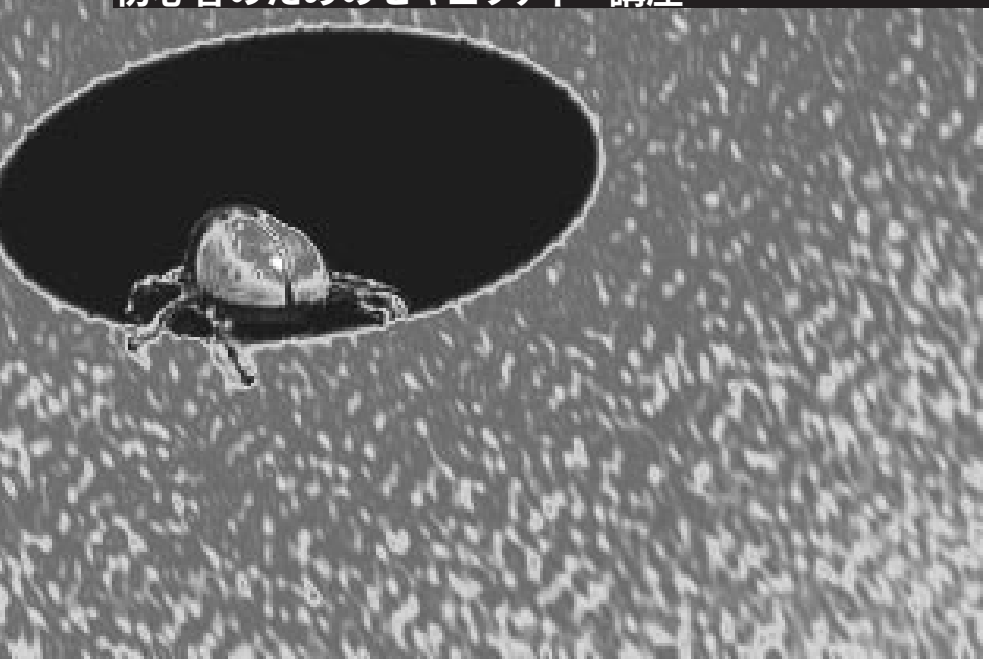
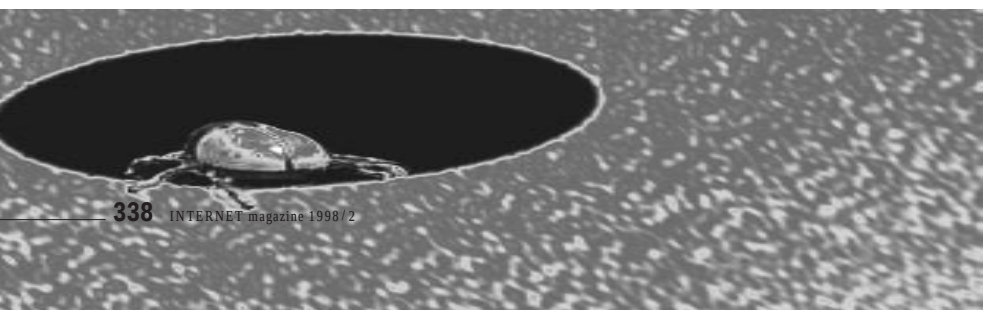


インターネットでの不正行為その傾向と対策

もし、あなたが乗っている車に欠陥があったらどうしますか？
当然、ディーラーに持っていて修理してもらいますね。でも、ソフトに欠陥があったらどうしますか…。
ソフトウェアには実は無数のバグが存在します。
そのバグの中には実はやっかいなものがあるのです。車にたとえるなら、窓が勝手に開いてしまったり…。今回は、そういったソフトにまつわる話です。

第6回 ソフトウェアのバグとセキュリティー
日頃の情報収集と迅速な対応がカギ

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



バグとは何か

ソフトウェアに紛れ込んでいる誤りをバグといいます。広く使われる言葉ですが、バグという言葉は、ソフトウェア品質の分野で使われる3つの厳密な定義、ソフトウェア故障（Software Failure）、ソフトウェアフォールト（Software Fault）、ソフトウェアエラー（Software Error）を全部含んだ、少し曖昧な言葉です。

この意味を少し説明すると、ソフトウェア故障とは、ソフトウェアの動作の誤った現象を指します。ソフトウェアフォールトとは、ソフトウェア故障の原因となった誤りを指します。ソフトウェアエラーとは、原因となった誤りを作り込んでしまった行為やプロセスを指します。このエラーとフォールトの違いを短く補足すると、ソフトウェアエラーとは、単にソースコードの間違えた記述だけではなく、要求する機能や性能を間違えてとらえていたり、見落としていたり、仕様が正しくプログラムに反映されていなかったりといったことも含めています。そのソフトウェアエラーが表面化したのが、ソフトウェアフォールトです。

ソフトウェアを使う際には、次のことを前提にしなければなりません。『ソフトウェアには、バグがつきものです。ソフトウェアには何かしらのバグがあることを前提に使いましょう』。そう言い切ってしまうと、少々とまどう人も多いのではないかと思います。コンピュータの無謬性、つまりコンピュータには間違いがないという、実は現実からは程遠い幻想が、かなり広範囲に信じられているように見受けられるからです。

多くの方が理解されているように、ソフトウェアとはコンピュータをどのように動かすかを決めるものです。ソフトウェアが間違っていれば、当然、コンピュータは正しく動作しません。しかし、ソフトウェアとは、人間が、どのように動作するかを設計して、その命令手順を作り上げたものです。その作る人間が間違いを犯すと、当然、その間違いがソフトウェアの中に組み込まれてしまいます。人間

が完璧ではない以上、ソフトウェアも同様に完璧ではありません。

そして、ソフトウェアは、その内部構造の複雑性と動作の状態遷移の複雑性から、完全なテストを行うのは、非常に困難を極めるのです。また、十分にテストを行うためには、莫大なコストと時間が必要になります。また、ソフトウェア開発の特徴として、人やお金をつぎこんだからといって、開発のスピードやソフトウェアの品質が格段に向上するわけではないという、通常の工業生産とはまったく異なる特徴があるのです。

バグが発生するタイミングも、ソフトウェアを開発するプロセスの、いずれの段階でもありえます。ソフトウェアの仕様を決める段階であったり、ソフトウェアの設計を行う段階であったり、ソフトウェアを実装する段階であったり、実にさまざまです。

難しいことを書いているように感じられるでしょうが、言いたいことは至って簡単です。それは「ソフトウェアにバグはつきものである」ということなのです。そのために、ソフトウェアにも、なんらかのメンテナンスが必要になります。

バグによるセキュリティーホール

ソフトウェアの内部に潜在しているバグが現れるのは、たとえどんな形でも困るものです。使用しているアプリケーションが暴走し、マシンが入力を受け付けなくなってしまったり、使用中のファイルが壊れてしまったりするバグもあります。あるいは、システムソフトウェアやオペレーティングシステム自体にバグがあり、使用しているシステムが停止してしまうような場合もあります。

そのようなバグの中には、外部からの不正アクセスのターゲットとなるような、セキュリティーホールとなってしまうものがあります。よく知られている例が、いくつかのオペレーティングシステムのネットワーク機能には、規定より大きなサイズのデータが入ってきた場合にオペレーティングシステム自身がダウンしてしまうバグです。それまでの各種のオペレーティングシステムでは、規定より大きいサイズのデータを送り出そうとしても、そのようなデータは異常データであり、送り出せない機構になっていました。したがって、規定より大きなデータサイズである異常データは、ネットワーク上に存在しなかったのです。当然、オペレーティグシステムには、長い期間にわたり、そのバグが潜んでいたにもかかわらず、決して、そのバグが現れることがなかったのです。

ところが、今まで送り出せなかったはずの、規定サイズより大きな異常データを送り出すことをしてしまうオペレーティングシステムが現れてしまいました。今まで、潜在していたバグが、オペレーティングシステムをダウンさせるという致命的な形で表面化してしまいました。この異常なデータは、管理者権限など必要なく、通常のユーザーでも送り出すことができるので、さらに問題は深刻でした。この話には2つの大きな教訓があります。まず第一点は、どんなに長年安心して使っていたソフトウェアでもバグを抱えている可能性があるということ。

第二点は、それがいつどんな状況で現れるかは、予想できないことです。

一般に、新しく作ったソフトウェアは、稼働実績が少ないので、まだバグを十分に潰しきれていないため注意が必要だということが言われます。しかし、長年使ってきたソフトウェアですら、周りの状況が変化すれば、新しいバグは見つかるのです。ソフトウェアとバグの関係は、そんなに単純な関係ではないことが、このことからもよく分かると思います。

情報入手までの時間差

このようなソフトウェアのバグによるセキュリティーホールの発生を事前に察知したり予測したりすることによって対処することは、非常に困難です。したがって、発見された後の対処をいかに迅速に行うかが不正アクセスへの現実的な対処方法になります。

一般的には、深刻なセキュリティーの問題を引き起こすバグに関しては、発見され次第、短い時間で修正がなされ、対処済みの新しいバージョンの配布が開始されます。その対処されたことに関する情報は、JPCERTやCERTといったIRTや、ベンダーからアナウンスされます。

ここには1つの問題があります。それは、セキュリティーホールを修正したソフトウェアに関する情報を入手する時間差があることです。本稿を読んでいるような方々は、それだけセキュリティーに関心を払っている方々なので、最新のセキュリティー情報に注意を払い、このような修正に関してすぐに対処する人がほとんどだと思います。

しかし、セキュリティー情報に関心を払わないため、あるいは、ソフトウェアの特性をよく理解していないため、ソフトウェアにもメンテナンスが必要だということに注意を払わない人たちは、修正するのが遅れる、あるいは修正をしないままの状態になってしまう可能性があります。これは非常に危険な状態であるということに多くの人が気づいてほしいと思います。

システム管理者が注意を怠ったため、オペレーティングシステムやシステムソフトウェアのバグをついて不正アクセスが行われてしまうということになりかねません。

必ずしもオペレーティングシステムやシステムソフトウェアだけが問題だというわけではありません。パーソナルコンピュータの場合、ユーザーの権限で自由にシステムを操作できますので、ユーザーアプリケーションのバグによるセキュリティーホールのため、コンピュータ上の任意のファイルを盗んだり、あるいはハードディスクの内容を全部消すといった不正アクセスも最悪の事態として考えられるのです。

セキュリティー情報の収集

セキュリティーホールとなったバグは、修正を行うベンダーや開発者だけではなく、やが

て不正アクセスを行う側に対しても同じく知られることになります。そのため、そこから先は、修正済みのソフトウェアにいち早くアップデートすることと、そのバグを利用して不正アクセスを行うこととの競争になります。不特定のネットワーク使用者からアクセスされるサーバーを管理している管理者は特に注意が必要です。外部からの不正アクセスを考えた場合、インターネット上には星の数ほどサーバーがあるので、自分の管理しているサーバーが攻撃対象となる確率はわずかだと考えるかもしれません。しかし、それは誤りです。

例えば、自動的にセキュリティーをチェックするソフトウェアを悪用すれば、インターネット上に存在する多数のサーバーを片っ端からチェックするようなことが可能だからです。これらのシステムのセキュリティーをチェックするソフトウェアには、すでにセキュリティーホールとして知られているバグを持っているバージョンを使っていたら、すぐに検知してくれる機能を持つものもあります。

システム管理者が使う分には、これほど便利なツールはありませんが、不正アクセスを行う者にとっても同様に便利なツールです。そのようなツールを使えば、狙ったシステムにセキュリティーホールが存在しているかを知ることが可能になるのです。

あるいは、特定の目標を決めずに、とにかく不特定多数のサーバーに対し、不正な命令をとにかく与えてみて反応を見るという、荒っぽい手法もあります。

とにかく、管理する側は、セキュリティーホールとなったバグが発見されたら直ちに、積極的に対処していくことが、不正アクセスを効果的に防ぐ方法であることは変わりありません。

ソフトウェアの導入

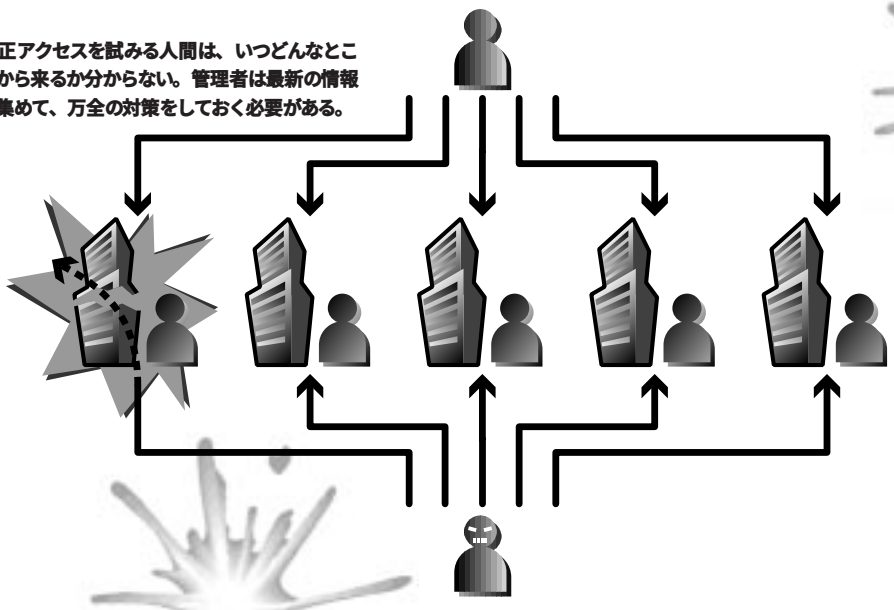
バグが修正されたソフトウェアを入手し、入れ換えを行い、セキュリティーホールを取り除く時の注意点についていくつか書いてみます。

なんといっても、信頼できるソフトウェアを入手することが肝要です。これをチャンスとばかりに、悪意を持って不正アクセスを狙った者が、バグを修正したふりをして、トロイの木馬であるようなソフトウェアを配布する可能性も否定できません。誰が変更を行ったか分からないようなソフトウェアなどは、使用しないようにしましょう。

入手したソフトウェアあるいはパッチファイルが改ざんされていないか、あるいは偽造されたものではないかなどを、電子署名を使って、あるいは一貫性チェックを使って確認しましょう。なお、確認する方法としては、ここで説明する以外にもいろいろなツールや方法がありますし、時とともに変化したり改良されたりしていくので、必ずしもここで挙げた方法でなければいけないというわけではありませんので、注意してください。

現在、多くの場合、ソフトウェアの配布元は、一貫性に関するデータや電子署名を検証するための公開鍵といった情報を事前に配布していたり、あるいは公開したりしています。確実に確認したい時は、前記のようなデータを直接入手してチェックします。特にアップデート用のパッチファイルといったものは、直接配布元から配布される以外にも、例えば、BBSやネットニュースに流されるといった具合に、いろいろな経路で入手できる場合があります。このように間接的に入手した場合は、確実にチェックを行ってください。

直接ベンダーから入手していないような場合、特にパーソナルコンピュータは、コンピュータウィルスに犯されやすいので注意が必



不正アクセスを試みる人間は、いつどんなところから来るか分からない。管理者は最新の情報を集めて、万全の対策をしておく必要がある。

要です。再インストールやアップデートの手間をおしんで、どこかのパーソナルコンピュータ上にインストールされたソフトウェアをそのままコピーして使うといったことは、コンピュータウィルスの感染原因になる可能性があるので、なるべくやめましょう。

管理責任の明確化

複数の利用者が機具を共有したりする場合や、実際に作業を行うシステム管理者とそのシステムの運営担当者が異なる場合などは、いったい誰が責任を持ってソフトウェアのバグに対処していくかを明確化しなければいけません。なぜなら、ソフトウェアのアップデートに金銭的負担がかかったり、あるいは、入れ換えのための作業負担が発生したりする場合も考えられるからです。常時運転しているサーバーマシンであれば、時によっては、サーバー機能を停止させたうえで作業しなければいけない場合もあるでしょう。その際に、あらかじめ管理責任の明確化を行っていないと、迅速な対処が難しくなる場面が出てくる可能性もあります。そのように迅速な対処が行えない間、システムが不正アクセスに対して無防備な状態が続くことになりかねません。

設定ミスやその他

必ずしもソフトウェアのバグではなく、設定ミスであるような場合が考えられます。例えば、UNIXなどでは、サーバー機能として用意しているソフトウェアでも、デーモンとして実行するのか、それともinetdとして実行するのかなど、同じソフトウェアでも、実行環境によって状況が異なる場合があります。そのように、状況も変わってしまうことによって、セキュリティーの問題を引き起こす場合と引き起こさない場合が出てしまいます。この違いも注意してください。

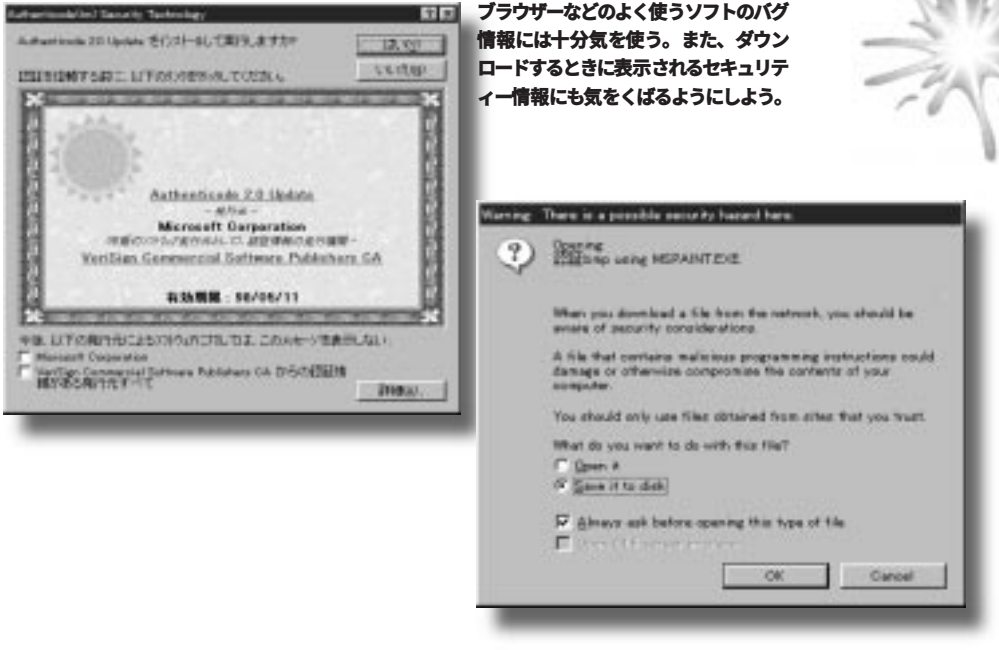
あるいは、必要のないサーバー機能を入れていて、その存在を忘れている場合もあります。実際には使用していないサーバー機能なので存在が忘れられ、セキュリティーホールを持った古いバージョンのまま放置されていたという例が見受けられます。もう一度システムの見直しを行い、使わないサーバー機能は削除するか、あるいは実行不可能にしておきましょう。

まとめ

ソフトウェアのバグが引き起こすセキュリティーホールは、ソフトウェアの宿命だとも言えるものです。特に近年は、短時間のうちに新しいソフトウェアが活発に発表されたり、既存のソフトウェアに大幅な改造や拡張が行われたりする傾向にあります。

新しい機能を採り入れたが、十分に安全を確認しないまま配布してしまったというようなソフトウェアが散見されると同時に、既存のソフトウェアにとっても、動作する環境がどんどん変化していくため、今まで安全だったから今後も安全だとは言い切れない状況になっています。しかも、そのようなバグによるセキュリティーホールを専門に狙う不正アクセスが後を絶たないという状況もあります。やはり、そのような状況に対処するには、ベンダーやIRTが出す情報に常に注意を払い、最新のセキュリティー情報を入手することが必要だと言えるでしょう。

JPCERT/CCでは、本連載のバックナンバーをウェブサイト上で公開しております（PDF形式）。
URL http://www.jpcert.or.jp/magazine/beginners.html



ブラウザーなどのよく使うソフトのバグ情報には十分気を使う。また、ダウンロードするときに表示されるセキュリティー情報にも気をくばるようにしよう。