# Implementation Support Handbook for Food Defense, Edition 1.0

**Japan Food Safety Management Association**
**February 25, 2026**

# Table of Contents

# BACKGROUND AND PURPOSE

Food Defense refers to measures taken to protect food from intentional contamination and acts of sabotage during the food manufacturing and distribution process.
In recent years, incidents involving foreign material contamination and sabotage of food products have been reported both in Japan and overseas, making this a realistic threat regardless of company size. Small and medium-sized enterprises (SMEs), in particular, tend to face delays in responding due to limitations in personnel and resources, which increases the risk of losing the trust of business partners and consumers. For this reason, Food Defense has become an issue that should be addressed by the organization as a whole, in addition to the operation of a Food Safety Management System.
This Handbook is a practical guide to help companies effectively implement, maintain, and improve Food Defense. Its purpose is to present concrete measures that can be carried out by SMEs even under limited resources, and to support the establishment of a sustainable Food Defense system.
The practice of Food Defense not only reduces risk, but also enhances the reliability of products and brands, and serves as a foundation for being recognized by business partners and consumers as a company committed to protecting food safety and consumer confidence.

# 1. REQUIREMENTS

## JFS-C Version3.2 | FSM7 Food Defense

### Requirements

The organization shall document, implement, and record assessment procedures to identify potential and overt threats to hazards of intentional food contamination by persons within or outside the organization and prioritize response to those threats. Appropriate knowledge and expertise shall be utilized to develop and maintain an effective plan for this assessment.
The organization shall document, implement, verify and maintain a food defense plan that specifies the actions that the organization implements to mitigate or exclude the identified food defense threat.
This plan shall also be checked at intervals determined by the organization, or when a new threat is established, and reviewed, if necessary, as a result.
The organization shall also establish access controls for areas where food defense threats have been identified.
The organization shall establish and implement procedures for responding to possible intentional contamination of product.

Concepts, specific examples

1. Food defense means measures to prevent, avoid, and respond to the intentional contamination of food by persons inside or outside the organization with physical, chemical, and biological hazards.
2. In the threat assessment of food defense (analyzing threats and identifying weak points), the risks of intentional food contamination described in 1. are identified, their magnitude is evaluated, and the defensive measures are formulated as a food defense plan. In light of the above, appropriate knowledge and expertise shall be utilized to develop and maintain an effective plan for this assessment. Examples of how this can be utilized include looking at other organizations' case studies posted on government recall sites, past case studies within the organization, receiving specialized external training, and obtaining the participation and advice of external food hygiene experts. Since it is difficult to completely protect against intentional food contamination because it is a human activity, priorities are determined, documented, implemented, and recorded by contrasting the contents of each extracted threat with the management resources that can be invested.
3. Document and implement procedures for conducting threat assessments of facilities.
4. Based on the results of the food defense and facility threat assessment, document, implement, verify and maintain a food defense plan that includes methods, responsibility and authority, and decision criteria to prevent intentional food contamination, tampering, etc. This food defense threat assessment shall also be checked at intervals determined by the organization, and/or when a new threat is established, and reviewed, if necessary, as a result. The food defense plan shall be revised/updated as necessary and shall be implemented, verified, and maintained.
5. The food defense plan includes the following elements:
   1) Personnel from each discipline with food defense responsibilities have been designated

2) Have policies and procedures in place to record and control employees, contractors, and visitors entering and leaving the facility area
3) Have procedures to ensure the safety of raw materials, utensils, containers and packaging materials, drugs, and food during storage and distribution.
4) The site shall be physically secured (security)
5) Have procedures and carry out in place for dealing with discovered or suspected intentionally contaminated or deteriorated food, packaging, or equipment
6) Have an effective recall program (see FSM 22.1)
7) Provide necessary education and training to personnel in accordance with the food defense plan established by the organization

6. Access controls implemented for areas where food defense **threats** are identified are also included in the food defense plan. Access controls can include guards, ID cards, or systems that limit or record access to authorized personnel.
7. Reference
   1) In addition to monitoring cameras and lock controls, communication among employees is a deterrent to food protection.
   2) Excessive reliance on hard measures of food defense may instead damage the good relationship between employees and managers. Thus, for example, an organization could explain to employees that the monitoring cameras are not installed based on suspicion of employees, but so that the company can prove the actions of employees in the event of a food accident.
   3) Food defense is not limited to physical measures of the facility; internal attacks from interested parties must also be anticipated. Ensuring that there are no short-term workers or disgruntled or disgruntled workers is particularly useful.
   4) A mechanism for examining trends in social cases, cases of other companies in the same industry, prevention cases, and predictive signs is required.

8. For specific examples of food defense, please refer to the following. (1), (2), and (3) are applicable in Japan.)
   1) Ministry of Health, Labour and Welfare "Guidelines for Food Defense Measures (for Food Production Plants)" (Draft revised in 2019)
   2) Ministry of Health, Labour and Welfare "Guidelines for Food Protection Measures for Large-Scale Events (Manufacturing Plants)" (Revision 2)
   3) Ministry of Agriculture, Forestry and Fisheries "Voluntary Action Plan for Enhancing Confidence in the Food Industry" Guidance for Formulation

-Five Basic Principles - (Revised January 2016)
(Basic Principle 1) Clarify the consumer's point of view
(Basic Principle 2) Establish compliance awareness
(Principle 3) Basis of proper hygiene and quality control
(Basic Principle 4) Establish systems for appropriate hygiene and quality control
(Basic Principle 5) Efforts to collect, communicate, and disclose information

4) FDA "Food Defense Mitigation Strategies Database (FDMSD)".
https://www.cfsanappsexternal.fda.gov/scripts/fooddefensemitigationstrategies/index.cfm

**Explanation of Terms Used in This Handbook**

| Term | Description |
|---|---|
| Food Defense | Prevention and response measures to protect food against intentional contamination and acts of sabotage. Reference: GFSI Benchmarking Requirements v2024 |
| Threat | Any act or situation that may intentionally contaminate or tamper with food. Reference: FDA Food Defense Training |
| Threat Assessment | The process of identifying and analyzing threats, and evaluating their likelihood and impact in order to determine priorities. Reference: Food Defense Plan Builder (FDPB) |
| TACCP (Threat Assessment Critical Control Point) | A framework for threat assessment focused on intentional contamination risks (a method for identifying vulnerable points and establishing countermeasures). Reference: PAS 96:2017 – *Guide to protecting and defending food and drink from deliberate attack* |
| Food Defense Plan | A documented plan that sets out preventive measures, monitoring, initial response procedures, responsibilities, and records based on the results of the threat assessment. Reference: Food Defense Plan Builder (FDPB) |
| Access Control | A system for restricting and recording entry to and exit from critical areas in order to prevent unauthorized access or contact. Reference: 21 CFR Part 121 – *Mitigation Strategies to Protect Food Against Intentional Adulteration* |

# 2. IMPLEMENTATION STEPS

Food Defense systems can be established in various ways depending on the scale of the business and the characteristics of the products handled. This Handbook presents, as an example of implementation, a method for developing a Food Defense system through the following eight steps.

2.1 Organizational Arrangements
2.2 Understanding the Current Situation
2.3 Information Gathering
2.4 Threat Assessment
2.5 Development and Documentation of the Plan
2.6 Operation of the Plan
2.7 Review
2.8 Improvement

## 2.1 Organizational Arrangements

Purpose: To clarify the chain of command and authority, and to establish a system in which personnel at the operational level can report and respond to suspicious events without hesitation.

Key considerations

| Activity | Purpose / Key points |
|---|---|
| Appointment of responsible personnel | Appoint a Food Defense Officer (e.g. the Plant Manager or the Quality Assurance Manager) and designate responsible personnel in each department as well. |
| Documentation of roles and authority | Document the criteria for decision-making, reporting lines, and stop-work authority when suspicious persons or suspicious objects are identified. Also clearly designate alternates for periods of absence, such as night shifts, holidays, or business trips. |
| Communication | Post the organizational structure and communication flow at the operational level so that it is immediately clear who should be informed and what information should be communicated. |

Explanation:

- The effectiveness of Food Defense depends on the clarity of responsibilities and on employees' understanding and cooperation.
- The system should be built on Food Safety Culture and should place greater emphasis on trust and psychological safety than on surveillance.

## 2.2 Understanding the Current Situation

**Purpose:** To review the current facility layout, access control, personnel, and operational rules from a Food Defense perspective, and to identify areas that are particularly vulnerable to attack or insufficiently protected.

Items to be checked

① Responsibility structure:

- Are the responsible person, alternate, organizational chart, and decision-making criteria functioning effectively?
- Is the chain of command during absences, such as at night, on holidays, or during business trips, also clearly defined?

② Implementation of access control:

- Are access control for high-risk areas, temporary pass management, and rules for items brought onto the premises being properly implemented?

③ Control of raw materials and packaging materials, and handling of product data:

- Do the handling processes for raw materials and packaging materials incorporate defensive measures from the perspective of deterrence, prevention, and early detection of intentional acts?

- Are product data and records protected against tampering and equipped with audit trails so that they can be used to identify causes in the event of abnormalities?
- Raw materials: Verification at receipt, segregated storage, control after opening, and clear handling of returns and disposal
- Packaging materials: Quantity control and disposal control for packaging and labels, and segregation of obsolete materials
- Product data: Reliability of test results and lot information, prevention of record tampering, and retention of audit trails

④ Implementation of physical measures:

- Are locks, monitoring devices, retention periods, and patrol records being properly maintained?

⑤ Establishment of abnormality response procedures:

- Have the criteria for reporting, isolation, and preservation of evidence been fully embedded at the operational level so that initial response can be carried out without delay?

⑥ Establishment of a recall system:

- Does the system include scenarios involving intentional acts?

⑦ Implementation of training and exercises:

- Are training plans and records in place for each level, including basic knowledge, practical job training, and practical exercises?
- Basic training: Training on the purpose of Food Defense, threats, and the importance of reporting
- Practical job training: Training on the company's own procedures, roles, reporting lines, decision-making procedures, and recall
- Practical exercises: Activities to ensure effective retention and consistent execution of what has been taught in training

Criteria for assessment

- ○ Functioning: The system and its operation are functioning consistently in line with the intended purpose.
  △ Partial: A system exists, but its effectiveness is weak and/or the linkage is insufficient.
- × Insufficient: Control, training, and operation are inadequate, and the system is not functioning effectively.

Explanation:

- Confirm whether existing measures are effectively contributing to defense on the basis of Food Safety Culture.
- By building on measures already in place, a Food Defense Plan can be established in a way that is suited to the organization's actual circumstances.

Understanding the Current Situation (Example of Completed Form)

| No. | Item to be checked | Example | Result | Remarks |
|---|---|---|---|---|
| ① | Responsibility structure | The Plant Manager is clearly designated as the responsible person, and the Quality Assurance Section Manager as the alternate. The organizational chart is posted, and the reporting route has already been communicated. | ○ | Reviewed once a year |
| ② | Implementation of access control | The processing room is controlled by ID access, and access history is reviewed once a month. However, there have been cases in which the return of permits by external contractors was not confirmed. | △ | External contractor control needs to be strengthened |
| ③ | Control of raw materials and packaging materials, and handling of product data | Verification of raw material receipt is in place. Obsolete packaging materials are segregated. However, the function to log changes to product data has not yet been set. | △ | Introduction of an Excel log function under consideration |
| ④ | Implementation of physical measures | Cameras are installed at major entrances and exits, and recordings are retained for 30 days. However, confirmation of warehouse door locking is conducted irregularly. | △ | Recording in the patrol checklist should be made mandatory |
| ⑤ | Establishment of abnormality response procedures | A suspicious object reporting form is available, and there is a record of isolation having been carried out. However, training for night-shift personnel has not yet been conducted. | △ | Additional training for night-shift personnel is required |
| ⑥ | Establishment of a recall system | Procedures are documented. Recall exercises are conducted once a year, but the content focuses mainly on hygiene incidents. | △ | Scenarios involving intentional acts should be added |
| ⑦ | Implementation of training and exercises | Basic training has been conducted, and exercises are carried out once every six months. However, Food Defense is not yet included in new employee training. | △ | Food Defense elements are planned to be added to the training materials |

**2.3 Information Gathering**

Purpose: To continuously collect signs of concern and external case information and reflect them in the assessment and countermeasures.

Examples of information to be collected

| Type of information | Examples |
|---|---|
| Internal signs within the organization | - Reports of abnormalities at the operational level<br>- Complaints from inside and outside the organization<br>- Tampering with seals<br>- Inconsistencies in access records<br>- Audit findings related to internal and external threats<br>- Anonymous reports made to the organization |
| Information from industry peers and business partners | Cases of foreign material contamination, label substitution, tampering, etc. |
| External knowledge | Public recall information; warning notices issued by authorities; topics discussed in industry groups, academic societies, and training sessions |

Examples of reference sources

Ministry of Health, Labour and Welfare (MHLW): Search System for Public Recall Cases
https://ifas.mhlw.go.jp/faspub/IO_S020501.do?_Action_=a_backAction

Consumer Affairs Agency (CAA): Recall Information Website
https://www.recall.caa.go.jp/index.php

Ministry of Agriculture, Forestry and Fisheries (MAFF): Voluntary Reporting Information
https://www.maff.go.jp/j/syouan/kanshitoppage.html#sochi

Explanation:

- To understand the anxieties and dissatisfaction that employees may have, labor-management checks can also be a useful source of information.
- The purpose is not merely collection, but prediction and countermeasures.
- Even regular checks of public information and case examples can contribute to risk reduction.
- Information collected should not simply be accumulated; it should be reflected in the assessment and in countermeasures.

**2.4 Threat Assessment**

Purpose: To assess the threats associated with the items identified through the review of the current situation and information gathering, and to clarify the priorities for countermeasures.

Assessment procedure

① Identification of scope

In this Handbook, the scope of the threat assessment is first identified on the basis of the existing HACCP process steps (e.g. receipt / storage / production / packaging / shipment / information management).

Each step, from the receipt of raw materials through production, packaging, storage, and shipment, is organized using the same process units as HACCP, and each is reviewed to determine whether intentional contamination or sabotage could occur.

At the same time, threats are not limited to the internal HACCP process steps. In order to ensure a comprehensive assessment, it is desirable to include in scope the following external offenses and externally originating risks:

- Suppliers and carriers handling incoming and outgoing raw materials, secondary materials, packaging materials, and waste
- Outsourced service providers for cleaning, equipment maintenance, and pest control
- Shared distribution centers, external warehouses, and OEM sites that handle the company's products outside its own facilities
- Visitors, temporary agency workers, short-term part-time workers, and other persons entering the site who are not regular employees
- Departments handling recipes, product information, packaging specifications, and labeling data, such as R&D, product planning, and packaging design
- Access routes to critical information and systems, including recipes, production conditions, inventory information, surveillance camera footage, and access records
- As necessary, utilities and support functions such as procurement, purchasing of materials, information systems, and water supply

② Assessment

②-1 Identification of threats

For each process step, identify potential intentional acts that could arise from internal or external sources.

Examples:

- Receipt: substitution of raw materials
- Packaging: spraying of chemicals
- Storage: removal of products
- Information management: tampering with data

②-2 Evaluation of threats

Evaluate the priority of the identified threats using two axes: severity of impact and feasibility of attack (ease of carrying out the attack).

It is recommended that countermeasures be considered based on the priority determined using these two axes. However, for a more detailed assessment, the additional perspective of detectability (how easily the act can be noticed) can also be effective.

③ Use of assessment results

Threats assessed as High or Medium priority should be addressed as key items in the development of the Food Defense Plan.

Reassessment should be conducted promptly whenever new threats arise or when organizational or equipment changes occur.

The assessment results should be documented and retained so that they can be referred to at the next review.

Explanation:

Organize threats based on the process steps:
Use the HACCP-controlled process steps as the starting point, and identify threats separately for internal and external sources.
Determine priorities:
Use severity of impact as the primary axis, adjust by feasibility of attack, and, where appropriate, take detectability into account.
Clarify the basis for the assessment:
Use objective information such as past incidents, examples from other companies, and expert opinions so that the assessment does not rely excessively on subjective judgment.
Link to the development of countermeasures:
Use the assessment results as the basis for designing measures in the Food Defense Plan.

Example of Threat Assessment Criteria
The following is an example of the perspectives that may be used as reference in the assessment.

| Perspective | High | Medium | Low |
|---|---|---|---|
| Severity of impact | - There is a possibility that health impacts could be widespread and affect a large number of people.<br>- There may be serious and long-term effects on brand trust, relationships with business partners, and continuity of supply. | - Health impacts are expected to be limited to specific lots or areas.<br>- Impacts on the brand and finances are also temporary and are expected to be brought under control through appropriate response. | - No health impact occurs, or the impact is extremely minor.<br>- The scope of impact is limited and can be resolved in a short period, with little effect on the brand or business relationships. |
| Feasibility of attack | - Can be carried out in a short time and by a small number of people, including a single person, with little need for special skills or equipment.<br>- Access to the target area is easy, and existing controls such as surveillance and key management are insufficient to deter the act.<br>- Similar attacks have been reported multiple times in the past. | - Requires a certain level of preparation, knowledge, or equipment, and can be carried out when conditions are met, such as a particular time, place, or the presence of an insider.<br>- Existing controls can be expected to provide a certain degree of deterrence. | - Requires highly specialized skills, special equipment, or organized involvement by multiple people.<br>- Access to the target area is inherently difficult, and existing controls alone can be expected to provide a considerable degree of deterrence.<br>- Similar attacks have rarely been reported. |
| Detectability | - Signs can hardly be identified through | - Detection may be possible if specific | - Abnormalities can be detected relatively |

| | | | |
|---|---|---|---|
| | normal inspection, monitoring, or routine operations, making detection extremely difficult.<br>- Even if the act occurs, it may go unnoticed for a long period. | inspections, monitoring, or record reviews are carried out, but under the current operation there remains a risk of overlooking it. | quickly through the existing monitoring system, inspections, and record review. |

Determination of Priority

| Severity of impact | Feasibility of attack: High | Feasibility of attack: Medium | Feasibility of attack: Low |
|---|---|---|---|
| High | Priority: High | Priority: High | Priority: Medium |
| Medium | Priority: High | Priority: Medium | Priority: Low |
| Low | Priority: Medium | Priority: Low | Priority: Low |

Specific Examples of Threat Assessment

| Process Step | Potential Threat (Internal / External) | Severity of Impact | Feasibility of Attack | Priority | Existing Controls | Notes / Basis |
|---|---|---|---|---|---|---|
| Receipt | Raw material substitution (external)<br>Unauthorized contamination (internal) | High | Medium | High | - Lot verification at receipt is conducted<br>- Only one witness is assigned at receipt<br>- Risk assessment when changing suppliers is not documented | The number of suppliers of raw materials is increasing, and the possibility of external threats, including those driven by economic motives, is high.<br>Having only one witness provides limited deterrence against insider acts. |
| Storage | Removal of products or raw materials (internal)<br>Breaking of | Medium | Medium | Medium | - Refrigerated and frozen storage areas are kept locked<br>- Night patrols | Key management is in place, but the absence of |

| | | | | | | |
|---|---|---|---|---|---|---|
| | seals (internal) | | | | are irregular and not recorded<br>- Seal numbers are not controlled | access logs and patrol records reduces deterrence. Without control of seal numbers, early detection of abnormalities is difficult. |
| Production | Intentional contamination (internal)<br>Introduction of foreign materials into equipment (internal) | High | Low | Medium | - Only employees are allowed to enter the work area<br>- Some lines are not covered by surveillance cameras<br>- Reassignment of workers is not planned systematically | The production process is the step at which hazards can be amplified most significantly. Although access restrictions are in place, blind spots remain and deterrence against internal threats is insufficient. |
| Packaging | Spraying of chemicals (internal)<br>Introduction of foreign materials by an external intruder | Medium | Medium | Medium | - Packaging materials are controlled for quantity and disposal<br>- Entry and exit control for the packaging room is paper-based only and records are incomplete<br>- Rules for escorting visitors near | The packaging process has a high density of work activities, making it possible for attacks such as spraying to have a wide-ranging impact in a short time. Incomplete |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | work areas are inconsistently applied | entry and exit records make it difficult to trace insider acts or external intrusion. |
| Shipment | Substitution of shipped products (internal)<br>Theft or removal during transportation (external) | High | Low | Medium | - Shipment checks are performed by two persons<br>- The shipping area is locked, but there are blind spots in surveillance camera coverage<br>- No Food Defense guidance has been provided to transport contractors | Minimum physical shipment controls are in place, but dependence on external contractors is high, Food Defense training is insufficient, and blind spots during truck loading remain a risk. |
| Information Management | Attack intended to cause system shutdown or malfunction (internal / external) | High | Medium | High | - Access rights are set only on some PCs<br>- Restrictions on USB use are not set<br>- Revision histories can be freely deleted | Revision histories in Excel can currently be deleted. |
| Waste Handling | Reuse or removal of discarded products (internal) | Medium | Medium | Medium | - A disposal list is prepared<br>- Witnessing of disposal is omitted on some days<br>- The waste storage area is locked irregularly | Control of locking for the waste storage area is inadequate. |

Example of How to Summarize the Assessment Results

| Process Step | Potential Threat | Severity of Impact | Feasibility of Attack | Priority | Existing Controls in Place |
|---|---|---|---|---|---|
| Receipt | Raw material substitution | High | Medium | High | Yes |
| Packaging | Chemical spraying | Medium | Medium | Medium | No |

Summary of Results (Example of Analysis)

High Priority: Receipt (raw material substitution) / Information management (record tampering)
→ Set the highest-priority measures in the Food Defense Plan
Medium Priority: Storage, packaging, shipment, waste handling
→ Focus on strengthening existing controls and developing procedures
Low Priority: None applicable
→ However, pay attention to changes in conditions at the time of reassessment

## 2.5 Development and Documentation of the Plan

Purpose: Based on the results of the threat assessment, to organize specific control measures and operational methods for high-priority items.

### 2.5.1 Development

For high-priority threats, make visible who will do what, when, and how to prevent them.
Build an effective interim framework based on current operations while preparing for future expansion.

Contents to be included in the Food Defense Plan

① Purpose and Scope

- To reduce food safety risks arising from intentional contamination and acts of sabotage.
- Example of scope: receipt of raw materials → production → packaging → storage → shipment → disposal and re-distribution, records, and monitoring systems

② Responsibility Structure

Purpose: To clarify decision-making, reporting, and the chain of command so that personnel can act without hesitation.

Contents to be established:
Define responsible persons, alternates, contact networks, and decision-making authority.

Points to consider:

- Are alternates designated for periods of absence, including business trips?
- Has the structure been communicated so that the operational level can respond immediately?

③ Access Control

Purpose: To control the movement of people and minimize opportunities for misconduct.

Contents to be established:
Define zoning, entry and exit rules, and methods for managing visitors and external contractors.

Points to consider:

- Are access restrictions to high-risk areas clearly defined?
- Are entry and exit records maintained in a condition that allows traceability and verification?

④ Control of Raw Materials and Packaging Materials, and Handling of Product Data

Purpose: Based on the results of the threat assessment, to establish protective measures for raw materials, packaging materials, and product data in line with the HACCP process steps.

Contents to be established:
Review current control procedures and strengthen and improve them in stages, starting with the process steps identified as high priority in the threat assessment.

Points to consider:

- Make use of existing systems and establish a realistic and effective defense framework.
- High-cost measures, such as electronic recordkeeping and enhanced monitoring systems, should be organized as “reference information” requiring management decision, and considered at the next review. First, practical and feasible measures for the relevant threats should be examined.

⑤ Establishment of Physical Measures

Purpose: To achieve deterrence and early detection through locking, monitoring, patrols, and similar measures.

Contents to be established:
Define the methods and responsibilities for locking, monitoring, and patrols.
Define inspection methods and frequency, as well as rules for records and their retention.

Points to consider:

- Do the locking and monitoring arrangements for critical areas reduce risk effectively?
- Are inspections and patrols incorporated into routine operations?

⑥ Establishment of Abnormality Response Procedures

Purpose: To anticipate abnormal situations, including intentional acts, and ensure reliable reporting, isolation, and corrective response.

Contents to be established:
Define criteria for abnormality reporting and the initial response flow.
Clarify rules for preservation of evidence, reporting routes, and related matters.

Points to consider:

- When responding to abnormalities, is the situation assessed with the possibility of intentional attack in mind, rather than assuming it is only an accidental incident?
- Do the procedures include a perspective on intentional acts?

- Is there a system that enables immediate reporting and isolation at the operational level?

⑦ Establishment of the Recall System

Purpose: To respond rapidly and appropriately when defects occur, including those caused by intentional acts, and to prevent expansion of damage.

Contents to be established:
Define activation criteria, initial response actions, and reporting and communication arrangements.

Points to consider:

- Are scenarios involving intentional acts taken into account?
- Do the reporting routes and decision-making flow continue to function even when responsible personnel are absent?
- Do all relevant personnel understand the importance of the situation and can they act immediately?

Example of development:

| Item | Content |
|---|---|
| Activation criteria | Consider immediate shipment suspension when a report is received regarding contamination, tampering, broken seals, record inconsistencies, etc. |
| Initial response | - Identify the scope of the affected products based on lot information and distribution records, and share this with relevant departments.<br>- Review surveillance footage and seal logs as necessary.<br>- At the same time as shipment suspension, isolate the affected products and preserve evidence (samples and records). |
| Reporting and communication system | Internal: Plant Manager → Quality Assurance → Top Management<br>External: Contact authorities, business partners, and customers, with the person responsible for communication clearly identified |
| Training and review methods | - Conduct mock recalls regularly, including scenarios such as intentional contamination.<br>- Review performance based on such factors as time taken to initiate response and the accuracy of reporting.<br>- Reflect the results in the following year’s training content and countermeasures. |

⑧ Establishment of Training and Exercises

Purpose: To maintain a state in which all personnel can autonomously practice deterrence, early detection, reporting, and corrective action.

Contents to be established:
In basic training and job-specific training, define the target personnel, frequency, and methods, and design staged training according to roles.

Plan exercises assuming abnormality detection, reporting, initial response, and prevention of escalation.

Examples include recall exercises, response exercises for abnormalities detected at the operational level, response exercises for suspicious persons or suspicious objects, and initial response exercises for information system failures. Exercise results should be evaluated and reflected in improvement.

Training framework (example):

| Type | Target | Training content / Purpose |
|---|---|---|
| Basic Training | All employees | Purpose, threats, and the importance of reporting |
| Job-specific Training | Frontline personnel | Company procedures, roles, reporting routes, and decision-making procedures |
| | Managers and responsible personnel | Receipt of reports, initial decision-making, and guidance on recurrence prevention measures |
| Practical Exercises | Frontline personnel | Exercises based on the content of job-specific training |

Point: Introducing actual incident cases helps personnel view the issue as personally relevant and increases motivation to learn.

Reference link: Ministry of Agriculture, Forestry and Fisheries, “Food Defense and Food Hygiene E-learning Materials (prepared by Nara Medical University)”
https://hpm.naramed-u.ac.jp/e-learning/fd/index.html

⑨ Implementation, Verification, and Review

The Food Defense Plan should be maintained through the following cycle.

