特別論説 情報処理最前線

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

Security Issues in the Internet and Incident Response Teams by Suguru YAMAGUCHI (Nara Institute of Science and Technology).

山口 英[1]

1 奈良先端科学技術大学院大学

1. はじめに

1980年代から開発が続けられてきたインターネットは，1990年代初頭に商用化が行われた．これによりインターネットは全世界で爆発的に拡大し，現在では重要な通信インフラとして社会に根づいた．同時に，インターネットを利用した商業活動も盛んになり，業務上の連絡手段としての電子メール利用だけでなく，WWWを用いた物品の販売や予約サービスの提供といったインターネットを利用した直接的な商業活動も行われるようになった．このため，1980年代にインターネットがまだ研究実験ネットワークであったころと比較して，現在のインターネット環境では経済的に価値ある情報が膨大に交換されるようになった．たとえば，インターネット上の商品購入に使われるクレジットカード番号などはその代表的な価値ある情報といえる．このため，インターネットにおけるセキュリティ保全技術の開発と利用は急務となっている．

一方，1988年に発生したいわゆる“Internet Worm”事件[1]を契機として，インターネットの研究者・技術者の間ではセキュリティ技術の重要性が認識され，インターネット環境に有効なセキュリティ技術を積極的に研究開発するようになった．また，電子メールなどの既存のアプリケーションを利用して価値ある情報が交換されることを予想して，既存のアプリケーションのセキュリティ機能を高める作業も並行して努力されてきた．この結果として，PGP[2]やS/MIME[3]などの暗号化電子メール，X.509と公開鍵暗号系を技術基盤とするCA(Certificate Authority)サービスといったユーザ認証システム[4]，OTP(One Time Password)技術[5]などが生み出されてきた．また現在インターネットで最も頻繁に使われているWWWではSSL(Secure Socket Layer)サービス[6]を利用して通信データの暗号化を実現できるようになった．現在ではこれらの技術を用いれば，原理的にセキュリティ保全が可能になっている．しかしながら，インターネットで利用されているアプリケーションやシステムには，数多くのセキュリティホールがあり，それを完全に除去することはできていない．このため，インターネット上で交換される「価値ある情報」を求めて，アプリケーションやシステムのセキュリティホールを巧みに用いて，システムに対する不正アクセスやファイルなどの盗難といった能動的な攻撃(Active Attack)が頻発するようになってしまった．また，インターネットに接続されているシステムが爆発的に増加したことから，セキュリティ管理が十分行われていないシステムも数多い．このような運用上不備を抱えたシステムに侵入して，ネットワークを盗聴しパスワードを不正に入手するような受動的な攻撃(Passive Attack)も広く行われている．

現在のインターネットで頻発しているセキュリティ問題の多くは，セキュリティホールか運用上の不備を抱えたシステムを利用されることが多い．また最近では，特定の攻撃者が，インターネット上の数多くのシステムに連続して攻撃を加える広域型のクラッキング(cracking)もしばしば発生する．

このようなことから，インターネットにおけるセキュリティ問題に関連する情報をインターネットコミュニティが共有し，その情報を基に管理技

術を向上させたり，アプリケーションのセキュリティホールを除去したりすることが重要であると考えられてきた．また，広域的なクラッキングからシステムを守るために，現在発生しているクラッキングに対する警告をインターネットコミュニティに対して発するサービスも必要であると認識されてきている．このようなことから，インターネット上のセキュリティ問題に対応するための組織作りが全世界で広く進められている．

米国においては，1988年の“Internet Worm”事件を契機に，インターネット上のセキュリティ問題に関する情報センターとして，CERT/CC (Computer Emergency Response Team Coordination Center)[7]が1988年に設立された．CERT/CCでは，インターネット上で発生しているセキュリティ問題についての情報を収集し，その原因を解析し，対応策の開発を促進することを行っている．また，被害を受けたサイトの管理者に，どのように対応したらよいのかというコンサルティングを提供している．CERT/CCのようなインターネットにおけるセキュリティ面での緊急対応組織を一般にIRT(Incident Response Team)と呼ぶ．

本稿では，現在のインターネットにおけるセキュリティ問題の概要を説明し，IRTがもつべき要件を述べ，さらに，1996年10月から活動を開始したJPCERT/CCについて紹介する．

