# サイバーレスキュー隊（J-CRAT） 活動状況
# [2017 年度上半期]

2017 年 10 月 30 日
IPA（独立行政法人情報処理推進機構）
技術本部セキュリティセンター

サイバーレスキュー隊（J-CRAT）における、2017 年度上半期(2017 年 4 月～2017 年 9 月)の活動状況を以下に示す。

## 1　活動結果

2017 年 4 月～2017 年 9 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、そのうち当該組織での対応が必要と判断し隊員を派遣したオンサイト支援の件数を、表1に示す。

**表 1　J-CRAT 支援件数の推移**

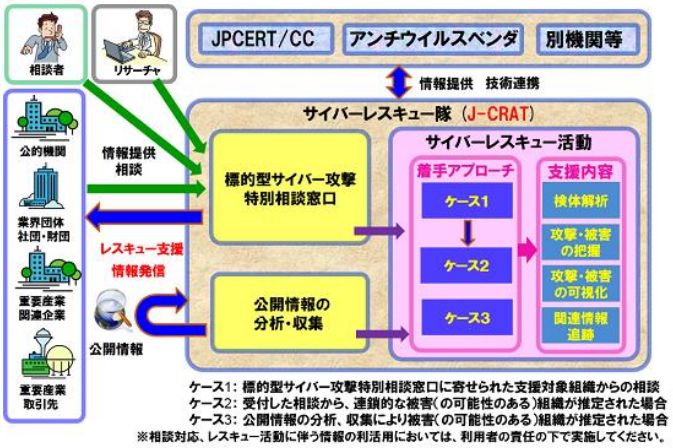
| | 2014 年度 | 2015 年度 | 2016 年度 | 2017 年度 (上半期) |
|---|---|---|---|---|
| **相談件数** | 107 | 537 | 519 | 254 |
| **レスキュー支援数** | 38 | 160 | 123 | 85 |
| **オンサイト支援数** | 11 | 39 | 17 | 17 |

※1　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 **254 件**であった。このうち、**レスキュー支援**へ移行したものは **85 件**、うち**オンサイト支援**を行った事案数は **17 件**であった。

レスキュー支援へ移行した 85 件の組織ごとの内訳は、独立行政法人 3 件、社団・財団法人 18 件、企業 30 件、学術関係組織 25 件、大学 5 件、地方自治体 1 件、その他 3 件であった。

2017 年度上半期の支援件数を**昨年の同時期（2016 年 4 月～2016 年 9 月）**と比較すると、**相談件数**がおよそ **0.9 倍**、**レスキュー支援件数**が **1.3 倍**、**オンサイト支援件数**が **1.4 倍**となった。



## 2　2017 年度上半期の活動を通じてみられた特徴的な事項

### (1) 政治・経済・安全保障に関わる組織に対する情報窃取

2017 年上半期にわたり、国際政治・経済・安全保障に関わる組織に対する継続的な標的型メール攻撃[1]が複数見られた。攻撃の手口は、メディア業界や攻撃対象組織に実在する人物などを装い、受信者の興味を引く企画書やレポートと称してマルウェア付きのメールを送付するという、従来見られる標的型攻撃の手法だった。国際政治・経済・安全保障分野への攻撃は昨年度より継続して観測されており、特に、国際会議や関連諸国の主要な政治的イベントを目前に控えた時期に活発化する傾向があると見ている。

標的型攻撃メールの送信元として、フリーメールサービスの他に、実在組織の管理する Web メールサービスが踏み台として使用されたケースも、昨年度に引き続き見られている。

一方、使用されたマルウェアのタイプには変化が見られている。初回送付されるマルウェアとしては、従来使用されている遠隔操作ツール（RAT）に加え、Windows OS 標準のスクリプト言語（PowerShell）だけで記述された遠隔操作プログラムをダウンロードさせて実行するタイプが新しく見られた。このスクリプトを用いるタイプは、コンピュータ上にファイルを作成することなく実行されるという特徴を持つことから、アンチウイルスソフトやウイルス対策ゲートウェイに検知されにくい傾向にある。

### (2) 長期間の攻撃に気が付かなかった事例

標的型メール攻撃では、攻撃者に一度標的にされた組織が執拗に、繰り返し攻撃を受ける傾向にある。今期のレスキュー活動においても、直近に発生した標的型攻撃の調査を進めていく中で、安全保障に関係する組織が約 4 年間もの長期に渡り、繰り返し攻撃を受け続けていた痕跡が見つかったケースがあった。

攻撃の間隔は最短で1ヵ月以内から、長い場合は半年以上空いていたが、各時期における攻撃に利用された遠隔操作ツール(RAT)を調査した結果、各々に関連性がみられた。このことから、少なくとも2つの攻撃グループにより継続的に情報窃取活動が行われていた可能性が考えられている。

本事例では、遠隔操作ツール（RAT）のうちいくつかは、後日アンチウイルスソフトに検出されていたものの、感染当時は検出されていなかった。したがって、被害者はそれが標的型サイバー攻撃によるものかどうか判断できず、長期間攻撃にさらされていることに気づけなかったものと考えられる。

過去に標的型攻撃メールを一度でも受信した組織は、自組織が今後も標的とされる可能性を自覚していただくとともに、未だ標的型サイバー攻撃を受けたことがないと認識されている組織においても、過去数年間に受信したメールの中に標的型攻撃メールと思われる不審メール[2]がないか、アンチウイルスソフトの検知履歴に標的型攻撃で用いられるツール[3]が含まれていないかを確認いただき、懸念点等があれば当隊へご相談いただきたい。

### (3) 攻撃に使用されたツールの通信先の傾向に変化

標的型攻撃で使用される遠隔操作ツールは攻撃者からの指令を受けるための通信を行う。標的型サイバー攻撃の通信先には、正規の組織やサービスに似せたドメイン名、正規のブログサービス、及び攻撃者が踏み台とした正規サーバのドメイン等を利用することで、不審な通信の発覚を遅らせる傾向にある。

---

[1] 本活動報告では、標的型メール攻撃を、ランサムウェアやバンキングトロージャン、一般的なフィッシングメール、ビジネスメール詐欺（BEC）ではなく、秘密裏に情報を窃取することを目的とした「サイバーエスピオナージ」に関わる攻撃を指すものとする。

[2] 「標的型攻撃メールの例と見分け方」参照
https://www.ipa.go.jp/security/technicalwatch/20150109.html

[3] 「サイバーレスキュー隊(J-CRAT)分析レポート 2016」
4.1.1 節　表 4.1-1　検知名で出る危険な単語　参照
https://www.ipa.go.jp/security/J-CRAT/report/20170127.html

しかし、今期のレスキュー活動で見られた遠隔操作ツールの大半は、ドメイン（FQDN）を指定せず海外の IP アドレスへ直接通信するものと、無料で取得可能なダイナミック DNS サービスのドメインへ通信するものであり、特別な工夫は見られなかった。これらの通信は、プロキシサーバ、URL フィルタ、次世代ファイアウォールなどのフィルタリングルールへカテゴリとして登録することで検知または遮断も可能である。

(4) 知的財産を狙った攻撃の継続

大学・研究機関など知的財産を保有する組織を狙った攻撃は今期も引き続き見られた。

大学研究室の PC より標的型攻撃に関係する不審通信が発見された事例、及び省庁管轄の研究関連組織が所有する Web サービスへパスワード攻撃が行われた事例等が確認されている。

知的財産としては、我が国の政策に関わるものから、安全保障や輸出管理に関わる情報、また情報によっては核兵器の開発に転用可能な情報が含まれることも考え、漏洩嫌疑事案については詳細な状況把握と対策を念頭に置く必要がある。

(5) Web 改ざんの裏に潜むバックドア：WebShell

Web サイトの脆弱性（Java や CMS の脆弱性）をつき、Web サイトを改ざんする攻撃（見える攻撃）の背後で、ひそかに WebShell と呼ばれるバックドアが仕掛けられている事例を確認した。WebShell は、標的型サイバー攻撃において標的型攻撃メールとあわせて侵入経路の確保に使われるため、Web 改ざんへの注意においては、コンテンツの改ざん･削除だけではなく、「意図せぬファイルが増えていないか」といった注意が必要である（マルウェア設置も同様）。

## 3 活動を通じての提言

2017 年度上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。これまでの提言と重複する内容が多いが、標的型攻撃メールによる情報窃取活動（サイバーエスピオナージ）の手口は 2005 年に国内での標的型攻撃メールによる情報窃取活動が観測されて以来、変化が少ないため、一部補足して再掲する。

(1) マルウェア感染の可能性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、攻撃手口自体は変化しないものの、メールフィルタやアンチウイルスソフトで完全に防御することは困難であると考えられる。

マルウェア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の適切な設定といった技術面の対策（※2）、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の危機管理対策を行うことが望ましい。

また、各端末やサーバでは、感染を前提とした対策として、「ファイル操作やレジストリ操作の挙動を記録する」ことも有益であり、とくに「端末上の変化を察知する（レジストリ変更、ファイル追加削除）」ことが有効である。

