教育現場におけるセキュリティ対策 Ⅱ
（物理的セキュリティ）

合同会社KUコンサルティング　高橋 邦夫

National Institute for
School Teachers
and Staff Development

独立行政法人教職員支援機構

目次

1　物理的セキュリティ

基本的な考え方

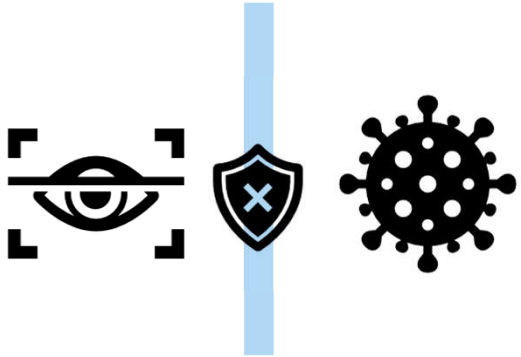
物理的セキュリティ対策とは、サーバ、通信回線等の機器の設置や設定、保守管理に関する措置や機器等の管理区域の適切な管理等の物理的な方法を通じて情報資産を守る対策を指します。

自然災害・停電等の緊急時の業務の継続性の確保に有効であるとともに、情報資産の盗難や不正取得による情報資産の漏えいを防ぐことにもつながります。

また、取り扱う情報資産の重要性に応じて機器等を適切に廃棄することにより、情報資産の漏えいを防ぐことも重要です。

物理的セキュリティの具体例

多要素認証



不適切なウェブページの閲覧防止

マルウェア感染対策

2　物理的セキュリティ（サーバ等の管理）

【ポイント】

教育情報システム管理者は、サーバ等の機器を安全な環境に設置し、特に重要性分類Ⅱ以上の情報資産を取り扱うサーバは冗長化、予備電源を備える等の措置を行います。また、機器の定期保守、修理の実施も重要です。さらに、機器の廃棄の際にはその機器に保存されている情報資産の重要性分類に応じて処分方法を検討する必要があります。

教育情報セキュリティポリシーに関するガイドライン（抄）

【例文】

＜前略＞

（７）機器の廃棄等

教育情報システム管理者は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

【解説】

＜前略＞

（７）機器の廃棄等

機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS及び記憶装置の初期化（フォーマット等）による方法は、ハードディスク等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている方法により、記録されている情報資産の重要性分類に応じて、機器の廃棄等を行わなければならない。

（参考）重要性分類に応じた機器の廃棄等の方法

分類	機器の廃棄等の方法	確実な履行を担保する方法
（１）重要性分類Ⅰ・Ⅱ	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	校内等において（２）で後述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（２）重要性分類Ⅲ	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。具体的には、（１）で先述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。OS及び記憶装置の初期化（フォーマ ット等）による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない。	校内等において消去を実施し、教職員等が作業完了を確認する方法など適切な方法により確認を行う。

3　物理的セキュリティ（教職員等の利用する端末等の管理）

【ポイント】

教育情報システム管理者は、教職員等の利用する端末や電磁的記録媒体等に対して、適切な認証設定、データ暗号化、マルウェア感染対策等の管理を実施します。

教育情報セキュリティポリシーに関するガイドライン（抄）

【例文】

＜前略＞

（４）教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。特に、パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

【解説】

＜前略＞

（４）多要素認証の利用

取り扱う情報の重要度等に応じて前述したID及びパスワード等の知識認証、生体認証（指紋、静脈、顔、声紋等）、物理認証（ICカード、USBトークン、トークン型ワンタイムパスワード等）のうち、異なる認証方式２要素以上を組み合わせた多要素認証を利用することによって、よりセキュリティ機能は強化されることになる。＜略＞

（参考）多要素認証

知識認証（ID及びパスワード等）、生体認証（指紋、静脈、顔、声紋等）、物理認証（ICカ ード、USBトークン、トークン型ワンタイムパスワード等）のうち、異なる認証方式２種類を組み合わせる利用者認証の方法

認証要素	認証手段	概要	例
要素A	知識	本人だけが知っている情報	パスワード
要素B	生体	本人だけに備わっている情報	静脈、顔、指紋、網膜、虹彩
要素C	物理	本人だけが持っている情報	ICカード、USBキー、トークン

上記の要素の異なる２種以上の認証を組み合わせつつも

学校現場の実態や特徴を踏まえ、端末の電子証明書等を用いた端末認証と、知識認証・生体認証のいずれかを組み合わせて利用者認証を行うことも考えられる。

4　物理的セキュリティ（学習者用端末のセキュリティ対策）

【ポイント】

１人１台端末は、学校内（教室）での活用だけではなく、学校外における調べ学習や家庭に持ち帰っての学習など様々な学習活動で使用されます。児童生徒に対する学習者用端末の管理方法等についての指導を前提として、利用するネットワークや場所にとらわれないセキュリティ対策を講じることが必要です。

教育情報セキュリティポリシーに関するガイドライン（抄）

【例文】

（１）不適切なウェブページの閲覧防止

児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

＜対策例＞ ①Webフィルタリング ②検索エンジンのセーフサーチ ③セーフブラウジング

＜中略＞

（３）端末を不正利用させないための防止策

端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

（４）セキュリティ設定の一元管理

児童生徒への端末配布後においても、端末のセキュリティ設定やOSアップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましい。

（５）端末の盗難・紛失時の情報漏洩対策

児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

【解説】

（１）不適切なウェブページの閲覧防止

＜中略＞

なお、目的は児童生徒による不適切なウェブページの閲覧防止であるため、実現したい機能や実際の運用に応じて適切に整備することが重要である。

これらの対策としては例えば次のものがある。

① Webフィルタリング

端末に標準的に搭載された製品、インターネットサービスプロバイダーが提供する製品、セキュリティ事業者が提供する製品・サービスなどがある。＜中略＞ 実現したい機能やフィルタリングの精度、実際の運用等を考慮して適切に整備すること。＜略＞

② 検索エンジンのセーフサーチ

検索エンジンの検索結果に不適切な情報が含まれる場合に表示させないようにする機能であり、有害情報を閲覧する機会の低減に繋がる。

③ セーフブラウジング

ウェブページ閲覧時に不正なサイトであることが疑われる場合、利用者に対して警告を表示する機能である。

＜略＞

学校現場においては児童生徒の情報活用能力の向上を図りつつ、過剰な規制に陥ることなく、フィルタリング等の設定を適切に行い、安全・安心で豊かな学習機会を全ての児童生徒に保障することが重要です。

【解説】
＜前略＞
（3）端末を不正利用させないための防止策
　学習者用端末の利用においては、端末の端末認証やユーザ認証の徹底が求められる。また、学習者用端末の利用においては、端末のセキュリティ状態の監視に加えて、学習に不適切なアプリケーションやコンテンツの利用を制限し、教員の目の届かない環境下でも常に安全で児童生徒が安心して利用できる状態を維持しなければならない。そのため、児童生徒の利用アカウントに対してアプリケーションのインストール・アンイ ンストールを自由に行う権限を与えないことや、MDM（モバイル端末管理：Mobile Device Management）等によりセキュリティ制御を行うこと。

（4）セキュリティ設定の一元管理
　児童生徒への端末配布後においても、端末のセキュリティ設定やOSやウェブブラウザを含むソフトウェアのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましいため、MDM等によりセキュリティ制御を行うこと。ただし、実現したい機能・規模・コストを鑑みて柔軟に検討すること。

- **学習に不適切なアプリケーションやコンテンツの利用を制限し、教員の目の届かない環境下でも常に安全で児童生徒が安心して利用できる状態を維持するためにMDM 等によりセキュリティ制御を行うことが必要です。**
- **児童生徒の利用アカウントに対してアプリケーションのインストール・アンインストールを自由に行う権限を与えないことや、端末のセキュ リティ設定や OS アップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状確認などの作業を、離れた場所からでも一元管理できるようにすることが望ましいです。**

【解説】

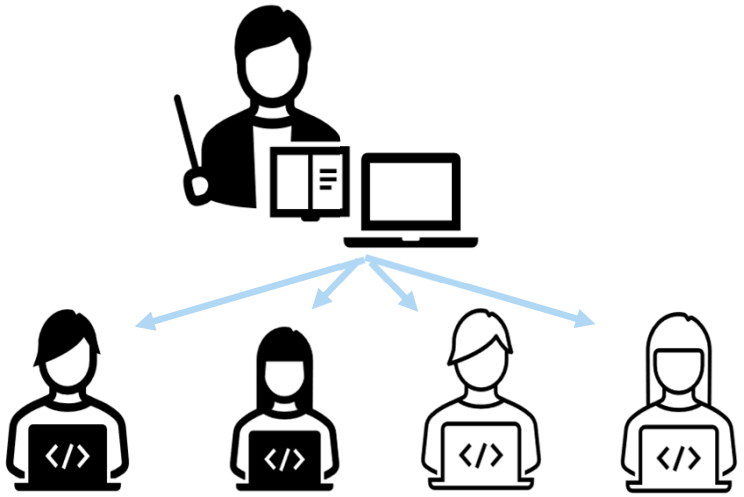
＜前略＞

（５）端末の盗難・紛失時の情報漏洩対策

端末の盗難・紛失などのインシデントが発生した場合においても重要性が高い情報が漏えいすることが無いように対策を講じる必要がある。具体的にはデータの保存はクラウドサービスを利用することにより端末内部に情報を保存しないようにする運用や、MDMなどにより管理者が離れた場所からでも端末をロックする、あるいは必要に応じてデータの削除や端末の初期化を行うリモートワイプ機能などの対策を講じること。また、これらの機能を事前に周知すること自体が盗難、転売対策にもなる。

- **端末の盗難・紛失などのインシデントが発生した場合においても重要性が高い情報が漏えいすることがないよう、データの保存はクラウドサービスを利用することにより原則端末内部に情報を保存しないようにする運用や、**
- **MDM等により管理者が離れた場所からでも端末をロックする、あるいは必要に応じてデータの消去や端末の初期化を行うリモートワイプ機能などの対策を講じることが必要です。**

（参考イメージ図）MDM等による管理



5　まとめ

最初のスライドの復習になりますが．．．．

物理的セキュリティ対策とは、サーバ、通信回線等の機器の設置や設定、保守管理に関する措置や機器等の管理区域の適切な管理等の物理的な方法を通じて情報資産を守る対策を指します。

自然災害・停電等の緊急時の業務の継続性の確保に有効であるとともに、情報資産の盗難や不正取得による情報資産の漏えいを防ぐことにもつながります。

また、取り扱う情報資産の重要性に応じて機器等を適切に廃棄することにより、情報資産の漏えいを防ぐことも重要です。

そのうえで

GIGAスクール構想により１人１台端末を用いた学習におけるクラウド活用が進みました。さらに、次世代校務DXの考え方に基づき、校務でのクラウド活用が進みつつあります。パブリッククラウド上で教育関係システムを運用することにより、大規模災害発生時等の非常時にデータの損失やデータにアクセスできない事態の発生を防ぎ、場所や時間を選ばない迅速な情報共有や意思決定、業務実施が可能になると考えられます。