基本のキ。セキュリティ入門（第3回）

セキュリティ対策ツールのアップデートの必要性

2020.03.12

セキュリティ対策をしていないことは「裸で戦場を歩いている状態」と言われるほど危険な状態です。セキュリティ対策を施しても、定期的なアップデートを行う必要があるのをみなさんはご存じでしょうか。

今回は、セキュリティ対策におけるアップデートの重要性と合わせて、リスク・脅威に備えるNTT西日本のセキュリティ対策「セキュリティおまかせプラン」を紹介します。

セキュリティ対策における「アップデート」の必要性

セキュリティ対策において、定期的にソフトウエアをアップデートすることは非常に重要です。その理由と合わせて、混合しやすい「バージョンアップ」「更新」といった言葉との違いについて見ていきましょう。

＜アップデートが必要な理由＞
アップデートは、セキュリティ対策ソフトウエアをはじめ、普段利用しているソフトウエアやOSでも行われています。アップデートが定期的に行われる理由は、最新の脅威に対応するためです。

具体的には、あらゆるソフトウエアにはセキュリティ的に弱い部分（脆弱性、セキュリティホール）が含まれており、その弱い部分を補う目的でアップデートが行われています。みなさんが今利用しているソフトウエアの作りが悪いということではなく、日々巧妙化するサイバー攻撃への対策として、アップデートは行われるのです。そのため、定期的なアップデートを行わないと脆弱性・セキュリティホールを放置することになり、情報漏えいや不正アクセス、データの改ざんといったリスクにさらされることになります。

2020年1月現在で一番注目するべきは、2020年1月14日でWindows7のサポートが終了することでしょう。サポートが終了す

るとWindows7は今後アップデートされなくなります。そのため、Windows7をお使いの方は、Windows10へのバージョンアップを行う必要があります。

＜アップデート・バージョンアップ・更新の違い＞
アップデートの必要性については紹介した通りですが、「バージョンアップ」や「更新」など、似たような言葉の違いについてご存じでしょうか。

セキュリティ対策におけるアップデート、バージョンアップ、更新の違いは次の通りです。

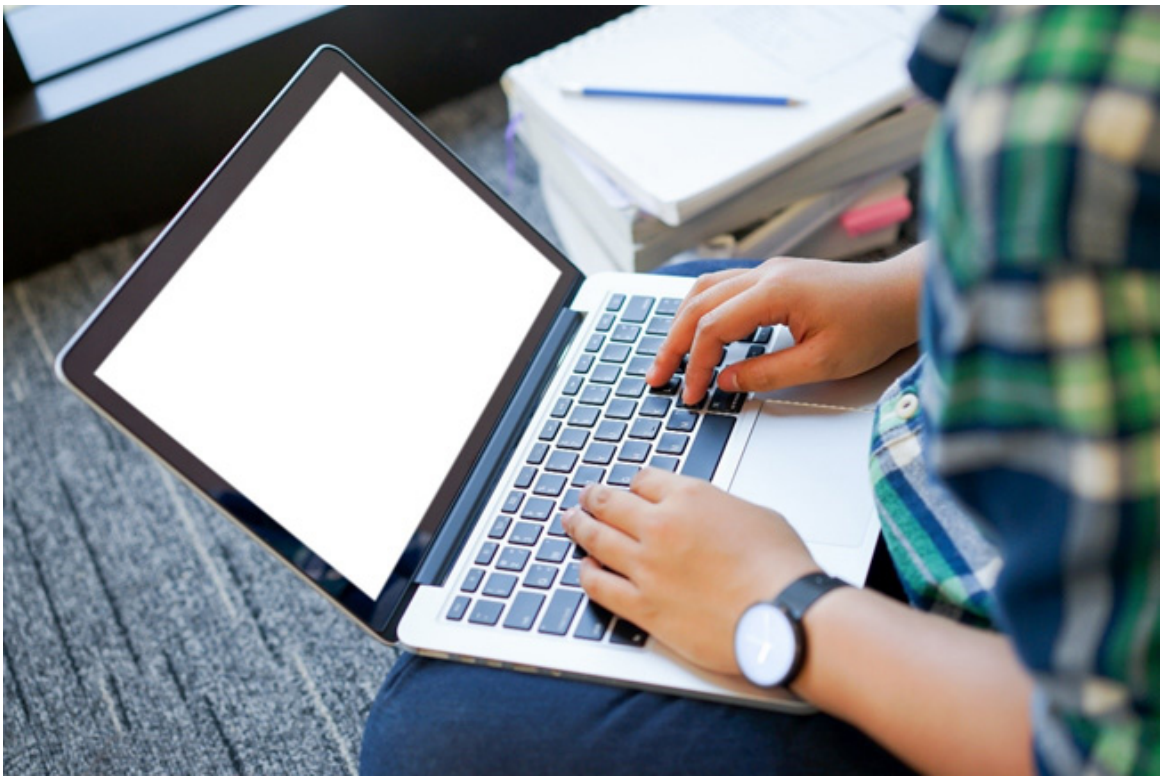
単語	意味
アップデート	新たな脅威に対応できるよう、最新の状態にすること
バージョンアップ	新たな機能が追加された状態にすること
更新	セキュリティ対策ソフトウエアの有効期限を延長すること

