NTTにおけるCSIRT活動

近年，ブロードバンドやPCの普及の中で，ボットやフィッシング，DDoS（Distributed Denial of Service）攻撃等のセキュリティ脅威は，巧妙化し，組織的になってきました．今や，サイバー攻撃は常に起こり得るものとして，防御する側も組織的な活動が必要となってきています．本稿では，CSIRT活動と，NTT情報流通プラットフォーム研究所が取り組んでいるNTT-CERTについて紹介します．

長島 雅夫（ながしま まさお）/杉浦 芳樹（すぎうら よしき）/安部 哲哉（あべ てつや）
吉田 尊彦（よしだ たかひこ）/向山 明夫（むかいやま あきお）
NTT情報流通プラットフォーム研究所

コンピュータセキュリティインシデントとは

コンピュータセキュリティインシデント（インシデント）とは何でしょうか．さまざまな見方がありますが，侵入やウイルス感染といった重大なものばかりでなく，ポートスキャンや脆弱性探索なども含めて，セキュリティに関して何らかの対応や判断が必要と思われるものは，すべてインシデントだと考えられます．

インシデントを対応する組織

コンピュータセキュリティに対応するために，CSIRT（Computer Security Incident Response Team）という枠組みがあります．NTTではNTT情報流通プラットフォーム研究所の中にNTTグループのCSIRTとして，NTT-CERT（NTT Computer Security Incident Response and Readiness Coordination Team）を2004年10月に発足させ，NTTグループ内のセキュリティに関する諸問題に取り組んでいます．また，NTTグループ会社におけるCSIRT体制を整備する活動も実施しています．

CSIRTとは

CSIRTは「シーサート」と呼びます．ほかにCERT*（後述），IRT（Incident Response Team），CIRC（Computer Incident Response Capability）といった呼び方がありますが，これらはCSIRTとほぼ同じものと考えていただいて構いません．

CSIRTは，インシデントに対し，分析，対応，教育，研究開発などの活動を行う組織です．さまざまなCSIRTが世界各地に存在していますが，特に有名なものとしては，米国のCERT/CC，US-CERT（米国政府）や，日本であればJPCERT/CC（JPCERTコーディネーションセンター）が挙げられます．また，日本の企業では，ほかにHIRT（㈱日立製作所），IIJ-SECT（㈱インターネットイニシアティブ）などがCSIRTを立ち上げて活動しています[1]．

CSIRTの概要を**図1**，**2**で説明します．

図1にあるようにインシデントのライフサイクルにおける，さまざまな側面をサポートし，インシデントを防止し，不幸にしてインシデントが起こってしまった場合には，被害の局限化に貢献することがCSIRTの役割です．

また，図2に示したように，対応の調整，技術支援，情報の収集・分析・提供などを関係者に対して行うこともCSIRTの役割です．例えば，社内の最高情報責任者（CIO: Chief Information Officer）やセキュリティ最高責任者（CSO: Chief Security Officer）などのセキュリティ管理者とシステム運用者や開発者への情報提供や技術支援を行うとともに，外部のCSIRTやセキュリティ技術者と連携して，セキュリティ技術協力や情報交換等を行い，インシデントの予防やインシデント発生時の対応に役立てることも重要な仕事です．

CSIRTの要件

CSIRTには，「こういう組織だ」と明確に定義されたものはありませんが，主に次の4点が必要と考えられています．

(1) インシデントへの対応を行うこと

セキュリティ上の問題点や情報を入手したら，それらを分析して対応を検討し，適切な部署や担当者に伝えます．その際，技術的内容，対処方法

＊CERTは米国におけるCERT/CCの登録商標です．

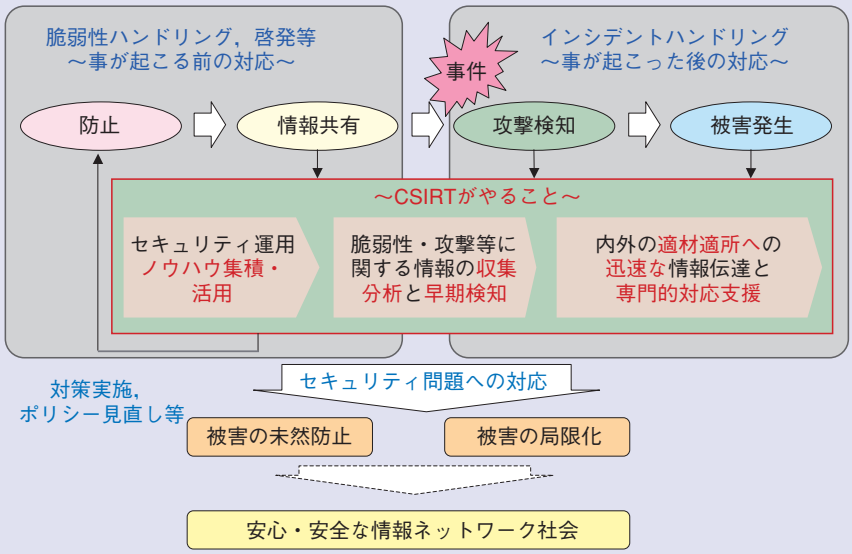

図１　CSIRT の活動

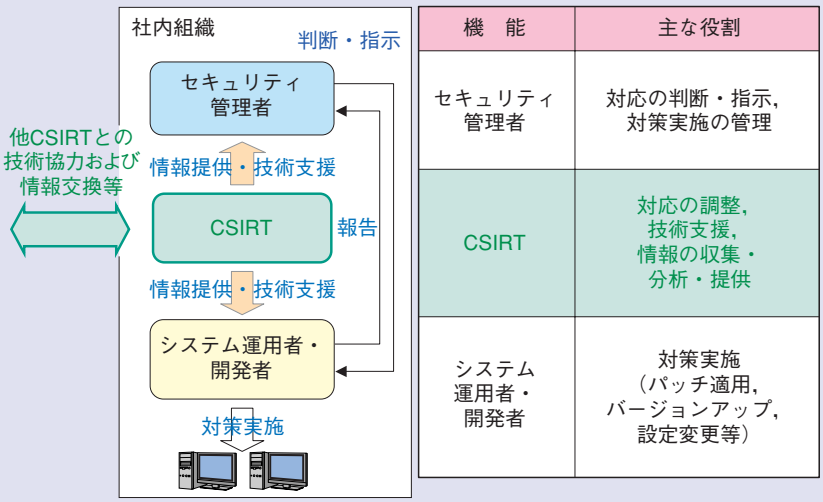

図２　CSIRT の役割

に関して支援を行います．

⑵　コーディネーションを行うこと

セキュリティ上の問題を抱えた組織が複数ある場合，協調して解決に取り組む手助けをするという観点から，外部の組織，あるいは内部の組織との間に立って，セキュリティ情報のやり取りの調整（コーディネーション）を行います．

⑶　対象者が明確に定義されていること

次の「信頼できるチームであること」でも述べますが，インシデント対応のために常にデリケートな情報を扱っているため，CSIRTが提供するサービスの対象者を明確にしておくことは重要です．またそうすることにより，緊急時，所定の対象者にサービスを素早く提供することが可能になります．

⑷　信頼できるチームであること

CSIRTが扱う情報の多くは機密情報です．その取り扱いに関しては細心の注意を払わなくてはなりません．インシデントの報告者から，「ここなら情報を提供しても心配ない」との信頼感を持ってもらうことが大切です．

ここまでCSIRTについて概要を述べてきました．CSIRTについては日本語でも文書がありますのでご参照ください[(2)，(3)]．

なぜCSIRTが必要か

事前防御的なセキュリティ対策だけでは，すべてのインシデントを未然に防ぐことはできません．またビジネスプロセスや情報システムは，ネットワークを介して相互に依存しているため，１つの組織や限定された担当者だけで有効なセキュリティ対策を講じることは困難です．

セキュリティ対策の専門チームであるCSIRTは，発生したインシデントについて情報を流通させたり，問題解決に向けた情報調整を行うことによって，インシデント発生時の被害を最小限に食い止めること，そして，将来同様のインシデントが再発するのを防ぐことを活動の大きな目的としています．インシデントに関する情報を定常的に収

集し分析することにより，インシデントの報告者に対して，必要な対策をタイムリに明示することができるのです．

また機密性の高い情報を取り扱いながら，内外の組織との間で密な情報交換や連携を行う業務には，より厳格な情報管理が求められます．そのためにもCSIRTという組織が必要になってきます．情報管理能力を備えた組織という属性を持っていることが，CSIRTが世の中から信頼される理由の１つでもあります．

FIRSTとは

CSIRTの集まりとしてFIRST（Forum of Incident Response and Security Teams）[4] という国際的な組織があります．昨今のようにインシデントの国際化および巧妙化が進む中では，コンピュータセキュリティにかかわる問題は，１つの組織や地域では対処できません．

1990年，世界各地のCSIRTが国や地域，組織の枠組みを超えてセキュリティ情報を交換したり，インシデント対応で協力関係を築くことを目的に，11の組織が集まってFIRSTが設立されました．前述の米国CERT/CCは創設メンバであり，日本のJPCERT/CCも1998年より加盟しています．

2010年１月現在，世界40以上の国と地域から200チーム以上がFIRSTに加盟し，インシデントの事例や対応のノウハウなど，メーリングリストを通じてさまざまな情報を交換しています．

企業ではBTCERTCC（British Telecom），Telekom-CERT（Deutsche Telekom），MSCERT（Microsoft），Sun（Sun Microsystems）など欧米を中心に加盟しています．NTT-CERTは2005年１月から加盟しています．

日本からは2010年１月現在，前述のJPCERT/CC，HIRT，IIJ-SECTのほかにもNISC（内閣官房），CFC（警察庁）など16チームが加盟しています[5]．

FIRSTの主なイベント

FIRSTは毎年６月ごろに定期総会（Annual Conference）を開いています．この定期総会は，世界中からCSIRTのメンバやセキュリティ技術者が集まるユニークな国際会議で，CSIRT運営のノウハウに関する情報や，一般的なセキュリティ技術に関する問題など，多彩なテーマで発表が行われており，FIRSTのメンバでなくても参加できます．

2008年の会場はカナダのバンクーバーでした．2009年は，日本では初めての開催となり，京都にて６月28日から７月３日まで開催されました．場所が日本ということもあり，日本の方々が多く参加していました．また，参加国の数が過去最高の52カ国となるなど，海外の参加者からも高い評価を得ています[6]．

このほか，セキュリティ技術に関する話題を中心とした技術会合（TC: Technical Colloquium）が年に数回世界の各地域で開催されますが，こちらはメンバだけを対象としています．NTT-CERTからも適宜参加してセキュリティに関するディスカッション，ヨーロッパや米国の動向収集，チーム連携などを行っています．

日本シーサート協議会(NCA)とは

1998年当時，日本からのCSIRTのFIRST加盟チームはJPCERT/CCだけでした．NTT-CERTがFIRSTに加盟した2005年１月においては６チームでした．2010年１月現在，日本からは16チームに拡大しています．この数字を見ても分かるように，元々は欧米が中心であったCSIRTの活動が日本国内でも活発になってきました．

このような状況の中，日本国内においても，互いに協調する場を持ち，これまでにない高いレベルでの緊密な連携体制の実現を目指しながら，共通の問題を解決する場を設けることを目的として，2007年にNTT-CERTはJPCERT/CC，HIRT，IIJ-SECT，JSOC（㈱ラック），SBCSIRT（ソフトバンクグループ）とともに日本シーサート協議会（NCA: Nippon CSIRT Association）[7] を設立しました．2010年１月現在，企業を中心に14チームまで会員が拡大しています．

日本シーサート協議会の主なイベント

日本シーサート協議会は年１回の総会，ほぼ四半期ごとに１回行われる会員向けの情報交換会などを実施しています．各会員の方々が興味のある課題に対してサブグループを立ち上げ（ワーキンググループ），技術文書の作成，CSIRTの課題検討，脅威情報の共有

などに取り組んでいます．CSIRT構築支援の一環として，CSIRTへの関心が高い組織とのディスカッションや日本シーサート協議会への加盟支援を行って，日本におけるCSIRT活動を推進しています．

また，後述のCSIRT構築・運用のために，CSIRTトレーニングであるTRANSITS[8]を日本の組織向けに実施したり（2009年３月）[9]，アジアのCSIRTの団体であるAPCERTが主催するサイバー演習に協力しています（2007年12月，2008年12月）．

NTT-CERTの活動

NTT情報流通プラットフォーム研究所がこれまで行ってきた情報セキュリティに関する取り組みを基盤として，前述のとおり2004年10月からNTT-CERTが活動を開始しました．NTTグループにおける中核CSIRTとして，セキュリティに関し信頼される相談窓口となること，またグループ内外の組織や専門家と協力して，インシデントの検知，分析，被害の局限化，予防などを支援することにより，NTTグループだけではなく，情報ネットワーク社会におけるセキュリティの向上に貢献することを活動目的として掲げています．NTT-CERTの活動の５つの柱を次に示します（**図３**）．

⑴　信頼できる相談窓口

セキュリティに関するNTTグループ内外の組織やコミュニティとグローバルなネットワークを構築し，NTTグループ内部組織，および外部組織に対して，信頼できる窓口（PoC: Point of Contact）を提供します．

⑵　セキュリティ情報の収集・分析・提供

セキュリティに関する膨大な情報ソースを分析し，注意喚起やアドバイザリを発行するとともに，インシデント対応や予防に関するノウハウの公開，水平展開を行います．

必要に応じてインシデントが発生したシステムに対する分析の実施・支援も行います．その分析の際には，システムを調査するための特殊な手法（フォレンジック）を用いることで，システム上に存在するインシデントの痕跡に極力影響を与えないようにしながら，インシデントの原因を調査します．調査の手順は，①データの保全，②保全したデータの分析，③分析結果の報告書作成，④必要な部署に対して分析結果を水平展開，というようになります．調査によってインシデントの原因を明確にすることにより，同様のインシデントに対する再発防止策を検討することができます．また，インシデントが発生したシステムと同様のシステムを利用している部署に分析結果を水平展開することによって，同様のインシデントが発生することを防止します．

⑶　CSIRT構築支援

組織内の運用担当者，NTT-CERT，他のCSIRTなどと連携して，組織内のインシデント管理を推進，調整するチーム（CSIRT）の構築を支援します．NTT-CERTではヨーロッパのTERENA（Trans-European Research and Education Networking Association）[10]と呼ばれる学術ネットワークの組織が開発したTRANSITSの日本語訳をJPCERT/CC，NTTデータと作成し，NTTグループ向け（NTT-CERT主催），日本の企業などの組織向け（日本シーサート協議会主催）にそれぞれ実施しています．

図３　NTT-CERTの活動５つの柱

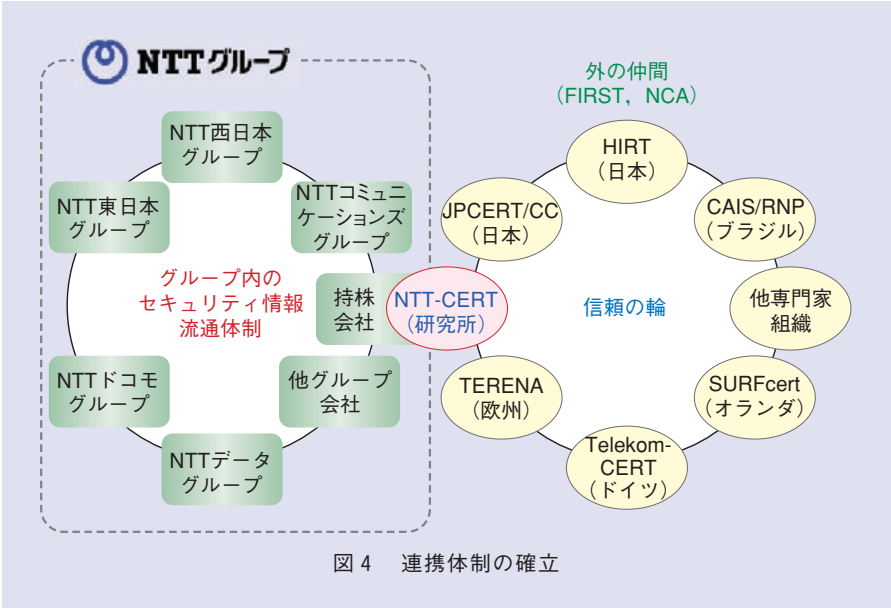

図 4　連携体制の確立

⑷　トレーニング＆教育

NTTグループのセキュリティ向上を目指し，グループ会社のセキュリティ人材育成の面でも支援しています．日々のCSIRT業務で得たインシデント管理支援，コーディネーション，情報収集・分析，また研究開発などで蓄積した知見を，セキュリティ技術者育成向けの高度なトレーニングコンテンツとして提供しています（トレーニングの場は定期的に開催）．また，グループ各社と連携し，タイムリな話題に関して，ワークショップなどディスカッションの場を定期的に設けています．

⑸　セキュリティに関する研究開発

新たな脅威に対する防御技術やセキュリティマネジメントを効率化するシステムやCSIRTを効率的に構築・運用するためのフレームワークなどの研究開発を推進し，成果をNTTグループ企業に展開します．

今後の展開

NTTのような巨大なグループ企業では，セキュリティ向上のために，グループ会社のセキュリティ部門どうしが連携する体制も必要になります．さらなるCSIRTの構築や，NTTグループ内のCSIRTどうしの連携に際して，NTT-CERTは全面的に支援していきたいと考えています．

また，昨今のようにインシデントの国際化および巧妙化が進む中では，単独チームでさまざまなインシデントに対応することはますます厳しくなってきています．そのため，FIRSTや日本シーサート協議会のメンバとの協力体制を推し進めることが，今後ますます重要になると考えています（**図 4**）．

■参考文献

⑴　http://www.nca.gr.jp/member/index.html
⑵　http://www.ipa.go.jp/security/rfc/RFC2350JA.html
⑶　http://www.jpcert.or.jp/csirt_material/
⑷　http://www.first.org/
⑸　http://www.first.org/members/map/
⑹　http://internet.watch.impress.co.jp/docs/column/security/20090709_300875.html
⑺　http://www.nca.gr.jp/
⑻　http://www.terena.org/activities/csirt-training/
⑼　http://www.nca.gr.jp/2009/transits/
⑽　http://www.terena.org/

NTT-CERTでは質問を受け付けています．

ただし，必ずしも問題の解決を保証するものではありません．また，内容によっては対応できないケースがありますのでご了承ください．NTT-CERTへの連絡方法は下記のとおりです．

PGP暗号化して送信したい場合は，以下のPGP公開鍵をご利用ください．

URL http://www.ntt-cert.org/nttcert.asc
Key ID 0x7E34EEFD
Key fingerprint = C932 7F8C BCB8 97E3 5B4F 1626 139E 6AC6 7E34 EEFD

（後列左から）長島　雅夫/ 杉浦　芳樹
（前列左から）安部　哲哉/ 吉田　尊彦/
向山　明夫

NTT-CERTでは，インシデント報告をはじめとして，セキュリティ問題に関する情報や質問を受け付けています．特にNTTグループ企業の業務に携わる方であればどなたでも結構です．お気軽にご連絡ください．

◆問い合わせ先

NTT情報流通プラットフォーム研究所
TEL　0422-59-7800
FAX　0422-59-7801
E-mail　cert@ntt-cert.org
URL　http://www.ntt-cert.org/