教育現場におけるセキュリティ対策Ⅳ
（技術的セキュリティ）

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

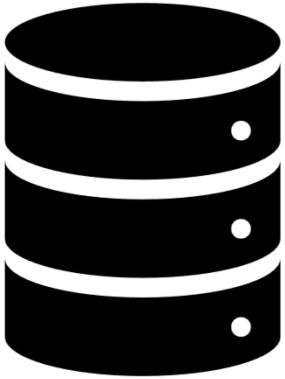
1　技術的セキュリティ
2　コンピュータ及びネットワークの設定管理
3　アクセス制御
4　セキュリティ情報の収集
5　まとめ

1　技術的セキュリティ

基本的な考え方

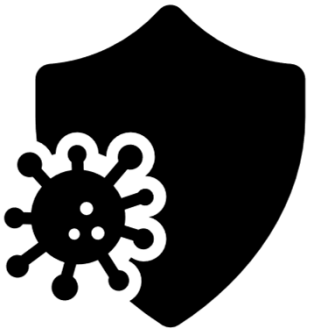
技術的セキュリティ対策とは、ハードウェア・ソフトウェアやネットワークなどに対するアクセス制御、不正プログラム対策、不正アクセス対策等の技術的な安全管理措置を通じて情報資産を守る対策を指します。GIGAスクール構想による１人１台端末を用いた学習におけるクラウド活用に加えて、**次世代校務DXの考え方の下で、校務でのクラウド活用も進んでいます**。クラウド上で重要性の高い情報を扱う場面も増える中、**教育委員会はこの変化に合わせた技術的セキュリティ対策の実施に対応することが求められます**。

技術的セキュリティの具体例



ログの取得等

強固なアクセス制御による対策



不正プログラム対策

2　技術的セキュリティ（コンピュータ及びネットワークの設定管理）

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）重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクへの対応

① 教育情報システム管理者は、強固なアクセス制御による対策を講じたシステム構成の場合は、各システムにおけるアクセス権管理の徹底をしなければならない。 ネットワーク分離による対策を講じたシステム構成の場合は、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系）を論理的又は物理的に分離をしなければならない。

② 教育情報システム管理者は、校務系システムとその他のシステム（校務外部接続系システム、学習系システム）との間で通信する場合には、各システムにおけるアクセス権管理の徹底を行う等の適切な措置を図らなければならない。また、ネットワーク分離による対策を講じたシステム構成ではウイルス感染のない無害化通信など、適切な措置を図らなければならない。

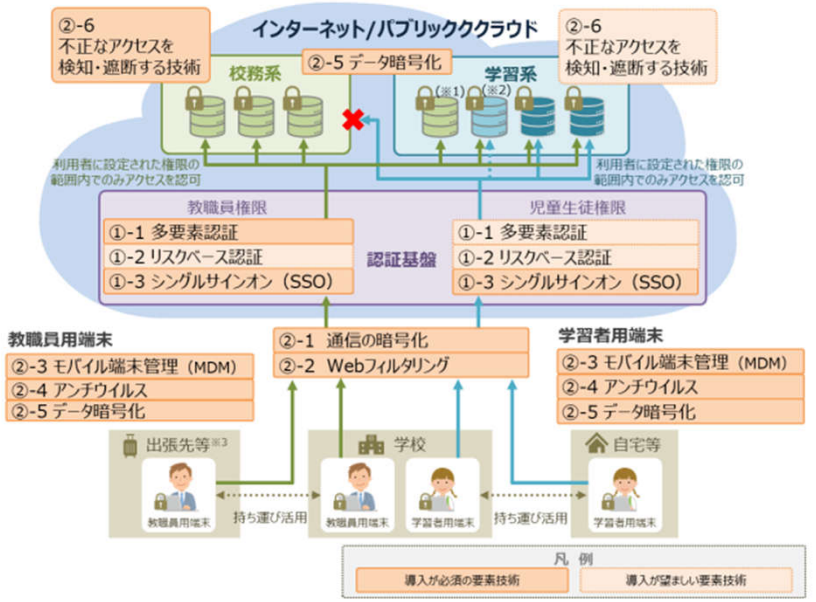
強固なアクセス制御による対策

強固なアクセス制御による対策とは、**インターネットを通信経路とする前提で、**内部・外部からの不正アクセスを防御するために、**多要素認証による利用者認証、端末認証、端末・サーバ・通信の監視・制御等を組み合わせたセキュリティ対策を指します。**この対策を講じるに当たっては、利用者毎に情報へのアクセス権限を適切に設定するとともに、アクセスの真正性、端末・サーバ・通信の安全性を確保する観点から、端末とクラウドサービスを提供するサーバ間の通信を暗号化し、認証により利用者のアクセスの適正さを常に確認しなければいけません。パブリッククラウド上で重要性分類Ⅱ以上の情報を取り扱う際には、強固なアクセス制御による対策を講じなければいけません。学校における働き方改革、教育活動の高度化、教育現場のレジリエンスの確保に資する**次世代校務DXの実施に際しては、重要性分類Ⅱ以上の情報をパブリッククラウド上で取り扱うため強固なアクセス制御を講じる必要があります。**

