

ネットワークセキュリティ に係る動向

山口 英

奈良先端科学技術大学院大学情報科学研究科
suguru@is.aist-nara.ac.jp

近年のインターネットの急速な普及と利用の拡大に伴い、インターネット基盤環境そのものを防護し、多くのユーザが信頼感を持って日々利用できるようにするためのセキュリティ管理が重要となっている。また、最近の近年の広帯域常時接続環境の広がりや、攻撃手法の高度化の影響を受け、さらに、セキュリティ管理を支えるさまざまな技術自体の高度化も著しい。本稿では、インターネットにおけるセキュリティ管理に大きな影響を与えている最近の変化について言及し、どのような新たな課題を産み出しているかを述べる。さらに、最近、研究開発が活発に行われている領域について概観し、技術開発の方向性や将来像について述べる。



はじめに

インターネットは社会におけるさまざまな活動を担う基盤環境に成長してきた。インターネットにおけるセキュリティ技術は、この基盤環境を誰もが安心して信頼を持って使える環境を提供するための技術である。ネットワークセキュリティ技術そのものは、1960年代のコンピュータ間でのデータ通信が開発運用されて以来研究開発が続けられている領域である。さらに、1990年代に入ってインターネットが急速に普及するにつれて、ネットワークセキュリティ技術は著しく発展し、現在でも積極的な研究開発が続けられている。

しかしながら、インターネット環境で使われるセキュリティ技術、あるいは、セキュリティ対策を考えた場合に、2001年というのは重大な転換点になった年とい

えるだろう。これに3つの要因を挙げることができる。

■広帯域常時接続環境

1つ目が、広帯域常時接続環境の一般化である。

インターネットとの接続回線を考えた場合、企業や大学・研究所等の法人ユーザの大半はデジタル専用回線を用いた常時接続を使用している。常時接続の場合、外部のインターネット側から常に内部のネットワークにアクセスできることから、外部の悪意あるユーザがさまざまな不正アクセス行為を行う可能性がある。このことから、問題を発生し得るアクセスを阻止することを目的として、ファイアウォールなどのセキュリティ保全機構をインターネットとの接続点に実装するのが当然となっている。

一方、これまでは一般ユーザではインターネット利用形態の大部分がダイヤルアップ接続であり、利用可能帯域は数十Kbpsと狭く、接続も間歇的であり、接続のたびに割り当てられるIPアドレスが変化する。このため、特定のホストを狙いにくく、接続帯域の絶対的な不足によって不正アクセス行為が実施しにくいことなどが理由となって、不正アクセスのターゲットとはなりにくかった。

ところが、昨年からは一般ユーザをターゲットにした広帯域常時接続環境が広がり始めている。この動きは、最初 ISDN サービスにおいてインターネット利用時の定額料金設定から始まり、ADSL、CATV インターネット接続、FWA を利用してマンション等の集合住宅におけるインターネットアクセス集約化、さらに、光ファイバを直接家庭に設備する FTTH (Fiber To The Home) 型接続とい

ったサービスが提供されるようになった。つまり利用可能帯域においても一般ユーザは法人ユーザと遜色のない広帯域での常時接続環境を手にいれることができしまい、結果として一般ユーザにおいても法人ユーザ並みのセキュリティ対策を施すことが必要になっている。しかし、広帯域常時接続環境を手にいれた個人ユーザがその環境に応じた十分なセキュリティ対策を行っているとは現状では言い難い。

さて、2001年は Windows 系OSのセキュリティホールを利用する不正アクセスが蔓延した年であった。この被害にあった一般ユーザのシステムは膨大な数に上り、特に後述する分散型使用不能攻撃を構成するトラフィック生成器として利用されてしまう事例が増えてきている。このため、広帯域常時接続を利用する一般ユーザでのセキュリティ対策の充実が必須となってきている。

