サイバーレスキュー隊（J-CRAT） 活動状況
[2018 年度上半期]

2018 年 11 月 22 日

1　活動結果

2018 年 4 月～2018 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	2018 年度 (上半期)
相談件数	537	519	412	155
レスキュー支援数	160	123	144	34
オンサイト支援数	39	17	27	8

※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 **155 件**であった。このうち、**レスキュー支援**へ移行したものは **34 件**、うち**オンサイト支援**を行った事案数は **8 件**であった。

2　2018 年度上半期の活動を通じてみられた特徴的な事項

前期から引き続き、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[1]が継続的に行われた。
今期に見られた特徴として以下を挙げる。

- 政治・経済・安全保障・国際関係など情勢への関心が高いと考えられる活動と、先端技術や輸出管理対象となるような知財に関心が高いと考えられる活動が並存している。
- 特定の集団にとって興味を掻き立てられるメール文面や添付ファイル名であるなど、巧妙に添付ファイルやリンクを開かせようとする騙しの手法が多い。
- フリーメール（プロバイダメールを含む）を利用し、表示名は実在の人物が多い。不正利用、または詐称と推測。
- あきらかな日本語文法の間違いは少ないが、稚拙なミスは散見される。
  添付ファイルは暗号化されておりパスワードが別送されるケースが多い。メール中継上での検知を避けるためと推測。
- 添付ファイルの内容（おとり文章）は粗雑で不自然な構成が多い。

[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）などサイバークライムやマルウェア SPAM ではなく、秘密裏に侵攻し情報を窃取することなどを目的とした「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。

3　活動を通じて感じたこと

サイバーレスキュー隊（J-CRAT）では、主に国益（ナショナルインタレスト）に影響すると考えられるサイバーエスピオナージ（サイバー諜報活動）に対する相談やレスキュー活動、情報収集を行っている。

このような情報活動は、J-CRAT で把握している限り 2000 年代初頭から行われており、継続して政治・経済・安全保障・国際関係、及び学術機関、またその関係組織・人を対象としていると判断している。

また、情報活動に利用されたツールやウイルス、通信先（IP アドレス、ドメイン名）を、公開されたサイバー攻撃者推定情報と照らしてみると、ステートスポンサードとよばれる情報活動と合致していた。

このような情報活動に対しては、攻撃の実態を日本として把握し、我が国の安全保障を脅かすサイバー空間における脅威と捉え、同盟国・有志国と連携し、さまざまな有効な手段と能力を活用した対応を行うことが重要である。そのためには、侵害の把握だけではなく情報活動行為の把握を推進し我が国のサイバー状況把握を高めることが重要であり、さらに、日本への攻撃の実態を国が把握することで、さまざまな有効な手段と能力を活用した対応が行える状態であることが求められる。

そのためには、各組織、各個人は個々のサイバー攻撃対策に加え、被害の実態や情報活動の痕跡を「対抗処置の材料」に転じられるよう、J-CRAT、警察など政府機関への積極的な情報提供を行い、ともに対抗活動へ参加いただきたい。

次に、具体的な対応に必要であると考えられることを列記する。

(1) サイバー諜報活動の妨害

サイバー諜報活動は、Computer Network Exploitation（CNE）とも呼ばれる秘密浸透活動の一種と考えられる。攻撃者は、気づかれないよう侵入し活動することを第一の目的としているため、被害を早期に発見するためには、気づいた時点で端末の隔離や、通信の抑制など活動環境を停止させることが有用である。活動に気づくためには、不審なメールを開いたことへの自覚に対する感度の向上や、その行為を早急に連絡する体制が重要である。

加えて、情報提供を早急に行い、同時に攻撃されているが気づいていない組織における発見と対策に活用可能な防具（インディケータ：IoC）に転じさせることが重要である。

情報提供により得られたインディケータには、メールに関わる痕跡情報、通信に関わる痕跡情報、端末に関わる痕跡情報から構成される。そのため、そのような情報の活用のためには次の作業が行えるようにしておく。

1：メールを検索できること

各個人のメール環境や、システム全体で、メールアドレス、件名、本文などをキーワード検索できるようにする。添付ファイル名を検索できることが望ましい。

2：通信の制御ができること

サイバー諜報活動で使われる IP アドレスや FQDN（例：www.example.com）に対して通信制御（フィルタリングし、警告またはブロック）ができるようにする。FQDN の一部を設定できることが望ましい。また、URL パスなど、上位レイヤーでの通信制御ができるとさらに効果がある。

3：端末痕跡を探せること

特定のディレクトリ（フォルダ）や Windows レジストリの検索ができるようにする。多数の端末を保有する場合は、IT 資産管理ツールなどによる一括調査が行えるとさらに効果がある。

4：管理者作業の把握

感染拡大につながるラテラルムーブには RDP など正規の管理者用ツールが使われることがある。これらのツールをシステム管理者が使用する際の場所やアカウント名などを限定し把握しておくと、攻撃者の例外的な使用をあぶりだすことができる。普段の運用作業を把握し、運用作業で実施したコマンドや時間の作業記録をイベントログ等と定期的に突き合わせることで攻撃痕跡を発見できることがある。

J-CRAT では 2018 年 3 月に、Windows 端末や Windows サーバ上におけるサイバー諜報活動で用い

られるツールを発見するする手段の一つとして、Windows OS の標準コマンドを利用したウイルスの痕跡の抽出を行う例を公開した。インシデント発生時の初動調査の手引きに調査観点を載せているため参考にしていただきたい[2]。

また、不審メールに対するメール利用者の感度向上のためには、「標的型攻撃メールの見分け方」[3]を熟読し、サイバー諜報メールなのか、ばらまき型なのかを識別するために JC3[4]やフィッシング対策協議会[5]での情報発信に日々気を配ることが重要である。

(2) サイバー諜報活動への対抗

我が国としてのサイバー諜報活動への対抗では、各組織からの相談や情報提供が重要であり、日々変化するサイバー諜報活動へ対抗するためには、情報提供、情報共有の輪を拡大することが必要不可欠である。

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、J-CRAT や警察、関連団体などからの脅威情報を活かすとともに、インシデント発生時、そしてインシデント発生後、とくに過去のインシデント情報をサイバー諜報活動への対抗手段に転じるためにも、情報提供、情報共有、情報活用に積極的に参加することをお願いしたい。

また、一般的に、サイバー諜報活動のうち、ステートスポンサード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。

最後に、サイバー諜報活動の実行者には、インテリジェンスサイクルにおける「情報要求/収拾努力指向」と呼ばれる指示や受益先があると推測される。そのようなモデルでは、収拾のためにサイバー空間以外での活動がなされるかもしれない。収拾される「情報」に対して、サイバー以外ではどのような手段がありえるかを考え、リスクの排除や緩和、対策処置など複合的な対応まで含んで「サイバー諜報活動対抗」となりえることを認識しなければならない。

[2] 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

[3] 標的型攻撃メールの見分け方
https://www.ipa.go.jp/security/technicalwatch/20150109.html

[4] 一般財団法人 日本サイバー犯罪対策センター (JC3)
https://www.jc3.or.jp/topics/virusmail.html

[5] フィッシング対策協議会
https://www.antiphishing.jp/