JPCERT CC®

CSIRT ガイド

一般社団法人 **JPCERT** コーディネーションセンター

2015 年 **11** 月 **26** 日

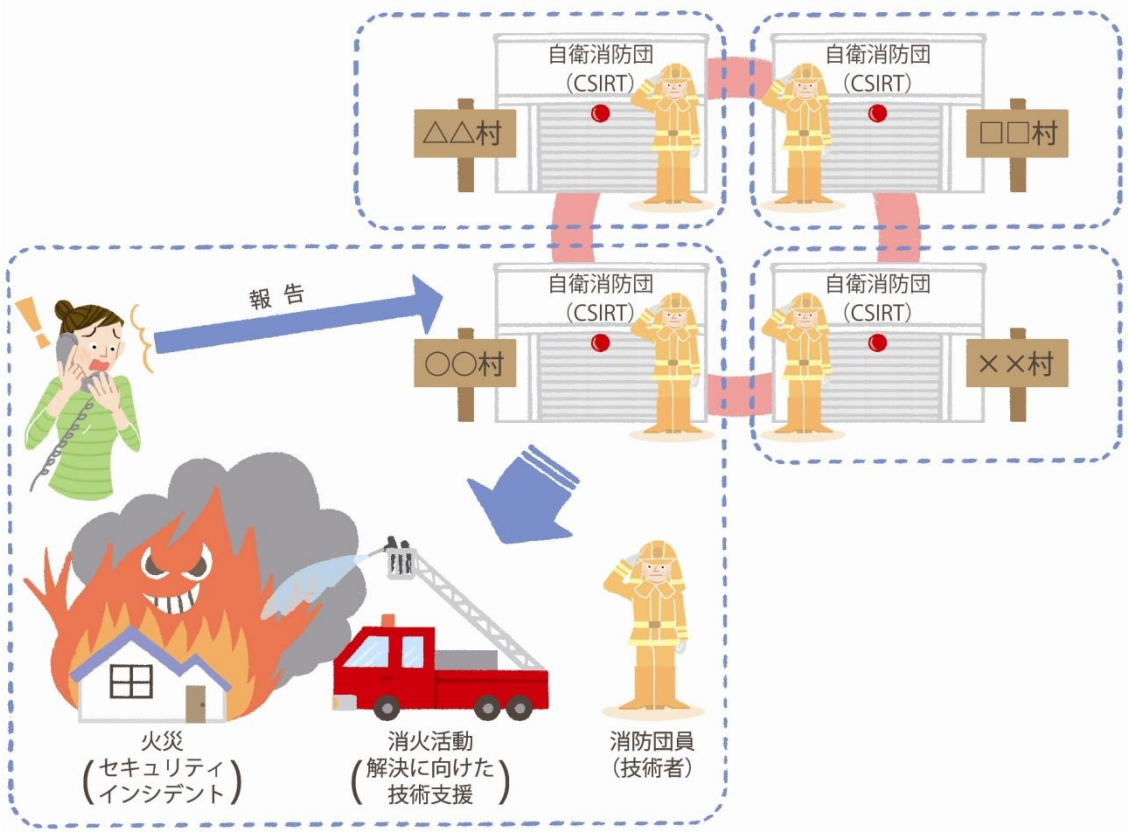
JPCERT CC®

はじめに

近年の組織(企業)の IT 化に伴い、情報セキュリティ対策は組織にとって重要な問題となってきています。かつての IT 利用は文房具の延長に過ぎず、そのため、情報セキュリティを含む IT にかかわる諸問題は、情報システム部などのシステム管理者さえ頑張ればよいと言えるレベルのものでした。しかし現在では、高度に複雑化し、且つインターネットを介して大容量のデータを瞬時に、しかも容易に世界中とやりとりできる IT システムを利用するようになったことで、単に「現場 = システム管理者」の頑張りだけで済む問題ではなくなってきているのです。例えば、顧客の個人情報が、コンピュータウイルスに感染したことで世界中にばら撒かれてしまったといった事態を考えてみれば、情報セキュリティの問題が、もはやシステム管理者だけの問題ではなく、経営層が積極的に関与しなければならない問題であることは容易に想像できると思います。

このような中で、組織の情報セキュリティ対策として注目されているのが、組織内の情報セキュリティ問題を専門に扱う CSIRT(シーサート: Computer Security Incident Response Team) の構築です。

これまでの情報セキュリティ対策が、ウイルス検知ソフトやファイアウォールの導入によるウイルス感染をはじめとする「不正アクセス」の防止といった「事故を未然に防ぐ」=「事前対応」が中心だったのに対し、CSIRT の活動範囲はもっと広いものになっています。CSIRT は、「事前」の対応はもちろん、事故が発生している最中にその被害を最小限に食い止めるといった、言うなれば「事中」の対応、更に事故からの復旧、事故の原因究明および再発防止策の検討・実施などの「事後」の対応までを行ないます。このような「事前」「事中」「事後」の活動は、消防署の活動に似ています。また、組織を 1 つの村と考えれば、CSIRT は次の図のように「自衛消防団」にたとえることができます。



JPCERT CC®

既に日本でも大企業を中心に、自組織内に CSIRT を構築する動きが活発化してきていますが、欧米の組織に比べると、その動きはまだまだ小さいものと言えます。また CSIRT に関する資料も数多く存在していますが、普遍性を追求するあまり、抽象的な内容になっていたり、また欧米向けに書かれているために日本の事情には合わなかったりする部分があります。
そこで本書では、情報セキュリティ対策として、自組織内に CSIRT を構築しようと考えている CIO (Chief Information Officer、最高情報責任者) など、経営層の方や、CSIRT のメンバーになる可能性のある社員の方向けに、CSIRT とはどのような組織でどのような活動をするのか、また CSIRT には何が必要なのかといった点を簡潔に説明します。

> 米国 CERT/CC が作成し、JPCERT/CC が翻訳した「コンピュータセキュリティインシデント対応チーム (CSIRT) のためのハンドブック」が CSIRT 構築前だけでなく、構築後も「辞書」として使えるものであるのに対し、本書は CSIRT 構築前に読む「読み物」という位置づけになります。

なお本書では、様々な種類の CSIRT (詳細は後述) がある中で、企業内で発生したセキュリティ問題に対応するための CSIRT「組織内 CSIRT」に対象を絞って解説します。
また注意していただきたいのは、本書で紹介する CSIRT についての記述は「推奨」レベルのものであり、ISMS のような「標準規格」を示すものではないということです。組織ごとに、セキュリティ上守るべき対象やポリシーが異なるように、CSIRT 自体の実装も異なります。CSIRT に「規格」はないのです。
本書が、読者の皆様の組織にとって「ふさわしい」CSIRT を構築するにあたっての「第一歩」としてお役に立てれば幸いです。

一般社団法人 JPCERT コーディネーションセンター

JPCERT CC®

目次

1. CSIRT とは？

CSIRT（シーサート）とは、そもそも「Computer Security Incident Response Team) = コンピュータセキュリティインシデントに対応するチーム」の略です。そこで、まず「コンピュータセキュリティインシデント (以降「インシデント」と略) とは何かというところから説明します。

1.1 インシデントと CSIRT

「インシデント (incident)」とは、一般的に「重大な事故に至る可能性がある出来事」を意味し、「アクシデント (accident: 偶発事故)」や「ハプニング (happening: 出来事)」とは区別されます。また情報セキュリティにおいては、「不正アクセス」と同義に使われることもありますが、厳密には「不正アクセス」は「インシデント」の 1 つに過ぎません。情報セキュリティにおける「インシデント」とは、コンピュータウイルスやサービス運用妨害攻撃、情報漏えいなど、IT システムの正常な運用または利用を阻害する (実害のある) 事象だけでなく、そのような事象に繋がる可能性のある (まだ実害のない) 弱点探索 (プローブ、スキャン) なども含まれます。

なお、「不正アクセス」という言葉の使用を避けるべき理由としては、「不正」として何を持って「正しくない」と定義されるのかが国際的な局面では非常にあいまいであり (国や文化によって異なる法的不正や倫理的不正、システムによって異なる仕様上の不正など)、また日本においては、「不正アクセス禁止法」によって「不正アクセス」が主に実害のあるものに限定された内容で定義されているからです。

[表 1.1-1 インシデントの例]

- プローブやスキャンなどの不審なアクセス（Scan）
- 送信ヘッダを詐称した電子メールの配送（Forged）
- システムへの侵入（Intrusion）
- フィッシング詐欺（Phishing）
- 分散型サービス運用妨害（DDoS）
- コンピュータウィルスの感染（Virus）
- 迷惑メール（Spam）
- 先進的で執拗な脅威（APT）

このように定義される「インシデント」に対して CSIRT が行なうのが「インシデント対応(インシデントハンドリング、インシデントレスポンスなどとも呼ばれる。詳細は後述)」です。

具体的には、(1)インシデントを検知し、あるいはその報告を受けることにより認知し、影響の拡大を防ぐとともに、(2)情報を収集して分析を加え、インシデントの全体像や原因について把握し、(3)復旧措置や再発防止のための措置を取る一連の活動を指します。

このようなインシデント対応において、まず意識すべき点は、インシデントの発生を完全に回避する予防策はないということです。

かつての情報セキュリティ対策は、ウイルス検知ソフトやファイアウォールの導入といった、インシデントの発生を未然に防ぐことに主眼が置かれていました。もちろんセキュリティ対策として、このような事前の対策が重要なのは言うまでもなく、適切な事前対策によってインシデントの発生確率を減らすことは可能です。しかし、実際に発生したインシデントの原因を分析すると、次のようなものが少なくありません。

（1）パッチの適用忘れなどの人為的ミス

初歩的なミスですが、人間のやることである以上、人為的ミスを完全になくすことはできません。

（2）未知の(公知になっていない＝回避策のない)脆弱性の悪用

悪用される脆弱性の全てに対してパッチが提供されているとは限りません。悪意のある者が自ら発見した (または何らかの方法で手に入れた) 脆弱性を、悪用することを目的に隠匿しているケースもあるのです。

（3）技術的な対応の限界

システムの設計上、特定のインシデントの発生を防ぐ機能がない、すなわち根本的にシステムを入れ替えない限り、対応が不可能な場合もあります。例えば、パスワードを設定しなければ危険なネットワーク機器が、そもそもパスワードを設定する機能を持っていなかったといったケースもあります。

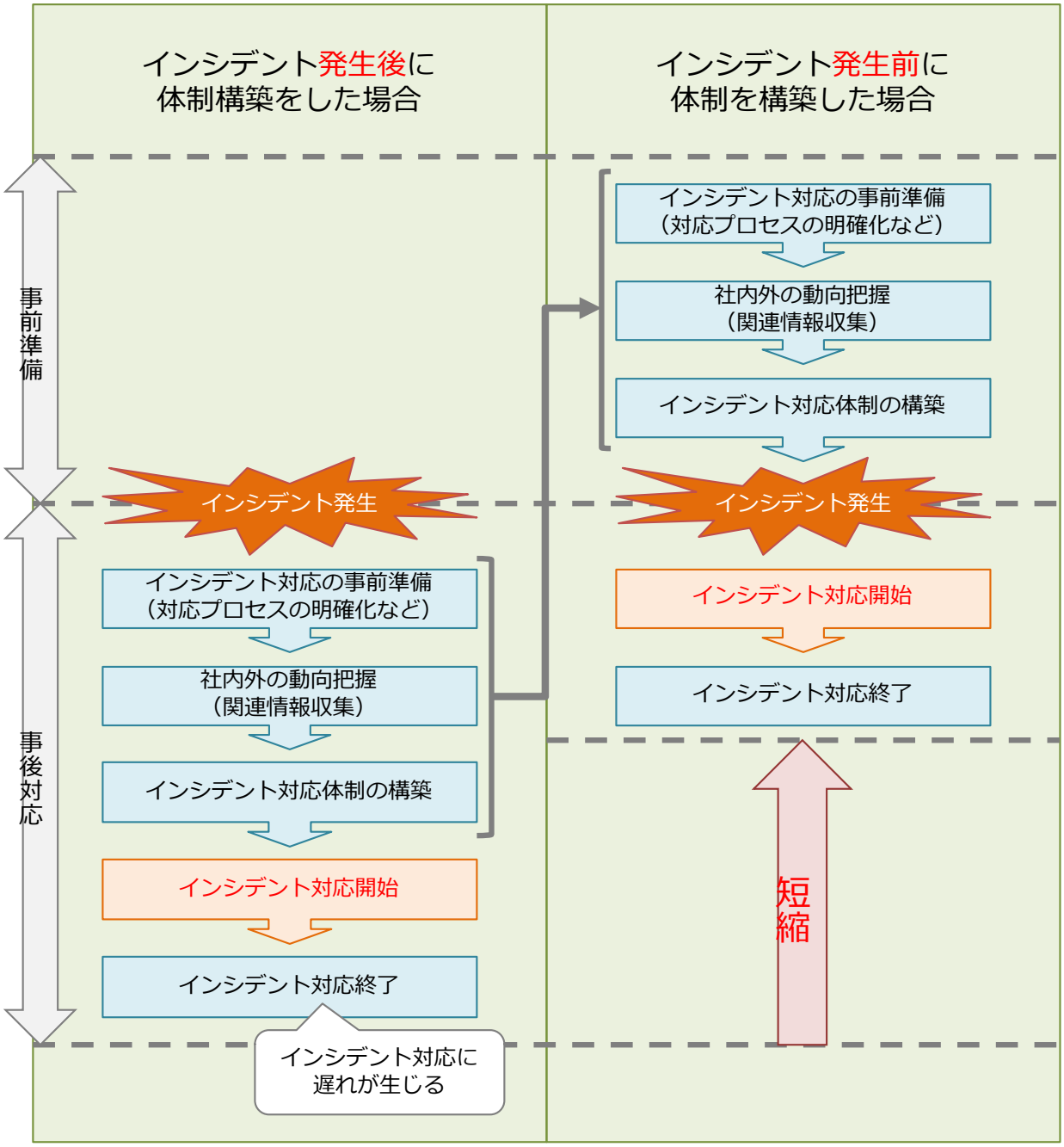
（4）必ず存在してしまう社員の意識に頼る事項

セキュリティに関わる事項は複雑多岐に渡るため、100%全てをセキュリティポリシーに定めることは事実上不可能です。どうしても担当する社員の「考え」や「好み」で左右されてしまう曖昧な事項が残ってしまうものです。

これらの原因から分かるように、どんなにインシデントの未然防止策を講じていたとしても、インシデントを発生させる余地を残してしまいます。

そこで、適切なインシデント対応として求められるのは、まずインシデントの発生を完全に防ぐことは不可能であるという「事故前提」の意識の下、インシデント発生時に「いか

にして被害を最小限に食い止めるか」、そして発生後「いかにして速やかに復旧するか」といった点なのです。そのためには、インシデント発生前にあらかじめインシデント対応体制を構築しておくことが推奨されます。

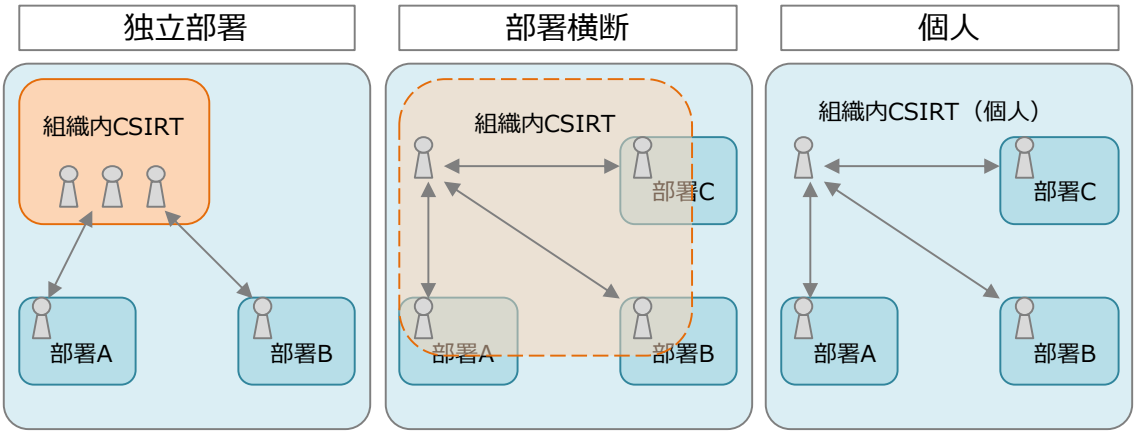


[図 1.1-1 あらかじめインシデント対応体制を構築しておけば対応が速やか]

また、組織をとりまく環境の変化にも注目しなければなりません。そもそもインシデントは災害や犯罪に比べて原因が分かりづらいものですが、IT 依存度の高まりとともに、IT システムが複雑化することで、インシデントの発見や原因の特定が一層困難になり、復旧に時間がかかるようになってきています。更に、攻撃の潜在化や攻撃手法の高度化、また特定の組織を狙った標的型攻撃やソフトウェアの未知の (= 回避策が困難な) 脆弱性を悪用したゼロデイ攻撃、標的とした組織に対し執拗かつ長期的に活動を行う高度サイバー攻撃(APT)の増加など、対応には技術的に高い専門性だけではなく、業務に対する幅広い知識も必要になるため、情報システム部などのシステム管理を行う部署だけでは対応が難しい場合が増えてきています。

このような背景から「組織的なインシデント対応」が必要となってきており、それを実現するための実装が CSIRT です。

CSIRT は Computer Security Incident Response Team の略であることから、どうしても「チーム = 専門部署」のイメージを持たれがちですが、CSIRT は必ずしも「インシデント対応を専門に行なう部署」である必要はありません。必要なのは「インシデント対応を専門に行なう機能」としての CSIRT であり、組織によっては他の関連業務と兼務したメンバーによる部署を横断した形態で CSIRT の機能のみを実装している例は少なくありません。そこで CSIRT ではなく、CSIRC (シーサーク: Computer Security Incident Response Capability = コンピュータセキュリティインシデントに対応する機能、能力) という表現が使われることもあります。



[図 1.1-2 CSIRT の実装は様々(独立部署、部署横断、個人)]

1.2 サービス対象 と CSIRT

CSIRT にとって重要なのは、まず「どこのインシデント」に対応するのか、つまり CSIRT のサービスが提供される対象 (活動範囲) がどこであるかということを明確に定義することです。英語では、それを「Constituency」といいますが、本文書では、「サービス対象」と呼びます。

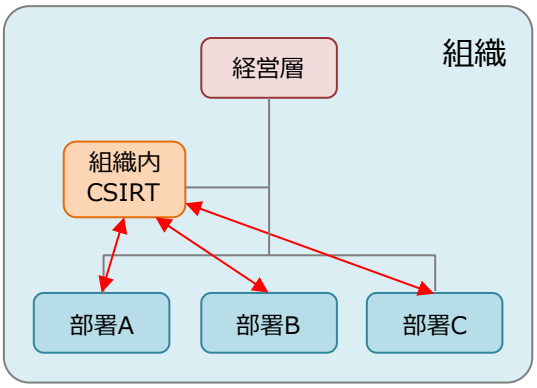
CSIRT (の機能) はサービス対象によって、次のように分類されます。

- 組織内 CSIRT
- 国際連携 CSIRT
- コーディネーションセンター
- 分析センター
- ベンダチーム
- インシデントレスポンスプロバイダ

それぞれの CSIRT の説明を次に示しますが、この分類方法は一例に過ぎず、他にも様々な視点で分類されることがあります。

(1) 組織内 CSIRT

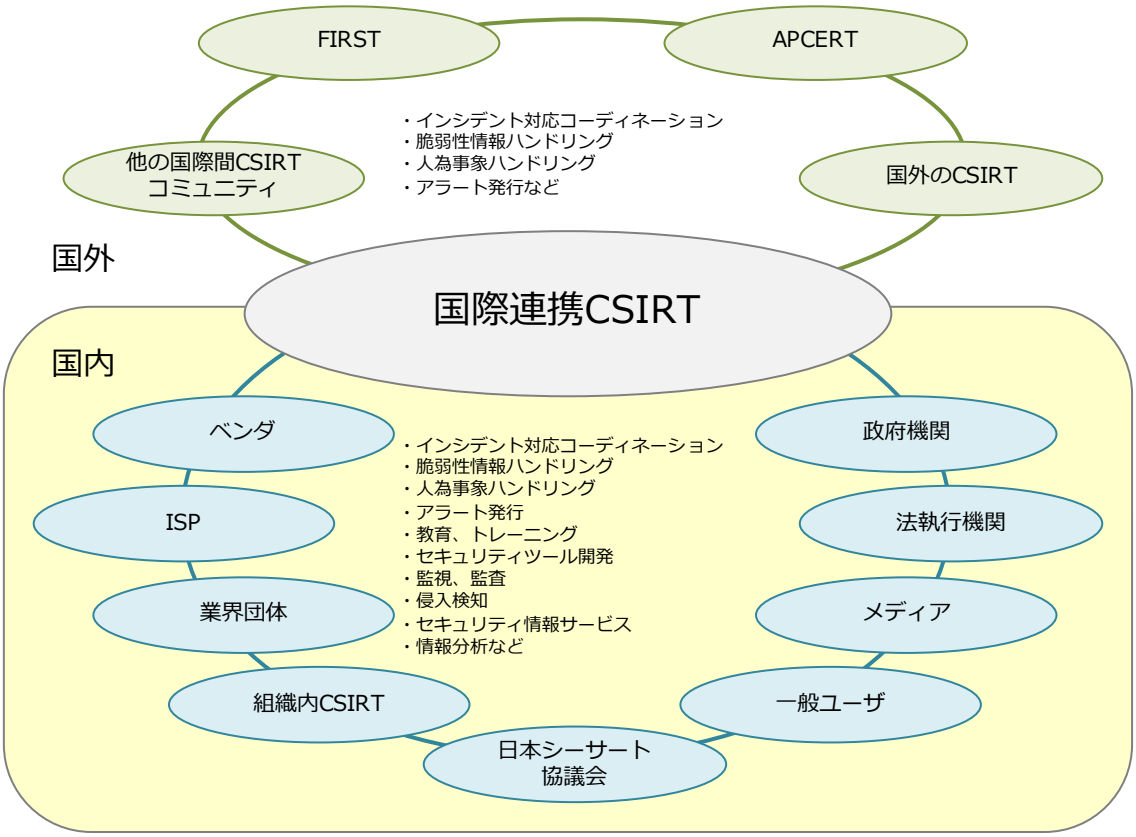
サービス対象は CSIRT が属する組織の人、システム、ネットワークなど。組織にかかわるインシデントに対応する。企業内 CSIRT。



[図 1.2-1 組織内 CSIRT のサービスモデル]

(2) 国際連携 CSIRT

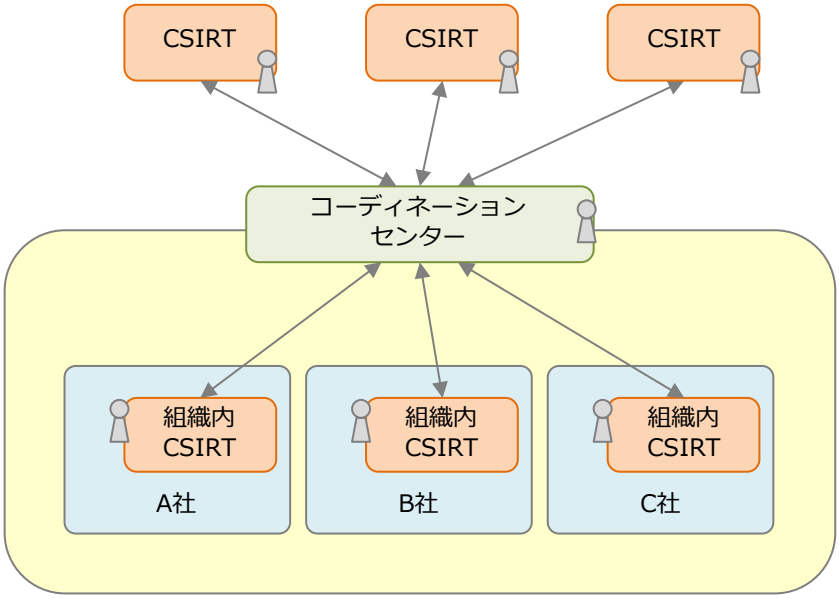
サービス対象は(広義の)国や地域。このようなサービス対象をもつ CSIRT は、国を代表するインシデント対応のための連絡窓口として活動する。



[図 1.2-2 国際連携 CSIRT のサービスモデル]

(3) コーディネーションセンター

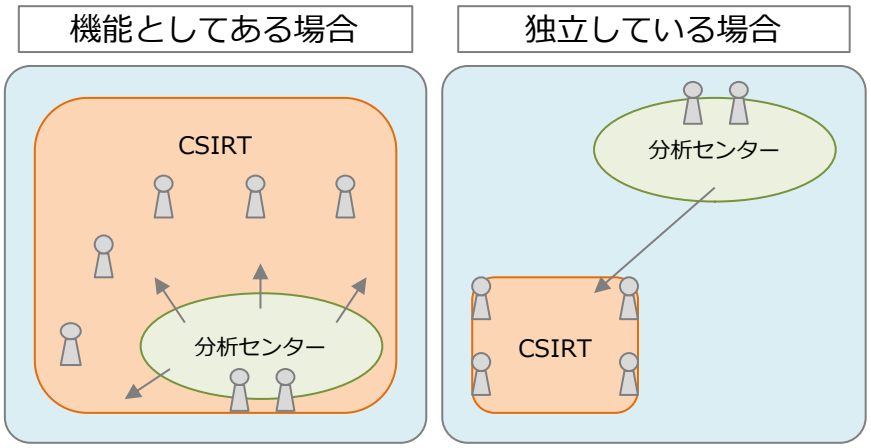
サービス対象は協力関係にある他の CSIRT。インシデント対応において CSIRT 間の情報連携、調整を行なう。グループ企業間の連携を担当する。



[図 1.2-3 コーディネーションセンターのサービスモデル]

(4) 分析センター

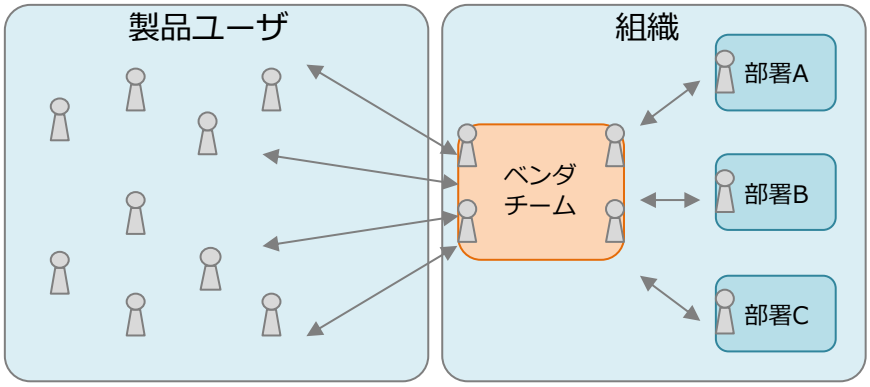
サービス対象は親組織または国や地域。インシデントの傾向分析やマルウェアの解析、侵入等攻撃の痕跡の分析を行ない、必要に応じて注意喚起を行なう。独立した組織の場合もあるが、CSIRT の中に機能として設けられる場合も多い。



[図 1.2-4 分析センターのサービスモデル]

(5) ベンダチーム

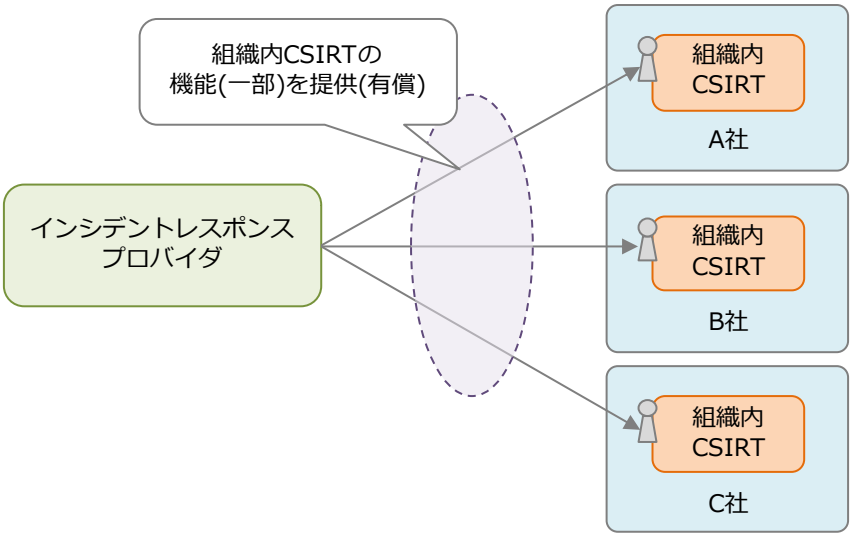
サービス対象は組織および自社製品の利用者（個人ユーザと法人ユーザの場合がある）。自社製品の脆弱性に対応し、パッチを作成したり、注意喚起をしたりする。組織内 CSIRT を兼ねるケースもある。



[図 1.2-5 ベンダチームのサービスモデル]

(6) インシデントレスポンスプロバイダ

サービス対象は顧客。組織内 CSIRT の機能 (の一部) を有償で請け負うサービスプロバイダ。セキュリティベンダ、SOC 事業者など。



[図 1.2-6 インシデントレスポンスプロバイダのサービスモデル]

なお本書は、上記分類のうち「組織内 CSIRT」に対象を絞っています。

CSIRT の中には、1 つの CSIRT で上記のように分類された機能を複数有しているものもあります。例えば、日本国内の既存の CSIRT の機能は、次のように分類できます。

