



あなたの会社のサーバが狙われています。  
セキュリティ対策は大丈夫ですか？

## ソフトウェアメンテナンスの重要性

ソフトウェアメンテナンスは“サーバセキュリティ対策の第一歩”です。

### ！ セキュリティとは？

#### インターネットから自分を守るもの

セキュリティとは、“自分のPCを第三者による望ましくないすべての行為から守ること”です。

お客様のPCがインターネットに接続するという事は、インターネットに接続している第三者から逆にお客様のPCに接続できるということになります。もし、第三者に悪意があれば、お客様のPCデータを盗んだり、重要なファイルを壊したりできてしまいます。最近では、ウィルスを自動で配布するものもあり、非常に危険度が高くなっています。さらに悪意がなくても間違っただけでアクセスされて、データを壊されてしまうこともあります。

このような不正アクセスのチェックをしなければなりません。

### ！ セキュリティホールとは？

#### OSやアプリケーションの不具合または弱点によるもの

ソフトウェアは完全なものではなく、どうしても不具合が残っています。特にOSなどの大きなソフトではなおさらです。もちろん不具合を減らすための様々な理論や技術が、多くの人によって、何十年前前から開発されています。しかし、まだ完全ではないのです。高度な知識を持つクラッカーで悪意のある者は、その不具合を探し出し、データを盗んだり、壊したりする場合があります。

不具合のソフトを早急にバージョンアップしなければなりません。

#### 設定ミス

PCをインターネットに設定する場合、ネットワークに関するすべてのソフトとその設定に注意する必要があります。高度なネットワークの知識を持ったシステム管理者がいても、OSやアプリケーションによって設定方法が異なり、非常に複雑で困難になってきています。この事が原因で設定ミスなどが起こり、そのミスがセキュリティホールとなってしまいます。

設定や変更を慎重に行わなければなりません。

#### ユーザ名から推測されやすいパスワード

実際にユーザが付けているパスワードのうち、約6～8割がユーザの名前から類推できるもの、3文字以下の文字列、名前、地名など辞書に載っている単語になっているといわれています。安易なパスワードは、クラッカーの攻撃などで破られる確立が非常に高くなります。万が一破られた場合、そのアカウントを使ってメールの読み書き、ファイルの作成/削除、さらにネットワークを通じて別のホストのアカウント検索などが行われる危険性があります。

安易なパスワードは使わず、ランダムなものをお勧めします。