情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

特定課題研究報告発表会
グローバル組織に求められるＣＳＩＲＴ
ーインシデントマネジメントの観点からー

２０２０年2月２２日（土）

後藤研修士課程１年
学籍番号　5595704
氏名　中元　隼

研究成果

背景、課題

・海外展開する日本企業に適したCSIRTガイドラインが存在しない。

本研究成果

・CSIRTと信頼の関係について考察した。
・複数の先行研究から海外拠点の組織の問題点を分析して独自に整理した。
・グローバル組織の場合、インシデントマネジメントの各段階で特有の課題が存在することを示した。
・海外拠点での情報セキュリティリスクをケーススタディを用いて分析した。

研究成果の活用者

・グローバル組織でCSIRTを運営・構築している人間。これから海外展開するCSIRT担当者

＊：グローバル組織とは日本本社で海外展開する組織を想定する。

本発表内容

①CSIRTの概要と信頼について
②グローバル組織の動向と課題
③グローバル組織におけるインシデントマネジメント上の課題
④グローバル組織における、拠点別の情報セキュリティリスク
⑤全体のまとめと今後の課題

①　CSIRTの概要と信頼について

CSIRT

CSIRT（シーサート）とは、Computer Security Incident Response Team
＝コンピュータセキュリティインシデント
（以降「インシデント」と略）に対応するチームの略

インシデントとは、一般的に「重大な事故に至る可能性がある出来事」を意味しており、コンピュータウイルスやサービス運用妨害攻撃、情報漏えいなど、ＩＴシステムの正常な運用または利害を阻害する（実害のある）事象だけでなく、そのような事象に繋がる可能性のある（まだ実害のない）弱点探索（プローブ、スキャン）なども含まれる。

CSIRTを構築するメリット

- 情報セキュリティに関する情報の一元的管理
- 窓口の一本化
- 外部とのインシデント対応に必要な信頼関係の構築

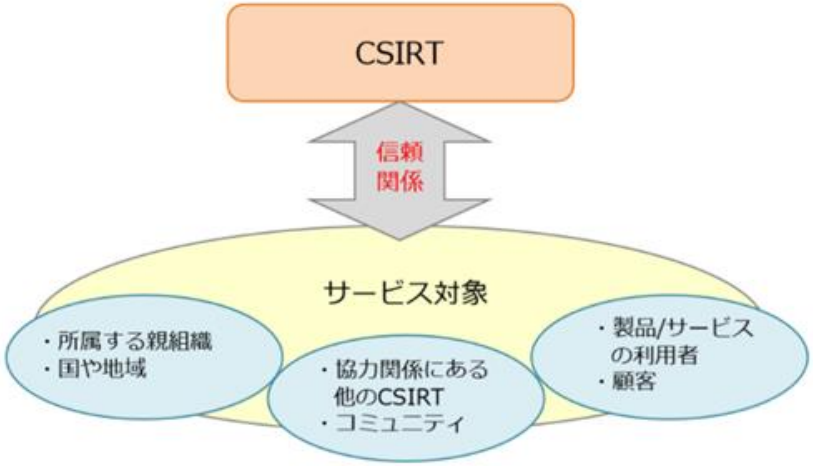
CSIRTに必要な能力

■　CSIRTに必要な能力としては**信頼**が挙げられる

先行調査・研究①

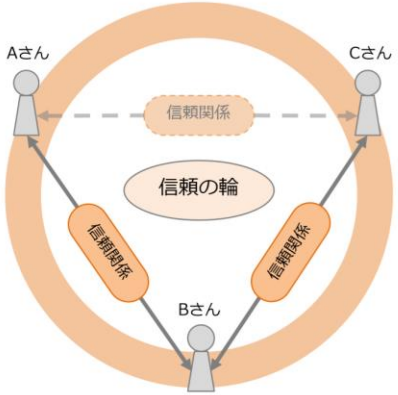
一般社団法人JPCERTコーディネーションセンター「CSIRTガイド」（２０１５年）

- CSIRTにとって最も重要なものは信頼関係。
- CSIRTの活動に大きな効果を生むためには、信頼関係に基づく信頼の輪を形成して共有できる情報を広げる必要がある