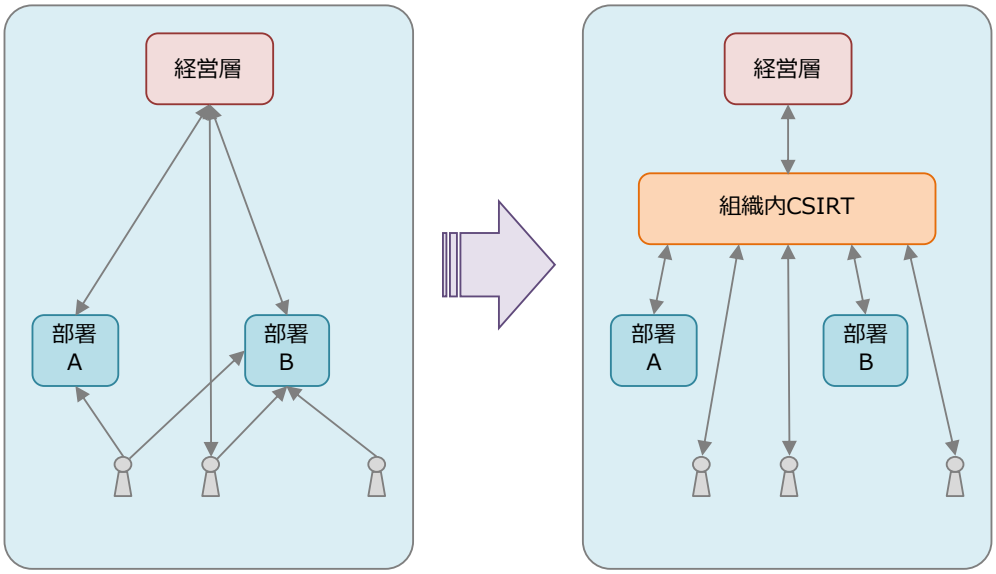
[表 1.2-1 既存 CSIRT の例]

	JPCERT/CC	A社 CSIRT	B社 CSIRT	C社 CSIRT	D社 CSIRT
組織内 CSIRT		○	○	○	○
国際連携 CSIRT	○				
コーディネーション センター	○	○			○
分析センター	○	○		○	
ベンダチーム					○
インシデントレスポンス プロバイダ				○	

2. CSIRT の必要性

CSIRT を構築することで得られる「メリット」には次のようなものがあります。

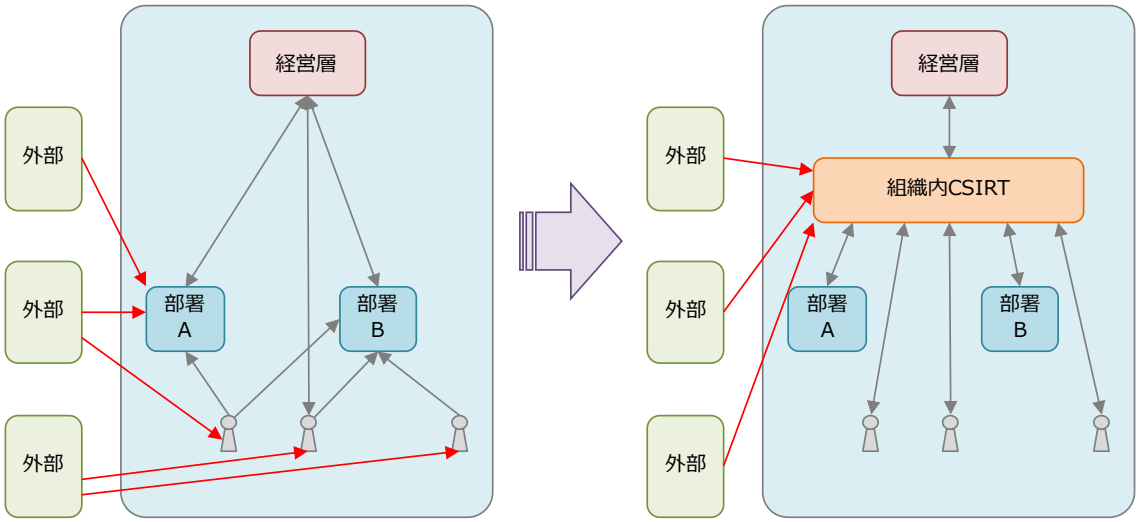
(1) 情報セキュリティ (インシデント関連) に関する情報管理



[図 2-1 組織内 CSIRT のメリットのイメージ 1]

CSIRT が存在しない場合、組織内で発生したインシデントなどの情報セキュリティに関する情報が各部署からばらばらとまとまりのない形で経営層に伝達されるため、経営層側で整理をしなければならなくなります。また、対応に関する指示は (一般的に専門的知識のない) 経営層から各部署に個別に行なわなくてはならなくなります。

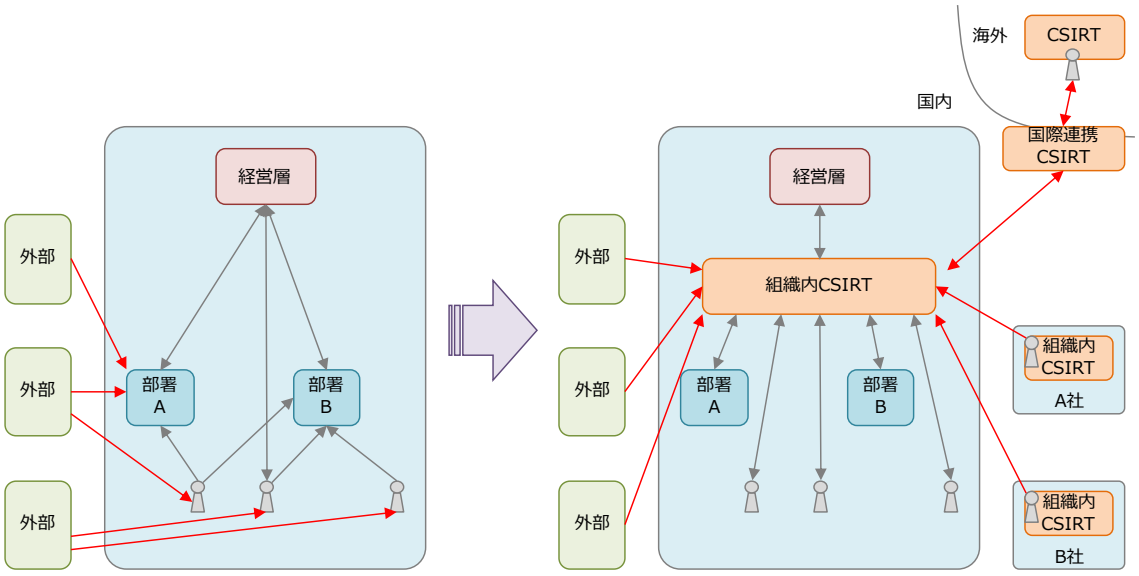
(2) (組織内のインシデントに関する) 統一された窓口



[図 2-2 組織内 CSIRT のメリットのイメージ 2]

(3) (外部との) インシデント対応に必要な信頼関係の構築

CSIRT が存在しない場合、組織内で発生したインシデントに関して外部から問い合わせを受ける窓口が一元化せず、複数の窓口に届けられた個々の情報間の連携、関連付けが難しくなり、結果としてインシデントへの対応が混乱し、遅れる可能性があります。



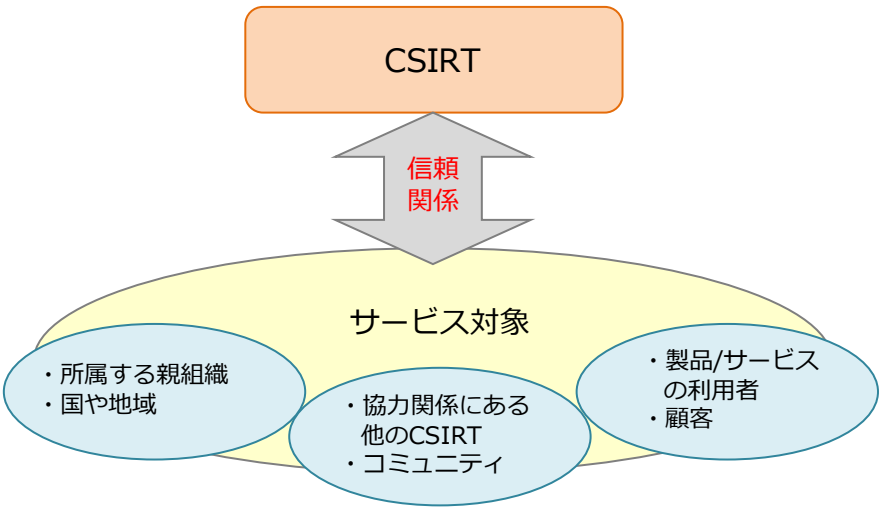
[図 2-3 組織内 CSIRT のメリットのイメージ 3]

インシデントに関する情報を他組織と共有することで自組織のインシデント対応に役立てることができます。しかし組織にとって「不名誉な情報」であるインシデント関連情報を外部に出すことは一般的に難しいことです。したがって、そのような情報を共有する上で最も必要なことは、お互いに関係者以外に情報を漏らさないという「信頼」です。しかし、CSIRT が存在しない場合、情報を提供する先が複数に分散してしまうため、一般的に信頼関係の構築は難しくなります。逆に CSIRT があれば、CSIRT が外部に対する「信頼の窓口」として機能することで組織間の信頼関係の構築が容易になるのです。

3. CSIRT に求められること

3.1 信頼の輪の重要性

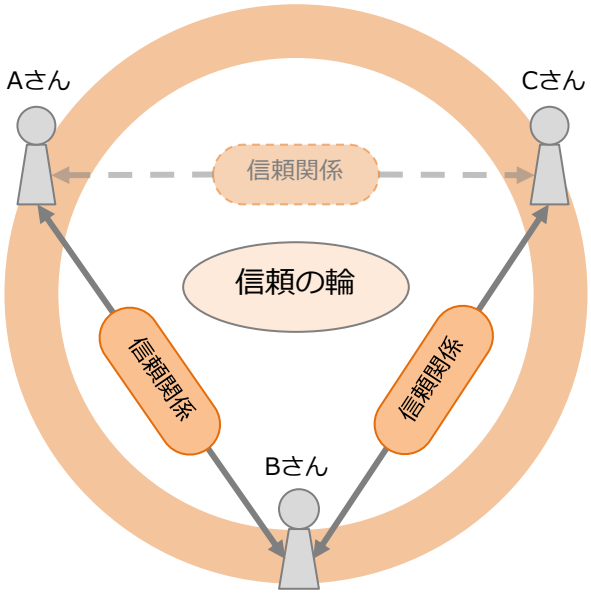
CSIRT にとって最も重要なものは「信頼関係」です。これは CSIRT が扱う情報がインシデントそのものに関する情報をはじめ、社内の機密にあたるものが多いからです。機密情報を適切に扱ってくれないような、「信頼」できない CSIRT にインシデント対応を依頼するサービス対象はいないでしょう。CSIRT が CSIRT たりうる最も重要な要素はサービス対象との「信頼関係」なのです。



[図 3.1-1 CSIRT は「信頼関係」が命]

また、CSIRT にとって必要とされる「信頼関係」はサービス対象との信頼関係だけにとどまりません。円滑なインシデント対応においては、他の CSIRT など、関連のある組織との情報連携・情報共有が欠かせません。具体的には、今どのようなインシデントが世の中で起こっていて、その原因や対策といったインシデント対応に必要な情報を、常に平常時から十分に把握しておけば、万が一自社において同じようなインシデントが発生しても速やかに対応することができ、復旧までの様々なコスト (時間、人手など) を軽減することができるのです。

しかしインシデントに関する情報は多くの場合、機密にあたります。そのため、インシデント関連情報を他者と共有するためには、まず何より、関係者以外に情報を漏らさないという「信頼」がお互いに必要です。そして、このような「信頼関係」に基づくコミュニティ＝「信頼の輪」によって共有できる情報の幅が広がり、結果として、CSIRT の活動に大きな効果を生むのです。



[図 3.1-2 信頼の輪]

A と B の間に信頼関係があり、かつ B と C の間に信頼関係がある場合、A と C の間に直接の面識がなくても、A と C の間に信頼関係を成り立たせることができる。

また、「信頼の輪」は CSIRT 同士のコミュニティにとどまりません。

CSIRT の活動の中心にあるインシデント対応において、必要に応じて事実を公表しなければならないことがあります。具体的には、情報漏えい事故により顧客の個人情報が漏えいした場合、その事実を Web や電子メールを通じて当該顧客に告知するだけでなく、告知対象が多い場合は、プレスリリースや記者会見などを通じて広く告知する必要があります。

このようなインシデントに絡む公表に際しては、対応を誤れば、組織の大幅なイメージダウンに繋がりかねないだけに、慎重に行なう必要があります。そのために、事実が歪曲されて伝えられることがないよう、普段からメディアとの「信頼関係」を構築しておくことが推奨されます。

3.2 信頼の輪の作り方

サービス対象からの信頼を得るためには、まず CSIRT の存在をサービス対象に充分に認知してもらうことがもっとも重要です。

具体的には、サービス対象が閲覧できる (社内) Web サイトを設置して、活動内容や問合せ先といった情報を掲載します。

また普段からサービス対象との情報共有を密に行ないます。

具体的には、CSIRT は常に組織内外問わず、特にサービス対象で発生する可能性が少しでも関わるインシデント及び関連する技術情報を積極的に収集し、それが社内システムにかかわる場合は担当する部署に対して情報提供をします。また一般社員にも必要とされるような情報であれば、社員向けに注意喚起を行ないます。更に社員向けの普及啓発セミナーやインシデント対応の予行演習の実施など、CSIRT の活動を普段から社員に示すことで信頼を得ることができるのです。

他にも、サービス対象に限らず、CSIRT 外部から CSIRT に何らかの問い合わせや要求が来た場合には、たとえそれが CSIRT にとって実際に対応すべきインシデント(または関連事項)でなくても、無視することなく、必ず何らかの形で反応を示すことも、CSIRT への信頼を得るために必要なことと言えます。例えば、対応できないのであれば、その旨、理由を添えて回答します。ただし、必ず反応すべきとは言っても、UCE(Unsolicited Commercial E-mail) などの「迷惑メール」に反応する必要は、もちろんありません。

一方、「コミュニティ」の形成や既存の「コミュニティ」への参加にあたっては、特に注意が必要です。

CSIRT の日常的な活動はインターネットを介した情報収集など、「顔が見えない」形でのコミュニケーションが中心になります。そのため、コミュニティも「顔が見えない」メーリングリストによるコミュニケーションだけで済んでしまうのではないかと思われがちですが、それではコミュニティは成立しません。

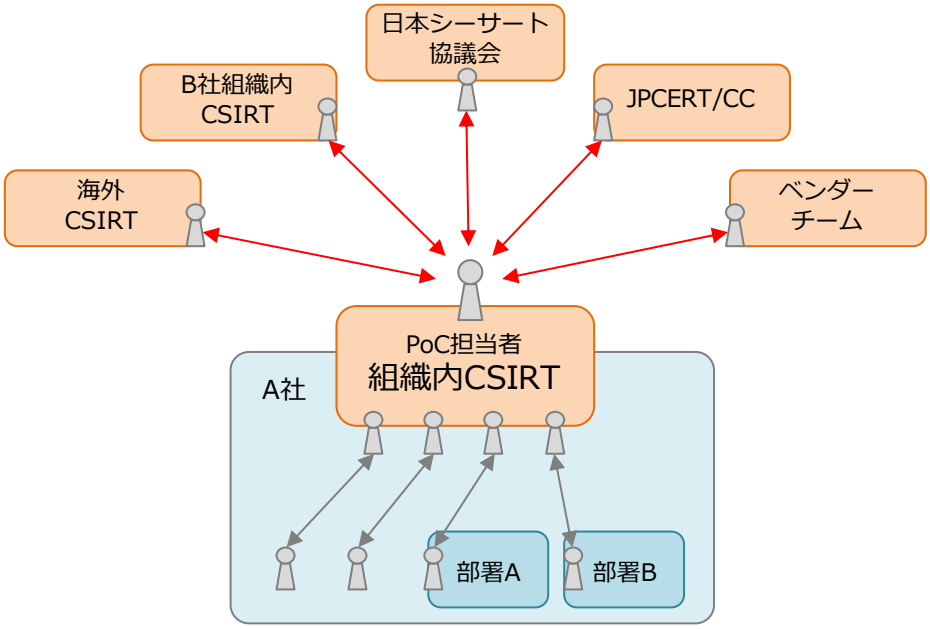
既に述べたように CSIRT の情報共有に必要なのは「信頼関係」です。この信頼関係は「顔が見えない」形でのコミュニケーションでは形成できません。まず直接、顔をあわせてのディスカッションや懇親会などを通じて、どの CSIRT にどのようなメンバーがいて、どのような活動をしているのか、またどのように情報が取り扱われているのかといったことを互いに「共有」することが求められます。特に密な情報共有を行ないたい CSIRT とはメンバー全員と互いに顔見知りになっておく場合もあります。

しかし現実にはメンバー全員と顔見知りになるのは難しいですし、メンバーの担当任務の内容によっては外部に顔を知られては困る場合もあるかもしれません。また複数のメンバーが対外的な活動をする場合は、CSIRT としての対外的な意識の統一が難しい場合もあるでしょう。

そこで通常は、各 CSIRT に PoC (Point of Contact) と呼ばれる「代表者」を用意し、その PoC が CSIRT の「顔」として他の CSIRT との信頼関係を構築したり、コミュニティとの情報共有の窓口としての役目を果たしたりします。
また、PoC には、あらかじめ CSIRT 間で取り決めたフローでは対応できないような「想定

外の事態」が発生した場合の「柔軟性のある」連絡窓口としての役目もあります。

PoC の存在は、組織における組織内 CSIRT の位置づけと同様に、外部との情報共有、連携の窓口という点で、「CSIRT 内の CSIRT 機能」と言い換えても良いかもしれません。



[図 3.2-1 組織内の CSIRT]

PoC は、CSIRT の顔としてコミュニティとの「信頼関係」を構築するために、国際会議や意見交換会などの、コミュニティのメンバーが集う場に継続的に参加し、積極的に交流を深め、「顔の見える」信頼関係を構築および維持するよう努める必要があります。

PoC は CSIRT を代表する立場であることから、CIO が兼務する場合もありますが、必ずしも組織としての代表者である必要はありません。実務レベルにおいて、責任を持って情報をコミュニティに提供できる権限とコミュニティから得られた情報を CSIRT 内で展開できる権限を有する必要があります。

また PoC に求められるものとしては、高いコミュニケーション能力とコミュニティで得られた情報を的確に判断して処理する能力、そして CSIRT の「顔」としての役目を果たせるだけの充分な知識とセキュリティを扱う者としての高い倫理観などが挙げられます。

注意しなければならないのは、PoC があくまで CSIRT を代表する「顔」にすぎず、「親組織」を代表しているわけではないという点です。つまり PoC を窓口として形成された信頼関係は、親組織対親組織 (会社対会社) ではなく、あくまで PoC 同士の個人の信頼関係を基盤とする CSIRT 対 CSIRT の信頼関係であるということを忘れてはいけません。

コミュニティとの情報共有には、様々な方法が使われます。日常的な情報のやりとりにはメンバーに限定されたメーリングリストが用いられます。必要に応じて暗号化機能を持ったメーリングリストを用いることもあります。暗号化の手法としては、PGP や S/MIME が

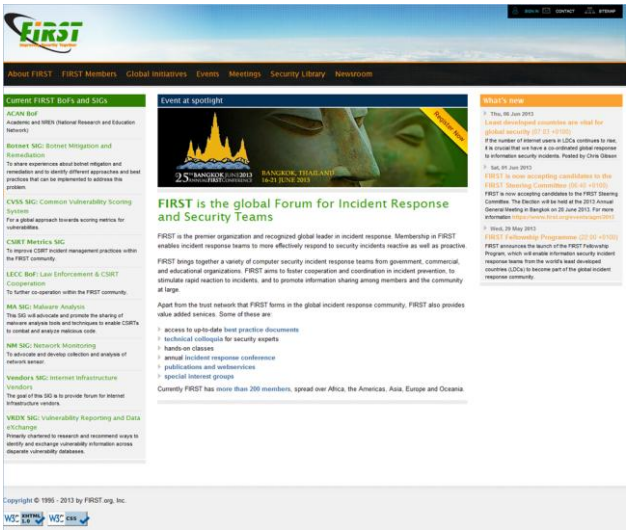
代表的ですが、CSIRT のコミュニティでは PGP が使われることが多いです。他にもメンバーのみが閲覧可能な Web サイトを設置する場合もあります。

3.3 CSIRT のコミュニティ

CSIRT によるコミュニティには次のようなものがあります。

(1) FIRST (Forum of Incident Response and Security Teams)

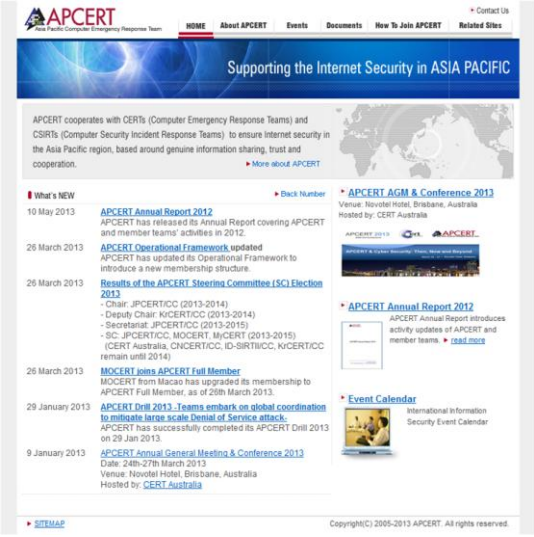
http://www.first.org/



CSIRT による国際フォーラム。FIRST が定めたルールに沿う CSIRT ならどのような CSIRT でも参加可能。

(2) APCERT (Asia Pacific Computer Emergency Response Team)

http://www.apcert.org/



アジア太平洋地域の CSIRT によるフォーラム。APCERT が定めたルールに沿う CSIRT のみ参加可能。

(3) 日本シーサート協議会 (日本コンピュータセキュリティインシデント対応チーム協議会、Nippon CSIRT Association)

http://www.nca.gr.jp/

日本国内の CSIRT によるフォーラム。日本シーサート協議会の使命および活動内容に賛同し、且つ協議会から得られた情報を適切に取り扱うことができる日本国内で活動するシーサートであれば、参加可能。

上記の 3 つのコミュニティはいずれも新規参加にあたっては既存メンバーによる推薦を必要としています。これは文字通り「信頼の輪 (Web of Trust)」の考えに基づくものです。

また、国際フォーラムである FIRST では各参加 CSIRT に必ず 1 名の Rep (Representative、代表者) の存在を義務付けています。これは PoC と同義で、各 CSIRT を「代表」して、コミュニティ (厳密には FIRST の事務局) との連絡窓口の役目を果たします。

4. CSIRT の位置づけ

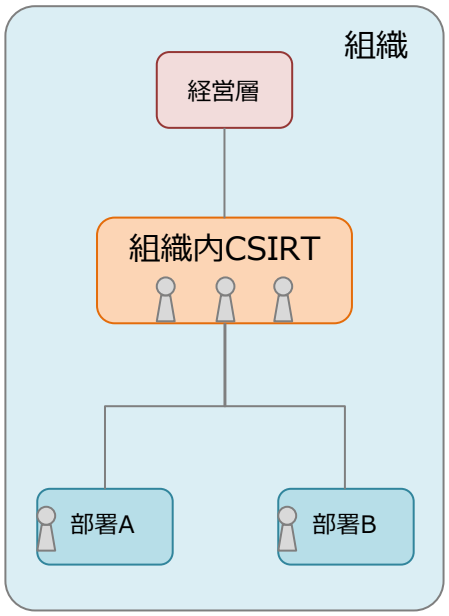
CSIRT は、組織によってサービス内容が異なるだけでなく、そのサービス内容によって実装も大きく異なります。

厳然たるチーム (=部署) として実装される場合もありますが、バーチャルなチームとして、他業務と兼務するメンバーによる「CSIRT 機能」として実装される場合もあります。また文字通りチームとして複数のメンバーによって構成されることもあれば、規模の小さな組織では CSIRT 機能を有した個人である場合もあります。

ここでは、CSIRT (およびその機能) を組織としてどのような位置づけにすべきか、いくつか例を挙げて紹介します。

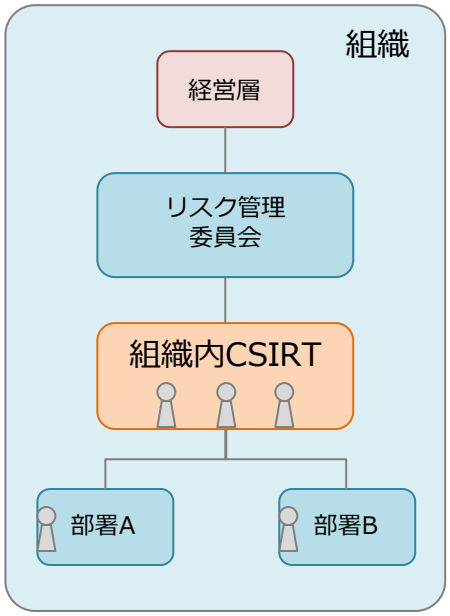
(1) 経営層直下にある場合

経営層から委譲された権限の下、各部署と連携します。



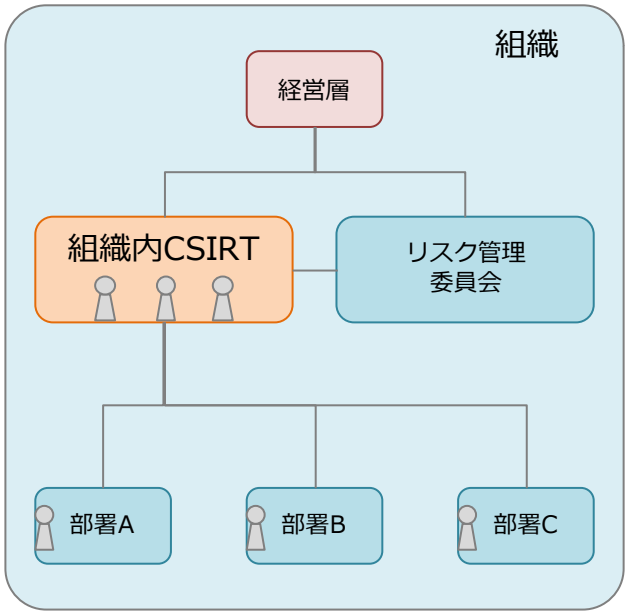
(2) 経営層直下にあるリスク管理委員会の下にある場合

リスク管理委員会から委譲された権限の下、各部署と連携します。



(3) 経営層直下にあり、リスク管理委員会と並立している場合

経営層から委譲された権限の下、各部署およびリスク管理委員会と連携します。



5. CSIRT にあらかじめ必要なこと

ここでは、CSIRT を構築するにあたって、あらかじめ決めておかなければならないこと、やらなければならないことを紹介します。

5.1 サービス対象の明確化

既に 1.2 でも説明したように、CSIRT にとって重要なのは、まず「誰のインシデント」に対応するのか、つまり CSIRT にとってのサービス対象者 (活動範囲) が誰であるかということを明確に定義することです。

5.2 活動目的の明確化

CSIRT の活動目的を明確にしておく必要があります。被害の局限化・最小化、被害からの迅速な復旧など、いくつかの目的が考えられますが、それらのうち、どの目的を最優先するかといった優先順位付けをしておくことで、あらかじめ対応マニュアルを用意していない「予期せぬインシデント」にも速やかに対応できるようになるのです。

また「何のための CSIRT なのか？」を明確にすることで、その CSIRT が提供すべきサービス内容や CSIRT の具体的な実装も変わってきます。

ミッションの例

- 会社内および子会社の従業員に対して、コンピュータセキュリティインシデントによる被害を軽減および局限化するための環境およびシステムの構築を支援する。
- 会社内および子会社の従業員に対して、コンピュータセキュリティインシデントが発生した場合の対応を支援する。
- インターネット接続サービスを契約している顧客が、そのインターネット接続サービスを起因とするコンピュータセキュリティインシデントに巻き込まれた場合、その被害を軽減し、迅速に復旧する。
- ○○グループ内で発生したコンピュータセキュリティインシデントの検知、解決、被害の軽減・局限化および発生の予防を支援することにより、○○グループのセキュリティの向上に貢献する。

5.3 サービス内容の定義

CSIRT は、サービス対象に対して提供するサービス (活動内容) を定義し、サービス対象にあらかじめ告知しておく必要があります。具体的な活動内容は、サービス対象のニーズに応じて変わります。

CSIRT のサービス内容を定義する際にありがちな誤解として、CSIRT が経営層による社員の監視といった「ガバナンス(統制)」のための機能であるというものがあります。しかし、CSIRT はあくまでサービス対象のインシデントに対して「中立な立場で」対応するためのものです。したがって CSIRT のサービスを定義する際には、サービス対象に対するヒアリングや過去に実際に発生したインシデントや今後想定されるインシデントを可能な限り詳細に分析しておく必要があります。また技術の進歩や取り巻く環境、状況の変化に応じて、適宜サービス内容を見直し、再定義することも重要です。

[表 5.3-1 サービスリストの例]

事後対応型サービス	事前対応型サービス	セキュリティ品質管理サービス
・アラートと警告 ・インシデントハンドリング - インシデント分析 - オンサイトでのインシデント対応 - インシデント対応支援 - インシデント対応調整 ・脆弱性ハンドリング - 脆弱性分析 - 脆弱性対応 - 脆弱性対応調整 ・アーティファクトハンドリング - アーティファクト分析 - アーティファクト対応 - アーティファクト対応調整	・告知 ・技術動向監視 ・セキュリティ監査または審査 ・セキュリティツール、アプリケーション、インフラ、およびサービスの設定と保守 ・セキュリティツールの開発 ・侵入検知サービス ・セキュリティ関連情報の提供	・リスク分析 ・ビジネス継続性と障害回復計画 ・セキュリティコンサルティング ・意識向上 ・教育 / トレーニング ・製品の評価または認定

実際には、CSIRT によってサービスリストの種類及びそれらの定義づけが異なります。

ところで、提供するサービスを決める際には、もう 1 つ重要な点があります。
当然のことながら CSIRT のリソースは無限ではありません。したがって、全てのインシデントに対応できるとは限りませんので、優先順位付け (トリアージ) の基準をあらかじめ定めておく必要があります。そのためには、まず対応すべきインシデントを定義し、分類しておきます。そして、定義付けし、分類分けしたそれぞれのインシデントに対して対応マ

ニュアルを作成しておきます。なお、対応マニュアルについては、別冊の「インシデントハンドリングマニュアル」を参照してください。

5.4 通信チャネルの設置

対応するインシデントの内容によっては、CSIRT メンバーだけで対応し切れない場合が多々あります。まず当事者であるサービス対象からの情報提供などの協力、連携が重要であることはもちろん、サービス対象でない当該インシデントの当事者との連携が必要なこともあります。例えば、自組織から他組織に対する攻撃 (逆の場合もある) の可能性が指摘された場合、当事者である他組織に事実確認を依頼する必要があります。

そこで、サービス対象および当該インシデント関係者との間の通信チャネルを用意し、その方法を明示しておくことが推奨されます。まず Web サイトの URL、連絡用メールアドレス、電話番号など用意した通信チャネルに関する情報をサービス対象に確実に告知します。また、サービス対象以外からの連絡 (通報、問い合わせ) が想定される場合は、親組織の Web サイトなどに連絡方法を明記します。

6. インシデントハンドリング概論

6.1 インシデントマネジメント、ハンドリング、レスポンス

CSIRT がインシデントに対して行なう業務(広義のインシデント対応)は大きく次の 3 つにステージに分類されます。

(1) インシデント発生前

CSIRT が平常時に行なう日常業務であり、万が一のインシデント発生に備えた「準備」の活動でもあります。

CSIRT の日常業務としては、一般的に「セキュリティ対策」と呼ばれることの多い、ウイルス検知ソフトやファイアウォールの導入など、インシデントの未然防止策の実施が代表的なものとされています。

しかし CSIRT の日常業務として最も重要なのは、インシデントに関する情報の収集とそれが自組織のシステムに与える影響の分析、そして自組織のリスク許容度を評価することです。日々、大量に提供されるセキュリティ関連情報の中から自組織のシステムに関係するものをピックアップし、現時点で当該システムが晒されている脅威を把握し、必要な対策(パッチの適用、設定変更など)を講じることでインシデントを未然に防ぐ可能性が高まります。またインシデントを防ぐことができなくても、被害を最小限に抑えたり、被害から復旧したりする上で必要な情報を蓄積しておくことで、対応が速やかに行なえるようになるのです。

更に、システム管理者のみならず、一般社員も知っておく必要がある情報があれば、普及啓発のセミナーを開いたり、緊急を要するものであれば、注意喚起を行ったりします。

また、万が一のインシデント発生時に備えて、「異常」を速やかに検知する仕組み (装置および体制) を導入し、インシデント検知後の対応マニュアルを整備しておくことが重要です。そして、一連の対応手順が有効であることを確かめる目的で、予行演習を定期的に行なうことが推奨されます。これは、防災訓練のように実際に作業を行なうようなスタイルもあれば、マニュアルどおりに連絡が取れるかといった「コミュニケーションチェック」のみを行なう場合もあります。予行演習により問題が見つかった場合は、対応マニュアルなど、一連の対応手順を修正します。

(2) インシデント発生時

インシデントが発生したときに、被害を局限化、最小化し、速やかな復旧につなげることを目的とする活動です。

まず大事なのは、インシデントを速やかに検知することです。CSIRT 自らが検知するための仕組み (装置および体制など) が必要であることはもちろん、外部からの通報を受け付ける窓口を設置することも重要です。インシデントの内容によっては自らでは検知しにくいものもあり、そのようなインシデントは多くの場合、外部からの通報で知ることができるのです。

また、CSIRT の資源は無限ではありませんので、同時に複数のインシデントに対応しなければならないような場合には、個々のインシデントに対して、あらかじめ決めた基準に従って、優先順位付け (トリアージ) をします。高度サイバー攻撃(APT)を検知したのであれば、高度サイバー攻撃(APT)によるリスクと自組織のリスク許容度、直ちに脅威を排除するべきか、範囲特定を試みるべきか等について討議し、対応方針を検討しなくてはなりません。

あとは対応マニュアルやチェックリストにしたがって、必要な関係者への連絡やハードウェアもしくはソフトウェアの対応(ネットワーク切断、電源オフ、設定変更など)を実施する、あるいはインシデント範囲の特定をしてから脅威の排除を実施します。

(3) インシデント発生後

インシデントから復旧し、再発を防止することを目的とする活動です。

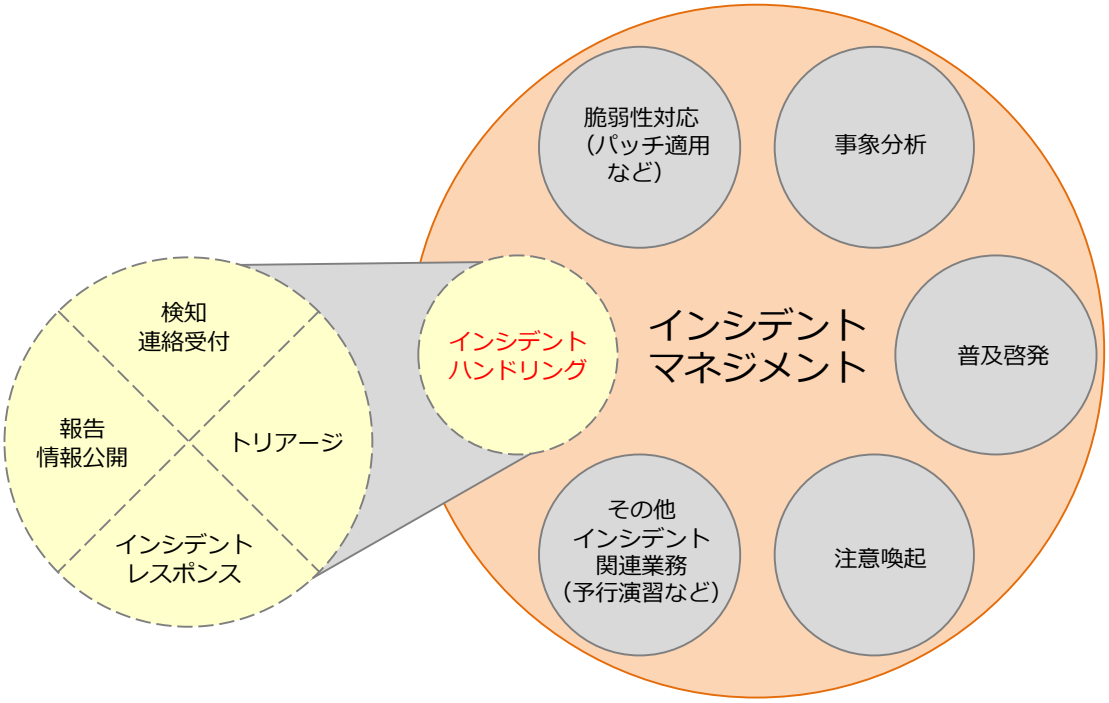
インシデントによる被害から復旧し、システムを元の状態に戻しても、インシデントの原因を取り除かなければ、同じインシデントが発生してしまいます。そこで、まず行なわなくてはならないのはインシデントの直接の原因の究明です。インシデントの原因としては、パッチの適用忘れや設定間違いといった初歩的なミスから、未知の脆弱性の悪用まで、様々なものがあり、場合によっては外部の専門機関に判断を委ねなければならないほど複雑で究明が困難なケースもあります。とにかく原因を究明し、その原因を取り除くまでは、元に戻しただけの状態のシステムを運用に移すのは大変危険です。

ここで重要になってくるのは、原因究明に必要な情報収集であり、特に外部の信頼できる組織との情報共有が有効に働く場合があります。

原因を究明し、同じインシデントが発生しないような対策(パッチ適用、ファームウェアの更新、設定変更など)を講じた上で、システムを運用に戻します。その後、インシデントの原因が生じた理由を究明し、同じ原因が生じないようにします。例えばパッチの適用忘れが起こった理由を調べ、既存の運用ポリシーに問題があれば、見直します。

また対応において使用したマニュアルに、実施上の問題がなかったかを確認し、必要に応じて修正、改訂します。

このような、インシデントに対して CSIRT が行なう一連の業務をまとめて「インシデントマネジメント」と呼びます。また、このうち「(2)インシデント発生時」と「(3)インシデント発生後」のような実際に発生したインシデントに対して行なう一連の業務を「インシデントハンドリング」と呼び、特にその中で、インシデントに実際に対応する業務を「インシデントレスポンス」と呼びます。これらの関係を示したのが次の図です。



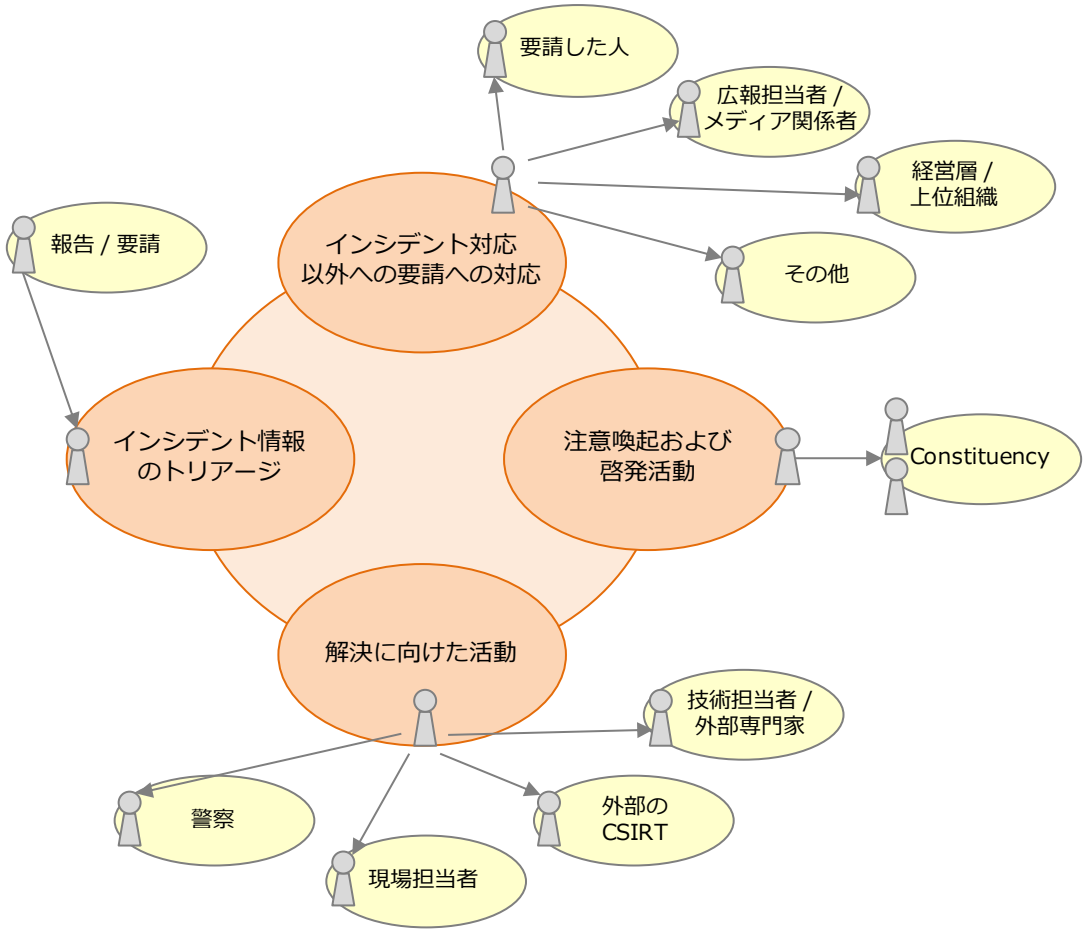
[図 6.1-1　インシデントマネジメント、ハンドリング、レスポンスの関係]

