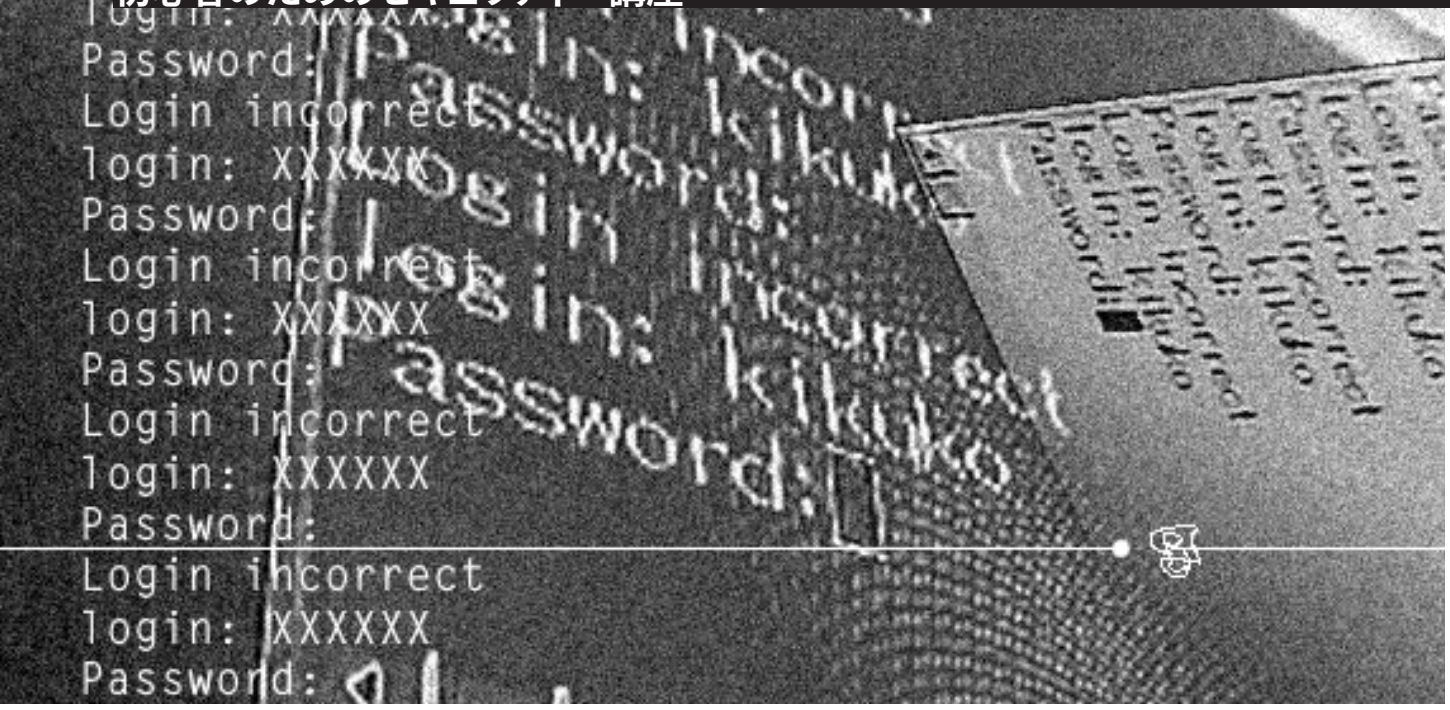
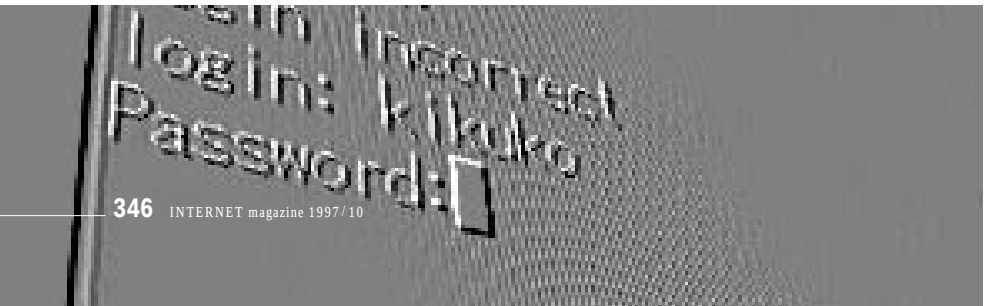


インターネットでの 不正行為 その傾向と対策

不正アクセス。ちょっと耳慣れない言葉かもしれませんが、これはいったいどんなことを意味するのでしょう。私たちは、インターネット上でどんなリスクと隣り合わせているのでしょうか。
不正アクセスの具体的な内容をまず知って、意識しておくようにしましょう。

第2回 不正アクセスとは何か？

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



今回は不正アクセスとは何かの話をしましょう。不正アクセスとは、前回もお話ししたとおりに、「システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと」です。もう少し分かりやすい言葉でいうと、侵入者（イントルーダー）や攻撃者（アタッカー）が企業、団体、個人などのシステムを権限もないのに不正に利用したり、運用を妨害したり、破壊（クラック）したりすること(脚注)です。

一般的な傾向として、業務などでインターネットを使っている人は、セキュリティーに対して配慮をしているものですが、趣味などで使っている人は、あまり気にかけない傾向があります。「別に自分のアカウントに侵入されても、もともと使っていないのだから、特に困ることはない」という話をよく耳にします。

しかし、そのような使っていないアカウントこそ、そこから最終的な目標であるサイトへの侵入を行ったり、違法な行為を行うための連絡口に使うといったときの絶好の隠れミ

脚注：英文では、無法な侵略者、破壊者という意味でヴァンダル“ Vandals ”という表現を用いる場合もあります

ノになります。不正アクセスの説明の中で、踏み台サイトとか踏み台アカウントとかいうときの、踏み台は、このような隠れミノに使われていることを意味しています。この場合、不正アクセスを行なった者が非難されるだけではなく、その踏み台として悪用されてしまったサイト自体も社会的、道義的な責任を問われて非難の対象となる可能性があります。

不正アクセスは、ケースによって刑事および民事の法的問題へと発展する可能性もありますが、その件に関しては、JPCERT/CCが関与できる話題ではないので、ここでは言及しません。また、ページの都合上、ここで紹介する個々の不正アクセスに関する対策の詳細は、次回以降の連載で取り上げていきます。

不正アクセスの種類(ユーザー編)

不正アクセスで、まず主に一般ユーザーが直接に被害を受ける可能性があるものに関して取り上げます。

パスワードの盗難

パスワードは、システムを利用する際に認証の目的で使われるコード(文字の並び)です。このパスワードを知っているかどうかで、ユーザー本人であるかどうかの認証を行っています。つまり、パスワードを盗まれると、あたかもユーザー本人であるかのように偽ってシステムを悪用されることになります。

他人のパスワードを入手する方法には、多種多様な方法があります。最も古典的な方法は、たとえばサイト管理者になりすまし、電話口で「あなたのパスワードのチェックをします。そのために現在のパスワードを教えてください」などといって聞き出す方法です。ごく一般的とも言える詐欺の手法ですが、パスワードの盗難によく使用される手口です。

その他の古典的な方法としては、パスワードを入力しているとき、背後から入力を盗み見るというものがあります。どんなに速くキーボードをタイプしても、慣れた人が見るとだいたいどんなキーを押したか分かってしまいます。また、パスワードを忘れないように書いてあったメモを盗み見られるという、初歩的なミスも挙げられるでしょう。

以上は、直接、ユーザーにコンタクトする必要がありますが、ユーザーにまったくコンタクトすることなしに、パスワードを取ってしまうこともあります。その1つの方法に、パスワードの類推(Guess)があります。

たとえば、Yamada Taroという人が、パスワードでyamadaとかtaroといったものを使っているとしたら、あるいはアカウント名NSC29188のためのパスワードがNSC29188であったりするなら、それは正常なパスワードとしての役目を果たしているとはいえないでしょう。単純なパスワードは、はるかに短い時間で見つけられてしまいます。特に後者の例のように、アカウント名＝パスワードは、パスワード類推をする際に、まず最初に試みられるパターンです。

また、英単語をそのまま使っている場合も危険です。英単語辞書を使って、片っ端から試していけばいいからです。いちいち手で入力する必要はなく、専用のソフトウェアを用意して自動化します。一般ユーザーからパスワードファイルが見えてしまうシステムでは、あるいはパスワードファイルが盗まれてしまった場合は、いくらパスワードファイル内のパスワードが暗号化されているからといっても、英単語1語などの安易なパスワードを使っていれば、数時間で確実に破られてしまいます。

もし、管理者用のアカウントであるルートのアカウントに対してこのような弱いパスワードが設定されていたら、システム全体が危機にさらされることになります。

まずは個人個人がしっかりしたパスワードを付けるとか、あまり長い期間にわたって同じパスワードを使い続けないといったことに気を配ることによって、パスワード盗難の可能性を低くすることができます。