2. 頻発するセキュリティ問題

近年のインターネットでは，セキュリティ問題が頻発している．また，従来は攻撃者が海外のサイトから侵入を図ることが多かったが，現在では日本国内にも攻撃者が多数存在し，不正侵入を試みることが多くなってきた．

2.1 最近の傾向

最近のインターネットにおけるセキュリティ問題は，以下のような傾向がある．

(1) システム侵入が第一目標

セキュリティ問題を引き起こす攻撃者(attacker)は，これまでと同じようにシステムへの侵入を第一の目標としている．攻撃者は，攻撃対象のシステムにあるアカウントのパスワードを入手するためにさまざまな手法を試みる．これらの手法では，システムやアプリケーションがもつセキュリティホールを用いて，パスワードファイルを不正に入手することが大部分である．いったんパスワードファイルが攻撃者の手に渡ってしまうと，crackなどのパスワード解析プログラムを使って平易なパスワードを破ることが簡単にできてしまい侵入を許してしまう．また，ネットワークトラヒックの盗聴や，あるいは，闇市場での売買などによって手に入れたパスワードを利用して侵入を図ることもある．このため，現在でも不正侵入からシステムを防御すること，とくにアカウントの保護は，セキュリティ保全の上で最も重要なことであることに変わりはない．

(2) 踏台攻撃

いったん攻撃者がシステムに侵入すると，そのシステムに接続されているネットワークに対する盗聴によってほかのユーザのパスワードを不正に入手したり，あるいは，トロイの木馬を仕掛け，特権ユーザのパスワードを入手しようとする．そして，ほかのシステムに対する新たな攻撃を開始する．このような攻撃を踏台攻撃と呼ぶ．この段階になると，単に侵入されたシステムだけでなく，そのシステムが接続されているネットワーク上のほかのシステムに対しても被害が及んでしまう．また，踏台攻撃は管理者から攻撃者を発見され難くする効果があるため，攻撃者は踏台攻撃を行うことが多い．

(3) なくならない古典的な侵入手法

従来からよく使われている古典的な手法[8]による不正侵入は，依然としてかなり多く発生している．ネットワーク環境が急速に広がった結果，十分な管理がされていないシステムも増える傾向にあり，セキュリティホールが残っている古いソフトウェアを利用しているシステムや管理者の目が届いていないシステムに侵入されることがかなりある．

(4) ツールの流通

攻撃者が使用するツールは，インターネット上で広く流通している．とくに，攻撃ツールを集めたWWWサイトがインターネット上にいくつか存在しているために，有効なツールは瞬く間に攻撃者のコミュニティに広がってしまう．このため，攻撃パターンや使用されているトロイの木馬プログラムは流行があり，似通ったツールが使われることが多い．また，攻撃者のコミュニティでの侵

入ツールの流通が速いために，既知のセキュリティホールを放置することは，重大な問題を引き起こす可能性が高い．管理者は，つねにセキュリティホールの情報を入手し，ソフトウェアの更新に心がける必要がある．大規模なネットワーク環境を運用している組織では，迅速なソフトウェアの更新作業を行える状況を用意する必要がある．このためには既存の管理体制を強化することが必須である．

(5)スキャナ攻撃

スキャナといわれる，不正侵入可能なホストの発見を半自動的に行うツールが使われることが多い．スキャナとは，特定のネットワークに接続されたホストに対して，セキュリティホールがないかどうかを自動的に検査するツールで，代表的なものとしてISS SAFEsuit[9]などがある．侵入可能なホストの発見に，これらのツールが悪用されることがある．スキャナを使って攻撃を広範囲かつ多数のサイトに対して同時に行うことが多い．

(6)愉快犯の減少

以前は，単にシステムに侵入するだけの愉快犯的な攻撃者が多かった．しかし，現在ではシステムに侵入した攻撃者は通常ファイルを破壊したり，あるいは，クレジットカード番号やパスワードなどの価値ある情報を盗み出す．また，これらの情報は闇市場で売買されることが多いようだ．このため，パスワードなどが闇市場に出回ると，情報が盗み出されたシステムでは何度も攻撃を受けることがしばしばある．

(7)サービス不能攻撃の増加

最近の注目されている新たなセキュリティ問題として，サービス不能攻撃（denial of service attack）がある．たとえば，特定のユーザに対して膨大な数の電子メールを送りつけて，ディスクを溢れさせたり，あるいは，特定のサーバに対して短時間に大量のIPパケットを送り込んでサーバを過負荷にしてダウンさせたりといった攻撃である．サービス不能攻撃は，インターネットだけの問題ではなく，一般にどの種の通信システムでも発生しうる攻撃である．たとえば，電話システムであれば悪戯電話がこの種の攻撃に含まれる．サービス不能攻撃に対しては，一般に有効な防御策が作りにくいだけでなく，攻撃者の発見も困難であることが多い．サービス不能攻撃は，インターネットでも着実に増加しており，その防止をいかにして実現するかが課題となっている．

2.2 基本的な対策

システム運用において近年のセキュリティ問題に対応するには，いろいろなセキュリティ技術を駆使して，システムとネットワークを守らなければならなくなった．具体的には，使用しているアプリケーションやシステムのセキュリティホールの除去，OTPを利用したパスワードの保護強化，管理体制を強化しすべてのシステムでの管理作業が円滑に行える体制整備などが必須である．

ファイアウォールのような，外部からのアクセスを制限する機構を導入することは，もはやインターネットに接続されている組織では必須である．日本においては大学のような教育研究機関におけるファイアウォールの導入が遅れており，このために教育研究機関のシステムが攻撃者の踏台に利用されることが多い．踏台攻撃に利用できるシステムを放置することは，インターネットのほかのサイトに対しても迷惑をかけることになりうる．したがって，教育研究機関においてもファイアウォールの導入を積極的に進めるべきだ．

不幸にもシステムへの不正侵入を許してしまったときには，不正侵入の迅速な発見と排除，被害規模の特定と証拠の保全，トロイの木馬などのシステムに残された不正プログラムの発見と除去，さらに，侵入されたシステムが接続されたネットワーク全体でのセキュリティ保全作業を行わなければならない．さらに，JPCERT/CCなどの緊急対応組織への通知や，警察に対する被害届け出，さらに，攻撃者が特定できた場合には侵入にともなう被害に対する損害賠償請求といった法的対応も必要になる．

不正侵入によって引き起こされる対応作業は，システム管理者にとっても，組織にとってもやっかいで手間のかかる作業であり，それにともなう余分な費用負担も発生する．このような無駄な費用を発生させないためにも，セキュリティシステムに対して投資を行い，強力なシステムの導入と運用に努めることは，インターネットに接続されたネットワーク環境を管理運用する上で必須である．

3. 緊急対応組織

最近のインターネットにおけるセキュリティ問題は着実に増加しており，インターネット接続では利用するシステムやネットワーク機器でセキュリティ保全を行うことは必須となっている．また，現在のセキュリティ問題の多くはシステムやアプリケーションのセキュリティホールを利用して引き起こされている．このため，セキュリティホールの発見，対応策の開発，さらに対応策の流通と迅速な適用が必要となっている．さらに，発生してしまった不正侵入などの事例について情報収集を行い，原因を特定することも，未知のセキュリティホールを発見するために必要な作業である．しかしながら，この作業をインターネットで接続された各組織で独立して行うことは非効率で無駄が多い．このため，インターネット環境におけるセキュリティ問題に関する情報の収集と管理を一元化し，発見されたセキュリティホールに関連する企業に対して対応策の開発を依頼したり，発生した不正アクセスの原因解析を行う専門組織の設立が望まれてきた．さらに，セキュリティ問題が頻発するにしたがって，インターネット全体のセキュリティ向上のために，発生しているセキュリティ問題に関する情報の流通と，開発された対応策の積極的な配布を行う体制の整備が望まれてきた．これを具体化したものが，インターネットにおける緊急対応組織(IRT: Incident Response Team)である．

3.1 IRTの機能

IRTは，インターネットコミュニティに対して，以下の機能を提供する．

(1)情報収集

発生したセキュリティ問題に対する情報を収集し，その分類，被害範囲の特定などを行う．この情報収集によって，現在のセキュリティ問題の特徴を同定できる．

(2)原因解析

未知の手法による不正侵入が発生した場合には，同じ手口による問題の頻発を避けるために，その原因特定が必須である．さらに，その手口がもつインパクトの評価も必要となる．もしも，インターネット全体で広く使われているソフトウェアでの問題とすれば，インターネットコミュニティに対するインパクトは大きい．大きなインパクトをもった手口である場合には，インターネットコミュニティに対して迅速に警告を発する必要がある．

