サイバーレスキュー隊（J-CRAT） 活動状況
[2018 年度下半期]

2019 年 7 月 24 日

1　活動結果

2018 年 4 月～2019 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、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、及び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
相談件数	537	519	412	413
レスキュー支援数	160	123	144	127
オンサイト支援数	39	17	27	31

※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 **413 件**であった。このうち、**レスキュー支援**へ移行したものは **127 件**、うち**オンサイト支援**を行った事案数は **31 件**であった。

2　2018 年度下半期の活動を通じてみられた特徴的な事項など

サイバーレスキュー隊（J-CRAT）では、ステートスポンサードとみられる攻撃者によ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。本活動報告で紹介するサイバー諜報活動の一端が、セキュリティ対策への手がかりとなることを望む。

2.1 標的型サイバー攻撃メール以外の侵入手口～ネットワーク-端末境界貫通型攻撃

標的型サイバー攻撃の侵入段階における手口として、引き続き標的型攻撃メール[1]が用いられた他に、ネットワーク経由で侵入され攻撃活動が開始されたと推定される事例が複数の組織で確認された。

後者は、遠隔保守メンテナンス用途で解放された RDP ポートや OpenVNC のサーバ機能が侵入契機と推定されるが、該当端末には標的型攻撃メールのような明確な痕跡が残っていないため、ディスクイメージの調査（ディスクフォレンジックなど）や各種 OS の痕跡（ログなど）の調査から推測せざるを得なかった。

その他、本来社内ネットワークで使う用途のクライアントーサーバシステムのエージェントがインストールされた端末を外部に持ち出した結果、意図せずインターネット側から接続可能な状態となったために侵入された事例や、侵入には至らなかったものの、Web サイト改ざんによるサービス妨害、コンテンツ侵害の事例を情報提供いただき、当隊で拝見したところ、ひっそりと設置されていた WebShell と呼ばれるバックドアを発見した事例もあった。

攻撃者は、標的への侵入方法を公開情報や様々な情報源から積極的に収集しているであろう。そうして得られた情報や、攻撃者の保有する資源を組み合わせて、サイバー攻撃以外の手段も含めた様々な選択肢の中からインターネット経由の攻撃手段（メールを使う、ネットワーク越しに侵入するなど）を決定している

[1] 本活動報告では、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に関わるメールではなく、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」に関わるメールを指すものとする。

と考えられる。

ネットワーク越しに攻撃リスクがもちこまれると想定した場合、各情報資源のインターネット境界におけるサイバー状況把握、すなわちどのような通信が外部へ出ているか、どのような通信が内部につながるのか、普段どのような通信が行われているのか、どのような機器と設定で構成されているのか、といったネットワーク状況把握を定期的に行い、攻撃を防ぐための手立てや、侵入後の活動に気づくために必要な処置を検討し、実行するべきである。特に、その境界における重要な要素として「認証」を考えた場合、「適切なアカウントパスワード管理」や「認証が行える人・組織・接続元通信アドレスの制限」といった運用面の見直しも合わせて実施すべきであろう[2]。

また、各組織で十分な管理がなされていないインターネット上の資源が標的型サイバー攻撃の踏み台やC2 サーバなど攻撃者のネットワーク資源として悪用されており、意図せず攻撃者に加担してしまう例もある。

インターネット上に意図しない機器や通信手段が公開されていないかを確認する方法の一つとして、IPA では SHODAN などの検索サービスを用いた対策方法を公開しているので、自身の管理する IP アドレスなどに対する調査確認の参考としていただきたい[3]。

2.2 攻撃対象の傾向

標的とされる分野の傾向には大きな変化は見られず、政治・経済・安全保障といった情勢に係る分野に加え、科学技術や生産技術など知財に係る分野への攻撃が継続している。

地理的な特徴としては、海外の現地法人を狙った攻撃が複数観測されている。これは標的型サイバー攻撃の常套手段である攻撃の連鎖を目的として、セキュリティの比較的甘い関連組織が狙われたものとも考えられる。

従って、サイバーリスクマネジメントに携わる者は、ニュースなどで報じられる世界情勢にも目を向け[4]、自組織に関係する地域で情報活動が行われる可能性を脅威として把握し、重点的に注意を払うべき地域を選定することが重要である。重点地域においては、不審メールや不審通信のチェックといった基本的なセキュリティ対策を施すとともに、標的型サイバー攻撃の痕跡が端末に残っていないかを点検することが望ましい。

2.3 その他の傾向

不審な通信が出ていると外部機関から連絡を受けたことを契機として、3 年間以上の長期感染が確認される事例も依然として観測されている。セキュリティソフトを導入し、OS やアプリケーションの最新化を行っているにも関わらず検知されないバックドアや侵入ツールが仕掛けられているケースも見られた。

その他、侵入後の段階で見られた攻撃者の活動の特徴として、侵入した Web サーバにコインマイナーを設置するケースが複数観測されている。これは、サイバー諜報活動と平行してサイバークライムを行う攻撃者の存在を示唆している。見方を変えれば、サイバークライムやコンテンツ改ざん、サービス妨害など「被害が見える・気づける」インシデントがあった場合、その裏に「被害が見えない・気づくことが困難」な侵入活動が隠れていないか十分注意する必要がある[5]。当隊では、各組織で実施頂いたサイバークライムのインシデント対応結果を拝見し、サイバー諜報活動とのつながりについて助言する活動も行っている。過去の事例や対応過程において、情報の内容や提供方法は問わないため、是非ご連絡いただきたい。

3 活動を通しての所感

今期に観測された標的型サイバー攻撃のツールや通信先から、ステートスポンサードとみられる攻撃者による情報活動は依然活発に継続していると判断する。さまざまな侵入手口、オープンソースを組み込んだ

---

[2] メールサービス、統合認証システム、VPN や遠隔保守用システム、Web ミドルウェア、CRM システムなど

[3] IPA テクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」
https://www.ipa.go.jp/security/technicalwatch/20160531.html

[4] CISTEC（安全保障貿易情報センター）の発行する CISTEC ジャーナルなど
http://www.cistec.or.jp/journal/journal.html

[5] コンテンツの改ざんや削除だけでなく、意図しないファイルが設置されていないか確認すること

攻撃ツールの使用、最新の脆弱性の悪用も確認されていることから、攻撃者が圧倒的に有利な状況は変わらず、一組織が単独で標的型サイバー攻撃を防御・検知・抑止することはより一層困難になっていると感じる。

このような情報活動に対抗していくためには、以前より述べていることではあるが、攻撃の実態を我が国として把握し、同盟国・有志国と連携して様々な手段と能力を活用し対処していくことが重要である。具体的には、被害状況だけではなく攻撃者の情報活動行為の全体像を把握し、我が国のサイバー状況把握を高めるとともに、政治的・外交的に実効性のある抑止力として保持していくことが必要である[6]。

一方、各組織、各個人においては、個々のサイバー攻撃対策を自ら行うとともに、万一被害を受けた場合等はその情報活動の痕跡を収集し、対抗処置に資するよう、J-CRAT へ情報提供するとともに、政府関係機関、NISC、警察等から提供される情報を積極的に活用し、有効な対処に取り組んでいただきたい。

また、各組織から外部機関への情報共有については、組織の規模、規則、体制により差異はあるものの、報告のコストが大きいことから慎重となる傾向にあり、タイムリーな行動が難しいことも多々あるのが実情と思われる。

J-CRAT では、標的型サイバー攻撃インシデントの初動対応支援の一環として次のようなケースでも相談を受け付けており、可能な範囲の助言を行っている。

- 断片的な情報しか揃っておらず、標的型サイバー攻撃か否かの判断ができていないケース
- インシデント対応中や対応後で、所定の様式への整理は終わっていないが攻撃に関する情報を持っているケース
- 他組織やセキュリティベンダに相談済のケース

相談者の負担も考慮し、状況に応じてオンサイトでの相談も受付けることも可能であるため、インシデント初動段階でのご相談を検討いただきたい。

関係者の皆様には本稿をご活用いただくとともに、当隊の活動改善のためのご指摘やご教示をいただければ幸甚である。

[6] サイバーセキュリティ 2019 （2018 年度報告・2019 年度計画）
https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf