CWS@CSS
組織論の視点からみた
CSIRT

明治大学経営学部教授
日本シーサート協議会専門委員
中西　晶
https://www.facebook.com/NakanishiAki

自己紹介：中西晶（なかにし　あき）

- 2005年　情報セキュリティ政策会議　技術戦略専門委員会　委員
- 2007年　「高信頼性組織の条件」出版
- 2009年　企業情報化協会　IT人材活性化研究会コーディネイター、IT賞審査員
- 2010年　FIRSTを覗いてみる
- 2016年　内閣府SIP（戦略的イノベーション創造プログラム）「重要インフラ等におけるサイバーセキュリティの確保」推進委員会委員、セキュリティ運用WG主査
- 2017年　東京都「ICT先進都市・東京のあり方」懇談会　構成員「想定外のマネジメント【第3版】」翻訳
- 2018年　内閣サイバーセキュリティセンター普及啓発・人材育成専門調査会　構成員

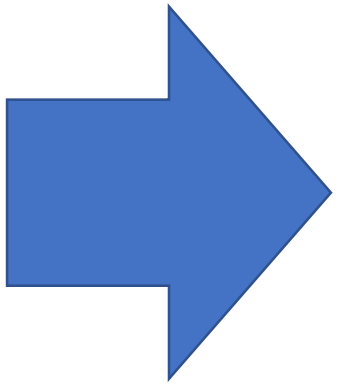
故・山口英氏@Internet Week 2003

思いもよらないところからでてくるからこそトラブルであり、それがトラブルの本質

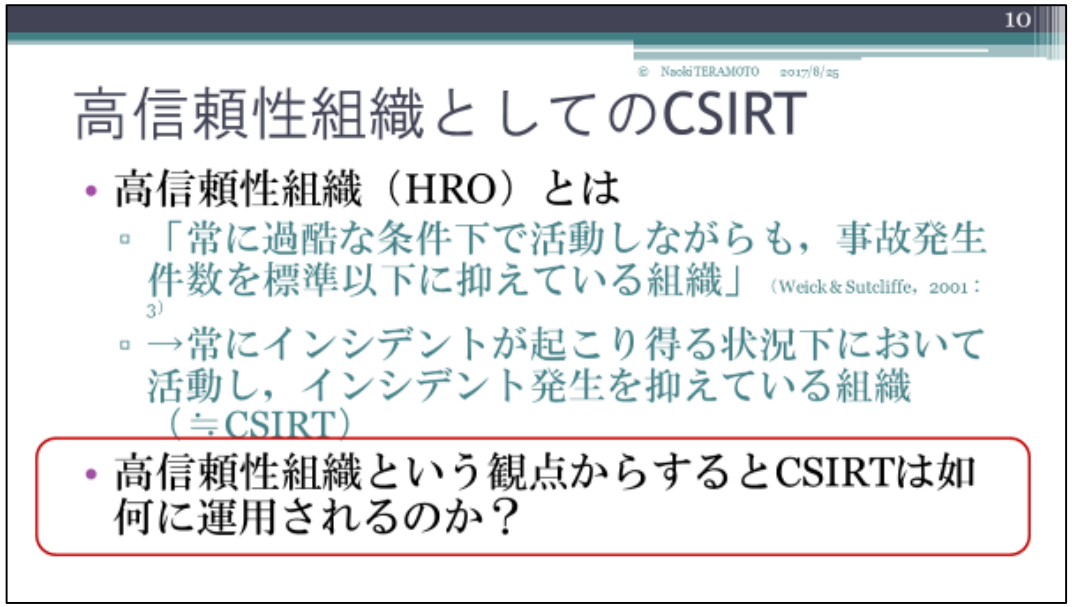
想定外のことにいかにうまく対応していくかがセキュリティ管理の課題

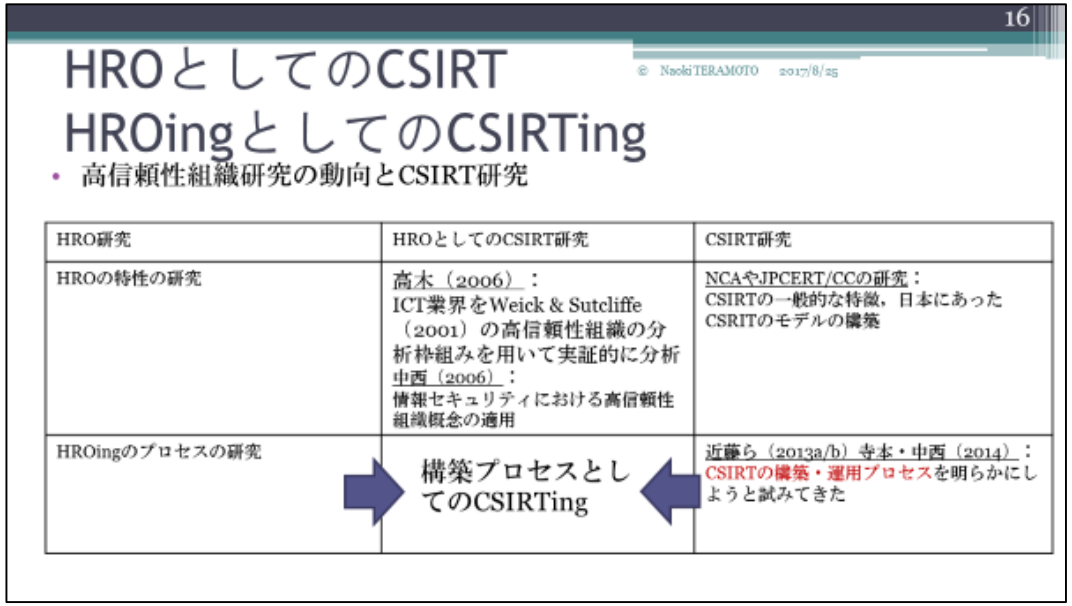
Security Day 基調講演「セキュリティ管理と高信頼性組織の構築」
http://www.itmedia.co.jp/enterprise/0312/04/epn01.html

想定外のマネジメントに強くなる



高信頼性組織とCSIRT研究





寺本直城・近藤光(2017)「CSIRTからCSIRTingへ　―高信頼性組織化の視点から―」
＠日本情報経営学会第74回全国大会（東京理科大学）

われわれの理解（その１）

5

CSIRTの現状

© NaokiTERAMOTO 2017/8/25

⇒各CSIRTは協力関係にあり、複雑化するインシデントに対して、連携し、情報収集・情報共有を行っている。

- FIRST（Forum of Incident Response and Security Teams）

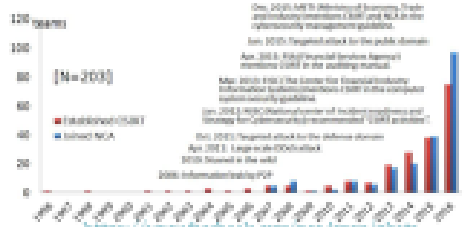
CSIRT間でのWorldwideな連携を取るための連合体
⇒約60か国・約300チームが加盟（日本からは28チームが加盟）
（http://www.first.org/about/organization/teams：2017年6月1日現在）

- NCA（日本CSIRT協議会）

日本国内におけるCSIRTの連合体
⇒日本国内のCSIRT・234チームが加盟
（http://www.nca.gr.jp/member/index.html：2017年6月1日現在）

CSIRT
日本シーサート協議会

徐々に増えつつあるが、企業の数からするとまだまだ少ない
組織がCSIRTを実装するにあたって、いくつかの課題がある



https://www.facebook.com/nca.japan/photos/a.[illegible]/[illegible]/?type=3&theater（2017年6月1日）

寺本直城・近藤光(2017)「CSIRTからCSIRTingへ　―高信頼性組織化の視点から―」
＠日本情報経営学会第74回全国大会（東京理科大学）

われわれの理解（その２）

CSIRTの問題点（まとめ）

- パフィーマンスの維持が困難
  1. 構想フェーズ
     - 何らかの問題が実際に起こる
     - 組織の意思決定者が何らかの脅威を感じる
     - 情報セキュリティに関わる現場が危機感を感じる
  2. 構築フェーズ
     - 以上のような問題点からCSIRTが構築される
  3. 運用フェーズ
     - 問題が起こっていないときのCSIRTの運用
     - CSIRT構築時と現状の環境等の違い
     - 運用コストの問題
- 多くのCSIRTにおいて，構想・構築フェーズはそれなりに乗り越えられるが，運用フェーズにおいては多くの問題が生じ，結果として「形骸化」や「存続の危機」といった問題点に繋がってくる

寺本直城・近藤光(2017)「CSIRTからCSIRTingへ　―高信頼性組織化の視点から―」
＠日本情報経営学会第74回全国大会（東京理科大学）

過去の調査研究結果より　1

- JPCERT/CC x 明治大学での調査（2006）
  - https://www.jpcert.or.jp/research/ICT.html
  - マインドにおける問題解決志向の高さ（カテゴリの精緻化）が稼働率につながる。
  - 多様な情報共有手段（オールドメディア含む）の利用
  - 業務特性・制約を考慮したうえでの教育訓練のための取り組み

過去の調査研究結果より　2

- TELECOM_ISAC ACCESS_WG×明治大学（2008）
  - すべてのメンバーが参加できるようにコミュニケーションを工夫
    - 「2回やる」「現場でやる」「オフィスレイアウトを工夫」など
  - 新任者が1人前になるまでの教育プロセス
    - 「座学」→「1対1でOJT」→「チーム参加」→「ペアでお泊り」→「1人でお泊り」
  - モチベーション向上のための機会
    - 研修機会の提供や表彰制度（管理者の推薦、職場での互選）、表彰はしないが「GOOD対応」を管理者からフィードバックなど

過去の調査研究結果より　3

- ストーリーテリングによる知識伝承（2010）
  - 手順書やマニュアルに落とし込めない部分の「疑似経験」ツール

組織論からみたCSIRT

組織ルーティン

チームビルディング

越境学習

レジリエンス

正統性の獲得

ストーリーテリング

CSIRT

実践としてのセキュリティ

組織文化

イシューセリング

高信頼性組織

世代間知識伝承

人材育成

コミュニティ・オブ・プラクティス

セキュリティ心理学

組織マネジメント

最近考えていること

- AI, IoT, BigDataといったバズワードとCSIRT
- 組織人/プロフェッショナルとしてのキャリアとモチベーション
- コミュニティ発展のための課題
  - 世代間での知識とマインドの伝承
- 「公衆衛生モデル」の妥当性
  - 家庭の手洗いからBSL４まで
- リスク/クライシスマネジメントやBCM（事業継続マネジメント）における位置づけ
- Safety（OT：PSIRT)とSecurity（IT:CSIRT)の共通言語

2019年度科研費「情報社会とトラスト」に申請