Implementation: Clearly define the persons responsible for each measure and the frequency of implementation, and embed them in routine operations.
Verification: Check regularly whether the plan is being implemented as intended and whether it is functioning effectively.
(Examples: monthly confirmation by the responsible person, internal audit, second-party audit, etc.)
Review: Update the assessment and plan when any of the following occurs:

- Emergence of new threats
- Equipment changes
- Organizational changes
- Occurrence of incidents, etc.

⑩ Control of Documents and Records

Establish a policy for the management of the Food Defense Plan and related documents.

### 2.5.2 Documentation

Purpose: To prepare the established Food Defense Plan as a document that can be shared, implemented, and maintained throughout the organization.

Points to consider:

- The plan should include the purpose, scope, responsibility structure, threat assessment results, countermeasures, and review method.
- When revisions are made, approval, communication, and training should be carried out, and the reasons for revision should be recorded.
- The latest version should be maintained in a form that can be reliably checked at the operational level, whether in paper or electronic format.
- Consistency should be ensured with related procedures such as purchasing, quality, inspection, and records management.

Explanation:

- Strengthening the Food Defense Plan should be based on the concept of making use of existing systems and supplementing deficiencies in stages.
- To deter internal threats, trust among employees and a culture in which concerns can be reported without hesitation are essential, and training results should always be reflected in the defense plan and training plan.
- The plan is not merely a document, but an organizational implementation plan, and should be operated as an integral part of daily operations.
- The structure should clearly show who is to do what and how in each department, so that no confusion arises at the operational level.
- Through regular review, training, exercises, and records, the effectiveness of the plan should be continually confirmed and improved.

### 2.6 Operation of the Plan

Purpose: To ensure that the operational level can consistently carry out the measures that have been established.

Points to note during operation

| Point | Content |
|---|---|
| (1) Responsibility structure | - Maintain a condition in which all personnel understand the flow of decision-making and reporting.<br>- When changes occur, such as shift changes or personnel transfers, update the organizational chart and communicate it promptly. |
| (2) Access control | - Entry and exit records and checks should not become a mere formality, but should be used both for deterrence and for traceability.<br>- Measures for access control should be applied consistently to all types of visitors, including customers, external contractors, and temporary agency workers. |

| | |
|---|---|
| (3) Control of raw materials and packaging materials, and product data | - Ensure that the measures based on the results of the threat assessment function effectively and are implemented reliably.<br>- When changes occur, conduct the threat assessment again and update the countermeasures. |
| (4) Physical measures | - Establish a shared understanding that facilities and equipment are not for monitoring employees, but for protecting employees.<br>- During patrol inspections, confirm not only whether facilities are functioning properly, but also whether employees are able to work with a sense of security.<br>- When defects, malfunctions, aging deterioration, or security holes are found, they should not be left unattended, but should be reported promptly and linked to improvement. |
| (5) Response to abnormalities | - Maintain training and effective procedures so that the person who discovers the abnormality can move without hesitation from “reporting → isolation → investigation.”<br>- Give positive feedback on abnormality reports and welcome reporting.<br>- If the initial response is delayed, review the system rather than blaming individuals. |
| (6) Recall system | - In the event of a recall, all personnel should recognize the seriousness of the situation and act accordingly.<br>- Consumer safety should be the highest priority, and countermeasures should be considered and implemented promptly. |
| (7) Training and exercises | - In basic training, clearly communicate the purpose of Food Defense and share why these measures are necessary.<br>- In exercises, use assumed scenarios to establish a state in which “detect → report → isolate” can be carried out naturally in abnormal situations.<br>- Record the results of training and exercises and reflect them in the next cycle.<br>- Training should take into account whether the content has been embedded in behavior, regardless of whether the target is a new or experienced employee. |

Explanation:

- At the operational stage, the Purpose is not merely to maintain the form, but to continue functioning effectively.
- Training and exercises should be implemented as two complementary components: training to deepen understanding, and exercises to embed behavior.
- Records and data should be used not merely as evidence, but as a foundation for deterrence, detection, and assurance of trust.

- In operation, continuity should be valued more than perfection; by embedding the measures in routine work, defense can become part of the culture.

## 2.7 Review

Purpose: To verify the effectiveness of the plan and maintain a state in which the organization can keep up with changes.

Regular review

- Confirm the degree of implementation, records, and effectiveness at defined intervals through internal audits, meetings, and similar activities.
- Collect operational difficulties and suggestions for improvement by listening to voices from the operational level.

Ad hoc review

- Conduct review promptly when new threats arise or when social case examples occur, such as recalls, accidents, or incidents.

Explanation:

- By confirming both through regular and ad hoc review, the organization can respond to new threats and changes.
- Reflecting voices from the operational level is what transforms a desk-based plan into an effective system.

## 2.8 Improvement

Purpose: To carry out improvements based on the results of operation.

| Classification | Content |
|---|---|
| Corrective Action | Identify the cause of the occurrence based on review results and implement measures to prevent recurrence. |
| Preventive Action | Take measures in advance against potential causes. |
| Reflection of New Threats | Incorporate social case examples and new risk information into the plan. |
| Communication and Training | Communicate revised content to all personnel and, as necessary, reimplement training and exercises so that the revisions are embedded. |

Explanation:

- Improvement and updating are the mechanisms by which the plan is kept aligned with current threats.
- Information published by authorities and industry organizations, as well as information from local industry networks, should be incorporated regularly and used in reviewing the plan.

# 3. CASE STUDIES

**Examples of Food Defense Plans**

**Type 1: Nationwide, Multi-Site, Integrated Food Manufacturer Model**

- A multilayered management structure consisting of a head office oversight function and responsible persons at each plant
- Operation based on standard documents established by the head office, supplemented by site-specific appendices reflecting the equipment and staffing conditions of each plant
- Management of access, records, and audit trails in coordination with IT systems such as core business systems and production record systems
- Integrated management of outsourced parties, such as contract manufacturers and external logistics providers, through contracts and audits
- Horizontal deployment of training, internal audit, and corrective action results across the group

**Type 2: Mid-Sized to Upper Mid-Sized, Multi-Brand, Group Company Model**

- A structure consisting of group companies, each operating one or several plants or centers
- The head office quality and food safety function prepares and distributes common standards, formats, and checklists, and audits the operational status of each company and site
- Management of packaging materials, labeling, and labels—items that are particularly vulnerable to fraud and tampering—is treated as a key control area
- External personnel who have ongoing contact with the company, such as contractors, temporary agency workers, and long-term on-site personnel, are also managed under common rules
- A consistent level of defense is maintained through a combination of group standards and checklist-based operation, even where plant size and staffing structures differ

**Type 3: Community-Based, Single-Plant Model (SMEs / Specialized Processors)**

- A small-scale structure in which quality, production, general affairs, and other functions are handled concurrently
- Rather than introducing expensive surveillance equipment, the focus is on measures that can be incorporated into daily operations, such as key control, entry and exit records, segregation of packaging materials, and witnessing of disposal
- Simple procedures and communication are established so that initial response actions—such as reporting abnormalities, temporary isolation of products and materials, and preservation of evidence—can be carried out promptly
- Psychological safety is ensured so that employees can report and seek advice without fear of disadvantage, thereby contributing to the deterrence of internal threats

**Food Defense Plan (Example)**
**Type 1: Nationwide, Multi-Site, Integrated Food Manufacturer Model**
Issue Date: November 1, 2025
Version: 1.0
Prepared by: Food Defense Officer
Approved by: Plant Manager

## 1. Purpose and Scope

### 1.1 Purpose

The purpose of this Plan is to prevent intentional contamination and acts of sabotage in activities related to manufacturing, logistics, and information management at this site, and to minimize damage should such an event occur.

### 1.2 Scope

Scope of application:

| Category | Description |
|---|---|
| HACCP process steps established for this site | Receipt of raw materials and packaging materials / Production / Packaging / Storage / Shipment / Disposal |
| External sites and operations covered | Shared logistics centers / External warehouses / Contract manufacturers (OEM) / External testing laboratories |
| Departments and information systems covered | Departments handling product design information and labeling data, such as R&D, product planning, and packaging design, and the related information systems |

Control method:
The above external sites and operations, as well as the above departments and information systems, shall be controlled through contracts and procedures based on this Plan.

## 2. Responsibility Structure

| Category | Name | Role | Main responsibilities |
|---|---|---|---|
| Food Defense Officer (Plant) | ○○ ○○ (Quality Assurance Department) | Overall control | Conduct threat assessment; develop and review the Plan; manage training and exercises; confirm conformity of OEMs and outsourced logistics providers |
| Alternate (Plant) | △△ △△ (Production Department) | Acts in the absence of the responsible person | Direct initial response in emergencies; oversee reporting and communication; ensure on-site isolation and preservation of evidence |
| Department Manager | Each department head | Operation within the department | Conduct routine checks; report abnormalities; implement correction and corrective action |
| Corporate Food Defense Lead (Head Office) | □□ □□ (Corporate Quality Assurance Division) | Oversight and support | Oversee major incidents; horizontally deploy lessons learned to other sites; chair the annual review; coordinate with IT and information security functions |

Reporting flow (site → head office):
Frontline personnel → Department Manager → Food Defense Officer (site) → Plant Manager → (when escalation criteria are met) Corporate Food Defense Lead (head office) → Senior Management / Corporate Communications and Legal
Note: Cases involving a suspected intentional act or shipment suspension shall be reported to head office immediately.

**3. Summary of Threat Assessment Results and Countermeasure Policies**
Threat analysis was conducted based on the HACCP process steps, and risk priorities were established using severity of impact × ease of execution.

| Process Step | Potential Threat | Assessment Result (Priority) | Main countermeasure policy |
|---|---|---|---|
| Receipt | Raw material substitution or fraud (external) / Unauthorized contamination (internal) | High | Double-check seals and lot numbers plus photographic records; assign a fixed receiving witness; require head office approval for new and dormant suppliers (linked to supplier evaluation) |
| Storage | Removal of products or raw materials; breaking of seals (internal) | Medium | Two-factor authentication and access logs for high-risk areas; door opening/closing logbook; night patrol checklist; video retention for 90 days (high-risk areas) and 30 days (medium-risk areas) |
| Production | Intentional contamination; introduction of foreign materials into equipment (internal) | Medium | Eliminate camera blind spots; establish methods for orderly control of tools and utensils at critical points and for checking removal; confirm seals at line changeover |
| Packaging | Spraying of chemicals (internal) / Introduction of foreign materials by external intrusion | Medium | Restrict access to the packaging room to authorized persons and record entry/exit; keep opened products within the operator's line of sight; cover or temporarily remove opened products when the line is stopped |
| Shipment | Product substitution; theft or removal during transport (internal/external) | Medium | Review surveillance coverage at the shipping area; two-person verification and seal photographs; control sequential seal numbers during transport through shared logistics centers |
| Information Management | Tampering with test data (internal) / External intrusion into data | High | Separate data entry and approval; enable audit trails in the electronic document management system and manufacturing record system; prohibit USB use and require approval |

| | | | |
|---|---|---|---|
| | | | for bringing in storage media; separate IT and manufacturing equipment networks |
| Waste Handling | Reuse or removal of discarded products (internal) | Medium | Two-person witnessing and photography; verification against the disposal list; monthly review of key control and inventory discrepancies |

Note: Detailed threat risk evaluations shall be managed using the Threat Assessment Sheet.

**4. Implementation Measures (Specific Controls)**

| Item | Implementation measure | Responsible department | Supplementary notes |
|---|---|---|---|
| ① Responsibility structure | Prepare the organizational chart and contact network, and document the reporting route including alternates | Quality Assurance Department | Reviewed once a year / mutual inter-site review once a year |
| ② Access control | Apply physical and procedural controls according to zoning (“low- to high-risk areas”); assign individual IDs, obtain compliance declarations, and retain entry/exit records for visitors, contractors, and long-term on-site personnel | General Affairs Department | Two-factor authentication for high-risk areas; records retained for 5 years |
| ③ Control of raw materials, packaging materials, products, and data | Review receipt, storage, disposal, and records, and strengthen procedures so they are also effective against intentional acts; separate approval for version control | Production Department / Quality Assurance Department | For future consideration: integrated electronic records linked to the core business system |
| ④ Physical protection | Incorporate locking, monitoring, and patrols for high-risk areas into regular inspections, and review inspection results monthly | General Affairs Department | Equipment inspection twice a year / video retention standard: 30 days for medium-risk areas, 90 days for high-risk areas |
| ⑤ Response to abnormalities | Clearly state the perspective of “suspecting intentional acts,” and immediately implement reporting → isolation → preservation of evidence → correction → corrective action | All departments | Refer to procedure manual / operate evidence preservation checklist |
| ⑥ Recall response | Conduct exercises including scenarios involving intentional acts twice a year (once at site level and once group-wide) | Quality Assurance Department | Training records managed / coordinated with head office corporate |

| | | | |
|---|---|---|---|
| | | | communications and legal |
| ⑦ Training and exercises | Provide basic training to all employees once a year; personnel related to high-risk areas receive training twice a year; extend the scope to include OEM and logistics center personnel | Quality Assurance Department | Training records managed / e-learning used in combination |

**5. Verification and Review**

Regular review:

Once a year (every April), the responsible person shall lead a review of effectiveness, operational status, and records. The Corporate Food Defense Lead at head office shall consolidate the results from all sites and horizontally deploy key findings.

Ad hoc review:

Conducted when new threats arise, or when there are equipment changes, organizational changes, or incidents.

**6. Document and Record Control**

- The Plan shall clearly indicate the revision date, approver, and revision history, and past versions shall be traceable.
- The latest version shall be immediately accessible at the operational level in either electronic or paper form (with version control and access control in the electronic document management system).
- Records relating to access control, seals, video, training, exercises, and corrective action shall be retained for 3 years for medium-risk areas and 5 years for high-risk areas.
- Contracts and procedures with OEMs and outsourced logistics providers shall be linked to this Plan, and both parties shall be notified when revisions are made.

**7. Appendices and Reference Information**

Appendix 1: Threat Assessment Sheet

Appendix 2: Recall Response Procedure

Appendix 3: Training and Exercise Plan and Records

Reference information: Items for possible future introduction

(integration of electronic record systems, expansion of surveillance systems, strengthening of network segmentation between IT and manufacturing equipment, multilingualization of the anonymous reporting hotline)

End of Example Food Defense Plan: Type 1 – Nationwide, Multi-Site, Integrated Food Manufacturer Model

**Food Defense Plan (Example)**
**Type 2: Mid-Sized to Upper Mid-Sized, Multi-Brand, Group Company Model**
Issue Date: November 1, 2025
Version: 1.0
Prepared by: Food Defense Officer
Approved by: Plant Manager

**1. Purpose and Scope**
Purpose:
The purpose of this Plan is to prevent intentional contamination and acts of sabotage in activities related to manufacturing, logistics, packaging materials/labeling, and information management at this plant, and to minimize damage should such an event occur.
Scope:

- HACCP process steps established for this plant:
  Receipt of raw materials / Production / Packaging / Storage / Shipment
- Related facilities and external sites:
  Packaging material warehouse / Outsourced warehouse / Contract manufacturers (OEM)
- Covered departments and external resident personnel:
  Departments responsible for packaging material control and labeling control, and the work activities and access control of external resident personnel such as temporary agency workers and contractor personnel
- Covered information systems:
  Information systems handling test results, lot information, artwork data, and related information

**2. Responsibility Structure**

| Category | Name | Role | Main responsibilities |
|---|---|---|---|
| Food Defense Officer | ○○ ○○ (Quality Assurance Department) | Overall control | Threat assessment, development and review of the Plan, management of training and exercises, alignment with group standards |
| Alternate | △△ △△ (Production Department) | Acts in the absence of the responsible person | Direct initial emergency response, oversee reporting and communication |
| Packaging Material and Labeling Control Manager | □□ □□ (Quality Assurance Department) | Artwork and label control | Artwork approval, segregation and disposal of obsolete versions, management of printing parameters, witness verification |
| Outsourced Partner Management Manager | ◎◎ ◎◎ (SCM Department) | OEM / external warehouses | Contracts, audits, follow-up of improvements, tracking of correction and corrective action requests |
| Information Security Representative | ×× ×× (IT) | Information protection | Access rights and logs, maintenance of audit logs for |

| | | | |
|---|---|---|---|
| | | | electronic records and related systems |

Reporting flow:
Frontline personnel → Department Manager → Food Defense Officer → Plant Manager
(reporting to and coordination with the Head Office Quality Lead as necessary)

**3. Summary of Threat Assessment Results and Countermeasure Policies**
Priorities were established based on severity of impact × ease of execution, using the HACCP-defined process steps as the basis.

| Process Step | Potential Threat | Assessment (Priority) | Main countermeasure policy |
|---|---|---|---|
| Receipt | Raw material substitution or fraud (external) / Unauthorized contamination (internal) | Medium | Photographic records of receiving seals and lot verification; Quality Assurance approval for new suppliers; strengthened supplier audits |
| Packaging | Spraying of chemicals (internal) / Introduction of foreign materials through external intrusion | High | Restrict access to the packaging room to authorized personnel and record entry and exit; keep opened products within the operator's line of sight; cover or temporarily remove opened products when the line is stopped |
| Storage | Removal of products or materials; breaking of seals | Medium | Locking and door opening/closing logs; night patrol checklist; correction of camera blind spots |
| Production | Contamination with foreign materials; introduction into equipment | Medium | Optimization of operator placement, installation of additional cameras for blind spots, line cross-over control, strengthened training |
| Shipment | Product substitution; theft during transportation | Medium | Review of shipping area surveillance, two-person verification, clarification of requirements for external transport providers |
| Information Management | Tampering with artwork data, test results, or lot data; external intrusion | High | Separation of data entry and approval, minimization of access rights, audit trails for electronic logs, restrictions on the use of removable media (e.g. USB devices) |
| Contract Manufacturing / OEM | Concealment of specification deviations; substitution of labels or packaging materials | High | Explicit Food Defense requirements in contract clauses; spot audits; mandatory submission of evidence for disposal of labels and packaging materials |

Note: Details are managed in the Threat Assessment Sheet.

**4. Implementation Measures (Specific Controls)**

| Item | Implementation measure | Responsible department | Supplementary notes |
|---|---|---|---|
| ① Responsibility structure | Prepare the organizational chart and contact network, and document alternates and decision-making criteria | Quality Assurance Department | Reviewed once a year |
| ② Access control | Access control by zoning level; ID management for external resident personnel and persons with long-term access | General Affairs Department | Immediate deactivation of IDs upon resignation or contract termination |
| ③ Control of packaging materials, labeling, and data | Standardize the artwork approval workflow; witness segregation and disposal of obsolete versions; authority lock and change logs for printing settings | Quality Assurance Department / Production Department / IT | For future consideration: integration with the core business system |
| ④ Physical protection | Incorporate locking, patrols, and surveillance for high-risk areas into routine inspections | General Affairs Department | Equipment inspection: twice a year |
| ⑤ Response to abnormalities | Clearly state the possibility of intentional acts in procedures, and implement reporting → isolation → preservation of evidence → investigation → correction / corrective action | All departments | Refer to recall response procedure |
| ⑥ Recall response | Conduct one mock recall per year, including scenarios involving labeling errors or tampering with artwork data | Quality Assurance Department | Training records maintained |
| ⑦ Training and exercises | Basic training for all personnel once a year; practical exercises for packaging line personnel and outsourced partners | Quality Assurance Department | Training records maintained |

**5. Verification and Review**

Regular review:
Once a year (every April), confirm effectiveness and operational status.
Ad hoc review:
Conducted when new threats arise, or when there are equipment changes, organizational changes, or incidents.

**6. Document and Record Control**

- The Group Standard shall be the higher-level document, and procedures at this plant shall be managed in alignment with it using an appendix structure.

- The revision date, approver, and revision history shall be clearly identified. The latest version shall be immediately accessible at the operational level in either electronic or paper form.
- Artwork data, printing settings, disposal records, and outsourced partner inspection records shall be retained in a traceable manner.
  Retention period: 3 years

**7. Appendices and Reference Information**

Appendix 1: Threat Assessment Sheet
Appendix 2: Recall Response Procedure
Appendix 3: Training and Exercise Plan and Records

End of Example Food Defense Plan: Type 2 – Mid-Sized to Upper Mid-Sized, Multi-Brand, Group Company Model

**Food Defense Plan (Example)**
**Type 3: Community-Based, Single-Plant Model (SMEs / Specialized Processors)**
Issue Date: November 4, 2025
Version: 1.0
Prepared by: Group Food Defense Officer (Head Office)
Approved by: Executive Officer in Charge of Quality

**1. Purpose and Scope**
**Purpose:**
The purpose of this Plan is to prevent intentional contamination and acts of sabotage throughout the series of activities at this plant, from receipt of raw materials through production, packaging, storage, shipment, disposal, logistics, and information management, and to minimize damage should such an event occur.
Scope: Covered process steps, sites, and functions

- HACCP process steps established for this plant: Receipt of raw materials / Production / Packaging / Storage / Shipment / Disposal
- Related facilities and external sites: Raw material and packaging material warehouses, finished product warehouses, waste storage areas, local partner plants, external logistics sites, etc.
- Covered departments and external resident personnel: Departments such as packaging material control, labeling control, and R&D / trial production, and the work activities and access control of external resident personnel (temporary agency workers and contractor personnel)
- Covered information systems: Core business systems and information systems handling test results, lot information, shipment information, artwork data, etc.

**2. Responsibility Structure**

| Category | Position / Department | Role | Main responsibilities |
|---|---|---|---|
| Food Defense Officer (Plant) | Quality Assurance | Overall control | Establish policies and standards, consolidate threat assessments, develop training plans, and manage correction / corrective action |
| Alternate | Head of Production | Deputy for the Food Defense Officer | Direct initial emergency response, horizontally deploy actions, and supervise progress |
| Crisis Management Task Force | Quality / Production / Purchasing / Logistics / Legal / Corporate Communications / Information Security | Crisis response | Decision-making in major incidents, response to authorities, customers, and media, and legal advice |
| Site Food Defense Leader | Each plant / each distribution center | Site operation | Monitoring, inspection, and recordkeeping; abnormality reporting; on-site implementation of correction / corrective action; and training |

| | | | |
|---|---|---|---|
| OEM / External Logistics Provider Liaison | Purchasing / Logistics | Control of external parties | Contract requirements, audits and corrective action requests, and confirmation of compliance with access control, seal control, and label control |

Reporting flow:
Person who identifies the issue → Site Food Defense Leader (within 15 minutes) → Food Defense Officer (within 1 hour)
During night shifts or holidays, the duty officer / emergency contact network shall be used.

**3. Summary of Threat Assessment Results and Countermeasure Policies**
Assessment was conducted covering the HACCP process steps as well as the supply chain, and priorities were established based on severity of impact × ease of execution.

| Process / Area | Potential Threat | Priority | Main countermeasure policy (excerpt) |
|---|---|---|---|
| Receipt of raw materials | Raw material substitution (external), unauthorized contamination (internal) | High | Image records of seal and lot verification, witnessed receipt for high-risk raw materials, supplier approval and audits, thorough temporary isolation when abnormalities occur |
| Packaging materials and labels | Spraying of chemicals (internal) / introduction of foreign materials by external intrusion | Medium | Restrict access to the packaging room to authorized personnel and record entry/exit; keep opened products within the operator's line of sight; cover or temporarily remove opened products when the line is stopped |
| Production | Intentional contamination, process bypass | Medium | Eliminate blind spots in surveillance cameras, two-person verification at critical points, control of tools brought into the area, and strengthen employees' ability to notice abnormalities through training |
| Storage | Removal of products / raw materials, breaking of seals | Medium | Locking and access logs for critical warehouses, patrol inspection records, extended video retention periods (90 days for high-risk areas) |
| Shipment / Logistics | Substitution, removal during transportation, tampering by external logistics providers | Medium | Two-person shipment verification, linked control of seal numbers, audits of external logistics providers and inclusion of requirements in contracts, use of temperature / location logs |
| Information Management | Record tampering (internal), external intrusion | High | Segregation of duties for data entry and approval, activation of audit trails, restriction of USB / external media, review of access rights |
| R&D / Trial Production | Removal of trial products, misuse of labeling | Medium | Entry/exit control for trial rooms, distinction of labels for trial products, application criteria for pilot production |

| | | | |
|---|---|---|---|
| OEM / Partner Plants | Unauthorized changes to labels / formulations, ineffective use of seals | Medium | Contracts specifying controls equivalent to JFS-C, regular audits and follow-up of corrective action, on-site verification of seals and reconciliation checks |

Note: Refer to the Threat Assessment Sheet for details.

**4. Implementation Measures (Specific Controls)**

| Item | Implementation measure | Responsible party | Supplementary notes |
|---|---|---|---|
| ① Responsibility structure | Operate based on head office standards plus site standards; clearly document alternates and night-duty arrangements | Quality | Reviewed once a year / temporary revision when changes occur |
| ② Access control | Standardize zoning and access record formats; apply the same standards to visitors, external contractors, and long-term resident personnel | General Affairs / Site | For high-risk areas, maintain dual evidence through access records plus video |
| ③ Control of raw materials, packaging materials, products, and data | Reinforce procedures for receipt, storage, disposal, and records so that they are also effective against intentional acts; strengthen checks for high-risk raw materials / packaging materials | Production / Quality / Purchasing | Future consideration: serialization of major raw materials / electronic records |
| ④ Physical protection | Incorporate locking, monitoring, and patrols into routine operations; apply video retention periods of 30 to 90 days according to site risk | General Affairs / Site | Communicate that equipment is for “protection,” not for “surveillance” of employees |
| ⑤ Response to abnormalities | Immediately implement “reporting → isolation → preservation of evidence → cause analysis → correction / corrective action” | All departments | Procedures shall explicitly include the perspective of suspecting intentional acts |
| ⑥ Recall response | Led by the Group Crisis Management Task Force; conduct annual exercises based on intentional contamination scenarios; standardize communication with authorities and customers | Quality / Corporate Communications / Legal | Shipment stop thresholds and initial response procedures shall be documented |
| ⑦ Training and exercises | Provide role-based training by level (all personnel / frontline personnel / managers / OEMs and external logistics | Head Office Quality / Site | Communicate the reporting hotline and psychological safety |

| | | | |
|---|---|---|---|
| | providers); combine e-learning with on-site exercises | | |

Site Application Rules (Summary)

- Differences in equipment and staffing from head office standards shall be clearly described in site-specific appendices; substitute controls must always be specified.
- Exceptions require risk assessment and approval by the Site Food Defense Leader and the Food Defense Officer.
- OEMs and external logistics providers shall be bound by contract clauses covering seals, access control, records, and correction / corrective action, and compliance shall be verified through audits.

**5. Verification and Review**

Regular review:
Conducted once a year (April), led by the Food Defense Officer.
Effectiveness shall be verified using such indicators as the number of reports, completion rate of correction / corrective action, number of seal discrepancies, and occurrence of exceptional access.
Internal audit:
Head office teams shall conduct rotational audits of sites according to the annual plan. OEMs and external logistics providers shall also be included within the audit scope.
Ad hoc review:
Conducted immediately in the event of major complaints, social incidents, or equipment / organizational changes. Deadlines shall be set for horizontal deployment of lessons learned.

**6. Document and Record Control**

- Version control shall be managed in the document control system, with revision history, approval, and distribution list visible.
- The latest version shall be immediately accessible at the operational level.
- Audit trails in the core business system shall be configured to prevent tampering. Retention periods for paper records shall be clearly categorized.
- Consistency of related procedures, checklists, and training materials shall be checked periodically.

**7. Appendices and Reference Information**

Appendix 1: Threat Assessment Sheet
Appendix 2: Recall Response Procedure
Appendix 3: Training and Exercise Plan / Records
Appendix 4: Site-Specific Appendices (zoning maps, differences in access policies, video retention periods, list of substitute controls)
Reference: Items for future consideration
(electronic recordkeeping for key process steps, serialization of seals, strengthening of logistics traceability, etc.)

End of Example Food Defense Plan: Type 3 – Community-Based, Single-Plant Model (SMEs / Specialized Processors)

**Food Defense Case Studies**

**I. Defense Against Human Factors**

**Case①: Suitability Checks at the Hiring Stage (Defense at the Point of Entry)**

**Content:**

From the recruitment interview stage, personnel evaluation was conducted from a Food Defense perspective. Specifically, interview questions were prepared to assess applicants' integrity, cooperativeness, and safety awareness, positioning "hiring trustworthy personnel" itself as the first step in defense.

For interviewers, prior training was provided on "interviewing with a Food Defense perspective," and a system was introduced to identify early signs of problematic behavior or criminal tendencies through attitude, remarks, and work history.

**Explanation:**

The starting point of Food Defense is not "preventing intrusion into the facility," but controlling the point of entry for people. No matter how robust the defense measures may be, if a person with malicious intent is hired into the organization, the defense system can collapse. Safety considerations at the hiring stage are as important as security control, and selecting people who can share the organization's Food Safety Culture is the first defensive action.

**Key points:**

- Hiring is the point of entry for defense; bringing in trustworthy people is the greatest risk reduction.
- Training interviewers to recognize Food Defense concerns is important; behavioral tendencies should be prioritized over superficial career history.
- A system that incorporates Food Defense awareness from the stage of evaluating people is effective.

**Case②: Thorough Training on Seal Control**

**Content:**

Training was conducted so that employees understood the purpose of seals (e.g. cable ties). The reason for leaving the excess tail uncut was explained in terms of tamper prevention and preservation of evidence, resulting in consistent operation at the operational level.

**Explanation:**

The key to embedding this practice is not merely training on work procedures, but training that promotes understanding of the intent behind the behavior. Once employees understand the purpose, they can make correct judgments more quickly than by relying on manuals alone.

**Key points:**

- Training that helps personnel understand "why it is done this way" is essential.
- Understanding the purpose leads to autonomous behavior and strengthens defense.

**Case③: Implementation of On-Site Patrols**

**Content:**

Regular patrols by personnel were conducted to detect unusual signs that cameras could not capture. Through conversations with employees, awareness of Food Defense was also strengthened.

**Explanation:**
Patrols should be regarded not as “surveillance,” but as opportunities for dialogue. By going to the operational level in person, changes in atmosphere that machines cannot detect can be sensed.

**Key points:**

- Human senses are more delicate sensors than AI.
- The purpose of patrols is not only “detection of abnormalities,” but also “building trust with the operational level.”

**Case④: Training Ended Only as “Knowledge Sharing” (Poor Example)**
**Content:**
Food Defense training was conducted in a classroom format, but participants were unable to relate it to their own work, and no change in behavior was observed.

**Explanation:**
The purpose of training is not “increasing knowledge,” but “changing behavior.” Training that only conveys knowledge creates an organization in which many people know the information but cannot act. In Food Defense training, practical exercises that assume abnormality detection, reporting, and initial response are indispensable.

**Key points:**

- Training effectiveness should be measured by “response speed” and “repeatability.”
- Follow-up after training, such as exercises and role-play, is necessary to embed behavior.
- The Purpose is not to create knowledgeable people, but people who can make judgments.

**Case⑤: Training for Outsourced Parties Was Overlooked (Poor Example)**
**Content:**
Food Defense training was not provided to logistics providers and OEM contractors, resulting in differences in understanding regarding seal control and receiving procedures. As a result, seal control during transportation became careless, causal tracking was not performed, and the effectiveness of the seals was lost.

**Explanation:**
Food Defense does not end within the site boundary. A perspective is needed in which contractors and business partners are regarded as part of the organization. If training is not shared, the entire supply chain becomes uneven and vulnerable to attack.

**Key points:**

- The scope of training should not be limited to the plant, but expanded to external parties that may be affected.
- Joint exercises with contractors and logistics providers are effective.
- Weaknesses in external coordination can nullify internal defense.

**Case⑥: Preparedness for Behavioral Risks Arising from Ideology, Beliefs, or a Sense of Religious Mission**
**Content:**
The organization assumed the possibility that individuals inside or outside the organization might

intentionally contaminate, damage, or adulterate food based on internal beliefs such as ideology, personal convictions, or a sense of religious mission. In the defense plan, the basic policy was to recognize and manage such acts not as a denial of any specific religion or ideology, but as a risk of behavioral deviation. In training and exercises, initiatives were implemented to clearly communicate the principle that, while personal beliefs should be respected, any act that compromises food safety is unacceptable regardless of motive.

**Explanation:**
Threats in Food Defense are not limited to economic, emotional, or personal motives. Social, ideological, or religious beliefs may also drive a person through a sense of justice or mission. Such value-driven behavior is difficult to detect in advance, but by explicitly stating that deviant behavior will not be accepted even if justified by ideology, the organization can maintain consistency and fairness in its defense culture.

**Key points:**

- Mature defense means having a system that anticipates all possible motives and prevents deviant acts before they occur.
- The Purpose is not to deny religion or ideology, but to manage deviations from behavioral standards as a risk.
- Training and exercises should clearly communicate a stance of respecting beliefs while prioritizing safety.

**II. Physical and Facility-Related Defense**
**Case⑦: Design Improvements to Pockets in Work Uniforms**
**Content:**
To reduce the risk of bringing foreign materials or unnecessary items into or out of the plant, the use of uniform pockets and carried items was reviewed for each process step. At the time of introduction, the reasons for the measure were explained carefully in order to gain cooperation.
In process steps with a high risk of foreign material contamination, operations were changed so that pockets were not used, for example by sealing pockets or using uniforms without pockets, while necessary items were managed in transparent pouches or as shared equipment.
In process steps where it was necessary to carry communication devices such as PHS handsets, pockets were retained, but rules were established on what could and could not be placed in them, and inspections were carried out.

**Explanation:**
This approach achieved defense not through prohibition, but through understanding and acceptance. By providing alternative means instead of simply restricting behavior, voluntary cooperation was encouraged. At the same time, if rules are not defined for pockets and similar features, unrestricted carrying practices may develop. It is therefore necessary to establish and operate rules for carried items. In addition, sufficient consideration should be given to occupational safety, such as ensuring emergency means of communication like PHS devices.

**Key points:**

- Defensive measures become embedded through understanding and acceptance.
- Systems that compensate for inconvenience generate cooperation.
- Motivation based on shared purpose, rather than simple prohibition, is the key.

**Case⑧: Access Control Using IC Tags**
**Content:**
Entry to and exit from high-risk areas was controlled using IC tags, with authority set according to job position and task. Access history was recorded automatically, and rights were changed and tags collected immediately when personnel were transferred or left the company.

**Explanation:**
The key to IC tags is not the technology itself, but how it is operated. Delays in updating authority or failures to collect tags create vulnerabilities. Clarifying management responsibility and establishing update procedures improved the overall level of defense.

**Key points:**
- Designing operational rules is more important than introducing technology itself.
- A system is needed that enables immediate updates and collection of access rights.
- The measure should be positioned not as “surveillance,” but as “visible reassurance.”

**Case⑨: Color-Coding of Uniforms**
**Content:**
Uniforms were color-coded by work area so that unauthorized entry or suspicious behavior could be identified at a glance.

**Explanation:**
The simplest defensive measure is visibility, and it is also effective. A system that anyone can recognize immediately increases daily deterrence and the accuracy of monitoring.

**Key points:**
- A system that is easy for everyone to understand is important.
- Visual management is low-cost and highly effective.

**Case⑩: Multi-Purpose Use of Equipment (Body Temperature Measurement Camera)**
**Content:**
Cameras introduced during the COVID-19 period were used not only for temperature screening but also for suspicious person detection.

**Explanation:**
The idea of “reuse rather than new introduction” is important regardless of company size. By making multi-purpose use of existing equipment, a practical and sustainable defense system can be established.

**Key points:**
- Thinking in terms of repurposing rather than new installation promotes sustainability.
- Assigning equipment a role in protecting safety changes awareness.

**Case⑪: Insufficient Data Storage Capacity for Surveillance Cameras (Poor Example)**
**Content:**
More than 100 surveillance cameras were installed for deterrence, but video retention and

inspection systems were not properly established, and more than half of the units stopped operating. It was necessary to consider not only installation cost but also operational cost.

**Explanation:**
When the Purpose of defense measures becomes merely “introducing them,” they collapse once operational capacity is exceeded. In Food Defense, cameras are not intimidation devices, but tools that must serve both deterrence and verification.

**Key points:**

- The essence of defensive equipment lies not in installation, but in operational design.
- Cameras require both a layout that creates reassurance and a system that enables actual review.

**Case⑫: Inadequate Inspection of IC Tags (Poor Example)**
**Content:**
IC tags for access control were introduced, but inspections were overlooked, and failures went unnoticed, resulting in missing access records.

**Explanation:**
For technical countermeasures, introduction is not the point of completion, but the beginning of operation. The reliability of defense depends on whether maintenance is embedded into the system by defining who checks what, when, and how.

**Key points:**

- Technical defense requires planning that includes operation.
- Responsibility for detecting failures should be clearly assigned and incorporated into the audit cycle.

**Case⑬: Intrusion Following Damage to the Receiving Gate (Poor Example)**
**Content:**
When the receiving gate was damaged, an outside passerby mistakenly entered the site before repairs were completed.

**Explanation:**
Defense plans are often designed only for normal operating conditions. In reality, however, vulnerabilities often become visible in unexpected situations.

**Key points:**

- The real value of a Food Defense Plan is tested in exceptional situations.
- Emergency response should be defined and embedded through routine training.

**III. Information and Technical Defense (Digital and Data Management)**
**Case⑭: Reconstruction of the Product Management System (Blockchain)**
**Content:**
Blockchain was used to prevent tampering with product data and to achieve a high level of transparency.

**Explanation:**
Information tampering is a typical example of invisible insider wrongdoing. While the introduction of digital technology has increased convenience, it has also made risks more apparent. However, by creating a new layer of defense through reliable linkage of records, such risks can be reduced.

**Key points:**
- Information protection is a new theme in Food Defense.
- Digital technology can secure transparency by leaving traces and linking records.

**Case⑮: "Ambiguity of Responsibility" After System Introduction (Poor Example)**
**Content:**
A new defense system, such as IC tags and seal control, was introduced, but operation began without clearly defined responsible persons. Inspections and reporting were handled on an ad hoc basis by individuals, and failures were not noticed.

**Explanation:**
The lifespan of a system is determined by the clarity of responsibility. If authority, alternates, and inspection responsibility are not defined at the time of introduction, the system becomes hollow as personnel changes occur. Deciding who is responsible for maintaining the system forms the backbone of the defense structure.

**Key points:**
- A system requires clear responsibility, authority, and alternates.
- Training must be conducted when managers are replaced.
- Unclear responsibility becomes a vulnerability.

**IV. External and Supply Chain Defense (Transactions and Distribution Stages)**
**Case⑯: Introduction of a Registration System for Shipping and Receiving Destinations**
**Content:**
Contracts, audits, and certification criteria were clarified, and transactions were limited to trustworthy business partners.

**Explanation:**
The most effective way to address externally originating threats is to block them at the point of entry. More than post-incident response, pre-selection rules provide the strongest defense.

**Key points:**
- Entry-point defense in the supply chain is crucial.
- Trustworthiness is established at the contract stage.

**Case⑰: Inadequate Seal Control (Poor Example)**
**Content:**
A tanker truck driver possessed a large number of seal stickers, rendering the reliability of the seals meaningless. There were no rules for controlling seal numbers or issuance records, and there was no way to detect tampering.

**Explanation:**
A seal is both physical evidence and psychological deterrence. If seals are easily obtained or exchanged, they no longer function as seals. Defense is established only by consistently controlling who manages them, who uses them, and who verifies them.

**Key points:**

- The value of a seal lies in its scarcity and consistency of control.
- In Food Defense measures that depend on cooperation with suppliers, mutual understanding of the Purpose is key to reliability.

**V. Organizational and Cultural Defense (Systems, Standardization, and Principles)**
**Case⑱: Installation of Boxes for Unnecessary Items**
**Content:**
Boxes for unnecessary items were placed at the operational level to create a habit of removing foreign materials and unneeded objects.

**Explanation:**
Orderliness is the first step in defense. An environment in which abnormalities can be detected immediately is itself a form of defense.

**Key points:**

- Orderliness is defense. A workplace where abnormalities can be noticed easily is effective not only from a hygiene perspective, but also from a defensive perspective.

**Case⑲: Certification or Conformity Assessment of All Business Sites to JFS-C and Related Schemes**
**Content:**
All sites obtained JFS-C certification, thereby standardizing both systems and operation.

**Explanation:**
Third-party certification provides visible proof of trust. It helps suppress variation among sites and has the effect of unifying organizational culture.

**Key points:**

- Certification is a tool through which trust is externally assured.
- Standardization raises the overall level of defense across the organization.

**Incident Examples**

- Incident Example①: Frozen Food Pesticide Contamination Incident (2013)
- Incident Example②: Ransomware Attack on a Major Domestic Beverage Manufacturer (2025)
- Incident Example③: Inappropriate Video at a Major Pizza Chain (2021)
- Incident Example④: Nuisance Videos at Conveyor-Belt Sushi Chains (2023–2025)
- Incident Example⑤: Bolt and Nut Contamination Incident (2025)

**Incident Example①: Frozen Food Pesticide Contamination Incident (2013)**
**Overview:**
Pesticide (malathion) was found in frozen food products manufactured at a plant in Gunma Prefecture, and consumers reported a series of complaints involving unusual odors and health problems. The investigation revealed that the contamination had been intentionally caused by a plant employee, and the case developed into a criminal matter.

**Food Defense Analysis:**

- A typical example of an internal threat: The key point is that the contamination was caused not by outside intrusion but by an internal employee. It showed that employee dissatisfaction and motive can be underlying factors, and that physical measures alone are not sufficient to prevent such incidents.
- Limits of access control: Because workers inside the plant have legitimate access rights, preventing external intrusion alone is not enough. A defensive culture that includes internal monitoring and psychological safety is also required.
- Lessons in response: Products already in distribution were recalled, authorities were notified, and the investigation was conducted transparently; however, restoring consumer trust took a long time. This highlighted the need not only for post-incident response, but also for preventive training and system building.

**Key Lessons:**

- The risk of insider misconduct can never be reduced completely to zero. It is essential to build a culture in which employees are treated not as “subjects of surveillance” but as “trusted colleagues,” while also maintaining systems that enable abnormalities to be detected at an early stage.

**Incident Example②: Ransomware Attack on a Major Domestic Beverage Manufacturer (2025)**
**Overview:**
In 2025, a major domestic beverage manufacturer was targeted by a ransomware cyberattack, which caused shutdown of the core systems responsible for order processing and shipment. As a result, temporary production and shipment stoppages occurred at multiple plants, and the impact spread across the supply chain, including delays in new product launches and temporary shortages of some products. The company also disclosed the possibility that personal information relating to

customers and business partners had been leaked externally. This case demonstrated that food and beverage supply can be disrupted even by cyber-originated attacks.

Food Defense Analysis:

**An example showing that "information management" must also be treated as a defense target**

- The attack did not directly target production equipment itself. However, by encrypting and shutting down the information systems supporting order processing, inventory control, shipment, and traceability, it created a situation in which the company could no longer confidently state that products had been "produced safely" or "shipped safely."
- This supports the need to position **information management** as a formal process area within the Food Defense Plan. If records or lot information are tampered with, deleted, or rendered inaccessible, the reliability of traceability and manufacturing records is at risk.

**Intentional, external, non-contact attacks can directly stop supply**

- Even without physically entering a plant, an attacker can deliberately paralyze information systems through a cyber route and thereby severely disrupt production, shipment, and sales.
- If Food Defense is understood only as the control of people and materials within a facility, these kinds of external, non-contact threats may be overlooked.

**The issue is not only "whether recovery is possible," but also "whether evidence can be preserved to show that data has not been tampered with"**

- In a ransomware attack, the key issue is not only whether systems can be restored, but also whether the company can demonstrate which data has not been altered or deleted.
- Dual recordkeeping for process records (online plus offline), physical separation of backups, segregation of access rights, and preservation of audit trails all need to be incorporated into Food Defense as measures that enable the organization to explain the authenticity of records after the fact.

**Attacks may continue after the core system is down**

- An attack on a core system may not aim only at causing system downtime itself. In some cases, the attacker may exploit the weakened security state after shutdown in order to destroy, steal, or alter internal data.
- For this reason, threat assessment should not be limited to the system itself being attacked; it is also important to consider attacks on the data stored in that system.

**Key Lessons:**

- When the data and systems that serve as the basis for shipment suspension decisions or recall decisions are attacked, the organization may fall into a state in which it "wants to protect consumers, but no longer has the basis on which to make that judgment."
- In addition to physical and human defensive measures, it is essential to incorporate **information defense** into the Food Defense Plan so that records cannot be tampered with, cannot be deleted, and can be traced afterward.
- Information defense should not be treated as a mere appendix to the plan. It is necessary to clarify which systems affect which process steps and decisions if they stop, and which records must be designed so that they can never be deleted or altered, and to position **information defense** with the same weight as physical and human measures.

**Incident Example③: Inappropriate Video Posted from a Major Pizza Chain Store (2021)**
**Overview:**
In this case, a part-time employee at a pizza chain store filmed and posted unsanitary behavior, such as putting ingredients in their mouth during food preparation. The company issued an apology and announced measures to prevent recurrence. The store was identified, and the video spread widely on social media.
**Food Defense Analysis:**

- This is a typical example of internal × non-malicious in intent (careless / done for amusement). Even if there was no clear intent to attack, the outcome still required the same type of response as intentional contamination, including suspension of sales and efforts to restore trust.
- It is necessary to define, together with hygiene rules, the extent to which personal smartphones and filming in work areas are permitted or prohibited. Otherwise, this type of incident cannot be prevented.
- It is not enough to address the problem only at the individual store level; the head office must also use monitoring and training to eliminate the same pattern of inappropriate behavior across the organization.

**Key Lessons:**

- "Pranks" or behavior aimed at gaining attention on social media will not be understood as unacceptable unless concrete examples are shown in training.
- Clearly documenting prohibited acts in advance and communicating disciplinary policies for violations also functions as a defensive measure.

**Incident Example④: Spread of Nuisance Videos and Inappropriate Conduct at Conveyor-Belt Sushi Chains (2023–2025)**
**Overview:**
In 2023, a series of cases occurred in which customers at conveyor-belt sushi chains filmed and posted videos on social media showing themselves licking cups and soy sauce bottles intended for other customers, or touching sushi on the conveyor line. Similar nuisance conduct continued to be reported in 2025, prompting major chains to strengthen monitoring and announce claims for damages.
**Food Defense Analysis:**

- This is a typical example in which conduct by customers, ranging from non-malicious to semi-intentional, leads to the same outcome for the company as intentional contamination.
- Installing cameras alone is not sufficient. Layout design that reduces customer access to food, together with operational deterrents such as patrols and verbal intervention, is also necessary.
- Because social media spreads information so quickly, brand damage can occur before the facts are fully confirmed. Therefore, initial public communication and retention periods for security footage must also be regarded as part of defense.

**Key Lessons:**

- The targets of monitoring are not only employees, but all persons who temporarily gain access to the plant or store.

- External, non-malicious, or prank-like behavior should also fall within the scope of Food Defense.

**Incident Example⑤: Bolt and Nut Contamination Incident at a Food Manufacturing Plant (Nagasaki, 2025)**

**Overview:**

At a food manufacturing company in Omura City, Nagasaki Prefecture, a former employee became the subject of a police investigation on suspicion of intentionally mixing bolts, nuts, and similar items into products inside the plant. The company proceeded with product recall and investigation of the cause.

**Food Defense Analysis:**

- This is a typical **internal × intentional** attack in which a person with legitimate access to the plant used readily available items such as tools and parts as the means of attack.
- It raises the question of how to control objects that are readily available near the line and could be used for contamination, such as lockers, tools, and replacement parts.
- The case also suggests that the timing of resignation or contract termination, as well as deterioration in human relationships, can increase risk, indicating that cooperation with the human resources function is also necessary in Food Defense.

**Key Lessons:**

- Physical locks and cameras alone cannot fully control “foreign materials that are within reach of people already inside.”
- Systems that keep inspections, line monitoring, and abnormality reporting operating continuously are critical.

# 4. Q&A

1. Basic Understanding

Q1. What is the difference between Food Safety (HACCP) and Food Defense (TACCP)?
Q2. Why is Food Defense now necessary in Japan as well?
Q3. What does Food Defense protect, and from what?

2. Practice and Implementation

Q4. What does it mean to think from the attacker's perspective?
Q5. How far do we need to go? What is sufficient?
Q6. If the budget is limited, what countermeasures should we start with?
Q7. Are cameras essential? Even if many are installed, can they really provide defense?
Q8. What should we do if a business partner asks where the cameras are located?

3. Understanding the Workplace and People

Q9. Employees may feel that they are being monitored. How should this be communicated?
Q10. How can employee dissatisfaction or frustration be identified?
Q11. How are labor management and employees' dissatisfaction or distrust related to Food Defense?
Q12. Is it possible to prevent an attack completely?

4. Audit, Assessment, and External Response

Q13. What points are checked in an audit?
Q14. How can external attacks or warning signs be identified?

**1. Basic Understanding**

**Q1. What is the difference between Food Safety (HACCP) and Food Defense (TACCP)?**

**A1:** HACCP is a system for preventing accidental and naturally occurring hazards (e.g. bacterial contamination, temperature deviations, etc.), whereas TACCP (**Food Defense**) is a system for protecting food against intentional and malicious acts (e.g. foreign material contamination, sabotage, insider attacks, etc.).

| Item | HACCP | TACCP |
|---|---|---|
| Primary Purpose | Prevention of accidental hazards | Protection against intentional and malicious hazards |
| Nature of risk | Accidental / unintentional | Intentional / malicious |
| Focus of control | Microorganisms, foreign materials, temperature, process steps | People, behaviors, psychological conditions, and facility management |
| Main activities | Hazard analysis and control | Threat assessment; identification of motive, means, and opportunity |
| Functions involved | Production / Quality Assurance | Managers / Food Defense team / Top Management |

**Q2. Why is Food Defense now necessary in Japan as well?**

**A2:** In the past, it was commonly believed in Japan that Food Defense was necessary overseas but not domestically. However, in 2013, an incident occurred at a frozen food company in Gunma Prefecture in which a contract employee intentionally mixed pesticide into products, making it clear that intentional acts originating from within the company could also occur in Japan. This incident helped spread the recognition that Food Defense is also an essential system in Japan as part of food safety.

**Q3. What does Food Defense protect, and from what?**

**A3:** Food Defense is a system for protecting against intentional attacks on food. Its purpose is not only to protect the food itself, but also to maintain trust. Food Defense is not limited to preventing physical harm; it is also a system for minimizing risk and ensuring that the company's credibility is not lost even if a problem occurs. In this sense, Food Defense supports the organization's trust, not merely its risk management. Although it primarily addresses **intentional attacks**, in recent years it has also become necessary to consider acts such as pranks or careless behavior that may, as a result, lead to serious damage.

**2. Practice and Implementation**

**Q4. What does it mean to think from the attacker's perspective?**

**A4:** It means reviewing the process steps from the viewpoint of, "If I were the attacker, where would I target?" For example, if you imagine yourself as a part-time worker, cleaning staff member, or external contractor, vulnerabilities that would otherwise go unnoticed may become visible. This is a method based not on an optimistic assumption of goodwill, but on the perspective of assuming bad intent, and it greatly improves the quality of the defense plan.

**Q5. How far do we need to go? What is sufficient?**

**A5:** It is not necessary to implement countermeasures for every possible threat. Instead, assess **severity of impact** and **ease of execution** through threat assessment, and address the higher-

priority threats first. Even for low-priority threats, simply identifying and understanding them is itself a meaningful measure.

**Q6. If the budget is limited, what countermeasures should we start with?**
**A6:** It is effective to begin with **soft measures**, such as training, awareness-building, and reporting systems. Even without relying on hard measures such as cameras or fences, there are many low-cost but effective approaches, including checklists, seal control, entry/exit records, and reporting exercises. The most important point is to **start with what can be done**.

**Q7. Are cameras essential? Even if many are installed, can they really provide defense?**
**A7:** Cameras are equipment for **recording**; they do not in themselves stop an attack. What matters is operation in a way that enhances deterrence. For example, by posting notices such as "Recording in progress" or "Monitoring for Quality Assurance," and by operating the system in a way that gives employees a sense of reassurance, it is possible to achieve both psychological deterrence and trust.

**Q8. What should we do if a business partner asks where the cameras are located?**
**A8:** For security reasons, it is not necessary to disclose all detailed camera locations. One possible explanation is:
"They are installed for crime prevention and quality assurance purposes, and are positioned so as to minimize blind spots; however, the detailed layout is managed as internal control information."
It is also advisable to limit the number of people who understand the full picture and to divide control responsibility by department. By managing information in a distributed manner, the defense plan itself can also be protected. For example:

- Coverage of camera installation: Engineering / Facilities function
- Format and update frequency of entry permits: General Affairs function
- Monitoring items for quality inspection: Quality function

**3. Understanding the Workplace and People**
**Q9. Employees may feel that they are being "monitored." How should this be communicated?**
**A9:** Food Defense is not a system for "suspecting people," but for **protecting people**.
Understanding can be shaped by the words used. For example, internal cameras may be referred to not as "surveillance cameras," but as "quality assurance cameras" or "safety support cameras." It is important to explain carefully that defense is a system for reassurance and safety.

**Q10. How can employee dissatisfaction or frustration be identified?**
**A10:** Because dissatisfaction and isolation can become motives for insider acts, ensuring **psychological safety** is important. The following approaches are effective:

- Regular one-on-one discussions and check-ins
- Observation in day-to-day operations (e.g. isolation, changes in facial expression, etc.)
- Use of anonymous suggestion boxes or reporting channels
- Feedback on reports, including sharing of response measures

A system that makes employees feel, "I'm glad I spoke up," becomes the strongest form of defense.

**Q11. How are labor management and employees' dissatisfaction or distrust related to Food Defense?**
**A11:** Employee dissatisfaction or distrust needs to be considered in Food Defense because it can become a risk factor leading to intentional or semi-impulsive acts from within the organization. For

this reason, proper labor management is important, including transparency in wages, work shifts, and evaluation, so that employees do not feel that they are being treated unfairly. It is also important to establish an environment in which abnormalities or concerns can be reported immediately. Measures such as anonymous reporting, hotlines, and routes for consultation other than one's direct supervisor are effective in lowering the psychological barrier to reporting. In addition, when a report is made, it is important to respond promptly and provide feedback to the reporter, thereby building a relationship of trust in which employees feel that reporting was worthwhile. Such systems help achieve both early detection and prevention. In Food Defense, not only physical surveillance and access control, but also people-related management—psychology, reporting, and communication—should be positioned as an essential element.

**Q12. Is it possible to prevent an attack completely?**
**A12:** Complete prevention is difficult. However, it is possible to minimize damage by **raising the barriers to committing an attack** and by **detecting it at an early stage**. For example, combining entry/exit records, seal control, and reporting exercises can create an environment in which misconduct is difficult to carry out and likely to be discovered quickly.

**4. Audit, Assessment, and External Response**
**Q13. What points are checked in an audit?**
**A13:** The following three points are mainly checked:

- Whether threats have been identified appropriately
- Whether the countermeasures are suitable for the company's own circumstances
- Whether the countermeasures are actually functioning in practice

The focus of evaluation is not on formality, but on **effectiveness**. It is important to be able to explain how the company understands its own threats and how it is addressing them.

**Q14. How can external attacks or warning signs be identified?**
**A14:** Early detection of suspicious persons or unusual behavior begins with everyday awareness. It is effective to share examples of warning signs such as the following:

- An unfamiliar person wandering around the premises
- Persistent questioning about process steps or working hours
- An increase in suspicious phone calls or e-mails
- Bringing in unnecessary items or equipment

Audits are also an effective means of identifying external threats and abnormalities. From the auditor's side, confirming whether suppliers and business partners have appropriate Food Defense arrangements can help identify risks at an early stage. From the auditee's side as well, external audits provide a valuable opportunity to identify weaknesses and areas for strengthening the company's own defense arrangements and to improve them. The most effective defensive measure is not to ignore a sense of something being wrong.

# 5. REFERENCE INFORMATION, SCENARIOS, AND LINKS

**1. Column:**

**“Pranks” in the Grey Zone Between Intentional and Unintentional Acts**

**2. Reference Scenarios and Case Examples**

**Overview: Threats, Defense Points, and Vulnerabilities by Process Step**

- Bulk liquid / batch processes
- Dry / powdered raw materials
- High-value dairy products (receiving process)
- On-site addition processes such as bakery and deli production
- Outsourcing, rework, and material control
- Packaging, labeling, and final shipment
- Logistics, warehousing, and the cold chain
- Retail, events, and e-commerce (public-facing environments)
- Mass catering and peak-demand periods (e.g. school meals)
- Misuse of waste and rework
- Reliability of testing and data
- Tampering with tasting corners (cases amplified on social media)

**3. Scenario Analysis, Evaluation Methods, and Domestic / International Guidelines and Links**

- Scenario analysis (impact, accessibility, detectability)
- KAT (Key Activity Types) method
- Threat assessment method: CARVER+Shock
- Threat assessment using MAFF checklists
- Threat assessment based on Nara Medical University Department of Public Health materials and the Food Defense Guidelines
- Support for developing mitigation strategies (use of FDMSD)
- Japan Food Safety Management Association

**4. Appendix**

**Food Defense Plan [Template]**

**1. Column: “Pranks” in the Grey Zone Between “Intentional” and “Unintentional”**
**— Thinking about Food Defense in Terms of Organizational Impact Rather than Motive —**

Food Defense was once regarded as an issue outside Japan. While the Japanese food industry developed primarily around hygiene and quality control, preparedness for intentional attacks on food was long underestimated. However, the pesticide contamination incident involving frozen foods that occurred in Japan in 2013 changed that perception. In that case, a contract employee intentionally mixed malathion into products within the plant, confronting the industry with the fact that “Japanese food was intentionally contaminated by a Japanese employee,” and demonstrating that Food Defense is also a realistic issue in Japan. Following that incident, more companies introduced surveillance cameras and access control, but the question remained: what kind of system can truly prevent such events? The issue is not only the establishment of equipment and rules, but also how to deal with the ambiguity of human behavior and motivation.

**“Intentional” and “Unintentional” Exist on a Continuum in Human Behavior**

When discussing food attacks, intentional and unintentional acts are often considered separately. In reality, however, there is a broad grey zone between them. “Intentional” refers to acts carried out with the purpose of harming the organization or its products, whereas “unintentional” refers to acts arising from ignorance, misunderstanding, carelessness, or impulsive behavior often described as a “prank.” For the organization, however, both can cause damage and therefore both fall within the scope of defense. The essence of Food Defense lies not in determining motive, but in designing systems in which the act itself cannot be successfully carried out.

**Food Attack Assumption Map: Capturing the Full Range of Acts**

When organized according to the actor’s intent and whether the act originates internally or externally, the scope of defense expands as follows:

| Classification of attack | Intentional (clear intent to attack) | Unintentional (ignorance, carelessness, prank) |
|---|---|---|
| Internal acts | Contamination or destruction out of retaliation or dissatisfaction; data tampering; false records | Operational mistakes due to insufficient training; careless acts such as social media posting or filming; “for-fun” pranks |
| External acts | Direct contamination through intrusion; fraudulent labeling; intentional attacks by competitors or anti-social groups | Contractors’ or visitors’ lack of understanding of rules; inappropriate posting or sharing for attention; “for-fun” pranks |

Even unintentional acts such as ignorance, carelessness, and pranks should be anticipated as defense targets because they can still result in loss of trust, recalls, and other serious consequences.

**A Shift in Thinking: Do Not Underestimate “Pranks”**

In recent years, careless posts and inappropriate videos have spread rapidly on social media, instantly damaging corporate credibility. Many of these acts are not driven by malice, but by curiosity or a momentary lapse in judgment. However, the resulting damage to the company can be just as serious as that caused by deliberate harm. Therefore, even “pranks” should be treated as defense targets. Rather than dismissing them as unavoidable because there was no malicious intent, it is important to understand the structure by which ignorance, carelessness, and poor judgment can turn into an attack.

**Practical Directions for Response**

| Category | Purpose | Examples of initiatives |
|---|---|---|
| Education and Training | Help people understand that even without malice, serious consequences can arise | Include examples of pranks and operational mistakes in new employee training; clearly state social media conduct rules |
| Psychological Safety | Foster a workplace culture where even small abnormalities or concerns can be reported | Consultation and reporting systems built on Food Safety Culture |
| Rule Development | Eliminate ambiguous areas | Clearly document and periodically train on filming, posting, access, disposal, etc. |
| Audit and Verification | Check whether operation has become merely formal | Verify training effectiveness and level of compliance in the annual review |

These initiatives are not merely about establishing codes of conduct, but about forming a culture that prevents attacks arising through human behavior.

**The Most Effective Defense Is to Think Like the Perpetrator**

The true value of Food Defense does not lie in equipment or documents, but in embedding within the organization the perspective of “thinking as if you were the perpetrator.” Imagine where an attacker would target and what kinds of actions could succeed. Through this thought experiment, previously unseen blind spots and weaknesses within the company become visible. This is not a pessimistic view of human nature, but a realistic risk management perspective. What matters is to address risks that could arise under any circumstances, whether they stem from crime, pranks, or mistakes.

## 2. Reference Scenarios and Case Examples

### Cases Where Food Defense and Food Fraud Overlap

This chapter organizes cases such as “label substitution,” “raw material substitution,” and “reintroduction through repackaging,” which might at first glance be classified as Food Fraud, as threats, weaknesses, and defense points from a Food Defense perspective.

In general, **Food Defense** refers to malicious intentional acts aimed at causing harm to consumer health or disrupting business continuity, whereas **Food Fraud** refers to intentional deception for economic gain or unfair advantage. In actual operations, however, the two often overlap. For example, economically motivated substitution of raw materials may ultimately impair food safety, or unexpected allergen contamination may occur.

In this Handbook, such cases are organized on the basis that, regardless of whether the motive is economic, acts that may result in harm to health should also be treated as important Food Defense threats. In practice, it is important not to force a distinction between “defense” and “fraud,” but to examine weaknesses from both perspectives.

### Overview: Threats, Vulnerabilities, and Defense Points by Process Step

#### 1) Bulk Liquid / Batch Processes (Tanks / Filling / Cooling)

Possible acts include introduction of harmful substances through charging ports, spraying into cooling tanks, and falsification or destruction of seals affecting large lots.

**Vulnerabilities likely to attract attackers:**

- Blind spots during night shifts or low-staff periods; weak control of duplicate keys or spare seals
- Witnessing that has become merely formal; inability to trace logs afterward
- Openings such as cooling tanks and headspaces that are not adequately controlled

**Defense points:**

- Eliminate sole discretion through seals, key control, and two-person witnessing
- Ensure completeness of opening and inspection logs (who / when / what)
- Make the pre-packaging gate functional as a critical checkpoint for focused inspection and isolation decisions

#### 2) Dry / Powdered Raw Materials (Powders / Spices)

Possible acts include bag substitution (lot substitution), introduction of harmful substances or foreign materials into powders, and tampering with seal numbers during receipt to storage.

**Vulnerabilities likely to attract attackers:**

- Unclear accountability in intermediary distribution segments
- Insufficient sampling at receipt; omission of seal verification
- Unmonitored temporary storage areas

**Defense points:**

- Three-part control set: receiving test + seal number verification + lot traceability
- Stricter supplier selection through supplier approval and audits
- Immediate isolation in the event of abnormalities, followed by routine cause tracing

Note: Bag or lot substitution may also constitute Food Fraud when driven primarily by economic motives. Here it is also treated as a Food Defense threat as an intentional intervention that undermines safety and traceability.

**3) High-Value Dairy Products / Raw Milk (Receiving Control)**
Possible acts at receipt include dilution or substitution of raw materials, application of foreign matter to tank surfaces, and injection into raw milk tanks.
**Vulnerabilities likely to attract attackers:**

- Weak monitoring of high-value items, leaving room for substitution
- Lack of rapid testing for raw milk; seal control of tanks having become merely formal
- Confusion during busy receiving operations

**Defense points:**

- Dual-layer control through segregation of duties (purchasing × receipt) and periodic analysis
- Surface-origin checks immediately before shipment (appearance / wipe tests)
- Seal control and access control for farms and milk collection tanks

**4) On-Site Addition Processes such as Bakery and Deli Production**
Possible acts include foreign material contamination during weighing and addition, intentional bringing in of allergen powders, and tampering with addition instructions.
**Vulnerabilities likely to attract attackers:**

- Omission of checks during busy periods
- Gaps in daily checks of detection equipment
- Poor visibility in preparation areas

**Defense points:**

- Thorough double-checking (person × person / person × system)
- Verification of allergen control and metal detection validity
- Access control for preparation areas and consistency during changeovers

**5) Outsourcing, Rework, and Material Control (External Parties and Material Lifecycle)**
Possible acts include mixing of unauthorized substances by contractors, substitution of packaging versions or labels, and alteration through unofficial rework.
**Vulnerabilities likely to attract attackers:**

- Blind trust based on “because it is outsourced”; insufficient verification
- Rework becoming a breeding ground for off-record operations
- Weak version control and disposal control of packaging materials

**Defense points:**

- Explicit Food Defense requirements in contracts and on-site audits
- Visualization and approval control to prevent unofficial outsourcing
- Integrated management of packaging materials from receipt through disposal, including segregation of obsolete versions

**6) Packaging, Labeling, and Final Shipment**
Possible acts in the final stage include insertion of items into final packaging, intentional label substitution, and falsification or destruction of sealing.
**Vulnerabilities likely to attract attackers:**

- Lack of double-checking for label substitution
- Blind spots on the final line and sealing control that has become merely formal
- Staff shortages just before shipment

**Defense points:**

- Final reconciliation of formulation × label and retention of process logs
- Restricted entry + monitoring deployment + seal control
- Witnessed final inspection and verification of seal numbers

Note: Intentional label substitution is a serious Food Defense threat because discrepancies between contents and labeling may result in health harm, such as allergen exposure, and can lead to difficult or incorrect recalls. Although this overlaps with economically motivated fraud, the focus here is on the defensive function of stopping incidents or attacks at the final process.

**7) Logistics, Warehousing, Cold Chain, and Returned Containers**

Possible acts include opening or injection during transport, opening of cartons or substitution of contents at external warehouses, and intentional temperature deviation causing quality deterioration.

**Vulnerabilities likely to attract attackers:**

- Unmonitored periods during transport
- Failure to verify seals or address inventory discrepancies at external warehouses
- Lack of suitability assessment for returned containers

**Defense points:**

- Seal number verification + stop/opening logs + location/temperature records
- Access control, monitoring, and routine reconciliation of inventory discrepancies
- Acceptance judgment for returned containers (verification of cleaning records and immediate disposal of nonconforming containers)

**8) Retail, Markets, Events, and E-commerce (Public-Facing Environments)**

Possible acts include opening displayed items and inserting foreign materials, surface contamination of tasting samples, and insertion of foreign materials into e-commerce packages.

**Vulnerabilities likely to attract attackers:**

- Insufficient patrols during peak periods
- Unprotected surfaces of tasting items and displayed products
- Unclear accountability in e-commerce packaging operations

**Defense points:**

- Layout and blind spot design, plus monitoring deployment
- Shelf sealing / seal control / management of evidence of opening
- Immediate isolation → notification → recording of abnormal products

**9) Mass Catering and Peak-Demand Periods (Seasonal Demand / School Meals)**

Possible acts include contamination of large kettles or large lots, contamination just before serving, and misdelivery caused by labeling or changeover errors (including allergen contamination).

**Vulnerabilities likely to attract attackers:**

- Omission of checks due to staff shortages or deployment of new personnel
- Broad impact of large kettles and large lots
- Weak control of temporary lines

**Defense points:**

- Peak-period controls (temporary training, simplified procedures, focused inspection)
- Blocking of serving routes and mutual verification
- Verification of effectiveness using KPIs such as initial response time and recall rate

**10) Misuse of Waste and Rework (Reintroduction)**

Possible acts along disposal and return routes include diversion of discarded products, repackaging and reintroduction, unauthorized reintroduction of returned products, and tampering with disposal records.

**Vulnerabilities likely to attract attackers:**

- Unattended time periods during disposal
- Formalized records with insufficient supporting evidence such as photographs
- Complete dependence on contractors

**Defense points:**

- Strict operation of witnessed disposal and recordkeeping
- Blocking of return routes and dual approval for re-entry into inventory
- Audits of disposal contractors

**Note:** Reintroduction or repackaging of discarded products is an area where “fraud-like” intent, such as cost reduction, and harmful acts, such as intentionally distributing expired or deteriorated products, can easily overlap. Here it is treated as a Food Defense target from the perspective of intentional harm and supply chain disruption through misuse of disposal routes.

**11) Reliability of Testing and Data**

Possible acts during testing and inspection include sample substitution, tampering with test results or logs, and falsification or substitution of test reports.

**Vulnerabilities likely to attract attackers:**

- No signatures or seals at handover
- Single-person editing rights for data
- Weak oversight of outsourced laboratories

**Defense points:**

- Audit trails (revision history and access logs)
- Deterrence through switching or duplication of laboratories

**Note:** Falsification or tampering of inspection data can represent both fraud through substitution of pass/fail results and a Food Defense weakness that conceals abnormalities and leads to the manifestation of harm.

**12) Tampering with a Tasting Corner (Aimed at Social Media Spread)**

A visitor at a tasting stand in a commercial facility smeared something resembling a foreign substance on the surface of bread, filmed it, and posted it online. Complaints of “foreign material contamination” followed, though no health harm occurred.

**Vulnerabilities likely to attract attackers:**

- Unattended tasting stands; exposed serving; unclear rules

**Defense points:**

- Serve with lids or as individually wrapped items, with staff always present
- Post notices such as “Filming permitted / contact with food prohibited”
- If a concern arises, immediately isolate, record, and initiate social media response

**3. Scenario Analysis and Evaluation Methods**

**Scenario Analysis (Impact, Accessibility, Detectability)**

This method evaluates each scenario on a five-point scale for three elements: impact, accessibility, and detectability, and calculates the RPN (Risk Priority Number). This enables the threat level of each scenario to be understood, and scenarios assessed as severe can then be subjected to more detailed evaluation using methods such as KAT or CARVER+Shock.

Reference: *Mitigation Strategies to Protect Food Against Intentional Adulteration: Guidance for Industry*

https://www.fda.gov/media/113684/download

**KAT (Key Activity Types) Method**

KAT is a preliminary assessment method used in the FDA's Intentional Adulteration approach. It efficiently and reproducibly identifies activities or process steps within the overall manufacturing operation that could result in significant public health impact or wide-ranging harm if intentional contamination occurred. After identification, the method can be used to support more detailed assessment using CARVER+Shock or the consideration of mitigation strategies, as well as to determine resource allocation and response priorities.

Reference: *Mitigation Strategies to Protect Food Against Intentional Adulteration: Guidance for Industry*

https://www.fda.gov/media/113684/download

**Threat Assessment Method: CARVER+Shock**

CARVER+Shock is a method for evaluating vulnerabilities in process steps and facilities from multiple perspectives and supporting the prioritization of threats and the development of defense measures.

- It can be used to evaluate in detail specific process steps, such as high-threat activities identified through KAT.
- Vulnerabilities are scored using multiple indicators, and mitigation measures are selected and implemented systematically according to priority.

Reference: *FDA CARVER+SHOCK PRIMER*

https://www.fda.gov/food/food-defense-initiatives/carver-shock-primer

**Threat Assessment Using MAFF Checklists**

Checklist-based evaluation is a method for clarifying potential threats and vulnerabilities by setting specific checkpoint items under major and subcategories such as organizational management, human factors (employees and outsiders), facility management, and operations.

References:

- *Checklist for Preventing Intentional Food Contamination in Food Factories*
  https://www.maff.go.jp/j/syouan/seisaku/kiki/attach/pdf/index-7.pdf
- *Checklist for Preventing Intentional Food Contamination in Food Logistics Facilities*
  https://www.maff.go.jp/j/syouan/seisaku/kiki/attach/pdf/index-8.pdf

**Threat Assessment Based on Nara Medical University Department of Public Health Materials and the Food Defense Guidelines**

This is a method of evaluation based on comparison of the organization's situation against the Food Defense Guidelines. It considers priority and feasible measures to reduce threats of intentional

contamination across such areas as the organization, employees, outsiders, facility management, and inbound/outbound logistics management.
Reference: *Food Defense Guidelines (for Food Manufacturing Plants), FY2023 Edition*
https://hpm.naramed-u.ac.jp/pdf/fd_guideline/r5_gl_food-manufacturing.pdf

**Support for Developing Mitigation Strategies (Using FDMSD)**
FDMSD (Food Defense Mitigation Strategies Database) is an FDA-provided database of Food Defense mitigation measures. It can be used to systematically introduce mitigation strategies for high-threat process steps identified through CARVER+Shock or similar methods.

- Mitigation strategies are categorized into areas such as physical barriers, access control, employee training, and strengthened procedures.
- It also presents implementation procedures and points to note according to the type of food, process, and threat.
- By checking and improving the status of applying mitigation measures to each process step based on evaluation examples, the effectiveness of the Food Defense Plan can be enhanced.

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

**Appendix: Food Defense Plan [Template]**
Issue Date: _____ / _____ / _____
Version: _____
Prepared by: _____ (Position: _____)
Approved by: _____ (Position: _____)

**1. Purpose and Scope**

**1.1 Purpose**

The purpose of this Plan is to reduce **Food Defense risks**, including intentional contamination, adulteration, and acts of sabotage, and to ensure the safety and trust of consumers and business partners.

**1.2 Scope (to be completed)**

- Covered process steps:
  Example: receipt of raw materials / production / packaging / storage / shipment / logistics, etc.
  → (  )
- Covered facilities:
  Example: plant, packaging material warehouse, outsourced warehouse, shared logistics center, etc.
  → (  )
- Covered external parties (if applicable):
  □ Contract manufacturer (OEM)
  □ External logistics provider
  □ External testing laboratory
  □ Other: (  )

*Add or delete items as appropriate to reflect the actual circumstances of the company.*

**2. Responsibility Structure**

| Category | Name | Department / Site | Role | Main responsibilities (summary) |
|---|---|---|---|---|
| Food Defense Officer (site / plant) | | | Overall control | - Establish and communicate the Food Defense policy<br>- Lead the threat assessment and the development / review of this Plan |
| Alternate (site / plant) | | | Acts in the absence of the responsible person | - Direct initial emergency response<br>- Coordinate reporting and communication |
| Department Manager (Production) | | Production Department | Operation within the department | - Operate and inspect zoning, access control, and defensive measures on the production line |

| | | | | |
|---|---|---|---|---|
| Department Manager (Quality Assurance) | | Quality Assurance Department | Operation within the department | - Operate and inspect defensive measures relating to testing, records, label control, etc. |
| Department Manager (General Affairs / Facilities) | | General Affairs / Facilities | Physical defense | - Operate and manage locks, surveillance cameras, patrol inspections, etc. |
| Head Office Food Defense Lead (if applicable) | | (Head Office Quality / Food Safety Department, etc.) | Oversight and support | - Approve major incidents and oversee external response<br>- Horizontally deploy lessons learned between sites and chair the annual review |
| OEM / External Logistics Management Contact | ( ) | (Purchasing / SCM / Logistics, etc.) | Control of external parties | - Contract requirements, audits and corrective action follow-up, confirmation of seal control, access control, and record management |

Reporting flow (example / revise for company use):
Person who identifies the issue → Department Manager → Food Defense Officer (site / plant) → Plant Manager / Site Manager → (if necessary) Head Office Food Defense Lead → Senior Management / Corporate Communications and Legal

- Cases involving a suspected intentional act or shipment suspension shall be reported immediately to the Head Office Food Defense Lead.

**3. Threat Assessment Results and Countermeasures (Summary)**

**3.1 Assessment Method (to be completed)**

- Assessment targets:
  □ Receipt of raw materials
  □ Production
  □ Packaging
  □ Storage
  □ Shipment / Logistics
  □ Information management
  □ Packaging materials / Labels
  □ Waste handling
  □ OEM / External logistics
  □ Other ( )
- Assessment axes (example):
  - Severity of impact: High / Medium / Low
  - Ease of execution: High / Medium / Low

- Priority determination:
  Based on severity of impact × ease of execution, determine the priority as:
  □ High □ Medium □ Low etc.

**3.2 Assessment Results (summary form to be completed)**

| Process / Area | Potential Threat | Priority (High / Medium / Low, etc.) | Main countermeasure policy (summary) |
|---|---|---|---|
| (Example: Receipt of raw materials) | (Example: Unauthorized contamination / substitution of raw materials) | | |
| (　　) | | | |
| (　　) | | | |
| (　　) | | | |

*Detailed assessments shall be managed separately in the "Threat Assessment Sheet."*

**4. Implementation Measures (Specific Controls)**

**4.1 List of Control Policies (to be completed)**

| Item | Implementation measure | Responsible department | Supplementary notes |
|---|---|---|---|
| ① Responsibility structure | (Example: Prepare organizational chart and contact network, and document alternates and reporting routes) | (Quality Assurance / Head Office Quality, etc.) | (Reviewed once a year, etc.) |
| ② Access control | (Example: Access control by zoning level, retention of entry/exit records) | (General Affairs / Engineering, etc.) | (Two-factor authentication for high-risk areas, etc.) |
| ③ Control of raw materials, packaging materials, products, and data | (Example: Reinforce receipt, storage, disposal, and record procedures with intentional acts also in mind) | (Production / Quality Assurance / Purchasing / IT, etc.) | (Strengthened checks for high-risk items, etc.) |
| ④ Physical defense | (Example: Incorporate locking, surveillance cameras, and patrol inspections into routine operations) | (General Affairs / Facilities / Site) | (Video retention period:<br>Medium-risk = ___ days<br>High-risk = ___ days, etc.) |
| ⑤ Response to abnormalities | (Example: Establish procedures for "reporting → isolation → preservation of evidence → investigation → correction / corrective action") | (All departments) | (Explicit inclusion of the perspective of suspecting intentional acts, etc.) |
| ⑥ Recall response | (Example: Conduct exercises ___ times per | (Quality Assurance / Corporate | (Training record format, |

| | | | |
|---|---|---|---|
| | year, including scenarios involving intentional contamination and label tampering) | Communications / Legal, etc.) | standardization of communication with authorities and customers, etc.) |
| ⑦ Training and exercises | (Example: Once a year for all personnel, twice a year for personnel responsible for critical process steps, etc.) | (Quality Assurance / Human Resources, etc.) | (Training records, use of e-learning, etc.) |

*Delete unnecessary rows and add any items needed for your company.*

**5. Verification and Review**

- Regular review
  Frequency: ___ times per year (example: once a year, every _____)
  Person responsible: ( )

Review items (example / revise as necessary):

  - Appropriateness of the threat assessment results and countermeasures
  - Operational status of access records, seal records, surveillance camera footage, etc.
  - Number of reports, implementation status of correction / corrective action
  - Results of mock recalls and exercises, etc.

- Ad hoc review
  An ad hoc review shall be conducted promptly when any of the following occurs:
  - Emergence of new threats, social incidents, or regulatory observations
  - Equipment changes, organizational restructuring, or major process changes
  - Occurrence of major complaints, incidents, or abnormal events, etc.

**6. Document and Record Control**

- For this Plan
  □ Clearly record the revision date, revised content, reason for revision, and approver
  □ Manage the latest version in either paper or electronic form so that relevant personnel can access it immediately
- Main related records (examples / add as necessary)
  □ Access control records
  □ Seal number management logs and opening records
  □ Surveillance camera footage (retention period: High-risk ___ days / Medium-risk ___ days, etc.)
  □ Training and exercise records
  □ Records of abnormalities, reports, and corrective action
  □ Audit records and corrective action follow-up records for OEMs / external logistics providers

Retention period (guideline)

- Records equivalent to Medium-risk: _____ years
- Records equivalent to High-risk: _____ years
- (Set and specify according to company standards)

**7. Appendices and Reference Information**

Appendix 1: Threat Assessment Sheet
Appendix 2: Recall Response Procedure
Appendix 3: Training and Exercise Plan / Records
Appendix 4: Site-Specific Appendices (zoning maps, differences in access policies, etc.)
Reference: Items for possible future introduction
(Example: electronic record systems, serialization of seals, strengthening of logistics traceability, etc.)



**Disclaimer**：This translated document is provided for information purposes only. In the event of a difference of interpretation or a dispute, the original Japanese version of this document is binding.