内外CSIRTの現状

松尾正浩 （株）三菱総合研究所
matsuo@mri.co.jp
山口 英 奈良先端科学技術大学院大学
suguru@is.aist-nara.ac.jp

インターネット上では，侵入やDoS攻撃など，さまざまなセキュリティ上のトラブルが日々大量に発生している．こうしたトラブルの発生を少しでも減らしたり，また万が一発生してしまった場合に迅速な解決を図って被害の拡大を防止しようと努めている組織がCSIRTである．本稿では，そもそもCSIRTとは何か，どういった活動をしているのか，世界にはどのようなタイプのCSIRTがあるのか等について述べ，日頃あまり耳にすることのない組織がどのように活躍しているのか，その一端をご紹介したい．

CSIRTとは何か

CSIRTは，Computer Security Incident Response Team の略である．RFC2350[4]では，Computer Security Incidentを「コンピュータやネットワークセキュリティのいずれかの側面を危険にさらす（compromise）ような，敵意を持ったあらゆるインシデント」としている．ここで少々分かりにくいインシデントという単語が出てくるが，これは事件，出来事，小戦闘といった意味合いを持っている．したがってCSIRTとは，そうした事件や出来事に対応するチームということになる．

現在，世界中に多くのCSIRTが設立され，それぞれに活躍しているが，そもそもこうしたチームができたのは，1988年に発生した，いわゆるインターネット・ワーム事件が大きなきっかけとなっている[1]．この事件では，一人の人間が放ったワームによって，まだ小規模ではあったが当時のインターネット全体が麻痺してしまい，その解決のために多くの接続組織間での緊密な連絡と協調が必要となった．

そうした事件を契機として，多数の組織に関連する大規模かつ分散型の事件に対しては，事件の全体像を的確に把握し，個々の接続組織に対してタイムリーに的確な情報を提供したり，接続組織間の連携を推進するような仕組みの必要性が認識されるに至った．

そうした状況下で，世界で初めてのCSIRTであるCERT/CC（Computer Emergency Response Team / Coordination Center）[7]が米国ピッツバーグにある，カーネギーメロン大学の付属研究機関SEI（Software Engineering Institute）の中に設立された．

その後，1990年代に入ると，同様の組織が各国でも設立されるようになった．その代表格が，ドイツにあるDFN-CERTやオーストラリアにあるAUSCERTである．また少し遅れて，日本においても1996年にJPCERT/CC[2), 3), 5)]が設立されている．

どんな仕事をしているのか

CSIRTの仕事を理解する上では，constituencyという概念が重要である．これもなかなか適当な訳語が見つからないのだが，おおよそサービス対象者とか対象範囲と捉えていれば間違いないだろう．つまり警察署や消防署に管轄があるように，CSIRTにもそれぞれの役割に応じた対象範囲がある．対象範囲はCSIRTが自ら定めるが，規定する単位は組織やサイトであったり，ネットワー

クであったり，ユーザ層であったりとさまざまである．

個々のCSIRTの業務内容は，それぞれの設立背景や立場によって異なる面も多いが，最低限でも担うべき機能として，自ら定めたサービス対象者に影響を及ぼす，次に述べるような事件への対応が求められている．

- 情報の機密性（confidentiality）を失わせる
- 情報の完全性（integrity）を危険にさらす
- サービスを妨害する（DoS: denial of service）
- サービス，システム，情報を濫用する
- システムにダメージを与える

こうした事件の対応においては，CSIRTとサービス対象者の二者で解決できる場合もあるが，多くの場合，インシデントは複数のサービス対象者をまたいで連鎖的に発生すること，また昨今多発している分散型 DoS（DDoS:Distributed DoS）では，莫大な数のサイトが踏み台として悪用されることなどから，複数の関係者間での連絡や協調（coordinate）が必須である．そのためCSIRT では，次に述べるようなサービスも提供する．

- インシデントに関する情報を受け取るための安全な通信路の設置
- インシデントに関連する情報のサービス対象者やその他の関係者への伝達

CSIRTのフォーラム

インターネットには国境がなく，1つのインシデントが1つの国や地域だけで局所的に行われるとは限らないため，1つのCSIRTだけでは解決できない問題が生じる場合もある(実際，国をまたいだインシデントの例は多い)．そうした事態に効率的に対処するには，異なるサービス対象範囲を持つ，いくつかの CSIRT が密に連携をとりながら対処する必要がある．

万が一の事態が発生した場合に，さまざまな設立背景を持つCSIRT同士が，緊急の対処を円滑に進めるためには，日常から相互に信頼関係を築く努力を実施し，事前に情報交換のフレームワークを定めておくことが重要である．

こうした目的に沿って，CSIRT同士の情報交換や，相互支援・協調を促進するために FIRST（Forum of Incident Response and Security Teams）[6] というフォーラムが 1992 年に設立された．本稿で紹介するCSIRTは，すべてFIRSTに参加しているチームである．

FIRST は，参加者であるCSIRTの中から選挙で選ばれたメンバを構成員とする運営委員会が中心となって運営している．FIRSTに加盟するには，既存のメンバチームからの推薦と，前述した運営委員の3分の2以上の賛成が必要である．

FIRST の正式会合は，AGM（Annual General Meeting） と呼ばれる，年に1回の総会，年に4回の TC（Technical Colloquia）と呼ばれる技術討論会，上述の運営委員会などで構成される．AGMの多くのセッションは公開であり，FIRSTメンバでなくても参加が可能となっている．ただし一部の（メンバとしての議決権を行使したり，機微な情報を取り扱う）セッションは非公開とされている．またTCは，個々の脆弱性やインシデント，クラッキングツールなどをテーマに議論するため，FIRSTメンバ以外に対しては，アジェンダや参加者も含めて情報公開が厳しく制限されている．

FIRSTに加盟するためのプロセスについては，ここでは詳述しないが，既存のFIRSTメンバに推薦者となることを依頼し，その推薦者による実地監査などを経て推薦を受け，運営委員会の承認を得るというのがおおよそのプロセスである．

なおFIRSTに加盟しているCSIRTの一覧表や，上述した内容の詳細については，FIRSTのWebページで公開されている．同じWebページ内に，FIRSTメンバ限定の情報も置かれているが，もちろんそれらはメンバ以外には読むことはできないよう制限（暗号化）されている．

どんなCSIRTがあるのか

CSIRTに対する理解を深めるためには，CSIRT をいくつかの視点から整理・分類してみるとよい．ここでは，サービス対象範囲と設立・運営母体という2つの軸で分類を試みる．いずれの視点にしても，すべての CSIRT を綺麗に区分することは難しいが，全体像を理解するには役に立つであろう．

■サービス対象範疇による区分

(1) インターネット全体を対象とする CSIRT

ここに分類される CSIRT は，世界で唯1つ，先にも触れた米国の CERT/CC のみであろう．CERT/CC は，サービス対象範囲を the Internet としており，名実ともに世界で最大・最強の CSIRT といって過言ではない．

(2) 1つの国や地域全体を対象とする CSIRT

ここに分類されるCSIRT は，これも先に述べたAUSCERTや JPCERT/CC などがある．こうした CSIRT は，National IRTと呼ばれることもあり，国や地域全体といった広域をカバーし，その国や地域の代表として他国のCSIRT との連絡の任にあたっている．

またこうしたCSIRTは，サービス対象地域で新しいCSIRTを設立する際の支援をしたり，サービス対象地域内にある複数の CSIRT間での調整役を担う場合もある．

この分類に属するCSIRTには，.auドメインを対象とする AUSCERT（Australian Computer Emergency Response Team），クロアチア全体を対象とする CARNet CERT（Croatian Academic and Research Network CERT），韓国のサイトを対象とするCERTCC-KR（CERT Coordination Center - Korea），イタリアのサイトを対象とする CERT-IT（CERT Italiano），ポーランドのユーザを対象とする CERT POLSKA（Computer Emergency Response Team Polska），ドイツ全域を対象とする DFN-CERT，デンマークのサイトを対象とする DK-CERT（Danish Computer Emergency Repsonse Team），限定的ではあるがスペイン全体を対象とするIRIS-CERT，日本のインターネットコミュニティを対象とする JPCERT/CC（Japan CERT Coordination Centre），.mxドメインを対象とするMxCERT（Mexican CERT），限定付きだがスロベニアのネットワーク全体を対象とする SI-CERT（Slovenian CERT），.sgドメインを対象とするSingCERT（Singapore CERT）などがある．

(3) 特定組織の構成員を対象とする CSIRT

ここに分類されるCSIRTは，次に示すいくつかの形態にさらに分類することができる．

- 学生や教職員を守るために大学等が設置している CSIRT
- 社員等を守るために民間企業が設置している CSIRT
- 職員等を守るために政府機関が設置している CSIRT

それぞれ，具体的にどのようなCSIRTが属しているのかは，設立・運営母体による区分の中で詳述するので，そちらを参照していただきたい．

共通しているのは，ある組織が自らの構成員や主要な関係者のセキュリティを維持・向上するために自ら設置したCSIRTということであり，外向け（顧客向け等）にサービスを提供することを目的としたチームではない．

(4) 特定組織の利用者（顧客）を対象とする CSIRT

ここに分類されるCSIRTは，おおよそ次に示す形態にさらに分類することができる．

- ネットワーク運営組織（非商用・学術団体）が設置している CSIRT
- ネットワーク運営組織（商用）が設置している CSIRT
- ベンダ等が自社製品ユーザ向けに設置している CSIRT

それぞれ，具体的にどのようなCSIRTが属しているのかは，やはり設立・運営母体による区分の中で詳述するので，そちらを参照していただきたい．

共通しているのは，ある組織が自らの利用者（顧客）のセキュリティを維持・向上するために設置した CSIRTということであり，組織の構成員ではなく外向けのサービスに主眼を置いている．

(5) 有料で不特定多数の顧客を対象とする CSIRT

ここに分類されるCSIRTは，契約を締結した不特定多数の顧客に対して，セキュリティ・サービスを有償で提供するチームである．数年前までは，ここに分類されるチームはきわめて稀であったが，ネットワークセキュリティ関連のトラブルが増加するにつれて，組織をこうした危険から守る専門サービスに対する需要が増加し，その結果としてこうした CSIRTが増えてきているものと思われる．確かに，この数年程の推移を見ていると，そうした傾向が顕著に感じられる．

■設立・運営母体による区分

(1) 大学が設置しているCSIRT

日本の大学では稀かもしれないが，海外の大学では，生徒や教職員を合わせると数万人規模のネットワーク利用者を抱える場合がある．加えて卒業生に対してもネットワークサービスを提供するケースもあり，そうした場合では利用者は莫大な数に上る．そのため，セキュリティを維持するための専門チームが必要となり，

CSIRTを設置する場合がある.

具体的には，Wisconsin-Madison大のBadgIRT，DePaul大のDIRT（DePaul Incident Response Team），Georgia工科大のGTCERT（Georgia Institute of Technology CERT），Israeli大のILAN-CERT（Israeli Academic CERT），Indiana大のIU-CERT（Indiana University CERT），Northwestern大のNU-CERT，Ohio州立大のOSU-IRT（the Ohio State University Incident Response Team），Oxford大の OxCERT（Oxford University IT Security Team），Pennsylvania 州立大の PSU （Pennsylvania State University），Stanford大の SUNSeT（Stanford University Network Security Team），Georgia大のUGaCIRT（The University of Georgia Computer Incident Response Team），Norwegian 州立大の UNINETT CERT などがある.

多くのチームは，米国の大学内にあるが，イランやメキシコといった米国外の大学チームも存在している．この中でも特に有名なのは，オックスフォード大学のOxCERTや，スタンフォード大学のネットワークセキュリティチームのSUNSeTであろう.

(2) 民間企業が設置しているCSIRT

民間企業の中でも，多数の国に進出している大規模な企業では，事業所の数も多く，そこで働く従業員も数万人規模になる場合がある．そうした企業では，企業全体のセキュリティを維持するために，専門のチームが必要となり，CSIRTを設置する場合がある．具体的には，金融や保険関係の企業にそうした事例が多い.

具体的には，Bank of America のBACIRT（Bank of America CIRT），Citigroupの CitigroupCIRT，Goldman,Sachs and Company のチーム，Prudential Insurance Company の PruCERT（the Prudential Insurance Company CERT），German Savings Banks の S-CERT（CERT of the German Savings Banks Organization），VISA のVISA-CIRTなどがある.

また，金融・保険以外にも，Accenture社が同社内部向けに設置している ACIRTやBoeing社が同社向けに設置しているBCERTなど，企業内部向けの CSIRTが設置されている.

(3) 政府機関（軍を除く）が設置しているCSIRT

政府機関は，その立場上から種々の攻撃にさらされる危険性が高い．そこで，自らを守るため，あるいは自らの関係諸機関を守るために CSIRTを設置する場合がある.

具体的には，米エネルギー省のCIAC（US Department of Energy's Computer Incident Advisory Capability），米国下院のHOUSECIRT（US House of Representatives Computer Incident Response Team），米 NASA の NASIRC（NASA Incident Response Center），米 NIHの NIHIRT（NIH Incident Response Team），米NISTの NIST/CSRCなどがある.

(4) 軍関係組織が設置しているCSIRT

軍関係組織も立場上から種々の攻撃にさらされる危険性がきわめて高い．そこで，自らを守るために CSIRTを設置する場合がある．具体的には，米空軍が設置しているAFCERT（Air Force CERT），米国防総省が設置しているDOD-CERT（US Department of Defense CERT），米海軍が設置している NAVCIRT（Naval Computer Incident Response Team），加国防省が設置している DND CIRT，英国防省が設置しているMODCERT（MOD Computer Emergency Response Team）などがある.

(5) ネットワーク運営組織（非商用・学術団体）が設置しているCSIRT

インターネット発展の歴史を振り返ってみると，非営利の学術研究団体等が中心となって構築したネットワークの果たした役割は大きい．そうした非商用のネットワーク運営組織が，参加の接続組織において生じるトラブルを解決するために CSIRTを設置する場合がある．ここに分類されるCSIRTは，そうした過去の経緯から歴史の長いチームが多い.

具体的には，オランダのSURFnetに接続された組織のためのCERT-NL，欧州の研究用ネットワークのためのDANTE（Delivery of Advanced Network Technology to Europe, Ltd.），英国のJANETに接続された組織のための JANET-CERT，デンマーク，フィンランド，アイスランド，ノルウェー，スウェーデンといった北欧諸国のネットワークのためのNORDUnet，スイスのSWITCHに接続された組織のためのSWITCH-CERT（Swiss Academic and Research Network CERT）などがある.

(6) ネットワーク運営組織（商用）が設置しているCSIRT

インターネットの発展当初は，上述した非営利学術

研究系のネットワークが主流であったが，今日では立場が入れ替わり，商用のネットワーク運営組織，いわゆる商用インターネットサービスプロバイダ（ISP）が多くの国で主流となっている．こうした背景から，商用ISPを利用する利用者が急激に増加し，そうした利用者のセキュリティを確保するために，商用 ISP が自らCSIRTを設置する例も増えてきている．

具体的には，AT&Tのインターネットサービス顧客向けチーム，British TelecomのBTCERTCC（British Telecommunications CERT Co-ordination Centre），Earthlink の ELN-FIRST（Earthlink Network FIRST），MCIWorldComのチーム，Sprint のチーム，ドイツテレコムの Telekom-CERT（Internal CERT for Deutsche Telekom）等々がある．

なお，こうした CSIRT が増えている背景には，インシデント発生後のトラブル解消よりも事前予防の方が効率的でコストが低く済むというお家事情もありそうである．

（7）ベンダ等が自社製品ユーザ向けに設置しているCSIRT

コンピュータやネットワーク機器を開発・販売しているハードウェアやソフトウェアのベンダが，自社製品（すなわち直接の攻撃対象）に関するセキュリティを確保し，顧客へのサービスを向上するために，自らCSIRTを設置するケースが増えている．こうしたCSIRTでは，自社製品に関連するセキュリティホール情報や，具体的な対策のとり方を自社製品の顧客に迅速に伝達することを重要な使命としている．

具体的には，Cisco Systems社のCisco PSIRT（Cisco Product Security Incident Response Team），Compaq Computer 社の Compaq SSRT（Compaq Software Security Response Team），Hewlett-Packard 社のチーム，Silicon Graphics 社のチーム Sun Microsystems 社のチーム，Unisys 社のUCERT（Unisys CERT）などが代表的な例であろう．

（8）独立に運営されている CSIRT

上述してきたタイプの CSIRTとは異なり，できるだけ設立母体や運営主体の影響を受けず，中立・公平な立場でセキュリティ問題の解決を図ろうとしているのが，ここで述べるCSIRTである．セキュリティの問題は，立場の異なる組織の利害が複雑に絡むケースがあるため，こうした中立・公平な立場を持つ組織が必要となる．具体的には，先に述べた1つの国や地域全体を対象とするCSIRTがこうした形態をとる場合が多い．

ただし，こうした組織には，中立・公平性を守るために特定の資金源に依存することができず，いかにして安定に運営するかという問題に常に直面せざるを得ないという共通の課題がある．

本来であれば，受益者から広く薄く公平に負担を求め，自主独立の運営を心がけることが望ましいが，そうした受益者負担について理解を求めることは難しく，各CSIRTはそれぞれに苦労している．

今後の展望

つい先ごろ（2001年10月10日），電子政府の情報セキュリティを確保するため，2002年度中に，内閣官房において緊急事態に対処するための「ナショナル・チーム」（National Incident Response Team; NIRT）を編成するというアクションプランが情報セキュリティ対策推進会議から打ち出された．

このアクションプランの中では，万が一サイバー攻撃等が発生した場合の緊急対処のために，早急に原因を解明して対応措置を講じ，また広く情報提供を行って再発防止に努める体制が必要であるとしている．そのための具体策として，先のNIRTを編成して日頃から訓練を実施し，関係機関との情報交換等に努めて，緊急事態に備えることとしている．

この構想が実現すれば，国内においてCSIRTが1つ増えることになるが，自らのセキュリティは自らの責任において確保すべきであること，単一のCSIRTが1つの国のありとあらゆる組織をカバーするのは困難であること，同一の属性を持つ組織群を対象とする専門の CSIRTを設立することは，知識・情報の集約や迅速かつ円滑な緊急対応を実現しやすいことなどから歓迎すべき動きといえよう．

今後は，日本国内においても，大学が生徒や教職員を守るために設置する CSIRT，ネットワーク接続組織が顧客を守るために設置する CSIRT，ベンダ等が自社製品の利用者を守るために設置する CSIRT等，さまざまな CSIRTが設立され，それらが連携をとりつつ一致協力してインターネットのセキュリティ確保に貢献するように活動していくことが望まれる．

参考文献

1）山口　英：インターネットにおけるセキュリティ問題と緊急対応組織，情報処理，Vol.38，No.10，pp.863-869（Oct. 1997）.
2）山口　英，大林正英: JPCERT/CC の現状と展望，情報処理，Vol.40, No.3, pp.328-332 (Mar. 1998).
3）大林正英，石田晴久: インターネットにおける不正アクセス対応とJPCERT/CC，信学技報，FACE98-24, pp.23-27 (Dec. 1998).
4）Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2530.txt
5）松尾正浩: JPCERT/CC の活動，bit別冊 情報セキュリティ，pp.282-289 (Jan. 2000).
6）http://www.first.org/
7）http://www.cert.org/

（平成13年11月12日受付）