（参考）強固なアクセス制御に関わる要素技術

①アクセスの真正性に関する要素技術		
①-1	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 要素以上を組み合わせる認証方法。なりすましや不正アクセスを防ぐ。 ※強固なアクセス制御の基づくセキュリティ対策を講じるに当たっては、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
①-2	リスクベース認証	端末の IP アドレスや位置情報、使用されている Web ブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める認証方法。なりすましや不正アクセスを防ぐ。
①-3	シングルサインオン（SSO）	一度の認証で複数のシステムへのアクセスが可能となる仕組み。利便性を向上させるとともに、認証の煩雑化によるセキュリティリスクの低減を図る。
②端末・サーバ・通信の安全性に関する要素技術		
②-1	通信の暗号化	通信又は通信経路を暗号化し保護すること。第三者から通信内容を盗み見られることを防ぐ。
②-2	Web フィルタリング	インターネット上の特定のコンテンツや Web サイトへのアクセスを制限する機能。セキュリティリスクの高い Web サイトへのアクセスを防ぐ。
②-3	モバイル端末管理（MDM）	端末を一元的に監視・管理する機能。端末のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防ぐとともに、紛失・盗難等の際に遠隔でデータ消去を行い情報漏洩を防ぐ。
②-4	アンチウイルス	コンピュータウイルスやマルウェア感染への対策。既知のパターンファイル（マルウェア情報）からのマルウェアの検知・駆除や、不審な挙動をするプログラムの検知（ふるまい検知）・駆除等を行う。
②-5	データ暗号化	元データを変換し、第三者が簡単にデータの内容を解読できない状態にすること。アクセス権限が無い者の情報へのアクセスを制限する。
②-6	不正なアクセスを検知・遮断する技術	不正な通信を検知し、アクセスを遮断する等の制御を行う。 ※不正なアクセスの検知（IDS）または遮断（IPS）による対策、エンドポイント対策（EDR 等）、インターネットと繋がっているサーバ（Web サーバ）への外部からの攻撃を検知・防御する対策（WAF）、ネットワークとセキュリティを統合したクラウドサービスである SASE 等の活用が考えられる。

（参考）強固なアクセス制御による対策（イメージ図）



（※１）学習系システムにおいて、児童生徒の情報がまとまったデータを扱う領域（学級/学年/学校に属する児童生徒全員の名簿や、学級/学年/学校に属する児童生徒全員の学習アプリの利用履歴等）。

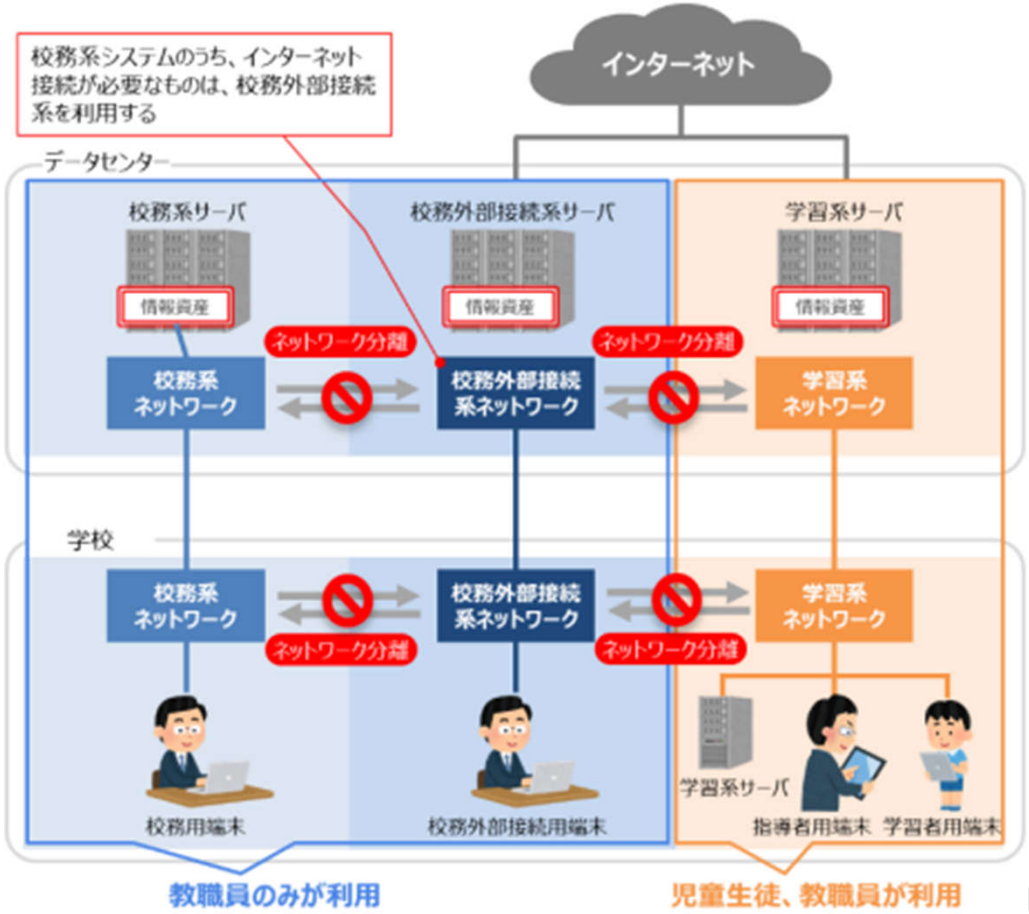
（※２）児童生徒本人またはその保護者が、当該児童生徒に関する重要性分類Ⅱ以上の情報資産のみにアクセスすることを想定したデータを扱う領域（健康診断票、通知表、定期考査・テスト等の採点結果等）。
多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

