基本のキ。セキュリティ入門（第2回）

Windows10のセキュリティ対策を徹底解説！

2020.03.11

Windows10では、セキュリティ対策ソフトウエアとして「Windows Defender」が標準インストールされています。無料で使えることもあり、市販のセキュリティ対策ソフトウエアを導入する必要はないと考えている方も多いのではないでしょうか。

結論からいえば、Windows Defenderはセキュリティ対策機能が豊富だとはいえないため、市販のセキュリティ対策ソフトウエアを導入するべきです。今回は、Windows Defenderの機能の紹介と合わせて、市販のセキュリティ対策ソフトウエアを導入すべき理由、その他のWindows10のセキュリティ対策について解説します。

Microsoftのセキュリティ対策ソフトウエア「Windows Defender」

MicrosoftのWindowsを利用している場合、標準でセキュリティ対策ソフトウエアであるWindows Defenderが導入されています。Windows Defenderの概要から機能、簡単な設定方法について見ていきましょう。

＜Windows Defenderとは＞

Windows Defenderは、Windowsの開発元であるMicrosoft社製のセキュリティ対策ソフトウエアです。Windows8やWindows10等のOSには標準インストールされています。

Windows8やWinodws10などのパソコンを利用している場合は、無料で利用できます。Windows利用者がセキュリティ対策ソフトウエアを導入していない場合もあり、標準インストールされるようになった背景があります。

＜Windows Defenderの機能＞

Windows Defenderの主な機能は以下です。

・アンチウイルス（アンチマルウエア）
・不正Webサイトへのアクセス制限
・ファイアウォール機能

など

ウイルスを含む不正なソフトウエア（マルウエア）を検出し、対応できるのをはじめ、不正Webサイトへのアクセス制限や不正アクセスを防ぐファイアウォール機能など、必要最低限のセキュリティ対策はWindows Defenderで可能です。

ただ、Windows Defenderでは、迷惑メール保護や、Webサイトの広告ブロックなどの対策はできません。

＜Windows Defenderの設定方法＞
ここではWindows Defenderを無効／有効とする手順について解説します。

【Windows Defenderを無効にする手順】
1.「Windowsキー + S」を入力し、「Windows セキュリティ」と入力
2.「Windows セキュリティ」を開く
3.「ウイルスと脅威の防止」をクリック
4.「ウイルスと脅威の防止の設定」から「設定の管理」をクリック
5.「リアルタイム保護」をオフに変更

Windows Defenderを有効にする場合は、「リアルタイム保護」をオンに変更します。注意点として、Windows Defenderを無効とした場合でも、再起動や一定時間が経過することで自動的に有効となるのを覚えておきましょう。

Windows Defenderを完全無効化するためには、レジストリを修正する必要がありますが、Windowsが利用できなくなる可能性がありますので、不用意に修正するべきではありません。Windows Defenderを利用しないのであれば、市販のセキュリティ対策ソフトウエアを導入しましょう。

Windows10に市販のセキュリティ対策ソフトウエアは必要

＜市販のセキュリティ対策ソフトウエアは必要＞
セキュリティ対策ソフトウエアの性能を示す指標として、「マルウエアの検知率」と「誤検知率」があります。マルウエアの検知率はマルウエアをきちんと検知できるかを表す指標であり、誤検知率はマルウエアでないソフトウエアを誤って検知してしまうことを表す指標です。

これらの検知率に関しては、一昔前まではWindows Defenderよりも市販のセキュリティ対策ソフトウエアのほうが明確に性能は良いとされていました。しかし、セキュリティ対策ソフトウエアの性能を評価する第三者機関「AV-Comparatives」のデータによれば、Windows Defenderも、市販のセキュリティ対策ソフトウエアと同等の性能を持つと報告されています。

しかし、Windows Defenderよりも市販のセキュリティ対策ソフトウエアのほうが、以下の点で優れているといえます。
・セキュリティ対策機能の豊富さ
・ユーザーインターフェースの使いやすさ
・サポート体制

セキュリティ対策ソフトウエアは、マルウエア対策だけではありません。セキュリティトラブルの手口は多種多様であり、さまざまなセキュリティトラブルへの対策が必要です。

Windows Defenderでは迷惑メール対策やWebサイト広告ブロックなどの機能がありませんが、市販のセキュリティ対策ソフトウエアは多くのセキュリティ対策機能が搭載されており、統合的なセキュリティ対策が可能なのです。さらに、市販のものはセキュリティ対策の設定を行いやすく、細かな設定もWindows Defenderよりも簡単に行えるものが多いです。

もしもセキュリティトラブルに巻き込まれたとしても、市販のセキュリティ対策ソフトウエアなら、あなたをサポートするための体制がしっかりしている点もメリットといえるでしょう。

Windows Defenderでもセキュリティ対策は行えますが、統合的なセキュリティ対策を施すためには市販のセキュリティ対策ソフトウエアを導入するべきです。

＜市販のセキュリティ対策ソフトウエアを導入する際の注意点＞
市販のセキュリティ対策ソフトウエアを導入する際は、Windows Defenderと併用できないケースがあることを覚えておきましょう。2つのセキュリティ対策ソフトウエアを動かせば、より強力なセキュリティ対策ができると思いがちですが、セキュリティ対策ソフトウエアは併用できないのが一般的です。

Windows Defenderだけに限った話ではありません。セキュリティ対策ソフトウエアは併用を想定していないため、予期しない動作をする可能性があります。セキュリティ対策ソフトウエアによっては、導入する際に自動的にWindows Defenderを無効化するものもありますが、もし市販のセキュリティソフトウエアを導入する際は、Windows Defenderを無効化すると覚えておいてください。

また、市販のセキュリティ対策ソフトウエアは有効期限が設けられ、有効期限を過ぎると利用できません。導入する市販のセキュリティ対策ソフトウエアによって、有効期限後の動作は異なりますが、Windows Defenderが無効化されたままとなる可能性もあります。その場合には、Windows Defenderを有効化するのを忘れないようにしましょう。

その他のWindows10に必要なセキュリティ設定

Windows10を利用する際には、Windows Defenderを含むセキュリティ対策ソフトウエアを導入すること以外にも必須な設定があります。
・アカウント設定
・2段階認証の設定
・プライバシー設定

Windows10のユーザーアカウントは、「Microsoftアカウント」と「ローカルアカウント」があります。パスワード忘れや不正アクセス防止のために、Microsoftアカウントには2段階認証が設定可能ですので、特別な理由がない限りはMicrosoftアカウントを利用しましょう。

2段階認証は、IDとパスワードによる認証と合わせて、異なる形式の認証を組み合わせる方式であり、セキュリティ対策として非常に有効です。2段階認証の認証手段としては「アプリ」「電話番号」「メールアドレス」から選択できます。

最後にプライバシー設定ですが、位置情報やカメラ・マイク、連絡先といった情報を扱えるソフトウエアを限定できる設定です。カメラやマイクが付いているパソコンの場合、知らないうちにマルウエアによって盗撮・盗聴される可能性があります。必

要なソフトウエアにのみ必要な情報を扱えるように設定しましょう。

Windows Defenderだけに頼らず、対策ツールも導入しよう

MicrosoftのWindows10では、Microsoft社製のセキュリティ対策ソフトウエアであるWindows Defenderが標準インストールされています。ウイルス対策や不正Webサイトのアクセス制限など、必要最低限のセキュリティ対策は行えますが、統合的なセキュリティ対策のためには、市販のセキュリティ対策ソフトウエアを導入するべきです。

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