ただし、これらの区別は厳密なものではなく、CSIRT によって異なります。

以降は、これらのうち、実際に発生したインシデントに対して行なう「インシデントハンドリング」について詳細に解説します。

6.2 インシデントハンドリングの機能

前節では「業務」の視点で説明しましたが、「機能」の視点で見た場合、「インシデントハンドリング」は「インシデント情報のトリアージ」、「解決に向けた活動」、「注意喚起及び啓発活動」、「インシデント対応以外の要請への対応」の 4 つの機能から成り立っています。



[図 6.2-1　4 つの機能の関連]

（1）インシデント情報のトリアージ

CSIRT が対応すべきインシデントに対して一次分析を行い、その内容や深刻度、緊急度などから対応の優先順位付けをします。この順位付けの判断基準はあらかじめ可能な限り詳細に定めておく必要があります。このトリアージのタイミングで高度サイバー攻撃(APT)を検知できる場合もあります。

（2）解決に向けた活動

当該インシデントに関連したサイトや他の CSIRT、必要に応じて専門家などと情報をやりとりし、必要な対応につなげます。

（3）注意喚起及び啓発活動

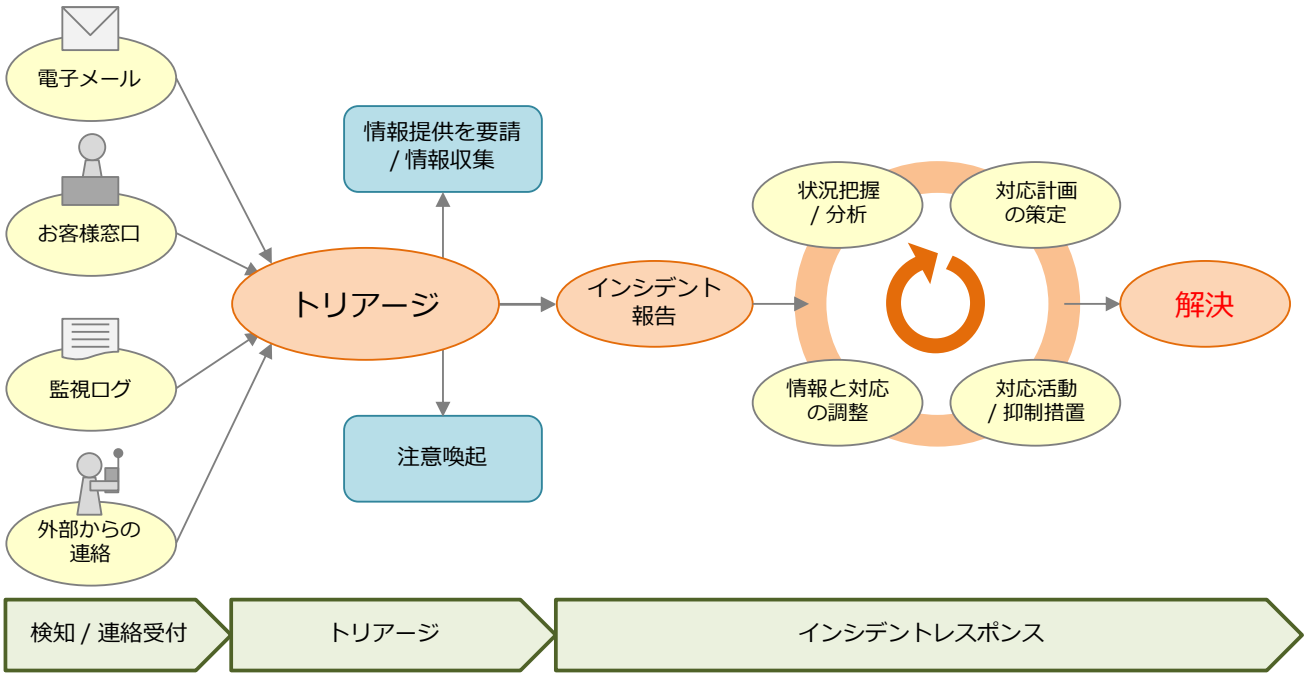
インシデントの被害拡大の防止などを目的にサービス対象に対して注意喚起や普及啓発を行ないます。

（4）インシデント対応以外の要請への対応

インシデント対応の結果 (顛末など) を、当該インシデントについて CSIRT に対応を要請した方や関係者(上位組織や監督官庁など)に報告したり、必要に応じて広報担当者を通じて情報を公開したりします。

6.3 インシデントハンドリングの流れ

代表的なインシデントハンドリングの流れを示したのが次の図です。



[図 6.3-1 代表的なインシデントハンドリングの流れ]

監視システムなどからの情報や外部からの通報などで検知または認知したインシデントを、必要に応じた外部との情報共有などに基づいてトリアージして、実際に対応すべきインシデントか否かを判断します。対応すべきインシデントに対しては、状況の把握、分析を行ない、対応計画を策定します。インシデントが高度サイバー攻撃(APT)によるものだと判断

される場合は、インシデントによるリスクと組織のリスク許容度に基づいて取るべき措置を検討します。脅威を排除することよりもインシデントの範囲特定を優先とするかを判断し、対応計画に盛込みます。

次に策定した計画に基づいて対応を行ない、抑制措置や範囲特定を実施します。その後、実施した対策が適切であったかを関連情報の調整を行なうことで確認し、必要であれば、改めて状況の把握と分析を行ない、対応計画を練り直します。このような「繰り返し」の結果として最終的な解決に導きます。

7. CSIRT 構築にあたって

7.1 CSIRT のメンバー

インシデントが IT に基づくものであることから、CSIRT のメンバーには IT に関する技術的専門知識が必要とされることは確かです。しかし、そのような専門知識や IT 分野における経験は、ないよりはあるに越したことはありませんが、CSIRT メンバーとして必ずしも「必須要件」とはなりません。

これまで説明してきたように、CSIRT に最も必要な「信頼」を維持し、そして速やかに且つ的確にインシデントに対応するためには、関係者とのコミュニケーションが最も重要です。

したがって、CSIRT メンバーに必ず必要とされるのは、サービス対象をはじめとする CSIRT メンバー以外の外部の関係者とのコミュニケーションを適切に取ることができる能力、そして「個人プレイ」に走ることなく、チームメンバー間で情報を共有し、「チームプレイ」で動ける能力です。

CSIRT がサービス対象に対して提供するサービス内容によって、当然ながら、メンバーに求められる能力に違いはありますが、一般的に、技術的な知識や経験が不足していても、優れた対人スキルとコミュニケーション能力のある人材を起用し、CSIRT 特有の技術的知識を身に付けさせるほうが、その逆より望ましいと言えます。

また、CSIRT メンバーの「心得」として、**サービス対象に対して情報セキュリティを担う者としての模範たる姿勢を示すこと**が求められます。これがなければ、CSIRT に対するサービス対象からの信頼を獲得し、維持することはできません。

7.2 設備

CSIRT が扱う情報の多くは機密情報です。したがって、その管理には充分なセキュリティ対策が必要です。ここでは一般的なセキュリティ対策の他に、CSIRT に特徴的な設備として既存 CSIRT で広く用いられているものについて簡単に紹介します。ただし、これはあくまで「例」であり、必ずしもここで紹介したものと同等以上のものが必須というわけではありません。セキュリティポリシーやサービス内容、災害時におけるサービスの継続性などに応じて必要なものを選択してください。また設計にあたっては、CSIRT メンバーの「心得」と同様、情報セキュリティを担う部署または機能として、サービス対象に対して「模範」的なものであることが強く求められます。

(1) 執務スペース

セキュリティ上安全に保護すべきエリアを明確に定義(レベル分け)し、保護の必要のないエリアとは完全に分離します。一般的に、保護されたエリアへ入るには物理鍵以外の認証方法が使われます。例えば、既存 CSIRT では、生体認証や IC カード、暗証番号などが単一

もしくは複数の組み合わせで用いられています。

(2) 通信設備 

インターネット(電子メールなど)

- サービス対象をはじめとする外部からの連絡を受け付けるアドレス宛に送られてきたメールは、複数のユーザが何らかの形で確実に見られるようにしておきます。
- 暗号化および電子署名付きメールが使えるようにしておきます。なお、CSIRT のコミュニティでは PGP/GnuPG が事実上の標準となっています。
- CSIRT がやり取りするメールなどを CSIRT メンバー以外が読むことがないように、メールサーバやそこへの外部からの配送経路、また外部とのインターネット接続を、CSIRT 以外の業務と分離しておくとよいでしょう。
- 電話およびファックス
- CSIRT メンバー以外がアクセスすることがないように、CSIRT 以外の業務を行なう場所とは物理的に切り離された(アクセスに何らかの認証が必要な) 場所に電話機およびファックス装置を設置します。
- (主に CSIRT コミュニティからの) 緊急時の連絡が可能な電話番号を用意します。多くの場合、CSIRT の PoC 担当者の携帯電話に繋がるようにしておきます。
- 他の業務で用いられている番号へ誤って繋がることがないように、似た番号を使うのを避ける場合もあります。

(3) データ管理・破棄 

機密情報については、紙や CD-R などの物理的なものは耐火金庫、電子データは暗号化ファイルシステムを用いたハードディスク上に保管しておくことがあります。また物理データの破棄用に、紙だけでなく CD-R などについても粉砕できるシュレッダーを用意します。

(4) インシデントトラッキングシステム(ソフトウェア) 

一般的に CSIRT ではインシデントの対応進捗状況を管理するシステムが使われています。このようなトラッキングシステムとして、オープンソースのソフトウェアである RTIR (Request Tracker for Incident Response) などが有名ですが、多くの CSIRT では独自に開発したシステムが使われているようです。

RTIR: RT for Incident Response <http://bestpractical.com/rtir/>