学校自治体向け通信技術

セキュリティ確保へのお役立ち情報

～セキュア環境構築の基本「ゼロトラスト」～

要点＆ポイント図解

モバイルコンピューティング推進コンソーシアム
ワイヤレスシステム活用委員会

2025年3月

目　次

なお、本誌は「学校自治体向け通信技術　- GIGA スクール：通信品質確保へのお役立ち情報 -」の続編となります。

ワイヤレスシステム活用委員会　技術解説書公開
「学校自治体向け通信技術ー GIGA スクール：通信品質確保へのお役立ち情報ー」（PDF 41.1MB）

GIGA スクール / 自治体 DX

ネットワークの通信品質を向上させる入門情報を提供します課題時の解決での一助にご利用下さい

はじめに

GIGA スクールや自治体 DX での無線 LAN 導入が進み、インターネット接続を含む能力確保も話題となるようになりました。並行して、グローバルに深刻化するセキュリティ問題に対して、「ゼロトラスト」という新しい考え方を適用したシステム体系を導入する指針が公開されています。これは、政府により 2020 年から推奨されている考え方で、その情報はデジタル庁より 2022 年 6 月に「ゼロトラストアーキテクチャ適用方針」、2023 年 5 月には「ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート」が公開されています。この考え方は、自治体や学校にとっても重要です。

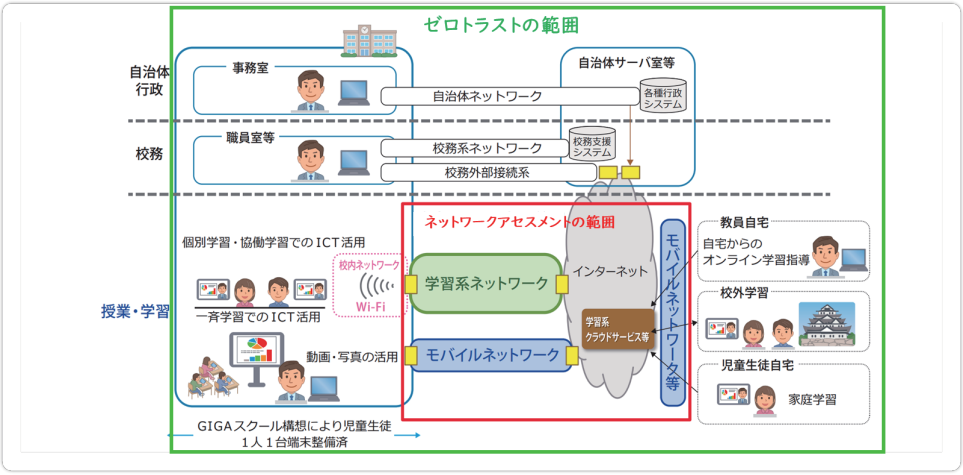
本誌では、その内容理解を深めるために「ゼロトラストに関するポイント解説情報」をお届けします。

デジタル庁 デジタル社会
推進標準ガイドライン

モバイルコンピューティング推進コンソーシアム（MCPC）
ワイヤレスシステム活用委員会 委員長
小林 佳和

参考

GIGA スクール構想により、一人一台端末をはじめとする ICT 環境の整備が進みました。しかし、実際に利用してみると様々な課題が明らかになっています。それを受けて、文部科学省は児童生徒および教職員が快適かつ安定的にネットワークを使用できることを目的に「学習系ネットワークにおける通信環境最適化ガイドブック」を公開しています。授業・学習を対象としたネットワークアセスメントは下記図の赤枠で示した範囲となりますが、今回はそれより広い緑枠で示した範囲が本書で取り扱う対象となります。



出典：文部科学省　学習系ネットワークにおける通信環境最適化ガイドブック【本章】

1 学校自治体でも、企業でも セキュリティの基本はゼロトラスト

セキュリティは、家の防犯のように必須の対策です。

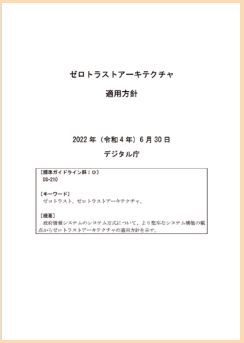
家の防犯

情報も同じ

情報の保護

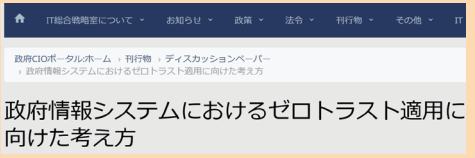
ネットワークにおいても、セキュリティは大切
（ゼロトラストという言葉をまず心にとめよう）

生成 AI を活用しての挽回や克服などの解決体験は、情報の活用力・解決力を高めます。



ゼロトラストアーキテクチャ
適用方針

2022 年（令和 4 年）6 月 30 日
デジタル庁



IT総合戦略室について　お知らせ　政策　法令　刊行物　その他　IT

政府CIOポータルホーム › 刊行物 › ディスカッションペーパー
› 政府情報システムにおけるゼロトラスト適用に向けた考え方

政府情報システムにおけるゼロトラスト適用に向けた考え方

デジタル庁　ゼロトラストアーキテクチャ適用方針

「ゼロトラスト」によるセキュリティ確保が、政府機関では推進されています。
内閣府やデジタル庁を中心に各省庁や自治体へ展開が進められています。

GIGA スクール構想のセキュリティは、「強固なアクセス制御」を実現する重要な役割を担っています。

*「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～」
（ https://www.mext.go.jp/content/20230308- mxt_jogai01-000027984_001.pdf）（令和 5 年 3 月 8 日）
p.18 にて示されている、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、利用者認証（多要素認証）、端末認証、アクセス経路の監視・制御等を組み合わせたセキュリティ対策を指す。

出典：文部科学省　教育情報セキュリティポリシーに関するガイドライン（令和 6 年 1 月）
https://www.mext.go.jp/content/20240202-mxt_jogai01-100003157_1.pdf
参考：内閣府からのゼロトラスト含むシステム要件 _ 公開例：
https://www8.cao.go.jp/space/comittee/bunkakai/bunkakai-dai18/sankou2.pdf

2 グローバルにゼロトラスト対応が進む

「ゼロトラスト」は、グローバルな考え方です。

日本での信号機の基本

世界でも同じ

世界でも同じ

ゼロトラストは世界標準

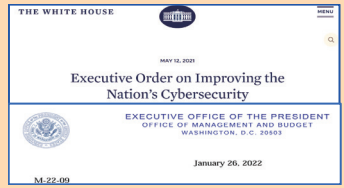
政府情報システムにおける
ゼロトラスト適用

各省庁・自治体

世界でも同じ

米国政府機関のサイバーセキュリティ
に関する改善の通知

M-22-09 Federal Zero Trust Strategy.pdf


THE WHITE HOUSE

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

CISA ゼロトラスト成熟度モデル ５つの柱

CISA: Cybersecurity and Infrastructure Security Agency
Zero Trust Maturity Model | CISA

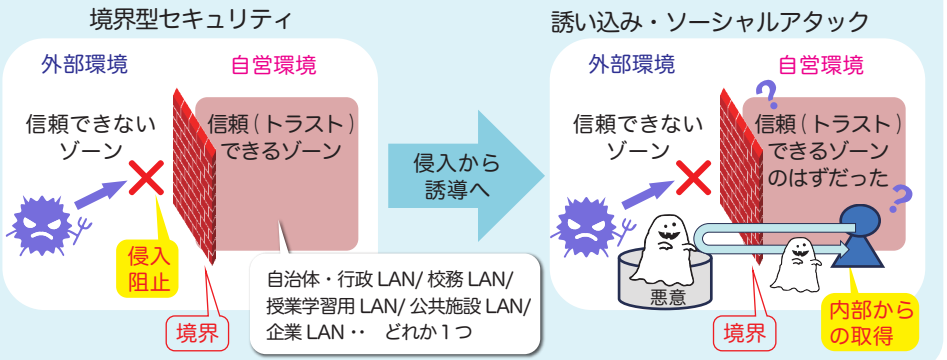
米国での「ゼロトラスト」の流れが、
世界へ、当然日本へも

学校の通信インフラの能力を確認するのに、データ通信帯域だけでなく、同時通信を考慮したセッション数の確保も大切で、アセスメントの重要な要素になっています。また並行して、セキュリティの確保を行うことも重要です。

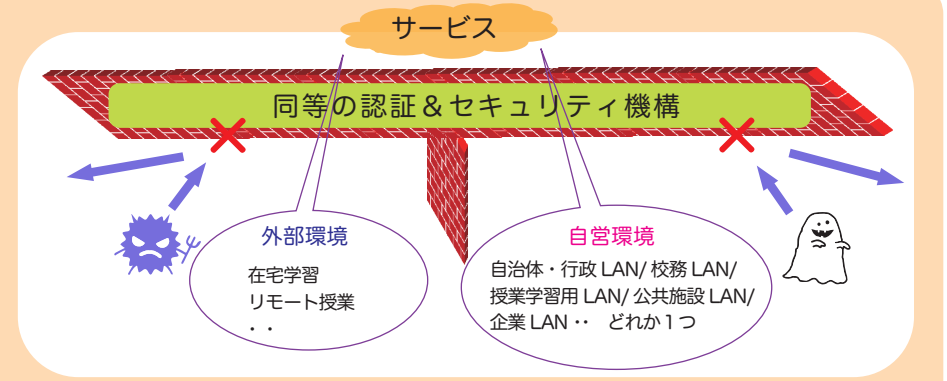
米国での政府系システムにおけるゼロトラスト適応は、欧州、アジアへと広まっています。当然、日本でも重要な事項になっています。セキュリティ管理対象は、タブレットやPC だけでなく、学校で使う IoT 機器全般に及びます。それは、電子黒板、投影機、書画カメラなど授業で使う機器だけでなく、防犯用のカメラや各種センサーも含まれます。

3 境界型セキュリティとゼロトラスト

私たちは、定期的な健康診断により現在の体調を知ることができます。



内部の信頼できるゾーンから、ソーシャル的に人気の高いキーワード (例えば教育・健康・美容など) を起点として、悪意のあるネットリソースへ誘い込む攻撃。このような攻撃で、信頼できるゾーンの境界が明確でなくなる。



信頼 (トラスト) できるゾーンを設けない（ゼロ）という考え方でセキュリティを高めるのが「ゼロトラスト」

セキュリティの考え方は、従来の外部（信頼できない）ゾーンと内部（信頼できる）ゾーンに分け、不正侵入などから境界を起点に守ることを重要とした「境界型」から「ゼロトラスト」へとシフトしています。

ゼロトラストという用語は、外部だけでなく内部もトラストできるゾーンではなくなったことに起因してつけられています 。

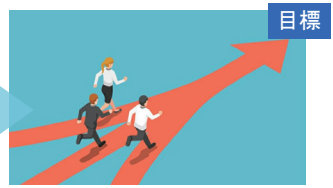
ゼロトラストでは、内部も外部も、個々のアクセスを確認して、必要最小限のリソースにアクセスにしてセキュリティを守ることになります。

4 管理項目（米国政府の管理項目）

ポイントを押さえて、運動や勉強などの活動をすると効果が出やすいことがわかっています。

目標なし

目標あり



フォーム調整や筋力強化など、個々の課題項目をもとに目標を達成していく

ゼロトラストの注目点

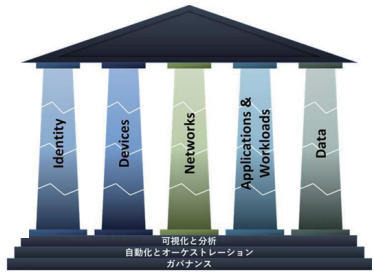
ゼロトラストの考え方

2022 年 1 月米国政府機関の
サイバーセキュリティに関する改善の通知
Memorandum 22-09　Moving the U.S. Government Toward Zero Trust　Cybersecurity Principles
M-22-09 Federal Zero Trust Strategy.pdf

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09



ゼロトラスト成熟度モデル 5 つの柱
Zero Trust Maturity Model | CISA

2020 年 8 月 米国国立標準技術研究所（NIST）が ゼロトラストを実現するために参考となるガイドラインを公開
NIST SP800 207 Zero Trust Architecture
SP 800-207, Zero Trust Architecture | CSRC