(3)企業との連携

現在利用されているソフトウェアは大部分が商用パッケージである．このため，不正侵入の原因特定や対応策の開発には開発企業の協力が必須である．このために，必要な情報を提供し，開発企業に対応策を開発してもらうための交渉・調整が必要である．

(4)情報の流通

現在流行しているセキュリティ問題についての情報や警告，開発された対応策についての情報を広く流通させ，インターネット全体のセキュリティの向上に努めることは，IRTが行うべき活動である．また，管理者や一般利用者が高いセキュリティ意識をもつことは，セキュリティ保全で重要であり，このための啓発活動も実施すべき活動である．これらの活動を多くのIRTが実施している．

(5)被害者に対してのコンサルティング

不正侵入などの攻撃を受けた被害者に対して，対応策の情報を提供したり，管理作業に対してアドバイスすることは，将来のセキュリティ問題の再発を防ぐ上で有効である．このため，IRTでは，セキュリティ問題の届け出を受けるだけでなく，被害者に対してのコンサルティングを同時に提供することも望まれている．このようなサービスは本来ISP(Internet Service Provider)やシステムインテグレータなどが提供すべきサービスであるが，現状ではこれらのサービスを提供している企業があまりにも少ないことから，IRTがその役割を果たしていることが多い．

3.2 IRTの設立

このような目的で，1988年に米国CERT/CCが最初のIRTとして設立された．1990年代に入ると，セキュリティ問題が頻発するにしたがってCERT/CCと同様の組織を各国が設立し始めた．これが，いわゆるNational IRTであり，オーストラリアのAUSCERTや日本のJPCERT/CCなどがある．現在では，インターネットの整備が進んでいる北米，欧州，さらにアジア各国において次々にNational IRTが設立されている．また，

多国籍企業や政府組織など大規模な組織では，その組織内のセキュリティ問題に迅速に対応するために，組織内にIRTを組織し始めている．これらはOrganizational IRTと呼ばれ，米国NASAや米国空軍などで設立されるようになってきている．このように，IRTが対象とする領域や，IRTの設立母体によって，その活動は多少差があるが，基本的にはどのIRTも上記のサービスを提供している．そして，IRTが情報交換を行い，国際的にも協調した活動を行うためにFIRST(Forum of Incident Responce and Security Teams)[10]が組織された．FIRSTでは，主にIRT間での情報交換の促進を目的としているが，さらにIRTの設立の促進や協力体制の確立を検討する場としても利用されている．

4. JPCERT/CC

JPCERT/CCは，1996年10月から活動を開始した日本におけるNational IRTである．

4.1 発足にいたるまで

1990年代に入ると，日本国内におけるインターネットでも不正アクセスなどのセキュリティ問題が頻発するようになってきた．このような状況に対応して，不正アクセスに関する情報収集や，被害者に対するコンサルティングの提供が必要であるとの認識が高まった．この状況に対応するために，日本におけるインターネットの技術的な将来性を検討する円卓会議である日本インターネット技術検討委員会JEPG/IP[12]が中心になって，1993年頃からボランティアベースのIRTとしてJPCERT(Japan Computer Emergency Response Team)を創設し活動を開始した．活動開始当初は，インターネットの商用化が始まってなかったために，希に被害報告が寄せられる程度であった．しかしながら，1995年になると，インターネットの急速な拡大にともない，数多くの被害報告が寄せられるようになってきた．このため，JEPG/IPでは，セキュリティ問題に関する情報の定常的な収集や，セキュリティ技術の普及に対する普段からの啓発活動の必要性を認識し始め，ボランティアベースではなく，安定した組織としてのJPCERT作りを模索し始めた．そのような中で1996年になると，通産省が設立経費と当初2年間の運営資金を支援することとなり，1996年10月よりJPCERT/CC (Japan Computer Emergency Response Team Coordination Center)として，活動を統括するセキュリティ専門家によるアドバイザリグループと，具体的な活動を実施する専属スタッフ6名からなる新たな体制での活動を開始した．

4.2 現在の活動状況

JPCERT/CCでは，3章に述べたIRTの活動を積極的に実施している．

まず，これまでの緊急対応活動では，1997年6月末までに約300件の被害報告を受け付け，対応活動を行った．また，JPCERT/CCでは，インパクトの大きな問題に対しては，インターネットコミュニティに対して警告を流している．これまでに，sendmail, INN, DNSを利用した広範囲の攻撃に対する警告と技術情報を国内インターネットに対して提供している．これらの情報は，JPCERT/CC WWWサービス[11]から入手できる．また，JPCERT/CCでは，セキュリティ情報流通のためのメーリングリスト運用も行っている．

また，利用者や管理者のための啓発活動としては，国内で開催される会議，イベントなどでセミナやチュートリアルを実施している．

4.3 組織改革

JPCERT/CCは，小さな活動規模ながら設立することができた．JPCERT/CCの活動は，現状では十分といえないまでも，IRTが基本的に提供すべきサービスを実施している．しかしながら，頻発するセキュリティ問題に迅速に対応するためにも，専属スタッフの充実が必須となっている．また，JPCERT/CCは，インターネットコミュニティにとって信頼できる組織でなければ，今後の活動を継続することは不可能に近い．このために，現在JPCERT/CCが収集した被害情報の確実な保護管理や，インターネットコミュニティに対する的確な情報提供といった，組織としての信頼性確保と信頼感の確立は，今後も継続して実施していかなければならない．さらに，JPCERT/CC自体の組織の中立性・公正性確保のために，組織運営のオープン化，安定した資金基盤の確立が今後の円滑な活動を継続する上で必須である．

このために，より多くの資金ソースからの運営資金の確保，専属スタッフの増強による活動の拡大，さらに，会員制度の導入による運営体制のオ

ープン化を行うことを予定している．これらの組織改革は1997年中に実施し，より早い段階での活動の拡大を目指す．

4.4 国内におけるほかのIRTとの関係

日本国内においては，すでにIRTと呼べる組織が3つ存在している．1つが，JPCERT/CCであり，残りの2つが警察庁ネットワークセキュリティ対策室と，IPAセキュリティセンター[13]である．警察庁ネットワークセキュリティ対策室は，インターネットなどのネットワーク環境で発生した犯罪に対してネットワーク専門家が捜査に協力し，円滑な事件解決を支援する機能を提供するとともに，ネットワーク犯罪に対する広範囲の情報収集を目的として1996年に設立された．

IPAセキュリティセンターは，通産省の政策実施機関の1つであるIPAに1997年設立された．IPAセキュリティセンターは，もともとPCなどで蔓延しているウィルスに関する被害の届け出機関を行っていたIPAが活動を拡大し，インターネットにおける不正アクセスに関する被害届も取り扱うために設立された組織である．さらに，IPAセキュリティセンターは，現在の情報処理におけるさまざまなセキュリティ問題について通産省の政策を実施する実行機関としての役割も果たしている．

JPCERT/CCは，上記2つの機関とは異なり，どの組織からも中立・公正な立場での活動を推進していることが最大の特徴である．JPCERT/CCはインターネット全体のセキュリティレベルの向上を目的に，インターネットにおけるセキュリティ領域についての情報センタを目指している組織である．JPCERT/CCがインターネットにおける多くのセキュリティ問題に対応していくためには，インターネットにかかわる多くの人たちの協力，情報提供が必須である．また，セキュリティホールに対する対応策の開発において必要となる企業との交渉・調整は，利害にとらわれない立場で行わなければ成り立たない．これらの活動を円滑に進めるために，JPCERT/CCは中立・公正な立場を貫いている．

インターネットで発生するセキュリティ問題への対応では，技術的な問題解決だけでなく，法的な対応，さまざまな利害調整，被害者の救済といったことも考慮されなければならない．しかしこれらの問題については，警察機構や司法機関による対応，行政機構による政策の実施，あるいは，保険システムの整備といった既存の社会システムによって対応されるべき問題である．上記2つの機関は，このような技術領域以外の問題に対応することを重視した機関と考えることができる．このことから上記2つの機関と比較した場合，JPCERT/CCはよりセキュリティ技術に焦点をあてた活動が中心となっている．とくに，対応策の開発と配付，被害者に対する技術的なコンサルティングの提供は，JPCERT/CCの特徴的な活動である．

しかしながら，この3つの組織はインターネット全体でのセキュリティレベル向上という目標は同じであり，その理由によりJPCERT/CCでは上記2つの機関との意見交換などの交流を進めている．

4.5 諸外国のIRTとの関係

JPCERT/CCでは，FIRSTに対して日本におけるNational IRTとして加盟をするとともに，米国CERT/CC，オーストラリアAUSCERTなどとの情報交換を進めている．さらに，アジア太平洋地区におけるIRTフォーラムであるAPCERTの設立についてもほかのIRTと協力している．インターネットは，特定の国に閉じた通信網ではなく，全世界を包みこむ国際情報通信網である．このようなことから，今後とも諸外国のIRTとの協調・協力関係の確立は重要な使命である．

5. おわりに

本稿では，最近のインターネットにおけるセキュリティ問題の傾向を概観し，さらに，CERT/CCに代表されるIRTを紹介した．また，我が国におけるNational IRTであるJPCERT/CCの活動状況について簡単に述べた．

JPCERT/CCは，不正侵人などのインターネットで頻発するセキュリティ問題に対する公共情報センターとしての機能を提供している．この活動が円滑に進められるためには，インターネットコミュニティの協力，情報提供が必須である．

JPCERT/CCでは，広く情報の提供やさまざまな意見を求めている．JPCERT/CCには下記の方法でコンタクトできる．もしも，読者の皆さんが，

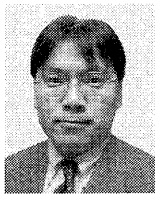
不正侵入の被害に遭われたならば，ぜひともJPCERT/CCに対して情報提供を行ってほしい．提供された情報は，インターネットのセキュリティ向上に必ず役立つものである．皆さんの協力をお願いしたい．

e-mail:info@jpcert.or.jp
電話:03-5575-7762
FAX:03-5575-7764

参考文献

1) Denning, P.J.: Computer Under Attack: Intruders, Worms, and Viruses, ACM Press Books(1990).
2) Atkins, D., Stallings, W. and Zimmermann, P. : PGP Message Exchange Formats, RFC1991 (Aug. 1996).
3) Dusse, S., Lundblade, L., Hoffman, P., Repka, L. and Ramsdell, B. : S/MIME Message Specification, Internet Drafts, Draft-dusse-smime-msg-02.txt(July 1997).
4) Solo, D., Housley, R., Ford,W. and Polk, T. : Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile, Internet Drafts, Draft-ietf-pkix-ipki-part1-05.txt(Aug. 1997).
5) Metz, C. et al. : A One-Time Password System, Internet Drafts, Draft-ietf-otp-01.txt (Mar. 1997).
6) Freier, A. O., Karlton, P. and Kocher, P.C. : The SSL Protocol − Version 3.0, Internet Drafts, Draft-ietf-tls-ssl-version3-00.txt (Nov. 1996).
7) http://www.cert.org/
8) Grafinkel, S. and Spafford, G. : Practical UNIX & Internet Security, 2nd Edition, O'Reilly & Associates(Apr. 1996).
9) http://www.iss.net/
10) http://www.first.org/
11) http://www.jpcert.or.jp/
12) http://www.jepg-ip.ad.jp/
13) http://www.ipa.go.jp/SECURITY/

(平成9年8月11日受付)



山口　英（正会員）

昭和61年大阪大学基礎工学部情報工学科卒業．昭和63年同大学院博士前期課程修了．平成2年同博士後期課程を退学し，同大学情報処理教育センター助手に着任．以後，平成4年奈良先端科学技術大学院大学情報科学センター助手，同助教授を経て，平成5年同大学情報科学研究科助教授．平成3年工学博士（大阪大学）．インターネットアーキテクチャ，ネットワークセキュリティ，高速ネットワークに関する研究に従事．WIDE Project運営委員，JPEG/IP委員，認証実用化実験協議会諮問委員会委員長，JPCERT/CCアドバイザリグループ代表として，国内のインターネット環境の構築に従事．最近はアジア地域における研究ネットワークの構築とインターネット研究の推進に，AI3代表，APNG運営委員として精力的に活動．電子情報通信学会，IEEE，Internet Society各会員．