CSIRT の最低要件

萩原健太[†1]　杉浦芳樹[†2]

概要：サイバー攻撃によるセキュリティインシデントの増加に伴い、企業や大学などの組織で CSIRT の設置が進んでいる。しかしながら、CSIRT が期待したレベルで運用できているか疑問を抱えている組織も散見される。また、中小企業などにおいても、インシデント対応体制の構築に関する課題を抱えている。本論文では、CSIRT に関する様々なアンケート結果から、CSIRT の現状や課題、本来の在り方、最低要件を明らかにするものである。

キーワード：セキュリティ，CSIRT，組織

Minimum Requirements of CSIRT

Kenta Hagihara[†1] and Yoshiki Sugiura[†2]

Abstract: Increase of security incidents due to cyber-attack, is progressing the creating of CSIRTs in companies and universities. However, some organizations have doubts as the CSIRT can be operated at the level expected. Also, there are many issues, such as how to build an incident handling capability in small and medium enterprises. In this paper, we clarify the current issue of CSIRT, what CSIRT is and the minimum requirements of CSIRT.

Keywords: Security, CSIRT, Organization

1. はじめに

平成 24 年に情報セキュリティ対策推進会議が発表した『情報セキュリティ対策に関する官民連携の在り方について』や、平成 27 年に経済産業省が発表した『サイバーセキュリティ経営ガイドライン』などを背景に CSIRT（Computer Security Incident Response Team）の設置が進んでいる。

しかし、CSIRT は百社百様と言われ、各組織特有の CSIRT を構築してきたことから、「名ばかり CSIRT」と言われる、実態のない、または質の低い CSIRT まで登場することとなった。

そこで本稿では国内の CSIRT の現状や課題を踏まえながら、国内の CSIRT が健全に構築、運用、発展することを目指し、CSIRT の最低要件をまとめるものである。

2. CSIRT の現状

日本を代表するシーサートコミュニティである日本シーサート協議会の加盟組織数は、平成 26 年には 69 組織であったが、平成 28 年には 173 組織まで増加している。

また（独）情報処理推進機構（IPA）の『CISO や CSIRT に関する実態調査 2017』において CSIRT の現状がまとめられ、CSIRT を設置している組織は 22.6%となっている。米国の 55.6%と比べると半分以下の割合であり、CSIRT の構築がまだ少ない現状である。CSIRT 設置を確認するための同項目では「CSIRT という名称ではないが、インシデント対応を担当する組織がある」といった項目が 44.2%と最も多い割合を占めており、インシデント対応組織が全体で 66.8%の組織で有しているとしている。

さらに CSIRT 等の有効性評価として「期待したレベルを満たしている」と回答しているのは日本が 18.4%に対し、米国は 60.8%、欧州は 45.4%と日本と大きな差が生じている。

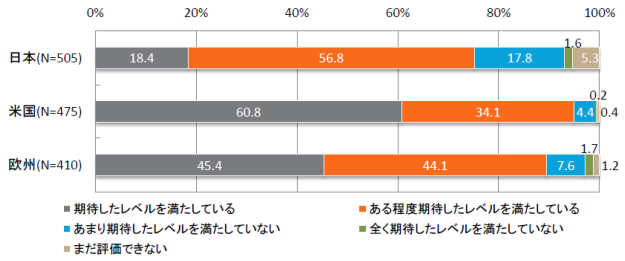

図 1：CSIRT 等の有効性の全体評価

（出典：IPA「CISO や CSIRT に関する実態調査 2017」

図 3.2-52 CSIRT 等の有効性の全体評価）

3. CSIRT の課題

IPA の同報告書における、CSIRT 等の有効性評価が低い理由として、能力・スキル、予算などを質問項目として挙げているが CSIRT の視点で考えるとそれ以前の問題がある。

†1 トレンドマイクロ(株), Trend Micro Incorporated.
†2 NTT データ先端技術(株), NTT Data Intellilink Corporation.

3.1 組織として承認されていない

まずCSIRTを構築する上で欠かせない要素の1つは「経営層の承認」である。これは「Security Incident Management Maturity Model」1の組織モジュールの最初の評価項目にも挙げられている。

国内で経営層の真の承認が得られていない理由は構築段階での「資源」の確保の観点から説明できる。

例えば、設立時は10名未満の体制が8割超であるのに対し、活動開始後はその割合が5割未満と減少している。また予算についても設立時より増加しているのが43.3%と、活動を開始すれば有用性が理解され、ようやく「資源」の拡張につながっている。

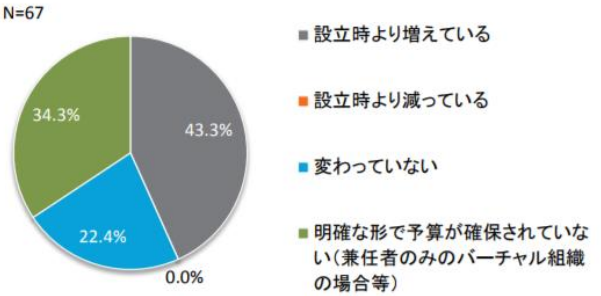

図 2：設立時からの予算増減

(出典：IPA「CISOやCSIRTに関する実態調査2016」

付録1-21 設立時からの予算増減)

予算における課題は「明確な形で予算が確保されていない」といった割合が34.3%となっており、明確な金銭面の資源が確保されていないことも課題であり、組織としての真の承認がされていないと考えられる。

3.2 現業との差別化の難しさ

CSIRTの構築が急速に進んでいるため、ITやセキュリティ知識に富んだ人や組織が構築している傾向が強い。構築の主幹組織となっているのは情報システム部門が48%、セキュリティ対策部門が28%と約8割のCSIRTがITやセキュリティ部門によって構築されていることとなる。

確かに技術的な知識は他部署よりも組織内では高いため、スピード感をもって構築するためには適切な部門ではあるが、部署横断的な連携や現業との差別化という観点からはリスク対策そのものを担う部門や総務部門等の方が適している。

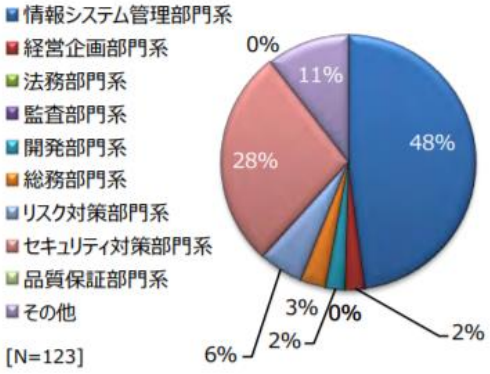

図 3：取り纏め部署

(出典：日本シーサート協議会「加盟組織一覧2016」

図 3：取り纏め部署)

4. そもそもCSIRTとは

4.1 CSIRTの定義

CSIRTとはインシデントに関する様々な対応活動を実施する組織である。日本シーサート協議会によると、「CSIRTとは、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です。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します」2とある。このことからも、ただ単にインシデントが起こった後にインシデント対応を実施するだけではなく、予防やセキュリティ対策など、インシデント対応は多岐に渡る。

「T」はチーム(Team)であるが、過去には「Computer Security Incident Response Capability」という名称が使われていたこともあることから機能で実施すれば良い。CSIRTは消防署や消防団に例えられることもあるが、そのような「団」や「隊」などのチームのイメージ、およびチームで実施することによる協働作業の重要性から、CSIRTという言葉のみが残ったと考える。

4.2 CSIRTの歴史

CSIRTの発祥は1988年まで遡る。この年に「Morrisワーム」と呼ばれる事件が起きた。Morrisはインターネットに接続された多数のコンピュータを利用不能に追い込んだ、世界初のワームと言われている。当時、インターネットにつながっているのは米国軍関係、学術団体、少数の先駆的企業のコンピュータくらいで、世界中数えても6万台ほどである。Morrisワームが麻痺状態にしたコンピュータは約6,000台と考えられ、この事件を契機に世界で初めてのCSIRTであるCERT/CC3が作られた。

1 https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

2 http://www.nca.gr.jp/outline/index.html

3 http://www.cert.org

CERT/CC 設立後、米国はじめ世界各地に CSIRT が誕生したが、CSIRT ごとに活動目的や財政基盤など事情が異なる上、言語の違いや時差もあることから、チーム同士の交流はなかなか進まなかった。

CSIRT 間の連携が行われないうちに、1989 年 10 月には再び大きなインシデントが発生した。今度は「Wank」と呼ばれるワームで、政治的なメッセージを残した初のワームとして知られている。このワーム事件を通して CSIRT 間の連携不足が浮き彫りになり、翌年の 1990 年、CERT/CC が中心となって FIRST（Forum of Incident Response and Security Teams）4を発足させた。

FIRST 設立の背景からも、外部組織との連携が CSIRT の機能のうち重要な役割であることがわかる。

4.3 CSIRT の活動内容

では CSIRT とはどのような活動をする組織なのか。

4.3.1 インシデント対応の流れ

図 4 はインシデント予防から発生までの流れを表したものである。

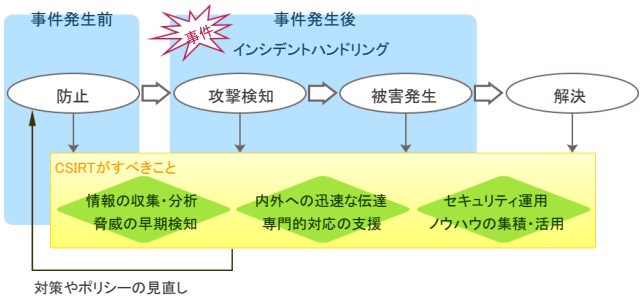

図 4：インシデント発生から対応の流れ

「防止」では、脅威情報などの情報収集・分析によって早期検知を行い、「攻撃検知」した後には早急にインシデントハンドリングを実施し、内外への迅速な伝達などを実施する。検知に留まらず「被害発生」となった場合には、専門的支援を実施し、解決に向けてインシデントハンドリングを継続していく。またインシデントを収束させても終わりではなく、対策やポリシーの見直しなどにつなげていく「解決」の活動も重要である。

また、組織の中における CSIRT の役割は、システム運用者や開発者と経営層の間に入り、技術用語などの通訳者としての役割を担うとともに、他の CSIRT との連携やセキュリティ関連組織との連携も実施する。（図５）

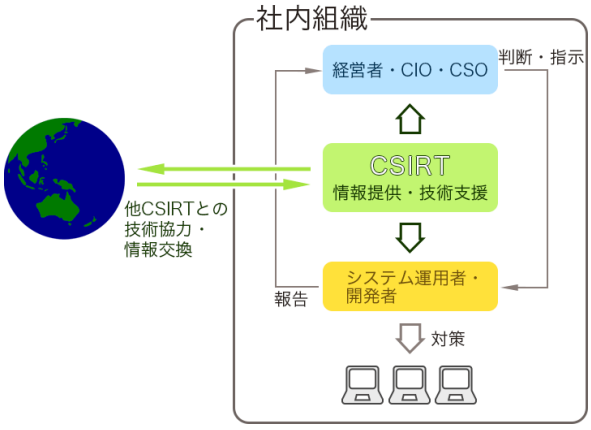

図 5：CSIRT の役割

4.3.2 CSIRT が提供するサービス

CSIRT のサービス(役務)には図 6 に示す通り、大きく３つのカテゴリにわけられる。事前対応型、事後対応型、品質管理である。事後対応型のインシデントハンドリングを実施しない組織はないと思われるが、これらすべてを実施している CSIRT は少ない。組織における CSIRT の使命や目的(Mission)によって、組織で投資できるリソースを鑑み、取捨選択して実施する必要がある。

図 6：CSIRT のサービス5

4.3.3 CSIRT のオペレーション

実際に CSIRT のオペレーションの概要を表現すると図 7 となる。CSIRT が提供する役務(サービス)の対象のことを活動範囲(コンスティチュエンシー)と呼ぶ。

インシデント対応の流れとしてインシデントの報告元を４つ上げているが、CSIRT 自らも公開情報や SNS などの情報を検索し、インシデントの発見に努めている組織もある。

4 FIRST Forum of Incident Response and Security Teams
http://www.first.org/

5 CERT/CC「CSIRT Services」(http://www.cert.org/incident-management/services.cfm)を元に作成。

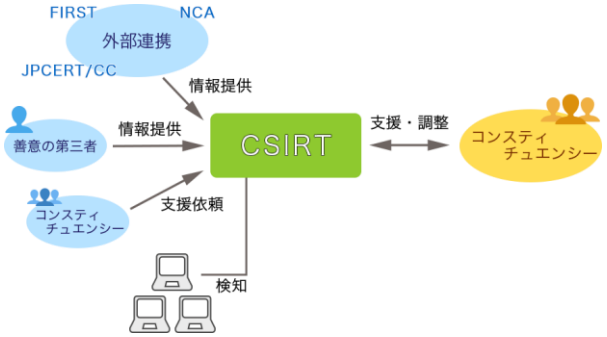

図 7：CSIRT のオペレーション概要

CSIRT は報告を受け付けると「トリアージ」を実施する。トリアージとは緊急医療からの言葉であり、大規模火災や事故などで、患者が大量に運ばれてきた時の治療の優先順位を決める考え方である。サイバーセキュリティの世界では一度に多くのインシデントが発生することは少ない。そのため CSIRT におけるトリアージは重大度や緊急性、担当の割り当てなどを実施することを意味している。

インシデントレスポンスでは、状況把握や対応計画、対応の実施、調整などを解決まで実施することになる。合わせて、常に新しい情報の入手のための活動や、被害の拡大防止や、他の組織やシステムなどでの発生防止を目的に注意喚起などを発出することも必要である。

