特集・情報ネットワーク講演会（第4回）より

インターネットとセキュリティ

中野厚史*

1. インターネットの現状

インターネット, WWW (World Wide Web) などと云った言葉は, たった二年ほど前までは, 大学や研究所もしくはコンピュータを趣味・職業にしている人の間でしか通じない言葉でした. ところが, 昨年暮れの流行語大賞にもノミネートされ, またここ数カ月のTV・新聞を始めとするマスコミでもインターネットという言葉を見かけない日はありません. コマーシャルを見てもコンピュータ関係・情報関係の会社が Home Page やインターネットがらみの広告を出しているのみならず, 化粧品・食品会社等のコンピュータとは無縁の会社の新聞・TV 広告にさえ「当社のホームページの URL は....., eMail address は.....」といった文字が頻繁に見られるようになってきました. これはインターネットという先進的なものにも企業として取り組んでいるという企業イメージのアップといった面もありますが, 情報の受け手としてのインターネット人口の増大および, メディアとしてのインターネットが根付きはじめたといえます. 企業サイドとしても, ホームページの設置は他のメディアよりも有利な面もあります. というのも, 昨年あたりまでの, インターネット上での広告・アンケート, 求人広告等はコンピュータを利用する人を対象にしたものが大半でしたが, 最近のインターネットばかりによって, 流行に敏感な人を対象にアンケート調査が可能なメディアとして利用され始めているようで, 懸賞商品等と上手に組み合わせてアンケート等を行っている様にも感じられます. こうした既存の企業のインターネットへの進出とは逆に, イ

ンターネットなかから生まれてきた企業もあります. 例えば, 玉石混濁な情報の洪水であるインターネットの中から自分に必要な情報を得るのは簡単なことではありません. そこで, 検索サイトの登場となるわけですが, これをビジネス化した人々がいます. インターネット上の各種情報を検索するための場所はインターネットの利用者は必ず利用するサイトになるので, そこに各企業からのバナー広告を集めることによって企業として成立させております.

実際にまどのくらいのコンピュータがインターネットに繋がっているのでしょうか? インターネットに接続されているホスト数は現在1,000万台を越えており, 利用者はその数十倍はいるといわれてお

図ー1 検索サイトの例 バナー広告が見られる
http://www.yahoo.co.jp/Science/Ecology/

* 国立循環器病センター研究所

Atsushi NAKANO, e mail : nakano @ ri. ncvc. go. jp

図-2 インターネット上のドメイン数
<http://www.nw.com/zone/WWW/report.html>

図-3 デジキャッシュに関する記事
<http://opendoors.asahi-np.co.jp/sp0929/spe/index2.htm> Fire Wall FAQ
<http://www.v.one.com/pubs/fw-faq/fag/.htm>

ります。しかも、現在もなお増加の一途を辿っております。また、最新のある統計に因ると WWW の Home Page の数は53日で倍増しているという報告もあります。

このような指数的ともいえるインターネット人口

の増大は、インターネットを数年前までの「限られた・良識のある・研究目的」のものから「日常的な・個人を対象とした・商用を含む目的」へと変貌を遂げてきています。例えば電子メール (eMail) は直接相手のコンピュータに直接電子可読な文字情報やファイルを IP reachable な場所であれば世界中のどこでもほぼリアルタイムに送ることが可能です。電子メールを利用しはじめると、従来の他の通信手段 (通常の郵便や fax) が面倒に思えてくるほどです。しかしながら、電子メールはその認証性の面で問題がないわけではありません。一人一台以上のコンピュータ環境で、そのコンピュータをその人しか利用しない状態ならばいいわけですが、多人数で共用する場合には、他人の私信を覗くことや他人の名前で誹謗中傷をすることもできないわけではありません。つまり、まったく他人のふりをして eMail を発信することすら可能なわけです。そして、手紙や fax と違い筆跡がありませんから簡単には判別することができません。それだけではなく、インターネット上を流れるメールやその他の情報を途中で盗聴することも技術的にはそれほど困難ではありません。

確かに、インターネットは地理的距離をなくし、ますますボーダーレスな社会を形成しつつあります。そして新しいビジネスや既存のビジネスに様々な局面を加えていくことになると思います。近年インターネットを利用した商取引、つまりエレクトリックコマース (電子商取引) やデジキャッシュ (電子通貨) などのもそろそろ実用化され始めました。商取引以外にも各国毎の風習やモラルの違いによる様々な問題もこれから発生してくると思われます (アダルト映像のサーバーの摘発は記憶に新しい所ですが、これも現在は海外にサーバーを設置するケースが増えている)。

インターネット上の必要以上の規制は必ずしも必要だとは思いませんが、こういった問題以外にも、インターネットから企業に侵入してそのデータを悪用することや、インターネット上のデータを改竄する事などといった、新たな犯罪も生み出しております。今後ますますインターネット化していくにつれ、社内や所内のネットワークの外部からのアクセスに対するセキュリティや各個人のパスワード等の管理は、ネットワーク社会に生きる人間として個人個人が、常識としてもっていくべきだと思っております。

2. インターネット上の脅威

さて、実際のコンピュータ・ネットワークでのセキュリティ上での脅威としてはどんなものがあるでしょうか？

大別すると、

- ・ホストコンピュータやネットワークの安定した稼働を妨げるもの。
- ・ホストコンピュータ内やネットワーク上を流れる情報を不正に破壊、漏洩、改竄するもの。

に分けられます。

第一の「ホストやネットワークの安定した稼働を妨げる」手法としては、大量の mail を送りつけたり、ping 等を連続的に行うといった極めて単純なものから、コンピュータウィルスの類を用いてシステムやネットワークを不安定にさせるといったものがあります。

第二の「破壊・漏洩・改竄」を一般にインターネットの三悪と呼んでいる。上でもあげたウィルスによるシステムやネットワークを破壊することから、単純に他人の eMail やパスワード、クレジットナンバー等の機密情報を覗き見や改変する場合、他人になりすましてネットワーク上でいたずらや破壊行為を行うといった類のものまで様々なものがあります。

3. 現実の事件

これまで発生した事件をいくつか紹介すると、1988年11月 Robert Morris によって放たれたインターネットワームがかなり規模の大きなものとして有名です。これはマシンのセキュリティホールを手がかりにパスワードクラックを行い侵入し、CPU パワーの食い潰しを目的としたワームでした。ただ、不幸中の幸いともいえるのがシステムの破壊行為は行わなかった点です。しかしながら、2,000~6,000 台の Sun, VAX が一夜にして麻痺しましたが、ほぼ一週間後には収束したと報告されています。

また、自分のコンピュータから他の組織のコンピュータに入り込み、そこの組織の人間のふりをして犯罪を行うというケースも多々報告されており、有名なものとして、Kevin Mitnick の事件があります。これはアドレスの詐称やコネクションのハイジャックなど、巧妙な手口を用いて約 2 万人のクレジットカード番号を盗み不正に利用したというも

のです。この事件の解決には、下村努氏の多大なる努力がありました。

こうした事件は対岸の火事でしょうか？ 決してそうではありません。確かに、これまで日本国内で大規模な事件は表面化していません（企業は公表しない場合がほとんどであるため）が、インターネットには国境という壁は全くありません。さらに、インターネットがここ一年で急速に成長した日本は、クラッカー達の格好の標的となっている感もあります。実際、たくさんの攻撃は受けていてもそのときには発見できず、他の組織からこの時期おかしくなかったかとの報告を受けてコンピュータのログを確認すると確かに不審な行動があったということに気づくことも多々あるようです。さらに、海外での事件の踏み台にされたケースも報告されています。特に企業に比べてセキュリティの弱い研究・教育機関は格好の「ちょっかい」の対象になっております。

次に問題になるのが、こうした攻撃や被害を受けたときにどこに届けばいいのか？ という問題です。まさか、交番に届けるわけにもいきません。実際ネットワークの先進国である、米国には CERT や CIAC といった、コンピュータやネットワークの安全を脅かすような事態に対処べく作られた組織が存在しており、各種コンピュータのセキュリティホールやインターネット上の事件なども詳細にレポートされておりますが、日本ではまだまだ JPCERT 設立が準備段階でしかなく、wide プロジェクトの有識者たちに協力を求めるというのが現状での回答でしょう。

4. 防御の考え方

まず、「何を守る必要があるのか？」を組織で十分考える必要があります。何を禁止し、公開するのか？

そして、外部からのログインをどのような形態で許すのか？ さらには通信の管理をどこまで行うのか？ を十分検討する必要があります。こうしたセキュリティのポリシーは、大学・研究機関・企業といった業種でも異なってきますし、またその内部で扱う情報が、学術研究であるのか、メール等の私信であるのか、また上にもあげた商取引や、医療情報の様に機密性の高い情報であるのかに依存します。

ここで気をつけなければいけないのは、「うちには守るべきものがないから。」といって全くセキュリティをしないのも前述したように踏み台として利用さ

れる可能性もあります。また、一般に防御には金銭的にも人的にもかなりコストを要します。ある意味での完全なセキュリティはインターネットに接続しないこととなってしまいます。実際一部の企業では社内には2種類のネットワークを設置して、一方はインターネット接続用、他方は社内研究開発用と完全に分離させているケースも聞かれます。一般には内部に存在する、守るべき対象の重要さとインターネットによる利便さ、ファイヤーウォールによる不自由さを天秤にかけてその組織でのセキュリティポリシーを決定していく必要があります。近年は以前にもましてファイヤーウォールの重要性が叫ばれておりますが、実際自分のサイトにどの程度のセキュリティが必要かを十分見極めて設定する必要があります。

5. ファイヤーウォール

ファイヤーウォールとは、内部のネットワークとインターネットとの接続点に緩衝用セグメントを設置し、そこにあるルータやマシンに対して集中的にセキュリティ対策を行う手法の総称です。実際問題としても、数百台にも及ぶ内部ネットワークのすべてのマシンに対して、一定のセキュリティを保つことは労力的な限界もあり事実上不可能です。

もっとも単純なファイヤーウォールは、インターネットとの接続点であるルータで外部からの危険な

パケット (RPC, NIS, NFS...) を切る方法が用いられます。大学や研究所等で、各研究室レベルでWWWの発信を許可する場合にはこういったシステムになってしまいます。ただこの場合でも Telnet などの外部からの login には安全な使い捨てパスワードを利用することが推奨されます。

企業などの場合では、ファイヤーウォール上に外部からのアクセスの必要なホストだけを設置し、内部から外部には直接のアクセスは許可せず、これらのファイヤーウォールホストを介してアクセスをするという構成を良くとります。中継ホストで、こういったアプリケーションを通過させるかを設定する手法です。従来この方法では、マルチメディアアプリケーション (RealAudio や StreamWorks) が通過しないという問題がありましたが、近年徐々に解決されてきております。最近では、ファイヤーウォールとともにプライベートアドレスを用いるシステムも同時に動作させることが多くなりました。これはインターネット人口の急増とともに IP アドレスの枯渇が問題となっていますが、ファイヤーウォール上で内部のアドレスが外部に出ないようにしてやることによって、内部に自由にプライベートアドレスを使うというものです。こうしたファイヤーウォールシステムにも問題がないわけではありません。セキュリティを厳重にすればするほど内部としては使にくくなるわけですし、アプリケーションやパケ

図-4 MacPGP の使い方
<http://www2.escosys.co.jp/~tsuruta/pgp/>

ットを監視してフィルターするわけですので外部との速度も低下といった問題も近年の高速ネットワークシステムでは問題となってきています。

6. 暗号化技術

ファイヤーウォールと並んで重要なセキュリティ技術として電子メールの暗号化があります。これは電子メールに対する暗号化により、盗聴・改竄を防ぐ目的と電子署名による偽称を防ぐ目的があります。暗号化には公開鍵暗号化と秘密鍵暗号化があり、これらを組み合わせることによって現在用いられ始めている PGP (pretty good privacy) やさらに公証局を使うことによって身元証明まで行える PEM (privacy enhanced mail) 等のシステムがあります。

しかし、こうした暗号化技術は米国連邦政府による輸出規制の問題や、万能 Key の問題等解決してい

かなければならない問題がいくつもあります。

これ以外にも Telnet に暗号化したものも開発されておりますし、ファイヤーウォールのところに暗号化装置を設置し、企業の支店間を結ぶ様な手法も実用化されております。さらに、IP の枯渇問題は先にふれたが、現在 IPv6 と呼ばれる拡張 IP が検討されておりこのシステムでは IP Packet そのものに対する暗号化も実装されることになっております。

最後に

インターネットはまだ未成熟の社会です。やはりエンドユーザー一人一人のセキュリティ意識：「家に戸締まりする感覚でのセキュリティ、封筒に糊付けする感覚での暗号化」が、インターネット社会でのセキュリティを高める上でもっとも重要なことに違いありません。

環境計測・分析分野への入門書として最適です。

わかり易い最新の 環境計測・分析技術講座

A 5 判 137 頁 定価 3,900 円 (本体 3,786 円) 送料 350 円

☆環境計測や分析業務に従事しておられる技術者へ

最新の技術をより深く理解するために
★その他環境関連分野でご活躍の方へ
計測、分析で得られた情報を
十分活用するために

【編集】宗 森 信 大阪府立大学名誉教授
日 色 和 夫 京都教育大学教授

【内容】第1講 イオンクロマトグラフ法
第2講 フローインジェクション分析法
第3講 ICP発光分光分析法
第4講 バイオセンサー
第5講 マススペクトル分析法
第6講 機器的放射化分析法
第7講 分析データのとり方

発行 環境技術研究協会
TEL : 06-357-7611
FAX : 06-357-7612