急増するサイバー攻撃にワンストップで対応し、制御システムの安定稼働を支える「セキュリティ監視・分析支援サービス」

「制御システム向けセキュリティ監視・分析支援サービス」は、電力、鉄道、ガス、水道など、重要な社会インフラにおける制御システムへのサイバー攻撃を防御し、安定稼働を支援するサービスです。日立のOT※1とITを網羅する多様な分野で培ってきたセキュリティの知見と専門チームのノウハウを結集し、お客さまのSOC※2運用をトータルにサポートします。

※1 Operational Technology　※2 Security Operation Center

制御システムにも求められるサイバー攻撃対策

IoTや5Gといった新たなネットワーク技術が進展するなか、サイバー攻撃が電力や水道、鉄道など、人々の生活を支える社会インフラの運用を担う制御システム（OT）も標的にするようになり、セキュリティ対策の見直しが急務となっています。その手口は年々高度化・巧妙化しており、サイバー攻撃によって万一、制御システムが侵害されると、業務停止に陥り、その被害が社会全体にまで及ぶ可能性もあります。

安定稼働が求められる制御システムには、サイバー攻撃を未然に防ぎ、インシデントの監視や、その原因の分析、対策までを一貫して迅速に行うSOCおよびセキュリティ対応体制の構築が必要です。

しかし、お客さまが自社内でセキュリティの専門人財を育成・確保し、体制を構築するのは非常に困難です。また、制御システムはITシステムと異なり、基本的に外部ネットワークへの接続が想定されていないため、オンラインでの遠隔常時監視が困難なケースがあります。

そこで日立は、高度なスキルを持った専門チームが長年にわたり制御システムの運用・保守をサポートするなかで培った、多様なセキュリティの知見とノウハウを生かし、24時間365日、「制御システム向けセキュリティ監視・分析支援サービス」で、お客さまのSOC運用を支援します。

サービスの特長

インシデント対応専用チームが被害を最小化

お客さま環境に設置されたログ収集・監視装置と日立が用意するセキュリティ監視基盤をオンラインまたはオフラインでつなぎ、制御システムセキュリティに関する高度な知識と技術を持つ日立の専門チームが、セキュリティイベントの監視・分析から発生したインシデントへの対応まで、一連のセキュリティ運用サービスを提供。お客さまのSOC運用に求められるリソースや負担を大幅に軽減し、セキュリティ被害を最小化します。

日立の専門チームでは、セキュリティイベントを監視し、大量のイベントからインシデントを抽出・分析するセキュリティアナリストをはじめ、現地へ迅速に駆けつける保守員、実際

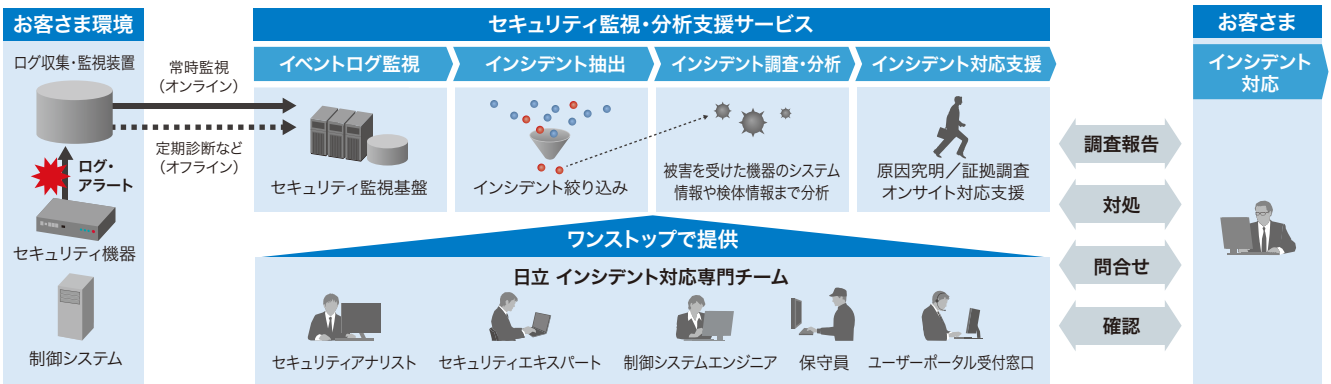

図1 制御システム向けセキュリティ監視・分析支援サービスの概要

のインシデント対応支援を行うセキュリティエキスパート、制御システムに精通したエンジニアなど経験豊富な人員で構成され、必要に応じてワンストップでサービスを提供します。

専門人材がワンストップで インシデントに対応

本サービスは次の4つのメニューで構成されています。「イベントログ監視」では、セキュリティイベントログを高度な監視基盤を用いて監視し、マルウェアの侵入や制御システムのぜい弱性をチェックし、アラートを検知します。「インシデント抽出」では、検知したアラートに対し、セキュリティアナリストが関連機器のログを調査、インシデントを絞り込みます。誤検知によるアラートは制御システムエンジニアが事前にフィルタリングするため、お客さまのセキュリティ担当者の業務負荷を軽減することが可能です。

「インシデント調査・分析」では、抽出したインシデントに対し、サーバーや端末内の情報をもとに、被害を受けた機器のシステム情報や検体情報までの分析を実施。「インシデント対応支援」では、分析結果から推定できる原因や影響範囲を提示し、必要に応じて現場へ駆けつけ、対応することで被害を最小限に抑えます。

外部ネットワークに接続しない制御システムにも 導入可能なオフラインメニュー

本サービスは、お客さまの制御システムと日立のセキュリティ監視基盤をオンラインで結んだ常時監視だけでなく、ポリシーなどで外部ネットワークに接続をしない制御システムについても、オフラインでの定期診断や緊急対応が可能です。

オフラインの場合は、お客さまの環境に設置したログ収集・監視装置に蓄積したログを定期的に日立がチェックし、マルウェアの進入やぜい弱性などを見極め、結果を報告するとともに迅速な初動対応へとつなげます。また、セキュリティ機器からアラートが検知された際などの緊急時には、インシデント調査・分析から対応・支援まで、お客さまの環境に合わせた柔軟なサービスを提供いたします。また、ログ収集・監視装置が未設の場合は、必要となる初期構築（ログ蓄積装置や、現場でのログを一元的に蓄積・管理し保安上の脅威となる事象をいち早く検知・分析するSIEM※3構築など）の導入を日立が支援し、お客さまによる負担を軽減することで、オフラインサービスの導入を容易にします。

※3 Security Information and Event Management

幅広い分野の制御システムを脅威から守る

本サービスの第1弾では、電力と鉄道分野向けのメニューを提供し、順次、産業をはじめとする幅広い分野へ適用範囲を拡大していきます。

これからも日立は、複雑化するサイバー攻撃の最新動向を踏まえ、本サービスの機能強化を図り、社会インフラの安定稼働を支援し、安全・安心な社会の実現に貢献していきます。

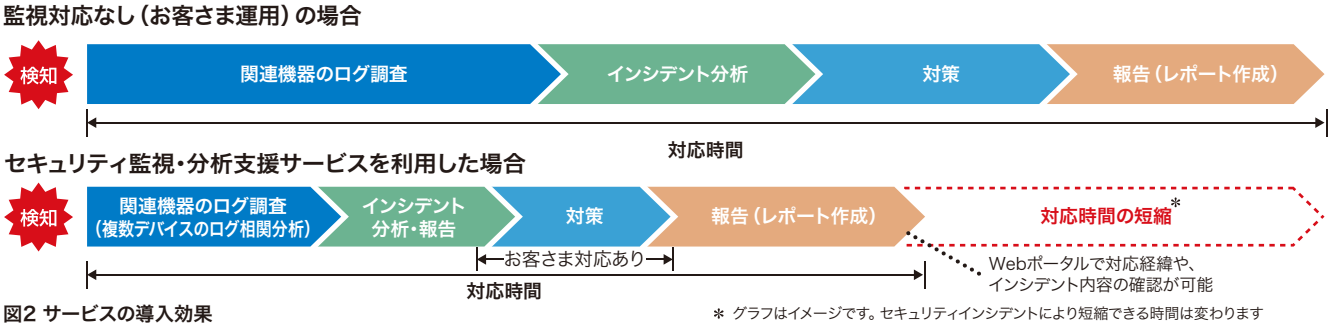

図2 サービスの導入効果

＊ グラフはイメージです。セキュリティインシデントにより短縮できる時間は変わります

お問い合わせ先・情報提供サイト

（株）日立製作所 制御プラットフォーム統括本部
https://www.hitachi.co.jp/security-control/