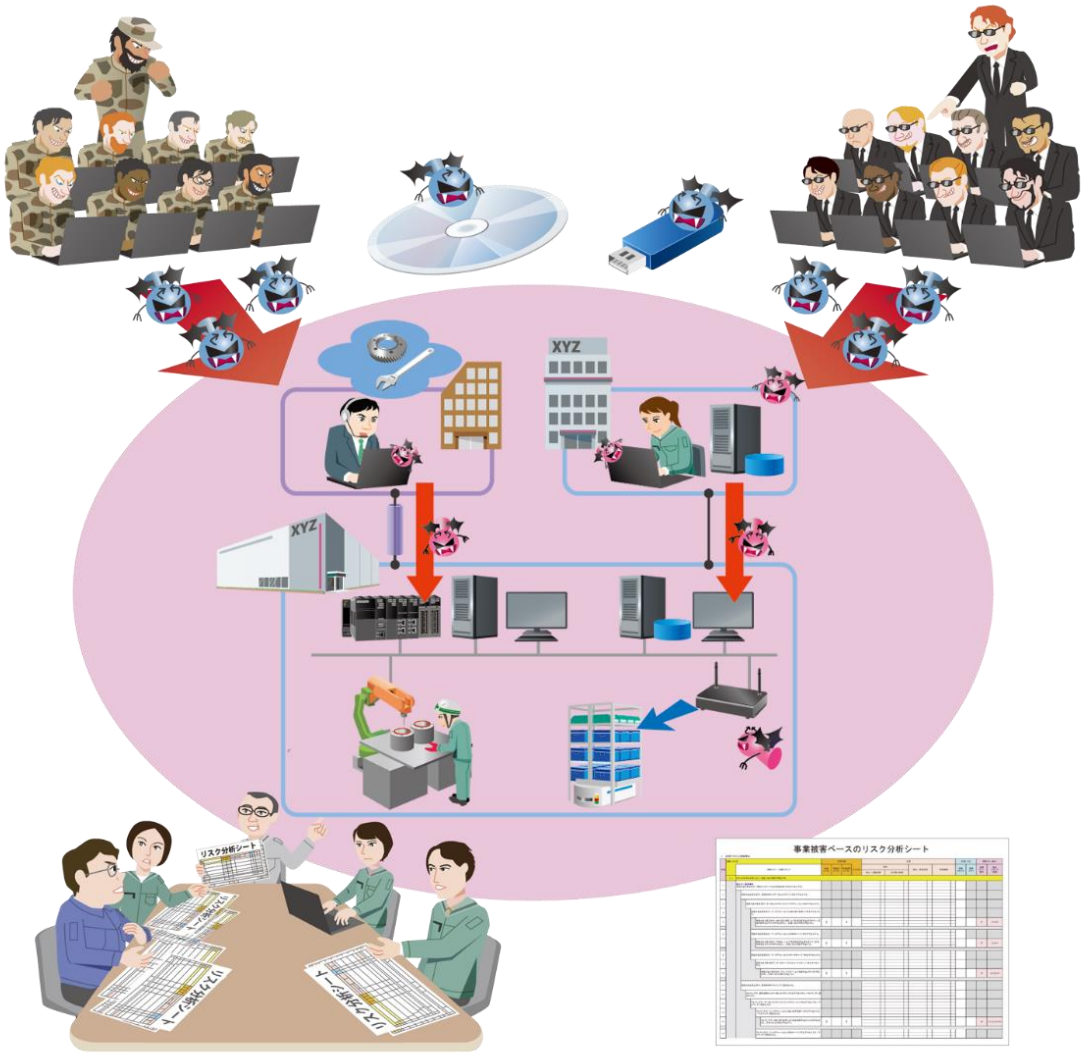
制御システムに対する
リスク分析の実施例
第2版　事例2

～制御システムのセキュリティリスク分析ガイド　別冊～
社外サービスと接続した制御システムに対するリスク分析



2026 年 4 月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

目 次

はじめに.....6
1. 本書の概要.....7
1.1. 公開の背景.....7
1.2. 本書の特徴.....8
1.2.1. 外部サービスとのネットワーク接続.....9
1.3. 本書の対象読者.....11
1.4. リスク分析実施例の概要.....12
1.5. リスク分析対象システム概要.....14
1.5.1. システムの概要.....14
1.5.2. 外部サービスとのネットワーク接続構成の概要.....15
1.5.3. システムの構成資産（機器・ネットワーク）.....18
1.6. リスク分析の流れとアウトプット.....20
2. リスク分析のための事前準備.....23
2.1. 資産一覧.....28
2.2. システム構成図.....33
2.3. データフローマトリックス.....35
2.4. 資産の重要度の判断基準.....39
2.5. 各資産に対する重要度一覧.....40
2.6. 事業被害レベルの判断基準.....41
2.7. 事業被害と事業被害レベルの検討.....42
2.8. 脅威レベルの判断基準.....44
2.9. 対策レベル（脆弱性レベル）の判断基準.....45
3. 資産ベースのリスク分析.....46
3.1. 脅威レベルの検討.....47
3.2. 資産ベースのリスク分析シートの作成.....51
3.3. リスク値のまとめ.....59
4. 事業被害ベースのリスク分析.....62
4.1. 攻撃シナリオ一覧の作成.....63
4.2. 外部からの侵入口の検討と選定.....65
4.3. 攻撃者と侵入口の検討と選定.....67
4.4. 攻撃ルートの作成.....68
4.5. リスク分析シートの作成.....72
4.6. リスク値のまとめ.....81

5. リスク分析の活用 82
5.1. リスク低減効果の検討 82
5.2. リスク低減策の実施計画の検討 86
5.3. リスク低減効果の把握 88
付録 A. 資産ベースのリスク分析実施結果 89
付録 B1. 事業被害ベースのリスク分析実施結果 シナリオソート版 89
付録 B2. 事業被害ベースのリスク分析実施結果 侵入口ソート版 89
付録 C. モバイル閉域網とインターネット VPN を組み合わせた外部接続の事例 90
更新履歴 99

図 目 次

図 1-1 制御システムと外部サービスとの代表的な構成例 9
図 1-2 システム構成概要（ガイド別冊 左図、本書 右図） 12
図 1-3 制御システムの外部とのデータフロー（ガイド別冊 左図、本書 右図） 12
図 1-4 リスク分析範囲（ガイド別冊 左図、本書 右図） 13
図 1-5 サイバー攻撃の侵入口（ガイド別冊 左図、本書 右図） 13
図 1-6 分析対象システムの構成図（外部ネットワーク接続の詳細は本分析対象外） 14
図 1-7 インターネット VPN による外部接続構成 15
図 1-8 モバイル閉域網と VPN を組み合わせた外部接続構成 16
図 1-9 リスク分析の流れと成果物 22
図 2-1 事前準備作業の流れ 23
図 2-2 システム構成図 33
図 2-3 データフロー図（全体） 36
図 2-4 データフロー図（制御・エンジニアリング） 37
図 2-5 データフロー図（プロセスデータ・参照） 38
図 3-1 資産ベースのリスク分析作業の流れ 46
図 4-1 事業被害ベースのリスク分析作業の流れ 62
図 4-2 侵入口の候補 65
図 4-3 攻撃ルート図 71
図 C-1 「スマート工場のセキュリティリスク分析調査報告書」より 90
図 C-2 システム構成例 91
図 C-3 データフロー 92
図 C-4 侵入口と攻撃ルート例 95

表 目 次

表 1-1 制御システムと外部サービスとの接続形態ごとの特徴と主な脅威 10
表 1-2 分析対象システムの資産概要 18
表 1-3 アウトプット一覧表 21
表 2-1 事前準備作業のアウトプット一覧 23
表 2-2 管轄部門のまとめ（例） 26
表 2-3 資産一覧表 29
表 2-4 データフローマトリックス 35
表 2-5 資産の重要度の判断基準の定義例 39
表 2-6 資産の重要度 40
表 2-7 事業被害レベルの判断基準例 41
表 2-8 事業被害の一覧表 42
表 2-9 事業被害一覧と事業被害レベル 43
表 2-10 脅威レベルの判断基準 44
表 2-11 脆弱性レベル（対策レベル）の判断基準 45
表 3-1 利用する事前準備のアウトプット 46
表 3-2 資産ベースのリスク分析作業で作成するアウトプット 46
表 3-3 分析対象の資産に想定される脅威一覧表 47
表 3-4 FW(発電)の脅威レベルと根拠 49
表 3-5 資産の脅威レベルまとめ表 50
表 3-6 資産ベースのリスク分析シート 53
表 3-7 資産ベースのリスク分析 脆弱性レベルまとめ表 59
表 3-8 資産ベースのリスク分析 リスク値まとめ表 60
表 3-9 リスク値の変化 61
表 4-1 利用する事前準備のアウトプット 62
表 4-2 事業被害ベースのリスク分析作業で作成するアウトプット 62
表 4-3 攻撃シナリオ一覧表 63
表 4-4 侵入口の検討表 66
表 4-5 攻撃者と侵入口の選定例 67
表 4-6 攻撃ルート一覧表（シナリオソート版） 68
表 4-7 事業被害ベースのリスク分析シート（シナリオソート版） 73
表 4-8 事業被害ベースのリスク分析結果 リスク値まとめ表 81
表 4-9 事業被害ベースのリスク分析結果 リスク値まとめ表（侵入口ベース） 81
表 5-1 共通の攻撃ルートを持つ攻撃ツリーによるまとめ 83
表 5-2 リスク低減のためのセキュリティ緩和策の例 84

表 5-3 セキュリティ緩和策実施計画の検討例 86
表 5-4 事業被害ベースのリスク分析結果 リスク値まとめ表.....88
表 5-5 事業被害ベースのリスク分析結果 リスク値まとめ表（侵入口ベース）.....88
表 C-1 侵入口となる資産・ネットワークと分析対象の検討表 93
表 C-2 攻撃ルートの検討表 94
表 C-3 事業被害ベースのリスク分析実施例 96

はじめに

本書は、ガイド本編第 2 版で解説するリスク分析手法の実施例の 2 つ目の事例として 2024 年 12 月に公開したものであり、外部ネットワークに接続した制御システムを対象にしたリスク分析例を提示している。

今回、ガイド本編の第 2 版改定で追加・変更された内容にあわせて、本書で提示しているガイド本編への参照先情報の修正を行った。また、記載ミスなどの修正も行っている。

本書が、制御システムを有する事業者の多くが、詳細リスク分析の実施に踏み出す一助となることを期待している。

独立行政法人　情報処理推進機構	内田　努
独立行政法人　情報処理推進機構	木下　弦
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	辻　宏郷
独立行政法人　情報処理推進機構	平澤　満
独立行政法人　情報処理推進機構	市野澤　昌弘
独立行政法人　情報処理推進機構	松島　伸彰
独立行政法人　情報処理推進機構	高見　穣

1. 本書の概要

1.1. 公開の背景

近年、制御システムにおいて生産性、設備稼働率、安全性、品質、および保守性等の向上を実現する観点で、制御システムが外部サービスに直接または間接的に接続する事例が増えている。

これまでの「制御システムのセキュリティリスク分析ガイド 第 2 版(2023 年 3 月版)[1]」(以下、「ガイド本編」と呼ぶ)」、「ガイド別冊:制御システムに対するリスク分析の実施例 第 2 版(2023 年 12 月版)[2]」(以下、「ガイド別冊」と呼ぶ)では、制御システムが外部サービスと接続しない構成であった。

本書では、「ガイド別冊」のシステム構成を拡張し、制御システムが外部サービスと直接ネットワーク接続する構成において、“外部ネットワークから攻撃者が侵入する脅威”を新たに想定し、リスク分析をした実施例を提示する。

本書のリスク分析実施例を通し、外部ネットワークと制御システムが接続した構成におけるリスク分析について理解が深まるとともに、事業者がリスク分析に取り組む一助となり、事業者のセキュリティレベルが高まることを期待している。

1 「制御システムのセキュリティリスク分析ガイド 第 2 版(2023 年 3 月版)」(公開当時)
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

2 「ガイド別冊:制御システムに対するリスク分析の実施例 第 2 版(2023 年 12 月版)」(公開当時)
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

1.2. 本書の特徴

本書の特徴として以下の 4 点を示す。

- 制御システムから外部システムへの”データ収集”と、制御システムに対する”リモート保守”のデータフロー

  リスク分析対象システムでは、外部システムにおいて制御システムのデータ収集するデータフローとベンダー保守拠点より制御システムの資産をリモートで保守を行うためのデータフローが存在する。本書では、この 2 種類のデータフローを中心に制御システムのセキュリティリスク分析を実施する。

- 資産ベースのリスク分析の実施例

  制御システムが外部ネットワークと接続する影響で、制御ネットワーク上の資産において「不正アクセス」等の脅威レベルが変化する。このため、資産ベースのリスク分析の実施例で、制御システムが外部ネットワーク接続する前のリスク分析結果と接続した後のリスク分析結果を比較している。

- 事業被害ベースのリスク分析の実施例

  制御システムが外部ネットワークと接続することで生まれた「脅威：侵入口」の検討と選定を行った。また、これらの侵入口から派生する攻撃ルートについて、事業被害ベースのリスク分析を行い、リスク結果を提示している。

- リスク分析結果の活用例

  事業被害ベースのリスク分析の実施例をもとに、外部ネットワークからのサイバー攻撃のリスクを低減するための方策を検討し、例を提示している。

1.2.1. 外部サービスとのネットワーク接続

事業者の制御システムと外部サービスのネットワーク接続には様々な構成があるが、代表的な例[3]を以下に示す(図 1-1)。

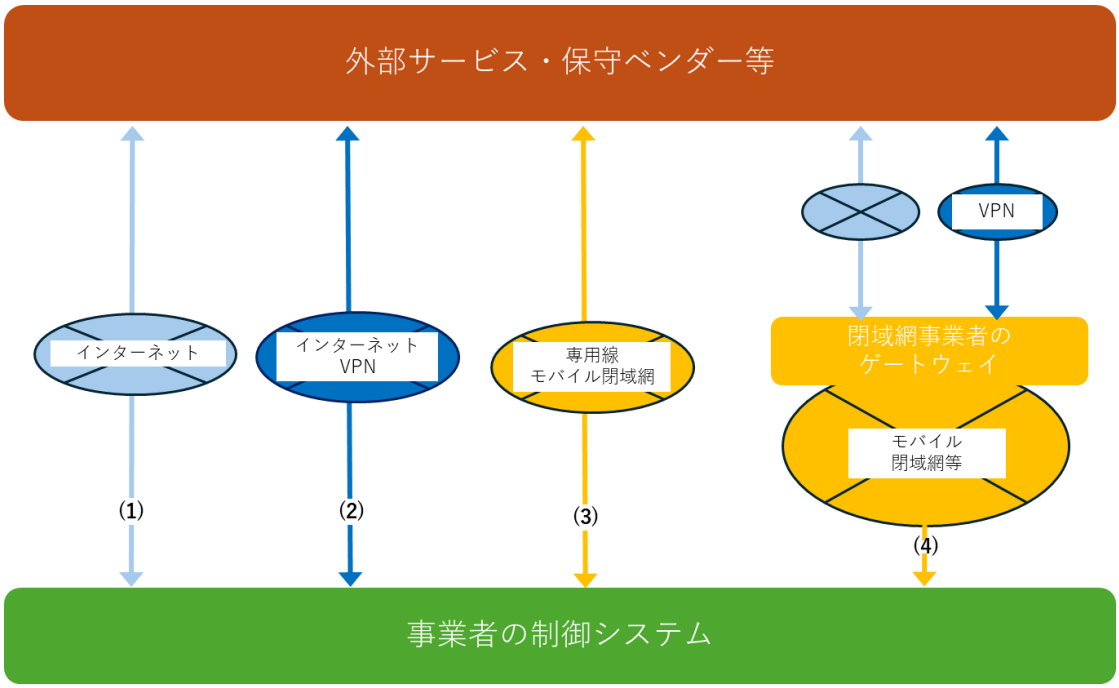


図 1-1 制御システムと外部サービスとの代表的な構成例

(1) インターネット(VPN なし)による接続形態

低コストで導入・運用が可能であり、制御システムと外部サービスや保守ベンダーとの接続方法に柔軟性を持たせることができる。一方、ファイアウォールや通信暗号化、多要素認証などのセキュリティ対策なしの環境では、この接続形態の不正アクセスや通信の盗聴や改ざんに対する脅威が高くなる。

(2) インターネット VPN を利用した接続形態

既存のインターネット回線を利用して暗号化通信を実現でき、専用線と比較すると低コストに導入が可能である。制御システム側がサーバーとして VPN 機器を利用する場合は、インターネット側から侵害のリスクがあるため、VPN 機器の適切な運用が必須となる。

(3) 専用線やモバイル閉域網を利用した接続形態

事業者と外部サービス双方がインターネットからの脅威をうけなくなり、最も高いセキュリティ構成となる。一方で、専用線接続は(1)(2)と比較するとコストが高くなる。

---

[3] LPWA による接続例は"「スマート工場のセキュリティリスク分析調査」調査報告書 第 2 版" P87 で解説

（4） モバイル閉域網と VPN を経由する接続形態

事業者の制御システムはモバイル閉域網と接続し、モバイル閉域網と外部サービスを別途インターネット VPN などで接続する構成をとる。専用線の構成より低コストであること、外部サービスと柔軟な接続が可能なこと、事業者側の資産がインターネットに公開されない利点がある。ただし、モバイル閉域網と外部サービスとの通信など、完全な閉域網ではない経路がセキュリティ侵害される可能性がある。

また、（1）～（4）の構成例で共通して、外部サービス・保守ベンダー経由で事業者の制御システムが侵害される、サプライチェーンの脅威がある。閉域網によって事業者の制御システムがインターネットに露出しなくなるが、外部サービス経由もしくは保守ベンダー経由で閉域網への侵害が起きる可能性は残る。

表 1-1 制御システムと外部サービスとの接続形態ごとの特徴と主な脅威（1/2）

#	接続形態	特徴	インターネットにおける主な脅威
(1)	インターネット（VPN なし）	・低コストで導入、運用が可能で、制御システムと外部サービスの接続に柔軟性がある ・インターネット経由での脅威には追加のセキュリティ対策が必要となる	・インターネットに公開した制御システムの端末への攻撃（誤って公開された端末、サービスを含む） ・非暗号化通信の場合、通信経路での盗聴や改ざん
(2)	インターネット VPN	・通信経路の暗号化が標準で可能である ・VPN サーバーやクライアントの機能により、不正アクセスなどの脅威に対抗できる場合がある	・制御システムの VPN サーバーに対する攻撃
(3)	単独の専用線やモバイル閉域網	・制御システムと外部サービスとの通信がインターネットに露出しない ・(1)(2)の方式と比較して費用が増加する場合がある	（閉域網に接続するネットワーク経由の脅威が残る）

表 1-1 制御システムと外部サービスとの接続形態ごとの特徴と主な脅威(2/2)

#	接続形態	特徴	インターネットにおける主な脅威
(4)	モバイル閉域網とインターネット VPN を経由する接続	・制御システム側はインターネットを使用しない ・制御システムをインターネットに接続せずに、インターネット上で公開される外部サービスの接続点や保守ベンダーが用意する VPN 装置に接続できる ・(1)(2)の方式と比較して費用が増加する場合がある	（閉域網に接続するネットワーク経由の脅威が残る）

本書では、制御システムが「(2)インターネット VPN」により外部サービスと接続するシステム構成でリスク分析を実施する。また、「(4)モバイル閉域網とインターネット VPN を経由する接続」については、本書付録 C にて事業被害ベースのリスク分析実施例を簡単に説明している。
本書で解説しない、「(1)インターネット(VPN なし)」、「(3)単独の専用線やモバイル閉域網」により外部サービスと接続するシステム構成については、IPA で公開している「スマート工場のセキュリティリスク分析調査」調査報告書において、システム構成・脅威とリスク分析・対策例の提示[4]をしているのでリスク分析を実施する際の参考としてほしい。

1.3. 本書の対象読者

本書の主な読者として以下を想定している。

- 制御システムを運用する、セキュリティ統括部署、事業責任者、制御システムの運用部門、制御システムの設計開発検討部門
- 制御システムに関与するベンダー

[4] 「スマート工場のセキュリティリスク分析調査」調査報告書 第 2 版
https://www.ipa.go.jp/security/controlsystem/controlsystem-smartplant.html
実装モデル 2、3、4、5、7 が参考になる

1.4. リスク分析実施例の概要

本書に掲載しているリスク分析実施例について、「ガイド別冊」との違いを踏まえ簡単に説明する。

（1）システム構成の概要

「ガイド本編」「ガイド別冊」でリスク分析対象としている制御システムは、事業者の情報システム以外のネットワーク接続を持たないシステム構成となっている。

本書のシステム構成では、他拠点制御システムを「発電システム」と明確化し、「発電システム」がインターネット経由で外部サービスと接続する構成が追加した。

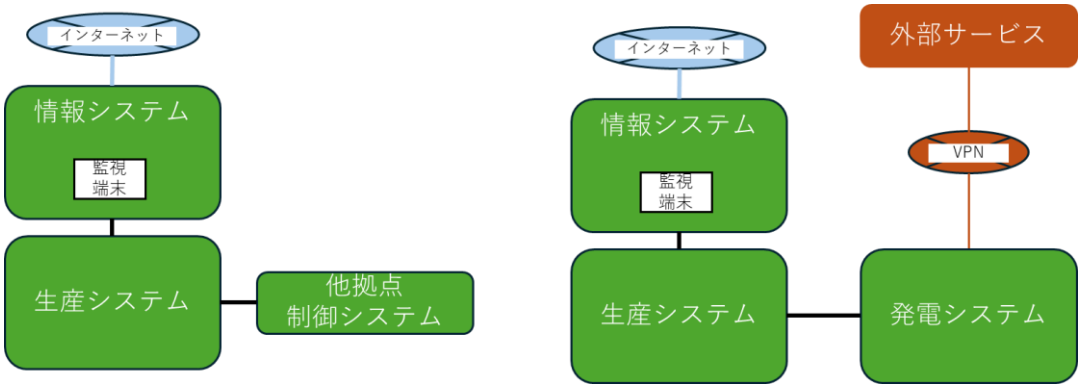


図 1-2 システム構成概要（ガイド別冊　左図、本書　右図）

（2）制御システム外部とやりとりするデータフロー

外部サービスでは制御システムのデータを受信し利用する一方、ベンダーが外部から保守サービスを実施するデータフローを追加した。

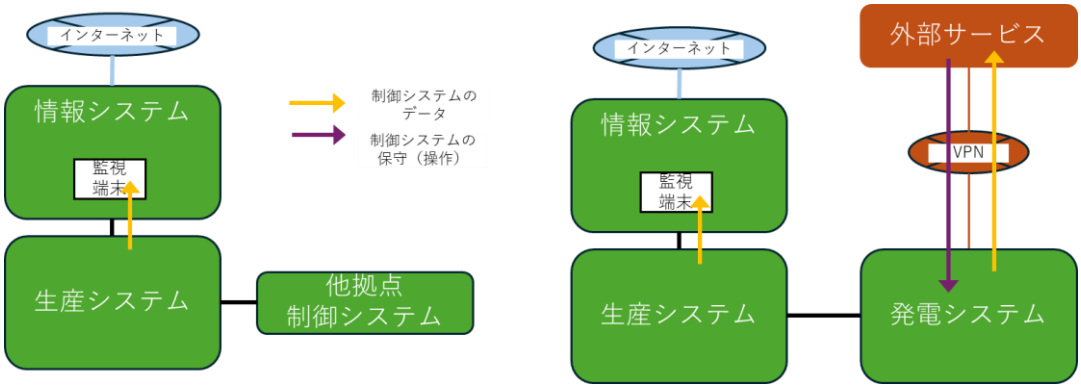


図 1-3 制御システムの外部とのデータフロー（ガイド別冊　左図、本書　右図）

（3）リスク分析範囲

ガイド別冊でのリスク分析の範囲は、一つの制御システム「生産システム」とそれに接続する情報システム上の監視端末の資産までをリスク分析範囲としていた。

本書では、それに加えて生産システムと接続する発電システムをリスク分析範囲として追加し、外部サービスとネットワーク接続することによるサイバーセキュリティリスクを分析する。

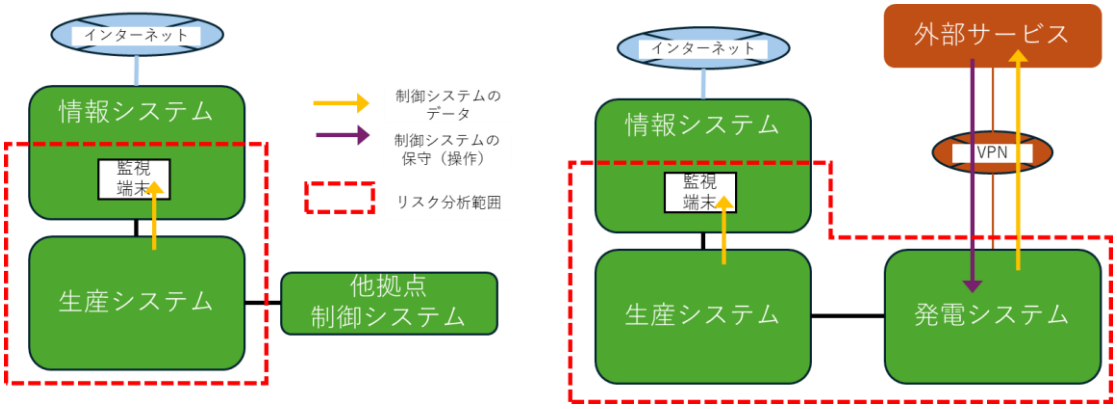


図 1-4 リスク分析範囲（ガイド別冊　左図、本書　右図）

（4）リスク分析対象とするサイバー攻撃の侵入口

「ガイド別冊」では、攻撃者がインターネットから情報システムを経由して生産システムを攻撃すること、事業者の情報システムや生産システムがあるエリアに物理的に侵入を行ってから生産システムを攻撃するといった攻撃ルートを検討した。

本書では、事業者の制御システムが外部サービスと接続することによる新しい脅威に着目してリスク分析を行う。このため、侵入口は事業者の発電システムの外接点を狙った攻撃ルート、不正アクセスされた外部サービス経由での攻撃ルートに絞って攻撃ルートを検討した。

