アンラボ・セキュリティレター

Press Ahn

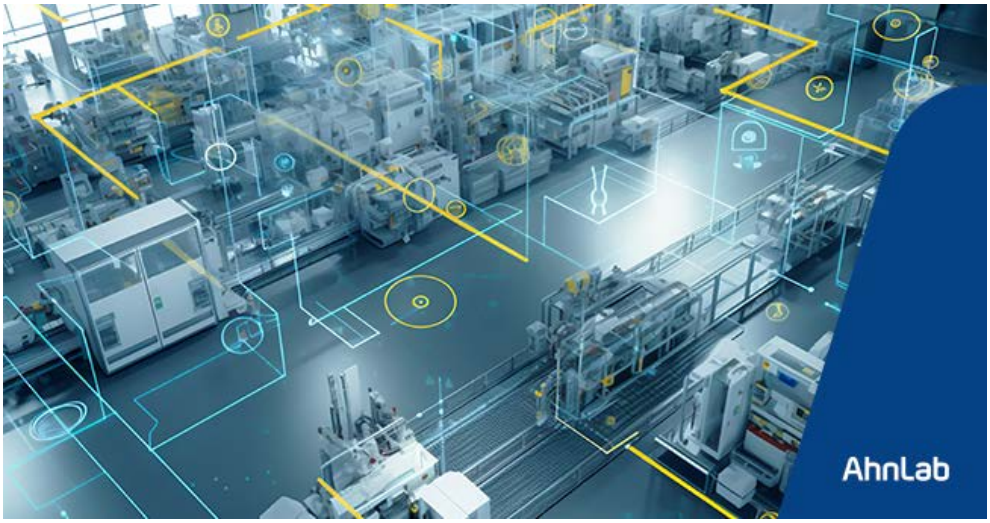
2024.04　Vol.123

AhnLab EPS の新規バージョンをリリース、より強力になった OT セキュリティ

AhnLab EPS の新規バージョンをリリース、より強力になった OT セキュリティ

アンラボは 3月末、同社の OT エンドポイントセキュリティソリューション「AhnLab EPS」の新規バージョンをリリースした。AhnLab EPS は、アンラボがナオンワークスと共に構築した「統合 OT セキュリティフレームワーク」の核心を担うソリューションで、今回の新規バージョンを通じて顧客により強力な統合 OT セキュリティ能力を提供できると期待されている。

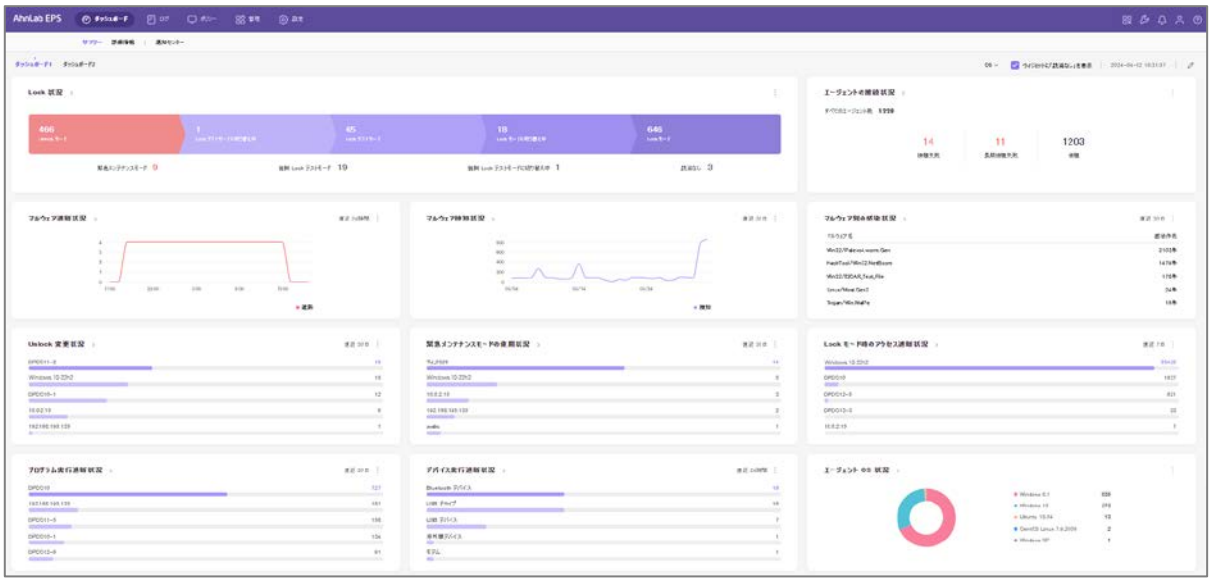
この記事では、AhnLab EPS の新規バージョンがどのように変わったかを紹介する。



今回お披露目した AhnLab EPS は v3.0 であり、2020年に v2.0 をリリースしてから、約 4年ぶりにメジャーアップグレードバージョンでリリースすることとなった。AhnLab EPS は、今回の新規バージョンを通じて ▲ユーザーインターフェース (UI) の改善 ▲突発的な状況にするための機能強化 ▲ユーザビリティの向上 ▲ 製品仕様およびサポート対象OSの拡大 ▲日本語対応の観点から改善を成し遂げた。

より洗練され、より強力になった AhnLab EPS

#1. ユーザーインターフェース（UI）およびユーザビリティの向上



[図 1] AhnLab EPS 3.0 ダッシュボード

まず、最も顕著な変更点は、製品のユーザーインターフェース（UI）のデザインと構成の改善だ。UI デザインは最新のトレンドに合ったスタイルに完全に変え、全体的なメニュー構造と構成もユーザーがより直感的にセキュリティ状況を把握し、措置を取れるように改善した。

また、コンソールでエージェント（agent）を属性に合わせてまとめて管理するグループのデプス（depth）を既存の 5個から 10個以上に増やした。これにより、ユーザーが事業所で運用中の AhnLab EPS エージェントを目的に応じて柔軟に管理できるようにした。

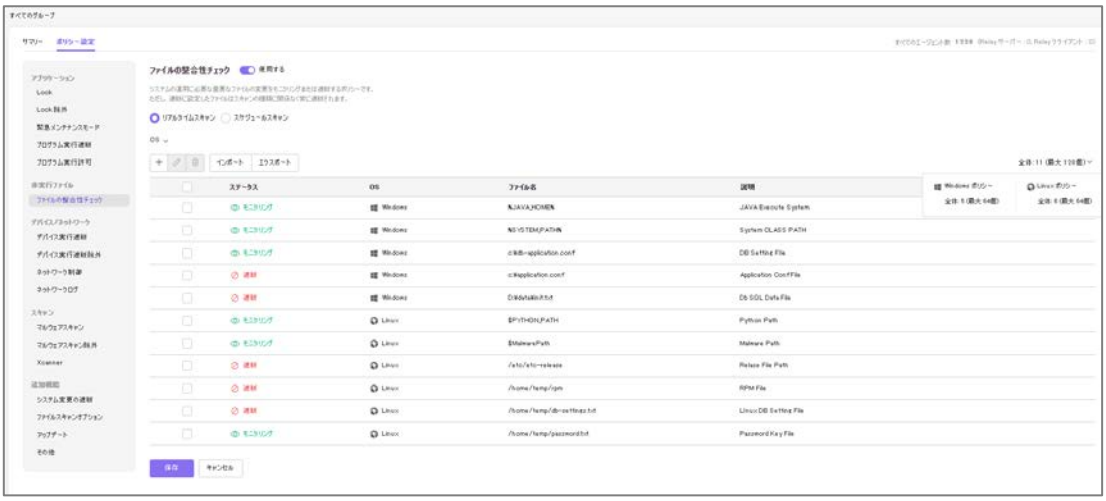
#2. 突発事象に対応およびファイル整合性を確保するための機能の強化

OT 環境では、システムの可用性（availability）が何よりも優先されるべきであり、これらの特性を考慮し、今回の新規バージョンに ▲緊急メンテナンスモード中の緊急デバイス実行の許可 ▲エージェントの緊急単独パッチ ▲主要ファイルの整合性監視および遮断などの機能を追加した。

A. 緊急メンテナンスモード中の緊急デバイス実行の許可：ユーザーがシステムの緊急点検を実施している間でも、運用上の理由で緊急に特定のデバイスの許可が必要な場合がある。このとき、エージェント環境設定で「緊急デバイス実行許可」を有効にすると、許可したデバイスを緊急メンテナンスモードでも実行できるようになる。

B. エージェントの緊急単独パッチ：通常、エージェントのパッチはサーバーを介して一括して行われる。ただし、AhnLab EPS 3.0 は、緊急事態に対応するために、必要に応じてサーバーマイグレーションなしにエージェントの単独パッチを提供する。ユーザーは、エージェントの単独パッチのために Windows と Linux バージョンごとのパッチセットを個別に管理できる。

C. 主要ファイルの整合性監視および遮断：OT 環境で運用中の主要ファイルは、システムの可用性とセキュリティを確保するために、変更の有無と履歴を徹底的に管理する必要がある。今回の新規バージョンでは、システム運用上重要なファイルの変更履歴をモニタリングし、必要に応じて変更自体を遮断できる。



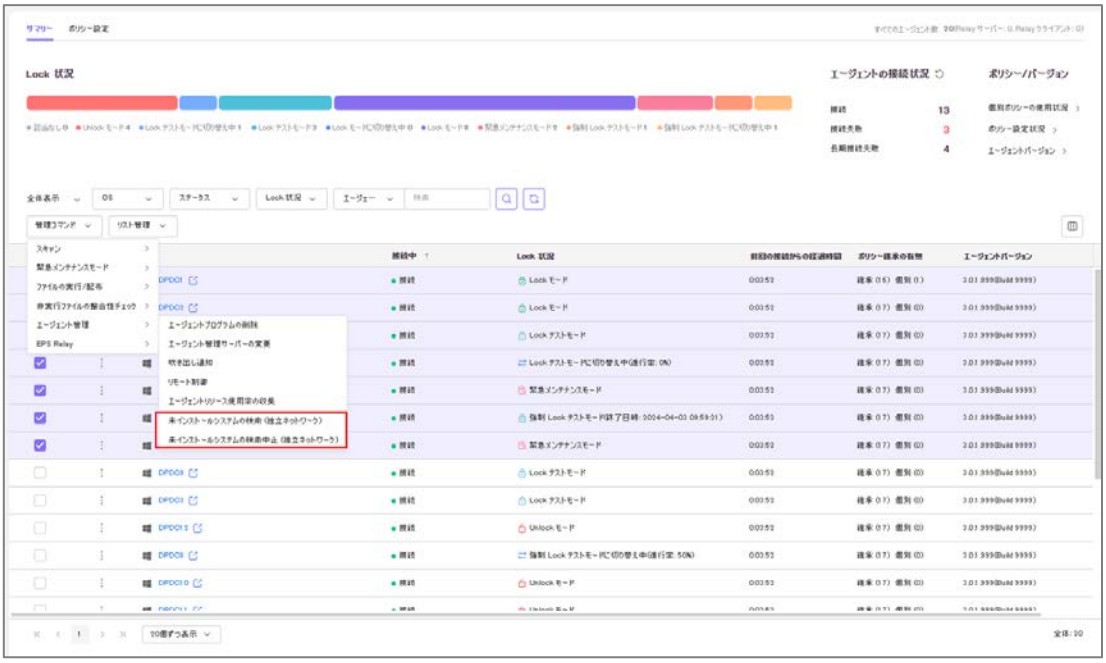
[図 2] 主要ファイルの整合性監視および遮断

使用方法を簡単に説明すると、まずファイルベースラインを生成するために整合性チェックポリシーとエージェント連携機能を追加する。そして、ファイルに対して「モニタリング」および「遮断」を設定できる。モニタリング状態に設定したファイルは変更履歴を「ファイルの整合性モニタリング」タブで確認でき、遮断に設定したファイルはエージェントログで遮断履歴を確認できる。

