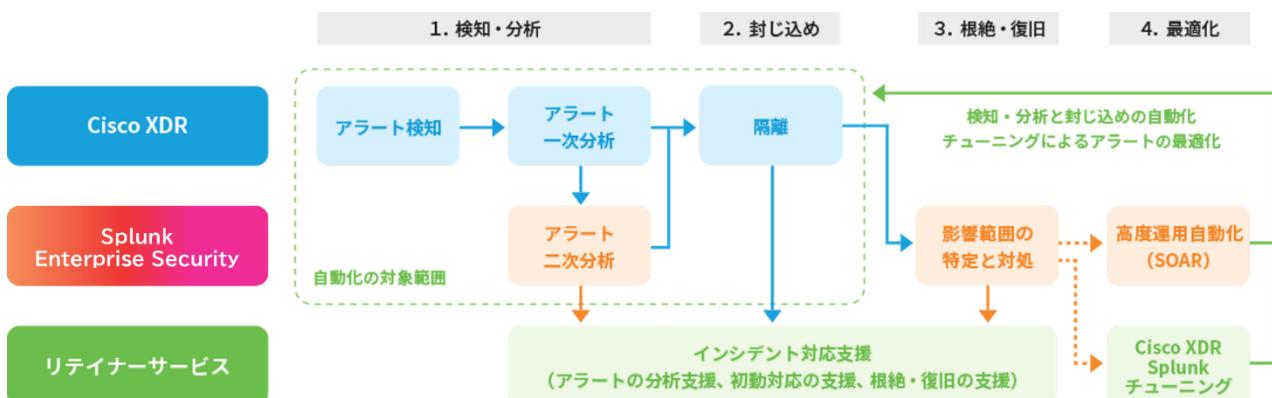


2026年1月23日
SCSKセキュリティ株式会社

企業標的型攻撃の初動対応を強化 SCSKセキュリティ、Cisco XDRとSplunk連携の 攻撃拡大防止サービスを提供開始

SCSKセキュリティ株式会社(本社:東京都江東区、代表取締役社長:小峰 正樹、以下 SCSKセキュリティ)は、「Cisco XDRによるSOCモダナイゼーションサービス」の提供を2025年12月から開始しました。企業を狙った標的型攻撃やランサムウェア被害が拡大する中、初動段階で攻撃を止める「自動封じ込め」への需要が高まっています。SCSKセキュリティは、Cisco XDRのAI機能を活用した攻撃検知と対処の自動化、Splunk Enterprise Securityによる高度な分析を組み合わせた新サービスを提供、エンドポイント隔離や相関分析、復旧支援までを一体的に提供し、セキュリティ運用リソースに課題を抱える企業のインシデント対応力向上を図ります。

1. サービスの概要



(1) AIを活用した初動対応の自動化

企業のエンドポイント(PC・スマホなど)、ネットワーク機器、クラウドサービスのログや挙動データを集約し、Cisco XDRのAI分析エンジンが、通常と違う振る舞いや攻撃の兆候を自動的に相関分析します。攻撃の可能性が高い場合、端末の隔離(ネットワーク遮断)などの初動対応を自動で実行し、被害拡大を抑制します。

(2) 専門家による詳細な二次分析

初期対応後、Splunk Enterprise Securityのログ検索機能や可視化機能を用いて、侵入経路・影響範囲・攻撃の手口を詳細に調査します。

SCSKセキュリティのアナリストが分析結果をもとに、システムの復旧や再発防止策の策定を支援します。

(3) 脅威検知と対処を高度化するチューニング

XDRとSplunk Enterprise Securityを組み合わせてアラート精度の向上・自動化・運用負荷の削減を実

施します。

従来の SIEM 運用で課題だった「アラート過多」「誤検知」「運用の属人化」を軽減します。

(4) 繼続支援を前提としたリテイナー契約

日常の監視設計から、インシデント発生時の解析・復旧まで、平時と有事を一貫支援する外部 SOC として機能自社にセキュリティ専門組織や人材がいない企業でも導入可能です。

詳細は下記 URL をご参照ください。

Cisco XDR : https://scsksecurity.co.jp/services/cisco_security/cisco_xdr/

Splunk : <https://scsksecurity.co.jp/services/splunk/>

リテイナーサービス : <https://scsksecurity.co.jp/services/ssr/>

2. Cisco Securityについて

Cisco Security(シスコセキュリティ)は、Cisco Systems, Inc.が提供する包括的なセキュリティソリューション群であり、ネットワークからクラウド、エンドポイントに至るまで、IT 環境全体を統合的に保護します。世界最高水準の脅威インテリジェンスチーム「Cisco Talos」によるリアルタイムの脅威情報を活用し、高度なサイバー攻撃に対応できます。

3. 今後の予定

今後は、Cisco Security 製品群の一つである IAM^{※3} 製品の「Cisco Duo」、SASE^{※4} 製品の「Cisco Secure Access」などを含めた関連サービスも順次拡充していく予定です。

・「Cisco Duo」関連サービス 2026 年 2 月提供予定

・「Cisco Secure Access」関連サービス 2026 年 3 月提供予定

※3 Identity and Access Management の略称

※4 Secure Access service Edge の略称

SCSKセキュリティについて

SCSKセキュリティは、サイバーセキュリティ対策に特化したSCSKグループの専門事業会社です。SI事業で培ったコンサルティング・基盤構築・運用サービスと、最新技術を活用した高品質なプロダクトを組み合わせることで、顧客企業のサイバーセキュリティリスクを低減するとともに、セキュリティ領域における投資対効果を最大化させ、安心・安全な社会の実現に貢献いたします。

商号 : SCSKセキュリティ株式会社

代表者 : 代表取締役社長 小峰 正樹

本社所在地 : 東京都江東区豊洲 3-2-20

出資比率 : SCSK株式会社 100%

事業内容 : セキュリティサービス開発・販売(コンサルティング、脆弱性診断/評価、トレーニング等)、
セキュリティ製品販売

URL : <https://scsksecurity.co.jp/>



SCSKセキュリティ

SCSKグループのマテリアリティ

SCSKグループは、経営理念「夢ある未来を、共に創る」の実現に向けて、社会と共に持続的な成長を目指す「サステナビリティ経営」を推進しています。

社会が抱えるさまざまな課題を事業視点で評価し、社会とともに成長するために、特に重要と捉え、優先的に取り組む課題を7つのマテリアリティとして策定しています。

本取り組みは、「安心・安全な社会の提供」に資するものです。

－企業標的型攻撃に対する初動対応を強化し、被害の拡大を抑制

－高精度な脅威検知から復旧支援まで、一貫した支援によりセキュリティ対策の高度化を支援

・SCSKグループ、経営理念の実践となる 7 つのマテリアリティを策定

<https://www.scsk.jp/corp/csr/materiarity/index.html>

本件に関するお問い合わせ先

【製品・サービスに関するお問い合わせ先】

SCSKセキュリティ株式会社

ビジネス開発本部 ソリューション営業部 第三課

E-mail: sys-info@scsksecurity.co.jp

【報道関係お問い合わせ先】

SCSKセキュリティ株式会社

管理本部 コーポレートマネジメント部 広報担当

E-mail: koho@scsksecurity.co.jp

※ 掲載されている製品名、会社名、サービス名はすべて各社の商標または登録商標です。