サイバーレスキュー隊（J-CRAT）の活動概要

～標的型サイバー攻撃に対する IPA の取組み～

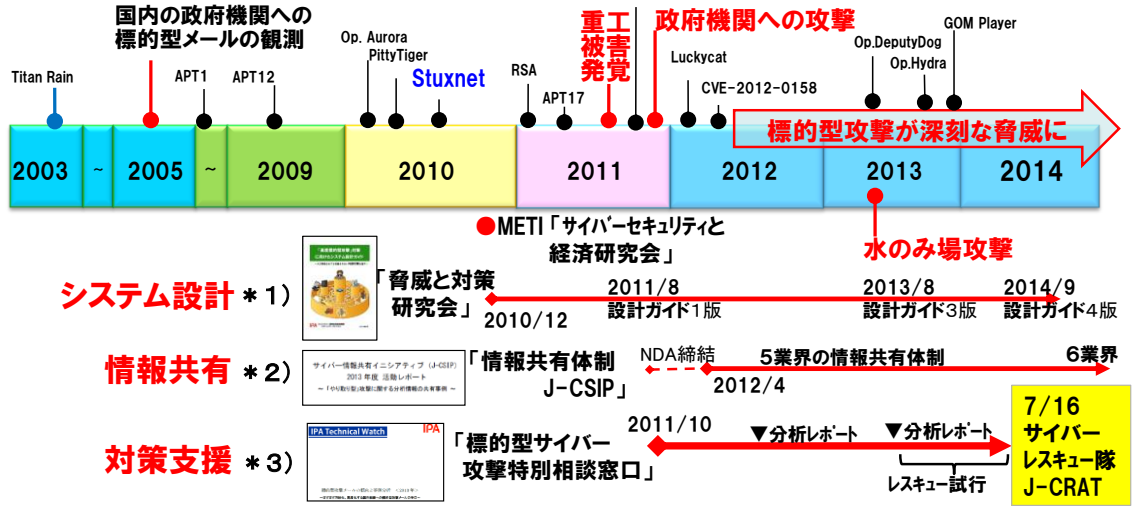
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

目次

1. はじめに ～標的型サイバー攻撃に対する IPA の取組み～

標的型サイバー攻撃は、益々脅威を増してきています。2010 年に発覚した、イランの原子力設備を狙った「Stuxnet」の事案は、標的型サイバー攻撃の脅威と深刻度を改めて認識する契機となりました。それに対応する動きとして、2010 年 12 月には、経済産業省の下で「サイバーセキュリティと経済研究会」が実施され、翌 2011 年 8 月 5 日に報告書　中間とりまとめが公開されましたが、その中の三つの政策提言の一つとして、「標的型サイバー攻撃への対応」が挙げられています。その公開から一月後の 9 月に、大手重工業企業の標的型サイバー攻撃による被害事件が明らかとなり、また 10 月には政府機関への標的型サイバー攻撃による事件が報道されました。

こうした動向に応える形で、IPA では、以下に示す三つの活動を実施してきています。図 1.1 はその全体の流れを示しています。



*1) https://www.ipa.go.jp/security/vuln/newattack.html

*2)https://www.ipa.go.jp/security/J-CSIP/index.html

*3)https://www.ipa.go.jp/about/press/20140716_1.html

図 1.1　標的型サイバー攻撃に対する IPA の取組み

（1） **システム設計**：　2010 年 12 月に「脅威と対策研究会」を発足し、巧妙に組織システムに潜入する標的型サイバー攻撃の実態を明らかにするとともに攻撃活動の早期検知と被害の低減を図るためのシステム設計ガイドとしてまとめて、公開、改訂を実施しています。

（２） **情報共有**：　2011 年 10 月から重要工業や重要インフラに関わる業界に対する情報共有のための NDA（秘密保持契約）の締結に着手し、2012 年 4 月 1 日より、サイバー情報共有イニシアティブ J-CSIP[1]（ジェイ・シップ）を立上げました。J-CSIP では、標的型サイバー攻撃を受けた参加組織が IPA に情報を提供し、IPA はそのメールを含む検体情報を分析および加工して、類似攻撃の検知や攻撃の抑止に役立つ（かつ提供元の組織情報を含まない）情報として参加組織間に情報共有を実施します。これによって、攻撃の早期検知と回避に繋げる枠組みです。J-CSIP は継続的に新たな業界や参画組織を増大してきており、2015 年 5 月時点で、6 業界、59 組織から成っています[2]。

（３） **対策支援**：　2011 年 10 月に「標的型サイバー攻撃特別相談窓口」を設置、標的型サイバー攻撃を受けた組織や個人の相談を広く受け付け、標的型攻撃メールの収集および分析を行い、その特徴や見分け方等のレポートを公開してきました[3]。その活動を一歩進め、事案によっては、社会や産業に重大な被害を及ぼし兼ねない標的型サイバー攻撃や、標的型サイバー攻撃の連鎖の元（ルート）となっている組織に対して、その攻撃の把握、被害の分析、対策の早期着手の支援をする、サイバーレスキュー隊 J-CRAT[4]（ジェイ・クラート）を 2014 年 7 月 16 日に立ち上げました。

この三つの活動の位置づけは、「設計ガイド」は個々の組織システムをいかに強固にするか、「J-CSIP」は特定の業界や組織の集合体を情報共有によっていかに強固にするか、「J-CRAT」は攻撃を受けている組織の対応や対策を加速し、組織間をまたがる標的型サイバー攻撃の連鎖をいかに断っていくか、標的型サイバー攻撃に対する組織や業界や社会における多層的な防御として捉えることができます。

以降では、三番目の「J-CRAT」に関して、その活動の概要について紹介します。

---

[1] J-CSIP (Initiative for Cyber Security Information sharing Partnership of Japan)
[2] https://www.ipa.go.jp/about/press/20150527.html
[3] https://www.ipa.go.jp/security/technicalwatch/20140130.html
https://www.ipa.go.jp/security/technicalwatch/20150109.html
[4] J-CRAT (Cyber Rescue and Advice Team against targeted attack of Japan)

2. J-CRAT 活動の概要

本章では、サイバーレスキュー隊「J-CRAT」発足に至った経緯を示すと共に、活動の概要を説明します。

2.1. 背景と経緯

IPA は、コンピュータウイルス・不正アクセスの届出機関として活動してきました[5]。2005 年以降、届出の中に“標的型攻撃メール”が散見されるようになってきました。これを受け、2008 年に標的型攻撃メールの届出の受付けを開始しました。その後、2011 年 9 月に発覚した重工業企業に対する深刻な標的型サイバー攻撃事件の発生を契機として、2011 年 10 月以降、図 2.1 に示す「標的型サイバー攻撃特別相談窓口」を設置しました。標的型攻撃メールの情報提供や相談を受け、その分析による調査結果の伝達とアドバイス、得られた情報の共有[6]や攻撃検体のセキュリティベンダーへの提供などを実施する業務に拡大してきました。

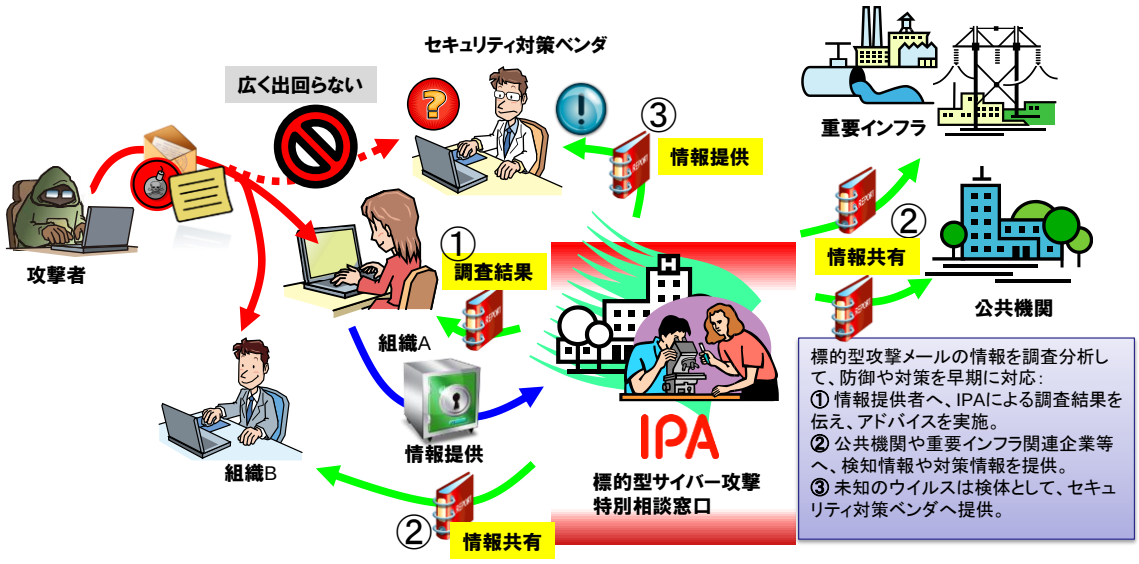


図 2.1　標的型サイバー攻撃特別相談窓口の活動概要

2013 年には、標的型攻撃メールの分析や情報共有に加え、相談を受けた一部の重要な被害組織の分析と対策支援の試行を実施してきました。その試行経験の中で、以下のような事実が分かってきました。

---

[5] https://www.ipa.go.jp/security/outline/todoke-top-j.html

[6] IPA として予め報告を決めている公共機関や、標的型特別相談窓口へ情報提供頂き、以降の情報共有（提供）を了解頂いた組織に対して実施しています。

（１） 攻撃を検知してもその深刻さに理解が及ばず、対策に適時に踏み出せない組織が多い

（２） 被害が顕在化した時点で、かなり以前から組織に潜入されている事案が散見される

（３） 標的型攻撃メールを分析すると、公的機関を含む関連組織への攻撃の連鎖が追跡できる

（１）では、被害状況の把握自体に相応の調査費用が発生することから、組織内の予算や承認を急遽得ることは困難が伴っています。加えて（２）では、顕在した時点では既に深刻な被害に至っており、対策はかなり後手になってしまっています。また（３）では、図 2.2 はそれを模式的に表していますが、該当する組織への直接の攻撃だけでなく、組織階層の上下双方向に業務や組織の関わりを悪用して攻撃が行われているケースが存在しています。

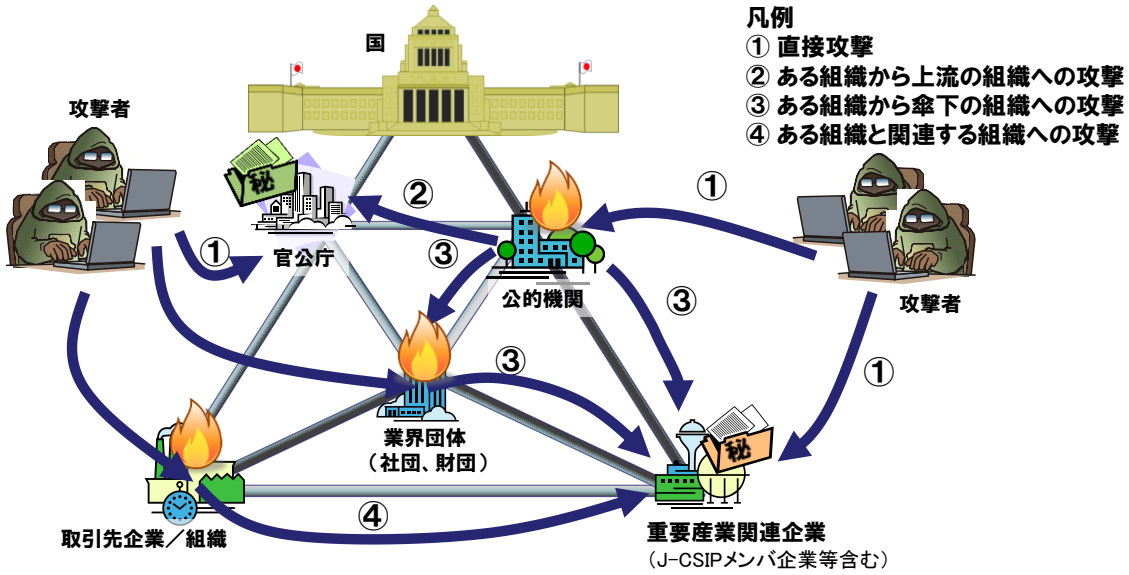


図 2.2　標的型サイバー攻撃の経路

（１）（２）はその組織自体の被害に関わることですが、長い間感染を放置してしまうと感染組織を踏み台にした（３）の攻撃にも連鎖し、社会組織全体に広く被害を及ぼす要因ともなってきます。

従って、標的型攻撃に対抗するには、こうした課題を解決していく活動が望まれます。

このような背景を受け、IPA では、2014 年 7 月 16 日に、（１）～（３）に対応して、対策を支援する活動として、サイバーレスキュー隊 J-CRAT を立ち上げました。

2.2. サイバーレスキュー隊「J-CRAT」

（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つの活動を実施することです。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フェーズにもっていくための支援です。

（1-1）被害の低減：　標的型攻撃メールが届いている組織や、検知した不審通信や不正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、標的型攻撃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します。発覚した攻撃のフェーズに沿った支援活動のイメージを図 2.3 に示します。

（1-2）被害の拡大防止：　標的型サイバー攻撃の事案の対応の中で、標的型サイバー攻撃による感染の連鎖（図 2.2 参照）を解明し、一連の攻撃の対象となっていることを検知できずに「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します。

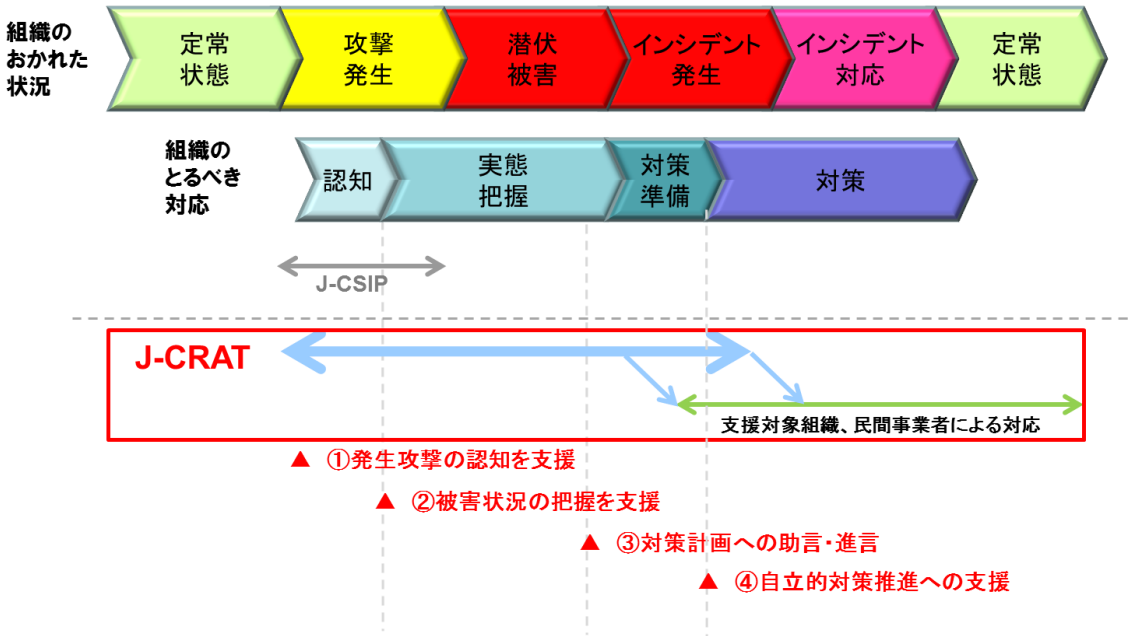


図 2.3　J-CRAT における支援範囲と内容

（２）主な支援対象

支援をする組織として、以下を活動の主な対象としています：

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組織

典型的には以下のような組織を指します。

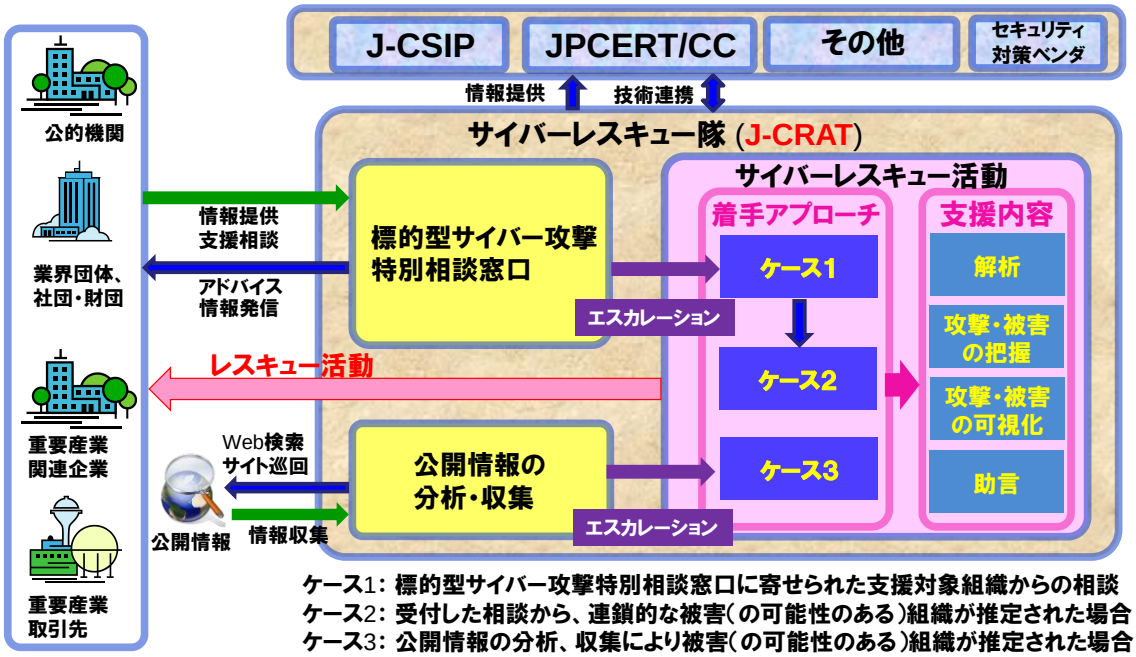
- 独立行政法人
- 地方独立行政法人
- 国と関係の深い業界等の団体
- 民間企業（標的型サイバー攻撃 特別相談窓口で受け付け、状況等から対応が必要と判断された場合）

（３）J-CRAT の活動スキーム

図 2.4 に J-CRAT 活動の全体像を示します。

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ます。提供された情報を分析して調査結果による助言を実施しますが、その中で、上記（１）の目的に合致し（２）に該当する事案に対しては、サイバーレスキュー活動にエスカレーションします（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します。この活動は、メールや電話ベースでのやり取りを支援活動の基本としますが、事案によっては、現場組織に赴いて行う「オンサイト支援」を実施します。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します。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します。

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 からその組織にコンタクト（ドア･ノック）してサイバーレスキュー活動を実施します。



ケース1: 標的型サイバー攻撃特別相談窓口に寄せられた支援対象組織からの相談
ケース2: 受付した相談から、連鎖的な被害(の可能性のある)組織が推定された場合
ケース3: 公開情報の分析、収集により被害(の可能性のある)組織が推定された場合

図 2.4　J-CRAT の活動の全体像とスキーム

3. おわりに

サイバー攻撃の高まりと IT 社会へのその大きな脅威に備え、2015 年 1 月 9 日に「サイバーセキュリティ基本法」が全面施行され、内閣官房情報セキュリティセンターは「内閣サイバーセキュリティセンター」に改組されました。そのさなかの 2015 年 6 月には、年金機構をはじめとする十件以上のウイルス感染や情報窃取のインシデントが、報道により明らかになりました。この数年、標的型サイバー攻撃の被害事例が報道されてきましたが、改めてその大きな脅威を認識した状況となっています。

今後も、個人情報や機密情報や知財情報の窃取から、社会インフラに対する妨害や破壊活動など、組織に巧妙に侵入してくる標的型サイバー攻撃の脅威は益々増してくることが予見されます。一方、IoT という用語に象徴されるように益々ネットワークインフラに依存する社会に向かっており、また、2020 年に迎える東京オリンピック・パラリンピックなどの国の威信をかけたイベントも控えており、攻撃者にとっては格好の標的となりかねないことが懸念されます。

IPA では、国内の関係機関とも連携して、標的型サイバー攻撃の脅威の回避、被害低減に寄与する活動を鋭意推進し、各組織やその集合体の対応力の向上を目指す活動を推進していきます。

なお、「標的型サイバー攻撃特別相談窓口」は広く一般組織からの情報提供や相談にも対応しております。標的型サイバー攻撃に対抗する活動の効果を上げるために非常に貴重な情報源となりますので、標的型攻撃メール等の情報提供をお願いいたします。