NTTデータ先端技術　セキュリティ運用自動化ソリューション（SOAR）

セキュリティ運用の効率化・高度化を実現する「SOAR」の導入を支援

自動化を基軸にセキュリティ運用の効率化・高度化を実現するソリューションとして、「SOAR[*1]」が注目を集めています。サイバー攻撃が質量ともに激化するなか、限られた要員による迅速な対応が求められるSOC[*2]やCSIRT[*3]などでは、セキュリティ運用業務の効率化・高度化は解決すべき喫緊の課題です。SOARは、インシデント対応の迅速化とコスト削減に有効なセキュリティ運用を自動化するソリューションです。NTTデータ先端技術では、このセキュリティに特化した自動化ソリューションについて、SOAR製品の「Splunk Phantom」をはじめとするSOAR製品の検証を現在実施しており、この検証結果を踏まえて、SOARの導入支援ビジネスを展開することとしています。

*1　Security Orchestration, Automation & Response
*2　Security Operation　Center
*3　Computer Security Incident Response Team

注目され始めた「SOAR」とは

わが国では、セキュリティ人材は2020年に37.1万人必要と推計されていますが、十分な人材確保は難しく、19.3万人不足と見込まれています※。しかし、セキュリティ運用の現場では、アラートが増大し、攻撃側の技術も速度も向上していることから、より迅速な対応が求められています。

セキュリティに特化した自動化ソリューションであるSOARにより、高度化する攻撃、増大するアラート、迅速な対応が求められるセキュリティ業務の人材不足を緩和できます。

SOARは、導入済みのさまざまなセキュリティシステムからのデータ収集・可視化・分析、さらにはインシデント管理と対応の自動化を実現するソリューションです。セキュリティ運用業務で必要となる自動化は、複数のセキュリティデバイスから出力されるアラートを統合（オーケストレーション）して分析し、自動化（オートメーション）する必要があります。また、攻撃側の速度も上がっており、迅速に対応（レスポンス）する必要がありますが、ここでも自動化による対応速度向上が有効となります。さらに自動化により、貴重なセキュリティ人材の単純作業を代行し、高度な分析・判断に集中することができるようになります。

OODAループの高速化により高度なセキュリティ運用を実現

SOARの基本的な考え方を、OODAループという管理メソッドに基づいて整理します。セキュリティ運用の中で、どのような自動化が可能かOODAループを用いて説明します。

OODAループとは、アメリカの軍事戦略家であるジョン・ボイド氏が発明した、先の読めない状況で成果を出すための意思決定方法です。図1に示したように、「観察（Observe）」「（状況判断）（Orient）」「意思決定（Decide）」「実行（Act）」の4つからなるループです。工場の生産性を高めるために作られたPDCAサイクルと異なり、戦場で迅速に意思決定をするために考えられたフレームワークであり、セキュリティ運用に向いたフレームワークといわれています。

セキュリティ運用をOODAループに当てはめて考えると、観察（Observe）としては、各種セキュリティデバイスのセキュリティアラートの検出が該当します。状況判断（Orient）としては、観察されたセキュリティアラートの内容に応じた

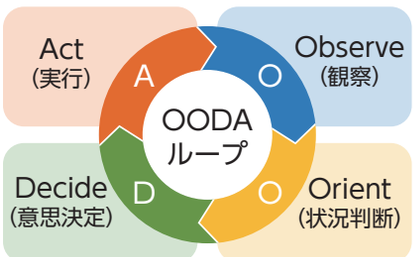

図1　OODAループの概要

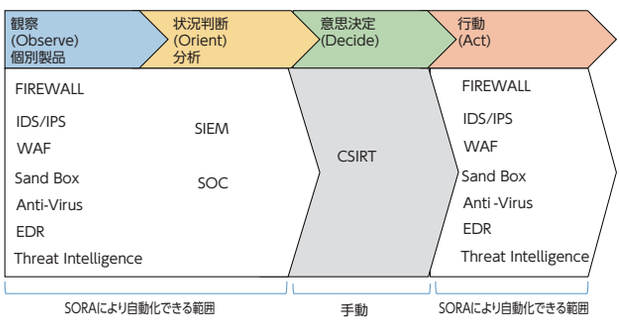

図 2　OODA ループのセキュリティ運用自動化による高速化

SIEM を用いた SOC での分析や、各種の関連するセキュリティデバイスやセキュリティ情報サービスからの情報収集が該当します。この状況判断を受けて、意思決定（Decide）を行う必要がありますが、セキュリティ運用の場合には CSIRT での、意思決定が該当します。さらに実行（Act）では FIREWALL へのルール反映等のセキュリティデバイスへの対応策適用作業が該当します。

SOAR では、上記 OODA ループでの Observe（観察）、Orient（状況判断）、Act（行動）を自動化でき、手動作業は Decide（意思決定）のみとすることができます。自動化により高速で正確な対応を実現することができます（図 2）。

SOAR によるメール対応の自動化例：30 分以上かかっていた対応時間が 40 秒に削減

PC でのデスクワークの自動化ツールとして導入が拡大している RPA（ロボティック・プロセス・オートメーション）は、定型的で反復の多い業務や、繁忙期に一時的に業務量が増える仕事、データ量が多くミスが発生しやすい業務などの効率化に向いているとされていますが、SOAR でも同様に、定形的で反復して実行する必要がある業務の効率化に大きな効果を発揮すると考えられます。SOAR では自動化に際し、運用作業プロセスを定義したシナリオ（プレイブック）が必要になります。Splunk Phantom のセキュリティオペレーションプラットフォームは、このシナリオを GUI により容易に作成することが可能なほか、220 種以上のセキュリティ製品と 1100 以上の API 連携が可能です。種々のセキュリティ製品の導入状況に合わせてプレイブックを作成することができ、多種のユーザーの環境に適合させることができます。また、豊富なユースケース・プレイブック例を掲載したポータルサイトも用意されており、すでに他社等で実績のあるプレイブックを即座に使用することができます。

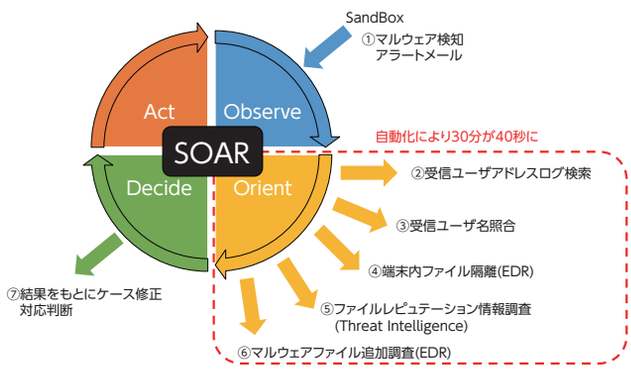

図 3　実際のオートメーション例

図 3 に Splunk Phantom のセキュリティオペレーションプラットフォームの適用事例を示します。この例では誤検知の多かった SandBox からのマルウェア検知アラートメールを受けて、端末へのマルウェアを含むメールの配信状況や端末でのマルウェア検知状況、外部の Threat Intelligence への照会等の追加調査を自動化した例となります。この事例では自動化により、30 分以上かかっていたマルウェア付きメール対応時間を 40 秒に短縮することに成功しています。このように SOAR の適用により、手動での作業を減らし工数を大幅に削減できるとともに、インシデントに高速に対応することが可能となります。

＜参考 URL＞
※わが国のサイバーセキュリティ人材の現状について
http://www.soumu.go.jp/main_content/000591470.pdf
https://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

NTT データ先端技術では SOAR の導入支援を行っています。SOAR 製品・サービスを用いたセキュリティ運用の設計・自動化環境構築・運用支援を提供可能です。セキュリティ運用の効率化・高度化にご興味があれば、ぜひご相談ください。

NTT データ先端技術
セキュリティ事業本部　セキュリティレジリエンス事業部
セキュリティオペレーション担当
【左側】担当課長　**水野 健生**
【右側】チーフエンジニア　**山本 航平**

お問い合わせ先
NTT データ先端技術株式会社　セキュリティレジリエンス事業部　セキュリティオペレーション担当
TEL：03-5259-5423　E-mail：sec-info@intellilink.co.jp　URL：https://www.intellilink.co.jp/