AhnLab

ホワイトペーパー

CPS 環境に「統合セキュリティ」が必要な理由

IT、OT そして CPS を理解する

今や、組織にとって IT (Information Technology) はとても馴染みのある概念である。そして、OT (Operation Technology) についてもある程度の理解が進んでいくなか、CPS (Cyber-Physical System) という概念が登場した。これらの定義はどのようなものだろうか? 互いにどのような関連性があるのだろうか? また、効果的な統合セキュリティ戦略とは何だろうか?

まず、OT とは産業の運用技術環境であり、産業用制御システム (Industrial Control System: ICS) などの広範囲の領域を指すものである。その延長線上で、OT セキュリティとは OT 環境を保護する行為やシステムを指す。次に、IT セキュリティと OT セキュリティの概念との違いについて理解する必要がある。基本的な答えは、単語そのものに含まれている。IT セキュリティは 「情報 (Information) 」 に焦点を置いている一方、OT セキュリティは 「運用(Operation) 」 に焦点を置いている。単に見るだけでは大差ないこともあるが、このような本質の相違により根本的なアプローチが変わっていく。

セキュリティの 3つの要素の側面から IT と OT セキュリティを紐解いてみる。セキュリティの 3つの要素とは、機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) である。これら 3つの要素はセキュリティの必須要件であり、優先順位をつけることができる。

通常、IT セキュリティでは機密性を最優先事項とし、完全性、可用性の順に重要度を位置付けている。これを、アルファベットの略字では 「CIA」 という。一方、OT セキュリティでは優先順位が多少異なる。可用性を保障することが最も重要であり、完全性、機密性の順に優先順位が確立されている。アルファベットの略字では 「AIC」 にすることができる。では、なぜこのような違いが生じるのだろうか? その理由は意外とシンプルである。コンピューターは再起動すればよいが、工場設備は安定性が最優先であり、絶対に止めることができないからである。

IT と OT 環境では、構成される機器にも違いがある。IT 環境はすでによく知られているように、PC、ノートパソコン、モバイル、サーバーなどの IT 機器により構成される。一方、OT 環境は従来の IT 機器に産業用制御システム (Industrial Control System: ICS) が加わる。産業用制御設備の代表例として、PLC (Programmable Logic Controller) を挙げることができる。PLC とは簡単に説明すると、ポンプ、バルブ、ロボットアームなど、工場内の設備に制御コマンドを送信する装置である。寿命にも違いがあり、IT 機器の寿命は約 3〜4年と短い一方、OT 機器は 20〜25年程度と、長期に渡り使用する傾向がある。

まとめると、IT と OT 環境には本質的な違いがあり、これが IT ネットワークと OT ネットワークを分ける理由でもある。これまで、OT 領域は外部からのアクセスが厳しく統制される環境の閉鎖性により、セキュリティの重要性が相対的にあまり強調されてこなかった。しかし、デジタル化が急速に進み IT 領域との接点が増加するにつれ、OT 環境を狙う攻撃が増加しており、被害規模もともに拡大している状況である。

よって、組織は (少なくとも) IT と OT を連携した統合セキュリティ戦略をもとに、ビジネスを保護しなければならない。これこそが、「CPS セキュリティ」 という概念が誕生した背景である。

CPS とは OT、IT、IoT、クラウドなどの幅広い領域のサイバー (cyber) および物理的 (physical) 要素を含む概念である。従来の製造業の枠を超え、スマートファクトリー、メディカルシステム、自動運転車などの様々な活用事例 (use case) を包括する。複数の領域を包括する CPS を保護するためには、システムの可用性を保障するなかで、様々なセキュリティモジュールの統合管理を通してセキュリティの効率性を確保し、資産に対する幅広い可視性も備えなければならない。

侵害事例

従来の OT 環境は、10年以上運用され、古い OS を使用しているケースが多く、パッチが不十分であり脆弱性が多数存在する。サイバー攻撃による被害が拡がりやすい理由でもある。これにより、CPS 環境とビジネス全体が危険に陥る可能性がある。

最近の主な CPS セキュリティ被害事故は、攻撃が製造業に集中しており、発電、エネルギー等のインフラ施設を狙うこともある。OT 環境に対する攻撃手法は、大きく 2種類に分けられる。1つ目は、IT 環境の攻撃手法を OT 環境に適用するものである。IT 環境と同様に OT 環境でもランサムウェア感染が増加する傾向が見られ、不十分な内部システムのセキュリティパッチにより残存する脆弱性を悪用したマルウェア感染事例も多い。もう 1つは、制御コマンドを改ざんして工程そのものを打撃し、被害をもたらすものである。各攻撃手法の代表的な事例を 1つずつ掘り下げていく。

まず、2019年の台湾半導体企業 TSMC の WannaCry ランサムウェア感染事例がある。TSMC はこの事故により 48時間ほど工場稼働が中断され、相当な金銭的被害を被った。TSMC のランサムウェア感染は OT ネットワークの内部設備に感染した USB メモリを使用したことから始まり、「Eternal Blue」により SMB 脆弱性を利用して素早く拡散した。この工場と連携する海外の工場までランサムウェアが感染し、被害が拡大した。

次は、米国フロリダ州の都市、オールドスマー (Oldsmar) の水処理施設のハッキング事件である。攻撃者は脆弱性を利用して施設管理者がアクセスしそうな Web サイトにマルウェアを埋め込み、社内ネットワークシステムに侵入してアカウント情報と制御設備の接続情報を窃取した。その後、リモート接続プログラムの TeamViewer を通じて水の水酸化ナトリウム濃度を操作しようとしたが、幸いにもモニタリング中であった管理者がマウスの異常な動きを捕捉し、攻撃を食い止めた。だが、下手をすれば数万人の市民の飲料水を 「苛性ソーダ」 に変える大規模テロに発展しかねない事件であった。

CPS の脅威を理解する

CPS に対する攻撃は、OT システムの外部露出が拡大するにつれ、次第に複雑化している。ただし、これを紐解いてみると、CPS 環境全体を攻撃するために IT (または外部) ネットワーク、資産および攻撃方法を活用して OT システムを侵害するものと簡単に理解することができる。

この観点から、CPS を狙った攻撃は大きく分けて ▲IT ネットワーク ▲遠隔操作プログラム ▲ストレージデバイス ▲サードパーティアクセス ▲サプライチェーンを通じて発生している。

1. IT ネットワーク

OT ネットワークは通常、外部とのインターネット接続が断絶されており、直接的な攻撃は容易でない。しかし、IT ネットワークと接続された OT ネットワーク内のシステムは、IT ネットワークを通じてマルウェアが流入する場合がある。攻撃者は OT ネットワークを直接攻撃せずに、IT ネットワークを通じて OT ネットワークへの攻撃を試みる。OT ネットワークシステムも IT ネットワークでの一般的な Windows や Linux を使用するケースが多いため、マルウェアを IT 環境と同様に使用できる。また、不完全なネットワークセグメンテーションも OT 環境が攻撃を受ける原因となる。

2. 遠隔操作プログラム

多くの OT 設備が、遠隔操作プログラムにより管理されている。攻撃者がこのプログラムを制御できるようになると、OT システムを容易に侵害、または操作することが可能になる。したがって、組織は当該プログラムのクレデンシャル情報が窃取されないよう、特に注意する必要がある。

3. ストレージデバイス

OT システムは、USB などのストレージデバイスと直接接続する場合が多い。原則的には、メンテナンス担当者が生産ラインシステムに接続される記録メディアをアンチウイルスプログラムでスキャンしてから搬入するべきである。しかし、これをきちんと確認せずに記録メディアを使用する際にワームやランサムウェアなどのマルウェアに感染することで、内部の脆弱なシステムから記録メディアが感染し、他のシステムに接続することで拡散することもある。深刻な場合、台湾の TSMC の事例のように自己伝染機能を持つランサムウェアに感染することで生産ラインが停止することもある。

4. サードパーティアクセス

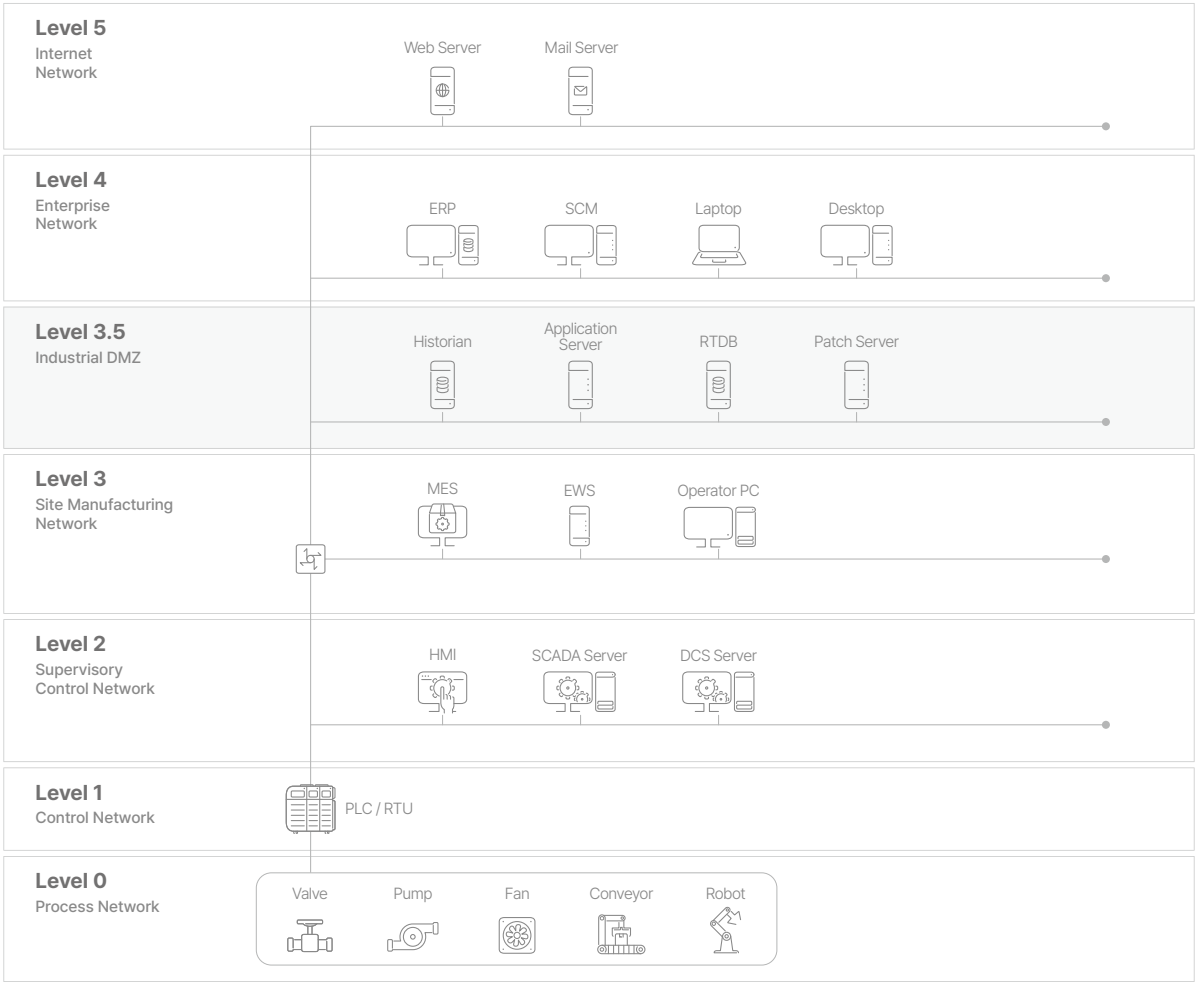
メンテナンス等を遂行する協力会社は、OT ネットワーク内のシステムに直接アクセスする場合が多い。攻撃者が協力会社で使用する記録メディア等にマルウェアを仕込むと、内部システムへすぐに侵入することができる。

5. サプライチェーン

OT ネットワーク内で運用されるシステムは専門の制作業者が提供する。攻撃者はそれらの企業を攻撃し、制作されるプログラムにマルウェアを含ませたり、マルウェアが仕込まれたインストーラーに差し替えたりする。2013年に発見された 「Havex マルウェア」 は、OT ネットワークで運用されるソフトウェアの制作者サイトをハッキングし、インストーラーにマルウェアを仕込んだ代表的なケースである。このように、サプライチェーンが提供するソフトウェアにマルウェアが含まれている場合、感染の事実を知ることが難しい。

CPS アーキテクチャ

効果的な CPS セキュリティ戦略を策定するためには、まず CPS の構造をよく理解する必要がある。これに関しては、OT 階層を Level 0から 5まで細分化した 「Purdue モデル」 は、OT セキュリティのアーキテクチャを構成するにあたり、標準として広く受け入れられている。もちろん、遠い将来の CPS には Purdue モデルを越えたアプローチが必要なものと予想されるが、IT と OT を連携したセキュリティ要件を解決するという観点において、Purdue モデルは現在、そして近い将来の CPS セキュリティにおいては依然として効果的なモデルである。



[図 1] Purdue モデル

Level 0: Process Network- 現場で運用される設備がある階層である。バルブ、ポンプ、コンベア、ロボット等の生産設備や機器のデータを収集するセンサー (sensor)、開閉装置のように 1階層からのコマンドを受け取り動作するアクチュエーター (actuator) 等で構成される。

Level 1: Control Network - 1階層は 2階層から送信されるコマンドを処理し、0階層に送る。また、0階層で収集された情報とデータを 2階層に送る。代表的な機器には、冒頭で紹介した現場の設備にコマンドを送信して統制する PLC (Programmable Logic Controller)、RTU (Remote Terminal Unit) 等がある。

Level 2: Supervisory Control Network - 2階層は現場の設備をリモートで管理し運用するシステムで構成されている。主なシステムには、SCADA (Supervisory Control And Data Acquisition) と HMI (Human Machine Interface) が存在する。SCADA は現場のデータを 1階層の PLC と RTU を通じて収集し、複数の装置をまとめて制御する。HMI は管理者が工程プロセスの特定領域のデバイスを制御できるようにする。

Level 3: Site Manufacturing Network - 3階層は全体的な生産システムを管理し、運用効率性を高める。この階層は生産活動全般を最適化する MES (Manufacturing Execution System)、機器制御のための EWS (Engineering Workstation)、製品のライフサイクルを管理する PLM (Product Lifecycle Management) 等で構成される。また、メイン HMI をホスティングして施設全体を管理する。

Level 3.5: Industrial DMZ - 産業用 DMZ (非武装地帯) とも呼ばれるこの階層は、OT 環境と外部 IT 環境が連携されるポイントである。センサーのデータを保存する RTDB (Real-Time Database) と Historian、アプリケーションサーバー、およびパッチサーバー等が Level 3.5 に属する。OT セキュリティの侵害事例が増加し、IT-OT 統合セキュリティの重要性が強調されつつある中で注目されている階層である。

Level 4: Enterprise Network – 資源管理 (ERP)、サプライチェーン管理 (SCM)、顧客関係管理 (CRM) 等、企業が一般的に IT 環境で使用する資源により構成される。工程と関連する全社的なビジネスを管理する。

Level 5: Internet Network – 5階層はインターネットまたは外部環境と最前線で接する資産が存在する階層である。設備としては、Web サーバー、メールサーバー等がある。

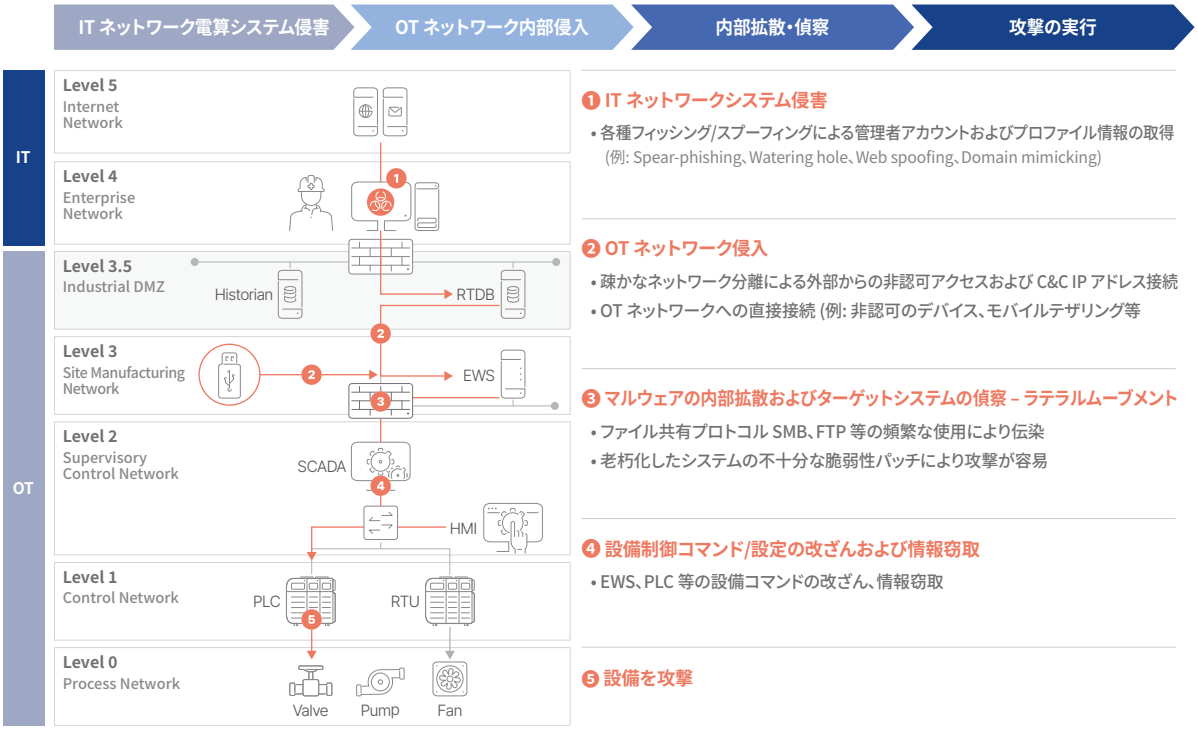
CPS の攻撃展開プロセス

セキュリティの観点から見ると、前述した Level 0~5をネットワークベースで以下のように区分できる。大きく IT ネットワーク (Level 4~5) と OT ネットワーク (Level 0~3.5) に分けられ、OT ネットワークは更に制御ネットワーク (Level 0~2) と運用ネットワーク (Level 3~3.5) に分かれる。以下は、OT 環境の階層とネットワーク別の構造とコンポーネントを総合してまとめたものである。

Level	Type	Key Components	Description
0	制御ネットワーク (OT)	· Sensors · Actuators · Production devices	現場で作業を遂行する設備
1		· PLC · RTU	現場の設備にコマンドを送信して統制
2		· SCADA · HMI · DCS	現場の設備をリモートで管理して運用するシステム
3	運用ネットワーク (OT)	· MES · PLM	生産システムの全体的な管理と運用
3.5	DMZ	· RTBD · Historian · Application servers	OT と IT 領域の接点または緩衝地帯
4	企業ネットワーク (IT)	· ERP · SCM · CRM	工程と関連する全社的なビジネス管理
5	外部インターネット (IT)	· Web servers · Mail servers	外部ネットワークと接している資産

[表 1] ネットワーク階層別コンポーネントおよび役割

上記の内容をもとに、CPS 環境を侵害する最新の攻撃フロー図を見ていく。



[図 2] CPS の攻撃展開プロセス

繰り返すが、CPS 攻撃は IT 環境から始まる場合が多い。OT ネットワークに非認可のデバイスをダイレクトに接続するケースもあるが、ほとんどは IT ネットワークのシステムが侵害された後 OT ネットワークに繋がる。OT 環境は一般的に閉域網であり、エアギャップ (Air-Gap) によるネットワークの分離とネットワークセグメンテーション (Segmentation) により構成され、攻撃対象領域 (Attack Surface) が制限される。しかし、OT 環境は IT ネットワークの管理者システムと繋がっており、IT ネットワークのシステムが先にセキュリティ脅威にさらされると、OT ネットワークのシステムネットワーク接続情報やアカウント情報が攻撃者に奪われる場合がある。

攻撃のプロセスを見ると、攻撃者は OT ネットワークを管理する IT ネットワークのシステムに、フィッシングや高度標的型攻撃 (Advanced Persistent Threat: APT) などの様々な手法で侵入する。その後、OT ネットワークシステム接続のための管理者アカウントや IP アドレス、URL 等の様々なプロファイル情報を窃取する。そして、疎かなネットワーク分離ポリシーや管理が不十分なポイントを捕捉し、OT ネットワークへ侵入する。このほかにも、セキュリティ管理がなされていない USB を通じて OT ネットワークにマルウェアが感染するか、モバイルテザリングにより非認可のノート PC を設備に直接接続する場合にも OT ネットワークのペリメータセキュリティを回避するマルウェアが侵入することがある。

その後の攻撃作業は、攻撃者側にとって簡単な方である。攻撃対象のシステムを検知してマルウェアに感染させるにあたり、OT 環境の業務の特性上、SMB ポート、リモートファイル転送、リモート接続を頻繁に使用し、パッチが不十分な老朽化したシステムが多いことにより素早く拡散していく。その後、SCADA や HMI などの運用システムに接続し、EWS または PLC を通じて異常な制御コマンドを送信したり、設備の設定を操作する等、運用に直接的な打撃を与える。

ここまで、CPS 攻撃の展開プロセスを説明した。重ねて強調するが、CPS セキュリティのためには OT セキュリティの枠を越え、IT と OT を連携した統合セキュリティ戦略が必要になる。

CPS セキュリティの要件と統合セキュリティのアクセス方法

CPS セキュリティは基本的に 「識別 > 検知 > 対応」 のプロセスが求められる。OT 領域だけでなく、IT と OT の接点、そして IT 領域までを含む 「IT & OT 統合セキュリティ」 システムを備えるべきだという事実に留意しなければならない。IT & OT 統合セキュリティは 「識別 > 検知 > 対応」 プロセスにより、エンドポイント、ネットワーク、ICS セキュリティまで漏れなく備える必要がある。以下は、全体プロセスとセキュリティ領域別の要件をまとめた内容である。

[図 3] CPS セキュリティプロセスおよびセキュリティ領域別要件

A.識別

CPS セキュリティにおいて 「識別」 とは、運用中の資産や関連情報に対する透明な 「可視性」 の確保を意味する。CPS 環境で可視性が必要な理由は、効率的なセキュリティのための根幹となるためである。OT ネットワークには様々な資産が存在し、寿命も長いため、資産の位置、状態、ネットワーク通信等を総合的に管理するのが容易ではない。したがって、各資産が正確に識別されなければ、セキュリティ脅威や可用性を侵害する設備の誤作動を検知して対応することは難しい。

可視性の基準は、資産の観点とネットワークの観点に区分できる。資産の観点では制御ネットワークの各種設備や運用ネットワークの様々なサーバーやワークステーションに区分することができ、ネットワークの観点では各資産間に接続されたネットワークセッションとこれらが使用する様々な IT/OT アプリケーションプロトコルが挙げられる。

OT ネットワーク環境の特性上、IT 環境に比べて資産やネットワークの変化が頻繁ではないため、識別された要素をベースラインにし、識別されていないセキュリティ脅威と異常な振る舞いを検知すればよい。

OT ネットワークの制御ネットワークから見てみると、資産の種類や提供ベンダー、ソフトウェアバージョン等の資産情報や設備の産業用プロトコル、およびトラフィックセッションをモニタリングする必要がある。特に、混在している異なる産業用プロトコルを標準に統合し、解析を行う能力が必須である。

次に運用ネットワークだが、エンドポイントとネットワーク領域別にセキュリティ要件が存在する。まず、エンドポイント領域ではシステム情報に対する可視性を確保する必要がある。システム情報とは、システムの種類や提供ベンダー、ソフトウェアバージョン等の様々な情報を包括する。また、工程全体にわたり使用中のアプリケーションやプロセス、そしてリムーバブルデバイスまで把握が必要である。ネットワーク領域は、ネットワークプロトコルとトラフィックセッションのモニタリングが求められる。

B.検知

識別によって可視性を確保したあとは、CPS 環境に存在する脅威要素と異常兆候を検知する必要がある。

まず、制御ネットワークでは OT 設備の異常兆候を把握する必要がある。制御コマンドの誤作動、設備障害の有無から、非認可プロトコルおよびトラフィックセッションの存在有無を総合的にモニタリングし、常に設備の安定性を保障しなければならない。

運用ネットワークでは、まずエンドポイント領域でのマルウェア検知が基本的に求められる。併せて、認可されていないアプリケーションやリムーバブルデバイスの存在有無を確認する必要がある。ネットワーク領域では、マルウェアの送信、非認可トラフィック等の脅威要素があるかどうか、持続的な検知が必要になる。

C.対応

最後に、対応とは、これまでに識別し検知した内容をもとに、最適の対策を模索し、工程に及ぼす影響を最小化することを意味する。CPS 環境の特殊性を考慮したとき、最適な対応のためには設備管理者とセキュリティ専門家の協力が求められる。CPS セキュリティの最優先課題は、運用の連続性を阻害しないことである。

OT 環境は IT 環境に比べて脅威対応に制約はあるが、運用ネットワークに対しては能動的な対応が可能である。エンドポイントセキュリティの脅威を検知した場合は、マルウェアのスキャンと駆除を行い、被害を最小化できる。デバイスの制御と脆弱性に対するパッチによる、全般的なセキュリティ強化も可能である。ネットワークセキュリティの脅威については、基本的に「セグメンテーション (segmentation)」によってネットワークを細分化し、モニタリングおよび脅威対応の効率性を向上させることができる。また、IT と OT 間のネットワーク分離によって OT 環境を保護し、アクセス制御を強化することも効果的である。

このように体系的なセキュリティアーキテクチャを備えるためには、どのようなセキュリティモジュールが必要だろうか? まずネットワーク側を見ると、サイバー脅威の検知と資産の可視性確保のための専用 IDS が要求される。また、ファイアウォールによるネットワークセグメンテーションも必要になる。一方向データ転送モジュールを活用すれば、OT ネットワークと外部ネットワーク間の通信に対するセキュリティを強化することができる。

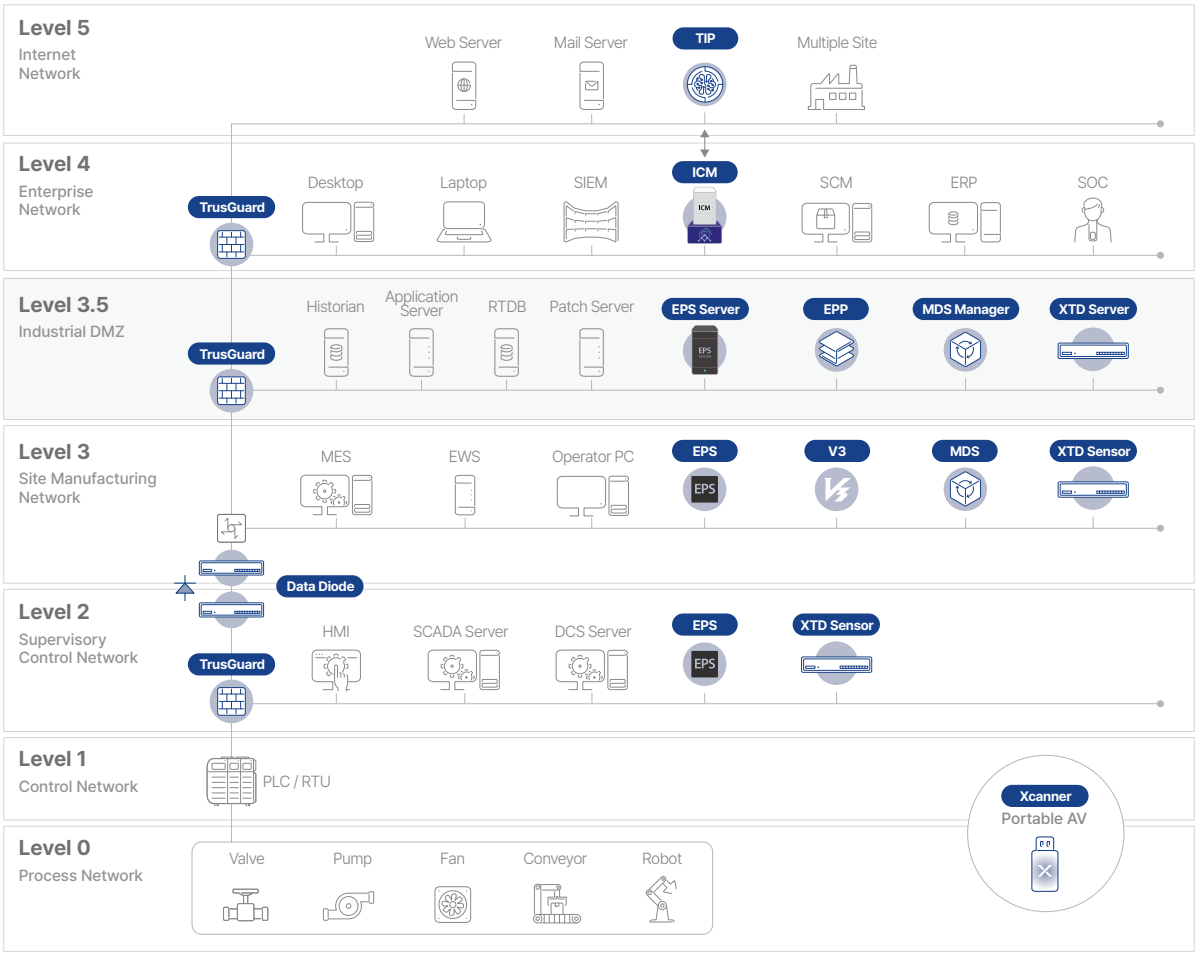
CPS のエンドポイント保護のためには、非認可の実行を防止するために許可リストに基づいたアプリケーションおよびデバイスコントロールが必要である。パッチ管理とポータブルアンチマルウェアモジュールは、CPS 設備の攻撃対象領域を減らし、マルウェアへの対応に役立つ。さらに、CPS 環境を効果的に保護するためには、使用中の IT 機器のセキュリティも備える必要がある。強力な EPP を使用することが、良いスタートになり得る。

これに加え、複数のセキュリティモジュールが統合管理される必要がある。現在の CPS セキュリティ脅威は、単一のソリューションだけでは対応が難しい。組織は、プラットフォームに基づいたアプローチにより、統合モニタリングと管理能力を備えなければならない。

AhnLab CPS PLUS: 統合 CPS セキュリティプラットフォーム

アンラボの CPS 統合セキュリティプラットフォーム 「AhnLab CPS PLUS」 は、OT エンドポイント、ネットワーク、そして OT ネットワークと接続した IT 領域までを含む CPS 環境を保護する。このプラットフォームは、これまでに製造、エネルギー、運輸など、様々な産業群の顧客のビジネスを保護してきた。

AhnLab CPS PLUS は、競合他社に比べて最も広いセキュリティカバレッジを提供するという点において差別化を図ることができる。構成モジュールの柔軟な連携に基づいたプラットフォーム戦略は、ユーザーに強力なセキュリティの効率性とビジネスの生産性を提供する。



[図 4] AhnLab CPS PLUS の構造図

AhnLab ICM
CPS 統合モニタリングに基づく
可視性の提供、および
セキュリティモジュールの管理

AhnLab EPS
OT エンドポイントプロセスおよび
デバイスコントロール、
マルウェア検知

AhnLab XTD
OT ネットワークの可視性の確保、
および異常な振る舞いなどの脅威検知

AhnLab Xcanner
OT エンドポイントの
マルウェア検知と駆除のための
ポータブルアンチマルウェア

AhnLab TrusGuard
OT ネットワークセキュリティおよび
セグメンテーション

AhnLab Data Diode
物理的な一方向データ転送による
OT 環境のアクセス制御

AhnLab MDS
ネットワークのサンドボックス解析により、未知のマルウェアを検知

AhnLab EPP/V3
CPS 環境内の IT 機器に対する
アンチマルウェアおよび
統合パッチ管理

AhnLab TIP
IT と OT 環境にわたる
CPS 脅威インテリジェンス

アンラボの脅威検知＆対応能力と OT セキュリティ技術を結集した AhnLab CPS PLUS は、CPS 環境全般にわたり 「識別 > 検知 > 対応」 につながる統合セキュリティプロセスを構築する。プラットフォームは計 9つのセキュリティモジュールで構成されており、統合管理モジュールである AhnLab ICM を通じてモニタリングおよび中央管理が行われる。

ドメイン	モジュール	1段階：モニタリング & 識別	2段階：脅威の検知	3段階：対応	4段階：後続措置
IT & OT	ICM	• IT & OT 資産リストの収	• ログ解析 • 詳細解析レポートの照会	• Lockdown 除外処理項目の変更 • マルウェアポリシーが適用されていないエージェントの確認	• 駆除の必要有無の確認 • Rest API 対応ポリシーの適用
Endpoint (OT)	EPS	• 生産設備資産の識別	• 既知のマルウェア	• マルウェアスキャン • 非認可プロセス遮断 • デバイス実行遮断	• Lock モードへの切替 • AhnReport 解析のリクエスト
Network (OT)	XTD	• OT 資産の識別 • 資産別トラフィックの識別	• マルウェア拡散 • 脆弱性等のネットワーク脅威 • 異常な PLC ロジック	• 脅威検知対応アラート	
Endpoint (OT)	Xcanner			• 感染設備でマルウェアの検知/駆除	
IT & OT	TrusGuard		• ネットワーク脅威 • 非認可トラフィック	• ACL 基盤の非認可セッションの遮断 • 有害トラフィック遮断	• ファイアウォールポリシーの設定 • ネットワークセグメンテーション
Network (OT)	Data Diode			• 一方向データ転送	
IT & OT	MDS		• 既知/未知のマルウェア • 感染設備のネットワークでの異常な振る舞い • 振る舞い解析の回避	• MDS 正·誤検知の確認 • ピンポイントスキャン	
Endpoint (IT)	EPP/V3	• パッチ管理	• IT マルウェア	• IT マルウェアの駆除	• EPP/AV ポリシーの設定
IT & OT	TIP				• 脅威情報の照会

[図 5] AhnLab CPS PLUS のモジュール別の役割

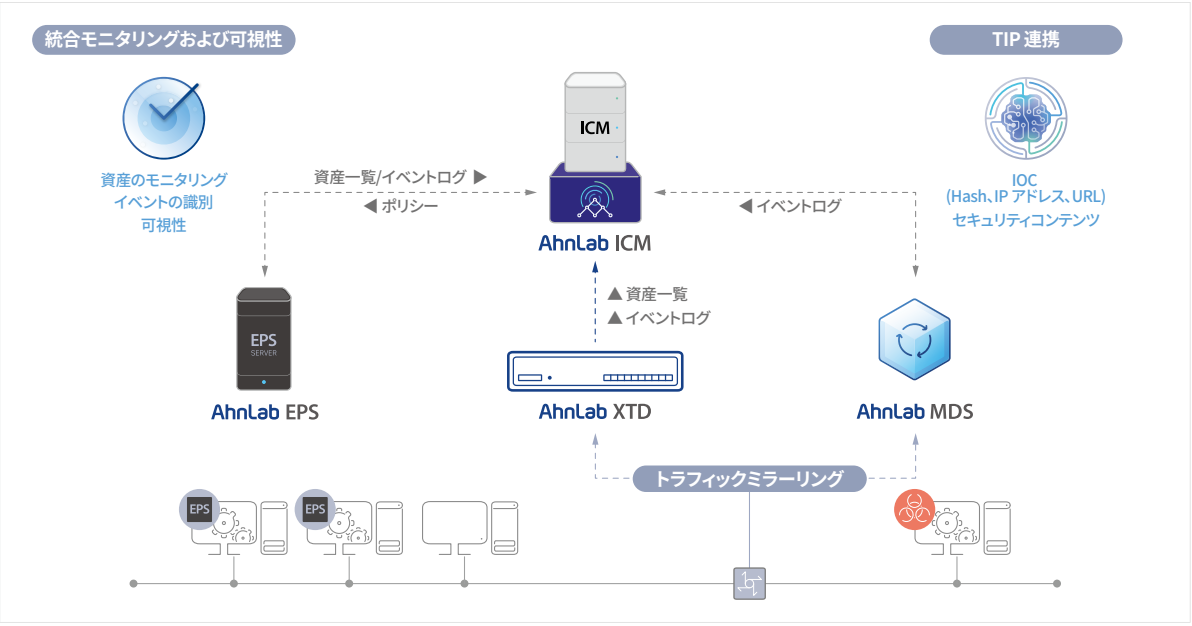
AhnLab CPS PLUS セキュリティモジュールの役割

AhnLab CPS PLUS の 9つのセキュリティモジュールは、CPS を保護するという共通の目的を持ちつつ、異なる役割を遂行する。各セキュリティモジュールの役割と、それぞれが互いにどう連携するかを説明する。

ICM (+TIP)

セキュリティプラットフォームにおいて最も重要な能力は、連携するモジュールを統合モニタリングおよび管理することである。AhnLab CPS PLUS では、AhnLab ICM がその役割を遂行する。管理者は、直観的なダッシュボードを通じて CPS 環境全般の可視性を確保し、CPS セキュリティの核心となるモジュールを中央管理することができる。

AhnLab EPS、XTD、MDS 等、CPS セキュリティモジュールと連携する ICM は、モジュール状況やログ統合照会、および検索機能を提供し、管理者が措置が必要なイシューを即刻確認できるようにする。ユーザーは ICM を活用してビジネスの連続性、効率性と生産性を強化し、真の 「CPS セキュリティプラットフォーム」 の恩恵を享受できる。

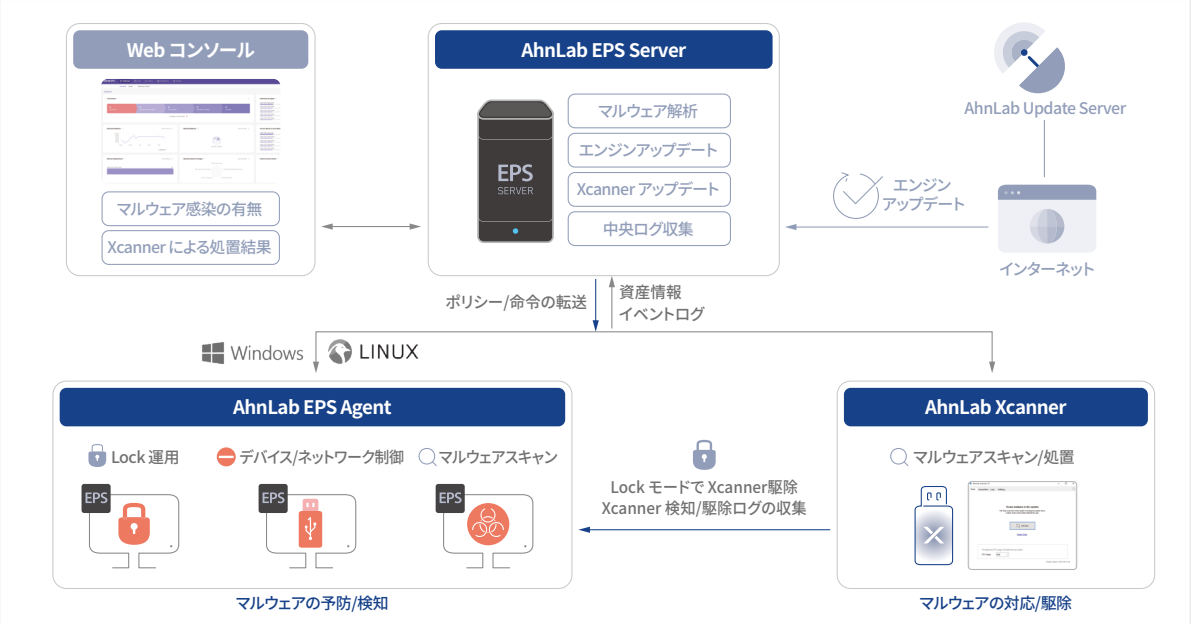


[図 6] AhnLab ICM の中央管理アーキテクチャ

また、ICM は当社の脅威インテリジェンスプラットフォーム、AhnLab TIP との連携により、真のインテリジェンスベースの CPS セキュリティを実現する。管理者は、IT と OT が統合された CPS 環境のセキュリティ脅威に対する侵害指標 (IoC) を通じて、より詳細な情報をリアルタイムで確認できる。

EPS (+Xcanner)

OT エンドポイントセキュリティモジュール AhnLab EPS は、長きに渡り製造業、発電所等、様々な産業群の企業の CPS 環境を保護してきた。EPS の直観的な Web ベースコンソールは、事業所内の OT 設備を正確に識別し管理できるようにする。OT 設備の運用安定性のため、エージェントをできる限り軽くしており、各種スキャンや解析などの負荷を与えることができるタスクはサーバーで実行する構造である。EPS は、Windows、Linux など、セキュリティアップデートやパッチが適切に行われていない古い OS までスムーズにサポートする。



[図 7] AhnLab EPS と Xcanner の構造

EPS の特長は、許可リスト (allowlist) ベースの制御技術を適用し、認可されたデバイスとネットワークのみが実行されるようにし、潜在的な侵害の可能性を最小化することである。認可された許可リストは自動で作成・適用されるため、ポリシー設定に対する管理者の負担を軽減させる。

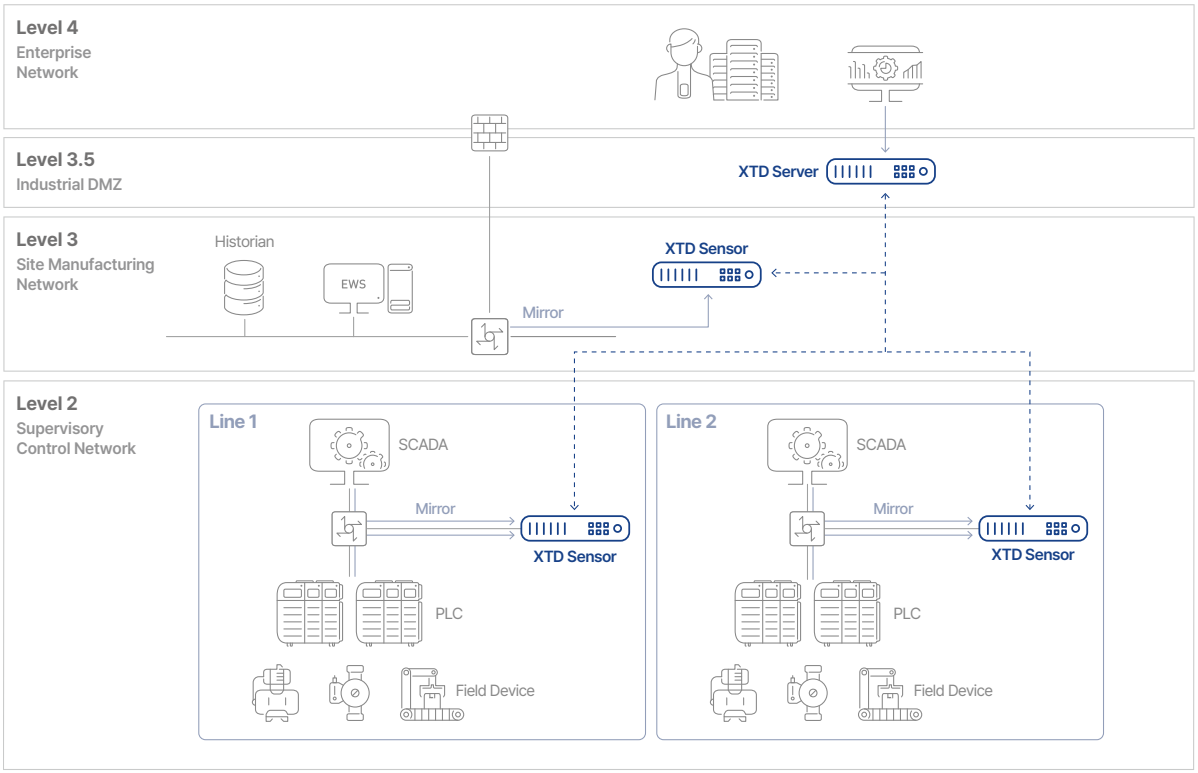
EPS は 3段階の運用モードに対応しており、ユーザーの利便性とセキュリティ設定の安定性を強化する。まず、3段階の運用モードにはシステムアップデートのためにロックを解除する Unlock Mode、運用機器のために Lock Mode の運用前にポリシーを検証する Lock Test Mode、そして実際のシステム運用時に適用する Lock Mode がある。Lock Mode は、運用の安定性と連続性を保障するため、システム上で除外処理した項目を除く、いかなる変更も許可しない。

また、EPS は OT 設備を標的とする既知のマルウェアを検知および遮断する。エージェントでマルウェアを検知し、サーバーで詳細解析を行う。これにより、システムに負荷をかけることなくマルウェアのリアルタイム検知、解析および遮断が可能となる。

OT 設備がマルウェアに感染した場合、ポータブルのアンチウイルス、AhnLab Xcanner を利用してマルウェアを駆除できる。Xcanner は認可済みの USB にインストールするか、EPS エージェントを活用してダウンロードすることができる。Xcanner のスキャンおよび駆除の履歴と関連ログは、EPS サーバーでモニタリングおよび管理される。Xcanner の長所は、マルウェア対応プロセスを簡単かつ直観的に設計することで、専門家でなくとも侵害事例に容易に対応できるようにした点である。

XTD

AhnLab XTD は、ネットワークベースの OT ネットワーク可視性を提供し、セキュリティ脅威および異常な振る舞いをリアルタイムで検知する。可用性を重視する OT 環境の特性を考慮し、設備運用に影響を与えないよう、ネットワークトラフィックをミラーリングする 「パッシブモニタリング」方式で動作し、運用の安定性を保障する



[図 8] AhnLab XTD の運用構造

XTD は OT エンドポイントセキュリティモジュールと連携し、エンドポイント領域に対する可視性とマルウェアスキャン、そして駆除までを提供することが特徴である。また、多数の OT プロトコルに対する DPI (Deep Packet Inspection) 解析技術を通じて、様々な種類の設備の識別や異常な制御ロジックの検知および解析能力を提供する。

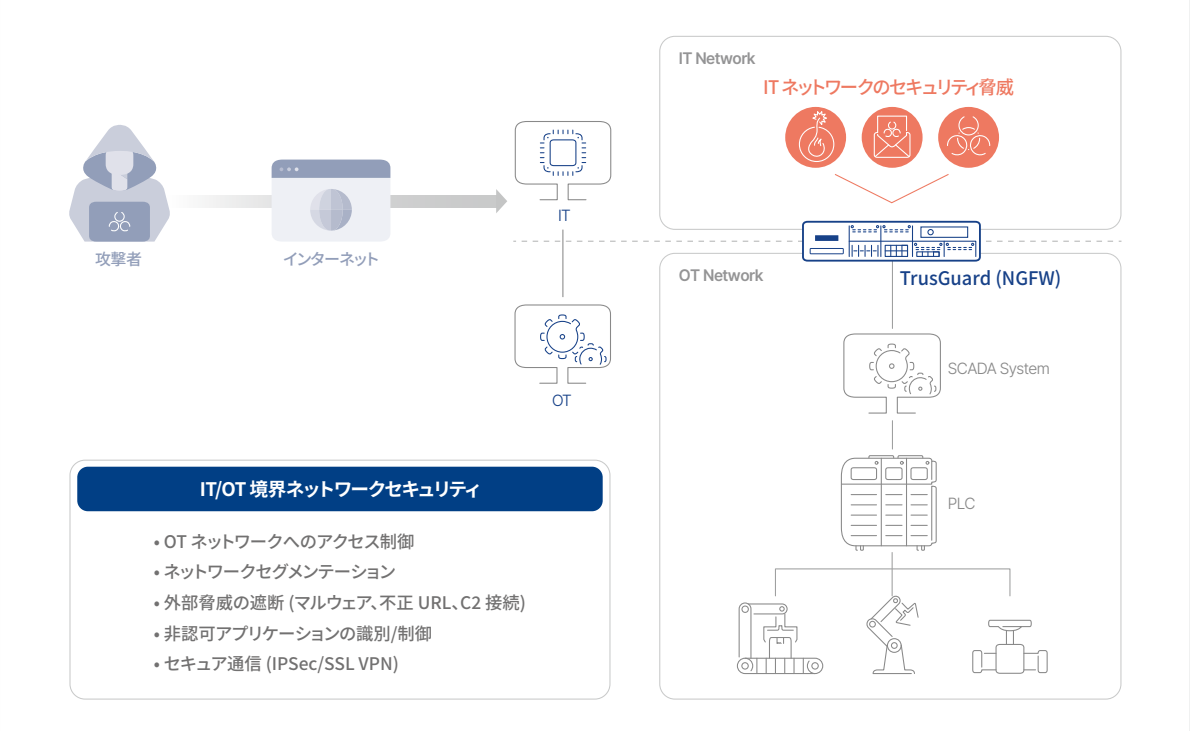
XTD を EPS と連携すると、OT ネットワークに接続されているエンドポイントまで可視性を拡大できる。同種のソリューションのほとんどは、ネットワーク領域までの資産状況を提供する。しかし、XTD は EPS と連携してネットワーク領域だけでなく、OT ネットワークに接続されているサーバーおよびワークステーション (Workstation) の OS パッチバージョン等、エンドポイントの詳細情報まで可視性を拡大できる。

Xcanner と連携すると、マルウェアのスキャン領域も拡張できる。一次的にネットワークでマルウェアの拡散または脆弱性を悪用する有害トラフィックが検知されると、エンドポイント領域に位置する疑わしいシステムに対しても再度マルウェアのスキャンを実行することができる。また、ネットワークでのセキュリティ脅威の検知だけを提供するほとんどの同種のソリューションとは異なり、脅威の根源に対するマルウェアスキャンまで可能であるため、より能動的な脅威対応が可能である。

このほかに、検知した脅威の配布元をトレースバックして脅威インテリジェンスを通知する「脅威トラッキング (Threat Tracking)」機能も提供する。この機能は、攻撃の配布元を確認し、攻撃の伝播および移動経路を把握できるようにする。これにより、ユーザーは検知した脅威イベントの配布元、および最初に発生した資産等、脅威間の連携性を確認し、体系的な脅威対応を行うことができる。

TrusGuard

ファイアウォールモジュール AhnLab TrusGuard は、OT ネットワークの境界でインバウンドおよびアウトバウンドトラフィックを制御し、マルウェア、URL、C2 接続トラフィックなどの有害トラフィックを遮断し、IPSec/SSL VPN などのセキュア通信とネットワークセグメンテーションなどの機能もサポートする。

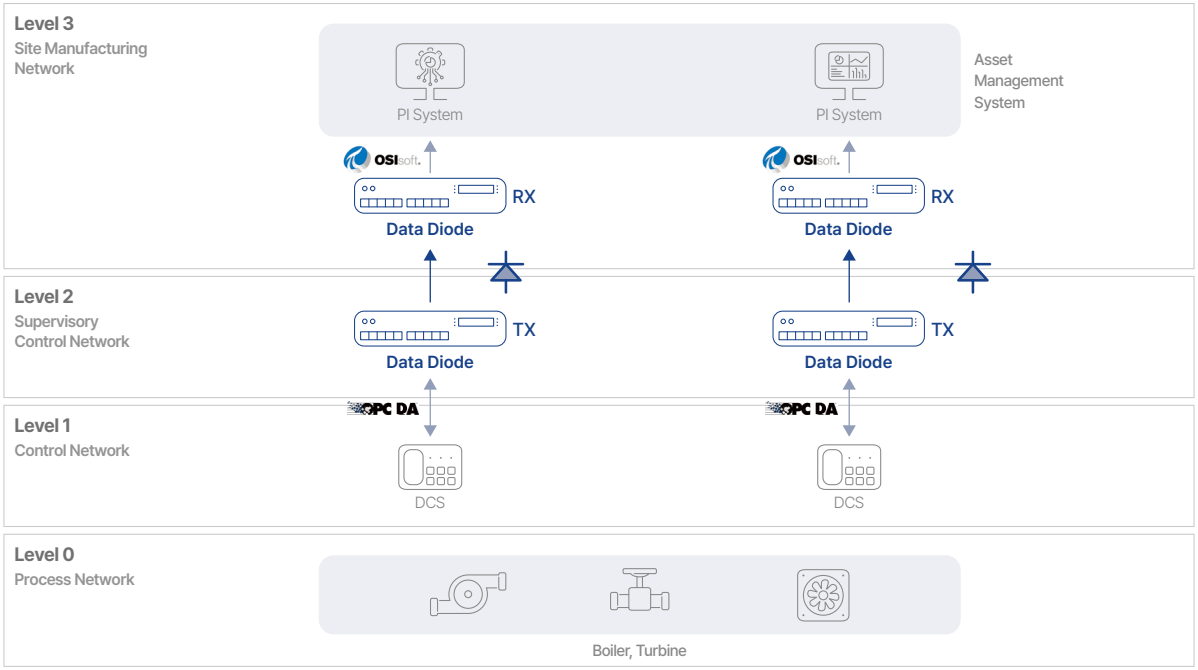


[図 9] AhnLab TrusGuard のネットワーク境界のセキュリティ構造

また、OT プロトコル解析技術を適用し、OT ネットワーク内部で産業用プロトコルを細かく制御できる。具体的には Modbus、DNP3 等のプロトコル別の制御だけでなく、Function Code までを識別して制御することが可能である。

Data Diode

AhnLab Data Diode は、セキュリティレベルが異なるネットワーク間の接続において、セキュリティレベルが高いところへのアクセスを強化するために、物理的な一方向転送に基づき必要なデータのみを安全に外部へ転送する。データの暗号化、前方誤り訂正 (Forward Error Correction、FEC)、データ送信エラー制御、マルウェアスキャンなど、様々な技術を適用し、転送データの信頼性と安定性を最大化した。



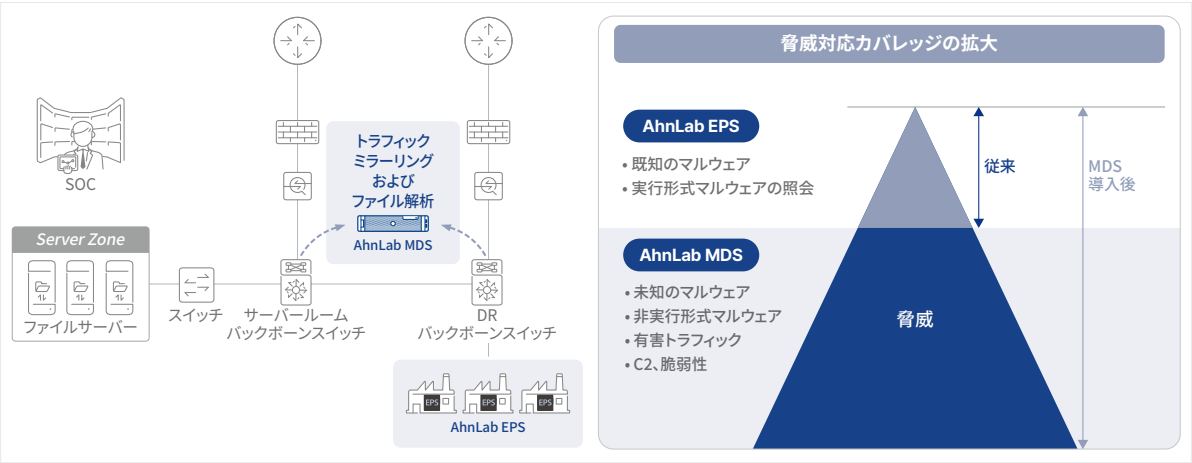
[図 10] AhnLab Data Diode の構造図

また、OT プロトコル解析技術を適用し、OT ネットワーク内部で産業用プロトコルを細かく制御できる。具体的には Modbus、DNP3 等のプロトコル別の制御だけでなく、Function Code までを識別して制御することが可能である。

MDS

最近、サイバー脅威が高度化し続けている中、高度標的型攻撃 (Advanced Persistent Threat: APT) や新種/亜種のマルウェアが増加傾向にある。したがって、既知 (Known) のマルウェアだけでなく、未知 (Unknown) のマルウェアに対する解析と対応が必要になった。

ネットワークサンドボックスモジュール、AhnLab MDS は、生産ネットワークのトラフィックに存在するファイルを収集して解析し、未知のマルウェアに対する動的解析を行う。また、攻撃者の C&C IP アドレスの接続まで検知して解析するため、OT ネットワークのマルウェア拡散経路、C&C、脆弱性等、様々なセキュリティ脅威のモニタリングと感染した設備の駆除および対応を提供する。

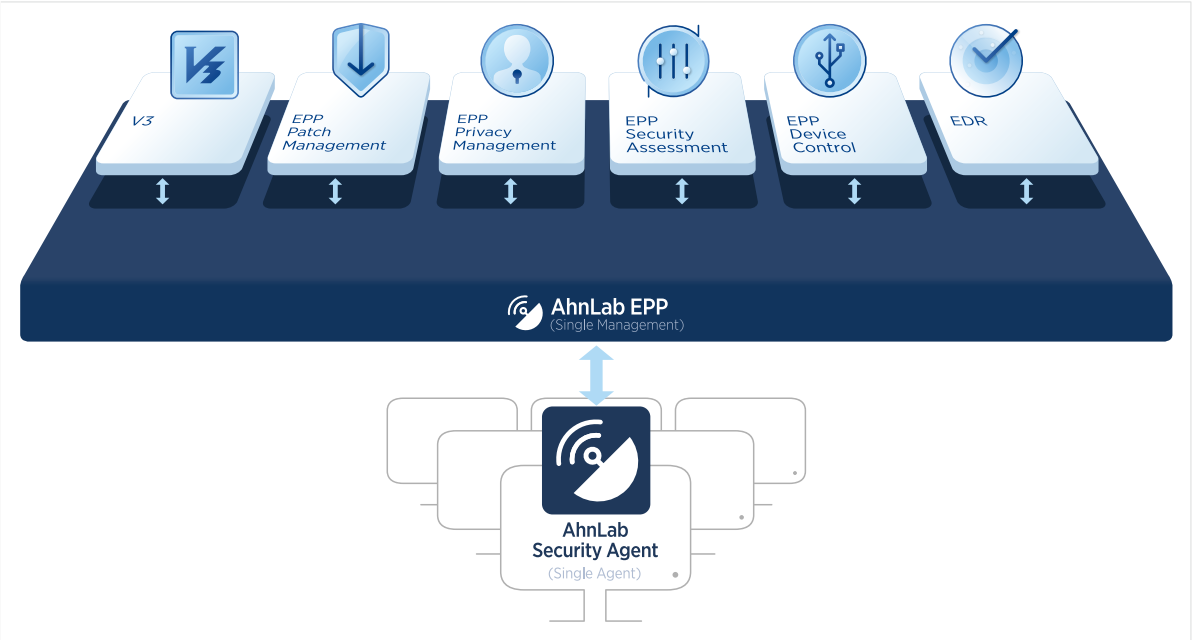


[図 11] AhnLab EPS と AhnLab MDS の連携による脅威カバレッジの拡大

特に、EPS と連携すると、MDS の動的解析機能をもとに新種、亜種および未知のマルウェアまで防御することが可能となり、総合的な脅威対応カバレッジを拡大できる。

AhnLab EPP/V3

CPS 環境では OT セキュリティだけでなく、OT 環境と接続された、または OT 環境を管理する IT 領域のセキュリティも考慮する必要がある。必須となる能力は、パッチ管理による脆弱性の最小化と、アンチマルウェアによる脅威の強力な遮断である。



[図 12] AhnLab EPP の構造図

AhnLab EPP はアンチマルウェアからパッチ管理まで、様々なモジュールを有機的に連携させ、IT 環境における脅威が OT 環境を侵害することを防ぐ。まず、複数のエンドポイントシステムに安定的、かつ幅広いパッチ管理機能を提供し、エンドポイントの攻撃対象領域を減らす。また、アンチマルウェアモジュール (V3) は AV-TEST などグローバル認証評価において、長期にわたってトップレベルの検知率を記録しており、実績のある技術力に基づいて世界トップレベルの脅威遮断能力を提供する。

導入効果

AhnLab CPS PLUS は、IT-OT 統合セキュリティをベースに、CPS セキュリティの要件を効果的に解決する。これにより、ユーザーは真のデジタル革新に拍車をかけることができる。

導入効果 #1: 運用可用性の保障

CPS 環境の最優先課題は、設備運用の可用性を保障することである。AhnLab CPS PLUS は、CPS 環境の特殊性に最適化された複数のセキュリティモジュールを通して、システム負荷なしで強力なセキュリティを実現する。

導入効果 #2: 体系的な脅威管理プロセス

AhnLab CPS PLUS は、「識別 > 検知 > 対応」 につながる体系的な脅威管理プロセスを備えている。CPS の資産詳細を識別し、OT ネットワーク内部に拡散する各種脅威や異常兆候を検知して、工程に影響を及ぼさない最適な対応能力を提供する。

導入効果 #3: 便利な統合管理とモニタリング

AhnLab CPS PLUS は統合管理コンソール AhnLab ICM を通じて、CPS エンドポイントおよびネットワークセキュリティモジュールだけでなく、SIEM、TIP とも柔軟に連携する。これによって、CPS 環境のセキュリティ脅威を効果的に管理できるよう、運用利便性を提供する。

結論

CPS 環境を狙うサイバー攻撃は持続的に増加しており、被害規模もますます拡大していくものと予想される。組織は OT セキュリティの理解を深めている段階にあるが、今後は IT と OT という異なる環境を統合した CPS セキュリティの観点から考えていく必要がある。これは組織にとっても簡単ではない課題だが、CPS セキュリティのアプローチ方法とアーキテクチャを正しく理解していれば、不可能なミッションではない。

組織が CPS セキュリティイニシアチブを推進するにあたって留意べき 3つの推奨事項は、次の通りである。

#1.OT セキュリティだけでなく、IT セキュリティもセットで考えること

本文書で何度も述べたように、OT 環境を標的とする脅威は OT と接続された IT 領域から始まる。したがって、CPS セキュリティを効果的に遂行するためには、IT と OT を融合した統合セキュリティのアプローチを目指す必要がある。遠い将来では、CPS の接続ポイントが IT と OT を越え、様々な領域に拡大する見通しだ。

#2.「識別 > 検知 > 対応」 につながるセキュリティプロセスを構築する

資産の識別と脅威検知および対応は、CPS セキュリティの根幹である。特に、OT 環境においては資産やネットワークの変更があまり発生しないため、十分な資産の可視性と正確な脅威検知能力をもとに脅威対応プロセスを構築すれば、長期的に大きな効果が期待できる。

#3.単体のソリューションではなく、プラットフォームに基づいたアプローチを目指すこと

今日の CPS セキュリティ脅威は、もはや単一ソリューションで解決できるレベルを超えている。そして、脅威はこれからも更に高度化していくだろう。ゆえに、複数のセキュリティモジュールが柔軟に相互連携する CPS セキュリティプラットフォームが必要になる。最適なセキュリティ機能と統合的な可視性、および管理能力を提供する CPS セキュリティプラットフォームは、日に日に進化する CPS の脅威に対応するための唯一の手段である。

アンラボは、日々増大する CPS セキュリティの要件を解決する最適なパートナーとしての地位を確固たるものにしている。AhnLab CPS PLUS は、IT と OT 環境にわたって連携する複数のセキュリティモジュールを中央管理・モニタリングし、プラットフォームの幅広いセキュリティカバレッジは競合他社と比べて差別化された要素である。各産業にわたる様々な顧客リファレンスはプラットフォームの優秀性を立証し、これからも各モジュールの機能を強化していくとともに、連携と連動を強化して未来志向的な活用事例 (use case) に対応する予定である。

AhnLab

株式会社アンラボ
東京都港区芝4丁目13-2 田町フロントビル3階 〒108-0014
Tel: 03-6453-8315 | URL: www.ahnlab.com/jp | Mail: jp.sales@ahnlab.com