インターネットでの不正行為 その傾向と対策

この「インターネットでの不正行為、その傾向と対策」の連載を始めて、早くも11回目を迎えました。ここまで適当なテーマを選択し、その説明や解説などを行ってきました。今回は、スタイルを変えて、読者の方々から送られた質問に対して答える形で進めていきたいと思います。

第11回 読者からの質問に答える

JPCERT/CC（コンピュータ緊急対応センター）
URL http://www.jpcert.or.jp/

質問1

インターネットサービスプロバイダー（以下プロバイダー）にダイアルアップ接続でつないでいます。不正にアカウントを使用する事件が新聞などで取り上げられていますが、もし第三者にパスワードを盗まれてアカウントを不正に使われた場合、自分が気が付かないことが考えられます。これを調べる手立てはありますか。また事前の防衛策はありますか。

解答

「調べる手立てがありますか」ということですが、これはプロバイダー側でユーザーのアクセス記録を提供するサービスを用意していれば可能です。もし不正に使用されていれば、アクセス記録を調べて自分が使っていない時間帯や不自然な課金があれば判明するでしょう。このことから、システムを管理しているプロバイダーの協力なしにユーザーが独自に知ることはほぼ不可能です。

自衛する手段は現状ではパスワードを徹底して管理するという方法しかありません。「十分に強いパスワードを使用しているか」ということと「ある程度、使い続けたら変更を行っているか」という2点をいつも思い出してください。

十分に強いパスワードとは、英大文字、英小文字、記号文字、数字を同時に含み、適度な長さを持つ文字列からできているパスワードです（図1）。もし、簡単に推測できる弱いパスワードを使っていれば、数分から数時間で破られてしまいます。

強いパスワードといっても永遠に安全であるというわけではありません。何事にも「絶対」ということはありません。したがって、長期間にわたり同じパスワードを使い続けるようなことは避けましょう。

ユーザー認証のためにワンタイムパスワードといった技術が導入されていれば、知らない間にパスワードが漏洩したりパスワード破

りが発生したりするといった心配はほとんどなくなります（図2）。もし将来、ワンタイムパスワードのような技術が広く一般に提供されるようになれば、不正なアカウント利用の心配は今よりずっと少なくなるでしょう。

質問2

クライアントとしてTELNETやFTP、WWWなどを使う場合の注意点はだいたいわかりました。しかし、インターネットにはまだまだいろいろなツールがあります。たとえばプッシュ型ソフトウェアとかICQのようなチャット、メッセージソフト、ストリーミングソフトなどさまざまです。このようなツールを使ううえで気を付けなければならないことはどんなことですか。

解答

これは非常に難しい問題です。ソフトウェアが安全かどうかは、1つ1つチェックを行わなければわかりません。しかし、新しいソフトウェアは誰でも作れますし、実際に次々と新しい技術を用いたソフトウェアが現れます。

TELNET、FTP、WWW、電子メールといったサービスを提供する、インターネットを支える基本的なソフトウェアがセキュリティーホールを持っている場合、インターネットという基盤自体が危険にさらされます。多くの場合、これらの重要度の高いソフトウェアは、さまざまな組織が注意深くチェックし、問題があれば警告を行っています。

しかし、より一般的で現実的な認識として、インターネット上で動作しうるすべてのソフトウェアをチェックするというのは不可能であることを理解しなければなりません。また、商用ソフトウェアでソースコードがオープンになっていないものは外部からチェックすることができません。

どんなソフトウェアであれ、バグ（ソフトウェアの不具合）からは逃れられません。そしてそのバグがセキュリティーホールとなる可能性は常にあります。

いずれにしろ、どんなソフトウェアを使うにしてもリスクは伴います。それを理解したうえで使用する必要があります。

質問3

ダイアルアップルーターを使ってインターネットに接続しています。どのようなことに気を付ければいいのでしょうか。

解答

一般的なダイアルアップルーターは、ISDNのTA機能とルーターの機能を同時に持っているネットワーク機器です。最近は高機能化、低価格化が顕著になり、かなり普及してきています。そのため、ISDN用のTAを使ってダイアルアップを行う代わりに、ダイアルアップルーターを使う人も多くなってきているようです。

ダイアルアップルーターは、PPPによる接続機能を本体内部に持つルーターです。ルーターとはネットワーク制御機能に特化した小さなコンピュータのようなものだと考えてください。そのためISDN用のTAとは性格が異なります。

ダイアルアップルーターを使ううえで一番問題となるのが、ユーザーがダイアルアップルーターのパスワードを設定し忘れていることでしょう。これは、ダイアルアップルーターをISDN用のTAの代わりとして理解していると陥りやすいミスです。もし、パスワードを設定しない状態でインターネットに接続していると外部からルーターの設定機能にアクセスして勝手にルーターの設定を変え、使用不能の状態にされるおそれがあります。ぜひ注意してください。

最近では高機能なダイアルアップルーターがいろいろ出回ってきています。パケットフィルタリング機能を持つダイアルアップルーターを使用しているなら、ファイアーウォールの一部として活用することを考えてみてく

図1　強いパスワードと弱いパスワード

■強いパスワード

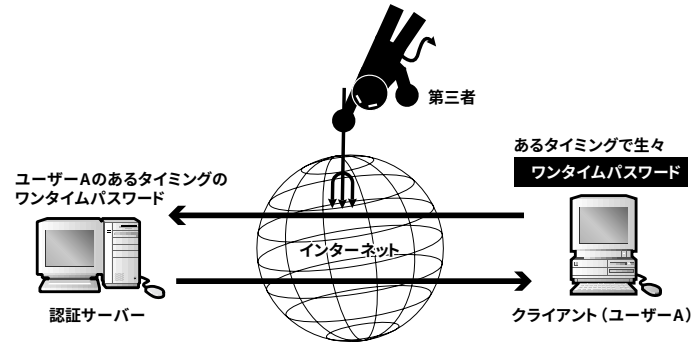
aZ$e2pq3

大文字、小文字、数字、記号をランダムに組み合わせている

■弱いパスワード

tanaka（人名を使用）
impress（会社名を使用）
19620817（生年月日を使用）
RXY32531（ユーザーIDと同じ）
jaguar（辞書に載っている言葉を使用）

図2　ワンタイムパスワード



ワンタイムパスワードはあるタイミングで一回のみ有効なので、たとえネットワーク上で第三者に盗み読みされても第三者はそのパスワードを使うことはできない。

ださい。ルーターをファイアーウォールの一部として上手に使うと、外部からの不正アクセスを防ぐことができます（図3）。

パケットフィルタリングの基本的な考え方には、大きく2通りあります。

1つは必要なパケットのみを通過させ、それ以外はすべて遮断する「all deny」という考え方であり、もう1つは、不要なパケットのみを遮断し、それ以外はすべて通過させる「all allow」という考え方です。もちろん前者のほうがより安全であることは言うまでもありません。

もし、インターネット側から内部のネットワーク上の資源にアクセスする場合には、アクセスに必要なパケットの種類は何であるかをあらかじめ調べておき、設定時に必要最小限のパケットのみを通すようにします。

これらの注意事項は、専用線でインターネットに常時接続する際、ダイアルアップルーターを通常のルーターとして使う場合も同様です。

質問4

暗号について雑誌などでみかけるのですが、実際どんな場面で使われているのかがよくわかりません。電子メール用の暗号ソフトを手に入れる機会があったのですが、使う場面もよくわかりません。

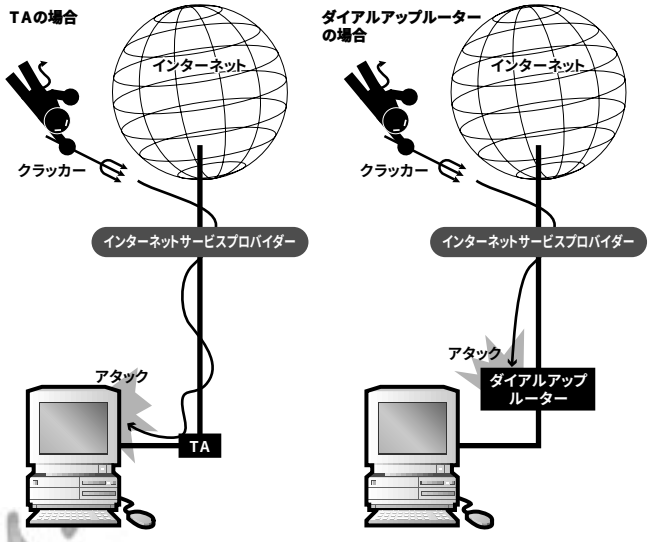
解答

よく見聞する例は、WWWブラウザーで使われているSSL（Secure Sockets Layer）でしょう。WWWブラウザー経由でパスワードやクレジットカード番号などを入力するとき、通信の内容を盗聴から保護する目的で暗号を用いています。金銭にかかわったり、パスワードのように人に知られてはいけなかったりするような情報を保護するために用いられます。

ネットワーク盗聴から通信を保護する目的での暗号利用は非常に有用です。たとえば、システム管理者がネットワーク経由でシステムのメンテナンスをするという状況を考えてみましょう。システム管理者は（ネットワーク経由で）システムにログインするためにパスワードを入力します。それをネットワーク上で盗聴されてしまえば、そのままパスワードが漏洩してしまいます。もし、ネットワークに流すデータが暗号化されていればパスワードを解読することはほとんど不可能でしょう。

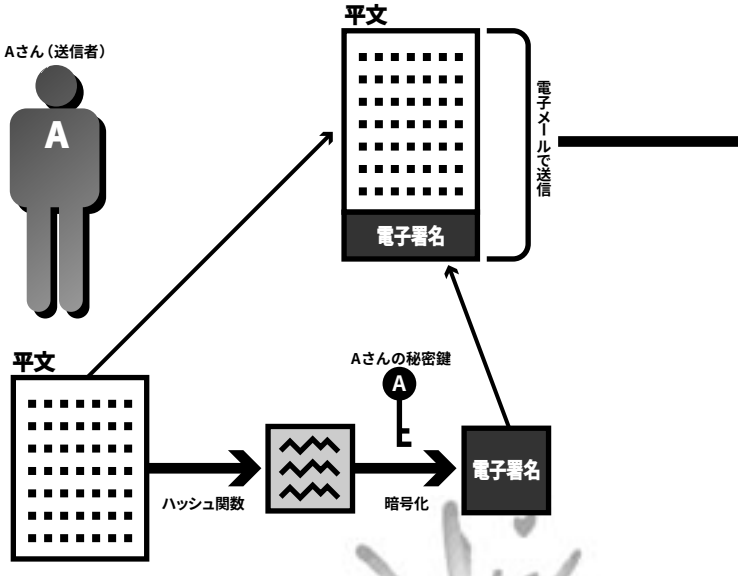
次に電子メール用の暗号ソフトウェアに関してですが、これは、電子メールの内容を暗号化するという技術も役に立ちますが、電子署名という技術も役に立ちます。たとえば、いつもメールをやりとりしている人から、唐突に不審なメールが届いたとします。そのメールの送り主が、正しい送り主かどうかを確認するのは難しい問題です。このような場合、電子署名を用いれば誰がその内容を書いたのかという証明を行うことが可能になります。また、電子的な文章（データ）は、紙に書いたものとは違い、そのままでは内容を改ざんしてもその痕跡が残りません。電子署名を行なえば、内容が改ざんされたかどうかを検出することが可能となります（図4）。

図3　ダイアルアップルーターを使った場合のセキュリティー



TAを使った場合、コンピュータ自身のセキュリティーを高めなければならない。ダイアルアップルーターを使った場合、ダイアルアップルーターによってアクセス制御を行い、セキュリティーを高めれば内部のコンピュータは守られる。

図4　署名付きメール



質問5

個人でPC-UNIXを使っています。

1）個人でWWWサーバーを立ち上げて運用する際のチェックポイントを教えてください。

2）FTPサーバーが勝手に立ち上がってしまうのですが、それを止める方法はありますでしょうか。

解答

1）WWWサーバーのセキュリティーについて

ポイントを押さえて解説するために、WWWサーバー以外のセキュリティーが保たれているホストを使用しているとしましょう。

何よりもまずWWWサーバーに関しては、最新のものを使うように心がけてください。古いWWWサーバーをインストールしたまま不正アクセスに対するメンテナンスを怠ると、WWWサーバーの脆弱性に対して攻撃が行われ、それが成功してしまう可能性があります。

WWWサーバーとしてよく使われているApacheの最新版では、任意の不正なCGIプログラムの起動に対してエラー処理を行う設定が可能になっています。たとえば、phfに対する不正アクセスはすでに知られて久しく、多くのサイトで対処済みとなっていますが、いまだに存在しないphfに対して攻撃を試みようとする者がいます。この最新版Apacheでは（すでにサーバーには存在していない）phfに対してアクセスしようとすると、自動的にアクセスを行ったユーザーのIPアドレスなどの情報を記録するような機能を設定できます。

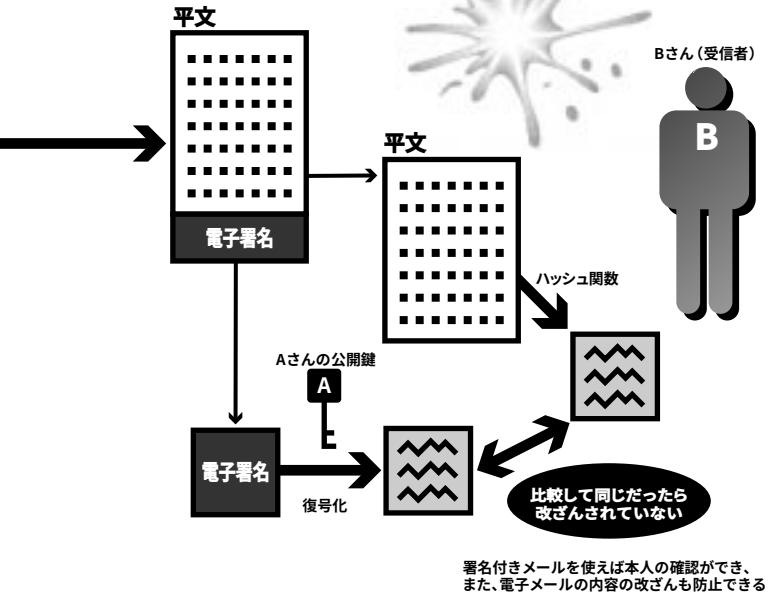
CGIプログラムに関しては、さまざまなフリーソフトが出回っています。しかし、それらすべてがセキュリティーに対して十分な配慮を行っているプログラムであるという保証はどこにもありません。入手して使用しているCGIプログラムの脆弱性を突いた攻撃が行われるかもしれません。また、十分に信頼できる配布先からコピーしない限り、悪意を持った者が「トロイの木馬」としてCGIプログラムに何かを仕掛けるという危険性は常にあります。どこから手に入れたかわからないようなプログラムは使うべきではありません。

2）FTPサーバーが立ち上がらなくなる方法

/etc/inetd.confの中のFTPサービスをコメントアウトし、デーモンとして動作しているinetdにroot権限でHUPシグナルを送ります。inetdはHUPシグナルを受け取ると自動的に/etc/inetd.confの読み込みを初期化します（図5）。

また、セキュリティーを考慮して、ftpdだけではなく不要なネットワークサービスのエントリーを同様にコメントアウトしてください。たとえばPC-UNIXをクライアントとして使っているような場合、POPやIMAPといったメールサーバーの稼動は不必要になります。そのようなときは、/etc/inetd.confにあるPOPとIMAPの設定部分をftp同様にコメントアウトしてinetdにHUPシグナルを送ってください。

ほかに、サーバープログラムをデーモンとして起動している場合は、/etc/rc.*や/etc/rc*.d/*といったファイルを調べて不要なエントリーをコメントアウトしたうえで、動作中のプロセスをkillするか、あるいはシステムを再起動するなどしてください。



署名付きメールを使えば本人の確認ができ、
また、電子メールの内容の改ざんも防止できる

図5　FTPサーバーが勝手に立ち上がらなくなる方法

❶ /etc/inetd.confのftpサービスの部分をコメントアウトする

Linuxの場合

```
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  wu.ftpd -l -i -a
 ↓コメントアウト
#ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  wu.ftpd -l -i -a
```

FreeBSDの場合

```
ftp     stream  tcp     nowait  root    /usr/libexec/ftpd       ftpd -l
 ↓コメントアウト
#ftp     stream  tcp     nowait  root    /usr/libexec/ftpd       ftpd -l
```

❷ PSコマンドでinetdのプロセス番号を調べる

```
% ps axuw | grep ‘inetd’
user     15609  0.0  1.3   932   308  p3 S   09:16   0:00 grep inetd
root        81  0.0  0.3   844    72  ?  S  May 15   0:00 /usr/sbin/inetd
```

↑プロセス番号

❸ killコマンドでinetdプロセスにHUPシグナルを送り初期化する

```
% kill -HUP 81
```

↑プロセス番号