シーサート

企業におけるCSIRTの役割

～情報漏えいへの対応～

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
運営委員長　寺田真敏

2015年07月14日

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team (CSIRT、シーサート)体制による活動への期待が高まっています。日本シーサート協議会は、連携と問題解決の場の提供を通して、シーサート活動を支援しています。
本講演では、日本シーサート協議会の活動ならびに企業におけるシーサートの役割を紹介します。

- 情報漏えいへの対応
- シーサートとは
- 日本シーサート協議会の活動
- 企業におけるシーサートの役割

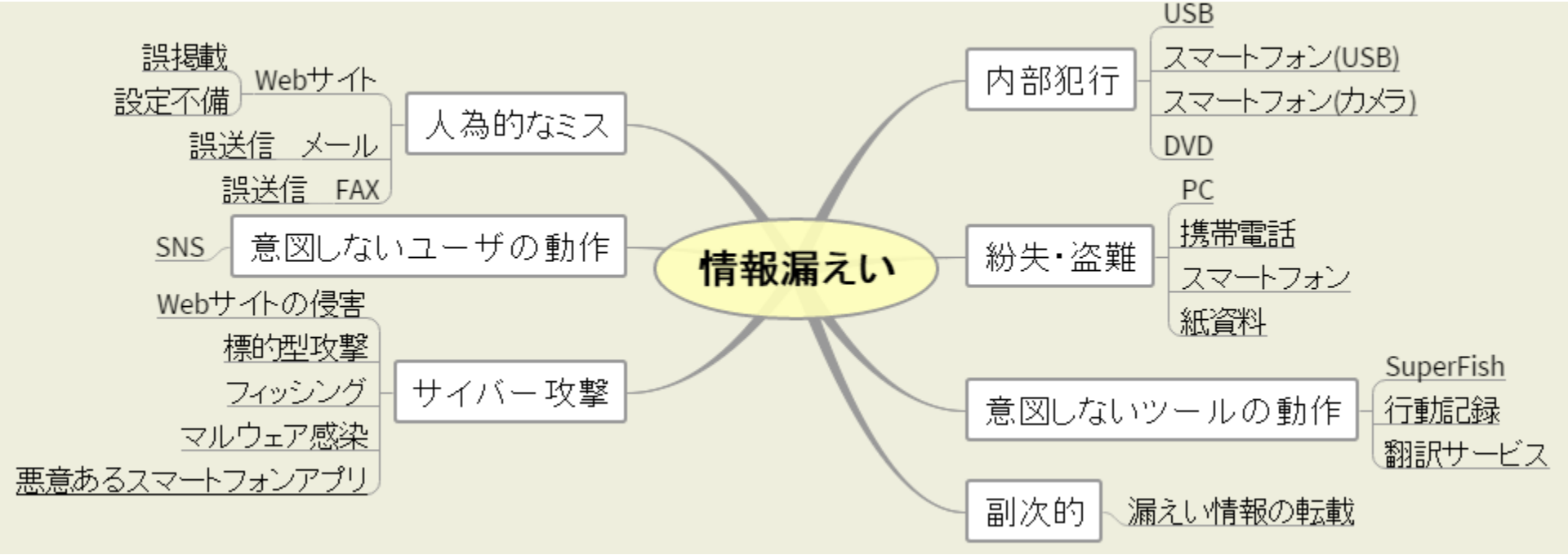
1 情報漏えいへの対応

- NISTサイバーセキュリティフレームワーク
  - サイバーセキュリティリスクを把握・管理し、サイバーセキュリティリスクを低減するためのアクションと優先順位付けの実現

機能	内容
特定 IDENTIFY	リスクの特定 どこにどの様な攻撃が？
防御 PROTECT	状況に応じた防御策の実施 ベターな防御策は？
検知 DETECT	イベントの検知 攻撃の早期発見
対応 RESPOND	防御を突破された際の対応 インシデントの分析、軽減策検討
復旧 RECOVER	復旧計画の作成、改善、伝達

1 情報漏えいへの対応

- **特定 (IDENTIFY)： どこにどの様な攻撃が？**



セキュリティ機能は危殆化し、また、攻撃は進化する。
⇒ グッドプラクティスの共有

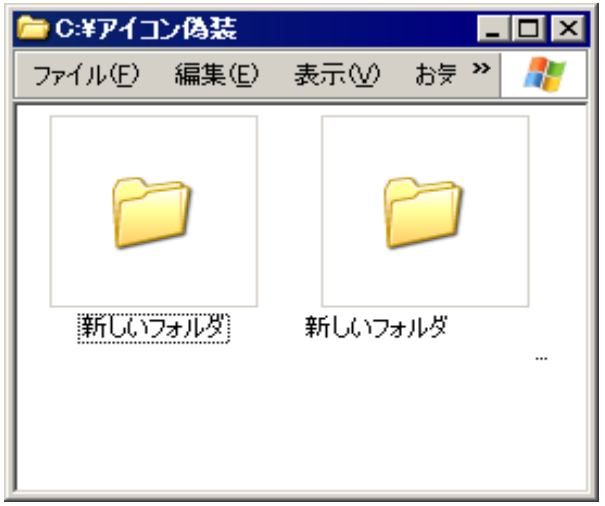
1 ソーシャルエンジニアリング攻撃

- 社会工学的な観点から発生する脆弱性（人間の心理的な隙や行動上の隙）を利用した攻撃方法
  - 人間の心理的な隙を利用する事例
    - コンピュータ管理者になりすまして、「（システム管理上）あなたのパスワードを送ってほしい」というメールを送り、パスワードを聞き出す
    - 電話や、面と向かって個人情報を盗み出そうと働きかける
  - 人間の行動上の隙を利用する事例
    - ゴミ箱に廃棄された紙ゴミから重要情報を読み取る
    - 肩越しに画面や利用者の手の動きからパスワードを盗み見る

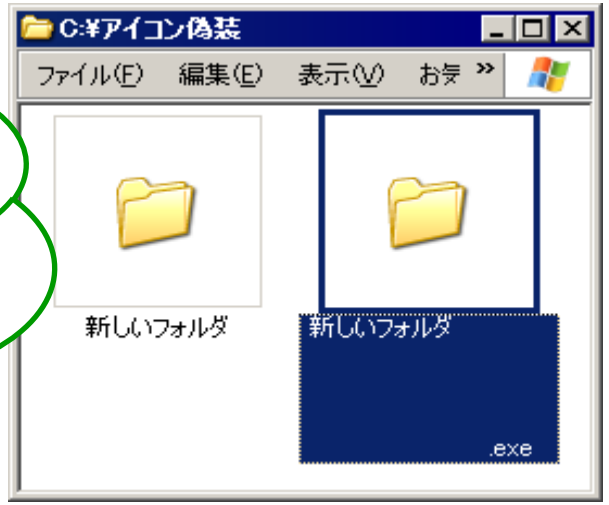
1 ソーシャルエンジニアリング攻撃
問題のない操作であると勘違いさせる

- **【アイコン偽装＋ファイル名偽装】**
  Anntinny(2003年)

  情報漏えいウイルスとも呼ばれ、Winnyでの情報漏えい被害を発生させた
  アンティニィ(Antinny)は、実行可能ファイル(＝ウイルス本体)をアイコン偽装していた。

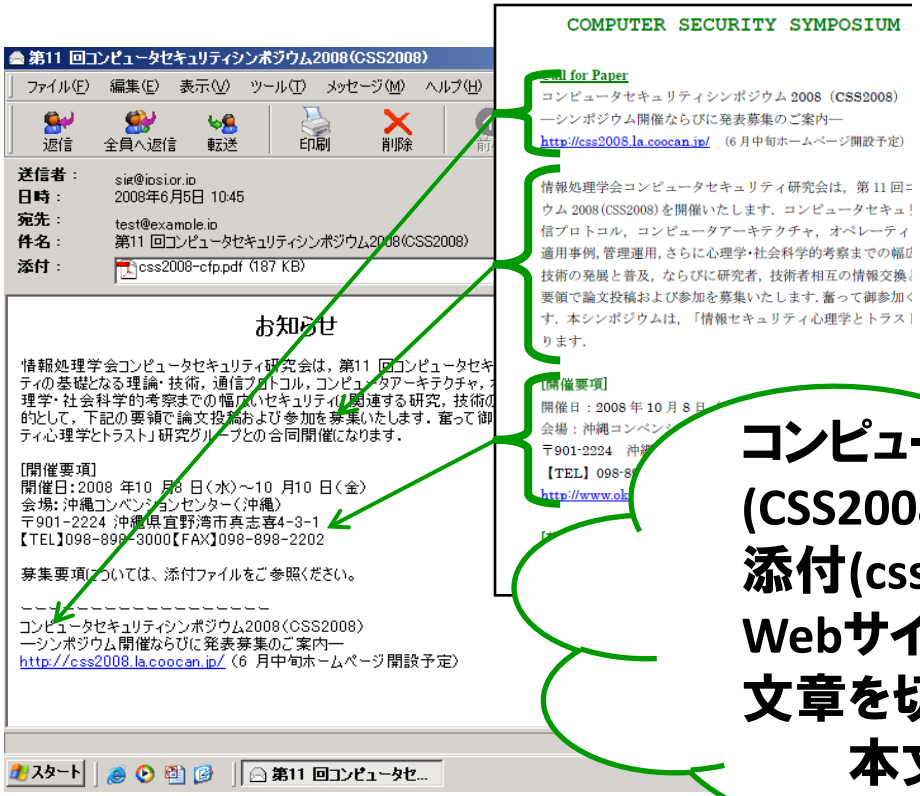


右側のアイコンは一見フォルダに見えるが、
実はフォルダと同じアイコンを表示する、
非常に長いファイル名
(コピー～新しいフォルダ2・・・空白文字・・・.exe)
を使って偽装された実行可能ファイル
(＝ウイルス本体)である。



1 ソーシャルエンジニアリング攻撃 本物を活用する

- 【再利用：カット＆ペースト】
  標的型攻撃メール(欧米2005年～、国内2005年～)



2008年あたりから、「怪しいメールには気をつけなさい」という注意喚起では通用しなくなる事例が出始めた。この頃から、サイバー攻撃の活動基点が「怪しい」から「怪しくない(怪しさを感じさせない)」に切り替わり始めた。

コンピュータセキュリティシンポジウム2008(CSS2008)の募集要項を装ったウイルス添付(css2008-cfp.pdf)メールである。
Webサイトに掲載されているPDFから文章を切り貼りして電子メールの本文が作成されている。

1 2010 年　Advanced Persistent Threat
攻撃対象を狙い撃ちした高度な潜伏型攻撃

- 特定組織を対象とし(標的型)、
  組織内ネットワークを活動基点とした(潜伏型)侵害活動

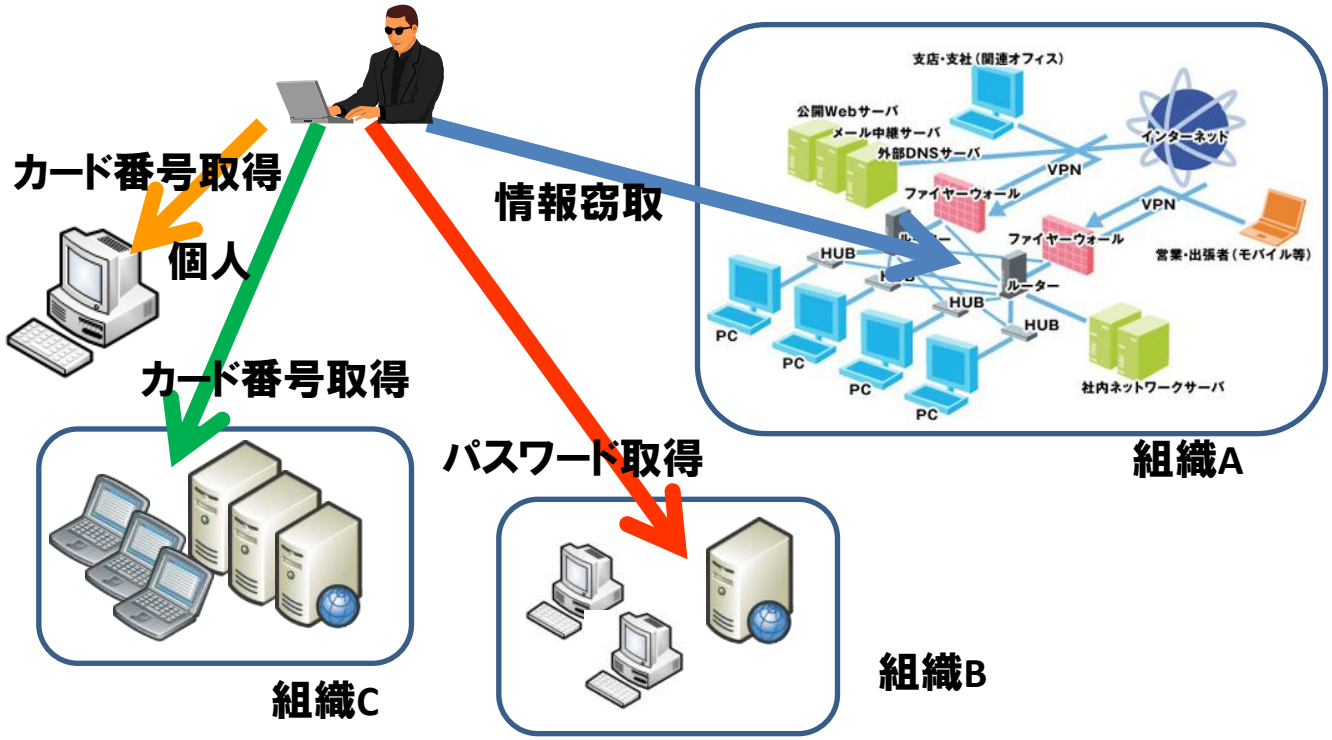
- 【初出】オンライン誌Bloomberg Businessweek (2008年4月)
  An Evolving Crisis - BYZANTINE FOOTHOLD
  2007. A new form of attack, using sophisticated technology, deluges outfits from the State Dept. to Boeing. Military cyber security specialists find the "resources of a nation-state behind it" and call the type of attack an "advanced persistent threat." •••
  2006年頃から始まった米国政府や米国軍事関連企業を標的とした攻撃

- 【普及】マカフィー作成の「重要資産の保護」レポート(2010年1月)
  オーロラ攻撃など、標的型サイバー攻撃からの防護方法を詳述

1 攻撃のモデル化と対処【単独型の標的型攻撃】

- 【事例】アカウント、パスワード、カード番号などの情報収集、情報窃取、動作阻害など、個々の機器に侵入した後、用途毎のツールをインストールして遠隔操作

簡易モデル



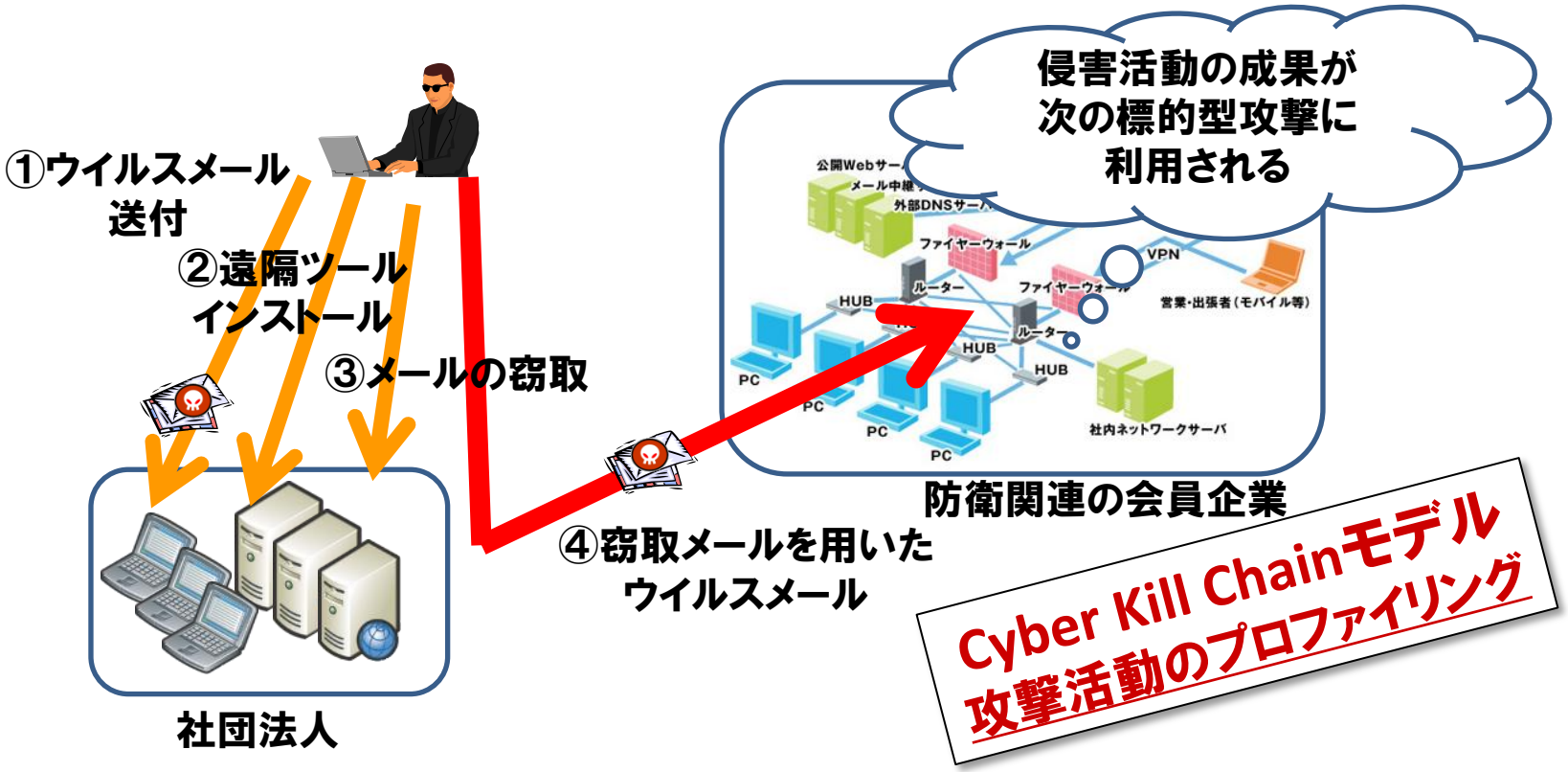
1 攻撃のモデル化と対処【モデル：簡易モデル】

- 特定組織を対象とし(標的型)、
  組織内ネットワークを活動基点とした(潜伏型)侵害活動

A	Step1(侵入)：ソーシャルエンジニアリングを用いた攻撃 ● 標的型メール ● 悪意あるWebサイトへの誘導(⇒ウイルス：Gumblar) ● USB経由(⇒ウイルス：Conficker)	共通攻撃
P	Step2(潜伏)：潜伏中は外部との通信環境を維持 ● 攻撃指令管理ホストとの接続 ● 新たな機能や自身の更新のためファイルダウンロード	
T	Step3(窃取や妨害)：最終目標(脅威)に合わせて変更 ● ソフトウェア構成管理システムへの攻撃(⇒オーロラ攻撃) ● 機密情報の窃取(⇒ナイトドラゴン、米EMC社) ● 制御システムの動作妨害(⇒スタクスネット)	個別攻撃

1 攻撃のモデル化と対処【連鎖型の標的型攻撃】

- 【事例】2011年10月、社団法人のコンピュータが、情報を窃取するタイプのウイルスに感染していた(①～③)。さらに、窃取されたメールにウイルスが仕込まれ、防衛関連の会員企業に対する標的型攻撃メールに転用されていた(④)。



1 攻撃のモデル化と対処【モデル：Cyber Kill Chain】

- Kill Chain(F2T2EA)
  米国空軍の軍事コンセプトで、発見(Find)⇒ 固定(Fix)⇒ 照準(Targeting) ⇒ 追跡(Track)⇒ 交戦(Engage または Employ)⇒ 査定(Access)の6段階からなるサイクル

- Cyber Kill Chain＝Kill Chainのコンセプトをサイバー攻撃に応用
  ① Reconnaissance(偵察)
  ② Weaponization(武器化)
  ③ Delivery(配送)
  ④ Exploitation(攻撃)
  ⑤ Installation(インストール)
  ⑥ Command and Control(C2)(遠隔制御)
  ⑦ Actions on Objectives (実行)

1 Cyber Kill Chain モデルでの分析

- 初期段階での分析ならびに検知へ(入口対策の強化)
  - 観測事象(Observable；攻撃によって観測された事象)、
    検知指標(Indicator；攻撃を検知するために使用できる事象)の活用

- 攻撃活動分析(Campaign Analysis)
  - 攻撃者のパタン、行動、TTP(Tactics, Techniques and Procedures：戦術、技術及び手順)を明らかにする。
  - 攻撃者の意図を明らかにする。

1 情報漏えい発生時の対応ポイント集

http://www.ipa.go.jp/security/awareness/johorouei/

1 基本的な考え方
2 情報漏えい対応の基本ステップ
3 情報漏えいのタイプ別対応のポイント
  3.1 紛失・盗難の場合の対応
  3.2 誤送信・Webでの誤公開の場合の対応
  3.3 内部犯行の場合の対応
  3.4 Winny/Share等への漏えいの場合の対応
  3.5 不正プログラム(ウイルス、スパイウェア等)の場合の対応
  3.6 不正アクセスの場合の対応
  3.7 風評・ブログ掲載の場合の対応
4 発見・報告におけるポイント
5 通知・報告・公表等におけるポイント
6 参考情報

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team (CSIRT、シーサート)体制による活動への期待が高まっています。日本シーサート協議会は、連携と問題解決の場の提供を通して、シーサート活動を支援しています。
本講演では、日本シーサート協議会の活動ならびに企業におけるシーサートの役割を紹介します。

- 情報漏えいへの対応
- シーサートとは
- 日本シーサート協議会の活動
- 企業におけるシーサートの役割

2 シーサートとは

- シーサート(CSIRT)
  Computer Security Incident Response Team
- コンピュータセキュリティにかかるインシデントに対処するための組織の総称(機能)
- インシデント関連情報、脆弱性情報、攻撃予兆情報を収集、分析し、対応方針や手順の策定などの活動
- シーサートの目的、立場(組織内での位置付け)、活動範囲、法的規制などの違いからそれぞれ各チームがそれぞれの組織において独自の活動している。

注：Cyber Security Incident Readiness Teamと呼ぶ場合もある。

2 シーサートとは

- **シーサートに規格はなく、各組織の実態に即したシーサートを実装⇒ 2つとして同じシーサートは存在しない**

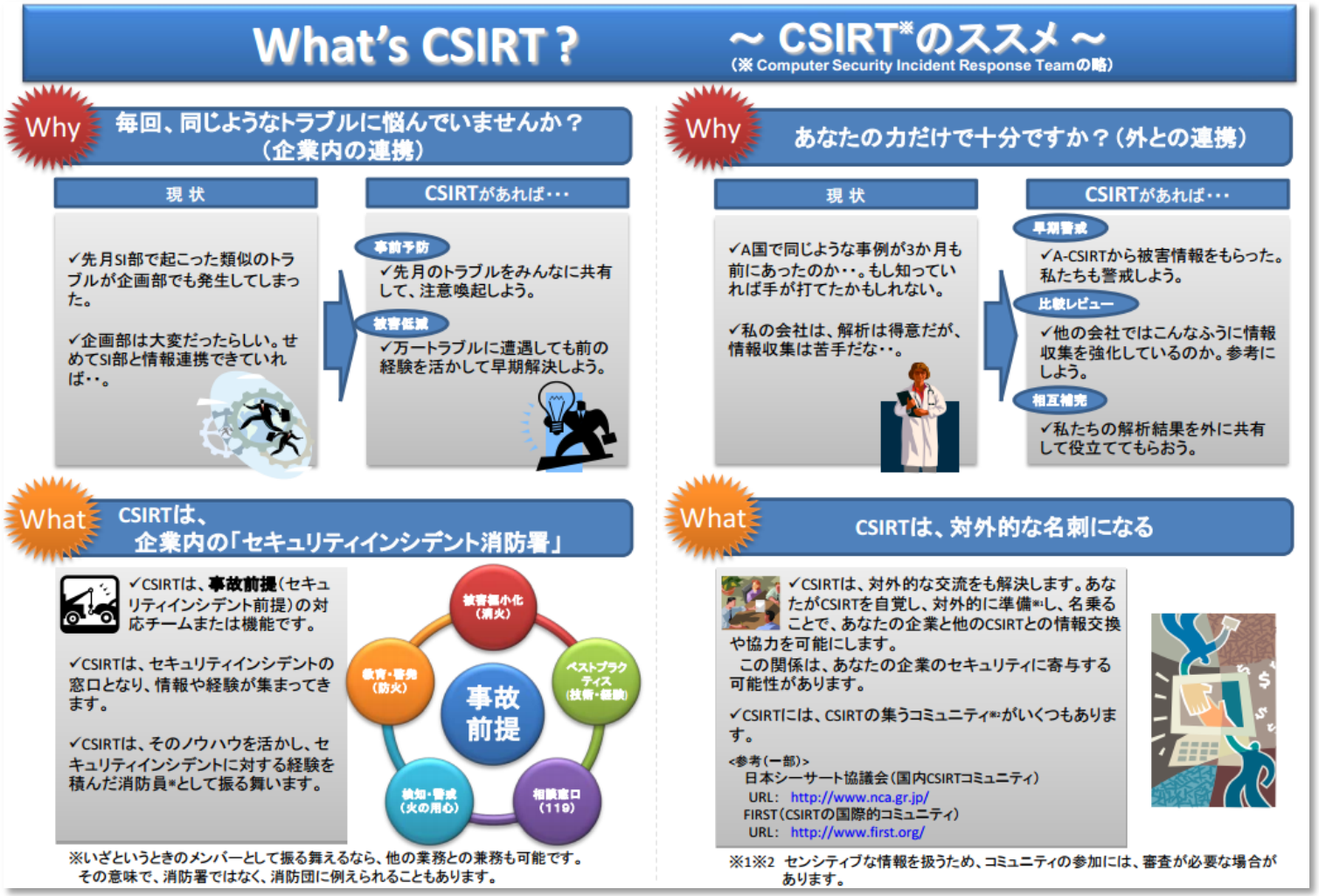
官民の連携に当たっては、漠然と組織間で情報共有を行うのではなく、各組織が情報セキュリティインシデントに関する緊急時対応の機能を有した専門的な部隊(以下「CSIRT(Computer Security Incidents Response Team)等」という。)を組織し、官民を含む各組織内 CSIRT 等の間で、専門的、実務的な連携を図ることが必要である。

以上、当分科会は、官民における CSIRT 等 の整備と各 CSIRT 等の間での情報連携の推進のため、以下の5分野について新たに9項目の対策を取りまとめた。

情報セキュリティ対策推進会議「情報セキュリティ対策に関する官民連携の在り方について(平成24年1月19日)」でのシーサートの説明

⇒ シーサートのコンセプトと特長を明確にしておくことが重要
≒組織文化の反映

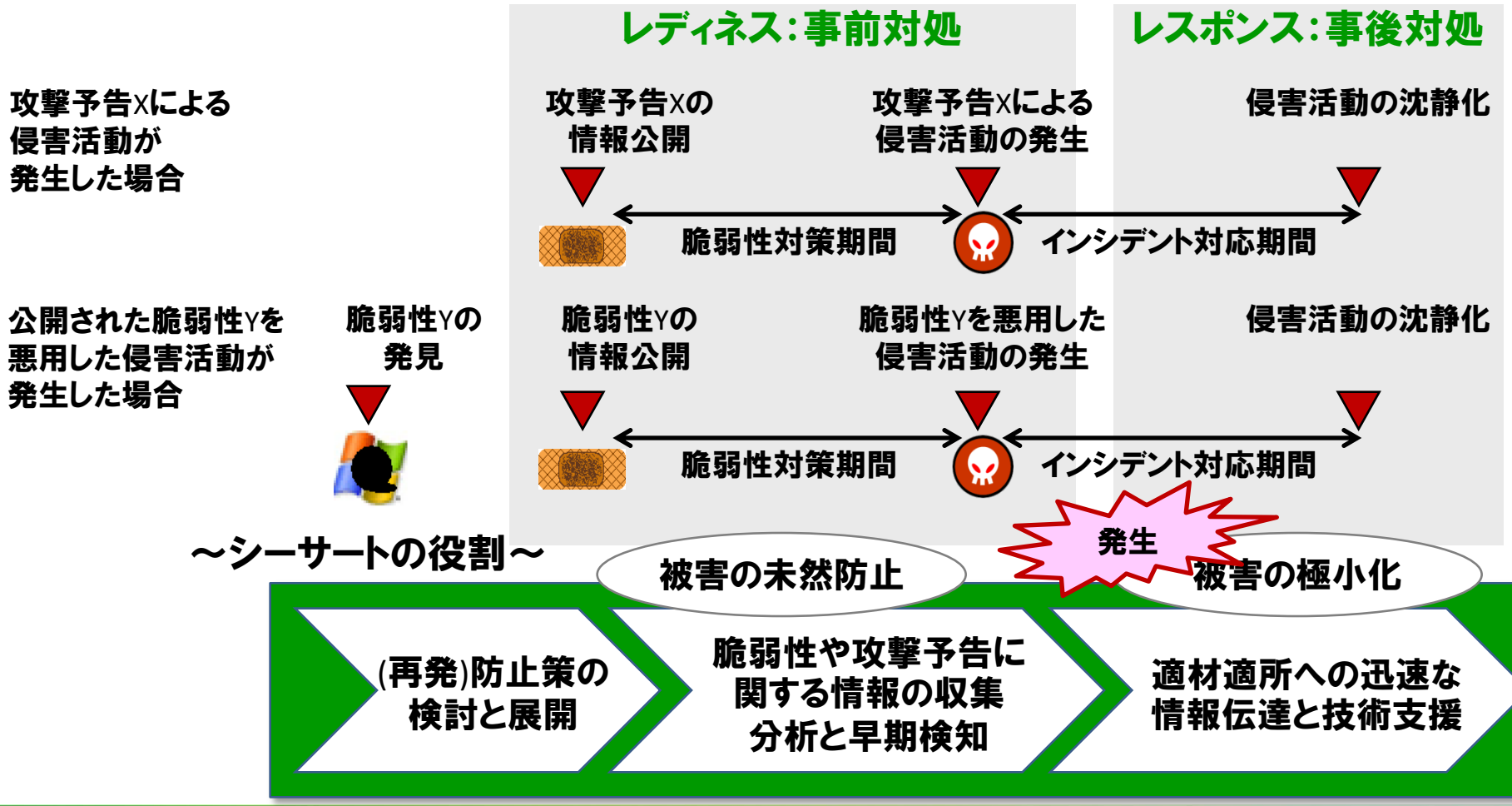
2 シーサートとは



http://www.nca.gr.jp/imgs/CSIRT.pdf

2 シーサートとは

- 一般的に認識されているシーサートの役割



2 シーサートとは　～歴史～

- インターネットワームの出現を契機に、米CERT/CC 設立

1998年のインターネットワームの出現を契機に、インシデントの原因や対応方法などの情報を共有することの重要性が認識された。

- 1988年
  国防総省高等研究計画局 (DARPA: Defense Advanced Research Projects Agency) が中心となり、CERT/CCを設立した。

1989年10月、SPAN VAX/VMS システムを攻略するWankワームが出現した際に、国境、組織をまたがったシーサート間のコミュニケーションの欠落が適切なインシデント対応の推進を妨げた。

- 1990年
  インシデント対応チームの組織間ならびに国際間連携のため、大学、研究機関、企業、政府、軍などのシーサートコミュニティから構成されるFIRSTが組織された。
- 1996年
  国内初のシーサート組織、JPCERT/CC(Japan Computer Emergency Response Team/Coordination Center)が活動を開始した。

2 シーサートとは　～歴史～

電子メール型ワーム(1999年～)、ネットワーク型ワーム(2000年～)、ボット(2004年～)、標的型メール攻撃(2005年～)

- 2007年
  国内のインシデント対応チームの組織間連携のため、日本シーサート協議会が設立された。

標的型攻撃の顕在化(2011年～)

- 2012年
  内閣官房情報セキュリティセンター内に、情報セキュリティ緊急支援チーム(CYber incident Mobile Assistant Team：CYMAT)が発足された。

CERT/CC (Computer Emergency Response Team/Coordination Center)
http://www.cert.org/

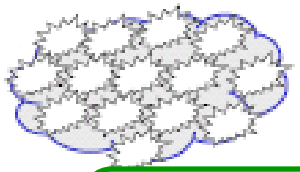
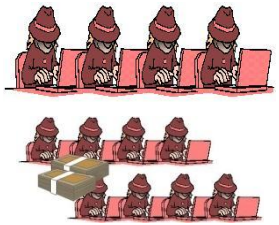
米国におけるセキュリティ事案情報、脆弱性情報の収集ならびに調整機関

FIRST (Forum of Incident Response and Security Teams)
http://www.first.org/

信頼関係に結ばれた世界におけるシーサートの国際コミュニティ、2015年6月末現在、70カ国321チームが加盟

2 シーサートとは　～歴史～

- より高度なシーサート連携が求められてきている

年代	特徴	被害の模式図
2000年 ～2001年	均一的かつ広範囲に渡る単発被害 Webサイトのページ書き換え	
2000年 ～2005年	均一的かつ広範囲に渡る連鎖型被害 ウイルス添付型メールの流布 ネットワーク型ワームの流布	異なる組織のシーサート同士がつながり、手段を共有することで問題解決を図る
2005年～	類似した局所的な被害 SQLインジェクションによるWebサイト侵害 Winny、Shareによる情報流出 フィッシング、スパイウェア、ボットなど	
2006年～	すべてが異なる局所的な被害 標的型攻撃 攻撃組織基盤化 2009年～ 攻撃組織間連携 	 異なる組織のシーサート同士がつながり、侵害活動を鳥瞰することで問題解決を図る

2 シーサートとは　～分類～

- **シーサートは多種多様**

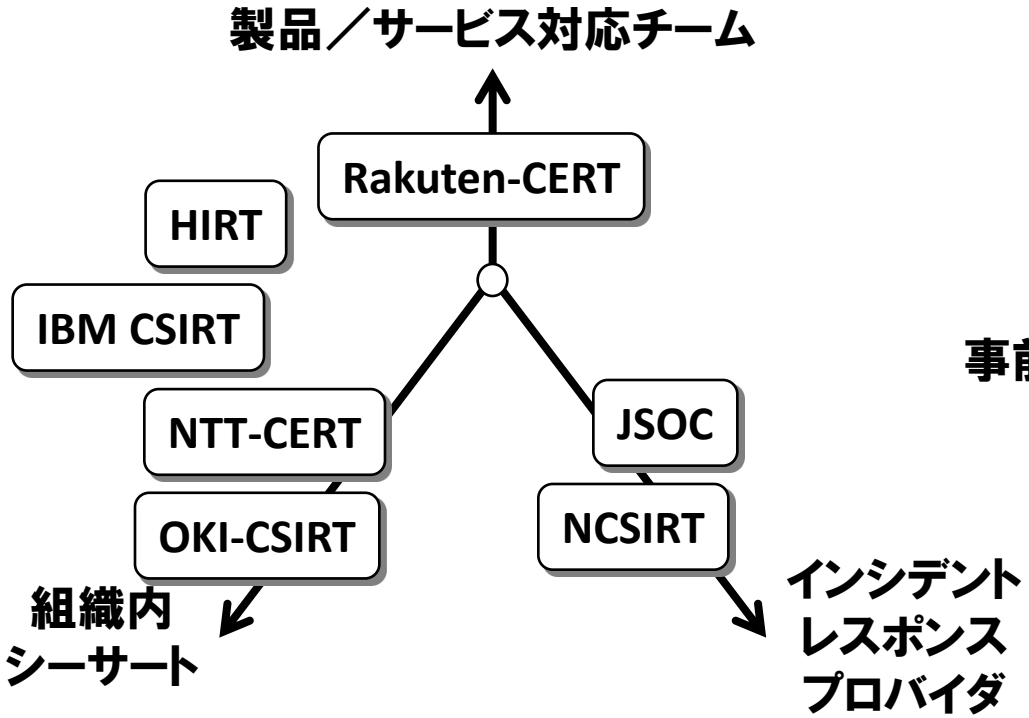
  活動範囲の視点から、組織内シーサート、国際連携シーサート、コーディネーションセンター、分析センター、製品対応チーム、インシデントレスポンスプロバイダなどに分類されることもあるが、サービス対象、内容、体制などの違いによって、多種多様なシーサートが構成されている。
  - 対象範囲：国、自組織、顧客
  - 内容(フェーズ)：事前対処、事後対処
  - 内容(機能)：脆弱性ハンドリング、インシデントハンドリング、動向分析、リスク分析など
  - 体制：集約型／分散型、専任型／兼務型

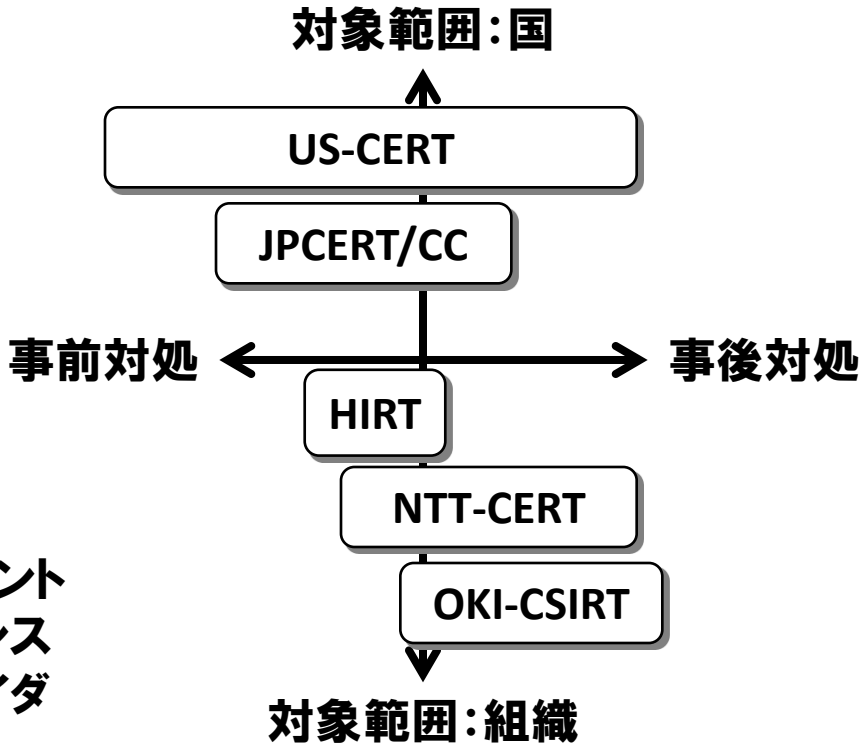
組織内シーサート
自組織内に関係したインシデントに対応するシーサートと定義する。

製品／サービス対応シーサート
提供する製品やサービスのインシデントに対応するシーサートと定義する。

2 シーサートとは　～分類～

- 対象範囲、内容(フェーズ)、内容(機能)による分類
  - サービス対象、内容、体制などの違いによって、多種多様なシーサートが構成されている。





http://www.nca.gr.jp/member/index.html

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team (CSIRT、シーサート)体制による活動への期待が高まっています。日本シーサート協議会は、連携と問題解決の場の提供を通して、シーサート活動を支援しています。
本講演では、日本シーサート協議会の活動ならびに企業におけるシーサートの役割を紹介します。

- 情報漏えいへの対応
- シーサートとは
- **日本シーサート協議会の活動**
- 企業におけるシーサートの役割

3 組織概要

- 設立
  - 2007年3月
- 名称
  - 正式名称：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
  - 略称：日本シーサート協議会
  - 英語名：NIPPON CSIRT ASSOCIATION
  - Web：http://www.nca.gr.jp/
- 使命
  - 本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す
  - 社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る

3 活動概要

- さまざまな場の提供
  - シーサート間の交流の場
  - シーサート間の連携のあり方に関する検討の場
  - 共有方法検討等
- シーサート構築支援
  - 構築推奨
  - 課題検討
- シーサート活動支援
  - セキュリティインシデントへの対応支援
  - 事例情報提供、対策情報提供等

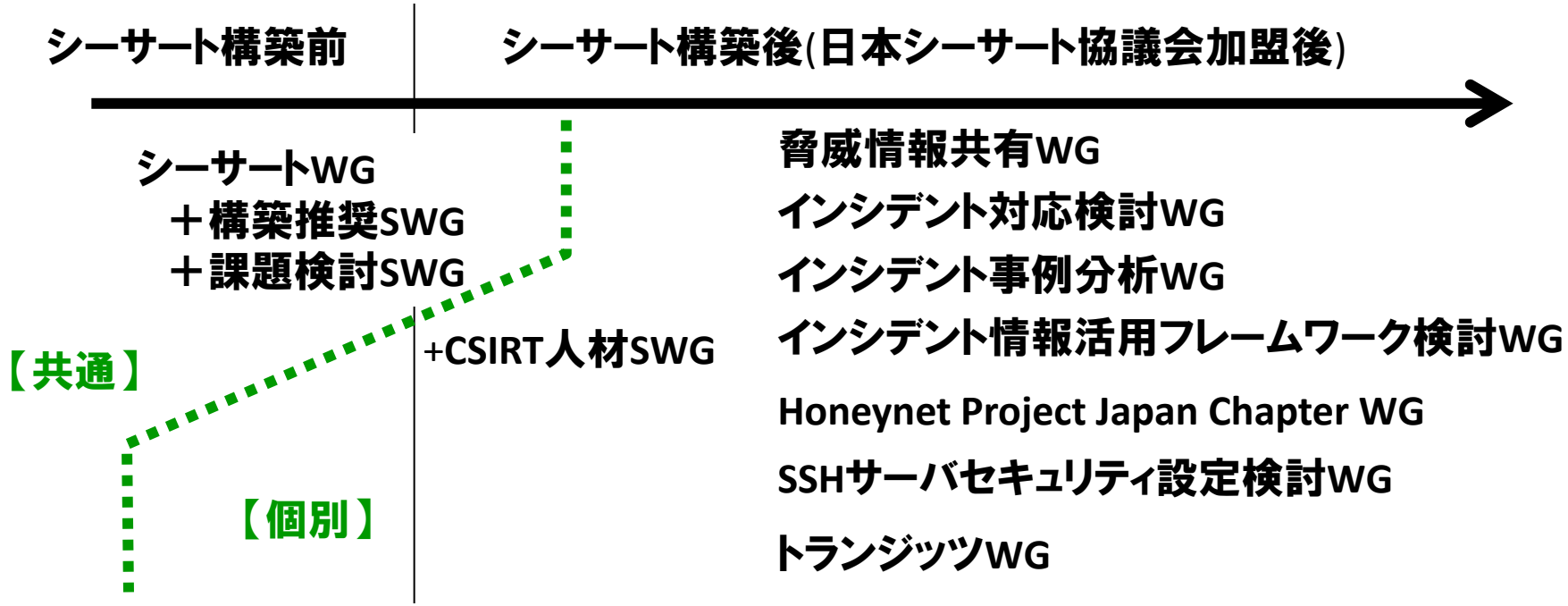
3 年間スケジュール

- 3月　WG会合(各WGの活動報告、新規加盟チームの紹介など)
- 8月　総会＋WG会合(年間の活動報告など)
- 9月　チーム登録書／メンバの更新手続き
- 12月　シーサート企画イベント(JPNIC主催 Internet Week)

- 上記以外(対外的なイベント開催)
  - TRANSITS ワークショップ
    シーサート設立の促進や能力向上を目的とした教育プログラム
  - CSIRTフォーラム
    シーサートを構築したい組織と既存シーサートとの交流の場
  - シーサートWG
    日本シーサート協議会に加盟したい組織と既存シーサートとの交流の場

3 ワーキンググループ(WG)

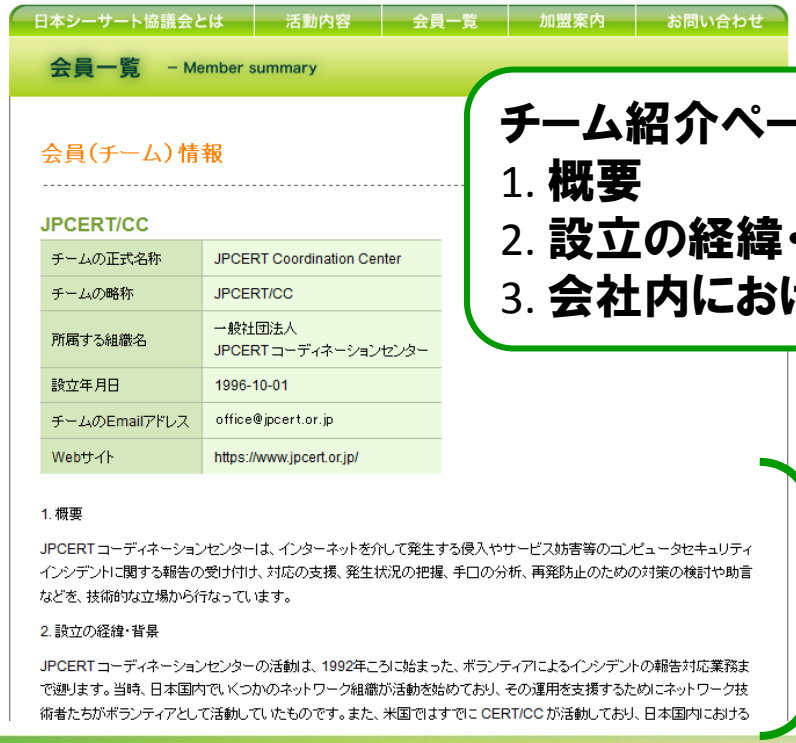
- **問題提起と解決のための活動としてWGを立上げ、会員ならびに協議会外部の協力者と共に、問題解決を図る。**
  http://www.nca.gr.jp/activity/index.html



【活動中のワーキンググループの位置付け】

3 日本シーサート協議会加盟組織一覧

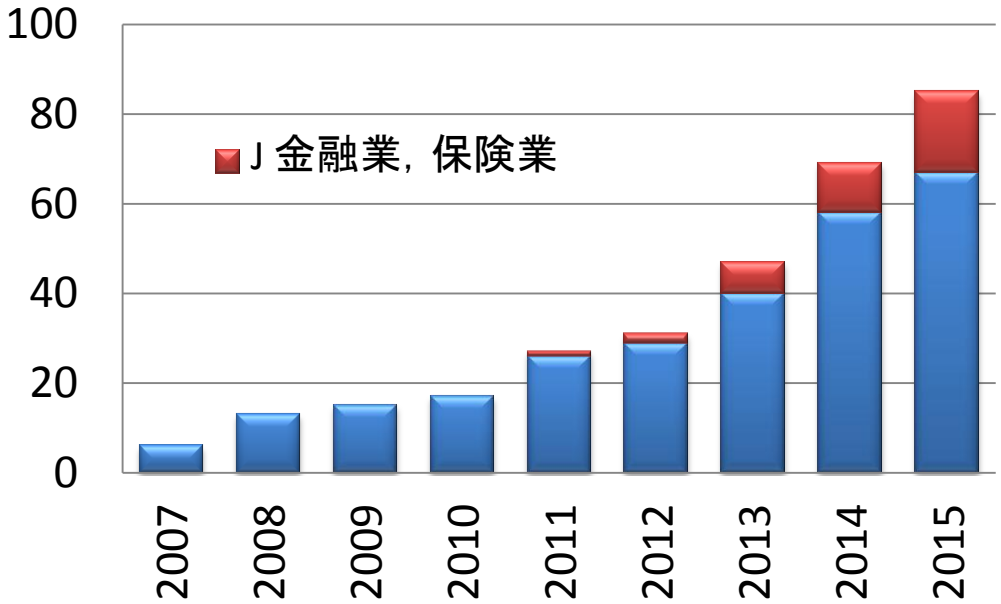
- **体制、対象とする分野、取りまとめる部署などのアンケート調査の集計結果と共に、日本シーサート協議会のWebサイトに掲載しているチーム情報をまとめた資料**
  http://www.nca.gr.jp/member/index.html

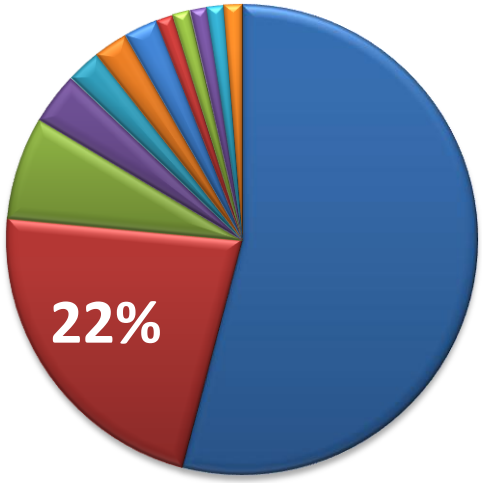


チーム紹介ページの拡充(2013年4月～)
1. **概要**
2. **設立の経緯・背景**
3. **会社内における位置づけおよび活動内容**

3 アンケートから見えてきたシーサート活動体制

- 加盟チーム数の推移
  - 2011年頃から、J 金融業、保険業(日本標準産業分類項目)分野からの加盟が増えている。



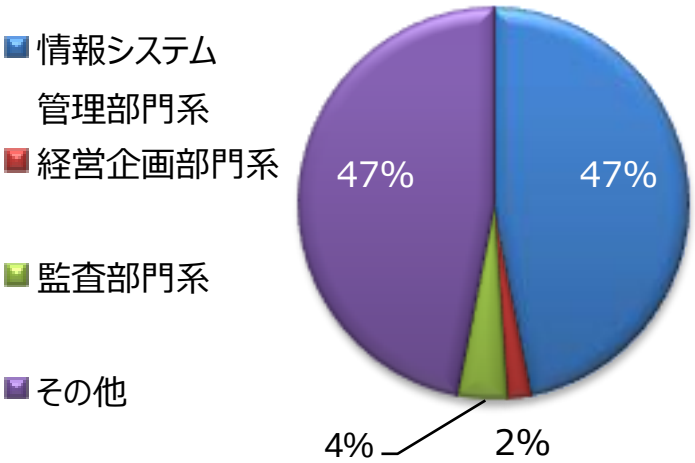


日本標準産業分類項目

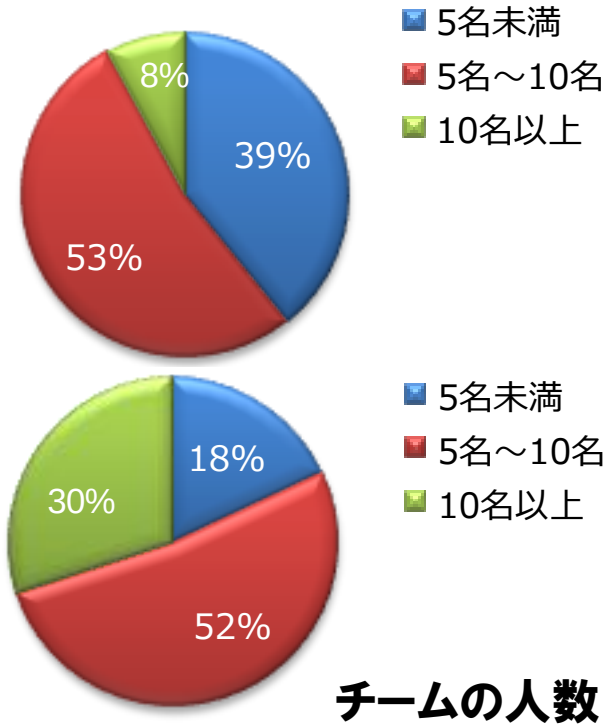
- G 情報通信業
- J 金融業，保険業
- E 製造業
- N 生活関連サービス業，娯楽業
- H 運輸業，郵便業
- L 学術研究，専門・技術サービス業
- R サービス業（他に分類されないもの）
- D 建設業
- I 卸売業，小売業
- K 不動産業，物品賃貸業
- M 宿泊業，飲食サービス業

3 アンケートから見えてきたシーサート活動体制

- **加盟組織の体制**
  - **加盟組織の多くは、『情報システム管理部門系』が取り纏め部署**
  - **チーム人数は、活動開始後に増員しており、全体としてスモールスタート**



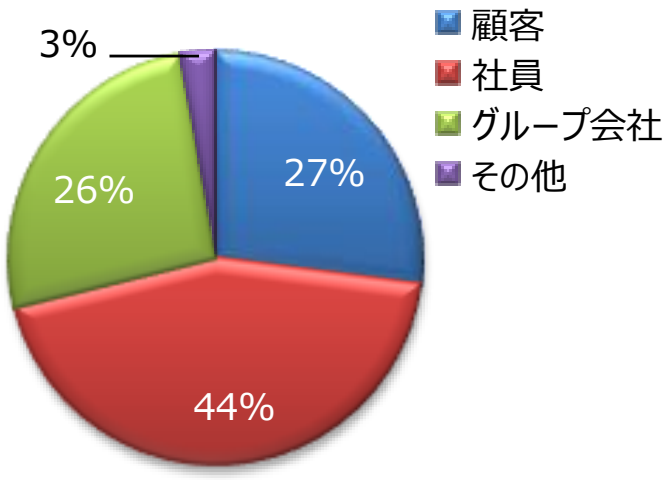
取り纏め部署



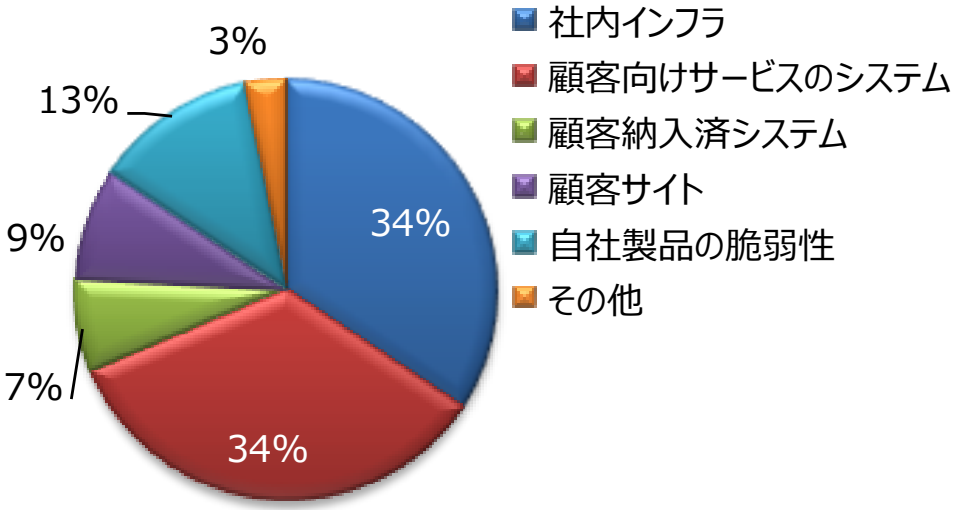
チームの人数
(上：設立時、下：活動開始後)

3 アンケートから見えてきたシーサート活動体制

- **加盟組織のサービス**
  - **7割近くが、CSIRTが所属する組織のインシデント対応を想定した活動(社内インフラ、顧客向けサービスのシステム)**



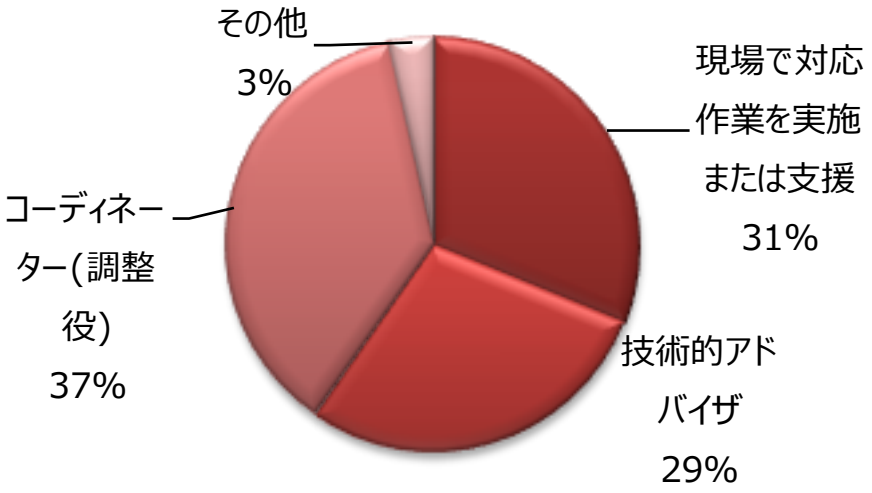
対象とする利用者



対象とする分野

3 アンケートから見えてきたシーサート活動体制

- インシデント対応時のCSIRTの位置付け
  - これまでの日本企業独自の形態として紹介してきた『技術アドバイザ』という側面に加え、組織内の横断的な協力体制整備のためのコーディネーター(調整役)の側面が顕在化



インシデント対応時のCSIRTの位置付け

目次

サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team (CSIRT、シーサート)体制による活動への期待が高まっています。日本シーサート協議会は、連携と問題解決の場の提供を通して、シーサート活動を支援しています。
本講演では、日本シーサート協議会の活動ならびに企業におけるシーサートの役割を紹介します。

- 危険の認識
- シーサートとは
- 日本シーサート協議会の活動
- **企業におけるシーサートの役割**

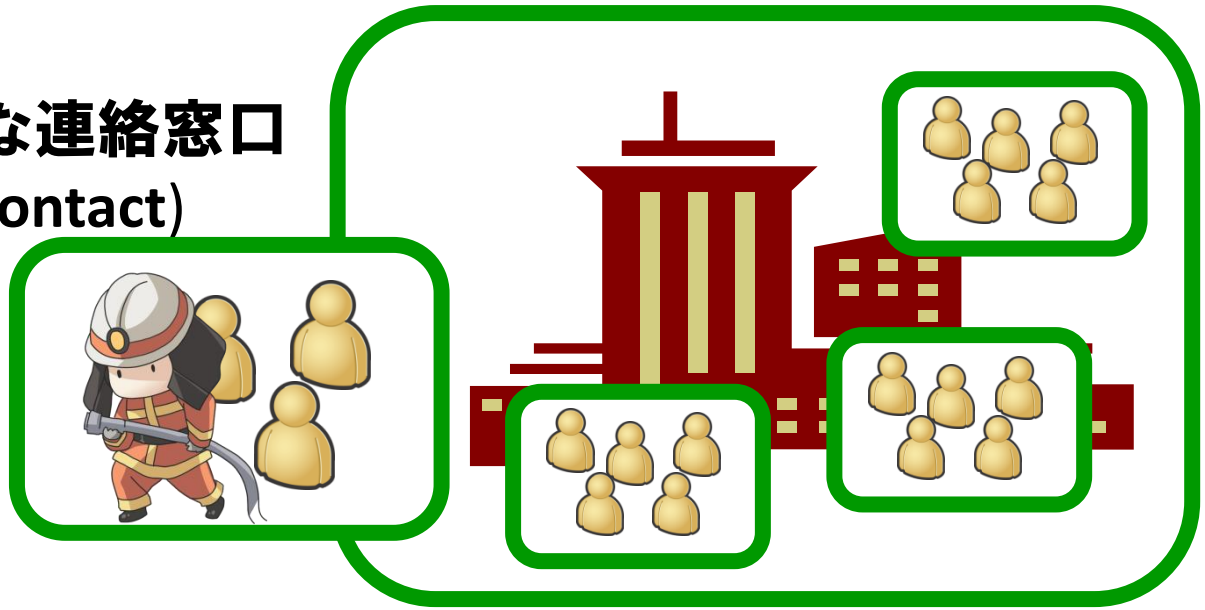
4 シーサート活動の特徴

- 対外的な連絡窓口であること
- 技術的な問合せに関して対応が可能であること
- インシデントレスポンス（事後対処）だけではなく、インシデントレスポンスなどの実践的な活動経験を元に、インシデントレディネス（事前対処）を進めていること
- 部署間を横断した組織体制をとっていること

4 対外的な連絡窓口

- 対外的な連絡窓口が明らかになっていることの利点
  - [通知側] 脆弱性対策やインシデント対応の通知先を探さずに済む。通知の背景説明を省略できる。通知をたらい回しにされない。
  - [受領側] 通知をトリガに、脆弱性対策やインシデント対応をベストエフォートで動かし始めることができる。

シーサート
＝対外的な連絡窓口
(Point of Contact)



4 技術的な問合せに対応可

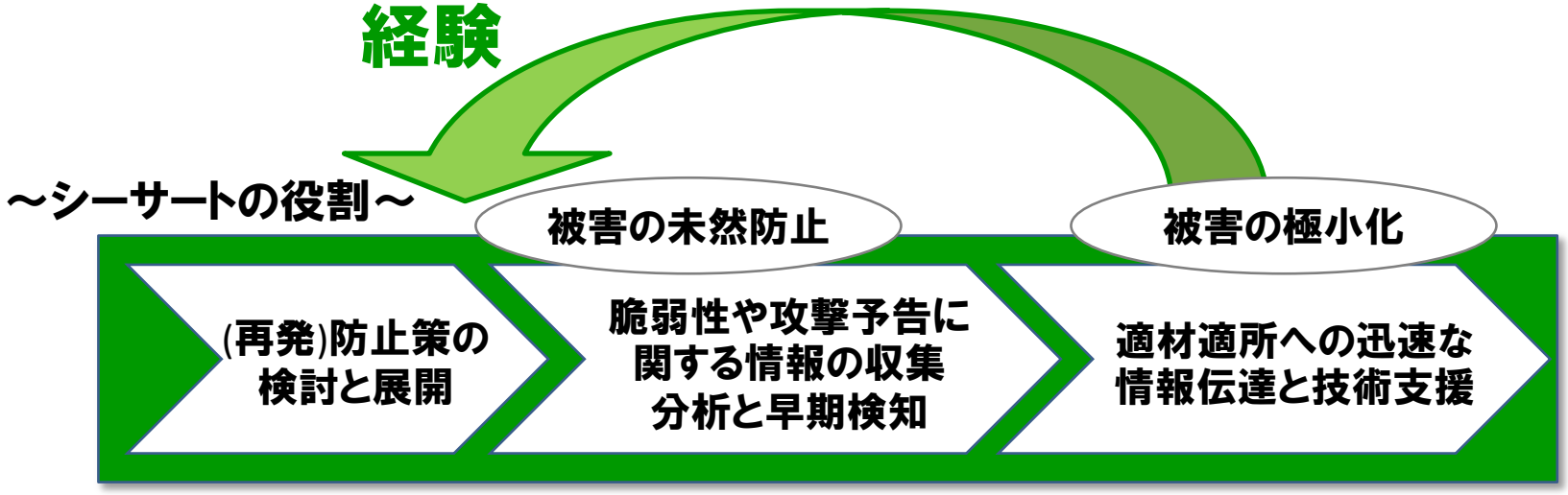
- 対外的な連絡窓口が、技術的な問合せに関しても対応可能であることの利点
  - [通知側] 脆弱性対策やインシデント対応の技術的な通知をたらい回しにされない。

- 連絡窓口(シーサート)に期待したい要件
  - 技術的な視点で脅威を推し量り、伝達できること
  - 技術的な調整活動ができること
  - 技術面での対外的な協力ができること

技術的な通知や依頼に対して対処してくれることを期待しているのであり、必ずしも、シーサート内に技術的な専門家が必要であるという指摘ではない。

4 インシデントレディネス(事前対処)

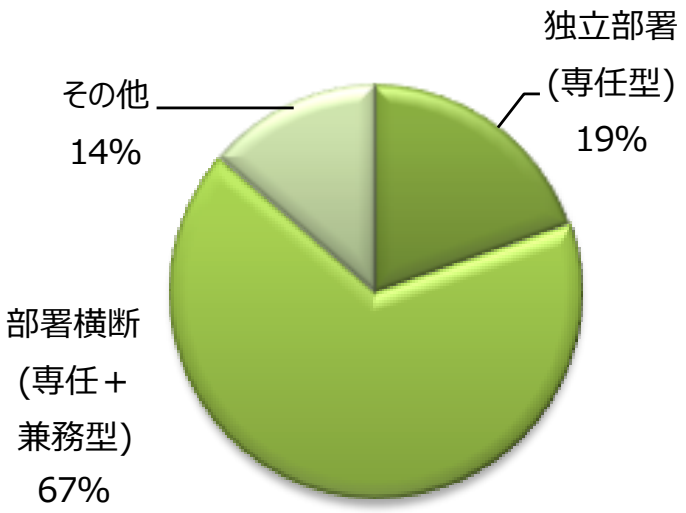
- インシデントレスポンス(事後対処)などの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めることの重要性



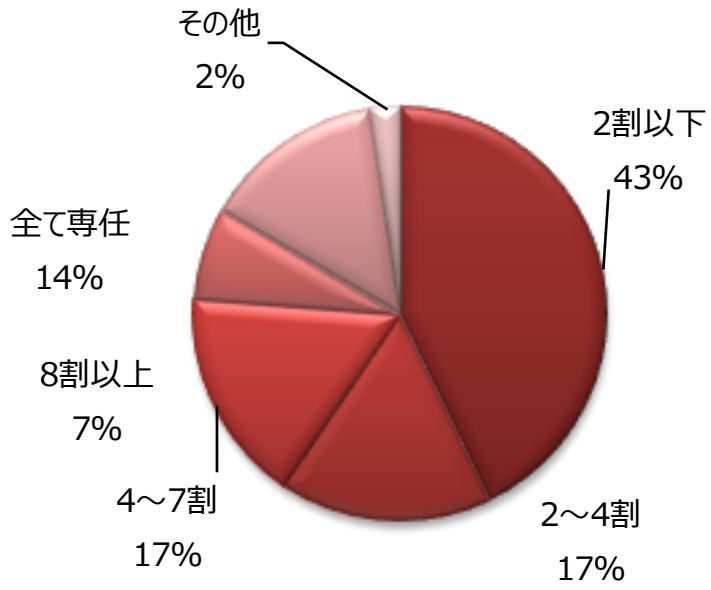
- 経験があるからこそ、「問題解決」に向けての想像力も働く。
- 経験ができないならば、他のインシデントレスポンス(事後対処)の疑似体験を通して、「問題解決」に向けての想像力を養う。

4 部署間を横断した組織体制

- CSIRT実装の多くは、専任のCSIRT要員を抱えた部署を核とした部署横断型⇒部署間を横断した組織体制の構築、すなわち、組織内の横断的な協力体制整備への期待



実装の形態



専任の割合

ご清聴ありがとうございました。

シーサート同士の積極的なコミュニケーションを図ることによって、より良いセキュリティ対応を考え、そして、実現していきます。

シーサートに関して： csirt-pr@nca.gr.jp
加盟に関して： nca-sec@nca.gr.jp

CSIRT
日本シーサート協議会

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