企業を狙う標的型攻撃の動向とサイバーセキュリティ対策ソリューション

石原 健司　小林 洋平　楠田 徹　小嶋 章裕

要 旨

2011年ごろから日本国内でその名が知られるようになった「標的型攻撃」は、現在も、以前にも増して巧妙化・高度化した形で行われており、企業のみならず、官公庁、大学、公的機関など、あらゆる業種で被害が報告されています。本稿では、標的型攻撃の代表的な手法である「標的型攻撃メール」による被害を中心に、攻撃の概要と対策ポイントを紹介します。

KeyWords
サイバー攻撃／サイバーセキュリティ／標的型攻撃／情報漏えい／メール／マルウェア／マイナンバー／多層防御／サンドボックス／SOC／SIEM／フォレンジック

1. はじめに

ネットワークやインターネットを通じて、企業のITインフラを脅かすサイバー攻撃は、年々増加傾向にあり、特に最近では、特定の業種や企業を狙って、執拗に攻撃を行う「標的型攻撃」による被害が拡大しています。

標的型攻撃は、事前に用意周到な計画が立てられ、巧妙かつ洗練された手法で行われるため、従来型のセキュリティ対策で防ぐことが困難になっています。そこで、有効な対策を多面的に行い、随時、対応状況をチェックしながら、改善していく運用が必要になります。

本稿では、昨今の標的型攻撃の手法を、実例を挙げて紹介するとともに、これからの企業に求められる対策について説明します。

2. 標的型攻撃の概要

標的型攻撃は、多くの場合、マルウェアと呼ばれる、コンピュータ上で不正な動作をするプログラムやコードを、ユーザーのPC上で実行させることから始まります。また、そのマルウェアをPCに送り込み、実行させる手段としては、「標的型攻撃メール」と呼ばれる電子メールを送付する形が一般的になっています。

標的型攻撃メールは、送信元のメールアドレスやタイトル、本文などを、あたかもユーザーの日常業務や、社内外の重要手続に関連するかのように見せかけたものが多く、ユーザーが疑問を抱かずにメールを開き、マルウェアに感染することを狙って送信されます。

マルウェアへの感染は、マルウェアを仕込んだ添付ファイルを開かせる形が一般的ですが、最近では、メール本文に、実在するサイトを装ったURLを記載し、そのURLにアクセスすることで感染させる手法も増えています。

ユーザーのPCをマルウェアに感染させた後は、そのPCを踏み台にして、社内のサーバや他ユーザーのPCにアクセスを行い、本来の目的である、重要情報の持ち出しや、金銭の搾取、システム破壊などを行います。

また、目的を果たした後は、ログの削除や改ざんにより攻撃の痕跡を隠蔽する工作を行い、一連の攻撃を終了します。

このように、ユーザーにとって、あたかも日常の業務のなかの、ごく普通のPC操作が、重要情報や金銭の搾取、システム破壊につながり、また、ファイアウォールやウイルス対策ソフトなど、従来型のセキュリティ対策では対応しきれないところが、標的型攻撃の大きな特徴といえます。

3. 標的型攻撃の対象

日本国内で標的型攻撃メールが確認された2005年から約10年が経過し、そのターゲットや目的は刻々と変わっています。現在では、機密情報や個人情報を大量に保有する政府/公共サービス機関、また、価値の高い知的財産を多く保有する製造業が主要なターゲットとされ、その目的は主に下記に分類されます。

(1) 個人情報の搾取

昨今の情報漏えい事件が示すように、氏名や住所、電話番号などの個人情報は、それ自体が金銭的な価値を有しており、搾取した情報を名簿業者に売却する、あるいは、入手した個人情報リストに記載された各個人に対し、新たな詐欺を画策することなどを目的として行われます。

日本国内では、マイナンバー制度の導入により、今後更なる個人情報漏えい事件が発生することが懸念されています。

(2) 機密情報の搾取

製品の企画・開発情報や特許情報、機密情報を搾取することにより、競合他社への情報の売却、特許の先願、諜報活動への活動や、建物に関する情報を元にしたテロの画策など、幅広い目的を持って行われます。

