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。

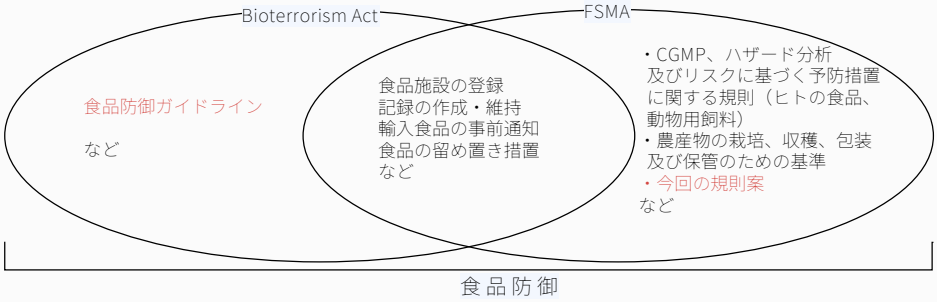
✓IA規則は、緩和戦略、戦略の組み合わせ、またはFDP全体が適切に実施されていない場合など、特定の状況において、食糧防衛計画(FDP)の再分析を要求しています。

✓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

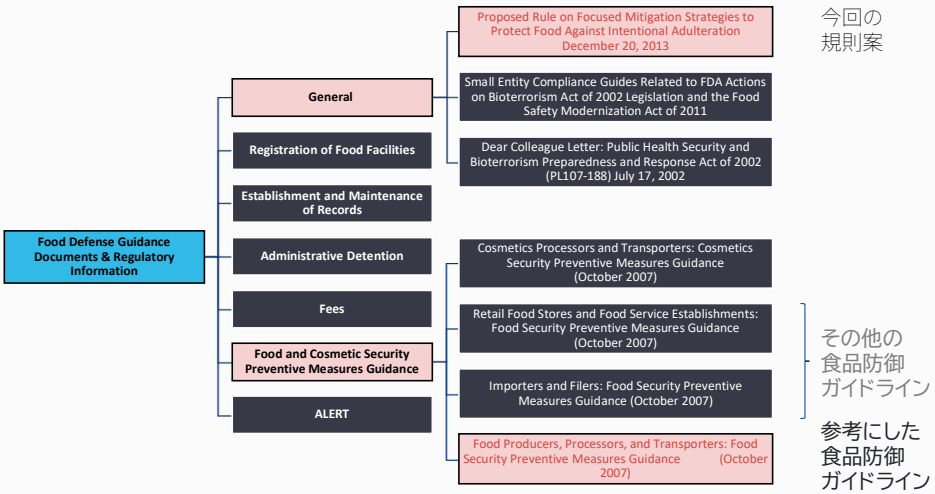
- FDA食品防御ガイドラインは、Bioterrorism Act(2002)を踏まえ、非拘束的な食品テロ予防措置として作成(*1)
  - 現在も2007.10ver.を最新版として公開(*2)
- FSMA(2011)は、食品安全・防御強化の一環として食品防御対策を検討・策定
  - Bioterrorism Actの関係規則・施策の一部を充実・強化
  - 追加的な規則・施策を作成・運用⇒今回の規則案 など



*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。

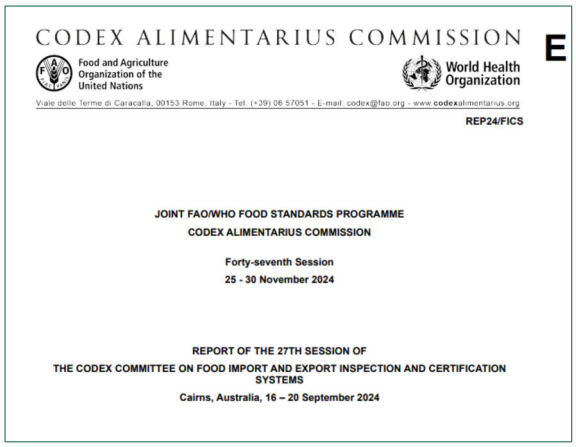
今後の展望:

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

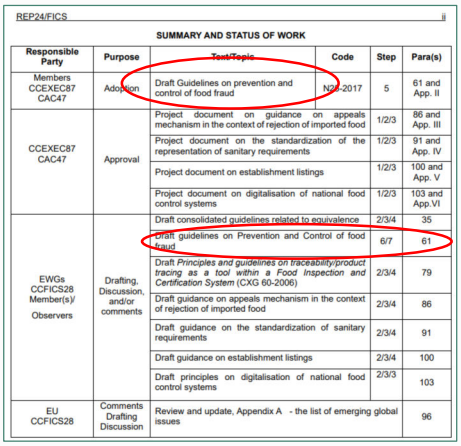
Forty-seventh Session

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。

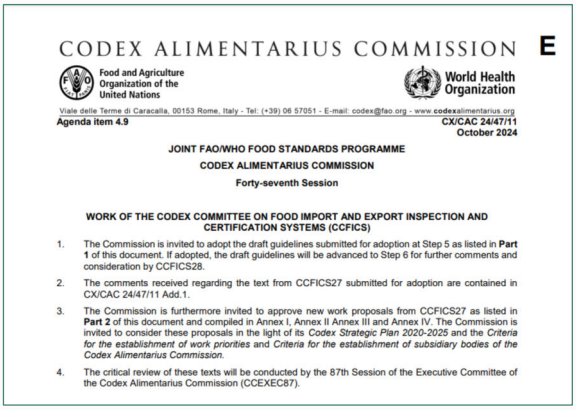
(2)電子的作業部会の設置: ガイドライン原案の改訂を進めるため、電子的作業部会（EWG）が設置されることが決定されました。この作業部会は、米国が議長国を務め、英国、中国、EU、イラン、パナマが共同議長国として参加します。

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

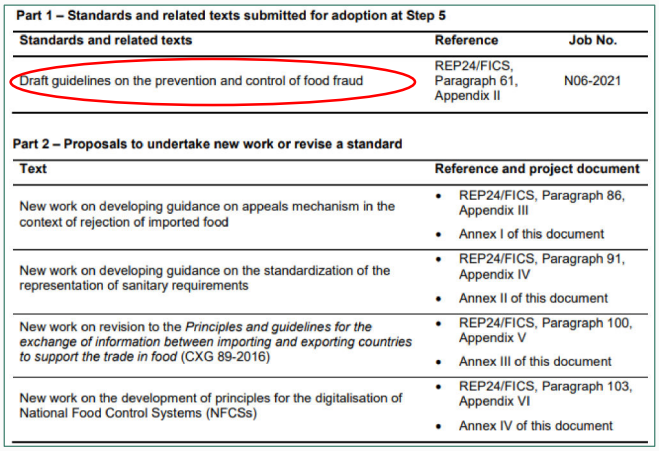
JOINT FAO/WHO FOOD STANDARDS PROGRAMME

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。

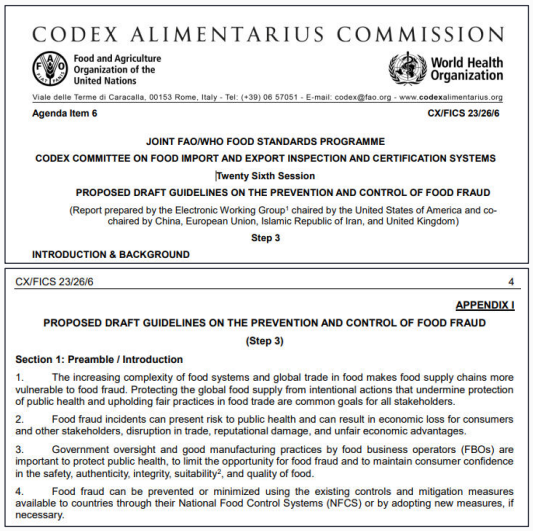
対処方針

・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）。

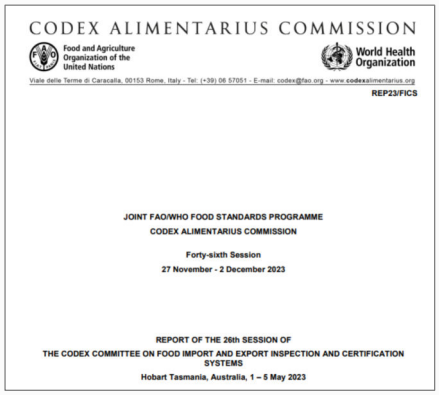
■「食品偽装の防止及び管理に関するガイドライン」の今後

- 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

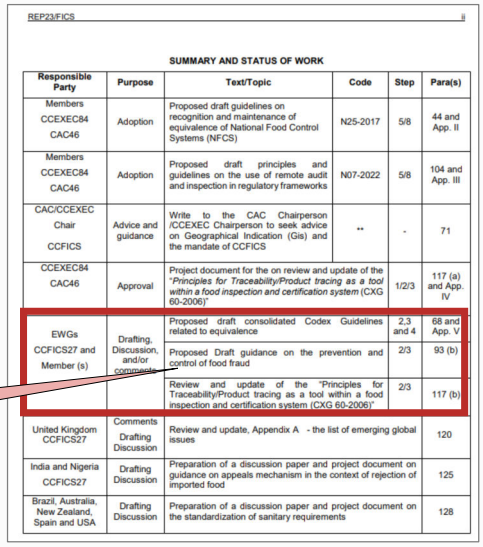
Forty-sixth Session

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

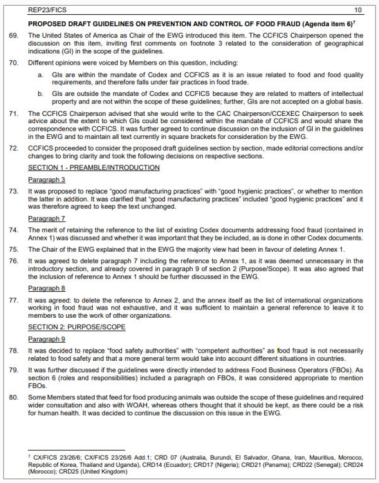
TABLE OF CONTENTS

- 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

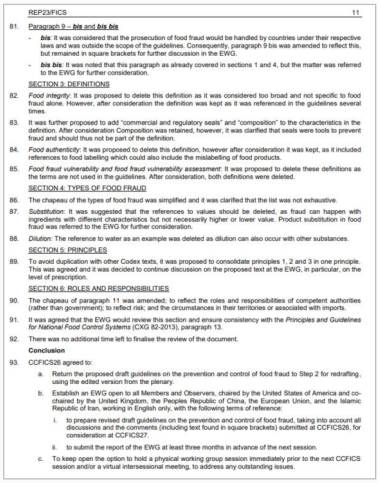
Paragraph 9

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。

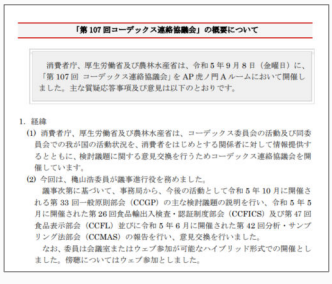
・同じく議題 6 について、菅沼修委員から、GI に関する議論に関して、本ガイドラインの所掌範囲内とすべきというEUと、所掌範囲外とすべきという米国で対立構造になっているのか、また、この議論については今後も電子的作業部会（EWG）において継続されるようだが、打開策はあるのか、質問がありました。これについ て、GI については WTO の「知的所有権の貿易関連の側面に関する協定（TRIPS）」など、他の会議体での議論においても、GI の保護を拡充しようとする国々とそれに反対する国々との間で対立構造ができており、本ガイドラインの議論でも同様の構造が見られていること、我が国としては GI については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。

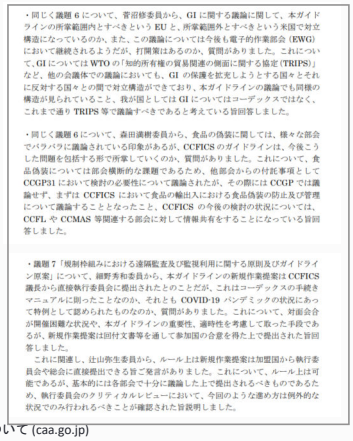
(2) 今回は、穐山浩委員が議事進行役を務めました。

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）

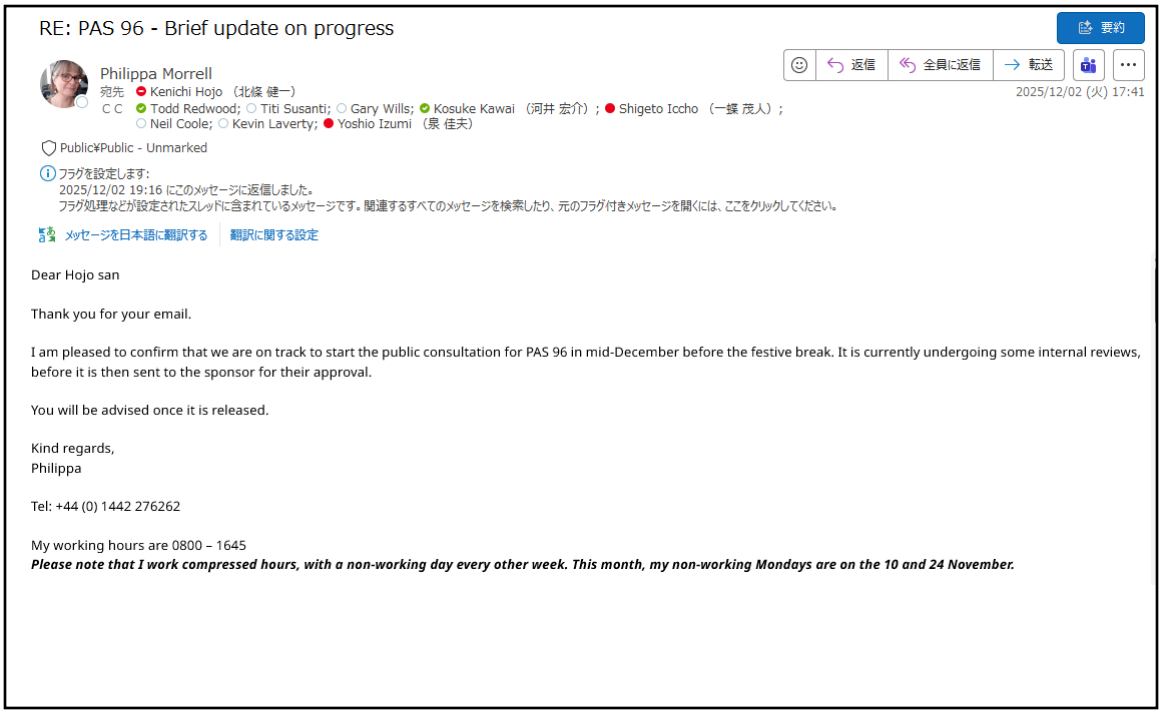
２）サイバー・IT・遠隔操作由来の脅威の明確化デリバリー、遠隔制御、オンライン受注等を想定したケースを提示物理的混入に限らない食品防御の対象範囲を明確化（論拠：Case study（FryByNite 等）、Annex G）

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

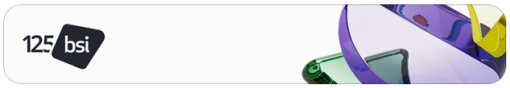
When making a comment please also provide a proposal for how your comment could be resolved.

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

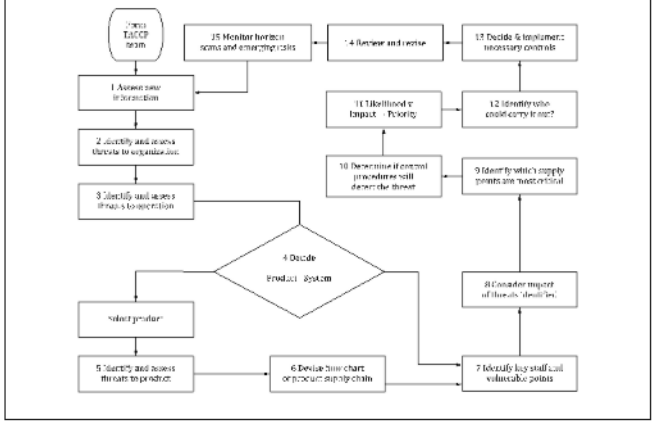
7) maintaining information and intelligence systems to enable revision of priorities and controls when circumstances change.

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).

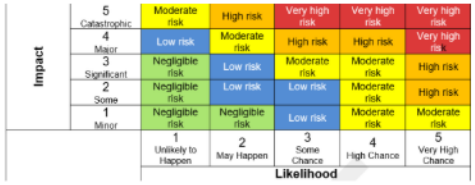
The impact or potential consequences if a threat were successfully carried out, can be assessed by evaluated using two assessment criteria.

