O-040

国内組織における CSIRT 構築と運用に関する調査
Survey on Maturity Level of CSIRTs in Japanese Organizations

松田 亘† 青木 翔† 満永 拓邦‡ 洞田 慎一†
Wataru Matsuda Sho Aoki Takuho Mitsunaga Shinichi Horata

1. はじめに

標的型攻撃など昨今のサイバーセキュリティを取り巻く環境の変化は、国内の多くの組織における CSIRT (Computer Security Incident Response Team) の構築の必要性を高めていると考えられる。日本シーサート協議会 (NCA) においても、2015 年だけで 37 チーム の CSIRT が加盟し、参加 CSIRT は合計 106 チームとなった[1]。NCA に加盟していない CSIRT や、組織内でインシデント対応をすることになってはいるが CSIRT と名乗っていない緊急対応体制などを加えれば、国内の多数の組織で、何らかの取組がなされている。CSIRT 構築の動きや議論は、現在もなお進行しており、今後も CSIRT を構築する組織は増加すると考えられる。

NCA には、様々な業種、規模の組織が属している。JPCERT/CC では、それらの CSIRT における個別具体的な事例が、同業種や同規模の組織において、CSIRT を構築・運用する際の大きな参考となるのではないかと考え、2015 年度に「CSIRT 構築および運用における実態調査」として、CSIRT の構築・運用を行っている 66 の CSIRT に対して、アンケートやインタビューを実施し、CSIRT の多様な実像と課題や方向性を明らかにすることを試みた。この結果は、JPCERT/CC の Web サイトでの公開を予定している。本論文では、その概要を示す。

2. CSIRT 構築と運用調査

2.1 調査方法

CSIRT の組織体制や、メンバー構成、ポリシー整備についてアンケートと評価を行った。アンケート項目は、CSIRT の成熟度モデルである Security Incident Management Maturity Model (SIM3) [2] を参考に、独自に作成した。調査対象は、NCA メンバーであり、アンケートへの協力に応じた CSIRT である。

多数の組織に対するアンケートに加え、各種業界を牽引している主だった CSIRT に対してインタビューを行い、各組織の取組状況や課題についてヒアリングを実施し、取組や課題などの定性的な評価も併せて実施している。

2.2 調査結果と考察

SIM3 では、CSIRT サービス*[1][3]に関連する定義の文書化や CSIRT 活動報告体制、組織内外との情報連携が取り上げられている。本調査では、さまざまな項目について質問したが、ここでは、組織における CSIRT の役割を論ずる上で重要な示唆を与える「CSIRT における文書の重要性」、「CSIRT 活動を発信する重要性」、「CSIRT における連絡窓口の重要性」について、それぞれの調査結果の概要を紹介する。

2.2.1 CSIRT における文書化の重要性

組織における CSIRT の役割について調査するために、CSIRT サービス対象者や権限、サービス内容、インシデントについてアンケートを行った。当然、組織によって、事業内容や部門構成、想定しているリスクなどは異なるが、CSIRT の役割をどの程度まで文書化しているかは、組織が考えている CSIRT の重要性を示す尺度として重要と考えられる。

アンケートの結果から、全体の約 6 割の組織で、CSIRT の役割が文書化されていた（図 1 参照）。また、組織における情報セキュリティ対策方針や行動指針であるセキュリティポリシーに関しては、8 割を超える CSIRT が経営陣に承認を受けていると回答している。

これらのことから、多くの組織で、CSIRT の体制やポリシーに関する定義が文書化され、経営陣の承認を得て、組織の方針として活動していることがわかる。文書化により、想定リスクに対し、組織が責任を持って対応すること、また CSIRT がどのような役割を果たすべきかを公言していると考えられる。さらには、インシデント対応や、体制の見直しなど、組織で CSIRT 活動を効果的に推進することに繋がる。

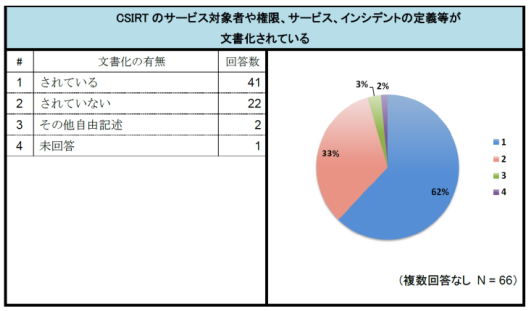

図 1 CSIRT サービスに関する定義の文書化

2.2.2 CSIRT 活動を発信する重要性

一方で、CSIRT や情報システム部門など、情報やセキュリティに関わる部門は、費用対効果が見えづらく、組織においてコストだけがかかる部門と認識されてしまうこともある。組織全体に向けて、活動の成果を発信することは、コストの妥当性の認知だけでなく、組織からの信頼を得ることに繋がると考えられる。従って、CSIRT の活動成果を他の部門に向けて発信することが、活動を円滑に進める上で重要であると考えて調査項目に加えた。

アンケート結果からは、CSIRT の活動について、約半数の CSIRT で経営陣を含む情報セキュリティ委員会などへの定期的な活動報告の体制が定められていた（図 2 参照）。

*[1] CSIRT サービス：CSIRT が行うインシデントレスポンスの具体的内容

また、約半数の CSIRT が定期的にレポートを発行していることもわかっている。レポートには、特定の関連部署を対象としたものの他、社内全体に向けて広く情報を共有している例もあった。個別に実施したインタビューからは、CSIRT 活動を社内的に評価する基準について悩んでいるとの声もあった。