[図 3.1-1 CSIRT は「信頼関係」が命]

引用：ＣＳＩＲＴガイド
URL：https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf



[図 3.1-2 信頼の輪]
A と B の間に信頼関係があり、かつ B と C の間に信頼関係がある場合、A と C の間に直接の面識がなくても、A と C の間に信頼関係を成り立たせることができる。

引用：ＣＳＩＲＴガイド
https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf

CSIRTに必要な能力

先行調査・研究②

副島恵子、原田要之助「組織の情報セキュリティ向上の取り組みについて-CSIRTとISMSの類似と相違に着目した考察」（２０１７）

・従業員が異常に気付きCSIRTに報告することの重要性を指摘。

・報告の心理的ハードルを下げるために相談しやすい空気、普段から従業員とCSIRT間でコミュニケーションのパイプを持つこと。

先行調査・研究③

萩原健太、杉浦芳樹「CSIRTの最低要件」（２０１７）

・「信頼できる窓口」を構築することが最低要件の一つと言える。

先行調査・研究④

リクルートテクノロジーズ「現場で使えるセキュリティ事後対応」（２０１６）

・現場からの感謝がCSIRTの原動力であり、感謝されることで前向きに次のインシデントに備えることができる。

・感謝されるポイントとしては、インシデントを発生した人を責め、責任追及や批判しないことが重要。

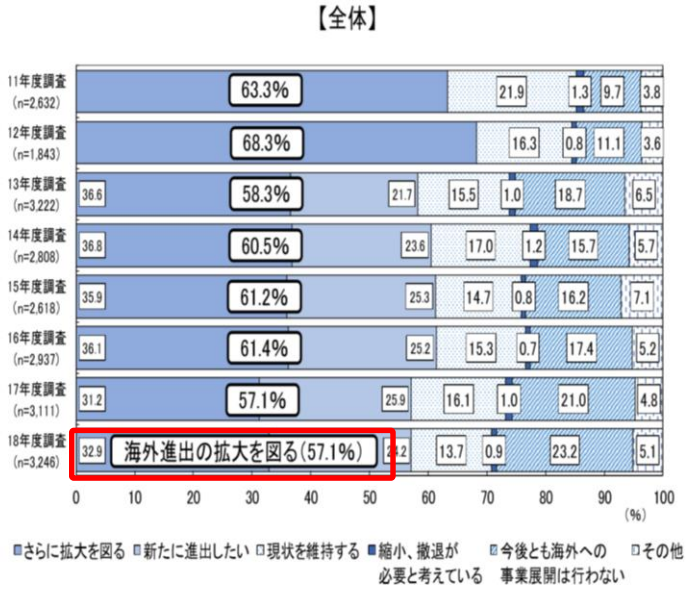
②　グローバル組織の動向と課題

日本企業の海外展開状況

日本の企業の海外進出が加速
人口減で国内から海外市場への移行する企業が増加している。

- 約６割の企業が今後３年で海外進出拡大を図る。
- 国外に進出している日系企業の拠点数は７万５,５３１拠点。
  （過去１０年間で約３９%増。前年度より約５.２%増）

⇒今後も海外進出は広がることが予想される。
広がるのは良いが問題点も存在。



地域	平成20年	21年	22年	23年	24年	25年	26年	27年	28年	29年	全体比	前年比
アジア	38,380	39,682	40,189	44,314	42,520	44,729	48,203	49,983	49,673	52,860	70.0%	+6.42%
大洋州	1,205	1,213	1,193	1,217	1,206	1,180	1,301	1,315	1,287	1,300	1.7%	+1.01%
北米	6,349	6,835	6,934	7,551	7,619	7,941	8,584	8,649	9,225	9,417	12.5%	+2.08%
中米	526	556	582	614	709	844	985	1,130	1,290	1,386	1.8%	+7.44%
南米	712	725	779	832	1,004	1,118	1,102	1,378	1,402	1,450	1.9%	+3.42%
西欧	4,787	5,097	5,198	5,210	5,138	5,280	5,577	5,773	5,810	5,833	7.7%	+0.40%
東欧・旧ソ連	1,127	1,209	1,287	1,360	1,414	1,423	1,451	1,458	1,544	1,613	2.1%	+4.47%
中東	625	629	650	635	618	678	713	756	851	877	1.2%	+3.06%
アフリカ	457	484	520	562	560	584	657	687	738	795	1.1%	+7.72%
南極	－	－	－	－	－	－	－	－	－	－	－	－
全世界	54,168	56,430	57,332	62,295	60,788	63,777	68,573	71,129	71,820	75,531	100.0%	+5.17%

引用：2018年度「日本企業の海外事業展開に関するアンケート調査」（ジェトロ）

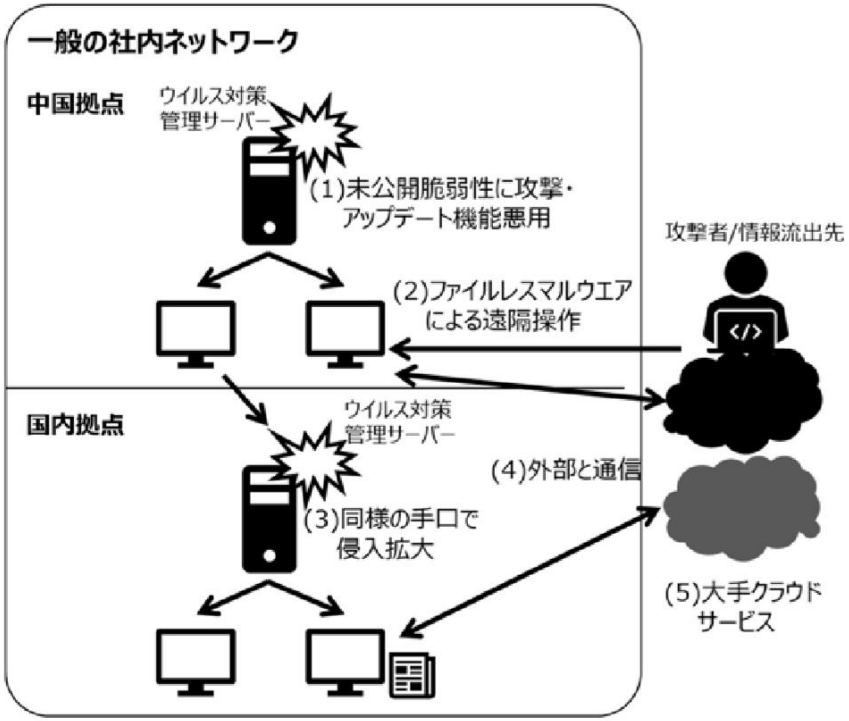
引用：海外在留邦人数調査統計（外務省）

海外拠点への攻撃事例

①三菱電機への不正アクセス事案
- ２０１９年３月１８日に中国拠点内にあるウイルス対策管理サーバに対してゼロデイ攻撃
- 中国拠点の端末を介して国内複数拠点の端末に侵入を拡大
- 同年６月２８日に挙動検知機能により、国内拠点の端末で不審な挙動を検知

②WannaCry（日立製作所）
- 最初に感染した端末は、欧州拠点にある検査機器（顕微鏡）
- 検査機器にパッチ適用が必要だと導入現場が認識できていなかった。

⇒ **海外拠点がセキュリティホールになる可能性**



引用：三菱電機：「不正アクセスによる個人情報と企業機密の流出可能性について（第３報）」
URL: https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

海外拠点を持つ組織の問題点

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■海外拠点を持つ組織の問題点を分析・整理するにあたって、以下の調査・先行研究を参考にした。

①企業における情報セキュリティ実態調査２０１７（ＮＲＩセキュアテクノロジー）
- NRIセキュアテクノロジーが毎年実施している企業の情報セキュリティに関する取り組みの実態調査。
- 質問の一部に海外拠点のセキュリティに関する質問。

②日本企業のグローバルITガバナンス（富士通総研：２０１２年）
- 海外で事業を行う一般企業を対象にグローバルITガバナンスの実態についてアンケート調査。
- ITグローバル人材、地域における課題を挙げる。

③淺井達夫「経済活動のグローバル化に伴う情報セキュリティ管理上の人的諸問題」（２０１２年）
- 異文化環境下においてセキュリティ・ポリシーを徹底しようとする際に、文化の違いによってどのような問題が発生するかを明らかにする。

海外拠点を持つ組織の問題点

分類	具体的な問題
人材（IT担当者）	・専任のIT管理者がいない傾向。存在したとしてもIT・セキュリティに関する知識が少ない。兼任の場合は経営や人事等の業務に忙殺され統制に手が回らない。 ・英語力もITもできる人は少ない ・駐在員の計画的ローテーションができていない
人材（現地採用職員）	・言語や文化が異なり、コミュニケーションが困難であり、教育やガイドライン・ポリシーの整備や遵守が困難 ・離職率が高く定着率が低い。教育しても離職されるとセキュリティのレベルが下がる。離職した後に以前いた企業の機密情報を使われる

海外拠点を持つ組織の問題点

分類	具体的な問題
環境・時差	・日本よりもインフラが弱い傾向にあり安定性に欠ける ・回線が細く、電力・通信が遅れており通信障害が発生する可能性 ・複数の海外拠点が存在する場合、拠点の規模が異なり標準化が困難 ・IT機器・サービスの調達・仕様の全体最適化が困難 ・IT利活用のモニタリング・資産管理が困難 ・法人格が異なることで情報セキュリティガバナンスがきかせにくい ・M&Aや合併化等により、情報セキュリティガバナンスがきかせにくい ・日本とは時差や距離が存在するため、コミュニケーションに時間がかかる ・地政学的理由によるサイバー脅威（政治状況、国際関係）が存在

海外拠点を持つ組織の問題点

分類	具体的な問題
地域特性（ASEAN）	①人材流動性の高さ ・人材流動性が顕著であり、様々な背景を持つ人間が存在 ②セキュリティリテラシーの不足 ・欧米では「悪意のある人」が脅威の前提だが、ASEAN地域ではリテラシー不足の人を脅威の前提とすべき ③国と文化の多様性 ・国によって経済的格差があり、シンガポールではPCやソフトウェアなどの調達は問題ないが、それ以外の国では現地調達が難しい場合がある。 ・中国系の社会では、夕食を自宅で食べ、その後で自宅で仕事をする文化が存在
地域特性（欧米）	・既に自社システムが確立されていることも多く、ガバナンスを強化しようとしても日本本社の意思を通しにくい。 ・独立性が高く独自の方針で決めたがり、経済合理性がなければ納得しない。 ・欧米関連会社のトップダウン方式が日本にあてはまらないため、スピードに差が出る。

第２章（まとめ）

■日本企業の海外進出が加速している一方で海外拠点を狙った攻撃も発生している。

■複数の先行研究・調査から海外拠点の問題点を整理・分析した。

■海外拠点を持つ組織には固有の問題（人材、環境・時差、地域特性）が存在する

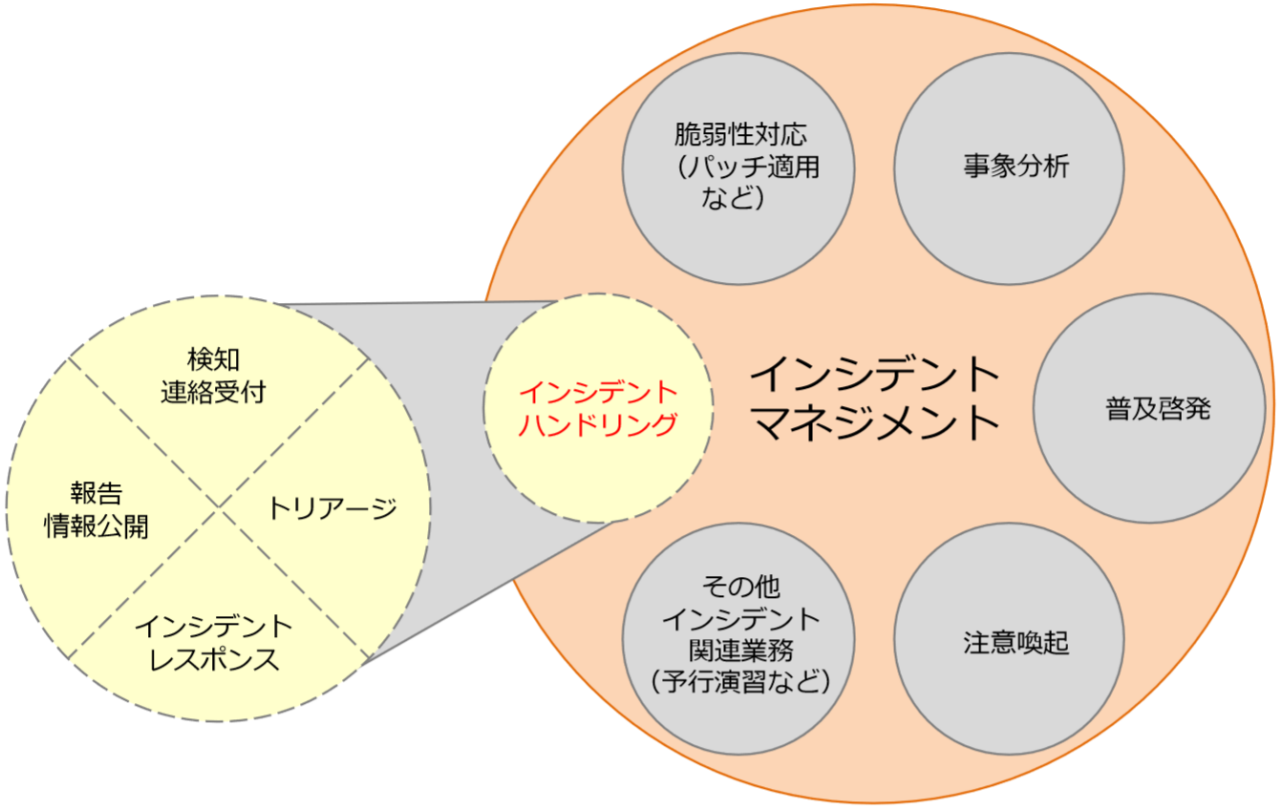
■これらの問題を踏まえた上でグローバルＣＳＩＲＴは構築・運用されなければならない

③　グローバル組織におけるインシデントマネジメント上の課題

インシデントマネジメント

■先ほどの海外拠点での問題点を踏まえて、インシデントマネジメントの観点からグローバル組織の問題点を列挙する

インシデントマネジメント：CSIRTがインシデントに対して行う活動全般



引用：JPCERT「インシデントハンドリングマニュアル」
URL：https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf

インシデントマネジメントの観点から見た課題

段階	グローバルCSIRTの課題
脆弱性対応	・IT資産管理ができていないため、脆弱性が把握できない ・利用するIT機器やソフトウェアが多様でありパッチの適応に時間がかかる ・海外拠点側ではパッチ適用の重要性を認識してもらえない
事象分析	・特定の地域を狙った脅威にも対応する必要 ・標的型攻撃の際、様々な言語に対応する必要
普及啓発・注意喚起	・言語や文化が異なるため、日本式の情報セキュリティ教育や情報セキュリティポリシーの遵守が上手くいかない、また翻訳による本来のニュアンスが変わる可能性

インシデントマネジメントの観点から見た課題

段階	グローバルCSIRTの課題
インシデントハンドリング	環境 ・ログ 　リアルタイム性、ログの送付漏れ、地域法の拘束 ・端末調査、フォレンジック ・回線の細さ 時差 　トリアージ、エスカレーション、端末調査 人材 　ヒアリング（意思疎通、嘘）、トリアージ（判断ミス、注意喚起） 　エスカレーション

- 各段階においてグローバル組織特有の問題が存在する。
- 現地側からの信頼があれば、特にインシデントハンドリングの段階においてリスクを低減できる。よってグローバル組織のＣＳＩＲＴでも信頼関係の構築が重要である。

④　グローバル組織における拠点別の情報セキュリティリスク

グローバル組織の仮定

拠点別の情報セキュリティリスクを考える上で、以下のようなグローバル組織のモデルを想定する。

組織のタイプ	A組織
本拠地	日本（東京）
海外拠点数	100拠点以上
従業員数	2万人
内、現地職員数	1万人
資本金	1000億円
CSIRTのモデル	統合（分散/集中）型CSIRT
M&Aの有無	なし

＊拠点別のリスクを具体的に考える上で、以下の８拠点を代表的に選択した。
アメリカ（ニューヨーク、ロサンゼルス）、英国、ロシア、中国、インド、シンガポール、南アフリカ

拠点別情報セキュリティリスク

海外拠点	規模	現地職員のリテラシー	環境・文化の影響	法律（サイバーセキュリティ）	法律（個人情報保護）	時差
アメリカ（ニューヨーク）	大	高	・日本の思いを通しにくい。既に自社システムが確立。 ・経済合理性で納得しないと共通化しない ・トップダウン方式が日本に当てはまらないため、スピードに差が出る	サイバーセキュリティ情報共有法	包括的な個人情報保護法はなし	-14
アメリカ（ロサンゼルス）	小	高				-17
英国（ロンドン）	大	高		ネットワーク・情報システム規則	GDPR、データ保護法	-9
ロシア（モスクア）	大	低	要調査	包括的なサイバーセキュリティ法はない	個人情報法	-6

＊拠点の規模を大、中、小に分類。（大が１５０人、中が５０人、小が１０人）
大拠点は日本人の専門のIT担当官が存在、
中拠点は日本人がIT業務を他業務と併任。小拠点には現地職員のみ。
GCIの順位を10位以内の場合は、現地職員のリテラシーを高、11以下の場合は低とした。

拠点別情報セキュリティリスク

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

海外拠点	規模	現地職員のリテラシー	環境・文化の影響	法律（サイバーセキュリティ）	法律（個人情報保護）	時差
中国（北京）	大	低	・自宅で持ち帰って仕事を実施する環境 ・現地のセキュリティ意識が低い。 ・IT機器・サービスの調達・仕様の全体最適化が困難 ・セキュリティルール類の整備委が困難。 ・IT利活用のモニタリング、資産管理が困難	中華人民共和国サイバーセキュリティ基本法	中華人民共和国サイバーセキュリティ基本法	-1
インド（デリー）	中	低	要調査	IT法	包括的な個人情報保護法はなし	-3.5
シンガポール	中	高	東南アジアの中ではPC等の現地調達がしやすい環境	サイバーセキュリティ法	個人情報保護法（PDPA）	-1
南アフリカ（ケープタウン）	小	低	要調査	要調査	要調査	-7

代表的なインシデント

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ10大脅威 2019(組織)	現地採用職員リテラシー	IT担当者リテラシー	時差	言語	文化・環境
標的型攻撃による被害	✓			✓	
ビジネスメール詐欺による被害	✓			✓	
ランサムウェアによる被害			✓		✓
サプライチェーンの弱点を悪用した攻撃の高まり					
内部不正による情報漏えい	✓				✓
サービス妨害攻撃によるサービスの停止		✓	✓		
インターネットサービスからの個人情報の摂取		✓	✓		✓
IoT機器の脆弱性の顕在化		✓			✓
脆弱性対策情報の公開に伴う悪用増加		✓			✓
不注意による情報漏えい	✓				✓

第４章まとめ

■グローバル組織を想定して拠点別の情報セキュリティリスクを整理した。

■想定したグローバル組織で代表的なインシデント（情報セキュリ１０大脅威）が発生した場合を考察した。

■１０大脅威のいずれもが海外拠点で発生する可能性が存在し、日本拠点で発生するよりもリスクことが予想される。海外拠点でも文化・環境、言語、時差、従業員のリテラシーによってリスクが変わることが予想される。これらの問題に適切に対処できるCSIRTが求められる。

⑤　全体のまとめと今後の課題

今後の課題

■グローバルCSIRTを構成・運用する際の問題点は整理することができたが、具体的な解決方法、CSIRTの構築・運営方法を提示する必要がある。

■クラウドの活用、AI・機械学習の技術発達など最新動向を踏まえて考える必要がある。