IoTセキュリティセミナー　2018.2.26

IoT時代のCSIRT

～ PSIRT構築の課題 ～

株式会社ラック

原子　拓

アジェンダ

0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

アジェンダ

0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

はじめに

いろいろな物がインターネットに繋がるIoT化が進むのに伴い、付加価値が生まれ便利になる一方、IoT機器に脆弱性があれば誤作動を起こしたりサイバー攻撃に利用されたりする可能性があります。
本セッションでは、IoT時代の企業内CSIRT（PSIRT：Product Security Incident Response Team）のあり方について、現状のCSIRTの実態を明らかにしつつ、あるべき姿と実現に向けた課題について解説します。

はじめに

大事なページには、ポイント マークがあります。

そこだけ覚えておいてください。

アジェンダ

0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

1. プロフィール

ポイント

原子　拓
はらこ　　たく

株式会社ラック

1988年　株式会社日立情報ネットワーク入社、日立製作所システム開発研究所にて
　　ネットワーク関連の研究開発に従事。
1991年　ヤマハ発動機株式会社入社、情報システム部門にて26年間インフラ・アーキテク
　　チャ全般の企画を担当。YMC-CSIRT リーダー。
　　Webサイトについては、公式Webサイト立ち上げから20年間インフラ・セキュ
　　リティを担当。2012年にYMC-CSIRTを立ち上げ、その後NCA加盟。
　　デジタル戦略Gを兼務して IoT、SmartFactoryのセキュリティを担当。
2017年　株式会社ラックに入社、サイバーセキュリティ関連業務に従事。

2016年　日本シーサート協議会（NCA）運営委員。

1. プロフィール

原子　拓
はらこ　　たく

株式会社ラ

1988年　株式会社日立情報ネットワーク入社、日立製作所システム開発研究所にて
ネ

1991年　ヤマハ　　テク
チ
W　　セキュ
リ　　を担当、2013年にYMC-CSIRTをたちあげ、その後NCA加盟
デ

2017年　株式会

2016年　日本シーサート協議会（NCA）運営委員。

ネットワーク・セキュリティ エンジニア

グローバルエンタープライズIT

インターネット（Web・PKI・IoT）

CSIRT歴6年

1. プロフィール

■ヤマハ発動機のCSIRTやってました。

今はLACERT（ラック社内サート）メンバーです。

1. プロフィール

■最近の活動

- **日本シーサート協議会運営**
- **安全なWebサイト＆CSIRT**
  - ZDNet『Security Day 2017』
  - NanoOpt「Security Days Spring 2017」
  - 日経BP「情報セキュリティSummit」
- **クラウド、IoT、デジタル関連**
  - 翔泳社 「Security Online Day 2017」
  - 翔泳社「EnterpriseZine Day」 など

■消防団班長として、実火災・災害等の
リアルインシデントと戦っています。

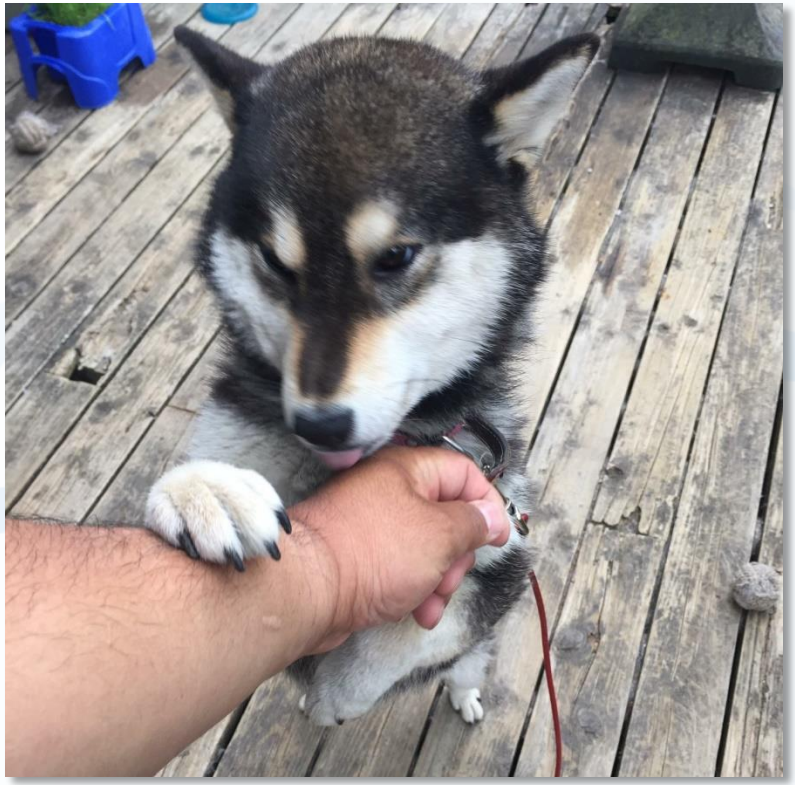
某市消防団

火災出動の様子

ポイント

LAC

■黒柴ちゃん🖤　飼ってます



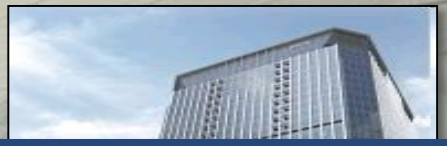
癒されてます

株式会社ラック ご紹介

名　称	株式会社ラック　(LAC Co., Ltd.)
本社所在地	〒102-0093 東京都千代田区平河町2丁目16番1号 平河町森タワー
事業所	アクシス事業所（喜多方） 名古屋事業所 福岡事業所
創　立	2007年10月1日
年間売上高	連結：371億円（2017年3月期）
従業員数	連結：1,734名（2017年4月1日現在）
上場市場	東京証券取引所　ジャスダック市場
事業概要	・セキュリティソリューションサービス ・システムインテグレーションサービス ・情報システム関連商品の販売およびサービス

株式会社ラック ご紹介

名　称	株式会社ラック　(LAC Co., Ltd.)
本社所在地	〒102-0093 東京都千代田区平河町2丁目16番1号
上場市場	東京証券取引所　ジャスダック市場
事業概要	・セキュリティソリューションサービス ・システムインテグレーションサービス ・情報システム関連商品の販売およびサービス



30年
歴史
セキュリティのパイオニアとして業界をリードしています

1,700人
従業員
私たちにとって、人材こそが最高の資産です

880
契約顧客・団体
JSOC®による国内最高レベルの監視サービスを提供しています

アジェンダ

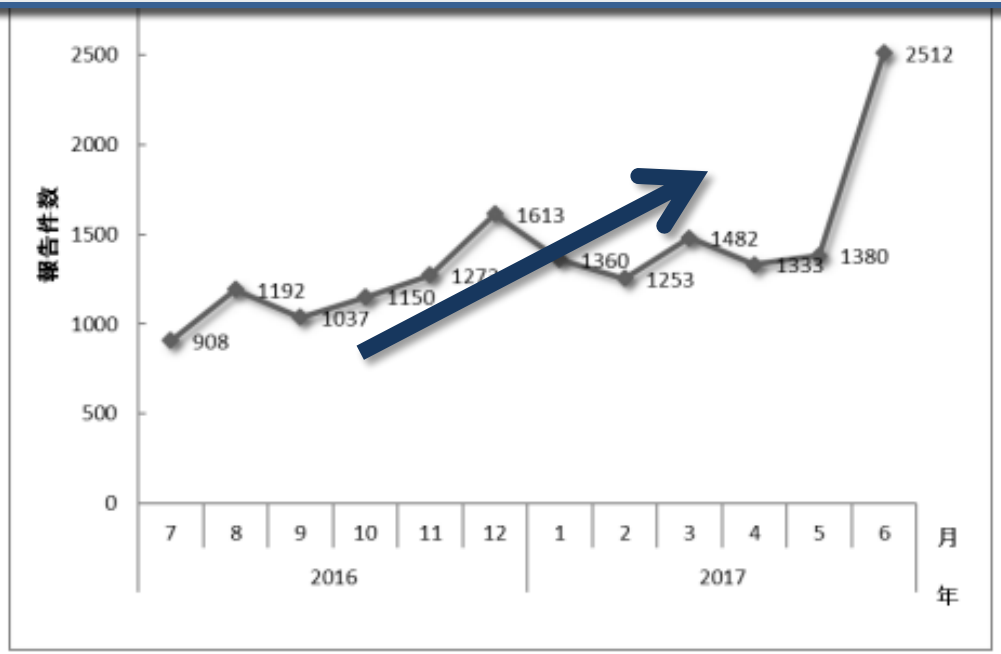
0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

インシデント報告件数

［図 1 インシデント報告件数の推移］
出典　JPCERT/CC より

インシデント報告件数

インシデント報告件数↗増加傾向



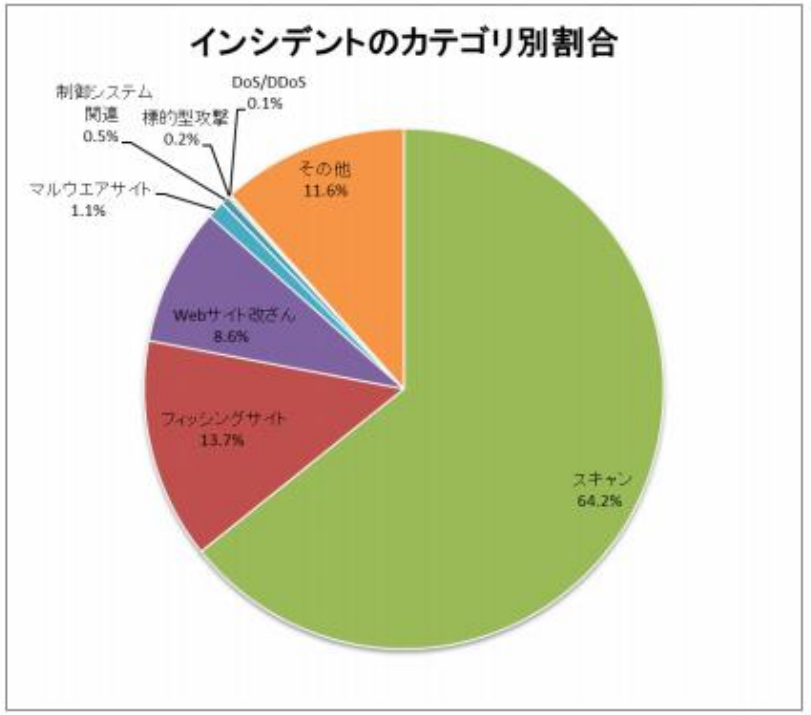
［図 1 インシデント報告件数の推移］

出典　JPCERT/CC より

報告件数の内訳

［表 2 カテゴリ別インシデント件数］

インシデント	4 月	5 月	6 月	合計	前四半期合計
フィッシングサイト	225	221	290	736	707
Web サイト改ざん	138	155	168	461	967
マルウエアサイト	24	15	20	59	91
スキャン	751	812	1884	3447	2391
DoS/DDoS	1	1	1	3	75
制御システム関連	25	2	0	27	4
標的型攻撃	6	1	2	9	11
その他	206	181	236	623	610



出典　JPCERT/CC より

「情報セキュリティ 10大脅威」:2017年版

1	標的型攻撃による情報流出
2	ランサムウェアによる被害
3	ウェブサービスからの個人情報の窃取
4	サービス妨害攻撃によるサービスの停止
5	内部不正による情報漏えいとそれに伴う業務停止
6	ウェブサイトの改ざん
7	ウェブサービスへの不正ログイン
8	IoT機器の脆弱性の顕在化
9	攻撃のビジネス化（アンダーグラウンドサービス）
10	インターネットバンキングやクレジットカード情報の不正利用

～「2017年版 10大脅威 」　https://www.ipa.go.jp/security/vuln/10threats2017.html

出典　IPA より

「情報セキュリティ 10大脅威」:2017年版

ポイント

LAC

IoT機器関連の脅威も増加

3	ウェブサービスからの個人情報の窃取
4	サービス妨害攻撃によるサービスの停止
5	内部不正による情報漏えいとそれに伴う業務停止
6	ウェブサイトの改ざん
7	ウェブサービスへの不正ログイン
8	IoT機器の脆弱性の顕在化
9	攻撃のビジネス化（アンダーグラウンドサービス）
10	インターネットバンキングやクレジットカード情報の不正利用

～「2017年版 10大脅威 」　https://www.ipa.go.jp/security/vuln/10threats2017.html

出典　IPA より

LAC観点での統計情報

統計データソース

ポイント

JAPAN SECURITY OPERATION CENTER

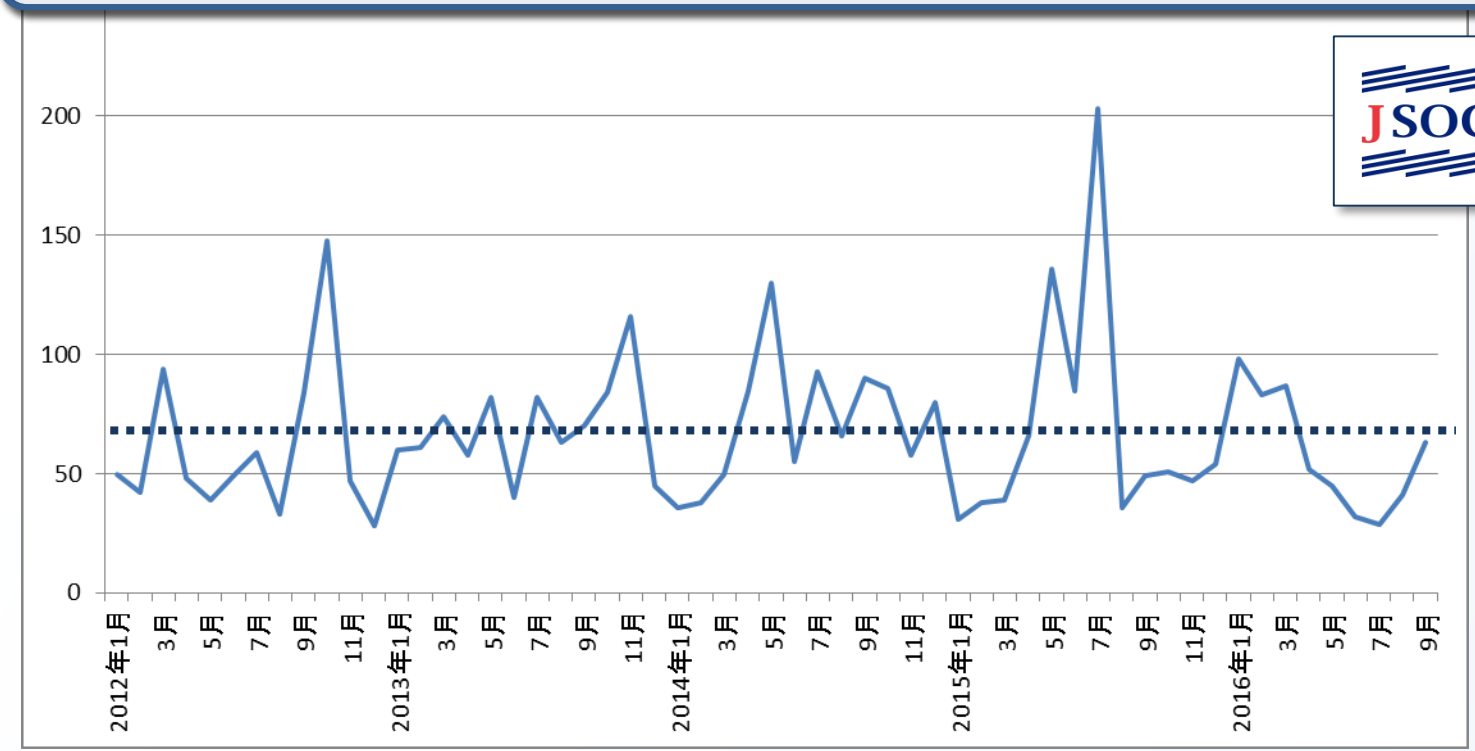
JSOC
：セキュリティ監視センター

CYBER EMERGENCY CENTER

サイバー救急センター
：セキュリティインシデント対応部隊

JSOCにおける検知傾向（2012～2016）

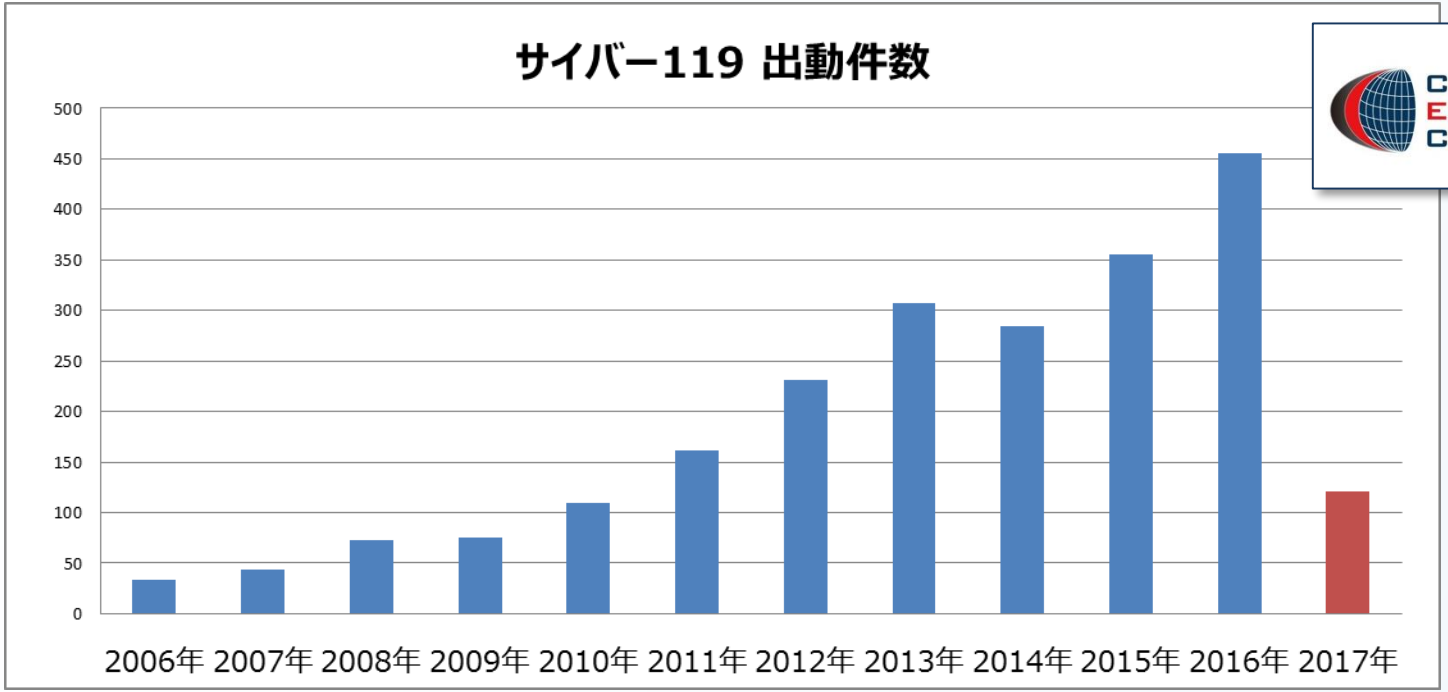
平均70件/月のコール



JAPAN SECURITY OPERATION CENTER

サイバー救急センター　出動件数

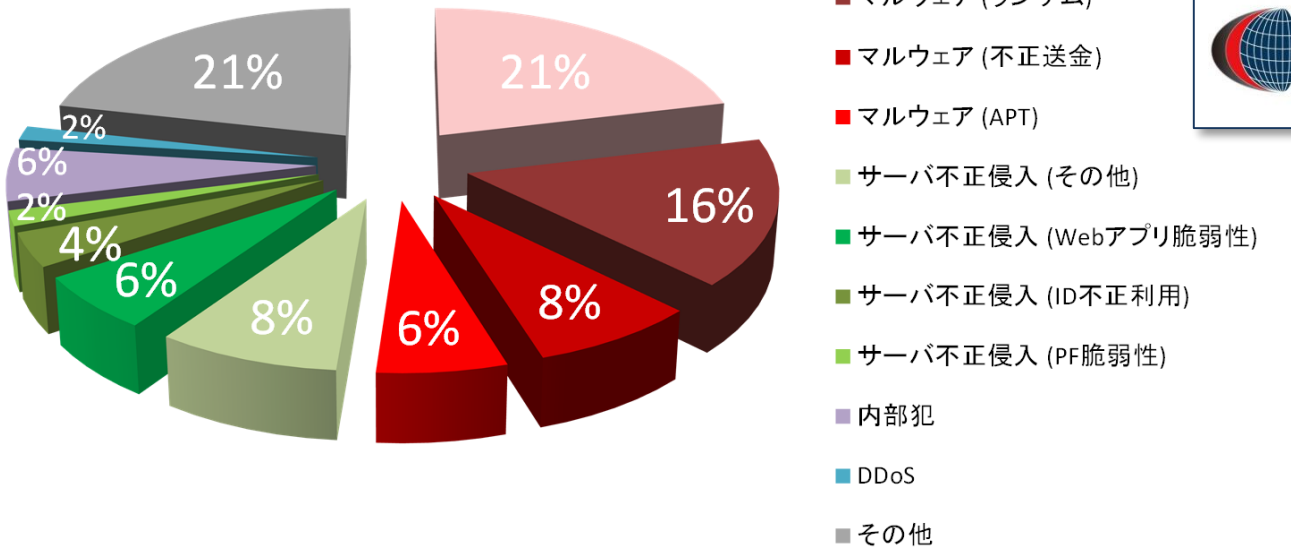
1件/日の出動要請



CYBER EMERGENCY CENTER

サイバー救急センター 出動理由の割合

マルウェア関連　50%
サーバー関連　20%



CYBER EMERGENCY CENTER

インシデントはなくならない

インシデントは“０”にはならない

インシデントはなくならない

インシデントは“０”にはならない

インシデント対応が重要

インシデントはなくならない

ポイント

インシデントは“０”にはならない

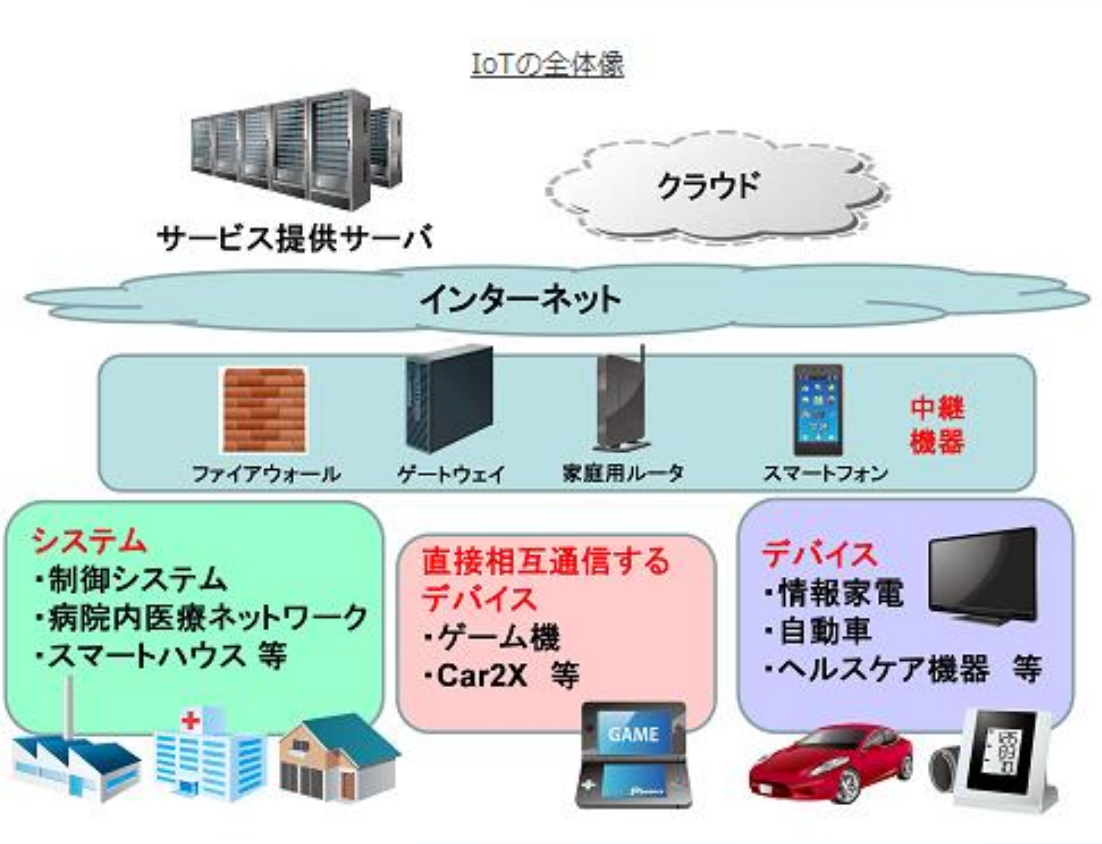
インシデント対応が重要

要CSIRT体制の整備

アジェンダ

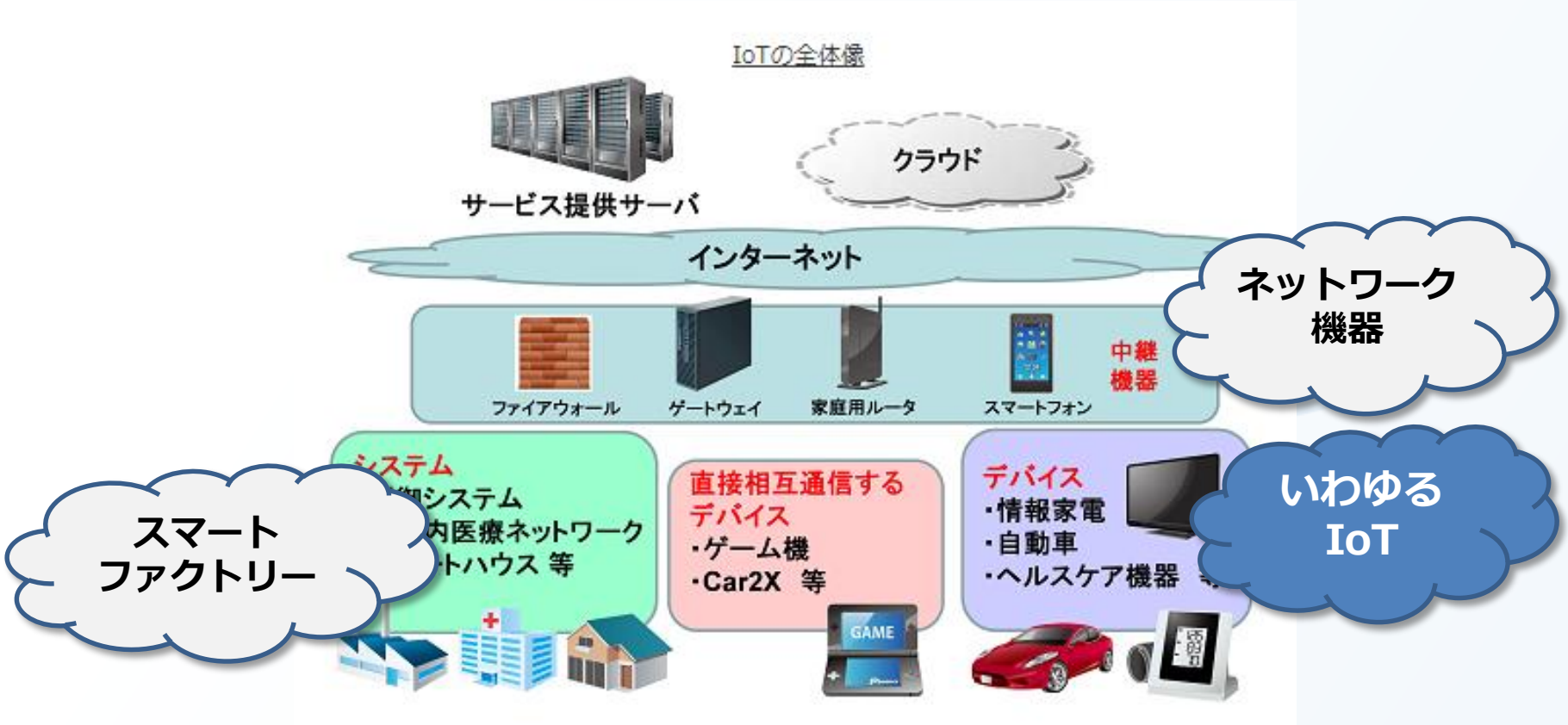
0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

