lacking the capability to actually carry out the threat. In these cases, the business might assess the claim as not credible but should still report and respond seriously to the threat.

6 . 1 Broad themes Add/View comments (0)

TACCP should be used by food businesses as part of their broader risk management strategy. It may be used as a framework to systematically assess the risk of an attack from specific threats.

TACCP aims to:

a) reduce the likelihood (chance) of a deliberate attack;

b) reduce the impact (consequences) of an attack;

c) protect organizational reputation;

d) provide reassurance to customers and the public that proportionate steps are in place to protect food from malicious actions;

e) satisfy global food sector expectations and support the work of trading partners; and

f) demonstrate that reasonable precautions are taken and due diligence is exercised in protecting food.

TACCP can achieve this by:

1) identifying specific threats to an organization, operation and their products;

2) identifying vulnerabilities that could allow for a specific threat to be carried out;

3) assessing the likelihood of an attack by evaluating the motivation and capability of the potential attacker in context of associated vulnerabilities;

4) projecting the potential impact by evaluating the consequences of a successful attack;

5) establishing priorities for evaluating threats by comparing their likelihood and impact;

6) deciding on proportionate controls to deter the attacker and provide early detection of an attack; and

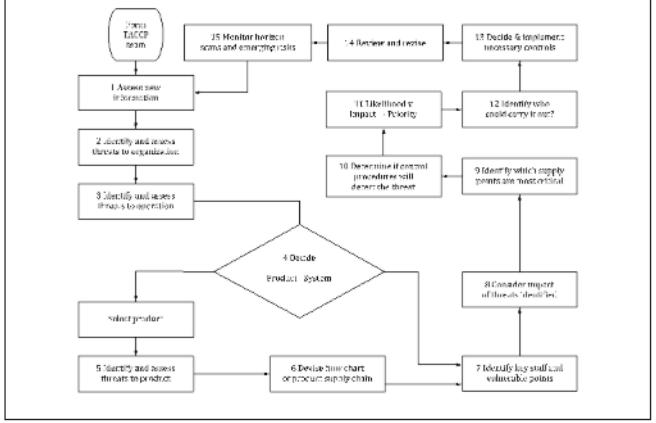
7) maintaining information and intelligence systems to enable revision of priorities and controls when circumstances change.

TACCP cannot stop individuals or groups from claiming to have contaminated food. However, it enables a business to assess the plausibility of such claims and determine their likely validity. Any credible claim or actual incident should be treated as a crisis (see Clause 9). The business should take measures to maintain operations and communicate effectively with all relevant parties.

6 . 2 TACCP process Add/View comments (0)

The flow chart of the TACCP process shown in Figure 1 incorporates all threats with a focus on deliberate adulteration and contamination.

Figure 1 – Outline TACCP process Add/View comments (0)



6 . 3 TACCP team Add/View comments (0)

The TACCP team is intended to be a cross-functional collaboration across the business to comprehensively identify potential threats, with a smaller team tasked with determining and implementing proportionate controls. For many small businesses, the team approach is not feasible and it may be the job of one person.

The TACCP team should adapt the TACCP approach to best meet their needs, addressing the following four questions.

a) Who might want to attack us? (see **6.4.2** to **6.4.7**)

b) How might they do it? (see **6.4.8**)

c) Where are we vulnerable (see **6.4.9** to **6.4.13**)

d) How can we stop them? (see **6.4.14**)

The TACCP team could include individuals with the following expertise:

1) security;

2) human resources;

3) food technology;

4) food safety and quality;

5) process engineering;

6) production and operations;

7) purchasing and procurement; distribution and logistics;

8) information technology;

9) legal;

10) communications;

11) commercial/marketing; and

12) senior leadership and management.

The team may also consult with a broader group of specialists including Environment, Health & Safety (EHS) and the Business Continuity Team.

NOTE 1 The team may include representatives of key suppliers and customers.

NOTE 2 While the HACCP team might serve as a starting point, expertise beyond food safety is often needed. The business continuity team could be a more suitable model. The TACCP team is typically an established group, able to regularly review decisions, adjust priorities and revise controls.

As the TACCP process can cover sensitive material and could be of assistance to a prospective attacker, team members should be knowledgeable of actual processes, trustworthy, discreet and have an awareness of the implications of the TACCP process. This might include non-disclosure agreements where appropriate.

6 . 4 Application of TACCP Add/View comments (0)

6 . 4 . 1 General Add/View comments (0)

The TACCP process provides a systematic approach for conducting risk assessments. It enables the TACCP team to identify potential threats, and assess vulnerabilities associated with each one. The team then evaluates the adequacy of existing controls and assigns a risk score to each threat. Where necessary, additional proportionate controls are implemented. Finally, the assessment is reviewed regularly to address emerging threats.

6.4.2 Assess new information Add/View comments (0)

Assess all new information related to food defence incidents, evolving risks, emerging threats, changes to the supply chain and potential impacts which come to its attention.

6.4.3 Identify and assess threats to an organization Add/View comments (0)

Identify and assess threats to the organization: individuals and/or groups which could be a threat to the organization and its systems, especially electronic systems, and assess their motivation, capability and determination (see Annex A).

6.4.4 Identify and assess threats to an operation Add/View comments (0)

Identify and assess threats to the operation: individuals and/or groups which could be a threat to the specific operation, e.g. premises, factory, site (see Annex A).

6.4.5 Decide on a product or system approach Add/View comments (0)

Decide if a product specific threat assessment is needed to differentiate product threats from other threats.

a) If a product threat assessment is required, select a product which is representative of a particular process, such as a vulnerable product from a particular production line (see Annex A).

b) For non-product threats, continue to **6.4.7** .

6.4.6 Identify and assess threats to product Add/View comments (0)

Identify and assess threats to product, individuals and/or groups that might want to target the specific product.

a) Adulterants could include low-cost alternatives to premium components whereas contaminants could include toxic agents, industrial chemicals, readily available noxious materials or the introduction of allergens.

b) Adulterants could be selected for their ability to withstand food processing processes. For example, cleaning procedures might remove them, heat treatments could degrade them and interactions with other ingredients could neutralize their effects.

6.4.7 Devise flow chart Add/View comments (0)

Draw a supply chain map to provide a visual representation of each stage of the supply chain from farm to fork (see Annex A). Particular attention should be paid to less transparent or controlled parts of the supply chain. Least visible parts of a supply chain might include primary production inputs, bulk commodity handling and transport logistics.

6.4.8 Identify vulnerabilities Add/View comments (0)

Identify key employees and vulnerable points in the supply chain; examine each stage of the supply chain to identify the vulnerable points where an attacker might hope for success and the people who would have access to the product.

The TACCP team might need to apply lateral thinking to ask, "If we were trying to undermine our business, what would be the best way?" . This could include consideration of the availability and cost of adulterants, their toxicity or allergenicity and their physical form.

6.4.9 Consider impact Add/View comments (0)

Consider impact of threats identified relevant to the organization or operation across the supply chain, or to the product at each step in the process flow diagram. Assess how the process can mitigate the impact of the threat.

6.4.10 Identify critical supply points Add/View comments (0)

Identify which supply chain points are most critical, where a threat would have the greatest impact and where it could be detected.

6.4.11 Assess adequacy of controls Add/View comments (0)

Determine if existing product, process or system controls are capable of detecting the threat.

a) Product controls involve directly testing or inspection of food and drinks (raw, in-process or finished). This could include mass balance/yield reconciliation, foreign object detection, sensory assessments, positive release via micro testing, supplier COA and random verification testing of raw materials. For example, routine laboratory analysis could detect added water or the presence of unexpected fats and oils.

b) Process controls involve monitoring equipment, process parameters and steps during a production process. This could include cleaning verification programs, environmental monitoring, in process chemical tests (e.g. pH, Brix), temperature monitoring and camera anomaly detections. For example, unexpected variances in inline chemical tests could indicate changes to process set points.

c) System controls involve data, access and verification systems that safeguards the system, prevents cover-ups and enables traceback. For example, oversight of procurement would challenge unusual purchase orders.

6.4.12 Conduct risk assessment Add/View comments (0)

Score the likelihood of the threat happening and the impact it would have to determine the threat priority (see **7.3**). Revise if the risk assessment score does not fit with the logic of the TACCP team.

6.4.13 Identify potential attackers Add/View comments (0)

Where the threat priority is scored as very high or high, identify who could carry it out. Consider who has unsupervised access to the product or process, whether they are trustworthy and if that trust is justified.

6.4.14 Implement controls Add/View comments (0)

Decide and implement controls which are proportionate to the identified threats. Document the controls, maintaining confidentiality where required, and implement in a timely manner. This could include a confidential reporting and recording procedure that allows management action on decisions but does not expose weaknesses.

6.4.15 Review and revise Add/View comments (0)

Review and revise when there are changes to the threat environment, an increase or decrease in vulnerabilities or following significant changes to products, processes or their supply chains.

6.4.16 Monitor emerging risks Add/View comments (0)

Monitor horizon scans and emerging risks; maintain a routine watch of new information to provide an early warning of changes that can become new threats or change the priority of existing threats, including more local issues as they develop.

NOTE See Annex E for an outline of some information and intelligence systems.

7 Assessment Add/View comments (0)

7 . 1 Assessing threats Add/View comments (0)

The organization, operation and product can be the target of an attack from a range of groups and individuals (see Clause **5**). Each element should be assessed separately. The TACCP team should assess and consider risks factors such as suppliers under financial stress, alienated employees and former employees, competitors, terrorist organizations, organized crime groups and local activist groups.

A shorter supply chain with fewer participants and less touchpoints might pose lower risks than a longer, more complex one. Additionally, the level of visibility across the supply chain is a key factor in assessing opportunities for threats.

For a list of question prompts that the TACCP team could consider to assess threats for the organization, the operation and the product, see Annex B.

7 . 2 Assessing vulnerabilities Add/View comments (0)

7 . 2 . 1 General Add/View comments (0)

Individual organizations have different business needs and operate in different contexts. The TACCP team can assess which vulnerability assessments are the most relevant and proportionate to the threats they identify.

7 . 2 . 2 Cyber vulnerabilities Add/View comments (0)

Vulnerabilities to cyberattack can arise from a range of systems and devices, these include:

a) information technology systems for email, Enterprise Resource Planning (ERP), e-commerce and cloud platforms;

b) operational systems for Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLCs), sensors and cold chain temperature monitors; and

c) Internet of Things (IoT) devices including cameras and barcode scanners.

For a list of question prompts that the TACCP team could consider to assess cyber vulnerabilities, see Annex C.

7 . 2 . 3 Economically motivated adulteration (EMA) vulnerabilities Add/View comments (0)

A typical feature of EMA (see **4.3**) is the substitution of a low-cost item in place of a relatively high-cost component/ingredient. The TACCP team should be alert to the availability of such alternatives.

Products with provenance or identity preserved claims are known risks for EMA. These include claims for organic, non-GMO, locally grown, free range or with protected designations of origin. The attacker is likely to have ready access to lower value equivalents, which are almost indistinguishable from the authentic product.

For a list of question prompts that the TACCP team could consider to assess vulnerabilities for EMA, see Annex C.

7 . 2 . 4 Malicious contamination vulnerabilities Add/View comments (0)

Vulnerabilities for malicious contamination may vary depending on the product type, the production process, packaging and access to the product post-production, prior to consumer use.

For a list of question prompts that the TACCP team could consider to assess vulnerabilities for malicious contamination, see Annex C.

7 . 2 . 5 Evolving food sector vulnerabilities Add/View comments (0)

Impacts from climate change are expected to increase the risks of both EMA and intentional malicious contamination of food. Climate change disrupts crop yields, exacerbates resource scarcity, drives price volatility and lengthening supply chains for climate-sensitive commodities (e.g. olive oil, honey, spices, coffee, cocoa and seafood). This makes substitution, dilution and counterfeiting more economically attractive for fraudulent activities. At the same time, resource shortages can intensify social grievances, potentially fuelling ideological motives for deliberate attacks. Extreme weather events disrupt infrastructure and security controls, creating temporary windows of vulnerability that malicious attackers might exploit.

Efforts to meet Environmental Social Governance (ESGs) commitments, particularly through carbon-neutral and net-zero claims can inadvertently create vulnerabilities for malicious tampering, misuse or diversion. Pressure to substantiate ESG claims can require companies to source from new, alternative or distant suppliers, leading to longer, more complex supply chains with reduced visibility and oversight, increasing the risk of deliberate substitution, adulteration or contamination. In extreme cases, the perception of greenwashing or unsubstantiated environmental claims might motivate ideologically driven insiders or external activists to deliberately contaminate or sabotage products, aiming to expose perceived corporate hypocrisy and inflict reputational harm.

The donation of surplus edible food to food rescue organizations to reduce food waste introduces additional supply chain partners which could amplify risk. Potential vulnerabilities arise from the reliance on volunteer personnel, absence of secure food storage facilities and limited oversight. These factors might increase the risks of malicious tampering, contamination or diversion of donated food into unauthorised channels or black markets, bypassing food defence controls.

Threat assessments should assess vulnerabilities arising from climate-change impacts, the promotion of ESG claims and the donation of surplus edible food to reduce food waste, as each can heighten the risk of food defence threats.

7 . 3 Assessment of risk Add/View comments (0)

Organizations should identify the full range of threats relevant to their operations, but focus attention and resources on those that pose the greatest risk. For each identified threat, the TACCP team should assess its likelihood and potential impact, then combine the two scores to determine an overall risk rating. This prioritised risk rating enables the TACCP team to identify where controls are most needed, see Table 1 and Figure 2.

Table 1 – Risk assessment scoring Add/View comments (0)

Like	Score	Impact		
		Descriptor	Human health / Public safety	Business / Financial / Reputational
Very high chance	5	Catastrophic	Death	Business / site closure
High chance	4	Major	Illness or injury requiring medical treatment	Brand damage
Some chance	3	Significant	Generally mild symptoms, may require medical treatment	Regulatory non - compliance or recall / withdrawal
Might happen	2	Some	Mild symptoms lasting a few days	Negative media reports
Unlikely to happen	1	Minor	Mild symptoms prompt recovery	No perceived impact

NOTE 1 This is an example scoring matrix; organizations may choose their own risk assessment methodology.

NOTE 2 Impacts could be assessed in human and financial terms.

The likelihood of a threat happening can be assessed by evaluating:

a) whether an attacker would achieve their aims if successful;

b) whether an attacker could have access to the product or process;

c) whether existing controls would deter the attacker;

d) whether an attacker would prefer other targets, due to higher visibility, value or vulnerability; and

e) whether an attack would be detected causing impact.

The likelihood of a threat occurring can be assessed as point in time or over a defined period (e.g. 5 years).

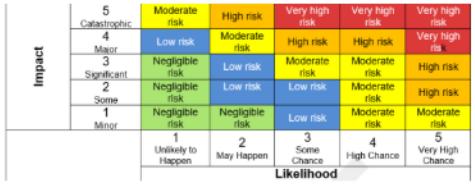
The impact or potential consequences if a threat were successfully carried out, can be assessed by evaluated using two assessment criteria.

1) Human health/public safety impact.

2) Business/financial/reputational impact.

The TACCP team decides which impact assessment criteria is most applicable to the specific threat scenario and applies this to scoring descriptor.

Figure 2 – Risk scoring matrix Add/View comments (0)



NOTE This is an example of a risk scoring matrix; organizations may choose different criteria for the different risk categories.

A business might decide to implement additional proportionate controls or protective arrangements for threats assessed as high or very high risk.

7 . 4 TACCP reporting Add/View comments (0)

A report documenting the application of the TACCP process within the business should be created to demonstrate due diligence in the event of an attack. The principles of this PAS should be integrated into existing risk and crisis management procedures.

Four fictional case studies demonstrating the application of the TACCP process that can be adapted to suit an individual company's requirements, see Annex E.

8 Controls Add/View comments (0)

8 . 1 General Add/View comments (0)

TACCP controls are measures intended to reduce vulnerability to deliberate threats against an organization, operation or product. They can include access controls, tamper detection, and employee risk management measures.

Controls need to be proportionate to the risks identified in the TACCP assessment and be tested and validated to confirm their effectiveness. Periodic challenge testing is recommended to expose any remaining weaknesses.

8. 2 Controlling access Add/View comments (0)

The objective is to minimize the opportunity for any attack by restricting access to authorised individuals with legitimate needs through physical controls.

For a list of question prompts that the TACCP team could use to assess the adequacy of access controls, see Annex D.

8.3 Tamper detection Add/View comments (0)

Raw material storage, distribution vehicles and many packaged foods can be made tamper evident. If an attacker gains access, tamper evident measures provide an opportunity that the attack can be detected in time to avoid the impact.

For a list of question prompts that the TACCP team could use to assess the adequacy or need for tamper detection controls, see Annex D.

8.4 Assuring personnel security

Add/View comments (0)

Personnel security measures can be used to mitigate the insider threat to the organization. These measures can be used by food businesses to assess their confidence in the capabilities and integrity of supply chain partners for goods and services.

A food protection culture [1]) supports robust protective security, mitigating insider risks and external threats such as hostile reconnaissance. It consists of shared organizational values that guide how everyone thinks about and approaches security.

For a list of question prompts that the TACCP team could use to assess the adequacy of personnel controls, see Annex D.

9 Response to an incident

Add/View comments (0)

9.1 Proportionate controls

Add/View comments (0)

Implementation of proportionate controls can mitigate the risk of an attack, but they cannot eliminate it entirely. Robust emergency response and business continuity protocols are essential to manage any incident.

9.2 Planning for an emergency response

Add/View comments (0)

An effective emergency response for a food defence attack should be integrated into a business' crisis management system to:

a) minimize physical and financial harm to consumers, customers, employees and others;

b) collaborate with investigatory and enforcement authorities

c) secure public support for the organization;

d) reduce financial, reputational and personal impacts of the incident;

e) prevent recurrence;

f) identify offenders; and

g) safeguard long-term consumer trust in food.

Emergency responses are best developed before a food defence incident occurs. This can include practice for different threat scenarios to test a business's preparedness and response capability, see **G.1** .

9.3 Management of a food defence incident

Add/View comments (0)

Where contamination is suspected, immediate quarantine, withdrawal and recall of affected products might be necessary. This requires clear and effective lines of communication to those with responsibility and authority [2]) .

In cases of suspected criminal activity, specialist police or law enforcement agencies should be engaged at the earliest opportunity to preserve evidence, see Annex F. The appropriate law enforcement agency depends on the jurisdiction. Evidence such as photos, samples, CCTV and logs might need to be secured to allow for further investigation.

Proactive communication with media and the public can prevent undue alarm and reputational damage.

9.4 Management of a cyber-attack

Add/View comments (0)

Speed of response can greatly reduce the damage caused by a cyber-attack and the time taken to recover . The complexity and variety of attacks can be vast, so engaging a specialist cyber security contractor, in advance of any incident, could benefit a business.

The UK's National Cyber Security Centre [3]) provides a free Early Warning Service, which helps organizations investigate cyber-attacks on their network by notifying them of malicious activity which has been detected in international feeds.

Businesses should increase cyber resilience by having an effective incident response plan, regularly exercising cyber incidents across the business and have plans in place to work with an assured cyber incident response service provider where required.

9.5 Maintaining business continuity following an attack

Add/View comments (0)

Business continuity management principles provide effective resilience to react to and recover from an attack. Examples could include changing production to a verified alternate supplier, activating backup sites or co-packers and rerouting via secondary logistics.

10 Review of food protection arrangements

Add/View comments (0)

Food protection arrangements should be reviewed when there are changes which could affect the suitability of the existing controls, following a suspected or actual incident, or a breach of site security. A review could also be prompted when the controls or food protection arrangements are found to be ineffective.

The TACCP team should regularly review food protection arrangements in line with other corporate policies. There might also be expectations from regulators or external standards for an annual review.

Specific prompts for review can include:

a) new threat information or emerging insider or external threat profiles;

b) new types of adulterants e.g. biological, chemical and radiological;

c) an actual product tampering event or a near miss event;

d) changes in suppliers or raw materials (ingredients or packaging);

e) changes to equipment, processes or layout relevant to controls;

f) changes in key personnel, e.g. TACCP team members or loss of trusted employee working in sensitive areas;

g) facility expansions, renovations or new access points;

h) introduction of bulk liquid receiving, storage or other vulnerable process steps;

i) repeated deviations from food safety critical limits or failures in monitoring;

j) new regulatory or customer requirements relating to food defence; or

k) to address deficiencies found through a challenge test of controls, or through internal and external audits.

The TACCP team should also be involved and consulted as a part of organizational change management procedures, whenever a significant change in product, process, equipment or organization structure is initiated. Robust, ongoing food defence training should be provided to all personnel across the food industry. Training strengthens knowledge and expertise, enabling food businesses to consider "what if"' scenarios to proactively develop the future controls needed to reduce the risk of an attack, safeguarding the integrity of the global food supply against deliberate harm.

The TACCP team should monitor official or reputable websites for updates in national threat assessments and for information on emerging risks, see Annex F.

A concise report of the review should have only limited circulation within the business.

The TACCP report and any review documents are commercially sensitive and confidential. Only trusted senior managers with a "need to know" and enforcement officials should be allowed access.

NOTE A business may publish a generic overview for internal use and/or to present to external auditors. Such an overview avoids detail which could be of value to an attacker. External auditors are to respect the sensitive nature of the TACCP process.

Successful TACCP implementation requires a proactive and dynamic approach as the threat landscape is constantly shifting due to new vulnerabilities and the growing sophistication of malicious actors. Food businesses, in collaboration with regulators, need to continually strengthen their preventive controls, detection systems and horizon-scanning capabilities to effectively deter, detect and respond to emerging threats throughout the food supply chain.

Annex A (informative)
The food supply chain Add/View comments (0)

The food supply chain is global, interconnected and time-sensitive. A single ingredient can travel through dozens of organizations and countries before reaching the consumer, which is why protecting every link in the chain is essential to food defence.

The food supply chain is central to food defence for the following reasons:

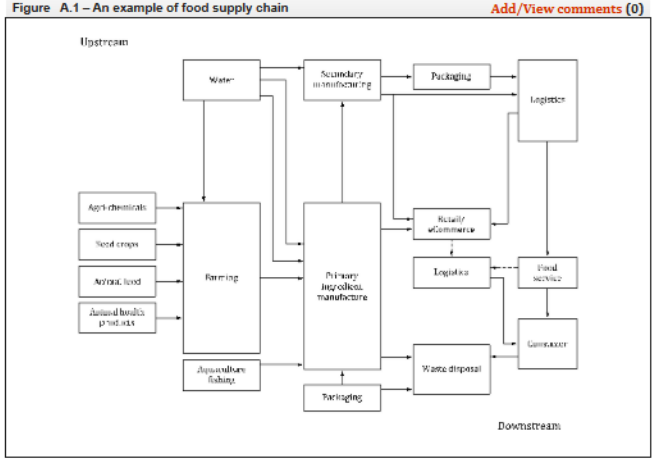
a) There are multiple vulnerable points as the modern food supply chain is long, complex and global from primary production (farms, fisheries), ingredient suppliers, manufacturers, logistics (storage, transport and distribution), through to retail and food service. Each step in the chain can provide potential access points for a motivated attacker.

b) Supply chains have an amplification effect where deliberate contamination that is introduced early in the chain (e.g. at a raw material or ingredient stage) can impact thousands or millions of consumers, creating widespread illness, death or economic disruption.

c) Food is a critical infrastructure sector. A successful attack can simultaneously threaten public health, consumer confidence, brand reputation, national economies and in extreme cases, social stability.

d) Potential attackers include disgruntled employees, criminals seeking extortion payments, competitors, terrorists, or state-sponsored actors. Each may target different parts of the supply chain to maximise harm or leverage.

Figure A.1 – An example of food supply chain Add/View comments (0)



Annex B (informative)
Assessing threats Add/View comments (0)

B . 1 Mitigating risk Add/View comments (0)

The first step in mitigating risk is recognizing factors that could increase the likelihood of threats to the organization, the operation, sensitive products, or a combination of these. Review of responses to these questions can give an understanding of the factors that can contribute to a threat risk. The TACCP team could ask the following questions to identify potential threats.

B . 2 Factors that could increase the likelihood of a threat to an organization Add/View comments (0)

Questions that the TACCP team can ask to assess the likelihood of a threat to their organization.

a) Are we operating under foreign ownership by nations involved in international conflict?

b) Do we have a celebrity, or high-profile senior executive or prominent owner?

c) Do we have a reputation for connections to customers, suppliers in geopolitically unstable regions?

d) Are any of our brands considered as controversial by certain groups?

e) Do we, or our customers, supply high-profile individual, organizations or events?

f) Does social media activity indicate potential targeting for cyber intrusion?

B . 3 Factors that could increase the likelihood of a threat to an operation Add/View comments (0)

Questions that the TACCP team can ask to assess the likelihood of a threat to an operation (premises).

a) Are the premises located in a politically or socially sensitive area?

b) Do the premises share access or key services with controversial neighbouring entities?

c) Does the company lack robust screening procedures for new recruits. Especially agency and casual employees?

d) Are services to the premises unprotected/easily accessible?

e) Are utilities to the premises too easily accessible?

f) Are hazardous materials, which could be valuable to hostile groups, stored on site?

g) Do large numbers of people, including the general public, use the location?

h) Do any employees have reason to feel disgruntled or show signs of dissatisfaction?

i) Do we lack an effective confidential reporting procedures for concerns about disgruntled employees or insider threats?

j) Are internal audit arrangements truly independent, with auditors having no operational responsibility for the area, process or site being audited?

k) Have key roles been occupied by the same employee for many years with little supervision?

l) Are our Supervisory Control and Data Acquisition (SCADA) and other control systems, used for real-time monitoring and management of manufacturing, infrastructure, or facility-based processes shared with organizations that could be prime targets?

B . 4 Factors that could increase the likelihood of a threat to a product Add/View comments (0)

Questions that the TACCP team can ask to assess the likelihood of a threat to specific product or process.

a) Have there been significant cost increases affecting this product?

b) Does the product hold specific religious, cultural, ethical or moral significance for certain consumer groups?

c) Could this product be used as an ingredient in a wide range of popular foods?

d) Does the product contain ingredients or other material sourced from other countries?

e) Is the product considered economically high value?

f) Is the product or its brand well known and/or highly recognisable?

NOTE This is not exhaustive of all questions that might be asked to assess a threat.

Annex C (informative)
Assessing vulnerabilities Add/View comments (0)

C . 1 Identifying vulnerabilities Add/View comments (0)

The next step in mitigating risk is identifying vulnerabilities that could enable a threat to succeed. Review of responses to these questions can give an understanding of the factors that can contribute to a threat risk. The TACCP team could ask the following questions to assess potential vulnerabilities.

C . 2 Cyberattack Add/View comments (0)

Questions that the TACCP team can ask to assess both the likelihood and potential impact of cyberattack.

a) Have senior leaders implemented a cyber strategy that clearly defines accountability and responsibility for cybersecurity?

b) Does the organization have an effective approach to managing cyber risks?

c) Are employees likely to recognize and report suspicious electronic communications (e.g. emails, SMS)?

d) Are employees trained on common cyberattack techniques (e.g. phishing, ransomware) and equipped to respond effectively?

e) Is all data appropriately protected in transit, at rest, and at end of life, commensurate with the assessed risks? [4]

f) Are passwords or other authentication methods used?

g) Do policies for employee onboarding, internal transfers or leaving address all accounts, devices and access privileges?

h) Are local Wi-Fi connections encrypted and inaccessible to external users?

i) Does operational technology follow secure design principles?

j) Are internet-enabled processes secure (e.g. can process parameters be changed without proper authorization, or cloud-based records corrupted)?

k) Are data backup data and storage processes effective in protecting business critical information?

l) Are operators promptly notified of changes to production or operational configurations (e.g. product formulations)?

m) Is externally sourced data (from email, internet or removable media) examined for malware before being imported?

n) Does remote access to company systems require multi-factor authentication and the extent of access limited?

o) Are critical computerized systems tested and have offline backups?

p) Are business continuity and disaster recovery plans for IT and production systems in place, routinely tested and deemed effective?

q) Are the identities of suppliers and customers verified before conducting online transactions?

C . 3 Vulnerabilities that could increase the risk of EMA Add/View comments (0)

Questions that the TACCP team can ask to identify vulnerabilities for the risk of EMA.

a) Do we have sufficient trust in our suppliers, and their suppliers (e.g. through verification and audits, or indicators such as food safety incidents, recalls, regulatory non-compliances or do external audit results suggest potential integrity issues)?

b) Do key suppliers implement robust personnel security practices?

c) Do suppliers think we monitor their operation and routinely test their products?

d) Which suppliers are not routinely audited?

e) Are materials supplied through remote, obscure, or indirect channels such as brokers or intermediates?

f) How do our suppliers dispose of excessive waste materials?

g) Are we aware of process shortcuts that could impact our operations or products?

h) Are our employees and those of our suppliers, encouraged to report concerns (e.g. confidential reporting or whistleblowing)?

i) Are certificates of certification or accreditation and certificates of analysis issued by independent parties?

j) Are low-cost substitute materials available?

k) Have there been significant increases in material costs?

l) Has pressure on suppliers' trading margins increased?

m) Are major materials becoming less available (e.g. due to repeated crop failures) or alternatives plentiful (e.g. due to overproduction)?

n) Have there been unexpected increases or decreases in demand?

o) Are product samples retained, especially for items with short shelf life?

C . 4 Vulnerabilities that could increase the risk of malicious contamination Add/View comments (0)

Questions that the TACCP team can ask to evaluate the vulnerability to intentional contamination in its own operations and throughout its supply chain.

a) Could a contaminant be brought into the facility?

b) Could a contaminant be added to the water source (e.g. ground water, rainwater, desalinated water, recycled water) provided by the local or municipal supply?

c) Do storage containers and transportation units have tamper-evident seals?

d) Does the production process involve liquid receiving, storage, handling and loading steps where large volumes make contaminants hard to detect and liquid transfer enables rapid distribution? [28]

e) Are there open and exposed production steps, such as mixing and blending, that allow insider access, where contaminants could blend into the product and be difficult to detect? [28]

f) Is there secondary ingredient preparation involving small volumes but potentially high potency (e.g. allergens or toxins)? [28]

g) Are there fast moving, unattended, high-volume production lines that are difficult to monitor continuously? [28]

h) Would routine quality or food safety monitoring detect a contamination or adulteration in the product?

i) Are personnel security procedures in place and enforced?

j) Is employee boredom, low morale, discipline or recruitment a problem?

k) Do any employees hold a grudge against the organization?

l) Are employees under investigation for misconduct temporarily suspended or reassigned from roles involving direct handling, oversight or access to food production areas?

m) Is there opportunity for access by sympathizers of single-issue groups?

n) Have business competitors been accused of espionage or sabotage?

NOTE This is not exhaustive of all questions that might be asked to assess a vulnerability.