（※３）特に重要性の高い情報については閲覧可能な場所を学校内等に限定することも考えられる。

ネットワーク分離による対策

ネットワーク分離による対策とは、インターネットを介した外部からのリスクの高いシステムと重要性の高い情報との論理的又は物理的な分離を行い、かつ校務系システムと学習系システム間の通信経路の論理的又は物理的な分離を講じるセキュリティ対策を指します。この対策を講じたシステム構成には「校務系ネットワーク」、「校務外部接続系ネットワーク」、「学習系ネットワーク」の３種類のネットワークが存在することから、ネットワーク分離による対策は、「三層の対策（三層分離）」とも呼ばれます。この対策を講じたシステム構成の場合、「校務系システム」、「校務外部接続系システム」、「学習系システム」の間で通信する場合には、各システムにおけるアクセス権管理の徹底、無害化通信など適切な措置を講じる必要があります。

（参考）ネットワーク分離による対策（イメージ図）



3　技術的セキュリティ（アクセス制御）

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）アクセス制御等
　統括教育情報セキュリティ責任者又は教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員等がアクセスできないように、システム上制限しなければならない。特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産へのアクセスについては、多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、当該システムへの認証強度の向上とアクセス権管理を徹底すること。
＜略＞

【解説】
（１）アクセス制御
　各情報資産の分類に応じてアクセス制御を適切に講じることが重要である。例えば重要性分類Ⅱ以上の情報資産については、教職員等が職務上必要な場合に限って情報資産にアクセスできるよう設定することや、児童生徒およびその保護者が児童生徒本人の情報のみに限ってアクセスできるよう設定することが、情報セキュリティの確保において非常に重要である。権限を付与する際は、必要な権限のみ（編集・閲覧・複製・ダウンロード等）を付与することにも留意されたい。また、そのアクセス権限が運用実態に沿った適切なものかどうか、定期的に確認することが必要である。
＜略＞

4　技術的セキュリティ（セキュリティ情報の収集）

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＞
（３）情報セキュリティに関する情報の収集及び共有
　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

【解説】
（３）情報セキュリティに関する情報の収集及び周知
　情報セキュリティに関する技術は、新たな技術の開発や普及状況の変化により、期待した情報セキュリティの有効性が失われることや新技術への移行によって既存技術を利用したサービスを受けることができなくなる等、新たなリスクを発生する可能性もあり、情報システム等の情報セキュリティインシデントやセキュリティ侵害の未然の防止のために情報セキュリティに関する技術の動向や技術環境等の変化に関する情報収集と対策を行う必要がある。

情報セキュリティを取り巻く社会環境や技術環境等は常に変化していることから、統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティホールをはじめとするセキュリティ情報を収集し、教職員等の関係者に共有するとともに、ソフトウェア更新等の対策を検討する必要があります。

5　まとめ

最初のスライドの復習になりますが．．．．

技術的セキュリティ対策とは、ハードウェア・ソフトウェアやネットワークなどに対するアクセス制御、不正プログラム対策、不正アクセス対策等の技術的な安全管理措置を通じて情報資産を守る対策を指します。GIGAスクール構想による１人１台端末を用いた学習におけるクラウド活用に加えて、次世代校務DXの考え方の下で、校務でのクラウド活用も進んでいます。クラウド上で重要性の高い情報を扱う場面も増える中、教育委員会はこの変化に合わせた技術的セキュリティ対策の実施に対応することが求められます。

クラウドサービスを活用した教育活動