これらの結果から、CSIRT が組織にとって有益であり、有効な投資であることを如何に組織全体のコンセンサスとするかが、課題として認識されていることが推測される。その解決策の 1 つとして、活動成果の情報発信に力を注いでいる CSIRT もあれば、事前にリスク評価を行い、組織のインシデント対応コストをどの程度低減できたかを評価するなどの方法で、活動成果の「数値化」を推進している CSIRT もあった。

経営層(あるいは経営層を含む情報セキュリティ委員会等)に CSIRT 活動について定期的に報告を行う体制が定められているか

#	定義や文書の有無	回答数
1	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	7
2	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	19
3	明確に設定され、文書として存在しているが、正式に承認されていない	5
4	だいたいの目安になるものは設定されているが、文書として存在していない	18
5	設定されておらず、発生の都度検討している	13
6	未回答	4

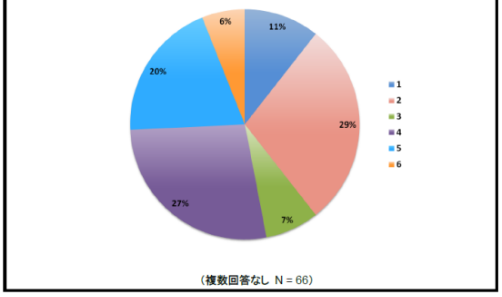

図 2　経営陣を含むセキュリティ委員会などへ CSIRT 活動についての定期報告を行う体制の整備

2.2.3 CSIRT における連絡窓口の重要性

CSIRT 機能の 1 つに、連絡窓口 (Point of Contact) を挙げることができる。NCA では、連絡窓口の明確化を加盟条件に含めている。

CSIRT はインシデント発見などの外部通報を受けて対応することもあるが、その際にも連絡窓口が重要な役割を担う。アンケートの結果によれば、外部の組織から通知を受け取ったことのある CSIRT は 7 割以上あった。また、外部の組織が展開するサイバー攻撃に関する情報共有の枠組みに参加している CSIRT も多く見られる（図 3 参照）。

サイバー攻撃に関する情報共有の枠組みに参加しているか

#	情報共有の枠組み	回答数
1	IPA(J-CSIP)	8
2	金融 ISAC(各種ワーキンググループ)	11
3	警察庁(CCI)	13
4	JPCERT/CC(WAISE)	32
5	その他自由記述	9

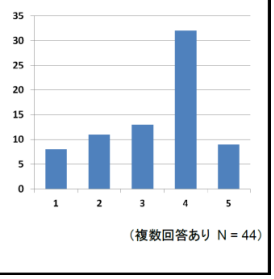

図 3 サイバー攻撃に関する情報共有の枠組みへの参加

3. おわりに

多くの組織で、CSIRT の構築やその運用が進むなか、CSIRT の成熟度について悩む組織は多いと考えている。JPCERT/CC が実施した調査の結果は、あくまでも一つの側面でしかないが、国内の CSIRT の実態について検討する上での示唆を含んでいるものと考えている。

インシデント対応体制を持つということは、組織に対する脅威を認識し、脅威を受ける可能性やその被害を極小化することに責任を持つための第一歩である。CSIRT の提供するサービスを内製するか外部委託するかに関わらず、どのような責任がどこにあるのかを明確にした上で、それぞれの責任を組織や CSIRT が全うしなければならない。そのため、組織内の業務と、CSIRT が対応すべき範囲を把握した上で、CSIRT の構築・運用に着手することが望まれる。

また、緊急時における情報共有や対応に際して、CSIRT やそれに準ずる機能について、関係部署からの理解が得られず、緊急時対応に窮するといったことも考えられる。今回インタビューした CSIRT でも同様の問題を抱えていた。ヒアリング結果などを総合すると、CSIRT の運用実績や演習などの訓練を積み重ね、組織内に共有することで、強固な信頼関係を構築することが解決に向けた方策の 1 つである。

アンケート結果からは、多くの CSIRT で連絡窓口機能を重視していることが読み取れる。加えてインタビューなど実際の声を聞いてみると、NCA をはじめとするコミュニティに参加し、他組織とインシデント対応事例を共有し、技術に関して積極的に意見を交わすなどして、自組織におけるインシデント対応について見直しを図っている。

連絡窓口の担当者は、組織内外との連携が求められ、円滑なコミュニケーションが図れる人物が適切であると考えられる。連絡窓口として、活動を進める中で周囲からの信頼を獲得していくことで、さらに情報収集のアンテナを広げることが可能になり、CSIRT 活動の活性化に繋がると考えられる。

組織全体から認められ、尊重される CSIRT への成長は、一朝一夕にはいかず、組織内外で活動しつつ、技術や経験知を CSIRT に蓄積する必要がある。まずは、類似業種で同規模の組織に設置された CSIRT を参考に、スモールスタートで無理のない範囲から CSIRT の構築を始め、段階を踏んで成熟した CSIRT に成長することを呼び掛けたい。

謝辞

本調査におけるアンケートやインタビューにご協力くださった NCA および CSIRT の皆様に厚く感謝申し上げます。

参考文献

[1] 日本シーサート協議会, http://www.nca.gr.jp/member.
[2] Don Stikvoort, SIM3:Security Incident Management Maturity, 1 September 2010.
[3] 日本シーサート協議会, CSIRT スタータキット Ver 2.0

† JPCERT コーディネーションセンター, Japan Computer Emergency Response Team Coordination Center
‡ 東京大学情報学環 セキュア情報化社会研究グループ, The University of Tokyo, Secure information society research group