近時のランサムウェア等による被害の増加を踏まえ、学校・教育委員会における情報セキュリティの確保に向けた対策の検討をお願いします。

事　務　連　絡
令和４年１２月２７日

各都道府県教育委員会
各指定都市教育委員会
附属学校を置く各国公立大学法人
各都道府県私立学校主管部課
構造改革特別区域法第１２条第１項の認定を受けた
各地方公共団体の学校設置会社担当課
学校における情報セキュリティ担当　御中

文部科学省初等中等教育局
学校デジタル化プロジェクトチーム
警察庁サイバー警察局
サイバー企画課

ランサムウェア等によるサイバー攻撃について（注意喚起）

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、警察庁が把握した企業・団体等におけるランサムウェアの被害は、令和２年下半期以降右肩上がりで増加しています（参考資料１参照）。

ランサムウェアは、不正アクセス等によりシステムに侵入し、サーバや端末等に保存されているデータを暗号化して使用できない状態にし、当該データを復号する対価として金銭を要求する不正プログラムです。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ます。

【ランサムウェアにより想定される被害の例】
- 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

直近では、教育委員会が管理する小・中学校の校務用サーバ等がランサムウェアに感染し、児童生徒の成績情報等を含む学校業務全般に関するデータが暗号化された事案も生じているところです（参考資料２参照）。

文部科学省では、令和４年３月に改訂を行った「教育情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」といいます。）において、ランサムウェア等によるサイバー攻撃を防止するための対応策をお示ししています。各学校設置者においては、当該ガイドラインを参考としつつ、改めて下記について御検討いただくようお願いします。

各都道府県教育委員会におかれては、本事務連絡の内容を域内の市（区）町村教育委員会（学校組合を含む。）に周知いただくようお願いします。

各都道府県私立学校主管部課及び構造改革特別区域法第１２条第１項の認定を受けた地方公共団体の学校設置会社担当課におかれては、所轄の学校法人等に対し、周知いただくようお願いします。

記

１．ランサムウェアによる被害の予防等の観点から、運用事業者等と連携しつつ、以下に示す対策例の実施を検討すること

（１）予防の観点からの対策の例

① 学校や教育委員会で利用している端末やサーバ、ソフトウェア、ネットワークを構成する機器等の脆弱性に関する情報に留意し、必要な対策（※１）を講じること。その際、インターネットとの接続点となるＶＰＮ（Virtual Private Network）機器の脆弱性を突いた攻撃事例が多いため、ＶＰＮ機器を利用している自治体においては、導入しているＶＰＮ機器に関する脆弱性の情報を意識的に収集し、必要な対応を検討すること（※２）（参考資料３参照）

（※１）考えられる対策の例：
- 端末やサーバ：ＯＳのセキュリティアップデートを随時実施することや、ウイルス対策ソフトウェアの定義ファイルを最新の状態に保つこと
- ソフトウェア：セキュリティパッチを随時適用すること
- ネットワークの構成機器：ファームウェアの更新を随時適用すること

（※２）ＶＰＮ機能を備えたＵＴＭ（Unified Threat Management）機器の中には、近時脆弱性が発表されたものもあることから、ＵＴＭ機器等についてもＶＰＮ機器と同様に必要な対応を検討すること。

② 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も速やかにデータを復旧し、業務を継続することができるよう、定期的にデータのバックアップを取ること。その際、バックアップデータは被害を受けない領域に隔離して保存（※）すること

（※）バックアップ用のＨＤＤを用意してサーバ等から定期的にバックアップを取るとともに、バックアップ後は必ず当該ＨＤＤをサーバ等から物理的に切断する（通信ケーブルを抜く）といった方策や、ＬＴＯオートローダー等のテープメディアを使った自動バックアップ等が考えられる

③ 重要な情報資産（校務情報等）へのアクセスには、多要素認証を必須とすること

④　ＶＰＮ機器等のネットワークを構成する機器の管理等に利用するＩＤ・パスワードについては、一般に出荷時に設定されている初期ＩＤ・パスワードをそのまま利用することは不正アクセス被害のリスクが高いため、これらの機器について初期ＩＤ・パスワードのまま利用していないかを確認するとともに、初期ＩＤ・パスワードを利用している場合は、速やかに推測されにくいＩＤ・パスワードへと変更すること

⑤　アクセス権限に関する管理を徹底（※）するとともに、アクセス権限が職務内容に応じた最小限のものとなるようにすること　等

（※）ＩＤの棚卸を行い、異動・退職等に伴い使用しなくなったＩＤを削除したり、異動等に伴うアクセス権限の変更等を確実に反映する等

（２）検知・拡大防止の観点からの対策の例

①　ランサムウェアへの感染の端緒となり得る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するとともに、必要に応じてふるまい検知等の活用を検討すること

②　システムに侵入したランサムウェアの感染拡大を防止するため、必要に応じてＥＤＲ（Endpoint Detection and Response）等の活用を検討すること　等

（３）対応・復旧の観点からの対策

①　被害を受けた場合でも、冷静に対応できるよう、連絡体制の整備など対処態勢を構築すること

②　バックアップデータから迅速・確実に復旧ができるよう、復旧可否の再確認や、復旧手順の整理等、実際に復旧を行う場面を見据えた準備をしておくこと

③　復旧にあたっては、被害の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すること　等

２．学校に対するサイバー攻撃による被害を防止するため、教職員や児童生徒が学校において利用する端末の更新プログラムの適用を徹底すること。その際、端末のＯＳに応じて対応方法が異なることから、以下を参考とすること

①　iPad OSの場合

「iPadの管理と運用 OSアップデート（2022年11月）」

https://education-static.apple.com/geo/jp/IT/GIGA/OS_Update.pdf

※手動更新手順はP5。MDMによる更新管理はP6参照。

②　Google Chrome OSの場合

「Google for Educationの構築運用ガイドブック（GIGA スクール構想対応）第2.0版（2021年６月）」

https://services.google.com/fh/files/misc/gfe_guide_giga.pdf

※自動更新設定にしていれば操作不要。手動更新設定にしている場合はP54-55参照。

③　Microsoft Windowsの場合

「GIGA スクール端末の運用管理ガイド　Windows 10 OS のアップデート 第1.0版（2022年11月）」

https://www.microsoft.com/cms/api/am/binary/RE5cvW2

※MDMによる更新管理はP6-21。手動更新はP22-24参照。

【上記の検討にあたっての補足事項】

①　文部科学省の「ＩＣＴ活用教育アドバイザー事業」を活用いただくことで、専門的な知見を持つアドバイザーから無償で学校の情報セキュリティに関する助言や支援を求めることができます（参考資料４参照）。

②　令和４年度第２次補正予算に計上された「ＧＩＧＡスクール運営支援センター事業」は、学校に関する情報セキュリティの状況を診断し、必要な対策を検討すること（セキュリティアセスメント）も補助対象とする予定です（参考資料５参照）。

③　上記のほか、「年末年始休暇において実施いただきたい対策について（注意喚起）」（令和４年１２月経済産業省・総務省・警察庁・内閣官房内閣サイバーセキュリティセンター）においてもランサムウェア対策に関する情報がまとめてありますので、必要に応じて御参照ください。

https://www.nisc.go.jp/news/notice/20221220.html

３．ランサムウェア被害が発生した際は、速やかに都道府県警察本部又は管轄警察署（以下「警察機関」といいます。）へ通報・相談すること。また、平素から通報先をあらかじめ確認しておくほか、警察機関（サイバー部門）の職員を研修講師として招くなど連携強化に努めること

なお、研修講師の派遣に当たっては、都道府県警察のサイバーセキュリティ担当課に問い合わせること

【参考資料】

○参考資料１：

「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和４年９月１５日付け広報資料・警察庁）

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

○参考資料２：

「市内小中学校の校務ネットワークに対する不正アクセスについて」

https://www.city.minamiboso.chiba.jp/0000017149.html

「市内小中学校の校務ネットワークに対する不正アクセスについて（第２報）」

https://www.city.minamiboso.chiba.jp/0000017428.html

○参考資料３：

「IPA（独立行政法人 情報処理推進機構）」

https://www.ipa.go.jp/index.html

※ウェブページ中の「重要なセキュリティ情報」等を御覧ください。

「JPCERT/CC（一般社団法人JPCERT コーディネーションセンター）」

https://www.jpcert.or.jp/

※ウェブページ中の「注意喚起」「脆弱性関連情報」「Weekly Report」等を御覧ください。

○参考資料４：

「ICT活用教育アドバイザーについて」

https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1369635.html

「ICT活用教育アドバイザー事業ポータルサイト」

https://ictadvisor.mext.go.jp/

○参考資料５：

「ＧＩＧＡスクール運営支援センター事業について」

https://www.mext.go.jp/content/20221206-mxt_kouhou02-000017672_1.pdf

【本件担当】
初等中等教育局学校デジタル化プロジェクトチーム
情報基盤整備係　　伊藤、川﨑、小形、佐藤
電　話　０３－５２５３－４１１１（内線３２６３）
E-mail　digipt-kiban@mext.go.jp