AhnLab EPS

OT 環境での産業用制御システムに最適化されたセキュリティ制御

産業用制御システムの可用性を保証する軽量エージェント
ロックダウン機能を通じた新変種のセキュリティ脅威の先制遮断

製品概要

AhnLab EPS (Endpoint Protection System) は、事前に定義されたプロセスを実行し、限られたアプリケーションのみを使用する必要がある OT 環境での産業用制御システムに最適化された専用のセキュリティソリューションです。 AhnLab EPS は、生産設備システム (ICS)、POS 端末、キオスク (KIOSK)、自動発行機など、さまざまな産業用制御システムの可用性を維持しながら安全に保護します。

- 可用性保証
- ダウンタイムを最小限に抑える
- システムリソースの占有を最小限に抑える
- アプリケーションの使用制限
- さまざまな環境をサポート

特長

許可リスト (Allowlist) ベースのプログラム制御

- 許可リスト (Allowlist) を作成し、運用に必要なプログラムのみ実行
- システムロックダウン対応により、安全なシステム運用環境を維持
- 指定された信頼できるアップデータ (Trusted Updater) を使用し、ロックダウンモード (Lock モード) での運用に不可欠なプログラムのインストールとアップデートをサポート

セキュリティ強化のためのさまざまな遮断ポリシー

- 遮断リスト (BlockList) を作成し、不要なプログラムの実行を遮断
- システムの主要設定の変更経路を遮断
- ネットワーク固有の攻撃を遮断、ホストベースのファイアウォール設定
- USB デバイス、CD/DVD ドライブ、Bluetooth デバイスなどのデバイス制御
- 大容量ファイルの ASD (AhnLab Smart Defense) クラウド検知

クライアントセキュリティ管理の効率性

- クライアント未インストール PC の検索
- デバイスパッチ情報の詳細照会 (Windows KB、Linux RPM)
- 重要ファイルの整合性モニタリングと遮断

EPS クライアントの統合管理とモニタリングによる運用の利便性

- モニターセンター (ダッシュボード) を利用したリアルタイム統合モニタリング
- さまざまな OS にインストールされている EPS クライアントポリシーの統合管理と照会
- 管理の利便性の向上とメンテナンスのためのクライアントリモートコントロール

安全かつ安定したシステム運用

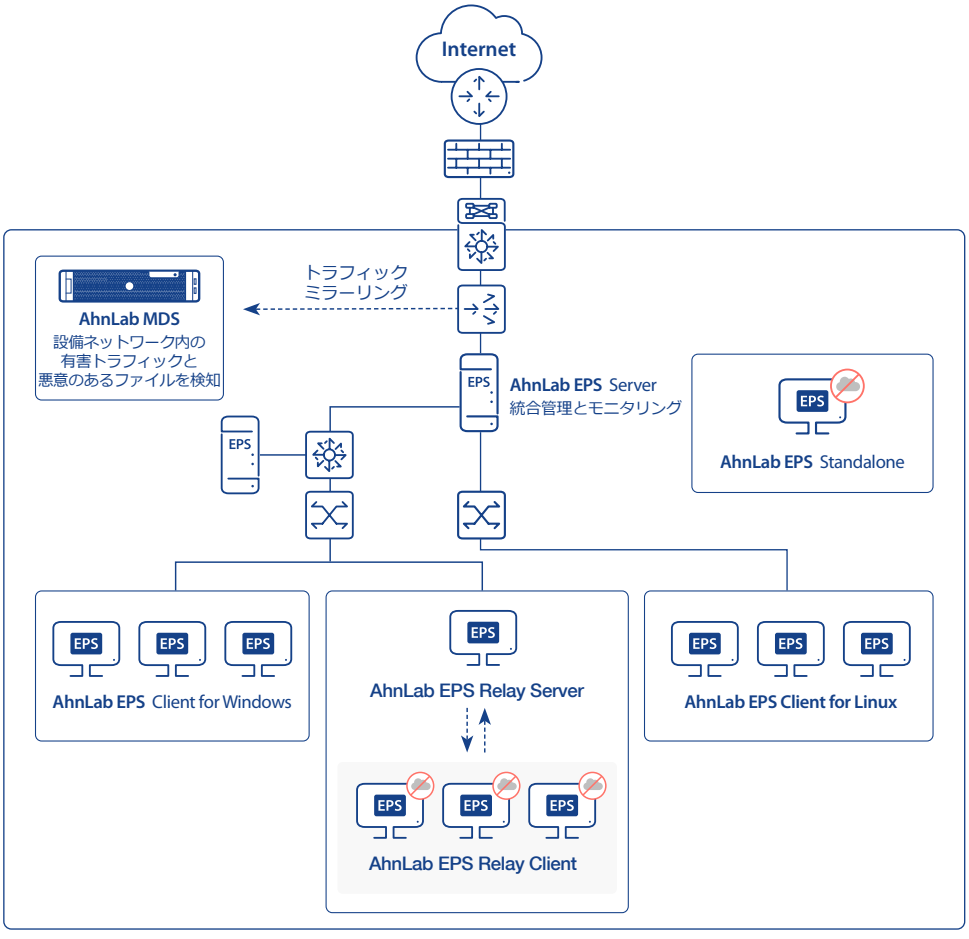
- 信頼性の高い専用エンジンを搭載したサーバー (AhnLab EPS Server) と超軽量エージェント (AhnLab EPS Client)
- システムリソースの占有の最小化および可用性中心の強力なセキュリティフレームワークの構築

