AhnLab

AhnLab CPS PLUS

統合 CPS セキュリティで実現するデジタル革新

IT-OT を融合した
CPS 統合セキュリティプラットフォーム

背景

これまで、OT 環境は外部からのアクセスが厳しく統制される閉鎖性により、IT 環境より比較的安全だと考えられてきました。しかしながら、急速に進むデジタル化によって IT 領域との接点が増加し、OT 環境に対するサイバー攻撃も増加している傾向があります。今や、OT セキュリティの重要性が高まっていることはもちろん、OT と IT を連携した新たな統合セキュリティのアプローチが必要な状況です。

サイバーフィジカルシステム（CPS: Cyber-Physical System）は、従来の OT 領域における外部接続の拡大にともない、OT、IT を合わせた包括的な領域を網羅する概念です。複数の環境をカバーする CPS を効果的に保護するためには、基本的に OT 環境で優先される「可用性（availability）」を保障しつつ、資産の可視性を提供するなかで、複数のセキュリティモジュール間の連携および中央管理によってセキュリティの効率性を確保できる必要があります。

可用性の確保

IT と OT を統合する CPS 環境では、まず寿命が長く、セキュリティパッチが困難な OT 環境での複数の設備をセキュリティ脅威から保護し、安全に動作できるようにする必要があります。

可視性の確保および脅威検知/対応

可視性の確保が困難な OT 環境において、資産情報、ネットワーク状態、セキュリティ脅威および脆弱性状況に関する可視性を確保する必要があります。また、各種設備の可用性を保障できる範囲内で、セキュリティ脅威を検知し、対応する必要があります。

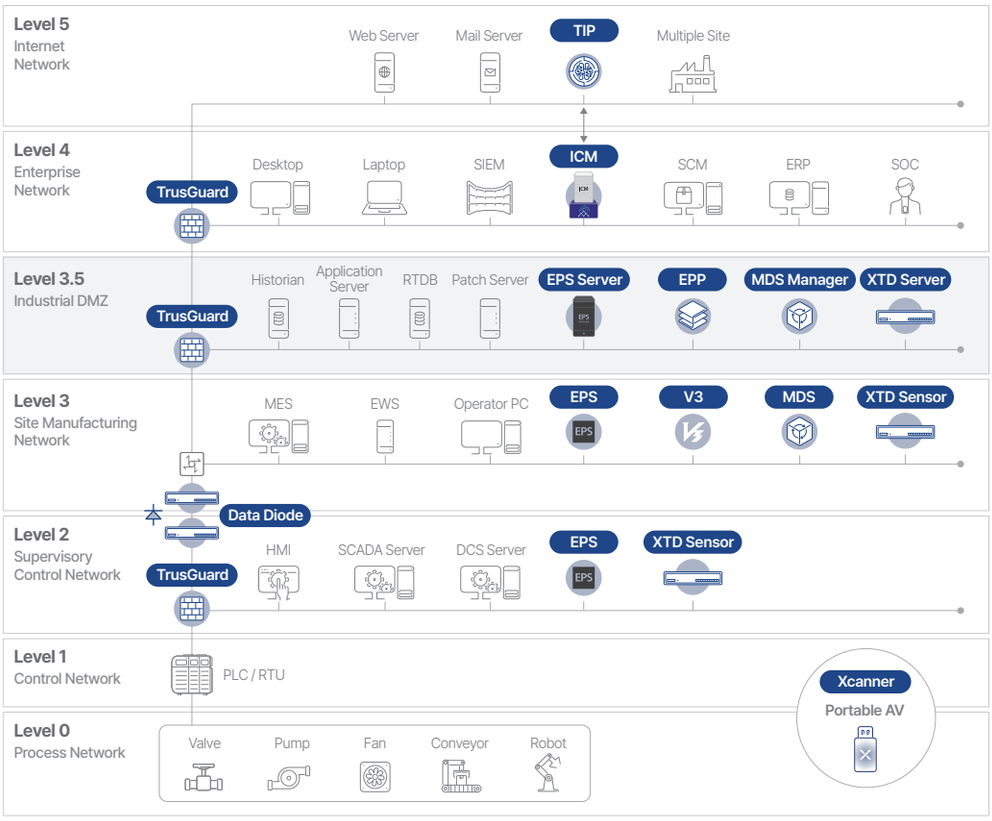
IT と OT の連携セキュリティ

OT ネットワークは閉域網ですが、IT ネットワークシステムとの接点が拡大し、様々な攻撃が頻繁に発生しています。そこで、IT と OT セキュリティを連携した CPS セキュリティの観点からのアプローチが必要となります。また、個別のソリューションではなく、セキュリティモジュール間の連携と中央管理に対応する統合セキュリティプラットフォームが求められます。

Why AhnLab CPS PLUS

AhnLab CPS PLUS は、製造、精油、運送などの各種産業の OT エンドポイントとネットワーク、さらに OT と接続された IT 環境まで、幅広く保護する統合 CPS セキュリティプラットフォームです。AhnLab の脅威検知＆対応の専門性と OT の技術力を結集した AhnLab CPS PLUS は、エンドポイントとネットワークセキュリティの技術をもとに、IT と OT を含む CPS 環境において ▲識別（可視性）▲脅威検知 ▲対応につながる抜かりのないセキュリティを提供します。プラットフォーム内で柔軟に連携できるセキュリティモジュールは、CPS セキュリティ統合管理ソリューション「AhnLab ICM」によって効率的にモニタリング、運用することが可能です。

AhnLab CPS PLUS は、現在市場で提供されている CPS セキュリティプラットフォームのうち、最も幅広いカバレッジを誇ります。さらに、卓越した技術力と統合のシナジーが加わることで、顧客に差別化された CPS セキュリティ体験を提供します。



AhnLab ICM
CPS 統合モニタリングベースの可視性の提供と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とデバイスコントロール、マルウェア検知

AhnLab XTD
OT ネットワーク可視性の確保、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を検知・駆除する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を通じて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

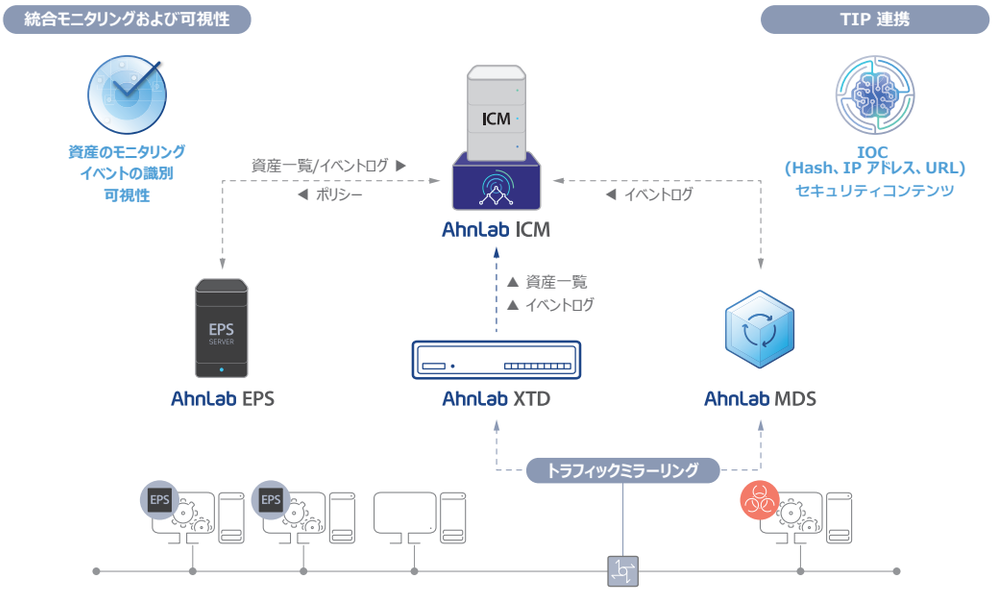
AhnLab TIP
IT と OT 環境を含む CPS 脅威インテリジェンス

構成モジュール

1.AhnLab ICM (+TIP)

CPS セキュリティの統合管理を担当する AhnLab ICM は、ひと目で連携モジュールの状況把握が可能なダッシュボードにより、CPS 環境の統合的な可視性を確保することができます。AhnLab EPS、XTD、MDS などの CPS 環境全般にわたるモジュール状況と資産情報の収集、イベントモニタリングを通じて、対応が必要なイシューをリアルタイムで確認できます。このようなプラットフォームベースの中央管理能力をもとに、統合的な可視性と総合的な脅威モニタリングを提供し、イシューに対する措置に要する時間を短縮させ、業務の連続性と生産性を向上させます。

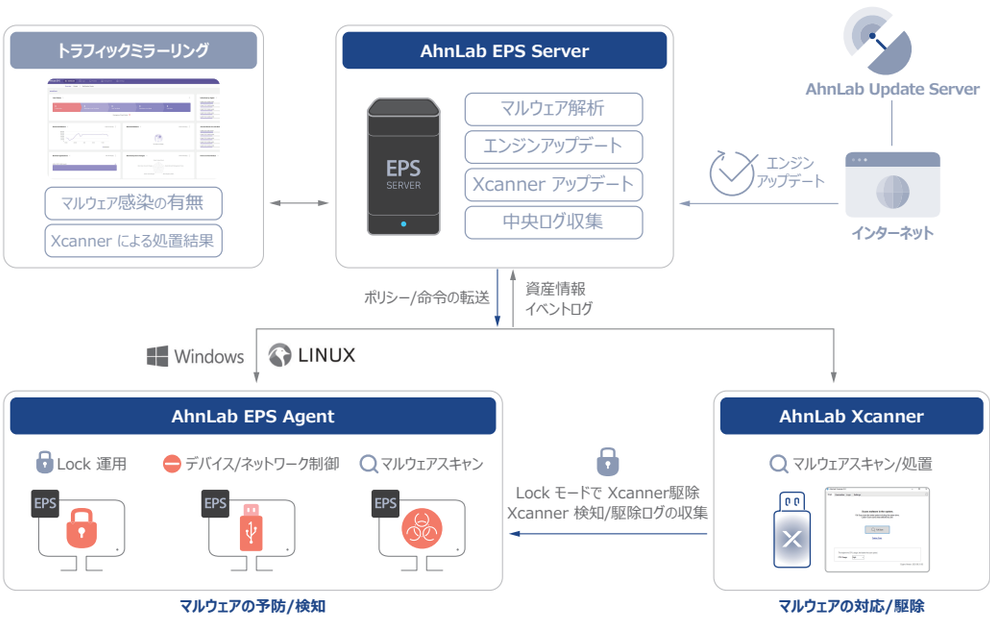
AhnLab TIP は AhnLab ICM との連携により、CPS セキュリティプラットフォームに脅威インテリジェンスを供給します。AhnLab ICM で、IT と OT を含む CPS 環境のセキュリティ脅威に対する侵害指標 (IoC) を通じて、より詳細な情報をリアルタイムで確認できます。



2.AhnLab EPS & Xcanner

OT ネットワーク設備のセキュリティに最適化された AhnLab EPS は、ビジネス連続性の確保のために、不要なプログラム、リムーバブルデバイス、ネットワーク接続などを遮断します。また、設備の寿命が長い環境の特性に合わせて、Windows、Linux、組み込みバージョンなどの様々な OS に対し、旧バージョンから最新バージョンまで運用をサポートしています。設備可用性の保障のための超軽量エージェントによりシステムリソースの消費を最小化し、許可リストに基づく統制を適用するときは 3段階の Lock 運用モードをサポートしており、ポリシーを柔軟に適用できるようにします。

