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

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

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

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

A．研究目的

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

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

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

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

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

B．研究方法

研究方法の基本的枠組み

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

1．制度および規格の企画分析

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

分析対象としたのは、次のような国内外の制度・規格である。

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

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

分析にあたっては、いくつかの観点をあらかじめ設定した。具体的には、

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

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

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

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

2．海外事例の系統的検索

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

（1）検索対象

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

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

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

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

（2）検索キーワードおよび検索式

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

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

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

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

した。具体的には、

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

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

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

（3）選定基準および除外基準

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

まず、分析対象として含める基準は以下のとおりである。

① 含める基準

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

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

一方で、以下のような事例は分析対象から除外した。

② 除外基準

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

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

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

（4）分析枠組みおよび評価項目

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

① 初期侵入経路

まず、攻撃がどのような経路から始まったのかを整理した。具体的には、

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

等の可能性を確認した。特に、本研究

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

② 権限拡大および横展開

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

③ 被害拡大要因

さらに、被害が広がった要因についても整理した。具体的には、

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

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

④ 操業停止および供給への波及

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

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

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

⑤ 政策的対応

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

ここでの整理の意味

ここで行った海外事例の整理は、単に事例を紹介することが目的ではない。

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

を目的として実施した。

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

C．研究結果

1．制度・規格分析の結果

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

（1）米国における位置づけ

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

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

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

（2）欧州連合（EU）における位置づけ

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

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

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

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

（3）制度構造の比較

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

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

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

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

表 1　食品防御とサイバーリスク管理に関する制度比較（米国・EU・日本）

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

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

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

（4）監視カメラの制度的位置づけ

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

一方で、日本では監視カメラは主に防犯設備として扱われることが多く、食品

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

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

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

(5) 制度的空白の抽出

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

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

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

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

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

D. 考察

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

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

ない。

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

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

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

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

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

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

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

考え方を次の段階へ進めるための第一歩になると考えられる。

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

2. 制度分断と責任のあいまいさ

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

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

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

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

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

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

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

3. 監視カメラ流出と供給停止リスクのつながり

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

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

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

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

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

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

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

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

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

・従業員の動き方
・出入口の施錠の様子

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

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

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

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

4. 現場で見えてきた弱点と運用の課題

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

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

また、サポートが終了した機器がその

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

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

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

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

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

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

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

5. 経済安全保障とのつながり

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

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

域社会全体に影響が及ぶ可能性がある。

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

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

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

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

E. 結論

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

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

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

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

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

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

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

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

F. 健康危機情報

なし

G. 研究発表

1. 論文発表

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

2. 学会発表

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

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

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

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

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

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

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

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

H．知的財産権の出願・登録状況

1.特許所得

　なし

2.実用新案登録

　なし

3.その他

　なし