サイバーセキュリティ岐阜

令和５年 第３０号

岐阜県警察本部
サイバー犯罪対策課
058-271-2424

ランサムウェアによるサイバー攻撃に注意!

～学校・教育委員会における情報セキュリティの確保を～

昨今、ランサムウェア等によるサイバー攻撃が活発化しており、学校で利用している**校務支援システム**や**共有ファイル サーバ**がランサムウェアに感染すると、校務支援システムや共有ファイルサーバが利用できなくなるだけでなく、**個人情報の流出**も懸念されています。

ランサムウェアにより想定される被害例

- 校務支援システム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
- 校務支援システムに保存されていた過去のデータ（出欠、成績管理、イントラメールの履歴等）を利用できなくなる
- 共有ファイルサーバに保存されていた各種学校行事の記録写真等が喪失し、記念冊子（卒業アルバム等）の作成が困難となる
- 共有ファイルサーバに保存されていた過去の授業教材等が全て使用できなくなり、授業に支障が生じる
- 児童生徒や保護者、教職員の個人情報等の流出も懸念される

ランサムウェア被害に遭ったら、警察に通報を!

ランサムウェア被害を発生させない 環境づくりが大切！

～運用事業者等と連携対応し、以下のポイントのチェックを～

1.脆弱性対策

利用している機器やOS等の更新ファイルやパッチ等を適用し、脆弱性を残さない!

その際、インターネットとの接続点となるVPN（Virtual Private Network）機器の脆弱性対策を!

ウイルス対策ソフトウェアの定義ファイルを最新状態にすることも忘れずに!

2.バックアップ

ネットワークから切り離して、定期的にバックアップデータを保管!

学校運営に関するシステムがランサムウェアの被害にあった場合においても、速やかなデー タ復旧と業務の継続に繋がる!

3.多要素認証

重要な情報資産（校務情報等）へのアクセスには、必ず多要素認証の導入を!

4.適正管理

ログインに必要なパスワードの適切な設定と管理を!

特にリモートから端末を操作できるネットワーク機器（VPN機器等）の脆弱性対策を!

初期ID・パスワードをそのまま利用しないで!

5 .権限最小化

データが暗号化されるなどの被害の拡大を防止するために、アカウントに割り当てる権限やアクセス可能範囲を最小限に設定を!

定期的なIDの棚卸（削除や変更）を行いましょう!

6.ネットワークの監視

不正アクセスを迅速に検知するため、 サーバやネットワーク機器等のログ監視を強化!

EDR （Endpoint Detection and Response）等を導入し、「ランサムウェアの感染拡大防止」

7.連絡体制の整備

冷静に対応できるよう、連絡体制の整備などの対処態勢の構築とシステムの復旧手順の確認!

復旧にあたっては、被害に遭った可能性のあるサーバ・機器等のパスワードを確実に変更を!

8.脆弱性の修正

脆弱性を補完するための更新プログラム「パッチ」の公開を確認し、被害のリスクを低減しましょう!

その際、教職員や児童生徒使用の端末のOSに応じ て対応を!

ランサムウェア被害に遭ってもあわてない!