CSIRT小史

v1.0

一般社団法人 日本シーサート協議会
2025年10月9日

連絡先:https://www.nca.gr.jp/contact/index.html

本文書の取り扱いは**TLP:CLEAR**でお願いします。TLPについては次を参照してください。

FIRST: TLP Standards Definitions and Usage Guidance - Version 2.0
https://www.first.org/tlp/docs/v2/tlp-v2_ja.pdf （日本語版）

はじめに

CSIRTが世界で初めて誕生したのは今から40年近く前のことです。この40年という歳月は、「歴史」としてくくるには短かすぎる時間かもしれません。しかし、めまぐるしく変化するサイバー世界にある時は歩調を合わせ、ある時はさきがけて、CSIRTも変化しながら足跡を印し続けています。これからお話しする事柄はそのCSIRTの歴史の一部に過ぎませんが、みなさんが今後CSIRT/PSIRTを構築、あるいは運用される際の一助になれば幸いです。正確さよりも読みやすさを優先したため、推測による記述がしばしば含まれる点をご了承ください。

CSIRT先史

1988年11月、インターネットをモリスワームが襲いました。世界で初めてのインターネットワームでした。このワームによって、世界中の6,000台のコンピュータがダウンさせられたといわれています。今となっては「たかが6,000台」ですが、当時のインターネットはその程度の規模でした。なお、日本にはモリスワームの影響はなかったとされていますが、いくつかのマシンがダウンしたという説もあります。

公平を保つために少し触れておくと、モリスワームは悪意を持って作られたのではありません。アメリカのコーネル大学の学生、ロバート・T・モリスが単なる知的実験としてワームを作ったのですが、拡散の仕組みに制限などを設けなかったことから、結果としてDDoS攻撃を引き起こしてしまったようです。このワームはUNIXのsendmailやFingerプロトコルなどにあった脆弱性や、推測しやすいパスワードを利用するといった、現在のワームと同じような機能を備えていました。

CSIRTの夜明け

1988年11月、米国・カーネギーメロン大学のSEIにCERT/CCが設立されました。世界初のCSIRTの誕生です。CERT/CCは上述のモリスワーム事件をきっかけに作られたといわれています。しかし、モリスワームがインターネット上に放たれたのは1988年11月2日であり、CERT/CC設立も同年同月なので、これは俗説かもしれません。ただ、確実に言えるのは、モリスワーム事件をきっかけに、インターネットのセキュリティやインシデント対応への意識が一気に高まった、ということです。結果、主に米国でCSIRTが次々と作られました。

礎の時代

CSIRTが一つ、また一つと増えるに従って、CSIRT同士の協力や連携の枠組みが必要だと考えられるようになりました。そして、モリスワー ム事件から2年経った1990年、セキュリティチームの世界的なコミュニティであるFIRSTが誕生しました。

https://www.first.org/about/history

FIRST設立の前年の1989年にはWANKワーム事件が発生しています。WANKは政治的なメッセージが込められた初のワームといわれています。このワーム事件を機にFIRSTが作られたという説もあります。

FIRSTの活動開始と、その後10年ほどの間に起きたいくつかの出来事は、CSIRTが展開していくための礎（いしずえ）や契機になった、と言っても過言ではないでしょう。まず、CSIRTにとって活動の指針となる重要な文書が2点、相次いで公開されました。

1998年6月、IETFがRFC2350:Expectations for Computer Security Incidentを公開しました。

https://tools.ietf.org/html/rfc2350
https://www.nic.ad.jp/ja/tech/ipa/RFC2350JA.html

同年12月には、CSIRTのバイブルともいえる”CSIRT Handbook”がCERT/CCから公開されました。次は2003年4月に公開された最新版の第2版です。

Handbook for Computer Security Incident Response Teams (CSIRTs)

https://insights.sei.cmu.edu/documents/1606/2003_002_001_14102.pdf

JPCERT/CCが日本語訳を公開しています。

『コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック』

https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf

また、既存、新設にかかわらず、CSIRTの活動は非常に活発でした。米国のみならずヨーロッパでもCSIRT活動はさかんで、EuroCERTがヨーロッパのCSIRTを束ねていました（EuroCERTは2001年ごろ活動終了）。世界中のアンダーグラウンドのコミュニティやBotnetといったダークネットを観察し、報告しているCSIRTもありました。

当時もしばしばソフトウェア製品の脆弱性が原因となってインシデントが起きました。自社製品の脆弱性に対処しなくては、とベンダー各社が危機感を募らせ、PSIRTが作られ始めました。レッドコード・ワーム事件が起きたのはちょうどその頃、2001年のことです。レッドコードは中国のハッカーグループが作成したワームで、マイクロソフト社のIISサーバーの脆弱性を悪用して拡散しました。約60万台のサーバーに感染して、数億ドルに上る被害をもたらしたといわれています。このワーム事件はソフトウェアベンダーに対し、脆弱性の発見や修正の重大さを再認識させました。マイクロソフト社のPSIRTはじめ、ベンター各社のPSIRT活動が目立ってきたのもこの頃です。

初めて設立されたPSIRTがどのベンダーのチームなのか諸説があり、はっきりしたことはわかりませんが、シスコシステムズ社のPSIRTはごく初期から活動していました。1999年の設立以来、Cisco PSIRTは製品のセキュリティ問題に対処し、脆弱性情報を公開してきました。その活動は他の企業がPSIRTを立ち上げる際のモデルとなるなど、業界全体に影響を与えています。

さて、2003年9月、米国にUS-CERTが設立されました。

United States Computer Emergency Readiness Team

https://www.us-cert.gov/

US-CERTは米国国土安全保障省の国家サイバーセキュリティ部門（National Cyber Security Division。略称NCSD）の実働部隊として、注意喚起の配信などCERT/CCの機能を一部引き継いでいます。

面白いのは名称に”Readiness”という語を用いている点です。US-CERTは「Computer Emergency Response Teamではない」と言っていますが、それはつまり、「CERT/CCやCSIRTは緊急対応組織ではない」という主張なのでしょう。一般的

にCSIRTに対し、警察や消防のように電話1本ですぐに駆けつけてくれるという誤解があるため、“Response”（対応）ではなく”Readiness”（備えること、準備）を採用したのではないかと推測しています。

ResponseからReadinessに変わった点、このころからResilienceという言葉も聞くようになりました。これは一つのCSIRTという枠組みが、まさしく組織のResilienceをたかめるという役割であったと感じます。

このセクションの最後の話になりますが、少し遡ること1999年、Melissa（メリッサ）による事件が発生しました。Melissaは、電子メールの添付ファイルを開くことによって感染する初のコンピュータウイルスです。この事件がきっかけになって、CSIRTはソーシャルエンジニアリング攻撃を強く意識するようになったといわれています。

それではこのあとしばらく、日本に注目してみたいと思います。

90年代の日本のCSIRT

世界のあちこちにCSIRTが立ち上がり活動していた90年代、日本はどんな様子だったのでしょうか。

4年間のボランティア活動を経て、1996年10月、JPCERT/CCが設立されました。日本で最初のCSIRTの誕生です。2年後の1998年には、日本で初めてのチームとしてFIRSTに加盟しました。一方、1998年4月、日立グループは研究プロジェクトとして企業初のCSIRTを発足させました（現・HIRT）。同グループのチーム設立は、日本の民間企業におけるコンピュータセキュリティへの開眼と言えるでしょう。

この2チーム以外にも、IIJ-SECTやJSOC（現・LACERT）などが活動していましたが、CSIRTを運営する組織はごくわずかでした。そして、インシデントが発生しても組織全体で対応する所は限られていました。また、日本は経済規模が大きいにも関わらず、数年の間FIRST加盟チームがJPCERT/CCのみだったことから、海外のCSIRTから「日本は加盟チームが少ないね」と寂しがられることもあったそうです。

日本のCSIRTの躍進

数の上では出遅れ気味だった日本のCSIRTでしたが、新しい世紀に入って間もなく、国内外の事件や事象、あるいは政府の施策をきっかけにCSIRTに対する認識が深まり、CSIRTを運営する組織が増えていきました。また、特に2002年の日本には、CSIRTやセキュリティコミュニティに関する大きな出来事が続きました。その中から3つ挙げましょう。

まず、3月、JPCERT/CCによってAPSIRC（Asia Pacific Security Incident Response Coordination Conference）が東京で開催されました。これを機に、翌年2月にはアジア地域の国際連携CSIRTの集合体であるAPCERTが設立されました（Asia Pacific Computer Emergency Response Team。日本語名「アジア太平洋コンピュータ緊急対応チーム」）。

https://www.apcert.org/

当時、ヨーロッパでTF-CSIRTというCSIRTのコミュニティが活発に活動するなど、地域における連携の重要性が世界的に高まっていました。APCERTの設立も必然の流れであり、時宜を得たと言えるでしょう。

そして、4月には内閣官房情報セキュリティ対策推進室に「緊急対応支援チーム」としてNIRTが設立されました（National Incident Response Team。現・NCO）。翌年8月にFIRSTに加盟しています。

また、7月にはTelecom-ISAC Japanが設立されました。日本初のISAC（Information Sharing and Analysis Center。「情報共有分析センター」）であり、通信業界初のセキュリティコミュニティです。

https://www.telecom-isac.jp/

Telecom-ISAC Japanの活動は、2016年6月にICT-ISACに継承されました。

https://www.ict-isac.jp/

CSIRTの起源はインターネットの発展とも深く関わっています。海外同様、日本のテレコム系企業もインターネット普及期の初期からセキュリティに力を注いでいました。

NCAの誕生と今

日本でもさまざまな組織にCSIRTが作られ活動するようになりましたが、インシデントは多様化の一途をたどり、もはや個々のCSIRTだけでは解決が困難な時代に入っていました。CSIRT同士の連携や協力関係を培うFIRSTのような場が日本にもぜひ必要だ、との気運が形をとり、2007年3月、有志のCSIRTによって日本シーサート協議会が設立されました（現・一般社団法人 日本シーサート協議会）。

略称：NCA 英語名：Nippon CSIRT Association

http://www.nca.gr.jp/

わずか6チームでのスタートでしたが、現在では600チーム以上が参加しています（2025年9月1日現在）。設立当時は、まさかこれほどまで大きな注目を集める組織に成長するとは思いもしませんでした。

2011年秋、内閣サイバーセキュリティセンター（NISC、現NCO）が政府CISOの設置に言及しました。また、2015年12月には経済産業省およびIPAが、「サイバーセキュリティ経営ガイドライン」を策定しました。政府のこうした施策をきっかけに、CSIRT、そしてNCAの活動に対する関心が高まっていきました。NCAの会員数は、特に後者のガイドライン公開後に大きく増加しています。

https://www.nca.gr.jp/member/

対サイバー犯罪とCSIRT

インターネットを利用した犯罪が急増する中、2014年の日本には特筆すべき2つの組織が誕生しました。金融ISACとJC3です。

金融ISACは、金融業界のセキュリティコミュニティとして2014年8月に設立されました。米国のFS-ISACを参考に作られたと思われます。演習を行うなど活動は活発で、金融業界のCSIRT活動を活性化したばかりでなく、のちの交通、自動車、ソフトウェアなど、金融以外の業界のISAC設立にも影響を与えました。

金融ISAC: http://www.f-isac.jp/ FS-ISAC: https://www.fsisac.com/

そして、11月には日本サイバー犯罪対策センター（Japan Cybercrime Control Center。略称JC3）が活動を開始しました。

JC3: https://www.jc3.or.jp/

米国に、サイバー犯罪に関する情報共有や捜査支援などを目的とする非営利団体、NCFTA（National Cyber-Forensics & Training Alliance）があります。JC3はこのNCFTAの日本版ともいえる組織で、NCFTA同様、産業界、学術機関、法執行機関などの情報共有の枠組みとして設立されました。その10年ほど前は、法執行機関の参加と聞くと、多くのCSIRTコミュニティには拒絶反応に似た雰囲気がありました。犯人逮捕という視点と、インシデント解決への取り組みという方向性の違いから起きたものでしょう。しかし、サイバーの世界も犯罪に利用される事態が増え、今や法執行機関との協力、連携は必須の時代となりました。

NCFTA: https://www.ncfta.net/

それでは、グローバルな話題へと戻りましょう。

災いから見えてきた課題

2001年9月11日、米国で同時多発テロ事件が勃発しました。インターネット、あるいはCSIRTが直ちに影響を被ることはありませんでしたが、ほどなくして政治的な意図を持つサイバー攻撃が増えたことから、この事件を機に、実世界が抱える諸問題にインターネットも巻き込まれるようになったことは確かです。

10年後の2011年3月11日、日本で東北地方太平洋沖地震が発生しました。当時、緊急体制に入ったCSIRTは、NTT-CERTなどごく少数のチームを除いてほとんどなかったと思われます。この巨大地震に端を発した震災によって、自然に起因する災害であってもサイバー世界は影響を受け、緊急時におけるCSIRTのサポート能力が問われるのだと、あらためて気付かされました。日本では東日本大震災をきっかけに、CSIRTのメンバーはじめ多くの関係者がリスク管理の必要性を強く認識し、実際にCSIRTをリスク管理やクライシスマネジメントに組み込んでいく組織が増えました。

リスク管理に関して同様の話が海外からも伝わっています。2007年、ロシアからのDDoS攻撃によってエストニアの官公庁や銀行などのウェブサイトがダウンし、市民生活が大混乱に陥りました。同じくバルト海東岸に位置するリトアニアはエストニアの苦境を間近で見聞きし、自国へのDDoS攻撃を警戒しました。数年後、リトアニアに対するロシアからの攻撃が現実のものとなりましたが、ある公的機関のCSIRTではリスクマネジメントの準備があったため、どうにか切り抜けることができたそうです。

さて、昨今、ランサムウェアによる被害が世界中で頻発していますが、脆弱性に対するパッチが当てられていなかったとか、停止すべきアカウントが有効のまま放置されていたなど、多くの場合、小さなインシデントを見逃したり、対応を怠っていた事が被害につながっています。このことからも、自組織の問題点を事前に発見したり、インシデントに対して地道に対応していくという基本的な業務を再確認することが、CSIRTやPSIRTなどセキュリティチームにあらためて求められています。

連携は途切れることなく

最後に、CSIRTなどセキュリティコミュニティの連携の「今」についてお話しして、この小史を締めくくりたいと思います。

2020年3月、世界保健機関（WHO）は新型コロナウイルスについてパンデミック（世界的大流行）が起きていると発表しました。そのような状況下にあっても、CSIRTが活動を停止することはありませんでした。制約こそあれ、FIRSTもNCAもオンラインを活用してコミュニティ活動を継続しました。NCAでも主に地区活動委員会がオンラインを活用しワークショップを継続的に開催しました。このまさしくResilienceという活動こそが、コミュニティの価値でしょう。パンデミック終了後のCSIRT活動の立ち上がりを早めることもできたと感じます。

2021年になると各地のコミュニティで会合の現地開催が復活しました。2022年6月には、Annual FIRST Conferenceがアイルランドの首都ダブリンで開催されました。FIRST主催の年間最大の会合である年次総会が、実に3年ぶりに対面形式で行われたのです。

さて、過去は言うまでもなく、今現在もさまざまな分断や衝突が世界のあちこちで起きています。近年の大きな出来事としては、2021年1月のアメリカ合衆国議会議事堂襲撃事件、そして、その翌年2月のロシアによるウクライナ侵攻が挙げられるでしょう。2023年10月にはハマスとイスラエルが武力衝突しました。このアジアにも不安が見え隠れしています。

こうした対立が、CSIRTやセキュリティコミュニティの連携、あるいは協力にも暗い影を落としていることは、紛れもない事実です。それでもCSIRTの活動が立ち止まったり後退することはありませんでしたし、これからもあり得ないでしょう。さまざまな溝を超えてサイバーセキュリティをより強固なものにしようとする努力が、世界中のCSIRTやコミュニティで続けられています。

改訂履歴

Ver1.0 2025年9月30日 新規作成