インターネットのセキュリティ技術

1.インターネットとセキュリティ

インターネットで安全性がこれまで重要な課題として広く問題になることはなかったのは、インターネットがもともとは学術用のネットワークとして発展してきた歴史を持ち、そこではセキュリティよりも自由なコミュニケーションによるオープンな情報共有に重きが置かれていたからである。

しかし、商用ネットワークが登場しインターネットが爆発的に成長を遂げている現在、そこでは実社会と同様の活動が行われるようになってきている。インターネットに多数の民間企業などがつながり、重要な情報にアクセスできるようになると、侵入などの行為を組織的に行う犯罪者（cracker*）も現れてそれに対する備えが必要となってきた。またインターネット上でのオンライン取引に対する期待が高まるとともに、暗号化や認証といった技術に対する要求も高まっている。

cracker
ネットワークを利用して犯罪行為を行う悪意の侵入者に対しては、cracker（crack=砕く）という呼び名を使う。この意味でハッカーを使うのは誤り。

後述するように、ネットワークのセキュリティを守るための基本的な技術はすでにあるといってよい。しかし、そうした知識や技術を普及させ、またそれを実効あるものとするためには、まだまだ多くの努力が必要である。現状では、セキュリティ技術を正しく理解して適用するのは簡単とはいえないが、努力して対策を施せば、十分安全にインターネットは利用することができる。

2.セキュリティの考え方

インターネットに接続するにあたってまず大事なのは、技術的な問題を議論する前に、セキュリティについての運用方針（セキュリティ・ポリシー）を確立することである。そもそもインターネットを使って何をし、また何を守らなくていけないのかがはっきりしていなければ対策を立てることはできない。

ひと口にインターネットの利用といっても、大学、非営利研究機関、企業の研究開発部門、企業の事業部などその立場はさまざまである。まず、何をどのレベルまで守る必要があるかを明確にする必要がある。場合によっては組織内の部門によって防御の必要性のレベルが異なり、それに対応した対策をとらなくてはならない場合もあるであろう。

次に重要なのは、セキュリティと利便性は二律背反ということである。泥棒を防ぐために家に鍵をたくさん付ければ安全性は確かに増すが、家族が出入りするためには面倒になる。インターネットの安全も、

セキュリティ×使い易さ=コスト（技術）

の公式で表せるように、セキュリティと使い易さの両方を完全に満足させることはできない。セキュリティ対策を導入する際は、この使い易さが損なわれる部分があるという点をよく評価してユーザーにも納得してもらう必要がある。危険を恐れるあまりインターネットに接続しないというのも、本末転倒である。インターネットに接続するにあたっての危険は、正しい知識を持てば十分に評価および

コントロールできるものだ、という認識を持つことが大切である。

ここで、先の公式の右辺は一定値ではないことに注目してほしい。コストをかければ、ある程度は安全性と利便性を両立させることができる。この場合のコストには、セキュリティ対策に必要なハードウェア・ソフトウェアのような直接的なコストだけでなく、組織内でのセキュリティのマネージャーの育成や教育・啓蒙活動などの間接的な要素も含む。むしろ長期的には間接的な部分の方が大きくなるかもしれない。

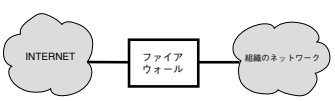
以上のような点に配慮して、その時点でベストと思われるセキュリティ対策を導入したとしても、バグのないソフトウェアがないように、完全なセキュリティ対策というものはないことも理解しておく必要がある。侵入者の手口が高度化して新たなセキュリティ上の問題が生じる場合もあるし、運用上の齟齬（そご）で問題が起こるケースもあり得る。セキュリティを保ためには、継続的に努力する必要があり、それにはコストがかかるということである。

3.ファイアウォールによる防御

インターネットの基本的なモデルは、インターネットに接続しているすべてのコンピュータの間で直接の通信ができる、すなわちコネクティビティがあることを前提としている。組織のLANをインターネットに接続すれば、WWWなどで世界中のコンピュータに自由にアクセスすることができるわけである。これは裏を返せば、LANに接続されているコンピュータがインターネットからの攻撃を受ける可能性があるということでもあり、これがインターネットのセキュリティが弱いといわれる一因となっている。

最近のようにワークステーションやPCが安価になり、1人1台の環境が普通になってくると、多数のコンピュータをきちんと管理することはきわめて困難である。新米のユーザーにセキュリティ対策を期待することはできないし、有能で献身的な管理者がいたとしても、彼または彼女が面倒を見られるコンピュータの台数には自ずから限度がある。

そこで登場したのが、ファイアウォール（防火壁）の考え方である。内部（組織内のLAN）と外部（インターネット）を接続する部分に情報の壁を設けて、外部と内部の間のアクセスをその壁の所で制限することによって、内部のコンピュータの安全性を高めようという方法である。



ファイアウォールによって組織内のネットワークを防御

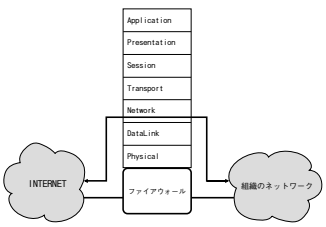
インターネットへの接続の必要上、外部から直接アクセスできることが必要なネームサーバーやメールサーバー、あるいはWWWなどの情報提供などの機能を果たすコンピュータについては、ファイアウォールの外に設置をするか、内部に中継する仕組みが必要である。しかし、そうした外部に対してむき出しのコンピュータは高々数台程度に抑えられるから、きちんと管理して集中的に守ることは十分に可能である。

どのレベルのアクセス制限を行うかは、組織のセキュリティポリシーから決定

されるべきものである。前述のように安全性と利便性はトレードオフの関係にある。ファイアウォールの技術の要は、安全性を維持しながらいかにサービスを提供するかにあるわけであるが、もちろん万能ではない。ファイアウォールによって何が失われるのかをよく評価して、その導入を決定する必要がある。

4.ファイアウォールの構成

ファイアウォールというものは、単一の製品や技術を指すものではなく、さまざまな技術を組み合わせて、ネットワークの安全性を高めるための総合技術である。その性格上、単にファイアウォールの部分だけでは完結せず、IPレベルの接続性からアプリケーション、オペレーションのレベルまでインターネット接続のすべての側面に関わりが生じる。それだけに、ネットワーク全体のデザインをよく考慮に入れて、ファイアウォールの導入は進めなくてはならない。



ファイアウォールが関わるインターネット接続のレベルを考慮する

ファイアウォールを構成する要素としてはルーター、デュアルホーム・ゲートウェイ、そしてその他のサービスホストなどがある。ルーターは一般にインターネットとの接続の部分に使われるが、多くのルーター製品はある程度のアクセス制限の機能を持つ。ルーターだけで本格的なファイアウォールを構成することはできないが、簡易もしくは補助的にルーターのアクセス制限を利用することはよく行われる。

デュアルホーム・ゲートウェイはイーサネットなどのネットワークインターフェイスを2枚持ち、それぞれ外部接続のセグメントと内部接続のセグメントに接続されて、ファイアウォールで中核的な役割を果たす。内と外のあいだの通信はすべてここを通過しチェックやアクセス制限が行われる。また、内と外のサービスを中継する仕事もデュアルホーム・ゲートウェイ上で行われることが多い。

さらに、デュアルホーム・ゲートウェイ以外にもホストが外部接続のセグメントに置かれる場合もある。これらのサービスホストは、ファイアウォールの他の構成要素と連携して、中継サービスやインターネットサーバーの機能などを果たす。もちろん、これらの外部から直接アクセスできるホストについては常にも増して厳重に管理（要塞ホスト化）する必要があり、一般的な注意の他にも、たとえば管理者以外のアカウントは作成しない、必要のないデーモン*や機能はすべて停止しておく、などの対策も必要であろう。

デーモン（daemon）
UNIXシステムのバックグラウンドで、1つのタスクを実行するプログラム。通常は待機状態にあり、必要に応じて処理をスタートする。

5.パケット・フィルタリング

ファイアウォールは、内部と外部の間でIPパケットをフォワードするものと、しないものの2つのタイプに分類することができる。前者をパケット・フィルタリング、後者をアプリケーション・ゲートウェイと呼ぶ。パケット・フィルタリングではIPパケットの通過を（送信元アドレス、ポート番号、送信先アドレス、ポート番号）の組み合わせで許可または禁止する。許可されたパケットは直接宛先のコンピュータに届く。パケット・フィルタリングは柔軟な設定が可能なのが

特徴で、たとえばインターネットで新しいアプリケーションが登場したときに（本当に安全かどうかは別問題であるが）対応はしやすい。

また、処理のオーバヘッドが少なく、ファイアウォールを入れたことによる速度の低下が少ない。反面、正しい（安全な）設定をするにはプロトコルに関する知識が必要で、IPパケットを一つひとつ独立に検査するという性格から、単純なフィルタリングではうまく対応できないケースもある。

パケット・フィルタリングはルーターで行うことも可能であるが、通常のルータのアクセス制限の機能は設定も煩雑であり、またログをとることができないため、設定が正しいかのチェックがしづらいという欠点がある。そのため、あくまで補助的なものと考えておいたほうがよい。ワークステーション上のソフトウェアとして実現されたパケットフィルターとしては、DECで開発されたフリーソフトのscreend、商品としてはCheckPoint Software社のFireWall-1などが代表的である。

6.アプリケーション・レベル・ゲートウェイ

IPパケットのフォワードを行わず、上位層での中継サービスを提供するタイプのファイアウォールを、最近ではアプリケーション・ゲートウェイタイプのファイアウォールと総称して呼ぶことが多い。

昔から「出島ホスト」方式のファイアウォールというものがあり、外に出るにはいったん出島ホストにログインしてからtelnetやFTPをするというやり方はポピュラーであった。アプリケーション・ゲートウェイも機能的にこれと似ていなくもないが、大きく異なるのは、ゲートウェイのマシンのアカウントにログインはしないで中継を行うことである。そのため、いったん接続した後では、たとえばインターネット上のanonymous FTPサーバーから直接手元のマシンにファイルを転送することができる。ゲートウェイ上のマシンに弱点となるユーザーのアカウントを作成する必要はないというメリットも生まれる。

利用者の観点からは、クライアントを使用するときにファイアウォールの存在をいちいち意識する必要があるかどうかが重要である。WWWのhttp proxyなどの場合は、最初にクライアントでプロキシサーバーの設定を行えば、その後ユーザーがそれを意識する必要はない。それに対してFTPやtelnetの場合はそのような仕組みはないので、ユーザーがいったんゲートウェイに接続して、改めて接続したいドメイン名を入力するという二度手間が必要となる。これは、アプリケーション・ゲートウェイの弱点の1つである。

FTPなどのクライアント側でファイアウォール対応と称して、この手間を自動的に処理してくれるものもあるが、ファイアウォールごとに処理は違うので万能とはいかない。この問題を解決するために、最近の商用ファイアウォール製品では、transparent proxy（透過プロキシー）とよばれる技術が採用されているものが増えている。これは、telnetやFTPのパケットを検出して、対応するプロキシ

サーバーを自動起動して対応させることによって、ユーザーには中継サーバーの存在を意識させない手法である。

アプリケーション・ゲートウェイは、アプリケーション層まで見て処理をするので、パケットレベルでの細工をしてくる侵入手口を未然に排除できる可能性が高い。また場合によってはプロトコルの内容にまだ立ち入った細かいコントロール、たとえばFTPのgetは可能だがputは駄目といった制御をすることもできる。その代償としてオーバーヘッドが大きく、高速な回線（6Mbps以上）でインターネットに接続している場合や、組織内のLANとLANの接続に使用する場合は、その性能評価を十分に行う必要がある。

一般的には、アプリケーションゲートウェイ型のファイアウォールは、セキュリティを重視し、その代わり使えるアプリケーションは電子メールとニュース、WWW程度で十分と割り切れるような場合に適しているといえる。もちろん、お仕着せではなく設定変更やソフトウェアを追加するなどすれば、より多くの要求に対応することは可能であるが、それには十分な技術的検討が欠かせない。

また、アプリケーション・ゲートウェイの場合、IPパケットを直接中継しないので、内部のアドレスは外部に直接見えない。したがって内部にはNICから正式に割り当てを受けたglobal address*ではなくprivate address*を使用することができる。昨今のようにIPアドレスの枯渇が問題になり、その浪費を抑制しなくてはならない状況では、private addressを利用するためにファイアウォールの設置が必要となるケースも増えてきている。

global address
NIC（Network Information Center）から割り当てを受けた世界で唯一であることが保証されているアドレス。

private address
インターネットと直接接続しないネットワークで使用するために予約されているアドレス。

7. 電子メールのセキュリティ

現在普通に利用されているインターネット電子メールには、セキュリティのための機能は組み込まれていない。原理的には、盗聴や改竄（ざん）や第三者になりすましてのメール送信などが可能である。もっとも実際には盗聴行為などに遭う危険は、たとえば通常の加入者電話が盗聴される危険と比べてとりわけ重大であるとはいえない。プロバイダーの設備やデジタル専用線に物理的にアクセスすることは簡単ではないので、電子メールの配送経路の安全性はかなり信頼できるとも考えられる。しかし、データがデジタルであるという性格上、いったん盗聴行為が仕掛けられると非常に効率良く大量のデータが盗み出される可能性があるし、電子メールが到着して蓄積されるサーバーに侵入されると個々のメールのプライバシーを守れないという弱点もある。

さて、そういう実質的な安全性は別としても、インターネットがリアルなものになってくると、現実世界の書留郵便に相当する仕組みが、電子メールでも必要というのは当然のことである。それに応えるのが暗号化電子メールである。暗号化電子メールの目的は、3つある。まず、本文を暗号化することによって盗聴を防ぐことである。次にチェックサム*を付けることによって内容の改竄が行われた際にそれを検出できるようにする。3つ目は電子署名を添付することによって、

チェックサム
データに、ある一定の演算をほどこして、もとのデータ量よりもずっと少ないデータでそのデータの特徴をあらわせるようにした指標。

差出人を間違いなく特定できるようにすることである。

実際に、暗号化メールのソフトウェアとしては、PGP（Pretty Good Privacy）やPEM（Privacy Enhanced Mail）といったものが開発され、UNIXやPCの上で利用できるようになっている。これまであまり普及しなかったのは、良いユーザーインターフェイスがなかったことと、後節で述べるような暗号・認証技術の問題点があったからである。が、そうした問題も解決しつつあるので、今後は本格的な普及が期待されている。

暗号化電子メールで使われているのは2の暗号技術の組み合わせである。1つは米国政府が標準的に採用しているDES*に代表される、送り手と受け手で共通の鍵を使う秘密（共通）鍵暗号である。これは、メール本文の暗号化に使われている。共通鍵暗号だけでは、送受信する間であらかじめ別の手段で鍵の交換を行わなくてはならないので、不特定多数の間のメールのやり取りには使えないというジレンマがある。

DES
Data Encryption Standard = 米国政府が標準的に採用している秘密鍵暗号。鍵の長さは 64 bit (実効 56 bit)。

この問題を巧妙に解決したのが、RSA*に代表される公開（非対称）鍵暗号である。公開鍵暗号では、2つのペアの鍵を生成し、そのうち1つを公開してしまう。ペアの一方の鍵で暗号化したデータは、もう一方の鍵でしか復号化することはできない。したがって、送り先の公開鍵で暗号化して送ればそれは送り先が持っている秘密鍵でしか解読できない。この仕組みをつかって、本文の暗号化に使う秘密鍵やチェックサムなどを送るというのが暗号化電子メールの基本的なアイデアである。電子署名も、ある人の秘密鍵で暗号化したデータがもしその人の公開鍵で解読できたら、それは間違いなくその人が暗号化したデータだという特性を利用している。

RSA
開発者3名 R.Rivest.A.Shamir,L.Adlemanの頭文字をとった公開鍵暗号。もっとも広く普及している公開鍵暗号である。RSA Data Security社がパテントを持っている。

8.WWWのセキュリティ

インターネットをこれだけ普及させるきっかけとなったのは、いうまでもなくWorld Wide Webである。したがって、その上でオンラインショッピングや契約ユーザー向けの情報提供などを行いたいという要望は早くからあった。ところが、WWWでやり取りされるデータについてはいっさい暗号化などはされていなかった。これがために、インターネットでオンラインショッピングをする際にクレジットカードの番号を送ったりするのは危険であるという常識が定着してしまった。

しかし、インターネットのWWWのやり取りでクレジット番号を送るのと、誰が目にするのかわからないFAXでそれを送るのとどちらが危険であろうか？　また、インターネットで送ろうが、店頭で本人が使おうが、良からぬ店ならカード番号を悪用されることは同じである。そう考えると、実際的には過度に心配することもないように思われる。問題はむしろクレジットカード会社がまだインターネット上での取り引きに対して対応体制ができていないことかもしれない。

インターネット上の使用で被害にあった場合、カード会社による保証が適用さ

れない可能性があるし、カード会社によってはそもそもインターネット上での利用を認めないところもある。そのあたりはルールが確立するまでは自己責任でやってくださいということになるのであろう。

それはさておき、本格的なオンラインショッピングのへの活用にはやはり暗号化や認証・決済の仕組みが必要である。ここでも使われる基本的な仕組みは暗号化電子メールと同じく、公開鍵暗号と秘密鍵暗号の組み合わせである。WWW Consortiumの提案するshhtp（secure http）とNetscape Communication社のSSL（Secure Sokcet Layer）に加えて、やや遅れてMicsosoft社からSST/PCTというプロトコルが提案されている。

すでにNetscape社のSSLに対応したコマースサーバーとブラウザーによる暗号化はかなり利用されるようになってきているが、現状ではまだどの方式が主流になるかはわからない。それぞれの陣営がクレジットカード会社などと連携して、De Fact Standardとするべく勢力拡大を図っているという状態である。プロトコルの乱立はユーザーの利益にはならないが、1つのブラウザーが複数のプロトコルに対応することは可能であるので、独占よりも競争があることはむしろ良いことであろう。

9. 暗号・認証技術の問題点

さて、暗号化電子メールやWWWの認証技術の普及のためには、やっかいな問題がある。それは、暗号技術そのものの問題である。

暗号技術は、米国連邦政府にとって国家安全保証上の重要な技術であり、米国外への輸出に厳しい規制がある。具体的には、DESを実装したソフトウェアの輸出は原則禁止、Netscape Navigatorにも使われているRSA社の秘密鍵暗号もその鍵の長さが輸出分は40bitに制限されている。またPGPを開発したP. Zimmermann氏が、DESのコードを含むPGPのパッケージをanonymous FTPサーバーに置いたことが輸出にあたるとして訴追を受ける恐れにさらされている。

しかし、国際情勢の変化、インターネット・コミュニティや自由な輸出を望む業界の働きかけもあって、これまでほとんど認められなかった案件ベースの輸出承認でRSAの開発キットの日本への輸出が許可されたり、Zimmermann氏への訴追の調査が中止されたり、米国政府の態度も変化してきている。そうはいえ、米国以外で独自の暗号化技術を開発し、それを標準として広める努力は欠かせないであろう。

暗号システムそのものの安全性の問題もある。そもそも暗号の安全性というものも絶対的なものでない。暗号そのものに欠陥があって簡単に解読されてしまうというのは論外としても、一定のコスト（主として計算機のパワー）をつぎ込めば暗号は破れると思ったほうがよい。つぎ込むコストが、暗号を破ることによっ得られる利益より十分大きければ安全といえるだけである。たとえば、NetscapeのSSLの輸出向けの40bitの暗号は多数のコンピュータを使った力まかせの解読で

破られたが、これはSSLが30秒に1回キーを変更していることも考えれば今のところは問題ではない。しかし、暗号の設計は安全でも、それをソフトウェアに実装する際に問題が起こる場合もある。Netscape Navigator1.2のSSLや、MicrosoftのWindows 95のパスワードキャッシュの暗号化で問題になったのがこれで、どちらもキーを生成するところの実装が安易であったため比較的簡単に推測されてしまうというものであった。

一方、認証の方にも問題がある。個人の認証を行う電子署名の仕組みそのものはうまく働くことが実証されているが、証明書をどこが発行するかが問題である。政府なのか、プロバイダーなのか、クレジットカード会社なのか？　現実には、お金のやりとりと直結するWWWの分野では、ブラウザーのベンダーと提携したクレジットカード会社が積極的に動いている。そうなると、今度は複数のカード会社の間の相互認証をどうするかという問題が持ち上がる。

また、決済などの仕組みは国ごとの商習慣によって異なるので、そのあたりのローカライズと統合をどうするかという点もこれからの課題である。電子メールの認証では、U.S.Postal Serviceが全米の市民を対象に認証局を運営する計画を進めており、そのような大規模なシステムがうまく働くかどうか注目される。

（白橋明弘）

参考資料

1「カッコウはコンピューターに卵を生む」（クリフォード・ストール）
2「Practical UNIX Security」（S.Garfinkel & G.Spafford, O'Reilly & Associates,Inc.）　邦訳：「UNIX セキュリティー」（山口英監訳、アスキー出版局）
3「Firewalls and Internet Secutiry ー Repelling the Wily Hackerー」（Che swick & Bellovin, Addison-Wesley, 1994）邦訳：「インターネット接続でのファイアウォール」（川副博監訳、ソフトバンク）
4「UNIX MAGAZINE 1994年 5月号〜 転ばぬ先のセキュリティ」（山本和彦）
5「UNIX MAGAZINE 1994年8月号、ファイアウォールと proxy」（吉村伸）
6「企業ユーザーのためのインターネットハンドブック PART5 セキュリティ編」（日経BP社）
http://www.phys.s.u-tokyo.ac.jp/people/sirahasi/security.html
7「日経コミュニケーション 1995.7.3. No.201 特集 インターネットの危うさと　付き合う」
8「日経コミュニケーション1996.2.19 No.216ファイアウォールの性能をテスト」
http://www.data.com/Lab_Tests/Firewalls.html
9「インターフェース 1995/9　特集 マルチメディア時代のインターネット技術、Chapter4 ファイアウォールの基礎と実際」（谷村透）
10「E-Mailセキュリティ,」（B.Schneier著、力武健次監訳、オーム社）

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp