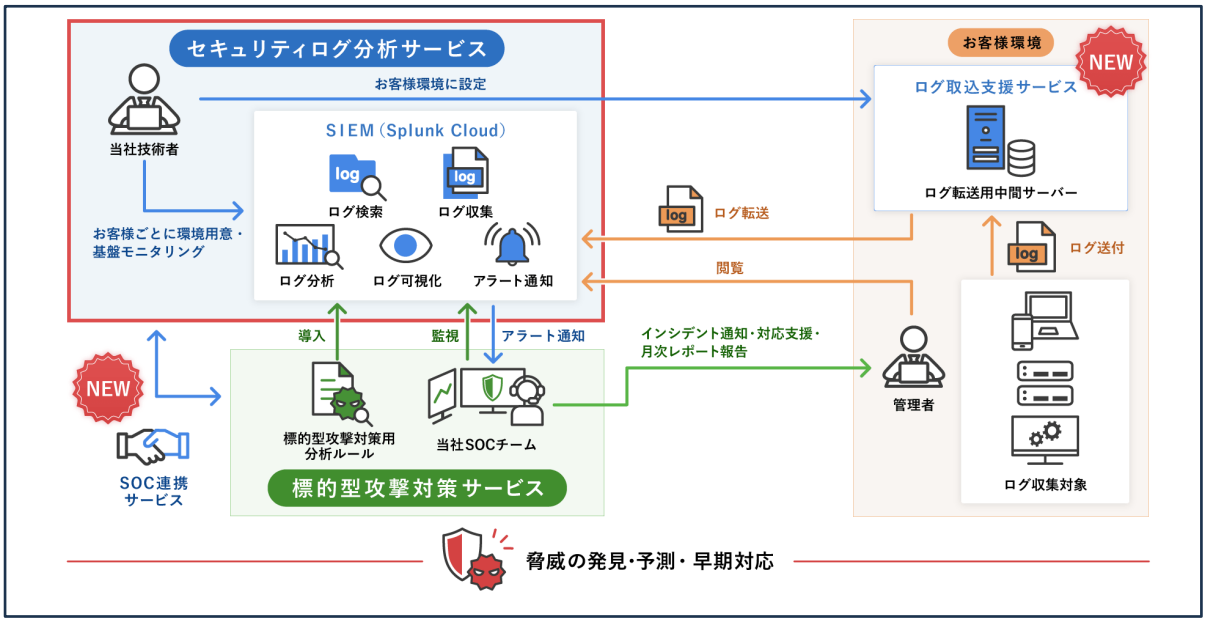
MITSUBISHI ELECTRIC
Changes for the Better

NEWS RELEASE

2025 年 9 月 16 日
三菱電機デジタルイノベーション株式会社

サイバー攻撃の発見から対策までを一括支援する「セキュリティログ分析サービス」を発売

「標的型攻撃対策サービス」との連携で高度なセキュリティ運用監視を実現



機能強化した「セキュリティログ分析サービス」利用イメージ

三菱電機デジタルイノベーション株式会社（本社：東京都千代田区、代表取締役　取締役社長：武田 聡）は、サイバー攻撃の発見から対策までを一括支援する「セキュリティログ分析サービス」（以下「本サービス」）の営業活動を本日より開始し、2025 年 10 月 1 日からサービス提供を開始します。

本サービスは、「標的型攻撃対策サービス」との連携により、多様なログ形式に対応可能な SIEM※1 へ高度な検知ルールを取り込み、検知されたインシデントに対しては、SOC※2 による 24 時間 365 日体制の監視・インシデント対応を支援します。

さらに、当社技術者による SIEM 基盤の運用支援やログ取込に関する技術支援を通して、お客様環境へのスムーズな SIEM 導入をサポートします。

これらの機能強化を含む本サービスにより、お客様は SIEM と SOC を個別に選定することなく、高度なセキュリティ運用監視を実現できます。

発売の狙い

近年、加速度的に増大し高度化するサイバー攻撃が企業経営の大きなリスクとなっています。特に、標的型攻撃のような巧妙な脅威には、多様なログを統合的に分析する SIEM の活用と、攻撃の兆候を捉える高度な検知ルールの整備が重要です。一方で、SIEM の導入・運用にはコストや技術的な複雑さが伴うため、導入を躊躇する企業も少なくありません。

当社は、これまでサイバー攻撃の発見・予測を実現する SIEM を提供してきましたが、本サービスでは、SIEM 導入支援を強化するとともに、「標的型攻撃対策サービス」との連携にも対応しました。これにより、標的型攻撃の検知に加え、25 年以上の実績を持つ当社 SOC（統合運用管制センター）による 24 時間 365 日の運用監視とインシデント対応支援が可能となります。

SIEM と SOC を組み合わせることで、サイバー攻撃の発見から対策までを一貫して支援する包括的かつ強固なセキュリティ体制をワンストップで提供します。

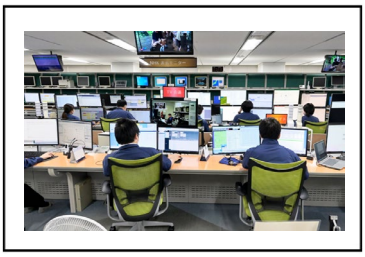
※1　SIEM（Security Information and Event Management）：収集したログのリアルタイム分析、検知アラート、レポート出力などにより異常を分かりやすく可視化する仕組み

※2　SOC（Security Operation Center）：24 時間 365 日体制でサイバーセキュリティインシデントを監視・検出・分析し、対処をおこなうための組織

サービスの特長

1.「標的型攻撃対策サービス」との連携による高度なセキュリティ運用監視の実現

・「標的型攻撃対策サービス」の提供を通じて培った高度な検知ルールを、本サービスの SIEM に取り込むことで、標的型攻撃の検知が可能になります。これにより、お客様は従来のセキュリティ対策では見逃されがちな巧妙かつ執拗な攻撃を早期に把握し、被害の拡大を未然に防ぐことが可能です。さらに、検知されたインシデントに対して、当社 SOC が、24 時間 365 日体制で運用監視します。25 年以上の運用実績を持つ当社 SOC では、専門アナリストがセキュリティインシデントを継続的に監視・分析し、お客様のインシデント対応力の向上を支援します。



当社統合運用管制センター

2. 多様なログ形式に対応した SIEM の安定運用が可能

・本サービスでは SIEM 市場で長年高いシェアを誇り、多様なログ形式に対応可能な Splunk LLC（以下「Splunk 社」※3の Splunk® Cloud（以下「Splunk ソフトウエア」）を採用しています。従来のサービスで実現していた SaaS 提供によるお客様の導入負荷軽減のメリットはそのままに、当社の Splunk 技術者が基盤モニタリングを行い、SIEM 基盤の運用支援を行います。例えば、契約ログ量の超過状況を継続的に監視することで、利用料の適正化に貢献します。契約時に定められたログ量の閾値を超過した場合には、当社からお客様に連絡を行うため、お客様はログ量管理にかかる手間を省くことができます。これにより、SIEM 基盤の運用効率が向上し、安定したセキュリティ運用が可能となります。

3. Splunk ソフトウエアへのログ取り込みを支援

・SIEM 導入時に課題となるログ取り込みを支援するオプションサービスを提供します。お客様環境のログ転送用の中間サーバーに、Splunk Heavy Forwarder と呼ばれるクライアントソフトウエアを導入・設定することで、ログのフィルタリングや変換が可能となり、取り込むログ量を調整できます。これにより、Splunk ソフトウエアの利用料軽減に繋がります。

今後の展開予定

今後、Splunk ソフトウエア上のログ分析を支援する「ログ分析支援サービス」を 2026 年度中に提供開始予定です。さらに、Splunk 技術に関する当社のノウハウを活かした更なる支援サービスを展開することで、高度化する脅威への対策強化を支援します。

※3　Splunk 社：ガートナー社による 2024 年 セキュリティ情報およびイベント管理（SIEM）部門のリサーチ(マジック・クアドラント)で 10 年連続リーダーに認定されている市場のトッププレーヤー

サービス概要

名称		主な機能	提供開始日	価格
セキュリティログ分析サービス	基本サービス	SIEM の提供及び、SIEM 環境のモニタリングサービスを提供	2025 年 10 月 1 日	個別見積
	ログ取込支援サービス	お客様環境のログ転送用の中間サーバーにクライアントソフトウエアを導入・設定し、ログ取込を支援するサービスを提供		
	SOC 連携サービス	「標的型攻撃対策サービス」との連携		
	ログ分析支援サービス	SIEM におけるログ分析に関する支援サービスを提供	2026 年度中	
標的型攻撃対策サービス		標的型攻撃を検知する SIEM と 24 時間 365 日の SOC による監視を提供	提供中	個別見積

商標関連

Splunk は、Cisco および/またはその関連会社の米国および他の国における商標または登録商標です。

参考情報

・「セキュリティログ分析サービス」
サービス紹介ページ URL：https://www.mdis.co.jp/service/security-log-analysis/

・「標的型攻撃対策サービス」
サービス紹介ページ URL：https://www.mind.co.jp/service/targeted_attack.html

三菱電機デジタルイノベーションについて

三菱電機デジタルイノベーション株式会社は、三菱電機グループの DX・IT・セキュリティに関する技術・人財・ノウハウを結集し、デジタル基盤「Serendie®（セレンディ）」を活用して、あらゆるデータをこれまでにない価値に変える「イノベーティブカンパニー」を目指します。 私たちの企業理念に込めた想い「見えない課題を、未来のチカラに」に基づき、約 6,000 人の多様な人財が集結しています。デジタルの力を活用してお客様のビジネスに変革をもたらす新しい価値を創出し、お客様の成長と多様化する社会課題の解決に貢献してまいります。
詳細は www.MitsubishiElectric.co.jp/medigital/ をご覧ください。

お問い合わせ先

＜報道関係からのお問い合わせ先＞
三菱電機デジタルイノベーション株式会社
〒100-8310 東京都千代田区丸の内2丁目7番3号 東京ビル
https://medigital.satori.site/contact/pr/

＜お客様からのお問い合わせ先＞
三菱電機デジタルイノベーション株式会社
セキュリティログ分析サービスチーム
MAIL：security-log-analysis@pb.MitsubishiElectric.co.jp