Annex D (informative)
Controls Add/View comments (0)

D . 1 Approaches to control access to an operation Add/View comments (0)

Access controls are critical preventive measures for food defence because almost every serious intentional contamination or sabotage incident requires the attacker to get close enough to the product, ingredients or key processes. TACCP teams are encouraged to consider the relevance and proportionality of their current to determine if new controls or improvements to current controls are required .

a) Access to premises (operation).
   1) Are premises zoned to restrict access to authorized personnel only?
   2) Is access restricted to individuals with a legitimate business need?
   3) Is vehicle parking located outside the perimeter?
   4) Is there visible and comprehensive perimeter fencing?
   5) Is there a perimeter alarm system in place?
   6) Is there controlled access to utility services?
   7) Is there CCTV monitoring and recording of perimeter vulnerabilities?

b) Access to product or process equipment.
   1) Is there ease of access to open or exposed ingredients, work in process (WIP) or finished products?
   2) Is there ease of access to process equipment, ingredient addition points or food safety devices?

c) Access to food transport vehicles.
   1) Are access points monitored?
   2) Are approach roads equipped with traffic-calming devices to slow transit of vehicles?
   3) Are all deliveries scheduled?
   4) Are there documentation checked before admittance?
   5) Are missed deliveries investigated?

d) Access to people.
   1) Are there electronic chip & PIN access controls? [5])
   2) Are changing facilities provided to separate personal clothing and belongings from work wear?
   3) Is visitor access by appointment only?
   4) Is visitor proof of identity required?
   5) Are visitors accompanied throughout the premises?
   6) Is there positive identification of all employees and visitors?
   7) Is there CCTV monitoring and recording of sensitive areas storage and processing areas?

e) Access to electronic systems.
   1) Is there routine monitoring and implementation of best practice cybersecurity measures?
   2) Is there challenge testing by external personnel to access premises, products and process equipment?
   3) Is there routine cyber awareness training for employees?

f) Other considerations.
   1) Is there secure handling of mail and of posted items, (samples, ingredients or customer returns)?
   2) Are there restrictions on portable electronic and camera equipment in sensitive areas?
   3) Are cyber security management systems complaint to industry standards?

D . 2 Tamper detection controls Add/View comments (0)

Tamper detection is an important and cost-effective food defence measure for the TACCP team to consider because it can deter many would-be attackers. Even if prevention fails, visible or recorded evidence of tampering allows the business to stop contaminated product from reaching consumers and to trigger an immediate incident response.

TACCP teams are encouraged to consider the relevance and proportionality of their controls to prevent product tampering.

a) Are there numbered seals on bulk storage silos, (where applicable)?
b) Are there numbered seals on stores of labels and labelled packs?
c) Are effective tamper evident seals applied to retail packs?
d) Are there numbered seals on hazardous materials?
e) Is there close stock control of key materials?
f) Is there recording of seal numbers on delivery vehicles?
g) Are seal numbers confirmed as issued by the supplier on arrival of delivery vehicles?
h) Is there use of continuous seal logs?
i) Are there investigation processes for seal discrepancies?

D . 3 Assuring personnel security Add/View comments (0)

TACCP teams are encouraged to consider the relevance and proportionality of their controls for personnel security .

a) Pre-employment checks.
   1) Is proof of identity required and verified prior to employment?
   2) Is there proof and verification of qualifications?
   3) Is there verification of temporary employees and contractors?
   4) Is there screening of new employees, with more rigorous checks for those in sensitive roles?

b) On-going personnel security.
   1) Are employees in sensitive roles motivated and monitored?
   2) Are confidential reporting arrangements in place?
   3) Are temporary employees and contract workers supervised?
   4) Are individuals able to work alone?
   5) Is there a proactive food protection culture?

c) End of contract arrangements.
   1) Is notification of contract termination sent to relevant personnel for awareness?
   2) Are access cards, ID cards and keys recovered post termination?
   3) Are computer accounts closed or suspended, and hardware (e.g. laptop, mobile phones, etc.) recovered?
   4) Is there reporting of unauthorized access by cyber systems?
   5) Is it standard procedure to have a termination interview to assesses security implications?
   6) Are all branded uniforms returned when personnel leave the business?

NOTE These prompts are not intended to be exhaustive of all controls which might be relevant or proportionate to reduce a risk.

Annex E (informative)
TACCP case studies Add/View comments (0)

E . 1 Introduction Add/View comments (0)

The case studies provided in this annex are entirely fictitious and any resemblance to real organizations is coincidental.

In all case study examples, the TACCP process is applied in varied ways, using different formats from that described in Clause 5 to encourage users of this PAS to adopt a flexible and open-minded approach.

Four case studies are documented to provide examples of how the TACCP threat assessment processes may be adapted and reported by different food businesses.

a) Case study 1, Burgers4Me is a national Quick Service Restaurant (QSR) fast-food chain;

b) Case study 2, Bridgeshire Cheese Company is a small family enterprise that manufactures a range of organic cheeses.

c) Case study 3, FryByNite is a food initiative by an established internet based, non-food operator. The focus of this case study is on cyber threats.

d) Case study 4, F. Armer & Daughters Ltd is an agricultural business that provides a range of fresh produce that is aiming to explore new digital opportunities.

E . 2 Case study 1 Add/View comments (0)

Case study 1 presents an example report following the investigative work of the TACCP team at Burgers4Me, a national QSR chain. The burger range includes standard, jumbo, veggie, cheese and chilli options.

The TACCP team includes Operations Director (Team Leader), Human Resources Manager, Procurement Manager, Technical Manager and the Internal Auditor. The TACCP team also receives contributions from other managers on specialist topics.

a) The Operations Director of Burgers4Me leads the company's Emergency Planning and Business Continuity Committee.

b) The internal auditor has delegated responsibility for security and fraud prevention and is also the company's regulatory compliance officer.

Table E.1 – Burgers4Me threat information Ad

No.	Threats to company and information systems from:	Possible method of operation	Comments
A	Animal rights activists	Vandalism or sabotage	Little evidence of curr
B	Hacktivists 1	Distributed denial of service (DDoS) attack on website	Developing company
C	Hacktivists 2	Ransomware attack	Experienced in 2020;
D	Company buyers	Fraud; collusion with suppliers	Established team wor
E	Criminals	Counterfeiting; misappropriation of packaging	Increasing risk as bra
No.	**Threats to locations from:**	**Possible method of operation**	**Comments**
F	Supporters of local businesses	Adverse publicity; "Guilty by association" with fast food	Some locations report interest
G	Overworked company employees, disenchantment; alliance with extremists (e.g. activists or terrorists)	Petty contamination; possible serious malicious contamination	Some employee short overtime;
H	Single issue groups	Deliberate infiltration of premises	Some recent precede
I	Front line employees	Theft; collusion with customers	Rigorous audit in plac trustworthy (personne
No.	**Threats to product from:**	**Possible method of operation**	**Comments**
J	Suppliers of meat	EMA – non-animal protein, or non-beef meats, replacing meat	Beef is specified and claimed in publicity
K	Front line employees	Deliberate undercooking of patty	Variable rosters minim collusion
L	Front line employees	Selling burger too long after wrapping	
M	Ideologically motivated group	Malicious contamination of component	Official threat level un

NOTE Press reports of concerns about food authenticity are pertinent.

Figure E.1 – Burgers4Me product process threat identification Add/View comments (0)

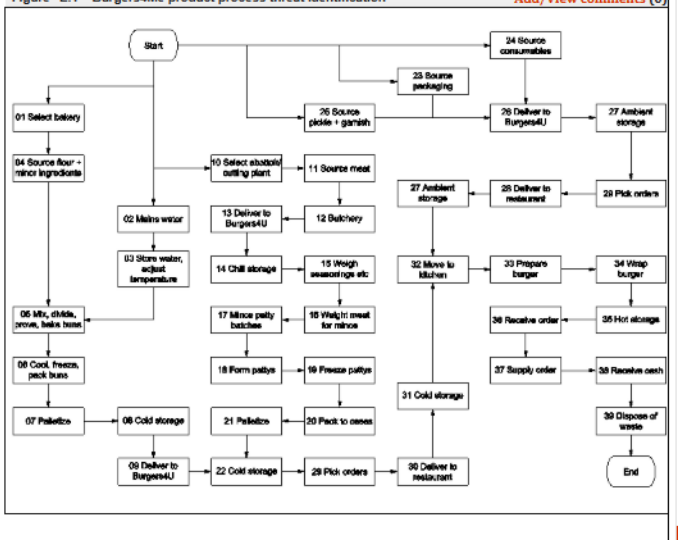


Table E.2 – Burgers4Me threat identification Add/View comment

Step	Process step	Threat	Vulnerability	Access	Mitigation	Adulterant contamination	Impact of process	GA/GC	Likelihood
01A	Select bakery	Various	Casual employees	Production employees	Contracts require personnel security protocols	—	—	—	—
01B		Fraud	Collusion	Buyers	Little	—	—	—	2
02	Mains water	Malicious contamination	Bulk storage reservoirs	Services engineers	Effective control of access	Soluble toxins	Can inhibit yeast; affect dough handling	Can fail sensory tests	1
03	Store water; adjust temperature	Malicious contamination	Batch storage reservoirs	Services engineers	Effective control of access	—	Water may not reach required temperature to effectively clean equipment and utensils	Can contribute to poor sanitation	1
04	Source flour + minor ingredients	Fraudulent substitution	Little cost advantage to fraudster	—	—	—	—	—	—
05	Mix, divide, prove, bake buns	Malicious contamination	Batch mixing operation	Skilled mixer operative	Trained experienced employees	Powdered toxin	Can inhibit yeast; affect dough handling	Can fail sensory tests	1
06	Cool, freeze, pack buns	—	—	—	—	—	—	—	—
07	Palletize	—	—	—	—	—	—	—	—
08	Cold storage	—	—	—	—	—	—	—	—
09	Refrigerated delivery	—	—	—	—	—	—	—	—
10A	Select abattoir/ boning plant	Fraud	Collusion	Buyers	Little	—	—	—	3
10B		Fraudulent substitution	Poor segregation of species	Delivery drivers; process employees	Unique animal identification recorded	Meat from cheaper sources	Negligible	Random tests can detect unless collusion	2

11	Source meat	Fraudulent substitution	Poor segregation of species	Process managers and employees	Inspect meat on receival; confirm from approved suppliers.	Meat from cheaper sources	Negligible	Random tests can detect unless collusion	4
12	Butchery	Fraudulent substitution	Poor segregation of species	Process managers and employees	Check it meets specification for species (e.g. beef)	Meat from cheaper sources	Negligible	Random tests can detect unless collusion	2
13	Delivery to site	Diversion of consignment	Supplier responsibility	—	—	—	—	—	—
14	Chilled storage	—	—	—	—	—	—	—	—
15	Weigh seasonings	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May fail sensory tests	1
16	Weigh meat for mince	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May fail sensory tests	1
17	Mince patty batches	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May fail sensory tests	1
18	Form patties	Malicious contamination	Manual operation	Process managers and employees	Rigorous hygiene standards	Powdered toxins	Negligible	May fail sensory tests	1
19	Freeze patties	—	—	—	—	—	—	—	—
20	Pack to cases	—	—	—	—	—	—	—	—
21	Palletize	—	—	—	—	—	—	—	—
22	Cold storage	—	—	—	—	—	—	—	—
23	Source packaging	Misappropriation Counterfeiting	Supplier warehouse security	Agency delivery drivers	Little	—	—	—	2
24	Source consumables	—	—	—	—	—	—	—	—
25	Source pickle + garnish	Unauthorised ingredient substitution	—	—	Established brands; reliable contracts	—	—	—	—
26	Ambient delivery to site	—	—	—	—	—	—	—	—
27	Ambient storage	—	—	—	—	—	—	—	—
28	Deliver to restaurant	—	—	—	—	—	—	—	—
29	Pick orders	—	—	—	—	—	—	—	—
30	Deliver to restaurant	—	—	—	—	—	—	—	—
31	Cold storage	—	—	—	—	—	—	—	—
32	Move to kitchen	Malicious substitution	Out of hours; unsupervised	Night store-employees	Tamper evident cases	'Spiked' patties	Little	None	1
33	Prepare burger	Deliberate undercooking / malicious contamination	Lone worker	Restaurant employees	Rigorous food safety protocols	—	—	None	1
34	Wrap burger	—	—	—	—	—	—	—	—
35	Hot hold	—	—	—	—	—	—	—	—
36	Receive order	Ransomware	Online ordering	Hacktivists	NCSC cybersecurity protocols	—	—	—	2
37	Supply order	Deliberate breach of food safety – Sale of burgers past holding period	Restaurant manager under wastage pressure	—	Personnel security procedures	—	—	—	2
38	Receive cash	Theft	Restaurant employees	Counter employees	Automated cash tills; rigorous audit	—	—	—	4
39	Dispose of waste	Misappropriation	Unlocked external bins	Public	Daily removal of waste	—	—	—	1

NOTE The symbol "—" indicates "not applicable" or "not significant".

TACCP outcomes for Case study 1:

a) The TACCP process identified 20 threats, of which 13 have satisfactory controls in place, with none requiring urgent remedial action.

b) With the growth of online business via web-based agents, a ransomware attack was identified as the primary threat to Burgers4Me. Tenders are invited from cybersecurity consultants to evaluate existing protective measures and to support incident response and recovery activities.

c) Fraud in the selection of abattoir or boning plants remains an ongoing risk, potentially resulting in significant financial penalties and reputational damage. Closely related threats include species substitution and the use of non-meat proteins. The Technical Manager is responsible for overseeing proportionate controls through a mix of remote and on-site supplier audits.

d) As the brand is recognised for its quality and integrity, the risk of counterfeit packaging has increased. A new supplier of branded packaging has been onboarded, demonstrating sufficient controls; however ongoing monitoring is required.

e) Although the Burgers4Me website is not a primary sales platform, it serves a vital marketing role. IT and internal audit activities have been adequately resourced to mitigate cybersecurity threats, particularly DDoS attacks.

f) The Technical Manager monitors official and industry sources for intelligence on emerging risks, and in consultation with the TACCP Team Leader, decides whether to reconvene the team ahead of its scheduled six-monthly meeting.

E . 3 Case study 2 Add/View comments (0)

Case study 2 presents an example threat assessment report for the Bridgeshire Cheese Company (BCC), a family farm owned and operated organic cheese producer selling to speciality retailers and food service businesses. The company makes cheese from their own farm produced milk, supplemented with externally sourced milk when needed.

Figure E.2 illustrates a vulnerability assessment flowchart.

Figure E.2 – Bridgeshire Cheese company vulnerability assessment Add/View comments (0)

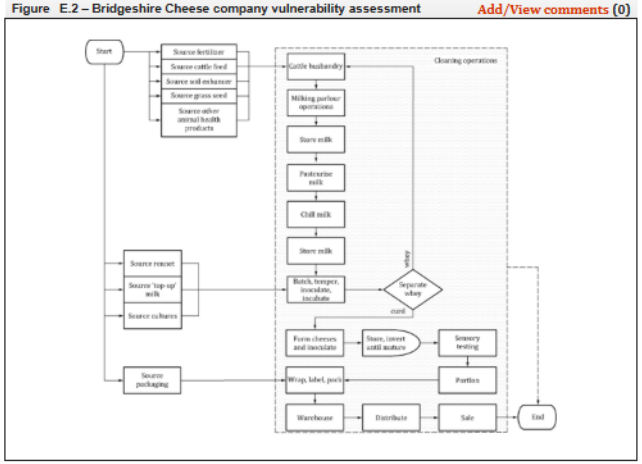


Table E.3 – Bridgeshire Cheese company threat assessment report Add/View comments (0)

Threat No.	Threat / Vulnerability	Consequence	From / Perpetrator	Impact	Likelihood	Score	Protective measures
1	Nonorganic supply from "top-up" milk	Loss of organic status	Suppliers	5	2	10	All raw materials sourced from certified suppliers. Require certificate of conformance for all ad hoc milk purchases.
2	Widespread livestock disease due to right of way through farm	Loss of herd, Loss of insurance cover	Farmers from neighbouring properties	3	2	6	Biosecurity aligned with best practice.
3	Malicious contamination due to unsupervised manual operations	Unsafe product	Operators	5	1	5	All products metal detected prior to release. Production area monitored by CCTV daily. Personal hygiene protocols prevent unauthorised items in production areas. Internal audits assess compliance to personal hygiene protocols twice per year. All employees are family members or long-term trusted partners. Sensory assessment of all batches completed prior to release.
4	Trials of GM crops on perimeter land	Loss of organic status	Farmers from neighbouring properties	5	2	10	Regular communication with adjacent farmers regarding activities that may compromise organic status.
5	Theft of product during transport	Value of goods; Loss of reputation for reliability	Opportunist criminals	2	3	6	Use of approved contracted transport providers. GPS tracking of vehicles. Security seal applied to trailer at dispatch. Records of traceability maintained.
6	Remote cyberattack on cloud controlled production process	Tampering with food safety controls in "Off the peg" SCADA system to reduce pasteurisation time/temperature	Cyber criminals	5	1	5	Maintain separate QC analysis of product. Follow NCSC cyber security advice. Software supplier has proven firewalls and malware protection.

7	Dilution of milk - addition of water	Product dilution	Farmer	3	1	3	Use of approved supplementary milk suppliers. Routine testing to detect added water. Product traceability maintained.
8	Deliberate mislabelling	Unauthorised extended shelf life, loss of traceability	Operators	3	1	3	Automated coding and labelling systems. 'Buddy system' for packing and labelling activities. Independent verification checks completed for each production run.
9	Deliberate use of out-of-date product	Consumer harm	Sales and engineering	3	1	3	Traceability maintained. Regular stock checks. Waste management protocols.
10	Deliberate by-passing of food safety pasteurisation	Under pasteurised product	Operators	5	1	5	Routine product testing for pasteurisation of each batch.

TACCP outcomes for Case study 2.

a) Six threats to BCC operations were identified.

b) All were assessed to be under proportionate control.

c) A cyberattack on the SCADA monitoring and control system could have a significant impact, however BCC is an unlikely target and protective measures are up to date.

d) Loss of organic status would harm the business, but reasonable precautions are in place.

E . 4 Case study 3 Add/View comments (0)

FryByNite (FbN) is a new venture launched by a major internet-based general trading company, offering a hot food delivery service. The company is a world leader in its software and logistics management but is new to food business operations. It recognizes its weakness in food operations and has engaged a consultant food safety specialist for the duration of the launch and consolidation phases of FryByNite.

FryByNite aims to deliver freshly cooked, hot food to customers' doorsteps within 30 minutes of receiving a web or telephone order. The standard offering is fish and chips, with each delivery vehicle carrying programmable fryers.

Raw product is ordered over the internet from a network of contracted fast-food outlets. These outlets pre-prepare the food and load it into the frying baskets used by the delivery vehicle.

A global positioning system (GPS) estimates the time to customers' premises and initiates the frying process on route. When ready, the frying baskets withdraw automatically, the food is packaged and kept hot, so that customers receive hot, freshly cooked food as if they had visited the outlet in person.

The TACCP team includes:

a) Director of Human Resources (Team Leader);

b) Director of Information Systems;

c) Food safety consultant; and

d) Facility and security manager.

Figure E.3 – FryByNite workflow Add/View comments (0)

Table E.4 – FryByNite threat information Add/

No	Threat actors	Threats to organization:	Possible method of operation	Comments
1	Hacktivists	Failure of web-based ordering system	DDoS attack	Protected by and inhouse
2	Nation states	Loss of GPS-based navigation	Over-commitment and/or inadequate maintenance by satellite operators	No control o strong contra operators
3	Extortionists	Exfiltration of sensitive data	Phishing emails to employees	Ransomwar
4	Insiders	Theft of IP	Unauthorized access to administrative privileges	—
Threats to product				
5	Aggrieved suppliers	Contamination resulting in food borne illness	Inadequate handling of product	—
6	Competitors	Contamination resulting in food borne illness	Failure of van cooking regime	From power f process contr
7	Aggrieved employee	Contamination resulting in food borne illness	Malicious contamination	Personnel se proportionate
Threats to operations				
8	Criminals	Attack on vehicle/driver	Mugging for cash	Signs: "No ca place
9	Vandals	Petty damage to vehicle	Random unplanned opportunism	Riskier areas
10	Fraudsters	Loss of income	Use of stolen personal data to create false account	—

Table E.5 – FryByNite threat assessment Add/

Step	Threat	Threat	Vulnerability	Mitigation	Contaminant	Comment
A	DDoS (1)	A1	High – public site	Corporate systems give early warning	—	Nuisance; loss of sales; annoyed customers.
A	Inter-bank failure (2)	A2	Electronic funds transfer system is a prime cyber target, but well protected	Maintaining close links with system operators.	—	Small chance of major loss.
B	Fraudulent account (10)	B1	Fictitious delivery point	Check new accounts on set - up	—	Time waster
C	Supplier not available	C1	Databases out of date	Close partnership with suppliers	—	Time waster
C	Product contamination (5) (6) (7)	C2	Batter may be target	Suppliers vetted for HACCP operation	Toxic chemicals; spore-forming bacteria	Supplier does not know customer identity, unless collaboration.
C	Product substitution (5)	C3	Opportunistic food fraud	As C2	Exchange of species	Reputation and regulation
D	GPS failure	D1	Poor signal	Liaison with telecoms providers	—	Contingency plans in place
F	Corruption of control system with malware (1) (4)	F1	New technology: problems likely	Trials show resilience	—	Fire, overcooked or undercooked food possible
G	Undercooking	G1	Oversized fillets	Size limits	—	Product inedible
G	Product contamination (4)	G2	Unsupervised manual operation	Personnel screening	Toxic chemicals	—
H	Delays on route	H1	Unexpected traffic or roadworks	Automatic updates of satnav	—	Compensation if food inedible
H	Assault on employee (8)	H2	Some difficult customers and areas	Employee training in conflict avoidance	—	A key concern in some areas.
H	Damage to vehicle (9)	H3	Vehicle unsupervised during delivery	Riskier areas noted on satnav system	—	Largely nuisance
J	Inappropriate disposal of waste oil (7)	J1	Employees under pressure seeking shortcuts	Replacement "new for old"	—	Reputation damage
J	Use of wrong oil	J2	Employees under pressure seeking shortcuts or covering mistakes	Replacement 'new for old'	Other inedible oils Toxic organic chemicals	Issues: labelling; allergy; integrity; toxicity; fire safety.

Figure E.4 - FryByNite Threat Prioritization Add/View comments (0)

Impact		1 Unlikely to Happen	2 May Happen	3 Some Chance	4 High Chance	5 Very High Chance
5 Catastrophic			H2	F1		
4 Major		C2 J2	A2 G2			
3 Significant						
2 Some		H3 J1		C3	A1	
1 Minor		B1 C1 D1 G1		H1		
		Likelihood				

Table E.6 – FryByNite threat register Add/View comments (0)

Threat	Rating (Likelihood - Impact)	Description	Further defensive action	Responsibility	Comment
F1	(3,5)	Corruption of process control system for fryers	Daily review through roll-out and consolidation phases. Build contact with software provider.	Director of InfoTech	Target (2.3) within one year.
A1	(4,2)	DDoS - website	Build NCSC contact. Track social media chatter.	Director of InfoTech	Ongoing. Risk assessment score unlikely to change.
H2	(2,5)	Assault on employee	Evaluate use of body cameras	Director of InfoTech	With Director of Human Resources
C3	(3,2)	Fraudulent product substitution	Introduce low level overt product sampling	Consultant food technologist	Target (1,2)
A2	(2,4)	Inter-bank funds transfer failure	Continue current protocols.	Director of InfoTech	Insurance cover adequate.
G2	(2,4)	Malicious product contamination	Introduce on-going personnel security routines.	Director of Human Resources	Target (1,4)
H1	(3,1)	Delays on route	Continue current protocols.	—	Under proportionate control.
J1	(1,2)	Inappropriate disposal of waste oil	Review and promote 'new for old' model.	Director of Human Resources	Target (1,1) within one year.
H3	(1,2)	Damage to vehicle	Continue current protocols.	—	Under proportionate control.
C2	(1,4)	Malicious product contamination	Include handling of non-food chemicals in supplier accreditation.	Consultant food technologist	Risk assessment score unlikely to change.
J2	(1,4)	Use of wrong oil	Build technology into induction training.	Director of Human Resources	Risk assessment score unlikely to change.
B1	(1,1)	Fraudulent customer account	No further action required.	—	Under proportionate control.
C1	(1,1)	Supplier not available	Review training of database admin.	Director of Human Resources	—
D1	(1,1)	GPS failure	No further action required.	—	Under proportionate control.
G1	(1,1)	Undercooked product	No further action required.	—	Under proportionate control.

TACCP outcomes for Case study 3 .

a) The TACCP Team plans to meet monthly to review developments until the new processes are embedded.

b) The TACCP Team has identified 15 threats, of which 8 require the implementation of substantive protective measures.

c) Remote control of the frying operation creates the risk for new threats (F1) which have been prioritized and addressed at the senior management level.

d) Precautions, i.e. appropriate training, from the launch of the initiative have kept the likelihood of assault on employee low, but it is recognised that further work is needed.

e) The parent company's senior management maintains a low-profile public image reducing the likelihood of FbN being targeted.

E . 5 Case study 4 Add/View comments (0)

Case study 4 is based on an established agricultural company, F. Armer & Daughters Ltd. This business has evolved from a family-owned, mixed farming operation, supplying seasonal produce to local markets to a dynamic operation offering a wide range of fresh vegetables under its "Fresh as Can Be" proposition to retail outlets. Additionally, it cultivates select fruits and specialty cereals to complement its vegetable rotation and is exploring opportunities to expand its produce range for the food service sector.

The business is managed on a day-to-day basis by the descendants of the farm's founder. It employs a small team to run the highly mechanized cleaning and packing facility but has a heavy reliance on agricultural contractors for farming work, using temporary employees during peak periods. It is committed to external verification of its processes and risk-based procedures and receives exemplary reports from certification bodies and multiple customers alike.

The company has recently undertaken an extensive upgrade in automation and remote control of both farming and pack-house operations. It is committed to the use of unmanned aerial vehicles (UAVs) for crop surveillance to better manage irrigation, application of pesticides, fertilizers, other treatments and time of harvesting. It intends to fully integrate chilling, cleaning, trimming and packing processes, to significantly reduce the time from field to dispatch.

As part of this initiative and as it rolls out, the Directors have contracted a consulting information security specialist to conduct a TACCP exercise related specifically to the new precision agriculture technologies. Risk management of the conventional business is well established. The intention is to implement proportionate controls.

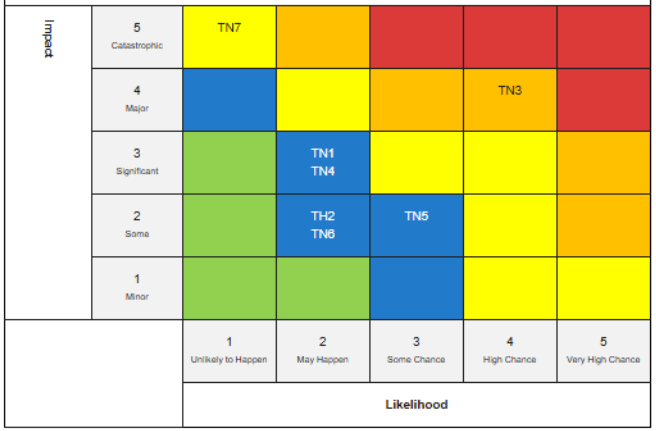
Table E.7 – F. Armer & Daughters Ltd possible sources of malicious activity Add/View comments (0)

Greatest threat from:	Moderate threat from:	Lowest threat from:
Hacktivists	Alienated former employees seeking vengeance	Competitors
Sabotage of IT support infrastructure	Activists seeking publicity	Environmental campaigners
Extortionists	—	Contractors
Criminals stealing innovative IP	—	—

Table E.8 – F. Armer & Daughters Ltd risk assessment Add/View comments (0)

Threat No.	System	Threat	Vulnerability	Mitigation	Comment	Likelihood	Impact
TN1	Electronic ordering from customers	Communication disruption (weather events, accident, sabotage, incompetence)	Operation can be slow but has not failed in 5 years	Strong personal arrangements with buyers so mobile call is an expedient	—	2	3
TN2	Electronic ordering from customers	Data corruption during transfer	Intervention by unauthorized parties	Significant variances from planned volumes would prompt as investigation	—	2	2
TN3	Raising processing orders for pack-house	Malfunction of data transfer	Disruption to the cleaning/packing operation leading to waste, product shortages and downtime.	Secure, tamper-evident housing for equipment.	Manual entry delays the packing operation to an unacceptable degree.	4	4
TN4	Raising vehicle loading and delivery papers	Data corruption	Major cost penalties from rejected consignments	None identified	Contracted transport provider unlikely to note discrepancies.	2	3
TN5	UAV monitoring of crops	Remote control of device can be taken over by malicious actors	Cameras and sensors fail to spot emerging problems	Routine software updates installed	Both harm caused and theft of the device could be motives for interference.	3	2
TN6	Computer farm record system	Takeover for ransom by criminals	Remote access by Directors over the Internet provides opportunity for criminals	Independent back-up daily would reduce losses. Two-factor verification in place.	Key to operational practice and external certification.	2	2
TN7	Industrial control systems	Sabotage of electronic controls	High cost highly sophisticated instruments cannot be duplicated, so non-operation = non-production	Updating and maintenance is rigorous. Access tightly restricted with two-factor verification.	Contracted service engineer on call 24/7	1	5

Figure E.5 – F.Armer & Daughters Ltd Risk Prioritization Add/View comments (0)



TACCP outcomes for Case study 4.

a) The Company has adopted an integrated manufacturing approach to enhance efficiency and customer service but lacks awareness of the inherent vulnerabilities.

b) The consultant Information Security Specialist has been further contracted to complete the threat assessment and recommend proportionate controls.

c) So far as practicable, duplicate systems are operated until completion of the assessment.

d) Support and advice from the National Cyber Security Centre is used to raise awareness among key contractors and trusted employees.

e) Monthly reviews are planned.

Annex F (informative)
Sources of information and intelligence – UK and EU Add/View comments (0)

F. 1 General Add/View comments (0)

From a global perspective, there are several organizations that contribute information for horizon scanning. The WHO, (World Health Organization), through INFOSAN (International Food Safety Authorities Network), and the FAO, (Food and Agriculture Organization) through EMPRES (Emergency Prevention System) and GIEWS (Global Information and Early Warning System) of the United Nations coordinate global efforts to identify new risks and enact control measures to minimize their impact.

This information is then disseminated to national food organizations like the FSA, (Food Standards Agency), in the United Kingdom. National food organizations cascade this information to food businesses, typically through trade associations.

The FSA provides information about emerging risks to food supply and horizon scanning. For further information see:

a) FSA Emerging Challenges and opportunities, https://www.food.gov.uk/research/emerging-challenges-and-opportunities

b) FSA Research & Evidence Platform, https://science.food.gov.uk

c) FSA Food Alerts, https://www.food.gov.uk/search?filter_type%5BFood%20alert%5D=Food%20alert&filter_type%5BAllergy%20alert%5D=Allergy%20alert

NOTE Paid subscription services which provide helpful information include:

- *HorizonScan, which monitors global food integrity issues [6];*
- *Food Fraud Database [7]; and*
- *US-CERT: United States Computer Readiness Team [8].*

F. 2 Information and intelligence levels Add/View comments (0)

Figure F.1 illustrates the global dissemination and exchange of information and intelligence about emerging risks to food which may be used to update TACCP assessments. Five levels, ranging from 1 (lowest) to 5 (highest), may be used to describe different levels of information sharing:

a) Level 1 – Food organization;

b) Level 2 – Local;

c) Level 3 – National;

d) Level 4 – European; and

e) Level 5 – International.

Figure F.1 – Dissemination of information and intelligence about emerging risks to food
Add/View comments (0)

F.3 International organizations Add/View comments (0)

In addition to the organisations responsible for the international dissemination of information and intelligence on emerging risks, the following entities provide varying levels of support in the area of food defence. Further details can be found on their respective websites.

a) European Food Safety Authority (EFSA) provides scientific support.

b) Europol provides law enforcement.

c) Rapid Alert System for Food and Feed (RASFF) provide EU alerts.

F.4 European organizations Add/View comments (0)

European Government and Food Industry Associations may provide additional sector specific food defence guidance, best practice recommendations, training and confidential industry alert systems. Further details can be found on their respective websites.

a) AIPCEE CEP (Fish Processors & Traders).

b) CEEREAL (European Breakfast Cereal Association).

c) CLITRAVI (The Liaison Centre for the Meat Processing Industry in the European Union).

d) COPA & COGECA (European Farmers).

e) Eucolait (European Dairy Trading).

f) European Dairy Association (European Milk Processing).

g) European Chilled Food Federation (ECFF).

h) European Smoked Salmon Association (ESSA).

i) European Sprouted Seeds Association.

j) FEFAC (European Feed Manufacturers Federation).

k) Food Drink Europe.

l) Fresh Fel (Fresh Produce).

m) Profel (European Association of Fruit & Vegetable Processors).

n) UECBV (European Livestock & Meat Trades Union).

F.5 National UK organizations Add/View comments (0)

UK Government and Food Industry Associations may provide additional sector specific food defence guidance, best practice recommendations, training and confidential industry alert systems. Further details can be found on their respective websites.

a) Animal and Plant Health Agency (APHA).

b) Agricultural Industries Confederation.

c) Association of Independent Meat Suppliers.

d) British Frozen Food Federation.

e) British Meat Processors Association.

f) British Poultry Council.

g) British Veterinary Association.

h) Chilled Food Association.

i) Cold Chain Federation.

j) Council for Responsible Nutrition UK.

k) Dairy UK.

l) Food and Drink Federation.

m) Fresh Produce Consortium.

n) Foodchain and Biomass Renewables Association.

o) Health Food Manufacturers Association.

p) International Meat Trade Association.

q) National Farmers Union of England and Wales.

r) Nut and Dried Fruit Trade Association.

s) Packaging Federation.

t) Proprietary Association of Great Britain.

u) Provision Trade Federation.

v) Rice Association.

w) Road Haulage Association.

x) Science and Advice for Scottish Agriculture (SASA).

y) Scottish Salmon.

z) Specialist Cheesemakers Association.

aa) The Association of Port Health Authorities.

bb) The Shellfish Association of Great Britain.

cc) UK Flour Millers.

dd) UK Pet Food.

F.6 Reporting food defence incidents and concerns Add/View comments (0)

Reporting an actual food defence incident helps authorities understand the nature and extent of food defence threats and can prevent wider harm.

The appropriate agency depends on the location of the food business, the type of food product and the nature of the incident. Incidents and concerns of criminal activity can be provided to the following organizations:

a) Food Standards Agency https://www.food.gov.uk/contact/businesses/report-safety-concern/report-a-food-crime ; and

b) Scottish Food Crime Hotline 0800 028 7926 https://www.foodstandards.gov.scot/about-us/contact-us/report-a-food-problem .

Annex G (informative)
Complementary approaches to food and drink protection Add/View comments (0)

G. 1 FDA Food Defence Mitigation Strategies Database (USA) Add/View comments (0)

The Food Defence Mitigation Strategies Database is an FDA-developed online tool that serves as a reference library of practical mitigation strategies to help food facilities reduce vulnerabilities due to intentional adulteration. It can assist food businesses in identifying and selecting mitigation measures for actionable process steps (high-risk points identified in vulnerability assessments).

This database includes a list of mitigation strategies tied to common high-risk activities, e.g. bulk liquid handling, ingredient staging, and provides examples covering physical, operational and personnel-based controls.

For further information see https://www.fda.gov/food/food-defense-tools/mitigation-strategies-database .

Free basic food defence awareness training available. Further information can be found on their website: https://www.fda.gov/food/food-defense-training-education/food-defense-101-front-line-employee .

The FDA also provides scenarios based on intentional and unintentional food contamination events to test emergency response plans, protocols and procedures. Further information can be found on their website: https://www.fda.gov/food/food-defense-tools/food-related-emergency-exercise-bundle-free-b .

G.2 Food Crime Risk Profiling Tool, Scottish Food Crime and Investigations Unit, (SFCIU)
Add/View comments (0)

The SFCIU has developed a Food Crime Risk Profiling Tool to assist Food Business Operators in assessing their vulnerability to food crime and identifying measures to mitigate these risks. Further information can be found on their website: https://www.foodstandards.gov.scot/business-guidance/running-a-food-business/food-crime-and-your-business/food-crime/food-crime-risk-profiling-tool .

G.3 UK Food Crime Strategic Assessment

Add/View comments (0)

The UK Food Crime Strategic Assessment (FCSA) is a joint assessment produced by the Food Standards Agency's National Food Crime Unit (NFCU) and Food Standards Scotland's Scottish Food Crime and Incidents Unit (SFCIU). This guide uses a risk-based framework to evaluate threats, covering 7 types of food crime:

a) document Fraud – e.g. fake certificates of conformity;

b) theft – e.g. hijacked shipments;

c) waste diversion – e.g. illegal reuse of expired goods;

d) unlawful processing – e.g. unlicensed slaughter;

e) substitution – e.g. cheaper meats sold as premium;

f) misrepresentation – e.g. false origin labelling; and

g) adulteration – e.g. adding undeclared substances.

This tool can be downloaded from their website: https://www.food.gov.uk/sites/default/files/media/document/FSA-Food%20Crime%20Strategy%202024.pdf .

G.4 Food Standards Agency (UK)

Add/View comments (0)

The Food Standards Agency's National Food Crime Unit (NFCU) has developed a Food Fraud Resilience Self-Assessment Tool to provide support, guidance, and advice to food businesses on food fraud. Further information can be found on their website: https://www.food.gov.uk/food-fraud-resilience-self-assessment-tool .

G.5 SSAFE

Add/View comments (0)

SSAFE offers a free Food Fraud Vulnerability Tool to help food businesses identify vulnerabilities to fraudulent activity, develop mitigation plans, and assess risk at the ingredient, product, or company-wide level. Further information can be found on their website: https://www.ssafe-food.org/tools/food-fraud-vulnerability-assessment-tool .

G.6 UK Food and Drink Federation

Add/View comments (0)

The UK Food and Drink Federation's (FDF) Guide , *Food authenticity: Five steps to help protect your business from food fraud* [29] follows on from FDF's guide, *Risks under the radar - Anticipating supply chain risks for the UK food and drink sector* [30] and provides information on:

a) mapping a business supply chain;

b) identifying impacts, risks and opportunities;

c) assessing and prioritizing the findings;

d) creating a plan of action; and

e) implementing, tracking, reviewing and communicating.

Further information can be found on their website: https://www.fdf.org.uk/fdf/resources/publications/guidance/food-authenticity/

G.7 USDA

Add/View comments (0)

The USDA provides a Food Defence Surveillance Findings Checklist that can be used by businesses to assess threats to a business. This form can be downloaded from their website: https://www.fsis.usda.gov/sites/default/files/FSIS-Form/5420-3.pdf.

NOTE Carver + Shock was referenced in previous FAS editions. It has been removed from this edition as although it can still be used, it is no longer the primary FDA-recommended methodology for FSMA Intentional Adulteration (IA) Rule compliance (21 CFR 121 *) [31].*

Bibliography

Add/View comments (0)

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN 17972:2024, *Food authenticity – Food authenticity and fraud – Concepts, terms and definitions*

BS EN ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

Other publications

[1] FOOD AGRICULTURE ORGANIZATION (FAO) and WORLD HEALTH ORGANIZATION (WHO). *General Principles of Food Hygiene* . Codex Alimentarius Code of Practice, No. CXC 1-1969. Codex Alimentarius Commission. Rome, 2023.

