サイバーレスキュー隊（J-CRAT） 活動状況
[2017 年度下半期]

2018 年 7 月 11 日

1　活動結果

2017 年 10 月～2018 年 3 月に、「標的型サイバー攻撃特別相談窓口」に対して寄せられた相談件数と、緊急を要する事案に対してレスキュー支援を行った件数とオンサイトでの支援件数を、表1に示す。

表 1 J-CRAT 支援件数の推移

	2015 年度	2016 年度	2017 年度 (上半期)	2017 年度 (下半期)
相談件数	537	519	254	158
レスキュー支援数	160	123	85	59
オンサイト支援数	39	17	17	10

※1 つの事案に対して複数回のオンサイト対応を要した場合も、1件として集計

「標的型サイバー攻撃特別相談窓口」に対して寄せられた**相談件数**は **158 件**であった。このうち、**レスキュー支援**へ移行したものは **59 件**、うち**オンサイト支援**を行った事案数は **10 件**であった。

全体的な傾向として、Windows10 への移行や端末・サーバのリプレースが進んでいるためか、感染が長期化している潜伏被害の件数は減少傾向に見える一方で、政治・経済・安全保障・国際関係・科学技術・学術といった幅広い分野にわたり、新たな橋頭堡としてのバックドア設置を狙った攻撃が増えている印象がある。

また、メールシステムがインターネット上のクラウドサービスへの移行に乗じて、認証情報を詐取するフィッシングメール攻撃の手法が、単一個人のみへ送付されるといった標的型メール攻撃が複数行われていることが確認されている。

2　2017 年度下半期の活動を通じてみられた特徴的な事項

サイバーレスキュー隊（J-CRAT）では、ナショナルインタレストに関わるサイバーエスピオナージ（サイバー諜報活動）に対して相談やレスキュー活動を行っている。今期の活動を通して見られた特徴的な事項を以下に記す。

(1) 政治・経済・安全保障に関わる組織に対する情報窃取が継続

2017 年上半期から引き続き、特定の攻撃グループによると思われる標的型メール攻撃が、国際政治・経済・安全保障に関わる組織に対して断続的に見られた。

攻撃に用いられたウイルスとしては、2016 年春頃より RedLeaves と呼ばれる RAT(遠隔操作ツール)、及び 2017 年春頃より ANEL と呼ばれる RAT が確認されている。

ANEL が用いられた事例では、標的型メールと添付ファイルの内容は標的にされた組織毎にカスタマイズされており、標的組織が Web で公表している直近のイベントなどが題材に使用されていた。

また、攻撃者は標的の端末へ ANEL を感染させる前段として、オフィスソフトの脆弱性や仕様を介し

て Koadic と呼ばれるオープンソースのペネトレーションテストツールを攻撃ツールとして送り込んでいた。Koadic はファイルレスで動作するためアンチウイルスソフトでの検知率が低いという特徴を持つ。標的が感染すると、攻撃者は直ちに Koadic を用いて感染端末のシステム情報を読み取ったうえで、サイバーエスピオナージ対象であることを確認したのちに ANEL を設置するという素早さと慎重を感じさせる挙動が見られた。

このようなサイバーエスピオナージの事例は当隊の発足以前（2005 年ごろ）から途切れることなく実行され続けており、標的型メール攻撃はインテリジェンス活動の確立した手段として用いられていることを知るべきである。

(2) 先端科学技術を狙った攻撃

先端科学技術を扱う学術組織が 2017 年度上半期から数ヶ月間の長期にわたり情報窃取の被害を受けていたことが、外部機関からの情報提供を受けて発覚した。ウイルスの感染被害は複数のサーバに広がっており、攻撃者が遠隔操作で組織内の端末を次々と感染させていった痕跡が発見された。攻撃活動は数ヶ月の間にいくつかのピークが存在し、各時期（フェーズ）において、橋頭堡確立、横移動、情報識別といった特徴をうかがわせる痕跡がみつかった。これらの状況把握は、事案対処で忙しい中、具体的な暫定対策に加えて根気強い「状況把握のための活動痕跡の収集」を被害組織で実施していただいたおかげである。

(3) 日本以外の国で活動するとされる攻撃者による、日本への攻撃を観測

2017 年末頃に、これまで主に台湾の政府組織を標的としてきたウイルス（Taidoor）が国内の企業で発見され、2018 年以降も活動の痕跡が見られている。事例では、一般に利用される共有 web サービスやブログがウイルスの配信先に用いられており、セキュリティ製品による不審通信先としての検知を回避する狙いが見られた。

さらに 2018 年初頭より、上述のものとは別種の、こちらもこれまで主に台湾の政府組織を標的としてきたウイルス（PLEAD）が添付された標的型メールが国内の重要人物に送付された事例が見られている。

(4) ウイルスに感染したが情報窃取を免れた事例

経済に関係する組織に標的型メールが送付された事例にて、メール受信者が添付ファイルを開いてしまいウイルスに感染した。攻撃者は感染の直後に感染端末へ遠隔操作で侵入し別種のウイルスを設置・実行したが、既知の不審通信であったためネットワークのゲートウェイ装置により通信がブロックされた。その後、攻撃者が様々なウイルスの設置を試みている段階で感染端末は特定され、ネットワークから切り離された。

本事例では、ゲートウェイ装置のシグネチャが最新化されており、かつアラートの監視体制が整っていたことで、ウイルス感染を許したものの次の攻撃段階に進まなかったケースと言える。

(5) 不正アクセスの被害を受けた組織に残る攻撃痕跡の類似性

2017 年度に発生した学術関係組織への不正アクセス事例の調査を複数進めていくなかで、攻撃痕跡にいくつかの類似点が見られている。具体例を以下に記載する。

・不正ツールが設置されやすいフォルダがある （C:¥Temp や C:¥Intel が使われやすい）
・バックドアは複数仕掛けられる （サービス登録やスタートアップへの設置）
・侵入後に感染を広める手法は複数用いられる （リモートデスクトップ、PsExec）
・感染を広めるための中継サーバが作られる

なお、当隊では標的型攻撃インシデント発生時の初動対応の手引きを 2018 年 3 月に公開している[1]。上記の攻撃痕跡を含めた調査観点を載せているため参考にしていただきたい。

3　活動を通じての提言

2017 年度下半期の活動を通じて見られた標的型サイバー攻撃の対応事例を元に、以下の通り提言する。

(1) 攻撃被害の記録と発見を前提とした対策の必要性

メールに不審なファイルを添付する、メールに不審なリンク先を記載するなど、標的型攻撃の手口自体は大きく変化していないものの、攻撃者は 2 項(1)(2)(5)で紹介したような感染率を高めるための手法を組み合わせるため、メールフィルタやアンチウイルスソフトといった入口対策で完全に防御することは困難だと言える。

従来からの提言の繰り返しとなるが、ウイルスの感染はありえることを前提とし、被害の拡大防止を目的として、従前からの内部対策や出口対策に加え、特に自組織のシステム構成の把握、ファイアウォールやプロキシサーバログの適切な取得といった技術面の対策、不審メール受信時の対応手順、インシデント発生時の組織的な対応体制の確立など運用面の危機管理対策を行うことが望ましい。

2 項(4)で紹介した事例のように、技術と運用両面の対策によりインシデントの発生から対応までの時間を極力短縮することで被害の拡大を防げるケースもある。

(2) 情報共有活動への積極的な参加

J-CRAT では、標的型攻撃に関する相談や情報提供を元に攻撃の連鎖をたどるとともに、提供された情報、抽出した攻撃の特徴を関連する組織と共有することで被害の早期検知と拡大防止に努めている。

当隊の活動は攻撃情報を得た組織からの相談や情報提供に支えられており、日々変化する標的型攻撃を追うためには情報共有の輪を拡大することが必要不可欠であると考える。

社会全体のサイバー攻撃対応能力の向上のため、各組織は、IPA や警察、関連団体などからの注意喚起情報を自組織のサイバーセキュリティ対策に活かすとともに、インシデント発生時、そしてインシデント発生後の情報共有に、積極的に参加することをお願いしたい [2] [3]。

わが国のサイバードメインアウェアネス(CDA)として、日本におけるサイバーエスピオナージの状況把握のためにも、新旧含めどんな情報でもかまわないので情報提供していただきたい。

(3) サイバーエスピオナージへの対応処置

一般的に、サイバーエスピオナージのうち、ステートスポンサード（他国の政府が支援）と思しきサイバー攻撃への対応は、各々の攻撃被害組織への対応だけで終結するものではない。

日本がこれらの攻撃の総体を把握し、対応する必要があるともいえる。情報提供や意見交換の場を設ける検討をいただくなど、国のサイバー状況把握のために、ご協力いただければ幸甚である。

---

[1] サイバーレスキュー隊（J-CRAT）技術レポート 2017　インシデント発生時の初動調査の手引き
～WindowsOS 標準ツールで感染を見つける～
https://www.ipa.go.jp/security/J-CRAT/report/20180329.html

[2] サイバーセキュリティ経営ガイドライン Ver 2.0
3．5．ステークホルダーを含めた関係者とのコミュニケーションの推進
http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf

[3] サイバーセキュリティ戦略（案）
http://www.nisc.go.jp/active/kihon/cyber-security-senryaku_2018.html