なぜシーサートが必要なのか

～ CSIRTの現状と構築のすすめ～

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(NCA)
副運営委員長　萩原 健太

平成28(2016)年10月18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では、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。

- シーサートとは
- 日本シーサート協議会の活動
- アンケートから見えてきたシーサート活動体制
- 企業におけるシーサートの役割
- シーサートの構築
- 日本シーサート協議会の役割

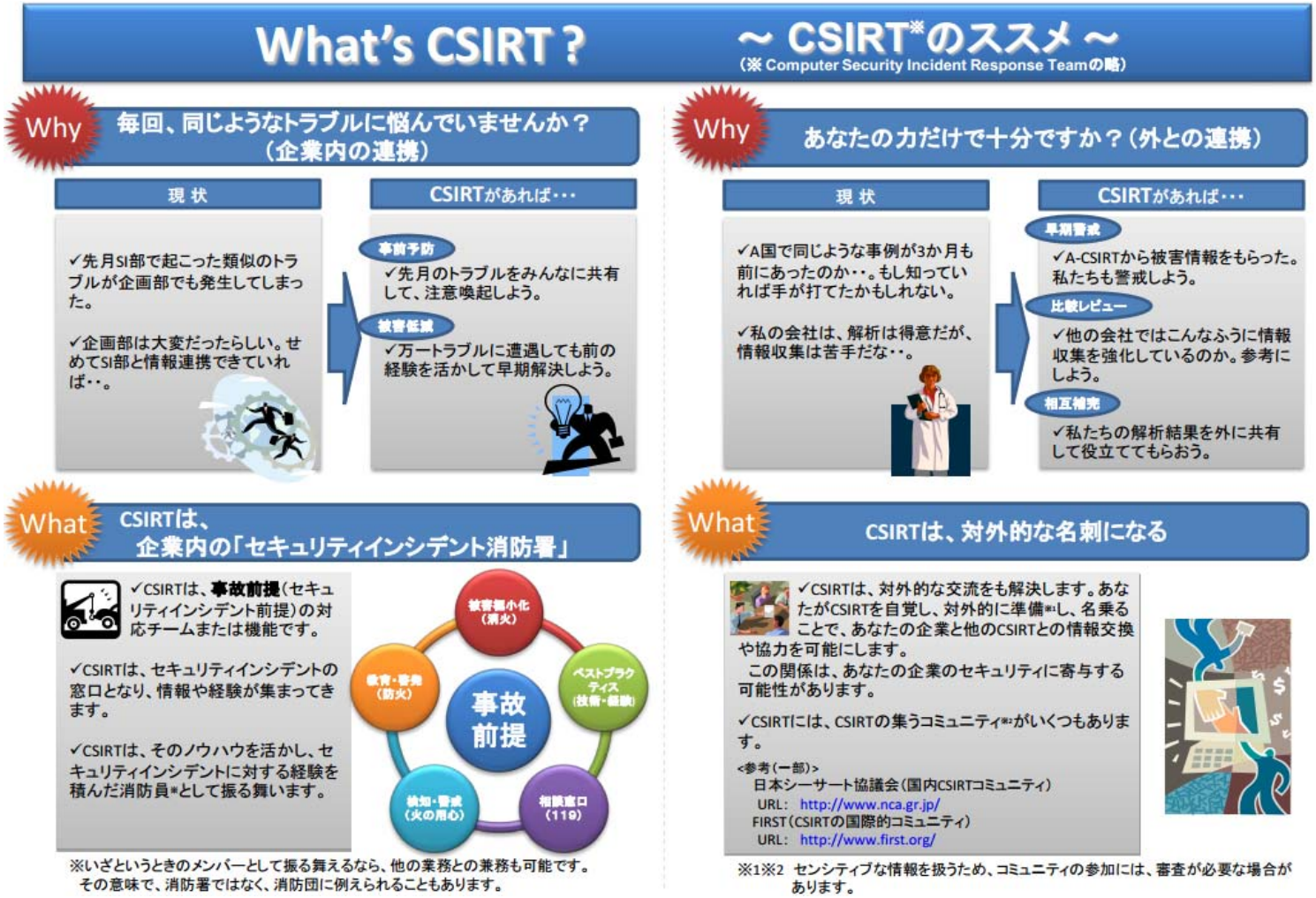
1 シーサートとは

- Computer Security Incident Response/Readiness Teamの略
  - 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。

    ⇒ CSIRTに規格はなく、各組織の実態に即したCSIRTを実装
    ⇒ 1つとして同じCSIRTは存在しない

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

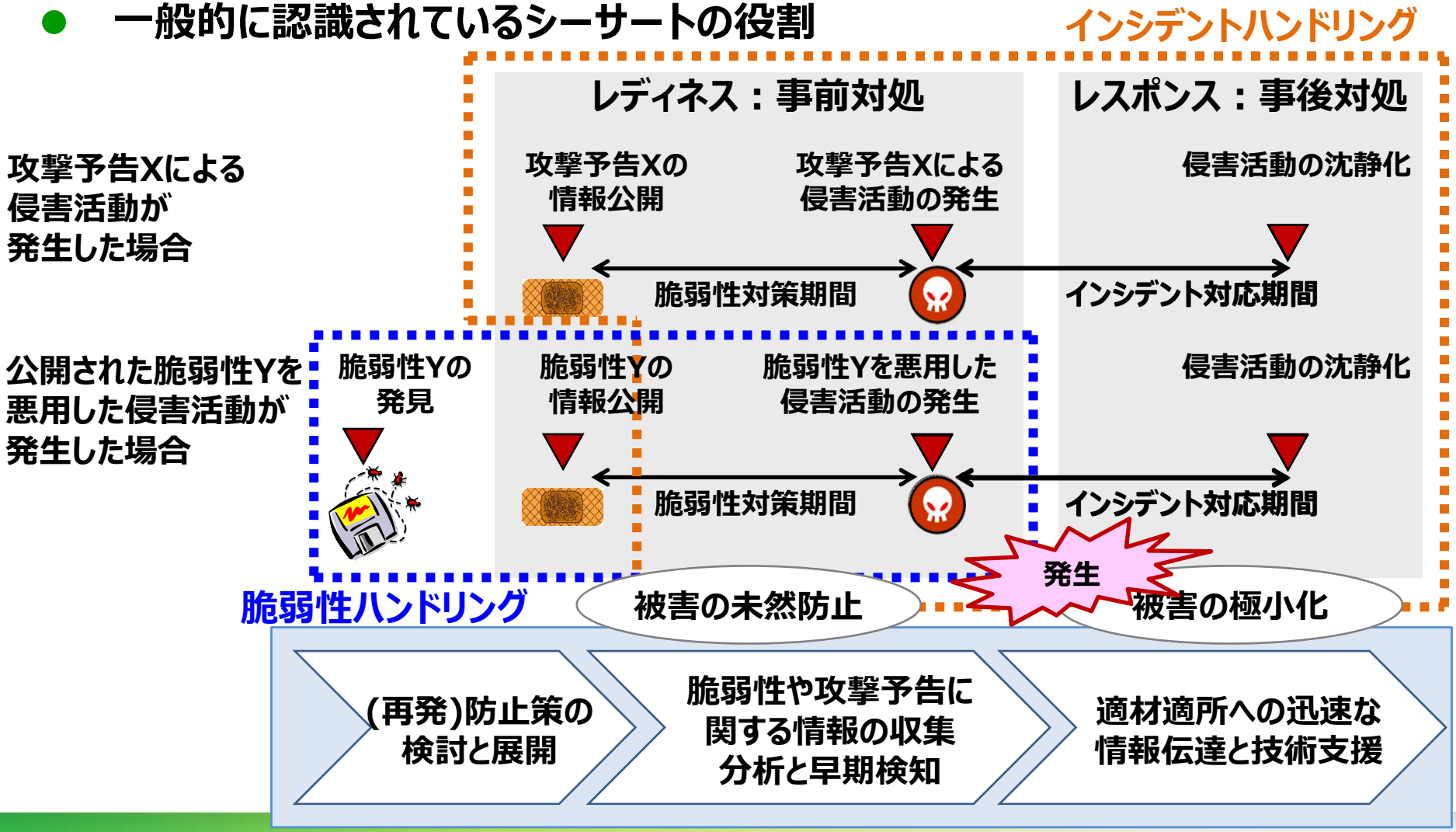
1 シーサートとは



出典：日本シーサート協議会 http://www.nca.gr.jp/imgs/CSIRT.pdf

1 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



1 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

1988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。

1 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/Coordination Center
(設立当初はComputer Emergency Response Teamの略であった)
http://www.cert.org/

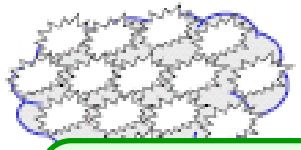
米国におけるセキュリティ事案情報、脆弱性情報の収集ならびに調整機関

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９月末現在、73カ国328チームが加盟

1 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	 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
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	
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

1 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。

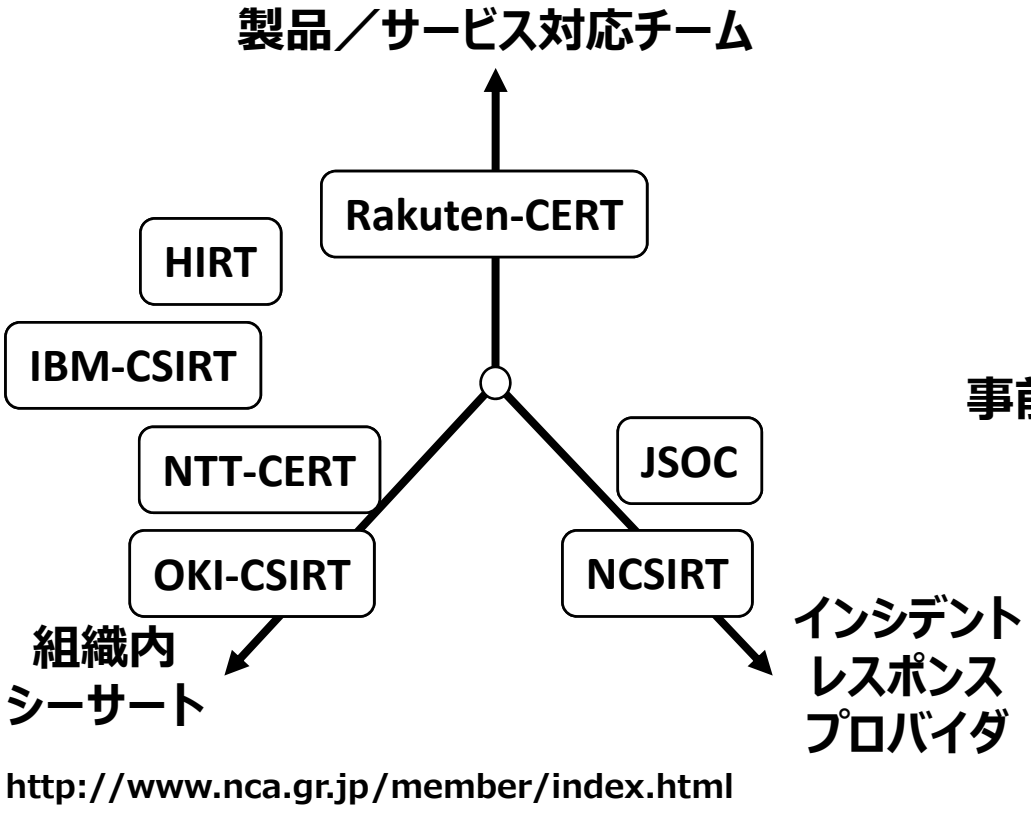
  - **対象範囲：国、自組織、顧客**
  - **内容(フェーズ)：事前対処、事後対処**
  - **内容(機能)：脆弱性ハンドリング、インシデントハンドリング、動向分析、リスク分析など**
  - **体制：集約型／分散型、専任型／兼務型**

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。

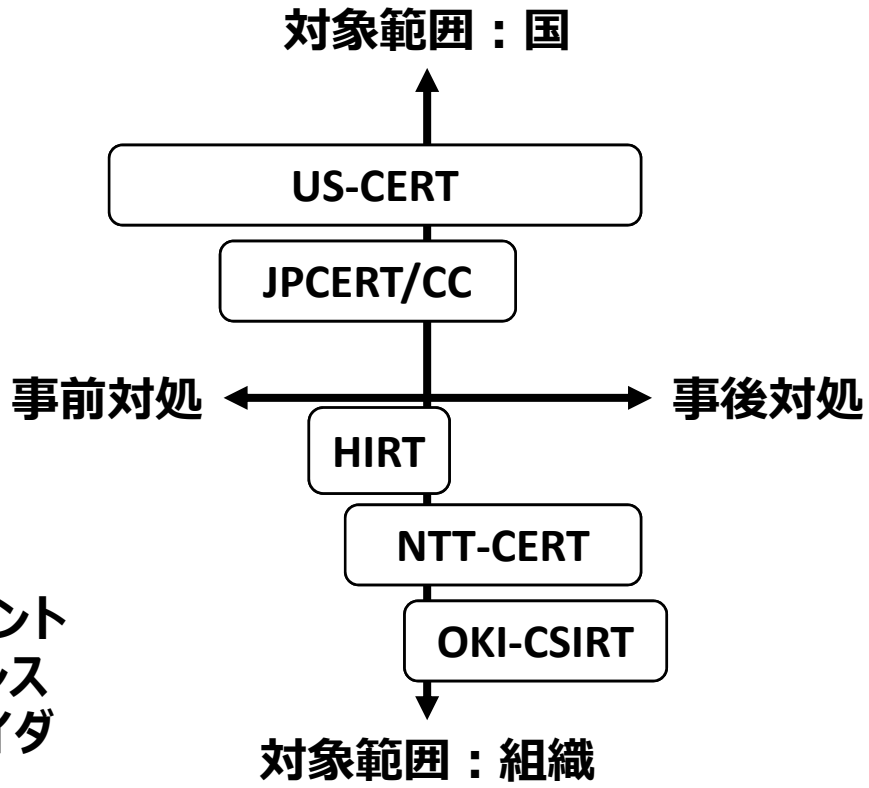
製品／サービス対応シーサート
提供する製品やサービスのインシデントに対応するシーサートと定義する。

1 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。

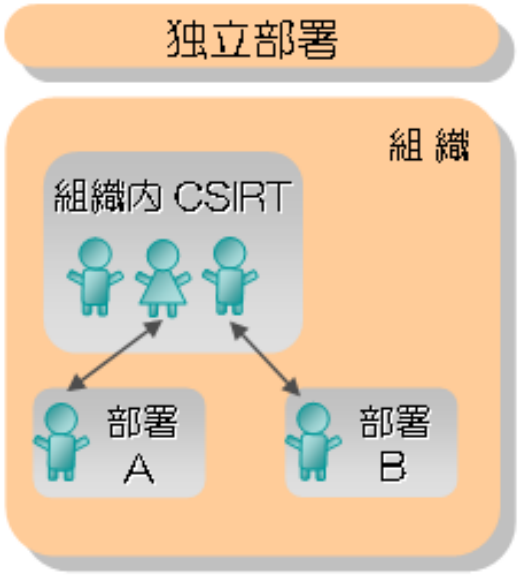


http://www.nca.gr.jp/member/index.html

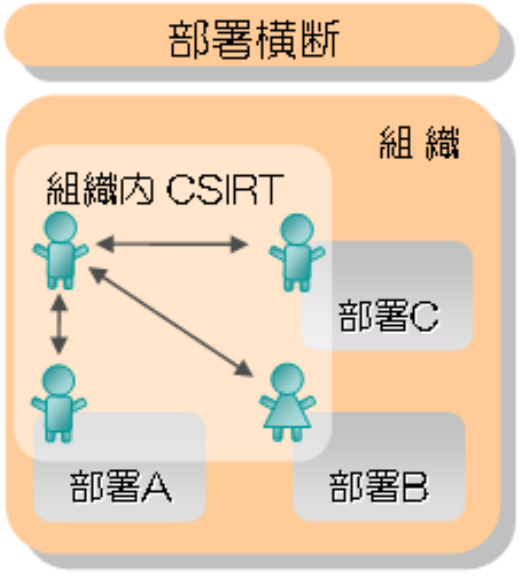


1 シーサートとは ～実装形態～

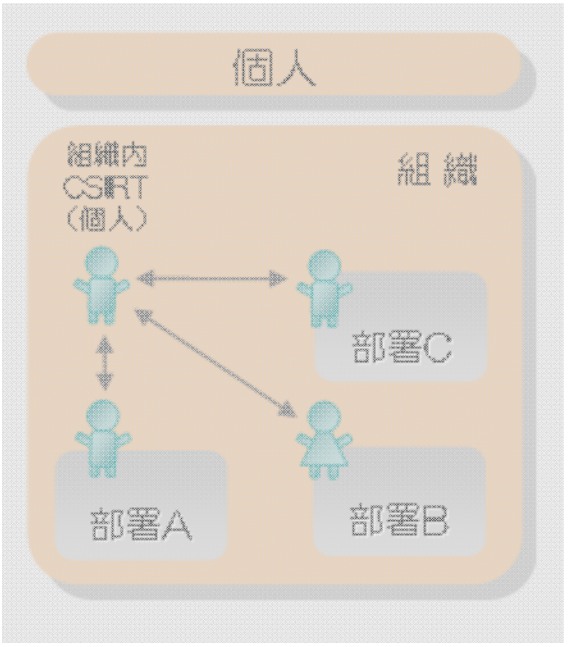
- **組織における実装形態**



専任のメンバー



兼務のメンバー
（バーチャルチーム）



出典：JPCERT/CC「CSIRTガイド」
http://www.jpcert.or.jp/csirt_material/files/guide_ver1.0.pdf

1 シーサートとは ～内容（機能）～

インシデント 事後対応サービス	インシデント 事前対応サービス	セキュリティ品質向上 サービス
・インシデントハンドリング ・コーディネーション ・オンサイトインシデントハンドリング ・インシデントハンドリングサポート ・コンピュータ・フォレンジックス ・アーティファクトハンドリング	・セキュリティ関連情報提 ・脆弱性情報ハンドリング ・インシデント/セキュリティイベント検知 ・技術動向調査 ・セキュリティ監査/査定 ・セキュリティツールの開発	・リスク評価・分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング ・セキュリティ教育/トレーニング/啓発活動 ・製品評価・認定

表 1 CSIRT のサービス概要

出典：日本シーサート協議会「CSIRTスタータキット」

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では、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。

- シーサートとは
- **日本シーサート協議会の活動**
- アンケートから見えてきたシーサート活動体制
- 企業におけるシーサートの役割
- シーサートの構築
- 日本シーサート協議会の役割

2 組織概要

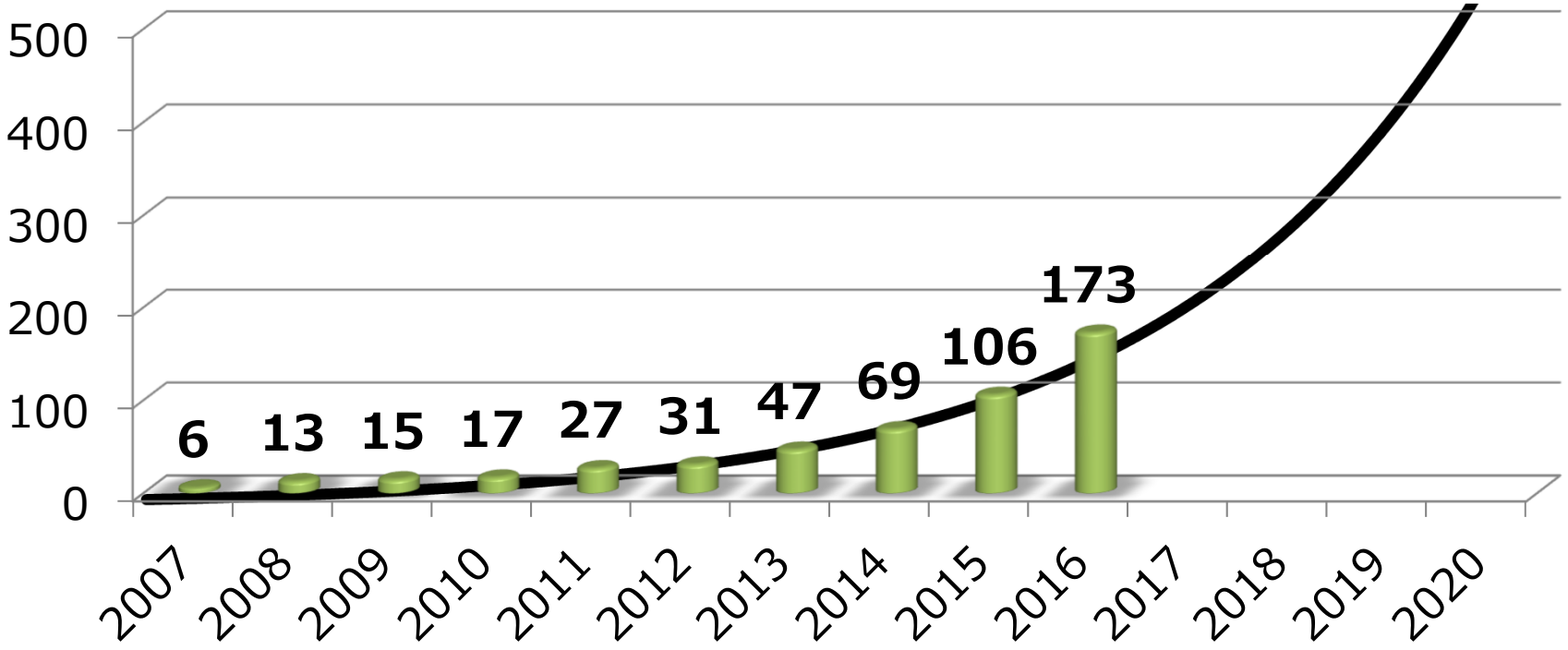
- 設立
  - 2007年3月
- 名称
  - 正式名称：日本コンピュータセキュリティインシデント対応チーム協議会
  - 略称：日本シーサート協議会
  - 英語名：NIPPON CSIRT ASSOCIATION
  - ウェブ： http://www.nca.gr.jp/

CSIRT
日本シーサート協議会

- 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

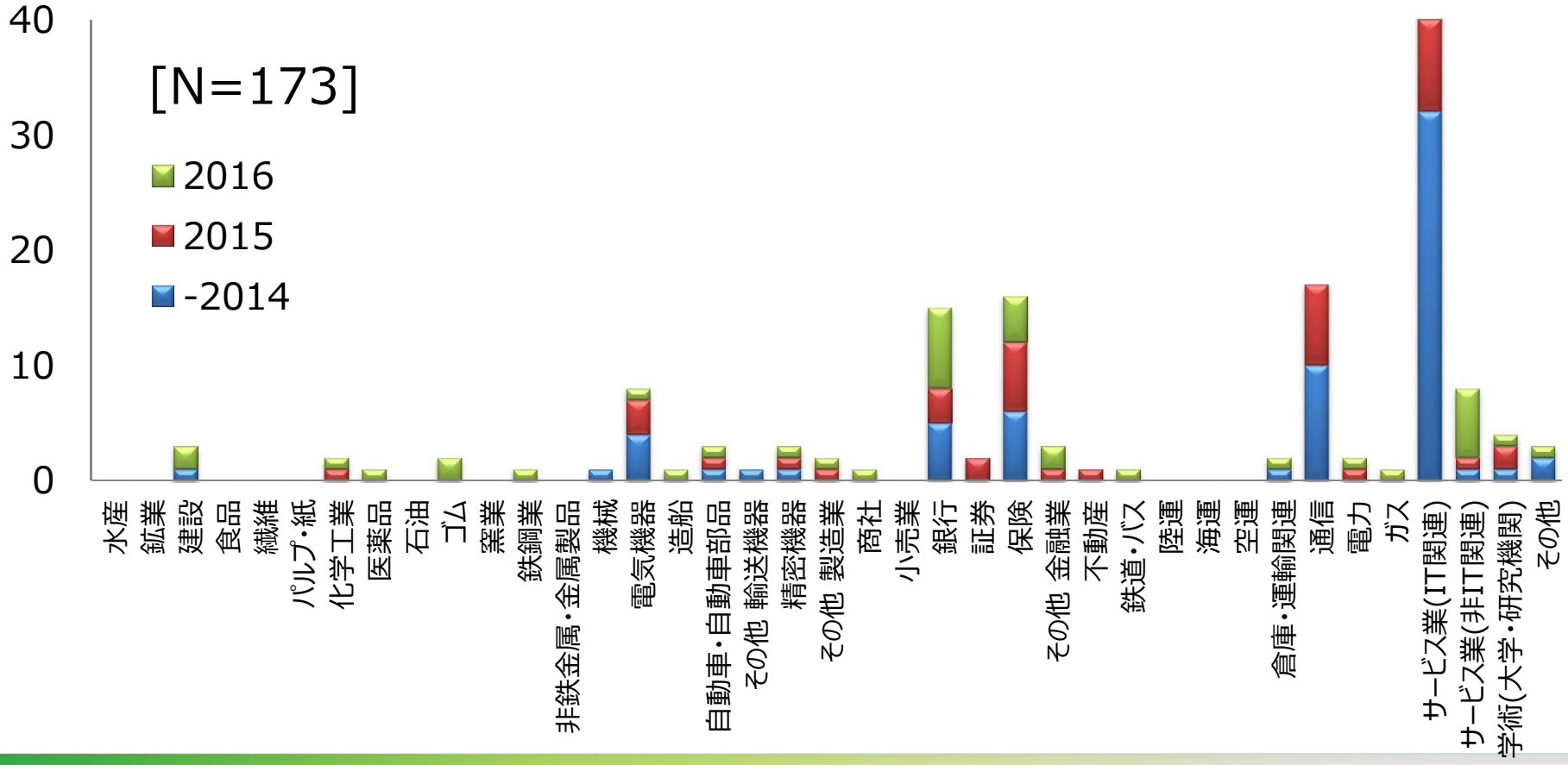
2 加盟企業の推移

- **加盟数(累積)の推移**
  - 173チーム(2016年8月1日現在)
  - このままいくと、2020年には、 500チーム???



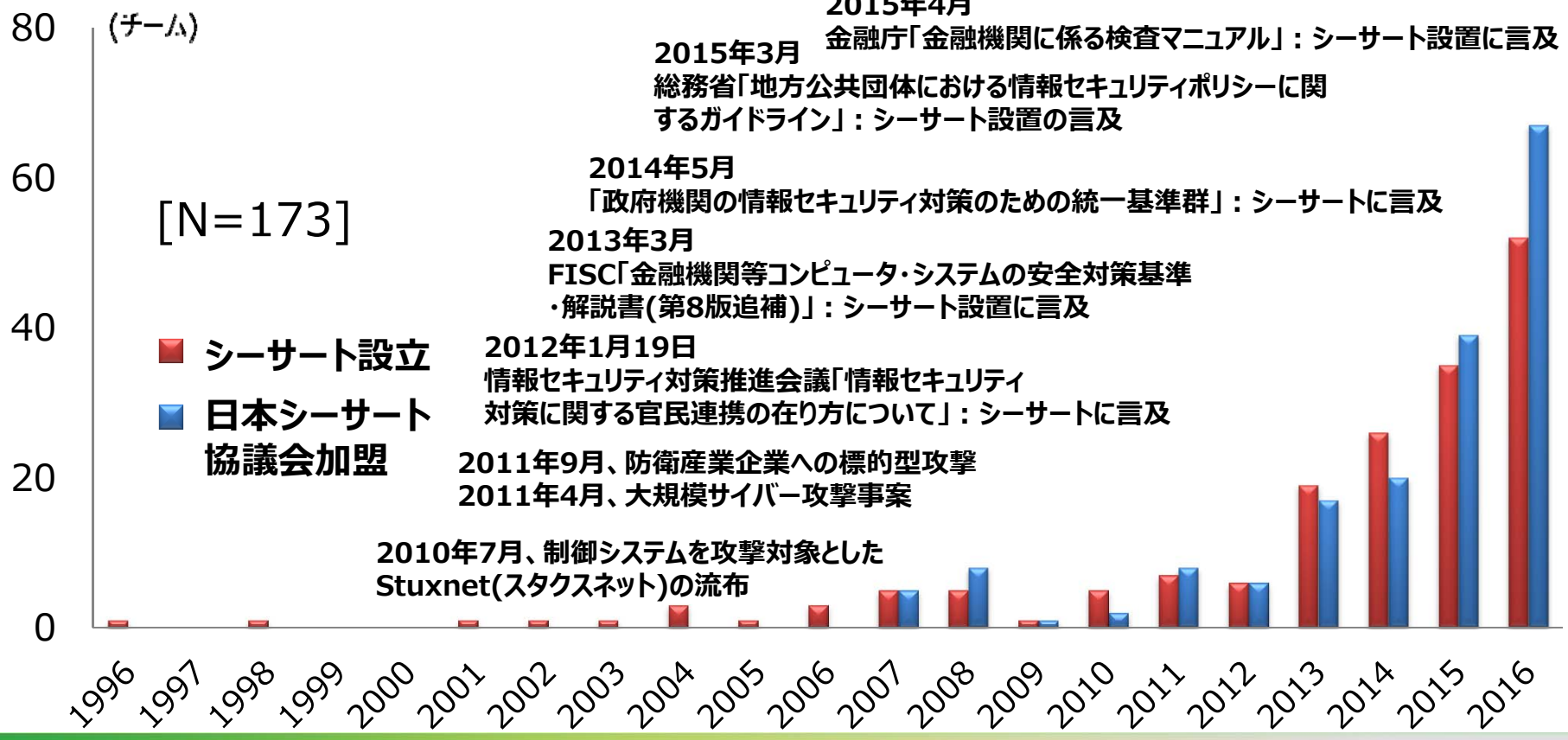
2 加盟企業の分類

- **業種による分類**
  - 多様な分野でシーサート構築が進んでいる。



2 加盟企業の分類

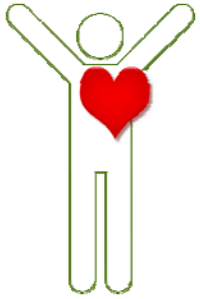
- **シーサート設立年と加盟年の推移**
  - 2013年以降、シーサート設立と加盟が急速に進んでいる。



2 日本シーサート協議会の特色

- **ボランタリーな活動**
  - 問題提起と解決のためのワーキンググループ活動
  - MLサービス、ドメイン、ウェブ運用
  - 事務局
  - 運営委員

- **マインド、モチベーションの高い仲間**



- **多様性**
  - 情報関連企業だけでなく
  - 製造(自動車、家電)
  - 金融、建設、流通　他

目次

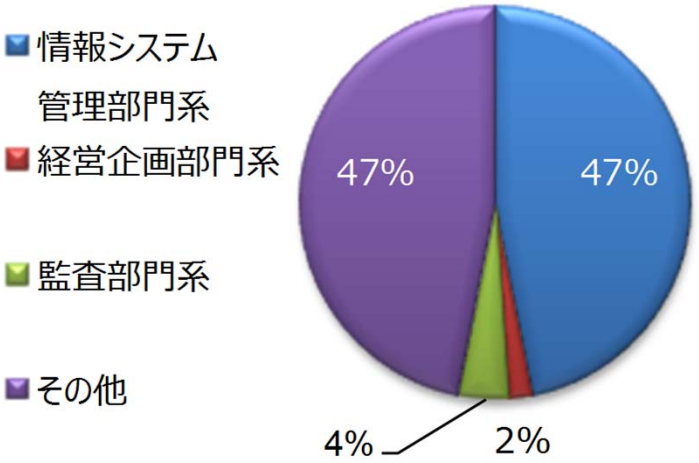
サイバー攻撃に対するセキュリティ施策として、インシデント対応、情報交換や組織間の連携など、Computer Security Incident Response Team (CSIRT、シーサート)体制による活動への期待が高まっています。日本シーサート協議会では、連携と問題解決の場の提供を通して、シーサート活動を支援しています。本講演では、日本シーサート協議会の活動ならびに企業におけるシーサートの役割を紹介します。

- シーサートとは
- 日本シーサート協議会の活動
- **アンケートから見えてきたシーサート活動体制**
- 企業におけるシーサートの役割
- シーサートの構築
- 日本シーサート協議会の役割

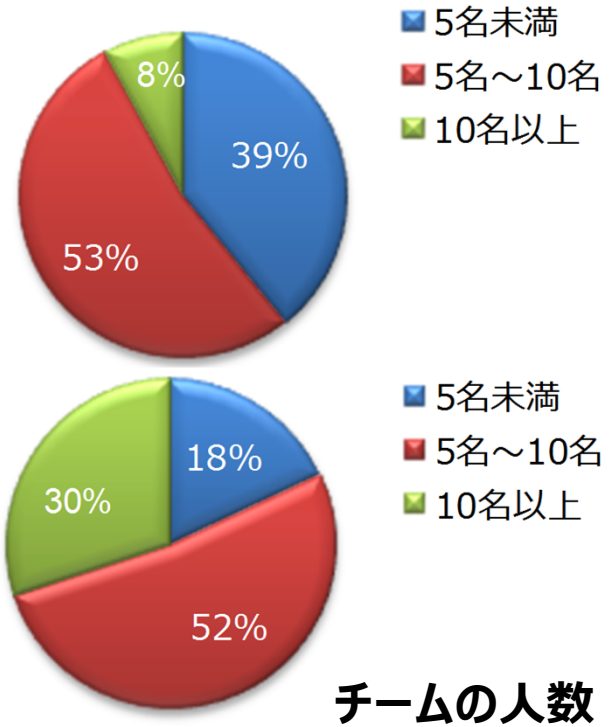
3 アンケートから見えてきたシーサート活動体制

※日本シーサート協議会加盟組織向け
2014年アンケート結果より

- **加盟組織の体制(1)**
  - **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

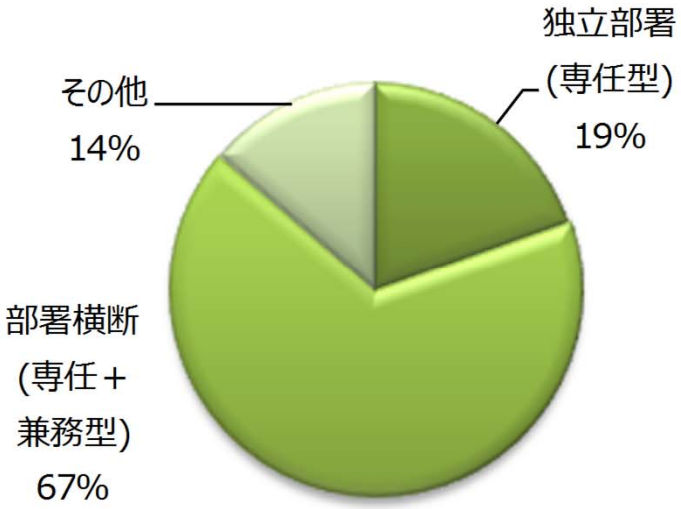


チームの人数
(上：設立時、下：活動開始後)

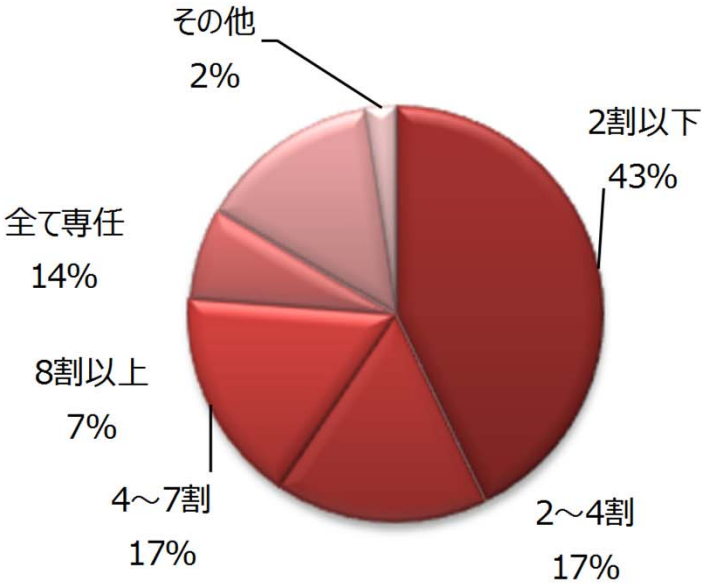
3 アンケートから見えてきたシーサート活動体制

※日本シーサート協議会加盟組織向け
2014年アンケート結果より

- **加盟組織の体制(2)**
  - **シーサート実装の多くは、専任のシーサート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**



実装の形態

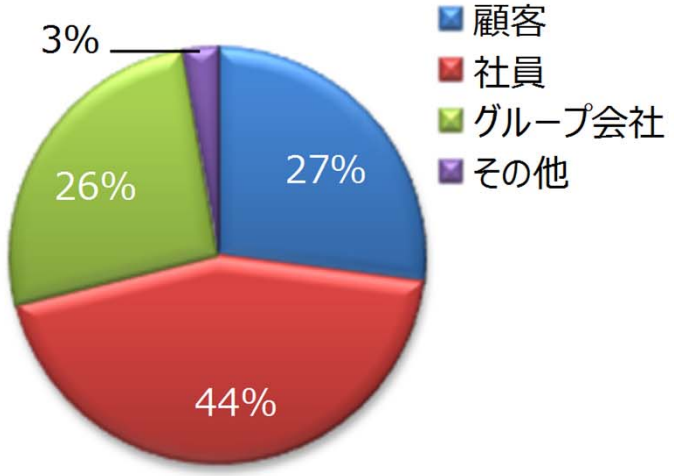


専任の割合

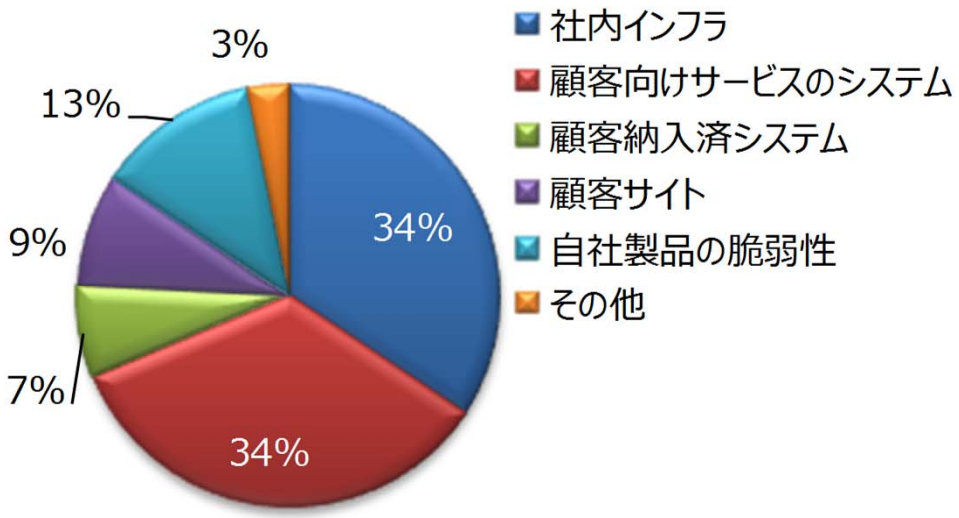
3 アンケートから見えてきたシーサート活動体制

※日本シーサート協議会加盟組織向け
2014年アンケート結果より

- **加盟組織のサービス**
  - **7割近くが、シーサート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

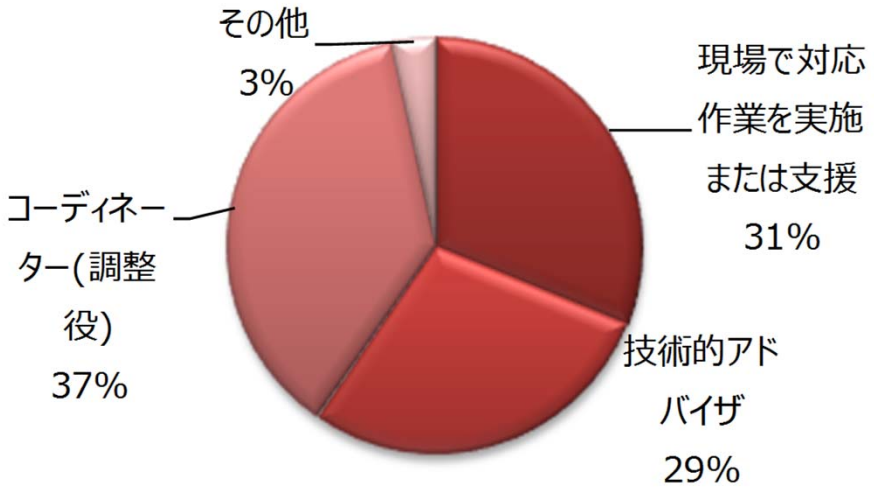


対象とする分野

3 アンケートから見えてきたシーサート活動体制

※日本シーサート協議会加盟組織向け
2014年アンケート結果より

- **インシデント対応時のシーサートの位置付け**
  - **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シーサートの位置付け

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では、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。

- シーサートとは
- 日本シーサート協議会の活動
- アンケートから見えてきたシーサート活動体制
- **企業におけるシーサートの役割**
- シーサートの構築
- 日本シーサート協議会の役割

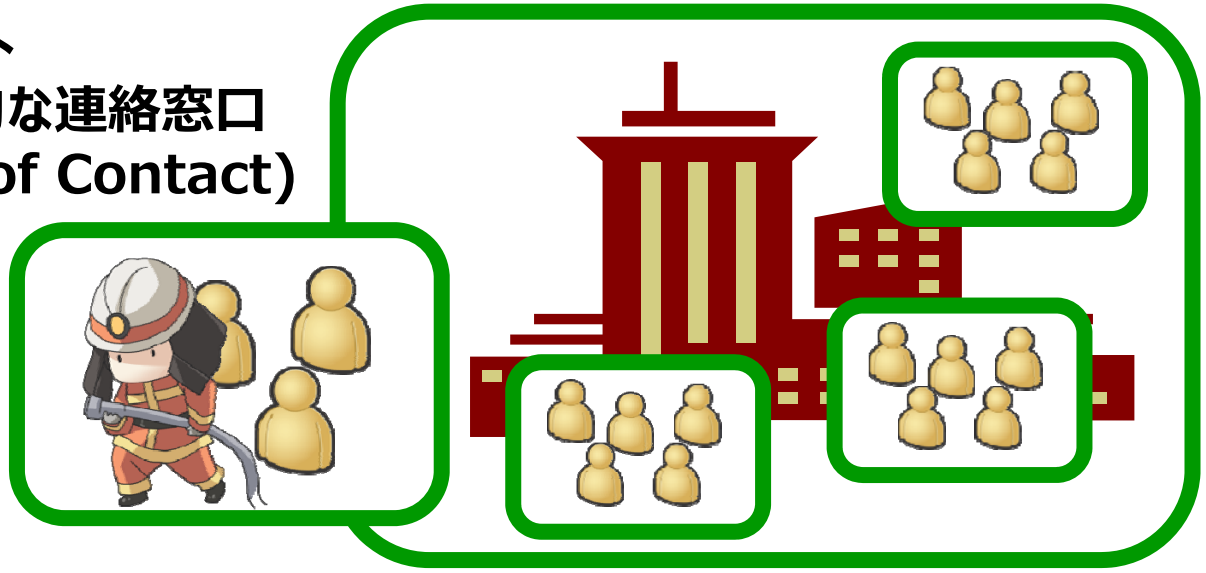
4 企業におけるシーサートの役割

- シーサート活動から導かれる企業におけるシーサートの役割
  - 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)



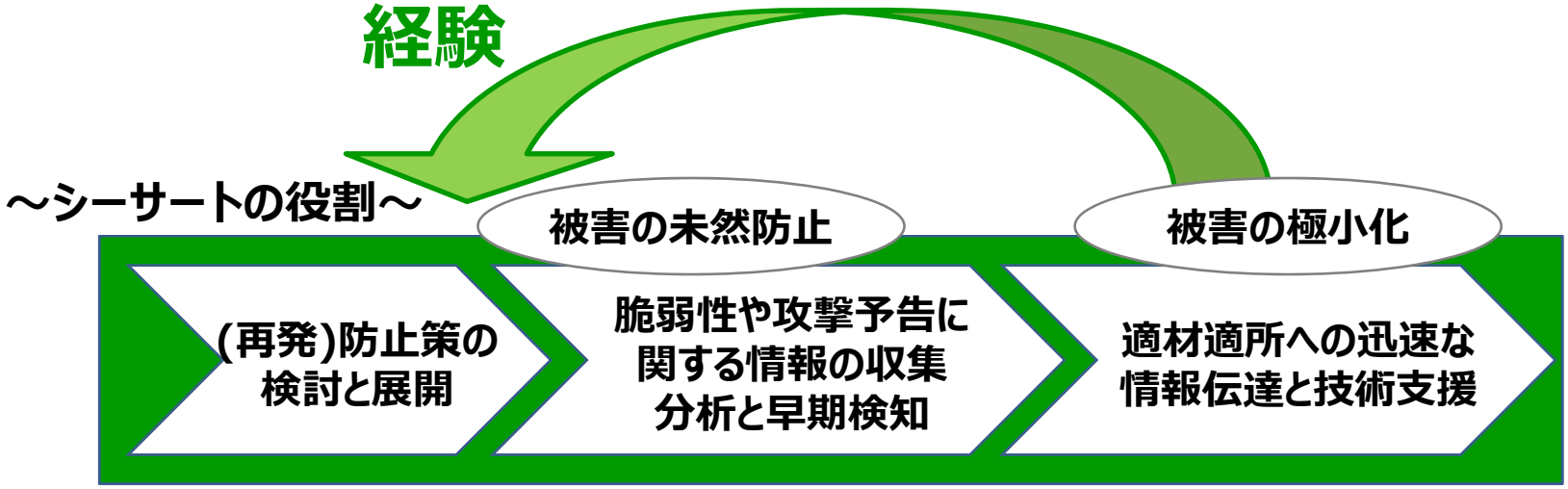
4 技術的な問合せに対応可

- 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。
まず重要なのは技術力ではなく、「コミュニケーション能力」

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

- シーサート実装の多くは、専任のシーサート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

サイバーセキュリティ対策の推進
特定の部署だけが頑張れば良い(お任せ)モデルから
組織全体で頑張る(連帯)モデルへ

シーサートは万能薬ではない。
組織のセキュリティ文化そのもの。

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では、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。

- シーサートとは
- 日本シーサート協議会の活動
- アンケートから見えてきたシーサート活動体制
- 企業におけるシーサートの役割
- **シーサートの構築**
- 日本シーサート協議会の役割

5 Mission（使命）を考える

出典：日本シーサート協議会「CSIRTスタータキット」

- なぜシーサートが必要なのか
  - シーサートのミッションを定義する
    - 組織が置かれている立場・状況
    - 目標を達成するために遂行する手段
    - 達成すべき目標

ABC-CSIRTのミッション

ABC社のセキュリティ分野における取組みの中核として、情報セキュリティに関する信頼できる相談窓口を提供し、ABC社内外の組織や専門家と協力して、セキュリティインシデントの検知、解決、被害局限化、および発生の予防を支援することにより、ABC社および情報ネットワーク社会のセキュリティ向上に貢献します。

5 インシデントを考える

出典：日本シーサート協議会「CSIRTスタータキット」

- シーサートが取り扱うインシデントとは何か
  - 組織におけるインシデントとは何か

プローブ、スキャン、そのほか不審なアクセス	- 弱点探索（サーバプログラムのバージョンのチェックなど） - 侵入行為の試み（未遂に終わったもの） - ワームの感染の試み（未遂に終わったもの）
サーバプログラムの不正中継	- メールサーバやプロキシサーバなどの、管理者が意図しない第三者による使用
不審なアクセス	- From: 欄などの詐称
システムへの侵入	- システムへの侵入、改ざん（root kitなどの専用ツールによるものも含む） - DDoS 攻撃用プログラムの設置（踏み台）
サービス運用妨害につながる攻撃（DoS）	- ネットワークの輻輳（混雑）による妨害 - サーバプログラムの停止 - サーバ OS の停止や再起動
コンピュータウイルス・ワームへの感染	
その他	- UCE(いわゆるスパムメール)の受信

表 3 一般的なインシデントの大別

5 Service（役務内容）を考える

出典：日本シーサート協議会「CSIRTスタータキット」

- シーサートが提供するサービスは何か
  - シーサートのサービスを定義する
    - インシデント事後対応サービス
      - インシデントの被害局限化を目的とした、インシデントやインシデントに関連する事象への対応を行うためのサービス。
    - インシデント事前対応サービス
      - インシデントの発生抑制を目的とした、インシデントやセキュリティイベントの検知や、発生の可能性を減少させるためのサービス。
    - セキュリティ品質向上サービス
      - 社内セキュリティの品質を向上させることを目的としたサービス。CSIRT としての視点や専門知識での見識を提供し、社内組織と連携することにより効果的な活動を実施できる。間接的にインシデントの発生抑制をすることが可能。

5 Constituency（活動範囲）を考える

- シーサートはどの範囲でサービスを提供するのか
  - シーサートのコンスティテュエンシーを定義する
    - 組織
    - 社内/社外
    - 部門
    - 人
    - システム など

- さらなる詳細は日本シーサート協議会「CSIRTスタータキット」をご参照ください
  http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

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では、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。

- シーサートとは
- 日本シーサート協議会の活動
- アンケートから見えてきたシーサート活動体制
- 企業におけるシーサートの役割
- シーサートの構築
- **日本シーサート協議会の役割**

6 場の整備

国内のシーサートコミュニティの急速な拡大への対応

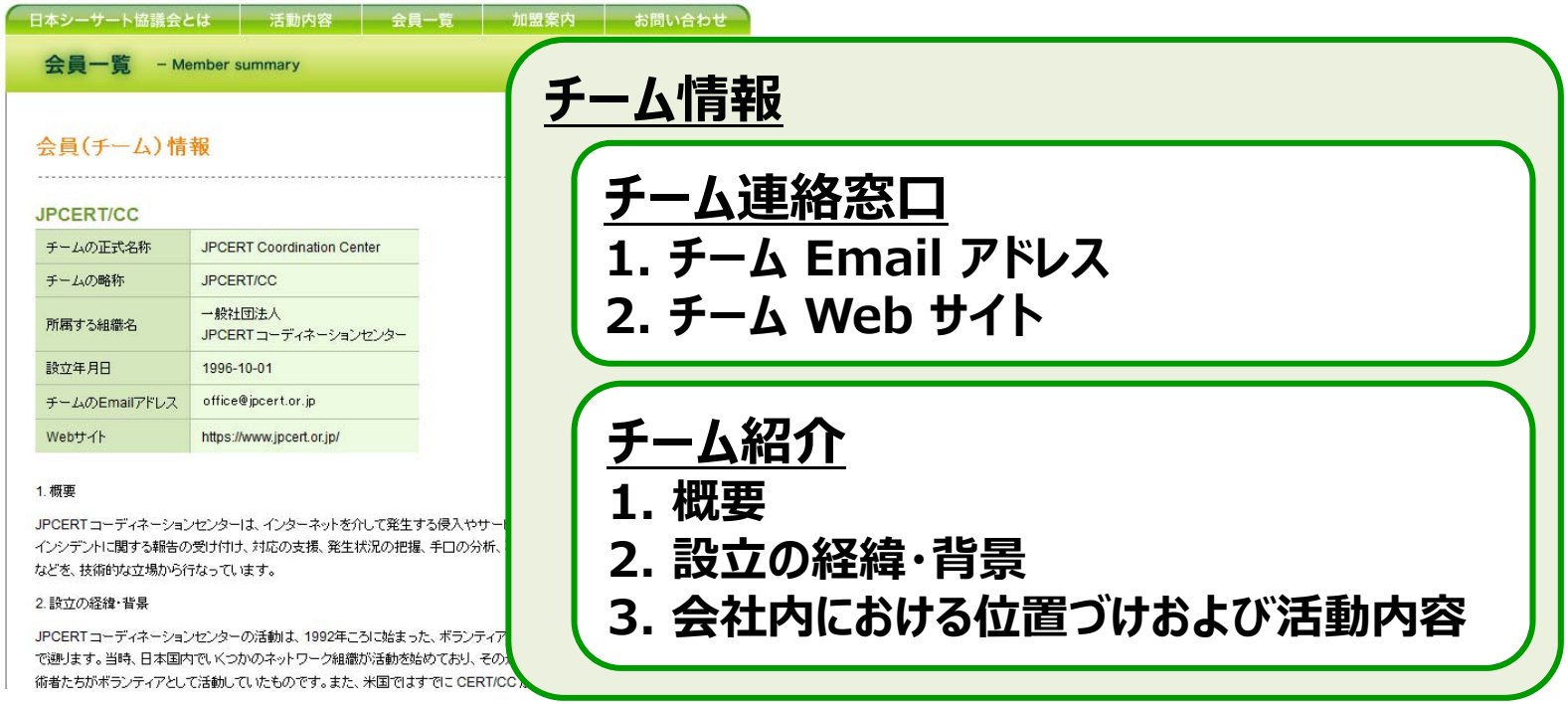
- **{組織間の協力 x (事前対処＋事後対処)}に向けた場の提供**
  - 分野横断的な場の提供
  - セキュリティ業界のパイプ役

- **{組織間の協力 x (事前対処＋事後対処)}に向けた場の整備**
  - ディレクトリ(日本シーサート協議会加盟組織一覧)の整備
  - シーサート活動の暗黙知(慣習)の明文化

国内のシーサートコミュニティが、いざというときに協力して活動できるための場の提供と整備

6 シーサート連絡窓口（PoC）の整備

- アドレス帳(日本シーサート協議会加盟組織一覧)の整備
  - 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、チーム情報をまとめた資料
    ⇒シーサート連絡窓口(PoC: Point of Contact)の整備

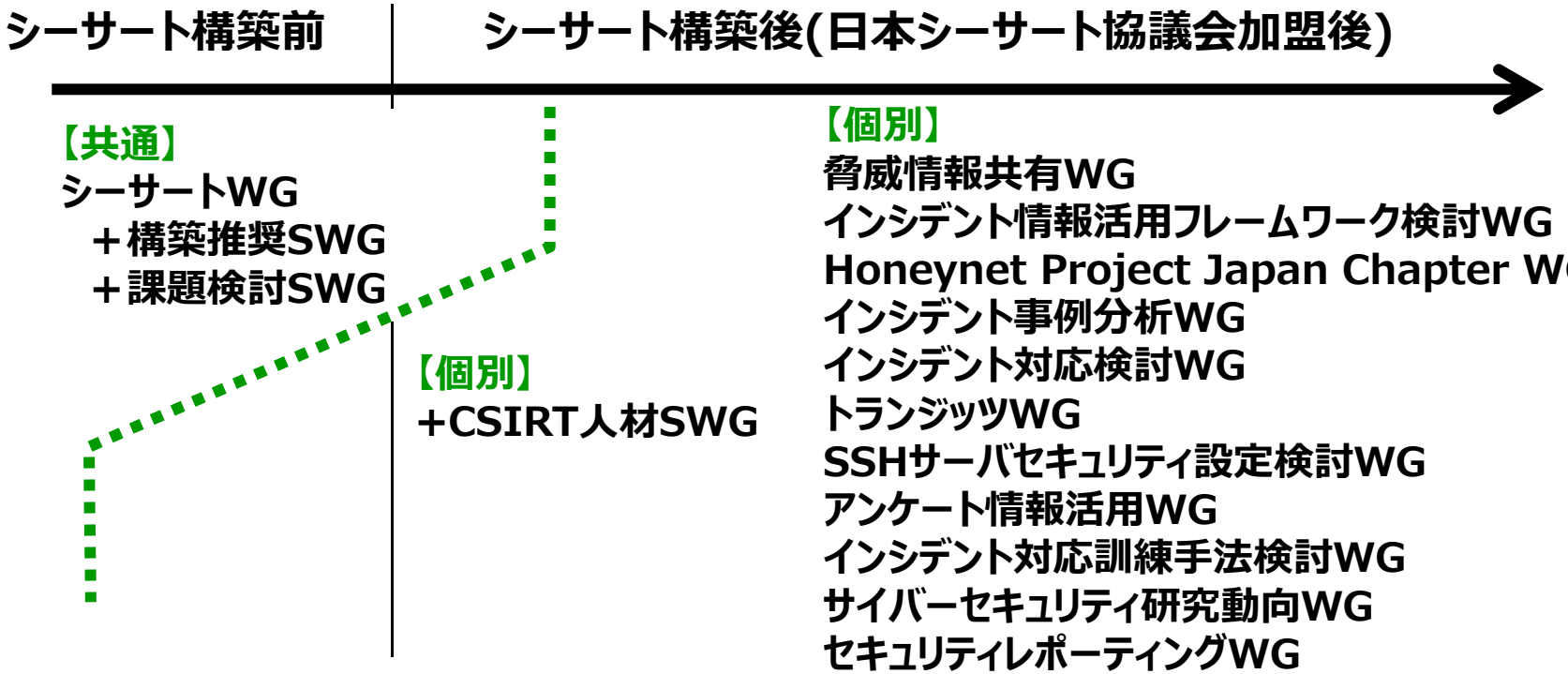


http://www.nca.gr.jp/member/index.html

6 ワーキンググループ活動

※2016年9月時点

- ワーキンググループ
  - 問題提起と解決のための活動としてワーキンググループを立ち上げ、会員ならびに協議会外部の協力者と共に、問題解決を図っていきます。



【活動中のワーキンググループの位置付け】

6 場の整備

- シーサート活動の暗黙知(慣習)の明文化
  - 会合、メーリングリスト等でのチャタムハウスルールの徹底

Chatham House Rule

The Chatham House Rule reads as follows:

> *When a meeting, or part thereof, is held under the* **Chatham House Rule**, *participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.*

http://www.chathamhouse.org/about/chatham-house-rule

6 場の整備

- シーサート活動の暗黙知(慣習)の明文化
  - 用語の定義差異を踏まえた対応

あなたが使っている「インシデント」と、
先方が使っている「インシデント」は、同じですか?

日本シーサート協議会に加盟している組織を俯瞰すると、
体制、対象とする分野、取りまとめる部署など、
一つとして同じ形態のシーサートはなく、百社百様。
⇒用語の使い方についても、違いがでてきている。
同じ単語が、必ずしも同じものを意図するわけではない。

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/