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:

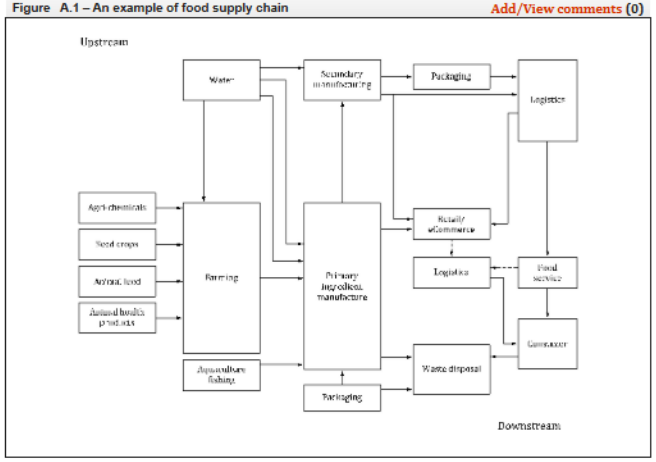
a) There are multiple vulnerable points as the modern food supply chain is long, complex and global from primary production (farms, fisheries), ingredient suppliers, manufacturers, logistics (storage, transport and distribution), through to retail and food service. Each step in the chain can provide 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)

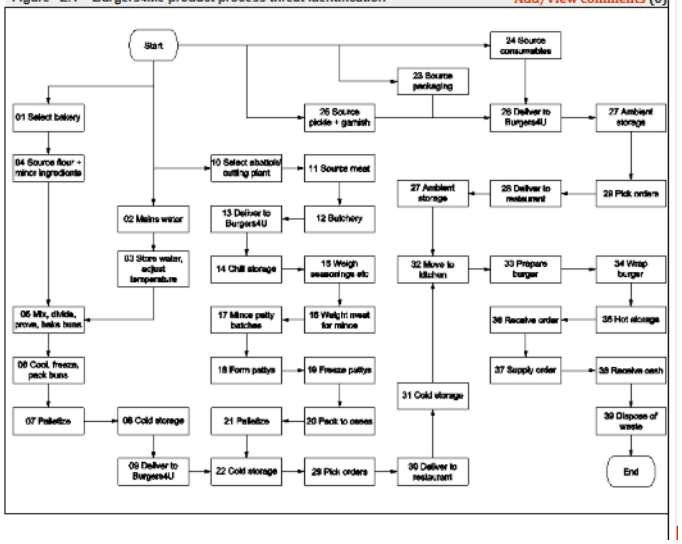


Table E.2 – Burgers4Me threat identification Add/View comment

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)

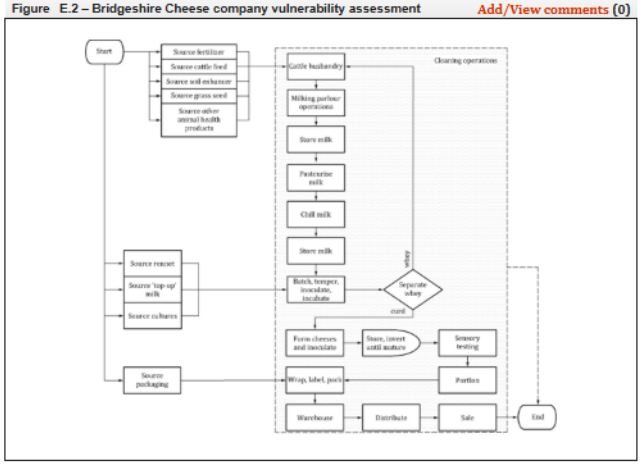


Table E.3 – Bridgeshire Cheese company threat assessment report Add/View comments (0)

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.

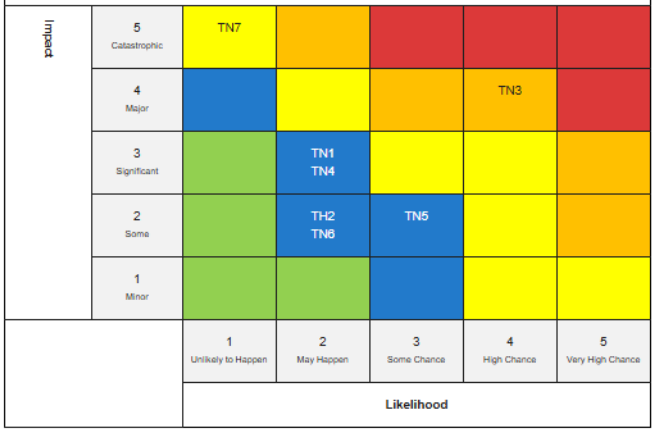
Table E.7 – F. Armer & Daughters Ltd possible sources of malicious activity Add/View comments (0)

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.