解説

JPCERT/CCの現状と展望

山口　英　コンピュータ緊急対応センター／奈良先端科学技術大学院大学
大林正英　コンピュータ緊急対応センター

はじめに

インターネットでの大規模なセキュリティトラブルが初めて発生したのは，1988年に起きたインターネット・ウォーム事件[1]といわれている．インターネット・ウォーム事件は，インターネットを構成するコンピュータシステムが持つ技術的脆弱性を明らかにしただけでなく，インターネットの運用管理面での弱さを露呈させることにもなった．この事件を契機に，インターネットコミュニティは，インターネット環境のセキュリティレベルの向上，脆弱性の除去，さらに，事件・事故に即応できる運用管理体制の整備を積極的に進めるようになった．この意味で，インターネット・ウォーム事件は，インターネットのためのセキュリティ技術発展の歴史において，まさにエポックメーキングな出来事であった．インターネット・ウォーム事件から10年が経過した現在では，インターネットに関連するセキュリティ技術は格段の発展を遂げ，現在のインターネット環境構築では，10年前と比べて格段にセキュリティレベルの向上が可能になった．開発された技術を用いて，セキュリティレベルの高いインターネット環境を構築することも，一般的に行われるようになっている．

では，技術の進歩によってインターネット環境でのセキュリティトラブルが根絶しているかというと，残念ながらそうではない．逆に年々深刻さを増しているということができる．システムに対する不正侵入といった不正アクセス事件は，ここ数年増加の一途をたどっている．従来であればパスワードの漏洩から発生する不正アクセス事件が大半であったが，最近はシステムソフトウェアのセキュリティホールを利用した不正侵入，ネットワークの盗聴，TCP/IP通信コネクションの乗っ取りなどの高度な手法も広く使われるようになっている．また，SPAMに代表される可用性に対する攻撃（Denial of Service Attack）も広く行われるようになっている．さらに，従来であれば不正アクセス事件は愉快犯あるいは「いたずら」的な要素が強く，実害が生じることが少なかった．しかし，インターネットの利用が拡大するにつれて，不正アクセス事件は実害を引き起こすようになり，経済的な損失を生み出すようになっている．

この状況を踏まえ，インターネット環境での不正アクセスを防止するために，より組織的に，かつ，よりシステマティックに対応することが求められている．具体的には，インターネットにおける不正アクセス対策として

(1) セキュリティ技術の開発と実用化
(2) 不正アクセスに関する情報収集
(3) 不正アクセスの技術的な解析
(4) 被害者の支援
(5) 不正アクセスの犯罪化と捜査実施
(6) 不正アクセスを防止するための法整備

を実現する努力が必要であると考えられている．特に1997年頃からは，インターネット環境での不正アクセスに対する取り組みについて，OECDやG7といった先進国間の政策協議の場においても議論されるようになり，対策実施の緊急性が広く認知されたといえる．

我が国においては，米国，欧州各国と比較して，上記の対策に対する着手が多少遅れたと言わざるを得ない．しかしながら，少なくとも1996年頃から複数の組織が具体的な対策活動を展開するようになった．

(1) については従来より大学，研究機関，民間企業，技術標準化団体（たとえばIETFなど）が積極的に取り組んでいる．最近では政府機関からの研究資金援助も積極的に行われており，技術開発を加速する努力が行われている．

(2)，(3)，(4) については，これまで通産省関連組織である情報処理振興事業協会（IPA）のセキュリティセンターと，本稿で紹介する日本コンピュータ緊急対応センタ

ー（JPCERT/CC： Japan Computer Emergency Response Team Coordination Center）が活動を展開している．

一方，(5) および (6) については，警察庁において1997年頃から，ハイテク犯罪捜査チームの編成や対応窓口の設置といった，インターネットを用いた犯罪に対する捜査強化プログラムが実施されている．しかし法制度整備に関しては，我が国は他先進国と比較して遅れていると言わざるを得ない．現時点では昭和62年の刑法改正で追加されたいくつかの条文（たとえば刑法234条の2電子計算機損壊等業務妨害）が整備されているだけであり，一部の不正アクセスを犯罪化できているに過ぎない．これは諸外国の不正アクセス防止のための法制度と比較して不十分と言わざるを得ず，日本のインターネットサイトがさまざまな不正アクセス実施の拠点として利用されたとしても，その取り締まりができない恐れが諸外国から指摘されている．このため，より広範囲な不正アクセスを犯罪化するために，警察庁が中心となって1998年から不正アクセス防止法の制定作業に着手した．

JPCERT/CCは技術的な視点から不正アクセスの問題を解決することを目的として1996年に設立された．JPCERT/CCでは，インターネットで発生する不正アクセスについての情報を収集し，その発生のメカニズムや傾向を調査し，必要に応じて，国内のインターネットコミュニティに対してセキュリティ保全を実施するための技術情報を発信している．また，個々の不正アクセス事件の解決のために，不正アクセスの被害者，関連サイト，ベンダ，ISP（Internet Service Provider）との連絡調整業務も併せて提供している．さらに，インターネット環境でのセキュリティレベル向上のための啓発活動も展開している．JPCERT/CCの活動はインターネットコミュニティの理解と協力の上に成り立っている活動である．本稿では，読者の皆さんにJPCERT/CCの活動をより深く理解してもらうことを目的として，JPCERT/CCの活動状況，さらに，今後の活動の展開について述べる．

IRTとは

JPCERT/CCは，一般にIRT（Incident Response Team）と呼ばれる組織に類別される．

もともとIRTとは，地震や洪水などの大規模災害に即応する組織を指していた．IRTは災害の事前対策の計画実行，災害が発生した場合のライフラインの確保，関係組織間の連絡調整などを受け持つ組織である．代表的なIRTとしては，米国FEMA（Federal Emergency Management Agency）[2] がある．このIRTの概念を拡張し，インターネットでのセキュリティ問題に即応する組織もIRTと呼ぶ．

インターネットでの不正アクセスは年々増加しているだけでなく，無差別攻撃が行われたり，システムのセキュリティホールを利用したり，他組織を経由した踏台攻撃を行うなど非常に高度化・複雑化している．このため，不正アクセス防止に取り組むためには，不正アクセスに関連した組織間での協調体制，不正アクセスに関連した情報の積極的な収集と技術的解析，ISPやコンピュータベンダの間での情報交換が必須となっている．また，不正アクセスが発生した場合，その被害の拡大を防止するため，緊急対応体制も必須となる．インターネット関連のIRTでは，協調体制の構築や情報収集・交換の基盤を形成し，不正アクセスに即応する体制を構築することを目的としている．

インターネット関連のIRTとして初めて設立されたのが，米国CERT/CC（Computer Emergency Response Team Coordination Center）[3] である．CERT/CCの設立には，1988年のインターネット・ウォーム事件が大きく影響しており，インターネットでのセキュリティトラブル即応組織として1988年のインターネット・ウォーム事件直後に米国国防総省（DoD）の資金援助を受けて設立された．その後，インターネット関連のIRTは各国で次々と設立されている．代表的な組織としては，米国CIAC[4]，オーストラリアのAUSCERT[5]，ドイツのDFN-CERT[6] がある．これらはすべて1990年代前半に設立されている．さらに，世界各国のIRTのフォーラムとしてFIRST（Forum of Incident Response and Security Teams）[7] が1990年に組織され，IRT間の情報交換，調整，技術交流などの基盤を作り上げている．

FIRSTには現在約70組織が加盟している．IRTとして国際的に認知されており，かつ，他のIRTとの相互協力体制を備えていることがFIRST加盟の条件になっていることから，FIRSTに加盟しているIRTは信頼できるIRTとして考えることができる．

JPCERT/CCの活動

JPCERT/CCは，通産省の資金援助を受けて1996年8月に設立され，1996年10月より活動を開始している．JPCERT/CCは，中立・民間・非営利の任意団体として活動している．

○役割

JPCERT/CCは，日本国内のインターネットについてIRT業務を提供している．具体的には，

(1) 不正アクセスに関する情報収集
(2) 被害者に対する技術支援
(3) 不正アクセスに関係したサイトとの連絡
(4) 不正アクセスの技術的解析
(5) インターネットでの不正アクセス動向調査と報告
(6) インターネットでの不正アクセス防止のための技術情報の提供

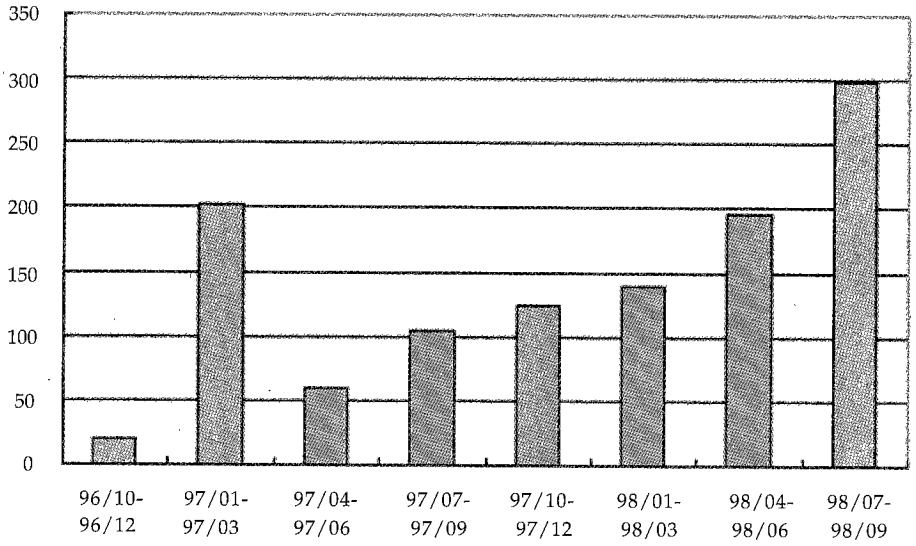

図-1　JPCERT/CCへの不正アクセス情報届け出状況

(7) 他のFIRST加盟IRTとの協力
(8) 啓発活動
を実施している.

一方，JPCERT/CCでは，以下の業務は行っていない.
(a) 不正アクセスを起こした犯人発見の捜査
(b) 個々の組織に対するシステムコンサルティング
(c) 損害賠償請求といった法律面での支援

これは次の理由による.

(a) は捜査権限を持つ司法機関（たとえば警察）だけが可能な業務である．JPCERT/CCは民間団体であるので捜査活動は不可能である.

(b) は多くの企業が営利業務としてサービスを提供している．JPCERT/CCは非営利団体であり，既存の企業活動が存在している領域について業務を展開する必要はないと考える.

(c) は弁護士だけが実施可能な業務である．JPCERT/CCでは弁護士活動は行っていない.

○緊急対応活動

JPCERT/CCは，不正アクセスに関する情報届け出に基づいて活動をしている．現在，JPCERT/CCでは国内のインターネット利用者からの不正アクセスに関する情報届け出を広く受け付けている.

JPCERT/CCにとって情報届け出は，日本国内のインターネットで発生している不正アクセスの状況を知るための重要な情報源となっている．最近の不正アクセスは同時多発的に大規模・広範囲に実施される傾向が強い．このため，不正アクセスの発生状況を知るために，インターネット利用者から広く情報を収集することが必須となっている．JPCERT/CCでは，インターネット利用者が遭遇した不正アクセスについての緊急情報についてももちろんであるが，不正アクセスが未遂に終わったケース，あるいは，すでに対応してしまい終息したケースについても情報を広く求めている.

不正アクセス情報届け出では，
(1) 不正アクセスを受けたサイト
(2) 連絡先
(3) 影響を受けたホストの情報
(4) 不正アクセスの内容
についてhttp://www.jpcert.or.jp/form.htmlの届け出様式に従って情報を受け付けている．当然のことながら，届け出られた情報についてはJPCERT/CC内部のみで利用し，機密状態で厳重に管理され，外部に対して開示することはない．JPCERT/CCでは届け出られた情報に基づいて，被害者に対する技術的支援，不正アクセスに関係したサイトとの連絡，不正アクセス手法の解析を行う．また，海外からの不正アクセスでは，海外のIRTと連絡を取り合って被害状況の把握を行う.

○関連情報の提供

また，上記の個々のケースへの対応だけでなく，届けられた不正アクセス情報を解析し，必要に応じて国内のインターネットコミュニティに対して次のような働きかけをしている.

- 大規模な不正アクセスが実施されている場合には，「緊急報告」を作成しインターネットコミュニティに不正アクセス再発防止対策を行うような警告を発する.
- 多発している不正アクセスについては，その防止対策について技術メモを発行する.
- 発生している不正アクセスについて，4半期ごとにリポ

題　　目	発行日
'96年末から'97年始にかけての不正アクセスに関する緊急報告	1997/07/02
phf CGIプログラムを悪用したアタックに関する緊急報告	1997/08/05
IMAPサーバ・プログラムを悪用したアタックに関する緊急報告	1997/09/09
ネットワークニュースのサービスを悪用したアタックに関する緊急報告	1998/02/10
statdサーバプログラムを悪用したアタックに関する緊急報告	1998/02/26
namedサーバプログラムを悪用したアタックに関する緊急報告	1998/06/04
POPサーバプログラムを悪用したアタックに関する緊急報告	1998/07/02
ポートスキャンを用いた不正アクセスに関する緊急報告	1998/07/10
JPCERT/CC活動報告［1996年10月1日～1997年3月31日］	1997/05/10
活動概要：不正アクセスの動向［1997年4月1日～1997年6月30日］	1997/07/18
活動概要：不正アクセスの動向［1997年7月1日～1997年9月30日］	1997/10/16
活動概要：不正アクセスの動向［1997年10月1日～1997年12月31日］	1998/01/16
活動概要：不正アクセスの動向［1998年1月1日～1998年3月31日］	1998/04/22
活動概要：不正アクセスの動向［1998年4月1日～1998年6月30日］	1998/07/24
活動概要：不正アクセスの動向［1998年7月1日～1998年9月30日］	1998/10/16
電子メール配送プログラムの不正利用（予期しない中継）	1998/01/14
sendmailバージョンアップマニュアル	1998/07/24

表-1　JPCERT/CCの発行文書一覧（1998.11.30現在）

ートを発行し，未対策サイトでの予防を促したり，また，セキュリティ対策の必要性について広い認知を与える努力をする．

これまでJPCERT/CCでは図-1に示す届け出を受けている．これらの情報に基づいて，表-1に示す情報をインターネットコミュニティに対して提供してきた．また，これらの情報を効率よく提供するために，メーリングリスト，および，WWWサーバを運用している．メーリングリスト購読については，http://www.jpcert.or.jp/announce.htmlを参照してもらいたい．また，WWWサーバについては，http://www.jpcert.or.jpでアクセスが可能である．これまでに提供してきたJPCERT/CC文書だけでなく，CERT/CC Security Advisoryやその翻訳などの関連情報，ソフトウェアアーカイブなども提供している．今後も内容を充実させ，インターネットに接続されているサイトでのセキュリティ対策に役立つ情報を提供していくことを目標としている．

○啓発活動

JPCERT/CCでは，国内で開催されるさまざまなイベントの機会を利用して，インターネット環境でのセキュリティ向上のための方法などについてのセミナを開催し，多くの人たちにセキュリティ対策の重要性を認知してもらうとともに，併せてセキュリティ対策のための技術情報の提供も行っている．JPCERT/CCが行う啓発活動は，できる限り多くの人々に我々の活動を伝え，また，セキュリティ対策のポイントや技術情報を提供することを目的としている．最近では，1998年12月15日から開催されたInternet Week 98[8]で，セキュリティ関連セミナを開催するとともに，JPCERT/CCの活動に対する議論をするためのBOFセッションの開催を行っている．

○国際活動

JPCERT/CCは1998年9月にFIRSTに加盟した国内最初のIRTである．FIRST加盟を契機に，諸外国の多くのIRTとの情報交換，協調活動が開始されている．特に複数国にまたがった不正アクセスでは，共同して，発生した不正アクセスの実態の解明と緊急対応を行っている．

また最近では，JPCERT/CCはアジア太平洋地域の国々でのIRT設立を支援するためのAPSIRC（Asia Pacific Security and Incident Response Coordination）の活動にも協力している．APSIRCはIRT間の情報交換やIRT設立を準備している国々への技術的支援を中心に1997年に活動を開始している．

JPCERT/CCの今後

JPCERT/CCの活動開始から約2年が経過した．この2年間の活動から，さまざまな課題が明らかになってきている．特に大きな問題が，IRT活動の強化を今後どのように実現していくのかという問題である．

日本国内においてIRTとしての業務を提供しているのは，先に述べたように警察，JPCERT/CC，IPAセキュリティセンターの3つの組織しか存在しない．現時点では人員数，技術力などの問題から，この3つの組織で日本国内の

すべての不正アクセス問題を処理するのは到底不可能である．また，これら3つの組織の間での技術交流のような，業務そのものではない領域での相互協力は可能ではあるが，組織の性質上，直接業務を補完しあうことは不可能である．

この問題を解決するにはいくつかのアプローチがある．

1つが組織そのものを強化するアプローチである．組織強化では，人材育成と財政基盤の問題を解決することが必要である．たとえば，司法機関である警察の場合，他の組織によって業務体制を強化することはできない．このため，警察における不正アクセスに取り組む体制そのものを強化する以外に解決方法はない．現在の警察の捜査体制を強化するためには，捜査技術を持った要員を確保しなければならない．しかしながら，現在ネットワークセキュリティについて十分な知識を持ち，さらに，捜査に適用できる要員は国内にはほとんど存在していないと言ってもよい．また，JPCERT/CCにしても人材不足は大きな問題となっている．IRT業務を遂行できる技術者の確保は非常に難しい．このようなことから，IRT業務に従事できる人材育成を積極的に行うことが必要となっている．

また，組織強化のための財政基盤の整備も重要な課題となっている．たとえば，現在のJPCERT/CCは通産省からの資金援助によって活動しているが，継続的な活動の維持を考えた場合，複数の資金源を持つ方が望ましいことは明らかである．しかしながら，JPCERT/CCのように民間で非営利の任意団体として，組織を構成している場合，資金確保は難しく，さらに，最近の経済状況の悪化が問題をより難しくしている．また，警察やIPAのような行政機構においても，人員増や予算増は基本的に難しい状況にあり，国の財政状況の悪化が大きな影響を及ぼしている．この問題は政治的な課題ではあるが，今後のインターネット上での経済活動の拡大が予想されている現在，経済活動の基盤となるコンピュータシステムの基盤環境の保全を実施する政策立案と実施が強く求められる．

もう1つのアプローチが，IRT業務を行える組織を国内に作り出していくことである．

現時点での国内に存在しているIRTを役割的に見ると，司法機関（警察）と情報センター（JPCERT/CCなど）の役割を果たす組織しか構成されていない．特に，被害者の支援，啓発活動については，現在のIRT組織では十分に展開できていないと言わざるを得ない．また，IRTにおける重要な活動である不正アクセス情報の収集では，独立した組織が行うよりも，たとえばISPやコンピュータベンダのユーザ・カスタマセンターのようなところが，ユーザサポート活動の中で情報を収集する方が，より多くの情報が収集できるのではないかと考えられる．このようなことから，コンピュータベンダやISPにIRT的な機能を実施できる体制を作り出すことが望ましいのではないかと考えている．また，今後インターネットが小中高等学校へ急速に広まっていくことは確実である．インターネットでのセキュリティ保全では，これら学校関係者に対する教育，啓発活動も重要視されている．特に，学校でのインターネット環境のセキュリティ保全に対する認識を高めるとともに，コンピュータリテラシ教育の一貫としてセキュリティについての教育も併せて行われることが期待される．このために，教育機関向けのIRTも必要になってくるものと思われる．

JPCERT/CCでは，上記の検討を踏まえ，現在のIRT組織との技術的協力体制を充実させるとともに，セキュリティ技術者の人材育成への積極的な取り組み，他のIRT機関の設立，コンピュータベンダやISPとの連携強化を目指している．

おわりに

本稿では，インターネット環境でのIRT機能を提供している日本コンピュータ緊急対応センター（JPCERT/CC）の成り立ち，機能，さらに，今後の展望について述べた．

インターネット環境は，セキュリティ的に脆弱な環境であると述べる人達が数多くいる．

しかしながら，大多数の不正アクセスはその予防方法が明らかになっているものであり，ネットワーク管理とシステム管理を適切に行えば防止できるものである．読者のまわりにあるシステムやネットワークが適切に管理されているかどうか，今1度確認してほしい．必要なセキュリティパッチは適用してあるか，アカウントやパスワードの管理は正しく行われているか，ファイアウォールは設定されているかなど，基本的なセキュリティ対策を確実に行ってほしい．

そして，もしも不幸にも不正アクセスが発生してしまった場合には，JPCERT/CCに連絡をしてほしい．JPCERT/CCは，皆さんの助けになるはずである．JPCERT/CCの連絡先は次の通り．

- Hotline ：(03)5575-7762
- Fax ：(03)5575-7764
- E-mail:info@jpcert.or.jp
- URL-http://www.jpcert.or.jp/

参考文献
1） Denning,P. J. : Computers Under Attack: Intruders, Worms and Viruses, ACM Press / Addison-Wesley(1990).
2） http://www.fema.gov/
3） http://www.cer.org/
4） http://ciac.llnl.gov/
5） http://www.auscert.org.au/
6） http://www.cert.dfn.de/
7） http://www.first.org/
8） http://www.nic.ad.jp/iw98/

（平成11年1月8日受付）