インターネットでの不正行為その傾向と対策

昨年ほどセキュリティーの問題が、新聞や雑誌、テレビなどのメディアで取り上げられた年はなかったのではないでしょうか。インターネットという世界に入ってきた人間が増えたことで、さまざまなトラブルが起きています。'98年の本連載の最初は、'97年の不正アクセスの動向を振り返ってみましょう。

第7回 1997年のインターネットセキュリティー問題を振り返る

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

インターネットセキュリティーの春夏秋冬

今回は、初心者講座という所から少し離れて、97年を振り返るという形で、不正アクセスの傾向を考えてみたいと思います。本文で取り上げる問題は、サイト管理者に対しての情報ばかりですが、一般の利用者であっても、不正アクセスに関する広い知識という意味で、無駄にはならない情報だと思います。

97年の流行

97年の特徴は、春夏秋冬の季節にあわせて不正アクセスの流行があったことです。インフルエンザのように不正アクセスにも流行があるのは面白い傾向です。しかし、どの不正アクセスの方法も広く知れ渡り、かつ、既に防御方法が用意されている古典的な方法ばかりでした。これは、きちんと不正アクセスに対する適切な処置を事前に行っていれば、防げる（防げた）ということを改めて確認したと言えるでしょう。

ただし、残念なことに、このような広く知られた基本的、古典的ともいえる不正アクセスの手法であるにもかかわらず、対処を行っていないサイトがまだまだ存在するのも事実ですし、また実際に被害も出ています。その中でもJPCERT/CCへ報告されたのは、成功不成功にかかわらず、不正アクセスが行われている事例のごくごく一部でしょう。

よく氷山の一角という言葉がありますが、JPCERT/CCに報告して頂いた不正アクセスは、全体の不正アクセスから比べると、さらに少なく氷山の一角にも満たないのではないかと考えています。

多く初心者の方は、「広く知られた」「基本的」「古典的」と言われるようなセキュリティーの問題をなぜ放置しておくのか不思議に思うかもしれません。理由はいくつか考えられますが、なんといってもセキュリティーに対

する認識不足、あるいはセキュリティーに対して積極的に注意を払っていなかったというのが最大の理由でしょう。

今回取り上げるすべての不正アクセスに対する対処法がJPCERT/CCのウェブサイトから入手可能です。もし、対処していないケースがありましたら、早急に対処を行うことを推奨します。対処に必要な関連情報は次のURLから入手できます。

URL http://www.jpcert.or.jp/

本稿の中では、ソフトウェアの安全な最新バージョンに関してのバージョン情報は、あえて載せていません。それは、本稿執筆時に安全なバージョンであっても、読者が本稿を読む時には、それがまだ安全であるという保証がないからです。ですから、最新の情報に関しては、前途のURLを必ず参照してください。

また、最新のソフトウェアに関する情報は次のURLを参照してください。

URL ftp://ftp.jpcert.or.jp/pub/cert/lastest_sw_versions/

冬〜電子メールへの不正行為

96年年末から97年年始にかけて大規模に不正アクセスが行われました。これは、sendmail R5と一般によばれる古いバージョンのsendmail（UNIXのメール転送プログラム）への攻撃です。このsendmailというプログラムは、インターネット上のサイト間でメールをやり取りするときに使われるソフトウェアで、現在のインターネットのメール配布の中心を占めるソフトウェアでもあります。

ただし、この攻撃は古いバージョンに対してのみ有効な以前から広く知られている攻撃だったので、きちんとメンテナンスさえ行われていれば、被害がありません。

技術的な面では見るべきところがありませんが、年末年始の連続した長期休暇を狙った不正アクセスであることが特筆すべき点だと言えるでしょう。

年末年始のように、長期間に渡ってシステムログをチェックできない日が続くような時は、事前にログを保存する期間を長くするなどして、確実に管理者がログを参考できるようにしておく必要があります。

さて、この古いsendmailへの攻撃ですが、この攻撃の主目的は、パスワードファイルの盗用（不正コピー）です。不正アクセスの最終目的はルート権限の詐取ですが、アカウント狙いは、そこに至る道筋の重要な通過ポイントです。

パスワードファイルが盗まれたからといって直ちにシステムへの侵入が始まるわけではありません。パスワードファイルには既に暗号化されたパスワードが収められていますが、その暗号化されたパスワードを手掛かりに、元のパスワードを探しださなければいけないからです。パスワードの安全性に関しては、97年11月号を参照してください。また次のURLからも情報を入手できます。

URL http://www.jpocert.or.jp/magazine/beginners.html/

とはいえ、盗難にあってからパスワード変更の対処を行うまで、パスワードを探しだされる危険性は、そのタイムラグに比例して高くなります。特にパスワードに関するセキュリティー教育をユーザに徹底していないサイトでは、簡単に破られてしまう危険性がさらに高まります。

このときの攻撃を検出する方法は、まずsendmailのログを収めたファイルの中に、“ /etc/passwd ”といったような不審な文字列がないかをチェックします。もしログの中に“ /etc/passwd ”という文字があったら、それに対応するメールの送信記録があるので、それをチェックします。

もし送信記録に“ stat=Sent ”という記録があればそれはサイトから“ /etc/passwd ”がメールで送りだされたということを意味しています。ただし、相手が本当にメールを受け取ったかどうかは、送信側には分かりません。

なお、この例は、96年12月末から97年1月初めにかけての攻撃が/etc/passwdを盗む攻撃だったので、それがログに記録されていないかをチェックしているにすぎませんので注意してください。古いsendmailを使っている場合は、同様な手口で他のファイルを盗むことが可能です。

▶対処法 最新のsendmailにアップデートします。

春〜ネットニュースへの攻撃

春はINNに対する攻撃が流行しました。INNは、インターネットのネットニュースの送受信および中継をする代表的なシステムです。そのINNのバージョンが1.5.1より前には、コントロールメッセージに書かれたコマンドを実行するというセキュリティーホールが存在していました。春のINNへの攻撃は、そのセキュリティーホールを悪用されて行われたのです。これも以前から指摘されているセキュリティーホールでした。

この春のINNに対する攻撃は、“ /etc/passwd ”を盗むというものでしたが、この攻撃が与える危険性には2つの場合が考えられます。もちろん攻撃されたサイトでのデータの盗用、あるいは破壊の危険があるのは当然ですが、もう1つは、INNの攻撃をそのまま他のサイトを攻撃するための踏み台として利用される危険も可能性として考えられます。

▶対処法 最新のINNにアップデートします。特に1.5.1バージョンより前のものである場合は、直ちにアップデートします。

夏〜cgi-binプログラムへの攻撃

夏にはcgi-binプログラムの中のphfコマンドに対する攻撃が流行しました。cgi-bin（あるいはcgi-binプログラムとも呼びますが）

とはWWWサーバーと協調して利用者のリクエストを処理するプログラムの総称です。これは、プログラムの中の1つであるphfを不正利用するような攻撃でした。

現在では、すでにWWWサーバーの配付パッケージからはphfは削除されていますので問題はないですが、古い配付パッケージをインストールしたり、以前のphfが削除されないまま残っている場合は問題となります。

最近ではphfへの攻撃というのは、あまりにも有名になってしまっていて、定番と呼べるほどになっています。WWWのシステムを管理している人は、httpdはエラーのログも取れますので、そのエラーログの中にphfという文字がどれくらいの現れているかをチェックしてみると良いでしょう。特定のサイトへの不正アクセスを狙う時も、必ずといっていいほど、真っ先にサイトに対しphfの攻撃が有効かどうかを確認するといっても過言ではない程です。

phfが存在していた場合、サイト上のファイルを盗んだり、あるいは改竄、破壊が行われる可能性があります。

▶対処法 cgi-binプログラムのphfを削除する。それ以外にも不必要なcgi-binプログラムは削除しておきます。

秋 秋～IMAPへの攻撃

秋にはIMAPサーバーに対する攻撃が流行しました。IMAPとは、メールサーバーからメールを取り出す1つの方法（手順）です。IMAPに対応したメールリーダーがクライアントとなり、IMAPと通信し、メールをクライアント側（パソコン側）に取りだす働きをします。

IMAPにはいくつかの異なる実装形式がありますが、そのうちのいくつかのIMAPサーバー（と、IMAPサーバーを参照するようないくつかのPOPサーバーも含む）がセキュリティーホールを持っています。たとえば、ワシントン大学の開発したIMAPではIMAP4rev1より前のバージョンは、このセキュリティーホールを持っています。

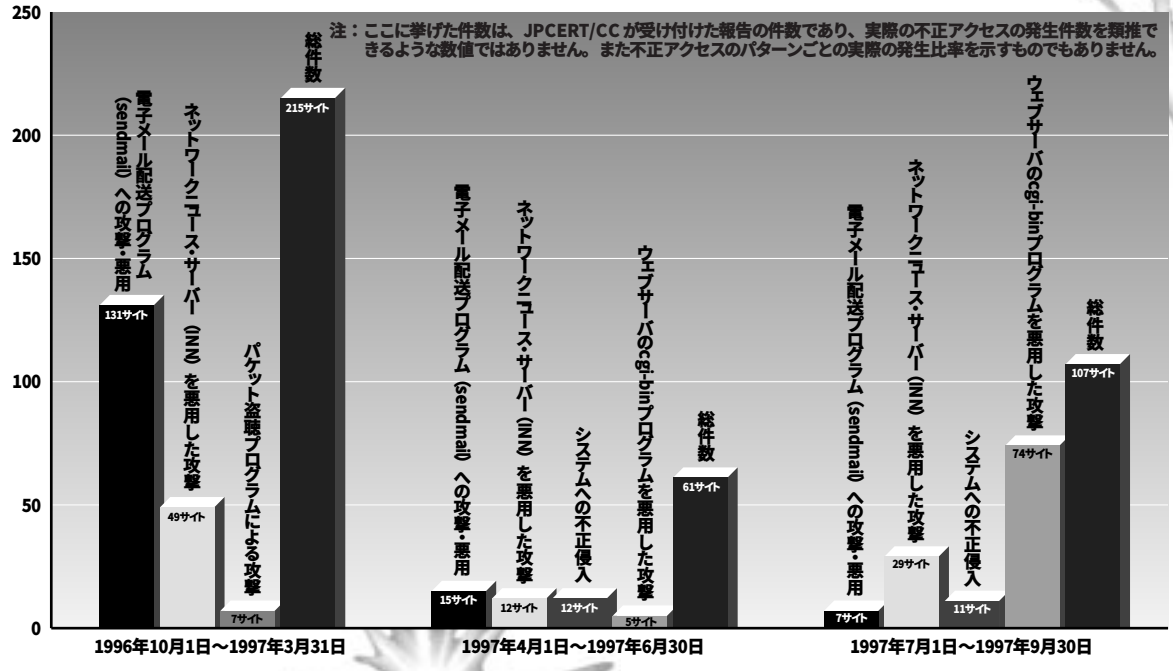
このセキュリティーホールを持つIMAPは、不正アクセスを行う者が送り込んだ不正なプログラムがシステム管理者の権限（ROOT権限で）で実行されるという、危険度が高いものです。

