ICSCoE_TLP:WHITE/CLEAR【第7期】

制御システムへのリモートアクセスに関する セキュリティ対策指南書

2024 年 7 月

独立行政法人情報処理推進機構

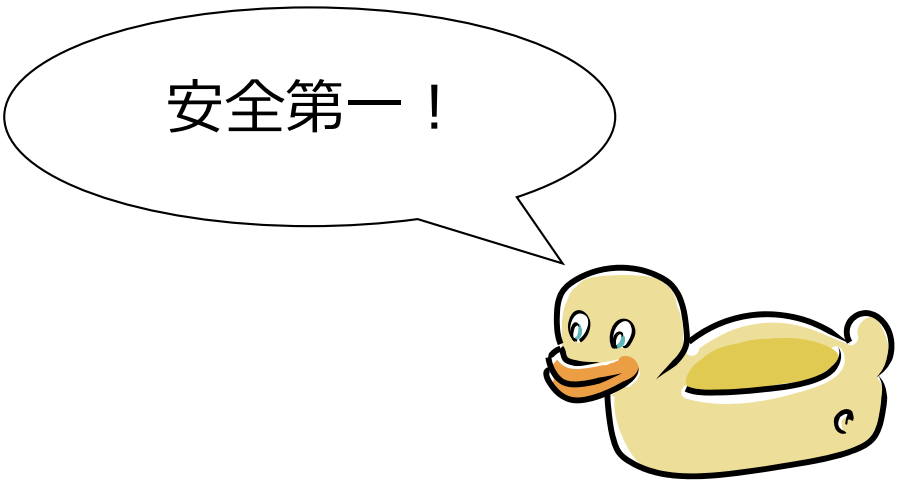
産業サイバーセキュリティセンター

中核人材育成プログラム 第 7 期受講生 卒業プロジェクト

「安全第一！ リモートＯ＆Ｍ＋セキュリティ」

改訂履歴

版数	発行日	改訂内容
第 1 版	2024 年 6 月 17 日	初版発行（TLP_GREEN）
第 2 版	2024 年 6 月 25 日	文書校正、図表差替え
第 3 版	2024 年 7 月 31 日	誤記修正、TLP 変更（TLP_CLEAR）



目次

はじめに

近年、国内の労働人口の減少や柔軟な働き方へのニーズの高まりなど、社会情勢の変化が産業システム全体にも影響を与えています。また従来、外部のネットワークと隔離されていた OT システムも、情報通信技術の進化と社会情勢の変化によりその状況が大きく変わってきています。これらの変化に伴い、工場やプラントの OT システムにおいてもリモートオペレーション（遠隔操作）やリモートメンテナンス（遠隔保守）のニーズが拡大しています。

リモートモニタリング（遠隔監視）がプロセス情報をデータヒストリアンなどに蓄え、遠隔で監視することが一般的であるのに対し、リモートオペレーションやリモートメンテナンスは実際にシステムの操作や設定変更を行うものであり、OT システムの中核をなす制御システムの深い階層までアクセスする必要があります。そのため、そのアクセス経路からセキュリティインシデントが発生すると、直接的に生産活動に影響を与えるリスクが伴うことから、セキュリティ対策は事業の継続性と安全性の確保に直結する重要な要素となります。

本書ではリモートオペレーションとリモートメンテナンスを総称して「リモート O&M（Remote Operation & Maintenance）」と呼ぶことにし、制御システムを取り扱う技術者やセキュリティ担当者を対象に、このリモート O&M を「安全第一」に実施するためのセキュリティ対策をまとめたものです。基本的なリモートアクセス方式から始まり、リスク分析手法、各種ガイドラインから整理したセキュリティ対策を紹介し、事例をあげながらシステム構成を決定するまでの検討プロセスを示しています。

本書を活用いただき、技術者たちが直面するセキュリティ課題に対処し、より安全で効率的な運用環境を構築するための一助となればと考えています。

第1章 本書について

1.1 本書の目的

本書は、制御システムの技術者やセキュリティ担当者向けに、リモート O&M（Remote Operations & Maintenance）のためのセキュリティ対策等をまとめたものである。制御システムへのリモートアクセス環境を構築する場合や、基本的なシステム構成を検討し仕様書に必要事項を記載する際の参考資料として活用してもらうことを目的とする。

1.2 本書の構成

本書は以下の章で構成されている。

- 第 1 章「本書について」では、本書の目的、構成、想定読者、利用規約について記載する。
- 第 2 章「企業アンケートから見えてくる課題」では、アンケート結果から制御システムにおけるリモートアクセスのニーズや課題などを記載する。
- 第 3 章「リモートアクセス方式」では、制御システムで利用され得る代表的なリモートアクセス方式を記載する。なお、通信回線をはじめとする情報通信技術について知見がない方は先に付録 A「リモートアクセスの基本技術」を参照されたい。
- 第 4 章「制御システムにおけるリスク分析手法」では、制御システムにおける代表的なリスク分析手法とリスク管理のフレームワークについて記載する。
- 第 5 章「リモートアクセスにおけるセキュリティ対策」では、リモート O&M を実施する制御システムにおけるセキュリティ対策の推奨事項を記載する。
- 第 6 章「要件定義に基づくシステム構成検討プロセス」では、リモート O&M を実施するための基本的なシステム構成を検討する際に、どのようなプロセスでシステム構成を決定する必要があるか具体例を交えながら記載する。
- 第 7 章「事例検証」では、簡易的な模擬プラントでセキュリティ対策とその効果について検証を実施したため、その内容を記載する。
- 第 8 章「まとめ」では、本書のまとめを記載する。
- 付録 A「リモートアクセスの基本技術」ではリモート O&M 時に利用される基本的な情報通信技術を記載する。
- 付録 B「リモートアクセスに関連するサイバーインシデント事例」ではリモートアクセスに関連したインシデント事例を記載する。
- 付録 C「用語集」では用語の定義と解説を記載する。

・ 付録 D「引用・参考文献」では引用・参考にした文献や資料を記載する。

1.3 想定読者

本書の読者は、以下の企業または組織に属する制御システムの技術者やセキュリティ担当者を想定している。ただし、想定の読者以外にも知見を得られるような内容や表現としている。

表 1-1：本書の想定読者像

組織	対象企業	・ 制御システムを保有し制御システムに対してリモート O&M を実施している、または計画している企業（※） ・ 制御システムに対して HMI などの GUI（Graphical User Interface）機能を利用してリモート O&M を実施している、または計画している企業
	企業のセキュリティリソース	・ 制御システムに対するセキュリティ対策の必要性を認識している企業 ・ 外部委託も含めて“必要な”セキュリティ予算・人材を捻出できる企業
人	対象者	・ 上記企業に属する制御システムの技術者やセキュリティ担当者
	セキュリティリテラシー	・ 「適切に…」等の読者に解釈を委ねるような抽象的なセキュリティ要求だけでは、対応すべき内容がわからない
	OT/IT リテラシー	・ ICS・PLC・DCS・HMI・SCADA・EWS 等の基本的な制御システムの用語については仕組みを理解している ・ VPN・フィルタリング・アンチウイルス等の基本的な IT 用語は聞いたことがあり利用シーンはイメージできるが、仕組みとしては理解していない

※設定変更や操作を伴わない“遠隔監視”のみを実施している、または計画している企業は、システム構成やセキュリティ対策のアプローチが異なるため対象外

1.4 利用規約

1.4.1 著作権及びその他すべての知的所有権

・ 本書に関する著作権およびその他すべての知的所有権は、独立行政法人情報処理推進機構 産業サイバーセキュリティセンター中核人材育成プログラムにおける第 7 期受講生 卒業プロジェクト「安全第一！ リモート O＆M＋セキュリティ」のプロジェクトメンバー（以下、作成者）に帰属する。

・ 作成者の許可なく、本資料の記載内容を複写、転載することを禁止する。

1.4.2 免責事項

・ 本書は単に情報として提供され、内容は予告なしに変更される場合がある。本書に誤りが無いことの保証や、商品性又は特定目的への適合性の黙示的な保証や条件を含め明示的又は黙示的な保証や

条件は一切無いものとする。

- 本書に記載の内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、作成者の見解に基づいている。
- 本書の利用によるトラブルに対し、作成者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は、発行日から２年間とする。

第2章　企業アンケートから見えてくる課題

2.1　　アンケートの概要

2.1.1　目的

制御システムを有する企業に対してリモートアクセスの実施状況、利用目的、管理状況等について、実態把握を目的に企業アンケートを実施した。

2.1.2　調査対象

企業アンケートは、中核人材育成プログラムに参加経験のある企業の制御システム部署またはセキュリティ部署に対して、WEB 形式によるアンケートを実施した。

なお、中核人材育成プログラムは、独立行政法人情報処理推進機構の産業サイバーセキュリティセンターが主催する 1 年間のトレーニングプログラムであり、社会インフラや産業基盤のサイバーセキュリティ対策の強化を図っている企業を対象とし、経営層と現場担当者を繋ぐ中核人材を育成するものである。

2.2　　アンケートの結果と分析

企業アンケートは 50 社から有効回答を得ることができ、そのうち制御システムを有する会社は 42 社であった。個別の回答および結果を踏まえた分析について以下に記載する。

(1) 制御システムへのリモートアクセス実施状況

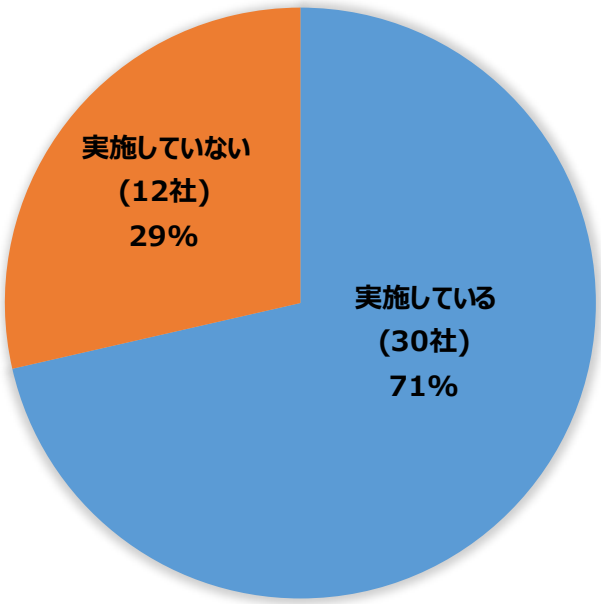


図 2-1：制御システムへのリモートアクセス実施状況ヒアリング結果 (N=42)

回答結果より、約 70％の会社で制御システムへのリモートアクセスを実施または計画していることが判明した。なお、「いいえ」と回答した 12 社に対して実施していない理由を確認したところ、9 社が「セキュリティ上の懸念がある」と回答いただいた。即ち、セキュリティに関する懸念が無ければ約 90%の企業がリモートアクセスを導入または計画している可能性が高く、制御システムへのリモートアクセスのニーズは非常に高いことが分かる。

(2) 制御システムへのリモートアクセス実施目的

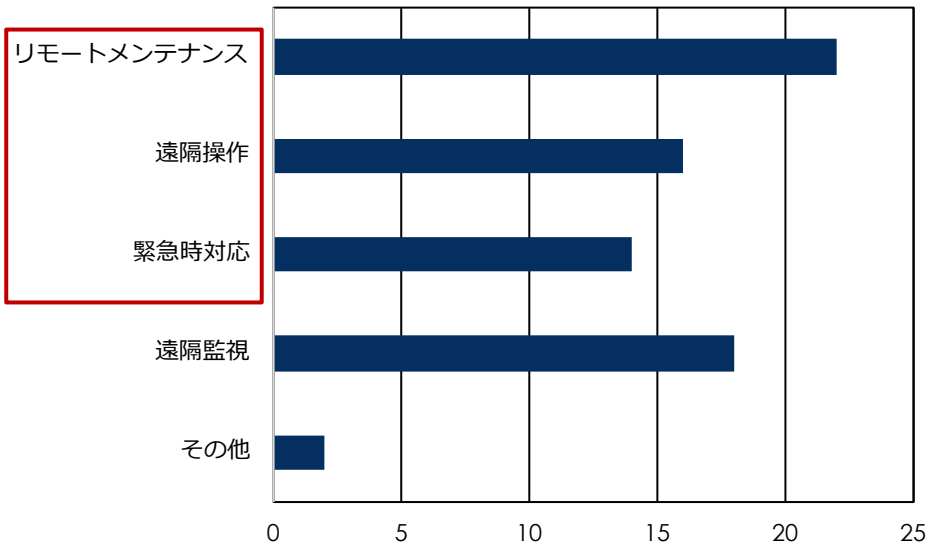


図 2-2：制御システムへのリモートアクセス実施目的 (N=30) (複数回答可)

回答結果より、リモートメンテナンスで利用している事業者が最も多く(約 70％)、遠隔操作や緊急時対応も半数近くの事業者で利用されていた。遠隔監視に対するニーズも 60％程度あるが、緊急時対応も含めた操作やメンテナンスといった制御システムの深い階層までアクセスする必要があるリモートO&M(リモートメンテナンス、遠隔操作、緊急時対応)のニーズを多くの企業が抱えていることが分かる。

(3) 制御システムへのリモートアクセス管理部門

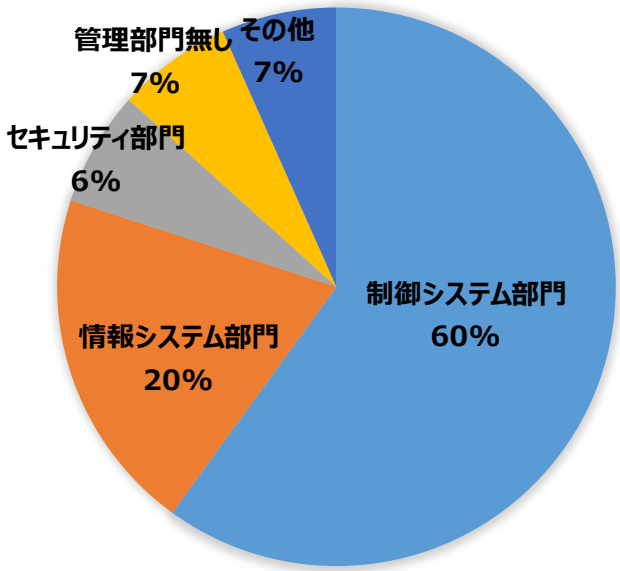


図 2-3：制御システムへのリモートアクセス管理部門 (N=30)

回答結果より、60%の事業者にて制御システムを有する OT システム部門が管理していることが分かった。さらに、管理部門無しも合わせると 3 分の 2 以上の事業者で情報システム部門やセキュリティ部門といった IT 関連部門以外が管理していることが分かる。IT 技術やセキュリティに長けていない組織・部門が管理していることから、セキュリティ対策を十分に実装できない、または実装の方法がわからない等の課題が考えられる。

(4) 制御システムへのリモートアクセス環境構築時の社内ルール

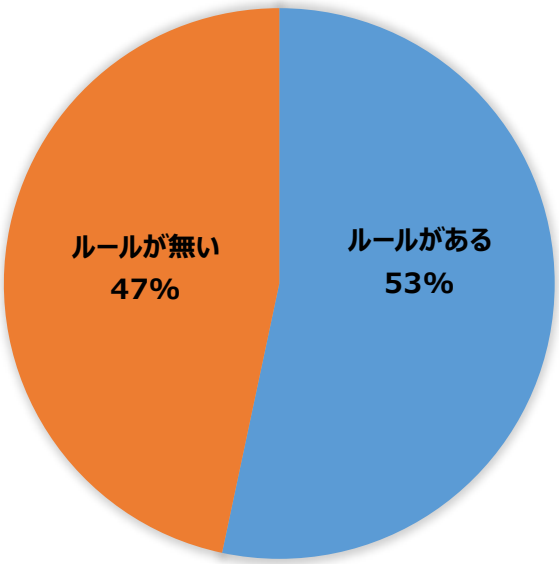


図 2-4：制御システムへのリモートアクセス環境構築時の社内ルール有無 (N=30)

回答結果より、ルールが存在しない事業者が半数近くを占めていることが判明した。前述の(3)と踏まえると、セキュリティ部署ではない制御システムを有する OT システム部署が管理しており、構築する際の社内ルールが存在していないことから、十分なセキュリティ対策が実装されていない可能性が高いと考えられる。

(5) 制御システムへのリモートアクセス利用時に使用している回線

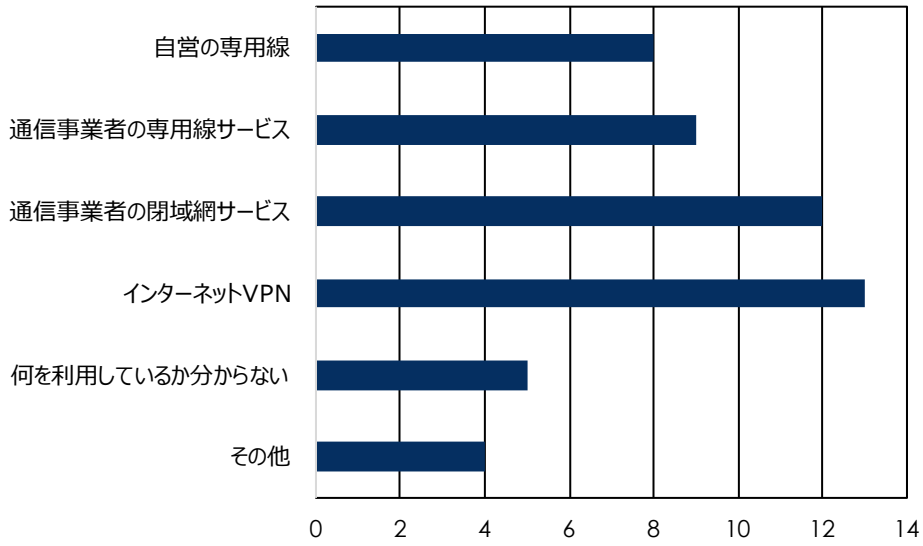


図 2-5：制御システムへのリモートアクセス利用時に使用している回線 (N=30) (複数回答可)

上記結果から、制御システムへリモートアクセスする際には様々な通信回線が用いられていることが分かる。制御システムの重要度や規模に応じて様々な回線が選択されていると考えられる。なお、各通信回線の違いについては「付録 A リモートアクセスの基本技術」を参照されたい。

(6) 制御システムへのリモートアクセスに起因するセキュリティインシデント

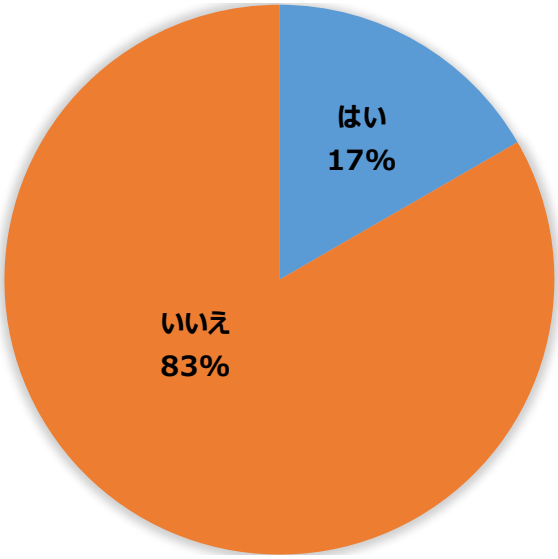


図 2-6：制御システムへのリモートアクセスに起因するセキュリティインシデント経験の有無 (N=30)

この結果から、30 社中 5 社が制御システムに関してリモートアクセスに起因するセキュリティインシデントを経験したことがあることが判明した。割合としては 17%とそこまで高い数字ではないが、重要インフラ事業者を含む企業の 17%が制御システムに対して何かしらのセキュリティインシデントを経験していることを考えると、決して軽視できない結果といえる。このように制御システムに対するサイバー攻撃も一定数の事業者が被害を受けているという実態を踏まえ、適切なセキュリティ対策を実装していくことが非常に重要となってくる。

2.3 アンケートの総括

アンケート結果およびそれぞれの傾向を分析した結果、多くの企業が制御システムへのリモート O&M を実施しており、様々な回線を利用していることが分かった。一方、管理主体の過半数が、制御システム部門等の IT 技術やセキュリティ技術に関する知識が十分ではないと考えられる組織であり、かつリモートアクセス環境構築時の社内ルールが無い会社が半数近くを占めていた。また制御システムへのリモートアクセスを起因としたセキュリティインシデントも発生していることが判明した。

これらの結果から、リモート O&M のセキュリティ対策の重要性が浮き彫りになった。制御システムの技術者やセキュリティ担当者が、リモートアクセス環境の構築や基本的なシステム構成を検討する際に、本書の内容が有用であることが期待される。

第3章 リモートアクセス方式

3.1 リモートアクセス方式の全体像

コロナ禍以降、企業における一般的な業務形態の一つとしてテレワークが定着してきているが、テレワークも社内の IT システムへリモートアクセスすることで実現されている。IT システムでは多くの製品やサービスが充実していることから、テレワークも様々な方式がある。

一方で制御システムへのリモートアクセスについては制御システムの本体である制御装置（PLC や DCS など）は現場で稼働しており、遠隔地からのリモート O&M を実施する場合には現場で操作する場合と同等の再現性が求められる。そのため、テレワークで利用されるリモートアクセスの方式が同様に適用されるわけでない。なお、本書における「現場」とは、制御システムが設置され、その指令によって産業機械などが稼働する場所を指し、「遠隔地」とは現場の外にあり、物理的に離れた場所でリモート O&M を行うための場所全般を指すものとする。

本章では、制御システムの特性を考慮し、制御システムで利用され得る代表的なリモートアクセス方式として「プライベートネットワーク方式」「リモートデスクトップ方式」「仮想デスクトップ方式」の 3 つに分類して紹介する。下図に紹介するリモートアクセス方式の関係図を示す。関係の詳細については次節以降で説明するため、本関係図と照らし合わせて確認されたい。

なお、利用目的によっては複数の拠点間を接続させ、複数の利用者がリモートアクセスする場合もあるが、本章では「制御システムがある現場」と「遠隔地」を 1 対 1 の関係としてリモートアクセス方式を紹介することに留める。利用目的および要件定義に基づくリモートアクセス方式の選択、組合せなどの検討プロセスについては「第 6 章 要件定義に基づくシステム構成検討プロセス」で記載する。

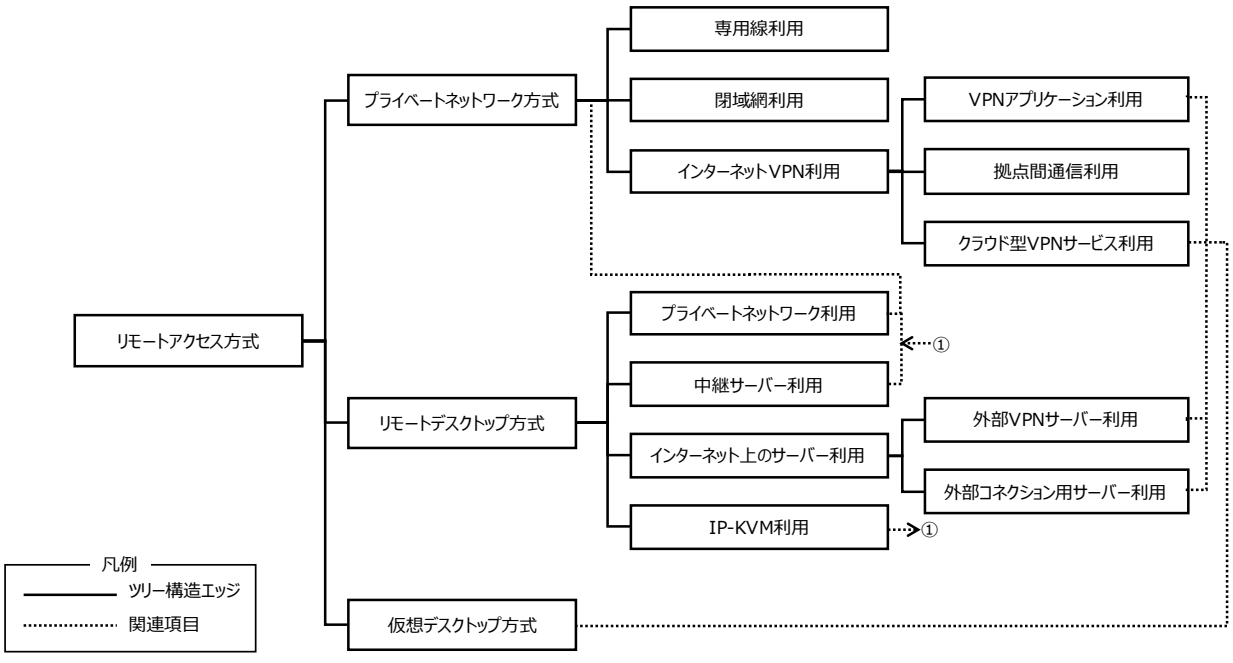


図 3-1：本書で紹介する代表的なリモートアクセス方式の関係図

3.2　プライベートネットワーク方式

プライベートネットワークを経由して、制御装置へ直接アクセスするプライベートネットワーク方式を紹介する。なお、プライベートネットワークについては「付録 A リモートアクセスの基本技術」を参照されたい。

プライベートネットワーク方式は現場の制御装置と、遠隔地に設置されたリモートアクセス端末をプライベートネットワークで接続し、リモート O&M を実施する方式である。これにより、遠隔地のリモートアクセス端末が物理的に現場のネットワーク内にある場合と同様に現場の制御装置へ指令を出すことが可能となり、制御装置がある現場で HMI/EWS 端末を操作する際と同等の再現性を得ることができる。しかしながら、遠隔地のリモートアクセス端末上にデータが保存される場合もあるため、端末の紛失や盗難による情報漏えいリスクがある。

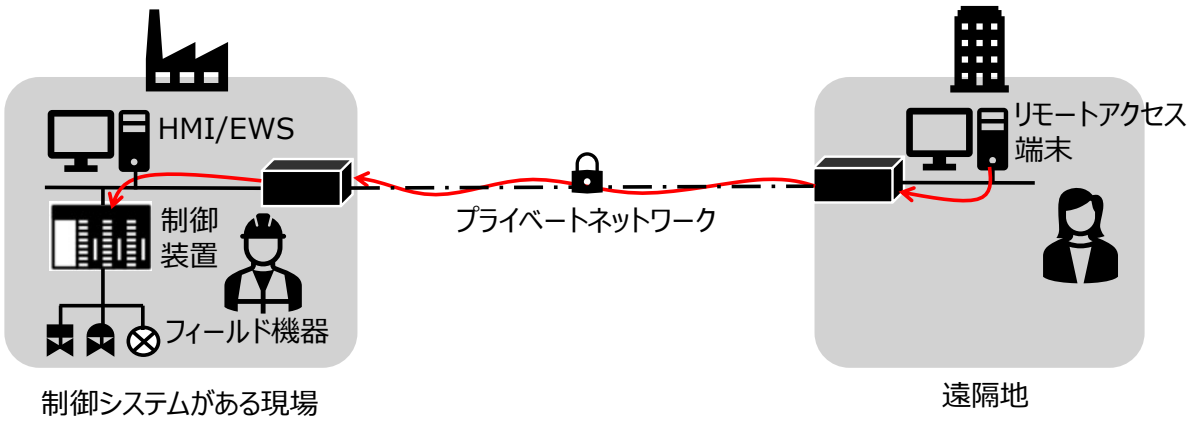


図 3-2：プライベートネットワーク方式-概念図

このプライベートネットワークは様々な通信回線から、通信の安定性やセキュリティ上の差異、コストなどを考慮して選択する。この方式の場合、リモートアクセス端末から制御装置に対して直接通信を行うため、制御装置に対応したプロトコルを利用する必要がある。そのため、選択する通信回線によってプロトコルの制限を受けるため注意が必要である。プライベートネットワークは複数の選択肢があることから、参考として専用線、閉域網ならびにインターネット VPN の構成概念を記載する。

(1) 専用線によるプライベートネットワーク方式

まず初めに専用線を利用した場合を以下に示す。この方式では現場の制御システム内の制御装置と HMI/EWS 端末間のネットワークを専用線の終端装置に接続し、遠隔地においてもリモートアクセス端末を専用線の終端装置に接続する。終端装置間の通信には専用の通信線（ダークファイバーなどの借り物を含む）が利用されており、物理的に接続されたプライベートネットワークを構築することでリモートアクセス端末から制御装置への通信経路を確立するものである。なお、専用線の概要については「付録

A.4.1 専用線」を参照されたい。

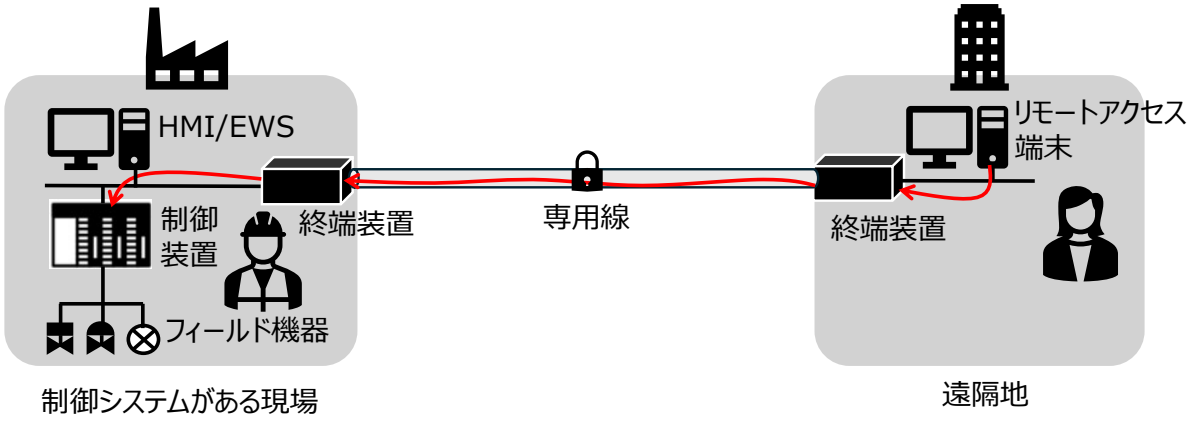


図 3-3：専用線によるプライベートネットワーク方式-概念図

(2) 閉域網によるプライベートネットワーク方式

次に閉域網を利用した場合を以下に示す。この方式では現場の制御システム内の制御装置と HMI/EWS 端末間のネットワークを閉域網の終端装置に接続し、遠隔地においてもリモートアクセス端末を閉域網の終端装置に接続する。これにより、論理的に接続された仮想的なプライベートネットワークを構築することでリモートアクセス端末から制御装置への通信経路を確立するものである。なお、閉域網の概要については「付録 A.4.2 閉域網」を参照されたい。

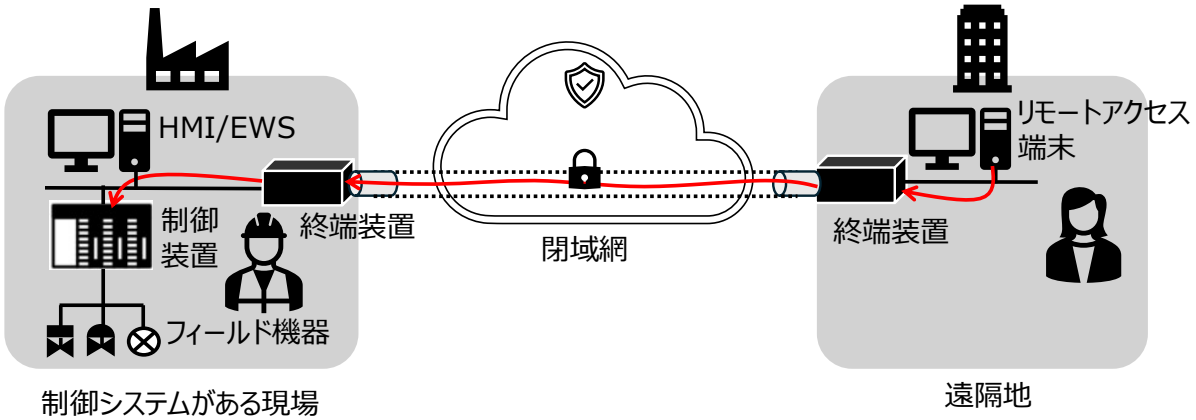


図 3-4：閉域網によるプライベートネットワーク方式-概念図

(3) インターネット VPN によるプライベートネットワーク方式

(a) VPN 用アプリケーションを利用したプライベートネットワーク方式

次にインターネット VPN のうち、VPN 用のアプリケーションを利用した場合を以下に示す。この方式で

は現場の制御システム内の制御装置と HMI/EWS 端末間のネットワークに VPN 機器を設置し、遠隔地ではリモートアクセス端末に VPN 用アプリケーションをインストールするか、VPN 機器(サーバー)のポータルサイトに WEB ブラウザ等でアクセスできるようにする。リモートアクセスする利用者は、VPN 機器(サーバー)にアクセスして認証を行い、安全な VPN 接続を確立する。これにより、現場の VPN 機器とリモートアクセス端末間に仮想的なプライベートネットワークを構築することでリモートアクセス端末から制御装置への通信経路を確立するものである。

１つの拠点（制御システムがある現場）に対し複数のリモートアクセス端末を接続したい場合に、インターネットへ接続されたリモートアクセス端末で VPN 用アプリケーションなどを利用させることで、柔軟にアクセス環境を提供できることから拡張性が高い。

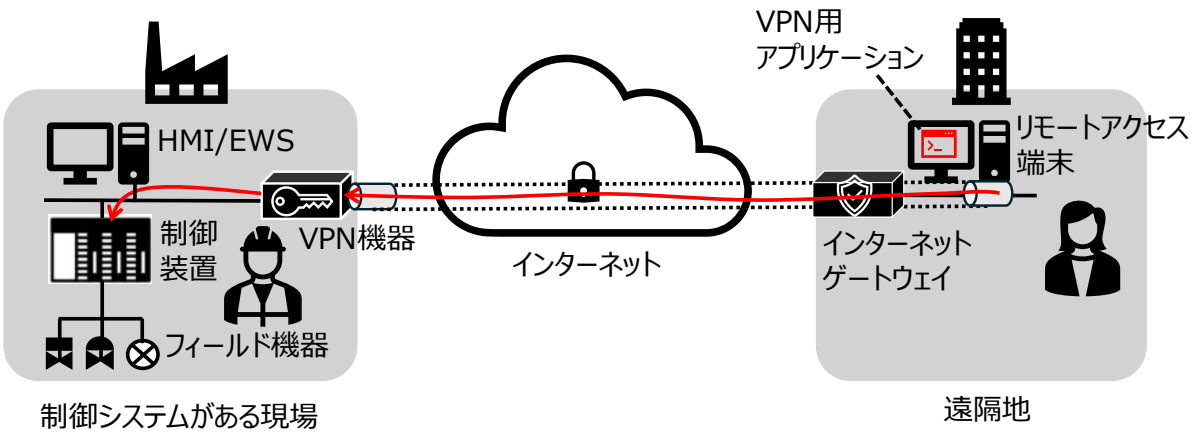


図 3-5：VPN 用アプリケーションを利用したプライベートネットワーク方式-概念図

(b) 拠点間通信を利用したプライベートネットワーク方式

次にインターネット VPN の拠点間通信を利用した場合を以下に示す。この方式では現場の制御システム内の制御装置と HMI/EWS 端末間のネットワークに VPN 機器を設置し、遠隔地においてもリモートアクセス端末を VPN 機器に接続する。これにより、VPN 機器を利用して拠点間の仮想的なプライベートネットワークを構築することでリモートアクセス端末から制御装置への通信経路を確立するものである。

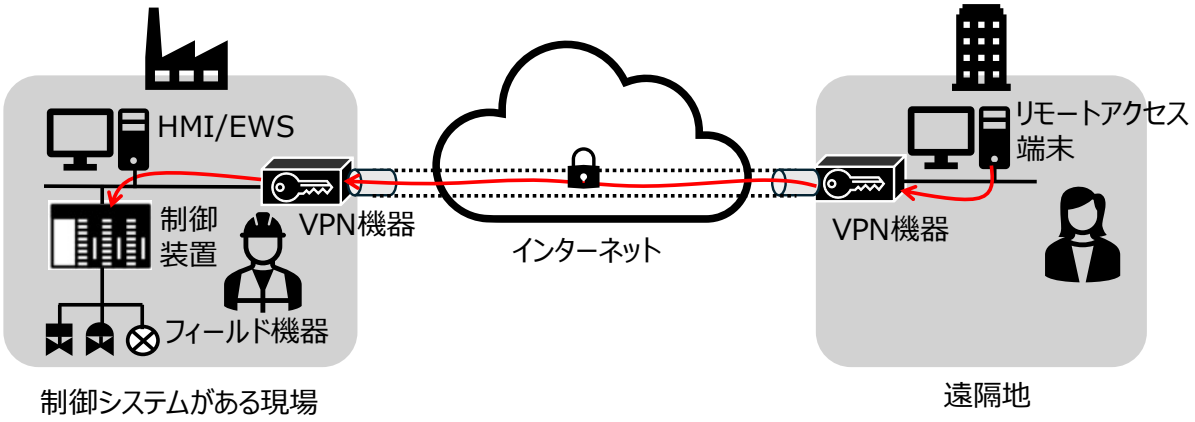


図 3-6：拠点間通信を利用したプライベートネットワーク方式-概念図

(c) クラウド型 VPN サービスを利用したプライベートネットワーク方式

次にインターネット VPN によるプライベートネットワーク方式の派生的な方式として、クラウド型の VPN サービスを利用した方式を示す。これは現場の制御装置と、遠隔地に設置されたリモートアクセス端末を、クラウド型の VPN サービスを介してプライベートネットワークで接続する。

