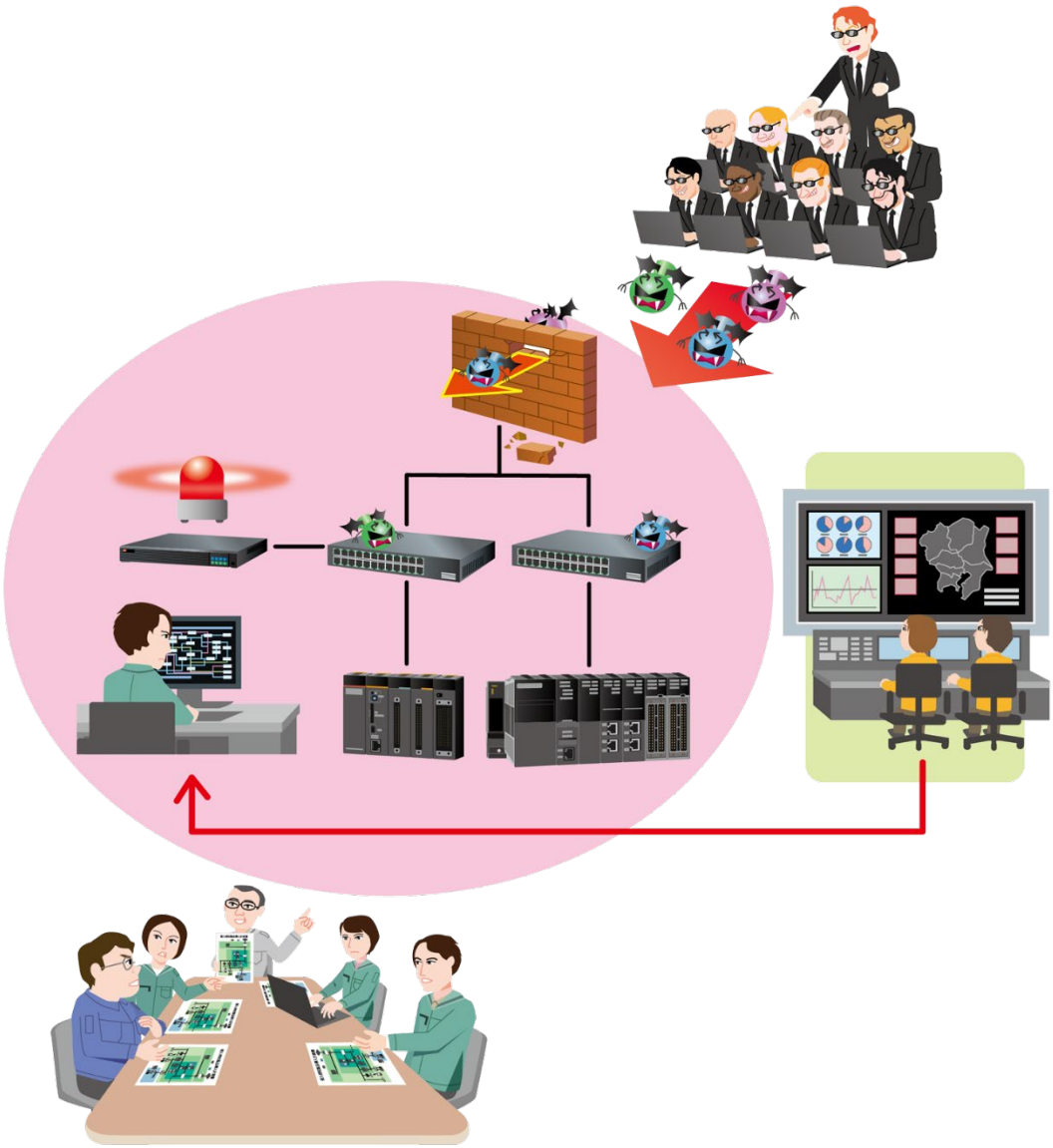
産業用制御システム向け
侵入検知製品等の導入手引書



令和５年６月

IPA
独立行政法人情報処理推進機構
セキュリティセンター

Rev	発行理由	日付
	対象ページ	
0	初版発行	2023/06/19
	全ページ	

目次

第1章　手引き作成の背景と目的

本章では、本手引きの作成の背景や目的・ねらい、構成について説明します。

1.1. 「手引き」作成の背景

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ます。

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す。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等（以下、「侵入検知製品等」とする。）が存在しており、経済産業省が公表する「ビル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」[1]や「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」[2]の中でも必要となる対応策の要件として盛り込まれています。

しかしその一方で、このような侵入検知製品等については、導入方法や運用方法等が分かりにくいため、導入を躊躇する企業が少なくないのが現状です。このため、侵入検知製品等を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考えている企業に対して、導入するにあたって考慮すべき基本事項や導入の進め方、導入後の留意点等、導入・運用に役立つ情報を提供し、導入を支援することが重要となっています。

1.2. 「手引き」の目的・ねらい

本手引きは、これから産業用制御システム向け侵入検知製品等を導入しようと考えている企業における導入を支援することは勿論のこと、産業用制御システム向け侵入検知製品等に対する認知度を向上させることや、産業用制御システム向け侵入検知製品等の普及促進に繋げることをねらいとしています。

[1] 経済産業省が公表する「ビル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」
https://www.meti.go.jp/policy/netsecurity/wg1/building_guideline.html

[2] 経済産業省が公表する「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」
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

1.3. 「手引き」の対象

本手引きは、産業用制御システム向け侵入検知製品等を導入しようと考えている組織、事業者の導入・運用担当者、関係者を想定読者としています。

1.4. 「手引き」の構成

本編と付録により構成されています。付録には、本手引きで用いている主な用語の説明が含まれています。

本手引きの全体構成

構成		概要
本編	第 1 章　手引き作成の背景と目的	本手引きの作成の背景や目的・ねらい、構成について説明しています。
	第 2 章　侵入検知製品等の基本事項	産業用制御システム向け侵入検知製品等の導入検討を行う上でポイントとなる、侵入検知製品等の基礎知識、導入の目的と留意点、導入にあたって考慮すべき基本事項について説明しています。
	第 3 章　侵入検知製品等の導入の進め方	産業用制御システム向け侵入検知製品等の導入の進め方について、「構築」、「試験運用」、「本格運用」の各フェーズにおける検討のポイントを説明しています。
	第 4 章　侵入検知製品等の導入後の留意点	産業用制御システム向け侵入検知製品等の本格運用を開始した後に留意すべき点ついて説明しています。
付録	本手引きで用いている主な用語の説明	本手引きで用いている主な用語の定義について説明しています。

第2章　侵入検知製品等の基本事項

本章では、産業用制御システム向け侵入検知製品等の導入検討を行う上で
ポイントとなる、製品等の基礎知識、導入の目的と留意点、
導入にあたって考慮すべき基本事項について説明します。

2.1. 侵入検知製品等の基礎知識

本手引きで扱う侵入検知製品等は、産業用制御システム(ICS)およびそのネットワークを対象とする不正侵入を検知することを目的とした製品等です。

侵入検知製品は、製品を導入すればすぐに使えるというものでなく、アラートの設定を行う際に何らかの学習が必要なケースが多く、また検知されたアラートやログについて確認・分析することも必要となります。このような必要作業において重要な役割を果たすのが SOC（Security Operation Center）です。SOC の運用については導入企業が自ら行うか、専門的な外部サービスに委託するか決定する必要があります。

侵入検知製品の運用を委託できる専門的な外部サービスは、Managed Security Service（MSS）と呼ばれています。本手引きでは、このようなサービスも含めて扱うため、侵入検知製品ではなく、侵入検知製品等としています。なお、侵入検知製品等については、Network Detection and Response（NDR）と呼ばれることもあります。

ここでは、侵入検知製品等について理解いただくために、侵入検知製品等の種類や特徴を見分けるポイントとなる検知手法と検知方法、提供形態、IDS の形態、導入検討から本格運用までの流れについて説明します。

※IDS は、Intrusion Detection System の略称で、システムおよびそのネットワークを監視し、不正侵入を検知するシステムのことを指します。本手引きでは、IDS の中でも、産業用制御システム(ICS)およびそのネットワーク向けの IDS を対象としています。

2.1.1. 定義

侵入検知製品等の種類や特徴は、侵入の検知手法と検知方法として、どのような手法・方法を実装しているかによって決まります。侵入の検知手法と検知方法の種類を以下に示します。

(1)検知手法の種類

侵入検知製品等に実装される検知手法ついては、大別すると、以下に示す 5 つの手法が存在します。

侵入検知製品等に実装される検知手法の種類
①シグネチャ型 ②ルールベース（仕様ベース） ③ステートフルプロトコル解析 ④振る舞い検知型（量的解析（フローベース）、質的解析（コンテンツベース）） ⑤サンドボックス型

それぞれの検知手法は、検知に用いるデータの比較方法に違いがあります。それぞれの概要について以下に説明します。

検知手法の概要

検知手法	概要
①シグネチャ型	脆弱性を悪用する既知の攻撃に関する一連の脅威となる行動手順パケットをデータベース化し、そこから読み取れる不正な侵入に関わる通信のパターン ＝ シグネチャに基づいて不正な侵入を検知する手法。シグネチャーベースの検知では、観測されたイベント、例えば、不正アクセス等の活動に起因するパケットやログなどとシグネチャとを比較し、イベントがシグネチャに一致した場合にアラートを生成します。シグネチャは、通常、侵入検知製品ベンダーによって提供され、新たな攻撃手法が検出されるたびに更新されます。
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します。
③ステートフルプロトコル解析	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検知します。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ます。
④振る舞い検知型	観測したイベントと監視対象デバイスに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異常な活動（例えば、ワーム、バックドア、ポリシー違反等）であると判断します。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ます。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 2 つの方法があります。

⑤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[3] と呼ばれるコントロールされた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。

注 1）量的解析（フローベース）では、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します。

注 2）質的解析（コンテンツベース）では、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、観測結果に基づいてネットワーク・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、アラートを生成します。

また、いずれの検知手法にも一長一短があり、万能なものはありません。このような特徴を十分考慮の上、適切な検知手法を選定することが重要です。

検知手法の長所と短所

検知手法	長所	短所
①シグネチャ型	● 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す。	● 正規のコマンドを使用した攻撃については、シグネチャが存在しないため、検知できません。 ● 新たな攻撃手法が発見されるたびにシグネチャを更新しなければなりません。
②ルールベース（仕様ベース）	● 既知および未知の脅威の両方に対応可能です。	● 検知精度を高めるために、ICS プロセスに関するホワイトリストを作成する作業に費用と期間を要します。
③ステートフルプロトコル解析	● 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ます。	● 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ません。 ● 一般に受容可能なプロトコルに反しない攻撃（DoS 攻撃など）を検知できません。

[3] 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。

④振る舞い検知型	［量的解析（フローベース）］ ● 新しい攻撃にも対応可能です。 ［質的解析（コンテンツベース）］ ● 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ます。	［量的解析（フローベース）］ ● 検知対象の脅威が、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ます。 ［質的解析（コンテンツベース）］ ● 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ます。 ● 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、検知できません。
⑤サンドボックス型	● 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す。	● 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については、検知が難しい。 ● 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が出来ない可能性があります。

(2)検知方法の種類

侵入検知製品等に実装される検知方法ついては、大別すると、以下に示す 3 つの方法が存在します。

侵入検知製品等に実装される検知方法の種類
①ネットワーク監視型（インライン型、受動型） ②エージェント型 ③ヒストリアン型

それぞれの検知方法は、監視する場所や監視対象のデータに違いがあります。それぞれの概要について以下に説明します。

検知方法の概要

検知手法	概要
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。ネットワークセグメント境界（境界ファイアウォールまたはルータ、VPN サーバ、リモートアクセスサーバ、無線ネットワークなどの接続点付近）に設置される形態が最も一般的です。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の 2 つの形態があります。
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、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ます。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します。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、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、ディスク、プロセッサの使用率）等の情報の収集・前処理を行い、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ます。検知エンジンにおいて、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ます。

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が設置されます。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します。ヒストリアンサーバ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ります。

注 1）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ます。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ます。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す。

注 2）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ます。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ます。

また、いずれの検知方法についても、検知手法と同様、一長一短があり、万能なものはありません。このような特徴を十分考慮の上、適切な検知方法を選定することが重要です。

検知方法の長所と短所

検知手法	長所	短所
①ネットワーク監視型	● 侵入検知に加えて、不正と判断されたパケットを遮断することができます。（インライン型の場合） ● スパンポートやネットワークタップ、ロードバランサを利用して、さまざまな方法でトラフィックを監視することができます。（受動型の場合）	● スイッチに高い負荷がかかっているときに、通信障害が発生すればトラフィックの一部が欠損したり、通信処理が間に合わずにスパニングが一時的に無効になったりする場合があります。（スパンポートを利用した場合） ● 設置の際にネットワークを一時的に停止する必要があります。（ネットワークタップ [4]を利用した場合） ● 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、問題が生じる可能性があります。（ロードバランサ [5] を利用した場合）
②エージェント型	● パケットレベルではなく、イベントレベルで分析するため、信頼性の高い形で不正な侵入を検知することができます。 ● 暗号化された状態でのデータやイベントについても、監視対象のデバイス内で復号化が可能であるため、検知することができます。	● チューニング及びカスタマイズの作業に大きな手間を要します。 ● 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ります。
③ヒストリアン型	● パケットレベルではなく、通信トラフィックの状態の時系列変化のレベルで分析するため、信頼性の高い形で不正な侵入を検知することができます。	● ヒストリアンサーバの設置にコストを要します。 ● ヒストリアンサーバのデータが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ります。

侵入の検知手法と検知方法についてもっと詳しく知りたい方は、IPA が 2022 年 9 月に公表している「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（以下の URL より入手可能）を併せて参考にしてください。

[4] スイッチ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、スイッチを通過する通信トラフィックのコピーをセンサーに分岐させるための装置
[5] ネットワークにかかる負荷を、平等に振り分けるための装置

https://www.ipa.go.jp/security/controlsystem/icsidsreport.html

2.1.2. 提供形態

前述の 2.1.1.で示した検知手法・検知方法を実装した侵入検知製品等については、大別すると、以下に示す 4 つの提供形態が存在します。

侵入検知製品等の提供形態
①IDS ベンダーが提供する「IDS」 ②セキュリティ機器ベンダーが提供する「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」 ③セキュリティサービスベンダーや制御機器・システムベンダーが提供する「IDS 運用監視サービス（MSS）」 ④制御機器・システムベンダーが提供する「IDS 機能を有するネットワーク運用監視サービス」

①については、「IDS」の設計・開発を IDS ベンダーが行っていますが、販売については、直販を行っておらず、代理店経由となる場合が多いです。

また、構築・導入や運用監視については、代理店が行う場合のほか、導入企業が自ら行う場合や、後述する「IDS 運用監視サービス（MSS）」を提供するセキュリティサービスベンダーや制御機器・システムベンダーが行う場合などが存在します。

