産業用制御システム向け侵入検知製品の実装技術の調査

調査報告書

令和 4 年 9 月

独立行政法人情報処理推進機構

更新履歴

2022 年 9 月 20 日	初版

目次

図目次

表目次

1. 本調査の概要

本調査においては、産業用制御システム用の侵入検知製品の技術を、検知手法、検知方法および侵入検知製品の付加機能の 3 つの観点から整理し、全体を俯瞰する説明資料を作成した。また、侵入検知製品を利用している事業者での侵入検知技術の実際の使われ方を調査し、利用形態や参考になるポイントをまとめた報告書を作成した。

1.1. 本調査の背景と目的

重要インフラの各種システム、工場の製造システム等の産業用制御システムのオープンネットワーク化と情報技術の活用の進展に伴い、産業用制御システムのネットワークセキュリティリスクへの対策が急務となっている。ネットワークセキュリティリスクへの対策においては、防御と並んで、重要な要素が検知である。産業用制御システムに対する侵入検知手段としては、産業用制御システム向けのネットワークへの不正侵入を検知する製品が登場してきている。

他方、このような侵入検知製品については、導入方法や運用方法等が分かりにくいため、導入を躊躇する事業者が少なくないのが現状である。

このような状況を踏まえ、侵入検知製品を重要インフラの各種システムや工場の製造システム等の産業用制御システムに実際に導入し、検知に活用してセキュリティリスクを低減しようとする事業者に対して、円滑な導入方法や有効な運用方法等、導入に役立つ情報を提供することを目的として、本調査を行った。

1.2. 侵入検知技術の説明資料の作成の概要

産業用制御システム用の侵入検知製品の技術について、検知手法、検知方法および侵入検知製品の付加機能の 3 つの観点から、技術全体を俯瞰できるような説明資料（「産業用制御システムにおける侵入検知製品の技術の分類・整理結果」）を作成した。これを第 2 章に示す。

産業用制御システムにおける侵入検知製品の技術の分類・整理にあたっては、当該技術分野の公的文書である「NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems(侵入検知および侵入防止システムに関するガイド)」や、産業用制御システム用の侵入検知製品を提供する各種ベンダーの公開資料等を参考にするとともに、専門家によるレビューを受けて、専門的な知見を反映した。

1.3. 侵入検知技術の利用動向調査の概要

事業者での侵入検知技術の実際の使われ方の調査として、実際に侵入検知製品を利用している事業者での利用動向をヒアリングによる利用動向調査で把握した。

利用動向調査では、実際に侵入検知製品をビルシステムに適用している不動産・ビル業界の 2 事業者、重要インフラの各種システムに適用している運輸・交通業界の 4 事業者、石油

精製プラントの制御システムに適用している石油・エネルギー業界の 1 事業者の計 7 事業者に対してヒアリングを行い、侵入検知技術の実際の使われ方を把握し、利用形態や参考になるポイント等を取りまとめた。結果を第 3 章と第 4 章に示す。

尚、利用動向調査は、ヒアリング先の事業者の生の意見を、極力そのまま記載することとし、IPA としての何等かの推奨や推薦、逆に非推奨や反対等の意見を示すものではない。

2. 産業用制御システムにおける侵入検知製品の技術の分類･整理結果

2.1. 検知手法

侵入検知システムにおける検知手法について、NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems(侵入検知および侵入防止システムに関するガイド)等の資料に基づいて分類・整理を行った。分類・整理にあたっては、産業用制御システムに特有の観点について考慮した。以降においては、産業用制御システムを ICS と記載する。(ICS: Industrial Control System)

2.1.1. シグネチャー型

シグネチャーとは、マルウェアや不正アクセス等による既知の攻撃のパターンである。シグネチャーは、通常、侵入検知製品ベンダーによって提供され、新たなマルウェアや攻撃手法が検出されるたびに更新される。シグネチャーの例としては、電子メールに添付されたファイルの名称、セキュリティポリシーに違反したコマンド、通常は記録されることがない OS ログの値等がある。シグネチャーベースの検知では、観測された事象とシグネチャーとを比較し、事象がシグネチャーに一致した場合にアラートを生成する。具体的には、シグネチャーに記載された文字列をマルウェア等の活動(パケット、ログ項目など)と比較し、一致するかどうかを判定する。

シグネチャー型の検知は、既知の脅威に対しては非常に有効であるが、未知の脅威や、検知を回避するテクニック(難読化処理)により偽装された脅威、既知の脅威の変種に対しては効果を発揮できないことが多い。また、シグネチャー型の検知では、通信の状態やパケットの対応関係を追跡することはできないため、たとえば、Web ページに対するリクエストの応答としてステータスコード 403(リクエストの処理をサーバーが拒否したことを示すコード)が返されても、その対応関係を認識することができない。

また、それまでに行われたリクエストを記憶しながら現在のリクエストを処理することもできない。シグネチャー型の検知には、このような制約があるため、複数のイベントから構成される攻撃の場合、いずれか 1 つのイベントに明確な攻撃の形跡が含まれていない限り検知することができない。

(1) 長所

○既知のよく知られているマルウェアや、ソフトウェアの脆弱性を悪用した攻撃に対しては非常に有効である。

(2) 短所

○既知のマルウェアや誤動作しか検知できない。

○正規のコマンドを使用した攻撃については、シグネチャーが存在しないため、

検知できない。

○高度な攻撃者であれば、検知をすり抜けることができる。

○新たな攻撃手法が発見されるたびにシグネチャーを更新しなければならない。特に、侵入検知システム全体を管理する管理サーバーが用意されていない場合、監視対象のシステムの数が多くなると、全ての監視システムのシグネチャーのアップデートに時間を要する場合がある。

○シグネチャーが厳格過ぎる場合や、特定の ICS ネットワークにおけるトラフィックの種類によっては、誤検知が発生する可能性がある。

2.1.2. ルールベース（仕様ベース）

ネットワークトラフィックを監視し、予め作成された、正常なネットワークトラフィックのパターンが登録されているホワイトリストに一致しないネットワークトラフィックを検知した場合にアラートを生成する。ホワイトリストは、通信トラフィックのパターンの他に、OSI（Open Systems Interconnection）[1]の 7 階層参照モデルの各レイヤにおいて定義することができる。すなわち、機器の MAC アドレスや IP アドレス、通信に使用されるポート番号、アプリケーション（プロトコル/コマンド内容含む）のそれぞれについて、許可対象の属性をホワイトリストに定義しておき、一致するかどうかの判断に基づく侵入検知を行うことができる。一般の情報システムを対象とする侵入検知システムにおけるホワイトリストは、アプリケーションを対象とするホワイトリストを指していることが多いが、ICS を対象とする侵入検知システムにおいては、ICS 機器の IP アドレスが固定されていて、ICS 機器間における通信の相手先もほぼ決まっているため、ICS 機器の MAC アドレスや IP アドレスのような、より低いレイヤの属性を対象とするホワイトリストも有効である。

有効性と使いやすさは、監視対象の ICS ネットワークのトラフィックおよびプロトコルの解析がどれだけ正確に実施できるかによって決まる。検知ルールは、監視対象の ICS のプロセスを熟知した専門家によって、手作業で作成される。

(1) 長所

○ホワイトリストに基づく検知によって、基本的には、マルウェアの Command & Control 通信からオペレーターの誤操作まで、既知および未知の脅威の両方に対応可能である。

(2) 短所

○検知の精度を高めるために、ICS のプロセスで使用される全てのメッセージ

[1] コンピュータ間通信に関する国際標準で、ISO/IEC 7498-1 として規格化されている。通信に必要な機能を 7 つの階層に分けて整理していることから、7 階層参照モデル(Seven layer reference model)と呼ばれている。
https://www.iso.org/ics/35.100/x/

のタイプとフィールド値に関するホワイトリストを作成する必要があり、そのための作業に予算と期間を要する。

〇ネットワークやシステムの構成が変更されるたびに、検知ルールのアップデートが必要となる。

〇ホワイトリストで許可された範囲内の正規のコマンドによる誤操作や攻撃（停止コマンド発行など）については、検知できない。

2.1.3. 振る舞い検知型

振る舞い検知は、観測したイベントと監視対象デバイスにおける正常とみなされる活動(プロファイル)とを比較し、正常な活動からの重大な逸脱があった場合にアノマリーと判断する。振る舞い検知では、ユーザー、ホスト、ネットワーク接続、アプリケーションなどについての正常な挙動をプロファイルとして規定する。プロファイルは、システム・ネットワークにおける通常の活動内容の特徴をある一定期間にわたって監視することにより作成される。ネットワークトラフィックを検証し、通常と異なるトラフィックフローを生成する脅威を特定することにより、分散サービス妨害(DDoS：Distributed Denial of Service)攻撃やある種のマルウェア(ワーム、バックドアなど)、ポリシー違反(たとえば、クライアントシステムから他のシステムへのネットワークサービス提供)などを検知する。

たとえば、ネットワークのプロファイルに、通常の就業時間帯における Web トラフィックがネットワーク帯域幅に占める割合がしきい値として規定されている場合、統計的な手法を用いて、現在のネットワーク活動に見られる特徴とこのしきい値とを比較する。Web トラフィックが消費するネットワークの帯域幅が、しきい値を大幅に上回る場合にアノマリーとして検知され、管理者に警報が通知される。

他のプロファイルの例としては、たとえば 1 人のユーザーが送信する電子メールの件数、1 台のホストに対するログインの試みの失敗回数、1 台のホストにおける一定期間内のプロセッサ稼働率のレベルなど、挙動に関するさまざまな属性が考えられる。

振る舞い検知は、未知の脅威の検知に対して非常に有効である。コンピュータが新種のマルウェアに感染した場合、コンピュータリソースの消費量の増加や多数の電子メールの送信、多数のネットワーク接続の開始等、当該コンピュータについて作成済みのプロファイルと大きく異なる動作が生じるため、アノマリーの検知が可能である。

最初のプロファイルは、一定期間(通常数日程度、場合により数週間)を経て生成される。この期間は、トレーニング期間とも呼ばれる。プロファイルの生成は、ほとんどの場合、AI アルゴリズムを使用してシステムおよびネットワークの正常な状態を学習することにより行われる。

振る舞い検知に使用されるプロファイルには、静的プロファイルと動的プロファイルがある。静的プロファイルは、一度生成されたあとはそのまま使用され続け、新しいプロファイ

ルを生成するように明示的に指示されない限り変更されない。一方、動的プロファイルは、システムおよびネットワークの挙動の変化に合わせて変化する。システムおよびネットワークは、時間の経過とともに変化するため、それに応じてシステムおよびネットワークの正常な挙動のベースラインも変化する。そのため、静的プロファイルは、徐々にシステムおよびネットワークの挙動の実態に合わなくなるため、定期的に更新する必要がある。動的プロファイルにはこの問題がない一方、攻撃者による検知回避の試みの影響を受けやすい。たとえば、攻撃者が、悪意のある活動を少量ずつ間隔をおいて実行し、活動の量や頻度を徐々に引き上げていくという攻撃手法をとることがあるが、この変化の速さが十分に緩やかであれば、攻撃が正常な活動であると判断され、検知されない可能性がある。また、最初のプロファイルを構築する期間内に悪意のある活動が行われると、正確なプロファイルを生成することができない可能性もある。

振る舞い検知には、量的解析 （フローベース）と質的解析 （コンテンツベース）の二つの方法がある。以下、それぞれの方法について説明する。

2.1.3.1. 量的解析（フローベース）

ネットワークに接続された機器間でやり取りされるネットワークフローデータのバイト数、新規のネットワーク接続数等を考慮したネットワークフローモデルを構築し、モデルから乖離したネットワークフローを検知した場合にアラートを生成する。

ネットワーク構成の変化に合わせて、自動的にネットワークフローモデルが調整される。

(1) 長所

〇枯れた技術であり、新しい攻撃にも対応可能である。

〇検知精度を向上させるためのチューニングが容易である。

(2) 短所

〇検知対象の脅威の範囲が限定される。具体的には、データ量やネットワーク通信の一時的な増加をもたらす誤動作、DoS 攻撃、水平・垂直（ポート）スキャン、総当たり攻撃等に限定される。

〇誤動作や誤設定、運用上のミス、高度なサイバー攻撃については、ネットワークフローの変化を伴わないため、検知できない。

2.1.3.2. 質的解析（コンテンツベース）

一定の時間、ネットワーク通信やプロトコルメッセージを観測し（学習フェーズ）、観測結果に基づいて通常トラフィックとして期待されるトラフィックを記述するためのネットワーク・プロトコル検知モデルを構築し、このモデルから逸脱したトラフィックを観測した場

合に、アラートを生成する。

(1) 長所

○理論的には、未知のソフトウェア脆弱性を悪用する攻撃を検知することができるが、正規のコマンドを使用した攻撃については、検知モデルからの逸脱がないため、検知できない。

○基本的には、予備知識や設定を必要とせずに導入可能であるが、学習フェーズにおいては、通信プロトコルに関する理解が必要となるケースも多い。製品によっては、通信プロトコルに依存しない形態での学習が可能なものもある。

(2) 短所

○検知の正確性、製品の使いやすさは、使用するアルゴリズムによって左右される。

○機械学習ベースのソリューションは、ノーマルトラフィックモデルを構築するためにクリーンなトラフィックのデータを大量に必要とすることおよび、所望の検知精度を得るためのチューニングが非常に複雑なものとなるため、導入前に準備作業が必要となる、専門家によるチューニング作業を要する等、導入までに一定の時間を要することに留意する必要がある。

○検知精度を維持するために、ネットワークが変更されるたびに、ネットワーク・プロトコル検知モデルの全面的な再構成が必要となる。

2.1.4. サンドボックス型

実環境においてプログラムを実行する前に、sandbox[2] と呼ばれる環境でプログラムを実行し、観測された挙動を、既知のプログラムの挙動を比較することにより、プログラムがマルウェアかどうかを判断する手法。電子メールの添付ファイル、バイナリファイル、pdf ファイル、Office 文書のような疑わしいデータを捕捉し、コントロールされた環境(サンドボックス)においてそれらを実行し、センシティブなプロセス、データ、設定ファイル(Windows Registry)をチェックして、ボットネットクライアントをドロップする等の有害活動を行わないかどうかを検知する。たとえば、管理者権限を取得しようとするプログラムや、システムの実行ファイルを上書きしようとするプログラムは、マルウェアと判断する。

(1) 長所

○バックオフィスネットワークや監視ネットワークにおける検知に適している。

○悪用されるソフトウェア脆弱性が既知のものであるか未知のものであるかに

[2] マルウェアなどの不正なプログラムの挙動を解析することを目的として構築されたコンピューティング環境で、sandbox 内でマルウェアを実行しても、マルウェアによる悪意のある活動が、他のシステムに波及しないよう他の情報システムや本番環境から隔離されている。

よらず、ファイル経由で拡散する高度なマルウェアや脅威の検知に有効である。

○IT システムとの境界付近に設置されている ICS サーバーに対しては、Sandbox による侵入検知が有効である可能性がある。

(2) 短所

○近年、サンドボックス内で実行されていることを感知するマルウェア等、サンドボックスによる検知を回避するマルウェアが増加しているため、サンドボックスを使用する検知システムの検知率が低下する傾向にある。

○正規のプロトコルコマンドを使用する攻撃や、ICS の脆弱性をついた攻撃を検知することはできない。

○検知モデルを構築するための分析に一定の時間を要するため、ICS ネットワークには適していないケースがある。

2.1.5. ステートフルプロトコル解析

ステートフルプロトコル解析は、個々のプロトコル状態に関し、『正常と判断された特定のプロトコルの通信パターン』として定義されたプロファイルと観測されたイベントとを比較して、プロファイルから逸脱した活動を特定するプロセスである。

2.1.3.で前述した振る舞い検知では、ホストやネットワークごとに固有のプロファイルが使用されるのに対し、ステートフルプロトコル解析では、個別のプロトコルがどのように使用されるべきか／使用されるべきではないかを指定した汎用的なプロファイルが使用される。プロファイルは、通常、侵入検知製品ベンダーにより作成される。

ステートフルプロトコル解析の「ステートフル」とは、状態(ステート)の概念を持ったネットワーク、トランスポート、およびアプリケーションプロトコルについて、侵入検知システムがその状態を認識および追跡する能力を備えていることを意味する。

たとえば、FTP(File Transfer Protocol) において、セッションの認証が完了していない状態では、ヘルプ情報の表示やユーザー名・パスワードの指定のような少数のコマンド以外は実行すべきでない。侵入検知システムは、ユーザーによる FTP の認証に対応するレスポンスに含まれるステータスコードを見つけることにより、認証が成功したかどうかを判断する。認証が成功した場合、セッションは認証済み状態に移行し、ユーザーは、任意のコマンドを実行できるようになる。これらのコマンドのほとんどは、セッションが未認証の状態において実行された場合は疑わしいとみなされるが、認証済み状態において実行された場合はほとんどが無害と見なされる。

ステートフルプロトコル解析では、予期していないコマンドシーケンス(同じコマンドが何回も連続して実行されたり、先に実行されるべきコマンドが実行されずに、後続のコマンドだけが実行されたりするなど)を識別することができる。ステートフルプロトコル解析のもう一つの特徴は、認証プロトコルについては、各セッションで使用された認証子を追跡し、疑わしい活動に使用された認証子を記録することができることである。これは、インシデン

