先生！狙われてますよ！

サイバー空間の脅威のターゲットは今や企業や官公庁だけではありません。
最近では学校を始めとする教育機関を狙った攻撃が増加しています。

道内の学校がランサムウェア被害!!

ランサムウェアは、金銭を脅し取ることを目的としたマルウェアです。ランサムウェアに感染するとコンピュータ内のファイルが暗号化され、使用が不可能になる上、暗号化の解除などの名目で「身代金」を要求されます。

発生要因/手口

①ソフトウェア（VPN等）の脆弱性によりネットワークに不正侵入される
②外部公開しているサーバに不正アクセスされる
③メールの添付ファイルや本文中のURLリンクを開かせる

【ランサムウェアにより想定される被害の例】

・校務ネットワークが稼働するサーバや共有ファイルサーバを利用した業務の継続が困難となる。
・共有ファイルサーバに保存された過去の授業教材等が全て使用できなくなる。
・児童生徒や保護者、教職員の個人情報等の流出の可能性がある。

感染リスクを減らすため

①VPN等の周辺機器やソフトウェアは適宜、修正プログラムを適用して脆弱性を残さない。
②パソコンや周辺機器のOS、ウイルス対策ソフトなどは常に最新の状態にアップデートしておく。
③公開サーバのログイン試行回数の制限やパスワードの複雑化など不正アクセス対策を行う。
④不用意にメールの添付ファイルや本文中のURLリンクを開かない。

万が一感染した場合に備えて

①重要なデータは必ずバックアップを取る。
②バックアップを取った媒体は、必ずネットワークから切り離して保管する。
③有事に備えて専門担当部門（CSIRT）を設置し、対応手順の策定や教育等を行う。

北海道警察サイバーセキュリティ対策本部