サイバーだより

令和２年９月１日

長野県警察本部
サイバー犯罪捜査課

ソフトウェアの脆弱性対策
～アップデート（更新プログラム適用）の重要性～

先日、テレワーク等で企業が採用しているVPN（仮想専用ネットワーク）の暗証番号が多数流出した旨の報道が大きく取り上げられました。
安全にデータをやり取りする仕組みが、サイバー攻撃の標的になりました。
この被害は、攻撃者がVPNの脆弱性を狙ったもので、VPNの更新プログラムを適用していれば、防げたものです。

脆弱性（ぜいじゃくせい）とは

- ○ コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因で発生したセキュリティ上の欠陥（セキュリティホールとも呼ばれる）
- ○ 脆弱性の完全対策は困難で、新たな脆弱性が次々と発見される
- ○ 脆弱性をふさぐには、ソフトウェアの開発メーカが提供する更新プログラムを適用する必要がある

※ パソコンの場合、メーカは、更新プログラムを自動的に通知・適用する機能（Windows Update等）を提供していますが、サーバコンピュータの場合、管理者自身が更新プログラムを適用する必要があります。

脆弱性は公開されるので、サイバー攻撃者にとって、格好の標的です。
攻撃者は、脆弱性が公開されたソフトウェアが稼働しているコンピュータを探し出し、脆弱性を突いた攻撃を仕掛けます。　脆弱性が放置されていれば、攻撃が成功し、不正アクセス、ホームページの改ざん、情報漏洩等の様々な被害が発生します。

○ 一般利用者の方へ
脆弱性を残しておくと、サイバー攻撃者に利用される危険性があります。
Windows Updateや更新通知を適用し、ソフトウェアを最新の状態に保ちましょう。

○ 企業・組織の担当者の方へ
脆弱性は、特にインターネットに接続しているサーバコンピュータで大きな被害になる危険性があります。県内でも、脆弱性の放置が原因でホームページが改ざんされた事案が、たびたび発生しています。
IPA（独立行政法人情報処理機構 http://www.ipa.go.jp）では、脆弱性とその対策について「重要なセキュリティ情報」としてホームページで公開しています。
サーバコンピュータ等で使用しているソフトウェアの脆弱性が公開された場合は、適切な対応をお願いします。
サーバの管理を委託している場合は、脆弱性について対応しているか委託業者に確認しましょう。