■基盤環境への成長

2つ目の要因として、インターネットが社会における基盤環境、いわゆるインフラとして受け入れられたことが挙げられる。

これまでインターネットは、E-commerce に代表とされる商業活動から社会のさまざまな分野での利用が進められてきた。総務省が取りまとめた平成13年度版情報通信白書¹⁾によれば、我が国では従業員300人以上の法人事業所においては、その95.8%がインターネットを利用している状況にある。さらに、個人ユーザにおいても全体の34%がインターネットを利用するというように、急激にインターネットが社会に普及している。このような状況の中で、いよいよインターネットを社会基盤として利用し、行政サービスや、そのほかの社会的な活動で積極的に利用していこうとする動きが本格化している。特筆すべきは、我が国においては2000年秋に「IT基本法」が成立し、我が国が情報通信技術を積極的に利用し、新たな社会を作り出していくための基本的な姿勢が法律として成立したことである。IT基本法では、ネットワークを国民生活を支える重要な基盤環境として認知し、誰もが安心して使用できるための要件と、その実施目標を法律とした。インターネットが社会における基盤環境として機能するようになってきて、当たり前であるが誰もが信頼をおけるようになるために、十分なセキュリティ対策の実施が求められているのは当然である。これはIT基本法第22条においても、「高度情報通信

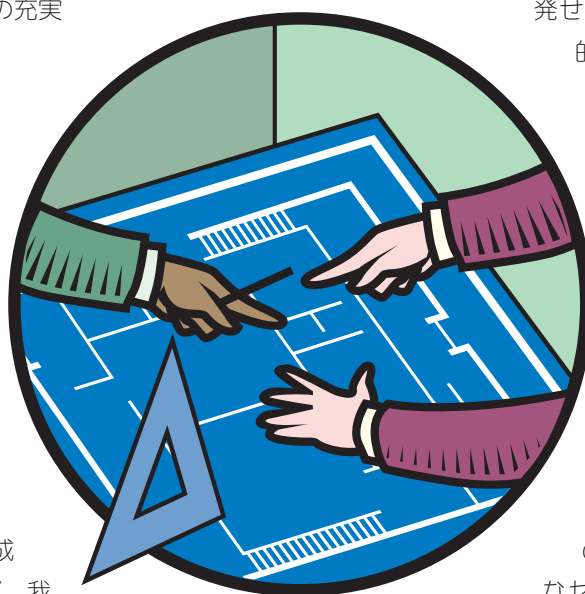
ネットワークの安全性の確保等」として条文を用意し、セキュリティ対策の重要性を訴えている。

しかしながら、実際にインターネット環境におけるセキュリティ管理を十分に行うことも難しい状況にある。1つは、インターネットサービスを提供するISP (Internet Service Provider) において、セキュリティ管理に対する投資が実施しにくい状況にあることだ。これにはさまざまな原因が存在する。サービス価格競争の激化はISPの収益悪化を招いているだけでなく、景気悪化により市場からの資金調達環境の悪化も足を引っ張る形になっており、結果としてセキュリティ機能強化等の直接収益改善に繋がらない投資に対してISPは消極的

にならざるを得ない状況にある。また、データ通信事業者としてのISPにとっては、ユーザから発せられたビットストリームを透過的に到達させることがユーザに提供する基本的なサービスであり、エンドユーザのためのセキュリティ強化は付加価値サービスとして位置づけられることが多い。このため、セキュリティ強化サービスは付加価値サービスとして、ユーザの追加的な費用負担の元を実施されるものだという取り扱いを行っているISPも多い。このようなことから、ISPが追加的なセキュリティ対策を積極的に実施することは、現時点の構造では考えにくい。

一方、この状況を改善させる動きが、インターネット環境での犯罪行為に対する法整備の動きと、サイバーテロ対策である。

2000年2月に成立した不正アクセス禁止法が、現時点での唯一の不正アクセス防止のための法整備であるが、今後さまざまな形で不正アクセスを防止するための法律が整備されると考えられている。特に、2001年春には欧州評議会からサイバー犯罪防止のための国際条約が提示され、現在先進国を含めた多くの国々において批准が検討されている。日本においても、本条約に対しては批准する方向で検討が進められており、批准する場合には必要に応じて国内法を整備する必要がある。また、欧州評議会だけでなく、G8 グループにおいてもインターネット等を用いたハイテク犯罪に対する法的対抗措置を共同歩調を保って整備することが検討されており、我が国もG8メンバー国としてより一層の法整備が進む可能性がある。



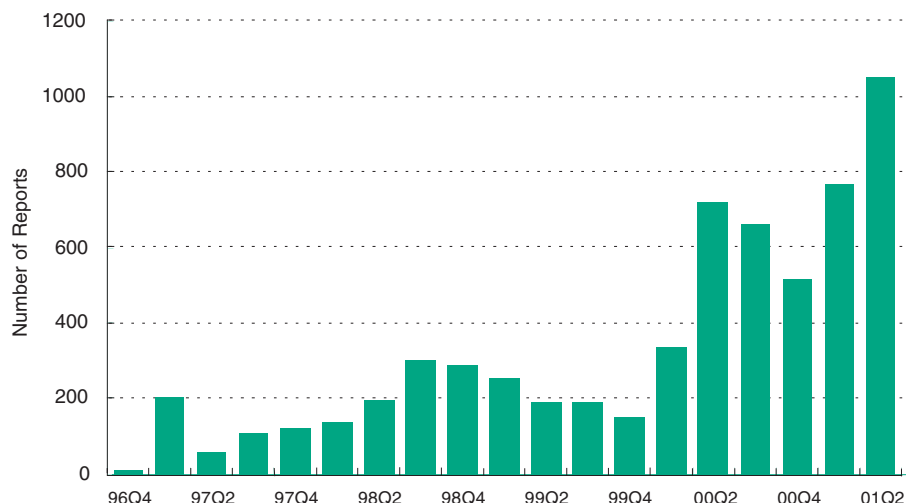


図-1 JPCERT/CC に報告されたセキュリティインシデント数

一方、サイバーテロ対策については、体制が作り出される可能性がある。我々の社会は、高度な情報通信基盤環境を用いており、これらの基盤に対するテロ行為は、社会活動に大きく影響を与えていると考えられている。このため、社会の基礎となっている情報通信基盤環境に対するテロ行為を防止するためのさまざまな方策が検討されている。現状では、インターネットそのものに対するテロ行為について、脅威の洗い出し、実際にテロ行為が発生した場合の影響範囲の同定、さらに、その防止方法を検討している段階にある。たとえば、昨年度より内閣府において重要インフラ防衛のための研究会が開催され、政府内部での検討が進んでいる。

また、テロリストがインターネットを利用する行為に対しては、法的対応が米国を中心に急速に進みつつある。特に、テロリストの追跡と逮捕のために、テロリストたちがインターネットを利用した通信記録を確保するための行為を合法化したり、より簡素化された手続きで可能にしようとする動きが活発になってきている。米国においては2001年9月11日発生した大規模同時テロに対抗するための法整備が行われ、2001年10月末に成立したテロ対策法では、インターネット上で行われるテロリスト達の通信を司法機関がより簡単に捕捉することができるような法改正が行われた。このような動きは、米国以外にも広がるのではないかと考えられている。

■巧みな攻撃の広がり

3つ目の要因として、システムを攻撃する手法の高度化が挙げられる。

2001年は、従来とは異なる攻撃手法を用いたシステムへの不正アクセスが頻発した年である。図-1を見ても分かるように、1999年以降 JPCERT/CC へ報告される不正アクセス件数が急増している。これはインターネットの普及のペースとほぼ同じ形で増加しており、今後のインターネット普及が進めば、不正アクセスもより多く顕在化してくると思われる。さらに、JPCERT/CC へ報告された不正アクセスの解析によって、近年の攻撃手法が従来の手法から着実に高度化されていることが明らかになっている。

現在の不正アクセスの大半は、ツールを用いてほぼ自動化された攻撃が主流となっている。さらに、不正アクセスの手法としては各システムで稼働するサーバプログラムが持つバッファ溢れ (buffer overflow) のセキュリティホールを利用した攻撃が大部分となっている。バッファ溢れを利用した攻撃では、稼働しているサーバプロセスの中に “shell code” と呼ばれるプログラムを埋め込み、shell code を実行させることで、システムにある別のプログラムを実行させたり、外部からシステムシェルに無権限状態のままアクセスしたりすることができる。

2001年には、バッファ溢れを利用してプログラム自身を増殖させる Worm プログラムが不正アクセスで広く使われた。この不正アクセス手法では、Worm を使って複数のシステムに攻撃プログラムを急速に伝播させる。各システムに埋め込まれた攻撃プログラムは、さらに別のシステムに攻撃を行うような構造となっている。

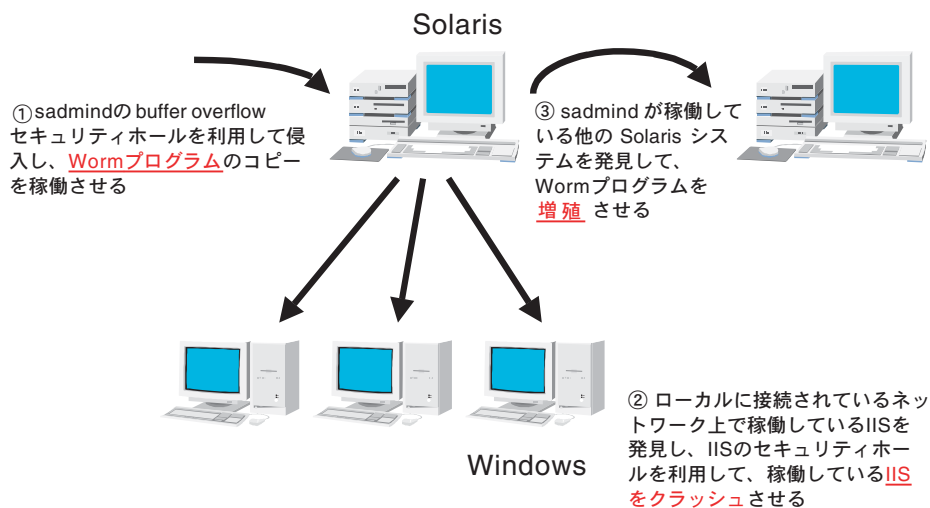


図-2 Solarisの sadmind を利用した攻撃

たとえば、2001年6月頃に流行した Solaris に用意された sadmind を利用した攻撃では、Solaris が稼働するシステムでデーモンとして稼働している sadmind のバッファ溢れを利用した攻撃が広がった。基本的には、sadmind を利用して攻撃プログラムを自己増殖させる Worm が広がり、各攻撃プログラムは、同一ネットワーク内にある Windows システムで稼働している IIS に対して攻撃を仕掛けるというものであった（図-2参照）。このような複数のプラットフォームを利用した攻撃手法が今や一般的になっている。同種の攻撃は、2001年7月後半から流行した CodeRed、さらには、2001年9月に流行を見せた Nimda などでも利用されている。

このような複数のプラットフォームを利用した攻撃は、これまで見られなかった攻撃手法であり、比較的セキュリティホールの存在が多い Windows 系システムに対して攻撃を効果的に仕掛けることができる。さらに、これまで Windows 系システムではネットワークセキュリティ対策よりもウィルス対策が重要な課題であったが、CodeRed や Nimda で明らかになったようにウィルス対策もネットワークセキュリティ対策も区別なく実施しなければならない状況になってしまった。これは攻撃手法の急速な高度化の結果であり、セキュリティ対策を実施する側からは頭の痛い問題である。また、攻撃手法のツール化も短時間に行われるようになり、高度な攻撃手法をいわゆる scripty kids でも行えるようになってきている傾向も顕著である。この傾向は昨年の TFM などのツールの開発の頃から指摘されているが、最近では特に攻撃手法のツール化が積極的に行われている。ツール化の進展は不正アクセスの増加の一因となっている。



セキュリティ技術の開発

急増する不正アクセスに対抗し、より信頼のおけるネットワーク環境を構築するために、さまざまなセキュリティ技術が開発されている。ここでは、最近注目されているいくつかのセキュリティ技術について概観する。

■DDoS対策技術

現在のインターネット環境で最も頭を悩ませている攻撃手法が分散型使用不能攻撃（DDoS 攻撃: Distributed Denial of Service Attack）である。この攻撃は、次のような攻撃手法を用いて行われる。

1. バッファオーバーフロー手法を用いて shell code を埋め込むホストをポートスキャンによって発見する。攻撃者は、発見した侵入可能なホストのリストを作成する。
2. 作成したリストに基づいて、各ホストにトラフィック生成のためのプログラムを埋め込む。埋め込まれるトラフィック生成器は、特定の packets（トリガ: trigger）を受信することで、指定されたターゲットホストに対してトラフィックを生成する。トリガとしては ICMP packets が使われることが多い。
3. 攻撃者は、トリガとなる packets にターゲットとなるホストの IP アドレスを指定して、各トラフィック生成器を仕込んだホストに送りつける。これにより、各トラフィック生成器がターゲットに対して膨大なトラフィックを送り始める。このトラフィックは単純な UDP ストリームや TCP SYN 攻撃を行うようにしてい

る場合もある。

最近のDDoS攻撃には自動化したツールが使われ、一台のトラフィック生成器が用意されるのには数秒しかかからない。また、トラフィック生成器として利用されるホストが数十台から数百台になることもあり、さらに、インターネット接続の広帯域化のために一台の生成器が生成できるトラフィックが増加していることから、分散型使用不能攻撃に狙われたホストでは数百Mbpsものトラフィックを受信することもある。さらに、トラフィック生成では、パケットに書かれる送信元IPアドレスをランダムに生成する Source address spoofing の技法を利用して、送信ホストをカモフラージュすることが多い。このため、最近のDDoS攻撃によって被害に合ったサイトでは、膨大なトラフィックのためにサイトを接続するリンクが飽和してまったくサービスを提供できなくなったり、あるいは、ネットワーク自体は膨大なトラフィックを転送できたがシステム側が対応できずにクラッシュするケースが見られている。さらに、送信元のカモフラージュによって、DDoS攻撃に数日間に渡って晒されるというようなことも発生している。このようなことから、DDoS攻撃は実害を生む攻撃で、かつ、対処が難しい攻撃と考えられてきた。

近年、DDoSに対応するための技術が生れつつある。基本的には、(1) 送信元IPアドレスを偽造した場合に対応する技術と、(2) DDoS攻撃に使われているトラフィックの検出技術を作り出すことを目指している。たとえば前者の技術としては、IP trace back と呼ばれる技術²⁾を挙げることができる。この方法では、注目しているトラフィックについて、そのトラフィックを中継したルータがどのインタフェースから別のどのインタフェ

ースに中継しているかを報告するような機構 (ICMP traceback option) を用いる。これにより、仮に発信ホストIPアドレスが書き換えられていたとしても、順次中継したルータを辿っていくことで、原理的には送信元を発見できる。現在、このような技術開発が行われており、近い将来発信ホストIPアドレスを変更することで行われるなりすましを発見できるような環境が整備される可能性が高い。これ以外にも、Ingress Router Filtering と呼ばれる手法も運用技術としてあり、加入者ネットワークから送り込まれるパケットについて、送信元IPアドレスの値が正当なものかどうかを検査する機構も提案されている。一方、後者の技術としては、QoS管理で使われるトラフィック解析技術を応用して、DDoSを構成するフローを取り出して、ブラックホールインタフェースに流し込むことで攻撃を回避させることが考えられている。実際、DDoSを構成するトラフィック生成器からのトラフィックを実時間で検出する技術はできつつあり、一部のIDSでは実装が始まっている。

■バッファ溢れ対策

現在の不正アクセスでは、バッファ溢れ (buffer overflow) を用いてシステムに侵入するケースが大半である。このために、バッファ溢れを引き起こさない環境の整備が急務となっている。

根本的にバッファ溢れの発生を防ぐには、スタックに積み上げられたプログラムコードを実行できないようにするか、スタックに積み上げられた局所変数の境界検査を行うのどちらかを実装するしかない。しかし前者のような改変を行うと、マルチスレッドプログラムの高速な実行などができなくなるなどさまざまな問題が発生する。このため、バッファ溢れ対策は後者の方法をとることになる。この境界検査は、OSレベルでサポートする方法、境界検査を行う関数群のみを使うようにプログラムを構成する方法、さらに、境界検査を行う特別なライブラリをリンクする方法などがある。しかしながら、これらの手法が広く使われているとは言い難い。これは、OSレベルでのサポートは特定のOS (たとえば OpenBSD) でのみ実現されており特に商用環境で広く使われるには無理があること、境界検査を行う関数だけでプログラムを構成するようにプログラムを指導しても、どの関数を使うかはプログラマに任されており、依然としてプログラマのうっかりミスでバッファ溢れを持つ関数が作られてしまうことがあることなどが大きな原因となっている。

バッファ溢れの問題は深刻であるにもかかわらず、依然として多くのソフトウェアベンダが対応しきれないのは、ソフトウェア開発環境の問題が大きく、バッファ溢れのテスト技術も十分にできていないことにも



原因がある。このようなことから、ネットワークに使用されるプログラムの開発環境を根本的に見直す動きもでてきている。

■IDS

IDS (Intrusion Detection System) は、不正アクセス行為を発見するための機構として、今や広く使われている機構である。

これまでのIDSは、MID (Misuse-based Intrusion Detection) の考え方に基いて構成されており、不正アクセスの特徴を抽出した signature (あるいは footprint) と呼ばれるパターンに合致するアクセスを発見する。この場合、IDSとしての優劣は、収集された signature の量と質に依存する (これはウィルス対策ソフトウェアと同じ状況にある)。このため、現在のIDSベンダの多くは、signature の収集と改善に日々努力している。

さらに最近では、異常状態を発見することを目標とした AID (Anomaly based Intrusion Detection) も実現するIDSも開発が始まっている。たとえば、SRI や U.C. Davis が中心となって開発を始めている Emerald システムでは、AID に基づいた異常状態の検出も目指している。

また、ネットワーク上に分散した複数のIDSを用いて、全体としてより多くの事象を発見しようという試みが行われている。たとえば、使用不能攻撃、IP source address spoofing などが行われている通信などを発見する場合には、単一のIDSを用いるよりも、複数のIDSが連動して検査を行った方が発見確率を高めることができる。このアイディアに基づいて、複数のIDSを用いた分散型IDSの開発も着手され始めている。

■PKIと認証技術

X.509 に基づいた認証基盤、いわゆる PKI (Public-Key Infrastructure) は、電子政府においても基盤技術として使われることから、近年急速に研究開発、および、製品開発が行われている領域である。

これまで X.509 に基づいた認証基盤は、WWW における SSL/TLS を利用したサーバ認証、電子メールにおける S/MIME に基づいた電子証明と暗号化で使われてきた。これが電子政府の推進に伴い、電子署名された公文書の作成、インターネットを經由しての申請業務処理、法人登記における公開鍵登録制度の開始、さらには、国民一人一人にICカードを分け、そのカード内に公開鍵と暗号鍵のペアを保存するようにするという総務省の試みなどが発生している。これらのPKIを用いた行政におけるアプリケーションが実現されてくるにつれて、運用面での課題、特に、電子署名された電子化書類の原本性の確保や、暗号自体の強度確保の問題、さらに

は、他の暗号方式への移行の問題などが浮彫りにされた。これらの問題を解決すべく、さまざまな研究開発が行われるようになっていく。また、法的な面からも、行政サービスにおいて PKI を使う場合の環境整備が積極的に行われている。



おわりに

本稿では、現在のインターネット環境でのセキュリティ対策に大きな影響を与えた要因と、現在のセキュリティ技術の開発動向を概観した。

インターネットが社会に浸透していくにつれて、インターネットそのものへの信頼感の醸成が重要になってくる。これを支える技術がセキュリティ技術であるが、まだまだ多くの課題が残されており、研究開発から、実際の運用環境の構築までを行う必要がある。また、セキュリティ技術の研究開発は、企業が中心に活動を展開する実業的な面が多いと考えている人たちが多いが、依然として学術研究領域であり、実際多くの大学や研究機関が活動を展開している。今後、セキュリティ技術の果たす役割は、今以上に大きくなることが予想されることから、より多くの研究者の育成と参加が必要となっている。本稿が、ネットワークセキュリティの技術開発を担う人たちの助けになれば幸いである。

参考文献

- 1) 平成13年度版情報通信白書、<http://www.soumu.go.jp/hakusyo/tsushin/index.html> より閲覧、および、PDF 版ファイルのダウンロード可能、総務省。
- 2) IP Trace-back 技術については、米国ワシントン大学の Web ページに関係論文がまとめられている。
<http://www.cs.washington.edu/homes/sagade/traceback.html>
(平成13年11月12日受付)

