サイバーレスキュー隊（J-CRAT）の活動報告

～2014 年度および J-CRAT 発足 1 年（2014/7～2015/6）～

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

目次

1. サイバーレスキュー隊(J-CRAT)とは

サイバーレスキュー隊（J-CRAT[1]）は標的型サイバー攻撃の対策支援を目的として 2014 年 7 月 16 日に設立された。本章では J-CRAT の活動の概要を説明する。

（１）サイバーレスキュー活動の目的

標的型サイバー攻撃の被害の低減と、拡大の防止を目的に、以下の２つの活動を実施している。

なお、このいずれの活動においても、IPA で実施するのは、緊急処置のアドバイスと攻撃実態の理解を支援することで、組織の対応体制の早急な立上げと民間セキュリティ事業者による適切な対策を得られる環境構築の支援である。

(1-1) 被害の低減： 標的型攻撃メールが届いている組織や、検知した不審な通信やログなどに対してその深刻度を認識できずにいる組織に対して、不審メールや組織のログ等の情報を分析することにより、感染経路の把握、感染の範囲などを分析し、必要な対策の早期着手を支援する。標的型サイバー攻撃における組織の“おかれた状況”、“とるべき対応”に J-CRAT の支援活動の領域をあてはめたイメージを図 1.1 に示す。

(1-2) 被害の拡大防止：標的型サイバー攻撃への支援では、標的型サイバー攻撃による感染の連鎖を解明し、一連の攻撃の対象[2]となっていることを検知できないために、別の組織に「潜伏被害」を許してしまっていた場合に、その組織にコンタクトすることにより、攻撃の連鎖の遮断を支援する。

---

1 Cyber Rescue and Advice Team against targeted attack of Japan

2 ①攻撃の標的とされていること、②実際に攻撃を受けていること、③攻撃の結果被害を受けていること

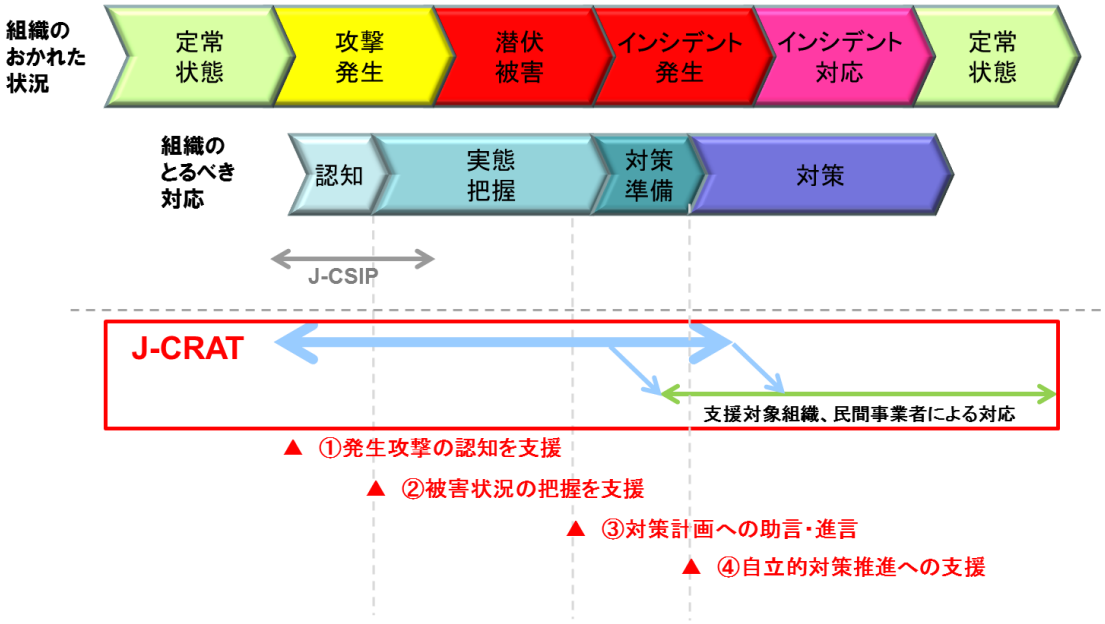

図 1.1　J-CRAT における支援範囲と内容

（２）支援対象

支援をする対象の組織として、以下を当面の活動の対象としている。

①標的型サイバー攻撃の被害を放置することが、社会や産業に重大な影響を及ぼす組織

②公的機関や重要組織との関係が深く、標的型サイバー攻撃の連鎖のルートとなる。

基本的には以下のような組織を指す。

- 独立行政法人
- 地方独立行政法人
- 国と関係の深い業界等の団体
- 民間企業（標的型サイバー攻撃 特別相談窓口で受け付け、状況等から対応が必要と判断された場合）

（３）J-CRAT の活動スキーム

図 1.2 に J-CRAT 活動の全体像を示す。

J-CRAT への情報提供や支援依頼は、「標的型サイバー攻撃特別相談窓口」にて、広く一般から受付けている。提供された情報を分析して調査結果による助言を実施するが、その中で、上記（２）の対象に対して、かつ（１）の目的に合致した事案に対して、サイバーレスキュー活動にエスカレーションする（ケース１）。この活動では当初提供された情報だけでなく、組織のシステムや端末のログなどの提供も受けて解析し、攻撃・被害の把握等を支援する。この活動は、メールや電話でのやり取りを支援活動の基本とするが、事案によっては、現場組織に赴いて行う「オンサイト支援」を実施する。オン

サイト支援の場合は、可能な範囲で組織システムの構成図などの開示を受け、攻撃ルートや感染の可能性のある端末やシステムの特定などを支援する。場合によっては、その組織のシステムを運用管理しているベンダーやセキュリティ事業者なども交えて、対応、対策の計画策定に向けた議論なども支援する。

上記の情報提供や相談によるルートに加え、事案の分析の結果、攻撃の連鎖に組み込まれている別組織（ケース２）や、インターネット上での各種情報の分析によって潜在的に被害の兆候が伺える組織（ケース３）に対しては、IPA からその組織に連絡を取ってサイバーレスキュー活動を実施する。

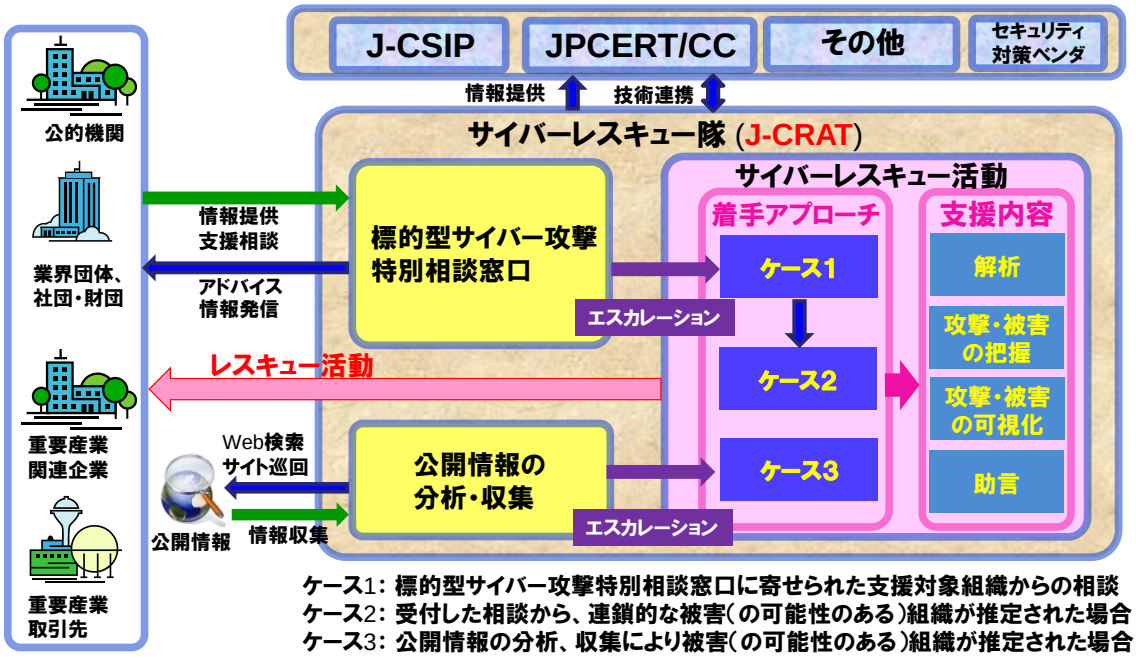

図 1.2　J-CRAT の活動の全体像とスキーム

2. J-CRAT の活動実績

本章では、サイバーレスキュー隊「J-CRAT」の活動実績を説明する。

2.1. 標的型サイバー攻撃特別相談窓口への情報提供状況

2014 年 4 月から 2015 年 3 月に標的型サイバー攻撃特別相談窓口へ寄せられた件数を表 1 に示す。情報提供を受けた主な組織は独立行政法人、社団法人、財団法人、一般企業である。また、この他、IPA からの提供依頼により入手できた情報も含まれている。提供を受けた中には、一部削除されたメール情報や、加工が施されたものも含まれる。

表 1 情報提供の状況 (2014 年度：2014 年 4 月～2015 年 3 月)

項目			件数
相談窓口受付メール件数			609
	添付ファイルつきメール数		532
		圧縮ファイル[3]の添付	364
		非圧縮ファイル[4]の添付	168
	URL リンクつきメール数		36
	添付・URL リンクなしメール数		19
	その他		22

メール種別、From アドレス、不審添付ファイルを分析した結果、特徴的な事項は以下である。

① ウイルスを「ZIP」や「RAR」等で圧縮し添付する不審メールが全体の 60%と多い結果となった。これはファイル形式で不信感を抱かせないようにし、最終的にユーザの開封率をあげようとする意図や、セキュリティ対策製品による検知を逃れる意図などが考えられる。

② メール送信元にフリーメールを利用する事例は全体の 48%と依然多く、フリーメールから送信されるメールへの対策[5]が必要である。一方で、メール本文や文中の署名に

[3] 圧縮ファイル([zip][rar][lzh][7z]等)が添付されたメール数
[4] 非圧縮ファイル([exe][doc][ppt][xls][pdf]等])が添付されたメール数

実在のドメインを詐称したケースも見られており、メール差出人の真正性を確認する技術[6]の利用も有効である。

③ 利用された圧縮ファイルは「.zip」が全体の 69%、「.rar」が 19%、「.lzh」が 7%である。これは「.zip」が Windows Vista から「.lzh」が Windows7 から標準で解凍可能になったことが背景にあると考えられる。

④ ウイルスのファイル種別は実行形式（「.exe」「.scr」「.cpl」）だけで 66%となっており、ソフトウェアの脆弱性を使うことなくウイルス感染を狙う攻撃に、注意が必要である。

なお、メール種別、From アドレス、不審添付ファイルの分析結果の詳細は「付録 1：メール分析結果」を参照いただきたい。

[5]メール送信元がフリーメールサービスであった際、メールシステムにて、メール件名や本文に当該メールの受信者向けの警告メッセージを付加し、注意を促す等の対策

[6]なりすましメール撲滅に向けた SPF（Sender Policy Framework）導入の手引き
http://www.ipa.go.jp/security/topics/20120523_spf.html

2.2. サイバーレスキュー隊の活動状況

表 2 サイバーレスキュー隊の活動状況（2014 年 4 月～2015 年 6 月）を表 2 に示す。

2014 年度（赤枠）は標的型サイバー攻撃特別相談窓口等を通じて、107 件の相談があり、38 件に対して、痕跡情報の調査やシステム構成・ネットワーク構成のヒアリング、被害状況や深刻度を助言するなどのサイバーレスキュー支援を実施した。このうち 11 件に対しては現地を訪問（オンサイト支援）し、状況分析、被害把握、暫定および恒久対策を行うための支援・アドバイスを行った。

また、2015 年度 4 月～6 月は標的型サイバー攻撃特別相談窓口等を通じた相談が 77 件、このうちサイバーレスキュー支援を 35 件実施した。この内オンサイト支援を 18 件行った。なお、表中の青枠は、J-CRAT 発足から 1 年（2014/7～2015/6）の活動を示しており、サイバーレスキュー支援数の累計は 66 件となっている。そのレスキューの支援先の内訳は、独立行政法人（12）、社団・財団法人（24）、企業（19）、その他公共機関等（11）となっている。

表 2 サイバーレスキュー隊の活動状況（2014 年 4 月～2015 年 6 月）

	2014年			2015年		2014年度	発足1年
	4月～6月	7月～9月	10月～12月	1月～3月	4月～6月	2014/4～2015/3	2014/7～2015/6
相談件数	16	25	32	34	77	107	168
レスキュー支援数	7	10	14	7	35	38	66
オンサイト	4	2	3	2	18	11	25

四半期毎の活動概要：

2014 年 4 月から 6 月：サイバーレスキュー隊発足の準備期間中に対応を行ったものである。主だった事案としてはメールに添付されていた不審ファイルを実行してしまい端末がウイルスに感染してしまったケースや、サーバにシステム管理者が見覚えの無い実行ファイルが存在していたため調査を行ったところ、標的型サイバー攻撃で多用されるウイルス（RAT）の感染が発覚したケースがあった。

2014 年 7 月から 9 月：自組織のウェブサイト改ざんを契機とした標的型サイバー攻撃の他、水のみ場攻撃、情報漏洩、また不審メールによるウイルス感染が組織内で広がったケースがあった。

2014 年 10 月から 12 月：不審な通信の発見を契機とした標的型サイバー攻撃の発覚や、不審メールによるウイルス感染が組織内で広がったケースがあった。

2015 年 1 月から 3 月：不審メールによるウイルス感染が組織内で広がったケースの他に、ウイルスメールの踏み台となったケースがあった。

2015 年 4 月から 6 月：標的型サイバー攻撃に使われたウイルスメールの感染やその対策に関する相談が多かった。特に 6 月に発覚した公的機関のウイルス感染事件を受け、社会や産業に対して影響のある組織での感染有無の検査やセキュリティ対策状況への助言の支援が急増した。また、オンサイト支援件数は、四半期あたり平均 3 件程度であったが、2015 年 4 月から 6 月は 6 倍の 18 件となった。これは発覚した時点でシステムの広域や深部にまで感染が広がっており、オンサイトでの速やかな対応が必要となったためである。

サイバーレスキュー支援に要した期間：

2014 年度のサイバーレスキュー支援 38 件に要した期間は、1 ヶ月以内が 31 件（82%）、1 ヶ月以上が 7 件（18%）であった。

オンサイト 11 件に要した期間は 1 ヶ月以内が 5 件、1 ヶ月以上が 6 件であった。

2.3. OSINT[7]：公開情報の収集・分析・活用

J-CRAT では、標的型サイバー攻撃特別相談窓口への情報提供を契機とした活動以外に、インターネット上に公開された情報を活用し、サイバーレスキュー活動に役立てている。例えば公開情報の分析から攻撃被害の潜在事案の発掘に繋げることなどである。この活動をきっかけにサイバーレスキュー支援へ発展したケースは 5 件（2014 年度）あった。また、公開情報は相談事案の分析にも活用している。本活動での典型的なケースを以下に紹介する。

(1) 自組織が詐称された標的型サイバー攻撃の不審メールに対する注意喚起を発信している組織に対して、組織名の詐称だけでなく、標的型サイバー攻撃の被害に遭っていないか、連絡を取り確認を行った。
(2) セキュリティ事業者より公開されるホワイトペーパーやブログ記事に、標的型サイバー攻撃の被害にあったと記載されている組織に連絡し、そのことを認識しているかを確認した。
(3) SNS 検索やインターネット検索を実施し、第三者や研究者がある組織への標的型サイバー攻撃を察知していた場合、その組織がそれに気づいているかどうか連絡を取り確認を行った。
(4) SNS やインターネットの検索などを実施し、わが国への標的型サイバー攻撃の予告、または攻撃方法や事例の掲載の有無について情報収集を行った。

これらの情報を収集することで、次の効果をあげている。

[7] open source intelligence の略

- 標的型サイバー攻撃の不審メールの差出人として詐称された組織や、セキュリティ事業者の情報に例示された組織を J-CRAT で調査したところ、すでに標的型サイバー攻撃の被害に遭い、攻撃の踏み台として悪用されていたことが判明。被害の情報を伝え、被害組織が民間のセキュリティ事業者と対策を講じるまでの間助言を実施した。
- 詐称された組織から標的型サイバー攻撃の不審メールが送付された相手組織に対し、標的型サイバー攻撃の被害を被っていないか確認した。
- 標的型サイバー攻撃の不審メールを受け取った事に気がついていない受信者や組織に対して、情報の提供を依頼した。情報提供された不審メール、及び添付ファイルを調査して得られた結果を IPA として注意喚起に活用した。また J-CSIP の参加組織を始め、その他関連組織へ不審メールについて対策情報として情報共有し、多組織における攻撃の検知とその拡大防止に活用した。
- 入手したウイルスに関する公開情報を調査し、被害抑止に向けた対策に活用できるよう関連するウイルスの情報を収集した。収集した情報は支援対象組織に提供したり、広く一般向けに注意喚起を実施したりした。
- 海外からの攻撃予告の有無を確認し、セキュリティ事業者との情報交換を実施、被害を最小限にとどめるために活動を展開した。

2.4. 標的型サイバー攻撃の連鎖の解明

標的型攻撃特別相談窓口およびサイバーレスキュー業務の中で、標的型サイバー攻撃に用いられる不審メールの分析や被害組織の調査により、攻撃の連鎖をたどって、別組織への連絡や情報提供の依頼、検査のアドバイスなどを実施している。その典型的なケースは以下となり、これまで、およそ 10 件程度の実施を行っている：

（１）発信元、メール内容の分析

メールで詐称されている組織、メール本文で語られている内容に該当する組織、メール本文を窃取されている可能性がある組織、あるいは添付ファイルの原本を所有すると推測される組織などを分析し、該当組織に連絡し上述した対応をとっている。

（２）送信先、同報先の分析

不審メールで宛先（ヘッダーT0）や同報先に複数人のメールアドレスが表示されている場合には、相談組織以外でウイルスに感染してしまうことも考えられる。標的型サイバー攻撃ではその目的から限られた宛先に配信されるケースも多いが、業界団体の複数

メンバーや同一研究会のメンバーなど、異なる組織の複数の宛先に送られた。これは複数の宛先を見せることで受信者を安心させたり、複数組織へまたがる業界への感染を狙うケースなどが挙げられる。宛先に実際のメールアドレスが含まれている場合や、メール文面の内容などから判断して、対象組織に連絡を取っている。

（３）レスキュー対象組織内からのメール配信の分析

被害を受けている組織から、不審メールが他組織に配信されていないか、調査を実施し、配信が確認された場合には、該当組織に上述した対応をとっている。あるいは、（１）の結果、その対象組織から実際に不審メールが配信されていた場合には、類似のメールが他組織に送信されていないか、を調査し、同様の対応をとっている。

3. J-CRAT の活動紹介

標的型サイバー攻撃の被害にあっていることに気づくのは、外部のセキュリティ事業者などから「不審な通信が確認された」といったケースや、組織におけるシステム運用の過程で、サーバや端末の動作や、ファイアウォール・Web プロキシサーバのログ集計結果などから異変に気づくケース、組織内の各人の気づきが発端となるケースがある。その後、各システムの担当組織は、セキュリティ対策製品のサポート担当や、システムの運用管理会社に相談をしながら対応を進めるが、標的型サイバー攻撃に対する有効な運用体制が確立されていない場合、初動の遅れとなることが少なくない。いくつかの事案においては、組織内で運用体制が確立されていない状況で標的型サイバー攻撃特別相談窓口に連絡があり、IPA の助言によって、迅速な対策の立ち上げができたケースもある。

以下では、典型的なレスキュー事案について紹介する。

3.1. 大規模システムにおける感染事案

数百台以上の端末と海外拠点を有する大規模システムにおける事案である。

本事案では、端末の動作が遅いため、システム運用管理会社による調査の過程において不審ファイルが発見された。その後 IPA へ情報提供され、標的型サイバー攻撃において多用されるウイルス（RAT）であることが判明。他の端末・サーバへの感染の可能性が疑われ、IPA が調査を行うことで、広範囲の感染を確認した事案である。図 4.3-1 は、サイバーレスキュー活動の中で次々と明らかになっていった攻撃の痕跡の全体像を示している。

IPA が調査を行った当初、すでに AD サーバが感染していたため（①、②）、対策としては現状把握と感染原因、暫定対策と恒久対策を平行して実施する必要があった。被害組織は CSIRT などインシデント対応の体制は確立されていなかったが、役員まで被害の状況が報告されており、そのため即座に体制を構築することができた。その体制において被害組織はシステム運用会社に加え、本事案に対応するセキュリティ事業者を含め準備を行った。

事案対処開始の契機となった攻撃を止めるために、同種被害の有無を全端末、全サーバに対し実施し（③、④）、あわせて攻撃経路となりうるインターネット接続箇所の集約（⑤、⑩）とファイアウォールによる通信遮断を実施した。この結果複数の端末が感染していることが判明し、それら端末の隔離と保全作業を行った。

このような対応の最中、システムに存在する VPN 装置や外部のウェブメールに対する執拗な不正アクセス（⑥、⑧）や、外部公開ウェブサーバへの不正なツール（WebShell）設置（⑦）等の新たな攻撃が確認された。また、対策中、同じ C2 サーバを設定した新手の標

的型攻撃メールが被害組織の所有する国内外のドメイン宛に確認（⑨）され、被害組織と攻撃者のサイバー空間における攻防が確認された。（このような過程は、他事案においてもよく見受けられることである。従って、標的型サイバー攻撃は対策中にも攻撃があり得ると考えるべきで、攻撃が無いとみなされるということは逆に検知できていない可能性もあることを踏まえ、より慎重な対応が必要である。）

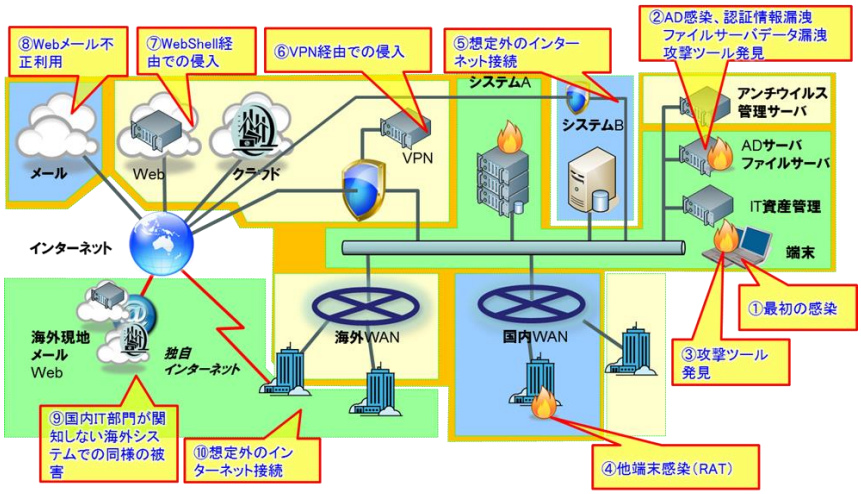

図 3.1-1：攻撃の痕跡の全体像

本事案から得られる教訓は以下となる：

・露見した事象より、はるかに奥深く、全体にわたって侵入されていることがある
・特に大きな組織では、想定外の異なる複数の入口が存在していることがある
・攻撃は、対策中であっても継続的かつ執拗に繰り返し行われる

本事案の対策においては、被害組織と運用会社が協力しあい、暫定的な運用の改善や恒久的なセキュリティ対策、適切なタイミングでのセキュリティ事業者の活用も図って進めた。しかし、上記のような攻防が見られていたため、当初の被害は迅速に終了したものの、対策と経過観察を終えるまでには最終的に 1 年近くを要した。この中で、多数の端末、サーバを調査するツールとして IT 資産管理ツールが有効であることを再認識した。なお、組織における脆弱性管理を含め、IT 資産管理ツールの活用を検討すべきである。

3.2. 標的型サイバー攻撃の連鎖の事案

本事案では、攻撃者の動きが、時間をさかのぼって解明する事ができた例となる。

説明のために、図 3.2-1 は、攻撃フローに沿った図を示している。

「組織 A を詐称した不審メールが送りつけられた(⑧)との連絡が組織 B からあった」と組織 A から標的型サイバー攻撃特別相談窓口に相談があった。

相談内容を受けて調査した結果、次のことが判明した。

- 不審メールの文面及び添付ファイル名は、組織 A の従業員と組織 B しか知りえない情報であった。
- 組織 A の担当者を詐称した組織 B への不審メールの送信元はフリーメールだった。
- 組織 A からの組織 B への不審メールは複数回送られていた。

J-CRAT では、「組織 A がすでに標的型サイバー攻撃の被害に遭い（⑥）、情報が漏洩し（⑦）、攻撃者に悪用されている可能性が高い（⑧）」と判断し、端末の感染調査方法についての助言を実施、組織 A と連携をとり、必要な情報の収集、感染の痕跡が発見されやすいフォルダやレジストリ等の調査を行った。

この結果、ウイルス（RAT）に感染し C2 サーバと通信が行われている端末には組織 A の従業員 A と、別事業所の従業員 B の 2 台が発見された。

まず、被害の拡大を抑えるために従業員 A と B の感染端末 2 台をネットワークから切り離す決断をし、当該端末を隔離するとともに、感染端末のハードディスクを保全した。ハードディスクの調査の結果、攻撃者によって組織 A の関係者と組織 B しか知りえない情報が含まれるファイルが圧縮ファイル（.rar）として保存され、インターネット上の無料ストレージサービスにアップロードされている痕跡が確認された。攻撃者は、この窃取したデータを用いて組織 B に対して攻撃を行ったものと考えられる。

さらに、組織 A で見つかったウイルスの痕跡を追跡調査した結果、従業員 A は発覚の半年前に感染(②)していたことが判明した。また、従業員 B の端末に見つかったウイルスは、従業員 A の感染後、従業員 A が従業員 B とやりとりをしたメールが攻撃者により窃取され、攻撃者はそれを改造してウイルスを添付して従業員 B に送り、その結果従業員 B が感染した(⑥)ことがわかった。さらに従業員 B の業務メールを窃取し(⑦)、それを改造して、組織 B に送られた(⑧)ことが分かった。

本事案の攻撃フロー(時系列)を、図 3.2-2 および表 3 に示す。

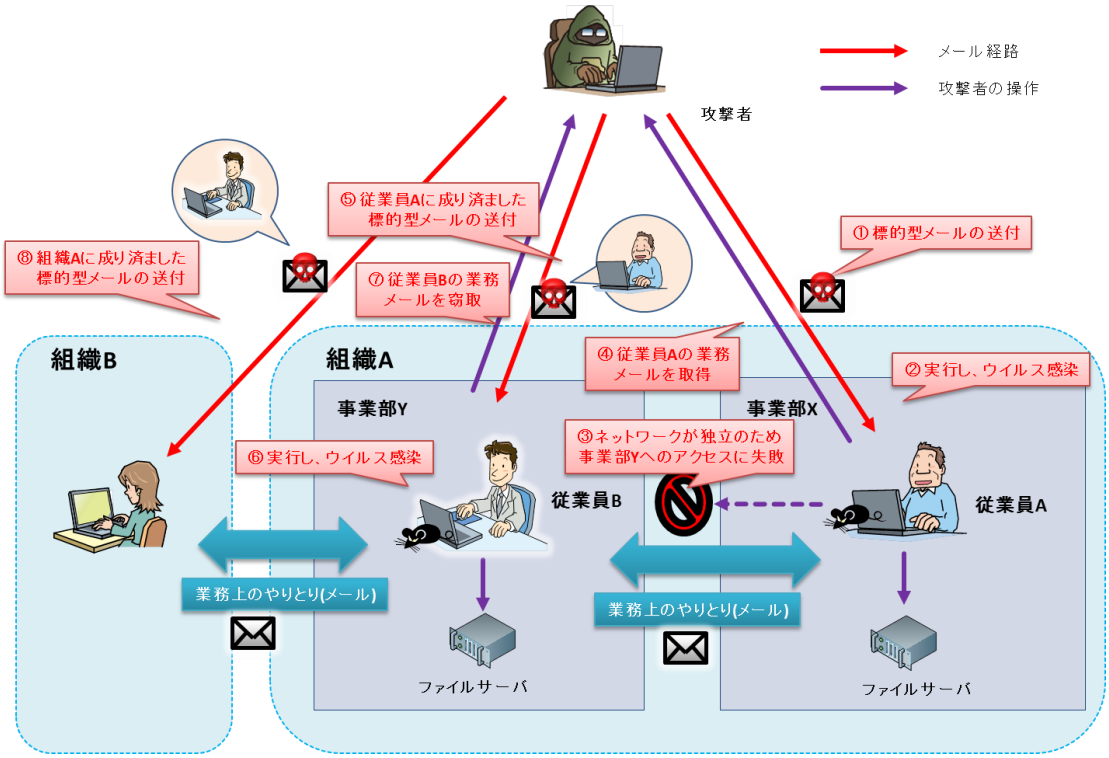

図 3.2-1：解明された攻撃フロー

表 3 攻撃のタイムライン

時期	事象（①～⑧は図 4.3-2 の数字を示す）
基準日	組織 A の従業員 A が不審メールを受信（①）し、添付ファイルを開いたため感染。（②） 攻撃者は組織内の横展開をもくろんだが不成功に終わった模様。（③）
約 6 ヵ月後	攻撃者は組織 A の従業員 A と従業員 B がやりとりする業務メール（添付ファイルつき）を窃取（④）した。
その 1 日後	攻撃者は従業員 B へ窃取したメールを加工し、フリーメールからウイルスを仕込んだ添付ファイルを送付。（⑤）同日、従業員 B は添付ファイルを開いたため感染。（⑥） 感染後、攻撃者はファイルサーバの業務データを圧縮し無料のストレージサービスにコピーした。（⑦）
さらに 4 日後	攻撃者は組織 A になりすました標的型サイバー攻撃を仕掛け、不審メールを組織 B にフリーメールから送信した。(⑧)

4. 活動のまとめ

2014 年 7 月 16 日に発足したサイバーレスキュー隊「J-CRAT」の活動実績は、標的型サイバー攻撃特別相談窓口への相談件数が 1 年（2014 年 7 月～2015 年 6 月）で 168 件、調査や対応の支援をするサイバーレスキュー活動にエスカレーションした件数はそれぞれ 66 件、その内オンサイト（現地訪問）での支援となった件数が、25 件となった。特に、今年 6 月に発覚した公的機関のウイルス感染事件を受け、感染有無の検査やセキュリティ対策状況への助言の支援が急増している。

これらのサイバーレスキュー活動によって以下に貢献できたと考える：

（1）攻撃に対する早期の対応の立上げを支援したことによる、被害の低減。

（2）攻撃の連鎖を追うことでの、攻撃の拡がりの抑止。

（3）ウイルスや攻撃の分析を実施したことによる、巧妙な攻撃活動の一端の明確化。

一方、J-CRAT の一年の活動を通して見えてきた標的型サイバー攻撃への備えの観点での課題（懸念）や特徴として、以下が挙げられる：

① インシデントが発生してはじめて、システムの全体像（所管部署やベンダーの相違なども一因）や外部通信口を充分に掌握できていないことが発覚し、対策に向けた対応の立上げに長時間要するケースがあった。

② 支援を行った法人で、重要な位置づけにあり他組織や公的機関に関与が深い組織であるにもかかわらず、組織が小規模でセキュリティ対策が充分でなかったために組織へのウイルス感染、侵入を許してしまった法人が複数あり、他組織への不審メールの踏み台となるケースもあった。

③ 大きな組織でシステム管理やセキュリティ対策がかなりなされている組織でも、発覚した時点よりかなり以前から複数回に渡って、攻撃、侵入がされており、システムの深部に侵攻されているケースもあった。

また、J-CRAT の活動によって得られた知見やノウハウを広く一般に活用、普及啓発するため以下を公開した。

■標的型サイバー攻撃特別相談窓口に寄せられた情報を分析し、「騙しのテクニック」に引っかからないための普及啓発素材として、レポート「標的型攻撃メールの例と見分け方」

を 2015 年 1 月に公開した[8]。今年 6 月の事件を受け、ダウンロード数が急増し、累計で 10 万件以上となっている。組織内での教育素材として使われているケースもある。

■ウイルス感染の早期発見、被害の低減を目的に、6 月の事件を受け、サイバーレスキュー活動での知見や実施するノウハウを織り込んで、３回の注意喚起を実施した[9]。自組織の潜在被害の早期発見や、標的型サイバー攻撃に対する統合的な対策と運用管理に活用できるものと考える。

[8] IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」
http://www.ipa.go.jp/security/technicalwatch/20150109.html

[9] 【注意喚起】潜伏しているかもしれないウイルスの感染検査を今すぐ！
http://www.ipa.go.jp/security/ciadr/vul/20150629-checkpc.html

付録 1: メール分析結果

(1) メール種別割合

相談を受けた 609 件の不審メールのうち、添付ファイルや URL リンクの有無について集計したものを 図 A-1 に示す。

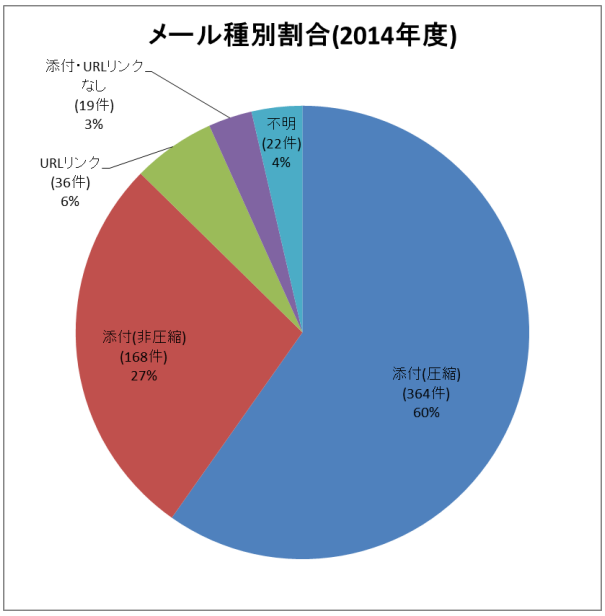

図 A-1：メール種別割合（2014 年度）

- 圧縮されたファイルが添付されたメールが 60%、圧縮されていないファイル(実行ファイル等)が直接添付されたメールが 27%、双方あわせて添付つきのメールが 87%であった。また、メール本文に URL リンクのついたメールが 6%であった。
- 添付や URL リンクのないメールは 3%となった。これには、ウイルス付きのメールを送る前に送られた「窓口の確認」などのメールや、ウイルスにパスワード圧縮をかけて送った際の、2 通目以降に送付されたパスワードの連絡メールが含まれる。
- 圧縮ファイルが非圧縮ファイルより多い理由として、攻撃者が最終的に実行をさせたいウイルスの拡張子をメーラー上で表示させず、アイコンなどの偽装と合わせてエクスプローラーで表示させる事で、利用者に実行させようとする意図や、パスワード付きで圧縮することで、ゲートウェイに設置されているメール向けセキュリティ対策製品での検知を逃れる事を狙っていると考えられる。

(2)From メールアドレス割合

相談を受けた 609 件の不審メールのうち、From メールアドレスが判別可能であった 328 件についてドメイン情報を集計したものを 図 A-2　に示す。

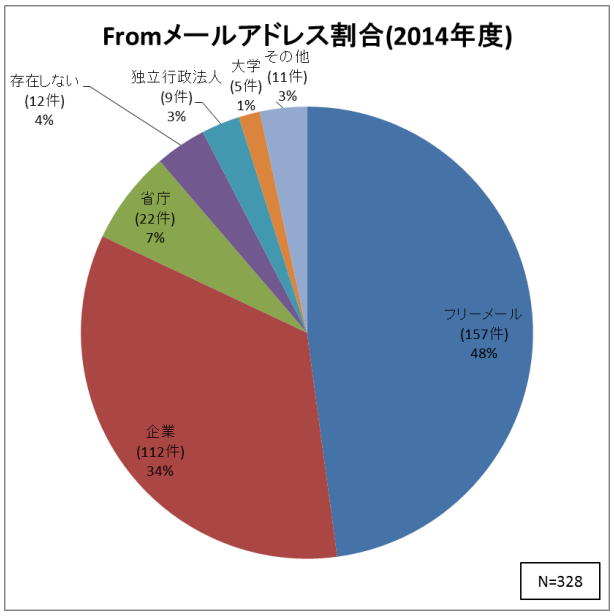

図 A-2：From メールアドレス割合（2014 年度）

- フリーメールを使用したものが 48%であった。その他、企業が 34%、省庁が 7%、メールアドレスのドメインが存在しないものが 4%、独立行政法人が 3%、大学が 1%であった。また、「その他」の 3%には「社団法人・財団法人」や、「政治家」、「政党」のドメインを使ったものが含まれる。
- フリーメールが多い理由としてメール差出人の真正性を確認する技術[10]の普及も考えられる。この技術を使うことで、偽装した送信元メールアドレスを設定していたメールを排除する事が可能だが、送信元メールアドレスを偽装せずフリーメールで送られた場合は排除する事はできないためである。ただし多くの英文メールや一部の日本語を使用したメールにてメール本文や文中の署名に即した実在のドメインを騙るケースもあるため、フリーメール以外についても引続き注意は必要である。

[10]なりすましメール撲滅に向けた SPF（Sender Policy Framework）導入の手引き
http://www.ipa.go.jp/security/topics/20120523_spf.html

(3) 不審ファイル種別割合

IPA へ相談を受けた不審メールのうち、「添付ファイル」や「URL リンク」のリンク先から取得できた不審ファイルの種別を集計したものを示す。

(3-1) ファイル圧縮形式割合

相談を受けた 609 件の不審メールのうち、添付に使われた圧縮ファイル 367 件[11]に使われた圧縮形式について集計したものを 図 A-3 に示す。

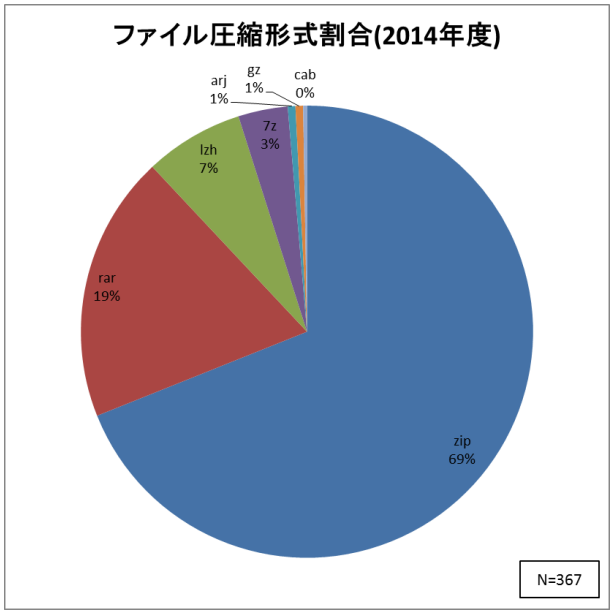

図 A-3：ファイル圧縮形式割合（2014 年度）

- 「.zip」を使用したものが 69%であった。「.rar」が 19%、「.lzh」が 7%、「.7z」が 3%であった。
- 僅かではあるが「.arj」や「.gz」、「.cab」を使ったものも見られた。
- 近年では Windows Vista から標準で解凍可能となった「.zip」や Windows7 から標準で解凍可能となった「.lzh」が使われやすい傾向にあると考えられる。

11 圧縮ファイルの添付されたメールは 364 件であるが、1 つのメールに複数のファイルを添付しているためファイル数は 367 件である。

(3-2) 不審ファイル種別割合

相談を受けた 609 件の不審メールのうち、メールに添付の圧縮ファイルを解凍して得られたもの、及び「URL リンク」のリンク先から最終的に取得した不審ファイル 480 件を集計したものを 図 A-4　に示す。

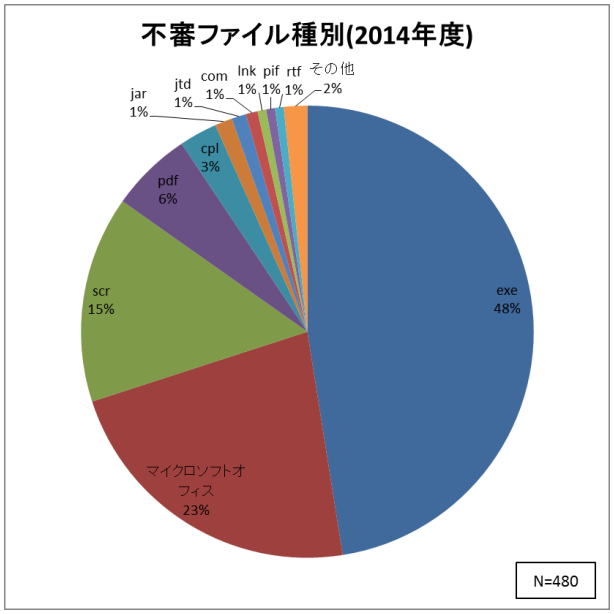

図 A-4：不審ファイル種別割合（2014 年度）

- 実行ファイル形式の「.exe」が 48%、「.doc」や「.xls」や「.ppt」などのマイクロソフトオフィス系拡張子が 23%、スクリーンセーバ実行ファイル形式の「.scr」が 15%、PDF 形式の「.pdf」が 6%、コントロールパネルにつけられる拡張子「.cpl」が 3%であった。
- 結果として、実行ファイル形式とされる「.exe」、「.scr」、「.cpl」、をあわせると 66%となった。ソフトウェアの脆弱性を使うことなくウイルス感染を狙う実行ファイルを使った攻撃に、引続き注意が必要である。

サイバーレスキュー隊(J-CRAT)の活動報告
～2014 年度および J-CRAT 発足1年(2014/7～2015/6)～

［発　　行］2015 年 8 月 5 日
［著作・制作］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
［執　筆　者］伊東宏明　竹田光徳　青木眞夫