Microsoft

クラウド型校務支援システムを安全に利用するためには？

～設計と構築の指針～

日本マイクロソフト株式会社
ソリューションスペシャリスト
中田　寿穂

教育界はデジタル技術の進展により大きな変革を迎えており、クラウド型校務支援システムが教育の質と教職員の作業効率を向上させています。遠隔地からのアクセスも可能で、新しい働き方や学び方を実現しますが、セキュリティリスクも伴うため、慎重な対策が必要です。本ガイドは、文部科学省が推進する次世代校務DXを背景に、安全な利用を支援する指針を紹介します。特にITに詳しくない教職員や教育委員会向けに、セキュリティの課題を理解し、効果的な対策を実施するための実践的アドバイスを提供します。

次世代の校務 DX とは？

校務情報化の現状と課題

GIGA スクール構想の推進とともに、校務情報化への取り組みが加速しています。しかし、この進展には、いくつかの課題が存在します。次世代の校務 DX（デジタルトランスフォーメーション）の推進に向けた取組では、教育現場の情報化を進め、教育の質の向上と教職員の働き方改革を実現するために、さまざまな点に注力する必要があります。

現状
- GIGA スクール構想進行中
- 統合型校務支援システムの普及
- 職員室中心のシステム運用
- 導入コストの高さ など

課題
- 柔軟な働き方の困難さ
- データの標準化不足
- セキュリティと災害対策
- 導入コストの問題

校務 DX に向けた取り組み
- 校務系、学習系ネットワークの統合　・教職員の研修と能力向上
- 情報セキュリティポリシーの策定と改訂　・セキュリティ対策の強化
- データ連携基盤の構築　・校務支援システムのクラウド化
- 災害時の業務継続計画（BCP）の策定

文科省の教育情報セキュリティポリシーガイドラインとは

「教育情報セキュリティポリシーに関するガイドライン」は、文部科学省によって令和 6 年 1 月に改訂された文書で、地方公共団体の各教育委員会が教育情報セキュリティポリシーの策定や見直しを行う際の参考資料です。このガイドラインは、教育情報セキュリティの基本理念と考慮すべき点について解説し、GIGA スクール構想の進展や校務 DX の推進に伴う教育情報システムおよび情報セキュリティの高度化と重要度の増大に対応しています。「教育情報セキュリティポリシーに関するガイドライン」では、パブリッククラウド上で学習系・校務系情報を取り扱う際に、従来の境界防御型セキュリティから、強固なアクセス制御を前提とするセキュリティの考え方に変更する必要があると述べています。これは、ゼロトラストセキュリティモデルの原則に沿ったアプローチを指しており、内部・外部からの不正アクセスを防御するために、利用者認証（多要素認証）、端末認証、アクセス経路の監視・制御などを組み合わせた対策を実施することを推奨しています。

実施すべき主なセキュリティ対策
- 多要素認証の導入　・教育情報セキュリティ対策基準の適用
- 情報セキュリティポリシーの策定、見直し　・アクセス制御の強化

なぜ学校現場に
ゼロトラストセキュリティ？
の解説はこちら ▶

ゼロトラストセキュリティモデルとは

～デジタル庁の「ゼロトラストアーキテクチャ適用方針」より～

ゼロトラストセキュリティモデルとは？

ゼロトラストセキュリティは、セキュリティ戦略の一環として、どのような環境でも適用可能な一連の原則に基づいています。これは、特定の製品やサービスではなく、セキュリティの設計および実装方法に焦点を当てたアプローチです。ゼロトラストの基本的な原則には、「明示的に検証する」「最低特権アクセスを使用する」「侵害を前提とする」というものがあります。

ゼロトラストセキュリティを実現するためには

ゼロトラストセキュリティモデルを実現するためには、単にゼロトラストセキュリティに対応した製品を 1 つ購入するだけでは不十分です。ゼロトラストは、製品そのものではなく、組織全体のセキュリティを強化するための戦略的アプローチです。このモデルは、「決して信頼せず、常に確認する」という原則に基づき、組織内のあらゆるユーザー、デバイス、アプリケーション間の信頼関係を再構築します。そのため、ゼロトラストモデルを実装するには、組織全体で一連のセキュリティ対策を統合的に計画し、実行する必要があります。したがって、ゼロトラストモデルの導入においては、それを実現するための機能要件を満たす製品やサービスを選定し、組織の特定のニーズに合わせてこれらを統合的に活用することが求められます。製品選定に必要な機能要件は右のようなものがあります。製品を選定する際には、これらの機能要件を包括的に満たしているかどうかを慎重に確認することが重要です。

ゼロトラストの基本原則

1. 明示的に検証する
2. 必要最小限のアクセス権限を提供する
3. 侵害を前提とする

実施すべき主なセキュリティ対策

アイデンティティとアクセス管理
- 多要素認証 (MFA)
- リスクベース認証
- 条件付きアクセス
- 最小限の権限

セキュリティ監視と対応
- セキュリティ情報イベント管理 (SIEM)
- 自動化された脅威対応

データ保護
- データ暗号化
- データ損失防止 (DLP)

ネットワークセキュリティ
- マイクロセグメンテーション
- 暗号化された通信

デバイスセキュリティ
- デバイスコンプライアンス
- エンドポイント保護

継続的なリスク評価と改善
- セキュリティ評価ツール
- ユーザー教育と訓練

ゼロトラストモデルによる安全な設計指針とは

ゼロトラストセキュリティモデルに基づく、安全な利用のための設計指針は以下のような形になります。これらの指針は、デジタル庁が 2022 年 6 月 30 日に公開した「ゼロトラストアーキテクチャ適用方針」に沿っています。

アクセス管理

リスクベース認証

何をする？

ユーザーの行動パターンやアクセス地点の異常を検知し、リスクが高いと判断された場合に追加の認証手続きを要求します。

対応しないと…

不正アクセスやアカウント乗っ取りのリスクが高まります。ユーザーの異常な行動を検知して追加認証を要求しない場合、攻撃者が盗んだ認証情報だけでシステムにアクセスできる可能性があります。

条件付きアクセス

何をする？

アクセス許可を出す前に、デバイスの状態やユーザーのロケーションなど、特定の条件を基に評価します。

対応しないと…

セキュリティが不十分なデバイスや不審な場所からのアクセスを許可してしまうリスクがあります。これにより、マルウェアの感染拡大やデータ漏洩の可能性が高まります。

最小限の権限

何をする？

ユーザーやデバイスには、業務遂行に必要最小限のアクセス権限のみを付与し、不必要なリスクの露出を防ぎます。

対応しないと…

ユーザーやデバイスに必要以上のアクセス権限を付与することで、内部からの脅威や誤操作によるセキュリティインシデントの発生リスクが高まります。また、攻撃者がシステムに侵入した場合に、より多くのリソースやデータにアクセスできる可能性があり、被害を大きくします。

データ保護

データの暗号化

何をする？

保存中および転送中のデータを暗号化し、外部からの不正アクセスによる情報漏えいを防ぎます。

対応しないと…

暗号化されていないデータは、サイバー攻撃者にとって容易なターゲットとなり得ます。攻撃者がこれらのデータにアクセスした場合、機密情報が盗まれるリスクがあり、これにより企業の評判、顧客の信頼、さらには法的責任に関わる重大な問題が発生する可能性があります。

データ損失防止 (DLP)

何をする？

機密情報が組織外に不正に流出することを防ぐための策を講じます。

対応しないと…

DLP 策を実施しない場合、従業員による意図的または非意図的な機密情報の漏洩が起こりうります。これは組織のセキュリティ違反につながり、重要なビジネス情報の損失や競争上の不利益、顧客データの漏洩による信頼失墜など、組織に甚大な損害を与えかねません。

インシデント対応計画

インシデント検出と迅速な対応

何をする？

セキュリティインシデントを検出するためのシステムを設置し、発生した場合には迅速に対応するプロセスを整備します。

対応しないと…

インシデント検出システムや迅速な対応プロセスが不在の場合、セキュリティ違反やデータ漏洩が発生してもそれを早期に発見できず、問題が拡大するリスクがあります。対応が遅れることで、企業の損害が増大し、顧客やパートナーの信頼を損なう可能性が高まります。

事後分析と改善

何をする？

インシデントの原因を徹底的に分析し、再発防止のための改善策を講じます。

対応しないと…

インシデント後の分析や改善策の実施が不足している場合、同じ種類のセキュリティ違反が再発するリスクが高くなります。組織が同じ過ちを繰り返すことで、セキュリティ対策の無効性が露呈し、長期的に組織のセキュリティ姿勢の弱さが固定化する可能性があります。

エンドユーザー教育

セキュリティ意識の向上

何をする？

定期的なセキュリティ教育を実施し、エンドユーザーがセキュリティリスクを理解し、適切な対応ができるようにします。

対応しないと…

セキュリティ教育を怠ることで、従業員がセキュリティ脅威の兆候を見逃すリスクが高まります。これは組織内でのセキュリティ違反やデータ漏洩の発生確率を増加させ、企業の評判や財務への損害を引き起こす可能性があります。

フィッシング対策教育

何をする？

フィッシング攻撃などのサイバー脅威に対する認識を高め、不審なメールやリンクに対する正しい対処法を教育します。

対応しないと…

フィッシング対策の教育を受けていない従業員は、フィッシング詐欺により個人情報や企業の機密情報を漏らしてしまう可能性が高くなります。これにより、重要なビジネスデータの損失や身代金要求などのセキュリティインシデントに直面するリスクが増大します。

文科省「GIGA スクール構想の下での校務の情報化の在り方に関する専門家会議」で提示されたセキュリティ対策

令和 5 年 3 月、「GIGA スクール構想」のもとで開催された「校務の情報化の在り方に関する専門家会議」では、将来の教育情報システムにおける理想像が提示されました。この会議では、校務系ネットワークと学習系ネットワークの統合、ならびにパブリッククラウド環境を基盤とした次世代校務 DX の構想が明らかにされました。また、パブリッククラウドで学習系及び校務系情報を扱う際に、従来の境界防御型セキュリティから脱却し、強化されたアクセス制御を核とするセキュリティ方針の必要性が強調されました。資料の 17, 18 ページではクラウド上で校務系システムを利用する際のセキュリティ対策について述べられています。提案された技術要素には、ゼロトラストセキュリティに関する要素技術に加えて、一般的なセキュリティ対策も含まれています。また、デジタル庁が 2022 年 6 月 30 日に公表した「ゼロトラストアーキテクチャ適用方針」に記載されている設計や実装方法の一部は、この文書では触れられていません。

文科省から発信の
ドキュメントはこちら ▶

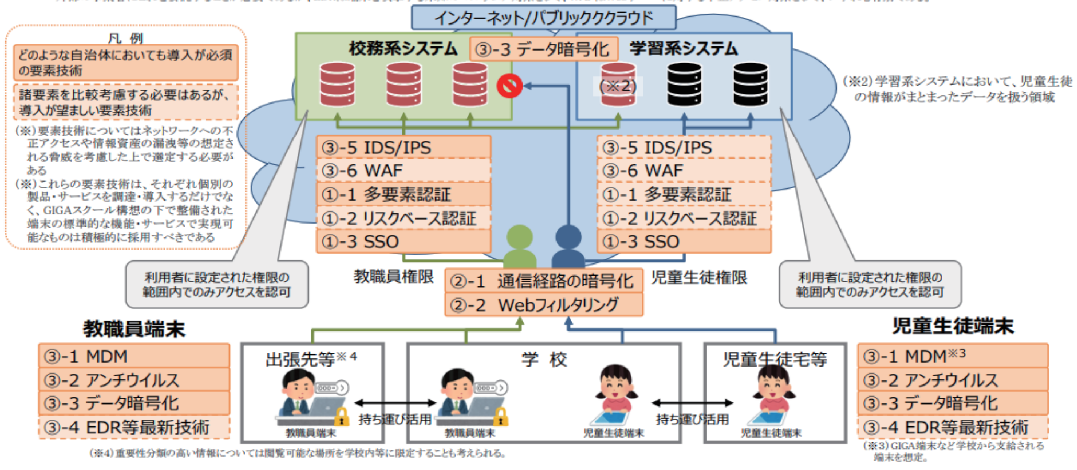
いわゆるゼロトラストセキュリティに関する要素技術イメージ

①アクセスの真正性に関する要素技術		
①-1	**多要素認証**	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	**リスクベース認証**	情報・データへのアクセスに対する認証に当たり、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技術
①-3	**シングルサインオン（SSO）**	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	**通信経路の暗号化**	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	**Webフィルタリング**	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	**モバイル端末管理（MDM）** (Mobile Device Management)	端末等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止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	**アンチウイルス**	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	**データ暗号化**	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	**EDR** (Endpoint Detection and Response)	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	**IDS/IPS** (Intrusion Detection System/Intrusion Prevention System)	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	**WAF** (Web Application Firewall)	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し、防御する機能。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、事前に定義した不正アクセスパターンとマッチングすることによりWebサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

アクセス制御を前提としたネットワークにおける情報セキュリティの確保イメージ

- 校務系システムに蓄積される情報や、学習系システムにおいて教員がアクセスし得る複数の児童生徒の学習履歴など、学校現場で取り扱う情報のうち機微度が高いものへのアクセスについては、前ページで示したセキュリティ技術を複数組み合わせることが適当。また、技術的対策だけでなく利用者のリテラシーも高める必要がある。
- 教職員が使用するネットワークや端末は、こうした情報・データを扱うことから、**【①-1 多要素認証、①-3 SSO、②-1 通信経路の暗号化、②-2 Webフィルタリング、③-1 MDM、③-2 アンチウイルス、③-3 データ暗号化、③-5 IDS/IPS】**の導入によるセキュリティの確保はどのような自治体においても必須である※1。

（※1）他方、上記以外の要素技術もセキュリティの向上に資するものであり、取り扱うデータの重要度やリスク要因の発生頻度を踏まえたセキュリティリスクと導入・運用費用、以下のような特徴等の諸要素を比較考慮する必要はあるが、導入が望ましいものと考えられる。**①-2 リスクベース認証**は、リスクの判定基準によりセキュリティと利便性のバランスが変わり得るものであるが、適切な判定基準が用いられることで認証の強度を高め得るものである。**③-4 EDR**、**③-6 WAF**は、その効果を最大限に発揮するためには専門的な知識を持つ人材による事前のチューニングとログ分析が必要であり、管理者がそのためのスキルを取得するか、外部の事業者にこれを委託することが必要であるが、EDRは端末を攻撃する未知のマルウェア対策として、WAFはWebサーバに対する不正アクセス対策として、いずれも有効である。



Microsoft のサービスでどのように対応できる?

セキュリティ対策		O365	M365 A for Device	M365 A3	M365 A3 + M365 A5 Security	M365 A3 + M365 A5 Compliance	M365 A5	Azure	Microsoft Learn	備考
ゼロトラストセキュリティを実現するための対策										
アイデンティティとアクセス管理	多要素認証	○	○	○	○	○	○	−	−	
	リスクベース認証	×	×	×	○	×	○	−	−	
	条件付きアクセス		○	○	○	○	○	−	−	
	最小限の権限	○	○	○	○	○	○	−	−	Microsoft 365 の管理者権限は役割ごとに最小限の権限を付与可能
データ保護	データの暗号化(デバイスストレージ)	○	○	○	○	○	○	−	−	BitLocke (Winodws OS に標準搭載)
	データの暗号化(コンテンツ)	×	×	△	△	○	○	−	−	Microsoft Purview Information Protection
	データ損失防止(メールとファイル)	×	×	○	○	○	○	−	−	Microsoft Purview Information Protection
	データ損失防止(エンドポイント)	×	×	×	×	○	○	−	−	Microsoft Purview
ネットワークセキュリティ	マイクロセグメンテーション	−	−	−	−	−	−	○	−	
	暗号化された通信	○	○	○	○	○	○	○	−	
	デバイスコンプライアンス	×	○	○	○	○	○	−	−	Intune
デバイスセキュリティ	エンドポイント保護 (EDR)	×	×	×	○	×	○	○	−	Defender for Endpoint
	セキュリティ情報インベントリ管理(SIEM)	△	△	△	○	△	○	○	−	Microsoft Sentinel
	自動化された脅威対応	△	△	△	○	△	○	−	−	
継続的なセキュリティ評価	セキュリティ評価ツール(Microsoft 365)	○	○	○	○	○	○	−	−	Defender for Office 365
	セキュリティ評価ツール(デバイス)	×	×	×	○	✖	○	−	−	
	セキュリティ評価ツール(Azure)	−	−	−	−	−	−	○	−	
	ユーザー教育と訓練	−	−	−	−	−	−	−	○	
GIGAスクール構想の下での校務DXについて ~教職員の働きやすさと教育活動の一層の高度化を目指して~ に記載されている対策										
デバイスの保護	端末管理(MDM)	×	○	○	○	○	○	−	−	Intune
	ウイルス対策	○	○	○	○	○	○	○	−	Defender for AntiVirus
校務支援システムの保護	IDS/IPS	−	−	−	−	−	−	○	−	Defender for Cloud
	WAF	−	−	−	−	−	−	○	−	Azure Web Application Firewall
	SSO	○	○	○	○	○	○	○	−	Microsoft Entra ID (SAML, OpenID, OAuth に対応)

ゼロトラストセキュリティの観点から見ると、Microsoft 365 A5 は最も包括的なセキュリティ機能を提供するため、クラウド型の校務支援システムにおける理想的な選択肢 です。Microsoft 365 A5 が提供する先進的なセキュリティ機能の一部を使わずに他のプランを選択する場合、いくつかのリスクが考えられます。たとえば、Microsoft 365 A3 を選択した場合のリスクとしては、A5 Security または A5 Compliance が提供する高度なセキュリティおよびコンプライアンス機能が利用できないため、セキュリティとコンプライアンスの両面におけるリスクがあります。そのため、サードパーティのセキュリティおよびコンプライアンスツールを選定し、必要な機能をカバーする、パスワードポリシーの強化や多要素認証の徹底を含む厳格なアイデンティティ管理プロセスを導入するといった、追加の対策が必要です。最終的には、教育機関がセキュリティに割り当てることができる予算とリソースを考慮しながら、リスクを最小限に抑えつつ、最大限のセキュリティ効果を得るためのバランスを見つける必要があります。

クラウド型校務支援システムを
安全に利用するための設計指針 ▶

Microsoft の製品、サービスでクラウド型校務支援システムを
安全に利用できる環境は構築できるのか? ▶

編集・執筆担当者 :

日本マイクロソフト株式会社
ソリューションスペシャリスト
中田 寿穂

2000 年まで青山学院大学理工学部物理学科で教員として勤務。2000 年から 2006 年まで、High Performance Computing (HPC) 分野のハードウェアおよびソフトウェアの開発に従事。2002 年に東京工業大学に導入した Athron MP クラスター「Presto III」がスーパーコンピューティングランキング「TOP500」で世界 47 位にランクイン。x86 クラスターとしては国内一位に輝く。2007 年、日本で初めて Google Apps (現 Google Workspace) を日本大学に導入。その後、100 以上の大学に同サービスを展開。2011 年、Microsoft が日本で Office 365 for Education を提供開始すると同時に、立教大学に同サービスを日本で初めて導入し、その後多数の大学での導入を携わった。2015 年に日本マイクロソフト株式会社に入社。Microsoft 365、Azure のソリューションスペシャリストとして勤務。2016 年に東京大学の事務基盤を Microsoft Azure 上に移行。2021 年に文部科学省のデータプラットフォーム事業「マテリアル先端リサーチインフラ事業」に参画。物質材料データの収集基盤を Microsoft Azure 上に構築。2023 年に文部科学省の次世代の校務デジタル化推進事業で秋田県の Microsoft 365 A5 + Microsoft Azure を利用した校務支援システムのクラウド化のプロジェクトに参画。現在、日本マイクロソフトで務める傍ら、香川大学と大阪工業大学の客員教授、及び秋田県教育庁の ICT 教育コーディネーターとして活動中。

本リーフレットついてのお問い合わせ

Microsoft
日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー