インターネットのセキュリティ問題とＪＰＣＥＲＴ／ＣＣ

(Japan Computer Emergency Response Team Coordination Center)

１.はじめに -この一年をふりかえって-

インターネットの拡大と普及が進むにつれ、インターネットにおけるさまざまな不正アクセス行為が重大な被害をもたらす可能性が現実のものになってきています。

JPCERT/CC（コンピュータ緊急対応センター）は、JEPG/IP におけるボランタリーベースでの活動を経て、1996 年 10 月より National IRT(Incident Response Team:緊急対応組織)として設立され活動してきました。

これまでの緊急対応活動では、設立から 1997 年 9 月末までに 383 件の被害報告を受け付け、さまざまな対応活動を行ってきています。また、JPCERT/CC では届出を受けた不正アクセスの内容を検討し、インターネットを経由した不正侵入、破壊、妨害、またはそれを目的とした不正アクセスでその影響が広範囲に及ぶ可能性があると判断した問題に対しては、インターネットコミュニティに対する警告を流してきています。これまでに、sendmail,INN,phf,IMAP サーバ を利用した広範囲の攻撃に対する警告と技術情報を WWW サービスより提供しています。

また、JPCERT/CC では、セキュリティ情報を迅速に流通させるためのメーリングリストの運用も行っています。さらには、利用者や管理者のための啓発活動として国内で開催される会議、イベントなどでセミナーやチュートリアルを行ってきています。

これ以降では、頻発するセキュリティ問題の傾向と、JPCERT/CC の活動の方向性などについてご報告いたします。

２.最近のセキュリティ問題の傾向

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てしまうこと (踏み台) が多く発生しています。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) もしばしば発生しています。

特に、一般ユーザを含めて認識して頂きたいポイントとして、以下のものがあります。

(1) 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による不正侵入は依然としてかなり多く発生しています。ネットワーク環境が急速に広がった結果、十分に管理されていないシステムが増える傾向にあり、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が十分に行われていないシステムに侵入されるようなケースが多く発生しています。

(2) 踏み台攻撃

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など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試みます。そして、ほかのシステムに対する新たな攻撃を開始されてしまうことになるのです。このような攻撃を踏み台攻撃と呼んでいます。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ことになります。また、踏み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、攻撃者は踏み台攻撃を行うことが多くなるのです。自らのシステムの管理上の不備によってインターネットコミュニティ全体のセキュリティ問題を増幅し深刻にさせているのです。

(3) 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ます。特に、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っています。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には流行があり、似通ったツールが使われることが多くなります。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くなります。管理者の方々は、常にセキュリティホールに関する情報を入手し、ソフトウェアの更新に心がけておく必要があります。このためには、既存の管理体制を強化することが必須になります。

(4) 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) があります。例えば、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す。サービス不能攻撃は、インターネットのみの問題ではなく、一般にどの種の通信システムにおいて

も発生し得る攻撃です。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はなく、攻撃者の発見も困難を極めます。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、その防止を如何にして実現するかが課題となっています。

３.今後の活動の方向性について

JPCERT/CC は、IRT が基本的に提供すべきサービスを、限られたリソースの中から提供してきています。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になってきています。

また、JPCERT/CC は長期的に安定した活動を継続していかなければなりません。このため、インターネットコミュニティにとって信頼できる組織としての中立性や公平性の確保のために、組織運営のオープン化や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要になってきています。

このためにより多くの資金ソースの中から運営資金を確保し、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計画しています。これらの組織改革は、可能な限り早期に実施し、早い段階で活動に生かせるようにしていきたいと考えています。