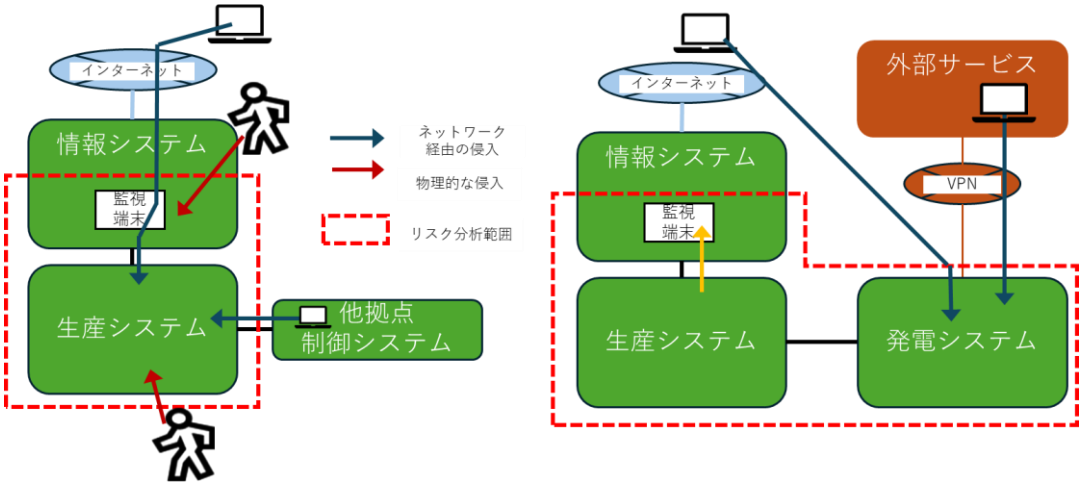


図 1-5 サイバー攻撃の侵入口（ガイド別冊　左図、本書　右図）

1.5. リスク分析対象システム概要

本書のリスク分析対象システムについて、簡単に説明する。

1.5.1. システムの概要

事業者は製造業で、生産設備を制御する制御システムを含む工場を保有している。また、工場の動力は、自家発電システムによる給電により稼働している。

自家発電システムの発電量等の利用状況を情報ネットワーク上の端末から閲覧する目的で、自家発電システムを納入したベンダーが提供する外部サービスと、自家発電システムがネットワーク接続されている。

また、自家発電システムを納入ベンダーが遠隔監視・遠隔保守する目的で、納入ベンダーの保守拠点より自家発電システムへネットワーク接続可能な構成となっている。

システム構成図を図 1-6 に示す。また、次項 1.5.2 で外部ネットワーク接続構成 2 種類を説明する。

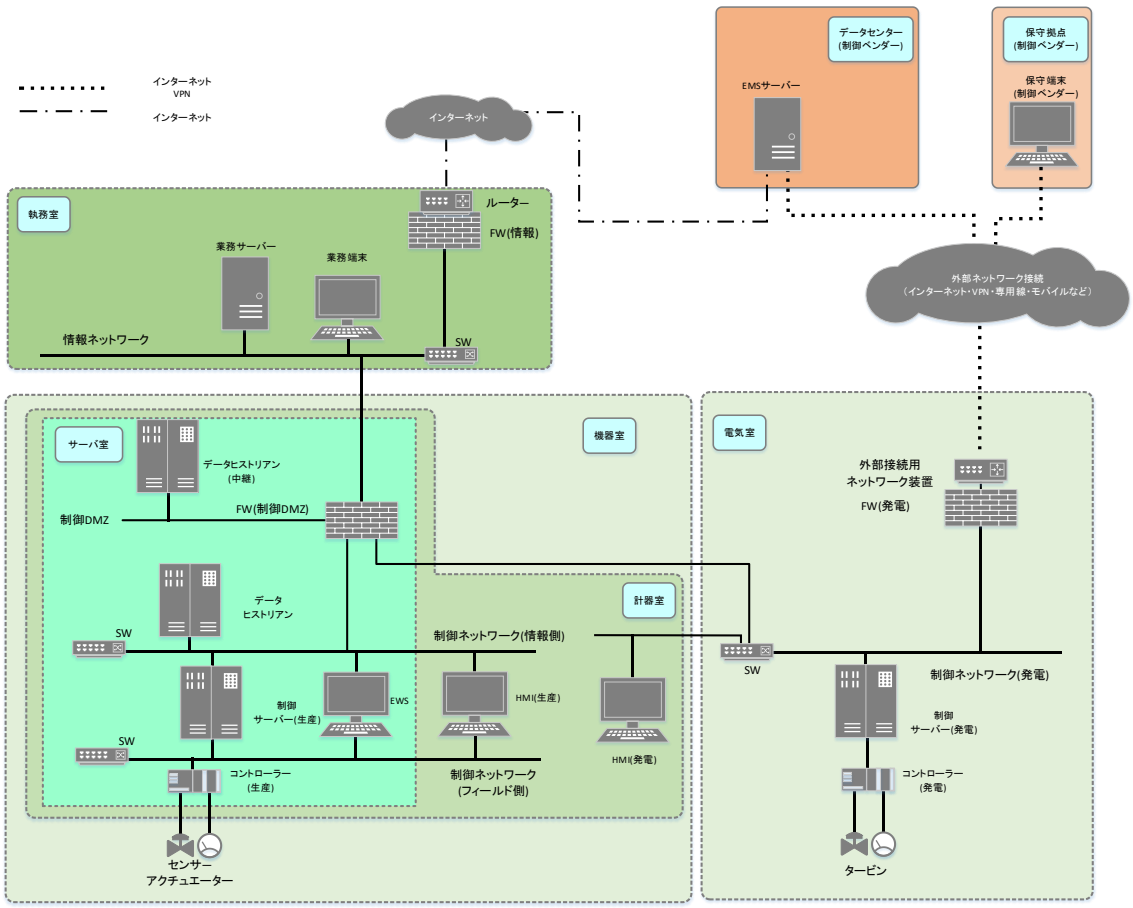


図 1-6 分析対象システムの構成図(外部ネットワーク接続の詳細は本分析対象外)

1.5.2. 外部サービスとのネットワーク接続構成の概要

制御システムと外部サービスの接続構成は多くのものがあるが、代表的な接続構成について「1.2.1 外部サービスとのネットワーク接続」で紹介した。ここでは、「インターネット VPN による外部接続構成」と「モバイル閉域網と VPN を組み合わせた外部接続構成」について、概要図を示す。

1.5.2.1. インターネット VPN による外部接続構成

図 1-7 に、制御システムが外部サービスとインターネット VPN を利用して接続している構成例を示す。この構成図では、インターネット VPN は拠点間を IPsec-VPN で接続する方式とした。

本編の 1.5.3 以降では、本構成を分析対象システムとして説明をしている。

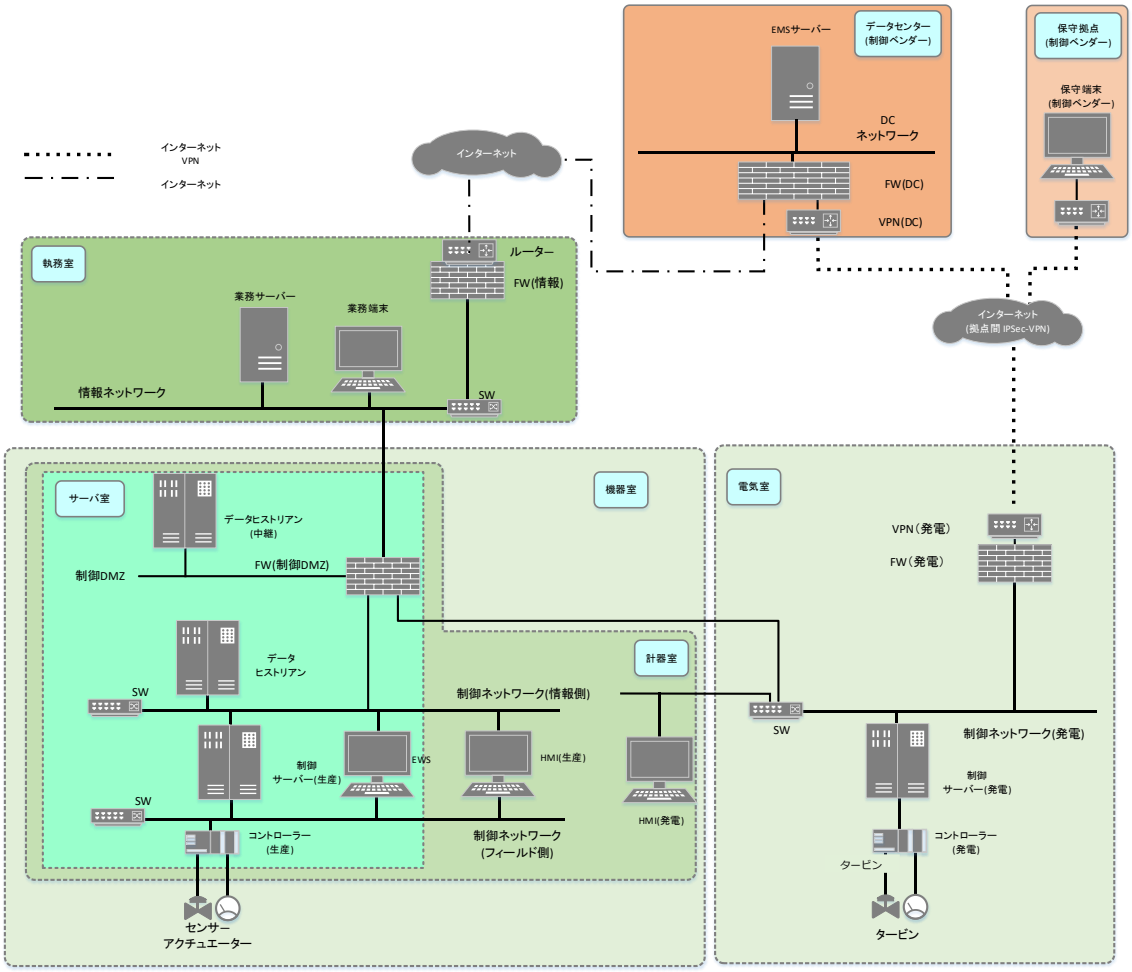


図 1-7 インターネット VPN による外部接続構成

SSL-VPN 方式で接続している場合でも、上図に似たシステム構成となるが、SSL-VPN の場合は、VPN クライアントより VPN サーバーとなる VPN 装置がインターネット経由の脅威が高くなる点に留意が必要である。

1.5.2.2. モバイル閉域網と VPN を組み合わせた外部接続構成

図 1-8 に、制御システムがモバイル閉域網と VPN を組み合わせて外部サービスと接続している構成例を示す。青い破線で囲まれた箇所が「1.5.2.1 インターネットVPNによる外部接続構成 図 1-7」と構成が異なる箇所である。

この構成では、事業者側に固定のインターネット回線を設置する必要がないので、固定のインターネット回線を設置できない場合などで採用されている。

本構成でのリスク分析の中間成果物とリスク分析結果は、付録 C で提示している。

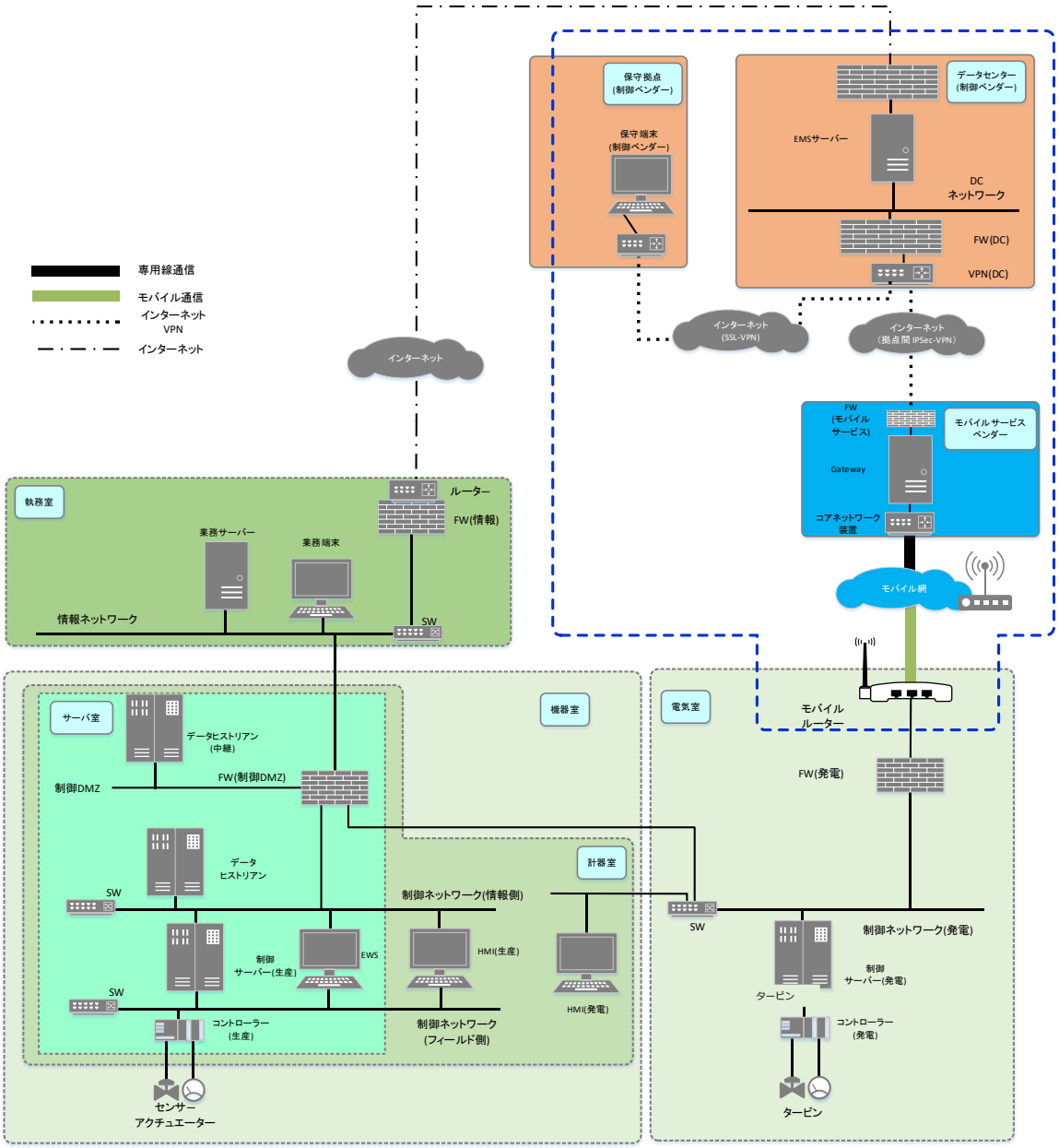


図 1-8 モバイル閉域網と VPN を組み合わせた外部接続構成

この構成では、モバイルルーターと SIM、ベンダーデータセンター側の VPN サーバーと接続する Gateway サービス（Gateway は VPN クライアント機能を兼ねる）が「モバイル閉域網接続サービス」としてモバイルサービスベンダーから提供されている。

制御システム側の外接点がインターネットに公開されていないため、インターネットから直接制御システムが脅威に晒されず、制御システム側にモバイルルーターを設置すれば外部サービスと接続可能となる手軽さがある。

しかし、外部サービス経由で不正アクセスされるリスクは完全には無くならないことに留意が必要である。例えば、「モバイル閉域網接続サービス」のモバイルルーターは、設定やファームウェア更新がモバイルサービスベンダーのシステム経由で実施する機能が提供されていることがある。また、このような機能を悪用したサイバー攻撃事例[5]が報告されている。不要であるならば、モバイルルーターの遠隔制御機能を無効にすることが望ましい。

また、本構成例ではモバイルルーターと制御システムをファイアウォール（FW）で分離し、必要最小限の通信のみを制御システムが受け入れる構成としているが、「モバイル閉域網接続サービス」にはファイアウォールの費用は含まれないので、ファイアウォールが必要な場合は事業者側が追加で用意する必要がある。制御システム事業者がファイアウォールを追加で用意するかどうかは、外部サービス経由でのサイバー攻撃によるリスクについて、本書を参考にセキュリティリスク分析を実施して判断して欲しい。

外部委託業者管理の観点（サプライチェーンの観点）では、ベンダーデータセンターと事業者とのネットワーク接続の間に、モバイルサービスベンダーがある。「1.5.2.1 インターネット VPN による外部接続構成」と比較して意識すべき外部委託業者が1社以上[6]増加することに留意する必要がある。

[5] IPA: 【事例 10】2022 年 衛星通信網へのサイバー攻撃の事例
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/incident_10.pdf

[6] モバイルネットワークサービスが MVO・MVNO が提供されるものかによって変化し、MVO 単体のケースと MVO・MVNO などによるケースとネットワーク構成は多様なものとなる。ただし、本書は制御システムのセキュリティリスク分析が主題のため、ネットワークサービスのセキュリティ分析については深堀しないものとする。

1.5.3. システムの構成資産（機器・ネットワーク）

以降、本編では「1.5.2.1. インターネット VPN による外部接続構成」を分析対象システムとして説明をしている。構成資産の概要を以下に示す(表 1-2)。

表 1-2 分析対象システムの資産概要 (1/2)

資産名	概要	分析対象 ○：対象 △：侵入口として分析 —：対象外
情報ネットワーク	事業者の OA 端末が接続されている情報ネットワーク。情報ネットワークと制御ネットワークの間には FW（制御 DMZ）があり、制御 DMZ 経由でデータフローがある。	—
業務サーバー	制御 DMZ 上のデータヒストリアン(中継)とデータフローがあるサーバー。	—
業務端末	業務サーバーに蓄積されたデータヒストリアンのデータを参照可能。また、発電システムの発電量を参照・加工するために、外部サービスの EMS サーバーを参照する。	—
FW(制御 DMZ)	情報ネットワークと制御ネットワークを分離する境界装置。	○
制御 DMZ	情報ネットワークと制御ネットワーク間のデータを受け渡すためのネットワーク。	○
データヒストリアン(中継)	制御 DMZ に設置されたデータ転送サーバー。データヒストリアンのデータを業務サーバーに受け渡しをする。	○
データヒストリアン	制御システムのヒストリアンデータを収集・蓄積するデータベースシステム。	○
制御ネットワーク(情報側)	主に、HMI・EWS・制御サーバーのヒストリアンデータをデータヒストリアンに転送する用途で利用される。	○
制御ネットワーク(フィールド側)	生産システムのコントローラーと HMI・EWS・制御サーバー間でやりとりされるデータを転送する用途で利用される。このネットワークは冗長化されている。	○
制御サーバー(生産)	生産システムのコントローラー(生産)からのプロセス値をうけとり、データヒストリアンに転送する。冗長化されている。	○
EWS	生産システムのエンジニアリングワークステーション。コントローラーのエンジニアリングデータを変更する。冗長化されている。	○
HMI(生産)	生産システムのヒューマンマシンインターフェース（監視制御端末）。冗長化されている。	○
コントローラー(生産)	生産システムの生産設備を制御する機能を持つ。冗長化されている。	○
センサー・アクチュエイター	製造設備に関係するセンサー群とアクチュエイター群をさす。	—

表 1-2 分析対象システムの資産概要 (2/2)

資産名	概要	分析対象 ○:対象 △:侵入口として分析 —:対象外
制御サーバー(発電)	コントローラー(発電)から各種プロセスデータやアラートを受信し、発電設備の状況を表示する機能を持つ。また、発電量を外部サービスへ送信する一方、ベンダーの監視端末から遠隔保守可能な機能がある。冗長化されている。	○
HMI(発電)	発電設備のヒューマンマシンインターフェース(監視制御端末)。冗長化されている。	○
コントローラー(発電)	発電設備(ガスタービン)の制御を行い、各種プロセスデータを受信する。冗長化されている。	○
タービン	生産システムの副生ガスを燃料として発電をする。	○
制御ネットワーク (発電)	HMI(発電)が制御サーバー(発電)と接続し、コントローラー(発電)の監視制御を実施するためのネットワーク。	○
FW(発電)	インターネットと制御ネットワーク(発電)間の境界装置。	○
VPN(発電)	インターネット用ルーター兼 VPN 装置。VPN は、発電システム納入ベンダーが提供する外部サービスと、納入ベンダーの保守拠点とインターネット VPN で接続する。	○
ONU	事業者の電気室に設置されたインターネット光回線の終端装置。システム構成図では非表示。	—
EMS サーバー	発電システムを納入した制御ベンダーが保有するデータセンターに設置されたサーバー上で運用されている Web アプリケーション兼データベースサーバー。マルチテナントで運用されている。セキュリティ状況は不明。 発電システムの各種情報を収集・分析し、電力量のピークシフトとタービン駆動用熱エネルギー供給の最適値を提示する機能がある。	△
FW(DC)	発電システムを納入した制御ベンダーが保有するデータセンターに設置された FW。セキュリティ状況は不明。	△
VPN(DC)	発電システムを納入した制御ベンダーが保有するデータセンターに設置された VPN。事業者の電気室とインターネット VPN で接続している。セキュリティ状況は不明。	△
保守端末 (ベンダー保守拠点)	発電システムを納入した制御ベンダーの保守拠点にある保守端末。セキュリティ状況は不明。	△
VPN (ベンダー保守拠点)	発電システムを納入した制御ベンダーの保守拠点にある VPN。事業者の電気室とインターネット VPN 接続をしている。セキュリティ状況は不明。	△

1.6. リスク分析の流れとアウトプット

- **本書の前提**

  本書は、ガイド本編で説明されているリスク分析手法の内容とリスク分析結果の活用方法を理解していることを前提とする。また、本書ではリスク分析の手順の詳細はガイド本編を参照する記載としており、文中の青字斜体の章節項番号(*x.y.z*)と図表番号(*図 x-y*、*表 x-y*)はガイド本編を参照していることを意味している。

- リスク分析の流れとアウトプット

  リスク分析の流れと2～5章で説明する実施例のアウトプットを、図 1-9に示す。(図 1-9は、ガイド本編の*図 2-2* に本書で示すアウトップットを数字(①～⑱)で示したものである)図中の  はリスク分析者が作成するアウトプットを意味し、  はガイド本編に示された例をカスタマイズして得られるアウトプットを意味している。

- アウトプットの例示と解説

  本書でのリスク分析は「リスク分析の流れ」に沿って実施し、各ステップではリスク分析を完了させるための中間的な資料(アウトプット)を作成する。それらアウトプットをリスク分析の流れに沿って例示する。

表 1-3 アウトプット一覧表

2. リスク分析のための事前準備				
本書見出し	アウトプット		アウトプットの利用	ガイド本編
2.1.	①	資産一覧	資産/事業被害ベース	*3.1.5. 表 3-10*
2.2.	②	システム構成図	資産/事業被害ベース	*3.2.3. 図 3-8*
2.3.①	③	データフローマトリックス	資産/事業被害ベース	*3.3.1. 表 3-11*
2.3.②	④	データフロー図	資産/事業被害ベース	*3.3.2. 図 3-10*
2.4.	⑤	資産の重要度の判断基準	資産ベース	*4.2.2. 表 4-5*
2.5.	⑥	各資産に対する重要度一覧	資産ベース	*4.2.3. 表 4-9*
2.6.	⑦	事業被害レベルの判断基準	事業被害ベース	*4.3.2. 表 4-11*
2.7.	⑧	事業被害及び各事業被害に対する事業被害レベル一覧	事業被害ベース	*4.3.3. 表 4-12*
2.8.	⑨	脅威レベルの判断基準	資産/事業被害ベース	*4.4.5. 表 4-21～表 4-24*
3. 資産ベースのリスク分析				
本書見出し	アウトプット			ガイド本編
3.1.	⑩	脅威レベルまとめ表		*5.3.4 表 5-5*
3.2.	⑪	資産ベースのリスク分析シート		*5.1. 図 5-3、図 5-4*
3.3.①	⑫	脆弱性レベルまとめ表		*5.5.3 表 5-10*
3.3.②	⑬	リスク値まとめ表		*5.6.3 表 5-13*
4. 資産ベースのリスク分析				
本書見出し	アウトプット			ガイド本編
4.1.	⑭	攻撃シナリオ一覧		*6.2.2. 表 6-6*
4.4.	⑮-1	攻撃ルート一覧		*6.5.1. 表 6-11～表 6-12*
4.4.	⑮-2	攻撃ルート図		*6.5.1. 図 6-10*
4.5.	⑯	事業被害ベースのリスク分析シート		*6.1.3 図 6-5、図 6-6*
4.6.	⑰	リスク値まとめ表		*6.11.3. 図 6-32*
5. リスク分析の活用				
本書見出し	アウトプット			ガイド本編
5.	⑱	制御システムのリスク分析結果		*7 章*

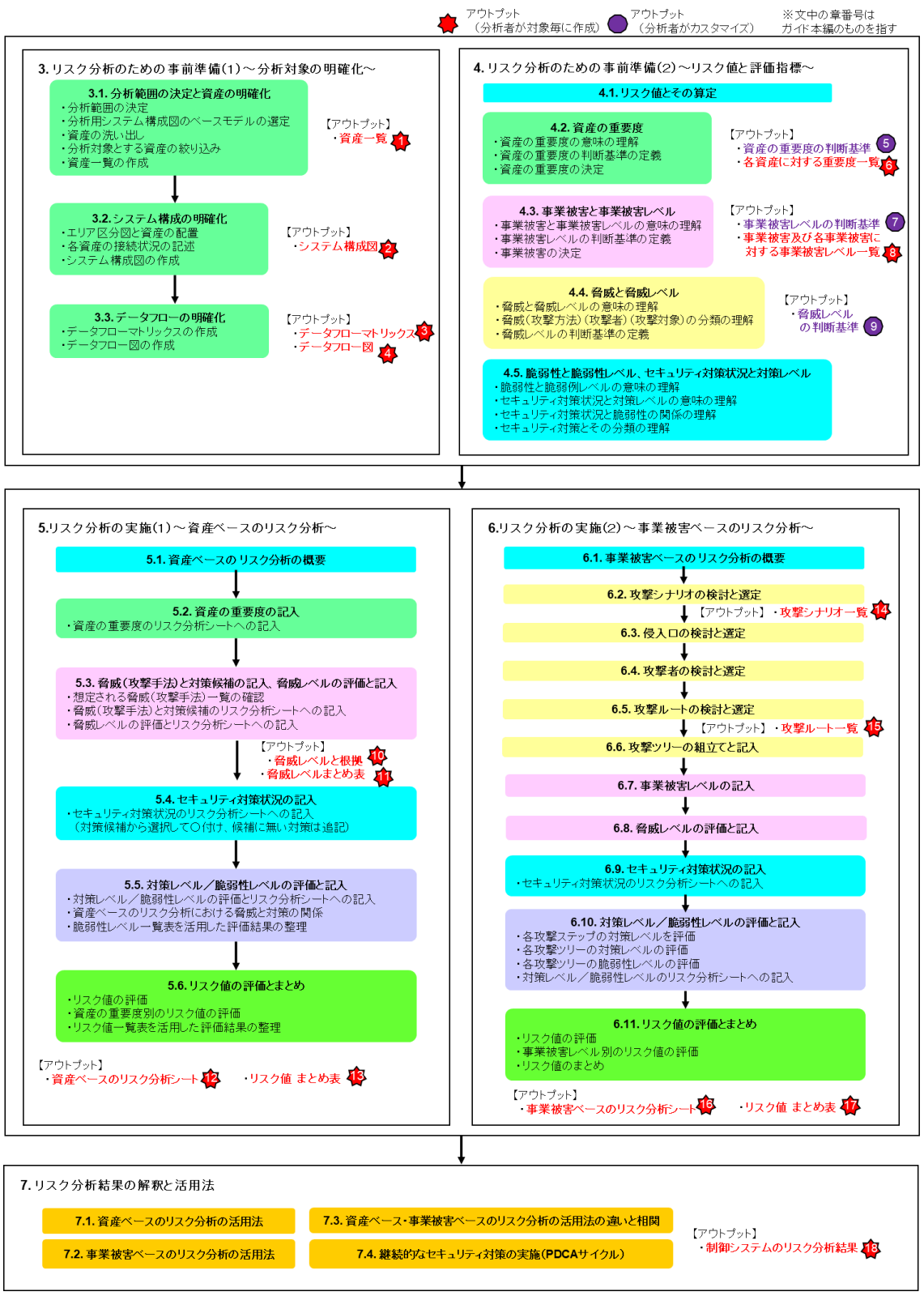


図 1-9 リスク分析の流れと成果物

2. リスク分析のための事前準備

リスク分析のための事前準備作業で作成するアウトプットを以下に示す(表 2-1)。

表 2-1 事前準備作業のアウトプット一覧

本書見出し	アウトプット	アウトプットの利用	ガイド本編
2.1.	資産一覧	資産/事業被害ベース	*3.1.5. 表 3-10*
2.2.	システム構成図	資産/事業被害ベース	*3.2.3. 図 3-8*
2.3.①	データフローマトリックス	資産/事業被害ベース	*3.3.1. 表 3-11*
2.3.②	データフロー図	資産/事業被害ベース	*3.3.2. 図 3-10*
2.4.	資産の重要度の判断基準	資産ベース	*4.2.2. 表 4-5*
2.5.	各資産に対する重要度一覧	資産ベース	*4.2.3. 表 4-9*
2.6.	事業被害レベルの判断基準	事業被害ベース	*4.3.2. 表 4-11*
2.7.	事業被害及び各事業被害に対する事業被害レベル一覧	事業被害ベース	*4.3.3. 表 4-12*
2.8.	脅威レベルの判断基準	資産/事業被害ベース	*4.4.5. 表 4-21～表 4-24*

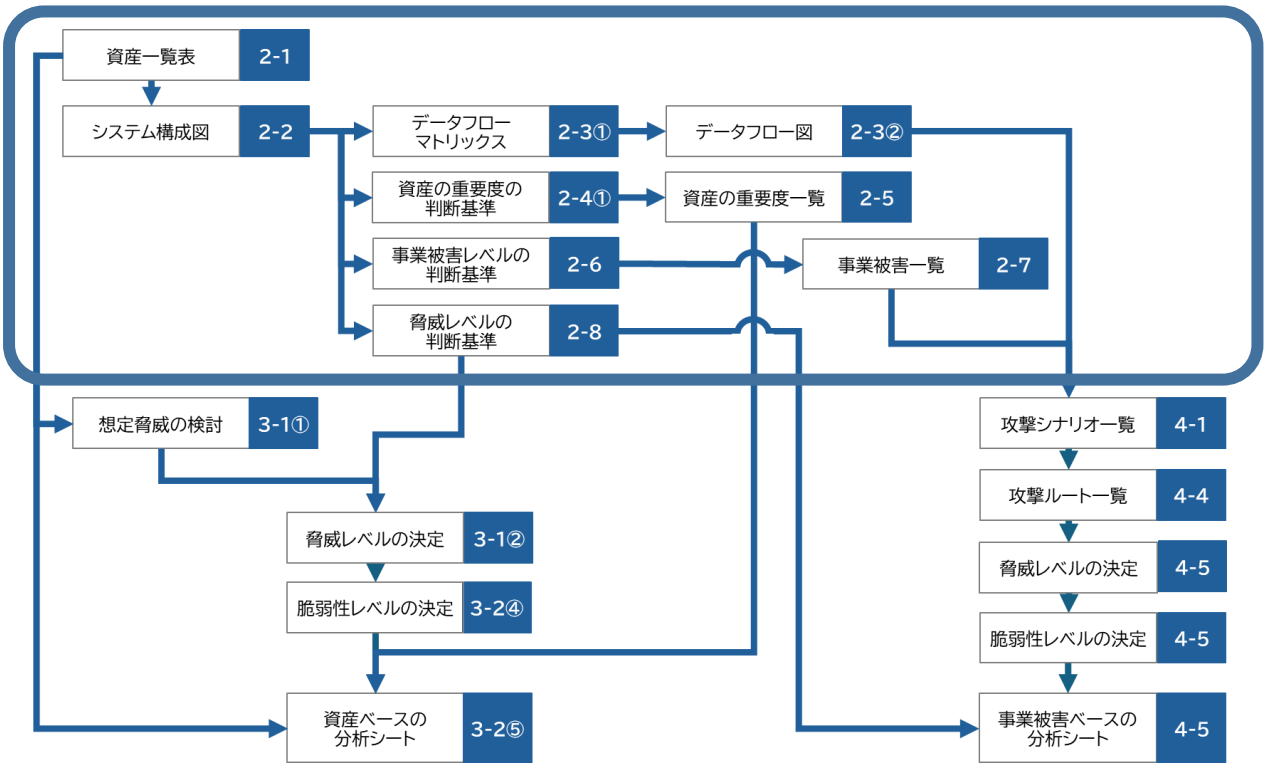


図 2-1 事前準備作業の流れ

事前準備作業における共通事項について以下にまとめる。

（1）リスク分析に参加・関連する部門・外部組織について

制御システムのセキュリティリスク分析は、リスク分析対象となる制御システム部門が中心となって実施することが多いが、リスク分析に必要な情報を制御システム部門が全て持っているとは限らない。情報システム部門など制御システムの関連組織、制御システムの導入・保守ベンダーなどの外部組織との協力も必要となることが多い。

特に、資産一覧・システム構成図・データフローなど「リスク分析の事前準備作業のためのアウトプット」の作成においては、制御システムの関連組織との連携、外部組織への問い合わせが発生することが多い。

ここでは、本書におけるリスク分析作業での自組織と外部組織の関わりを示す。

●自組織の関連組織

・制御システム部門（制御システムの設計運用部門）

本実施例におけるリスク分析の実施チーム[7]である。

制御システムの設計運用部門は、制御システムの資産とネットワークを運用管理している。

・現場部門（保守・設備管理）

制御システムの運用部門は、制御システムの資産やネットワークが置かれた区画の物理的なセキュリティや、制御システムの運用について責任を持つ。

リスク分析の過程では、制御システムの物理的なセキュリティや運用的なセキュリティについて、確認を行う。

・情報システム部門

情報システム部門は、情報システムの資産とネットワーク、情報システムと制御システムの接点となるネットワーク（DMZ）と資産を運用管理している。

リスク分析の過程では、情報システムと DMZ の資産やネットワークについて、データフローやセキュリティ状況の詳細について、確認を行う。

7 リスク分析実施チームは、事業者全体のセキュリティ推進・責任部門である情報システム部門が主体となる場合もある。また、リスク分析実施チームは情報システム部門と制御システム部門の混合チームで編成されることも多い。

・制御システムの責任者（または経営層）

リスク分析チームは、制御システムのセキュリティリスクマネジメントの責任者（経営層）に対して、制御システムのリスクアセスメント作業の一部であるリスク分析の必要性を説明し、リスクアセスメント作業への関連部門からの支援の確約の承認を得る。リスク分析チームは、組織の事業継続計画にある事業継続リスクを念頭に事業被害を設定し、リスク分析とリスク評価を行う。リスク評価結果を制御システムの責任者（または経営層）に報告し、リスク対応について判断を仰ぐ。

●外部組織

リスク分析に必要な情報をベンダーに問い合わせる場合、ベンダーが事業者との保守サポートの範囲内で対応可能か、もしくは別途費用が必要となるか対応が分かれる。リスク分析の立ち上げ時に、ベンダーに費用を問い合わせておくとよい。

・制御ベンダー（構築ベンダー・制御機器ベンダー・制御ネットワークベンダー）

本書では、生産システムの構築・保守ベンダーと発電システムの構築・保守ベンダーの 2 社が関連する。

リスク分析の過程では、制御システムの資産やネットワークについて、データフローやセキュリティ状況の詳細について、確認を行う。

また、リスク分析実施後にリスク低減策を検討する際は、制御システムの資産やネットワークに追加検討するセキュリティ低減策について、制御ベンダーがサポートしているか確認が必要となることもある。

・外部サービス提供ベンダー

本書の外部サービスは、下記の 2 つが該当する。

・事業者の発電システムへの遠隔監視サービスと遠隔保守サービス

・モバイル閉域網のネットワークサービスベンダー（付録 C のみ）

リスク分析の過程では、外部サービスのネットワーク機器について、データフローやセキュリティ状況の詳細について、確認を行う。

リスク分析において調査項目とそれを管轄する部門ならびに関連する外部組織を以下の表にまとめた。

表 2-2 管轄部門のまとめ（例）

#	調査項目	管轄部門	外部組織（ベンダー）
1	生産システム	制御システムのシステム設計部門	生産システム導入ベンダー
2	発電システム	制御システムのシステム設計部門	発電システム導入ベンダー
3	制御システムの物理的セキュリティや運用的セキュリティ	制御システムの運用部門	導入ベンダー
4	DMZ	情報システム部門 制御システム部門	（問い合わせ不要）
5	情報システム	情報システム部門	（問い合わせ不要）
6	外部サービス：遠隔監視サービスと遠隔保守サービス	制御システム部門	遠隔監視サービスベンダー 遠隔保守サービスベンダー
7	外部サービス：モバイル閉域網のネットワークサービスベンダー	制御システム部門	ネットワークサービスベンダー

(2) 外部サービス(外部委託業者)のセキュリティ

リスク分析を実施する上で、外部サービスのシステム構成、機能、運用、セキュリティを含めて外部サービスの契約内容を把握する必要がある。例えば、インターネットからの不正アクセスに対するセキュリティ対策状況、システム(特に運用セグメント)のインターネットや社内情報ネットワークとの分離状況、運用セグメントの物理的・運用的なセキュリティ対策状況等を把握する。外部サービスの契約書やセキュリティティ規約から判断する、または外部サービスに問い合わせるなどして情報を収集し、外部サービス経由で事業者の制御システムにサイバー攻撃をうける脅威を評価していく。

ただし、外部サービスベンダーのセキュリティについて、契約書やセキュリティ規約以上の情報が得られない場合もあるので留意する必要がある。その場合、外部サービス経由でのサイバー攻撃の脅威をどう評価するかが重要なポイントとなる。セキュリティリスクがあると判断する場合は、外部サービスの変更や事業者の制御システム側へのセキュリティ対策の追加などを実施していくことになるだろう。

2.1. 資産一覧

【作業 2.1①】分析対象システムにおける資産一覧表を作成すること。

- ガイド本編 *表 3-10* を参考に、資産の分類、機能、設置場所、接続先 NW、管理ポートの有無、ベンダー、OS、プロトコルを明記すること。

【アウトプット 2.1①】

資産一覧表を次項に示す(表 2-3)。

【解説 2.1①】

- 詳細リスク分析を行う上で必要となる情報の分析に利用しやすい形への整理

  詳細リスク分析を行う上で必要となる情報を資産一覧表にまとめることを推奨する。これらをどこまで精度良く実施するかで、後の工程での工数、分析精度に大きく影響する。

  ただし、資産一覧表に全て記載する必要はなく、項目によっては既存のドキュメントを参照する方式でも構わない。また、分析を進めながら必要となった事項を都度資産一覧表に追加・詳細化しても構わない。

- 接続先ネットワーク(NW)の明確化

  資産が通常のネットワーク経路とは別の管理ネットワークや監視ネットワークに接続されている場合がある。これらのネットワークは自社のネットワーク図に記載されていない場合もあるため、明確化が必要である。

- 資産一覧表作成に必要な調査工数の配慮

  最新の資産一覧表を整備されていない事業者においては、制御システムの運用者や構築業者、ベンダーへのヒアリングが必要になる場合がある。この作業はそれなりの工数を伴うため、事前準備の期間を長めに用意する必要があることを留意すること。

表 2-3 資産一覧表 (1/3)

No		1	2	3	4	5	6
資産名		FW(制御DMZ)	制御DMZ	データヒストリアン（中継）	制御ネットワーク（情報側）	データヒストリアン	制御サーバー（生産）
資産名（略称）				DH（中継）	制御NW(情)	DH	
資産種別	情報機器			○		○	○
	制御機器						
	ネットワーク資産（通信制御機能有）	○					
	ネットワーク資産（通信制御機能無）		○		○		
資産の持つ機能	入出力			○		○	○
	データ保存			○		○	○
	コマンド発行						○
	ゲート	○	○		○		
回線種類			LAN		LAN		
設置場所		サーバ室	サーバ室	サーバ室	サーバ室	サーバ室	サーバ室
接続先NW	情報NW	○					
	制御DMZ	○	○	○			
	制御NW(情)	○			○	○	○
	制御NW(フ)						○
	フィールドNW						
	制御NW(発電)	○					
	インターネット						
	その他						
管理ポートの接続先		情報NW	－	－	－	－	－
操作I/Fの有無		－	－	○	－	○	○
USBポート／通信I/Fの利用		USB	－	USB	－	USB	－
媒体・機器接続の定常運用の有無		有	－	有	－	有	－
無線機能の有無		－	－	－	－	－	－
定常稼働、非定常稼働		定常	定常	定常	定常	定常	定常
データの種類と経路		データフローマトリックスに記載					
構築ベンダー／機器メーカー		AR社／YT社	AR社／YT社	ZI社／JO社	ZI社／ZI社	ZI社／JO社	ZI社／ZI社
OSの種類／バージョン		独自	独自	Windows系	独自	Windows系	Windows系
使用するプロトコル		IP	IP	IP	IP	IP	IP／独自

表 2-3 資産一覧表 (2/3)

No		7	8	9	10	11	12
資産名		制御ネットワーク（フィールド側）	コントローラー（生産）	HMI(生産)	EWS	制御ネットワーク（発電）	制御サーバー（発電）
資産名（略称）		制御NW(フ)				制御NW(電)	
資産種別	情報機器			○	○		○
	制御機器		○				
	ネットワーク資産（通信制御機能有）						
	ネットワーク資産（通信制御機能無）	○				○	
資産の持つ機能	入出力		○	○	○		○
	データ保存		○	○	○		○
	コマンド発行		○	○	○		○
	ゲート	○				○	
回線種類		LAN				LAN	
設置場所		サーバ室	サーバ室	計器室	サーバ室	電気室	電気室
接続先NW	情報NW						
	制御DMZ						
	制御NW(情)			○	○		
	制御NW(フ)	○	○	○	○		
	フィールドNW						
	制御NW(発電)					○	○
	インターネット						
	その他						コントローラー(発電)
管理ポートの接続先		－	－	－	－	－	－
操作I/Fの有無		－	○	○	○	－	○
USBポート／通信I/Fの利用		－	－	USB	USB	－	－
媒体・機器接続の定常運用の有無		－	－	有	有	－	－
無線機能の有無		－	－	－	－	－	－
定常稼働、非定常稼働		定常	定常	定常	定常	定常	定常
データの種類と経路		データフローマトリックスに記載					
構築ベンダー／機器メーカー		ZI社／ZI社	ZI社／MR社	ZI社／ZI社	GA社／GA社	GA社／GA社	GA社／GA社
OSの種類／バージョン		独自	独自	Windows系	Windows系	独自	Windows系
使用するプロトコル		IP／独自	独自	IP／独自	IP／独自	IP	IP／独自

表 2-3 資産一覧表(3/3)

No		13	14	15	16	17	18
資産名		HMI(発電)	コントローラー（発電）	FW(発電)	VPN（発電）	業務端末	業務サーバー
資産名（略称）							
資産種別	情報機器	○				○	○
	制御機器		○				
	ネットワーク資産（通信制御機能有）			○	○		
	ネットワーク資産（通信制御機能無）						
資産の持つ機能	入出力	○	○			○	○
	データ保存	○	○			○	○
	コマンド発行	○	○			○	
	ゲート			○	○		
回線種類					Internet		
設置場所		計器室	電気室	電気室	電気室	執務室	執務室
接続先NW	情報NW					○	○
	制御DMZ						
	制御NW(情)						
	制御NW(フ)						
	フィールドNW						
	制御NW(発電)	○		○			
	インターネット				○		
	その他		制御サーバー（発電）	VPN(発電)	FW(発電)		
管理ポートの接続先		－	－	コンソールポート	コンソールポート	－	－
操作I/Fの有無		○	－	－	－	○	○
USBポート／通信I/Fの利用		USB	－	－	－	－	－
媒体・機器接続の定常運用の有無		有	－	－	－	－	－
無線機能の有無		－	－	－	－	－	－
定常稼働、非定常稼働		定常	定常	定常	定常	定常	定常
データの種類と経路		データフローマトリックスに記載					
構築ベンダー／機器メーカー		GA社／GA社	GA社／GA社	AR社／YT社	GA社／RT社	D社／V社	D社／V社
OSの種類／バージョン		Windows系	独自	独自	独自	Windows系	Windows系
使用するプロトコル		IP	独自	IP	IP	IP	IP

このページは空白です。

2.2. システム構成図

【作業 2.2】分析対象システムのシステム構成図を作成すること。

- ガイド本編 *図 3-8* を参考にすること。
- システム構成図で、ネットワーク接続状況と資産の物理的な設置場所が把握できるようにすること。

【アウトプット 2.2】

システム構成図を(図 2-2)に示す。

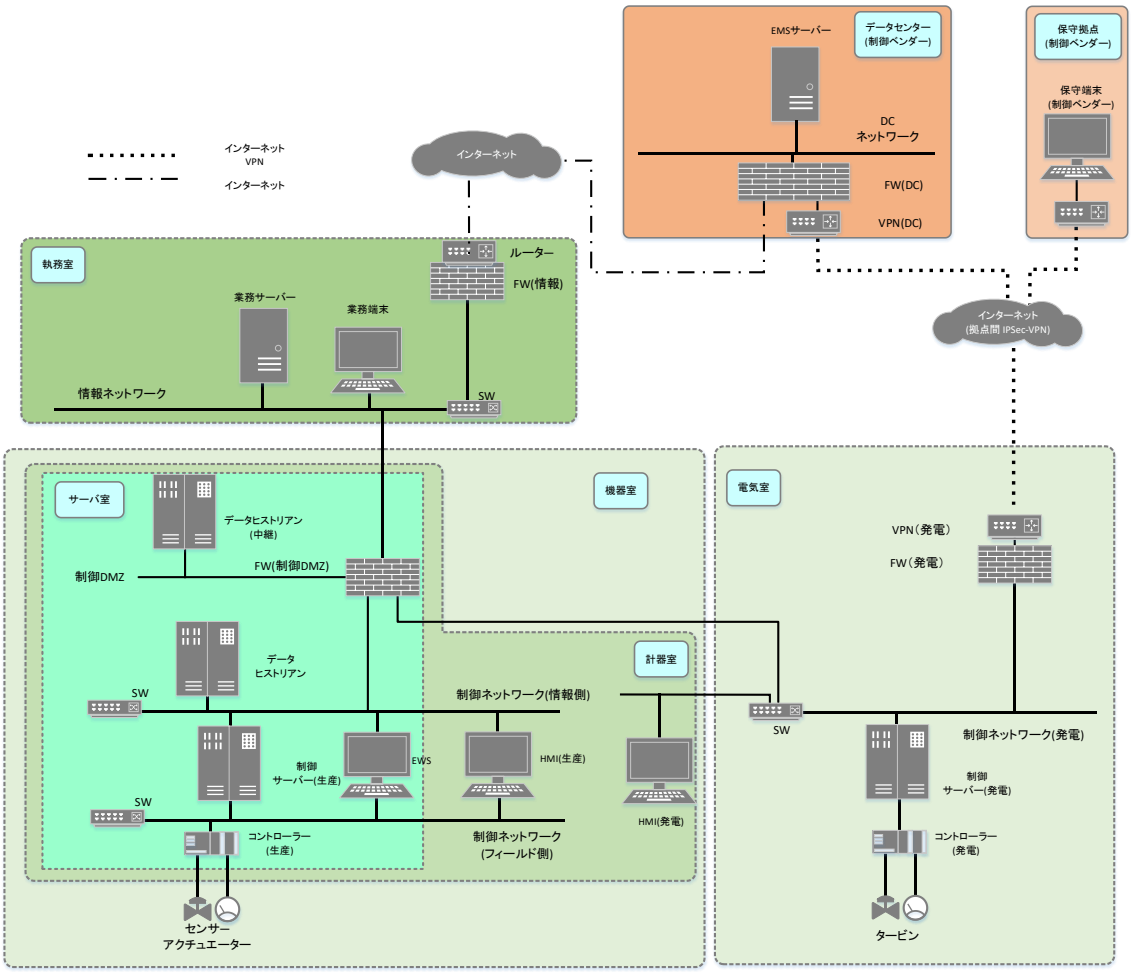


図 2-2 システム構成図

【解説 2.2】

- 外部サービスとの接続を含めた制御システムの全体構成図を作成

  制御システムのネットワーク図は、生産システムや発電システムなど担当部門ごとに図面が分かれているケースがあり、この場合生産システムと発電システムを統合した全体構成図が存在せず、リスク分析の事前準備フェーズで全体構成図の作成が必要になる。初めて作る場合は、工数がかかる作業となる。

  また、外部サービスとの接続については、通信先のホスト名や IP アドレスのみの把握にとどまり、詳細が不明であるケースもある。
  よって、必要であれば外部サービスを提供しているベンダーにヒアリングを行い、外部サービスの接続を明確にしていく必要がある。

- 外部サービスとのネットワークセキュリティの明確化

  外部サービスとの接続に利用しているネットワークについて、事業者側でグローバル IP を持ってサーバーをインターネットに公開しているか、VPN や（モバイル）閉域網を利用しているか、VPN であれば事業者側は VPN サーバーを公開しているか把握する。また、事業者と外部サービスとのネットワークでどの区間が VPN・閉域網の区間なのかを把握する。
  例えば、「1.5.2.2 モバイル閉域網と VPN を組み合わせた外部接続構成」では、事業者と外部サービスとのネットワーク全てが、モバイル閉域網と認識されてしまいかねないが、事業者と外部サービスとの間には「閉域網と VPN を中継するネットワークベンダー」が存在する。ネットワークベンダーの存在を把握してシステム構成図を作成し、後工程のリスク分析を実施することが必要である。

- 実際のネットワーク構成とのずれ

  事業者が保有している制御システム導入・変更時の図面は、実際の（最新の）ネットワーク構成とずれていることがある。また、機器の管理用のネットワークの存在が不明であることもある。このため、セキュリティ上重要な資産や外接点（外部ネットワークや情報ネットワーク、他システムとの接点）は現状視察やネットワークキャプチャデータの採取などをして、現状を正しく把握することが望ましい。

2.3. データフローマトリックス

【作業 2.3①】分析対象システムの資産間で送受信されるネットワークデータを、データフローマトリックス表にまとめること。

- 表のフォーマットはガイド本編 *表 3-11* を参考すること。

【アウトプット 2.3①】

データフローマトリックスを以下に示す（表 2-4）。

表 2-4 データフローマトリックス

受信側 / 送信側	経路	EMSサーバー	保守端末	制御サーバー（発電）	HMI(発電)	コントローラー(発電)	データヒストリアン（中継）	データヒストリアン	HMI(生産)	EWS	制御サーバー（生産）	コントローラー(生産)	業務端末	業務サーバー
EMSサーバー	インターネット													
保守端末	インターネット	参照		エンジニアリング										
制御サーバー(発電)	制御NW（発電）	プロセス値						プロセス値						
	コントローラー(発電)					制御コマンド								
HMI(発電)	制御NW（発電）			参照 制御コマンド										
コントローラー(発電)	制御サーバー(発電)			プロセス値										
データヒストリアン（中継）	制御DMZ													プロセス値
データヒストリアン	制御NW(情)						プロセス値							
HMI(生産)	制御NW(情)													
	制御NW(フ)											参照 制御コマンド		
EWS	制御NW(情)													
	制御NW(フ)											エンジニアリング		
制御サーバー(生産)	制御NW(情)							プロセス値						
	制御NW(フ)											制御コマンド		
コントローラー(生産)	制御NW(フ)										プロセス値			
業務端末	情報NW	参照												参照
業務サーバー	情報NW													

【作業 2.3②】分析対象システムの資産間で送受信されるデータを、データフロー図にまとめること。

- ガイド本編 *図 3-10* を参考すること。
- システム構成図の上にデータフローを追記すること。

【アウトプット 2.3②】

分析対象システムのデータフロー図を以下に示す(図 2-3)。

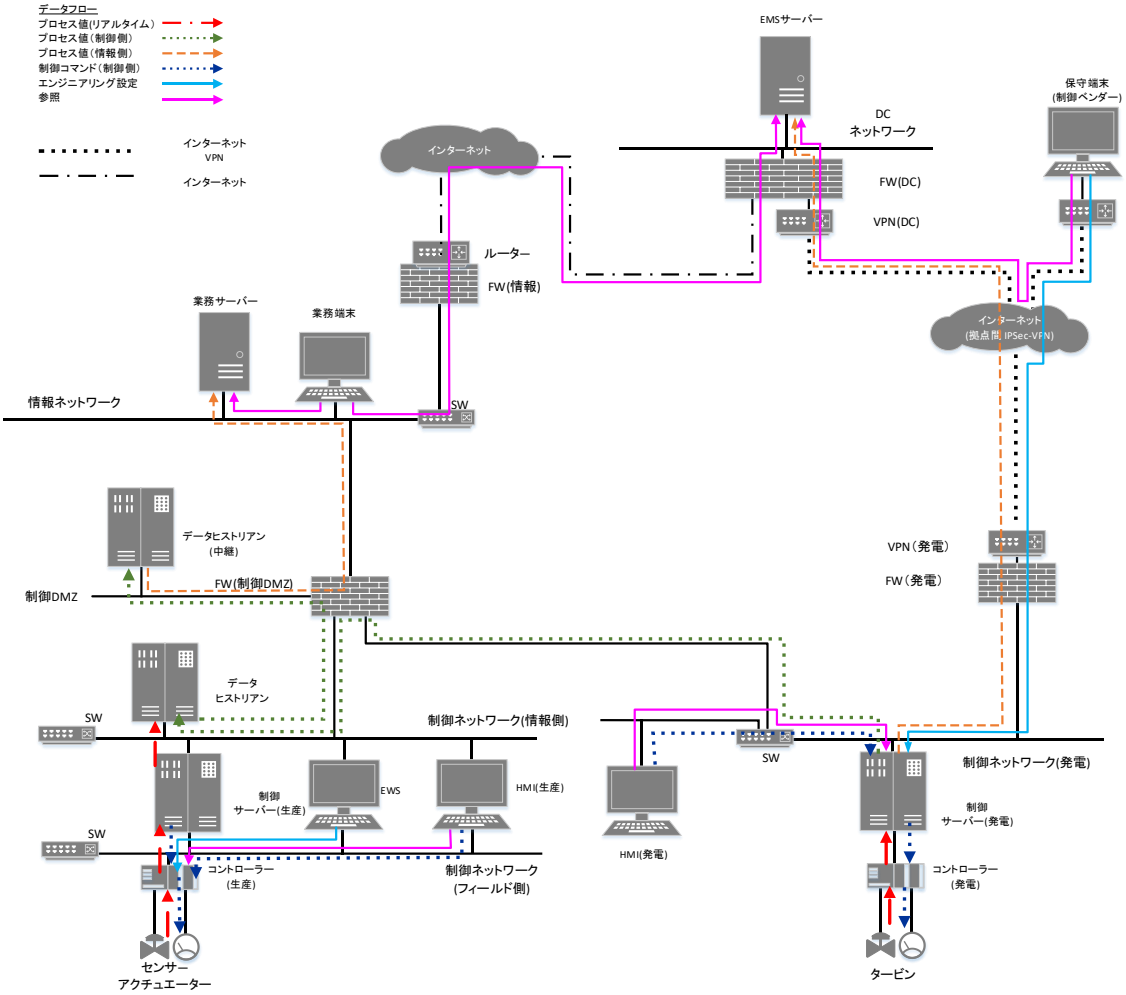


図 2-3 データフロー図(全体)

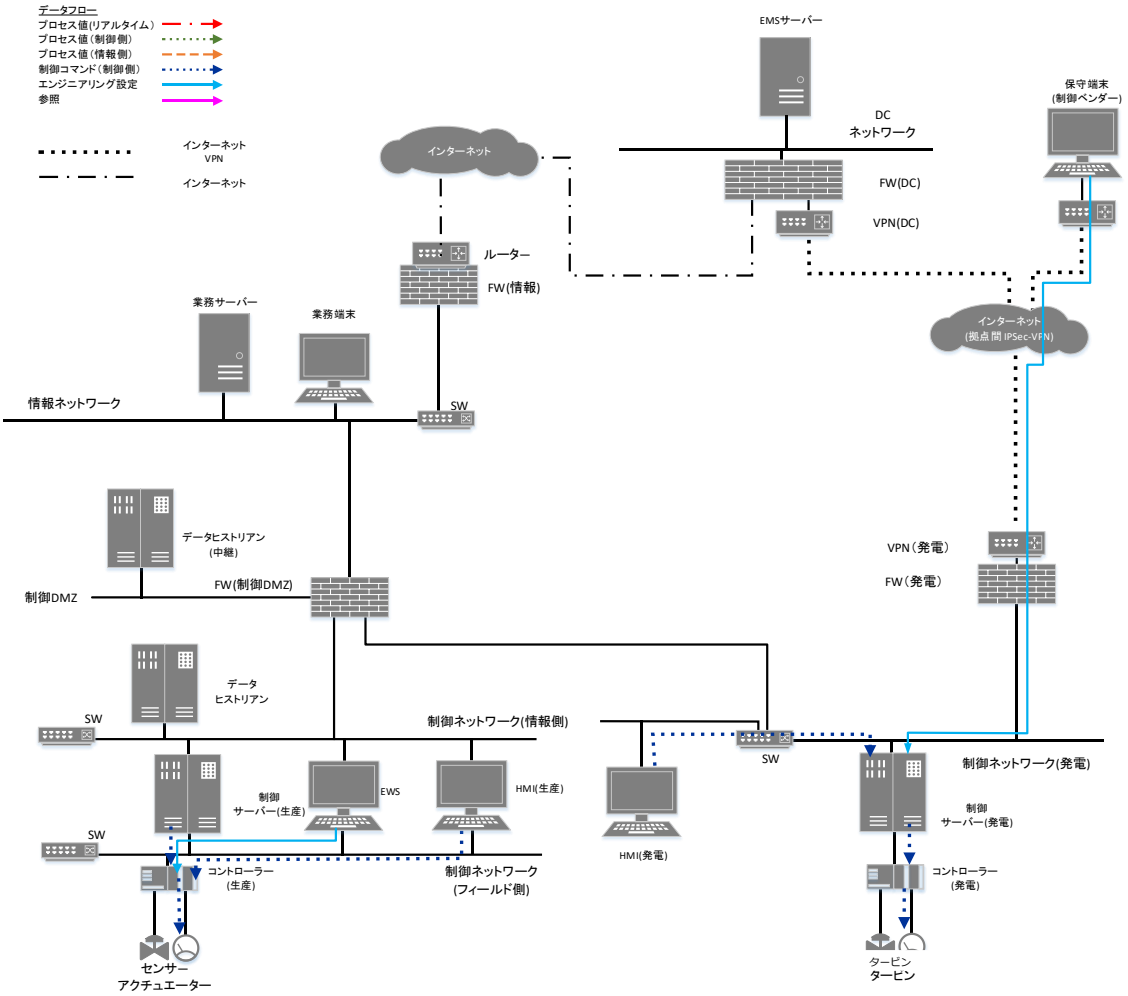


図 2-4 データフロー図(制御・エンジニアリング)

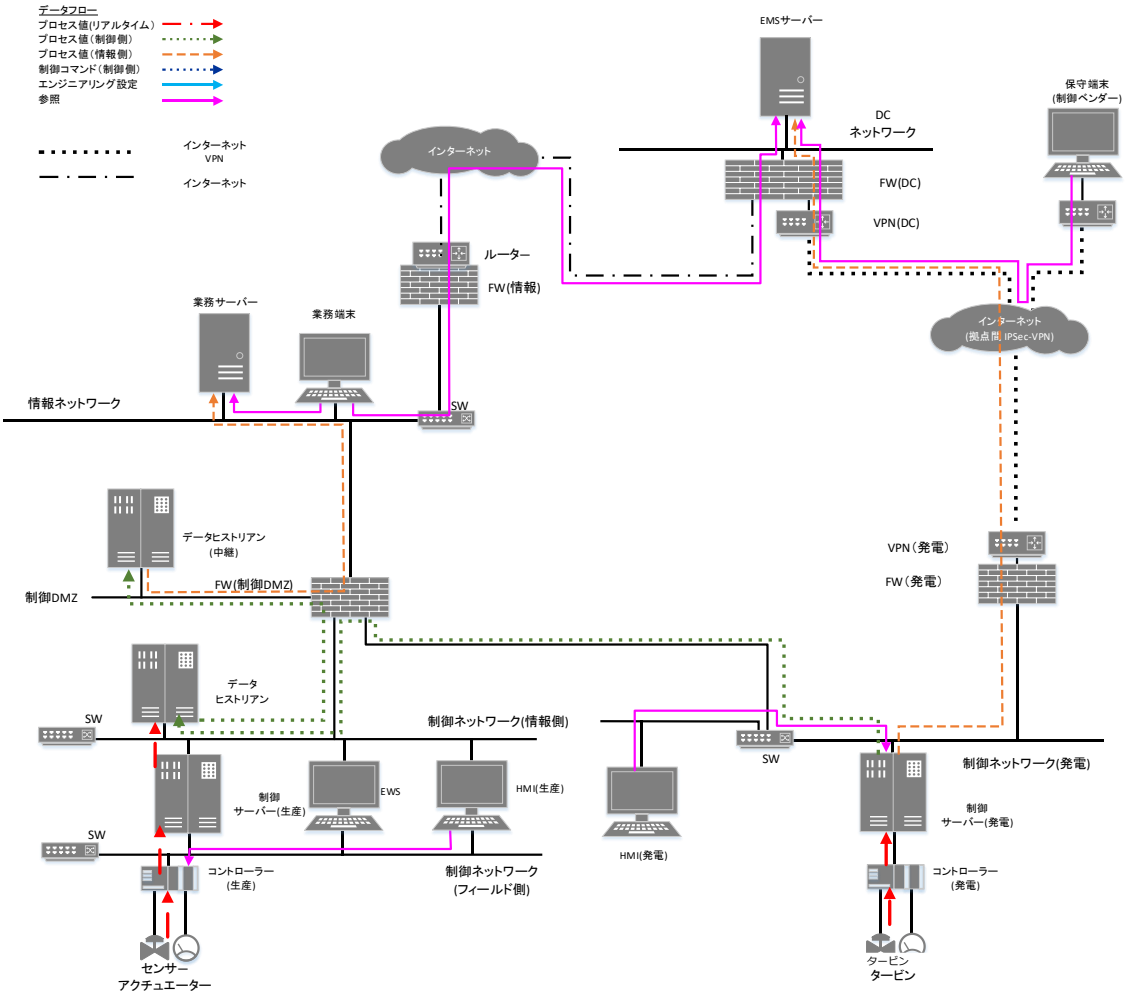


図 2-5 データフロー図(プロセスデータ・参照)

2.4. 資産の重要度の判断基準

【作業 2.4】資産の重要度を 3 段階で評価する場合の判断基準(被害大:3＞被害中:2＞被害小:1)を作成すること。

- ガイド本編 *表 4-5* を参考にして、事業者の事業特性に応じた明確な数値を評価値の境界値として定義すること。また、境界値の根拠をあわせて記載すること。

【アウトプット 2.4】

資産の重要度の判断基準例を以下に示す(表 2-5)。

表 2-5 資産の重要度の判断基準の定義例

評価値	判断基準
3	・資産が失われた、もしくは不正に操作された場合、事業上の被害大となる。 －システムが長期間停止(2 週間以上停止)する恐れがある。 －システムが制御不能になり周辺環境の破壊・汚染発生し、環境基準を逸脱する恐れがある。
2	・資産が失われた、もしくは不正に操作された場合、事業上の被害中となる。 －システムが一定期間停止(3 日～2 週間未満停止)する恐れがある。 －システムの停止により手動での製造工程を維持する必要がある。 －システムが制御不能になり周辺環境の破壊・汚染発生し、社内基準を逸脱する恐れがあるが、環境基準を逸脱する恐れはない。
1	・資産が失われた、もしくは不正に操作された場合、事業上の被害小となる。 －システムが一定期間停止(3 日未満)する恐れはない。 －システムが制御不能になることで制御システムの損傷が発生する恐れはない。

制御システム運転停止期間の基準: 備蓄在庫が 2 週間あるため、2 週間未満の制御システム運転停止につながる場合は重要度(事業被害)2、 それ以上は重要度(事業被害)3 とする。

- 重要度異なる評価値となる判断基準に該当する場合は、重要度が高い評価値とする。

2.5. 各資産に対する重要度一覧

【作業 2.5】資産の重要度を決定すること。

- 「2.4 資産の重要度の判断基準」に従い、各資産の重要度を決定する。
- 重要度を決定した根拠を記載すること。

【アウトプット 2.5】

資産の重要度とその判断根拠を以下に示す（表 2-6）。

表 2-6 資産の重要度

#	資産	重要度	判断根拠
1	FW(制御 DMZ)	3	FW(制御 DMZ)を突破されるとセキュリティ対策が不十分な制御ネットワーク以下への侵入を許し、操業に大きな影響が発生する恐れがある。
2	制御 DMZ	1	制御 DMZ ネットワークが利用不可となっても操業への影響がない。
3	データヒストリアン(中継)	1	ヒストリアンデータが参照不能でも操業への影響がない。
4	制御ネットワーク(情報側)	1	制御ネットワーク(情報側)が利用不可となっても操業への影響がない。
5	データヒストリアン	1	ヒストリアンデータが参照不能でも操業には影響がない。
6	制御サーバー(生産)	3	コントローラーの設定値が変更され、操業に大きな影響が発生する恐れがある。
7	EWS	3	コントローラーのプログラム・しきい値・設定値が変更され、操業に大きな影響が発生する恐れがある。
8	制御ネットワーク (フィールド側)	3	制御システムの監視・設定変更が不能となり、操業に大きな影響が発生する恐れがある。
9	コントローラー(生産)	3	制御システムの監視・設定変更・制御が不能となり、操業に大きな影響が発生する恐れがある。
10	HMI(生産)	3	制御システムの監視・設定変更が不能となり、操業に大きな影響が発生する恐れがある。
11	HMI(発電)	1	計器室からの監視が不可となるが、電気室での監視は可能であるため、操業への影響がない。
12	制御ネットワーク(発電)	1	制御ネットワーク(発電)が利用不可となっても操業への影響がない。
13	制御サーバー(発電)	2	コントローラーの監視・設定変更が不能となるが、コントローラー単体で安定稼働することができる。
14	コントローラー(発電)	3	コントローラーの設定値が不正に変更され、操業に大きな影響が発生する恐れがある。
15	FW(発電)	3	FW(発電)を突破されるとセキュリティ対策が不十分な制御ネットワーク以下への侵入を許し、操業に大きな影響が発生する恐れがある。
16	VPN(発電)	1	EMS サーバーへのヒストリアンデータの送信とリモート監視ができなくなるが、操業への影響はない。
17	EMS サーバー	1	ヒストリアンデータが参照不能でも操業への影響がない。

2.6. 事業被害レベルの判断基準

【作業 2.6】事業被害を 3 段階で評価する際の判断基準(3:被害大＞2:被害中＞1:被害小)を決めること。

- ガイド本編 *表 4-11* で提示している判断基準を具体化することが望ましい。

【アウトプット 2.6】

事業被害レベルの判断基準例を以下に示す(表 2-7)。

表 2-7 事業被害レベルの判断基準例

評価値		判断基準
3	事業上の被害が大きい	・障害が発生した場合、以下の事象となる。 - システムが長期間停止(2 週間以上停止)する恐れがある。 - 損失コストが 5 億円以上発生する恐れがある。 - 周辺環境の破壊・汚染が発生する恐れがある。
2	事業上の被害が中程度	・障害が発生した場合、以下の事象となる。 - システムが一定期間停止(3 日～2 週間停止)する恐れがある。 - 損失コストが 1 億円以上 5 億円未満発生する恐れがある。 - 事業会社敷地内での被害が発生する恐れがある。
1	事業上の被害が小さい	・障害が発生した場合、以下の事象となる。 - システムが短期間停止(3 日未満停止)する恐れがあるが、大きな影響はない。 - 損失コストが 1 億円未満発生する恐れがあるが、大きな影響はない。 - 事業会社敷地内での被害が発生する恐れはない。

2.7. 事業被害と事業被害レベルの検討

【作業 2.7①】分析対象システムで想定される事業被害とその概要を決定すること。

- 事業被害の概要には、事業被害を引き起こす「原因」とその「影響」を簡単に記載すること。
- ガイド本編「*4.3.1* 項 事業被害と事業被害レベルの意味」や、*表 4-12* 事業被害の定義例（1）が参考になる。

【アウトプット 2.7①】

分析対象システムの事業被害を以下に示す（表 2-8）。

表 2-8 事業被害の一覧表

#	事業被害	事業被害の概要
1	生産システムの停止	生産システムへのサイバー攻撃により、装置に停止・異常動作が発生することで、復旧までの間生産が 2 週間以上停止する。
2	基準値を超えた環境汚染物質の流出	生産システムまたは自家発電システムへのサイバー攻撃により、装置の異常動作が発生し、大気、水、土壌への特定物質の排出が増加する。
3	自家発電システムの停止による購入電力費用の増加	発電システムへのサイバー攻撃により、装置に停止・異常動作が発生し、自家発電システムを停止する。自家発電システム復旧まで、購入電力費用が増加する。

【作業 2.7②】事業被害レベルを重要度判断基準に従って決定すること。

- 「2.6 事業被害レベルの判断基準」に従った事業被害レベルの判断根拠をあわせて記載すること。

【アウトプット 2.7②】

事業被害の事業被害レベルとその判断根拠を以下に示す（表 2-9）。

表 2-9 事業被害一覧と事業被害レベル

事業被害	事業被害の概要	事業被害レベル	根拠
生産システムの停止	生産システムへのサイバー攻撃により、装置に停止・異常動作が発生することで、復旧までの間生産が 2 週間以上停止する。	3	生産システムの停止期間が 2 週間以上となる恐れがあるため、レベル「3」の評価とする。
基準値を超えた環境汚染物質の流出	生産システムまたは自家発電システムへのサイバー攻撃により、装置の異常動作が発生し、大気、水、土壌への特定物質の排出が増加する。	3	周辺環境に大きな被害が出るため、レベル「3」の評価とする。
自家発電システムの停止による購入電力費用の増加	発電システムへのサイバー攻撃により、装置に停止・異常動作が発生し、自家発電システムを停止する。自家発電システム復旧まで、購入電力費用が増加する。	2	発電システムの停止原因究明、機器の再セットアップ等の復旧作業に要する期間にもよるが、おおむね損失コストが 1 億円以上 5 億円未満発生すると想定し、レベル「2」の評価とする。

2.8. 脅威レベルの判断基準

【作業 2.8】脅威レベルの判断基準(発生可能性 3:高＞2:中＞1:低)を決定すること。

- ガイド本編 *表 4-21～4-24* に判断基準の例を参考にしてもよい。

【アウトプット 2.8】

脅威レベルの判断基準を以下に示す(表 2-10)。

表 2-10 脅威レベルの判断基準

脅威レベル	悪意のある第三者による攻撃による判断基準	資産の論理的な配置による判断基準	資産の物理的な配置による判断基準
3	・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。	・インターネットと接続可能なネットワーク(情報ネットワーク)上にある資産。	・敷地と部屋への入室制限がなく、誰でもアクセスできる場所にある資産。
2	・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。	・情報ネットワークと間接的に接続しているネットワーク(制御ネットワーク)上にある資産。	・敷地と部屋への入室制限がある場所にある資産。
1	・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。	・隔離されたネットワーク上にある資産。	・厳重な有人監視体制と、敷地と部屋への入室制限に厳重な認証を有する部屋にある資産。

※脅威が異なる脅威レベルに当てはまる場合は、総合的に脅威レベルを判断するものとする。

2.9. 対策レベル（脆弱性レベル）の判断基準

表 2-11 脆弱性レベル（対策レベル）の判断基準

対策レベル	脆弱性レベル	判断基準
3	1	脅威に対して有効なセキュリティ対策が何もない、現在実施しているセキュリティ対策が不十分である。
2	2	脅威に対して十分有効なセキュリティ対策が 1 つ以上実施されている。
1	3	想定しうる脅威を正確に把握した上で、脅威に対して高度なセキュリティ対策が実施されている。

3. 資産ベースのリスク分析

資産ベースのリスク分析では、事前準備で作成した下記のアウトプットを利用して、リスク分析作業を実施する。

表 3-1 利用する事前準備のアウトプット

本書見出し	事前準備のアウトプット	ガイド本編
2.1.	資産一覧	*3.1.5. 表 3-10*
2.2.	システム構成図	*3.2.3. 図 3-8*
2.3.①	データフローマトリックス	*3.3.1. 表 3-11*
2.3.②	データフロー図	*3.3.2. 図 3-10*
2.4.	資産の重要度の判断基準	*4.2.2. 表 4-5*
2.5.	各資産に対する重要度一覧	*4.2.3. 表 4-9*
2.8.	脅威レベルの判断基準	*4.4.5. 表 4-21～表 4-24*

資産ベースのリスク分析作業で新たに作成するアウトプット一覧を下記に示す。

表 3-2 資産ベースのリスク分析作業で作成するアウトプット

本書見出し	資産ベース アウトプット	ガイド本編
3.1.	脅威レベルまとめ表	*5.3.4 表 5-5*
3.2.	資産ベースのリスク分析シート	*5.1. 図 5-3、図 5-4*
3.3.①	脆弱性レベルまとめ表	*5.5.3 表 5-10*
3.3.②	リスク値まとめ表	*5.6.3 表 5-13*

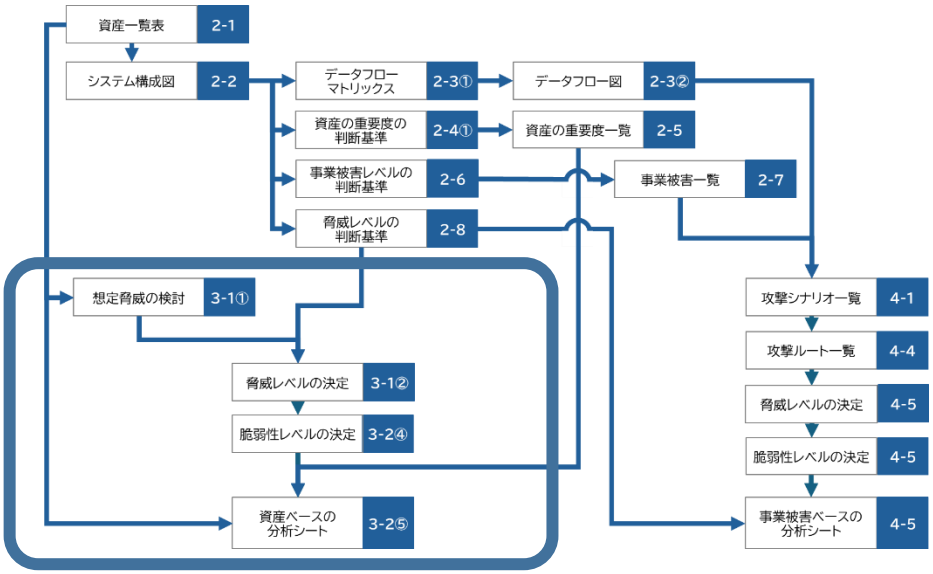


図 3-1 資産ベースのリスク分析作業の流れ

3.1. 脅威レベルの検討

【作業 3.1①】分析対象の資産に対して発生する脅威（攻撃手法）を検討し決定する。

- ガイド本編「*表 5-4* 想定される脅威（攻撃手法）一覧と資産種別の対応」を参照すること。
- 分析対象資産の資産種別は「2.1 節 表 2-3 資産一覧」を参照すること。

【アウトプット 3.1②】

分析対象の資産に対して発生する脅威（攻撃手法）のまとめ表を以下に示す（表 3-3）。

表 3-3 分析対象の資産に想定される脅威一覧表

#	脅威＼資産	FW(DMZ)	DMZ	データヒストリアン（中継）	制御ネットワーク（情報側）	データヒストリアン	制御サーバー（生産）	EWS	制御ネットワーク（フィールド側）	コントローラー（生産）	HMI（生産）	HMI（発電）	制御ネットワーク（発電）	制御サーバー（発電）	コントローラー（発電）	FW（発電）	VPN（発電）
	情報系機器			○		○	○	○			○	○		○			
	制御系機器									○					○		
	NW系資産（通信制御機能有）	○														○	○
	NW系資産（通信制御機能無）		○		○				○				○				
1	不正アクセス	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
2	物理的侵入	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
3	不正操作	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
4	過失操作	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
5	不正媒体・機器接続	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
6	プロセス不正実行	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
7	マルウェア感染	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
8	情報窃取	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
9	情報改ざん	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
10	情報破壊	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
11	不正送信	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
12	機能停止	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
13	制御不能・異常動作	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
14	高負荷攻撃	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
15	窃盗	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
16	盗難・廃棄時の分解による情報窃取	✔		✔		✔	✔	✔		✔	✔	✔		✔	✔	✔	✔
17	経路遮断	✔	✔		✔				✔				✔			✔	✔
18	通信輻輳	✔	✔		✔				✔				✔			✔	✔
19	無線妨害																
20	盗聴	✔	✔		✔				✔				✔			✔	✔
21	通信データ改ざん	✔	✔		✔				✔				✔			✔	✔
22	不正機器接続	✔	✔		✔				✔				✔			✔	✔

✔：資産に対して発生する脅威（攻撃手法）

グレーアウト：資産に対して発生しない脅威（攻撃手法）

機器（情報系機器・制御系機器）の場合に、#1～#16 の脅威が発生しうるとした。ネットワーク系資産（NW 系資産）の場合は、#17～#22 の脅威が発生しうるとした。今回のネットワーク系資産は無線機能を利用していないため、#19 無線妨害の脅威は発生しないこととした。

【作業 3.1②】各資産において、脅威（攻撃手法）の脅威レベルを決定する。

- 攻撃者の想定は、「悪意のある第三者」とする（第三者の過失、内部関係者の過失、悪意のある内部関係者は資産ベースのリスク分析において除外する）。
- 「2.8 脅威レベルの判断基準」の判断基準を使い、特定の資産に対する脅威（攻撃手法）の脅威レベルを決めること。
- 脅威レベルを決定した根拠を合わせて記載すること。

【アウトプット 3.1②】

FW(発電)について脅威レベルとその根拠を設定した表を以下に示す(表 3-4)。全ての資産の脅威レベルは【アウトプット 3.1③】を参照して欲しい。

表 3-4 FW(発電)の脅威レベルと根拠

#	脅威（攻撃手法）	脅威 レベル	根拠
1	不正アクセス	2	インターネット側に管理ポートを公開していないが、内部ネットワークから不正アクセスされる可能性があるため、脅威は中程度。
2	物理的侵入	2	一定のソーシャルエンジニアリング能力（構内侵入等）を持った攻撃者により可能なため、脅威は中程度。
3	不正操作	2	物理的に侵入(#2)すれば、スキルを問わず攻撃者によりコンソール操作が可能なため、脅威は中程度。
4	過失操作	1	インターネット閲覧やメール利用をしない機器のため、過失操作によるマルウェア感染等の脅威は低い。
5	不正媒体・機器接続	2	物理的に侵入(#2)すれば、スキルを問わず攻撃者により不正媒体や機器接続が可能であり、脅威は中程度。
6	プロセス不正実行	2	一定スキルを持った攻撃者により可能であるが、脅威は中程度。
7	マルウェア感染	2	ファームウェアの改ざんによりマルウェアの感染が可能であり、脅威は中程度。
8	情報窃取	2	マルウェアに感染した場合(#7)、起こり得るため脅威は中程度。
9	情報改ざん	2	マルウェアに感染した場合(#7)、起こり得るため脅威は中程度。
10	情報破壊	1	情報破壊による制御システムへの影響がないため脅威は低い。
11	不正送信	2	マルウェアに感染した場合(#7)、起こり得るため脅威は中程度。
12	機能停止	1	機能停止による制御システムへの影響がないため脅威は低い。
13	制御不能・異常動作	1	制御不能・異常動作による制御システムへの影響がないため脅威は低い。
14	高負荷攻撃	1	高負荷攻撃による制御システムへの影響がないため脅威は低い。
15	窃盗	2	一定のソーシャルエンジニアリング能力（構内侵入等）を持った攻撃者により可能なため、脅威は中程度。
16	盗難・廃棄時の分解による情報窃取	2	窃盗(#15)により可能で、機器は汎用品のため情報接種は容易であるため、脅威は中程度。
17	経路遮断	2	物理的に侵入(#2)すれば、スキルを問わず攻撃者によりコンソール操作が可能なため、脅威は中程度。
18	通信輻輳	1	ネットワーク上に資産が少ないため脅威は低い。
19	無線妨害	―	無線機能がないため対象外。
20	盗聴	2	マルウェアに感染した場合(#7)、起こり得るため脅威は中程度。
21	通信データ改ざん	2	マルウェアに感染した場合(#7)、起こり得るため脅威は中程度。
22	不正機器接続	2	物理的に侵入(#2)すれば、スキルを問わず攻撃者により不正媒体や機器接続が可能であり、脅威は中程度。

【作業 3.1③】分析対象の全資産で脅威レベルを検討し、それらを一覧表にまとめる。

- 資産と脅威の種類の組み合わせにおける、脅威レベルの分布の把握や見直しができる。

【アウトプット 3.1③】

資産の脅威レベルまとめ表を以下に示す(表 3-5)。

表 3-5 資産の脅威レベルまとめ表

		脅威レベルを見直さなかった資産											脅威レベルを見直した資産				新規資産
資産の場所		サーバ室									計器室		電気室				
#	脅威 ＼ 資産	FW(DMZ)	DMZ	データヒストリアン（中継）	制御ネットワーク（情報側）	データヒストリアン	制御サーバー(生産)	EWS	制御ネットワーク（フィールド側）	コントローラー(生産)	HMI(生産)	HMI(発電)	制御ネットワーク（発電）	制御サーバー(発電)	コントローラー(発電)	FW(発電)	VPN(発電)
	情報系機器			○		○	○	○			○	○		○			
	制御系機器									○					○		
	NW系資産(通信制御機能有)	○														○	○
	NW系資産(通信制御機能無)		○		○				○				○				
	重要度	3	1	1	1	1	3	3	3	3	3	1	1	2	3	3	1
1	不正アクセス	2		2		1	1	1		1	1	2		3	2	2	3
2	物理的侵入	2		2		2	2	2		2	2	2		2	2	2	2
3	不正操作	2		2		2	2	2		2	2	2		2	2	2	2
4	過失操作	1		1		1	1	1		1	1	1		1	1	1	1
5	不正媒体・機器接続	2		2		2	2	2		2	2	2		2	2	2	2
6	プロセス不正実行	2		2		2	2	2		2	2	2		3	2	2	2
7	マルウェア感染	2		2		2	2	2		2	2	2		3	2	1	2
8	情報窃取	2		2		2	2	2		2	2	2		3	2	2	2
9	情報改ざん	2		2		2	2	2		2	2	2		3	2	2	2
10	情報破壊	1		2		2	2	2		2	2	2		3	2	1	1
11	不正送信	2		2		2	2	2		2	2	2		3	2	2	2
12	機能停止	1		1		1	2	2		2	2	2		3	2	1	1
13	制御不能・異常動作	1		1		1	2	2		2	2	2		3	2	1	1
14	高負荷攻撃	1		1		1	2	2		2	2	2		3	2	1	1
15	窃盗	2		2		2	2	2		2	2	2		2	2	2	2
16	盗難・廃棄時の分解による情報窃取	2		2		2	2	2		2	2	2		2	2	2	2
17	経路遮断	2	2		2				2				2			2	2
18	通信輻輳	1	1		1				2				1			1	1
19	無線妨害																
20	盗聴	2	2		2				2				2			2	2
21	通信データ改ざん	2	2		2				2				2			2	2
22	不正機器接続	2	2		2				2				2			2	2

3.2. 資産ベースのリスク分析シートの作成

ガイド本編「*5 章* 資産ベースのリスク分析」で解説された手順に基づき、分析対象システムの資産ベースのリスク分析を実施する。詳細な手順はガイド本編を参照するものとして、ここでは作業の大きな流れを説明する。

【作業 3.2①】資産ベースの分析シートに重要度を記載する。

- 「表 2-6 資産の重要度」で定義した数値を分析シートに記載する。

【作業 3.2②】資産ベースの分析シートに脅威レベルを記載する。また、想定しない脅威はグレーアウトとして表示する。

- 「表 3-3 分析対象の資産に想定される脅威一覧表」を参照し、資産に対して想定する脅威に脅威レベルを記載する。また想定しない脅威はグレーアウトする。

【作業 3.2③】脅威に対する対策状況を確認し、実施している対策に〇を記入する。対策の実施内容について補足があれば追記する。また、必要に応じて対策項目を追記する。

- 「表 2-3 資産一覧表」のセキュリティ対策項目と資産ベースの分析シートの対策状況を比較し、該当する対策状況に〇を記入する。

【作業 3.2④】対策内容から対策レベルを評価し、対策レベルと脆弱性レベルを分析シートに記入する。

- ガイド本編「*5.5.1 項 表 5-7*」を基準として採用し、対策レベルと脆弱性レベルを記載する。

【作業 3.2⑤】重要度レベル、脅威レベル、脆弱性レベルからリスク値を決定し、分析シートに記入する。

【アウトプット 3.2】

資産ベースのリスク分析シートの記入例について、53 頁以降に示す（表 3-6）。

このページは空白です。

表 3-6 資産ベースのリスク分析シート（1/6）

凡例: ○ 対策実施　　空欄 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威　対策の緑字: 対策の補足情報

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	事業継続	
									侵入/拡散段階		目的遂行段階				脅威毎
1	情報系資産	1.HMI(発電)	2	1		E	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。	ファイアウォール 通信相手の認証（ID・パスワード） IPS/IDS パッチ適用 脆弱性回避 デフォルトパスワードの変更	 ○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム		3
2			2	2		D	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（敷地内への入退管理） 施錠管理 24時間有人監視	○ ○			監視カメラ 侵入センサー		2
3			2	2		D	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 デフォルトパスワードの変更	 ○					2
4			1	1		E	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レビューシ メールフィルタリング メール・Webの利用なし	 ○					3
5			2	2		D	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 24時間有人監視	 ○	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		2
6			2	3		D	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		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		機器異常検知 機器死活監視 ログ収集・分析		1
7			2	3		D	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。	アンチウィルス 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		1
8			2	3		D	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		権限管理 アクセス制御 データ暗号化 DLP		ログ収集・分析 統合ログ管理システム		1
9			2	3		D	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		権限管理 アクセス制御 データ署名		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			2	3		D	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			2	3		D	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		セグメント分割/ゾーニング データ署名 重要操作の承認		ログ収集・分析 統合ログ管理システム		1
12			2	3	1	D	機能停止	機器の機能を停止する。			パッチ適用 脆弱性回避		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 安全計装システム(SIS)	○ ○	1
13			2	3		D	制御不能・異常動作	機器を制御不能にする。異常動作を引き起こす。			パッチ適用 脆弱性回避		機器異常検知 ログ収集・分析 統合ログ管理システム	フェールセーフ設計 安全計装システム(SIS)	○ ○	1
14			2	3		D	高負荷攻撃	(D)DoS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。	(D)DOS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
15			2	2		D	窃盗	機器を窃盗する。	施錠管理		施錠管理		施錠管理			2
16			2	3		D	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		耐タンパー 難読化 セキュア消去					1
17							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 侵入センサー	冗長化		
18							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。	ファイアウォール 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		
19							無線妨害	無線通信を妨害する。	メッシュネットワーク				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		
20							盗聴	ネットワーク上を流れる情報を盗聴する。	データ暗号化 通信路暗号化 専用線 無線通信経路のアクセス制限							
21							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。	データ暗号化 通信路暗号化 専用線 無線通信経路のアクセス制限				ログ収集・分析 統合ログ管理システム			
22							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 無線通信経路のアクセス制限				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			

表 3-6 資産ベースのリスク分析シート (2/6)

凡例: ○ 対策実施　　空欄 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威　対策の緑字: 対策の補足情報

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	ネットワーク系資産	2.制御ネットワーク(発電)					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。	ファイアウォール 通信相手の認証(ID・パスワード) IPS/IDS パッチ適用 脆弱性回避 デフォルトパスワードの変更	 ○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム		
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。	入退管理(敷地内への入退管理) 施錠管理 24時間有人監視	○ ○			監視カメラ 侵入センサー		
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。	操作者認証 デフォルトパスワードの変更	 ○					
4							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 メール・Webの利用なし	 ○					
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。	デバイス接続・利用制限 24時間有人監視	 ○	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		
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。	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		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		機器異常検知 機器死活監視 ログ収集・分析		
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。	アンチウィルス 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		
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。	権限管理 アクセス制御 データ暗号化 DLP		権限管理 アクセス制御 データ暗号化 DLP		ログ収集・分析 統合ログ管理システム		
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。	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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	
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。	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	
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。	セグメント分割/ゾーニング データ署名 重要操作の承認		セグメント分割/ゾーニング データ署名 重要操作の承認		ログ収集・分析 統合ログ管理システム		
12					2		機能停止	機器の機能を停止する。			パッチ適用 脆弱性回避		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 安全計装システム(SIS)	○ ○	
13							制御不能・異常動作	機器を制御不能にする。異常動作を引き起こす。			パッチ適用 脆弱性回避		機器異常検知 ログ収集・分析 統合ログ管理システム	フェールセーフ設計 安全計装システム(SIS)	○ ○	
14							高負荷攻撃	(D)DoS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。	(D)DOS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	○ ○	
15							窃盗	機器を窃盗する。	施錠管理		施錠管理		施錠管理		
16							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		耐タンパー 難読化 セキュア消去				
17			2	3		B	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(敷地内への入退管理) 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 侵入センサー	冗長化	1
18			1	1		D	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。	ファイアウォール 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	3
19							無線妨害	無線通信を妨害する。	メッシュネットワーク				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	
20			2	3		B	盗聴	ネットワーク上を流れる情報を盗聴する。	データ暗号化 通信路暗号化 専用線 無線通信経路のアクセス制限						1
21			2	3		B	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。	データ暗号化 通信路暗号化 専用線 無線通信経路のアクセス制限				ログ収集・分析 統合ログ管理システム		1
22			2	2		C	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 無線通信経路のアクセス制限				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		2

表 3-6 資産ベースのリスク分析シート (3/6)

凡例: ○ 対策実施　　空欄 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威　対策の緑字: 対策の補足情報

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	事業継続	
									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									脅威毎
1	情報系資産	3.制御サーバー(発電)	3	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。	ファイアウォール				IPS/IDS		2
									通信相手の認証(ID・パスワード)	○			ログ収集・分析		
									IPS/IDS				統合ログ管理システム		
									パッチ適用						
									脆弱性回避						
									デフォルトパスワードの変更	○					
2			2	1		D	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(敷地内への入退管理)	○			監視カメラ		3
									施錠管理	○			侵入センサー		
3			2	2		C	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・パスワード)	○					2
									デフォルトパスワードの変更	○					
4			1	1		D	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						3
									メールフィルタリング						
									メール・Webの利用なし	○					
5			2	3		B	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		デバイス接続・利用制限		デバイス接続・利用制限		1
													ログ収集・分析		
													統合ログ管理システム		
6			3	3		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	○	権限管理				1
									アクセス制御		アクセス制御		機器異常検知		
									ホワイトリストによるプロセスの起動制限		ホワイトリストによるプロセスの起動制限		機器死活監視		
									重要操作の承認		重要操作の承認		ログ収集・分析		
7			3	3		B	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。	アンチウィルス				機器異常検知		1
									ホワイトリストによるプロセスの起動制限				機器死活監視		
									パッチ適用				ログ収集・分析		
									脆弱性回避				統合ログ管理システム		
									データ署名						
8			3	2		B	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	○	権限管理		ログ収集・分析		2
									アクセス制御		アクセス制御		統合ログ管理システム		
									データ暗号化		データ暗号化				
									DLP		DLP				
9			3	2		B	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	○	権限管理		機器異常検知	データバックアップ	2
									アクセス制御		アクセス制御		ログ収集・分析		
									データ署名		データ署名		統合ログ管理システム		
10			3	2		B	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	○			機器異常検知	データバックアップ	2
									アクセス制御				ログ収集・分析		
													統合ログ管理システム		
11			3	3		B	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		セグメント分割/ゾーニング		ログ収集・分析		1
									データ署名		データ署名		統合ログ管理システム		
									重要操作の承認		重要操作の承認				
12			3	3	2	B	機能停止	機器の機能を停止する。			パッチ適用		機器異常検知	冗長化 ○	1
											脆弱性回避		機器死活監視	フェールセーフ設計 ○	
													ログ収集・分析	安全計装システム(SIS)	
													統合ログ管理システム		
13			3	2		B	制御不能・異常動作	機器を制御不能にする。異常動作を引き起こす。			パッチ適用		機器異常検知	フェールセーフ設計 ○	2
											脆弱性回避		ログ収集・分析	安全計装システム(SIS) ○	
													統合ログ管理システム		
14			3	3		B	高負荷攻撃	(D)DoS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。	(D)DOS対策				機器異常検知	冗長化 ○	1
													機器死活監視	フェールセーフ設計 ○	
													ログ収集・分析		
													統合ログ管理システム		
15			2	3		B	窃盗	機器を窃盗する。	施錠管理		施錠管理		施錠管理		1
16			2	3		B	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		耐タンパー				1
									難読化		難読化				
									セキュア消去		セキュア消去				
17							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				機器異常検知	冗長化	
									施錠管理				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		
													侵入センサー		
18							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。	ファイアウォール				機器異常検知	冗長化	
									IPS/IDS				機器死活監視		
									DDoS対策				ログ収集・分析		
													統合ログ管理システム		
19							無線妨害	無線通信を妨害する。	メッシュネットワーク				機器異常検知	冗長化	
													機器死活監視		
													ログ収集・分析		
													統合ログ管理システム		
20							盗聴	ネットワーク上を流れる情報を盗聴する。	データ暗号化						
									通信路暗号化						
									専用線						
									無線通信経路のアクセス制限						
21							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。	データ暗号化				ログ収集・分析		
									通信路暗号化				統合ログ管理システム		
									専用線						
									無線通信経路のアクセス制限						
22							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		
									無線通信経路のアクセス制限				ログ収集・分析		
													統合ログ管理システム		

表 3-6 資産ベースのリスク分析シート (4/6)

凡例: ○ 対策実施　　空欄 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威　対策の緑字: 対策の補足情報

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	制御系資産	4.コントローラー(発電)	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。	ファイアウォール				IPS/IDS		2
									通信相手の認証(ID・パスワード)	○			ログ収集・分析		
									IPS/IDS				統合ログ管理システム		
									パッチ適用						
									脆弱性回避						
									デフォルトパスワードの変更	○					
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(敷地内への入退管理)	○			監視カメラ		3
									施錠管理	○			侵入センサー		
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・パスワード)	○					2
									デフォルトパスワードの変更	○					
4			1	1		C	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						3
									メールフィルタリング						
									メール・Webの利用なし	○					
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		デバイス接続・利用制限		デバイス接続・利用制限		1
													ログ収集・分析		
													統合ログ管理システム		
6			2	3		A	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	○	権限管理				1
									アクセス制御		アクセス制御		機器異常検知		
									ホワイトリストによるプロセスの起動制限		ホワイトリストによるプロセスの起動制限		機器死活監視		
									重要操作の承認		重要操作の承認		ログ収集・分析		
7			2	2		B	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。	アンチウィルス				機器異常検知		2
									ホワイトリストによるプロセスの起動制限				機器死活監視		
									パッチ適用				ログ収集・分析		
									脆弱性回避				統合ログ管理システム		
									データ署名						
8			2	3		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		権限管理		ログ収集・分析		1
									アクセス制御		アクセス制御		統合ログ管理システム		
									データ暗号化		データ暗号化				
									DLP		DLP				
9			2	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		権限管理		機器異常検知	データバックアップ	1
									アクセス制御		アクセス制御		ログ収集・分析		
									データ署名		データ署名		統合ログ管理システム		
10			2	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				機器異常検知	データバックアップ	1
									アクセス制御				ログ収集・分析		
													統合ログ管理システム		
11			2	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		セグメント分割/ゾーニング		ログ収集・分析		1
									データ署名		データ署名		統合ログ管理システム		
									重要操作の承認		重要操作の承認				
12			2	3	2	A	機能停止	機器の機能を停止する。			パッチ適用		機器異常検知	冗長化 ○	1
											脆弱性回避		機器死活監視	フェールセーフ設計 ○	
													ログ収集・分析	安全計装システム(SIS)	
													統合ログ管理システム		
13			2	3		A	制御不能・異常動作	機器を制御不能にする。異常動作を引き起こす。			パッチ適用		機器異常検知	フェールセーフ設計 ○	1
											脆弱性回避		ログ収集・分析	安全計装システム(SIS) ○	
													統合ログ管理システム		
14			2	3		A	高負荷攻撃	(D)DoS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。	(D)DOS対策				機器異常検知	冗長化 ○	1
													機器死活監視	フェールセーフ設計 ○	
													ログ収集・分析		
													統合ログ管理システム		
15			2	2		B	窃盗	機器を窃盗する。	施錠管理	○	施錠管理	○	施錠管理	○	2
16			2	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		耐タンパー				1
									難読化		難読化				
									セキュア消去		セキュア消去				
17							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				機器異常検知	冗長化	
									施錠管理				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		
													侵入センサー		
18							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。	ファイアウォール				機器異常検知	冗長化	
									IPS/IDS				機器死活監視		
									DDoS対策				ログ収集・分析		
													統合ログ管理システム		
19							無線妨害	無線通信を妨害する。	メッシュネットワーク				機器異常検知	冗長化	
													機器死活監視		
													ログ収集・分析		
													統合ログ管理システム		
20							盗聴	ネットワーク上を流れる情報を盗聴する。	データ暗号化						
									通信路暗号化						
									専用線						
									無線通信経路のアクセス制限						
21							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。	データ暗号化				ログ収集・分析		
									通信路暗号化				統合ログ管理システム		
									専用線						
									無線通信経路のアクセス制限						
22							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		
									無線通信経路のアクセス制限				ログ収集・分析		
													統合ログ管理システム		

表 3-6 資産ベースのリスク分析シート (5/6)

凡例: ○ 対策実施　　空欄 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威　対策の緑字: 対策の補足情報

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	ネットワーク系資産	S,FW(発電)	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。	ファイアウォール	○			IPS/IDS				2
									通信相手の認証（ID・パスワード）	○			ログ収集・分析				
									IPS/IDS				統合ログ管理システム				
									パッチ適用								
									脆弱性回避								
									デフォルトパスワードの変更	○							
2			2	2		B	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（敷地内への入退管理）	○			監視カメラ				2
									施錠管理	○			侵入センサー				
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・パスワード）	○							2
									デフォルトパスワードの変更	○							
4			1	1		C	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								3
									メールフィルタリング								
									メール・Webの利用なし	○							
5			2	2		B	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	○	デバイス接続・利用制限	○	デバイス接続・利用制限	○			2
													ログ収集・分析				
													統合ログ管理システム				
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	○	権限管理	○					2
									アクセス制御		アクセス制御		機器異常検知				
									ホワイトリストによるプロセスの起動制限		ホワイトリストによるプロセスの起動制限		機器死活監視				
									重要操作の承認		重要操作の承認		ログ収集・分析				
7			1	3		B	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。	アンチウィルス				機器異常検知				1
									ホワイトリストによるプロセスの起動制限				機器死活監視				
									パッチ適用				ログ収集・分析				
									脆弱性回避				統合ログ管理システム				
									データ署名								
8			2	2		B	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	○	権限管理	○	ログ収集・分析				2
									アクセス制御	○	アクセス制御	○	統合ログ管理システム				
									データ暗号化		データ暗号化						
									DLP		DLP						
9			2	2		B	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	○	権限管理	○	機器異常検知		データバックアップ		2
									アクセス制御	○	アクセス制御	○	ログ収集・分析				
									データ署名		データ署名		統合ログ管理システム				
10			1	2		C	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	○			機器異常検知		データバックアップ		2
									アクセス制御	○			ログ収集・分析				
													統合ログ管理システム				
11			2	2		B	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	○	セグメント分割/ゾーニング	○	ログ収集・分析				2
									データ署名		データ署名		統合ログ管理システム				
									重要操作の承認		重要操作の承認						
12			1	3	2	B	機能停止	機器の機能を停止する。			パッチ適用		機器異常検知		冗長化	○	1
											脆弱性回避		機器死活監視		フェールセーフ設計	○	
													ログ収集・分析		安全計装システム(SIS)		
													統合ログ管理システム				
13			1	3		B	制御不能・異常動作	機器を制御不能にする。異常動作を引き起こす。			パッチ適用		機器異常検知		フェールセーフ設計	○	1
											脆弱性回避		ログ収集・分析		安全計装システム(SIS)	○	
													統合ログ管理システム				
14			1	3		B	高負荷攻撃	(D)DoS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。	(D)DOS対策				機器異常検知		冗長化	○	1
													機器死活監視		フェールセーフ設計	○	
													ログ収集・分析				
													統合ログ管理システム				
15			2	2		B	窃盗	機器を窃盗する。	施錠管理	○	施錠管理	○	施錠管理	○			2
16			2	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		耐タンパー						1
									難読化		難読化						
									セキュア消去		セキュア消去						
17			2	2		B	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（敷地内への入退管理）	○			機器異常検知		冗長化		2
									施錠管理	○			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				
													侵入センサー				
18			1	1		C	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。	ファイアウォール	○			機器異常検知		冗長化		3
									IPS/IDS				機器死活監視				
									DDoS対策				ログ収集・分析				
													統合ログ管理システム				
19							無線妨害	無線通信を妨害する。	メッシュネットワーク				機器異常検知		冗長化		
													機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
20			2	3		A	盗聴	ネットワーク上を流れる情報を盗聴する。	データ暗号化								1
									通信路暗号化								
									専用線								
									無線通信経路のアクセス制限								
21			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。	データ暗号化				ログ収集・分析				1
									通信路暗号化				統合ログ管理システム				
									専用線								
									無線通信経路のアクセス制限								
22			2	2		B	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	○			2
									無線通信経路のアクセス制限				ログ収集・分析				
													統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート (6/6)

凡例: ○ 対策実施　　空欄 対策未実施　　グレーアウト行: 該当資産で考慮しない脅威　対策の緑字: 対策の補足情報

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	ネットワーク系資産	6.VPN(発電)	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。	ファイアウォール	○			IPS/IDS				2
									通信相手の認証（ID・パスワード）	○			ログ収集・分析				
									IPS/IDS				統合ログ管理システム				
									パッチ適用								
									脆弱性回避								
									デフォルトパスワードの変更	○							
2			2	2		B	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（敷地内への入退管理）	○			監視カメラ				2
									施錠管理	○			侵入センサー				
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・パスワード）	○							2
									デフォルトパスワードの変更	○							
4			1	1		C	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								3
									メールフィルタリング								
									メール・Webの利用なし	○							
5			2	2		B	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	○	デバイス接続・利用制限	○	デバイス接続・利用制限	○			2
													ログ収集・分析				
													統合ログ管理システム				
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	○	権限管理	○					2
									アクセス制御		アクセス制御		機器異常検知				
									ホワイトリストによるプロセスの起動制限		ホワイトリストによるプロセスの起動制限		機器死活監視				
									重要操作の承認		重要操作の承認		ログ収集・分析				
7			1	3		B	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。	アンチウィルス				機器異常検知				1
									ホワイトリストによるプロセスの起動制限				機器死活監視				
									パッチ適用				ログ収集・分析				
									脆弱性回避				統合ログ管理システム				
									データ署名								
8			2	2		B	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	○	権限管理	○	ログ収集・分析				2
									アクセス制御	○	アクセス制御	○	統合ログ管理システム				
									データ暗号化		データ暗号化						
									DLP		DLP						
9			2	2		B	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	○	権限管理	○	機器異常検知		データバックアップ		2
									アクセス制御	○	アクセス制御	○	ログ収集・分析				
									データ署名		データ署名		統合ログ管理システム				
10			1	2		C	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	○			機器異常検知		データバックアップ		2
									アクセス制御	○			ログ収集・分析				
													統合ログ管理システム				
11			2	2		B	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	○	セグメント分割/ゾーニング	○	ログ収集・分析				2
									データ署名		データ署名		統合ログ管理システム				
									重要操作の承認		重要操作の承認						
12			1	3	2	B	機能停止	機器の機能を停止する。			パッチ適用		機器異常検知		冗長化	○	1
											脆弱性回避		機器死活監視		フェールセーフ設計	○	
													ログ収集・分析		安全計装システム(SIS)		
													統合ログ管理システム				
13			1	3		B	制御不能・異常動作	機器を制御不能にする。異常動作を引き起こす。			パッチ適用		機器異常検知		フェールセーフ設計	○	1
											脆弱性回避		ログ収集・分析		安全計装システム(SIS)	○	
													統合ログ管理システム				
14			1	3		B	高負荷攻撃	(D)DoS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。	(D)DOS対策				機器異常検知		冗長化	○	1
													機器死活監視		フェールセーフ設計	○	
													ログ収集・分析				
													統合ログ管理システム				
15			2	2		B	窃盗	機器を窃盗する。	施錠管理	○	施錠管理	○	施錠管理	○			2
16			2	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		耐タンパー						1
									難読化		難読化						
									セキュア消去		セキュア消去						
17			2	2		B	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（敷地内への入退管理）	○			機器異常検知		冗長化		2
									施錠管理	○			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				
													侵入センサー				
18			1	1		C	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。	ファイアウォール	○			機器異常検知		冗長化		3
									IPS/IDS				機器死活監視				
									DDoS対策				ログ収集・分析				
													統合ログ管理システム				
19							無線妨害	無線通信を妨害する。	メッシュネットワーク				機器異常検知		冗長化		
													機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
20			2	3		A	盗聴	ネットワーク上を流れる情報を盗聴する。	データ暗号化								1
									通信路暗号化								
									専用線								
									無線通信経路のアクセス制限								
21			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。	データ暗号化				ログ収集・分析				1
									通信路暗号化				統合ログ管理システム				
									専用線								
									無線通信経路のアクセス制限								
22			2	2		B	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	○			2
									無線通信経路のアクセス制限				ログ収集・分析				
													統合ログ管理システム				

3.3. リスク値のまとめ

【作業 3.3①】脆弱性レベルのまとめ表を作成すること。

- 資産と脅威の種類の組み合わせにおける、脆弱性レベルの分布の把握や見直しができる。

【アウトプット 3.3①】

脆弱性レベルのまとめ表を以下に示す（表 3-7）。

表 3-7 資産ベースのリスク分析 脆弱性レベルまとめ表

資産の場所		サーバ室									計器室		電気室				
#	脅威 ＼ 資産	FW(DMZ)	DMZ	データヒストリアン（中継）	制御ネットワーク（情報側）	データヒストリアン	制御サーバー(生産)	EWS	制御ネットワーク（フィールド側）	コントローラー(生産)	HMI(生産)	HMI(発電)	制御ネットワーク（発電）	制御サーバー(発電)	コントローラー(発電)	FW(発電)	VPN(発電)
	情報系機器			○		○	○	○			○	○		○			
	制御系機器									○					○		
	NW系資産（通信制御機能有）	○														○	○
	NW系資産（通信制御機能無）		○		○				○				○				
	重要度	3	1	1	1	1	3	3	3	3	3	1	1	2	3	3	1
1	不正アクセス	2		2		1	1	1		1	1	1		2	2	2	2
2	物理的侵入	1		1		2	2	2		2	2	2		1	1	2	2
3	不正操作	1		1		2	2	2		2	2	2		2	2	2	2
4	過失操作	1		1		1	1	1		1	1	1		1	1	1	1
5	不正媒体・機器接続	2		2		2	2	2		2	2	2		3	3	2	3
6	プロセス不正実行	2		2		2	3	3		3	3	3		3	3	2	2
7	マルウェア感染	2		2		2	3	3		3	3	3		3	2	3	3
8	情報窃取	2		2		2	3	3		3	3	3		2	3	2	2
9	情報改ざん	2		3		3	3	3		3	3	3		2	3	2	2
10	情報破壊	2		3		3	3	3		3	3	3		2	3	2	2
11	不正送信	2		3		3	3	3		3	3	3		3	3	2	2
12	機能停止	2		3		3	3	3		3	3	3		3	3	3	3
13	制御不能・異常動作	2		3		3	3	3		3	3	3		2	3	3	3
14	高負荷攻撃	2		3		3	3	3		3	3	3		3	3	3	3
15	窃盗	1		1		2	2	2		2	2	2		3	2	2	2
16	盗難・廃棄時の分解による情報窃取	1		1		1	1	1		1	1	3		3	3	3	3
17	経路遮断	2	2		3				3				3			2	2
18	通信輻輳	1	1		1				3				1			1	1
19	無線妨害																
20	盗聴	2	2		3				3				3			3	2
21	通信データ改ざん	2	2		3				3				3			3	2
22	不正機器接続	2	2		2				2				2			2	2

【作業 3.3②】リスク値まとめ表を作成する。

【アウトプット 3.3②】

リスク値のまとめ表を以下に示す（表 3-8）。

表 3-8 資産ベースのリスク分析 リスク値まとめ表

		脅威レベルを見直さなかった資産									脅威レベルを見直した資産		新規資産				
資産の場所		サーバ室									計器室		電気室				
#	脅威＼資産	FW(制御DMZ)	制御DMZ	データヒストリアン（中継）	制御ネットワーク（情報側）	データヒストリアン	制御サーバー(生産)	EWS	制御ネットワーク（フィールド側）	コントローラー(生産)	HMI(生産)	HMI(発電)	制御ネットワーク（発電）	制御サーバー(発電)	コントローラー(発電)	FW(発電)	VPN(発電)
	情報系機器			○		○	○	○			○	○		○			
	制御系機器									○					○		
	NW系資産（通信制御機能有）	○														○	○
	NW系資産（通信制御機能無）		○		○				○				○				
	重要度	3	1	1	1	1	3	3	3	3	3	1	1	2	3	3	1
1	不正アクセス	B		D		E	C	C		C	C	E		B	B	B	D
2	物理的侵入	C		E		D	B	B		B	B	D		D	C	B	D
3	不正操作	C		E		D	B	B		B	B	D		C	B	B	D
4	過失操作	C		E		E	C	C		C	C	E		D	C	C	E
5	不正媒体・機器接続	B		D		D	B	B		B	B	D		B	A	B	D
6	プロセス不正実行	B		D		D	A	A		A	A	D		B	A	B	D
7	マルウェア感染	B		D		D	A	A		A	A	D		B	B	B	D
8	情報窃取	B		D		D	A	A		A	A	D		B	A	B	D
9	情報改ざん	B		D		D	A	A		A	A	D		B	A	B	D
10	情報破壊	C		D		D	A	A		A	A	D		B	A	C	E
11	不正送信	B		D		D	A	A		A	A	D		B	A	B	D
12	機能停止	C		E		E	A	A		A	A	D		B	A	B	E
13	制御不能・異常動作	C		E		E	A	A		A	A	D		B	A	B	E
14	高負荷攻撃	C		E		E	A	A		A	A	D		B	A	B	E
15	窃盗	C		E		D	B	B		B	B	D		B	B	B	D
16	盗難・廃棄時の分解による情報窃取	C		E		E	C	C		C	C	D		B	A	A	D
17	経路遮断	B	D		D				A				D			B	D
18	通信輻輳	C	E		E				A				E			C	E
19	無線妨害																
20	盗聴	B	D		D				A				D			A	D
21	通信データ改ざん	B	D		D				A				D			A	D
22	不正機器接続	B	D		D				B				D			B	D

また、前回リスク分析結果と今回外部サービスとの接続後で脅威レベルを見直した資産について、リスク値がどのように変化したのかを下表にまとめる。

表 3-9 リスク値の変化

#	脅威 ＼ 資産	HMI(発電)		制御ネットワーク(発電)		制御サーバー(発電)		コントローラー(発電)	
	重要度	1		1		2		3	
		前回	今回	前回	今回	前回	今回	前回	今回
1	不正アクセス	E	E			D	B	C	B
2	物理的侵入	D	D			D	D	C	C
3	不正操作	D	D			C	C	B	B
4	過失操作	E	E			D	D	C	C
5	不正媒体・機器接続	D	D			B	B	A	A
6	プロセス不正実行	D	D			B	B	A	A
7	マルウェア感染	D	D			B	B	B	B
8	情報窃取	D	D			C	B	A	A
9	情報改ざん	D	D			C	B	A	A
10	情報破壊	D	D			C	B	A	A
11	不正送信	D	D			B	B	A	A
12	機能停止	D	D			B	B	A	A
13	制御不能・異常動作	D	D			C	B	A	A
14	高負荷攻撃	D	D			B	B	A	A
15	窃盗	D	D			B	B	B	B
16	盗難・廃棄時の分解による情報窃取	D	D			B	B	A	A
17	経路遮断			D	D				
18	通信輻輳			E	E				
19	無線妨害								
20	盗聴			D	D				
21	通信データ改ざん			D	D				
22	不正機器接続			D	D				

4. 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では、事前準備で作成した下記のアウトプットを利用して、リスク分析作業を実施する。

表 4-1 利用する事前準備のアウトプット

本書見出し	事前準備のアウトプット	ガイド本編
2.1.	資産一覧	*3.1.5. 表 3-10*
2.2.	システム構成図	*3.2.3. 図 3-8*
2.3.①	データフローマトリックス	*3.3.1. 表 3-11*
2.3.②	データフロー図	*3.3.2. 図 3-10*
2.6.	事業被害レベルの判断基準	*4.3.2. 表 4-11*
2.7.	事業被害及び各事業被害に対する事業被害レベル一覧	*4.3.3. 表 4-12*
2.8.	脅威レベルの判断基準	*4.4.5. 表 4-21～表 4-24*

事業被害ベースのリスク分析作業で新たに作成するアウトプット一覧を下記に示す。

表 4-2 事業被害ベースのリスク分析作業で作成するアウトプット

本書見出し	資産ベース アウトプット	ガイド本編
4.1.	攻撃シナリオ一覧	*6.2.2. 表 6-6*
4.4.	攻撃ルート一覧	*6.5.1. 表 6-11～表 6-12*
4.4.	攻撃ルート図	*6.5.1. 図 6-10*
4.5.	事業被害ベースのリスク分析シート	*6.1.3 図 6-5、図 6-6*
4.6.	リスク値まとめ	*6.11.3. 図 6-32*

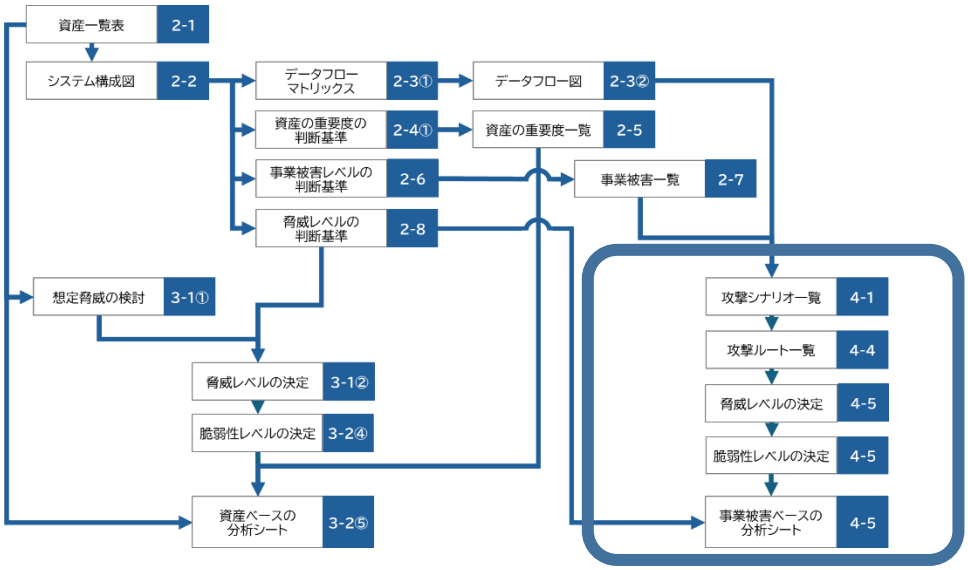


図 4-1 事業被害ベースのリスク分析作業の流れ

4.1. 攻撃シナリオ一覧の作成

ここでは、2.7 節で作成した「表 2-8 事業被害の一覧表」を基に、具体的な攻撃シナリオを作成した。攻撃シナリオ一覧表を以下（表 4-3）に示す。

表 4-3 攻撃シナリオ一覧表 (1/2)

<table>
<tr><th>項番</th><th>事業被害</th><th colspan="5">事業被害の概要と攻撃シナリオ</th><th>事業被害レベル</th></tr>
<tr><td rowspan="4">1</td><td rowspan="4">生産システムの停止</td><td colspan="5">生産システムへのサイバー攻撃により、装置が停止・異常動作が発生することで、復旧までの間生産が 2 週間以上停止する。</td><td rowspan="4">3</td></tr>
<tr><td>シナリオ #</td><td>攻撃シナリオ</td><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td></tr>
<tr><td>1-1</td><td>ランサムウェア感染により機器を使用不可となり、安全のためにシステムを停止せざるを得なくさせる。</td><td>データヒストリアン</td><td>制御サーバー(生産)
EWS
HMI(生産)</td><td>ランサムウェアで機器を利用不能にする。</td></tr>
<tr><td>1-2</td><td>コントローラーのプログラムを改ざんし、設備の異常動作を発生させる。</td><td>EWS</td><td>コントローラー(生産)</td><td>不正な制御コマンドを送信する。</td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">基準値を超えた環境汚染物質の流出</td><td colspan="5">生産システムまたは自家発電システムへのサイバー攻撃により、装置の異常動作が発生し、大気、水、土壌への特定物質の排出が増加する。</td><td rowspan="3">2</td></tr>
<tr><td>シナリオ #</td><td>攻撃シナリオ</td><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td></tr>
<tr><td>2-1</td><td>コントローラーのプログラムを改ざんし、設備の異常動作を発生させる。</td><td>EWS</td><td>コントローラー(生産)</td><td>不正な目標値を送信する。</td></tr>
</table>

表 4-3 攻撃シナリオ一覧表 (2/2)

項番	事業被害	事業被害の概要と攻撃シナリオ					事業被害レベル
3	自家発電システムの停止	発電システムへのサイバー攻撃により、装置に停止・異常動作が発生し、自家発電システムを停止する。自家発電システム復旧まで、購入電力費用が増加する。					2
		シナリオ #	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃	
		3-1	ランサムウェア感染により機器を使用不可となり、安全のためにシステムを停止せざるを得なくさせる。	制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。	
					HMI(発電)		
		3-2	コントローラーのプログラムを改ざんし、設備の異常動作を発生させる。		コントローラー(発電)	不正な制御コマンドを送信する。	

4.2. 外部からの侵入口の検討と選定

外部サービスの導入によって新たに侵入口となりえる資産・ネットワークを洗い出し、分析対象とする侵入口を選定する。侵入口は、事業者管理の資産・ネットワークと、外部サービス、事業者と外部サービス間の通信経路が候補となりえる。それらを図示したのが下図（図 4-2）である。

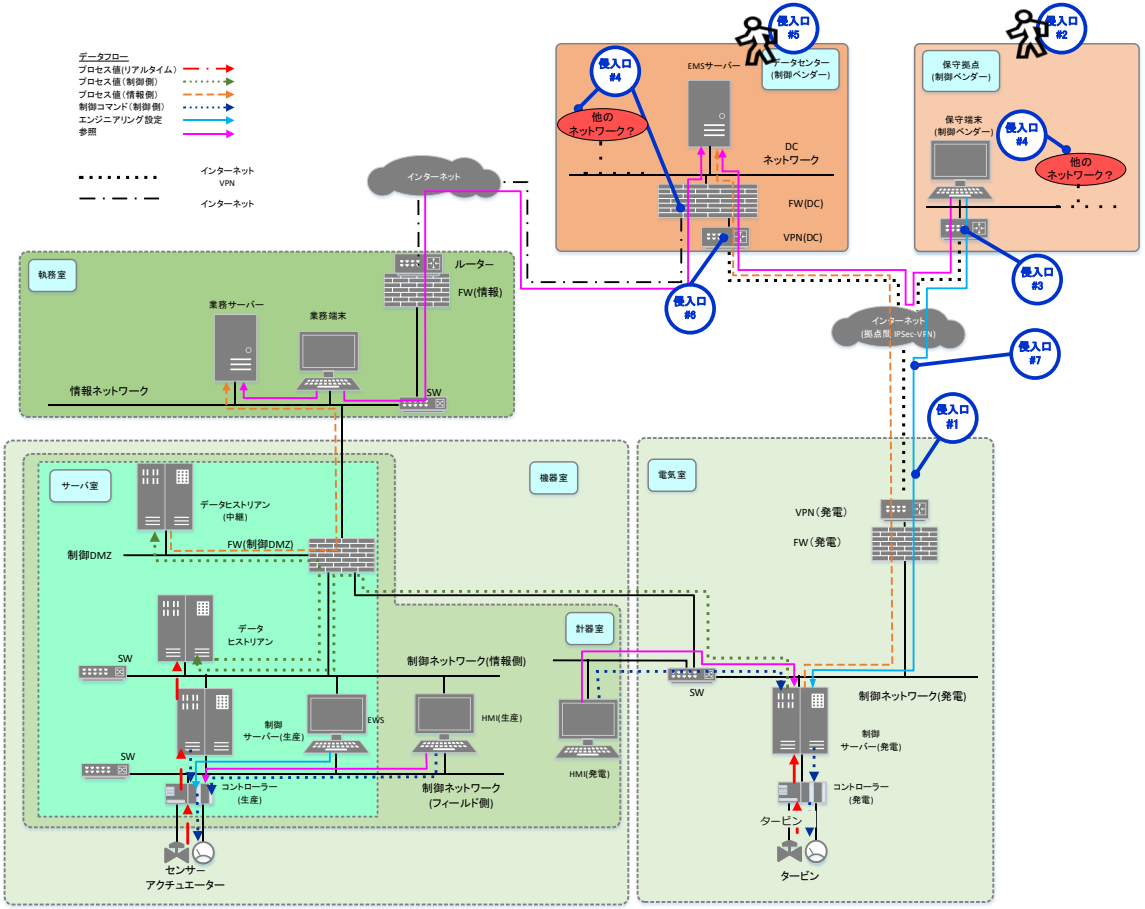


図 4-2 侵入口の候補

これらの侵入口の候補から、リスク分析対象とする侵入口を下表（表 4-4）の通り選定した。

表 4-4 侵入口の検討表

#	侵入口	施設・資産・ネットワーク管理の責任分界	分析対象（〇）
1	VPN(発電)のグローバル IP	事業者	〇
2	ベンダー拠点＜物理的侵入＞	外部サービス提供ベンダー	〇 （侵入口#2,#3 から#4 を経由して制御システムを攻撃すると想定し、侵入口を#4 に統合する）
3	ベンダー拠点の VPN のグローバル IP	外部サービス提供ベンダー	
4	保守端末・保守端末のネットワーク	外部サービス提供ベンダー	
5	データセンター＜物理的侵入＞	外部サービス提供ベンダー	〇 （侵入口#5,#6 から#7 を経由して制御システムを攻撃すると想定し、侵入口を#7 に統合する）
6	データセンターの VPN のグローバル IP	外部サービス提供ベンダー	
7	EMS サーバー・データセンターネットワーク	外部サービス提供ベンダー	
8	インターネットのネットワーク経路	ネットワークサービス提供ベンダー	対象外 （通信の盗聴・改ざんといった脅威を検討すべきだが、分析対象システムにおいて拠点間 IPSec-VPN を利用しているため、脅威を検討しない）
9	情報ネットワーク	事業者	対象外 （既にリスク分析済みであり、また、外部サービス導入により分析対象とすべき侵入口はない）
10	執務室＜物理的侵入＞	事業者	
11	電気室：物理的侵入	事業者	
12	機器室・計器室・計算機室＜物理的侵入＞	事業者	

4.3. 攻撃者と侵入口の検討と選定

4.2 節で選定した侵入口について、攻撃者を検討する。ここでは、「悪意のある第三者」「内部関係者」のレベルで攻撃者を分類し、攻撃者と侵入口による分析範囲を選定した。それを下表（表 4-5）に示す。

表 4-5 攻撃者と侵入口の選定例

#	侵入口	施設・資産・ネットワーク管理の責任分界	攻撃者		
			悪意のある第三者	内部関係者の過失	悪意のある内部関係者
1	VPN(発電)のグローバル IP	事業者	○	× （定常運用がない）	× （認証情報を不正に入手した悪意のある第三者と同等と扱う）
2	保守端末 ベンダー保守拠点のネットワーク	外部サービス提供ベンダー	○	× （過失でマルウェア感染にするシナリオが考えられるが、悪意のある第三者による攻撃と同等と考える）	× （事業者の責任範囲外となるため、外部サービスの契約でリスクを低減するのがよい[8]）
3	EMS サーバー データセンターネットワーク	外部サービス提供ベンダー	○	× （過失でマルウェア感染にするシナリオが考えられるが、悪意のある第三者による攻撃と同等と考える）	× （事業者の責任範囲外となるため、外部サービスの契約でリスクを低減するのがよい）

8 外部サービスのサービス仕様書や契約書等で、“第三者機関によって外部サービスのサイバーセキュリティ品質が定期的に監査されていること“が明示されているか確認する。第三者機関による監査が行われていない場合、監査の要求や外部サービスの変更をすることが望ましい。

4.4. 攻撃ルートの作成

4.1 で作成した攻撃シナリオ一覧を元に、攻撃ルートを作成する。シナリオ番号でまとめた攻撃ルート一覧表（表 4-6）を示す。

表 4-6 攻撃ルート一覧表（シナリオソート版）(1/3)

攻撃シナリオ	攻撃ツリー番号	誰が	どこから	どうやって					
		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
1-1	1-1	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)		データヒストリアン	制御サーバー(生産)	ランサムウェアで機器を利用不能にする。
1-1	1-2	悪意のある第三者	VPN(発電)	制御サーバー(発電)	データヒストリアン(中継)		データヒストリアン	制御サーバー(生産)	ランサムウェアで機器を利用不能にする。
1-1	1-3	悪意のある第三者	EMS サーバー	制御サーバー(発電)	データヒストリアン(中継)		データヒストリアン	制御サーバー(生産)	ランサムウェアで機器を利用不能にする。
1-1	1-4	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)		データヒストリアン	EWS	ランサムウェアで機器を利用不能にする。
1-1	1-5	悪意のある第三者	EMS サーバー	制御サーバー(発電)	データヒストリアン(中継)		データヒストリアン	EWS	ランサムウェアで機器を利用不能にする。
1-1	1-6	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)		データヒストリアン	HMI(生産)	ランサムウェアで機器を利用不能にする。
1-1	1-7	悪意のある第三者	EMS サーバー	制御サーバー(発電)	データヒストリアン(中継)		データヒストリアン	HMI(生産)	ランサムウェアで機器を利用不能にする。
1-2	1-8	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)	データヒストリアン	EWS	コントローラー(生産)	プログラムを改ざんし、設備の異常動作を発生させる。

表 4-6 攻撃ルート一覧表（シナリオソート版）（2/3）

攻撃シナリオ	攻撃ツリー番号	誰が	どこから	どうやって					
		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
1-2	1-9	悪意のある第三者	EMS サーバー	制御サーバー(発電)	データヒストリアン(中継)	データヒストリアン	EWS	コントローラー(生産)	プログラムを改ざんし、設備の異常動作を発生させる。
2-1	2-1	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)	データヒストリアン	EWS	コントローラー(生産)	不正な目標値を送信する。
2-1	2-2	悪意のある第三者	EMS サーバー	制御サーバー(発電)	データヒストリアン(中継)	データヒストリアン	EWS	コントローラー(生産)	不正な目標値を送信する。
2-2	2-3	悪意のある第三者	保守端末(ベンダー拠点)				制御サーバー(発電)	コントローラー(発電)	不正な目標値を送信する。
2-2	2-4	悪意のある第三者	EMS サーバー				制御サーバー(発電)	コントローラー(発電)	不正な目標値を送信する。
3-1	3-1	悪意のある第三者	保守端末(ベンダー拠点)				制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。
3-1	3-2	悪意のある第三者	EMS サーバー				制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。

表 4-6 攻撃ルートー覧表(シナリオソート版) (3/3)

攻撃シナリオ	攻撃ツリー番号	誰が	どこから	どうやって					
		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
3-1	3-3	悪意のある第三者	保守端末(ベンダー拠点)				制御サーバー(発電)	HMI(発電)	ランサムウェアで機器を利用不能にする。
3-1	3-4	悪意のある第三者	EMS サーバー				制御サーバー(発電)	HMI(発電)	ランサムウェアで機器を利用不能にする。
3-2	3-5	悪意のある第三者	保守端末(ベンダー拠点)				制御サーバー(発電)	コントローラー(発電)	不正な目標値を送信する。
3-2	3-6	悪意のある第三者	EMS サーバー				制御サーバー(発電)	コントローラー(発電)	不正な目標値を送信する。

侵入口から攻撃拠点までの攻撃ルートをシステム構成図上で表現した攻撃ルート図を以下に示す(図 4-3)。

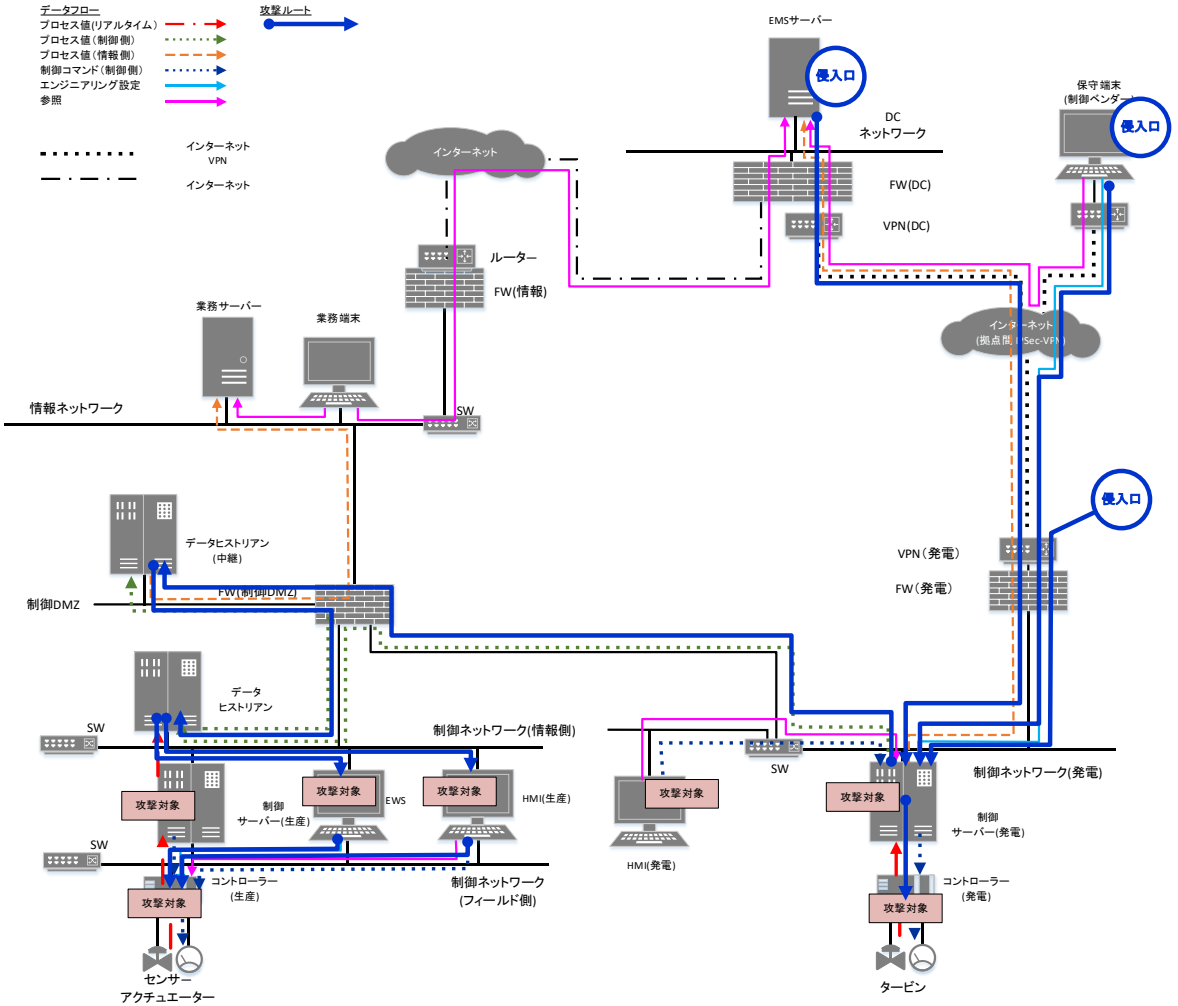


図 4-3 攻撃ルート図

4.5. リスク分析シートの作成

事業被害のリスク分析シートを、73 頁以降に「表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）」として示す。

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(1/9)

1. 生産システムの停止

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	ランサムウェア感染により機器を使用不可となり、安全のためにシステムを停止せざるを得なくさせる。														
1	1-1	**侵入口=保守端末(制御ベンダー)** 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末からEMSサーバーに不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証（ID・パスワード） パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
2		悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」を含む。これらの脅威に対する対策は斜線で表記。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
3		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		3			
4		悪意ある第三者が、制御サーバー(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		1			
5	1-1	悪意ある第三者が、制御サーバー(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	1	3	C	アンチウィルス ホワイトリスト パッチ適用		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	3	#1-1a	1,2,3,4,5
6		悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		1			
7	1-1	悪意ある第三者が、EWSにランサムウェアを感染させ、機器を利用不能にする。	2	1	3	C	アンチウィルス ホワイトリスト パッチ適用		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	3	#1-4a	1,2,3,6,7
8		悪意ある第三者が、HMI(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		1			
9	1-1	悪意ある第三者が、HMI(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	1	3	C	アンチウィルス ホワイトリスト パッチ適用		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	3	#1-6a	1,2,3,8,9
10	1-1	**侵入口=保守端末(制御ベンダー)** 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末からEMSサーバーに不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証（ID・パスワード） パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
11		悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」を含む。これらの脅威に対する対策は斜線で表記。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
12		FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。									IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1	○ ○ ○	2			
13		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
14		悪意ある第三者が、制御サーバー(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		1			
15	1-1	悪意ある第三者が、制御サーバー(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	2	3	B	アンチウィルス ホワイトリスト パッチ適用		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	2	#1-1b	10,11,12,13,14,15
16		悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		1			
17	1-1	悪意ある第三者が、EWSにランサムウェアを感染させ、機器を利用不能にする。	2	2	3	B	アンチウィルス ホワイトリスト パッチ適用		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	2	#1-4b	10,11,12,13,16,17
18	1-1	悪意ある第三者が、HMI(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	2	3	B	アンチウィルス ホワイトリスト パッチ適用		権限管理 アクセス制御 （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	2	#1-6b	10,11,12,13,14,18
19		**侵入口=VPN(発電)** 悪意ある第三者が、VPN(発電)に不正アクセスをする。					FW 通信相手の認証（固定IPアドレス、IPSec、IKE 事前共有キー） 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 *機器死活監視*	 ○ ○ ○	3			
20		悪意ある第三者が、VPN(発電)に侵入し脆弱性を悪用しEMSサーバーへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(発電) 通信相手の認証（ID・パスワード） パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		3			
21		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
22		悪意ある第三者が、制御サーバー(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		3			
23		悪意ある第三者が、制御サーバー(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		1			
24	1-1	悪意ある第三者が、制御サーバー(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	1	3	C	アンチウィルス ホワイトリスト パッチ適用		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	3	#1-2	19,20,21,22,23,24

委託先ベンダーのネットワーク経由で不正アクセスされる事例はいくつかあるため、脅威レベルは2とした。

データヒストリアンからデータヒストリアン（中継）へセッションを張る通信がFWで許可されていないため、攻撃ステップ#3を成立させるための難易度が高い。

委託先ベンダーのネットワーク経由で不正アクセスされる事例はいくつかあるため、脅威レベルは2とした。

FWの設定の技術的、業務的なレビューは実施していないものとした。

IPSec-VPNのIK事前共有キーが漏洩して、VPNに不正アクセスされるリスクはあるものとした。

IPSec-IKEはメインモードで運用され、登録された固定IPアドレス以外からはVPNにアクセスできない。

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(2/9)

1. 生産システムの停止

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	ランサムウェア感染により機器を使用不可となり、安全のためにシステムを停止せざるを得なくさせる。												

25		侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。 悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○ ○	 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			3			
26		悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
27		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			3			
28		悪意ある第三者が、制御サーバー(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
29	1-1	悪意ある第三者が、制御サーバー(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	1	3	C	アンチウィルス ホワイトリスト パッチ適用		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	3	#1-3a	25,26,27,28,29
30		悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
31	1-1	悪意ある第三者が、EWSにランサムウェアを感染させ、機器を利用不能にする。	2	1	3	C	アンチウィルス ホワイトリスト パッチ適用		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	3	#1-5a	25,26,27,30,31
32		悪意ある第三者が、HMI(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
33	1-1	悪意ある第三者が、HMI(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	1	3	C	アンチウィルス ホワイトリスト パッチ適用		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	3	#1-7a	25,26,27,32,33
34		FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。					 				IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1			1			
35		侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。 悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○	 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
36		悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
37		FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。					 				IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1	○ ○ ○		2			
38		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	 ○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
39		悪意ある第三者が、制御サーバー(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
40	1-1	悪意ある第三者が、制御サーバー(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	2	3	B	アンチウィルス ホワイトリスト パッチ適用		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	2	#1-3b	35,36,37,38,39,40
41		悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
42	1-1	悪意ある第三者が、EWSにランサムウェアを感染させ、機器を利用不能にする。	2	2	3	B	アンチウィルス ホワイトリスト パッチ適用		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	2	#1-5b	35,36,37,38,39,41,42
43		悪意ある第三者が、HMI(生産)の脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
44	1-1	悪意ある第三者が、HMI(生産)にランサムウェアを感染させ、機器を利用不能にする。	2	2	3	B	アンチウィルス ホワイトリスト パッチ適用		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	2	#1-7b	35,36,37,38,39,43,44
X																	

委託先ベンダーのネットワーク経由で不正アクセスされる事例はいくつかあるため、脅威レベルは2とした。

制御サーバー（発電）が外部からのアクセスがFWで禁止されている。データヒストリアンからデータヒストリアン（中継）へセッションを張る通信がFWで許可されていないため、攻撃ステップ83を成立させるための難易度が高い。

委託先ベンダーのネットワーク経由で不正アクセスされる事例はいくつかあるため、脅威レベルは2とした。

FWの設定の技術的、業務的なレビューは実施していないものとした。

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(3/9)

1. 生産システムの停止

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							
	1-2	コントローラーのプログラムを改ざんし、設備の異常動作を発生させる。													
45	1-2	**侵入口=保守端末(制御ベンダー)** 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末からEMSサーバーに不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○	 *権限管理* 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			2			
46	1-2	悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」を含む。これらの脅威に対する対策は斜線で表記。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			2			
47	1-2	悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
48	1-2	悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
49	1-2	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	1	3	C	権限管理 アクセス制御 データ署名	 アクセス制御 データ署名	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	3	#1-8a	45,46,47,48,49
50	1-2	**侵入口=保守端末(制御ベンダー)** 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末からEMSサーバーに不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○	 *権限管理* 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			2			
51	1-2	悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」を含む。これらの脅威に対する対策は斜線で表記。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			2			
52	1-2	FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1	○ ○ ○		2			
53	1-2	悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	 ○ ○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			2			
54	1-2	悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
55	1-2	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	2	3	C	権限管理 アクセス制御 データ署名	 アクセス制御 データ署名	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	2	#1-8b	50,51,52,53,54,55
56	1-2	侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーから制御サーバー(発電)へ不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○ ○	 *権限管理*	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
57	1-2	悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			2			
58	1-2	悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
59	1-2	悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
60	1-2	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	1	3	C	権限管理 アクセス制御 データ署名	 アクセス制御 データ署名	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	3	#1-9a	56,57,58,59,60

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(4/9)

1. 生産システムの停止

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									
	1-2	コントローラーのプログラムを改ざんし、設備の異常動作を発生させる。																
61		FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。									IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1				1			
62		侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。 悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」（特権昇格）を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証（ID・パスワード） パッチ適用 脆弱性回避 *権限管理*	 ○ 			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				2			
63		悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ 			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				2			
64		FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。									IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1	○ ○ ○			2			
65		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	 ○ ○ 			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				2			
66		悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ 			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				1			
67	1-2	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	2	3	C	権限管理 アクセス制御 データ署名	 	権限管理 アクセス制御 データ署名		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	2	#1-9b	61,62,63,64,65,66,67
X																		

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(5/9)

2. 基準値を超えた環境汚染物質の流出

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								
	2-1	生産システムのコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。														
68	2-1	**侵入口=保守端末(制御ベンダー)** 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末からEMSサーバーに不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) ○ 通信相手の認証（ID・パスワード） ○ パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*				2			
69	2-1	悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」を含む。これらの脅威に対する対策は斜線で表記。					FW(DMZ) ○ 通信相手の認証 パッチ適用 ○ 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				2			
70	2-1	悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) ○ 通信相手の認証 ○ パッチ適用 ○ 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				3			
71	2-1	悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 ○ パッチ適用 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				1			
72	2-1	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	1	2	D	権限管理 アクセス制御 データ署名	権限管理 アクセス制御 データ署名	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 フェールセーフ設計	○ ○	1	3	#2-1a	68,69,70,71,72
73	2-1	**侵入口=保守端末(制御ベンダー)** 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末からEMSサーバーに不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) ○ 通信相手の認証（ID・パスワード） ○ パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*				2			
74	2-1	悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」を含む。これらの脅威に対する対策は斜線で表記。					FW(DMZ) ○ 通信相手の認証 パッチ適用 ○ 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				2			
75	2-1	FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ○ ログ収集・分析 ○ 統合ログ管理システム ○ 設定監査※1				2			
76	2-1	悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 ○ パッチ適用 ○ 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				2			
77	2-1	悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 ○ パッチ適用 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				1			
78	2-1	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	2	2	D	権限管理 アクセス制御 データ署名	権限管理 アクセス制御 データ署名	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 フェールセーフ設計	○ ○	1	2	#2-1b	73,74,75,76,77,78

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(6/9)

2. 基準値を超えた環境汚染物質の流出

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						
	2-1	生産システムのコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。												
79		侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。 悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○ ○	 *権限管理*	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			3			
80		悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
81		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			3			
82		悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ 	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
83	2-1	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	1	2	D	権限管理 アクセス制御 データ署名	 アクセス制御 データ署名	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 ○ フェールセーフ設計 ○	1	3	#2-2a	79,80,81,82,83
84		FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1		1			
85		侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。 悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	 ○ 	 *権限管理*	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
86		悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
87		FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ○ ログ収集・分析 ○ 統合ログ管理システム ○ 設定監査※1		2			
88		悪意ある第三者が、脆弱性を悪用しデータヒストリアン（中継）へ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	 ○ ○ 	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
89		悪意ある第三者が、EWSの脆弱性を悪用し不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ 	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1			
90	2-1	悪意ある第三者が、EWSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	2	2	D	権限管理 アクセス制御 データ署名	 アクセス制御 データ署名	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 ○ フェールセーフ設計 ○	1	2	#2-2b	84,85,86,87,88,89,90
X														

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(7/9)

2. 基準値を超えた環境汚染物質の流出

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		防御 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	攻撃ツリー番号 攻撃ツリー番号	構成ステップ（項番）
	2-2	発電システムのコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。																
91	2-2	**侵入口=保守端末(制御ベンダー)** 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末から制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○		*権限管理*	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
92	2-2	悪意ある第三者が、制御サーバー(発電)からコントローラー(発電)のプログラムを改ざんし、設備の異常動作を発生させる。	1	3	2	C	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	1	#2-3a	91,92
93	2-2	侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○ ○		*権限管理*	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			3			
94	2-2	悪意ある第三者が、制御サーバー(発電)からコントローラー(発電)のプログラムを改ざんし、設備の異常動作を発生させる。	1	1	2	D	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	3	#2-4a	93,94
95	2-2	FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。									IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1				1			
96	2-2	侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○		*権限管理*	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2			
97	2-2	悪意ある第三者が、制御サーバー(発電)からコントローラー(発電)のプログラムを改ざんし、設備の異常動作を発生させる。	1	2	2	D	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	2	#2-4b	96,97
X																		

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(8/9)

3. 自家発電システムの停止

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		防御 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	攻撃ツリー番号 攻撃ツリー番号	構成ステップ（項番）
	3-1	ランサムウェア感染により機器を使用不可となり、安全のためにシステムを停止せざるを得なくさせる。																
99	3-1	侵入口=保守端末(制御ベンダー) 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末から制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*			2			
100	3-1	悪意ある第三者が、制御サーバー(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	3	2	B	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	1	#3-1a	99,100
101	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	3	2	B	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	1	#3-3a	99,101
102	3-1	侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*			3			
103	3-1	悪意ある第三者が、脆弱性を悪用しデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					FW(DMZ) 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*				2			
104	3-1	悪意ある第三者が、制御サーバー(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	1	2	D	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	3	#3-2a	102,104
105	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	1	2	D	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	3	#3-4a	102,105
106	3-1	FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。									IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1				1			
107	3-1	侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*			2			
108	3-1	悪意ある第三者が、制御サーバー(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	2	2	C	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	2	#3-2b	107,108
109	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	2	2	C	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	2	#3-4b	107,109
X																		

表 4-7 事業被害ベースのリスク分析シート（シナリオソート版）(9/9)

3. 自家発電システムの停止

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		防御 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	攻撃ツリー番号 攻撃ツリー番号	構成ステップ（項番）
	3-2	コントローラーのプログラムを改ざんし、設備の異常動作を発生させる。																
110	3-2	侵入口=保守端末(制御ベンダー) 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末から制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*			2			
111	3-2	悪意ある第三者が、EMSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	3	2	C	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	1	#3-5a	110,111
112	3-2	侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○ ○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*			3			
113	3-2	悪意ある第三者が、EMSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	1	2	D	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	3	#3-6a	112,113
114	3-2	FW(DMZ)の設定不備により、本来アクセスを禁止しているデータヒストリアン（中継）のサービスにDMZ側からアクセスできる状態である。									IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1				1			
115	3-2	侵入口=EMSサーバー 悪意ある第三者が、何らかの手段でEMSサーバーに不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理*	○			IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* *権限管理*			2			
116	3-2	悪意ある第三者が、EMSからコントローラーのプログラムを改ざんし、設備の異常動作を発生させる。	1	2	2	D	権限管理 アクセス制御 データ署名		権限管理 アクセス制御 データ署名		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 フェールセーフ設計	○ ○	1	2	#3-6b	115,116
X																		

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

設備の異常動作を発生させるほどのプログラムによる攻撃の脅威は低いとした。

4.6. リスク値のまとめ

事業被害ベースのリスク分析を実施し、外部サービスと制御システムが接続したことに起因するリスク値を以下の表にまとめた(表 4-8)。

表 4-8 事業被害ベースのリスク分析結果 リスク値まとめ表

リスク値	合計 攻撃ツリー数	事業被害シナリオ		攻撃ツリー数 (事業シナリオ毎)
A	0	(なし)		0
B	8	1	生産システムの停止	6
		2	基準値を超えた環境汚染物質の流出	2
C	15	1	生産システムの停止	11
		2	基準値を超えた環境汚染物質の流出	1
		3	自家発電システムの停止	3
D	10	2	基準値を超えた環境汚染物質の流出	6
		3	自家発電システムの停止	4
E	0	(なし)		0
合計	33			33

また、侵入口ベースでリスク値をまとめた例を以下に示す(表 4-9)。

表 4-9 事業被害ベースのリスク分析結果 リスク値まとめ表(侵入口ベース)

#	リスク値	侵入口	攻撃ツリー数	合計 攻撃ツリー数
1	A	(なし)	0	0
2	B	保守端末(ベンダー拠点)	5	8
3		EMS サーバー	3	
4	C	保守端末(ベンダー拠点)	7	15
5		VPN	1	
6		EMS サーバー	7	
7	D	保守端末(ベンダー拠点)	2	10
8		EMS サーバー	8	
9	E	(なし)	0	0
合計			33	33

5. リスク分析の活用

5.1. リスク低減効果の検討

本節では、事業被害ベースのリスク分析結果からリスク値が高い B と C の攻撃ツリーについて、攻撃ツリーの脆弱性レベルが不十分なもの（脆弱性レベル 2 と 3 と評価）について、リスクを低減するために攻撃ツリーの脆弱性レベルを低減するための対策案を検討する。

ただし、セキュリティ防御策による**リスク値低減**を行っても、サイバー攻撃により高い事業被害が引き起こされる**リスクそのものがなくなるわけではない**ことに留意が必要である。

【作業 5.1①】共通の攻撃ルートを持つ攻撃ツリーをまとめる。

以下の表は、事業被害ベースのリスク分析で攻撃ツリーのうち、リスク値が高いBとCの攻撃ツリーについて、攻撃ツリーの脆弱性レベルが不十分なもの（脆弱性レベル2と3と評価）について、共通の攻撃者と侵入口となる攻撃ツリーでまとめたものである。

表 5-1 共通の攻撃ルートを持つ攻撃ツリーによるまとめ

		誰が	どこから		どうやって							対策前			
攻撃ツリー番号#	シナリオ番号#	攻撃者	侵入口	経由1	経由2	経由3	経由4	経由5	攻撃拠点	攻撃対象	最終攻撃	脅威	脆弱性	事業被害	リスク値
1-1	#1-1b	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>			データヒストリアン	制御サーバー(生産)	ランサムウェアで機器を利用不能にする。	2	2	3	B
1-1	#1-4b	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>			データヒストリアン	EWS	ランサムウェアで機器を利用不能にする。	2	2	3	B
1-1	#1-6b	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>			データヒストリアン	HMI(生産)	ランサムウェアで機器を利用不能にする。	2	2	3	B
1-2	#1-8b	悪意のある第三者	保守端末(ベンダー拠点)	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>	データヒストリアン		EWS	コントローラー(生産)	プログラムを改ざんし、設備の異常動作を発生させる。	1	2	3	C
2-2	#2-3a	悪意のある第三者	保守端末(ベンダー拠点)						制御サーバー(発電)	制御サーバー(発電)	不正な目標値を送信する。	1	3	2	C
3-1	#3-1a	悪意のある第三者	保守端末(ベンダー拠点)						制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。	2	3	2	B
3-1	#3-3a	悪意のある第三者	保守端末(ベンダー拠点)						制御サーバー(発電)	HMI(発電)	ランサムウェアで機器を利用不能にする。	2	3	2	B
3-2	#3-5a	悪意のある第三者	保守端末(ベンダー拠点)						制御サーバー(発電)	コントローラー(発電)	プログラムを改ざんし、設備の異常動作を発生させる。	1	3	2	C
1-1	#1-3b	悪意のある第三者	EMSサーバー(リモート)	<FW(リモート)の設定不備>	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>		データヒストリアン	制御サーバー(生産)	ランサムウェアで機器を利用不能にする。	2	2	3	B
1-1	#1-5b	悪意のある第三者	EMSサーバー(リモート)	<FW(リモート)の設定不備>	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>		データヒストリアン	EWS	ランサムウェアで機器を利用不能にする。	2	2	3	B
1-1	#1-7b	悪意のある第三者	EMSサーバー(リモート)	<FW(リモート)の設定不備>	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>		データヒストリアン	HMI(生産)	ランサムウェアで機器を利用不能にする。	2	2	3	B
1-2	#1-9b	悪意のある第三者	EMSサーバー(リモート)	<FW(リモート)の設定不備>	制御サーバー(発電)	データヒストリアン(中継)	<FW(制御DMZ)の設定不備>	データヒストリアン	EWS	コントローラー(生産)	プログラムを改ざんし、設備の異常動作を発生させる。	1	2	3	C
3-1	#3-2b	悪意のある第三者	EMSサーバー(リモート)	<FW(リモート)の設定不備>					制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。	2	2	2	C
3-1	#3-4b	悪意のある第三者	EMSサーバー(リモート)	<FW(リモート)の設定不備>					制御サーバー(発電)	HMI(発電)	ランサムウェアで機器を利用不能にする。	2	2	2	C

【作業 5.1②】①でまとめた攻撃ツリーのリスク値を低減可能な追加対策を検討する。

前表に登場する、侵入口～経由～攻撃拠点～攻撃対象の資産、もしくは資産が配置されたネットワークにおいて、脆弱性の緩和のための設定や構成の変更、運用の変更や導入等を検討する。

以下の表に、リスク低減のためのセキュリティ緩和策をまとめた。

表 5-2 リスク低減のためのセキュリティ緩和策の例 (1/2)

#	対象攻撃ステップ	現状の攻撃ツリーリスク値(表 4-9 と対応)	対策資産	現状の対策 (対象となる脅威への対策)	追加対策(対策の改善案、強化策)	追加対策後の 攻撃ツリー リスク値
1	・FW(制御 DMZ)の設定不備 ・データヒストリアン(中継)からデータヒストリアンへの不正アクセス	B(対策レベル 2)：6 C(対策レベル 2)：1	FW(制御 DMZ)	IPS/IDS、ログ収集分析、統合ログ管理システム	・設定変更内容のレビューや定期的な設定監査等の実施 ※「9.4 節 ファイアウォールにおける各種設定」を参照して実施することが望ましい。	**B→C** **(対策レベル 2→3)：6** C→C (対策レベル 2→3)：1
2	・FW(発電)の設定不備 ・EMS サーバーから制御サーバー(発電)への不正アクセス	B(対策レベル 2)：3 C(対策レベル 2)：3	FW (発電)	なし	・設定変更内容のレビューや定期的な設定監査の実施 ・SIEM を利用した統合ログ管理システムの導入等 ※「9.4 節 ファイアウォールにおける各種設定」を参照・して実施することが望ましい。	**B→C** **(対策レベル 2→3)：3** C→C (対策レベル 2→3)：1 **C→D** **(対策レベル 2→3)：2**

表 5-2 リスク低減のためのセキュリティ緩和策の例 (2/2)

#	対象攻撃ステップ	現状の攻撃ツリーリスク値(表 4-9 と対応)	対策資産	現状の対策 （対象となる脅威への対策）	追加対策（対策の改善案、強化策）	追加対策後の 攻撃ツリー リスク値
3	保守端末（ベンダー拠点）から制御サーバー(発電)への不正アクセス	B(対策レベル 1)：2 C(対策レベル 1)：2	制御サーバー （発電）	通信相手の認証 （ID・パスワード）	・案（１）または（２）の実施 案（１）：保守端末から直接アクセスさせる踏み台用のサーバーを別途設置し、認証踏み台サーバーへのアクセスに多要素認証を設定する。 案（２）：制御サーバー(発電)への対策実施 - 保守端末から制御サーバー(発電)への多要素認証 -リモート管理サービスの停止やログイン ID の無効化などにより、事業者の承認なしにリモート管理を不可とする。 ・脆弱性パッチの適用 ・不要なサービスの削除等のハードニング ・リモート管理操作ログの取得や監査の実施	**B→C** **(対策レベル 1→2)：2** **C→D** **(対策レベル 1→2)：2**
4	保守端末（ベンダー拠点）から制御サーバー(発電)への不正アクセス	B(対策レベル 1)：2 C(対策レベル 1)：2	保守端末 （ベンダー拠点）	通信相手の認証 （ID・パスワード）	・リモート接続のセキュリティに関する契約の見直し 【保守用 PC の常時起動・ネットワーク常時接続の禁止など】	**B→C** **(対策レベル 1→2)：2** **C→D** **(対策レベル 1→2)：2**
5	EWS でコントローラー(生産)のプログラムを改ざんする	B(対策レベル 1)：2	EWS	なし	・常時エンジニアリングモード運用の是正。エンジニアリングが不要な際に、エンジニアリングモードをオフにする。	**B→C** **(対策レベル 2→1)：2**

5.2. リスク低減策の実施計画の検討

前節で検討したリスク低減のためのセキュリティ緩和策について、導入に必要なコストや難易度、あるいは制御システムの運用に与える影響度を考慮して、実施計画を検討する。その際、制御システムを停止する定修期間に合わせた実施計画などの短中期的観点や、制御システムのリプレースを見据えた中長期的観点でも改善時期を考慮する。

表 5-3 セキュリティ緩和策実施計画の検討例 (1/2)

対策No	対策資産	追加のセキュリティ緩和策	推定対策コスト	難易度	運用への影響	改善実施
1	FW(制御 DMZ)	設定変更内容のレビューや定期的な設定監査等	低	低	低	即時実施
2	FW (発電)	設定変更内容のレビューや定期的な設定監査等	低	低	低	即時実施
		情報ネットワーク経由での常時監視	低	低	低	情報システム部門との調整後に実施
3	踏み台サーバー（新規）	保守端末から直接アクセスさせる踏み台用のサーバーを別途設置	中	低	低	中期的計画（ベンダーとの調整が必要）
4	制御サーバー (発電)	多要素認証、ハードニング	中	低	中	見送り
5	制御サーバー (発電)	脆弱性パッチ	低	中	中	短中期的計画（ベンダーとの調整が必要）
6	制御サーバー (発電)	不要な場合はリモート操作を無効化（手動）	低	低	中	短期的計画（ベンダーとの調整が必要）
7	制御サーバー (発電)	リモート管理操作ログの取得や監査をする。	低	低	低	即時実施

表 5-3 セキュリティ緩和策実施計画の検討例 (2/2)

対策No	対策資産	追加のセキュリティ緩和策	推定対策コスト	難易度	運用への影響	改善実施
8	保守端末（ベンダー拠点）	リモート接続に関するセキュリティに関する契約の見直し	低	中	低	中期的計画 （社外保守会社との調整が必要）
9	EWS	常時エンジニアリングモードの運用の是正	低	低	中	見送り

5.3. リスク低減効果の把握

対策実施前と実施後でリスク値がどのように変わるかをまとめる。対策実施前と後でのツリーのリスク値の分布を以下に示す（表 5-4）。

表 5-4 事業被害ベースのリスク分析結果 リスク値まとめ表

リスク値	事業被害シナリオ		攻撃ツリー数		改善後 攻撃ツリー数	
A	（なし）		0	0	0	0
B	1	生産システムの停止	8	6	2	0
	2	基準値を超えた環境汚染物質の流出		2		2
C	1	生産システムの停止	15	11	21	17
	2	基準値を超えた環境汚染物質の流出		1		1
	3	自家発電システムの停止		3		1
D	2	基準値を超えた環境汚染物質の流出	10	6	12	6
	3	自家発電システムの停止		4		6
E	（なし）		0	0	0	0
合計			33	33	33	33

侵入口ベースでリスク値（A,B）をまとめた例を以下に示す（表 5-5）。

表 5-5 事業被害ベースのリスク分析結果 リスク値まとめ表（侵入口ベース）

#	リスク値	侵入口	攻撃ツリー数	改善後 攻撃ツリー数
1	A	（なし）	0	0
2	B	保守端末(ベンダー拠点）	5	2
3		EMS サーバー	3	0
4	C	保守端末(ベンダー拠点）	7	10
5		VPN(発電)	1	1
6		EMS サーバー	7	8
7	D	保守端末(ベンダー拠点）	2	2
8		EMS サーバー	8	10
9	E	（なし）	0	0
合計			33	33

付録 A. 資産ベースのリスク分析実施結果

別途 Excel ファイル形式で提供している。

付録 B1. 事業被害ベースのリスク分析実施結果 シナリオソート版

別途 Excel ファイル形式で提供している。また、攻撃ツリーの脅威レベルの判断理由をセルのコメントで記載している。

付録 B2. 事業被害ベースのリスク分析実施結果 侵入口ソート版

別途 Excel ファイル形式で提供している。また、攻撃ツリーの脅威レベルの判断理由をセルのコメントで記載している。

付録 C. モバイル閉域網とインターネット VPN を組み合わせた外部接続の事例

制御システム（特に IoT 機器）から情報を収集・利用する通信形態として、キャリア回線（モバイル回線）を利用した閉域網を経由して制御システムから情報を収集し、クラウド上のサービスまたは事業者や制御ベンダーの保守拠点に情報を集約する方式がある。

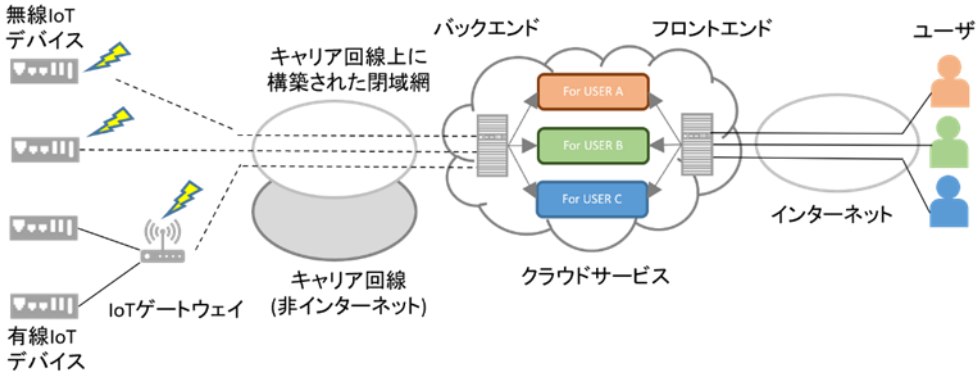


図 C-1「スマート工場のセキュリティリスク分析調査報告書[9]」より

この方式の特徴は、制御システムもしくは IoT デバイスがモバイル閉域網へ接続することでインターネットからの直接脅威にさらされないこと、モバイル閉域網とその先のシステムとは様々な接続方法が選択可能なことである。

ここでは、前図の方式を採用しているもしくは検討している事業者のセキュリティリスク分析の参考となるよう、リスク分析対象システムの"外部接続方法を前図の方式に変更したリスク分析例"を一部提示する。

- 提示するアウトプット
  - システム構成例
  - データフロー例
  - 侵入口と攻撃ルート例
  - 事業被害ベースのリスク分析シート記入例（一部）

9 「スマート工場のセキュリティリスク分析調査」調査報告書 第 2 版 P86
https://www.ipa.go.jp/security/controlsystem/controlsystem-smartplant.html

- システム構成図

  システム構成図を以下に示す(図 C-2)。青破線で囲まれている箇所が変更された資産とネットワーク構成となる。

  - 事業者の制御システムは、非インターネットのモバイル網[10]によって「モバイルサービスベンダー」と接続する。「モバイルサービスベンダー」と「ベンダーデータセンター」は、インターネット VPN で接続されている。

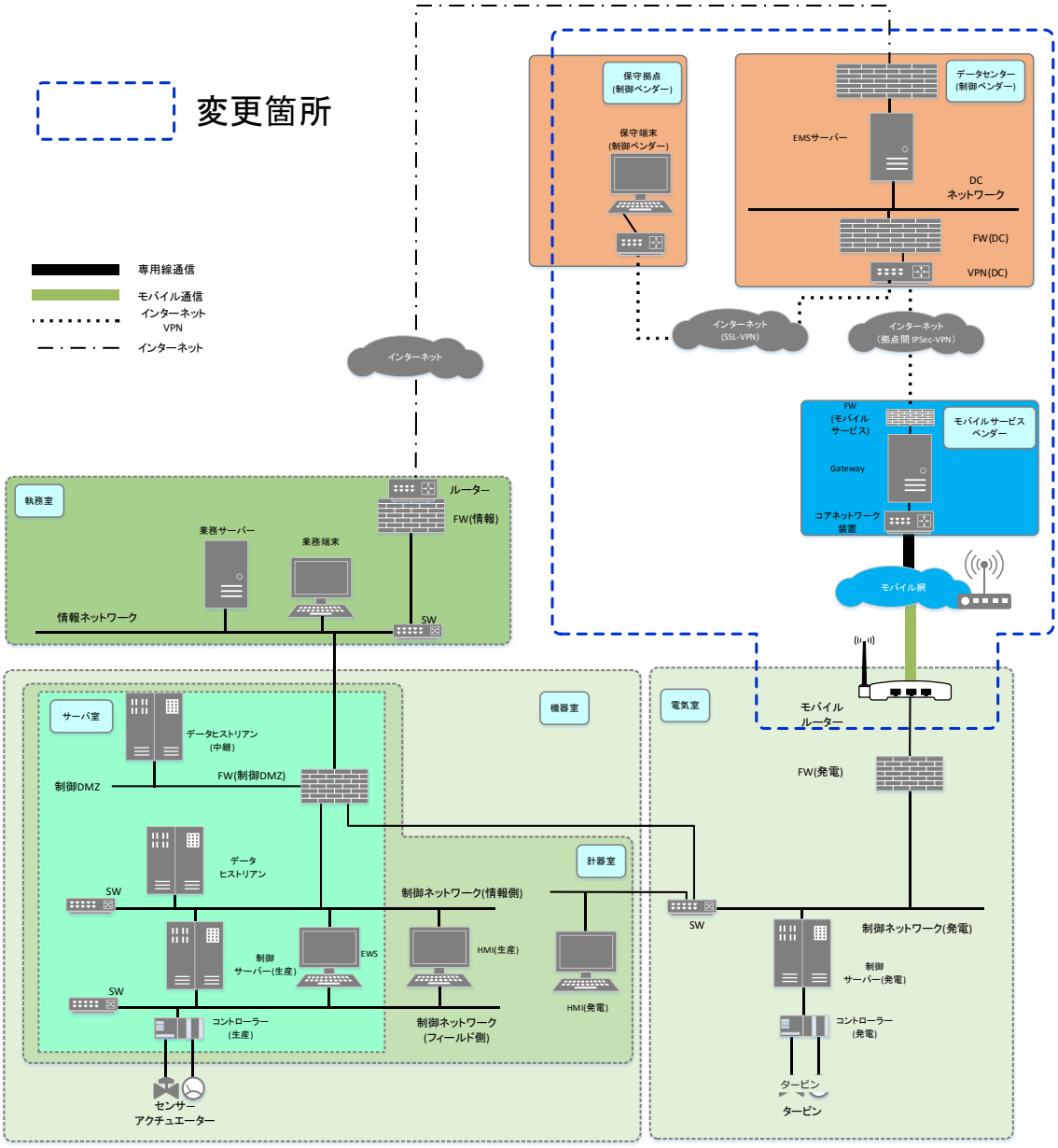


図 C-2 システム構成例

10 モバイルルーターとモバイル網が無線通信で、モバイル網からモバイルサービスベンダーのコアネットワーク装置は専用線などの接続と想定する。

- データフロー
  - 制御システムから外部へのデータフローは、制御サーバー（発電）のプロセス値をモバイルルーター経由で EMS サーバーに送信がある。
  - 外部から制御システムへのデータフローはない。[11]

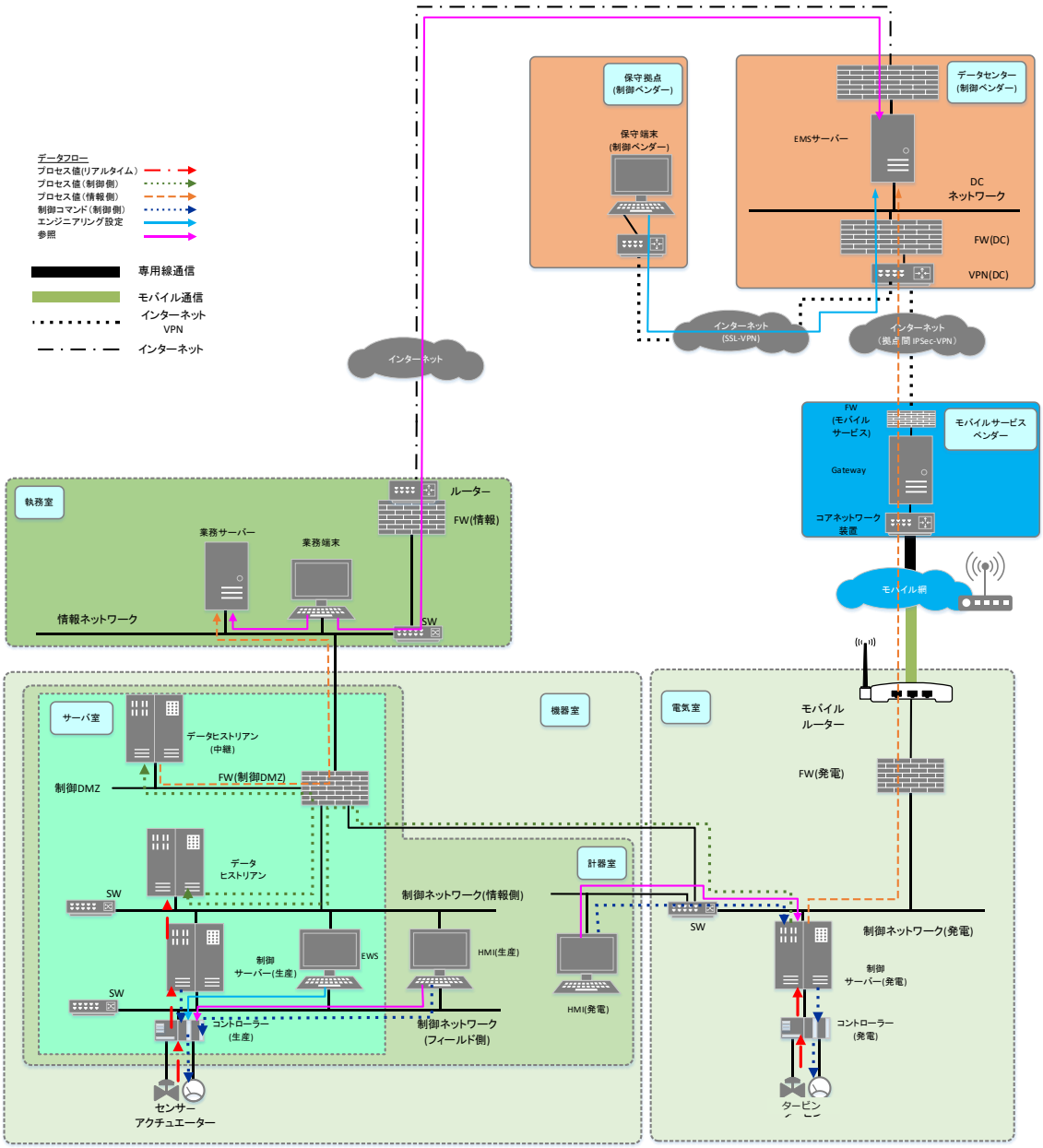


図 C-3 データフロー

11 事業者の制御システムにあるモバイルルーターは外部から遠隔でファームウェアの変更や設定変更が可能な機能を持つことがある。事業者がこのようなシステムを導入する際は、モバイルルーターが外部から遠隔操作可能な状態かを確認することを推奨する。

- 侵入口と攻撃ルート

  外部サービスの導入によって新たに侵入口となりえる資産・ネットワークを洗い出し、分析対象とする侵入口を選定する。

表 C-1 侵入口となる資産・ネットワークと分析対象の検討表

#	侵入口	施設・資産・ネットワーク管理の 責任分界	分析対象
1	モバイルルーター	資産管理：事業者 資産・ネットワーク：モバイルサービス提供ベンダー	× （閉域網のため）
2	モバイル網	モバイルサービスベンダー	× （閉域網のため）
3	モバイルサービスベンダー Gateway 等	モバイルサービスベンダー	○
4	モバイルサービスベンダー側のグローバル IP	モバイルサービスベンダー	○
5	保守端末・保守端末のネットワーク	外部サービスのベンダー	○
6	データセンターの VPN のグローバル IP	外部サービスのベンダー	○
7	EMS サーバー・データセンターネットワーク	外部サービスのベンダー	○

最も攻撃ルートが短くなる攻撃シナリオ 3-1 について考察する。攻撃シナリオ 3-1 の攻撃ルート表を以下に示す(表 C-2)。

表 C-2 攻撃ルートの検討表

攻撃シナリオ#	攻撃ツリー#	誰が	どこから	どうやって						
		攻撃者	侵入口	経由 1	経由 2	経由 3	経由 4	攻撃拠点	攻撃対象	最終攻撃
3-1	3-1	悪意のある第三者	保守端末(ベンダー拠点)	EMS サーバー	<FW(発電)>			制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。
3-1	3-2	悪意のある第三者	VPN(DC)	EMS サーバー	<FW(発電)>			制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。
3-1	3-3	悪意のある第三者	EMS サーバー	<FW(発電)>				制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。
3-1	3-4	悪意のある第三者	Gateway (VPN 側)[12]	<FW(発電)>				制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。
3-1	3-5	悪意のある第三者	Gateway (内部側)[13]	<FW(発電)>				制御サーバー(発電)	制御サーバー(発電)	ランサムウェアで機器を利用不能にする。

[12] Gateway(VPN 側): モバイルサービス提供ベンダー の Gateway のもつインターフェースのうち、外部ベンダーの VPN と接続しているインターフェースを示す。
[13] Gateway(内部側): モバイルサービス提供ベンダーの Gateway のもつインターフェースのうち、内部ネットワークと接続しているインターフェースを示す。

侵入口と攻撃ルート例を図示したものを以下に示す(図 C-4)。

閉域網を含む制御システムの外部ネットワークと制御ネットワーク(発電)の間に FW(発電)が設置されており、FW(発電)が外部ネットワークから制御ネットワークへの接続が禁止されているものとする。ファイアウォールが適切に設定されている場合は、サイバー攻撃を成立されるのは困難だが、FW(発電)の設定ミスといった条件の下ではサイバー攻撃の可能性がある。

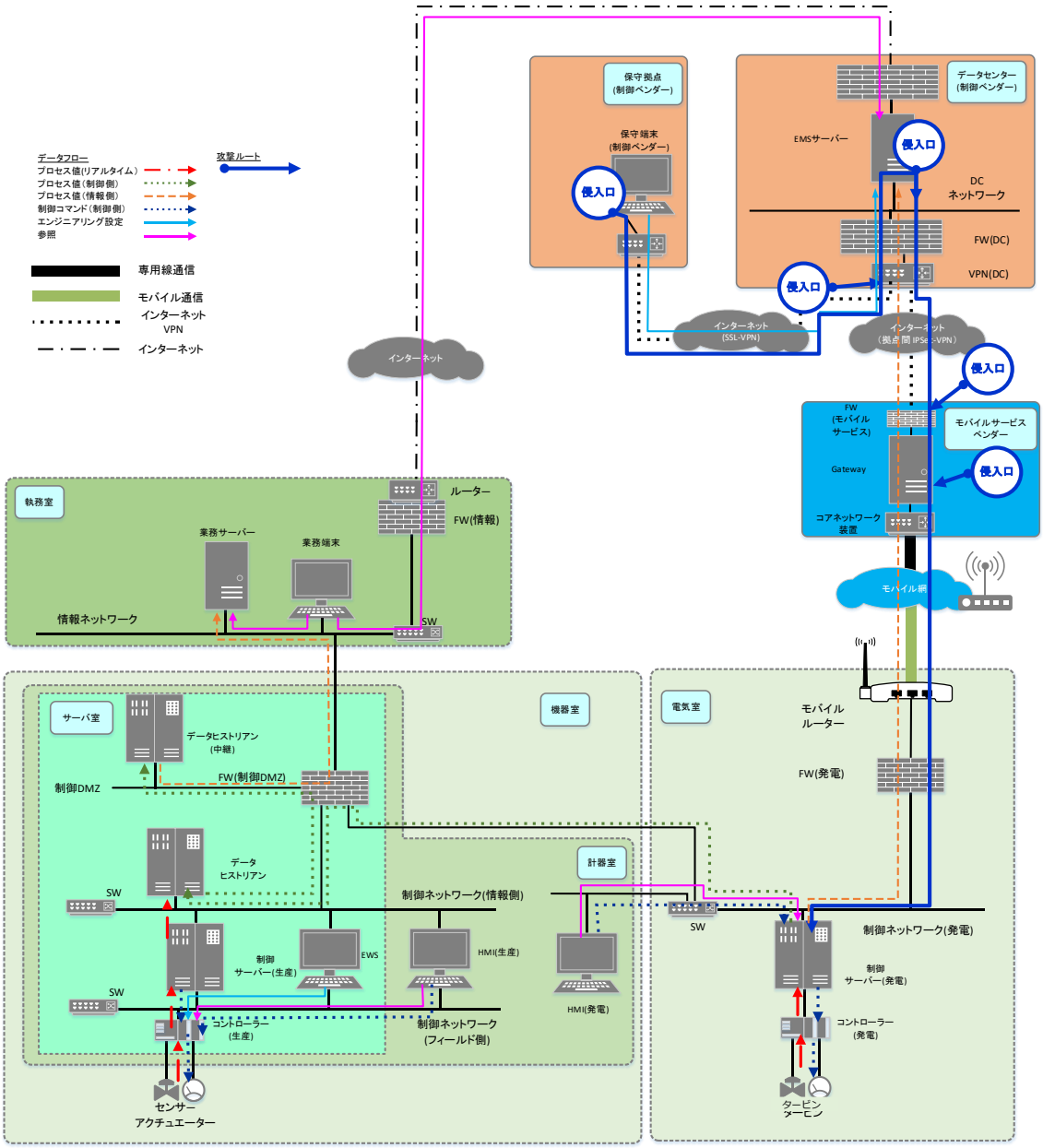


図 C-4 侵入口と攻撃ルート例

- 事業被害ベースのリスク分析シート
  別途 Excel ファイル形式でも提供している。

表 C-3 事業被害ベースのリスク分析実施例

3. 自家発電システムの停止

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							
	3-1	ランサムウェア感染により機器を使用不可となり、安全のためにシステムを停止せざるを得なくさせる。													
1		侵入口=保守端末(ベンダー拠点) 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意ある第三者が、保守端末から正規の権限でEMSサーバーに不正アクセスする。					ベンダー拠点、EMSサーバーのセキュリティは不明のため、対策ならびに攻撃ステップの対策レベルの評価はしない。								
2		悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○ *権限管理* 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
3	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	1	2	D	権限管理 アクセス制御 データ署名	権限管理 アクセス制御 データ署名	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 フェールセーフ設計	○ ○	1	3	#3-1a	1,2,3
4		侵入口=VPN(DC) 悪意ある第三者が、VPN(DC)に脆弱性を悪用して不正アクセスをしたものとする。悪意ある第三者が、EMSサーバーへ不正アクセスする。					VPN（DC）、EMSサーバーのセキュリティは不明のため、対策ならびに攻撃ステップの対策レベルの評価はしない。								
5		悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○ *権限管理* 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
6	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	1	2	D	権限管理 アクセス制御 データ署名	権限管理 アクセス制御 データ署名	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 フェールセーフ設計	○ ○	1	3	#3-2a	4,5,6
7		侵入口=EMSサーバー 悪意ある第三者が、EMSサーバーに脆弱性を悪用して不正アクセスをしたものとする。悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○ *権限管理* 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
8	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	1	2	D	権限管理 アクセス制御 データ署名 *ホワイトリスト*	権限管理 アクセス制御 データ署名	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 フェールセーフ設計	○ ○	3	3	#3-3a	7,8
9		侵入口=Gateway(VPN) 悪意ある第三者が、Gateway(VPN)に脆弱性を悪用して不正アクセスをしたものとする。悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○ *権限管理* 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
10	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	1	2	D	権限管理 アクセス制御 データ署名 *ホワイトリスト*	権限管理 アクセス制御 データ署名	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 フェールセーフ設計	○ ○	3	3	#3-4a	9,10
11		侵入口=Gateway（内部） 悪意ある第三者が、EMSサーバーに脆弱性を悪用して不正アクセスをしたものとする。悪意ある第三者が、Gateway（内部）から制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					FW(発電) 通信相手の認証(ID・パスワード) パッチ適用 脆弱性回避 *権限管理* *アンチウイルス* *ホワイトリスト*	○ ○ *権限管理* 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視* 			3			
12	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	2	1	2	D	権限管理 アクセス制御 データ署名 *ホワイトリスト*	権限管理 アクセス制御 データ署名	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 フェールセーフ設計	○ ○	3	3	#3-5a	11,12
X															

表 C-3 事業被害ベースのリスク分析実施例 (2/2)

3. 自家発電システムの停止

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						
	3-1	ランサムウェア感染により機器を使用不可となり、安全のためにシステムを停止せざるを得なくさせる。												
1		侵入口=保守端末(ベンダー拠点) 悪意ある第三者が、何らかの手段でベンダー拠点の保守端末に不正アクセスをしたものとする。悪意のある第三者が、保守端末から正規の権限でEMSサーバーに不正アクセスする。					ベンダー拠点、EMSサーバーのセキュリティは不明のため、対策ならびに攻撃ステップの対策レベルの評価はしない。							
2		FW(発電)の設定不備により、本来アクセスを禁止している外部から制御サーバー(発電)のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1		1			
3		悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					**FW(発電)** 通信相手の認証(ID・パスワード) ○ パッチ適用 脆弱性回避 *権限管理* *権限管理* *アンチウイルス* *ホワイトリスト*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
4	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	**2**	2	2	C	権限管理 アクセス制御 データ署名	権限管理 アクセス制御 データ署名	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 ○ フェールセーフ設計 ○	1	2	#3-1b	1,2,3,4
5		侵入口=VPN(DC) 悪意ある第三者が、VPN(DC)に脆弱性を悪用して不正アクセスをしたものとする。悪意のある第三者が、EMSサーバーへ不正アクセスする。					VPN(DC)、EMSサーバーのセキュリティは不明のため、対策ならびに攻撃ステップの対策レベルの評価はしない。							
6		FW(発電)の設定不備により、本来アクセスを禁止している外部から制御サーバー(発電)のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1		1			
7		悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					**FW(発電)** 通信相手の認証(ID・パスワード) ○ パッチ適用 脆弱性回避 *権限管理* *権限管理* *アンチウイルス* *ホワイトリスト*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
8	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	**2**	2	2	C	権限管理 アクセス制御 データ署名	権限管理 アクセス制御 データ署名	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 ○ フェールセーフ設計 ○	1	2	#3-2b	5,6,7,8
9		侵入口=EMSサーバー 悪意ある第三者が、EMSサーバーに脆弱性を悪用して不正アクセスをしたものとする。悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					**FW(発電)** 通信相手の認証(ID・パスワード) ○ パッチ適用 脆弱性回避 *権限管理* *権限管理* *アンチウイルス* *ホワイトリスト*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
10		FW(発電)の設定不備により、本来アクセスを禁止している外部から制御サーバー(発電)のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1		1			
11	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	**2**	2	2	C	権限管理 アクセス制御 データ署名 *ホワイトリスト*	権限管理 アクセス制御 データ署名	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 ○ フェールセーフ設計 ○	2	2	#3-3b	9,10,11
12		侵入口=Gateway(VPN) 悪意ある第三者が、Gateway(VPN)に脆弱性を悪用して不正アクセスをしたものとする。悪意ある第三者が、EMSサーバーから制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					**FW(発電)** 通信相手の認証(ID・パスワード) ○ パッチ適用 脆弱性回避 *権限管理* *権限管理* *アンチウイルス* *ホワイトリスト*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
13		FW(発電)の設定不備により、本来アクセスを禁止している外部から制御サーバー(発電)のサービスにDMZ側からアクセスできる状態である。							IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1		1			
14	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	**2**	2	2	C	権限管理 アクセス制御 データ署名 *ホワイトリスト*	権限管理 アクセス制御 データ署名	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 ○ フェールセーフ設計 ○	2	2	#3-4b	12,13,14
15		侵入口=Gateway(内部) 悪意ある第三者が、EMSサーバーに脆弱性を悪用して不正アクセスをしたものとする。悪意ある第三者が、Gateway(内部)から制御サーバー(発電)に不正アクセスする。 ※遠隔操作を可能とするための「プロセス不正実行」「マルウェア感染」を含む。これらの脅威に対する対策は斜線で表記。					**FW(発電)** 通信相手の認証(ID・パスワード) ○ パッチ適用 脆弱性回避 *権限管理* *権限管理* *アンチウイルス* *ホワイトリスト*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
16									IPS/IDS ログ収集・分析 統合ログ管理システム 設定監査※1		1			
17	3-1	悪意ある第三者が、HMI(発電)にランサムウェアを感染させ、機器を利用不能にする。	**2**	2	2	C	権限管理 アクセス制御 データ署名 *ホワイトリスト*	権限管理 アクセス制御 データ署名	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 ○ フェールセーフ設計 ○	2	2	#3-5b	15,16,17
X														

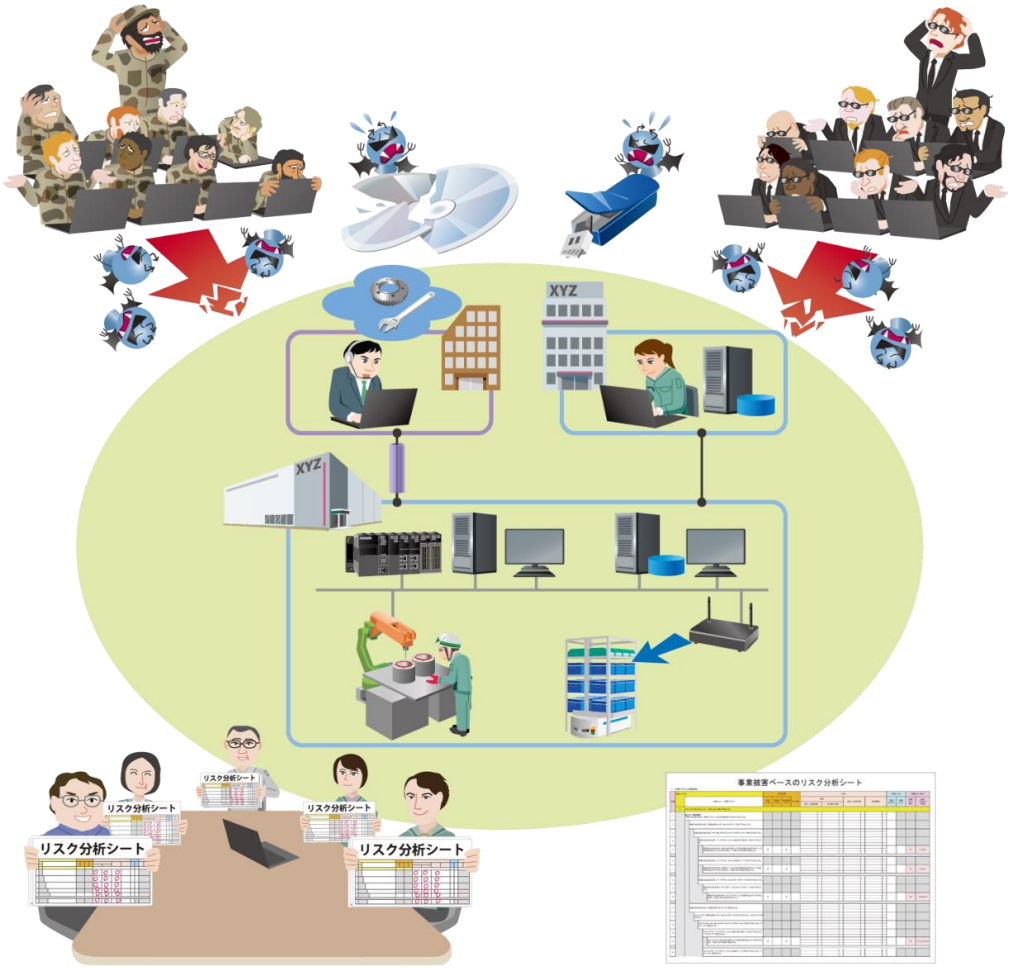
このページは空白です。

更新履歴

2024 年 12 月 16 日	初版
2026 年 4 月 6 日	表紙タイトルを修正、はじめにを追加、その他記載ミスの修正

本書は、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



独立行政法人情報処理推進機構
セキュリティセンター

〒107-0052
東京都港区赤坂２丁目４番６号
赤坂グリーンクロス　25 階
https://www.ipa.go.jp/security/