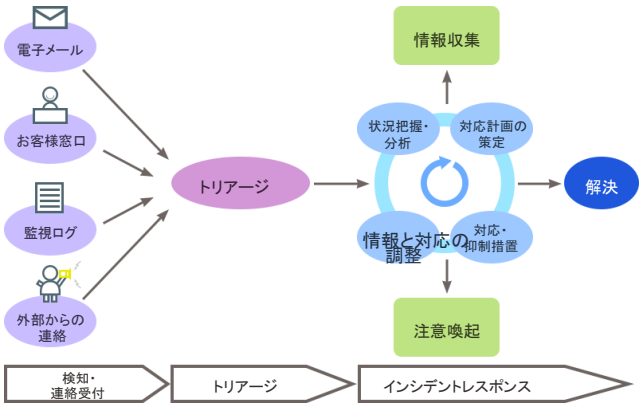

図 8：検知からインシデントレスポンスの流れ

5. CSIRT の最低要件

CSIRT に求められる活動は多岐にわたるため、身の丈に合った機能を設け、適切に CSIRT を構築しないと CSIRT は破綻する。

まず重要なことは「何のための CSIRT」であるのか、また「誰のための CSIRT であるのか」など、そもそも CSIRT が組織に必要な理由を明確にするために、さらには自組織の CSIRT が経営層から真の承認を得るために「使命（Mission）」「役務（Service）」「活動範囲（Constituency）」の 3 要素を定義づけることが重要である。

さらに CSIRT は組織内外の連携を欠かすことができない。そこで組織内部や組織内外の連携、経営層との橋渡しになる「窓口」が重要となる。より多くの情報を集め、連携や橋渡しを行う上で「信頼」という要素は欠かすことができない。信頼を得るために先に問うべきは技術力ではなく、信頼を構築できる「コミュニケーション能力」こそ、窓口の機能に求めるべきである。つまり「信頼できる窓口」（CSIRT では Point of Contact という）を構築することも CSIRT の最低要件の 1 つと言える。

そしてこの 2 つの要件を兼ね備え「経営層の真の承認」を得ることが最後の要件と言える。承認があればこそ資源の確保や普段の活動を行うことができ、インシデントが発生した際も慌てず冷静に対応することが出来る。

また、3 要素を明確に定義するためには、組織における資産（守るべき対象）の明確化や、資産に対する脅威へのリスク分析が行われていると 3 つの最低要件は容易に準備することが可能であると考える。

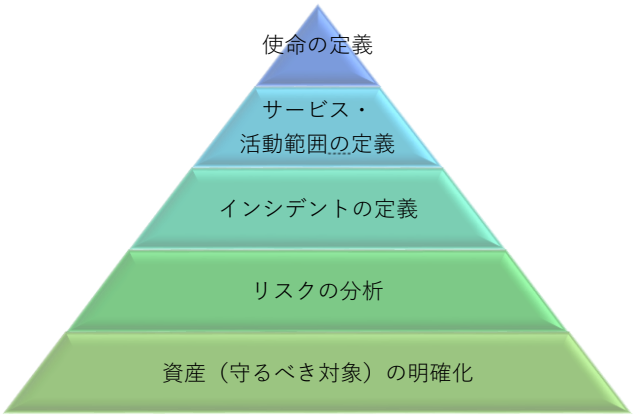

図 9：CSIRT 構築の階層

6. おわりに

本稿では CSIRT の現状や課題、CSIRT の活動についてまとめ、CSIRT の最低要件を明らかにした。CSIRT 構築は決して大規模な組織だけが構築するものではなく、サイバー空間と向き合う組織すべてにおいて必要であり、構築可能であると考える。

「3 要素」「（信頼できる）窓口」「経営層の（真の）承認」を軸に組織規模関係なく、検討を開始することが CSIRT 構築への第一歩となり、この 3 つの要件がサイバー空間と向き合う組織の一助となることは間違いないであろう。

参考文献

(独)情報処理推進機構「企業の CISO や CSIRT に関する実態調査 2017」

https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html

(独)情報処理推進機構「企業の CISO や CSIRT に関する実態調査 2016」

https://www.ipa.go.jp/security/fy27/reports/ciso-csirt/index.html

一般社団法人 JPCERT コーディネーションセンター「CSIRT マテリアル」

http://www.jpcert.or.jp/csirt_material/

日本シーサート協議会 「CSIRT スターターキット」

http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

日本シーサート協議会 「What's CSIRT」

http://www.nca.gr.jp/imgs/CSIRT.pdf

日本シーサート協議会 「加盟組織一覧 2016」

http://www.nca.gr.jp/imgs/nca_teams_2016.pdf

CERT/CC 「CSIRT Services」

http://www.cert.org/incident-management/services.cfm?

SIM3 Security Incident Management Maturity Model

https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

FIRST Forum of Incident Response and Security Teams

http://www.first.org/