#3. 可視性および検知機能の拡大

OT セキュリティの必須要件の 1つは、環境全体にわたって運用中のシステム可視性を確保し、適切な検知を通じてシステムを抜け目なく保護することだ。その一環として、今回の AhnLab EPS 3.0 では ▲プライベートネットワーク PC の検索と照会 ▲OS パッチ状況管理 ▲大容量ファイルクラウドスキャン機能が追加された。

A. プライベートネットワークでのエージェント未インストールシステムの検索と照会: この機能は、OT 環境でも特殊な環境である独立した閉域網でエージェントがインストールされていないシステムを特定するために追加された。2022年、独立した閉域網内部に隠された資産のセキュリティ管理のために、AhnLab EPS に「EPS Relay」機能を追加した。今回の新規バージョンで補強された機能により、EPS Relay を構成する前に、独立した閉域網でエージェントがインストールされていないシステムを把握し、管理することができる。



[図 3] プライベートネットワークでのエージェント未インストールシステムの検索と照会

これにより、ユーザーはプライベートネットワークで運用中のエージェント未インストールシステムを管理できるようになり、環境全体で運用中のシステムの可視性を高めるとともに、より体系的に管理できるようになった。

B. デバイス OS 詳細情報の確認: OT 環境に対するセキュリティが大幅に改善されたが、未だに資産に対するパッチ履歴管理などがきちんとできない場合が多い。AhnLab EPS 3.0 は、このような課題を解決するためにデバイス OS 詳細情報の可視性を強化し、パッチ履歴を体系的に管理できるようにした。さらに、関連する脆弱性に対する管理も効率的にサポートできるようになった。

今回の新規バージョンでは、デバイスごとに運用中の OS についてエージェントが提供する情報が拡大され、OS の種類別に Windows エージェントの KB パッチ履歴と Linux エージェントの RPM 変更履歴を照会するページが提供される。また、エクスポート機能により個別に Excel ファイルでパッチ状況を管理できる。

C. 大容量ファイルクラウドスキャン: OT 環境のシステムは基本的に閉域網で運用され、マルウェア検知もシステムに負荷をかけない状態で実行される。しかし、AhnLab EPS 3.0 は、サーバーがインターネットに接続されている場合に限って、エージェントが転送する 10MB 以上の大容量ファイル (最大 300MB) に対しても、クラウドスキャン機能でマルウェアを検知する。これにより、高度化された OT セキュリティ脅威に対抗して、ユーザーにより幅広いマルウェア検知オプションを提供できるようになった。

#4. パフォーマンスのアップグレード

AhnLab EPS 3.0 は、サーバー 1台あたりのエージェントサポート数量を既存の 8,000台から 20,000台まで拡大した。また、ハードウェアと OS 仕様をアップグレードし、Windows と Linux エージェントのクライアント OS のサポート範囲を拡大するなど、全体的なパフォーマンスを強化した。

