複雑化/高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス

有松 龍彦　矢野 由紀子　高橋 豊

要 旨

サイバー攻撃が高度化・巧妙化するなか、新たに開発される対策製品が一定の成果を上げる一方で、その多くは運用者の判断能力を必要とするものが多く、その運用の難しさも相まって、被害が減少する状況には至っていません。セキュリティオペレーションセンター（SOC）による監視サービスは、その運用をエンドユーザーに代わってプロフェッショナルが代行するサービスであり、サイバーセキュリティ分野でも特に関心の高いサービスです。本稿では、セキュリティ監視サービスを提供しているSOCについて、現在の主要な課題や課題解決のための新たな取り組みを解説するとともに、SOCの今後のあるべき姿を展望します。

KeyWords　セキュリティオペレーションセンター／SOC／セキュリティ監視サービス／AI／機械学習

1. サイバー空間を取り巻く環境

1.1 サイバー攻撃の高度化・巧妙化

ここ数年、メールによる標的型攻撃やWebサイトの脆弱性を突く攻撃など、サイバー攻撃による情報流出の被害が拡大しています。また、バンキングマルウェアやランサムウェアなど、金銭の不正取得を目的としたサイバー攻撃も増加傾向にあります。特に、プロのサイバー犯罪組織によるものと見られる攻撃は、高度化・巧妙化が著しく、対策が非常に難しくなっているのが現実です。

例えば、アンチウイルスソフトやIDS・IPSなどのパターンマッチング型の対策製品では、新たな攻撃手法や新種のマルウェアは検知しないケースが多く、攻撃された組織で被害が発覚し、製品ベンダーからシグネチャが配布されるまでは、対象の攻撃に対して有効な対策となりません。近年、普及が進んだサンドボックス型製品やAIを活用した製品も、一定の成果を見せている一方、その対策を回避する攻撃手法が現れているのが現実です。例えば、マルウェアを暗号化した圧縮ファイルにする手法、マルウェアのコードに不要なコードを大量に付加してファイルを大容量化する手法などは、それらの検知を回避する手法の一例です。

これまでも言われてきたとおり、セキュリティ製品単体での対策には限界があり、対策を組み合わせて組織の守りを強固にしていく必要があります。

1.2 セキュリティオペレーションセンター（SOC）へのセキュリティ運用のアウトソース

実際に、複数のセキュリティ対策を導入し、サイバー攻撃への備えを着実に進めている組織は数多く存在します。一方で、インターネット経由でやり取りされるデータの増加に伴い、セキュリティ対策装置（以下、セキュリティデバイス）から生成されるログやアラートも増加の一途を辿っており、その対応に苦慮している組織が多いことも事実です。それらのログやアラートに対して、誤検知なのか、重要ではないイベントなのか、それとも注意すべきイベントなのかなどを迅速かつ適切に判断するためには、セキュリティデバイスについての知識に加え、ネットワークスキル、サイバー攻撃手法や脆弱性情報などのセキュリティの知識、システム・ネットワーク環境の把握など、幅広い知識・ノウハウを必要とします。

このような状況において、多くの組織では、セキュリティログやアラートに関わる監視・運用を、外部のセキュリティ専門会社が運営するSOCにアウトソースする動きが加速

しています。なお、これまではセキュリティデバイスが発するアラートを顧客へレポートするだけのSOCにも一定のニーズがありましたが、サイバー攻撃の巧妙化・高度化に伴い、適切な事象判断を行うスキルを持ったSOCによるセキュリティ運用監視サービスへの期待・ニーズが今後一層大きくなってくると考えられます。

2. SOC運用の現状

2.1 ログ分析における課題

NECとNECグループのセキュリティ専門会社の1つである株式会社インフォセック（以下、インフォセック）が運営しているサイバーセキュリティ・ファクトリーでは、セキュリティデバイスが発する大量のログ・アラートに対してアナリストが独自で分析を加え、イベントの重要性・深刻度を判断しています。実際に、セキュリティデバイスが発した警戒レベルと、アナリストの分析を経た警戒レベルは異なることが多く、アナリストはそのログから生成されたイベントが誤検知なのか、Level1～4のどのレベルに該当するのかを分析・判断しています（**図1**）。この分析作業によって、ユーザーにとって必要な事象のみ、適切に通知することを可能としています。

しかし、従来の日本のセキュリティ監視サービス市場では、セキュリティデバイス単位でサービス契約を結ぶことが一般的です。その一方で、セキュリティデバイス単体のログ・アラートだけでは、イベントの事象レベルを判断する材料が足りないことが多く、アナリストの過去の知見（顧客のシステム環境や通信傾向の知識など）や、二次的な判断材料の取得を必要としているのが実態です（**図2**）。これが、分析業務を難しくしている一因となっています。

実際のイベントの傾向としては、誤検知や攻撃失敗が占める割合が大きいため、アナリストの分析業務においても、誤検知の判断、攻撃失敗の判断を下すために多くの時間を要している現状があります（**図3**）。

また、図3の前年比でのイベント数の増加傾向からも分かるとおり、アナリストの分析業務負荷は高まる一方です。早急にこの状況を改善することが、求められています。

2.2 SOCアナリストのリソース面の課題

サービスへのニーズが高まるなか、その需要に対応するにはアナリストの増員という解決策が考えられます。しかし、ここにも大きな課題があります。

経済産業省の調査によると、情報セキュリティ人材は2016年の時点で約13万人が不足しており、2020年には19万人超に拡大すると言われています。SOCアナリストという職種においても不足の状況は同様です。特に、SOCアナリストに求められる技術知識は高く、他のセキュリティエンジニアと比べても育成に時間が掛かるところに、より大きな課題があります。

例えば、ゲートウェイ型のセキュリティデバイスの監視を

図1　セキュリティイベントの分類

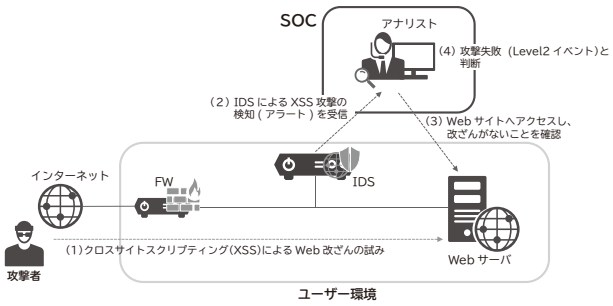


図2　攻撃成功/失敗の判断における追加調査の例

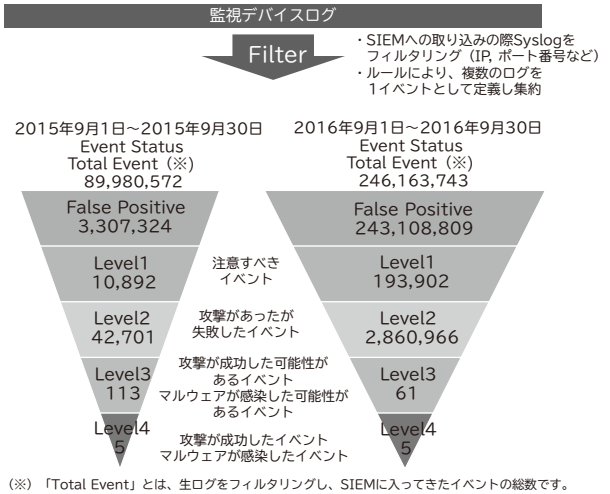


図3　サイバーセキュリティ・ファクトリーにおけるカテゴリ別イベント数とイベント増加状況

行うには、ネットワークに関する正確な知識が必要となります。イベントによってはパケットを確認する作業も発生することから、プロトコルに応じたパケット構造を正しく把握しておくことも必要です。特に、SOCでは分析・判断にスピードが求められるため、すぐに頭から取り出せるレベルでの技術理解が非常に重要です。場合によっては、マルウェア解析が必要な場面もあり、プログラムコードを読むスキルも求められます。

前述した内容は一般のIT・ネットワーク知識がベースとなるスキルですが、それに加え、典型的なサイバー攻撃手法や流行りの攻撃手法など、攻撃の手口についても継続的にキャッチアップしていく前向きな取り組み・好奇心も必要です。

また、アナリストに求められる技術レベルを考慮すると、机上での知識習得だけでなく、OJTによる現場（SOC）での育成プロセスは欠かせません。しかし、OJTを行うには既に現場での運用を担っているアナリストの手が掛かるため、育成可能な人数には限りがあります。このように、恒常的にアナリスト人材の育成を行う努力とそのプロセスは継続しているものの、アナリストを短期育成・大量育成し、リソースを拡大するという施策は非現実的であると言えます。

3. AIによる新たな取り組み

前述のとおり、SOCによる監視サービスの拡大には、ログ分析の処理量の増大、アナリストリソース不足が大きな課題として立ちはだかっています。そこでNEC、インフォセックでは、ログ分析の省力化を目的として、AI（人工知能）を活用した「脅威分析サーバ」の開発に取り組みました。「脅威分析サーバ」では、個々のイベントに関連する通信パケットの特徴量とアナリストの判断結果を学習データとすることで学習済みAIを構築し、更にリアルタイムの実データで検証することで、判断精度の向上を図ってきました。一方で、できるだけ高い精度で誤検知のアラートを「誤検知である」と判断させようと設定値（しきい値）を変えると、そのトレードオフとして偽陰性（見逃し、実際の攻撃を誤検知と判断すること）が稀に起こってしまいます。しかし、偽陰性を限りなくゼロに維持することはサービスの特性上必須であることから、偽陰性を起こさないよう、設定値（しきい値）のチューニングは非常に慎重に行っています。

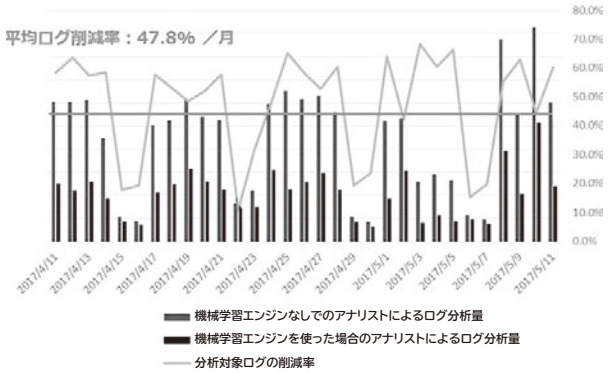


図4　サイバーセキュリティ・ファクトリーにおけるAI（機械学習）によるログ分析の効率化

また、最近では、AIの適用範囲を拡大し、誤検知だけでなく、Level1、Level2の事象までAIで判断する取り組みを開始しています。現時点においても、50%程度の分析対象ログの削減を実現しており、アナリスト業務の効率化につながっています（**図4**）。

このように、AIを活用しアナリスト業務の多くを占める軽微なイベントを自動的に分析・判断することで、アナリストは高度化する攻撃への対処法や検知精度の向上策を検討するといった、より重要な業務に集中することができます。

AIの積極活用によって、監視サービス品質がより標準化されるとともに、アナリストの新しい取り組みによって、高度な攻撃に対しても高い検知能力を備える高品質なサービスの実現にも寄与することになると考えています。

4. 監視サービスの高度化に向けて

これまでにも述べたとおり、セキュリティデバイス単体のログ・アラートだけでは、アナリストは判断材料が足りず、分析に手間が掛かっているのが実態です。また、あるアラートが本当の攻撃を検知しているにも関わらず、攻撃の成否判断までできないケース（Level3と判断した事象など）も存在し、分析精度の観点でも課題があります。

今後、複雑化する脅威に対抗していくには、やはり複数のセキュリティデバイス、更にはサーバ群やクライアントのログまでを組み合わせ、組織として防ぐべき脅威を明確にし、脅威単位で分析していく必要があります（**図5**）。

そのためには、従来のようなセキュリティデバイス単体

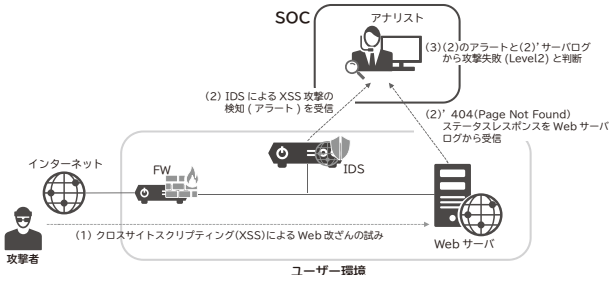


図5　複数ログの組み合わせによる効率的判断の事例

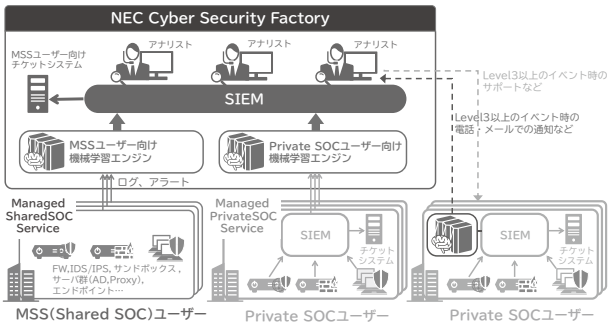


図6　サイバーセキュリティ・ファクトリーにおけるSOCの目指す姿

の監視サービスだけではない監視サービス市場を、形成していくことも必要であると考えています。

また、複数デバイスのログ・アラート（入力）とそれに基づくアナリストの判断結果（出力）がデータとして蓄積されていくことで、入力と出力の相関がより高い学習データが構築されることが予想され、AIによる分析精度も高まり、SOCにおけるAIの活用範囲もより広がっていくものと推測されます。

5. SOCの将来展望

今後、サーバやクライアントまで含めたさまざまな機器のログを複合的に監視するサービスを実現するためには、現在にも増して多くのログ・アラート量をSOCとして受け取ることになります。そのため、前述のとおり、AIの活用によって重要でないイベントのフィルタ機能を整備し、重要イベントだけをアナリストが分析・判断できるようにするプロセスを実現する必要があります。

また、大規模組織では、独自にSOCを構築し（以下、プライベートSOC）、ログ・アラートを内部で一元管理している事例も複数あります。一方で、アナリストまで独自に抱えることは難しいため、プライベートSOCの運用をアウトソースするケースも今後増えていくことが予想されます。

しかし、プライベートSOCの運用は組織ごとに異ならざるを得ない部分も多く、ベンダー側のリソース面の課題も相まって、それをベンダー側でそのまま請け負うことは難しいのが実態です。そのため、プライベートSOC専用に汎用的なイベントをフィルタする機能を実装し、重要なイベントのみをサービス提供側のアナリストが分析する仕組みを整備していく必要があると考えています（**図6**）。

また、SOCで検知したインシデントの可能性が高いイベントに対して、ファイアウォールのポートを閉じるなどといった既存の簡易なインシデント対応に加え、サーバやクライアントの調査を含めた高度なインシデント対応までSOCから迅速かつシームレスにサービス提供していくことをNECは目指しています。

NEC及びインフォセックスは、セキュリティ運用の観点から、重大インシデントを未然に防ぐことを担保し、お客様のサイバーセキュリティに関わる不安を解消することで、お客様が本業へ集中するためのサポートを提供し続けたいと考えています。

執筆者プロフィール

有松 龍彦
株式会社インフォセック
サイバーインテリジェンスセンター
センター長

矢野 由紀子
ナショナルセキュリティ・
ソリューション事業部
シニアエキスパート

高橋 豊
セキュリティ事業推進室
マネージャー

関連URL

株式会社インフォセック
https://www.infosec.co.jp/

24時間365日監視！ 巧妙化するサイバー攻撃から企業を守るNECの「セキュリティオペレーションセンター」
http://jpn.nec.com/info-square/mitatv/discover/34/index.html

AIを活用した脅威分析サーバを開発　SOC運用の最大80%の効率化を目指す
http://jpn.nec.com/cybersecurity/journal/06/interview_01.html

NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

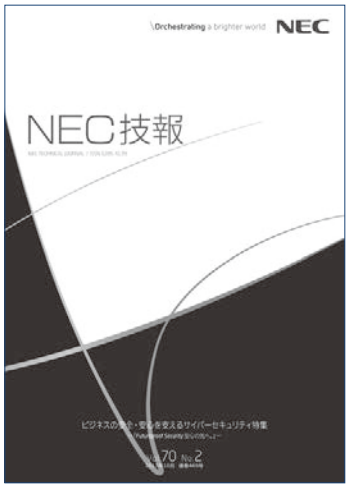
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP