Internet Week 2013
T1：CSIRTの実例から学ぶ企業のセキュリティ対策の今

国内CSIRTの傾向

日本シーサート協議会　専門委員
CSIRT研究家
山賀正人

はじめに

- CSIRTに規格はない
  - インシデント対応のガイドライン
    - RFC2350 “Expectations for Computer Security Incident Response”
    - ISO/IEC 27035 “Information security incident management”
    - NIST SP 800シリーズ

- 各企業の実情・現状に即したCSIRTの実装
  2つとして同じCSIRTは存在しない

CSIRTの分類（CERT/CCのCSIRT FAQより）

- 組織内CSIRT（Internal CSIRT）
  - 組織内で発生したインシデントに対応
- 国際連携CSIRT（National CSIRT）
  - 日本ではJPCERT/CC
- コーディネーションセンター（Coordination Center）
  - 協力関係にある他のCSIRTとの連携・調整
  - グループ企業間の連携など
- 分析センター（Analysis Center）
  - インシデント傾向分析、マルウェア解析、痕跡分析、注意喚起など
- ベンダチーム（Vendor Team）
  - 自社製品の脆弱性に対応
- インシデントレスポンスプロバイダ（Incident Response Provider）
  - セキュリティベンダ、SOC事業者など

本資料で解説

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

CSIRT 日本シーサート協議会

組織内CSIRT

「組織内」の対象範囲によって実装も運用も異なる

- 社内インフラ
  - 広報用Webサイトなども含む
- ネットワーク経由の顧客サービス用サイト
  - オンラインショッピング
  - クラウド、XaaSなど
- 顧客サイト
  - （主に）SIビジネスで納入したシステム
  - 実質的「インシデントレスポンスプロバイダ」機能

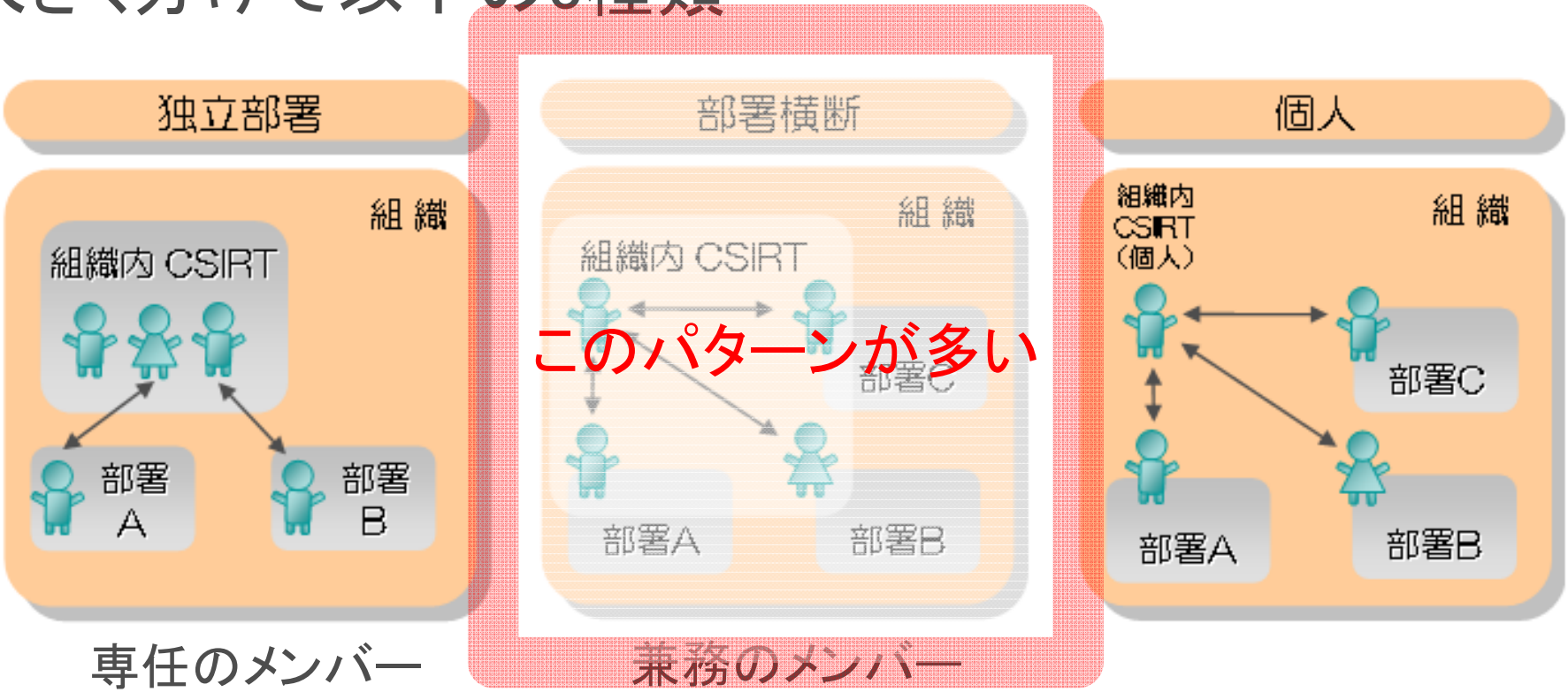
CSIRT設立の理由・経緯

- 深刻なインシデントの経験
- 現場の問題意識
- 事業者としての責任、品質保証のため
- 対外的なコミュニケーション、情報交換のため
  - 既に体制としては出来上がっているケースも
- 調達要件に含まれている
- 監督省庁からの指示
- 同業他社の動き

など

CSIRTの実装形態

大きく分けて以下の3種類



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

CSIRT 日本シーサート協議会

コアとなる部署の有無

- あり
  - 情シス
  - 研究所
  - 品質保証
  - 開発
  - 企画（経営企画、IT企画など）
  - リスク管理、災害対策
  - 総務

  など

- なし（完全にフラット）
  - WG、タスクフォース、委員会、ボランティアなど

サービス内容

コアとなる部署の役割と密接に関係

- 技術的対応支援のみ
  - アドバイザーの位置づけ
  - 必要に応じて現場に出動（特殊専門部隊）
- IT系インシデントのみに対応
- IT系に限定せず各種インシデントに対応

対応指示・命令に従わせる権限

- あり
  - セキュリティポリシー等の規定に明記
- なし
  - 権限を持つ人（or部署）と完全に分離され、必要に応じて連携
  - 権限を持つ人（or部署）が兼務することで実質的に権限を有している
  - 権限を持つ人（or部署）に直接（容易かつ速やかに）エスカレーションできる体制

権限の有無は、IT系か否か、新しい企業か否かによらない

CSIRT構築の障害

- 以前から今もある障害
  - 経営層をはじめとする社内の理解を得られない
    - 費用対効果を説明できない
    - 現状の体制で充分との思い込み

- 最近の傾向
  - CSIRTに対する経営層の過大な期待
    - 政府の文書などにCSIRTの名前が載るようになったことで知名度は上がったがCSIRTそのものの理解は不充分
    - CSIRTさえ作れば、それで全てが解決するとの幻想
    - 「教科書」通りでなければいけないとの思い込み
    - はじめから「完璧」なものを作ろうとしてしまう

構築後のCSIRTが抱えている課題

- 予算の確保
  - 兼務の場合の労務管理の問題を含む
  - メンバーの所属部署の持ち出し
  - 品質保証の予算に計上しているケース
- 人材の確保、継続性
  - 現在の担当者個人への依存度が高い
  - 特に非IT系企業における人材確保問題
- 成果の見せ方

ご清聴ありがとうございました。

CSIRTに関して：csirt-pr@nca.gr.jp
NCAおよび加盟に関して：nca-sec@nca.gr.jp

CSIRT
日本シーサート協議会

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