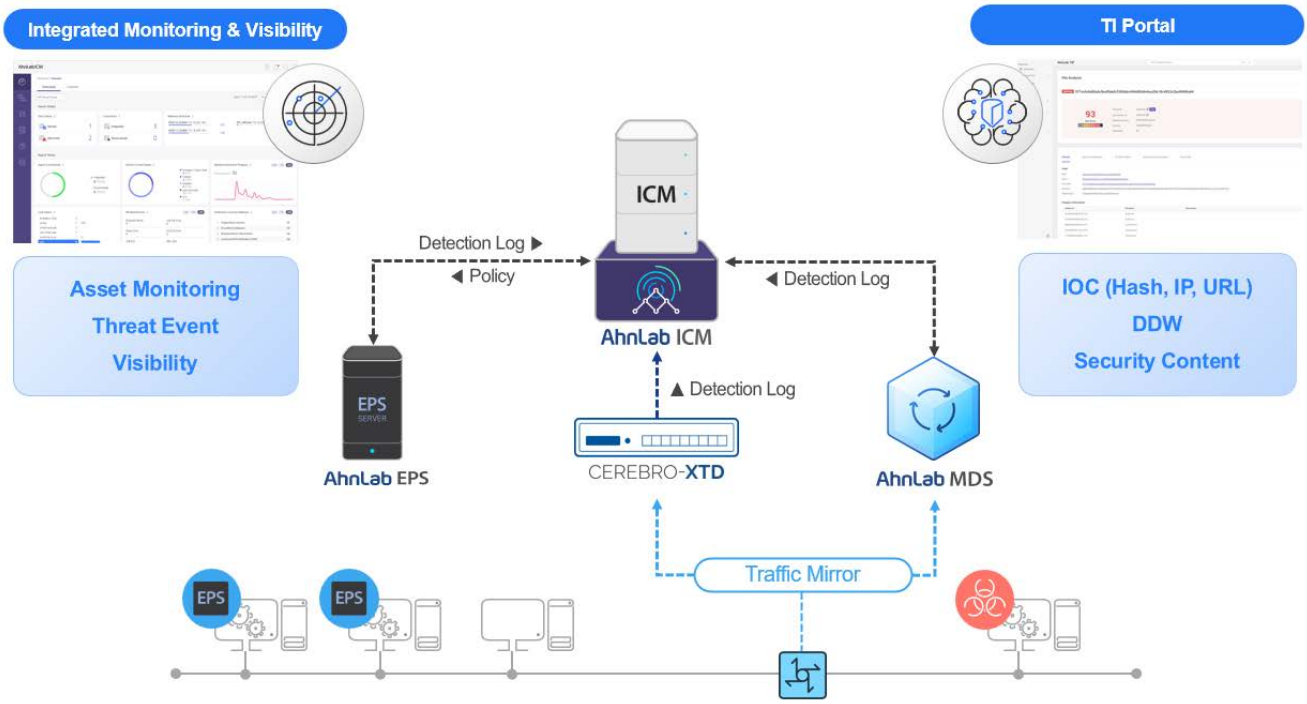
#5. 日本語対応

韓国語、英語、中国語で提供されていた AhnLab EPS は、v3.0 から日本語にも対応する。これにより、日本企業や日本で事業を運営している韓国企業に、よりローカライズされたソリューションを提供できるようになった。

AhnLab ICM、真の OT 統合セキュリティの始まり

アンラボは、OT セキュリティ企業のナオンワークスを買収した後、ナオンワークスと共に OT の高度化に拍車をかけており、今回の AhnLab EPS 3.0 リリースも総合的な OT セキュリティ能力の強化を一環として行われた。

同じ観点から、2023年 9月には OT セキュリティ統合管理ソリューション「AhnLab ICM」の新規バージョン (v2.0) をリリースした。AhnLab ICM 2.0 は、既存の AhnLab EPS と MDS 中心のセキュリティ管理の幅を、アンラボとナオンワークスが共同開発した OT ネットワークの可視性および脅威検知ソリューション「CEREBRO-XTD」まで拡大した。これにより、CEREBRO-XTD が識別した資産を AhnLab ICM で照会および管理し、CEREBRO-XTD と AhnLab EPS の連携を通じて確保した資産の可視性も、AhnLab ICM で一度に確認できるようにした。



[図 4] AhnLab ICM 統合セキュリティ構造

また、自社の脅威インテリジェンスプラットフォーム「AhnLab TIP」と連携して収集されたログに対する侵害指標（IoC）を照会できるようにし、真のインテリジェンスベースのセキュリティ（Intelligent-driven Security）の実装に拍車をかけている。このほか、AhnLab ICM 2.0 では、AhnLab EPS のエージェントごとの OS の脆弱性も一度に確認でき、より安定したシステム運用に貢献する。

アンラボとナオンワークスの統合 OT セキュリティフレームワークの詳細については、アンラボホームページで確認できる。
►統合 OT セキュリティフレームワークの紹介ページへ

https://www.ahnlab.com/jp

https://www.ahnlab.com/en

https://www.ahnlab.com/ko

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)