

資料ダウンロード
<https://bit.ly/2ZrkLeC>

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 功一朗

koichiro.komiyama@jpcert.or.jp

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)

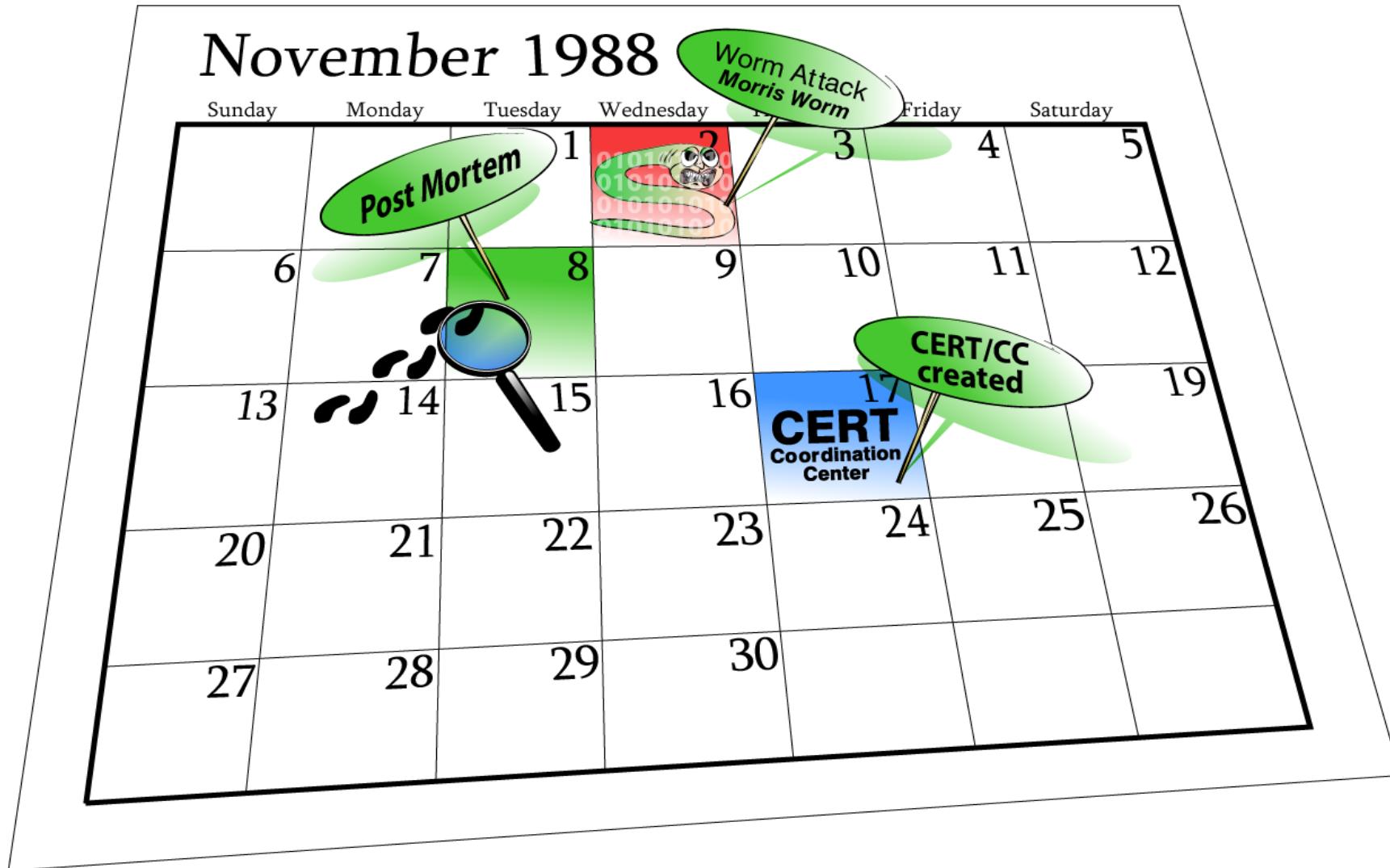
第三部

CSIRTは互恵主義の文化を保てるのか(未来)

CSIRT コミュニティの成功

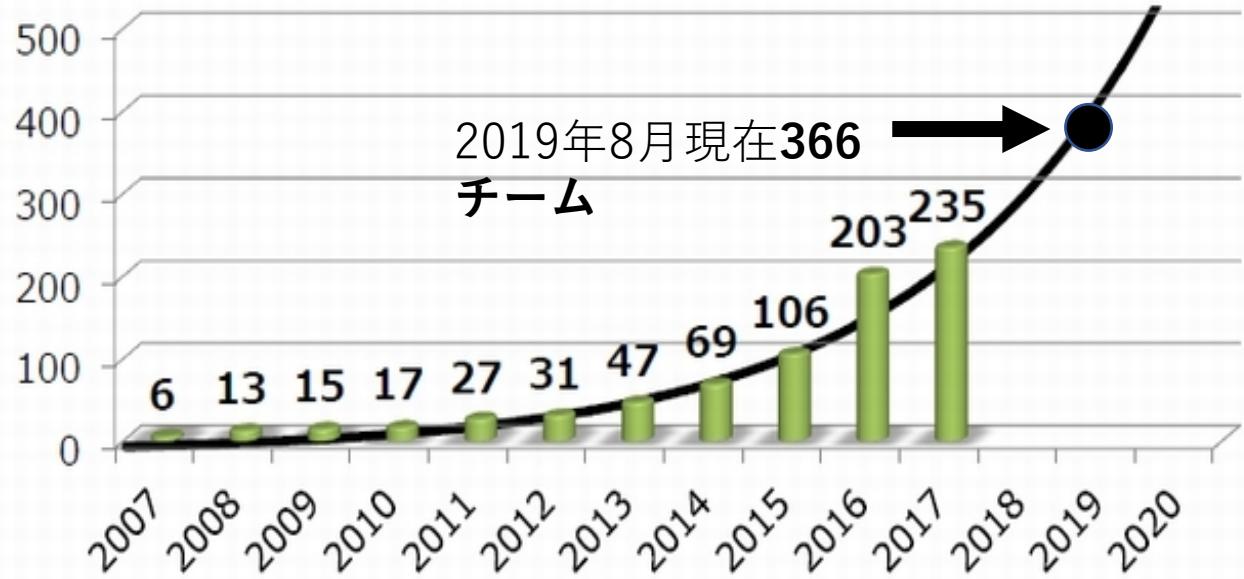
(1988-2010年頃)

CSIRTが生まれて30年が経った



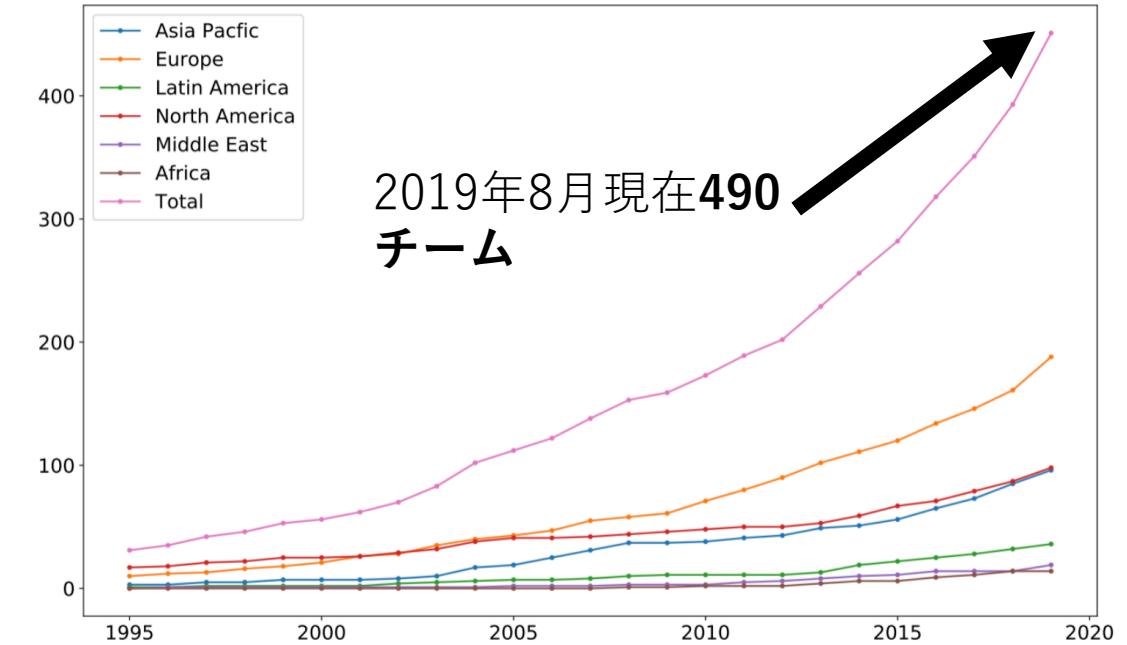
コミュニティの拡大

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.pdf> より

国際社会の合意

- 2015年7月に国連の政府専門家会合が提案し、後に総会で承認された11の提案 (UN, 2015)
 - (国家は) 意図して自らの国に存在するインフラを第三者が攻撃に利用するのを放置してはならない。
 - (国家は)他国のCERT/CSIRTを攻撃してはならない。
 - (国家は)自国のCERT/CSIRTをサイバー攻撃活動に関与させてはならない。

成功が招いた諸問題

(2015-現在)

CSIRTの課題

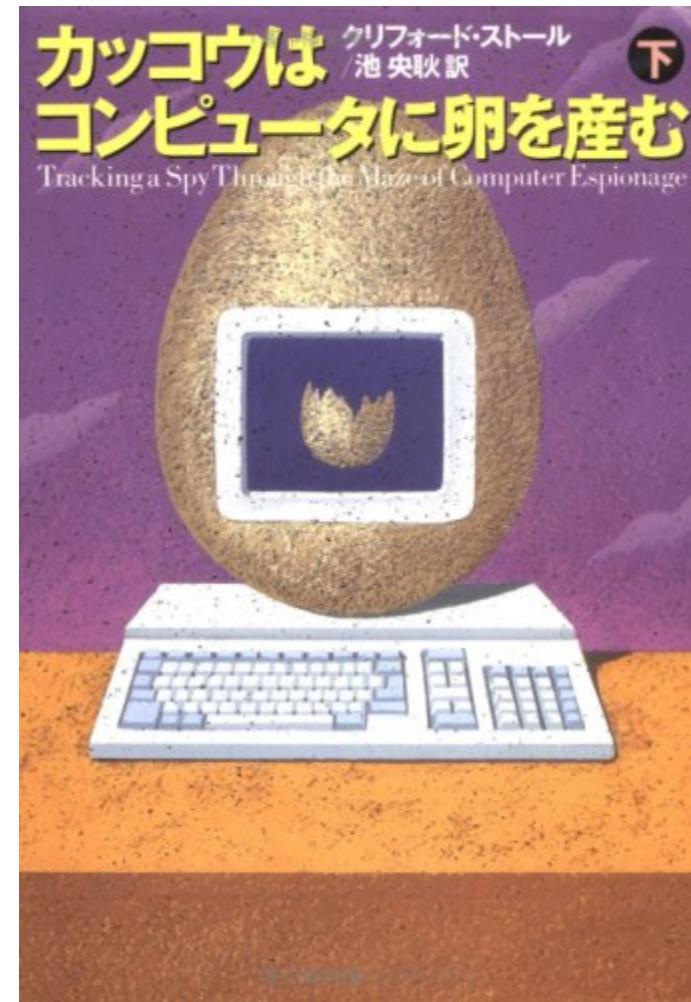
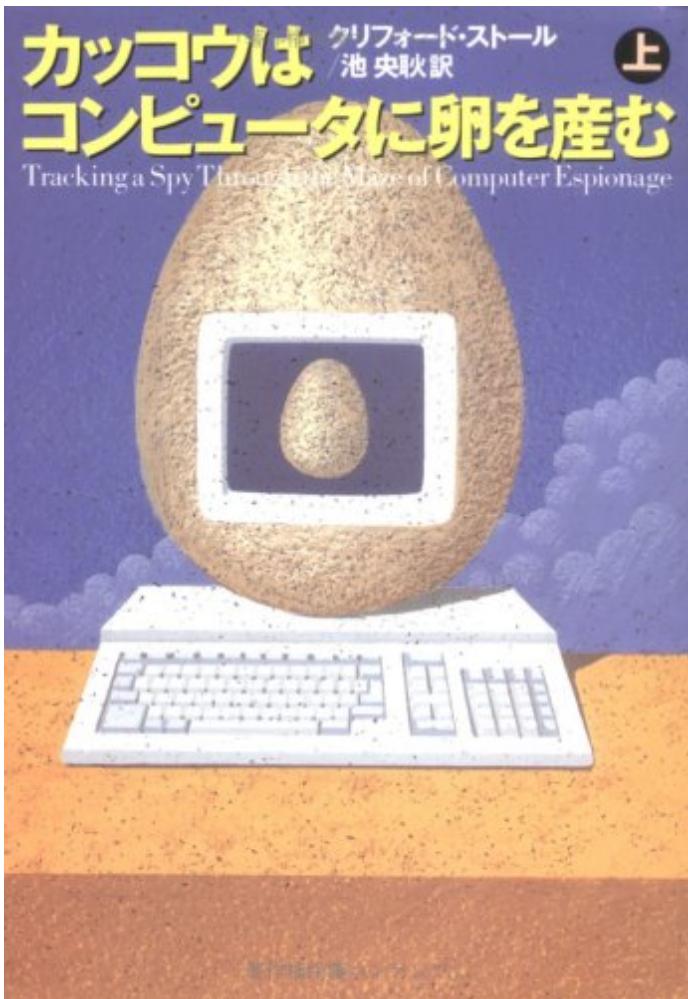
外的要因

- ・安全保障問題
- ・攻撃の高度化と先鋭化
- ・「サイバーセキュリティ」の守備範囲拡大

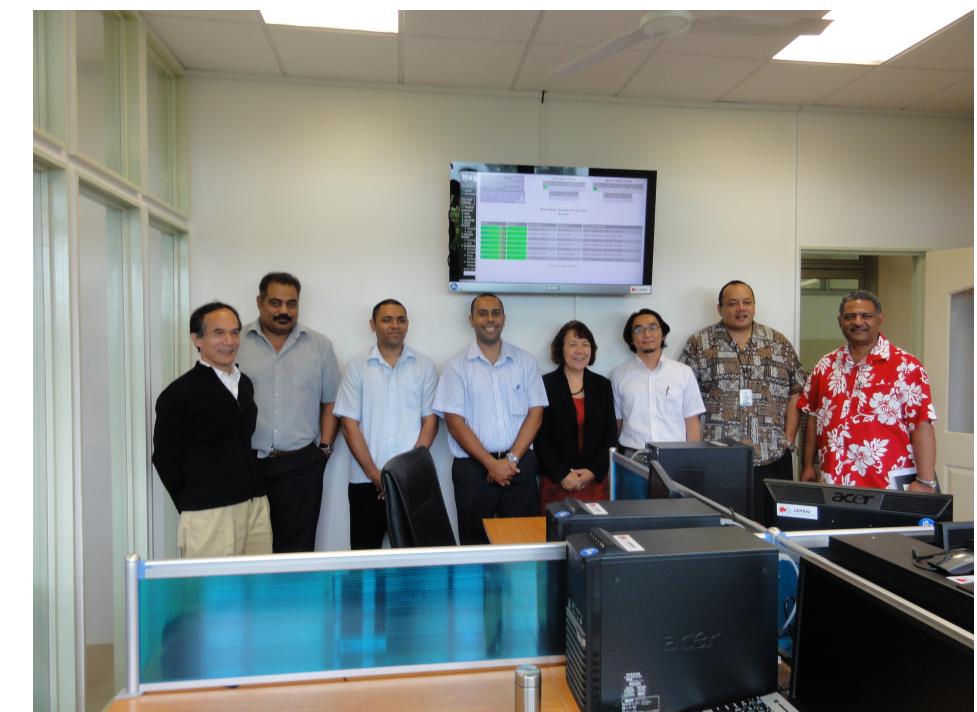
内的要因

- ・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

攻撃の高度化と先鋭化



安全保障問題 化



守備範囲拡大

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、タリンマニュアル	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

National CSIRTの変質

国名	現在のナショナルCSIRT（略称）	資金拠出組織（略称）	設置、設立年
米国	US-CERT	サイバーセキュリティ・インフラセキュリティ庁 (CISA)	2003年
オーストラリア	サイバーセキュリティセンター(ACSC)	通信電子局 (CSE)	2010年
ドイツ	CERT-Bund	情報セキュリティ庁 (BSI)	2001年
カナダ	センター フォーサイバーセキュリティー (CCCS)	通信保安局 (CSE)	(2003年)
フランス	CERT-FR	情報システムセキュリティ庁 (ANSSI)	2014年
日本	JPCERT/CC	経済産業省	1996年
日本	内閣サイバーセキュリティセンター(NISC)	内閣官房	2005年
イタリア	IT-CERT	経済開発省	2014年
韓国	KrCERT/CC	インターネットセキュリティ庁 (KISA)	2003年
韓国	KN-CERT	ナショナルサイバーセキュリティセンター (NCSC)	2004年
中国	CNCERT/CC	共産党網絡安全和信化委員会弁工室 (CAC)	2002年
シンガポール	SingCERT	サイバーセキュリティ庁 (CSA)	1997年
ニュージーランド	CERT NZ	ナショナルサイバーセキュリティセンター (NCSC)	2016年
英国	ナショナルサイバーセキュリティセンター (NCSC)	政府通信本部 (GCHQ)	2016年
フィンランド	NCSC-FI	通信規制局	2002年
ロシア	GOV-CERT.RU	ロシア政府	2012年
インド	CERT-In	電子情報技術省	2004年
メキシコ	CERT-MX	連邦警察	2010年
ブラジル	CERT.br	NIC.br(民間)	1997年

主要国のナショナルCSIRTと資金拠出組織 小宮山(2019)より

National CSIRTは役割も歴史も権限も組織の性格も大いに違う。

"National CSIRTの共通点については「技術的な問題についての、国際的に承認された連絡窓口機能をそなえること」という点くらいしかない"(Klimburg & Zylberberg, 2015)

CSIRTの課題 (再掲)

外的要因

- ・安全保障問題
- ・攻撃の高度化と先鋭化
- ・「サイバーセキュリティ」の守備範囲拡大

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

CSIRTは互恵主義の文化を保
てるのか

(2019~)

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

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 「互恵主義」

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. 互恵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。

いくつかの道筋

1. 共通の信条を「システムの正しさをもとにサイバー空間の安定を維持する」におき、サイバー版国際赤十字社として発展する可能性。
 - ホリスはe-SOSというコンセプトを提唱した。e-SOSは彼我の区別なく、サイバーに関連する分野において危機に陥ったものにたいして、人道の観点から技術的な支援を提供する仕組み (Hollis, 2011)
2. 共通の信条を「サイバー空間の公衆衛生確保する」とし、サイバー版WHOとして発展する可能性
 - ヒーリーらは世界からボットネットをなくすというクリーンアップ活動の中核をCSIRTが担えるとしている。(Healy & Knake, 2018)

まとめにかえて FIRST TC(大阪, 2018)で思ったこと



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/>
- Healey, Jason, and Robert K Knake. 2018. “Zero Botnets, Building a Global Effort to Clean Up the Internet.” : 40.
- Hollis, Duncan B. 2011. “An E-SOS for Cyberspace.” *Harvard International Law Journal* 52 (2) : 373–432.
- Internet Governance Forum. 2014. “Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security.” : 16. (URL省略)
- 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*.
- Choucri, 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。そちらのほうが今後の土台になる予定)
- 日本シーサート協議会. 2011. “CSIRTスタートキット.” : 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