# インターネットでの不正行為その傾向と対策

**インターネットサービスプロバイダーが低価格な常時接続サービスを提供し始め、家庭における常時接続が現実のものとなりつつあります。
常時接続はダイアルアップ接続と違い、ネットワークやセキュリティーの知識を必要とします。そこで今回は、常時接続での注意点について紹介します。**

## 第10回
## IP常時接続における問題点

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

### 家庭での常時接続が始まる

インターネットを取り巻く環境は常に変化しています。特に、ここ1、2年（1998年春現在）は、インターネットサービスプロバイダー（以降ISPとします）が低価格な専用線による常時接続サービスを提供するようになり、普及の兆しを見せています。

これまで、家庭から個人的利用として、あるいは小規模オフィスにおけるグループ利用として、IPによるインターネットへの接続といえば、商用のISPにダイアルアップという形で必要に応じて接続していました。手元にあるパーソナルコンピュータは、クライアント的性格を帯びた利用であるものがほとんどでした。

ほんの10年前までは、研究所、大学、あるいは先端的な企業でしか行われていなかった専用線による常時接続が、現在では家庭でも現実のものとなっています。それらの需要に応じて、必要な周辺機器も小規模な利用を前提としたものが販売されるようになりました。今後、このような傾向はさらに強まるでしょう。

### 求められる技術は同じ

しかし、どんなに低価格な器材や簡便な使用方法であっても、インターネット上でのセキュリティーに関しての基本的知識は同じことを求められます。自動車の運転にたとえればわかりやすいと思います。自動車のドライバーは、誰もがよき交通社会の一員であることが求められ、また、安全な交通運転を行うための基本的な技量、知識、そして経験を求められます。

一方、（普通免許で運転できる範囲での）運転をするためのハードウェアとしての自動車は、軽自動車、大衆車、高級車まで、その価格に2ケタの開きがあります。大衆車や軽自動車はより多くの人たちの手に行き渡るような価格設定がされており、日本も含めて

先進国では高い普及率となっています。

だからといって、普及している大衆車や軽自動車が高級車よりも運転が簡単だとはいえません。安全運転のために求められる基本技術というのは、自動車の価格に関係ありません。また、路上で運転するすべてのドライバーに対し、等しく安全運転のための基本技術が求められます。

ところがコンピュータの世界では、価格および普及率と必要な知識が比例しているという考え方が一般には広がっているように見受けられます。つまり、低価格で普及しているものは、必要な利用技術に関する知識も少なくて済むという考え方で、コンピュータは家電製品に限りなく近づくという考え方に由来しています。

これは現状を反映していない考え方です。現在のコンピュータを考えてみましょう。コンピュータというのは情報を処理するという非常に汎用的な目的のために用意されたツールです。使用目的は多様であり、また、使用目的自体もどんどん変化しています。また、その必要に応じて機能や性能が非常に速いテンポで変化しています。

自動車もよく似ています。自動車とは、移動するという非常に汎用的な目的のために作られたツールです。その利用の目的、使用される状況、利用者に求められる知識や技量などは多種多様です。

スイッチを入れればユーザーやドライバーが何もしなくても、コンピュータや自動車が勝手に動いてくれたり運転してくれたりということは、少なくとも現在はありません。

人間が目的を持ち、かつ必要な知識や操作技術を身につけ、機械をコントロールして、はじめて安全に利用できるのではないでしょうか。

## 常時専用線接続

インターネットへの専用線常時接続という状況を考えてみましょう。今まで企業や研究所、大学でネットワーク管理をしていた専門家の知識だと思われていたものが、そうではなくなります。家庭における個人的利用、あるいは小規模オフィスにおけるグループ利用のための管理をする人たちも同じ基本的な知識を知る必要が出てきます。

しかも、現状のインターネットの状況を冷静に見つめれば、以前のような牧歌的な状況はすでに過ぎ去り、いろいろな面で複雑な問題が出てきています。自動車の運転にたとえるならば、大都会の混雑した道路状況の中を運転するといった様相だといっても過言ではありません。

不正アクセスに関して考えてみましょう。（今までは）専用線を用いてインターネット接続を行っている所では、ネットワークに関する知識をもった専門の管理者を割り当てているか、あるいは、それに近いような運用を行っている所がほとんどです。不正アクセスを防ぐためにインターネットへの接続構成の一環としてファイアーウォールを築いたり、ネットワーク接続周辺機器やコンピュータのシステムに対して適切な設定を行うことによって、外部からの攻撃を防ぐための施しをしたり、あるいは、不正アクセスの手掛かりを与えないための手段を講じていたりします。

図1　自動車とコンピュータの操作

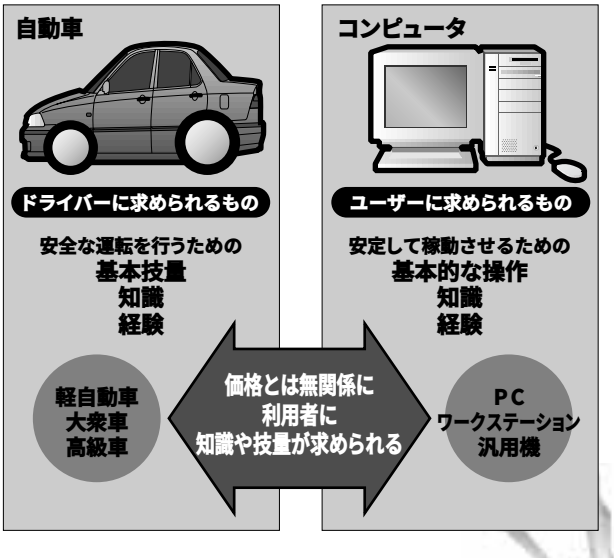
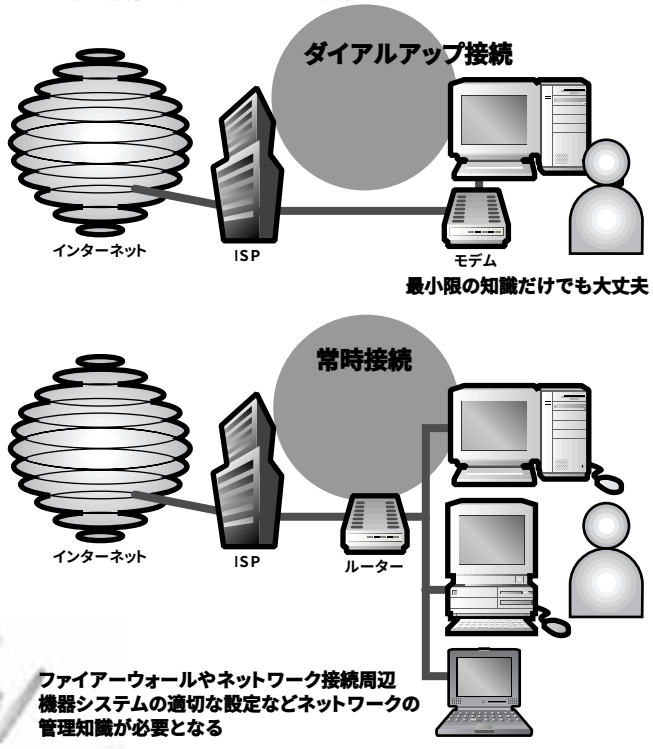



図2　常時接続とダイアルアップ接続の違い



不正アクセスに対してより注意を払っている組織などでは、運用責任者（あるいは運用責任者に相当する者やグループ）により、セキュリティーポリシーと呼ばれるような、組織内においてのセキュリティー指針を制定し、運用している所もあるでしょう。

JPCERT/CCやほかのIRTが提供するようなアナウンスや、アラート、セキュリティーに関する報告やドキュメントに常に注意を払い常時チェックしている管理者も多いことでしょう。

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

残念ながらそのように専門の管理者を置いて運用しているサイトであっても、すべてがすべて不正アクセスを考慮して対処しているとは限りません。不正アクセスに対する認識が甘かったり、あるいは、技術的に十分に対応できていないサイトも少なからず存在します。

今後は、専用線常時接続を行う誰もが不正アクセスに対する対抗策を講じるために、単純に当面の時間や手間がかかるだけではなく、最新の知識を修得するために不断の努力を払う必要が出てきます。

## なぜ、うちのサイトが!?

「よく知られている企業や大学といった大きなサイトは、不正アクセスを行う者の攻撃の対象になるというのは理解できるが、なぜ個人的に使っているようなサイトまでが攻撃対象になるのか。また、小規模のサイトであるにもかかわらず、どうやって見つけるのか」と疑問に思う人がたくさんいると思います。まずは、その疑問に答えたいと思います。

不正アクセスを行う者にとって、どんな小さな専用線常時接続であるサイトであっても、それを踏台サイトとして使う可能性があります。踏台サイトとは、本来の攻撃目標に対しての隠れ蓑となるサイトのことです。事前にほかのセキュリティーが甘いサイトをいくつか事前にクラックしておき、その踏台サイトをいくつか経由して、本当の攻撃目標に対して本格的な不正アクセスを行います。

攻撃にさらされているサイトから攻撃側を探した場合、最悪だと、セキュリティーの甘い第三者のサイトが不正に使われていることしかわからなくなってしまう場合もあります。

家庭で趣味の範囲で使われているデスクトップのコンピュータであっても、現在のマシンの計算能力は、攻撃に使う踏台マシンとしては十分です。また回線速度も十分です。

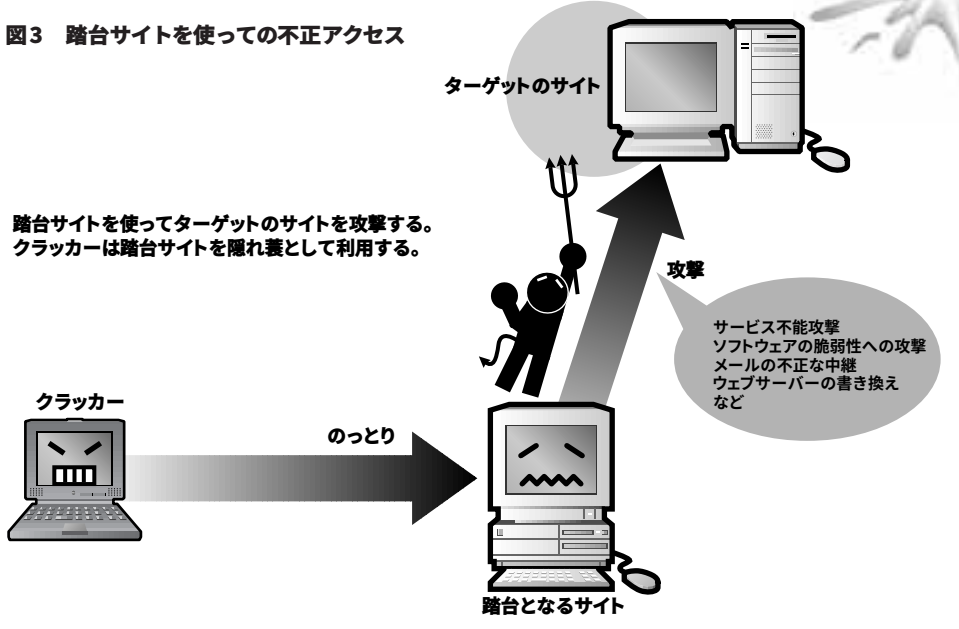
読者の中には、「自分のサイトなんて趣味以外のものは何も入っていないし、全部壊されてもいいや」と思っているかもしれません。しかし、セキュリティーが甘いため、踏台サイトとして使われた場合、まったく知らない間にほかで発生しているより深刻かもしれない不正アクセスの事件に、何らかの形であなた自身も巻き込まれてしまう危険性があることをよく承知しておいてください。

さて、次は踏台にするサイトをどうやって見つけるかです。方法は簡単です。とにかく可能なIPアドレスをスキャンし、しらみつぶしにアタックしてみるからです。より効率よく探査の可能性を高める方法はいくつかありますが、基本的スタンスは、試行錯誤によって手あたりしだいに探します。

一説には、世界には数千万のサイトが接続されていると言われています。毎秒10サイトの割合で探査を行っていけば、たとえ1億サイトであったとしても115日でチェックできる計算になります。実際は、もっと効率のよい探査を行うので、さらに少ない時間ですむと予想されます。

ですから、地球の裏側にいる不正アクセス

図3　踏台サイトを使っての不正アクセス



の行為者があなたのサイトを見つけて使っている可能性もあるのです。

## 考えられる攻撃

考えられる不正アクセスのタイプを以下に挙げてみますが、これらの問題は、研究所、大学あるいは企業といった以前からインターネットに専用線で接続していた組織が過去から現在に至るまで直面してきた問題とまったく同じものです。

●サービス不能攻撃（Denial of Service Attack）：オペレーティングシステムのネットワーク機能の脆弱性に対して攻撃を行い、システムを使用不能な状態にする。

最近は、莫大な数のサイトに対し、無差別かつ一斉に行う傾向があります。サイトの大小、有名無名にかかわらず、きちんと対処していない数多くのサイトが使用不能に陥ることになります。

●ソフトウェアの脆弱性への攻撃：IMAPやstatdなど実際は使っていないにもかかわらず、システムにインストールされているソフトウェアに対して攻撃を行い、各種の問題を引き起こす。

実際には使用していないけれども、システムインストール時にインスールしていて、そのまま存在を忘れている例が多く見られます。そのまま放置すると、不正アクセスの絶好のターゲットになってしまう危険性があります。これらを突破口にさらに深刻なシステムへの侵入およびルート権限略奪といった事態に進行していく可能性があります。

●メールの不正な中継：不正中継を防ぐsendmailの設定をしていないサイトを経由してスパムを大量送付する。

現在、一度に数百万の単位で送出されると言われているスパムの不正中継に使われる可能性があります。また、不正中継を許したサイトも同罪だという社会的風潮も一部で見られ、厳しい批判を受ける場合もあります。

●違法なファイルのコピーサイト：商用ソフトウェアの不正コピーやポルノといった違法なファイルのファイルサーバーとして使用される。

FTPなどの設定を間違えていると、外部から勝手にファイルを置かれ、違法なファイルのコピーを中継するサーバーとして使われる場合があります。

●ルート権限略奪：ルートの権限を入手して、サイトを乗っ取る。

システムに対し、深刻な脆弱性をもった古いソフトウェアをそのまま使用していて、かつ間違えた設定を行っているとルート権限が略奪されることにつながりかねません。これが発生すると非常に深刻な問題になります。

それ以前の問題として、ソフトウェアに問題がなくても設定に深刻なミスがあれば、ルート権限略奪の恐れがあるのは言うまでもありません。また、ルート権限略奪の危険性はコンピュータだけでなく、ルーターといったネットワーク機材に対しても存在しています。

●ウェブページの書き換え：ウェブページを不正に書き換える

ソフトウェアの脆弱性をそのまま放置していて、さらに設定ミスが重なることによって、システムに直接侵入しなくとも、外部からウェブページを書き換えることが可能になります。

## 何を行う必要があるのか

企業や組織では、セキュリティーポリシーと呼ばれる不正アクセスに対する運用基準を明文化してそれに沿って対処する、あるいは対策を立てるということが行われます。そして、ある程度のコストをかけて対策を施します。

しかし、家庭で趣味で行う範囲や小規模オフィスでこれらの本格的なセキュリティーを施すのは、現実的には難しいでしょう。ISPによっては、そのような運用の大変さをカバーするようなサービスを提供している場合もあるでしょう。専用線常時接続サービスを開始するに当たり、ISPに対して事前に相談するのも1つの手段です。

専用線常時接続では、単に常時接続にしていてクライアントを置いているだけなのか、あるいはメールサーバーやウェブサーバーを用意するのかなどで設定も全然違ってきます。今回のような短い説明で、何が必要で何が不必要か、あるいはどのような対処をすべきなのかを説明するのは無理なので、また別の機会に改めて説明したいと思います。

## まとめ

最近普及している低価格での専用線常時接続サービスは、10年前まで研究所、大学、あるいは先端的企業でしか行っていなかったインターネットへの専用線接続を、自宅や小さなオフィスでも可能にするものです。その恩恵は非常に大きいといっても、決して言い過ぎではないと思います。しかし、不正アクセスに対する危険性も同じものを背負うということを同時に理解しなければいけません。

**編集部から**

次号のこの連載では「初心者のためのセキュリティー講座スペシャル」と題しまして、皆さんから寄せられたご質問に対するQ&Aを企画しております。
本連載に対するご意見やご質問、不正アクセスに関して知りたいことがありましたら以下のメールアドレスまでお送り下さい。
E-mail ip-security@impress.co.jp