効率的な
セキュリティ運用

AhnLab EPS は 「3段階運用モード」 を提供し、産業用制御システムの効率的なセキュリティ運用と管理に貢献します。 ロックダウン機能の 「解除 (Unlock モード) > テスト (Lock テストモード) > ロックダウン (Lock モード)」 によりシステムを停止することなく、最適化されたセキュリティポリシーの設定と管理が可能です。

導入方式および
主要機能

AhnLab EPS は、さまざまな産業用制御システムの運用環境を保護するために 「サーバー-クライアント型 (マネージド型)」 と 「独立型 (スタンドアロン型)」 で提供されます。



1. サーバー-クライアント型 (マネージド型)

産業用制御システムの安定稼働のために、中央モニタリングとポリシー管理のためのサーバー (EPS Server) と、端末システムにインストールされる軽量エージェント (EPS Client) で構成されます。複数の PC 組み込み設備など、EPS サーバーと直接通信できない独立ネットワーク環境ではリレーサーバーとリレークライアントを適用して端末の中央セキュリティ管理が可能です。

構成要素		主要機能
サーバー	AhnLab EPS Server	・クライアント、リレーサーバーとリレークライアントのポリシーを統合管理および統合モニタリング
クライアント	AhnLab EPS Client for Windows	・Windows OS ベースの端末セキュリティ ・ロックダウン、デバイスコントロール、システム変更の遮断、ファイアウォール、ネットワーク攻撃の検知、マルウェアスキャン
	AhnLab EPS Client for Linux	・Linux OS ベースの端末セキュリティ ・ロックダウン、システム変更の遮断、マルウェアスキャン
リレーサーバー	AhnLab EPS Relay Server for Windows	・EPS Relay Client と EPS Server 間の通信を中継 ・ロックダウン、デバイスコントロール、システム変更の遮断、ファイアウォール、ネットワーク攻撃の検知、マルウェアスキャン
リレークライアント	AhnLab EPS Relay Client for Windows	・EPS Server と直接通信できない環境の端末のセキュリティ ・ロックダウン、デバイスコントロール、システム変更の遮断、ファイアウォール、ネットワーク攻撃の検知

2. 独立型 (スタンドアロン型)

オフライン状態で、特定のアプリケーションのみを使用する産業用制御システムを保護するためのスタンドアロン型エージェント (AhnLab EPS Standalone) で提供されます。

構成要素	主要機能
AhnLab EPS Standalone	・Windows OS ベースのオフライン端末のセキュリティ ・管理ポリシーの設定、ログの保存と照会 ・ロックダウン、デバイスコントロール

連携による CPS セキュリティの強化

近年、OT 環境の外部接続が増えるにつれて、OT だけでなく OT に接続された IT 環境など、さまざまな領域まで包括する CPS (Cyber-Physical System) セキュリティの概念が台頭しています。AhnLab EPS は、アンラボの CPS セキュリティプラットフォーム 「AhnLab CPS PLUS」内の複数のセキュリティモジュールと連携して CPS セキュリティの脅威に効率的に対応し、セキュリティを強化します。

AhnLab Xcanner	**非インストール型ポータブルマルウェアスキャン** ・マルウェア感染クライアントの検知と駆除 ・AhnLab EPS サーバーを通じたリモート実行
AhnLab MDS	**ネットワークサンドボックス化** ・APT 攻撃と新変種マルウェアの動的分析 ・AhnLab EPS サーバーにマルウェア分析結果を送信
AhnLab XTD	**OT ネットワークの可視性と脅威の検知** ・IT/OT プロトコル分析資産の識別および OT ネットワークのマルウェアと脆弱性の検知 ・AhnLab EPS と連携したデバイス詳細情報の収集および疑わしいシステムの Xcanner リモートスキャン
AhnLab ICM	**CPS 環境の統合モニタリングと管理** ・各モジュールで収集された情報を基に統合可視性とモニタリングを提供 ・Multi Site にインストールされた複数の AhnLab EPS サーバーの管理

使用環境

1. サーバー-クライアント型 (マネージド型)

AhnLab EPS Server

区分		最小システム要件
ハードウェア	CPU	インテル® Xeon® プロセッサー E5 Family (8コア以上、3GHz 以上、8MB キャッシュ以上)
	メモリ	16GB 以上
	HDD	OS 用: 300GB x2 (RAID1) 以上の空き領域 データ用: 1TB 以上の空き領域 (RAID 構成を推奨)
OS		RHEL 9.2 (64ビット)
VM 環境		VMware、AWS
コンソール (ブラウザ)		Google Chrome 96 以上 Microsoft Edge ※ Internet Explorer はクライアントインストールファイルのダウンロード目的にのみ使用

* 8000 Agent 基準です。20,000 Agent のサポートは別途お問い合わせください。HDD は、顧客のファイル収集量に応じて増設が必要になる場合があります。

AhnLab EPS Client for Windows

区分		推奨仕様
ハードウェア	CPU	Pentium 133Mhz 以上
	メモリ	15MB 以上
	HDD	100MB 以上の空き領域
OS	Embedded OS	Windows Embedded XP / Standard 2009 / Standard 7 / POSReady 2009 / POSReady 7、8.1 Industry / 10 IoT Enterprise / 11 IoT Enterprise
	Desktop OS	Windows 2000 / XP / Vista / 7 / 8(8.1) / 10 / 11
	Server OS	Windows 2000 Server / Windows 2000 Advanced Server Windows Server 2003 / 2008 / 2012 / 2016 / 2019 / 2022

* SHA-1 証明書のサポート終了により、OS ごとに使用可能なバージョンと機能に違いがある場合があります。
* 上記 OS の 32/64ビットに対応

AhnLab EPS Relay Server, AhnLab EPS Relay Client

区分		推奨仕様
ハードウェア	CPU	Pentium 133Mhz 以上
	メモリ	15MB 以上
	HDD	100MB 以上の空き領域
OS	Embedded OS	Windows Embedded Standard 2009 / 7 / 7 SP1(KB4490628、4474419 パッチ環境) Windows Embedded POSReady 2009 / 7 Windows Embedded 8.1 Industry Windows Embedded 10 IoT Enterprise / 11 IoT Enterprise
	Desktop OS	Windows 2000 / XP / XP SP3 / Vista / Vista SP2(KB4493730、4474419 パッチ環境) / 7 / 7 SP1(KB4490628、4474419 パッチ環境) / 8(8.1) / 10 / 11
	Server OS	Windows 2000 / 2003 / 2003 R2 / 2008 / 2008 SP2(KB4493730、4474419 パッチ環境) / 2008 R2 / 2008 R2 SP1(KB4490628、4474419 パッチ環境) / 2012 / 2016 / 2019 / 2022

* 上記 OS の 32/64ビットに対応
* Relay Client は Windows 2000 および XP のみサポートします。
* Relay Server は Windows XP SP3 のみサポートします。

AhnLab EPS Client for Linux

区分		最小システム要件
ハードウェア	CPU	Intel (32/64ビット)
	メモリ	1GB 以上
	HDD	500MB 以上の空き領域
OS		CentOS 3.3 ~ 8.1 / Red Hat Enterprise 3.3 ~ 8.1、8.4 / Red Hat Linux 9 / antiX Linux 13.2、15、16.2、17.2 / Ubuntu 10.04、11.04、11.10、12.04、14.04、18.04 / Ruby Duck release 5.6(Marcy 5.1) / SUSE Linux 9.2 / Fedora 8、14

2. 独立型 (スタンドアロン型)

AhnLab EPS Standalone

区分		推奨仕様
ハードウェア	CPU	Pentium 233MHz 以上
	メモリ	64GB 以上
	HDD	1.5GB 以上の空き領域
OS	Embedded OS	Windows Embedded Standard 2009 / Standard 7 / POSReady 2009 / POSReady 7 / 8.1 Industry(Pro、Enterprise) / 10 IoT Enterprise
	Client OS	Windows XP SP2、SP3 Professional / Vista(Enterprise、Ultimate) / 7(Professional、Enterprise、Ultimate) / 8、8.1(Pro、Enterprise) / 10(Pro、Enterprise) / 11(Professional、Enterprise)
	Server OS	Windows Server 2008(Standard、Enterprise) / 2012(Essentials、Standard) / 2016(Essentials、Standard) / 2019(Essentials、Standard) / 2022 (Essentials、Standard)

* 上記 OS の 32/64ビットに対応

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