[2] DOMESTIC PREPAREDNESS. Domestic Preparedness - Looking Back to Look Ahead to Protect the Food Supply. October 2022 [9])

[3] FOOD STANDARDS AGENCY (FSA). Food Crime Strategic Assessment 2024 [10])

[4] THE NATIONAL CYBER SECURITY CENTRE (NCSC). NCSC Advice and Guidance - Glossary [11])

[5] NATIONAL PROTECTIVE SECURITY AUTHORITY (NPSA). National Protective Security Authority NPSA. May 2023 [12])

[6] OFFICE FOR NATIONAL STATISTICS. Nature of fraud and computer misuse in England and Wales: year ending March 2022. September 2022 [13])

[7] SCOTTISH GOVERNMENT. Scottish Crime and Justice Survey 2023/24: Main findings [14])

[8] FBI PUBLIC INTELLIGENCE. FBI Cyber Bulletin: Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector. March 2016 [15])

[9] CNN BUSINESS NEWS. Fired Disney employee allegedly hacked into company system to change allergen info on menus. October 2024 [16])

[10] NCA, NCSC and. NATIONAL CYBER SECURITY CENTRE (NCSC). The cyber threat to UK business. 2018 [17])

[11] BLEEPING COMPUTER. Food Delivery Service in Germany Under DDoS Attack. March 2020 [18])

[12] NATIONAL CYBER SECURITY CENTRE (NCSC). Ransomware: What you need to know about ransomware [19])

[13] BBC NEWS. Meat giant JBS pays $11m in ransom to resolve cyber-attack. June 2021 [20])

[14] Stergios Melios, Afroditi A. Asimakopoulou, Ciara M. Greene, Emily Crofton, Simona Grasso . SCIENCE DIRECT. Food-related fake news, misleading information, established misconceptions, and food choice. June 2025 [21])

[15] BBC NEWS. Why people believe the myth of 'plastic rice'. July 2017 [22])

[16] OLIVE OIL TIMES. Italy Arrests 33 Accused of Olive Oil Fraud. February 2017 [23])

[17] THE ECONOMIC TIMES. Delhi Spice Scam: Police uncover massive racket; acid, wood dust allegedly mixed in masala. May 2024 [24])

[18] DAILY NATION. Nakuru traders selling 'poisoned' milk arraigned in court. April 2016 [25])

[19] WORLD HEALTH ORGANIZATION (WHO). Disease Outbreak News. September 2008 [26])

[20] EUROPOL. Operation OPSON IX. 2021 [27])

[21] BBC NEWS. Japan food pesticide scare: Factory worker arrested. January 2014 [28])

[22] FOOD STANDARDS AUSTRALIA NEW ZEALAND (FSANZ). Strawberry tampering incident. September 2019 [29])

[23] BBC NEWS. Factory worker who contaminated food destined for Nando's jailed. October 2022 [30])

[24] EURPOL. European Union Terrorism Situation and Trend Report 2018 (TESAT 2018). 2018 [31])

[25] BBC NEWS. BBC Derby terror plot: The online Casanova and his lover. January 2018 [32])

[26] BBC NEWS. Tesco blackmail plot: Nigel Wright contaminated baby food. August 2020 [33])

[27] US DEPARTEMNT OF JUSTICE. Chinese National Pleads Guilty to Economic Espionage Conspiracy. January 2022 [34])

[28] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, FDA & CENTER FOR FOOD SAFETY AND APPLIED NUTRITION. Mitigation Strategies to Protect Food Against Intentional Adulteration: Guidance for Industry. 2019 [35])

[29] FOOD AND DRINK FEDERATION. Guidance. Food Authenticity: Five steps to help protect your business from food fraud . 2024 [36])

[30] FOOD AND DRINK FEDERATION. Risks under the radar - Anticipating supply chain risks for the UK food and drink sector [37])

[31] U.S. FOOD AND DRUG ADMINSTRATION (FDA). FSMA Final Rule for Mitigation Strategies to Protect Food Against Intentional Adulteration [38])

Further reading

Business continuity and crisis management

BS EN ISO 22313 , *Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301*

BS ISO 22301, *Security and resilience – Business continuity management systems – Requirements*

ISO 22361, Security and resilience – Crisis management – Guidelines

Supply chain security

BS ISO 28000, *Security and resilience – Security management systems – Requirements*

PD CEN/TR 16412, *Supply chain security (SCS) – Good practice guide for small and medium sized operators*

Information security

BS ISO/IEC 27001, *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

Other standards

BS 10501, *Guide to implementing procurement fraud controls*

---

[1]) Further information is available from https://www.npsa.gov.uk/security-best-practices/security-culture/security-culture-tool .

[2]) Further information on management of an incident is available from https://www.npsa.gov.uk/protected-procurement-business-leaders .

[3]) Further information is available from https://www.ncsc.gov.uk ; (.

[4]) Further information is available from https://www.ncsc.gov.uk/collection/10-steps.

[5]) Further information is available from https://www.ncsc.gov.uk/information/top-tips-for-staff .

[6]) Further information is available from https://horizonscan.fera.co.uk

[7]) Further information is available from https://www.foodchainid.com/products/food-fraud-database

[8]) Further information is available from https://www.ebsco.com/research-starters/computer-science/us-computer-emergency-readiness-team-us-cert

[9]) Available at https://www.domesticpreparedness.com/cbrne/preparedness-looking-back-to-look-ahead-to-protect-the-food-supply-2/.

[10]) Available at https://www.food.gov.uk/sites/default/files/media/document/FSA-Food%20Crime%20Strategy%202024.pdf.

[11]) Available at https://www.ncsc.gov.uk/section/advice-guidance/glossary.

[12]) Available at https://www.npsa.gov.uk/resources/npsa-insider-risk-definition.

[13]) Available at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingm

[14]) Available at https://www.gov.scot/publications/scottish-crime-and-justice-survey-2023-24-main-findings/pages/fraud-and-computer-misuse/.

[15]) Available at https://publicintelligence.net/fbi-smart-farm-hacking/.

[16]) Available at https://edition.cnn.com/2024/10/30/business/fired-disney-employee-allegedly-hacked-into-company-system-to-change-allergy-info-on-menus.

[17]) Available at https://www.ncsc.gov.uk/files/ncsc_nca_report.pdf.

[18]) Available at https://www.bleepingcomputer.com/news/security/food-delivery-service-in-germany-under-ddos-attack/.

[19]) Available at https://www.ncsc.gov.uk/ransomware/home.

[20]) Available at https://www.bbc.com/news/business-57423008.

[21]) Available at https://www.sciencedirect.com/science/article/pii/S2214799325000396?ref=pdf_download&fr=RR-2&rr=99621f4d5a34d5e0.

[22]) Available at https://www.bbc.com/news/blogs-trending-40484135.

[23]) Available at https://www.oliveoiltimes.com/business/italy-arrests-33-accused-olive-oil-fraud/55364.

[24]) Available at https://economictimes.indiatimes.com/industry/cons-products/food/delhi-spice-scam-15-tonnes-of-adulterated-masalas-seized-3-arrested/articleshow/109670561.cms?from=mdr.

[25]) Available at https://nation.africa/kenya/counties/nakuru/Agency-arrests-Nakuru-traders-selling--poisoned--milk/1183314-3148894-j26vi3/index.html.

[26]) Available at https://www.who.int/emergencies/disease-outbreak-news/item/2008_09_29a-en.

[27]) Available at https://www.europol.europa.eu/cms/sites/default/files/documents/opson_ix_report_2021_0.pdf.

[28]) Available at https://www.bbc.com/news/world-asia-25901568.

[29]) Available at https://www.foodstandards.gov.au/publications/Strawberry-tampering-incident.

[30]) Available at https://www.bbc.com/news/uk-england-hereford-worcester-66997510.

[33] Available at https://www.bbc.com/news/uk-england-lincolnshire-53849726.

[34] Available at https://www.justice.gov/archives/opa/pr/chinese-national-pleads-guilty-economic-espionage-conspiracy.

[35] Available at https://www.fda.gov/media/105742/download.

[36] Available at https://www.fdf.org.uk/fdf/resources/publications/guidance/food-authenticity/ .

[37] Available at https://www.fdf.org.uk/globalassets/resources/publications/risks-under-radar-april2020.pdf.

[38] Available at https://www.fda.gov/food/food-safety-modernization-act-fsma/fsma-final-rule-mitigation-strategies-protect-food-against-intentional-adulteration.

別紙４

R7研究成果の刊行に関する一覧表

書籍

著者氏名	論文タイトル名	書籍全体の編集者名	書　籍　名	出版社名	出版地	出版年	ページ

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
甲斐剛志、葛西伶乃凛、古澤魁世、菊島優菜、岩崎雄介、伊藤里恵、田口貴章、堤智昭、今村知明、穐山浩	食品テロ対策のためのヒト血液中のシアン化物イオン及びチオシアン酸イオンの同時分析法の確立	日本食品科学学会誌	32(1)	10-14	2025 島津賞受賞
畠山理沙、佐々木国玄、赤星千絵、小河内麻衣、駒根綾子、清水英明、渡辺麻衣子、工藤由起子、岡部信彦	流通食品表面におけるSARS-CoV-2汚染実態調査について	食品衛生学雑誌	66(5)	106-111	2025
長田瑞花、多川優也、田崎ひなた、薮内琉也、今村知明、加藤礼識.	飲食店における食品防御対策の新たな課題「ロボット配膳システム」における食品防御対策の検討	食品衛生研究	76巻１号	9-19	2026.01

令和８年２月３日

厚生労働大臣　殿

機関名　公立大学法人奈良県立医科大学

所属研究機関長　職　名　理事長

氏　名　細井　裕司

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　食品の安全確保推進研究事業

２．研究課題名　新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究

３．研究者名　（所属部署・職名）　公衆衛生学講座・教授

（氏名・フリガナ）　今村　知明・イマムラ　トモアキ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。

（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和8年　3月　　12日

厚生労働大臣

機関名　川崎市健康安全研究所

所属研究機関長　職　名　所長

氏　名　三﨑　貴子

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　食品の安全確保推進研究事業

２．研究課題名　新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究

３．研究者名　（所属部署・職名）川崎市健康安全研究所・参与

（氏名・フリガナ）岡部　信彦・オカベ　ノブヒコ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和　8年　3月　31日

厚生労働大臣
~~（国立医薬品食品衛生研究所長）~~ 殿
~~（国立保健医療科学院長）~~

機関名　　国立保健医療科学院

所属研究機関長　職　名　　院長

氏　名　浅沼　一成

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　食品の安全確保推進研究事業

２．研究課題名　新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究

３．研究者名　（所属部署・職名）　医療・福祉サービス研究部・部長

（氏名・フリガナ）　赤羽　学・アカハネ　マナブ

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること （指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。

令和8年3月16日

厚生労働大臣 殿

機関名　茨城キリスト教大学

所属研究機関長　職　名　学長

氏　名　東海林　宏司

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　食品の安全確保推進研究事業

２．研究課題名　新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究

３．研究者名　（所属部署・職名）　生活科学部食物健康科学科　講師

（氏名・フリガナ）　加藤　礼識　（カトウ　ヒロサト）

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。

（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。

・分担研究者の所属する機関の長も作成すること。

令和8年3月2日

厚生労働大臣

機関名　国立大学法人九州大学

所属研究機関長　職　名　総長

氏　名　石橋 達朗

次の職員の令和７年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　食品の安全確保推進研究事業

２．研究課題名　新型コロナ感染症拡大収束後の食品等事業者の新たな営業形態にも対応した食品防御の推進のための研究

３．研究者名　（所属部署・職名）　大学院医学研究院・准教授

（氏名・フリガナ）　入江　芙美（イリエ フミ）

４．倫理審査の状況

	該当性の有無 有　無	左記で該当がある場合のみ記入（※1）		
		審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。

（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　）

（留意事項）　・該当する□にチェックを入れること。