NIST Publicación especial 800-207

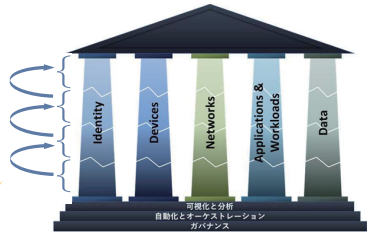
Arquitectura de confianza cero

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

ゼロトラスト成熟モデルの 5 つの柱

- アイデンティティ (ID)
- デバイス
- ネットワーク
- アプリケーションとワークロード
- データ

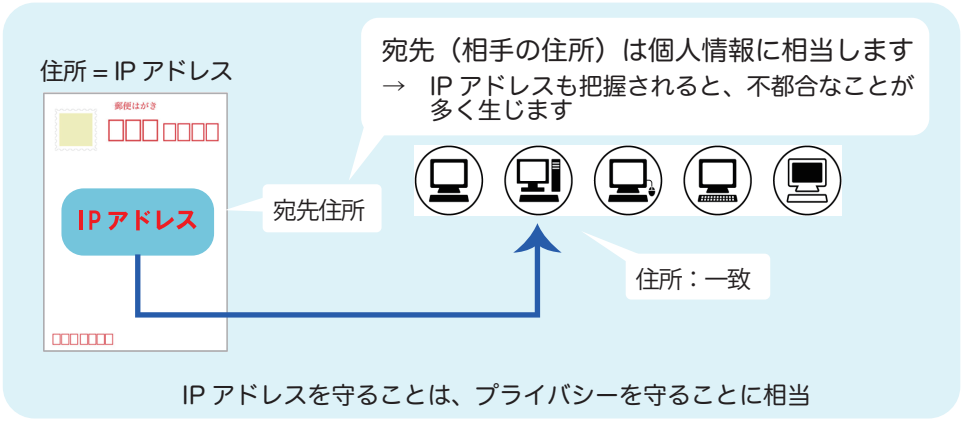
目標を「明示」して、順次レベルを上げる



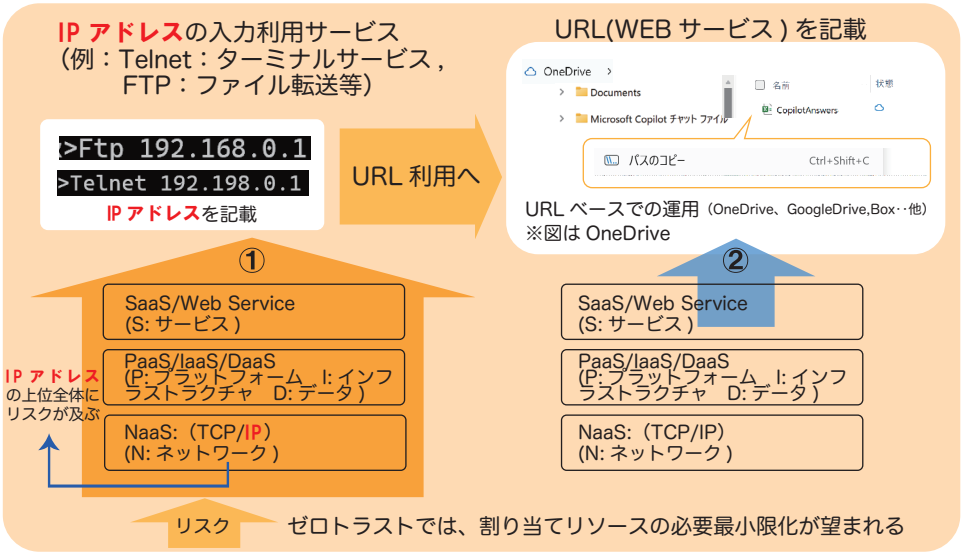
個々の目標を明確にし、達成レベルを向上していく考え方が、米国の文書で示されています。

5 守るべきポリシー　IP アドレスを隠蔽

IP アドレスは個人情報に相当し、隠蔽することでセキュリティが向上します。



IP アドレスを守ることは、プライバシーを守ることに相当



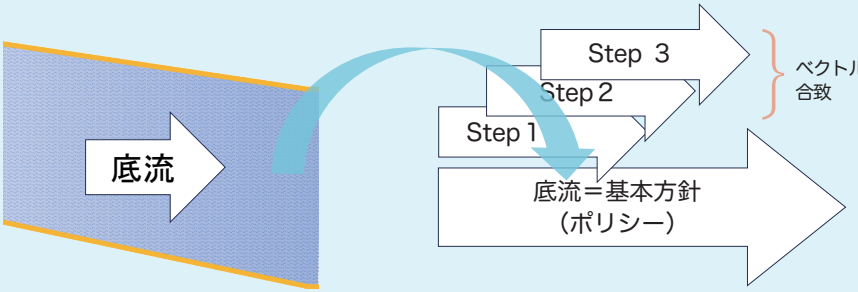
IP アドレスが悪意に特定されると、下記リスクが発生する。（上記左図①で示した赤矢印の範囲）

・地図上のロケーション
・ISP 情報（利用プロバイダー）
・IP トラッキングからの利用者活動追跡、嗜好などの分析（広告にも利用される）
・トラッキングと連動しての利用 SNS、サービスなどの分析
・IP アドレスの階層とその上のリソース分の乗っ取り・踏み台にされる

これに対して、WEB サービスは、使っているサービスの範囲（上記右図②で示した青矢印の範囲）に限定し、影響範囲をより絞ることができる。

6 検討の流れと基本方針

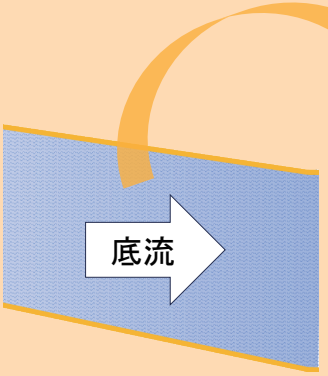
「ゼロトラスト」の実装推進を検討する際は、まず基本方針（ポリシー）定めます。

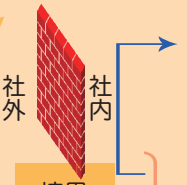


「ID/ パスワードの流出だけではアクセスできない仕組み」と「アクセスされる範囲の必要最小限化」をポリシーの一要素として考えます。その実現方法として、IP アドレス隠蔽と多要素認証などが挙げられます。

ゼロトラストの底流（基本方針）

基本事項





境界で認証を分けず、全アクセスを検証

認証は多要素認証とし、アクセス経路も複数を認める。

リソースアクセスの、必要最小限化を進める

SaaS/Web Service	アプリケーション
PaaS/IaaS/DaaS	認証、ミドル、DB
NaaS	ネットワーク

利用サービスとアクセス範囲を必用最小限にし、アクセスします。

ポリシーの実現は、現実的なステップを踏んで段階的に整えていくことが提案されています。

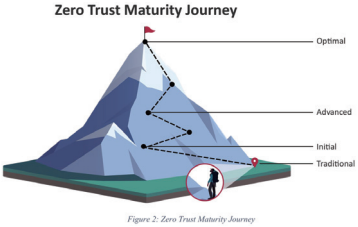


Figure 2: Zero Trust Maturity Journey

米国 CISA Zero Trust Maturity Model の Figure 2: Zero Trust Maturity Journey では、段階的にゴールへ向かう過程が説明されています。