▶対処法 安全が確認できていないIMAPを使用している場合、サービスを停止するか、あるいは、ワシントン大学で開発したIMAPの最新バージョンへ早急にアップデートする必要があります。

TCP/IPのバグはなぜか秋に現れる??

かなり安定していると言われているUNIX系のTCP/IPですが、古くから潜んでいるバグによるセキュリティーホールが、なぜか96年、97年、と2年連続で秋に現れています。この2つのバグは、BSD UNIXと呼ばれるUNIXが持つTCP/IPのコードから継承されてきた古くからのバグですが、必ずしもすべてのUNIX系のオペレーティングシステムが持っているバグではありません。

96年の秋は、一般にPing Of Deathとして



知られている、長いパケットを受け取るとオペレーティングシステムがダウンしてしまうバグが発見されました。

それから約1年後の97年秋には、一般にLAND Of ATTACKとして知られている、送信先偽造のパケットを受け取ってしまうバグが発見されました。どちらもオペレーティングシステムがダウンしてしまう危険性がある重大なバグですが、バグ自体は非常に単純なバグで、今まで誰も気が付かなかったのが不思議に思えるほどです。

さて、これには1つの教訓があります。それは、どんなに以前から広く使われているようなものでも、セキュリティーホールとなるバグが潜んでいる可能性があるということです。昨日まで長い間安全だったものも、明日になれば安全ではなくような可能性が常に存在しているのです。常時セキュリティーに対する情報をチェックしておかなければ、サイトの安全な運用が難しいと言えるでしょう。

この両方のセキュリティーホールですが、いくつかのUNIXベンダーは、すでに気が付いていて独自に修正していたため、これらの問題が出なかったUNIX系オペレーティングシステムもいくつかあります。もちろん、これらの問題はすでに対処できています。次のCERT/CCのアドバイザリーを参考にしてください。

* CERT Advisory CA-96.26 - Denial-of-Service Attack via ping
* CERT Advisory CA-97.28 - Teardrop_Land

CERT/CCが発行するすべてのアドバイザリーは、CERT/CCの許可を得て、次のURLにミラーを用意しています。

URL ftp://ftp.jpcert.or.jp/

不正アクセスの届け出に関して

97年は、春夏秋冬とそれぞれの季節にそれぞれの不正アクセスの流行があったわけですが、流行した不正アクセスは、その手法から推論すると、成功不成功に関係なく、非常に大規模な範囲にわたっていると想像できます。JPCERT/CCに情報が届けられたものは、全体の数からは非常にわずかであると考えざるを得ません。

JPCERT/CCが、不正アクセスの全体像や傾向を正確につかむために、不正アクセスの具体的な被害がなくとも、あるいはJPCERT/CCの支援が必要なくとも、不正アクセスを受けたならば、その情報を不正アクセス情報届出形式にて届けて頂ければ非常に助かります。次のURLにアクセスしてください。

URL http://www.jpcert.or.jp/form.html/

不正アクセスの全体像や傾向がいち早くつかめるようになれば、緊急報告や対処に必要な情報などをさらに効果的に出すことも可能になります。

それが、攻撃者への先手を打つ形で利用でき、まだ不正アクセスの被害に遭われていないサイトの防御に役立ててもらえることにつながるかもしれません。

まとめ

97年に流行した不正アクセスに関して、大きく2つのまとめができると思います。

第一点目は、対象を絞らずに、多数のサイトに対して攻撃を行っていたということ。第二点目は、それらの攻撃手法はすでに知られているものであり、きちんと不正アクセスに対する防御を事前に行っているサイトに対してはそれらの攻撃がすべて不成功に終わったという点です。