制御システムの
セキュリティリスク分析ガイド

～セキュリティ対策におけるリスク分析実施のススメ～

2017 年 10 月

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

目 次

図 目 次

表 目 次

公開にあたって

様々な「モノ」にソフトウェアが組み込まれ、通信機能を保有する装置やシステムが増加する IoT（Internet of Things）技術の適用と普及・拡大において、コスト（製造及び運用管理両面）の削減や利便性の向上を達成する反面、明らかに増大するセキュリティ脅威群とそれらに対する備え（セキュリティ対策）が課題になっている。IPA では、2007 年頃からこれらの課題を認識し、組込みシステムのセキュリティに対する様々な調査報告やガイドの策定と公開を実施してきた[1]。その一環として、2010 年から制御システムのセキュリティ（脅威と対策）の調査に取り組んできた[2]。その中では、セキュリティ基準の選定や、セキュリティレベルやセキュリティマネージメントシステム（CSMS: Cyber Security Management System）を評価認証する仕組みの確立を行い、IEC 62443 の活用の推進や CSMS 適合性評価制度の立上げ等に寄与してきた[3]。また、実システムの評価として、スマートメーターシステムのセキュリティリスク分析（以下、リスク分析と記載）や[4]、更に重要インフラを支える様々な分野の制御システムのリスク分析を実施している[5]。

実効的なセキュリティ対策を実施するためには、保護資産の明確化とそれらに対する脅威や脆弱性の評価によってリスクを算定するリスク分析は、非常に重要で不可欠なプロセスである。例えば、ISMS（Information Security Management System）や CSMS 等、統合的なセキュリティ対策であるセキュリティマネージメントシステムの適合性評価制度では、リスク分析の実施を審査（認証）の必須要件としている。しかしながら、制御システム分野においては、リスク分析を具体的に手引きする適切なガイドが存在していないことが、その実施を困難にしている。

こうした背景を受け、以下に示す目的のもと、本ガイドを作成・公開することとした。

- リスク分析の全体像の理解を深め、その取り組みを促すこと
- リスク分析を具体的に実施するための手順や手引きを示すこと
- IPA において実践したリスク分析でのノウハウを手引きに織り込むこと

本ガイドを活用することで、セキュリティ対策におけるリスク分析作業をより身近に感じ、制御システムのリスク分析に取り組んでいく組織が増加すること、結果として各組織におけるセキュリティレベ

---

[1] IPA: IoT のセキュリティ
https://www.ipa.go.jp/security/iot/index.html
[2] IPA: 制御システムのセキュリティ
https://www.ipa.go.jp/security/controlsystem/index.html
[3] IPA: 制御システムにおけるセキュリティマネージメントシステムの構築に向けて ～IEC62443-2-1 の活用のアプローチ～
https://www.ipa.go.jp/security/fy24/reports/ics_management/index.html
[4] 原子力損害賠償・廃炉等支援機構: 東京電力スマートメーターシステムの情報セキュリティ対策に関する意見
http://www.ndf.go.jp/press/at2015/20150731bt.pdf
[5] 経済産業省: 平成 27 年度補正予算の概要（PR 資料）（p.21）
http://www.meti.go.jp/main/yosan/yosan_fy2015/hosei/pdf/pr_01.pdf

ルの抜本的な向上と継続的な維持見直しが達成されることを期待する。

なお、本書は制御システムのセキュリティリスク分析のガイドの位置付けではあるが、詳細リスク分析の手法自体は、情報システムでも共通である。個々の資産に注目したリスク分析（本書では資産ベースのリスク分析）は通常実施されているが、攻撃者の視点に立ったリスク分析（本書では事業被害ベースのリスク分析）の手法も解説しており、情報システムのリスク分析においても、本書は参考になるものと考える。

また、本書の後半では、リスク分析結果の検討後に、必要に応じて実機を用いた環境（本番環境または模擬環境）での検証（セキュリティテスト）を実施する際の手引きを解説している。更に、リスク分析を実施する上でも参考となる、特化した攻撃（標的型攻撃、内部不正等）に対する対策の全体像、セキュリティを検討する上で固有の技術（暗号技術、ファイアウォール等）に関する解説、それらのセキュリティ対策の状況を確認する様々なチェックリスト等を掲載している。これらは、制御システムに限らず、広く一般のシステムのセキュリティ対策の検討に活用できる内容となっている。

本書が、リスク分析の実施の促進、セキュリティ対策の向上に活用されることを期待している。

2017 年 10 月 2 日
神無月　桜紅葉の候

独立行政法人　情報処理推進機構	辻　　宏郷
独立行政法人　情報処理推進機構	岡下　博子
独立行政法人　情報処理推進機構	工藤　誠也
独立行政法人　情報処理推進機構	塩田　英二
独立行政法人　情報処理推進機構	福原　　聡
独立行政法人　情報処理推進機構	小助川　重仁
独立行政法人　情報処理推進機構	木下　　仁
独立行政法人　情報処理推進機構	吉田　和之
独立行政法人　情報処理推進機構	桑名　利幸
独立行政法人　情報処理推進機構	金野　千里

1. セキュリティ対策におけるリスク分析の位置付け

1.1. 制御システムにおけるセキュリティ対策の必要性とアプローチ

1.1.1. 制御システムにおけるセキュリティ対策の必要性

従来、制御システムは、固有システムで構成され、外部ネットワークや共用システムとは接続されていない等の認識の下で、セキュリティの脅威は殆ど問題視されてこなかった。しかし、近年、以下の様なシステム構成や利用環境の変化、システムの特性や位置付け、及び脅威の増大を背景に、セキュリティ対応の必要性が非常に高まってきている。

（1）構成システム、コンポーネントの変化

- システムを構成するコンポーネントとして、Windows や UNIX といった汎用のプラットフォームが活用されてきている。
- システムでの通信は、汎用で標準的なプロトコルを採用し、その上に制御用データを乗せる形で利用されてきている。

（2）外部ネットワークとの接続、外部からの記憶媒体の持込み

- 管理のために、情報システムとのネットワーク接続経路を有しているケースも出てきている。
- リモートメンテナンス等、保守管理の利便性から、外部との通信が利用されるケースも出てきている。
- 制御の利便性から、無線 LAN が使われるケースも出てきている。
- システムやコンポーネントのパラメータ変更のため、外部記憶媒体が利用されるケースも多く見受けられる。

（3）システムの特性、位置付け

- システムの利用期間が、10～20 年と非常に長期間の利用が前提とされている（情報システムで用いられている OS 等のサポート期限をはるかに超えている）。
- 24 時間、365 日の可用性が、最も重要な要件として挙げられている。
- 社会基盤、産業基盤を支えており、攻撃等で稼働が阻害されるとなると、社会的な影響、事業継続上の影響が非常に大きい。

（4）脅威、事件・事故の出現と傾向

- 2010 年に発覚したイランの原子力設備を標的としたマルウェア（ワーム）Stuxnet の出現により、制御システムを周到に狙った攻撃が世界を震撼させた[6]。
- 制御システムの構成機器に関する脆弱性の報告が増加している[7]。
- 生産ラインや制御システム等への標的型サイバー攻撃やマルウェア感染等の報告が増加してきており、海外ではそれらによる大規模停電等も発生している[8]。

[6] 付録 C. 制御システムのインシデント事例 #3 参照
[7] NCCIC: ICS-CERT Annual Vulnerability Coodination Report 2016
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202016_Annual_Vulnerability_Coordination_Report.pdf
[8] 付録 C. 制御システムのインシデント事例 #16 参照

1.1.2. セキュリティ対策のアプローチ

前述の背景の下で、制御システム分野でも、様々なセキュリティ基準が策定されている。個別の業界分野（電力、交通、石油・化学等）に特化した基準や、業界に依らず汎用的に活用できることを意図した基準も策定されている。また、セキュリティに対応しようとすると、そのシステムを利用する組織全体のセキュリティマネージメントに関する課題から、利用するシステムの構築に関する課題、更にはシステムを構成する各機器・デバイスに関する課題等、多岐に渡る検討が必要となる。

日本では、特定分野に限定されず汎用的な基準であり、セキュリティマネージメントからシステムや機器・デバイスまでをカバーすることから、国際標準である IEC 62443（Industrial communication networks -Network and system security-）[9]を選定し、その活用を推進している。図 1-1 に、IEC 62443 の構成を示す。

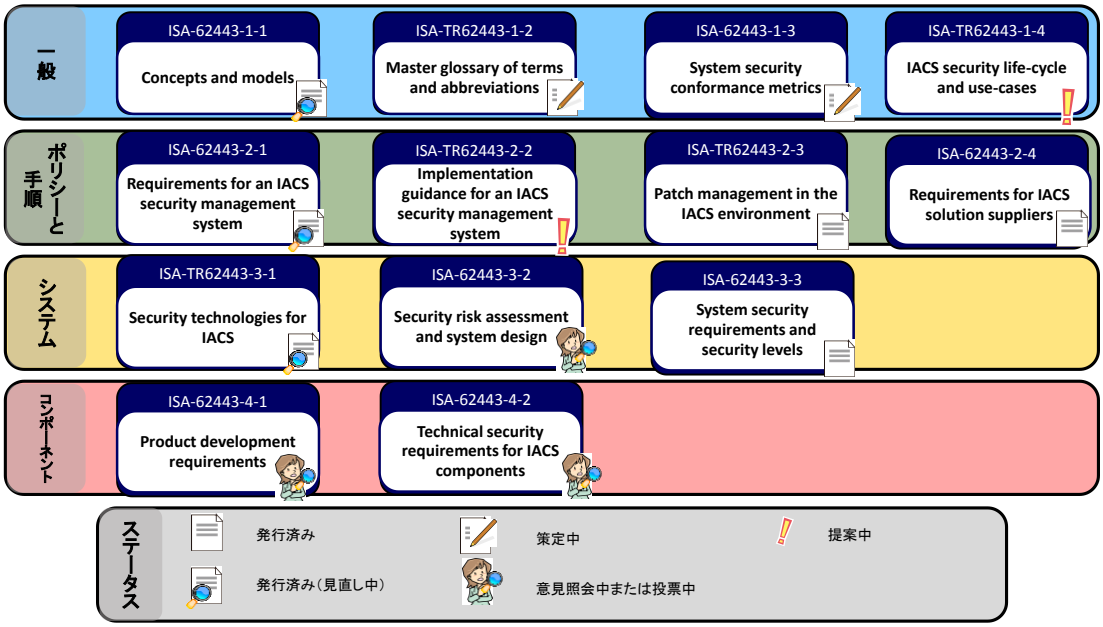


図 1-1 IEC 62443（ISA-62443）の構成

（出典）ISA99 Committee「ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security」（2017 年 8 月時点）[10]を基に IPA が編集

IEC 62443 を基にした、制御システムで使用される制御機器のセキュリティの認証制度[11]、及び制御システムを運用する組織におけるセキュリティマネージメントシステムの適合性評価制度[12]も、

[9]国際電気標準会議（IEC: International Electrotechnical Commission） TC 65/WG 10 と国際計測制御学会（ISA: The International Society of Automation）ISA99 Committee により開発されている、制御システムのセキュリティに関する国際標準規格。ISA から発行される場合は、ISA-62443 の規格番号が付与される。

[10] http://isa99.isa.org/

[11] EDSA（制御システム機器の評価認証制度） http://www.css-center.or.jp/

[12] CSMS（セキュリティマネージメントシステムの適合性評価制度） https://www.jipdec.or.jp/

2014 年より開始されている。

事業者にとって、抜本的かつ継続性のあるセキュリティ対策を実現しようとするには、セキュリティマネージメントシステムの構築は不可欠となる。この構築にあたって、最も基本となる作業が、保護対象となるシステムのセキュリティの実態を把握するリスク分析である。リスク分析に基づいて、セキュリティ対策を計画的に進めることが、最も効果的なアプローチである。

1.2. リスク分析の位置付けと重要性

リスク分析とは、保護すべきシステムやそれによって実現している事業（サービス等含む）に対する脅威と被害のレベル（可能性と大きさ等）を明確にするプロセスである。

評価対象であるシステムや事業を、

① 評価対象（保護すべきシステムや事業）の価値（重要性）、想定される被害の規模・影響
② 評価対象に対して想定される脅威とその発生の可能性
③ 想定される脅威が生じた際の受容可能性（評価対象の脆弱性）

の 3 つの評価指標によって評価し、保護すべき対象が損なわれる「可能性と被害のレベル」を相対評価可能なリスク値として算定する。このリスク値を明確にすることにより、被害の発生確率と影響度を把握し、優先順位付けしたリスク対策計画を立案することが可能となる。例えば、①と②が given であれば、③の対策を強化することによって、リスク値は低減することができるが、リスク値の高い箇所の特定、該当箇所の対策強化によって、全体的なリスク値のレベルをどの程度低減できるかを検討可能となる。即ち、保護すべきシステムや事業等を構成する対象におけるリスク値を明確化することにより、リスク低減に最も効果的な対策強化箇所を特定すると共に、残留しているリスクのレベル把握が可能である。

ここで、①の評価対象としては、様々な「保護すべきもの」を定義することが考えられる。例えば、システムを構成する物理的な資産、そのシステムに格納されている情報資産、更には事業自体とその継続性を評価対象とすることも可能である。評価対象の洗い出しや想定される脅威の明確化の具体的な手法については、3 章で解説する。

経営課題でもあるセキュリティ対策を実施する上で、重要な観点は、効果的な対策の選定、コストの最適化、継続的（残留脅威や新たな脅威に対する対応可能）なスキームの確立である。

これらを明確かつ体系的に実現するためには、リスク分析が不可欠となる。リスク分析を実施することによって、保護すべきシステムや事業を明確化し、それに対して想定される脅威を明確化し、その脅威に対する対策を明確化し、限られたコスト（予算）の中でリスク低減に効果的な対策を優先順位付けして実施する計画を立案・決定することが可能となる。こうしたプロセスを経て、最初のリスク分析（第一ステップ）で実施された対策による脅威への対策実施状況やリスクの低減度、対策が見送られた脅威によるリスクの残留度を評価する。また、時間の経過に従い、システムやサービス上に新たな脅威が発生することが想定される。それらを受けて、再度リスク分析（次のステップ）を実施し、その残留脅威に対する対策の検討・実施によって、継続的にリスクの低減を図っていくことが可能となる。いわゆる、PDCA（plan-do-check-act）のサイクルを継続的に回していくことが可能となる。図 1-2 に、セキュリティ向上の PDCA サイクルにおけるリスク分析の位置付けを示す。

まとめると、リスク分析は以下に示す効果があり、組織がセキュリティ対策を行う上で必要不可欠なプロセスである。

- 実効的なリスクの低減の実現
- 効果的な投資の実現（追加対策、有効なテスト箇所の抽出）
- PDCA サイクルの確立とセキュリティの維持向上を継続するためのベース

従って、リスク分析は一定の工数を要するプロセスであるが、制御システムのセキュリティの維持・向上の長期的な視点に立てば非常に有効な施策であり、各組織において実施することが重要である。

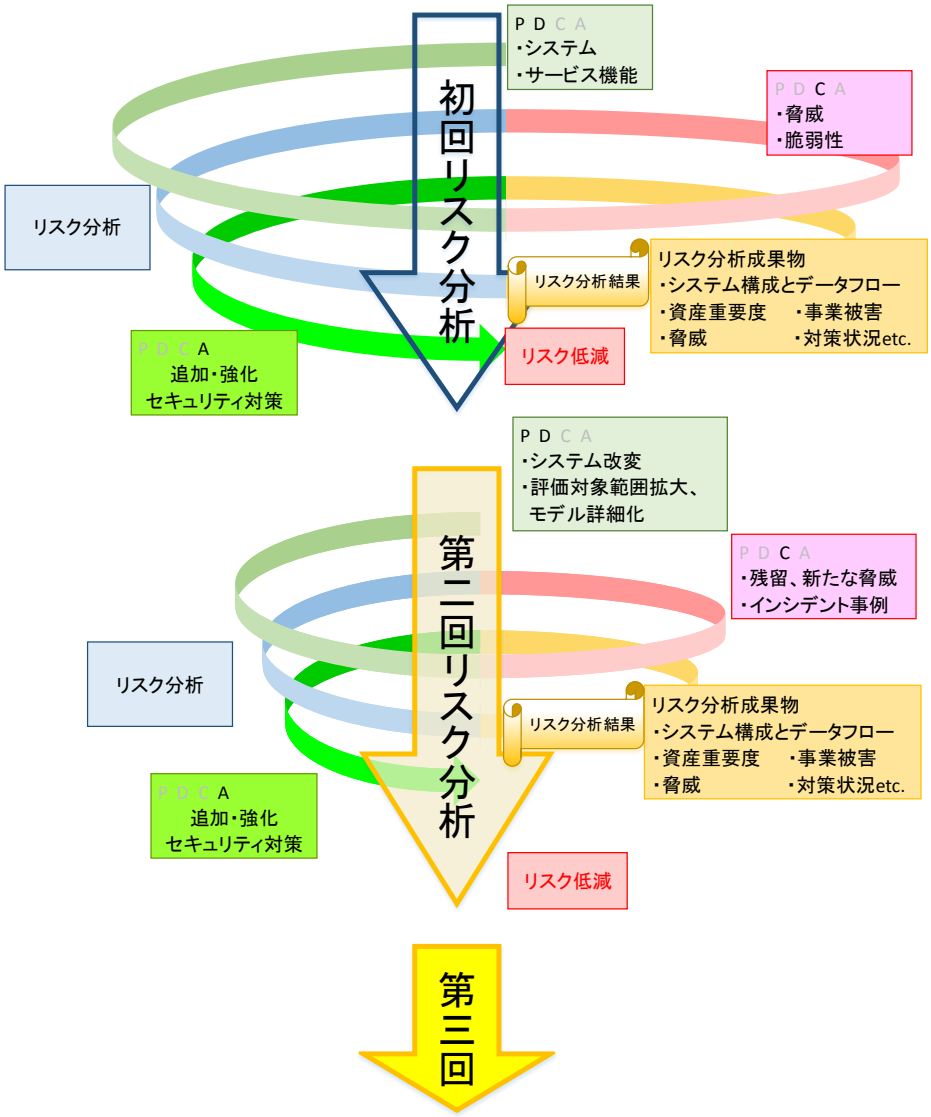


図 1-2 セキュリティ向上の PDCA サイクルにおけるリスク分析の位置付け

2. リスク分析の全体像と作業手順

2.1. リスク分析の全体像

(1)リスク分析の全体像(種別含む)

リスク分析には、様々な手法が存在する。

① **ベースラインアプローチ**
既存の標準や基準をもとに、想定する典型的なシステムに対して、予め一定の確保すべきセキュリティレベルを設定し、それを達成するためのセキュリティ対策要件を定め、評価対象となるシステムの対策の適合度等をチェックする。

② **非形式的アプローチ**
組織や担当者の経験や判断によってリスクを評価する。

③ **詳細リスク分析**
評価対象のシステム自体に対して、そのシステムもしくはそれにより実現されている事業を、「重要度」(あるいは損なわれた場合の被害レベル)「脅威」「脆弱性」の評価指標の下で、リスクを評価する。

④ **組み合わせアプローチ**
複数のアプローチを併用し、作業の効率化、異なった評価視点の活用によって、分析精度の向上と、作業工数増大の回避を図る。

表 2-1 に、それぞれのリスク分析の長短比較を示す。

表 2-1 リスク分析手法の比較

リスク分析手法	長所	短所
ベースライン アプローチ	● 決められた対策要件をチェックすることにより、作業の工数は大きくない。 ● 既存の基準をもとにしているので、あるレベルの評価の目安としては利用できる。	● 対策基準に対する適合レベルのチェックであり、自分のシステムの状況に沿ったリスク分析にはなっていない。 ● 事業被害を起こさない裏づけには間接的にしかならない。 ● 未実施の対策群があった場合、自分のシステムに沿った選択基準が得られない。
非形式的 アプローチ	● 経験値を活用するので、属人的ではあるが工数は小さい。	● リスク分析にはなってない。 ● 起こりうる脅威、あるいは新たな脅威に対しての対応が困難である。 ● 属人的であり、継続的なセキュリティレベルの向上は困難である。
詳細リスク分析	● 自分のシステム自体に対する、正確なリスク分析が可能である。 ● 一度実施すると、それをベースに継続的なセキュリティレベルの向上が可能となる。 ● セキュリティ投資の優先順位等、組織として戦略的に検討していくことができる。	● システムの規模や手法によっては、かなりの工数がかかることがある。
組み合わせ アプローチ	● 上記、各手法の長所の取り込みの可能性である。 ● 上記、各手法の短所の改善の可能性がある。	● どう組み合わせるのか、それぞれのシステムや事業者によって異なってくるが、その指針は示されていない。

（2）詳細リスク分析の優位性

リスク分析の中でも、詳細リスク分析は、以下の点で、最も実態の把握と対策を検討するのに適している。

- 評価対象の実態に沿った評価を行うことで、評価対象のリスクを明確化できる。
- 対策の優先順位の客観的な決定と、リスク低減に最も効果的な選定が可能である。
  （組織内における対策の優先順位の共通の理解と認識を有することができる。）
- 一度確立しておくと、それをベースに、システムの拡張や新たな脅威の出現等にも継続的に見直しや更新をしていくことが可能である。

（3）詳細リスク分析の概要と長短解説

詳細リスク分析には、いくつかのアプローチがある。以下は、その概要である。

① 資産ベース

保護すべきシステムを構成する資産を対象に、各資産（サーバ、端末、通信機器等）に対して、その重要度（価値）、想定される脅威、脆弱性の3つを評価指標として、リスク分析を実施する。この場合のリスク値としては、想定される「脅威の受容の可能性とそれにより損なわれる資産価値」の相乗値を算出することになる。リスク値が高い脅威に対しては、その受容性を低減する対策の強化を検討することになる。

② シナリオベース

保護すべきシステムにおいて実現されている事業やサービスに対して、回避したい事業被害を定義し、発生した際の事業被害のレベル、その被害を起こしうる攻撃シナリオによる脅威、そのシナリオに対する脆弱性（そのシナリオの受容可能性）の3つを評価指標として、リスク分析を実施する。この場合のリスク値としては、攻撃シナリオの「成功可能性と発生する被害のレベル」の相乗値を算定することになる。リスク値が高い攻撃シナリオに対しては、その成功可能性を低減する対策の強化を検討することになる。

シナリオベースのリスク分析には、以下の 2 通りの解析手法が存在する。

- 攻撃ツリー解析（ATA: Attack Tree Analysis）
  攻撃者視点で、トップダウンに、誰が、どこから、どのルートを経由して被害発生を引き起こしうるかのシナリオを、攻撃ツリー（攻撃のステップからなる一連の攻撃フロー）として構成する。攻撃の侵入口は複数存在し、また攻撃経路も（下流に向けて）枝分かれして、事業被害を引き起こす攻撃へと連なる。こうして構成したツリーの各攻撃事象を受容してしま

うのかの脆弱性を評価して、攻撃ツリーの成立の可能性を算定する。

- フォルトツリー解析（FTA: Fault Tree Analysis）
  被害（インシデント等）事象を起点として、ボトムアップに、その被害に至る1ステップ前の攻撃事象を、更にそれを引き起こす1ステップ前の攻撃事象を順じ追跡するツリー（フォルトツリー）を構成して、攻撃の起点までを構成していく。当然、1ステップ前は、複数の事象に分かれることもあり、それに応じて（上流に向けて）枝分かれしていく。こうして構成したフォルトツリーを受容してしまうのかの脆弱性を評価して、ツリーの成立の可能性を算定する。
  この FTA に関しては、原子力設備や航空機等の重大事故等の要因を網羅的に検証する手法として用いられている事例や実績が報告されており、セキュリティ面だけが脅威ではなく、人為的なミス等も要因に組み入れて、起こり得る可能性を網羅的に検証していくケースで使用されている。

このどちらの詳細リスク分析も、3 つの評価指標（資産の重要度／事業被害、脅威、脆弱性）を用いて評価する。リスク分析手法と評価指標の関係を、表 2-2 に示す。但し、脅威、脆弱性の意味は分析手法によって異なっており、例えば、資産ベースでの脅威は資産に対する一次攻撃としての脅威であり、脆弱性はその脅威ごとに定義されるが、シナリオベースにおける脅威は個々のシナリオ自体の成立の可能性であり、脆弱性はそのシナリオに対する受容可能性によって評価することになる。

表 2-2 リスク分析手法と評価指標の関係

リスク分析手法	評価指標			
	資産の重要度	事業被害	脅威	脆弱性
資産ベースのリスク分析	○	－	○	○
シナリオベースのリスク分析	－	○	○	○

（4）各詳細リスク分析の長短比較

各詳細リスク分析手法の長所や短所を着目した比較を、表 2-3 に示す。

表 2-3 詳細リスク分析手法の比較

詳細リスク分析手法		長所	短所
資産ベース		● システム資産を構成する各要素に対する一次（初段）の脅威は網羅的に洗い出すことができる。 ● 分析工数は、資産を構成する要素の数やまとめ方に依存はするが、比較的小さい。	● 資産の要素間を渡って被害を及ぼす攻撃を追跡することは困難である。 ● 事業被害に対するリスクを評価することは困難である。
シナリオベース	攻撃ツリー解析（ATA）	● システムに対する攻撃の入口を網羅して、最終被害を引き起こす攻撃の連鎖を追跡することができる。 ● 事業被害を起こしうるリスクを直接評価できる。 ● サイバー攻撃による被害を分析するには、想定しうる攻撃のステップを追跡するアプローチが自然である。	● システムの構成や攻撃ツリーの作り方等によるが、攻撃ツリーの数が増大して、分析工数が膨大になる。
	フォルトツリー解析（FTA）	● 最終被害（回避したい事象）を詳細に分解して、網羅的なその要因の経緯を追跡することが可能である。 ● 事業被害を起こしうるリスクを直接評価できる。	● システムの構成によるが、フォルトツリーの数が増大して、分析工数が膨大になる。 ● 事業被害の事象ごとに構成されるフォルトツリー間の重複が見分けにくく（まとめにくく）、個々のツリーを追う事で、工数は膨大となる。

（5）本書で採用するリスク分析

前項で各詳細リスク分析手法の長短比較をしたが、リスク分析を実際に事業者において実施するにあたって、満たすべき要件は以下が挙げられる。特に、②は制御システムにおいては重要となる。

① **脅威と対策の網羅的な把握**
保護すべき資産に対して、想定される脅威とその対策を一通り把握して評価できること。

② **事業被害の回避の検証**
制御システムにおいて、一番重要なことは、重大な最終被害に至らないことであり、その検証を行えること。

③ **工数が膨大になり過ぎない事**
人員や予算は限られており、現実的な工数で、達成が可能であること。

この①を満たすものとして、資産ベースのリスク分析が適している。しかし、一次の脅威を洗い出すことはできても、攻撃の連鎖で生じうる、②の事業被害の回避を検証することは困難である。それを補完する手法としては、シナリオベースのリスク分析を用いる必要が出てくる。一方で、このシナリオベースのリスク分析を全て詳細に実施するとなると、システムによっては膨大な工数となり、③の要件が満たせないことが想定される。

以上のことから、本書では、以下の 2 通りのリスク分析を相互補完的に用いることを解説する。更に、要件の③を満たし、かつ、ATA と FTA を相互補完する方法を取り入れて解説することとする。

- **資産ベース**
- **事業被害ベース**（攻撃ツリーを用いたシナリオベースを、本書ではこう呼ぶ。）
  攻撃ツリーの構成にあたって、ATA の攻撃起点となる攻撃者と攻撃口を網羅し、また、FTA の被害起点となる最終攻撃ステップ（攻撃拠点と攻撃対象）を網羅する考え方を提示する。その途中の経路は、枝分岐が多くなることが想定されるが、それは、共通のルートを一通りだけ評価するまとめ方や、典型的なルートだけを選定して評価対象とすること等で、工数の（爆発的な）増大を回避する案である。サイバー攻撃に対する分析であるので、攻撃の入口となる箇所を全て把握すること、攻撃の最終被害を回避できるかを評価することにフォーカスする。

2.2. リスク分析手順

本節では、相互補完する 2 種類のリスク分析手法の骨子と概要を説明する。それぞれの詳細については、3 章、4 章を参照されたい。

2.2.1. 資産ベースのリスク分析

資産ベースのリスク分析は、保護すべき制御システムを構成する資産群を明確化し、各資産に対して、システム構成上及び運用管理上に想定される脅威、各資産の重要度とその脅威の受容可能性(脆弱性)の相乗値を評価するリスク分析手法である[13]。分析手順の流れの概要は、以下の通りである。

① **資産の定義とその重要度を定義する** (☞ 3.2 節)
資産の物理的なまとまりや論理的な機能単位(サーバ、端末、装置等)の観点で、各資産と、その重要度を定義する。

② **各資産に対する脅威とそのレベルを定義する** (☞ 3.4 節・4.1 節)
各資産に対して、ネットワーク構成や接続機器、ユーザの利用状況を考慮して、想定される脅威とその脅威レベル(それが実行される可能性)を定義する。

③ **資産の各脅威に対する脆弱性を評価する** (☞ 3.5 節・4.1 節)
各脅威に対する想定される対策と、その実施レベルから、当該脅威に対する脆弱性を評価する。

④ **各資産の脅威に対するリスク値を算定する** (☞ 4.1 節)
①②③の相乗値によって、各資産の各脅威に対するリスク値を算定する。

2.2.2. 事業被害ベースのリスク分析

事業被害ベースのリスク分析は、回避したい事業被害を明確化し、そこに至る攻撃が成り立つ可能性を評価し、被害のレベルと攻撃成功可能性(脆弱性)の相乗値を評価するリスク分析手法である[14]。分析手順の流れの概要は、以下の通りである。

① **事業被害(製造停止、供給停止、システム破壊、情報漏えい等)を定義する** (☞ 3.3 節)
事業に直接影響を及ぼす被害を洗い出す。

---

[13] 資産の重要度、脅威の受容可能性(脆弱性)については、詳細な定義は 3 章で行うので、ここでは一般的用語の範囲で理解頂きたい。

[14] 被害のレベルと攻撃成功可能性(脆弱性)については、詳細な定義は 3 章で行うので、ここでは一般的用語の範囲で理解頂きたい。

② **事業被害を引き起こす攻撃シナリオを定義する**（☞ 3.3 節・4.2 節）

・例えば、供給停止という事業被害を引き起こしうるシナリオは複数ありうる。
供給停止を引き起こすシナリオとして、供給装置に不正な制御コマンドを送るケースや、制御装置のソフトウェア自体に攻撃（改ざん等）を行うケース等、様々考えられる。

・実際に事業被害を引き起こす（最終）攻撃によってシナリオを分類し構成する。

③ **攻撃シナリオを実現する攻撃ツリーを構成する**（☞ 4.2 節）

攻撃シナリオを（必要に応じて）サブ攻撃シナリオに分類する。例えば、不正な制御コマンドを送るのが、システム内部に感染したマルウェアであったり、内部の不正者であったり、様々考えられる。

攻撃シナリオを実現する攻撃ツリーを構成するが、その構成にあたっては、事業被害を引き起こす最終攻撃（上記例では、不正コマンドの送出や、制御装置への不正アクセスやマルウェア感染による改ざん等）に向けて、攻撃のステップを書き下すが、一つの攻撃シナリオに対して、複数の攻撃ツリーが考えられるケースもある。

攻撃ツリーの構成にあたっては、システム構成図やシステムの諸機能に依って、最終攻撃に向かって、攻撃者の視点で、概ね以下を念頭において、攻撃のステップを明確化していく。

(ア) 誰が攻撃するか

(イ) 攻撃の侵入口はどこか（ネットワークからの侵入口、システムへの侵入口、攻撃者等によって分類）

(ウ) （ネットを経由した）最終攻撃を仕掛けるためのシステム内部への侵攻

(エ) （最終攻撃に向けた）システムの情報（認証情報、暗号鍵等）の奪取等の実行

(オ) 最終攻撃の実施（コマンドの発行、システムの改ざん・破壊、情報の窃取等）

（注） 次ページに、構成のイメージを示す。

④ **攻撃ツリーの発生する可能性を評価する**（☞ 3.4 節・4.2 節）

攻撃ツリーを構成する一連の攻撃ステップの難易度等を考慮して、その攻撃ツリーの発生する可能性を評価する。

⑤ **攻撃ツリーの成功の可能性を評価する**（☞ 3.5 節・4.2 節）

攻撃ツリー全体の成功（被害を及ぼす）可能性は、各攻撃ステップがどの程度の可能性で成立するか、各ステップに対する脆弱性（対策の不十分さ）の評価に基づいて評価する。

⑥ **攻撃ツリーのリスク値を算定する**（☞ 4.2 節）

①④⑤の相乗値でリスク値を算定する。

【事業被害から攻撃シナリオ、攻撃ツリー、攻撃ステップの構成】

事業被害を挙げ、攻撃シナリオ、攻撃ツリーにブレークダウンしていくことで、網羅的なリスク分析を行うことを目的としており、イメージは以下である:

・起こっては困る事	→	・どこで、何をする	→	・誰が、どこから、どうやって
【事業被害】		【攻撃シナリオ】		【攻撃ツリー／攻撃ステップ】

但し、攻撃シナリオを複数の攻撃ツリー群にブレークダウンするのが分かりやすいか、攻撃シナリオを細分割するかは、対象に依って異なる。

その構成概念を以下に示す。

例えば、供給停止を引き起こすという事業被害1に対して、「不正アクセスにより供給装置が制御され供給停止する」という攻撃シナリオ1－1に対して、制御コマンドをシステム上流から送付することで引き起こす攻撃もあれば、供給装置へマルウェア感染等で直接攻撃する攻撃も考えられるので、2つの攻撃ツリーに分けている(パターン例1)。一方、事業被害2のケースでは、想定した攻撃シナリオ2－1を更に細分した二つの攻撃シナリオに分け、それぞれに対して攻撃ツリーを記載している(パターン例2)。最終攻撃に至るルートの個数が攻撃ツリーの数である。

この事業被害ベースのリスク分析は、システムと機能構成やデータフロー等を前提に、机上での仮想的なペネトレーションテスト[15]を実施していることに相当する。

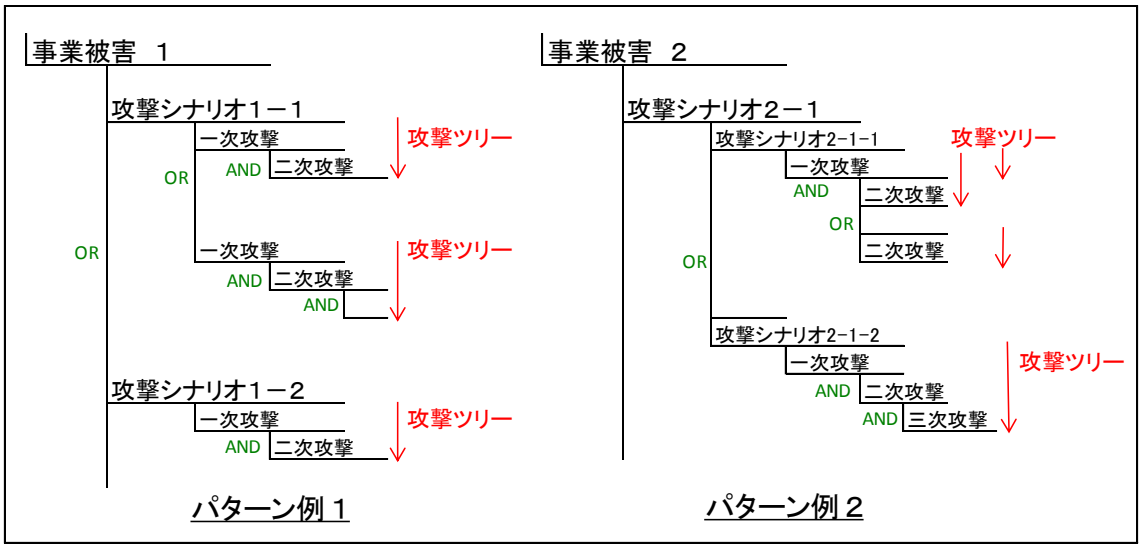


図 2-1 事業被害・攻撃シナリオ・攻撃ツリー・攻撃ステップの関係

15 ペネトレーションテストについては、6 章(6.4 節)を参照。

2.3. 本ガイドの構成と利用方法

本ガイドの第一の目的は、制御システムに対するセキュリティリスク分析の手法を解説し、リスク分析の実施を手引きすることである。従って、2.3.1 項、2.3.2 項では、セキュリティリスク分析の実施について解説した 3 章から 5 章における構成と利用方法とリスク分析実施にあたっての提言について述べる。

また、本書のその他の章と付録においては、リスク分析結果を活かしたセキュリティテストや、リスク分析を実施する上でも参考となる、特定のセキュリティ対策に関する基準、特化した脅威（標的型攻撃、内部不正等）に対する対策を解説している。2.3.3 節で、その構成と利用方法を述べる。

【コラム】

資産ベースのリスク分析と事業被害ベースのリスク分析の位置付け

詳細リスク分析の手法と比較を 2.1 節で解説したが、システムが直面する様々な脅威（攻撃）の観点から、資産ベースのリスク分析と事業被害ベースのリスク分析の守備範囲の捉え方を、このコラムでは解説する。攻撃には、攻撃形態と目的、それに応じた攻撃活動があるので、その備えとして 2 通りのリスク分析が果たす役割は、下表のように捉えることもできる。

<table>
<tr><th></th><th>攻撃形態</th><th>目的</th><th>特徴</th><th>リスク分析
の有効性</th><th>有効性理由・観点</th></tr>
<tr><td rowspan="2">攻撃種別</td><td>・バラマキ
・無差別</td><td>・妨害
・混乱
・脅迫
・金銭</td><td>・ネットワークの入口を無差別に攻撃
・組織内ネットワーク経由で拡散
・手当たり次第攻撃</td><td rowspan="2">資産ベースのリスク分析
【己を知る】

事業被害ベースのリスク分析
【敵を知る】</td><td>・資産を網羅的に分析、対策強化可能
・機器やシステムのゾーン境界を直接評価可能</td></tr>
<tr><td>・標的型
・意図的</td><td>・情報窃取
・誤作動
・停止
・破壊
・二次被害誘発</td><td>・様々な侵入口を探索
・侵入後、システムを分析して侵攻
・正規ルート等を悪用して目的遂行</td><td>・攻撃ルートの検証、抑止策検討可能
・最終被害の回避、リスク低減可能</td></tr>
</table>

2.3.1. 本ガイドの構成

制御システムに対するリスク分析の流れと本書の章・節との対応を、図 2-2 に示す。リスク分析の手順は↓に沿って実施することになる。3 章はリスク分析のための事前準備であり、4 章で具体的な手順に沿ってリスク分析を実施し、5 章でそのリスク分析結果の活用法を述べる。各節における作業で生成される成果物(アウトプット)を明示している。その手順の概要は以下となる:

【第一ステップ】(3 章 3.1 節)

システム構成とデータフローの明確化を行うステップである。保護すべき資産やそこで行われる処理機能やデータフロー等、リスク分析する対象を明確化して以下のアウトプットを作成する:

- システム構成図(ネットワーク構成・主要機能等を含む)
- 資産一覧表(物理資産・情報資産等)
- データフロー図(情報、コマンドフロー等)

【第二ステップ】(3 章 3.2 節～3.5 節)

第一ステップで明確化した保護対象に対して、リスク分析を行うための各評価指標の定義と、ある判断基準に基づいたその評価値を決定する。

① 資産の重要度の決定(3.2 節)
② 事業被害とそのレベルの定義(3.3 節)
③ 脅威レベルの定義(3.4 節)
④ セキュリティ対策項目の確認(3.5 節)

【第三ステップ】(4 章 4.1 節、4.2 節)

リスク分析の2つの手法を実施する具体的な手順を説明しており、これに沿って各保護対象に対して実施する。それぞれの手法において、第二ステップで定義した各評価指標に基づいて、リスク分析シートの様式(作り方)と、それを用いた分析の手順を説明している。

【第四ステップ】(5 章)

リスク分析結果により、全体としてのリスク値の分布を把握し、リスク値の高い資産箇所や攻撃シナリオを抽出し、リスク値を低減させるため、脆弱性や脅威の低減策を検討し、対策強化の検討や、実施の優先順位付けを決定する。

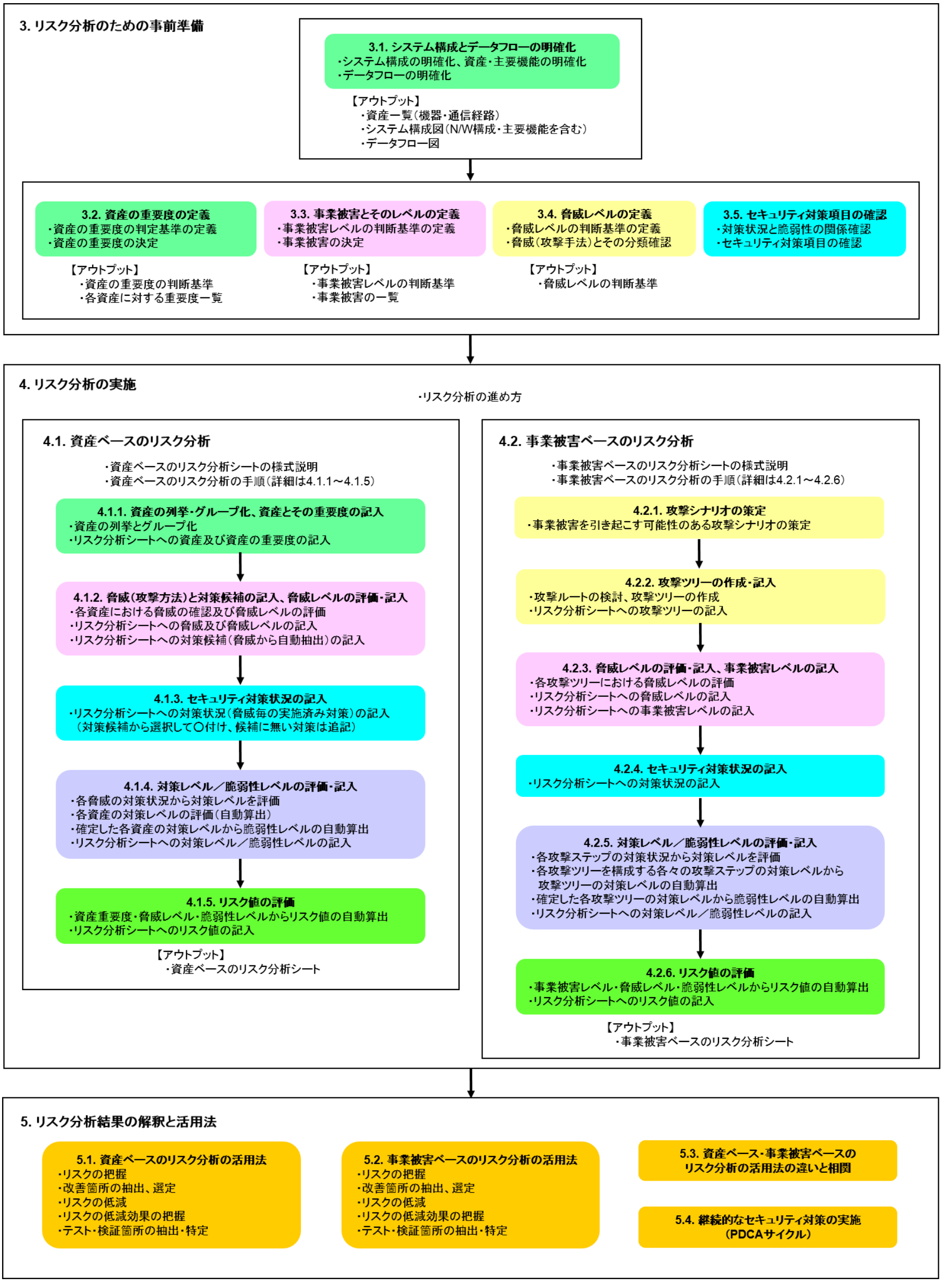


図 2-2 制御システムのリスク分析の流れ

このページは空白です。

2.3.2. 実際のリスク分析実施にあたっての提言

本書は、典型的な制御システムを例にとって、リスク分析を実施する場合の、事前準備の工程(3章)とリスク分析の実施手順(4 章)を解説している。3 章は、リスク分析の事前準備の位置付けであるが、セキュリティ対策に取り組む全ての事業者にとって、対象とする制御システムの全体像と状況、及びそれを取り巻くセキュリティ上の課題を正確に把握する上で、3 章の全項目を実施する必要がある。

(1)リスク分析手法の選択

4 章で解説する 2 通りのリスク分析手法の選定の根拠に関しては、2.1 節(5)で述べた。しかし、事業者にとっては、分析作業の工数の増大が最大の課題になるものと考えられる。その限られた工数の下でリスク分析を実施する場合、2 通りのリスク分析に関して、実施範囲の選択と優先度の方針を示す。

① 資産ベースのリスク分析(4.1 節)は必ず実施する。
② 事業被害ベースのリスク分析(4.2 節)は、一通り全ての事業被害に対して分析することが望ましいが、工数等の制約がある場合は、攻撃シナリオと攻撃ツリーを深刻な事業被害に絞って実施する。

この選定方針の根拠は以下である:

- 資産ベースのリスク分析は、保護資産を網羅的に把握、評価する上では不可欠である。また、資産のグループ化等の工夫をすれば、工数はそれ程膨大にはならない。なお、各資産の重要度を検討する際に、その資産に起因して想定される事業被害を考慮に入れて評価することで、事業被害ベースのリスクの観点を取り入れた効果も期待できる。
- 事業被害を回避できるかの検証は資産ベースだけではどうしても限界がある。従って工数の許容する範囲で、事業被害ベースのリスク分析を深刻な事業被害を生じさせる可能性のある攻撃シナリオと攻撃ツリーを選択、限定して実施する。このリスク分析は攻撃シナリオを構成する攻撃ツリーの数が、攻撃の様々な入口の存在や経由する攻撃ルートが複数に分岐すること等で膨大となる傾向にある。攻撃シナリオや攻撃ツリーの選定にあたっては、最も回避したい事業被害を引き起こしうる攻撃の最終攻撃ステップ(群:複数存在しうる)を抽出して、その攻撃ステップ(群)を少なくとも一つは含む攻撃ツリーの集合を選定対象にする。最終攻撃ステップに至る攻撃ツリーのリスク値を把握し、その回避が可能かを工数の許す範囲で確認することに目標をおく。

※ 初回のリスク分析の実施年度以降、分析を見送った攻撃ルートや、新たな脅威に対して、あるいはシステムの更改等様々な変更に対して、本ガイドに沿って作成・実施したリスク分析結果を元に、それを継続的に見直して追加・修正していくことが可能である。それを実施して

いくことが、先鋭化するサイバー攻撃に対抗するセキュリティを維持・継続・向上していく上で、最善の対応となる。

(2)リスク分析の実施

本書を参照して、リスク分析を実施する上での留意事項について説明する。

① 手順や実施項目のカスタマイズ

記載事項を全てそのままの内容で実施することは求めていない。本ガイドは、あくまで IPA のリスク分析実施経験から得たノウハウに基づいており、各事業者の評価対象システムや事情、更には固有の知見等によって適宜カスタマイズして利用、あるいは独自の方法等を導入することでも構わない。

※ 評価方法や分析リストの利用方法等、IPA のノウハウを紹介する目的で掲載している。

② 固有の定義の導入

資産の重要度や事業被害の考え方は、事業分野によって様々な観点があることから、自組織や業界の置かれたそれぞれの環境にそった定義を導入することでも構わない。

③ 評価指標のレベル

3 章で導入する評価指標は、3 段階をベースとしている。本ガイドではレベル判断の難しさと煩雑さを回避するために典型的な 3 段階を用いているが、多段階(4～5)を採用することでも構わない。

④ 結果の掘り下げ

リスク分析を実施した結果、リスク値の高い箇所が抽出された場合、脅威や脆弱性の評価内容とレベルの正しさを再確認して、リスク値を精査する。続いて、脆弱性の低減等によってそのリスク値をどの様に下げることが可能か等、詳細な検討を実施していく。

⑤ 継続的な実施

リスク分析を実施するにあたって、評価対象システムの詳細度が工数に大きく影響する。資産のグループ化や、ネットワークを主要(本流)のルートだけに限定すること等を工夫して、組織が許容できる工数に収まる範囲で実施することが重要である。リスク分析は、1 回で終わりということではなく、繰り返していくことが重要であり、その際に、前回では省かれた箇所の追加や詳細化等を取り込んで、分析の精度を高めていくことを検討していく。

2.3.3. 6 章以降の構成と活用方法

6 章では、リスク分析結果の検討後に、必要に応じて実機（もしくは模擬環境）での検証（セキュリティテスト）を実施する際の手引きを解説している。

7 章以降及び付録は、特化した攻撃に対する対策の全体像、セキュリティを検討する上で固有の技術に関する解説、セキュリティの状況を確認する様々なチェックリスト等からなる。本章以降は、制御システムに限らず広く一般システムのセキュリティ対策の検討に活用できる内容となっている。

（1） 6 章 セキュリティテスト

この章では、セキュリティテストの全体像を概観し、制御システムに対して実施されることが想定される 3 種類（脆弱性検査、ペネトレーションテスト、パケットキャプチャテスト）のテストに関して、その手順を解説している。セキュリティリスク分析の結果を受けて、リスク値の高い機器や、懸念が残る攻撃ルート等への実際のテストを実施する際の手引きである。

（2） 7 章 特定セキュリティ対策に対する追加基準

この章では、以下の点に対して、追加的な検証をするための解説と対策の基準について述べている。この章は一般的な情報システムにおいても活用が可能である：

① セキュリティの基盤となる暗号技術の活用基準

セキュリティの基盤となっている暗号の選定及び強度の選択、暗号鍵の運用及び管理基準等を把握しておくことが重要である。特に国際基準等に照らして、暗号技術の活用が行われているかを検証する。

② 特定の攻撃に対するセキュリティ対策

特定の攻撃として、標的型攻撃と内部不正を取り上げている。その理由は、情報ネットワークへの侵入からの伝播やメディアの持ち込み経由や人間が介在して多段で行われるこれらの攻撃は、個々の脅威の対策として追うだけではなく、その攻撃の全体像を捉えておくことが重要であり、その観点から検証する。

③ 境界での脅威に対する対策

脅威や攻撃は、上流である境界で食い止めるのが得策である。ネットワークの入口であるファイアウォールの活用方法と、運用上で(限定的な)使用を禁止できないケースが見受けられる外部記憶媒体に対するセキュリティ対策を検証する。

7 章の構成の一覧は以下である:

- **暗号技術の選定と活用基準** (☞ 7.1 節・付録 B.1)
- **標的型攻撃対策** (☞ 7.2 節・付録 B.2)
- **内部不正対策** (☞ 7.3 節・付録 B.3)
- **ファイアウォールにおける各種設定** (☞ 7.4 節・付録 B.4)
- **外部記憶媒体におけるセキュリティ対策** (☞ 7.5 節・付録 B.5)

(3) 付録

付録では、7 章における各対策項目に対するチェックリストを用意している。このチェックリストは、各種の国際・国内基準も参照しつつ、IPA が策定したものである。また、制御システムのインシデント事例を付録 C に掲載している。

3 章～5 章のセキュリティリスク分析においては、IPA が実システムに対して実施してきたリスク分析業務での試行錯誤も通し、ノウハウや知見を極力具体的に説明することに注力して解説している。また、その活用を最大限図って頂くために、リスク分析シート等のテンプレートは Microsoft Excel 形式で入手できる様に IPA のホームページで公開している。更に、共通の概念や言葉で脅威や対策を議論できる様にするため、脅威の一覧や対策の一覧を IPA で定義し、それを用いて記述している。勿論、その一覧に修正加筆頂くことも可能である。

なお、本書では、ある制御システムを評価対象モデルとして、リスク分析の手順の説明を中心に解説し、紙面の都合で、リスク分析シートのフルセットは掲載していない。そこを補完する目的で、あるモデルに対してリスク分析を仮想的に実施した結果(リスク分析シートのフルセット)を、別冊として、ホームページで公開している。この別冊も合わせて利用頂きたい。

3. リスク分析のための事前準備

本章では、リスク分析を実施するために必須の事前準備作業を説明する。

本書で述べる詳細リスク分析を実施しない事業者においても、本章で述べる準備作業は、セキュリティ対策を検討する上で必要不可欠な作業である。セキュリティ対策においては、自組織のシステムを分析して状況を把握し、脅威を理解することで、効果的な施策を実施可能となるからである。

3.1 節は、まず自組織の分析・把握の第一歩であり、システム構成とデータフローの明確化を行う。本作業を高精度に実施することが望ましいが、詳細性を追求すると現実的な時間内に実施することが困難となることが懸念されるため、根幹となるシステム資産と主要なデータフローの捉え方、整理方法について説明する。

3.2 節から 3.5 節は、3.1 節で明確化したシステム構成に対して、4 つの観点:

- **資産の重要度とそのレベルの定義** （☞ 3.2 節）
- **事業被害とそのレベルの定義** （☞ 3.3 節）
- **脅威レベルの定義** （☞ 3.4 節）
- **セキュリティ対策状況の明確化** （☞ 3.5 節）

から、自組織のシステムの整理・明確化、対策状況（脆弱性）の明確化を行って分析を実施すると共に、脅威を理解する。自組織の分析は、3.2 節、3.3 節、3.5 節に、脅威の理解は 3.4 節に相当するが、各々の分析において自組織と脅威の両者を想定・考慮して検討することによって、より高精度の分析（明確化）が可能となる。

各節における事前準備作業とそのアウトプットの関係を、表 3-1 に示す。アウトプットには、リスク分析作業の最終成果として、そのまま「リスク分析結果」の一部となる情報と、リスク分析で用いる 2 種類の分析シート（資産ベースのリスク分析シート、事業被害ベースのリスク分析シート）に転記すべき情報がある。

これらの明確化をベースとして、4 章では 2 通り（資産ベース／事業被害ベース）の詳細リスク分析の手順を説明するが、直接的には、3.2 節は資産ベースのリスク分析、3.3 節は事業被害ベースのリスク分析の基となる。しかしながら、資産の重要度（3.2 節）を検討する場合においても、その資産の棄損で生じ得る事業被害（3.3 節）の観点が不可欠であるため、これらの 4 つの観点の準備作業は、どちらのリスク分析に対しても有効な作業となる。

表 3-1 事前準備作業とそのアウトプット

節	準備作業	アウトプット
3.1	● システム構成（ネットワーク構成を含む）の明確化 ● 資産・主要機能の明確化 ● データフローの明確化	● 資産一覧（例：表 3-6） ● システム構成図（例：図 3-6） ● データフロー図（例：図 3-11）
3.2	● 資産の重要度の判断基準の定義 ● 資産の重要度の決定	● 資産の重要度の判断基準（例：表 3-10） ● 各資産に対する重要度一覧（例：表 3-14）
3.3	● 事業被害レベルの判断基準の定義 ● 事業被害の決定	● 事業被害レベルの判断基準（例：表 3-18） ● 事業被害の一覧（例：表 3-19）
3.4	● 脅威レベルの判断基準の定義 ● 脅威（攻撃方法）の分類確認	● 脅威レベルの判断基準（例：表 3-21）
3.5	● 対策状況と脆弱性の関係確認 ● セキュリティ対策項目の確認	

【コラム】

「己を知り、敵を知れば、百戦危うからず」

中国、春秋時代の軍事戦略家、孫武が執筆したとされる兵法書『孫子』に示された名句の一つに、「彼を知り己を知れば百戦殆うからず」がある。これは、敵のことも己のことも、実情を熟知していれば、百回戦っても負けることはない、という意味である。

この故事において、敵＝脅威（攻撃者を含む）、己＝自組織と置き換えてみると、セキュリティ対策において効果的な施策を実施するための教えとなる。

リスク分析は、

己を知り、敵を知れば、百戦危うからず

を実現する、サイバーセキュリティ時代の兵法であると言える。

3.1. システム構成とデータフローの明確化

本節の目的は、のちの資産ベースのリスク分析と事業被害ベースのリスク分析を行う上で、分析対象を明確化し、必要となる情報を分析に利用しやすい形に整理することにある。

リスク分析の事前準備の第一ステップとしては、以下の 3 項目を実施する。

- 資産の洗い出し
- システム構成（ネットワーク構成を含む）についての明確化、論理化
- データフローの明確化

これらの作業に必要となる、分析対象についての事前情報（インプット）として、予め以下の情報等を準備しておく。

- システムの資産台帳
- 仕様書
- ネットワーク構成図（システムにおける資産の接続関係を記した図面）

本節でのアウトプットは以下となる。

- 分析対象の資産一覧（表等、任意の形式）
- 論理的なネットワーク構成を含むリスク分析作業用システム構成図
- システム構成図に基づくデータフロー図

データフロー図を事前作成しておくことは、以下の理由により、4 章でリスク分析を実施する際の優先順位付けに有効である。

- 攻撃者から見ると、データフローに沿った攻撃は低コストであるため、最も発生する可能性が高い。
- 全ての攻撃ルートに従ったリスク分析の実施が困難であるならば、データフローを沿った攻撃に対する分析を優先的に実施する。

3.1.1. システム構成図の作成の流れ

システム構成とデータフローの明確化は、下記の工程に従って実施する。

① **分析範囲の決定**:
リスク分析を実施する範囲を決定する。

② **分析用アーキテクチャ(ベースモデル)の明確化**:
ネットワーク構成図から分析用にモデル化したシステム構成図を作成するために、ベースとなる分析用アーキテクチャ(ベースモデル)を決定する。

③ **資産の洗い出し**:
リスク分析実施範囲内に存在する資産、及び分析に必要となる各資産の情報を洗い出す。

④ **分析対象とする資産の絞り込み**:
分析の工数を減らすため、同一の機能を有する資産をまとめて、分析対象を統合する。また、定常の稼働状態では制御システムに影響を与えない資産を、分析対象から除外する。

以上の工程で、分析対象の資産一覧表が完成する。

⑤ **エリアごとの資産の配置**:
エリアごとに物理的なセキュリティのレベルが異なる場合があるため、資産の設置されているエリア区分図を作成する。

⑥ **各資産の接続状況の記述**:
各資産のネットワークによる接続関係を図式化する。

以上の工程で、システム構成図が完成する。

⑦ **データフローの明確化**:
資産の洗い出しでまとめた表を元にデータの流れを整理して、システム構成図に書き込む。

以上の工程で、データフロー図が完成する。

以下、上記①～⑥の各工程における実施内容の詳細を解説する。工程⑦の詳細は、3.1.3 項で解説する。

（1）分析範囲の決定

制御システムに対して、セキュリティリスク分析を実施する範囲を決定する。分析範囲として、実施対象の事業所（物理的なロケーションを含む）、事業所内の実施範囲を決定する。本分析では制御システムが対象となることから、基本的にはOA系の処理を行うための機器及びネットワークは対象外とする。

また、分析範囲と外部との接続部分のネットワーク機器の切り分けを行う。具体的には、ネットワーク構成図を見ながら外部との接続部分を探す。接続部分にはルータやファイアウォール等の機器があるのでその機器を接続点とする。外接点における機器は、保護すべきシステムの外部からの入口となるので、当然分析対象とすべきである。但し、組織によっては、当該機器は制御システムを管理している部門とは別の部門にて管理されている場合もある。その場合には、分析に必要となる資産や対策状況の情報のヒアリングを実施する必要がある。

図 3-1 に、分析範囲の決定例を示す。本例においては、制御ネットワーク（制御ネットワーク上の機器を含む）及びフィールドネットワークを分析範囲としている。バルブやセンサ等のフィールド機器は、機器固有の安全対策という視点から分析を行うべきものと考え、本件の主題であるサイバーセキュリティの観点からは分析対象から除外している。本書では、PLC 等の制御機器に接続するフィールドネットワークは評価対象とするが、制御機器からフィールド機器へ接続されているセンサバスは評価対象外とする。何故ならば、制御システムに対するサイバー攻撃においては、フィールド機器が接続された上位の制御機器を攻撃対象と考えれば、十分な分析ができるからである。

また、情報ネットワーク（情報ネットワーク上の資産を含む）は、原則的に分析の対象外とする。但し、情報ネットワーク上に存在する監視端末や制御に影響を与える可能性のあるサーバが存在する場合は、情報ネットワーク及びそれらの機器を分析対象に含むことを推奨する。

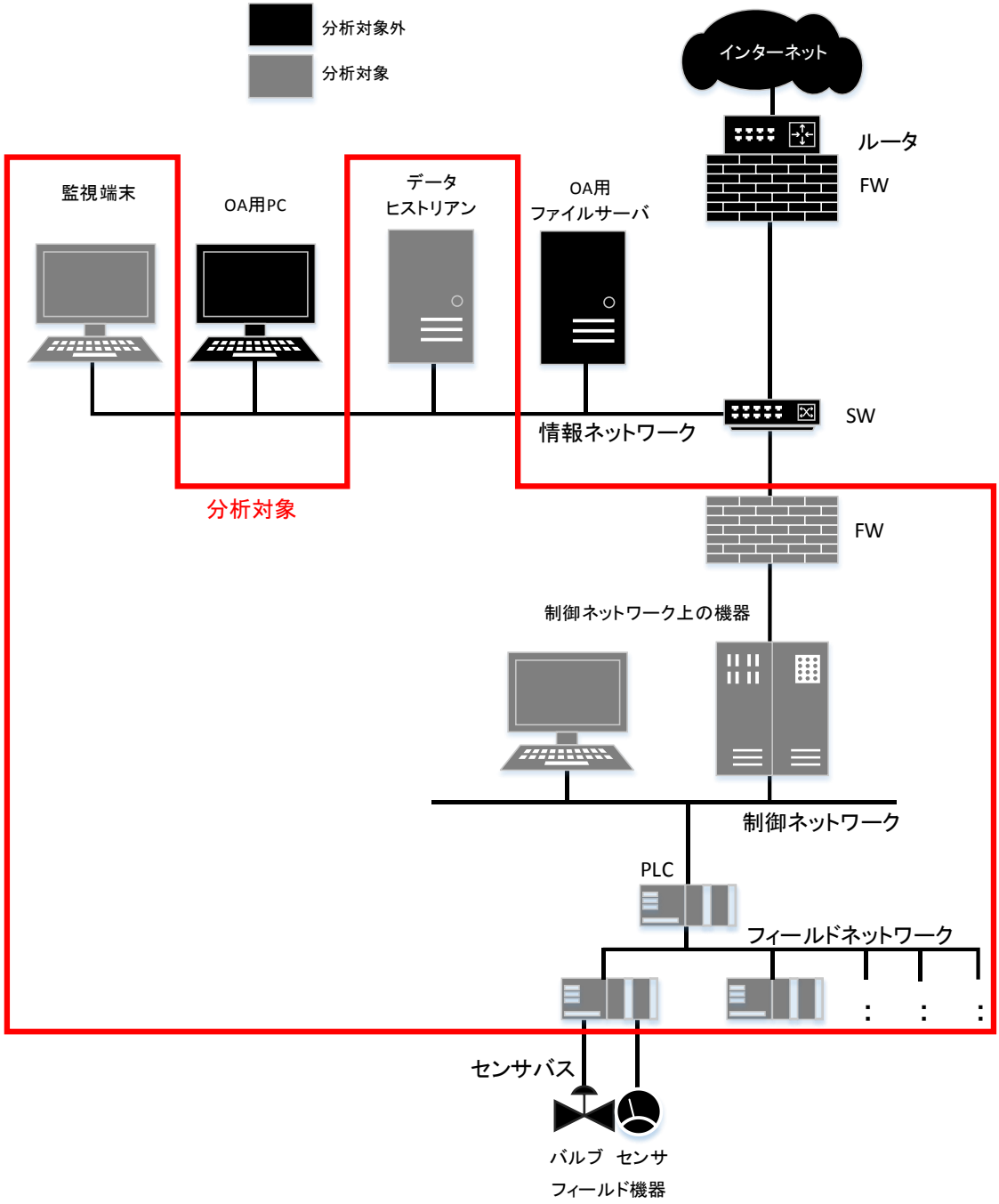


図 3-1 セキュリティリスク分析における分析範囲

（2）分析用アーキテクチャ（ベースモデル）の明確化

システム構成図を作成する際のベースになるネットワーク構成（アーキテクチャ）を整理する。

分析を実施する際、例えば、システム構成時に作成した物理構成を示すネットワーク構成図を元に分析用システム構成図を作成した場合、複雑なため、全体の論理構成が読み取りにくい場合がある。そこで、論理構成を示すネットワーク構成図を元に、分析用システム構成図を作成する。

セキュリティ分析を行う上では、制御システムのネットワーク構成を明確にすることが必要であるが、特に制御ネットワークと情報ネットワークのセグメント分割方式や DMZ（DeMilitarized Zone：非武装地帯）の有無を明確化することが重要である。

制御システムにおけるネットワーク分割方式を示すアーキテクチャとして、「NIST SP800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security」[16]において、4 種類の基本アーキテクチャが提唱されている（表 3-2・図 3-2）。

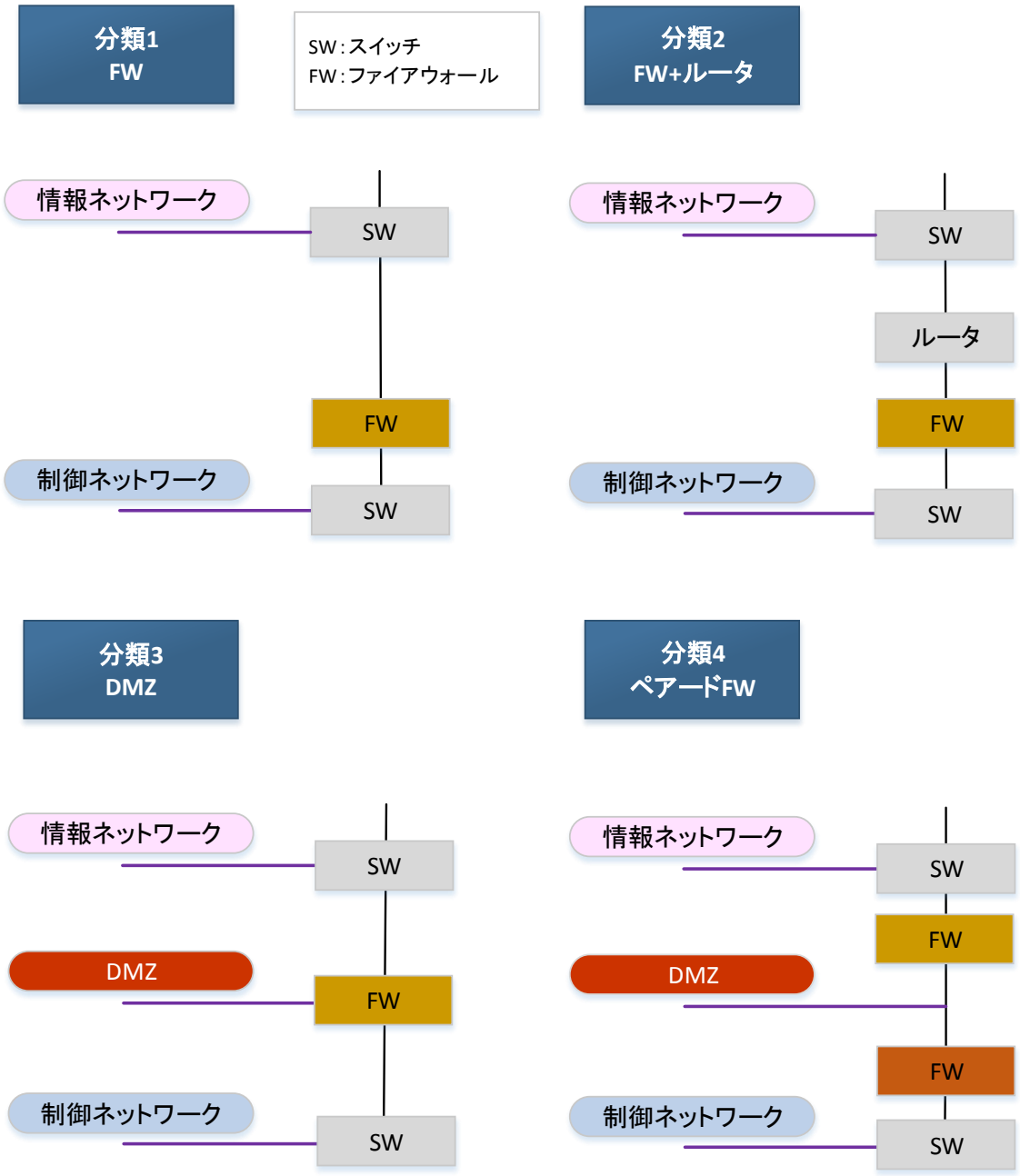
そこでまず、分析対象のネットワーク構成が 4 つのどのアーキテクチャに相当するのかを検討し、それをベースにシステム構成図を作成していくことを推奨する。

なお、現実の分析対象のシステムは、必ずしもこの 4 種類のアーキテクチャに分類されるとは限らず、これらの組合せやまったく異なる構成を取りうる。その様な場合でも、まず前述した様に制御ネットワークと情報ネットワークの接続方式、DMZ の有無、ファイアウォール・ルータ・スイッチの接続状態を把握しながら論理構成を明確化し、実際の分析目的に十分利用可能なシステム構成図を作成する。

表 3-2 制御システムのネットワーク分割方式のアーキテクチャ分類

本書での分類・名称		NIST SP800-82 における定義・名称	
分類	名称	項	名称
分類 1	FW	5.5.2	Firewall between Corporate Network and Control Network (Figure 5-1)
分類 2	FW＋ルータ	5.5.3	Firewall and Router between Corporate Network and Control Network (Figure 5-2)
分類 3	DMZ	5.5.4	Firewall with DMZ between Corporate Network and Control Network (Figure 5-3)
分類 4	ペアード FW	5.5.5	Paired Firewalls between Corporate Network and Control Network (Figure 5-4)

[16] http://dx.doi.org/10.6028/NIST.SP.800-82r2
JPCERT/CC から日英対訳版「産業用制御システム（ICS）セキュリティガイド」が公開されている。
https://www.jpcert.or.jp/ics/information02.html#NISTSP800-82



用語の対応	本書での表記	NIST SP800-82
	情報ネットワーク	Corporate Network
	DMZ	
	制御ネットワーク	Control Network

図 3-2 制御システムのネットワーク分割方式のアーキテクチャ分類

（3）資産の洗い出し

制御システムに存在する資産を全て洗い出す。また、各々の資産について、今後のリスク分析作業において利用する、資産に「付帯する情報」を洗い出す。

付帯する情報の種類と意味を、表 3-3～表 3-4 に示す。資産は大別して「機器」と「通信経路」に分類され、洗い出すべき情報の種類が異なる。

表 3-3 資産に付帯する情報（1/2）

情報の種類	意味
資産名	資産の名前。
資産分類	「機器」または「通信経路」（WAN、LAN 等）のいずれか。
定常稼働、非定常稼働	定常的に稼働している資産か、必要な場合のみ稼働させる資産かを記す。非定常稼働機器を分析対象に含めるか除外するかは、最初の段階で方針を明確に決めておく。除外する場合は、最初から資産一覧表にまとめる作業は行わない。
資産の持つ機能	資産分類＝「機器」の場合、 資産の持つ機能を記す。機能とは、その資産がシステムの中でどの様な動作をするかを明確にするための分類で、セキュリティ対策に密接に関連する。機能の分類は、 ● 入出力 ● データ保存 ● （制御装置への）コマンド発行 ● ゲート: ルータ、ファイアウォール（FW）、スイッチ（SW）等ネットワーク上でデータが通過する経路上に存在する機器 の 4 種類またはその組合せ（複数の機能を持つ機器）となる。 セキュリティ対策との関連とは、例えば制御に利用するデータ保存機能を持つ資産では、その値が改ざんされると、システムに被害が生じる恐れがある。また、正規のコマンド発行機能を持つ資産から発行された不正なコマンドは、不正であると判断するのは難しく、誤動作を生じる恐れがある。
回線種類（ネットワーク）	資産分類＝「通信経路」の場合、 機器間の通信が、WAN か LAN か、専用線かインターネット経由か、有線か無線かを明確にする。通信回線によっても、それぞれの特性に応じたセキュリティ対策が必要となる。

表 3-4 資産に付帯する情報(2/2)

情報の種類	意味
設置場所	資産が設置されている場所を記載する。設置場所により、物理的なセキュリティ対策状況(入室時の認証方法等)が異なる場合があるため、明確にする。
接続先 ネットワーク	資産がどの階層や機器にどの様に接続されているかを明確にする。
管理ポートの 接続先	資産分類=「機器」の場合、 ファイアウォール機器等ではメンテナンスをネットワーク越しに行う様なケースがあり、通信ポートとは別の管理ポート経由で通信できる様になっている場合がある。この様な管理ポートは脅威となり得るため、詳細を調査しておく。
データの 種類と経路	資産分類=「機器」の場合、 データ(コマンドを含む)の種類と経路(送信者、中継者、受信者)を明確にする。
構築ベンダー ／ 機器メーカー	資産の提供元によって納入時やファームウエアアップデート等メンテナンスのポリシーが異なる場合があるので、個別に調べておく。
OS の種類／ バージョン	資産分類=「機器」の場合、 OS の種類(ディストリビューションを含む)やバージョンによっては、既にサポートが終了してセキュリティパッチが提供されないケースがあるため、個々の資産の OS を調べておく。
使用する プロトコル	攻撃対象となりやすいプロトコルが使用されている場合もあり、対策が必要なケースがあるため、プロトコルも調査しておく。
セキュリティ 対策	それぞれの資産が現在行っているセキュリティ対策を列挙しておく。セキュリティ対策の詳細は 3.5 節で説明する。

これらの情報は、3.1 節で全て必要とする情報ではなく、3.2 節及び 4 章以降の工程で必要となる情報も含まれている。各情報とその情報を利用する工程の関係を、表 3-5 に記す。但し、収集に当たって構築ベンダー／機器メーカー等と情報交換が必要な情報に関しては、一度に全ての情報をまとめて収集した方が、効率が良いと考えられる。

表 3-5 洗い出した情報と利用工程

情報の種類	情報の利用先、利用工程						
	資産リスト	ネットワーク図	データフロー	セキュリティ対策状況	資産のグループ化	資産ベースリスク分析シート	事業被害ベースリスク分析シート
	3.1 節、3.2 節	3.1 節	3.1 節	3.5 節	4.1 節	4.1 節	4.2 節
資産名	○	○	○	○	○	○	○
資産分類	○	○	○	○	○	○	○
定常稼働、非定常稼働	○	○					
資産の持つ機能	○	○	○	○	○	○	○
回線種類（ネットワーク）	○	○	○	○	○	○	
設置場所	○	○		○	○	○	○
接続先ネットワーク	○	○			○		
管理ポートの接続先	○	○		○			
データの種類と経路	○		○				○
構築ベンダー／機器メーカー	○			○	○		
OS／バージョン	○			○	○		
使用するプロトコル	○			○			
セキュリティ対策	○			○		○	○

（4）分析対象とする資産の絞り込み

資産の洗い出しの完了後、分析の対象とする資産を絞り込み、分析対象の資産一覧を作成する。セキュリティリスク分析では、分析対象が多数あると工数が膨大になるため、分析対象とする資産を絞り込むことを検討する。但し、分析漏れ等の問題が生じる場合があるため、絞り込む際は注意が必要である。

ここでは 2 つの絞り込み（統合と除外）について説明する。

① 同一機能を有する資産の統合

ここでいう機能とは、資産分類＝「機器」である各資産の洗い出しを行った際に分類した、「入出力」「データ保存」、「コマンド発行」、「ゲート」という 4 種類の機能を意味する。同じ機能を持つ機器がトポロジ的に同じ位置にある場合、一つにまとめることで、評価対象機器を減らすことが可能となる。

例えば、同一ネットワーク上に複数の監視端末がある様なケースでは、それらがほぼ同じ機能を持っているのであればまとめることができる。また、ルータとファイアウォール、スイッチという機器もデータが直列に通過する場合は、ネットワーク機器としてまとめることができる。機能の絞り込みの実施例を、図 3-3 に示す。

注意すべき点は、マルチベンダーによる機器構成の場合、あるベンダーの機器は十分なセキュリティ対策を実施しているが、別のベンダーの機器は、殆どセキュリティ対策を実施していない場合が考えられる。この様に、セキュリティレベルが極端に異なる様な資産をまとめる際には、セキュリティレベルの判定には注意が必要である。

例えば、データを並列で処理する機器を一つにまとめる場合、各機器のうち、最も低いセキュリティレベルが、まとめた機器全体のセキュリティレベルとなる。一方、データを直列に処理するネットワーク機器等の場合は、各機器のうち、最も高いセキュリティレベルが、まとめた機器全体のセキュリティレベルとなる。この点については 4.1 節で詳しく記述する。

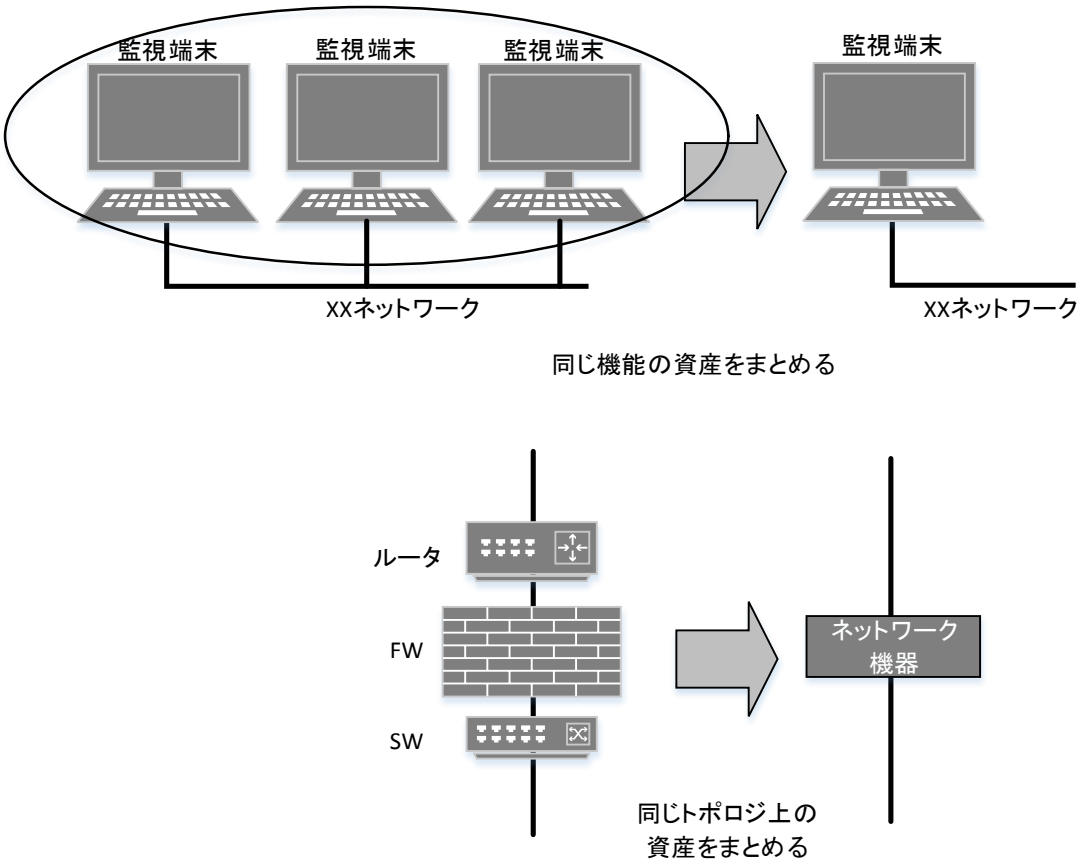


図 3-3 機能からの絞り込み例

② 非定常稼働機器の除外

一時的にしか稼働しない非定常稼働機器を、分析対象に含めるか除外するかを検討する。

非定常稼働機器とは、例えば、保守用 PC の様に、定常の稼働状態では制御に影響を与えず、メンテナンス時のみ稼働する様な機器を指す。

非定常稼働機器は、定常稼働品と比較して管理が不十分であることがあり得る。この場合、非定常稼働機器の存在がセキュリティ上の脅威となるケースも想定される。

しかしながら、非定常稼働機器を分析対象とすると、対象が増加し分析時の条件設定が膨らみ、セキュリティリスク分析の工数が増大して、作業が難航する場合もある。最終的には分析対象とすべきと考えられるが、非定常稼働機器は別途セキュリティ管理を行うことを前提に、分析対象から除外する事も検討する。例えば、初回の分析では除外し、2 回目以降の分析で加えることも選択肢となる。

本書では、非定常稼働機器は除外して説明を行う。

【分析対象の資産一覧表の例】

資産の洗い出し、分析対象とする資産の絞り込みが終了したら、次のプロセスで利用しやすい様に、収集した資産の情報を「分析対象の資産一覧表」としてまとめておくと良い。その際に、資産が(2)で定めたどのネットワーク上に存在するかも併せて記載しておく。

資産一覧表のフォーマットは任意であるが、表 3-6 に一例を示す。

表 3-6 分析対象の資産一覧表の例

No.		1	2	3	4
資産名		データサーバ	PLC	制御 ネットワーク	PLC 回線
資産分類		機器		通信経路	
定常稼働、非定常稼働		定常	定常	定常	定常
資産の 持つ 機能	入出力				
	データ保存	○			
	コマンド発行		○*1		
	ゲート				
回線種類（ネットワーク）				有線 LAN	専用線
設置場所		サーバ室	フィールド		
接続先 ネット ワーク	情報ネットワーク				
	DMZ				
	制御ネットワーク（情報側）	○			
	制御ネットワーク（フィールド側）	○	○	○	
	その他		フィールド機器		PLC−PLC
管理ポートの接続先		無し	無し		
データの種類と経路		プロセス値： PLC →データサーバ →HUB →データヒストリアン	プロセス値： フィールド機器 →PLC →データサーバ コマンド： 制御サーバ →PLC		
構築ベンダー／機器メーカー		XXX 社	YYY 社	ZZZ 社	QQQ 社
OS／バージョン		Windows Server	独自		
使用するプロトコル		独自、UDP	TCP、UDP	独自	TCP
セキュリティ対策		ホワイトリスト	USB ポートロック	デバイス 接続制限	通信相手 の認証
		アカウント管理			
		USB ポートロック			
		セキュリティ パッチ			
備考		パッチは1週間 以内に適用			

*1 操作器に対してのコマンド発行とみなした

(5)エリアごとの資産の配置

システム構成図を作成する際には、資産が配置されているエリアにより物理的なセキュリティ対策が異なる場合があるため記録が必要になる。

例えば、ある資産の設置場所がオフィスで、別の資産は入退認証のあるサーバ室であるという様に、分析対象の設置されている場所により物理的セキュリティのレベルが異なるケースがあるため、資産の置かれているエリアをシステム構成図作成時に明確にする。

そこで、物理セキュリティレベルの異なる場所は別のエリアとした区分図を作成し、次に作成したエリアごとに資産を配置する(図 3-4)。

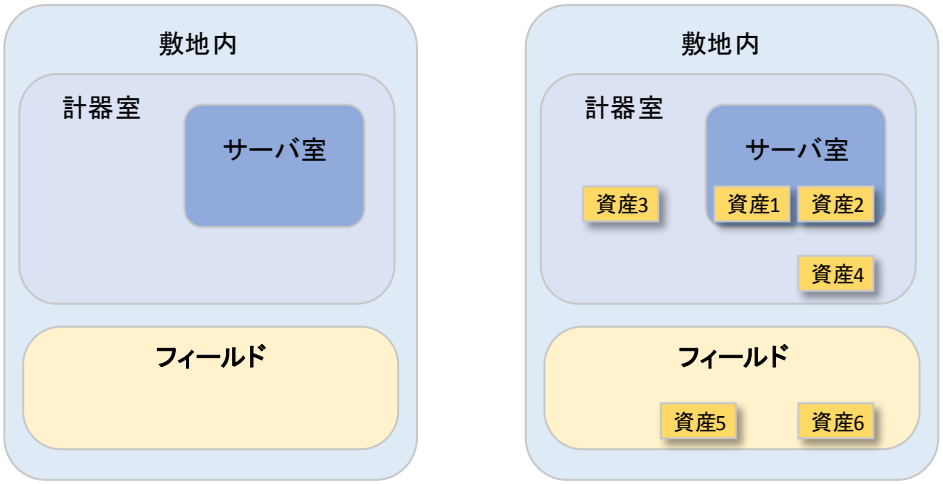


図 3-4 エリアと資産配置

(6)各資産の接続状況の記述

ネットワークを配置し、資産をネットワークに接続する。このとき、分析対象の資産一覧表を作成する際に調査した、各資産の接続先ネットワーク(情報ネットワーク、DMZ、制御ネットワーク(情報側／フィールド側)、フィールドネットワーク)の情報に従い、接続する(図 3-5)。

また、ファイアウォール等の様に管理ポートを持つ資産では、管理ポートの結線状態も明記する。例えば、管理ポート経由での管理者権限のログイン、設定変更によるファイアウォールとしての機能を無効化する攻撃が考えられるため、管理ポートのセキュリティ対策の分析が必要となる。

資産の接続関係を明確にすることは、主に 4.2 節の事業被害ベースのリスク分析で正確な分析を行うために重要である。

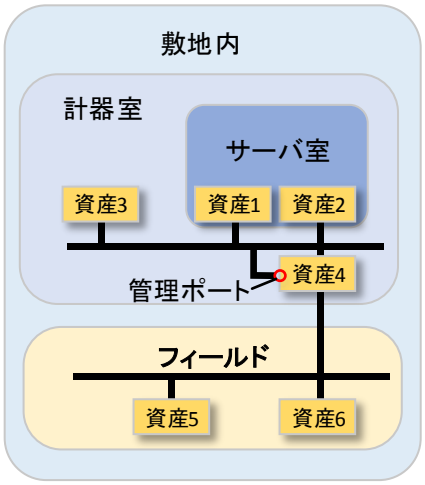


図 3-5 資産配置と接続

【コラム】

セキュリティ対策上の要所

ファイアウォールやスイッチの様な機器は、通常の通信を行うポート以外に、機器の設定管理用の管理ポートを持っている場合がある。管理ポートの形態は、他の機器と同様にネットワークに接続されるポートの場合や、イーサネットとは別のシリアルポート等の場合もあるが、管理ポートから接続設定の変更が可能なため、セキュリティ対策上の要所である。

管理ポートを分析対象とするか否かは、ケースバイケースだが、見落としがちな部分であるため、最低限、通常どこにどの様に接続されていて、どの様な扱いになっているか、確認しておくことを推奨する。

3.1.2. システム構成例

（1）典型的なシステム構成

3.1.1 項（図 3-3）で紹介した 4 種類の制御システムのネットワークセグメント分割方式アーキテクチャのうち、最も広く採用されていると考えられる、分類 3「DMZ」を元にして作成した、分析用システム構成図の例を図 3-6 に示す。

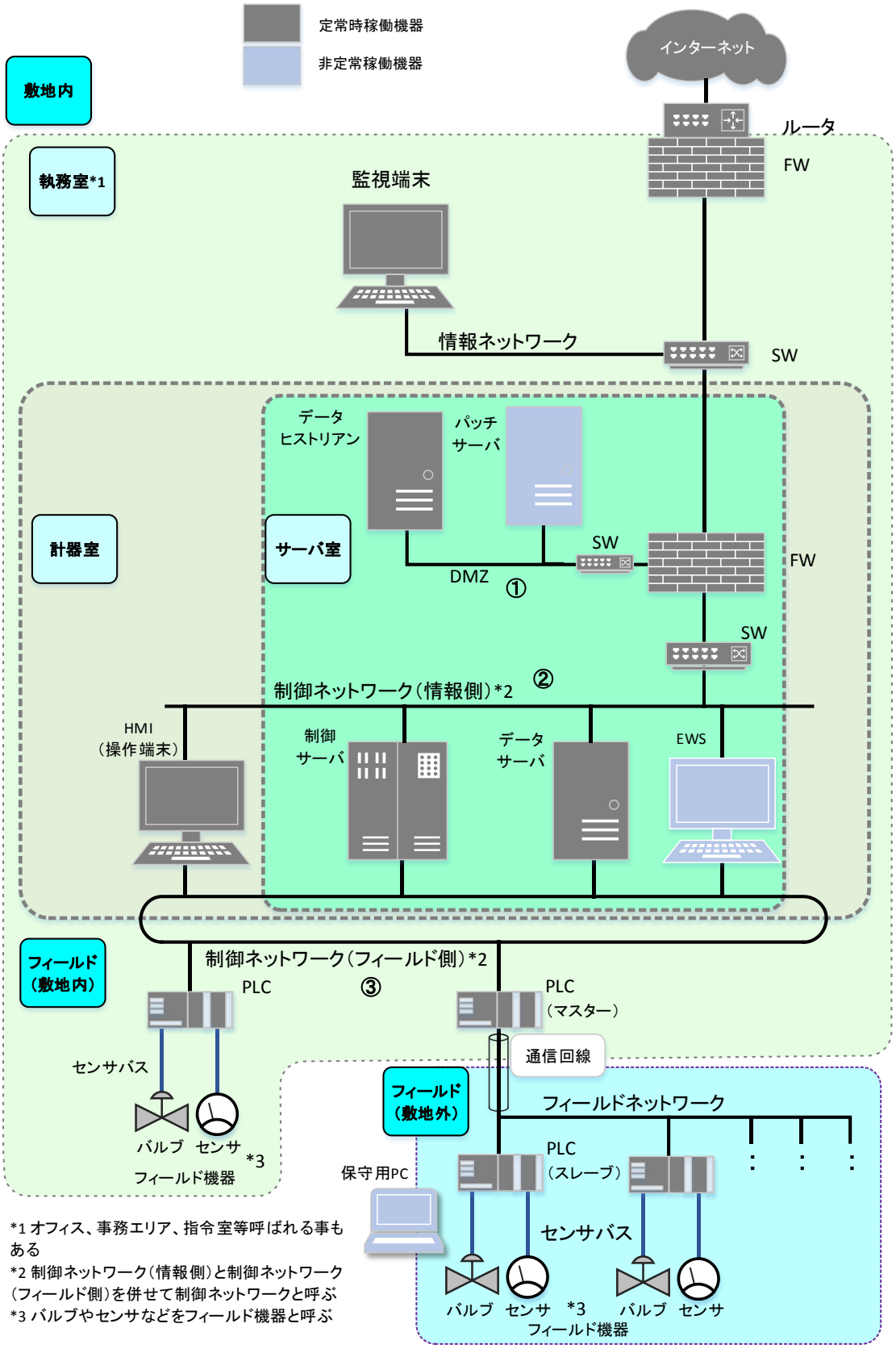
本アーキテクチャにおける制御システムのネットワークは、「情報ネットワーク」、「DMZ」、「制御ネットワーク」（情報側／フィールド側）、「フィールドネットワーク」から構成されている。各ネットワークの定義、他の標準規格等における名称との関係を、表 3-7 に示す。

情報ネットワークと制御ネットワークの間に DMZ があり、DMZ を介して制御ネットワークのデータが情報ネットワーク上の監視端末に送信される（①）。

制御ネットワークは、大量のデータを転送するための「制御ネットワーク（情報側）」（②）と、フィールド機器への指示値とプロセス値をリアルタイムに転送するための「制御ネットワーク（フィールド側）」（③）から構成されている。

なお、情報ネットワーク、DMZ 及び制御ネットワーク（情報側）は、Ethernet や標準プロトコル等の汎用的なネットワーク技術が用いられているが、制御ネットワーク（フィールド側）では、セキュリティや制御の応答時間の保証等の理由から、制御機器ベンダー固有のネットワーク技術（独自仕様のネットワークやプロトコル）が利用されている場合が多い。

表 3-8～表 3-9 に、各資産とその役割を示す。



*1 オフィス、事務エリア、指令室等呼ばれる事もある
*2 制御ネットワーク（情報側）と制御ネットワーク（フィールド側）を併せて制御ネットワークと呼ぶ
*3 バルブやセンサなどをフィールド機器と呼ぶ

図 3-6 典型的な制御システムの構成図（分類 3：DMZ）

【コラム】

制御システムの構成要素（PLC, DCS, SCADA）の名称と定義

図 3-6 において、PLC の位置には、DCS や I/O コントローラと呼ばれる PA（プロセスオートメーション）用の制御機器が接続される場合もあるが、本書では制御ネットワーク（フィールド側）に接続される代表的な制御機器として、PLC を用いて以降の説明を行う。

DCS（Distributed Control System）は、主に PA（Process Automation）におけるプロセス値を連続的に変化させる複雑な制御に用いられ、制御周期は 0.5～1 秒程度である。一方、PLC は、FA（Factory Automation）におけるスイッチや機器のロジック制御やシーケンス制御を行うために用いられ、制御周期は 1 ミリ秒程度と高速である。しかしながら、その適用範囲は両者ともに広がっており、機能上の区別は難しくなってきている。

DCS の接続形態は、PLC と完全に同じであるとは限らない。また、DCS という用語自体、分散化したシステム全体を指す場合や I/O を含む等、定義範囲が不明確な場合がある。

更に、フィールドネットワークや制御ネットワーク（フィールド側）に接続されたシステム全体を指して、SCADA（Supervisory Control and Data Acquisition）と表現する場合がある。図中のデータサーバ、制御サーバの機能を SCADA（ソフト）と表現する場合がある。

この様に、制御システムの構成要素の名称・定義は明確に定まっていないため、本ガイドで採用している用語を、各自用いている名称との間で、適宜読み替えをして頂きたい。

表 3-7 制御システムにおけるネットワークの定義

名称	定義	他の標準規格等における名称		
		NIST SP800-82 Clause 5.5	IEC 62443-2-1 Annex A.3.3.4.2	IPA 調査報告書（2009 年 3 月）
情報ネットワーク	企業内で構築されたローカルエリアネットワーク（LAN）で、外部ネットワーク（インターネット等）との接続点に存在する。本書においては、制御ネットワーク（DMZ 経由を含む）と接続されている LAN を示す。 制御システムによっては、外部ネットワークから隔離されており、情報ネットワークが存在しない場合もある。	Corporate Network	WAN, Site LAN	情報ネットワーク
DMZ	DeMilitarized Zone の略で、直訳すると「非武装地帯」。本書においては、情報ネットワークと制御ネットワークとの境界に設けられるネットワークを示し、制御システムによっては、DMZ が存在しない場合もある。制御ネットワークからの情報は DMZ 上の機器にいったん保存され、情報ネットワークからは DMZ 上の機器にアクセスすることで、情報ネットワークと制御ネットワークの間の直接通信を、全て排除または大幅に削減する。	DMZ	DMZ	（未定義）
制御ネットワーク	制御目的に使用するデータを転送する LAN。	Control Network	PCN: Process Control Network	（未定義）
制御ネットワーク（情報側）	情報ネットワークまたは DMZ 上の機器（サーバ等）との間で、制御目的に使用するためのステータス（接点の状態）情報やデータを転送するためのネットワーク。			制御情報ネットワーク
制御ネットワーク（フィールド側）	自ネットワーク及びフィールドネットワーク上の機器（PLC）との間で、制御目的に使用するためのステータス情報やデータを即時転送するためのネットワーク。制御に特化した高い応答性を持つ。			制御ネットワーク
フィールドネットワーク	制御ネットワーク（フィールド側）の PLC 等の接続機器とフィールドに存在する機器の間の通信に用いられるネットワーク。 センサバスを含めて「（広義の）フィールドネットワーク」と呼ぶこともあるが、本書では狭義の意味で用いる。	（未定義）	RCN: Regulatory Control Network, FDN: Field Device Network	フィールドネットワーク

表 3-8 典型的な制御システム構成における資産とその役割(1/2)

名称	説明	機能	データの種類と経路	定常/ 非定常
監視端末	工程や現場の状況を確認するための端末。	入出力	長期トレンドデータ: データヒストリアン→(監視端末)	定常
データ ヒストリアン	長期間のプロセス値や管理パラメータが保存され分析されるサーバ。 データサーバより静的なデータを扱う。	データ保存	プロセス値: データサーバ→(データヒストリアン)→監視端末	定常
HMI (操作端末)	制御機器やフィールド機器に対する指示を入力する端末。	コマンド発行	設定値: (HMI)→制御サーバ プロセス値: データサーバ→(HMI)	定常
制御サーバ	制御機器やフィールド機器に対し設定値やコマンドを送出するサーバ。	コマンド発行	制御コマンド、設定値: HMI→(制御サーバ)→PLC	定常
データサーバ	制御ネットワーク上にありプロセス値を収集するサーバ。更に PLC から届いたプロセス値を転送する。	データ保存	プロセス値: PLC→(データサーバ)→データヒストリアン→監視端末	定常
PLC	センサからの信号により接点や操作器を制御する等入出力信号を扱う機器。 制御サーバやデータサーバと PLC との間の通信を中継する PLC も存在し、中継する側を「PLC(マスター)」、中継される側を「PLC(スレーブ)」と示す。	コマンド発行	コマンド: 制御サーバ→(PLC)→フィールド機器 プロセス値: フィールド機器→(PLC)→データサーバ	定常

表 3-9 典型的な制御システム構成における資産とその役割(2/2)

名称	説明	機能	データの種類と経路	定常/非定常
ルータ／スイッチ	複数のネットワークを集線、中継する機器。	ゲート	メール、Web 等: インターネット→(各スイッチ／ルータ)→情報ネットワーク 長期トレンドデータ: 情報ネットワーク→(各スイッチ／ルータ)→DMZ	定常
ファイアウォール(FW)	外部のネットワークからの攻撃や侵入を防ぐための機能を有する機器。	ゲート	長期トレンドデータ: DMZ→(FW)→情報ネットワーク プロセス値: 制御ネットワーク→(FW)→DMZ	定常
パッチサーバ	接続された機器の OS やソフトウェアのアップデートやパッチ、アンチウイルスのパターンファイル等を提供するサーバ。	データ保存	パッチデータ: インターネット、または情報ネットワーク上のパッチサーバ→(パッチサーバ)→データヒストリアン	非定常
EWS	PLC のラダープログラムの改造や制御サーバのプログラムの変更等を行うためのコンピュータ。	データ保存、コマンド発行	プログラム: プログラム入手先→(パッチサーバ)→PLC、またはフィールド機器等	非定常
保守用 PC	PLC やフィールド機器のメンテナンスを行うための PC。	コマンド発行	制御コマンド等: (保守用 PC)→PLC、またはフィールド機器	非定常

【コラム】

ゾーン（セキュリティゾーン）について

制御システムに関する標準規格において、領域を意味する「ゾーン」という言葉が用いられている。これらは、正確には「セキュリティゾーン」の省略形で、ネットワークを分割（セグメント化）する単位である。セキュリティリスクを管理し、ネットワークセグメントごとに目標のセキュリティレベルを達成するためには、制御システムにおける重要資産を、共通のセキュリティレベルを持つゾーンに分離することが望ましい、とされている。

例えば、IEC 62443 では、IT 系のビジネス業務用のネットワークが存在する領域を Business/Enterprise zone、制御システムが稼働する領域を Control zone、その中間で主に制御ゾーンの機器のサポートを行う機器が存在する領域を DMZ と記している（図 A）。

一方、IEC 62443 シリーズの母体となった ISA 62443 を開発している ISA99 委員会では、近年、ミッションの重要度によって実現すべきセキュリティレベルを設ける際に、新たにゾーンの概念を提唱し、細かなゾーン分け（ゾーニング）を推奨している（図 B）。

また、ベンダー等の情報を見る限り、「ゾーン」という言葉は、定義が曖昧なまま、様々な区分をするために用いられている場合が見受けられる。

これらの現状を考慮し、本書では「ゾーン」という言葉を用いずに、セグメント化された「ネットワーク」と、ネットワーク上の「資産」という表現を用いて説明している。

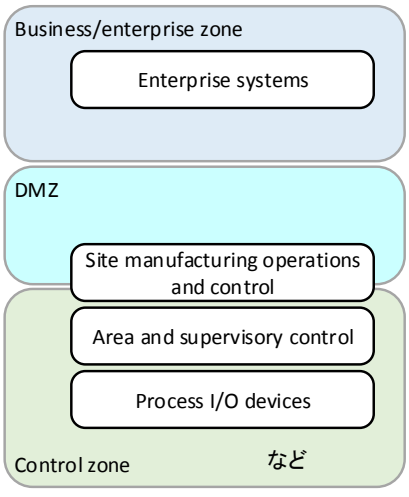


図 A　IEC 62443-2-1 におけるゾーン

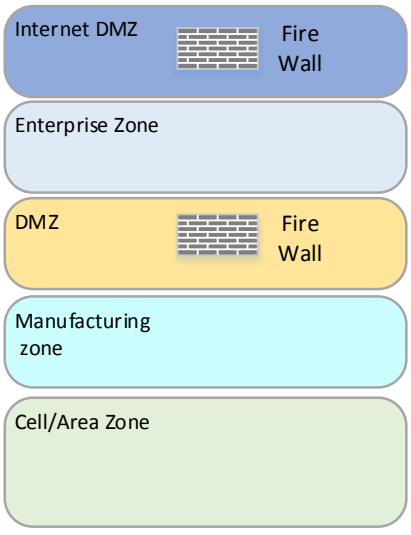


図 B　ISA99 におけるゾーン

（2）その他のシステム構成

残りの 3 種類のネットワークセグメント分割方式アーキテクチャを元にして作成した、分析用システム構成図の例を、図 3-7、図 3-8、図 3-9 及び図 3-10 に示す。以下、それぞれのシステム構成について説明する。

【分類 1】 FW （図 3-7）

情報ネットワークと制御ネットワークはファイアウォールで分離しているが、DMZ が存在しない最も単純な構成。

【分類 2】 FW＋ルータ （図 3-8）

分類1と同様情報ネットワークと制御ネットワークはファイアウォールで分離しているが、DMZ が存在しない構成。ルータはパケットのフィルタリングの役割を果たし、ファイアウォールはステートフルパケットインスペクション等の複雑な処理を行う。DoS 攻撃に備えファイアウォールの負荷を減らすことができ、2 種類のデバイスを通過する必要が出てくるため多層防御の効果もある。

【分類 4】 ペアード FW （図 3-9）

情報ネットワークからファイアウォールを介して DMZ を設け、DMZ 上の機器から更にもう一つのファイアウォールを介して制御ネットワークへ接続する構成。情報ネットワーク側のファイアウォールは、不定のパケットが制御ネットワークやデータヒストリアンに流れない様にブロックし、制御ネットワーク側のファイアウォールは、データヒストリアンにセキュリティ上の問題が発生した際に、制御ネットワークへの侵入を防ぐためにある。これら 2 段のファイアウォールの種類を別のものにしておくと、例えばファームウエアの脆弱性が露見した様な場合でも、制御ネットワークの侵入を困難にして保護することができる。

【その他の例】 アプリケーション GW （図 3-10）

分類 1 または分類 2 の変形として、通常のファイアウォールの代わりに、アプリケーションゲートウェイ（アプリケーションゲートウェイ型ファイアウォール）を利用する構成が考えられる。アプリケーションゲートウェイは、HTTP や FTP 等アプリケーション層でフィルタリングを行い、ネットワーク間の不正な直接通信を防止する。本構成では、データヒストリアン等他の機能を併せ持たせることができるため、機器の数を削減できる利点がある。

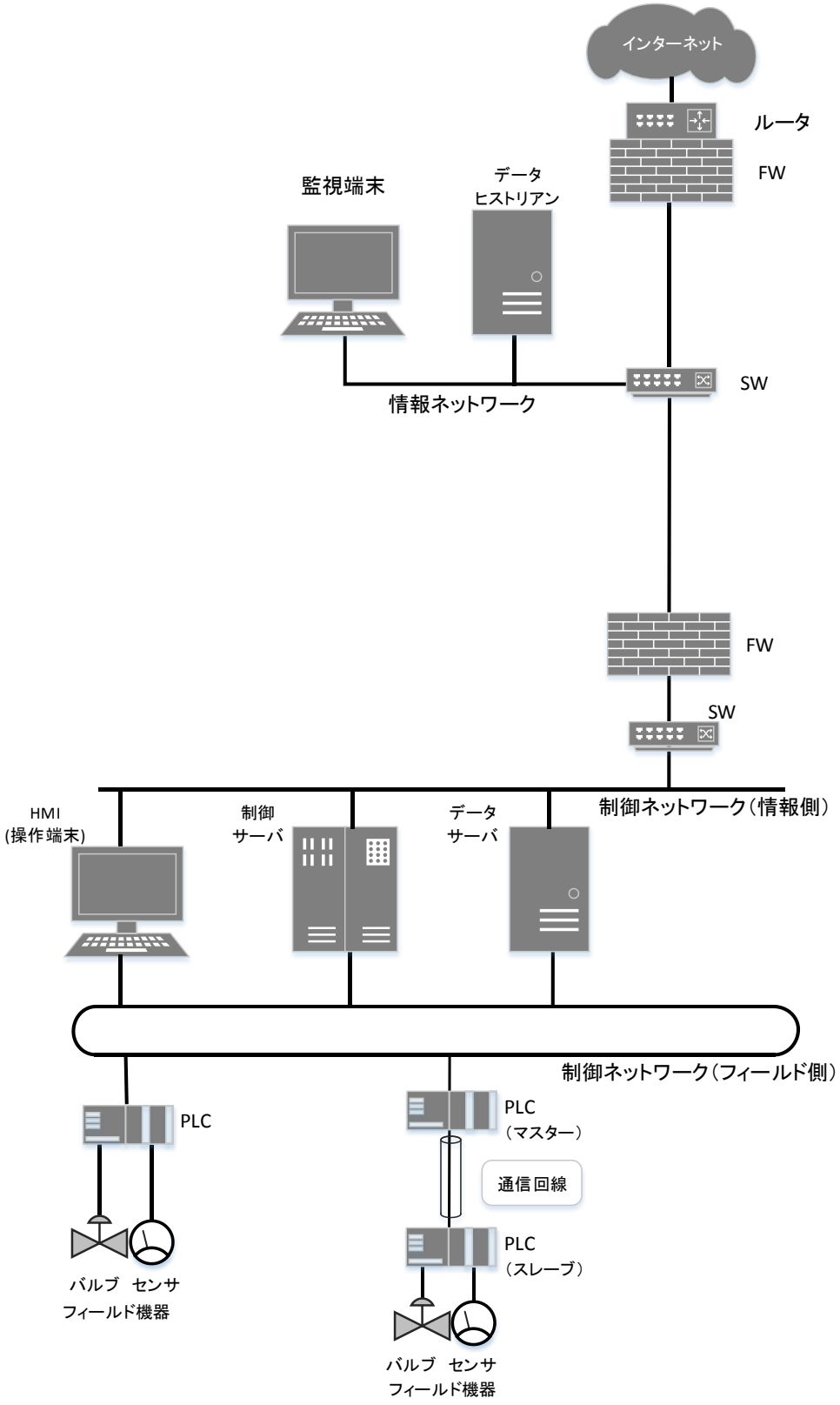


図 3-7 その他の制御システム構成図（分類 1：FW）

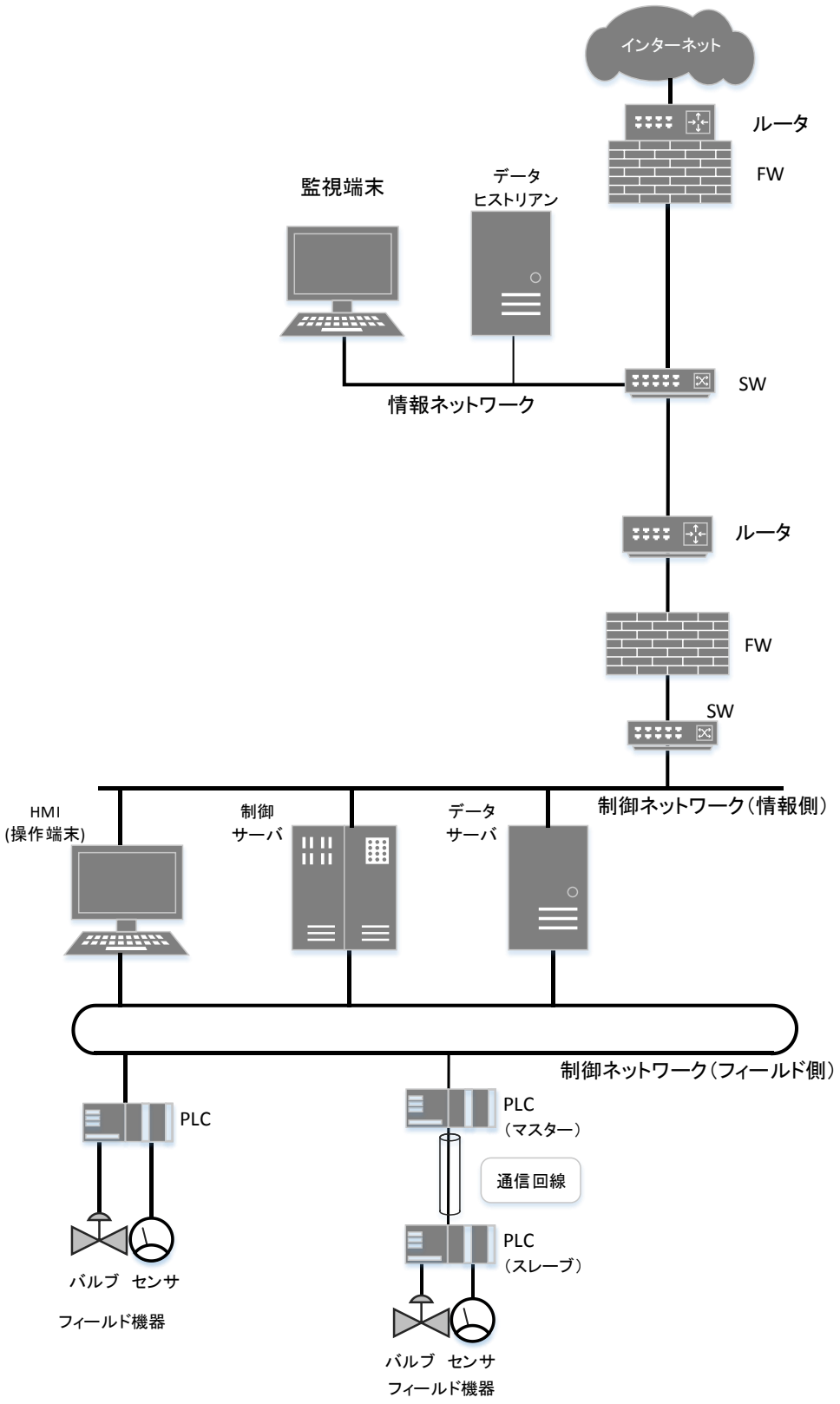


図 3-8 その他の制御システム構成図（分類 2：FW＋ルータ）

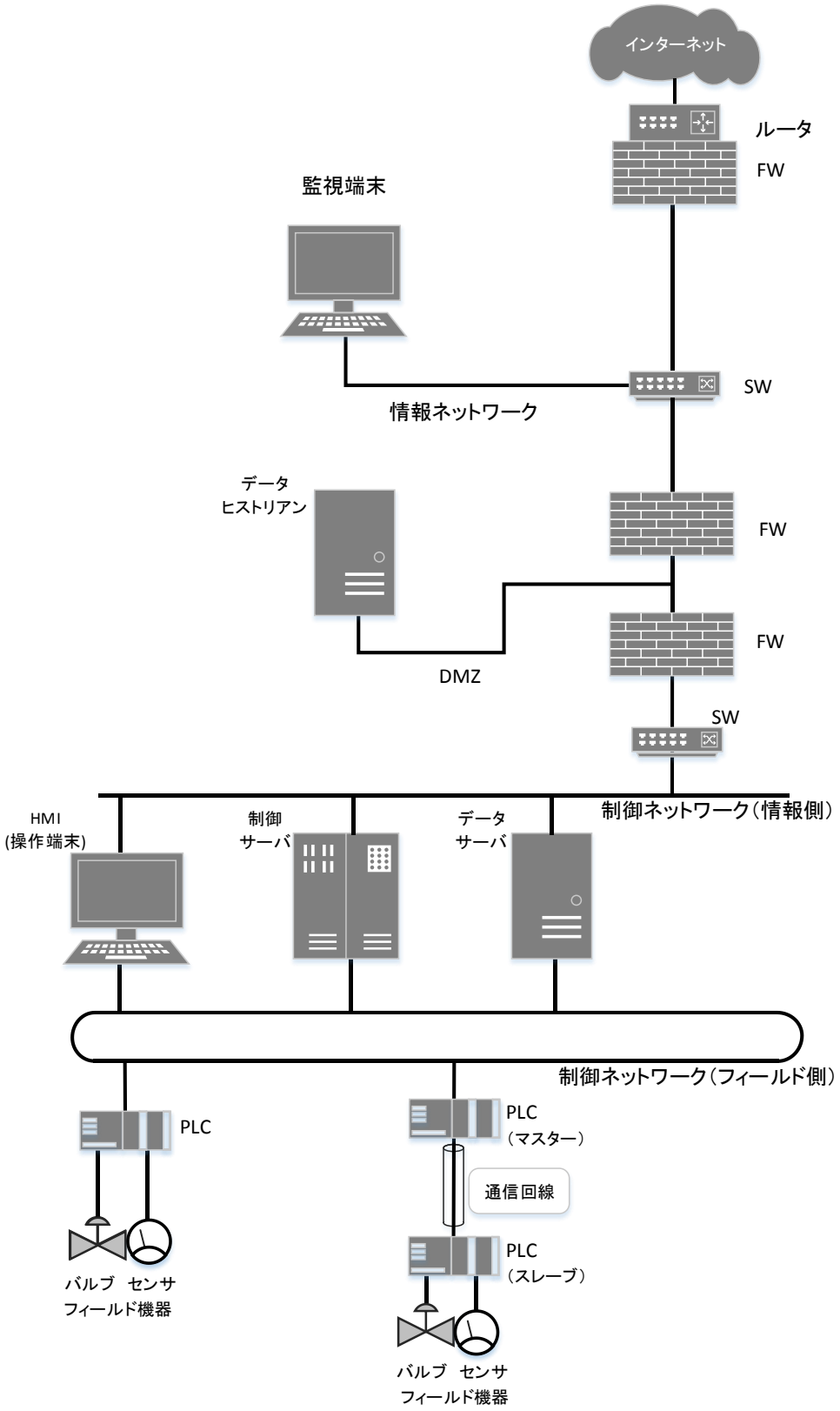


図 3-9 その他の制御システム構成図（分類 4：ペアード FW）

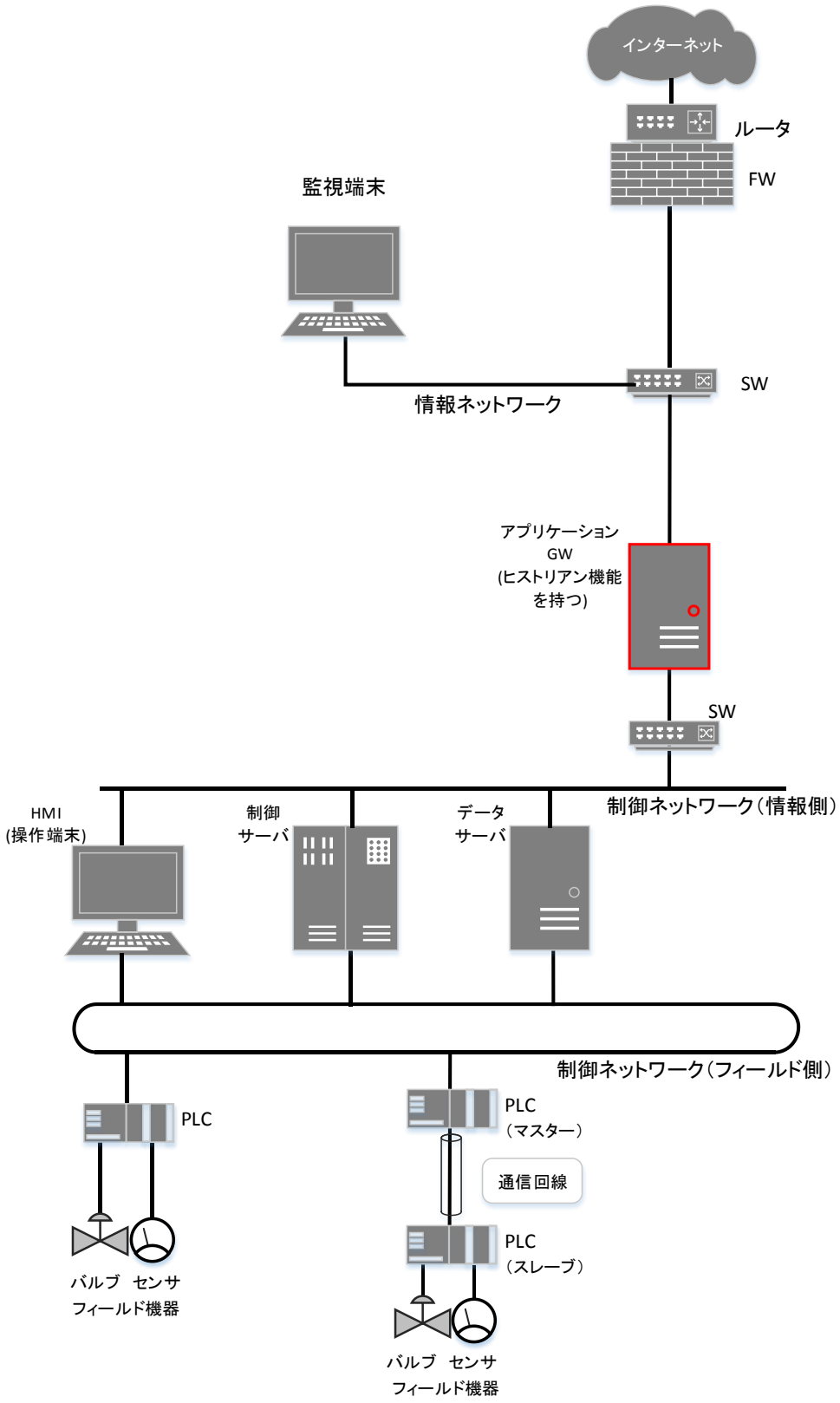


図 3-10 その他の制御システム構成図（分類 2'：アプリケーション GW）

3.1.3. データフローの明確化

データフローを明確にするには、3.1.2 項で記載したデータの送信元とデータの転送先のデータを用いる。注意すべき点は、経路となる機器が存在する場合、いったんその機器にデータが保存される（改ざんの恐れがある）のか、転送されるだけなのかを確認することである。

データフローをシステム構成図に直接記載をすることで、システム全体の仕組みを容易に理解できる様になる。

（1）典型的なデータフロー

3.1.1 項で紹介した分類 3「DMZ」の制御システム構成（図 3-6）における典型的なデータフローとしてここでは、以下を紹介する。

ここでは制御とその結果を監視するデータフローを想定している。

【制御時のデータフロー】

HMI → 制御サーバ → PLC → フィールド機器

【監視時のデータフロー】

フィールド機器 → PLC → データサーバ → FW → データヒストリアン → 監視端末

実際のシステムでは、データが一時的に保存される場合や、例外的に異なる経路を通るデータが存在する場合もあるので、漏れのない様に記述する。

（2）典型的なシステム構成におけるデータフローの例

図 3-11 は、システム構成図（図 3-6）上にデータフローを記載したものである。

制御ネットワーク（フィールド側）からの情報は、データサーバに保存された後、DMZ にあるデータヒストリアンへフィールドのデータを転送する。情報ネットワークからは、このデータヒストリアンにアクセスすることで、プロセス状態を監視することができる。

本システムでは、情報ネットワークから制御ネットワークへ直接通信を行うことはできないと仮定して、データフローを記載した。また、実際の認証情報やリクエスト等通信自体は多数の機器相互間で行われるが、ここでは説明をわかりやすくするため、データとコマンドの流れのみに注目したフローを記している。

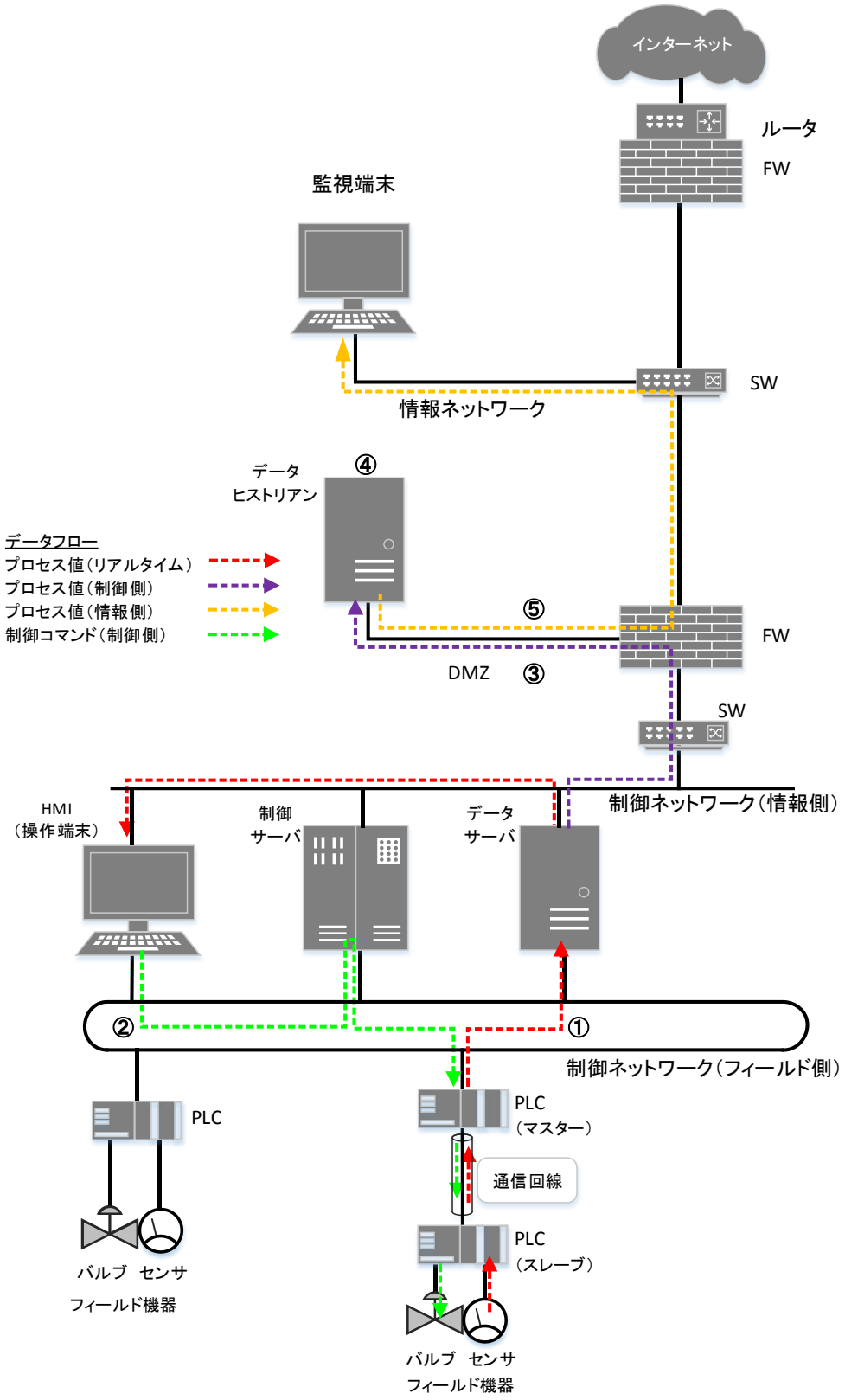


図 3-11 典型的な制御システム（分類 3：DMZ）におけるデータフローの例

この図において、更に細かくデータフローを追うと、以下の様に表現できる。

① フィールドのセンサの測定値（プロセス値）は、PLC にまとめられデータサーバに送られる。従って、データサーバには各所のセンサからのリアルタイムのプロセス値が集約されている。また、データサーバ内のプロセス値は HMI から参照できる。
② 制御ネットワーク（情報側）上の HMI では、データサーバの示すプロセス値にしたがい、新たな設定値をフィールド機器に送付する。設定は制御サーバを介して行われるので、HMI からの命令→制御サーバ→制御サーバからのコマンド発行→PLC がコマンドを受信して、フィールド機器へデータを転送する。
③ データサーバのプロセス値は、一定の周期で、DMZ 上にあるデータヒストリアンに転送される。
④ データヒストリアンでは、データサーバからのプロセス値が蓄積され、長期的なトレンドデータとして利用が可能となる。大量のデータを用いて、長期間の分析が行われる。
⑤ 分析結果は、情報系ネットワーク上の監視端末でモニタされ、稼働状況を把握することができる。

（3）その他のシステム構成におけるデータフローの例

3.1.2 項と同様に、分類 3 以外の制御システム構成（図 3-7～図 3-10）におけるデータフローの例を、図 3-12、図 3-13、図 3-14 及び図 3-15 に示す。以下、それぞれのデータフローの概要と特徴について説明する。

【分類 1】 FW （図 3-12）

分類 3 と比べると DMZ がないため、プロセス値は直接情報ネットワーク上のデータヒストリアンに保存される。従って、情報ネットワークと制御ネットワーク間で直接通信が生じる。

【分類 2】 FW＋ルータ（図 3-13）

分類 1 と同様に DMZ がないためプロセス値は直接情報ネットワーク上のデータヒストリアンに保存される。データフローは基本的に分類 1 と同じ。

【分類 4】 ペアード FW （図 3-14）

分類 3 と同様にデータは一度 DMZ 上のデータヒストリアンに保存される。情報ネットワークからの制御データの参照は、ファイアウォール経由で DMZ 上のデータヒストリアンと通信を行う形となり、情報ネットワークから制御ネットワークへの直接通信を不要にする設計が可能である。

【その他の例】 アプリケーション GW （図 3-15）

本例では、アプリケーションゲートウェイを介して情報ネットワークと制御ネットワーク間の通信が行われる。プロセスデータは、データヒストリアン機能を持つアプリケーションゲートウェイに蓄積される。情報ネットワーク側からの制御データの参照は、このアプリケーションゲートウェイへのアクセスで行われ、情報ネットワーク側から制御ネットワーク側への直接通信を不要にする設計が可能である。

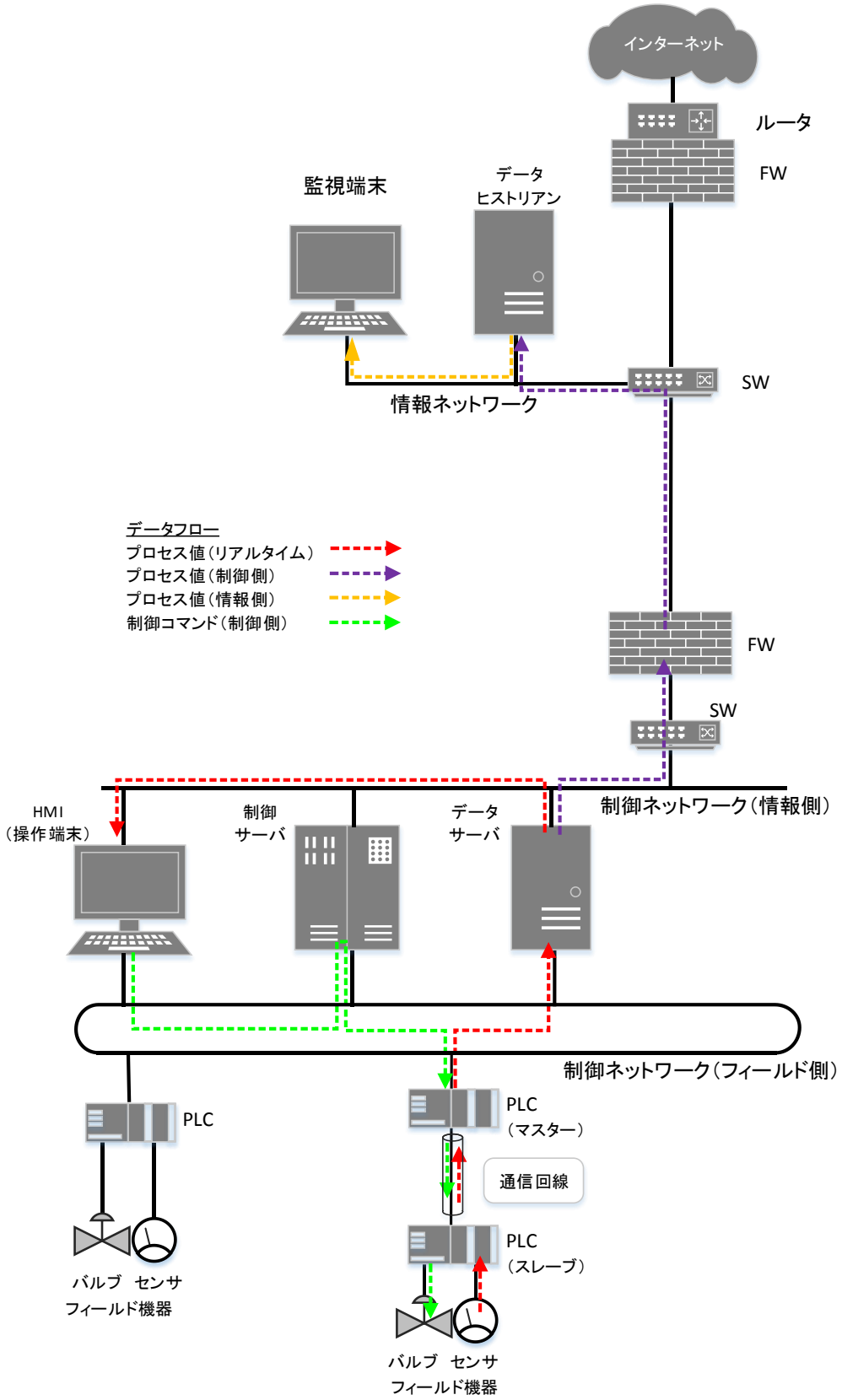


図 3-12 その他の制御システム（分類 1：FW）におけるデータフローの例

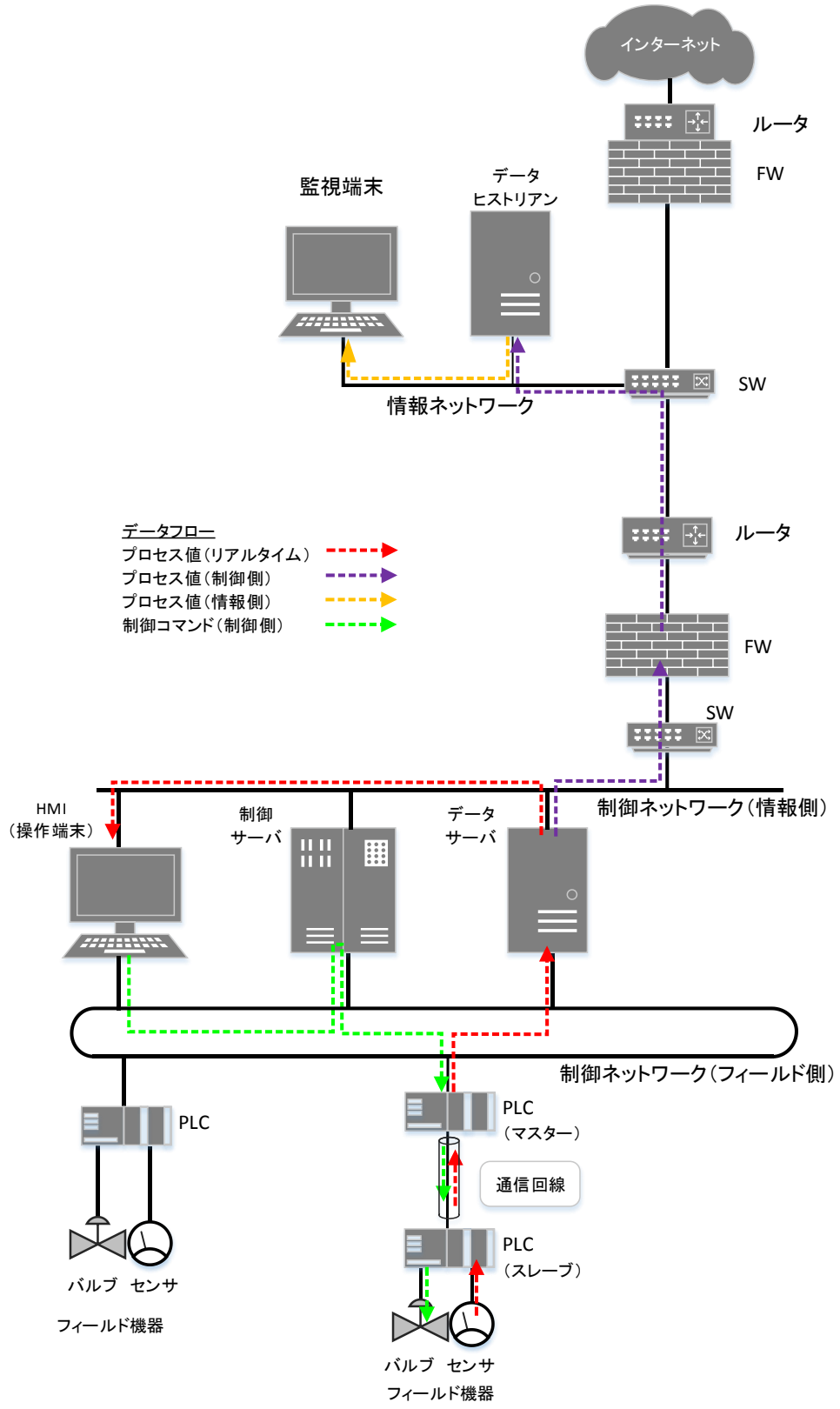


図 3-13 その他の制御システム（分類 2：FW+ルータ）におけるデータフローの例

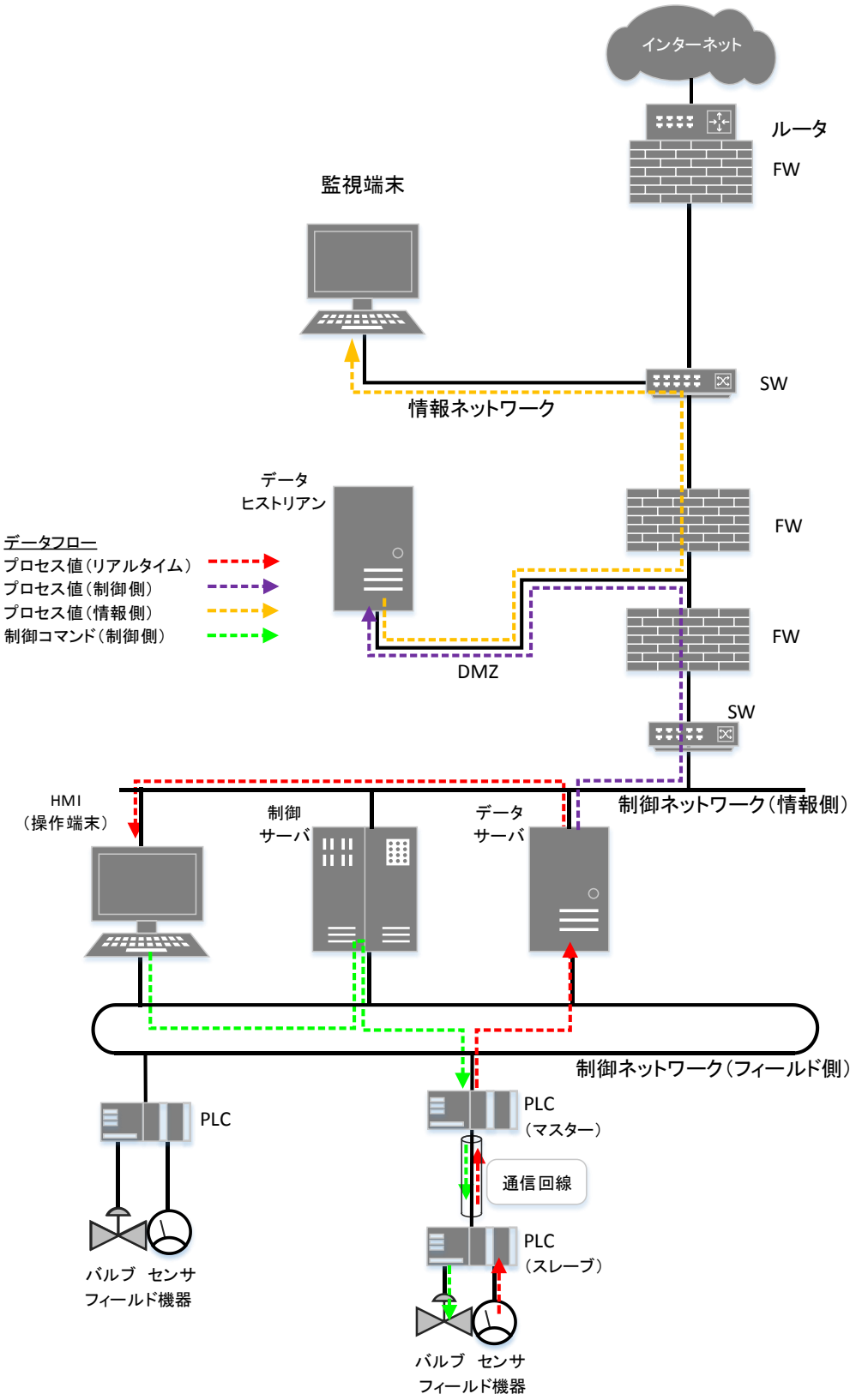


図 3-14 その他の制御システム（分類 4：ペアード FW）におけるデータフローの例

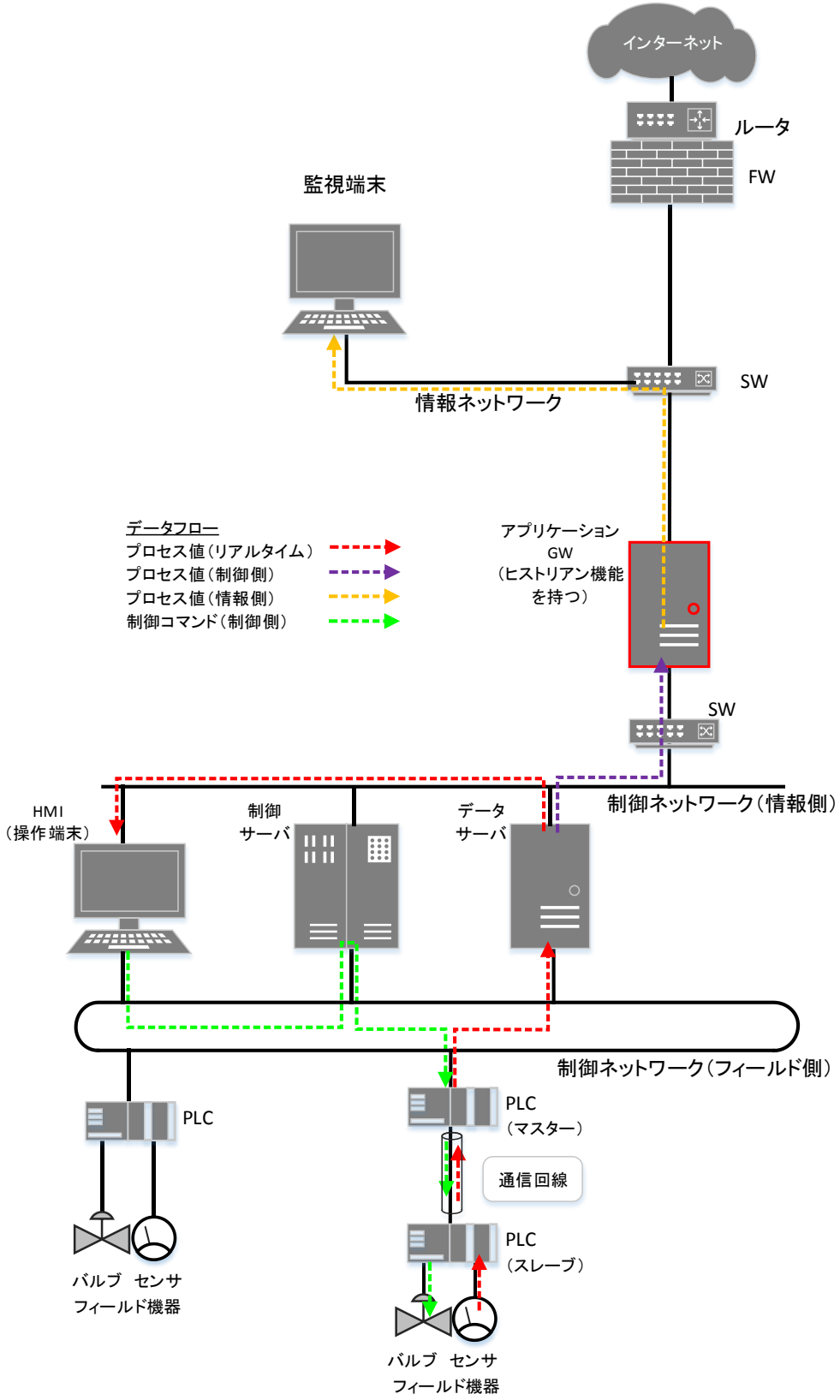


図 3-15 その他の制御システム（分類 2'：アプリケーション GW）におけるデータフローの例

3.2. 資産の重要度の決定

本節では、資産ベースのリスク分析における評価指標の一つである資産の重要度の定義を行う。

資産の重要度とは、

① システム資産としての価値

その資産がサイバー攻撃を受けることによって想定される、

② 事業被害
③ 事業継続性の影響

を考慮して、その資産をどの程度のセキュリティ強度で守っていく必要性があるか、を示す指標である。上記①～③を検討する上で、攻撃によって実際に生じることが想定される、事業停止、サービス混乱、情報漏えい、情報改ざん等を念頭に置き、資産の重要度を決定する。例えば、その資産への攻撃による障害で事業停止に陥るならば、その資産に対する重要度は高く評価する。

本節のアウトプットは、以下となる。

- **資産の重要度の判断基準** （☞ 3.2.1 項）
- **各資産に対する重要度一覧** （☞ 3.2.2 項）

3.2.1. 資産の重要度の判断基準の定義

資産ベースのリスク分析において、資産の重要度は、3 段階(1～3)の値で評価する。資産の重要度＝“3”は重要度が高い(最も重要である)ことを意味し、資産の重要度＝“1”は重要度が低い(余り重要ではない)ことを意味する。

資産の重要度の観点は事業者ごとに異なるため、3.2 節の冒頭で示した①～③を考慮して各事業者にての判断基準を決定する。表 3-10 に資産の重要度の判断基準の定義例を示す。

表 3-10 資産の重要度の判断基準の定義例(1)

評価点	判断基準
3	・資産が攻撃された場合、システムが長期間停止する恐れがある。 ・資産から情報が漏えいした場合、巨額の損失が発生する恐れがある。 ・資産が攻撃された場合、大規模の人的／環境被害が発生する恐れがある。
2	・資産が攻撃された場合、システムが一定期間停止する恐れがある。 ・資産から情報が漏えいした場合、ある程度の損失が発生する恐れがある。 ・資産が攻撃された場合、中規模の人的／環境被害が発生する恐れがある。
1	・資産が攻撃された場合、システムが短期間停止する恐れがある。 ・資産から情報が漏えいした場合、小額の損失が発生する恐れがある。 ・資産が攻撃された場合、小規模の人的／環境被害が発生する恐れがある。

上記の例は、評価点の境界となる定量的な判断基準を曖昧なままの表現とした。実際には、各事業者の事業特性に応じて、明確な数値を評価点の境界値として定義することが望ましい。

その判断基準を具体化する際の参考情報として、IEC 62443-2-1 の Annex A.2.3.3.7(Table A.2 – Typical consequence scale)に示された、リスク分析のための典型的な結果の尺度例を、表 3-11 に示す。例えば、資産が攻撃された場合、あるいは資産から情報漏えいが発生した場合のリスク(被害の大きさ)を本表に従って 3 段階のレベルに分類し、その値を基に資産の重要度を定義するための判断基準の一つの参考となる。

表 3-12 は、表 3-11 の尺度の一部を参考に、表 3-10 で示した資産の重要度の判断基準の定義を、具体的に定義し直した例である。

表 3-11 IEC 62443-2-1 における典型的な尺度例

結果									
	リスク領域								
	事業継続性計画の作成		情報セキュリティ			産業活動の安全性		環境的安全性	国民への影響
カテゴリー	1 サイトでの製造停止	複数サイトでの製造停止	コスト[17]	法的	公衆の信頼	サイト内の人	サイト外の人	環境的安全性	基盤及びサービス
A(高)	7 日以上	1 日以上	5 億円以上	重い刑事犯罪	ブランドイメージの喪失	死亡	死亡または重大な地域のインシデント	地域機関もしくは国家機関からの召喚、または広範囲におよぶ長期間の重大な損傷	複数の事業分野に対する影響または地域サービスの大規模な動作中断
B(中)	2 日以上	1 時間以上	500 万円以上	軽い刑事犯罪	顧客の信頼喪失	休職または重傷	苦情または地域社会への影響	地域機関からの召喚	1 社の事業分野を超えるレベルでの事業分野への影響の可能性。地域サービスの影響の可能性
C(低)	1 日未満	1 時間未満	500 万円未満	なし	なし	応急手当または記録すべき怪我	苦情なし	報告可能限度額を下回る小規模かつ限定的な放出	個々の会社を超えるレベルでの事業分野への影響の可能性なし。地域サービスの影響なし。

[17] 1USD=¥100 で換算

表 3-12 資産の重要度の判断基準の定義例(2)

評価点	判断基準
3	・資産が攻撃された場合、システムが 1 週間以上停止する恐れがある。 ・資産から情報が漏えいした場合、5 億円以上の損失が発生する恐れがある。 ・資産が攻撃された場合、従業員の死亡事故が発生する恐れがある。
2	・資産が攻撃された場合、システムが 24 時間以上 1 週間未満停止する恐れがある。 ・資産から情報が漏えいした場合、500 万円以上 5 億円未満の損失が発生する恐れがある。 ・資産が攻撃された場合、従業員の重傷事故が発生する恐れがある。
1	・資産が攻撃された場合でも、システムが 24 時間以上停止する恐れはない。 ・資産から情報が漏えいした場合でも、500 万円以上の損失が発生する恐れはない。 ・資産が攻撃された場合でも、従業員の重傷事故が発生する恐れはない。

なお、表中に記した定量的な数値(システムの停止時間の長さ、被害金額等)は、対象とするシステム分野によって異なる。特に、システムの事業継続性を基にしたリスク分類の具体系な尺度は業界ごとに大きく異なっており、重要インフラの各分野における尺度の例(NISC 資料[18]より引用)を、表 3-13 に示す。

[18] 重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書(第1版)
https://www.nisc.go.jp/active/infra/pdf/shishin-tebiki1.pdf

表 3-13 業界ごとのサービス維持レベル

重要インフラ分野	対象・水準
電力	● IT の不具合により、供給支障電力が 10 万 kW 以上で、その支障時間が 10 分以上の供給支障事故が生じないこと。
ガス	● IT の不具合により、供給支障戸数が 30 以上の供給支障事故が生じないこと。
医療	● 医療機器の誤作動の招来等により、人の生命に危険が及ばないこと。 ● IT の不具合により、診療の継続に支障が生じないこと。
水道	● IT の不具合により、断減水、水質異常、重大なシステム障害のうち給水に支障を及ぼすものが生じないこと。
化学	● IT の不具合により、石油化学製品の供給に著しく重大な支障が生じないこと。
石油	● IT の不具合により、石油の供給の確保に支障が生じないこと。
鉄道	● IT の不具合により、旅客の輸送に支障を及ぼす列車の運休が生じないこと。
航空	● IT の不具合により、貨客の運送に支障を及ぼす定期便の欠航が生じないこと。
情報通信 （電気通信役務）	● 電気通信設備の故障により、役務提供の停止・品質の低下が、3 万以上の利用者に対し 2 時間以上継続する事故が生じないこと。
情報通信 （放送）	● 基幹放送設備の故障により、放送の停止が 15 分以上継続する事故が生じないこと。 ● 特定地上基幹放送局等設備及び基幹放送局設備の故障により、放送の停止が 15 分以上（中継局の無線設備にあっては、2 時間以上）継続する事故が生じないこと。
情報通信 （ケーブルテレビ）	● ケーブルテレビ設備の故障により、放送の停止が、3 万以上の利用者に対し 2 時間以上継続する事故が生じないこと。

各事業者において、これらの情報等を参考に、資産の重要度の判断基準を定義する。

3.2.2. 資産の重要度の決定

本項では、3.1.2 項に示した典型的な制御システムの構成（図 3-6）を例に、各資産の重要度を決定する手順を例示する。同図において、評価対象なる資産を列挙すると以下になる。

- 監視端末
- スイッチ
- ファイアウォール（機器）[19]
- データヒストリアン
- データサーバ
- 制御サーバ
- HMI（操作端末）
- PLC

なお、非定常稼働機器及びバルブ、センサ等のフィールド機器は本評価の対象外としている[20]ため、資産対象からも除外している。また、3.1 節にて記載した通り、スイッチとファイアフォールはまとめてネットワーク装置として資産の重要度を考える。ネットワーク装置にはネットワーク装置そのものと通信回線が含まれる。上記の資産に対して、表 3-10 を参考にして資産の重要度を確定した例を、表 3-14 に示す。

表 3-14 資産とその重要度の定義例

資産名	重要度レベル
監視端末	2
ネットワーク装置 ・スイッチ ・ファイアウォール（機器）	3
データヒストリアン	2
データサーバ	3
制御サーバ	3
HMI（操作端末）	3
PLC	3

19 一般的に、ファイアウォールは、ファイアウォールの機能を有する機器（ハードウェア、アプライアンス品）とファイアウォール機能自体（例えば、ルータによるアクセスリストの制限等）を意味する場合が考えられる。本節では、前者の意味で用いているため、”ファイアウォール（機器）”と表記して、ファイアウォール機器であることを明示的に区別している。

20本評価では、サイバー攻撃による攻撃が可能な装置機器に限定するため、常時稼働していない非定常稼働機器やバルブ、センサ等のフィールド機器は対象外とした。

【補足】CIA 要件及び HSE 要件を考慮した資産の重要度の評価例

3.2.2 項にて資産の重要度を決定したが、より詳細に資産の重要度を検討することも可能である。その手法を補足として例示する。

制御システムが備えるべきセキュリティ要件として、CIA（C：機密性、I：完全性、A：可用性）、及び HSE（H：健康、S：安全性、E：環境への影響）が考えられる。これら CIA 及び HSE を用いて資産の重要度レベルを決定する際の判断基準を定義する手法を紹介する。

情報システムにおけるセキュリティ要件である機密性（C）、完全性（I）、及び可用性（A）は、以下の様に定義される。

機密性：　アクセスを認可された者だけが、情報にアクセスできることを確実にすること。
可用性：　認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。
完全性：　情報及び処理方法が正確であること及び完全であることを保護すること。

情報システムにおいては、機密性が最も重視され、次いで完全性、可用性の順になるが、制御システムにおいては、可用性、完全性、機密性の順になる。例えば、制御システムでは、サービスが常時稼働していることが最優先の要件とされているケースが多い。また、制御システムにおいては、資産の重要度を考える際、上述の CIA の観点に加え、HSE の観点も併せて考慮すべきである。

資産そのものを攻撃した際、CIA の観点では、資産自身が受ける影響、及び攻撃されたことによってシステムに及ぼす影響として評価できる。一方、HSE の観点では、資産が攻撃を受けた後に攻撃されたことによって事業や社会に及ぼす影響として評価できる。HSE による評価は、更に、その影響を分類している。そのため、より具体的な事業被害を考慮する必要がある。

3.2.2 項に示した資産に対して、可用性（A）、完全性（I）、機密性（C）、健康（H）、安全性（S）、及び環境への影響（E）の尺度を、3 段階（3：重要度高、2：重要度中、1：重要度低）で評価する。資産によっては、上記尺度のいずれかを評価できない場合が考えられるが、その場合、当該尺度は無視する。6 つの尺度に対して、付与されたレベル値の最大値を、その「資産の重要度」の値と定義する。この判断基準は、本書における一例であり、各事業者において独自の判断基準を定義の上、資産の重要度を決定してもよい。

例えば、ある資産に関して、可用性=2、完全性=1、機密性=1、健康=2、安全性=1、及び環境

への影響=2 となった場合、その資産の重要度は”2”となる。上記尺度のうちいずれか一つでも“3”になった場合、資産の重要度は“3”となる。

健康（H）、安全性（S）、及び環境への影響（E）の尺度で評価する場合、これらの項目は、当該装置が攻撃を受けたと仮定し、その結果生じたシステムの障害、規定外の動作等による影響を評価する。そのため、これらの尺度を考慮する装置群は原則、コマンドやデータの送信ルートに位置する装置が対象となる。図 3-6 に示した装置群において、HSE の尺度で評価する対象装置群は HMI（操作端末）、制御サーバ、及び PLC になる。また、本項での検討は、HSE の尺度をまとめて評価することとするが、個別に評価可能であるならば、個別に検討することも選択肢となる。

このアプローチで上記の資産の重要度を決定した例を、表 3-15～表 3-17 に示す。

表 3-15 資産の重要度の検討例（1/3）

資産名	評価の説明	各尺度の評価値	重要度
監視端末	監視端末は制御信号を直接送受信していないので、破壊されてもサービス提供において直接影響は与えない。しかしながら、監視できない状態が長時間継続すると、真にシステム障害が発生した場合、その事実を検知できない可能性がある。そのため、可用性の観点での評価は“2”とする。機密性に関しては、データサーバ～監視端末間のデータ送受のみのため、コマンドシーケンスが窃取されたとしても、重大なインシデントが発生する可能性は低く、顧客への影響は低いと考える。よって、機密性の評価は“1”とする。	可用性:2 完全性:1 機密性:1	2
ネットワーク装置 ・スイッチ ・ファイアウォール（機器）	本装置群は、データの通過点である。本装置群が破壊もしくはシステムダウンに陥ると、制御データを正常に送信できない可能性がある。そのため、可用性の評価は“3”とする。仮に当該機器もしくはネットワークが破壊されても、システムに影響を及ぼさない場合もしくは影響が限定される場合は、評価を“1”もしくは“2”にすることも考えられる。また、スイッチやファイアウォールの設定情報の窃取、改ざんされる脅威も存在し、設定情報の窃取、改ざんによってシステムが停止する可能性はあるが、直接顧客に影響を与える被害は少ないと考えられる。よって、完全性、機密性に関する評価は“1”とする。完全性、機密性に関しても、可用性同様、顧客への影響度合いに応じて、評価を“1”もしくは“2”にすることも可能である。	可用性:3 完全性:1 機密性:1	3
データヒストリアン	データヒストリアンは、主にデータを保存しているため、データを改ざんされることが脅威となる。データヒストリアンで用いられるデータは直接制御に用いられることはないが、監視用のデータが含まれている可能性がある。データヒストリアンのデータが改ざんされ、改ざんされたデータに基づいてシステム監視を行った場合、システムの正常性を把握できない可能性がある。結果的にシステムの異常を検知できず、少なからず顧客影響が出ることも想定できるため、データヒストリアンの完全性に関する評価は“2”とする[21]。一方、当該装置群が破壊されたとしても、システムが停止する可能性は低く、また情報窃取されたとしても、顧客に影響をあたえる可能性は低いと推定される。よって、可用性及び、機密性に関する評価は“1”とする。	可用性:1 完全性:2 機密性:1	2

[21] 監視を行う上で必要なデータに加えて、設定情報もデータヒストリアンの資産の一部である。設定情報が改ざんされた場合、データヒストリアンが稼働停止になることが想定されるが、影響範囲がデータヒストリアンのみであればシステムダウンを誘発する可能性は低く、顧客への影響は限定されると考える。よって、完全性に関しては“2”とする。データヒストリアンの設定情報が改善され、システムダウンに陥る、もしくは顧客影響が発生することが想定できる場合は、完全性の資産価値を“3”とすることも検討する。

表 3-16 資産の重要度の検討例(2/3)

資産名	評価の説明	各尺度の評価値	重要度
データサーバ	データサーバは、データを格納している意味において、データヒストリアンと同様の機能を有している。データヒストリアンとの違いは、①HMI(操作端末)と通信する、②監視用データ以外に制御データも格納されている点である。完全性に関しては、改ざんされたデータを元に制御が行われると、重大なインシデントの発生につながり、顧客に影響を与える可能性が高いと考えられる。そのため、本書では、データサーバの完全性の評価を“3”とする。一方、データヒストリアンと同様、データサーバが破壊されるもしくは情報窃取されたとしても顧客への影響は低いと考えられるため、可用性及び、機密性に関する評価は“1”とする。	可用性:1 完全性:3 機密性:1	3
制御サーバ	制御サーバは、コマンド発行を主としているため、コマンド自体の改ざんやコマンドシーケンスを窃取されることが脅威となる。コマンド改ざんは重要なインシデントの発生を誘発しうるため、完全性に関する評価は“3”とする。データヒストリアン同様、サーバの設定情報の改ざんに関しても考慮する必要があるが、コマンド改ざんによる検討において評価が既に“3”になっているため、更なる検討は不要である。コマンドの改ざんによる検討を行った結果、評価が“2”以下になった場合は別途サーバの設定情報に関する評価を検討する。 一方、情報窃取に関しては直接的な被害は想定しにくいが、窃取した情報を元にコマンド改ざんさせる脅威は想定される。そのため、機密性に関する評価は“2”とする。また、当該装置群が破壊された場合もシステムの維持が困難になることも想定される。よって、可用性に関する評価は“3”とする。また、制御サーバが破壊もしくは情報改ざんされることにより、実際の事業に対して影響を与える可能性は高く、結果として、健康、安全性、環境に影響をあたえる可能性も高い。よって、HSE に関する評価は“3”とする。	可用性:3 完全性:3 機密性:2 HSE:3	3

表 3-17 資産の重要度の検討例(3/3)

資産名	評価の説明	各尺度の評価値	重要度
HMI(操作端末)	HMI は、コマンド発行を主としているため、制御サーバ同様、コマンド自体の改ざんやコマンドシーケンスを窃取されることが脅威となる。よって、完全性及び機密性に関する評価はそれぞれ“3”、“2”とする。また、HMI が破壊された場合、直接制御システムの稼働に影響を与える可能性は低いが、一定時間以上停止した場合は、システムが制御不能に陥る可能性がある。よって、可用性に関する評価は“2”とする。HMI が発行した誤ったコマンドによって、事業被害が引き起こされる可能性は存在するが、直接的にシステムに影響を与える可能性は低いと考える。よって、HSE に関する評価は“2”とする。	可用性:2 完全性:3 機密性:2 HSE:2	3
PLC	PLC は主に制御信号を受信し、フィールド機器に指示する装置である。そのため、PLC 自身が破壊されると、PLC が制御しているフィールド機器が制御不能に陥る可能性が非常に高い。よって、可用性に関する評価は“3”とする。一方、データは格納していないため、制御データの情報窃取、改ざんの脅威は少ないと考える。またフィールド機器へ指示するコマンドの改ざんも想定されるが、本評価において、フィールド機器は対象外としているため、その様な脅威も想定しない。以上より、完全性、機密性に関する評価は“1”とする[22]。前述の通り、PLC が破壊された場合、直接的にシステムに影響を与える可能性が高いので、PLC における HSE に関する評価は“3”とする。	可用性:3 完全性:1 機密性:1 HSE:3	3

[22] 図 3-6 において、PLC は、単独で動作する PLC と、主従関係にある PLC(マスター)と PLC(スレーブ)の 3 種類がある。仮に各 PLC において、機能的差分があり、それによって各基準(可用性、完全性、及び機密性)の資産価値が変わる場合は、PLC 各々に対して資産価値を修正する必要が生じる。

3.3. 事業被害とそのレベルの定義

本節では、事業被害ベースのリスク分析における評価指標の一つである事業被害とそのレベルの定義を行う。

制御システムを保有する事業者にとって、事業被害を明確化（定義）することは、リスク分析する上で不可欠な作業である。何故なら、事業被害のリスクを低減するための対策を抽出、選定することがリスク分析の最終目的の一つだからである。

制御システムにおける事業被害は、同じくコンピュータとソフトウェアとネットワーク等で構成されている（狭義の）情報システムとは、大きく異なった側面を持っている。制御システムは、製造ラインや供給ライン、社会インフラ、更にはそれを取り巻く環境等にも大きく関わっている。従って、事業被害を考察する場合には、情報システムでの典型的な観点である、CIA（C：機密性、I：完全性、A：可用性）という指標だけではなく、HSE（H:健康、S：安全性、E:環境への影響）という観点を考慮に入れることが必要となる 。ただ、この 2 つの観点は関連しており、因子として CIA の阻害によって、その結果として HSE への影響が生じるという因果関係にあり、両観点から、事業被害を捉えることで、より正確に事業におけるリスクを捉えることができるものと考えられる。

制御システムが担っている各事業において、これらの観点から、サイバー攻撃や人的不正操作等に起因して想定される事業被害を定義することが必要である。

以下では、これらの観点から、典型的に取り上げられる例について、述べる。

① 事業の停止、劣化（CIA 観点から）
- 製造ライン、供給ラインの停止
- 製造物、供給物の品質の低下
- サービス（供給、運行等）の停止、混乱

② 情報漏えい（CIA 観点から）
- 機密情報（製品設計データ、製造パラメータ等）の窃取、漏えい
- 顧客情報の窃取、漏えい

③ 事業継続性への影響（CIA 観点から）
- 事業の根幹となるデータ（例えば使用量数値等）の改ざん

④ 人的被害（HSE 観点から）
- 制御システムの支配下にある装置や設備の不具合や暴走等による人的損傷
- 製造物の品質劣化による健康被害

⑤ システム破壊（HSE 観点から）

- エネルギー関連装置の暴走、制御の閾値超過等による爆発
- 製造物の流出による環境汚染

⑥ 法令順守抵触事象発生

- 各業法に定められた報告事案発生
- 個人情報漏洩、環境汚染等の届出・報告必要事案の発生

3.3.1. 事業被害レベルの判断基準の定義

事業被害ベースのリスク分析では、脅威によって生じる事業上の被害を 3 段階(1～3)の事業被害レベルで評価する。事業被害レベル＝“3”は事業上の被害が大きいことを意味し、事業被害レベル＝“1”は事業上の被害が小さいことを意味する。

事業被害の観点は事業者ごとに異なるため、発生した場合の被害範囲や会社経営上の打撃を基に、各事業者にて自社の事業への影響を考慮し、事業被害レベルの判断基準を定義する。表 3-18 に、一般的な事業被害レベルの判断基準の定義例を示す。

表 3-18 事業被害レベルの判断基準の定義例

評価点	判断基準
3	事業上の被害が大きい。 【例】 ・発生した場合、被害範囲はシステム全体に及ぶ。 ・会社の経営上、致命的もしくは永続的な打撃を与える可能性がある。
2	事業上の被害が中程度。 【例】 ・発生した場合、被害範囲がシステムの一部に限定される。 ・会社の経営上、大きなもしくは長期的な打撃を与える可能性がある。
1	事業上の被害は小さい。 【例】 ・発生した場合、被害範囲はシステムの極一部に限定される。 ・会社の経営上、中程度以下もしくは一時的な打撃を与える可能性がある。

評価点の境界を定量的な値とし、判断基準を具体化する際の参考情報として、資産の重要度の判断基準(3.2.1 項)にて紹介した、IEC 62443-2-1 の Annex A.2.3.3.7(Table A.2 - Typical consequence scale)(表 3-11)も参考になる。

3.3.2. 事業被害の決定

事業被害レベルの判断基準を定義した後、事業被害及びそれを生じる攻撃シナリオ、それらに対する事業被害レベルの値を決定する。

表 3-19～表 3-20 に、事業被害の定義例を示す。表 3-19 は、事業被害と事業被害レベルの値を定義した例である。表 3-20 は、事業被害と攻撃シナリオ、事業被害レベルの値を定義した例である。ここでは事業被害を定めるに留め、事業被害を生じる攻撃シナリオの具体的な検討は、事業被害ベースのリスク分析作業（4.2 節）において実施してもよい。

表 3-19 事業被害の定義例（1）

項番	事業被害	事業被害の概要	事業被害レベル
1	広域での〇〇供給停止	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、広域において供給停止が発生し、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。	3
2	限定地域での〇〇供給停止	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、限定地域において供給停止が発生し、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。	2
3	仕様不良〇〇の供給	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、規定の仕様を満たさない〇〇を顧客に供給してしまい、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。	2
4	設備の破壊	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、設備が破壊されて供給停止が発生すると共に、従業員や近隣住民の死傷者が出て、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。	3
5	大規模対策費用の発生	サイバー攻撃を受け、〇〇の供給停止の被害は発生しなかったものの、現行対策の脆弱性が明らかとなり、その解消のために膨大な対策費用が発生する。	1

表 3-20 事業被害の定義例(2)

項番	事業被害	事業被害の概要、攻撃シナリオ		事業被害レベル
1	広域での〇〇供給停止	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、広域において供給停止が発生し、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。		3
		1-1	〇〇製造設備へのサイバー攻撃	
		1-2	〇〇供給設備へのサイバー攻撃	
		1-3	供給指令センターへのサイバー攻撃	
2	限定地域での〇〇供給停止	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、限定地域において供給停止が発生し、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。		2
		2-1	〇〇製造設備へのサイバー攻撃	
		2-2	〇〇供給設備へのサイバー攻撃	
		2-3	供給指令センターへのサイバー攻撃	
3	仕様不良〇〇の供給	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、規定の仕様を満たさない〇〇を顧客に供給してしまい、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。		2
		3-1	〇〇製造設備へのサイバー攻撃	
		3-2	〇〇供給設備へのサイバー攻撃	
		3-3	供給指令センターへのサイバー攻撃	
4	設備の破壊	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、設備が破壊されて供給停止が発生すると共に、従業員や近隣住民の死傷者が出て、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。		3
		4-1	〇〇製造設備へのサイバー攻撃	
		4-2	〇〇供給設備へのサイバー攻撃	
5	大規模対策費用の発生	サイバー攻撃を受け、〇〇の供給停止の被害は発生しなかったものの、現行対策の脆弱性が明らかとなり、その解消のために膨大な対策費用が発生する。		1
		5-1	インターネット接続点から制御系ネットワークへの侵入	
		5-2	暗号鍵の解読・漏えい	

3.4. 脅威レベルの定義

本節では、資産ベース及び事業被害ベースのリスク分析における評価指標の一つである脅威レベルの定義を行う。

本書では、「脅威」に対応する評価指標として、脅威が発生する可能性を「脅威レベル」と呼び、使用する。脅威レベルの判断基準は、各事業者にて定義する(☞ 3.4.1 項)。

脅威の意味は、リスク分析の手法によって異なる。

資産ベースのリスク分析(4.1 節)では、一次攻撃に対する脅威であり、資産に対する個々の脅威が発生する可能性を脅威レベルと呼ぶ。資産に対する脅威は、攻撃手法によって分類する(☞ 3.4.2 項)。

事業被害ベースのリスク分析(4.2 節)では、攻撃ツリーに対する脅威であり、個々の攻撃ツリーが発生する可能性を脅威レベルと呼ぶ。

3.4.1. 脅威レベルの判断基準の定義

本書では、それぞれのリスク分析手法において想定する脅威[23]が発生する可能性を「脅威レベル」と呼び、3 段階(1～3)の値で評価する。脅威レベル＝“3”は脅威が発生する可能性が高いことを意味し、脅威レベル＝“1”は脅威が発生する可能性が低いことを意味する。

表 3-21 に、一般的な脅威レベルの判断基準の定義例を示す。各事業者において、本定義を参考に自社の制御システムに対する脅威を考慮し、判断基準を定義する。

表 3-21 脅威レベルの判断基準の定義例

評価点	判断基準
3	発生する可能性が高い。 【例】 ・個人の攻撃者(スキルは問わない)によって攻撃された場合、攻撃が成功する可能性が高い。 ・近未来に発生することが予想される。
2	発生する可能性は中程度。 【例】 ・一定のスキルを持った攻撃者によって攻撃された場合、攻撃が成功する可能性がある。 ・分析対象システムのライフサイクルにおいて、発生することが想定される。
1	発生する可能性は低い。 【例】 ・国家レベルのサイバー攻撃者(軍隊及びそれに準ずる団体)によって攻撃された場合、攻撃が成功する可能性がある。 ・分析対象システムのライフサイクルにおいては、発生することが想定しがたい。

[23] 資産ベースのリスク分析手法において想定する脅威は 4.1 節で、事業被害ベースのリスク分析手法において想定する脅威は 4.2 節で、それぞれ説明する。

3.4.2. 脅威（攻撃手法）とその分類

資産ベースのリスク分析においては、各資産に対して想定される攻撃手法を脅威と見なす。

攻撃手法の視点で分類した脅威を、以下、「脅威（攻撃手法）」と示す。「脅威（攻撃手法）」は、資産の分類（機器及び通信経路）によって異なる。機器に対して想定される脅威（攻撃手法）を表 3-22 に、通信経路に対して想定される脅威（攻撃手法）を表 3-23 に示す。

表 3-22 資産(機器)に対する脅威(攻撃手法)

#	脅威(攻撃手法)	説明	具体例
1	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	● 不正入手した認証情報の悪用(不正ログイン) ● 認証機構を持たない機器への侵入 ● 機器に内在する脆弱性の悪用 ● 設定不備(不要プロセス動作や不要ポート開放等)の悪用
2	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。 あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	● 敷地内／計器室／サーバ室への不正侵入 ● ラック／設置箱の不正開放
3	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	● 不正入手した認証情報の悪用(不正ログイン) ● 認証機構を持たない機器への侵入 ● 機器に内在する脆弱性の悪用
4	過失操作	内部関係者(社員や協力者のうち、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	● メール添付ファイル開封 ● マルウェアに感染した正規媒体の持ち込み
5	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVD や USB 機器等)を接続し、攻撃を実行する。	● 不正媒体の接続 ● 媒体からの読み込み／媒体への書き出し
6	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	● プログラム／コマンドの不正実行 ● サービスの不正起動
7	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	
8	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	● 制御パラメータの窃取
9	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	● 制御プログラムの改ざん ● 制御パラメータの改ざん
10	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。	● 制御データの削除 ● 制御データの強制暗号化
11	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	● 制御コマンド／データ送信命令の不正実行 ● 送信データの改ざん
12	機能停止	機器の機能を停止する。	● 停止命令の不正実行
13	高負荷攻撃	DDoS 攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	● 機器に対する大量データ送信 ● 機器の脆弱性を悪用したサービス例外処理要求
14	窃盗	機器を窃盗する。	● 機器のネットワークからの切り離し、不正持出 ● 保守用モバイル端末の盗み出し
15	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	● リバースエンジニアリング

表 3-23 資産(通信経路)に対する脅威(攻撃手法)

#	脅威(攻撃手法)	説明	具体例
1	経路遮断	通信ケーブルを切断し、通信を遮断する。 あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	
2	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	
3	無線妨害	無線通信を妨害する。	● 妨害電波の送出
4	盗聴	ネットワーク上を流れる情報を盗聴する。	
5	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	
6	不正機器接続	ネットワーク上に不正機器を接続する。	● 無許可のモバイル PC 不正接続 ● 不正な無線中継器の設置

このページは空白です。

【コラム】

脅威のモデル化と各リスク分析手法における脅威の意味

脅威という用語は、情報セキュリティマネジメントシステムの国際標準規格（ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary）において、以下の様に定義されている。

- 脅威（threat）
  セキュリティを侵害して損害を引き起こす可能性のある事情、能力、アクションまたは事象が存在する場合に生じる、セキュリティ違反の可能性。

制御システムに対するリスク分析において脅威を検討する際、上記の概念をベースに、脅威のモデルを整理してみることも有効である。

- 脅威事象（threat event）
  セキュリティを侵害して損害を引き起こす可能性のある事象または状況。現実に脅威事象発生した場合、「インシデント（incident）」と呼ぶ。
- 脅威源／脅威エージェント（threat source / threat agent）
  脅威事象を生じる起源となる人物または物事。
  ①敵性要因（悪意を持つ攻撃者等）、②偶発性要因（内部要員の過失等）、③構造的要因（ソフトウェア障害等）、④環境的要因（自然災害等）に分類される。①及び②に属する起源（人的起源）の場合、「攻撃者（threat actor）」と呼ぶことがある。
- 脅威ベクタ／攻撃ベクタ（threat vector / attack vector）
  脅威事象において、攻撃に悪用される弱点（脅威のモデル化においては「脆弱性（vulnerability）」と表現されることが多い）に至る攻撃経路。
- 脅威対象／対象（threat target / target）
  脅威事象において、影響を受ける対象（人物や資産等）。即ち、攻撃対象。
- 発生可能性（likelihood）
  脅威事象が発生し、脅威対象に対する影響が生じる可能性。
- その他の要素
  脅威事象を詳細にモデル化するため、「攻撃手法（attack type）」「攻撃目的（attack objective）」「想定結果（potential consequence）」の観点で分類することもある。

本書での資産ベースのリスク分析における「脅威」は、特に「脅威対象」ごとの「攻撃手法」に注目して分析・評価するものである。事業被害ベースのリスク分析における「脅威」は、「脅威事象」全体を分析・評価するものである。いずれの分析方法においても、「脅威レベル」は、「発生可能性」に対応する。

3.5. セキュリティ対策項目の確認

本節では、資産ベース及び事業被害ベースのリスク分析における評価指標の一つである脆弱性とその値について説明し、脆弱性を求めるためにセキュリティ対策状況を明確化する必要性があることを示す。

3.5.1. セキュリティ対策状況と脆弱性の関係

本書では、それぞれのリスク分析手法において、脆弱性（発生した脅威を受け入れる可能性）を、3 段階（1～3）の「脆弱性レベル」で評価する。脆弱性レベル＝“3”は脅威を受け入れる可能性が高いことを意味し、脆弱性レベル＝“1”は脅威を受け入れる可能性が低いことを意味する。

脆弱性レベルの算定に当たっては、各脅威に対するセキュリティ対策状況を、3 段階（1～3）の「対策レベル」で評価して利用する。対策レベル＝“3”は脅威に対するセキュリティ対策が高いことを意味し、対策レベル＝“1”は脅威に対するセキュリティ対策が低いことを意味する。

脆弱性レベルと対策レベルの定義（評価点と判断基準）を、表 3-24 に示す。

表 3-24 脆弱性レベルと対策レベルの定義（評価点と判断基準）

評価点		判断基準
脆弱性レベル	対策レベル	
3	1	脅威が発生した場合、容易に受けいれる可能性が高い。 脅威の対策が実施されておらず、攻撃が成功する可能性が高い。 【例】 ・過去の事例において、脆弱性を利用した攻撃が発生・成功し、被害が生じたことが確認されている。
2	2	脅威が発生した場合、受け入れる可能性が中程度である。 脅威の対策が実施されているが、十分とは言えないため、攻撃が成功する可能性は中程度である。 【例】 ・一般的な対策を実施しており、攻撃が成功するか否かは攻撃者のレベルに依る。 ・過去の事例において、脆弱性を利用した攻撃が発生したが、大きな被害に至らなかったことが確認されている。
1	3	脅威が発生した場合、受け入れる可能性は低い。 脅威の対策が十分実施されている。 【例】 ・効果的な対策や、多層的な対策を実施しており、攻撃が成功する可能性は低い。 ・過去の事例において、脆弱性を利用した攻撃は発生していない。

3.5.2. セキュリティ対策とその分類の確認

前項で示した通り、リスク分析の評価指標「脆弱性」の評価値を求めることは、脅威に対するセキュリティ対策状況の評価値を求めることに等しい。資産ベースのリスク分析では、システムを構成する個々の資産において、想定される各脅威に対応するセキュリティ対策状況で評価する。事業被害ベースのリスク分析では、事業被害につながる個々の攻撃ツリーにおいて、攻撃ツリーを構成する攻撃ステップ内の資産に対する脅威とセキュリティ対策状況の組合せから、総合的に評価する。

従って、4 章で説明する 2 種類のリスク分析の準備作業として、セキュリティ対策とその分類を確認・理解しておく必要がある。

本書では、制御システムにおいて実施し得るセキュリティ対策の一覧を用意している[24]。

最初に、対策の用途・目的を「防御（初期潜入段階、内部侵攻・拡散段階、目的遂行段階）」「検知」「被害把握」「事業継続」に分類しており、これらの定義を表 3-25 に示す。

各々のセキュリティ対策の定義を、表 3-26～表 3-29 に示す。一部の対策については、利用している機能の範囲や実現方式、運用方針等によって、セキュリティ対策としての有効性や有効範囲が異なり、対策状況の評価値が異なってくる可能性がある。この様な対策については、選択肢（チェックボックスや任意記入欄）を設けて、これらの相違点を区別可能となっている。

3.4.2 項（表 3-22 及び表 3-23）で示した各々の脅威（攻撃手法）に対して、有効と考えられる技術的対策／物理的対策の候補一覧との関係を、表 3-30～表 3-32 に示す。

[24] セキュリティ対策は、様々な名称や定義が与えられているので、評価や事業者間の議論において整合性を取るために、本書では対策の一覧表を用意し、基本的にそこから選択することを推奨している。

表 3-25 セキュリティ対策の用途・目的

用途・目的		説明	対策例
防御	初期侵入段階	攻撃の最上流（初期段階）における、外部との接続点を介したネットワーク経由の攻撃、あるいはシステム（サーバ・操作端末・機器等）設置場所への攻撃者の物理的侵入を防止する目的で実装される対策。 また、攻撃者（内部犯行者を含む）による、システム（サーバ・操作端末・機器等）への不正ログイン等を防止する目的で実装される対策。	ファイアウォール（FW）、IPS、 アンチウイルス、 パッチ適用、脆弱性回避、 通信相手の認証、操作者認証、 入退管理
	内部侵攻・拡散段階	システム（サーバ・操作端末・機器等）への侵入を果たした攻撃者（人間あるいは不正プログラム）による、内部の情報収集や侵入範囲拡大（侵入したシステム内部での拡大及び他のシステムへの拡散）を防止する目的で実装される対策。	セグメント分割／ゾーニング、 APT 対策ツール、 アクセス制御、 ホワイトリストによるプロセスの起動制限
	目的遂行段階	「情報窃取」「データ改ざん」「制御乗っ取り」「システム破壊」等、攻撃者による最終目的の実現を防止する目的で実装される対策。	重要操作の承認、 データ暗号化、データ署名、 フェールセーフ設計
検知		攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策。	IDS、 アンチウイルス、APT 対策ツール、 統合ログ管理システム、 機器異常検知、機器死活監視、 入退管理、侵入センサ
被害把握		攻撃の成功による被害や影響範囲の把握を目的に実装される対策。あるいは、監査における証跡提示のため、攻撃内容の詳細の把握等を目的に実装される対策。	ログ収集・分析、 統合ログ管理システム
事業継続		攻撃の成功による被害を最小限に留めるために実装される対策。あるいは、サービスの継続、被害の早期復旧を実現することを目的に実装される対策。	データバックアップ、冗長化、 暗号鍵更新、 フェールセーフ設計

このページは空白です。

表 3-26 セキュリティ対策項目一覧(1/4)

#		セキュリティ対策 ○:主対象 △:利用可	用途・目的				定義
			防御		検知／被害把握	事業継続	
			初期侵入段階／内部侵攻・拡散段階	目的遂行段階			
	技術的対策						
1		FW(パケットフィルタリング型)	○	△	△		不正通信を遮断するために、送信元及び宛先の IP アドレス(ネットワーク層)・ポート番号(トランスポート層)を確認して、通信を制限する、ファイアウォールの一分類。単に**「ファイアウォール」**と呼ばれることが多いが、他のファイアウォールと区別する際は、**「パケットフィルタリング型ファイアウォール」**等と呼ぶ。
2		FW(アプリケーションゲートウェイ型)	○	△	△		アプリケーションを狙った攻撃を検知・防御するために、プロキシサーバの機能を内包し、アプリケーション層のプロトコルデータ(通信の中身)を確認して通信を制限する、ファイアウォールの一分類。正式には、**「アプリケーションゲートウェイ型ファイアウォール」**等と呼ぶ。なお、Web アプリケーションに特化したアプリケーションゲートウェイは、**「WAF」**(**項番 12** 参照)に分類する。
3		一方向ゲートウェイ	○	△			不正通信を遮断するために、ハードウェアレベルで一方向の通信しかできない様に工夫された、特殊なファイアウォール。代表例として、ダイオード素子を活用した一方向ゲートウェイである**「データダイオード」**等がある。
4		プロキシサーバ	○	△	△		外部の攻撃者に対して内部のネットワーク情報(IP アドレスやネットワーク構成等)を隠蔽して攻撃への悪用を困難とするために、内部ネットワークと外部ネットワークの境界点に設置して、クライアント・サーバ間の通信を一旦終端した後、通信内容を中継する。ウェブサイトへのアクセスを中継する**「HTTP プロキシ」**、電子メールを中継する**「SMTP プロキシ」**等がある。**「サーキットレベルゲートウェイ型ファイアウォール」**と分類されることもある。なお、通常のプロキシサーバの機能に加えて、中継する際にアプリケーション層のデータを確認して通信制限する機能を有するプロキシサーバは、**「FW(アプリケーションゲートウェイ型)」**(**項番 2** 参照)または**「WAF」**(**項番 12** 参照)に分類する。また、ウェブサイトとの通信を許可／遮断する機能を有するプロキシサーバは**「URL フィルタリング／Web レピュテーション」**(**項番 5** 参照)に分類する。
5		IPS/IDS □IDS(検知)機能のみ □IPS(遮断)機能併用	○		○		不正アクセスを検知・抑止するために、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う(**「ネットワーク型 IPS/IDS」**)。また、監視対象上の入出力データや内部の変化を監視し、不正な通信の検知及び遮断を行う(**「ホスト型 IPS/IDS」**)。不正通信の検知のみ行う(**IDS 機能のみ使用**する)場合と、検知した不正通信を遮断する(**IPS/IDS 機能を併用**する)場合がある。
6		DDoS 対策		○		○	DDoS(Distributed Denial of Service)攻撃による被害を最小化するために、DDoS 対策機器の導入や DDoS 対策サービスの利用によって、高負荷攻撃への耐性を向上する。負荷分散装置(**「ロードバランサ」**)による耐性向上を含む。
7		通信相手の認証	○		△		通信相手へのなりすましによる被害を防止するために、通信相手が本物であるか否か、正当性を確認する。通信を確立する過程で、通信プロトコルの一部(ハンドシェーク処理等)として認証する場合と、通信確立後のアプリケーションにて認証する場合がある。
8		専用線	○				通信路上の盗聴・改ざんによる被害を最小化するために、電気通信事業者が提供する特定の顧客専用に設置された回線を利用する。電気通信事業者が信用できない場合は、「通信路暗号化」と併用することが望ましい。
9		通信路暗号化	○				通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化し、仮に通信路上のデータ漏えいが発生しても、「無価値化する(攻撃者にとって無意味なものとする)」。電子署名や MAC(メッセージ認証コード)、認証機能付き暗号化等の暗号技術を用いて、通信路上でのデータの改ざんを検知可能とする場合を含む。
10		アンチウイルス □パターンマッチング方式 □ヒューリスティック方式	○		○		ウイルス感染を防止するために、ウイルスを検知・除去する。ウイルス検知方式としては、ウイルスの特徴を記録した「パターンファイル」「定義ファイル」「シグネチャ」と比較してウイルスを検出する**「パターンマッチング方式」**の他、検査対象を自動解析して不審な動作を行うコードが含まれていることを検出する**「ヒューリスティック方式」**が存在する。 また、設置場所としては、保護対象である計算機(PC やサーバ)上にインストールする**「エンドポイント型」**と、ウイルス感染経路となるネットワーク上に設置する**「ゲートウェイ型」**がある。後者は、ウェブサイトとの通信やメールの送受信データを監視し、いずれか一方のみに対応するもの、両方に対応するものが存在する。
11		WAF	○	△	△		Web アプリケーションを狙った攻撃を検知・防御するために、ウェブサーバの前段に設置し、ウェブサイトの脆弱性を突いた攻撃から防御する。正式名称は、**「Web アプリケーションファイアウォール」**。分類上は、**「アプリケーションゲートウェイ型ファイアウォール」**の一種。

表 3-27 セキュリティ対策項目一覧(2/4)

#		セキュリティ対策 ○:主対象 △:利用可	用途・目的				定義
			防御		検知／被害把握	事業継続	
			初期侵入段階／内部侵攻・拡散段階	目的遂行段階			
	技術的対策						
12		URL フィルタリング／Web レビュテーション □URL フィルタリング □Web レピュテーション	○	△			不正サイトとの通信を遮断してウイルス感染等の被害を防止するために、ウェブサイトとの通信を遮断する。ウェブサイトのコンテンツに基づいたブラックリストまたはホワイトリストを用いて、ウェブサイトとの通信を許可／遮断するものを**「URL フィルタリング」**と呼ぶ。また、ウェブサイトの信頼度／危険度を複数の評価基準に基づいて評価し、通信を許可／遮断するものを**「Web レピュテーション」**と呼ぶ。
13		メールフィルタリング	○				スパム(迷惑メール)や不審な電子メールの受信を排除するために、メールの送信者・送信サーバ・件名等のヘッダ情報、メール本文・添付ファイルの種類等を確認し、不審なメールの選別・注意喚起の挿入・排除(配信拒否)を行う。特に、スパムの排除に特化したものを**「スパムフィルタ」「アンチスパムフィルタ」**等と呼ぶことがある。また、不審なメールの判定に際して、メール送信サーバ等の信頼度／危険度を複数の評価基準に基づいて評価し、配信を許可／遮断するものを**「メールレピュテーション」**と呼ぶことがある。
14		APT 対策ツール □サンドボックス機能 □内部通信監視機能 □その他(　　)	○	○	○		未知のウイルスや未知の脆弱性を突いた攻撃等、高度な手法を用いた APT を防御するために、APT に対応する対策ツールを導入する。保護された領域で不審なプログラムを実装に動作させて確認する**「サンドボックス機能」**や、システム内部の通信を監視して不審な動作・通信を検出・遮断する**「内部通信監視機能」**等がある。
15		パッチ適用 □随時適用 □定期適用(頻度:　　)	○	○			脆弱性を悪用した攻撃を防止するために、パッチを可能な限り速やかに適用し、脆弱性を解消する。
16		脆弱性回避 □仮想パッチ □その他(　　)	○	○			脆弱性を悪用した攻撃を防止するために、「パッチ適用」以外の手段を用いて、脆弱性を突いた攻撃を回避する。例えば、システムを一時停止できない／動作確認していないのでパッチを適用できない、サポート期間を終了した製品のためパッチが提供されない等の状況が想定される。これに対して、例えば、攻撃経路上に設置したネットワーク機器(IPS/IDS 等)において、脆弱性を突いた攻撃を検知・遮断する(**「仮想パッチ」**)。あるいは、脆弱性につながる一部機能を停止して運用を継続し、攻撃を受けない様にする等の方法が考えられる。
17		セグメント分割／ゾーニング	○	△			外部ネットワークから内部ネットワークへの侵入や内部ネットワークにおける侵攻拡散を防止するために、ネットワークを複数のセグメントに分割して運用する。正式には、**「ネットワークのセグメント分割(network segmentation)」「ネットワーク・ゾーニング(network zoning)」「ネットワーク・セキュリティ・ゾーニング(network security zoning)」**等と言う。この時、特に、外部ネットワークと内部ネットワークとの間に、公開サーバ等を設置するために設けたセグメントを**「DMZ(非武装地帯)」**と呼ぶ。また、外部に接続されたネットワークと重要情報等を扱う内部専用ネットワークを完全に分割することを、**「ネットワーク分離」「インターネットからの分離」**等と呼ぶ。
18		操作者認証 □ID／PW □多要素認証(　　)	○	△	△		操作者へのなりすましによる脅威を防止するために、操作者が本物であるか否か、正当性を確認する。特に、認証に成功した操作者に重要な権限(例:システム全体の停止)が与えられる場合、複数の認証要素を組み合わせた多要素認証技術を採用することが望ましい。
19		デバイス接続・利用制限	○	○	△		外部から持ち込まれたウイルスによる感染や機密情報の外部への持ち出しを防止するために、許可されていないデバイス(PC・タブレット端末・スマートフォン・USB 機器・Blu-ray/DVD/CD の媒体等)の接続・利用(機器への接続、ネットワークへの接続、データの読み書き等)を禁止する。例えば、登録されていない機器のネットワーク接続を禁止する**「MAC アドレス認証」**、USB ポートへの機器接続を物理的または論理的に禁止する**「USB ポートロック」**、光学ドライブの書き込み機能をレジストリ設定で禁止する等の方法が考えらえる。
20		重要操作の承認	△	○	△		攻撃者によって虚偽の重要操作(例:システム全体の停止)が実行されることを防止するために、重要操作を実行する際に、特別な承認フロー(ワークフローによる申請、複数承認者による承認、書面を用いた指示等)を実行する。
21		プロセス監視			○		攻撃者による重要プロセスの停止攻撃を検知するために、プロセスの稼働状況を監視する。
22		ホワイトリストによるプロセスの起動制限	○		△		ウイルス感染を防止するために、起動を許可するプロセスを記載したホワイトリストを作成し、リストに掲載されていないプロセスの起動を禁止する。

表 3-28 セキュリティ対策項目一覧(3/4)

#		セキュリティ対策 ○:主対象 △:利用可	用途・目的				定義
			防御		検知／被害把握	事業継続	
			初期侵入段階／内部侵攻・拡散段階	目的遂行段階			
	技術的対策						
23		権限管理	○	○	△		不正行為、主に不正アクセス(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、ユーザの権限及び関連する属性を適切に管理する。ここでは、権限管理に従って、ユーザに権限(例:アクセス権)を与える**「認可」**を含むこととする。最低限必要なユーザに対して、必要最小限の権限を与えることが望ましい。 【注】「ユーザ」=「アカウント管理」及び「認証」によって操作者と対応付けられた、システム内における論理的存在。
24		アクセス制御	○	○	△		不正アクセス(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、権限管理の中で実施した認可に基づいて、アクセス(読み／書き／実行)の許可または拒否を行う。
25		データ暗号化	△	○			データ漏えいによる被害を最小化するために、暗号技術を用いてデータを暗号化し、仮に蓄積時または通信時のデータが漏えいしたとしても、無価値化する(攻撃者にとって無意味なものとする)。
26		データ署名	△	○			データ改ざんによる被害を最小化するために、電子署名や MAC(メッセージ認証コード)、認証機能付き暗号化等の暗号技術を用いて、データの改ざんを検知する。ウイルス感染したソフトウェアや不正改造されたソフトウェア(ファームウェアを含む)の動作を防止するため、署名されたソフトウェアの動作のみ許可する**「ソフトウェア署名」「コード署名」**を含む。
27		DLP(情報漏えい防止ツール)	△	○			機密情報の漏えいを防止するために、保護対象の機密情報を機密データとして登録し、システム内部での機密データの移動、一部データの切り出し、ネットワーク経由あるいはデバイス経由での外部への持ち出しを監視し、必要に応じて遮断措置を取る。
28		耐タンパー	○	○			内部構造や記憶しているデータの解析や改変を困難とするために、ハードウェア技術を用いて、タンパー耐性を強化する。具体的には、内部処理の違いによる消費電流／処理時間変動が発生しない様な回路構成にする、筐体開封を検知すると回路が破損する／内部情報の自動消去を行う等、様々な方法が考えられる。一般に、「耐タンパー」性はハードウェアとソフトウェアの両方に適用する性質であるが、本項目はハードウェア技術を用いた場合に限定する。
29		難読化	○	○			内部構造や記憶しているデータの解析や改変を困難とするために、プログラムやデータ構造の難読化等を行う。**「ソフトウェア技術を用いた耐タンパー対策**(の一方式)**」**と呼ぶこともある。
30		セキュア消去	○	○			過去に記憶していたデータの解析を困難とするために、復元不可能な状態で消去すること。英語の"zeroization/zeroisation"に相当する。ハードディスクに対するセキュア消去操作を、**「ホワイトニング」**と呼ぶこともある。
31		データバックアップ □定期実施(頻度:) □ライトワンス	○	△		○	データの物理的破壊や論理的破壊による被害からの回復のために、データのバックアップ(コピー)を作成する。バックアップデータに対する破壊攻撃を防止するため、一回のみ書き込み可能なデバイスへバックアップを実施する、**「ライトワンス・バックアップ」**を含む。
32		冗長化		△		○	システムに対する攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。
33		機器死活監視			○		システムを構成する各機器に対する攻撃(不正アクセスやマルウェア感染等)の予兆を早期検知するために、あるいは事後調査(被害状況把握)に利用するために、各機器の正常稼働状況を監視する。
34		機器異常検知			○		システムを構成する各機器に対する攻撃(不正アクセスやマルウェア感染等)の予兆を早期検知するために、あるいは事後調査(被害状況把握)に利用するために、各機器の正常稼働状況を監視する。
35		ログ収集・分析 □収集のみ □収集＋異常検知時分析 □収集＋定期分析(頻度:)			○		システムへの攻撃を早期検知するために、あるいは事後調査(被害状況把握)に利用するために、ログを収集する。加えて、収集したログを定期的に、あるいは異常検知時に分析する。 【注】ログの種類を特定可能な場合は、枝番で示した各々の対策ごとに分類してもよい。
-1		認証ログ収集・分析			○		認証に関するログ(成功・失敗、連続して失敗した回数等)の収集・分析を行う。
-2		通信ログ収集・分析			○		ネットワーク機器(ファイアウォール、プロキシサーバ、ネットワークスイッチ等)のログの収集・分析を行う。
-3		操作ログ収集・分析			○		操作者による操作に関するログの収集・分析を行う。
-4		アクセスログ収集・分析			○		重要情報や重要リソースに対するアクセスに関するログの収集・分析を行う。

表 3-29 セキュリティ対策項目一覧(4/4)

#		セキュリティ対策 ○:主対象 △:利用可	用途・目的				定義
			防御		検知／被害把握	事業継続	
			初期侵入段階／内部侵攻・拡散段階	目的遂行段階			
	技術的対策						
36		パケットキャプチャ			○		システムに対する攻撃を早期検知するために、あるいは事後調査(被害状況把握)に利用するために、ネットワーク上を流れる通信パケットを採取・解析する。特に、全てのパケットを採取する機能を有する場合を、**「フルパケットキャプチャ」**と呼ぶ。
37		統合ログ管理システム			○	△	システムに対する攻撃を早期検知するために、あるいは事後調査(被害状況把握)に利用するために、システムの各種ログ(通信ログ、認証ログ、アクセスログ、オペレーションログ、エラーログ等)、機器設定、ステータス情報等を一元的に集め、相関的な分析を行うことで、単一のログだけでは分からなかった脅威や攻撃の兆候、異常を検出する機能を有するシステム。**「SIEM(Security Information and Event Management)」**はその一例である。
38		設備警報(プロセスアラーム)			○		システムに対する攻撃を早期検知するために、アラームを設置して、運転状態の変化をオペレータに通知する。
39		おとりサーバ	○	○	○		ネットワーク上に脆弱性を有するサーバを故意に設置し、攻撃者の情報を収集する。実際にシステムへの侵入を許可する**「ハニーポット」**と、侵入までは許可しない**「デコイサーバ」**に分類される。
	物理的対策						
40		入退管理 □暗証番号(PIN) □IC カード □生体情報	○		○		物理的なアクセスによる攻撃(不正操作、破壊、窃取等)を防止するために、重要な設備、装置、システム、機器、情報等がある敷地、建屋、区画、部屋等への入(退)室を認証し、記録する。入退ゾーンの重要度に応じ、ID カード、生体認証等を使い分けたり、組み合わせたりする。
41		監視カメラ	△		○		物理的なアクセスによる攻撃(不正操作、破壊、窃取等)を抑止するために、あるいは事後調査(発生状況把握)に利用するために、重要な設備、装置、システム、機器、情報等がある敷地、建屋、区画、部屋への出入や、通路、部屋内の状況を録画・監視する。
42		侵入センサ	△		○		(主に無人状態や少人数状態における)物理的なアクセスによる攻撃(不正操作、破壊、窃取等)を早期検知するために、重要な設備、装置、システム、機器、情報等がある敷地、建屋、区画、部屋への出入口(窓を含む)からの侵入を検知する。
43		施錠管理	○		○		物理的なアクセスによる攻撃(不正操作、破壊、窃取等)を防止するために、重要な設備、装置、システム、機器、情報等は施錠可能な建屋、ラック、収納盤、キャビネット等に収納し、鍵の持ち出しを管理する。また、必要に応じて、予定にない開閉等の異常を検知する。例えば、フィールド上に設置された、通常運用中は開閉操作が行われるはずのない機器に対する「開封検知」機構を有し、異常発生時に直ちに係員が急行できる様にする。
44		フェールセーフ設計		○		○	安全(または供給継続)を確保するため、不正操作、誤操作、誤動作、異常発生時に設備、装置、システム、機器等を安全な(または供給継続の)方向に導く。
	運用面での対策						
45		暗号鍵更新 □鍵漏えい時更新 □一定期間ごとに更新(頻度:) □一定利用ごとに更新(頻度:)	○	○		○	暗号鍵の推測による漏えいを防止するために、利用開始後、一定の期間を経過した暗号鍵や一定の回数使用した暗号鍵を更新する。暗号鍵の漏えいが発覚した場合、漏えいした暗号鍵の不正利用を防止するため、速やかに暗号鍵を更新する。
46		アカウント管理	○		○		重要な設備、装置、システム、機器、情報等へのアクセスや重要な操作を制限し、行ったユーザの特定を可能にするため、ユーザアカウントを適切に管理する。例えば、ID/PW の共用や管理用の共通特権アカウントの禁止、移動や離職時のタイムリーなアカウント変更／削除、適切なパスワードの運用(強度、アカウントロックの実施等)／保管を行う。
47		モバイル機器・媒体管理	○		○		システムで使用するモバイル機器(ノート PC・タブレット端末・スマートフォン・ハンディ端末等)や媒体(USB メモリ・Blu-ray/DVD/CD 等)の攻撃者(内部攻撃者を含む)による不正利用を防止するために、機器の持ち込み・持ち出し・持ち帰り、利用状況等を厳重に管理する。

表 3-30 脅威（攻撃手法）と技術的対策／物理的対策の候補一覧（1/3）

#	資産（機器）に対する脅威（攻撃手法）	技術的／物理的対策候補			
		防御		検知／被害把握	事業継続
		初期侵入段階／内部侵攻・拡散段階	目的遂行段階		
1	不正アクセス	・FW（パケットフィルタリング型） [1] ・FW（アプリケーションゲートウェイ型） [2] ・一方向ゲートウェイ [3] ・プロキシサーバ [4] ・WAF [11] ・通信相手の認証 [7] ・IPS／IDS [5] ・パッチ適用 [15] ・脆弱性回避 [16]		・IPS/IDS [5] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	
2	物理的侵入	・入退管理 [40] ・施錠管理 [43]		・監視カメラ [41] ・侵入センサ [42]	
3	不正操作	・操作者認証 [18]			
4	過失操作	・URL フィルタリング／Web レピュテーション [12] ・メールフィルタリング [13]			
5	不正媒体接続	・デバイス接続・利用制限 [19]	・デバイス接続・利用制限 [19]	・デバイス接続・利用制限 [19] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	
6	プロセス不正実行	・権限管理 [23] ・アクセス制御 [24] ・重要操作の承認 [20]	・権限管理 [23] ・アクセス制御 [24] ・重要操作の承認 [20]	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	
7	マルウェア感染	・アンチウイルス [10] ・ホワイトリストによるプロセスの起動制限 [22] ・パッチ適用 [15] ・脆弱性回避 [16] ・データ署名 [26]		・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	
8	情報窃取	・権限管理 [23] ・アクセス制御 [24] ・データ暗号化 [25] ・DLP [27]	・権限管理 [23] ・アクセス制御 [24] ・データ暗号化 [25] ・DLP [27]	・ログ収集・分析 [35] ・統合ログ管理システム [37]	
9	情報改ざん	・権限管理 [23] ・アクセス制御 [24] ・データ署名 [26]	・権限管理 [23] ・アクセス制御 [24] ・データ署名 [26]	・機器異常検知 [34] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	・データバックアップ [31]
10	情報破壊		・権限管理 [23] ・アクセス制御 [24]	・機器異常検知 [34] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	・データバックアップ [31]
11	不正送信	・セグメント分割／ゾーニング [17] ・データ署名 [26] ・重要操作の承認 [20]	・セグメント分割／ゾーニング [17] ・データ署名 [26] ・重要操作の承認 [20]	・ログ収集・分析 [35] ・統合ログ管理システム [37]	
12	機能停止			・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	・冗長化 [32] ・フェールセーフ設計 [44]

対策候補におけるカッコ内の番号は、セキュリティ対策項目の一覧表（表 3-26～表 3-29）における項目番号を表す。

表 3-31 脅威（攻撃手法）と技術的対策／物理的対策の候補一覧（2/3）

#	資産（機器）に対する脅威（攻撃手法）	技術的／物理的対策候補			
		防御		検知／被害把握	事業継続
		初期侵入段階／内部侵攻・拡散段階	目的遂行段階		
13	高負荷攻撃		・DDoS 対策 [6]	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	・冗長化 [32] ・フェールセーフ設計 [44]
14	窃盗・略奪	・施錠管理 [43]	・施錠管理 [43]	・施錠管理 [43]	
15	盗難・廃棄時の分解による情報窃取	・耐タンパー [28] ・難読化 [29] ・セキュア消去 [30]	・耐タンパー [28] ・難読化 [29] ・セキュア消去 [30]		

対策候補におけるカッコ内の番号は、セキュリティ対策項目の一覧表（表 3-26～表 3-29）における項目番号を表す。

表 3-32 脅威（攻撃手法）と技術的対策／物理的対策の候補一覧（3/3）

#	資産（通信経路）に対する脅威（攻撃手法）	技術的／物理的対策候補			
		防御		検知／被害把握	事業継続
		初期侵入段階／内部侵攻・拡散段階	目的遂行段階		
1	経路遮断	・入退管理 [40] ・施錠管理 [43]		・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37] ・監視カメラ [41] ・侵入センサ [42]	・冗長化 [32]
2	通信輻輳	・FW（パケットフィルタリング型） [1] ・FW（アプリケーションゲートウェイ型） [2] ・WAF [11] ・IPS／IDS [5] ・DDoS 対策 [6]		・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	・冗長化 [32]
3	無線妨害			・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	・冗長化 [32]
4	盗聴	・通信路暗号化 [9] ・データ暗号化 [25] ・専用線 [8]			
5	通信データ改ざん	・通信路暗号化 [9] ・データ署名 [26] ・専用線 [8]		・ログ収集・分析 [35] ・統合ログ管理システム [37]	
6	不正機器接続	・デバイス接続・利用制限 [19]		・デバイス接続・利用制限 [19] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	

対策候補におけるカッコ内の番号は、セキュリティ対策項目の一覧表（表 3-26～表 3-29）における項目番号を表す。

4. リスク分析の実施

本章では、2 通りの詳細リスク分析手法の具体的な実施手順について詳細に解説する。

- 資産ベースのリスク分析（4.1 節）
- 事業被害ベースのリスク分析（4.2 節）

それぞれのリスク分析は、資産ベースのリスク分析シート、及び事業被害ベースのリスク分析シートを完成させることで実施する。それぞれのリスク分析シートの作成方法を、3 章の図 3-6 にて説明した“典型的な制御システムの構成図”の制御システムを評価対象システム（以下、「モデルシステム」と呼ぶ）として、具体的な手順を説明していく。なお、3 章で述べたこのモデルシステムの各構成機器の機能や環境の条件を前提として作成を進める。

詳細リスク分析の最大の課題は、分析工数の膨大化である。そのため、敬遠される傾向にあるが、分析工数の膨大化を如何に抑えつつ、効果的なリスク分析を実施できるかが、重要な鍵となる。

資産ベースのリスク分析では、資産を構成する要素（システム、機器、ネットワーク等）の数に工数が大きく依存するので、個々の要素をリスク分析の視点で如何に統合（グループ化）するかが重要となる。その考え方を入れつつ、リスク分析を進める手法を解説する。

事業被害ベースのリスク分析では、資産に対して事業被害を生じさせる攻撃シナリオ及びそれを構成する攻撃ツリー（ルート）の数に工数が大きく依存する。重大な事業被害を起こさせる攻撃シナリオや攻撃ツリーに絞り込んで分析するための考え方を織り交ぜながら、リスク分析を進める手法を解説する。

以下の各節を読む上で、このモデルシステムのシステム構成図（図 3-6）を別紙として脇において、確認やイメージを持ちながら読み進めることをお奨めする。また、各項では、モデルシステムに対して分析シートの各欄を具体的に埋めていく手順を説明するが、本書は手順や考え方を理解することが目的であるので、リスク分析シートの完成版については分量が多くなるため掲載していない。このモデルシステムに対する実際のリスク分析結果例に関しては、**別冊「制御システムに対するリスク分析の実施例」**として、IPA のホームページに掲載しているので合わせて参照頂きたい。

4.1. 資産ベースのリスク分析

本節では、資産ベースのリスク分析の手順を解説する。

資産ベースのリスク分析は、対象とするシステムを構成する資産（例えば、サーバやネットワーク装置等）に対して、想定される直接の脅威と、それに対する対策状況を把握し、対策の十分性を評価し、資産に対するリスク分析を行うことを目的としている。

資産ベースのリスク分析は、以下の手順にて行う。

① 制御システムを構成する装置及び各装置を接続しているネットワーク等のシステム資産、情報資産[25]の列挙とその重要度の決定 （☞ 4.1.1 項）
② 当該資産に想定される脅威（攻撃手法）とそれぞれの脅威（攻撃手法）の対策候補の記入 （☞ 4.1.2 項）
③ 実際実施している対策状況の記入 （☞ 4.1.3 項）
④ 対策レベル及び脆弱性レベルの評価 （☞ 4.1.4 項）
⑤ 脅威、脆弱性、重要度よりリスク値の算定 （☞ 4.1.5 項）

以下では、3 章で述べたモデルシステム（図 3-6）を評価対象システムとし、3.2 節で述べたシステム資産を対象に具体的な手順を説明する。

図 4-1 に、リスク分析を実施するために作成する、資産ベースのリスク分析シートのフォーマットを示す。この時点では、項番及び横軸の項目名のみが記載されている。

図 4-2 に、フォーマットに必要事項を記入して作成した、資産ベースのリスク分析シートの完成例を示す。

本節において、フォーマットから資産ベースのリスク分析シートを作成する手順を説明する。シート中の各項目の記入方法については、図 4-1 の上段に示している各項番号（4.1.1 項～4.1.5 項）において説明する。資産ベースのリスク分析シートは、対象とするシステムを構成する資産ごとに作成する[26]。資産ベースのリスク分析シートに記載される項目の説明を表 4-1 及び表 4-2 に示す。

[25] 製造データ等の事業者にとって重要な情報を保有するシステム資産の場合、それらの情報も情報資産として考慮することが望ましい。
[26] シートは独立した紙である必要はなく、記載量によっては複数の資産が一枚の紙に記載されても構わない。

資産ベースのリスク分析シート

凡例:〇 対策実施　　× 対策未実施

4.1.1項　4.1.5項　4.1.2項　4.1.4項　4.1.3項

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策				対策レベル
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			防御		検知/被害把握	事業継続	脅威毎
									侵入/拡散段階	目的遂行段階			
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													

図 4-1　資産ベースのリスク分析シート(フォーマット)

資産ベースのリスク分析シート

凡例: ○ 対策実施　　× 対策未実施　　グレーアウト行：該当資産で考慮しない脅威

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策						対策レベル
									防御				検知/被害把握		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階			事業継続	脅威毎
1	情報系資産	**データサーバ**	2	2		B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 ○ IPS／IDS パッチ適用 脆弱性回避				IPS／IDS ログ収集・分析 統合ログ管理システム		2
2			2	1		C	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。 あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理 (ICカード、生体認証) ○ 施錠管理 ○				監視カメラ ○ 侵入センサ ○		3
3			2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass) ○						2
4			2	3		A	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング						1
5			2	3		A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		1
6			2	2		B	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 ○ アクセス制御 ホワイトリストによるプロセスの起動制限 ○ 重要操作の承認		(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
7			1	2		C	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 ○ パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
8			3	2		A	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 ○ アクセス制御 データ暗号化 DLP		(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム		2
9			3	3		A	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名		(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ ○	1
10			3	3		A	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 ○ アクセス制御		機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ ○	1
11			3	3	3	A	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム		1
12			2	3		A	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計	1
13			3	3		A	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計	1
14			2	2		B	窃盗	機器を窃盗する。	施錠管理 ○		(同左)		施錠管理 ○		2
15			3	3		A	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去		(同左) (同左) (同左)				1
16			3	2		A	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 (ICカード、生体認証) ○ 施錠管理 ○				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ ○ 侵入センサ ○	冗長化	2
17			1	3		B	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化	1
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化	
19			2	3		A	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線						1
20			2	3		A	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム		1
21			3	3		A	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		1

図 4-2　資産ベースのリスク分析シート(完成例)

表 4-1 資産ベースのリスク分析シートにおける各項目の説明(1/2)

項目名		説明
項番		評価対象の各資産に対する攻撃手法の通し番号。 項番は、後述する脅威(攻撃手法)ごとに付与する。
資産種別		対象となる資産の機能や役割別の属性集合。当該資産の分類、例えば、情報系資産、制御系資産、ネットワーク装置(回線含む)等の種別を記載する。本節において、情報系資産とはサーバ(DB サーバを含む)、操作端末、監視端末等パソコンやサーバの類の資産を意味し、制御系資産とは PLC 及び PLC より下流にあるバルブ、センサ等のフィールド機器を意味する。
対象装置		資産種別に含まれる個々の資産の名称。例えば監視端末、制御サーバ、PLC 等を記載する。
評価指標		当該資産のリスク値を 3 つのパラメータ(脅威レベル、脆弱性レベル、資産の重要度、以下に記載)を用いて算定する。
	脅威レベル	評価指標「脅威レベル」は、想定する脅威の発生する可能性を表す。発生する可能性は、攻撃者のスキルや攻撃の容易性を判定する。詳細は 3.4 節を参照。
	脆弱性レベル	評価指標「脆弱性レベル」は、想定する脅威が発生した場合、その脅威を受け入れる可能性(受容可能性)を意味する。受容可能性は、現在行われているセキュリティ対策の「対策レベル」の値を元に判定する。詳細は 3.5 節を参照。
	資産の重要度	評価指標「資産の重要度」は、対象資産がサイバー攻撃を受けることによって想定される①事業被害、②事業継続性の影響、及び③システム資産としての価値を考慮して、その資産をどの程度のセキュリティ強度で守っていく必要性があるか、を示す指標である。評価指標「重要度」の値を資産の重要度として定義する。詳細は 3.2 節を参照。
	リスク値	脅威レベル、脆弱性レベル及び資産の重要度の評価点を元にリスク値を算定する。リスク値は、A(リスクが高い)～E(リスクが低い)の 5 段階で評価する。
脅威(攻撃手法)		システムを構成する資産に対して想定される攻撃手法を意味する。例えば、対象となる資産への不正アクセス、サーバ等に格納されているデータの改ざんや資産そのものの破壊等である。脅威の一覧は表 3-22 及び表 3-23 を参照。

表 4-2 資産ベースのリスク分析シートにおける各項目の説明(2/2)

項目名			説明
対策			攻撃者による攻撃から制御システムを防御するために実施する対抗手段。その目的から 4 区分に分類する。本対策項目に記載されている対策候補は、項目「脅威(攻撃手法)」に記載した攻撃が行われたことを想定した対策候補である。脅威に対応する対策項目の一覧は表 3-26~表 3-29 を参照。
	防御	侵入/拡散段階	攻撃の最上流(初期段階)における対策。例えば、外部との接続点を介したネットワーク経由の攻撃、あるいはシステム(サーバ・操作端末等)設置場所への攻撃者の物理的侵入を防止する目的で実装される対策。また、攻撃者(内部犯行者を含む)による、システム(サーバ・操作端末等)への不正ログイン等を防止する目的で実装される対策。更に、システム(サーバ・操作端末等)への侵入を果たした攻撃者(人間あるいは不正プログラム)による、侵入範囲拡大(侵入したシステム内部での拡大及び他のシステムへの拡散)を防止する目的で実装される対策も含まれる。
		目的遂行段階	「情報窃取」、「データ改ざん」、「制御乗っ取り」及び「システム破壊」等、攻撃者による最終目的の実行を防止する目的で実装される対策。
	検知/被害把握		攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策、攻撃の成功による被害を最小限に留めるために実装される対策、もしくはサービスの継続、被害の早期復旧を実現するための状況把握することを目的に実装される対策。
	事業継続		攻撃の成功による被害を早期に回復して、事業の継続性を維持する目的に実装される対策。
対策レベル			当該資産に対して脅威(攻撃手法)欄に示す脅威が発生した場合、当該資産の対策結果を元に対策強度(レベル)を判定する。詳細は表 3-24 参照。

4.1.1. 資産の列挙・グループ化、資産とその重要度の記入

資産ベースのリスク分析を行うにあたり、最初に行うことはシステムを構成している資産を全て列挙することである。列挙された資産の数が少ない場合は、その資産各々に対して資産ベースのリスク分析シートを作成することが望ましい。一方で資産の数が著しく多い場合、資産各々に対して資産ベースのリスク分析シートを作成することは、作業工数が膨大になる懸念がある。その様な場合には、列挙した資産をその資産の設置場所、資産種別、論理的ネットワーク、資産の重要度及び機能等によりグループ化することを推奨する。グループ化することによって、リスク分析を行う資産の数を低減することができ、結果として、作成すべき資産ベースのリスク分析シートの枚数を減らすことが可能になる。

図 4-3 に、資産の列挙とグループ化の流れを示す。

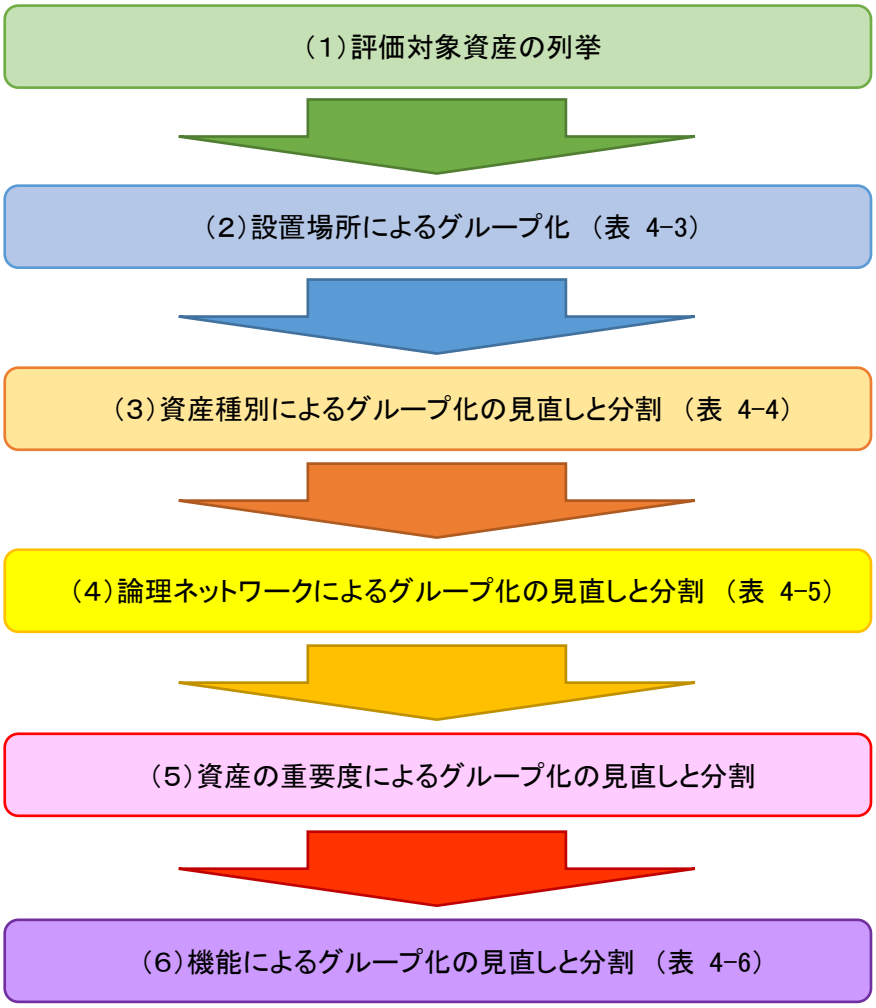


図 4-3 資産の列挙とグループ化の流れ

以下では、モデルシステムを例として、資産の列挙とグループ化の手順を説明する。

（1）評価対象資産の列挙

最初に、評価対象資産を列挙する。3.1 節で作成した資産一覧表の例（表 3-6）またはシステム構成図（図 3-6）から評価対象となる資産を抽出し、以下の評価対象資産を列挙する。

- 監視端末
- ファイアウォール
- スイッチ（DMZ 内）
- データヒストリアン
- DMZ
- スイッチ（制御ネットワーク（情報側）内）
- HMI（操作端末）
- 制御サーバ
- データサーバ
- 制御ネットワーク（情報側）
- PLC
- PLC（マスター）
- PLC（スレーブ）
- 制御ネットワーク（フィールド側）
- フィールドネットワーク

なお、以下の資産は 3.1 節にて評価対象外としたため、資産ベースの分析においても対象外とする[27]。

- ルータ
- スイッチ（情報ネットワーク内）
- 情報ネットワーク
- パッチサーバ
- EWS
- バルブ・センサ（フィールド機器）
- 保守用 PC

[27] 3.1 節に記載した通り、本評価はサイバー攻撃によって直接攻撃可能な装置、機器を対象としている。そのため、常時稼働していない非定常稼働機器や直接攻撃されないと想定されるバルブ、センサは評価対象外としている。

（2）設置場所によるグループ化

（1）にて列挙した資産に対して、設置場所によるグループ化を行う。設置場所を考慮することにより、その資産が設置されている場所のセキュリティ対策状況を併せて意識することができる。即ち、第三者が当該事業者の設備に侵入を試みる場合、当該資産の設置場所からそこにたどり着くまでに越えなければいけない障壁（困難さ）を意識できる。例えば、モデルシステムの場合は、

- 敷地内
- 計器室
- サーバ室内
- フィールド

の 4 つの場所が存在する。本システムの場合、敷地内から計器室に侵入することができなければ（施錠を開錠しなければ）、その奥にあるサーバ室内に入り込むことができないことを意味している。（1）にて列挙した評価対象資産の集合に対して、上記の設置場所と各資産の対応付けの一覧を、表 4-3 に示す。表中の二重線は、本作業にて分類された資産を示している（以下同様）。

表 4-3 設置場所による資産のグループ化

設置場所	資産
敷地内	監視端末
計器室	HMI（操作端末）
サーバ室	ファイアウォール
	スイッチ（DMZ 内）
	データヒストリアン
	DMZ
	スイッチ（制御ネットワーク（情報側）内）
	制御サーバ
	データサーバ
	制御ネットワーク（情報側）
フィールド	PLC
	PLC（マスター）
	PLC（スレーブ）
	制御ネットワーク（フィールド側）
	フィールドネットワーク

本作業により、評価対象外の資産を除いた 15 の資産を 4 のグループに分けることができた。しかしながら、場所によるグループ化だけでは脅威や対策を検討する上では粗すぎるので、次に述

べるグループ化を行う。

（3）資産種別によるグループ化の見直しと分割

次に、資産種別によるグループ化の見直しと分割を行う。機能目的、攻撃経路、攻撃目標等の観点に立ち、資産種別を「情報系資産」、「制御系資産」、「ネットワーク資産」に分類する。情報系資産とは、パソコンやサーバの様な資産であり、制御系資産とは、PLC やバルブ、センサ等のフィールド機器を示す資産である。ネットワーク資産はスイッチ、ルータ、ファイアウォール等のネットワーク装置に加え、ネットワークそのものもネットワーク資産に含まれるものと考える。

表 4-3 において、監視端末及び HMI（操作端末）は同一の設置場所に対して単一の資産しか存在しないため、一つのグループのままとし、サーバ室内の資産、及びフィールド内の資産を資産種別ごとのグループに分解することを考える。即ち、この作業では、サーバ室内の資産は、ネットワーク資産と情報系資産に分類する。また、フィールド内の資産は、ネットワーク資産と制御系資産に分類する。資産種別によりグループ化を見直した結果を、表 4-4 に示す。

表 4-4 資産種別による資産のグループ化の見直しと分割

設置場所	資産種別	資産
敷地内	―	監視端末
計器室	―	HMI（操作端末）
サーバ室	ネットワーク資産	ファイアウォール
		スイッチ（DMZ 内）
		DMZ
		スイッチ（制御ネットワーク（情報側）内）
		制御ネットワーク（情報側）
	情報系資産	データヒストリアン
		制御サーバ
		データサーバ
フィールド	ネットワーク資産	制御ネットワーク（フィールド側）
		フィールドネットワーク
	制御系資産	PLC
		PLC（マスター）
		PLC（スレーブ）

（4）論理ネットワークによるグループ化の見直しと分割

次に、資産が配置されている論理ネットワークによるグループ化の見直しと分割を行う。

図 4-4 は、モデルシステムのシステム構成図（図 3-6）に、論理ネットワークを示す点線を追記した図である。橙色の破線は制御システムの論理ネットワークの分割境界を示している。

図において、モデルシステムは、論理的に

- 情報ネットワーク
- DMZ
- 制御ネットワーク（情報側）
- 制御ネットワーク（フィールド側）
- フィールドネットワーク

によって構成されている。論理的に分割されたネットワークによって、サーバ室内の資産とフィールド内の資産のグループ化の見直しを検討する。

サーバ室内の資産は、DMZ または制御ネットワーク（情報側）に配置されているので、サーバ室内のネットワーク資産及び情報系資産を、各々の資産が配置されている論理ネットワークによってグループ化の見直しを行う。

また、フィールド内の資産は、制御ネットワーク（フィールド側）またはフィールドネットワークに配置されているので、フィールド内のネットワーク資産及び制御系資産を、各々の資産が配置されている論理ネットワークによってグループ化の見直しを行う。

以上により、評価対象の資産を 10 のグループに再編した結果を、表 4-5 に示す。

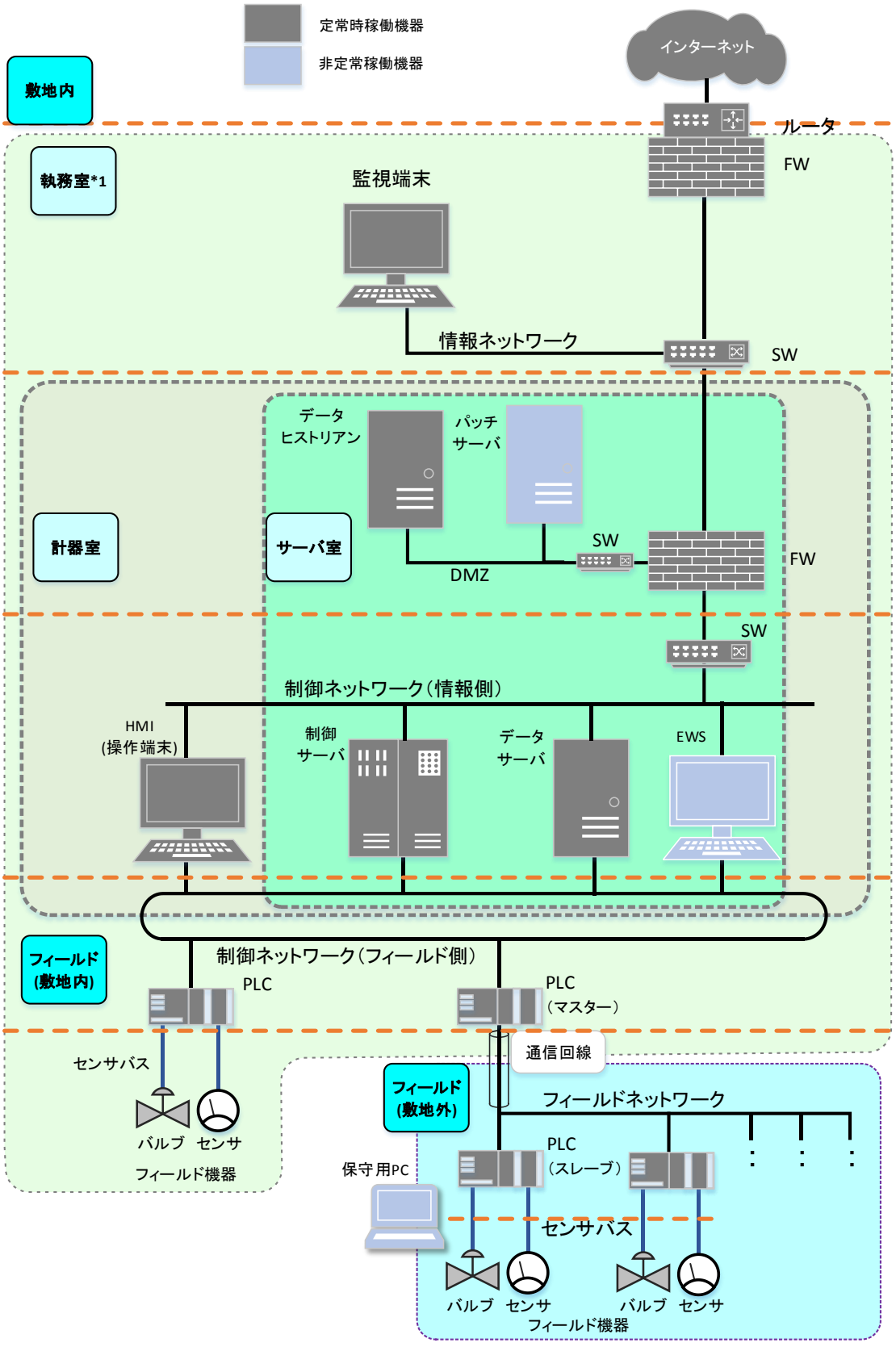


図 4-4 制御システムの論理ネットワーク図

表 4-5 論理ネットワークによる資産のグループ化の見直しと分割

資産グループ	設置場所	資産種別	接続先 NW	資産
グループ a	敷地内	－	情報 NW	監視端末
グループ b	計器室	－	制御 NW(情)	HMI(操作端末)
グループ c	サーバ室	ネットワーク資産	DMZ	ファイアウォール
				スイッチ(DMZ 内)
				DMZ
グループ d			制御 NW(情)	スイッチ(制御ネットワーク(情報側)内)
				制御ネットワーク(情報側)
グループ e		情報系資産	DMZ	データヒストリアン
グループ f			制御 NW(情)	制御サーバ
				データサーバ
グループ g	フィールド	ネットワーク資産	制御 NW(フ)	制御ネットワーク(フィールド側)
グループ h			フィールド NW	フィールドネットワーク
グループ i		制御系資産	制御 NW(フ)	PLC
				PLC(マスター)
グループ j			フィールド NW	PLC(スレーブ)

(5)資産の重要度によるグループ化の見直しと分割

次に、資産の重要度によるグループ化の見直しと分割を行う。

資産ベースのリスク分析においては、同一グループに属する資産の重要度は同一にすることが前提となる。即ち、資産の重要度が異なれば、異なるグループにする。従って、これまでのグループ化によって資産の重要度が一致しているか否かを最終的に確認し、一致していない場合はグループを分割する必要がある。

モデルシステムの例では、上記条件を満たす箇所は存在しない(表 3-14 参照)ため、表 4-5 はそのままでよい。

（6）機能によるグループ化の見直しと分割

最後に、機能によるグループ化を見直して必要な分割を行い、資産のグループ化を確定すると共に、資産グループごとの「資産の重要度」を決定する。その観点として、以下の様な項目が挙げられる：

① OS、ソフトウェア
② 機能的役割（データ管理、コマンド発行他）

例えば、同一グループに分類された資産においてもベンダーや OS が異なれば、機能や脅威、脆弱性レベルが異なるので別のグループとして扱うことが必要である。

本観点において、表 4-5 のグループ f 及びグループ i を再考する。

グループ f には制御サーバとデータサーバが含まれている。制御サーバとデータサーバの違いは、制御サーバは他装置に対してコマンドを発行することができるが、データサーバにはコマンド発行機能がなく、データを格納する機能のみを有している。制御サーバとデータサーバ間において機能差分があるため、各資産を分割する必要がある。

グループ i はいずれも PLC であるが、PLC の詳細な仕様、機能に関しては本書において細かく規定していない。よって、本書においてグループ i は分割しない。仮に PLC（マスター）が中継機能のみを有する等、機能が限定されているもしくは仕様が異なる場合は、グループ i を分割する必要が生じる。

以上より、モデルシステムの資産のグループ化を実施した最終結果を、表 4-6 に示す。15 種類の評価対象資産を、最終的に 11 のグループに分割した。

表 4-6 資産のグループ化（最終結果）

資産 グループ	設置場所	資産種別	接続先 NW	資産
グループ 1	敷地内	－	情報 NW	監視端末
グループ 2	計器室	－	制御 NW（情）	HMI（操作端末）
グループ 3	サーバ室	ネットワーク資産	DMZ	ファイアウォール
				スイッチ（DMZ 内）
				DMZ
グループ 4			制御 NW（情）	スイッチ （制御ネットワーク（情報側）内）
				制御ネットワーク（情報側）
グループ 5		情報系資産	DMZ	データヒストリアン
グループ 6			制御 NW（情）	制御サーバ
グループ 7				データサーバ
グループ 8	フィールド	ネットワーク資産	制御 NW（フ）	制御ネットワーク（フィールド側）
グループ 9			フィールド NW	フィールドネットワーク
グループ 10		制御系資産	制御 NW（フ）	PLC
				PLC（マスター）
グループ 11			フィールド NW	PLC（スレーブ）

分割された各資産グループに対して、資産ベースのリスク分析シートを作成し、リスク分析シートの「資産の重要度」の欄に、3.2 節で確定した資産の重要度を転記する。

4.1.2. 脅威（攻撃手法）と対策候補の記入、脅威レベルの評価と記入

本項では、「評価対象資産[28]」に対して、脅威の特定とその対策候補の選定を行い、資産ベースのリスク分析シートに記入する。また、評価指標の一つである脅威レベルの評価を実施し、その値をリスク分析シートに記入する。その手順の流れを、以下に示す。

【脅威（攻撃手法）の記入】

① 想定される脅威（攻撃手法）一覧（表 4-7）の確認
② 資産グループごとに対する、攻撃者視点による攻撃用途（侵入口、経由、攻撃拠点、攻撃対象）の対応付け（表 4-9）の作成
③ 脅威（攻撃手法）と攻撃者視点による攻撃用途の対応付け（表 4-10）の確認
④ 資産グループごとに対する脅威（攻撃手法）一覧の作成とリスク分析シートへの記入
アウトプット： 資産グループごとの脅威（攻撃手法）（表 4-11 及び表 4-12）

【脅威（攻撃方法）の対策候補の記入】

⑤ 脅威（攻撃手法）に対する対策候補一覧の作成とリスク分析シートへの記入

【脅威レベルの評価と記入】

⑥ 評価指標「脅威レベル」の評価とリスク分析シートへの記入

以下では、モデルシステムを例として、①～⑥の手順を説明する。

なお、脅威（攻撃手法）の記入の最終的なアウトプットは表 4-11 及び表 4-12 であるが、①～④において、その作成過程を詳述する。

[28] 資産のグループ化（4.1.1 項）を実施した場合は、「資産グループ」を意味する。実施しなかった場合は、3.1 節で洗い出した「資産」そのものを意味し、以後の「資産グループ」は「資産」と読み替える。

（1）想定される脅威（攻撃手法）一覧の確認

想定される脅威（攻撃手法）一覧を確認する。表 4-7 は、3.4 節に示した、制御システムに対して想定される脅威（攻撃手法）の一覧（表 3-22 及び表 3-23 からの抜粋）である。評価対象のシステムや個別の事業分野において過不足がある場合には、適宜修正する。

表 4-7 想定される脅威（攻撃手法）一覧

項番	脅威（攻撃手法）	説明（概要）
1	不正アクセス	ネットワーク経由での機器侵入と攻撃実行
2	物理的侵入	制限区画・領域への不正侵入、または 物理的アクセス制限機器の制限解除
3	不正操作	直接操作での機器侵入と攻撃実行
4	過失操作	内部関係者の過失操作の誘発と攻撃実行、または 正規媒体・機器の機器への接続による攻撃相当の実行
5	不正媒体・機器接続	不正持ち込み媒体・機器の機器への接続と攻撃実行
6	プロセス不正実行	攻撃対象機器上の正規プロセスの不正実行
7	マルウェア感染	攻撃対象機器へのマルウェア感染と動作
8	情報窃取	機器内の情報の窃取
9	情報改ざん	機器内の情報の改ざん
10	情報破壊	機器内の情報の破壊
11	不正送信	他の機器に対する不正制御コマンド／データの送信
12	機能停止	機器の機能停止
13	高負荷攻撃	DoS 攻撃等による機器の正常動作妨害
14	窃盗	機器の窃盗
15	盗難・廃棄時の分解 による情報窃取	盗難機器や廃棄機器の分解による、機器内の情報の窃取
16	経路遮断	通信ケーブル切断、または機器からの通信ケーブル引き抜き
17	通信輻輳	容量以上の通信トラフィック発生
18	無線妨害	無線通信の妨害
19	盗聴	ネットワーク上の情報の盗聴
20	通信データ改ざん	ネットワーク上の情報の改ざん
21	不正機器接続	ネットワーク上への不正機器の接続

（2）資産グループごとに対する攻撃者視点による攻撃用途の対応付けの作成

本項の目的は、評価対象資産（グループ化した資産）に対して、その資産グループが受ける脅威とその脅威に対する対策候補を選定し、分析シートに記入することである。そこで、まず、各々の資産グループに対して、「攻撃者視点による資産の攻撃用途」を明確にする。攻撃者視点による資産の攻撃用途とは、攻撃者が実際攻撃する際に、当該資産がどの様な役割を担うかを表し、「侵入口」、「経由」、「攻撃拠点」及び「攻撃対象」の 4 つの攻撃用途に分類する。各攻撃用途の概要を表 4-8 に示す。

表 4-8 攻撃者視点による資産の攻撃用途

攻撃用途	説明	例
侵入口	攻撃者がサイバー攻撃を行う際に侵入する入口。	● ネットワーク経由で侵入する場合に最初にログインする装置 ● 攻撃対象の機器が設置されているサーバルーム等
経由	侵入した攻撃者が攻撃拠点、もしくは攻撃対象に到達するまでに経由する装置等。	● ファイアウォールやスイッチといったネットワーク機器等 ● ネットワーク上のサーバ機器類
攻撃拠点	攻撃対象に対して攻撃を実行する（コマンド等を送信する）ことが可能な装置等。攻撃拠点と攻撃対象となる装置が同一になる場合もある。	● HMI（操作端末）等
攻撃対象	攻撃が行われ、破壊、情報窃取、改ざん等が行われる装置等。	● 制御サーバ、制御データ管理サーバ等 ● PLC 等

各々の資産グループに対して、攻撃者の視点に立って、その資産の攻撃用途を検討し、4 種類の用途に該当するか否か判断することによって、資産グループとその攻撃用途との対応付け[29]を作成する。この検討は、制御システムのネットワーク構成図を十分確認しながら、攻撃者視点に立って実施する。

4.1.1 項で分類したモデルシステムの資産グループ 1～11 に対して、表 4-8 に記載した攻撃用途との対応付けを、表 4-9 に示す。

[29] 判断に迷う場合は、4 種類全ての攻撃用途に該当する（可能性がある）と判断する。

表 4-9 資産グループと資産の攻撃用途の対応付け[30]

資産グループ	攻撃用途			
	侵入口	経由	攻撃拠点	攻撃対象
グループ 1 (監視端末)	○			
グループ 2 (HMI(操作端末))	○		○	
グループ 3 (ファイアウォール、スイッチ(DMZ 内)、 DMZ)	○	○	○	○
グループ 4 (スイッチ(制御ネットワーク(情報側)、 制御ネットワーク(情報側))	○	○	○	○
グループ 5 (データヒストリアン)	○		—[31]	○
グループ 6 (制御サーバ)	○	○	○	○
グループ 7 (データサーバ)	○	○	○	○
グループ 8 (制御ネットワーク(フィールド側))		○		
グループ 9 (フィールドネットワーク)		○		
グループ 10 (PLC、PLC(マスター))	○	○	○	○
グループ 11 (PLC(スレーブ))	○	○		○

[30] 本表を作成する際、資産グループと資産の攻撃用途を対応付けすることが困難である場合、全てのグループは全ての攻撃用途を持ちうると解釈し、即ち、表内の全ての枠に○を付けて、手順(3)へ読み進んでもよい。
[31] 本例において、データヒストリアンに格納されているデータを改ざんすることにより提供サービスに影響をあたることがないことを前提にしている。仮にデータヒストリアンに格納されているデータもしくはデータヒストリアンの設定情報が改ざんされた場合にサービスに影響を与えるのであれば、本項目は○になる。

(3)脅威(攻撃手法)と攻撃者視点による攻撃用途の対応付けの確認

各攻撃用途に対応する脅威(攻撃手法)の詳細項目を決定する。脅威(攻撃手法)と資産が持つ攻撃用途の対応付けを、表 4-10 に記す。

手順(2)にて資産グループと攻撃用途の対応付けを行ったので、それと組み合わせて、最終的に各資産グループとその資産グループが受ける脅威を対応付けることができる(手順(4)参照)。

表 4-10 脅威(攻撃手法)と資産の持つ攻撃用途の対応付け

脅威(攻撃手法)	攻撃用途			
	侵入口	経由	攻撃拠点	攻撃対象
不正アクセス	○	○		
物理的侵入	○			
不正操作	○	○	○	
過失操作	○	○	○	
不正媒体・機器接続	○		○	
プロセス不正実行			○	
マルウェア感染			○	
情報窃取				○
情報改ざん				○
情報破壊				○
不正送信			○	
機能停止				○
高負荷攻撃	○	○	○	○
窃盗	○	○	○	○
盗難・廃棄時の分解による情報窃取	○	○	○	○
経路遮断		○		
通信輻輳		○		
無線妨害		○		
盗聴		○		
通信データ改ざん		○		
不正機器接続	○			

（4）資産グループごとに対する脅威（攻撃手法）一覧の作成とリスク分析シートへの記入

資産グループごとに対する脅威（攻撃手法）を一覧にまとめて、リスク分析シートに記入する。

- 手順（2）で作成した、「資産グループ」と「攻撃者視点の攻撃用途」の対応（表 4-9）
- 手順（3）で確認した、「脅威（攻撃手法）」と「攻撃者視点の攻撃用途」の対応（表 4-10）

を元に、「攻撃者視点の攻撃用途」をキーにして、「資産グループ」と「脅威（攻撃手法）」の対応表を作成する。

例えば、表 4-9 において、資産グループ 1（監視端末）は「侵入口」の攻撃用途のみを有するので、その用途における脅威（攻撃手法）は、表 4-10 における、

- 不正アクセス
- 物理的侵入
- 不正操作
- 過失操作
- 不正媒体・機器接続
- 高負荷攻撃
- 窃盗
- 盗難・廃棄時の分解による情報窃取
- 不正機器接続

であることが確認できる。

資産グループ 2 以降も同様に考えると、モデルシステムにおける資産グループごとの脅威（攻撃手法）一覧は、表 4-11 及び表 4-12 となる。

資産グループと脅威（攻撃手法）の対応表ができたら、資産ベースのリスク分析シートに記入する。リスク分析シートは資産グループごとに作成するため、各資産グループに対してシートを用意して、グループに属する資産を、分析シートの「資産種別」欄及び「対象装置」欄に記入（転記）する。また、資産グループに該当する個々の脅威（攻撃手法）を、分析シートの「脅威（攻撃手法）」欄に記入（転記）する。

モデルシステムの例においては、11 の資産グループに対して、11 シートの資産ベースのリスク分析シートを作成し、各々のシートに対応する資産と脅威（攻撃手法）を転記する。

表 4-11 資産グループごとの脅威(攻撃手法)(1/2)

資産グループ	脅威(攻撃手法)
グループ 1 (監視端末)	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、不正機器接続
グループ 2 (HMI(操作端末))	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、プロセス不正実行、 マルウェア感染、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、不正機器接続
グループ 3 (ファイアウォール、 スイッチ(DMZ 内)、 DMZ)	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、プロセス不正実行、 マルウェア感染、情報窃取、情報改ざん、情報破壊、 不正送信、機能停止、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん、 不正機器接続
グループ 4 (スイッチ(制御ネットワーク (情報側)、 制御ネットワーク(情報側))	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、プロセス不正実行、 マルウェア感染、情報窃取、情報改ざん、情報破壊、 不正送信、機能停止、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん、 不正機器接続
グループ 5 (データヒストリアン)	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、情報窃取、情報改ざん、情報破壊、 不正送信、機能停止、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、不正機器接続
グループ 6 (制御サーバ)	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、プロセス不正実行、 マルウェア感染、情報窃取、情報改ざん、情報破壊、 不正送信、機能停止、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん、 不正機器接続

表 4-12 資産グループごとの脅威(攻撃手法)(2/2)

資産グループ	脅威(攻撃手法)
グループ 7 (データサーバ)	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、プロセス不正実行、 マルウェア感染、情報窃取、情報改ざん、情報破壊、 不正送信、機能停止、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん、 不正機器接続
グループ 8 (制御ネットワーク(フィールド側))	不正アクセス、不正操作、過失操作、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん
グループ 9 (フィールドネットワーク)	不正アクセス、不正操作、過失操作、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん
グループ 10 (PLC、PLC(マスター))	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、プロセス不正実行、 マルウェア感染、情報窃取、情報改ざん、情報破壊、 不正送信、機能停止、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん、 不正機器接続
グループ 11 (PLC(スレーブ))	不正アクセス、物理的侵入、不正操作、過失操作、 不正媒体・機器接続、情報窃取、情報改ざん、情報破壊、 不正送信、機能停止、高負荷攻撃、窃盗、 盗難・廃棄時の分解による情報窃取、経路遮断、 通信輻輳、無線妨害、盗聴、通信データ改ざん、 不正機器接続

何も書かれていない資産ベースのリスク分析シートのフォーマットに当該グループの脅威(攻撃手法)を記入する方法以外に、予め分析シートに表 4-10 に示した全ての脅威(攻撃手法)を記入しておき、不要な項目を削除する方法もある。

（5）脅威（攻撃手法）に対する対策候補一覧の作成とリスク分析シートへの記入

手順（4）でリスク分析シートに記入した、資産グループに想定される各々の脅威（攻撃手法）に対して、当該脅威（攻撃手法）への対策候補一覧を作成し、リスク分析シートに記入する。

対策候補は、3.5 節に示した「セキュリティ対策項目一覧」（表 3-26～表 3-29）より抽出する。本書においては、IPA の実績を基に、当該脅威（攻撃手法）に対して有効と考えられる対策候補として列挙している。対策候補は、本節の冒頭（表 4-1 及び表 4-2）に記載した、「防御（侵入／拡散段階）」、「防御（目的遂行段階）」、「検知・被害把握」、「事業継続」に分類の上、資産ベースのリスク分析シートの「対策」欄に記入する。

表 4-13～表 4-18 は、3.5 節に示した、各脅威（攻撃手法）に対して有効と考えられる対策候補の一覧（表 3-30～表 3-32 からの抜粋）である。また、対策項目の後ろに記した括弧つき番号は、「セキュリティ対策項目一覧」（表 3-26～表 3-29）に記載している対策項目番号である。

対策候補は、表 4-13～表 4-18 を活用して機械的（一律）に選択して記入することが可能だが、全ての候補から以下の観点を考慮した選定（絞り込み）を行って記入することも可能である[32]：

- 当該資産の位置付けと機能を考慮した際の対策としての適合性
- 当該資産の配置箇所を考慮した場合の対策候補としての可能性
- 当該資産の対策候補となる具体的な製品の存在の有無

対策候補の選定（絞り込み）により、以下の利点が得られる。

- 機器の種類や設置場所から適用対象外となる対策候補を除外することによって、リスク分析後に実施する追加対策の検討作業を効率化
- リスク分析シート膨大化を回避（事業被害ベースのリスク分析において引用する際にも有効）

表 4-19 と表 4-20 に、脅威（攻撃手法）に対する対策候補の絞り込み例を示す。〇印は、当該の資産グループに対して有効と考えられる対策である。対策候補の絞り込みを実施する場合は、これらの表を参考にするとよい[33]。

なお、各事業者において、表 4-13～表 4-18 に記載した以外の対策を実施している場合は、当該対策を資産ベースのリスク分析シートに記入してもよい。

---

[32] 対策候補から除外してしまった場合、その後に実施するリスク分析において、当該対策項目は考慮対象外となってしまう点に留意する必要がある。対策項目を絞りこむ際は慎重に行うべきである。

[33] 但し、対策候補の絞り込み作業は必須ではない。対策が有効であるか否かの判断に不安を感じたり、時間を要したりするのであれば、全ての対策候補を記入しておき、実施／未実施の段階で判断することを推奨する。

表 4-13 脅威(攻撃手法)に対する対策一覧(1/6)

項番	脅威(攻撃手法)	用途・目的	対策項目
1	不正アクセス	防御(侵入／拡散段階)	・ファイアウォール [1, 2, 3, 4, 11] ・通信相手の認証 [7] ・IPS／IDS [5] ・パッチ適用 [15] ・脆弱性回避 [16]
		検知／被害把握	・IPS/IDS [5] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
2	物理的侵入	防御(侵入／拡散段階)	・入退管理 [40] ・施錠管理 [43]
		検知／被害把握	・監視カメラ [41] ・侵入センサ [42]
3	不正操作	防御(侵入／拡散段階)	・操作者認証 [18]
4	過失操作	防御(侵入／拡散段階)	・URL フィルタリング ／Web レピュテーション [12] ・メールフィルタリング [13]
5	不正媒体・機器接続	防御(侵入／拡散段階)	・デバイス接続・利用制限 [19]
		防御(目的遂行段階)	・デバイス接続・利用制限 [19]
		検知／被害把握	・デバイス接続・利用制限 [19] ・ログ収集・分析 [35] ・統合ログ管理システム [37]

表 4-14 脅威(攻撃手法)に対する対策一覧(2/6)

項番	脅威(攻撃手法)	用途・目的	対策項目
6	プロセス不正実行	防御(侵入／拡散段階)	・権限管理 [23] ・アクセス制御 [24] ・ホワイトリストによるプロセスの起動制限 [22] ・重要操作の承認 [20]
		防御(目的遂行段階)	・権限管理 [23] ・アクセス制御 [24] ・ホワイトリストによるプロセスの起動制限 [22] ・重要操作の承認 [20]
		検知／被害把握	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
7	マルウェア感染	防御(侵入／拡散段階)	・アンチウイルス [10] ・ホワイトリストによるプロセスの起動制限 [22] ・パッチ適用 [15] ・脆弱性回避 [16] ・データ署名 [26]
		検知／被害把握	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]

表 4-15 脅威(攻撃手法)に対する対策一覧(3/6)

項番	脅威(攻撃手法)	用途・目的	対策項目
8	情報窃取	防御(侵入／拡散段階)	・権限管理 [23] ・アクセス制御 [24] ・データ暗号化 [25] ・DLP [27]
		防御(目的遂行段階)	・権限管理 [23] ・アクセス制御 [24] ・データ暗号化 [25] ・DLP [27]
		検知／被害把握	・ログ収集・分析 [35] ・統合ログ管理システム [37]
9	情報改ざん	防御(侵入／拡散段階)	・権限管理 [23] ・アクセス制御 [24] ・データ署名 [26]
		防御(目的遂行段階)	・権限管理 [23] ・アクセス制御 [24] ・データ署名 [26]
		検知／被害把握	・機器異常検知 [34] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
		事業継続	・データバックアップ [31]
10	情報破壊	防御(目的遂行段階)	・権限管理 [23] ・アクセス制御 [24]
		検知／被害把握	・機器異常検知 [34] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
		事業継続	・データバックアップ [31]

表 4-16 脅威(攻撃手法)に対する対策一覧(4/6)

項番	脅威(攻撃手法)	用途・目的	対策項目
11	不正送信	防御(侵入／拡散段階)	・セグメント分割／ゾーニング [17] ・データ署名 [26] ・重要操作の承認 [20]
		防御(目的遂行段階)	・セグメント分割／ゾーニング [17] ・データ署名 [26] ・重要操作の承認 [20]
		検知／被害把握	・ログ収集・分析 [35] ・統合ログ管理システム [37]
12	機能停止	検知／被害把握	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
		事業継続	・冗長化 [32] ・フェールセーフ設計 [44]
13	高負荷攻撃	防御(目的遂行段階)	・DDoS 対策 [6]
		検知／被害把握	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
		事業継続	・冗長化 [32] ・フェールセーフ設計 [44]
14	窃盗	防御(侵入／拡散段階)	・施錠管理 [43]
		防御(目的遂行段階)	・施錠管理 [43]
		検知／被害把握	・施錠管理 [43]
15	盗難・廃棄時の分解による情報窃取	防御(侵入／拡散段階)	・耐タンパー [28] ・難読化 [29] ・セキュア消去 [30]
		防御(目的遂行段階)	・耐タンパー [28] ・難読化 [29] ・セキュア消去 [30]

表 4-17 脅威(攻撃手法)に対する対策一覧(5/6)

項番	脅威(攻撃手法)	用途・目的	対策項目
16	経路遮断	防御(侵入／拡散段階)	・入退管理 [40] ・施錠管理 [43]
		検知／被害把握	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37] ・監視カメラ [41] ・侵入センサ [42]
		事業継続	・冗長化 [32]
17	通信輻輳	防御(侵入／拡散段階)	・ファイアウォール [1, 2, 11] ・IPS／IDS [5] ・DDoS 対策 [6]
		検知／被害把握	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
		事業継続	・冗長化 [32]
18	無線妨害	検知／被害把握	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]
		事業継続	・冗長化 [32]

表 4-18 脅威(攻撃手法)に対する対策一覧(6/6)

項番	脅威(攻撃手法)	用途・目的	対策項目
19	盗聴	防御(侵入／拡散段階)	・通信路暗号化 [9] ・データ暗号化 [25] ・専用線 [8]
20	通信データ改ざん	防御(侵入／拡散段階)	・通信路暗号化 [9] ・データ暗号化 [25] ・専用線 [8]
		検知／被害把握	・ログ収集・分析 [35] ・統合ログ管理システム [37]
21	不正機器接続	防御(侵入／拡散段階)	・デバイス接続・利用制限 [19]
		検知／被害把握	・デバイス接続・利用制限 [19] ・ログ収集・分析 [35] ・統合ログ管理システム [37]

表 4-19 脅威(攻撃手法)に対する対策項目の絞り込み例(1/2)

項番	脅威(攻撃手法)	対策項目	対策項目の絞り込み例			
			ネットワーク資産	サーバ	クライアント	制御装置
			・ルータ ・FW ・スイッチ ・情報ネットワーク ・制御ネットワーク	・データヒストリアン ・制御サーバ ・データサーバ	・監視端末 ・HMI(操作端末)	・PLC
1	不正アクセス	・ファイアウォール [1, 2, 3, 4, 11]	○			
		・通信相手の認証 [7]	○	○		
		・IPS／IDS [5]	○			
		・パッチ適用 [15]	○	○	○	○
		・脆弱性回避 [16]	○	○	○	
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
2	物理的侵入	・入退管理 [40]				
		・施錠管理 [43]	○	○		○
		・監視カメラ [41]				
		・侵入センサ [42]				
3	不正操作	・操作者認証 [18]	○	○	○	○
4	過失操作	・URL フィルタリング ／Web レピュテーション [12]	○	○		
		・メールフィルタリング [13]	○			
5	不正媒体・機器接続	・デバイス接続・利用制限 [19]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
6	プロセス不正実行	・権限管理 [23]	○	○	○	
		・アクセス制御 [24]	○	○		
		・ホワイトリストによるプロセスの 起動制限 [22]		○		
		・重要操作の承認 [20]	○	○		
		・機器異常検知 [34]	○	○	○	○
		・機器死活監視 [33]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
7	マルウェア感染	・アンチウイルス [10]		○	○	
		・ホワイトリストによるプロセスの 起動制限 [22]		○		
		・パッチ適用 [15]	○	○	○	○
		・脆弱性回避 [16]	○	○	○	
		・データ署名 [26]		○		
		・機器異常検知 [34]	○	○	○	○
		・機器死活監視 [33]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
8	情報窃取	・権限管理 [23]	○	○	○	
		・アクセス制御 [24]	○	○		
		・データ暗号化 [25]	○	○	○	
		・DLP [27]		○		
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
9	情報改ざん	・権限管理 [23]	○	○	○	
		・アクセス制御 [24]	○	○		
		・データ署名 [26]		○		
		・機器異常検知 [34]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○	○	○
		・データバックアップ [31]	○	○		
10	情報破壊	・権限管理 [23]				
		・アクセス制御 [24]				
		・機器異常検知 [34]				
		・ログ収集・分析 [35]				
		・統合ログ管理システム [37]				
		・データバックアップ [31]				

表 4-20 脅威（攻撃手法）に対する対策項目の絞り込み例（2/2）

項番	脅威（攻撃手法）	対策項目	対策項目の絞り込み例			
			ネットワーク資産	サーバ	クライアント	制御装置
			・ルータ ・FW ・スイッチ ・情報ネットワーク ・制御ネットワーク	・データヒストリアン ・制御サーバ ・データサーバ	・監視端末 ・HMI（操作端末）	・PLC
11	不正送信	・セグメント分割／ゾーニング [17]	○			
		・データ署名 [26]		○		○
		・重要操作の承認 [20]		○		
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
12	機能停止	・機器異常検知 [34]	○	○	○	○
		・機器死活監視 [33]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
		・冗長化 [32]	○	○		○
		・フェールセーフ設計 [44]				○
13	高負荷攻撃	・DDoS 対策 [6]	○	○		
		・機器異常検知 [34]	○	○	○	○
		・機器死活監視 [33]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
		・冗長化 [32]	○	○		○
		・フェールセーフ設計 [44]				○
14	窃盗	・施錠管理 [43]				
15	盗難・廃棄時の分解による情報窃取	・耐タンパー [28]				
		・難読化 [29]				
		・セキュア消去 [30]		○		○
16	経路遮断	・入退管理 [40]				
		・施錠管理 [43]	○			
		・機器異常検知 [34]	○	○	○	○
		・機器死活監視 [33]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
		・監視カメラ [41]				
		・侵入センサ [42]				
		・冗長化 [32]	○	○		○
17	通信輻輳	・ファイアウォール [1, 2, 11]	○			
		・IPS／IDS [5]	○			
		・DDoS 対策 [6]	○			
		・機器異常検知 [34]	○	○	○	○
		・機器死活監視 [33]	○	○	○	○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
		・冗長化 [32]	○	○		○
18	無線妨害	・機器異常検知 [34]	○	○		○
		・機器死活監視 [33]	○	○		○
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
		・冗長化 [32]	○	○		○
19	盗聴	・通信路暗号化 [9]	○			
		・データ暗号化 [25]				
		・専用線 [8]	○			
20	通信データ改ざん	・通信路暗号化 [9]	○			
		・データ暗号化 [25]				
		・専用線 [8]	○			
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○
21	不正機器接続	・デバイス接続・利用制限 [19]	○			
		・ログ収集・分析 [35]	○	○	○	○
		・統合ログ管理システム [37]	○	○		○

（6）評価指標「脅威レベル」の評価とリスク分析シートへの記入

手順（4）でリスク分析シートに記入した、資産グループに想定される各々の脅威（攻撃手法）に対して、評価指標「脅威レベル」の評価を実施し、その値をリスク分析シートに記入する。

脅威レベルの値は、3.4.1 項にて事業者が定義した評価基準に基づき、脅威ごとに判断して決定し、分析シートの「脅威レベル」欄に記入する。

【参考】 脅威レベルマトリックスを活用した評価結果の整理

「脅威レベル」の評価及びリスク分析シートへの評価値の記入に際して、脅威レベルマトリックス（表 4-21）を作成し、そのセルに「脅威レベル」の評価値を記入・整理する方法を紹介する。

表において、無色のセルは、当該の資産グループにおいて脅威（攻撃手法）が存在することを示し、グレーアウトのセルは、脅威（攻撃手法）が存在しないことを意味している。従って、前者（無色のセル）に対して、3.4.1 項にて定義した評価基準に基づき「脅威レベル」の値（1～3）を決定し、セル内に記入する。この様な表を作成して、脅威レベルの値を一通り検討し、確定した後にリスク分析シートに転記する。これにより、例えば、

- リスク分析シートは、資産グループごとに分かれているが、この表で全ての脅威レベルの評価値を俯瞰することができる。
- この結果、同種の脅威（攻撃手法）に対して、資産グループごとの脅威レベル値を横串で比較し、同一であること、あるいは資産グループによって異なることの妥当性を再確認する手助けとなる。

といった点で、脅威レベルの評価作業を整理・見直すことができる。

表 4-21 脅威レベルマトリックス（資産グループと脅威（攻撃手法）の対応表）の例

	グループ 1	グループ 2	グループ 3	グループ 4	グループ 5	グループ 6	グループ 7	グループ 8	グループ 9	グループ 10	グループ 11
不正アクセス											
物理的侵入								■	■		
不正操作											
過失操作											
不正媒体・機器接続								■	■		
プロセス不正実行	■				■			■	■		■
マルウェア感染	■				■			■	■		■
情報窃取	■	■						■	■		
情報改ざん	■	■						■	■		
情報破壊	■	■						■	■		
不正送信	■	■						■	■		
機能停止	■	■						■	■		
高負荷攻撃											
窃盗											
盗難・廃棄時の分解による情報窃取											
経路遮断	■										
通信輻輳	■										
無線妨害	■										
盗聴	■										
通信データ改ざん	■										
不正機器接続								■	■		

4.1.3. セキュリティ対策状況の記入

前項までの手順で、評価対象システムの資産をグループ化し、グループ化した資産ごとに資産ベースのリスク分析シートを作成の上、資産及びその評価指標「資産の重要度」の値、資産に対して想定される脅威（攻撃手法）及びその評価指標「脅威レベル」の値、セキュリティ対策候補の記入が終了した。

本項以降では、各々の資産に対して実施しているセキュリティ対策状況を記入し、評価指標「脆弱性」の値を決定・記入し、最終的にリスク値の評価を行う。

本項では、実施しているセキュリティ対策状況を確認、記入する。分析シートの「対策」欄に記入済みの各々の対策候補に対して、対策名の右隣の欄に、

実施していれば　→　○を記入する。
未実施ならば　→　空欄のままとする。
　　但し、本来実施すべきと判断した対策が未実施の場合には、
　　以降の対策強化検討時の参考になるので、×を記入しておく。

なお、セキュリティ対策状況は、グループ化した資産を単位として評価するが、グループ内の資産において対策状況が異なる場合の評価について説明する。

図 4-5 は、本書のモデルシステムより抜粋した図（グループ 3 に属する資産）である。図に示す様に、対象資産が直列に繋がっている状態で、FW（ファイアウォール）に不正アクセスし、☆の SW（スイッチ）を通過し、その先にある制御サーバから不正コマンドを発行する様な攻撃が行われると想定する場合、いずれかの資産で攻撃を防御できれば良いと考えられる、従って、上段の SW、FW、下段の SW のいずれかの資産において、対策を実施していれば「○」とする。

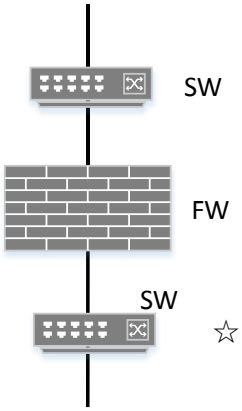


図 4-5 同一資産グループの構成例（直列）

本項までの作業をまとめ、図 4-6 に示す。本作業までにおいて資産ベースのリスク分析の準備が整った。4.1.4 項以降では、各評価指標のレベル値を決定し、最終的なリスク値を算定する過程を説明する。

【コラム】

資産ベースのリスク分析における脅威レベル決定の一方法

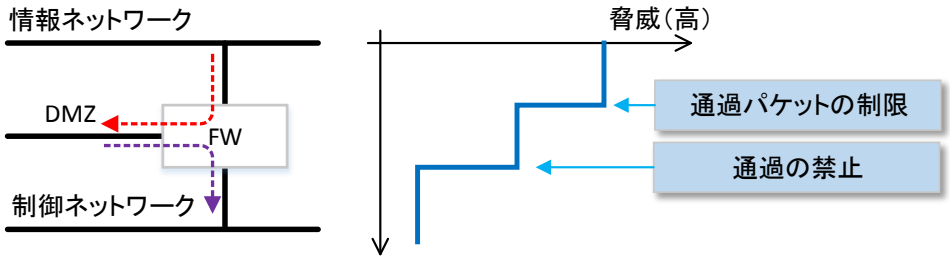
資産ベースのリスク分析は資産単体についての分析であるため、明示的にはシステムにおける資産の論理的/物理的な位置を考慮せず脅威レベルを決めている。

ここで紹介する資産ベースのリスク分析への論理的／物理的な位置を考慮した脅威レベル決定法の導入は、事業被害ベースのリスク分析を行うほどのリソースが確保できないがより現実に合った分析を行いたい場合に有効である。

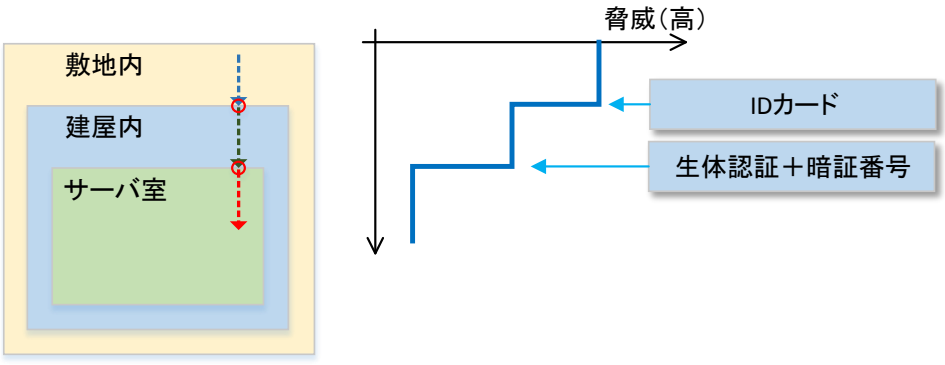
本方法では、下図に示した様に、資産ベースのリスク分析における脅威レベルは、基本的に、資産がどの様な保護装置の中に置かれているかを考慮して決定する。例えば、ファイアウォールに守られたネットワークや施錠された部屋等、十分に保護された環境では脅威は低く、誰もがアクセスしやすい環境では脅威は高いという考え方である。

この脅威は、ネットワーク（論理的位置）を介するケースと物理的アクセスを介するものがあるので、この 2 つを考えて脅威レベルの値を決めるのが望ましい。

・ネットワークを介する脅威の考え方（例）



・物理アクセスを介する脅威の考え方（例）



資産ベースのリスク分析シート

凡例: ○ 対策実施　　× 対策未実施　　グレーアウト行：該当資産で考慮しない脅威

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策						対策レベル
									防御				検知/被害把握		脅威毎
									侵入/拡散段階		目的遂行段階				
			脅威レベル	脆弱性レベル	資産の重要度	リスク値									
1	情報系資産	**データサーバ**	**2**	**2**		**B**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム		2
2			**2**	**1**		**C**	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。 あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理　(ICカード、生体認証) 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○	3
3			**2**	**2**		**B**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass)	○					2
4			**2**	**3**		**A**	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング						1
5			**2**	**3**		**A**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		1
6			**2**	**2**		**B**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○	(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
7			**1**	**2**		**C**	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 ○ 			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
8			**3**	**2**		**A**	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム		2
9			**3**	**3**		**A**	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名		(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	○	1
10			**3**	**3**		**A**	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御	○	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	○	1
11			**3**	**3**	**3**	**A**	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム			1
12			**2**	**3**		**A**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計		1
13			**3**	**3**		**A**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計		1
14			**2**	**2**		**B**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		施錠管理	○		2
15			**3**	**3**		**A**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去		(同左) (同左) (同左)					1
16			**3**	**2**		**A**	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理　(ICカード、生体認証) 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ	 ○ ○	冗長化		2
17			**1**	**3**		**B**	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化	1
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化	
19			**2**	**3**		**A**	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線						1
20			**2**	**3**		**A**	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム		1
21			**3**	**3**		**A**	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		1

図 4-6 リスク分析シートのテンプレートの例

このページは空白です。

4.1.4. 対策レベル／脆弱性レベルの評価・記入

資産グループに対して想定される脅威（攻撃手段）のセキュリティ対策状況の記入が終了したら、対策レベルの評価を実施する。各事業者にて、サイバー攻撃から当該資産を防御できるかの観点において、「対策レベル」の評価値を決定する。

分析シートの対策欄において「検知・被害把握」及び「事業継続」に分類される対策項目も記入しているが、これらの対策項目は、実際サイバー攻撃を防止できない。即ち、検知または被害把握は可能だが、攻撃を受けていること自体は防止できない。あるいは、事業継続上は有効な対策であるが、攻撃防止効果はない。従って、「対策レベル」の値は、防御（「防御（侵入／拡散段階）」及び「防御（目的遂行段階）」）に分類される対策項目の対策状況のみを用いて一次評価をする。但し、対策レベルの一次評価には使用しないが、「検知・被害把握」の対策が攻撃の侵入／拡散や目的遂行の防止につながる対策である場合には、適宜使用する。また、資産の重要度が高いものに対しては、「事業継続」の対策も評価に入れることが考えられる。

また、表 4-13～表 4-18 に記載した対策一覧以外のセキュリティ対策を記入した場合は、事業者にて当該対策の評価値を決定する。

3.5 節において定義した通り、評価指標の一つである「脆弱性レベル」の値は、「対策レベル」の双対の値として定義する。表 4-22 に、両者の値の関係を示す（表 3-24 の抜粋）。

表 4-22 対策レベル値と脆弱性レベルの値の関係

対策レベル	脆弱性レベル
3	1
2	2
1	3

従って、「対策レベル」の評価値を決定すると、自動的に「脆弱性レベル」の評価値が求まるので、両者の値を、リスク分析シートの該当欄に記入する。

【参考】 対策レベルの具体的な判断基準（指針）の例

なお、「対策レベル」の評価値の判断基準は、3.5 節（表 3-24）において定義しているが、統一した基準で評価を行うためには、より具体的な判断基準（指針）を事業者にて定めることが望ましい。表 4-23 及び表 4-24 に、具体的な判断基準（指針）の定義例を示す。

表 4-23 対策レベルの具体的な判断基準（指針）の例

対策レベルの値	具体的な判断基準の例
1	当該脅威（攻撃手段）において、「防御」可能な対策項目を実施していない。 即ち、〇が一つもついていない。
2	当該脅威（攻撃手段）において、「防御」可能な対策項目を実施している。 即ち、〇が一つ以上ついている。
3	当該脅威（攻撃手段）において、複数の「防御」可能な対策項目を実施しており（即ち、〇が二つ以上ついており）、かつ表 4-24 に示す基準を満たす対策を一つ以上実施している。

表 4-24 対策レベル＝3 の判断基準（指針）の例[34]

対策分類	対策項目	“3” になり得る典型的な対策例
防御 （初期潜入）	FW	● 一方向ゲートウェイの利用
	通信路暗号化	● チェックリストを満たす暗号技術による暗号化（7.1 節参照）
	パッチ適用	● 全パッチ即時適用 ● パッチ公開後、適用必要性を判断し、必要に応じて即時適用
	操作者認証	● 生体認証 ● 二要素認証
	デバイス接続・利用制限	● 物理的な接続禁止措置 ● 資産管理ソフトウェアの導入
	入退管理	● 生体認証 ● 二要素認証
	ホワイトリストによるプロセスの起動制限	● ホワイトリストを設定している(本対策項目に〇がついている)
防御 （目的遂行）	データ署名	● 「通信路暗号化」と同じ
	データ暗号化	● 「通信路暗号化」と同じ
	セキュア消去	● 記録デバイスの物理的な破壊 ● 磁気消去（磁気デバイスに対してのみ）

[34] このレベル評価は IPA の知見に基づき行った基準であり、各事業者にて適宜定義、変更してよい。

4.1.5. リスク値の評価

リスク値は、3 つの評価指標「資産の重要度」「脆弱性レベル」及び「脅威レベル」によって算定する。リスク値は A(リスクが高い)～E(リスクが低い)の 5 段階で評価する。

表 4-25 に、各評価値に基づくリスク値の算定基準を示す。また、各評価値とリスク値の関係を、図 4-7 に示す。

図 4-7 より、右上の領域のリスク値が高く、左下(原点)に近づくにつれてリスク値が低いことがわかる。これは、重要度の評価値が大きければリスク値が高くなり、各評価値が小さくなるにつれてリスク値が低くなることを図示している。脅威と脆弱性は相乗的な関係にあるので、その積で評価している。

表 4-25 に示した算定基準に従い、各資産及び脅威ごとにリスク値を算定し、資産ベースのリスク分析シートに記入する。

以上により、資産ベースのリスク分析シートが完成した。本節にて行った分析結果を元に、5 章にてその活用法を述べる。

表 4-25 資産ベースのリスク分析におけるリスク値の算定基準

評価指標と評価点			リスク値	判定条件
脅威レベル	脆弱性レベル	資産の重要度		
3	3	3	A	重要度＝3 6≦脅威×脆弱性≦9
3	2	3		
2	3	3		
2	2	3	B	重要度＝3 3≦脅威×脆弱性＜6
3	1	3		
1	3	3		
3	3	2		重要度＝2 6≦脅威×脆弱性≦9
3	2	2		
2	3	2		
2	1	3	C	重要度＝3 1≦脅威×脆弱性＜3
1	2	3		
1	1	3		
2	2	2		重要度＝2 3≦脅威×脆弱性＜6
3	1	2		
1	3	2		
3	3	1		重要度＝1 6＜脅威×脆弱性≦9
2	1	2	D	重要度＝2 1≦脅威×脆弱性＜3
1	2	2		
1	1	2		
3	2	1		重要度＝1 3＜脅威×脆弱性≦6
2	3	1		
2	2	1		
3	1	1	E	重要度＝1 1≦脅威×脆弱性≦3
1	3	1		
2	1	1		
1	2	1		
1	1	1		

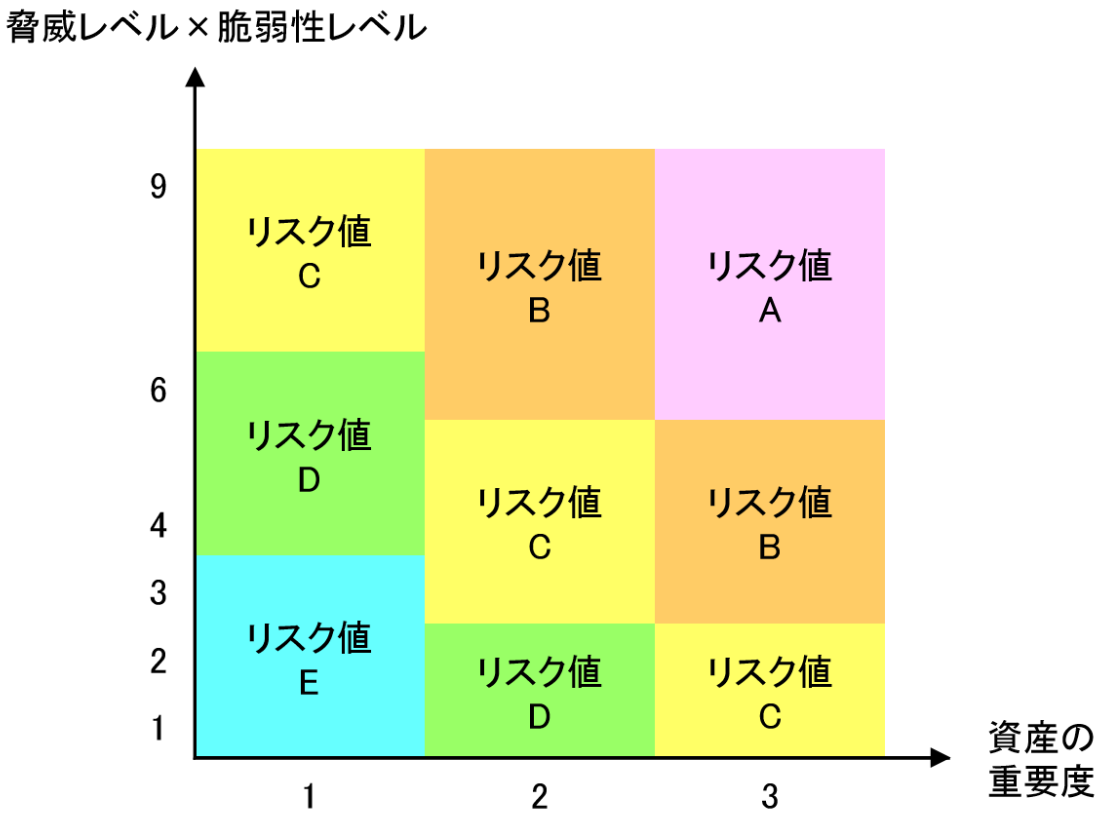


図 4-7 脅威レベル・脆弱性レベル・資産の重要度とリスク値の関係

4.2. 事業被害ベースのリスク分析

本節では、事業被害ベースのリスク分析の手順を解説する。

事業被害ベースのリスク分析は、回避したい事業被害を引き起こす攻撃シナリオと、攻撃者視点でそれらの攻撃シナリオを実現する攻撃ツリーを洗い出し、各攻撃ツリーのリスクの大きさ(リスク値)を算定する分析方法である。事業被害につながる攻撃を受けた場合に、現在の対策で攻撃や被害を防止できるか否かを確認し、攻撃や被害を防止できないリスクが高い箇所に講じる対策強化策を検討することを目的としている。

事業被害ベースのリスク分析は、以下の手順にて行う。

① 事業被害を引き起こす攻撃シナリオの策定 (☞ 4.2.1 項)
② 攻撃シナリオを実現する攻撃ツリーの作成 (☞ 4.2.2 項)
③ 各攻撃ツリーの脅威レベルと事業被害レベルの評価 (☞ 4.2.3 項)
④ 現在実施しているセキュリティ対策の記入 (☞ 4.2.4 項)
⑤ 対策レベル／脆弱性レベルの評価 (☞ 4.2.5 項)
⑥ 脅威、脆弱性、事業被害からのリスク値の評価 (☞ 4.2.6 項)

4 章の冒頭でも述べたが、以下では、3 章で述べたモデルシステム(図 3-6)を評価対象システムとし、各構成機器の機能や環境の条件を前提として、具体的な手順を説明する。

図 4-8 に、リスク分析を実施するために作成する、事業被害ベースのリスク分析シートのフォーマットを示す。この時点では、項番及び横軸の項目名のみが記載されている。

図 4-9 に、フォーマットに必要事項を記入して作成した、事業被害ベースのリスク分析シートの完成例を示す。

本節において、フォーマットから事業被害ベースのリスク分析シートを作成する手順を説明する。シート中の各項目の記入方法については、図 4-8 の上段に示している各項番号(4.2.1 項～4.2.6 項)において説明する。事業被害ベースのリスク分析シートに記載される項目の説明を表 4-26～表 4-28 に示す。

4.2.1項　4.2.2項　4.2.3項　4.2.6項　4.2.4項　4.2.5項

事業被害ベースのリスク分析シート

X. ＜事業被害＞

項番	攻撃シナリオ		評価指標				対策				対策レベル		攻撃ツリー番号	
		攻撃ツリー／攻撃ステップ	脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	X-X	＜攻撃シナリオ＞												
1		＜攻撃ステップ＞												
2		＜攻撃ステップ＞												
3		＜攻撃ステップ＞												
4		＜攻撃ステップ＞												
5		＜攻撃ステップ＞												
6		＜攻撃ステップ＞												
7		＜攻撃ステップ＞												
8		＜攻撃ステップ＞												
9		＜攻撃ステップ＞												
10		＜攻撃ステップ＞												
11		＜攻撃ステップ＞												
12		＜攻撃ステップ＞												
13		＜攻撃ステップ＞												
14		＜攻撃ステップ＞												
15		＜攻撃ステップ＞												

（注）＜＞には、記載項目の具体的な内容を記載

図 4-8　事業被害ベースのリスク分析シート（フォーマット）

事業被害ベースのリスク分析シート

１．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策								対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御				検知／被害把握		事業継続		攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階		目的遂行段階									
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。																
1		**侵入口＝監視端末** 悪意のある第三者が、情報ネットワーク上の監視端末に不正アクセスする。					FW（パケットフィルタリング型） パッチ適用 通信相手の認証 操作者認証	 〇 〇	権限管理 アクセス制御	 〇	ログ収集・分析	〇			2			
2		悪意のある第三者が、監視端末からデータヒストリアンに不正アクセスする。					FW（パケットフィルタリング型） パッチ適用 通信相手の認証 操作者認証	〇 〇	権限管理 アクセス制御	〇 〇	ログ収集・分析	〇			2			
3		悪意のある第三者が、データヒストリアンからファイアウォールに不正アクセスする。					FW（パケットフィルタリング型） パッチ適用 通信相手の認証 操作者認証	〇 〇 〇	権限管理 アクセス制御	〇 〇	ログ収集・分析	〇			2			
4		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。					パッチ適用 通信相手の認証 操作者認証	 〇	権限管理 アクセス制御	〇 〇	ログ収集・分析	〇			2			
5		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2	2	3	B			重要操作の承認 	 	機器異常検知 ログ収集・分析	〇 〇			1	2	#1	1,2,3,4,5
6		悪意のある第三者が、ファイアウォールから制御サーバに不正アクセスする。					パッチ適用 通信相手の認証 操作者認証	 〇	権限管理 アクセス制御	〇 〇	ログ収集・分析	〇			2			
7		悪意のある第三者が、制御サーバ上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2	2	3	B			重要操作の承認 	 	機器異常検知 ログ収集・分析	〇 〇			1	2	#2	1,2,3,6,7
8		悪意のある第三者が、ファイアウォールからデータサーバに不正アクセスする。					パッチ適用 通信相手の認証 操作者認証	 〇	権限管理 アクセス制御	〇 〇	ログ収集・分析	〇			2			
9		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。					パッチ適用 通信相手の認証 操作者認証	 	権限管理 アクセス制御	 	ログ収集・分析	〇			1			
10		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3	B			重要操作の承認 	 	機器異常検知 ログ収集・分析	〇 〇			1	2	#3	1,2,3,8,9,10
11		悪意のある第三者が、監視端末をマルウェアに感染させる。					アンチウィルス パッチ適用 ホワイトリストによるプロセスの起動制限リスト	〇 〇			機器異常検知 ログ収集・分析	 〇			2			
12		マルウェアが、監視端末からデータヒストリアンに不正アクセスする／マルウェアに感染させる。					FW（パケットフィルタリング型） パッチ適用 通信相手の認証 操作者認証 アンチウイルス ホワイトリストによるプロセスの起動制限	〇 〇 	権限管理 アクセス制御	〇 〇	機器異常検知 ログ収集・分析	 〇			2			
13		マルウェアが、データヒストリアンからファイアウォールに不正アクセスする／マルウェアに感染させる。					FW（パケットフィルタリング型） パッチ適用 通信相手の認証 操作者認証	〇 〇 〇	権限管理 アクセス制御	〇 〇	機器異常検知 ログ収集・分析	 〇			2			

図 4-9 事業被害ベースのリスク分析シート（完成例）

表 4-26 事業被害ベースのリスク分析シートの項目(1/3)

項目		説明
項番		各行の参照番号。
攻撃シナリオ		事業被害を引き起こす可能性のある攻撃のシナリオ。 例 事業被害が「供給停止」であれば、「供給停止操作を実行される」、「重要なデータの改ざんにより、供給停止が誘発される」等
攻撃ツリー／攻撃ステップ		攻撃ツリーは、攻撃シナリオを実現するための、侵入から最終的な目的遂行までの一連の攻撃手順。1 つの攻撃ツリーは複数の攻撃ステップから構成され、個々の手順が攻撃ステップとなる。 例 攻撃者が情報ネットワークから制御ネットワークに侵入し、制御サーバから供給停止操作を行う攻撃ツリー: 「攻撃ステップ① 情報ネットワークからファイアウォールに不正アクセスし、制御ネットワークに侵入する」 →「攻撃ステップ② 制御サーバに不正アクセスする」 →「攻撃ステップ③ 制御サーバ上で、供給停止操作を実行する」
評価指標	脅威レベル	想定した脅威が発生する(事業被害ベース分析では想定した攻撃ツリーが成立する)可能性を表す。発生する可能性は、攻撃者のスキルや攻撃の容易性を元に判定する。詳細は 3.4 節を参照。
	脆弱性レベル	想定した攻撃ツリーが成立した場合、その脅威を受け入れる可能性(受容可能性)を意味する。受容可能性は、現在行われているセキュリティ対策の「対策レベル」の値を元に判定する。詳細は 3.5 節を参照。
	事業被害レベル	想定した攻撃ツリーが行われた場合の被害範囲や会社経営上の打撃を表す。詳細は、3.3 節を参照。
	リスク値	脅威レベル、脆弱性レベル及び事業被害レベルの評価点を元にリスク値を算定する。リスク値は A(リスクが高い)～E(リスクが低い)の 5 段階で評価する。

表 4-27 事業被害ベースのリスク分析シートの項目(2/3)

項目			説明	
対策			攻撃者による攻撃から制御システムを防御するために実施する対抗手段。その目的から 4 区分に分類する。本対策項目に記載されている対策候補は、項目「攻撃ツリー／攻撃ステップ」に記載した攻撃が行われたことを想定した対策候補である。攻撃に対応する対策項目の一覧は表 3-26～表 3-29 を参照。	
	防御	侵入／拡散段階	攻撃の最上流(初期段階)における対策。例えば、外部との接続点を介したネットワーク経由の攻撃、あるいはシステム(サーバ・操作端末等)設置場所への攻撃者の物理的侵入を防止する目的で実装される対策。また、攻撃者(内部犯行者を含む)による、システム(サーバ・操作端末等)への不正ログイン等を防止する目的で実装される対策。更に、システム(サーバ・操作端末等)への侵入を果たした攻撃者(人間あるいは不正プログラム)による、侵入範囲拡大(侵入したシステム内部での拡大及び他のシステムへの拡散)を防止する目的で実装される対策も含まれる。	
			例	「セグメント分割／ゾーニング」、「IPS／IDS」、「操作者認証」、「アクセス制御」、「APT 対策ツール」
		目的遂行段階	情報窃取、データ改ざん、制御乗っ取り、及びシステム破壊等、攻撃者による最終目的の実行を防止する目的で実装される対策。	
			例	「データ暗号化」、「重要操作の承認」、「フェールセーフ設計」
	検知／被害把握		攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策、攻撃の成功による被害を最小限に留めるために実装される対策、もしくはサービスの継続、被害の早期復旧を実現するための状況把握することを目的に実装される対策。	
			例	「ログ収集分析」、「統合ログ管理システム」
	事業継続		攻撃の成功による被害を早期に回復して、事業の継続性を維持する目的に実装される対策。	
			例	「冗長化」、「データバックアップ」

表 4-28 事業被害ベースのリスク分析シートの項目(3/3)

項目		説明
対策レベル	攻撃ステップ	当該攻撃ステップにおいて、想定した攻撃が発生した場合に、現在行われている対策で防止できる可能性を判定する。詳細は 3.5 節を参照。
	攻撃ツリー	当該攻撃ツリー全体において、想定した一連の攻撃が発生した場合に、現在行われている対策で防止できる可能性を判定する。詳細は 3.5 節を参照。 本項目値の相対の値が、当該攻撃ツリーの脆弱性レベルとなる。
		例 「対策レベル＝1(対策なし)」 →「脆弱性レベル＝3(“高”)」
攻撃ツリー番号	攻撃ツリー番号	攻撃ツリーの通し番号(参照番号)
	構成ステップ (項番)	各攻撃ツリーを構成する攻撃ステップの番号(項番)のセット
		例 攻撃ツリー番号#1: 項番 1, 2, 3 攻撃ツリー番号#2: 項番 1, 2, 4 攻撃ツリー番号#3: 項番 1, 2, 5

【事業被害、攻撃ツリー、攻撃シナリオの関係】

事業被害ベースのリスク分析においては、冒頭に述べた手順に従い、事業被害を引き起こす攻撃シナリオを策定し、攻撃シナリオを実現する攻撃ツリーを構成して評価することで、リスク分析を実施する。図 4-10 に、事業被害と攻撃シナリオと攻撃ツリーの相関的な模式図を示す。本図を用いて、リスク分析の全体像を説明する。

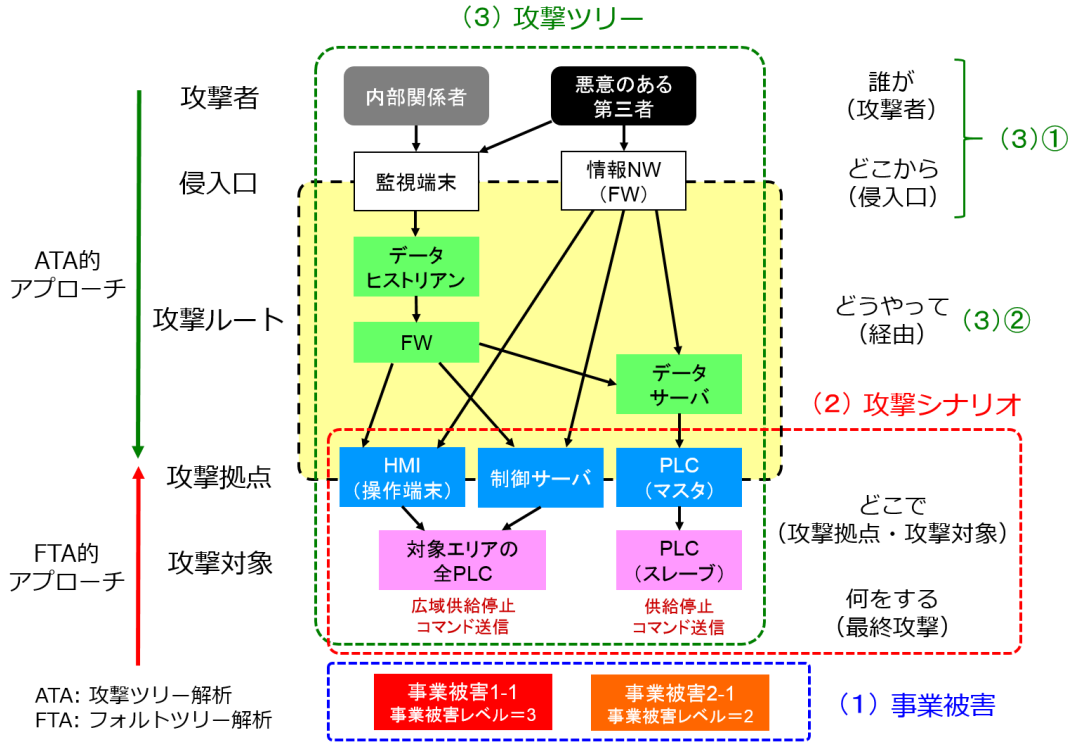


図 4-10 事業被害と攻撃シナリオと攻撃ツリーの模式図

事業被害は 3.3 節で述べた作業において定義される。その各事業被害に対して、まず、それがどの様な攻撃によって起こりうるのか（どの機器（攻撃拠点）からどの機器（攻撃対象）に対して何の攻撃をすることで事業被害の事象が発現するか）を明らかにする作業が攻撃シナリオの策定である。例えば、供給停止という事業被害は、供給を制御している機器（例えば PLC）に、制御サーバから供給停止コマンドを不正に送るという攻撃が一つの攻撃シナリオとなり、PLC が攻撃対象、制御サーバが攻撃拠点となる。この策定の考え方は、事業被害からみてそれを引き起こす直接的な要因をまず明確化することであり、FTA 的なアプローチとなる。

次に各攻撃シナリオに対して、攻撃ツリー（だれが、どこから、どの様に、どこで、何をする）を構成するが、これは、攻撃者視点で、攻撃拠点に向けたルートを明確化していく ATA 的なアプローチとなる。

【リスク分析の工数削減の有効性】

事業被害ベースのリスク分析では、対象とする全ての事業被害に対して、全ての攻撃シナリオを構成し、それらの攻撃ツリーを構成して分析することが望ましい。しかし現実的にはシステムの複雑さによっては、様々な攻撃シナリオや攻撃ルートが想定され、分析の工数が膨大となることが懸念される。限られた工数の制約の下、その回避策として分析の範囲の特定（絞り込み）を検討することが必要となるが、事業被害 → 攻撃シナリオ → 攻撃ツリーの流れにそって、以下の絞込みが効果的である。（(1)～(3)の対象箇所を、図 4-10 の右側に記載）

（1）事業被害の絞り込み（4.2.1 項参照）

事業被害レベルが高く最も回避したい事業被害に評価を特定する。

（2）攻撃シナリオの絞り込み（4.2.1 項参照）

事業被害を生じうる攻撃シナリオは明確化（把握）した上で、発生する可能性の高い攻撃シナリオを優先して分析する。

（3）攻撃ツリーの絞り込み（4.2.2 項参照）

攻撃の上流となる攻撃者と侵入口を明確化（把握）した上で、以下を行う。

① 脅威レベルの高い攻撃者と侵入口に特定して、攻撃ツリーを策定する。

② 途中の経由ルートは、起こりやすそうなルートに特定して、攻撃ツリーを策定する。

絞り込みを考慮しながら攻撃シナリオ、攻撃ツリーを策定する過程で、留意すべきことは以下である：

- **攻撃者、侵入口を全て明確化しておく。**
  攻撃の最上流である、想定される攻撃者、侵入口を全て把握しておくことは、攻撃ルートを検討する上で重要である。また、それらは、攻撃ツリーの一部としてではなく、それ自体の脅威レベルや脆弱性を（資産ベースのリスク分析の結果を活用することで）単体で評価することも可能である。
- **事業被害の攻撃シナリオは全て明確化しておく。**
  攻撃シナリオ自体は全て明確化し、攻撃ツリーを作成する対象を脅威レベルから選択することが重要である。リスク分析の対象外となった攻撃シナリオは脅威レベルや脆弱性をそれ単体（仮に攻撃拠点に攻撃者が到達した前提でそのパスだけ）で評価することも可能である。
- **絞り込みで評価対象から外した攻撃シナリオ、攻撃者／侵入口は把握しておく。**
  リスク分析は1回で終わるわけではないので、次回のリスク分析や、新たな脅威やインシデント事例が明らかになった場合には、評価対象から外したものを見直すことが重要である。

【追加調査の発生の可能性】

次項から、具体的な「事業被害ベースのリスク分析シート」の策定手順を、具体的に説明する。評価対象システム(3 章に示したモデルシステム)に対して、3.1 節で準備したシステム構成図(図 3-6)、資産一覧(表 3-6)、データフロー図(図 3-11)等を元(前提)に、攻撃シナリオや攻撃ツリーを検討、策定していくが、そのプロセスの中で不足する情報が様々出てくることが想定される。また、攻撃シナリオや攻撃ツリーを絞り込む上で、攻撃の成立の可能性や事業被害の範囲とレベルを確認する情報等の追加の調査が必要となってくる。そのフローのイメージを図 4-11 に示す。

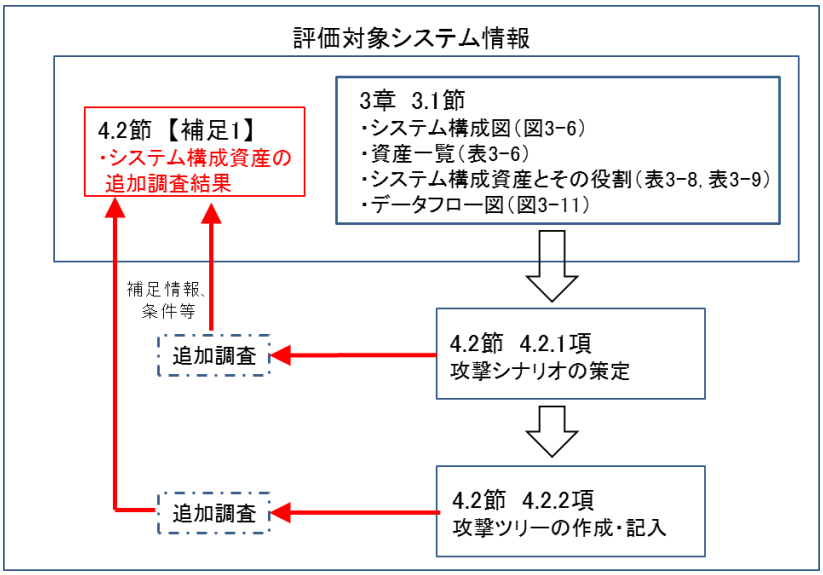


図 4-11 攻撃シナリオ・ツリー作成の流れ(追加調査の位置付け)

この追加調査で必要となるのは、以下の様な情報群である:

- 個々の機器の仕様や機能の詳細(特に攻撃での悪用や事業被害をもたらしうる部分)
- 事業被害に結びつくコマンド種別とコマンド発行機能の有無
- 保有する重要データの有無や内容、及びその改ざん等による操業への影響
- サーバが影響を及ぼす制御機器の範囲
- 手動操作等による代替運用手段の有無
- 業務の運用管理上の制約(操作者や運用者の制限等)
- 物理セキュリティ上の環境

これらの情報は、予め全て用意しておくことは困難であるので、分析の検討が進む中で、必要に応じてより詳細な調査を実施することによって、拡充していくことが必要となる。このプロセスは、保護対象である資産の状況(前提条件)をより深く理解する上で、非常に重要となる。次項以降の分

析を進める上で得られた情報の一覧と事項を、本節の末尾に**【補足 1】システム構成資産の追加調査結果**として示す。この中で、黒字の箇所は、3.1 節の作業で明らかになった部分で、赤字の箇所がリスク分析を進める中で、追加的に調査して明らかになった情報を示している。これらの情報を評価対象システムの条件として、攻撃シナリオ策定や攻撃ツリー作成の各箇所での考察や判定にどの様に活用されるかを引用して説明していく。引用の際には、当該箇所の後ろに補足 1 に示した追加情報の参照番号を記す（例：[補足 1:#8]等）。

4.2.1. 攻撃シナリオの策定

事業被害ベースのリスク分析では、まず、攻撃シナリオの策定を行う。回避したい事業被害を実際に引き起こす可能性のある最終攻撃（コマンドの発行、データ改ざん・破壊、情報窃取等）は何か、それらの攻撃が行われるシステムや機器はどこか（攻撃拠点・攻撃対象）を洗い出し、具体的な攻撃シナリオを策定する。

通常は 1 つの事業被害に対して複数の攻撃シナリオが存在すると考えられる。例えば、電力、ガス、水道等の「広域供給停止」という事業被害の場合、攻撃者によって既存の供給停止機能（送電停止操作、ガスの供給停止操作、送水停止操作等）を利用されることにより、広域に供給が停止する可能性（シナリオ）が考えられる。他には、操業に影響を及ぼす重要なデータやソフトウェアを改ざんされることにより、緊急対応（オペレータによる手動での設備・機器停止や、安全機構の発動による設備・機器の自動停止）を誘発され、広域に供給が停止する可能性（シナリオ）等も考えられる。

各事業被害について、FTA 的なアプローチで事業被害を引き起こす可能性がある機能や要件から攻撃シナリオを全て洗い出していくが、サイバー攻撃に対するリスク分析であることを踏まえ、物理的な攻撃によって設備や機器が破壊される様な攻撃シナリオは含めない。また、現実に発生したセキュリティインシデント事例等を参考にすることも有用である。

表 4-29 に、モデルシステムに基づき、表 3-19 の事業被害の定義例から事業被害を「広域での○○供給停止」とした場合の攻撃シナリオの策定例を示す。

表 4-29 攻撃シナリオの策定例(1)

項番	事業被害	攻撃シナリオ	
1	広域での〇〇供給停止	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。
			● 攻撃者が、HMI(操作端末)から広域供給停止操作を実行する(広域供給停止コマンドを不正送信する)。その結果、広域に及ぶ供給が停止する。[補足 1:#8]
			● 攻撃者が、制御サーバから広域供給停止操作を実行する(広域供給停止コマンドを不正送信する)。その結果、広域に及ぶ供給が停止する。[補足 1:#11]
			● 攻撃者が、PLC(マスター)から PLC(スレーブ)に、供給停止コマンドを不正送信する。その結果、広域に及ぶ供給が停止する。[補足 1:#22, #23]
			・ ・
		1-2	システム・機器上の重要なデータやソフトウェアの改ざんにより、システム・機器の誤操作/システム障害が発生し、広域に及ぶ供給が停止する。
			・ ・ ・
		1-3	重要なシステム・機器の停止・破壊により、広域に及ぶ供給が停止する。
			・ ・ ・

実際に事業者のシステムについて検討する際は、攻撃に悪用される可能性のある機能やデータの具体的な名称を明記することを推奨する。

攻撃シナリオのまとめ方としては、攻撃シナリオを「どこで」(攻撃拠点・攻撃対象)、「何をする」(最終攻撃)で整理した形式でまとめておくと、後で攻撃ツリーを作成する際に作業しやすい。表 4-30 に、攻撃拠点・攻撃対象・最終攻撃を整理した形で表 4-29 の攻撃シナリオを策定した例を示す。

表 4-30 攻撃シナリオの策定例(2): 攻撃拠点・攻撃対象・最終攻撃で整理した記載例

<table>
<tr><th>項番</th><th>事業被害</th><th colspan="4">攻撃シナリオ</th></tr>
<tr><td rowspan="9">1</td><td rowspan="9">広域での〇〇供給停止</td><td rowspan="3">1-1</td><td colspan="3">コマンドの不正送信により、広域に及ぶ供給が停止する。</td></tr>
<tr><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td></tr>
<tr><td>HMI
(操作端末)
(※)
制御サーバ</td><td>対象エリアの
PLC</td><td>攻撃者が、HMI(操作端末)／制御サーバから広域供給停止操作を実行する(広域供給停止コマンドを不正送信する)。その結果、広域に及ぶ供給が停止する。[補足 1: #8, #11]</td></tr>
<tr><td>PLC
(マスター)</td><td>PLC
(スレーブ)</td><td>攻撃者が、PLC(マスター)から PLC(スレーブ)に、供給停止コマンドを不正送信する。その結果、広域に及ぶ供給が停止する。[補足 1:#22, #23]</td></tr>
<tr><td colspan="3">・
・</td></tr>
<tr><td rowspan="3">1-2</td><td colspan="3">システム・機器上の重要なデータやソフトウェアの改ざんにより、システム・機器の誤操作／システム障害が発生し、広域に及ぶ供給が停止する。</td></tr>
<tr><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td></tr>
<tr><td colspan="3">・
・
・</td></tr>
<tr><td rowspan="3">1-3</td><td colspan="3">重要なシステム・機器の停止・破壊により、広域に及ぶ供給が停止する。</td></tr>
<tr><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td></tr>
<tr><td colspan="3">・
・
・</td></tr>
</table>

※HMI(操作端末)からの操作は、実際には制御サーバ経由で実行される。

以下に、攻撃シナリオを検討するにあたってのその他の留意事項を記す。

① 攻撃シナリオの区分

検討例では攻撃シナリオを、他の機器へのコマンド発行による攻撃か（表 4-29／表 4-30 の攻撃シナリオ 1-1）、機器自身のデータの改ざんやシャットダウンによる攻撃か（同表の攻撃シナリオ 1-2、1-3）で区分しているが、この区分は事業者にとって実施しやすい・わかりやすい区分で括ることを推奨する。事業者のシステム仕様・構成によっては、システムごと、設備ごと、機器ごと等の区分が実施しやすい・分かりやすい可能性もある。まずは、事業被害ごとに攻撃シナリオを洗い出し、整理しやすい区分があれば、括ることを検討するとよい。

② 攻撃シナリオの数や詳細度

攻撃シナリオの数や詳細度は、システムの仕様・構成等によって、表 4-29／表 4-30 に示した検討例とは大きく異なってくると推測される。事業被害を引き起こす可能性のある攻撃シナリオはできるだけ具体化し、漏れなく洗い出すことが望ましいが、攻撃シナリオを詳細に書き過ぎると、後で攻撃ツリーを作成する際に攻撃ツリーが膨大化する懸念がある。

状況に応じて、攻撃手法や結果的に起きる事象が同じ様な攻撃シナリオ等、まとめられる攻撃シナリオはまとめたり、リスク分析対象を絞り込んだりしていくことを考慮する必要がある。以下に、攻撃シナリオの絞り込みの例を示す。

- **事業被害レベルによる絞り込み**
  攻撃シナリオを策定するのは、事業被害のうち事業被害レベルが高いもの（例えば「3 のみ」、「3 と 2 のみ」）とする。

- **攻撃シナリオによる絞り込み**
  システム仕様・構成や対策状況等を考慮に入れ、事業被害が発生する可能性が高いと考えられる攻撃シナリオを優先する。

4.2.2. 攻撃ツリーの作成・記入

本項では、前項で洗い出した攻撃シナリオを実現する攻撃ツリーを作成する手順を記す。

本ガイドでは、**「誰が」**（攻撃者は誰か）、**「どこから」**（侵入口となり得るのはどこか）、**「どうやって」**（侵入口から攻撃拠点までの経由）、**「どこで」**（攻撃拠点・攻撃対象）、**「何をする」**（最終攻撃）の観点から、攻撃ルートを検討し、攻撃ツリーを作成していくアプローチを紹介する。

図 4-12 に、攻撃ツリーの作成の流れを示す。

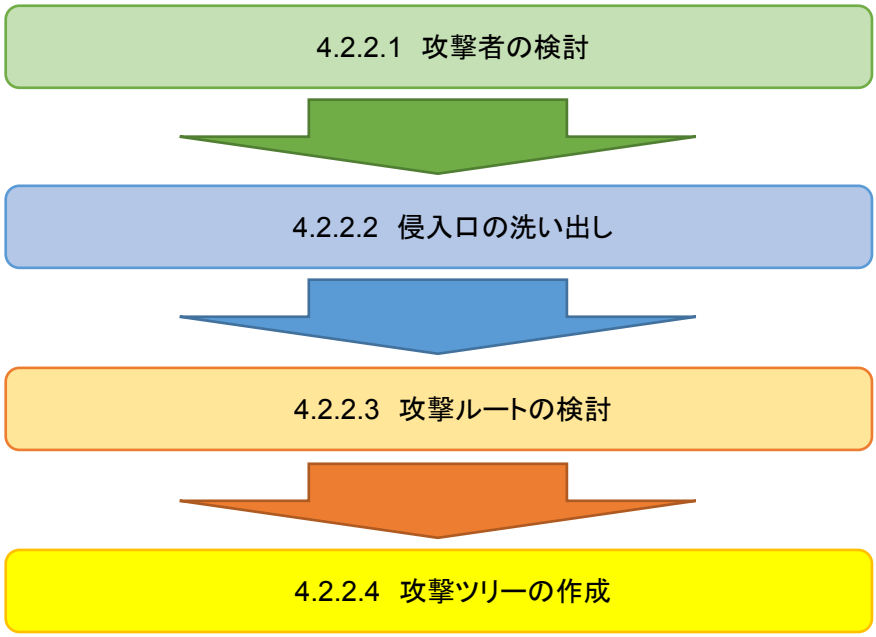


図 4-12 攻撃ツリー作成の流れ

各項において検討例を表や図で示しているが、事業者が実際に行う場合には、例示している表や図の形式にこだわらず、加筆・修正したり、あるいは事業者にとって実施しやすい・まとめやすい形式で行ったりして構わない。

以降に、各項における手順を説明する。

4.2.2.1. 攻撃者の検討

本項では、リスク分析において想定する攻撃者を検討する。

攻撃者は、一般的に「悪意のある第三者」、「内部関係者」（故意／過失）に大別される。通常のリスク分析では攻撃者を特に明示せず、「悪意のある第三者」と想定することが多い。但し、「悪意のある第三者」と「内部関係者」では、制御システムに関する知識やアクセス権の有無等の点で攻撃条件が大きく異なることから、理想としては内部関係者に対しても行うことが望ましい。

しかし、リスク分析対象の攻撃者が増えれば分析作業も増えるため、事業者のシステム仕様・構成、業務フロー・運用、物理的対策、内部不正対策等を考慮し、事業者の実状に応じて攻撃者を選定することを推奨する。

例えば、事業者の制御システムが制御ネットワーク以外のネットワークとは一切接続していないのであれば、「悪意のある第三者」によるそれ以外のネットワーク経由の攻撃を考慮する意義は小さいため、リスク分析から除外することが考えられる。または、事業者の敷地内にある制御システム機器の物理的対策が堅固であり、「悪意のある第三者」がサーバ室や計器室に物理的にアクセスすることが現実的に困難なのであれば、分析から除外すること等が考えられる[補足 1:#38～#40]。

一方で、制御システムが制御ネットワーク以外のネットワークにつながっているのであれば、「悪意のある第三者」によるそれ以外のネットワーク経由の攻撃を考慮することが望まれる。また、悪意ある内部関係者の出現性は低いと考えられるとしても、モバイル端末や USB メモリを制御システム機器に接続して作業する業務フローが存在するのであれば、内部関係者の過失による制御システム機器への物理アクセスによる攻撃は、リスク分析の対象とすること等が考えられる。

表 4-31 に、モデルシステムを基に、脅威レベル（発現可能性）から分析対象とする攻撃者を検討した例を示す。

表 4-31 攻撃者の検討例

<table>
<tr><th colspan="2" rowspan="3">攻撃場所</th><th colspan="3">攻撃者</th></tr>
<tr><th>悪意のある</th><th colspan="2">内部関係者</th></tr>
<tr><th>第三者</th><th>過失</th><th>故意</th></tr>
<tr><td rowspan="3">敷地内</td><td>制御 NW 以外の NW から制御 NW へのアクセス
（情報 NW から制御 NW への不正侵入、マルウェアへの感染等）</td><td>○</td><td>×
業務フローなし
[補足 1:#2]</td><td rowspan="4">×
内部不正対策あり
[補足 1:#41]</td></tr>
<tr><td>保守回線から制御 NW へのアクセス
（保守ベンダーにあるリモート保守端末からの不正侵入、マルウェア感染等）</td><td colspan="2">×
保守回線なし
（図 3-6）</td></tr>
<tr><td>制御システム機器への物理アクセス
（事業者敷地内にある制御システム機器への物理アクセスによる不正操作、モバイル機器・外部記憶媒体によるマルウェア感染等）</td><td>×
現実的に困難
[補足 1:#38～#40]</td><td>○</td></tr>
<tr><td rowspan="2">フィールド（敷地外）</td><td>通信回線・通信機器から制御 NW へのアクセス
（フィールドネットワークへの不正アクセスによる通信データの改ざん、機器なりすまし等）</td><td colspan="2">×
PLC 回線は専用線
（表 3-6）</td></tr>
<tr><td>制御システム機器への物理アクセス
（事業者敷地外にある制御システム機器への物理アクセスによる不正操作、モバイル機器・外部記憶媒体によるマルウェア感染等）</td><td>○</td><td>○</td></tr>
</table>

○：リスク分析対象　×：リスク分析対象外

4.2.2.2. 侵入口の洗い出し

本項では、制御ネットワークへの攻撃にあたって、侵入口となり得るネットワークや機器をシステム構成図から全て洗い出す。

(1)侵入口の考え方

侵入口は、ネットワーク経由の攻撃の侵入口と、物理アクセスによる攻撃の侵入口が考えられる。本ガイドでは以下の様に分類する。

- **ネットワーク経由の攻撃と侵入口**
  制御ネットワークにつながる制御ネットワーク以外のネットワークから、制御システムにアクセスしてくる攻撃の侵入口。制御ネットワークに接続している制御ネットワーク以外のネットワーク上にあって制御ネットワーク内の機器と通信を行う機器等からアクセスしてくるケース、制御ネットワークと制御ネットワーク以外のネットワークとの外接点に不正アクセスしてくるケース等が考えられる。

  具体的には、情報ネットワーク、バックアップサイトとつながる通信回線、保守回線、情報ネットワーク上にある監視端末や操業計画等の策定のため操業データにアクセスする事務PC、フィールドネットワーク上の制御機器、ベンダーにあるリモート保守端末、制御ネットワークの境界を形成する機器(ファイアウォール、アプリケーションサーバ、リモートアクセスサーバ等)が考えられる。

- **物理アクセスによる侵入口**
  制御ネットワーク(通信回線・機器)や制御システム機器に物理的にアクセスし、直接操作したり、不正な機器や媒体を接続したりして行う攻撃の侵入口。制御ネットワーク(通信回線・機器)及び制御システム機器等が考えられる。

  具体的には、制御ネットワークを構成する通信機器、情報ネットワークにある監視端末や事務 PC、HMI(操作端末)、制御サーバ、フィールドにある PLC 等が考えられる。

表 4-32 に、モデルシステムにおいて侵入口となり得る、全てのネットワーク・機器を示す。

表 4-32 侵入口となり得るネットワーク・機器

侵入口		所在
ネットワーク経由の攻撃の侵入口		
	監視端末	－
	情報ネットワーク（ファイアウォール）	－
	フィールドネットワーク（通信回線・機器）	－
物理アクセスによる攻撃の侵入口		
	監視端末	執務室
	ファイアウォール	サーバ室
	データヒストリアン	サーバ室
	データサーバ	サーバ室
	制御サーバ	サーバ室
	HMI（操作端末）	計器室
	PLC	フィールド（敷地内）
	PLC（マスター）	フィールド（敷地内）
	制御ネットワーク（通信回線・機器）	フィールド（敷地内）
	PLC（スレーブ）	フィールド（敷地外）
	フィールドネットワーク（通信回線・機器）	フィールド（敷地外）

※情報ネットワーク、パッチサーバ、EWS、保守 PC は 3.1 節で今回分析の対象外となっているため除外

（2）侵入口の絞り込み

表 4-32 の様に、侵入口となりうるネットワークや機器は全て洗い出すことが必須となるが、まとめることが可能なものや、脅威レベル（攻撃が発生する可能性）によって絞り込むことが可能なものもあると考えられる。以下に、侵入口の統合と除外の考え方を示す。

① 同種／同用途のネットワークや機器の統合

資産ベースのリスク分析において、資産の重要度や機能等によって機器の統合（グループ化）が実施されているが、そのままで問題ないか、更にまとめることができる機器があるか、見直しを行う。見直しの結果、評価上重要な相違がある場合は、まとめずに別の侵入口とするか、まとめた場合は後の手順において実施しているセキュリティ対策を記入・評価する際に、まとめた機器の中で最もセキュリティレベルの低い機器の対策を記入・評価する。

例えば、資産ベースのリスク分析では、モデルシステムの PLC と PLC（マスター）は同じグループ 11 としてまとめられている。侵入口として再考した場合、PLC は直接侵入できても不正に制御できるのは当該 PLC（につながるフィールド機器）のみであり、広範な攻撃のためにはそこから上位システム（HMI（操作端末）、制御サーバ、データサーバ）に侵入する必要がある。上位システムとの接続方法や対策が PLC（マスター）と同じであれば、侵入口としても PLC と PLC（マスター）とまとめたままで、評価上カバーできると考えられる。

② 攻撃の発生可能性に基づく除外

攻撃者の視点で見た場合に、攻撃のメリットが低いと考えられる様なネットワークや機器は、除外することが考えられる。例えば、モデルシステムではデータヒストリアン、制御サーバ、データサーバは全て同じサーバ室にあり、物理的なアクセス条件は同じである。この場合、悪用性の高さから制御サーバ、データサーバに直接侵入する方が遥かにメリットが大きいため[補足 1:#11～#13, #16, #17]、データヒストリアンは物理的アクセスによる攻撃の侵入口から除外することも考えられる。

但し、その様な機器がその先の攻撃に有用な内部情報を保有している、または他の機器に比べてセキュリティ対策が弱く侵入が容易である等、攻撃の対象となる懸念がある場合は評価対象とすることが望ましい。

表 4-33 に、モデルシステムにおける侵入口の絞り込みの検討例を示す。この検討例では、侵入口の統合と除外の考え方①②からデータヒストリアンと PLC を、また、表 4-31 の攻撃者の検討例の結果からフィールドネットワーク（通信回線・機器）を外している。

表 4-33 侵入口の検討例

侵入口		所在
ネットワーク攻撃の侵入口		
	監視端末	－
	情報ネットワーク（ファイアウォール）	－
物理アクセスによる攻撃の侵入口		
	監視端末	執務室
	ファイアウォール	サーバ室
	データサーバ	サーバ室
	制御サーバ	サーバ室
	HMI（操作端末）	計器室
	PLC（マスター）	フィールド（敷地内）
	制御ネットワーク（通信回線・機器）	フィールド（敷地内）
	PLC（スレーブ）	フィールド（敷地外）

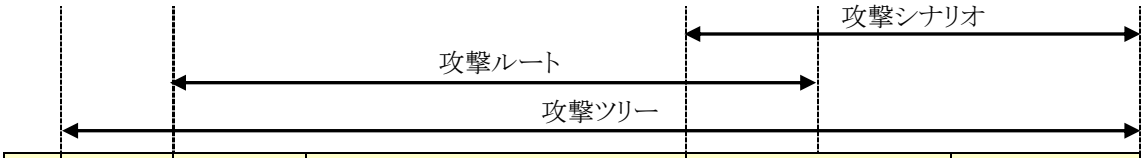
4.2.2.3. 攻撃ルートの検討

攻撃者と侵入口が検討できたら、4.2.1 項の手順で洗い出した攻撃シナリオと合わせ、「誰が」「どこから」「どうやって」「どこで」「何をする」の観点で攻撃ルートを検討する。

（1）攻撃ルートの検討

攻撃ルートは、攻撃者、侵入口、攻撃シナリオを整理し、最終的に攻撃ツリーを作成する攻撃ルートを全て洗い出す。攻撃ルートを検討する際のフォーマットの例を、表 4-34 に示す。

表 4-34 攻撃ルートの検討フォーマット



#	誰が	どこから	どうやって			どこで		何をする
	攻撃者	侵入口	経由 1	経由 2	経由 3	攻撃拠点	攻撃対象	最終攻撃

以降では、表 4-30 の攻撃シナリオの検討例から、攻撃シナリオ「1-1」（コマンドの不正送信により、広域に及ぶ供給が停止する）を例に、攻撃ルートの検討方法を説明する。

① 攻撃拠点・攻撃対象のシステム構成図上の所在の確認

まずは、攻撃ルートを洗い出したい攻撃シナリオの、「どこで」（攻撃拠点・攻撃対象）が、システム構成図上どこにあるかを確認する。

図 4-13 は、攻撃シナリオ 1-1 の「どこで」（攻撃拠点・攻撃対象）と、「何をする」（最終攻撃）を示している。広域供給停止につながるコマンドの送信が可能な機器は、「HMI（操作端末）」（広域供給停止コマンドの送信）、「制御サーバ」（広域供給停止コマンドの送信）、「PLC（マスター）」（配下の多数 PLC（スレーブ）への供給停止コマンドの送信）であるため[補足 1:#8, #11, #22, #23]、攻撃者はこれらのどれかの機器に侵入し、攻撃を行うことが考えられる。

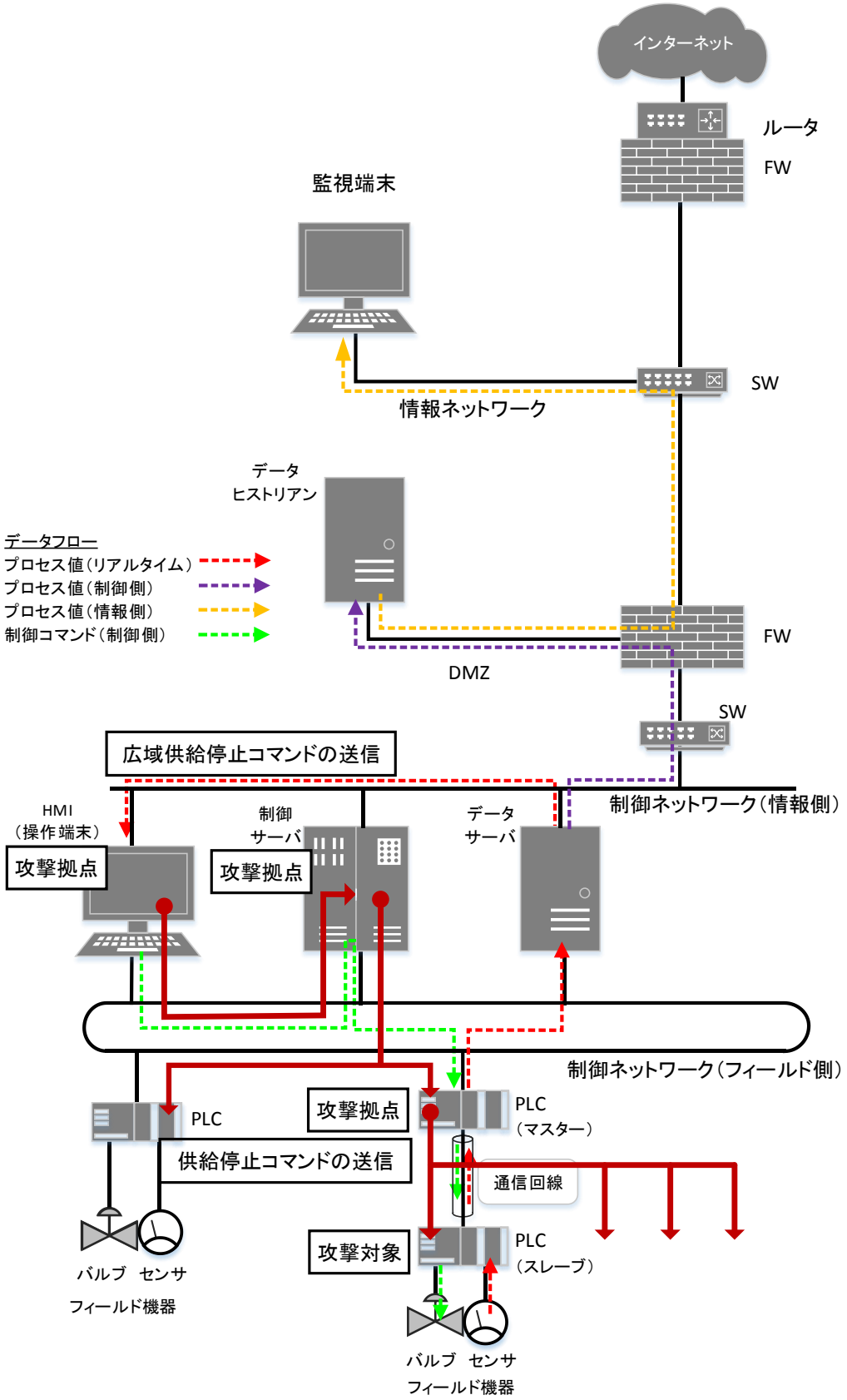


図 4-13 広域供給停止につながるコマンドを送信する機器

攻撃ルートの検討フォーマットに上記情報を埋めたものを、表 4-35 に示す。

表 4-35 攻撃シナリオ 1-1 の攻撃ルート（どこで、何をする）

#	誰が	どこから	どうやって			どこで		何をする
	攻撃者	侵入口	経由 1	経由 2	経由 3	攻撃拠点	攻撃対象	最終攻撃
						HMI	対象エリアの PLC	広域供給停止コマンド送信
						制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
						PLC-M（※1）	PLC-S 群（※2）	供給停止コマンド送信

※1 PLC-M：PLC（マスター）、 ※2 PLC-S：PLC（スレーブ）

② 侵入口から攻撃拠点までの攻撃ルートの洗い出し

次に、「どこから」、「どうやって」を、システム構成図から洗い出す。

ネットワーク経由の攻撃の攻撃ルートは、システム仕様やセキュリティ対策によって正規にはアクセスできないルートであっても、ネットワーク接続が存在していれば脆弱性の存在や設定不備等の何らかの方法によって突破される可能性があるため、ルートとして洗い出す。

物理アクセスによる攻撃の侵入口は、攻撃拠点への物理アクセス以外に、攻撃拠点がある制御ネットワーク以外のネットワーク上の機器や攻撃拠点と同じネットワーク上にある機器に物理アクセスし、そこから攻撃拠点にアクセスしてくることも考えられる。しかし、制御ネットワーク上の機器や制御ネットワーク以外のネットワーク上の機器に物理アクセスしての攻撃の攻撃ルートは、攻撃拠点に向かう攻撃ルートとしては、ネットワーク経由の攻撃の攻撃ルートと重複して評価される可能性がある。従って、事業被害を回避するという観点では、物理アクセスによる攻撃の侵入口は攻撃拠点に限ることも考えられる(**【補足 2】**参照)。

図 4-14に、攻撃シナリオ1-1を例に、ネットワーク経由の攻撃の侵入口(①～③)と攻撃ルート、物理アクセスによる攻撃の侵入口(④～⑥)と攻撃ルートを示す。「表 4-33 侵入口の検討例」から、ネットワーク経由で制御ネットワークに侵入する攻撃ルートは、以下の 3 通りが考えられる。

- 情報ネットワーク上の監視端末を侵入口として、データヒストリアンを経由し、ファイアウォールを突破する(①)
- 情報ネットワーク上の監視端末を侵入口として、ファイアウォールを突破する(②)
- 情報ネットワークから、ファイアウォールを突破する(③)

また、物理アクセスによる侵入口は、攻撃拠点に絞り、以下の 3 通りが考えられる。

- HMI(④)
- 制御サーバ(⑤)
- PLC(マスター)(⑥)

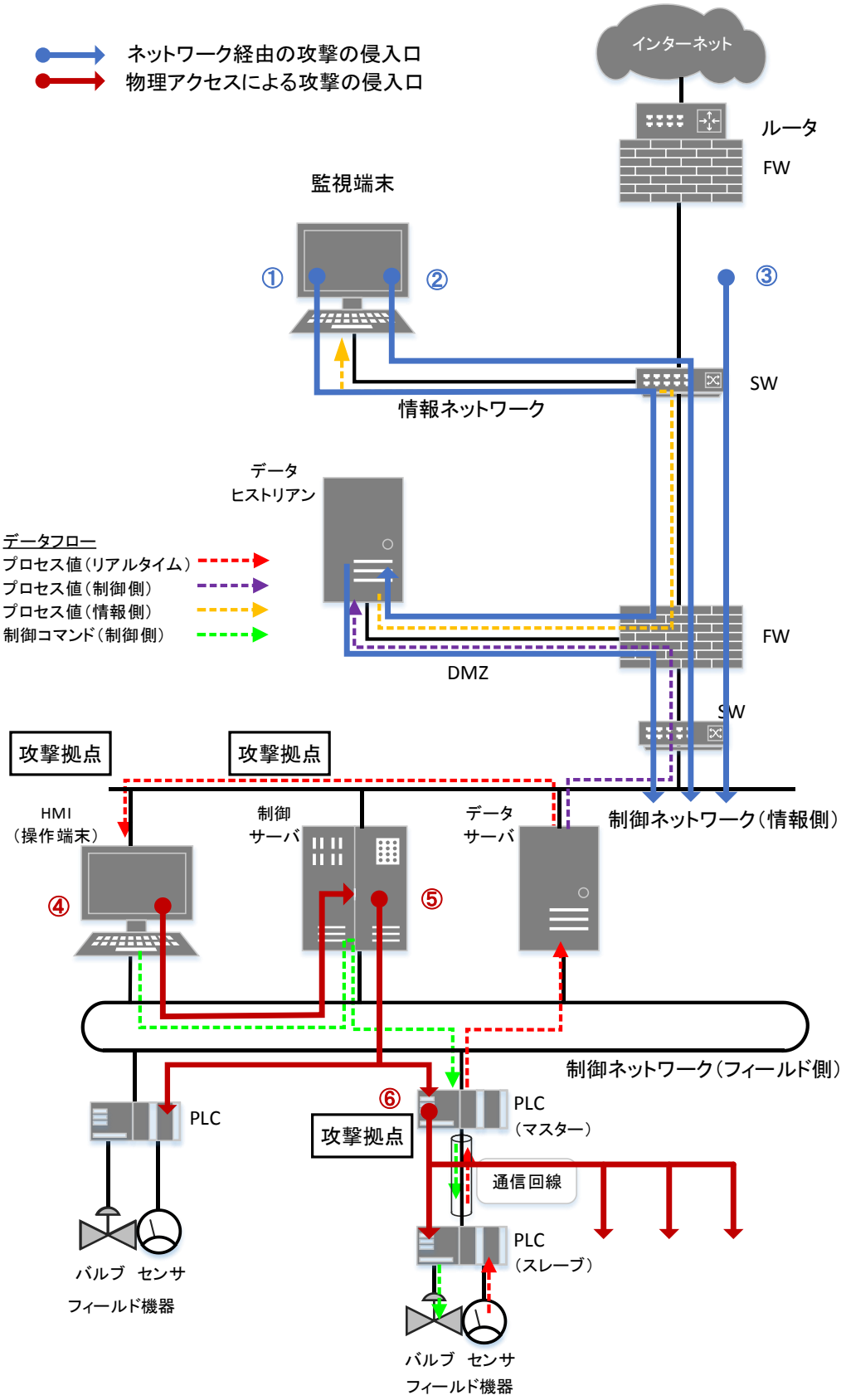


図 4-14 攻撃シナリオ 1-1 の侵入口

攻撃ルートは、これらの侵入口（6 パターン）と表 4-35 の攻撃拠点（3 パターン）との組み合わせを全て洗い出していく。例えば、図 4-14 の攻撃ルート①（情報ネットワーク上の監視端末を侵入口として、データヒストリアン、ファイアウォールを経由して制御ネットワークに侵入し、HMI（操作端末）または制御サーバに到達する場合）では、HMI（操作端末）と制御サーバは制御ネットワーク（情報側）にあるため、これ以上どこかを経由する必要はない。表 4-35 の攻撃拠点が HMI 及び制御サーバの行に、攻撃ルート①から侵入する場合の侵入口と経路情報を追記した例を、表 4-36 に示す。

表 4-36 攻撃ルート①の検討例（1）（攻撃ルート①→HMI／制御サーバ）

#	誰が	どこから	どうやって			どこで		何をする
	攻撃者	侵入口	経由 1	経由 2	経由 3	攻撃拠点	攻撃対象	最終攻撃
		監視端末	データヒストリアン	FW	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
		監視端末	データヒストリアン	FW	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信

一方、攻撃ルート①から制御ネットワークに侵入し、PLC（マスター）に到達するには、PLC（マスター）が制御ネットワーク（フィールド側）にあるため HMI（操作端末）、制御サーバ、データサーバのいずれかを経由する必要がある表 4-35 の攻撃拠点が PLC（マスター）の行に、攻撃ルート①から侵入する場合の侵入口と経路情報を追記した例を、表 4-37 に示す。

表 4-37 攻撃ルート①の検討例（2）（攻撃ルート①→PLC（マスター））

#	誰が	どこから	どうやって			どこで		何をする
	攻撃者	侵入口	経由 1	経由 2	経由 3	攻撃拠点	攻撃対象	最終攻撃
		監視端末	データヒストリアン	FW	HMI	PLC-M	PLC-S 群	供給停止コマンド送信
		監視端末	データヒストリアン	FW	制御サーバ	PLC-M	PLC-S 群	供給停止コマンド送信
		監視端末	データヒストリアン	FW	データサーバ	PLC-M	PLC-S 群	供給停止コマンド送信

同様にして、侵入口から攻撃拠点・攻撃対象に至る全ての攻撃ルートを洗い出す。表 4-38 に、攻撃シナリオ 1-1 に対する全ての攻撃ルートを洗い出した結果を示す。

表 4-38 攻撃シナリオ 1-1 の攻撃ルートの検討例

#	誰が	どこから	どうやって			どこで		何をする
	攻撃者	侵入口	経由 1	経由 2	経由 3	攻撃拠点	攻撃対象	最終攻撃
ネットワーク経由の攻撃								
1		監視端末	データヒストリアン	FW	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
2		監視端末	データヒストリアン	FW	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
3		監視端末	情報 NW（FW）	－	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
4		監視端末	情報 NW（FW）	－	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
5		情報 NW（FW）	－	－	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
6		情報 NW（FW）	－	－	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
7		監視端末	データヒストリアン	FW	HMI	PLC-M	PLC-S 群	供給停止コマンド送信
8		監視端末	データヒストリアン	FW	制御サーバ	PLC-M	PLC-S 群	供給停止コマンド送信
9		監視端末	データヒストリアン	FW	データサーバ	PLC-M	PLC-S 群	供給停止コマンド送信
10		監視端末	情報 NW（FW）	HMI	－	PLC-M	PLC-S 群	供給停止コマンド送信
11		監視端末	情報 NW（FW）	制御サーバ	－	PLC-M	PLC-S 群	供給停止コマンド送信
12		監視端末	情報 NW（FW）	データサーバ	－	PLC-M	PLC-S 群	供給停止コマンド送信
13		情報 NW（FW）	HMI	－	－	PLC-M	PLC-S 群	供給停止コマンド送信
14		情報 NW（FW）	制御サーバ	－	－	PLC-M	PLC-S 群	供給停止コマンド送信
15		情報 NW（FW）	データサーバ	－	－	PLC-M	PLC-S 群	供給停止コマンド送信
物理アクセスによる攻撃								
16		HMI	－	－	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
17		制御サーバ	－	－	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
18		PLC-M	－	－	－	PLC-M	PLC-S 群	供給停止コマンド送信

（2）攻撃ルートの絞り込み

次に、洗い出した攻撃ルートについて、攻撃ツリーの作成を省くことが可能なルートの有無を検討し、攻撃ルートを絞り込んでいく。絞り込みの観点を以下に示す。

①　複数の攻撃ルートが途中で合流しているルート

結果的に他の攻撃ルートとルートが重複するため、除外してもリスク分析に漏れは生じないと考えられる場合、そのルートは除外することが考えられる。

例えば、図 4-15 に示す様に、攻撃ルート 3～6 は、全て情報ネットワークからファイアウォールを突破する必要があるため、攻撃ルート 3,4 または 5,6 のどちらかを実施することでカバーできる可能性がある。同様に、攻撃ルート 10～15 についても、全て情報ネットワークからファイアウォールを突破して HMI（操作端末）／制御サーバ／データサーバに侵入する必要があるため、攻撃ルート 10～12 または 13～15 のどちらかを実施することでカバーできる可能性がある。本節の検討例では攻撃ルート 3, 4 及び 10～12 を省き、攻撃ルート 5, 6 及び 13～15 を実施するものとする。

但し、この様なルートが除外できるかは、システムの実装に依る。本理由でルートの除外を検討する場合は、必ずシステムの仕様や実装を確認のうえ、判断することが必須となる。

例として、モデルシステムでは監視端末は“監視のみ”可能だが、もしこれが HMI（操作端末）と同じ様な端末で、“監視制御”（例えば、コマンドの送信や設定変更）が正規に可能な機器の場合、監視端末から制御サーバへファイアウォールを通過する正規の通信フローが存在することになり、攻撃ツリー3,4 と 5,6、10～12 と 13～15 では条件が異なるため、除外できない。

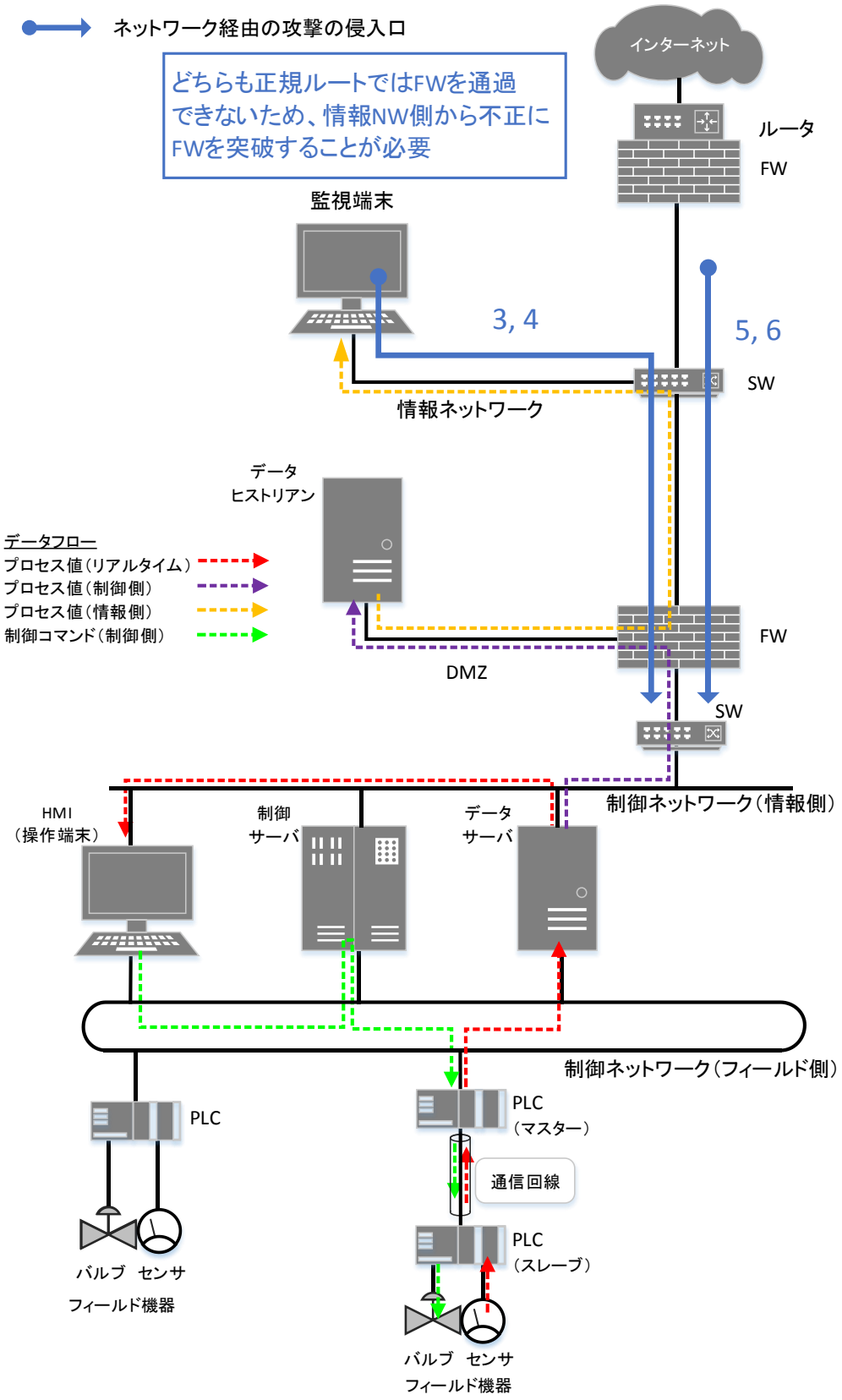


図 4-15 複数の攻撃ルートが途中で合流するケースの例（攻撃ルート 3,4 と 5,6）

② 侵入口から攻撃拠点となる機器までの「経由」にあたる機器で、当該攻撃ツリーの目的である最終攻撃が可能となり、攻撃が発生する可能性が低いルート

攻撃拠点に侵入する前に、同じ攻撃シナリオの実現が可能な別の攻撃拠点に侵入する必要がある場合には、そのルートは除外することが考えられる。

例えば、図 4-16 に示す様に、攻撃ルート 7, 8 は、情報ネットワーク上の監視端末からデータヒストリアンにアクセスし、ファイアウォールを突破して制御ネットワークに侵入し、HMI（操作端末）または制御サーバを経由して PLC（マスター）に侵入し、配下の多数の PLC（スレーブ）に供給停止コマンドを不正送信し、広域におよぶ供給停止を引き起こす攻撃ルートとなる。侵入口からの攻撃ルートを追うと、経由の HMI か制御サーバに侵入できた時点で広域供給停止コマンドの送信が可能であり、敢えて攻撃拠点の PLC（マスター）に侵入する必要はない。同様に、攻撃ルート 13, 14 についても、経由の HMI（操作端末）または制御サーバに侵入できた時点で攻撃が可能であり、敢えて攻撃拠点の PLC（マスター）に侵入する必要はない。従って、本節の検討例では、攻撃ルート 7, 8, 13, 14 は省くものとする。

表 4-38 の攻撃ルートの検討例に、攻撃ルートの絞り込みの考え方①②を反映した結果を、表 4-39 に示す。

【コラム】

攻撃ルートの絞り込み（補足）：
仕様上、攻撃が発生する可能性がない、または非常に低いルートの扱い

可能性のある攻撃ルートを全て洗い出していくと、ルートの重複等の観点では除外されないものの、システム仕様から攻撃が発生する可能性がない、または非常に低いルートが残る可能性がある。

例えば、フィールドにある機器を侵入口として、上位の制御システム機器へ侵入する攻撃ルートが洗い出された場合、仕様によってはフィールド機器からはごく限られたバイト数の決まったデータしか送信できず、上位機器への侵入や、上位機器をマルウェア感染させる様な攻撃が現実的に発生しないケースもあると考えられる。

その様な攻撃ルートは、ルートの重複等と同様に、理由を明記して攻撃ツリーの作成対象から除外するか、またはツリーは作成し、対策に理由を明記して対策レベル（攻撃を防止できる可能性）を「3」とすること等により対応することが考えられる。

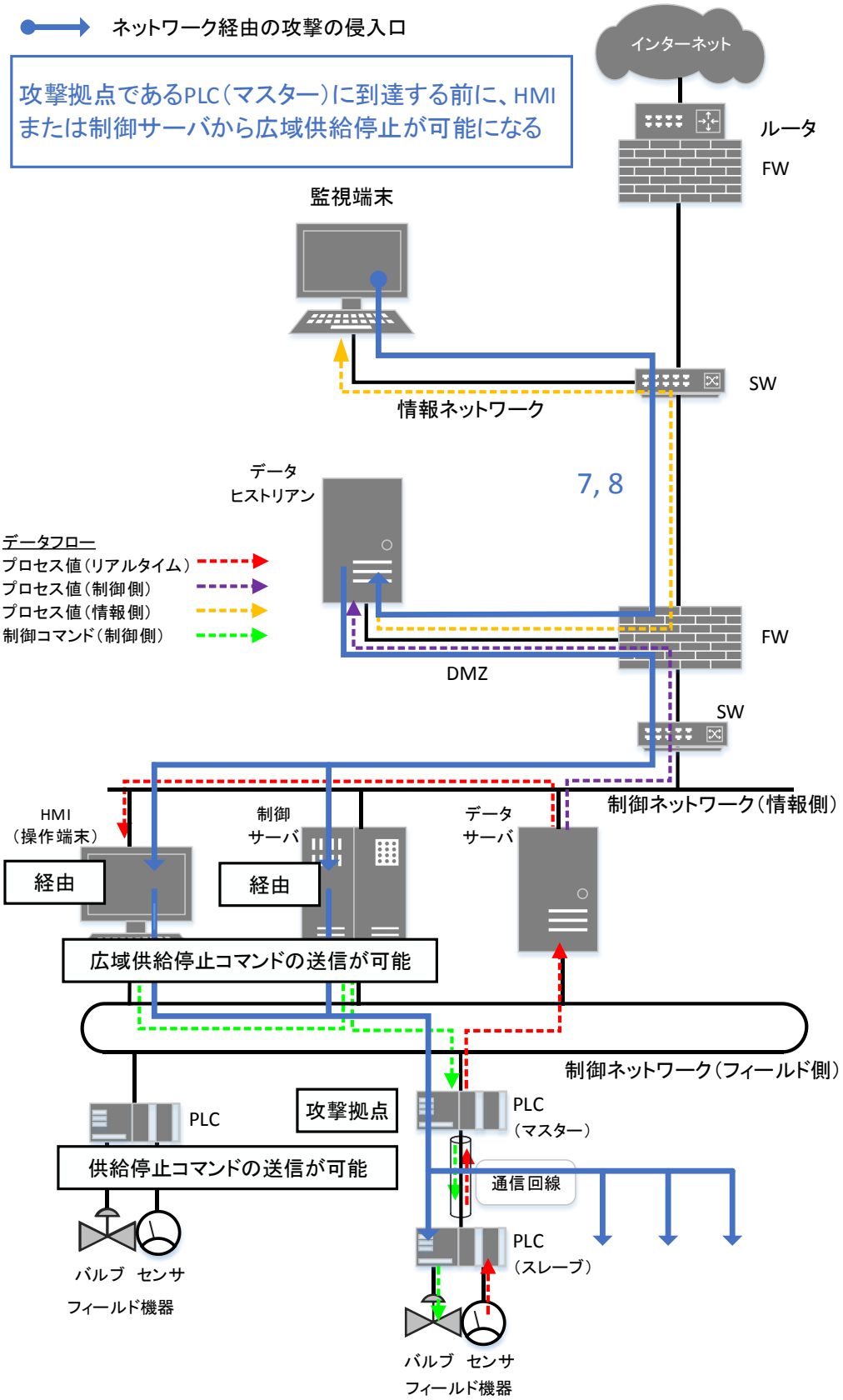


図 4-16 経路上の機器でも最終攻撃が可能なケース（攻撃ルート 7, 8）

表 4-39 攻撃シナリオ 1-1 の攻撃ルートの絞り込み例

#	誰が	どこから	どうやって			どこで		何をする
	攻撃者	侵入口	経由 1	経由 2	経由 3	攻撃拠点	攻撃対象	最終攻撃
ネットワーク経由の攻撃								
1		監視端末	データヒストリアン	FW	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
2		監視端末	データヒストリアン	FW	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
3		監視端末	情報 NW（FW）	－	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
4		監視端末	情報 NW（FW）	－	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
5		情報 NW（FW）	－	－	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
6		情報 NW（FW）	－	－	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
7		監視端末	データヒストリアン	FW	HMI	PLC-M	PLC-S 群	供給停止コマンド送信
8		監視端末	データヒストリアン	FW	制御サーバ	PLC-M	PLC-S 群	供給停止コマンド送信
9		監視端末	データヒストリアン	FW	データサーバ	PLC-M	PLC-S 群	供給停止コマンド送信
10		監視端末	情報 NW（FW）	HMI	－	PLC-M	PLC-S 群	供給停止コマンド送信
11		監視端末	情報 NW（FW）	制御サーバ	－	PLC-M	PLC-S 群	供給停止コマンド送信
12		監視端末	情報 NW（FW）	データサーバ	－	PLC-M	PLC-S 群	供給停止コマンド送信
13		情報 NW（FW）	HMI	－	－	PLC-M	PLC-S 群	供給停止コマンド送信
14		情報 NW（FW）	制御サーバ	－	－	PLC-M	PLC-S 群	供給停止コマンド送信
15		情報 NW（FW）	データサーバ	－	－	PLC-M	PLC-S 群	供給停止コマンド送信
物理アクセスによる攻撃								
16		HMI	－	－	－	HMI	対象エリアの PLC	広域供給停止コマンド送信
17		制御サーバ	－	－	－	制御サーバ	対象エリアの PLC	広域供給停止コマンド送信
18		PLC-M	－	－	－	PLC-M	PLC-S 群	供給停止コマンド送信

※グレーが、攻撃ルートの絞込みの考え方① 攻撃ルートの合流による除外、
水色が、攻撃ルートの絞込みの考え方② 経路上の機器で攻撃が可能になることによる除外

従って、本節の検討例では、攻撃ツリーに落とし込む攻撃ルートは、1, 2, 5, 6, 9, 15, 16, 17, 18（表 4-39 の白い行）となる。

図 4-17～図 4-22 は、これらの攻撃ルートをシステム構成図（図 3-6）上に図示したものである。表 4-40 に、各々の図番号と攻撃ルート番号及び攻撃ルートの説明との対応を示す。

表 4-40 攻撃ルートを示す図一覧

図番号	攻撃ルート番号	説明
図 4-17	1, 2	監視端末からデータヒストリアンを経由してファイアウォールを突破し、HMI／制御サーバに侵入して攻撃を実行
図 4-18	5, 6	情報ネットワークからFWを突破し、HMI／制御サーバに侵入して攻撃を実行
図 4-19	9	監視端末からデータヒストリアン経由して FW を突破し、データサーバを経由して PLC（マスター）に侵入して攻撃を実行
図 4-20	15	情報ネットワークから FW、データサーバを突破して PLC（マスター）に侵入し、攻撃を実行
図 4-21	16, 17	HMI／制御サーバに物理的にアクセスして侵入し、攻撃を実行
図 4-22	18	PLC（マスター）に物理アクセスして侵入し、攻撃を実行

攻撃ルートの絞り込みにあたっては、攻撃ルートと資産ベースのリスク分析の結果（資産のリスク値）からリスクが高いルートを抽出し、抽出したルートに対してのみリスク分析を実施する方法も考えられる。この方法を、**【補足 3】攻撃ルートの簡易探索法**に記す。リスク分析を行う工数を十分に確保できない場合には、こうした方法も参考にして、できる限り有効的にリスク分析を行うことを推奨する。

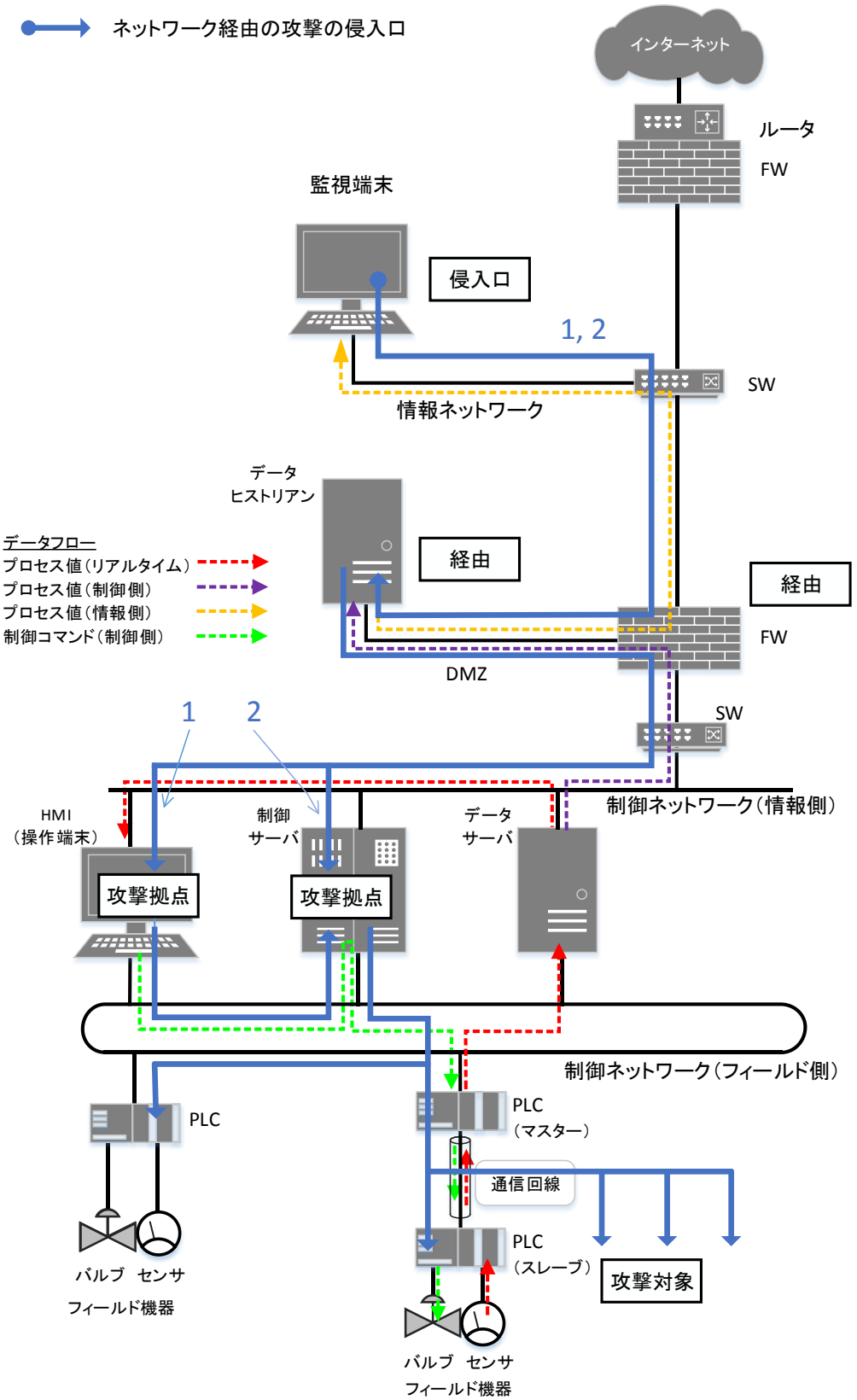


図 4-17 攻撃ルート 1, 2 の図示

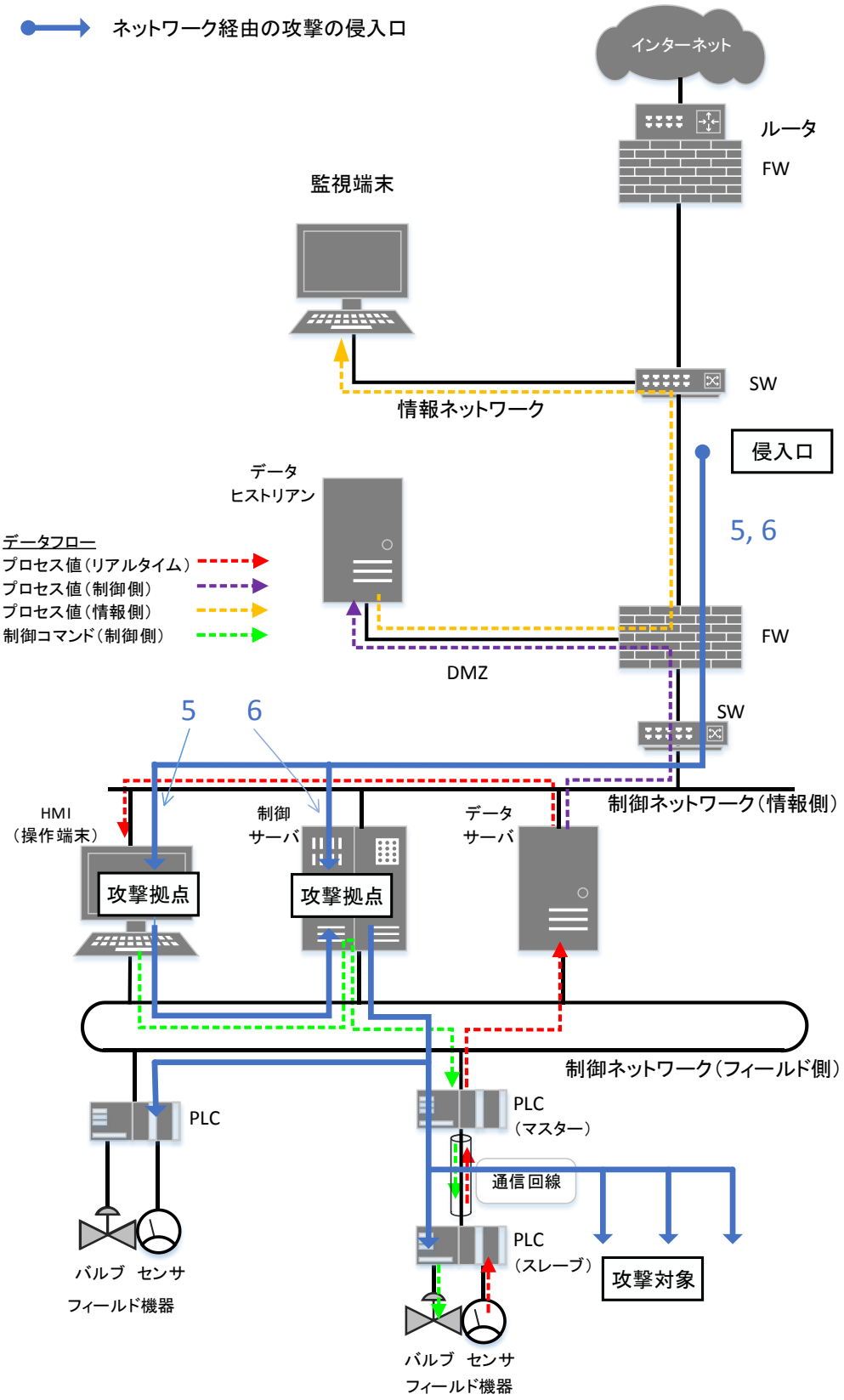


図 4-18 攻撃ルート 5, 6 の図示

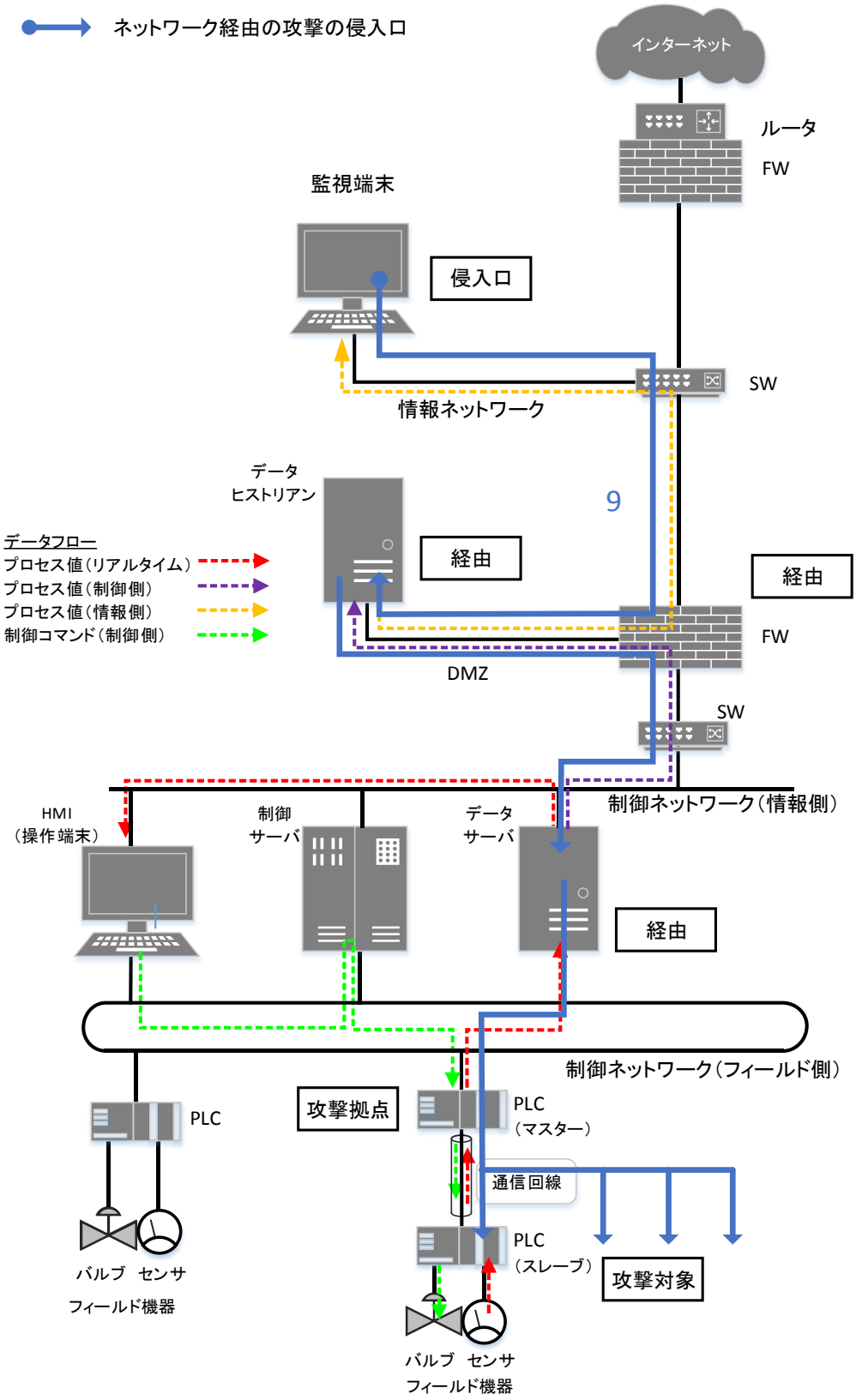


図 4-19 攻撃ルート 9 の図示

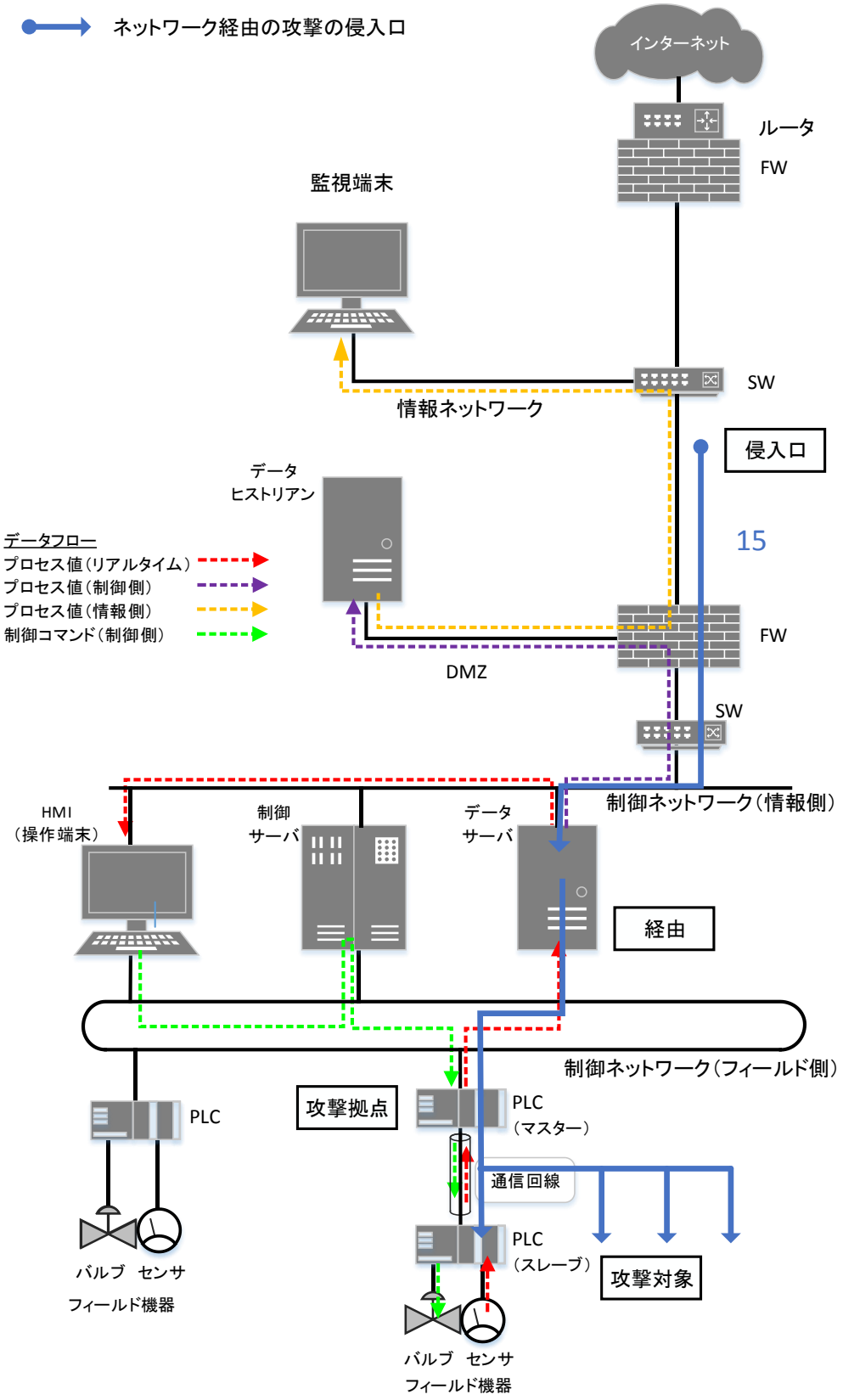


図 4-20 攻撃ルート 15 の図示

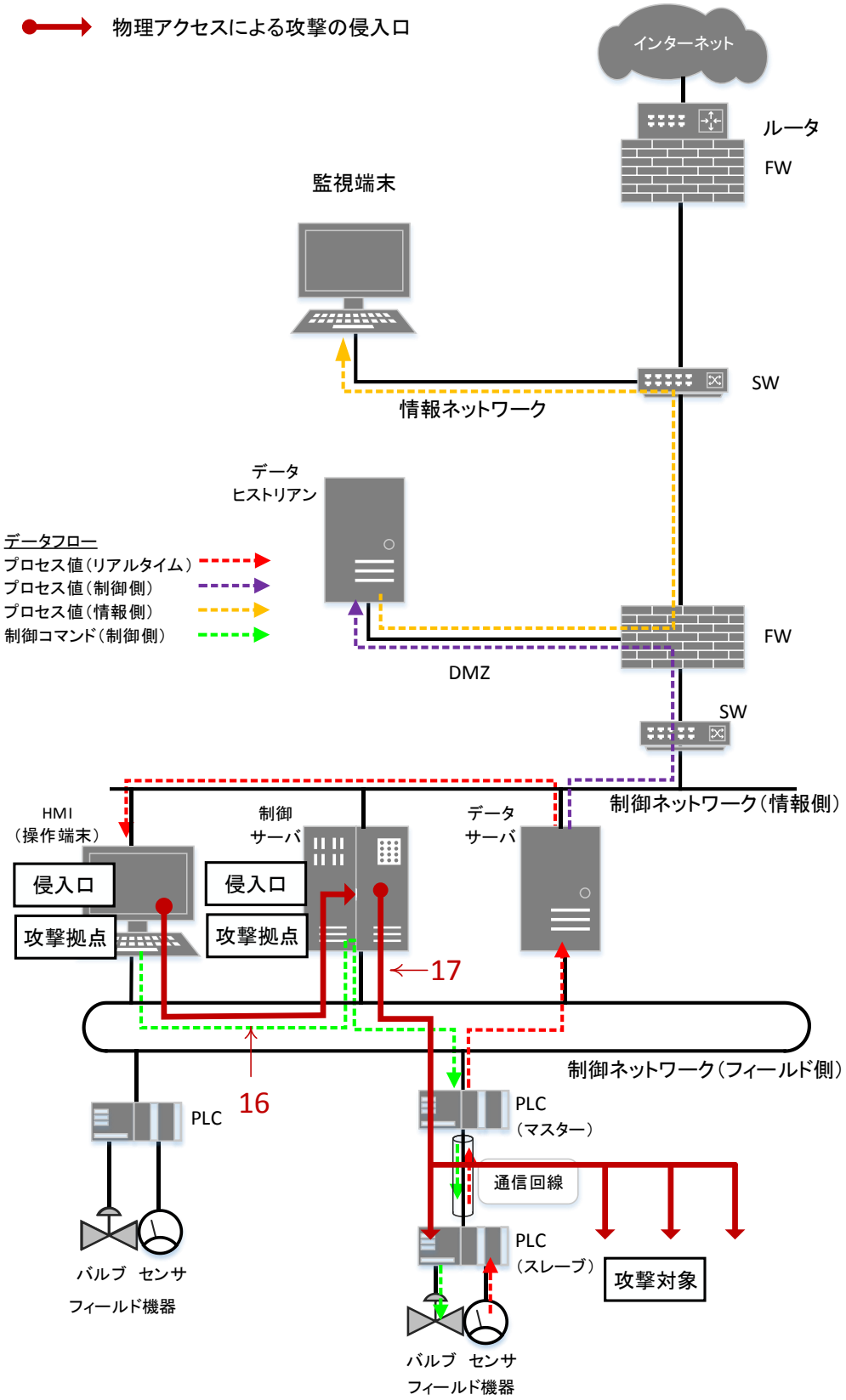


図 4-21 攻撃ルート 16, 17 の図示

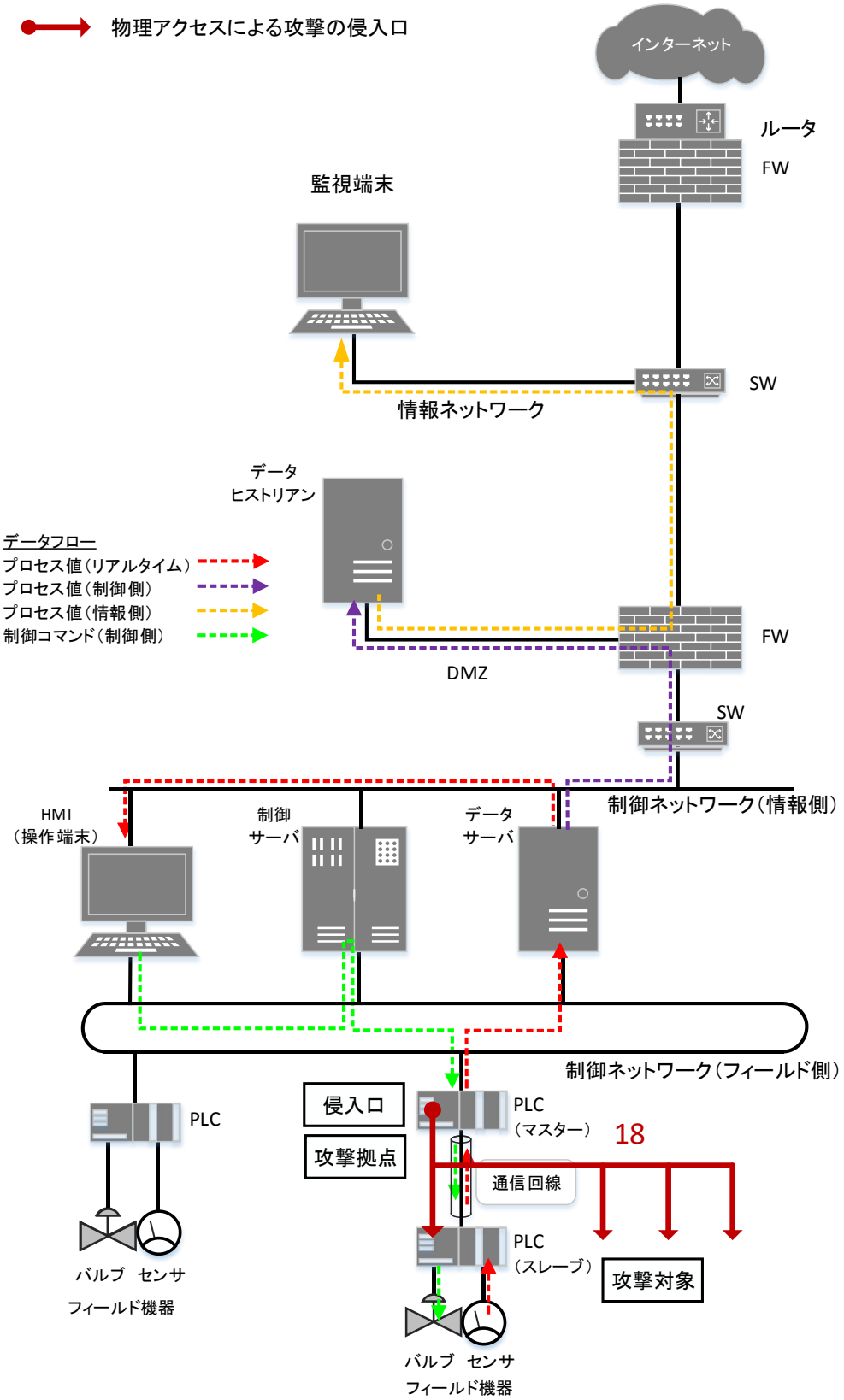


図 4-22 攻撃ルート 18 の図示

4.2.2.4. 攻撃ツリーの作成

攻撃ルートが整理できたら、攻撃ツリーを作成する。

各攻撃ツリーは、攻撃拠点で実行される最終攻撃に向けて、侵入口（例えば、表 4-41 の「情報 NW（FW）」）から攻撃拠点（同表「HMI」）まで進んで行く一連の攻撃となる。そして、進んで行く各攻撃段階（FW への不正アクセス、FW から HMI への不正アクセス、HMI での最終攻撃の実行）が、攻撃ステップとなる。

表 4-41 攻撃シナリオ 1-1 の攻撃ルート 5 抜粋

#	誰が	どこから	どうやって			どこで		何をする
	攻撃者	侵入口	経由 1	経由 2	経由 3	攻撃拠点	攻撃対象	最終攻撃
ネットワーク経由の攻撃								
5		情報 NW（FW）	－	－	－	HMI	対象エリアの PLC	広域供給停止コマンド送信

各攻撃ステップを記載する際は、基本形として以下を明確に記載することを推奨する。「攻撃者」は、「4.2.2.1. 攻撃者の検討」で事業者が想定した攻撃者を当てはめる。

【各攻撃ステップの基本形】

攻撃者が、 侵入口／経由から、 経由／攻撃拠点で （最終）攻撃を行う。

例えば、表 4-41 の攻撃ルート 5 は、情報ネットワークからファイアウォールに不正アクセスして制御ネットワークに入り、HMI に侵入して最終攻撃を実行するルートである。このルートの攻撃ツリーの一例を、表 4-42 に示す。制御ネットワーク以外のネットワークからの攻撃者は、表 4-31 の検討例に基づき「悪意のある第三者」となっている。

表 4-42 攻撃シナリオ 1-1 の攻撃ルート 5 の攻撃ツリーの記入例

攻撃ルート 5				
悪意のある第三者が、情報ネットワークからファイアウォールに不正アクセスする。			攻撃ステップ	攻撃ツリー
	悪意のある第三者が、ファイアウォールから HMI に不正アクセスする。		攻撃ステップ	
		悪意のある第三者が、HMI 上で広域供給停止操作を実行する（広域供給停止コマンドを送信する）。	攻撃ステップ	

以下に、攻撃ツリーの作成時及び事業被害ベース分析シートの記載方法のポイントを記す。

（1）攻撃ツリー作成時のポイント

①　1 つの攻撃ステップに記載する機器・攻撃の数

原則、1 つの攻撃ステップには、1 つの侵入先／攻撃拠点（「ファイアウォールに」、「制御サーバで」等）と、1 つの攻撃（「不正アクセスする」、「情報を改ざんする」等）を記載することが望ましい。これは、1 つの攻撃ステップに複数の機器や攻撃が記載されていると、4.2.4 項以降にて行う対策の記入と対策レベルの評価が複雑になるためである。

但し、攻撃ルート上に経由する機器が多数存在する場合には、それらの機器を 3.1.1 項や 4.1.1 項の資産のグルーピングに関する考え方を参考にまとめ、1 つの攻撃ステップに 1 つの機器グループを記載すること等、記載を工夫することが考えられる。

②　攻撃ステップに記載する攻撃

攻撃ステップに記載する攻撃は、システム仕様・構成、業務フロー・運用に沿って、リスク分析担当者・関係者が分かる様に記載する。例えば表 4-42 の最初のステップ（悪意のある第三者が、情報ネットワークから、ファイアウォールに不正アクセスする）を具体化することも考えられる。具体化の例を表 4-43 に示す。

表 4-43　攻撃ステップの具体化例

悪意のある第三者が、情報ネットワーク上でファイアウォールの管理者アカウント情報を窃取する。		
	悪意のある第三者が、窃取した管理者アカウント情報を用いて、ファイアウォールにログインする。	
		悪意のある第三者が、ファイアウォール上で、アクセス制御リストを変更し、情報ネットワークから侵入できる様にする。

但し、記載内容の具体化によって攻撃ステップが多層化しすぎると、攻撃ツリーが膨大化し、肝心のリスク分析が困難になる懸念がある。リスク分析担当者・関係者が読んでイメージできる程度の具体化と、攻撃ツリーの膨大化のバランスを考慮し、記載を工夫することを推奨する。

本書における攻撃ツリーの記入例では、資産ベースのリスク分析の結果を活用するため、攻撃ステップで想定する攻撃については資産ベースのリスク分析シートの「脅威（攻撃手法）」の表現をベースに記載している。攻撃は、「ネットワーク経由の攻撃」「物理アクセスによる攻撃」「攻撃者が手動で行う攻撃（直接操作）」「攻撃者が感染させたマルウェアが行う攻撃（マルウェア感染）」「コマ

ンドの不正送信」「データ改ざん」等の組み合わせとなると推測される。これらの攻撃を組み合わせた典型的な攻撃のツリーの例を、表 3-22 に示した脅威（攻撃手法）を用いて表 4-44 と表 4-45 に示す[35]。表 4-44 はネットワーク経由の攻撃で、攻撃者が手動で攻撃を行うケースの例、表 4-45 は、物理アクセスによる攻撃で、攻撃者がシステム・機器をマルウェアに感染させて攻撃を行うケースの例となる。

表 4-44 典型的な攻撃のツリーの例（1）

ネットワーク経由の直接攻撃		
＜攻撃者＞が＜侵入口＞に不正アクセスする。(#1)	攻撃ステップ	攻撃ツリー
＜攻撃者＞が＜侵入口＞から＜経由 1＞に不正アクセスする。(#1)	攻撃ステップ	
・・・	攻撃ステップ	
＜攻撃者＞が＜経由 n＞から＜攻撃拠点＞に不正アクセスする。(#1)	攻撃ステップ	
＜攻撃者＞が＜攻撃拠点＞で XX データを改ざんし(#9)（※1）、＜事業被害＞が発生する。	攻撃ステップ	

（）内の数字は脅威（攻撃手法）一覧の番号

※1 または、#8（情報窃取）、#10（情報破壊）、#11（不正送信）、#12（機能停止）

表 4-45 典型的な攻撃のツリーの例（2）

物理的侵入によるマルウェア感染		
＜攻撃者＞が＜侵入口（＝攻撃拠点）の設置場所＞に物理的に侵入する。(#2)	攻撃ステップ	攻撃ツリー
＜攻撃者＞が＜攻撃拠点＞を不正操作（不正ログイン）する。(#3)	攻撃ステップ	
＜攻撃者＞が＜攻撃拠点＞に不正媒体・機器を接続する。(#5)	攻撃ステップ	
＜攻撃者＞が＜攻撃拠点＞をマルウェアに感染させる。(#7)	攻撃ステップ	
マルウェアが＜攻撃拠点＞で XX データを消去して＜攻撃拠点＞を破壊し(#10)（※2）、＜事業被害＞が発生する。	攻撃ステップ	

（）内の数字は脅威（攻撃手法）一覧の番号

※2 または、#8（情報窃取）、#9（情報改ざん）、#11（不正送信）、#12（機能停止）

攻撃ツリーの作成にあたっては、この様な型を利用・加工し、リスク分析全体である程度一貫性のあるものにすると、見易くまとめることができる。攻撃ツリーの記入例に関しては、本ガイドの別冊となる**「制御システムのセキュリティリスク分析の実施例」**を参照することを推奨する。

図 4-23～図 4-26 に、攻撃シナリオ 1-1 全体の攻撃ツリーの作成例を示す。

[35] 他の典型的な例としては、「ネットワーク経由のマルウェア感染： #1→#7→#8 or 9 or 10 or 11 or 12」、「物理的侵入による直接攻撃： #2→#3→#8 or 9 or 10 or 11 or 12」等が考えられる。

事業被害ベースのリスク分析シート

１．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策						対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続			攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階								
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。														
1		**侵入口＝監視端末** 悪意のある第三者が、情報ネットワーク上の監視端末に不正アクセスする。														
2		悪意のある第三者が、監視端末からデータヒストリアンに不正アクセスする。														
3		悪意のある第三者が、データヒストリアンからファイアウォールに不正アクセスする。														
4		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。														
5		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。													#1	1,2,3,4,5
6		悪意のある第三者が、ファイアウォールから制御サーバに不正アクセスする。														
7		悪意のある第三者が、制御サーバ上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。													#2	1,2,3,6,7
8		悪意のある第三者が、ファイアウォールからデータサーバに不正アクセスする。														
9		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。														
10		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。													#3	1,2,3,8,9,10
11		悪意のある第三者が、監視端末をマルウェアに感染させる。														
12		マルウェアが、監視端末からデータヒストリアンに不正アクセスする／マルウェアに感染させる。														
13		マルウェアが、データヒストリアンからファイアウォールに不正アクセスする／マルウェアに感染させる。														
14		マルウェアが、ファイアウォールからHMI（操作端末）に不正アクセスする／マルウェアに感染させる。														
15		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。													#4	1,11,12,13,14,15

図 4-23 攻撃シナリオ 1-1 の攻撃ツリー作成例（1/4）

事業被害ベースのリスク分析シート

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。												
16		マルウェアが、ファイアウォールから制御サーバに不正アクセスする／マルウェアに感染させる。												
17		マルウェアが、制御サーバ上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。											#5	1,11,12,13,16,17
18		マルウェアが、ファイアウォールからデータサーバに不正アクセスする／マルウェアに感染させる。												
19		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェアに感染させる。												
20		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。											#6	1,11,12,13,18,19,20
21		**侵入口＝情報ネットワーク（FW）** 悪意のある第三者が、情報ネットワークからファイアウォールに不正アクセスする。												
22		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。												
23		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。											#7	21,22,23
24		悪意のある第三者が、HMI（操作端末）をマルウェアに感染させる。												
25		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。											#8	21,22,24,25
26		悪意のある第三者が、ファイアウォールから制御サーバに不正アクセスする。												
27		悪意のある第三者が、制御サーバ上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。											#9	21,26,27
28		悪意のある第三者が、制御サーバをマルウェアに感染させる。												
29		マルウェアが、制御サーバ上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。											#10	21,26,28,29
30		悪意のある第三者が、ファイアウォールからデータサーバに不正アクセスする。												

図 4-24 攻撃シナリオ 1-1 の攻撃ツリー作成例（2/4）

事業被害ベースのリスク分析シート

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策			対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御	検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階					
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。											
31		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。											
32		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。										#11	21,30,31,32
33		悪意のある第三者が、データサーバをマルウェアに感染させる。											
34		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェア感染させる。											
35		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。										#12	21,30,33,34,35
36		**侵入口＝HMI（操作端末）** 内部関係者が、計器室に入室する。											
37		内部関係者が、HMI（操作端末）にログインする。											
38		内部関係者が、HMI（操作端末）上で過失により広域供給停止操作を行い（広域供給停止コマンドを送信し）、広域に及ぶ供給が停止する。										#13	36,37,38
39		内部関係者が、HMI（操作端末）に（不正）媒体・機器を接続する。											
40		内部関係者が、過失によりHMI（操作端末）をマルウェアに感染させる。											
41		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。										#14	36,37,39,40,41
42		**侵入口＝制御サーバ** 内部関係者が、サーバ室に入室する。											
43		内部関係者が、制御サーバにログインする。											
44		内部関係者が、制御サーバ上で過失により広域供給停止操作を行い（広域供給停止コマンドを送信し）、広域に及ぶ供給が停止する。										#15	42,43,44
45		内部関係者が、制御サーバに（不正）媒体・機器を接続する。											
46		内部関係者が、過失により制御サーバをマルウェアに感染させる。											

図 4-25 攻撃シナリオ 1-1 の攻撃ツリー作成例（3/4）

事業被害ベースのリスク分析シート

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策			対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御	検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階 / 目的遂行段階						
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。											
47		マルウェアが、制御サーバ上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。										#16	42,43,45,46,47
48		**侵入口＝PLC（マスター）** 内部関係者が、フィールド（敷地内）のPLC（マスター）設置場所に入室する。											
49		内部関係者が、PLC（マスター）に（不正）媒体・機器を接続する。											
50		内部関係者が、PLC（マスター）にログインする。											
51		内部関係者が、PLC（マスター）上で過失により供給停止コマンドを送信し、広域に及ぶ供給が停止する。										#17	48,49,50,51
52		内部関係者が、過失によりPLC（マスター）をマルウェアに感染させる。											
53		マルウェアが、PLC（マスター）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。										#18	48,49,50,52,53

図 4-26 攻撃シナリオ 1-1 の攻撃ツリー作成例（4/4）

（2）事業被害ベースのリスク分析シートの記載方法及びまとめ方のポイント

事業被害ベースのリスク分析シートに攻撃ツリーを記入し、分析シートを作成するにあたってのポイントを以下に示す。

① 攻撃ツリーのまとめ方（並べ方）
攻撃ツリー（分析シート数）の膨大化を防ぐためのポイント

② 攻撃ステップのインデント
攻撃ツリーの構造を可視化し、追跡しやすくするためのポイント

③ 攻撃ツリー以外の項目の記載方法
各評価値等の記載箇所の明確化、及び分析シート全体を見やすくするためのポイント

④ 繰り返し出現する攻撃ステップの記載方法
何回も出現する同じ攻撃ステップについて、分析シートの作成を効率化するためのポイント

以下に、各ポイントについて説明する。

① 攻撃ツリーのまとめ方（並べ方）

攻撃ツリーのまとめ方は、「事業被害／攻撃シナリオごと」「攻撃ルート（侵入口・経由）ごと」等が考えられる。図 4-27 にそれを模式的に示す。この図の記載では、一つの事業被害 N に対して、複数存在する攻撃シナリオをシナリオ N-m で表している。

事業被害／攻撃シナリオごとに、攻撃ツリーを記載しているのが、図中の（A1）である。この様に攻撃ツリーには、共通の侵入口と経由が、複数の攻撃ツリーに表れるケースが存在する。この共通の部分を、共通の事業被害内で統合したのが、図中の（A2）である。

一方で、異なる事業被害であるが、侵入口と攻撃ルートが共通となる攻撃ツリーが多数存在するケースも存在する。その場合、図中の（B）の様に、侵入口と攻撃ルートで攻撃ツリーを統合することが考えられる。これが、「攻撃ルート（侵入口・経由）ごと」のまとめ方である。攻撃ツリーの各ステップで、対策状況を検証して、その攻撃ツリーがどの程度のリスクかを評価するので、共通な攻撃ステップはできるだけ統合する方が、評価はしやすくなる利点はあるが、リスク分析の観点からは、できるだけ事業被害や攻撃シナリオごとにまとまっていた方が見通しがよいという利点がある。

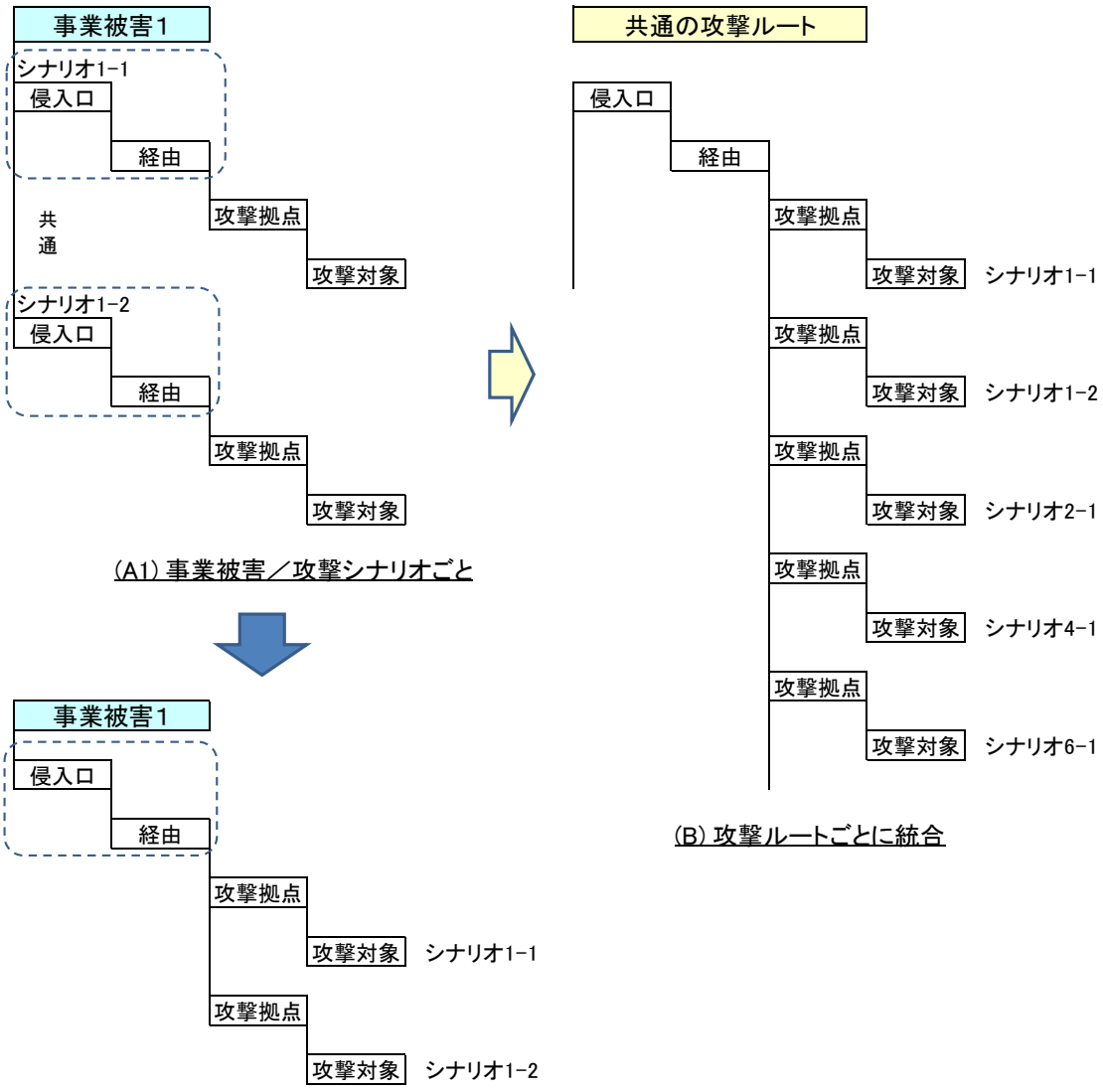


図 4-27 攻撃ツリーのまとめ方の違い

表 4-46 に、両者の想定される長所と短所を挙げる。システムの規模と複雑さ(侵入口や経由の多さ)、攻撃シナリオの数(攻撃拠点や攻撃対象の分散)、注視したい観点や、事業被害ベースのリスク分析シートの今後の使い方等に応じて、どちらかのまとめ方を採用する。一概にどちらが良いということはないため、事業者にとって記述しやすく見やすいまとめ方を検討する。なお、「事業被害／攻撃シナリオごと」で作成したあとに、評価においては、「攻撃ルート(侵入口・経由)ごと」にソートして実施することも考えられる。図 4-23～図 4-26 に示した分析シートの例は、「事業被害／攻撃シナリオごと」を用いている。

表 4-46 攻撃ツリーのまとめ方(並べ方)

	事業被害／攻撃シナリオごと	攻撃ルート(侵入口・経由)ごと
まとめ方(並べ方)	事業被害／攻撃シナリオごとにまとめる。	同じ侵入口・経路の攻撃ツリーごとにまとめる。
長所	事業被害ごと／攻撃シナリオごとのリスクが見えやすい。特定の事業被害に着目して分析する場合は、このまとめ方の方が、適している。	同じ攻撃ルート(侵入口・経由)を何度も重複して記載するのを防ぐことができる。
短所	各事業被害／攻撃シナリオの攻撃拠点・攻撃対象が一部の機器に集中し、結果的に各事業被害／攻撃シナリオの攻撃ツリーがほぼ同一または互いのサブセットとなった場合、ほぼ同一内容の分析シートを多数作成することになる可能性がある。	多くの最終攻撃が並列に列記されるため、最終攻撃の数が一定数を超えると分かり難くなる可能性がある。 事業被害ごと／攻撃シナリオごとのリスクが見え難い。

② 攻撃ステップのインデント

攻撃ステップのインデントは、攻撃の段階や分岐を示している。一番左に来る攻撃ステップを各攻撃ツリーの「ルート」とし(例えば、図 4-23～図 4-26 の項番 1, 21, 36 等)、その後に直列に発生する攻撃ステップについては、1 段ごとにインデントをつける(項番 2, 3, 4, 5 等)。また、並列に発生する攻撃ステップについては、並列する攻撃ステップと同じインデントで記載する(項番 2 と 11、4 と 6 と 8 等)。

③　攻撃ツリー／攻撃ステップ以外の項目の記載方法

事業被害ベースのリスク分析シートに攻撃ツリーを作成する際には、攻撃ツリーに合わせ、4.2.3 項以降のリスク分析で使用する「評価指標」より右側の項目の記載方法を明確化するために、フォーマットの作成が必要となる。表 4-47 に、「評価指標」以降の項目のフォーマットの作成にあたっての記載方法を、図 4-28 に、事業被害ベースのリスク分析シートにおける各項目のフォーマットを示す。

表 4-47　攻撃ツリー／攻撃ステップ以外の項目の記載方法

項目		説明・整形例
評価指標		「脅威レベル」、「脆弱性レベル」、「事業被害」、「リスク値」は、攻撃ツリー単位で評価する。例では、最終攻撃ステップの行に記載欄を設け、その他の箇所はグレーアウトしている。
対策		対策（「侵入段階」、「目的遂行段階」、「検知・被害把握」、「事業継続」）は、攻撃ステップ単位に記入する。
対策レベル	攻撃ステップ	各攻撃ステップで実施している対策の対策レベルを評価する（評価方法は 4.2.5 項を参照）。
	攻撃ツリー	構成ステップの対策から、攻撃ツリー全体としての対策レベルを評価する（評価方法は 4.2.5 項を参照）。例では、最終攻撃ステップの行に記載欄を設け、その他の箇所はグレーアウトしている。
攻撃ツリー番号	攻撃ツリー番号	攻撃ツリーの参照番号（通し番号）を記載する。例では、最終攻撃ステップの行に記載欄を設け、その他の箇所はグレーアウトしている。
	構成ステップ（項番）	各攻撃ツリーを構成するステップの番号（項番）を記載する。例では、最終攻撃ステップの行に記載欄を設け、その他の箇所はグレーアウトしている。

最終攻撃ステップ

評価指標

対策

対策レベル（攻撃ツリー）

攻撃ツリー番号

事業被害ベースのリスク分析シート

対策レベル（攻撃ステップ）

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。												
1		**侵入口＝監視端末** 悪意のある第三者が、情報ネットワーク上の監視端末に不正アクセスする。												
2		悪意のある第三者が、監視端末からデータヒストリアンに不正アクセスする。												
3		悪意のある第三者が、データヒストリアンからファイアウォールに不正アクセスする。												
4		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。												
5		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。											#1	1,2,3,4,5
6		悪意のある第三者が、ファイアウォールから制御サーバに不正アクセスする。												
7		悪意のある第三者が、制御サーバ上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。											#2	1,2,3,6,7
8		悪意のある第三者が、ファイアウォールからデータサーバに不正アクセスする。												
9		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。												
10		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。											#3	1,2,3,8,9,10
11		悪意のある第三者が、監視端末をマルウェアに感染させる。												
12		マルウェアが、監視端末からデータヒストリアンに不正アクセスする／マルウェアに感染させる。												
13		マルウェアが、データヒストリアンからファイアウォールに不正アクセスする／マルウェアに感染させる。												
14		マルウェアが、ファイアウォールからHMI（操作端末）に不正アクセスする／マルウェアに感染させる。												
15		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。											#4	1,11,12,13,14,15

図 4-28 事業被害ベースのリスク分析シートにおける「評価指標」以降の項目の記載箇所

このページは空白です。

④　繰り返し出現する攻撃ステップの記載方法

攻撃ツリーを作成していくと、同じ攻撃ステップが出現することが推測される。図 4-23～図 4-26 の例に見てみると、例えば以下の攻撃ステップが全く同じであることがわかる。

- 項番 6「悪意のある第三者が、ファイアウォールから制御サーバに不正アクセスする。」（＝項番 26）
- 項番 15「マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。」（＝項番 25, 41）

この様な“重複”については、既出の項番を引用し、対策欄の記載を「項番〇〇と同じ」と省略するとよい。これによって後段での対策記入の工数を削減できるほか、記入ミス（対策が同じ項番からのコピーミスや、対策を 1 箇所修正した場合の他箇所への修正の反映漏れ等）を防止することができる。省略の一例を、図 4-29 に示す。

このページは空白です。

事業被害ベースのリスク分析シート

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。												
31		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。					項番9と同じ							
32		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。					項番10と同じ						#11	21,30,31,32
33		悪意のある第三者が、データサーバをマルウェアに感染させる。												
34		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェア感染させる。					項番19と同じ							
35		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。					項番20と同じ						#12	21,30,33,34,35
36		**侵入口＝HMI（操作端末）** 内部関係者が、計器室に入室する。												
37		内部関係者が、HMI（操作端末）にログインする。												
38		内部関係者が、HMI（操作端末）上で過失により広域供給停止操作を行い（広域供給停止コマンドを送信し）、広域に及ぶ供給が停止する。											#13	36,37,38
39		内部関係者が、HMI（操作端末）に（不正）媒体・機器を接続する。												
40		内部関係者が、過失によりHMI（操作端末）をマルウェアに感染させる。												
41		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。					項番15と同じ						#14	36,37,39,40,41
42		**侵入口＝制御サーバ** 内部関係者が、サーバ室に入室する。												
43		内部関係者が、制御サーバにログインする。												
44		内部関係者が、制御サーバ上で過失により広域供給停止操作を行い（広域供給停止コマンドを送信し）、広域に及ぶ供給が停止する。											#15	42,43,44
45		内部関係者が、制御サーバに（不正）媒体・機器を接続する。												
46		内部関係者が、過失により制御サーバをマルウェアに感染させる。												

図 4-29 繰り返し出現する攻撃ステップの記載方法の例

このページは空白です。

4.2.3. 脅威レベルの評価・記入、事業被害レベルの記入

攻撃ツリーの作成が終了したら、次に、各攻撃ツリーの脅威レベルを評価し、事業被害ベースのリスク分析シートに記入する。また、3.3 節で定めた事業被害レベルをリスク分析シートに記入する。

（1）脅威レベルの評価・記入

脅威レベルは、想定した攻撃ツリーが成立する可能性を表す。脅威レベルは攻撃ツリー単位での評価となるため、各攻撃ステップではなく、攻撃ツリー全体で評価する。3.4 節で定めた判断基準に基づいて評価し、リスク分析シートの「評価指標」の「脅威レベル」欄に記入する。

評価に悩んだ場合は、原則として高い方向に評価することが望ましい。判定に悩んだ攻撃ツリーについては、最終的にそう評価した根拠を、備考欄を作成し、残しておくことを推奨する[36]。

（2）事業被害レベルの記入

事業被害レベルは、想定した攻撃ツリーが行われた場合の被害範囲や会社経営上の打撃を表す。3.3 節で定めた事業被害レベルを、リスク分析シートの「評価指標」の「事業被害レベル」欄に記入する。

例えば、表 3-19 から、事業被害「広域での○○供給停止」の事業被害レベルは「3」であるから、広域供給停止を引き起こす可能性のある攻撃シナリオ（攻撃ツリー）の事業被害レベルは「3」となる。

図 4-30 に、脅威レベル、事業被害レベルのリスク分析シートへの記入例を示す。

[36] リスク分析は、1 回で終わるものではない。全体のリスク評価を終え、リスク値の高い攻撃ツリーのリスク低減を検討する際、当該攻撃ツリーの評価を改めて精査することになる。精査の際に、当初の評価時に何故そう評価したのか、本当にそれだけのリスクがあるのか、評価の根拠が残っていると有用である。また、翌年以降に、システム環境の変化や新たな脅威の出現等によって評価を見直す際にも有用となる。

このページは空白です。

事業被害ベースのリスク分析シート

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。												
31		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。					項番9と同じ							
32		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2		3		項番10と同じ						#11	21,30,31,32
33		悪意のある第三者が、データサーバをマルウェアに感染させる。												
34		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェア感染させる。					項番19と同じ							
35		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	1		3		項番20と同じ						#12	21,30,33,34,35
36		**侵入口＝HMI（操作端末）** 内部関係者が、計器室に入室する。												
37		内部関係者が、HMI（操作端末）にログインする。												
38		内部関係者が、HMI（操作端末）上で過失により広域供給停止操作を行い（広域供給停止コマンドを送信し）、広域に及ぶ供給が停止する。	1		3								#13	36,37,38
39		内部関係者が、HMI（操作端末）に（不正）媒体・機器を接続する。												
40		内部関係者が、過失によりHMI（操作端末）をマルウェアに感染させる。												
41		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2		3		項番15と同じ						#14	36,37,39,40,41
42		**侵入口＝制御サーバ** 内部関係者が、サーバ室に入室する。												
43		内部関係者が、制御サーバにログインする。												
44		内部関係者が、制御サーバ上で過失により広域供給停止操作を行い（広域供給停止コマンドを送信し）、広域に及ぶ供給が停止する。	1		3								#15	42,43,44
45		内部関係者が、制御サーバに（不正）媒体・機器を接続する。												
46		内部関係者が、過失により制御サーバをマルウェアに感染させる。												

図 4-30 事業被害ベースのリスク分析シート（脅威レベル、事業被害レベルの記入例）

このページは空白です。

4.2.4. セキュリティ対策状況の記入

脅威レベル、事業被害レベルの評価・記入が終了したら、次に、実施しているセキュリティ対策を事業被害ベースのリスク分析シートに記入する。

セキュリティ対策は、想定した攻撃に対して現状実施（実装）している対策を、攻撃ステップ単位で「対策」欄に記入する。各対策は、その用途と目的によって 4 つの分類（「防御：侵入／拡散段階」「防御：目的遂行段階」「検知／被害把握」「事業継続」に分けて、該当欄に記入する。表 4-48 に、各分類の意味と具体的なセキュリティ対策の例（表 4-27 の抜粋）を示す。

表 4-48 対策の用途・目的

項目			説明
対策	防御	侵入／拡散段階	攻撃の最上流（初期段階）における対策。例えば、外部との接続点を介したネットワーク経由の攻撃、あるいはシステム（サーバ・操作端末等）設置場所への攻撃者の物理的侵入を防止する目的で実装される対策。また、攻撃者（内部犯行者を含む）による、システム（サーバ・操作端末等）への不正ログイン等を防止する目的で実装される対策。更に、システム（サーバ・操作端末等）への侵入を果たした攻撃者（人間あるいは不正プログラム）による、侵入範囲拡大（侵入したシステム内部での拡大及び他のシステムへの拡散）を防止する目的で実装される対策も含まれる。
			例 「セグメント分割／ゾーニング」「IPS／IDS」「操作者認証」「アクセス制御」「APT 対策ツール」
		目的遂行段階	情報窃取、データ改ざん、制御乗っ取り、及びシステム破壊等、攻撃者による最終目的の実行を防止する目的で実装される対策。
			例 「データ暗号化」「重要操作の承認」「フェールセーフ設計」
	検知／被害把握		攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策、攻撃の成功による被害を最小限に留めるために実装される対策、もしくはサービスの継続、被害の早期復旧を実現するための状況把握することを目的に実装される対策。
			例 「ログ収集分析」、「統合ログ管理システム」
	事業継続		攻撃の成功による被害を早期に回復して、事業の継続性を維持する目的に実装される対策。
			例 「冗長化」「バックアップの取得」

対策の記入には、資産ベースのリスク分析の結果を活用することができる。資産ベースのリスク分析シートには、制御システムを構成する資産（対象装置）、各資産に対する脅威（攻撃手法）、及び各脅威に対して実施している対策が整理されている。資産ベースのリスク分析シート上の該当する対象装置と脅威（攻撃手法）は、事業被害ベースの分析シートの各攻撃ステップの記載内容を参考に、マッピングすることができる。

【対象装置】 各攻撃ステップの「経由／攻撃拠点で」にあたる機器
【脅威（攻撃手法）】 各攻撃ステップの「（最終）攻撃を行う」にあたる攻撃

例えば、攻撃ステップが「悪意のある第三者が、データベース上で重要データを改ざんし、広域に及ぶ供給が停止する」であれば、資産ベースのリスク分析シートの「対象装置」が「データサーバ」、「脅威（攻撃手法）」が「情報改ざん」の行の対策欄を参考にすることができる。図 4-31 に、資産ベースのリスク分析シート上の参照箇所を例示する。

資産ベースのリスク分析シートから対策をそのまま転記することで、作業の効率化を図ることができる。または、資産ベースのリスク分析シートの対策を参考に、該当する攻撃ステップの攻撃を防止できるか見直し、有効と考えられる対策を選択して転記することで、より実状を反映したリスク分析を行うことができる。

実施している対策に○をつけるが、評価対象の攻撃ステップの攻撃者等によっては、実施している対策が攻撃の防止に有効でないケースもあると考えられる（例えば、内部関係者に対する入退管理や操作者認証等）。その様な場合には、○を外すか、実施しているが有効でないことがわかる様に工夫する。

該当する攻撃や対策が資産ベースのリスク分析シートにない場合には、3.5 節の「セキュリティ対策候補一覧」から選択する。「セキュリティ対策候補一覧」にもない場合、実施している対策の内容を簡潔に記入する。

なお、攻撃ツリーの作成時に、繰り返し出現する攻撃ステップの対策欄を「項番○○と同じ」として省略した箇所は、対策の記入は不要となる。

図 4-32 に、セキュリティ対策のリスク分析シートへの記入例を示す。

資産ベースのリスク分析シート

凡例: ○ 対策実施　　× 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策						対策レベル
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			防御				検知/被害把握	事業継続	脅威毎
									侵入/拡散段階		目的遂行段階				
1	情報系資産	**データサーバ** **対象装置**	2	2		B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	○			IPS／IDS ログ収集・分析 統合ログ管理システム		2
2			2	1		C	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。 あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○	3
3			2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証	○					2
4			2	3		A	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレビュテーション メールフィルタリング						1
5			2	3		A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		1
6			2	2		B	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○	(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
7			1	2		C	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
8			3	2		A	情報窃取 **脅威(攻撃手法)**	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	(同左) (同左) (同左) (同左)	**対策**	ログ収集・分析 統合ログ管理システム		2
9			3	3		A	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名		(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	○	1
10			3	3		A	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御	○	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	○	1
11			3	3	3	A	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム			1
12			2	3		A	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計		1
13			3	3		A	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計		1
14			2	2		B	窃盗	機器を窃盗する。	施錠管理 モバイル機器・媒体管理	○	(同左) (同左)		施錠管理 モバイル機器・媒体管理	○		2
15			3	3		A	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去		(同左) (同左) (同左)					1
16			3	2		A	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ	○ ○	冗長化		2
17			1	3		B	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化	1
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化		
19			2	3		A	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線							1
20			2	3		A	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム			1
21			3	3		A	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム			1

図 4-31　資産ベースのリスク分析シートから対策を転記する際の参照箇所の例

事業被害ベースのリスク分析シート

１．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策								対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御				検知／被害把握		事業継続		攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階		目的遂行段階									
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。																
14		マルウェアが、ファイアウォールからHMI（操作端末）に不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	〇	機器異常検知							
							通信相手の認証		アクセス制御	〇	ログ収集・分析	〇						
							操作者認証	〇										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	〇										
15		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2		3				データ署名		機器異常検知	〇					#4	1,11,12,13,14,15
									重要操作の承認		ログ収集・分析	〇						
16		マルウェアが、ファイアウォールから制御サーバに不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	〇	機器異常検知							
							通信相手の認証		アクセス制御	〇	ログ収集・分析	〇						
							操作者認証	〇										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	〇										
17		マルウェアが、制御サーバ上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2		3				データ署名		機器異常検知	〇					#5	1,11,12,13,16,17
									重要操作の承認		ログ収集・分析	〇						
18		マルウェアが、ファイアウォールからデータサーバに不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	〇	機器異常検知							
							通信相手の認証		アクセス制御	〇	ログ収集・分析	〇						
							操作者認証	〇										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	〇										
19		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェア感染させる。					パッチ適用		権限管理		機器異常検知	〇						
							通信相手の認証		アクセス制御		ログ収集・分析	〇						
							操作者認証											
							ホワイトリストによるプロセスの起動制限											
20		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	1		3				データ署名		機器異常検知	〇					#6	1,11,12,13,18,19,20
											ログ収集・分析	〇						
21		**侵入口＝情報ネットワーク（FW）** 悪意のある第三者が、情報ネットワークからファイアウォールに不正アクセスする。					FW（パケットフィルタリング型）	〇	権限管理	〇	ログ収集・分析	〇						
							パッチ適用	〇	アクセス制御	〇								
							通信相手の認証											
							操作者認証	〇										
22		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。					項番4と同じ											
23		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2		3		項番5と同じ										#7	21,22,23
24		悪意のある第三者が、HMI（操作端末）をマルウェアに感染させる。					パッチ適用				機器異常検知							
							アンチウィルス				ログ収集・分析	〇						
							ホワイトリストによるプロセス起動制限	〇										
25		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2		3		項番15と同じ										#8	21,22,24,25

図 4-32 事業被害ベースのリスク分析シート（セキュリティ対策の記入例）

4.2.5. 対策レベル／脆弱性レベルの評価・記入

セキュリティ対策の記入が終了したら、次に、対策レベルと脆弱性レベルを評価し、事業被害ベースのリスク分析シートに記入する。

（1）対策レベルの評価と記入

対策レベルは、想定する攻撃を実施している対策が防止できる可能性を表す。対策レベルの評価は、攻撃ステップの対策レベルの評価と、攻撃ツリーの対策レベルの評価の 2 段階で行う。

① 攻撃ステップの対策レベルの評価

攻撃ステップの対策レベルは、資産ベースのリスク分析の結果を参照して、3.5 節で定めた判断基準に基づいて評価し、「対策レベル（攻撃ステップ）」欄に記入する。

例えば、攻撃ステップが、「悪意のある第三者が、データサーバ上で重要データを改ざんし、広域に及ぶ供給が停止する」であれば、資産ベースのリスク分析シートの「対象装置」が「データサーバ」、「脅威（攻撃手法）」が「情報改ざん」の行の「対策レベル（脅威ごと）」に記載されている対策レベル（「1」）を参考にする。図 4-33 に、資産ベースのリスク分析シート上の参照箇所を例示する。記入した対策が、当該攻撃ステップの攻撃を防止できるか否かを検討し、資産ベースのリスク分析シートの対策レベル（上術の例では「1」）が 3.5 節で定めた判断基準に照らして妥当であればこの値を採用する。変更が必要であれば、適切な対策レベルに補正する。

対策レベルの補正を考慮する例として、内部関係者に対する入退管理や操作者認証等については、実際的な有効性がない可能性がある。対策レベルの妥当性を確認する際には、こうした事情も踏まえるとより正確にリスク分析を行うことができる。

対策が資産ベースのリスク分析シートを参考に記入したものではない場合は、3.5 節で定めた判断基準に照らして個別に評価する。

② 攻撃ツリーの対策レベルの評価

攻撃ツリー全体の対策レベルは、攻撃ツリーを構成する攻撃ステップの対策レベルのうち最も高い対策レベルを採用し、「対策レベル（攻撃ツリー）」欄に記入する。これは、各攻撃ツリーは直列する攻撃ステップから構成されているため、攻撃ステップの中で最も高い対策レベルが、当該攻撃ツリーの実行を抑止する最大の防波堤になるとの考えに基づく。表 4-49 に、攻撃ツリーの対策レ

ベルの算定の具体例を示す。例えば、攻撃ツリー#1 の対策レベルは「2」、攻撃ツリー#2 の対策レベルは「1」、攻撃ツリー#3 の対策レベルは「3」となる。

表 4-49 攻撃ツリーの対策レベルの算定の具体例

攻撃ステップ	攻撃ツリー#1		攻撃ツリー#2		攻撃ツリー#3	
	対策レベル		対策レベル		対策レベル	
	攻撃ステップ	攻撃ツリー	攻撃ステップ	攻撃ツリー	攻撃ステップ	攻撃ツリー
1	1		1		2	
2	1		1		1	
3	1		1		3	
4	2	2	1	1	1	3

(2)脆弱性レベルの評価と記入

脆弱性は、想定する攻撃ツリーを受け入れてしまう可能性を表す。3.5 節において定義した通り、評価指標の一つである「脆弱性レベル」の値は、「対策レベル」の双対の値として定義する。表 4-50 に、両者の値の関係を示す(表 3-24 の抜粋)。

表 4-50 攻撃ツリーの対策レベルと脆弱性レベルの値の関係

攻撃ツリーの対策レベル	脆弱性レベル
1	3
2	2
3	1

脆弱性レベルも攻撃ツリー単位で評価するため、攻撃ツリーの対策レベルの双対の値を、リスク分析シートの「評価指標」の「脆弱性レベル」欄に記入する。

従って、表 4-49 の例であれば、攻撃ツリー#1 の脆弱性レベルは「2」、攻撃ツリー#2 の脆弱性レベルは「3」、攻撃ツリー#1 の脆弱性レベルは「1」となる。

図 4-34 に、対策レベル、脆弱性レベルのリスク分析シートの記入例を示す。

資産ベースのリスク分析シート

凡例: ○ 対策実施　　× 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策						対策レベル
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			防御				検知/被害把握	事業継続	脅威毎
									侵入/拡散段階		目的遂行段階				
1	情報系資産	データサーバ 対象装置	2	2		B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム		2
2			2	1		C	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。 あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○	3
3			2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証	○					2
4			2	3		A	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング						1
5			2	3		A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		1
6			2	2		B	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○	(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
7			1	2		C	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 ○ 			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
8			3	2		A	情報窃取 脅威(攻撃手法)	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム		2
9			3	3		A	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名		(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ ○	1
10			3	3		A	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御	○	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ ○	1
11			3	3	3	A	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム		1
12			2	3		A	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計	1
13			3	3		A	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計	1
14			2	2		B	窃盗	機器を窃盗する。	施錠管理 モバイル機器・媒体管理	○	(同左) (同左)		施錠管理 モバイル機器・媒体管理	○	2
15			3	3		A	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去		(同左) (同左) (同左)				1
16			3	2		A	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ	 ○ ○	冗長化	2
17			1	3		B	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化	1
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化	
19			2	3		A	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線						1
20			2	3		A	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム		1
21			3	3		A	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		1

対策レベル

図 4-33　資産ベースのリスク分析シートから対策レベルを参考にする際の参照箇所の例

事業被害ベースのリスク分析シート

１．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策						対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御				検知／被害把握		事業継続		攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階		目的遂行段階									
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。																
14		マルウェアが、ファイアウォールからHMI（操作端末）に不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	〇	機器異常検知				2			
							通信相手の認証		アクセス制御	〇	ログ収集・分析	〇						
							操作者認証	〇										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	〇										
15		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3				データ署名		機器異常検知	〇			1	2	#4	1,11,12,13,14,15
									重要操作の承認		ログ収集・分析	〇						
16		マルウェアが、ファイアウォールから制御サーバに不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	〇	機器異常検知				2			
							通信相手の認証		アクセス制御	〇	ログ収集・分析	〇						
							操作者認証	〇										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	〇										
17		マルウェアが、制御サーバ上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3				データ署名		機器異常検知	〇			1	2	#5	1,11,12,13,16,17
									重要操作の承認		ログ収集・分析	〇						
18		マルウェアが、ファイアウォールからデータサーバに不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	〇	機器異常検知				2			
							通信相手の認証		アクセス制御	〇	ログ収集・分析	〇						
							操作者認証	〇										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	〇										
19		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェア感染させる。					パッチ適用		権限管理		機器異常検知	〇			1			
							通信相手の認証		アクセス制御		ログ収集・分析	〇						
							操作者認証											
							ホワイトリストによるプロセスの起動制限											
20		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	1	2	3				データ署名		機器異常検知	〇			1	2	#6	1,11,12,13,18,19,20
											ログ収集・分析	〇						
21	**侵入口＝情報ネットワーク（FW）** 悪意のある第三者が、情報ネットワークからファイアウォールに不正アクセスする。						FW（パケットフィルタリング型）	〇	権限管理	〇	ログ収集・分析	〇			2			
							パッチ適用	〇	アクセス制御	〇								
							通信相手の認証											
							操作者認証	〇										
22		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。					項番4と同じ								2			
23		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2	2	3		項番5と同じ								1	2	#7	21,22,23
24		悪意のある第三者が、HMI（操作端末）をマルウェアに感染させる。					パッチ適用				機器異常検知				2			
							アンチウィルス				ログ収集・分析	〇						
							ホワイトリストによるプロセス起動制限	〇										
25		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3		項番15と同じ								1	2	#8	21,22,24,25

図 4-34 事業被害ベースのリスク分析シート（対策レベル、脆弱性レベルの記入例）

4.2.6. リスク値の評価

リスク値は、想定する攻撃ツリーの総合的なリスクの度合いを表す。算定方法は資産ベースのリスク分析と同じだが、資産ベースのリスク分析における「資産の重要度」の代わりに、事業被害ベースのリスク分析では「事業被害レベル」を使用する。評価指標「脅威レベル」「事業被害レベル」「脆弱性レベル」からリスク値を算定し、事業被害ベースのリスク分析シートの「評価指標」の「リスク値」欄に記入する。

本ガイドで用いるリスク値の算定式を、表 4-51 に示す。リスク値は「A（リスクが高い）」から「E（リスクが低い）」の 5 段階で評価する。

図 4-35 に、「脅威レベル」「脆弱性レベル」「事業被害レベル」と「リスク値」の関係を示す。同図から、リスク値の高い（脅威レベル、脆弱性レベル、事業被害レベルが高い）領域が、右上に集まることが見て取れる。これは、事業被害レベルが同一であれば、脅威レベルもしくは脆弱性レベルが下がるほどリスク値が低くなり、脅威レベル×脆弱性レベルの値が同一であれば、事業被害レベルが下がるほどリスク値が低くなることを示している。一般的に言えば、リスク分析を実施した結果、右上に分布している攻撃（攻撃ツリー）のリスクを減じる対策から取り組む必要がある。

表 4-51 事業被害ベースのリスク分析におけるリスク値の算定基準

評価指標と評価点			リスク値	判定条件
脅威 レベル	脆弱性 レベル	事業被害 レベル		
3	3	3	A	事業被害＝3 6≦脅威×脆弱性≦9
3	2	3		
2	3	3		
2	2	3	B	事業被害＝3 3≦脅威×脆弱性＜6
3	1	3		
1	3	3		
3	3	2		事業被害＝2 6≦脅威×脆弱性≦9
3	2	2		
2	3	2		
2	1	3	C	事業被害＝3 1≦脅威×脆弱性＜3
1	2	3		
1	1	3		
2	2	2		事業被害＝2 3≦脅威×脆弱性＜6
3	1	2		
1	3	2		
3	3	1		事業被害＝1 6＜脅威×脆弱性≦9
2	1	2	D	事業被害＝2 1≦脅威×脆弱性＜3
1	2	2		
1	1	2		
3	2	1		事業被害＝1 3＜脅威×脆弱性≦6
2	3	1		
2	2	1		
3	1	1	E	事業被害＝1 1≦脅威×脆弱性≦3
1	3	1		
2	1	1		
1	2	1		
1	1	1		

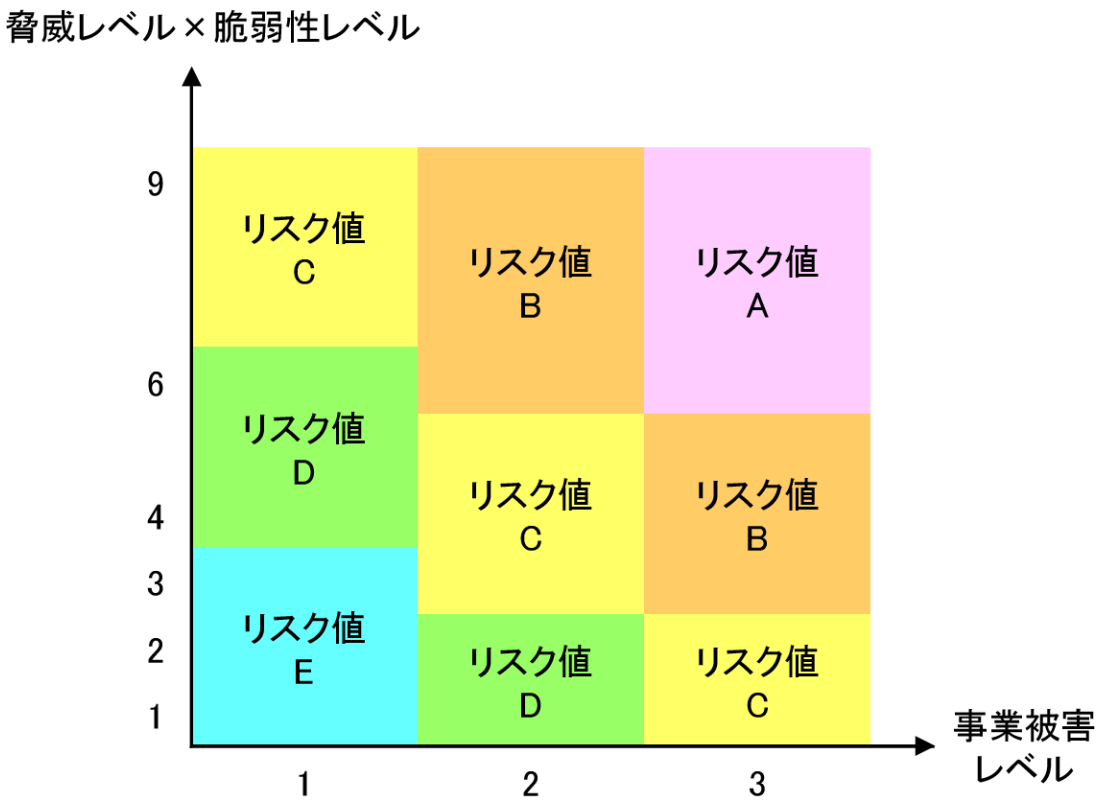


図 4-35 脅威レベル・脆弱性レベル・事業被害レベルとリスク値の関係

図 4-36 に、リスク値の記載例を示す。例えば、攻撃ツリー#6 であれば、「脅威レベル」＝「1」、「脆弱性レベル」＝「2」、「事業被害レベル」＝「3」のため、表 4-51 から「リスク値」＝「C」となる。また、攻撃ツリー#7 であれば、「脅威レベル」＝「2」、「脆弱性レベル」＝「2」、「事業被害レベル」＝「3」のため、表 4-51 から「リスク値」＝「B」となる。

以上により、事業被害ベースのリスク分析シートが完成した。本節にて行った分析結果を元に、5 章にてその活用方法を述べる。

【コラム】

攻撃ツリーの絞り込みの考え方のまとめ

全ての攻撃ツリーを評価することは、工数的制約の下で、現実的でないケースが出てくるものと考えられる。事業被害ベースのリスク分析における攻撃ツリーでの評価は、机上でのペネトレーションテストに相当するが、ペネトレーションテストにおいても全ての攻撃ルートをテストするのは工数的にも非現実的である。

ここでは、攻撃ツリーを絞り込んでいく考え方、論点を整理しておく。攻撃ツリーは、「事業被害→攻撃シナリオ→侵入口→攻撃ツリー」の手順で検討、構成していくので、その上位から絞り込みを実施することが自然かつ効果的である。従って、その手順は以下となる。(1)～(3)の絞り込みを経て、評価の対象とする事業被害、攻撃シナリオ、侵入口が特定される。それらを対象に、攻撃ツリーを構成することになるが、攻撃ツリーの策定にあたって、攻撃ルート／攻撃ツリーを絞り込んでいく考え方が(4)となる。

(1)事業被害の絞り込み: 最も回避したい事業被害に対象を限定する。
事業被害レベル等を参考に検討する。
(2)攻撃シナリオの絞り込み: 最も回避したい攻撃シナリオに対象を限定する。
資産ベースのリスク分析結果も参考にし、攻撃の容易性等を考慮して検討する。
(3)侵入口の絞り込み: 資産ベースのリスク結果も参考にし、侵入の可能性の高い
侵入口に対象を限定する。

(4)攻撃ルート／攻撃ツリーの絞り込み:
絞り込みにおいて、優先的に評価対象とする攻撃ルートの考え方を列挙する:
① 最短の攻撃ルートを優先する
② 通常運転でのデータフローに存在している攻撃ルートを優先する
③ 攻撃者の視点で、現実的な(より容易な)攻撃ルートを優先する
④ 防御側の視点で、防御が弱い攻撃ルートを優先する
優先度を下げる考え方を列挙する:
⑤ 別の攻撃ルートの迂回ルートは優先順位を下げる
⑥ 別の攻撃ルートのスーパーセットになっている攻撃ルートは省略する
(別の攻撃ルートでの評価で、スーパーセットの評価を代替できる)

※ 初回のリスク分析で絞り込んで省略した攻撃ツリーは、PDCA サイクルを回す中で、
次回以降のリスク分析での評価の必要性を見直すことが重要である。

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	評価指標 脆弱性レベル	評価指標 事業被害レベル	リスク値	対策 防御 侵入／拡散段階		対策 防御 目的遂行段階		対策 検知／被害把握		対策 事業継続		対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ（項番）
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。																
14		マルウェアが、ファイアウォールからHMI（操作端末）に不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	○	機器異常検知				2			
							通信相手の認証		アクセス制御	○	ログ収集・分析	○						
							操作者認証	○										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	○										
15		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3	B			データ署名		機器異常検知	○			1	2	#4	1,11,12,13,14,15
									重要操作の承認		ログ収集・分析	○						
16		マルウェアが、ファイアウォールから制御サーバに不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	○	機器異常検知				2			
							通信相手の認証		アクセス制御	○	ログ収集・分析	○						
							操作者認証	○										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	○										
17		マルウェアが、制御サーバ上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3	B			データ署名		機器異常検知	○			1	2	#5	1,11,12,13,16,17
									重要操作の承認		ログ収集・分析	○						
18		マルウェアが、ファイアウォールからデータサーバに不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	○	機器異常検知				2			
							通信相手の認証		アクセス制御	○	ログ収集・分析	○						
							操作者認証	○										
							アンチウイルス											
							ホワイトリストによるプロセスの起動制限	○										
19		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェア感染させる。					パッチ適用		権限管理		機器異常検知	○			1			
							通信相手の認証		アクセス制御		ログ収集・分析	○						
							操作者認証											
							ホワイトリストによるプロセスの起動制限											
20		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	1	2	3	C			データ署名		機器異常検知	○			1	2	#6	1,11,12,13,18,19,20
											ログ収集・分析	○						
21		**侵入口＝情報ネットワーク（FW）** 悪意のある第三者が、情報ネットワークからファイアウォールに不正アクセスする。					FW（パケットフィルタリング型）	○	権限管理	○	ログ収集・分析	○			2			
							パッチ適用		アクセス制御	○								
							通信相手の認証											
							操作者認証	○										
22		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。					項番4と同じ								2			
23		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2	2	3	B	項番5と同じ								1	2	#7	21,22,23
24		悪意のある第三者が、HMI（操作端末）をマルウェアに感染させる。					パッチ適用				機器異常検知				2			
							アンチウィルス				ログ収集・分析	○						
							ホワイトリストによるプロセス起動制限	○										
25		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3	B	項番15と同じ								1	2	#8	21,22,24,25

図 4-36 事業被害ベースのリスク分析シート（リスク値の記入例）

このページは空白です。

【補足 1】システム構成資産の追加調査結果

表 4-52 システム構成資産とその役割の追加調査結果(1/5)

名称	説明 ※	機能	データの種類と経路	定常/非定常
監視端末	1. プロセスや現場の状況を確認するための端末。 2. 監視端末から制御ネットワーク内の機器にアクセスする業務フローはない。 3. 保有データの改ざんや機能停止による事業継続への直接的な影響はない。	入出力	長期トレンドデータ: データヒストリアン→(監視端末)	定常
データヒストリアン	4. 長期間のプロセス値や管理パラメータが保存され分析されるサーバ。 5. データサーバより静的なデータを扱う。 6. 保有データの改ざんや機能停止による事業継続への直接的な影響はない。	データ保存	プロセス値: データサーバ→(データヒストリアン)→監視端末	定常
HMI (操作端末)	7. 制御機器やフィールド機器に対する指示を入力する端末。 8. 広域供給停止コマンド(予め決められた対象エリアへの供給を一括して停止するコマンド)を発行可能(発行自体は制御サーバ経由)。 9. 機能停止してもフィールド機器の直接操作により事業継続可能。	コマンド発行	設定値: (HMI)→制御サーバ プロセス値: データサーバ→(HMI)	定常

※ 3.1 節(表 3-8)に対して追加調査で得られた情報を赤字で追記。

表 4-53 システム構成資産とその役割の追加調査結果(2/5)

名称	説明 ※	機能	データの種類と経路	定常/非定常
制御サーバ	10. 制御機器やフィールド機器に対し設定値やコマンドを送出するサーバ。 11. 広域供給停止コマンドを発行可能。 12. 改ざんされると、システム障害が発生し、広域供給停止を引き起こす可能性のある重要なデータ(★★データ)を保有。 13. 機能停止すると事業継続に影響を及ぼす。	コマンド発行	制御コマンド、設定値: HMI→(制御サーバ)→PLC	定常
データサーバ	14. 制御ネットワーク上にありプロセス値を収集するサーバ。 15. 更に PLC から届いたプロセス値を転送する。 16. 改ざんされると、不正なデータが HMI(操作端末)に表示され、オペレータが誤って広域供給停止コマンドを発行する可能性のある、重要なデータ(■■データ)を保有。 17. 機能停止すると事業継続に影響を及ぼす。	データ保存	プロセス値: PLC→(データサーバ)→データヒストリアン→監視端末	定常

※ 3.1 節(表 3-8)に対して追加調査で得られた情報を赤字で追記。

表 4-54 システム構成資産とその役割の追加調査結果(3/5)

名称	説明 ※	機能	データの種類と経路	定常/非定常
PLC	18. センサからの信号により接点や操作器を制御する等入出力信号を扱うフィールド機器。 19. 制御サーバやデータサーバと PLC との間の通信を中継する PLC も存在し、中継する側を「PLC(マスター)」、中継される側を「PLC(スレーブ)」と示す。 20. 改ざんされると、システム障害が発生し、供給停止を引き起こす可能性のあるデータ(ラダープログラム)を保有。 21. 機能停止すると、安全機構の発動により供給が停止する。 22. PLC(マスター)は、上位システムからの供給停止コマンドを、下位の PLC(マスター)に中継して発行。 23. PLC(マスター)の下位には、広域供給停止を引き起こしうる数の PLC(スレーブ)が存在。	コマンド発行	コマンド: 制御サーバ→(PLC)→フィールド機器 プロセス値: フィールド機器→(PLC)→データサーバ	定常

※ 3.1 節(表 3-8)に対して追加調査で得られた情報を赤字で追記。

表 4-55 システム構成資産とその役割の追加調査結果(4/5)

名称	説明 ※	機能	データの種類と経路	定常/非定常
ルータ／スイッチ	24. 複数のネットワークを集線、中継する機器。 25. 機能停止してもフィールド機器の直接操作により事業継続可能。	ゲート	メール、Web 等: インターネット→(各スイッチ／ルータ)→情報ネットワーク 長期トレンドデータ: 情報ネットワーク→(各スイッチ／ルータ)→DMZ	定常
ファイアウォール(FW)	26. 外部のネットワークからの攻撃や侵入を防ぐための機能を有する機器。 27. 設定情報を改ざんされると、攻撃や侵入を許す可能性がある。 28. 機能停止してもフィールド機器の直接操作により事業継続可能。	ゲート	長期トレンドデータ: DMZ→(FW)→情報ネットワーク プロセス値: 制御ネットワーク→(FW)→DMZ	定常
パッチサーバ	29. 接続された機器の OS やソフトウェアのアップデートやパッチ、アンチウイルスのパターンファイル等を提供するサーバ。 30. 保有データの改ざんや機能停止による事業継続への直接的な影響はない。 31. 非定常稼働機器により、今回のリスク分析対象外。	データ保存	パッチデータ: インターネット、または情報ネットワーク上のパッチサーバ→(パッチサーバ)→データヒストリアン	非定常
EWS	32. PLC のラダープログラムの改造や制御サーバのプログラムの変更等を行うためのコンピュータ。 33. 保有データの改ざんや機能停止による事業継続への直接的な影響はない。 34. 非定常稼働機器により、今回のリスク分析対象外。	データ保存、コマンド発行	プログラム: プログラム入手先→(パッチサーバ)→PLC、またはフィールド機器等	非定常

※ 3.1 節(表 3-9)に対して追加調査で得られた情報を赤字で追記。

表 4-56 システム構成資産とその役割の追加調査結果(5/5)

名称 ※	説明 ※	機能	データの種類と経路	定常/非定常
保守用 PC	35. PLC やフィールド機器のメンテナンスを行うためのコンピュータ。 36. 保有データの改ざんや機能停止による事業継続への直接的な影響はない。 37. 非定常稼働機器により、今回のリスク分析対象外。	コマンド発行	制御コマンド等: (保守用 PC)→PLC、またはフィールド機器	非定常
その他の追加情報[37]	38. 制御システム機器が設置されている事業者敷地、建屋、部屋(サーバ室、計器室)、ラック等には、物理的対策(警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等)が実施されている。 39. 事業者敷地外のフィールド機器は、鍵付きのコンテナや設置箱等の中に設置されている。 40. 制御システム機器にアクセスできる人間は、物理的・論理的に、必要最低限の内部関係者に制限されている。 41. 事業者では、内部不正対策(教育)が実施されている。	―	―	―

※ 3.1 節(表 3-9)に対して追加調査で得られた情報を赤字で追記。

[37] こうした物理セキュリティや運用管理状態のセキュリティに関わる事項や、表 4-52～表 4-56 に示したシステム資産の役割に伴うセキュリティに関わる事項は、リスク分析を進める中で、システムの詳細の確認や現場の構築・運用関係者のヒアリング等を通して明らかになってくる。こうした情報は、システムのセキュリティの状況をより詳細に把握する上で非常に重要である。また、これらの情報は、リスク分析において現実的な脅威となる攻撃シナリオや攻撃ツリーを構成し、かつ工数の制約上の絞り込みを検討する上で不可欠な情報であり、脅威レベルをより正確に評価する上でも有効な情報となる。

【補足 2】物理アクセスによる攻撃の侵入口

物理アクセスによる攻撃の侵入口は、攻撃拠点への物理アクセス以外に、攻撃拠点と同じ制御ネットワーク上にある機器や制御ネットワーク以外のネットワーク上の機器に物理アクセスし、そこから攻撃拠点にアクセスしてくることも考えられる。しかし、制御ネットワーク上や制御ネットワーク以外のネットワーク上の機器に物理アクセスしての攻撃は、攻撃ルート的にネットワーク経由の攻撃の攻撃ルートと重複する可能性がある。例として制御サーバを攻撃拠点、監視端末と HMI（操作端末）を侵入口とした場合の攻撃ルートを、図 4-37 に示す。

図に見る様に、制御サーバへの攻撃にあたって監視端末を物理アクセスによる攻撃の侵入口とした場合（①）、結果的に侵入後の攻撃ルートは監視端末をネットワーク経由の攻撃の侵入口とした場合（②）と同じとなる（③）。従って、攻撃ルートとしては、ネットワーク経由の攻撃（②）の評価によってカバーしていると見なすことができる。

HMI（操作端末）を侵入口とする場合（④）も、同じネットワーク内の機器とはいえネットワーク越しの攻撃となることから、結果的にネットワーク経由（②）の攻撃によってカバーしていると見なすことができる。

【コラム】

物理アクセスによる侵入口から除外した機器の、物理アクセスによる攻撃への対策状況の確認

監視端末と HMI（操作端末）を制御サーバへの攻撃の物理アクセスによる攻撃の侵入口から除外することで、リスク分析に漏れが生じる可能性があるとすれば、監視端末または HMI への物理アクセスによる攻撃への対策状況である。これらのリスクは、別の攻撃シナリオで監視端末や HMI（操作端末）を攻撃拠点とする最終攻撃が存在すれば、監視端末や HMI（操作端末）を物理アクセスによる攻撃の侵入口とする攻撃ルートが間違いなく分析対象として出現するため、そちらの攻撃シナリオ／攻撃ルートでカバーできる。また、そうした攻撃シナリオ／攻撃ルートが存在しない場合でも、資産ベースのリスク分析によって、個別には確認されることになる。

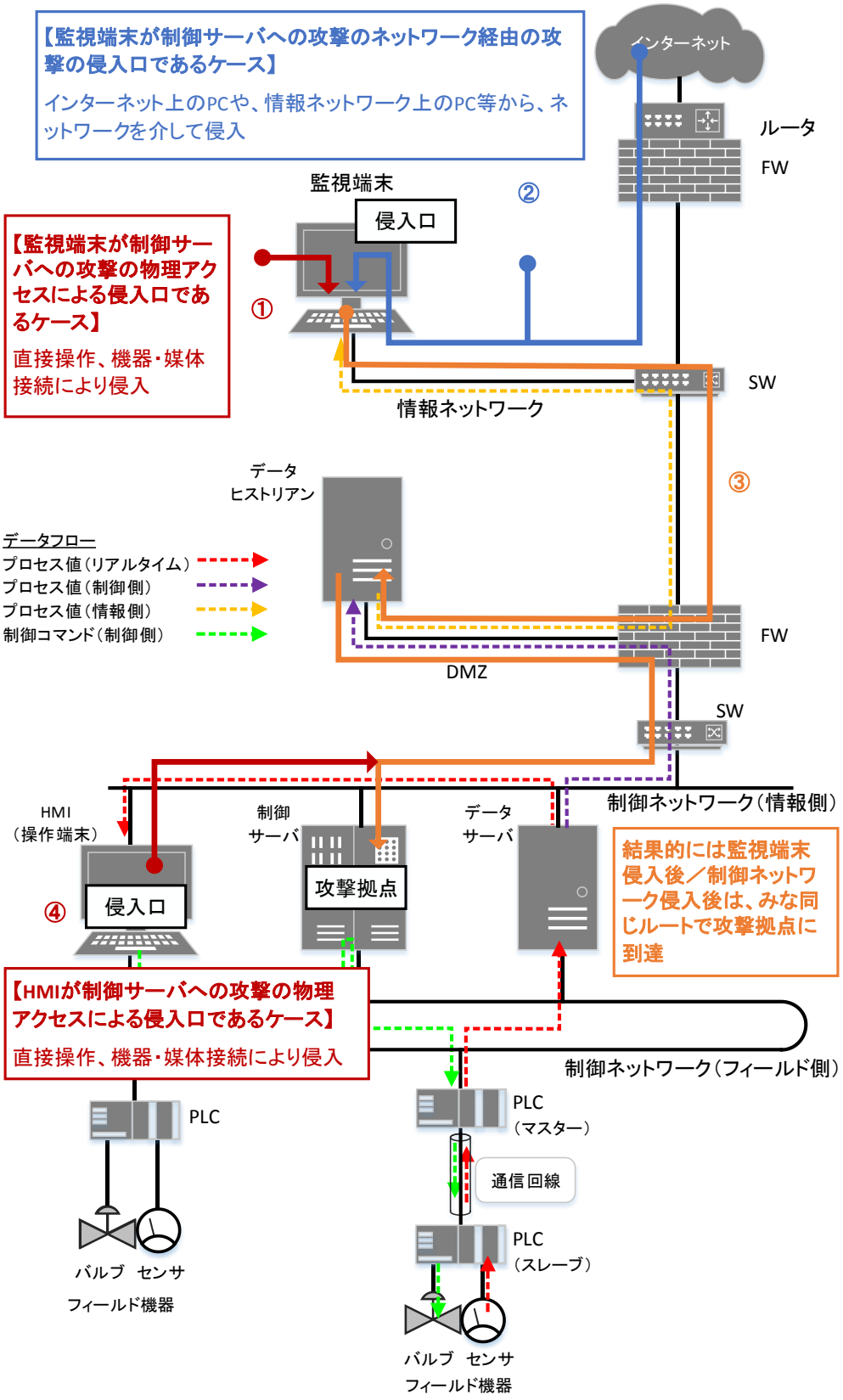


図 4-37 物理アクセスによる攻撃とネットワーク経由の攻撃の攻撃ルートの重複の例

【補足 3】攻撃ルートの簡易探索法

大きな事業被害につながる可能性のある資産の洗い出しや多層防御を利用した対策を検討するため、事業被害ベースのリスク分析を実施することは効果的である。しかしながら、リスク分析を行うリソースを十分に確保できない場合には、ここに記載する簡易探索法を参考にして探索した攻撃ルートの分析のみを実施し、全体工数を削減する手段がある。

この探索法は、攻撃者は、最も攻撃の手間がかからないルートで攻略しようとするという考えに基づいている。換言すると、システムの有するデータフローやコマンドや機能を悪用するということで、これは前述した資産ベースのリスク分析を実施しシステムに対する理解が深まった者にとっては、それ程難しい作業ではないと思われる。図 4-38 に、攻撃ルートの簡易探索法を示す。

攻撃ルートを考える手順は以下の通り。

① 攻撃対象の把握： 事業被害レベルが 2 または 3 といった大きな被害を引きおこす元となる攻撃対象を見つける。
② 攻撃拠点の把握： ①の攻撃対象に手間をかけず被害を与えることのできる攻撃拠点を見つける。
③ 侵入口の把握： そのシステムの侵入口を特定する。
④ 攻撃ルートの抽出： 侵入口から攻撃拠点、攻撃対象へのルートを抽出する。
⑤ リスク値のリストアップ： 資産ベースのリスク分析の結果から
(ア) 侵入口の資産については入口に対する脅威についてのリスク値を拾ってくる（リスク値が B,C 等）。
(イ) 攻撃対象に至るまでの資産では、経由に対する脅威についてのリスク値を拾ってくる。
(ウ) 攻撃拠点、攻撃対象の資産では、被害を生じさせる動作に対するリスク値を拾ってくる。
⑥ リスク値の計数化： ④で求めたリスク値を A→1, B→2, C→3, D→4, E→5 として数値に置き換え、システム構成図にマッピングする。
⑦ 積の計算： 侵入口～攻撃拠点～攻撃対象で考えられる複数のルートで⑤でマッピングした数値を拾ってきて、積を求める。
⑧ 攻撃ルートの決定： 積の値が最も小さい攻撃ルートで、セキュリティ対策を検討する。これは積の大きさが攻撃のコスト（容易性）の相対的な目安となっていることを応用している。

この様な手順でいくつかの事業被害に対して攻撃ツリーを考えて、要所の検証と対策を行う。

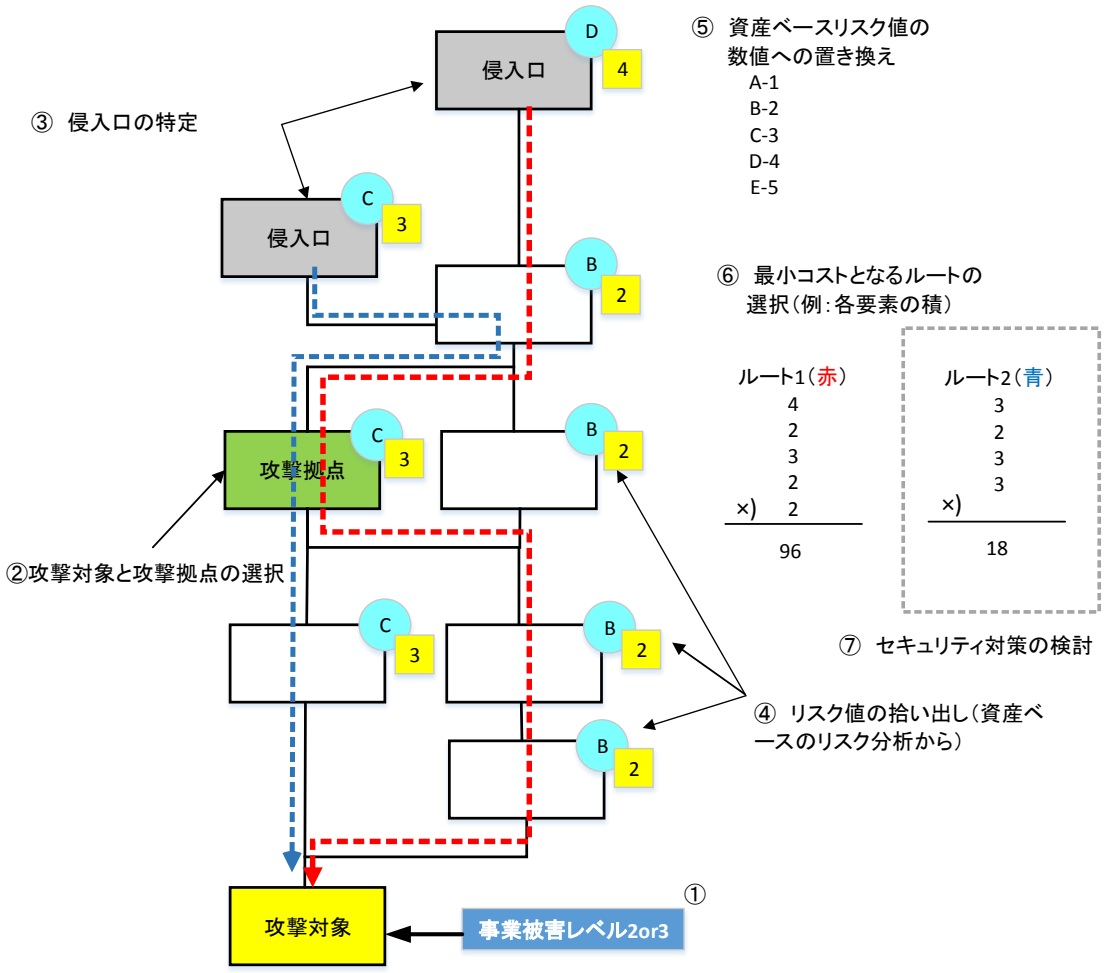


図 4-38 攻撃ルートの簡易探索法

5. リスク分析結果の解釈と活用法

本章では、リスク分析の実施結果の解釈と活用の仕方について説明する。

4 章までに示したリスク分析を実施した結果として、

- 資産ベースのリスク分析結果である資産ごとのリスク値
- 事業被害ベースのリスク分析結果である事業被害レベルの値と攻撃ツリーのリスク値

が得られた。

リスク分析結果の解釈及び活用のねらいは、制御システムのセキュリティ上の弱点を見つけ、サイバー攻撃に対するリスクを低減することにある。そのためには、得られたリスク値を可能な限り低減することが理想的ではあるが、コスト上の制約や有効な対策が見当たらない、システムの稼働状態等の理由から現実的には難しい。以下では、上記の結果の有効な活用の仕方について説明する。

これらのリスク値は以下の内容に活用することができる。

① **リスクの把握**:
対象システムにおけるリスク値の分布と、総合的なリスクのレベルを把握することができる。資産ベースのリスク分析においては、資産ごとのリスク値を、事業被害ベースのリスク分析においては、大きな事業被害をもたらす攻撃ごとのリスク値を把握することができる。

② **改善箇所の抽出、選定**:
全体のリスク値を低減するためには、まずリスク値が高い部分を抽出、選定してその改善を検討することが最も効果的である。資産ベースのリスク分析においては、リスク値の高い資産を、事業被害ベースのリスク分析においては、大きな事業被害をもたらす攻撃シナリオと攻撃ツリーを抽出、選定することができる。

③ **リスクの低減**:
資産ベースのリスク分析シートを用いて、改善箇所として選定した資産に対して、リスク値を高くなっている脅威に対する、追加すべき対策項目を検討することができる。事業被害ベースのリスク分析シートを用いて、改善箇所として選定した攻撃シナリオと攻撃ツリーに対して、そのリスク値を低減するために効果的な、対策箇所（攻撃ステップ）と追加すべき対策項目を検討することができる。この検討にあたっては、追加すべき対策項目の優先順位を判断することができる。

④ **リスクの低減の効果の把握**:
③で検討した追加すべき対策項目を実施した場合、各対象箇所のリスクの低減とシステム全体におけるリスクの低減として期待される効果を、定量的に把握することができる。また、実際

に追加対策を実施した後、期待通りの効果が得られたか否かを、定量的に確認することができる。

⑤ **セキュリティテストの対象箇所の抽出、特定**:
リスク分析結果と追加対策によるリスクの低減効果を基に、実システムにおけるセキュリティテストの必要性の有無の検討を行う。セキュリティテストについては 6 章で詳細を説明するが、本番環境、模擬環境等の実機環境を用いた各種のテストのことを指す。これらのテストは、現状のシステム上の不備や机上評価の限界を補うために有効ではあるが、非常に時間とコストがかかるだけでなく、稼動システムへの影響も十分に考慮しなければならない。従って、リスク分析の結果を活用して、攻撃の懸念が高く、かつ実機での検証が必要と判断される箇所や攻撃を抽出、特定して実施を検討することが、現実的な対応となる。

上記の①～⑤のそれぞれは、制御システムの抜本的なセキュリティの向上を図る上で、重要な項目となる。また、④は、追加対策(コスト)の必要性と有効性を組織幹部に説明する上でも不可欠な項目となる。

以下の各節では、資産ベースのリスク分析と事業被害ベースのリスク分析のそれぞれの結果の活用法を解説する。

- 資産ベースのリスク分析の活用法 (☞ 5.1 節)
- 事業被害ベースのリスク分析の活用法 (☞ 5.2 節)
- 資産ベース・事業被害ベースのリスク分析の活用法の違いと相関 (☞ 5.3 節)
- 継続的なセキュリティ対策の実施(PDCA サイクル) (☞ 5.4 節)

各リスク分析結果の活用にあたっては、勿論個別でも有効ではあるが、二つのリスク分析は相互補完的な関係にあり(2.1 節参照)、それを 5.3 節で説明する。また、このリスク分析の結果の活用は上述した①～⑤のポイントにとどまらず、制御システムの事業者が今後継続的にセキュリティの維持と向上を図っていく上で基盤となることを、5.4 節で解説する。

5.1. 資産ベースのリスク分析の活用法

(1)リスクの把握

- リスク値とリスクの高さ
  資産ベースのリスク分析のリスク値はA～Eのレベルで評価し、Aが最もリスクが高い。
  資産ベースのリスク分析における「リスク値が高い」という分析結果は、重要な資産において発生する可能性が高い脅威に対して、対策が不十分であることを意味する。

- 資産ベースのリスク分析のリスク値の算定
  4.1 節(表 4-25)の算定基準に示した通り、資産ベースのリスク分析のリスク値は、一つの資産における様々な脅威(攻撃手法)に対する脅威レベルと脆弱性レベル(対策の不十分さ)と、資産の重要度からリスク値を算定する。即ち、ある資産において、それぞれの脅威(攻撃手法)について脅威レベルと脆弱性レベルがそれぞれ定まり、リスク値も攻撃手法ごとに算定する。

  例えば、重要度2のある資産において、不正アクセスという脅威(攻撃手法)に対しては、脅威レベルが 2、脆弱性レベルが 3、このときのリスク値は B と算定される。資産ベースのリスク分析では、資産単体の脅威(攻撃手法)に対しての強度がわかり、その弱点を埋める事で、当該資産のセキュリティを高めていくことができる。

(2)改善箇所の抽出、選定

- 基本的な改善の考え方
  資産ベースのリスク分析では、基本的にそれぞれの脅威(攻撃手法)に関して評価されたリスク値の中で高いリスク値を低減することにより、セキュリティを向上させることになる。

- 資産ベースのリスク分析での改善箇所の抽出・選定
  4.1節で示した資産ベースのリスク分析シートの完成例(図 4-2)の一部を、図 5-1 に示す。資産ベースのリスク分析では、基本的に高いリスクの箇所を抽出する。
  例えば、制御サーバに対して、リスク値 A の不正媒体・機器接続の脅威を抽出する(図中①)。

対象装置	評価指標				脅威(攻撃手法)	説明	② 対策	
	脅威レベル	脆弱性レベル	資産の重要度	リスク値			防御	
							侵入/拡散段階	
制御サーバ	2	2	3	B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型)	
							FW(アプリケーションゲートウェイ型)	
							一方向ゲートウェイ	
							プロキシサーバ	
							WAF	
							通信相手の認証	○
							IPS/IDS	
							パッチ適用	
							脆弱性回避	
	2	1		C	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。 あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理 (ICカード、生体認証)	○
							施錠管理	○
	2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass)	○
	2	④ 3		① A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限 ③	

図 5-1 資産ベースのリスク分析シート(抜粋)

(3)リスクの低減

リスク値を低減するためには、基本的にセキュリティ対策を強化し、脆弱性を低減させる必要がある。脆弱性レベルを低減するためには、資産ベースのリスク分析シートに記載した対策候補の中で、未実施の対策項目について、当該資産に対する有効性、実施の可能性、コスト等を勘案して、対策を選定する。

資産ベースのリスク分析シート(図 5-1)では、脅威(攻撃手法)ごとにその対策項目と実施の有無が記載されている(図中②)。リスク値を改善するには、その追加対策を検討して対策レベルを上げる。例えば、不正媒体・機器接続という脅威(攻撃手法)に対するリスク値(図中①)を改善するためには、未実施対策であるデバイス接続・利用制限(図中③)を追加実施する。その結果、対策レベルの双対の値である、評価指標「脆弱性レベル」(図中④)を 3→2 に低減することで、リスク値が A→B に低減される。

資産ベースのリスク分析結果を活用した追加対策の検討表の例を、表 5-1 に示す。本表は、各資産における高リスクの脅威を洗い出し、それぞれの脅威(攻撃手法)に対して、資産ベースのリスク分析シートの対策欄から選択した、想定される対策案を記している。例えば、図 5-1 の対策③は本表の No.2 に対応する。また、対策コスト、対策によるリスク値の低減効果、及びそれらを考慮して決定した優先度等をまとめ、最終的な改善の記録を記している。改善方法の欄でシステムと運用と分けて実施内容を記載しているのは、分析シートに記録されているシステム(資産)の改善以外に運用面での改善がなされている場合の記録を残すためである。

表 5-1 での優先度の付け方は分析者の判断次第であるが、基本的に資産の重要度が高い資産に対する追加対策、あるいは、脅威×脆弱性の値が高い(例えば 6 以上の)項目に対する追加対策を優先的に検討すべきである。これらの条件に加えて、例えば、対策コスト、システムや周囲の機器への影響度、資産のリプレースやメンテナンスのタイミング等が、追加対策の優先度を決定する際の判断材料となる。また、運用上対策が困難であるため優先度を下げた No.1, No.6 や、同じく対策のコスト面から下げた No.4 に対しては、備考欄に今後の検討事項等を記載している。

表 5-1 資産ベースのリスク分析結果を活用した追加対策の検討表例

No.	資産名	高リスク値の脅威	リスク値	想定される対策	「効果」対策後リスク値	推定対策コスト	改善方法		優先度	改善実施	備考
							システム	運用			
1	制御サーバ	マルウェア感染	A	パッチ適用	B	高	○		低	×	負荷の検討が必要
2		不正媒体・機器接続	A	デバイス接続・利用制限	B	低	○		高	○	
3		情報改ざん	A	アクセス制御	B	低	○	○	高	○	アカウント管理徹底
4	HMI(操作端末)	不正操作	A	操作者認証(2 要素)	C	高		○	低	×	方法を検討中
5		不正媒体・機器接続	A	デバイス接続・利用制限	C	低	○		高	○	持ち込み管理徹底
6		プロセス不正実行	A	ホワイトリスト	B	高	○		低	×	実現可能性を調査中

(4)リスクの低減効果の把握

前述した様に、資産ベースのリスク分析では、各資産の様々な脅威(攻撃手法)に対するリスク値を算定する。

対策前と対策後の効果を可視化するのに、レーダーチャートを利用するのが適している。

図 5-2 は、ある資産に対する各種の脅威(攻撃手法)に関しての、リスク低減対策前／対策後の対策レベルを示すレーダーチャートの例で、チャートの面積が大きいほど対策がなされていることになる。この図では枝の1本1本が脅威に相当し、対策レベルは枝の目盛りに相当する。ここで例えば、対策前には物理的侵入・操作という脅威に対する対策レベルは対策前に 1 であったが(図中①)、対策後はレベル 2 に上がったという表現で種々の脅威に対して対策の効果が把握できる。

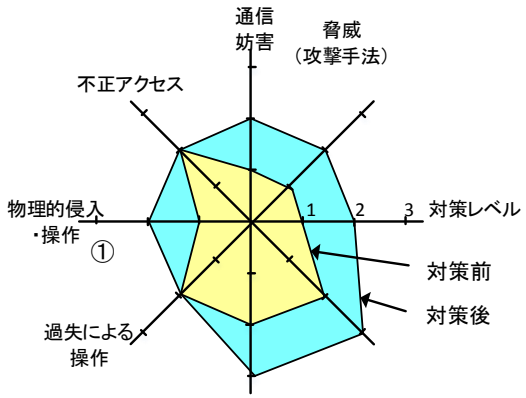


図 5-2 ある資産に対する各種の脅威と対策レベル(対策前／対策後)

図 5-3 に、資産ベースの分析によるシステム資産全体に対するリスク値の分布図の例を記す。この様に、システム全体のリスク値の改善効果を把握するには、リスク値ごとのヒストグラムを作成するのがわかりやすい。リスク値ごとの分布を見て例えばリスク値 A, B といった高リスク値の件数がどれだけ減少したかという評価を行う。更に改善後も、高いレベルのリスク値が残留している箇所(例えば、図 5-3 におけるリスク値 A の 2 件、リスクと B の 6 件)を認識し、今後の継続的なリスク分析の実施時に役立てていく。

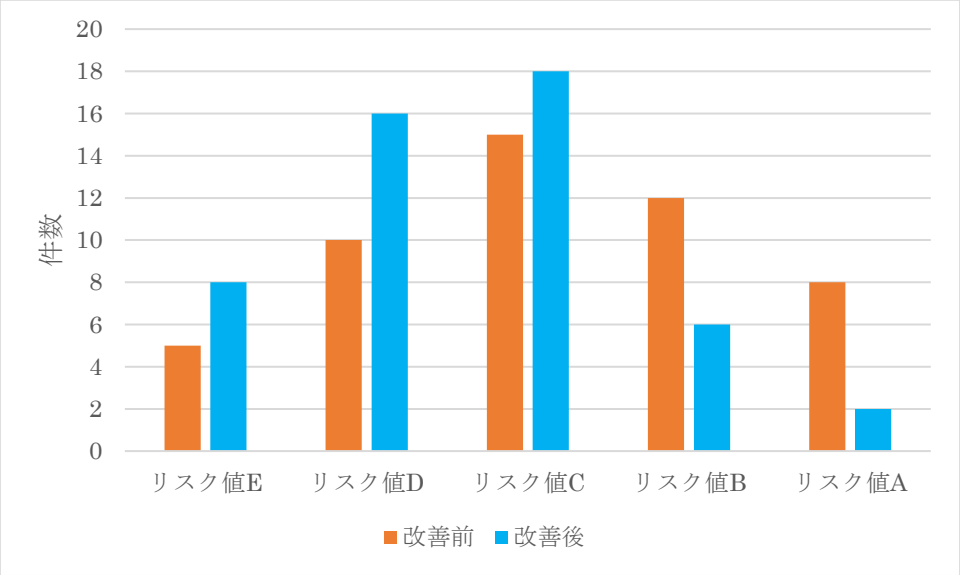


図 5-3 リスク値のヒストグラム（資産ベースの分析）

(5)テスト・検証箇所の抽出・特定

表 5-2 に、リスク分析結果を受けて実施するテストの目的とテスト対象を示す。サイバー攻撃に対するセキュリティ強度の実システム(本番環境または模擬環境)における確認手法として、脆弱性検査、ペネトレーションテスト、パケットキャプチャテストが挙げられる。各手法の詳細は 6 章で説明するが、これらのテストのうち、脆弱性検査とパケットキャプチャテストは特定の資産や箇所に対してのテストであり、ペネトレーションテストはネットワークを介しての侵入や攻撃が可能(成功する)かをテストするもので、いずれも固有のツールの利用や専門家によるマニュアル(手作業)等によって実施される。

表 5-2 主なテストの目的とテスト対象

テスト種類	目的	テスト対象
脆弱性検査	資産に既知や未知の脆弱性がないか確認する	個々のシステム資産
ペネトレーションテスト	様々な攻撃手法でシステムへの侵入、不正な操作ができないか確認する	ネットワークの界面とネットワーク内の制御端末や重要サーバ等の資産
パケットキャプチャテスト	想定外の通信や操作が行われていないか確認する	制御ネットワーク

資産ベースのリスク分析においては、個々の資産ごとのリスク値が評価でき、それを受けリスク値を下げるため、追加対策を実施する(本節の(1)~(4))。しかし、以下の様な様々な事由で、対策が見送られてリスク値が高いままの機器も残るケース(リスクの保有)や、リスク値はある程度まで低減する措置をとったが、十分には下げきれていないケース等もある。

- システムの可用性上、セキュリティパッチをあてることは、実施を見送った
- システムの制約上、セキュリティ対策の機能を追加することができなかった
- 対策コスト面の事情から、実施を見送った
- 外部のネットワークの境界面に近い対策を優先して実施し、内部の対策は見送った

そうしたケースでは、対策の必要性を再認識するためには、実システムに対するテストを実施することが選択肢として出てくる。資産ベースのリスク分析の結果を受け、各資産のリスク値と脅威レベルを考慮して、以下の観点からテストの対象とする資産を抽出、特定することが可能である。

① 外部との境界面に位置しているネットワーク装置等の資産
② 重要な処理が可能な操作端末
③ 保守要員等、外部の要員が操作する可能性のある端末

④　重要度の高い資産（サーバ類等）で、リスク値レベルを十分に下げられていない資産

実施するテストとしては、以下が挙げられる：

- 脆弱性検査：　攻撃に備えての資産に存在している脆弱性の検査
- パケットキャプチャテスト：　ネットワークの入口や重要な資産とその周辺等で、現行の稼動システムへの想定外の通信や操作が発生していないかを検証

後者は、運用中のシステムへの攻撃の発生の有無、あるいは既にマルウェア感染が発生していないか、内部不正の兆候がないか等、脅威の存在の検証を行う位置付けである。いずれのテストも、本番環境において実施する場合には、運用への支障や性能面での影響等も合わせて考慮する必要がある。また、本番環境でのテストで困難が予想される場合には、模擬環境や機器単体でのテストを検討することになる。

5.2. 事業被害ベースのリスク分析の活用法

(1)リスクの把握

- リスク値とリスクの高さ

  事業被害ベースのリスク分析のリスク値は、資産ベースのリスク分析と同様に A～E のレベルで評価し、A が最もリスクが高い。

  事業被害ベースのリスク分析における「リスク値が高い」という分析結果は、事業被害が大きく、発生する可能性が高い脅威に対して、対策が不十分であるということを意味する。

- 事業被害ベースのリスク分析におけるリスク値の解釈

  事業被害ベースのリスク分析では、事業被害を生じさせる攻撃シナリオとそのシナリオを引き起こす攻撃ツリーを作成し、そのリスク値を算定する。即ち、どういった攻撃ルートで、どの様な攻撃シナリオで攻撃が行われた場合、どれ程の事業被害が生じるかを把握することができる。

  リスク値の大きな攻撃ツリーが特定できると、その攻撃ツリー上の攻撃ステップのどこか最低 1 か所でも攻撃を止められれば、その攻撃ツリーのリスク値は低減する。資産ベースの分析では評価できない、複数の資産にまたがる攻撃に対して、効率的に対策箇所を検討・特定しやすいという利点がある。

  この事業被害ベースのリスク分析は、システムと機能構成やデータフロー等を前提に、机上での仮想的なペネトレーションテスト[38]を実施していることに相当する。

[38] ペネトレーションテストについては、6 章(6.4 節)を参照。

（2）改善箇所の抽出、選定

- 基本的な改善の考え方

  事業被害ベースのリスク分析は、攻撃ツリー単位でリスク値が算定されるため、基本的に高いリスク値を持つ攻撃ツリーのリスク値を低減することにより、セキュリティを向上させることになる。また、リスク値の高い複数の攻撃ツリーを洗い出して、共通する攻撃ルートの上流の経路上や機器等において、一つの対策によって効果的に改善できる箇所がないかも含め検討する。

  図 5-4 の改善案1は、攻撃ツリーの改善案の例を示す。攻撃ツリーの改善は、ツリーを構成する各攻撃ステップにある資産の中から対策可能なものを選び対策レベルを改善する方法（改善案1-攻撃ルート A）や、ツリー内の特定の場所にセキュリティ対策を追加し改善する（改善案1-攻撃ルート B）方法がある。

- 事業被害ベースのリスク分析での改善箇所の抽出・選定

  改善箇所は改善案2-攻撃ルート A の様に、攻撃ツリー内の一つの機器で改善するだけでなく、複数の機器で改善する事も検討し、併せて、前述した他の高リスク値の攻撃ツリーも含めて、どこを改善するのが効果的かという視点で改善箇所を検討する。改善案3は、2 つの攻撃ルート A、B に共通の攻撃ステップ2を改善することで、両ルートのセキュリティ対策となっている。

  4.2 節に示した事業被害ベースのリスク分析シート（図 4-34）の一部（攻撃ツリー番号#4～#6）を、図 5-5 に記す。ここに示されている攻撃ツリーのリスク値は、評価指標の欄を見ると B（図中①）と C（図中②）となっている。相対的にリスク値が高い攻撃ツリー（図中①）を改善必要箇所とすると、2 つの攻撃ツリー（図中③④）が抽出される。これらの攻撃ツリーは複数の攻撃ステップから構成されており、改善箇所はそのステップの中で対策が不十分である箇所、有効な対策がしやすい箇所となる。これは攻撃ツリー／攻撃ステップの内容から判断を行う。

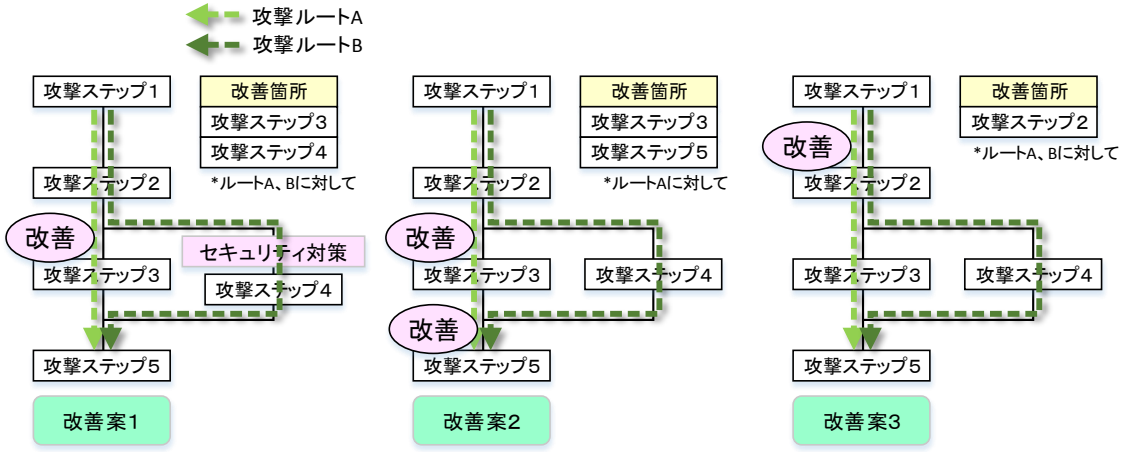


図 5-4 攻撃ツリーの改善案の検討例

事業被害ベースのリスク分析シート

1．広域での〇〇供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階		目的遂行段階		検知／被害把握		事業継続		対策レベル 攻撃ステップ	攻撃ツリー
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。														
1		**侵入口＝監視端末** 悪意のある第三者が、情報ネットワーク上の監視端末に不正アクセスする。					FW（パケットフィルタリング型）		権限管理	○	ログ収集・分析	○			⑥ 2	
							パッチ適用	○	アクセス制御	○						
							通信相手の認証									
							操作者認証	○								
13		マルウェアが、データヒストリアンからファイアウォールに不正アクセスする／マルウェアに感染させる。	対策案2			⑭	FW（パケットフィルタリング型）	○	権限管理	○	機器異常検知				⑥ 2 →3	⑮
							パッチ適用		アクセス制御	○	ログ収集・分析	○				
							通信相手の認証									
							操作者認証	○								
14		マルウェアが、ファイアウォールからHMI（操作端末）に不正アクセスする／マルウェアに感染させる。	対策案1			⑦	パッチ適用		権限管理	○	機器異常検知				⑥ 2 →3	⑧
							通信相手の認証		アクセス制御	○	ログ収集・分析	○				
							操作者認証	○								
							アンチウイルス									
							ホワイトリストによるプロセスの起動制限	○								
15		マルウェアが、HMI（操作端末）上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2 →1 ⑩	3	B →C ⑪	①		データ署名		機器異常検知	○			⑤ 1 ⑬→2	2 →3 ⑨
								⑫	重要操作の承認		ログ収集・分析	○				
16		マルウェアが、ファイアウォールから制御サーバに不正アクセスする／マルウェアに感染させる。	対策案1			⑦	パッチ適用		権限管理	○	機器異常検知				⑥ 2 →3	⑧
							通信相手の認証		アクセス制御	○	ログ収集・分析	○				
							操作者認証	○								
							アンチウイルス									
							ホワイトリストによるプロセスの起動制限	○								
17		マルウェアが、制御サーバ上で広域供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2 →1 ⑩	3	B →C ⑪	①		データ署名		機器異常検知	○			⑤ 1 ⑬→2	2 →3 ⑨
								⑫	重要操作の承認		ログ収集・分析	○				
18		マルウェアが、ファイアウォールからデータサーバに不正アクセスする／マルウェアに感染させる。					パッチ適用		権限管理	○	機器異常検知				2	
							通信相手の認証		アクセス制御	○	ログ収集・分析	○				
							操作者認証	○								
							アンチウイルス									
							ホワイトリストによるプロセスの起動制限	○								
19		マルウェアが、データサーバからPLC（マスター）に不正アクセスする／マルウェア感染させる。					パッチ適用		権限管理		機器異常検知	○			1	
							通信相手の認証		アクセス制御		ログ収集・分析	○				
							操作者認証									
							ホワイトリストによるプロセスの起動制限									
20		マルウェアが、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	1	2	3	C	②		データ署名		機器異常検知	○			1	2
											ログ収集・分析	○				

図 5-5 事業被害ベースのリスク分析シート（抜粋）

(3)リスクの低減

攻撃ツリーのリスク値を低減するには、基本的にセキュリティ対策を強化して、対策レベルを向上させる。攻撃ツリーの対策レベルを向上するために、どの攻撃ステップを改善するのが有効か、強化策を検討した例を、図 5-6 に示す。攻撃ツリーのリスク値は各攻撃ステップの対策レベルの最大値で決定される(4.2 節の表 4-49 参照)から、基本的に現状の攻撃ツリーの対策レベルより高い対策レベルが施せる攻撃ステップを探す必要がある。例えば、強化案 1 の様に、対策レベルが 1 の攻撃ステップ 3 の対策レベルを 2 に上げても、ツリー全体の対策レベルは最大値の 2 のままである。強化案 2 や強化案 3 の様に、いずれかの攻撃ステップの対策レベルを 3 に強化することによって、攻撃ツリー全体の対策レベルを 3 とすることができる。

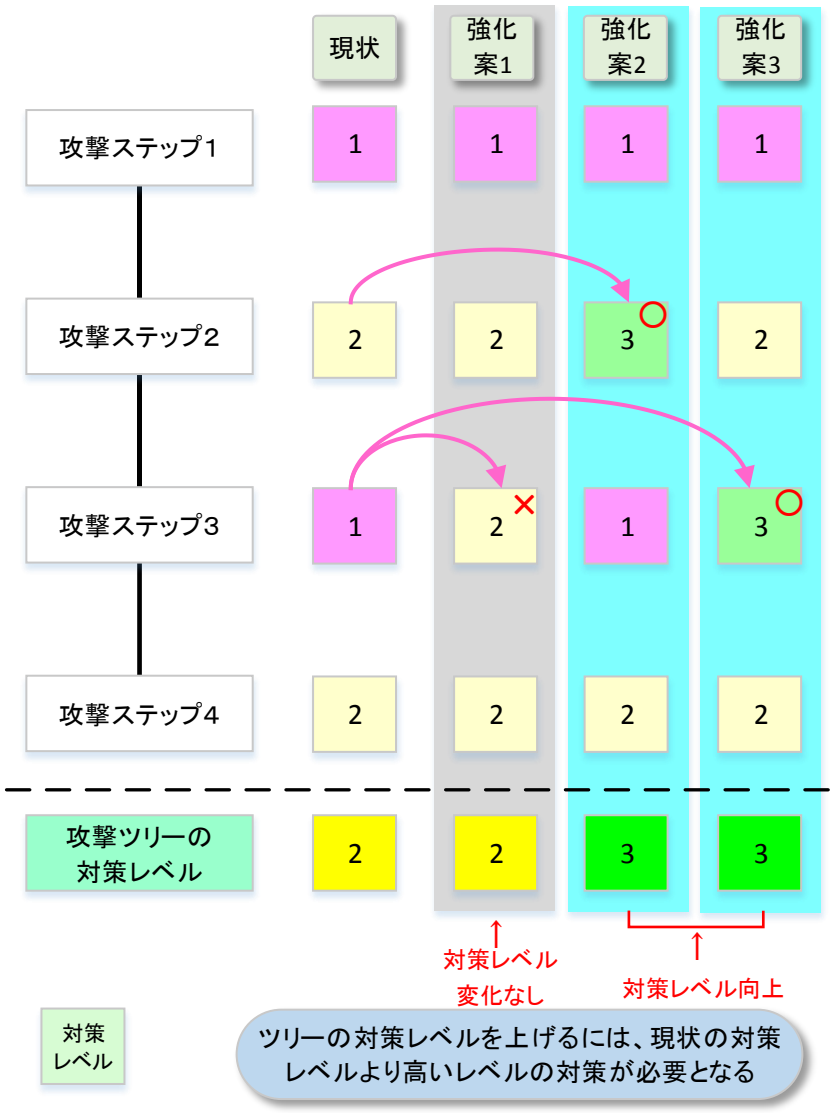


図 5-6 攻撃ツリーの対策レベル強化案の検討例

具体的な低減策の考え方を、図 5-5 に示したリスク分析シートを用いて説明する。

図 5-5 の攻撃ツリー③④の各資産（各攻撃ステップ）の対策レベルの値は、表の「対策レベルー攻撃ステップ」欄で確認することができる。基本的な考え方は、前述した様に、攻撃ツリーを構成するどれかの攻撃ステップの対策レベルを上げることによって攻撃ツリーの対策レベルを上げることであるが、ここでは対策レベルが 1 となっている攻撃ステップ（図中⑤）と対策レベルが 2 となっている攻撃ステップ（図中⑥）がある。この様なケースでは、どの攻撃ステップの対策強化が最も効率的であるか否かを検討することになる。

ここでは、2 件の攻撃ツリーの各々の攻撃拠点である HMI（操作端末）と制御サーバ上の対策を強化する「対策案 1」と、2 件の攻撃ツリーの共通の経由であるファイアウォールの対策を強化する「対策案 2」を比較検討する。

例えば、対策案 1 では、HMI と制御サーバの対策として即時パッチの適用（図中⑦）を加えると、この攻撃ステップの対策レベルが 2→3 となり（図中⑧）、それに関連して攻撃ツリーの対策レベルが 2→3 に（図中⑨）、脆弱性レベルが 2→1 となる（図中⑩）。リスク値は脅威レベル、脆弱性レベル、事業被害レベルの組み合わせで算定されるので、算定基準（表 4-51）によってリスク値は B→C と低減される（図中⑪）。また、重要操作の承認（図中⑫）を加えることでも対策レベルを 1→2 に上げることができるが（図中⑬）、この対策だけでは攻撃ツリーの対策レベルは 2 のままで、結果的に攻撃ツリーのリスク値は変わらない。

一方、対策案 2 では、ファイアウォールに対する対策として即時パッチ適用（図中⑭）を対策として採用して、この攻撃ステップの対策レベルを 2→3 とし[39]（図中⑮）、それに関連して攻撃ツリーの対策レベルが 2→3 に（図中⑨）、脆弱性レベルが 2→1となり（図中⑩）、リスク値は B→C と低減される（図中⑪）。更に、これにより、2 件の攻撃ツリー③、④の対策を一度に行えることになる。

この様に、リスク値の低減の手法は、対策の容易さや対策コスト、効率等を考慮しながら検討する。リスク分析で抽出した課題とその対策方針は、今後の改善のために記録を取っておくことが望ましい。表 5-3 に、リスク分析結果のまとめの例を記す。

本書では、サイバー攻撃に対する技術的対策を中心にリスク分析の実施を述べている。しかしながら、様々な理由から、技術的対策による対策強化が困難であるケースも考えられる。その様なケースでは、運用管理面での対策でセキュリティレベルを上げることも選択肢となるので、事業者においてその観点は追加して検討して頂きたい。

[39] 表 4-24 の判断基準例では、即時パッチ適用だけでは対策レベルは 3 にはならないが、設定チェックリストの確認とセキュリティテストを実施した結果、対策レベル＝3 と判定した。

表 5-3 事業被害ベースのリスク分析結果対策表の例

#	攻撃ツリー概要	想定されるシナリオ	対策箇所	想定される対策	推定対策コスト	改善方法		優先度	改善実施	備考
						システム	運用			
1	内部の人:USB 経由で制御サーバがマルウェアに感染	USB メモリ持ち込みで制御サーバがマルウェア感染	制御サーバ	USB 端子のロック	低	○		高	○	
2	テレメータから制御サーバ経由で PLC 攻撃	侵入者による不正コマンド発行	テレメータ	施錠、扉センサ	中	○		低		
3	情報ネットワークからファイアウォール経由で制御サーバを攻撃	ファイアウォールの脆弱性を攻められ制御サーバを攻撃	ファイアウォール	管理者アカウントの強化、パスワード管理徹底	低	○	○	高	○	
4	保守 PC から PLC 攻撃	保守 PC がマルウェアに感染し PLC ラダーを書き換え	保守 PC	アンチウイルスの導入	中	○		低	○	

(4)リスクの低減効果の把握

事業被害ベースのリスク分析のリスク値は、想定される事業被害を引き起こす、それぞれの攻撃ツリーについて算定される。事業被害ベースのリスクの低減効果は、高いリスク値の攻撃ツリーの数をどれだけ減らせるか、まだ比較的高いリスク値の攻撃ツリーがどれだけ残留しているかを把握することにある。従って、リスク値と件数を表すヒストグラムを作成し、そのリスク値の分布がどの様に変化したかで、効果を確認することを推奨する。

例えば、対策前には高いリスク値を持つ攻撃ツリーが m 個あったのが、改善後には n 個に減少したという評価を行う。図 5-7 では、改善前には、リスク値 A, B がそれぞれ 3 個、5 個あったのが改善後にはリスク値 A, B がともに 0 個となったという例を示している。高いレベルのリスク値の攻撃ツリーが残留している場合は、今後の継続的なリスク分析の実施時に役立てていく。

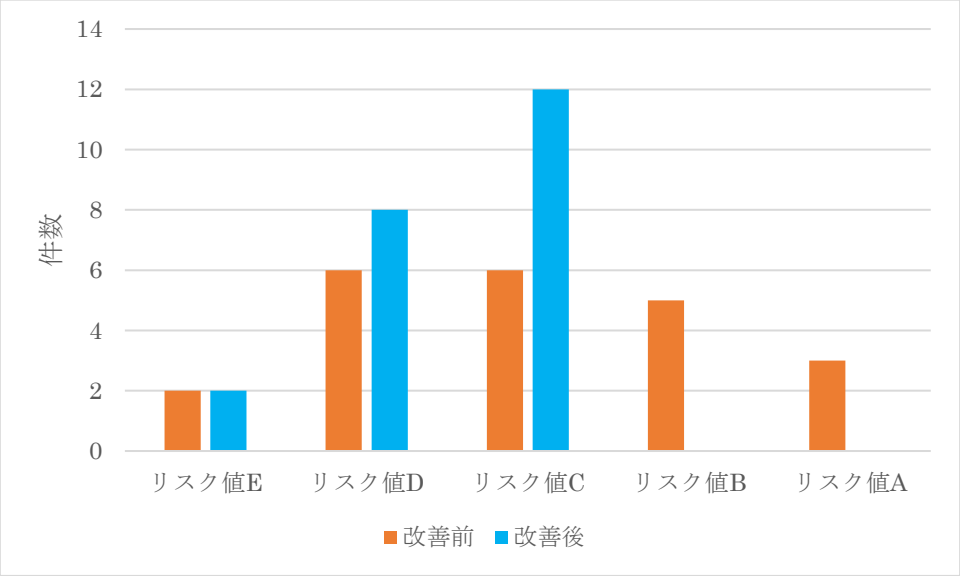


図 5-7 リスク値のヒストグラム(事業被害ベースの分析)

(5)テスト・検証箇所の抽出・特定

表 5-2(5.1 節(5)の再掲)に、リスク分析結果を受けて実施するテストの目的とテスト対象を示す。サイバー攻撃に対するセキュリティ強度の実システム(本番環境または模擬環境)における確認手法として、脆弱性検査、ペネトレーションテスト、パケットキャプチャテストが挙げられる。各手法の詳細は 6 章で説明するが、これらのテストのうち、脆弱性検査とパケットキャプチャテストは特定の資産や箇所に対してのテストであり、ペネトレーションテストはネットワークを介しての侵入や攻撃が可能(成功する)かをテストするもので、いずれも固有のツールの利用や専門家によるマニュアル(手作業)等によって実施される。

表 5-2 主なテストの目的とテスト対象 (再掲)

テスト種類	目的	テスト対象
脆弱性検査	資産に既知や未知の脆弱性がないか確認する	個々のシステム資産
ペネトレーションテスト	様々な攻撃手法でシステムへの侵入、不正な操作ができないか確認する	ネットワークの界面とネットワーク内の制御端末や重要サーバ等の資産
パケットキャプチャテスト	想定外の通信や操作が行われていないか確認する	制御ネットワーク

事業被害ベースのリスク分析においては、事業被害を引き起こす可能性のある攻撃ツリーが評価でき、それを受けリスク値を下げるため、追加対策を実施する(本節の(1)~(4))。攻撃ツリーとしてのリスク値の低減を目標に、攻撃ツリー上の攻撃ステップの資産に対する対策の強化を多層防御的な観点から行う。一連の攻撃である攻撃ツリー上の攻撃ステップのどこかで抑止(遮断)することを念頭に追加の対策を検討することになる。しかし、以下の様な様々な事由で、リスク値を十分に下げきれないケース等もある。

- システムの可用性上、セキュリティパッチをあてることは、実施を見送った。
- システムの制約上、セキュリティ対策の機能を追加することができなかった。
- 対策コスト面の事情から、実施を見送った。
- ある攻撃ステップで確実に攻撃を抑止できる対策までは実施できなかった。

そうしたケースでは、対策の必要性を再認識するためには、実システムにおけるテストを実施することが選択肢として出てくる。事業被害ベースのリスク分析の結果を受け、リスク値の高い攻撃ツリーと脅威レベルを考慮して、以下の観点からテストの対象とする攻撃ツリーとその攻撃ルートを抽出、特定することが可能である。

① 十分にリスク値を下げきれていない、深刻な事業被害をおよぼしうる攻撃ツリー
② リスク値が高いまま、対策が見送られた攻撃ツリー
③ 複数の攻撃ツリーの入口や境界となっている機器（ネットワーク機器、操作端末、サーバ等）
④ 複数の攻撃ツリーで共通の攻撃ルート

実施するテストとしては、以下が挙げられる：

- ペネトレーションテスト： 攻撃ツリーに該当するルートからの試行的な侵入や攻撃ステップの実行可能性の検証、攻撃の入口やネットワークの境界における機器への侵入、等からなるペネトレーションテスト
- パケットキャプチャテスト： 攻撃の入口や攻撃ルート等で、現行の稼動システムへの想定外の通信や操作が発生していないかを検証

前者は、実際の攻撃が発生した際の防御能力を検証する位置付けである。後者は、運用中のシステムへの攻撃の発生の有無、あるいは既にマルウェア感染が発生していないか、内部不正の兆候がないか等、脅威レベルの検証を行う位置付けである。いずれのテストも、実システムに対して実施する場合には、運用への支障や性能面での影響等も合わせて考慮する必要がある。また、実システムでのテストで困難が予想される場合には、模擬環境や機器単体でのテストを検討することになる。

【コラム】

改善してもリスク値が下がらない場合

リスク分析の目的は現状のリスクを把握し改善することにあり、その程度を測るための目安としてリスク値を採用している。しかしながら、本書で用いている評価指標（脅威レベル、脆弱性レベル（対策レベル）、資産の重要度／事業被害レベル）は 3 段階評価のため、脆弱性レベルの低減が必ずしもリスク値の低減に反映されず、改善の目安とならない場合もある。例えば、脅威レベルが「3」、脆弱性レベルが「3」、事業被害レベルが「2」の算定結果、リスク値が「B」である攻撃ツリーがあったとする。この攻撃ツリーの対策を強化することにより、脆弱性レベルが「2」に改善したとしても、算定基準上、リスク値は元の値と変わらず「B」のままとなる。

この様に改善しているのにかかわらず、目に見えた形で示すことができない場合には、改善の度合いを把握するためにリスク値以外の指標を用いることを検討する。例えば、脆弱性レベルの変化に着目して、高いリスク値を持つ攻撃ツリーの脆弱性がどれだけ低減されているかを目安としたり、更には、高いリスク値を持つ攻撃ツリーを構成する各攻撃ステップを分析して、それらの攻撃ステップの中で対策レベルが何件改善されたかという数値を改善の目安としたりするという方法もある。

5.3. 資産ベース・事業被害ベースのリスク分析の活用法の違いと相関

図 5-8 は、資産ベースと事業被害ベースのリスク分析の結果から対策を行う際の違いを表わしている。

資産ベースのリスク分析（図 5-8・上）の場合は、全ての資産の各攻撃手法に対してリスク値の高い部分のリスク値の低減策を考える。改善を行うことにより個々の資産のセキュリティ強度が上がり、システム全体でもセキュリティの強度は高まる。その際の優先順位付けは、基本的にリスク値が高く改善が容易にできる資産、作成しているシステム構成図（3.1 節）を参照して攻撃の上流に位置する資産等を考慮して、高い優先順位を付ける。図 5-8 に、優先順位例を示す（①）。

しかしながら、制御システムにおいて各資産のリスクを一つ一つ全て低減するのは、現実的には可用性の面（例えば、稼働状態でパッチが当てられない）、コストの面（例えばリスク値の高い資産が多数ある場合に対策強化を一律にはできない）、技術的な面（例えば、OS を刷新やセキュリティ機能の搭載ができない）等から、非常に困難であるケースが多い（②）。そのために、事業被害ベースの分析を合わせて行い、リスクの高い攻撃ツリーを求め、その攻撃ツリー上のどの資産のどの脅威への対策を強化することがリスク低減に有効かを考える方が最適な解が得られやすい。

事業被害ベースのリスク分析の結果（図 5-8・下）からは、リスク値の高い攻撃ツリーが経由する資産の中で、どの資産のどの脅威に対する対策を行うと最も効果的に攻撃ツリーのリスク値を低減できるかを考えることができる。この場合、高いリスクを持っているが対策が困難だったり対策に高いコストが発生したりする資産があっても、隣接する資産の脅威の低減や対策レベルの向上により当該攻撃ツリーに対するリスク値を低減できる可能性がある。また、複数の攻撃ツリーのリスク値を見渡すことにより効率的に対策箇所を選定することができる（③）。攻撃ツリーのリスク値の低減にあたっては、仮に攻撃ツリー上の一つの資産で十分に脆弱性を低減できない様なケースでも、多層防御の観点から対策の容易な複数の資産に対してセキュリティ対策を施すという考え方も適用することができる（④）。図 5-8 のケースでは、2 つの攻撃ツリーで共通の侵入口または経由の対策の強化を選択した例（③）、侵入口と経由の両方の対策の強化を選択した例（④）を示している。

表 5-4 に、資産ベースのリスク分析と事業被害ベースのリスク分析の結果の活用法と効果の違い、相互補完的な関係の一覧を示す。

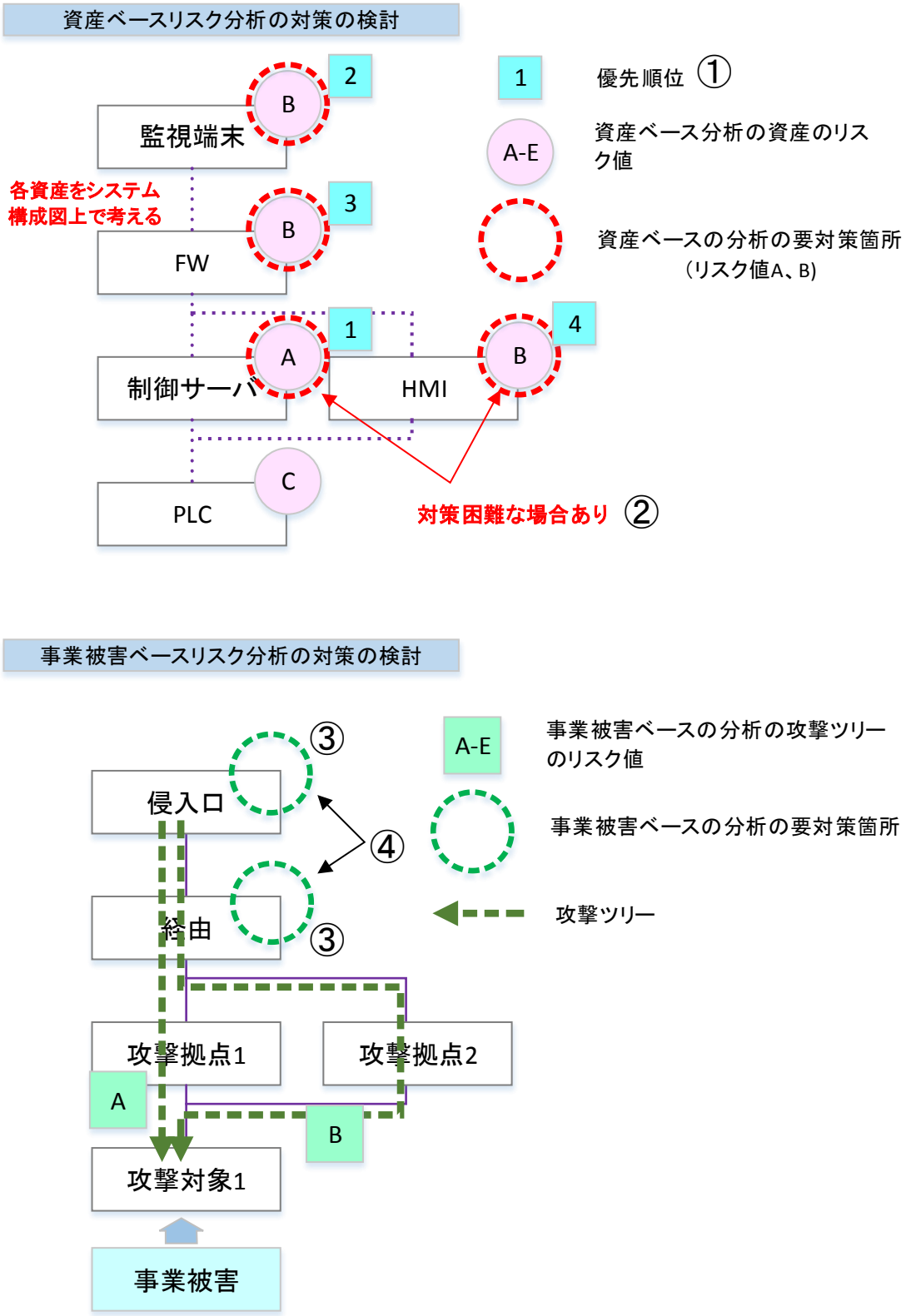


図 5-8 資産ベースと事業被害ベースにおける対策箇所検討方法の違い

表 5-4 両リスク分析の活用法の違いと相関

#			資産ベースのリスク分析	事業被害ベースのリスク分析
1	リスク値の対象		全てのシステム資産	被害を生じさせる可能性のある攻撃ツリー
2	改善対象箇所		個々のシステム資産	攻撃ツリーの攻撃ステップ上にあるシステム資産
3	対策箇所		リスク値の高い対象資産における脆弱性レベルの高い脅威に対する対策	リスク値の高い攻撃ツリーの対策レベルの低い攻撃ステップの資産における対策
4	リスク低減の効果		システム全体の個々の資産のリスク値の低減	事業被害をもたらす攻撃ツリーのリスク値の低減
5	テスト箇所の抽出特定		リスク値の高い資産 ● 脆弱性検査 ● パケットキャプチャテスト	リスク値の高い攻撃ツリー（攻撃ルート） ● ペネトレーションテスト ● パケットキャプチャテスト
6	特徴	長所	全ての資産を単体で網羅的にリスク分析と対策の検討が可能	事業被害をもたらす攻撃ツリーに対する多層防御的な観点で、対策を検討することが可能
7	特徴	限界・短所	資産を一律に評価するので、事業上の対策優先順位付けに考慮が必要となる。	想定（対象）外の攻撃の入口や、攻撃ツリーで経由しない資産や、経由した資産での直接の攻撃（不正アクセスや操作等）以外の攻撃に対する対策の検討は、見落とされる可能性がある。

5.4. 継続的なセキュリティ対策の実施（PDCA サイクル）

現行の制御システム（もしくは新規構築予定のシステム）に対しての 3 章、4 章で述べた資産の明確化とリスク分析は、それ以降のセキュリティマネージメントシステムの PDCA サイクル（Plan（計画）-Do（実施）-Check（確認・監査）-Act（見直し・改善））を継続していく上で中核的な役割となる。セキュリティ対策は、一度実施したら終わりとはならない。日々、新しい攻撃やインシデントが発生し、新たな脆弱性も発見される一方で、新しいセキュリティ対策技術や手法も開発される。そのため、セキュリティレベルを維持・向上していくためには、継続的に見直しを実施していくことが求められる。

図 5-9 に、セキュリティ向上の PDCA サイクルにおけるリスク分析の位置付けを示す。

PDCA サイクルでは、3 章及び 4 章の手順で実施するリスク分析、その結果として作成されるリスク分析成果物が基盤となる。リスク分析結果を活用して、追加・強化セキュリティ対策を決定し、実施することになる。また、必要に応じて、セキュリティテストを実施する。この初回のリスク分析の実施は、相応の工数が必要となるが、一度出来上がったリスク分析成果物は、セキュリティを維持・管理・向上していく上での基盤となるデータベース（システム構成とデータフロー、資産の重要度、事業被害、脅威、対策状況、リスク分析結果）として、次回以降のリスク分析でも有効に活用される。第 2 回目以降のリスク分析では、このデータベースを元に、追加された条件（以下に例示）に対する差分や追加修正等を加えてリスク分析を実施することで、合理的な工数の下で効果的な実施が可能となる。必要な工数が初回よりかなり削減されるだけでなく、リスク分析の精度やセキュリティレベルを向上させることが可能となる。

また、制御システムは複数の事業所で類似の制御システムが稼動していることが多く見受けられる。そうしたケースでは、得られたリスク分析成果物の、それらのシステムへの活用や結果の適用（例えば類似箇所のセキュリティ対策の強化）等の横展開が考えられる。

第 2 回目以降のリスク分析の実施で想定される、もしくは組み入れられる要件として、以下の様な項目が挙げられる：

① 評価対象システムの変更、機能の追加
- システムの改変、機器や新たなサービス機能等の追加等

② リスク分析の精度向上
- 評価対象範囲の拡大、非定常稼働機器の追加、周辺システムや通信経路の追加等
- モデルの詳細化、分析粒度の細分化、グループ化単位の見直し
- 初期の分析で見送った資産や攻撃シナリオの見直し

③　周囲環境（脅威、脆弱性、インシデントの発生）の変化

- 新たな脅威の出現、新たな脆弱性の発見に対する対応
- 発生したインシデント事例に対する攻撃ツリーの検討

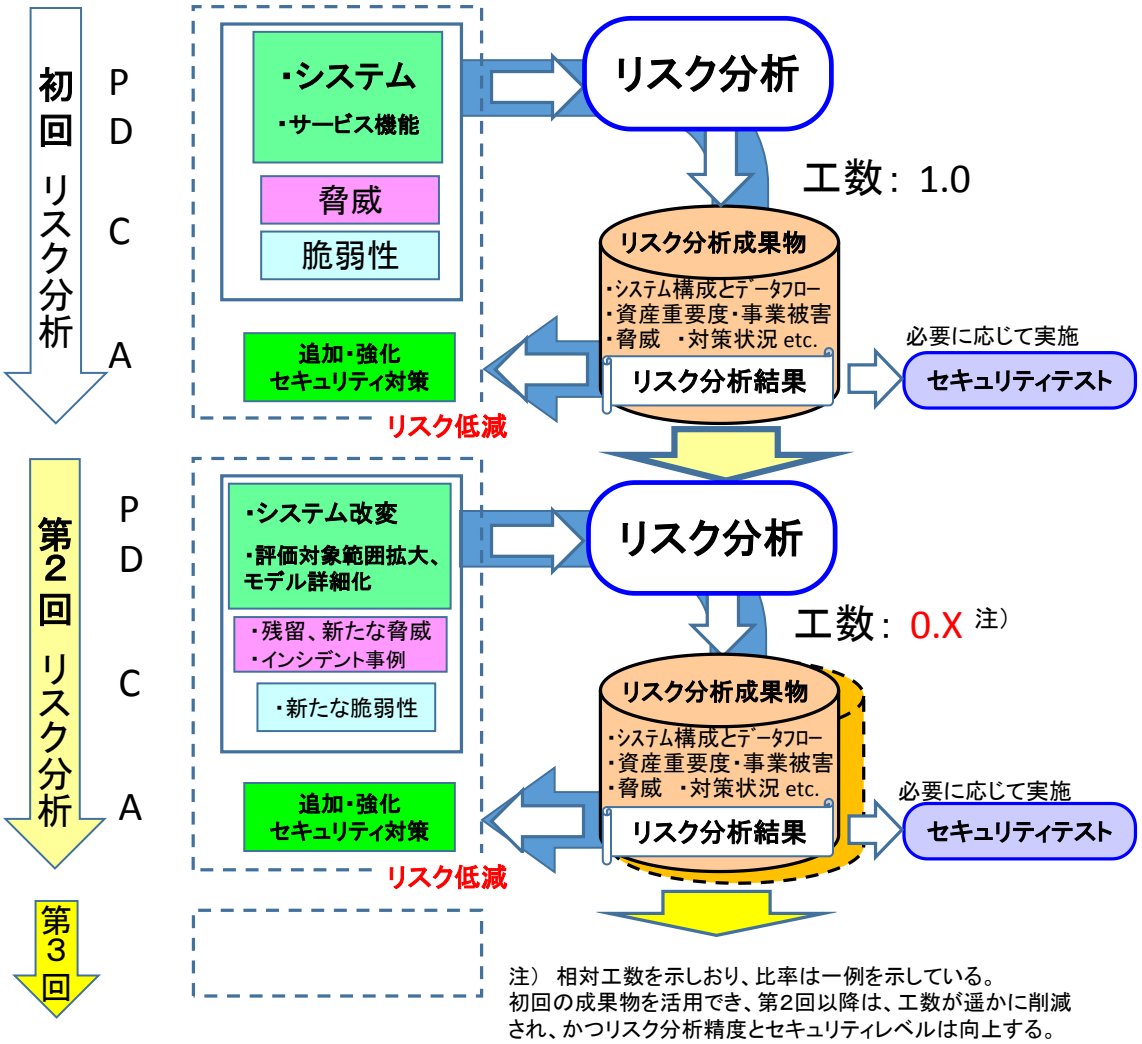


図 5-9　セキュリティ向上の PDCA サイクルにおけるリスク分析の位置付け

6. セキュリティテスト

本章では、リスク分析の結果を踏まえて、実施の候補となるセキュリティテストについて説明する。

6.1. セキュリティテストの位置付け

制御システムに対してセキュリティテストを実施する目的と効果について説明する。

（1）制御システムのリスク分析結果の実機での確認

机上のリスク分析では対象システムの対策状況を評価するが、対策の確実性や有効性、脅威に対する堅牢性（Robustness）までは検証できていない。また、リスク分析でリストアップできなかった機器やネットワーク経路等に含まれる脆弱性、機器やサービスの設定不備等による脆弱性を突いた攻撃によるリスクが残存する場合もある。

従って、実機を使用した環境（本番環境または模擬環境）でセキュリティテストを実施し、対象システムの対策の確実性や攻撃に対する堅牢性を確認することが有効である。

- **本番環境でのテスト**
  実際の制御システムを対象に、稼働前または実運用中にテストを実施する。
- **模擬環境でのテスト**
  テスト対象範囲の機器、ネットワーク構成、OS、アプリケーション、設定内容等を本番環境に模擬した（可能な限り同一とした）制御システムを用意し、テストを実施する。

（2）制御システムの現状調査

制御システムにおいては可用性が重視されるため、可用性が阻害される可能性があるセキュリティテストを本番環境で行うことは難しい場合が多い。しかしながら、制御システムの本番環境において制御システムへの影響度が低い方法を用い、制御システムへの攻撃の発生頻度、外部からの攻撃の有無、マルウェア感染等の脅威の有無、制御システム内における不審な操作や通信・データフローの有無等について、現状調査することは有効である。

6.2. セキュリティテストの種類

セキュリティテストの種類には様々なものがある。制御システムに適用可能な代表的なセキュリティテストについて、テストの種類、目的、テスト対象の一覧を、表 6-1 に示す。

表 6-1 代表的なセキュリティテストの種類・目的・対象

<table>
<tr><th rowspan="2">テスト目的</th><th colspan="3">テスト対象</th></tr>
<tr><th>ネットワーク</th><th>OS／ミドルウェア</th><th>アプリケーション</th></tr>
<tr><td rowspan="2">既知の
脆弱性検出</td><td>・脆弱性検査
（システムセキュリティ
検査）</td><td>・脆弱性検査
（システムセキュリティ
検査）</td><td>・脆弱性検査
（Web アプリケーション
診断）</td></tr>
<tr><td rowspan="2">未知の
脆弱性検出</td><td colspan="2" rowspan="2">・ファジング</td></tr>
<tr><td>・ソースコード
セキュリティ検査</td></tr>
<tr><td>侵入可否の
検証</td><td colspan="3">・ペネトレーションテスト</td></tr>
<tr><td>不審通信の
検査</td><td colspan="3">・パケットキャプチャテスト</td></tr>
<tr><td>不正な
ネットワーク
機器の調査</td><td>・ネットワークディスカバリ
・ワイヤレススキャン</td><td colspan="2"></td></tr>
</table>

表 6-1 に示したセキュリティテストのうち、制御システムのリスク分析結果を踏まえて実施するセキュリティテストとして、本章では脆弱性検査、ペネトレーションテスト、パケットキャプチャテストを説明する。これらのテストの概要を、表 6-2 に示す。また、その他のテストの概要を、表 6-3 に示す。

表 6-2 本書で紹介するセキュリティテストとその概要

種類	概要
脆弱性検査 （☞ 6.3 節）	制御システムにおける既知の脆弱性を検出することを目的としたセキュリティテスト。 代表的なものに、ネットワーク機器、サーバ、OS、ミドルウェアにおける脆弱性や設定不備を検査するセキュリティシステム検査（プラットフォーム診断）、Web アプリケーションにおける脆弱性を調査する Web アプリケーションセキュリティ検査がある。
ペネトレーションテスト （☞ 6.4 節）	制御システムへの侵入可否を検証することを目的としたセキュリティテスト。 システムに対して、実際にどこまで侵入できるのか、何ができるのか、試行する。テストにおいては、運用上のシステムに残存している既知の脆弱性を狙う、設計段階での不備を狙う等を実施する。 ペネトレーションテストは、テスト対象の侵入口の糸口となる脆弱性を探す調査段階と、発見された脆弱性を悪用する攻撃段階に分かれる。
パケットキャプチャテスト （☞ 6.5 節）	制御システムのネットワーク上のパケットに不審な通信が含まれていないかを分析することが目的としたセキュリティテスト。 システムのネットワークにパケットキャプチャ用の装置を設置し、ネットワークのパケットを収集、分析する。

表 6-3 その他のセキュリティテストの概要

種類	概要
ファジング[40]	制御システムにおける既知及び未知の脆弱性を検出することを目的としたセキュリティテスト。 脆弱性を発生させやすい文字列等のデータを連続してテスト対象に送信し、脆弱性の有無を検査する。
ソースコードセキュリティ検査[41]	事業者が開発した制御システム用アプリケーションにおける未知の脆弱性の検出を目的としたセキュリティテスト。 ソースコード中の脆弱性を引き起こしやすい関数の検索、構文解析等により、問題点の有無を検査する。
ネットワークディスカバリ[42]	制御システムのネットワークに不正接続された機器の検出を目的とするセキュリティテスト。 ネットワーク上に接続された全ての機器を洗い出し、不正接続機器の有無を確認する。
ワイヤレススキャン[42]	制御システムにおける不正な無線通信機能の検出（許可されていない無線 LAN アクセスポイントの設置等）を目的とするセキュリティテスト。 無線アナライザを用いて、不正な無線通信の存在の有無を確認する。

40 詳細は、IPA 脆弱性対策：ファジングを参照。 http://www.ipa.go.jp/security/vuln/fuzzing.html

41 詳細は、IPA テクニカルウォッチ『ソースコードセキュリティ検査』に関するレポートを参照。
http://www.ipa.go.jp/about/technicalwatch/20111117.html

42 詳細は、NISTSP 800-115 Technical Guide to Information Security Testing and Assessment を参照。
http://dx.doi.org/10.6028/NIST.SP.800-115

6.3. 脆弱性検査

（1）脆弱性検査の目的

脆弱性検査の目的は、制御システムを構成する資産やアプリケーションに対して、主に既知の脆弱性の有無を確認することである。脆弱性の有無に加えて、不要なサービスの公開や設定不備等が発見されることもある。資産やアプリケーションで既知の脆弱性が発見された場合、その影響度を考慮して対策を見直す必要がある。

（2）脆弱性検査の対象と実施例

脆弱性検査の対象は、制御システムを構成するネットワーク機器、端末、サーバ、サービスアプリケーションである。5.1 節（5）を参照し、資産ベースのリスク分析結果を踏まえて、以下の条件からテスト箇所を選定する。

① 外部との界面に位置しているネットワーク装置等の資産（ファイアウォール等）
② 重要な処理が可能な操作端末
③ 保守要員等、外部の要員が操作する可能性のある端末
④ 重要度の高い資産（サーバ類等）で、リスク値を十分に下げられてない資産

本ガイドのモデルシステムから脆弱性検査の対象を選定すると、以下が候補となる。

- ファイアウォール、データヒストリアン （条件①）
- HMI（操作端末） （条件②）
- 制御サーバ、データサーバ （条件④）

脆弱性検査を実施する装置（テスト端末）をネットワーク上のどこに設置し、どの対象資産を検査するかで、様々な形態が考えられるが、上記の場合の脆弱性検査の実施例を、図 6-1 に示す。

本実施例においては、モデルシステム中の 3 箇所に設置したテスト端末を用いて、脆弱性検査を実施するケースを説明している。テスト端末の位置ごとの脆弱性検査の対象と目的を、表 6-4 に示す。脆弱性検査の対象と目的、及び外部のテスト事業者を活用する場合の実施者の所在場所等を考慮して、決定する必要がある。

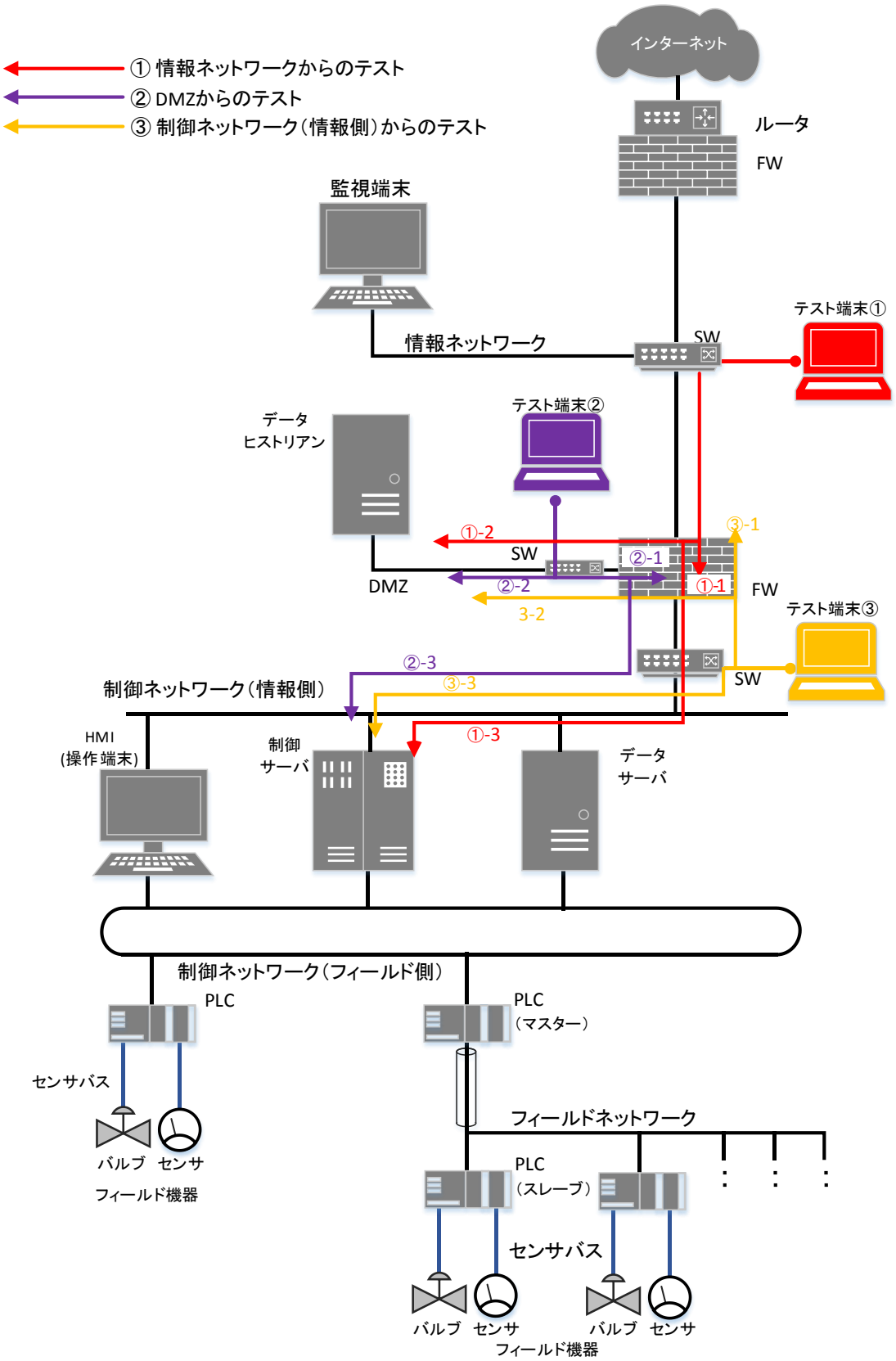


図 6-1 脆弱性検査の実施例

表 6-4 テスト端末の位置と脆弱性検査の対象と目的

テスト端末の位置		脆弱性検査の対象と目的	
①	情報ネットワークに設置した端末①を侵入口と想定した脆弱性検査	①-1	情報ネットワーク側からみたファイアウォールの脆弱性を調査する。
		①-2	情報ネットワーク側からみた DMZ の機器の脆弱性を調査する。
		①-3	情報ネットワーク側から制御ネットワーク（情報側）の機器へ直接攻撃できるかの観点での脆弱性を調査する。
②	DMZ に設置した端末②を侵入口と想定した脆弱性検査	②-1	DMZ からみたファイアウォールの脆弱性を調査する。
		②-2	同一セグメントから攻撃された場合の DMZ の機器の脆弱性を調査する。
		②-3	DMZ からみた制御ネットワーク（情報側）の機器の脆弱性を調査する。
③	制御ネットワーク（情報側）に設置した端末③を侵入口と想定した脆弱性検査	③-1	制御ネットワーク（情報側）からファイアウォールの脆弱性と情報ネットワークに直接アクセスできる脆弱性がないかを調査する。
		③-2	制御ネットワーク（情報側）から DMZ の機器の脆弱性を調査する。
		③-3	同一セグメントから攻撃された場合の制御ネットワーク（情報側）の機器の脆弱性を調査する。

（3）脆弱性検査の実施環境

制御システムの脆弱性検査の実施環境は、脆弱性検査による制御システム稼働への影響を考慮して、脆弱性検査の対象が本番環境か検証環境かを選択する。脆弱性検査の実施環境による長所・短所等を比較したものを、表 6-5 に示す。

表 6-5 脆弱性検査の実施環境による比較

実施環境による比較	本番環境	模擬環境
長所	本番環境の脆弱性の有無を評価できる。	テストによる本番環境の不具合や停止のリスクがない。
短所	テストによる制御システムへの障害が発生する場合がある。	模擬環境の構築の費用、構築の期間が追加で必要となる。
実施前の準備	テストを実施する場合は、検査対象機器に障害が発生するリスクを把握し、障害発生時に備える必要がある。 テストの対象装置の事前のバックアップとリカバリ手順を含めたリカバリテストが完了していることが必要である。	試験対象の機器を揃え、本番と同じネットワーク構成、ソフトウェア構成、設定を用意してテストを行う必要がある。
実施タイミング	新規の制御システム稼働前や制御システムの定修[43]期間に本番環境での脆弱性検査の実施を検討する。	―

（4）脆弱性検査の注意点

- **フォールスポジティブ（過検知）**

  フォールスポジティブは、脆弱性がない箇所を脆弱性があると誤って検知することである。脆弱性検査で検出された脆弱性には誤検知が含まれるため、検出された脆弱性の精査には脆弱性の分析が経験豊富なセキュリティエンジニアが必要である。

- **フォールスネガティブ（検知漏れ）**

  フォールスネガティブは、脆弱性がある箇所を検知できず、脆弱性がないと判定することである。脆弱性検査で検出されない脆弱性が隠れている可能性があることに留意が必要である。

[43] 定期的に設備を一定期間停止し、点検や修理を行うこと。

6.4. ペネトレーションテスト

（1）ペネトレーションテストの目的

脆弱性検査では、主に既知の脆弱性の有無を明らかにするが、発見された脆弱性を使って何ができるかまでは検証しない。一方、ペネトレーションテストでは悪用可能な脆弱性や、機器の設定不備（不要な空きポートやサービス許可、脆弱なパスワード等）を利用し、対象システムへ「どこまで侵入可能か」、「どの様な機微情報を入手可能か」、更に「どの様な操作（攻撃）が可能か」等を確認するのが目的である。

ペネトレーションテストには様々な形態（選択項目）と手法（選択肢）があり、代表的なものを、表 6-6 に示す。形態と手法によって、実施可能なテストと得られるテスト結果に大きな差異が想定される。テストの目的、システム情報の秘匿性や事業者の負担等を考慮して、試験実施者（セキュリティベンダ等）と十分話し合い、テスト方法を決めるのが一般的である。

表 6-6 ペネトレーションテストの代表的な形態と手法

形態 （選択項目）	手法 （選択肢）	概要
試験実施者への情報開示	ブラックボックステスト	試験実施者へ攻撃対象システムの情報を与えない、もしくは最低限の情報のみを与えてテストを実施する。悪意のある第三者による攻撃を想定したテストを実施できる。
	ホワイトボックステスト	試験実施者へ攻撃対象システムを把握できる情報（ネットワーク構成、機器、OS、利用するアプリケーション、データフロー、ユーザアカウント名等）を与えてからテストを実施する。攻撃者視点で詳細なペネトレーションテストができるが、外部（試験実施者）への情報開示は組織の判断が必要となる。また、業務への影響を判断しながらテストを実施する目的で、システム管理者と密に連絡を取り合って実施する場合もある。
攻撃起点 （侵入口）	攻撃対象の外部	攻撃対象となるシステムの外部を攻撃の起点とする。制御システムを対象としたテストでは、組織外のインターネット経由だけではなく、制御システムと接続する情報ネットワークの端末も外部の攻撃起点とする。
	攻撃対象の内部	攻撃対象となるシステムの内部を攻撃の起点とする。組織関係者の内部犯行や組織内ネットワークに侵入したマルウェアによる攻撃を想定している。制御システムを対象としたテストでは、制御システム内の端末を内部の攻撃起点とする。
テスト方法・手段	無料・商用ツール	第三者が入手・購入可能なツールによりテストを実施する。
	試験実施者独自ツール・ノウハウ（手法）	試験実施者の独自のテストフレームワークやノウハウ（手法）、必要に応じて侵入コードを独自に開発する等、攻撃対象システムに応じて柔軟に対応する。

（2）ペネトレーションテストの対象と実施例

ペネトレーションテストの対象は、制御システムへの侵入可否、制御システムの重要操作が可能な端末や重要サーバへの侵入と不正操作可否の検証である。

5.2 節（5）を参照し、事業被害分析ベースのリスク分析結果を踏まえて、以下の条件からテスト箇所を選定する。

① 十分にリスク値を下げきれていない、深刻な事業被害をおよぼしうる攻撃ツリー
② リスク値が高いまま、対策が見送られた攻撃ツリー
③ 複数の攻撃ツリーの入口や境界となっている機器
④ 複数の攻撃ツリーで共通の攻撃ルート

本ガイドのモデルシステムからテスト対象を選定すると、以下が候補となる。

- HMI へ侵入する攻撃ツリー （条件②）
- 制御システムのファイアウォール、制御システムのデータヒストリアン経由で制御ネットワーク内に侵入する攻撃ツリー （条件③④）
- PLC へ侵入する攻撃ツリー （条件④）

どこを攻撃起点としてどの様な経路で侵入するか、様々な攻撃ルートが考えられるが、本モデルシステムにおけるペネトレーションテストの実施例を、図 6-2 に示す。また、本実施例におけるペネトレーションテストの概要を、表 6-7 に示す。

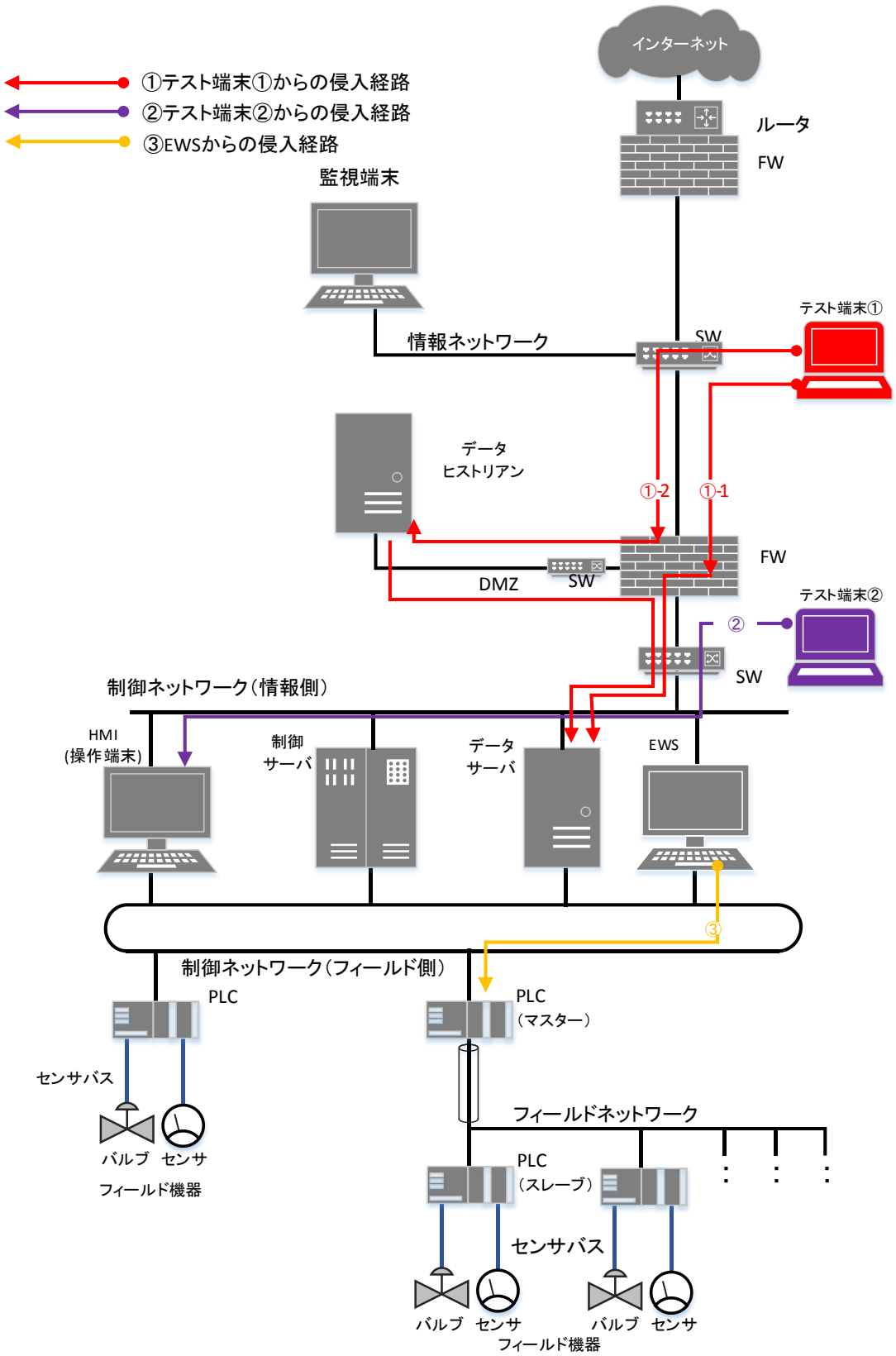


図 6-2 ペネトレーションテストの実施例

表 6-7 テスト対象の攻撃ツリーとペネトレーションテストの概要

<table>
<tr><th>攻撃拠点（侵入口）</th><th colspan="2">テスト対象の攻撃ツリー</th><th colspan="2">ペネトレーションテストの概要</th></tr>
<tr><td rowspan="2">制御システム外部に設置したテスト端末[44]</td><td rowspan="2">①</td><td rowspan="2">制御システムのファイアウォール、制御システムのデータヒストリアン経由で制御ネットワーク内に侵入する攻撃ツリー</td><td>①-1</td><td>情報ネットワークに接続したテスト端末①から、ファイアウォールの脆弱性等を利用し、管理者権限を奪取して侵入する。ファイアウォールの設定を変更し、情報ネットワークから直接、制御ネットワーク（情報側）のサーバや端末に侵入を試みる。</td></tr>
<tr><td>①-2</td><td>情報ネットワークに接続したテスト端末①から DMZ 上のデータヒストリアンの脆弱性等を利用し侵入する。データヒストリアンから、情報ネットワーク（情報側）のサーバや端末へ侵入を試みる。</td></tr>
<tr><td rowspan="2">制御システム内部に設置したテスト端末</td><td>②</td><td>HMI を攻撃対象とする攻撃ツリー</td><td colspan="2">マルウェア感染している保守端末を制御ネットワーク（情報側）に接続したと仮定し、テスト端末②から HMI へ侵入を試みる。</td></tr>
<tr><td>③</td><td>PLC を攻撃対象とする攻撃ツリー</td><td colspan="2">制御ネットワークからの攻撃で EWS まで不正侵入されたと仮定し、EWS から PLC の管理者権限を奪取し PLC へ侵入を試みる。</td></tr>
</table>

44 制御システムへの侵入方法には、インターネットから事業者の情報システムに侵入し、更に制御システムに侵入することが考えられる。しかし本ガイドは制御システムを対象としているため、情報システムには攻撃者が既に侵入していること（マルウェアが潜伏している等）を前提とし、インターネットから情報システムへの侵入はテスト対象から省略している。インターネットから情報システムを経由せずに制御システムと接続できる場合は、インターネットからの侵入をテスト対象から省略しない方がよい。例えば、インターネットからアクセス可能となっている制御機器の事例があるが、その場合はテスト対象に含めた方がよい。制御システムがインターネットからアクセス可能か否かを調査する際は、以下のレポートが参考になる。
「増加するインターネット接続機器の不適切な情報公開とその対策」 http://www.ipa.go.jp/security/technicalwatch/20160531.html

(3)ペネトレーションテストの実施環境

制御システムのペネトレーションテストの実施環境は、テストによる制御システム稼働への影響を考慮して、テストの対象を本番環境か検証環境かを選択する。テスト実施環境による長所・短所等を比較したものを、表 6-8 に示す。

表 6-8 ペネトレーションテストの実施環境による比較

実施環境 による比較	本番環境	模擬環境
長所	本番環境に対する侵入可能な脆弱性を評価できる。	テストによる本番環境の不具合や停止のリスクがない。
短所	テストによる制御システムへの障害が発生する場合がある。	本番環境と同等の模擬環境構築の費用、構築の期間が必要となる。模擬環境にはなく本番環境にしかないネットワーク経路や機器がある状態でのテストでは、侵入につながる脆弱性を十分に評価できない場合がある。
実施前の準備	テストを実施する場合は、検査対象機器に万が一の障害が発生するリスクを把握し、障害発生時に備える必要がある。 テストの対象装置の事前のバックアップとリカバリ手順を含めたリカバリテストが完了していることが必要である。	本番環境と同じ機器、OS、ソフトウェア構成、設定を用意してテストを行う必要がある。
実施タイミング	新規の制御システム稼働前や制御システムの定修期間に本番環境での脆弱性検査の実施を検討する。	—

（4）ペネトレーションテストの注意点

- **テスト実施範囲の明確化**
  テスト実施前にテスト実施範囲とテスト禁止範囲（アクセス可能機器、IP アドレス、ポート番号、ユーザアカウント等）を決定し、試験実施者に伝える必要がある。

- **制御システム独自の通信プロトコルを使ったレイヤへのテスト**
  制御システムにおいては、独自の通信プロトコルが利用されていることも多い。制御システム固有の通信プロトコルに精通した試験実施者が必要である。

【コラム】

本番環境での脆弱性検査・ペネトレーションテスト

通信の応答速度やタイミングの制約が厳しい制御システムにおいて、本番環境での脆弱性検査やペネトレーションテストを行うことは難しい。しかし、サイバー攻撃手法は日々進化しており、重要な制御システムに対しては本番環境でのテストの実施を検討することが望ましい。

新規制御システムの稼働前は、本番環境で脆弱性検査やペネトレーションテストを実施するよい機会である。制御システムのライフサイクルは情報システムに比べて長いため、制御システム稼働前試験において、脆弱性検査やペネトレーションテストを実施する工数を確保することを推奨する。

本番稼働後の制御システムに対しては、定修期間等、システムの停止が可能なタイミングでの実施を検討する。本ガイドのモデルシステムを例にすると、制御ネットワーク（フィールド側）の PLC と PLC に接続したフィールド機器が停止する際に、FW や DMZ の機器への脆弱性試験やペネトレーションテストが実施できないかを検討する。

制御システムの FW は制御システムの要のセキュリティ装置であり、FW の脆弱性の存在や設定不備、構成不備（3.1.1 項（6）参照）は制御システムのセキュリティを著しく損なう。このため、付録 B.4 のファイアウォール設定チェックリストを活用すると共に、FW の脆弱性検査は定期的に本番環境で実施することを推奨する。

6.5. パケットキャプチャテスト

（1）パケットキャプチャテストの目的

パケットキャプチャテストの目的は、制御システムの機器やサーバ、端末におけるマルウェア感染や不正操作によるネットワーク上の不審な通信の有無を調査することである。不審な通信が発見された場合は、マルウェアの感染の有無や正規の操作であるか否かを確認する。マルウェア感染や不正操作と確認できた場合はそれを取り除き、再発防止策を講じるのがよい。

不審な通信の代表例は、感染したマルウェアによる外部との通信や制御システム内部での不正コマンド発行であり、他には内部犯行者による不正操作等が考えられる。

パケットキャプチャテストでは、既存もしくはテスト用に設置したスイッチやルータで複製したパケットを取得し、取得したパケットを分析する。マルウェア感染調査のサービスでは、セキュリティベンダの保有するブラックリスト（通信相手や通信内容等）との照合、セキュリティベンダの独自ノウハウによるパケット分析等が行われる。一方、内部犯行者等の不正操作を確認する方法としては、事前に収集しておいた平常時の操作・通信のパケットとテストで取得した比較し、平常時にはなかった操作・通信を抽出する方法が取られる。

（2）パケットキャプチャテストの対象と実施例

制御システムのパケットキャプチャテストの対象は、制御ネットワーク以外（DMZ・情報ネットワーク等）から制御ネットワークへの通信、制御ネットワーク内の通信、制御ネットワークから制御ネットワーク以外への通信である。

パケットキャプチャの箇所が多い場合は、5.1 節（5）、5.2 節（5）を参照し、リスク分析結果を踏まえてテスト箇所を絞りこむとよい。

本ガイドのモデルシステムにおけるパケットキャプチャテストの対象範囲の例を、図 6-3 に示す。図中に示した、パケットを取得するためのキャプチャ装置の設置位置①～③と、その場合のパケットを取得するネットワーク範囲の関係を、表 6-9 に示す。

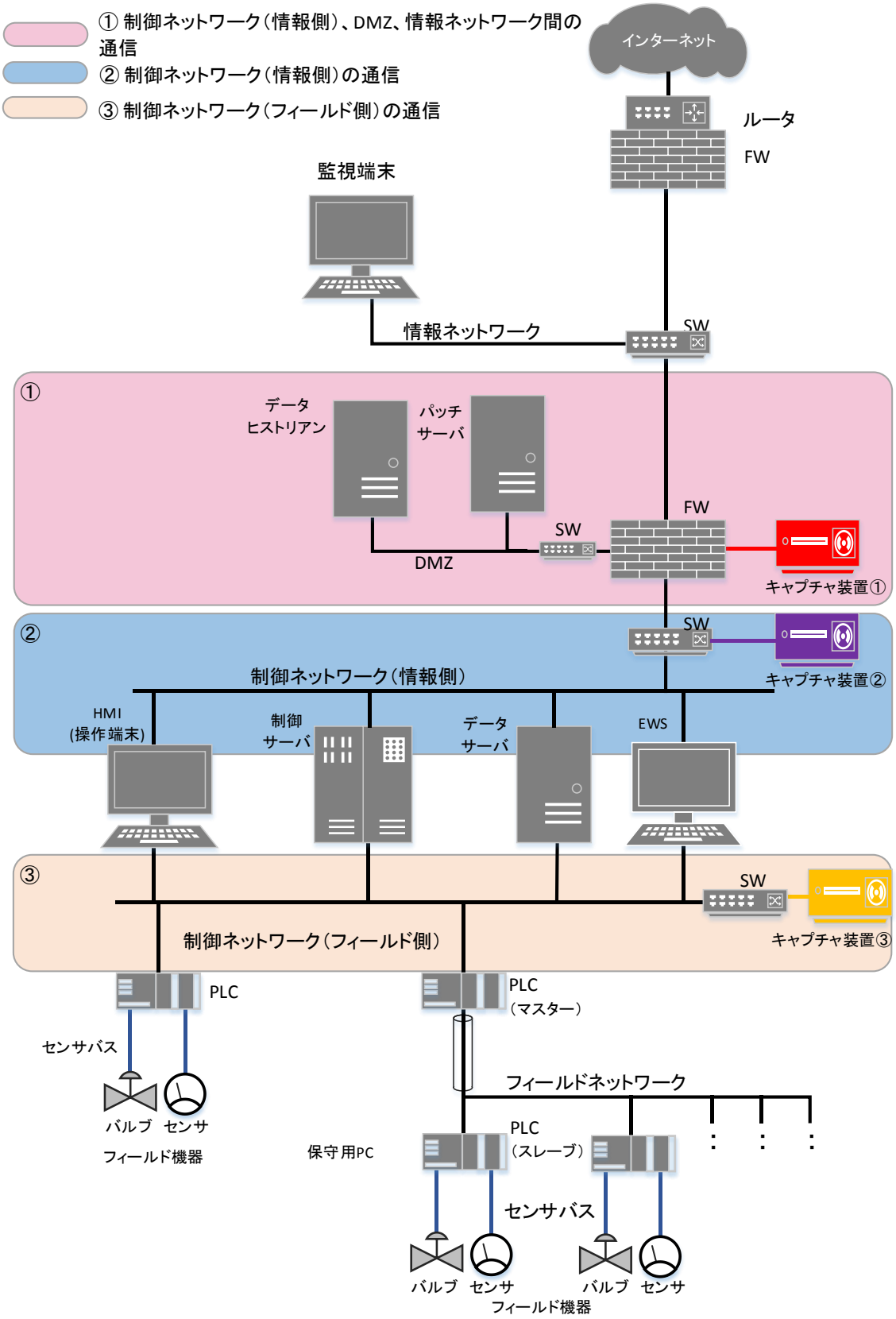


図 6-3 パケットキャプチャテストの対象範囲の例

表 6-9 キャプチャ装置の位置とパケットキャプチャ範囲

キャプチャ装置の設置位置		パケット取得対象のネットワーク
①	ファイアウォール	ファイアウォールを経由する通信 ・制御ネットワーク（情報側）と DMZ 間の通信 ・制御ネットワーク（情報側）と情報ネットワーク間の通信 ・DMZ と情報ネットワーク間の通信
②	制御ネットワーク （情報側）スイッチ	制御ネットワーク（情報側）スイッチを経由する、制御ネットワーク（情報側）内の通信
③	制御ネットワーク （フィールド側）スイッチ	制御ネットワーク（フィールド側）スイッチを経由する、制御ネットワーク（フィールド側）内の通信

（3）パケットキャプチャテストの実施環境

パケットキャプチャテストは、制御ネットワーク上における不審な操作・通信の有無を調査するテストのため、パケットの取得は本番環境で実施する必要がある。

（4）パケットキャプチャテストの注意点

- パケットキャプチャテストだけでは、潜伏しているマルウェア（ネットワーク通信をしていないマルウェア）を検出することはできない。常時、あるいは定期的にパケットキャプチャテストを実施することが望ましい。

- パケットを複製している機器の CPU やメモリのリソースを圧迫して通常業務に悪影響を及ぼさない様に、パケットを複製する対象範囲（送信元ネットワーク範囲、送信先ネットワーク範囲、取得するプロトコルやアプリケーションの種類）を調整することが望ましい。

- 制御ネットワーク内の通信（特に制御ネットワーク（フィールド側））は、制御システム固有の通信プロトコルが利用される場合が多い。この場合は、制御システム固有の通信プロトコルに対応したパケットキャプチャ装置やソフトウェアを選択する必要がある。

6.6. セキュリティテスト結果の活用

セキュリティテストで制御システムに明らかな脆弱性が発見された場合、追加のセキュリティ対策が必要となる。

追加対策の優先順位の判断が必要な場合は、追加対策が該当するリスク分析の資産または攻撃ツリーの脅威レベルや脆弱性レベルを見直し、リスク値を再検討する。再検討したリスク値が高い資産や攻撃ツリーに対しての追加対策を優先的に実施するという判断が可能である。

セキュリティテストは、工数とコスト、実施形態や手法等の制約から、テスト可能な範囲（機器やルート等）が限定されることがある。仮に、脆弱性が検出されなかったとしても、実施範囲以外において脆弱性が残留している恐れがあることを認識すべきである。従って、テストの実施範囲や実施したテストのレベル等の詳細を記録に残し、以後の PDCA サイクルの検討の中で活用していくことが重要である。

7. 特定セキュリティ対策に対する追加基準

本章では、特定のセキュリティ対策に対する追加基準を示す。

各追加基準は、いくつかに分類された複数の評価項目からなる。各評価項目には、「必須」または「推奨」のセキュリティ要件を設定し、要件のもととなった国際標準・業界標準等の関連箇所を参照として記載した。また、各々の詳細評価項目一覧表は「チェックリスト」として利用可能となっており、各社における対応状況（各評価項目に対する判定とその根拠）を記入することで、それぞれのセキュリティ技術に関する設計・運用状況を明確化し、第三者によって適切であるか否かを判定する際に利用することができる。

各々の表における各項目の意味は、以下の通りである。

- 「評価項目とセキュリティ要件」
  特定のセキュリティ対策に対して設定した評価項目と、それに対する必須及び推奨のセキュリティ要件。

- 「参照」
  評価項目とセキュリティ要件のもととなった国際標準・業界標準等の参照箇所。

- 「回答想定者／部門」
  内部不正対策の追加基準のみに存在する項目で、評価項目と要件に記載された質問（対策実施の有無）に回答すべき回答想定者（経営層）あるいは回答想定部門。

- 「チェックリスト回答欄」
  各電力会社において、セキュリティ要件への対応を記入することによって、特定のセキュリティ技術に関する対策実施状況を視覚化するチェックリストとして使用するための回答欄。
  判定欄において「○（合格）」「×（不合格）」「－（非該当）」のいずれかを選択し、根拠（任意記入欄）にその理由をフリーテキストで記入できる様になっている。

7.1. 暗号技術の選定と活用基準

制御システムにおいては、保護資産に対する不正アクセス、盗聴、改ざん・偽造、なりすましといった脅威への対策として、暗号技術を用いた認証、電子署名、暗号化を導入することが考えられる。しかしながら、暗号技術を導入しても、暗号アルゴリズムの鍵長の選択、暗号鍵の管理(鍵の生成・配布・保管・用途・廃棄、鍵の一意性)、鍵関連情報(パラメータ)の取り扱いに不備が存在した場合、それらの脆弱性を攻撃して認証、電子署名、暗号化の効果を無効化する攻撃が成立する。

付録 B.1 に、評価対象システムで採用した暗号技術の安全性を確認する詳細評価項目と要件を記載する。評価項目の設定に当たっては、米国政府機関である NIST(National Institute of Standards and Technology、アメリカ国立標準技術研究所)が定めた暗号鍵のガイドライン(NIST Special Publication 800-57, Recommendation for Key Management)[45]、スマートグリッドのセキュリティガイドライン (NISTIR 7628, Guidelines for Smart Grid Cybersecurity)[46]、CRYPTREC(Cryptography Research and Evaluation Committees)で定めた電子政府推奨暗号リスト[47]等の規定を参考に評価項目を設定した。

[45] http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
[46] http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
[47] http://www.cryptrec.go.jp/list.html

7.2. 標的型攻撃対策

近年、政府機関や企業に対する標的型攻撃が問題となっているが、重要インフラである制御系システムに対する標的型攻撃も発生している。一般に、標的型攻撃においては、攻撃対象組織が導入しているマルウェア対策技術を含む組織情報を事前に調査し、その防御方法を突破する技術を用いたり、人間を含む運用管理の脆弱性を突いたりすることによって、マルウェアの侵入を試みる。イランの核施設攻撃に用いられた Stuxnet は、これまで一度も使用されたことがない、攻撃対象専用に作り込まれた、非公開の脆弱性を突いた(ゼロディの)専用マルウェア(ワーム)であり、USB メモリを介して侵入したと言われている。

付録 B.2 に、評価対象システムにおける標的型攻撃対策を確認する詳細評価項目と要件を記載する。標的型攻撃における攻撃技術及びその防御技術は日々進歩しており、完璧な対抗策を示すことは困難であるが、各評価項目では考慮しておくべき攻撃・防御のポイントを示している。また、重要インフラに対する標的型攻撃対策のガイドラインは現時点で存在しないため、各項目と「政府機関の情報セキュリティ対策のための統一基準(平成 28 年度版)」[48]との関係を示す。

[48] http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf

7.3. 内部不正対策

近年、企業における内部不正による情報漏えいや企業機密の不正流出といった情報セキュリティ事故が発生し、事業の根幹を脅かしている。海外における制御システムにおいても、金銭目的で従業員がシステムのセキュリティを破り、高額の損害を生じる事件が発生している。内部関係者はシステム内部の構成を熟知しているため、内部犯罪によるシステムへの攻撃は甚大な被害へと繋がる可能性が高い。今後は、重要インフラへの脅威として、攻撃者が意図的に手先の者を事業者へと送り込み、内部からの情報窃取や攻撃・破壊を試みる可能性も考えられるため、内部不正対策は重要であると考えらえる。

付録 B.3 に、評価対象システムにおける内部不正対策を確認する詳細評価項目と要件を記載する。評価項目の設定に当たっては、IPA が作成・公開している「組織における内部不正防止ガイドライン」[49]の内部不正チェックリスト、米国カーネギーメロン大学ソフトウェア工学研究所に設置された CERT／内部脅威センターによって発行された「内部脅威への 19 のベストプラクティス（Best Practices Against Insider Threats in All Nations）」[50]の規定を参照・抽出した。

[49] https://www.ipa.go.jp/security/fy24/reports/insider/index.html
[50] http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_59084.pdf

7.4. ファイアウォールにおける各種設定

近年、制御システムの汎用化に伴い、制御システムがインターネットの様な公衆網に直接もしくは間接的に接続されるケースが多くなってきている。従来の情報系システムにおいてはインターネットからの攻撃を想定した対策が施されているが、制御システムにおいてはその対策は十分とは言い難い。一般的な対策として制御システムにおける外部接続点にファイアウォールを設置し、制御システムを隔離することが対策として挙げられている。

付録 B.4 に、NIST Special Publication 800-82 Revision 2 を参考に、制御システムの境界防御チェックリスト、境界ファイアウォールチェックリストの 2 つを提示する。各チェックリストの内容を、以下に示す。

- **制御システムの境界防御チェックリスト**
  対象制御システムにおける、制御ネットワーク及びフィールドネットワークの境界（DMZ 及びその他の外接点）全般に関するセキュリティ要件を記載
- **境界ファイアウォールチェックリスト**
  対象制御システムにおいて、制御ネットワークと情報ネットワークの間に設置される、境界ファイアウォールに関するセキュリティ要件（ファイアウォールルール設定時の注意事項、プロトコルごとのルール設定注意事項等）を記載

ファイアウォールに関する要件は、NIST SP800-82 の規定を継承し、全て推奨項目となっているが、いずれの要件も重要な項目である。要件を満たしていない場合は、リスク分析の結果として重大事業被害を引き起こす恐れがある項目は即時の対策を実施すると共に、システム更改時には全ての要件を満たす様にシステム設計を行うことを推奨する。なお、セキュリティ要件は、ファイアウォールの機種に依存する機能については極力除外し、一般的なファイアウォールが有していると想定される機能を要件としている。

本チェックリストは、導入しているファイアウォールの設定内容を確認する目的で作成している。よって、4.1.4 項及び 4.2.5 項で述べた対策レベルの評価において検討するファイアウォールの対策レベルとは直接関係していない点は留意していただきたい。

また、付録 A にファイアウォールに関する概要、分類、ファイアウォールを活用したシステムアーキテクチャをまとめているので、興味のある方は参照していただきたい。付録 A に記載したファイアウォールのアーキテクチャごとに対応する確認項目をチェックリストの構成パターンの欄に記している。自組織のアーキテクチャと照らし合わせて、当該項目を中心に確認することを推奨する。

7.5. 外部記憶媒体におけるセキュリティ対策

近年、企業における不正プログラム感染や内部不正による情報漏えい、企業機密の不正流出や基幹業務システムの停止に繋がる様な各種の情報セキュリティ事故が発生し、事業の根幹を脅かしている。その原因の中でも、外部記憶媒体を介した不正プログラム感染や情報漏えいのリスクは大きく、その利用におけるセキュリティ対策は重要である。

付録 B.5 に、外部記憶媒体におけるセキュリティ対策を確認する詳細評価項目と要件を記載する。評価項目の設定に当たっては、内閣官房・内閣サイバーセキュリティセンターが作成・公開している「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」[51]及び「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」[52]を参照した。

なお、外部記憶媒体としては、

- USB メモリ等の端末の USB ポートに接続可能な USB マスストレージクラスのデバイス
- CD、DVD や SD カード等

を想定しており、セキュリティ上の脅威としては、

- 情報漏えい
- 不正プログラム感染

を想定したものとなっている。

[51] https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf
[52] https://www.nisc.go.jp/active/general/pdf/guide28.pdf

参考文献

【IPA 公開情報】

制御システムのセキュリティ, IPA, 2017/5/19
https://www.ipa.go.jp/security/controlsystem/index.html

「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」, IPA, 2009/3/30
https://www.ipa.go.jp/files/000025097.pdf

「制御システムセキュリティの推進施策に関する調査報告書」, IPA, 2010/5/31
https://www.ipa.go.jp/about/press/20100531_3.html

「2010 年度 制御システムの情報セキュリティ動向に関する調査 調査報告書」, IPA, 2011/5/9
https://www.ipa.go.jp/files/000025095.pdf

「制御システムにおけるセキュリティマネジメントシステムの構築に向けて ～IEC 62443-2-1 の活用のアプローチ～」, IPA, 2012/10/10
https://www.ipa.go.jp/files/000014265.pdf

「組織における内部不正防止ガイドライン（日本語版）第 4 版」, IPA, 2017/1/31
https://www.ipa.go.jp/files/000057060.pdf

「制御システム利用者のための脆弱性対応ガイド 第 3 版」, IPA, 2017/3/30
https://www.ipa.go.jp/files/000058489.pdf

【NISC（内閣サイバーセキュリティセンター）文書】

「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」, NISC, 2016/8/31
https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf

「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」, NISC, 2016/8/31
http://www.nisc.go.jp/active/general/pdf/guide28.pdf

「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第1版）」, NISC, 2015/5/25

https://www.nisc.go.jp/active/infra/pdf/shishin-tebiki1.pdf

【国際標準規格】

IEC/TS 62443-1-1: 2009, Industrial communication networks - Network ans system security - Part 1-1: Terminology, concenpts and models

IEC 62443-2-1: 2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

【NIST 文書】

NIST Special Publication 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy, NIST, 2009/9
http://csrc.nist.gov/publications/PubsSPs.html#800-41

NIST Special Publication 800-57 Part 1 Rev.4, Recommendation for Key Management, Part 1: General, NIST, 2016/1
http://csrc.nist.gov/publications/PubsSPs.html#800-57pt1r4

NIST Special Publication 800-57 Part 1 Revision 4, 鍵管理における推奨事項 第一部:一般事項, IPA, 2016/11/11
https://www.ipa.go.jp/files/000055490.pdf

NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security, NIST, 2015/5
http://csrc.nist.gov/publications/PubsSPs.html#800-82

NIST SP800-82 第 2 版 産業用制御システム(ICS)セキュリティガイド SCADA、DCS、PLC、その他の制御システム設定 日英対訳版, JPCERT/CC, 2016/3/14
https://www.jpcert.or.jp/ics/information02.html#NISTSP800-82

付録 A. ゾーニングにおけるファイアウォールの活用パターン

付録Aでは、制御システムを保護する上で重要な役割を果たしているファイアウォールの解説を行い、本付録にて扱っているファイアウォールを定義、分類する。更に、制御システムにおけるファイアウォールを用いたシステムアーキテクチャを整理する。

A.1. ファイアウォールの定義

広義のファイアウォールの定義において、ファイアウォールは以下の機能を有すると捉えられている。

① トラフィックをモニタし、定義済みのセキュリティルールセットに基づいて、特定のトラフィックを「許可する」もしくは「拒否する」のいずれかを決定する。
② 許可もしくは拒否するプロトコル、レイヤ、実装手段は問わない。

上記定義では、プロトコル、レイヤを特定していない。そのため、メールフィルタや URL フィルタ等の機能も含まれることになる。また、実装手段も規定していないため、ファイアウォール専用のアプライアンス機器[53]に加えて、アクセスコントロールリストを設定したルータや PC／サーバの OS 上のファイアウォール機能（Windows ファイアウォール）等も含まれる。

この定義では、ファイアウォールとして捉えられる幅が広く、制御システムのセキュリティ対策としての検討が多岐にわたり発散することが懸念される。そこで、本付録では、次項による分類を行い、狭義のファイアウォールを定義する。

[53] ファイアウォール専用のアプライアンス機器は、複数のレイヤ、プロトロコルに対応している場合もある。

A.2. ファイアウォールの分類

ファイアウォールを分類する前に、ファイアウォールが有する主な機能を説明する。

ファイアウォールの主要な技術は、「NIST SP800-41 Rev.1: Guidelines on Firewalls and Firewall Policy」[54]において定義されているが、制御システムのセキュリティ対策の観点で整理すると、ファイアウォールの代表的な機能としては、以下が挙げられる。

- パケットフィルタリング（ステートレスインスペクション）
- ステートフルインスペクション
- アプリケーションプロキシファイアウォール
- アプリケーションファイアウォール（DPI: Deep Packet Inspection）
- ウェブアプリケーションファイアウォール（WAF）

（1）パケットフィルタリング（ステートレスインスペクション）

最も基本的なファイアウォールの機能であり、パケットのヘッダに含まれる、送信元アドレス、宛先アドレス、送信元ポート番号、及び宛先ポート番号に基づいて、トラフィックの許可と拒否を行う。実装コストが安価であり、かつ、パケットを高速に処理することができることが特徴である。反面、パケットのヘッダ部では拒否できないパケット、例えば、マルウェアを添付したメールやブラウザの脆弱性を突いたアクセスを防御することはできない欠点を有する。

（2）ステートフルインスペクション

ステートフルインスペクション[55]は、パケットの内容をトランスポート層でも評価するフィルタリング機能である。具体的には、あるアプリケーションの通信においてやり取りされるパケットを順番に見て、その通信の状態を把握する。そして、次に届くパケットの状態（例えば、DNS の戻りパケット等）を予測し、届いたパケットが矛盾していれば不正パケットとして拒否する機能である。例えば、TCP パケットが順番通りになっていなければ不正パケットとして判断する。ステートフルインスペクションは、パケットフィルタリングに比べセキュリティレベルは向上するが、設定が複雑になる欠点もある。また、パケットフィルタリングと同様、マルウェアを添付したメールを防ぐことはできない。

ステートフルインスペクションは、動的パケットフィルタリング[56]、サーキットレベルゲートウェイ型フ

---

54 http://dx.doi.org/10.6028/NIST.SP.800-41r1
55 http://itpro.nikkeibp.co.jp/article/lecture/20070508/270250/
56 動的パケットフィルタリングとステートフルインスペクションを区別する場合もある。この場合、前者は通信開始時に当該ポートを開き、通信終了時にそのポートを閉じる機能として用いられている。

ァイアウォールとも呼ばれている。

（3）アプリケーションプロキシファイアウォール

アプリケーションプロキシファイアウォールは、パケットをアプリケーション層で検証し、特定のアプリケーションルールに従ってトラフィックをフィルタリングする。クライアントは外部サーバに直接接続せずに、アプリケーションプロキシファイアウォールに接続し、アプリケーションプロキシファイアウォールは要求された外部サーバへの接続を開始する。アプリケーションプロキシファイアウォールは telnet、FTP、HTTP 等プロトコルごとに個別に設置することも、まとめることもある。

アプリケーションゲートウェイ型ファイアウォール、アプリケーション・プロキシゲートウェイファイアウォールとも呼ばれている。

（4）アプリケーションファイアウォール（DPI）

パケットのヘッダ部分だけではなく、データ部まで検査する機能を有するファイアウォールを、アプリケーションファイアウォールという。アプリケーションファイアウォールは、ディープパケットインスペクション（以下、DPI）とも呼ばれる。データの内容まで調べることにより、プロトコルの準拠、マルウェアの有無、スパムメールか否か、及び不正アクセスの兆候を調べることが可能となる。検査結果を元に、当該パケットをフィルタリングすることができる。パケットフィルタリングは IP ヘッダによってフィルタリングを実施し、ステートフルインスペクションは TCP ヘッダや UDP ヘッダによってフィルタリングを実施するのに対して、DPI はデータの更に深い部分の内容を検査している。故に、DPI を悪用すると、誰がどの様な情報に関心を持っているか、どの様なデータを送受信しているか把握される危険をはらんでいる。

（5）ウェブアプリケーションファイアウォール（WAF）

ウェブアプリケーションの脆弱性を悪用した攻撃を防御するファイアウォールを、ウェブアプリケーションファイアウォール（以下、WAF）という。事前に定義された検出パターンによって、パケットを検査する。ウェブアプリケーションに特化している点が特徴である。

ファイアウォールの主要機能（1）～（5）のうち、一つもしくは複数の機能を有するシステムを、狭義のファイアウォールと定義する。本定義では、広義の定義において含まれたメールフィルタリング機能や URL フィルタリングの機能は含まれないことになる。また、実装形態は広義の定義と同様、規定していないため、ルータの一機能としての実装、専用ハードウェア（アプライアンス機器）としての実装、汎用パソコン等による実装いずれでも可とする。

上記のファイアウォール機能を、パケットを検査するネットワークレイヤによる分類を行った結果を、表 A-1 に示す。

また、ファイアウォール機能を、防御できる攻撃によって分類した結果を、表 A-2 に示す。

表 A-1 TCP/IP 階層モデルによるファイアウォールの分類

OSI 階層モデル	代表的なプロトコル	パケットフィルタリング型	ステートフル インスペクション型	アプリケーション ファイアウォール	プロキシ ファイアウォール	WAF
アプリケーション層 プレゼンテーション層 セション層	HTTP/FTP/ SMTP/POP3			○	○	○
トランスポート層	TCP/UDP		○			
ネットワーク層	IP/ICMP	○	○			
データリンク層	Ethernet/PPP/					

表 A-2 防御する攻撃手法によるファイアウォールの分類

攻撃対象	攻撃手法	パケットフィルタリング型 ステートフルインスペクション型	IPS/IDS[57]	WAF
WEB アプリケーション WEB サーバ WEB システム	SQL インジェクション クロスサイトスクリプティング			○
OS	DoS 攻撃 Syn フラッド攻撃		○	
ネットワーク	ポートスキャン	○		

[57] IPS/IDS の有する IPS（Intrusion Prevention System）機能は広義の定義においてファイアウォール機能と考えることができる。但し、IDS/IPS はシグネチャと呼ばれるパターンファイルによって外部からの侵入の検知、防止を図っている。そのため、狭義の定義においては、ファイアウォールとは別装置と考えることとする。

A.3. ファイアウォールの実装アーキテクチャ

本節において、制御システムにおけるファイアウォールの実装アーキテクチャの分類を行う。CPNI（Centre for the Protection of National Inftrastracture）が公開している「Firewall Deployment for SCADA and Control Networks - Good Practice Guide」[58]において定義されている、7 パターンのファイアウォールのアーキテクチャを紹介する。また、各アーキテクチャのシステム構成上の長所短所について、末尾の表 A-3 に示す。

各事業者において、自組織のシステム内のどの位置に（どこに）、どの様な形態（アプライアンス機器、ルータ、パーソナルファイウォール）で設置しているかを確認することが望ましい。付録 B.4 に記載する「ファイアウォール設定チェックリスト」を実施する事業者は、自組織のファイアウォールのアーキテクチャがどのパターンに属しているかを、事前に確認しておくこと。

[58] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/2005022-gpg_scada_firewall.pdf

（1）パターン#1（デュアルホーミング）

情報ネットワークと制御ネットワークの双方に情報アクセスを必要とするサーバに、ネットワークインタフェースカード（NIC）を 2 枚挿すアーキテクチャである。この技術をデュアルホーミングと呼ぶ。デュアルホーミングを用いた構成図を、図 A-1 に示す。このアーキテクチャは最小限のネットワークの分離を可能にしているが、一つのネットワークに到着したパケットを別のネットワークに自動的に転送するが可能である。更に、NIC を 2 枚挿しているサーバは制御ネットワークの一部でもあり、かつ、インターネットへアクセスできるネットワークの一部でもある。このことは、制御ネットワークからインターネットに直接接続されないというセキュリティ要件を満たしていない可能性がある。パターン#1 はネットワークを分割しているが、ファイアウォールとしての機能を有しているとは言い難い。そのため、付録 B.4 に添付したチェックリストの構成パターンから本例は除外している。

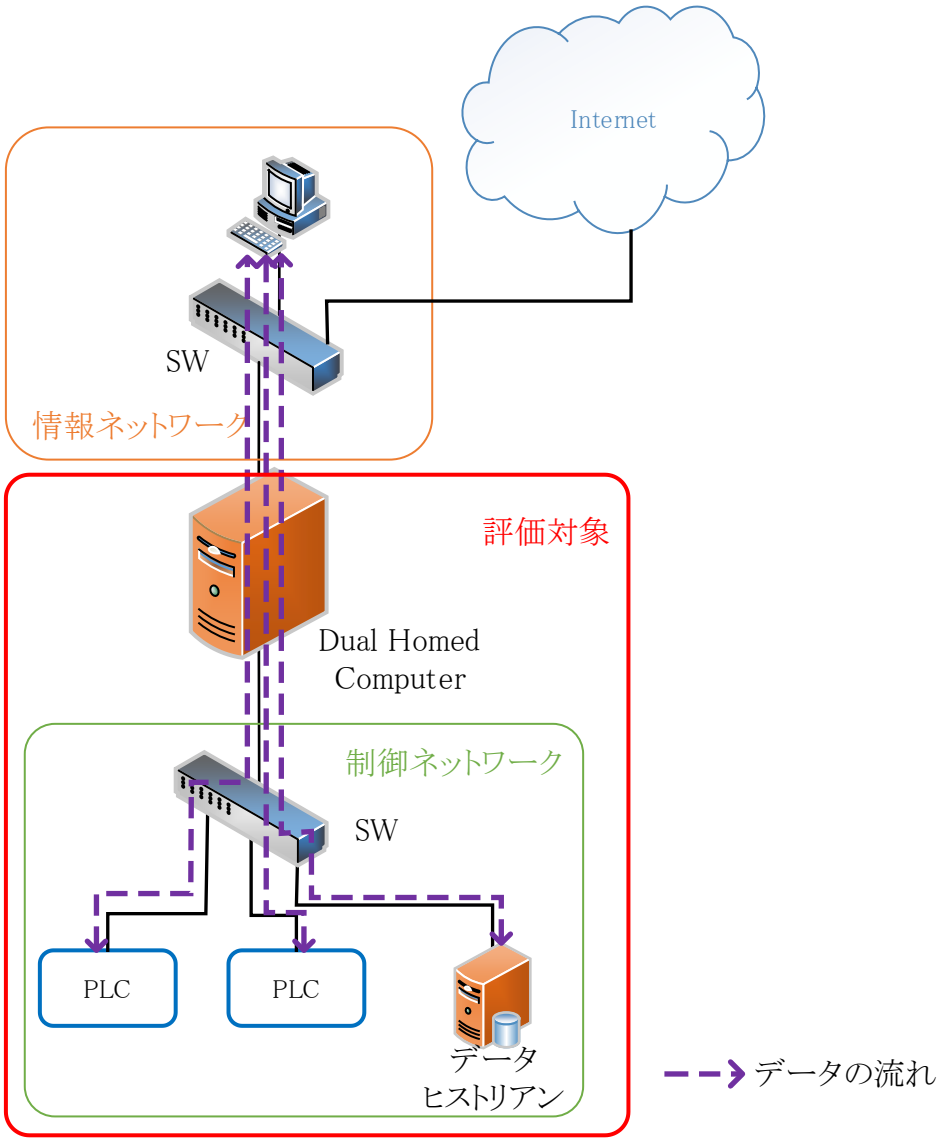


図 A-1 デュアルホーミングを用いたアーキテクチャ（パターン#1）

（2）パターン#2（パーソナルファイアウォールを有するデュアルホーミング）

図 A-1 に示したデュアルホーミングのアーキテクチャに、パーソナルファイアウォールのソフトウェアをインストールしたアーキテクチャである。本アーキテクチャにおけるデュアルホーミングサーバは、データヒストリアンと同一であることが多い。本アーキテクチャを、図 A-2 に示す。このアーキテクチャは、情報ネットワークと制御ネットワーク間のトラフィックは、共有履歴データ（データヒストリアンに格納されているデータ）のみであり、パーソナルファイアウォールをデータヒストリアンから業務ユーザへのデータ要求だけを許可する様に使用するのであれば、低コストでセキュリティ対策を実施できる。

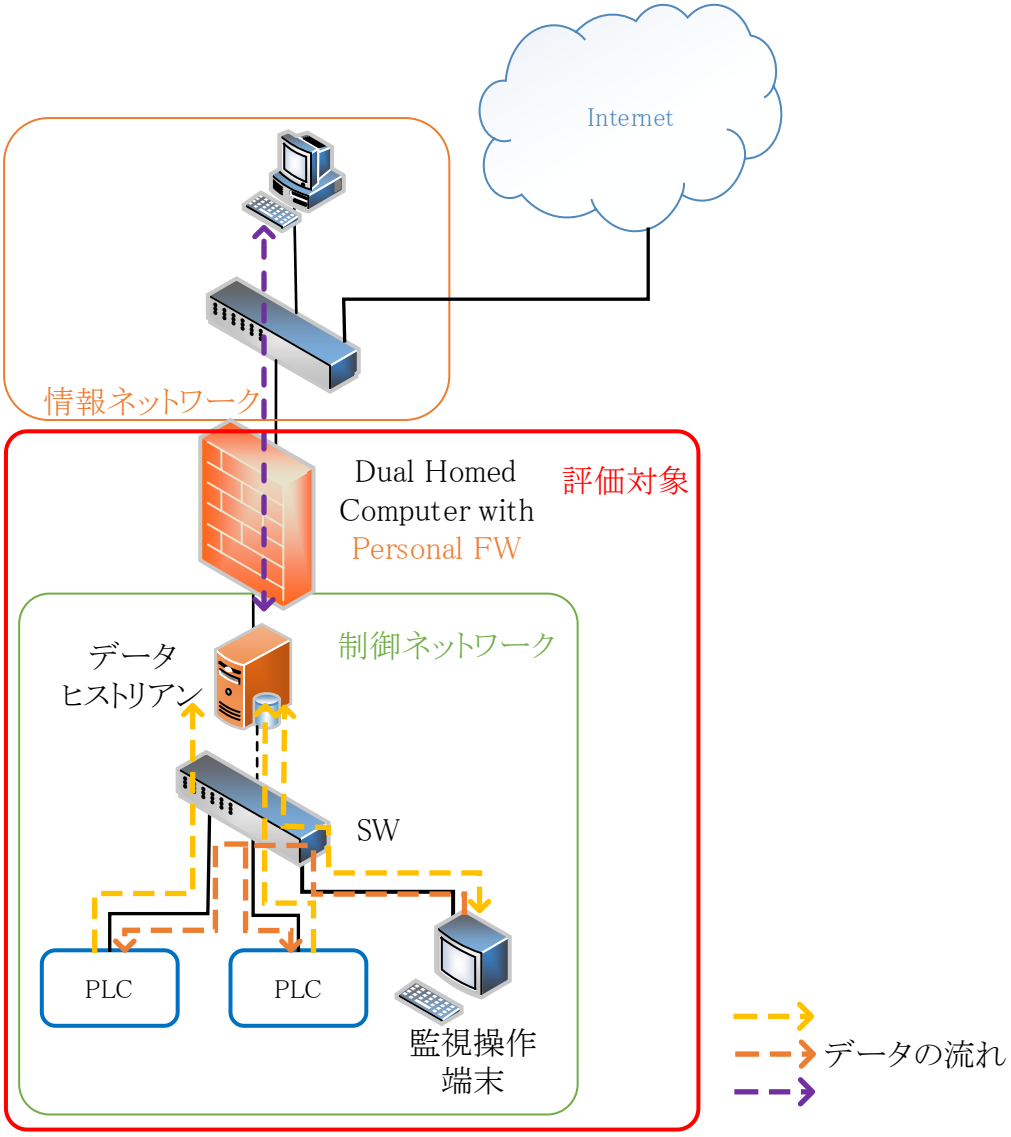


図 A-2 パーソナルファイアウォール機能用いたアーキテクチャ（パターン#2）

通常、本アーキテクチャにおいては、履歴データ（状態管理データ）の送受信が情報ネットワークとデータヒストリアンの間、及び PLC もしくは管理操作端末とデータヒストリアンの間で行われ、これらの通信はデータヒストリアンで終端する（図 A-2 におけるデータの流れ）。履歴データ以外に情報ネットワークから制御ネットワークに送信される通信（例えば、リモート保守端末から PLC へのアクセス等）がある場合、本アーキテクチャでは、その通信を完全にブロックするか、もし当該通信をブロックすることができなければ、制御ネットワークへの侵入のリスクが高まり、制御ネットワーク自身のセキュリティレベルが低下する。また、データヒストリアンが複数台ある場合、複数のデータヒストリアンに対して、首尾一貫したルールセットを設定し、管理維持することは非常に困難である。

（3）パターン#3（パケットフィルタリング機能）

トラフィックをルータもしくは L3SW（Layer3 スイッチ）[59]の機能によって制御するアーキテクチャを、図 A-3 に示す。

このアーキテクチャはパケットフィルタリング型ファイアウォールの機能を有しているが、ステートフルインスペクションの機能を持たないため、フラグメンテーション[60]等を巧みに用いた攻撃を防ぐことは困難である。情報ネットワークが非常に安全に設計されている場合は、このアーキテクチャは有効である。

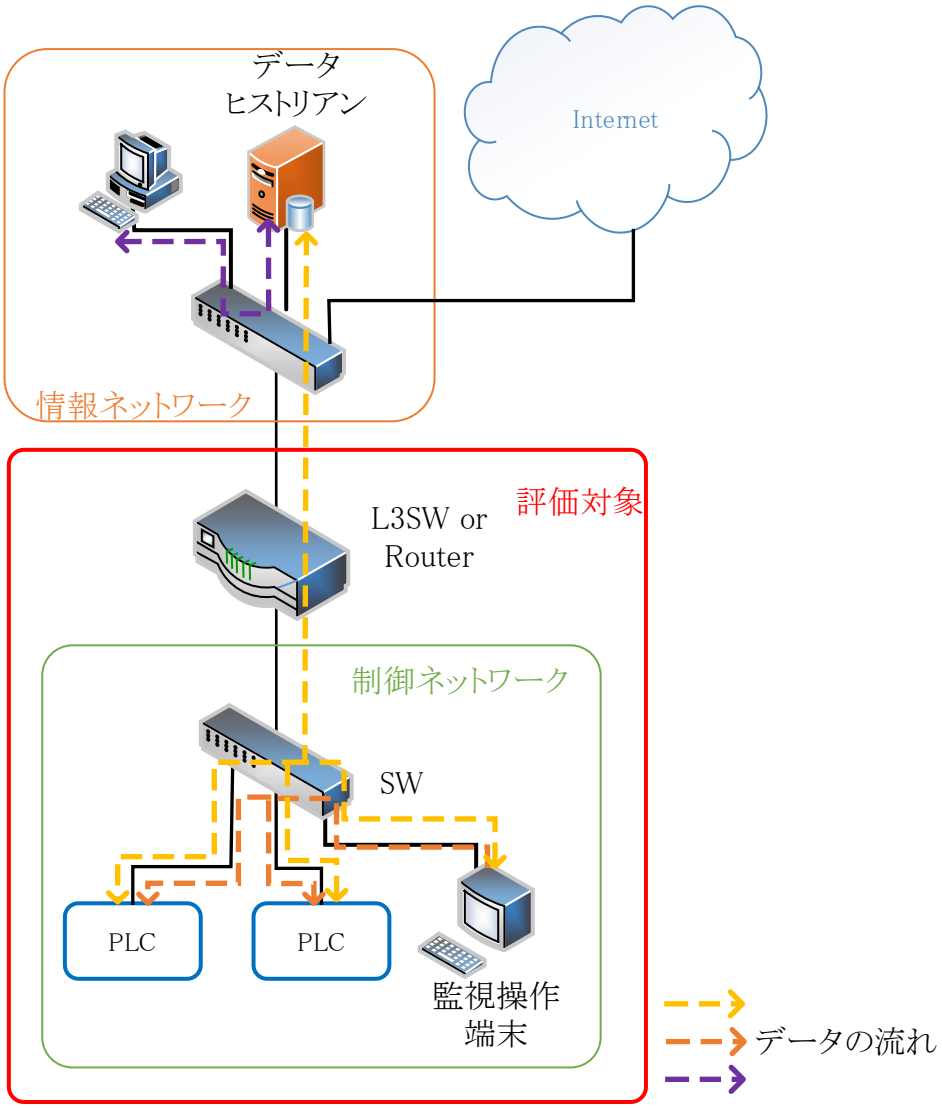


図 A-3 パケットフィルタリング機能を用いたアーキテクチャ（パターン#3）

59 パケットフィルリング機能のみを有するファイアウォールのアプライアンス機器も存在するが、現在ではその様な製品は少ないと思われる。反面、ルータや L3SW ではパケットフィルタリング機能のみしか実装できない機器があるため、ルータ、L3SW とした。

60 一度に送信することができない大きなパケットをいくつかに分割して送信する技術をフラグメンテーションと言う。

（4）パターン#4（ステートフルインスペクション機能＋プロキシ機能）

アプライアンス機器として提供されるファイアウォールの多くは、パケットフィルタリング機能に加え、ステートフルインスペクションやアプリケーションレイヤのプロキシ機能を有している。ステートフルインスペクション機能を有するファイアウォールを用いたアーキテクチャを、図 A-4 に示す。本ファイアウォールにより、全 TCP パケットに対するステートフルインスペクションを提供し、FTP、HTTP、SMTP 等のアプリケーションレイヤのプロトコルに対してプロキシサービスを提供することが可能である。設定を強固にすることで、外部ネットワークから制御ネットワークへの攻撃が成功する可能性を低下させることが期待できる。

本アーキテクチャを採用する場合、データヒストリアンの設置場所に応じて、ファイアウォールの設定ルールを考慮する必要がある。図 A-4 に示した様に、データヒストリアンが情報ネットワークに設置された場合、データヒストリアンが制御ネットワーク上の制御装置との通信を許可するルールをファイアウォールに設定する必要がある。情報ネットワーク上に悪意のあるホストまたは誤って設定されたホストからのパケットは個々の PLC に転送される可能性がある。また、図例に示していないが、データヒストリアンが制御ネットワーク上に設置された場合、情報ネットワーク内の全てのホストがデータヒストリアンとの通信を許可するルールをファイアウォールに設定しなければならない。この様な通信は SQL や HTTP のリスクエスト等が考えられ、データヒストリアンに脆弱性が存在した場合、攻撃が可能である。データヒストリアンがマルウェアに感染すると、制御ネットワークの残りのノードも拡散し、外部からの攻撃が容易になることも考えられる。

また、許可されたプロトコルになりすました不正なパケットがファイアウォールを通過し、制御ネットワークに影響を及ぼす可能性がある。例えば、HTTP パケットがファイアウォールの通過を許可されている場合、監視操作端末に感染したマルウェアが遠隔制御され、正当なトラフィックとして偽装したデータを遠隔の攻撃者に送信する恐れがある、という問題を含んでいる。先の例のデータフローを、図 A-4 に示す。

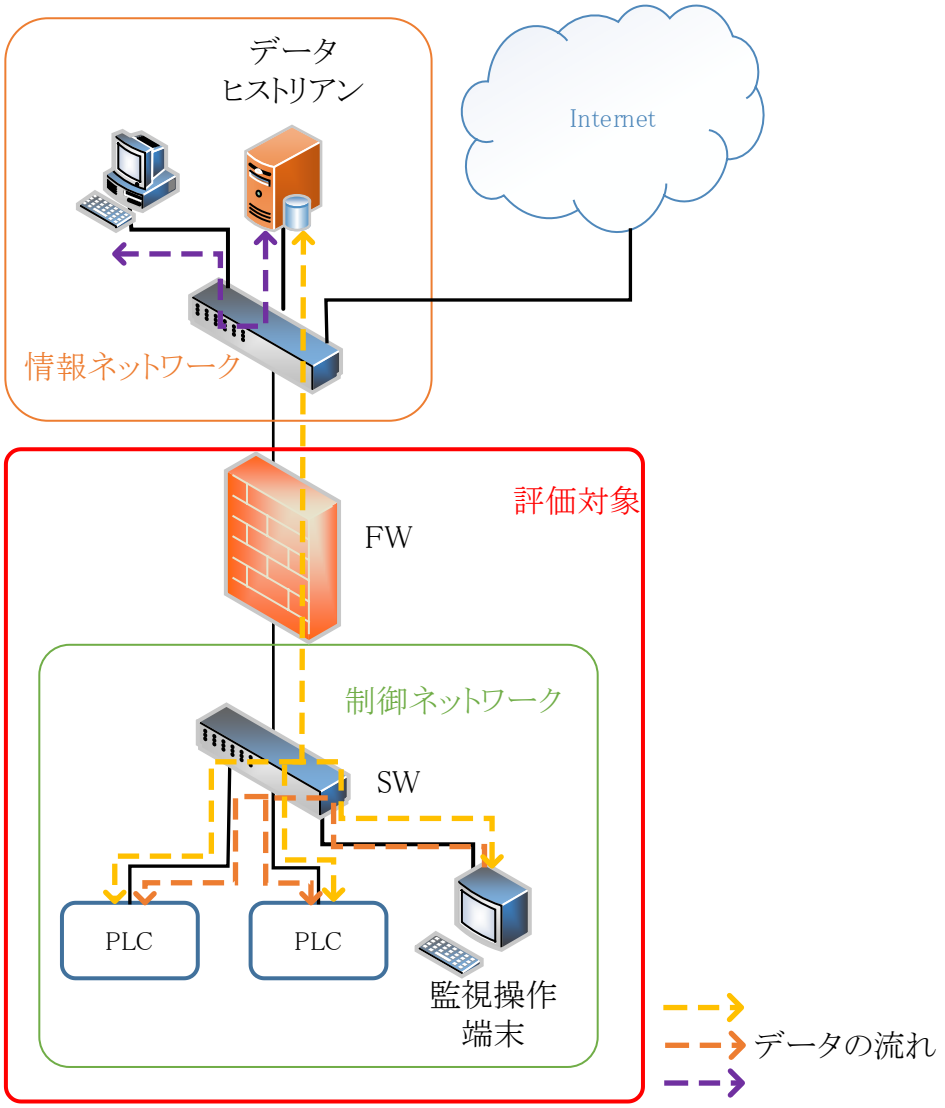


図 A-4 ステートフルインスペクション＋プロキシ機能を用いたアーキテクチャ（パターン#4）

（5）パターン#5（DMZ）

情報ネットワークと制御ネットワークの間に DMZ（非武装地帯）を設け、DMZ にデータヒストリアンを設置することにより、セキュリティレベルを改善することができる。情報ネットワークと制御ネットワーク間に設置されたファイアウォールによって、情報ネットワーク、制御ネットワーク、及び DMZ に分割する。DMZ を実装したアーキテクチャを、図 A-5 に示す。情報ネットワークがアクセスする機器（データヒストリアン等）は、全て DMZ に設置する。情報ネットワークから制御ネットワークへ直接通信する経路は不要となる。このアーキテクチャでは、情報ネットワークからの恣意的なパケットが制御ネットワークへ送信されることを拒否するが、それ以外のネットワークからのトラフィックも規制することになる。

このアーキテクチャのリスクは、攻撃者が DMZ 内の機器に不正アクセスした場合である。この場合、攻撃者は、不正アクセスに成功した機器を経由して、制御ネットワークへ攻撃することが可能になる。よって DMZ 内の機器にパッチをあてる等、強固に防御すると共に、制御ネットワークと DMZ 間は、制御ネットワーク側の機器から通信を開始した場合にのみ許可するようルールを設定する（DMZ の機器から通信を開始することができない設定にする）必要がある。

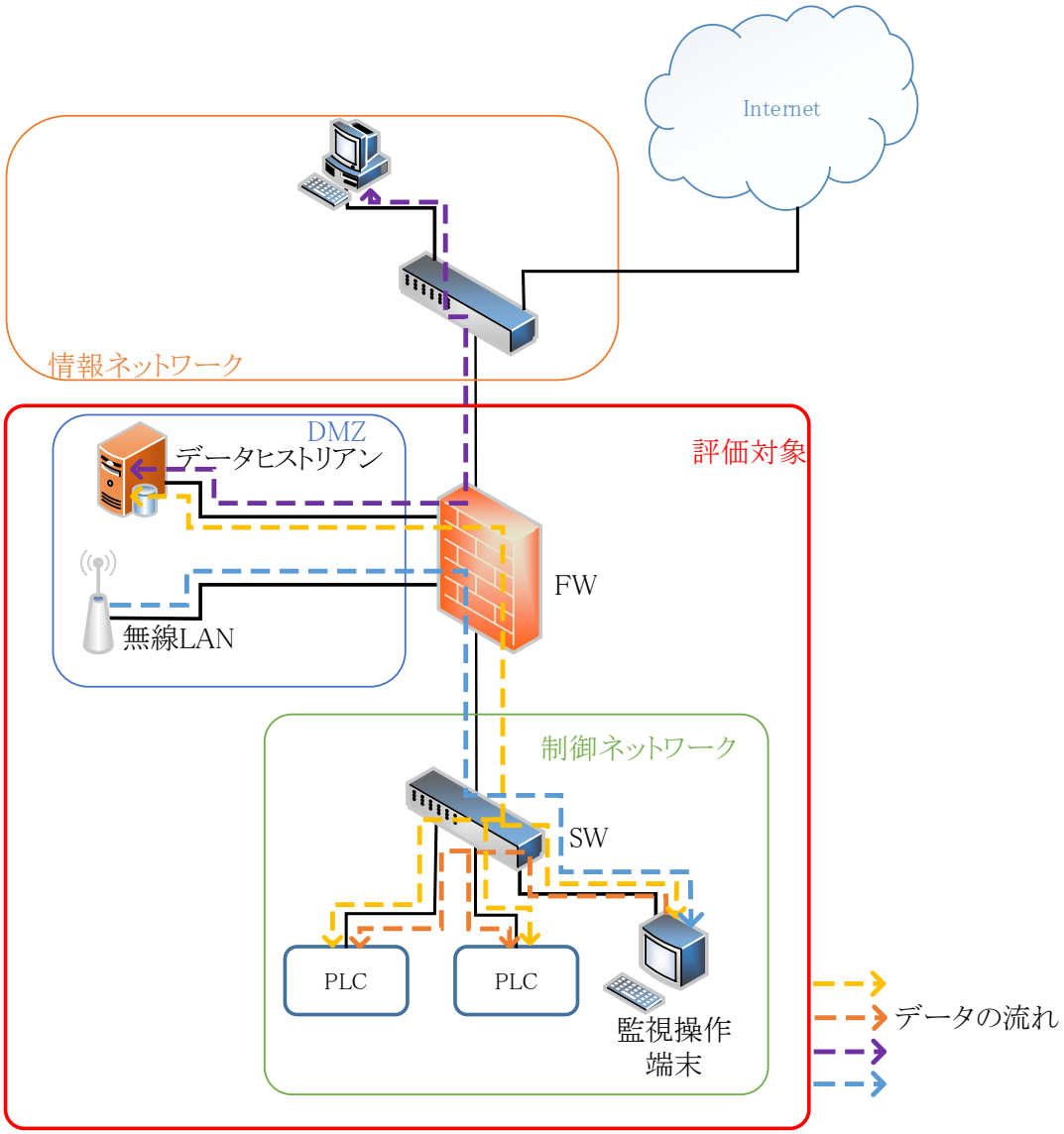


図 A-5　DMZ を有するアーキテクチャ（パターン#5）

（6）パターン#6（ペアード FW）

パターン#5 の進化形で、データヒストリアンが設置されている DMZ を 1 対（2 台）のファイアウォールで挟むアーキテクチャを、図 A-6 に示す。このアーキテクチャでは、FW#1 によって情報ネットワークからはデータヒストリアンもしくは制御ネットワークに向けての恣意的なパケットを拒否し、FW#2 によって、例えばマルウェアに感染したデータヒストリアンからの無用なトラフィックが制御ネットワークに送信されることを防ぐ、もしくは、制御ネットワークからのトラフィックがデータヒストリアンに影響を及ぼすことを防ぐことができる。

FW#1 と FW#2 を異なるベンダーの機器にすることより、セキュリティレベルをより強固にすることができる。また、FW#1 は情報システム系の資産、FW#2 を制御システム系の資産として扱うことにより責任分解を明確にすることができる。このアーキテクチャの短所は、高コストとルールセットの複雑さである。

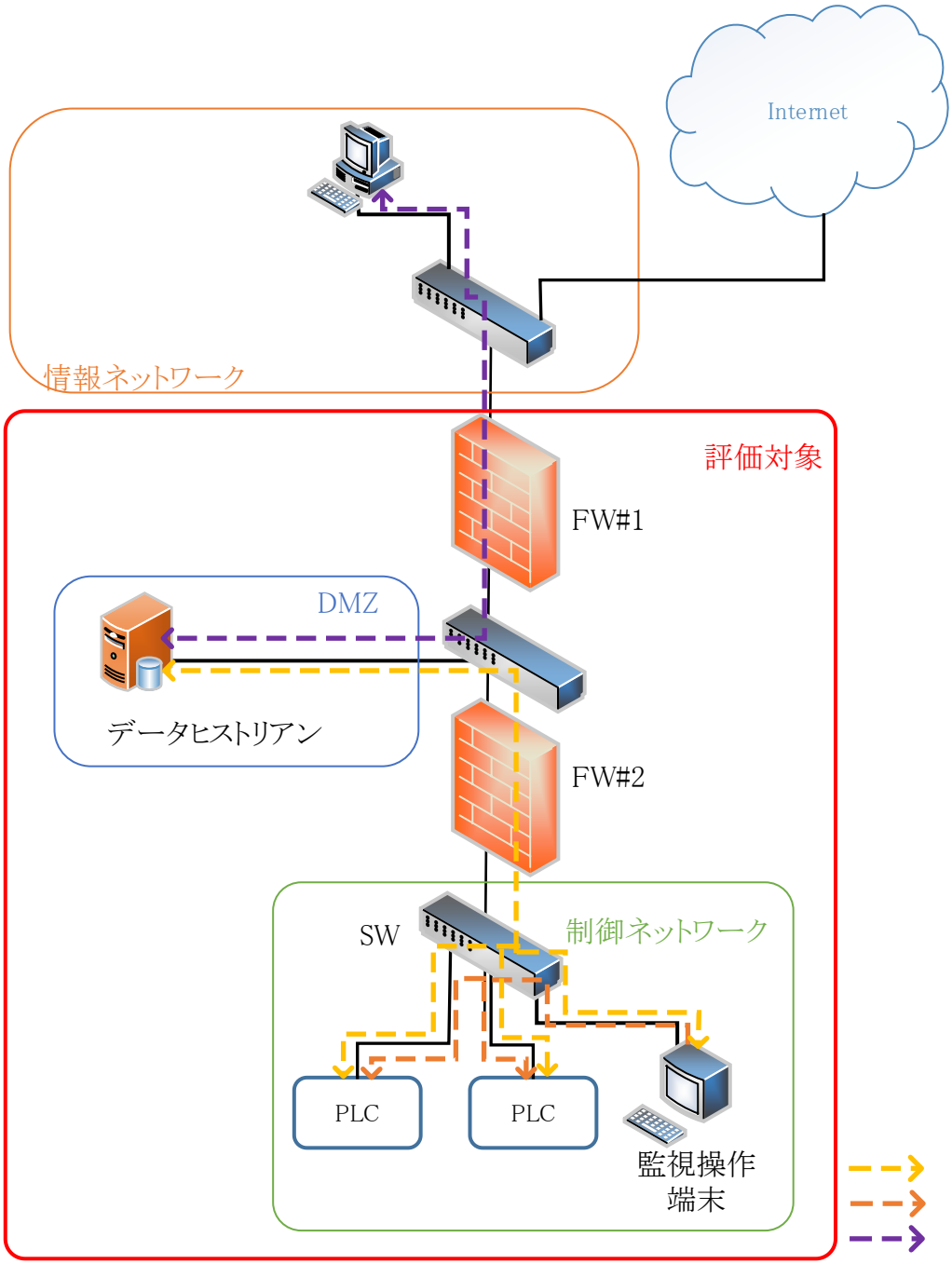


図 A-6　ペアード FW によるアーキテクチャ（パターン#6）

（7）パターン#7（VLAN）

ファイアウォールと VLAN を組み合せたアーキテクチャを、図 A-7 に示す。制御ネットワークを複数の区域に分割する場合、ファイアウォール配下に L3SW を設置し、更にその配下に VLAN を設定する SW を設置する。L3SW ではパケットフィルタリング機能を実装し、VLAN 間の通信を制御する。この VLAN は制御ネットワークによる不測のアクセス、もしくはマルウェアに感染した端末からの無用なトラフィックが、制御ネットワーク全体に伝搬することを防止する。パターン#6 同様、本アーキテクチャの短所は、高コストと設定の複雑さである。

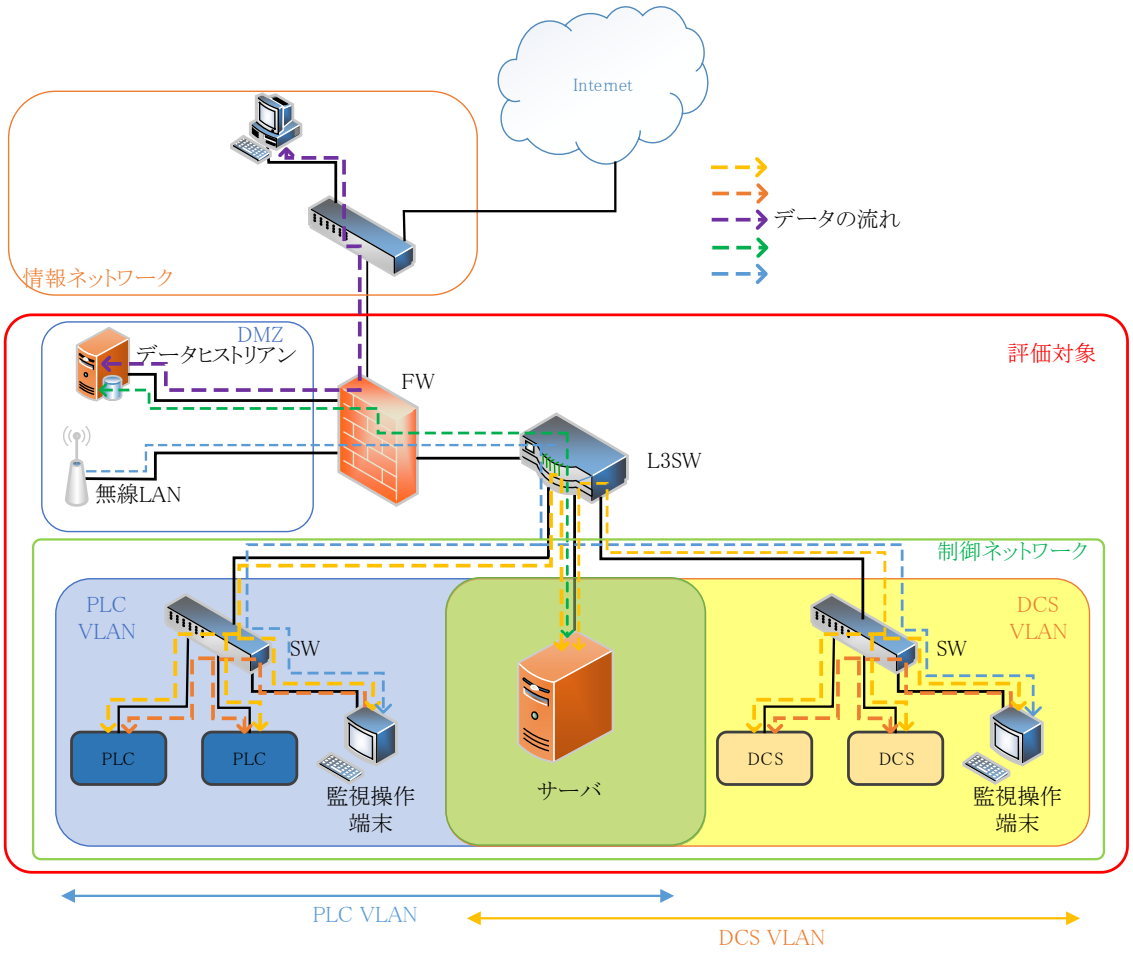


図 A-7 ファイアウォールと VLAN を組み合わせたアーキテクチャ（パターン#7）

表 A-3 アーキテクチャパターンの長所と短所

アーキテクチャパターン	長所	短所
パターン#1	● ネットワークの分割は可能	● 制御ネットワークから直接インターネットに接続可能 → セキュリティ要件に違反
パターン#2	● 低コストで実現可能	● データヒストリアンを介在した通信以外に、制御ネットワーク→情報ネットワークへの通信がある場合、その通信を完全にブロックするか、当該通信をブロックすることができなければ、制御ネットワークのセキュリティレベルを低下させる。 ● データヒストリアンが複数ある場合、管理維持が煩雑
パターン#3	● （情報ネットワークが非常に安全であれば）パケットフィルタリング機能は有効 ● ルータ／L3SW によって最低限のルールセットを構成することが可能	● ステートフルインスペクション機能がないため、フラグメンテーションパケットを用いた攻撃を防御することは困難
パターン#4	● ステートフルインスペクション機能を実装可能 ● プロキシ機能により代表的なプロトコルを制限可能 ● 外部からの攻撃に対して強固な設定が可能	● データヒストリアンの設置場所によりシステムが脆弱になる可能性がある ● なりすましパケット（制御ネットワークに対して許可されている）によって、制御ネットワーク内の機器にマルウェアが感染する可能性がある
パターン#5	● 情報ネットワークと制御ネットワーク間の通信を分離することが可能	● DMZ 内の機器に不正アクセスされると、制御ネットワークへの攻撃が可能 ● ルールセットの設定が複雑
パターン#6	● パターン#5 の短所を克服 ● FW のベンダーを分けることで、より強固なアーキテクチャを実現 ● 情報ネットワークと制御ネットワークの責任分解点の明確化	● コスト高 ● ルールセットの設定が複雑
パターン#7	● 制御ネットワークに複数の区画がある場合、VLAN による分割を行うことが可能	● コスト高 ● ルールセットの設定が複雑

自組織の制御システムにおけるファイアウォールのアーキテクチャが、7 種類のうち、どのパターンに属しているかを判断するための判定フローを、図 A-8 に示す。図中における[分類 1～4]は、本ガイドの 3.1.2 項に紹介した、制御システムのネットワークセグメント分割方式のアーキテクチャ分類における分類 1～4 との対応を示す。

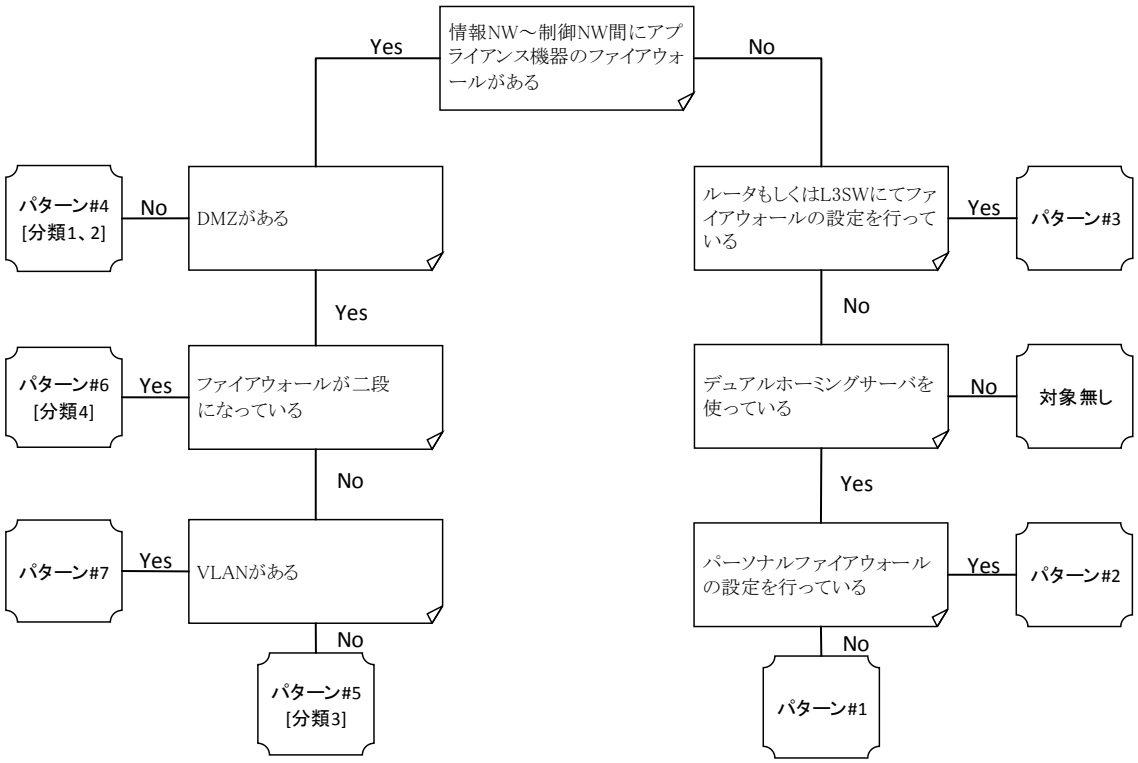


図 A-8 ファイアウォールのアーキテクチャの判定フロー

付録 B. 特定セキュリティ対策に対するチェックリスト

付録 B では、7 章で示した特定セキュリティ対策に対する追加基準の観点から、制御システムのセキュリティ対策状況を確認するためのチェックリストを添付する。

各チェックリストは、いくつかに分類された複数の評価項目からなる。各評価項目には、「必須」または「推奨」のセキュリティ要件を設定し、要件のもととなった国際標準・業界標準等の関連箇所を参照として記載した。要件の重み付けとその意味を、以下に示す。

重み付け	意味
必須	その要件を必ず満たすことが求められる項目。 国際標準規格[61]や業界標準規格[62]において、MUST/MUST NOT や SHALL/SHALL NOT、REQUIRED の表現を用いて規定される項目に相当する。 本書においては、文章の冒頭に◎を付与すると共に、「…すること。」の文体で表現する。
推奨	その要件を満たすことが推奨される項目。 国際標準規格や業界標準規格において、SHOULD/SHOULD NOT や RECOMMENDED/NOT RECOMMENDED の表現を用いて規定される項目に相当する。 本書においては、文章の冒頭に〇を付与すると共に、「…することが望ましい。」の文体で表現する[63]。

制御システムにおける対応状況（各評価項目に対する判定とその根拠）を記入することで、特定セキュリティ対策の実施状況を明確化し、第三者によって適切であるか否かを判定する際に利用することができる。

61 ISO: How to write standards
https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/how-to-write-standards.pdf
62 IETF: RFC 2119 Key words for use in RFCs to Indicate Requirement Levels
https://www.ietf.org/rfc/rfc2119.txt
63 国際標準規格や業界標準規格の日本語訳によっては、「…すべきである。」の文体で表現されている場合も存在するが、本書における「…することが望ましい。」は、意味や重み付けに関して同等である。

各チェックリストと 7 章との対応を、以下に示す。

タイトル	7 章との対応
B.1. 暗号技術利用チェックリスト	7.1
B.2. 標的型攻撃対策チェックリスト	7.2
B.3. 内部不正対策チェックリスト	7.3
B.4. ファイアウォール設定チェックリスト	7.4
B.5. 外部記憶媒体対策チェックリスト	7.5

B.1. 暗号技術利用チェックリスト

		暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注】	チェックリスト回答欄	
				判定	根拠（任意記入欄）
暗号アルゴリズムと鍵長					
	1	【暗号化アルゴリズム（共通鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された共通鍵暗号を採用することが望ましい。 〇共通鍵暗号としてブロック暗号を採用する場合、 CRYPTREC 暗号リストに掲載された暗号利用モードを採用することが望ましい。 ◎鍵長 128 ビット以上の暗号鍵を選択すること。	・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・NIST SP800-57 Part 1: 4.2.2, 5.6 ・NIST SP800-131A: 2 ・CRYPTREC 暗号リスト		
	2	【電子署名アルゴリズム（公開鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された公開鍵暗号を採用することが望ましい。 ◎有限体上の離散対数問題または素因数分解問題に基づく公開鍵暗号の場合、鍵長 2048 ビット以上（西暦 2030 年まで） または鍵長 3072 ビット以上（西暦 2031 年以降）の暗号鍵を選択すること。 ◎楕円曲線上の離散対数問題に基づく公開鍵暗号の場合、鍵長 256 ビット以上の暗号鍵を選択すること。	・NISTIR 7628: 4.1.2.2, 4.1.2.5, 4.2.1.1, 4.2.1.7 ・NIST SP800-57 Part 1: 4.2.4, 5.6 ・NIST SP800-131A: 3 ・CRYPTREC 暗号リスト		
	3	【鍵共有／鍵配送アルゴリズム（公開鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された公開鍵暗号を採用することが望ましい。 ◎有限体上の離散対数問題または素因数分解問題に基づく公開鍵暗号の場合、鍵長 2048 ビット以上（西暦 2030 年まで） または鍵長 3072 ビット以上（西暦 2031 年以降）の暗号鍵を選択すること。 ◎楕円曲線上の離散対数問題に基づく公開鍵暗号の場合、鍵長 256 ビット以上の暗号鍵を選択すること。	・NISTIR 7628: 4.1.2.2, 4.1.2.5, 4.2.1.1, 4.2.1.7 ・NIST SP800-57 Part 1: 4.2.5, 5.6 ・NIST SP800-131A: 5, 6 ・CRYPTREC 暗号リスト		
	4	【鍵ラッピングアルゴリズム（共通鍵暗号）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された共通鍵暗号を採用することが望ましい。 ◎鍵長 128 ビット以上の暗号鍵を選択すること。	・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・NIST SP800-57 Part 1: 4.2.5.4, 5.6 ・NIST SP800-131A: 7 ・CRYPTREC 暗号リスト		
	5	【鍵生成（導出）アルゴリズムを使用している場合】 ◎安全なアルゴリズムを選択すること。 〇内部で他のアルゴリズムを使用している場合、 CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたアルゴリズムを採用することが望ましい。 ◎共通鍵暗号ベースの場合、鍵長 128 ビット以上の暗号鍵を選択すること。	・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・NIST SP800-131A: 8 ・CRYPTREC 暗号リスト		
	6	【ハッシュアルゴリズムを使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたハッシュ関数を採用することが望ましい。	・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・NIST SP800-57 Part 1: 4.2.1 ・NIST SP800-131A: 9 ・CRYPTREC 暗号リスト		
	7	【メッセージ認証アルゴリズム（メッセージ認証コード）を使用している場合】 ◎安全なアルゴリズムを選択すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたメッセージ認証コードを採用することが望ましい。 ◎鍵付きハッシュベースの場合、セキュリティ強度（共通鍵換算の鍵長）128 ビット以上の暗号鍵を選択すること。 ◎共通鍵暗号ベースの場合、鍵長 128 ビット以上の暗号鍵を選択すること。	・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.7 ・NIST SP800-57 Part 1: 4.2.3, 5.6 ・NIST SP800-131A: 10 ・CRYPTREC 暗号リスト		
	8	【乱数生成アルゴリズムを使用している場合】 ◎安全なアルゴリズムを選択すること。 〇内部で他のアルゴリズムを使用している場合、 CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載されたアルゴリズムを採用することが望ましい。	・NISTIR 7628: 4.1.2.2, 4.2.1.1, 4.2.1.4, 4.2.1.7 ・NIST SP800-57 Part 1: 4.2.7 ・NIST SP800-90A ・NIST SP800-131A: 4 ・CRYPTREC 暗号リスト		

		暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注】	チェックリスト回答欄	
				判定	根拠（任意記入欄）
鍵の生成					
	9	【共通鍵暗号（共通鍵）を使用している場合】 ◎安全な方法を用いて、鍵を生成すること。 〇共通鍵は、以下のいずれかの方法で生成することが望ましい。 （1） ローカル（鍵を使用する機器内）で、以下のいずれかの方法で生成する。 ・機器配布前に疑似乱数生成アルゴリズムに初期 seed を設定し、稼働中の不確定要素を用いて seed を更新して鍵生成する。 ・機器内に事前設定済みの長期鍵から、鍵生成関数（KDF: Key Derivation Function）を用いて鍵生成する。 （2） リモート（同一の鍵を使用する他の機器や信頼できる第三者（例：鍵サーバ））において生成した鍵を受け取る。 〇共通鍵は、過去に生成した鍵と重複しないことを確認した上で生成することが望ましい。	・NISTIR 7628: 4.2.1.2, 4.2.2.3		
	10	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎安全な方法を用いて、鍵ペアを生成すること。 〇耐タンパー性を有する H/W（例：HSM、暗号専用回路を持つ IC）の内部にて鍵ペアを生成することが望ましい。	・NISTIR 7628: 4.1.2.4.2		
鍵の配布					
	11	【共通鍵暗号（共通鍵）を使用している場合】 ◎共通鍵は、完全性及び機密性を満たす条件の下で配布すること。 〇鍵の配布に用いるメカニズム（例：暗号アルゴリズム）は、少なくとも鍵と同等の強度を持っていることが望ましい。	・NISTIR 7628: 4.2.2.3, 4.3.3.3 ・NIST SP800-57 Part 1: 6.1.1		
	12	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎公開鍵は完全性を、秘密鍵は完全性及び機密性を満たす条件の下で配布すること。 〇鍵の配布に用いるメカニズム（例：暗号アルゴリズム）は、少なくとも鍵と同等の強度を持っていることが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part 1: 6.1.1		
鍵の保管					
	13	【共通鍵暗号（共通鍵）を使用している場合】 ◎共通鍵は、完全性及び機密性を満たす条件の下で保管すること。 〇永続的に利用する共通鍵は、耐タンパー性を有する H/W（例：暗号専用回路を持つ IC）の内部で保管することが望ましい。	・NISTIR 7628: 4.2.2.3, 4.3.3.3 ・NIST SP800-57 Part 1: 6.1.1		
	14	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎公開鍵は完全性を、秘密鍵は完全性及び機密性を満たす条件の下で保管すること。 〇秘密鍵は、耐タンパー性を有する H/W（例：HSM、暗号専用回路を持つ IC）の内部で保管することが望ましい。	・NISTIR 7628: 4.1.2.4.2, 4.3.3.3 ・NIST SP800-57 Part 1: 6.1.1		
鍵の用途					
	15	〇一つの鍵は、単一の用途（例：暗号化、認証、鍵ラッピング、乱数生成、電子署名）で利用することが望ましい。 ・単一の暗号鍵の暗号処理が同時に複数の機能を実現する場合（例：署名と認証、暗号化と認証）を除く。 ・鍵共有／鍵配送用途の公開鍵／秘密鍵ペアに対する公開鍵証明書発行要求のための電子署名を除く。	・NIST SP800-57 Part1: 5.2		
鍵の一意性					
	16	【共通鍵暗号（共通鍵）を使用している場合】 ◎同報通信に利用する場合を除き、暗号化通信する一対の機器ごとに一意の共通鍵を使用すること（三台以上の機器で共通鍵を共用しないこと）。	・NISTIR 7628: 4.1.3, 4.3.3.3		
	17	【公開鍵暗号（公開鍵／秘密鍵のペア）を使用している場合】 ◎機器ごとに一意の公開鍵ペアを使用すること（二台以上の機器で秘密鍵を共用しないこと）。	・NISTIR 7628: 4.1.3, 4.3.3.3		

	暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注】	チェックリスト回答欄	
			判定	根拠（任意記入欄）
鍵関連情報（パラメータ）				
18	【楕円曲線暗号アルゴリズムを使用している場合】 ◎安全なドメインパラメータを使用すること。 ◎ドメインパラメータは、完全性を満たす条件の下で配布・保管すること。	・NISTIR 7628: 4.1.2.5 ・NIST SP800-57 Part 1: 6.1.2		
19	【ブロック暗号を使用している場合】 ◎ブロック暗号は、適切な利用モード（CBC モード、CTR モード等）を選択した上で利用すること。 〇CRYPTREC 暗号リストの「電子政府推奨暗号リスト」に掲載された利用モードを採用することが望ましい。	・NIST SP800-57 Part1: 4.1.2.2, 4.2.2.3 ・CRYPTREC 暗号リスト		
20	【ブロック暗号の CBC モード、CFB モード、OFB モードを使用している場合】 ◎CBC モード、CFB モードにおける初期化ベクタ（IV）は、予測不能性を満たすこと。 ◎OFB モードにおける初期化ベクタ（IV）は、一意の（互いに異なる）値を使用すること。 ◎初期化ベクタ（IV）は、完全性を満たす条件の下で配布・保管すること。	・NIST SP800-57 Part 1: 6.1.2 ・NIST SP800-38A: 5.3, Appendix C		
21	【ブロック暗号の CTR モードを使用している場合】 ◎同一の共通鍵で使用される全てのカウンタが互いに異なること（同一の共通鍵で同じカウンタを再使用しないこと）。	・NIST SP800-38A: 6.5, Appendix B		
22	【ブロック暗号の CCM モードを使用している場合】 ◎同一の共通鍵で使用される全ての Nonce が互いに異なること（同一の共通鍵で同じ Nonce を再使用しないこと）。	・NIST SP800-38C: 5.3		
23	【ブロック暗号の GCM モード、GMAC モードを使用している場合】 ◎初期化ベクタ（IV）は、一意の（互いに異なる）値を使用すること。 ◎初期化ベクタ（IV）は、完全性を満たす条件の下で配布・保管すること。	・NIST SP800-57 Part 1: 6.1.2 ・NIST SP800-38D: 5.2.1.1, 8.2, 9, Appendix A		
24	【共有秘密情報（Shared Secrets）を使用している場合】 ◎共有秘密情報は、完全性及び機密性を満たす条件の下で配布・保管すること。 ◎使用の終了した共有秘密情報は、速やかに廃棄すること。	・NIST SP800-57 Part 1: 6.1.2		
25	【乱数生成用 seed を使用している場合】 ◎乱数生成用 seed は、十分なエントロピーを持った値を使用すること。 ◎乱数生成用 seed は、完全性及び機密性を満たす条件の下で配布・保管すること。 ◎一回使用した乱数生成用 seed は、速やかに廃棄すること。	・NISTIR 7628: 4.1.2.1, 4.2.1.2, 4.2.1.4 ・NIST SP800-57 Part 1: 6.1.2		

	暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注】	チェックリスト回答欄	
			判定	根拠（任意記入欄）
鍵の更新				
26	【データ暗号化用途の共通鍵（共通鍵暗号）を使用している場合】 ◎データ暗号化用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇データ暗号化用途の共通鍵は、高頻度に利用する場合、1 日～1 週間以内に更新することが望ましい。 〇データ暗号化用途の共通鍵は、中頻度に利用する場合、1 ヶ月以内に更新することが望ましい。 〇データ暗号化用途の共通鍵は、低頻度に利用する場合、2 年以内に更新することが望ましい。	・NISTIR 7628: 4.2.2.3, 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
27	【認証用途の共通鍵（共通鍵暗号）を使用している場合】 ◎認証用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇認証用途の共通鍵は、2 年以内に更新することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
28	【鍵ラッピング用途の共通鍵（共通鍵暗号）を使用している場合】 ◎鍵ラッピング用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇鍵ラッピング用途の共通鍵は、高頻度に利用する場合、1 日～1 週間以内に更新することが望ましい。 〇鍵ラッピング用途の共通鍵は、中頻度に利用する場合、1 ヶ月以内に更新することが望ましい。 〇鍵ラッピング用途の共通鍵は、低頻度に利用する場合、2 年以内に更新することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
29	【マスター鍵用途の共通鍵（共通鍵暗号）を使用している場合】 ◎マスター鍵用途の共通鍵は、適切な利用期間を経過した後、鍵を更新すること。 〇マスター鍵用途の共通鍵は、少なくとも 1 年ごとに更新することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
30	【乱数生成用途の共通鍵（共通鍵暗号）または公開鍵／秘密鍵ペア（公開鍵暗号）を使用している場合】 ◎乱数生成用途の共通鍵・公開鍵／秘密鍵ペアは、適切な利用期間を経過した後、鍵ペアを更新すること。 〇乱数生成アルゴリズムが鍵の更新について規定している場合は、それに従うことが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
31	【電子署名用途の公開鍵／秘密鍵ペア（公開鍵暗号）を使用している場合】 ◎電子署名用途の公開鍵／秘密鍵ペアは、適切な利用期間を経過した後、鍵ペアを更新すること。 〇電子署名用途の公開鍵／秘密鍵ペアは、1 年～3 年以内に更新することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
32	【認証用途の公開鍵／秘密鍵ペア（公開鍵暗号）を使用している場合】 ◎認証用途の公開鍵／秘密鍵ペアは、適切な利用期間を経過した後、鍵ペアを更新すること。 〇認証用途の公開鍵／秘密鍵ペアは、1 年～2 年以内に更新することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
33	【鍵共有用途の静的（永続的）な秘密鍵／公開鍵ペア（公開鍵暗号）を使用している場合】 ◎鍵共有用途の静的な秘密鍵／公開鍵は、適切な利用期間を経過した後、鍵ペアを更新すること。 〇鍵共有用途の静的な秘密鍵／公開鍵は、1 年～2 年以内に更新することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
34	【鍵共有用途の一時的な秘密鍵／公開鍵ペア（公開鍵暗号）を使用している場合】 ◎鍵共有用途の一時的な秘密鍵／公開鍵は、一回利用する度に、鍵ペアを更新すること。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
35	【鍵配送用途の秘密鍵／公開鍵ペア（公開鍵暗号）を使用している場合】 ◎鍵配送用途の秘密鍵／公開鍵は、適切な利用期間を経過した後、鍵ペアを更新すること。 〇鍵配送用途の秘密鍵／公開鍵は、2 年以内に更新することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 5.3		
36	◎鍵の漏えいが発覚した場合、速やかに鍵を更新すること。	・NIST SP800-57 Part1: 8.2.3		
37	〇同一の共通鍵を用いて暗号化を行う回数には、制限を設けることが望ましい。 〇適切な利用回数を経過した後、鍵を更新することが望ましい。	・NISTIR 7628: 4.2.2.3 ・NIST SP800-57 Part1: 8.2.3		
38	◎鍵の更新は、以下のいずれかの方法を用いて、安全に行うこと。 ・古い鍵には依存しない形で新しい鍵を生成する（Re-keying）。 ・古い鍵に依存する形で新しい鍵を生成する（Key Update）。この場合、新しい鍵から古い鍵を類推不可能なこと。	・NIST SP800-57 Part1: 8.2.3		

暗号技術の詳細項目とセキュリティ要件 （◎必須、〇推奨）			参照 【注】	チェックリスト回答欄	
				判定	根拠（任意記入欄）
鍵の廃棄					
	39	◎不要となった鍵は、安全に廃棄すること。 〇不要となった鍵（共通鍵暗号の共通鍵、公開鍵暗号の秘密鍵）は、その時点で速やかに削除することが望ましい。	・NISTIR 7628: 4.3.3.3 ・NIST SP800-57 Part1: 8.4		
	40	◎運用期間中に継続使用する鍵について、運用終了後の安全な廃棄計画を立てておくこと。 〇運用期間中に継続使用する鍵は、運用期間終了後、速やかに削除することが望ましい。	・NIST SP800-57 Part1: 8.4		
危殆化対策					
	41	暗号アルゴリズムや鍵長の危殆化（想定を上回る安全性の低下）に備えて、 ◎暗号アルゴリズムの入れ替えや鍵長の延長を考慮しておくこと。 〇予備の暗号アルゴリズムを実装しておくことが望ましい。	・NISTIR 7628: 4.2.1.3		

【注】 参照において、「CRYPTREC 推奨暗号リスト」とは、CRYPTREC が公開する「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（平成 29 年 3 月 30 日版）を指す。
http://www.cryptrec.go.jp/images/cryptrec-ls-0001-2016.pdf
今後、同リストが改定された場合、推奨される暗号アルゴリズムやモードは変更される可能性を考慮する必要がある。
例えば、設計・開発時に採用した暗号がリストから削除された場合は、別の推奨暗号へ移行することが望ましい。
このため、暗号アルゴリズムの入れ替えや鍵長の延長を考慮しておくことが必須要件である（項番 41 参照）。

このページは空白です。

B.2. 標的型攻撃対策チェックリスト

	標的型攻撃対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注】	チェックリスト回答欄	
			判定	根拠（任意記入欄）
入口対策				
1	【保護対象システムが以下のいずれかの条件を満たす場合】 ①外部ネットワークからの電子メールの受信機能を有している。 ②外部ネットワークからの電子メール受信機能を有する別のシステムと、直接的または間接的に接続されている。 〇電子メール経由で侵入・感染を試みる未知の不正プログラム（マルウェア）を、ネットワークの入口（ゲートウェイ）において、 例えば以下に示す技術等を用いて、検知・遮断できることが望ましい。 ・サンドボックス ・ファイル解析 ・通信内容解析 ・振る舞い解析 ・レピュテーション この時、項番 3 の要件を満たす対策とは異なる検知ロジックを有していることが望ましい。	・統一基準： 6.2.4 遵守事項(1)(a) ・統一基準： 6.2.2 遵守事項(1)(b)		
2	【保護対象システムが以下のいずれかの条件を満たす場合】 ①外部ネットワークの Web サーバへのアクセス機能を有している。 ②外部ネットワークの Web サーバアクセス機能を有する別のシステムと、直接的または間接的に接続されている。 〇Web サーバ経由で侵入・感染を試みる未知の不正プログラム（マルウェア）を、ネットワークの入口（ゲートウェイ）において、 例えば以下に示す技術等を用いて、検知・遮断できることが望ましい。 ・サンドボックス ・ファイル解析 ・通信内容解析 ・振る舞い解析 ・レピュテーション この時、項番 3 の要件を満たす対策とは異なる検知ロジックを有していることが望ましい。	・統一基準： 6.2.4 遵守事項(1)(a) ・統一基準： 6.2.2 遵守事項(1)(b)		
3	【保護対象システムにおけるサーバや端末が以下のいずれかの条件を満たす場合】 ①ネットワーク（外部ネットワークから隔離されているネットワークを含む）に接続されている。 ②媒体（CD/DVD、USB メモリ、外付け HDD 等）の読み込み機能を有している。 ◎（電子メール・Web サーバ・媒体等を経由して）侵入・感染を試みる未知の不正プログラム（マルウェア）を、 サーバや端末（エンドポイント）において、例えば以下に示す技術を用いて、検知・遮断できること。 ・サンドボックス ・ファイル解析 ・通信内容解析 ・振る舞い解析 ・レピュテーション	・統一基準： 6.2.4 遵守事項(1)(a) ・統一基準： 6.2.2 遵守事項(1)(a)		

標的型攻撃対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）			参照 【注】	チェックリスト回答欄	
				判定	根拠（任意記入欄）
内部対策					
	4	〇内部のネットワークを監視し、例えば以下に示す技術を用いて、不正プログラムの侵入を早期に検知できることが望ましい。 ・サンドボックス ・ファイル解析 ・通信内容解析 ・振る舞い解析 ・レピュテーション ・相関分析	・統一基準： 6.2.4 遵守事項(1)(b)		
	5	〇例えば、以下に示す技術を用いて、侵入・感染した不正プログラムの内部における不信な活動（管理者権限の奪取、不正アクセス、痕跡消去等）や侵入範囲の拡大を困難化できることが望ましい。 ・ネットワークのセグメント分割 ・認証・アクセス制御の強化 ・管理者権限の管理強化	・統一基準： 6.2.4 遵守事項(1)(b) ・統一基準： 6.1.1 遵守事項(1)(a), (1)(b) ・統一基準： 6.1.2 遵守事項(1)(a), (1)(b) ・統一基準： 6.1.3 遵守事項(1)(b)		
	6	【保護対象システムが以下のいずれかの条件を満たす場合】 ①外部ネットワークへのアクセス機能（Web 閲覧、メール送信等）を有している。 ②外部ネットワークのアクセス機能を有する別のシステムと、直接的または間接的に接続されている。 〇ネットワークの出口（ゲートウェイ）にて、例えば以下に示す技術を用いて、侵入・感染した不正プログラムの内部における不信な活動（管理者権限の奪取、不正アクセス、痕跡消去等）を検知できることが望ましい。 ・レピュテーション この時、項番 7, 8 の要件を満たす対策とは異なる検知ロジックを有していることが望ましい。	・統一基準： 6.2.4 遵守事項(1)(b)		
	7	〇内部のネットワークを監視し、例えば以下に示す技術を用いて、侵入・感染した不正プログラムの内部における不信な活動（管理者権限の奪取、不正アクセス、痕跡消去等）を検知できることが望ましい。 ・レピュテーション ・相関分析 この時、項番 6, 8 の要件を満たす対策とは異なる検知ロジックを有していることが望ましい。	・統一基準： 6.2.4 遵守事項(1)(b)		
	8	【保護対象システムにおけるサーバや端末がネットワークに接続されている場合】 〇サーバや端末（エンドポイント）において、例えば以下に示す技術を用いて、侵入・感染した不正プログラムの内部における不信な活動（管理者権限の奪取、不正アクセス、痕跡消去等）を検知できることが望ましい。 ・レピュテーション この時、項番 6, 7 の要件を満たす対策とは異なる検知ロジックを有していることが望ましい。	・統一基準： 6.2.4 遵守事項(1)(b)		
	9	◎サーバや端末において、侵入・感染した不正プログラムを検知した場合、駆除できること。	・統一基準： 6.2.2 遵守事項(1)(a)		
	10	〇システム内部の重要情報を暗号化し、漏えいしたとしても無価値化することが望ましい。 （暗号化は、データ単位またはファイル単位で行うことが望ましい。）	・統一基準： 6.1.5 遵守事項(1)(a), (1)(b), (2)		

		標的型攻撃対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注】	チェックリスト回答欄	
				判定	根拠（任意記入欄）
出口対策					
	11	【保護対象システムが以下のいずれかの条件を満たす場合】 ①外部ネットワークへのアクセス機能（Web 閲覧、メール送信等）を有している。 ②外部ネットワークのアクセス機能を有する別のシステムと、直接的または間接的に接続されている。 ◎ネットワークの出口（ゲートウェイ）にて、例えば以下に示す技術を用いて、外部との不信通信を検知・遮断できること。 ・レピュテーション ・アプリケーション制御 ・データ漏えい防止（DLP） ・外部送信データの強制暗号化	・統一基準： 6.2.4 遵守事項(1)(b)		
	12	【保護対象システムが以下のいずれかの条件を満たす場合】 ①外部ネットワークへのアクセス機能（Web 閲覧、メール送信等）を有している。 ②外部ネットワークのアクセス機能を有する別のシステムと、直接的または間接的に接続されている。 〇内部のネットワークを監視し、例えば以下に示す技術を用いて、外部との不信通信を検知できることが望ましい。 ・レピュテーション ・相関分析 この時、項番 11, 13 の要件を満たす対策とは異なる検知ロジックを有していることが望ましい。	・統一基準： 6.2.4 遵守事項(1)(b)		
	13	【保護対象システムにおけるサーバや端末がネットワークに接続されている場合】 〇サーバや端末（エンドポイント）において、例えば以下に示す技術を用いて、外部との不信通信を検知・遮断できること が望ましい。 ・レピュテーション ・アプリケーション制御 この時、項番 11, 12 の要件を満たす対策とは異なる検知ロジックを有していることが望ましい。	・統一基準： 6.2.4 遵守事項(1)(b)		
ログ分析（統合ログ管理、相関分析）、フォレンジック					
	14	〇システム内の複数の機器のログを一元管理し、相関分析技術を用いて、標的型攻撃活動を検知・可視化できること が望ましい。	・統一基準： 6.1.4 遵守事項(1)(b), (1)(c)		
	15	◎標的型攻撃によるインシデント発生時の被害を解明するために、通信ログを収集・保存すること。 〇標的型攻撃によるインシデント発生時の被害を解明するために、通信パケットを収集・保存しておくことが望ましい。	・統一基準： 6.1.4 遵守事項(1)(a)		

【注】 参照において、「統一基準」とは、「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」を指す。
https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf

このページは空白です。

B.3. 内部不正対策チェックリスト

		内部不正対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注1】【注2】	回答想定者／部門	チェックリスト回答欄	
					判定	根拠（任意記入欄）
基本方針						
	1	◎内部不正の対策は経営者の責任であり、経営者は組織内外に示す「基本方針」を策定し、役職員に周知徹底していること。	・IPA ガイドライン: 4-1 (1)-① ・（CERT BP: Practice 2）	・経営者（最高責任者）		
	2	◎「基本方針」に基づき対策を実施するためのリソースが確保されるよう、経営者は必要な決定、指示をしていること。	・IPA ガイドライン: 4-1 (1)-② ・（CERT BP: Practice 16）	・経営者（最高責任者）		
	3	◎経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を行っていること。	・IPA ガイドライン: 4-1 (2)-① ・（CERT BP: Practice 16）	・経営者（最高責任者）		
	4	◎総括責任者は、基本方針に則り組織横断的な管理体制を構築し、実施策を策定していること。	・IPA ガイドライン: 4-1 (2)-② ・（CERT BP: Practice 16）	・総括責任者		
	5	〇文書化して一貫性のある方針、統制を実行し、例えば以下の様な対策を実施することが望ましい。【注3】 ・役職員に対して、雇用時及び定期的に、組織の方針を理解して遵守することを誓約するための署名を要求する。	・CERT BP: Practice 2	・直接部門 ・（総務部門） ・（人事部門） ・（法務・知財部門）		
	6	〇経営者により承認された内部不正対策として、例えば以下の様な対策を実施することが望ましい。【注3】 ・法務・知財部門は、情報収集に関して、全ての証拠が法的基準に従って収集・維持されていることを確認する。 ・法務・知財部門は、役職員の健康情報の様なプライバシーがインサイダー脅威チームの間で保護されていることを確認する。	・CERT BP: Practice 16	・法務・知財部門 ・（総務部門） ・（人事部門）		
秘密指定						
	7	◎重要情報を把握し、重要度に合わせて格付け区分し、取り扱い可能な役職員の範囲を定めていること。	・IPA ガイドライン: 4-2-1 (3) ・CERT BP: Practice 6	・直接部門		
	8	◎重要情報の作成者は、定めた格付け区分を選択し、その選択について上司等に確認を得ていること。	・IPA ガイドライン: 4-2-1 (4)-① ・CERT BP: Practice 6	・直接部門		
	9	◎重要情報を含む電子文書には、役職員が分かる様に機密マーク等の表示をしていること。	・IPA ガイドライン: 4-2-1 (4)-② ・CERT BP: Practice 6	・直接部門		
	10	〇不正なデータ持ち出し防止のため、例えば以下の様な対策を実施することが望ましい。【注3】 ・重要資産（人、情報、技術、機能）、アクセスを許可されるべき人、実際にアクセスする人、資産の場所を特定する。 ・重要資産が如何にコピー可能であるか、削除可能であるかを理解する。 ・物理的に、あるいはワイヤレスで情報システムに接続可能な全ての機器を考慮する。	・CERT BP: Practice 19	・直接部門 ・（情報システム部門）		
アクセス権指定						
	11	◎情報システムを管理・運営する担当者は、利用者 ID 及びアクセス権の登録・変更・削除等の設定手順を定めて運用していること。	・IPA ガイドライン: 4-2-2 (5)-① ・CERT BP: Practice 6	・情報システム部門		
	12	◎情報システムを管理・運営する担当者は、異動または退職により不要となった利用者 ID 及びアクセス権を、直ちに削除していること。	・IPA ガイドライン: 4-2-2 (5)-②	・情報システム部門		
	13	◎複数のシステム管理者がいる場合は、情報システムの管理者 ID ごとに適切な権限範囲の割り当てを行い、相互に監視できるように設定していること。あるいは、システム管理者が一人の場合は、ログ等により監視していること。	・IPA ガイドライン: 4-2-2 (6) ・（CERT BP: Practice 10）	・直接部門 ・（情報システム部門）		
	14	◎情報システムでは、共有 ID や共有のパスワード・IC カード等を使用せず、個々の利用者 ID を個別のパスワード・IC カード等で認証していること。	・IPA ガイドライン: 4-2-2 (7) ・CERT BP: Practice 7	・情報システム部門 ・（直接部門）		

内部不正対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）			参照 【注1】【注2】	回答想定者／部門	チェックリスト回答欄	
					判定	根拠（任意記入欄）
物理的管理						
	15	◎重要情報の格納場所や取り扱う領域等を物理的に保護するために壁や入退管理策によって保護していること。	・IPA ガイドライン: 4-3 (8)	・直接部門 ・（情報システム部門） ・（総務部門）		
	16	◎PC 等の情報機器や USB メモリ等の携帯可能な記録媒体は、盗難や不正持ち出し等がない様に管理・保護していること。	・IPA ガイドライン: 4-3 (9)-①	・直接部門 ・（情報システム部門）		
	17	◎情報機器や記録媒体を処分する際には重要情報が完全消去されていることを確認していること。	・IPA ガイドライン: 4-3 (9)-②	・直接部門 ・（情報システム部門）		
	18	◎モバイル機器や携帯可能な記録媒体を外部に持ち出す場合には、持ち出しの承認及び記録等の管理をしていること。	・IPA ガイドライン: 4-3 (10) ・（CERT BP: Practice 13）	・直接部門 ・（情報システム部門）		
	19	◎個人のモバイル機器及び記録媒体の業務利用及び持込を制限していること。	・IPA ガイドライン: 4-3 (11) ・（CERT BP: Practice 13）	・情報システム部門 ・（直接部門）		

	内部不正対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注1】【注2】	回答想定者／部門	チェックリスト回答欄	
				判定	根拠（任意記入欄）
技術・運用管理					
20	◎組織のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトや SNS、外部のオンラインストレージ等の使用を制限していること。	・IPA ガイドライン: 4-4 (12) ・CERT BP: Practice 18	・情報システム部門		
21	〇特権ユーザに対する厳格なアクセス制御と監視方針を実行し、例えば以下の様な対策を実施することが望ましい。【注3】 ・特権ユーザの職務終了時、（特権ユーザとしての）アクセスが完全に遮断されたことを確認する。	・CERT BP: Practice 10	・直接部門 ・（情報システム部門）		
22	〇システム変更管理として、例えば以下の様な対策を実施することが望ましい。【注3】 ・ハードウェア及びソフトウェア構成のベースラインを識別・文書化すると共に、変更に応じて更新する。 ・変更ログ、バックアップ、ソースコード、他のアプリケーションファイル等を保護する変更管理プロセス。 ・変更管理プロセスを通して、役割を異なる役職員に割り当てる。	・CERT BP: Practice 11	・直接部門 ・（情報システム部門）		
23	〇ログ相関エンジンやセキュリティイベント・情報管理システム（SIEM）を導入し、役職員の行動を記録・監視・監査することが望ましい。【注3】	・CERT BP: Practice 12	・直接部門 ・（法務・知財部門） ・（人事部門） ・（情報システム部門）		
24	〇モバイル機器を含む全てのエンドポイントからの遠隔アクセスの監視・制御のため、例えば以下の様な対策を実施することが望ましい。【注3】 ・全ての遠隔トランザクションに関して、密接にログの記録及び監査を行う。 ・役職員の退職時、アカウントの削除やアクセス権限の剥奪等により、確実にアクセスを無効化する。	・CERT BP: Practice 13	・情報システム部門 ・（直接部門）		
25	〇セキュアなバックアップとリカバリ手続きの実装として、例えば以下の様な対策を実施することが望ましい。【注3】 ・全ての SLA（サービス品質保証）の遵守を保証するために、セキュアな、テストされたバックアップとリカバリ手順を持つ。 ・一人の IT 管理者がバックアップとリカバリ手順を不正に変更できない様に、任務を分離すること。 ・IT 管理者が悪意のある活動の記録を隠ぺい・削除できない様に、業務ログを保護すること。	・CERT BP: Practice 15	・直接部門 ・（情報システム部門） ・（総務部門）		
26	〇通常のネットワーク機器の振る舞い（ベースライン）の確立として、例えば以下の様な対策を実施することが望ましい。【注3】 ・ネットワーク上の通常の振る舞いと異常な振る舞いを区別するため、ベースラインとしての振る舞いを捉える。 ・非技術的な職場の行動も収集する。 ・企業全体・部門・グループ及び個人の各々のレベルでのネットワークの通常の振る舞いを、可能な限り広範囲で、長期間に渡って収集する。	・CERT BP: Practice 17	・情報システム部門 ・（総務部門） ・（人事部門）		
27	〇不正なデータ持ち出し防止のため、例えば以下の様な対策を実施することが望ましい。【注3】 ・重要資産（人、情報、技術、機能）、アクセスを許可されるべき人、実際にアクセスする人、資産の場所を特定する。 ・重要資産が如何にコピー可能であるか、削除可能であるかを理解する。 ・物理的に、あるいはワイヤレスで情報システムに接続可能な全ての機器を考慮する。	・CERT BP: Practice 19	・直接部門 ・（情報システム部門）		
28	◎委託先等の関係者への重要情報の受渡しは、受渡しから廃棄までを含めて管理していること。	・IPA ガイドライン: 4-4 (13)-①	・直接部門 ・（情報システム部門）		
29	◎インターネット等の組織外を介す重要情報の受渡しでは、誤って関係者以外に渡ってしまうことも考慮し、暗号化等で保護していること。	・IPA ガイドライン: 4-4 (13)-② ・（CERT BP: Practice 9）	・直接部門 ・（情報システム部門）		
30	◎組織外部で利用・取り扱い可能な重要情報を限定し、重要情報や情報機器を保護していること。	・IPA ガイドライン: 4-4 (14) ・（CERT BP: Practice 9）	・直接部門 ・（情報システム部門）		
31	◎組織外で重要情報を用いた業務を行う際に、周囲の環境やネットワーク環境等を考慮して保護していること。	・IPA ガイドライン: 4-4 (15) ・（CERT BP: Practice 9）	・直接部門 ・（情報システム部門）		
32	◎委託する業務内容に応じたセキュリティ対策を契約前に確認・合意し、契約期間中にも契約通りにセキュリティ対策が実施されていることを確認していること。	・IPA ガイドライン: 4-4 (16)	・直接部門 ・（情報システム部門）		

		内部不正対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注1】【注2】	回答想定者／部門	チェックリスト回答欄	
					判定	根拠（任意記入欄）
証拠確保						
	33	〇重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護していることが望ましい。	・IPA ガイドライン: 4-5 (17) ・（CERT BP: Practice 12）	・情報システム部門 ・（直接部門）		
	34	◎システム管理者のアクセス履歴や操作履歴等のログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していること。	・IPA ガイドライン: 4-5 (18) ・（CERT BP: Practice 12）	・情報システム部門		
人的管理						
	35	◎全ての役職員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底していること。	・IPA ガイドライン: 4-6 (19)-① ・CERT BP: Practice 3	・直接部門 ・（総務部門） ・（人事部門）		
	36	◎教育を定期的に繰り返して実施し、教育内容を定期的に見直して更新していること。	・IPA ガイドライン: 4-6 (19)-② ・CERT BP: Practice 3	・直接部門 ・（総務部門） ・（人事部門）		
	37	〇役職員への教育（項番 35 及び 36）では、例えば以下の様な内容の教育を実施することが望ましい。【注3】 ・組織に対するリスク、従業員を犯罪に勧誘する標的となり得る可能性を認識すること、重要資産の保護方法 ・インサイダー脅威の振る舞い（例えば、①組織内データの不正コピー、②パスワードや組織情報の窃取を試みるソーシャルエンジニアリングの試みや施設への不正アクセス、③組織や役職員への脅威） ・不審な振る舞いを発見した場合の報告手順	・CERT BP: Practice 3	・直接部門 ・（総務部門） ・（人事部門）		
	38	〇役職員や派遣職員を雇用段階から監視し、例えば以下の様な対策を実施することが望ましい。【注3】 ・内定者、請負業者、取引先企業からの派遣職員に対して、個人、専門性、財政上のストレスを確認するために、身元調査を行うと共に、定期的に再調査を行う。	・CERT BP: Practice 4	・直接部門 ・（総務部門） ・（人事部門）		
	39	〇雇用の終了時に秘密保持義務を課す誓約書の提出を求めていることが望ましい。	・IPA ガイドライン: 4-6 (20) ・（CERT BP: Practice 14）	・直接部門 ・（総務部門） ・（人事部門） ・（法務・知財部門）		
	40	◎役職員の雇用終了時及び請負等の契約先との契約終了時に、取り扱いを委託した情報資産の全てを返却または完全消去し、情報システムの利用者 ID や権限を削除していること。	・IPA ガイドライン: 4-6 (21) ・CERT BP: Practice 14	・直接部門 ・（総務部門） ・（人事部門） ・（法務・知財部門）		
	41	〇ソーシャルメディアに対する特別な警戒として、例えば以下の様な対策を実施することが望ましい。【注3】 ・方針や手続き（項番 20 記載の使用制限等）に加えて、ソーシャルメディアに関する従業員の教育を実施する。	・CERT BP: Practice 18	・情報システム部門 ・（総務部門） ・（人事部門）		
	42	〇取引先企業からの脅威も考慮し、例えば以下の様な対策を実施することが望ましい。【注3】 ・取引先企業の身元調査を行い、彼等に対して「秘密保持契約（NDA）」への署名を要求する。	・CERT BP: Practice 1	・直接部門 ・（総務部門） ・（法務・知財部門）		
コンプライアンス						
	43	◎就業規則等の内部規程を整備し、正式な懲戒手続を備えていること。	・IPA ガイドライン: 4-7 (22) ・CERT BP: Practice 4	・直接部門 ・（総務部門） ・（人事部門） ・（法務・知財部門）		
	44	◎役職員に対して重要情報を保護する義務があることを理解させるために「秘密保持誓約書」等の提出を要請していること。	・IPA ガイドライン: 4-7 (23) ・CERT BP: Practice 1	・直接部門 ・（総務部門） ・（人事部門） ・（法務・知財部門）		

内部不正対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）			参照 【注1】【注2】	回答想定者／部門	チェックリスト回答欄	
					判定	根拠（任意記入欄）
職場環境						
	45	〇公平で客観的な人事評価を整備すると共に、業績に対する評価を説明する機会を設ける等、人事評価や業績評価の整備を推進していることが望ましい。	・IPA ガイドライン: 4-8 (24) ・CERT BP: Practice 5	・人事部門 ・（総務部門）		
	46	〇業務量及び労働時間の適正化等の健全な労働環境を整備すると共に、業務支援を推進する体制や相談しやすい環境を整える等職場内において良好なコミュニケーションを組織全体で推進していることが望ましい。	・IPA ガイドライン: 4-8 (25) ・CERT BP: Practice 5	・総務部門 ・（人事部門）		
	47	〇相互監視ができない環境における単独作業を制限し、単独作業には事前承認、事後確認等の手続きを定めていることが望ましい。	・IPA ガイドライン: 4-8 (26) ・CERT BP: Practice 8	・直接部門 ・（総務部門） ・（人事部門）		
事後対策						
	48	◎内部不正の影響範囲を特定するために、事象の具体的状況を把握すると共に、被害の最小化策や影響の拡大防止策を実施し、必要に応じて組織内外の関係者との連携体制を確保していること。	・IPA ガイドライン: 4-9 (27)	・直接部門 ・（情報システム部門）		
	49	◎内部不正者に対する処罰を検討し、内部不正の事例を内部に告知することを検討していること。	・IPA ガイドライン: 4-9 (28)	・直接部門 ・（情報システム部門）		
組織の管理						
	50	◎内部不正と思わしき事象が発生した場合についての通報制度を整備し、通報受付を複数設置し、必要に応じて通報者の匿名性を確保していること。	・IPA ガイドライン: 4-10 (29)	・直接部門 ・（情報システム部門）		
	51	◎内部不正対策の項目を抽出し、定期的及び不定期に確認（内部監査等の監査を含む）し、確認した結果は、経営者に報告し、必要に応じて対策の見直しを実施していること。	・IPA ガイドライン: 4-10 (30)	・直接部門 ・（情報システム部門）		

【注1】参照において、「IPA ガイドライン」とは、IPA が発行する「組織における内部不正防止ガイドライン（日本語版）第 4 版」（平成 29 年 1 月 31 日公開）を指す。
https://www.ipa.go.jp/security/fy24/reports/insider/index.html

【注2】参照において、「CERT BP」とは、CERT が発行する「Best Practices Against Insider Threats in All Nations」（2013 年 8 月公開）を指す。
https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59082

【注3】「CERT BP」に Best Practice として記載されているが、「IPA ガイドライン」に対応項目が存在しない対策の一部を抽出して追記。

このページは空白です。

B.4. ファイアウォール設定チェックリスト

B.4.1. 制御システムの境界防御チェックシート

	制御システムの境界防御の詳細項目とセキュリティ要件 （◎必須、〇推奨）	構成パターン 2	3	4	5	6	7	参照	チェックリスト回答欄 判定	根拠（任意記入欄）
制御システムのネットワークの分離と分割（他のシステムからの分離）										
1	〇通信トラフィックはデフォルトでは拒否し、例外を許可（「全て拒否、例外として許可」等）することが望ましい。 「全て拒否、例外として許可」の通信トラフィックポリシーは、承認済みの接続だけが許可されることを保証する。 （これはホワイトリストポリシーとして知られている。） Denying communications traffic by default and allowing communications traffic by exception (i.e., deny all, permit by exception). A deny-all, permit-by-exception communications traffic policy ensures that only those connections which are approved are allowed. This is known as a white-listing policy.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		
2	〇プロキシサーバを実装し、制御システム領域の情報システムリソース（ファイル、接続、サービス等）に対する、外部からの要求を仲介させることが望ましい。 Implementing proxy servers that act as an intermediary for external domains' requesting information system resources (e.g., files, connections, or services) from the ICS domain.			〇	〇	〇	〇	・NIST SP800-82: 5.2		
3	〇認可されていない情報の持ち出しを防止することが望ましい。 例えば、アプリケーションファイアウォール（Deep Packet Inspection: DPI）や XML ゲートウェイ等を用いる。これらのデバイスは、プロトコルのフォーマットや仕様に準拠しているかをアプリケーション層で検証し、ネットワーク層やトランスポート層で動作するデバイスでは検出できない脆弱性を見つける役目を果たす。 Preventing the unauthorized exfiltration of information. Techniques include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		
4	〇組織、システム、アプリケーション及び個人のうち 1 つ（1 人）または複数による、認可され、認証された送信元と宛先アドレスのペア間の通信のみを許可することが望ましい。 Only allowing communication between authorized and authenticated source and destinations address pairs by one or more of the organization, system, application, and individual.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		
5	〇入退管理を実施し、制御システムの構成要素へのアクセスを制限することが望ましい。 Enforcing physical access control to limit authorized access to ICS components.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		
6	〇制御システムの構成要素のネットワークアドレスが分からない様に隠蔽し（公開しない、DNS に登録しない等）、知らないとアクセスできない様にすることが望ましい。 Concealing network addresses of ICS components from discovery (e.g., network address not published or entered in domain name systems), requiring prior knowledge for access.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		
7	〇管理用やトラブルシューティング用の、特に（訳注：攻撃者による）ネットワークの検索に有益な、ブロードキャストメッセージを使うサービス及びプロトコルを無効化することが望ましい。 Disabling control and troubleshooting services and protocols, especially those employing broadcast messaging, which can facilitate network exploration.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		
8	〇セキュリティドメインには、それぞれ別のネットワークアドレスを設定することが望ましい（例えば、全て不連続なサブネットアドレスにする等）。 Configuring security domains with separate network addresses (i.e., as disjoint subnets).	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		
9	〇プロトコルの検証に失敗した場合に、送信側にフィードバックを送らない様にし（詳細表示モード等）、攻撃者が情報を得られない様にすることが望ましい。 Disabling feedback (e.g., non-verbose mode) to senders when there is a failure in protocol validation format to prevent adversaries from obtaining information.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.2		

	制御システムの境界防御の詳細項目とセキュリティ要件 （◎必須、○推奨）	構成パターン						参照	チェックリスト回答欄	
		2	3	4	5	6	7		判定	根拠（任意記入欄）
制御システムのネットワークの分離と分割（他のシステムからの分離）										
10	○制御ネットワーク及び DMZ にパッシブモニタリングを設置して異常通信を能動的に検出し、アラートを発報する様にすることが望ましい。 【訳注】SP800-82 における ICS network は、記載箇所によって微妙に意味が異なっていると考えられるが、5.2 の記述では、モデルシステムにおける制御ネットワーク及び DMZ に相当すると解釈した。 Establishing passive monitoring of ICS networks to actively detect anomalous communications and provide alerts.	○	○	○	○	○	○	・NIST SP800-82: 5.2		
11	○特に、異なるセキュリティドメイン間では、単方向のデータフローを実装することが望ましい。 Implementing one-way data flow, especially between different security domains.				○	○	○	・NIST SP800-82: 5.2		
12	○制御ネットワーク及び DMZ にアクセスしようとする全てのユーザに対して、セキュアな認証を実施することが望ましい。 認証には、単純なパスワード、複雑なパスワード、多要素認証、トークン、生体認証、スマートカード等、様々な強度の方法がある。 使用可能な方法を使用するのではなく、保護すべき制御ネットワーク及び DMZ の脆弱性を鑑み、見合った方法を選択する。 【訳注】SP800-82 における ICS network は、記載箇所によって微妙に意味が異なっていると考えられるが、5.3 の記述では、モデルシステムにおける制御ネットワーク及び DMZ に相当すると解釈した。 Enforce secure authentication of all users seeking to gain access to the ICS network. There is flexibility to employ varying protection levels of authentication methods including simple passwords, complex passwords, multi-factor authentication technologies, tokens, biometrics and smart cards. Select the particular method based upon the vulnerability of the ICS network to be protected, rather than using the method that is available at the device level.	○	○	○	○	○	○	・NIST SP800-82: 5.3		
13	○情報システムでは適切ではないかもしれないが、制御システムに適した運用ポリシーを許可することが望ましい。 例えば、電子メール等のセキュリティの低い通信の禁止、覚えやすいユーザ名やグループパスワードの使用等。 Permit the ICS to implement operational policies appropriate to the ICS but that might not be appropriate in an IT network, such as prohibition of less secure communications like email, and permitted use of easy-to-remember usernames and group passwords.	○	○	○	○	○	○	・NIST SP800-82: 5.3		
14	○トラフィックの監視、解析及び侵入検知のため、情報のフロー（流れ）を記録することが望ましい。 Record information flow for traffic monitoring, analysis, and intrusion detection.	○	○	○	○	○	○	・NIST SP800-82: 5.3		
15	○制御ネットワークと情報ネットワークの間のアクセスポイントは最低限（なるべく 1 箇所のみ）とし、文書に明記されていることが望ましい。 ○冗長（バックアップ等）のアクセスポイントがある場合には、必ず文書化することが望ましい。 【訳注】SP800-82 における ICS network は、記載箇所によって微妙に意味が異なっていると考えられるが、5.4 の記述では、モデルシステムにおける制御ネットワークに相当すると解釈した。 There should be documented and minimal (single if possible) access points between the ICS network and the corporate network. Redundant (i.e., backup) access points, if present, must be documented.	○	○	○	○	○	○	・NIST SP800-82: 5.4		
16	○制御ネットワークと情報ネットワーク間のステートフルファイアウォールは、明確に認可されたもの以外、一切のトラフィックを拒否する様に設定することが望ましい。 【訳注】No.15 の訳注参照 A stateful firewall between the ICS network and corporate network should be configured to deny all traffic except that which is explicitly authorized.	○	○	○	○	○	○	・NIST SP800-82: 5.4		
17	○ファイアウォールルールでは、トランスミッションコントロールプロトコル（TCP）及びユーザデータグラムプロトコル（UDP）ポートのフィルタリング、インターネット制御メッセージプロトコル（ICMP）タイプ及びコードのフィルタリングに加えて、最低でも送信元及び宛先のフィルタリング（メディアアクセス制御[MAC]アドレスでのフィルタリング等）を行うことが望ましい。 The firewall rules should at a minimum provide source and destination filtering (i.e., filter on media access control [MAC] address), in addition to TCP and User Datagram Protocol (UDP) port filtering and Internet Control Message Protocol (ICMP) type and code filtering.	○	○	○	○	○	○	・NIST SP800-82: 5.4		

	制御システムの境界防御の詳細項目とセキュリティ要件 （◎必須、○推奨）	構成パターン						参照	チェックリスト回答欄	
		2	3	4	5	6	7		判定	根拠（任意記入欄）
DMZ										
18	○異なる 2 つのベンダーのファイアウォールを使用することが望ましい（リスク低減視点で利点となる）。 If firewalls from two different manufacturers are used, then this solution may offer an advantage.					○		・NIST SP800-82: 5.5.5		
サーバ（データヒストリアン）										
19	○2 ゾーンシステム（DMZ なし）を避けて 3 ゾーンシステム（訳注：DMZ あり）を採用し、データを収集する装置は制御ネットワーク内に、データを蓄積するヒストリアンコンポーネントは DMZ 内に配置することが望ましい。 The best solution is to avoid two-zone systems (no DMZ) and use a three-zone design, placing the data collector in the control network and the historian component in the DMZ.	○	○	○	○	○	○	・NIST SP800-82: 5.10.1		
リモートアクセス										
20	○リモートネットワークから制御ネットワークにアクセスする全てのユーザは、トークンベース認証等の強力な認証メカニズムを使用して、認証を要求されることが望ましい。 Any users accessing the control network from remote networks should be required to authenticate using an appropriately strong mechanism such as token-based authentication.	○	○	○	○	○	○	・NIST SP800-82: 5.10.2		
21	○インターネットまたはダイアルアップモデム経由で接続してくるリモート保守員は、企業のネットワークに接続するために、企業の VPN 接続クライアント、アプリケーションサーバ、セキュア HTTP アクセス等の暗号化プロトコルを使用し、トークンベース多要素認証等の強力な認証メカニズムを使用することが望ましい。 Remote support personnel connecting over the Internet or via dialup modems should use an encrypted protocol, such as running a corporate VPN connection client, application server, or secure HTTP access, and authenticate using a strong mechanism, such as a token based multi-factor authentication scheme, in order to connect to the general corporate network.	○	○	○	○	○	○	・NIST SP800-82: 5.10.2		
22	○リモートアクセスで接続後、制御ネットワークファイアウォールにおいて、トークンベース多要素認証等の強力なメカニズムを使用して再度認証を要求してから、制御ネットワークへのアクセスを許可することが望ましい。 Once connected, they should be required to authenticate a second time at the control network firewall using a strong mechanism, such as a token based multi-factor authentication scheme, to gain access to the control network.	○	○	○	○	○	○	・NIST SP800-82: 5.10.2		

B.4.2. 境界ファイアウォールチェックリスト

	ファイアウォール設定の詳細項目とセキュリティ要件 （◎必須、〇推奨）	構成パターン						参照	チェックリスト回答欄	
		2	3	4	5	6	7		判定	根拠（任意記入欄）
ファイアウォールのルールセット										
23	〇ルールセットの基本は全て拒否し、何も許可しない（を出発点）とすることが望ましい。 The base rule set should be deny all, permit none.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.7		
24	〇全て「許可」ルールは、IP アドレス及び TCP/UDP ポートを特定し、適切であればステートフルとすることが望ましい。 All “permit” rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.7		
25	〇全てのルールは、トラフィックを特定の IP アドレスまたはアドレス範囲に限定することが望ましい。 【訳注】以下は、「Firewall Checklist」(SANS Institute, SCORE (Security Consensus Operational Readiness Evaluation) Checklist Project) より引用。 ・以下のアドレス（アドレス範囲）は使用不可。 255.255.255.255, 127.0.0.0, 10.0.0.0～10.255.255.255(*), 172.16.0.0～172.31.255.255(*), 192.168.0.0～192.168.255.255(*), 240.0.0.0 等 (*) インターネットに接続している場合、当該 IP は使用不可。インターネット未接続時は、使用可。 All rules should restrict traffic to a specific IP address or range of addresses.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.7		
26	〇インバウンド・トラフィックのルールのアドレスは、情報ネットワーク上の特定のアドレスセットから、制御ネットワーク上のごく小数の共有デバイス（データヒストリアン等）へのトラフィックに限定することが望ましい。 The address portion of the rules should restrict incoming traffic to a very small set of shared devices (e.g., the data historian) on the control network from a controlled set of addresses on the corporate network.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.7		
27	〇制御ネットワーク内のサーバへのアクセスを、情報ネットワーク上のいかなる IP アドレスに対しても許可することは推奨しない。 また、許可ポートは用心のため、HTTPS 等の比較的セキュアなプロトコルに限定することが望ましい。 Allowing any IP addresses on the corporate network to access servers inside the control network is not recommended. In addition, the allowed ports should be carefully restricted to relatively secure protocols such as Hypertext Transfer Protocol Secure (HTTPS).	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.7		
28	〇HTTP、FTP その他のセキュアでないプロトコルがファイアウォールを通るのは、トラフィックのスニッフィングや改ざんの恐れがあるため、セキュリティリスクとなる。制御ネットワーク外のホストが制御ネットワーク上のホストへの接続を開始できない様にルールを追加すること。制御ネットワーク内のデバイスだけに制御ネットワークの外に接続することを許すルールにすることが望ましい。 Allowing HTTP, FTP, or other unsecured protocols to cross the firewall is a security risk due to the potential for traffic sniffing and modification. Rules should be added to deny hosts outside the control network from initiating connections with hosts on the control network. Rules should only allow devices internal to the control network the ability to establish connections outside the control network.	〇	〇	〇	〇	〇	〇	・NIST SP800-82: 5.7		
29	〇DMZ アーキテクチャを使用している場合は、トラフィックが情報ネットワークと制御ネットワーク間で直接やり取りされない様にシステムを設定することが望ましい。 幾つかの特殊な例外はあるが、いずれの側からのトラフィックも DMZ 内のサーバで終端させることが可能である。 If the DMZ architecture is being used, then it is possible to configure the system so that no traffic will go directly between the corporate network and the control network. With a few special exceptions (noted below), all traffic from either side can terminate at the servers in the DMZ.				〇	〇	〇	・NIST SP800-82: 5.7		

		ファイアウォール設定の詳細項目とセキュリティ要件 （◎必須、○推奨）	構成パターン						参照	チェックリスト回答欄	
			2	3	4	5	6	7		判定	根拠（任意記入欄）
ファイアウォールのルールセット											
	30	○制御ネットワークのファイアウォールを通るアウトバウンドのトラフィックは、必須、かつ、認可された DMZ 上サーバからのトラフィックのみに限定することが望ましい。 Outbound traffic through the control network firewall should be limited to essential communications only and should be limited to authorized traffic originating from DMZ servers.				○	○	○	・NIST SP800-82: 5.7		
	31	○トラフィックは、制御ネットワークから情報ネットワークへ直接送信されない様にすることが望ましい。即ち、（制御ネットワークから送信される）全てのトラフィックは、DMZ で終端することが望ましい。 Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in the DMZ.				○	○	○	・NIST SP800-82: 5.7		
	32	○制御ネットワークと DMZ 間で許可されたプロトコルと同じプロトコルは、DMZ と情報ネットワーク間（その逆方向も）では、明示的に禁止することが望ましい。 Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).				○	○	○	・NIST SP800-82: 5.7		
	33	○制御ネットワークから情報ネットワークへの全てのアウトバンドのトラフィックは、サービスとポートにより送信元及び宛先制限を設けることが望ましい。 All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
	34	○制御ネットワークまたは DMZ からのアウトバウンドのパケットは、送信元アドレスが制御ネットワークまたは DMZ 内のデバイスに割り当てられた正しい IP アドレスである場合にのみ許可することが望ましい。 Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices.				○	○	○	・NIST SP800-82: 5.7		
	35	○制御ネットワーク内のデバイスからのインターネットアクセスは、許可しないことが望ましい。 Control network devices should not be allowed to access the Internet.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
	36	○制御ネットワークは、ファイアウォールで保護されていても、直接インターネットに接続しないことが望ましい。 Control networks should not be directly connected to the Internet, even if protected via a firewall.	○	○	○	○	○	○	・NIST SP800-82: 5.7		

		ファイアウォール設定の詳細項目とセキュリティ要件 （◎必須、○推奨）	構成パターン						参照	チェックリスト回答欄	
			2	3	4	5	6	7		判定	根拠（任意記入欄）
管理者権限											
	37	○全てのファイアウォール管理トラフィックは、分離されたセキュアな管理用ネットワーク、または、多要素認証を備えた暗号化ネットワークを使うことが望ましい。 All firewall management traffic should be carried on either a separate, secured management network (e.g., out of band) or over an encrypted network with multi-factor authentication. Traffic should also be restricted by IP address to specific management stations.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
	38	○トラフィック（ファイアウォールの管理用トラフィック）は、IP アドレスにより、特定の管理端末に限定することが望ましい。 Traffic should also be restricted by IP address to specific management stations.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
管理											
	39	○制御ネットワーク環境と情報ネットワーク間のポート及びサービスは、ケースバイケースでの判断に基づいて、ポートとサービスを利用許可し、有効化することが望ましい。 Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
	40	○許可されたアウトバウンドまたはインバウンドのデータフローについては、それぞれリスク分析に基づく経営上の根拠及び許可した責任者を付し、文書化することが望ましい。 There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
	41	○全てのファイアウォールポリシーは、定期的に検証することが望ましい。 All firewall policies should be tested periodically.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
	42	○全てのファイアウォールは、稼働させる直前にバックアップすることが望ましい。 All firewalls should be backed up immediately prior to commissioning.	○	○	○	○	○	○	・NIST SP800-82: 5.7		
ファイアウォールのプロトコル設定（telnet）											
	43	○遠隔管理には、（訳注：telnet の代わりに）セキュアシェル（SSH）プロトコルを使用することが望ましい。 It is recommended to use the Secure Shell (SSH) protocol [5.8.6] for remote administration.	○	○	○	○	○	○	・NIST SP800-82: 5.8.4, 5.8.6		
	44	○情報ネットワークから制御ネットワークへのインバウンドの telnet セッションは、トークンベースの多要素認証及び暗号化トンネルを使用してセキュリティが確保されていないならば、禁止することが望ましい。 Inbound telnet sessions from the corporate to the control network should be prohibited unless secured with token-based multi-factor authentication and an encrypted tunnel.	○	○	○	○	○	○	・NIST SP800-82: 5.8.4		
	45	○（訳注：制御ネットワークから情報ネットワークへの）アウトバウンドの telnet セッションは、認可された特定のデバイスに対して、暗号化トンネル（VPN 等）でのみ許可することが望ましい。 Outbound telnet sessions should be allowed only over encrypted tunnels (e.g., VPN) to specific authorized devices.	○	○	○	○	○	○	・NIST SP800-82: 5.8.4		
ファイアウォールのプロトコル設定（DNS）											
	46	○ほとんどのケースにおいて、制御ネットワークから情報ネットワークに対する DNS リクエストを許可するに足る理由はまずなく、制御ネットワークに対する DNS リクエストを許可する理由はない。制御ネットワークから DMZ に対する DNS リクエストは、ケースバイケースで検討すること。ローカル DNS やホストファイル（host file）を使用することが望ましい。 In most cases there is little reason to allow DNS requests out of the control network to the corporate network and no reason to allow DNS requests into the control network. DNS requests from the control network to DMZ should be addressed on a case-by-case basis. Local DNS or the use of host files is recommended.	○	○	○	○	○	○	・NIST SP800-82: 5.8.1		

		ファイアウォール設定の詳細項目とセキュリティ要件 （◎必須、○推奨）	構成パターン						参照	チェックリスト回答欄	
			2	3	4	5	6	7		判定	根拠（任意記入欄）
ファイアウォールのプロトコル設定（HTTP/HTTPS）											
	47	○HTTP は、インターネット/情報ネットワークから制御ネットワークへ通さないことが望ましい。 HTTP should not be allowed to cross from the public/corporate to the control network.	○	○	○	○	○	○	・NIST SP800-82: 5.8.2		
	48	○インターネット／情報ネットワークから制御ネットワークに対して HTTP を使用する場合（ウェブベース技術の使用が必須な場合）、以下を適用することが望ましい。 ・ホワイトリストを使用して、ウェブベースサービスへアクセスをデータリンク層またはネットワーク層で制御する ・送信元及び宛先の双方でアクセス制御を行う ・データリンク層、ネットワーク層ではなく、サービスへのアクセス認可の仕組みをアプリケーション層で実装する ・必須の技術のみを使用してサービスを実装する（スクリプトは必要な場合のみ使用する等） ・知られているアプリケーションセキュリティ実践例（プラクティス）に従ってサービスをチェックする ・Web サービスを利用しようとする全ての試みを記録する ・HTTP の代わりに HTTPS を使用し、認可された特定デバイスのみとする If web-based technologies are absolutely required, the following best practices should be applied: – Control access to web-based services on the physical or network layer using white-listing; – Apply access control to both source and destination; – Implement authorization to access the service on the application layer (instead of physical or network-layer checks); – Implement service using only the necessary technologies (e.g., scripts are used only if they are required); – Check service according to known application security practices; – Log all attempts of service usage ; and – Use HTTPS rather than HTTP, and only for specific authorized devices.	○	○	○	○	○	○	・NIST SP800-82: 5.8.2		
ファイアウォールのプロトコル設定（SNMP）											
	49	○制御ネットワークから、及び、制御ネットワークへの SNMPV1 と V2（V2C を含む）のコマンドは、分離されたセキュアな管理ネットワークを通じて行う場合以外は、禁止することが望ましい。 【訳注】 SNMPV1 と V2（V2C を含む）では、平文のパスワードを使用している。 SNMP V1 & V2 commands both to and from the control network should be prohibited unless they are over a separate, secured management network, …	○	○	○	○	○	○	・NIST SP800-82: 5.8.9		
ファイアウォールのプロトコル設定（DCOM／分散型コンポーネント・オブジェクト・モデル）											
	50	○DCOM プロトコルは、制御ネットワークと DMZ 間でのみ許可し、DMZ と情報ネットワーク間では明示的にブロックすることが望ましい This protocol should only be allowed between control network and DMZ networks and explicitly blocked between the DMZ and corporate network.				○	○	○	・NIST SP800-82: 5.8.10		
	51	○ユーザは、DCOM 使用デバイス（訳注：PC、サーバ等）のレジストリを変更し、使用するポートの範囲を限定することが望ましい。 Users are advised to restrict the port ranges used by making registry modifications on devices using DCOM.	○	○	○	○	○	○	・NIST SP800-82: 5.8.10		
ファイアウォールのプロトコル設定（SCADA と産業用プロトコル・MODBUS/TCP, EtherNet/IP, DNP3 等）											
	52	○Modbus/TCP、EtherNet/IP、IEC 61850、ICCP、DNP328 の様な SCADA 及び産業用プロトコルは、ほとんどの制御機器にとって必須のプロトコルである。これらのプロトコルの使用は、制御ネットワーク内でのみ許可し、制御ネットワークから情報ネットワークへは許可しないことが望ましい。 SCADA and industrial protocols, such as Modbus/TCP, EtherNet/IP, IEC 61850, ICCP and DNP328, are critical for communications to most control devices. These protocols should only be allowed within the control network and not allowed to cross into the corporate network.	○	○	○	○	○	○	・NIST SP800-82: 5.8.11		

		ファイアウォール設定の詳細項目とセキュリティ要件 （◎必須、○推奨）	構成パターン						参照	チェックリスト回答欄	
			2	3	4	5	6	7		判定	根拠（任意記入欄）
ファイアウォールのプロトコル設定（ファイル転送・FTP/TFTP）											
	53	○FTP 通信については、アウトバウンドのセッションのみ、またはトークンベースの多要素認証かつ暗号化トンネルでセキュリティを確保した場合のみ、許可することが望ましい。 FTP communications should be allowed for outbound sessions only or if secured with additional token-based multi-factor authentication and an encrypted tunnel.	○	○	○	○	○	○	・NIST SP800-82: 5.8.3		
	54	○TFTP 通信は、全てブロックすることが望ましい。 【訳注】TFTP は、ユーザ認証機能がない。 All TFTP communications should be blocked.	○	○	○	○	○	○	・NIST SP800-82: 5.8.3		
	55	○可能であれば常に、セキュア FTP（SFTP）やセキュアコピー（SCP）といった、よりセキュリティの高いプロトコルを採用することが望ましい。 More secure protocols, such as Secure FTP (SFTP) or Secure Copy (SCP), should be employed whenever possible.	○	○	○	○	○	○	・NIST SP800-82: 5.8.3		
ファイアウォールのプロトコル設定（メール・SMTP）											
	56	○電子メールメッセージにはマルウェアが含まれていることが多いため、インバウンドの電子メールは、いかなる制御ネットワークデバイスに対しても通さないことが望ましい。 制御ネットワークから情報ネットワークへの送信 SMTP メールメッセージは、アラートメッセージの送信時には許される。 Email messages often contain malware, so inbound email should not be allowed to any control network device. Outbound SMTP mail messages from the control network to the corporate network are acceptable to send alert messages.	○	○	○	○	○	○	・NIST SP800-82: 5.8.8		
ファイアウォールのプロトコル設定（SOAP）											
	57	○SOAP ベースサービスに関連したトラフィックフローは、情報ネットワークのセグメントと ICS ネットワークのセグメントの間のファイアウォールで制御することが望ましい。 Traffic flows related to SOAP-based services should be controlled at the firewall between corporate and ICS network segments.	○	○	○	○	○	○	・NIST SP800-82: 5.8.7		
ファイアウォールのプロトコル設定（メッセージ交換用 XML ベース形式のシンタックス）											
	58	○SOAP ベースサービスが必要な場合、ディープパケットインスペクションまたはアプリケーション層ファイアウォールのいずれか又は両方を使用して、メッセージ内容を制限することが望ましい。 If these services are necessary, deep-packet inspection and/or application layer firewalls should be used to restrict the contents of messages.	○	○	○	○	○	○	・NIST SP800-82: 5.8.7		

B.5. 外部記憶媒体対策チェックリスト

外部記憶媒体対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）			参照 【注1】【注2】	チェックリスト回答欄	
				判定	根拠（任意記入欄）
規程/手順（人）での対策					
	1	【「申請～利用」の局面】 ◎媒体利用おける利用可能な媒体の定義、申請、承認、報告の一連の手順が以下の事項を含めてルール化されていること。 ・申請においては、要管理区域への媒体の持込み／持出しの手順を含むこと。 ・媒体を専用化する場合は、その貸出しの手順を含むこと。 貸出し手順には、媒体の初期化や返却時のデータ消去の手順を含むこと。 ・媒体利用時の媒体ごとの管理責任者を明確にすること。	・統一基準： 遵守事項 3.1.1(4)(e) ・統一基準： 遵守事項 8.1.1(1)(c)		
	2	【「調達～廃棄」の局面】 ◎利用する媒体の調達、廃棄の一連の手順がルール化されていること。 なお、調達においては、技術的な要件も含むこと。	・統一基準： 遵守事項 3.1.1(4)(e) ・統一基準： 遵守事項 8.1.1(1)(c)		
	3	【「監査」の局面】 ◎媒体の利用おける記録の採取と手順の監査の実施に関して、ルール化されていること。 なお、利用の記録としては、システム的なログ、貸出し台帳、申請書類等を含むこと。	・統一基準： 遵守事項 3.1.1(4)(e) ・統一基準： 遵守事項 8.1.1(1)(c)		

外部記憶媒体対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）			参照 【注1】【注2】	チェックリスト回答欄	
				判定	根拠（任意記入欄）
媒体における対策					
	4	【「調達」の局面】 〇媒体の調達に際しては、要件を明確にした上で、安全な調達先、製品を選択することが望ましい。	・統一基準： 遵守事項 5.2.1(2)(d) ・ガイドライン： 基本対策事項 5.2.1(2)-6 a) ・経済産業省 「IT 製品の調達におけるセキュリティ要件リスト」 ・統一基準： 遵守事項 8.1.1(1)(c) ・ガイドライン： 基本対策事項 8.1.1(1)-4 b)		
	5	【「利用（媒体の入手）」の局面】 〇利用する媒体は、組織で管理している安全な媒体を利用するのが望ましい。 なお、媒体の調達に関しては 項番 4 を参照。	・統一基準： 遵守事項 8.1.1(1)(c) ・ガイドライン： 基本対策事項 8.1.1(1)-4 a)		
	6	【「利用（媒体の輸送と保管）」の局面】 〇媒体からの読み出し、媒体への書き込みに際しては、データ保護の観点より媒体自身の認証機能が利用できることが望ましく、同認証機能を用いることにより、保存されたデータの漏洩、消失、改ざんを防止できることが望ましい。	・統一基準： 遵守事項 3.1.1(4)(a), (d) ・ガイドライン： 基本対策事項 3.1.1(4)-1 c) ・統一基準： 遵守事項 3.1.1(6)(a), (b) ・ガイドライン： 基本対策事項 3.1.1(6)-2 c) ・統一基準： 遵守事項 8.1.1(1)(c) ・ガイドライン： 基本対策事項 8.1.1(1)-4 b)		
	7	【「利用（媒体の輸送と保管）」の局面】 〇媒体からの読み出し、媒体への書き込みに際しては、データ保護の観点より媒体自身の暗号化機能が利用できることが望ましく、同暗号化機能を用いることにより、保存されたデータの漏洩、改ざんを防止できることが望ましい。	・統一基準： 遵守事項 3.1.1(4)(a), (d) ・ガイドライン： 基本対策事項 3.1.1(4)-1 c) ・統一基準： 遵守事項 3.1.1(6)(a), (b) ・ガイドライン： 基本対策事項 3.1.1(6)-2 c) ・統一基準： 遵守事項 8.1.1(1)(c) ・ガイドライン： 基本対策事項 8.1.1(1)-4 b)		
	8	【「利用（媒体の各種機器への接続）」の局面】 〇媒体と各種機器との接続に際しては、媒体自身の不正プログラムチェック機能が利用できることが望ましく、同不正プログラムチェック機能を用いることにより、媒体への不正プログラムの感染を防止できることが望ましい。	・統一基準： 遵守事項 3.1.1(6)(a), (b) ・ガイドライン： 基本対策事項 3.1.1(6)-2 c)		
	9	【「利用（不要データの削除）」の局面】 〇不要となったデータは、媒体から速やかに削除することが望ましく、データの利用が終了した時点で速やかに削除し、その漏洩を防止することが望ましい。 〇削除に際しては、復元不可能な方式での削除が望ましい。	・統一基準： 遵守事項 3.1.1(7)(a), (b) ・統一基準： 遵守事項 8.1.1(1)(c) ・ガイドライン： 基本対策事項 8.1.1(1)-4 c)		
	10	【「廃棄」の局面】 ◎不要となった媒体は、物理的に破壊するか媒体中のデータを復元不可能な方式で消去を行うこと。 ◎不要となった媒体の利用が終了した時点で上記手段により速やかに廃棄し、情報漏洩を防止すること。	・統一基準： 遵守事項 3.1.1(7)(a), (b)		

	外部記憶媒体対策の詳細項目とセキュリティ要件 （◎必須、〇推奨）	参照 【注1】【注2】	チェックリスト回答欄	
			判定	根拠（任意記入欄）
端末における対策				
11	【「調達」の局面】 〇端末の調達に際しては、端末への媒体の挿入を監視する機能の実装を要件として盛込むことが望ましい。	・統一基準： 遵守事項 5.2.1(2)(a) ・ガイドライン： 基本対策事項 5.2.1(2)-4 b)		
12	【「利用（媒体の端末への接続）」の局面】 媒体利用が不要な端末の場合、 ◎接続の可能性のあるポートを物理的に塞ぐ、もしくは、ソフト的に利用不可とすること。 なお、ソフト的に利用不可とする場合は、OS の機能や同機能を有するソフトウェアの導入／適用等にて実施すること。	・統一基準： 遵守事項 6.2.4(1)(a) ・ガイドライン： 基本対策事項 6.2.4(1)-2 e), f)		
13	【「利用（媒体の端末への接続）」の局面】 媒体利用が必要な端末の場合、 〇接続の必要なポート以外を物理的に塞ぐ、もしくは、ソフト的に利用制限することが望ましい。 なお、ソフト的に利用制限する場合は、OS の機能や同機能を有するソフトウェアの導入／適用等にて実施することが望ましい。	・統一基準： 遵守事項 6.2.4(1)(a) ・ガイドライン： 基本対策事項 6.2.4(1)-2 e), f)		
14	【「利用（媒体の端末への接続）」の局面】 〇媒体の識別番号等により、接続可能な媒体以外の利用制限ができることが望ましく、 事前に登録された識別番号等により、接続を制限できるソフトウェアの導入／適用等にて実施することが望ましい。	・統一基準： 遵守事項 6.2.4(1)(a) ・ガイドライン： 基本対策事項 6.2.4(1)-2 a), f)		
15	【「利用（媒体の端末への接続）」の局面】 〇媒体の接続時に、媒体中のプログラムや実行ファイルの自動実行を防止できることが望ましく、 端末側にて、接続用ポートや媒体での自動実行の機能を停止することが望ましい。	・統一基準： 遵守事項 6.2.4(1)(a) ・ガイドライン： 基本対策事項 6.2.4(1)-2 c)		
16	【「利用（媒体の端末への接続）」の局面】 〇媒体の接続時に、媒体中のプログラムや実行ファイルの直接実行を防止できることが望ましい。 なお、媒体に格納されたプログラムや実行ファイルの実行が必要な場合は、端末側にコピーした上で実行する運用とする ことが望ましい。	・統一基準： 遵守事項 6.2.4(1)(a) ・ガイドライン： 基本対策事項 6.2.4(1)-2 d)		
17	【「利用（媒体の端末への接続）」の局面】 〇媒体の接続、データの入出力、媒体の切離し等の一連の動きをログとして記録できることが望ましい。 なお、記録するログには、操作の内容だけでなく、入出力したデータのファイル名等も記録として保管することが望ましく、 記録されたログは、管理者のみ閲覧可能で、改ざんができない様な形式で保管することが望ましい。	・統一基準： 遵守事項 6.2.4(1)(a) ・ガイドライン： 基本対策事項 6.2.4(1)-2 f)		
18	【「利用（媒体の端末への接続）」の局面】 ◎媒体の接続時に、不正プログラムの検知、駆除できること。媒体を接続する端末に不正プログラムを検知、駆除する機能を 実装/導入できない場合は、別の端末にて、事前に媒体上の不正プログラムの検知、駆除できる様にすること。	・統一基準： 遵守事項 6.2.4(1)(a) ・ガイドライン： 基本対策事項 6.2.4(1)-2 b) ・統一基準： 遵守事項 8.1.1(1)(c) ・ガイドライン： 基本対策事項 8.1.1(1)-4 d) ・統一基準： 遵守事項 8.1.1(7)(a) ・ガイドライン： 基本対策事項 8.1.1(7)-1 a), b), c), d)		
19	【「利用（媒体の輸送と保管）」の局面】 〇媒体への書き込みに際しては、データ保護の観点より暗号化機能が利用できることが望ましく、 同暗号化機能を用いることにより、保存されたデータの漏洩、改ざんを防止できることが望ましい。	・統一基準： 遵守事項 3.1.1(4)(a),(d) ・ガイドライン： 基本対策事項 3.1.1(4)-1 c) ・統一基準： 遵守事項 3.1.1(6)(a),(b) ・ガイドライン： 基本対策事項 3.1.1(6)-2 a),b)		

【注1】参照において、「統一基準」とは、「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」を指す。
https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf

【注2】参照において、「ガイドライン」とは、「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」を指す。
https://www.nisc.go.jp/active/general/pdf/guide28.pdf

このページは空白です。

付録 C. 制御システムのインシデント事例

制御システムのインシデント事例を表形式で整理した。

2008 年以降のインシデント事例を対象に、種々の分野の事例を掲載するよう考慮したが、適切なインシデント事例が見つけられなかった分野に関しては、講演の内容等を掲載した。

表における各項目の意味は、以下の通り。

項目名	意味
事例名	インシデントの名称
業界／分野	インシデントが発生した分野（重要インフラの 13 分野等）
発生国	インシデントが発生した国
発生年月	インシデントが発生した年月
影響・被害	対象、発生事象、規模（金額・時間・人数・事業所数等）
内容（原因等）	原因（攻撃の種類等） ● 攻撃／侵入経路、攻撃方法、 ● 影響を与えた因子 制御妨害、プログラム変更、偽情報、不正操作等
参考情報（出典等）	出典、関連解説/レポート等（URL 等）

このページは空白です。

制御システムのインシデント事例一覧（1/5）

#	事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）	参考情報（出典等）
1	ポーランドの鉄道におけるトラックポイントの不正操作	鉄道	ポーランド	2008 年 1 月	路面電車システムがハッキングされ、4 両の車両が脱線し、12 人の負傷者を出した。	14 歳の少年が、テレビのリモコンを改造したコントローラを用いて、路面電車システムに対してハッキングを行い、ポイント切替機を不正に操作した。	http://www.theregister.co.uk/2008/01/11/tram_hack/ http://www.intellilink.co.jp/article/column/sec-controlsys01.html
2	スマートメーターを対象としたサイバー攻撃	電力	米自治領プエルトリコ	2009 年	攻撃を受けた会社のスマートメーターを配置した地域内で、電力消費記録設定が改ざんされた。	攻撃者はインターネット上で見つかったツールを利用し、メータ管理を横取りし、プログラムを変更することでデータを改ざんした。	http://www.meti.go.jp/meti_lib/report/2014fy/E003791.pdf（p.73） https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/
3	ウラン濃縮施設の遠心分離機における Stuxnet 感染	電力	イラン	2010 年 11 月	ウラン濃縮施設の遠心分離機がマルウェアに感染し、約 8,400 台の遠心分離機が停止した。	USB メモリを介して、マルウェア（ワーム）Stuxnet に感染。Stuxnet は、周波数変換装置を制御する PLC に侵入し、周波数を変え回転速度を通常よりも上げたり下げたりすることで、最終的に遠心分離機を破壊した。	https://eset-info.canon-its.jp/malware_info/trend/detail/160308.html https://wired.jp/2012/06/04/confirmed-us-israel-created-stuxnet-lost-control-of-it/ http://www.meti.go.jp/meti_lib/report/2014fy/E003791.pdf（p.75）
4	ロンドンオリンピックの電力系統への DoS 攻撃	電力	英国	2012 年 7 月	オリンピック開会式（2012 年 7 月 27 日）の際に、照明システム（電力系統）への DoS 攻撃を受けたが、実際の被害には及ばなかった。	照明システム（電力系統）への DoS 攻撃が 40 分間続き、北米や欧州の 90 の IP アドレスから 1,000 万のアクセスがあった。	http://www.icr.co.jp/newsletter/global_perspective/2013/Gpre2013115.html
5	世界的大手の石油企業におけるワークステーションへの攻撃	石油	サウジアラビア	2012 年 8 月	世界的大手の石油企業の約 30,000 台のワークステーションがマルウェアに感染し、コンピュータ上のファイルが消去され、1 週間以上にわたって社内ネットワークを停止させられた。幸いにも、石油生産はネットワークが独立したシステムになっていたため影響を受けなかった。	ハッカーグループによる Shamoon と呼ばれるマルウェアを用いた攻撃によるものであった。	https://wired.jp/2012/08/28/worlds-largest-oil-producer-falls-victim-to-30k-workstation-attack/ http://www.risidata.com/Database/Detail/computer_virus_targets_saudi_arabian_oil_company http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2012.pdf
6	尖閣諸島問題等と関連したとみられるサイバー攻撃	政府・行政機関等	日本	2012 年 9 月	総務省統計局、政府インターネットテレビ等、少なくとも 11 のウェブサイトが一定の間、閲覧困難となった。また、裁判所や東北大学病院等、少なくとも 8 のウェブサイトが、中国の国旗等の画像や尖閣諸島は中国のものである旨の文章等が表示するよう改ざんされた。	中国のハッカー集団「紅客連盟」の掲示板等において、攻撃対象として日本の行政機関や重要インフラ事業者等が掲示されたほか、中国の大手チャットサイト「YY チャット」等では、最大 4 千人が参加し、攻撃予告や攻撃ツール等に関する書き込みがなされた。	http://www.npa.go.jp/keibi/biki3/20120919kouhou.pdf http://www.shield.ne.jp/ssrc/topics/SSRC-ER-12-046-ja.html

制御システムのインシデント事例一覧（2/5）

#	事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）	参考情報（出典等）
7	韓国の 3.20 サイバーテロ	銀行・報道機関	韓国	2013 年 3 月	少なくとも 2 つの放送局と 3 つの金融機関で、パソコンを再起動するよう促したり、画面におかしな文字を表示したりしてから、一切の動作を停止する事態が続出した。その結果、銀行では ATM や決済が一時的に停止し、放送局では手作業で放送を継続するという大変な事態に陥った。	マスターブートレコード（MBR）のワイパー攻撃により、銀行、報道機関のコンピュータ約 32,000 台が停止した。	http://www.nikkei.com/article/DGXNASFK0101X_R00C13A4000000/ http://www.nids.mod.go.jp/event/symposium/pdf/2016/j_02.pdf（p.28）
8	国際宇宙ステーションにおけるマルウェア感染	宇宙	ロシア	2013 年 5 月	マルウェアに感染した時期や感染による影響については明らかにされていない。	国際宇宙ステーション（ISS）がロシア人宇宙飛行士によって持ち込まれた USB メモリからマルウェアに感染した。	http://gigazine.net/news/20131112-iss-infected-malware-by-russian-usb/
9	監査報告：オーストラリア ヴィクトリア州における水道局の監査	水道	オーストラリア	2013 年 12 月	監査報告のため、影響・被害なし。	ヴィクトリア州の州監査官による水道局の監査において、システムに多くの脆弱性があることが判明した。ほとんどの水道局で、重要なシステムへの特権アクセスのログが取られていたものの、ログのレビューが全く行われていなかった。アカウントが適切に管理されていない局が 6、パッチ管理が行われていない局が 2 あり、全体では 19 の水道局で 22 の脆弱性が発見された。	http://www.itnews.com.au/News/367442,vic-water-authorities-vulnerable-to-cyber-attack.aspx
10	エネルギー業界を標的とした産業制御システムへの攻撃	電力	米国 スペイン フランス イタリア ドイツ トルコ ポーランド	2014 年 6 月	攻撃を仕掛けているのは Dragonfly と呼ばれる集団で、スパイ活動や継続的なアクセスを目的として多数の組織に侵入している。攻撃側がその気になれば、電力供給網に対する妨害工作を仕掛けられる恐れもあった。	Dragonfly は、産業制御システム（ICS）メーカーのソフトウェアに、リモートアクセス機能を持ったトロイの木馬を感染させ、ソフトウェアアップデート経由で ICS を運用しているコンピュータにマルウェアをダウンロードさせる手口を使っていた。	http://www.itmedia.co.jp/news/articles/1407/01/news034.html https://www.symantec.com/connect/tr/blogs/dragonfly-0?page=1 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
11	ソウルの地下鉄の PC 管理サーバへの攻撃	鉄道	韓国	2014 年 7 月	北朝鮮偵察総局と推定されるサイバーテロ組織が、ソウルの地下鉄 1～4 号線を運営するソウルメトロの PC 管理サーバを少なくとも半年以上掌握していた。	PC 管理プログラムの運営サーバの権限を奪われ、地下鉄の運営をリアルタイムで監視する総合管制所等の核心部署の PC58 台が悪性コードに感染していた。	http://japanese.donga.com/List/3/all/27/429558/1
12	韓国の原発運営会社へのサイバー攻撃	電力	韓国	2014 年 12 月	北朝鮮がサイバー攻撃を実行し、韓国水力原子力発電会社からデータを盗んだ。 2 基の原子炉の設計図とマニュアル類、1 万を超える従業員の個人情報、フローチャート、近隣住民の予測される被ばく線量等が流出した。"	攻撃者は、同社の多数の従業員へ、マルウェアを仕込んだ文書を添付した電子メールを送付した。 今回のハッキングに使用された悪意あるコードは、北朝鮮のハッカーたちが使用する、いわゆる kimsuky（マルウェア）と、構造や機能が同様だった。	http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Korean+Nuclear+Plant+Faces+Data+Leak+and+Destruction http://wired.jp/2015/03/20/south-korea-claims-north-hacked-nuclear-data/ http://www.hackread.com/south-korean-nuclear-operator-hacked/ http://www.theregister.co.uk/2014/12/22/nuclear_hack_threats_prompts_skorea_cyber_war_exercise/

制御システムのインシデント事例一覧（3/5）

#	事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）	参考情報（出典等）
13	ドイツの製鉄所へのサイバー攻撃	製造（鉄鋼）	ドイツ	2014 年 12 月	ドイツの製鉄所で、サイバー攻撃によって溶鉱炉が正常にシャットダウンできず、装置及び製鉄システム（操業）に大きな損害を与える事件が発生した。	攻撃は、特定の従業員らに対する標的型攻撃（スピアフィッシング）を通じて認証情報や機微な情報を窃取して、OA ネットワークに侵入し、その後、生産システムに侵入を拡大した。	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile http://www.bbc.com/news/technology-30575104 http://www.techweekeurope.co.uk/security/cyberwar/steelworks-damaged-cyber-attack-158107
14	フランスの国際放送局へのサイバー攻撃	放送	フランス	2015 年 4 月	フランス語の国際放送局が、イスラム過激派組織から大規模なサイバー攻撃を受け、番組の放送ができない状況に陥った。同局の Web サイトやソーシャルメディアも被害に遭い、同局を脅迫する様な内容とイスラム教のシャリア法を称賛する内容の声明が掲載された。	攻撃はインターネットネットワーク経由で発生した。何者かが盗んだパスワードやマルウェアを使って社内システムに侵入したとみられる。攻撃が始まって間もなく社内のコンピュータシステムがダウンした。	http://www.itmedia.co.jp/enterprise/articles/1504/10/news047.html https://the01.jp/p000159/
15	DEF CON（one of the world's largest hacker conventions）講演：化学プラントのハッキング	化学	ー	2015 年 8 月	講演のため、影響・被害なし。	制御システムのハッキングに必要となる制御システムへの理解度やプロセスを、攻撃の具体的なシミュレーションを通じて紹介している。	http://nationalcybersecurity.com/cyber-physical-attacks-hacking-a-chemical-plant/ http://www.networkworld.com/article/2968432/microsoft-subnet/cyber-physical-attacks-hacking-a-chemical-plant.html https://www.blackhat.com/docs/us-15/materials/us-15-Krotofil-Rocking-The-Pocket-Book-Hacking-Chemical-Plant-For-Competition-And-Extortion-wp.pdf
16	ウクライナ電力施設へのサイバー攻撃	電力	ウクライナ	2015 年 12 月	ウクライナ西部の州の半分と州都の一部で停電が発生、復旧までに約 6 時間を要し 40～70 万人程度が影響を受けた。ICS が使えず、復旧は手動により行われた。	変電所を監視する SCADA システムに侵入し、ワークステーションやサーバをマルウェア BlackEnergy3 に感染させた。その後、監視機能を停止させると共に SCADA システムのファイルを削除した。	https://www.jpcert.or.jp/present/2016/20160217_CSC-JPCERT01.pdf (p.6) http://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
17	イスラエル電力公社への大規模なサイバー攻撃	電力	イスラエル	2016 年 1 月	電力供給を管轄する電力公社が大規模なサイバー攻撃を受け、コンピュータ多数が使用不能になる深刻な事態に陥った。	電力公社のコンピュータを使用不能に陥れたのはランサムウェア。メールで送られてきたマルウェアが公社内のネットワーク全体に広がって多数のコンピュータが暗号化され、身代金を要求するメッセージが表示されていた。	http://www.itmedia.co.jp/enterprise/articles/1601/28/news060.html

制御システムのインシデント事例一覧（4/5）

#	事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）	参考情報（出典等）
18	ドイツの原子力発電所におけるマルウェア感染	電力	ドイツ	2016 年 4 月	原子力発電所で、核燃料棒を操作しているコンピュータがマルウェアに感染しているのが発見された。マルウェアが発見されたコンピュータは、インターネットに接続していなかったため、マルウェアが活動を始めることはなく、発電所の運転に影響はなかった。	3 基の原子炉のうち、稼働中の B 号機のコンピュータから、PC を遠隔操作できる W32.Ramnit と、PC 内部のファイルを盗み取る Conficker という 2 種類のマルウェアが、発電所の技師により発見された。また、原子炉の操作システムを管理している場所から離れた別のオフィスでは、マルウェアに感染した USB メモリ 18 本が見つかった。なお、Conficker と W32.Ramnit は、どちらも USB メモリ経由で拡散する。	http://gigazine.net/news/20160428-nuclear-plant-computer-virus/ http://wired.jp/2016/04/30/german-nuclear-plants-fuel-rod-system-swarming/ http://www.ibtimes.co.uk/gundremmingen-nuclear-power-plant-bavaria-shut-due-computer-malware-1556893 https://www.rt.com/news/341083-germany-gundremmingen-plant-virus/
19	サウジアラビアの空港、政府機関への攻撃	航空	サウジアラビア	2016 年 11 月	民間航空総局の事務管理システムの PC 数千台が破壊される被害が発生、業務が数日間停止した。 運航や空港業務、航空システムには影響は出ていない。 少なくとも 8 つの政府系組織で被害が確認された。	マルウェア Shamoon の新型が攻撃に使われた。Shamoon は、起動時に読み込まれるマスターブートレコードを消去し、コンピュータを機能不全にする。	http://d.hatena.ne.jp/Kango/20161201/1480614666
20	サンフランシスコの交通システムにおけるランサムウェア感染	交通	米国	2016 年 11 月	サンフランシスコの交通公社で、最大 2,112 台のコンピュータがランサムウェアに感染し、料金徴収が不能になった。電車やバスの運行自体には影響なく、市営鉄道の改札を開放して対応し、3 日後に完全復旧した。	コンピュータがランサムウェアに感染し、ハッカーらは復号鍵と引換えに 100 ビットコインを要求し、支払わなければ盗んだ 30GB のデータを公開するとも脅迫したが、内部調査の結果データ窃取はハッカーのハッタリと判断し、脅しを無視した。感染経路は従業員によるメールの添付ファイル／ポップアップ／リンクのクリックと見られる。	http://www.sfgate.com/bayarea/article/S-F-Muni-says-hacker-cost-agency-50-000-in-lost-10688275.php http://www.theregister.co.uk/2016/11/27/san_francisco_muni_ransomware/
21	ウクライナ電力施設へのサイバー攻撃	電力	ウクライナ	2016 年 12 月	ウクライナの首都キエフ北部とその周辺地域において停電が発生した。手動運用に切り替え、30 分以内に電力供給が再開され、約 1 時間 15 分後に完全に復電した。	電力会社のシステムがマルウェア Industroyer/Crashoverride に感染し、送電変電所の遮断機が不正操作された。	https://www.pcworld.com/article/3152010/security/cyberattack-suspected-in-ukraine-power-outage.html https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ https://dragos.com/blog/crashoverride/
22	英国最大の病院におけるランサムウェア感染	医療	英国	2017 年 4 月	英国で最大規模の病院グループで、IT 障害のため 136 件の手術と数百件のがん患者の化学療法の予約をキャンセルする事態が発生した。抗がん剤を処方するシステムや医用画像情報システムが使用不能になったほか、血液検査等も不能になった。遠隔で画像を確認することもできなくなった。	WannaCry（ランサムウェア）の感染が原因であった。なお、同病院では、セキュリティに問題がある Windows XP が現役で使われていた。	http://www.telegraph.co.uk/news/2017/05/01/cancer-patients-limbo-five-hospitals-suffer-major-crash/ http://www.zdnet.com/article/after-the-ransomware-attack-hospitals-are-still-recovering-from-the-wannacry-infection https://japan.cnet.com/article/35101196/ https://www.businessinsider.jp/post-33600 http://www.eweek.com/security/embedded-windows-medical-devices-infected-by-wannacry-ransomware

制御システムのインシデント事例一覧（5/5）

#	事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）	参考情報（出典等）
23	日本国内の自動車の生産システムにおけるランサムウェア感染	製造（自動車）	日本	2017 年 6 月	自動車の生産工場で、工場設備に付帯する PC が WannaCry に感染しているのが発見され、約 1 日間生産ラインを停止し、1,000 台が生産できなかった。他工場への影響はなく、同工場も翌日には操業を再開した。	生産ラインの管理等に使用する PC が WannaCry に感染した。 5 月に世界中で WannaCry 感染が報告されたのを受けて対策を固めていたが、完全に防ぐのは難しいことが改めて示された。	http://tech.nikkeibp.co.jp/it/atcl/news/17/062101713/ http://tech.nikkeibp.co.jp/it/atcl/news/17/062101717/ https://www.researchsnipers.com/honda-shuts-production-wannacry-ransomware-cyber-attack-prevails/
24	オーストラリア ヴィクトリア州の交通関連のカメラにおけるランサムウェア感染	交通	オーストラリア	2017 年 6 月	ヴィクトリア州で、159 台のスピード違反取り締まりカメラと交差点監視カメラが、WannaCry に感染した。感染により断続的に再起動を繰り返す状態が発生した。7,500 件の違反切符について一旦取り消すと発表した。	保守作業用に持ち込まれた USB メモリによって WannaCry に感染した。	http://www.zdnet.com/article/wannacry-now-claiming-159-traffic-cameras-in-victoria/
25	世界的物流会社の子会社におけるマルウェア感染	物流	オランダ	2017 年 6 月	世界的物流会社の子会社のグローバルな業務システムがサイバー攻撃を受け、業務と通信が大きな影響を受け、顧客へのサービスと請求で広範な遅れが発生した。更に、取引高の減少によって売り上げが減少した。	Petya（マルウェア、NotPtya とも呼ばれている）がウクライナの税務ソフトウェアソリューションに仕込まれた後、同社がウクライナで営業しているほか、被害に遭ったソフトウェアを使用しているため、Petya がグローバルネットワーク全体に侵入し、データを暗号化した。	http://www.businesswire.com/news/home/20170721005555/ja/ http://s1.q4cdn.com/714383399/files/oar/2017/AnnualReport2017/AnnualReport2017flat/docs/FedEx_2017_Annual_Report.pdf（p.17） http://news.softpedia.com/news/fedex-systems-may-never-fully-recover-after-petya-cyber-attack-517032.shtml http://www.ibtimes.co.uk/fedex-braces-financial-loss-global-cyberattack-leaves-computer-systems-offline-1630850
26	重要インフラ事業者の制御システムへの侵入による安全計装システムのマルウェア感染	不明	サウジアラビア	2017 年 8 月	事業者が使用している特定の安全計装システム（SIS）を狙ったマルウェア Triton（別名 Trisis、HatMan）に、SIS が感染した。何台かの SIS コントローラが異常状態に陥ったため緊急シャットダウンが作動し、一部の制御プロセスが停止した。	SIS のエンジニアリングワークステーションにリモートアクセスされ、Triron に感染した。Tiriton は SIS コントローラと通信し、プログラムを改ざんする機能を持っており、攻撃の過程で攻撃者のミスにより誤って緊急シャットダウンが引き起こされたと推測されている。	https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
27							
28							

このページは空白です。

付録 D. 用語集

本書における各用語の定義を記す。説明文中の青字の箇所は、本用語集で定義された用語であることを示す。

用語	説明
【あ行】	
悪意のある第三者	制御システムに対する攻撃者のうち、内部関係者以外の人物・組織・団体。
暗号技術	暗号アルゴリズムを用いて、認証・電子署名・暗号化等のセキュリティ対策を行うための技術。暗号アルゴリズムと鍵長に加えて、暗号鍵の管理、鍵関連情報の取り扱い、危殆化対策等の技術を含む。
インシデント	セキュリティを侵害して損害を引き起こす可能性のある事象または状況のうち、実際に発生した事象を指す。
【か行】	
外部ネットワーク	制御システムを構成するネットワークと接続された、外部のネットワーク（インターネット等）。
監視端末	制御システムを構成する資産の一つで、工程や現場の状況を確認するための端末。
脅威	セキュリティを侵害して損害を引き起こす可能性のある事情、能力、アクションまたは事象が存在する場合に生じる、セキュリティ違反の可能性。 （ISO/IEC 27000 における定義から引用）
脅威（攻撃手法）	本書で紹介する資産ベースのリスク分析において、各資産に対して想定される攻撃手法の視点で分類した脅威。
脅威レベル	本書で紹介する資産ベースのリスク分析及び事業被害ベースのリスク分析における評価指標の一つ。それぞれの分析手法において、想定する脅威が発生する可能性であり、資産ベースのリスク分析においては「資産に対する脅威が発生する可能性」、事業被害ベースのリスク分析においては「攻撃ツリーが成立する可能性」を意味する。脅威レベルは、3 段階（1：低～3：高）の値で評価し、その判断基準は、リスク分析を実施する事業者が定義する。
経由	攻撃用途の分類の一つで、侵入した攻撃者が攻撃拠点、もしくは攻撃対象に到達するまでに経由する装置等。
攻撃拠点	攻撃用途の分類の一つで、攻撃対象に対して攻撃を実行する（コマンド等を送信する）ことが可能な装置等。
検知／被害把握	セキュリティ対策をその用途・目的によって分類する際の一つ。「検知」は、攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知すること。「被害把握」

用語	説明
	は、攻撃の成功による被害や影響範囲を把握すること。
攻撃シナリオ	本書で紹介する事業被害ベースのリスク分析において、事業被害を引き起こす可能性のある攻撃拠点・攻撃対象・最終攻撃を具体化したシナリオ。
攻撃者	制御システムに対する攻撃の意思を有する人物・組織・団体。
攻撃ステップ	本書で紹介する事業被害ベースのリスク分析において、攻撃ツリーを構成する個々の攻撃手順。
攻撃対象	攻撃用途の分類の一つで、攻撃が行われ、破壊、情報窃取、改ざん等が行われる装置等。
攻撃ツリー	本書で紹介する事業被害ベースのリスク分析において、攻撃シナリオに含まれる攻撃拠点・攻撃対象・最終攻撃に加えて、攻撃シナリオを実現する攻撃者・侵入口・経由を具体化した一連の攻撃手順。
攻撃ツリー解析	シナリオベースのリスク分析手法における解析手法の一つ。攻撃者視点で、トップダウンに、誰が、どこから、どのルートを経由して被害発生を引き起こしうるかのシナリオを、攻撃ツリー（攻撃のステップからなる一連の攻撃フロー）として構成し、各ツリーの成立の可能性を算定する手法。
攻撃用途	本書における制御システムの資産の分類方法の一つとして、攻撃者の視点から見た資産の用途（悪用方法）。本書では、「侵入口」「経由」「攻撃拠点」「攻撃対象」のいずれかに分類する。
攻撃ルート	本書で紹介する事業被害ベースのリスク分析において、攻撃ツリーを作成する過程で検討する、侵入口から経由を経て攻撃拠点に至るまでのルート。
【さ行】	
最終攻撃	本書で紹介する事業被害ベースのリスク分析において、事業被害を引き起こす最終的な攻撃。例えば、事業被害が「制御システムの停止」の場合、最終攻撃は「システムのシャットダウンコマンドの実行」等となる。
最終攻撃ステップ	最終攻撃を実行する攻撃ステップ。
事業継続	攻撃の成功による被害を最小限に留めること、あるいは、サービスの継続、被害の早期復旧を実現することによって、事業を継続すること。セキュリティ対策をその用途・目的によって分類する際の一つ。
事業被害	事業（製品やサービスの製造・開発・提供等）の妨害、評判の低下等、組織の事業の安定的な運営や継続を阻害する事象・状況。
事業被害ベースのリスク分析	本書で紹介するリスク分析手法の一つで、攻撃ツリーを用いたシナリオベースのリスク分析手法を、本書ではこう呼ぶ。回避したい事業被害を明確化し、そこに至る攻撃が成り立つ可能性（脅威）、事業被害の度合い、攻撃を受け入れてしまう可能性（脆弱性）の相乗値を評価する。

用語	説明
事業被害レベル	本書で紹介する事業被害ベースのリスク分析における評価指標の一つ。想定した攻撃が行われた場合の被害範囲や会社経営上の打撃の度合い。事業被害レベルは、3 段階(1:低～3:高)の値で評価し、その判断基準は、リスク分析を実施する事業者が定義する。
資産	制御システムを構成する物理的な資産に加えて、システムに格納されている情報資産を含む。攻撃者による攻撃から防御すべき事業者の所有物。
資産グループ	本書で紹介する資産ベースのリスク分析において、資産のグループ化を行うことによって得られる資産の集合。
資産種別	本書で紹介する資産ベースのリスク分析において、資産のグループ化を行う際の分類基準の一つ。「情報系資産」「制御系資産」「ネットワーク資産」の 3 種類のいずれかに分類する。
資産のグループ化	本書で紹介する資産ベースのリスク分析において、作業工数を削減するために、制御システムを構成する資産を、その資産の設置場所・資産種別・資産が配置されている論理ネットワーク・資産の重要度・資産の機能によりグループ化すること。
資産の重要度	本書で紹介する資産ベースのリスク分析における評価指標の一つ。資産の重要度は、3 段階(1:低～3:高)の値で評価し、その判断基準は、リスク分析を実施する事業者が定義する。
資産ベースのリスク分析	本書で紹介するリスク分析手法の一つ。詳細リスク分析の一手法。保護すべき制御システムを構成する資産を対象に、各資産の重要度、想定される脅威、脆弱性の 3 つを評価指標として、リスク分析を実施する。
システム構成図	制御システムに対するリスク分析を実施するために、実際のシステムを明確化・論理化した分析用のシステムとネットワークの図。資産の名前と設置場所、論理ネットワーク構成等の情報を含む。
シナリオベースのリスク分析	詳細リスク分析の一手法。保護すべきシステムにおいて実現されている事業やサービスに対して、回避したい事業被害を定義し、発生した際の事業被害、その被害を起こし得る脅威、脆弱性の 3 つを評価指標として、リスク分析を実施する。
詳細リスク分析	リスク分析の手法の分類の一つ。評価対象のシステムに対して、そのシステムまたはシステムにより実現されている事業を、重要度・脅威・脆弱性の評価指標の下でリスク分析を実施する。
情報系資産	本書で紹介する資産種別の一つで、サーバ、操作端末、監視端末等パソコンやサーバの類の情報を管理することを目的とした資産。
情報ネットワーク	制御ネットワークと接続された企業内 LAN で、外部ネットワークとの接続点。
侵入口	攻撃用途の分類の一つで、攻撃者がサイバー攻撃を行う際に侵入する入口。
制御系資産	本書で紹介する資産種別の一つで、PLC 及び PLC より下流にあるバルブ、センサ

用語	説明
	等のフィールド機器等の制御に直接関わっている資産。
制御サーバ	制御システムを構成する資産の一つで、制御機器やフィールド機器に対し設定値やコマンドを送出するサーバ。
制御システム	社会インフラや工場・プラントの監視・制御や生産・加工ラインにおいて、他の機器やシステムを管理・制御するために用いられている機器群。
制御ネットワーク	制御システムを構成するネットワークの一つで、制御目的に使用するデータを転送する LAN。本書においては、情報側とフィールド側の 2 つで構成される。
制御ネットワーク（情報側）	制御ネットワークのうち、情報ネットワークまたは DMZ 上の機器（サーバ等）との間で、制御目的に使用するためのステータス情報やデータを転送するためのネットワーク。
制御ネットワーク（フィールド側）	制御ネットワークのうち、自ネットワーク及びフィールドネットワーク上の機器（PLC）との間で、制御目的に使用するためのステータス情報やデータを即時転送するためのネットワーク。制御に特化した高い応答性を持つ。
脆弱性	リスクにつながる脅威を受け入れてしまう受容性で、評価対象に内在するセキュリティ上の弱さ。
脆弱性検査	セキュリティテストの一手法であり、本書においては、制御システムにおける既知の脆弱性を検出することを目的に実施する。
脆弱性レベル	本書で紹介する資産ベースのリスク分析及び事業被害ベースのリスク分析における評価指標の一つ。それぞれのリスク分析手法において、発生した脅威を受け入れる可能性を意味する。脆弱性レベルは、3 段階（1：低～3：高）の値で評価し、各脅威に対するセキュリティ対策状況を 3 段階に評価した「セキュリティ対策レベル」の値を利用して算定する。その判断基準は、3.5 節における定義に従う。
セキュリティ対策	攻撃者による攻撃から制御システムを防御するために事業者が実施する対抗手段。本書においては、「技術的対策」、「物理的対策」、「運用面での対策」のいずれかに分類する。
セキュリティ対策レベル	評価指標「脆弱性レベル」の値を算定する際、中間的に利用する評価指標。資産ベースのリスク分析及び事業被害ベースのリスク分析手法において、発生する脅威に対するセキュリティ対策状況を意味する。セキュリティ対策レベルは、3 段階（1：低～3：高）の値で評価し、それぞれが脆弱性レベル＝3～1 の値に対応する。その判断基準は、3.5 節における定義に従う。
セキュリティテスト	サイバー攻撃に対する制御システムのセキュリティ強度を確認するための手段としての検査・試験方法。
セキュリティパッチ	OS やプログラムにセキュリティ上の問題が発見されたときに、それらの問題を修正するためのプログラム。

用語	説明
操作端末	「HMI」を参照。
ゾーニング	外部ネットワークから内部ネットワークへの侵入や内部ネットワークにおける侵攻拡散を防止するために、ネットワークを複数に分割すること。
【た行】	
対策候補	資産ベース及び事業被害ベースのリスク分析手法において、発生する脅威に対して有効と考えられるセキュリティ対策の候補。
対策レベル	「セキュリティ対策レベル」を参照。
多層防御	複数の異なるセキュリティ対策を組み合わせることで、1 つの対策が破られても次の（そのまた次の）対策で攻撃を抑止し、攻撃が重要部に到達する前に検知及び対応できる様にする、セキュリティアプローチ。
データサーバ	制御システムを構成する資産の一つで、制御ネットワーク上にありプロセス値を収集するサーバ。更に PLC から届いたプロセス値を転送する。
データヒストリアン	制御システムを構成する資産の一つで、長期間のプロセス値や管理パラメータが保存され分析されるサーバ。データサーバより静的なデータを扱う。
データフロー	制御システムにおけるデータの流れ（種類と経路）。本書においては、システム構成図中に図示して表現することとし、データは制御システムのプロセス値やコマンドを意味する。
【な行】	
内部関係者	制御システムに対する攻撃者のうち、システムの所有者や保守・運用関係者等の人物・組織・団体。
内部不正	内部関係者による制御システムに対する攻撃行為。
ネットワーク資産	本書で紹介する資産種別の一つで、スイッチ、ルータ、ファイアウォール及び、それらの機器を接続している回線。
【は行】	
パケットキャプチャテスト	セキュリティテストの一手法であり、本書においては、制御システムのネットワーク上のパケットに不審な通信が含まれていないかを分析することを目的に実施する。
パッチ	OS やプログラムに機能上の問題が発見されたときに、それらの問題を修正するためのプログラム。セキュリティパッチを含む。
パッチサーバ	制御システムを構成する資産の一つで、接続された機器の OS やソフトウェアのアップデートやパッチ、アンチウイルスのパターンファイル等を提供するサーバ。
標的型攻撃	特定の組織や個人を攻撃対象として、重要情報や知的財産等の不正取得や組織の活動妨害等を目的に行われるサイバー攻撃。
ファイアウォール	制御システムを構成する資産の一つで、外部のネットワークからの攻撃や侵入を防ぐための機能を有する機器、または同機能。

用語	説明
フィールド機器	制御システムにおいて、PLC に接続されたバルブやセンサ等。
フィールドネットワーク	制御システムを構成するネットワークの一つで、制御ネットワーク（フィールド側）の PLC 等の接続機器とフィールドに存在する機器の間の通信に用いられるネットワーク。
フォルトツリー解析	シナリオベースのリスク分析手法における解析手法の一つ。被害（インシデント等）事象を起点として、ボトムアップに、その被害に至る１ステップ前の攻撃事象を順じ追跡するツリー（フォルトツリー）を攻撃の原点までを構成し、各ツリーの成立の可能性を算定する手法。
ペネトレーションテスト	セキュリティテストの一手法であり、本書においては、制御システムへの侵入可否を検証することを目的に実施する。
防御（侵入／拡散段階）	セキュリティ対策をその用途・目的によって分類する際の一つ。攻撃者による初期侵入、内部の情報収集や侵入範囲拡大を防止すること。
防御（目的遂行段階）	セキュリティ対策をその用途・目的によって分類する際の一つ。攻撃者による最終目的の実現を防止すること。
保守用 PC	制御システムを構成する資産の一つで、PLC やフィールド機器のメンテナンスを行うための PC。
【ま行】	
モデルシステム	本書で紹介する資産ベースのリスク分析及び事業被害ベースのリスク分析を説明するために使用する、典型的な制御システムの構成からなる評価対象システム。
【や行】	
【ら行】	
リスク値	本書で紹介する資産ベースのリスク分析及び事業被害ベースのリスク分析において、脅威レベル、脆弱性レベル、資産の重要度／事業被害レベルの評価点を元に算定する、各資産／攻撃ツリーの総合的なリスクの度合い。
リスク分析	保護すべきシステムやそれによって実現している事業（サービス等含む）に対する脅威と被害のレベル（可能性と大きさ等）を明確にするプロセス。
【わ行】	
【A】	
ATA	Attack Tree Analysis の略語。本書においては、「攻撃ツリー解析」。
CIA	情報システムが備えるべきセキュリティ要件。機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)の頭文字。
CRYPTREC 暗号リスト	電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を

用語	説明
	調査・検討するプロジェクトである CRYPTREC（Cryptography Research and Evaluation Committees）において、総務省及び経済産業省が公表している、電子政府における調達のために参照すべき暗号のリスト。
CSMS	Cyber Security Management System の略語。 制御システムを運用する組織におけるセキュリティマネージメントシステムの適合性評価制度。
DCS	Distributed Control System の略語。 プロセス制御で使用される制御システムで、複数のコンピュータを用いて統合的な制御を実現する。
DMZ	DeMilitarized Zone の略語で、直訳すると「非武装地帯」。 本書においては、外部ネットワークと制御ネットワークとの境界に設けられるネットワーク。
EWS	Engineering Workstation の略語。 制御システムを構成する資産の一つで、PLC のプログラムの改造や制御サーバのプログラムの変更等を行うためのコンピュータ。
FTA	Fault Tree Analysis の略語。本書においては、「フォルトツリー解析」。
HMI	Human Machine Interface の略語。 制御システムを構成する資産の一つで、制御機器やフィールド機器に対する指示を入力する端末。
HSE	健康(Heaith)、安全(Safety)、環境(Environment)の頭文字であり、事業活動に伴う労働安全性問題や環境問題を示す。 （JIPDEC CSMS ユーザーズガイドにおける定義から引用）
ISMS	Information Security Management System の略語。 情報システムを運用する組織におけるセキュリティマネージメントシステムの適合性評価制度。
PLC	Programmable Logic Controller の略語。 制御システムを構成する資産の一つで、センサからの信号により接点や操作器を制御する等入出力信号を扱う機器。
SCADA	Supervisory Control and Data Acquisition の略語。 制御とデータ収集を行うシステムの総称。

更新履歴

2017 年 10 月 2 日	初版
2017 年 11 月 10 日	誤字修正
2017 年 12 月 19 日	コラムの追加（p.27, p.220）、図の差し替え（図 1-2、図 4-10）、誤字修正
2018 年 4 月 2 日	付録 B.1（暗号技術利用チェックリスト）の更新、付録 C（制御システムのインシデント事例一覧）の更新

本ガイドは、以下の URL からダウンロード可能です。

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

IPA 独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコート センターオフィス
TEL: 03-5978-7527　FAX: 03-5978-7552
https://www.ipa.go.jp/security/