この方式の特徴として、クラウド型の VPN サービスは、VPN 機器やリモートアクセス端末のアクセス管理、通信のログ収集、セキュリティチェック機能を備えている場合が多い。これにより、拠点数やリモートアクセス端末が多い場合でも、一元的に管理することが可能となる。

ただし、VPN 機器だけでなくクラウドサービスについても一定の知見が必要である。加えて、クラウドサービスには契約約款等で損害賠償の上限額が規定されている場合が多く、通常は数ヶ月間に支払った利用料金と相殺されることが一般的である。クラウド事業者の過失による大規模な被害が生じた際、この制約がユーザーの経営上どのようなリスクを生じさせるかを十分に分析する必要がある。また、重過失であれば全額保障される可能性もあるが、重過失の立証責任はユーザー側にあることが多く、実際に立証できるかどうかも重要な検討事項となる。

例としてインターネット VPN の拠点間通信を利用した場合を以下に示す。「3.2(3)(b) 拠点間通信を利用したプライベートネットワーク方式」の構成と、現場および遠隔地はほぼ同様であるが、各々の VPN 機器がクラウド型の VPN サービスへ暗号化された通信で一旦接続し、アクセスが制限されたクラウドの中で一旦復号の上、ルーティングされることで拠点間の仮想的なプライベートネットワークを構築される点が異なる。

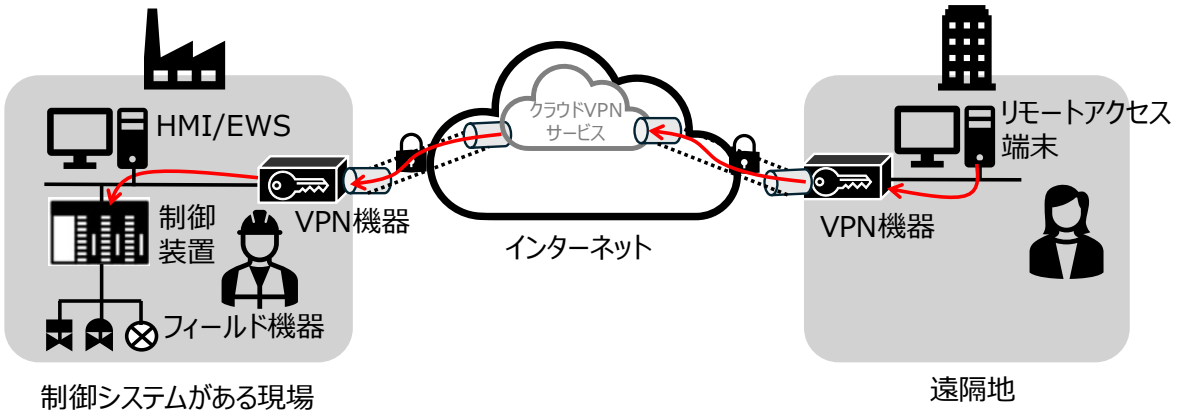


図 3-7：クラウド型 VPN サービスを利用したプライベートネットワーク方式-概念図

（拠点間通信を利用した場合）

なお、VPN 機器を利用せずに VPN 用アプリケーションを制御装置やリモートアクセス端末にインストールして接続する場合もあるが、「3.2(3)(a) VPN 用アプリケーションを利用したプライベートネットワーク方式」との組み合わせであり、拡張性の観点も同様である。

ここでは一例として、リモートアクセス端末側で VPN 用のアプリケーションを利用し、クラウド型の VPN サービスを介してプライベートネットワークで接続する場合を示す。

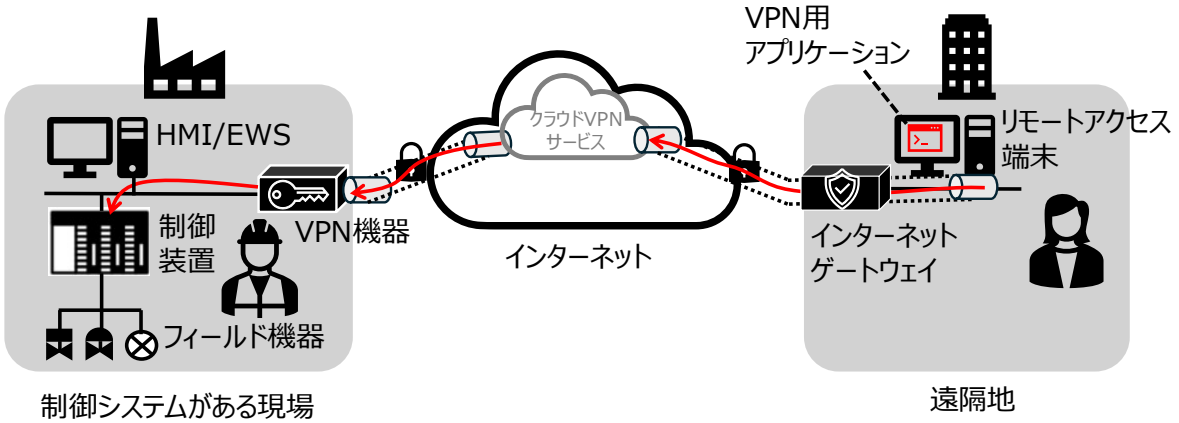


図 3-8：クラウド型 VPN サービスを利用したプライベートネットワーク方式-概念図

（VPN 用アプリケーションを利用した場合）

3.3 リモートデスクトップ方式

本節では、遠隔地のリモートアクセス端末から制御システム内に設置された HMI/EWS 端末のデスクトップ環境を介して制御装置にアクセスするリモートデスクトップ方式を紹介する。この方式は、遠隔地のリモートアクセス

端末から HMI/EWS 端末のデスクトップ環境に接続し、そのデスクトップ環境を遠隔操作することでリモート O&M を実現するものである。

なお、この方式ではリモートデスクトップ接続時の通信暗号化のためにプライベートネットワークを利用するものもあるが、遠隔地のリモートアクセス端末が直接制御システムの制御装置にアクセスするものではなく、またデータをリモートアクセス端末に保存しないという点で「3.2 プライベートネットワーク方式」とは異なるため、「リモートデスクトップ方式」として整理している。

この方式で実際にデータ処理を行うのは、遠隔操作される制御システム内に設置されている HMI/EWS 端末であるため、現場で操作する場合と同等の再現性を得ることができる。また、遠隔地のリモートアクセス端末上へのデータの保存を制限する設定ができるため、端末の紛失や盗難による情報漏えいリスクが低い。しかしながら、遠隔操作画面を遠隔地のリモートアクセス端末へ転送することになるため、頻繁にデータの送受信が発生し、通信遅延の影響を受ける。

このリモートデスクトップ方式も幾つかの手法があるため、代表的なものを記載する。

(1) プライベートネットワークを利用したリモートデスクトップ方式

まず初めにプライベートネットワークを利用したリモートデスクトップ方式を以下に示す。この方式は現場の制御システム内の HMI/EWS 端末へ接続されるネットワークをプライベートネットワークに接続し、遠隔地においてもリモートアクセス端末をプライベートネットワークに接続する。これにより、物理的または論理的にプライベートネットワークを構築することでリモートアクセス端末から HMI/EWS 端末への通信経路を確立するものである。その通信経路を経由して、遠隔地のリモートアクセス端末から制御システムの HMI/EWS 端末の OS 標準の「リモートデスクトップ接続」を利用することでデスクトップ環境を遠隔操作する。

このプライベートネットワークも様々な通信回線から、通信の安定性やセキュリティ上の差異を考慮して選択することになるため、「3.2 プライベートネットワーク方式」で説明した内容を参照されたい。なお、この方式の場合、使用されるプロトコルは RDP などの一般的なプロトコルに限定されるため、プロトコルによる通信回線の制約はほとんどない。

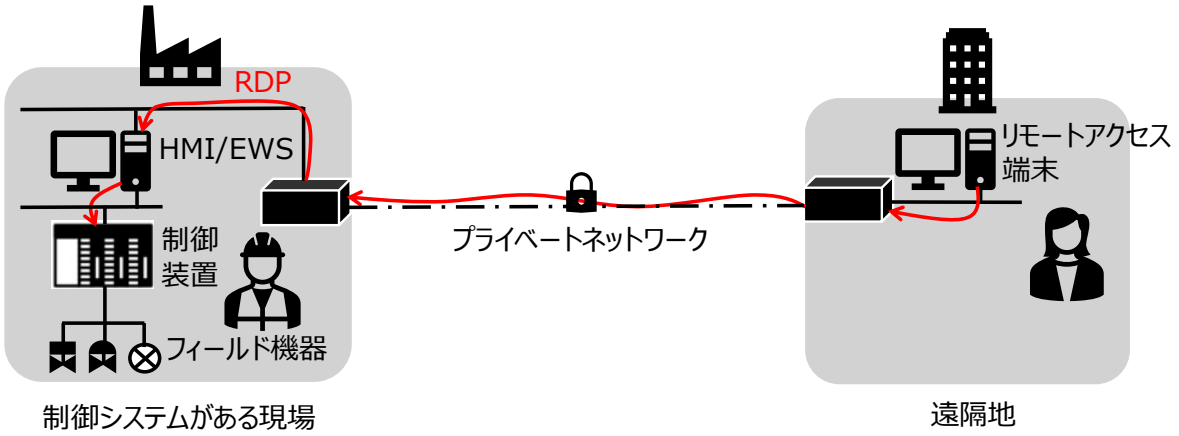


図 3-9：プライベートネットワークを利用したリモートデスクトップ方式-概念図

(2) 中継サーバーを利用したリモートデスクトップ方式

次に遠隔地のリモートアクセス端末から、制御システム内の中継サーバーを介して HMI/EWS 端末のデスクトップ環境に接続し、当該デスクトップ環境を遠隔操作する方式を紹介する。この方式は現場の制御システム内に中継サーバー（ゲートウェイサーバー）を配置し、遠隔地のリモートアクセス端末からのアクセスを RDP とは異なる暗号化されたプロトコル（HTTPS や SSH など）で受け、中継サーバーでの認証後にリモートデスクトップ接続し、HMI/EWS 端末のデスクトップ環境を遠隔操作するものである。

本方式もプライベートネットワークを介してアクセスした方がより安全性は高まるが、インターネット経由でアクセスする場合を例として示す。インターネットゲートウェイのポリシーでは一般的には RDP プロトコルを遮断することが多いため、本方式ではネットワークのルールを変更することなくアクセスできる。また、万が一中継サーバーが侵入者に乗っ取られても、分離している HMI/EWS 端末への侵入は防ぎやすく、安全性を高められる。その一方で、中継サーバーの設置や中継サーバー内のアカウント管理などが必要となる。

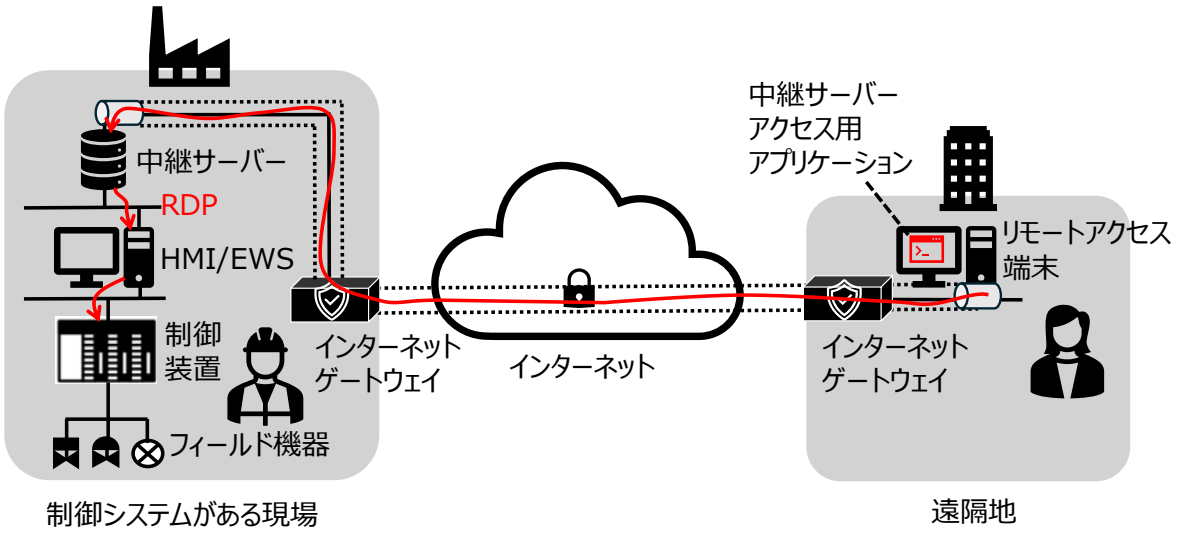


図 3-10：中継サーバーを利用したリモートデスクトップ方式-概念図

(3) インターネット上のサーバーを利用したリモートデスクトップ方式

次に遠隔地のリモートアクセス端末から、インターネット上に設置された外部のサーバーを利用して制御システムの HMI/EWS 端末のデスクトップ環境に接続し、当該デスクトップ環境を遠隔操作する方式を紹介する。「3.2(3)(a) VPN 用アプリケーションを利用したプライベートネットワーク方式」や「3.2(3)(c) クラウド型 VPN サービスを利用したプライベートネットワーク方式」に類似した方式ではあるが、制御装置に直接 VPN 用アプリケーションをインストールできない場合が多いため、この方式では HMI/EWS 端末に RDP 接続用アプリケーションをインストールすることで VPN 機器を設置せずにプライベートネットワークを構築しリモートデスクトップを実現する。ここでは 2 つの方式を紹介する。

(a) 外部 VPN サーバーを利用したリモートデスクトップ方式

この方式では現場の HMI/EWS 端末と遠隔地のリモートアクセス端末の各々に VPN 機能を有する RDP 接続用アプリケーションをインストール（リモートアクセス端末側から一般のウェブブラウザでアクセス可能なものもある）する。そして、そのアプリケーション等を利用してインターネット上の外部 VPN サーバーを介して SSL VPN によるプライベートネットワークを構築し、リモートアクセス端末から制御装置への通信経路を確立した上で、HMI/EWS 端末のデスクトップ環境を遠隔操作する。

HMI/EWS 端末をインターネット上の外部 VPN サーバーに接続するため、インターネットゲートウェイのネットワークのルール管理が非常に重要である。しかし、本方式では RDP プロトコルを直接使用するわけではないため、通常の RDP アクセスに必要なポリシー変更を行うことなく、アクセスが可能となる。ま

た、本方式の場合、専用の VPN 機器や中継サーバーの設置が不要であり、外部 VPN サーバーは集約的に管理されていることから、導入コストが低く抑えられることが多い。

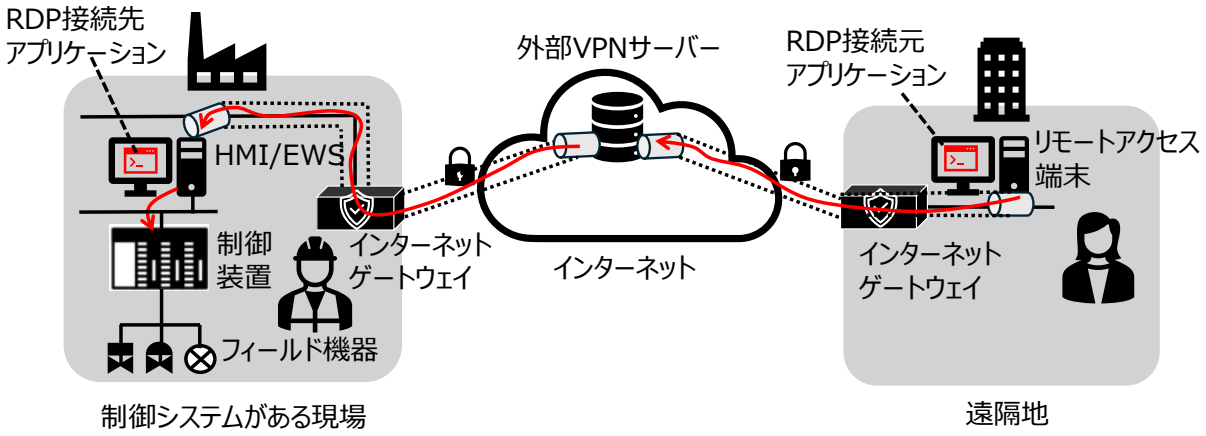


図 3-11：外部 VPN サーバーを利用したリモートデスクトップ方式-概念図

(b) 外部コネクション用サーバーを利用したリモートデスクトップ方式

この方式では現場の HMI/EWS 端末と遠隔地のリモートアクセス端末の各々に RDP 接続用アプリケーションをインストールし、インターネット上の外部コネクション用サーバーを介して暗号化の"暗号鍵"を交換し、直接 HMI/EWS 端末とリモートアクセス端末が直接、通信経路を確立した上で、HMI/EWS 端末のデスクトップ環境を遠隔操作する。

前述した「3.3(3)(a) 外部 VPN サーバーを利用したリモートデスクトップ方式」と同様に、RDP プロトコルを使用しないためネットワークのルールの変更することなくアクセスできる。また、VPN 機器や中継サーバーの設置が不要であり、外部コネクション用サーバーは集約的に管理されていることから、導入コストが低く抑えられることが多い。

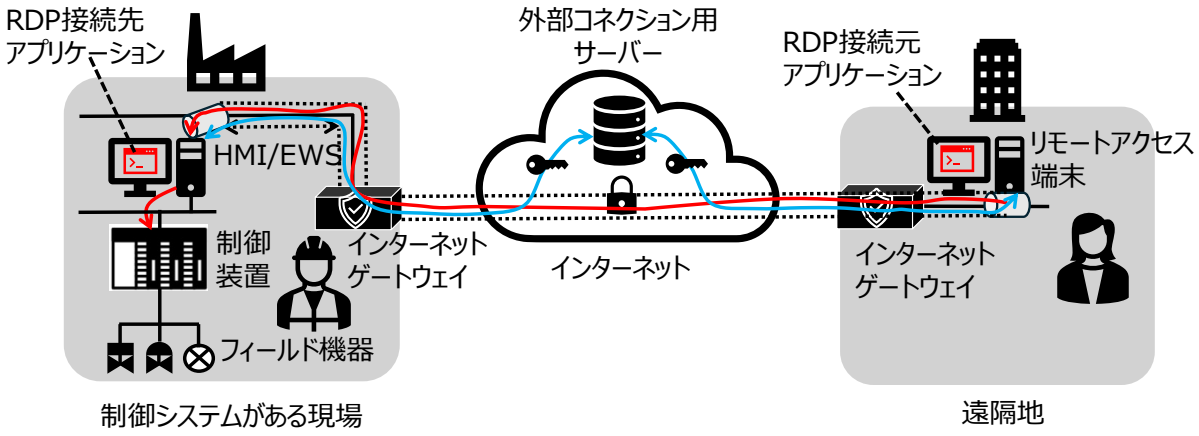


図 3-12：外部コネクション用サーバーを利用したリモートデスクトップ方式-概念図

(4) IP-KVM を利用したリモートデスクトップ方式

次に遠隔地のリモートアクセス端末から、HMI/EWS 端末に接続された IP-KVM と呼ばれる装置に接続し、当該デスクトップ環境を遠隔操作する方式を紹介する。

IP-KVM（Internet Protocol -Keyboard, Video, and Mouse）とは、キーボード・ビデオ・マウスの信号を IP プロトコルに変換し、TCP/IP のネットワーク経由で操作できるようにする装置である。この IP-KVM は HMI/EWS 端末へ特別なアプリケーションをインストールする必要がなく、KVM の信号を IP プロトコルに変換するケーブル（以下、KVM ケーブル）でのみ接続されるため、外部のネットワークから分離される。そのため、仮に悪意を持った人が不正に IP-KVM へアクセスして認証を突破したとしても HMI/EWS 端末のキーボード・ビデオ・マウスは操作できるが、ファイル転送ができないため直接マルウェアなどを外部ネットワークから展開することはできない。ただし USB 接続によるファイル転送機能を有するものもあるため、その点は留意が必要である。

遠隔地のリモートアクセス端末へは IP-KVM 接続用のアプリケーションをインストール（リモートアクセス端末側から一般のウェブブラウザでアクセス可能なものもある）し、プライベートネットワークを経由して IP-KVM へアクセスすることで HMI/EWS 端末のデスクトップ環境を遠隔操作する。このプライベートネットワークも様々な通信回線から、通信の安定性やセキュリティ上の差異を考慮して選択することになるため、「3.2 プライベートネットワーク方式」で説明した内容を参照されたい。IP-KVM へアクセスには TCP/IP のプロトコルが使用されており、プロトコルによる通信回線の制約はほとんどない。

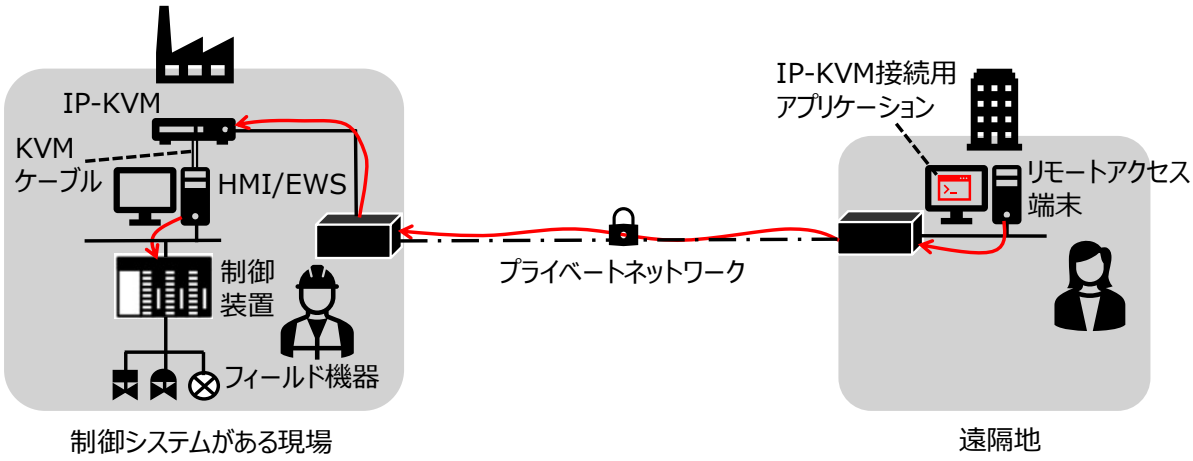


図 3-13：IP-KVM を利用したリモートデスクトップ方式-概念図

3.4　仮想デスクトップ（VDI）方式

最後に仮想デスクトップ/VDI（Virtual Desktop Infrastructure）を利用した方式を紹介する。遠隔地のリモートアクセス端末からクラウド上に設置された仮想デスクトップ（VDI）基盤に接続し、当該基盤上のデスクトップ画面を通じてリモート O&M を実現するものである。前述の「3.3 リモートデスクトップ方式」が制御システム内に設置されている HMI/EWS 端末に接続するのに対し、本方式では接続するデスクトップ環境として仮想デスクトップ（VDI）基盤を利用している点が異なる。クラウドサービスに接続する点では「3.2(3)(c) クラウド型 VPN サービスを利用したプライベートネットワーク方式」に類似した方式でもある。

仮想デスクトップ（VDI）基盤上に HMI/EWS 端末と同等の環境を構築することで、物理的に現場のネットワーク内にある場合と同様に現場の制御装置へ指令を出すことが可能となる。これにより、現場で HMI/EWS 端末を操作する際と同等の再現性を得ることができる。また、設定により遠隔地のリモートアクセス端末へのデータ保存の制限が可能なため、端末の紛失や盗難による情報漏えいリスクが低い。しかしながら、遠隔操作画面を遠隔地のリモートアクセス端末へ転送することになるため、頻繁にデータの送受信が発生し、通信遅延の影響を受ける。

この方式では、仮想デスクトップ（VDI）から VPN 機能を持つ中継サーバーを介して制御装置と通信する場合や、HMI/EWS 端末に RDP 接続する場合がある。

また、この方式には、リモートアクセス端末のアクセス管理、通信のログ収集、セキュリティチェック機能をクラウド側で提供するサービスがある。これにより、拠点数やリモートアクセス端末が多い場合などに、一元的に管理することが可能となる。

なお、「3.2(3)(c) クラウド型 VPN サービスを利用したプライベートネットワーク方式」で記載したように、クラウドサービスについても一定の知見が必要であり、クラウドサービス障害発生時のリスクについても十分に検討する必要がある。

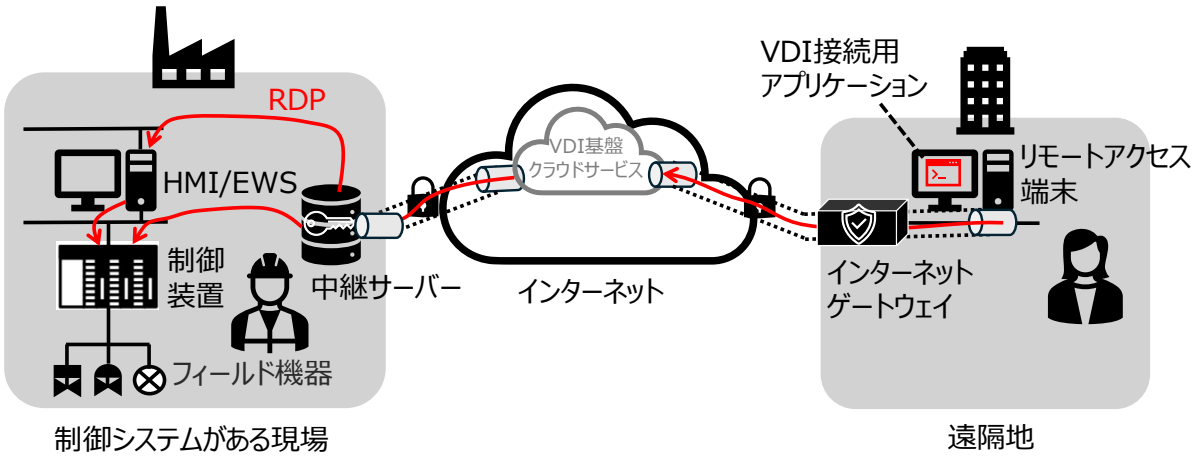


図 3-14：仮想デスクトップ（VDI）方式-概念図

3.5　リモートアクセス方式の総括

本章では、制御システムへのリモートアクセス方式を「プライベートネットワーク方式」「リモートデスクトップ方式」「仮想デスクトップ（VDI）方式」の 3 つに分類し、それぞれの特性とセキュリティ上の考慮点を紹介した。

プライベートネットワーク方式では、専用線や閉域網、インターネット VPN などを利用して、遠隔地のリモートアクセス端末から直接制御装置にアクセスする方法を解説した。リモートデスクトップ方式では、遠隔地のリモートアクセス端末から制御システム内の HMI/EWS 端末のデスクトップ環境を介して制御装置にアクセスする方法を説明し、プライベートネットワークや中継サーバー、外部 VPN サーバーなどを利用する具体例を示した。仮想デスクトップ（VDI）方式では、クラウド上の仮想デスクトップ基盤を利用してリモート O&M を実現する方法を紹介した。

各方式の選択は利用目的や要件に応じて行う必要があり、本章で示した情報を参考に最適なリモートアクセス方式を検討・選定されたい。利用目的および要件定義に基づくリモートアクセス方式の選択、組合せなどの検討プロセスについては「第 6 章 要件定義に基づくシステム構成検討プロセス」で詳述する。

第4章　制御システムにおけるリスク分析手法

4.1　　リスク分析とは

実効的なセキュリティ対策を行うには、まず保護すべき資産を明確にし、それらに対する脅威や脆弱性を評価することが重要である。このプロセスをリスク分析といい、リスク分析では、システムやサービスに対する脅威がもたらす被害の大きさや発生の可能性、受け入れられるリスクのレベルを明確にする。これによりリスクレベルが高い箇所に対策費用を集中させることができ、効率的な対策を講じることができる。リモート O&M においても外部インターネットからの侵入や攻撃の脅威があり、リスク分析を実施した後、適切なセキュリティ対策を実装していく必要がある。

システムや事業を分析する際には、次の 3 つの指標を使って評価する。

① 分析対象（保護すべきシステムや事業）の価値（重要性）と想定される被害の規模や影響

② 分析対象に対する脅威とその発生可能性

③ 脅威が発生した場合の受容可能性（分析対象の脆弱性）

これらの評価を基に、保護すべき対象が損なわれるリスクレベルを算出する。リスクレベルは、脅威の発生確率や被害の大きさを考慮し、相対的に評価されるリスク値として表される。

算定したリスク値を使って、システムや事業の中でリスクが高い箇所を特定する。そして、対策が不十分な部分を強化することで、全体のリスクレベルをどれだけ低減できるかを検討する。これにより、リスク低減に最も効果的な対策箇所を見つけ出し、優先順位を付けたリスク対策計画を立てることができる。

リスク分析にはいくつかのアプローチがあるが、本書では「資産ベースのリスク分析」と「シナリオベースのシリスク分析」の 2 つを紹介する。

4.2　　資産ベースのリスク分析手法

資産ベースのリスク分析は、組織が保護すべきシステムを構成する資産を中心に、リスクを評価する手法である。このプロセスは保護すべきシステムの資産（サーバー、端末、通信機器等）に対して、3 つの評価項目（重要度、想定脅威、脆弱性）に対し、それぞれ評価を行い、リスク分析を行う。

リスクの評価は脅威が発生する確率と脅威が実現したときの影響を掛け合わせて定量化し、リスクの重大性や優先順位を評価する。

資産ベースの評価は、全ての資産をリストアップし、それぞれの重要度、想定脅威、脆弱性を評価することで、システム全体のセキュリティ状況を把握でき、網羅的なリスク評価を行うことができる。また、リスクを定期的に見直し、対応策を講じることができ、継続的なリスク管理と改善に向いている。

反面、資産の特定と評価の複雑さ、脅威が発生する確率の見積もりや影響の評価の難しさ、リスク評価を

行うための人的リソースやスキルの問題など、難しさや課題もある。

資産ベースのリスク分析手法について詳しく知りたい場合は、引用・参考文献[22]を参照されたい。

4.3 シナリオベースのリスク分析手法

シナリオベースのリスク分析は、特定のリスクシナリオを想定し、そのシナリオが発生した場合の影響と対策を評価する方法である。この手法は資産ベースのリスク分析と比較して、具体的な脅威やイベントに焦点を当てることで、現実的かつ実践的なリスク評価を行うことができる。制御システムでは、システムのリアルタイム性と可用性が特に重要となる。このため、特定のシナリオ（例えば、システム停止や通信障害）に対する評価が重要となってくる。また、制御システムのセキュリティリスクは、物理的な安全や環境への影響を伴うことが多いため、シナリオベースの評価が効果的であると思われる。特に、リソースが限られている場合、シナリオベースのリスク分析を行い、特に重要なリスクシナリオに対して重点的に対応するのが効率的である。

反面、シナリオの選定が不適切であったり、仮定が現実と乖離していると、リスク評価の有効性が低下する。また特定のシナリオに焦点を当てるため、全体的なリスク評価が不足する可能性があることに注意が必要である。シナリオベースのリスク評価手法の一つとして、次項にて CCE を紹介する。

4.3.1 CCE

CCE（Consequence-driven Cyber-informed Engineering）は、2016 年に米国のアイダホ国立研究所で開発された「シナリオベース」の脅威分析手法である。この手法は、「起きてほしくない結果」から逆算してセキュリティ対策を考えるものであり、リスク値のような確率を評価するステップがないため、「発生してほしくない事象」と「セキュリティ対策」の関係が明確でわかりやすく、セキュリティ対策の優先順位も決めやすいというメリットがある。CCE は大きく 4 つの検討ステップに分かれている。

(1) ステップ 1

対象のシステムにおいて「発生してほしくない事象」を洗い出し、対応の優先順位をつける。ここでは、サイバーセキュリティのことは考えず、単に発生してほしくない事象を検討する。

(2) ステップ 2

それらの事象を引き起こす関連システムやサブシステムを洗い出す。

(3) ステップ 3

ステップ 1 の事象をステップ 2 のシステムを用いて発生させるには、どのようなサイバー攻撃が考えられるかを、サイバーキルチェーンを踏まえて検討する。

(4) ステップ 4

ステップ 3 のサイバー攻撃に対応し、サイバーキルチェーンを断ち切るセキュリティ対策を検討する。

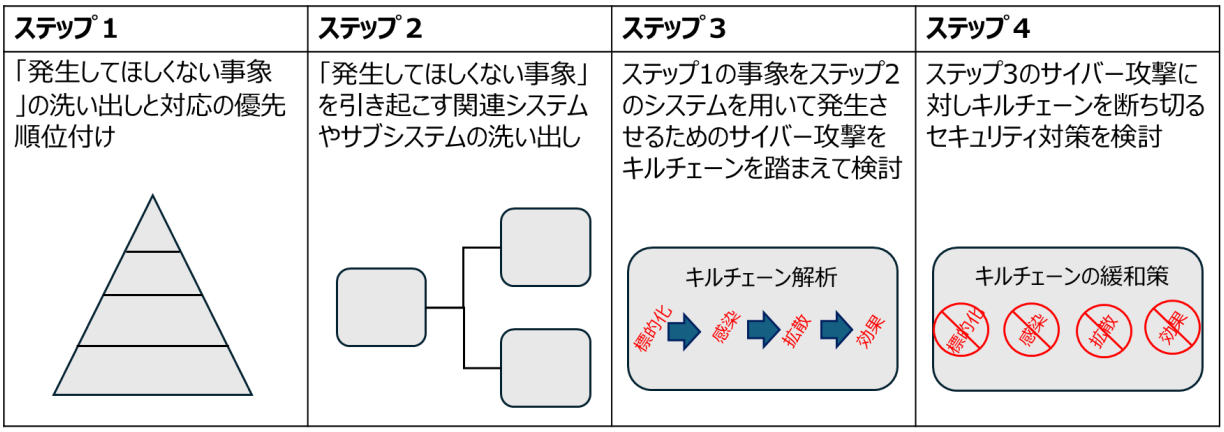


図 4-1：CCE の 4 つのプロセス手順

出典：https://www.osti.gov/servlets/purl/1341416/ をもとに作成

CCE は、特定の重要なインフラストラクチャやビジネスプロセスに対するサイバー攻撃の影響を最小限に抑えるための具体的な対策を実施するために利用されており、特定のシステムやプロセスに焦点を当て、具体的な脅威情報を基にした防御策の実装に適している。

ただし、想定した事象に対しては効果的な対策を実施できるが、想定外の事象には対応できないため、ベストプラクティスや標準に基づいた多層的な対策と併用することで、セキュリティ対策を強化する必要がある。

なお CCE について詳しく知りたい場合は、引用・参考文献[10]や[18]を参照されたい。

4.4 リスク管理のフレームワーク

シナリオベースのリスク分析では全体的な網羅性が欠如し、リスク評価が不足する可能性がある。そのため、リスク管理のフレームワークで全体のリスク状況を把握しながら、シナリオベースのリスク評価を活用して、特定の重要なリスクシナリオに対する詳細な評価と対策を策定することが効果的である。

本書ではリスク管理のフレームワークとして NIST CSF を次項「4.4.1 NIST CSF」にて紹介する。NIST CSF とシナリオベースのリスク分析を組み合わせることで、以下のような効果を期待できる。

- NIST CSF の包括的なフレームワークにより、組織全体のリスク管理態勢を強化する。これにシナリオベースの具体的なリスク分析を組み合わせることで、現実的かつ実践的なリスク対策を実施できる。
- シナリオベースの分析により、特定の脅威やインシデントに対する具体的な準備が可能になる。
- シナリオベースの分析結果を反映することで、NIST CSF の各機能を柔軟に強化できる。

・ NIST CSF とシナリオベースのリスク分析を組み合わせることで、継続的なリスク評価と対策の改善が可能になる。

4.4.1 NIST CSF

NIST CSF（Cyber Security Framework）は、2013 年に米国のオバマ大統領が「重要インフラのサイバーセキュリティを強化するための大統領令（13636 号）」を発出したことを受け、翌年 NIST により策定された、サイバーセキュリティリスクに対応するためのフレームワークである。一般に本フレームワークは、「サイバーセキュリティフレームワーク」や「CSF」と呼ばれることが多い。NIST CSF はサイバーレジリエンスを考慮した包括的な管理策が含まれ、その汎用性の高さから世界中の官・民の様々な組織で活用が進んできた。

NIST CSF の特徴は、フレームワークがカバーする領域の広さである。昨今のサイバー攻撃の高度化や複雑化に伴い、サイバーレジリエンス強化が求められている中で、CSF はこの状況に対応するため、脅威の侵入を防ぐ「事前対策」だけでなく、侵入などの有事が発生した後を想定した「事後対策」も含む、広範な管理策をカバーする。なお、本書で参照している NST CSF のバージョンは 2.0 である。

NIST CSF は、「Core（コア）」「Tier（ティア）」「Profile（プロファイル）」という 3 つの要素で構成されているが、それぞれの要素について説明する。

(1) Core（コア）：

組織の種類や規模感を問わず実施可能な、サイバーセキュリティの対策やその効果が記載されている。一定の分類で定められたセキュリティ管理策の一覧であり、下に示す(a) ～(f)の 6 つの機能と、図 4-2 に示す 22 のカテゴリーで構成される。カテゴリー毎にサブカテゴリーが用意されており、サブカテゴリーの合計は 106 項目になる。

(a) 統治（Govern）

組織のサイバーセキュリティリスクマネジメント戦略、期待、ポリシーが確立され、伝達され、監視されている。

(b) 識別（Identify）

組織の現在のサイバーセキュリティリスクが理解されている。

(c) 防御（Protect）

組織のサイバーセキュリティリスクを管理するための保護策を使用されている。

(d) 検知（Detect）

潜在的なサイバーセキュリティ攻撃および侵害が発見され、分析される。

(e) 対応（Respond）

検出されたサイバーセキュリティインシデントに関して措置が講じられる。

(f) 復旧（Recover）

サイバーセキュリティインシデントの影響を受けた資産および運用が復旧される。

機能	#	カテゴリー
ガバナンス	1	組織的背景
	2	リスク管理戦略
	3	サイバーセキュリティ・サプライチェーン・リスク管理
	4	役割、責任、権限
	5	方針、プロセス、手順
	6	監督
識別（特定）	7	資産管理
	8	リスク評価
	9	改善
防御	10	アイデンティティ管理、認証、アクセスコントロール
	11	意識向上とトレーニング
	12	データ・セキュリティ
	13	プラットフォーム・セキュリティ
	14	テクノロジー・インフラの回復力
検知	15	継続的モニタリング
	16	有害事象分析
対応	17	インシデント管理
	18	インシデント分析
	19	インシデント・レスポンスの報告とコミュニケーション
	20	インシデントの緩和
復旧	21	インシデント復旧計画の実行
	22	インシデント復旧のためのコミュニケーション

図 4-2：NIST CSF2.0 におけるカテゴリー

出典： https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf をもとに作成

(2) Tier（ティア）：

組織のサイバーセキュリティマネジメントの成熟度を数値化するための評価基準であり、ティア 1～4 までの 4 段階で記載されている。それぞれの段階における評価基準を図 4-3 に示す。

なお、目標とする Tier のレベルは組織ごとに適切なレベルを設定すればよく、必ずしも Tier４を目指す必要はない。

	Tier1 Partial (部分的)	**Tier2** Risk-Informed (リスク情報活用)	**Tier3** Repeatable (繰り返し適用可能)	**Tier4** Adaptive (適応的)
サイバーセキュリティリスクガバナンス	セキュリティリスク戦略および優先順位付けは場当たり的であり正式なものではない	セキュリティポリシーが確率されておらず、サイバーセキュリティの対応はリスクやビジネス要件に基づいて決められている	リスクマネジメントは公式に承認され、セキュリティーポリシーや手段はリスク情報に基づき、定期的に見直され更新されている	リスク情報に基づいたセキュリティポリシーと手段を使い、サイバーセキュリティリスクに対応している
サイバーセキュリティリスク管理	サイバーセキュリティリスクの認識が少なく、不定期にリスクマネジメントを行い、情報共有の手段がない	サイバーセキュリティリスクを認識しているが、一貫したマネジメント手法はない	サイバーセキュリティリスクをマネジメントし、情報を共有して一貫した方法で対応している	過去と現在のサイバーセキュリティ活動から学び、最新技術を使って脅威に迅速に対応している

図 4-3：サイバーセキュリティのリスクガバナンスやリスクマネジメントのための Tier の階層

出典： https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf をもとに作成

(3) Profile（プロファイル）

フレームワークを活用し、サイバーセキュリティ対策状況の評価を行うことで、現状の状態を明確にすることができる。また、組織が目指すべきレベルに至る考え方も記載されているため、現状の状態を踏まえて今後の方針を検討することができる。

NIST CSF のコア、ティア、プロファイルの 3 要素を活用することで、企業や組織はサイバーセキュリティ対策の現状と目標のギャップを分析し、必要な対策を整理し優先順位を付けることができる。また、組織全体のセキュリティリスクを包括的に管理し、改善のためのロードマップを作成することができる。

このように、NIST CSF は、セキュリティプログラムの成熟度向上や戦略的アプローチが必要な場合に適しており、全体的なセキュリティポリシーの策定や管理に有用である。また、社内外の関係者との「共通言語」としてサイバーセキュリティリスクや対策状況のコミュニケーションにも役立つものでもある。

本書においては後述する「第 5 章 リモートアクセスにおけるセキュリティ対策」において、リモートアクセスに関連する文献・ガイドラインに記載された推奨要件を NIST CSF の機能に分類し整理している。なお、NIST CSF について詳しく知りたい場合は、引用・参考文献[23]を参照されたい。

4.5 制御システムにおけるリスク分析手法の総括

本章では、制御システムにおけるリスク分析手法について説明した。リスク分析は、保護すべき資産の価値、脅威の発生可能性、脆弱性を評価することで、効率的なセキュリティ対策を講じるための重要なプロセスである。

CCE はセキュリティ戦略を具体的な重要システムやプロセスに適用するための詳細な手法を提供するものであり、また NIST CSF は広範なセキュリティ戦略の基盤を提供するものであるが、互いに補完し合い、組織のセキュリティリスク管理を強化するために併用されることが多い。

具体的な CCE を活用した検討事例は「第 6 章 要件定義に基づくシステム構成検討プロセス」にて紹介することとしたい。

第5章 リモートアクセスにおけるセキュリティ対策

本章ではリモートアクセスのユースケースやネットワーク構成に関わらず、リモートアクセスおよびテレワーク関連の各種文献・ガイドラインに記載された共通的に実施すべき要件を抽出した。本書作成にあたり、参考にした文献およびガイドラインを「表 5-1：参考文献・ガイドラインリスト」に記載する。

表 5-1：参考文献・ガイドラインリスト

No	文献名	概要	リモートアクセスおよびテレワークに関する記載事項
1	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver1.0 引用・参考文献[19]	工場のセキュリティ対策を企画・実行にあたりセキュリティ対策で参照すべき考え方やステップを提示したガイドライン （主な項目） ・工場システムにおけるセキュリティリスクの特定と評価方法 ・サイバーセキュリティ対策の基本方針と組織体制の構築方法 ・システムの設計・構築段階でのセキュリティ対策 ・システムの運用・保守段階でのセキュリティ対策 ・サプライチェーンにおけるセキュリティ管理 ・サイバー攻撃への備えとインシデント対応手順	識別：資産管理 防御：アイデンティティ管理、認証、アクセスコントロール 検知：継続的モニタリング、有害事象分析
2	制御システムのセキュリティリスク分析ガイド 第2版 引用・参考文献[22]	制御システムのセキュリティを向上する上で重要な位置付けとなるセキュリティリスク分析を事業者が実施できるようにするためのガイドライン （主な項目） ・制御システムの概要とセキュリティリスク分析の位置づけ ・セキュリティリスク分析のための基本的な手法とプロセス ・制御システムのセキュリティリスク分析における留意事項と具体的な手法 ・セキュリティリスク分析の結果を活用したセキュリティ対策の立案方法 ・実際の事例や具体的な手法の紹介	防御：アイデンティティ管理、認証、アクセスコントロール
3	NIST.SP.800-46 Revision2 「Guide to Enterprise Telework, Remote Access, a	テレワークやリモートアクセス、個人のデバイスのセキュリティに関するガイドライン （主な項目） ・リモートアクセスのセキュリティ ・テレワーク環境のセキュリティ	識別：資産管理 防御：アイデンティティ管理、認証、アクセスコントロール、プラットフォーム・セキュリティ、テクノロジー・インフラの

	nd Bring Your Own Device (BYOD) Security」 引用・参考文献[6]	・BYOD セキュリティ ・リスク管理 ・ポリシーと手順	回復力 検知：継続的モニタリング、有害事象分析 対応：インシデント・レスポンスの報告とコミュニケーション
4	NIST SP 800-53 Rev. 5 「Security and Privacy Controls for Information Systems and Organizations」 引用・参考文献[7]	情報システム系のセキュリティおよびプライバシー管理策に関するガイドライン （主な項目） ・セキュリティとプライバシーの統合 ・リスク管理フレームワークの強化 ・管理策の分類 ・柔軟性と適用性 ・プライバシー強化 ・最新の脅威に対応 ・ガバナンスとポリシー	防御：アイデンティティ管理、認証、アクセスコントロール
5	NIST.SP800-82r3 「Guide to Operational Technology (OT) 3 Security 」 引用・参考文献[8]	OT のセキュリティ管理策を提供するガイドライン （主な項目） ・OT 環境の特性とセキュリティ要件の理解 ・リスクマネジメントフレームワークの適用 ・セキュリティコントロールの実装 ・システムのライフサイクル管理 ・インシデント対応と復旧 ・規制と基準の遵守 ・サイバー脅威の進化に対応	識別：資産管理 防御：アイデンティティ管理、認証、アクセスコントロール 検知：継続的モニタリング
6	CPNI Good Practice Guidelines ～SCADA およびプロセス制御ネットワークにおけるファイヤーウォールの利用につい ての NISCC グッド・プラクティス・ガイド～ 引用・参考文献[1]	SCADA システムやプロセス制御ネットワークを保護するファイヤーウォールの適切な使用方法を解説するガイドライン （主な項目） ・導入の背景 ・ファイヤーウォールの基本概念 ・設計と配置 ・設定と管理 ・セキュリティポリシーの策定 ・リスク評価と脅威モデル ・テストと監査 ・ベストプラクティスの例	識別：資産管理 防御：アイデンティティ管理、認証、アクセスコントロール、プラットフォーム・セキュリティ 検知：継続的モニタリング、有害事象分析
7	NERC CIP CIP-005 — Cyber Security –	北米電力調整委員会（NERC）が策定した、電力会社が電子セキュリティ・ペリメータ（ESP）という内部ネットワークに対する外部からの不正ア	防御：アイデンティティ管理、認証、アクセスコントロール

	Electronic Security Perimeter 引用・参考文献[5]	クセスや攻撃から保護するための要件を定義したサイバーセキュリティ基準	
8	テレワークセキュリティガイドライン 第５版 引用・参考文献[20]	テレワークを安心かつセキュアに導入・運用するためのガイドライン （主な項目） ・テレワークのセキュリティ方針と組織の責任 ・テレワーク環境でのセキュリティ対策のポイント ・リモートアクセス環境でのセキュリティ対策 ・デバイスのセキュリティ対策 ・ネットワーク環境のセキュリティ対策 ・情報漏えい対策 ・インシデント対応	識別：資産管理 防御：アイデンティティ管理、認証、アクセスコントロール、プラットフォーム・セキュリティ 検知：継続的モニタリング、有害事象分析 対応：インシデント・レスポンスの報告とコミュニケーション

これらの文献およびガイドラインから抽出された共通的な要件は、「表 5-2：参考文献に記載された要件とNIST CSF のカテゴリーとの関係」に示す通り、それぞれの要件が関係する４つの機能（識別、防御、検知、対応）に分類整理した。要件が関係するカテゴリーを関連箇所の欄に〇にて示すこととし、次節以降でセキュリティ対策推奨事項として解説する。

なお、関連箇所に当てはまらないカテゴリーの内容については本書では言及しないが、それぞれの組織で目指す Tier を達成するため、別途対応が必要であることを付け加えておく。

表 5-2：参考文献に記載された要件と NIST CSF のカテゴリーとの関連

機能	#	カテゴリー	関連箇所
ガバナンス	1	組織的背景	―
	2	リスク管理戦略	―
	3	サイバーセキュリティ・サプライチェーン・リスク管理	―
	4	役割、責任、権限	―
	5	方針、プロセス、手順	―
	6	監督	―
識別（特定）	7	資産管理	〇
	8	リスク評価	―
	9	改善	―
防御	10	アイデンティティ管理、認証、アクセスコントロール	〇
	11	意識向上とトレーニング	―

	12	データ・セキュリティ	—
	13	プラットフォーム・セキュリティ	○
	14	テクノロジー・インフラの回復力	○
検知	15	継続的モニタリング	○
	16	有害事象分析	○
対応	17	インシデント管理	—
	18	インシデント分析	—
	19	インシデント・レスポンスの報告とコミュニケーション	○
	20	インシデントの緩和	—
復旧	21	インシデント復旧計画の実行	—
	22	インシデント復旧のためのコミュニケーション	—

5.1 識別

5.1.1 資産管理

未知の資産や管理されていない資産が存在すると、サイバー攻撃や不正アクセスのリスクが高まり、セキュリティインシデントや障害発生時に迅速な対応ができず被害が拡大しやすく、影響範囲を特定できず効果的な対応が難しくなる。

リモートアクセスに関するセキュリティ対策においても、資産管理を行うことで企業は所有するハードウェア、ソフトウェア、データの全体像を把握し、リスクの特定と評価が容易になり、適切なリスク軽減策を講じることが可能となる。さらに、資産の場所や状態を把握することで、セキュリティインシデント発生時に迅速かつ効果的に対応でき、問題が発生した場合の影響範囲を即座に特定し、適切な対応ができるようになる。

(1) 資産管理に関するセキュリティ対策推奨事項

(a) 資産管理台帳作成

資産の一覧を記載した台帳を作成し、定期的に棚卸を実施する。

(b) 台帳記載事項

台帳には資産の用途、設置場所、管理者などの情報を記載し、記載漏れや誤りがないことを確認する。

(c) 台帳管理

台帳は定められた期間保管し、意図せず改ざんされないように管理する。

(d) 正規機器と不正機器の識別

資産管理ツールでネットワーク機器の管理機能があれば、正規なネットワーク機器の MAC アドレス等を登録し、不正な機器の接続を防止する。

(2) 近年の技術動向

商品化された資産管理ツールの中には、ネットワークに接続された資産を自動的に検出・登録して、ハードウェア、ソフトウェア、ライセンス、ネットワーク機器などの資産を一元管理することができるものもある。このようなツールの導入することで資産管理が自動化され、人手による調査や記録作業をある程度削減することも期待できる。

5.1.2 脆弱性対応

攻撃の多くは既知の脆弱性を狙っているため、これを放置することは大きなリスクとなる。このため、各種文献・ガイドラインでも脆弱性対応に関する要件が記載されている。

(1) 脆弱性対応に関するセキュリティ対策推奨事項

(a) 脆弱性の特定とソフトウェア、ファームウェアのアップデート

(ｲ) 定期的な脆弱性診断やペネトレーションテストを実施する。

(ﾛ) 組み込み機器（PLC や IoT 機器など）のモデル情報やファームウェア情報を把握し、脆弱性情報を定期的に確認する。

(ﾊ) リモートアクセス端末も含め、最新の OS やソフトウェアおよびファームウェアのアップデートを随時行うことが望ましいが、パッチの適用可否や適用タイミングは、事業への影響や対処を見送った場合の影響などを考慮して決定する。

5.2 防御

5.2.1 リモートアクセスの認証

リモートアクセスする外部者の認証が不十分だと、不正な第三者に組織のネットワークに侵入されるリスクがあるが、認証を強化（多要素認証など）することで、不正アクセスや情報漏洩、システム破壊のリスクを減少させることができる。

(1) 認証に関するセキュリティ対策推奨事項

(a) 認証の強化

(ｲ) リモートアクセス時に多要素認証を必須にする設定を行う。

(ﾛ) パスワードだけでなく、SMS による認証コード、ハードウェアトークン、ソフトウェアの Authenticator (スマートフォン等)、生体認証（指紋や顔認証）などの多要素認証を導入することで、認証の信頼性を高める。ただし、例えばスマートフォン等によるソフトウェアの Authenticator の利用において

はスマートフォン特有のリスクもあるため、どの多要素認証技術を導入する際においても技術的なリスクの確認が必要である。

(ハ) 多要素認証の仕組みを持つシステムは DMZ に設定するか、あるいは、IT 部門がすでに設置している認証システムを使用する。

(ニ) デフォルトクレデンシャルはすべて削除するか変更する。

(b) セッション管理

(イ) 認証失敗時のアカウントロックを一定回数設定し、一定期間のログイン拒否を行う。

(ロ) リモートアクセスを一定時間不使用の場合、自動的にセッションを切断する。
再接続時には再度認証を要求するように設定する。

(ハ) リモートアクセスの時間帯を制限することで、不正なアクセスを防ぐ。

5.2.2 通信の保護（暗号化）

暗号化はデータと通信の安全性を確保し、サイバー攻撃や不正アクセスから保護するために不可欠な手段である。データを読み取り不能にし、改ざんリスクを低減し、正しい暗号鍵を持つ正当なユーザーのみがアクセスできるようにし、セキュリティインシデント時にもデータ漏洩や損失の影響を最小限に抑えることができる。

(1) 暗号化に関するセキュリティ対策推奨事項

(a) 通信の保護

(イ) プライベートネットワークのように外部からのアクセスが制限されたネットワーク（例：閉域網、VPN 等）を使用し、セキュアな通信経路を確保する。

(b) 通信の暗号化

(イ) 全てのリモートアクセスセッションで中間システムまでの通信も TLS や SSH などの暗号化技術を利用する。

(ロ) クラウドサービス接続時やデータ送受信時も、暗号化された手段を利用する。

5.2.3 DMZ の設置

DMZ（Demilitarized Zone）は、外部ネットワークと内部ネットワークの間にセキュリティ層を追加し、ネットワークをセグメント化して重要なデータやシステムを保護するものである。リモート接続用のサーバーやサービスを DMZ に配置することで、攻撃者の内部ネットワークへの直接的なアクセスや影響を最小限に抑え、リモートアクセスに対する防御を強化する。リモート接続において DMZ の設置は、セキュリティを強化し、ネットワークとデータの安全性を確保するために非常に重要である。

(1) DMZ に関するセキュリティ対策推奨事項

(a) リモートアクセスする際には、外部と直接現場の制御システムと通信しないように、3 つのゾーン（外部、DMZ、現場の内部ネットワーク）を使ったシステムを構築する。

(b) 外部ネットワークと内部ネットワーク間の通信をファイヤーウォールや DMZ 内のサーバーを経由させて社外システムと制御システムが直接通信することを防ぎ、外部からのアクセスを制御する。

(c) DMZ を境界防護するファイヤーウォールはそれぞれメーカーが異なる複数のファイヤーウォール（ペアードファイヤーウォールあるいはマルチステージ・ファイヤーウォール）で構成することが望ましい。

(2) 近年の技術動向

DMZ の境界防護は、外部インターネットと DMZ 間の境界を防御するファイヤーウォールと DMZ と内部ネットワーク間の境界を防御するファイヤーウォールの 2 つのファイヤーウォール（ペアードファイヤーアウォール）で構成されることが多かったが、近年では DMZ を機能ごとにセグメントを細分化し、それぞれのネットワーク境界を防御するマルチステージ・ファイヤーウォールという概念で攻撃者の横展開（ラテラルムーブメント）を防止する DMZ を構築することを推奨するガイドラインも登場している。

5.2.4 ネットワーク境界の保護（ファイヤーウォールの設置）

ファイヤーウォールは、特定の通信のみを許可して未承認の通信をブロックし、異常な活動や不正な試みを監視・検出するものである。内部ネットワークへの不正アクセスを防止するものであり、リモートアクセスにおいてもセキュリティを強化しネットワークとデータの安全性を確保するために非常に重要である。

(1) 境界防御に関するセキュリティ対策推奨事項

ファイヤーウォール(FW) を導入し、ネットワーク境界における監視と保護を行う。以下、主要な設定項目について記載する。

(a) IP フィルタリング、MAC アドレスフィルタリング

リモートアクセスを許可する特定の IP アドレスや MAC アドレス、IP レンジを設定することで、許可された IP アドレスや MAC アドレスからのアクセスのみを受け入れるようにする。

(b) ポート制限

リモートアクセスに必要なポート（例えば、SSH の 22 番、HTTPS の 443 番、など）だけを開放し、それ以外のポートはすべて閉じる。

(c) プロトコル制限

特定のプロトコル（例えば、HTTP、HTTPS、RDP、SSH など）だけを許可し、それ以外のプロトコ

ルはブロックする。

5.2.5　リモートアクセス端末の管理

正規なリモートアクセス端末が不正利用された場合、リモートアクセスを拒否することが難しくなる。このため、リモートアクセス端末は企業や組織の IT 部門などによって管理されている端末を使用することが望ましい。

ここでは参考文献のテレワーク端末に関するアカウントの管理とエンドポイントセキュリティに関する要件を、制御システムへのリモート O&M に関連するリモートアクセス端末の要件として引用し、推奨事例として紹介する。

(1) リモートアクセス端末のアカウント管理に関するセキュリティ対策推奨事項

(a) アカウントの分離

(イ) 制限された権限のユーザーアカウントを使用し、管理者権限は別のアカウントで管理する。

(ロ) リモートアクセスはユーザーアカウントで行い、システムの設定変更などが必要な時にのみ管理者アカウントを使う。

(b) 管理者アカウント

(イ) 管理者権限の使用を最小限にし、かつ管理者アカウントでのログインは、特定の環境（例えば会社・オフィス）からのみしかアクセスできないように設定する。

(c) ユーザーアカウント

(イ) 各ユーザーに固有のアカウントを発行し、他人にそのアカウントを使わせない。
また操作履歴（いつ、だれが、何の操作をしたか）のログを記録し、特定可能にする。

(ロ) 複雑なパスワードを設定し(10 文字以上でアルファベット大文字、小文字、数字、記号を含むものを推奨)、パスワード入力時に画面に表示される文字を隠す。ログイン失敗が続くとアカウントをロックさせる。

(ハ) やむを得ず共用アカウントを使う場合は、操作履歴（作業記録や監視カメラで操作した人）を特定できるようにすることが望ましい。また定期的にパスワード変更を行う。

(ニ) 異動や担当者変更等に際して権限がなくなった者に対し、権限が残ったままにならないよう運用する。

(2) エンドポイントセキュリティに関するセキュリティ対策推奨事項

(a) OS 標準ファイヤーウォールの設定と有効化を行い、定期的に設定を見直す。

(イ) 不要なポートやサービスへのアクセスをブロックするように設定する。

(ロ) 最新の OS やソフトウェアおよびファームウェアのアップデートを随時行うことが望ましいが、パッチの適用可否や適用タイミングは、事業への影響や対処を見送った場合の影響などを考慮して決定する。

(b) アンチウィルスソフトの導入

(ｲ) アンチウィルスソフトをインストールし、常に最新の状態に保つ。

(c) EDR（Endpoint Detection and Response）ツールの導入

(ｲ) EDR ツールを導入し、異常な挙動を検知して即座に対応する。

(d) 不要なソフトウェアのアンインストール

(e) システム構築や変更時にセキュリティ機能の確認

(ｲ) システムやソフトウェアのセキュリティ設定が適切に構成されているかを確認する。

(ﾛ) 設定変更後に、セキュリティ機能が有効になっているかをチェックする。

5.2.6 機器のバックアップ

サイバー攻撃により影響を受けたシステムを元の状態に復元できないリスクを回避するため、データおよびシステムを迅速に復旧できるよう、機器のバックアップを取っておく必要がある。

(1) バックアップに関するセキュリティ対策推奨事項

(a) 代替機の準備

(ｲ) 代替機の用意: 現場の実機と同じスペックの PC やサーバーを用意。

(ﾛ) セットアップ: 必要なソフトウェアをインストールして設定。

(ﾊ) 保管: すぐに使えるように安全な場所に保管。

(b) バックアップと復旧手順の準備

(ｲ) バックアップ: 定期的にデータや設定のバックアップを取る。

(ﾛ) 保存: 安全な場所（オンサイトとオフサイト）にバックアップを保存。

(ﾊ) 手順書の作成: バックアップからの復旧手順を文書化。

(c) 復旧手順のテスト

(ｲ) テスト実施: 実際に代替機を使って復旧手順をテスト。

(ﾛ) 結果確認: テスト結果を確認し、問題がないかチェック。

(ﾊ) 手順の改善: 必要に応じて手順を修正し、再テスト。

(d) 定期的な確認

(ｲ) バックアップとテストの定期実施: 定期的にバックアップを取り、復旧テストを行う。

(ﾛ) 手順の更新: システムやソフトの変更に応じて手順を更新。

5.3　検知

5.3.1　監視・検知

通信の監視と検知を行うことで、ネットワーク上での異常な動きや攻撃の兆候を可視化し、脅威を把握することができ、より効果的な対策を講じることが可能となる。また、セキュリティ侵害や不正アクセスを早期に検知し、迅速な対応を取ることで、被害の拡大を防ぐことができる。

(1) 監視・検知に関するセキュリティ対策推奨事項

(a) ネットワーク監視

(ｲ) 侵入検知システム（IDS）と侵入防止システム（IPS）の導入を行い、ネットワーク境界や内部での不審な活動を監視・検出する。

(ﾛ) ネットワーク境界における監視強化を行い、社内ネットワークとインターネットの間の通信を監視する。

(b) 遠隔操作の監視

(ｲ) リモートセッションの監視を強化し、リモート操作中の活動をリアルタイムで監視する。

(ﾛ) リモートセッションの監視を行い、認可されたユーザーが正しくアクセスしているかを確認する。

(ﾊ) アクセスログを定期的にチェックし、異常がないかを監視する。不審な操作があれば即座にアラートを発する仕組みを整備する。

(c) 異常検知と対策

(ｲ) ネットワーク監視ツールを使用して、異常な活動（不審な送信元からの通信や不審なサービスへのアクセス等の異常な通信パターンやセキュリティイベントの増加等）を検知し、自動的に遮断する。

(ﾛ) 異常検知時には、セキュリティチームに通知する仕組みを設け、迅速な対応を行う。

(ﾊ) 異常検知と文書化のプロセスを確立し、検知された異常活動を詳細に記録し、分析や対策の基礎とする。

5.3.2　ログ収集・分析

ログは不審な操作履歴やセキュリティ侵害の兆候を検知し、セキュリティイベントをリアルタイムで把握するために重要である。ログの収集と分析により、セキュリティインシデントが発生した場合やシステムの問題がある場合に、迅速かつ効果的な対応を行うことができる。また、ログを確認することで、過去に発生したサイバー攻撃を検知できる場合がある。

(1) ログの種類

ログには以下のような種類がある

(a) アクセスログ

誰が、いつ、どこにアクセスしたかを記録する。例えば、VPN 接続ログやリモートデスクトップのセッションログなどである。

(b) 認証ログ

認証の成功や失敗の履歴を記録する。失敗したログイン試行回数や、どの IP アドレスからの試行かを記録する。

(c) 操作ログ

ユーザーが行った具体的な操作内容を記録する。例えば、ファイルの作成・変更・削除などの操作ログである。

(d) イベントログ

システムやアプリケーションで発生したイベントを記録する。例えば、システムの起動・停止やエラー発生などである。

(2) ログ収集・分析に関するセキュリティ対策推奨事項

(a) ログ収集と確認

リモートアクセスに関するログをできるだけ詳細に取得し、定期的に確認・分析する。

(ｲ) ログの定期的な確認:

取得したログを定期的に調べ、不審な活動がないか確認する。例えば、毎週または毎月ログをレビューし、異常なアクセスや操作がないかをチェックする。

(ﾛ) 確認すべき点:

作業時間外の操作: 深夜や休日など、予定外の時間に操作されていないか。

不正な利用者: 管理者アカウントなど、予定外の利用者が操作していないか。

予定外の操作: 予定されていた作業以外の操作・設定が実施されていないか。

(b) 機能の活用と補充

リモートアクセスソリューションが提供する詳細なログ機能を活用する。例えば、VPN アプリケーションやリモートデスクトップサービスのログ機能を使って、すべてのアクセスを記録する。

リモートアクセスサーバーが特定のログを取得できない場合、リモートアクセスを通じて使用されるリソース（クライアント側のデバイスやアプリケーション）でのロギングを検討する。

(c) ログの一元管理

ログを一元管理するために、Syslog サーバーを導入する。Syslog サーバーはネットワーク上の複数のデバイスからログを集約し、効率的に管理できるように設定する。

(d) ログのバックアップ

重要なログファイルは定期的にバックアップを取る。例えば、毎日バックアップを自動で実行し、バックアップファイルを安全な場所に保存する。

(e) 時刻同期

社内の NTP サーバーを設置する、あるいは GPS 受信機による時刻情報を取得させて、すべてのデバイスが定期的に時刻を同期するよう設定する。

5.4 対応

5.4.1 連絡・報告体制

サイバー攻撃への対処には、各人員の役割に応じた行動のルールや連絡方法などの体制を整備する必要がある。多岐にわたる関連システムに対応するため、迅速な初動と影響範囲の限定が重要である。適切な連絡・報告体制を整えることで、情報共有や緊急事態への迅速な対応が可能となり、リスク管理や情報セキュリティの強化にも役立つ。

(1) 連絡・報告体制に関するセキュリティ対策推奨事項

(a) 運転員からの報告への対応

現場の運転員がセキュリティ上の異常に気付く場合があるため、報告を見落とさないよう、連絡先や連絡内容を整理しておく。

(b) 社外の専門組織との連絡体制

社内だけでは対処が難しい場合に備えて、社外のセキュリティ専門組織との連絡体制を確立し、支援要請の方法を規定しておく。

(c) 事業継続への影響

封じ込めや根絶、復旧などのアクションは事業継続に影響を与える可能性があるため、事業継続の責任者を含む幹部層が適切な指示を出せるよう、全社的な連絡体制を構築しておく。

(d) 現場での対応体制

実際のシステムに対する対処は、現場の運転員がセキュリティ専門組織の指示を受けながら行うため、現場での連絡体制を整備しておく。

(e) 知識共有の重要性

インシデントへの対応が終了した後には、得られた知見を関連する組織間で共有できるよう、情報発信と情報受信・検討の組織を整備する。

5.5　リモートアクセスにおけるセキュリティ対策の総括

これまで、リモートアクセスに関連する文献・ガイドラインに記載された対策を述べてきたが、本書で記載した対策は制御システムに対する数あるセキュリティ対策の一部であり、これだけやっていればよいというものではない。

脅威に対応するためにはシステム構成面、物理面どちらか一方でなく双方の対策が重要となり、また、技術的な対策の他、従業員に対する継続的な教育実施など、運用面での対応も必要になってくる。

また、各企業の事業内容によって、制御システムに対するセキュリティ対策の深化や実施範囲は異なってくる。セキュリティ対策の検討に際しては、「第 4 章　制御システムにおけるリスク分析手法」で述べたリスク分析を実施したのち、組織にとって最も重要な対策から実施していくことが重要である。本書ではセキュリティ対策の検討も含めた具体的な適用事例についても、「第　6　章　要件定義に基づくシステム構成検討プロセス」に記載しているので参考にされたい。

なお、制御システムを含む工場システムに対するセキュリティ対策としては、以下の文献が参考になるので一読されたい。

- 引用・参考文献[19]：経済産業省／工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
- 引用・参考文献[24]：独立行政法人　情報処理推進機構／スマート工場のセキュリティリスク分析調査
- 引用・参考文献[25]：独立行政法人　情報処理推進機構／スマート工場化でのシステムセキュリティ対策事例 調査報告書

第6章　要件定義に基づくシステム構成検討プロセス

前章まではリモートアクセス方式や制御システムにおけるリスク分析手法、リモートアクセス時のセキュリティ対策推奨事項などを紹介した。本章では、リモート O&M を実施するための基本的なシステム構成を検討する際にどのようなプロセスでシステム構成を決定する必要があるか、具体例を示しながら記載する。

6.1　システム構成を検討する前に

制御システムへのリモート O&M をどのような目的で実施するか、対象拠点・範囲、アクセスするユーザーの定義、制御システムの重要度、運用管理体制、規制による制約などを踏まえた要件定義は、企業によって様々である。また、人材・予算などの経営資源も企業によって異なり、リモート O&M の導入により必ずしも利益を享受できるわけではないことを念頭に置く必要がある。

リモート O&M の導入により、安全で柔軟な労働環境の提供や、人的リソースの最適化、メンテナンス時の移動時間削減など、多くの＋(プラス)の効果を得ることができる。しかしながら、システムの導入や維持管理コストだけでなく、セキュリティ対策が不十分な場合、セキュリティインシデントの発生により大きな経営的損失を招く可能性もあることから、－(マイナス)の効果についても考慮する必要がある。そしてセキュリティ対策はそのセキュリティインシデントの発生を抑制するものであり、全体の経営上のバランスを見ながら最適なシステム構成の検討、リモート O&M の導入を進めることが肝要である。下図はその概念を示したものであり、参考にされたい。

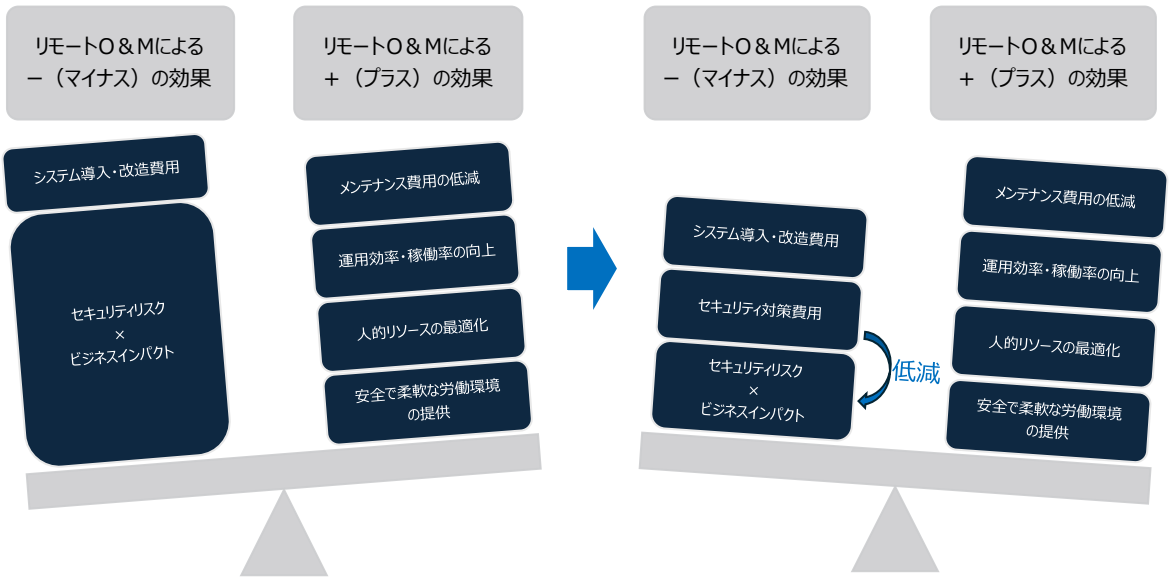


図 6-1：リモート O&M の導入による経営上のバランス

6.2　要件定義に基づくシステム構成検討プロセスの全体像

本節は、要件定義に基づくシステム構成検討プロセスの全体像を明示する。先述したように制御システムへのリモート O&M を実施する目的や条件などは企業によって様々であり、セキュリティ対策を考慮したシステム構成を一意に決定することはできない。しかしながらその検討プロセスを理解することで、段階的に必要な情報を収集・判断し、自社の目的にあったシステム構成を決定することができる。以下に各プロセスの概略図を示す。

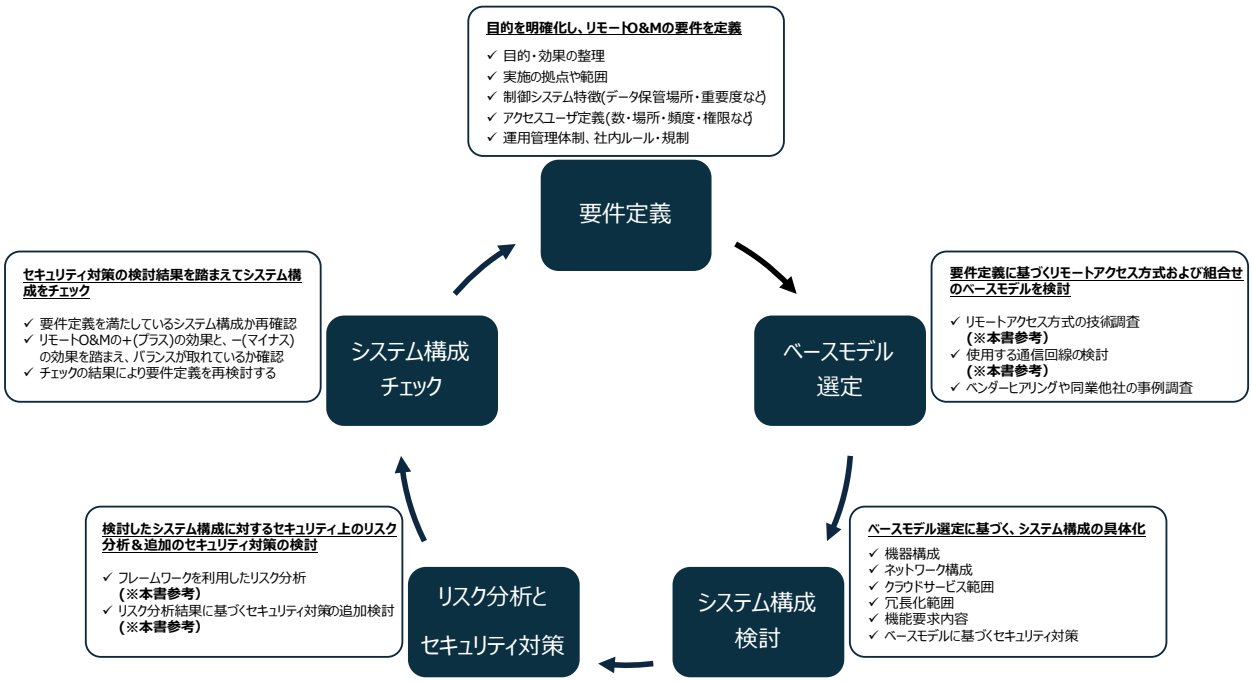


図 6-2：要件定義に基づくシステム構成検討プロセスの概略図

6.2.1　各プロセスの定義

本書では制御システムへのリモート O&M を実施するシステム構成を検討するプロセスを以下の(1)～(5)のように定義する。それぞれのプロセスの詳細な内容については次節以降で解説する。

(1) 要件定義

目的を明確化し、リモート O&M の要件を定義する。実施の拠点や範囲、アクセスするユーザーの定義、許容する通信障害への対応、運用管理体制、規制・社内セキュリティポリシーなどを含む。

(2) ベースモデル選定

要件定義に基づき、リモートアクセス方式および組合せのベースモデルを検討する。技術調査、ベンダー事例調査、通信回線の検討などを行う。

(3) システム構成検討

ベースモデル選定に基づき、システム構成の具体化を行う。機器構成、ネットワーク構成、クラウドサー

ビスの範囲、冗長化範囲、機能要件、ベースモデルに基づくセキュリティ対策を検討する。

(4) リスク分析とセキュリティ対策

検討したシステム構成に対するセキュリティ面のリスク分析と対策の検討を行う。フレームワークを用いたリスク分析、およびリスク分析結果に基づく追加のセキュリティ対策を検討する。ただし本書では制御システムへのリモート O&M に特化した内容としており、入退出管理などを含む制御システム全体に対するセキュリティ対策は別途実施する必要がある。

(5) システム構成チェック

セキュリティ対策の検討結果を踏まえてシステム構成をチェックする。リモート O&M の+(プラス)の効果と、ー(マイナス)の効果を踏まえ、バランスが取れているか確認しシステム構成を決定する。チェックの結果によっては要件定義からの見直しを要する。

6.3 要件定義

要件定義ではリモート O&M を実施する目的を明確化し、ベースモデルの選定に必要な要件を整理・定義する。この要件定義は後続のプロセスに大きな影響を与えるため、精緻な検討が求められる。

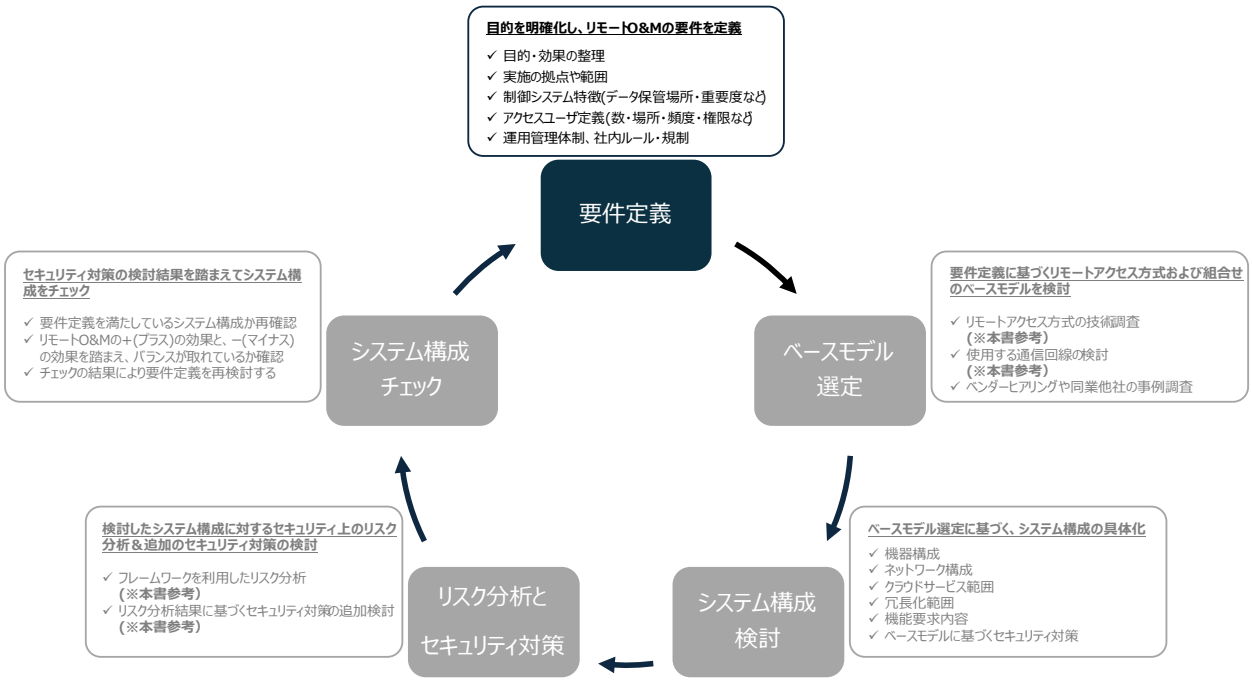


図 6-3：要件定義プロセス

6.3.1 目的・効果の明確化

本書では制御システムへリモートアクセスする目的をリモート O&M に限定しているが、リモートオペレーションと

リモートメンテナンスを誰がどのような目的で実施するのか要件定義にあわせて明確にする必要がある。また、リモート O&M を実施することで得られる＋(プラス)の効果についても自社の状況に応じて整理することで、最終的にバランスを見ながら最適なシステム構成を検討することができる。

6.3.2 目的・効果の整理例

ここでは既存の制御システムがある企業を想定し、リモート O&M の機能を制御システムへ付加する際の目的と効果について例示する。下記の表と図の通り、現状と課題を整理の上、リモート O&M の実施目的とその効果を明確化した。

表 6-1：リモート O&M の実施目的・効果の整理例

項目	内容
現状	・ とある製造ラインの現場では制御システムに接続されたプログラマブル表示器があり、オペレーション部門がそのプログラマブル表示器を利用して、24 時間 365 日体制で運転操作をしている。 ・ HMI/EWS 端末も制御装置に接続されており、制御装置の調整やメンテナンスが可能となっている。日勤のメンテナンス部門がオペレーション部門からの要請を受け、対応している。
課題	・ 普段はメンテナンス部門の担当者 2 名が日勤帯に対応しているが、出張などにより両名不在時に制御装置の調整やメンテナンスを要する場合には、製造ラインの停止を余儀なくされることもあり、生産効率の低下を招いている。 ・ 緊急時には自宅から呼び出しなども実施しており、メンテナンス部門の大きな負担となっている。
↓↓	
目的	・ 特定の拠点に縛らせず、出張先や自宅などから制御装置の調整・メンテナンスができる環境を、必要最小限のコストで構築し、上記課題の解決を図りたい。
効果	・ 制御装置の調整・メンテナンス即時対応を可能とし、製造ラインの停止期間短縮による生産効率の向上および収益向上。 ・ 緊急呼び出しの低減に伴うメンテナンス部門の負担軽減。

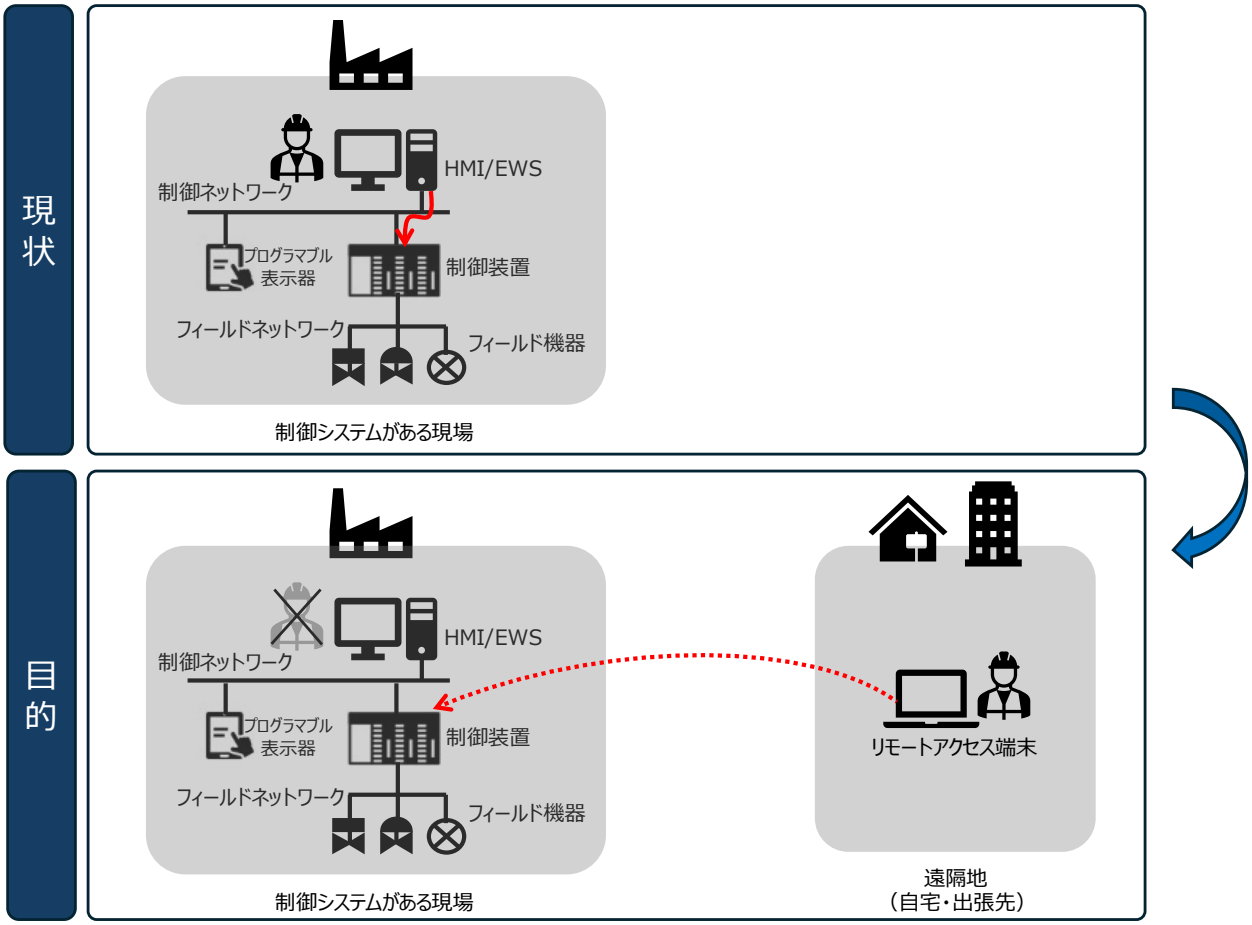


図 6-4：リモート O&M の実施事例-概念図

6.3.3　要件定義の項目

以下に要件定義の項目を示すが、目的に応じて必要な要件を追加設定することを推奨する。

(1) 対象拠点・範囲

リモート O&M の対象とする拠点や制御システムの範囲を明確に定義する必要がある。単一拠点へのリモートアクセスが必要な場合もあれば、複数拠点にわたるアクセスが求められることもある。また、制御システムが単一拠点に複数ある場合もあるため、対象となる制御システムの範囲を明確にする必要がある。

(2) 制御システムの特徴

リモート O&M を導入するにあたり、対象となる制御システムの特徴を明確にすることが重要である。これにより、適切なシステム構成を選定し、リスク分析とセキュリティ対策を効果的に実施することが可能となる。

(a) データ保管場所

データの保管場所を明確に定義する必要がある。例えば先述した「3.2 プライベートネットワーク方式」

の場合には、遠隔地のリモートアクセス端末上にデータが保存される場合があるため、端末の紛失や盗難による情報漏えいリスクがある。そのため、それが許容できない場合、他のリモートアクセス方式を選択する必要がある。

(b) 通信プロトコル

制御装置へ最終的にする通信プロトコルの確認・定義はリモートアクセス方式や通信回線の選択に大きく影響する。例えば先述した「3.2 プライベートネットワーク方式」の場合には、リモートアクセス端末から制御装置に対して直接通信を行うため、制御装置に対応したプロトコルを利用する必要がある。そのため、選択する通信回線によってプロトコルの制限を受ける。また、既存の制御システムをリモート O&M 化する場合、使用されるプロトコルが通信回線の選択を制限することになる。

(c) 許容する通信障害頻度

下記のビジネスインパクトとも関連するが、通信障害が発生すると、想定する利用目的へ大きな影響を及ぼす場合があるため、どの程度の通信障害を許容するか定義しておく必要がある。通信事業者の通信回線は一般的に SLA（Service Level Agreement）と呼ばれる契約に基づきサービスが提供され、その SLA 範囲内での保証がなされるが、事業機会の損失などは保証されないことが多い。例えば月に 1 回の定期メンテナンスと、24 時間 365 日体制でオペレーションしたい場合では許容される障害頻度は大きく異なる。

(d) 応答速度

リモート O&M の操作に対する制御システムの応答速度を定義する。応答速度は、通信インフラの選定や中継機器の数などに大きな影響を与える。例えば、発電プラントの制御システムでは、リアルタイム制御が必要であり、操作指示からシステムの反応までの遅延は数ミリ秒以下を求められる場合がある。

(e) ビジネスインパクト

制御システムが停止または故障した場合のビジネスへの影響を評価しておく必要がある。例えば、製造業では生産ラインが停止すると、納期遅延や顧客の信頼失墜に繋がる可能性がある。影響が大きい場合はリモート O&M を実施する通信回線やシステムの可用性などを高める必要があり、リスクとビジネスインパクトによってはリモート O&M の実施そのものを再検討する必要がある。

(3) アクセスユーザーの定義

(a) アクセスする人

自社の制御システムに対してリモート O&M を実施する人を明確に定義する必要がある。例えば社内の技術者であれば、一般的に自社の閉域網を利用することができるが、社外者は社内ルールで自社

の閉域網へのアクセスが禁止されている場合もある。制御システムへのリモートメンテナンスのためにアクセスしたい場合には専用の閉域網を構築するか、インターネット VPN を活用するなどする必要があり、通信回線を含むリモートアクセス方式の選定に影響する。

(b) アクセス数

想定される同時接続数やピーク時のアクセス数は、通信容量や、ユーザーがアクセスするシステム（制御装置、HMI/EWS 端末、VPN 機器など）の負荷にも係るため定義する必要がある。また多数のアクセスが見込まれる場合には、後述するアクセス管理も考慮に入れて、自社の人的リソースにあったリモートアクセス方式を選定していく必要がある。

(c) アクセス場所

制御システムへのリモートアクセスはプライベートネットワークを介して接続することが求められるため、アクセス場所によって通信回線の選択に大きな影響を及ぼす。また既存の自社の通信インフラを活用できるのかにも影響する。リモートアクセス方式の選択にもよるが、地理的に制限されたアクセスの場合には IP フィルタリングが有効な場合もあるため、アクセス場所の設定は重要である。

(d) アクセス頻度

アクセス頻度も、リモート O&M を実施する目的に応じて設定する。例えば、定期メンテナンスは月に 1 回行い、システム更新や緊急対応時には随時アクセスするなど、リモートメンテナンスの目的に応じてスケジュールに基づいて設定する。リモートオペレーションについても、24 時間 365 日体制で運用が必要なのか、緊急時の補助的なオペレーションなのかによってアクセス頻度は異なる。高頻度のアクセスが見込まれる場合には、アクセス数と同様にアクセス管理も考慮に入れて自社の人的リソースにあったリモートアクセス方式を選定していく必要がある。

(e) アクセス端末

アクセス端末が悪意を持った人に汚染された場合に、リモート O&M でアクセスする制御システムへ重大な影響を及ぼす。重要な制御システムへのアクセスには自社で管理された端末からアクセスすることが望ましいが、社外ベンダーによるリモートメンテナンスなど自社で管理していない外部接続端末からのアクセスを実施したい場合がある。リモートアクセス方式の選定や、外部接続端末へのセキュリティ対策内容に影響があるため、アクセス端末を設定する。

(4) 運用管理体制

リモート O&M を効果的に運用するための管理体制を定義する。これには、アクセス管理、監視、障害対応、脆弱性管理などが含まれ、この要件により自社の人的リソースにあったリモートアクセス方式を選

定していく必要がある。

(a) アクセス管理

リモートアクセスを行うユーザーの認証とアクセス権限の管理をどのように実施するか定義する。例えば、複数の拠点や制御システムへのアクセスが見込まれる場合には、それに対応し得る体制が整っているか、整っていない場合は体制を構築するのか、現状の体制で管理できるようにするかなどを定義する必要がある。

(b) 監視体制

リモート O&M を実施する制御システムに対する不正アクセスや異常な活動を検出できる体制を整備する必要がある。例えば、IT システム部門で既に監視体制が構築されている場合には連携をとり、SIEM（Security Information and Event Management）などを活用して、アクセスログの収集と解析を行い、セキュリティインシデントの早期発見と対応を図れるか確認する。連携が難しい場合には、自部門や外部機関で新たに体制構築を検討し定義する。

(c) 障害対応

リモートアクセスに関連する障害が発生した場合の体制・対応手順を定義する必要がある。例えば、制御システムがある現地側が有人か無人かで、障害対応の体制や手順も異なってくる。本書はリモート O&M に特化した内容であるが、対象となる制御システムの重要度や規制なども影響するため、考慮する必要がある。

(d) 脆弱性管理

リモートアクセスに関わる機器やソフトウェアの脆弱性を定期的に評価・管理する必要がある。また、脆弱性情報の収集と対応策の実施に関するプロセスを確立し、脆弱性が悪用される前に対策を講じる必要がある。近年、脆弱性を悪用した攻撃が増加しており、これらの攻撃は制御システムに深刻な影響を与える可能性があるため、設計段階からルールを明確に定め、実行性のある弱性管理体制を構築することが不可欠である。

(5) 規制・社内セキュリティポリシー

リモート O&M を実施するにあたり、関連する規制や社内セキュリティポリシーを明確に定義することが重要である。これにより、システム構成やリスク分析、セキュリティ対策の設計段階で遵守すべき要件が明確となり、適切な対策を講じることができる。

(a) 規制

業界特有の規制・コンプライアンスに遵守したシステムとする必要があるため、関連する要件を定義す

る。例えば高圧ガス保安法や電気事業法などの関連規定でサイバーセキュリティの確保が求められている。

(b) 社内セキュリティポリシー

社内のセキュリティポリシーを確認し、リモート O&M に適用するための要件を定義する。例えば、社内セキュリティポリシーで、制御システムへの直接的な VPN 接続禁止や多要素認証（MFA）の導入、管理者承認などが明示されている場合もある。

6.3.4 要件定義の整理例

要件定義の項目について説明をしたが、具体的な要件定義の整理例を以下に示す。

表 6-2：要点定義の整理例

要件定義項目		内容
(1)対象拠点・範囲	－	単一拠点・単一制御システム
(2)制御システムの特徴	(a)データ保管場所	・機微な設定データもあり、リモートアクセス端末にはデータを保管しない ・平日は現場の HMI/EWS 端末で作業するため、現場端末に一括してデータを保存したい
	(b)通信プロトコル	制御装置への通信は TCP/IP を利用した特殊プロトコル
	(c)許容する通信障害頻度	緊急呼び出しによる既存運用でカバーすることで許容可能
	(d)応答速度	要求しない
	(e)ビジネスインパクト	生産ライン停止による影響はあるが限定的
(3)アクセスユーザーの定義	(a)アクセスする人	社内メンテナンス部門技術者 A 氏および B 氏
	(b)アクセス数	上記社内技術者 2 人
	(c)アクセス場所	自宅や出張先など不特定な場所
	(d)アクセス頻度	月に 1 回～数回
	(e)アクセス端末	社内管理端末 2 台
(4)運用管理体制	(a)アクセス管理	単一拠点・単一制御システムのため既存のメンテナンス部門で管理
	(b)監視体制	IT 部門の 24 時間 365 日体制の SOC へ通知後、緊急連絡体制で対応
	(c)障害対応	現場側のオペレーション部門が 24 時間 365 日体制で対応
	(d)脆弱性管理	単一拠点・単一制御システムのため既存のメンテナンス部門で定期的に対応
(5)規制・社内セキュリティ	(a)規制	リモートアクセスや通信回線に関する規制なし

ポリシー	(b)社内セキュリティポリシー	制御システムへのリモートアクセス自体は禁止されてないが、現地システム内に中継機器を設置することを推奨

6.4　ベースモデル選定

次に要件定義に基づき、リモートアクセス方式および組合せのベースモデルを検討する。「第 3 章 リモートアクセス方式」で説明したようにリモートアクセス方式は様々な形態があり、要件定義に基づき、ベースとなるリモートアクセス方式を選定する。また通信回線についても複数の選択肢があることから要件定義に基づき、目的やコストを含めて検討していく。必要に応じてベンダーヒアリングや同業他社の事例も参考にしながら実施する。

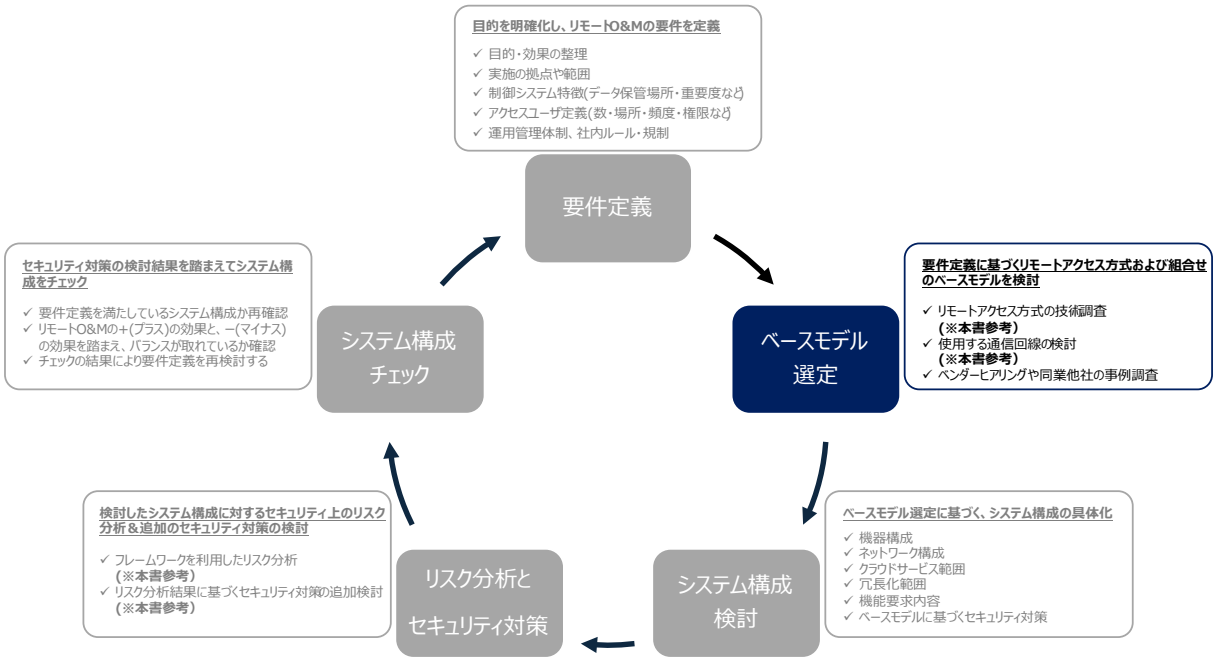


図 6-5：ベースモデル選定プロセス

6.4.1　ベースモデルの選定例

「6.3.4 要件定義の整理例」で定めた要件を元にベースモデルを選定していく。具体的な選定検討の検討内容の例を下表に示す。

表 6-3：要点定義に基づくベースモデルの選定検討例

要件定義内容			選定時の検討内容
(1) 対象拠点・範囲	−	単一拠点・単一制御システム	全てのリモートアクセス方式で要件は満足するが、拠点数も少ないことから高額

			な通信回線やクラウド型のアクセス管理機能は不要
(2)制御システムの特徴	(a)データ保管場所	・機微な設定データもあり、リモートアクセス端末にはデータを保管しない ・平日は現場の HMI/EWS 端末で作業するため、現場端末に一括してデータを保存したい	「プライベートネットワーク方式」と「仮想デスクトップ方式」は要件を満たさないため、「リモートデスクトップ方式」が適切
	(b)通信プロトコル	制御装置への通信は TCP/IP を利用した特殊プロトコル	技術的な通信回線の制約はない
	(c)許容する通信障害頻度	緊急呼び出しによる既存運用でカバーすることで許容可能	目的の「必要最低限のコスト」制約から、インターネットを利用した通信回線
	(d)応答速度	要求しない	同上
	(e)ビジネスインパクト	生産ライン停止による影響はあるが限定的	制御システムへのリモートアクセスを起因としたリスクは適切なセキュリティ対策を講じることで許容可能
(3)アクセスユーザーの定義	(a)アクセスする人	社内メンテナンス部門技術者 A 氏および B 氏	社内技術者のため、通信回線の制約はない
	(b)アクセス数	上記社内技術者の内最大 1 人	最大アクセスが 1 人のため、リモートアクセス方式であっても通信容量や機器の負荷は低い
	(c)アクセス場所	自宅や出張先など不特定な場所	特定の拠点がないため、拠点間通信は選択できない
	(d)アクセス頻度	月に 1 回～数回	高額なクラウド型のアクセス管理機能などは不要
	(e)アクセス端末	社内管理端末 2 台	自社でリモートアクセス端末のセキュリティ対策を講じる
(4)運用管理体制	(a)アクセス管理	単一拠点・単一制御システムのため既存のメンテナンス部門で管理	アクセス管理のアウトソースや高額なクラウド型のアクセス管理機能などは不要
	(b)監視体制	IT 部門の 24 時間 365 日体制の SOC へ通知後、緊急連絡体制で対応	セキュリティ装置などの異常検知を IT 部門へ通知するなどの処置を講じる
	(c)障害対応	現場側のオペレーション部門が 24 時間 365 日体制で対応	リモートアクセス障害による運用への影響は軽微であり、稼働率が高い SLA の通信回線は不要
	(d)脆弱性管理	単一拠点・単一制御システムのため既存のメンテナンス部門で定	通信事業者やクラウド型サービス以外の機器は自社で定期的に管理し、年次

		期的に対応	点検のタイミングで対応する
(5) 規制・社内セキュリティポリシー	(a)規制	リモートアクセスや通信回線に関する規制なし	リモートアクセス方式や通信回線の選択に関する制約はない
	(b) 社内セキュリティポリシー	制御システムへのリモートアクセス自体は禁止されてないが、現地システム内に中継機器を設置することを推奨	直接的に既存の制御システムへのアクセスを避ける処置が必要であり、内部に中継サーバーを設置する

以上の検討内容から「①リモートデスクトップ方式」「②拠点間通信を利用しないインターネット VPN」「③クラウドや外部サーバーは利用しない」「④システム内への中継サーバー設置」といった条件が整理される。

これらの条件を満足するリモートアクセス方式として、「3.2(3)(a)VPN 用アプリケーションを利用したプライベートネットワーク方式」で示したプライベートネットワークを利用した「3.3(2)中継サーバーを利用したリモートデスクトップ方式」をベースモデルとしてシステム構成の検討を進める。

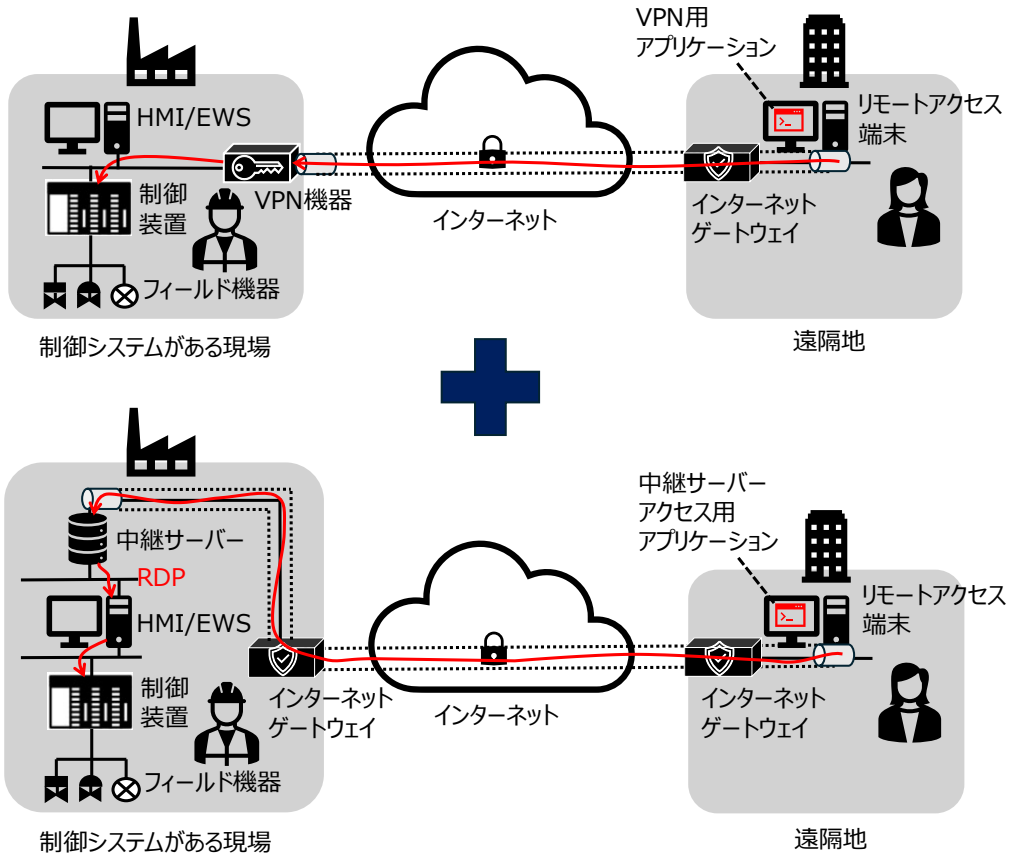


図 6-6：ベースモデルの選定例

6.5　システム構成検討

次にベースモデル選定に基づき、システム構成の具体化を行う。システム構成を具体化する際には、まずベースモデルに基づく構成要素の洗い出しを行い、それぞれの機能要件や非機能要件を明確にする必要がある。また、要件定義の内容を考慮しながら、システム全体のスループットや可用性を確保するために、負荷分散や冗長化の手法を検討し、適切なハードウェアおよびソフトウェアを選定する。

既存の制御システムがある場合にはその既存システムと同調を取りながら、どのようにベースモデルの機能を付加していくか検討する必要がある。なお、新規にリモートアクセス機能を有した制御システム全体を構築する場合には既存システムが無いことから自由度は高いが、要件定義の内容が精緻に定まっていないとベースモデル選定が難しく、システム構成の検討も難しいものとなる。

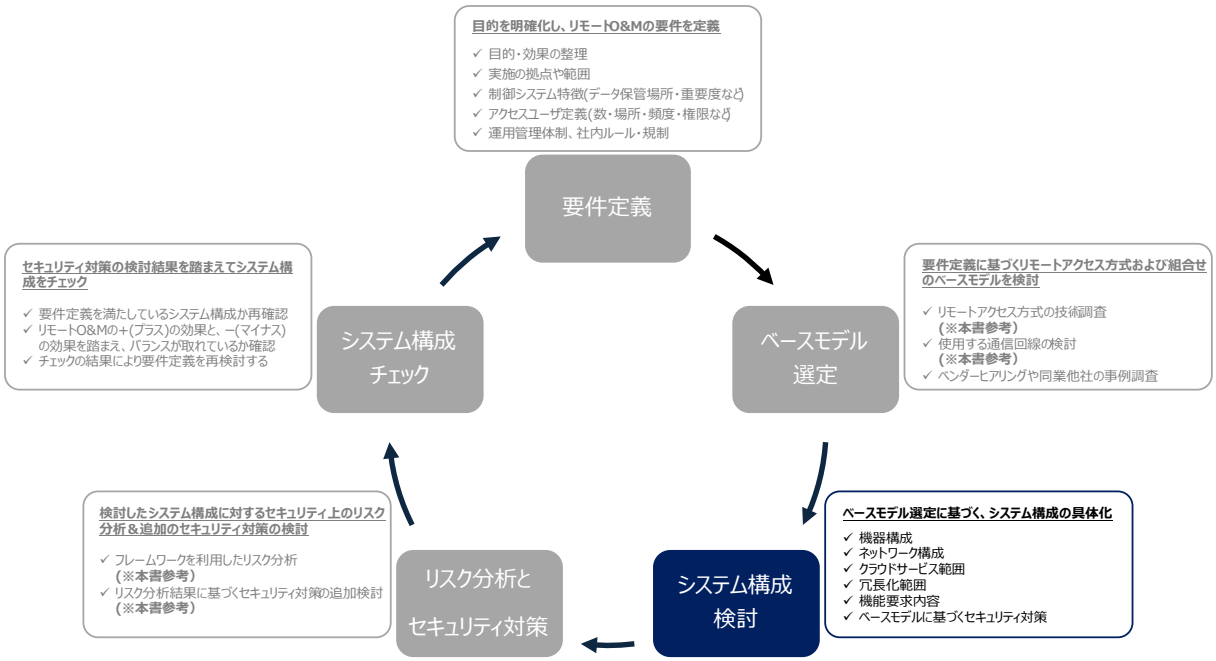


図 6-7：システム構成検討プロセス

以下に具体的な検討項目を示すが、必要に応じて追加することを推奨する。

(1) 機器構成

システムを構成するハードウェアの選定を行う。リモート O&M を実現するためのサーバー、ネットワーク機器、端末機器などが含まれる。

(2) ネットワーク構成

ネットワーク全体の構成を設計する。例えばインターネット VPN を利用する場合、外部からのアクセスを安全に確保するために必要な構成を検討する。また、社内ネットワークを利用する場合には、社内ネット

ワークとリモートアクセスネットワークのセグメント化を行う必要がある。

(3) クラウドサービスの利用範囲

クラウドサービスを利用する場合、その範囲を明確にする。例えば、監視システムとしてクラウドを活用する場合、その構成を詳細に設計する。

(4) 冗長化と可用性の確保

要件定義を考慮し、システムの可用性を確保し、スループットを向上させるために、負荷分散を含む冗長化の手法を検討する。

(5) 機能要件の詳細化

システムが提供する各機能について詳細に要件を定義する。リモート O&M に必要な機能を具体的に記載し、それぞれの実装方法を検討する。

(6) セキュリティ対策

リスク分析前であるため、ベースモデルに基づくセキュリティ対策をまず検討するものとし、追加のセキュリティ対策はリスク分析の結果によって実施する。

6.5.2 システム構成の検討例

「6.4.1 ベースモデルの選定例」で選定したベースモデルに基づき、具体的なシステム構成を検討していく。以下に、検討内容と検討した結果のシステム構成を示す。

表 6-4：システム構成の検討内容例

検討項目	内容
(1)機器構成	・VPN 機器（VPN サーバー機能、ルーティング機能、FW 機能を含む機器）を新たに設置し、インターネット VPN 経由で制御システムへアクセスできる環境を整備する。 ・中継サーバーをリモートデスクトップ先の HMI/EWS 端末と VPN 機器間に設置し、HMI/EWS 端末が直接外部と接続しない構成とする。 ・HMI/EWS 端末は流用の上、新たなネットワークカードを追加し、リモートデスクトップの機能を有効化する。 ・リモートアクセス端末は自社管理の端末とし、VPN 機器に対応した VPN 用アプリケーションをインストールする。
(2)ネットワーク構成	・VPN 機器の SSL VPN 機能を利用して、リモートアクセス端末とトンネリングする。暗号化方式は標準のものを使用する。 ・VPN のルーティング機能を利用して、中継サーバーと HMI/EWS 端末、インターネットのネットワークセグメントを分離する。
(3)クラウドサービスの利用範囲	・クラウドサービスは利用しない。

(4)冗長化と可用性の確保	・要点定義で整理したように通信障害は考慮しないため、リモートアクセスの構築に必要な機器・ネットワークの冗長化対策は実施しない。 ・アクセス数も限定的であるため、負荷分散のためのロードバランサー等は設置しない。
(5)機能要件の詳細化	・VPN 機器のユーザー認証方式は ID・パスワード入力による認証とする。 ・VPN 機器の異常検知を IT 部門へ通知できるようメール通知機能を有するものにする。 ・VPN 接続されたユーザーは一旦中継サーバーでの認証後に、HMI/EWS 端末に RDP 接続する。
(6)セキュリティ対策 （リスク分析前）	・DMZ を設ける。 ・VPN 機器の FW 機能を活用して、不要な通信を遮断する。 ・脆弱性対策をした VPN 機器、中継サーバーおよびリモートアクセス端末を設置し、設置後はメンテナンス部門で年次点検のタイミングで対応する。

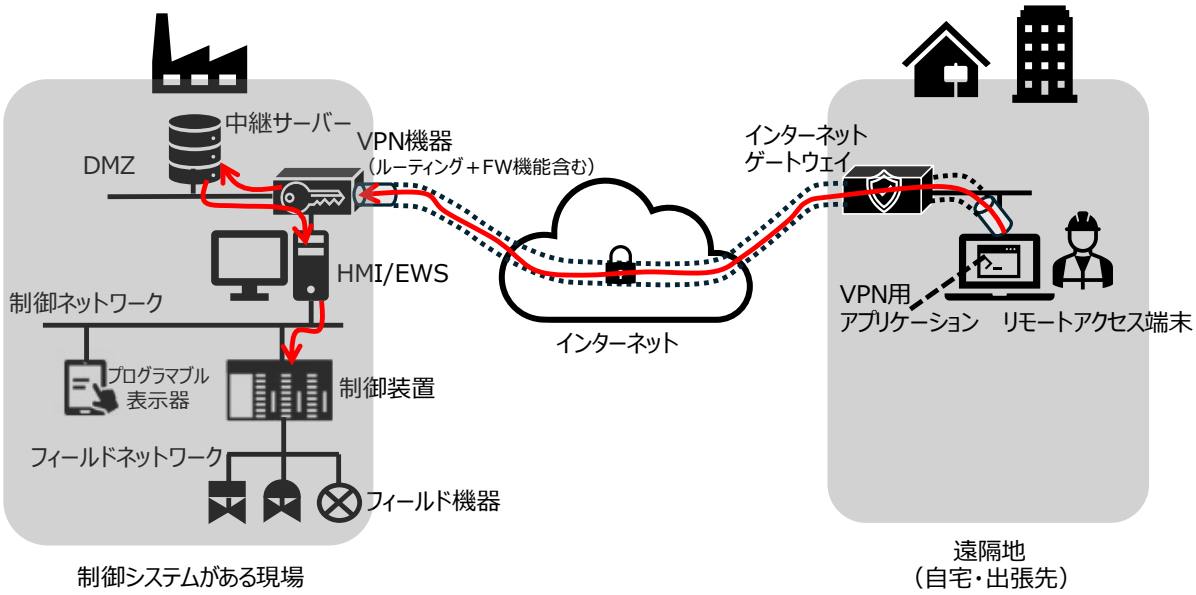


図 6-8：システム構成の検討例

6.6 リスク分析とセキュリティ対策

制御システムにリモートアクセスを導入する際には、リスク分析とそれに基づくセキュリティ対策が重要である。リスク分析は、システムが直面する可能性のある脅威を特定し、その影響を評価するプロセスである。本書ではリスク分析とセキュリティ対策を考えるための方法として、「4.3.1 CCE」で紹介した CCE（Consequence-driven Cyber-informed Engineering）によるリスク分析手法を実施する。

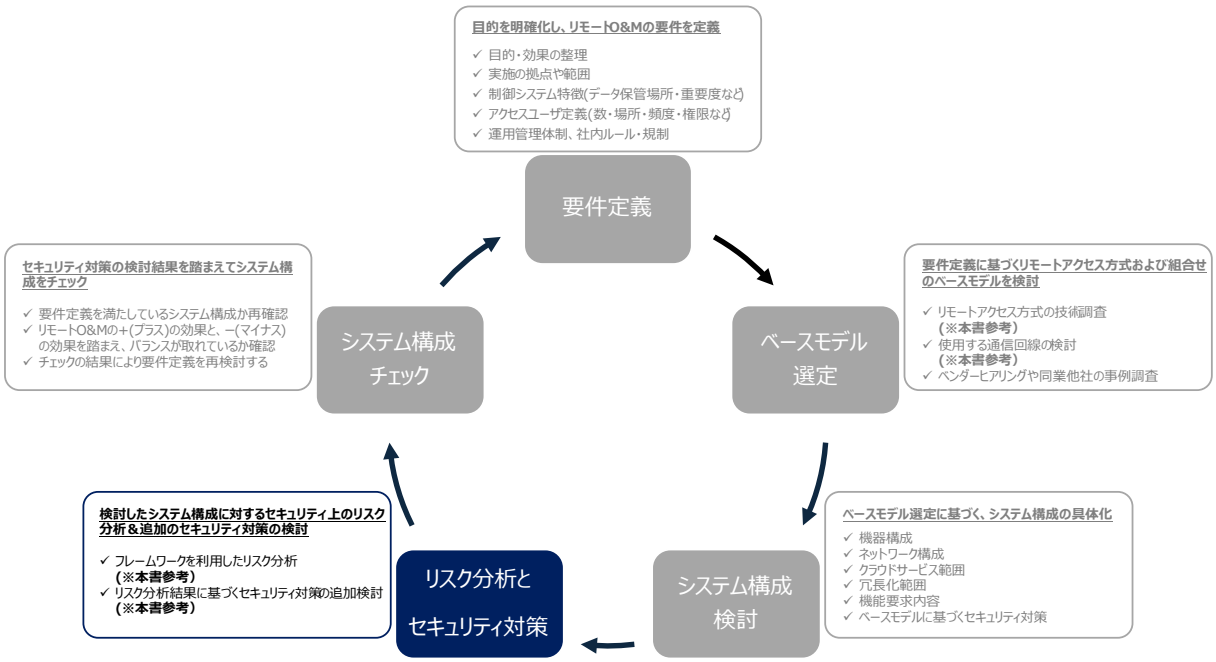


図 6-9：リスク分析とセキュリティ対策プロセス

6.6.1　CCE によるリスク分析とセキュリティ対策検討例

「6.5.2 システム構成の検討例」で検討したシステム構成に対して、CCE によるリスク分析例とセキュリティ対策検討を実施する。以下に、リスク分析内容とセキュリティ対策を講じた結果のシステム構成を示す。

(1) ステップ 1: 発生してほしくない事象の洗い出し

まず、システムにおいて発生してほしくない事象を洗い出し、対応の優先順位をつける。この段階ではサイバーセキュリティのことは考えず、単に発生してほしくない事象を検討する。

(a) 制御装置が暴走し、安全（事故・労災）に影響を及ぼす

(b) データの改ざんや漏洩により、業務運用に支障をきたす

(c) 不正アクセスにより、システムが停止し製造ラインが止まる

これらの事象をもとに、リスクの大きさや発生頻度を考慮して優先順位をつける。本ケースでは発生してほしくない事象として、「(a)制御装置が暴走して安全（事故・労災）へ影響を及ぼす」ことを最大のリスクとする。

(2) ステップ 2: 関連システムやサブシステムの洗い出し

次に、上記の事象を引き起こす可能性のある関連システムやサブシステムを洗い出す。ここでは STEP 1 に関連する関連システムとサブシステムに限定して洗い出しを実施し、以下の機器が該当することが分

かる。

(a) 制御装置

(b) プログラマブル表示器

(c) HMI/EWS 端末

(3) ステップ 3: サイバー攻撃の検討

次に、ステップ 1 で洗い出した事象を、ステップ 2 で特定したシステムやサブシステムを用いて発生させるには、どのようなサイバー攻撃が考えられるかを検討する。ここではリモートアクセスに関連するサイバー攻撃に限定して検討した。以下の攻撃を組合せることで HMI/EWS 端末を不正に操作し、攻撃目的が達成されることが整理される。なお、サイバーキルチェーン（Cyber Kill Chain）と呼ばれるサイバー攻撃のプロセスを理解し、防御策を講じるための概念的なフレームワークを併用して検討することもあるが、本書では割愛する。

(a) リモートアクセス端末のマルウェア感染による不正アクセス

(b) VPN ユーザーアカウント情報を利用した不正アクセス

(c) 中継サーバーの脆弱性を利用した攻撃

(d) HMI/EWS 端末の脆弱性を利用した攻撃

(e) VPN 機器の脆弱性を利用した攻撃

ステップ 1 からステップ 3 までの検討プロセスを纏めたものを下図に示す。

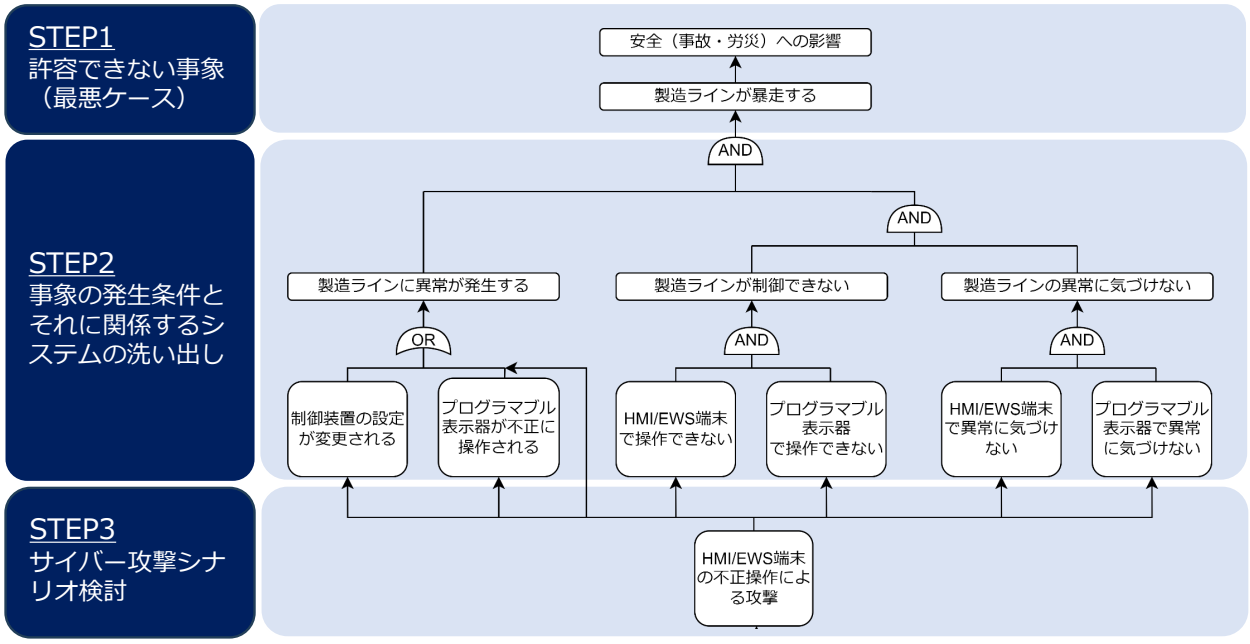


図 6-10：CCE によるリスク分析例とセキュリティ対策検討例(STEP1～STEP3)

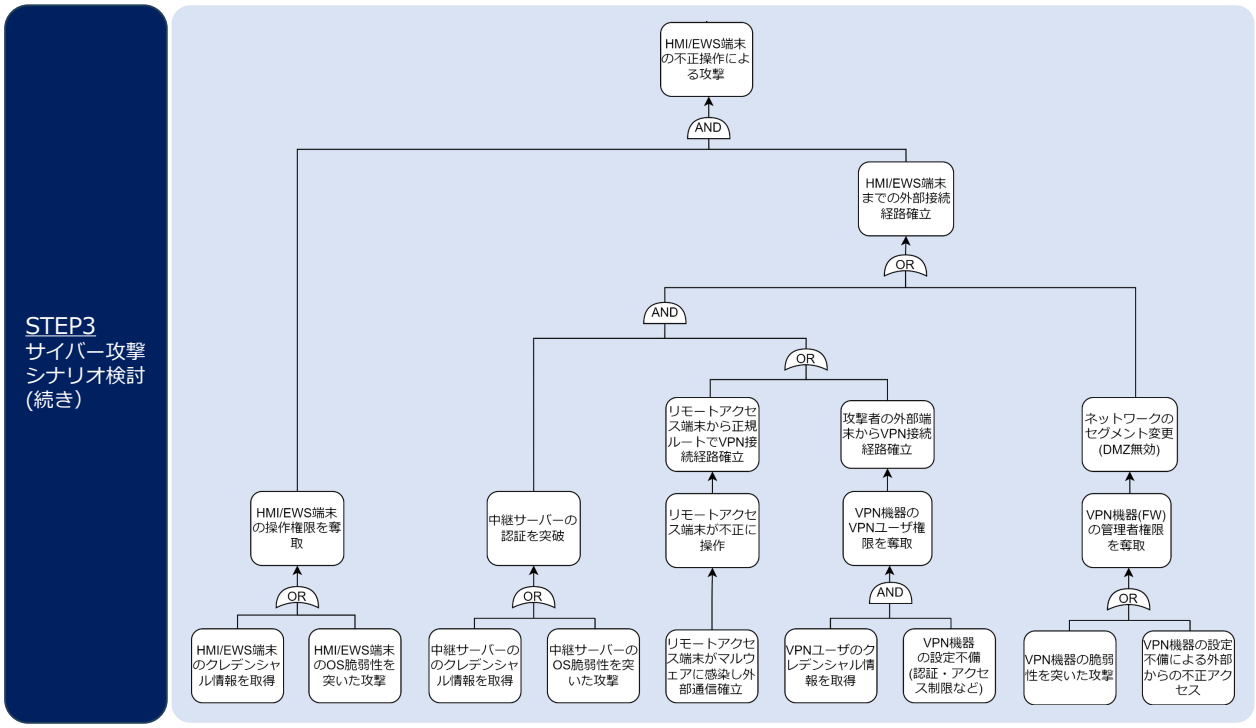


図 6-11：CCE によるリスク分析例とセキュリティ対策検討例(STEP3-続き)

(4) ステップ 4: セキュリティ対策の検討

最後にステップ 3 で特定したサイバー攻撃に対応するセキュリティ対策を検討する。今回のリスク分析結果からは防御策を大きく 4 つに分類した。ステップ 4 の検討プロセスを纏めたものを下記に示す。

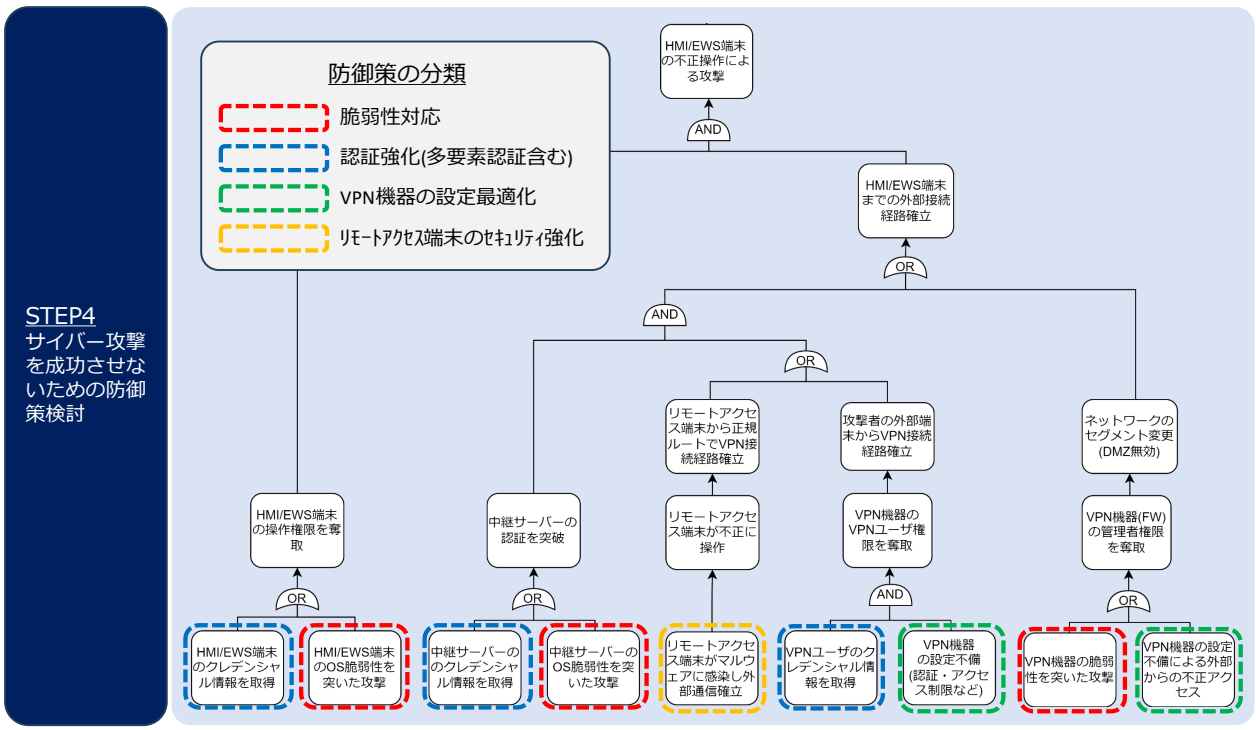


図 6-12：CCE によるリスク分析例とセキュリティ対策検討例(STEP4)

(a) 脆弱性対応

HMI/EWS 端末、中継サーバー、VPN 機器など全ての機器に対して、最新のファームウェアおよびソフトウェアのアップデートを適用する必要がある。システム構成検討のプロセスでは、脆弱性対応済みの機器を設置し、メンテナンス部門で年次点検のタイミングで対応することとしている。しかしながら、VPN 機器は脆弱性が頻発するため、年次点検のタイミングでは対応が遅れる可能性がある。追加対策として、VPN 機器（FW 機能付き）とは別にファイヤーウォールを新たに追加し、ペアードファイヤーウォール構成をとることで、VPN 機器の脆弱性により攻撃を受けた場合でも、HMI/EWS 端末までの外部接続経路を容易に確立できないようにする処置を講じる。なお、ペアードファイヤーウォール構成とする場合には、同一機種や同一メーカーであると同じ OS などの脆弱性により突破される可能性が高いため、異なるメーカーのものを採用することが望ましい。

(b) 認証強化

各機器の認証が弱いと攻撃を受ける可能性があるため、HMI/EWS 端末と中継サーバーのパスワードを強化し、ID についても初期アカウントではない特定されにくいものに変更する（デフォルトクレデンシャルの変更）。特に VPN 機器については、ID・パスワードの変更に加えて多要素認証を導入し、ログイン試行回数制限も利用することで、認証を強化する。

(c) VPN 機器の設定最適化

システム構成検討のプロセスでは、VPN 機器の FW 機能を活用して不要な通信を遮断することとしているが、設定不備により攻撃の起点となる可能性があるため、設定を最適化することとした。具体的には、権限の適正化、管理画面へのアクセス制限、IPS/IDS 機能の有効化、アラート機能のチューニング、ログサーバーの設置・連携、IP・MAC アドレスの制限、ポート制限などを設定する。

(d) リモートアクセス端末のセキュリティ強化

リモートアクセス端末が攻撃者によって不正に操作されると、正規の VPN 接続経路を通じて制御システム内部へアクセスされる恐れがあるため、セキュリティ対策を強化する。具体的には、IT 部門と連携して、アカウントの分離・管理者権限の適正化、パスワードの強化、OS 標準ファイヤーウォールの有効化、端末ログの収集と EDR ツールの導入を実施する。

以上の検討結果からセキュリティ対策を講じたシステム構成を以下に示す。

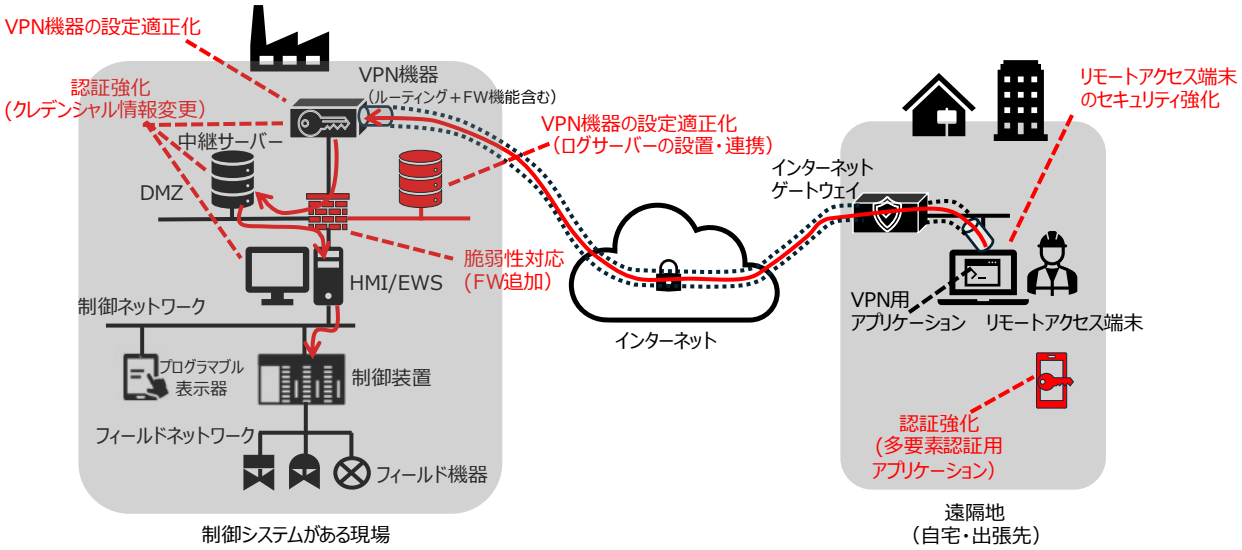


図 6-13：セキュリティ対策を講じたシステム構成の例

6.7　システム構成チェック

システム構成チェックでは、セキュリティ対策を講じたシステム構成が、要件定義で定めた各項目を漏れなく対応できているか確認する。更にリモート O&M の+(プラス)の効果と、−(マイナス)の効果を踏まえ、バランスが取れているか確認しシステム構成を決定する。結果によっては要件定義からの見直しを要する。

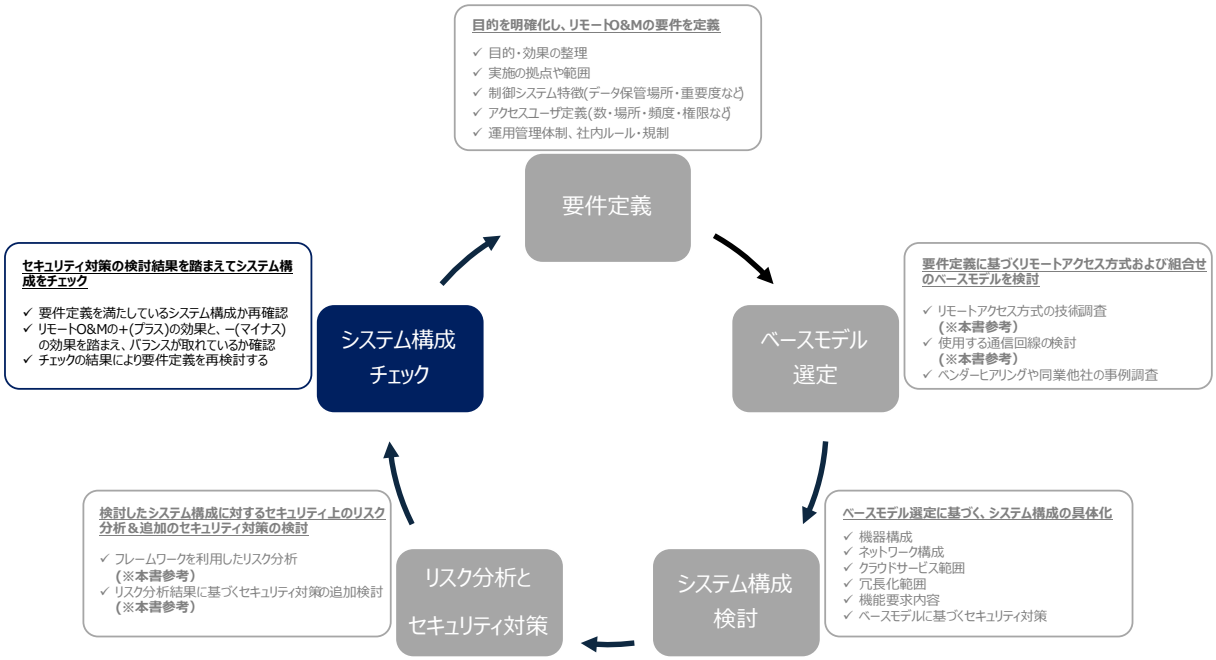


図 6-14：システム構成決定プロセス

6.7.1　システム構成チェックの検討例

セキュリティ対策後のシステム構成である「図 6-13：セキュリティ対策を講じたシステム構成の例」の構成を改めて確認し、「表 6-1：リモート O&M の実施目的・効果の整理例」および「表 6-2：要点定義の整理例」で纏めた要件が満たされているか確認する。

また今回のケースにおけるリモート O&M の+(プラス)の効果と、ー(マイナス)の効果を踏まえ、経営上もバランスが取れていると判断した場合にはシステム構成を決定する。

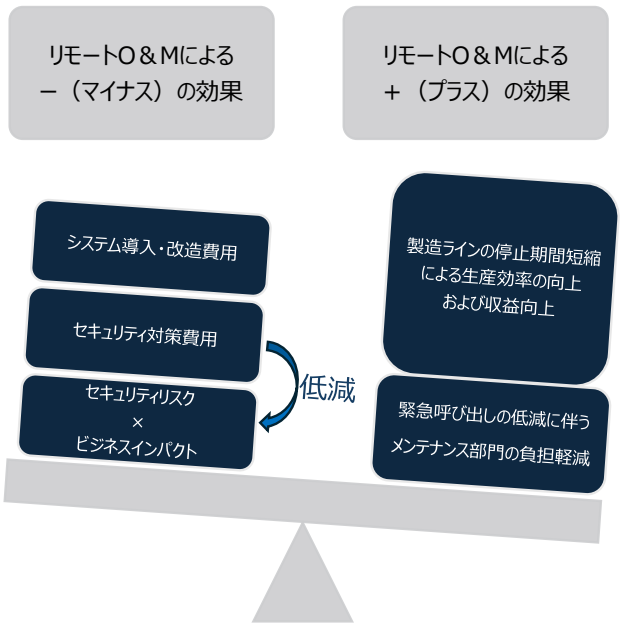


図 6-15：リモート O&M の導入によるバランス確認例

6.8　要件定義に基づくシステム構成検討プロセスの総括

本章では、リモート O&M を実現するためのシステム構成検討プロセスを段階的に説明した。各プロセスは、要件定義から始まり、ベースモデル選定、具体的なシステム構成検討、リスク分析とセキュリティ対策、そしてシステム構成チェックへと進む。

要件定義では、リモート O&M の目的、対象範囲、アクセスユーザー、システムの重要度、運用管理体制、規制・社内セキュリティポリシーなどを詳細に設定する。この要件定義に基づき、最適なリモートアクセス方式と通信回線のベースモデルを選定し、具体的なシステム構成を設計した。

次に、CCE 手法を用いたリスク分析とセキュリティ対策を実施し、システムが直面する可能性のある脅威を特定し、適切なセキュリティ対策を講じる。最後に、セキュリティ対策を踏まえてシステム構成をチェックし、リモート O&M のメリットとデメリットをバランスよく検討しながら、最終的なシステム構成を決定する。

これにより、リモート O&M を安全かつ効果的に実施するためのシステム構成が明確になり、企業の具体的な

ニーズに対応した柔軟なシステム構築が可能となる。本章で示したプロセスを参考に、自社の状況に応じた最適なリモート O&M のシステムを検討されたい。

第7章 事例検証

7.1 目的

前章までは制御システムへのリモートアクセスに関するセキュリティ対策などを、検討プロセスを含め説明してきた。しかしながら、OT システムでは IT システムに比べ、アップデートやパッチ適用などの脆弱性対応やクレデンシャル情報の管理が十分でない場合が多い。そのため、リモートアクセスに関連する機器の設定不備や脆弱性が存在するシステムにおいて、脅威シナリオがどのように顕在化するのか実際の機器を用いて検証した。また、顕在化した脅威シナリオに対して前章まで述べたセキュリティ対策を実施した場合、脅威に対する検知もしくは防御ができるのか、その有効性を確認することを目的に事例検証を実施した。

事例検証に使用する模擬プラントは、「6.5.2 システム構成の検討例」に示した制御システムを模したものとし、脆弱性を有するシステムを構築した。

セキュリティ対策の効果検証については、「第 5 章 リモートアクセスにおけるセキュリティ対策」から、いくつかを実装するものとし、セキュリティ対策前後でペネトレーションテストを実施することでその有効性を検証した。事例検証のフローを以下に示す。

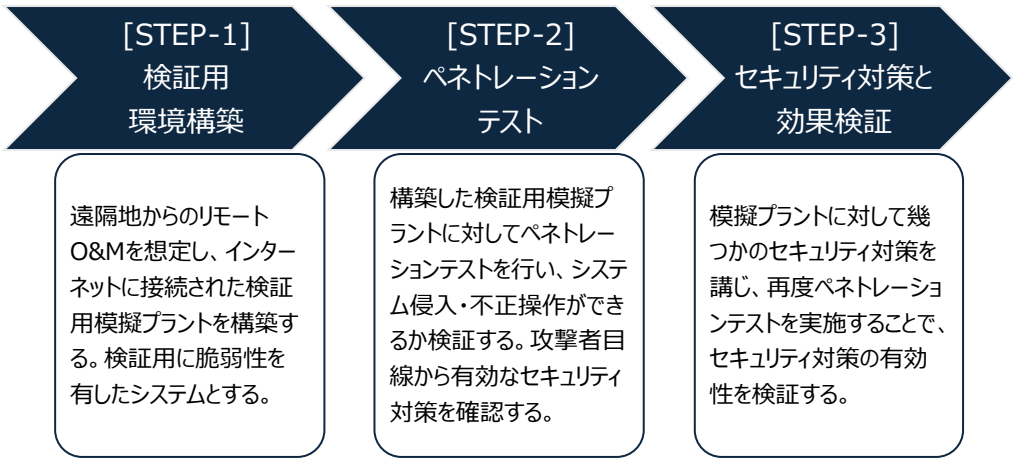


図 7-1：検証用模擬プラントを利用した事例検証フロー

7.2 [STEP-1]検証用環境構築

7.2.1 検証用模擬プラントの構成

検証用模擬プラントの機器構成を以下に示す。前述の通り、模擬プラントの構成は、「6.5.2 システム構成の検討例」に示した制御システムを遠隔地から制御するシステム構成を模したものとした。ただし、実際のインターネットに接続された検証環境整備のため、セキュリティ対策を講じていないインターネットゲートウェイを介して VPN 機器を接続した。また、検証時のログ確認のためログサーバーを予め設置している点も異なる。なお、本検証にあたっては学術用に管理されたネットワーク環境を利用しており、あくまで研究・教育の一環として実施して

いる点に留意いただきたい。

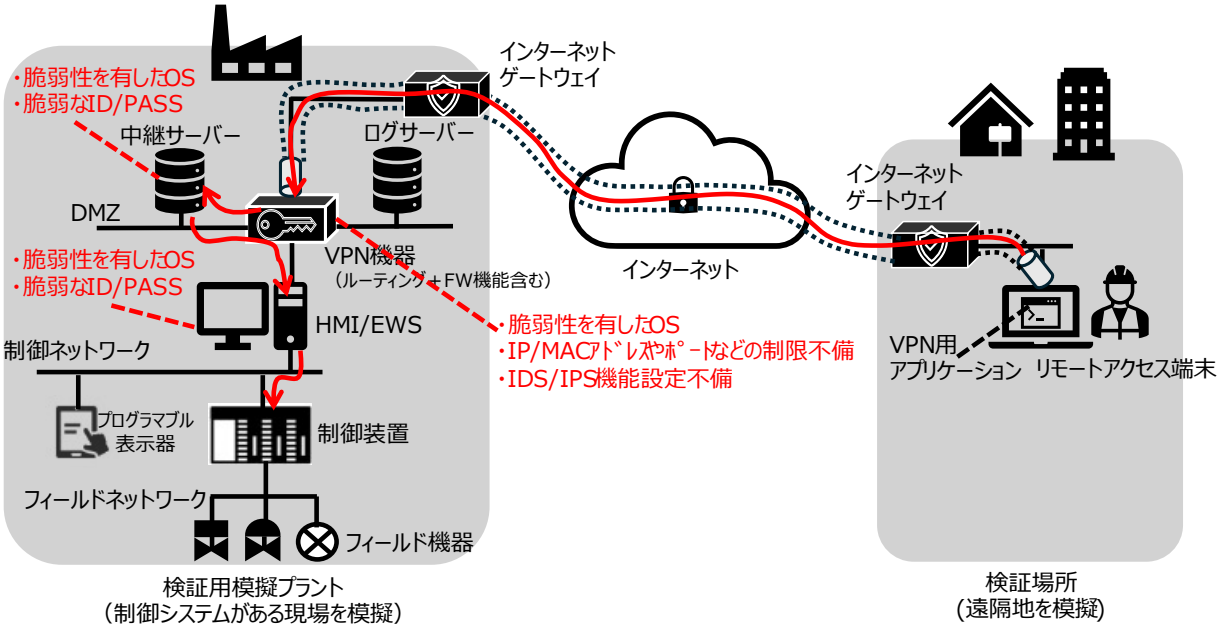


図 7-2：[STEP-1]検証用模擬プラント構成図

7.2.2　模擬プラントの前提条件および設定概要

模擬プラントの前提条件を下記に示す。その他の前提条件は「6.5.2 システム構成の検討例」に準じた。

- 複数拠点からリモートアクセスすることを想定
- VPN 機器-リモートアクセス端末間をインターネット VPN（SSL VPN）にて接続
- DMZ に中継サーバーを設置し
- 脆弱性を有した機器、脆弱なクレデンシャル情報、設定不備

また、システムを構成する機器の機能と設定概要については「表 7-1：[STEP-1]模擬プラント機器の機能と設定概要」にて示す。

表 7-1：[STEP-1]模擬プラント機器の機能と設定概要

場所	機器	機能・設定
遠隔地	インターネットゲートウェイ	・インターネット接続 ・固定 IP アドレス付与
	リモートアクセス端末	・現場 VPN 機器への認証接続 ・最新 OS の PC ・VPN 用アプリインストール
制御システムがある現場	インターネットゲートウェイ	・インターネット接続 ・固定 IP アドレス付与

	VPN 機器	・外部ユーザー端末認証接続 ・暗号化（SSL VPN） ・ルーティング機能よるネットワークセグメント構築 ・OS に脆弱性有 ・IP/MAC アドレス制限なし ・ポートによるサービス制限なし ・IPS/IDS 機能は不使用
	ログサーバー	・VPN 機器をはじめとする機器のログ収集 ・Syslog としてログ収集
	中継サーバー	・リモートアクセス端末からのアクセスを中継して HMI/EWS 端末へ RDP 接続 ・OS に脆弱性有 ・脆弱な ID/パスワード設定
	HMI/EWS 端末	・HMI：PLC の監視/操作 ・EWS：制御装置・プログラマブル表示器のプログラム及び設定変更 ・OS に脆弱性有 ・脆弱な ID/パスワード設定 ・PLC 監視操作用アプリケーション ・各種エンジニアリングアプリケーション
	プログラマブル表示器	・PLC の監視/操作 ・機器標準ソフトウェアで構成
	制御装置(PLC)	・フィールド機器の制御 ・ラダー回路で制御回路構築
	フィールド機器	・機器、状態検出 ・パトランプとトグルスイッチで構成

7.3 [STEP-2]ペネトレーションテスト

7.3.1 ペネトレーションテストの概要

STEP-1 で構築した模擬プラントに対し、インターネット越しにペネトレーションテストを実施し、最終標的のフィールド機器に到達し不正操作を行うことができるか検証した。ペネトレーションテストの概念図を以下に示す。

なお、ペネトレーションテストの実施者（以下、テスター）は IP アドレスを含むシステム構成図を予め入手済である前提でペネトレーションテストを実施した。具体的な検証内容と結果は次項「7.3.2 ペネトレーションテストの検証内容と結果」に示す。

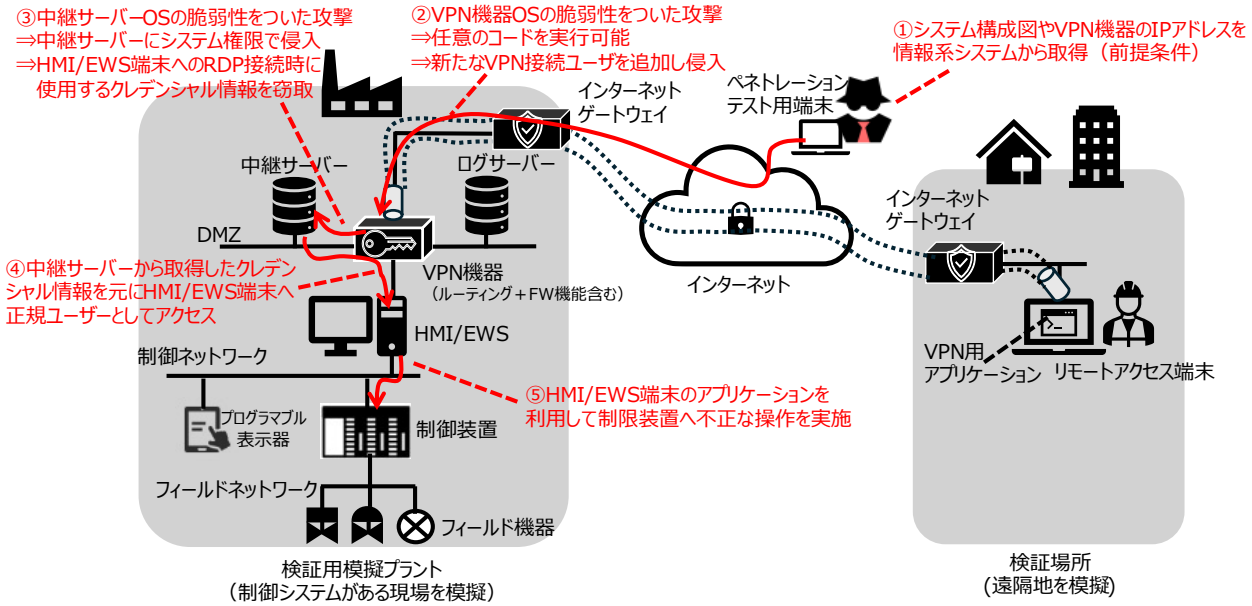


図 7-3：[STEP-2]ペネトレーションテスト概念図（1/2）

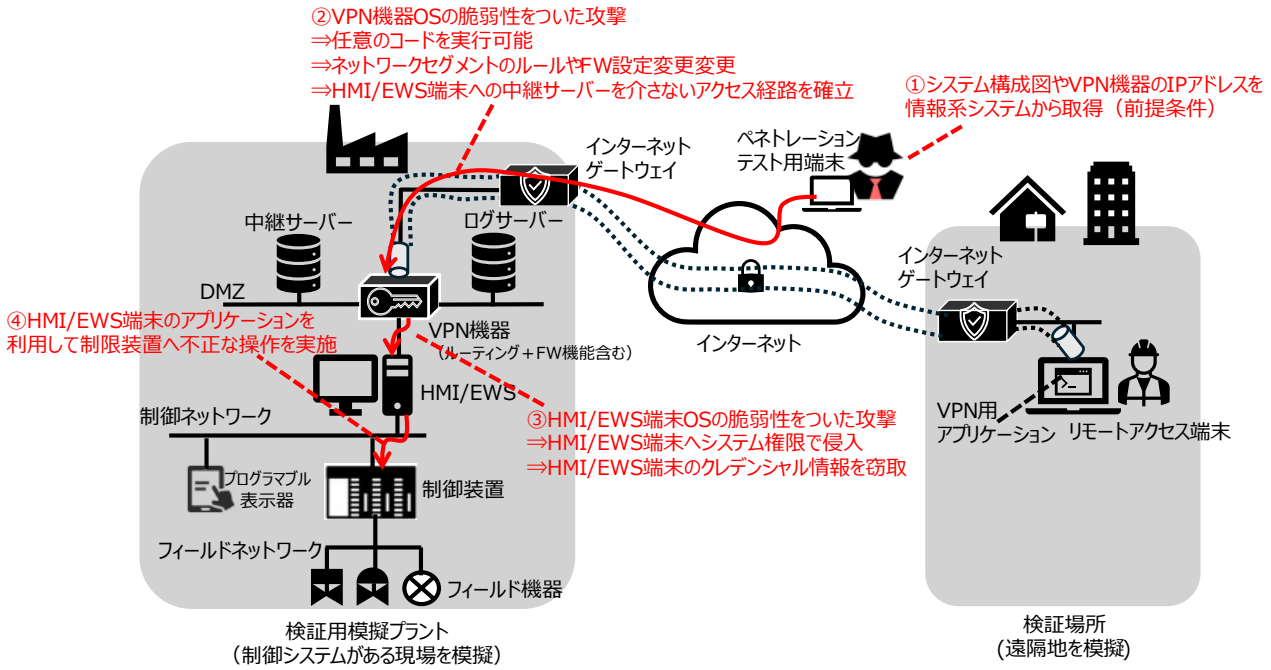


図 7-4：[STEP-2]ペネトレーションテスト概念図（2/2）

7.3.2　ペネトレーションテストの検証内容と結果

ペネトレーションテストの検証内容と結果を以下、「表 7-2：ペネトレーションテストの検証内容と結果」に示す。結果としてテスターは、VPN 機器の脆弱性を突いて管理者権限を取得し、下層までの侵入経路を確立す

ることができ、中継サーバーおよび HMI/EWS 端末 OS の脆弱性を突いて最終標的のフィールド機器まで到達し、不正操作が可能であることが確認された。

表 7-2：ペネトレーションテストの検証内容と結果

No	機器	検証内容	結果
1	VPN 機器	・OS の脆弱性を利用して、管理者権限を取得し、任意のコード実行	・脆弱性を利用し、管理者権限で VPN 機器の設定を書き換え ・新たな VPN ユーザー追加し VPN 接続の上、中継サーバー入口まで侵入に成功 ・ネットワークセグメントのルールや FW 設定も管理者権限で変更し、(中継サーバーを介さずに) HMI/EWS 端末入口まで侵入に成功
2	中継サーバー	・OS の脆弱性を利用し、ファイルレス攻撃よる侵入	・OS の脆弱性がマッチせず侵入不可
		・パスワードリスト攻撃によるパスワードの特定	・ログインパスワードを特定
		・OS の脆弱性を利用し、ファイルレス攻撃によるセッション取得	・取得したログインパスワードとファイルレス攻撃の組合せによりセッションを取得し、中継サーバーへのログイン成功
3	HMI/EWS 端末	・OS の脆弱性を利用し、ファイルレス攻撃による侵入	・OS の脆弱性を利用し侵入成功
		・クレデンシャル情報を窃取するツールによる HMI/EWS 端末ログインパスワードの特定	・ログインパスワードを特定
		・HMI/EWS 端末による制御装置(PLC)の不正操作	・取得したログインパスワードにより HMI/EWS 端末へのログイン成功 ・制御装置(PLC)の不正操作成功

7.3.3 ペネトレーションテストの考察とセキュリティ対策

- VPN 機器の脆弱性をついて侵入・管理者権限を奪取した場合、ネットワークセグメントのルールや FW 設定などを書き換えることで、最終攻撃対象まで到達可能であることが確認された。一方、VPN 機器の脆弱性を利用した攻撃でも（脆弱性の種類によるが）一定の条件を揃える必要があり、不要な機能を停止するなどの処置が有効であることが確認された。

- 脆弱なパスワードでは容易にパスワードクラックされることが確認された。また侵入後、クレデンシャル情報を窃取するツールなどの使用により、パスワードをはじめとするクレデンシャル情報が奪取されてしまうことが確認された。
- 制御システムの HMI/EWS 端末などは古いバージョンの OS 使用やアップデード未対応の場合が多く、一度同ネットワークに侵入した場合には攻撃は容易であることが確認された。
- 不要なポート閉塞や、OS ファイヤーウォール等の基本的なエンドポイントセキュリティ対策は一定程度有効であることが確認された。
- 多重的な防御・障壁により時間を要していれば、突破は困難であることが想定された。多重防御による時間稼ぎとともに、早期に検知するシステムを構築することの重要性が再確認された。

7.4 [STEP-3]セキュリティ対策と効果検証

前節「7.3 [STEP-2]ペネトレーションテスト」で防御できなかった結果に対し、模擬プラントに幾つかのセキュリティ対策を実装し、その有効性を検証した。

検証したセキュリティ対策は、以下の 5 項目となる。それぞれの内容は次項以降で述べる。

① 管理者・ユーザーのトークンによる多要素認証（防御）

② エンドポイントセキュリティ（防御・検知）

③ IPSec VPN による拠点間通信（防御）

④ クラウドシステムによる不正通信検知と防御（防御・検知）

⑤ IP-KVM による IP 通信変換（防御）

7.4.1 管理者・ユーザーのトークンによる多要素認証

VPN 機器の OS に脆弱性がある場合でも多要素認証が有効であるか、効果を検証した。具体的には、VPN 機器の管理者や VPN ユーザーアカウントに対する多要素認証のため、トークンデバイス（スマートフォン）にトークンアプリをインストールし、認証時にワンタイムパスワードによる認証を行うシステムとした。

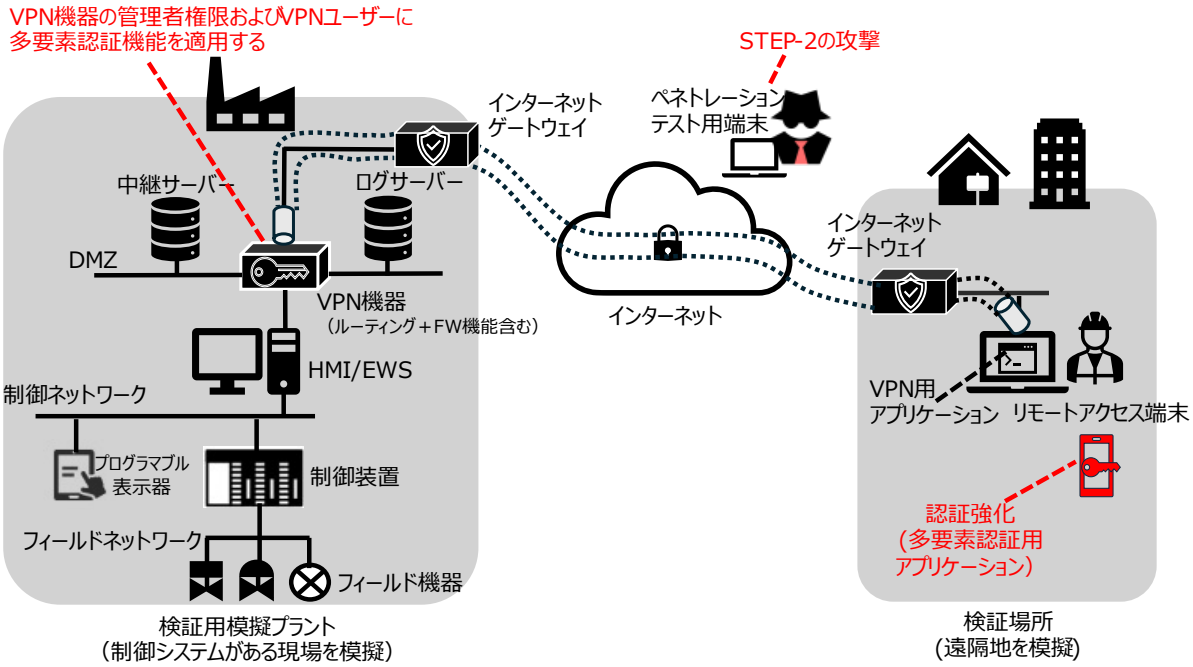


図 7-5：[STEP-3]多要素認証検証

(1) 検証結果

今回検証対象とした脆弱性の場合、トークンによる多要素認証は効果がなく、テスターは脆弱性を利用し管理者権限で VPN 機器の設定を任意のコードを実行することで、新規 VPN ユーザーの追加による VPN 接続や、FW の設定変更等に成功した。

(2) 考察

一般的には認証強化がセキュリティ対策として有効であると認識されているが、製品の脆弱性によっては根本的な対策として脆弱性対応が必要となることが確認された。通信機器・セキュリティ製品の導入時だけでなく、継続的なセキュリティ対策（脆弱性対応）の重要性が改めて浮き彫りとなったと考えられる。

7.4.2 エンドポイントセキュリティ

スタンドアロン向けの USB 型セキュリティチェックツールを中継サーバーに導入し、HMI/EWS 端末にはエンドポイントセキュリティソフトを導入することにより、前節「7.3 [STEP-2]ペネトレーションテスト」で実施した攻撃を防御できるかを検証した。

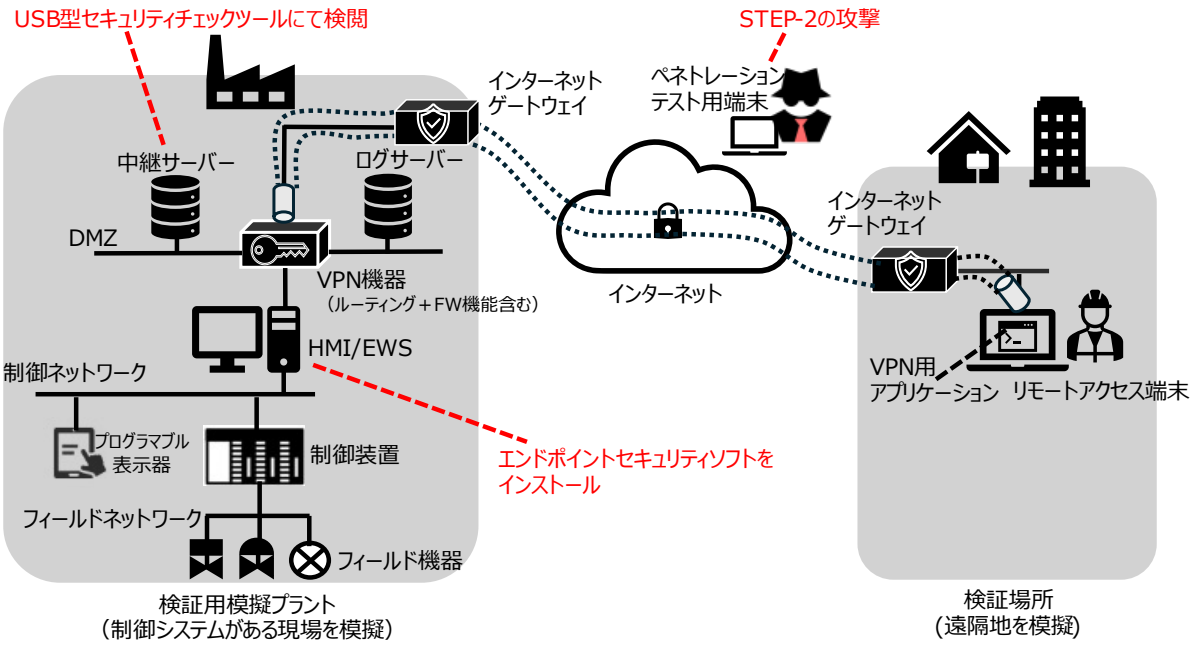


図 7-6：[STEP-3]エンドポイントセキュリティ検証

(1) 検証結果

中継サーバーに配置した USB 型セキュリティチェックツールにてパターンに一致した攻撃ツールなどが検知され、一定の効果を確認した。しかしながら攻撃ツールを暗号化した場合には検知されなかった。

また、HMI/EWS 端末にインストールしたエンドポイントセキュリティソフトは、ファイルレス攻撃に対しても一定の防御性能があることを確認した。

(2) 考察

USB 型セキュリティチェックツールは名称やファイルパターンをチェックしており、暗号化されたものは検知できない場合もある。また、USB 型ウィルスチェックはパターンファイルを常に最新のものに更新する必要がある。検査は一時的なものあり、検査対象装置に常駐して検知するものではない点にも注意する必要があると考えられる。

一般的にエンドポイントセキュリティ製品はインターネットに接続することで最新のパターンファイルに更新される。外部ネットワークへ接続できない環境の場合には、検知できない攻撃もあると想定される。

7.4.3 IPSec VPN による拠点間通信

VPN 機器の OS に脆弱性がある場合でも、必要最小限の設定とすることにより、外部からの攻撃に耐性があるか、検証した。

具体的には外部リモートアクセス端末側にも VPN 機器を設置し、対向する VPN 機器と IPSec VPN で 1:1 の拠点間通信の構成とし、かつ「拠点間以外の通信を遮断」、「管理画面へのポート閉塞」、「インターネッ

トからの IP アドレスの隠蔽」などの追加設定により、必要最低限の通信に制限することとした。

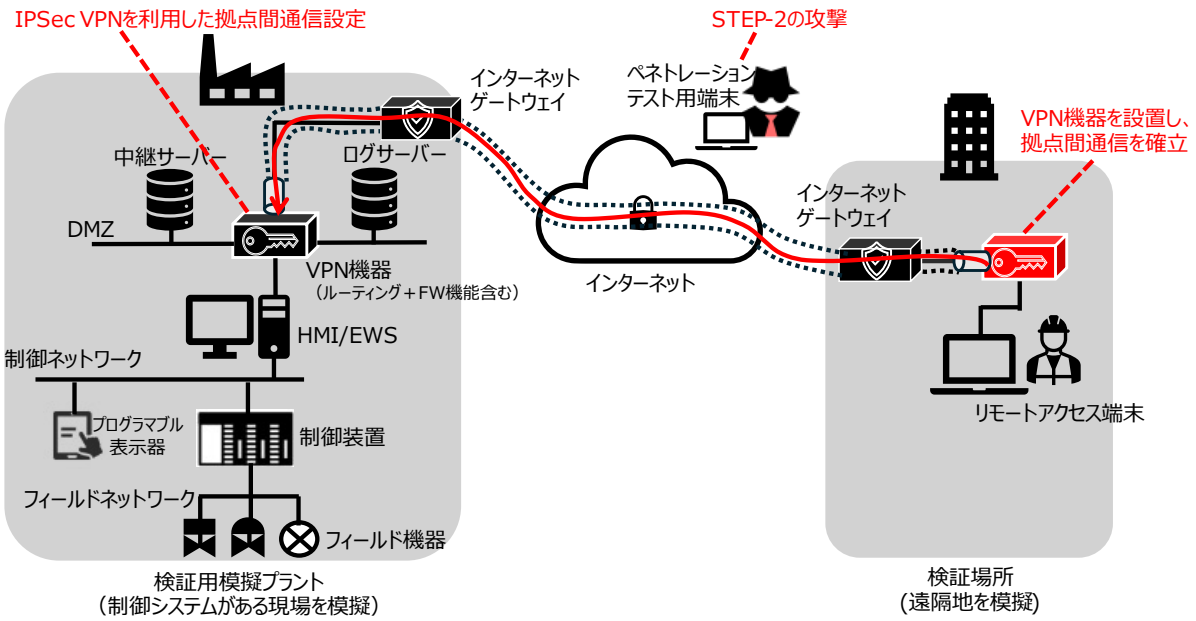


図 7-7：[STEP-3]拠点間通信検証

(1) 検証結果

外部インターネットから VPN 機器の脆弱性に対する攻撃を防ぎ、また外部インターネットからも IP アドレスを秘匿できたことを確認した。攻撃者によるインターネットからのホスト発見を困難にし、ターゲットとなるリスクを低減した。

(2) 考察

複数箇所からのアクセスを受ける場合、VPN 機器はポートを開けて待っている必要がある。すなわち、SSL VPN ではインターネットに対してポート(模擬プラントの設定では 4433/TCP)を開けて待ち受けてるため、インターネットから開きポートを秘匿にできないと考えられる。

対して拠点間通信の場合は、IPSec VPN 拠点間でポートを開けて待つ必要がないため、外部インターネットからは開きポートが秘匿され、必要最低限の通信に制限することの有効性が確認された。

7.4.4 クラウド型 VPN サービスによる不正通信検知と防御

クラウド型 VPN サービスを経由して攻撃された場合に検知・防御できるか、検証した。

リモートアクセス端末と OT システムに接続された VPN 機器は、それぞれクラウドサービスと IPSec VPN にて接続し、クラウドサービス内のルーティングで通信およびアクセス制御、監視とロギングを行う。

テスターは正規なリモートアクセス端末を乗っ取ったが、接続先である中継サーバーや HMI/EWS 端末のクレデンシャル情報は取得できていない前提で、クラウド型 VPN サービス経由で OT システムにアクセスの上、中継

サーバーや HMI/EWS 端末に対しファイルレス攻撃やポートスキャンを行い、検証した。

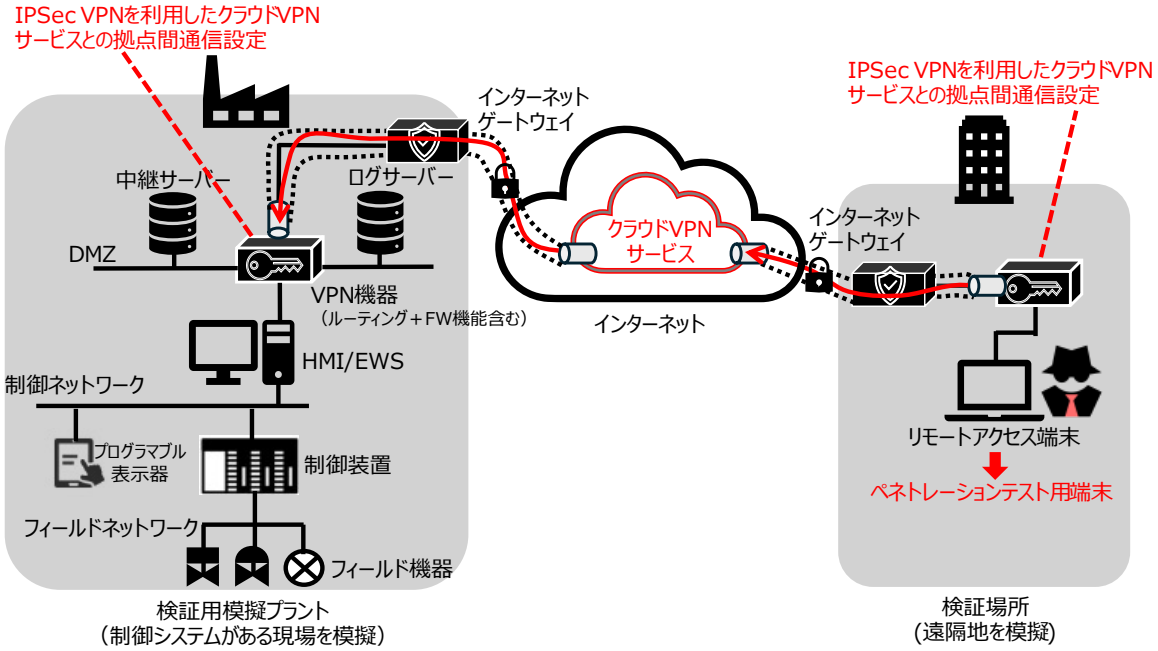


図 7-8：[STEP-3]クラウド型 VPN サービス検証

(1) 検証結果

リモートアクセス端末からの中継サーバーおよび HMI/EWS 端末への攻撃を防ぎ、かつ検知とロギングを行っていることを確認した。ただしデフォルト設定ではポートスキャンは検知のみだった。

(2) 考察

今回検証したクライアント型 VPN サービスの場合、VPN 機器とクラウドサービス間の IPSec VPN を常時接続でき、複数地点からのアクセスはクラウドサービス側で管理・検閲できるので、複数の拠点や複数の制御システムへのリモートアクセス管理に有効であると考えられる。

なお、サービスにもよるがユーザー側で設定する(できる)機能は多岐にわたっており、クラウドサービスとの接続設定やチューニングには一定の知識が必要であると考えられる。

7.4.5 IP-KVM による IP 通信のメディア変換

中継サーバーと HMI/EWS 端末間を IP-KVM を介して IP 通信をメディア変換することで、中継サーバーが攻撃された場合でも最終ターゲットである HMI/EWS 端末を防御できるか、検証した。

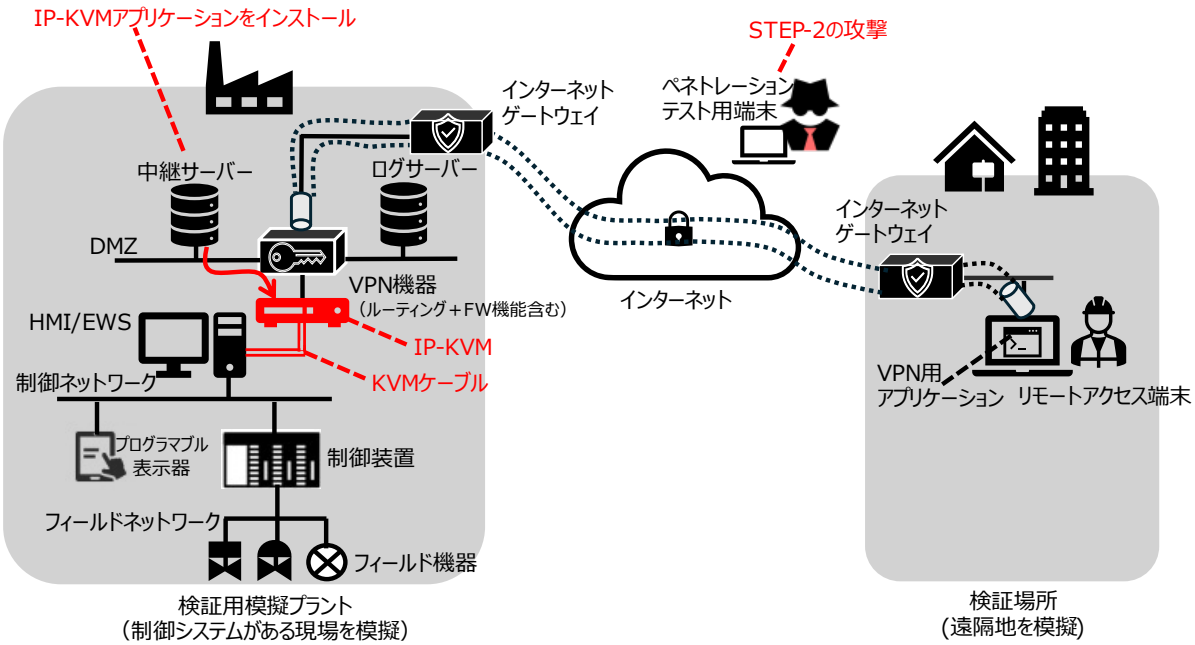


図 7-9：[STEP-3]IP-KVM 検証

(1) 検証結果

中継サーバーと HMI/EWS 端末間をネットワーク上分離することで、リモートアクセス端末からの HMI/EWS 端末への攻撃を防ぐことができた。

ただし、今回検証に使用した IP-KVM 装置の場合、IP-KVM に対する DoS 攻撃により、HMI/EWS 端末への遠隔操作が不能になった。

(2) 考察

IP-KVM には暗号化や認証機能が備わっていることが多く、不正なアクセスからの保護が期待できる。ただし、今回検証したように IP-KVM 自体が攻撃対象となる可能性があり、前段の VPN 機器の適切なセキュリティ設定やソフトウェアのアップデートが必要であると考えられる。

また IP-KVM を導入する場合、IP-KVM のセキュリティ機能や、サイバー攻撃を受けた場合の挙動等を調査し、目的に合ったものを選定することが重要である。

7.5　事例検証の総括

本章の事例検証において、模擬プラントを用いたペネトレーションテストと各種セキュリティ対策の効果検証を実施した。以下に総括を記載する。

(1) 脆弱性の管理と対処

多要素認証を導入しても機器の脆弱性をつかれ突破される可能性があることが確認された。攻撃者は既知の脆弱性を狙うことが多いため、これを放置することは大きなリスクとなる。事業への影響や対処の遅れを考慮し、既知の脆弱性に対する適切な対応が必要である。

(2) VPN 技術の選択と評価

模擬プラントにはインターネット VPN として SSL VPN と IPSec VPN を適用した。一般に IPSec VPN は設定が複雑だが強固なセキュリティを提供し、拠点間通信などに適している。一方、SSL VPN は簡便な設定と広範な互換性を持ち、迅速な導入が求められる環境や Web ベースのアプリケーションアクセスに向いている。VPN 技術の選択は、具体的な使用ケースやセキュリティニーズに依存するため、技術を適切に評価し、環境に合ったものを選ぶことが重要である。

(3) クラウド型 VPN サービスの利点と課題

クラウド型 VPN サービスを使用したリモートアクセスは、多数の拠点に対する管理負担が軽減され、効率的なセキュリティ管理が可能となる。ただし、導入には初期コストや運用コストが掛かるため、組織のニーズにより最適なサービス形態を選択することが重要である。

(4) エンドポイントセキュリティの限界と多層防御

エンドポイントセキュリティは重要な防御手段であるが、全ての攻撃因子を完全に検出できるわけではない。例えば未知の脆弱性への対応や、ファイルレスマルウェアの検出、暗号化された通信等は検知が難しいケースも多く、多層防御や脆弱性管理などの他のセキュリティ対策との組み合わせが必要である。

(5) IP-KVM の効果と運用上の注意点

IP-KVM は攻撃対象機器をネットワークから直接アクセスできなくするため、セキュリティ対策上有効な手段と考えるが、IP-KVM 自体への攻撃の可能への考慮、脆弱性管理や認証情報管理等の運用面なども考慮する必要がある。

本章ではごく一部のセキュリティ対策について検証結果を述べてきたが、一つの対策だけで制御システムを完全に守ることはできない。セキュリティは多層防御を基本とすることで、システム全体の防御力を高めることができる。一つの対策に頼るのではなく、複数の対策を組み合わせることで、より強固なセキュリティを実現することが重要である。

第8章 まとめ

制御システムへのリモートアクセスを安全に実施するためのセキュリティ対策などを紹介してきた。リモートオペレーションやリモートメンテナンスのニーズが高まる中、リモート O&M（Remote Operation & Maintenance）のセキュリティ対策は、事業の継続性と安全性に直結する重要な要素となる。

第 2 章では、企業アンケートの結果から、多くの企業がリモート O&M のニーズを持ちながらも、セキュリティ対策の不足や管理体制の未整備に課題があることが浮き彫りになった。特に、IT 技術やセキュリティ知識に乏しい可能性がある制御システム部門が管理しており、社内ルールの未整備がセキュリティリスクを高める要因となっている。

第 3 章では、リモートアクセス方式として、プライベートネットワーク方式、リモートデスクトップ方式、仮想デスクトップ方式（VDI）の 3 つの代表的な方式を紹介した。各方式の特性やセキュリティ上の考慮点を理解し、適切な方式を選択することが重要である。リモートアクセス方式の選択には、利用目的やアクセス場所、通信回線の選択など多岐にわたる要素が関与するため、全体のバランスを見ながら適切な方式を検討する必要がある。

第 4 章では、リスク分析の重要性とその手法を紹介した。CCE や NIST CSF など、国際的に認知されたリスク分析手法やリスク管理のフレームワークを活用し、システム全体の脆弱性を評価し、最適な対策を講じるプロセスを示した。これにより、潜在的なリスクを早期に発見し、効果的なセキュリティ対策を実施できる。

第 5 章では、リモート接続におけるセキュリティ対策について、識別、防御、検知、対応の 4 つの機能に分類し、具体的な対策事例を示した。資産管理や脆弱性対応、認証の強化、通信の暗号化、DMZ の設置、ファイヤーウォールの設定など、多岐にわたる対策を組み合わせることで、リモートアクセス時のセキュリティを強化することができる。なお、包括的なセキュリティ対策には、物理的なセキュリティ対策や従業員教育なども考慮する必要があることを強調しておく。

第 6 章では、要件定義に基づくシステム構成検討プロセスを明示した。リモート O&M の目的や効果を具体的に整理し、必要なシステム構成やセキュリティ対策を段階的に検討する手順を示した。このプロセスにより、企業は自社のニーズに最適なリモートアクセスシステムを設計・導入し、リスクを管理しながら効率的な運用を実現できると考えている。

第 7 章では、模擬プラントを用いたペネトレーションテストやセキュリティ対策の効果検証を実施し、その結果を報告した。具体的な事例を通じて、実際の運用環境でのセキュリティ対策の有効性を確認し、実装に向けた具体的な手法を提供することで、本書の内容がより実践的な参考資料となることを目指した。

最後となるが、リモートアクセスの導入と運用に際しては、技術的な対策だけでなく、管理体制や運用ルールの整備も欠かせない。これにより、制御システムの安全性を確保しつつ、業務の効率化を図ることが可能となる。本書が、安全なリモート O&M の導入・運用における一助となることを期待する。

謝辞

本書の作成にあたり、多くの企業の皆様にはアンケートへのご協力、制御システム向けのリモートアクセスソリューションに関する貴重な情報提供などをいただきましたことに心より御礼申し上げます。

また、産業サイバーセキュリティセンター中核人材育成プログラムの講師である小林和真先生、登大遊先生、松崎和賢先生、目黒有輝先生、前田一平先生、石原真太郎先生、横澤祐貴先生には、プロジェクト活動においてご指導・ご助言をいただくとともに、各検証機材のご支援を賜りましたことに改めて御礼申し上げます。

そして、本書の作成およびプロジェクトの実施において多大なる貢献をいただいた下記のプロジェクトメンバーの皆様にも深く感謝いたします。

プロジェクトメンバー

本書は、独立行政法人情報処理推進機構 産業サイバーセキュリティセンター中核人材育成プログラムにおける第 7 期受講生 卒業プロジェクト「安全第一！ リモート O＆M＋セキュリティ」の成果物として作成されました。

◎大野 孝侑

〇林　延行

益尾 文里

石村 祐太

辰巳 大祐

（◎リーダー,〇サブリーダー）

付録A リモートアクセスの基本技術

A.1　本付録の目的

本付録ではリモート O&M 時に利用される基本的な情報通信技術の概要を記載する。情報通信技術は多岐にわたっており本書で全てを網羅するものではないが、基本的な技術や概念について理解することで、適切なリモートアクセス環境を構築するための基礎知識を提供することを目的とする。

A.2　ネットワークの基本概念

A.2.1　ネットワークとは何か

ネットワークとは、コンピューターやその他のデバイスを互いに接続して情報をやり取りするシステムのことを指す。例えるなら、ネットワークは情報が流れる道筋のようなものである。コンピューター同士が通信回線やケーブルで接続されることで、情報の共有やメッセージのやり取りが可能となる。このシステムは「コンピューター」「ネットワーク機器」「伝送媒体」の 3 つの要素で構成されている。

コンピューターには、パソコンやサーバーなどが含まれ、これらはアプリケーションを提供したり利用したりする役割を果たす。ネットワーク機器には、ネットワークスイッチやルーターがあり、これらはデータを転送するための装置である。伝送媒体は、コンピューターとネットワーク機器を接続するためのもので、ケーブルや無線電波が使われる。

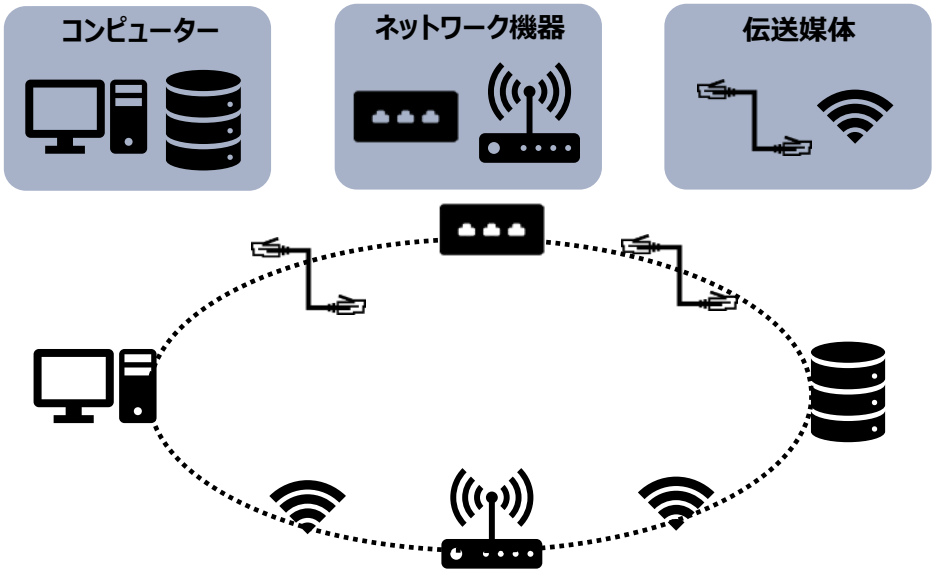


図 A-1：ネットワークの構成要素

出典：https://japan.zdnet.com/article/35137192/ をもとに作成

A.2.2　ネットワークの種類

ネットワークにはさまざまな種類があり、その規模や用途によって分類される。大きく分けると、「LAN」「WAN」「インターネット」の 3 つに分かれる。

(1) LAN（Local Area Network）

LAN は家庭や企業のオフィス、ビル内など、比較的狭い範囲のネットワークを指す。例えば、家の中で複数のコンピューターを接続したり、企業内のパソコンをネットワークでつないだりする際に使われる。LAN を使うことで、ファイルやプリンターなどのリソースを共有することができる。

(2) WAN（Wide Area Network）

WAN は、離れた場所にある複数の LAN を接続したネットワークである。例えば、企業の本社と支社をつなぐときに使われる。通信事業者が提供する回線を利用して、物理的に離れた場所でもネットワークを構築できる。

(3) インターネット

インターネットは、世界中のネットワークが相互に接続された巨大なネットワークである。インターネットサービスプロバイダ（ISP:Internet Service Provider）が提供する接続サービスを通じて、私たちはインターネットにアクセスし、世界中の情報に触れることができる。インターネットは広義の WAN の一種と言える。

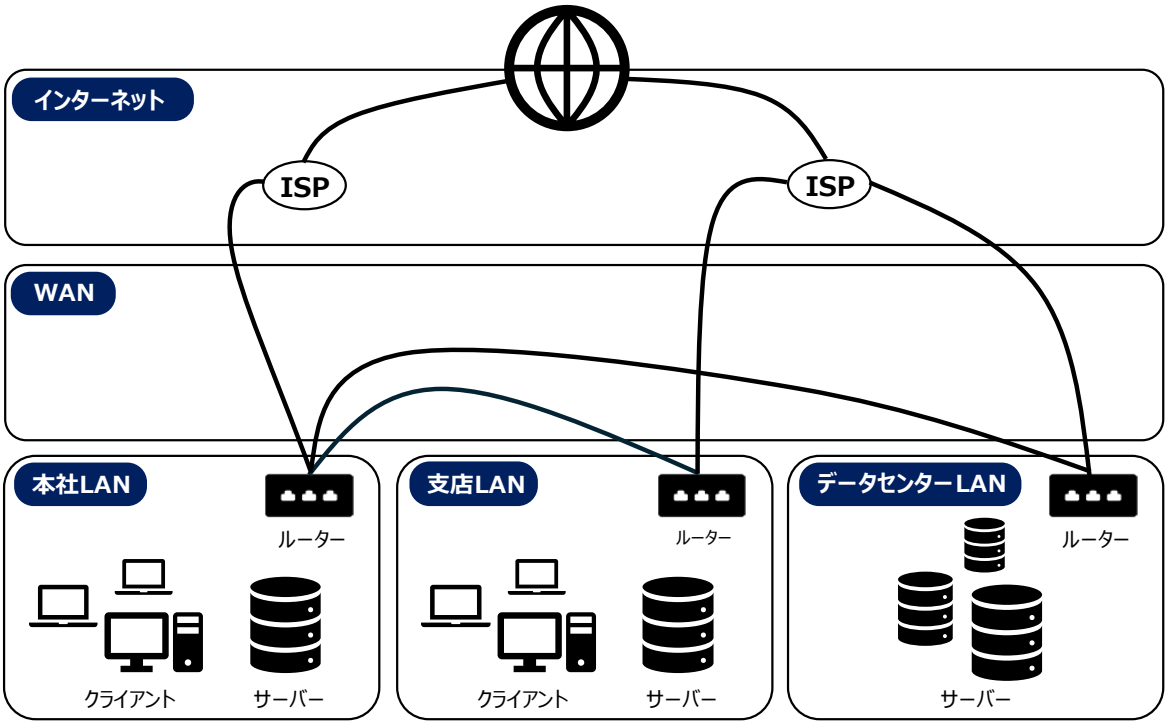


図 A-2：ネットワークの種類

出典：https://japan.zdnet.com/article/35137192/ をもとに作成

A.2.3　パブリックネットワークとプライベートネットワーク

ネットワークの区分として「LAN」「WAN」「インターネット」について説明したが、ネットワークには「パブリックネットワーク」と「プライベートネットワーク」という大きな区別もある。

(1) パブリックネットワーク

パブリックネットワークとは、多くの人々が自由に使うことができるネットワークのことを指す。例えば、インターネットはパブリックネットワークの一つであり、誰でもアクセスして情報をやり取りすることができる。インターネットの歴史を振り返ると、その起源は 1960 年代にまで遡る。アメリカ国防総省が開発した ARPANET（Advanced Research Projects Agency NETwork）というネットワークがその始まりであり、初めは大学や研究機関同士が情報を共有するためのものであった。

インターネットは、その後、商業利用が解禁され、一般の人々が利用できるようになったことで急速に普及した。パブリックネットワークとしてのインターネットは、情報を自由に交換し、世界中の人々とつながることを目的として設計されている。このため、多くの人々が情報を発信したり、受け取ったりするため、情報の共有が非常に活発に行われる。しかし、パブリックネットワークにはセキュリティ面での懸念も存在する。誰でもアクセスできるため、悪意を持った人々が不正に情報を取得したり、攻撃を仕掛けたりするリスクある。

(2) プライベートネットワーク

プライベートネットワークとは、特定の人々だけが利用できるネットワークである。例えば、ある会社の中だけで使われるネットワーク（WAN や LAN）がこれにあたる。このネットワークは外部からのアクセスが制限されており、会社の中だけで安全に情報をやり取りすることができる。プライベートネットワークを使うことで、会社の重要な情報が外部に漏れる心配が少なくなる。プライベートネットワークでは、情報のやり取りがより安全に行われ、外部からの不正なアクセスから保護される。

プライベートネットワークの一つのサービス形態として「閉域網」がある。閉域網は、通信事業者が提供する特定の利用者だけがアクセスできる専用のネットワークサービスである。これにより、利用者はパブリックネットワークであるインターネットを経由せずに、安全で信頼性の高い通信が可能となる。例えば、企業が全国に支店を持っている場合、各支店間の通信を閉域網で通じて行うことで、外部の影響を受けずに安全なデータのやり取りができる。

しかし、閉域網も完璧ではない。通信事業者の操作ミスや設定の誤り、あるいはネットワークへの侵入などの脅威が存在する。実際に日本国内でもインシデント事例が報告されており、通信事業者の閉域ネットワーク内で、ひとたびウイルス感染などが広がるとその影響が他の利用者にも及ぶ可能性がある。このため、閉域網を利用する場合でも、油断せずに適切なセキュリティ対策を実施する必要がある。

また、通信事業者との契約には損害賠償の上限額が規定されている場合が多く、通常は 1 ヶ月間に

支払った利用料金と相殺されることが一般的である。通信事業者の過失による大規模被害が生じた際にユーザーの経営に与えるリスクを十分に分析することが重要である。さらに、重過失であれば全額保障される可能性もあるが、重過失の立証責任はユーザー側にあり、実際に立証できるかどうかも重要な検討事項となる。

なお、閉域網の概要については「A.4.2 閉域網」で紹介する。

A.3 OSI 参照モデルと TCP/IP

次節「A.4 リモートアクセスに利用される通信回線」ではリモート O&M に使用される通信回線について説明するが、その前に、プロトコルや OSI (Open Systems Interconnection) 参照モデル、TCP/IP (Transmission Control Protocol/Internet Protocol) について簡単に紹介する。ここでは、通信が多くのプロトコルによって成り立っていることを理解してもらうため、各プロトコルの詳細な説明は割愛する。プロトコルや OSI 参照モデルについて詳しく知りたい場合は、引用・参考文献[12]を参照されたい。

A.3.1 通信プロトコルとは

通信プロトコルとは、コンピューター同士がデータをやり取りするためのルールや手順のことを指す。これは、手紙を送るときに似ている。手紙を書く際には、何語で書くか、誰に送るか、どうやって届けるかを決める必要がある。同じように、コンピューター同士がデータを交換するときにも、データの形式や送受信の手順、エラーが発生したときの処理方法などが決まっている。これらのルールが通信プロトコルである。このプロトコルがあることで、コンピューター同士が正確にデータをやり取りすることができる。例えば、インターネットで使われる HTTP やメールで使われる SMTP などが代表的な通信プロトコルである。通信プロトコルがなければ、コンピューター同士の通信は成立しない。

A.3.2 OSI 参照モデル・TCP/IP とは

OSI 参照モデルと TCP/IP は、コンピューターネットワークにおける重要な概念である。OSI 参照モデルは、通信に必要な機能を 7 つの階層に分けることで、複雑なネットワークプロトコルを理解しやすくするためのモデルである。一方、TCP/IP は、インターネットで標準的に使用されているプロトコルで、現在のインターネットの基盤を形成している。TCP/IP は、ARPANET プロジェクトから誕生し、その後に OSI 参照モデルが国際標準化機構（ISO : International Organization for Standardization）によって作成された。作成された時期が異なるため、OSI 参照モデルと TCP/IP の階層構造は完全には一致していない。しかし、TCP/IP の方が広く普及したため、現在では OSI 参照モデルはネットワークを説明するための概念として利用されている。

OSI参照モデル		TCP/IP参照モデル		
階層	階層名	階層	階層名	代表的なプロトコル
第7層	アプリケーション層	第4層	アプリケーション層	HTTP, SMTP, POP3 FTP, SSH
第6層	プレゼンテーション層			
第5層	セッション層			
第4層	トランスポート層			
第3層	ネットワーク層	第3層	トランスポート層	TCP, UDP
第2層	データリンク層	第2層	インターネット層	IP, ICMP
第1層	物理層	第1層	ネットワークインターフェース層	Ethernet, PPP

図 A-3：OSI 参照モデルと TCP/IP 階層モデル

出典：https://ryonotes.com/difference-between-osi-and-tcpip/ をもとに作成

A.3.3 OSI 参照モデルの各階層の役割

OSI 参照モデルは、通信に必要な機能を 7 つの階層に分け、それぞれの階層ごとに独立した役割を持たせることで、ネットワークプロトコルの複雑さを軽減する役割を果たしている。このモデルは、プロトコルや通信方法を考える際のガイドラインのような役割を担っている。例えば、OSI 参照モデルでは、各階層が独立しているため、ある階層のプロトコルに変更があっても、他の階層には影響を及ぼさない。このような構造により、システムの拡張性や柔軟性が向上する。ここでは、それぞれの階層の役割について簡単に説明する。

(1) 第 1 層：物理層

物理層は、データを物理的な信号として伝送する役割を担っている。この層では、ケーブルや無線といった伝送媒体を使って、ビット（0 と 1）を電気信号や光信号、無線信号に変換して送受信する。物理層は、ハードウェアの仕様や信号の特性、コネクタの形状など、物理的な側面を扱う。

(2) 第 2 層：データリンク層

データリンク層は、同じネットワーク内の隣接する機器間でデータを正確に転送する役割を持つ。この層では、データをフレームという単位にまとめ、エラーチェックやフロー制御を行う。データリンク層は、物理層で発生する可能性のある誤りを検出し、修正する機能も備えている。イーサネットや Wi-Fi がこの層の代表的なプロトコルである。

(3) 第 3 層：ネットワーク層

ネットワーク層は、データを送信元から目的地までルーティングする役割を担う。この層では、IP アドレス

を使ってデータの経路を決定し、パケットと呼ばれる単位でデータを転送する。ルーターなどのネットワーク機器がこの層で動作し、異なるネットワーク間をつなぐ役割を果たす。インターネットプロトコル（IP）がこの層の代表的なプロトコルである。

(4) 第 4 層：トランスポート層

トランスポート層は、データの送受信を管理し、信頼性の高い通信を提供する役割を持つ。この層では、データをセグメントという単位に分割し、通信の開始から終了までを管理する。トランスポート層は、データの誤り検出や再送要求を行い、正確なデータ伝送を保証する。代表的なプロトコルには、信頼性の高い TCP（Transmission Control Protocol）と、軽量で高速な UDP（User Datagram Protocol）がある。

(5) 第 5 層：セッション層

セッション層は、通信セッションの確立、管理、終了を行う役割を担う。この層では、通信の開始と終了を管理し、データ交換の対話を同期する。セッション層は、ネットワーク上での会話を追跡し、データの送受信を整理する。これにより、複数の通信が同時に行われても干渉しないようにする。

(6) 第 6 層：プレゼンテーション層

プレゼンテーション層は、データの形式を変換する役割を持つ。この層では、データの暗号化や復号、圧縮や解凍などが行われる。プレゼンテーション層は、アプリケーションが理解できる形式にデータを変換し、異なるシステム間でデータが正しく解釈されるようにする。例えば、文字コードの変換や画像データの圧縮などが含まれる。

(7) 第 7 層：アプリケーション層

アプリケーション層は、利用者が直接利用するアプリケーションに対してサービスを提供する役割を持つ。この層では、メール送受信やファイル転送、ウェブブラウジングなど、具体的なアプリケーションの機能が実現される。HTTP（Hypertext Transfer Protocol）や SMTP（Simple Mail Transfer Protocol）、FTP（File Transfer Protocol）などがこの層の代表的なプロトコルである。

A.4　リモートアクセスに利用される通信回線

リモートアクセスは、遠隔地からでもネットワークやシステムにアクセスできるようにするための技術である。リモート O&M もリモートアクセスの一つの利用形態と言える。その実現には、特定の組織や個人だけが利用できるプライベートネットワークであり、かつ信頼性が高い通信回線が必要不可欠である。

その通信回線は一部の事業者が使用する特殊な自営回線（電力線搬送通信、マイクロ波無線、電力用光通信など）を除き、OT と IT で本質的な違いはなく、通信事業者が提供することが一般的である。プライベートネットワークは物理的に分離されたものと論理的に分離されたものに大別され、また通信事業者が接続口までサービスする場合と、利用事業者側で機器設置・設定などをするものがある。下図は紹介するプライベートネットワークをその 2 軸で整理したものである。

本節では、リモートアクセスに利用される代表的なプライベートネットワークの通信回線について紹介する。

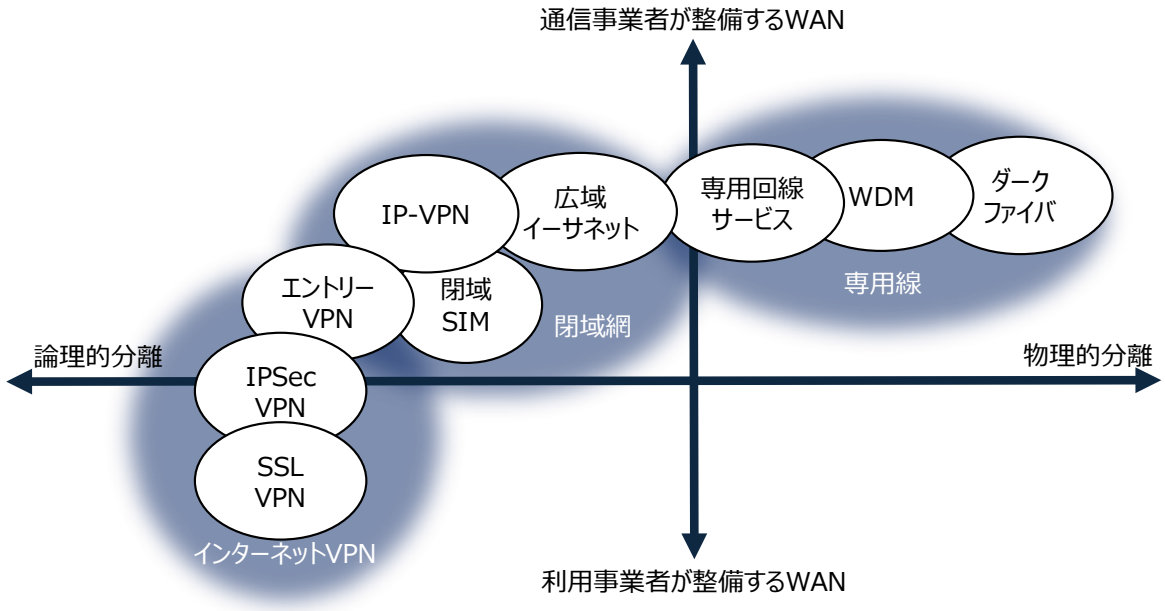


図 A-4：本書で紹介する代表的なプライベートネットワークの関係図

A.4.1　専用線

専用線とは拠点間を独立した専用の物理的な通信経路で結ぶものである。サービス提供者により専用線を閉域網の一つとして定義する場合やまたその逆もあるが、本書では区別して記載する。専用線は OSI 参照モデルの下層を利用したものであり、他の利用者と共有しないため、非常に安定した通信品質を提供し、高度なセキュリティが必要な環境に適している。ここではダークファイバーや WDM についても専用線の 1 つとして取り上げる。

(1) 専用線サービス

専用線サービスは、特定の利用者のみが利用できる高信頼性の通信回線である。他の利用者と回線を共有しないため、通信速度や品質が非常に安定しており、高度なセキュリティが求められる環境で利用されることが多い。重要拠点間を直接接続するため、企業の本社と支社間のデータ通信や金融機関での取引情報のやり取りなど、重要な業務に一般的に使用される。専用線サービスの利用にはコストがかかるが、その信頼性とセキュリティは高いとされている。

専用線サービスは OSI 参照モデルの第 1 層：物理層に該当し、主にイーサネット技術を使用して第 2 層：データリンク層でサービスが提供される。なお、次に紹介するダークファイバーとの違いは終端装置までを通信事業者が提供する点があげられる。

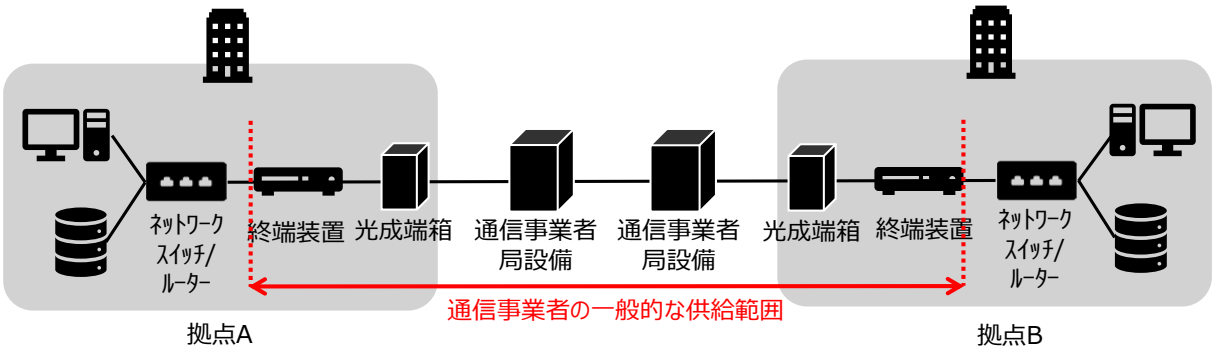


図 A-5：専用線サービス概念図

出典：https://www.ntt-west.co.jp/business/solution/digi/price/sub02/ をもとに作成

(2) ダークファイバー・WDM

ダークファイバーは、通信事業者が提供する未使用の光ファイバーケーブルであり、企業や組織が自分たちでネットワークを構築するために使用することができる。ダークファイバーは、企業が独自のネットワークを構築し、専用の通信インフラを持つことができるため、非常に高い通信速度とセキュリティを確保することができる。特に大規模なデータセンター間の通信や、金融機関の取引ネットワークに利用されることが多い。

ダークファイバーは OSI 参照モデルの第 1 層：物理層に該当する。ダークファイバーは、光ファイバーケーブル自体を提供するため、物理的なデータ伝送媒体を構成する。利用者は、ダークファイバーを使用して独自のネットワーク機器を配置し、必要な通信インフラを自由に構築することができる。

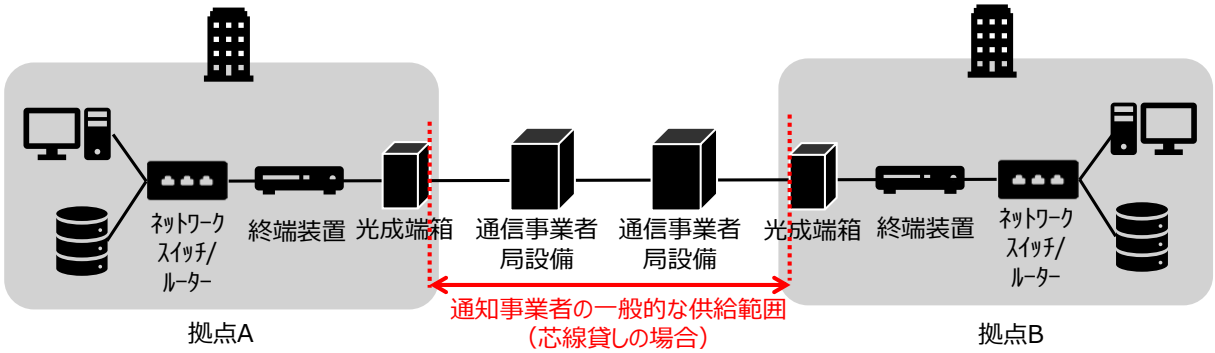


図 A-6：ダークファイバーの概念図

なお、WDM（Wavelength Division Multiplexing：波長分割多重方式）を活用して、一部の光波長を貸し出す WDM 専用線サービスもあるが、詳細については割愛する。

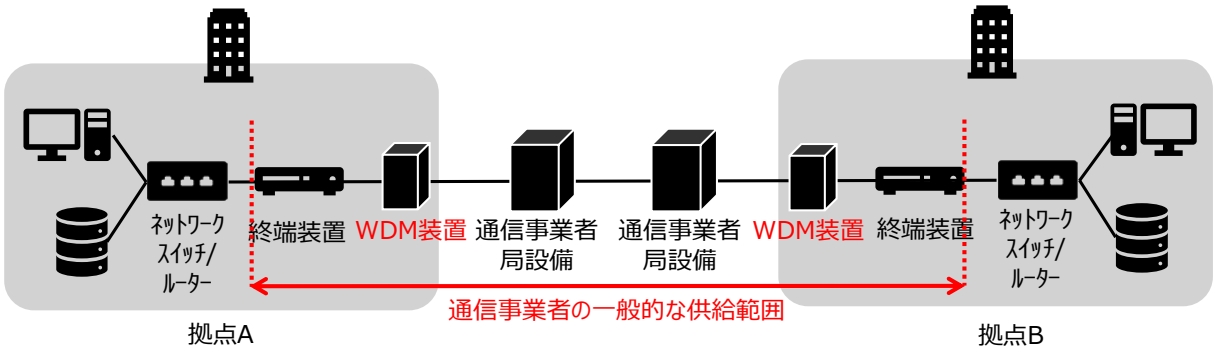


図 A-7：WDM 専用線の概念図

A.4.2 閉域網

閉域網も、特定の利用者だけが使用することができる通信回線である。「専用線」との大きな違いは、専用線が物理的に接続されたプライベートネットワークとされるのに対し、閉域網は VPN（Virtual Private Network）と呼ばれる仮想的なプライベートネットワークで構築されている点があげられる。

このような閉域網は論理的に他の利用者とは共有されないため、一般的にはセキュリティリスクが低いとされている。しかしながら、「プライベートネットワーク」で述べたように通信事業者の操作ミスや設定の誤り、あるいはネットワークへの侵入などの脅威は存在するため、閉域網はそれらのリスク管理を通信事業者に委託するものとの認識に立つ必要がある。

日本国内で利用されている閉域網には主に以下のような種類がある。なお、通信事業者が提供するサービスにより定義が異なることもあるため、その点は留意いただきたい。

（1）広域イーサネット

広域イーサネットは、広範囲にわたってイーサネット技術を利用して接続するサービスである。これは、企

業の拠点間を高帯域幅で接続し、大量のデータを迅速にやり取りすることができる。広域イーサネットは、都市部のオフィスビルや工場、データセンター間の接続に適しており、高速な通信が求められる場面で効果的である。このサービスは、イーサネット技術をそのまま広域ネットワークに適用するため、既存のネットワーク機器との互換性が高い。また広域イーサネットは、専用線に比べてコストが低く抑えられることが多い。

広域イーサネットは OSI 参照モデルの第 2 層：データリンク層に該当する。接続には第 2 層：データリンク層を使用するため、後述する IP-VPN と違って第 3 層：ネットワーク層で利用するプロトコルに制限がないことも特徴である。そのため、制御システムで利用される特殊なプロトコルを利用することもできる。

VLAN タグは、ネットワーク上のデータにタグを追加することで、そのデータがどの仮想 LAN（VLAN）に属しているかを識別する技術である。広域イーサネットで VLAN タグを利用することで、同じ物理ネットワーク上でも異なる拠点や部門のデータを論理的に分離して管理できる。これにより、企業の各拠点間でデータが混ざらず、セキュリティが向上する。また、ネットワークの混雑を避けて、安定した通信品質を保つのにも役立つ。

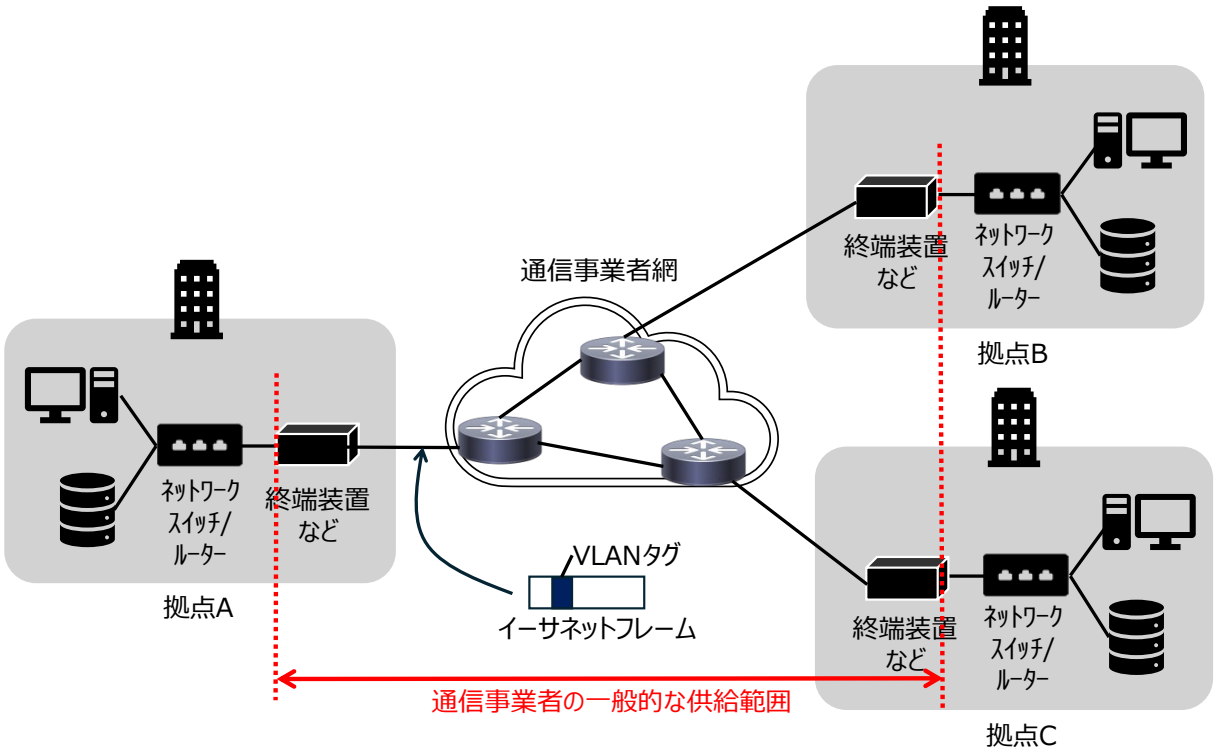


図 A-8：広域イーサネット概念図

出典：https://www.infraexpert.com/study/wan5.html をもとに作成

(2) IP-VPN

IP-VPN（Internet Protocol Virtual Private Network）は、インターネットプロトコルを使用し

て仮想的な専用ネットワークを構築するサービスである。IP-VPN は通信事業者の IP 網を経由することになるが、MPLS（Multiprotocol Label Switching）と呼ばれるデータをラベリングする技術を利用することで、各拠点間の通信を行う。企業の本社と支社、または複数の拠点をセキュアに接続するために広く利用されている。各拠点間の通信は通信事業者の IP 網内で行われ、MPLS ラベルにより通信したい拠点へデータを転送できるため、他企業の通信データが混ざらず、外部からの攻撃や不正アクセスのリスクを最小限に抑えることができる。また、IP-VPN はインターネットと同じインターネットプロトコルを使用しているため拡張性が高く、専用線や広域イーサネットに比べてコストが低く抑えられることが多い。

IP-VPN は OSI 参照モデルの第 3 層：ネットワーク層に該当する。IP-VPN は、MPLS を利用して第 3 層：ネットワーク層での効率的なルーティングを行い、拠点間の通信を確立する。そのため、IP-VPN は第 3 層：ネットワーク層で使用できるプロトコルが IP に制限される。ただし、IT システムで利用させるプロトコルは IP ベースがほとんどを占めており、近年は制御システムで利用させるプロトコルも IP ベースが多いことを言及しておく。

通信事業者の IP 網を他の利用者と共用することになるため、選択するサービスによっては通信品質が低下する場合もあるが、通信事業者の IP 網は十分な帯域が確保されているため安定した通信品質を保つことができる。

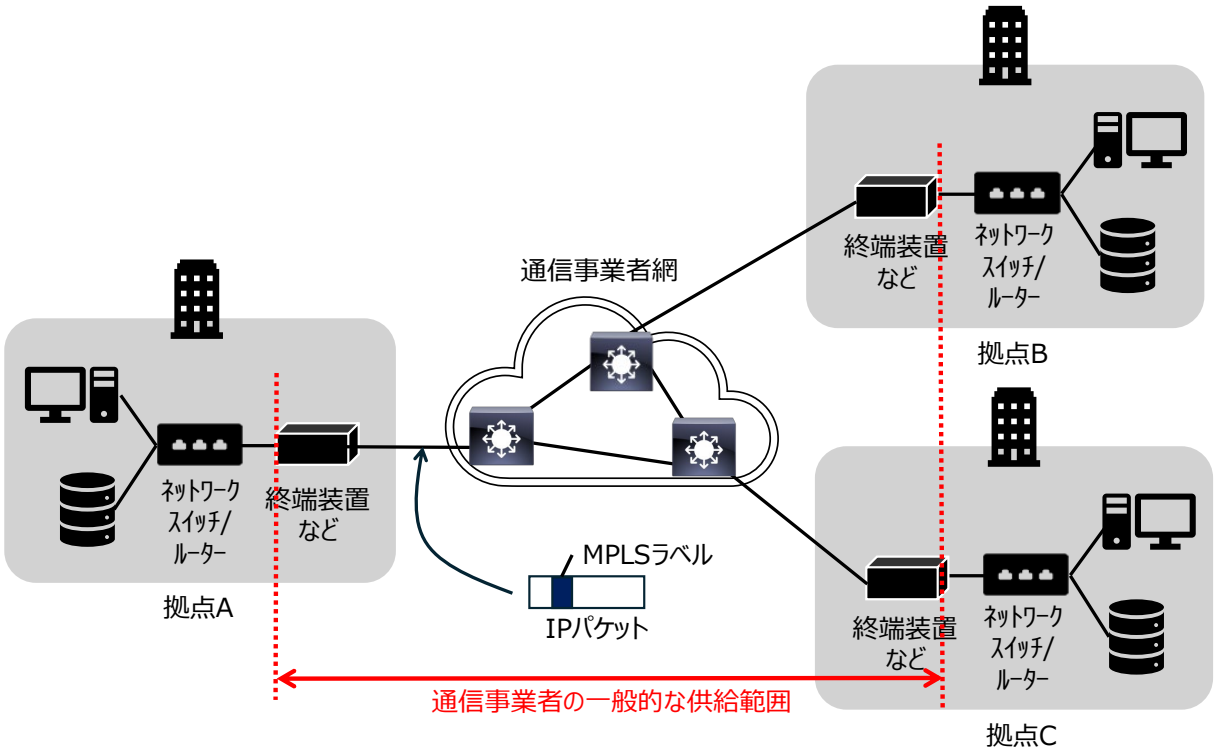


図 A-9：IP-VPN 概念図

出典：https://www.infraexpert.com/study/wan5.html をもとに作成

(3) エントリーVPN

近年エントリーVPN と呼ばれるサービスが通信事業者から提供されている。これは FTTH（Fiber to the Home）回線を利用した VPN サービスであり、前述した他の閉域網に比べ更にコストが低く抑えられることが多い。FTTH 回線は、光ファイバーを直接家庭やオフィスに引き込むことで、高速かつ安定したインターネット接続を提供する。(多くの読者の皆様のご家庭にも FTTH 回線が引かれているだろう。）エントリーVPN は、この FTTH 回線を活用して、各拠点間の通信を実現する。専用の VPN 機器やソフトウェアを使用して、データを暗号化し、安全な通信を確保する。

エントリーVPN は主に OSI 参照モデルの第 3 層：ネットワーク層に該当する。エントリーVPN は、FTTH 回線を利用し、ネットワーク層での IP 通信を基盤に、IPSec プロトコル（詳細は後述する）などを使用してデータを暗号化する。

FTTH の閉域網では、IPv6 のみ対応や、IPv4 は PPPoE（PPP over Ethernet）のみ対応など制限される場合があるが、エントリーVPN では利用者の通信をカプセル化してこの制限を回避する手法が取られる。

エントリーVPN は FTTH 回線の品質に依存するため、回線の混雑状況によって通信の安定性が変動する可能性がある。エントリーVPN の IP 網は、他のエントリーVPN 利用者やインターネットアクセスの契約者も利用し、IPSec という VPN 技術に依存しているため、「広域イーサネット」や「IP-VPN」といった閉域網とは異なる。このため、専用線や前述の閉域網と比較すると通信の安定性や信頼性に差があるが、適切な環境下では十分に安定した通信を提供することができる。

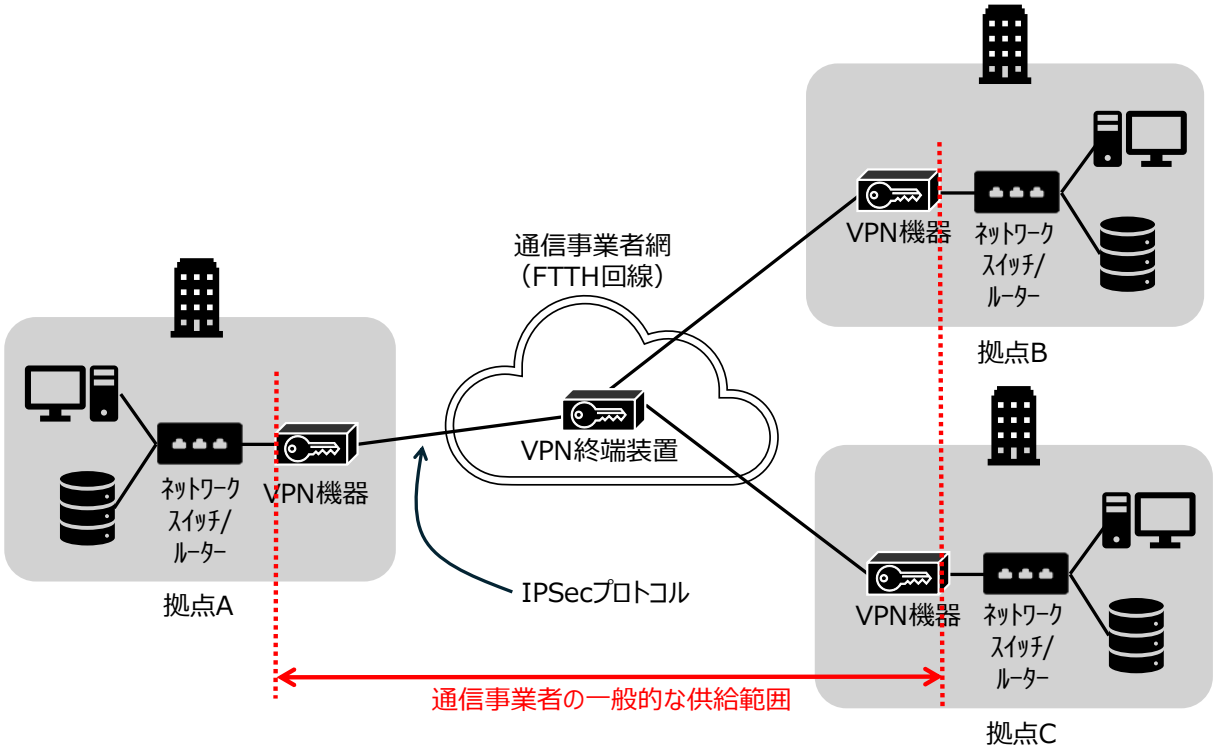


図 A-10：エントリーVPN 概念図

出典：https://techtarget.itmedia.co.jp/tt/news/0805/21/news01.html をもとに作成

(4) 閉域 SIM

閉域 SIM は専用の携帯通信サービスで、通常の携帯ネットワークとは異なり、インターネットを経由せずに特定の閉域網内で通信を行うことができる。このサービスは、例えば IoT デバイスやモバイルワーカーが企業ネットワークに安全に接続するために使用される。閉域 SIM は、専用の APN（Access Point Name）を設定することで、通信が特定の閉域網内に限定され、外部からのアクセスを遮断するものである。

閉域 SIM は OSI 参照モデルの第 1 層：物理層、第 2 層：データリンク層、第 3 層：ネットワーク層に該当する。第 1 層：物理層では、携帯通信の無線信号を利用し、第 2 層：データリンク層では、通信の確立と維持が行われる。第 3 層：ネットワーク層では、IP アドレスを使用してデータのルーティングが行われる。閉域網 SIM の利点は、モバイル通信の柔軟性と閉域網のセキュリティを組み合わせた点にある。

閉域 SIM の通信の安定性は、ネットワークの品質、サービスエリア、帯域幅、混雑状況、モバイル技術に依存する。携帯通信インフラを使うため、基地局の配置やサービスエリアの品質が重要である。都市部や基地局が多い場所では安定した通信が期待できるが、利用者が多いと速度低下や遅延が起こるこ

とがある。QoS（Quality of Service）技術を用いたサービスにより優先的に帯域を確保し、混雑時でも安定した通信を確保することもできる。

図 A-11：閉域 SIM 概念図

A.4.3 インターネット VPN

インターネット VPN も閉域網と同様に仮想的なプライベートネットワークである VPN の一つである。インターネット VPN は、パブリックインターネット即ちインターネットを経由して、VPN 機器やソフトウェアを用いることでプライベートネットワークを構築する技術である。閉域網に比べコストが低く抑えられるため、多くの企業で採用されている。この VPN は、リモートアクセス VPN や拠点間 VPN として利用され、利用者はインターネット接続を通じて（適切な設定・運用がされていれば）安全にプライベートネットワークにアクセスできる。インターネット VPN にはいくつかの分類があり、本書では代表的な 2 つを紹介する。

（1）SSL VPN

SSL VPN は、特定のアプリケーションのデータを暗号化し、安全に転送する技術である。SSL（Secure Sockets Layer）や TLS（Transport Layer Security）を使用して通信を暗号化し、データの安全性を確保する。SSL VPN はリモートアクセス端末に専用の VPN 用アプリケーションを使用する場合が多いが、Web ブラウザを利用してアクセスすることもできる。利用者は、VPN サーバーや指定された URL にアクセスして認証を行い、安全な VPN 接続を確立する。SSL VPN は、在宅勤務や出張中の従業員が企業ネットワークにアクセスする際に便利である。

SSL VPN は OSI 参照モデルの第 4 層：トランスポート層と第 7 層：アプリケーション層に該当する。

SSL/TLS プロトコルは第 4 層：トランスポート層で動作し、通信を暗号化する。利用者が利用するクライアントソフトウェアや Web ブラウザは第 7 層：アプリケーション層に位置する。

SSL VPN の利点は、導入が容易であり、既存のインフラを利用できる点にある。SSL/TLS を利用することでセキュリティを確保しながら、柔軟なアクセスを提供できる。

SSL VPN に限った話ではないが、インターネット VPN はパブリックネットワークであるインターネットを経由して利用される。そのためインターネット回線の品質に依存し、回線の混雑状況によって通信の安定性が変動する。また、パブリックなインターネットを利用するため、設定ミス、VPN 機器やソフトウェアの脆弱性などにより外部から侵入させるリスクがある。

SSL VPN には「リバースプロキシ方式」、「ポートフォワーディング方式」、「L2 フォワーディング方式」と呼ばれる 3 つの方式があるが本書では詳細は割愛する。SSL VPN について詳しく知りたい場合は、引用・参考文献[15]を参照されたい。

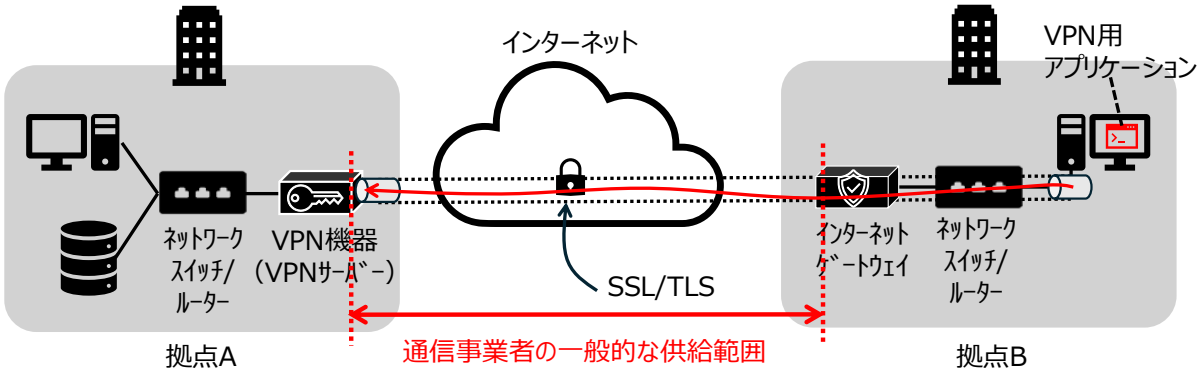


図 A-12：SSL VPN 概念図

(2) IPSec VPN

IPSec VPN は、IPSec（Internet Protocol Security）プロトコルを使用してデータを暗号化し、安全な通信を提供する VPN である。IPSec は、データの機密性、整合性、および認証を提供し、高いセキュリティを確保する。IPSec VPN は、拠点間 VPN として広く利用されている。企業の本社と支社間の通信や、リモートワーカーが企業ネットワークにアクセスする際に利用される。

IPSec VPN は OSI 参照モデルの第 3 層（ネットワーク層）と第 4 層（トランスポート層）に該当する。IPSec プロトコルは第 3 層（ネットワーク層）で動作し、IP パケットを暗号化する。また、第 4 層（トランスポート層）では、認証ヘッダ（AH）や暗号化ペイロード（ESP）を使用して、データの整合性と機密性を保証する。

IPSec VPN はトンネルモードとトランスポートモードの 2 つの動作モードを持ち、トンネルモードはネット

ワーク間のセキュアな通信に適しており、トランスポートモードはホスト間の通信に適している。IPSec VPN の利点は、一般的に SSL VPN に比べて高速であると言われており、拠点間 VPN で利用されることが多い。しかし、設定が SSL VPN に比べて複雑であり、導入には専門的な知見が必要である。

また、SSL VPN と同様に IPSec VPN もパブリックネットワークであるインターネットを経由して利用されるため、インターネット回線の品質に依存し、回線の混雑状況によって通信の安定性が変動する。また、パブリックなインターネットを利用するため、設定ミスや VPN 機器、ソフトウェアの脆弱性などにより外部から侵入されるリスクがある。

なお、L2TP/IPSec は、L2TP（Layer 2 Tunneling Protocol）と IPSec を組み合わせたもので、トンネリングとセキュリティを提供する方法の一つであるが、ここでは詳細を割愛する。

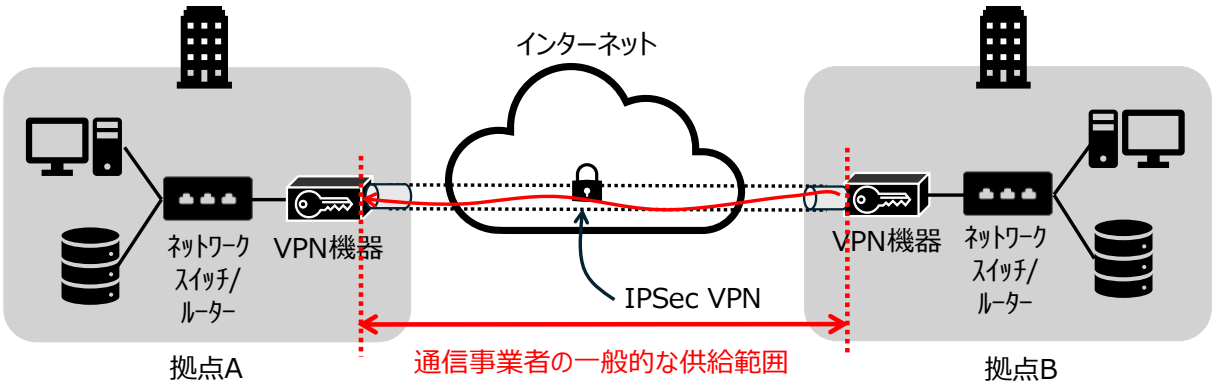


図 A-13：IPSec VPN 概念図(拠点間のトンネルモード)

付録B リモートアクセスに関連するサイバーインシデント事例

B.1 本付録の目的

制御システムへのリモートアクセスに関するサイバーインシデント事例について公開されているものは少ないが、2.2.(6)でも紹介したように一定数の会社はサイバー被害を受けている。リモートアクセスに関連するサイバー攻撃により発生する被害のイメージを持てるように事例を紹介する。

B.2 インシデントの概要

国内事業者にてリモートメンテナンス用回線を悪用されたと考えられるサイバーインシデント事例が 2023 年に発生した。このサイバー攻撃により当該事業者はシステム稼働が出来なくなり、復旧までに 3 日を要する被害となった。現場のオペレーションを担う機器は問題なかったが、支援システムがランサムウェア攻撃により全滅したことで全停止する事態となった。システムの復旧までの 3 日間は一部をマニュアル作業で対応を行い、その期間にバックアップから復旧を実施した。

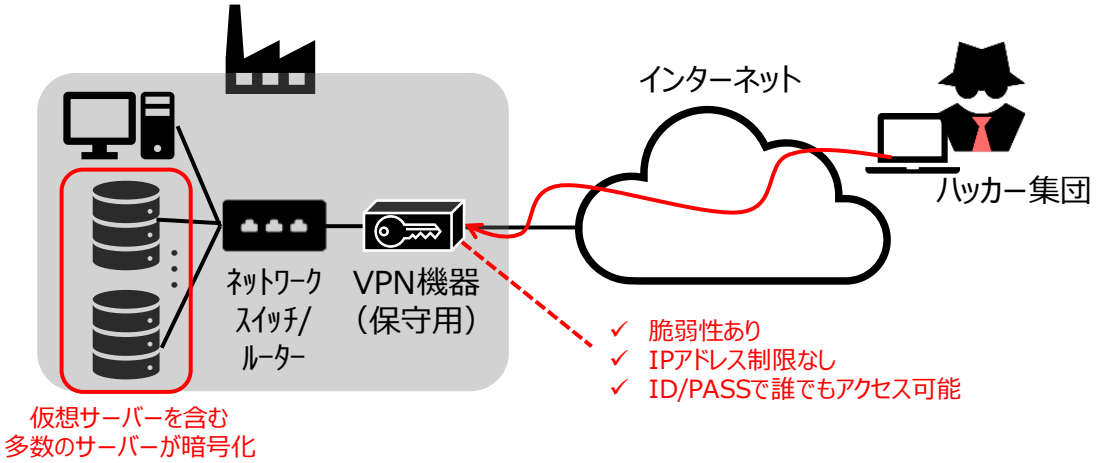


図 B-1：インシデントの概念図

B.3 インシデントの原因(侵入経路)

侵入経路として考えられる候補はいくつかあるが、リモートメンテナンス用に利用していた VPN 機器には脆弱性が存在しており、IP アドレス制限を実施しておらず ID とパスワードのみで誰でもアクセス可能な状態であったことから保守用 VPN 機器が侵入経路の可能性が高いとされている。

VPN 機器のログは別サーバー上に保存しており、そのサーバーも暗号化されてしまい、バックアップを取得していなかったため原因の特定には至っていないとされている。本事象はインシデント発生後の対応が迅速であったため 3 日間という短期間で復旧することができたが、セキュリティ機器を導入するだけでなく、導入時の設計をしっかり行っており脆弱性対応を行っていればそもそも攻撃自体を防げていた可能性が高いと考えられる。

付録C 用語集

番号	用語	意味・解説
1	CCE	Consequence-driven Cyber-informed Engineering： 結果重視型サイバー情報エンジニアリング CCE は、サイバー攻撃に対する防御を強化するためのセキュリティ分析手法。攻撃がもたらす可能性のある重大な結果に基づいて防御策を設計し、システムの最も重要な部分を保護することに焦点を当てている。
2	DCS	Distributed Control System：分散制御システム DCS は、工場やプラントで複数のコンピューターを使って機械を管理するシステム。各部分が独立して制御されるため、システム全体の信頼性が高まる。例えば、製造プロセスの監視や調整を行う。分散型アーキテクチャにより、柔軟性と拡張性が向上する。
3	DMZ	正式名称は「Demilitarized Zone（非武装地帯）」 外部ネットワーク（例えばインターネット）と内部ネットワーク（例えば企業の内部ネットワーク）の間に配置される中間領域を指す。この領域には公開サーバーやゲートウェイが配置され、外部からのアクセスを制限しつつ内部ネットワークのセキュリティを保護する。
4	DoS 攻撃	Denial of Service Attack：サービス妨害攻撃 DoS 攻撃は、ネットワークやサービスに大量のリクエストを送信して、正常な動作を妨げる攻撃。ターゲットのリソースを消耗させ、サービスを停止させることを目的とする。対策としては、ファイヤーウォールの設定強化やトラフィックの監視が重要。企業や公共サービスへの影響が大きい。
5	EDR	Endpoint Detection and Response：エンドポイント検知と対応 EDR は、エンドポイントで発生する異常をリアルタイムで検知し、迅速に対応するシステム。ウイルスや不正アクセスなどを自動で検出し、対策を講じる。高度な解析機能を持ち、詳細なログを保存してインシデントの調査にも役立つ。エンドポイントセキュリティの強化に欠かせないツール。
6	EWS	Engineering Workstation：エンジニアリングワークステーション エンジニアリングワークステーションは、工場やプラントの制御システムを設計、プログラミング、保守するためのコンピューター。PLC や DCS といった機器の設定や修正、HMI の管理を行い、システムの動作を監視する役割を持つ。
7	GUI	Graphical User Interface：グラフィカルユーザーインターフェース GUI は、コンピューターやソフトウェアを使いやすくするための画面デザインを指す。アイコンやボタン、メニューなどの視覚的な要素を使って、ユーザーがマウスやタッチパネルで操作できるようにする。これにより、コマンドを直接入力する必要がなく、視覚的にわかりやすい操作が可能になる。例えば、スマートフォンのアプリやパソコンのデスクトップ画面が GUI の代表例。

8	HMI	Human-Machine Interface：ヒューマンマシーンインターフェース HMI は、機械やコンピューターと人間がやり取りするための画面やボタン。工場の機械操作やプロセスの監視に使われる。操作パネルやタッチスクリーンなどがあり、直感的に操作できるように設計されている。HMI を通じて機械の状態をリアルタイムで確認し、必要な操作を行う。
9	HTTPS	HyperText Transfer Protocol Secure： セキュアハイパーテキスト転送プロトコル HTTPS は、インターネット上で安全にデータを送受信するためのプロトコル。通常の HTTP に SSL/TLS 暗号化を追加して通信を保護する。ウェブサイトのアドレスが「https://」で始まり、機密情報や個人情報を安全にやり取りするために使われる。オンラインショッピングやバンキングなどで広く利用されている。
10	ICS	Industrial Control System：産業制御システム ICS は、工場や発電所などの産業施設で使用される制御システムを指す。具体的には、製造装置や発電装置を自動的に操作・管理するためのハードウェアおよびソフトウェア技術を含む。例として、プログラマブル・ロジック・コントローラー（PLC）や分散制御システム（DCS）などがある。これらのシステムは、安全かつ効率的に施設を運用するために不可欠である。
11	IoT	Internet of Things：モノのインターネット IoT は、インターネットに接続された家電や機械などがデータをやり取りする技術。スマートホームでは、冷蔵庫やエアコンがインターネットを通じて操作できる。工場では、センサーや機械が連携して効率的な生産を実現する。データの収集と分析によって、新しいサービスやビジネスモデルを生み出す。
12	IPv4	Internet Protocol Version 4：インターネットプロトコルバージョン 4 IPv4 は、インターネットで使われる従来のアドレス体系。32 ビットのアドレス空間を持ち、約 43 億のユニークアドレスを提供する。現在でも多くのネットワークで使用されているが、アドレスの枯渇が問題となっている。IPv6 への移行が進む中、互換性のために併用されることが多い。
13	IPv6	Internet Protocol Version 6：インターネットプロトコルバージョン 6 IPv6 は、インターネットで使用される新しいアドレス体系で、膨大な数のデバイスを接続できるようにする。従来の IPv4 では不足していたアドレス空間を大幅に拡張し、より多くの機器がネットワークに接続可能。セキュリティやルーティング効率の改善も含まれており、次世代インターネットの基盤となる技術。
14	MAC ｱﾄﾞﾚｽ	MAC Address：MAC アドレス MAC アドレスは、ネットワーク機器に割り当てられた一意の識別番号。各デバイスが通信するときに使用され、ネットワーク上でデバイスを特定するために使われる。通常、ハードウェアに固定されており、変更が難しい。ネットワーク管理やセキュリティにおいて重要な役割を果たす。
15	NIST	NIST: National Institute of Standards and Technology NIST は米国国立標準技術研究所で情報セキュリティの標準やガイドライン

		を発行している。
16	NTP	Network Time Protocol：ネットワークタイムプロトコル NTP は、ネットワーク上のコンピューターの時計を正確に同期させるためのプロトコル。時間のズレを修正し、全ての機器が同じ時間を共有できるようにする。これにより、ログのタイムスタンプが一致し、システムのトラブルシューティングや監査が容易になる。ネットワーク全体の調整が重要な役割を果たす。
17	OT	Operational Technology：運用技術 Operational Technology は、工場やプラント、インフラ施設などの運用管理に関わるハードウェアおよびソフトウェア技術を指す。具体的には制御システム、監視装置、センサー、アクチュエーターなどが含まれる。
18	PLC	Programmable Logic Controller：プログラマブルロジックコントローラ PLC は、工場や生産ラインで機械を自動制御するための専用機器。プログラムを使って複雑な操作を簡単に実行できる。例えば、ベルトコンベアの速度調整や機械の稼働タイミングの管理に使われる。信頼性が高く、厳しい環境下でも安定して動作する。
19	RDP	Remote Desktop Protocol：リモートデスクトッププロトコル RDP は、遠隔地にあるコンピューターを操作するための通信プロトコル。離れた場所からコンピューターの画面を共有し、直接操作できる。これにより、システム管理者がリモートでトラブルシューティングを行ったり、ソフトウェアをインストールしたりできる。安全な接続を確保するため、暗号化技術が使われる。
20	SIEM	Security Information and Event Management： セキュリティ情報およびイベント管理 SIEM は、コンピューターやネットワークのセキュリティを監視し、異常があったときに通知するシステム。ログデータを収集し、分析して不正な動きを早期に検出する。セキュリティインシデントの管理や対応を効率化するために重要。
21	SLA	Service Level Agreement：サービスレベル契約 SLA は、サービス提供者と利用者の間でサービスの品質や範囲について明確にする契約。具体的には、応答時間や稼働時間、サポート対応の時間などが含まれる。SLA によって、提供されるサービスの水準を保証し、トラブルが発生した際の対応方法が決まる。
22	SOC	Security Operation Center：セキュリティ運用センター SOC は、コンピューターシステムやネットワークをサイバー攻撃から守るための施設やチームを指す。SOC では、専用のソフトウェアと専門家が 24 時間体制でシステムの監視、攻撃の検出、対応を行う。具体的には、ログ分析、異常検知、インシデント対応などが含まれ、システムの安全を維持する役割を果たしている。
23	SSH	Secure Shell：セキュアシェル SSH は、インターネットを通じて安全にリモートコンピューターに接続するためのプロトコル。データの送受信を暗号化し、不正アクセスを防止する。主にリモ

		ートログインやリモートコマンド実行に使われる。サーバー管理者が遠隔地からサーバーを操作する際に利用されることが多い。
24	Syslog	Syslog：シスログ Syslog は、コンピューターやネットワーク機器のログ情報を集め、保存するためのプロトコル。システムの動作状態やエラー情報を一元管理し、問題発生時に迅速な対応ができる。ログデータを分析することで、システムのパフォーマンスやセキュリティの向上につながる。
25	TLS	Transport Layer Security：トランスポート層セキュリティ TLS は、インターネット上でデータを安全に送受信するための暗号化プロトコル。HTTPS などで使われ、通信内容を保護する。TLS を使うことで、第三者がデータを盗み見ることを防ぎ、通信の信頼性を高める。ウェブブラウザやメールクライアントなど、多くのインターネットアプリケーションで使用される。
26	ｲﾝｼﾃﾞﾝﾄ	Incident：インシデント インシデントは、コンピューターやネットワークに関する問題や事件。セキュリティインシデントには、ウイルス感染、ハッキング、不正アクセスなどが含まれる。インシデントが発生すると、システムの正常な動作が妨げられ、データの漏洩やサービスの停止などの被害が生じることがある。
27	ｲﾝﾀｰﾈｯﾄｹﾞｰﾄｳｪｲ	Internet Gateway：インターネットゲートウェイ インターネットゲートウェイは、内部ネットワークとインターネットの間でデータをやり取りするための装置。企業のネットワークと外部のインターネットを接続するためのポイントで、データのルーティングやセキュリティの強化に役立つ。
28	ｴﾝﾄﾞﾎﾟｲﾝﾄｾｷｭﾘﾃｨ	Endpoint Security：エンドポイントセキュリティ エンドポイントセキュリティは、パソコンやスマートフォンなどの端末を守るためのセキュリティ対策。ウイルス対策ソフトやファイヤーウォール、暗号化などが含まれる。端末の安全性を保つことで、ネットワーク全体のセキュリティを強化する。特に企業では、エンドポイントの管理が重要となる。
29	ｸﾚﾃﾞﾝｼｬﾙ	Credential：クレデンシャル クレデンシャルは、システムやサービスへのアクセス権を証明するための情報。ユーザー名とパスワード、証明書、トークンなどが含まれる。クレデンシャルを適切に管理することで、不正アクセスを防ぐことができる。セキュリティの基本要素であり、認証と認可の基盤となる。
30	ｻｲﾊﾞｰｷﾙﾁｪｰﾝ	Cyber Kill Chain：サイバーキルチェーン サイバーキルチェーンは、サイバー攻撃がどのように進行するかを段階ごとに示すモデル。攻撃者が標的を選び、情報収集し、武器を作り、攻撃を実行し、目的を達成するまでの過程を理解するためのフレームワーク。このフレームワークを使うと、攻撃の各段階でどんな対策を取れば良いかがわかる。例えば、攻撃の準備段階で防御策を強化することで、攻撃を未然に防ぐことができる。これにより、サイバー攻撃からシステムを守るための効果的な対策ができる。

31	ｽﾙｰﾌﾟｯﾄ	Throughput：スループット スループットは、ネットワークや機械が一定時間内に処理できるデータ量を示す指標。高いスループットは、システムの性能や効率の高さを意味する。ネットワークの帯域幅や機械の処理能力を評価するために重要。性能向上のために、スループットの最適化が行われることが多い。
32	ｾｯｼｮﾝ	Session：セッション セッションは、コンピューターとユーザーの間で行われる一連のやり取り。ログインからログアウトまでの間に発生するすべての通信が含まれる。セッションを使うことで、ユーザーの状態を維持し、連続した操作をスムーズに行える。
33	ﾃﾞｰﾀﾋｽﾄﾘｱﾝ	Data Historian：データ履歴管理システム データヒストリアンは、機械やセンサーからのデータを長期間にわたって収集・保存するシステム。製造業やプラントで使われ、データを分析することで機械の効率や品質の向上に役立つ。例えば、過去のデータを基にトラブルの原因を探ったり、予防保全の計画を立てたりすることができる。
34	ﾈｯﾄﾜｰｸｽｲｯﾁ	Network Switch：ネットワークスイッチ ネットワークスイッチは、複数のコンピューターをネットワークで接続し、データのやり取りを効率的に行う装置。各デバイスが送受信するデータを管理し、最適な経路で転送する。ネットワークの拡張性とパフォーマンスを向上させるために重要な役割を果たす。企業やデータセンターで広く使用される。
35	ﾊｰﾄﾞｳｪｱﾄｰｸﾝ	Hardware Token：ハードウェアトークン ハードウェアトークンは、コンピューターに安全にアクセスするための物理的な装置。USB やスマートカードの形状をしており、多要素認証として使用される。パスワードに加えてトークンを使用することで、セキュリティを強化する。特に金融機関や企業の重要システムで利用される。
36	ﾊﾟｯﾁ	Patch：修正プログラム パッチは、ソフトウェアのバグを修正したり、セキュリティの脆弱性を改善するための小さなプログラム。ソフトウェア開発者が問題を発見し、それを修正するパッチを提供する。ユーザーはこれを適用することで、システムの安全性や機能を向上させることができる。定期的なパッチ適用が重要。
37	ﾌｧｲﾔｰｳｫｰﾙ	Firewall：ファイヤーウォール ファイヤーウォールは、ネットワークを守るために不正なアクセスを遮断するセキュリティシステム。ネットワークの出入り口に設置し、特定の通信だけを許可する。ハードウェアタイプとソフトウェアタイプがあり、企業のネットワークセキュリティに欠かせない。内部ネットワークを外部の脅威から守る役割を果たす。
38	ﾌｧｲﾙﾚｽ攻撃	Fileless Attack：ファイルレス攻撃 ファイルレス攻撃は、ファイルを使用せずにメモリ内で直接実行されるマルウェア攻撃。従来のウイルス対策ソフトでは検出が難しく、検知が遅れることが多い。システムの脆弱性を利用して侵入し、持続的な攻撃を行う。高度なセキュリティ対策と行動分析が必要。

39	ﾌﾟﾗｲﾍﾞｰﾄﾈｯﾄﾜｰｸ	Private Network：プライベートネットワーク プライベートネットワークとは、特定の人々だけが利用できるネットワーク。例えば、ある会社の中だけで使われるネットワークがこれにあたる。プライベートネットワークは外部からのアクセスが制限されており、会社の中だけで安全に情報をやり取りすることができる。プライベートネットワークを使うことで、会社の重要な情報が外部に漏れる心配が少なくなる。
40	ﾌﾟﾛｸﾞﾗﾏﾌﾞﾙ表示器	Programmable Display：プログラマブル表示器 プログラマブル表示器は、機械やシステムの状態を表示し、操作を簡単にする画面装置。工場の機械やプラントのプロセス監視に使われ、プログラムにより表示内容を自由に変更できる。直感的な操作性を提供し、現場の効率向上に役立つ。タッチスクリーンやカスタマイズ可能なインターフェースが特徴。
41	ﾍﾟﾈﾄﾚｰｼｮﾝﾃｽﾄ	Penetration Test：侵入テスト ペネトレーションテストは、システムに対して実際に攻撃を仕掛け、脆弱性を発見するテスト。攻撃者の視点でシステムの防御力を評価し、弱点を見つけて修正する。セキュリティ専門家が実施し、テスト結果をもとに具体的な改善策を提案する。企業のセキュリティ対策の一環として重要な手法。
42	ﾎﾟｰﾄ	Port：ポート ポートは、コンピューターがネットワークを通じてデータを送受信するための出入り口。ポート番号は、特定のサービスやアプリケーションに対応している。ファイヤーウォールでポートを管理することで、不要な通信をブロックすることができる。
43	ﾙｰﾀｰ	Router：ルーター ルーターは、異なるネットワーク間でデータを送り届けるための装置。インターネットと企業内ネットワークをつなぐ役割を持つ。ルーターは、パケットの送信先を決定し、最適な経路を選択してデータを転送する。企業のネットワークインフラの重要な要素であり、通信の中枢を担う。
44	ﾙｰﾃｨﾝｸﾞ	Routing：ルーティング ルーティングは、データを最適な経路で送り届けるためのプロセス。ネットワーク内でデータの流れを管理し、効率的に通信を行う。ルーターがその役割を担い、各デバイス間の通信を最適化する。適切なルーティングにより、ネットワークの速度や信頼性が向上する。
45	ﾚｼﾞﾘｴﾝｽ	Resilience：レジリエンス 困難や変化に直面しても、元の状態や機能に戻る能力を指す。例えば、サイバー攻撃に対して、迅速に回復し、事業を継続する能力を指す。組織やシステムがレジリエントであるためには、予測や準備、迅速な対応が重要である。また起きた後の復旧計画や再開プロセスも重要である。レジリエンスは、組織や個人が変化や困難に適応するための重要な能力と言える。
46	ﾛｰﾄﾞﾊﾞﾗﾝｻｰ	Load Balancer：ロードバランサー ロードバランサーは、複数のサーバーに処理を分散させて、システムの負荷を均等にする装置。これにより、サーバーの性能を最大限に引き出し、サービスの安定性を保つ。

47	暗号鍵	Encryption Key：暗号鍵 暗号鍵は、データを暗号化して安全に保管したり、送信したりするためのキー。暗号化は、データを保護するための技術であり、キーがないとデータを読み取ることができない。機密情報のやり取りには欠かせない。
48	仮想 LAN （VLAN）	Virtual Local Area Network：仮想ローカルエリアネットワーク VLAN は、一つの物理ネットワークを複数の仮想ネットワークに分ける技術。異なるネットワークセグメント間でのデータ通信を分離し、セキュリティとパフォーマンスを向上させる。例えば、企業の部署ごとに VLAN を設定することで、トラフィックの管理と制御が容易になる。ネットワークの柔軟性を高める。
49	脆弱性	Vulnerability：脆弱性 脆弱性は、コンピューターシステムやソフトウェアに存在するセキュリティ上の弱点。これを悪用されると、システムが不正に操作されたり、データが盗まれたりするリスクがある。脆弱性の原因は、バグや設定ミス、設計上の問題などさまざまで、定期的な検査と対策が必要。
50	脆弱性診断	Vulnerability Assessment：脆弱性診断 脆弱性診断は、システムのセキュリティをチェックして脆弱性を見つける作業。専門家がシステムを調査し、どこに弱点があるかを報告する。診断結果に基づいて対策を講じることで、システムの安全性を高める。定期的に実施することで、最新の脅威に対抗することができる。
51	多層的な対策	IT 環境で広く採用されている手法で、複数のセキュリティ対策を組み合わせて階層（レイヤー）を築くことにより、1 つの対策が破られても次の対策が攻撃を抑止し、重要な部分への侵入前に攻撃を検知して対応することができる。この方法は、攻撃の難易度（攻撃コスト）を上げる効果があり、攻撃者に断念させる効果も期待できる。
52	横展開 (ﾗﾃﾗﾙﾑｰﾌﾞﾒﾝﾄ)	Lateral Movement：横展開 横展開は、システムに侵入した攻撃者が、ネットワーク内で他のコンピューターに移動する行動。攻撃者は、初めに侵入した端末からさらに重要なシステムやデータにアクセスしようとする。これを防ぐために、ネットワークの分割やアクセス制御が重要となる。横展開は、セキュリティインシデントの拡大を防ぐ上で注目される概念。

付録D 引用・参考文献

[1] CPNI. ”SCADA およびプロセス制御ネットワークにおけるファイアウォールの利用についての NISCC グッド・プラクティス・ガイド”. https://www.jpcert.or.jp/research/2007/NISCC-GoodPracticeGuide-on-SCADA-Firewalls.pdf, (参照：2024-03-28).

[2] CPNI. ”グッド・プラクティス・ガイド プロセス制御と SCADA セキュリティ”. https://www.jpcert.or.jp/research/2007/GoodPractice-for-ProcessControl-and-SCADA-Security.pdf, (参照：2024-03-28).

[3] Jon C. Snader. VPNs Illustrated: Tunnels, VPNs, and IPsec. O’Reilly, 2005.

[4] Mike Erwin, Charlie Scott, Paul Wolfe. Virtual Private Networks, Second Edition. O’Reilly, 1998.

[5] NERC. ”CIP CIP-005 Cyber Security – Electronic Security Perimeter(s) ”. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf, (参照：2024-03-28).

[6] NIST. ”NIST SP.800-46 Revision 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security”. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf, (参照：2024-03-28).

[7] NIST. ”NIST SP800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations ”. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, (参照：2024-03-28).

[8] NIST. ”NIST SP800-82r3 Guide to Operational Technology(OT) Security”. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf, (参照：2024-03-28).

[9] NTT 西日本. "毎月の費用 - ディジタルアクセス（デジタル専用線）". NTT 西日本 法人向けサービス. https://www.ntt-west.co.jp/business/solution/digi/price/sub02/, (参照：2024-05-16).

[10] U.S. Department of Energy. "Consequence-driven Cyber-informed Engineering". https://www.osti.gov/biblio/1341416, (参照：2024-03-28).

[11] 池上祐太, 河田芳秀. 制御システムセキュリティ入門. NTT 出版. 2020.

[12] 井上直也, 村山公保, 竹下隆史, 荒井透, 苅田幸雄. マスタリング TCP/IP―入門編―. オーム社. 2019.

[13] 北尾辰也. "名古屋港コンテナターミナルを襲ったサイバー攻撃とその背景". 国土交通省. https://security-portal.nisc.go.jp/cybersecuritymonth/2024/seminar/pdf/03_kitao_2024.pdf, (参照：2024-05-17).

[14] ネットワークエンジニアとしての管理人. "WAN - IP-VPN / Wide Ethernet". ネットワークエンジニアとして. https://www.infraexpert.com/study/wan5.html, (参照：2024-05-16).

[15] 富士通株式会社. "SSL-VPN 入門". 1998. https://fenics.fujitsu.com/products/ipcom/catalog/data/ipcom_wp_sslvpn_01.pdf, (参照：2024-05-16).
[16] りょう. "OSI 参照モデルと TCP/IP 階層モデルの違いを分かりやすく解説！". RYONOTES. https://ryonotes.com/difference-between-osi-and-tcpip/, (参照：2024-05-16).
[17] 翁長潤. "初歩から理解するネットワークの基礎（1）--ネットワークの基本を分かりやすく解説". ZDNET Japan. https://japan.zdnet.com/article/35137192/, (参照：2024-05-16).
[18] 経済産業省 "民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0". https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/20230331_1.pdf, (参照：2024-05-27).
[19] 経済産業省. ”工場システムにおけるサイバー・フィジカル・セキュリィ対策ガイドライン Ver1.0”. https://www.meti.go.jp/press/2022/11/20221116004/20221116004.html, (参照：2024-03-28).
[20] 総務省. "テレワークセキュリティガイドライン 第 5 版”. https://www.soumu.go.jp/main_content/000752925.pdf, (参照：2024-03-28).
[21] 池田冬彦. "エントリーVPN の正体「安全、高速、安価な WAN」は本当か". Itmedia TechTarget ジャパン. https://techtarget.itmedia.co.jp/tt/news/0805/21/news01.html, (参照：2024-05-16).
[22] 独立行政法人情報処理推進機構. "制御システムのセキュリティリスク分析ガイド第 2 版". https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf, (参照：2024-03-28).
[23] 独立行政法人情報処理推進機構. ”重要インフラのサイバーセキュリティを改善するためのフレームワーク”. https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000071204.pdf, (参照：2024-05-27).
[24] 独立行政法人情報処理推進機構. ”スマート工場のセキュリティリスク分析調査". https://www.ipa.go.jp/security/controlsystem/controlsystem-smartplant.html, (参照：2024-05-27).
[25] 独立行政法人情報処理推進機構. ”スマート工場化でのシステムセキュリティ対策事例 調査報告書”. https://www.ipa.go.jp/security/controlsystem/securityreport-smartfactory-2023.html, (参照：2024-05-27).
[26] 独立行政法人情報処理推進機構. ”制御システムのセキュリティリスク分析ガイド 第 2 版”. https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf, (参照：2024-03-28).


Industrial Cyber Security Center of Excellence
ICSCoE