ＭＩＧＡコラム
「世界診断」

2014 年 9 月 24 日

日本における CSIRT をめぐる現況

山 賀 正 人

明治大学研究･知財戦略機構 客員研究員
日本シーサート協議会 専門委員

千葉大学の助手を経て、2001 年から JPCERT コーディネーションセンターに勤務し、情報セキュリティを専門とするようになる。その後、2006 年にフリーランスとなり、CSIRT 研究家、ライター、コンサルタントとして活動している。

昨今の複雑且つ高度化するサイバー攻撃による被害が連日のようにメディアで取り上げられる中、サイバー攻撃に対応するための組織横断の専門チーム CSIRT（シーサート、Computer Security Incident Response Team）を設置する企業や組織が増えてきている。実際に、2013 年 3 月には各府省庁への CSIRT 設置が完了した他、政府から各企業に対して CSIRT の設置が呼びかけられている。また、日本国内の CSIRT のコミュニティとして 2007 年に設立された日本シーサート協議会（以降、NCA と略）への加盟チーム数は急速に伸びており、2014 年 9 月時点の加盟チーム 61 のうち半分以上がこの 2 年間に加盟したチームである。

このように CSIRT が増えて行き、知名度が上がった一方で、CSIRT についての正しい知識が適切に伝わっておらず、間違った「イメージ」で捉えられているケースも散見されるようになった。そこで本稿では、CSIRT とはそもそも何であり、どうあるべきかを紹介する。また最後に、CSIRT に限らず、企業や組織の情報セキュリティ対策における今後の課題についても言及する。

(1) CSIRT の歴史

CSIRT の歴史は 1988 年に遡る。1988 年 11 月、世界初のワーム（自己増殖機能のあるコンピュータウイルス）「モリス・ワーム」が発生し、世界中の数千台のコンピュータを使用不能な状態に陥らせた。当時は、インターネットの利用者はもちろん、システムやネットワークの管理者もこのよう

な事態が発生することを全く想定していなかったため、原因だけでなく、そもそも何が起こっているのかということすら分からない状況が続き、結果として被害が世界中に拡散したのである。この事態を重く見た米国国防高等研究計画局（DARPA）はペンシルバニア州ピッツバーグにあるカーネギーメロン大学ソフトウェア工学研究所内に、インターネット・セキュリティに関する情報収集と分析、および情報発信を行う専門の機関として CERT/CC（CERT Coordination Center）を設置した。これが世界最初の CSIRT である。因みに CERT は CERT/CC の登録商標であり、一般名詞としては CSIRT を用いる。

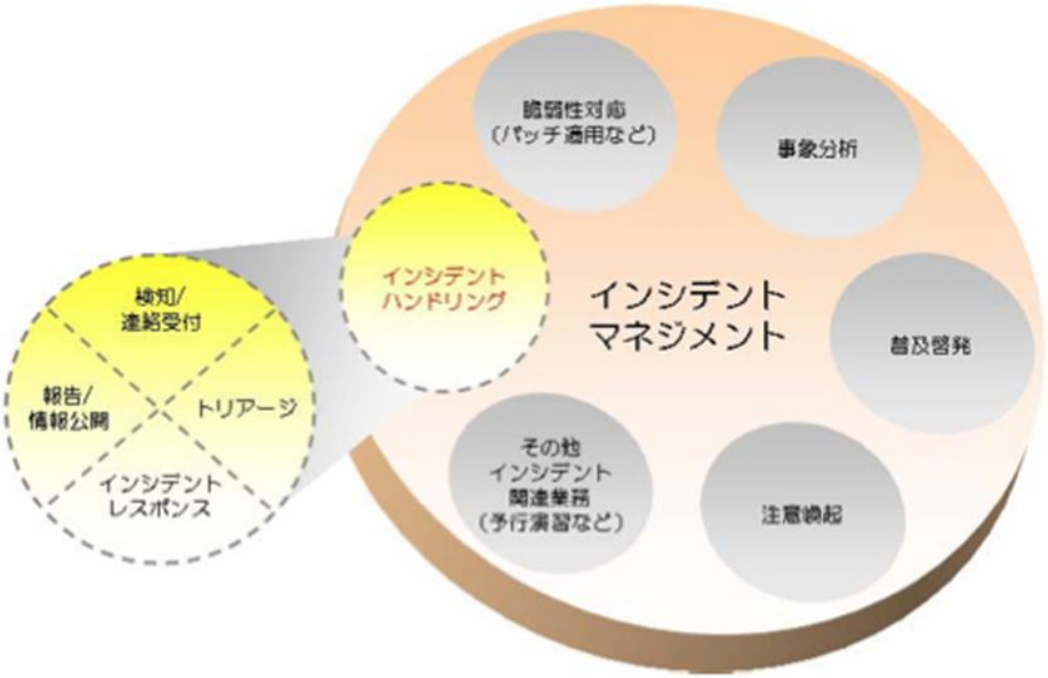
その後、米国内の政府機関や企業をはじめ、ヨーロッパにも同様の組織が作られるようになったことを受け、1990 年に CSIRT による国際的なコミュニティ FIRST（Forum of Incident Response and Security Teams）が設立された。2014 年 9 月現在、FIRST には世界 66 の国や地域から 305 チームが加盟しており、日本からも 23 チームが加盟している。

一方、日本では 1990 年代初頭にはじまるボランティアベースの活動をもとに、日本初の CSIRT として JPCERT/CC（JPCERT Coordination Center）が 1996 年 10 月に正式に発足、1998 年に日本の CSIRT として初めて FIRST に正式加盟している。

その後、日本でも企業を中心に CSIRT が作られるようになり、相互の連携強化を図る目的で、FIRST の日本版ともいうべき日本シーサート協議会（NCA）が 2007 年 3 月に設立された。

(2) CSIRT とは

企業や組織内で発生した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）に効果的且つ効率的に対応するためには、事故を完全に防ぐことはできないという「事故前提」の考えに基づき、自組織内で発生したインシデントに限らず、世の中で発生したインシデントに関する情報を集約・蓄積し、場当たり的ではない包括的な対策を検討・実施する「インシデント・マネージメント」が必要である。CSIRT はこのインシデント・マネージメントの中核を担うものである。ただし、あくまで中核を担うものであり、インシデント・マネージメントの全てを CSIRT が担う必要はない。



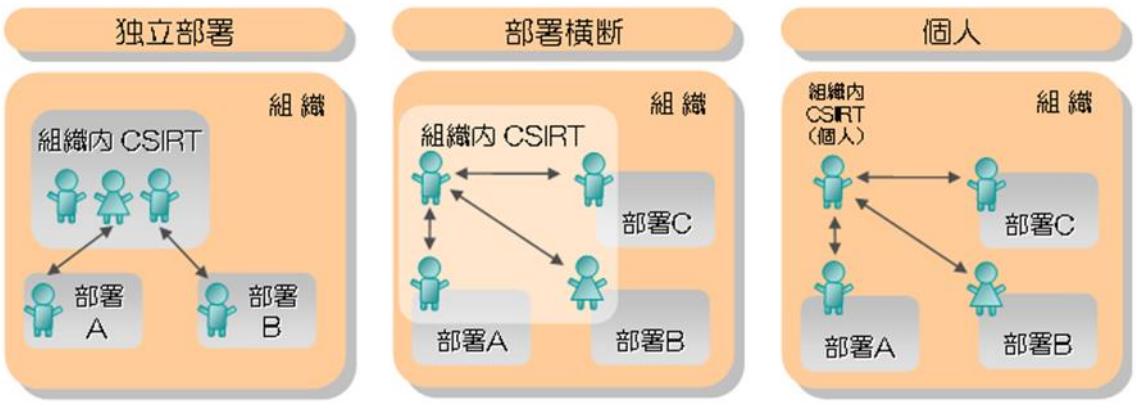
出典：JPCERT/CC インシデントハンドリングマニュアル

https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0.pdf

(3)　CSIRT に対する誤解

(3-1) CSIRT は専門部署?

CSIRT の T が Team であることから、部署でなければならないと考えている人がいる。しかし、これは大きな間違いである。実は 10 数年前までは CSIRT とは別に CSIRC (Computer Security Incident Response Capability) という言葉も使われていたのだが、現在では CSIRC の意味を含めて CSIRT と呼ぶのが一般的である。このことが示すように、CSIRT は専門部署でなくてもよく、「機能」として有していればよいのである。実際に多くの CSIRT は組織内の関係する部署のメンバーからなる「仮想チーム」の形態をとっている。専門部署の CSIRT を消防署に喩えるならば、仮想チームの CSIRT は消防団であり、そのメンバーは、普段は別の仕事をしているが、インシデント発生時など必要に応じて CSIRT のメンバーとして活動するというものである。



出典：JPCERT/CC「CSIRT ガイド」

http://www.jpcert.or.jp/csirt_material/files/guide_ver1.0.pdf

(3-2) 情報セキュリティ対応体制があればCSIRTは不要?

既に充分な情報セキュリティ対応体制があるので、CSIRTをわざわざ作る必要がないという声を耳にすることがある。確かに、充分に機能する体制があれば、CSIRTがなくても、問題ないように見える。しかし、それでもなおCSIRTが必要なのには理由がある。それは、自社単独では対応できないインシデントが増えているからである。

例えば、近年多く見られる攻撃手法として、特定の企業や組織を狙った「標的型攻撃」というものがある。これは実在の取引相手などの関係者を装った電子メールをターゲットに送り付け、相手を信用させた上で添付ファイルを開かせるなどの方法でウイルスに感染させるというものである。ところが、このような攻撃に関しては、ターゲットが特定の企業や組織に限定されているために、具体的な情報が公になることがほとんどない。そのため、攻撃に関する情報が他の企業や組織に伝わらず、結果として同様の被害を生み続けてしまうのである。

また他にも「リスト型攻撃」というものがある。これは何らかのサイトから何らかの形で漏れたIDとパスワードの組み合わせ一覧をもとに、攻撃者が別のサイトにログインし、アカウントを乗っ取るというものである。最近ではLINEのアカウント乗っ取りが一般のメディアでも大きく取り上げられている。

これらの攻撃に対応するためには、公になっている情報だけでは不充分であり、個々の企業や組織の間の「信頼に基づく情報交換」が必須である。このような「信頼に基づく情報交換」を実現するための枠組みとして既にグローバル・スタンダードになっているのがCSIRTであり、「CSIRTであること」は即ち、他のCSIRTと信頼関係を結んで情報交換ができることを意味する。極端な言い方をすれば、CSIRTを名乗り、CSIRTのコミュニティに加わり、「信頼」に基づいて他のCSIRTと情報交換することができれば、それだけでCSIRTと言えるのである。

(3-3) CSIRTは事後対応だけすればいい?

「CSIRTは事後対応のみを行うものである」という誤解もある。確かに、CSIRTが最も活躍しているように見えるのはインシデント発生後であるが、CSIRTの活動はそれだけではない。先ほど述べた「インシデント・マネージメント」には、使用しているソフトウェアやハードウェアの脆弱性対策（パッチ適用など)、利用者に対する注意喚起、普及啓発、更には予行演習など、事前の対応も含まれている。CSIRTはこれらの全てを担う必要はないが、事後対応を円滑に行い、被害を最小化するためには、このような事前の対応も欠かすことはできないのである。

(3-4) CSIRTははじめから完璧でなければいけない?

CSIRTの知名度が上がる中で最近になって見られるようになった誤解としては、CSIRTを最初から完璧な形で作ろうとしてしまうというものである。セキュリティを扱う以上、抜けや漏れがあっては

いけない、だから完璧なものを作らなければいけないという気持ちは理解できるが、それではいつまでたっても「使える CSIRT」は作れない。

例えば、海外に拠点のある企業、中でも海外の企業を買収したケースや、現地採用のスタッフが多数を占めているケースは、文化の違いもあり、日本国内と同様な形での体制を導入するのは難しい。ではそのような企業が実際にはどうしているかと言うと、多くの場合、まず日本国内での体制を整備して CSIRT の活動を開始、その実績を踏まえ、地道且つ丁寧な説明と調整を経て、徐々に CSIRT の対象範囲を広げて行っているのである。要はできるところから始めればいいのである。

いくら組織体制上「美しい」「理想的な」ものを、内部からの反発を無視して強引に作っても、内部から信頼されず、協力もされない、つまり「使えない（＝機能しない)」ものでは意味がない。まずは体制上「美しくない」「理想的でない」ものであっても、「使える（＝機能する)」CSIRT を作って活動実績を積むことこそが大事である。そのような実績があれば、その後の調整がスムースに進むことは明らかであろう。

(3-5) 外部の専門業者に任せれば CSIRT は不要?

近年の複雑・巧妙化したインシデントが発生した場合、その影響範囲や原因の特定には高度に専門的な知識に基づいた分析が必要とされることが多い。この機能を（IT を主たる業としない）一般企業が自前で持つのは現実的ではなく、外部のセキュリティ専門業者に依頼するのが望ましい。しかし、企業の中には外部の専門業者に「丸投げ」してしまい、本来企業側に必要な「意思決定」すらも、外部に任せてしまうケースがあるのだ。これは大変な間違いである。

セキュリティ専門業者は技術的に正しいことは言えるが、技術的に正しいことがその会社や組織にとって、例えば経営的な面から見ても正しいとは限らない。時間を充分にかけて影響範囲や原因の究明を行うのが技術的に正しいことは確かだが、時間をかけるということは即ち様々なコストがかかるということであり、状況によっては技術的分析作業よりも復旧を優先するという判断があってもいい。それを「絶対に間違っている」と言うことなどできないだろう。

このような組織全体を見て「正しい」つまり「最適」な対応を取るための判断は外部の業者にはできない。できるわけがないのだ。そのような判断は内部の人間がするのは当たり前のことである。ところが、実際にはその当たり前のことができない企業が珍しくないのである。

このような意思決定の権限（の一部）を CSIRT に持たせるケースもあるが、多くの場合、CSIRT は意思決定をする権限を持つ人や部署に対して必要な情報を提供して意思決定を促す役目を担う。CSIRT とは現場と意思決定をする者との間の「通訳」の役目を果たすものなのである。

(4)　企業や組織における情報セキュリティ対策の今後の課題

CSIRT が活動する上で現在抱えている課題は少なくない。特に深刻なのは人材である。これから CSIRT を作ろうとしている企業や組織にとって、どのような人材を配置すればよいのかは難しい課題であるが、実は既に活動している CSIRT にとっても深刻な問題なのである。

多くの CSIRT は、CSIRT 構築時のキーパーソンがまだ現役で現場にいるケースが多く、そのため、CSIRT の活動に対するメンバーの意識やモチベーションも比較的高い状態を維持できている。しかし、多くの日本企業では定期的な人事異動がある上、年月がたてば、当然のように「引退」もやってくる。また、今の時代であれば転職による離職も珍しくない。その場合にも同じだけの人材・人員を確保できるのか、また確保できたとしても、同じように高い意識やモチベーションを維持できるのかという問題がある。

もう 1 点は地域格差である。既に述べたように、CSIRT の活動において外部の専門業者の活用は重要であるが、首都圏以外ではそもそも専門業者の選択肢が極端に少なく、万が一の事態に「電話一本ですぐかけつける」という状況はまず期待できない。そのため、自前で何とかしようと試行錯誤してしまい、結果的に調査分析に必要な情報をすべて失ってしまう可能性・危険性もある。

上記 2 点について現時点で明確な解はないが、解決に向けた動きが何もないわけではなく、また成功事例も全くないというわけではない。今後はそのような成功事例をもとに、ある程度の一般化を図ることを考えている。今後も CSIRT と CSIRT コミュニティの動向には注目してもらいたい。

参考文献

日本コンピュータセキュリティインシデント対応チーム協議会（日本シーサート協議会）
http://www.nca.gr.jp/

JPCERT Coordination Center
https://www.jpcert.or.jp/

CSIRT 奮闘記
http://itpro.nikkeibp.co.jp/article/COLUMN/20091120/340847/

CSIRT をめぐる 5 つの誤解
http://www.atmarkit.co.jp/ait/articles/1406/12/news002.html