なお、国内ベンダーの中には、「IDS」を直販したり、構築・導入についてもプロフェッショナルサービスとして提供したりしているベンダーもいます。さらに、運用監視まで提供しているベンダーもいますが、そのようなベンダーは、①と③の 2 つの位置づけを持つベンダーと言えます。

導入企業がベンダーに対して求める 4 つの提供価値（IDS の設計・開発、販売、構築・導入、運用監視）に関して、IDS ベンダーが提供する「IDS」においてどの程度提供されているか、その提供度合いを以下の 3 段階で示します。

◎：ほぼすべてのベンダーがその価値を提供している

△：一部のベンダーのみがその価値を提供している

×：ほぼすべてのベンダーがその価値を提供していない

①IDS ベンダーが提供する「IDS」における提供価値への対応（状況）

設計・開発	販売	構築・導入	運用監視
◎	△～×	△～×	×

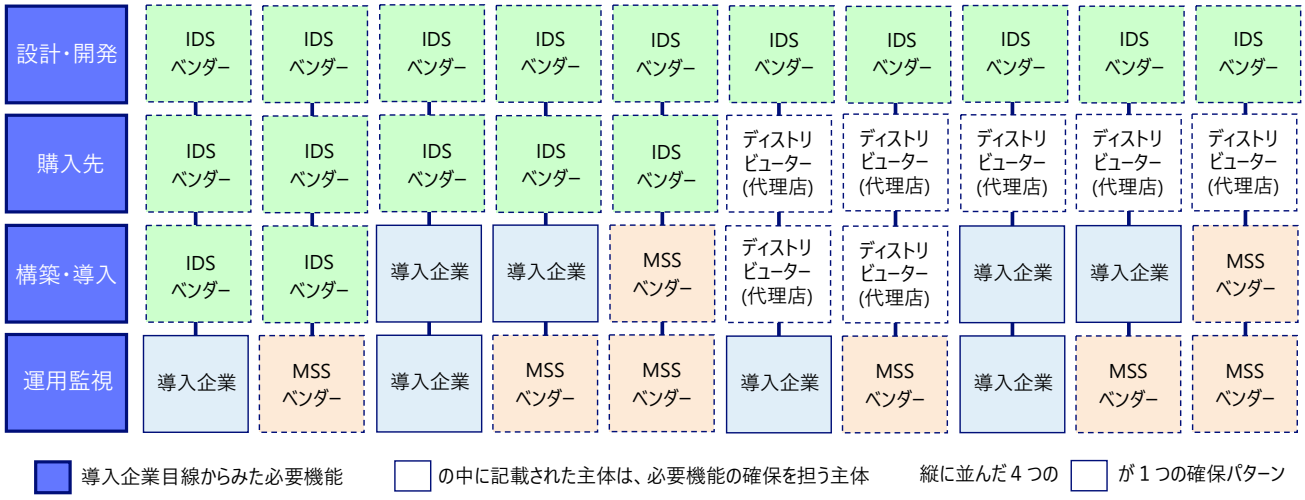
注）△は国内ベンダーの一部が該当

他方、①を利用する導入企業においては、構築・導入について、自ら実施するか、代理店や③の提供ベンダーに依頼して賄うかを判断しなければなりません。

また、運用監視についても、自ら実施するか、③の提供ベンダーに依頼して賄うかを判断しなければなりません。

構築・導入や運用監視について自ら実施する場合には、サイバーセキュリティに関わる専門知識・技術、運用スキル・ノウハウを有する人材を確保し、①の導入・運用担当者として配置することが必要となります。

導入企業目線からみた必要機能と
導入企業が①IDS ベンダーが提供する「IDS」を利用する際の必要機能の確保パターン



②については、「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」の設計・開発をセキュリティ機器ベンダーが行っていますが、販売については、直販を行っておらず、代理店経由となる場合が多いです。

また、構築・導入や運用監視については、代理店が行う場合のほか、導入企業が自ら行

う場合や、後述する「IDS 運用監視サービス（MSS)」を提供するセキュリティサービスベンダーや制御機器・システムベンダーが行う場合などが存在します。

なお、セキュリティ機器ベンダーの中には、直販していなくても、代理店やパートナーとなっている「IDS 運用監視サービス（MSS)」を提供するセキュリティサービスベンダーや制御機器・システムベンダーと協働して、構築・導入の支援を行っているベンダーもいます。

②セキュリティ機器ベンダーが提供する「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」における提供価値

設計・開発	販売	構築・導入	運用監視
◎	×	△～×	×

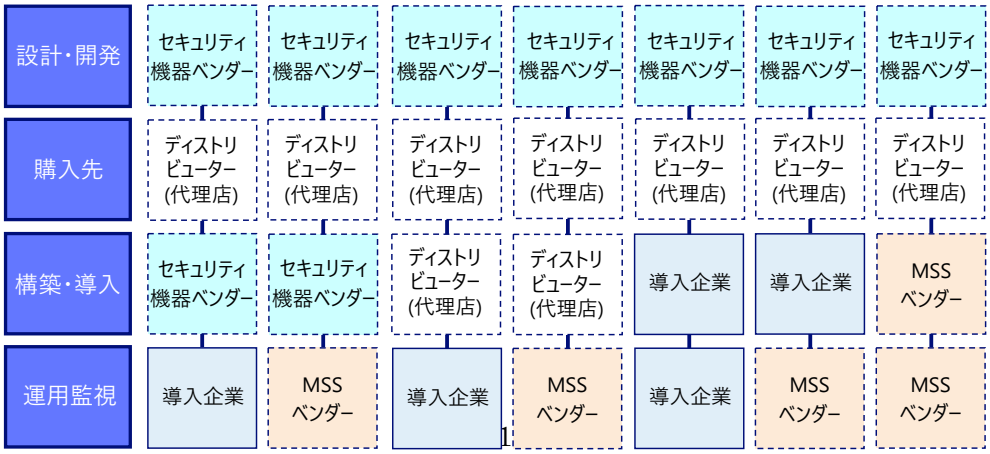
注）△は代理店や、「IDS 運用監視サービス（MSS)」を提供するセキュリティサービスベンダーや制御機器・システムベンダーと協働して構築・導入を支援している一部のベンダーが該当

他方、②を利用する導入企業においては、構築・導入について、自ら実施するか、代理店や③の提供ベンダーに依頼して賄うか（②のセキュリティ機器ベンダーが協働して実施する場合を含む）を判断しなければなりません。

また、運用監視についても、自ら実施するか、③の提供ベンダーに依頼して賄うかを判断しなければなりません。

構築・導入や運用監視について自ら実施する場合には、①と同様、サイバーセキュリティに関わる専門知識・技術、運用スキル・ノウハウを有する人材を確保し、②の導入・運用担当者として配置することが必要となります。

導入企業目線からみた必要機能と導入企業が②セキュリティ機器ベンダーが提供する「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」を利用する際の必要機能の確保パターン



③は、侵入検知製品等を設置して、運用監視を行うサービスです。

③については、一部のセキュリティサービスベンダーや制御機器・システムベンダーにおいて「IDS」の設計・開発を行っている場合もありますが、ほとんどの場合は、「IDS」の設計・開発を行っていません。ただし、「IDS」の設計・開発を行っている場合でも、自社の「IDS」にこだわらず、他社の「IDS」も含めて、利用している場合が多いです。販売については、直販の場合や、代理店経由となる場合が存在します。

また、構築・導入については、セキュリティサービスベンダーや制御機器・システムベンダーが直接行っていますが、代理店が行う場合も存在します。

運用監視については、セキュリティサービスベンダーや制御機器・システムベンダーが直接行っています。

なお、前述したとおり、③の提供ベンダーの中には、「IDS」の設計・開発を行っているベンダーもいますが、そのようなベンダーは、①と③の 2 つの位置づけを持つベンダーと言えます。

③セキュリティサービスベンダーや制御機器・システムベンダーが提供する「IDS 運用監視サービス（MSS）」における提供価値

設計・開発	販売	構築・導入	運用監視
×	△～×	◎～△	◎

注 1）販売の△は①や②の提供ベンダーの代理店となっている一部のベンダーが該当

注 2）構築・導入の△は、①や②の提供ベンダーやその代理店が該当

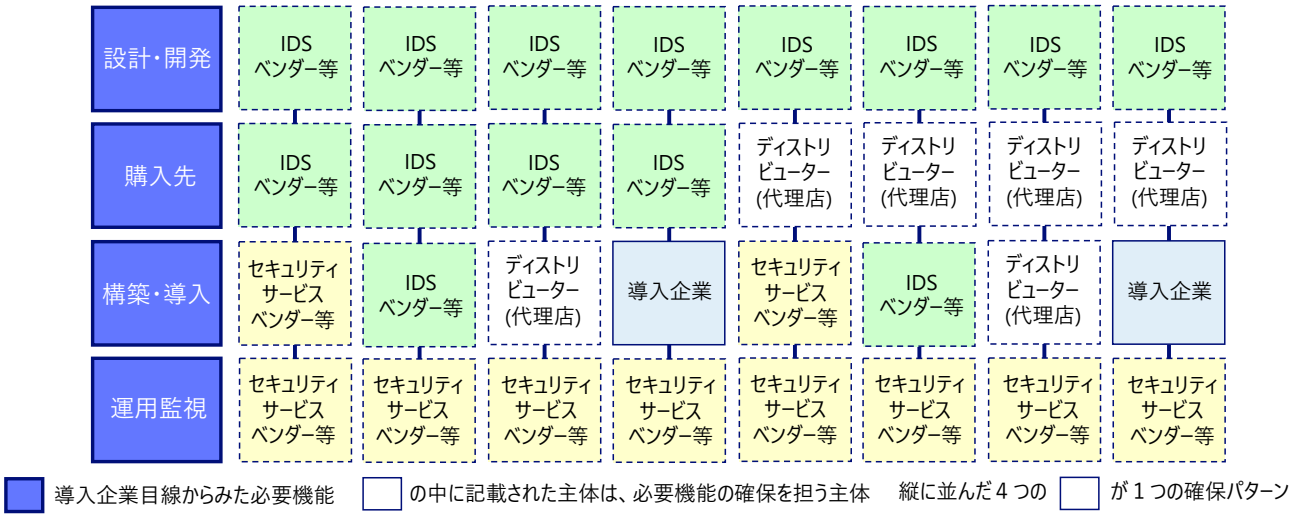
他方、③を利用する導入企業においては、①または②を調達しなければなりません。そのうえで、①または②の提供ベンダー（またはその代理店）からの調達を自ら実施するか、③の提供ベンダーに依頼して賄うかを判断しなければなりません。なお、③の提供ベンダーが、①または②の提供ベンダーの販売代理店となっているケースは多いです。

また、構築・導入についても、自ら実施するか、調達先となる①また②の提供ベンダー（またはその代理店）に依頼して賄うか、③の提供ベンダーに依頼して賄うかを判断しなければなりません。

なお、③の提供ベンダーの中には、自社で熟知している特定のベンダーが提供する①ま

たは②しか運用監視対象として扱わないベンダーもいますので、①または②の調達を自ら実施する場合には、注意が必要です。

導入企業目線からみた必要機能と
導入企業が③セキュリティサービスベンダーや制御機器・システムベンダーが提供する
「IDS 運用監視サービス（MSS）」を利用する際の必要機能の確保パターン



④は、既に保守契約を締結し、産業用制御システムの運用監視を行っている中で、その一環または別契約として、センター側で運用監視を通じて取得された各種情報・ログを分析し、侵入リスクの検知を行うサービスです。

④については、運用監視について、制御機器・システムベンダーが直接行う場合や、制御機器・システムベンダーと導入企業が一緒になって行う場合が存在します。

④制御機器・システムベンダーが提供する「IDS 機能を有するネットワーク運用監視サービス」における提供価値

設計・開発	販売	構築・導入	運用監視
—	—	—	◎～△

注）△は導入企業と協働して行う場合が該当

2.1.3. IDS の形態

前述の 2.1.2.で示した IDS ベンダーが提供する「IDS」の形態については、大別すると、単独アプライアンス型（ハードウェアアプライアンスをスイッチ等に外付けで設置するタイプの製品）、統合アプライアンス型（ハードウェアアプライアンスがネットワーク機器（スイッチやファイアウォール等）として統合され、一体的に提供されるタイプの製品）、ソフトウェア型（サーバやスイッチ等にソフトウェアをインストールするタイプの製品）の 3 つの形態が存在します。

このうち、単独アプライアンス型の IDS は、外付けでの設置となり導入しやすいため、使用している導入企業が多いです。

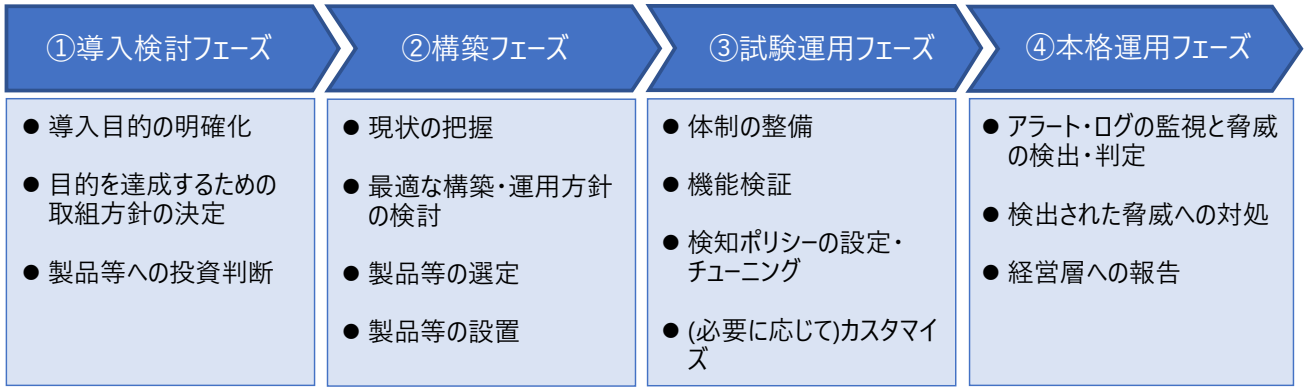
他方、統合アプライアンス型やソフトウェア型の IDS は、スイッチ上等でソフトウェアを起動できるため、外付けのアプライアンスが不要となり、管理対象を減らせることは勿論のこと、スイッチ等を格納する制御盤においても省スペース化を実現でき、サイズの最適化を図ることができます。また、制御盤のサイズの最適化は、生産コストの低減にも繋がります。

一方で、そのようなソフトウェア型の IDS を使用する場合には、スイッチ等における処理が過負荷の状態に陥らないよう、IDS 専用の CPU を搭載する高性能のスイッチ等を使用するなど、注意が必要です。

2.1.4. 導入検討から本格運用までの流れ

侵入検知製品等を使う際には、①導入検討、②構築、③試験運用、④本格運用の 4 つのフェーズを経るのが一般的です。

侵入検知製品等を使う際の導入検討から本格運用までの流れ



①導入検討フェーズでは、導入の目的や目的を達成するための取組方針を明らかにした上で、経営層に対して、侵入検知製品等の導入・運用が必要であることの妥当性や、侵入検知製品等の導入・運用にかかる予算が適正であることの妥当性、侵入検知製品等の導入・運用で得られるプラスアルファの効果等を提示し、投資判断を仰ぎます。(詳細は後述の 2.2.及び 2.3.を参照)

