AI（人工知能）を活用した未知のサイバー攻撃対策

西野 真一郎　喜田 弘司　木津 由也　八木 敬　榮 純明

要 旨

サイバー攻撃は高度化・巧妙化が進み、既存のセキュリティ対策では検知も難しく、検知できてもその結果の分析には高度なスキルと膨大な工数が必要という課題があります。この課題に対し、NECはAI技術を応用し、従来不可能だった未知のサイバー攻撃への対策サービスを開発しました。本サービスは攻撃プロセス全体（初期のマルウェア侵入からシステム内における感染拡大、データ搾取などの目的遂行まで）における未知の攻撃の「検知」と、更にその後の「分析」による原因究明・被害範囲特定の効率化を実現します。本稿では、サイバーセキュリティの現状と課題、基盤のAI技術、主な機能と特長、課題検証結果を紹介します。

KeyWords　サイバーセキュリティ／サイバー攻撃／未知のマルウェア／AI／ラテラルムーブメント／異常検知／分析／SOC／CSIRT／平常状態／エンドポイント

1. はじめに

昨今、サイバー攻撃は高度化・標的型化が進み、そこで使われるマルウェアは既存マルウェアを改良した亜種や、ターゲットごとにカスタムメイドされたもの、いわゆる未知のマルウェアが増えています。

この結果、情報セキュリティ対策として広く普及しているパターンマッチング型アンチウイルスソフトウェアはほぼ無力化されています。パターンマッチングは既知のマルウェアを検知する技術であり、未知のマルウェアを想定していないためです。NEC社内で行ったテストでは、既知のマルウェアの検体を亜種に変化させるだけでパターンマッチング型アンチウイルスソフトウェアの検知率は85%も低下しました。

未知のマルウェアを検知する技術として、サンドボックスがあります。マルウェアと疑われるプログラムを、本番システムから隔離した仮想環境で実行させて、その振る舞いからマルウェアか否かを判断する技術です。しかし、マルウェア製作者もサンドボックスを回避する仕組みを実装して対抗してきています。例えば、仮想環境であることを検知した場合は、マルウェアが動作しないようにすることなどです。

以上のように、マルウェアを知ることによって検知率を上げるという取り組みはマルウェア製作者側との“いたちごっこ”であり、常に100%検知し続けることは不可能です。

本稿ではこの状況を踏まえ、マルウェアを知ることによって検知するのではなく、視点を変え、新たな方法で攻撃を検知し、その後の分析も効率化するサービスを紹介します。

2. 課題

既存のセキュリティ対策をすり抜けたマルウェアは、エンドポイント（PCやサーバ）で活動を開始します。攻撃者はいきなり最終目標（機密情報が保管されているデータベースなど）にマルウェアを送り込むわけではなく、ラテラルムーブメント（Lateral Movement、水平移動、**図1**）と呼ばれる感染拡大活動を経て、侵入口から最終目標へ一歩一歩近づき、目的遂行（重要情報をデータベースから盗み出しインターネットに送信）に至ります。つまり、マルウェアに侵入されても被害が出る前にいち早く検知し、適切な処置を行うことが求められているのです。

NECの独自調査によると、未知のマルウェアのうち約3割はサンドボックスなどをすり抜けてしまうため、人手で対処を行っているというデータもあります。この状況から、

以下の２つの課題が浮かび上がります。

（1）攻撃の検知率向上

検知率を低下させる原因には前述したとおり未知のウイルスによる攻撃に加え、OS標準ツール（Windows PowerShellなど）を用いた攻撃があります。標準ツールはマルウェアではないため、アンチウイルスソフトウェアでは検知されません。しかし、攻撃に使われた場合、その使われ方は通常とは異なるため、この使われ方の異常性から攻撃を検知するアプローチが必要です。特に、複数のエンドポイントをまたいだ攻撃（ラテラルムーブメント）を検知できることが求められます。

（2）人手による対処の効率化

検知システムをすり抜けた攻撃に対しては、セキュリティの専門家が人手で対処する必要があります。

専門家による対処の代表例に、SOC(Security Operation Center)やCSIRT(Computer Security Incident Response Team)におけるセキュリティインシデントの調査が挙げられます。この業務には大量のログと格闘するなど、サイバーセキュリティに関する高度なスキルと膨大な工数が必要ですが、ハイレベルなセキュリティ人材は慢性的に不足しており、短期間での育成も困難なため、対処作業の効率化が大きな課題となっています。

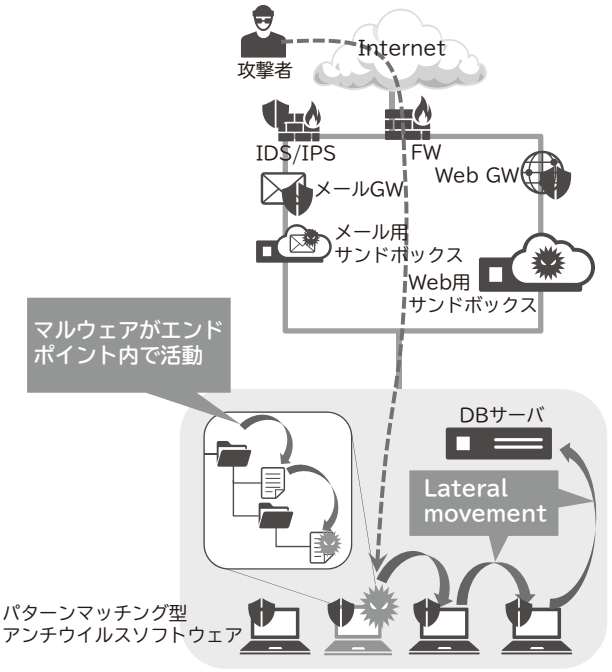


図１　ラテラルムーブメント

3. ASIの機能

本章では、AIを活用して未知の攻撃を検知し、原因や被害範囲の分析を効率化する「自己学習型システム異常検知技術」（Automated Security Intelligence：以下、ASI）[1) 2)]を紹介します。

ASIは、２つの技術的特長を持っています（**図２**）。

（1）AIを活用した自システムのリアルタイム異常検知

まず、PCやサーバなどシステム全体の動作状態（プログラム起動、ファイルアクセス、ネットワークアクセスなど）に関する詳細なデータをエンドポイントから収集、AIで分析し、システムの平常状態を把握します。次にAIは、現在のシステムの状態と平常状態とをリアルタイムに比較し、平常状態から外れた場合を「異常」と判定します。

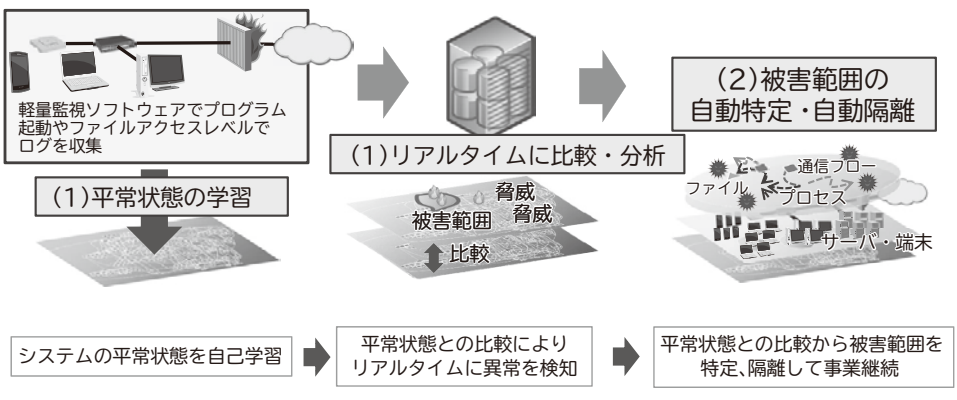


図２　ASIの技術的特長

(2)分析の効率化と対処の自動化

ASIはシステム全体の動きを詳細に把握しているため、検知した異常に関連するシステムの一連の動作を時系列で追跡・表示できます。これにより、原因究明・被害範囲特定のための分析作業を効率化できます。

次に、それらの特長を引き出す、システムの動作の「平常状態」について、例を挙げて説明します。

図3は、ある企業のネットワークシステムと、そのシステムにおける平常状態のイメージです。このシステムは以下の3つのサブネットワークから構成されています。

1）共用サブネットワーク：

Webプロキシサーバなど、企業内で共通的に使用されるサーバが設置

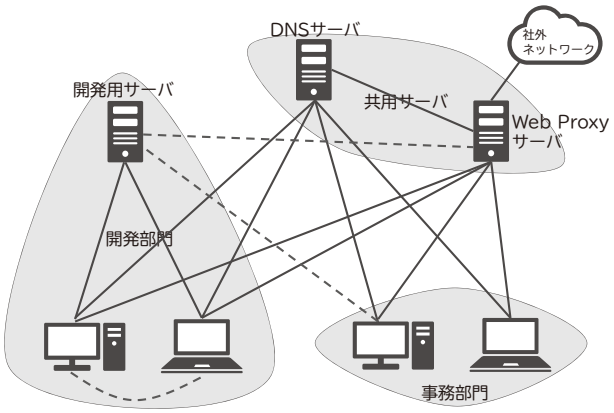


図3　ASIにおける平常状態のイメージ

2）開発部門サブネットワーク：

開発用のサーバやPCが設置され、開発部門が使用

3）事務部門サブネットワーク：

事務部門のPCが設置

通常、共用サーバは企業内のすべてのPCからアクセスされ、開発用サーバは開発部門のPCのみからアクセスされます。逆に、事務部門のPCが開発用サーバにアクセスすることは一般的には起こりません。このようなマシン間の関係を平常状態と呼びます（図3中の実線）。

平常状態では行われないネットワークアクセスを検知すると、ASIは「異常」と判断して管理者へ報告します。例えば、事務部門のPCから開発用サーバへのアクセスが行われた場合や、開発部門内のPC同士が直接通信を行った場合、または通常は社外ネットワークへの通信を行わない開発用サーバがWebプロキシサーバへの通信を行った場合などです（図3中の点線）。

部門内端末同士の直接の接続はラテラルムーブメントでよく見られ、また、開発用サーバからWebプロキシサーバへの接続はマルウェアの攻撃プロセスにおける目的遂行フェーズで行われます。

特にラテラルムーブメントの検知は重要です。従来のサイバー攻撃対策システムはマルウェアの初期潜入と目的遂行をとらえるものが主であり、いったん入口を突破されると攻撃の目的遂行まで検知が非常に困難になってしまうという問題があるからです。ASIは初期潜入と目的遂行の間、すなわちラテラルムーブメントでも検知できるため、

※本サービスは開発中のため、正式版は異なる場合があります。

図4　ASIによる異常検知の例

攻撃検知のチャンスをより増やせます。

図4に、ASIにおける異常検知の画面例を示します。右側中央の円状のグラフが監視対象のネットワークを示しており、実線がPCやサーバ間の平常のネットワーク接続、太い実線が平常でない（すなわち異常と見なした）ネットワーク接続を示しています。

本章では、PC・サーバ間のネットワーク通信を例として説明しましたが、ASIはエンドポイントのプログラムの起動やファイルアクセスなども平常状態を学習しているため、ネットワーク通信がないPC内部でも異常を検知できます。

また、異常の検知だけでなく、マルウェアの感染源や被害範囲の特定、対策の実施までを効率化することがASIの重要な機能と考え、サービス化・製品化を進めています。ASIをサービスとして提供することにより、自社内にセキュリティ要員が十分にいない企業でもASIを利用できます。

4. ASIによる課題の解決

第2章で挙げた課題に対して、ASIを適用した際の検証結果を紹介します。

4.1 課題1　攻撃の検知率向上

（1）未知のマルウェア

パターンマッチング型のアンチウイルスソフトウェア製品では検知できなかったマルウェアを対象に、他社のAIセキュリティ製品とASIで検知実験を実施しました。他社のAIセキュリティ製品の検知率が0%に対し、ASIは約80%であり、検知精度の高さが実証できました。

（2）OS標準ツールを用いた攻撃

NECグループ内の実オフィス環境で標的型攻撃を模した実験を行いました。データ窃取まで行うリアルな攻撃シナリオに基づき、OS標準コマンド（Windows PowerShellなど）を使った疑似マルウェアでサーバ約10台・PC約100台を攻撃したところ、攻撃の目的が達成される前にASIで100%検知できました。ASIは、OS標準ツールを用いた攻撃にも有効であることが実証できました。

4.2 課題2　人手による対処の効率化

人手による対処が必要な作業は「異常発生時の原因及び影響範囲の分析」と「誤検知への対応」の大きく2つあります。NECグループ内の実オフィス環境で実験を行ったところ、分析作業は1件当たり数日かかっていたものがASI導入により平均1.5時間に短縮（最大でも5時間程度）され、誤検知は毎日一端末当たり数十件発生していたのがASI導入により平均0.27件/日・端末にまで減少しました。この2つの効果が重なることで、人手での対処作業を大幅に効率化できます。

このように、ASIは従来のパターンマッチングやサンドボックスと異なり、実環境のエンドポイントを詳細に監視、AIで分析することにより未知の攻撃を検知し、その後の分析も効率化できるのです。

他にも、複数のエンドポイントを統合的に監視しているためマシン間にまたがるマルウェアの感染拡大活動（ラテラルムーブメント）も検知できること、検知から分析までの機能をオールインワンで、しかもサービスとして提供できることもASIの特長です。また、マルウェアだけでなく、内部不正対策にも応用できます。

本稿では未知の攻撃の検知・分析を担うASIを紹介しましたが、NECは今後、ASIを他の製品・サービス群と連携させ、SOC/CSIRTの業務プロセス全体をカバーするソリューションを提供する構想です（事前対策・監視・検知・分析・対処）。

参考文献

1) NECプレスリリース：NEC、AI（人工知能）を活用し未知のサイバー攻撃を自動検知する「自己学習型システム異常検知技術」を開発 ～ 未知のサイバー攻撃による被害範囲の特定時間を1/10以下に低減 ～, 2015.12
http://jpn.nec.com/press/201512/20151210_01.html
2) 多賀戸裕樹ほか：未知のサイバー攻撃を自動検知する自己学習型システム異常検知技術（ASI），NEC技報，Vol.69 No.1, 2016.9
http://jpn.nec.com/techrep/journal/g16/n01/160111.html

執筆者プロフィール

西野 真一郎
スマートネットワーク事業部
主任

喜田 弘司
スマートネットワーク事業部
マネージャー

木津 由也
スマートネットワーク事業部
主任

八木 敬
スマートネットワーク事業部
主任

榮 純明
セキュリティ研究所
プリンシパルクリエーター

関連URL

NEC Cyber Security Solutions
http://jpn.nec.com/cybersecurity/

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

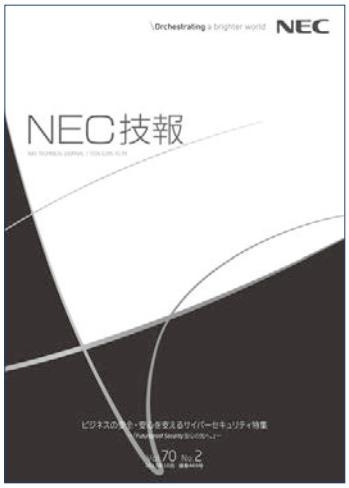
◇ 特集論文

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