トを調査する際に役立つ情報である。侵入検知システムによっては、認証子の情報を使用して、ユーザー種別や特定ユーザーごとに許容される活動を定義できるものもある。

ステートフルプロトコル解析の手法において実行される「プロトコル解析」には、主として、個別コマンドの妥当性チェック(たとえば、引数の長さの最大値と最小値など)が含まれる。あるコマンドが、通常は 1 個のユーザー名を引数とし、ユーザー名の最大長は 20 文字であるのに対して、1,000 文字の引数が指定された場合、そのコマンドの正当性は疑わしいと考えられる。引数にバイナリデータが含まれていれば、よりいっそう疑わしいと判断される。

ステートフルプロトコル解析の短所は、解析の複雑さや、同時に多数のセッションの状態を追跡することで生じるオーバーヘッドにより、リソースの消費がきわめて大きいことである。また、一般的に受容可能なプロトコル動作の特性に反しない形態での攻撃(無害の活動を短時間に多数実行することによる DoS(Denial of Service：サービス妨害)攻撃などを検知できないことも深刻な問題の一つである。さらに、特定のアプリケーションおよびオペレーティングシステムにおいて、特定のバージョンにおけるプロトコルの実装方法と侵入検知システムで使用されるプロトコルモデルに不整合が生じること、あるいは、クライアントおよびサーバーにおけるプロトコル実装の相違により、不正な通信として検出できない通信が生じる可能性があることも問題となる。

(1) 長所

○一連の通信シーケンスが正常なものであるかどうかの判断に基づいて、通常とは異なる(攻撃の可能性がある)コマンドシーケンスを検知することができる。

(2) 短所

○通信シーケンスの解析やセッションの状態を追跡するためのコンピュータリソースの消費が大きい。

○プロトコルモデルとプロトコル実装に相異がある場合に対応できない。

○一般に受容可能なプロトコル動作の特性に反しない攻撃(DoS 攻撃など)を検知できない。

2.2. 検知方法

侵入検知システムにおける検知方法は、NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems(侵入検知および侵入防止システムに関するガイド)等に基づいて分類した。

2.2.1. ネットワーク監視型

特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを

監視し、通信およびアプリケーションの活動を解析して疑わしい活動を特定する。

ネットワーク境界(境界ファイアウォールまたはルータ、VPN サーバー、リモートアクセスサーバー、無線ネットワークなどの近く)に設置される形態が最も一般的である。

ネットワーク監視型の侵入検知システムの設置形態には、インライン型と受動型がある。

2.2.1.1. インライン型

インライン型の侵入検知システムでは、監視対象のネットワークトラフィックが侵入検知センサーを必ず通過するように設置される。侵入検知センサーは、外部ネットワークとの接続部および分離する必要がある個々の内部ネットワークの間の境界など、異なるネットワークを分ける境界部分に置かれる。インライン型の侵入検知システムの設置例を図 2.1 に示す[3]。

インライン型のセンサーは一般に、監視対象のネットワークトラフィックがセンサーを必ず通過するように設置される。具体的には、ファイアウォールおよびその他のネットワークセキュリティ装置が設置される場所、つまり、外部ネットワークとの接続ポイントや分離する必要がある個々の内部ネットワーク間の境界など、異なるネットワークの境界となる部分に設置される。通常、監視するトラフィックの量が少なくなるよう、ネットワークのより安全な側に設置されるが、ネットワーク境界部に設置される装置を保護するために、ネットワークのより安全性の低い側に設置することもできる。

後述の 2.2.1.2 に記載する受動型侵入検知システムとの相違点として、インライン型の場合、侵入検知に加えて、不正と判断されたパケットを遮断できる点が特徴である。

[3] 出所：NIST SP 800-94 侵入検知および侵入防止システムに関するガイド

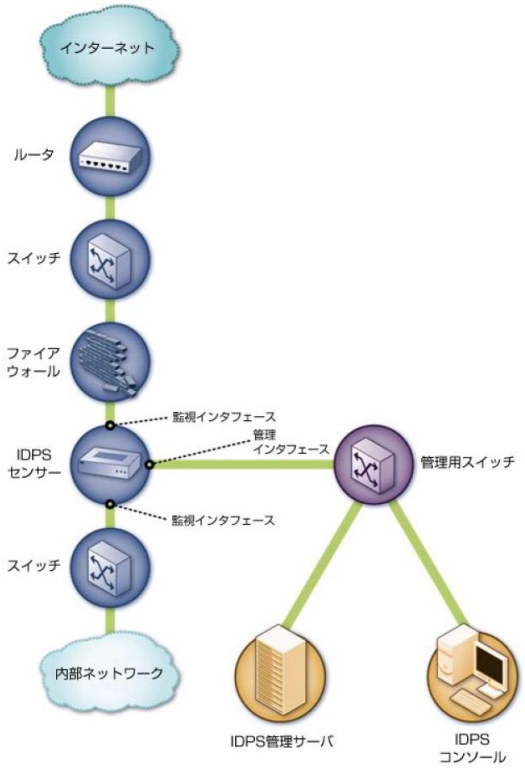

図 2.1 インライン形態のネットワーク監視型侵入検知システムの設置例

2.2.1.2. 受動型

受動型の侵入検知システムでは、侵入検知センサーは、実際のネットワークトラフィックのコピーを監視するような位置に設置される。実際のトラフィックは、侵入検知センサーを通過しない。受動型の侵入検知センサーは一般に、ネットワークの境界部分などのネットワークの主要な場所、および DMZ（Demilitarized Zone：非武装地帯）サブネットでの活動など主要なネットワークセグメントの監視を行うことができるように設置される。

受動型の侵入検知システムの設置例を図 2.2 に示す[4]。

[4] 出所：NIST SP 800-94 侵入検知および侵入防止システムに関するガイド

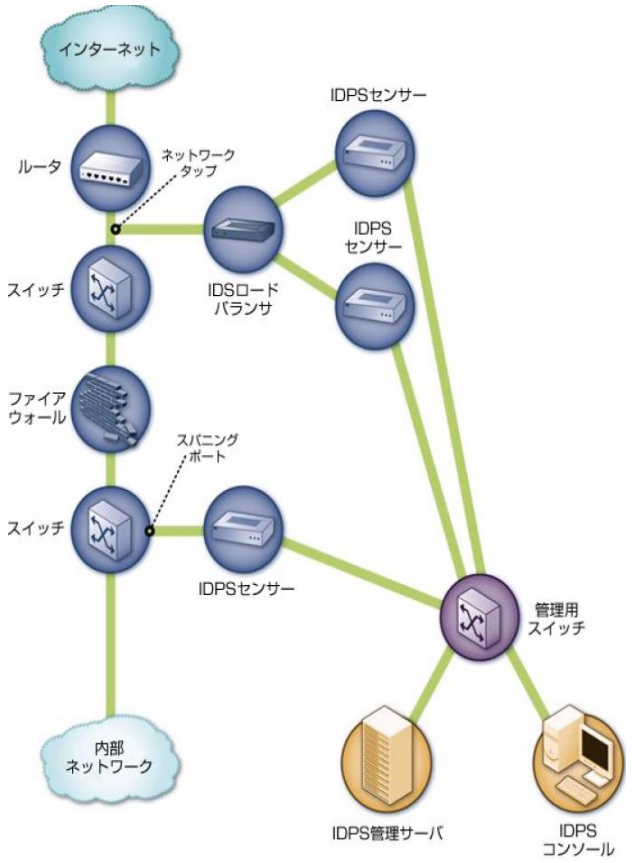

図 2.2 受動形態のネットワーク監視型侵入検知システムの設置例

受動型のセンサーは、実際のネットワークトラフィックではなく、トラフィックのコピーを監視するため、実際のトラフィックは、センサーを通過しない。

受動型のセンサーは一般に、ネットワークの境界部分や、DMZ (Demilitarized Zone：非武装地帯) サブネットでの活動など主要なネットワークセグメントの監視を行うことができるように設置される。

受動型センサーでは、以下のようにさまざまな方法でトラフィックを監視することができる。

2.2.1.2.1. スパニングポートを利用した監視

多くのスイッチは、スイッチを通過するすべてのトラフィックを監視することができるスパニングポートを備えている。スパニングポートにセンサーを接続することにより、多数のホスト間で送受信されるトラフィックを監視することができる。

スパニングポートはネットワークにすでに存在する場合が多い。スイッチに高い負荷(多量のトラフィック)がかかっているとき、そのスパニングポートでトラフィックの一部が見えなくなったり、あるいは、スパニングが一時的に無効にされたりする場合がある。

2.2.1.2.2. ネットワークタップを利用した監視

ネットワークタップは、スイッチやルータを接続するネットワークケーブルの信号を分岐させる装置で、ネットワークタップを使用して、スイッチを通過するトラフィックのコピーをセンサーに分岐させることによりトラフィックを監視することができる。ネットワークタップを設置する際は、ネットワークを一時的に停止する必要がある。また、ネットワークタップに問題が生じた場合にネットワークの停止が必要となる可能性がある。

ネットワークタップは、ネットワークに追加的に設置する必要があるため、新規に購入する必要がある。

2.2.1.2.3. ロードバランサを利用した監視

ロードバランサは、ネットワークトラフィックを集約して侵入検知システムのセンサーなどに送り込む装置である。ロードバランサは、1 つ以上のスパニングポートまたはネットワークタップからネットワークトラフィックのコピーを受け取り、複数の異なるネットワークのトラフィックを集約することができる（2 つのネットワークに分割された通信セッションを元の通信セッションに組み立て直すなど）。ロードバランサは、受信したトラフィックのコピーを、どのトラフィックをどの監視装置に提供するかを規定しルールセットに基づいて、侵入検知センサーを含む 1 つ以上の監視装置に配信する。ルールセットの一般的な設定としては、次のようなものがある。

○すべてのトラフィックを複数の侵入検知センサーに送る。

（高可用性を確保する場合や、同じトラフィック活動を複数の種類のセンサーで並行して解析する場合に使用する。）

○トラフィック量に応じてトラフィックを複数の侵入検知センサーの間で動的に振り分ける。

（一般に、トラフィックの処理とそれに対応する解析によってセンサーが過負荷になるのを防ぐための負荷分散を目的として使用する。）

○IP アドレス、プロトコル、その他の特性に基づいて、トラフィックを複数の侵入検知センサーに振り分ける。

（1 台のセンサーを Web 活動の監視専用にし、もう一台のセンサーにその他のすべての活動を監視させるなど、センサーの負荷分散を目的として行われる。また、トラフィックの振り分けを使用して特定のトラフィック（たとえば、最も重要なホストが関係するトラフィック）をより詳しく解析することもできる。）

トラフィックを複数のセンサーに振り分けることにより生じる問題として、以下のようなものがある。

○複数のステップにより構成される攻撃を検知しようとする場合で、攻撃の各ステップ単体では攻撃とはみなされないが、2 つのステップが順次実行されると悪意のある攻撃であるとみなされる場合、2 台のセンサーがそれぞれ単体の攻撃ステップのみを観測するように設定されているのであれば、このような攻撃が攻撃として検知されない可能性がある。

2.2.2. エージェント型

エージェント型の侵入検知システムでは、監視対象のサーバー、HMI(Human-Machine Interface)、ネットワークスイッチ、コントローラ等のデバイスに「エージェント」と呼ばれる検知用ソフトウェアがインストールされる。各エージェントは、単一のホスト上で行われる通信やアプリケーション等の活動を監視し、アノマリーを検知した場合にアラートを生成する。

エージェント型侵入検知システムが監視するイベントには、以下のようなものがある。

○プログラムの挙動
○システムコール
○アプリケーションおよびライブラリの使用
○ネットワークトラフィック
○ファイルシステムへのアクセス
○OS およびアプリケーションのログ
○ネットワーク設定

侵入検知システムの管理および監視には、管理・監視用コンソールが使用される。

エージェントは、監視対象デバイスに関する外付けメディアの使用、ログインしているユーザー、内向き／外向きのトラフィック、デバイスの設定、プロセス／プログラムの詳細、デバイスのパラメータ(メモリー、ディスク、プロセッサの使用率)等の情報の収集・前処理を行う。収集された情報は、セキュリティが確保された状態で検知エンジンへ送信され、事前に設定されたセキュリティポリシーやベースラインからの乖離が検知された場合に、アラートが生成される。

エージェント型の侵入検知システムの制約条件として、以下のようなものがある。

○チューニングおよびカスタマイズの作業に大きな手間を要する。
○管理サーバーへの警報データ転送をリアルタイムではなく定期的に実行する場合、侵入に対する対応措置の発動に遅れが生じる場合がある。
○インストールされたエージェントの動作によって、既存のアプリケーションの動作に不

具合が発生する可能性がある。

エージェント型の侵入検知システムの設置例を図 2.3 に示す[5]。

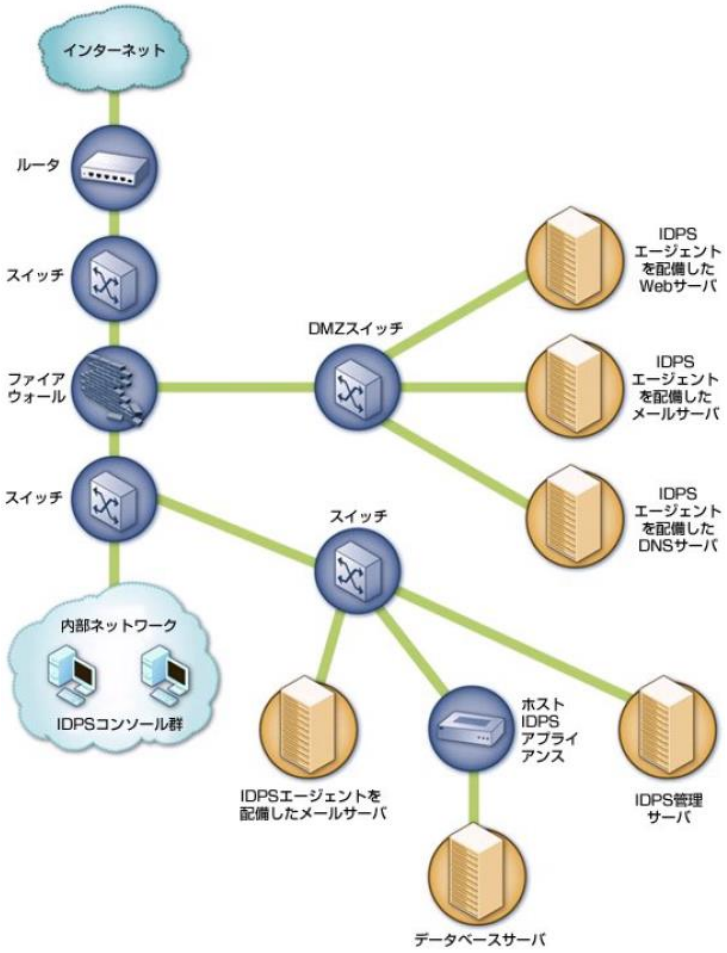

図 2.3 エージェント型の侵入検知システムの設置例

侵入検知エージェントは、通常、一般に公開されているサーバーや、機密性の高い情報が保存されているサーバーなど、組織のシステムの重要な構成要素に導入される。構成要素間の通信は通常、別個の管理ネットワークではなく、既存のネットワークを使用して行われる。必要があれば、システムの重要な構成要素以外のほとんどのサーバー、デスクトップ PC、ノート PC にエージェントを導入することが可能であるが、サポートされていない OS を使用している PC 等が存在する場合は、侵入検知エージェントを実行するための専用のアプライアンスを導入することになる。一般的に、網羅的かつ正確な侵入検知の観点からは、ホストにエージェントをインストールするほうが望ましいが、監視対象ホストにエージェントがインストールされることにより、当該ホストのパフォーマンスが過度に低下する場合は、ホストの負荷を軽減するために、エージェントを実行するためのアプライアンスを導入せざるを得

[5] 出所：NIST SP 800-94 侵入検知および侵入防止システムに関するガイド

ないことがある。

2.2.3. ヒストリアン型

運用に関する時系列データ(Historian)に基づくアノマリー検知手法。監視対象の ICS 関連コンポーネントの時系列データ(コンポーネント間で送受信されるデータやコマンド等)、管理パラメータ等を収集・保存・分析するヒストリアンサーバーが設置される。

一定期間に渡って収集した時系列データに基づいて、データ量の変動や異常なデータの有無等を監視・分析し、通常の運用状態からの乖離(アノマリー)を検知した場合にアラートを生成する。

ヒストリアン型の侵入検知システムの制約条件として、以下のようなものがある。

○ヒストリアンサーバーのデータは、ICS の制御に用いられるケースがあるため、ヒストリアンサーバーのデータが不正に改ざんされることにより侵入検知に影響が生じる可能性がある。ヒストリアンサーバーのデータが改ざんされると、改ざんされたデータに基づいてシステムの制御が行われることになり、検知に使用する時系列データもそれまでのデータと異なるものとなることから、正常な侵入検知ができなくなる可能性がある。

2.3. 侵入検知製品の付加機能 [6]

ICS を対象とする侵入検知製品に装備されているセキュリティ上の付加機能には、以下のようなものがある。特に資産管理機能は、監視対象となる機器の正確な把握や ICS ネットワークの正常な状態における通信の状況等に関するプロファイル(ベースライン)の生成を効率的かつ正確に行う上で非常に有効である。また、フォレンジック分析機能は、インシデント発生後の原因分析や対策の実施に有用である。

2.3.1. 資産管理機能

監視対象の ICS ネットワークを構成する IT 機器および ICS 機器等の資産に関する情報を収集・管理する機能。収集・管理する情報には、機器の種別、機器の接続状況(物理的および論理的)、インストールされている OS やファームウェア、使用する通信プロトコル、製造したベンダーの名称、既知の脆弱性に関する情報等がある。

資産管理機能には、以下のようなものがある。

○接続されている ICS の機器の種類や数の把握および変更があった場合の最新の状態への更新

○インターネットの標準的な通信プロトコルである TCP/IP 以外の通信プロトコルを使

[6] 各種侵入検知製品の資料等に基づく

用する ICS 機器の把握

○機器の資産のベンダー名、製品名、OS のバージョン、ファームウェアに関する情報、使用する通信プロトコル、IP アドレス、脆弱性情報

○資産のグループ化

○論理ネットワークの可視化

○機器の接続関係やサブネット単位での設定状況による物理ネットワークの可視化

○監視対象の ICS 機器の見える化：資産の一覧およびプロパティの表示

（収集した資産情報をダッシュボードなどで分かりやすく表示する。）

2.3.2. 脆弱性診断機能

ICS および ICS ネットワークを構成するネットワークおよびデバイスの脆弱性を自動的に検出し、収集する。収集する脆弱性には、許可されていないリモートアクセス接続、不正な（無許可の）デバイス、セキュリティ的に弱い認証、パッチ未適用の機器、安全ではない通信プロトコルの使用、サブネット間の許可されていないブリッジ、弱いファイアウォールなどが含まれる。収集した脆弱性に関する情報に基づいて、最新の CVE(Common Vulnerability Exposure)データとの比較を行い、システム・ネットワークの脆弱性の特定を行う機能や、脆弱性に関するレポートを作成する機能を有する製品もある。

2.3.3. 攻撃経路予測機能

収集した資産および脆弱性に関する情報と最新のサイバー攻撃に関する情報に基づいて、システム・ネットワーク内において最も狙われやすい機器を特定する機能、発生リスクの高い攻撃経路を予測する機能。AI を使用して、システム・ネットワークを構成するすべての機器の脆弱性とそれに対応するリスクを特定・分析し、攻撃者による攻撃が想定されるパスのうち、最も可能性の高いパスを特定する。

2.3.4. モニタリング・他のデバイスとの通信状況の可視化機能

監視対象のシステム・ネットワークを構成する IT 機器および ICS 機器間でやり取りされるパケットをモニタリングおよびキャプチャし、機器に関する情報、機器間におけるデータフロー、通信リンク、使用される通信プロトコルやポート、宛先 IP アドレス、機器の制御に使用されるパラメータ値等を収集し、収集した情報に基づいて、機器間での通信の状況を可視化する(グラフ・レポートを作成する)機能。システム・ネットワークの変化に合わせて自動的にアップデートする機能もある。

2.3.5. フォレンジック分析機能

インシデントが発生した場合にその発生原因や発生に至るまでの関連するイベントの特定等を行うための機能。通信ログや機器の操作ログ等の時系列データに基づいてイベントの相関を明確化し、どのような経緯で最終的なインシデントに至ったのかを明らかにする機能

である。インシデントの原因の特定から是正処置の実施まで、正確かつ尽速なインシデント対応を行うために有効な機能である。侵入検知製品に付属している場合と、フォレンジックツール専門のベンダーが提供するフォレンジックツールがあるが、実際に使用するにあたっては、ある程度の知識と経験が求められる。

2.3.6. パケットキャプチャ・保存機能

システム・ネットワークを構成する IT 機器および ICS 機器間でやり取りされるデータやコマンド等を記録・保存する機能。主としてインシデント発生時のフォレンジック分析において使用される。データの保存には、大容量のストレージが必要となるため、どの程度の期間に渡ってデータを保存するのかについては、組織ごとに判断されることになる。

2.3.7. コンプライアンス監査機能

各種法規制要件への準拠を目的として、複数の拠点を横断したガバナンス管理[7]のための監視および監視結果に関するレポートを自動的に作成したり、セキュリティポリシーに違反している機器の詳細や対応方法を自動的に提示したりする機能。たとえば、IEC 62443[8] におけるゾーン設計ポリシーに対する違反[9]を検出して、アラートを生成・通知するといった機能である。

2.3.8. 他社ネットワーク機器・SIEM 連携機能

他社製のシステム・ネットワーク機器との API による連携により、異常を検知した場合に該当する機器の特定から対応実施までの自動制御を行ったり、SIEM(Security Information and Event Management)機器との連携により、複数機器にまたがるイベントの相関を特定したりする機能。機器の通信・操作ログ(Syslog)や検知アラートのログを他社が提供する分析ツールに提供する機能を有する製品もある。

2.3.9. 管理コンソール機能

侵入検知システムを同一拠点内で複数台設置する場合や、複数拠点に複数台設置する場合の管理を行うための管理コンソール機能。リカバリに必要なすべての設定ファイルを定期的に受信するバックアップ管理機能を有する製品もある。

また、過去の通信ログ(IP アドレス、MAC アドレス、ポート、プロトコル固有の特定の機能コード、プロトコルサービス、モジュールなどに基づくクエリなど)をもとに、トラフィック履歴の詳細検索機能を有する製品もある。

---

[7] たとえば、NIST サイバーセキュリティフレームワークに基づく識別・防御への対応、IEC 62443-3-3 への遵守状況の確認等

[8] IEC : International Electrotechnical Commission(国際電気標準会議)が規定する制御システムのセキュリティに関する国際規格

[9] 具体的には、物理的または論理的なセグメンテーションの実装に関するポリシー違反を自動的にコンテクスト化し、対応の優先度をスコア付けする等

Appendix. ドイツの政府系サイバーセキュリティ機関であるBSIの ICS におけるアノマリー検知に関するガイドライン

ICS における侵入検知に関連して、ドイツの政府系サイバーセキュリティ機関である BSI が公開している『ICS におけるアノマリー[10] 検知に関するガイドライン[11]』がある。本ガイドラインは、技術的に整理されており、ICS における侵入検知の一助になると考えられるため、参考情報として記載する。

A.1. アノマリーの具体的な例

A.1.1. ネットワークにおける通常とは異なる、あるいは、異常なアクティビティ

ネットワークにおける通常とは異なる、あるいは、異常なアクティビティには、以下のようなものがある。

○新規デバイスの接続 : 新規のデバイスの接続が行われていないかどうかを監視し、許可されていない新規のデバイスが接続されていた場合にアノマリーと判断し通知する。
○未知のデバイスからのデータパケット
○以前に通信がないデバイス間でのデータ転送
○以前に使用されたことがないプロトコルによるデータ転送
○通常は使用されたことがないプロトコル、あるいは、目的外で使用されたプロトコルによるデータ転送
○通常は発生しない時間に発生したイベント
○想定外の IP アドレスの使用(パブリック IP アドレス等)
○アドレススキャンやポートスキャン等、一般的に注意すべきイベント
○ネットワークの高利用率、データパケットの往復に要する時間の増加、TCP ウインドウサイズの減少

A.1.2. 実運用環境のログに記録された異常なイベント

実運用環境のログに記録された異常なイベントには、以下のようなものがある。

○通常は発生しないエラーメッセージ
○サポートされていないファンクションコールや使用されたことがないファンクションコール
○偽造されたデータパケット

[10] BSI の文書におけるアノマリーの定義：規定されたルールや通常の運用状態からの逸脱
[11] https://www.bsi.bund.de/EN/Topics/Industry_CI/ICS/recommendations/ICS-Operators/recommendations-operators.html

○未知のファンクションコード
○異常なプロトコル動作
○プロトコル間での想定外の遷移

A.1.3. 通常とは異なるプロセスデータ(センサーデータ、コントロールデータ等)の変化

通常とは異なるプロセスデータ(センサーデータ、コントロールデータ等)の変化には、以下のようなものがある。

○規定された範囲外のデータ値
○頻度の変化
○周期の変化
○一定時間内での変動の変化

A.2. アノマリー検知システムに必要な機能に関する要件

A.2.1. 一般的な要件

一般的な要件には、以下のようなものがある。

○ネットワーク内で通信する全てのデバイスの概要
○ネットワークで使用される全てのプロトコルの明確化
○ネットワーク内の全ての通信リンクの明確化
○ネットワークの通信負荷(データ量、通信時間等)の監視
○検知基準の設定
○エスカレーションレベルの規定
○わかりやすい視覚化方法：イベントの通知・表示、イベントの相関の表示
○既存の信号・通知・アラームシステムとの統合のサポート
○スケーラビリティ(追加のストレージのサポート等)
○統計データの収集
○外部システムによる詳細解析のためのエクスポート機能
○内部ログ取得機能

A.2.2. 通常とは異なる、あるいは、異常なネットワークアクティビティに関する要件

通常とは異なる、あるいは、異常なネットワークアクティビティに関する要件には、以下のようなものがある。

【基本的な要件】

○ICS ネットワーク内の新規デバイスの特定
○以前に通信がなかったデバイス間での通信の特定
○以前に使用されたことがない TCP/UDP ポートを使用した通信の特定
○コンポーネント間における新たなプロトコルの特定、プロトコルの変更の特定
○セキュアではないネットワークへの接続の特定
○セキュアではない通信属性(暗号化していない等)の特定

【追加的な要件】
○データ量やデータ頻度の変動の特定
○通常とは異なるアクティビティの表示
○ドリルダウン等による詳細表示
○検知されたアノマリーとの関連や想定されるリスクのアセスメント

A.2.3. 実運用環境のログにおいて典型的な異常なイベントに関する要件

実運用環境のログにおいて典型的な異常なイベントに関する要件には、以下のようなものがある。

○以下のようなエラーメッセージの特定
・無効な、あるいは、サポートされていないファンクションコール
・無効なアドレス、あるいは、宛先
○利用不能・到達不能なアドレス・宛先(試行タイムアウト)
○以前に使用されたことがない ICS 特有の機能コードの特定
○ICS のログのフォーマットエラーの特定
○デバイスが通常使用しないアドレスに対するアクセス試行が適切かどうかを判断する能力

A.2.4. プロセスデータ(センサーデータ、制御データ)の通常とは異なる変化に関する要件

プロセスデータ(センサーデータ、制御データ)の通常とは異なる変化に関する要件には、以下のようなものがある。

○規定された値の範囲内での変動
○頻度の変化
○時間の経過に伴う挙動の変化
○一定の値の範囲内での傾向の変化

3. 侵入検知技術の利用動向調査結果

実際に侵入検知製品をビルシステムに適用している不動産・ビル業界の 2 事業者、重要インフラの各種システムに適用している運輸・交通業界の 4 事業者、石油精製プラントの制御システムに適用しているエネルギー業界の 1 事業者の計 7 事業者に対してヒアリング調査を行い、侵入検知技術の実際の使われ方を把握し、利用形態や参考になるポイント等を取りまとめた。また不動産・ビル業界の 1 事業者、運輸・交通業界の 1 事業者の計 2 事業者に対しては、利用動向調査を踏まえ、追加の情報収集を実施し、その内容についても併せて取りまとめた。

表 3.1 に、利用動向調査の調査実施日を示す。

表 3.1 利用動向調査の調査実施日

対象事業者	調査実施日
不動産・ビル業界 A 社	2021 年 11 月 11 日、2022 年 2 月 24 日
不動産・ビル業界 B 社	2021 年 11 月 10 日
運輸・交通業界 C 社	2021 年 12 月 20 日
運輸・交通業界 D 社	2022 年 1 月 7 日
運輸・交通業界 E 社	2022 年 1 月 31 日
運輸・交通業界 F 社	2022 年 2 月 10 日、2022 年 2 月 22 日
石油・エネルギー業界 G 社	2022 年 4 月 26 日

3.1. 不動産･ビル業界の調査結果から参考になるポイント

不動産・ビル業界では、実際に侵入検知製品をビルシステムに適用している 2 事業者にヒアリング調査を実施した。以下、不動産・ビル業界の調査結果から参考になるポイントをそれぞれの観点ごとに記載する。

3.1.1. 侵入検知製品の利用概要

利用概要では、システムの構成、侵入検知製品の適用範囲、採用している侵入検知製品技術、採用している侵入検知製品の付加機能、侵入検知製品と既存のセキュリティ対策技術の組み合わせの観点に沿い、参考になるポイントを記載する。

3.1.1.1. システムの構成

一般的なビルシステムの制御システム構成を図 3.1 に示す。今回の利用動向調査で収集した事例における、侵入検知製品の適用範囲を赤枠で示す。

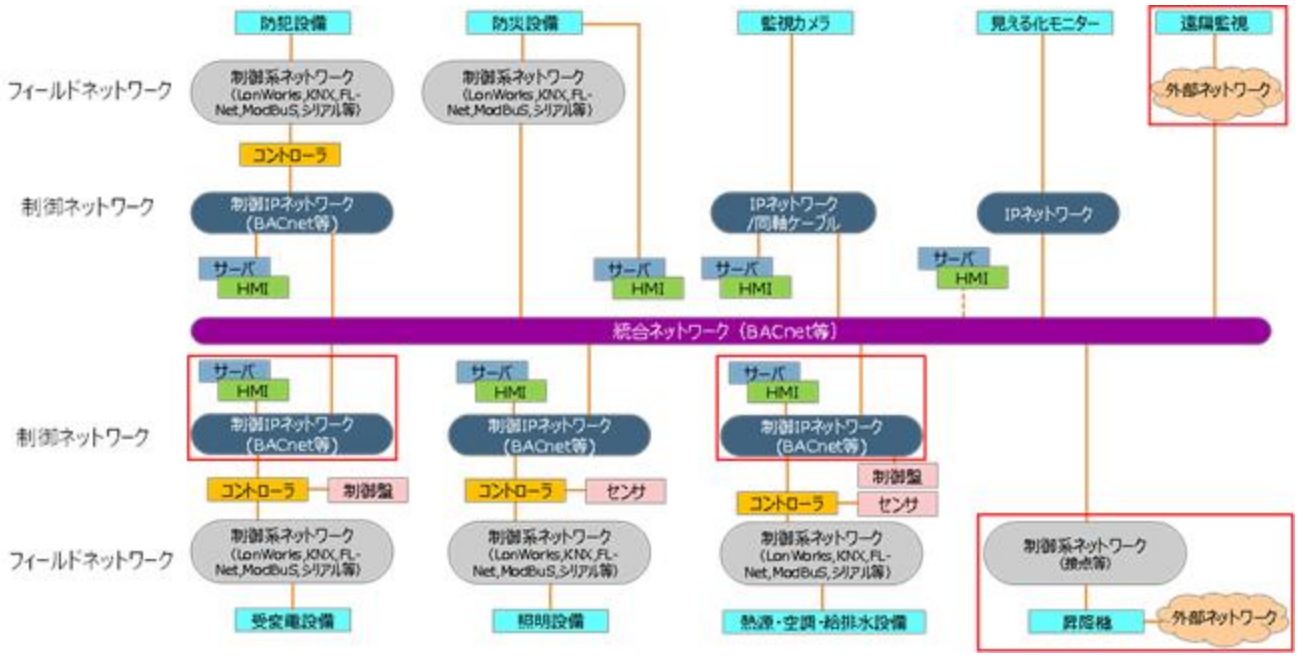

図 3.1 一般的なビルシステムの制御システム構成

制御システムのネットワークはフィールドネットワークと制御ネットワークと統合ネットワークから構成される。

一般的なビルシステムの制御システム構成を、IPA の「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」と照らし合わせると、フィールドネットワークが制御ネットワーク（フィールド側）[12]に概ね対応し、制御ネットワークと統合ネットワークが制御ネットワーク（情報側）[13]に概ね対応する。

各ネットワークには、ビルによって差があるが、①数万単位のコントローラ、②数千～数万単位の PLC、③百程度の DCS、④百程度のサーバー、HMI が接続されている。

3.1.1.2. 侵入検知製品の適用範囲

侵入検知製品の適用範囲は、主に①インターネット等の外部ネットワークと接続している境界、②熱源・空調・給排水設備の制御 IP ネットワークの HMI 周辺、③受変電設備の制御 IP ネットワークの HMI 周辺に設定される。システム上の侵入検知製品の適用範囲は図 3.1 の一般的なビルシステムの制御システム構成図で示すと図中の赤枠部分となる。

インターネット等の外部ネットワークと接続している境界に侵入検知製品を導入している理由は、不動産・ビルの制御システムは、外部との出入口は IT の領域に 1 つのみである

12 「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」の制御ネットワーク（フィールド側）

13 「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」の制御ネットワーク（情報側）

ことから、その出入口に侵入検知製品を導入している。

熱源・空調・給排水設備の制御 IP ネットワークの HMI 周辺、及び受変電設備の制御 IP ネットワークの HMI 周辺に侵入検知製品を導入している理由は、不動産・ビルの制御システムのうち、熱源・空調・給排水設備と受変電設備は特に重要なインフラ設備の為、侵入等の検知、監視を重点的に行うべきだと判断し実施している。

尚、現在のビルシステムでは、監視サービスをテナントに提供するためにインターネットに接続している程度であり、OA システムも繋がってはいない。しかし、最近のハイスペックビルでは、クラウド管理のものも増えており、テナント側が使う監視以外のサービスも増えると考えられることから、インターネットに接続するビルが増えていく可能性があると考えられる。

監視しているデータは、各侵入検知製品によって異なるが、①操作データ、②指示データ、③稼働データ、④制御信号、⑤送信されるデータ等のネットワークを通るデータ（パケットのヘッダ情報を含む）全てである。

3.1.1.3. 採用している侵入検知製品技術

採用している侵入検知製品技術は、今回の利用動向調査では以下の事例が挙げられた。

(1) 振る舞い検知型で、機械学習機能を搭載している製品を採用している場合。
この場合の機械学習機能は、チューニングの際に機能するだけではなく、運用期間中も機能し、ロジックを高度化している。

(2) 一般的な振る舞い検知型の製品を採用している場合。
侵入検知製品で検知に用いるデータは、ネットワーク監視型で取得している。

3.1.1.4. 採用している侵入検知製品の付加機能

採用している侵入検知製品の付加機能のうち、主に①資産管理機能、②SIEM 連携機能、③レポート機能が利用されている。侵入検知製品によっては、資産管理機能でパケットキャプチャを実施することで、自動で IP アドレスを吸い上げ、リスト化する機能も搭載している。

3.1.1.5. 侵入検知製品と既存のセキュリティ対策技術の組み合わせ

すべてのビルが侵入検知製品と既存のセキュリティ対策技術を意図的に組み合わせて利用することを念頭においているわけではないが、侵入検知製品と既存のセキュリティ対策技術を組み合わせている場合、既存のファイアウォールや、不正操作の検知等のセキュリティ対策技術についても、侵入検知製品側で一元管理することで、アラート監視等を効率的に実施している。

3.1.2. 導入にあたって参考となる事例

導入にあたって参考となる事例として、導入に至った背景、導入に向けた検討、チューニング、試用期間の観点に沿い、参考になるポイントを記載する。

3.1.2.1. 導入に至った背景

導入に至った背景は、ビルシステム全体のセキュリティ強化を目的とした検討の中で、ビルシステムの OT 分野のセキュリティの成熟度が十分でないことから、侵入検知製品が議題に上がり、試験的に導入することで侵入検知製品の効果や、ビルシステムへの必要性を検討することが挙げられた。

3.1.2.2. 導入に向けた検討

導入に向けた検討として、社内のセキュリティに関する部署や外部専門家と連携しつつ、製品比較を実施した。その際、カタログ情報等の公開情報の比較検討だけではなく、ビル管理の現場担当者の意見を収集し、システムに影響がないか、監視や運用を委託できるか、侵入が検知されてアラートが鳴った際にどのようなコミュニケーションが必要になるのか、どのような支援・運用体制によるサポートを受けられるのか、IT やセキュリティのプロではないビル管理の現場担当者と円滑なコミュニケーションが取れるか、資産管理の機能を搭載しているか、どのような脅威を検知できるか等、社内のステークホルダーにとって重要な観点を明らかにした上で、それらの情報について、重点を置いて選定を実施した。

3.1.2.3. チューニング、試用期間

チューニング、試用期間は、今回の利用動向調査では以下 2 つの事例が挙げられた。

尚、チューニング、試用期間に必要な期間は侵入検知製品によって異なった。更に、侵入検知製品によっては運用開始後、半年に 1 回程度、アラートの内容を調整する等のチューニングの機会を設けていた。

(1) チューニングを自動で行い、導入した導入事業者の負担なく試用期間を設けることが出来る場合。

(2) 対象ビルにとって必要なアラートを判断するために侵入検知製品ベンダーとコミュニケーションを取りながらチューニング、試用期間を設ける場合。

チューニングを実施するために、事前に侵入検知製品ベンダーと協議を行い、まずデータ収集のために 1 ヶ月の試用期間を設けたが、ビルシステムの特性上、1 ヶ月の試用期間では十分ではなかった。理由として、気温変化等から、それまでになかった制御が生じる為、全ての季節を跨る 1 年程度のデータが必要であった。実際は導入後、運用が始まってからもアラートが頻繁に挙がり、その都度侵入検知製品ベンダーと連携しながら検討を重ね、設定の調整等のチューニングを実施することとなってしまった。

加えて、チューニングを実施する際、自社内の既存の制御システムに関わる人材に加え、IT 系の人材を追加で配置したが、IT 系の人材は制御システムの知見を十分保有していないため、制御システム側の人材と IT 系の人材の連携が容易ではないことから負担が大きくなったことも明らかになった。

3.1.3. 運用にあたって参考となる事例

運用にあたって参考となる事例では、侵入検知製品の運用・監視体制、侵入を検知した際の対処方策、運用時のメリット・デメリット、明らかになった課題、今後のセキュリティに関する展望等の観点に沿い、参考になるポイントを記載する。

3.1.3.1. 侵入検知製品の運用・監視体制

侵入検知製品の運用・監視体制は、今回の利用動向調査では以下の事例が挙げられた。

(1) 運用・監視も含めて侵入検知製品ベンダーに依頼している場合。

アラートが鳴った際、侵入検知製品ベンダーがビル管理の現場担当者にアラートの内容を通知し、その連絡を受けて、ビル管理の現場担当者がアラートの対象設備の制御ベンダー（もしくは設備ベンダー）に連絡し、対応を依頼する運用となっている。この際、ビル管理の現場担当者や制御ベンダーは、IT やセキュリティの知識が豊富でなくとも、適切な対応が出来るような説明やコミュニケーションを侵入検知製品ベンダーに依頼している。

本事例では、課題として、侵入検知製品ベンダーから連絡を受けるビル管理の現場担当者には、制御システムに関する知見だけではなく、IT に関する知見を保有させることが重要だが、人材育成は容易ではなく、当該侵入検知製品に関する知見と、制御システムや実際の運用に関わる知見の双方を保有している人材は自社内に存在しないことが明らかとなった。そのため、社内の制御システムの知見と、侵入検知製品ベンダーの IT に関する知見を連携させ、運用を実施することが重要であった。

(2) ビル管理の現場担当者側で実施している場合。

アラートが鳴った際、ビル管理の現場担当者がアラートの対象設備の制御ベンダーに連絡し、対応を依頼する運用となっている。また、侵入検知製品を導入したことにより、アラートが鳴った際は対応の依頼を行うことについて、事前にビル管理側から制御ベンダーに説明を実施している。

3.1.3.2. 侵入を検知した際の対処方策

侵入を検知した際の対処方策は、前述した通り、どこかの段階ではビル管理の現場担当者が対応しなくてはいけないことから、侵入が検知され、アラートが鳴った際に、各アラートが何を示しているのか、どのような対応を実施すべきなのか等を記載したマニュアルを作成している。マニュアル作成は、チューニング、試用期間後にアラートが適切に作動するよう

に設定が完了した後に作成する場合が多く、作成には約１ヶ月程度を要する。加えて、ビルによっては、マニュアルの作成だけではなく、ビル管理の現場担当者に向けて、侵入が検知され、アラートが鳴った際の手順の確認をする演習型の研修を定期的に実施するガイドラインも策定している。

3.1.3.3.　運用時のメリット・デメリット

運用時のメリットは、主に侵入検知製品が侵入を正しく検知し、アラートが鳴ることで、検知やアラートについての知見が得られただけではなく、実際にサイバーインシデントが発生した際の業務フローの検討も実施できた。このように、侵入検知製品としてのメリットに限らず、ビル全体としてのセキュリティ対策の検討に資する情報、知見を得られることを実感したことも挙げられた。

一方、運用時のデメリットは、主に対象ビルにとって必要なアラートを判断するために侵入検知製品ベンダーとコミュニケーションを取りながらチューニング、試用期間を設ける侵入検知製品の場合、侵入を正しく検知していることで、当初のビル管理側の想定よりも多様なアラートが頻繁に鳴り、その対応に工数が割かれた。しかし、アラートの内容と頻度については調整が可能であり、又、制御ベンダーによる保守メンテナンスの際の接続等も検知してアラートが鳴るため、今後重大な侵入が発生した際でも正しく検知し、アラートが鳴るという安心感に繋がっているとも言えるとの声が有った。

3.1.3.4.　明らかになった課題

侵入検知技術について明らかになった課題は、現状、ビルシステムのネットワークは、インターネット経由で外部と接続している境界も限られていることから、重大な侵入も頻繁に起きるわけではないため、侵入検知製品の機能を十分に活用することができずにコストに見合わないのではないかという内部の議論が起きることが挙げられる。インターネットに接続していないビルもあり、すべてのビルにお金をかけて導入するかも課題と言える。

今後ビルシステムがクラウド化され、外部との接続が増えれば変わるかもしれないが、現状、ビルシステムのネットワークは外部との接続を限定していることから、侵入検知製品を試験的に導入後に、IT のセキュリティ対策として侵入検知製品を導入することが適切か、他のセキュリティ対策で十分かどうか含めて検討の必要性がある。

3.1.3.5.　今後のセキュリティに関する展望等

今後のセキュリティに関する展望等は、将来的にビルのシステムがクラウドに移行し、複数のビルを一括で管理、監視、運営する場合、その管理体制をどのように保有するかが検討課題となっている。この課題に対し、マニュアルの整備やサイバーインシデントに対応する演習を通して、ビル管理の現場担当者を育成するだけではなく、制御ベンダーに対しても同様のマニュアルの作成、サイバーインシデントに対応する演習の共同実施等も視野に入れて検討を進める必要があるとしている。

3.2. 運輸・交通業界の調査結果から参考になるポイント

運輸・交通業界では、実際に侵入検知製品を運輸・交通の制御システムに適用している 2 社と、不正な端末の接続検知製品[14]・不正なソフトウェア検知製品[15]を運輸・交通の制御システムに適用している 2 事業者に対し、ヒアリングによる利用動向調査を実施した。以下、運輸・交通業界の調査結果から参考になるポイントをそれぞれの観点ごとに記載する。

不正な端末の接続検知製品と不正なソフトウェア検知製品は、一般的には侵入検知製品に分類されないが、不正な端末の接続検知製品はネットワーク型の侵入検知技術の一部、不正なソフトウェア検知製品はエージェント型（ホスト型）の侵入検知技術の一部ととらえて、この報告書にまとめている。

3.2.1. 侵入検知製品、不正な端末の接続検知製品・不正なソフトウェア検知製品の利用概要

利用概要では、システムの構成、侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品の適用範囲、採用している侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品技術、採用している侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品の付加機能、侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品と既存のセキュリティ対策技術の組み合わせの観点に沿い、参考になるポイントを記載する。

3.2.1.1. システムの構成

一般的な運輸・交通システムのシステム構成を図 3.2 及び図 3.3 に示す。図 3.2 は一般的な旅客案内のシステム構成を示すシステム構成図である。図 3.3 は、一般的な運行管理・電力管理制御システム構成を示すシステム構成図である。

14 不正な端末の接続検知製品：ネットワークに参加している端末がホワイトリスト（IP アドレス、MAC アドレス、ホスト名等の組合せ）にない場合、不正端末として検知する機能を持つ。不正な端末の接続検知製品には、ネットワーク機器と連携し、不正端末の通信を遮断する機能や通信を妨害する機能を備えるものもある。

15 不正なソフトウェア検知製品：不正なソフトウェア検知製品は様々な形態があるが、本書のヒアリング事業者ではアプリケーションホワイトリストを利用していた。アプリケーションホワイトリストは、事前にホワイトリストとするプログラム（実行プログラムやライブラリ）以外の実行された場合に、実行を禁止ないし警告を出す機能を備える。ホワイトリストは、プログラムのハッシュ値、プログラムのコード署名、ファイル名等が用いられる。

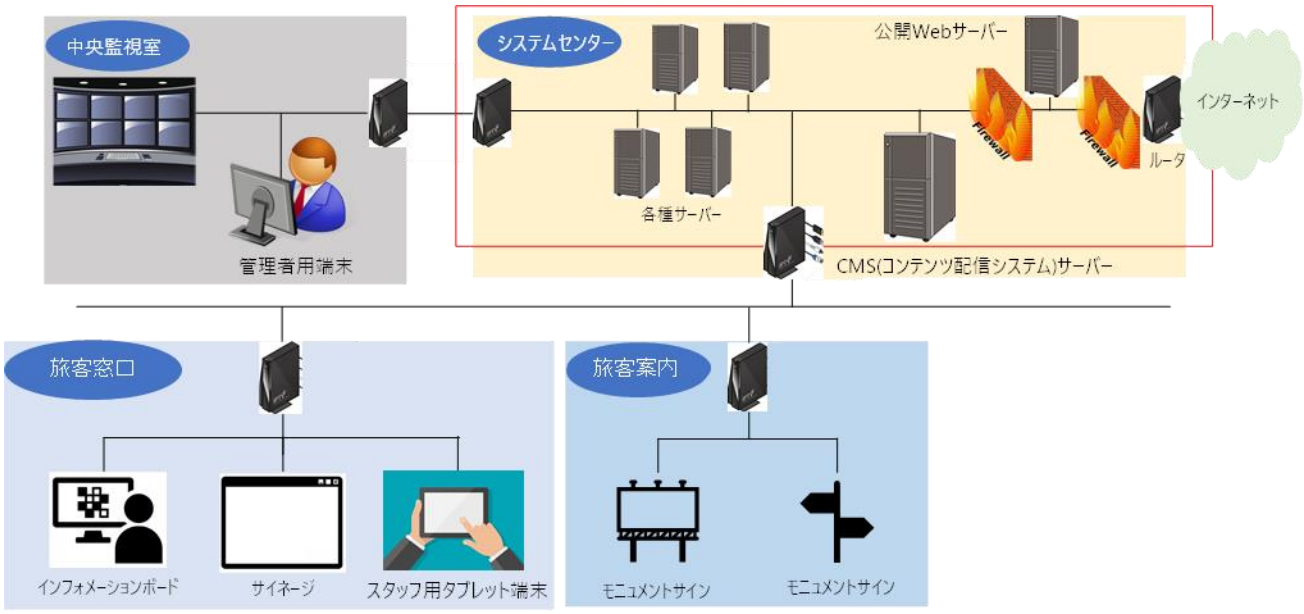

図 3.2 運輸・交通における一般的な旅客案内システム構成

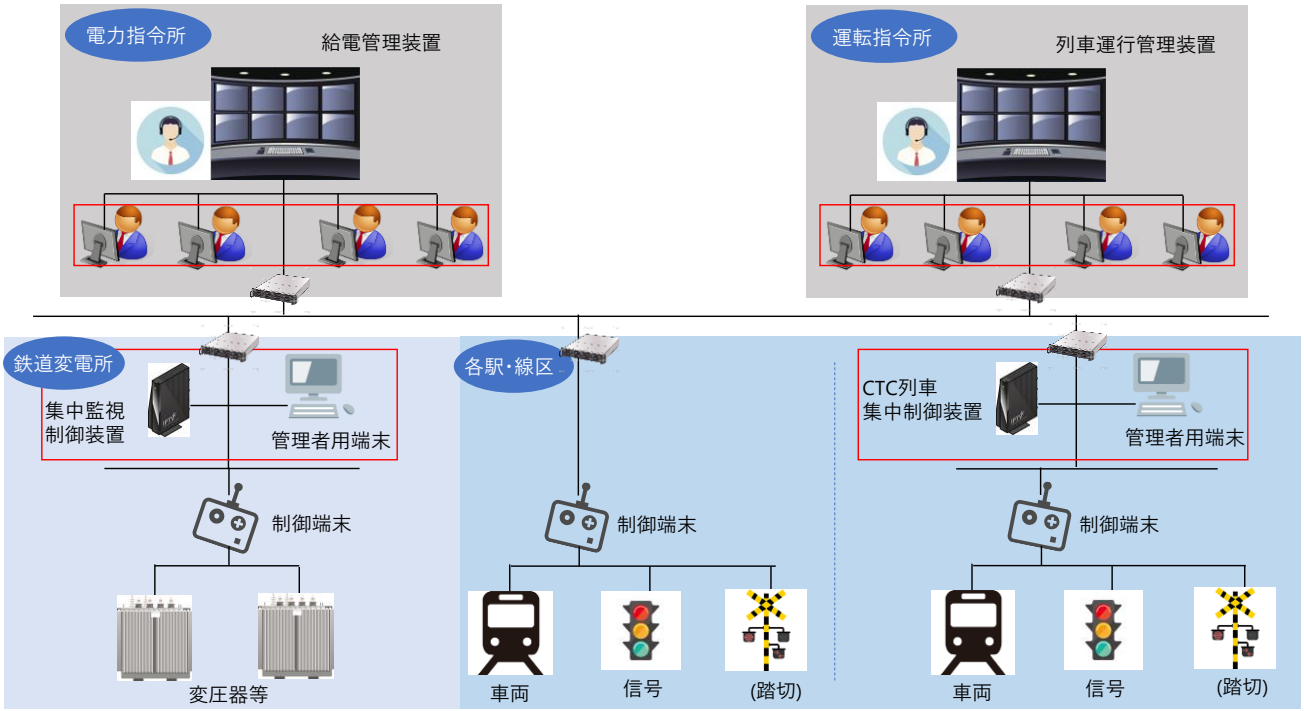

図 3.3 運輸・交通における一般的な運行管理・電力管理制御システム構成

制御システムのネットワークは、制御システムと中央監視室とシステムセンターで構成、もしくは制御システムを所管している部署ごとに分けて構成している。

この制御システムのネットワークは、IPA の「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」の制御ネットワーク（フィールド側）、制御ネットワーク（情報側）を合わせたものに概ね対応する。

3.2.1.2. 侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品の適用範囲

侵入検知製品、不正な端末の接続検知製品・不正なソフトウェア検知製品の適用範囲は、今回の利用動向調査では以下の事例が挙げられた。システム上の侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品の適用範囲は、図 3.2 及び図 3.3 の赤枠部分である。

(1) 侵入検知製品を侵入検知が必要な範囲に適用している場合。

○外部に公開しているウェブサイトのファイアウォールの周辺や、職員が利用する端末が集約される WAN とサーバーの間等、IT と OT 間の検知が必要と考えられる範囲に導入している。

○お客様が利用する予約センター等の企業と個人間の取引(B2C)ネットワークの境界付近や、サプライチェーンの観点から、他社のシステム間の接続を行う企業間取引(B2B)のネットワークの境界付近等、検知が必要と考えられる範囲に導入している。

(2) 不正な端末の接続検知製品・不正なソフトウェア検知製品をデータが集約されるネットワークに適用している場合。

○効率的に不正な端末検知を実施するために、データが集約される管理者用監視端末やその通信を集約している管理端末が接続しているネットワークに導入している。

集中制御や管理を行っている範囲に導入している理由は、適用範囲を決定する際、侵入口として考えられる範囲のうち、担当部署等が責任を持って管理者等を設け、管理・監視できる範囲に限定することとしたことに依るとのことであった。すなわち、制御システムのネットワークにおいて、管理者が設けられていない範囲も多く存在するが、その範囲に不正な端末の接続検知製品・不正なソフトウェア検知製品を導入したとしても、適切な運用を実施することが難しく、十分な効果が得られないと考え、不正な端末の接続検知製品・不正なソフトウェア検知製品の適用範囲から外すこととした。

また既存の適用範囲からネットワーク上の管理者用監視端末やその通信を集約している管理端末に導入範囲を広げる、もしくは現場のネットワーク上のパケットを活用して解析をする製品等をネットワーク上の管理端末に導入し、適用範囲を広げることについては、制御システム側のポリシーの可用性重視、既存のシステムを優先する考え方に合わないため、現状難しいと考えている。あくまで既存の通常業務を阻害しない範囲でのセキュリティ対策の実施を目指しているとのことであった。

それぞれの事例において、監視しているデータを以下に示す。

(1) 侵入検知製品を侵入検知が必要な範囲に適用している場合。

○外部に公開しているウェブサイトは、外部からの公開ウェブサーバーへの通信を監視している。職員が利用する端末が集約される WAN(Wide Area Network)とサーバーの間は、WAN に流れる全てのデータを見ている。このデータは、かなりの通信量になるため、通信量に応じた侵入検知製品を増大して導入している。WAN の構成上にもよるが、冗長

化のために複数台導入する等の対策を実施している。

○お客様が利用する予約センター等の B2C ネットワークの境界付近、サプライチェーンの観点から、他社のシステム間の接続を行う B2B のネットワークの境界付近のすべてのトラフィックデータを監視している。

サプライチェーンの観点から、他社のシステム間の接続を行う B2B のネットワークでは、情報連携先の企業がウイルスに感染していないか、安全かどうかは保障できないため、通信の際に侵入されないように監視している。具体的には、通信に証明書を活用して相互認証を行い、その上で振る舞い等を監視している。

(2) 不正な端末の接続検知製品・不正なソフトウェア検知製品をデータが集約される集中監視制御装置や、管理者用監視端末やその通信を集約している管理端末に適用している場合。

○ネットワークに接続される端末の MAC アドレスと IP アドレスを監視している。

○データを監視せずに、起動されるアプリケーションを監視している。

3.2.1.3. 採用している侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品技術

採用している侵入検知製品技術、もしくは不正な端末の接続検知製品技術・不正なソフトウェア検知製品技術は、今回の利用動向調査では以下の事例が挙げられた。

(1) シグネチャー、ルール、振る舞い検知、サンドボックスでも検知できる製品を採用している場合。

○外部に公開しているウェブサイトで採用している。

○侵入検知製品で検知に用いるデータは、ネットワーク監視型で取得している。

(2) 次世代型のファイアウォールで、シグネチャー、ルール、振る舞い検知、サンドボックスでも検知できる製品を採用している場合。

○職員が利用する端末とサーバーの間で採用している。

○侵入検知製品で検知に用いるデータは、ネットワーク監視型で取得している。

○侵入検知製品を導入している端末には、侵入検知製品を提供しているベンダーのウイルス対策ソフトを導入しており、侵入検知製品とウイルス対策ソフトが連携することで、境界部分で検知できなかった侵入を端末側で検知できるよう、データ連携を実施している。

(3) コンテンツデリバリーネットワーク(CDN)のセキュリティ機能を採用している場合。

○お客様が利用する予約センター等の B2C ネットワークの境界付近で採用している。

○侵入検知製品で検知に用いるデータは、ネットワーク監視型で取得している。

○お客様からの通信に紛れて、ボット等の通信も含まれるため、それらを CDN で検知・ブロックし、通過した内容を CDN が持つ Web アプリケーションへの不正な攻撃を防ぐ機能である WAF(Web Application Firewall)機能でフィルタリングした上で自社内に取り込んでいる。

(4) 一般的なホワイトリスト型の制御を実施し、ネットワークの中で許可された端末以外

の接続を検出した場合、アラートがあがり、設定によっては検知だけではなくブロックまで実施する製品を採用している場合。

〇制御システム全般で採用している。

〇不正な端末の接続検知製品で検知に用いるデータは、ネットワーク監視型で取得している。

〇許可される端末は、通常時に利用する端末として MAC アドレス、IP アドレス等の事前登録が必要である。

(5) 不正なソフトウェア検知製品を採用し、導入時に許可されるアプリケーション以外の稼働を検知した場合、アラートがあがる場合。

〇制御システムに負荷をかけないために、制御システムの管理者用監視端末やその通信を集約している管理端末に導入している。

〇データを監視せずに、起動されるアプリケーションを監視することで不正な操作が行われないように対策している。

〇集中監視制御装置や、管理者用監視端末やその通信を集約している管理端末は、ほとんどが指令所のセンター側に集約されている。しかし、現状では、指令所等で、現場のネットワークでの異常を検知するためのシステムは存在せず、障害等が発生した際、自社の調査で解決できない場合は、構築ベンダーと連携し、対応を実施することとしている。

3.2.1.4. 採用している侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品の付加機能

採用している侵入検知製品、不正な端末の接続検知製品・不正なソフトウェア検知製品の付加機能は、主に資産、構成管理機能が搭載されていることが多い。

他のセキュリティ対策製品と連携し、検知や防御の効果を高めることが出来る製品の場合、SIEM 連携機能を活用してデータを連携することで、システム全体のセキュリティレベルを向上している。

一方、侵入を検知することや不正な端末を検知することに目的を絞り、導入先システムの負担やコストを鑑み、侵入検知製品、不正な端末の接続検知製品・不正なソフトウェア検知製品の付加機能を理解した上で、付加機能を利用しないことを選択する事業者も存在する。

3.2.1.5. 侵入検知製品・不正な端末の接続検知製品・不正なソフトウェア検知製品と既存のセキュリティ対策技術の組み合わせ

すべての運輸･交通業界のシステムが侵入検知製品、もしくは不正な端末の接続検知製品･不正なソフトウェア検知製品と既存のセキュリティ対策技術を意図的に組み合わせて利用することを念頭においているわけではないが、侵入検知製品、もしくは不正な端末の接続検知製品･不正なソフトウェア検知製品と既存のセキュリティ対策技術を組み合わせている場合、セキュリティ対策の個別最適化の改善や、システム全体のセキュリティレベルの向上を

目指し、侵入検知製品の SIEM 連携機能を活用し、他のセキュリティ対策技術と連携させることで、低い管理コストで一貫したセキュリティ対策を実施している。これにより、境界部分で検知できなかった侵入を端末側で検知する、自社以外の他社の検知情報も反映する等を実現している。

他にも、侵入や攻撃の早期発見のため、構成管理やエンドポイントのマルウェア検知と組み合わせている。この場合、SIEM 連携による自動化は行わず、EDR により、エンドポイント側で検知した結果を侵入検知製品に連携、反映させることで、迅速なネットワーク間の連携を実現している。

他にも、外部ネットワークへの接続は一方通行で出力するのみに限定することで、セキュリティ向上を実現している。

3.2.2. 導入にあたって参考となる事例

導入にあたって参考となる事例では、導入に至った背景、導入に向けた検討、チューニング、試用期間の観点に沿い、参考になるポイントを記載する。

3.2.2.1. 導入に至った背景

導入に至った背景は、社会情勢の変化や、サプライチェーンリスクに対するセキュリティ対策の必要性向上、経営層からのセキュリティ向上の指示等を受け、社内のセキュリティポリシーを改善する際に、運輸・交通業界のシステム全体のセキュリティ強化を目的とした検討の中で、既存のセキュリティ対策の個別最適化からの脱却や、インシデント発生時の影響範囲を拡大させないことを目指し、侵入検知製品や不正な端末の接続検知製品・不正なソフトウェア検知製品導入の検討が行われることが挙げられる。

他には、業界内のセキュリティ向上に向けた検討を受け、経営者からトップダウンで制御システムへのセキュリティ対策導入に向けた検討が進められることが挙げられる。

3.2.2.2. 導入に向けた検討

導入に向けた検討は、社内のセキュリティに関する部署や外部専門家と連携しつつ、製品比較の実施が行われることが多い。その際、既存の通常業務の機能を阻害しないこと、他のセキュリティ対策技術の連携が実施できるか、必要なセキュリティ対策機能を搭載できるか、機能を搭載した際に製品の性能が低下しないか等、侵入検知製品、もしくは不正な端末の接続検知製品・不正なソフトウェア検知製品を導入する上での優先順位を社内で検討し、明確にした上で、選定を実施している。

3.2.2.3. チューニング、試用期間

チューニング、試用期間は、今回の利用動向調査では以下の事例が挙げられた。

(1) 対象システムにとって必要なアラートを判断し、遮断するアラートを判断するために

侵入検知製品ベンダーとコミュニケーションを取りながらチューニング、試用期間を設ける場合。

本事例では、ホワイトリスト設定の際に社内の各部署と連携し、ネットワーク構成や機器の棚卸しを実施したことが明らかになった。ホワイトリストを設定する際、なにをもってホワイトだと定義し、ホワイトリストに含めて良いかという検討が非常に大きな課題となった。ネットワークとしては閉域網を前提に構成しており、ネットワーク構成が閉域網として保たれていることが明らかになれば十分であったが、接続される機器等について、端末のプログラムをすべてホワイトリストに含めてしまうと、既にマルウェアが混入している場合、マルウェアまでホワイトリストに含まれてしまうという懸念があった。この懸念を払拭するため、制御ベンダー等と密に検討を重ね、なにをホワイトリストに含めるか、なにを含めないかの判断を実施するための検討に最も工数をかけて実施した。

(2) 不正な端末の接続検知製品・不正なソフトウェア検知製品のホワイトリスト管理等の初期設定や、端末が故障した際のホワイトリストのアップデートとして各製品ベンダーに委託している場合。

いずれの事例も、適用範囲によっては誤検知の発生し易さが異なるため、全体を通して誤検知が発生しないよう、適用範囲ごとに設定を変更、調整するコストがかかる。通信量が多い範囲では、どこまで検知し、どこまで遮断するのかは侵入検知製品ベンダーとコミュニケーションを取りながら決定する。具体的には、侵入検知製品を導入した最初の 1 か月間は、チューニング期間とし、検知のみ実施して遮断しないパターンと、検知も遮断も実施するパターンで試験運用をし、比較した結果からどのようなアラートが上がった際に、どのように遮断するかを調整した。この様な調整を繰り返し、継続的に改善を行った。

3.2.3. 運用にあたって参考となる事例

運用にあたって参考となる事例では、侵入検知製品の運用・監視体制、侵入を検知した際の対処方策、運用時のメリット・デメリット、明らかになった課題、今後のセキュリティに関する展望等の観点に沿い、以下、参考になるポイントを記載する。

3.2.3.1. 侵入検知製品の運用・監視体制

侵入検知製品、不正な端末の接続検知製品や不正なソフトウェア検知製品の運用と監視体制は、今回の利用動向調査では以下の事例が挙げられた。

(1) 運用と監視を外部の専門会社に依頼している場合。

〇アラートが鳴った際、外部の専門会社からそれぞれのアラートに応じて、社内の設備やサーバー担当者か SOC に連絡が来る。外部の専門会社から連絡を受けた社内担当者

が、アラートの原因を調査し、対応を実施する運用となっている。この際、社内の担当者が実施すべき対処内容を明確にするため、どこで、どんなアラートが検知され、どういった対応が必要になっているのか等、詳細に連絡するよう、外部の専門会社には依頼している。

○システム全体において統一的な監視を実現するために、当該侵入検知製品、不正な端末の接続検知製品、及び不正なソフトウェア検知製品に関するアラートだけではなく、他のセキュリティ製品の監視も一括で依頼することで、管理コストの削減やセキュリティレベルの向上を実現している。

(2) 製品の運用監視と SOC を外部委託、CSIRT を社内で運用している場合。

○侵入検知製品に関する知識、スキルを自社で保有しようとすると非効率になってしまうため、侵入検知製品に関する知識、スキルを保有している専門会社に侵入検知製品の監視を委託している。この段階で、あきらかな不正について検知した場合、遮断を実施している。

○上記、委託先の専門会社で判断できなかった検知について、遮断するかどうかの判断を、委託先の SOC にエスカレーションする。SOC が遮断するかどうかを判断した上で、原因となる機器、ネットワーク、担当部署を明らかにする。

○上記、SOC の判断を受け、原因となった機器、ネットワーク、担当部署について、社内 CSIRT が当該部署に確認し、是非を検討し、再発防止に努める。

○委託先の専門会社には侵入検知製品のスキル、委託先の SOC には一般的なインシデント対応スキル、社内 CSIRT には業務に対する理解が求められ、それぞれ求められるスキルが異なる。それぞれの段階ごとの役割を明確にすることで、求められるスキルや知識を絞り、専門性高く効率的に監視、対処できるように設定している。

○補足として、セキュリティ業界は転職が多いため、属人的な管理にならないよう、その分野の専門家であれば対応できる内容のみを求め、多くは求めないで専門性を高く維持できるように努めている。

(3) 運用、監視も含めて、社内の PoC(Point of Contact)と CSIRT で連携、役割分担して実施している場合。

○アラートが鳴った際、検知された設備やネットワークを担当している部署の PoC(Point of Contact)に連絡がいき、社内の CSIRT に情報連携を行う。

○具体的なインシデントが把握された際は、社内の PoC(Point of Contact)と CSIRT が連携し、具体的な調査や対応に当たる。

○現場（指令所）の PoC(Point of Contact)は、機器故障等のフィジカルの機器故障等の担当者とは別に、各部署や指令所にサイバーセキュリティ専任の担当者として配置されている。

配置される PoC(Point of Contact)は各部署の情報推進リーダと指令所等のサイバーセキュリティ専任の担当者で構成されている。

情報推進リーダは、本体制を構築する前から各部署に配置され、その各情報推進リーダに対し、サイバーに関する情報や資料や機器の提供として、PC の配布、新しい機

能の紹介、サイバーに関するマニュアル配布等を実施し、各部署内への情報の浸透を実施していた。この情報推進リーダは各部署の管理担当者、役職者が実施している場合が多く、必ずしも、サイバーセキュリティに関する十分なスキルを有しているとは限らない。しかしながら、これまで情報推進リーダとして他部署との連携を実施してきた実績があることから、PoC(Point of Contact)の重要な役割である情報連携が確実に実施できると考え、体制に組み込んでいる。一方、24 時間 365 日体制で運用を実施している電力、運行、営業等の部署については、インシデントが発生した際に迅速な対応を実施できるよう、常に現場に従事している電力、運行、営業の各指令長をPoC(Point of Contact)として指名した。各指令長は当番制となっており、日替わりで実施している。この体制を設けることで、拠点でセキュリティインシデントが発生した場合は、各指令長に連絡が行き、各指令長から CSIRT に情報が連携されることで、迅速な対応を実現出来るようにしている。

(4) 運用・監視も含めて社内の現場担当者側で実施している場合。

○アラートが鳴った際、検知された設備やネットワークを担当する部署に連絡がいき、それぞれの部署内で対応する運用となっている。社内 24 時間監視を実施しているような SOC が存在せず、それぞれの設備やネットワークが汎用的ではない場合、担当する部署が対応を実施することが適切であると考え、組織体制に即した対応体制を設けている。

3.2.3.2. 侵入を検知した際の対処方策

侵入検知製品、不正な端末の接続検知製品・不正なソフトウェア検知製品が侵入や不正な端末を検知した際の対処方策は、今回の利用動向調査では以下の事例が挙げられた。

(1) 運用・監視も含めて外部の専門会社に依頼している場合。

○外部の専門会社に依頼しているため、外部の専門会社の指示の下、設備やサーバー担当者か SOC が対処を行う運用となっている。この際、社内の担当者が実施すべき対処内容は、外部の専門会社が社内の担当者に明確に指示できるよう、事前の調整等を実施している。

(2) 製品の運用監視と SOC を外部委託、CSIRT を社内で運用している場合。

○委託先の専門会社、SOC の対処内容については運用マニュアルが設けられている。CSIRT の対処内容については人的要因が多いため、マニュアル化はせず、訓練等でカバーしている。

(3) 運用、監視も含めて、社内の PoC(Point of Contact)と CSIRT で連携、役割分担して実施している場合。

○検知された際のマニュアル等の作成は、各部署や指令所に一任している。

○マニュアルの作成とは別に、年に 2 回、社内でサイバーセキュリティ訓練を実施しており、その内の 1 回は制御システムに関する訓練を実施し、実際にアラートが鳴った際の対応に関わる訓練を実施している。

(4) 運用・監視も含めて社内の現場担当者側で実施している場合。

〇それぞれの部署内で対応する運用となっているため、実際の対処内容の洗い出しや社内の役割分担等を示すマニュアルを作成することが必要となる。

3.2.3.3. 運用時のメリット・デメリット

運用時のメリットは、主に侵入検知製品が侵入を正しく検知、または不正な端末の接続検知製品・不正なソフトウェア検知製品が不正な端末を検知し、セキュリティの脅威に適切に対応することで、社内のセキュリティレベルが向上した。また、実際に制御系システムへの関与が薄かった CSIRT が、IT 系と制御系システム双方に関与する体制を構築するきっかけとなった。

他にも運用時のメリットとして、侵入検知製品を導入することで平常時に多くの攻撃を受け、その全てを侵入検知製品で防いでいることをわかりやすく経営層に伝えることが出来ることが挙げられる。セキュリティ対策を十分に実施していると、結果として社内では問題が起きず、セキュリティ対策が不要なのではないかという話になりやすい。そのような方向性に行かないように、侵入検知製品を導入することでこれだけ攻撃を受けていることや、リスクの再確認、セキュリティコストの有効度や、費用対効果を理解してもらうことが達成されることが大きなメリットとして挙げられる。

一方、運用時のデメリットは、運用・監視も含めて社内の現場担当者側で実施している場合、適用対象が汎用的なシステムでないことから、現場の担当者に運用・監視を一任する形となってしまい、アラートが鳴らない限り、導入後の継続的なフィードバックや、改善に向けたコミュニケーションが取りづらいことが挙げられる。しかしながら、これまで個々の担当者ごとで縦割りとなっていた組織が、部署横断的に同一のセキュリティ製品を導入することで、セキュリティに関する情報を共有する等のコミュニケーションを実施するようになり、長期的な社内セキュリティレベルの向上に資する情報の収集が可能になったとも言える。

3.2.3.4. 明らかになった課題

侵入検知製品、不正な端末の接続検知製品・不正なソフトウェア検知製品について明らかになった課題は、侵入検知製品や不正な端末の接続検知製品・不正なソフトウェア検知製品の適用範囲のネットワークが業務で分離されているため、事業者の制御システムで横断的な一括監視が難しいことである。

他には、セキュリティ対策はコストがかさむため、極力人的コストがかかるものは実施せずに、自動化を目指す等の継続的な検討や改善は重要である。セキュリティ対策を導入した際に、オーバースペックの機能を搭載しない、機能が重なっている場合は、重なってくる機能を取り除く、もしくは古いセキュリティ対策の利用を辞め、コストが重ならないようにすることが重要であり、常に変化し続けるリスクや脅威に対して、適切なコストをかけつつ、対応、検討し続ける体制が求められる。

加えて、制御システムのセキュリティ向上に係る人材の確保、人材育成は大きな課題であり、IT 系システムの人材に制御システムの教育を実施する、または制御システムの人材を

IT 系システムの検討に参加させる等の人材育成を進めることが求められる。インシデントが発生した際の社内の役割分担についても今後、改善の余地がある。

また、ネットワークにおいて侵入経路となり得る出入口を必要最低限に絞り、閉域網を保った上で不正な端末の接続検知製品・不正なソフトウェア検知製品を導入している事例について、追加の調査を実施したところ、不正端末の接続抑止は実施していないため、不正な端末は接続可能な状態となっていることが明らかになった。

3.2.3.5. 今後のセキュリティに関する展望等

今後のセキュリティに関する展望等は、上記の明らかになった課題の通り、導入後、侵入検知製品や不正な端末の接続検知製品・不正なソフトウェア検知製品から得られた知見を今後のセキュリティ対策に活かしていくことが挙げられる。具体的には、侵入検知製品や不正な端末の接続検知製品・不正なソフトウェア検知製品の機能の更なる活用や、制御システムと IT システムのセキュリティ向上の連携、社内のセキュリティ部門と制御ベンダー間の役割分担の効率化、社内の縦割りのセキュリティ対策の改善等に活用していくことが挙げられる。

具体的には、SOC など極力人的コストがかかるものは実施せず、自動化を目指していることとも関連し、今後、導入している侵入検知製品や不正な端末の接続検知製品・不正なソフトウェア検知製品とネットワーク全体の監視と対応を行う NDR (Network Detection and Response)を組み合わせ、更に、エンドポイントで検知した結果を、侵入検知製品や不正な端末の接続検知製品・不正なソフトウェア検知製品に反映させることが考えられる。結果として、早期発見、検知の分析負荷の軽減を実現することで SOC 等の負荷軽減を実現しようとしている。

また、継続的なセキュリティ対策を実施するためにもコストの効率化が重要であり、業界内の集団防衛として、他事業者や業界団体等との情報共有を積極的に実施することで、常にセキュリティについて高い意識を維持しつつ、業界全体やサプライチェーン全体でのセキュリティレベルの向上が目指される。

3.3. 石油・エネルギー業界の調査結果から参考になるポイント

石油・エネルギー業界では、実際に石油精製プラントの制御システムに適用している 1 事業者にヒアリング調査を実施した。以下、石油・エネルギー業界の調査結果から参考になるポイントをそれぞれの観点ごとに記載する。

3.3.1. 侵入検知製品の利用概要

利用概要では、システムの構成、侵入検知製品の適用範囲、採用している侵入検知製品技術、採用している侵入検知製品の付加機能、侵入検知製品と既存のセキュリティ対策技術の

組み合わせの観点に沿い、参考になるポイントを記載する。

3.3.1.1. システムの構成

一般的な石油精製プラントの制御システム構成を図 3.4 に示す。今回の利用動向調査で収集した事例における、侵入検知製品の適用範囲を赤枠で示す。

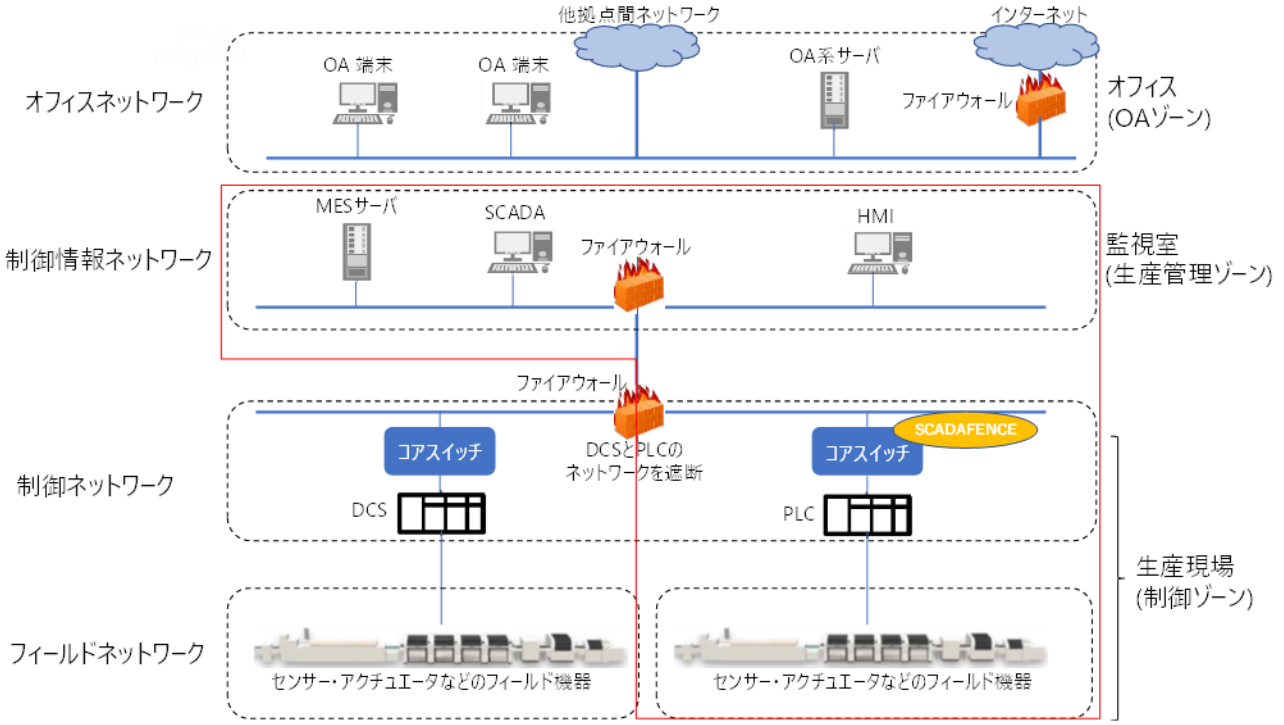

図 3.4 一般的な石油精製プラントの制御システム構成

制御システムのネットワークは、フィールドネットワークと制御ネットワークと制御情報ネットワークとオフィスネットワークから構成される。

一般的な石油精製プラントの制御システム構成を、IPA の「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」と照らし合わせると、一般的な石油精製プラントの制御システム構成のフィールドネットワークが制御ネットワーク（フィールド側）[16]に概ね対応し、一般的な石油精製プラントの制御システム構成の制御ネットワークと制御情報ネットワークが制御ネットワーク（情報側）[17]に概ね対応する。

侵入検知製品の適用範囲のネットワークには、350 台程度の SCADA が接続されている。

DCS と PLC のネットワークは、ファイアウォールを介してのみ接続されている。具体的に

16 「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」の制御ネットワーク（フィールド側）

17 「制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」の制御ネットワーク（情報側）

DCS 側にリモートセンサーを設定しており、ファイアウォールで該当通信のみを許可している。

現在は DCS ネットワーク側には侵入検知製品を導入していない。

3.3.1.2. 侵入検知製品の適用範囲

侵入検知製品の適用範囲は、制御ネットワークの PLC 側のコアスイッチに設定される。システム上の侵入検知製品の適用範囲は図 3.4 の赤枠部分である。

制御ネットワークの PLC 側のコアスイッチに侵入検知製品を導入している理由は、コアスイッチに PLC とフィールド機器の通信が集約される設定のため、コアスイッチで監視が可能となるためである。

監視しているデータは、全てのトラフィックである。

3.3.1.3. 採用している侵入検知製品技術

同社が石油精製プラントの制御システムに適用している侵入検知製品は、SCADAfence 社の SCADAfence Platform である。当該侵入検知製品は、通信内容を学習・解析し、論理ネットワーク構成を自動生成、かつ正常時の振る舞いをモデル化することで、セキュリティ事故につながる可能性のある動きを検知するものとのことであった。

侵入検知製品で検知に用いるデータは、ネットワーク監視型で取得している。

3.3.1.4. 採用している侵入検知製品の付加機能

採用している侵入検知製品の付加機能は、今回の調査では確認することが出来なかった。

3.3.1.5. 侵入検知製品と既存のセキュリティ対策技術の組み合わせ

侵入検知製品と組み合わせて利用しているセキュリティ製品は、産業オートメーション制御システム(ディレクトリ管理ツール)である。

産業オートメーション制御システム(ディレクトリ管理ツール)、PLC ネットワークのセキュリティ確保のために利用している。具体的に、デバイスが PLC ネットワークに接続するためには、産業オートメーション制御システム(ディレクトリ管理ツール)に登録されているか、認証される必要がある。

3.3.2. 導入にあたって参考となる事例

導入にあたって参考となる事例では、導入に至った背景、導入に向けた検討、チューニング、試用期間の観点に沿い、参考になるポイントを記載する。

3.1.2.1. 導入に至った背景

導入に至った背景に、PLC と SCADA システム用のネットワークは、インターネットからエ

アギャップされていることから、本質的に安全であると認識されていたが、その状態を過信することなく、不正な侵入等が起きた際に、それが悪意のある攻撃なのか、悪意のない事故なのか、正しく判断し、管理できる状態を実現したいという目的があった。

3.3.2.2. 導入に向けた検討

導入に向けた検討は、複数の侵入検知製品の比較検討が行われた。比較検討の際、侵入検知製品ベンダーが導入事業者の業務やシステムを理解した上で、オーダーメイド型の提案を行い、具体的に制御システム上でどのように製品が機能するかについて、直接の訪問による説明を実施した。加えて、営業担当者が制御システムやセキュリティ上の侵入について、豊富な知識を有しており、信用がおけると判断し、採用に至った。営業時に同ベンダーから提案された内容は、運用開始後も問題なく実施されており、問い合わせをする際も導入事業者の制御システムを熟知している担当者から適切な支援を得ることが出来ている。

3.3.2.3. チューニング、試用期間

チューニング、試用期間は、侵入検知製品ベンダーと連携しつつ、1 日 30 分程度、約 2 週間の時間をかけ自社で実施した。監視している範囲のすべての資産が停止するたびにアラートを出す必要はなく、必要なアラートのみが表示されるよう設定を行った。

導入後の微調整は、新しいアラートが発生した際の確認のみ必要となり、1 日数分程度で十分運用することが可能であった。具体的には新しいトラフィックが発生した際、管理画面上にポップアップでアラート表示され、担当者から端末を管理している担当部署等に確認をすることで、アラートの原因を明らかにし、今後当該アラートを表示するかしないかを設定している。

3.3.3. 運用にあたって参考となる事例

運用にあたって参考となる事例では、侵入検知製品の運用・監視体制、侵入を検知した際の対処方策、運用時のメリット・デメリット、明らかになった課題、今後のセキュリティに関する展望等の観点に沿い、参考になるポイントを記載する。

3.3.3.1. 侵入検知製品の運用・監視体制

侵入検知製品の運用・監視体制は、3 名の担当者で構成している。担当者側で判断できない事態、質問等がある場合は、適宜侵入検知製品ベンダーに問い合わせを行う。

3.3.3.2. 侵入を検知した際の対処方策

侵入を検知した際の対処方策は、担当者にアラートが通知され、必要な部署に確認を行い、必要に応じて分離して原因を特定するための対処を行う。例として、ある部署の PC の IP が変更され、その上で当該 PC が PLC を読み取りに行くとアラートが鳴る。そのアラートを受

け、担当者が PC を保有している部署に連絡をし、問題なければアラートを削除している。他の例として、ファイアウォールを経由して侵入が発生し、アラートが鳴った場合はファイアウォールを分離することとしている。

今後は侵入の深刻度によって、担当者にのみアラートを表示するか、現場の従業員に広くメールでアラートを出すか等、アラートの通知範囲を変更する運用を目指している。

現在、前述した対処方策等を取りまとめるマニュアルを作成中である。まずは既に侵入検知製品を導入している PLC と SCADA の範囲でマニュアルを作成し、今後侵入検知製品を導入する予定の DCS の範囲から、更には全社へと拡大していく予定である。

3.3.3.3. 運用時のメリット・デメリット

運用時のメリットは、導入する侵入検知製品にもよるが、管理コストを最小限に抑えられたことである。管理する資産が増加した際、管理コストも同様に増えると持続性が厳しくなる。その点、適用した侵入検知製品は管理する資産が増加しても、管理コストは変わらない。また侵入検知製品ベンダーによる顧客へのシステム理解を深めるためのコミュニケーションや、サポートも導入後時間が経っても劣化することがない点はメリットである。

一方の運用時のデメリットは、今回の調査では確認することが出来なかった。

3.3.3.4. 明らかになった課題

侵入検知技術について明らかになった課題は、導入事業者において、既存の石油精製プラントの制御システムに新規で侵入検知製品を導入することに抵抗のある部署が存在し、石油精製プラントの制御システム全体への一括導入の障壁となっていることである。

3.3.3.5. 今後のセキュリティに関する展望等

今後のセキュリティに関する展望等は、侵入検知製品の導入範囲の拡大である。次のステップとして、制御ネットワークの DCS 側にも導入することを予定しており、既にテスト運用を行い、端末やトラフィックを取得し、問題なく運用できることを確認済である。DCS 側のネットワークに導入後は、自社内のパイプラインやターミナルにも侵入検知製品を導入する意向があり、パイプラインやターミナルのような接続部分が多く、基幹的な役割を担っている範囲でも侵入検知を実現することを目指している。

又、制御ネットワークの強靭化に向けて、主要なシステムベンダーが推進する産業用共通プロトコル(Common Industrial Protocol(CIP))のセキュリティ規格を将来的に実装することも計画しているとのことであった。