②構築フェーズでは、資産、通信、脆弱性の観点から産業用制御システムの現状を把握し、それを踏まえて最適な構築・運用方針について検討するとともに、当該方針に則って、適切な製品等の選定や設置を行い、侵入検知製品等を運用できる状態にセットアップします。(詳細は後述の 3.1.を参照)

③試験運用フェーズでは、本格運用を始めてから不備が生じないよう、一定期間内での試験的な運用を通じて、侵入検知製品等の運用体制や監視・検知ポリシーについての具体的な詰めや、侵入検知製品等の機能検証を行い、運用の実効性を高めます。(詳細は後述の 3.2.を参照)

④本格運用フェーズでは、侵入検知製品等から通知されるアラートを監視し、通知されたアラートの内容や関連する各種ログの内容を見て、不正な侵入等の脅威の検出によるものか、誤検知によるものかを分析し判定します。また、脅威が検出された場合には、必要となる適切な対処方法を検討し実践するとともに、経営層に対して適切なタイミングでそれらの一連の状況や経過に関する報告を行います。(詳細は後述の 3.3.を参照)

※誤検知には、偽陽性（false positive）として、利用者の正常な状態の通信トラフィックが、「異常」として誤って判断されるものに加え、本来検知対象ではない通信トラフィックまで「異常」として誤って判断される過検知も含まれます。

2.2. 侵入検知製品等の導入の目的と留意点

侵入検知製品等を導入する際には、先ず導入の目的を明確しなければなりません。導入の目的が明確になっていなければ、導入企業にとってふさわしい侵入検知製品等を適切に選定することや、効果的な導入を行うことはできません。

また、導入の目的が明確になり、次の段階として、侵入検知製品等の選定を行う際には、運用に係る負荷や、ネットワークやシステムのパフォーマンスへの影響、付加機能の活用、導入・運用に係るトータルコストなど、さまざまな留意点について考慮しなければなりません。留意点が十分に考慮されないまま、侵入検知製品等を導入しても効果的な運用を行うことはできません。

このような考え方に基づいて、侵入検知製品等の導入の目的と留意点について参考となる事例を以下に示す。

2.2.1. 導入の目的

産業用制御システム向け侵入検知製品等は、産業用制御システムに対する侵入検知手段であり、さらに付加機能や他の対策製品等との連携を効果的に活用すれば、セキュリティリスクのより一層の低減に役立ちます。

産業用制御システム向け侵入検知製品等の導入・運用に向けては、達成すべき目的を明確にすることが必要です。産業用制御システム向け侵入検知製品等の一般的な目的の例としては、以下のことが挙げられます。

(1)対策目標の観点からみた導入の目的

これまでの産業用制御システムは、閉域網と専用の機器や通信プロトコルで構成されていたため、サイバー攻撃を受けにくいとされてきたが、近年の DX（デジタルトランスフォーメーション）の推進により、社内ネットワークから産業用制御システムへの外部接続や、遠隔監視や遠隔保守等の産業用制御システムへのリモート接続を行う機会が増加した結果、産業用制御システムがサイバー攻撃にさらされる機会が増えてきています。

一方で、産業用制御システムには、「リアルタイムでの制御」、「長期継続的な運用」といった厳しい条件を要求されているものが多く、このような条件を満たすため、ネットワークやシステムのパフォーマンスに悪影響をもたらす可能性がある要素やシステム停止に繋がる可能性がある要素を取り除く、あるいは新しい要素の追加による変更を回避

または最小限とすることに重点を置いた運用を基本としています。

万が一、このようなシステムがサイバー攻撃による被害を受ければ、サービス停止や事業停止を招くなど、国民生活や企業経営に少なからぬ影響を与え、社会に大きな混乱がもたらされることが懸念されています。

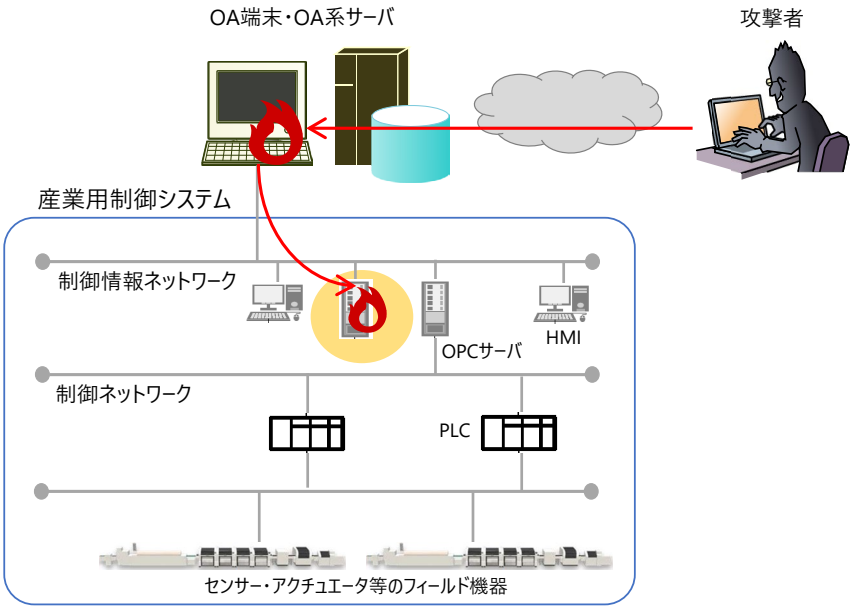
このため、産業用制御システムをサイバー攻撃から守るための対策手段の１つとして、産業用制御システム向け侵入検知製品等を活用する機会が増えています。

以下のような導入目的を有する企業にとって、「IDS」や「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等)」は有用な対策手段となっています。

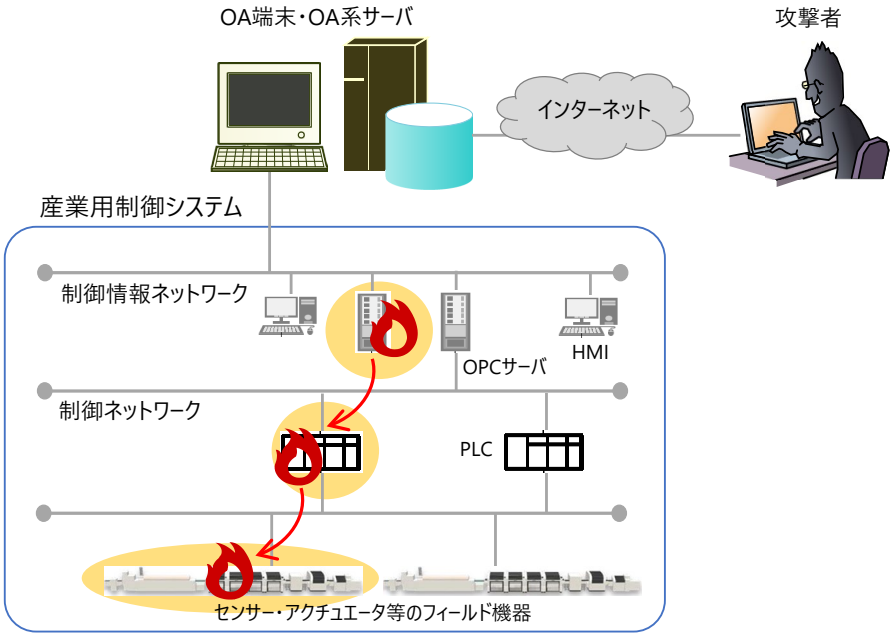
対策目標の観点からみた導入の目的

①IT 環境から OT 環境への不正な侵入を防ぐ

②OT 環境への侵入を許した脅威が OT 環境にもたらす被害の発生・拡大を防ぐ



IT 環境から OT 環境への不正な侵入



OT 環境への侵入を許した脅威が OT 環境にもたらす被害の発生・拡大

①を導入目的とする企業においては、産業用制御システム向け侵入検知製品等の中でも特に、既知の脅威に対する対策、IT 環境と OT 環境の境界防御対策として有用である「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」を活用している場合が多いです。

②を導入目的とする企業においては、IT 環境を経由した不正な侵入や、IT 環境を経由しない OT 環境内での不正な侵入といった脅威が想定されるとともに、目的を達成するための取組方針において、以下のようなレベル感の違いが見られます。

②の導入目的を達成するための取組方針

1）OT 環境における脅威検知の継続的な運用に進む前に、OT 環境における守るべき重要資産の特定や、脆弱性等のリスクアセスメントとその結果明らかになったリスクに対する改善といった予防対策を実施する

2）OT 環境のネットワークセグメント間の境界付近において、他の環境からの既知の脅威を対象とした侵入検知・防御対策を実施する

3）OT 環境内の全般において、上記 2）で示した既知の脅威に加えて、未知の脅威や、保守業者が持ち込む保守用の USB やパソコンを介したマルウェア感染、内部犯行やオペレーションミス等による内部脅威といった OT 環境内で想定されるあらゆる脅威を対象とした脅威検知対策を実施する

このようなレベル感の違いは、侵入・脅威を検知したとしても、前述したような厳しい条件の制約により、通信の制限や特定の機器の隔離等の対処が難しく、採り得る対処がかなり限定されることから、予防対策を重視せざるを得ないという考え方や、運用に係る負荷やネットワーク・システムへの対応力の高低で監視・検知対象とする脅威の範囲を判断するという考え方によるものです。

上記 1）の予防対策においては、資産可視化機能や脆弱性アセスメント機能など、予防対策として必要となる機能が付加機能として備わっている「IDS」が主に活用されています。

上記 2）では、先ず最初に IT 環境と OT 環境の境界付近における侵入検知・防御対策

を実施し、その後、対策運用に求められる知識・スキルの獲得や体制の整備が進んでから対策を拡充し、OT 環境のネットワークセグメント間の境界付近における侵入検知・防御対策を実施するといった形で段階的に対策を行う場合が多い。このような既知の脅威に対する侵入検知・防御対策においては、「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等)」が主に活用されています。

上記 3）の OT 環境内で想定されるあらゆる脅威に対する脅威検知対策においては、シグネチャ型やルールベース（仕様ベース)、振る舞い検知型など、複数の検知手法を組み合わせた高度な相関分析が必要となることから、そのような機能が備わっている「IDS」が主に活用されています。なお、「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等)」の中には、「IDS」と比較しても同等またはそれに匹敵するレベルで複数の検知手法を組み合わせた高度な相関分析ができる製品が存在します。そのような製品も、「IDS」と同じように活用されています。ただし、「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等)」においては、保守業者が持ち込む保守用の USB やパソコンを介したマルウェア感染に十分に対応できないため、注意が必要です。

なお、②を導入目的とする企業においては、②の導入目的を実現する上で、その前提として①の導入目的を実現することが必要不可欠となっています。そのため、「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等)」と「IDS」を併用して活用し、①、②の双方の導入目的を実現している場合があります。このような使い方を意識して、「IDS」には、「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等)」との連携機能が付加機能として備わっている場合が多いです。

(2)専門的な外部サービスの利用目的

産業用制御システム向け侵入検知製品等を円滑かつ効果的に導入・運用するには、導入企業において、構成する機器やネットワークを含む産業用制御システムとサイバーセキュリティの双方に関わる専門知識・技術、運用スキル・ノウハウを兼ね備えた人材を確保し、侵入検知製品等の導入・運用担当者として配置することが必要です。

その一方で、侵入検知製品等の導入・運用担当者を育成したり、労働市場から獲得したりする際には、教育コストや採用コストがかさむことから、現実的には内製による人材の確保が難しくなっています。このため、産業用制御システム向け侵入検知製品の導入・運用を扱う専門的な外部サービスの利用について検討することも有用な対策手段の 1 つとなっています。

以下のような導入目的を有する企業にとって、「IDS 運用監視サービス（MSS)」や「IDS 機能を有するネットワーク運用監視サービス」は有用な対策手段となっています。

専門的な外部サービスの利用目的

①産業用制御システムの停止やパフォーマンスへの悪影響といった不測の事態の回避を万全に行ったり、リスク分析に基づき監視・検知対象とする事象を特定した上で監視・検知方法の最適設計を行ったりするなど、OT 環境の現場の状況に見合った実効的な侵入検知対策を実施したい。

②ランサムウェア感染や標的型攻撃に代表されるような攻撃手口が複雑化かつ巧妙化する脅威に対応できるよう、高度な解析に基づく侵入検知対策を実施したい。

①を利用目的とする企業においては、産業用制御システム向け侵入検知製品等の中でも特に、構成する機器やネットワークを含め産業用制御システムの構築・運用全般について熟知している、制御機器・システムベンダーが提供する「IDS 運用監視サービス（MSS)」や、「IDS 機能を有するネットワーク運用監視サービス」を活用している場合が多いです。

①を利用目的とする企業の中には、「IDS」の導入がもたらす産業用制御システムの構成や設定等の変更によって、産業用制御システムに対し何らかのリスク・影響が及ぶことを極力回避したいと考える企業が多いです。

このような意向を踏まえて、制御機器・システムベンダーの中には、以下に示すような工夫により、リスク・影響を回避・軽減しているベンダーもいます。

○独自の検証基盤を構築・運用して、「IDS」の導入前にコンパチビリティ検証等の産業用制御システムへの影響評価を実施し、異常が起きないことを確認した上で実環境に導入する

○「IDS 運用監視サービス（MSS)」の監視対象を、熟知する自社製品の産業用制御システムのみに限定し、他社製品の産業用制御システムを対象外とする形でサービスを提供する

また、①を利用目的とする企業の中には、既に産業用制御システムの運用保守契約を締結しているベンダーに対し、運用保守契約の一環として、当該システム上で実際に起

こり得るリスク事象（非定常状態となるリスク事象）の検知を、その発生要因（故障、人為的ミスによる事故、セキュリティインシデント）の切り分けを含めて依頼したいと考える企業が多いです。

このような意向を踏まえて、リスク分析を実施し、監視・検知対象とすべきリスク事象（非定常状態となるリスク事象）を特定するとともに、当該リスク事象の発生要因の特定に必要となる最適な情報とその収集方法を提案するといった、現場の状況に見合った監視・検知方法の最適設計に注力しているベンダーもいます。

このように、①を利用目的とする企業においては、ベンダーにおけるリスク回避・軽減の考え方やそれを支える産業用制御システムの構築・運用に対する習熟度を見極めることが特に重要になります。

②を利用目的とする企業においては、産業用制御システム向け侵入検知製品等の中でも特に、サイバーセキュリティ対策の導入・運用全般について熟知し、信頼性の高いSOC基盤と高度な解析スキルを持つアナリストを保有している、セキュリティベンダーが提供する「IDS運用監視サービス（MSS)」を活用している場合が多いです。

②を利用目的とする企業の中には、侵入検知製品以外にも、「ファイアウォール」や「マルウェア検知製品」、「URL フィルタリング製品」、「サンドボックス製品」など、さまざまなセキュリティ対策機器を複合的に導入・運用することにより、侵入リスクの高度な検知・防御を行いたいと考える企業が多いです。

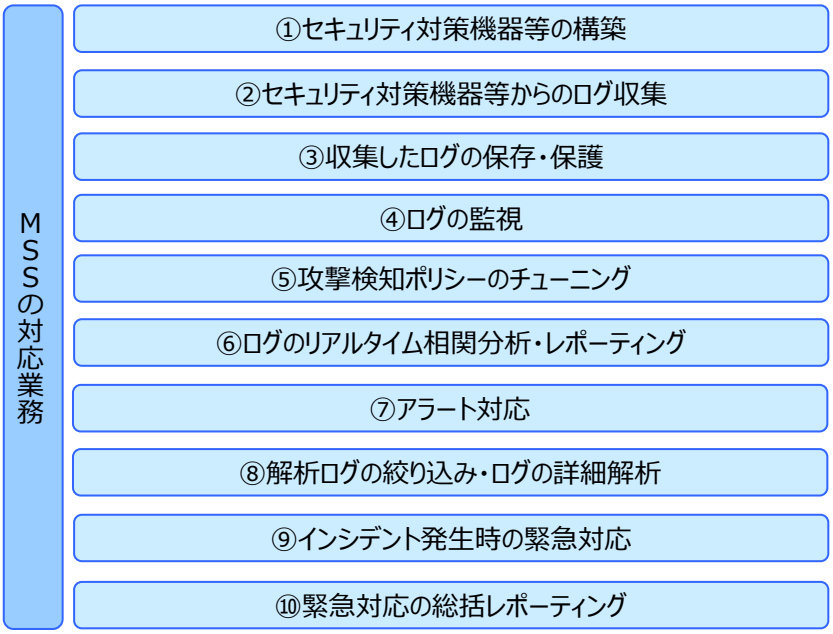
このような意向を踏まえて、セキュリティベンダーの中には、以下に示すような工夫により、侵入リスクの高度な検知・防御を実現しているベンダーもいます。

○高度な解析手法として、ベンダー独自の脅威インテリジェンスを活用したり、複数の異なる機器等から出力されるログのリアルタイム相関分析やログの詳細解析を実施したりすることで検知精度を向上させるとともに、インシデントが検知された場合に、原因究明調査や被害・影響範囲調査、被害拡大防止策の検討等といった緊急対応も併せて実施する

○導入企業が既に導入済みのセキュリティ対策機器を含め、多様な機器ベンダーが提供するセキュリティ対策機器の統合的な運用・監視を行う

○海外の複数拠点・SOC間の時差を利用して、24時間365日途切れることなく、アラート・ログの監視や脅威の検出・判定、アラートの通知を行う

このように②を利用目的とする企業においては、ベンダーにおける解析手法や対応業務、取扱い可能なセキュリティ対策機器のカバー範囲の広さを見極めることが特に重要となります。



IDS 運用監視サービス（MSS）における対応業務

産業用制御システム向け侵入検知製品の導入・運用を扱う専門的な外部サービスを利用することで、自社で賄えない必要リソースを補いながら、導入の目的を実現することは有効です。

2.2.2. 導入の留意点

産業用制御システム向け侵入検知製品等の導入・運用には、侵入リスクに対する対策といったメリットがありますが、「担当者の運用に係る負荷が大きくなる可能性がある」や「ネットワークやシステムのパフォーマンスに悪影響をもたらす可能性がある」、「予算化に向けたハードルが高くなる可能性がある」等といった注意点もあるため、しっかりと確認しておくことが必要です。

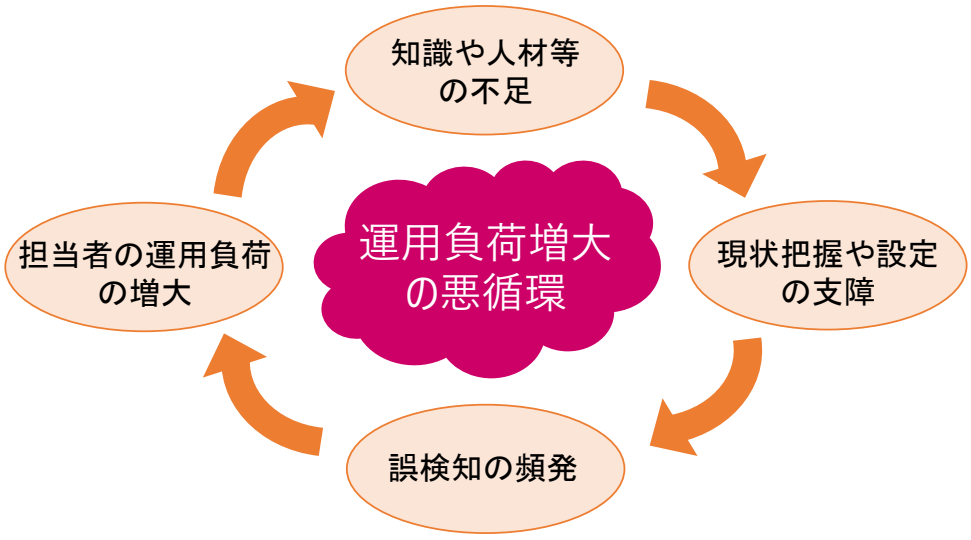
(1) 知識や人材等のリソースの考慮

産業用制御システムとサイバーセキュリティの双方に関わる専門知識・技術、運用ス

キル・ノウハウの獲得とそのような専門性を兼ね備えた人材の確保は、産業用制御システム向け侵入検知製品等を円滑かつ効果的に導入・運用する上で重要な課題となります。

このような課題を克服しないまま侵入検知製品等の導入・運用を進めた場合、監視対象の産業用制御システムの構成や通信等に関する情報の正確な把握や、検知のベースライン（しきい値）の適切な設定に支障が及ぶおそれがあります。

また、その結果として誤検知やアラート管理の非効率等の問題が生じることが懸念され、担当者の運用に係る負荷が大きくなることに、十分留意することが必要です。



担当者の運用負荷の増大に繋がる悪循環の構図

(2)ネットワークやシステムのパフォーマンスへの影響の考慮

産業用制御システム向け侵入検知製品等は、効果的な手段であるが、次のような場合において、産業用制御システムのパフォーマンスに影響が生じることがあるので、十分留意することが必要です。

産業用制御システムのパフォーマンスに影響が生じる可能性がある事例

①監視対象ホストに直接エージェントをインストールするエージェント型の侵入検知製品等を利用する場合、インストールされたエージェントの動作によって、既存アプリケーションの動作の不具合やネットワーク遅延が発生する可能性があります。

②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場合に、ネットワークタップの設置や障害対応のために、ネットワークを一時的に停止する必要があります。

③脆弱性を持つ OT の機器等の検出・特定のため、侵入検知製品から OT の機器等に接続を試みるアクティブモードでの通信や、当該通信を用いて OT の機器等の稼働状況や詳細な情報を取得するポーリングを使用する場合に、情報の取得頻度や量、対象となる OT の機器の台数の多寡によっては、ネットワークへの負荷が高まる可能性があります。

(3)費用と効果の考慮

達成すべき目的と得られる効果、必要となる費用について検討した上で、相互に比較しながら、自社にとって最適な形態で産業用制御システム向け侵入検知製品等の導入・運用を進めることが必要です。

2.3. 侵入検知製品等の導入にあたっての基本事項

導入の目的と目的を達成するための取組方針が決まった後、次の段階として、導入する侵入検知製品等とその運用方法を決める際には、前述の 2.2. で示したさまざまな留意点があるので、多様な観点による総合的な判断が求められます。

具体的には、運用に係る負荷の軽減、システムパフォーマンスへの影響の抑制、付加機能の効果的な活用、投資判断・予算化に向けた調整の円滑化といった多様な観点について検討した上で、導入企業が重視する条件に見合う運用方法に対応した適切な侵入検知製品等を選定し導入することが基本となります。

このような考え方に基づいて、侵入検知製品等の導入にあたっての基本事項について参考となる事例を以下に示します。

ただし、侵入検知製品等の導入の進め方および導入後の留意点については、それぞれ後段の第 3 章と第 4 章に記述していますので、併せて参照頂けると幸いです。

2.3.1. 運用に係る負荷の軽減

(1)検知ポリシーの設定・チューニング作業の省力化

ルールベース（仕様ベース）や振る舞い検知型の侵入検知製品を効果的に運用するためには、産業用制御システムの構成やトラフィック特性に見合った検知ポリシーの設定・チューニング作業が必要です。

検知ポリシーの設定・チューニング作業においては、異常な状態の通信トラフィックの定義を狭く絞り込み過ぎると、正常な状態の通信トラフィックが「異常」として扱われる誤検知リスク（偽陽性）の発生率は低くなる一方で、正常な状態の通信トラフィックの中に、異常な状態の通信トラフィックが含まれる検知漏れリスク（偽陰性）が高くなります。反対に、異常な状態の通信トラフィックの定義を広く取り過ぎると、正常な状態の通信トラフィックが「異常」として扱われる誤検知リスク（偽陽性）の発生率は高くなる一方で、正常な状態の通信トラフィックの中に、異常な状態の通信トラフィックが含まれる検知漏れリスク（偽陰性）が低くなります。

このような特性を踏まえつつ、検知ポリシーが十分に機能しなければ、正常な状態の通信トラフィックを「異常」として、またその逆に異常な状態の通信トラフィックを「正常」として扱い、誤検知・検知漏れに繋がるという悪循環が生み出されます。その

一方で検知ポリシーの設定・チューニング作業において十分な検知精度を実現するには煩雑性や困難性を伴います。次のような主な場面において、検知ポリシーの設定・チューニング作業が必要になります。

検知ポリシーの設定・チューニング作業が必要となる主な場面

①侵入検知製品の導入時において、産業用制御システム上で一定期間中に日々やりとりされる通信トラフィックを分析して、正常な状態の通信トラフィックを定義し、検知のベースライン（しきい値）を設定するが、当該ベースラインには季節や周期による変動、突発事象等による誤差が内包されます。このため、侵入検知製品の試験運用の中で、当該ベースラインの誤差に起因して発生する誤検知・検知漏れの発生回数・頻度が許容範囲となるまで、当該ベースラインを修正する必要があります。

②産業用制御システムの運用面の利便性を優先するという考え方により、侵入検知製品の導入時において、一部のアラートを意図的に許容する場合があります。このような場合には、アラートが上がらないように検知ポリシーの設定・チューニングを行う必要があります。

③侵入検知製品の運用開始後、産業用制御システム構成の変更に起因して、アラートが上がる場合があります。このような場合には、都度、検知ポリシーの設定・チューニングの再調整を行う必要があります。

④侵入検知製品の運用開始後、新たに発見された脅威や攻撃手法に対して、これまでの検知ポリシーが十分に機能しない場合があります。このような場合には、都度、検知ポリシーの設定・チューニングの再調整を行う必要があります。

特に専門性が不足している導入企業においては、このような煩雑性・困難性を踏まえ、検知ポリシーの設定・チューニング作業を支援する外部委託先の活用や、機械学習を用いて自動的にベースラインの初期設定を行う機能が備わっている「IDS」の活用を行うことにより、検知ポリシーの設定・チューニング作業に係る運用担当者の負荷を軽減することが必要です。

通常、検知ポリシーの設定・チューニング作業においては、一定期間内（1か月弱～3か月以内が1つの目安となる。但し作業期間は検知手法等により異なる。）で発生したアラートについて集計されたものをもとに、導入企業が1つ1つのアラートの内容を

確認して、チューニングが必要であるか否かを判断していく作業になります。検知のベースラインの初期設定の直後は、アラートの発生数が膨大になりがちであるため、導入企業の運用担当者の負荷が増大します。検知ポリシーの設定・チューニング作業を支援する外部委託先においては、導入企業に対して、効率的な確認作業を行うために必要な観点（例えば、新しい機器のネットワーク接続や、DHCP 上での IP アドレスの変更、ホスト名の変更等といったシグネチャ単位でアラートをまとめる等）を提示できるため、導入企業の運用担当者の負荷を軽減することができます。

参考情報 1　**運用開始後、検知ポリシーの設定・チューニングの再調整にも機械学習は使えるか？**

ベースラインの初期設定完了後、検知の精度を向上しながら、「IDS」を運用するためには、通常、人手による検知ポリシーの設定・チューニングの再調整作業が必要になりますが、このような再調整作業についても、継続的な機械学習を用いて自動的に行うことができる「IDS」が提供されています。

このような「IDS」を利用するにあたっては、提供ベンダーが持つ機械学習に対する知識や技術力などを含め、提供ベンダーが継続的な機械学習を用いることの妥当性について十分確認する必要があります。

また、機械学習については、自動学習状態にする前後で、検知傾向が変わる可能性があるため、注意が必要です。

さらに、侵入リスクの高度な検知に対し特段強いこだわりがなければ、検知ポリシーの設定・チューニング作業の手間を省力化できるシグネチャ型の「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等)」を活用するのも一案です。

(2)侵入リスクの監視と脅威検出・判定の省力化

侵入リスクの監視と脅威検出・判定を行うための専門組織である SOC（Security Operation Center）の運用が必要となります。

SOC（Security Operation Center）の構築形態は、侵入検知製品等の導入企業内に構築する形態や、侵入検知製品等の提供ベンダー内に構築する形態などさまざまですが、特に専門性が不足している導入企業においては、SOC の構築・運用がセットとなっている「IDS 運用監視サービス（MSS)」や「IDS 機能を有するネットワーク運用監視サービス」を活用することが有用です。

また、侵入検知製品等の導入企業内にSOCを構築・運用する場合においても、「IDS機能を有するネットワーク運用監視サービス」は有用な選択肢となります。「IDS機能を有するネットワーク運用監視サービス」の中には、リスク事象（非定常状態となるリスク事象）とその発生原因を検知・特定しようとする場合に、どのような情報を取得・監視・分析すればよいかという紐づけされた整理テーブルをナレッジとして蓄積し、それを実装しているサービスが存在するため、そのような分析がパターン化されたサービスを利用すれば侵入リスクの監視や脅威検出・判定に係る運用担当者の負荷を軽減することができます。

さらに、「IDS機能を有するネットワーク運用監視サービス」の中には、導入企業の要望によっては、提供ベンダーと導入企業の担当者が一緒になって、SOCを運用するサービスも存在するため、そのようなサービスを利用する場合には、導入企業の自社内に侵入検知製品等の運用に関わる専門性を獲得できるというメリットが得られます。

また、SOCの運用では、脅威の検出・判定作業として、「IDS」が検知したアラートに関連して、どのような通信が行われていたか、その通信は産業用制御システムに影響を与え得るものか等を分析することが必要になります。その際には、保存されている通信データを分析に活用することが前提となるため、機器間でやり取りされる通信データを記録・保存することができる「パケットキャプチャ・保存機能」を付加機能に持つ「IDS」や「IDS機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」を活用することが有用です。

(3)アラート検知後の対応要否判断の省力化

検知のベースライン（しきい値）を適切に設定するにあたっては、監視対象の産業用制御システムの構成や通信等に関する以下に示すような情報を正確に把握することが必要です。

把握すべき監視対象の産業用制御システムの構成や通信等に関する情報

①産業用制御システムの全体構成（ネットワーク構成、IT の機器や OT の機器の配置構成、外部ネットワークとの接続点等）

②産業用制御システムを構成する各機器の種類（ベンダー名、製品名、バージョン等）、台数、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 やファームウェアの種類（ベンダー名、製品名、バージョン等）、MAC アドレス、性能・パフォーマンス（メモリ容量等）

③産業用制御システムで使用する通信プロトコルの種類、IP アドレス、ポート番号

④ネットワークを流れるデータパケット（ヘッダ、ペイロード等）、データの種類（機器やプロセスとの紐づけ等）、通信量、通信頻度

⑤上記①～④に関わる既知の脆弱性

一方で、上記のような情報を正確に把握していない状態で、侵入検知製品等を導入・運用している場合には、アラート検知後の対応に関連して、「アラートの内容から産業用制御システムへの影響範囲が分からないため、対応の要否を判断することが難しい」、「脆弱性情報が公表された際に、脆弱性対策が必要となる機器を特定することが難しい」といった課題に直面する可能性があります。

よって、特に侵入検知製品の導入・運用を扱う専門的な外部サービスを利用していない導入企業においては、このような課題を踏まえつつ、監視対象の産業用制御システムの構成や通信等に関する情報を正確に把握することにより、アラート検知後の対応要否の判断に係る運用担当者の負荷を軽減することが必要です。上記のような情報の正確な把握を自社で対応する場合には、「資産管理機能」や「脆弱性アセスメント機能」を付加機能に持つ「IDS」や「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」を活用するのも一案です。

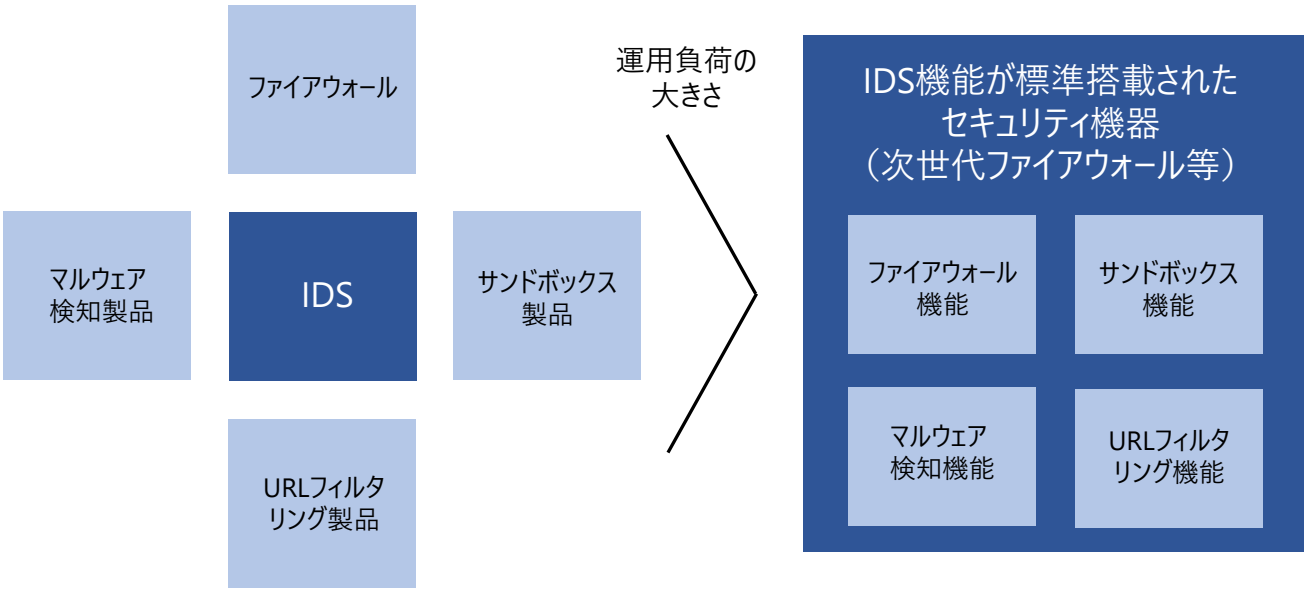
なおその際には、活用する「IDS」や「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」が、OT 環境内のどこまでの範囲の通信トラフィックを把握しているか確認することが重要です。

(4)セキュリティ対策製品の管理・運用の省力化

侵入検知製品等の導入企業においては、侵入リスクの高度な検知・防御のため、「ファイアウォール」や「マルウェア検知製品」、「URL フィルタリング製品」、「サンドボックス製品」など、他のセキュリティ対策製品を侵入検知製品等と組み合わせて運用している場合があります。

その一方で、提供ベンダーが異なる複数のセキュリティ対策製品を運用することによる弊害として、「製品知識や運用スキル・ノウハウを身につけるための学習コストが膨らむ」や「運用に係る担当者の負荷が増える」といった問題点が挙げられています。

上記のような問題点を抱える導入企業においては、1 つのプラットフォームの中で他のセキュリティ対策製品の機能をインストールして機能拡張することができ、統合的な管理・運用によって負荷を軽減できる「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」を活用するのも一案です。

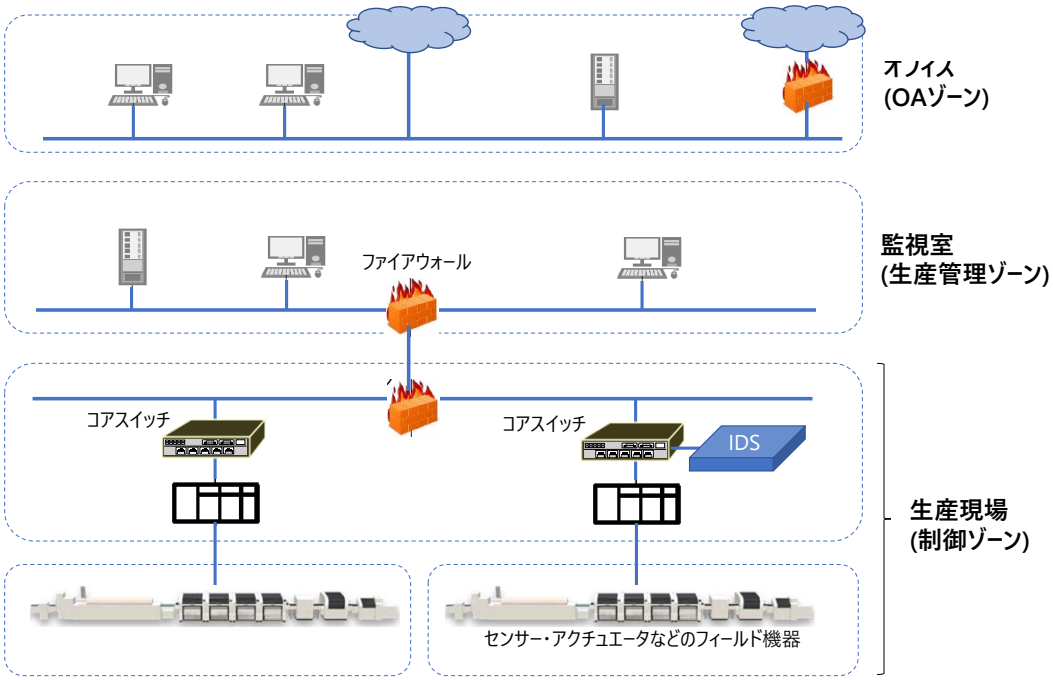


セキュリティ対策製品の個別運用と統合運用の比較

2.3.2. システムパフォーマンスへの影響の抑制

(1)適切な検知手法の選定

「IDS」においては、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を通過する通信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脅威を検知・特定するネットワーク監視型の IDS と、監視対象ホストに「エージェント」と呼ばれる検知用ソフトウェアをインストールするエージェント型の IDS の 2 つが主に活用されています。



IDS の導入イメージ(コアスイッチを通過する通信トラフィックを監視する形態)

2.2.2.で前述したとおり、エージェント型の侵入検知製品等を利用する場合には、インストールされたエージェントの動作によって、既存アプリケーションの動作の不具合やネットワーク遅延が発生する可能性があります。

このような産業用制御システムへの影響を許容できない導入企業においては、エージェント型の侵入検知製品等ではなく、ネットワーク監視型の IDS の一種であるインライン型（監視対象のネットワークトラフィックが侵入検知製品等のセンサーを必ず通過するように、監視対象のネットワーク上に設置するタイプ）の侵入検知製品等を選定する

ことが有用です。

インライン型の侵入検知製品等には、産業用制御システムへの影響を抑制するというメリット以外にも、侵入検知製品等を導入する際に、通信トラフィック量の制限など一部のネットワーク層の処理が必要となる場合を除いて、産業用制御システムのネットワーク構成を変更しなくても済むというメリットがあります。ただし、産業用制御システムに影響を与えることなく設置するためには、インライン型の侵入検知製品等を導入するネットワークについて、ネットワーク機器の設定状況や接続状況等の調査を行う必要があります。

また、産業用制御システムのネットワーク上には必要な情報を取得するセンサーのみ設置し、センサーから得られた情報の監視・分析をセンター側で実施する「IDS 機能を有するネットワーク運用監視サービス」を選定することも、使い方によっては、システムパフォーマンスへの影響を抑制する観点から有用です。次のような使い方による効用が特に大きいです。

○インライン型の IDS で検知可能な不正な侵入の監視・検知に活用する
○機器のネットワーク接続状況を監視して、不正な機器のネットワーク接続を検知したり、機器の処理プロセスを監視して、不正なソフトウェアの利用を検知したりするなど、特定のリスク事象の監視・検知に活用する

なお、「IDS 機能を有するネットワーク運用監視サービス」においては、リスク事象が発生した原因を細かく突き止めようとすればするほど、さまざまな情報（通信ログや機器の操作ログ、システムログ、アプリケーションログ、セキュリティログ等）を取得して、相関分析を行う必要があるため、「監視・検知対象の範囲の広さと分析の深さ」と「ネットワーク負荷」のトレードオフ関係について十分注意するとともに、必要に応じてネットワークや帯域幅の増強についても併せて検討することが必要です。

監視・検知対象とするリスク事象を特定のリスク事象のみに絞り込むような使い方は、ネットワークやシステムのパフォーマンスへの影響を抑制する観点からみても有用です。

(2)適切なトラフィック監視方法の選定

インライン型を始めとするネットワーク監視型の IDS においては、監視対象のネットワーク上に直接侵入検知センサーを設置して、当該ネットワークを流れる実際の通信トラフィックを監視します。

他方、侵入検知センサーが実際の通信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受動型の IDS においては、「スパンポートを利用した監視方法」と「ネットワークタップを利用した監視方法」の 2 つが主に活用されています。

注 1：「スパンポートを利用した監視方法」とは、スイッチを通過するすべての通信トラフィックを監視することができるスパン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通信トラフィックを監視する方法のことを指します。

注 2：「ネットワークタップを利用した監視方法」とは、スイッチ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通信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通信トラフィックを監視する方法のことを指します。

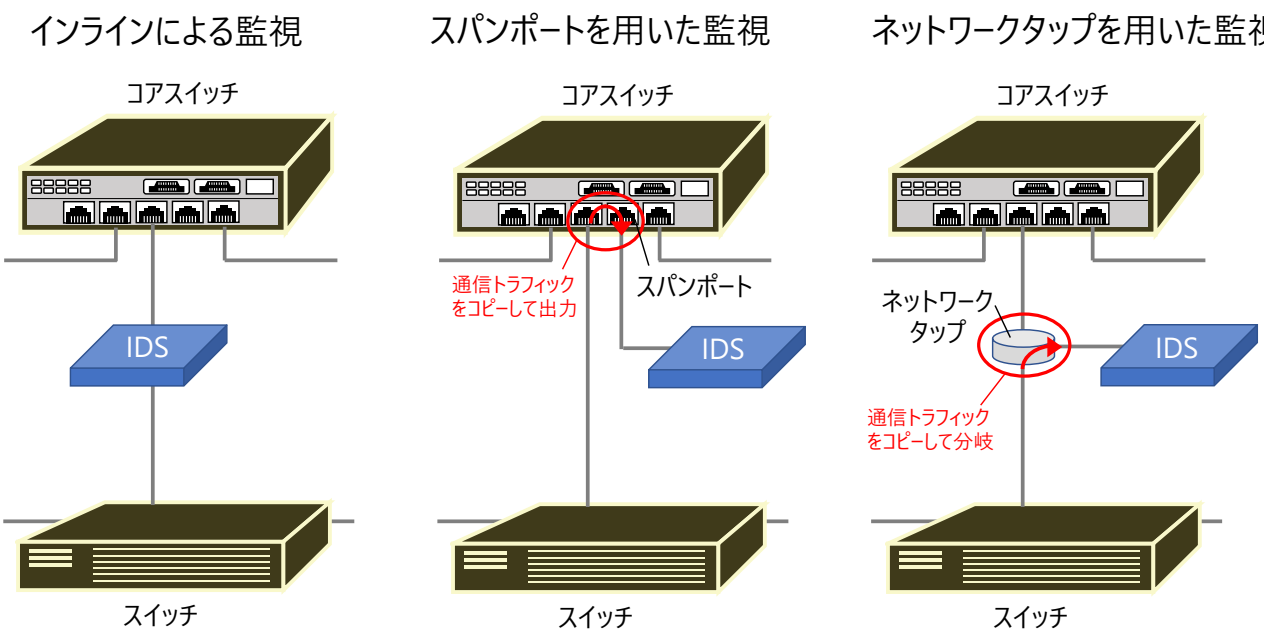
2.2.2.で前述したとおり、ネットワークタップを利用した監視方法を利用する場合に、ネットワークタップの設置や障害対応のために、ネットワークを一時的に停止する必要があります。

産業用制御システムへの影響を許容できない導入企業においては、ネットワークタップを利用した監視方法をベースとする侵入検知製品等ではなく、スパンポートを利用した監視方法をベースとする侵入検知製品等を選定することが有用です。

スパンポートを利用した監視方法をベースとする侵入検知製品には、産業用制御システムへの影響を抑制するというメリット以外にも、長年にわたる運用で培われたスキル・ノウハウを活かせるため、安定的な運用が可能であるというメリットがあります。

なお、ネットワーク監視型の IDS を利用する場合でも、受動型の IDS を利用する場合でも監視できる範囲は、監視対象のネットワークやスイッチを通過する通信トラフィックのみとなります。したがって、産業用制御システムのネットワーク上を流れるすべての通信トラフィックを監視するには、ネットワークセグメント毎の複数台設置が必要となります。

このような監視方法の導入が難しい導入企業においては、IT 環境から OT 環境への不正な侵入を防ぐという導入目的のもと、設置場所・監視場所が 1 箇所で済む、IT 環境と OT 環境の境界付近に侵入検知製品等を設置することも有用です。



トラフィック監視方法

(3)適切な動作モードの選定

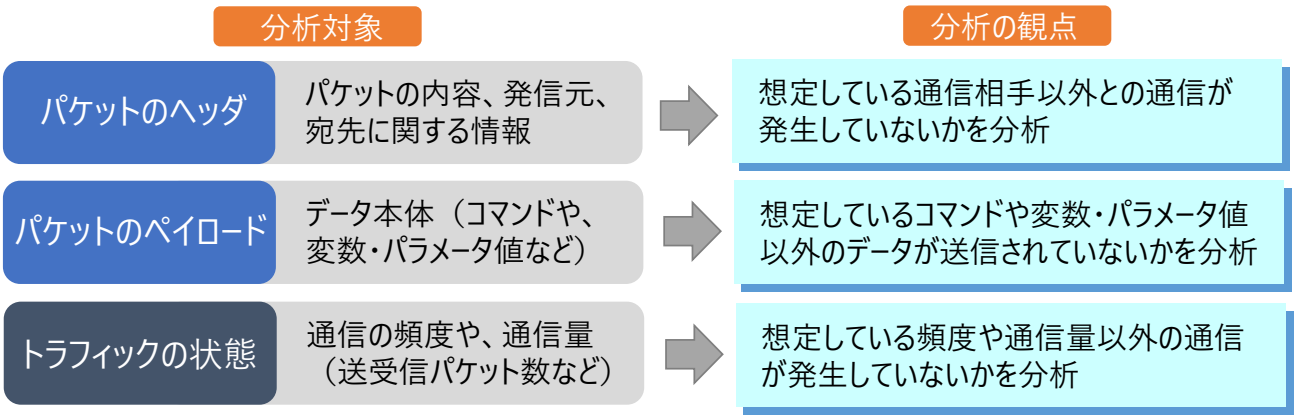
2.2.2.で前述したとおり、脆弱性を持つ OT の機器等の検出・特定のため、侵入検知製品から OT の機器等に接続を試みるアクティブモードでの FTP 通信や、当該通信を用いて OT の機器等の稼働状況や詳細な情報を取得するポーリングを使用する場合に、情報の取得頻度や量、対象となる OT の機器の台数の多寡によっては、ネットワークへの負荷が高まる可能性があります。

このような産業用制御システムへの影響を許容できない導入企業においては、アクティブモードで動作する侵入検知製品等ではなく、侵入検知製品からの指示のもと、OT の機器等から侵入検知製品に接続を試みるパッシブモードで動作する侵入検知製品等を選定することが有用です。

(4)適切なパケット分析・送信方法の選定

侵入検知製品等では、通信トラフィックのパケットの中身をみて、通信の内容を分析しています。このようなパケット分析方法にはレベル感があり、キャプチャされたパケットのヘッダのみ分析するものや、パケットのヘッダだけでなく、ペイロードも含めて

詳細に分析するものが存在します。後者のパケット分析手法は、DPI（Deep Packet Inspection）と呼ばれています。



パケット分析手法

他方、侵入検知製品の付加機能を用いて取得された資産情報や通信トラフィック情報、脆弱性情報等については、管理コンソール機能上で一元管理を行いたいと考える導入企業が多いです。そのような一元管理のため、上記の情報に関するキャプチャされたすべてのパケットを管理サーバに送信する場合に、パケット量の多寡によってはネットワークへの負荷が高まる可能性があります。

特に、監視対象のネットワークを流れる通信トラフィック量（パケット量）が多い場合には、ネットワークへの負荷を軽減する観点から、管理サーバに送信するデータについて、前述したDPIを活用することにより、通信の内容を分析し、その分析結果から一元管理に必要なデータをメタデータ化することが求められます。

さらにDPIの中には、管理サーバに送信するデータを圧縮することができるものがあるので、そのようなデータ圧縮機能を持つDPIを活用することも一案です。

その一方で、DPIは、侵入検知製品等の計算リソースを消費するため、CPUの使用状況を確認する等のパフォーマンス評価を事前に行うなど、活用上の注意が必要です。

またその他にも、ネットワークへの負荷を軽減する観点から、管理サーバにデータを送信するための専用ネットワーク（専用線等）を構築している場合があります。

(5)検証基盤を活用した事前の影響評価

侵入検知製品等の導入前にコンパチビリティ検証等の産業用制御システムへの影響評価を実施し、異常が起きないことを確認した上で実環境に導入することが有用です。

制御機器・システムベンダーの中には、研究所内にコンパチビリティ検証のための基

盤を保有しているベンダーも存在します。

参考情報 2　**ネットワーク全体の最適化と連動した形での侵入検知製品等の導入**

DX の推進が求められる中、産業用制御システムにおけるデータ利活用を推進し、業務プロセスの改善による生産効率の向上に取り組む企業が増えてきています。そのような企業においては、データ利活用の要件に見合う最適なネットワーク環境を設計・構築する場合が多いです。

侵入検知製品等を提供するベンダーの中には、ネットワーク全体の最適化と侵入検知製品等を一体的に提案するベンダーも存在するため、システムパフォーマンスへの影響の抑制を特に最重視する導入企業においては、そのようなベンダーが提供する侵入検知製品等を選定することも一案です。

最適なネットワーク環境の設計・構築では、侵入検知製品等を効果的に運用するという観点が盛り込まれ、ネットワーク・帯域幅の増強や、ネットワークを接続する機器の種類や重要度に応じて分割し、ネットワーク間の不正な通信に対する対策を容易にするネットワーク分離等を行ったり、ネットワーク接続の認証や有事の際の遮断といった他の対策と併用することにより侵入検知製品等を導入するネットワークの箇所を最小限に抑えたりすることによって、システムパフォーマンスへの影響を抑制しています。

2.3.3. 付加機能の効果的な活用

侵入検知製品等のうち、「IDS」や「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」の中には、検知精度の向上や、アラート検知後の対応要否判断の効率的な運用、インシデント対応の効率的な運用など、さまざまな目的を達成するために、以下に示すようなセキュリティ上の付加機能を併せて提供するものがあります。

IDS や IDS 機能が標準搭載されたセキュリティ機器が具備する主なセキュリティ上の付加機能

	付加機能	概要
特定	資産管理機能 [6]	監視対象の産業用制御システムを構成する IT の機器や OT の機器等の資産に関する情報（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、既知の脆弱性等に関連する様々な情報）を収集・管理する機能や、初期設定された資産に関する情報だけでなく、設置場所や管理責任者等の新たに管理したい情報を定義して、テーブルの追加を行う機能
	脆弱性アセスメント機能 [7]	監視対象の産業用制御システムを構成するネットワークおよび機器の脆弱性を自動的に評価・検出し、収集する機能。
	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、産業用制御システムにおいて最も狙われやすいネットワークの箇所や機器を特定したり、発生リスクの高い攻撃経路を予測したりする機能
	コンプライアンス監査機能	各種法規制要件への準拠性の確認を目的として、ガバナンス管理を複数の拠点間で横串を通して行うための監視を行い、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
	モニタリング・他のデバイスとの通信状況の可視化機能	監視対象の産業用制御システムを構成する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機能
	タグ生成機能	可視化された機器や通信プロトコル等の情報の中身を AI が理解して、自動的にタグ付けを行う機能
防御	パケットキャプチャ・保存機能	主にインシデントが発生した場合のフォレンジック分析において使用するために、監視対象の産業用制御システムを構成する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

[6] 資産管理機能には、受動型とアクティブ型があり、受動型は産業用制御システムの稼働に影響を与えるリスクが小さいが、資産情報や脆弱性情報を収集する際に扱う情報量が限定されるという制約があります。他方、アクティブ型は侵入検知製品から機器等に接続を試み、情報量が増えるため、産業用制御システムの稼働に影響を与えるリスクがあります。
[7] 脆弱性アセスメント機能にも、資産管理機能と同様、受動型とアクティブ型があり、それぞれの特徴も全く同じです。

	付加機能	概要
防御	変更管理・タイムマシン機能	導入企業が定める頻度で、ネットワークステータス（ネットワークに関する現在の状態）のスナップショットを取得・保存し、変更後の差分を可視化する機能
検知	他社ネットワーク機器・SIEM 連携機能	API を用いた他社製のシステムや機器との連携により、異常を検知した場合に発生原因となっている機器の特定から対応に至るまでの自動制御を行ったり、SIEM 機器との連携により、複数の機器にまたがるイベントの相関を特定したりする機能
	プロトコル SDK 機能	IDS の拡張機能を利用して、ベンダーがサポートしていない、導入企業の独自プロトコルの解析を可能にするスクリプトの追加ができるように、当該スクリプトを作成するために必要なツールを提供する機能
	管理コンソール機能	IDS 等を同一拠点内に複数台設置する場合や、複数の拠点に複数台設置する場合に、情報を集約し一元的な管理を行うための機能
	レポーティング・データ連携機能	IDS 等の運用監視や、IDS 等に具備された資産管理機能等の付加機能の活用により取得された、さまざまな情報を、検知されたアラート結果（アラートの内容や必要対策等）と組み合わせて帳票として自動的に出力する機能や、他の対策製品の管理コンソールと連携してデータ共有・連携を行う機能
対応	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、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、インシデント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
	SOAR 連携機能	SOAR との連携により、インシデントが検知された際の適切な対応のためのワークフローの効率化や自動化を行う機能
	プレイブック機能	同一または類似するアラートへの対応を円滑かつ迅速に行うため、運用担当者が実際に行ったアラート対応をメモとしてシステムに記録・保存し、アラート検知時において参照可能とする機能
	チケットシステム連携機能	チケットシステムとの連携により、アラートが発生した際に必要となる対応をチケットとして管理し、チケットの内容を組織内で共有することができる機能

IDS 等が具備するセキュリティ上の付加機能を効果的に活用することにより、IDS 等の運用力や総合的な侵入検知対策の推進力を高めることは有用である。

2.3.4. 投資判断と予算化に向けた調整の円滑化

(1)投資判断の確度を高めるための調整

産業用制御システムを構成するネットワークの多くは、これまでインターネットから分離されており、高度な侵入検知対策が不要とされてきたため、インターネットに繋がっているオフィスネットワーク等に侵入検知製品等を導入する場合に比べて、侵入検知製品等の導入ハードルが一般的に高いという状況があります。

一方で、近年の実態としては、インターネットに繋がっているオフィスネットワークが産業用制御システムに繋がっていたり、メンテナンス業者やテレワークで業務を行う運用担当者が VPN 経由等で産業用制御システムへのリモートアクセスを行っていたりするなど、インターネットからの分離が行われていない状況へと様相が変わりつつあります。今後ますます OT 領域と IT 領域の垣根がなくなってくることが予想されています。

産業用制御システムがインターネットに繋がっている状況を正確に把握し、その実態を分かりやすく経営層に説明することで、侵入検知製品等の導入ハードルが引き下がる余地がかなりあります。

また、投資利益率(ROI：Return On Investment)を重視する経営層においては、侵入検知製品等に限らずセキュリティ対策への投資は、利益を生むものではなく、損失を防ぐものであるため、投資に対する理解が得られにくいという状況があります。

加えて、侵入検知製品等の種類ごとの性能や使い方、得られる効果等の違いが分かりにくいという側面が、投資の躊躇に一層の拍車をかけ、侵入検知製品等の必要性に対する理解を得る際の大きな足かせとなる場合があります。

このような状況を踏まえつつ、侵入検知製品等への投資判断や予算化に向けた調整を円滑に進めるためには、経営層に対し、産業用制御システムを脅かすリスク事象の存在や、侵入検知製品等の導入・運用に係るトータルコストを含め、以下に示すような投資の判断材料となる情報を的確に提示して、投資判断の確度を高めることが重要となります。

経営層に対し侵入検知製品等への投資判断を仰ぐために提示すべき情報
①侵入検知製品等の導入・運用が必要であることの妥当性
②侵入検知製品等の導入・運用にかかる予算が適正であることの妥当性
③侵入検知製品等の導入・運用で得られるプラスアルファの効果

①を証明する必要がある導入企業においては、自社の産業用制御システムを対象としたリスク分析を実施し、産業用制御システムを脅かすリスク事象の発生可能性と、リスク事象が発現した際にもたらされる被害・影響の大きさについて明らかにすることが必要です。そのうえで、リスク・影響に見合う低減・回避策として、侵入検知製品等の導入・運用による最適な監視・検知・対処方法を設計し、経営層に対し提案することが重要となります。

②を証明する必要がある導入企業においては、侵入検知製品等の導入に係るイニシャルコストと、侵入検知製品等の運用に係るランニングコストを含めたトータルコストについて考えることが必要です。トータルコストは、侵入検知製品等の導入の目的や目的を達成するための取組方針、導入する侵入検知製品等とその運用方法をどのように設計するかによって大きく変動します。

コスト変動の大きなポイントとしては、以下のような点が挙げられます。

コスト変動のポイント

1）既知の脅威に加えて、未知の脅威まで検知を行うか

2）脅威の検知後に発生原因の究明まで行うか

3）IEC 62443 において提案されている機能参照モデル（Purdue モデル）[8]の各レベルのうち、どのレベルまでを保護対象とするか

レベル 0（センサーやアクチュエータ等のフィールド機器を制御するエリア）
レベル 1（PLC 等によりフィールド機器からデータを読み込んで製造プロセスを制御するエリア）
レベル 2（HMI や SCADA 等において製造プロセスを監視したり、制御したりするエリア）
レベル 3（現場の生産管理を行うエリア）
レベル 4（拠点の事業計画やロジスティクスアプリケーションを管理するエリア）
レベル 5（組織が使用する IT インフラストラクチャや IT アプリケーションを管理するエリア）

4）侵入検知製品等の設置場所や設置台数をどれぐらいの数にするか

5）侵入リスクの監視と脅威検出・判定に関する業務を平日の営業時間内に加えて、平日の営業時間外や土日祝日まで行うか

6）コスト低減に寄与する外部委託（専門的な外部サービスの利用）や、機械学習を用いた運用業務の自動化をどの程度採り入れるか

このようなコスト変動のポイントを踏まえて、採り得る選択肢を幅広く考慮した上で、侵入検知製品等の導入・運用による最適な監視・検知・対処方法を設計し、経営層に対し提案することが重要となります。

③をアピールする必要がある導入企業においては、侵入検知製品等が具備する付加機能を効果的に活用することが必要です。なかでも特に、「資産管理機能」や「脆弱性アセスメ

8 機能参照モデル（Purdue モデル）は、国際自動制御学会（ISA）が策定する制御システム向けセキュリティに関する標準規格である ISA99 において提唱されている、制御システムのアーキテクチャーを機能ごとのレベル分けしたモデルです。
https://gca.isa.org/blog/excerpt-2-industrial-cybersecurity-case-studies-and-best-practices
国際電気標準会議（IEC）により策定された標準規格である IEC 62443 では、機能参照モデル（Purdue モデル）を取り込んで、機能ごとのレベル分けをゾーンとコンジットにセグメント化する産業用制御システムアーキテクチャを提案しています。

ント機能」、「コンプライアンス監査機能」といった付加機能は、それ自体が単独のセキュリティ対策製品として市販されているものであり、レベルの違いがあるものの、特定のシーンにおいては、市販製品と遜色のないレベルで利用することができます。

このような侵入検知製品等が具備する付加機能の効果的な活用によって、本来、単独のセキュリティ対策製品として購入費用や導入工数が発生していたものを削減できるというプラスアルファの効果が得られることから、経営層に対しアピールすることが重要となります。

(2)組織横断的な推進体制の整備

侵入検知製品等の導入・運用や付加機能の活用によって取得されるさまざまな情報は、導入企業内の生産技術部門、保全部門、IT 部門、DX 部門といった複数部署のニーズを満たすものです。

例えば、生産設備の設定変更の履歴情報等は、生産技術部門が生産効率を上げるために役に立ちます。また、各種機器の稼働状況の情報等は、保全部門が機器の機能停止や故障の予兆等を把握するために役に立ちます。さらに、資産情報や脆弱性情報等は、IT 部門が効果的なセキュリティ対策を講じるために役に立ちます。そして、このような情報の幅広い利活用は、DX 部門の活動そのものです。

こうした情報提供が可能な侵入検知製品等の導入は、全社的な視点を持ち、組織横断的な活動として進められることが重要であり、関連する部署の巻き込みにより、侵入検知製品等の導入価値を最大化することによって、経営層に対するアピール力を高め、導入ハードルの引き下げに繋げる効果が期待されています。

(3)導入推進役となる適切な本社サイドの部署との調整

産業用制御システムを運用する企業においては、事業部門単位で採算性を見ている企業が多いため、事業部門が導入推進役となり、コストを負担しながら侵入検知製品等の導入・運用を行うには克服すべき課題が多いです。そのため、必要に応じて、本社サイドに導入推進役となってもらうことが重要です。

最近では、セキュリティインシデントが発生した際に緊急対応を行うための専門組織である CSIRT（Computer Security Incident Response Team）や、CSIRT のレベルには達していなくても CSIRT と同じ機能を持つ部署を、本社サイドに設置している企業が増

えていますので、そのような部署に導入推進役となってもらい、予算化に向けた調整を円滑に進めていくことが重要です。

特定の拠点のみのテスト導入完了後の全拠点への本格展開を見据えると、コーポレートガバナンスやリスクマネジメントの強化を推進している経営企画やリスク管理などの関連部署を導入推進役として巻き込むことも重要です。

第3章　侵入検知製品等の導入の進め方

本章では、産業用制御システム向け侵入検知製品等の導入の進め方について、「構築」、「試験運用」、「本格運用」の各フェーズにおける検討のポイントを説明します。

3.1. 構築の進め方

侵入検知製品等の構築フェーズにおいて必要となる作業とその進め方について、以下に説明します。

3.1.1. 現状の把握

現状の把握においては、「資産の可視化」、「脆弱性の可視化」、「通信の可視化」、「業務プロセスの可視化」が必要になります。参考となる手順を以下に示す。

現状の把握のための手順

①監視対象となるネットワーク上にある機器等を洗い出し、各機器等の資産情報（ベンダー名、製品名、OS・ファームウェアのバージョン、MAC アドレス、使用する通信プロトコル、既知の脆弱性等）を整理する。（「資産の可視化」）

②リスク分析（産業用制御システムを脅かすリスク事象の発生可能性と、リスク事象が発現した際にもたらされる被害・影響の大きさの分析）を行い、その結果に基づいて、守るべき重要資産の特定と優先順位付けを行う。（「脆弱性の可視化」）

③優先順位の高い重要資産を対象として、通信トラフィックデータと機器との紐づけ状況（ネットワーク論理構成図、通信フローリスト等）を整理する。（「通信の可視化」）

④内部犯行やオペレーションミスなどによる内部脅威にも対応できるように、OT 環境特有の通信プロトコルやそのコマンド・変数値等を把握し、通信トラフィックデータや機器と業務プロセスの紐づけ状況を整理する。（「業務プロセスの可視化」）

先ず最初に、監視対象のネットワークに接続されている資産を洗い出し、必要となる資産情報を一覧可能な形で整理することから始める必要があります。そのうえで、産業用制御システムのリアルタイムでの制御や長期継続的な運用といった観点からみた資産の重要度について整理していくことが重要です。このような資産情報は、リスク分析を行う際や、分析

結果に基づいて守るべき重要資産を特定する際にベースとなる基本情報となります。

次に、産業用制御システムのセキュリティ対策を検討する上で、その根拠を提供するリスク分析を行うことが必要になります。リスク分析は、産業用制御システムを脅かすリスク事象を特定することから始める必要があります。リスク事象を特定する際に、攻撃者が利用することでリスク事象を脅威として発現させ、産業用制御システムに被害・影響をもたらす可能性がある資産の脆弱性を洗い出すことが重要です。そのうえで、対策優先順位が高い守るべき重要資産を明らかにする観点から、資産の脆弱性をベースとして、リスク事象の発生可能性と、リスク事象が発現した際にもたらされる被害・影響の大きさについて分析していくことが重要です。このような資産の脆弱性情報は、前述の「資産の可視化」において把握され整理されたものを基本情報として活用します。産業用制御システムは、新しい要素の追加による変更を回避または最小限とすることに重点を置いた運用を基本としており、そのような運用に起因して、以下のような脆弱性が残存しがちです。

［産業用制御システムに残存しやすい脆弱性］

- OS・ファームウェア等が古いバージョンのまま利用されている問題
- セキュリティ機能が十分ではない通信プロトコルが利用されている問題

次に、重要資産を守るために、侵入検知製品等において監視・検知対象とする通信を洗い出し、通信トラフィックデータと機器との紐づけ状況（ネットワーク論理構成図、通信フローリスト等）の情報を整理し、ネットワークの利用状況（例えば、機器のリモートメンテナンス用通信がネットワークの帯域を消費し、それにより帯域不足になっていないか等）を確認することが必要になります。

最後に、内部犯行やオペレーションミスなどによる内部脅威に対応するため、OT 環境特有の通信プロトコルやそのコマンド・変数値等を把握し、通信トラフィックデータや機器と業務プロセスの紐づけ状況を整理し、相互の依存関係やプロセス間の依存関係を確認することが必要になります。

侵入検知製品等では、検知のベースライン（しきい値）として、産業用制御システム上で一定期間中に日々やりとりされる通信トラフィックを分析して、正常な状態の通信トラフィックを定義する必要がありますが、このような通信トラフィックデータと機器・業務プロセスとの紐づけ状況の情報は、正常な状態の通信トラフィックを定義する際にベースとなる基本情報となります。

3.1.2. 方針検討

導入企業は、3.1.1.で前述した現状把握の内容をもとに検討を行い、以下の項目を侵入検知製品等の導入・運用方針として明確化する必要があります。

明確化すべき項目
①どのリスク事象（脆弱性等）に対し、どのような対策の手を打てば、被害・影響が低減・回避されるか（前述の 2.3.4.を参考にして検討する） ②知識や人材等のリソースや、ネットワークやシステムのパフォーマンスへの影響といった留意点に対応する課題をどのように克服するか（前述の 2.3.1.及び 2.3.2.を参考にして検討する） ③侵入検知製品等に備わっているセキュリティ上の付加機能をどの程度有効活用するか（前述の 2.3.3.を参考にして検討する） ④侵入検知製品等の導入・運用による最適な監視・検知・対処方法

①を明確化する際の考え方は導入企業によってさまざまであるが、1 つの考え方として、例えば、工場の制御システムの場合に、以下について総合的に勘案した上で、侵入検知製品等の導入により、保護対象とすべき生産ラインや生産設備を選定している導入企業も存在します。

［リスク事象が発現した際にもたらされる被害・影響の大きさ］

- 稼働率が高く、稼働が停止した時の損害による事業上の影響を受けやすい生産ラインはどれなのか

［産業用制御システムを脅かすリスク事象の発生可能性］

- その生産ラインで稼働している生産設備には、脆弱性のある設備や、外部業者がメンテナンスのために USB メモリ等を持ち込まなければならない設備が多いのか
- その脆弱性のある生産設備には、変更の回避が不可欠である理由で、ファームウェアアップデート等によるバージョンアップ対策が困難な設備が多いのか

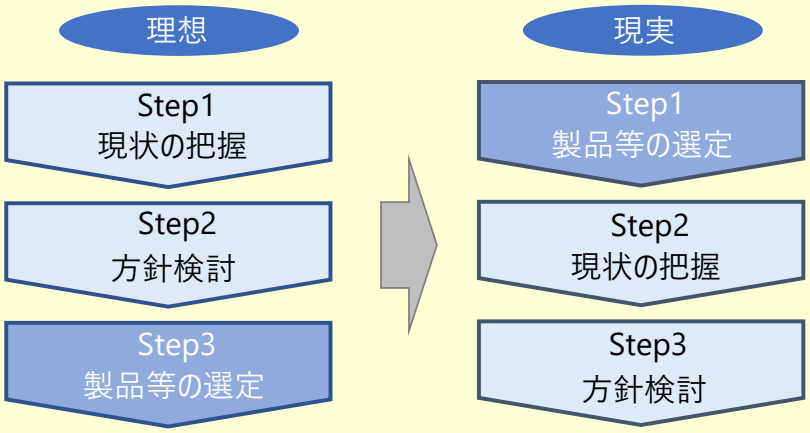
②を明確化する際の考え方は、前述の 2.3.1.及び 2.3.2.で、また③を明確化する際の考え方は、前述の 2.3.3.でそれぞれ示しているため、参考にしてください。

④は、①、②、③のそれぞれで明確化された内容を踏まえて明確化されます。最適な監視・検知・対処方法には、以下の内容が含まれます。

- 侵入検知製品等の導入対象システム、設置場所、監視対象・範囲
- 検知手法・検知方法・パケット分析方法
- アラート・ログの監視体制・監視項目
- アラートが発生した際の通知先・通知内容・通知方法
- 通知されたアラートに基づく脅威の検出体制・検出時の判定基準
- 検出された脅威への対処体制・手順

参考情報 3　現状の把握や方針検討は、侵入検知製品等の選定前に必要か？

「IDS」や「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」の中には、「資産管理機能」や「脆弱性アセスメント機能」を付加機能に持つ製品が多いため、現実的には、先ず最初に、侵入検知製品等の選定を行い、その後、「資産管理機能」や「脆弱性アセスメント機能」を活用して、現状の把握を行い、それをもとに方針検討を行う導入企業が多いです。



3.1.3. 製品等の選定

導入企業は、2.1.2.に前述した侵入検知製品等の種類を含め、侵入検知製品等の採り得る選択肢について幅広く考慮した上で、3.1.2.に前述した方針に見合う適切な侵入検知製品等を選定することが必要です。

またその際、産業用制御システムで使用されているさまざまな種類の通信プロトコルへの対応状況や、分析対象パケットのサンプリング状況、機械学習の活用状況等といった基礎的な情報についても確認することが必要です。

しかしその一方で、侵入検知製品等における製品・サービス間の性能の違いは単純な比較だけでは分かりにくいため、以下に示すような情報も考慮の上、適切な選定を行うことが重要です。

侵入検知製品等を選定する際に考慮すべき情報

①侵入検知製品等の導入・運用実績

②製品ライフサイクルマネジメントにおける新機能の追加や機能改善による品質向上の取組状況

③最新の脅威インテリジェンスの保有・活用・連携状況

④脆弱性対策におけるバージョンアップ対応の速さ

⑤優良パートナーとの提携状況

⑥柔軟性の高い課金モデル（サブスクリプション、チケット制等）

侵入検知製品等を調達・選定する際には、複数の提供ベンダーから提案募集を行うことや、PoC（Proof of Concept）を実施して、複数ベンダーが提供する侵入検知製品等を同時に試験運用し、製品等間の検証結果の比較による有用性評価を行うことも有用です。

提案の募集において提供ベンダーに提示する RFP（提案依頼書）は、前述の 3.1.2.について自社で検討した内容をもとに作成することが重要です。侵入検知製品等は、その種類の多さもさることながら、侵入検知製品等を活用した監視・検知・対処方法にも多種多様なパターンがあります。それゆえ、1 つの提供ベンダーですべてのパターンをカバーすることは難しく、それぞれの提供ベンダーには、自社が得意とするパターンが存在します。このため、RFP の作成において、提供ベンダーの言いなりになってしまうと、採り得る選択肢の幅が狭まることに注意が必要です。

PoC は、以下に示すような条件・内容について提供ベンダーと合意した上で実施し、侵入検知製品等の導入・運用に係る効果や課題の検証を行うために活用されています。

PoC の実施にあたって検討すべき条件・内容
①侵入検知製品等の構成
②侵入検知製品等の設置方法
③通信トラフィックデータ等の収集方法、監視方法、分析方法
④アラートされる内容、レポートされる内容
⑤試験運用の期間

3.1.4. 製品等の設置

侵入検知製品等を構築する際においては、導入する侵入検知製品等における検知手法や検知方法によって、導入効果を高めるための準備作業が異なりますので、注意が必要です。

侵入検知製品等の種類		必要となる準備作業
検知手法	ルールベース（仕様ベース）	機器ごとに実行を許可するプロセスと実行を許可しないプロセスを整理し、後者のプロセスによって起動されるプログラムを実行できないように制御することが必要となります。
	ネットワーク負荷が大きいログ相関分析	リスク事象が発生した原因を細かく突き止めるための高度な相関分析を行う際には、必要に応じて、ネットワークや帯域幅の増強を行うことが必要になります。
検知方法	ネットワーク監視型	監視対象のネットワークへの接続が認められている機器を登録し、登録されていない機器が当該ネットワークに接続できないように制御することが必要となります。

	受動型	スパンポートを利用した監視方法	侵入検知製品等を構成するサーバをネットワークスイッチのスパンポート（ミラーポート）に接続する必要があるため、既に実装済みの監視対象のネットワークスイッチにスパンポート（ミラーポート）が備わっていなければ、ネットワークスイッチにスパンポート（ミラーポート）を具備するネットワークスイッチに置き換えることが必要になります。
		ネットワークタップを利用した監視方法	監視対象のネットワークを一時的に停止して、監視対象のネットワークにネットワークタップを設置することが必要になります。
	エージェント型		監視対象の機器すべてに、「エージェント」と呼ばれる検知用ソフトウェアをインストールすることが必要になります。

3.2. 試験運用の進め方

侵入検知製品等の試験運用フェーズにおいて必要となる作業とその進め方について、以下に説明します。

3.2.1. 体制の整備

不正な侵入リスクの監視と脅威検出・判定を行うための専門組織である SOC（Security Operation Center）と、セキュリティインシデントが発生した際に緊急対応を行うための専門組織である CSIRT（Computer Security Incident Response Team）を整備・運用することが必要となります。

上記のような体制の整備・運用方法について大別すると、自社対応と外部委託の 2 つの選択肢があります。

自社対応においては、侵入検知製品等の付加機能の中に、以下に示すような自社対応による SOC や CSIRT の運用を支援する機能がありますので、そのような機能を効果的に活用することも一案です。

自社対応による SOC や CSIRT の運用を支援する機能

①フォレンジック分析機能（前述の 2.3.3.を参考にして検討する）

②他社ネットワーク機器・SIEM 連携機能（前述の 2.3.3.を参考にして検討する）
※別途、SIEM を自社で運用することが必要になります。

③SOAR 連携機能（前述の 2.3.3.を参考にして検討する）

外部委託においては、「IDS 運用監視サービス（MSS）」や「IDS 機能を有するネットワーク運用監視サービス」を活用することができます。このようなサービスの中には、通常は自社対応により SOC を運用しつつ、脅威検出・判定が難しい場合にのみ、チケット制にて脅威検出・判定を外部委託できるサービスもあります。

上記のようなさまざまな観点について十分考慮の上、SOC や CSIRT の適切な整備・運用方法を選択することが重要となります。

その他に、SOC や CSIRT を中心に据えた場合の現場とのやりとり（確認等の依頼する作業の内容や依頼の仕方等）や、インシデント発生時の対処や復旧における現場との役割分担についても、事前に検討しておくことが必要です。なかでも特に、インシデント発生時の対処や復旧においては、「リアルタイムでの制御」や「長期継続的な運用」という厳しい条件のもとで運用されている産業用制御システムの場合に、稼働しながら同時並行で対処や復旧を行うことが求められます。そのため、メンテナンスのタイミングで対処する等の工夫が必要となり、現場との役割分担が重要となります。

3.2.2. 機能検証

導入した侵入検知製品等が正常に動作するか確認するための機能検証を行うことが必要となります。この機能検証については、産業用制御システムにほとんど影響がない対象・動作から確認を開始し、問題がなければ、その後、徐々に対象・動作の範囲を拡げていくといった形で段階的に行うことが重要です。

3.2.3. 検知ポリシーの設定・チューニング

試験運用において、体制の整備と並んで特に重要なものが、検知ポリシーの設定・チューニングです。

2.3.1.に前述したとおり、検知ポリシーの設定・チューニングにおいては、「検知のベースライン（しきい値）の初期設定」と「検知のベースライン（しきい値）の修正」の段階的な作業が必要となります。

ここで言うベースライン（しきい値）には、正しい状態として定義されるある共通の特徴を持つ通信データのトラフィックパターンや、ホワイトリストに登録されるシグネチャ等が含まれます。

「検知のベースライン（しきい値）の初期設定」においては、多くの侵入検知製品等が、機械学習を用いて自動的にベースラインの初期設定を行う機能を具備しているため、この機能を活用することが重要です。

ただし、機械学習が導くベースラインの初期設定が最適であるとは限らないため、「検知のベースライン（しきい値）の修正」が必要となります。この作業では、ベースラインに内包される季節や周期、突発事象等による誤差に起因して発生する誤検知・検知漏れの発生回数・頻度が許容範囲となるまで修正を行うことが重要です。

この修正作業は、1つ1つのアラートの内容を確認して誤検知・検知漏れかどうかの判定を行うとともに、誤検知である場合には誤検知が発生しないようベースラインの設定を見直しして修正する必要があるため、かなりの時間と労力を伴います。季節や周期による変動や突発事象、特殊事情を含めた、産業用制御システムの運用方法に起因して発生した誤検知アラートについては、導入企業自身による確認・判定作業が必要不可欠です。

3.2.4. カスタマイズ

侵入検知製品等の中には、検知のベースライン（しきい値）の設定とは別に導入企業自身が組織文化やセキュリティリスクに対する考え方等に見合う独自の検知ポリシーを定義することができるものがあります。また、試験運用を行う中で、導入企業が採用している独自の通信プロトコルを利用していることが分かり、導入した侵入検知製品等がこれに対応していない場合に、「IDS 運用監視サービス（MSS)」の提供ベンダー等を経由して、「IDS」や「IDS機能を標準搭載したセキュリティ機器（次世代ファイアウォール等)」の提供ベンダーに対して、対応の依頼・相談ができる場合があります（なお、このような依頼・相談については、無償、有償のいずれの対応も想定されますので、確認の上で利用してください)。

侵入検知製品等の運用方法に強いこだわりがある導入企業においては、必要に応じて、そのような機能を活用してカスタマイズを行うことも重要です。

また、侵入検知製品等の付加機能の中にも、資産情報に設置場所や管理責任者等の新たに管理したい情報を定義してテーブルを追加できる資産管理機能など、カスタマイズして活用できる機能がありますので、必要に応じて活用することも重要です。

3.3. 本格運用の進め方

侵入検知製品等の本格運用フェーズにおいて必要となる作業とその進め方について、以下に説明します。

3.3.1. アラート・ログの監視と脅威の検出・判定

3.2.1.で前述したSOCにおいて、監視対象より日々収集される各種ログや、侵入検知製品等が検知した不正な侵入または不正な侵入が疑われる予兆に関するアラートを監視することが必要になります。

アラート対処の実効性を高めるため、侵入検知製品等が不正な侵入等を検知すると、そのアラートがSOCに速やかに転送されるようにシステム化またはアラート受領後の対応手順の策定を行うことが重要です。

その後、SOCでは、通知されたアラートについて監視対象より日々収集される各種ログを含めて分析し、そのアラートが監視対象の産業用制御システムに被害・影響をもたらす脅威を検出したものであるか判定することが必要になります。

アラート分析の効率性を高めるため、通知されたアラートや収集された各種ログを、資産情報や脆弱性情報、通信トラフィックデータ等と一緒に一覧できるようダッシュボード化することが重要です。

また、「IDS運用監視サービス（MSS)」においては、通知されたアラートや収集された各種ログをもとに、SIEM（Security Information and Event Management）を用いて自動的に相関分析（一次分析）を行い、その内容をみて詳細分析が必要であるかを判断し、必要であると判断された場合には、アナリストが詳細分析（二次分析）を行うといった形で効率的な運用を行っている提供ベンダーが多いです。

そのような状況を踏まえると、導入企業が自ら行う場合には、上記のダッシュボード化（データを収集し、分析するBI：ビジネスインテリジェンスとしてのツール化）に加えて、ツールとしてのSIEMを導入・運用することが重要です。

3.3.2. 検出された脅威への対処

検出された脅威への対処方法については、以下に示すように多様なレベルが想定されま

すので、人材・スキル面、予算面、運用面等を考慮した上で適切な対処方法を選択することが必要になります。

検出された脅威への対処方法

①侵入検知製品等の運用担当者において、アラートに記載される推奨対策のみ実施する

②IPS 機能やネットワークアクセス制御機能と連携して、侵入検知製品等が検知した不正な侵入または不正な侵入が疑われる予兆に関する異常な通信を自動的に遮断する

③SOC と連携して速やかに脅威の発生原因を究明するとともに、その結果を踏まえて、CSIRT と連携して、被害の拡大を防ぐための緊急対応を行う

アラート受領後の対応手順と同様、脅威検出後の対処手順についても予め策定しておくことが重要です。

なお、①のアラートについては、大別すると、「IDS」や「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」において検知された不正な侵入等を通知するアラートと、「IDS 運用監視サービス（MSS）」や「IDS 機能を有するネットワーク運用監視サービス」において検出された脅威を通知するアラートの 2 種類のアラートがあります。

前者においては、脅威の検出・判定を行っておらず、アラートに記載される推奨対策については、どちらかと言うと、不正な侵入等に関する通信の発生原因の裏返しのような対策となっており、なかには対処が不要なアラートも含まれています。このような対処が不要なアラートについても、推奨対策を実施してしまうことに留意する必要があります。

また、②の異常な通信の自動的な遮断については、「リアルタイムでの制御」や「長期継続的な運用」といった厳しい条件のもとで運用されている産業用制御システムにおいて実装は現実的ではありません。さらに、誤遮断に関わるリスクもあり、「IDS 運用監視サービス（MSS）」や「IDS 機能を有するネットワーク運用監視サービス」の提供ベンダーにおいても、自動的な遮断の仕組みまでは運用している場合は少なく、遮断の仕組みは実装しつつも、あくまで遮断するかどうかの決定は導入企業の裁量に委ねる形で運用している場合が多いのが実情です。②の異常な通信の自動的な遮断の実装にあたっては、このような産業用制御システムの運用上の制約や誤遮断に関わるリスクについて十分考慮する必要があ

ります。

さらに、③の CSIRT との連携による緊急対応については、脅威の発生原因の究明も大事ですが、その脅威が産業用制御システムにもたらす被害・影響についても判断できれば、より効果的な緊急対応が可能となります。例えば、脅威が検出されたとしても、その脅威によって産業用制御システムに被害・影響がもたらされる可能性がかなり低いと判断されれば、緊急対応まで行う必要はありません。このようにアラートに対して、産業用制御システムに対する危険度の観点からみた緊急対応の要否を判定するための基準を事前に策定しておくことが重要となります。

［緊急対応の要否を判定するための基準の例（工場の制御システムの例)］

- 既に生産活動に被害・影響が出ているもの
- 今後の生産活動に被害・影響が出る可能性が高いもの
- 今後の生産活動に被害・影響が出る可能性が低いもの
- 今後の生産活動に被害・影響が出るかどうかが不明であり継続監視が必要なもの

3.3.3. 経営層への報告

経営層にセキュリティ対策の更なる充実強化について考えるきっかけを提供するという観点から、適切なタイミングでアラートや脅威、実施した対処等に関する報告を行うことが必要です。

経営層への報告のタイミングとしては、以下に示すような目安を参考にして設定することが重要です。また、実際の報告を的確かつ円滑に行うことができるよう定期的に訓練を行うことも重要です。

経営層への報告のタイミング
（危険度が低いアラート） 月次での報告
（危険度が高いアラート） 脅威が検出されたタイミングでの報告
（脅威に対して実施した対処） 都度

第4章　検知製品等の導入後の留意点

本章では、産業用制御システム向け侵入検知製品等の本格運用を開始した後に留意すべき点ついて説明します。

4.1. 検知ポリシーの改善・更新

前述の 2.3.1.に記載した、検知ポリシーの設定・チューニングの再調整が必要となる主な場面を参考にして、専門的な知見を持った者が継続的に検知ポリシーの改善・更新のためのチューニングを行い、IDS のアラート対応担当者の負担を見直したり、現在検知できていない脅威に対応できるようにしたりする必要があります。

(1)最新の脅威インテリジェンスのフィードバックによる検知ポリシーの改善・更新

新たに発見された脅威や攻撃手法に対して迅速に対応できるようにするため、最新の脅威インテリジェンスを収集・分析し、その分析内容を検知ポリシーにフィードバックして設定・チューニングの再調整を行う形で、検知ポリシーの改善・更新における PDCA サイクルを運用することが必要となります。

(2)提供ベンダーの最新シグネチャへのアップデート

検知ポリシーの改善・更新が不要なシグネチャ型の IDS を導入・運用している企業においても、シグネチャを最新バージョンにアップデートすることや、各種ログを常に最新のものにすることが必要となります。

4.2. 他の対策製品等との連携

侵入リスクの検知精度の更なる向上や、侵入検知製品等の導入・運用を入口にして、新たな対策需要の付加によるセキュリティの向上を目指す導入企業においては、他の対策製品等を活用して、侵入検知製品等との効果的な連携を図ることが重要となります。

他の対策製品等と侵入検知製品等との効果的な連携を実現している参考事例を以下に示します。

他の対策製品等との効果的な連携を実現している事例

○IT 環境と OT 環境の境界付近に設置される「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」と、OT 環境内に設置される「IDS」との連携により、OT 環境内で脅威を検知した後、脅威と連動した効果的な防御対策を実現する

○最新の脅威インテリジェンスサービスと、侵入検知製品等との連携により、迅速な情報等のアップデートを行い、最新の脅威への対応スピード向上を実現する

(1)「IDS」と「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」との連携

IT 環境と OT 環境の境界付近に「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」を設置し、また OT 環境のネットワークセグメント間の境界付近に「IDS」を設置し、双方を連携させて運用することで、攻撃経路を分析し特定するなどの効果的な侵入検知対策を実現することができます。

また、「IDS 機能が標準搭載されたセキュリティ機器（次世代ファイアウォール等）」の中には、IDS 機能で検知された不正な侵入に関わる通信を遮断することができる防御機能として、「IPS 機能」が備わっているものが多いです。

「IDS」によって OT 環境内で検知された不正な侵入が、IT 環境を介して外部から侵入してくる不正な通信（アクセス）によるものであった場合に、IT 環境と OT 環境の境界付近に設置された「IPS 機能」と連携することで、外部からの不正な通信を遮断することができるため、効果的な防御対策を実施することができます。

(2)最新の脅威インテリジェンスサービスとの連携

4.1.で前述したとおり、検知ポリシーの改善・更新における PDCA サイクルを運用する上で、最新の脅威インテリジェンスの収集・分析は欠かせません。脅威インテリジェンスサービスと連携することにより、最新の脅威インテリジェンスと実際に現場で確認されたイベントを自動的に関連付けて、その内容を検知ポリシーにフィードバックすることができるため、最新の脅威への対応スピードを向上させることができます。

おわりに

本手引きは、これから産業用制御システム向け侵入検知製品等を導入しようと考えている企業における導入を支援し、産業用制御システム向け侵入検知製品等の基礎的な知識および留意点や、導入の進め方、導入前後の留意点などを、実際の導入済み先進企業や製品ベンダーおよびサービスベンダーへのヒアリング結果などからまとめました。

より適切な、導入目的に合わせた侵入検知製品等の選定と導入への一助となれば幸いです。

本ガイドは、以下の URL からダウンロード可能です。
https://www.ipa.go.jp/security/controlsystem/icsidshandbook.html

付録．本手引きで用いている主な用語の説明

本手引きにおける各用語の定義を示す。

用語	説明
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。本手引きでは、企業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。
SIEM ： Security Information and Event Management	サーバ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	本手引きでは、侵入検知製品の開発・提供を行う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	本手引きでは、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 OT 機器の制御を行う制御システムおよび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	本手引きでは、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。
エージェント(Agent)	監視対象のコンピューターにインストールされる侵入検知プログラムで、コンピューター上の活動の監視および解析を行う。
アラート	観測したイベントがセキュリティ上重要である(マルウェアの侵入等)と考えられる場合に発出される通知。
アノマリベースの検知 (Anomaly-Based Detection)	観測したイベントと、正常とみなされる活動内容とを比較し、正常とみなされる活動からの重大な逸脱を特定するプロセス。
アプリケーションベー	特定のアプリケーションサービス(Web サーバプログラム、データベ

スの侵入検知	ースサーバプログラムなど)を対象として、正常とみなされる活動からの逸脱の有無を監視する。
センサー	侵入検知および侵入防止システムの構成要素で、ネットワーク活動の監視および解析を行う。
シグネチャ (Signature)	マルウェアや不正アクセス等による既知の脅威に対応するパケットのパターン
ホワイトリスト (Whitelist)	無害であることが判明しているコンピューターやアプリケーションなどのリスト
ヒストリアン (Historian)	工場やプラントに設置されている OT 機器や制御プラットフォームから取得されたデータを時系列に管理するデータベース

This page is intentionally left blank

独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコート　センターオフィス
TEL: 03-5978-7527　FAX: 03-5978-7552
https://www.ipa.go.jp/security/