※2 例えば今期に見られた遠隔操作ツールに限れば、ファイアウォールやプロキシサーバ等でダイナミック DNS サービス、無料の PaaS サービス、無料のクラウドストレージサービス、及び IP アドレスへの直接通信をフィルタリングしていれば、感染後の実害を防止できたものも多い。

(2) ファイアウォールやプロキシサーバ、メールサーバの定期的なログ調査

ファイアウォールやプロキシサーバのログを取得していたにもかかわらず、ログの調査を行っていなかったために、攻撃に気づかないまま数年が経過してしまったケースが引き続き確認されている。

ファイアウォールやプロキシサーバのログには、マルウェアに感染した端末が不正アクセス先へ通信する際の送信元アドレスや送信先アドレスの痕跡が残る可能性がある。少しでも早い段階でマルウェア感染に気が付き、被害の拡大を防ぐためには、ログの調査を定期的に行うことが望ましい。

定期的なログ調査においては、通常時にどのようなログが出力されるのかを把握したうえで、それとは異なるログに着目することになる。

採取できるログの種類や形式は、情報システムの構成と用いられている機器により相違があるため、ログ調査を繰り返しながら各々の組織に合わせて調査方法を確立していくことが望ましい。特に、昨今の攻撃手法では、通常通信に攻撃通信をまぎれさせるものが主流のため、通信要件に合わない通信を記録するだけでなく、通常通信の記録もログとして取得しないと攻撃の痕跡を見落とすことになる。

また、サイバーインシデント情報の共有活動やセキュリティベンダー等を通して、不審メール・不審通信先・マルウェアの挙動といった感染痕跡情報（インディケータ）を入手できる場合は、それを各機器のログ調査やフィルタリングに活用できる環境を整えることが望ましい。

以下に示すインディケータを調査・フィルタリングする代表的な機能を有しているかできるかどうか確認するとともに、実際の対応フローを把握しておくことが重要である。

① 不審メール情報を使って、メール受信サーバやユーザメール環境で、検索やフィルタリングに活用できること。
- メール送信者（ヘッダ及びエンベロープ）
- 件名
- 本文
- 添付ファイル名
- 受信日時

② マルウェア感染痕跡情報を使って、端末やサーバに対する検索ができること。
- マルウェアによって作成されるフォルダ名／ファイル名
- マルウェアによって自動起動設定されるファイル／サービス
- マルウェアによって設定されるレジストリ値

③ 不審な通信先を使って、ゲートウェイ製品やネットワーク製品で検索やフィルタリングに活用できること
- FQDN
- IP アドレス
- URL パス
- Web リクエスト情報（User-Agent、POST 値）

(3) DNS サーバログの適切な利活用

組織内に独自の DNS サーバを設置していた組織でマルウェア感染が見つかった際に、DNS サーバのログが取られていないケースがある。

DNS サーバのログには、マルウェアに感染した端末が不正アクセス先へ通信する際に名前解決を行った痕跡が残る可能性がある。名前解決の記録と不正通信先のリストとを照合することで、システムの感染状況をより早く把握し、原因究明に役立てることができる。

2016 年上期のケースでは、IP アドレスが頻繁に変更される不正通信先との通信記録を調査するにあたり、DNS サーバのログが無いために調査範囲が拡大したことがあった。

DNS サーバのログを取得する際は、ファイアウォールなどその他の機器と組み合わせて調査することを念頭に、必要なログ項目、記録期間を設定することが望ましい。

特に、攻撃の過程においては、名前解決結果が 0.0.0.0 や 127.0.0.1 となり、感染端末から外部へ通信を発生させないよう潜伏することがあるため、そのような「一般にはとりえない名前解決結果を検知する」、「構成上、名前解決をする必要がない端末からの要求を記録する」など、DNS 通信自体を観測することで、感染後の調査に役立てることができる。

(4) DHCP サーバログの適切な利活用

ファイアウォールやプロキシサーバ、メールサーバ、DNS サーバログから、嫌疑端末を特定できても、DHCP 運用により「そのとき、どの端末にアサインされた IP アドレスかわからない」といったケースがあった。サーバログによっては、付加情報として端末情報があるため、嫌疑端末をトラッキングできるものもあるが、DHCP サーバがいつ、どこへ IP アドレスをアサインしたかは、ログの利活用として重要であるため、DHCP サーバログの取得を行うことが望ましい。

(5) 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へ提供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、関連団体等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 [4][5]することをお願いしたい。

日本におけるサイバー諜報活動(サイバーエスピオナージ)の実体把握のためにも、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。

---

[4] サイバーセキュリティ経営ガイドライン Ver 1.0
(8)情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

[5] 企業経営のためのサイバーセキュリティの考え方の策定について
2－③ サプライチェーン全体でのサイバーセキュリティの確保
http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf