日本シーサート協議会の活動について

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
2017年07月25日

目次

- シーサートとは
- 日本シーサート協議会とは
- 協議会の役割
- 協議会の活動
- 参考情報：アンケートから見えてきたシーサート活動

1 シーサートとは

- **CSIRT(シーサート)**
  Computer Security Incident Response Teamの略
  - 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に活動している。**
  - 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

- 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

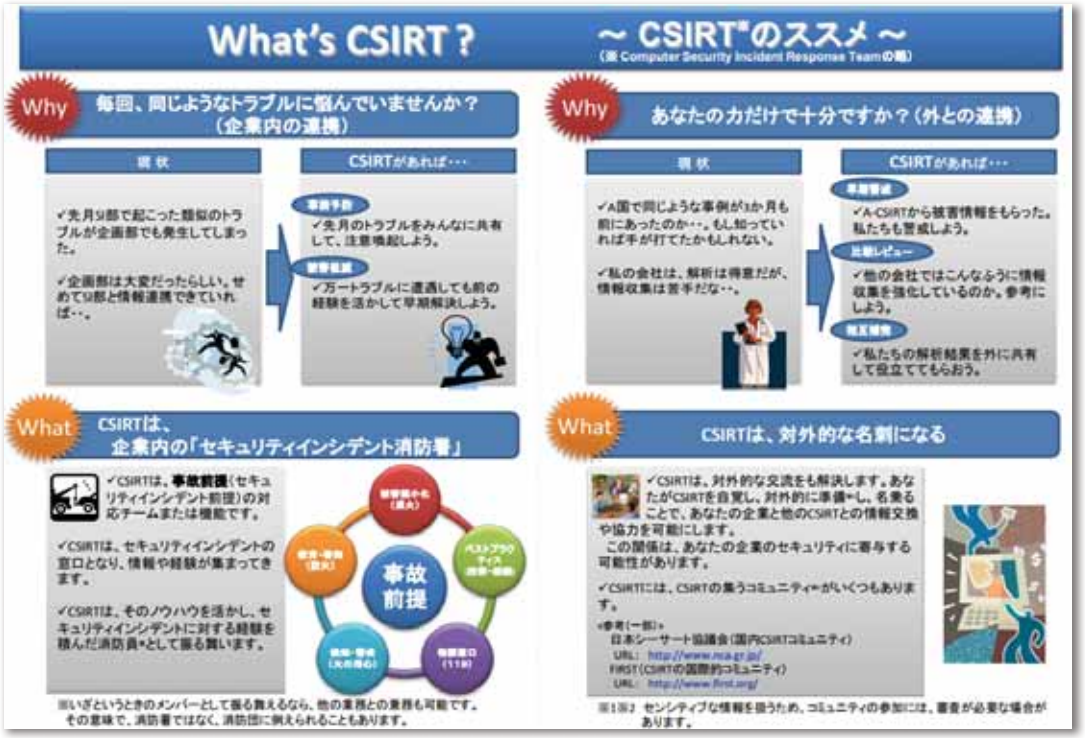
官民の連携に当たっては、漠然と組織間で情報共有を行うのではなく、各組織が情報セキュリティインシデントに関する緊急時対応の機能を有した専門的な部隊(以下「CSIRT(Computer Security Incidents Response Team)等」という。)を組織し、官民を含む各組織内 CSIRT 等の間で、専門的、実務的な連携を図ることが必要である。

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(2012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

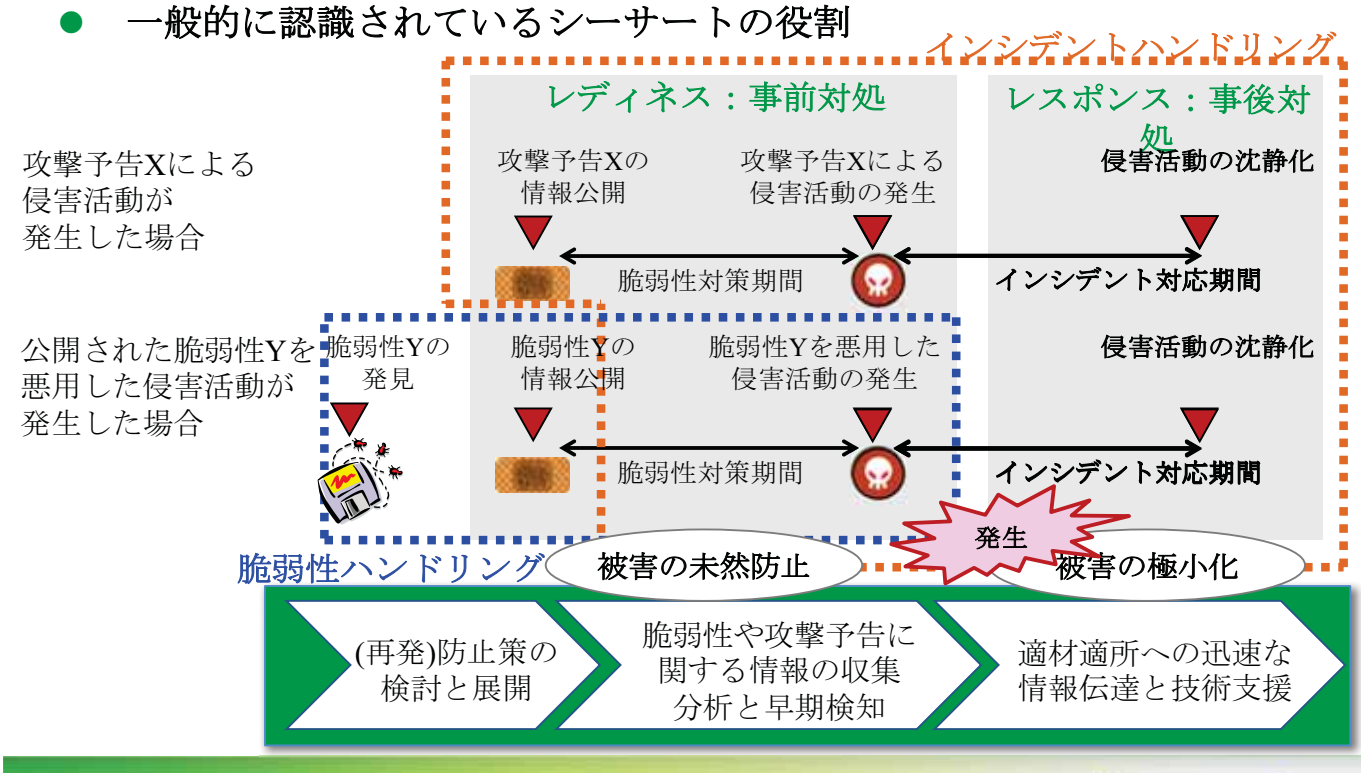
1 シーサートとは



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

- 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

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/

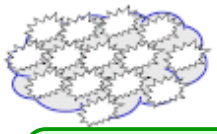
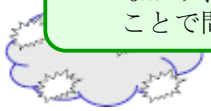
米国におけるセキュリティ事案情報、脆弱性情報の収集ならびに調整機関

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、2017年7月末現在、81カ国380チームが加盟

1 シーサートとは

- 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	
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、手段を共有することで問題解決を図る

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

- シーサートは多種多様

活動範囲の視点から、組織シーサート、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、対象範囲、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。

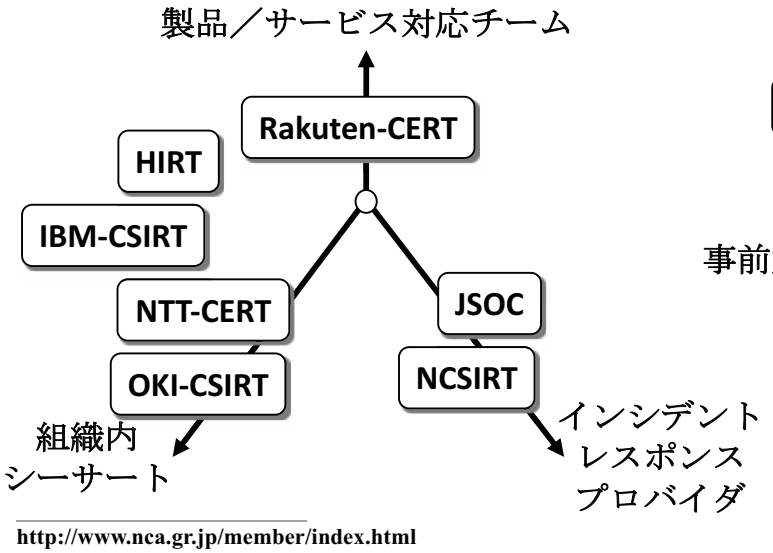
- 対象範囲：国、自組織、顧客
- 内容(フェーズ)：事前対処、事後対処
- 内容(機能)：脆弱性ハンドリング、インシデントハンドリング、動向分析、リスク分析など
- 体制：集約型／分散型、専任型／兼務型

組織シーサート
自組織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。

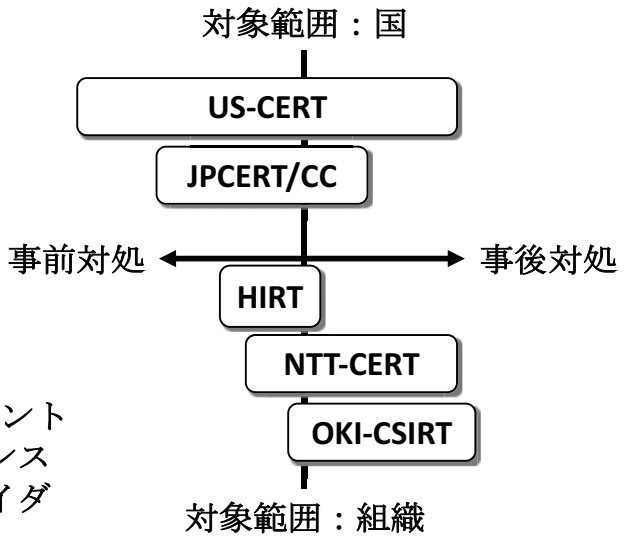
製品／サービス対応シーサート
提供する製品やサービスのインシデントに対応するシーサートと定義する。

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



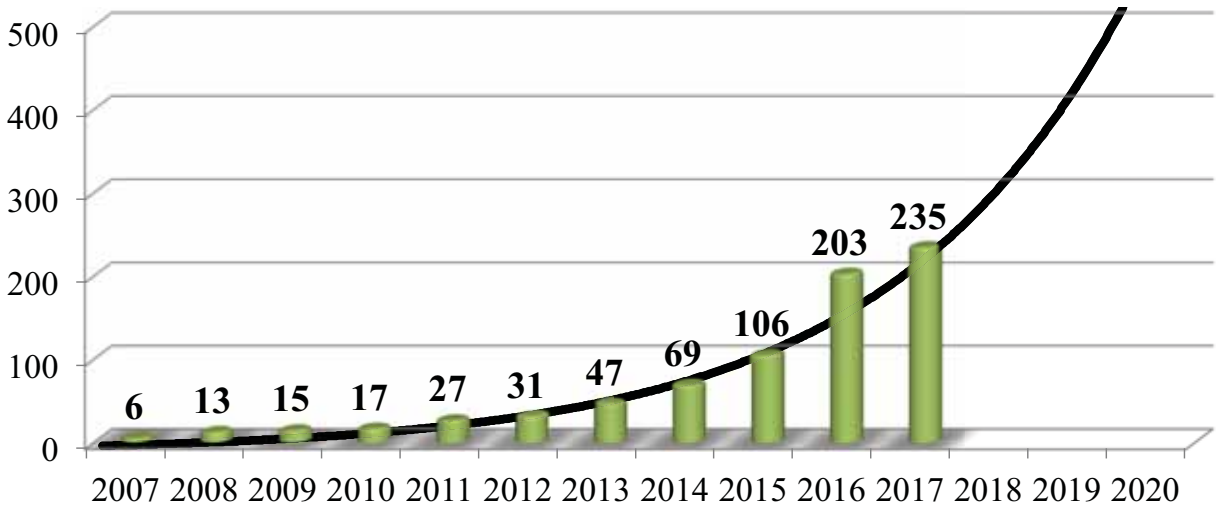
目次

2 組織概要

- 設立
  - 2007年3月
- 名称
  - 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/
- 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

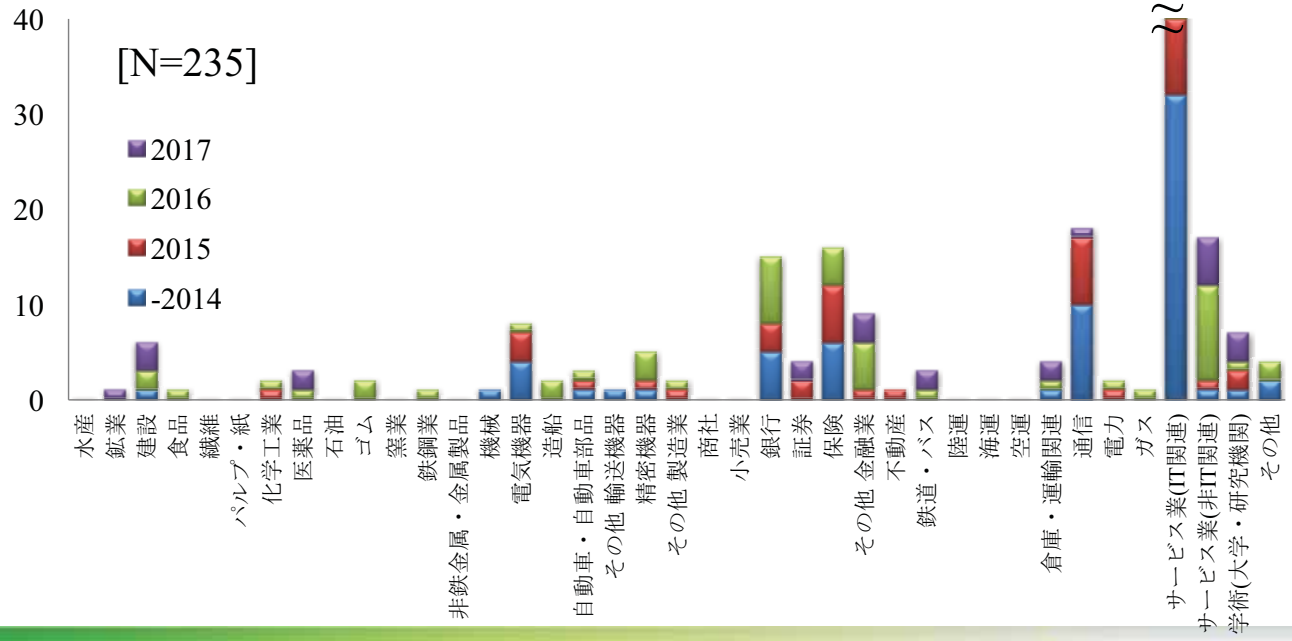
2 組織概要
～データからみた日本シーサート協議会～

- 加盟数(累積)の推移
  - 235チーム(2017年7月1日現在)
  - このままいくと、2020年には、 500チーム???



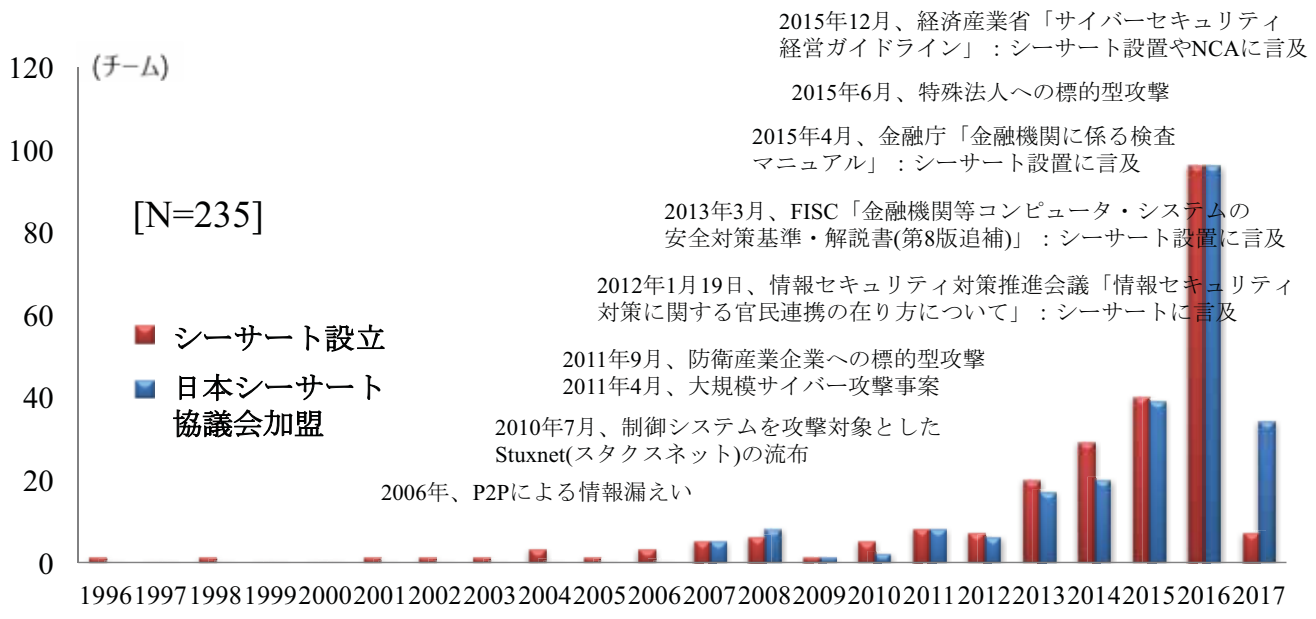
組織概要
～データからみた日本シーサート協議会～

- 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。



組織概要
～データからみた日本シーサート協議会～

- 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 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

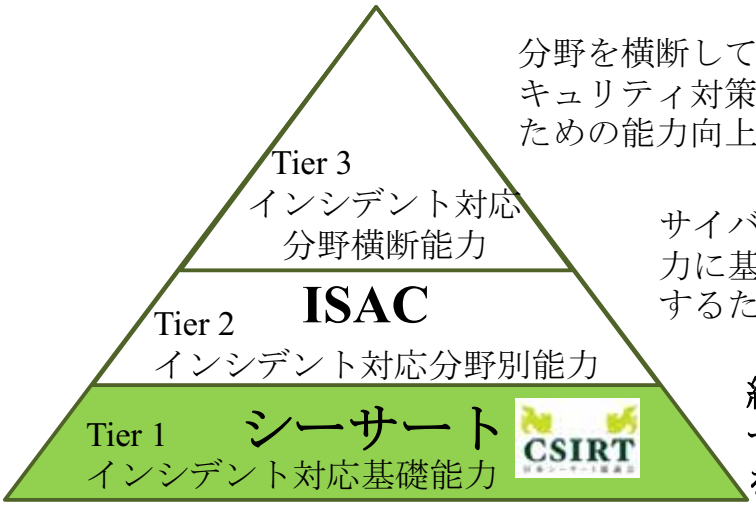
3 日本シーサート協議会の役割

- 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 × (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
    - 地区毎で顔の見える活動の場の提供
  - {組織間の協力 × (事前対処＋事後対処)}に向けた場の整備
    - アドレス帳(日本シーサート協議会加盟組織一覧)の整備
    - シーサート活動の暗黙知(慣習)の明文化
    - 地区毎で顔の見える活動の場の整備

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

3 日本シーサート協議会の役割

- 協力して活動できるための場の提供と整備
  - {組織間の協力 × (事前対処＋事後対処)}に向けた場
    - 組織自身が自主的に「インシデント対応基礎能力」の向上を図れる場



分野を横断してサイバーセキュリティ対策を推進するための能力向上を図る。

サイバーセキュリティ基礎能力に基づき、分野対策を推進するための能力向上を図る。

組織自身が自主的にサイバーセキュリティ基礎能力の向上を図る

目次

- シーサートとは
- 日本シーサート協議会とは
- 協議会の役割
- 協議会の活動
- 参考情報：アンケートから見えてきたシーサート活動

4 2017年度の活動方針

- **(1)行動指針に基づいた協議会運営**
  協議会に加盟する各社のシーサートが増えるにつれ、各シーサートが協議会内で活動する際の方向性や行動にばらつきが生じ、非効率的な活動が見られる。国内各所にシーサートが3,000チームできたときに機能する協議会体制とするためにも、行動指針に基づいた協議会運営を推進する。

正義の味方	社会貢献、トラブルをさっそうと解決する有志による無償の提供、積極的な姿勢、強制的にさせられている訳ではない、という事を端的に示す。
自由と責務	信頼関係を築くためには積極的な連携、情報提供が必要。黙って聞いているだけでは信頼は得られない。情報を提供した分だけ、信頼感があがると考えよ。
チャレンジと自己研鑽	常に自分を自己研鑽し、プロフェッショナルであること、新しい事、だれも手をつけていない事に積極的にチャレンジすべし。そして、メンバはその人を否定するのではなく、全力でフォローする事。
Open Door	協議会内、WG間で垣根を作らない事。どのメンバも参加、見学に対しては温かく迎える事。

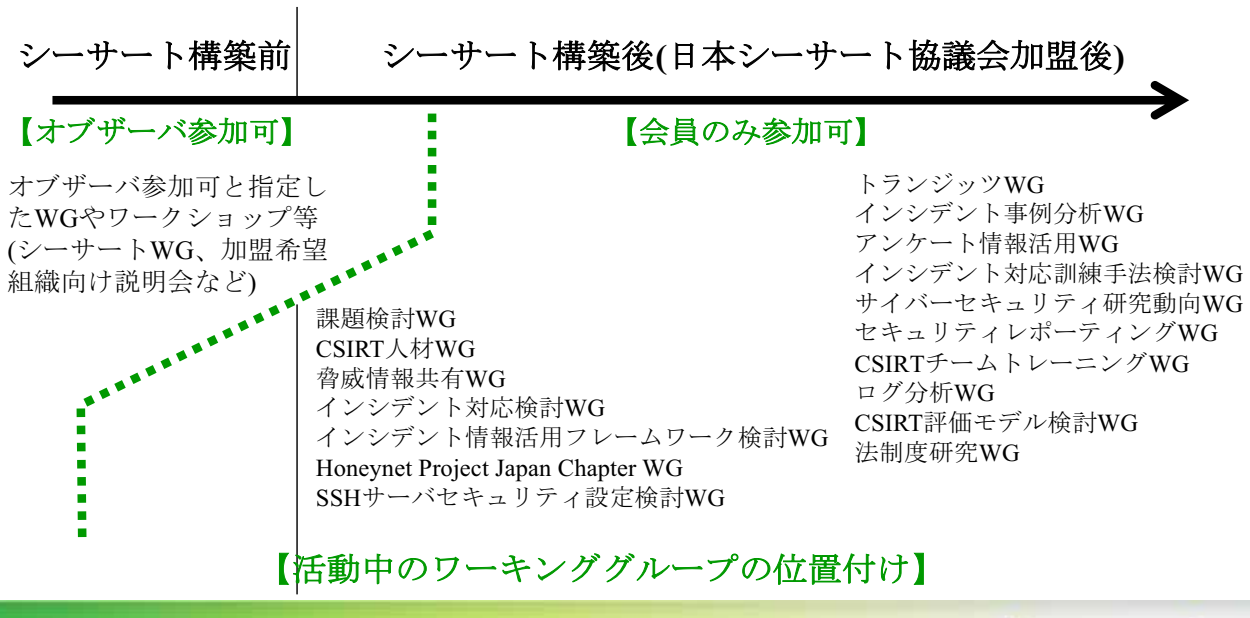
4 2017年度の活動方針

- **(2)シーサート組織の連携基盤の整備**
  「シーサート活動の暗黙知(慣習)の明文化」を通して、シーサート組織の連携基盤の整備を継続する。具体的には、「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」、「シーサート組織の連絡窓口(PoC)の啓発」、「ディレクトリの整備」を推進する。

- **(3)連携と規模拡大を想定した運営体制の推進**
  国内各所にシーサートが3,000チームできたときに機能する協議会運営体制となるよう推進する。具体的には、「加盟チーム以外も含めたシーサート組織の連絡窓口(PoC)の啓発教育」、「地区活動の継続(全体での場の提供だけではなく、地区毎での顔の見える活動の場の提供)」、「協議会運営基盤の整備」 「運営体制の改善」を実施する。

4 協議会の活動
～(1)行動指針に基づいた協議会運営～

- **ワーキンググループ活動**
  - 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、問題解決を図る。



協議会の活動
～(2)シーサート組織の連携基盤の整備～

- 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

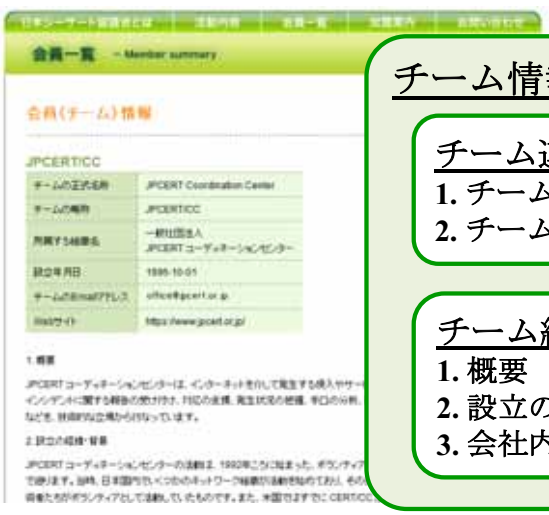
The Chatham House Rule reads as follows:

*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.*

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

協議会の活動
～(2)シーサート組織の連携基盤の整備～

- 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
  - 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



チーム情報

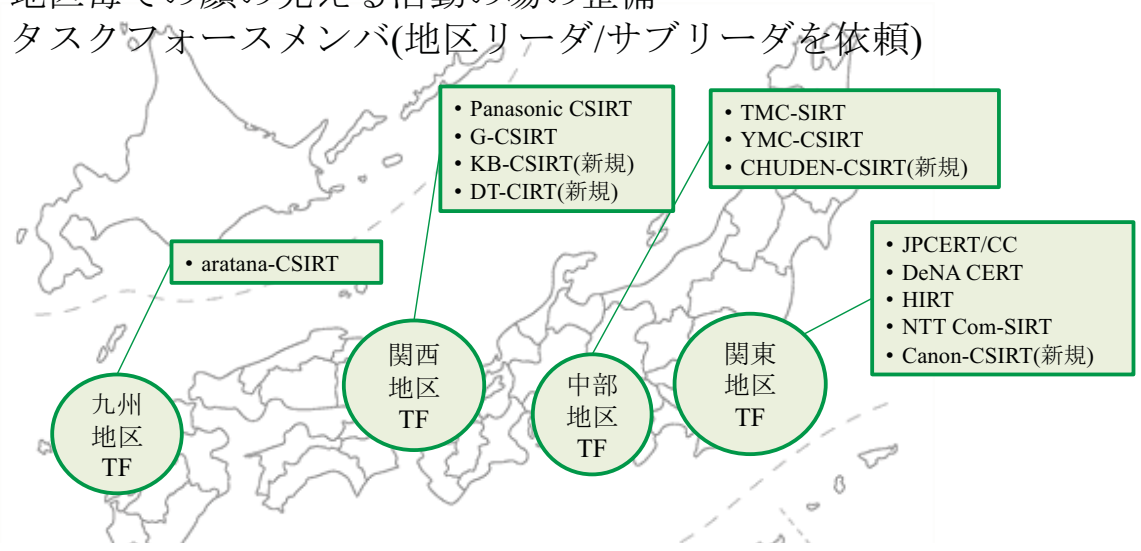
チーム連絡窓口
1. チーム Email アドレス
2. チーム Web サイト

チーム紹介
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

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

4 協議会の活動
～(3)連携と規模拡大を想定した運営体制の推進～

- **地区活動タスクフォース**
  - 地区毎での顔の見える活動の場の整備
  - タスクフォースメンバ(地区リーダ/サブリーダを依頼)



地域のシーサート構築促進に係るワークショップ等を企画運営し、加盟会員の増加や地域活動の推進に協力してもらっているチーム

4 協議会の活動
～(3)連携と規模拡大を想定した運営体制の推進～

- **<u>シーサートワークショップ</u>**
  - **関東地区**
    - 当初、加盟希望組織向け説明会から開始したが、一定の目的を達成したところから、加盟後チームの今の取り組み(チームアップデート)にフォーカスした会合に移行中

加盟希望組織向け説明会主体
- 第1回：2016年2月2日@DeNA CERT.渋谷(約30名)
- 第2回：2016年3月1日@JPCERT/CC.神保町(約20名)
- 第3回：2016年5月17日@HIRT.大森(約20名)
- 第4回：2016年7月6日＠CDI-CIRT.八重洲(約25名)
- 第5回：2016年10月17日＠YIRD.紀尾井町(約30名)
- 第6回：2016年12月9日＠OKI-CSIRT.虎ノ門(約30名)
- 第7回：2017年3月3日@Canon-CSIRT.下丸子(約30名)

チームアップデート主体
- 第8回：2017年5月16日@TM-SIRT.新宿(約25名)
- 第9回：2017年7月4日@Cy-SIRT.中央区(約35名)

4 協議会の活動
～(3)連携と規模拡大を想定した運営体制の推進～

- シーサートワークショップ
  - **中部地区**(渡辺先生@名古屋工業大学)
    - 2016年6月27日(月)@TMC-SIRT.名古屋
      中部地区：23名(20組織)、中部地区以外：24名(14組織)
  - **九州地区**(岡村先生@九州大学、廿日出先生@宮崎大学)
    - 2016年8月18日(木)@IIJ-SECT.福岡
      九州地区：17名(10組織)、九州地区以外：13名(10組織)
    - 2016年8月19日(金)@aratana-CSIRT.宮崎
      九州地区：15名(6組織)、九州地区以外：16名(11組織)
  - **関西地区**(中野先生@帝塚山学院大学)
    - 2016年9月27日(火)@Panasonic CSIRT.大阪
      関西地区：31名(13組織)、関西地区以外：11名(8組織)

4 協議会の活動
～(3)連携と規模拡大を想定した運営体制の推進～

- **2017年のシーサートワークショップ開催の目的**
  サイバーセキュリティ(地震、自然災害などのフィジカルセキュリティを含む)に備えるため、地域の学術、自治体、警察、企業(中小企業支援を含む)が少なくとも、年1回、顔を合わせる場を作ることから

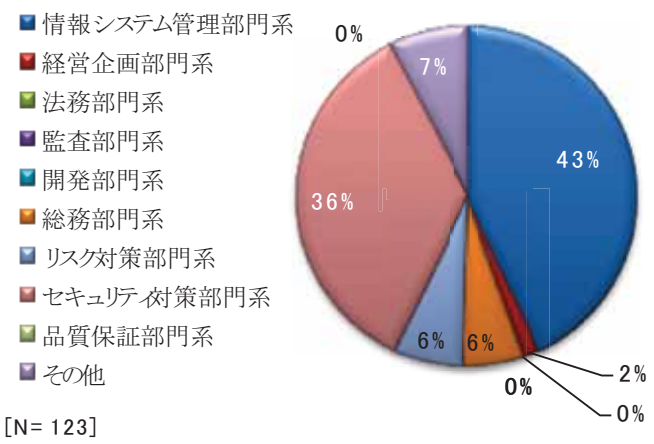
2017年度	地区	会場
2017年5月24日(水)	シーサートワークショップ in 名古屋 渡辺先生@名古屋工業大学	@CHUDEN-CSIRT
2017年7月18日(火)	シーサートワークショップ in 浜松	@Entetsu-SIRT
2017年秋	シーサートワークショップ in 大阪 中野先生@帝塚山大学	
2017年11月9日(木)	シーサートワークショップ in 福岡 岡村先生@九州大学	@Qdai CSIRT
2017年11月10日(金)	シーサートワークショップ in 宮崎 廿日出先生@宮崎大学	@aratana-CSIRT

目次

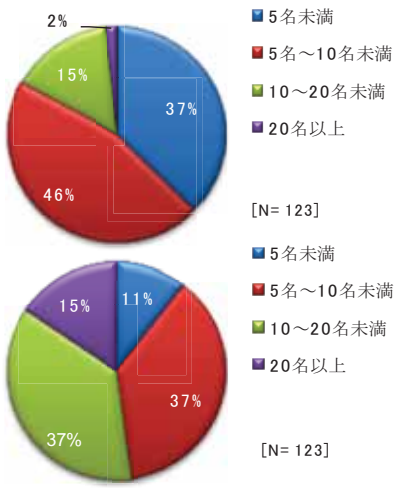
- シーサートとは
- 日本シーサート協議会とは
- 協議会の役割
- 協議会の活動
- 参考情報：アンケートから見えてきたシーサート活動

5 アンケートから見えてきたシーサート活動
～日本シーサート協議会加盟組織一覧2016より～

- **加盟組織の体制(1)**
  - 『情報システム管理部門系』『セキュリティ対策部門系』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



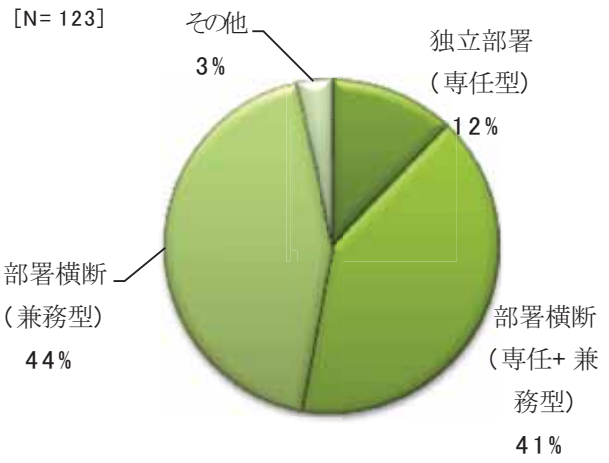
取り纏め部署



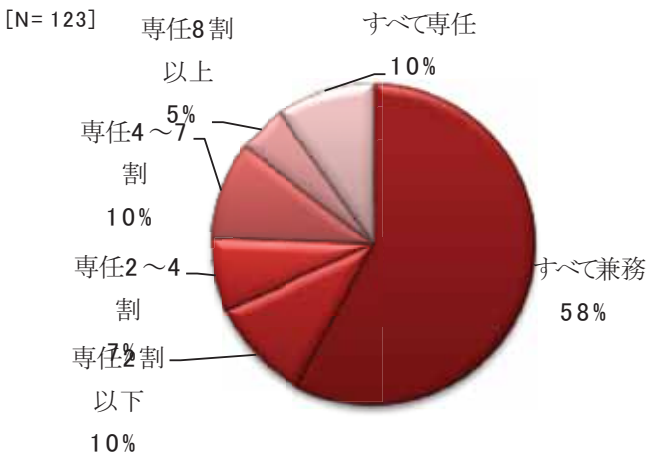
チームの人数
(上：設立時、下：活動開始後)

5 アンケートから見えてきたシーサート活動
～日本シーサート協議会加盟組織一覧2016より～

- **加盟組織の体制(2)**
  - シーサート実装の多くは部署横断型⇒**部署間を横断した組織体制の構築**



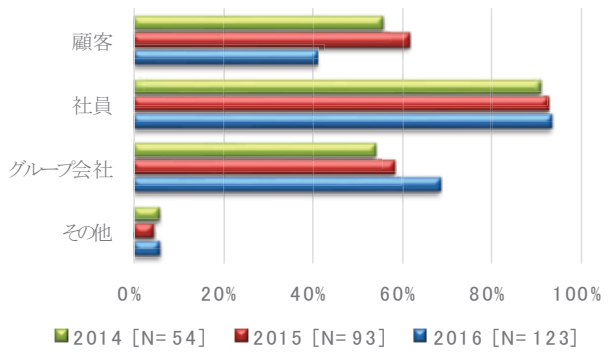
実装の形態



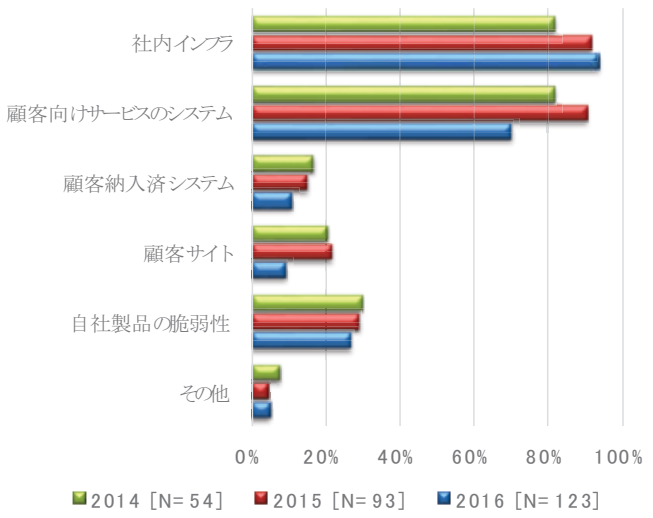
専任の割合

5 アンケートから見えてきたシーサート活動
～日本シーサート協議会加盟組織一覧2016より～

- **加盟組織の活動概要**
  - 主に、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)



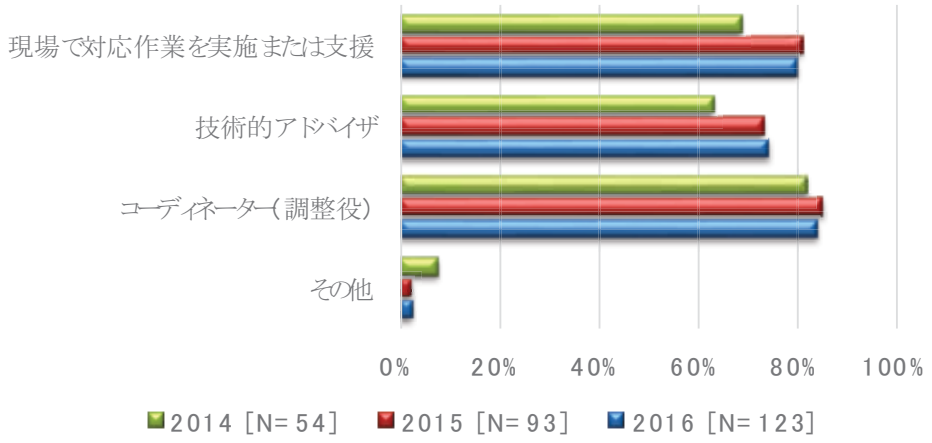
対象とする利用者



対象とする分野

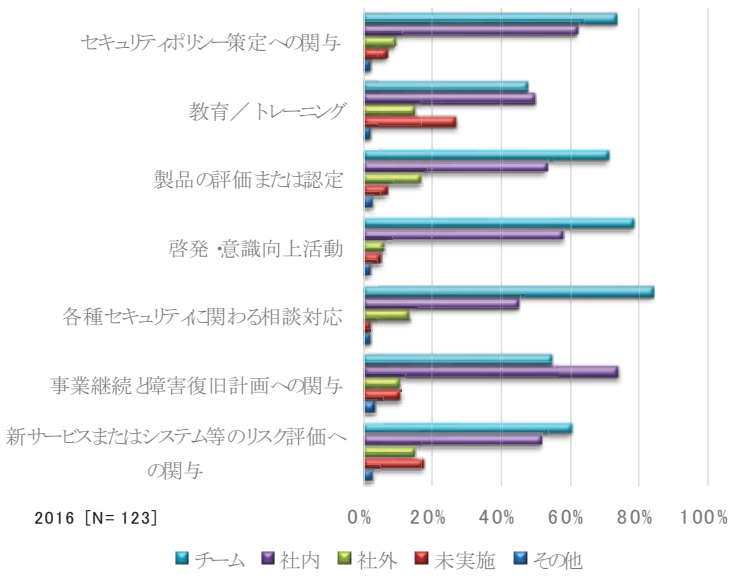
5 アンケートから見えてきたシーサート活動
～日本シーサート協議会加盟組織一覧2016より～

- 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)としての側面への期待



5 アンケートから見えてきたシーサート活動
～日本シーサート協議会加盟組織一覧2016より～

- セキュリティ相談窓口としての役割
  - 8割以上が各種セキュリティに関わる相談をチーム内で対応



ご清聴ありがとうございました。

CSIRT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。

CSIRT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/