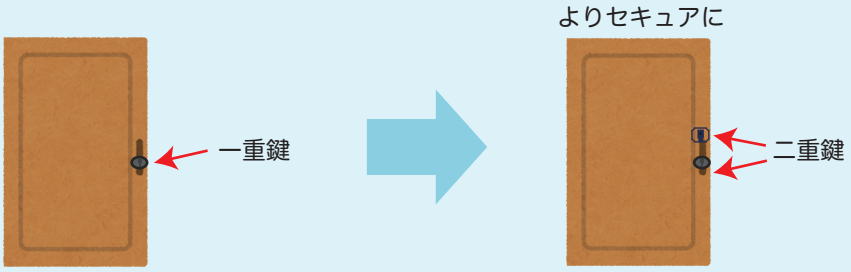
↓

目標に向かって、段階的に実現してしくことが重要です。

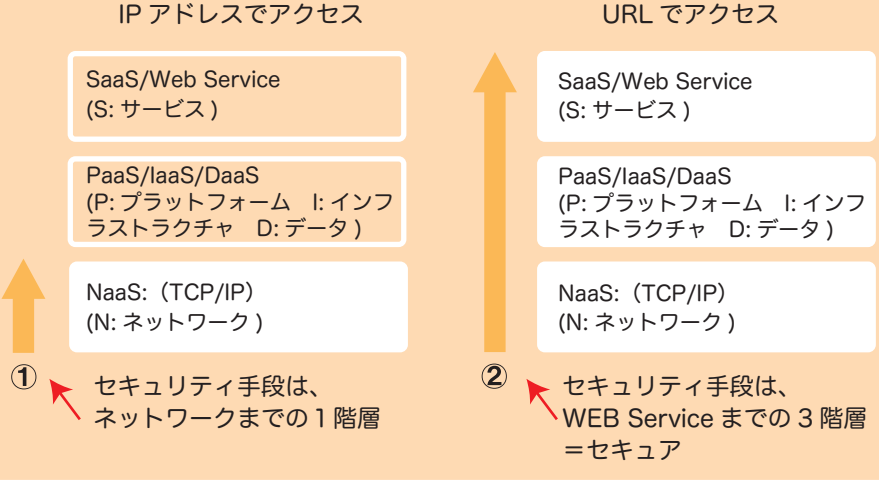
米国 CISA Zero Trust Maturity Model

7 階層を重ねて守る

鍵の二重化により、セキュリティが強化されます。



URL ベースでのアクセス（IP アドレスの秘匿化）により、
利用できるセリティ手段が増えます。



一重鍵より二重鍵の方が防犯力が高い

学校の通信インフラを守る機構も、上図の①だけの１階層より、②の３階層の方が防御力が高くなります。

IP アドレス隠蔽やアクセスリソースの最小化と合わせて、防御機構の多層化を考えることが重要です。

ゼロトラストは、ネットワーク層だけでなく、ミドル層からアプリ層まで連携させてセキュリティを保つ考え方です。逆に言うと、ゼロトラスト対応のネットワーク機器を導入するだけでは、ネットワーク層のセキュリティにとどまり、アクセスごとのリソース最小化には至りません。５本の柱全体でバランスさせて高度化していくことが求められます。

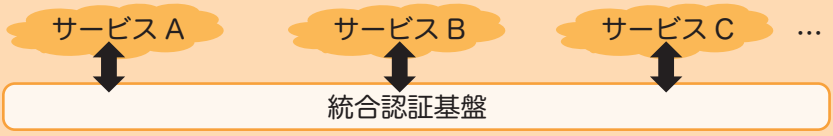
8 認証のセキュア化

私たちは、定常的な健康診断により現在の体調を知ることができます。
ID 管理は、ID そのものだけでなく、その使用方法も定期的にに診断しながら運用します。

認証

ID/ パスワードは、辞書攻撃や総当たり攻撃に弱いため、多要素認証を組み合わせた運用管理が必要です。

より高度な認証が必要



統合認証基盤（IAI: Integrated Authentication Infrastructure）の整備

シングルサインオン（SSO）：1 回のログインで複数のサービスにアクセス

ID ライフサイクル管理：正社員、派遣社員、パート社員の退社などに合わせたアカウント更新・削除の自動化

多要素認証（MFA: Multi-Factor Authentication）：ID/ パスワード＋α(多経路を含む)

アクセス管理（AM: Access Management）：
特権からゲストまで、必要な期間・最小範囲だけ提供＆更新
PAM(Privileged Access Management) による特権アクセスの管理、監視および制御
IGA(Identity Governance and Administration) による必要最小限のアクセス権限の管理
ネットワーク上の資源の検索・属性および運用管理（サービスディレクトリ）