4. 調査結果のまとめ

不動産・ビル業界、運輸・交通業界、石油・エネルギー業界の計 7 事業者における利用動向調査の結果を、表 4.1 に一覧表としてまとめた。

表 4.1 利用動向調査のまとめ

区分	観点	不動産・ビル業界		運輸・交通業界				石油・エネルギー業界
		A 社	B 社	C 社	D 社	E 社	F 社	H 社
概要	システム構成	設備ごとのフィールドネットワークと制御ネットワーク、集約する統合ネットワークから構成		制御システムを所管している部署ごとに分けて構成		制御システムと中央監視室とシステムセンターで構成		フィールドネットワークと制御ネットワークと制御情報ネットワーク
	適用範囲	①インターネット等の外部ネットワークと接続している境界 ②熱源・空調・給排水設備の制御 IP ネットワークの HMI 周辺 ③受変電設備の制御 IP ネットワークの HMI 周辺	①インターネット等の外部ネットワークと接続している境界	不正な端末の接続検知製品をデータが集約される集中監視制御装置や、管理者用監視端末やその通信を集約している管理端末に適用		侵入検知製品を関連システムと OT の間等、侵入検知が必要な範囲に適用している		制御ネットワークと PLC 側の制御情報ネットワーク、フィールドネットワークが監視範囲
	採用している侵入検知製品技術	振る舞い検知型＋機械学習機能 データはネットワーク監視型で取得	独自の機械学習アルゴリズムにより学習・解析し、論理ネットワーク構成を自動生成 ＋正常時の振る舞いをモデル化 データはネットワーク監視型で取得	不正なソフトウェア検知製品 データを監視せず、起動されるアプリケーションを監視	不正な端末の接続検知製品のホワイトリスト型 データはネットワーク監視型で取得	シグネチャー、ルール、振る舞い検知、サンドボックスでも検知できる製品 次世代型のファイアウォールで、シグネチャー、ルール、振る舞い検知、サンドボックスでも検知できる製品 データはネットワーク監視型で取得	コンテンツデリバリーネットワーク (CDN) のセキュリティ機能で検知・ブロックし、通過した内容を CDN の WAF 機能でフィルタリング データはネットワーク監視型で取得	SCADAfence Platform 通信内容を学習・解析し、論理ネットワーク構成を自動生成、かつ正常時の振る舞いをモデル化することで、セキュリティ事故につながる可能性のある動きを検知 データは、ネットワーク監視型で取得
	製品の付加機能	資産管理、SIEM 連携、ファイアウォール	資産管理機能、SIEM 連携機能、レポート機能	利用無し	利用無し	SIEM 連携	利用無し	利用無し
	他のセキュリティ対策技術との組み合わせ	ファイアウォール、不正操作の検知等のセキュリティ対策技術について、侵入検知製品側で一元管理	ファイアウォール	OS のポリシーと組み合わせて水際対策を実施 外部ネットワークへの接続は一方通行で出力するのみに限定	組み合わせは実施していない	システム全体のセキュリティレベルの向上を目指し、侵入検知製品の SIEM 連携機能を活用し検知情報を連携	構成管理やエンドポイントのマルウェア検知と連携（SIEM 連携は未実施） 今後 NDR による連携を検討	産業オートメーション制御システム(ディレクトリ管理ツール)
導入	背景	試験的に導入することで侵入検知製品の効果や、ビルシステムへの必要性を検討	ビルシステムの OT 分野のセキュリティの成熟度が十分でないことから、試験的に導入	セキュリティ向上に関する経営層からの指示により導入	社会情勢の変化によるセキュリティ向上のために導入	社内のセキュリティポリシーを改善に伴い導入	社会情勢の変化、サプライチェーンリスクに対するセキュリティ対策の必要性向上によるセキュリティ向上のために導入	不正な侵入等が起きた際に、正しく判断し、管理できる状態の実現のために導入
	導入に向けた検討	システムに影響がないか、監視や運用を委託できるか等を確認	社内のセキュリティに関する部署や外部専門家と連携しつつ、資産管理の機能を搭載しているか、どのような脅威を検知できるか等を確認	既存の通常業務の機能を阻害しない等を確認	既存の通常業務の機能を阻害しない等を確認	外部専門家と連携しつつ、他のセキュリティ対策技術の連携が実施できるか等を確認	必要なセキュリティ機能を搭載できるか、機能を搭載した際に製品の性能が低下しないか等を確認	自社のシステムを理解した上での支援が可能かを確認
	チューニング・試用期間	必要なアラートを判断するために侵入検知製品ベンダーとコミュニケーションを取りながらチューニング、試用期間を設けた	チューニングを自動で行い、負担なく試用期間を設けた	チューニング、試用期間の言及無し	チューニング、試用期間の言及無し	検知のみ実施して遮断しないパターンと、検知も遮断も実施するパターンで試験運用し、調整	チューニング、試用期間の言及無し	侵入検知製品ベンダーと連携しつつ、チューニング、試用期間を設けた

表 4.1 利用動向調査のまとめ（前ページからの続き）

区分	観点	不動産・ビル業界		運輸・交通業界				石油・エネルギー業界
		A 社	B 社	C 社	D 社	E 社	F 社	H 社
運用	運用・監視体制	侵入検知製品ベンダーに依頼	ビル管理の現場担当者側で実施	社内の PoC(Point of Contact)と CSIRT で連携して実施	社内の現場担当者側で実施	外部の専門会社に依頼	外部の専門会社と SOC、社内の CSIRT で連携して実施	社内の担当者で実施。適宜侵入検知製品ベンダーと連携
	対処方策	侵入検知製品ベンダーから連絡を受け対処。マニュアル等は未作成	マニュアルを作成。演習型の研修を実施し、演習を定期的に実施するガイドラインを策定	一部マニュアルを作成している部がある	マニュアル作成予定	外部の専門会社から連絡を受け対処。マニュアル等は未作成	委託先の専門会社、SOC でマニュアルを作成 CSIRT はマニュアルではなく、訓練等を実施	社内の担当者が確認と、必要に応じて分離して原因を特定。マニュアルは作成中
	メリット・デメリット	メリットは、今後のセキュリティ対策の検討に資する情報、知見を得られたこと デメリットは、当初のビル管理側の想定よりも多様なアラートが頻繁に鳴り、対応に工数が割かれること	メリットは、インシデントが発生した際の業務フローの研究が実施できること デメリットは、特になし	メリットは、IT と制御系システムのセキュリティ対策における連携、協業のきっかけとなり、さらなるセキュリティレベルの向上に資する検討の足掛かりを得る デメリットは、特になし	メリットは、IT と制御系システムのセキュリティ対策における連携、協業のきっかけとなり、さらなるセキュリティレベルの向上に資する検討の足掛かりを得る デメリットは、特になし	メリットは、今後のセキュリティ対策の検討に資する情報、知見を得られたこと デメリットは、特になし	メリットは、セキュリティリスクの再確認、セキュリティコストの有効度や、費用対効果の理解促進 デメリットは、特になし	メリットは、運用コスト低く、侵入検知を実現していること。侵入検知製品ベンダーの支援を受けることができること デメリットは特になし
	課題	重大な侵入が頻繁に起きないため、侵入検知製品の機能を十分に活用することができずにコストに見合わない懸念	インターネットに接続していないビルにお金をかけて導入するかは課題	制御システムのセキュリティ向上に係る人材の確保、人材育成	インシデントが発生した際の社内の役割分担	インシデントが発生した際の社内の役割分担	セキュリティ対策の重複回避含め、変化し続けるリスクや脅威に対して、適切なコストをかけつつ、対応、検討し続ける体制	既存の石油精製プラントの制御システムに新規で侵入検知製品を導入することに抵抗のある部署が存在し、石油精製プラントの制御システム全体への一括導入の障壁が存在すること
	今後の展望	将来的にビルのシステムがクラウドに移行し、複数のビルを一括で管理、監視、運営する場合の管理体制のあり方等への検討	制御ベンダーに対しても同様のマニュアルの作成、サイバーインシデントに対応する演習の共同実施を検討	IT と制御系システムのセキュリティ向上に向けた連携	IT と制御系システムのセキュリティ向上に向けた連携	社内のセキュリティ部門とベンダー間の役割分担の効率化	NDR 連携による早期発見、検知の分析負荷の軽減を実現することで SOC 等の負荷軽減を実現 業界全体やサプライチェーン全体でのセキュリティレベルの向上	侵入検知製品の導入範囲の拡大

4.1. 各業界における侵入検知製品の導入状況に関する考察

不動産・ビル業界、運輸・交通業界、石油・エネルギー業界の各業界間において見られた侵入検知製品の導入状況の違いについて考察する。

4.1.1. 不動産・ビル業界における侵入検知製品の導入状況に関する考察

侵入検知製品において、検知ポリシーの作成作業や、検知ポリシーに基づく設定のチューニング作業は、取り分け、時間と労力を要し、導入事業者側における負担が大きい。不動産・ビル業界では、制御システムにおけるセキュリティ対策の検討が始まったばかりであり、侵入検知製品ベンダー側にとっても侵入検知製品を導入する先行する導入事業者が業界のファーストユーザーとなることに加えて、導入事業者側において、セキュリティに関する知識・知見が必ずしも十分とは言えない状況であるため、導入事業者側における負担がより一層増幅されている。

具体的には、そのような作業を効率化し、導入事業者の負担を軽減する上で、侵入検知製品ベンダー側が、導入事業者側と同等のレベルで、導入する業界固有の制御システムに関する知識や運用に関する知見を把握することが重要かつ不可欠であるが、侵入検知製品ベンダー側において、業界固有の制御システムに関する知識・知見を十分に持ち合わせていないため、侵入検知製品ベンダーとの間のコミュニケーションや信頼関係の構築に支障が生じ、不要なアラートの消し込み作業が非効率になるなど、導入事業者の負担増大に繋がるさまざまな問題を引き起こしがちである。

不動産・ビル業界においては、このような問題が本格導入の足かせとなり、侵入検知製品の導入がテスト導入レベルにとどまっている状況が見られた。導入事業者側においては、業界固有の制御システムに関する知識・知見を保有する侵入検知製品ベンダーが提供する侵入検知製品を選定し、導入事業者側における負担を極力軽減できるようにしたいと考えている。

4.1.2. 運輸・交通業界における侵入検知製品の導入状況に関する考察

運輸・交通業界においては、各業界が運用するシステムの特性の違いにより、異なる侵入検知製品の導入状況が見られた。

閉域網で設計・構築・運用されている制御システムを持つ業界では、インターネットに接続された情報システムでは常識になっている、セキュリティ製品の導入について、導入事業者側では、制御システムの可用性を損なう可能性があると考えている。加えて、制御システムを運用する社内の OT 部署においては、侵入検知製品を含め、セキュリティ全般に関する専門知識やスキルが不足しがちであることから、制御システムにおけるセキュリティ製品の導入に二の足を踏む傾向がある。

このような業界においては、可用性重視の姿勢が強く、システム改変やセキュリティ製品の導入に対する抵抗感も根強く残っていることから、制御システムにおける侵入検知製品の導入が困難であるという状況が見られた。

他方、制御システムを所有せず、外部公開サーバーの使用や外部とのシステム連携を通じて、インターネットに接続された各種情報システムを運用している業界では、当該システム

について、導入事業者側では、攻撃を受けるリスクが高く、攻撃によって機能が停止または低下した場合に国民生活及び社会経済活動に多大な影響を及ぼしかねないと考えている。

このような業界においては、リスクに対する危機感が原動力となり、各種情報システムにおいて、侵入検知製品を本格的に導入し運用しているという状況が見られた。

前者の業界の導入事業者においては、以下に示す2つのセキュリティ製品を選択肢に含めて対策検討を行うことが重要である。

○集中監視制御装置や管理者用監視端末等の通信を集約している管理端末に導入することができ、可用性確保上の制約や、セキュリティ製品の導入に伴う想定外の挙動がもたらすシステム・業務への影響について気にしなくて済む、ホワイトリスト型による不正な端末の接続検知製品

○管理者用監視端末に導入することができ、可用性確保上の制約や、メンテナンス時における保守用端末の接続に伴うマルウェアの侵入がもたらすシステム・業務への影響について気にしなくて済む、ホワイトリスト型による不正なソフトウェア検知製品

4.1.3. 石油・エネルギー業界における侵入検知製品の導入状況に関する考察

海外先進事業者の導入事例であるため、国内事業者と状況が異なる可能性がある点について考慮に入れる必要はあるが、石油・エネルギー業界においては、石油精製プラントの制御システムにおけるセキュリティ向上の取組に対して、より積極的な姿勢が見られた。

具体的には、PLC と SCADA が繋がるネットワークがエアギャップ（物理的隔離）されたネットワークであっても、過信することなく、不正な侵入は必ず起こるものと考え、侵入検知製品を導入・運用しており、セキュリティを重視する意識がうかがえた。その他にも、侵入検知製品の追加導入により監視場所・範囲を DCS が繋がるネットワークへと拡大することや、既に導入済みである産業オートメーション制御システム(ディレクトリ管理ツール)に対して、主要なシステムベンダーが推進する産業用共通プロトコル(Common Industrial Protocol(CIP))のセキュリティ規格を将来的に実装することも計画しており、このような取組においても、セキュリティを重視する意識が強く現れていた。

他方、侵入検知製品を導入・運用する狙いとして、管理者個人の属人的な判断ではなく、侵入検知製品が行う客観的な判断に基づいて、不正な侵入を検知し管理できる状態を実現することに重点が置かれており、セキュリティを重視しつつ、ヒトに依存しないセキュリティ対応を通じて運用に係る負担を軽減するという意識も顕著であった。

4.2. 導入システムや導入場所、導入製品、監視・対処体制に関する考察

今回ヒアリング調査を行った事業者7社においては、侵入検知製品等の導入システムや導入場所について、以下の特徴が見られた。

(1) 外部からの遠隔制御・保守等が行われていない、閉域網で設計・構築・運用されている交通・運輸業界の制御システム・ネットワーク上の管理者用監視端末やその通信を集約している管理端末の付近

(2) 外部公開サーバーの使用や外部とのシステム連携が行われている交通・運輸業界の各種情報システム・ネットワークと、インターネットの境界付近
(3) 外部からの遠隔制御・保守等が行われている不動産・ビル業界のビルの制御システム・ネットワーク上の管理者用監視端末の付近
(4) 外部からの遠隔制御・保守等が行われている不動産・ビル業界のビルの制御システム・ネットワークと、インターネットの境界付近
(5) 外部からエアギャップ(物理的隔離)された石油・エネルギー業界の石油精製プラントの制御ネットワーク上の通信を集約しているコアスイッチの付近

以上のことから、外部接続に伴う攻撃リスクや、閉域網では避けて通れない保守用端末の接続を経由した攻撃リスクに備えて、適切なシステムや場所に侵入検知製品等を導入することが重要になると考えられる。

また、上記(1)～(5)のシステムや場所に導入されている侵入検知製品等については、以下の特徴が見られた。

○上記(1)～(5)のシステムについては、導入した製品によって、システムの安定的な稼働やパフォーマンスに影響がもたらされ、通常の業務に支障が生じることを一切回避しなくてはならないという可用性確保上の制約を抱えている点が共通点である。
○そのうえで、取り分け、上記(1)のシステムについては、制御システムであり、かつ上記(3)および(4)のシステムのような拠点・施設ごとにスタンドアローンで運用されるシステムではないため、万が一の場合には大規模かつ広範な影響が懸念され、可用性確保についてより一層高いレベルが要求されることから、OT 用の侵入検知製品の導入には困難を伴う。このため、そのような影響や制約について気にしなくて済む点を考慮して、ホワイトリスト型による不正な端末の接続検知製品や不正なソフトウェア検知製品が導入されている。
○上記(2)のシステムについては、情報システムであり、制御システムではないことから、IT 用の侵入検知製品が導入されている。
○上記(3)および(4)のシステムについては、制御システムであるが、利用形態として、拠点・施設ごとにスタンドアローンで運用されている点が特徴である。このような特徴について十分踏まえ、導入するシステムの範囲を限定して、OT 用の侵入検知製品が導入されている。
○上記(5)のシステムについては、制御システムであり、利用形態として、制御ネットワーク上で運用されている点が特徴である。概念実証(Proof of Concept)を活用した試行運用が実施されているものも含めると、PLC が繋がる制御ネットワークへの導入と、DCS が繋がる制御ネットワークへの導入が別々に進められており、監視するシステムや場所が細かく設定されている点も特徴である。

以上のことから、システムの規模やリスクの大きさ等の導入するシステムの特性や、可用性等の制約事項を考慮して、適切な侵入検知製品等の製品を選択することが重要になると考えられる。

さらに、上記(1)～(5)のシステムや場所に導入されている侵入検知製品等を用いた監視・対処体制については、以下の特徴が見られた。

○上記(1)のシステムについては、制御システムに関わる各設備・ネットワークを所管する部署が、ホワイトリスト型による不正な端末の接続検知製品や不正なソフトウェア検知製品の運用主体となっており、前者では、当該部署にアラートが通知された場合、当該部署から各設備の制御ベンダー・ネットワークベンダーに連絡を行い、各設備・ネットワークベンダーが必要となる対処を行っている。他方、後者では、当該部署にアラートが通知された場合、当該部署が現場で必要となる対処を行っている。

○上記(2)のシステムについては、監視を外部委託しているセキュリティベンダーが IT 用の侵入検知製品の運用主体となっており、セキュリティベンダーに重要なアラートが通知された場合のみ、当該ベンダーから社内のサイバーセキュリティ部署に連絡が入り、社内外の SOC や社内のサーバーチーム、CSIRT と調整しつつ、必要となる対処を行っている。

○上記(3)および(4)のシステムについては、防災センターが OT 用の侵入検知製品の運用主体となるケースと、監視を外部委託しているセキュリティベンダーが OT 用の侵入検知製品の運用主体となるケースの 2 種類が存在する。前者については、当該センターにアラートが通知された場合、当該センターから各制御ベンダーに連絡を行い、各制御ベンダーが必要となる対処を行っている。また後者については、セキュリティベンダーにアラートが通知された場合、当該ベンダーから社内のサイバーセキュリティ部署に連絡が入り、当該部署から各制御ベンダーに連絡を行い、各制御ベンダーが必要となる対処を行っている。

○上記(5)のシステムについては、PLC が繋がる制御ネットワークを所管する部署が、侵入検知製品の運用主体となっており、当該部署にアラートが通知された場合、当該部署から関連する部署に連絡を行い、事象の状況確認を行った上で対処可能な軽微な事象については当該部署のみで必要となる対処を行っている。また対処できない深刻な事象についても、当該部署がセキュリティベンダーと連携しつつ、必要となる対処を行っている。

以上のことから、監視・対処体制においては、社内における運用に係る人材の確保・育成や、アラートが通知された場合の社内外の役割分担が重要になると考えられる。

5. 侵入検知製品の導入を検討する事業者において参考となる事例

産業用制御システムや重要インフラの各種システムを運用する事業者において、侵入検知製品の導入促進を図るためには、円滑かつ継続的な運用のための予算と人的リソースの確保が必要であり、取り分け、侵入検知製品の導入効果について、経営層に分かりやすく、かつ定期的に説明し、理解してもらうことが重要である。

この高いハードルを乗り越えることができれば、社内外を含めた運用体制の構築や、最適な運用を実現するための必要となる人材の確保・育成等を含め、導入事業者が抱えるさまざまな課題を解決できる可能性が高まり、セキュリティレベルの向上やシステムの安定的な運用といった効果・メリットを享受できるという好循環を生み出すことができると考えられる。

以下では、侵入検知製品を導入し運用していく上での導入事業者が抱える課題について整理するとともに、課題の解決のための創意工夫が見られるヒアリング事例を、参考事例として示す。

5.1. 侵入検知製品を導入し運用していく上での課題

前述した「3.侵入検知技術の利用動向調査結果」及び「4.調査結果のまとめ」から見えてきた、侵入検知製品を導入し運用していく上での導入事業者が抱える課題について大別すると、以下の９点が挙げられる。

(1) 侵入検知製品に対する理解の難しさ
(2) 侵入検知製品を選定する際の難しさ
(3) 監視場所の設定の難しさ
(4) 端末のマルウェア感染を発端とする社内の侵害拡大に対する対応の難しさ
(5) 外部からの侵入対策全体を最適化することの難しさ
(6) 運用体制の構築の難しさ
(7) ステークホルダーとの対応連携の難しさ
(8) 侵入防御製品の運用の難しさ
(9) 侵入検知製品の導入効果を実感することの難しさ

5.2. 課題の解決のための創意工夫が見られる事例の取りまとめ

「5.1.侵入検知製品を導入し運用していく上での課題」で前述した導入事業者が抱える課題については、他事業者における具体的な対応事例を参考にしながら、課題解決の糸口を見つけることが重要である。課題の解決のための創意工夫が見られる事例を取りまとめ、以下に紹介する。

(1) 侵入検知製品に対する理解の難しさについては、侵入検知製品の導入検討の段階では、導入するシステムの安定的な稼働やパフォーマンスにどのような影響がもたらされるかなどの不明な点がどうしても多くなってしまうため、対策技術として有効であるかの判断が難しいことが、課題として挙げられる。このため、概念実証(Proof of Concept)を活用することにより、実際に侵入検知製品を使ってみて、実践的な観点から有効かどうかを判断している事例が見られる。

また、そもそも閉域網で設計・構築・運用されている制御系システムについては、制御ベンダーとの契約により何か問題が起きた時に対応する責任を制御ベンダー側が負っている場合も多く、例え、不正端末の接続検知製品や不正なソフトウェア検知製品のようなシステムへの影響を気にしないで済む製品の導入であったとしても、OT 側にその必要性について理解してもらうには困難を伴う。このため、IT 側、OT 側、制御系システムに関連するすべてのベンダーのそれぞれの担当者が一堂に会する意見交換の場を設定するとともに、重要と考えられるインシデントを想定した上で、当該インシデントが発生した際の対応責任の所在やカバーされる対応範囲をお互いに確認し合い、対応できない事象があることを明確化し認識することで OT 側の担当者の理解を得ている事例が見られる。

(2) 侵入検知製品を選定する際の難しさについては、侵入検知製品の製品選定時において、導入後に想定されるアラートの通知状況が分かりにくいため、社内にアラートの監視、対処などの対応能力を具備し、運用することができるかどうかの判断が難しいことが、課題として挙げられる。このため、導入後に、必要に応じて、アラートの監視、対処などの運用を外部のセキュリティベンダーに委託できるような侵入検知製品や、運用時の負荷を軽減するため、運用時におけるチューニングの更新を自動的に行うことのできる侵入検知製品を選択肢に含めて検討している事例が見られる。

また、上記(1)に関連して、導入した IDS によって、システムの安定的な稼働やパフォーマンスに影響がもたらされ、通常の業務に支障が生じることを一切回避しなくてはならないという可用性確保上の制約を抱えている導入事業者においては、概念実証(Proof of Concept)自体を活用することが難しい状況である。そのような可用性を重

視する導入事業者においては、システムごとに独立した閉域網を構築している場合が多いため、各閉域網内の通信を集約する端末において MAC アドレスと IP アドレス等のデータを検知するだけで一定のセキュリティ上の効果が得られ、かつ可用性確保上の制約や、セキュリティ製品の導入に伴う想定外の挙動がもたらすシステム・業務への影響を気にしないで済む使い方が可能な、ホワイトリスト型による不正端末の接続検知製品や、管理者用端末において許可されたアプリケーションのみを実行するだけで一定のセキュリティ上の効果が得られ、かつ可用性確保上の制約や、メンテナンス時における保守用端末の接続に伴うマルウェアの侵入がもたらすシステム・業務への影響を気にしないで済む使い方が可能な、ホワイトリスト型による不正なソフトウェア検知製品を選択肢に含めて検討している事例が見られる。

(3) 監視場所の設定の難しさについては、OT 側のシステムが IT 側のシステムから完全に独立して構築・運用されており、外部との接続点が、機器のリモートメンテナンス用のインターネット接続のみに限定されている場合など、導入事業者におけるシステムの利用環境や対処すべき脅威・リスクの想定内容はさまざまであり、そのような中で、適切な監視場所の設定とそれに見合う侵入検知製品の選定を行うことが難しいことが、課題として挙げられる。監視場所の設定とそれに見合う侵入検知製品の選定については、システムの利用環境や対処すべき脅威・リスクの想定内容以外にも、システムの可用性担保の要否や、コスト上の制約、資産管理対策の要否など、さまざまな要素が関連するため、それらを総合的に勘案しつつ、適切な監視場所の設定とそれに見合う侵入検知製品の選定を行っている事例が見られる。そのような事例の 1 つとして、OT 用の侵入検知製品を導入して、OT 側のネットワーク内における脅威・リスクの発生状況を一定期間の運用を経て十分確認した後、問題がないと判断された場合に、OT 側のネットワーク内から外部との接続点であるインターネットとの境界へと監視場所を移し、コストを低く抑えるという観点から IT 用の侵入検知製品に置き替えるといった費用対効果に見合う利用方法について検討している事例も見られる。

(4) 端末のマルウェア感染を発端とする社内の侵害拡大に対する対応の難しさについては、端末がマルウェアに感染した際に、そこから社内の他の端末やシステム、ネットワークへの侵害拡大を許してしまい、更なる被害へと発展する可能性があるが、そのような侵害拡大を迅速に発見し対処することが難しいことが、課題として挙げられる。取り分け、ネットワークを跨ぐ侵害拡大の検知については、ネットワーク間における相関分析が必要であるが、そのような相関分析にはある程度の時間を要するため、早期発見が難しいことが、課題として挙げられる。

このため、データ連携機能を付加機能に持つ侵入検知製品を活用して、ウイルス対策ソフトのエージェントとの連携を実現することにより、マルウェア検知後に生成・配布されるシグニチャの更新情報を侵入検知製品側にも取り込み、社内への侵害拡大に対する迅速な検知と、ネットワーク接続の遮断等による迅速な対処に繋げている事例が見られる。また、ボットの検知については、セキュリティベンダーが提供するプラットフォームを介して得られるインテリジェンス情報の中から、ボットに関する必要な情報を侵入検知製品側に取り込みつつ、効果的な検知を実現できるようにしている事例も見られる。さらに、侵入検知製品と連携した SIEM の活用の中で、さらに NDR を組み合わせて利用することにより、ネットワークを跨ぐ侵害拡大の早期発見に繋げる取組について検討している事例も見られる。

その他、HTTPS による暗号化通信に隠されたサイバー攻撃に対応するため、HTTPS による暗号化通信のデコード処理を行い、中身を確認したうえで検知を行うことができる、デコード(エンコード)処理機能を備えた侵入検知製品を選定している事例や、マルウェア検知の基礎的なニーズを満たすサンドボックス型の侵入検知製品を選定している事例も見られる。

(5) 外部からの侵入対策全体を最適化することの難しさについては、監視対象の通信におけるトランザクション特性によって、さまざまな侵入リスクが存在するため、侵入リスクに対して必要となるセキュリティ対策も異なる。このような状況のなかで、侵入検知製品をどのように位置づけ、他の対策製品を含め、どのように外部からの侵入対策全体の最適化を図るのか、どのように運用コストとのバランスを保持するかといった対策全体の方針を決めることが難しいことが、課題として挙げられる。このため、ファイアウォールと侵入検知製品を組み合わせた利用、侵入検知製品と連携した SIEM の活用などの侵入検知の精度の向上について期待できる方策を、監視対象の通信におけるトランザクション特性、侵入リスクに見合うように、適材適所に取り入れている事例が見られる。

(6) 運用体制の構築の難しさについては、侵入検知製品の監視を社内の SOC において実施していたとしても、アラートが通知された場合には、アラート対象機器の制御ベンダーに対して連絡を行い、各拠点(オンサイト)に来てもらい、復旧などの対処を行ってもらう必要があり、各拠点(オンサイト)を巻き込んだ運用体制構築が難しいことが、課題として挙げられる。アラートが通知された場合には、結局、各拠点(オンサイト)の担当者が対応しなければならないため、アラートへの対処に関する運用マニュアルを整備したうえで、各拠点(オンサイト)の担当者に対する必要な教育・演習を行って

いる事例や、同様の取組を、アラート対象機器の制御ベンダーに対しても広げていくことについて検討している事例が見られる。

他方、OT 側のシステム担当者に、IT・セキュリティ教育を実施し、知識を身につけてもらうことの難しさから、OT 側のシステム改修等の稟議に IT 側の担当者を携わらせたり、OT 側のシステム担当者を IT の部署に異動させ、双方の知見を融合させたりするなど、IT 側の担当者に OT 側の業務やシステムを理解させるための取組を積極的に行っている事例が見られる。

また、アラートの監視やアラートが通知された場合の対処には、監視対象の設備やシステム、ネットワーク等を含め業務全般の知識を持つ各システムの管理部署と、サイバーセキュリティチームの双方の関与が不可欠であるが、縦割り組織の弊害等により、各システムの管理部署とサイバーセキュリティチームの有機的な連携を図ることが難しい場合があることが、課題として挙げられる。このため、アラートが通知された場合の対処を担う各システムの管理部署において、担当者レベルで役割分担を設定しておくことが重要であるが、少なくとも、運用の委託ベンダーとの調整役の担当者や、アラートの通知によりインシデントが発覚した際に、政府機関等への報告等を担う社内のサイバーセキュリティチーム（CSIRT）への連絡役の担当者について設定している事例が見られる。

さらに、侵入検知製品の運用には、侵入検知製品に関する専門知識や運用スキルのほか、インシデント対応スキルや業務知識が必要になり、コスト効率性や専門性を考慮すると、それらの保有を導入事業者一社の担当者だけですべて充足することは難しいことが、課題として挙げられる。このため、侵入検知製品に関する専門知識や運用スキルは、侵入検知製品の運用を委託するベンダーで賄い、インシデント対応スキルはセキュリティベンダーで賄うなど、知識やスキルに見合った役割分担を設定することにより、高い専門性を確保しつつ、コスト効率に優れた形での監視・対処を可能にしている事例が見られる。また、侵入検知製品の運用を委託するベンダーやセキュリティベンダーとの役割分担においては、転職が多く、人的流動性が高いというセキュリティ業界の特性を踏まえて、属人的な対応が侵入検知製品の最適な運用体制を構築していく上で制約要因にならないよう業務分掌を設定している事例が見られる。

(7) ステークホルダーとの対応連携の難しさについては、他の事業者が保有する機器を対象としてアラートが通知された場合に、侵入検知製品の運用の委託ベンダーにアラートの内容を確認して、アラート対象機器の制御ベンダーに対して連絡を行い、アラートの内容について説明したうえで、双方の協議のもとチューニングの更新等の適切な対処をできるようにならなければならない。ステークホルダーを多く抱える場合や、

他の事業者において担当者とのコミュニケーションや担当者の対応スキル、担当者の人事異動による引継ぎに関わる問題が生じる場合には、このような双方の対応連携を円滑に行うことが難しいことが、課題として挙げられる。このため、侵入検知製品の運用の委託ベンダーとアラート対象機器の制御ベンダーとの間に立って、アラート通知時の適切な対処について双方の調整を担うことができる担当者を社内に育成している事例が見られる。

(8) 侵入防御製品の運用の難しさについては、侵入検知製品からアラートが通知された際に、不正な侵入を検知した通信の遮断を実行するポリシーについて決めることが難しいことが、課題として挙げられる。このため、侵入検知製品導入後のチューニング期間において、検知のみ実施して遮断を実施しない場合と、検知も遮断も実施する場合の双方について試験運用を行い、双方の比較結果を踏まえて、不正な侵入を検知した通信の遮断を実行するポリシーを調整するといった作業を、侵入検知製品ベンダーと共に繰り返し実践しながら、継続的な改善により、ポリシーの質的向上を図っている事例が見られる。

(9) 侵入検知製品の導入効果を実感することの難しさについては、侵入検知製品の導入後に、アラートが頻繁に通知され、そのほとんどがインシデントと関係がある深刻な重要アラートではないが、すべてのアラートの内容を確認して、チューニングの更新等のフィードバックを実施する作業には一定の工数を要する。安心感は高まるものの、工数の負荷も大きく、何かインシデントが発生するまで、侵入検知製品導入による効果を実感してもらえないという課題が挙げられる。アラートの通知状況によっては、過剰な対策のように受け止められる可能性があるため、侵入検知製品導入による費用対効果について、経営層を含め、社内における十分な理解を得ている事例が見られる。
また、セキュリティ担当者にとって、侵入検知製品の導入により、インシデントを発生させないようにすることは最大の使命であるが、そのような取組の結果としてインシデントが起きずに済むと、経営層に侵入検知製品の導入効果を理解してもらえず、ややもすれば、侵入検知製品の導入が不要なのではないかという間違った方向に話が進みかねない状況が生み出されるという課題も挙げられる。侵入検知製品には、平常時にどれぐらい攻撃を受けていて、侵入検知製品でそれらの攻撃を検知し防御しているという状況を見える化できる機能が備わっているため、このような機能を有効に活用して、経営層に対して、侵入検知製品の導入効果を分かりやすく、かつ定期的に示している事例が見られる。
また、新しい脆弱性が発覚した際の基本的な対処はセキュリティパッチを適用するこ

とから始まるが、サーバーによってはセキュリティパッチの適用前にアプリケーションの検証が必要となり、対処に一定の時間を要する場合がある。侵入検知製品を導入している場合には、脆弱性を突いた不正な侵入の検知が可能になるだけでなく、実際に不正な侵入を検知するまでの猶予の時間をアプリケーションの検証に当てることができるようになる。このように侵入検知製品の導入は必要となる脆弱性への対処を完了させるまでの時間稼ぎに繋がる効果も享受できるため、そのような導入効果を有効に活用している事例も見られる。

以上

用語集

本書における各用語の定義を示す。

用語	説明
ボット	ボット（BOT）は、遠隔操作が可能なマルウェアに感染したコンピュータを意味する。ボット群はボットネット（BOTNET）と呼ばれる。
CSIRT	Computer Security Incident Response Team コンピュータセキュリティインシデントの防止、検知、処理（インシデントハンドリング)、および対応のためのサービスを提供する組織。本書では、事業者内においてセキュリティインシデントの処理および対応に重点をおいたCSIRTを意味する。
PoC (Point of Contact)	セキュリティインシデントの検知や処理の際の窓口。CSIRTのサービスの一つでもある。本書では事業者内POCを意味する。
SIEM	Security Information and Event Management サーバーやネットワーク機器、セキュリティ関連機器、アプリケーション等から集められたログやイベント情報に基づいて、異常があった場合に管理者に通知したり対策を知らせたりする仕組みを意味する。
SOC	Security Operation Center システムやネットワークを監視し、ログやイベント、通信などのデータを分析し、サイバー攻撃の検知を行うサービスを意味する。
侵入検知製品 ベンダー	本書では、侵入検知製品の提供企業の意味に加えて、侵入検知製品の導入ならびにサポートサービスを提供する企業も意味する。
セキュリティベンダー	本書では、SOCサービスなどのサイバーセキュリティの専門サービスを提供する企業を意味する。
概念実証 (Proof of Concept)	新しい技術やシステムを実システム等に導入し、その効果を確かめる実証実験を意味する。
制御ベンダー	本書では、事業者の制御システムと制御対象となる設備・機器を提供する企業を意味する。
設備ベンダー	本書では、不動産・ビル業界において、事業者の制御システムの制御対象となる冷凍機やボイラなど設備・機器を提供する企業を意味する。 昇降機や自動ドアなど中央監視の対象であっても、制御システムを介さず制御を行う機器の場合もある。