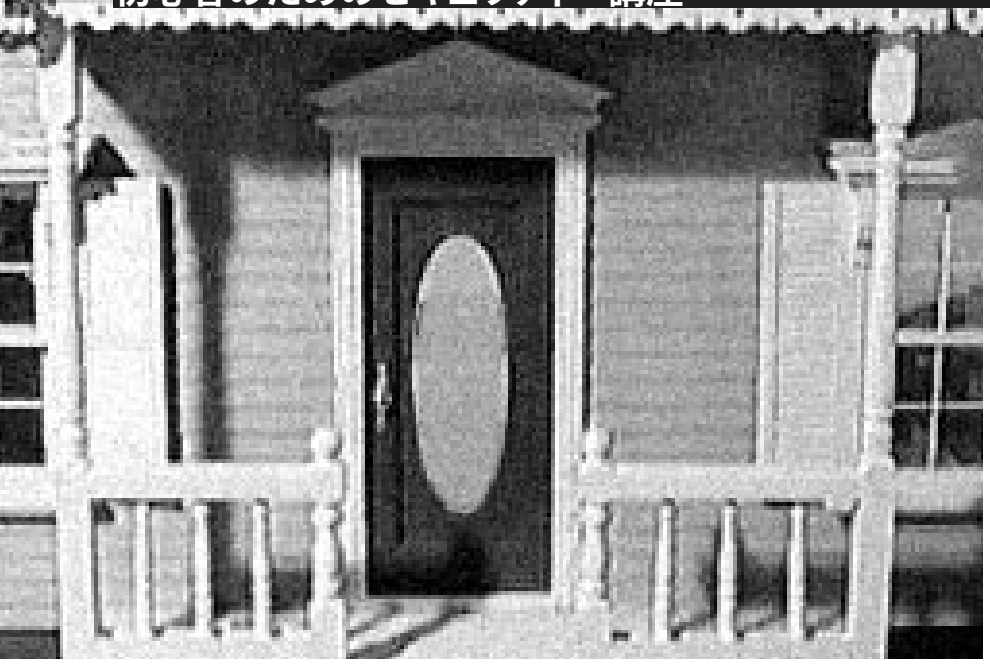
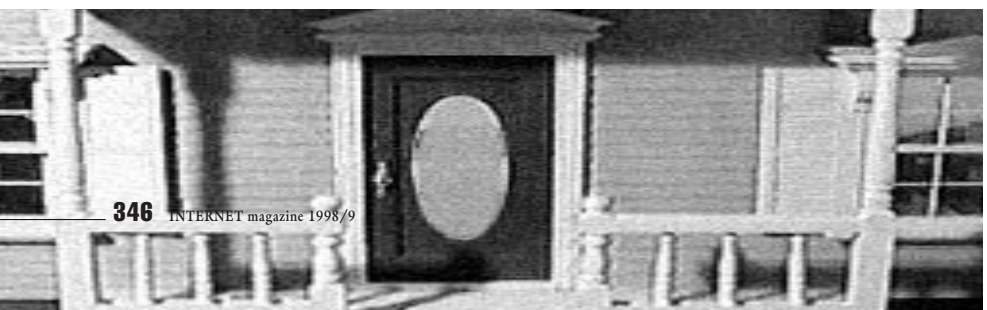


インターネットでの不正行為その傾向と対策

インターネットに常時接続しているSOHO環境ではどのような問題が発生するのか、また、不正アクセスに対するセキュリティーを高めるにはどのようにすればよいか。このことについて考え始めると、セキュリティーについて根本的なレベルから理解する必要があります。そこで、これから数回にわたりSOHO環境でのセキュリティー対策について解説します。

第12回 SOHO環境のネットワークセキュリティー その1

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



どんなサイトでも利用価値はある

ムーアの法則（18か月で半導体製品は2倍の能力を持つという法則）に従い、時間とともにハードウェアのコストが下がっていきます。10年前では数百万円という価格帯のコンピュータの性能が、今日では、普及品のパーソナルコンピュータのレベルとして提供されている状況になっています。また、ネットワークの普及とともに、ネットワーク接続コストも低くなってきました。

数年前までは、企業や大学、あるいは研究所のような組織でしか用意していなかったようなインターネットに常時接続されているネットワーク環境が、現在では小さなオフィスや家庭でも可能となりました。同時に、今まで企業や大学、あるいは研究所のような組織が抱えていたインターネットセキュリティーに関する問題が、小さなオフィスや家庭にやってきます。

現在では、もし何も対策を施さずにセキュリティーホールを持ったままインターネットに常時接続しているようなサーバーがあれば、ほぼ確実といっていいほど外部からセキュリティーホールを見つけられてしまいます。そうなれば、非常に高い確率で不正アクセスを受ける可能性があります。なぜならば、どんなサイトであれ利用価値があるからです。後の「保護対象について考えてみよう」で述べますが、自分が甘い考えを持っていると、とんでもないトラブルに巻き込まれる可能性があります。

常時接続における問題点に関しては、すでに本連載第10回「IP常時接続における問題点」（1998年6月号）でも取り上げています。そちらも参照してください。本連載のバックナンバーはPDF形式で公開されています。詳しくは下記URLを参照してください。

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

SOHO環境モデル

さて、ここでのSOHO環境とは何かを定義しましょう。SOHOとは、Small Office/Home Officeの略で、一般には、インターネット接続だけではなく、小規模なグループでコンピュータ同士をネットワークで接続した環境まで含んだ広い範囲を指している言葉です。本連載のテーマは不正アクセスなので、インターネットに接続しているSOHO環境に話題を絞ります。

話題を明確にするために、モデルとなるSOHO環境を想定します。ここで想定しているSOHO環境モデルの概要は次のようなものです（図1）。

- ●インターネットに常時接続されている
- ●サーバー用のコンピュータが用意され、各種サービスが行われている
- ●LAN上にクライアントとして使われる複数のコンピュータが接続されている

アクセスの許可を明確にする

繰り返しますが、インターネットに常時接続する限り、SOHO環境のように小さいグループや個人的に使うネットワークの規模でも、本格的に運用されている大組織のネットワークのような規模でも、セキュリティー対策の基本部分は同じです。それはアクセスが許された資源にはアクセスできるが、アクセスが許されない資源にはアクセスできないという、当然すぎる目的を達するためのセキュリティー対策です。

その前に、アクセスが許された資源とアクセスが許されない資源を明確化しなければなりません。そうでなければ、アクセスを許すべき資源に対してアクセスを許さず、反対にアクセスを許すべきではない資源にアクセスを許してしまうような事態になりかねないからです。また、どのような目的で、どこまでのアクセスを許すのかなども明確にしなければなりません。これは、せっかくセキュリティー対策を行ったにもかかわらず、本来の目的を達することができなかったり、あるいは過剰なセキュリティーコストをかけてしまうかもしれないからです。

セキュリティーポリシー

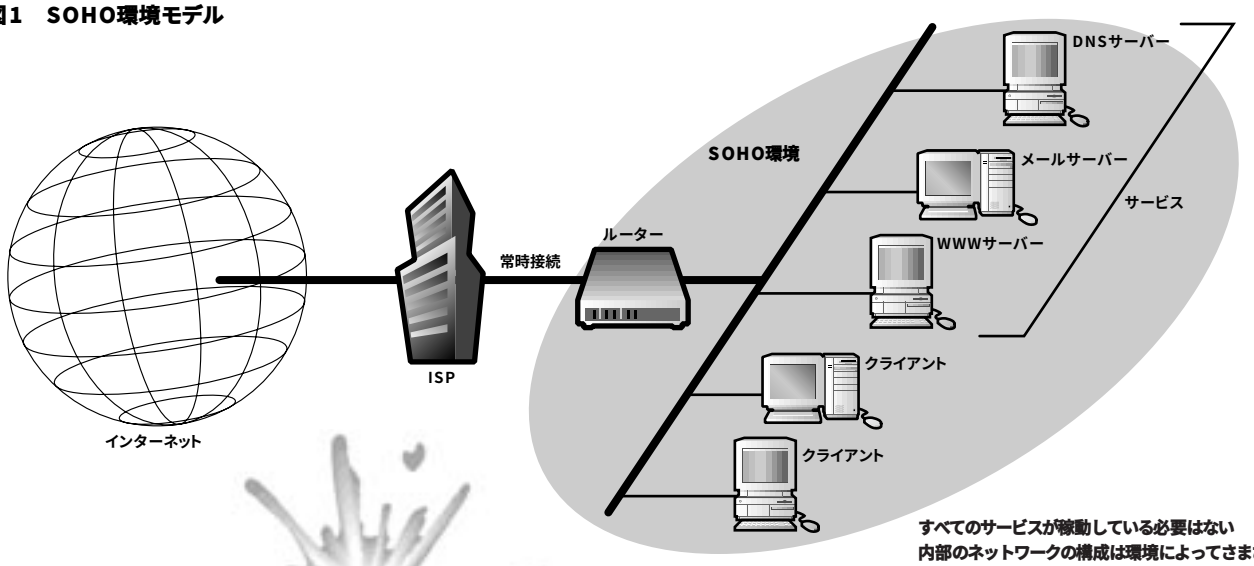
何を許し、何を許さないか、またそのためにどのような対処をしなければならないのかなどを明確にした方針を「セキュリティーポリシー」と呼びます。コストや手間をどう効率的、効果的に扱うかということを考えると、いきあたりばったりにセキュリティー対策を考えるよりも、セキュリティーポリシーを決めたほうがよいでしょう。これはセキュリティーに限ったことではなく、おおよそどのような問題でも、方針と計画を明確にした後に実行したほうが効率的かつ効果的であるのと同様のことです。

四六時中システムを監視する人員を割り当てて試行錯誤的にセキュリティーを高めるといったようなアプローチは、ほとんどのSOHO環境では無理でしょう。不正アクセスに対して必要な対策を確実に行い、効率的、効果的に行うことでコストや手間を減らすことが、SOHO環境で求められる要件になることでしょう。

まずは、セキュリティーポリシーを決めるために、具体的にどのようなことに注意しなければならないかを考えていきたいと思います。SOHO環境における使用目的、機材構成、外部へ提供するサービスは、個々の状況により千差万別でしょう。1つとして同じものがないと思われます。

本連載でこれから示すセキュリティーポリシーはあくまでも雛型であり、アドバイスとしての基本的な情報です。そのままの形です

図1　SOHO環境モデル



べてのSOHO環境に適用できるとは考えていません。したがって、実際のSOHO環境上で不正アクセス対策に責任を持つ人が、自ら責任を負って決めていかなければなりません。

文書に残そう

まず、その前に、ちょっとしたアドバイスがあります。守ろうとするSOHO環境に対するセキュリティーポリシーを決めるときや実際に作業を行う際は、文書にして残しておくようにしましょう。これは、別に正式な文書やたいそうなドキュメントにする必要はありません。メモ程度のものでも構いません。ただし、必要なときにすぐに参照できる記録にしてください（図2）。人の記憶に頼ってしまうと、時間が経って記憶があやふやになり、困る場合があるからです。

最初に決めたセキュリティーポリシーやセキュリティーのための設定が、永遠に有効であるとは限らないことを初めから理解してください。

時間が経てばいろいろな状況が変化します。新しい攻撃法が見つかり、それに対処しなければならないかもしれません。あるいは、機材の入れ換えなどによって設定を変える必要が出てくることもあるでしょう。そのときに以前の記録を参照できないことで、作業の手間が増えたり、ネットワーク設定などのトラブルのために悩んだりして不必要な時間を費やす場合も出てくるかもしれません。それ以上に、状況が変化したがゆえにセキュリティーの見落としが出てくる危険性も考えられます。

セキュリティーポリシーを決めるにしても設定を行うにしても、人間が行うことなので、100パーセント完全であるという保証はどこにもありません。見落としやミスがある可能性は十分にあります。そのためにトラブルが発生した際にも、以前にどのようなことを行ったのかの記録があれば、役に立つことでしょう。

保護対象について考えてみよう

不正アクセスから保護する対象には、次のようなものが考えられます。

- ●コンピュータ
- ●ネットワーク
- ●情報（データ）
- ●ユーザー
- ●社会的信用

1 コンピュータ

コンピュータに対する攻撃にはいろいろな種類のものがありますが、SOHO環境における危険性が高いものを考えてみます。

- ●許可を得ていない外部の者によるコンピュータ資源の使用：一般ユーザー権限での不正ログイン、不正なコマンドの実行など
- ●管理者権限の詐取：ルート権限での不正ログイン、不正なコマンドの実行など
- ●メールの不正中継：スパムの中継、メール爆撃の中継など
- ●サービス妨害攻撃（Denial Of Service Attack）：提供するサービスの妨害、システムの負荷増大による運用妨害、システムのハングアップなど

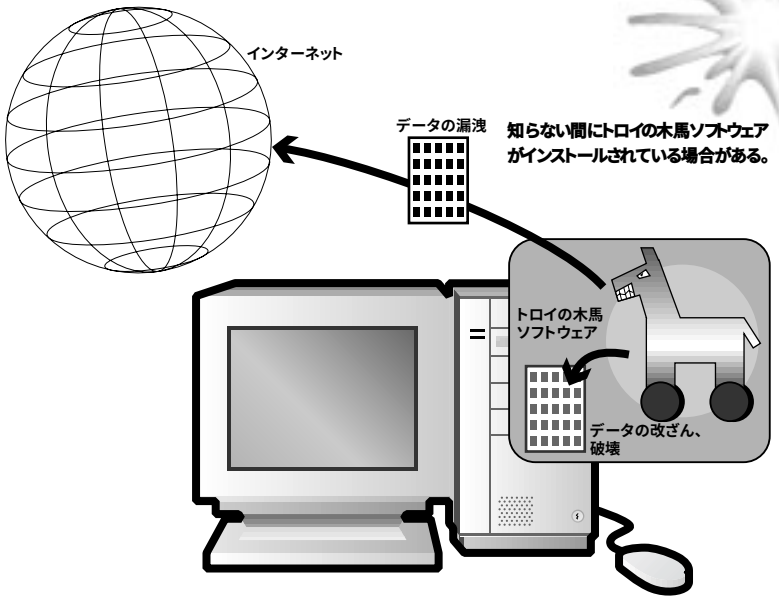
これらの中で、最初に挙げた一般ユーザーのアカウントに対する不正なログインに関しては、システムにはさして重大な影響がない

図2　セキュリティーに関する作業メモの例

```
1998.7.2.17:00
qpopのバージョンアップ
2.4→2.5

1998.7.5.19:00
ルーターのポート番号XXXを閉じる

1998.7.12.13:00
サーバーマシン1のバックアップをとる

1998.7.19.15:30
ftpdの起動を止める
```

日付や時間などと一緒に作業項目を文章にし、いつでも参照できるようにしておく。

図3　トロイの木馬



と思う方がいるかもしれません。しかし、不正アクセスを行う側は、あなたの管理するホストには興味がなくとも、そのホストを踏台にしてほかのサイトへ攻撃を行うかもしれませんし、ポルノ画像や海賊ソフトをコピーするための中継点に使うかもしれません。あるいは、スパムやメール爆撃のために使用するかもしれません。そうなれば、あなたのサイトの評判や社会的信用が大きく傷つくことでしょう。

2 ネットワーク

ネットワークについて考えられるのは、たとえばダイアルアップルーターにきちんとパスワードを設定していなかったために外部からルーター機能の設定を変えられたあとに、パスワードを勝手につけ変えられてしまうようなケースです。特にダイアルアップルーターは、モデムやTAと同様のネットワーク機材に思われがちなので、パスワードをつけ忘れるような初歩的なミスが見られます。

3 情報（データ）

情報（データ）の保護に関して考えましょう。保護しなければならない情報を大別すると、漏洩させてはならない情報と改ざんや破壊されてはならない情報の2つに分類されると思います。たとえば、サイトに届いたメールやパスワードファイルなどは、漏洩も改ざんもされてはなりません。WWWサーバーで提供されるWWWのページは、広く誰にでも公開する情報かもしれませんが、改ざんや破壊されてはならない情報です。サイト上の一切の情報に関して改ざんや破壊を許さないというポリシーに関しては異論のない所ですし、また、電子メールやパスワードファイルなどは漏洩しないように守る情報であるという部分も異論のない所でしょう。

しかし、時には隠すべき情報なのか、それとも公開する情報なのかを管理する人が決定しなければならないものもあります。たとえば、UNIXの「finger」コマンドは、ネットワーク経由で、ユーザーがシステムにログインしているかどうかなどの情報が取り出せるようになっています。これは、ユーザーが意図してfingerサービスを提供する場合、便利な機能であるといえるでしょう。一方、ユーザーが公開を意図しないままサービスを提供しているような場合、個人情報の漏洩につながる恐れがあります。これはユーザーの保護にも関係し、サイトごとに考えるべきことの1つです。

ネットワーク内部のデータの漏洩、改ざん、破壊を考える場合、コンピュータの保護で述べたように、外部からの不正侵入が最も考慮しなければならないポイントです。しかし、それ以外にも、トロイの木馬のような脅威も考慮しなければなりません。トロイの木馬とは、ギリシャ伝説に出てくるトロイ戦争において、ギリシャ軍が密かに木馬に隠れて城壁内に入り込んだ戦略から取られた名称です。ここでは、一見何の変哲もないソフトウェアに仕掛けが組み込まれており、ネットワーク内部で実行されると自動的にデータの漏洩、改ざん、破壊などを行うようなソフトウェアを指しています（図3）。

セキュリティー担当者の責任分担

一般の企業や大学といった組織においてセキュリティーポリシーを決めて実施するプロセスとSOHO環境でのセキュリティーポリシーを決めて実施するプロセスには若干の違いと注意点があるので、これについて述べたいと思います。

一般には、複数の担当者が責任を分担された形でネットワークセキュリティーにあたることが理想とされています。ある程度大きな組織になれば、このような形態も可能でしょう。

・セキュリティー対策の実施担当者
・不正アクセスを受けたときに対処する担当者
・セキュリティーポリシーが守られているかどうかを監査する担当者

実施と対処の担当者は兼任するすることが可能でしょうが、「監査担当者」は独立である必要があります。しかし、SOHO環境のように少人数での使用環境では、このような作業分担は難しい問題といえるでしょう。1人で使用しているSOHO環境も少なくはないと思います。ダブルチェックができない分、うっかりミスなどが発生しやすい点、あるいは管理がルーズになりやすい点に注意する必要があります。

シンプルなポリシーを適用

しかし、逆に小規模であることは、ユーザーのニーズが明確になりやすいという利点があります。大規模な組織では、ユーザーニーズが多様であったり、あるいは不明確であったりするので、セキュリティー対策は複雑になりがちで、その分コストも手間も必要になります。また、システムとしては必要なセキュリティーであっても、ユーザーの理解を得ることが難しいため断念するような場合もあるでしょう。ユーザーへのセキュリティー意識の徹底も大きい組織になればなるほど難しくなります。せっかく十分なセキュリティー対策を施したにもかかわらず、一部のユーザーが知らない間にセキュリティーを台無しにするような抜け道を作るというのもありがちな話です。会社や組織がデータ監査を行う必要があるため、ある特定の権限のある者は、すべてのシステム上のデータに自由にアクセスできなければならないというような場合もあるかもしれません。

SOHO環境ではそのような問題に頭を悩ませるケースは、非常に稀といえるでしょう。SOHO環境はシンプルなセキュリティーポリシーが適用できる場合が多く、その分、全体がコンパクトでシンプルなセキュリティー対策が可能になります。シンプルであることは、コストが低く、かつ、頑強なセキュリティーを構築するうえで大きなプラスの要因になります。このように、SOHO環境のように小規模であることの利点も欠点もあることをあらかじめ理解しておきましょう。