はじめに



出典　IPA IoT開発におけるセキュリティ設計の手引き より

IOTセキュリティのスコープ



出典　IPA IoT開発におけるセキュリティ設計の手引き より

IOTセキュリティのスコープ

■社内　　ネットワーク、サーバ＋設備と情報システム

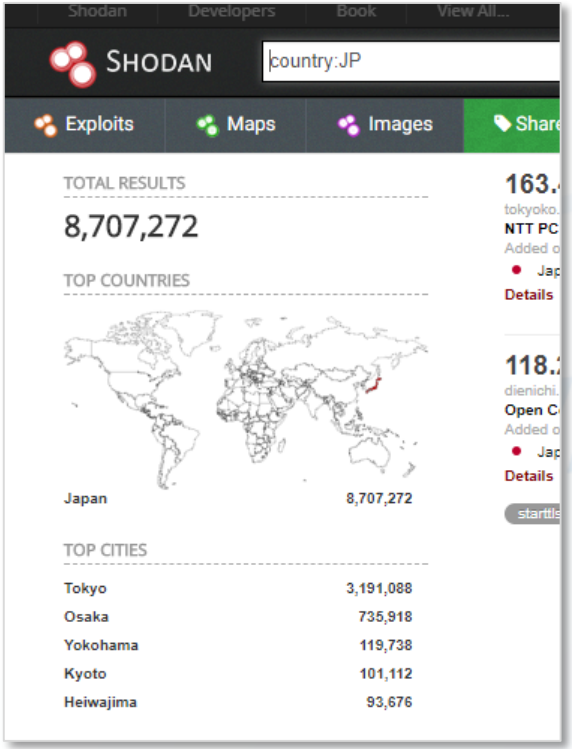
■IoT　　製品（サービス）とそれらを構成する部品

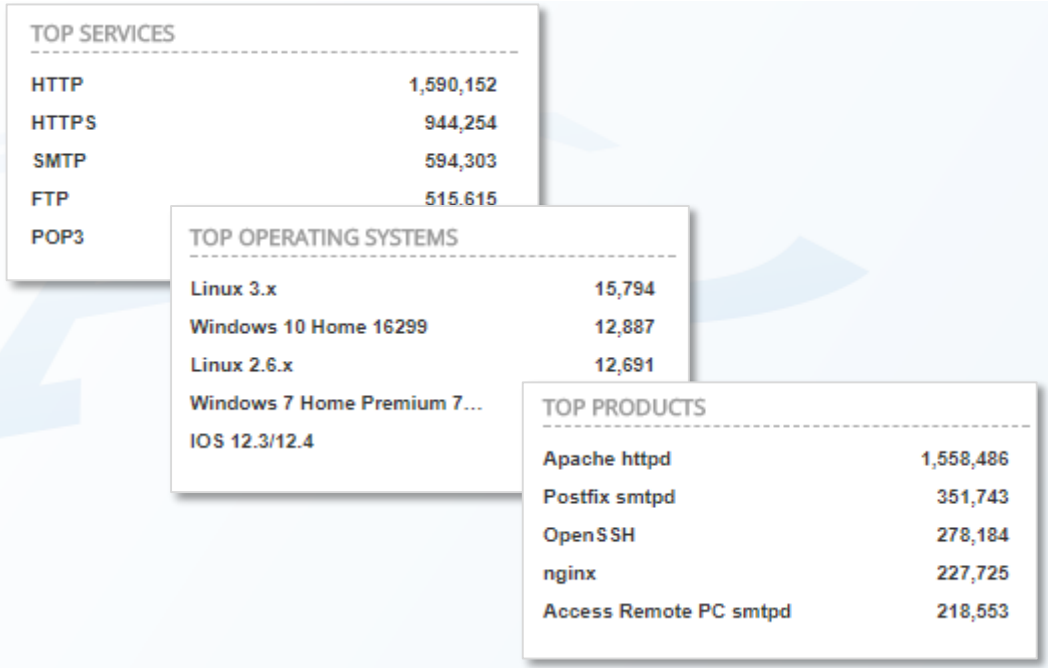
インターネットに公開されている物

ポイント

LAC

SHODANによると、
870万台のデバイス（もちろんサーバ含む）が公開





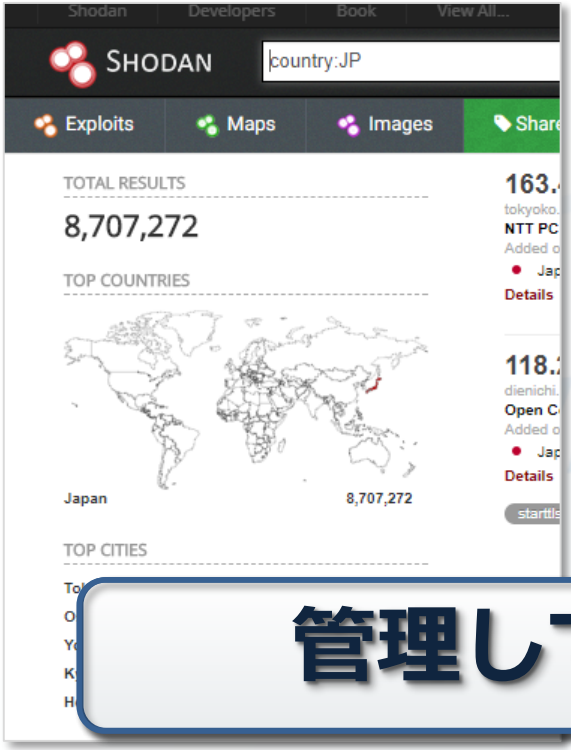
出典　SHODANより

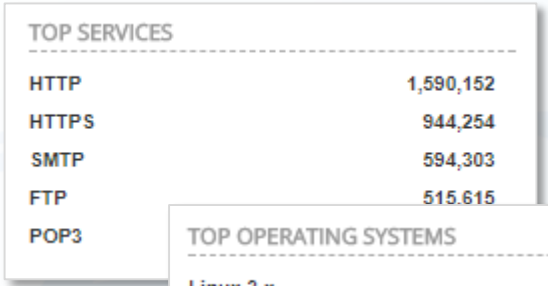
インターネットに公開されている物

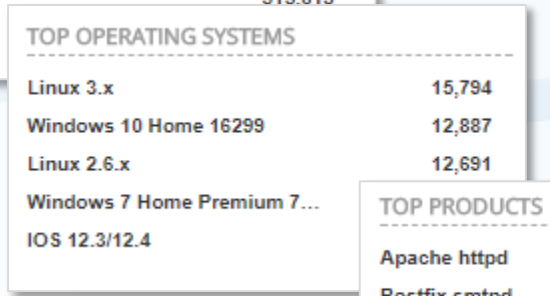
ポイント

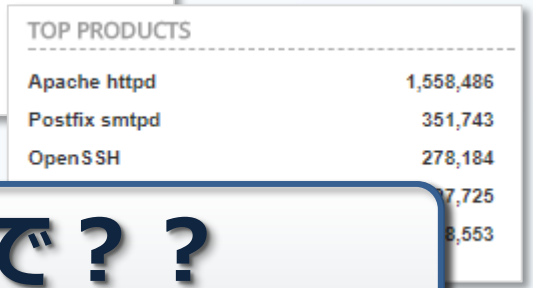
LAC

SHODANによると、
870万台のデバイス（もちろんサーバ含む）が公開









管理していないものまで？？

IOTセキュリティのスコープと優先順位

まずは、インターネットにさらされているIoTから！

出典　IPA IoT開発におけるセキュリティ設計の手引きより

アジェンダ

0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

インシデントはなくならない

インシデントは“０”にはならない

インシデント対応が重要

要CSIRT体制の整備

CSIRTとは

コンピュータシステムを驚異から防ぐためには、
そして、万が一問題が発生したら、、、

■ **予防活動**
- 各システムのチェック
- 対策や規定の見直し
- ユーザ啓発

■ **対応活動**
- 検知・通知
- 対応、原因究明

これらの活動する組織が必要

=

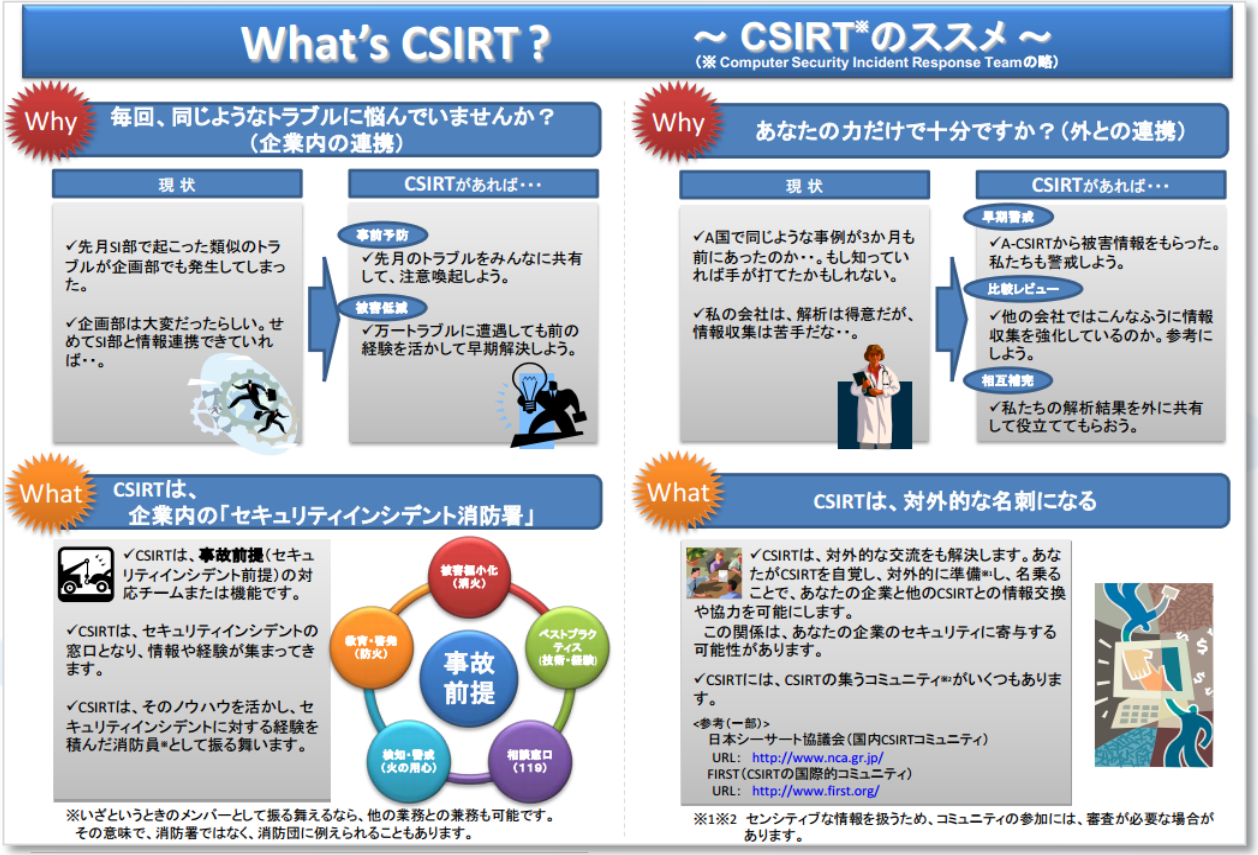
“CSIRT”

CSIRTとは

CSIRT :
Computer **S**ecurity **I**ncident **R**esponse **T**eam

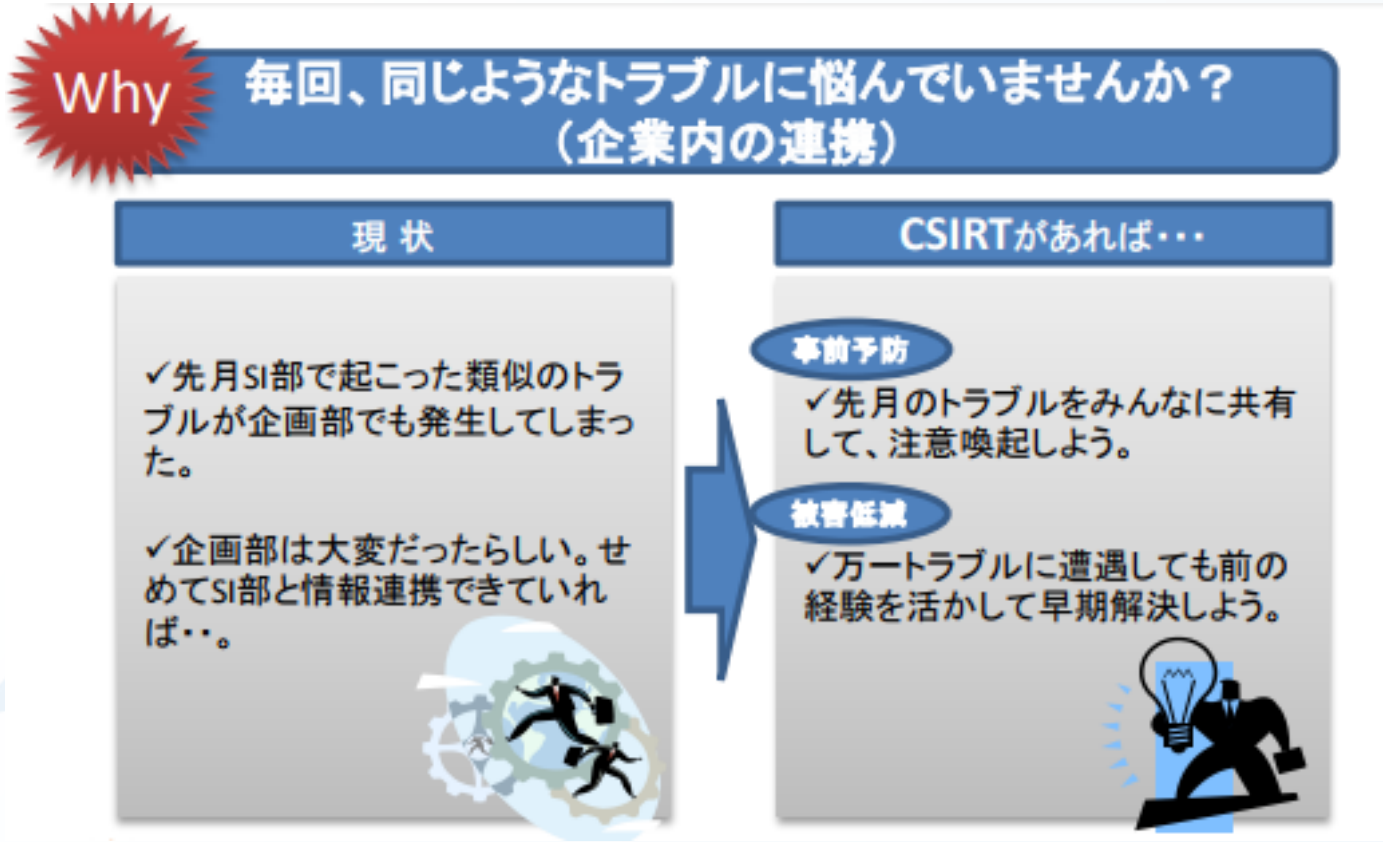
- **コンピュータセキュリティにかかわるインシデントに対処するための組織の総称**
- **インシデント関連情報、脆弱性情報、攻撃予兆情報を収集、分析し、対応方針や手順の策定などの活動**

CSIRTがあると良いこと



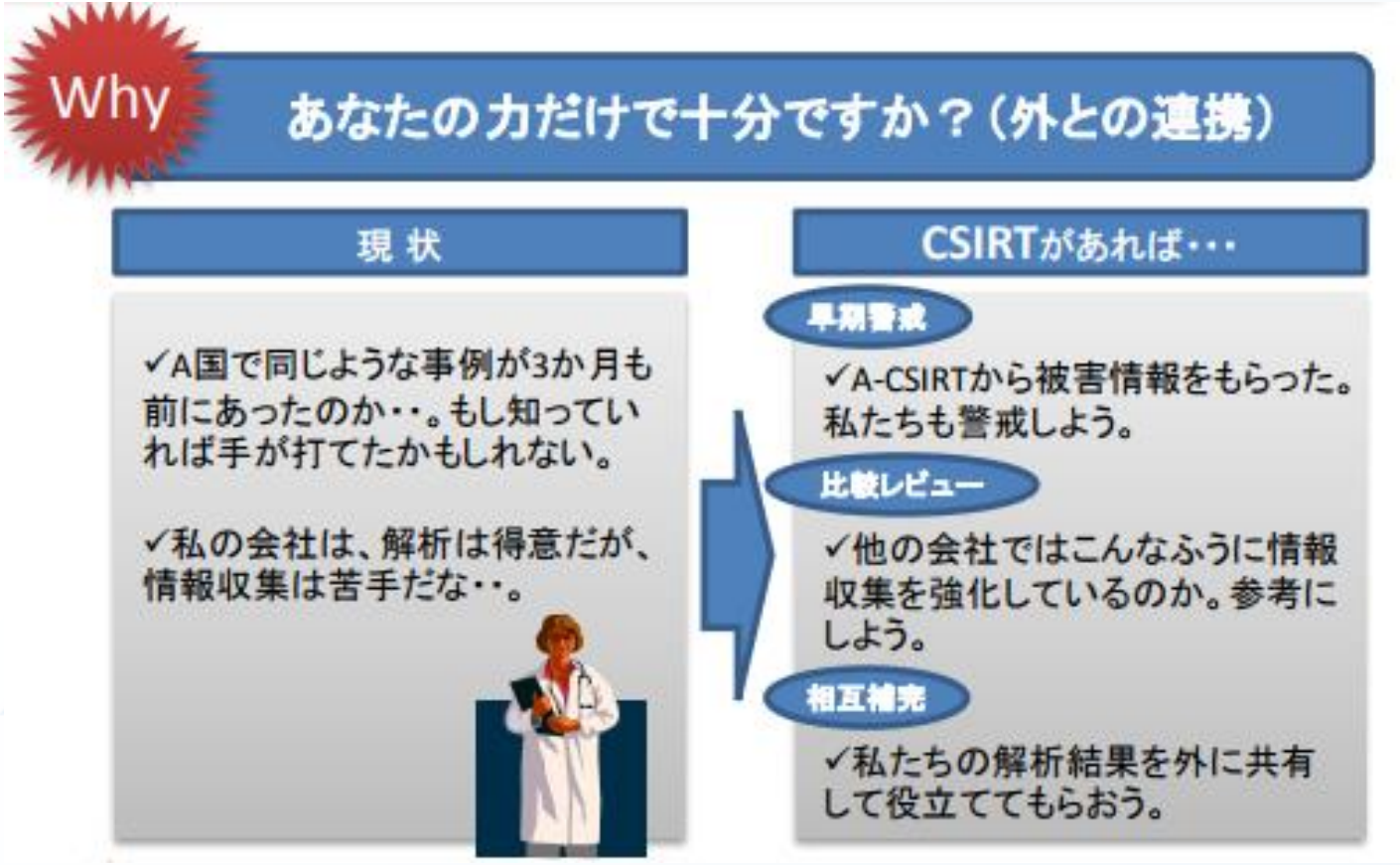
http://www.nca.gr.jp/imgs/CSIRT.pdf

CSIRTがあると良いこと



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

CSIRTがあると良いこと



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

CSIRTがあると良いこと

What

CSIRTは、
企業内の「セキュリティインシデント消防署」

✓CSIRTは、**事故前提**（セキュリティインシデント前提）の対応チームまたは機能です。

✓CSIRTは、セキュリティインシデントの窓口となり、情報や経験が集まってきます。

✓CSIRTは、そのノウハウを活かし、セキュリティインシデントに対する経験を積んだ消防員※として振る舞います。

※いざというときのメンバーとして振る舞えるなら、他の業務との兼務も可能です。
その意味で、消防署ではなく、消防団に例えられることもあります。

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

CSIRTがあると良いこと

What

CSIRTは、対外的な名刺になる

✓CSIRTは、対外的な交流をも解決します。あなたがCSIRTを自覚し、対外的に準備※1し、名乗ることで、あなたの企業と他のCSIRTとの情報交換や協力を可能にします。
この関係は、あなたの企業のセキュリティに寄与する可能性があります。

✓CSIRTには、CSIRTの集うコミュニティ※2がいくつもあります。

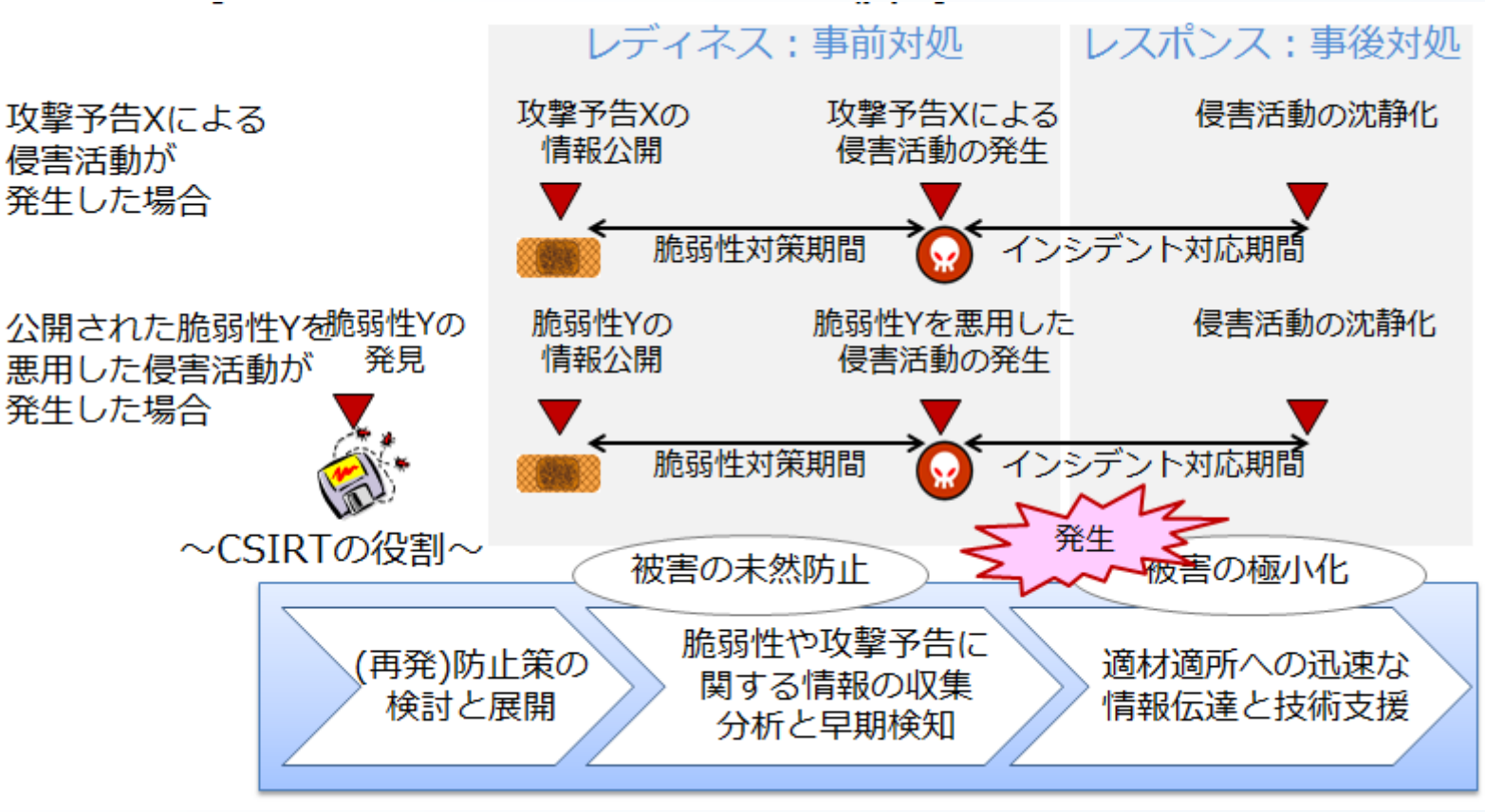
<参考(一部)>
日本シーサート協議会(国内CSIRTコミュニティ)
URL: http://www.nca.gr.jp/
FIRST(CSIRTの国際的コミュニティ)
URL: http://www.first.org/

※1※2 センシティブな情報を扱うため、コミュニティの参加には、審査が必要な場合があります。

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

CSIRTとは

■ 一般的に認識されているCSIRTの役割



CSIRTとは

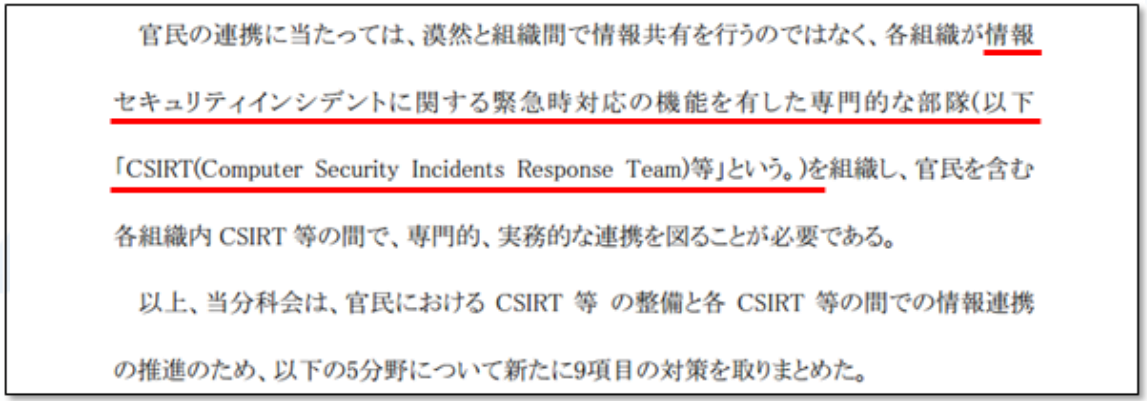
■ 役割を実現するために必要となるCSIRT活動

CSIRTとは

CSIRTに規格はなく、CSIRT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のチームがそれぞれの組織において独自の活動している。

⇒ 1つとして同じCSIRTは存在しない（※パターンはある）

・・・組織のセキュリティ文化が反映されている。



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CSIRTの説明

CSIRTとは

■ CSIRTの歴史

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。

CSIRTとは

■ CSIRTの歴史

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/

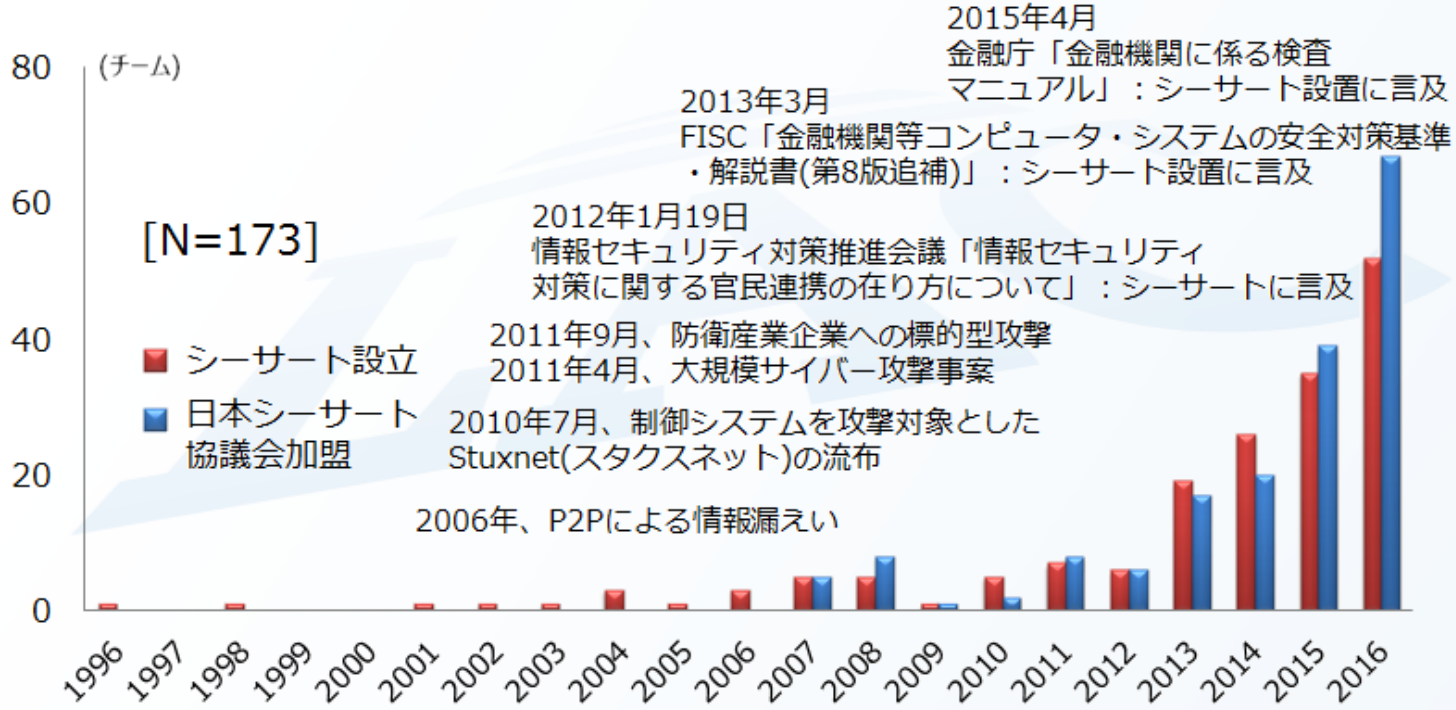
米国におけるセキュリティ事案情報、脆弱性情報の収集ならびに調整機関

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、2013年9月現在、61カ国282チームが加盟

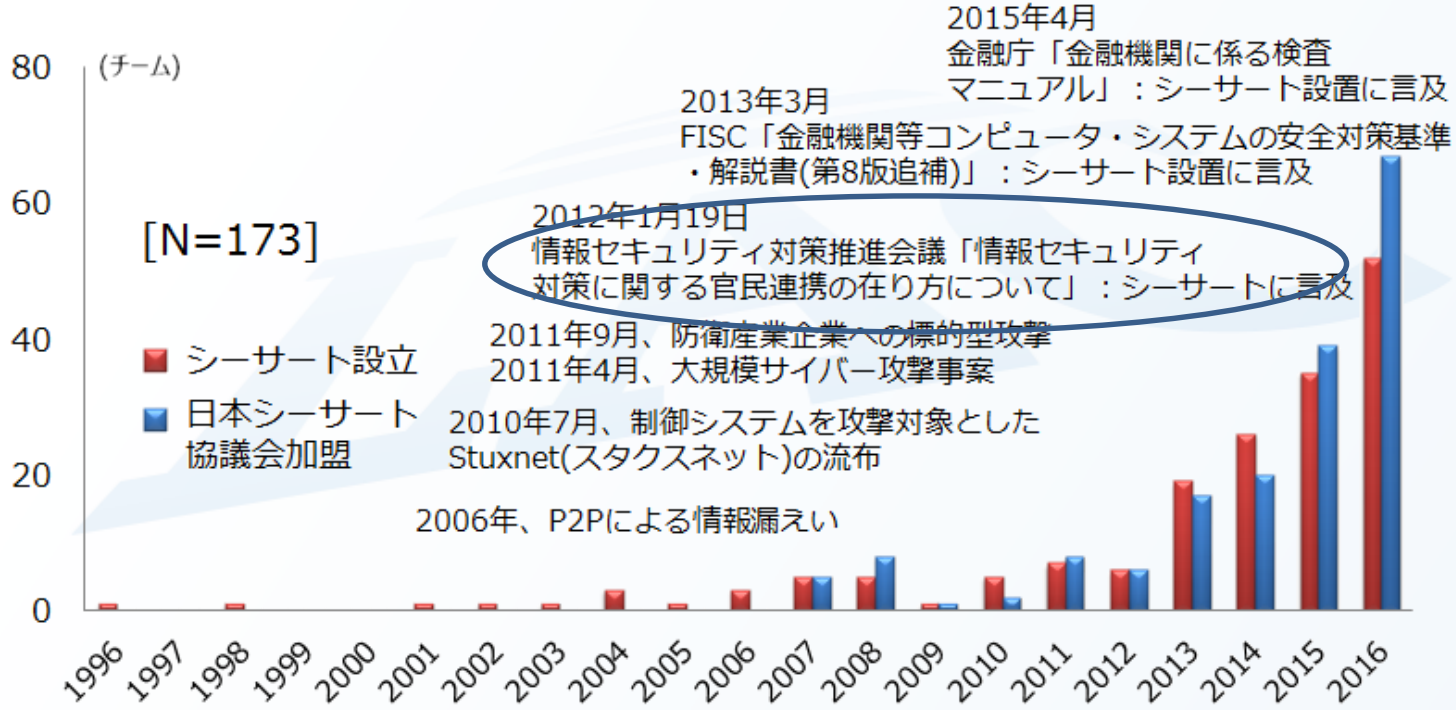
CSIRTとは

- CSIRT設立年と日本シーサート協議会（NCA）加盟年の推移
  - 2012年以前：旧来型CSIRTの加盟
  - 2013年以降：新設型CSIRTの加盟



CSIRTとは

- CSIRT設立年と日本シーサート協議会（NCA）加盟年の推移
  - 2012年以前：旧来型CSIRTの加盟
  - 2013年以降：新設型CSIRTの加盟



CSIRTとは

■ 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。

CSIRTとは

■ 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
シデントに
義する。

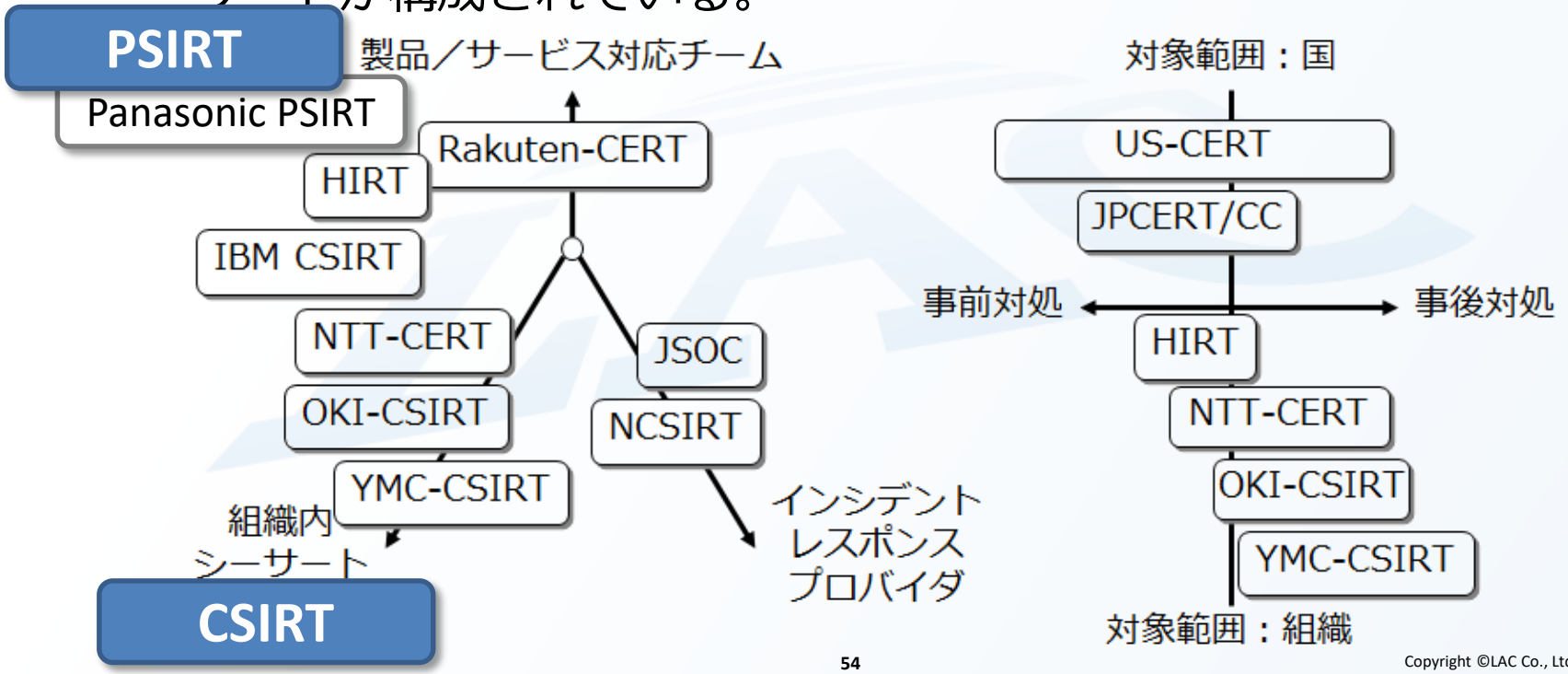
製品／サービス対応シーサート
提供する製品や
トに対応するシ

CSIRT

PSIRT

CSIRTとは

- 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。



CSIRTとは

①対外的な連絡窓口

組織の対外的な窓口になっている必要がある。

対外的な連絡窓口が明らかになっていることのメリット

- [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。

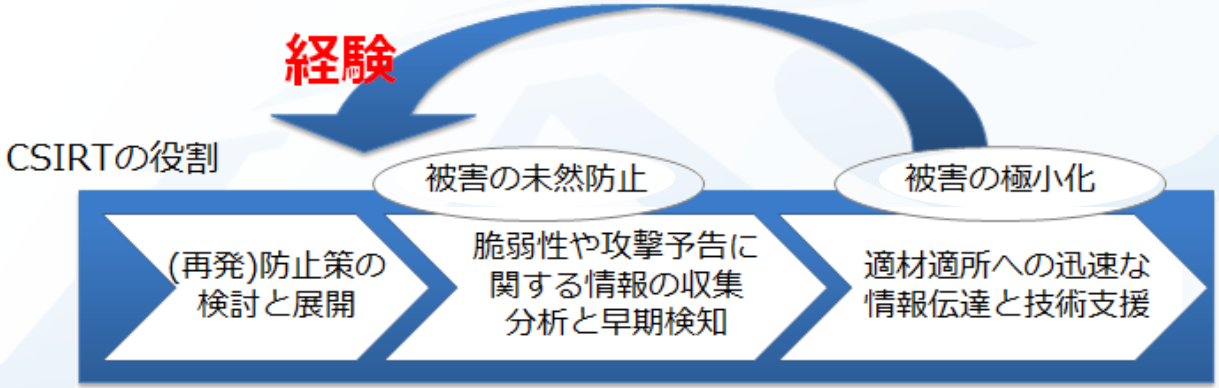
②技術的な問い合わせに対応

対外的な連絡や通知は技術的な内容が含まれ、組織としての対処を期待されている。

- 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メリット
  - 迅速なインシデント対応が可能となる。
  - [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

③事前対処（インシデントレディネス）

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)を進めることが重要



・インシデントレスポンスの経験は「問題解決」に向けて有益。
・他のインシデントレスポンスを知ることで「問題解決」を疑似体験し、被害を未然に防止・極小化する。

CSIRTと消防団

実際の消防団活動から、、

「消防団」
①月1回の定例演習
②月1回の機械器具点検
③年4回の合同訓練
④緊急出動指令
⑤地域防災訓練
⑥操法大会

「CSIRT」
アセスメントe-ラーニング、演習
定期アセスメント
NCA総会・WG
インシデントの連絡
部門との連携訓練
セキュリティコンテスト

ポイント

LAC

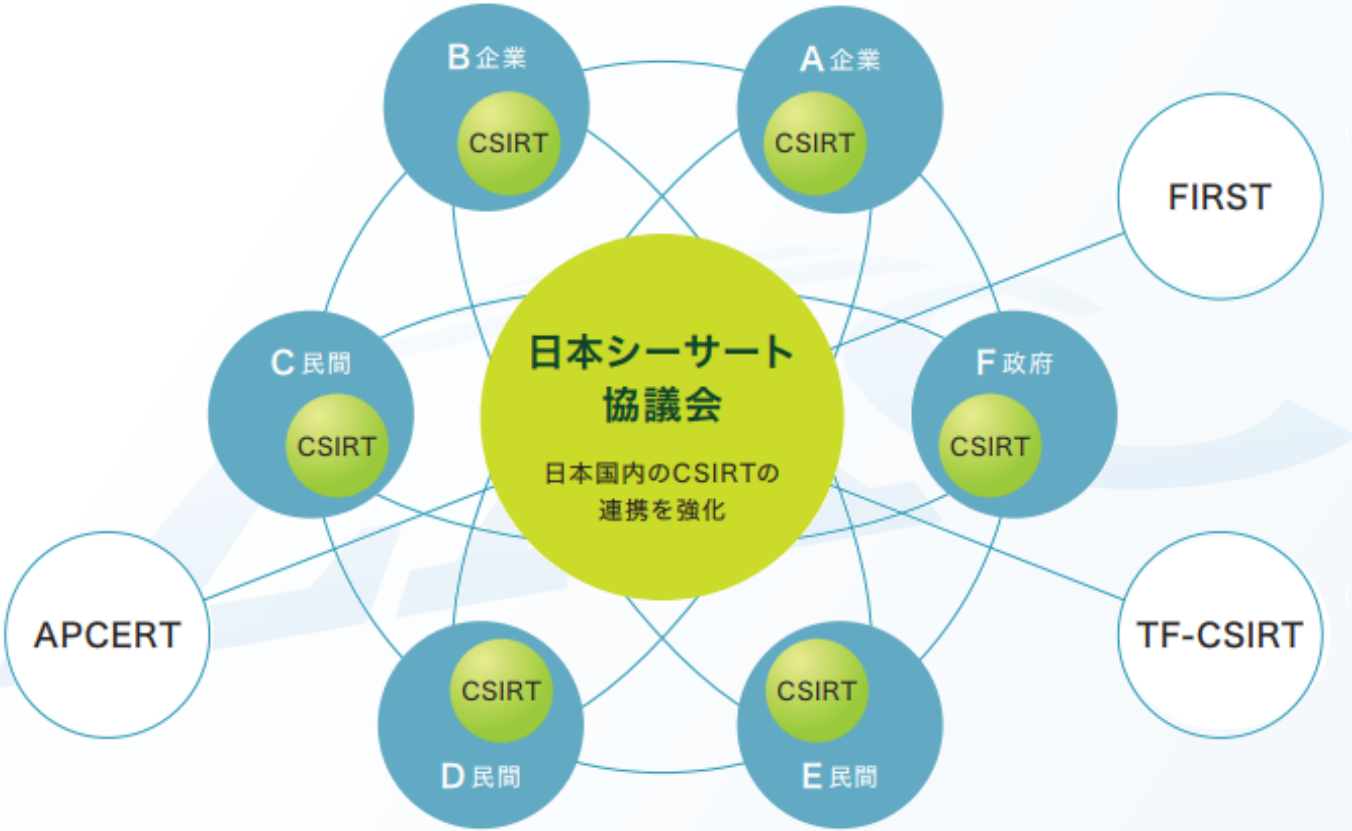
日本シーサート協議会（NCA）とは？

- **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

CSIRT
日本シーサート協議会

出典　日本シーサート協議会 より

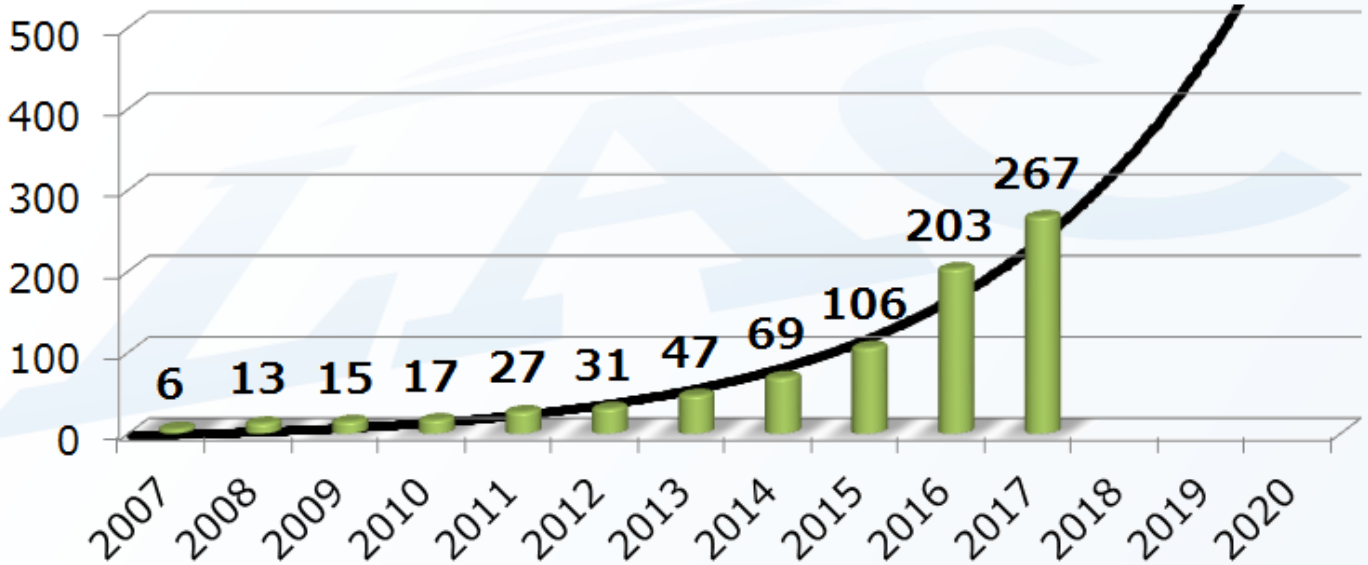
日本のCSIRTコミュニティ



出典　日本シーサート協議会 より

日本のCSIRTコミュニティ

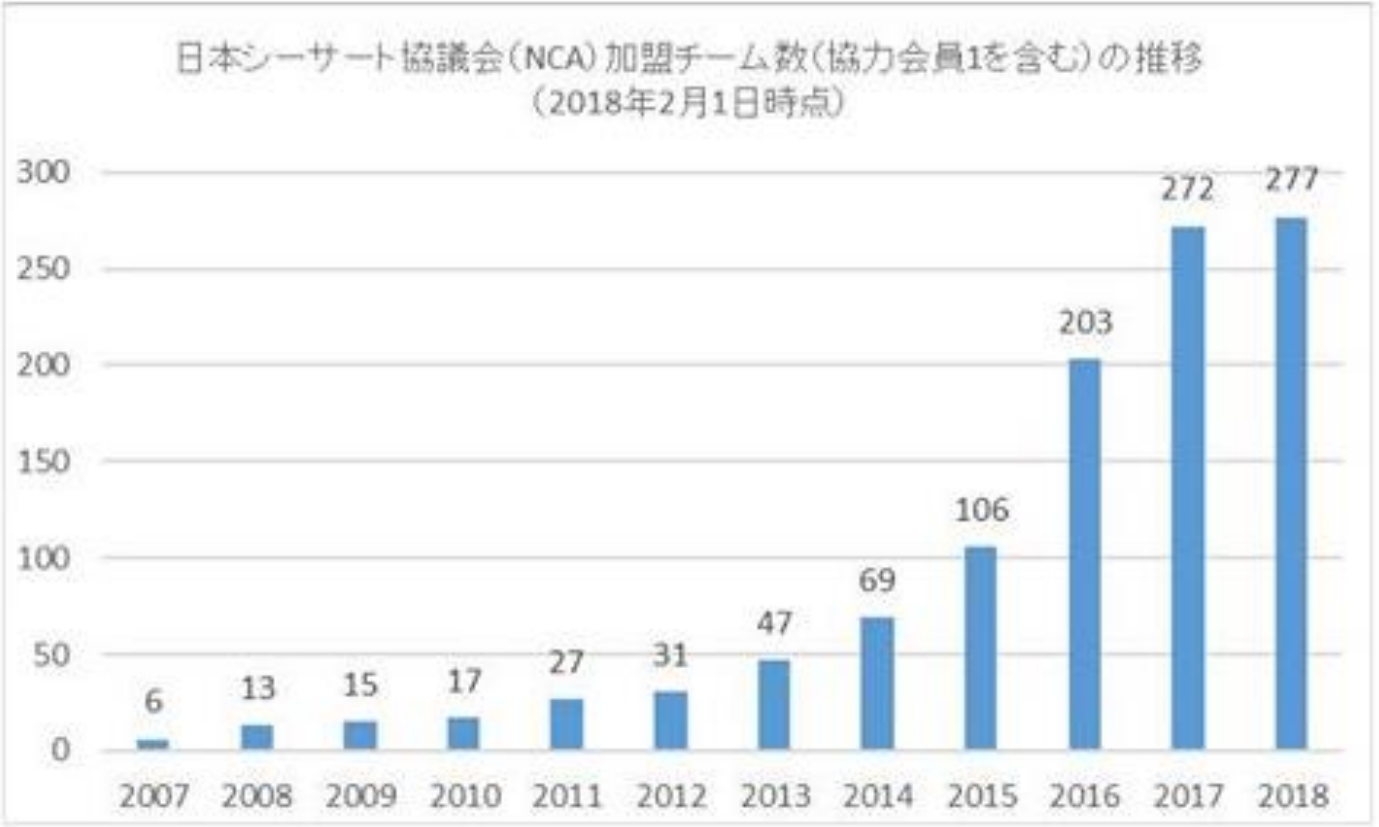
- **加盟数(累積)の推移**
  - 267チーム(2017年12月1日現在)
  - 2020年には、500チームに到達する勢い



出典　日本シーサート協議会 より

日本のCSIRTコミュニティ

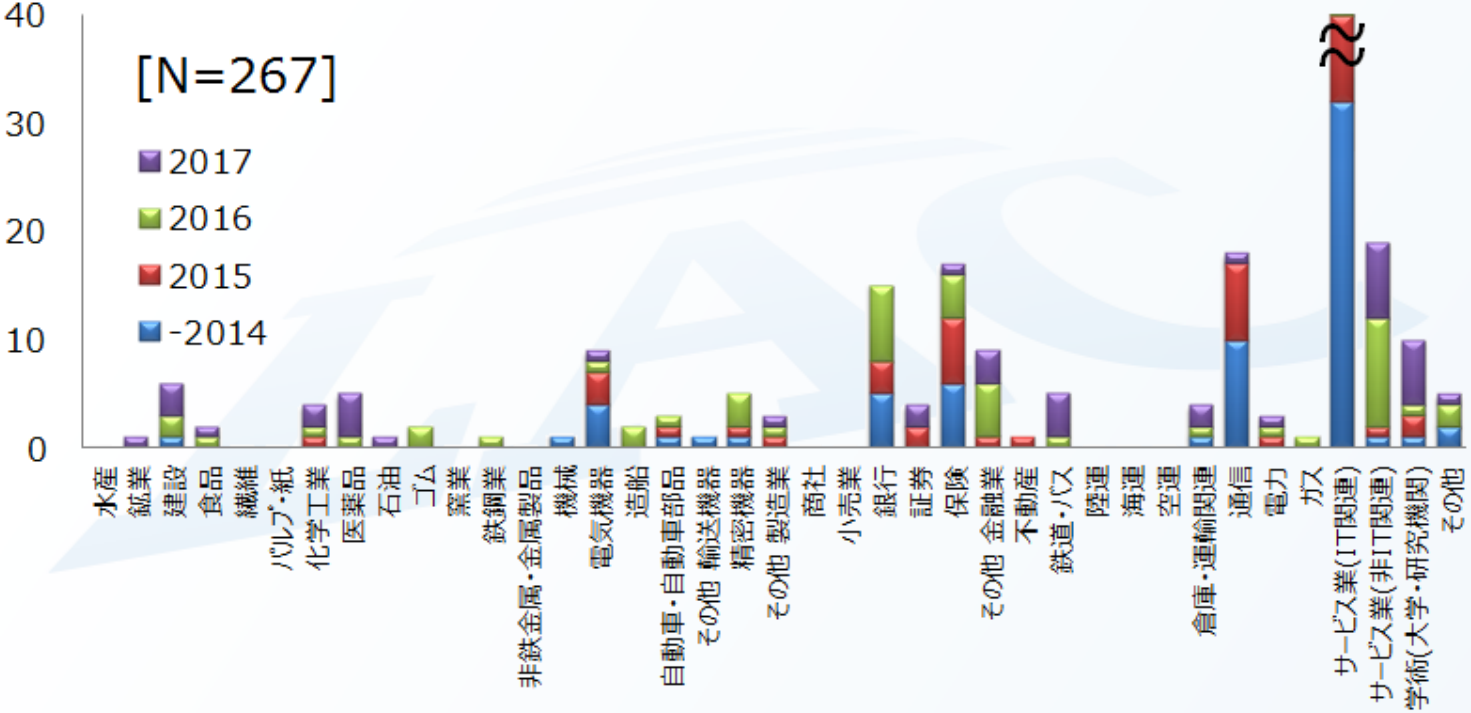
速報



出典　日本シーサート協議会 より

NCA加盟組織の分類

- **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。



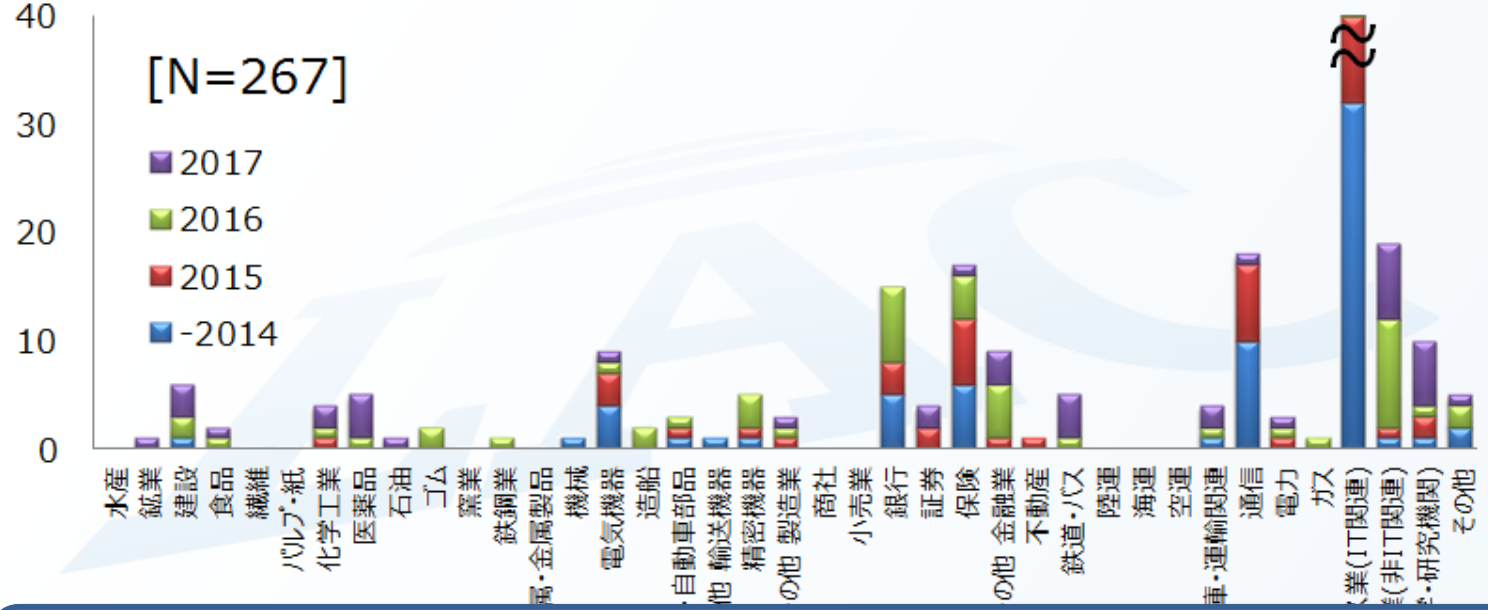
出典　日本シーサート協議会 より

NCA加盟組織の分類

ポイント

LAC

- 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。



既に多くの組織にCSIRTが

出典：日本シーサート協議会より

NCA加盟年の推移

- 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。

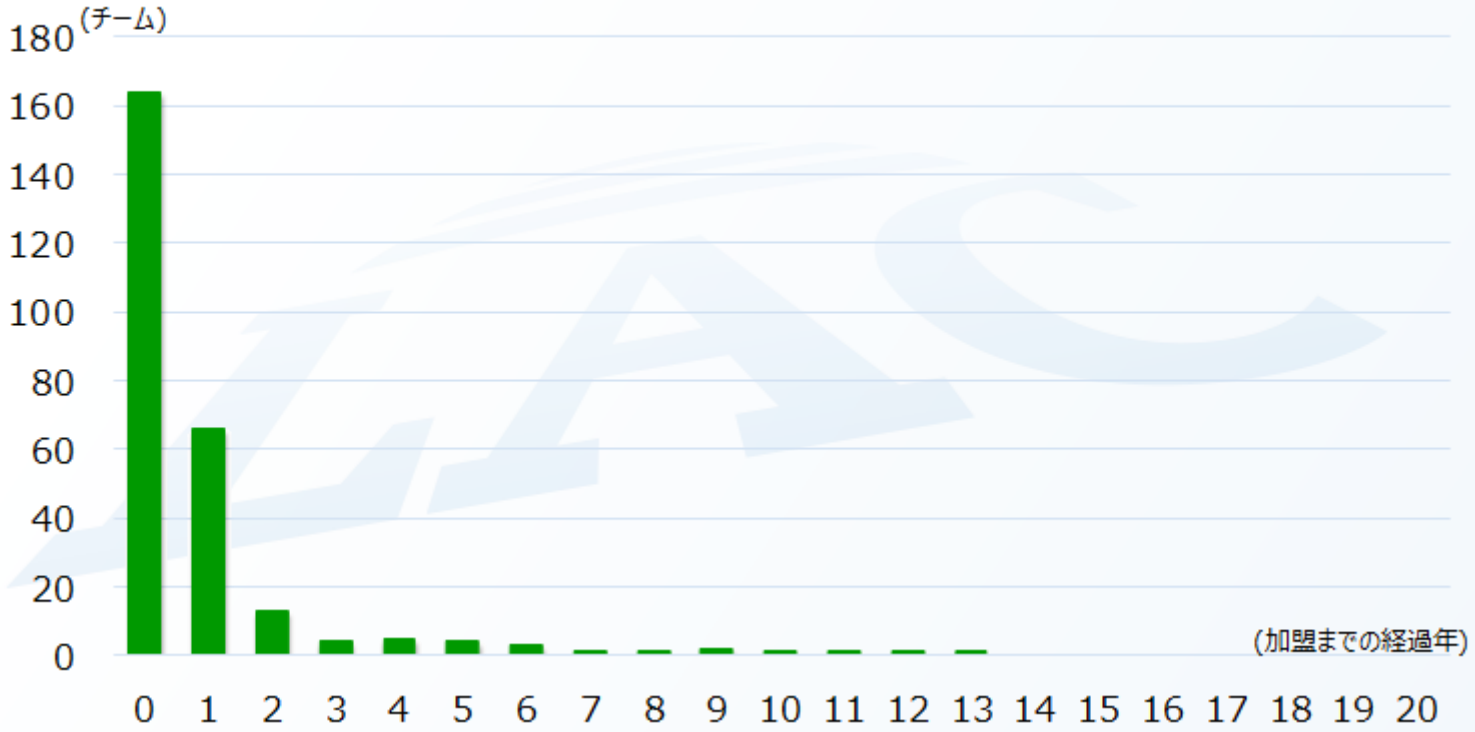
出典　日本シーサート協議会 より

各CSIRTとの連携

ポイント

LAC

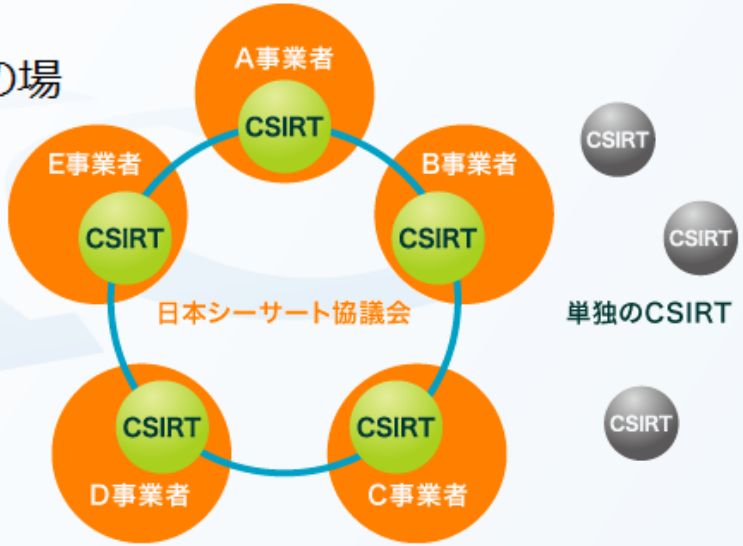
- 設立してから、どのくらいしてから加盟しているだろうか？



出典　日本シーサート協議会 より

NCAの活動

- **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**
- **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



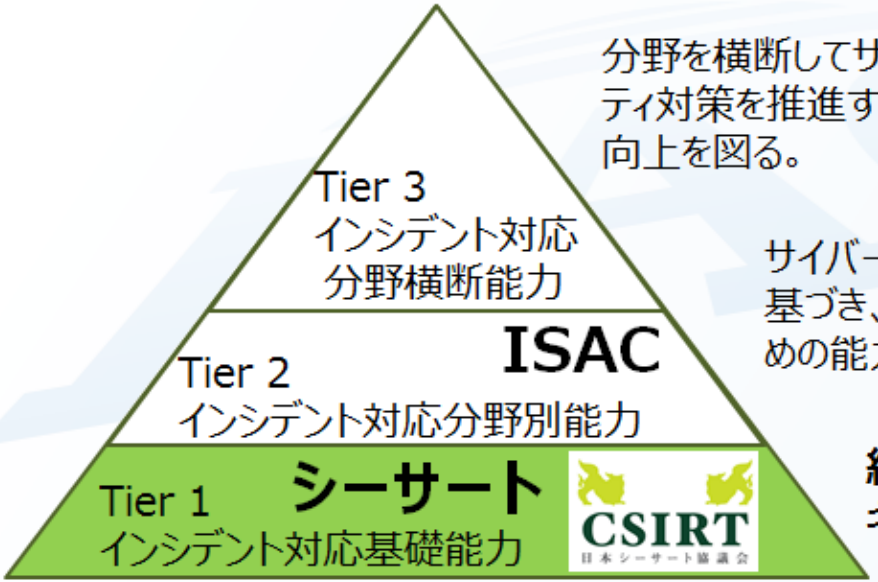
出典　日本シーサート協議会 より

NCAの位置づけ

ポイント

LAC

- **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 x (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

出典　日本シーサート協議会 より

NCA窓口

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/

出典　日本シーサート協議会 より

アジェンダ

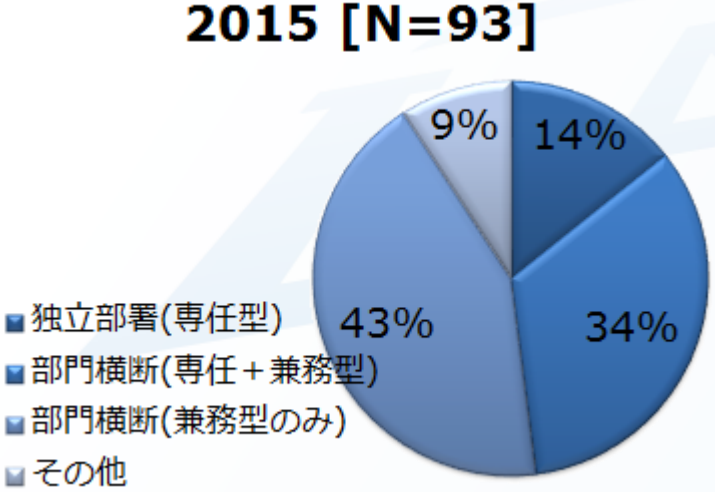
0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

CSIRTの現状と課題

組織内CSIRT実装の多くは、専任の要員が居る部門を核とした部門横断型になっている

部門間を横断した組織体制の構築

⇒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推進

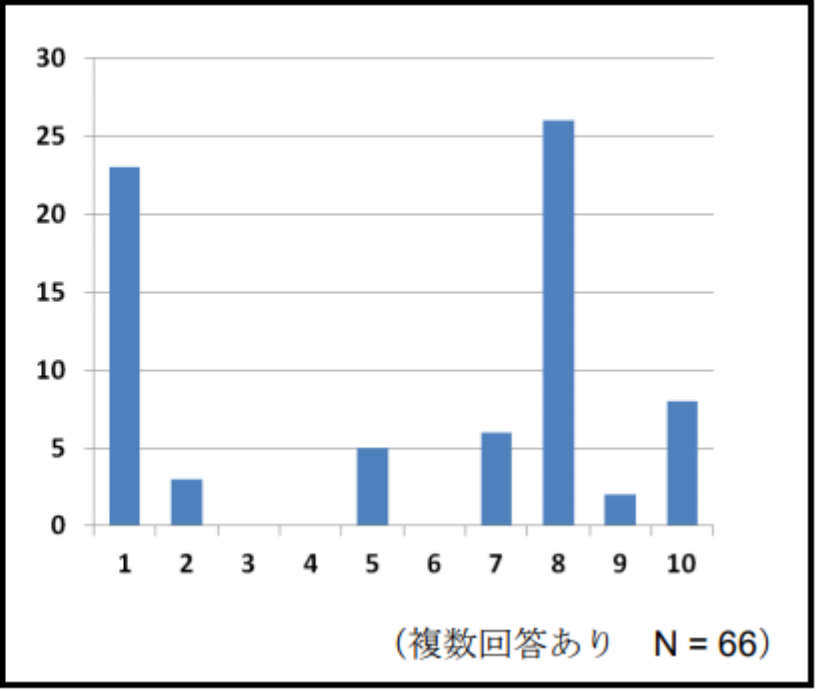
特定の部門だけが頑張れば良い(お任せ)モデルではなく、組織全体で頑張る(連帯)モデルが採用されている。

CSIRTは万能薬ではない。
組織のセキュリティ文化そのもの。

CSIRT構築を主導した部署

2.1.1. 構築を主導した部署

#	部署名	回答数
1	情報システム管理部門系	23
2	経営企画部門系	3
3	法務部門系	0
4	監査部門系	0
5	開発部門系	5
6	総務部門系	0
7	リスク対策部門系	6
8	セキュリティ対策部門系	26
9	品質保証部門系	2
10	その他自由記述	8

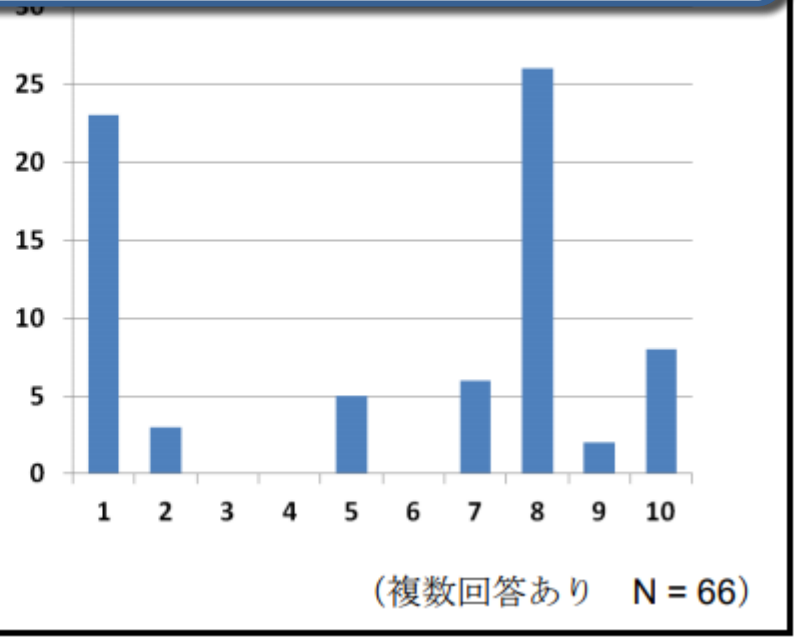


出典　JPCERT/CCより

CSIRT構築を主導した部署

情報システム→セキュリティ専門へ

1	情報システム管理部門系	23
2	経営企画部門系	3
3	法務部門系	0
4	監査部門系	0
5	開発部門系	5
6	総務部門系	0
7	リスク対策部門系	6
8	セキュリティ対策部門系	26
9	品質保証部門系	2
10	その他自由記述	8

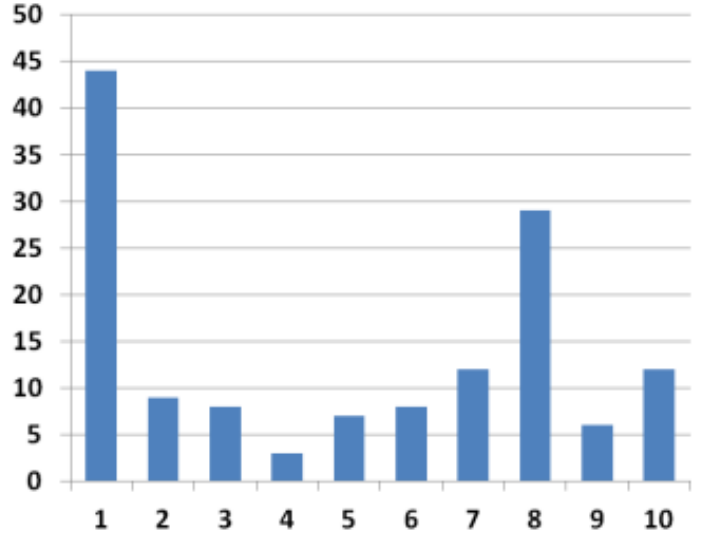


出典　JPCERT/CCより

CSIRT構築に携わった部署

2.1.2. 構築に関わった部署

#	部署名	回答数
1	情報システム管理部門系	44
2	経営企画部門系	9
3	法務部門系	8
4	監査部門系	3
5	開発部門系	7
6	総務部門系	8
7	リスク対策部門系	12
8	セキュリティ対策部門系	29
9	品質保証部門系	6
10	その他自由記述	12

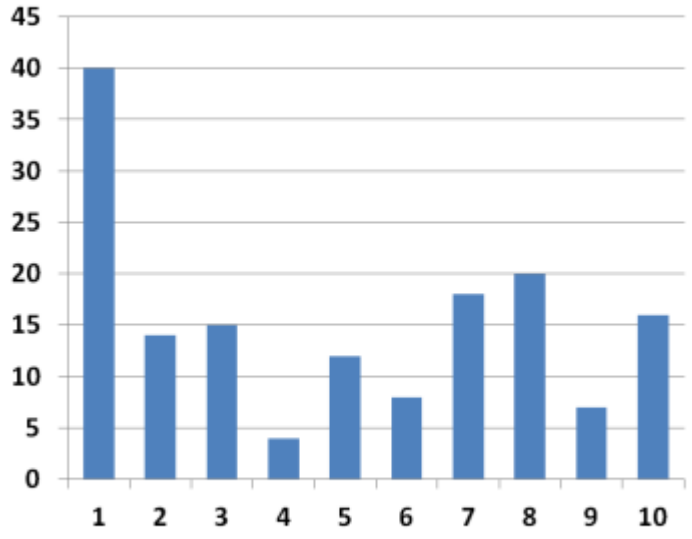


出典　JPCERT/CCより

CSIRT構築に調整が必要だった部署

2.1.3. 構築時に調整が必要だった部署

#	部署名	回答数
1	情報システム管理部門系	40
2	経営企画部門系	14
3	法務部門系	15
4	監査部門系	4
5	開発部門系	12
6	総務部門系	8
7	リスク対策部門系	18
8	セキュリティ対策部門系	20
9	品質保証部門系	7
10	その他自由記述	16

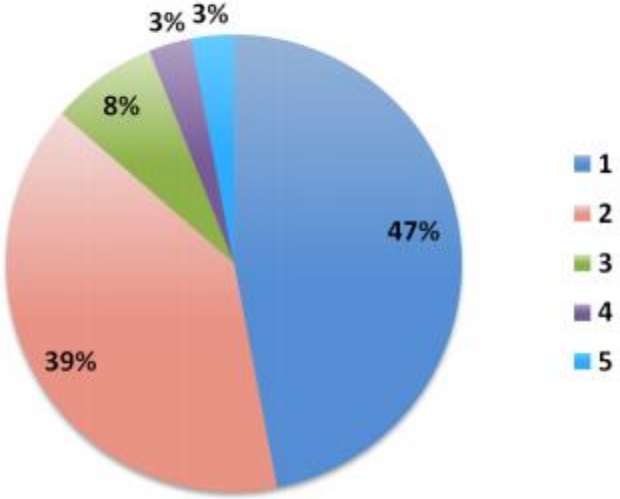


出典　JPCERT/CCより

CSIRT構築に携わった人数

2.1.4. 構築に携わった人数（外注含む）

#	人数	回答数
1	5 名未満	31
2	5 名以上 10 名未満	26
3	10 名以上 20 名未満	5
4	20 名以上	2
5	未回答	2

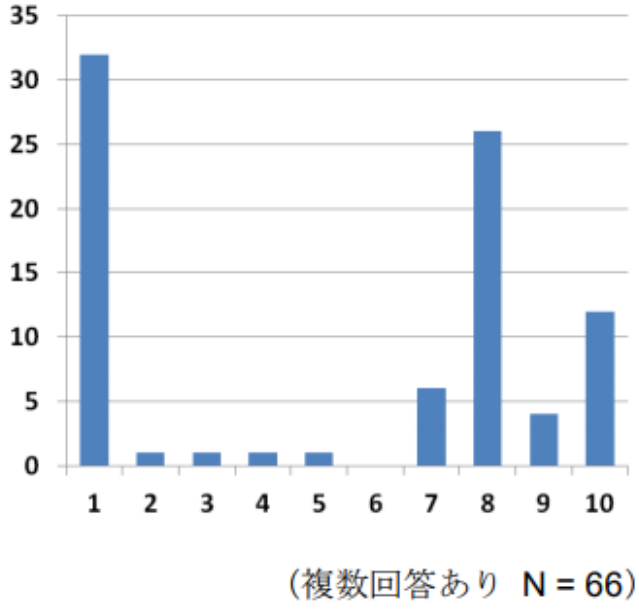


（複数回答なし N = 66）

CSIRTの体制　どの部門に配置されているか？

2.2.1. 組織内のどの部署に配置されているか

#	部署	回答数
1	情報システム管理部門系	32
2	経営企画部門系	1
3	法務部門系	1
4	監査部門系	1
5	開発部門系	1
6	総務部門系	0
7	リスク対策部門系	6
8	セキュリティ対策部門系	26
9	品質保証部門系	4
10	その他自由記述	12

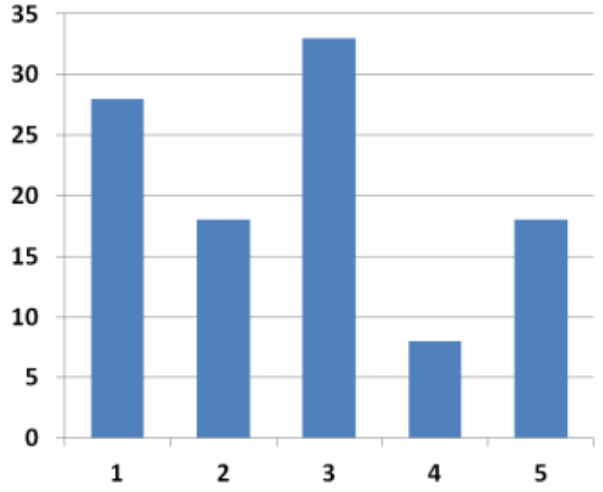


出典　JPCERT/CCより

外部からの問い合わせ状況

2.2.4. 過去に外部から CSIRT に対して連絡、問い合わせはあったか

#	連絡、問い合わせ内容	回答数
1	Web サービスの脆弱性に関するもの	28
2	製品の脆弱性に関するもの	18
3	インシデントに関するもの	33
4	その他自由記述	8
5	問い合わせはなかった	18



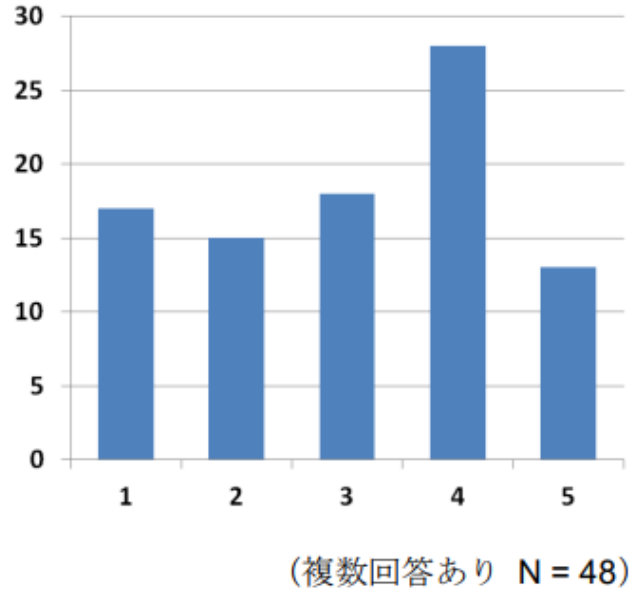
（複数回答あり N = 66）

出典　JPCERT/CCより

外部からの問い合わせ状況

2.2.4.1. CSIRT への連絡、問い合わせはどこからあったか

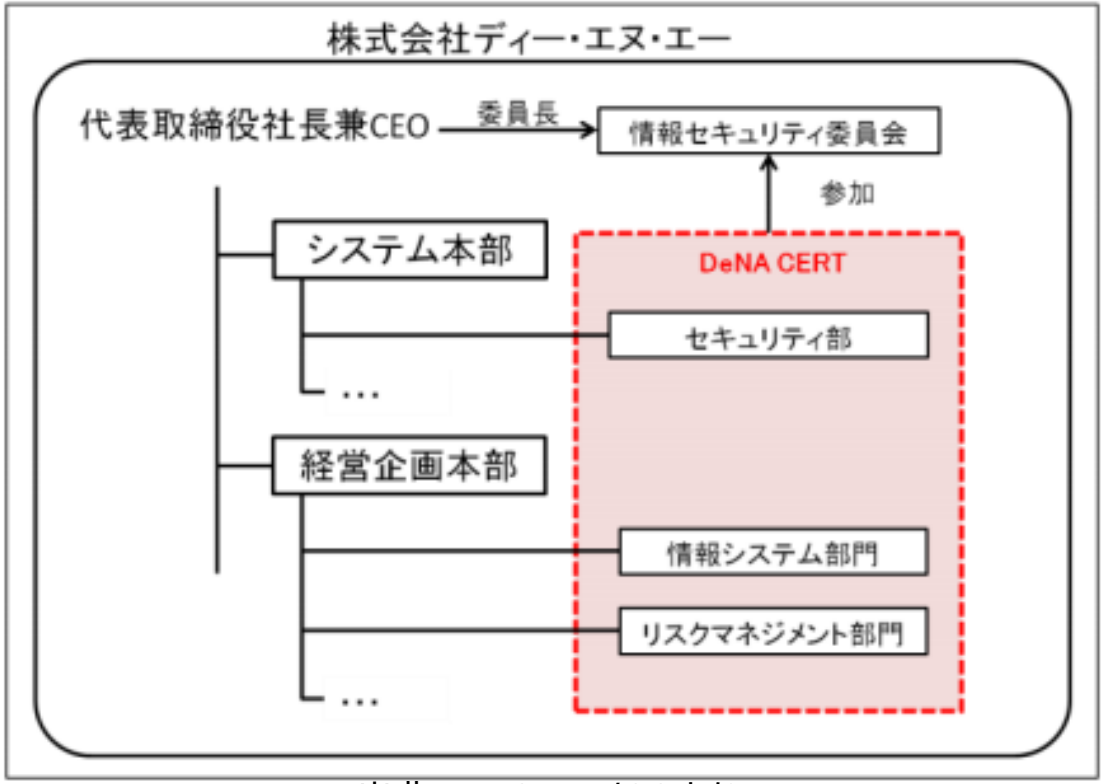
#	組織名	回答数
1	セキュリティベンダ	17
2	IPA	15
3	一般ユーザ	18
4	JPCERT/CC	28
5	その他自由記述	13



出典　JPCERT/CCより

5．CSIRT事例

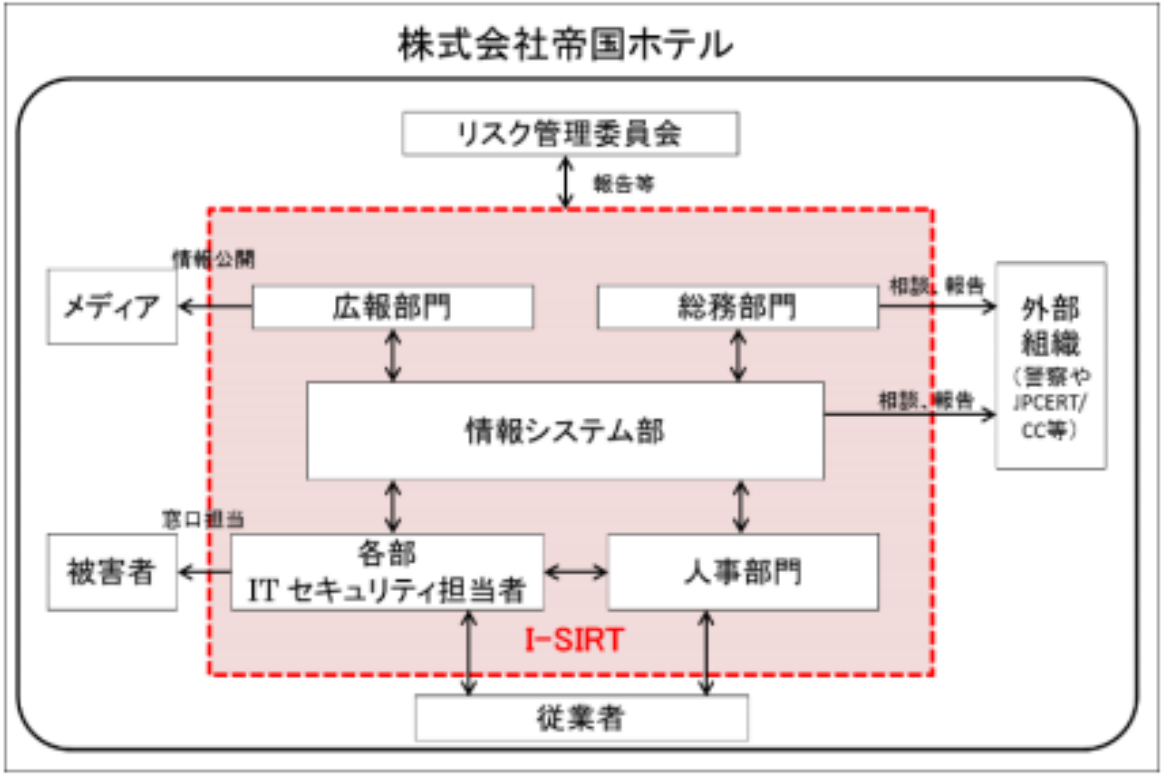
DeNA CERT・・・セキュリティ関連仮想組織



出典　JPCERT/CCより

5．CSIRT事例

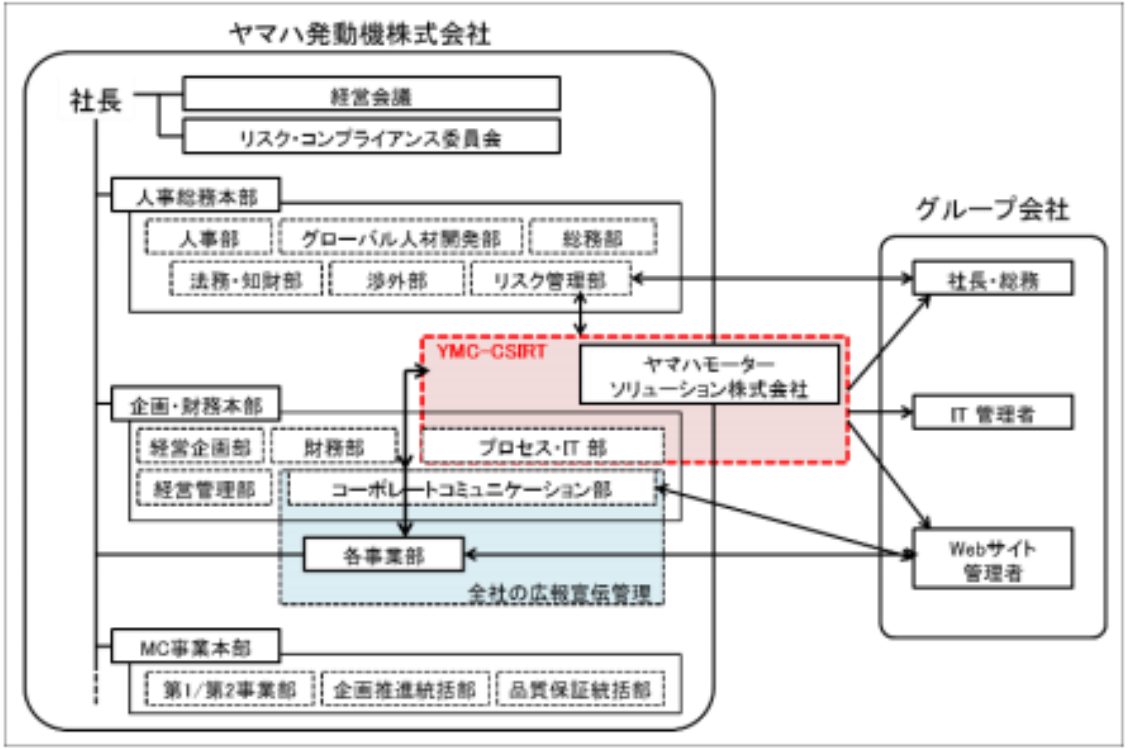
I-SIRT・・・部門横断仮想組織



出典　JPCERT/CCより

5．CSIRT事例

YMC-CSIRT・・・情報システム部門

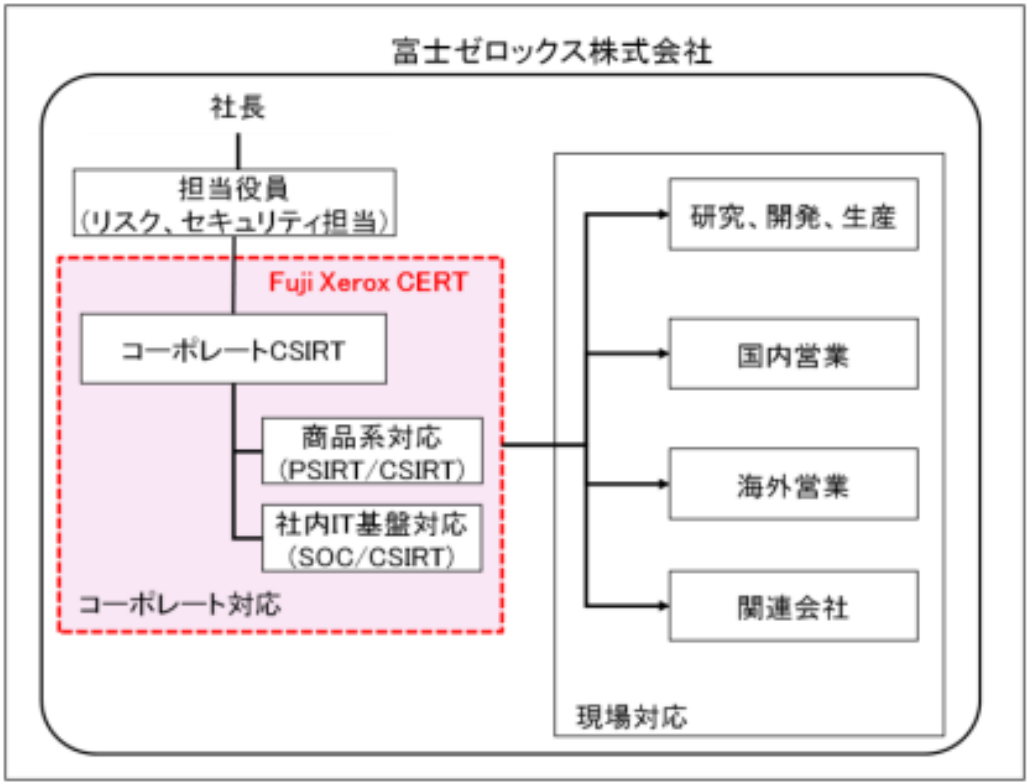


出典　JPCERT/CCより

5．CSIRT事例

ポイント

Fuji Xerox CERT・・・PSIRT/CSIRT統合型

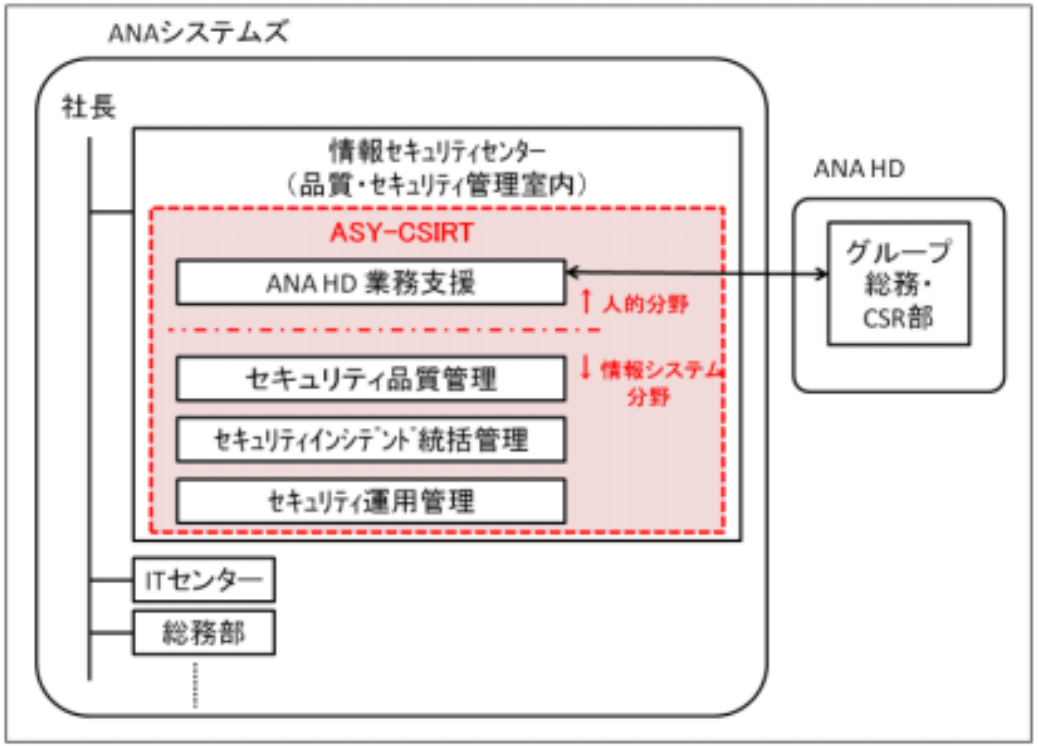


出典　JPCERT/CCより

5．CSIRT事例

ポイント

ASY-CSIRT・・・社長直下 PSIRT/CSIRT統合型



出典　JPCERT/CCより

5．CSIRT事例

ASY-CSIRT・・・スキルマップが整備されている

担当業務	着任対象者	着任後に習得すべき知識やスキル
適合確認系	システム開発経験者	・セキュリティやマネジメントに関する知識 ・ポリシーやガイドラインの作成 ・適合確認業務　等
SOC、CSIRT、IRT(インシデント対応)系	システム開発対応の経験に加え、障害対応経験者	・セキュリティやマネジメントに関する知識 ・ポリシーやガイドライン作成 ・インシデント対応業務
ドキュメント、教育、アセスメント、監査系	シニア層を含むスタッフやプレゼン経験者	・セキュリティやマネジメントに関する知識 ・教育資料の作成や従業員育成

出典　JPCERT/CCより

CSIRTの課題

ポイント

各CSIRTが抱える課題とは？

①人材問題

- 人員の確保
- 次世代人員の教育

②何をどこまでやったらいいのかわからない

- 対策レベルがわからない

③情報が入ってこない

- ベンダーに聞いても事例が無い

出典　NCAより

アジェンダ

0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

PSIRT構築のポイント

ポイント

LAC

①体制構築

既存の組織をベースに体制づくり。社外窓口必須。
CSIRTがあれば、CSIRTを中心に拡大。

②ポリシー・ガイドライン策定

守るものを明確に

③報告フロー策定

既存のフローをベースに

④NCA加盟

見極め。実際の事例入手可能。

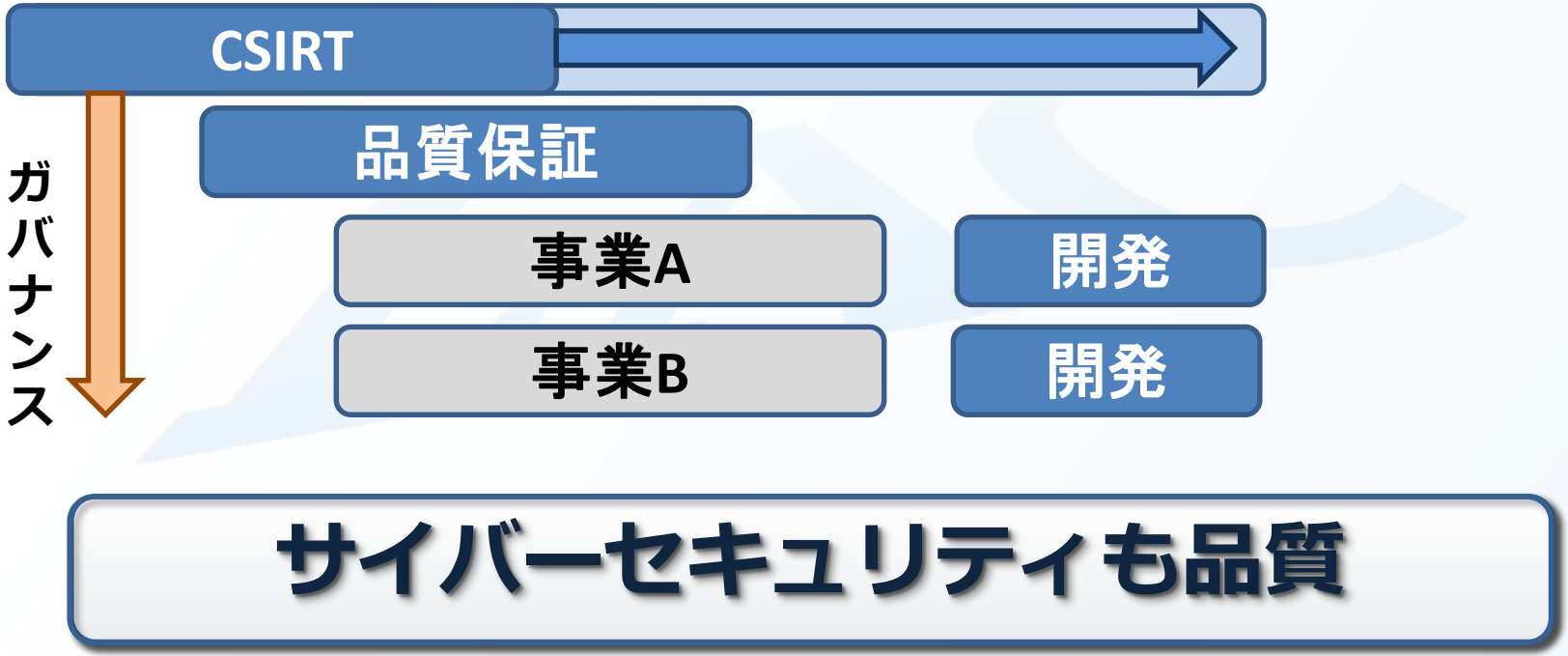
⑤組織拡充

PSIRT構築のポイント

①推進体制の整備

既存CSIRTベースに開発・品質保証部門との連携

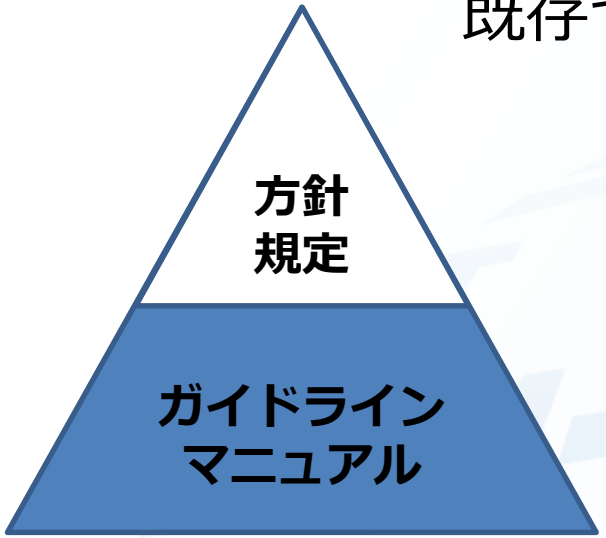
※既存CSIRTは全社に渡るガバナンス組織がほとんど。



②規定類の整備

規定・ガイドラインの整備

既存セキュリティガイドラインにIoTも追加



■セキュア開発、運用方針・規定・標準

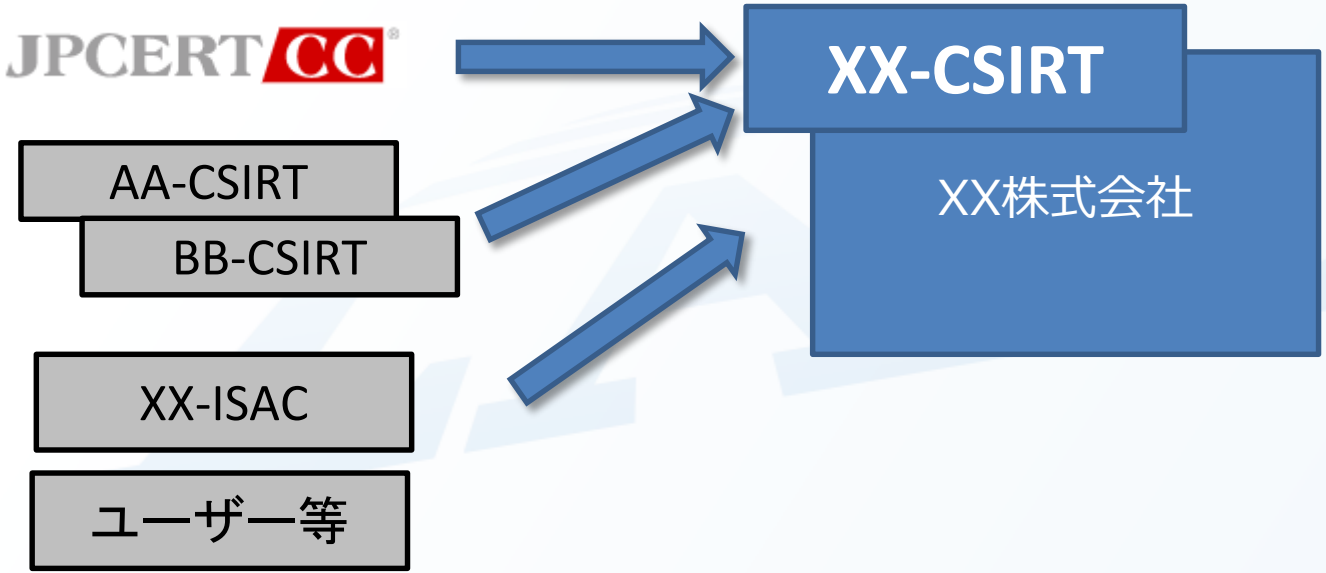
■各種ガイドライン、マニュアル

事業A	開発
事業B	開発

サイバーセキュリティガイドライン

③社外窓口の整備

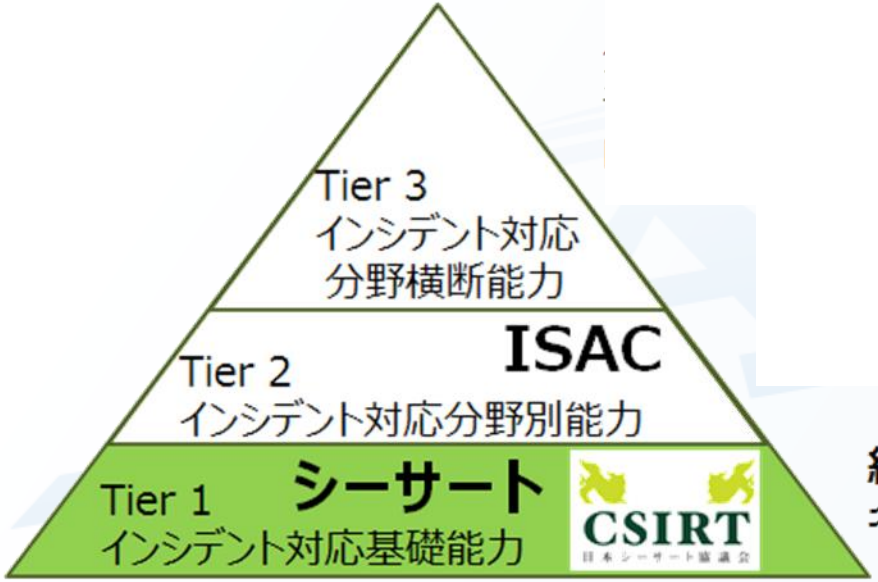
JPCERT/CCや社外からの連絡窓口の集約



社外連携には窓口が必須

PSIRT構築のポイント

NCA加盟により、現状の対策レベルを見極め、サイバーセキュリティ基礎能力を効率的に向上させる



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

加盟後にやるべきところをさらに磨けばよい

CSIRTの課題と施策

各CSIRTが抱える課題とは？（CSIRT/PSIRT共通）

①人材問題

- 人員の確保
- 次世代人員の教育

②何をどこまでやったらいいのかわからない

- 対策レベルがわからない

③情報が入ってこない

- ベンダーに聞いても事例が無い

出典　NCAより

CSIRTの課題と施策

ポイント

各CSIRTが抱える課題とは？（CSIRT/PSIRT共通）

①人材問題

・人員の確保

・次世代人員の教育

⇨ **適材適所でベンダーを活用**

②何をどこまで何をやったらいいのかわからない

・Topダウンでやれと言われたが、、

③情報が入ってこない

・ベンダーに聞いても事例が無い

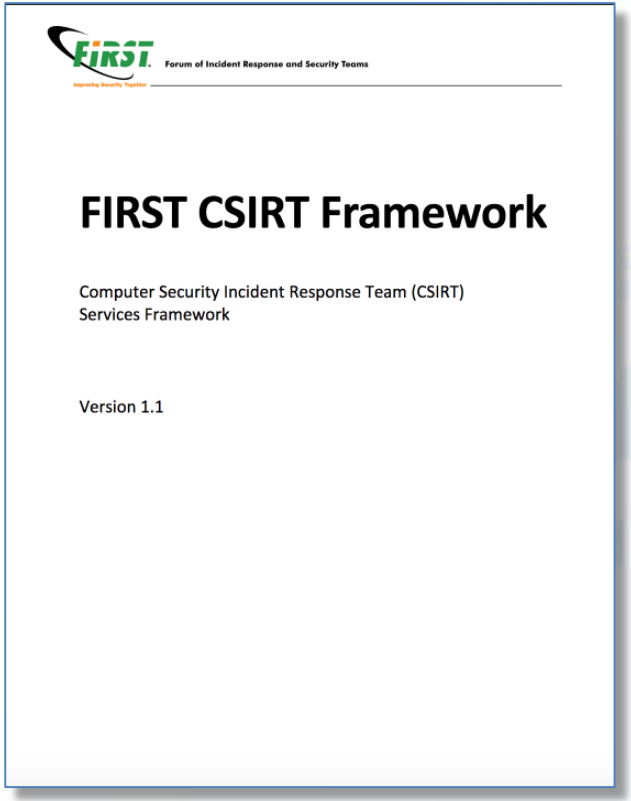
⇨ **まずは、NCAに加盟して**

出典　NCAより

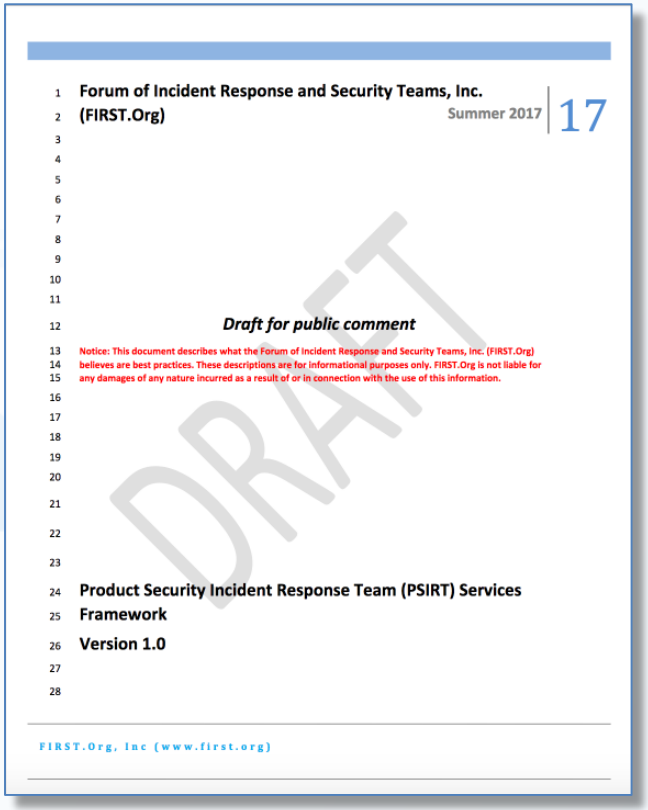
ご参考

ガイドラインとかいろいろありますが、

FIRST CSIRT SERVICES FRAMEWORK



CSIRT Framework V1.1



PSIRT Framework

アジェンダ

0．はじめに
1．プロフィール
2．インシデント発生状況
3．IoTセキュリティ
4．CSIRTのおさらい
5．CSIRT構築の課題
6．PSIRT構築のポイント
7．まとめ

7．まとめ

インシデントは“０”になりませんから、“０”に近づける活動と、インシデント対応のためにCSIRTが必要です。

7．まとめ

まずは、形ばかりで良いですから、CSIRTを立ち上げてNCAに加盟するところがスタート、それが成功の鍵。

7．まとめ

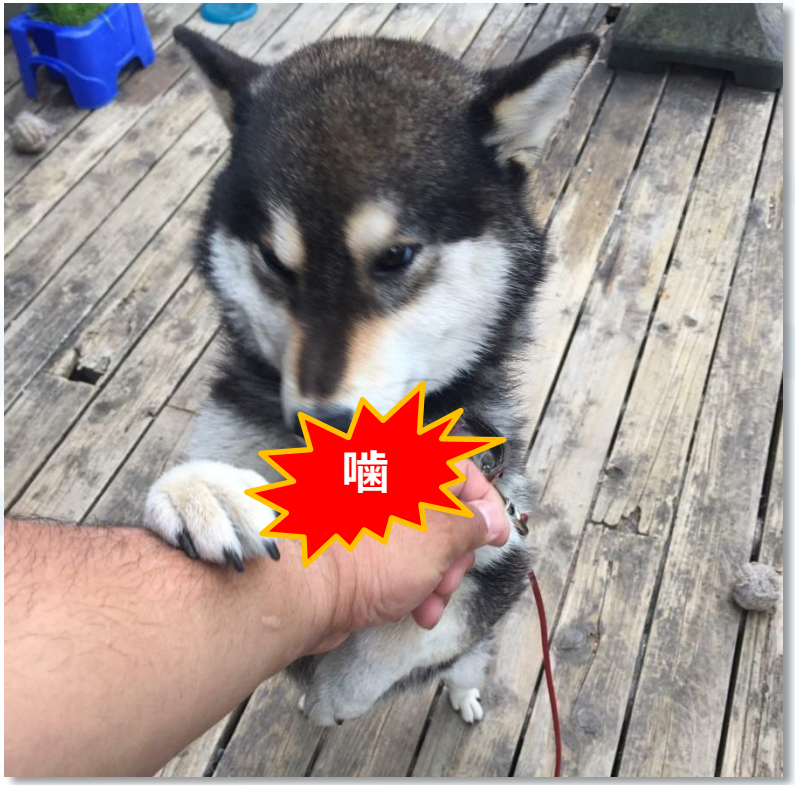
ポイント

なるべく既にあるものは使い、SOC運用など、本来の専門・業務でない部分は専業ベンダーを賢く活用すべき、それが早道。

おまけ

■黒柴ちゃん❤　飼ってます

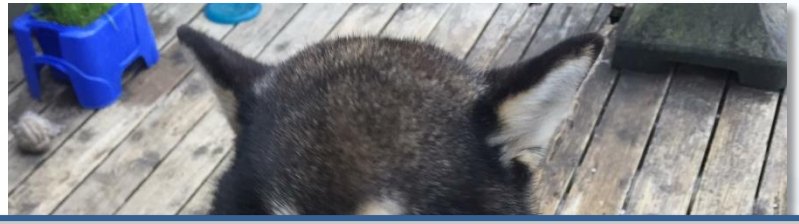
癒されてますが、



気を許すと噛みつかれます！！

■黒柴ちゃん❤　飼ってます

癒されてますが、



噛まれないように世話することと
噛まれた後の手当を迅速に！

気を許すと噛みつかれます！！

ご清聴ありがとうございました。

昨日の技術は過去のもの。明日の技術は自分の中に。

※ 本資料は2017年12月現在の情報に基づいて作成しており、記載内容は予告なく変更される場合があります。
※ 講演における発言等については、講演者の個人的見解を含んでおり、著作については講演者に帰属します。
※ 本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※ 本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。

株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1
平河町森タワー
Tel 03-6757-0113　Fax 03-6757-0193
sales@lac.co.jp
www.lac.co.jp