

インターネット通信機器は全てアップデートを…

# パソコンの アップデートだけで 終わっていませんか？

UPDATE

## 「アップデート」はパソコンだけでは足りない…



サイバー脅威に対して、お使いのパソコンのOSやウイルス対策ソフトのアップデート（更新）が必要なことは広く知られていますが、パソコン以外の周辺機器にもアップデートが必要な場合があることを知っていますか？

パソコン以外の周辺機器にも機器を制御するためのソフトが入っており、これらのソフトもアップデートしないとサイバー攻撃の被害に遭うことがあります。

パソコンのOSやウイルス対策ソフトだけでなく、パソコン以外の周辺機器のソフトウェアについてもアップデートを行うようにしましょう。

## 「ぜい弱性（ぜいじゃくせい）とは？」

攻撃者は、ソフトウェア等の「弱点」を突いて、情報システムに侵入したり、コンピュータにウイルスを感染させます。

このような「弱点」は、「ぜい弱性（ぜいじゃくせい）」と呼ばれています。

通信機器をインターネットに接続していると、そのぜい弱性を狙われ、機器が外部から不正利用されたり、コンピュータウイルスに感染したりして、トラブルが発生する可能性があります。



## ぜい弱性対策が必要な機器・ソフトウェアとは？

### 基本的対策

OSやソフトウェアを古のまま放置していると、セキュリティの問題が解決されず、それを悪用したウイルスに感染してしまう危険性があります。

OSやソフトウェアには修正・更新プログラムを適用し、最新版を利用するようにしましょう。

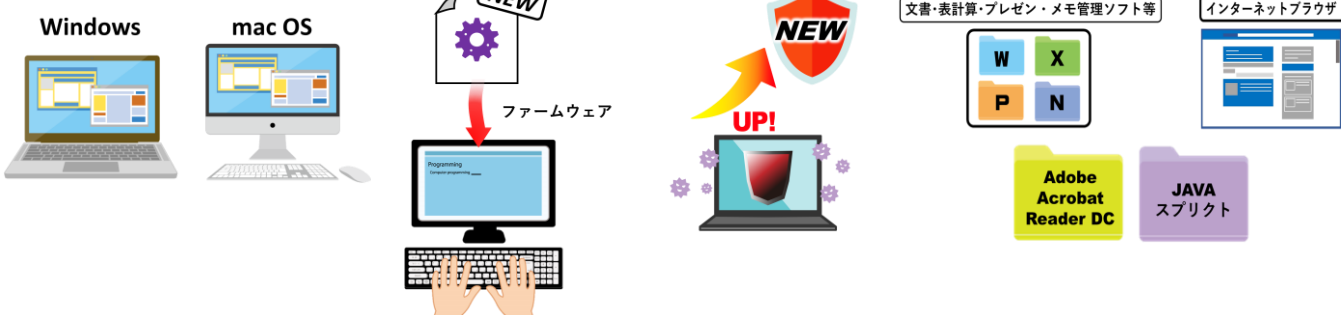
#### アップデートが必要な基本的なソフトウェア

##### OS（オペレーションシステム）

##### 本体のファームウェア

##### セキュリティソフト

##### インストールしたソフトウェアなど



OSやソフトウェア以外にも、インターネットに繋がっているルーター、VPN機器、監視カメラ、複合機などのIoT機器やファイヤーウォールの設定など、アップデートが必要な機器・ソフトウェアが存在します。

これらの機器やソフトウェアにも修正・更新プログラムを適用し、ぜい弱性を突かれた攻撃に遭わないように対策を行いましょう。

#### パソコン以外にもアップデートが必要な機器

##### 防犯カメラ

##### 複合機

##### ルーター

##### VPN機器

##### ファイヤーウォール



【その他】ネットワーク家電（ブルーレイレコーダー、テレビ、エアコン、ロボット掃除機等）、家庭用プリンタ、ネットワークカメラ、玩具、ゲーム機、スマートフォンやパソコンのアプリケーション等

※各機器・ソフトウェアのアップデート方法については各機器・ソフトウェアメーカーに問合せ下さい。

## ぜい弱性対策の必要性と基本的対策

新たなぜい弱性は日々発見されており、現在までに数万種類ものぜい弱性が公表されています。

攻撃者は、まず、このような既に判明しているぜい弱性の悪用を試みます。

したがって、既に判明しているぜい弱性を残してしまうことは避けなければなりません。

またぜい弱性は、ウイルス対策ソフトを使っても取り除くことができません。

何度コンピュータウイルスを駆除しても、ぜい弱性対策を行わなければ再び感染してしまう可能性があることに注意しましょう。

新たなぜい弱性が発見されれば、攻撃者はそれを狙った攻撃ツールやコンピュータウイルスを開発して攻撃を行います。

利用している機器、ソフトウェアに新たなぜい弱性が発見された場合には、速やかにぜい弱性を修正・更新しなければなりません。

ぜい弱性を突かれた攻撃を未然に防止するために

- 修正・更新が必要な機器を把握すること
- どんなソフトウェアを利用しているのかを把握すること  
(ソフトウェアの種類、バージョン、ぜい弱性の修正ソフトウェア（パッチ）の適用の有無等)
- ぜい弱性関連情報を収集すること
- 企業であればシステム管理部門担当者や専門業者等による定期的なぜい弱性検査を行うこと

を日頃から行なうようにしましょう。

ぜい弱性に関する情報を定期的に収集

情報収集

ぜい弱性対策

検査

利用機器ソフトウェアの把握

利用機器や利用しているソフトウェアの種類・バージョン等をあらかじめ把握

安全性が保たれているかぜい弱性検査を定期的実施