「アップデート」は、既存のソフトウエアに対して新たな脅威に対応できるように脆弱性・セキュリティホールを補い、最新の状態にすることを表します。

「バージョンアップ」は、新たな機能が追加され、利便性向上などの目的で行われます。先ほどのWindows7の例のように、サポートが終了する製品はバージョンアップする必要があることも覚えておきましょう。

最後に「更新」ですが、セキュリティ対策においてはセキュリティ対策ソフトウエアの有効期限の延長を表すことが多いものです。セキュリティ対策ソフトウエアには有効期限が定められており、期限内は定期的にアップデートが行われますが、有効期限以降はアップデートを受けられなくなるため、更新が必要となります。

アップデート以外でセキュリティ対策に必要なこと



これまでご紹介した通り、セキュリティ対策においてアップデートは非常に重要なものですが、より対策を強化するためには、そのほかにも対策を施す必要があります。

アップデート以外のセキュリティ対策として、代表的なものを簡単に紹介しますので、1つずつ見ていきましょう。

＜パスワード管理の徹底＞
パスワードはログインする際に利用するものです。Webサービスや社内システムなど、多くのパスワードを利用している方も多いのではないでしょうか。

パスワード管理の徹底はセキュリティ対策として有効です。パスワード管理では、特に次の2点に注意しましょう。

・単純なパスワードを使用しない
・パスワードは使い回さない

8桁未満、数字のみといった単純なパスワードは、簡単に解読できます。さらに、パスワードを使い回していると、仮に1つのシステムからあなたのパスワードが漏えいした場合、あらゆるシステムへの不正ログインが可能となってしまうのです。

パスワードは8桁以上、数字・英字・記号を含めた複雑なパスワードとし、システムごとにパスワードを変更して管理するのをお勧めします。

＜セキュリティ対策ソフトウエアの導入＞
OSのアップデートはもちろん重要ですが、セキュリティ対策ソフトウエアを導入することはさらに重要です。セキュリティ対策ソフトウエアはウイルス対策だけでなく、不正Webサイトへのアクセス制限や、ファイアウォール機能、迷惑メール対策など、多くのセキュリティ対策を施せます。

また、セキュリティ対策ソフトウエアを導入した後は、定期的なアップデートを行うことが大切です。

＜無線LANの暗号化＞
現代では、インターネットへの接続や社内LANへの接続に、無線LANを利用している人も多いのではないでしょうか。無線LANを利用する際に注意してほしいことが、無線LANの暗号化です。

無線LANは、有線接続でないため不正に利用されていても気付きにくいものです。また、セキュリティ的に弱い暗号化方式を利用している場合は、あなたの通信内容が盗まれることもあり得ます。

無線LANを利用する際には、WPA2（WPA2-PSK）かを確認してから利用するようにしましょう。

＜データのバックアップ＞
データのバックアップも、セキュリティ対策の一つとして考えます。不正なソフトウエア（マルウエア）の中に、「ランサムウエア」と呼ばれるものがあります。ランサムウエアは、あなたのデータを暗号化して読み取れなくし、人質として金銭を要求するマルウエアです。

ランサムウエアに感染すると、データを初期化するか、最悪の場合にはコンピューターの廃棄となります。あなたのデータも狙われる可能性があるため、定期的にデータのバックアップを取得して備えておくことが、セキュリティ対策となるのです。

アップデート通知が来たら早急に対応しよう

現代では、セキュリティ対策を施すことは一般常識と捉えられるほど重要です。普段利用する中で、アップデート通知を目にする機会も多いと思いますが、後回しにしてしまう人も少なくありません。しかし、アップデートを行うことでセキュリティ対策を施しています。アップデート通知が届いた際には早急な対応を意識しましょう。

アップデート以外にも、セキュリティ対策ソフトウエアを導入することは非常に重要であり、導入していない場合はセキュリティ対策としては不十分です。

多くのセキュリティ対策ソフトウエアが販売されていますが、NTT西日本では、進化し続ける脅威に対して、セキュリティ対策を複合的に組み合わせた「セキュリティおまかせプラン」をご用意しています。このプランでは、ゲートウェイでの防御や、企業向けセキュリティ対策ツール、サポートセンターでの通信監視・復旧支援など、手厚いサポートで脅威から企業を守ります。

※本機能はセキュリティに対するすべての脅威への対応を保証するものではありません
※掲載している情報は、記事執筆時点のものです