戦略的イノベーション創造プログラム(SIP)／
重要インフラ等におけるサイバーセキュリティの確保／
(b3) 評価検証プラットフォーム技術
「セキュリティ対策適用ガイドライン」

サイバー攻撃から重要インフラを守る

－ セキュリティ製品導入のための手引き －

2020 年 1 月

株式会社 日立製作所

本ガイドラインについて

本ガイドラインは、内閣府が進める「戦略的イノベーション創造プログラム(SIP)／重要インフラ等におけるサイバーセキュリティの確保／(b3) 評価検証プラットフォーム技術」の研究を通して得られた成果を基に、重要インフラ事業者がセキュリティ対策を適用する際に考慮すべき点を記載した。

重要インフラ事業者がセキュリティ対策を適用するためには、従来の情報システムでのセキュリティ対策における注意事項に加えて、既存の制御システムに影響を与えないように注意するなどの制御システムの特徴に合わせた検討も必要である。そこで、「(b3) 評価検証プラットフォーム技術」の研究では、「設計フェーズ」、「構築フェーズ」、「運用フェーズ」の各フェーズでの制御システム向けの具体的な実施内容を順次検討した。まず初めに、「設計フェーズ」では、対象システムを特定するための手法を検討し、新しい分析手法である「事業レベルでのリスク分析手法」を考案した。次に、「構築フェーズ」では、セキュリティコア技術の一つである「戦略的イノベーション創造プログラム(SIP)／重要インフラ等におけるサイバーセキュリティの確保／(a2) 制御・通信機器および制御ネットワークの動作監視・解析技術」で研究開発した成果を適切に現場に適用させるための評価検証の環境構築や、その検証環境を用いた評価検証を実施した。さらに、「運用フェーズ」では、重要インフラ事業者に適したセキュリティ組織の立ち上げやセキュリティ運用に関しても検討し、事業者に対する支援等を実施してきた。

本ガイドラインは、これらの検討内容を基に、重要インフラ事業者がセキュリティ対策を適用する場合に考慮すべき点について、従来のセキュリティ規格やガイドライン等では示されていない具体的な実現方法を記述し、重要インフラ事業者におけるセキュリティ対策導入を後押しすることを目的とする。

本研究の一部は，内閣府が進める戦略的イノベーション創造プログラム（ＳＩＰ）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されました。

目次

1章　背景・目的

1.1 背景

鉄道、電力、水道、ガスといった社会インフラを支える重要インフラ[1]システムは、ネットワークや装置への汎用技術の取り込みや、情報システムとの接続の増加に伴い、情報システムと同様のセキュリティ対策が求められてきている。近年、制御システムを狙ったサイバー攻撃の事例は国内外で増加傾向にあり、重要インフラシステムをターゲットにした攻撃も発生している（表 1）。重要インフラシステムで何らかの障害が発生した場合、死亡事故や環境汚染といった大きな影響を及ぼす恐れがあるため、セキュリティ対策を不可欠なものとして確実に実施していく必要がある。

表 1：近年のサイバー攻撃脅威事例

発生時期	分野	発生国・地域	ターゲット	被害および対応
2012年 8月15日	エネルギー （石油）	サウジアラビア	国営石油会社	・サイバー攻撃により30,000台のワークステーションが停止および破壊。 ・攻撃後の緊急措置として会社を完全にオフライン化。あらゆる業務は紙の書類を使い手作業。 ・石油販売を一時停止のち、17日後に無償提供を開始。
2013年 3月20日	放送 （テレビ）	韓国	民間企業	・テレビ局と銀行合わせて6社の社内システムがサイバー攻撃を受け、約3万2000台のPCやサーバーがダウンまたは再起動不可となった ・テレビ局の停止は回避、銀行のATMの使用が一部不可となる ・ある日時になるとウイルス対策ソフトを停止後、HDへの無意味なデータの上書き・消去を繰り返しデータを破壊するマルウェアが使用された
2014年 3月-8月	交通 （地下鉄）	韓国	公営企業	・サイバー攻撃により、5か月の間に58台のPCが悪意あるソフトウェアをインストールされる ・攻撃者は列車を制御しているシステムを収容するネットワークには到達することができず、いくつかの文書を盗んだのみで被害は小さい
2015年 12月24日	エネルギー （電力）	ウクライナ	電力会社	・電力会社がサイバー攻撃を受け、約6時間停電 ・同時に、コールセンターに電話が鳴り続け、顧客対応を妨害 ・同時に報道機関などへもサイバー攻撃
2016年 11月25日	交通 （鉄道）	アメリカ サンフランシスコ	市交通局	・約 900台のオフィスコンピュータがランサムウエアに感染 ・感染後2日間、地下鉄の券売機とゲートを停止し、運賃を無料化
2017年 7月	エネルギー （電力）	アメリカ	州電力運営会社	・情報システム系ネットワークがハッキングされる ・制御系システムに侵入された痕跡はなし
2018年 10月	ライフライン （水道）	アメリカ	州水道当局	・ランサムウェアに感染 ・運用やサービスに影響はなし

システムに対してセキュリティ対策を適用するには、図 1に示すような「設計」、「構築」、「運用」のライフサイクル全般での検討が必要となる。

具体的には、設計フェーズでは、事業レベルで想定すべきリスクを認識し対策が必要と判断したシステムに関して詳細なリスク分析および対策立案を実施し、適切で抜け漏れないセキュリティ対策を設計する。このような設計の考え方に関しては、重要インフラシステムを支える産業制御システム向けセキュリティ標準規格[i]や行動計画[ii]で要求されている。構築フェーズでは、設計フェーズで導入を決定したセキュリティ装置等を、既存のシステムに影響を与えないよう十分な事前検証等を実施したうえで、実際の環境に導入する必要がある。また、運用フェーズでは、セキュリティに関する迅速な意思決定等を行うための組織構築と、具体的な運用ポリシーや手順を決定し、それに従い運用する必要がある。

---

[1] 機能の停止や低下が起きると、国民生活や経済活動で大きな混乱が予想されるインフラのこと。政府は情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の 14 を重要インフラ分野と位置づけている[ii]。

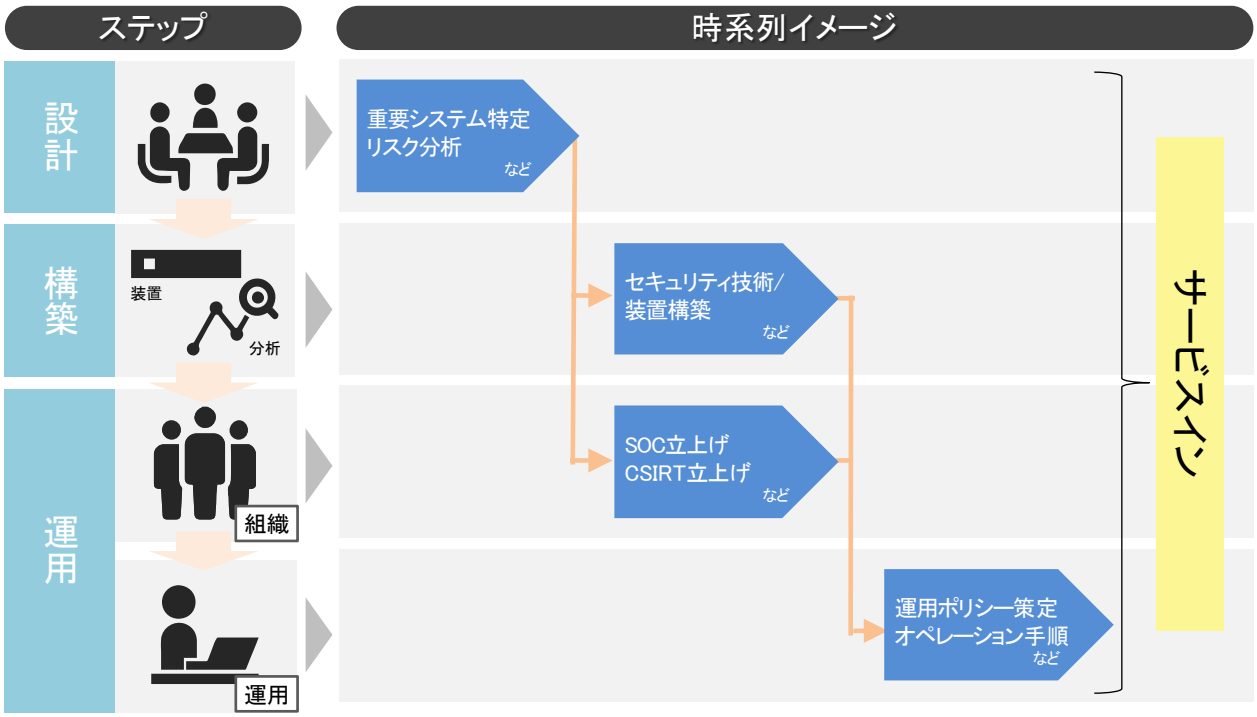

図 1：セキュリティ対策の導入ステップ

1.2 ガイドラインの目的

図 2 に、重要インフラシステムに実施すべき制御システムのセキュリティ対策に関連する規格・ガイドラインの概要を示す。なお、セキュリティに関する規格はこれら以外にも多々あり、以降の文中で必要に応じて紹介する。

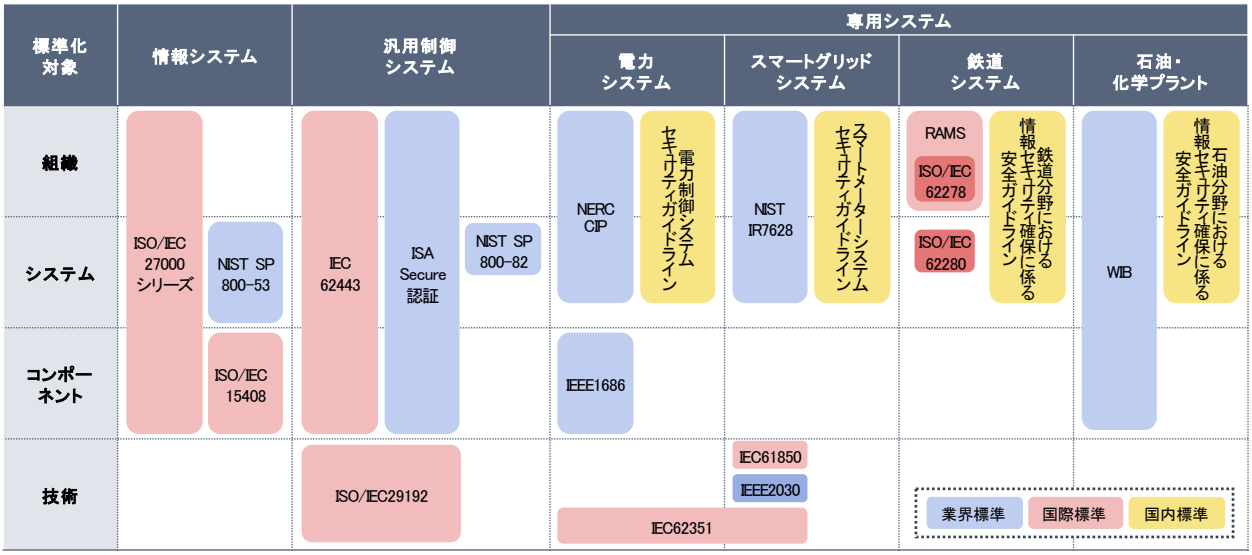

図 2：制御システムのセキュリティ向け規格・ガイドライン

図 2 にある規格・ガイドラインには、セキュリティ対策立案に対する要件や実施の考え方に関するものは多く見られるが、それを実現するための具体的な方法を示しているものは少ない。このため、セキュリティ対策は設計者のノウハウに依存した結果となってしまう恐れがある。

以上のような背景から、本ガイドラインでは重要インフラシステム等の制御システムにセキュリティ対策を適用する際の具体的な実現手法（重要ポイント、注意点、手順の具体化等）を示し、事業者のスムーズなセキュリティ対策導入を支援することを目的とする。

1.3 対象とする重要インフラの特徴

重要インフラシステムでは、事業全体に対するサイバーセキュリティリスクを正しく認識し、適切なセキュリティ対策を実施する必要がある。しかし、重要インフラシステムは事業規模が大きく、事業を構成する業務／システムも多種多様であるため、事業全体のリスクを網羅的に把握するのが困難である。さらには、重要インフラ事業は多数の事業と連携するため、他事業との依存関係を考慮したリスクの把握が必要であるが、他事業との複雑な依存関係の把握も困難である。また、これまでの各世代で導入された既存システムが入り混じっており、加えて機能の性質上可用性重視でサービスを止められないため、元のシステムに特別な加工を施すことなく追加する形（ボルトオン）でのセキュリティ対策適用が必須である。本ガイドラインでは、上記のような特徴を踏まえ、重要インフラシステム事業者が特に注意すべき点を記述する。

1.4 対象読者

本ガイドラインは、重要インフラ事業者を対象としている。セキュリティ対策の適用に関する決定権を持つ経営者、および導入作業を行う現場の運用者の両者を対象としている。また、重要インフラ事業者にシステムを納める SI ベンダも対象となり得る。

1.5 ガイドラインの全体構成

本ガイドラインの構成は次の通りである。

2 章では、設計フェーズにおける重要インフラシステム等の制御システムを対象とした事業レベルでのリスク分析の手法を示す。3 章では、構築フェーズの事前準備段階におけるセキュリティ対策をどのような構成・手順で導入するか説明する。4 章では、導入段階におけるセキュリティ装置導入時に必要となる準備および作業を、また 5 章では確認段階における導入の完了確認作業について説明する。最後に 6 章では、運用フェーズにおけるセキュリティ装置を導入した対象システムのセキュリティ脅威の監視、インシデント発生前の事前対処や発生時の迅速な対応について説明する。

2章　設計フェーズ

図 3 に、システムのセキュリティ設計の大まかな流れを示す。まず、事業レベルでのリスク分析で事業全体のうち優先的に対策すべき業務／システムを決定し、次にその部分に詳細リスク分析を実施して脅威の洗い出しおよびリスク評価を行い、その結果に基づき対策を立案する。本章では、これらの作業について説明する。

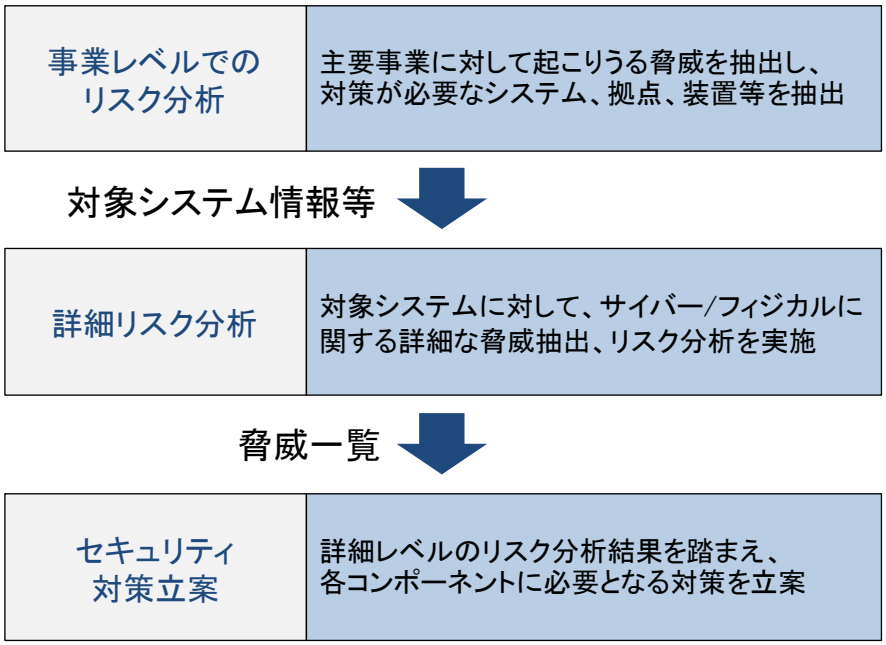

図 3：セキュリティ設計の流れ

2.1　事業レベルでのリスク分析（重要インフラシステムの特定）

重要インフラシステムを支える産業制御システム向けセキュリティ標準規格 IEC62443-2-1 では、事業レベルで想定すべきリスクを認識し、対策が必要と判断したシステムに関して詳細なリスク分析および対策立案を実施することが定められている。また、重要インフラ向け行動計画[ii]では、リスクマネジメントを踏まえた対処態勢の整備の推進として、リスク分析や事業継続計画の策定が要求されている。

しかし、重要インフラシステムは事業規模が大きく、事業を構成するシステムも多種多様であるため、事業全体のリスクを抽出し、それらを俯瞰したうえで優先的に対策すべき業務／システムを把握することが必要となってくる。この実現手段として、本ガイドラインでは事業レベルでのリスク分析について説明する。

2.1.1 事業レベルでのリスク分析の実施内容

本節では、重要インフラシステム等の制御システムにセキュリティを適用する具体的な実現手法を示した事業レベルでのリスク分析[iii][iv]の手順について説明する。これは対策を施すべき箇所に優先

順位をつけたうえで行う新しいリスク分析手法であり、「戦略的イノベーション創造プログラム(SIP)／重要インフラ等におけるサイバーセキュリティの確保／(b3) 評価検証プラットフォーム技術」で考案した。

［ステップ 1］対象事業のモデル化

この後のステップで必要となる対象事業の情報を整理する。

ステップ 1-1. 主要事業のモデル化…入出力や構成要素を抽象化し事業をモデル化する

ステップ 1-2. 事業外モデルの構築…事業同士の依存関係をモデル化する

ステップ 1-3. 事業内モデルの構築…事業内業務の依存関係をモデル化する

［ステップ 2］事業リスク抽出

対象事業のリスクを洗い出す。リスクの種類は以下の通り。

・事業外リスク…事業が生成する出力によって他者、他組織、環境等に悪影響を及ぼすリスク

・事業内リスク…事業を構成する要素（人、システム、装置等）に悪影響を及ぼすリスク

ステップ 2-1. 事業外リスクの抽出…意図しない状況と事業外に及ぼす悪影響を抽出する

ステップ 2-2. 事業内リスクの抽出…意図しない状況と事業内に及ぼす悪影響を抽出する

［ステップ 3］リスクレベルの見積り

ステップ 2 で抽出した事業リスクの影響の大きさを評価する。リスクを抽出し影響レベルを定義したうえで、リスクレベルを決定する。

［ステップ 4］事業リスク要因検討

事業リスクと周辺事業や事業内業務との関係性を明確化し、詳細分析を行うべき対象を明らかにする。各事業リスクについて要因として挙がる回数の多い周辺事業および事業内業務が、次の詳細分析を行うべき対象として優先度が高いものとする。

2.1.2 事業レベルでのリスク分析における重要ポイント

事業レベルでのリスク分析で、特に考慮すべきポイントを記載する。

表 2：事業レベルでのリスク分析における重要ポイント一覧

#	タイトル	関連ステップ
重要ポイント1.	優先的に対策すべき業務/システムの把握	ステップ1～4

重要ポイント１： 優先的に対策すべき業務／システムの把握

（１）ポイント

セキュリティ対策をシステムに導入する場合、事業レベルでのリスク分析により優先的に対策すべき業務やシステムを把握したうえで実施することが必要である。

（２）解説

重要インフラシステムは、事業規模が大きく、事業を構成するシステムも多種多様であるため、すべての業務／システムへのセキュリティ対策やその準備のためのリスク分析を実施することは困難である。そこで、事業レベルでのリスク分析により優先的に対策すべき業務／システムを把握することが必要となる。

事業レベルでのリスク分析の流れは以下の通り。

ステップ 1. 対象事業のモデル化　…この後のステップで必要となる対象事業の情報を整理する
ステップ 2. 事業リスク抽出　…対象事業のリスクを洗い出す
ステップ 3. リスクレベルの見積り　…ステップ 2 で抽出した事業リスクの影響の大きさを評価する
ステップ 4. 事業リスク要因検討　…事業リスクと周辺事業や事業内業務との関係性を明確化し詳細分析を行うべき対象を明らかにする

（３）実施例

■ステップ 1. 対象事業のモデル化

本ステップは、リスク抽出およびレベル見積り（ステップ 2.、3.）に必要な対象事業の情報を整理することを目的とする。本ステップは以下の様にさらに細分化されたステップから構成される。

ステップ 1-1. 主要事業のモデル化
ステップ 1-2. 事業外モデルの構築
ステップ 1-3. 事業内モデルの構築

それぞれの詳細は、以下の通り。

ステップ 1-1. 主要事業のモデル化

本手法では、品質マネジメント[2]の技法である 4M[3]に基づき、入出力や構成要素を抽象化し事業を図 4 のように図でモデル化する。

---

[2] 対象に本来備わっている特性の集まりが要求事項を満たす程度について、組織を指揮し管理するための調整された活動。JIS Q9000:2015 「品質マネジメントシステム－基本及び用語」-「3.3.4 品質マネジメント」参照。

[3] Man、Machine、Material、Method を指す。品質マネジメントでは、不良発生時の状況を示す情報の管理によく使われる要素のセット。

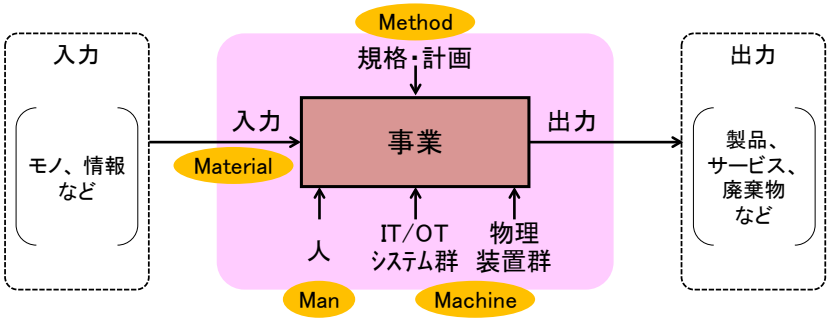

図 4：主要事業モデル

事業は事業者外からの入力（原料等のモノ、情報等）を用い、出力（製品・サービス、廃棄物等）を他者に対して提供する。また、入力と出力の他に、事業を実施するうえで必要な人、IT/OT システム、物理装置や、事業を実施するうえで従うべき規格・計画から構成される。なお、この事業モデルは経済産業省発行の”サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）”[v]中でも参照されている。

本ステップでは、分析対象の事業に関するこれらの構成要素を具体的に明確化する。図 5 に、原材料から供給物質を生成する事業を主要事業と想定した、事業モデル例を示す。ここでは、図 4 に示す構成要素（入力、出力、規格・計画、人、IT/OT システム群、物理装置群）に当たるものを具体的に挙げる。

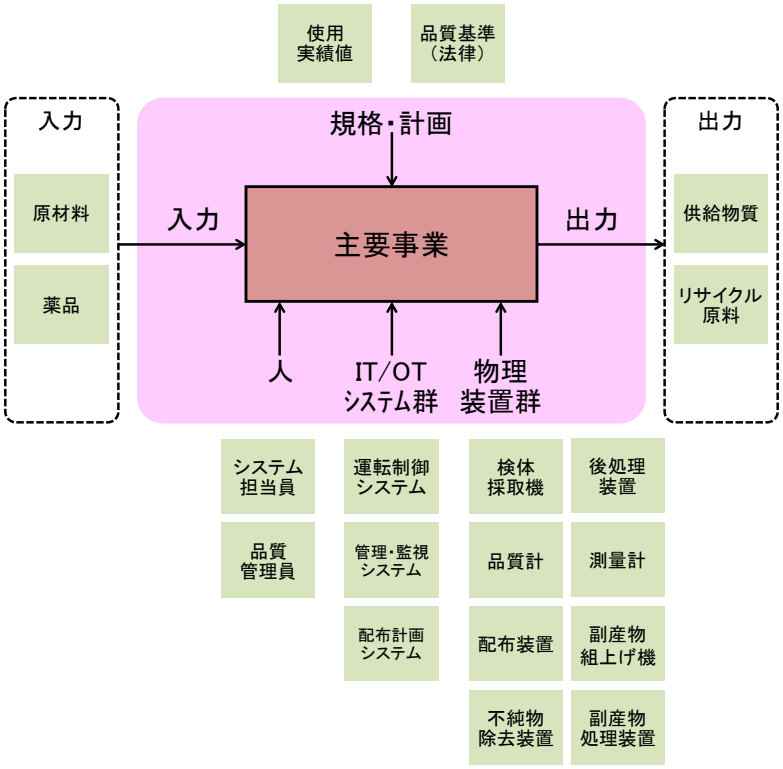

図 5：主要事業の事業モデル例

ステップ 1-2. 事業外モデルの構築

本手法では、事業の各構成要素は他の事業の出力から導かれると想定し、入力要素（「規格・計画」「入力」「人」「IT/OT システム群」「物理装置群」）が生成されターゲット事業に届くまでの事業同士の依存関係を「事業外モデル」として図 6 に示す図でモデル化する。

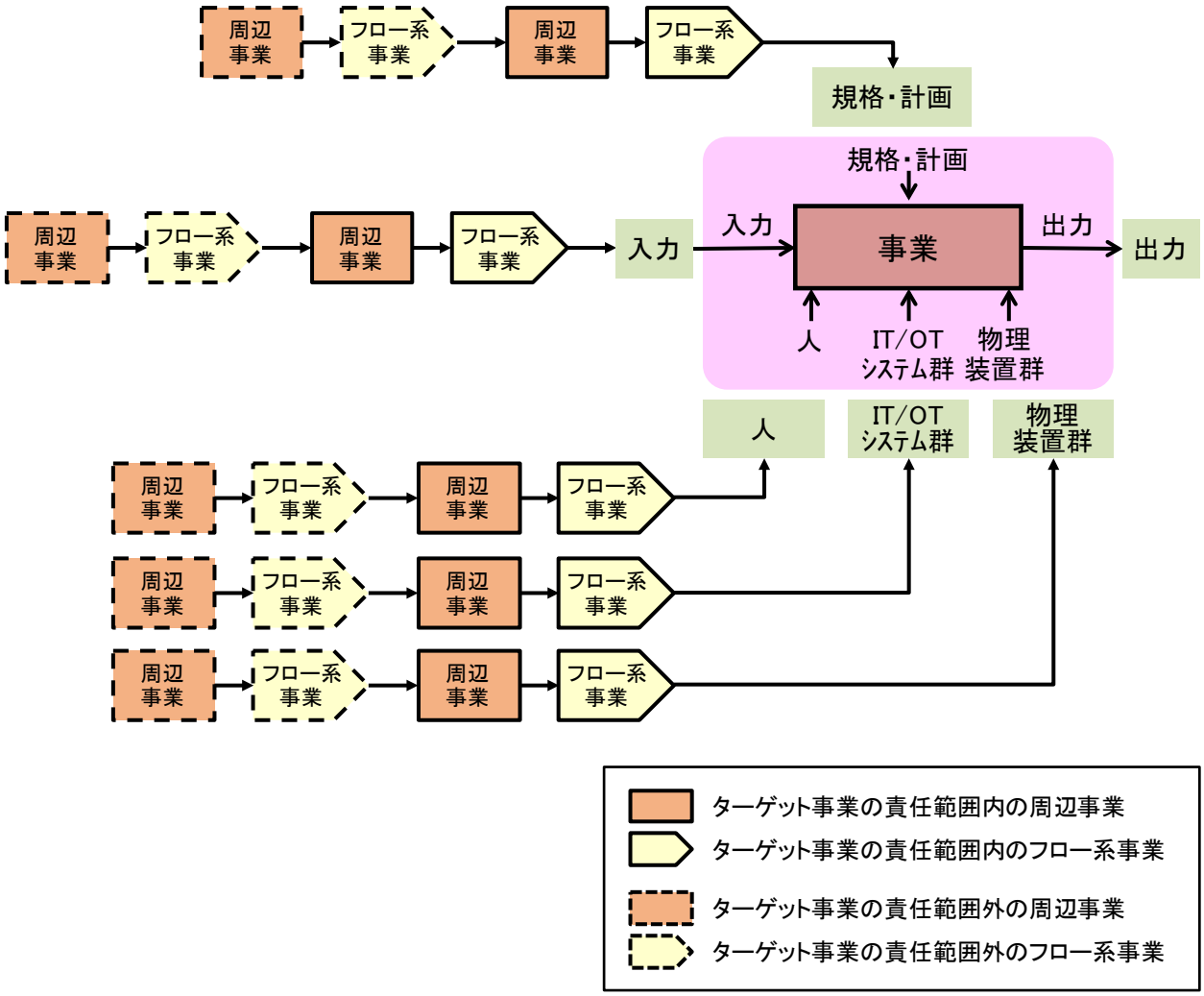

図 6：事業外モデルの概要

本ステップでは、入力を生成する事業を「周辺事業」、周辺事業の出力の運輸や伝達を行う事業を「フロー系事業」としてターゲット事業の入力要素をたどり、事業外モデルを構築する。周辺事業だけでなくフロー系事業も考慮に入れて分析を行うことで、例えば社内 IT 環境等の運営が止まれば主要事業の停止につながりかねない重要な事業に関するリスクについても評価できる。なお、ターゲット事業の責任範囲外である事業は破線で表す。図 7 に、主要事業の事業外モデルの例を示す。

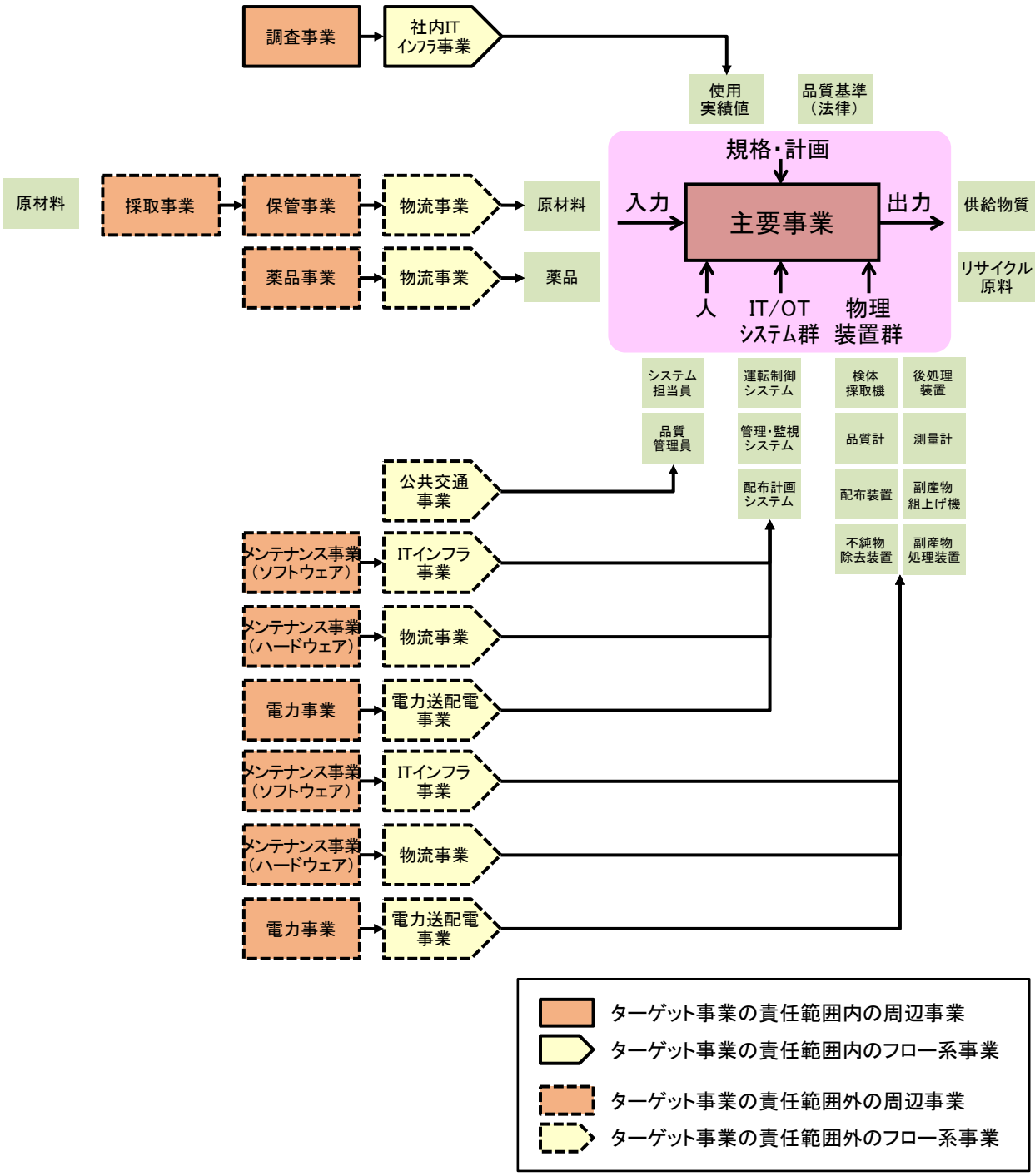

図 7：主要事業の事業外モデル例

ステップ 1-3. 事業内モデルの構築

本手法では、事業は内部に業務を保有しており、これらも事業と同様のモデルで表現可能と想定し、事業外モデルと同様に互いの依存関係を「事業内モデル」として図 8 に示す図でモデル化する。

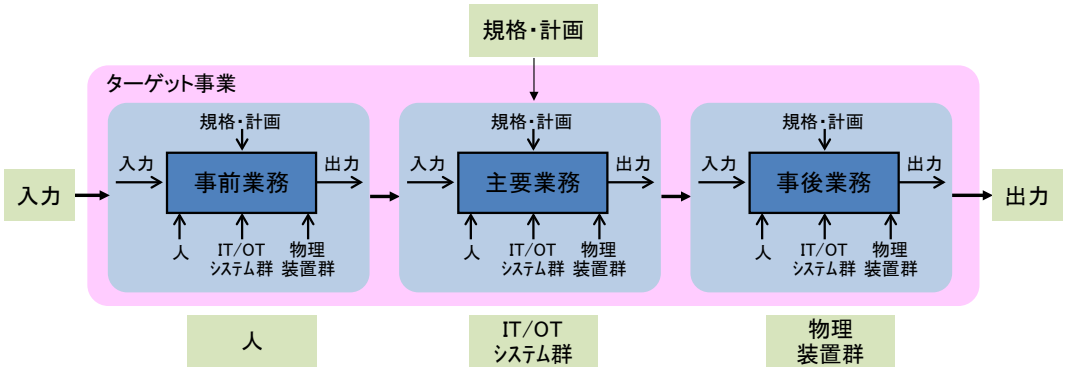

図 8：事業内モデルの概要

本ステップでは、ターゲット事業内の各業務を事前業務・主要業務・事後業務の観点で洗い出し、フロー系事業を除く形で事業外モデルと同じように依存関係を明確化して事業内モデルを構築する。図 9 に主要事業の事業内モデルの例を示す。

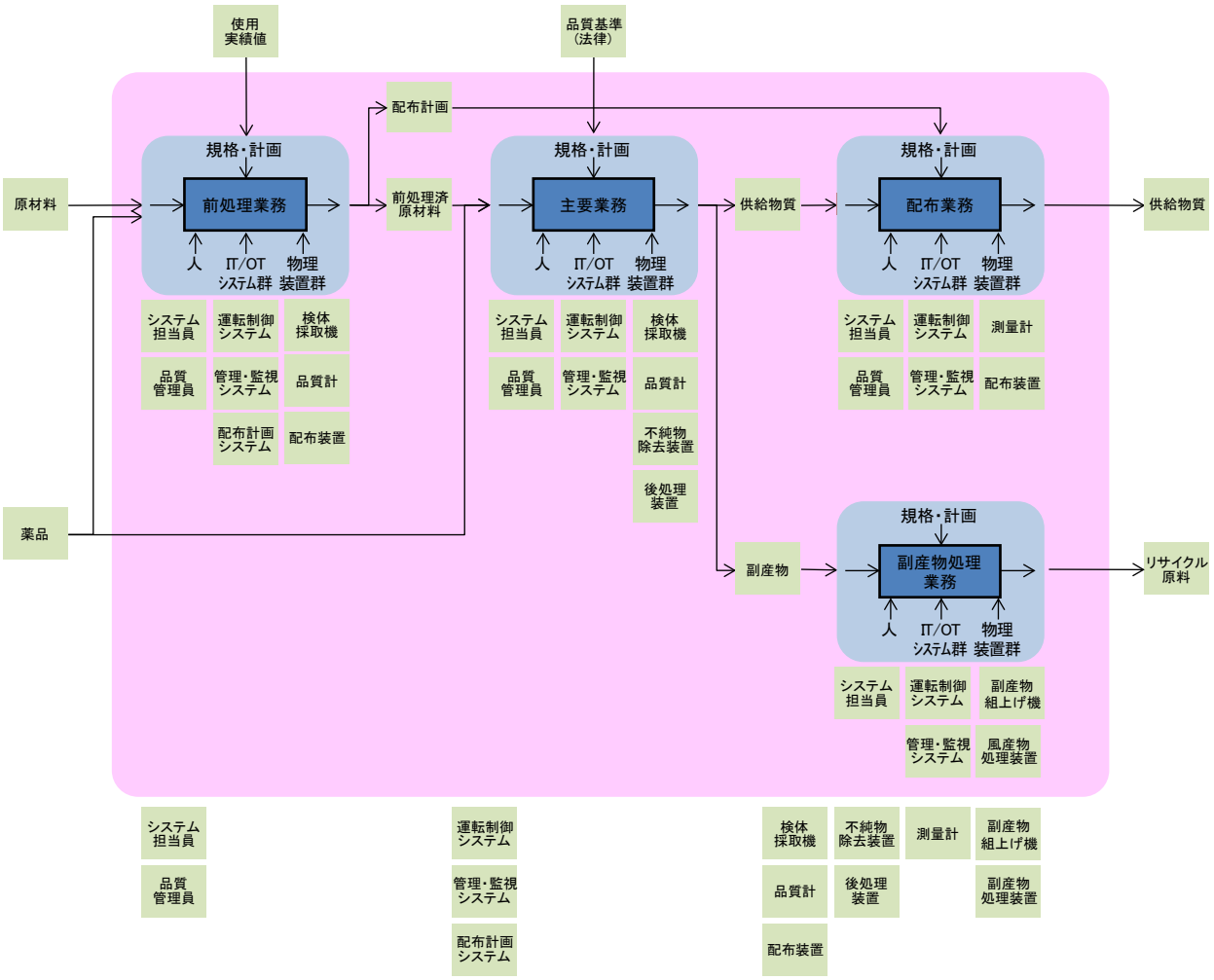

図 9：主要事業の事業内モデル例

■ステップ 2. 事業リスク抽出

本ステップは、対象事業のリスクを洗い出すことを目的とする。まず、本手法で抽出するリスクの種類および抽出の観点について述べる。

本手法では、事業外リスクおよび事業内リスクの 2 つを定義し、各事業に対しこれらのリスクの抽出を行う。2 つのリスクの定義は以下の通りとする。図 10 および図 11 にそれぞれの概要を示す。

・事業外リスク

…事業が生成する出力によって他者、他組織、環境等に対して悪影響を及ぼすリスク

・事業内リスク

…事業を構成する要素（人、システム、装置等）に対して悪影響を及ぼすリスク

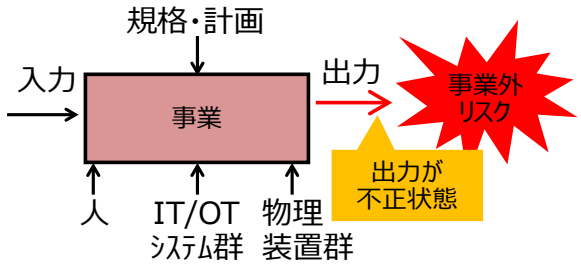

図 10：事業外リスクの概要

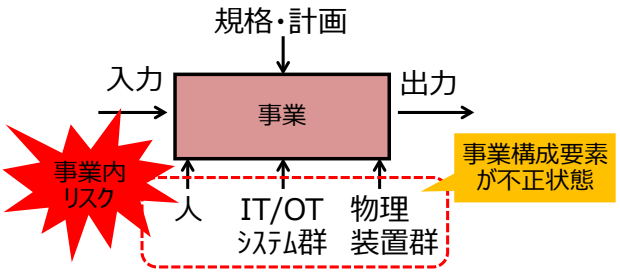

図 11：事業内リスクの概要

次に、リスク抽出の観点について述べる。表 3 に示すように、情報システムと制御システムでは保護対象や想定脅威が異なる[i][vi][vii]。具体的には、情報システムでは保護対象が「情報」であり、CIA[4]が損なわれることが想定脅威となる。これに対して制御システムにおける保護対象は「物理プロセス」であり、H&SEB[5]が損なわれることが想定脅威となる。このため、本手法の適用対象である制御システムでは、H&SEB の観点からリスクを抽出する。

---

[4] 情報セキュリティの 3 つの特性。機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）のそれぞれの頭文字をとって CIA と呼ぶ。

[5] 国際標準規格[i]では、産業用オートメーションおよび産業用システムの CIA が損なわれた場合の結果を理解すべき対象として挙げられている要素である。健康（Health）、安全性（Safety）、環境（Environment）、財務的結果（Business）の頭文字をとっている。なお、H&SE のうち H と S は、その性質上合わせて検討される場合が多いため、本手法では H&S として合わせて分析する。

表 3：情報システムと制御システムの違い

項目	情報システム	制御システム
保護対象	情報	物理プロセス
リスク顕在化時の影響	情報漏洩、金銭的被害	危険状態に陥る
想定脅威	CIAが損なわれること	H&SEBが損なわれること
要求される稼働率	95-99%	99.9%-99.999%
ライフサイクル	3年～5年	10年～20年

本ステップは以下の様にさらに細分化されたステップから構成される。

ステップ 2-1. 事業外リスクの抽出

ステップ 2-2. 事業内リスクの抽出

それぞれの詳細は、以下の通り。

ステップ 2-1. 事業外リスクの抽出

本ステップでは、各出力項目に対して、意図しない状況（出力上の不具合）とそれによって事業外に及ぼす悪影響を抽出する。意図しない状況については HAZOP（Hazard and Operability Study）[6] [viii]のガイドワード（なし／不正／過剰／不足）をベースに、また悪影響については H&SEB の観点から抽出する。事業外リスクの抽出例を表 4 に示す。

[6] プロセスや操作における危険源の抽出に用いられる安全性評価手法の一つ。

表 4：事業外リスクの抽出例

#	出力項目	ガイドワード	発生事象	観点	事業外リスク
1	供給物質	なし	供給物質が供給されない	H&S	供給物質が提供されず、生命維持に支障が生じ、
				E	衛生面での環境が悪化し、
				B	あらゆるサービスが広範囲で停止する
2		不正	利用困難な物質が供給される	H&S	利用困難な物質が提供され、生命維持に支障が生じ、
				E	衛生面での環境が悪化し、
				B	あらゆるサービスが限定的になる
3		過剰	供給物質が過剰に作られ工場の周辺に漏れ出す	E	供給物質が過剰に作られて工場の周辺に溢れ、
				B	生活全般および事業継続が困難となる
4		不足	供給物質の供給が不足する	H&S	供給物質の提供が不足し、健康被害が生じ、
				E	限定的に衛生面での環境が悪化し、
				B	事業範囲が縮小する
5	リサイクル原料	なし	リサイクル原料が生産されない	B	リサイクル原料が生産されず、リサイクル品製造業が停止する
6		不正	不純物の多いリサイクル原料が生産される	H&S	不純物の多いリサイクル品が生産され、強度不足のため事故が起き負傷者が出て、
				B	質の悪いリサイクル品を出荷したことで顧客の信頼が失墜する
7		過剰	リサイクル原料が過剰に作られる	E	リサイクル品が過剰に作られ、大量の廃棄物が出る
8		不足	リサイクル原料の生産が不足する	B	リサイクル品の生産が不足し、受注通りのリサイクル品が製造できず顧客の信頼が失墜する

ステップ 2-2. 事業内リスク抽出

本ステップでは、事業を構成する要素（人、IT/OT システム群、物理装置群）に対して、意図しない状況とそれにより事業内に及ぼす悪影響を抽出する。意図しない状況については HAZOP のガイドワード（なし／不正／過剰／不足）をベースに、また悪影響については H&SEB の観点から抽出する。事業内リスクの抽出例を表 5 に示す。

表 5：事業内リスクの抽出例

#	構成要素	ガイドワード	発生事象	観点	事業内リスク
1	運転制御システム	なし	運転制御システムが停止する	B	運転制御システムが停止し、供給物質の提供サービスが停止する
2		不正	運転制御システムが誤作動する	B	運転制御システムが誤作動し、適切な量で供給物質の提供サービスができなくなる
3	管理・監視システム	なし	管理・監視システムが停止する	B	管理・監視システムが誤作動し、適切な品質で供給物質の提供サービスができなくなる
4		不正	管理・監視システムが誤作動する	B	管理・監視システムが誤作動し、適切な品質で供給物質の提供サービスができなくなる
5	配布計画システム	なし	配布計画システムが停止する	B	配布計画システムが停止し、供給物質の提供サービスが停止する
6		不正	配布計画システムが誤作動する	B	配布計画システムが誤作動し、適切な量で供給物質の提供サービスができなくなる
…	…	…	…	…	…

■ステップ 3. リスクレベル見積り

本ステップは、抽出した事業リスクに対して、その影響の大きさを評価することを目的とする。本手法では、表 6 および表 7 に示すように H&SEB の観点で影響のレベルを定義し、リスクレベルを見積る。表 6 および表 7 は国際標準規格[i]の情報を基に作成している。この規格では、事業レベルでのリスク分析における観点（H&SEB）やリスクの種類、影響、リスクレベル等がそれぞれ独立に示されている。表 6 および表 7 ではこれらを H&SEB の観点に対応させる形でまとめ、さらに事業外リスクと事業内リスクを分けて定義した。

表 6：事業外リスクの影響レベル定義例

観点	リスクの種類	影響 【事業外リスク】	影響度
H&S	産業活動の安全性	不正な出力による死亡事故の発生	高
		不正な出力による傷病の発生	中
		なし	低
E	環境的安全性	不正な出力による広範囲、長期間の環境への重大な損傷	高
		不正な出力による地域行政への報告が必要な損傷	中
		なし	低
B	社会インフラ事業としての影響	出力利用主体の広範囲でのサービス停止	高
		出力利用主体の限定された地域でのサービス停止	中
		なし	低
	公衆の信頼	出力利用主体のブランドイメージ喪失	高
		出力利用主体の顧客信頼の喪失	中
		なし	低
	法的	出力利用主体による重い刑事犯罪	高
		出力利用主体による軽い刑事犯罪	中
		なし	低

表 7：事業内リスクの影響レベル定義例

観点	リスクの種類	影響 【事業内リスク】	影響度
H&S	産業活動の安全性	対象事業内における死亡事故の発生	高
		対象事業内における傷病の発生	中
		なし	低
E	環境的安全性	対象事業内における広範囲、長期間の環境への重大な損傷	高
		対象事業内における地域行政への報告が必要な損傷	中
		なし	低
B	社会インフラ事業としての影響	対象事業の広範囲でのサービス停止	高
		対象事業の限定された地域でのサービス停止	中
		なし	低
	公衆の信頼	対象事業のブランドイメージ喪失	高
		対象事業の顧客信頼の喪失	中
		なし	低
	法的	対象事業による重い刑事犯罪	高
		対象事業による軽い刑事犯罪	中
		なし	低

本手法では、事業リスクの影響度をスコア化して各事業リスクの大きさ（レベル）を表現する。具体的には、表 8 に示すような基準を作成し、リスクレベルを決定する。このリスクレベルの基準例では、「高」が 2 つ以上、または「高」が 1 つかつ「中」が 2 つの場合に、リスクレベルを「高」とするようにレベル付けしている。

表 8：リスクレベル基準例

観点 影響度				H&S		
				低	中	高
B	低	E	低	低	低	中
			中	低	中	中
			高	中	中	高
	中		低	低	中	中
			中	中	中	高
			高	中	高	高
	高		低	中	中	高
			中	中	高	高
			高	高	高	高

表 4 および表 5 の事業外／内リスクの抽出例に対し、表 8 に従いリスクレベルを評価した結果を表 9 に示す。このように抽出した事業外／内リスクのうち、一定の基準以上のものを「対象事業リスク」として設定し、これ以降のステップでは対象事業リスクを対象に検討を進める。

表 9：リスクレベル評価例

事業外リスク

#	出力項目	ガイドワード	発生事象	観点	事業外リスク	影響	リスクレベル
1	供給物質	なし	供給物質が供給されない	H&S	供給物質が提供されず、生命維持に支障が生じ、	H&S: 高 E: 高 B: 高	高
				E	衛生面での環境が悪化し、		
				B	またあらゆるサービスが広範囲で停止する		
2		不正	利用困難な物質が供給される	H&S	利用困難な物質が提供され、生命維持に支障が生じ、	H&S: 高 E: 高 B: 中	高
				E	衛生面での環境が悪化し、		
				B	またあらゆるサービスが限定的になる		
…		…	…	…	…	…	…
5	リサイクル原料	なし	リサイクル原料が生産されない	B	リサイクル原料が生産されず、リサイクル品製造業が停止する	B: 高	中
…		…	…	…	…	…	…
8		不足	リサイクル原料の生産が不足する	B	リサイクル品の生産が不足し、受注通りのリサイクル品が製造できず顧客の信頼が失墜する	B: 中	低

事業内リスク

#	構成要素	ガイドワード	発生事象	観点	事業内リスク	影響	リスクレベル
1	運転制御システム	なし	運転制御システムが停止する	B	運転制御システムが停止し、供給物質の提供サービスが停止する	B: 高	中
…	…	…	…	…	…	…	…
5	配布計画システム	なし	配布計画システムが停止する	B	配布計画システムが停止し、供給物質の提供サービスが停止する	B: 高	中
6		不正	配布計画システムが誤作動する	B	配布計画システムが誤作動し、適切な量で供給物質の提供サービスができなくなる	B: 中	低
…	…	…	…	…	…	…	…

■ステップ 4. 事業リスク要因検討

本ステップは、事業リスクと周辺事業や事業内業務との関係性を明確化し、詳細分析を行うべき対象を明らかにすることを目的とする。具体的には、ステップ 3 で抽出した対象事業リスクに関連が多い事業・業務は、重大な事業リスクを引き起こす可能性が高いため、優先的に対策する必要があるという考え方に基づき、対象事業リスクと周辺事業や事業内業務との関係性を明らかにする。まず、事業外モデルおよび事業内モデルから、周辺事業および事業内業務をリストアップする。周辺事業については、ターゲット事業の責任範囲内にあるものをリストアップする。各周辺事業および事業内業務と、ステップ 3 で抽出した対象事業リスクとの関係を検討し、対象事業リスクの要因となる周辺事業および事業内業務に“〇”を記す。この結果、対象事業リスクに多く関連している業務／システムが明らかになり、詳細分析を行うべき対象が明らかになる。

表 10 に、図 7 の事業外モデルおよび図 9 の事業内モデルを用い、表 9 にある事業リスクの要因となる周辺事業／事業内業務をリストアップしたものを示す。これより周辺事業では、調査事業および社内 IT インフラ事業が対象事業リスクと関係がある点がわかる [7]。また、事業内業務では前処理

[7] この事例では、事業外業務については、ターゲット事業の責任範囲内にある周辺事業の数が少ないため、その中で優先順位をつけるというより、それらに対策を施す（次の詳細分析のステップに進む）必要があることが確認できる。

業務および主要業務が詳細分析を行うべき対象であることが分かる（他と比較して“〇”がついている数が多い）。なお、この表で示すリスクは一例である。

表 10：主要事業における事業リスク要因検討例

			事業外リスク	事業内リスク	
			#2: 利用困難な物質が提供され、生命維持に支障が出、衛生面での環境が悪化し、またあらゆるサービスが限定的になる	#1: 運転制御システムが停止し、供給物質の提供サービスが停止する	#5: 配布計画システムが停止し、供給物質の提供サービスが停止する
分類	事業/業務	構成要素 ※出力以外（事業内業務のみ）	リスクレベル：高	リスクレベル：中	リスクレベル：中
周辺事業	調査事業	－			〇
	社内IT インフラ事業				〇
事業内業務	前処理業務	入力		〇	〇
		人	〇	〇	〇
		IT/OTシステム	〇	〇	〇
		物理装置		〇	〇
		規格・計画		〇	〇
	主要業務	入力	〇	〇	〇
		人	〇	〇	〇
		IT/OTシステム	〇	〇	〇
		物理装置	〇	〇	〇
		規格・計画			
	配布業務	入力			
		人	〇	〇	〇
		IT/OTシステム	〇	〇	〇
		物理装置		〇	〇
		規格・計画			
	副産物処理業務	入力			
		人		〇	〇
		IT/OTシステム		〇	〇
		物理装置		〇	〇
		規格・計画			

2.2 詳細リスク分析とセキュリティ対策立案

組織やシステムに効果的なセキュリティ対策を施すには、そこに内在するリスクの大きさや影響度を評価する必要があり、本手法ではこれらを把握するために詳細リスク分析を実施する。詳細リスク分析は対象となる組織やシステムの保護対象資産、脅威、脆弱性の洗い出しと評価を行い、そこからリスクの大きさを評価する分析手法である。対象の実態の把握や適用する判断基準等が整理・分類され、分析結果を客観的に評価することも可能であるため、フィードバック等による評価手法のブラッシュアップや見直し等、長期的な保守が必要な組織やシステムにも適している。セキュリティ設計仕様については、情報セキュリティの国際評価基準[ix]で手順の大枠が規定されている。

2.2.1 リスク分析と対策立案の実施内容

［ステップ 1］評価対象定義

セキュリティ対策実施の対象となるシステムとその内部の資産をモデル化する。

［ステップ 2］脅威分析

評価対象に対して発生しうる脅威を洗い出す。

［ステップ 3］リスク評価

抽出した各脅威のリスクを算出する。

［ステップ 4］対策方針策定

対策を行う脅威を明確にし、各脅威に対して実施する対策目標を策定する。

［ステップ 5］セキュリティ要件の選択

標準規格[xiii]のセキュリティ機能要件集から対策目標の具現化に必要な項目を選択する。

2.2.2 リスク分析と対策立案における重要ポイント

リスク分析と対策立案に、特に考慮すべきポイントを記載する。

表 11：リスク分析と対策立案における重要ポイント一覧

#	タイトル	関連ステップ
重要ポイント2.	詳細リスク分析を通した網羅的なリスク把握と規格に則った対策方針の決定	ステップ1～5

重要ポイント２ ： 詳細リスク分析を通した網羅的なリスク把握と規格に則った対策方針の決定

（１）ポイント

効果的なセキュリティ対策を施すため、詳細リスク分析を通した網羅的なリスク把握と規格に則った対策方針の決定によりセキュリティ設計を行う。詳細リスク分析および対策立案については、それぞれ記載のある規格・ガイドラインを参照のこと[x]。また、具体的な手法についても研究・提案がなされている[xi]。

（２）解説

組織やシステムに効果的なセキュリティ対策を施すには、そこに内在するリスクの大きさや影響度を評価する必要がある。これらを把握するために詳細リスク分析を実施し、リスクを網羅的に把握・評価したうえでセキュリティ対策を施す箇所を決定し、各リスクの内容に基づいて対策方針を決定する。

リスク分析から対策立案までの流れは以下の通り。

ステップ 1. 評価対象定義　…開発対象となるシステムとその内部の資産をモデル化
ステップ 2. 脅威分析　…評価対象に対して発生しうる脅威の洗い出し
ステップ 3. リスク評価　…抽出した各脅威のリスクを算出
ステップ 4. 対策方針策定　…対策を行う脅威を明確にし、各脅威に対して実施する対策目標を策定
ステップ 5. セキュリティ要件の選択…標準規格等[xiii]のセキュリティ機能要件集から対策目標の具現化に必要な項目を選択

（３）実施例

ステップ 1 では、セキュリティ対策実施の対象となるシステムをモデル化したうえで、保護対象資産やインタフェース等、守るべきシステムの構成要素を明確化する。図 12 に主要事業の例を示す。

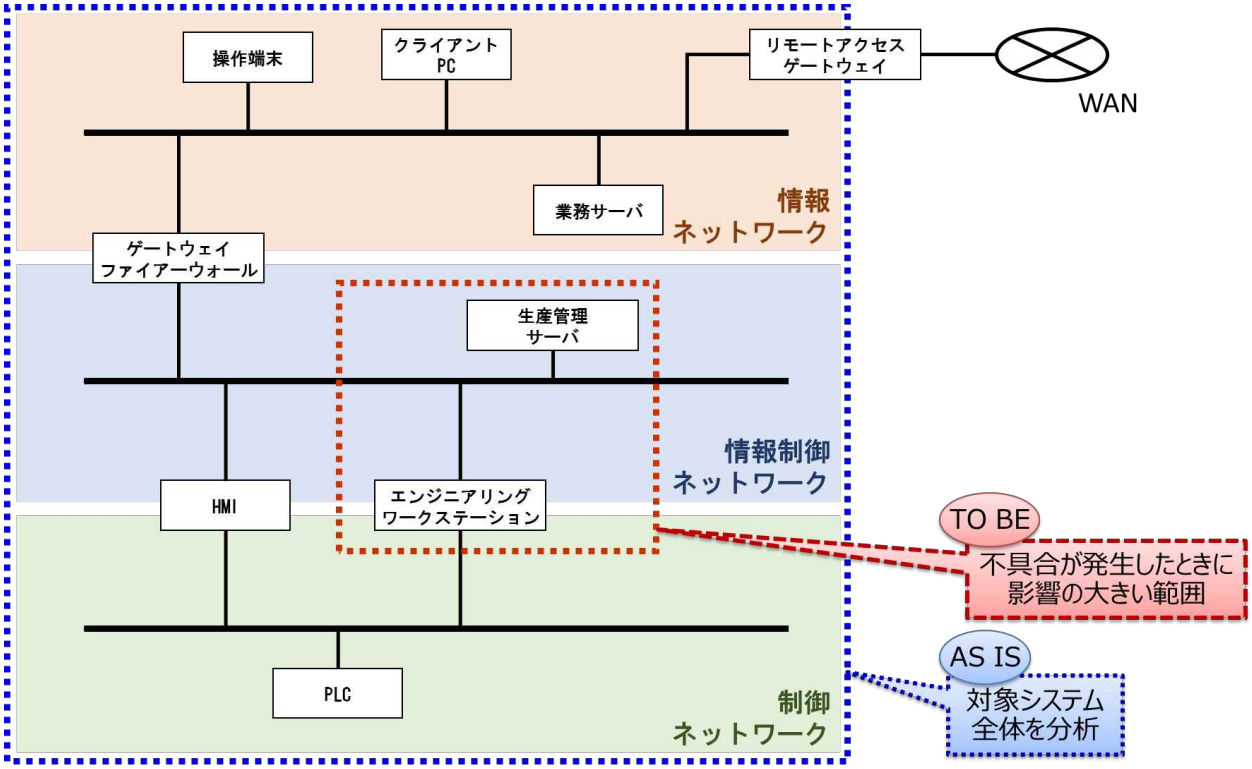

図 12：主要事業の運転制御システムにおける評価対象定義のモデル図例

（IPA の一般的な制御システムの図[xiii]を基に作成）

ステップ 2 およびステップ 3 の流れで詳細リスク分析を実施する。ステップ 2 の脅威分析の手法としては、例えば 5W 法[8]がある。図 13 に概要、図 14 に主要事業の運転制御システムの分析結果の例を示す。

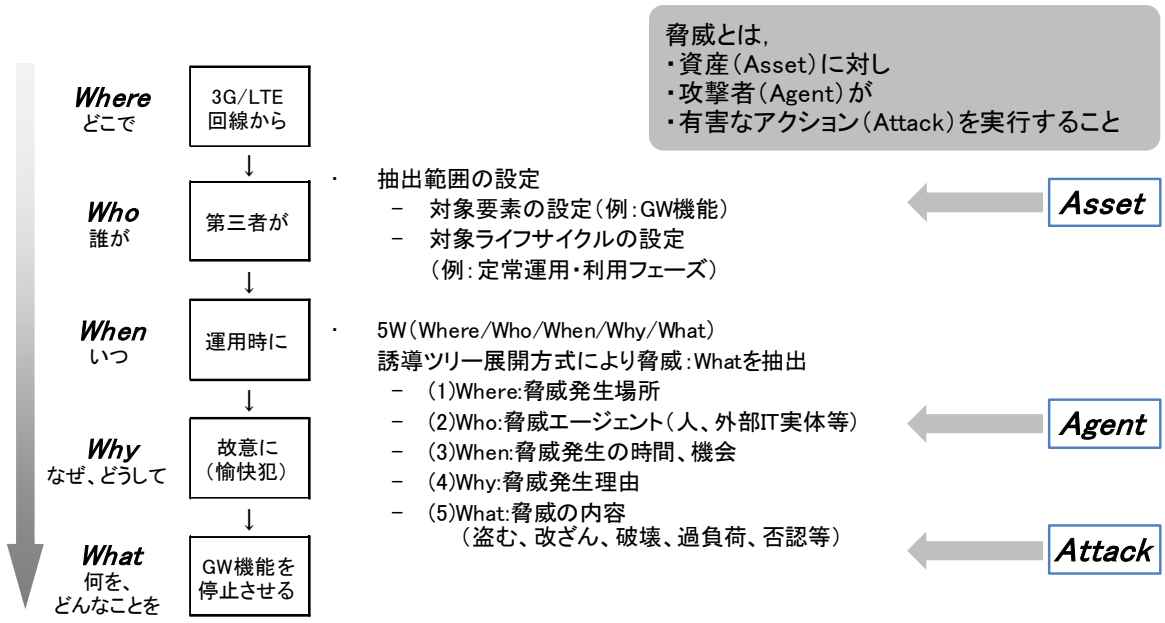

図 13：5W 法の概要

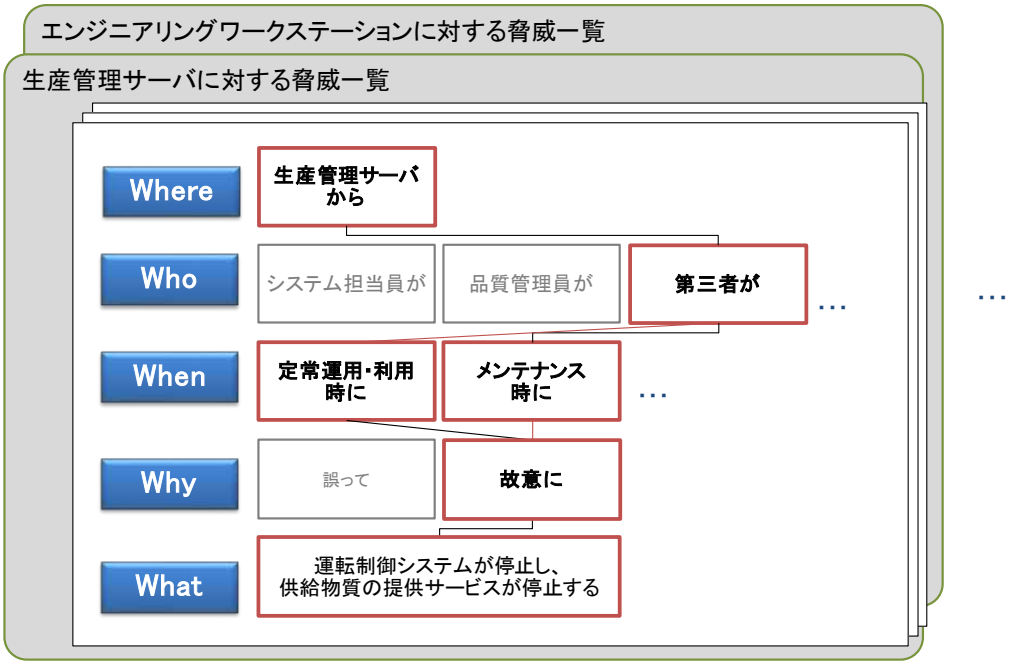

図 14：主要事業の運転制御システムの脅威分析における 5W 法の例

[8] 原因（Why）、対象（What）、地点（Where）、時間（When）、人物（Who）に基づいて事象を分析する手法。

また、ステップ 3 のリスク評価では、例えば ISMS[9]での以下のリスク値算出を用いてリスクの評価を行う。

リスク値＝「資産の価値」×「脅威」×「脆弱性」

例えば表 12 のようにランクを設定し、各脅威の内容に基づいて高中低を決定する。表 13 にリスク値の計算例を示す。

表 12：リスク値要素の定義例

評価項目	質問	ランク値（例） 高:3～低:1
資産の価値	資産の価値はどれくらいですか	高：漏洩すればビジネスへの影響は深刻 中：漏洩すればビジネスへの影響は大きい 低：漏洩すればビジネスへの影響は少ない
脅威	脅威の発生頻度は どれくらいですか	高：1ヶ月に1回以上 中：半年以内に1回あるかないか 低：1年に1回あるかないか
脆弱性	脆弱性の度合い、 突破されやすさは どれくらいですか	高：低い知識・スキルで突破できる 中：高い知識・スキルで突破できる 低：大変高い知識・スキルで突破できる

表 13：リスク値の計算例

脅威	資産の価値	脅威	脆弱性	リスク値
運転制御システムが停止し、供給物質の提供サービスが停止する	3	1	1	3
配布計画システムが誤作動し、適切な量で供給物質の提供サービスができなくなる	2	2	2	8

ステップ 4 では、ステップ 3 でリスク値の高かった脅威に対し対策方針を策定する。NIST Cybersecurity Framework[x]の大項目の「機能」には、「特定（Identify）」、「防御（Protect）」、「検知（Detect）」、「対応（Respond）」、「復旧（Recover）」があり各々カテゴリーが設けられ、さらにその下に複数のサブカテゴリーが存在する（表 14、表 15）。対策方針の策定では、これを参考に対策を立案する。詳しくは NIST Cybersecurity Framework を参照のこと。

9 情報セキュリティマネジメントシステム（Information Security Management System）。組織で情報セキュリティに関する活動を運用していくための枠組み。

表 14：フレームワークコアの構成

機能	カテゴリー
特定	資産管理
	ビジネス環境
	ガバナンス
	リスクアセスメント
	リスクアセスメント管理戦略
	サプライチェーンリスクマネジメント
防御	アクセス制御
	意識向上およびトレーニング
	データセキュリティ
	情報を保護するためのプロセスおよび手順
	保守
	保護技術
検知	異常とイベント
	セキュリティの継続的なモニタリング
	検知プロセス
対応	対応計画の作成
	コミュニケーション
	分析
	低減
	改善
復旧	復旧計画の作成
	改善
	コミュニケーション

表 15：資産管理カテゴリーとサブカテゴリー

カテゴリー	サブカテゴリー
資産管理	企業内の物理デバイスとシステムの一覧を作成している。
	企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。
	企業内の通信とデータの流れの図を用意している。
	外部情報システムの一覧を作成している。
	リソース（例：ハードウェア、デバイス、データ、ソフトウェア）を分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。
	すべての従業員と第三者である利害関係者（例：供給業者、顧客、パートナー）に対して、サイバーセキュリティ上の役割と責任を定めている。

なお、脅威から対策方針策定する手法としては、例えば FTA（Fault Tree Analysis）[10]がある。図 15 および表 16 に、FTA の実施例とこれを利用して作成した対策方針の例を示す。

[10] 特定の望ましくない事象を起点に因果関係のツリーを作成し、発生要因を洗い出す分析手法。

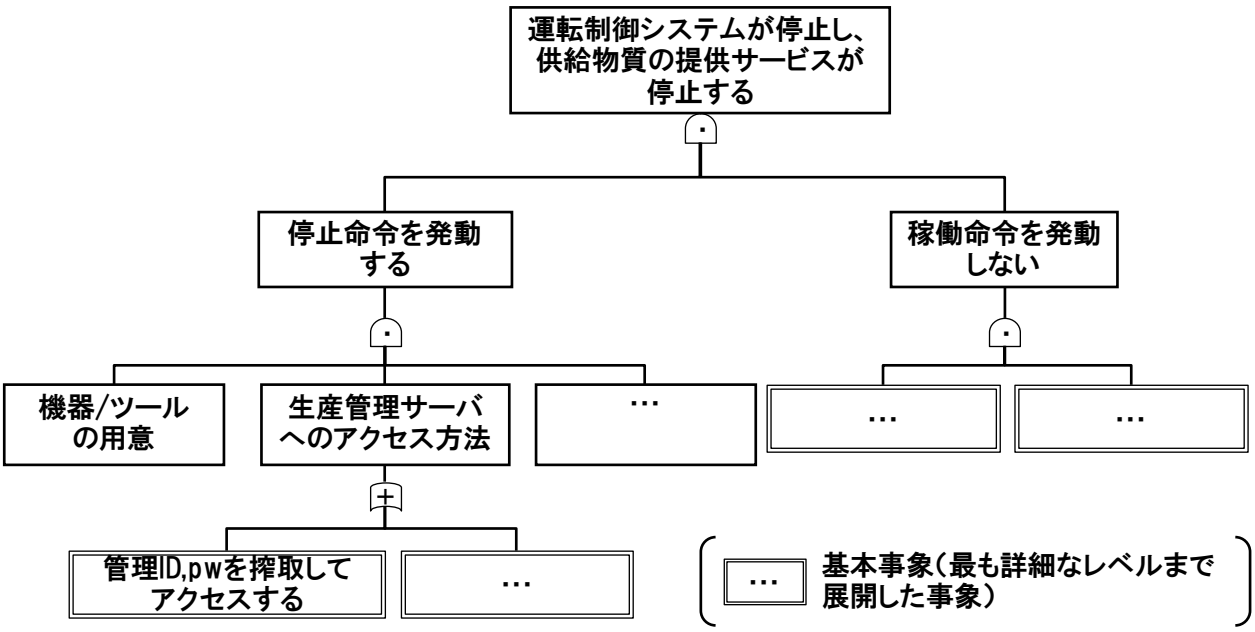

図 15：FTA の実施例

表 16：対策方針の例

脅威	基本事象(原因)	対策目標	対策方針		
			#	種別	方針内容
運転制御システムが停止し、供給物質の提供サービスが停止する	攻撃者に不正な命令を書き込む動機がある	攻撃の動機を防止する	1	環境 (Non-IT)	攻撃によって攻撃者が被る不利益（法的な罰則等）を啓発する
			2	環境 (IT)	生産管理サーバへのアクセスログを取得し、攻撃があった際に攻撃者を特定できるようにする
	不正な機器/ツールを入手し、利用	市販の機器からの攻撃が出来ないようにする	3	環境 (Non-IT)	接続した際に脅威となるような機器が市販されないよう関係方面に働きかける
	不正な機器/ツールを自作し、利用	正規ツールの仕様書の閲覧範囲を制限する	4	環境 (Non-IT)	関係者以外が正規ツールの仕様書を閲覧できないようにする
	脅威対象の生産管理サーバの場所が分かる	脅威対象の生産管理サーバであることが判明しないようにする	5	環境 (Non-IT)	脅威対象の生産管理サーバを搭載しているシステムであると外部から判別できないようにする
		脅威対象の探索活動を検知する	6	IT	ネットワークを監視し、探索活動等の不審な通信を検知する
	生産管理サーバに接続する	生産管理サーバに接続可能な機器を制限する	7	IT	事前に登録した機器のみが接続できるよう制限する
	不正な命令を書き込む	第三者による書き換えをできなくする	8	IT	生産管理サーバ利用者の認証を実施する
:		:		:	

ステップ 5 では、ステップ 4 で策定した対策方針の実現に必要な機能要件を決定する。例えば、標準規格[xiii]に記述されているセキュリティ機能要件集の中から、対策目標の具現化に必要な項目を選択する。

3章　構築フェーズ（事前準備）

3.1 構築フェーズ（事前準備）の実施内容

本フェーズでは、どのようなセキュリティ対策を、どのような構成・手順で導入するかを検討する。

重要インフラシステムではサービスの可用性が高く求められるため、システムに対してセキュリティ対策を適用する際に、誤って既存システムに影響を及ぼしてしまった場合には大きな影響につながってしまう。このため、実際にセキュリティ対策を適用する前に、事前の準備作業が大変重要となる。事前準備作業では、以下のような作業・検討を実施する。

［ステップ 3-1］対象システムの把握

対象システムのシステム構成、扱う情報、サービス時間等の情報を把握／再確認する。

［ステップ 3-2］セキュリティ装置の設置箇所・設置構成の検討

ステップ 3-1 の結果を踏まえ、対象システムのどこに、どのようなセキュリティ装置を設置すべきかを検討する。また、具体的な設置構成（装置やスペック）の検討や、設置するスペース等の検討、既存システムへの影響をどの程度考慮する必要があるか（例えば余分な通信パケットを出さないレベル等）の検討と、これらの検討結果に関する事業者およびベンダ間での認識合わせを実施する。

【本ステップで考慮すべきポイントを、重要ポイント 3 に記載】

［ステップ 3-3］事前検証

既存システムに追加でセキュリティ装置を設置する場合、既存システムに影響を与えないことが重要なポイントとなる。既存システムへ影響を与えないために、どのような項目を事前に確認すべきかを検討し、本番システムと同等の非本番環境を使用して検証を行う。本番環境では異常系の検証は実施できないため、事前検証時に正常系および異常系での検証を行う。また、脆弱性の確認も行う。

【本ステップで考慮すべきポイントを、重要ポイント 4 に記載】

［ステップ 3-4］セキュリティ装置導入に向けた手順検討および安全性検証

本番システムにセキュリティ装置を導入する際に、既存システムに影響を与えずに安全に導入するための手順を検討する。また、非本番環境でその手順を実際に実行することで、手順の安全性を検証する。

【本ステップで考慮すべきポイントを、重要ポイント 5 に記載】

3.2 構築フェーズ（事前準備）での重要ポイント

構築フェーズ（事前準備）で、特に考慮すべきポイントを記載する。

表 17：構築フェーズ（事前準備）における重要ポイント一覧

#	タイトル	関連ステップ
重要ポイント3.	セキュリティ対策を実施する箇所の決定	ステップ3-2
重要ポイント4.	非本番環境での安全性検証	ステップ3-3
重要ポイント5.	作業リスクの把握および対策の検討	ステップ3-4

重要ポイント３ ： セキュリティ対策を実施する箇所の決定

（１）ポイント

セキュリティ装置をシステムに導入する場合、リスクの大きさや効果、既存システムへの影響を考慮して設置箇所を決定する。さらには、物理的な設置可否も考慮する。

（２）解説

サイバー攻撃の監視システムや検知システムを導入する場合、その設置箇所は下記観点で検討を実施したうえで決定する必要がある。あらかじめ下記の観点を考慮することで、既存システムへ影響を及ぼすリスクを低減し、物理的制約による設置見直し等の手戻り発生を防止できる。

(A) リスクの大きさ ： 「2.2 詳細リスク分析とセキュリティ対策立案」で実施したリスク分析結果を踏まえ、重要業務に関連する箇所や、脆弱性（誰でも触れる場所にある等）が高い箇所を、優先的に監視／検知対象とする。

(B) 制約を踏まえた構成検討 ： 既存システムへ影響を及ぼさないように、制約事項等を考慮してセキュリティ装置の構成や設置箇所を検討する。例えば、既存システムへのソフトウェア追加が許容されない場合には、通信データをキャプチャして監視するようなセキュリティ装置を選定し、適切な設置箇所を検討する。

(C) 効果 ： 監視／検知対象を複数個所で監視／検知可能な場合、効果の大きい方を選択する。例えば、特定の通信を監視できる箇所と、多数の通信を監視できる箇所が候補としてある場合は、後者の方の効果が大きいと考えられるため、後者を優先する。

(D) 既存システムへの影響 ： 監視／検知システムが既存システムに悪影響を及ぼす可能性を考慮する。例えば、悪影響発生時に切り離し可能な部分を選定して設置する。

(E) 物理的制約 ： あらかじめ物理的制約も考慮して、導入機器を選定する。例えば、設置場所のスペースに制約がある場合は、導入機器の大きさを確認してから決定する必要がある。

（３）実施例

以下に、ネットワークの監視を行うセキュリティ対策の検討例を示す。一般的に重要インフラシステム（制御システム）は、システム全体を管理する情報ゾーン、複数の現場をまとめて管理する情報制御ゾーン、現場で実際にサービスを提供する制御ゾーンの三層構造から成り、それぞれの拠点は複数ある場合が多いが、その数は上位層から下位層に向かって増えていく。以下の実施例は、この前提の下に検討を行う。

また、本実施例では、下位層のシステムが機能不全に陥った場合、上位層のシステムからの指令により同じ層にある別のシステムが代行可能な仕組みを持つものとする。

(A) リスクの大きさの検討例

リスクの大きさの検討例として、監視対象の検討例を表 18 に、また重要インフラシステムに対する侵入ルートを示した脅威抽出の例を図 16 に示す。

本実施例では、上述の情報ゾーンが統合システム、情報制御ゾーンが拠点システム、制御ゾーンが現場システムに当たる。拠点システムおよび現場システムは複数あり、また現場システムは、他に比べ特別に規模が大きく関連機器の数が多い X 現場システム、それ以外の Y 現場システムの 2 種類がある。

リスクの大きさの検討の結果、統合ネットワークは重要度と影響範囲ともに大きくサイバー攻撃も受けやすいという点から監視対象とする。拠点ネットワークは影響範囲が統合ネットワークよりも限定的であるが、下位層の複数のシステムに影響が出てしまい被害が拡大しやすいという点から監視対象とする。また、X 現場ネットワークに関しても、重要度が拠点ネットワークと同程度かつ物理攻撃を受けやすいことから監視対象とする。一方、Y 現場ネットワークは、物理攻撃は比較的受けやすいものの重要度・影響範囲・サイバー攻撃の受けやすさが共に小さいため、非対象とする（表 18）。なお、表 18 にある物理攻撃とは部外者の侵入や機器の破壊等を、また物理対策とは各エリアでの入退室の管理やセキュリティカメラによる監視等を想定している。

これらの観点以外にも、システムや業務特有の重要装置や重要業務等の他の情報を考慮すべき場合もある。必要に応じて当該情報を選択すること。

表 18：リスクの大きさを考慮した監視対象の検討

	重要度	影響範囲	攻撃の受けやすさ		監視対象
			物理攻撃	サイバー攻撃	
統合ネットワーク （統合システム）	大	甚大	小 （物理対策：強）	大 （外部ネットワークとの繋がり：有り）	対象
拠点ネットワーク （拠点システム）	中	中	小 （物理対策：強）	小 （外部ネットワークとの繋がり：無し）	対象
X現場ネットワーク （X現場システム）	中	小	中 （物理対策：弱）	小 （外部ネットワークとの繋がり：無し）	対象
Y現場ネットワーク （Y現場システム）	小	小	中 （物理対策：弱）	小 （外部ネットワークとの繋がり：無し）	非対象

外部からの侵入ルートとしては、統合ネットワークに対して、外部ネットワークからのマルウェア感染等が考えられる。また、内部からの侵入ルートとしては、すべてのネットワークに対して、内部犯による正規機器の不正操作やマルウェアを格納した記憶媒体（USB 等）の挿入が考えられる（図 16）。

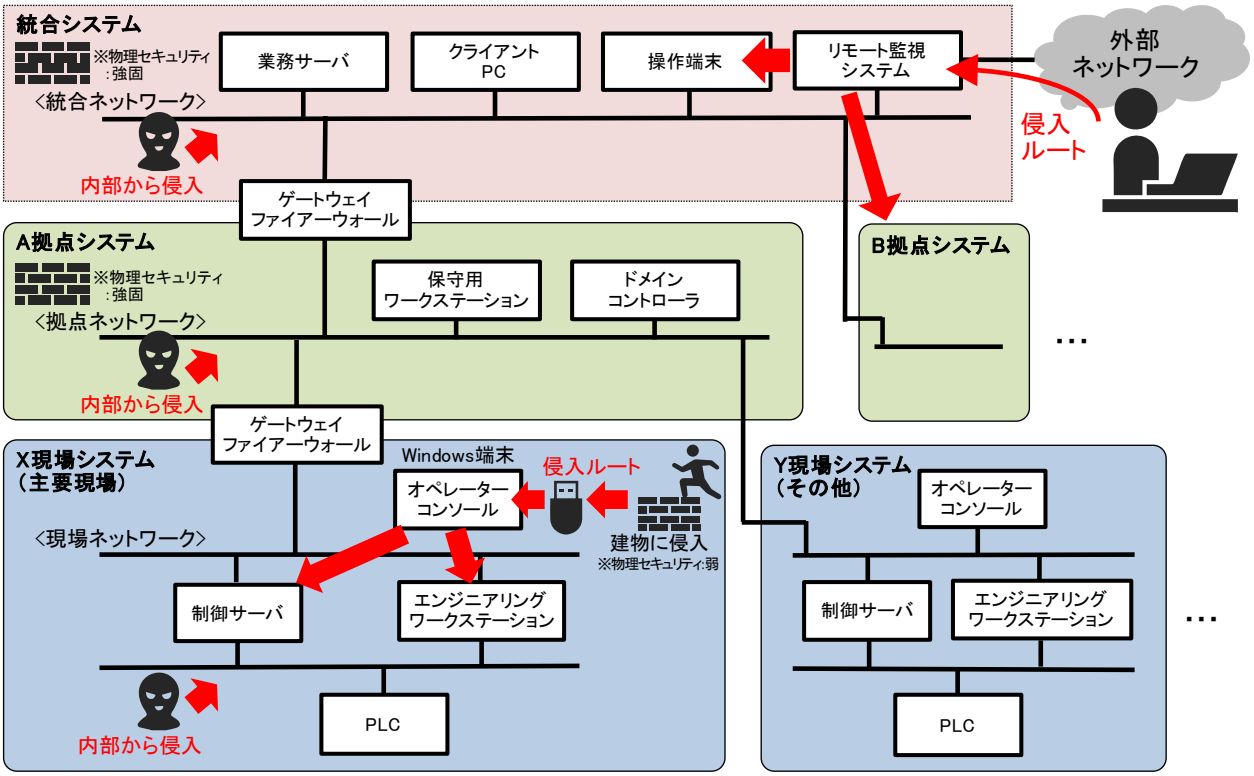

図 16：重要インフラシステムの脅威抽出（侵入経路）

(B) 制約を踏まえた構成検討

重要インフラシステムにおけるネットワーク監視箇所の検討結果を図 17 に示す。本システムでは各サーバにソフトウェア等を追加することは制限されているため、通信データをキャプチャすることで監視が可能なセキュリティ装置を入れることを検討する。

統合ネットワーク、拠点ネットワーク、現場ネットワークのそれぞれの通信を監視することが望ましい。ただし、監視拠点数に制限がある場合は、統合システムのような上位のネットワークを監視した方が監視拠点数を低減することが可能だが、下位のネットワーク内のみで行われている通信は監視できないため、監視するネットワークを精査する必要がある。

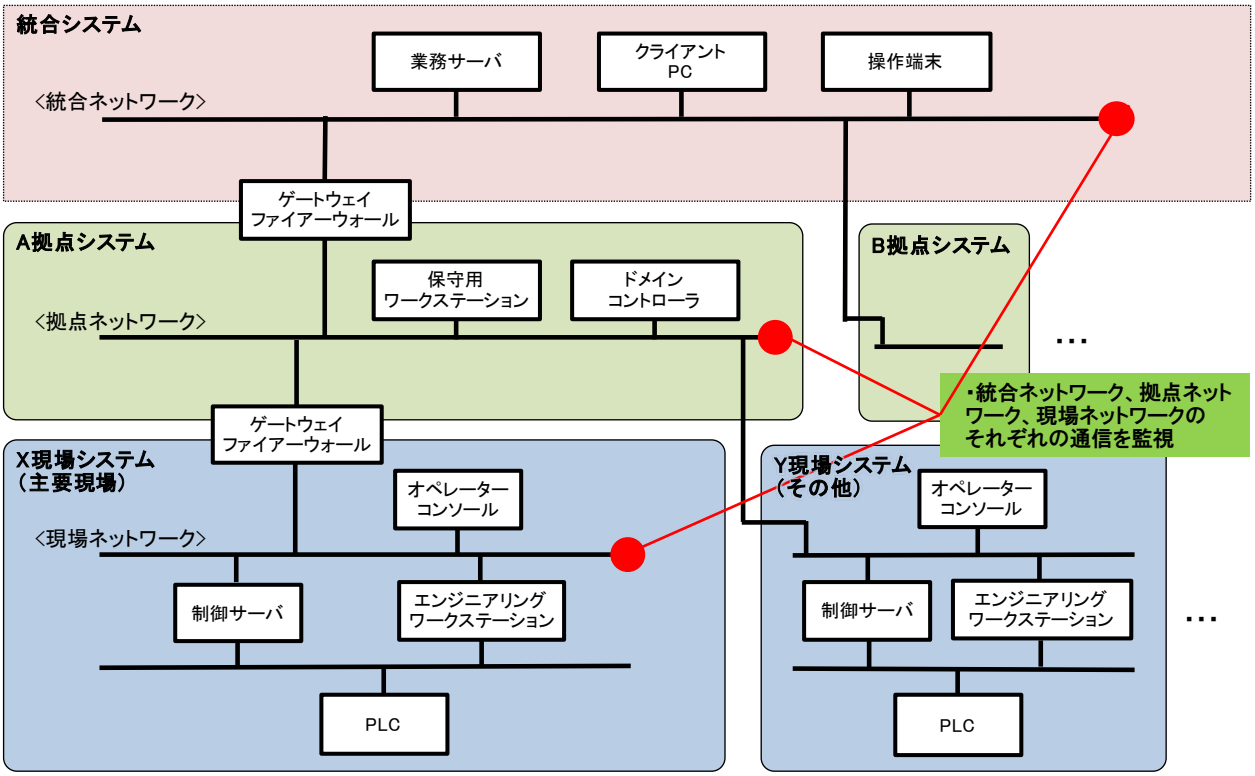

図 17：重要インフラシステムにおけるネットワーク監視箇所候補

(C) 効果を考慮した対策箇所の検討

重要インフラシステムにおけるネットワーク監視箇所候補検討（図 17）では、効果の面も考慮した検討を行う。統合ネットワークは、システム全体に影響がある通信を監視できるため、最も効果がある。拠点ネットワーク、X 現場ネットワークは拠点数が多くなりがちなため、効果も期待できる主要な拠点や現場を対象とするべきである。

(D) 既存システムへの影響を考慮した検討

重要インフラシステムにおけるネットワーク監視候補検討では、既存システムへの影響の面も考慮した検討を行う。セキュリティ装置を接続する箇所は、セキュリティ装置が異常動作を行った場合でも業務に重大な影響を及ぼしにくいポイント、または、冗長化されて切り替えが可能なネットワークを選択する等の考慮をするべきである。

(E) 物理的制約の検討

検討例として、重要インフラシステムにおけるセキュリティ装置選定検討結果を図 18 に示す。本システムにおけるセキュリティ装置の設置は、ネットワークを流れるデータ量および設置スペースの大きさから検討を行う。統合ネットワークおよび拠点ネットワークは流れるデータ量が多く、かつ設置スペースにも余裕があるため、大型のセキュリティ装置を選定する。X 現場ネットワークに関しては、流れるデータ量は少なく、また設置スペースが狭く装置の大きさに制約があるため、小型のセキュリティ装置を選定する。なお、このような場合は、必要に応じてセキュリティ装置の数を増やす

ことでデータ量の増減に対応することを併せて検討すべきである。

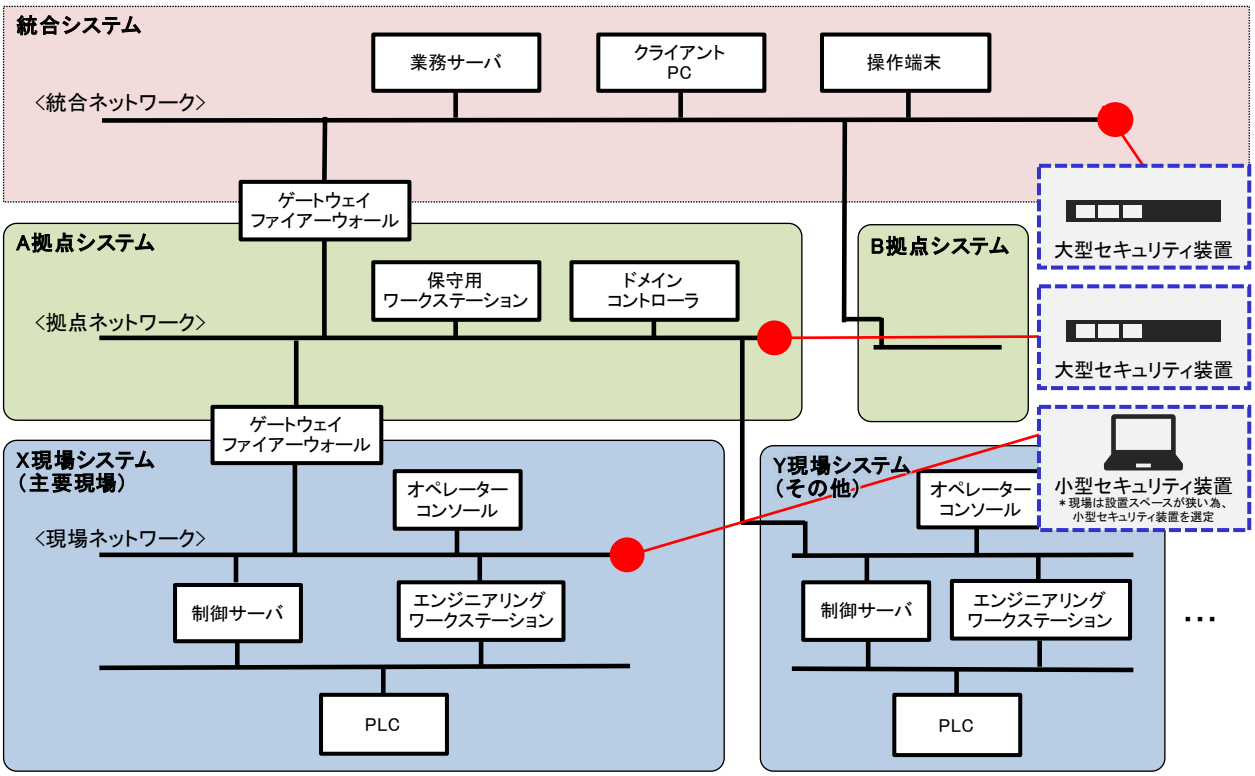

図 18：重要インフラシステムにおけるセキュリティ装置選定検討

重要ポイント４ ： 非本番環境での安全性検証

（１）ポイント

既存システムへ影響を与えないために、非本番環境を使用して事前に正常系および異常系での検証を行い、安全性を確認する。

（２）解説

既存システムに追加でセキュリティ装置を設置する場合、既存システムに影響を与えないことが重要なポイントとなる。既存システムへ影響を与えないために、本番システムと同等の非本番環境を使用して検証を行うことが重要である。本番環境では異常系の検証は実施できないため、事前検証時に正常系および異常系での検証を行う。具体的には、以下のような観点で検証を実施する。

- 既存システムへの影響
  既存システムへ影響を及ぼさないことを確認する。なお、影響を及ぼさないことをどのレベルで確認すべきかを、あらかじめ事前検証者（製品導入ベンダや自組織の担当者）と認識合わせをする必要がある。例えば、既存業務が正常に動作するレベル、余分な通信パケットを出さないレベル、スイッチの処理性能に影響を及ぼさないレベル、等のレベルのうち当該事業者と必要なレベルをあらかじめ合意する。具体的には、パケットを受信するだけの監視装置であれば、OS ブート時の ARP パケットも出す必要がないため、これらの不要なパケットの送信を停止する等の対処を実施する。
- 正常再起動の確認
  再起動しても OS・セキュリティ監視ソフトウェアが正常に起動し、再起動前と同一の設定となっているかを確認する。
- 停止中の安全性の確認
  セキュリティ装置が停止中にシステムに影響を与えていないことを確認する。
- ハードウェア異常発生時の安全性の確認
  セキュリティ装置に異常が発生した際にシステムに影響を与えないことを確認する。
- ソフトウェア異常発生時の安全性の確認
  セキュリティ装置のソフトウェアに異常が発生した際にシステムに影響を与えないことを確認する。
- ハードウェア異常停止時の安全性の確認
  セキュリティ装置が異常停止した際にシステムに影響を与えないことを確認する。
- ソフトウェア異常停止時の安全性の確認
  セキュリティ装置のソフトウェアが異常停止した際にシステムに影響を与えないことを確認する。

（3）実施例

検証項目の例を表 19 に示す。

本番環境では実施できない異常系動作や疑似攻撃時の動作の確認を含めて検証を実施する。

表 19：検証項目例

#	大項目	中項目	小項目	備考
1	正常起動していることの確認	OSの起動確認	OSが正常に起動していることを確認	
2		アプリの起動確認	アプリが正常に起動していることを確認	
3			DBが正常に起動していることを確認	DBを利用する場合
4			管理画面が正常に起動していることを確認	管理画面を利用する場合
5	外部装置へパケットを送信しないことの確認	セキュリティ装置が外部にパケットを送信しないことを確認	セキュリティ装置の各ポートをスイッチに接続し、当該ポートをミラーリングする。	セキュリティ装置が一定時間(24時間)パケットを出さない事の確認。
6			一定時間、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
7			セキュリティ装置をリブートする。	セキュリティ装置がリブートする時にパケットを出さない事の確認。
8			セキュリティ装置がリブートする際にミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
9			セキュリティ装置をシャットダウンする。	セキュリティ装置がシャットダウンする時にパケットを出さない事の確認。
10			セキュリティ装置がシャットダウンをする際に、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
11			セキュリティ装置を起動する。	セキュリティ装置が起動する時にパケットを出さない事の確認。
12			セキュリティ装置が起動する際に、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
13			セキュリティ装置に接続されているミラーリング用LANケーブルを差し抜きする。	セキュリティ装置に接続しているケーブルが差し抜きされた時にパケットを出さない事の確認。
14			セキュリティ装置に接続されているLANケーブルが抜かれた際、及び挿された際に、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
15		アプリが外部にパケットを送信しない事を確認	セキュリティ装置の各ポートをスイッチに接続し、当該ポートをミラーリングする。	
16			一定時間、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
17			アプリをリブートする。	
18			ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
19	リブート後の設定確認	OSリブート後の設定確認	SELinuxの設定が正しいことを確認	
20			iptablesの設定が正しいことを確認	
21		アプリのリブート後の設定確認	アプリの設定値がリブート前と変わらないことを確認	
22	動作の確認	アプリの動作確認	セキュリティ装置にミラーポートが接続されていること、スイッチにミラーリング設定がされていることを確認	
23			上記ミラーリングが設定されているスイッチに、PCを2台接続し、当該PC間でTCP通信、UDP通信、ICMP通信を実施し、当該パケットを収集して、当該情報が見えることを確認	
24		ホワイトリストの動作確認	ホワイトリストを設定し、ホワイトリストに設定してあるトラヒックを流した時に、アラートが発報されないことを確認	
25	異常時動作の確認	セキュリティ装置が外部にパケットを送信しないことを確認	セキュリティ装置の各ポートをスイッチに接続し、当該ポートをミラーリングする。	セキュリティ装置が異常時にパケットを出さない事の確認。
26			セキュリティ装置の電源ケーブルを引き抜き、異常終了させる。	
27			セキュリティ装置がハードウェア異常時に、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	
28		アプリが外部にパケットを送信しない事を確認	セキュリティ装置の各ポートをスイッチに接続し、当該ポートをミラーリングする。	
29			killコマンドでアプリを異常終了させる。	
30			アプリが異常時に、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認	

重要ポイント５ ： 作業リスクの把握および対策の検討

（１）ポイント

既存システムに対してセキュリティ装置を追加する作業に関して考えられるリスクを抽出し、当該リスクが発生しないように対策を検討する。また、リスクが発生した場合も考えて、影響範囲を拡大させないための対策を検討する。

（２）解説

すでにサービスを提供しているシステムに対してセキュリティ装置等を追加する場合、サービスに影響を及ぼさないようにシステム変更を行う必要がある。このため、セキュリティ装置を導入する際や、導入後に考えられるリスクをあらかじめ洗い出し、事前に予防できるものについては予防対策を施す。また、万が一リスクが発生した場合には、迅速な対処により影響範囲を拡大させないような対策をあらかじめ検討し、導入手順に明記しておく。

（3）実施例

リスク抽出例を表 20 に示す。

表 20：一般的なリスク抽出例

#	分類	リスク	対策	確認結果	備考
1	セキュリティ	装置からのマルウェア感染	搬出前に最新のパターンファイルで検疫する。		
2	セキュリティ	不正なUSBメモリを接続されてマルウェア等の感染	USB等の端子に物理的ロックを掛ける。		
3	セキュリティ	装置が不正に操作される	OSにログインパスワードを設定する。		
4	セキュリティ	装置側LANケーブルを抜かれて不正機器を接続される	ロック機能付きLANケーブルを利用する。		
5	セキュリティ	装置本体が盗難される	ワイヤーロックで机等に固定する。		
6	セキュリティ	装置からHDDが盗難される	鍵付のフロントベゼルを装着する。		
7	作業ミス	別端末を操作	操作端末にログインするユーザIDを本番環境接続と開発環境接続で異なるものにしていること。 ケーブルの差し替えやIPアドレスの手入力など、一つの作業・操作を誤っただけで誤接続となる手順がないこと。		
8	作業ミス	操作端末の追加、役割の変更	適切な設定／変更を実施すること。 変更前の環境に対する接続情報を削除していること。		
9	作業ミス	環境変更ツールなどの使用	ログインユーザのログオンシェルなどで接続先が誤りなく設定されるようになっていること。		
10	作業ミス	装置を接続対象とは別のスイッチに接続してしまう	手順書に接続先情報と状態確認方法、誤接続時の復旧方法を明記する。 作業時に2人以上でクロスチェックを行う。		
11	作業ミス	装置の電源プラグを使用する電源コンセントと別の場所に挿してしまう	手順書に使用する電源コンセントを明記する。 作業時に2人以上でクロスチェックを行う。		
12	作業ミス	動作中の別機器の電源を抜いてしまう	手順書に使用する電源コンセントを明記する。 電源ケーブルにタグを付けて、目視確認できるようにする。 作業時に2人以上でクロスチェックを行う。		
13	作業ミス	新しい機器への設定	設定パラメタを適切に変更していること。 (既存接続済の装置・ソフトウェアに対する設定値の単純コピーによる誤りはないか確認)		
14	作業ミス	新しい機器への操作	操作手順を適切に変更していること。 (既存接続済の装置・ソフトウェアに対する操作手順の単純コピーによる誤りがないことを確認)		
15	作業ミス	不要データの残留	本番環境に接続する前に追加する装置を試験などで使用した場合、過去の試験データ(入力/出力)など不要な情報を削除すること。		
16	不正操作	電源ボタンを不正に押下される(ON/OFF)	鍵付のフロントベゼルを装着する。		
17	不正操作	OSシャットダウンやデータ採取処理を不正に停止される。	OSにログインパスワードを設定する。		
18	不正操作	本番機と開発機の接続	開発(保守)機は本番機と物理的・論理的に分離する		
19	障害	保守員不在時にハード障害	データ採取時以外は電源OFF データ採取時のハード障害の連絡体制を確立。		
20	障害	保守員不在時にソフト障害	データ採取時以外は電源OFF データ採取時のソフト障害の連絡体制を確立。		

4章　構築フェーズ（導入）

4.1 構築フェーズ（導入）の実施内容

本フェーズでは、前章で記述した「構築フェーズ（事前準備）」で検討したセキュリティ装置の構成や導入手順に基づき、実際にセキュリティ装置を対象システムに導入するための準備および導入作業を行う。

重要インフラシステムではサービスの可用性が高く求められるため、本フェーズでも既存システムに影響を及ぼさないことが大変重要となる。セキュリティ装置の導入作業では、以下のような作業・検討を実施する。

［ステップ 4-1］導入機器の準備

実際に対象システムへ導入する装置を導入できる状態にするため、セキュリティ装置にソフトウェアをインストール、構成設定を行う。また、設定済みの装置に対する品質保証部門による設定確認や期待通りの動作をすることを確認する。

［ステップ 4-2］作業手順の準備

対象システムにセキュリティ装置を導入する手順を検討し、手順書を作成する。また、非本番環境を使用して、作成した作業手順書を実施しリハーサルを行うことで、予定している作業が問題なく実施できること、および作業を実施した際にサービスに影響を与えないことを事前に確認する。

［ステップ 4-3］関連部署における内容把握

導入作業の目的や作業内容を、関係する部署に対して周知し、何かあった場合の原因の可能性を共有する。導入作業の担当者は、作業直前には必要なものがそろっていることの確認や、危険予知ミーティング、当日の健康状態のチェックを行うことで、導入作業における障害発生リスクを可能な限り低減する。

［ステップ 4-4］導入作業の実施

これまでのステップで準備した作業手順に基づき、導入機器を対象システムに導入する。

【上記ステップ 4-1～4-4 全体で考慮すべきポイントを、重要ポイント 6 に記載】

4.2 構築フェーズ（導入）における重要ポイント

構築フェーズ（導入）で、特に考慮すべきポイントを記載する。

表 21：構築フェーズ（導入）における重要ポイント一覧

#	タイトル	関連ステップ
重要ポイント6.	計画に基づく確実な作業の実施	ステップ4-1～4-4

重要ポイント６ ： 計画に基づく確実な作業の実施

（１）ポイント

本番システムへの導入作業におけるミスは、サービスへ影響を及ぼす事故につながるため、事前に検証／確認した結果を手順書として残し、確実な作業を実施する。

（２）解説

サービスへ影響を及ぼす事故の発生リスクを可能な限り減らすために、具体的に以下のような点を考慮する必要がある。

(A) 作業スケジュール ： 導入作業の実施タイミングは、対象システムのピークタイム等を外す等の考慮が必要である。また、導入作業のスケジュールは、時間単位でスケジュールを定め、作業遅延等の問題発生時に備えて切戻しポイントを設定しておく。なお、切戻しポイントとは、次のシステム稼働時間までに導入作業が終わらないと予想される場合に、作業を始める前の段階へシステムの状態を戻すことを決定し作業を切り替えるタイミングのことである。

(B) 作業前体制の明確化 ： あらかじめ決定した作業体制に基づき、作業前および作業後に適切な管理者への報告や、問題発生時に適切なエスカレーションを実施できるようにする。

(C) 作業前の確認事項 ： 作業開始前には、危険予知ミーティングや、対象システムで定められる安全教育等を実施する。危険予知ミーティングは、作業完了後にも想定外の危険ポイントがなかったかの観点で実施する。

(D) 導入作業実施中の注意事項 ： 導入作業では、作業ログを残し、ダブルチェックを行うことで可能な限りミスを防止する。また、作業がスケジュールから遅延し始めた場合、作業終了時間までに終わるかどうかを判断する。終わらない場合、切戻し作業を実施する。

(E) 導入作業完了後の確認事項 ： 実施した導入作業が対象システムのサービス／業務に影響を及ぼしていないかを確認する。確認すべきポイントは、事前に定めておく。

（3）実施例

(A) 作業スケジュールの実施例

全体スケジュールの例を図 19 に示す。

作業の全体について大項目や中項目を記載して線表で表現することで、実施すべきタスクの洗い出しや進捗管理を実施することが可能となる。本実施例では、稼働中の本番環境で作業を実施する場合を想定しており、障害発生時にサービスへの影響が大きいと思われる日（ピークタイム）をお盆休みとしてその間は作業抑止期間とする。

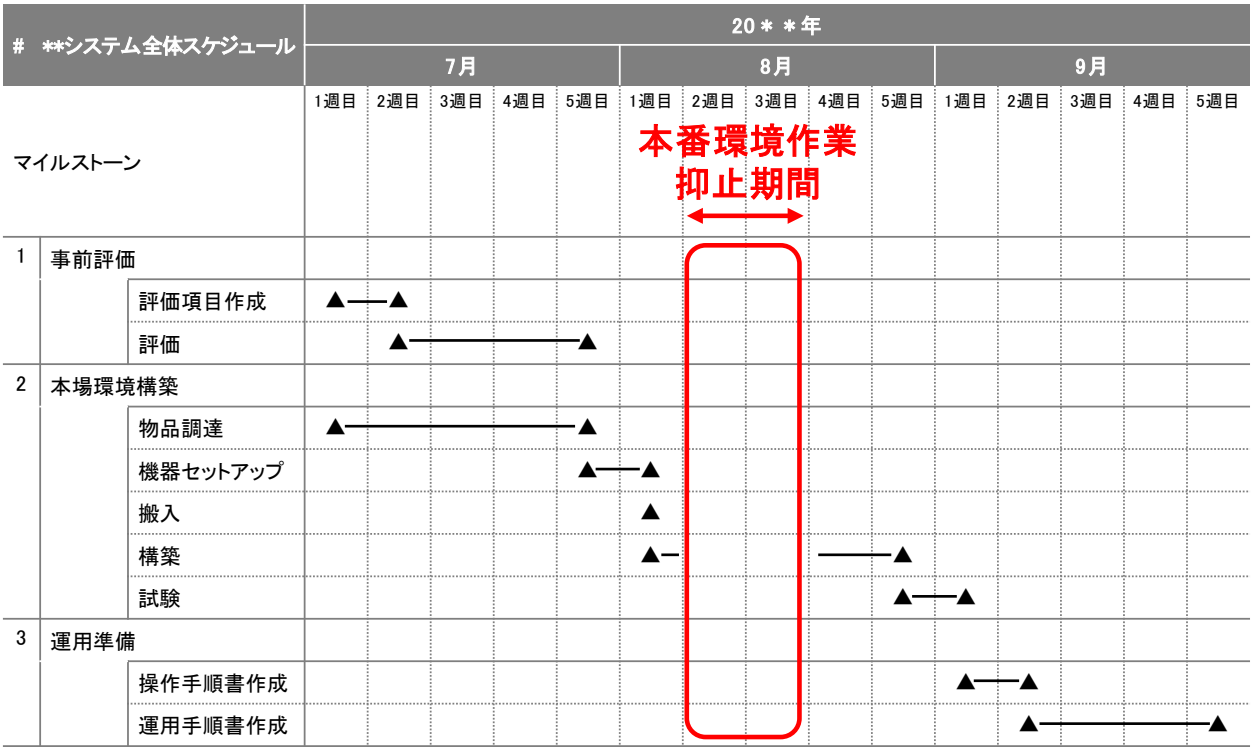

図 19：全体スケジュール例

作業日当日の作業スケジュール例を図 20 に示す。

作業日当日の作業タスクについて、詳細に時間を計画して管理することで、当日の作業漏れや進捗管理を可能とする。また、当該情報を事業者のシステム管理者と共有することで同一システムに対し同時に複数作業を実施することを回避し、作業リスクを低減する。

また、重要インフラシステムには作業終了時間に制限があるため、万が一終了予定時間までに作業が終了しない見込みとなった場合、速やかに切戻し等の対処が可能となるよう作業タスク毎の予定作業開始／終了時間を記載する。また、参照する手順書の間違いを防ぐため、各作業タスクで使用する手順書を作業名称と共に記載する。さらに、作業実施中の想定外事象の早期発見や、適切な作業切り替えを可能とするため切戻しポイントを設ける。

■作業スケジュール
(1) 作業名称：**システム設置作業
(2) 作業日時：20**年 **月 **日(*)
(4) 対象機器：分析装置、セキュリティ装置、対向装置(システム監視装置)
(5) 手　順　書：■設置作業：セキュリティ装置設置手順書
■現状分析：分析ツール操作手順書
■装置動作確認：セキュリティ装置操作手順書
(6) 作 業 者：[A社]＊＊＊＊＊＊
[B社]＊＊＊＊＊＊
(7)特記事項：16時までに作業が完了しない見込みの場合は、切り戻しを実施すること。

20**年 **月 **日 (*)

No.	内容		担当	開始 [計画]	終了 [計画]	所要時間	開始 [実績]	終了 [実績]
1	入館手続き/入館		A/B社	10:00	10:15	00:15		
2	事前準備	作業準備、物品確認	B社	10:15	10:20	00:05		
3		作業前ミーティング	A/B社	10:20	10:30	00:10		
4	機器搬入	機器搬入	A/B社	10:30	10:45	00:15		
5	設置作業	設置、結線	B社	10:45	11:00	00:15		
6	現状分析	ﾈｯﾄﾜｰｸ状態把握	B社	11:00	11:15	00:15		
7	装置起動	装置電源投入、起動	B社	11:15	11:30	00:15		
8	装置動作確認	装置動作確認	B社	11:30	12:00	00:30		
9		対向装置状態確認	B社	12:00	12:30	00:30		
10	業務影響確認		A社	12:30	13:00	00:30		
11	終了ミーティング		A/B社	13:00	13:15	00:15		
12	片づけ・退館		B社	13:15	13:30	00:15		

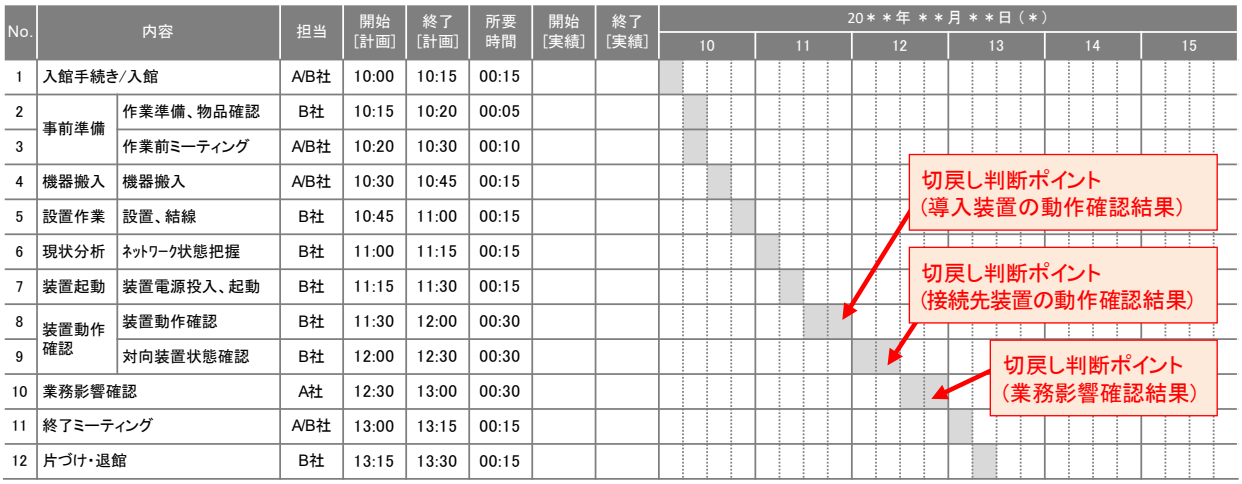

図 20：作業スケジュール例

(B) 作業前の体制明確化の実施例

作業前に体制を明確化し、想定外事象が発生した場合にも速やかな判断や対処を可能とする。作業体制図の例を図 21 に示す。

現場での作業体制だけではなくシステムを管理している事業者の体制や作業を実施する部隊のバックアップ体制も含めて記載することで、想定外事象発生時に早期対応が可能となる。

当該体制にアサインされたメンバーは、作業開始から作業終了まで連絡がとれる状態として待機する。

＜作業実施者＞

・作業実施現場での作業実施者[11]、作業確認者[12]、作業責任者[13]
・作業責任者の上位役割である作業管理者
・サポート SE
・品質保証部
・営業

11 手順書に基づき実際に作業を実施する作業者。各手順は作業確認者の確認の基に実施する。

12 作業実施者が手順書に基づき作業を実施していることを確認する作業者。作業のダブルチェックの役割を担う。

13 作業現場における作業全般に関わる責任者。

＜システム運用事業者＞

・作業実施現場におけるシステム運用事業者の作業立会者

・システム運用事業者の責任者

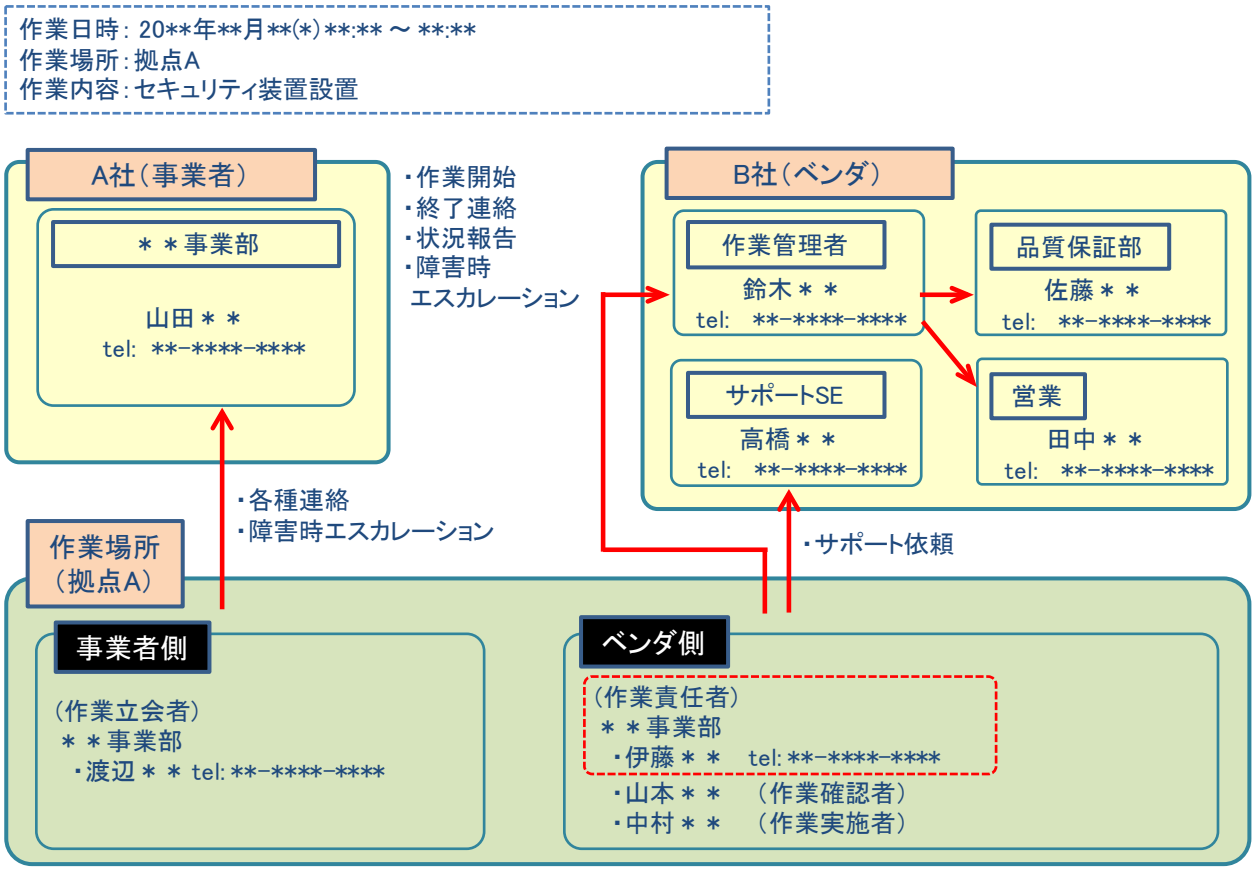

図 21：作業体制図例

(C) 作業前の確認事項の実施例

作業前および作業後確認事項として、危険予知ミーティングのチェックシートの例を図 22 に示す。

本チェックシートは事前にリスクがある作業内容や危険ポイントを洗い出して明確にすることによって、作業における危険を回避することが目的である。また、当該ミーティングは、事業者と一緒に実施することで事業者と危険／リスクを共有することが可能となりリスク低減につながる。

本実施例では、危険／リスクに関する作業内容や事象について洗い出した事前記入項目、それらを事業者と共に認識し合う作業開始前確認項目、作業終了後に危険／リスクの有無を共有しそれらの把握漏れや被害拡大を防止する作業後確認項目を記載する。

（1）事前記入項目

作業日				**予定時間**	開始予定時刻: ～ 終了予定時刻:		
作業場所				**作業責任者**			
事業者担当者				**事業者立会い**	有・無		
作業者/立会者							
搬入	有・無	**搬出**	有・無	**重機使用**	有・無	**鍵等の借用**	有・無
予備品準備	良・否	**鍵等の借用**	有・無	**危険作業**	有・無	**高所作業**	有・無
サービス影響	有・無	**有の場合の影響時間:**		**電源設備作業**	有・無		
作業内容 1）セキュリティ装置設置作業 2） 3）				**対象機器** **・セキュリティ装置（ホスト名：＊＊＊）**			
危険ポイント 1）電源差し作業があるため、誤って他電源を抜く。 2）異なるLANケーブルを接続する。 3）				対策 1）作業者、確認者は指差し等の確認を怠らないこと。 2）システム管理者に接続するLANケーブルを確認する。 3）			

（2）作業開始前確認項目

天候	晴れ・曇り・雨・雪・その他（ ）			**KYM実施時間**	: ～ :		
危険予知ミーティング出席者							
服装	良・否	**体調**	良・否	**作業分担**	良・否	**作業申請掲示**	良・否
作業開始連絡	事業者	ベンダ			その他		

（3）作業後確認事項

終了ミーティング実施時間	: ～ :						
ハードトラブル	無・有（ ）			**ソフトトラブル**	無・有（ ）		
工事トラブル	無・有（ ）			**その他トラブル**	無・有（ ）		
予定外の事項はお客様へ連絡・承認を得たか？			良・否	**故障被疑品がある場合、切り離し済みか？**			良・否
作業対象装置アラーム確認結果			良・否	**サービス影響確認結果**			良・否
作業終了連絡	事業者	ベンダ			その他		
持帰データ	有・無	**データ削除**	良・否	**借用物の返却**	良・否	**整理整頓**	良・否

図 22：危険予知ミーティングチェックシート例

5章　構築フェーズ（確認）

5.1 構築フェーズ（確認）の実施内容

本フェーズでは、前章で記述した「構築フェーズ（導入）」で実施したセキュリティ装置の導入作業の後で、問題なく導入作業が完了したことの確認を行う。

重要インフラシステムではサービスの可用性が高く求められるため、本フェーズでも既存システムに影響を及ぼさないことが大変重要となる。セキュリティ装置導入後の確認では、以下のような確認作業を実施する。

［ステップ 5-1］正常起動の確認

導入したセキュリティ装置のハードウェア・OS やソフトウェアが正常に起動していることを確認する。

［ステップ 5-2］動作中の安全性の確認

セキュリティ装置が動作中にシステムに影響を与えていないことを確認する。例えば、不要なパケットを送出していないことを確認するために、スイッチングハブのパケットカウントをチェックする等、標準的な出力情報で確認を行う。

［ステップ 5-3］正常動作の確認

セキュリティ装置が正常に動作していることを確認する。例えば、プロセスの起動状況チェック、画面表示の確認等の標準的な出力情報で確認を行う。また、対象システムのサービス／業務が正常に稼働していることの確認も行う。

【上記ステップ 5-1～5-3 全体で考慮すべきポイントを、重要ポイント 7 に記載】

5.2 構築フェーズ（確認）における重要ポイント

構築フェーズ（確認）で、特に考慮すべきポイントを記載する。

表 22：構築フェーズ（確認）における重要ポイント一覧

#	タイトル	関連ステップ
重要ポイント7.	業務に影響を与えない確認の実施	ステップ5-1～5-3

重要ポイント７ ： 業務に影響を与えない確認の実施

（１）ポイント

本番システムへのセキュリティ装置導入後の確認では、サービス／業務へ影響を与えないように正常系の確認をしっかりと行いながら実施する。

（２）解説

既存システムにセキュリティ装置を設置する場合には、業務が行われている状況で対象システムにセキュリティ装置を導入するため、導入後の確認作業もサービス／業務に影響を与えないように実施する必要がある。このため、異常系のテストは実施せず、標準的な出力情報等を用いて確認作業を実施する。

セキュリティ装置を導入後は、セキュリティ機能が正しく起動・動作すること、および OS が不要なパケットを送信しない等、従来のサービスに影響を与えていないことを確認する必要がある。これらは通常の業務に影響を与えない方法で確認する必要があり、例えば以下の方法で実施する。

(A) 画面出力の確認
(B) 各種ログの確認（エラーログ、動作ログ）
(C) 機器の LED の点灯・点滅確認
(D) ルータ等のネットワーク機器の LED 点灯やログ、パケットカウンターの確認
(E) HMI の画面表示等の状況から判断

なお、異常系のテストは、「構築フェーズ（事前準備）」の段階で十分に実施しておく必要がある。例えば、本番環境と同等の環境を準備し、本番システムと同じデータを活用する等、システム構成だけでなく、データも本番環境に近づけて実施する。また、セキュリティ機能の検証をするために、本番環境では実施できない模擬攻撃のテストも実施する。

（３）実施例

導入後の確認作業内容の例を以下に示す。

正常起動の確認の実施例として、OS およびセキュリティ装置のアプリの起動確認例を表 23、表 24 に示す。ここでは、LED 点灯、ログ、起動画面等から正常起動を確認する。

表 23：OS の起動確認例

① OSの起動確認

項番	作 業 内 容	チェック欄
(A)	セキュリティ装置の電源ボタンを押して、セキュリティ装置を起動	
	セキュリティ装置のLEDが正常に点灯がしていることを確認	
(B)	マシンを起動	
	起動後に、OSのログイン画面が表示されること	
(C)	ログインできることの確認	
	下記、ユーザ名、パスワードを入力し、エンターキーを押下。	
	ユーザ名　：　＊	
	パスワード：　＊	
	ログインができ、OSのデスクトップ画面が表示される。	
(D)	正常起動したことの確認	
	アプリケーションから端末を選択	
	ターミナルウィンドウが起動される事を確認	
	下記コマンドを入力	
	#cat /var/log/messages	
	システムログにエラーが出ていないことを確認	

表 24：セキュリティ装置のアプリの起動確認例

② セキュリティ装置のアプリの起動確認

項番	作 業 内 容	チェック欄
(A)	ターミナルを起動 アプリケーションから端末を選択 ターミナルウィンドウが起動される事を確認	
(B)	su にログイン #su△- パスワードを聞かれるので、以下パスワードを入力 * root権限でログインできた事を確認。(ターミナル画面のログインユーザ名がrootになっている事を確認)	
(C)	セキュリティ装置のアプリが正常に起動している事を確認。 以下のコマンドを入力。 #systemctl status app 出力結果が以下となっている事を確認。(Active ：active (running)と表示されている事を確認。) app.service Loaded: loaded (/usr/lib/systemd/system/app.service; enabled) Active: active (running)　　(以下省略)	
(D)	セキュリティ装置のアプリが正常に起動していない場合、セキュリティ装置のアプリを起動。 (セキュリティ装置のアプリが起動していない時の手順。セキュリティ装置のアプリが起動している場合は省略) (C)で入力したコマンドの出力結果が以下となっている場合、以下コマンドを入力し、セキュリティ装置のアプリを起動。 (出力結果がActive ；inactive (dead)となっている場合) app.service Loaded: loaded (/usr/lib/systemd/system/app.service; disabled) Active: inactive (dead)　　(以下省略) #systemctl start app #systemctl enable app 以下のコマンドを入力。 #systemctl status app 出力結果が以下となっている事を確認。(Active ：active (running)と表示されている事を確認。) app.service Loaded: loaded (/usr/lib/systemd/system/app.service; enabled) Active: active (running)　　(以下省略)	
(E)	DBアプリが正常に起動している事を確認。 以下のコマンドを入力。 #systemctl status db 出力結果が以下となっている事を確認。(Active ：active (running)と表示されている事を確認。) db.service Loaded: loaded (/usr/lib/systemd/system/db.service; enabled) Active: active (running)　　(以下省略)	
(F)	DBアプリが正常に起動していない場合、DBアプリを起動。(DBアプリが起動していない時の手順。DBアプリが起動している場合は省略) (E)で入力したコマンドの出力結果が以下となっている場合、以下コマンドを入力し、DBアプリを起動。 (出力結果がActive ；inactive (dead)となっている場合) db.service Loaded: loaded (/usr/lib/systemd/system/db.service; disabled) Active: inactive (dead)　　(以下省略) #systemctl start db #systemctl enable db 以下のコマンドを入力。 #systemctl status db 出力結果が以下となっている事を確認。(Active ：active (running)と表示されている事を確認。) db.service Loaded: loaded (/usr/lib/systemd/system/db.service; enabled) Active: active (running)　　(以下省略)	
(G)	管理画面アプリが正常に起動している事を確認。 以下のコマンドを入力。 #systemctl status mng 出力結果が以下となっている事を確認。(Active ：active (running)と表示されている事を確認。) mng.service Loaded: loaded (/usr/lib/systemd/system/mng.service; enabled) Active: active (running)　　(以下省略)	
(H)	管理画面アプリが正常に起動していない場合、管理画面アプリを起動。 (管理画面アプリが起動していない時の手順。管理画面アプリが起動している場合は省略) (G)で入力したコマンドの出力結果が以下となっている場合、以下コマンドを入力し、管理画面アプリを起動。 (出力結果がActive ；inactive (dead)となっている場合) mng.service Loaded: loaded (/usr/lib/systemd/system/mng.service; disabled) Active: inactive (dead)　　(以下省略) #systemctl start mng #systemctl enable mng 以下のコマンドを入力。 #systemctl status mng 出力結果が以下となっている事を確認。(Active ：active (running)と表示されている事を確認。) mng.service Loaded: loaded (/usr/lib/systemd/system/mng.service; enabled) Active: active (running)　　(以下省略)	

次に動作中の安全性の確認の実施例を表 25、表 26、表 27 に示す。表 25 ではサーバ起動・停止およびその後一定時間ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを、表 26 ではセキュリティ装置をリブートした際にセキュリティ装置がパケットを送信しないことおよびリブート後の OS の設定を、表 27 ではセキュリティ装置のアプリをリブートした際にセキュリティ装置のアプリがパケットを送信しないことを、それぞれ確認する。セキュリティ装置が外部装置へパケットを送信しないことを確認することで、システムに影響を与えず、安全であることを確認できる。

なお、異常系の動作については対象外であり、通常運用での操作による動作で確認を行う。

表 25：動作中の安全性の確認例①

① セキュリティ装置が外にパケットを送信しないことを確認
サーバ起動時、停止時、及びその後一定時間、ミラーリングをしている装置でセキュリティ装置がパケットを送信していないことを確認

項番	作 業 内 容	チェック欄
(A)	スイッチ、スイッチ制御用ノートPCの起動を確認	
	スイッチのLEDが正常に点灯している事を確認(スイッチの仕様に依存するため、スイッチの説明書を確認)	
	ノートPCにユーザ名、パスワードを入力し、ログインし、デスクトップ画面が表示される事を確認 (ノートPCに依存するため、ノートPCのユーザ名、パスワードを確認)	
(B)	スイッチとノートPCを接続し、ノートPCからスイッチにログイン	
	スイッチとノートPCをコンソールケーブルで接続	
	ノートPCのtera termを起動し、tera termのウィンドウが表示される事を確認	
	ノートPCのtera termのウィンドウで、"シリアル - スイッチに接続しているシリアルポート名" を選択	
	スイッチアクセスできた事を確認。(login画面が表示されることの確認)	
	スイッチにログイン(ユーザ名、パスワードはスイッチに依存するため、スイッチのユーザ名、パスワードを確認)	
(C)	スイッチの統計情報を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントを確認	
(D)	セキュリティ装置の電源ボタンを押して、セキュリティ装置を起動	
	セキュリティ装置のLEDが正常に点灯がしていることを確認	
(E)	セキュリティ装置がパケットを送信していない事を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントが増加していないことを確認	
(F)	セキュリティ装置のGUIの右上の電源アイコンをクリックし、シャットダウンをクリック	
	セキュリティ装置のLEDが消灯することを確認	
(G)	セキュリティ装置がパケットを送信していない事を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントが増加していないことを確認	
(H)	セキュリティ装置の電源ボタンを押して、セキュリティ装置を起動	
	セキュリティ装置のLEDが正常に点灯がしていることを確認	
(I)	一定時間(10分以上)経過後、セキュリティ装置がパケットを送信していない事を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントが増加していないことを確認	

表 26：動作中の安全性の確認例②

② セキュリティ装置が外にパケットを送信しないことを確認

セキュリティ装置をリブートした際に、セキュリティ装置がパケットを送信しないことを確認、リブート後のOSの設定確認

項番	作 業 内 容	チェック欄
(A)	スイッチ、スイッチ制御用ノートPCの起動を確認	
	スイッチのLEDが正常に点灯している事を確認(スイッチの仕様に依存するため、スイッチの説明書を確認)	
	ノートPCにユーザ名、パスワードを入力し、ログインし、デスクトップ画面が表示される事を確認 (ノートPCに依存するため、ノートPCのユーザ名、パスワードを確認)	
(B)	スイッチとノートPCを接続し、ノートPCからスイッチにログイン	
	スイッチとノートPCをコンソールケーブルで接続	
	ノートPCのtera termを起動し、tera termのウィンドウが表示される事を確認	
	ノートPCのtera termのウィンドウで、"シリアル - スイッチに接続しているシリアルポート名" を選択	
	スイッチアクセスできた事を確認。(login画面が表示されることの確認)	
	スイッチにログイン(ユーザ名、パスワードはスイッチに依存するため、スイッチのユーザ名、パスワードを確認)	
(C)	スイッチの統計情報を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントを確認	
(D)	セキュリティ装置のターミナルを起動	
	アプリケーションから端末を選択	
	ターミナルウィンドウが起動される事を確認	
(E)	セキュリティ装置にて、suにログイン	
	#su△-	
	パスワードを聞かれるので、以下パスワードを入力	
	*	
	root権限でログインできた事を確認。(ターミナル画面のログインユーザ名がrootになっている事を確認)	
(F)	セキュリティ装置にリブートコマンドを投入	
	以下のコマンドを投入	
	#reboot	
(G)	セキュリティ装置の起動確認	
	リブート後に、OSのログイン画面が表示されることを確認	
(H)	セキュリティ装置にログインできることの確認	
	下記、ユーザ名、パスワードを入力し、エンターキーを押下。	
	ユーザ名 ：*	
	パスワード ：*	
	ログインができ、OSのデスクトップ画面が表示される。	
(I)	リブート時にセキュリティ装置がパケットを送信していない事を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントが増加していないことを確認	
(J)	リブート後のOSの設定確認	
	以下のコマンドで、Firewalldが停止していることを確認。	
	# systemctl△status△firewalld →下図の通り、Firewalldが停止していることを確認する。	
	firewalld.service - firewalld - dynamic firewall daemon Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled) Active: inactive (dead) (以下省略)	
	以下のコマンドでIPv6のiptablesが有効になっている事の確認。	
	# systemctl△status△ip6tables →下図の通り、IPv6のiptablesが開始していることを確認する。	
	iptables.service - IPv6 firewall with iptables Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled) Active: active (exited) since Mon 2016-07-11 09:25:19 JST; 25s ago Process: xxxx ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS) Main PID: xxxx (code=exited, status=0/SUCCESS)	
	以下のコマンドでIPv6のキャプチャ用NIFによるパケット出力の抑止設定を確認	
	#ip6tables -L -v	
	下図のxxxxに設定したNICの名前が書いてる事を確認	
	Chain OUTPUT (policy ACCEPT 136 packets, 11680 bytes) pkts bytes target prot opt in out source destination 0 0 REJECT all any **xxxxxx** anywhere anywhere reject-with icmp6-port-unreachable	

表 27：動作中の安全性の確認例③

③ セキュリティ装置のアプリが外にパケットを送信しないことを確認
セキュリティ装置のアプリをリブートした際に、セキュリティ装置のアプリがパケットを送信しないことを確認

項番	作 業 内 容	チェック欄
(A)	スイッチ、スイッチ制御用ノートPCの起動を確認	
	スイッチのLEDが正常に点灯している事を確認(スイッチの仕様に依存するため、スイッチの説明書を確認)	
	ノートPCにユーザ名、パスワードを入力し、ログインし、デスクトップ画面が表示される事を確認 (ノートPCに依存するため、ノートPCのユーザ名、パスワードを確認)	
(B)	スイッチとノートPCを接続し、ノートPCからスイッチにログイン	
	スイッチとノートPCをコンソールケーブルで接続	
	ノートPCのtera termを起動し、tera termのウィンドウが表示される事を確認	
	ノートPCのtera termのウィンドウで、"シリアル - スイッチに接続しているシリアルポート名" を選択	
	スイッチアクセスできた事を確認。(login画面が表示されることの確認)	
	スイッチにログイン(ユーザ名、パスワードはスイッチに依存するため、スイッチのユーザ名、パスワードを確認)	
(C)	スイッチの統計情報を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントを確認	
(D)	セキュリティ装置のターミナルを起動	
	アプリケーションから端末を選択	
	ターミナルウィンドウが起動される事を確認	
(E)	セキュリティ装置にて、suにログイン	
	#su△-	
	パスワードを聞かれるので、以下パスワードを入力	
	*	
	root権限でログインできた事を確認。(ターミナル画面のログインユーザ名がrootになっている事を確認)	
(F)	セキュリティ装置のアプリをリブート	
	以下のコマンドを入力。	
	#systemctl resetart app	
(G)	セキュリティ装置のアプリがリブート前から起動するまでの間、セキュリティ装置がパケットを送信していない事を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントが増加していないことを確認	
(H)	DBアプリをリブート	
	以下のコマンドを入力。	
	#systemctl restart db	
(I)	DBアプリがリブート前から起動するまでの間、セキュリティ装置がパケットを送信していない事を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントが増加していないことを確認	
(J)	管理画面アプリをリブート	
	以下のコマンドを入力。	
	#service mng restart	
(K)	画面管理アプリがリブート前から起動するまでの間、セキュリティ装置がパケットを送信していない事を確認する。	
	セキュリティ装置に接続しているミラーポートのパケットカウントが増加していないことを確認	

最後に、正常動作の確認の実施例を表 28 に示す。ここでは、セキュリティ装置の正常動作を装置の管理画面から確認している。なお、疑似攻撃を行ってアラートが発報される等の確認は対象外としている。

表 28：セキュリティ装置のアプリの動作確認

① セキュリティ装置のアプリの動作確認

項番	作 業 内 容	チェック欄
(A)	管理画面操作用ノートPCの起動を確認	
	ノートPCにユーザ名、パスワードを入力し、ログインし、デスクトップ画面が表示される事を確認 (ノートPCに依存するため、ノートPCのユーザ名、パスワードを確認)	
(B)	管理画面操作用ノートPCを接続し、管理画面を起動	
	セキュリティ装置とノートPCをLANケーブルで接続	
	ノートPCで、Firefoxを立ち上げる	
	Firefoxのアドレスバーに以下を入力	
	http://"セキュリティ装置のIPアドレス"	
	セキュリティ装置の管理画面が表示されることを確認。	
(C)	管理画面で、対象システムのトラフィック情報が表示されることを確認	
(D)	セキュリティ装置がホワイトリストを生成できることを確認	
	管理画面で、ホワイトリスト生成ボタンを押下	
	ホワイトリスト生成が完了したら、ホワイトリストの内容を確認	
	(IPアドレスなどから対象システムのホワイトリストとして妥当であることを確認)	
(E)	セキュリティ検知一覧を確認	
	管理画面で、アノマリー覧画面を表示し、アノマリが検出されていないことを確認	

6章　運用フェーズ

6.1 運用フェーズの実施内容

本フェーズでは、対象システムにセキュリティ装置を導入した後で、対象システムのセキュリティインシデントを監視し、インシデント発生前の事前対処や、インシデント発生時の迅速な対応を行う。本節では、運用フェーズの実施内容として、セキュリティ運用を行うための組織体制、定常運用時の実施内容、インシデント発生時の実施内容をそれぞれ説明する。

6.1.1 組織体制

セキュリティ運用を推進するための組織体制の例を図 23 に示す。各組織の役割は事業者によって異なるが、本書では以下のような役割を持つものと定義する。重要インフラ事業者は、これらの役割を果たす組織を、事業社内に新たに設置するか、外部サービスを活用することで準備する必要がある。

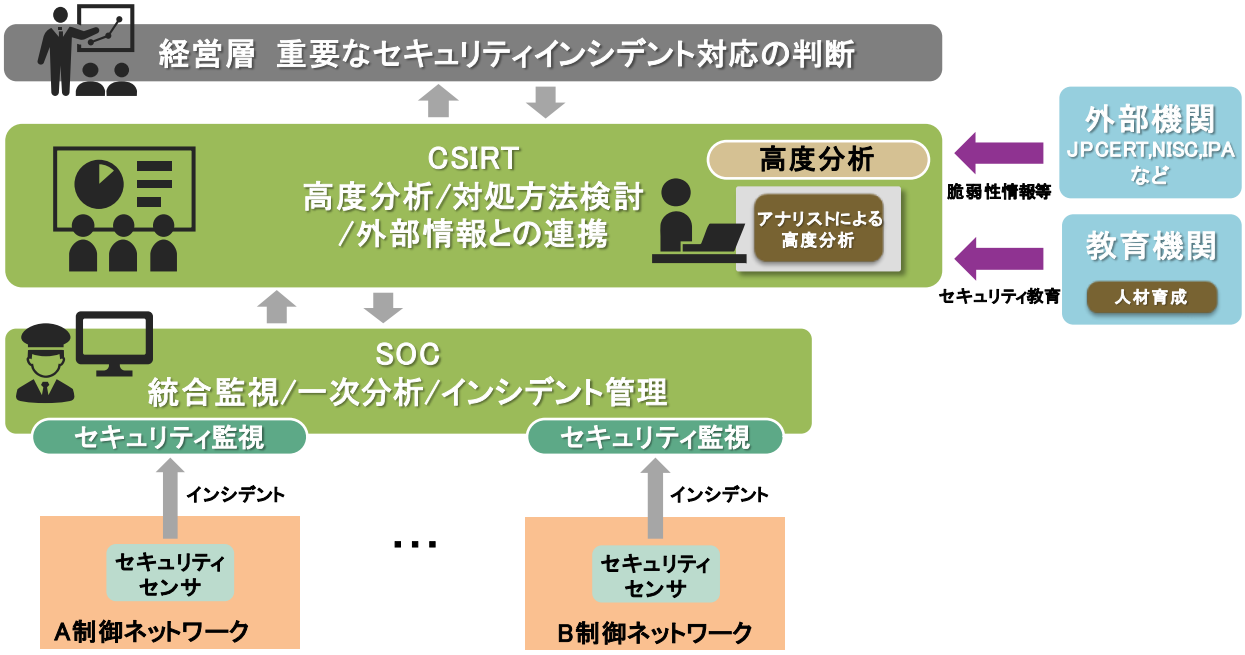

図 23：一般的なセキュリティ運用の組織体制の例

- SOC：Security Operation Center
  対象の制御システムを監視して、インシデント検知のための一次分析や管理を行う。
- CSIRT：Computer Security Incident Response Team
  SOC でインシデントを検知した場合に、そのインシデント対応として高度分析や対処方法の検討を行う。また、外部の団体／組織との情報連携を行い、最新の脅威情報の共有を行う。

【本フェーズで考慮すべきポイントを、重要ポイント 8～10 に記載】

6.1.2 定常運用時の実施内容

定常時におけるセキュリティ運用の実施内容を図 24 に示す。定常時には、CSIRT は外部のセキュリティ組織や他団体が共有する脆弱性情報等を監視し、当該脆弱性が自組織に関連するかどうかを判断する。自組織に関連する脆弱性情報である場合には、SOC や現場の運用者に情報を展開するとともに、対策方針の検討を行い、適切なタイミングで脆弱性への対処を行う。

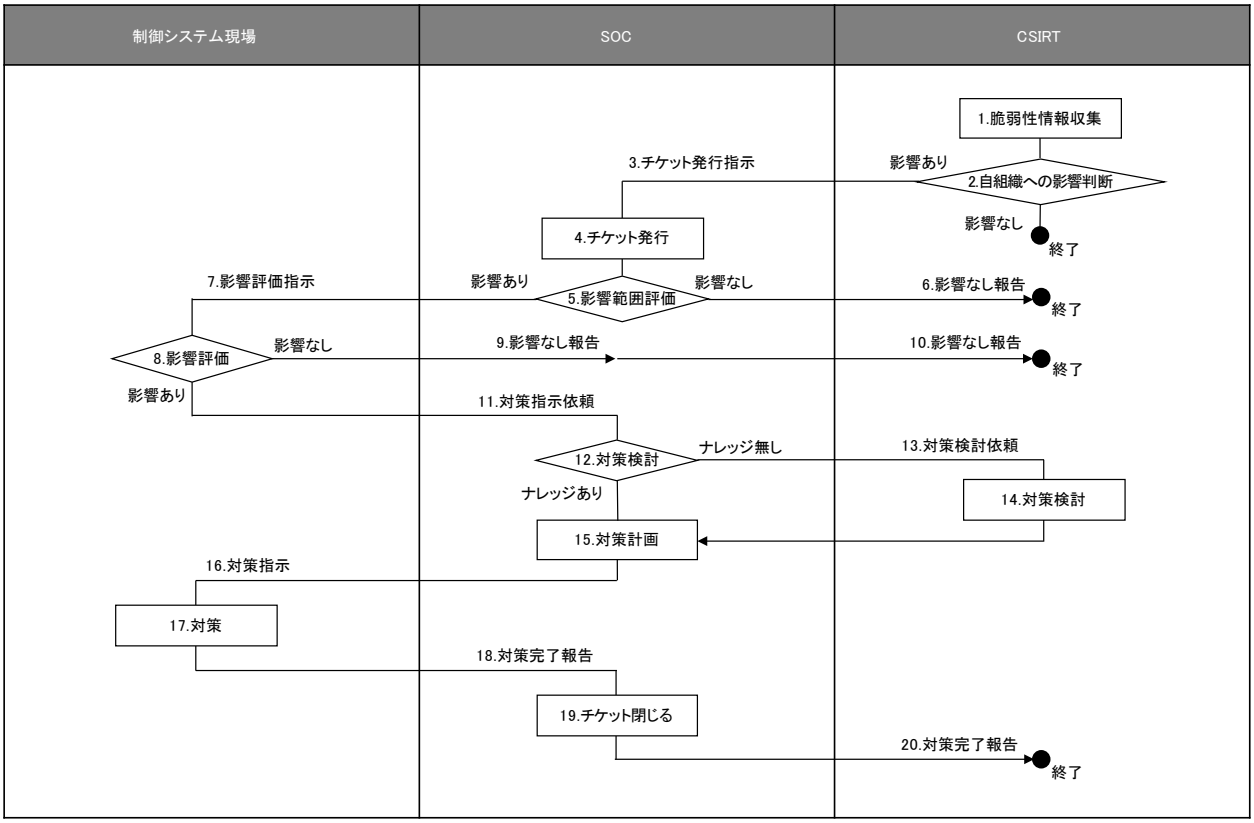

図 24：定常運用時の実施内容

【本フェーズで考慮すべきポイントを、重要ポイント 11、12 に記載】

6.1.3 インシデント発生時の実施内容

インシデント発生時におけるセキュリティ運用の実施内容を図 25 に示す。インシデント発生時には、対象システムで発生したアラートを基に、SOC がインシデント発生か誤検知かを一次分析して判断する。インシデント発生と判断した場合、CSIRT へインシデント情報が連絡され、CSIRT で高度分析や対処法の検討を行う。

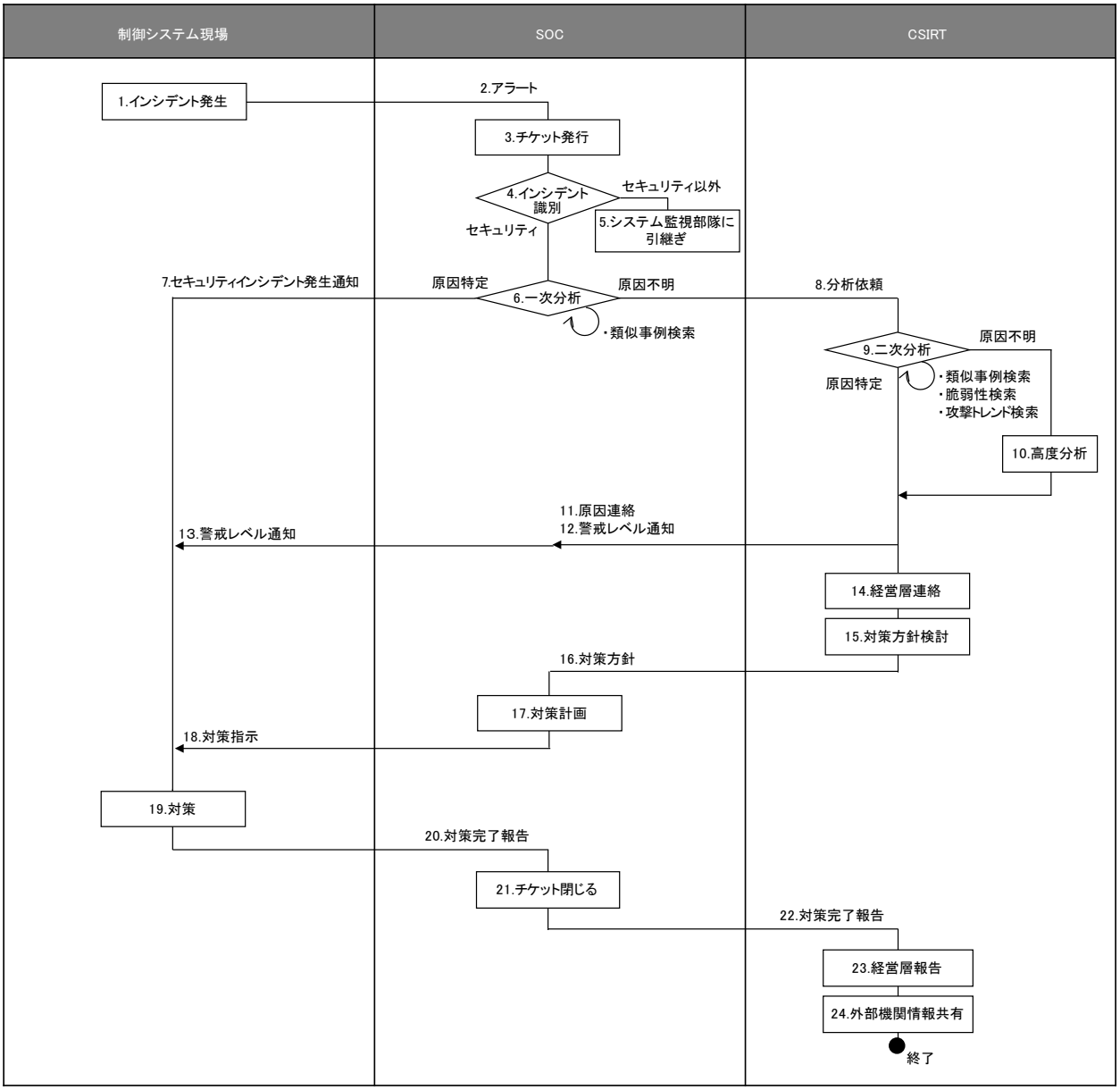

図 25：インシデント対応時の実施内容

【本フェーズで考慮すべきポイントを、重要ポイント 13 に記載】

6.2 運用フェーズにおける重要ポイント

運用フェーズで、特に考慮すべきポイントを記載する。

表 29：運用フェーズにおける重要ポイント一覧

#	タイトル	関連節
重要ポイント8.	組織の特徴に合わせたセキュリティ組織体制構築	6.1.1
重要ポイント9.	セキュリティ対応組織に必要な人材確保	6.1.1
重要ポイント10.	インシデント対応時の役割明確化	6.1.1
重要ポイント11.	システムの状況変化を考慮した運用方針整備	6.1.2
重要ポイント12.	把握しづらい業務・通信への対応	6.1.2
重要ポイント13.	サービス継続を第一優先としたインシデント対応	6.1.3

重要ポイント８ ： 組織の特徴に合わせたセキュリティ組織体制構築

（１）ポイント

SOC や CSIRT の組織構成は、重要インフラ事業者の特徴に合わせた体制を構築する。

（２）解説

重要インフラ事業者や制御システムは、様々なサービス／業務体系や特徴を持っている。例えば、複数の工場を有する事業者では、各工場でインシデントの早期発見・解決が必要となる。このため、各工場にセキュリティ関係組織を配置し、工場内で早期対処が可能な体制にすることが考えられる。

また、システム全体がネットワークに接続されているような事業者では、システム全体を監視してインシデントの早期発見・解決が必要となる。このため、システム全体に対応するセキュリティ関係組織を配置することが考えられる。

（３）実施例

各工場に SOC を配置したセキュリティ組織構成の例を図 26 に示す。

工場内に SOC を設置することで、セキュリティインシデント発生時に工場内で一次分析・一次対処を早期に実施できる。全社向けの SOC および CSIRT は、制御系／情報系の両システムを対象とし、工場 SOC に対しては高度分析等を支援する。

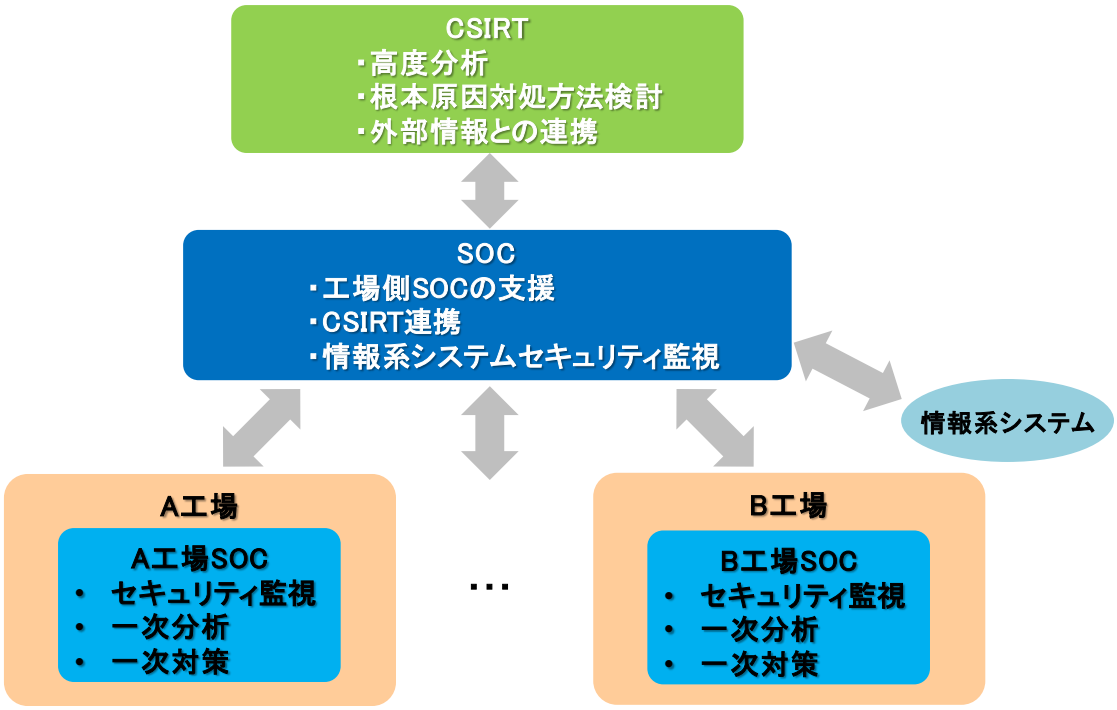

図 26：各工場に SOC を設置したセキュリティ組織構成の例

重要ポイント９ ： セキュリティ対応組織に必要な人材確保

（１）ポイント

インシデント対応を適切に実施するには、セキュリティの知識と、システムの知識の両方が必要であり、そのような人材をセキュリティ対応組織として確保することが重要である。

（２）解説

対象システムでは、エラーログやアラートが発報された場合に、それが故障によるものなのか、セキュリティインシデントによるものなのかを判断しなければならない。また、セキュリティインシデントに迅速に対処するには、サービス／業務情報を把握しておかなければならない。このような判断をするには、セキュリティの知識だけでなく、システムの知識も必要であるため、その両方を持つ人材を組織内で確保することが重要である。つまり、システム知識を持つ組織内の人員に、セキュリティ知識を習得させる必要がある。

ただし、そのような人材を確保するのが難しい場合には、セキュリティに特化した人材／組織を、システムの運用チームに合流させることで、システム知識を習得することも考えられる。

なお、組織内の人員にセキュリティ知識を習得させるための活動として、「戦略的イノベーション創造プログラム(SIP)／重要インフラ等におけるサイバーセキュリティの確保／(b4) セキュリティ人材育成」での成果を活用することが考えられる。

（３）実施例

重要インフラ事業者のサービス／業務の複雑さを考慮すると、業務知識を持つ従業員に対してセキュリティ知識を教育していくことが考えられる。このような教育の実現例として、重要インフラ事業者を対象にしたセキュリティ教育プログラムを提供しているサービス [14]がある。このようなサービスを利用して、重要インフラ事業者の環境を模擬的に再現した IT/OT システムの環境を用いて、組織内の現場部門から経営部門を対象に、サイバー攻撃発生時のインシデント対応の訓練ができる

[14] http://www.hitachi.co.jp/products/it/security/solution/securitymanagement/cyber/index.html

重要ポイント 10 ： インシデント対応時の役割明確化

（1）ポイント

セキュリティ組織体制を構築する場合には、インシデント対応時の役割分担を明確化し、迅速な行動・判断ができるように準備する。

（2）解説

CSIRT と SOC の役割分担は、明確に定められているものではなく、組織毎に異なる可能性がある。組織に合う役割を割り当てることで、スムーズな運用・インシデント対応ができるように考慮する。

例えば、インシデント対応の主体は CSIRT であり、SOC は CSIRT の作業をサポートする位置づけとする等の役割分担が考えられる。

（3）実施例

セキュリティ組織の役割分担の例を図 27 に示す。

下記の例では、セキュリティインシデント発生時、事業者はシステム毎に設置された SOC／CSIRT でインシデントの管理・対処方法検討等を行い、一次分析・高度分析はシステムベンダの SOC／CSIRT で対応するように役割分担している。各システムの有識者が集う全社向けに設置された CSIRT では、外部機関への連携や他システムへの拡散防止等の役割を担っている。全社向け CSIRT で特に重要だと判定されたセキュリティインシデントに対しては、経営層が対応を判断する。

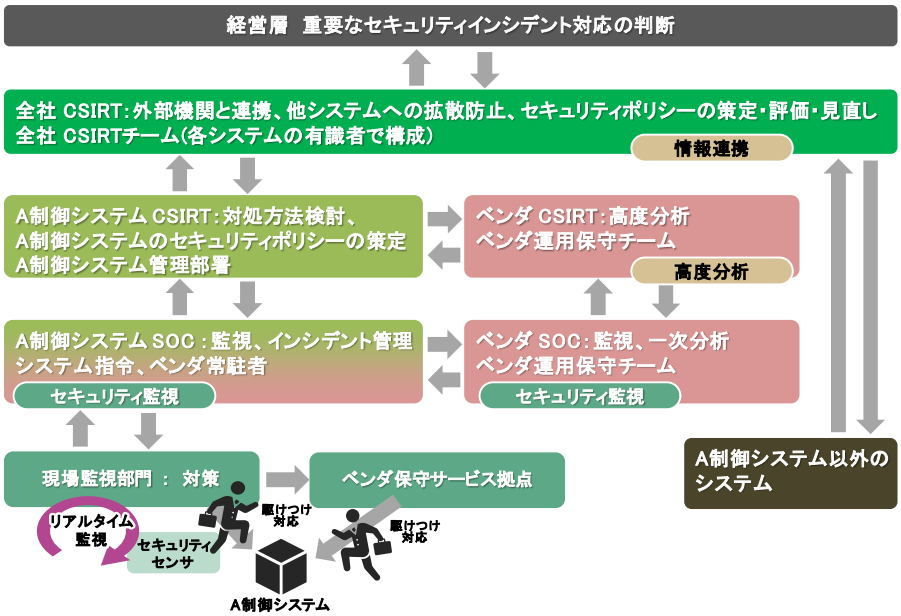

図 27：セキュリティ組織の役割分担の例

重要ポイント 11 ： システムの状況変化を考慮した運用方針整備

（1）ポイント

対象システムに対するリスクの変化やシステムの拡張・変更が起こることを考慮し、システムの状況変化に対応可能なセキュリティ装置の運用方針や運用手順をあらかじめ検討する。

（2）解説

重要インフラシステムは、サービス／業務を継続的に稼働しながら、システムの拡張や変更をしていくことが多く発生する。また、システムに対する攻撃手法等も常に進化しており、新たなリスクが発生する可能性もある。このため、セキュリティ装置では、あらかじめ定義したルール（ホワイトリストやブラックリスト）を基にセキュリティインシデントを検知する場合が多いが、保護対象のシステムの状況に変更が生じた場合には、これらのルールを再定義する必要があり、ルール再定義の手順等をあらかじめ設計・準備しておく必要がある。

（3）実施例

システム変更におけるルール再定義手順のイメージを図 28 に示す。

ルール定義（ホワイトリスト／ブラックリスト）を手動変更する場合は、システム変更前のルール定義を基にシステム変更完了までに変更内容に合わせて手動編集する。システム変更後に即時適用することで、変更後のシステムの監視を開始する。システム変更内容の把握、手動編集作業の実施等によって運用者負担が大きいが、システム変更後に即座にセキュリティ監視を開始できる。

ルール定義を自動再学習する場合は、システム変更後に一定の学習期間を置き、ルール定義の学習が成熟した後に、ルール反映を行い、変更後のシステムの監視を開始する。学習期間中はセキュリティ監視をできないが、運用者負担は小さい。

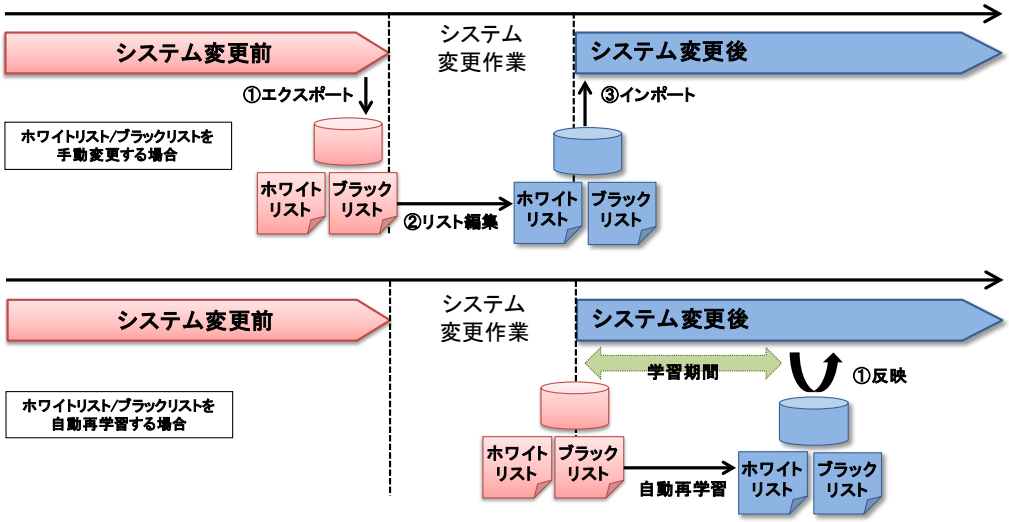

図 28：セキュリティ装置におけるルール再定義手順のイメージ

重要ポイント 12 ： 把握しづらい業務・通信への対応

（１）ポイント

業務が複雑で、長年使用しているシステムが混在しているような重要インフラシステムでは、把握しづらい業務・通信が存在する。そのため、そのシステムの特徴を踏まえたセキュリティ監視を実施する必要がある。

（２）解説

重要インフラシステムは、規模が大きく、業務が複雑になる場合が多い。また、長年使用しているシステムが多数混在していることで、詳細な仕様を常に正確に把握することが困難であるという特徴がある。詳細な仕様を把握しづらい場合の例としては、システムが古く仕様書が失われている場合、通信が非公開の場合等が考えられる。

このような特徴から、セキュリティ監視をするためのルールを仕様書から生成するだけでは、適切な監視ができない恐れがある。このため、例えば仕様書に基づいた監視のルール生成に加えて、通信情報（パケットキャプチャデータ）等に基づいた監視のルール生成も併用することで、把握しづらい業務・通信についても監視が可能になると考えられる。なお、「戦略的イノベーション創造プログラム(SIP)／重要インフラ等におけるサイバーセキュリティの確保／(a2) 制御・通信機器および制御ネットワークの動作監視・解析技術」の研究開発の成果を活用し、（株）日立製作所が開発したセキュリティ監視技術（HAD：Hitachi Anomaly Detector[15]）では、仕様書に基づいた監視ルール生成および通信情報からの監視ルール生成の両方に対応可能である。

（３）実施例

通信情報から監視ルールを生成する場合と、仕様から監視ルールを生成する場合の手順イメージを図 29 に示す。

通信情報から監視ルールを生成する場合は、通信情報から自動学習して監視ルールを生成するため、仕様不明なシステムに適用可能となる。

また、仕様から監視ルールを生成する場合は、通信情報から自動学習した監視ルールを基に、仕様書に照らし合わせて確認して、低頻度通信等の追加したい監視ルールの編集を行い、新たな監視ルールとして生成する。仕様が明らかで運用者自ら監視ルールの定義が可能なシステムに適用可能である。

---

[15] https://www.hitachi.co.jp/products/it/network/communimax/infra/had/index.html

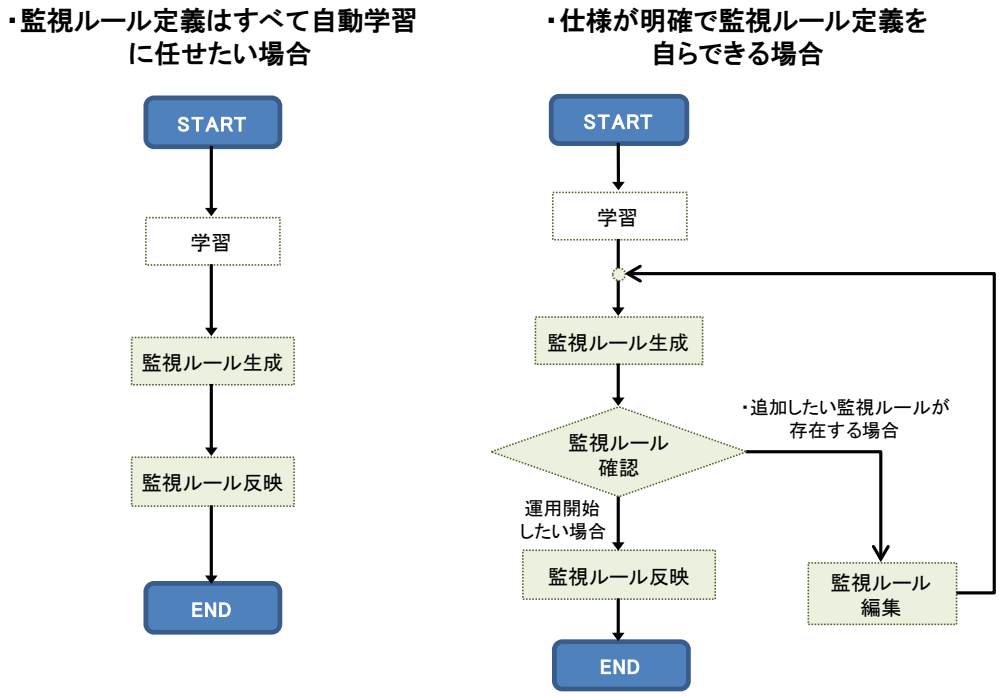

図 29：監視ルール生成手順イメージ

重要ポイント 13 ： サービス継続を第一優先としたインシデント対応

（1）ポイント

重要インフラシステムでインシデントが発生した場合には、原因究明の前にサービス継続を第一優先とした一次対処の実施が必要である。

（2）解説

重要インフラシステムは、サービスが停止した場合の影響が広範囲かつ重大な事象につながる恐れがある。このため、サービス継続を第一優先とした対処として、原因を究明する前に感染の封じ込めや縮退運転に切り替える等の一次対処を実施する必要がある。

例えば、インシデント発生時には以下のようなステップでインシデント対応を行う。

(A) トリアージ ： インシデント検知か、誤検知かを判断する。

(B) 一次対処 ： 被害拡大防止や、サービス継続を目的とした対処を行う。
一次対処の例としては、被害拡大防止のための一部通信の遮断、待機系への切り替え等がある。

(C) 高度分析・根本対策 ： 感染範囲の特定や原因究明、根本対策の検討、再発防止策の検討を行う。
本ステップでは、様々な機器からログ等の情報を収集し、高度な分析を行う。

（3）実施例

サービス継続を第一優先としてインシデント対応例を図 30 に示す。

インシデント検知時に、分析・対策の前にサービス継続を優先して、インシデント発生個所を待機系に切り替え、切り離しを実施する。

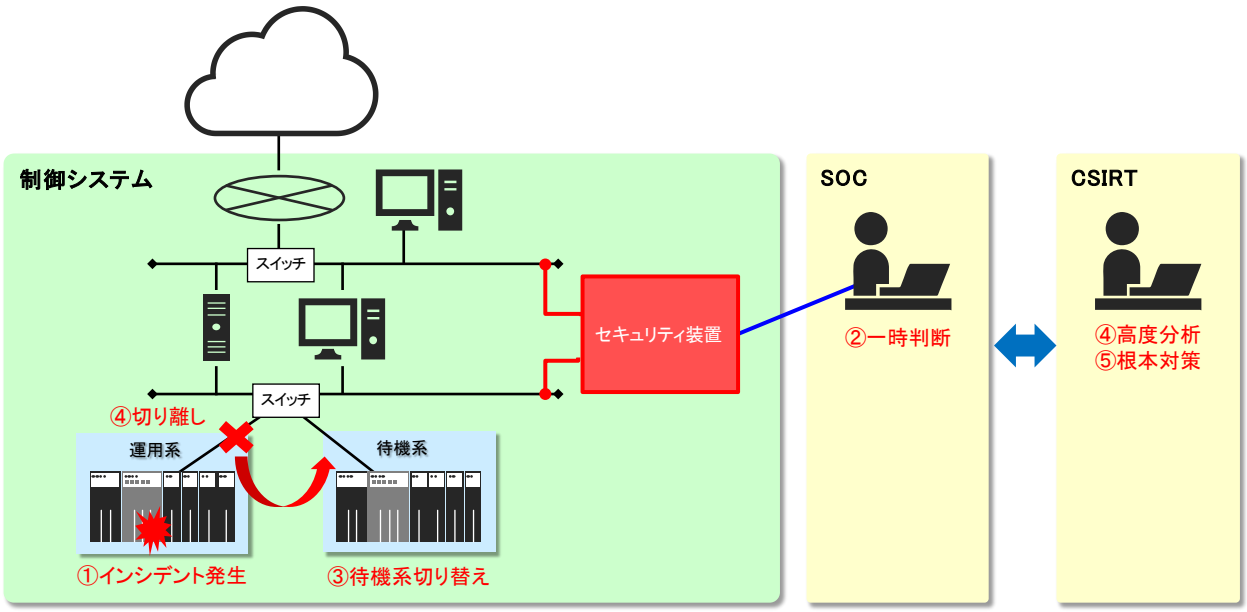

図 30：サービス継続を第一優先としたインシデント対応例

参考文献

[i] IEC：62443-2-1 “Industrial communication networks – Network and system security – Part2-1:Establishing an industrial automation and control system security program”, (2010)

[ii] NISC：「重要インフラの情報セキュリティ対策に係る第４次行動計画」, https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf, (2017)

[iii] 熊谷洋子, 松原佑生子, 内山宏樹, 鍛忠司, 藤田淳也, 中野利彦：「制御システム向け事業レベルでのリスク分析手法の提案」, 情報処理学会論文誌, Vol.60 No.9, pp.1518-1527 (2019)

[iv] 内山宏樹, 松原佑生子, 熊谷洋子, 鍛忠司, 藤田淳也, 中野利彦：「社会インフラ向け事業レベルでのリスク分析手法の提案」, 【C】平成 30 年電気学会電子・情報・システム部門大会プログラム, No.TC7-4, pp302-306 (2018)

[v] 経済産業省, 「サイバー・フィジカル・セキュリティ対策フレームワーク」, https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf, (2019)

[vi] 新 誠一ほか, "IoT 時代のサイバーセキュリティ―制御システムの脆弱性検知と安全性・堅牢性確保 単行本", NTS, (2018)

[vii] 情報処理推進機構“重大な経営課題となる制御システムのセキュリティリスク”, https://www.ipa.go.jp/files/000044733.pdf , (2015)

[viii] ISO/IEC：31010 “- Risk management - risk assessment technologies” , (2019)

[ix] ISO/IEC：15408 “Common Criteria”, (2017)

[x] NIST：“Cybersecurity Framework version 1.1” , (2018)

[xi] 太田原千秋, 内山宏樹, 井口慎也, 萱島信：「社会インフラシステムを対象としたテンプレート活用型セキュリティ対策立案手法の提案」, 情報処理学会論文誌, Vol.58 No.9, pp.1523-1534 (2017)

[xii] IPA：「重要インフラの制御システムセキュリティと IT サービス継続に関する調査」, https://www.ipa.go.jp/files/000013981.pdf（2009 年）

[xiii] IEC：62443-3-3 ”Industrial communication networks – Network and system security –Part 3-3: System security requirements and security levels”, (2013)