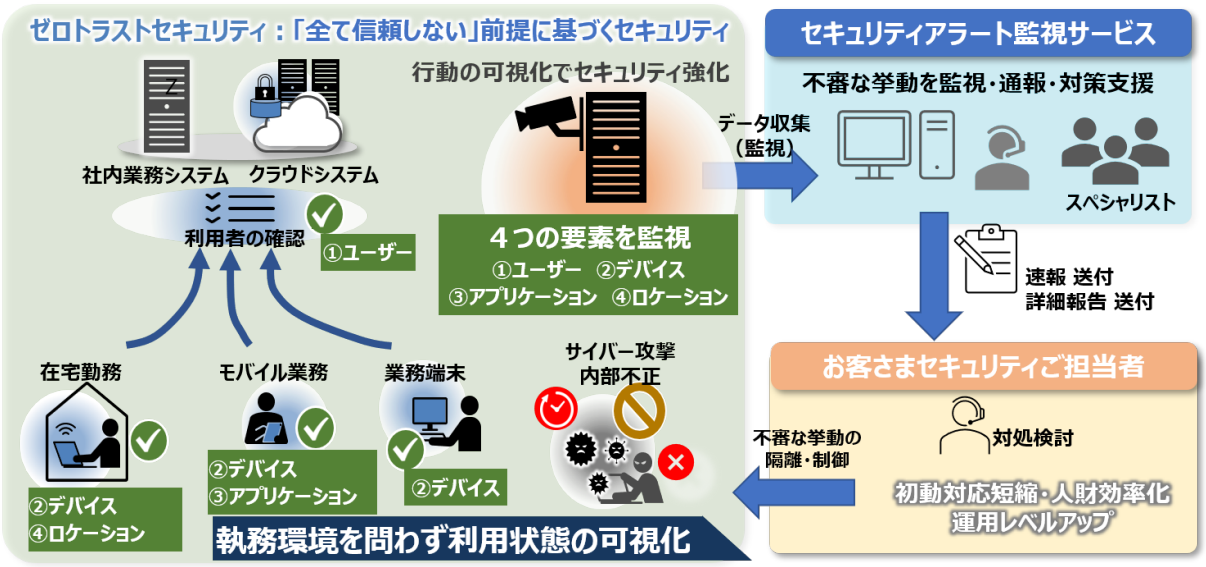
News Release

2021 年 2 月 8 日
株式会社日立情報通信エンジニアリング

多様化・複雑化するセキュリティ運用をゼロトラスト観点で支援する「セキュリティアラート監視サービス」の販売開始

～ セキュリティ運用での専任者不足を補い、サイバー攻撃への迅速な対応が可能に ～



「セキュリティアラート監視サービス」概要

株式会社日立情報通信エンジニアリング（代表取締役社長：岩崎 秀彦、本社：神奈川県横浜市）は、多様化・複雑化するセキュリティ運用をゼロトラスト観点で支援するサービスの第一弾として、エンドポイント（デバイス）およびネットワークのセキュリティ運用におけるアラート調査・報告を行う「セキュリティアラート監視サービス」を 2 月 15 日より販売開始します。セキュリティリスクの有無の判断と今後の対処の検討を可能とする調査速報、ならびに詳細報告書を提供することで、お客さまは、発生したアラートへの対処に集中でき、セキュリティ専任者不足の解消、サイバー攻撃への迅速な対応が可能となります。

昨今、ニューノーマルによる業務環境の変化、IoT の普及によるインターネット接続機器の多様化、標的型攻撃によるマルウェア感染などのサイバー攻撃のリスクが増加し、その対応が急務となっています。

この課題を解決するため、「全て信頼しない」というゼロトラストセキュリティの考え方が登場し、①ユーザー、②デバイス、③アプリケーション、④ロケーションの 4 つの要素に対し、その振る舞いを監視し、識別・アクセス制御を行うことが注目されています。その一方で、セキュリティ運用の多様化・複雑化による、セキュリティ技術者不足などの問題が発生しています。

当社はこれまで、円滑なエンタープライズネットワークを提供するベンダとして評価の高いシスコシ

ステムズ合同会社（以下、シスコ社）のソリューションを活用した数多くのネットワークソリューションを提供し、企業、自治体、公共施設の社会インフラを支えてきました。また、運用面では、カスタマーサポートとして、お客さまの IT 環境や機器の稼働監視サービスを提供し、多くの信頼を得てきました。

このたび、お客さまの大切な IT インフラを守るゼロトラストセキュリティの実現を支援するため、当社内にゼロトラストセキュリティ推進センタを設立しました。CISSP(*1)や CND(*2)などのセキュリティ専門資格を保有する専任チームが、体系的なゼロトラストセキュリティソリューションを保有するシスコ社の商材と、当社で培ったネットワークソリューション・運用サポートサービスのノウハウを組み合わせることで、ゼロトラストセキュリティ運用において負担が高くなる監視業務を支援するサービスを順次提供していきます。

＊1 CISSP: Certified Information Systems Security Professional
＊2 CND: Certified Network Defender

今回はその第一弾として、昨今対応が急務とされている、テレワークなどによりセキュリティリスクが高まっているエンドポイント（デバイス）セキュリティの運用を支援する「EDR(*3)アラート監視サービス」と工場・IoT を狙ったサイバー攻撃に有効なネットワークセキュリティの運用を支援する「NDR(*4)アラート監視サービス」を提供します。

＊3 EDR: Endpoint Detection and Response
＊4 NDR: Network Detection and Response

アラート発生時の対応として負担の大きいアラート調査プロセスを、当社がサービスとして提供することで、お客さまはアラート発生時の現地対応に注力することが可能となります。また、サイバー攻撃となりえる兆候の蓄積により、IT インフラのセキュリティ向上につなげることができます。

具体的なサービス内容は、次の通りです。

1．「EDR アラート監視サービス」

（1）課題

・安全なテレワーク環境を実現するためのエンドポイント（デバイス）の保護に必要な高度なセキュリティツールの導入

・ツールを使いこなし、不正な挙動を素早く見極め、対策を起こすための専門的な知識をもつ技術者による対応

（2）監視要素：デバイス、アプリケーション

（3）サービス概要

・PC のセキュリティ監視に有効な EDR を使用し、検知したセキュリティアラートについて速報し、その後に詳細な調査報告書を提供

・日立の独自の解析技術により、従来人手で対応をしていたイベント調査工程の効率化を支援

2.「NDR アラート監視サービス」

(1)課題

・アンチウイルスソフトなどのツールの導入が困難な工場・IoT ネットワーク環境で使用される機器へのサイバー攻撃発生時の早期発見・対応

(2)監視要素:デバイス、ロケーション

(3)サービス概要

・ネットワークの振る舞いからサイバー攻撃の兆候を検知する NDR を使用し、発生したセキュリティアラートについて速報し、その後に詳細な調査報告書を提供

なお、セキュリティ専任者を置けないお客さま向けに、被害拡大防止のため、デバイスのネットワーク隔離などの緊急オペレーションについてもオプションを用意しています。

今後、当社では、ゼロトラストセキュリティを実現する 4 要素の振る舞いを可視化するアラート監視サービスの拡充を行うとともに、ゼロトラストセキュリティを体験できる協創の場の提供、ゼロトラストセキュリティの導入支援のための上流コンサルテーション、システム構築などのサービスメニューの拡充を行い、お客さまの多様化・複雑化するセキュリティ運用を支えてまいります。

■セキュリティアラート監視サービスメニュー（*5）

サービス名	サービス内容	価格(月額、税別)
EDR アラート監視サービス	Cisco Secure Endpoints（旧 AMP for Endpoints）のアラート監視、調査、レポーティング	¥500,000～（*6）
NDR アラート監視サービス	Cisco Secure Network Analytics（旧 Stealthwatch）のアラート監視、調査、レポーティング	¥600,000～（*7）

＊5 本サービス利用には、Cisco Secure Endpoints, Cisco Secure Network Analytics, および付随する導入サービスが必要となります。また、ゼロトラストセキュリティコンサルテーションも別途受付けます。

＊6 EDR アラート監視サービスは、1,000 クライアントの参考価格です。

＊7 NDR アラート監視サービスは、500Flow の参考価格です。
Flow とは 2 つのエンドポイント間のセッションの開始から終了までの一連の通信です。Flow 数とは 1 秒あたりの Flow の数量を表します。

■パートナー企業からのコメント

シスコシステムズ合同会社 専務執行役員 パートナー事業統括 大中 裕士氏

シスコは、日立情報通信エンジニアリング様の「セキュリティアラート監視サービス」の販売開始およびゼロトラストセキュリティ推進センタの新設を歓迎いたします。情報セキュリティ対策が企業活動で重要視されている今日、日立情報通信エンジニアリング様が提供されるサービスと弊社製品を組み合わせることで、お客様のセキュリティ運用を効率化し、より健全なITプラットフォーム提供に付加価値をもたらすと確信しております。

■商標に関する表示

記載の会社名、製品名はそれぞれの会社の商標もしくは登録商標です。

■「セキュリティアラート監視サービス」に関するホームページ

https://www.hitachi-ite.co.jp/solution/platform/zerotrust/

■お客さまお問い合わせ先

株式会社 日立情報通信エンジニアリング 営業統括本部 プラットフォーム拡販推進部
〒220-6125 神奈川県横浜市西区みなとみらい 2 丁目 3 番 3 号 クイーンズタワーB 25 階
お問い合わせフォーム：https://www.hitachi-ite.co.jp/inquiry/

■報道機関お問い合わせ先

株式会社 日立情報通信エンジニアリング 経営戦略本部 経営企画部
〒220-6122 神奈川県横浜市西区みなとみらい 2 丁目 3 番 3 号 クイーンズタワーB 22 階
お問い合わせフォーム：https://www.hitachi-ite.co.jp/inquiry/

以上