(3) 金銭の搾取

ここ数年、インターネットバンキングシステムへの不正アクセス、不正操作により、金銭を搾取するケースが多く報告されています。また、米国を中心に、POSへの標的型攻撃により、POS上で扱われるクレジットカードなどの番号を搾取し、その番号を悪用して金銭や物品をだまし取る事件も増加しており、日本国内への拡散が懸念されています。

(4) 制御システムへの不正侵入、破壊

今日、工場や各種エネルギー・プラントで利用される制御システムでも、オープン化やネットワーク接続が進んでおり、同時に、悪意を持った攻撃の対象になるリスクが高まっているといえます。

制御システムへの標的型攻撃は、工場内のシステム破壊により、一企業の生産活動に壊滅的な被害を与えるほか、エネルギーや化学プラントのシステム破壊は、ライフラインの停止や、場合によっては人命を脅かす脅威になり得ます。

4. 標的型攻撃対策のトレンド

標的型攻撃は日を追うごとに巧妙化し、従来の対策では防ぐことが難しくなっているだけでなく、標的型攻撃を目的とした防御策であっても、単一の対策では防ぎきれないケースが増えています。このため、最近では、インターネット接続のファイアウォールや、内部ネットワーク、サーバ、PCなど、各ポイントで個々の対策を行い、全体として標的型攻撃からITインフラを守る「多層防御」の考え方が推奨されています。

また、対策ソリューション・製品の導入だけでなく、攻撃を早期に検知し、被害を最小限に抑えるための運用業務や、緊急時の対応手順・体制の整備、平常時からのユーザー教育など、システムと運用、体制、教育・訓練の各メニューが相互に連携し、解決に導ける仕組み作りが必要です。

5. 多層防御の実現例

多層防御を実現する対策システム群の例を、図に示します。標的型攻撃におけるデータの流れに沿って、ポイントごとに対策ソリューションを配置することにより、多層防御を実現します。

(1) 入口対策

社内ネットワークへの入口で、社外からの標的型攻撃を検知することは、水際で被害を最小限にとどめるという意味で、非常に重要であり、一般的に「入口対策」と呼ばれています。

従来は、インターネットなど、社外接続を行うポイントにファイアウォール、アンチウイルス、アンチスパムなどを配置し、不正な通信やウイルス・スパムメールから社内システムを防御する形が一般的でした。しかし昨今では、前述のとおり、通常のメールを装った標的型攻撃メールが攻撃の大半を占めており、装置が持つ、攻撃やウイルスパターンとの比較で検知を行う従来型の製品では、標的型攻撃を防ぐことは困難になっています。

現在では、サンドボックスと呼ばれる装置内の仮想空間で、メールに添付されたファイルやメール本文に記載されたURLへのアクセスを実行し、その振る舞いを調べる形で標的型攻撃を検知する製品が提供されており、従来の攻撃やウイルスのパターンにはない、未知のマルウェアへの対策を強化することが可能です。