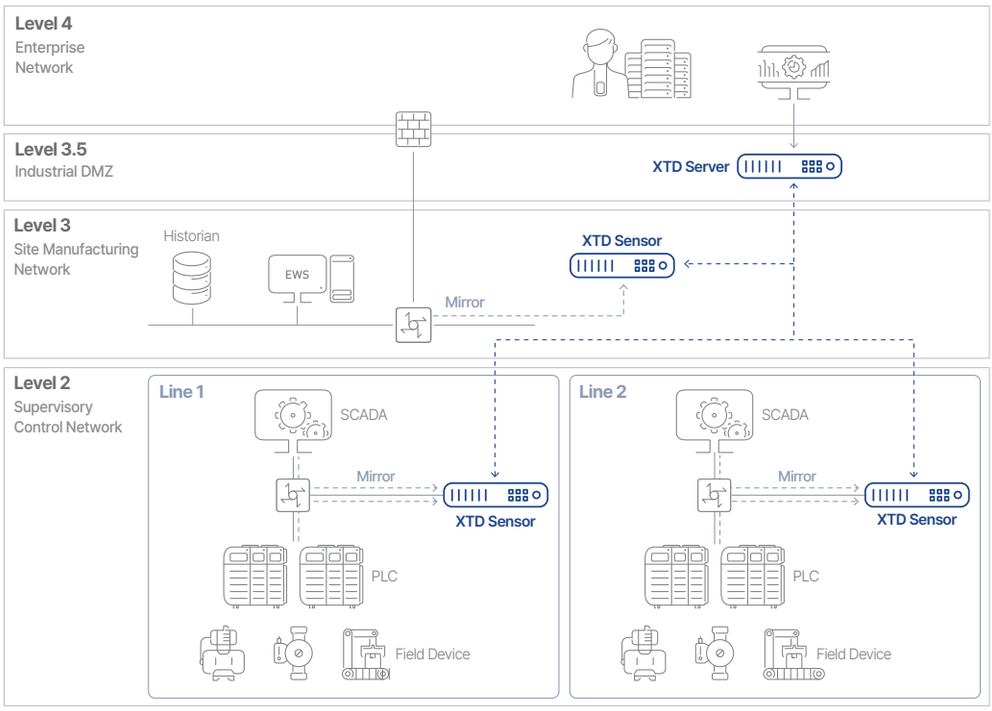
さらに、マルウェアへの感染が疑われるシステムに対しては OT ポータブルアンチマルウェアである AhnLab Xcanner を活用し、他のソリューションをインストールすることなく、マルウェアの検知および駆除が可能です。AhnLab Xcanner は認可されたリムーバブルディスクに搭載したり、EPS Server から EPS Agent に転送してリモートで実行する形式でも使用することができ、スキャンと駆除の状況は EPS Server でモニタリングおよび管理することができます。



3.AhnLab XTD

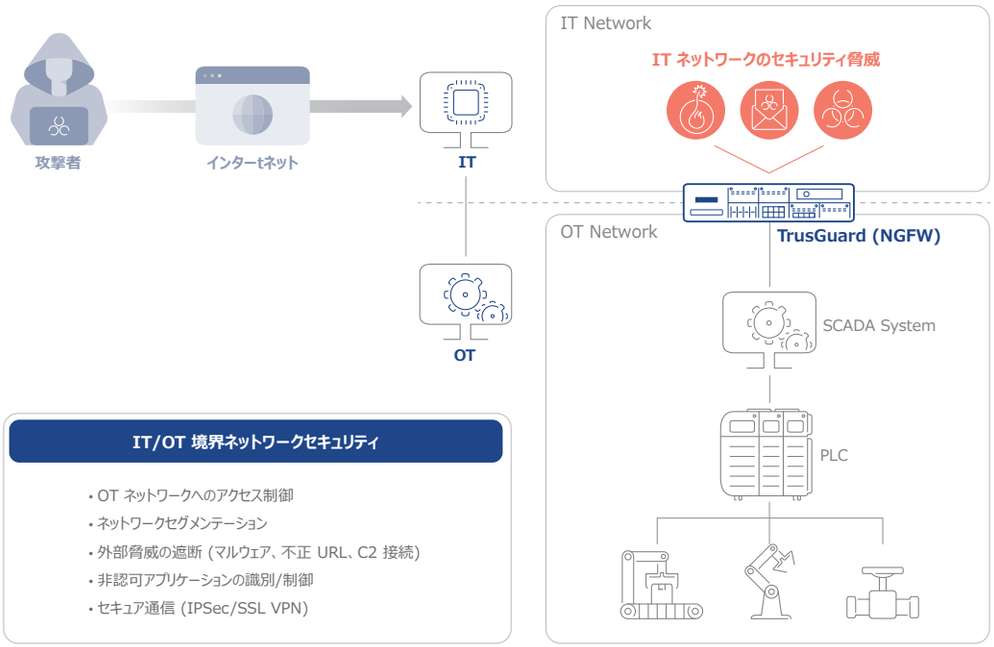
AhnLab XTD は OT ネットワークベースの可視性および脅威検知モジュールであり、様々な OT ネットワークの資産に対する可視性を提供します。また、IT ネットワークから流入または OT ネットワーク内部システム間で拡散するマルウェア、あるいは脆弱性などのセキュリティ脅威を検知します。OT 設備の可用性を保障するパッシブスキャン（passive scan）方式を使用し、自社開発したプロトコルプロファイリング技術とディープ・パケット・インスペクション（DPI）機能をもとに、様々な種類の設備の識別と異常な制御ロジックの検知と解析を提供します。

さらに、OT エンドポイントセキュリティモジュールである AhnLab EPS との連携により、エージェントから収集されたデバイスの詳細情報を結合し、幅広くて詳細な資産可視性を提供します。両モジュールの連携は、OT ネットワークへ拡散するセキュリティ脅威を検知して対応する側面においても、卓越した能力を発揮します。AhnLab EPS サーバーの Restful API 連携により、Xcanner のリモートスキャンをサポートし、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スキャンを実施できます。



4.AhnLab TrusGuard

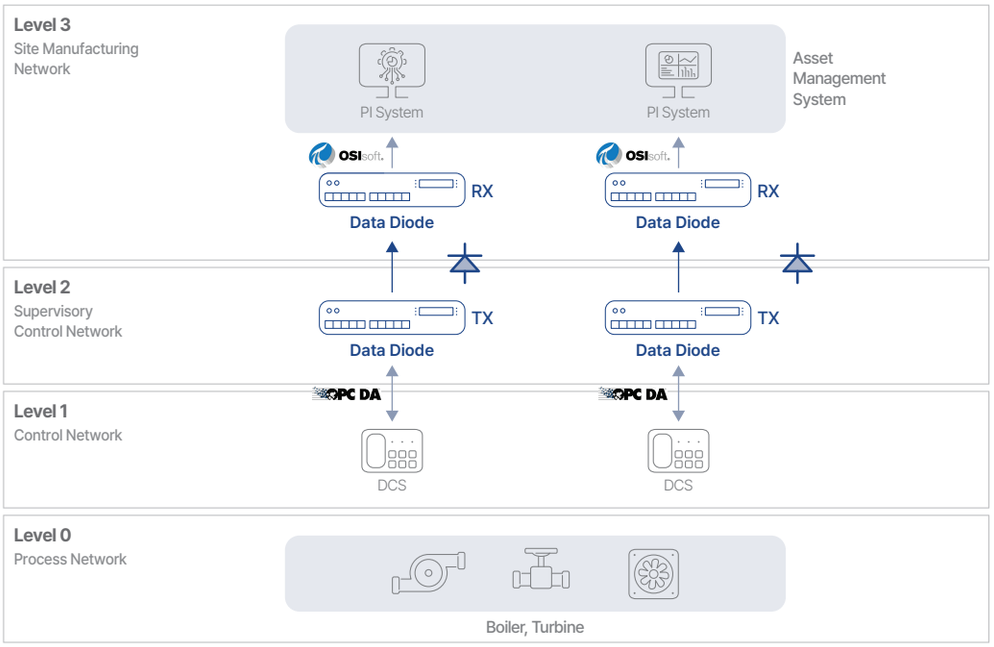
次世代ファイアウォールである AhnLab TrusGuard は、OT ネットワークの境界（ペリメータ）において、ネットワークアクセス制御とセグメンテーションを提供します。不正な URL と C&C 接続を遮断し、IPSec/SSL VPN などのセキュア通信をサポートします。また、OT プロトコル解析技術が適用され、OT ネットワーク内部で産業用プロトコルを詳細に制御できます。具体的には Modbus、DNP3 などのプロトコル別制御だけでなく、function code までを識別して制御することが可能です。



5.AhnLab 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場所へのアクセスを強化するため、物理的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します。転送するデータの暗号化、前方誤り訂正 (FEC: Forward Error Correction)、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て信頼性と安定性を最大化しました。

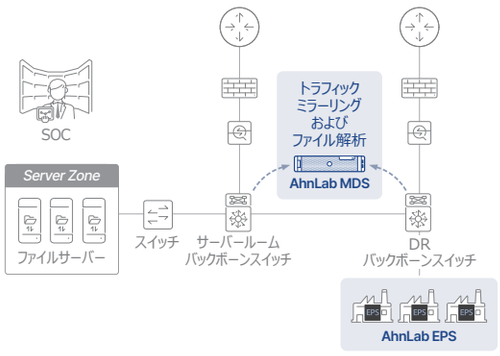
また、IT と OT 環境を統合した広範囲のプロトコル対応技術をもとに、様々な環境に最適化された形で適用が可能です。各種 IT/OT プロトコル、CCTV ストリーミングデータ、データベースなど、様々な活用事例 (use case) をカスタマイズして対応する柔軟性も備えています。

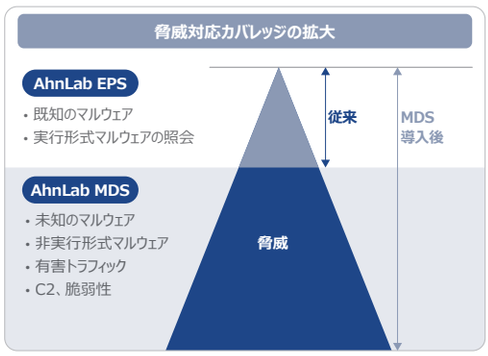


6.AhnLab MDS

ネットワークサンドボックスモジュールである AhnLab MDS は、高度化する未知の新種・亜種マルウェアに対応するために、生産ネットワークのトラフィックに転送されるファイルを収集し、マルウェアの動的解析を行います。また、攻撃者の C&C IP アドレス接続、マルウェアの拡散、脆弱性などの様々なセキュリティ脅威に対する検知とモニタリングに基づき、卓越した対応能力を提供します。

さらに、OT エンドポイントセキュリティモジュール、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ます。





7.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ります。必須とされる能力には、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遮断があります。

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ぎます。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、エンドポイントへのハードニング (Hardening) を提供します。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間にわたり最上位水準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最高レベルの脅威遮断能力を提供します。

導入効果

AhnLab CPS PLUS は、IT-OT の融合セキュリティにより CPS セキュリティの要件を効果的に解決し、顧客の皆さまによる真のデジタル革新を加速化できるようサポートします。

可用性の保障

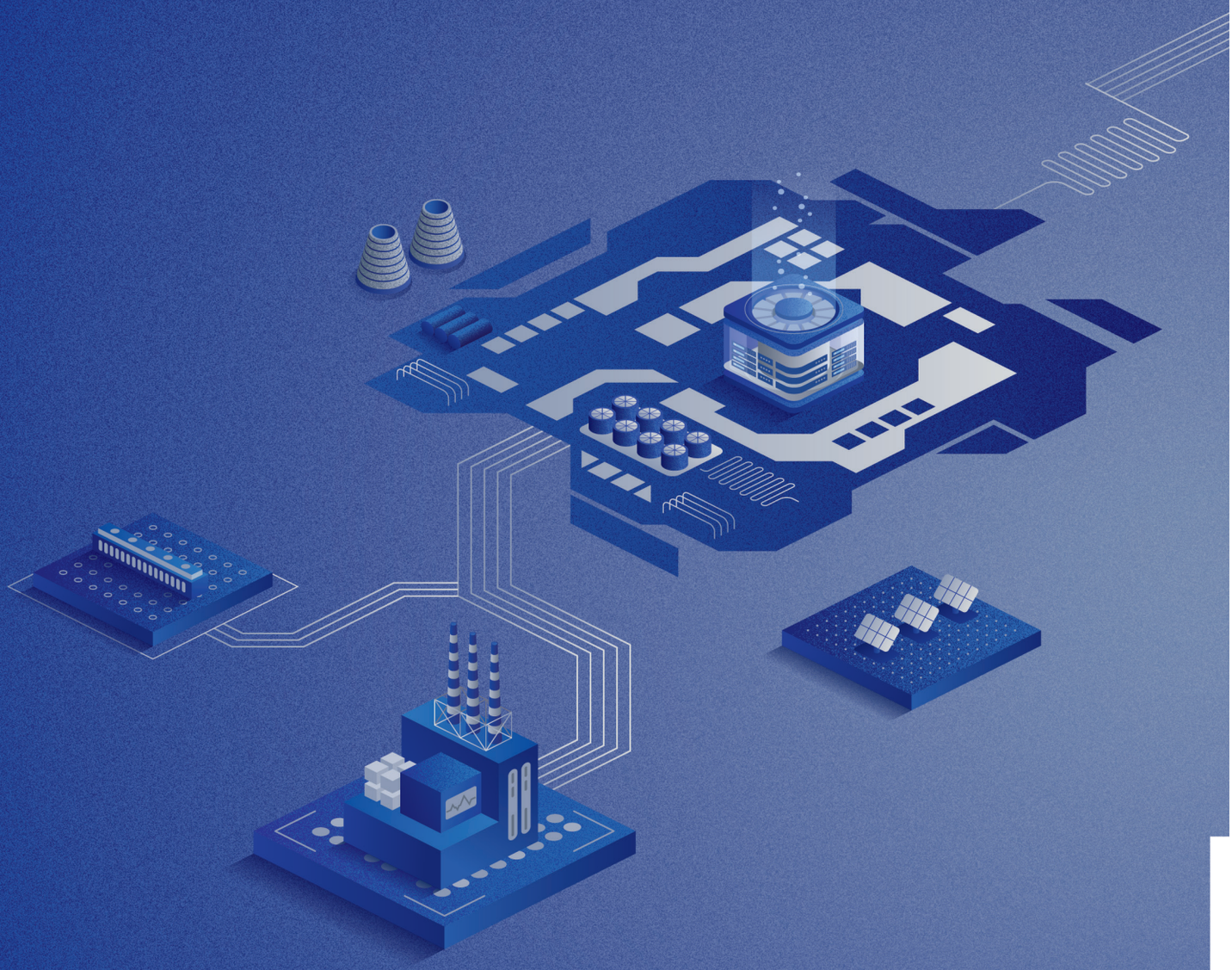
AhnLab CPS PLUS は、CPS 環境の特殊性を反映した複数のセキュリティモジュールを統合し、システム負荷なしで強力なセキュリティを実現します。

体系的な脅威管理

AhnLab CPS PLUS の各モジュール間の統合により「識別 > 検知 > 対応」につながるプロセスを実現し、体系的な脅威モニタリングと対応を提供します。

統合的な可視性および運用

統合管理コンソール AhnLab ICM により、CPS 環境の様々な資産とネットワーク状況の統合的可視性を提供し、SIEM、TIP との連携を通じて運用の利便性をさらに向上させます。



東京都港区芝4丁目13-2 田町フロントビル3階 〒108-0014
ホームページ: www.ahnlab.com/jp
TEL: 03-6453-8315 FAX: 03-6453-8316

AhnLab