エンドポイントセキュリティ：アクセス元の端末・デバイスのセキュリティ状態を確認し、アクセス要求ごとに必要最小限のアクセスを許可

継続的監視と改善：セキュリティ状態の監視をログも含めて実施
新たな脅威や働き方のプロセス革新に対応した適切な改善をサイクルで提供し、セキュリティ対策を順次実施

ID 管理は、多くの ID/ パスワードを様々なアプリケーションで用意すると、リスクが高まります。

そのため、シングルサインオン (SSO) を利用し、多要素認証を組み合わせることで、セキュリティを強化して運用します。

特に学校においては、卒業生や退職者を含む最新の利用者情報、児童生徒や先生更には各接続デバイスでのアクセス権限を正しく管理し、継続して運用していくことが重要です。

ここでは、5 本の柱の内のアイデンティティ (ID) に着目していますが、他の柱も同様に実施すべき項目を掘り下げて検討し運用する必要があります。

9 アプリケーションファイアウォール

サービスを利用する際、個々の通信についての振る舞い監視が必要です。

※画像は Copilot にて生成

関所にて通行者の振る舞いを確認

怪しい兆候
- 不審な行動や挙動
- 通行証が不完全
- 怪しい目的地

アプリケーションの、通信　管理

アプリケーションファイヤウォールの基本は、以下の 2 つです。

①アプリケーションプロキシ
メールプロキシのように、別の場所で通信を代行して処理する方式で、通信内容を検査し、不審な挙動や疑わしい振る舞いをチェックします。

②Web アプリケーションファイアウォール (WAF)
Web アプリケーションに対する攻撃を防ぐため、悪意のあるヘッダの挿入を検出して除去したり、負荷攻撃を軽減したりします。入力データの振る舞いを監視・解析することで、不正なリクエストをブロックし、正常な利用を維持します。

これらの 2 つの要素を基盤に、アプリケーションファイアウォールはさらに高度な挙動解析を行います。

アプリケーションファイアウォールは、上記①および②のような行動（振る舞い）監視を行い、必要に応じて以下の対応を行います。

- 通信パケットの変更
- 通信セッションに対するアプリケーションへのアクセス遮断
- 管理者へのアラート通知
- 生成 AI と連携し、ノウハウや対処方法を蓄積し、対処案の提示

10 一人ひとりを伸ばすセキュアなサービス活用

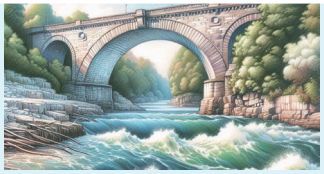
私たちは、セキュリティを確保しつつ、新しい考え方やチャンスが
広がるような機会を提供していくことが大切です。

水量の多い川に架けられた橋

※画像は Copilot にて生成

→危険なので、誰も橋にも近づかない。
つまり、誰も橋を使わない。

→より安全な橋の使用方法や、橋自体
の高度な機構への刷新を考える。



一人ひとりの成長を支えるサービス

アクティブラーニング

「教え合い」を「学び合い」に

授業実践　空間をセキュアに提供

Microsoft Teamsのイマーシブ スペースの概要

「能力は、遺伝か環境か？」という、議論があります。

　少なくとも、環境が大きな影響を与えることは知られています。
より良い環境に向けて、１人１台の情報端末や、GIGA スクール時代の学校、さらには生成 AI を活用できるような先端的な環境についても議論されています。才能を伸ばすためには、確かに様々な発想力や課題を見出すチャンス、さらにそれらの課題を克服したり、挽回したり、合意形成の経験を積んだりする機会が重要であり、大切です。

　そのような場をセキュアに、かつ常に安全な橋渡しを行いながら提供し、児童生徒たちの成長の芽を育んでいくことが期待されています。

終わりに

学校や自治体のネットワーク環境のセキュアな運用に役立つ情報をお届けしました。

一人一台端末での ICT 化の中で、多くの意見交換を行い、それをまとめるような授業の経験が重要です。このまとめには、合意形成のプロセスや、他の人に伝えるためにクイズや演劇などに置き換えて活用する経験も含まれます。

そのような中で、アプリケーションを使ったり、児童生徒同士が話し合ったりする環境を、セキュアに確保することが不可欠です。

そして、セキュア化で大切になってきているのが「ゼロトラスト」です。

その基本用語や 5 本の柱の確認、今後の拡充へのポイントを整理しました。

今回の内容は基本的な部分ですが、インターネットに接続することで、学校だけでなく自宅など、場所を問わずに上記経験を含む授業提供への一助となれば幸いです。

最後に、MCPC 会員の皆様、JAPET&CEC 様をはじめ、お世話になりました皆様に感謝申し上げます。

モバイルコンピューティング推進コンソーシアム（MCPC）
ワイヤレスシステム活用委員会 委員長
小林 佳和

一読後での、さらに進んだ検討に役立つ URL（参考）

文部科学省 ネットワークアセスメントの 2024 年説明
【事務連絡】通信ネットワーク環境の評価（アセスメント）の実施について（依頼）（令和 5 年 2 月 3 日）：文部科学省

文部科学省 セキュリティポリシー（2024 年）
「教育情報セキュリティポリシーに関するガイドライン」公表について：文部科学省

生成 AI の学校での利用ガイド
初等中等教育段階における生成 AI の利用に関する暫定的なガイドライン（mext.go.jp）

令和 5 年 3 月の答申
次期教育振興基本計画について（答申）（中教審第 241 号）：文部科学省（mext.go.jp）

Bing（Edge）用 Copilot
https://learn.microsoft.com/ja-jp/copilot/edge/?WT.mc_id=M365-MVP-38619

Bing AI を使って知の世界を理解する
Bing AI を使用して知識の世界を活用する | Microsoft Learn/

責任ある AI を理解する
責任ある AI に関する考慮事項を理解する - Training | Microsoft Learn

企業学校向けアカウントでの Copilot（旧 Bing Chat Enterprise）説明
Copilot の概要 | Microsoft Learn

テレワーク・自宅学習 お役立ち情報 - Microsoft atLife
https://www.microsoft.com/ja-jp/atlife/useful-for-home-and-family.aspx?%20WT.mc_id=M365-MVP-38619

AI 戦略会議（内閣府）
https://www8.cao.go.jp/cstp/ai/ai_senryaku/ai_senryaku.html

モバイルコンピューティング推進コンソーシアム
ワイヤレスシステム活用委員会
＜企画・編集メンバー＞

ワイヤレスシステム活用委員長	小林　佳和	日本電気株式会社 /ＮＥＣネッツエスアイ株式会社 / 山形大学客員教授（執筆、作図、校正）
学校自治体ネットワーク WG 主査	樋口　昌代	NEC プラットフォームズ株式会社 （参画）
学校自治体ネットワーク WG 副主査	西尾　由起	株式会社東陽テクニカ （参画、校正）
	松村　淳	IoT-EX 株式会社 （参画）
	沢田　健介	新潟工科大学（参画）
	藤井　新吾	KDDI 株式会社（参画）
	瀧澤　豊吉	日本アンテナ株式会社（参画）
	羽鳥　昭宏	日本アンテナ株式会社（参画）
	岸本　和久	日本アンテナ株式会社（参画）
事務局	宮坂　敏樹	MCPC（参画、校正）
JAPET＆CEC	乃一　志保	一般社団法人日本教育情報化振興会（参画、校正）

※企画・編集メンバーは 2025 年 3 月現在のメンバーです。

【MCPC について】
ワイヤレスデータ通信とコンピューティングシステム（モバイルシステム）の普及を促進するために、1997 年我が国を代表する移動体通信会社、コンピュータハードウェア / ソフトウェア会社、携帯電話、システムインテグレータなどにより組織化されました。現在、世界をリードするワイヤレステクノロジーで最先端の IoT・AI ソリューション追求し飛躍的発展を目指しており、そのための技術課題への対応、運用課題の調査・研究、開発の推進、標準化、相互接続性検証、普及啓発活動、人材育成などの活動を行っています。さらには、米国姉妹組織の USB-IF、Bluetooth SIG などと連携を図りながら、モバイル利活用の IoT・AI ソリューションの市場拡大と利用環境の高度化に務めています。
（2025 年 3 月現在　会員会社数 161 社）

本冊子ダウンロード用２次元コード
https://www.mcpc-jp.org/pdf/mcpc_zerotorasuto-20250303.pdf

５Ｇ＆Ｌ５Ｇで飛躍する
MCPC

学校自治体向け通信技術
セキュリティ確保へのお役立ち情報
～ セキュア環境構築の基本“ゼロトラスト” ～
要点＆ポイント図解

発　行　元　モバイルコンピューティング推進コンソーシアム（MCPC）
発　行　日　2025 年 3 月
製作／編集　MCPC ワイヤレスシステム活用委員会
　　学校自治体ネットワーク WG
　　ドローン WG
問合わせ先：MCPC 事務局
〒105-0011　東京都港区芝公園 3－5－12　長谷川グリーンビル 2 階
TEL：03-5401-1935　　FAX：03-5401-1937
E-mail：office@mcpc-jp.org　URL：https://www.mcpc-jp.org/