SPECIAL INTERVIEW

「SIEMの限界」を突破せよ

――攻撃者優位の時代に求められる次世代セキュリティ運用

SCSKセキュリティ株式会社
亀田 勇歩

×

パロアルトネットワークス株式会社
染谷 征良 氏

SCSK
SCSKセキュリティ株式会社

paloalto NETWORKS

サイバー攻撃がますます高度化・高速化し、「アタックサーフェス（攻撃対象領域）」が飛躍的に拡大している今日、従来型のセキュリティ運用体制では企業を守り切るのが至難になっている。とはいえ、売上規模が1,000億円を超え、世界規模でサプライチェーンや拠点を展開する大企業にとって、防御体制を再構築する難度は高い。その難題を解決する方策について、SCSKセキュリティのCTOであり、ZAPエバジェリストやDEFCONで開催されたRecon Village CTF優勝といった数々の実績を有する亀田 勇歩氏と、パロアルトネットワークス チーフサイバーセキュリティストラテジストであり、イギリス、カナダ、そして日本のセキュリティ企業での勤務経験を持ち日本国内・海外のセキュリティ事業にも精通している染谷 征良氏に伺う。

INTERVIEWEE

SCSKセキュリティ株式会社
CTO
亀田 勇歩

PROFILE

- Webアプリケーション脆弱性診断、プラットフォーム脆弱性診断をはじめ、SOC監視サービスやCSIRT運用、ASMなどサービス開発・企画や運用で多くのサービスに携わる
- OWASPのプロジェクトから生まれたOSSの脆弱性診断ツールであるZAP(Zed Attack Proxy)のエバンジェリスト
- DEFCONで開催されるCTFに出場し、2023年と2024年にOSINTに特化したCTFにおいて2年連続優勝
- 東京電機大学の国際化サイバーセキュリティ学特別コース(CySec)の外部講師として10年に渡って講義を担当
- SNSの利用に関する危険性や、OSINT技術を活用したテクニックについて複数の国内テレビ局などでコメント

パロアルトネットワークス株式会社
チーフサイバーセキュリティストラテジスト
染谷 征良 氏

PROFILE

- 10年以上に渡り海外セキュリティベンダーの本社で製品・技術戦略、営業・マーケティングを担当
- 世界各地の民間企業や公共機関のセキュリティを支援
- 世界のセキュリティエンジニアを対象としたCTF国際大会の企画運営責任者を4年間務める
- RSA Conference Asia Pacific & Japanのプログラム委員を5年間務める
- 経済産業省セキュリティキャンプで官民連携での実施に際し最初の実行委員を務める
- ZDNet Japan、Forbes Japanでオフィシャルコラムニストとして最新のセキュリティトレンドに関する記事を執筆
- サイバーセキュリティのトレンドに関して、国内全キー局ならびに公共放送やBBC、大手新聞社などでコメント

爆発的に広がる“アタックサーフェス”――攻撃者が「圧倒的優位」の時代に

10年前と今日では、企業のサイバーセキュリティを取り巻く状況がまったく異なっている。決定的な違いの1つは、SaaSなどのクラウドの普及だ。これにより、企業と国内外の各拠点やパートナーとを結ぶネットワークが複雑化し、社内外ネットワークの境界線を堅牢化するだけではセキュリティが担保できなくなった。また、リモートワークが定着したことで、社員が外部環境からクラウドに直接アクセスするようになり、ID・認証情報が狙われるケースも急増している。

こうした変化について、SCSKセキュリティの亀田氏はこうまとめる。

「クラウドやリモートワークの普及・定着は、大企業のシステム構造を複雑化させ、“アタックサーフェス（攻撃対象領域）”を一挙に拡大させました。その変化によって、サイバー攻撃に対する防御・検知の難度は以前とは段違いに高まっています」（亀田氏）

さらに、サイバー攻撃の高度化・高速化も進んでいると、パロアルトネットワークスの染谷氏は指摘する。

「近年では、特定の企業を狙った攻撃よりも『弱点があれば一気に攻撃する』という手口が目立ちます。ネットワーク機器の脆弱性や設定ミスなどの不備を突かれ、被害に遭うケースも珍しくありません。そのうえで、サイバー犯罪者は侵入に成功してから平均すると僅か2日間で重要情報を抜き取り終わっています」（染谷氏）

かたや、企業がセキュリティ侵害に気づくのには平均で13日間も要しているという。**「この攻撃者優位の状況を打開すべく大企業は『SIEM（Security Information and Event Management：セキュリティ情報・イベント管理）』をはじめとする各種ソリューションを導入してきましたが、従来型の対策には限界が見えています」**と染谷氏は指摘する。

では、どうすればアタックサーフェスの拡大や攻撃の高度化・高速化に対抗できるのだろうか。

行き詰まる大企業の従来型セキュリティ運用

先に染谷氏が触れたとおり、大手を中心に、多くの企業がこれまでコンプライアンスやセキュリティ監査を目的にSIEMを導入してきた。ただし、従来型のSIEMを使ったセキュリティ運用にはいくつかの問題があったと亀田氏は指摘する。

「SIEMは本来、エンドポイントやネットワークなど、異なる領域のシステムからログを収集し、相関分析することで威力を発揮する仕組みです。ところが、多様なシステムから膨大なログを収集し、相関ルールを作成するまでに多大な工数やコストがかかり、ゆえに『システム全体のログが入れられない』『チューニングや相関ルールの作り込みが追いつかず、誤検知・過剰アラートが続発する』といった問題を引き起こしてきました。結果としてSIEMが単なる『監査用ログの倉庫』と化してしまう例が多く見られてきたのです」（亀田氏）

加えて、これまでは「EDR（Endpoint Detection and Response：エンドポイント検知・対応）」や「ファイアウォール」、「クラウド監視」といったソリューションもバラバラに導入され、各ソリューションを使って監視を代行する協力会社（以下、監視ベンダー）もそれぞれ異なるのが一般的だった。それが結果として「ログの相関分析が行えない」「アラートの全体像が把握できない」といった問題を引き起こしている。

この問題について、亀田氏は**「セキュリティのソリューションや監視ベンダーがバラバラで、それぞれがサイロを成しているのが、大企業のセキュリティ運用によく見られる状況です。この場合、セキュリティ監視を担う現場のアナリストが、事あるごとにログを手作業でなめ回さなければならず、それがインシデントに対する初動の遅れへとつながってきました」**と指摘し、加えて**「こうした人手に頼ったセキュリティ運用は、優秀な人材に多くの負担をかけて疲弊させ、離職を招き、それが人材のさらなる不足につながるといった悪循環に陥るリスクも高いといえます」**と警鐘を鳴らす。

さらに、染谷氏はこう続ける。

「サイバー攻撃者が僅か数日で目的を達成する中で、初動対応の遅れをはじめ、インシデントに気づくまでの時間、対応に要する時間が長期化するのは致命的です。しかも、協力会社や海外拠点の間でガバナンスやセキュリティポリシーへの順守が徹底されていないと、日本の本社だけがいくら頑張ってもサイバー攻撃から自社を守り切れません。どこか1つでも脆弱性や不備があれば、そこから侵入されてしまうのです。協力会社や海外拠点で発生した被害でも、結果的に対応や公表に追われるのは本社です」（染谷氏）

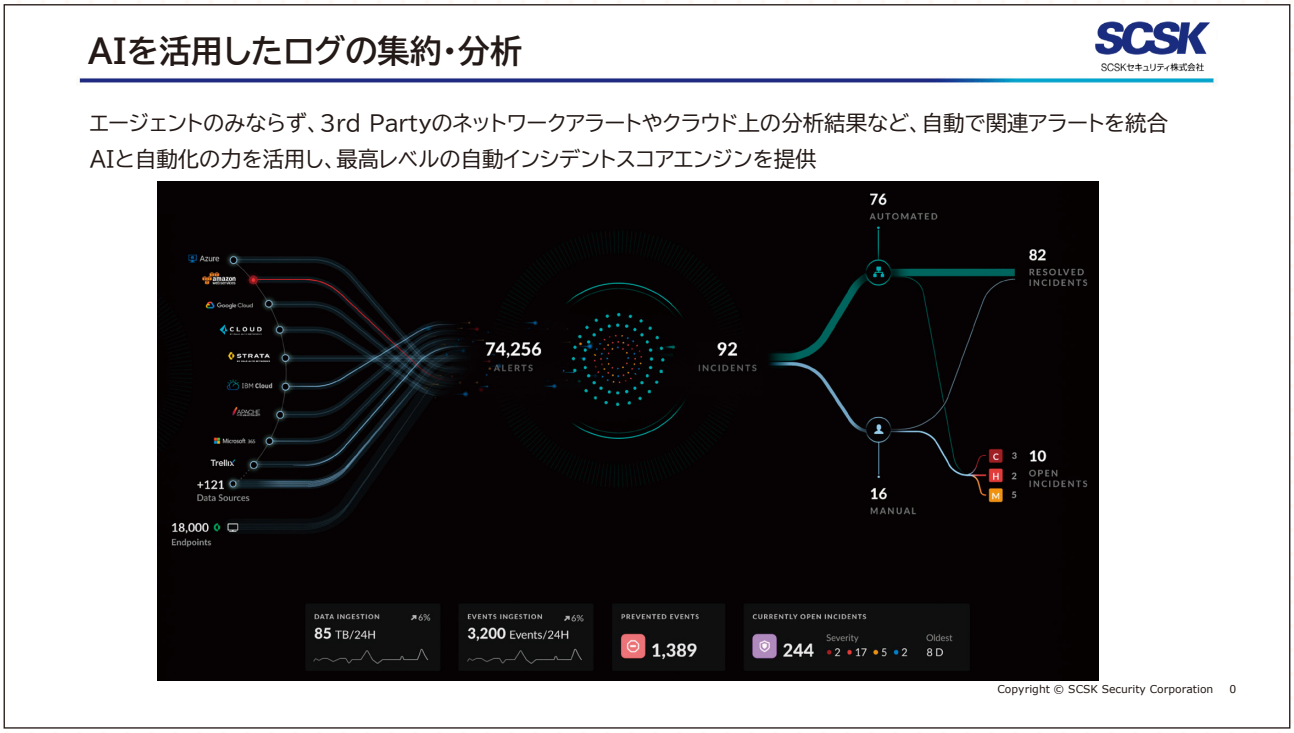
「AI×自動化」により運用を根本から変える
――次世代プラットフォーム「Cortex XSIAM」が打ち破る従来型SIEMの限界

「セキュリティ運用で苦しむなら、自動化できないか」――その発想から生まれたのが、パロアルトネットワークスの「Cortex XSIAM」だ。これはSIEM、XDR、SOAR（Security Orchestration, Automation and Response）、ASMなどのセキュリティ運用に必要な機能を包括的に統合したクラウド型の次世代プラットフォームである。

ログの取り込みから相関分析、自動対応までを一気通貫で実行でき、AIがアラートに優先順位を付ける。ゆえにアナリストは、本当に対応が必要なインシデントのみに集中することが可能になる。

同製品の優位性について染谷氏は**「Cortex XSIAMは、エンドポイントからネットワーク、クラウド、認証基盤に至るまで、あらゆるソースのログを自動収集し、AIが相関分析を行います。ですので、従来型SIEMのように相関ルールの作成やチューニングに多くの手間とコストをかける必要が極端に少なくなります。本製品では『自動封じ込め』の仕組みも強化され、24時間365日リアルタイムでサイバー攻撃や内部不正を狙い撃つことが可能です」**と説明する。

Cortex XSIAMでは、基本的なアラートはAIが判定し、平易なケースは自動で封じ込めまでを行う。その中でアナリストは「高度な脅威に関する最終的な判定」や「新たな攻撃パターンの解析」「インシデント後の事業影響評価」といった付加価値の高い業務に専念できる。染谷氏は、こうしたAIと人との役割分担によって優秀な人材のモチベーションがアップし、離職防止やセキュリティ監視の「内製化意欲」の向上にもつながっていくとしている。



「AI×自動化」によってアナリストによるログの収集・相関分析の手間を大きく引き下げるCortex XSIAMの管理画面

SCSKセキュリティの果たす役割
――Cortex XSIAMの運用定着までを一気通貫で支える

Cortex XSIAMには、セキュリティ運用のあり方を大きく変えられる可能性がある。ただし、同製品を導入すれば、自動的に運用が変えられるわけではない。

その点について、亀田氏は「Cortex XSIAMによる効果を最大限に引き出すうえでは、どのログを収集し、どこを自動化し、どの段階で人が介入すべきかの設計と運用をしっかりと行うことが必須です。その課題の解決に向けて、セキュリティに関する『技術力』と『運用ノウハウ』、そして『コンサルティング』を三位一体で提供することが、SCSKセキュリティが担う役割であり、価値を高めることにつながります」と語り、こうも続ける。

「SCSKセキュリティは、長年にわたってSOC監視やCSIRT運用、脆弱性診断、クラウド移行支援、さらには海外拠点に対する施策展開をサポートし、大企業が抱えるセキュリティ運用の課題を熟知しています。そうした当社の強みとCortex XSIAMを融合させれば、グローバル規模でのセキュリティ改革がスムーズに進むと確信しています」（亀田氏）

表1：SCSKセキュリティが有する3つの強み

①幅広いサービス実績	●Webアプリケーション／プラットフォームの脆弱性診断からSOC監視、CSIRT運用までを手がける総合力 ●ZAPエバンジェリストやRecon Village CTF優勝経験者など、ハイレベルな技術者が多数在籍
②一気通貫のコンサルティング＆導入支援	●クラウド環境におけるログ収集範囲や運用ルールの設計を含め、顧客企業のシステムと密接に連携 ●拠点・子会社・取引先も含めたガバナンスの設計支援をサポート
③ビジネス視点によるセキュリティ運用の最適化	●「攻撃を防ぐ」だけではなく「事業リスクを最小化」する視点でゼロトラストセキュリティやアクセス制御を構築 ●必要に応じて段階的に導入スコープを広げながら、コストと効果をバランスさせる

亀田氏の言葉を受けたかたちで染谷氏は、SCSKセキュリティに次のような期待を寄せる。

「Cortex XSIAMという“AI×自動化”のソリューションの導入は、セキュリティ運用を根本から変える大きなチャンスを切り開くものです。ただ、その効果を最大限に生かすうえでは、導入・運用・グローバル展開まで含めた総合的な支援体制が欠かせません。SCSKセキュリティは、そこを一貫してサポートできる数少ないパートナーです。同社が有するセキュリティ専門のコンサルティング力と運用力が組み合わさることで、グローバル全体を見渡したセキュリティ運用が可能になります」（染谷氏）

さらに染谷氏は「日本の大企業では、セキュリティ運用を担う幹部の多くが『海外拠点にセキュリティ上の統制を利かすのが難しい』『海外拠点で何が起きているか可視化できていない』といった悩みを抱えています。Cortex XSIAMを中心にしたSCSKセキュリティとの協業を通じて、そうした悩みも解消していきたいと考えています」と付け加える。

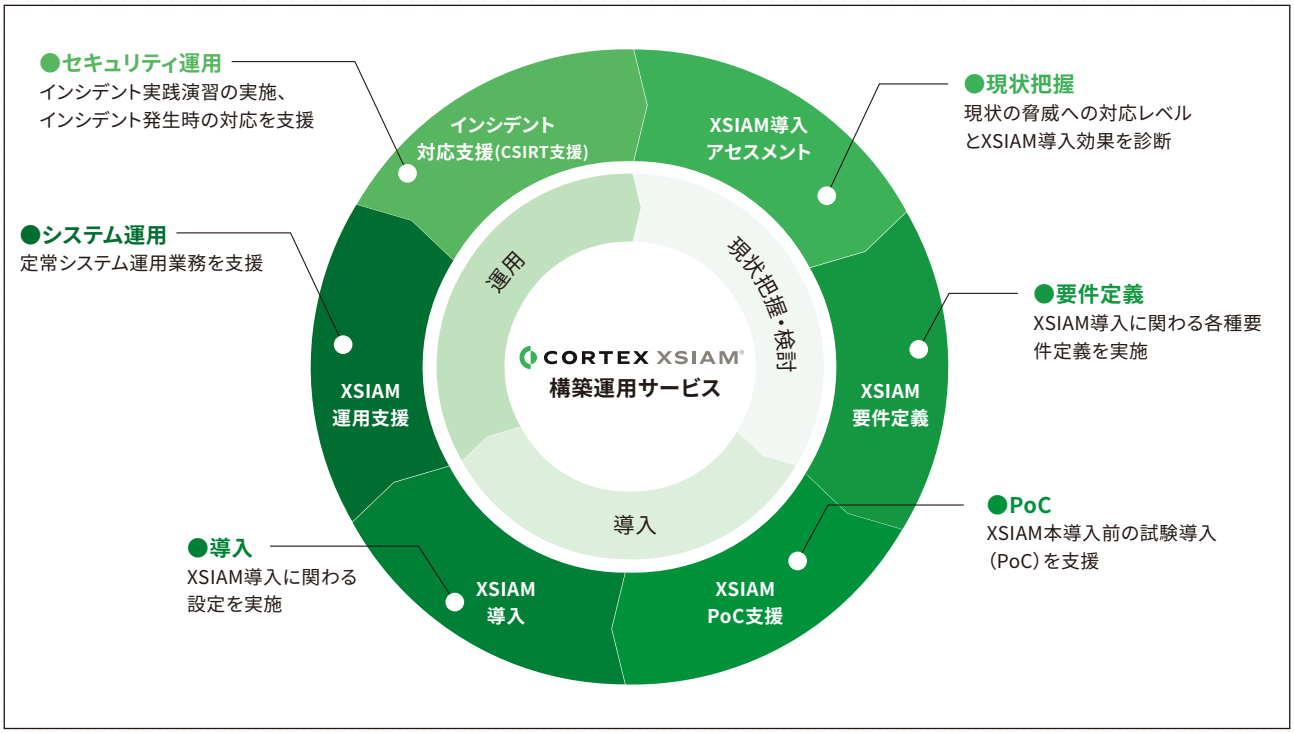
今こそ“セキュリティ運用の次元上げ”に踏み切る好機

アタックサーフェスが拡大し、サイバー攻撃の多様化・高速化も進む今日では、「いかに早くインシデントに気づき、対応するか」が、セキュリティ運用の要諦となっている。それを実現するには、これまでのようにSIEMやEDRといった特定課題を解決するための製品を個別に導入し、積み上げていくのではなく、ログの収集・分析・自動対応を包括的に実現できるプラットフォームと総合的な運用ノウハウを手に入れることが必須となる。言い換えれば「AI×自動化」によるセキュリティ運用の変革に向け第一歩を踏み出すことが重要であるわけだ。

その観点から、SCSKセキュリティでは、Cortex XSIAMを核とした大企業向けのセキュリティシステムの構築・運用サービスを展開している。その概要は次に示すとおりだ。

- グローバル規模での資産棚卸し・権限管理のアドバイス
- SOC/CSIRTサービスとの連携
- ゼロトラストセキュリティの実現に向けた段階的アプローチの提案・支援
- インシデント発生時の「初動」「対応」「再発防止策」の策定支援

同社ではこれらの支援内容をまとめた資料も取り揃えている。「今のセキュリティ運用に限界を感じている」「海外拠点を含む大規模ネットワークに自動化を導入したい」と考える方は、これらを参考にしてみてはいかがだろうか。



SCSKセキュリティが展開しているCortex XSIAM構築運用サービスの全体イメージ

SCSKセキュリティ株式会社
営業本部ビジネス開発部
〒135-0061 東京都江東区豊洲3-2-20 豊洲フロント

商品の詳細はこちらホームページをご覧ください
SCSKセキュリティ XSIAM

Cortex XSIAM 担当
sys-info@scsksecurity.co.jp
https://scsksecurity.co.jp/services/cortex-xsiam/