サイバーセキュリティ通信 Vol.15

令和5年２月

サイバァちゃん

サイバーセキュリティ月間

政府は、毎年２月１日から３月18日までを「サイバーセキュリティ月間」と定め、 サイバーセキュリティに関する取組を推進しています。
インターネットが日常となった今、サイバー攻撃への対策は限られた人だけでなく全員で向き合っていくことが必要です。

基本的なセキュリティ対策

①　OS、各種ソフトウェアを最新バージョンへ更新しましょう。

更新プログラムを実行しないままでいた場合、セキュリティホール（セキュリティ上の欠陥）がそのままの状態となるため、サイバー攻撃の被害に遭う危険が高くなります。
常に最新バージョンであることを心がけ、随時、更新を行いましょう。（自動更新に設定することも有効です。）

②　セキュリティソフト導入し、最新の状態に保ちましょう。

セキュリティソフトを導入することで、ウイルス感染などの危険を遠ざけることができます。
ただし、セキュリティ対策ソフトの多くは既知の情報に対応するものであるため、随時更新し、参照する定義ファイルを常に最新の状態に保つ必要があります。

③　パスワードの設定と管理を見直しましょう。

パスワードは最低でも10文字以上とし、大小英字、数字及び記号を組み合わせたものにしましょう。
同じパスワードを使い回すと、パスワードが流出した際に複数のサービスで不正アクセスの被害に遭う危険があるため、パスワードの使い回しはやめましょう。

④　機器の設定状況について、もう一度確認しましょう。

　機器の設定が購入時のままであったり、間違った設定にしていると、不正アクセスの被害に遭ったり、無関係な人に重要な情報を見られてしまう可能性があります。
　機器の設定について見直しを行いましょう。

⑤　バックアップをとりましょう。

　機器の故障やウイルス感染などの被害に遭った際、バックアップがないと、元の状態に戻すことができず、取り返しのつかないことになりかねません。
　常に3つのデータコピーを作成し、それらを2つの異なる媒体に保存し、そのうち1つを異なる場所（インターネットに繋がらない環境）で保管しておく、3－2－1ルールを実践しましょう。

⑥　脅威や攻撃の手口について情報を集めましょう。

　インターネットを用いた犯罪は常に改変が行われており、従来からある方法でも、より巧妙な手口に変化しています。
　脅威や攻撃の手口について最新の情報を入手し、犯罪の被害に遭わないように備えましょう。

　サイバー攻撃を受けた場合、被害者となる可能性があるのは自分だけではありません。
　自組織で感染した端末を足掛かりに、関係する多くの企業などにまで、サイバー攻撃の魔の手が伸びる危険があります。

自らが攻撃者の足掛かりにならないよう、自分のサイバーセキュリティ対策について、見直しを行いましょう。

長崎県警察本部サイバー犯罪対策課
095-820-0110（3451・3452）

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！
友だち登録お願いします！

@387ojopi