

CSIRT について

- CSIRT の現在地（資料 6－1）
- サイバーセキュリティにおけるインシデント対応コミュニティ
の発展（資料 6－2）

CSIRTの現在地

30年間の成果と今後コミュニティに求められるもの

JPCERT/CC

小宮山 功一郎



今日のお話は3部構成です。

第一部

CSIRTコミュニティの成功 (1988-2010年頃)

第二部

成功が招いた諸問題 (2015-現在)

CSIRTは互惠主義の文化を保てるのか(未来)

第三部

CSIRTを作りたい方へのポイント

(1988-2010年頃)

CSIRTコミュニティの成功

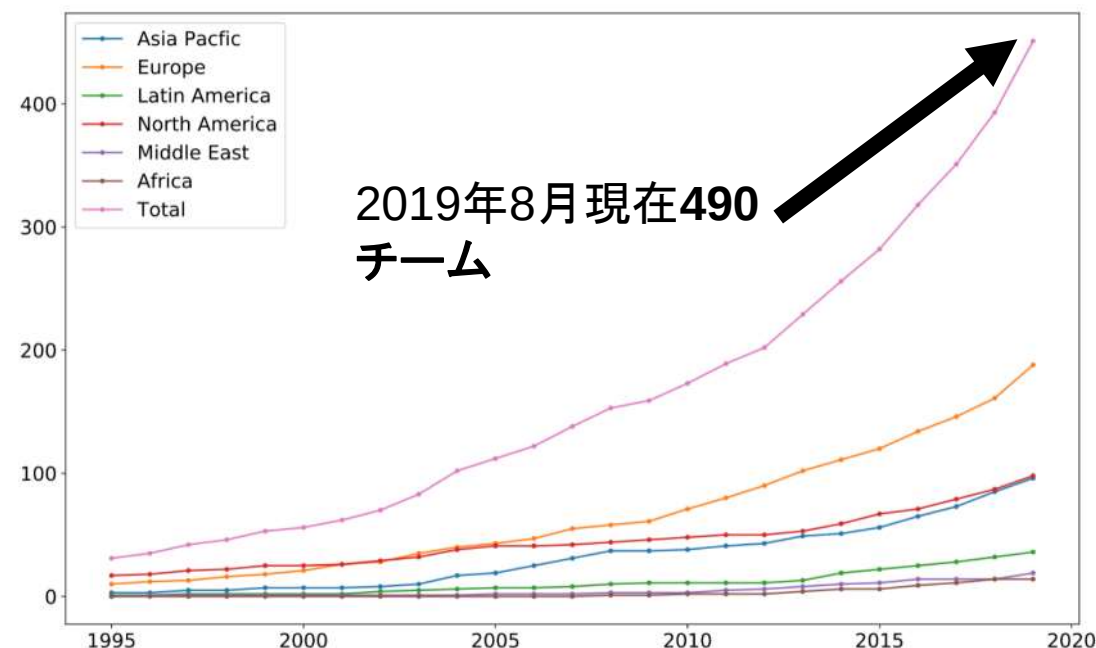
コミュニティの拡大

日本



NCA加盟チーム数 <https://japan.zdnet.com/article/35105208/>より

世界



<https://www.first.org/about/reports/FIRST-Annual-Report-2018-2019>

(2015-現在)

