食品防御

導入支援ハンドブック

Edition 1.0

一般財団法人　食品安全マネジメント協会

2026 年 2 月 25 日

目次

背景と目的

食品防御とは、食品製造や流通の過程において、意図的な汚染や妨害行為から食品を守る取り組みである。

近年、国内外で食品への異物混入や妨害事件が報告されており、企業規模を問わず現実的な脅威となっている。とりわけ中小企業では、人員や資源の制約から対応が遅れやすく、その結果、取引先や消費者からの信頼を失うリスクが高い。このため、食品防御は食品安全マネジメントシステムに加えて、組織全体で取り組むべき課題となっている。

本ハンドブックは、企業が食品防御を効果的に導入・維持・改善するための実践的な手引きである。中小企業が限られた資源の中でも実施できる具体策を示し、継続的な食品防御体制の確立を支援することを目的とする。

食品防御の実践は、単にリスクを減らすだけでなく、製品やブランドの信頼性を高め、取引先や消費者に「安全・安心を守る企業」として評価される基盤となる。

1.要求事項

JFS-C Version3.2 | FSM7 食品防御

要求事項

組織は、組織内または組織外の人による意図的な食品汚染のリスクに対する潜在的、及び顕在的な脅威を特定し、その脅威への対応に優先順位をつけるための評価手順を文書化し、実施し、記録しなければならない。
この評価の効果的な計画の開発および維持には、適切な知識と専門能力が活用されなければならない。
組織は、特定された食品防御の脅威の低減または排除に向けて組織が実施する対策を明記した食品防御計画を文書化し、実施、検証、維持しなければならない。また、この計画は、予め組織が定めた間隔で、または新たな脅威が確認されたときにチェックを行い、その結果、必要であれば、見直されなければならない。
組織は、食品防御の脅威が認められた箇所に対しては、アクセス管理を設けなければならない。
製品が意図的に汚染された可能性がある場合の対応手順を定め、これを実施しなければならない。

考え方、具体的事例

食品防御とは、物理的、化学的、生物的危害要因における組織内または組織外の人による意図的な食品汚染を、予防、回避、対応する手段を意味する。

食品防御の脅威評価（脅威を分析し、弱点を割り出す）では、1.の意図的な食品汚染のリスクを洗い出し、大きさを評価し、その防御策を食品防御計画として立案する。

この評価の効果的な計画の開発および維持には、上記を踏まえ、適切な知識と専門能力を活用する必要がある。

活用事例としては、官公庁のリコールサイト掲載の他社事例や社内の過去事例、専門の外部研修を受けることや、外部の食品衛生専門家の参画や助言を得るなどがある。

意図的な食品汚染は人が行う行為である以上完全な防御は困難なため、抽出した各脅威の内容と、投入できる経営資源を対比して優先順位を決定し、文書化し、実施し、記録する。

施設の脅威評価を実施する手順を文書化し、実施する。

食品防御及び施設の脅威評価の結果に基づき、意図的な食品汚染、いたずらなどを防止するための方法、責任権限、判断基準を含む食品防御計画を文書化し、実施、検証、維持する。

この食品防御の脅威評価は、予め組織が定めた間隔で、及び/または重大な変化が発生するたびにチェックを行い、その結果、必要であれば見直されるものとする。

必要に応じて、食品防御計画は修正/更新され、実施、検証、維持されねばならない。

食品防御計画は、以下のような要素を含む。

1）食品防御の責任を負う各分野からの担当者が指名されていること
2）従業員、契約者、訪問者の施設エリアへの入出を記録・管理する方針と手順があること
3）原材料、器具、容器包装資材、薬剤及び食品の保管・配送時の安全を確保する手順があること
4）敷地の物理的な安全確保（警備）がされていること
5）意図的に汚染、不良化された食品、包装、機器が発見された、または可能性がある場合にどう対応するのかの手順を定め、実施していること
6）効果的なリコールプログラムがあること（FSM22.1 参照）
7）組織が定めた食品防御計画に従って、要員に必要な教育と訓練を実施していること

食品防御の脅威が認められた箇所に対して実施するアクセス管理も、食品防御計画に含まれる。

アクセス管理には、守衛や ID カードなどによる管理、入退場者の制限や記録などの許可された従業員のみが入室できる仕組みなどがある。

参考

1）モニターカメラや施錠管理だけでなく、従業員同士のコミュニケーションは食品防御のためのけん制となる。
2）食品防御のハード対策への過度な依存は、かえって従業員と管理者との良好な関係を損ねることもある。

そのため例えば、組織は、「モニターカメラは従業員への疑いをもとに設置するのではなく、万が一、食品事故などがあった場合に、会社が従業員の行動を証明できるためのものである」と従業員に説明することもできる。

3）食品防御は施設の物理的対策だけではなく、利害関係者からの内部攻撃を想定する必要がある。短期就労者や不平、不満を持つ従事者がないことを確認することは特に有効である。
4）社会的な事例、同業他社の事例、未然防止事例、予兆などの傾向を検討する仕組みが必要となる。

食品防御の具体的事例については以下を参照されたい。1）、2）、3)は日本国内で適用する範囲

1）厚生労働省「食品防御対策ガイドライン（食品製造工場向け）」（令和元年度改訂版(案)）

2）厚生労働省「大規模イベント向け食品防御対策ガイドライン（製造工場編）」（改訂第 2 版）
～5 つの基本原則～（平成 28 年 1 月改訂版）
（基本原則 1）消費者基点の明確化
（基本原則 2）コンプライアンス意識の確立
（基本原則 3）適切な衛生管理・品質管理の基本
（基本原則 4）適切な衛生管理・品質管理のための体制整備
（基本原則 5）情報の収集・伝達・開示等の取組
3）農林水産省「食品業界の信頼性向上自主行動計画」策定の手引き
4）FDA「食品防御のための緩和戦略データベース（Food Defense Mitigation Strategies Database(FDMSD)）」
https://www.cfsanappsexternal.fda.gov/scripts/fooddefensemitigationstrategies/index.cfm

本ハンドブック中で使用する用語の説明

用語	説明
食品防御 （Food Defense）	意図的な食品汚染や妨害から守るための予防・対応 参照元：GFSI Benchmarking Requirements v2024
脅威（Threat）	意図的に食品を汚染・改ざんする可能性のある行為や状況 参照元：FDA Food Defense Training
脅威評価 （Threat Assessment）	脅威を特定・分析し、発生可能性と影響を評価して優先度を決めるプロセス 参照元：Food Defense Plan Builder (FDPB)
TACCP （Threat Assessment Critical Control Point）	意図的汚染リスクに特化した脅威評価の枠組み（狙われやすい箇所を特定し対策を設定する手法） 参照元：PAS 96:2017 – Guide to protecting and defending food and drink from deliberate attack
食品防御計画 （Food Defense Plan）	脅威評価に基づき、予防策・監視・初動手順・担当・記録等を定めた文書 参照元：Food Defense Plan Builder (FDPB)
アクセス管理 （Access Control）	重要区域への入退室を制限・記録し、不正な立ち入りや接触を防止する仕組み 参照元：21 CFR Part 121 – Mitigation Strategies to Protect Food Against Intentional Adulteration

2. 導入ステップ

食品防御の仕組みは、事業規模や製品特性に応じて様々な形で構築できる。本ハンドブックでは導入例として、食品防御の仕組みを 8 つのステップに分けて整備する方法を示す。

2.1 組織整備

2.2 現状把握

2.3 情報収集

2.4 脅威評価

2.5 計画の策定・文書化

2.6 計画の運用

2.7 レビュー

2.8 改善

2.1 組織整備

目的：指揮系統と権限を明確にし、不審な事象を現場が迷わず報告・対応できる状態をつくる。

重要な観点

実施内容	目的・ポイント
責任者の任命	食品防御責任者（例：工場長または品質保証責任者）を任命し、各部門にも担当者を置く。
役割・権限の文書化	不審者・不審物を見つけたときの判断基準、報告ルート、停止権限を文書で示す。 夜勤や休日、出張時などの不在時の代行者を明確にしておく。
周知	体制図と連絡フローを現場に掲示し、「誰に何を伝えればよいか」が一目で分かる状態にする。

解説：

- 食品防御の実効性は「責任の明確化」と「従業員の理解・協力」に左右される。
- 体制は食品安全文化を土台に置き、監視より信頼と心理的安全性を重視する。

2.2 現状把握

目的：現状の施設構造・入退管理・人員・運用ルールを食品防御の視点で棚卸しし、「狙われやすい・守りが薄い箇所」を明らかにする。

確認項目

① 責任体制：

- 責任者・代行者・体制図・判断基準は有効に機能しているか？
- 夜間、休日、出張時等の不在時の指揮も示せているか？

② 入退管理の実施：

- 高リスク区画のアクセス制御・臨時証管理・持ち込み品ルールは運用できているか？

③ 原材料・資材管理および製品データの取扱い：

原材料・資材の取扱い工程が防御的観点（意図的行為の抑止・防止・早期発見）を備えているか？
製品データや記録は改ざん防止・監査証跡を備え、異常時の原因特定に使えるか？

- 原材料：受入照合、区分保管、開封管理、返品・廃棄の明確化。
- 資材：包材・ラベルの数量・廃棄管理、旧版資材の隔離。
- 製品データ：検査値・ロット情報の信頼性、記録の改ざん防止・監査証跡の保持。

④ 物理的対策の実施：

施錠・監視機器・保存期間・巡回記録は維持されているか？

⑤ 異常対応手順の整備：

報告・隔離・証拠保全の基準が現場に浸透し、初動が滞りなくできるか？

⑥ リコール体制の整備：

意図的行為シナリオを含む体制が想定されているか？

⑦ 教育・訓練の実施：

基礎知識・実務教育・実践訓練の各層に教育計画と記録はあるか？

- 基礎教育：目的・脅威・報告の重要性についての教育
- 実務教育：自社手順・役割・報告ルート・判断手順・リコールについての教育
- 実践訓練：教育内容を確実に実行するために効果的な定着のための取り組み

確認基準：

○機能中：目的に沿って仕組みと運用が一貫して機能
△部分的：仕組みはあるが実効性が弱い／結びつきが薄い
×不十分：管理・教育・運用が不十分で機能していない

解説：

- 「既存の取組みが食品安全文化を土台に防御へ効いているか」を把握する。
- すでに取り組んでいることを基にすることで、組織の状況にあった食品防御計画を構築する。

現状把握（記入例）

No	確認項目	具体例	確認結果	備考
①	責任体制	工場長を責任者、品質保証課長を代行として明確化 体制図を掲示、通報ルートを周知済	○	年 1 回見直し済
②	入退管理の実施	加工室は ID 制御、履歴確認は月 1 回 外部業者の許可証返却に未確認事例あり	△	外部業者管理の強化要
③	原材料・資材管理および製品データの取り扱い	原材料受入照合 OK。包材旧版隔離済 製品データの修正ログ機能は未設定	△	Excel ログ機能導入検討中
④	物理的対策の実施	主要出入り口カメラ設置済、保存 30 日 倉庫扉の施錠確認が不定期	△	巡回表への記録義務化
⑤	異常対応手順の整備	不審物報告票あり 隔離実績あり 夜間担当者への教育が未実施	△	夜勤教育追加が必要
⑥	リコール体制の整備	手順書に記載あり 訓練は年 1 回、内容は衛生事故中心	△	意図的行為シナリオ追加要
⑦	教育・訓練の実施	基礎教育実施済、訓練半年 1 回 新入社員教育に食品防御項目未含	△	教材に防御要素追加予定

2.3 情報収集

目的：兆候や外部事例を継続的に取り込み、評価と対策に反映する。

収集する情報の例：

情報の種類	情報の例
組織内部の兆候	現場での異常報告 組織内外からの苦情 封印への攻撃 入退記録の不整合 監査での内外部の脅威に関する指摘 組織への匿名通報記録　等
同業・取引先の情報	異物混入事例、表示差替、改ざん　等
外部知見	公的回収情報 行政からの注意喚起情報 業界・学会・研修で議論の話題となる内容 参考先の例： 厚生労働省：公開回収事案検索 https://ifas.mhlw.go.jp/faspub/IO_S020501.do?_Action_=a_backAction 消費者庁：リコール情報サイト https://www.recall.caa.go.jp/index.php 農林水産省：自主申告情報 https://www.maff.go.jp/j/syouan/kanshitoppage.html#sochi

解説：

- 従業員の抱える不安や不満を把握する為には、労務上の確認も有益な確認となる。
- 目的は「収集」ではなく「予測と対策」。
- 公的情報と事例の定期確認だけでもリスク低減に資する。
- 収集した情報は蓄積で終えず、評価・対策へ反映する。

2.4 脅威評価

目的：現状把握と情報収集で整理した対象について、脅威を評価し、対策の優先順位を明確にする。

評価手順

① 範囲の特定

本ハンドブックでは、まず既存の HACCP の工程（受入／保管／製造／包装／出荷／情報管理等）を基礎として、脅威評価の範囲を特定する。
原材料受入から製造・包装・保管・出荷までの各工程を HACCP と同じ単位で整理し、それぞれについて「意図的な混入・妨害が起こり得るか」を確認する。

一方で、脅威は HACCP 工程の内部に限られない。網羅的な評価とするため、次のような「外部からの犯行・外部起点のリスク」も範囲に含めることが望ましい。

- 原材料・副資材・容器包装・廃棄物などの搬入・搬出業者
- 清掃・設備保守・防虫防鼠などの外部委託業者
- 共同物流拠点・外部倉庫・OEM 先など、自社外で自社製品を扱う拠点
- 来訪者・派遣社員・短期アルバイト等、恒常的従業員以外の出入り
- 研究開発・商品企画・包装設計等、レシピ・製品情報・包装仕様・表示データ等を扱う部門
- レシピ・製造条件・在庫情報・監視カメラ映像・入退室記録等、重要情報・システムへのアクセス経路
- 必要に応じて、購買・資材調達、情報システム、給水などのユーティリティー

② 評価

②-1 脅威の特定

各工程に、内部・外部から想定される意図的行為を洗い出す。

（想定される例）
受入：原料差替え
包装：薬剤の噴霧
保管：製品抜き取り
情報管理：データ改ざん

②-2 脅威の評価

洗い出した脅威を「被害の大きさ」と「攻撃実行可能性（攻撃のしやすさ）」の 2 軸を元に優先度を評価する。

※上記２軸に基づき決定した優先度により対策を検討することが推奨される。しかし、さらに詳細化するためには「気付きやすさ（検知性）」の観点が効果的である。

③　評価結果の活用

優先度「高」および「中」とされた脅威を、食品防御計画の策定で重点的に扱う。
新たな脅威や組織・設備変更が発生した際には速やかに再評価を実施する。
評価結果は記録し、次回見直し時に参照できるよう保存する。

解説：

工程を基に脅威を整理：
　HACCP の管理工程を出発点に、内部・外部脅威を区別して洗い出す。
優先度を決める：
　「被害の大きさ」を主軸に「攻撃実行可能性」で補正し、必要に応じ「気付きやすさ」を加味する。
評価の根拠を明確に：
　過去事例・他社事例・専門家意見など客観情報を用い、主観評価に偏らない。
対策立案との接続：
　評価結果は「食品防御計画」での方策設計の根拠とする。

脅威評価基準の例：

以下は、評価の際に参考となる観点の一例である。

観点	高	中	低
被害の大きさ	・健康被害が広範囲・多数に及ぶ可能性がある。 ・ブランド信頼、取引先との関係、供給継続性などに深刻で長期的な影響を与えるおそれがある。	・健康被害は限定されたロット・エリアにとどまると考えられる。 ・ブランドや経済的影響も一時的で、適切な対応により収束が見込まれる。	・健康被害は生じない、またはごく軽微である。 ・影響範囲も限定的かつ短期間で収束し、ブランド・取引関係への影響も小さい。
攻撃実行可能性	・特別な技術や設備をほとんど必要とせず、短時間・少人数（単独含む）で実行可能。 ・対象エリアへのアクセスが容易で、監視や鍵管理など既存の管理策では抑止が難しい。 ・類似の攻撃が過去にも複数報告されている。	・一定の準備・知識・設備が必要で、特定の時間帯・場所・内部協力者の存在など、条件がそろった場合に実行可能。 ・既存の管理策により一定程度の抑止が期待できる。	・高度な専門技術・特殊設備・複数人での組織的関与などが必要。 ・対象エリアへのアクセスがそもそも困難で、既存の管理策だけでも相当程度の抑止が期待できる。

			・類似の攻撃はほとんど報告がない。
気付きやすさ	・通常の検査・監視・日常業務では兆候をほとんど把握できず、発見が極めて困難。 ・発生しても、長期間見逃されるおそれがある。	・特定の検査・監視、記録確認などを実施すれば発見できる可能性はあるが、現状の運用のままでは見逃されるリスクが残る。	・既存の監視体制・点検・記録確認等により、比較的短時間で異常を検知しやすい。

優先度の決定：

	攻撃実行可能性：高	攻撃実行可能性：中	攻撃実行可能性：低
被害の大きさ：高	優先度：高	優先度：高	優先度：中
被害の大きさ：中	優先度：高	優先度：中	優先度：低
被害の大きさ：低	優先度：中	優先度：低	優先度：低

脅威評価　具体例：

工程	想定脅威（内部／外部）	被害の大きさ	攻撃実行可能性	優先度	現行対策	補足／根拠
受入	原料差替え（外部） 不正混入（内部）	高	中	高	・受入時のロット照合実施 ・立会者は 1 名のみ ・供給元変更時のリスク評価は文書化されていない	原料の供給元が増えており、外部脅威（経済的動機を伴う加害可能性）が高い 立会者 1 名では内部犯行抑止効果が弱い
保管	製品・原料の抜き取り（内部） 封印破壊（内部）	中	中	中	・冷蔵・冷凍庫は施錠管理 ・夜間巡回は不定期で記録なし ・封印の番号管理は未実施。	鍵管理は行われているが、入退室ログ・巡回記録がなく抑止力不足 封印番号管理がないため、異常の早期発見が困難
製造	意図的混入（内部）	高	低	中	・作業区域は社員のみ入室可能	加工工程は危害が最も増幅されやすい工程

	機器への異物投入（内部）				・一部ラインで監視カメラなし ・作業者の配置転換は計画的に行われていない	アクセス制限はあるが、死角が存在し、内部脅威の抑止が不十分
包装	薬剤・化学物質の噴霧（内部） 異物投入（外部侵入者）	中	中	中	・包材管理（数量・廃棄）は実施。 ・包装室の入退出管理は書面のみで記録不完全 ・来訪者は作業区域の近くまで同行する運用が不統一	包装工程は作業密度が高く、噴霧など短時間で広範囲に影響を及ぼす攻撃が可能 入退出記録不備により内部犯行・外部侵入の追跡困難
出荷	出荷品のすり替え（内部） 配送時の盗難・抜き取り（外部）	高	低	中	・出荷確認は 2 名で実施 ・出荷口は施錠されているが、監視カメラの視野に盲点あり ・配送業者への防御指導は未実施	物理的な出荷管理は最低限あるが、外部業者（第三者）への依存が高く、防御教育が不足、トラック積込み時の死角がリスク
情報管理	システムの停止・誤作動を意図的に引き起こす攻撃（内部／外部）	高	中	高	・アクセス権限設定は一部の PC のみ ・USB 使用制限が設定されていない ・改訂履歴は自由に削除可能	Excel 改訂履歴は削除可能状態
廃棄処理	廃棄品の再利用・持出（内部）	中	中	中	・廃棄リストを作成 ・廃棄立会いは日によって省略 ・廃棄倉庫の施錠が不定期	廃棄倉庫の施錠は管理不十分

評価結果のまとめ方（例）：

工程	想定脅威	被害の大きさ	攻撃実行可能性	優先度	現行対策の有無
受入	原料差替え	高	中	高	有
包装	薬剤噴霧	中	中	中	無

結果のまとめ（分析例）：

優先度「高」：受入（原料差替え）／情報管理（記録改ざん）
→「食品防御計画の策定」で最優先対策を設定
優先度「中」：保管、包装、出荷、廃棄処理
→現行対策の補強と手順整備を重点検討
優先度「低」：該当なし（ただし、再評価時に条件変化に留意）

2.5 計画の策定・文書化

目的：脅威評価の結果を踏まえ、優先度の高い項目について、具体的な管理手段と運用方法を整理する。

2.5.1 策定

優先度の高い脅威に対して、だれが・いつ・どう防ぐかを見える化する。

現行の運用を基盤に、実効性のある暫定体制を整え、将来的な拡充に備える。

食品防御計画策定内容：

① 目的・範囲

- 人為的な汚染・妨害行為による食品安全リスクを低減すること。
- 対象範囲例：原料受入～製造～包装～保管～出荷～廃棄・再流通、記録・監視システム

② 責任体制

目的：判断・報告・指揮系統を明確にし、迷わず動ける状態をつくる。
策定内容：
責任者・代行者・連絡網、判断権限を定める。
ポイント：
不在時（出張などを含む）の代行者が定まっているか。
現場が即対応できるよう周知できているか。

③ 入退管理

目的：人の出入りを制御し、不正の機会を最小化する。
策定内容：
ゾーニング、入退ルール、来訪者・外部業者の管理方法を定める。
ポイント：
高リスクエリアへのアクセス制限が明確か。
入退記録が追跡・検証に利用できる状態か。

④ 原材料・資材管理および製品データの取扱い

目的：脅威評価結果に基づき、HACCP 工程に沿った原材料・資材・製品データの防御策を策定する。
策定内容：

現行の管理手順を点検し、脅威評価で優先度の高い工程から段階的に補強・整備する。

ポイント：

既存の仕組みを活かし、現実的かつ実効性のある防御体制を整える。

※高コストな対策（例：電子記録化、監視システム強化など）は、経営判断を要する事項として「参考情報」に整理し、次回見直し時に検討とし、当該脅威に対して実行可能な方策をまず検討する

⑤ 物理的対策の整備

目的：施錠・監視・巡回などで抑止と早期発見を実現する。

策定内容：

施錠・監視・巡回の方法と責任を定める。

点検とその周期、記録とその保管ルールを定める。

ポイント：

重要区域の施錠・監視体制がリスクを低減できているか。

点検や巡回が定常業務に組み込まれているか。

⑥ 異常対応手順の整備

目的：意図的行為を含む異常事態を想定し、報告・隔離・是正を確実に実行する。

策定内容：

異常報告の判断基準と初動フローを定める。

証拠保全・通報経路の整理等のルールを明確にする。

ポイント：

異常対応時に偶発的な事故ではなく人為的な攻撃である可能性も視野に入れ事態を把握する。

「意図的な行為」に対する視点が手順に含まれているか。

現場で報告・隔離が即時に実行できる仕組みになっているか。

⑦ リコール体制の整備

目的：意図的行為を含む不具合発生時に迅速かつ的確に対応し、被害拡大を防止する。

策定内容：発動基準、初動対応、報告・連絡体制を定める。

ポイント：

意図的行為を含むシナリオが考慮されているか。

通報ルート・判断フローが担当者不在時も機能するか。

関係者全員が重要性を理解し即時行動できるか。

策定例：

項目	内容

発動基準	混入、改ざん、封印破壊、記録不整合などの報告を受けた時点で即時に出荷停止を検討する
初動対応	・ロット情報・配送履歴から対象範囲を特定し、関係部署へ共有 ・必要に応じ監視映像や封印ログを確認 ・出荷停止と同時に、該当製品の隔離と証拠の保護（サンプル・記録）を実施
報告・連絡体制	社内：工場長→品質保証→経営層への報告 社外：行政・取引先・顧客へ連絡（連絡責任者を明確化）
訓練・見直し方法	・定期的に模擬リコールを実施（「意図的混入」などのシナリオも含める） ・初動までの時間、報告内容の正確さ等を元に振り返り ・結果を次年度の教育内容や対策に反映する

⑧ 教育・訓練の整備

目的：全員が「抑止・早期発見・報告・是正」を自律的に実践できる状態を維持する。
策定内容：
基礎教育・実務教育では、教育の対象・頻度・方法を定め、役割別に段階的な教育を設計する
異常の発見・通報・初動対応・拡大防止を想定した訓練。
（例：リコール訓練、現場異常発見時の対応訓練、不審者・不審物発見時の対応訓練、情報システム障害時の初動訓練など）を計画し、訓練結果を評価・改善に反映する。

教育の枠組み（例）

種類	対象	教育の内容・目的
基礎教育	全従業員	目的・脅威・報告の重要性について
実務教育	現場担当者	自社手順・役割・報告ルート・判断手順について
	管理職・責任者	通報受理、初動判断、再発防止策の指導について
実践訓練	現場担当者	実務教育内容の訓練

ポイント：実際に発生した事故事例を紹介することで自分ごととして捉え学習意欲を高める。

参考リンク：農林水産省「食品防御・食品衛生 e ラーニング教材（奈良県立医科大学作成）」
https://hpm.naramed-u.ac.jp/e-learning/fd/index.html

⑨ 実施・検証・見直し

食品防御計画は、次のサイクルで維持する。

実施：各対策の実施者・頻度等を明確にし、日常の運用に定着させる。

検証：計画どおりに実行され、十分に機能しているかを定期的に確認する。（例：責任者の月次確認、内部監査、第二者監査など）

見直し：以下が生じた場合は評価と計画を更新する。

- 新たな脅威の発生
- 設備変更
- 組織改編
- 事故発生時など

⑩ 文書・記録の管理

食品防御計画書および関連文書の管理方針を定める。

2.5.2 文書化

目的：策定した食品防御計画を、組織全体で共有・実行・維持できる文書として整備する。

ポイント：

- 計画書には目的・範囲・責任体制・脅威評価結果・対策・見直し方法等を含める。
- 改訂時は承認・周知・教育を行い、改訂理由を残す。
- 最新版を現場で確実に確認できるよう（紙／電子）整備する。
- 購買・品質・検査・記録管理などの関連手順書と整合を取る。

解説：

- 食品防御計画の強化は、「今ある仕組みを活かし、不足部分を段階的に補う」という考え方を基本とする。
- 内部脅威の抑止には、従業員同士の信頼と、懸念をためらわずに通報できる文化が不可欠であり、訓練結果は必ず防御計画・教育計画に反映する。
- 計画は単なる文書ではなく「組織の実行計画」であり、日常業務と一体化して運用する。
- 部門ごとに「誰が・何を・どのように実施するか」を明確にし、現場で迷いが生じない構成とする。
- 定期レビュー・教育・訓練・記録を通じて、計画の実効性を継続的に確認・改善していく。

2.6 計画の運用

目的：決めた対策を現場が再現できる状態にする。

運用時の留意点：

留意点	内容
（1）責任体制	・判断・報告の流れを全員が理解している状態を維持する。 ・シフト変更や人事異動等の変更時には、体制図を更新し速やかに周知する。
（2）入退管理	・入退記録やチェックを形骸化させず、抑止力と追跡性の両面で活用する ・訪問者の種類を問わず、顧客、外部業者・派遣社員を含め、入退場管理の方策を一貫して適用する。
（3）原材料・資材管理および製品データ	・脅威評価結果に基づく方策を機能させ確実に実行する。 ・変更が発生した際には、脅威評価を再実施し、対策を更新する。
（4）物理的対策	・設備は「従業員を監視するため」ではなく「従業員を守るため」の取り組みであることを共通認識とする。 ・巡回点検では、設備が機能しているか等の状態確認に加え、従業員が「安心して働けているか」も確認する。 ・故障や経年劣化、動作不良等の不具合、セキュリティホールを見つけた際は放置せず、速やかに報告・改善につなげる。
（5）異常対応	・発見者が迷わず「報告→隔離→調査」に動けるよう、訓練と効果的な手順を維持する。 ・異常報告に対してはポジティブな声掛けを行い、報告を歓迎する。 ・初動が遅れた場合は、人ではなく仕組みを見直す。
（6）リコール体制	・リコール時は全員が事態の重要性を認識し行動する。 ・消費者の安全を最優先に速やかに方策を検討し対応する。
（7）教育・訓練	・基礎教育では食品偽装防止の目的を明確に伝え、「なぜこの取組が必要か」を共有する。 ・訓練では、想定シナリオを用い、異常時に「発見→報告→隔離」が自然に行動できる状態をつくる。 ・教育・訓練の結果は記録し、次回の内容に反映する。 ・教育内容は、新人・ベテランを問わず、教育内容が行動に定着できているかを踏まえて教育する。

解説：

- 運用段階では、「形を維持すること」ではなく「機能し続けること」を目的とする。
- 教育と訓練は、理解を深める教育と行動を定着させる訓練の両輪で実施する。
- 記録やデータは、単なる証跡ではなく抑止・発見・信頼確保の基盤として活用する。
- 運用は完璧さより継続性を重視し、日常業務に組み込むことで防御を文化として定着させる。

2.7 レビュー

目的：計画の有効性を検証し、変化に追随できる状態を保つ。

定期レビューの実施

- 内部監査や会議など、定めた間隔で浸透度・記録・有効性を確認する。
- 現場の声の聞き取りとして運用上の困りごとや改善提案を収集する。

臨時レビューの実施

- 新たな脅威や社会事例（リコール・事故・事件）発生時に速やかに見直す。

解説：

- 定期＋臨時の両面から確認することで、新しい脅威や変化に対応できる。
- 現場の声を反映することが、机上の計画を実効性のある仕組みに変える。

2.8 改善

目的：運用結果を踏まえ、改善を行う

分類	内容
是正措置	レビュー結果に基づく改善点に対して発生事象の原因を特定し、再発防止策を講じる。
予防措置	潜在要因に先回りして対策を打つ。
新しい脅威の反映	社会事例や新規リスク情報を計画に取り込む。
周知と教育	改訂内容を全員へ周知し、必要に応じて教育・訓練を再実施して定着させる。

解説：

- 改善と更新は、計画を「今の脅威に適合」させ続ける仕組みである。
- 行政・業界団体等が公表する情報や、地域の同業ネットワークからの情報を定期的に取り込み、計画の見直しに活用する。

3. 事例紹介

食品防御計画書の例

タイプ１：全国多拠点・総合食品メーカー型

- 本社による統括機能と各工場の責任者による多層的な管理体制
- 本社で定めた標準文書を基本とし、工場固有の設備・人員に応じた「拠点別付属書」を付して運用する
- 基幹システム・製造記録システム等の IT と連携した入退・記録・監査証跡の管理を行う
- 委託製造先・外部物流事業者等の外部委託先について、契約・監査により一体的に管理する
- 教育、内部監査、是正の結果をグループ内で水平展開している

タイプ２：中堅～準大手・多ブランド・グループ型

- 1 社あたり 1～数拠点の工場・センターをもつグループ会社が連なる構成
- 本社の品質・食品安全部門が共通の標準・様式・チェックリストを作成・配布し、各社・各拠点の運用状況を監査する
- 偽装・改ざんが生じやすい包材・表示・ラベル等の資材管理を重点管理項目としている
- 外部業者・派遣社員・長期常駐者など、自社と継続的に接触する外部人員の管理も統一ルールで運用する
- 「グループ標準＋チェックリスト運用」により、工場規模や人員構成の差異があっても一定の防御水準を確保する

タイプ３：地域密着・単一工場型（中小企業・専門加工業）

- 品質・製造・総務等が兼務する小規模体制
- 高価な監視設備の導入よりも、鍵管理・入退記録・包材の隔離・廃棄の立会いなど、日常業務に組み込める
- 異常の報告、製品・資材の一時隔離、証拠保全といった初動対応を迅速に行えるよう、簡潔な手順書と周知を整備
- 従業員が不利益を恐れず通報・相談できる心理的安全性を確保し、内部脅威の抑止につなげている

食品防御計画書（例）

タイプ 1：全国多拠点･総合食品メーカー型

発行日：2025 年 11 月 1 日
版：1.0
作成：食品防御責任者
承認：工場長

1.目的と適用範囲

1.1 目的

本計画は、当サイトにおける製造･物流･情報管理の各活動について、意図的な混入･妨害行為を未然に防止し、万一発生した場合の被害を最小化することを目的とする。

1.2 適用範囲

対象：

区分	内容
当サイトの HACCP で定めた工程	（原材料･資材受入／製造／包装／保管／出荷／廃棄）
対象外部拠点･業務	共同物流拠点･外部倉庫･委託製造（OEM）先･外部検査機関
対象部門･情報システム	研究開発／商品企画／包装設計など、製品設計情報･表示データ等を扱う部門及び上記に関連する情報システム

管理方法：　上記の外部拠点･業務および部門･情報システムは、本計画に基づく契約および手順により管理する。

2. 責任体制

区分	氏名	役割	主な職責
食品防御責任者（工場）	○○　○○ （品質保証部）	全体統括	脅威評価の実施、計画策定･見直し、 教育訓練の実施管理、 OEM/物流委託先の適合確認
代行者（工場）	△△　△△ （製造部）	責任者不在時の代行	緊急時の初動指揮、 報告連絡の統括、 現場隔離と証拠保全
部門責任者	各部門長	部門内運用	日常点検･異常時の報告、修正/是正処置の実施
食品防御統括（本社）	□□　□□ （品質保証本部）	監督･支援	重大事案の統括 他拠点への水平展開、 年次レビュー主宰、 IT/情報セキュリティ部門との連携

報告フロー（サイト→本社）：

現場担当者→部門責任者→食品防御責任者（サイト）→工場長→（基準該当時）食品防御統括（本社）→経営層/広報・法務

※「意図的行為の疑い」または「出荷停止を伴うケース」は本社へ即時連絡

3. 脅威評価の結果と対策（要約）

HACCP 工程に基づく脅威分析を実施し、「被害の大きさ×実行容易性」によりリスク優先度を設定した。

工程	想定脅威	評価結果（優先度）	主な対策方針
受入	原料の差替え・偽装（外部）/不正混入（内部）	高	封印・ロット番号のダブルチェック＋写真記録、受入場に立会い責任者固定、新規・休眠仕入先は本社承認（サプライヤ評価と紐付け）
保管	製品・原料の抜き取り、封印破壊（内部）	中	高リスク区画は二要素認証・入退ログ、開閉ログ記録簿、夜間巡回チェック表、映像保存 90 日（高リスク区画）、30 日（中リスク区画）
製造	意図的混入、機器への異物投入（内部）	中	カメラ死角の解消、要所への工具・器具の整頓と持出し確認方法、ライン交替時の封印確認
包装	薬剤噴霧（内部）/異物投入（外部侵入）	中	包装室への立入りを許可者に限定し、入退出を記録 開封状態の製品は作業者の視認範囲に置く ライン停止時は開封製品を被覆または一時回収
出荷	すり替え、配送時の抜き取り（内外）	中	出荷口監視範囲見直し、2 名照合・封印写真、共同物流センター輸送時の封印連番管理
情報管理	検査データ改ざん（内部）/外部データ侵入	高	入力と承認の分離、電子文書管理システム・製造記録システムの監査証跡有効化、USB 使用禁止・媒体持込申請、IT/製造設備用ネットワーク分離
廃棄処理	廃棄品の再利用・持出（内部）	中	2 名立会・撮影、廃棄リスト照合、鍵・在庫差異レビュー（月次）

※詳細な脅威リスク評価は脅威評価シートで管理

4. 実施内容（具体的対策）

項目	実施内容	担当部署	補足
①責任体制	組織図と連絡網を整備、代行者含む報告ルートを文書化	品質保証部	年 1 回見直し/拠点間相互レビュー（年 1 回）
②入退管理	ゾーニング（「低～高リスク区画）に応じた物理・手続的制御 来訪者・業者・長期常駐者は個別 ID・遵守誓約・入退記録を保存	総務部	高リスク区画は 2 要素認証、記録保管 5 年

③原材料・資材・製品・データ管理	受入・保管・廃棄・記録を点検し、意図的行為にも有効なよう手順補強 版管理は承認分離	製造部/品質保証部	将来検討：電子記録一元化（基幹システムとの連携）
④物理的防御	高リスク区域の施錠・監視・巡回を定期点検に組み込み、点検結果を月次レビュー	総務部	設備点検年 2 回／映像保存基準・中リスク区画=30 日、高リスク区画=90 日
⑤異常対応	「意図的行為を疑う」視点を明記し、報告→隔離→証拠保全→修正→是正を即時実施	各部門	手順書参照/証拠保全チェックリスト運用
⑥リコール対応	意図的行為シナリオを含む訓練を年 2 回（サイト 1 回＋グループ横断 1 回）	品質保証部	訓練記録　管理/本社広報・法務と連携
⑦教育・訓練	全従業員年 1 回基礎教育、高リスク区域関係者は年 2 回 OEM・物流センター担当者にも範囲拡張	品質保証部	研修記録管理/e ラーニング併用

5. 検証と見直し

定期レビュー：年 1 回（毎年 4 月）に責任者が主導し、有効性・運用状況・記録を確認。本社統括は全拠点の結果を取りまとめ横展開

臨時レビュー：新たな脅威・設備変更・組織改編・事故発生時に実施

6. 文書・記録の管理

- 計画書は改訂日・承認者・改訂履歴を明確化し、過去版追跡可能とする
- 電子・紙いずれでも最新版を現場で即時閲覧可能にする（電子文書管理システムで版管理・権限制御）
- 入退・封印・映像・教育・訓練・是正記録は中リスク区画：3 年、高リスク区画：5 年保管
- OEM/物流委託先との契約・手順書は本計画と紐付け、更新時は双方で改訂通知

7. 付録・参考情報

付録 1：脅威評価シート

付録 2：リコール対応手順書

付録 3：教育・訓練計画および記録

参考情報：将来導入検討項目（電子記録システム化、監視システム拡張、IT/製造設備用ネットワークセグメンテーション強化、匿名通報ホットラインの多言語化）

以上、食品防御計画書（例）：タイプ 1：全国多拠点・総合食品メーカー型

食品防御計画書（例）
タイプ 2：中堅～準大手・多ブランド・グループ型

発行日：2025 年 11 月 1 日
版：1.0
作成：食品防御責任者
承認：工場長

1. 目的と適用範囲

目的：本計画は、当工場における製造・物流・包材／表示・情報管理の各活動について、意図的な混入・妨害行為を未然に防止し、発生した場合の被害を最小化することを目的とする。

適用範囲：

当工場の HACCP で定めた工程：原料受入／製造／包装／保管／出荷

関連施設・外部拠点：資材倉庫・アウトソース倉庫・委託製造（OEM）先

対象部門・外部常駐者：包材管理・表示管理等の部門、および外部常駐者（派遣・協力会社）の作業・出入管理

対象情報システム：検査値・ロット情報・版下データ等を扱う情報システム

2. 責任体制

区分	氏名	役割	主な職責
食品防御責任者	○○　○○ （品質保証部）	全体統括	脅威評価、計画策定・見直し、 教育訓練の実施管理、 グループ基準との整合
代行者	△△　△△ （製造部）	責任者不在時の 代行	緊急時初動指揮、 報告連絡の統括
包材・表示管理責任者	□□　□□ （品質保証部）	版下・ラベル管理	版下承認、旧版隔離・廃棄、 印字パラメータ管理、 立会確認
委託先管理責任者	◎◎　◎◎ （SCM 部）	OEM/外部倉庫	契約・監査・改善フォロー、 是正・修正要求の追跡
情報セキュリティ担当	××　×× （IT）	情報防御	アクセス権限・ログ、 電子記録などの監査ログの維持

報告フロー：現場担当者→部門責任者→食品防御責任者→工場長（必要に応じて本社品質統括へ報告・連携）

3. 脅威評価の結果と対策（要約）

HACCP で定めた工程を基に「被害の大きさ×実行容易性」で優先度を設定。

工程	想定脅威	評価（優先度）	主な対策方針
受入	原料差替え・偽装（外部）/不正混入（内部）	中	受入封印・ロット照合の写真記録 新規取引時の品質保証承認、仕入先監査の強化

包装	薬剤噴霧（内部）／異物投入（外部侵入）	高	包装室への立入りを許可者に限定し、入退出を記録 開封状態の製品は作業者の視認範囲に置く ライン停止時は開封製品を被覆または一時回収
保管	製品・資材の抜き取り、封印破壊	中	施錠・開閉ログ 夜間巡回チェック表 カメラ死角の是正
製造	異物の混入、機器への投入	中	作業者配置最適化、死角カメラ追加 ライン交差制御、教育強化
出荷	すり替え、配送時盗難	中	出荷口監視の見直し、2 名照合 外部配送業者への要件明確化
情報管理	版下データ改ざん、検査値・ロット改ざん、外部侵入	高	入力と承認の分離、アクセス権限最小化 電子ログ監査証跡、有償媒体（USB 等）の使用制限
委託製造/OEM	仕様逸脱の隠匿、ラベル・資材すり替え	高	契約条項に食品防御要件を明記 抜取監査、ラベル・資材廃棄証跡の提出義務化

※詳細は威評価シート

4. 実施内容（具体的対策）

項目	実施内容	担当部署	補足
①責任体制	組織図・連絡網整備、代行者と判断基準を文書化	品質保証部	年 1 回見直し
②入退管理	ゾーニング別アクセス制御、外部常駐者・長期出入りの ID 管理	総務部	退職/契約終了時の ID 即時失効
③包材・表示・データ管理	版下承認ワークフロー標準化、旧版隔離・廃棄立会、印字設定の権限ロック・変更ログ	品質保証部／製造部／IT	将来検討：基幹システム
④物理的防御	高リスク区域の施錠・巡回・監視を定常点検へ組込み	総務部	設備点検：年 2 回
⑤異常対応	「意図的行為の可能性」を手順に明記、報告→隔離→証拠保全→調査→修正／是正	各部門	リコール対応手順書
⑥リコール対応	「表示誤り・版下改ざん」シナリオ含む模擬リコール年 1 回	品質保証部	訓練記録
⑦教育・訓練	全員年 1 回の基礎教育、包装ライン・委託先向け実践訓練	品質保証部	研修記録

5.検証と見直し

定期レビュー：年 1 回（毎年 4 月）に有効性・運用状況を確認

臨時レビュー：新脅威・設備/組織変更・事故発生時

6.文書・記録の管理

- グループ基準書を上位文書、当工場手順は付属書方式で整合管理
- 改訂日・承認者・履歴を明確化。電子/紙いずれでも最新版が現場で即時閲覧

- 版下・印字設定・廃棄記録・委託先点検記録はトレーサブルに保管（保存年限：3 年）

7.付録・参考情報

付録 1：脅威評価シート

付録 2：リコール対応手順書

付録 3：教育・訓練計画・記録

以上、食品防御計画書（例）タイプ 2：中堅～準大手・多ブランド・グループ型

食品防御計画書（例）

タイプ３：地域密着・単一工場型（中小企業・専門加工業）

発行日：2025 年 11 月 4 日
版：1.0
作成：グループ食品防御責任者（本社）
承認：品質統括役員

1. 目的と適用範囲

目的：本計画は、当工場における原料受入から製造・包装・保管・出荷・廃棄・物流および情報管理に至る一連の活動について、意図的な混入・妨害行為を未然に防止し、発生した場合の被害を最小化することを目的とする。

適用範囲：対象工程・拠点・部門

- 当工場の HACCP で定めた工程：原料受入／製造／包装／保管／出荷／廃棄
- 関連施設・外部拠点：原料・資材倉庫、製品倉庫、廃棄保管エリア、地域内協力工場、外部物流拠点など
- 対象部門・外部常駐者：包材管理・表示管理・R&D／試作などの部門、および外部常駐者（派遣・協力会社）の作業・出入管理
- 対象情報システム：基幹システム、検査値・ロット情報・出荷情報・版下データ等を扱う情報システム

2. 責任体制

区分	役職/部門	役割	主な職責
食品防御責任者（工場）	品質保証	全体統括	方針・標準策定、脅威評価の統合、教育計画、修正/是正処置の管理
代行者	製造統括	食品防御責任者　代行	緊急時の初動指揮、水平展開と進捗監督
危機対策本部	品質・製造・購買・物流・法務・広報・情報セキュリティ	危機対応	重大事案時の意思決定、行政・顧客・メディア対応、法的助言
拠点食品防御リーダー	各工場/各 DC	拠点運用	監視・点検・記録、異常通報、修正/是正処置の現場実施、教育
OEM/外部物流業者窓口	購買・物流	外部先統制	契約要件、監査・是正要求、入退/封印・ラベル統制の遵守確認

報告フロー：発見者→拠点食品防御リーダー（15 分以内）→食品防御責任者（1 時間以内）

夜間・休日は当直/緊急連絡網を用いる。

3. 脅威評価の結果と対策（要約）

HACCP 工程＋サプライチェーンまで含めて評価し、「被害の大きさ×実行容易性」で優先度を設定。

工程/領域	想定脅威	優先度	主な対策方針（抜粋）
原料受入	原料差替え（外部）、不正混入（内部）	高	封印/ロット照合の画像記録、ハイリスク原料の立会受入 仕入先承認と監査、異常時の一時隔離徹底

包材・ラベル	薬剤噴霧（内部）／異物投入（外部侵入）	中	包装室への立入りを許可者に限定し、入退出を記録 開封状態の製品は作業者の視認範囲に置く ライン停止時は開封製品を被覆または一時回収
製造	意図的混入、工程バイパス	中	監視カメラの死角解消、要所の 2 名確認 ツール持込み統制、教育で“気づき”の力を強化する
保管	製品/原料の抜取、封印破壊	中	重要倉庫の施錠・開閉ログ、巡回点検記録、 映像保存期間の延長（高リスク 90 日）
出荷/物流	すり替え、配送時抜取、外部物流業者での改ざん	中	出荷 2 名照合、封印番号連結管理 外部物流業者監査・契約要件化、温度/位置ログ活用
情報管理	記録改ざん（内部）、外部侵入	高	入力・承認の職務分離、監査証跡有効化、 USB/外部媒体制限、権限棚卸
R&D/試作	試作品の持出、表示誤用	中	試作室入退統制、試作品ラベル区別 パイロット生産への適用基準
OEM/協力工場	ラベル/配合の無断変更、封印の形骸化	中	契約で JFS-C 相当の統制を明記 定期監査/是正フォロー、封印・照合の実査

※詳細は脅威評価シート参照。

4. 実施内容（具体的対策）

項目	実施内容	担当	補足
①責任体制	本社標準＋拠点標準で運用 代行者・夜間当直まで明文化	品質	年 1 回見直し/変更時は臨時改訂
②入退管理	ゾーニング/入退記録の統一様式化 来訪・外部業者・長期常駐者も同一基準	総務/拠点	高リスク区画は入退＋映像の二重証跡
③原材料・資材・製品・データ	受入・保管・廃棄・記録の各手順を、意図的行為にも有効に補強 ハイリスク原料/包材は強化点検	製造/品質/購買	将来：主要原料のシリアル化/電子記録化
④物理的防御	施錠・監視・巡回を定常業務に内在化 映像保存は拠点リスクで 30～90 日	総務/拠点	機器は“監視”ではなく“保護”のためと周知
⑤異常対応	「報告→隔離→証拠保全→原因分析→修正/是正処置」を即時実行	各部門	意図的行為を疑う観点を手順に明記
⑥リコール対応	グループ危機対策本部主導 意図的混入シナリオの年 1 回訓練、行政/顧客連絡を標準化	品質/広報/法務	出荷停止閾値・初動手順を文書化
⑦教育・訓練	役割別層別教育（全員/現場/管理職/OEM・外部物流業者） e ラーニング＋現場訓練を組合せ	本社品質/拠点	通報ホットラインと心理的安全性の周知

拠点適用ルール（要旨）

- 本社標準に対し、設備・人員差を「拠点別別添資料」で明示（代替統制を必須記載）
- 例外はリスク評価と拠点食品防御リーダー、食品防御責任者承認を要する
- OEM/外部物流業者は契約条項（封印・入退・記録・修正/是正処置）で拘束し、監査で検証

5. 検証と見直し

定期レビュー：年 1 回（4 月）食品防御責任者主導
通報件数、修正/是正処置完了率、封印不整合件数、例外的なアクセスの有無で効果検証

内部監査：本社チームが拠点をローテーション監査（年次計画）。OEM/外部物流業者も範囲化

臨時レビュー：重大クレーム、社会事例、設備・組織変更時に即時。水平展開の期限を設定

6. 文書・記録の管理

- 文書管理システムで版管理（改訂履歴・承認・配布先を可視化）
- 現場は最新版を即時閲覧可能にする
- 基幹システムの監査証跡は改ざん防止設定を必須。紙記録は保管年限を区分明確化
- 関連手順書・点検表・教育資料の整合性を定期点検

7.付録・参考情報

付録 1：脅威評価シート

付録 2：リコール対応手順書

付録 3：教育・訓練計画/記録

付録 4：拠点別別添資料（ゾーニング図、入退ポリシー差分、映像保存期間、代替統制一覧）

参考：将来導入検討（主要工程の電子記録化、封印のシリアル化、物流トレーサビリティ強化等）

以上、食品防御計画書（例）タイプ 3：地域密着・単一工場型（中小企業・専門加工業）

食品防御事例集

Ⅰ．人的要素への防御（ヒューマンファクター管理）

- 事例① 採用時の適正確認（入口段階での防御）
- 事例② 封印教育の徹底
- 事例③ 場内巡回の実施
- 事例④ 教育が「知識共有」で終わった（悪い例）
- 事例⑤ 委託先の教育が抜け落ちた（悪い例）
- 事例⑥ 思想・信条・宗教的使命感による行動リスクへの備え

Ⅱ．物理的・設備的防御（施設・装備・運用管理）

- 事例⑦ 作業着のポケットの工夫
- 事例⑧ IC タグによる入室管理
- 事例⑨ ユニフォームの色分け
- 事例⑩ 設備の多目的活用（体温測定カメラ）
- 事例⑪ 監視カメラのデータストレージ不足（悪い例）
- 事例⑫ IC タグの点検不足（悪い例）
- 事例⑬ 搬入ゲート破損時の侵入（悪い例）

Ⅲ．情報・技術的防御（デジタル・データ管理）

- 事例⑭ 商品管理システムの再構築（ブロックチェーン）
- 事例⑮ 制度導入後の「責任の曖昧化」（悪い例）

Ⅳ．外部・サプライチェーン防御（取引・流通段階）

- 事例⑯ 入出荷先の登録制度導入
- 事例⑰ 封印管理の不徹底（悪い例）

Ⅴ．組織的・文化的防御（仕組み・標準化・理念）

- 事例⑱ 不要品箱の設置
- 事例⑲ JFS-C 関連認証の全事業所取得

Ⅰ．人的要素への防御

事例①　採用時の適正確認（入口段階での防御）

内容：採用面接の段階から、食品防御の観点を含めた人物評価を実施。

具体的には、応募者の誠実性・協調性・安全意識を確認する質問項目を設け、「信頼できる人材を採用すること自体を防御の第一歩」として位置づけた。
採用面接官向けには、“食品防御の視点を持つ面接”に関する事前研修を行い、問題行動や犯罪傾向の兆候（態度・言動・職務経歴など）を早期に見極める仕組みを導入した。

解説：食品防御の起点は「施設への侵入防止」ではなく、人の入口管理にある。

いかに堅牢な防御策を構築しても、内部に悪意を持つ人材を採用してしまえば防御は崩壊する。採用段階での安全配慮は、セキュリティ管理と同等に重要であり、「食品安全文化共有できる人を選ぶ」ことが最初の防御行動である。

ポイント：

- 採用＝防御の入口。信頼できる人を迎えることが最大のリスク低減
- 面接官への防御意識教育が重要（表面的な経歴より“行動傾向”を重視）
- 「人を見る」段階から食品防御を意識させる仕組みが有効

事例②　封印教育の徹底

内容：封印（インシュロック）の目的を理解させる教育を実施。余剰部分を切らずに残す理由（改ざん防止・証拠保全）を説明し、現場で統一的な運用を実現させた。

解説：作業方法の“手順教育”ではなく、“行動の意図理解”を促す教育が定着の鍵となる。目的を理解すれば、従業員はマニュアルよりも早く正しい判断ができる。

ポイント：

- 「なぜそうするか」を理解させる教育が本質である
- 目的理解による自律的行動が防御の強化につながる

事例③　場内巡回の実施

内容：人による定期巡回を実施し、カメラでは拾えない違和感を察知。従業員との会話を通じて防御意識を高めた。

解説：巡回は「監視」ではなく「対話」の機会として、現場に足を運ぶことで、機械には見えない雰囲気の変化を感知できる。

ポイント：

- 人の感覚は AI よりも繊細なセンサー
- 巡回の目的は「異常検知」より「現場との信頼構築」

事例④　教育が「知識共有」で終わった（悪い例）

内容：食品防御教育を座学で実施したが、受講者は自分の業務に結び付けられず、行動に変化が見られなかった。

解説：教育の目的は「知識の増加」ではなく「行動の変化」である。知識だけを伝える教育は「知っている人が多いが動けない組織」を生む。食品防御教育では、異常発見・報告・初動判断を想定した実践型訓練が不可欠である。

ポイント：

- 教育効果は「反応速度」と「再現性」で測定する
- 受講後のフォロー（訓練・ロールプレイ）で行動定着を図る
- 知識より「判断できる人」を育てるのが目的

事例⑤　委託先の教育が抜け落ちた（悪い例）

内容：物流・OEM 委託先に対する食品防御教育が実施されず、封印・搬入手順に理解の差が生じた。結果、輸送時の封緘の管理がずさんとなり、因数管理が行われず封印が効果を消失していた。

解説：食品防御は敷地内で完結しない。委託先・契約先も自社の一部として見る視点が必要である。教育を共有しなければ、サプライチェーン全体が不均一になり、弱点を突かれる。

ポイント：

- 教育範囲を工場内等に限定せず影響の及ぶ外部も考慮し拡張する
- 委託先・物流先との合同訓練が有効
- 外部連携の脆弱さは内部防御を無力化する

事例⑥　思想・信条・宗教的使命感による行動リスクへの備え

内容：組織内外の個人が、思想・信条・宗教的使命感などの内面的信念を動機として、食品への意図的な汚染・破壊・混入を行う可能性を想定。防御計画では、こうした「理念に基づく行動」を特定の宗教や思想を否定するものではなく、あくまで行動の逸脱リスクとして認識・管理することを基本方針とした。また、教育・訓練の中で、信条を尊重しながらも、「食品の安全を損なう行為はどのような動機であっても許されない」という原則を明確に伝える取り組みを行った。

解説：食品防御における脅威は、経済的・感情的・個人的な動機に限らない。社会的・思想的・宗教的な信念が「正義感」「使命感」として本人を突き動かす場合もある。このような価値観由来の行動は、事前に検知しにくいが、組織として「理念を理由にしても逸脱行動は容認しない」という姿勢を明文化することで、防御文化としての一貫性と公平性を維持できる。

ポイント：

- 防御の成熟とは、あらゆる動機を想定し、逸脱を未然に防ぐ仕組みを持つこと
- 宗教・思想を否定するのではなく、行動基準からの逸脱をリスクとして管理する
- 教育・訓練で「信条を尊重しつつも安全を優先する」姿勢を明確に示す

Ⅱ．物理的・設備的防御

事例⑦　作業着のポケットの工夫

内容：工場内への異物・不要物の持ち込み／持ち出しリスクを下げるため、作業着ポケットと携行物の運用を工程ごとに見直した。導入時には「なぜ必要か」を丁寧に説明し、協力を得た。

異物混入リスクが高い工程では、ポケットを使わない運用（ポケット封印やポケット無し作業着）とし、必要物は透明ポーチや共通備品で管理した。
PHS など連絡機器の携行が必要な工程では、ポケットを残しつつ、「入れてよい物／いけない物」をルール化し、点検を実施した。

解説：「禁止」ではなく「納得による防御」を実現した。現場の行動を制限する代わりに、代替手段を与えることで自発的な協力を促した。またポケットなどは、運用ルールが定まらない状態では、際限のない持ち込み運用がされてしまう恐れがある。持ち込み品についてのルールを定め運用することが必要となる。また、衛生的な運用と合わせて PHS などの緊急時の連絡手段は確保するなど労働安全面への配慮も十分考慮する必要がある。

ポイント：

- 防御策は「理解と納得」で定着する
- 不便を補う仕組みが協力を生む
- 「禁止」ではなく「目的共有」による動機付けが鍵となる

事例⑧　IC タグによる入室管理

内容：高リスクエリアへの入退室を IC タグで制御し、職位や業務別に権限を設定。履歴を自動記録し、異動・退職時には即時に権限変更・タグ回収を行った。

解説：IC タグは技術ではなく「運用」が要である。権限更新の遅れや回収漏れは防御の穴になる。管理責任を明確化し、更新手順を定めた点が防御の完成度を高めた。

ポイント：

- 技術導入よりも運用ルールの設計が重要
- 権限の更新・回収を即時対応できる仕組みを持つ
- 「監視」ではなく「安心の可視化」として位置づける

事例⑨　ユニフォームの色分け

内容：作業エリアごとにユニフォームを色分けし、誤入室や不審行動を一目で識別できるようにした。

解説：最も簡易な防御策が“見える化”であり効果的でもある。誰でも即時判断できる仕組みが、日常の抑止力と監視精度を高める。

ポイント：

- 「誰にでも分かる仕組み」が重要となる
- 視覚的管理は低コストで高効果

事例⑩　設備の多目的活用（体温測定カメラ）

内容：コロナ禍で導入したカメラを、体温測定と不審者対策に併用した。

解説：「新規導入ではなく再活用」という考え方は企業規模を問わず重要な考え方である。既存設備を多目的に活かすことで、無理のない防御体制を構築できる。

ポイント：

- 新設より「転用」の発想が継続を生む
- 設備に「安全を守る役割」を与えることで意識が変わる

事例⑪　監視カメラのデータストレージ不足（悪い例）

内容：抑止効果を狙って 100 台以上の監視カメラを設置したが、映像保存・点検体制が整わず、半数以上が稼働停止。導入コストのみではなく運用コストも含めて検討する必要があった。

解説：防御策が「導入すること自体」を目的化すると、運用力の限界を超えて崩壊する。食品防御におけるカメラは「威圧装置」ではなく「抑止と検証の両立ツール」である。

ポイント：

- 防御設備の本質は「設置」ではなく「運用設計」である
- カメラは“安心感を生む配置”と“確認できる体制”の両方が必要

事例⑫　IC タグの点検不足（悪い例）

内容：入退室管理用 IC タグを導入したが、点検が見落とされており、故障に気づかず、アクセス記録が欠落していた。

解説：技術的対策は導入時が「完成」ではなく「運用の始まり」である。防御の信頼性は、メンテナンスを「誰が、いつ、どう点検するか」を制度として埋め込めているかにかかる。

ポイント：

- 技術防御には「運用」を含めた計画が不可欠
- 故障発見の責任者を明確化し、監査サイクルに組み込む

事例⑬　搬入ゲート破損時の侵入（悪い例）

内容：搬入ゲートが破損し、修理までの間に外部の通行者が誤って敷地内に立ち入った。

解説：防御計画は正常稼働時だけで設計されることが多い。しかし実際に脆弱性が露呈するのは「想定外の場面」である。

ポイント：

- 食品防御計画は「例外時」に真価を問われる
- 非常時対応を定義し、平時の訓練で定着させる

Ⅲ．情報・技術的防御（デジタル・データ管理）

事例⑭　商品管理システムの再構築（ブロックチェーン）

内容：ブロックチェーンを活用して製品データの改ざん防止と高い透明性を実現させた。

解説：情報改ざんは“目に見えない内部犯行”の代表例である。デジタル技術の導入により、便利さが増すと同時にリスクも顕在化したが、「信頼できる記録の連結」という新しい防御層を構築することでリスクを低減することができた。

ポイント：

- 情報防御は食品防御の新たなテーマである
- デジタル技術は痕跡を残すこと、連結することで透明性確保の手段となる

事例⑮　制度導入後の「責任の曖昧化」（悪い例）

内容：新しい防御制度（IC タグ・封印管理など）を導入したが、管理責任者が不明確なまま運用開始。点検・報告が属人的に行われ、故障に気付かなかった。

解説：制度の寿命は“責任の明確さ”で決まる。導入時に権限や代行、点検責任を定義しなければ、制度は人の異動とともに形骸化する。制度を「誰が守るか」を決めることが、防御体制の骨格となる。

ポイント：

- 制度＝責任・権限・代行の明確化
- 管理者交代時の教育を必ず行う
- 不明瞭な責任の所在が脆弱性となる

Ⅳ．外部・サプライチェーン防御（取引・流通段階）

事例⑯　入出荷先の登録制度導入

内容：契約・監査・認証基準を明確化し、信頼できる業者のみと取引した。

解説：外部由来の脅威は“入口”で遮断するのが最も効果的。事後対応より、事前の選定ルールが最大の防御となる。

ポイント：

- サプライチェーンの入口防御が肝心
- 信頼性は契約段階で確立する

事例⑰　封印管理の不徹底（悪い例）

内容：ローリー車ドライバーが封印シールを大量に保有しており、封印の信頼性が形骸化。封印番号や発行記録の管理ルールがなく、改ざんを見抜く術がなかった。

解説：封印とは“物理的証拠”であると同時に“心理的抑止”でもある。入手や交換が容易な封印は、もはや封印ではない。防御とは「誰が管理し、誰が使い、誰が確認するか」を一貫して統制することにより成立する。

ポイント：

- 封印の価値は“希少性と管理の一貫性”にある
- サプライヤーとの協力で成り立つ食品防御対策では、相互の目的の理解が信頼性の鍵

Ⅴ．組織的・文化的防御（仕組み・標準化・理念）

事例⑱　不要品箱の設置

内容：現場に不要品箱を設け、異物や不要物を除去する習慣を形成した。

解説：整理整頓は“防御の第一歩”。異常がすぐに見つかる環境は、それ自体が防御になる。

ポイント：

- 整理＝防御。異常を見つけやすい現場は衛生管理のみではなく防御の観点でも効果的である

事例⑲　JFS-C 等第三者認証・適合証明等の全事業所取得

内容：全拠点で JFS-C 認証を取得し、仕組みと運用を標準化。

解説：第三者認証は「信頼の見える化」であり、拠点間のばらつきを抑え、組織文化を統一する効果がある。

ポイント：

- 認証は「信頼を外部が保証する」ツール
- 標準化は組織全体の防御水準を底上げする

インシデント紹介

- インシデント例① 冷凍食品農薬混入事件（2013）
- インシデント例② 国内大手飲料メーカーに対するランサムウェア攻撃（2025 年）
- インシデント例③ 大手ピザチェーンでの不適切動画（2021）
- インシデント例④ 回転寿司チェーンでの迷惑動画（2023～2025）
- インシデント例⑤ ボルト・ナット混入事件（2025）

インシデント例① 冷凍食品農薬混入事件（2013 年）

概要：群馬工場で製造された冷凍食品に農薬（マラチオン）が混入し、消費者から異臭や体調不良の苦情が相次いだ。調査の結果、工場従業員による意図的混入が判明し、刑事事件に発展した。

食品防御的な分析：

- 内部脅威の典型例：外部からの侵入ではなく、内部従業員による混入であった点が重要。従業員の不満や動機が背景にあり、物理的対策だけでは防ぎきれないことを示した
- 入退管理の限界：工場内の作業者は正規のアクセス権限を持つため、外部侵入防止だけでは不十分。内部でのモニタリングや心理的安全性を含めた防御文化が必要
- 対応面の教訓：流通済み製品の回収、行政への報告、原因究明の透明性が行われたが、消費者の信頼回復には長い時間を要した。これは、事後対応に加えて「予防的な教育・体制構築」の必要性を浮き彫りにした

学び：

- 内部犯行リスクは完全にゼロにはできない。従業員を「監視対象」ではなく「信頼できる仲間」とする文化づくりと、異常を早期に発見できる仕組みの両立が不可欠である。

インシデント例②国内大手飲料メーカーに対するランサムウェア攻撃（2025 年）

概要：2025 年、国内の大手飲料メーカーがランサムウェアによるサイバー攻撃を受け、受注・出荷などを担う基幹システムが停止した。その結果、複数工場で一時的な生産・出荷停止が発生し、新製品発売の延期や一部商品の品薄など、サプライチェーン全体に影響が及んだ。あわせて、顧客・取引先等の個人情報が外部に流出した可能性も公表され、サイバー起点でも食品・飲料の供給が止まり得ることを示した事案である。

食品防御的な分析：

「情報管理」も防御対象であることを示した事例

- 生産設備そのものではなく、受注・在庫・出荷・トレーサビリティなどを支える情報システムが暗号化・停止したことで、結果的に「安全に作った／出荷した」と言い切れない状況が生じた
- これは、防御計画の工程として「情報管理」を位置づけるべきであることを裏付ける。記録やロット情報が改ざん・消去・閲覧不能になると、トレーサビリティと製造記録の信頼性が失われるリスクが生じる

意図的・外部・非接触型の攻撃が供給を直接止め得る

- 工場に物理的に侵入しなくても、サイバー経路から“意図的に”情報システムを麻痺させることで、生産・出荷・販売を大きく止めることができてしまう
- 食品防御を「建物の中の人・モノの出入り」だけと捉えていると、この種の外部・非接触型の脅威を見落とす事となってしまう

“復旧できるか”だけでなく、“改ざんされていない証拠を残せるか”が重要

- ランサムウェア攻撃では、単にシステムを復旧できるかどうかだけでなく、「どのデータが改ざん・消去されていないと言えるか」が大きな課題となる
- 工程記録の 2 重化（オンライン＋オフライン）、バックアップの物理分離、アクセス権限の分離、監査証跡の保全などは、「事後に真正性を説明できる設計」として食品防御の一部に組み込む必要がある

基幹システムの運用ではシステムの停止状態に攻撃される。

- 基幹システムへの攻撃は、システムダウン自体が目的ではなく、システムダウンした後にセキュリティが弱体化した状態を狙い内部データの破壊、抜き取りや書き換えなど、保管しているデータに攻撃を与えることが目的の場合がある。そのため、システム自体への攻撃のみを脅威を考えるのではなく、保管しているデータに対して攻撃が及ぶことも想定し検討することが重要となる

学び：

- 出荷停止やリコール判断の根拠となるデータやシステムが攻撃されると、「守りたいのに、防御の根拠がない」という状態に陥り得る。・物理・人的な防御策だけでなく、「改ざんさせない・消させない・後から追える」情報防御を、食品防御の計画に含めることが不可欠である
- 計画書の本体に“情報防御”を位置づける必要性・サイバー攻撃は、製造・出荷・新製品発売・個人情報保護など事業全体に波及する
- 食品防御計画の中で「情報管理」を付録的に扱うのではなく、どのシステムが止まると、どの工程・判断に影響するのか、どの記録は「絶対に消せない・改ざんできない」ようにすべきかを明確にし、物理・人的対策と同じ重みで“情報防御”を位置づけることが、有効となる

インシデント例③大手ピザチェーン店舗での不適切動画投稿（2021 年）

概要：ピザチェーンの店舗で、アルバイト従業員が調理中の食材を口にするなど不衛生な行為を撮影・投稿し、企業が謝罪と再発防止策を公表した事案。店舗は特定され、SNS 上で大きく拡散した。

食品防御的な分析：

- これは「内部×非意図的（軽率・面白半分）」の典型。攻撃意思が明確でなくても、結果としては故意汚染と同じ対応（出荷・販売中止、信用回復）が必要になる
- 作業区域での私物スマホ使用や撮影行為をどこまで許容するかを、衛生ルールと一体で定めておかないと防げない
- 店舗単独ではなく本部側でのモニタリング・教育で「同じ型の不適切行為」を潰していく必要がある

学び：

- “いたずら”や“映え狙い”は、教育で具体例を示して禁止しないと伝わらない。禁止行為の明文化と、違反時の処分方針までを事前に周知しておくことが防御になる

インシデント例④　回転寿司チェーンでの迷惑動画・不適切行為拡散（2023～2025 年）

概要：2023 年に、回転寿司チェーンで来店客が他人用の湯飲みや醤油さしに口をつける、レーン上のすしに触るなどの動画を撮影し SNS に投稿した事案が相次いだ。2025 年にも同様の迷惑行為が続報として報じられ、チェーン各社が監視強化や賠償請求を表明する事態となった。

食品防御的な分析：

- 来店客による“非意図的～半ば意図的”な行為でも、企業にとっては「意図的汚染」と同じ結果を招くという典型例
- カメラを付ければ終わりではなく、「客が手を出せる動線」をそもそも減らすレイアウトや、パトロール・声かけなど運用面の抑止が必要
- SNS 拡散の速度が速く、事実確認より先にブランド毀損が起きるため、初動広報と防犯映像の保存期間設定が防御の一部になる

学び：

- 監視対象は従業員だけでなく「一時的に工場・店舗にアクセスするすべての人」が対象
- 外部からの非意図的・悪ふざけも食品防御の射程に入れるべきである

インシデント例⑤　事件紹介　食品製造工場でのボルト・ナット混入事件（長崎・2025 年）

概要：長崎県大村市の食品製造会社で、元従業員が工場内でボルトやナットなどを製品に混入させたとして警察の捜査対象となった。意図的な異物混入が疑われ、会社は回収と原因調査を進めた

食品防御的な分析：

- 工場への正規アクセス権を持っていた者が、工具・部材という“そこにあるもの”を使って攻撃しており、典型的な「内部×意図的」な攻撃である
- ロッカー・工具・交換部品など、ラインのすぐそばにある“混入に使える物”をどう管理するかが問われる
- 退職・契約終了のタイミングや人間関係のこじれがリスクを高めることを示す事案で、ヒューマンリソース部門との連携が食品防御でも必要になる

学び：

- 物理的施錠やカメラだけでは「中にいる人の手に届く異物」までは完全にコントロールできない。点検記録・ライン監視・異常申告を“止めずに回す仕組み”が重要

4. Q&A

1.基本理解

Q1.食品安全（HACCP）と食品防御（TACCP）は何が違うの？

Q2.なぜ今、日本でも食品防御が必要なの？

Q3.食品防御とは何を守る仕組みなの？

2.実践と導入

Q4.攻撃者の視点で考えるとはどういうこと？

Q5.どこまでやれば十分なの？

Q6.予算が限られている場合、どんな対策から始めればいい？

Q7.カメラは必須？いくら設置しても防御できないのでは？

Q8.取引先にカメラ位置を聞かれたらどうすればいい？

3.職場と人の理解

Q9.従業員が「監視されている」と感じてしまいそう。どう伝えれば？

Q10.従業員の不平や不満はどう把握すればいい？

Q11.労務管理や従業員の不満・不信感は食品防御とどう関わるの？

Q12.犯行を完全に防ぐことはできるの？

4.監査・評価と外部対応

Q13.監査ではどんな点を確認されるの？

Q14.外部からの犯行や兆候はどう見つける？

1. 基本理解

Q1.食品安全（HACCP）と食品防御（TACCP）は何が違うの？

A1:HACCP は偶発的・自然的な危害（例：細菌汚染、温度逸脱など）を防ぐ仕組みであり、TACCP（食品防御）は意図的・悪意的な行為（例：異物混入、破壊、内部犯行）から食品を守るための仕組みです。

項目	HACCP	TACCP
主な目的	偶発的危害の予防	意図的・悪意的危害からの防御
リスクの性質	偶発的/非意図的	意図的/悪意的
管理対象	微生物、異物、温度、工程	人、行動、心理状態、施設管理
主な活動	危害分析と管理	脅威評価、動機・手段・機会の特定
関与部門	製造・品質保証	管理職・防御チーム・経営層

Q2.なぜ今、日本でも食品防御が必要なの？

A2:かつて日本では「海外では必要だが国内では不要」という認識が一般的でした。しかし 2013 年、群馬県の冷凍食品会社で契約社員が意図的に農薬を混入させる事件が発生し、国内でも“自社内からの意図的行為”が現実化しました。この事件を契機に、日本でも食品防御は「食品安全の一部」として必要不可欠な仕組みという認識が広がりました。

Q3.食品防御とは何から何を守る仕組みなの？

A3:食品防御は、食品への意図的な攻撃から守る仕組みです。目的は、食品そのものを守るだけでなく、信頼を維持することです。防御は物理的な危害を防ぐだけでなく、リスクを最小化し、問題発生時にも企業の信頼を損なわないようにするための仕組みです。食品防御は、単なるリスク管理ではなく、組織の信頼を支えるものです。また主として「意図的な攻撃」を対象とするが、近年は“いたずら”や軽率な行為など、結果として重大な被害につながる行為も含めて検討する必要があるものも現れています。

2. 実践と導入

Q4.攻撃者の視点で考えるとはどういうこと？

A4:「もし自分が攻撃者だったら、どこを狙うか？」という視点で工程を見直すことです。もしも自分がパートタイマー、清掃担当、外部業者だったら――と想定すると、思いもよらない脆弱性が見えてきます。これは「性善説ではなく、性悪説の視点」で考える手法であり、防御計画の質を大きく高めます。

Q5.対策は、どこまでやれば十分なの？

A5:すべての脅威に対策を取る必要はありません。脅威評価で「被害の大きさ」「実行容易性」を評価し、優先度の高いものから着実に対策します。優先度の低い脅威は「把握しておく」こと自体が有効な取り組みです。

Q6.予算が限られている場合、どんな対策から始めればいい？

A6:ソフト対策（教育・意識・報告体制）から着手するのが効果的です。カメラやフェンスなどハード面に頼らずとも、チェックリスト、封印管理、入退記録、報告訓練など低コストでも実効性の高い方法があります。「できることから始める」が最も大切です。

Q7.カメラは必須？いくら設置しても防御できないのでは？

A7:カメラは“記録”のための設備であり、犯行を止める力はありません。重要なのは、抑止効果を高める運用です。たとえば「録画中」「品質保証のための監視」などの掲示を行い、従業員が安心感を持てる運用にすることで、心理的抑止と信頼の両立が可能です。

Q8.取引先にカメラ位置を聞かれたらどうすればいい？

A8:セキュリティ上、カメラの詳細な設置位置をすべて開示する必要はありません。「防犯・品質保証のために設置しており、死角が最小になるよう配置していますが、詳細なレイアウトは社内管理情報としております」と説明するのが一案です。全体像を把握する人を限定し、部署ごとに管理範囲を分けます。以下のように情報を分散管理することで、防御計画そのものを守ることができます。

- カメラの設置範囲：設備部門
- 入場証の書式・更新頻度：総務部
- 品質検査モニタリング項目：品質部門

3. 職場と人の理解

Q9.従業員が「監視されている」と感じてしまいそう。どう伝えれば？

A9:食品防御は「人を疑う」ではなく「人を守る」仕組みです。内部カメラは“監視カメラ”ではなく、“品質保証カメラ”“見守りカメラ”と呼ぶなど、言葉の工夫で理解が変わります。「防御＝安心のための仕組み」であることを丁寧に伝えましょう。

Q10.従業員の不平や不満はどう把握すればいい？

A10:不満や孤立は内部犯行の動機につながるため、心理的安全性の確保が重要です。以下のような方法が効果的です。

- 定期的な面談・声かけ
- 日常業務での観察（孤立・表情変化など）
- 匿名意見箱や通報窓口の活用
- 報告へのフィードバック（対応策の共有）

「話してよかった」と思える仕組みが、最も強い防御になります。

Q11.労務管理や従業員の不満・不信感は食品防御とどう関わるの？

A11:従業員の不満や不信感は、内部からの意図的・半ば衝動的な行為を引き起こすリスクになるため、食品防御でも考慮が必要です。そのためには、賃金・勤務シフト・評価の透明性といった労務管理を適正に行い、「不公平だ」と感じさせないことが大切です。また、異常や違和感を覚えた際に「すぐに報告できる環境」を整備することも重要です。匿名通報やホットラインの設置、上司以外にも相談できるルートの確保など、報告の心理的ハードルを下げる工夫が有効です。さらに、報告があった際には迅速に対応し、報告者にフィードバックを返すことで「報告してよかった」と感じられる信頼関係を築きます。

このような仕組みが、早期発見と未然防止の両立につながります。物理的な監視や入退室管理だけでなく、人に関する管理（心理・通報・コミュニケーション）を食品防御の一要素として位置づけます。

Q12.犯行を完全に防ぐことはできるの？

A12:完全に防ぐことは困難です。しかし、「犯行までのハードルを上げる」「早期に気づく」ことで被害を最小化することは可能です。たとえば、入退記録・封印管理・通報訓練などを組み合わせると、「やりにくい環境」「すぐ見つかる環境」をつくることができます。

4. 監査・評価と外部対応

Q13.審査ではどんな点を確認されるの？

A13:主に以下の 3 点が確認されます。

1. 脅威を適切に特定しているか
2. その対策が自社に適した方法であるか
3. 対策が実際に機能しているか

形式ではなく、実効性が評価の中心です。「自社の脅威をどう捉え、どう対策しているか」を説明できることが大切です。

Q14.外部からの犯行や兆候はどう見つける？

A:不審者や異常行動の早期発見は、日常の気づきから始まります。例として次のような兆候を共有しておくと効果的です。

- 見慣れない人物が構内を徘徊
- 工程や勤務時間を執拗に質問
- 不審な電話・メールが増える
- 不要な物品や機材の持ち込み

また、監査は、外部からの脅威や異常を発見するための有効な手段です。監査する側としては、サプライヤーや取引先の食品防御体制が適切かを確認し、リスクの早期発見に役立ちます。一方、監査される側としても、外部監査を通じて自社の防御体制の強化点や弱点を洗い出し、改善する良い機会となります。「違和感を放置しない」ことが最大の防御策です。

5. 参考情報・シナリオ・リンク集

1. コラム：

意図的と非意図的のあいだにある“いたずら”

2. 参考シナリオ・事例集

概要：工程別にみる脅威・防御ポイント・弱点

1） バルク液体・バッチ工程
2） 乾燥・粉体原料
3） 高付加価値乳製品（受入工程）
4） 製パン・惣菜など現場投入工程
5） 委託・再加工・資材管理
6） 包装・表示・最終出荷
7） 物流・倉庫・コールドチェーン
8） 小売・イベント・通販（対外公開環境）
9） 大量提供・繁忙期（学校給食等）
10） 廃棄・リワークの不正
11） 検査・データの信頼性
12） 試食コーナーへのいたずら（SNS 拡散事例）

3. シナリオ分析と評価手法、国内外ガイドライン・リンク集

- シナリオ分析（影響度・アクセス性・検知性）
- KAT（KeyActivityTypes）手法
- 脅威評価手法：CARVER＋Shock
- 農林水産省チェックリストによる脅威評価
- 奈良県立医科大学公衆衛生学講座資料　食品防御対策ガイドラインによる脅威評価
- 緩和策策定支援（FDMSD 活用）
- 一般財団法人食品安全マネジメント協会

4. 付録

食品防御計画書【テンプレート】

1. コラム：「意図的」と「非意図的」のあいだにある“いたずら”

――行為の動機ではなく、組織への影響で考える食品防御――

食品防御（Food Defense）は、かつて「日本以外の問題」と見なされてきた。日本の食品産業は衛生と品質管理を中心に発展してきたが、意図的な食品攻撃への備えは長く軽視されてきた。しかし、2013 年に国内で発生した冷凍食品への農薬混入事件がその認識を変えた。在職中の契約社員が工場内でマラチオンを混入させたこの事件は、「日本人が日本の食品を意図的に汚染した」という事実を突きつけ、食品防御が国内でも現実的な課題であることを示した。事件を契機に、防犯カメラや入退管理を導入する企業は増えたが、「本当に防げる仕組みとは何か」という問いは残った。それは設備やルールの整備だけでなく、人の行動と動機の曖昧さをどう扱うかという課題である。

■「意図的」と「非意図的」は、人の行動の中で連続している

食品攻撃を語るとき、しばしば“意図的”と“非意図的”を分けて考える。しかし実際には、この 2 つの間には広いグレーゾーンがある。“意図的”とは組織や製品を害する目的をもつ行為、“非意図的”とは無知・誤解・軽率さ、あるいは“いたずら”と呼ばれる衝動を含む行為を指す。だが、組織にとってはどちらも被害をもたらす点で同じであり、防御の対象となる。食品防御の本質は「動機の究明」ではなく、「行為が成立しない仕組み」を設計することにある。

■食品攻撃想定マップ：行為の全体像を捉える

行為者の意図と関与の位置（内部／外部）を軸に整理すると、防御の対象は次のように広がる。

攻撃の区分	意図的（明確な攻撃意思）	非意図的（無知・軽率・いたずら）
内部からの行為	・報復・不満による混入、破壊 ・データ改ざん、虚偽記録	・教育不足による誤操作、SNS 投稿・撮影などの軽率行動、“面白半分”のいたずら
外部からの行為	・侵入による直接汚染、偽装表示 ・競合・反社会勢力による意図的攻撃	・業者・訪問者のルール未理解、・注目目的の不適切投稿・拡散、・“面白半分”のいたずら

「無知」「軽率」「いたずら」等の非意図的行為も、信用喪失や回収等の被害につながるため、防御対象として想定すべきである。

■“いたずら”を軽視しないという発想の転換

近年、SNS 上での軽率な投稿や不適切動画が拡散し、一瞬で企業の信用を失う事例が相次いでいる。多くは悪意ではなく、“興味本位”や“一時の気の緩み”による行為だ。しかし、結果として企業に重大な損害を与える点で意図的被害と変わらない。したがって、“いたずら”であっても防御対象とすべきである。「悪意はないから仕方ない」とせず、「無知・油断・軽率が攻撃へ転化する構造」を理解することが重要である。

■実務的な対応の方向性

区分	目的	主な取組例
教育・訓練	「悪意がなくても重大な結果を招く」ことを理解させる	新人教育に“いたずら・誤操作”の事例を組み込み／SNS 行動指針の明示
心理的安全性	小さな異常や違和感も報告できる職場文化の醸成	食品安全文化を基盤とした相談・報告体制
ルール整備	曖昧な領域をなくす	撮影・投稿・立入・廃棄等の明文化と定期教育
監査・検証	「形だけの運用」になっていないかを点検	年次レビューで教育効果・遵守度を検証

これらの取組は、単なる行動規範の整備ではなく、「人の行動を通じて起こる攻撃を防ぐ文化の形成」を目的とするものである。

■犯人になったつもりで考えることが、最も有効な防御である

フードディフェンスの真価は、設備や書類の整備ではなく、「犯人になったつもりで考える」視点を組織内に根付かせることにある。

攻撃者の立場に立ち、「どの工程が脆弱か」「どんな行動なら成立してしまうか」を想像する。その思考実験の中で、新たな自社の盲点と弱点が明らかになる。このアプローチは、性悪説ではなく、現実的なリスクマネジメントの視座である。犯罪・いたずら・過失を分け隔てなく捉え、「どのような状況下でも成立し得るリスク」を潰していくことこそが、重要となる。

2. 参考シナリオ・事例集

食品防御と食品偽装が重なるケースについて

この章では、「ラベル差替え」「原料差替え」「再包装による再投入」など、一見すると食品偽装（Food Fraud）に分類される行為も含めて、「食品防御の観点から見た脅威・弱点・防御ポイント」として整理した。

一般に、食品防御（Food Defense）：消費者の健康被害や事業継続の停止を狙った「悪意ある意図的行為」、食品偽装（Food Fraud）：経済的利益・不正な優位性を目的とした「意図的な欺き」として区別される。実際の現場では、「経済目的の原料差替え」が結果的に食品安全性を損なう、「想定外のアレルゲンの混入の発生」といったように、両者が重なり合うケースが多く存在する。

本ハンドブックでは、こうしたケースについて、「経済的動機かどうか」に関わらず、健康被害を招き得る行為は、食品防御上も重要な脅威として扱うという考え方でシナリオを整理している。実務では「これは防御か偽装か」と無理に切り分けるのではなく、両方の観点で弱点を確認することが重要である。

概要：工程別にみる脅威・弱点・防御ポイント

1)バルク液体・バッチ工程（タンク／充填／冷却）

大量ロットに対する介入として、投入口への有害物質の混入／冷却槽内への散布／封緘の偽装や破壊が発生しうる

攻撃者が狙いたくなる弱点：

- 夜間・少人数帯の死角、合鍵・予備封印の管理甘さ
- 立会い形骸化やログの後追い不能
- 冷却槽・ヘッドスペースなどの開口部の管理漏れ

防御側ポイント：

- 封印・鍵・2 名立会いで単独裁量を排除する
- 開封・点検ログの完全性（誰が／いつ／何を）を担保する
- 包装直前ゲート（重点点検・隔離判断）の機能化

2)乾燥・粉体原料（粉・スパイス）

受入～保管区間で、袋の差替え（ロット差替え）／粉体への有害物質や異物の混入／封印番号の改ざんが発生しうる

攻撃者が狙いたくなる弱点：

- 中間業者区間の責任不明瞭
- 受入のサンプリング数の不十分さ、封印の照合省略
- 一時保管時の無監視エリア

防御側ポイント：

- 受入試験＋封印番号照合＋ロット追跡の三点セット
- 仕入先承認・監査で供給者選別の厳格化
- 異常時の即時隔離→原因トレースの定例化

※補足：袋・ロット差替えは、経済的動機が強い場合には食品偽装（Food Fraud）にも該当し得る行為である。上記では「安全性・トレーサビリティを損なう意図的介入」として食品防御上の脅威としても扱っている。

3)高付加価値・乳製品・生乳（受入管理）

受入段階で、原料の希釈や差替え／タンク表面への異物付与／生乳タンクへの注入（混入）

攻撃者が狙いたくなる弱点：

- 高価品の監視薄さ、差替え余地
- 生乳の迅速検査未実装・タンク封印の形骸化
- 受入場の混雑時の混乱

防御側ポイント：

- 職務分離（購買×受入）と定期分析の 2 層化
- 出荷直前の表面起点確認（外観・拭取り）
- 牧場/集乳タンクの封印・アクセス統制

4)製パン・惣菜など現場投入口

計量・投入時の異物混入／アレルゲン粉末の意図的持込み／投入指示の改ざん

攻撃者が狙いたくなる弱点：

- 繁忙時の確認省略
- 検出機の日常点検の抜け
- 下準備スペースの視認性不足

防御側ポイント：

- ダブルチェック（人×人／人×システム）の徹底
- アレルゲン管理と金属検出の妥当性確認
- 調理区画のアクセス統制と作業切替の整合

5)委託・再加工・資材（外部委託と資材ライフサイクル）

委託先によるレシピ外物質の混入／包材版やラベルの差替え（偽装）／非公式再加工による改変

攻撃者が狙いたくなる弱点：

- 「委託だから」の盲信、検証不足
- 記録外作業の温床となる再加工
- 包材の版管理・廃棄管理の緩み

防御側ポイント：

- 契約への食品防御要件明記と現場監査
- 非公式外注を発生させない可視化・承認制
- 包材の受入～廃棄の一体管理（旧版隔離）

6)包装・表示・最終出荷

最終工程で、最終包装への差し込み物混入／ラベルの意図的差替え／封緘の偽装・破壊

攻撃者が狙いたくなる弱点：

- ラベル差替えのダブルチェック欠落
- 最終ラインの死角と封緘管理の形式化
- 出荷直前の人手不足帯

防御側ポイント：

- 配合×ラベルの最終照合と工程ログ保存
- 入室制限＋監視配置＋封緘管理
- 最終検品立会い・シール番号照合

※補足：ラベルの意図的差替えは、内容物と表示の不一致による健康被害（アレルゲン等）および回収困難・誤回収を招く点で、食品防御上、重大な脅威となる。経済的動機のある「偽装」と重なる部分だが、ここでは「最終工程で事故・攻撃を止める」という防御機能に着目して取り上げている。

7)物流・倉庫・コールドチェーン・回収容器

輸送時の開封・注入（噴霧）／外部倉庫での箱開封や内容物の差替え／温度操作による品質劣化（意図的逸脱）

攻撃者が狙いたくなる弱点：

- 輸送区間の無監視時間帯
- 外部倉庫での封印未確認・在庫差異放置
- 回収容器の適合性判定の欠落

防御側ポイント：

- 封印番号照合＋停車/開封ログ＋位置/温度記録
- 入退室管理・監視と在庫差異の定例照合
- 回収容器の受入判定（洗浄記録照合・不適合即廃棄）

8)小売・市場・イベント・通販（対外公開環境）

対外公開環境で、陳列品の開封・差し込み／試食品の表面汚染／通販梱包への異物同梱（差替え）

攻撃者が狙いたくなる弱点：

- ピーク帯の巡回不足
- 試食・陳列の無防備な表面
- 通販梱包の責任所在不明確

防御側ポイント：

- 動線・死角設計と監視配置
- 棚封印／封緘・開封痕管理
- 異常品の即時隔離→通知→記録

9)大量提供・繁忙期（季節・学校給食）

大量提供時に、大鍋や大ロットへの混入／配膳直前の介入による汚染／表示・切替ミスによる誤配（アレルゲン混入）

攻撃者が狙いたくなる弱点：

- 人手薄・新人投入での確認省略
- 大鍋・大ロットの一括影響性
- 仮設ラインの統制不備

防御側ポイント：

- 繁忙期統制（臨時教育・手順簡素化・重点検査）
- 配膳動線の遮断と相互確認
- KPI（初動時間・回収率）で有効性検証

10)廃棄・リワークの不正（再投入）

廃棄・回収経路で、廃棄品の横流し・再包装による再投入／回収品の無断再投入／廃棄記録の改ざん

攻撃者が狙いたくなる弱点：

- 廃棄の無人時間帯
- 記録の形式化と写真等の証跡不足
- 委託先任せの丸投げ

防御側ポイント

- 廃棄立会い・記録の厳格運用
- 回収経路の遮断と再入庫の 2 重承認
- 廃棄委託先の監査

※補足：廃棄品の再投入や再包装は、原価低減などの「偽装的」な意図、有効期限切れ・品質劣化品を意図的に流通させる「危害行為」が混在しやすい領域である。ここでは、「廃棄経路を悪用した意図的な危害・サプライチェーン撹乱」の観点から食品防御の対象として整理している。

11)検査・データの信頼性

試験・検査段階で、検体のすり替え／検査結果やログの改ざん／検査報告書の偽造・差替え

攻撃者が狙いたくなる弱点：

- 受け渡し時の無署名・無封印
- データの単独権限編集
- 外部委託の監査希薄

防御側ポイント：

- 監査証跡（改版履歴・アクセス）
- 検査ラボの切替／2 重化による牽制

※補足：検査データの偽造・改ざんは、合否のすり替えによる「偽装」、異常を隠して危害の顕在化を招く「防御上の欠陥」の両方の脅威を持ち得る。

12)試食コーナーへのいたずら（SNS 拡散狙い）

商業施設の試食台で来場者がパン表面に異物様の物を塗り撮影・投稿。拡散で「異物混入」苦情が発生。健康被害なし。

狙われやすい弱点：

- 無人試食台・むき出し提供・ルール不明確

防御側ポイント：

- 蓋付き・個包装で提供、スタッフ常駐
- 「撮影可・食品接触禁止」を掲示
- 疑義発生時は即隔離・記録・SNS 対応

3. シナリオ分析と評価手法

シナリオ分析（影響度・アクセス性・検知性）

シナリオごとに「影響度」「アクセス性」「検知性」の 3 要素を 5 段階で評価し、RPN（RiskPriorityNumber）を算出する手法である。これにより、各シナリオの脅威度を把握でき、重篤なシナリオは KAT や CARVER＋Shock などの詳細評価につなげることができる。

参考：*Mitigation Strategiesto Protect Food Against Intentional Adulteration: Guidance for Industry*
https://www.fda.gov/media/113684/download

KAT（KeyActivityTypes）手法

KAT は FDA の IA（Intentional Adulteration）アプローチで用いられる予備評価手法である。製造工程全体から、「意図的汚染が発生した場合に重大な公衆衛生影響や広域被害をもたらす活動（工程）」を効率的かつ再現性をもって抽出する。抽出後は CARVER＋Shock などの詳細評価の実施、又は緩和策検討に活用し、資源配分や優先対応を決定することもできる。

参考：*Mitigation Strategiesto Protect Food Against Intentional Adulteration: Guidance for Industry*
https://www.fda.gov/media/113684/download

脅威評価手法：CARVER＋Shock

CARVER＋Shock は、工程や施設の脆弱性を多角的に評価し、脅威の優先順位付けと防御策策定を支援する手法である。

- KAT で抽出した高脅威工程等、特定の工程を対象に詳細を評価することが可能。
- 多角的な指標に基づき脆弱性を点数化し、優先度に応じた緩和策を計画的に選定・実施する。

参考：*FDACARVER+SHOCKPRIMER*
https://www.fda.gov/food/food-defense-initiatives/carver-shock-primer

農林水産省チェックリストによる脅威評価

チェックリスト評価は、組織マネジメント、人的要素（従業員・部外者）、施設管理、運営（オペレーション）に分け、大項目・中項目ごとに具体的なチェック項目を設定することで、潜在的脅威や脆弱性を明確化する手法である。

参考：食品工場における人為的な食品汚染防止に関するチェックリスト
https://www.maff.go.jp/j/syouan/seisaku/kiki/attach/pdf/index-7.pdf

食品に係る物流施設における人為的な食品汚染防止に関するチェックリスト
https://www.maff.go.jp/j/syouan/seisaku/kiki/attach/pdf/index-8.pdf

奈良県立医科大学公衆衛生学講座資料　食品防御対策ガイドラインによる脅威評価

「食品防御対策ガイドライン」に基づき、組織の状況を照合して評価する手法である。組織、従業員、部外者、施設管理、入出荷管理の各分野において、意図的汚染の脅威を低減する優先的・実施可能な対策を検討する。

参考：食品防御対策ガイドライン（食品製造工場向け）令和 5 年度版
https://hpm.naramed-u.ac.jp/pdf/fd_guideline/r5_gl_food-manufacturing.pdf

緩和策策定支援（FDMSD 活用）

FDMSD（Food Defense Mitigation Strategies Database）は、FDA 提供の食品防御緩和策データベースである。CARVER＋Shock などで特定された高脅威工程に対して、緩和策を体系的に導入できる。

- 緩和策は、物理的障壁、アクセス制御、従業員教育、手順強化などに分類される。
- 対象食品や工程、脅威の種類に応じた実施手順や留意点も示される。
- 評価例を基に、各工程への緩和策適用状況を確認・改善することで、食品防御計画の有効性を高めることが可能である。

参考：The Food Defense Mitigation Strategies Database(FDMSD)
https://www.maff.go.jp/j/syouan/seisaku/kiki/attach/pdf/index-8.pdf

付録：食品防御計画書【テンプレート】

発行日：　　年　月　日

版：

作成：　　（役職：　　）

承認：　　（役職：　　）

1.目的と適用範囲

1.1 目的

本計画は、意図的な混入・汚染・妨害行為などの「食品防御リスク」を低減し、消費者ならびに取引先の安全と信頼を確保することを目的とする。

1.2 適用範囲（記入）

- 対象工程：

  例）原料受入／製造／包装／保管／出荷／物流　など

  →（　　）

- 対象施設：

  例）工場、資材倉庫、アウトソース倉庫、共同物流拠点など

  →（　　）

- 対象とする外部先（該当する場合）

  □委託製造先（OEM）

  □外部物流業者

  □外部検査機関

  □その他：（　　）

※自社の実態に合わせて追記・削除すること。

2.責任体制

区分	氏名	部署／拠点	役割	主な職責（概要）
食品防御責任者（サイト／工場）			全体統括	・食品防御方針の策定・周知 ・脅威評価および本計画の策定・見直しの主導
代行者（サイト／工場）			責任者不在時の代行	・緊急時の初動指揮 ・報告連絡のとりまとめ

部門責任者（製造）		製造部	部門内運用	・ゾーニング・入退管理・製造ラインでの防御策の運用・点検
部門責任者（品質保証）		品質保証部	部門内運用	・検査・記録・ラベル管理等における防御策の運用・点検
部門責任者（総務／設備）		総務／設備	物理的防御	・施錠・監視カメラ・巡回点検などの運用管理
本社食品防御統括（該当する場合）		（本社品質／食品安全部等）	監督・支援	・重大事案の承認・対外対応の統括 ・拠点間の水平展開・年次レビュー主宰
OEM／外部物流管理窓口	（　　）	（購買／SCM／物流等）	外部先統制	・契約要件、監査・是正フォロー、封印・入退・記録管理の確認

報告フロー（例／自社用に修正）

発見者→部門責任者→食品防御責任者（サイト／工場）→工場長／事業所長→（必要時）本社食品防御統括→経営層／広報・法務

- 「意図的行為の疑い」または「出荷停止を伴うケース」は、本社食品防御統括へ**即時連絡**とする。

3.脅威評価の結果と対策（要約）

3.1 評価方法（記入）

- 評価対象：

  □原料受入　□製造　□包装　□保管　□出荷／物流

  □情報管理　□包材・ラベル　□廃棄処理　□OEM／外部物流　□その他（　　）

- 評価軸（例）

  -被害の大きさ：高／中／低

  -実行容易性　：高／中／低

- 優先度の決定：

  「被害の大きさ×実行容易性」により、

  □高　□中　□低　などのランクで判定する。

3.2 評価結果（記入用サマリー）

工程／領域	想定脅威	優先度（高・中・低等）	主な対策方針（概要）
（例：原料受入）	（例：原料への不正混入／差替え）		
（　　）			

（　　）			
（　　）			

※詳細な評価は別紙「脅威評価シート」で管理。

4. 実施内容（具体的対策）

4.1 管理方針一覧（記入用）

項目	実施内容	担当部署	補足
①責任体制	（例：組織図・連絡網整備、代行者と報告ルートを文書化）	（品質保証／本社品質等）	（年 1 回見直し等）
②入退管理	（例：ゾーニング別アクセス制御、入退記録の保存）	（総務／工務等）	（高リスク区画の 2 要素認証等）
③原材料・包材・製品・データ管理	（例：受入・保管・廃棄・記録手順を意図的行為も想定して補強）	（製造／品質保証／購買／IT 等）	（ハイリスク対象の強化点検等）
④物理的防御	（例：施錠・監視カメラ・巡回点検を定常業務に組込み）	（総務／設備／拠点）	（映像保存期間： 中リスク＝　日 高リスク＝　日　等）
⑤異常対応	（例：「報告→隔離→証拠保全→調査→修正／是正」を手順化）	（各部門）	（意図的行為を疑う視点の明記等）
⑥リコール対応	（例：意図的混入・表示改ざんシナリオを含む訓練を年　回）	（品質保証／広報／法務等）	（訓練記録の様式、行政・顧客連絡の標準化等）
⑦教育・訓練	（例：全員年 1 回、要注意工程担当者は年 2 回等）	（品質保証／人事等）	（研修記録、e ラーニング併用等）

※不要な行は削除し、自社に必要な項目を追加して使用。

5.検証と見直し

- 定期レビュー

  実施頻度：年　回（例：年 1 回、毎年　月）

  実施責任者：（　　）

  レビュー内容（例／必要に応じて修正）：

○　脅威評価結果と対策の妥当性
○　入退記録・封印記録・監視カメラ映像などの運用状況

- 通報件数、修正／是正処置の実施状況
- 模擬リコール・訓練の結果など

- 臨時レビュー

以下の事象発生時には、速やかに臨時レビューを行う。

- 新たな脅威・社会事例・行政指摘の発生
- 設備変更・組織改編・大規模な工程変更
- 重大クレーム・事故・異常事例の発生など

6.文書・記録の管理

- 本計画書について

□改訂日、改訂内容、改訂理由、承認者を明確に記録する

□最新版は、関係者が即時閲覧できるよう、（紙／電子）のいずれかで管理する

- 主な関係記録（例／必要に応じて追記）

□入退管理記録

□封印番号管理表・開封記録

□監視カメラ映像（保存期間：高リスク　日／中リスク　日など）

□教育・訓練記録

□異常・通報・是正処置記録

□OEM／外部物流業者の監査・是正フォロー記録

保存期間（目安）

- 中リスク　相当記録：　　年
- 高リスク　相当記録：　　年
- （自社基準に合わせて設定・明記）

7.付録・参考情報

付録１：脅威評価シート

付録２：リコール対応手順書

付録３：教育・訓練計画・記録

付録４：拠点別適用付属書（ゾーニング図、入退ポリシー差分等）

参考：将来導入検討（例：電子記録システム、封印シリアル化、物流トレーサビリティ強化等）

〒104-0042　東京都中央区銀座 8 丁目 17 番 5 号
THE HUB　銀座 OCT　605 号室
一般財団法人　食品安全マネジメント協会（JFSM）
Tel:　03-6268-9691　Email:　info@jfsm.or.jp