桑名レポート：サイバーセキュリティの現場から（5）

CSIRT（シーサート）と互助

NTT アドバンステクノロジ株式会社
常務取締役　セキュリティ事業本部
本部長　桑名 栄二
博士（工学）、CISSP

本稿ではセキュリティインシデント対応チームの構築・運用の課題と、その解決に向けた互助の考え方と事例について述べる。

予防だけでは防げない時代

CSIRT（シーサート、Computer Security Incident Response Team）はコンピュータセキュリティインシデント対応チーム※1のことで、セキュリティインシデントは必ず発生するのでそれに対応する消防署のような組織が必要であるとの考えから、1988年に米国で初めてCERT/CC（Computer Emergency Response Team/Coordination Center）が発足した。国内でも1996年にJPCERT/CCが設立され、現在、大企業、政府機関、地方自治体、大学等を中心に多くの組織内CSIRTが構築・運用されるに至っている。

2018年2月にMcAfee社とCenter for Strategic and International Studiesが発表したレポートでは、サイバー犯罪による損失額は世界で約6000億ドル（約66兆円）、世界全体のGDPの0.8%であり、損失額の伸びは年10%以上と報告されている[1,2]。増加の背景には、①サイバー犯罪者が最新テクノロジーを速やかに導入していること、②サイバー犯罪への参画が簡単になり、その拠点数が増加していること、③サイバー犯罪のエコシステムが出来上がり、サービスとしてのサイバー犯罪CaaS（Cybercrime-as-a-Service）がより巧妙化していること、④サイバー犯罪組織や犯罪者の財政状況が向上していること等がある。

攻撃者は何度失敗しようが一度成功すればよいが、CSIRTは攻撃者の侵入、改ざん、情報の窃取、DDoSなどの行為により被害を受けたネットワークや情報システムを毎回正常な状態に戻さなければならない[3]。

また、世界全体のセキュリティレベルを上げないと、サイバー攻撃に利用されているサーバ等への対応ができず、被害が減らないため、各種ガイドラインやマニュアルが発行されている。米国NISTのCybersecurity Framework[4,5]では、インシデントの特定（Identify）、防御（Protect）、検知（Detect）、対応（Respond）、復旧（Recover）のガイドラインやベストプラクティスを示している。日本でも経済産業省のサイバー経営ガイドライン[6]や金融庁の金融検査マニュアル[7]で、サイバー攻撃に対する防御や監視体制に加え、CSIRTの設置が盛り込まれている。

CSIRT、PSIRTの構築と課題

経済産業省のサイバー経営ガイドラインVer2.0（サイバーセキュリティ経営の重要10項目の指示7）では、企業経営者が情報セキュリティ責任者に指示すべき「インシデント発生時の緊急対応体制の整備」事項（例えば、影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる）を示し、対策を怠った場合のシナリオなどについても述べている[6]。

金融検査マニュアルでは、サイバー攻撃に対する監視体制、サイバー攻撃を受けた際の報告及び広報体制に加え、組織内CSIRT等の緊急時対応及び早期警戒のための体制等が構築されているか等を、検査の手引きとして示している[7]。このような背景もあり、2018年11月1日時点の日本シーサート協議会（NCA）[8]の会員数は320で、その数はヨーロッパCSIRTコミュニティよりも多く、その加盟組織増加率は世界のCSIRTコミュニティFIRST（Forum of Incident Response and Security Teams）よりも高いようである。

また、近年、Webカメラ等のIoTデバイスを利用したサイバー攻撃や発電所を含む社会インフラを狙った攻撃等も増加しており、コンピュータ以外への対応も重要になっているため、IoTデバイス製造会社や販売会社においてPSIRT（製

品脆弱性対応チーム、Product Security Incident Response Team）の構築も盛んに行われている[9,10]。FIRSTでは自社製品のセキュリティ上の脆弱性への対応を目的にPSIRT Services Framework[11]を公開した。CSIRTは組織のリスクマネージメントの一つとして、サイバー攻撃への対応や組織や情報システムに内在する脆弱性、それに対するリスクマネージメントを主眼としているが、PSIRTは自社が製造･販売した製品、部品、サービス等に内在するセキュリティ上の脆弱性・欠陥・不具合への対応に主眼をおいている。

さて、日本においてCSIRT構築はブームとも言えるような状況であるが、課題も多いようである。例えば、インシデント発生時の具体的な対応が明確化されていない、インシデント対応は担当者任せになっている、緊急連絡体制が定められていない、インシデント発生時の連絡に時間がかかるなど、CSIRTが名ばかりの存在となっていた事案も報告されている[12]。これは、各種ガイドラインや検査マニュアルに縛られ、構築ありきでCSIRTを作ったため、実際には経験者が不足しておりインシデント対応が十分に出来なかったことが原因のようである。組織の経営層は危機意識を持っているものの、いざ実運用となると、コンサルティング会社任せで構築したため運用が回らない、セキュリティ機器は設置したが実際のログ解析ができる技術者がいない等の問題に直面しているのである。また、脆弱性情報や攻撃情報などを含むCSIRTコミュニティで共有される最初の情報は英語ベースの情報が殆どであり、英語でのコミュニケーションを苦手とする人間が対応しなければならないなどの課題もある。

さらに中堅中小企業にはそもそもセキュリティ人材がおらず、セキュリティ対応すらままならない状態が多いようである。工場へのロボット導入、自動化により、各種ロボットや制御機器の脆弱性対応やサイバー攻撃対応が必須の状況に追い詰められているが、前述以外にも悩みと課題を抱えている。例えば、CSIRTを作ろうと計画しコンサルティング会社に相談したら高額を要求された、セキュリティ機器の導入が必要だと言われたが本当に必要かが判断できない、フィッシングサイトや不審なメールなどへの対応について外部機関へ相談をしたいがどのような相談をしたらいいのかわからない、人材を調達する費用がない等である。

CSIRTと互助

今から約200年ほど前、財政危機に苦しむ米沢藩を立て直すために、9代藩主 上杉鷹山は藩民の根本方針として「三助」（自助、互助、扶助）の精神を提唱し実践した。「自助」は自ら助ける、「互助」は近隣社会や地域コミュニティが互いに力をあわせて助け合う、「扶助」は国や公的機関が助けるである。CSIRTの構築と運用にとっても「三助」の精神は大変参考になる考え方である。特に、巧妙、多様化するサイバー攻撃に対する防御やインシデント対応を自組織だけで対応することは非常に困難な状況になりつつあり、CSIRT運用者が互いに助け合う「互助」が三助の中でも最も必要とされているのではないだろうか。例えば、日本シーサート協議会やFIRSTなどのコミュニティに参画することで、世界や国内のCSIRTメンバとの情報交換や業界連携が強化でき、最新情報や業界のベストプラクティスに基づくCSIRT構築や運用が可能になる。

また、中堅中小企業は種々の課題や悩みを抱えていると述べたが、これは日本だけでなく、ヨーロッパ企業も同様に困っているようである。ドイツでは、中小工場をまとめてCSIRTサービスを提供している機関がある[13]。日本でも互助の思想に基づき会員制でCSIRTのインシデント対応や情報共有の支援、セキュリティ講座の提供、さらにセキュリティ診断・解析・訓練・教育サービス等を提供するサービスが発表された[14]。今後このような互助の活動に期待したい。

[1]https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf
[2]https://tech.nikkeibp.co.jp/it/atcl/news/17/070601859/
[3]https://www.oreilly.co.jp/books/9784873118383/
[4]https://www.nist.gov/cyberframework
[5]https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[6]http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf
[7]https://www.fsa.go.jp/manual/manualj/yokin.pdf
[8]http://www.nca.gr.jp/
[9]https://www.panasonic.com/global/corporate/product-security/sec/psirt/jp.html
[10]https://www.first.org/members/teams/sony_psirt
[11]https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0
[12]http://report.jbaudit.go.jp/org/h28/ZUIJI4/2016-h28-Z4001-0.htm
[13]https://www.first.org/resources/papers/hamburg2018/TF-CSIRT-HH_Januar2018_final.pdf
[14]https://www.csirt-club.jp/

※1：CSIRTの他にも、CIRT、CERT、SIRT、IRT等と略称がある