成功が招いた諸問題

外的要因

- 安全保障問題
- 攻撃の高度化と先鋭化

内的要因

- サイバーセキュリティがビジネスとしての成立
- コミュニティの拡大
- ナショナルCSIRTの変質

サイバーセキュリティが大きな政治課題に

グループ	組織、会議体、ルールの例	主たる目的
インターネットガバナンス	ICANN、IANA、インターネットソサイエティ（ISOC）	インターネットの統治と管理
人権	市民的及び政治的権利に関する国際規約、フリーダムオンライン連合	サイバー空間における人権確保
テレコム	国際電気通信連合（ITU）	テレコムの管理
貿易	世界貿易機構（WTO）、ワッセナー・アレンジメント	公正な貿易確保、兵器輸出管理
法の執行	欧州評議会サイバー犯罪条約、インターポール、警察	サイバー攻撃者の検挙・訴追
国際法	サイバーGGE、国連総会、タリンマニユアル	サイバー空間における法の支配の確立
規範	サイバー空間安定化に関するグローバル委員会（GCSC）、ASEANリージョナルフォーラム（ARF）、欧州安全保障協力機構（OSCE）、テックアコード、信頼憲章	サイバー空間における期待される振舞いの設定
キャパシティビルディング	サイバー専門性に関するグローバルフォーラム（GFCE）、世界銀行	サイバー空間における格差の是正
標準化	IEEE、ISO、IETF、W3C	サイバー空間を支える技術の標準化
インシデント対応	CSIRT、警察	サイバー空間における被害者の救済と復旧
市民団体	電子フロンティア財団、プライバシーインターナショナル	サイバー空間における市民の権利保護
軍	NATO、各国軍隊	サイバー空間におけるパワーの行使
情報活動	ファイブアイズ、各国情報機関	サイバー空間を利用した情報活動

小宮山(2019)より

(2019～)

CSIRTは互惠主義の文化を保てるのか

CSIRTとはなんなのか？

提唱者	CSIRTとは何か
NCA, 2007	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。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。
ENISA, 2008他	(インターネットにおける) 消防署
JPCERT/CC, 2008	組織内の情報セキュリティ問題を専門に扱う、インシデント対応チーム
Internet Governance Forum, 2014	独立した技術者のネットワークであり、コンピュータセキュリティインシデントへの対応・解決策の調整および通知、情報の交換、インシデントの被害予防を助ける活動を行うもの
Klimburg and Zylberberg, 2015	保険や建築基準法の試験員や法執行機関の捜査員に似た存在
Bradshaw, 2015	広くインターネットコミュニティのために、自らの技能と知識を用いてインシデントの防止、検知、対応を行う専門家集団
Caccherola, 2018	准外交の役割を果たすもの
Tanczer et al., 2018	非中央集権の自主管理されたコミュニティの模範

これからのCSIRTのあるべき姿

サイバーセキュリティガバナンスのレジーム

目的「救済と復旧」

機能「インシデント対応」

文化「互惠主義」

CSIRT

CSIRTとは

1. 被害者救済とシステムの復旧という目的をもち
2. インシデント対応の機能を備え
3. 互惠主義の文化をもつ組織群のこと

3つの要素どれか1つでも失うと、ユニークさを失う。

CSIRTを作りたい方へのポイント

CSIRTマテリアルについて

- 組織内CSIRTを整備し運用しようとするときに参照するための手引書
 - 組織内CSIRTについての理解
 - 機能、活動、リソース
 - 組織内CSIRTの構築プロセス
 - 構築の実作業を支援する資料集

- https://www.jpcert.or.jp/csirt_material/

- 2007年6月に初版を公開、2015年11月に第2版、2019年度の改訂に向けて準備中

CSIRTマテリアルの構成

■ フェーズ1：CSIRT構想フェーズ

経営層が組織内CSIRTの位置付けや必要性を企業統治の考え方に取り込んで理解する

— 「経営リスクと情報セキュリティ」

■ フェーズ2：CSIRT構築フェーズ

組織内CSIRT構築プロジェクトによる実作業を支援する

— 「組織内 CSIRT の必要性」

— 「組織内 CSIRT の役割とその範囲」

— 「組織内 CSIRT の活動」

— 「組織内 CSIRT の要員」

— 「組織内 CSIRT の形態」

— 「組織内 CSIRT の構築プロセス」

— 「組織内 CSIRT の実作業」、フォームと作成例

— 「インシデント対応マニュアルの作成について」

— 「組織内CSIRT の情報管理と設備について」

— 「組織内CSIRT における電話対応について」

— 「PGP の説明に役立つデータ」

■ フェーズ3：CSIRT運用フェーズ

組織内CSIRTメンバがCSIRTの活動を理解し実践する

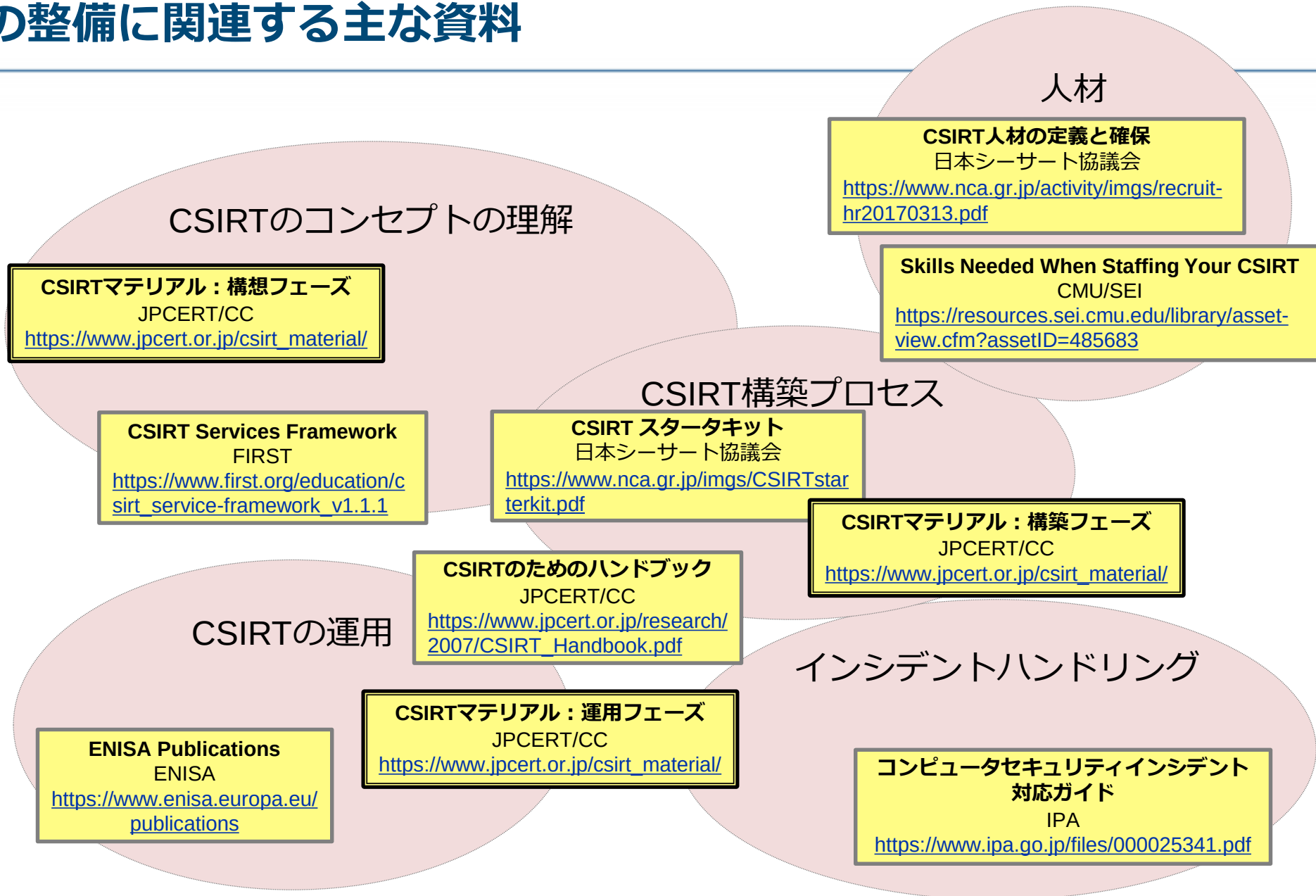
— 「CSIRT ガイド」

— 「インシデントハンドリングマニュアル」



CSIRT の基本的な枠組み	
サービス対象者	ポイント - CSIRT は「誰のために」あるいは「どの範囲に対して」活動をするのか - サービス対象者の定義と、その関係を明示する - サービス対象者を定義しない場合、その理由を明確にする。例えば、顧客がサービス対象である場合は、顧客情報及びサービス提供の詳細な内容を秘密にする場合がある - サービス対象者が、他の組織によるサービス対象者と重複する場合があるが、その際は、サービス対象者に対する権限の違いを明確にする (例) - 会社内及び子会社の従業員及び弊社インターネットサービスを契約している顧客
ミッションステートメント	ポイント - 上記で定義されたサービス対象者に対し何をするのかを記述する - 親組織のミッションに基づかなければならない、あるいは、その範囲内で解釈されるものでなければならない - CSIRT の設立目的を併記することが多い (例) - 会社内及び子会社の従業員に対し、コンピュータセキュリティインシデントによる被害が軽減されるための環境及び仕組みの構築への支援をする - 会社内及び子会社の従業員に対し、インシデントが発生した場合の対応の支援をする - インターネットサービスを契約している顧客が、弊社インターネットサービスを起因とするインシデントに巻き込まれた場合、その被害の軽減と、迅速な復旧をする
提供するサービス	ポイント - 上記で定義されたサービス対象に対する直接のインシデント対応、あるいは、インシデント対応を実施する組織や部署に対する支援活動が、最低限必要である - サービス分類の3つのカテゴリ(「事後対応型サービス」「事後対応型サービス」「セキュリティ品質管理サービス」)を参考にして記述する - サービス対象者のニーズ、親組織の経営層からの期待が強く影響する (例) - インシデント対応 - インシデント対応の支援 - インシデント対応の他の組織及び部署との調整 - 社内及び顧客向けのシステムに関する脆弱性のハンドリング - 技術動向の監視と社内へ適切な部署への展開

CSIRTの整備に関連する主な資料



結論

1. 「CSIRTは問題解決のために助け合う」のではない「助け合うからCSIRT」なのである
2. 公助より共助、共助より自助

参考文献

- Moira West Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek. 2003. *Handbook for Computer Security Incident Response Teams* (CSIRTs) .
- United Nation 2015, Consensus Report http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
- Klimburg, Alexander and Hugo Zylberberg. 2015. “Cyber Security Capacity Building: Developing Access,” p. 22. Norwegian Institute of International Affairs.
- NCA. 2017. “日本シーサート協議会とは,” <https://www.nca.gr.jp/outline/>
- Tanczer, Leonie Maria, Irina Brass, and Madeline Carr. 2018. “CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy.” *Global Policy* 9 (November) : 60–66.
- Bradshaw, Samantha. 2015. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*.
- Choucrist, Nazli, Stuart Madnick, and Jeremy Ferwerda. 2014. “Institutions for Cyber Security: International Responses and Global Imperatives.” *Information Technology for Development* 20 (2) : 96–121.
- FIRST. 2017. “FIRST CSIRT Framework Version 1.1.” https://www.first.org/education/csirt_service-framework_v1.1.
(v2.0ドラフトが2019年6月に出ました。そちらのほうが進む予定)
- 日本シーサート協議会. 2011. “CSIRTスタータキット.” : 1–34.
<http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf>
- 一般社団法人JPCERTコーディネーションセンター (JPCERT/CC) . 2008. “CSIRTマテリアル.” https://www.jpcert.or.jp/csirt_material/ (January 30, 2019) .
- 小宮山功一朗. 2019. “サイバーセキュリティにおけるインシデント対応コミュニティの発展 - 目的、機能、文化から見るCSIRT -.” *情報通信学会誌* 37(1):13–23.
https://www.jstage.jst.go.jp/article/jsicr/37/1/37_13/article/-char/ja

○ 論文引用

サイバーセキュリティにおけるインシデント対応コミュニティの
発展 - 目的、機能、文化から見る CSIRT -

小宮山功一朗. 2019. 情報通信学会誌 37(1):13-23.

リンク先

https://www.jstage.jst.go.jp/article/jsicr/37/1/37_13/_article/-char/ja