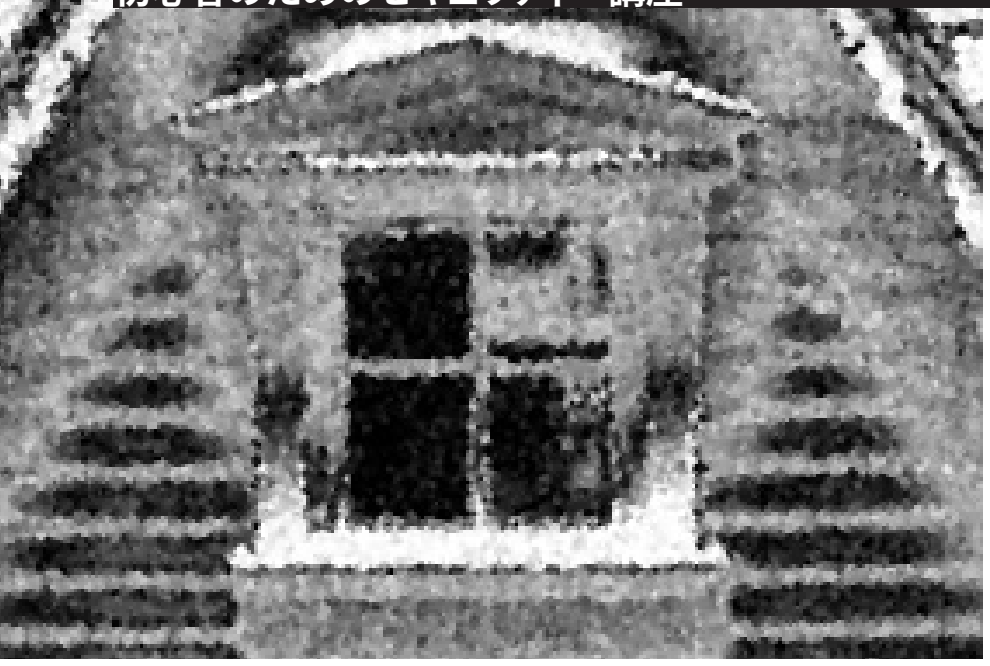
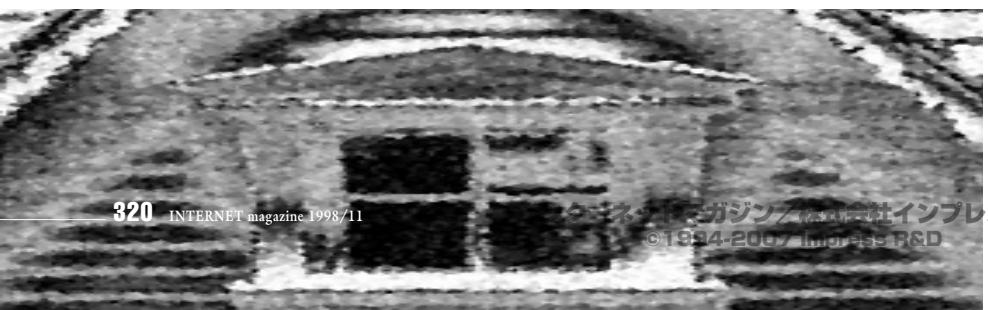


インターネットでの不正行為 その傾向と対策

前回までは、不正アクセスを事前に防ぐための方法について解説してきましたが、今回は不正アクセスを受けてしまった場合に気を付けなければならないことを中心に解説しましょう。不正アクセスを未然に防げるならばそれに越したことはありませんが、不正アクセスを受けてしまった場合の対処を知っておくこともシステムを管理するうえで重要になります。ここまでの一通りの知識を身につければ、不正アクセス対策の基本的なレベルはクリアしたといえるでしょう。

第14回 SOHO環境におけるネットワークセキュリティー その3

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



それでも不正アクセスを受けたら

物事に取り組む場合、常に最悪のケースを想定してこれに対応できる準備をしなければなりません。前回と前々回は、「不正アクセスを防ぐため」の話に集中しましたが、今回は「不正アクセスを受けてしまったら」という観点から話を進めます。また、SOHO環境におけるネットワークセキュリティーに関しての連載は、ここで一区切りを付けたいと思います。

よく「不正アクセスを受けてもマシンの中には貴重なものなどないので、マシンをネットワークから切り離し、ディスクをフォーマットしてシステムを再インストールすれば問題ない」という話を聞きます。もちろん、この方法は確実ですし、推奨できる方法の1つだと言えます。

それであっても、大切な前提が抜けています。それは「不正アクセスを受けていることを察知する」という部分です。もし、不正アクセスを受けていることに気が付かない場合は、対処のしようがありません。また、どのような不正アクセスを受け、何が原因だったのかをきちんと把握し、その問題を解決できる目処が立ったうえで対処することが肝要です。もしかすると、ディスクをフォーマットしてシステムを再インストールしたとしても、根本的な問題を解決していないために、また同じ不正アクセスが繰り返されてしまう可能性があるからです。

スクラップ・アンド・ビルドに関して

内容的に先走りしてしまいますが、SOHO環境でのスクラップ・アンド・ビルド（以前のものを破棄して新しく構築する）に関して少し考えてみたいと思います。

SOHO環境の場合、大きな組織で運用しているより利点があります。それは、比較的小規模なシステムのため、システム全体に対

してスクラップ・アンド・ビルドを行いやすいことです。大きな組織で運用されている大規模なシステムになればなるほど、スクラップ・アンド・ビルドは非常に困難になります。

もちろん、すべてのSOHO環境がスクラップ・アンド・ビルドを適用できるとは限りませんが、SOHO環境がコンパクトである点は一般的な傾向としてスクラップ・アンド・ビルドの適用の可能性を高めてくれています。

データのバックアップには注意が必要

不正アクセスを受けたマシン上のすべての情報を破棄してしまい、ゼロからインストールするのも1つの手ではありますが、多くの場合、貴重なデータを捨てるわけにはいかないことがほとんどです。

不正アクセスを使ってマシンに侵入した者が、証拠いん滅のためにディスクの中のすべての情報を破壊して逃げた場合、その被害は甚大になります。このような事態を防ぐためにデータをバックアップしておきましょう。

ただし、セキュリティーを考えたときのバックアップは、通常のディスク故障のためのバックアップとは少々考え方を変えなければいけない部分があります。システムのセキュリティーに関連しないデータは比較的問題ないのですが、システムのセキュリティーに関連するデータ類のバックアップには細心の注意が必要です。

たとえば、パスワードファイルがすでに侵入者によって書き換えられていた場合、あるいはパスワードファイルの中に侵入を許したアカウントがあるような場合を考えてみましょう。システムを再構築し、パスワードファイルをバックアップから戻した時点で、また不正アクセスの問題が発生します。

トロイの木馬のようなプログラムがユーザーのディレクトリーの中に潜んでいた場合も同様です。せっかくシステムを再インストールして安全になった場所に、バックアップを戻すと、トロイの木馬が戻ってしまいます（図1）。

したがって、不正アクセスを受けたときに戻すためのデータとしてバックアップするのは、戻しても安全であることが保証できるようなデータに限定するべきでしょう。

セキュリティーポシリーの一環としてバックアップのポリシーを考えるときは、次の点を明確にする必要があります。

・どんなデータをバックアップするか
・どんなタイミングでバップアップするか

重大な侵入を受けた兆候の察知

侵入を受けた兆候を察知するための方法に関するドキュメントとしてCERTの「Intruder Detection Checklist」（侵入者察知チェックリスト）があります。

このドキュメントをベースとして、SOHO環境での侵入チェックを考えてみましょう。

●Intruder Detection Checklist入手先
URL ftp://info.cert.org/pub/tech_tips/intruder_detection_checklist

❶アクセスログを調べる

UNIXのsyslogやlastといったログをチェックするのは、外部から不正なアクセスがあったかどうかを調べるのに最も基本的な方法です。また、FTPが転送結果を記録する

図1　セキュリティーのためのデータバックアップ

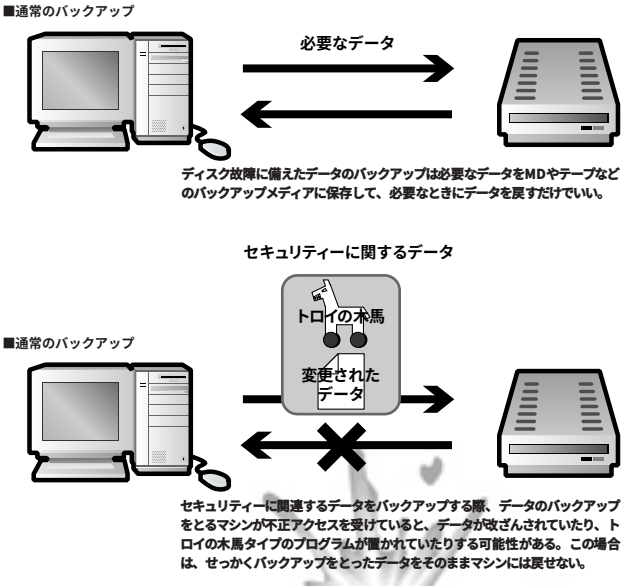
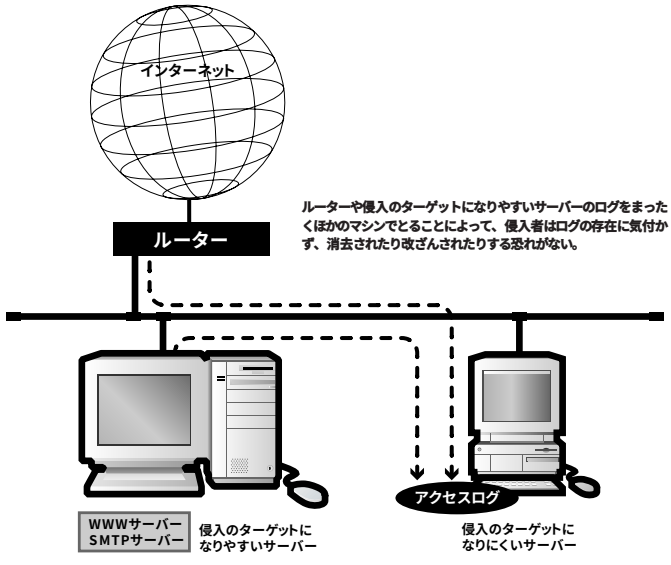


図2　ルーターやサーバーのログを別のマシンでとる



xferlogのように、サービスを行っているソフトウェアが用意しているログも重要です。さらにTCP wrapperのようなセキュリティーツールを使用して、より詳しいログをとるといったことも有効です。
このほか、ルーターのログも非常に役に立ちます。SOHO環境向けのダイアルアップルーターでも、ほかのマシン上でログの記録を取れる機能を持っているものがあります。このようなルーターのログを解析することによって外部からの侵入を察知できます。侵入のターゲットになりやすいサーバー以外のマシン上でsyslogやルーターのログなどが記録されている場合、侵入者がアクセスログの存在に気が付かない可能性が高くなります（図2）。もちろんこのマシンもセキュリティーを高めておくことは言うまでもありません。

❷setuidやsetgidが付いている不審なファイルを探す

所有者がrootである実行ファイルに、setuidやsetgidが設定されていた場合、その実行ファイルはrootの権限で実行されます。侵入者がよく行うパターンとしては、/bin/sh（あるいはこれに相当するコマンド）などをどこかに別名でコピーし、その偽造シェルにrootのsetuidを設定して使用するというのがあります。この偽造シェルを使えば、rootでのログインの形跡を残さなくともroot権限を使えるようになります。このようなファイルは、UNIXのfindコマンドを使うと効率的に探せます（図3）。

❸トロイの木馬を探す

すでにインストールされている実行ファイルの代わりに、侵入者がトロイの木馬を仕掛けるような場合があります。これは、rootが作業中、知らない間にトロイの木馬を実行してしまうことを期待しています。システムの設定に不備があり、本来はアクセスが許されないディレクトリーや実行ファイルに書き込みができる場合、侵入者はこのような実行ファイルの代わりにトロイの木馬を仕掛けることがあるのでチェックが必要です。特に、rootの使用している実行パスに含まれる実行コマンドが改ざんされていないかをチェックします。

一番オーソドックスな方法は、配布メディア（たとえばCD-ROM）の内容と、UNIXのcmpコマンドなどを使って直接比較することです。配布メディアの内容と単純には比較できない場合があります。たとえば、インストール後にパッチを当てた実行コマンドや、あるいは自分で再コンパイルしたような実行ファイルをチェックする場合です。このような場合は一貫性チェック（インティグリティーチェック）と呼ばれる方法が有効です。
一貫性チェックで、侵入者が仕掛けたトロイの木馬を検知するためには、最初のインストール時（あるいは、パッチを当てた直後など）に実行ファイルの記録をとっておかなければなりません（図4）。
通常はファイルの内容が同じかどうかを高速にチェックするのにUNIXコマンドのsumが使われますが、改ざんを強力にチェックするmd5sumが便利で安全です。md5sumで出力されたリスト内容を保存したファイルをフロッピーディスクやテープに保存しておきます。データを保存したフロッピーディスクやテープは、物理的に書き込み不可の状態にして、侵入者が変更できない

図3　不審なファイルの探し方

```
find / -user root -perm -4000 -print
```

図4　一貫性チェックの仕方

```
■リスト作成

% md5sum /sbin/*/usr/sbin/*/bin/*... >
md5_check_list

■チェック

% md5sum < md5_check_list
/sbin/agetty: OK
/sbin/arp: OK
/sbin/badblocks: OK
```

図5　rhostsによるバックドア

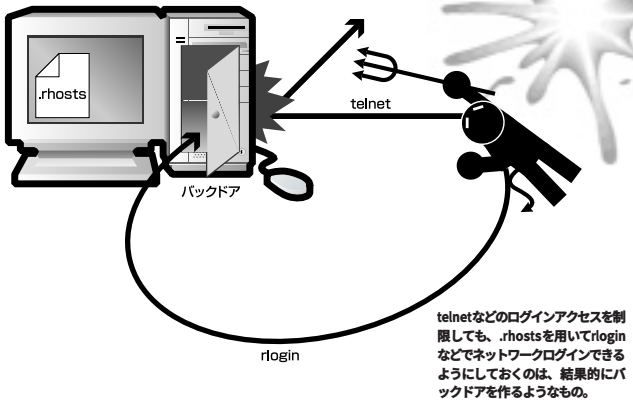


図6　不審なファイルの探し方

```
% find / -name '..*' -print -xdev ¦ cat -v
% find / -name '.*' -print -xdev ¦ cat -v
```

ようにしておきます。

❹自動的に実行されるエントリーをチェックする

/etc/rc*、/etc/rc.d/*、/etc/init.d/*のような起動時に実行されるスクリプトファイルも注意が必要なファイルなのでチェックします。
また、一定時間ごとに処理を実行するための機能であるcronや、特定の時間に処理を実行するatのエントリーに不審なものが仕掛けられていないかをチェックします。また、cronやatで呼び出されている実行ファイルが改ざんされていないかどうかをチェックする必要があります。

❺システムの設定ファイルの書き換えをチェックする

侵入者にパスワードファイルが書き換えられていないか、あるいは不正なネットワークサービスが追加されていないかなどをチェックします。
特に/etc/passwdや/etc/inetd.confなどは重点的にチェックします。また、/etc/hosts.equivや/etc/hosts.lpdといったネットワークで資源を共有するような設定、あるいは.rhostsなどがあるかもチェックします。
外部から厳しくログインアクセスを制限しているマシン上ではユーザーレベルでも.rhostsを用いて自動的にネットワークログインするのは好ましくはありません。これは秘密の抜け道を作る一種のバックドア（隠し戸）と呼ばれる種類の仕掛けに使われかねません（図5）。/etc/hosts.accessや/etc/hosts.denyのような、外部からのアクセスを制限するような設定に関連するファイルも、外部からの侵入を行うために改ざんのターゲットとなりやすいものです。

❻不審なファイル名を探す

侵入者はファイルを隠すときに、見つけづらいようなディレクトリー名やファイル名を作る場合があります。たとえば、ファイル名やディレクトリー名を“ .. ”（ドット、ドット、空白）であるような名称、あるいは、“ ..^G ”といった名称にして隠しておく場合があります。そこで、findを使って探します（図6）。
ただし、これは必ずしも有効とは限りません。一見、ごく普通のファイル、たとえば“ .x ”とか“ .pop ”といったような、もっともらしい名称にして隠す場合もあるからです。

バックアップしたデータを戻す

万が一、侵入者に情報を改ざんされたり、あるいは破壊されたりした場合、それを復旧しなければいけません。通常のハードウェアの障害の復旧と同じく、そこでバックアップしてとっておいたデータを使って復旧しようとするのが一般的な考え方だと思われます。

しかし、先に説明したように通常のハードウェア障害からの復旧と、不正アクセスを受けて侵入されたシステムの復旧は、まったく様相が違ってきます。

システムがネットワークに接続される前にバックアップをとっておいたものを使うのなら安全でしょう。しかし、侵入がいつから行われていたか確信が持てない場合は、バックアップを行ったデータの中にすでにトロイの木馬や改ざんされたデータなどが含まれている可能性があります。このように確信が持てない場合、オペレーティングシステムに関連する部分は再構築（再インストール）するほうが確実になります。大変といえば大変です。しかし、大規模な企業のシステムとは違い、SOHO環境の場合、すべてをチェックする労力より、新たに再インストールをするほうが確実で労力が少ない場合が多いでしょう。

また、システムに影響を与えないようなデータをバックアップから戻したときも、そのデータの中にトロイの木馬のようなプログラムが隠されていないか、バックドアなどが隠されていないかを注意深くチェックしてください。また、実行ファイルを戻すときは、さらに注意が必要です。その実行ファイル自身が改ざんされてトロイの木馬として使われてはいないか、相当厳しくチェックする必要があります。

関連ドキュメント

不正アクセスに対抗して安全にシステムを運用していくときのドキュメントなどはJPCERTのWWWサイト上にある次のウェブページを参照してください。

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

CERTが提供しているTech Tipsに含まれる数々のドキュメントが役に立ちますし、また、RFC2196“ Site Security Handbook ”なども非常に参考になります。

これらのドキュメントは上記URLからたどることができます。

お知らせ

1年数か月のあいだ、毎月連載していた「インターネットでの不正行為 その傾向と対策」は、ここで一休みします。今後は、特にみなさまにお知らせしたいようなトピックがあったときに紙面を通してお目にかかることになると思います。

本連載のバックナンバーは、下記のURLにPDF形式のファイルとしてまとめてあります。みなさまのご参考になれば幸いです。

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

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

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、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）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、写真の撮影者、イラストの作成者、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収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用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する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時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。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp