社会インフラの安全・安心を支える セキュリティ統合監視ソリューション

社会インフラの継続的な運用を守るためには、IT/OT※1/IoT※2システムのセキュリティ対策と、それらのシステムを一元的に管理・把握する統合SOC※3や、組織全体の対応力強化が必要です。日立は、これらのセキュリティ運用全体を支援する「セキュリティ統合監視ソリューション」により、お客さまの事業継続をサポートしていきます。

※1 Operational Technology　※2 Internet of Things　※3 Security Operation Center

IT/OT/IoTのセキュリティを一元的に監視

特定の企業や組織を狙ったサイバー攻撃が増加するなかで、社会を支えるインフラシステムでも多くの被害が発生しています。社会インフラシステムを構成するOTシステムやIoTシステムにも、ITシステムと同様のセキュリティ対策を施す必要がありますが、事業継続の観点からシステム停止が容易ではないため、システム改修をともなうセキュリティ対策を頻繁に施すことが困難な状況にあります。

そこで日立は、長年培ってきたOTシステムに関する技術やノウハウと、ITシステムに関する監視サービスの適用実績をもとに、多岐にわたるシステムを常時監視することで対策の有効性を検証しながら、日々巧妙化するサイバー攻撃に対応する「セキュリティ統合監視ソリューション」を開発しています。

本ソリューションでは、IT/OT/IoTの各システムに加え、プラントや重要施設に出はいりする人/モノ/車両などを監視するフィジカルセキュリティも一元的に管理できます。セキュリティ運用組織の統合・効率化、インテリジェンス情報の共有・活用といった運用課題を含めた解決策もトータルに提案し、お客さまの事業継続のための効率的なセキュリティ運用を支援します。

「中央」と「現場」でセキュリティを守る

セキュリティ監視は従来、SOCがITシステム全体を集中監視する形で行われてきました。しかしOTシステムでは、プラントやラインといった現場での稼動判断が必要となります。またITとOT/IoTの連携が進んできたことで、サイバー攻撃もITとOTの別なく波及する傾向にあるほか、悪意によって引き起こされる潜在的な脅威（不正アクセス、情報流出、重要施設への不正侵入など）にも備える必要があります。

日立のセキュリティ統合監視ソリューションでは、現場の役割と統合SOC（中央）の役割を明確化しています。現場ではインシデントを検知すると、その内容や影響範囲、稼働への影響を考慮して一次対処を行い、統合SOC（中央）に通知。統合SOC（中央）では現場からの情報やITシステムの状況、さらには外部機関の情報を収集し、統合的に分析して根本対策を検討するとともに、CISO※4に代表される経営層の判断を促すといった役割を担います（図1）。

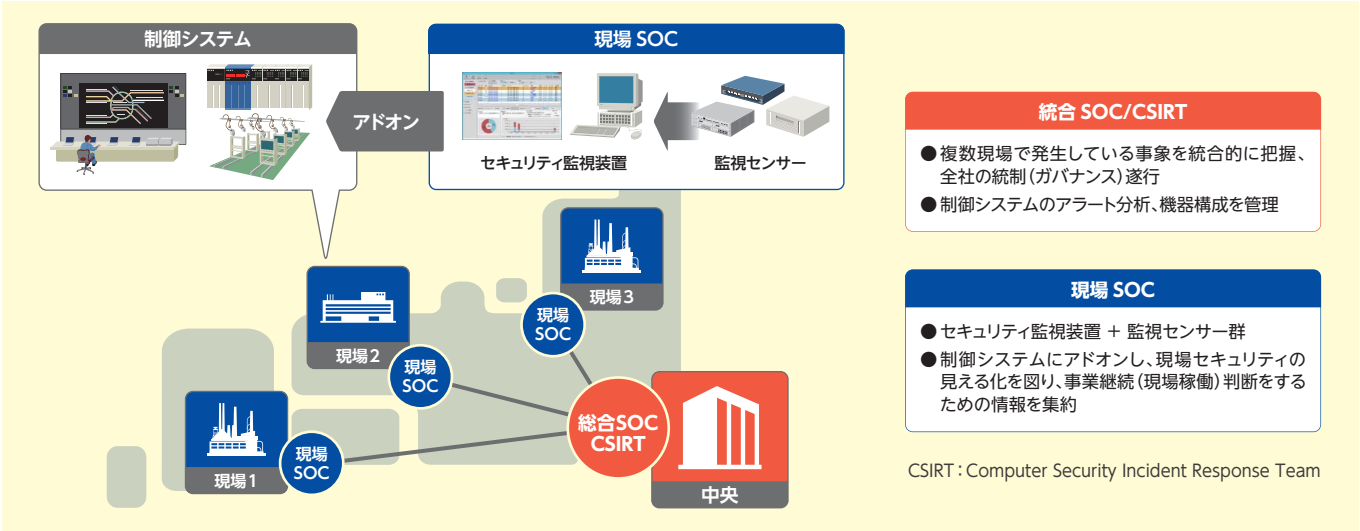

図1 セキュリティ統合監視における中央と現場の役割

これにより、現場・中央・経営層を含めた組織全体が連携して、サイバー攻撃から社会インフラシステムを守り、お客さまの事業継続を支援します。

※4 Chief Information Security Officer：最高情報セキュリティ責任者

多様な監視・検知装置群で一次対処を支援

サイバー攻撃による被害を未然に防ぐためには、不正な侵入を早期に検知することが重要です。例えば、WannaCry（ワナクライ）のようなワーム型のランサムウェアが拡散しはじめるときの通信や、標的型攻撃における攻撃者の一連の潜伏行動時などに発生する通信を監視することで不正侵入を検知することができます。このほかにも日立は多様な検知装置群を提供しており、制御システム向けのセキュリティ監視装置と組み合わせることによって、制御システムにおけるインシデント発生の早期検知や、これまで究明が困難だったインシデントの発生状況、影響範囲の迅速な把握を実現。サイバー攻撃による被害拡大を防ぐ一次対処を支援します。

サイバー・フィジカル連携セキュリティソリューション

指静脈認証を活用した入退室管理システムや監視カメラシステムは、不審者の侵入防止や監視に有効ですが、この指静脈認証をセキュアなPCログインにも活用すれば、ID/パスワードの煩雑な管理から解放され、利便性向上につながります。また監視カメラ映像※の画像解析やIoTセンサーのデータを経営的な観点で活用すれば、作業者の動態を把握した非効率作業や異常行動の検知、製造ラインや作業現場における品質管理や熟練技術の継承など、さまざまな業務改善や効率向上に役立てることができます。さらに、多くの利用者が集まる駅や空港、商業施設などの公共空間では、動態情報をマーケティングに活用して商業活性化を図ったり、混雑緩和に生かしたりするなど、お客さまサービスの向上やビジネス機会の拡大にもつなげることができます。

このようなフィジカルセキュリティまでを包含してセキュリティ監視することにより、人の操作や行動なども含めてサイバーインシデントの全体像を正確に把握し、的確に対応することが可能となります。日立は、このセキュリティ統合監視ソリューションにより社会インフラシステムの統合的なセキュリティ運用を支援していきます（図2）。

※ 映像データは、プライバシー保護などの対策を施したうえで活用します。

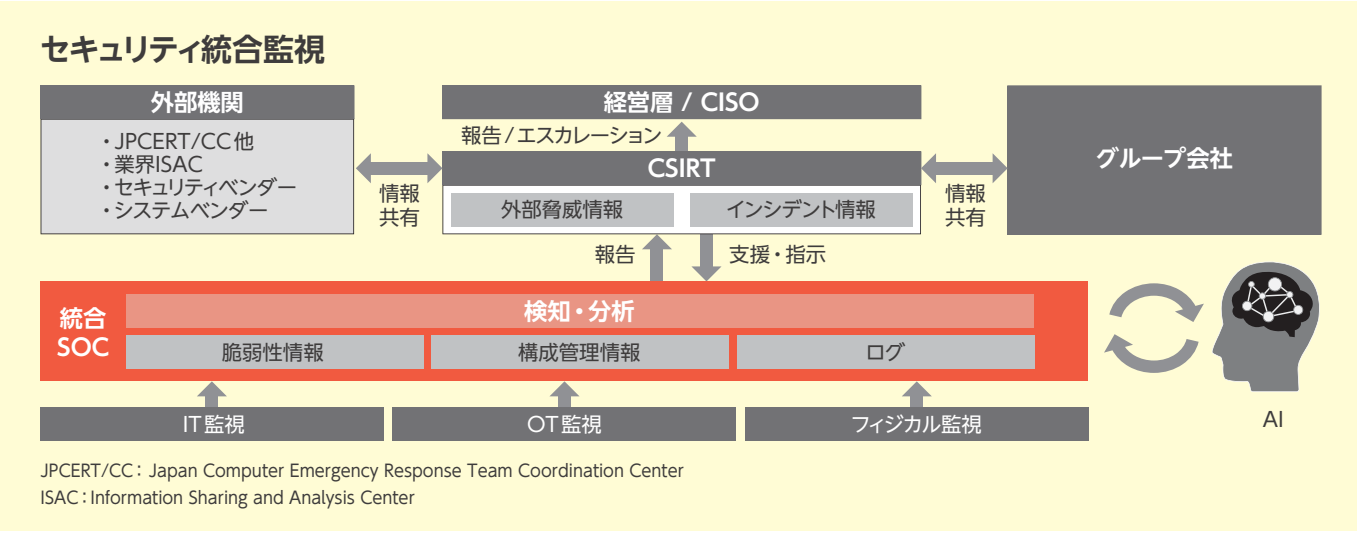

図2 セキュリティ統合監視の全体像

お問い合わせ先

(株)日立製作所 セキュリティ事業統括本部
http://www.hitachi.co.jp/security-inq/