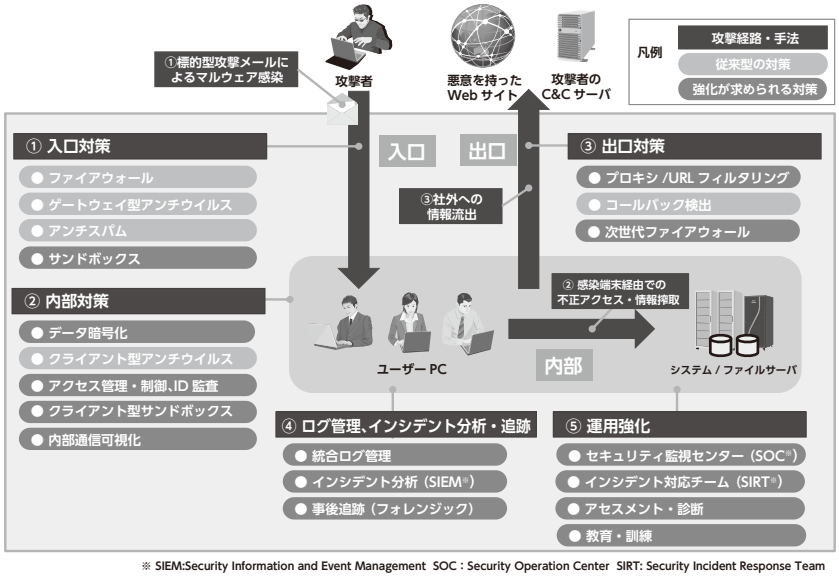


図　標的型攻撃における多層防御モデル例

(2) 内部対策

標的型攻撃は巧妙化が進み、最近では、入口対策を施していても、被害を受けたというケースが報告されています。

多層防御のポイントの2つ目として、内部のPCやネットワーク上での対策が挙げられます。

入口対策をすり抜けた標的型攻撃メールは、各ユーザーのPCに到達し、ユーザーが添付ファイルを開く、あるいは本文に記載されたURLにアクセスすることで、マルウェア感染が起こります。

攻撃者は、感染したPCを踏み台にして、社内の諸システムやファイルサーバへ不正にログインし、情報の搾取やシステム破壊を行うため、いかにPCのマルウェア感染を防ぎ、かつ、感染したPCの不正なアクセスや通信を検知できるかが重要になります。

これらの対策を一般的に「内部対策」と呼びます。具体的には、PC上でメモリやプロセスなどを監視することで、マルウェアがPCに感染しようとする挙動の停止と、PCのマルウェア感染を想定したうえで、PCから諸システムやサーバへの不正なログイン要求や出口まで到達しない不正な通信を検知するための、アクセス管理、ID監査、内部通信可視化などの対策も有効です。

また、PCやファイルサーバに格納されたデータを暗号化しておくことで、万一社外にデータが流出した場合でも、中身を閲覧することができず、社外への情報漏えいを防止することが可能です。

(3) 出口対策

標的型攻撃の大きな目的である、情報の搾取は、マルウェアに感染したPCから、外部とのWeb通信を装った形で行われることが多く、この外部への通信を検知することで、情報の流出を防止することが可能です。

具体的には、URLフィルタリングによる、悪意を持ったWebサイトへのアクセスの遮断、また、通信の振る舞いや、アプリケーション種別により、フィルタリングを行うことにより、外部との不正通信を遮断することなどが挙げられます。

(4) ログ管理、インシデント分析・追跡

(1) ～ (3) に挙げた諸対策により、標的型攻撃の被害を受けるリスクを大幅に低減することは可能ですが、攻撃が多様化、高度化する現在では、100%安心な対策はありません。

リスクを限りなく0に近づけるには、標的型攻撃への諸対策に加え、平常時からログを管理し、早期に異常の兆候を把握できることが必要不可欠です。

標的型攻撃対策製品の多くは、装置自身でシステムログ、アクセスログ、操作ログなどを記録する機能を持ち、個々のログから異常状態を検知することも可能です。しかし、昨今では複数の装置のログを収集し、統

合的に管理を行う「統合ログ管理」や、収集したログからインシデントの予兆検知や事故発生後の分析調査を可能にする「SIEM（Security Information and Event Management）」、インシデントの全容究明を行う「フォレンジック」の導入を検討する企業も増加しています。

(5) 運用強化

巧妙化かつ高度化する標的型攻撃への対策レベルを高めるには、前述の各種対策製品の機能と特長を理解し、的確な運用が行えること、また製品が発行するアラートやログの意味を理解し、万一、攻撃被害が確認された場合は早急に対応方針を決め、実行に移せることが重要です。

このように、迅速かつ的確に運用を行うには、最新の脆弱性や攻撃情報などの知識と、対策システムの運用ノウハウが求められ、24時間365日でセキュリティ監視を行い、有事には即座に対処する、セキュリティ監視センター（Security Operation Center：SOC）や、インシデント発生時に専門的な調査を行う、インシデント対応チーム（Security Incident Response Team：SIRT）を自社組織、またはアウトソーシングにより設置するケースがあります。

また、対策レベルを維持するには、定期的な自己評価と見直し改善も必要であり、セキュリティアセスメントや診断による対応状況と改善点の把握や、エンドユーザーに対する教育・訓練による、セキュリティ意識高揚の取り組みも推奨されています。

6. まとめ

標的型攻撃の対策は非常に幅広く、かつ高い経験とノウハウが必要であり、一朝一夕に万全な体制や対策が構築できるわけではありません。

本稿で紹介した、対策ポイントを段階的に導入しつつ、かつ運用ノウハウを蓄積していくことにより、対策レベルを高めていくことが、企業の標的型攻撃対策強化への近道であると考えます。

参考文献

1）情報処理推進機構（IPA）：標的型攻撃メール＜危険回避＞対策のしおり，2012年1月
2）情報処理推進機構（IPA）：「高度標的型攻撃」対策に向けたシステム設計ガイド，2014年9月

執筆者プロフィール

石原 健司
グローバルプロダクト・サービス本部
マネージャー

小林 洋平
グローバルプロダクト・サービス本部
主任

楠田 徹
グローバルプロダクト・サービス本部
主任

小嶋 章裕
グローバルプロダクト・サービス本部
主任

NEC 技報のご案内

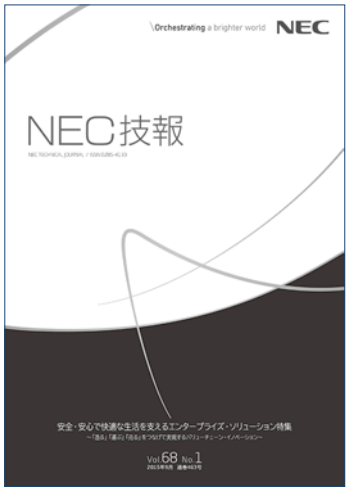
NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.68 No.1　安全・安心で快適な生活を支えるエンタープライズ・ソリューション特集
～「造る」「運ぶ」「売る」をつなげて実現するバリューチェーン・イノベーション～

安全・安心で快適な生活を支えるエンタープライズ・ソリューション特集によせて
NECが考えるバリューチェーン・イノベーション
～バリューチェーン・イノベーションが実現する安全・安心で快適な生活～



Vol.68 No.1
(2015年9月)

特集TOP

◇ 特集論文

バリューチェーン・イノベーション「造る」
製造業を元気に！ NECものづくり共創プログラム
IoTを活用した次世代ものづくり ～NEC Industrial IoT～
インダストリー4.0と自動車業界におけるものづくり改革の最新動向

バリューチェーン・イノベーション「運ぶ」
アジア新興国における物流可視化クラウドサービス

バリューチェーン・イノベーション「売る」
小売業の方向性とICTの貢献 ～Consumer-Centric Retailingの追求～
サービスの高度化を支える電子決済
オムニチャネル時代のポイントとECソリューション「NeoSarf/DM」
「おもてなし」をグローバルに展開するNEC Smart Hospitality Solutions

豊かな生活/豊かな暮らし
公共交通ICカードソリューションの取り組みと今後の展望
スマートモビリティへの取り組み
EV充電事業の商用化を支えるEV充電インフラシステム
IoTを活用した端末・サービス基盤と業際ビジネス実現に向けた取り組み

エンタープライズ領域を支える先進のICT/SIへの取り組み
新たな価値を創出するビッグデータ活用
補修用部品の在庫最適化に貢献する需要予測ソリューション
異種混合学習技術を活用した日配品需要予測ソリューション
プラント故障予兆検知サービスのグローバル展開
食品メーカーの商品需要予測へのビッグデータ技術活用
事業貢献を実現するマルチクラウド活用法と移行技術
SDNを活用したグループ統合ネットワーク ～東洋製罐グループホールディングス株式会社様～
企業を狙う標的型攻撃の動向とサイバーセキュリティ対策ソリューション
深刻化するサイバー攻撃対策を「確実な実践」に導くセキュリティアセスメント
今後のIoT時代を見据えた制御システムのセキュリティ
画像識別・認識技術を活用したVCAソリューションへの取り組み
短納期・低コストを実現する現場SEから生まれたWeb開発フレームワーク
IoT時代に新たな社会価値創造を実現する組込みシステムソリューション
NECにおけるSAPプロジェクトの先進的な取り組み