●

今回、いろいろなレベルの不正アクセスを紹介しますが、不正アクセス対策の基本中の基本は、パスワードを守ることです。パスワードを盗み、サイトへ侵入することが多くの不正アクセスの最初の侵入口であり、侵入しようとする者の目的達成の第一歩です。万が一侵入されてしまうと、そこを踏み台にして、さらに多くの不正アクセスを繰り返すといった不正アクセスの温床になってしまう恐れがあります。パスワード盗難には、くれぐれも注意してください。

電子メール偽造

電子メール偽造とは、差出人情報を偽造して、電子メールを送り、相手をだますような行為を指します。偽造にもいろいろなレベルがあります。単純なものは差出人のメールアドレスを嘘のアドレスにするというレベルから、送付履歴情報まで偽造して完全に見分けができなくしてしまうレベルまであります。基本的には「なりすまし」による被害です。なりすますことによる詐欺やいやがらせなどを行う土壌になります。単純なものは簡単に偽造を見破ることができますが、高度なものになると、電子メールに付いている情報が本物と見分けがつかなくなるわけですから、電子メールからは偽造かどうかが判断できなくなります。この場合、電子メールでのなりすましは、電子メールで送る文に対し、暗号技術を用いた電子署名を付けるようなことによって、防止することが可能です。

電子メール爆弾

大容量かつ莫大な数の電子メールを相手に送り付ける攻撃です。たとえば、巨大なメールや多量のメールを受け取ると、使っているメールソフトがハングアップしてしまったりする場合があります。もっと深刻なものになると、サーバー側の電子メール保管の許容量を超えてしまい、他の電子メールが受け取れない状況になることもあります。電子メールを業務で利用している場合、業務ができなくなることによる経済的損失などを被る可能性もあります。現在では、多くのサイトで電子メール爆弾に対する対策が進んでいます。

不正アクセスの種類(システム編)

サーバーなどのネットワークのシステムで問題となる不正アクセスに関して取り上げます。

SENDMAIL攻撃

電子メール転送プログラムSENDMAIL(多くのメール配送は、このSENDMAILというソフトによって行われる)の弱点を悪用して、不正な遠隔操作を行う方法です。SENDMAILのような広く普及しているソフトウェアを悪用した攻撃を防ぐうえでの大きな問題点は、ソフトウェアの弱点の発見から対策が実施されるまでにタイムラグが存在することです。ソフトウェアにまったく新しい弱点が発見された場合、その弱点に対応した新しいバージョンが発表されるまでの期間、そこへの攻撃には無防備になります。サーバー管理者の方は常に最新のセキュリティー情報に注意を払うことが大切です。ソフトウェアにセキュリティー上の弱点が発見されていることを知らずに続けると、その弱点を狙っての攻撃を受ける可能性があります。また、弱点の存在を知ってはいても、何らかの理由があってセキュリティー対策を施すことができないサイトも同様です。このような攻撃を受けると、遠隔操作によって不正なプログラムを実行されたり、あるいはパスワードファイルが盗難にあったりする可能性があります。

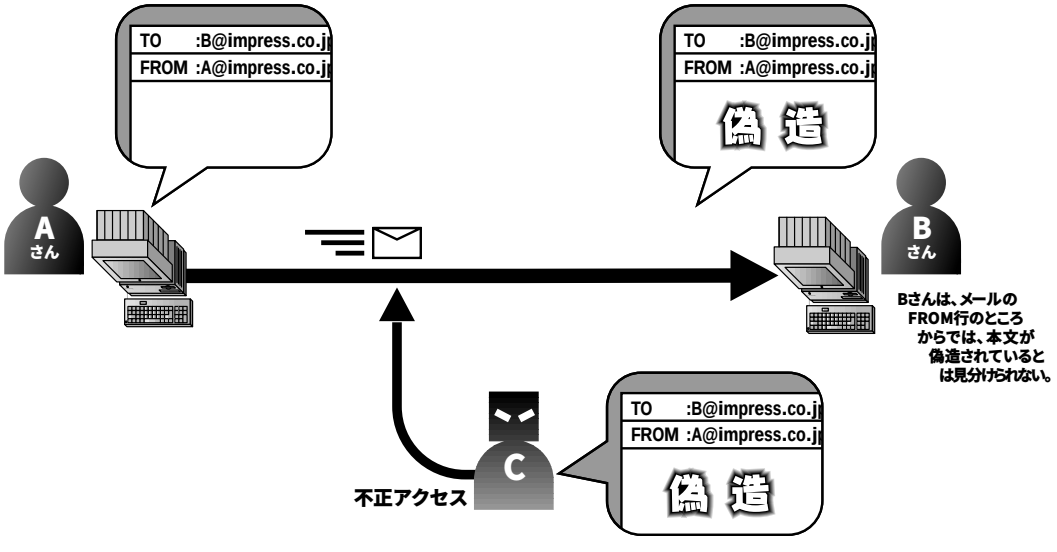
WWWサーバーCGIプログラム攻撃

CGI(Common Gateway Interface)は、WWWサーバーの機能をさまざまな形に拡張するために用意された仕組みです。たとえば、対話的に利用者のリクエストを処理するといったさまざまな機能拡張を行うための枠組を提供します。このCGIの枠組に準拠して作成され、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を総称してCGI-BINプログラムと呼びます。古いWWWサーバーのパッケージの中にもともと付属しているCGI-BINプログラムの一部には、外部から不正なコマンドを受け付けてしまうというソフトウェア上の弱点がありました。これもSENDMAILと同様に、最近のWWWサーバーのパッケージでは、すでに問題は解決されていますが、古いパッケージをそのまま使い続けていて、その問題の対策を行っていないサイトなどでは問題が発生します。CGIは、サーバー管理者がプログラムを自由に作成して追加することができますが、そのプログラムは外部から実行できるので、セキュリティー上の問題はないか、プログラム中にセキュリティー上の問題はないかといった点検を注意深く行う必要があります。また、中身をよく確かめずに安易にどこかのFTPサイトからCGIのプログラムをコピーしてくるといったことも、そのプログラムがセキュリティー上の穴になる危険性があるので、注意しなくてはなりません。

匿名(Anonymous)FTPの不正利用

不特定多数に対するファイル提供サービスを行うために用意したFTPサーバーでの設定の間違いや不注意から発生する不正利用です。匿名FTPを運用しているサイトで、ファイルやディレクトリーに対する読み書き権限を間違えて設定したり、あるいは不注意に外部からファイルを自由に書き込みできるように設

■電子メール偽造



定していた場合に問題となります。外部から自由にファイルの書き込み（転送）ができる場合、商用ソフトの海賊版をいったんそのFTPサーバーに置き、そのFTPサーバーを通して不法配布を行なうといった踏み台に悪用されます。アクセスのログを詳しく記録できるタイプのFTPサーバーを利用していても、ログをチェックして不審に気づき、その悪用に管理者が気がつくまで、この行為は継続されることになります。あるいは、短期間だけ利用して、あとはファイルを削除しておくといったことをされると、発見はさらに難しくなります。この問題は、正しくFTPの環境が設定されているかどうかを注意深くチェックすることによって回避できます。

パケット盗聴

侵入したサイト上で、侵入者にルート権限（これを持つことによって、ネットワーク管理者レベルのネットワークへのアクセスが可能になる）を盗まれてしまった場合、このパケット盗聴のソフトウェアを使うことによって、さらにそのホストが接続されているネットワーク全体に流れる情報を盗聴される恐れがあります。ネットワークを介して他のマシンにログインした場合、ネットワーク上にパスワードが流れてしまいますから、そのパスワードが盗まれてしまう可能性があります。このときはパスワードの類推などとは違い、ネットワーク上を流れる、キー入力したままの暗号化されていないパスワードが盗まれます。

不審なプロセスが長時間走っていないかなど注意するべき点はありますが、パケット盗聴は何の前触れもなく行われるわけではなく、そこに至るまでの何段階かのステップを踏んだ後に初めてできる種類のものです。ですから、その前の段階で不正アクセスをストップさせなければいけません。

不正パケット攻撃

ある種の通信パケットを不正に大量に送り付ける、あるいは、ある種の不正なタイプの通信パケットを送り付けることによって、オペレーティングシステムをマヒさせてしまう攻撃です。システムがマヒしてしまいますので、そのマシンの運用ができなくなってしまいます。不正パケット攻撃への対策済みのオペレーティングシステムにバージョンアップしたり、オペレーティングシステムへのパッチを利用することによって防ぐことができます。しかし、サイト内で動作しているソフトウェアが新しいオペレーティングシステムのバージョンに対応できていないため、どうしても古いオペレーティングシステムを使い続けなくてはならないという場合、問題は深刻です。

まとめ

今回は、ユーザー編、システム編の両方にわたって、主な不正アクセスの種類とその大まかな説明をしました。次回からは、ユーザー編を中心に、具体的にどのような点に注意すればいいのかについて説明していきたいと思います。この連載のほかにも、JPCERT/CCでは、WWWページでセキュリティー情報を提供しています。ぜひ御覧ください。

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

■パケット盗聴