サイバー攻撃監視技術

松原　大樹　　森田　達也

サイバー攻撃の高度化・巧妙化により、企業や団体からの情報流出事故が続発し被害が拡大する中、企業はサイバーセキュリティー対策を整備する責任を求められている。しかし、企業や団体でセキュリティー対策を実施、運用することが難しい状況である。OKIは長年サイバーセキュリティーに対する対策、運用を実施してきた実績、ノウハウがある[1)]。OKIは実績、ノウハウに基づいてAI技術を取り入れた次世代セキュリティー対策の取組みを紹介する。

従来のサイバー攻撃への対策

サイバーセキュリティー対策はネットワークとサーバーやパソコンへ適切な対策を配置して、IT全体を監視し、問題の発生を素早く発見、原因を分析、迅速な対策を取らなければならない。

サイバーセキュリティー対策の適切な配置には、サイバー攻撃などによる不正侵入やウイルスのダウンロードを防止するための「入口対策」、サーバーやパソコンがウイルスに感染しても外部への情報流出を防止するための「出口対策」、お客様からお預かりした重要な情報の不正な持出しを防止するためのファイルやデータベースのアクセスログ監視などの「不正防止対策」を効果的、かつ多層に配置することが重要である。対策を多層に配置する必要性は、例えば「入口対策」が破られて未知のウイルスが社内ネットワークへ侵入し、パソコンが感染しても、「出口対策」でウイルスの不正サーバーとのアクセスを遮断して、更なるウイルスの引込みや情報の流出を防げるからである。

参考として、OKIが導入している代表的な入口対策、出口対策、不正防止対策の仕組みを以下に述べ、サイバーセキュリティー対策の概要を **図1**に示す。

（1）入口対策

- ファイアウォール：外部からの不正侵入とDoS攻撃（Denial of Service attack）を遮断する
- 侵入検知／防御：外部からの不正なアクセス（スキャン活動など）を検知し、外部からの不正な侵入を遮断する
- メールフィルター：マルウェアやSPAMなどの危険な添付ファイルを除去する
- 振舞い型検知：ウイルス対策ソフトでは検知できない未知のウイルスをサンドボックスで動かしてその挙動からウイルスを検知、遮断する

（2）出口対策

- ファイアウォール：社内からの不正な通信（ウイルスの通信など）を遮断する
- IDS（Intrusion Detection System）/IPS（Intrusion Prevention System）：社内からの不正なアクセス（ウイルスの通信など）を検知、遮断する
- Webフィルター：ウイルスなどによる社内からの不正なサーバーへのアクセスを遮断する

（3）不正防止対策

- ネットワーク接続制御：802.1x認証により、不正な端末のネットワーク接続を遮断する
- 統合認証：Active Directoryの認証により、なりすましを防止する
- DLP（Data Loss Prevention）：可搬記憶媒体の使用制限、重要情報の保護により、情報流出を防止する
- DB監視：DBに対する不正なアクセス（管理者権限の不正利用、未許可の操作など）を監視し、情報流出を防止する

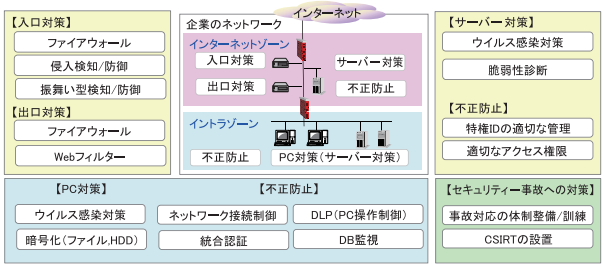

図1　サイバーセキュリティー概念図

OKIが提供するセキュリティーサービス

OKIは、社内で培ったノウハウを活かしたソリューションとして、セキュリティー運用監視サービスを提供する。

一般的にセキュリティーサービスには、**図2**に示すように「コンサルティング」「脆弱性診断」から「CSIRT（Computer Security Incident Response Team）構築・運営」「教育サービス」「SOC（Security Operation Center）アウトソーシング」などがあるが、OKIのサービスはSOCアウトソーシングに相当する。

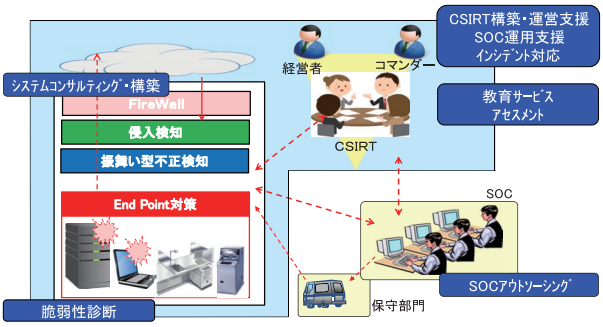

図2　セキュリティーサービス

主要なサービスの内容を、以下に示す。

- **コンサルティング**
  ガバナンス計画やセキュリティー強化のロードマップ策定支援、セキュリティー認証取得や体制構築/改善を支援する
- **脆弱性診断**
  Web診断、ネットワーク診断、モバイル・ワイヤレス環境診断により脆弱性の現状を分析する
- **CSIRT 構築・運営支援**
  CSIRTのセキュリティー専門組織の構想立案から運用設計までを支援する
- **教育サービス**
  情報セキュリティーの最新動向や事故事例・対策、社内ルールなど、ニーズに合わせて人材育成を支援する
- **SOC アウトソーシング**
  セキュリティー監視センタからのリモート監視により、異常トラフィックやログの解析業務に対応する。また、セキュリティー監視業務の高度化や改善支援を行う

効率的なサポートサイクルの実現

日々進化する脅威に対抗するには、情報セキュリティーのサポートサイクルをより効率的に回し続けることが求められる。その方法として、社内のシステムに散在するログを分析することで、情報セキュティーにおける改善点を見出すことが有効である。このログ分析をどのように実現するかが、効率的なサポートサイクルの実現につながるものと考えているが、そのためのソリューションとしてSIEM（Security Information and Event Management）と呼ばれる統合ログ管理システムがある。セキュリティー運用監視サービスでは、SIEMの導入を推奨している。

SIEMは、複数のセキュリティーデバイス、データベース、アプリケーションのログ、イベントを収集し一元管理することで、イベントログの可視化、横断的な相関分析、脅威の早期発見、対処を可能とする。SIEMの導入前後の導入効果を **図3**に示す。

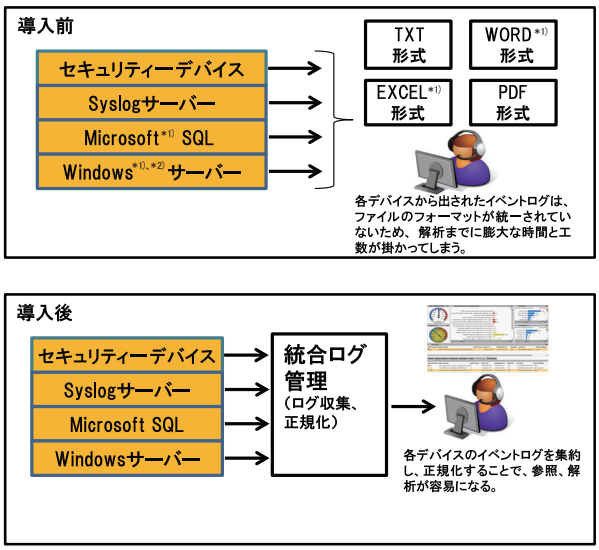

図3　SIEM の導入イメージ

SIEMの導入後のメリットを、以下に示す。

- **利便性の向上**
  複数デバイスのイベントログを集約して正規化することで、管理者が容易に参照、解析を実施することが可能となる
- **セキュリティー向上**
  一元管理しているイベントログを常時監視することで不正アクセス、異常な操作などのインシデントを早期発見、迅速に対処することが可能となる
- **運用工数、コスト削減**
  イベントログに対して常に可視化、相関分析を実施しているので、解析完了までの時間、工数を削減することが可能となる

次世代のセキュリティー対策

現在、1日で数万種類の新種ウイルスが発生している。新種ウイルスの発生量からパターンファイル更新が追い

＊1）Microsoft、WORD、EXCEL、Windowsは、米国Microsoft Corporationの米国及びその他の国における登録商標または商標です。　＊2）Windowsの正式名称は、Microsoft Windows Operating Systemです。

つかない状況になっている。パターンファイルは、侵入防止システム（IPS）のように過去に見つかった攻撃の特徴をシグネチャやブラックリストといったルールに落とし込んでいるものである。ユーザー端末上のファイルや、ネットワークのトラフィックをパターンファイルに照らし合わせて攻撃を見つけ出すのが一般的だった。しかし、新種ウイルスは、日々進化しパターンファイルが無い未知の攻撃などが多くなってきている。未知の攻撃に対して仮想環境でウイルスを動作させ検知するサンドボックスによる対策も出てきているが、近年、サンドボックスもすり抜けてくるタイプも存在している。従来のセキュリティー対策に限界がきている。そこで、注目を浴びているのがAI技術を用いた次世代のセキュリティー対策である。過去の攻撃やウイルスデータを機械学習法に入力することにより、ウイルスに共通する特徴を獲得する。大量のウイルスを機械学習させることで、検知の精度が高まり、未知の攻撃やウイルスを検知することが可能である。

OKI-CSIRTの対策

OKI-CSIRTは、サイバーキルチェーン[2]と呼ばれるサイバー攻撃の一連のステップの対策に取り組んでいる。サイバーキルチェーンは、**表1**に示すように7ステップに分類される。また、7つのステップに対してOKI-CSIRTが取り組んでいる対策の一例を示す。

プロキシサーバーのログは、サイバーキルチェーンの攻撃段階の、配送段階（マルウェアダウンロード）、遠隔操作段階(感染PCによる内部情報検索)を検知することが可能である。また、標的型ウイルスの約50%はプロキシ経由で外部通信するとの調査結果[3]があり、プロキシログの監視が最も重要である。

OKIの次世代のセキュリティー対策の取組み

現在、OKI-CSIRTでマルウェアや情報漏洩対策としてログ収集サーバーでログを統合し、セキュリティーログ分析している。しかし、膨大なセキュリティーログを人手で分析するのには限界があり、危険な攻撃ログを見落とす可能性がある。そこでOKIは、ログ収集サーバーのログ解析にAI技術を適用したサイバー攻撃監視支援システムの技術開発を行っている。**図4**にサイバー攻撃監視業務支援システムの概要を示す。

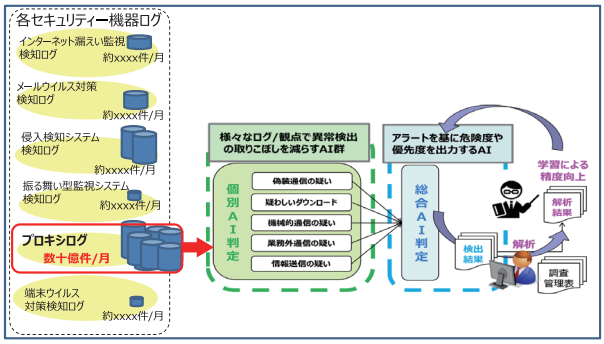

図4　サイバー攻撃監視業務支援システムの概要

図4に示すようにログ解析にAI技術を2段階適用したモデルを用いる。1段目の個別AI判定部で重要なログの見落としを減少させる異常検知AIを、2段目の統合AI判定部に1段目に異常と判定されたログに対し、1段目の判定結果を組み合わせて異常度を順位付けするAIを用いることによって、インシデントを早期かつ高精度に検出することが可能となる。

また社内では、サイバーキルチェーンの配送段階、遠隔操作段階を検知するために、それぞれを細分化した

表1　サイバーキルチェーンと OKI-CSIRT の一例対策

攻撃の段階	概要	OKI-CSIRTの一例対策
偵察	・インターネットなどから組織や人物を調査し、対象組織に関する情報を取得する	世の脆弱性情報をウォッチ
武器化	・攻撃コード(エクスプロイト)とマルウェアを作成する	
配送	・なりすましメール(マルウェアを添付)を送付する ・マルウェアを仕込んだWebサイトへアクセスさせ、ドライブバイダウンロードさせる。	入口対策(メールゲートウェイ、IDS、Firewall)
攻撃	・ユーザーにマルウェア添付ファイルを実行させる ・ユーザーをマルウェア設置サイトに誘導し、脆弱性を使用したエクスプロイトコードを実行させる	標的型攻撃メール訓練 セキュリティー教育の実施
インストール	・攻撃コードの実行された結果としてマルウェアがインストールされる。	端末のウイルス対策
遠隔操作	・マルウェアとC&Cサーバー*3)を通信させて、感染PC を遠隔操作する ・新たなマルウェアやツールのダウンロード等により、感染拡大や内部情報の探索を試みる	出入口対策
目的の実行	・探し出した内部情報を、加工(圧縮や暗号化等) した後、情報を持ち出す	Data Loss Preventionによる保護 パスワードの変更

・「ログを活用した高度サイバー攻撃の早期発見と分析」（JPCERT/CC　満永 拓邦、2015年11月17日）
（ https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf ）を加工して作成。
・「注意喚起」http://www.jpcert.or.jp/at/

*3) C&Cサーバーは、Command and Controlサーバーの略称です。

項目の観点で1段目の個別AI判断を実施し、異常検出を実施する。配送段階、遠隔操作の細分化項目の一例を **表 2**にまとめる。

表 2　個別 AI 判定における検知ロジックの例

検知ロジック名	ロジックの概要
偽装通信の疑い	マルウェアが、正しいホストの通信になりすまそうとしていることを検知
疑わしいダウンロード	通常起こりえないダウンロードを検知
機械的通信の疑い	人間が発生させることが困難である機械的な通信を検知
業務外通信の疑い	アクセス先と会社業務との関連性の薄さを検知
情報送信の疑い	データを外部に送信していることを検知

異常度の高いログから管理者が解析を実施し、その解析結果をAIにフィードバックを掛けることにより、異常検知の精度を向上させる。この仕組みにより、監視不要なログの除外、監視すべきログの蓄積、監視間隔の短縮と回数増加による精度の向上が可能となる。

このシステムは、プロキシサーバーに残るログからマルウェアの振る舞いや普段のログとの違いをAI技術によって学習して抽出し、不審な通信の見逃しや発見遅延を減らすことで、サイバー攻撃から社内情報資産を防御する。

AIによる異常判定可視化

OKIは、サイバー攻撃監視業務支援システムで、個別AI判定、総合AI判定の結果をGUI画面で表示するシステムも開発している（**図 5**）。GUI画面に表示することで、調査すべきログの優先順位が目視確認することができ、異常度の高いログから順に調査することが可能である。

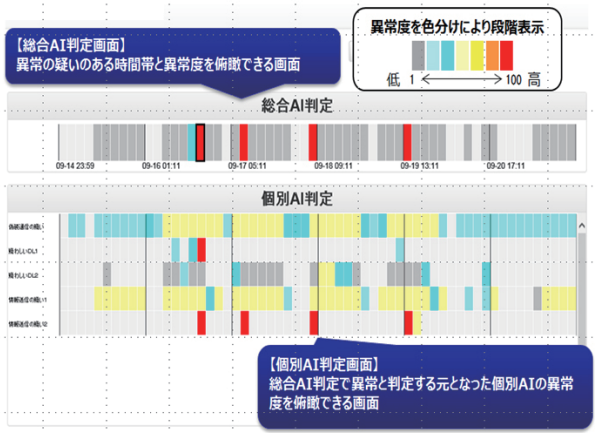

図 5　サイバー攻撃監視業務支援システムの GUI 画面

おわりに

本稿ではOKIのサイバーセキュリティーの社内事例とAI技術を使用したサイバー攻撃監視業務支援システムを紹介してきた。

OKIは社内で培ったノウハウとデータ解析及びAI技術を取り入れたサイバー攻撃監視業務支援システムを用いて社内で実績を積み、監視業務の高度化を目指し続ける。

■参考文献

1）原田融、濱田恒生：サイバーセキュリティーへの取組み、OKIテクニカルレビュー第228号、Vol.83 No.2、pp.34-37、2016年12月

2）JPCERT/CC、“ログを活用した高度サイバー攻撃の早期発見と分析”、2015年11月17日
https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf

3）独立行政法人情報処理推進機構、“標的型サイバー攻撃の実体と対策～攻撃者ツールのデモで見る脅威の身近さ～”、2012年12月7日
https://www.ipa.go.jp/files/000005383.pdf

●筆者紹介

松原大樹：Taiki Matsubara. 情報通信事業本部 IoTプラットフォーム事業部 EXaaSサービス部

森田達也：Tatsuya Morita. 情報・技術本部 情報企画部