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

～ゼロトラストの基本“ログイン /ID 管理”～

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

2026 年 3 月

GIGA スクールと自治体 DX

セキュリティを向上させる入門情報を ID 管理起点に提供します。

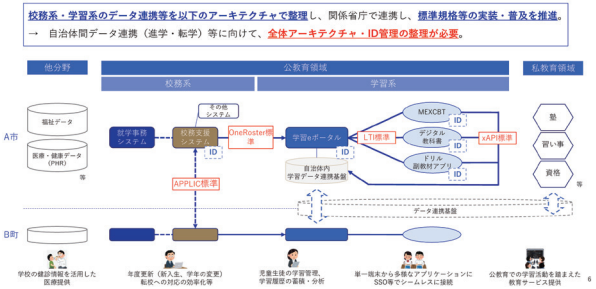
はじめに：GIGA スクールの現状

学校のネットワーク環境では、デジタル教科書の利用をはじめ、個々を伸ばす児童生徒自身での主体的な活用、先生と児童生徒やその保護者とのやり取りなど、DX(デジタルトランスフォーメーション) で付加価値をつけ、よりよい教育環境となる使われ方が期待されています。そのシステム活用の第一歩となるのがログイン /ID 管理です。ゼロトラストの 5 本の柱の一つにも「IDENTITY（ID 管理）」が挙げられています。「ログインする人」はそのまま「アクセスする人」でもあるため、アクセス管理と表現される場合も有ります。本冊子では、その ID 管理について紐解きます。

＜補足＞

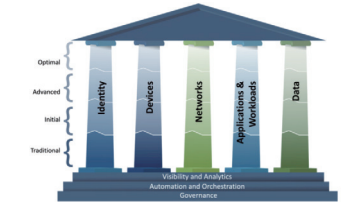
①デジタル庁：「教育 DX におけるデジタル庁の取組」

教育分野におけるデータ連携の考え方　https://www.mext.go.jp/content/20240419-mxt_syoto01-000035499_4.pdf



【資料 2-3】教育 DX におけるデジタル庁の取組 教育分野におけるデータ連携の考え方

②CISA（米国サイバーセキュリティ庁) :「ゼロトラストを構成する 5 本柱（Five Pillars）」



1．IDENTITY（アクセス者管理／ ID 管理）
2．DEVICES（アクセス端末）
3．NETWORK（通信路）
4．APPLICATIONS & WORKLOADS（アプリと動作）
5．DATA（情報）

Zero Trust Maturity Model | CISA　https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

③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」

https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

第 3 版に改定 : 令和 7(2025) 年 3 月

ID 管理に関して　多要素認証の推進が説かれ、それに付随して以下を進めることが説明されています

・アクセス権限の最小化
・端末管理 / 更新状況の確認
・データの機密性・可用性の確保

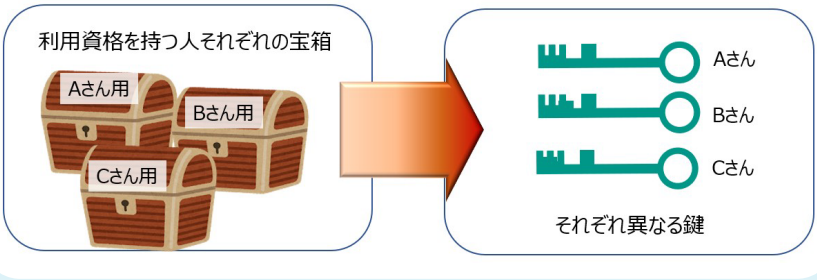
目　次

なお、本誌は「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」～」の続編となります。

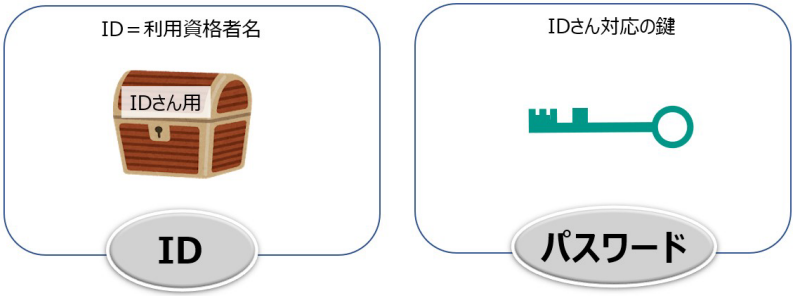
「学校自治体向け通信技術　セキュリティ確保へのお役立ち情報～セキュア環境構築の基本「ゼロトラスト」～」（PDF 58.7MB）

1 学校自治体でも、企業でも
サービス利用開始はログインから

宝箱のアクセス権 (利用権) を持つ人を想像してみましょう。
利用者は、各自自分の箱を選び、対応する鍵を使って箱を開けるでしょう。



情報機器利用開始 /
サービス利用開始



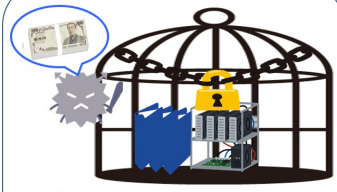
ID とパスワードは、情報機器やサービスの利用を開始するための重要な項目です。
忘れてしまうと利用に支障が出るため、しっかりと管理しましょう。

管理とは
・自分が忘れないようにすること
だけでなく
・他の人に知られたり奪われたりしないようにすること
も大切です。

2 サイバー攻撃の増加で高まる ID 管理の重要性

近年、学校や自治体を狙ったサイバー攻撃が急増しています。特に ID やパスワードの情報が狙われ、万が一奪われると、重要な資産や個人情報が簡単に悪用されてしまいます。

ランサムウエア



企業資産を使えなくして身代金を要求

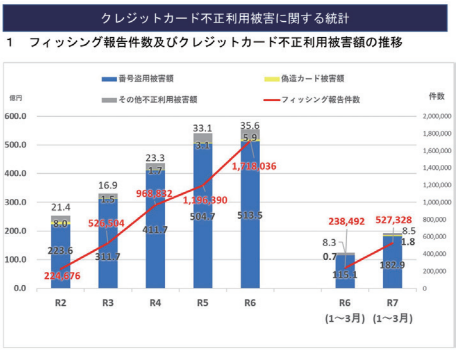
乗っ取り

本人になりすまし、証券の不正取引や悪意ある通信をしたりする

犯罪統計例

出典：警察庁

令和７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



https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

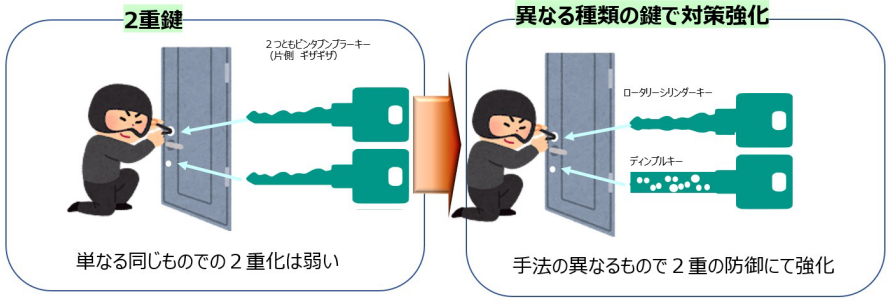
※1 フィシング：社会的な行動心理を利用し、偽物のサービスへ誘導してログインさせ、ID・パスワードを盗み取る攻撃

クレジットカードの不正利用被害だけを見ても、その攻撃の影響度は年々増加しています。
その背景には、フィッシングによる認証手段を奪う攻撃があります。
盗まれた認証情報を元に、「企業資産を使えなくして身代金を要求する」、「乗っ取って悪用する」といった行為が容易にできてしまうため、攻撃者にとって認証手段 (ID/パスワード) は格好の標的となっています。

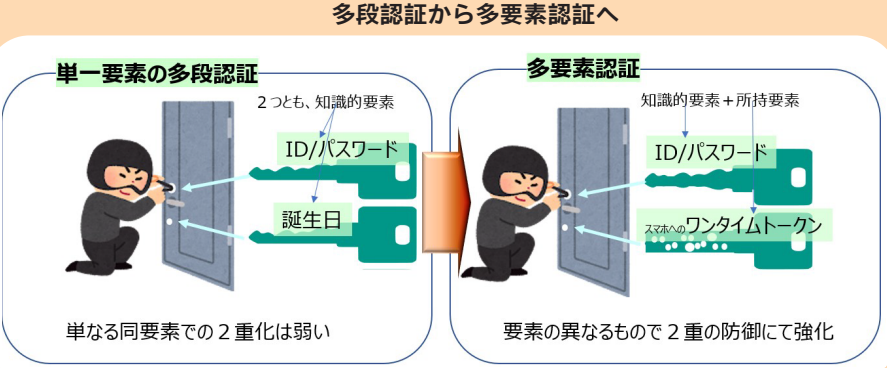
従来のセキュリティ対策では、一度認証される (ログインに成功する) と内部は “信頼” されてしまう設計が多く、ID やパスワードが奪われると被害が拡大しやすいという課題があり、それが容易さにつながっていました。ゼロトラストの考え方では、「認証情報が奪われることを前提」とし、被害を最小限に抑える設計が重要となります。それには、攻撃を受けた際の安全な復旧と事業や活動の継続性も含まれます。

3 ドアの２重鍵と多段認証・多要素認証

セキュリテイ対策として、私たちはドアを２重鍵にしたりします。



認証も異なる要素の組み合わせへ



多要素認証（MFA: Multi-Factor Authentication）に対する要素は、基本的には３つあります。

要素	例
知識要素 Knowledge	パスワード 絵や数字の場所と選択する順番、PINコード 秘密の質問/誕生日/住所/電話番号/生まれた市町村
所持要素 Possession	スマートデバイス カード/認証キー/社員証/ワンタイム用トークン(パスワード) QRコード/対応表/認証コード生成デバイス・アプリ
生体要素 Inherence	指紋認証/顔認証/ 虹彩認証/声紋認証/ 静脈認証/歩行パターンなどのモーション認証

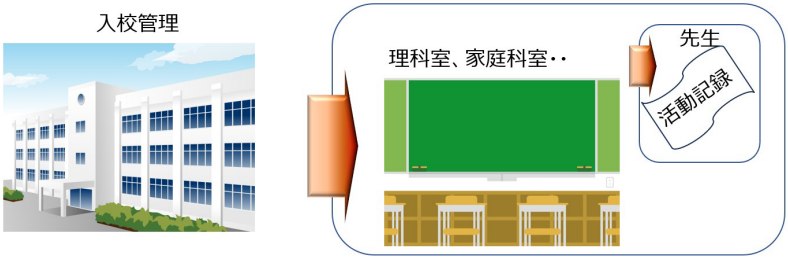
多要素を組み合わせて認証を行う多要素認証利用が求められています。知的要素と所持要素の組み合わせや、知的要素と生体要素の組み合わせといった構成が多要素認証になります。最近ではスマートフォンやタブレットでも、多要素認証が一般的に使われるようになっています。

生体認証だけあれば１段階の認証でも本人を示す固有情報なので安全ではないかという声もありますが、万能ではありません。例えば、指紋や顔認証も偽造や誤認識、端末依存といったリスクがあります。そのため、生体認証はあくまで「要素の一つ」として活用し、他の要素と組み合わせて多要素認証で利用することが重要です。

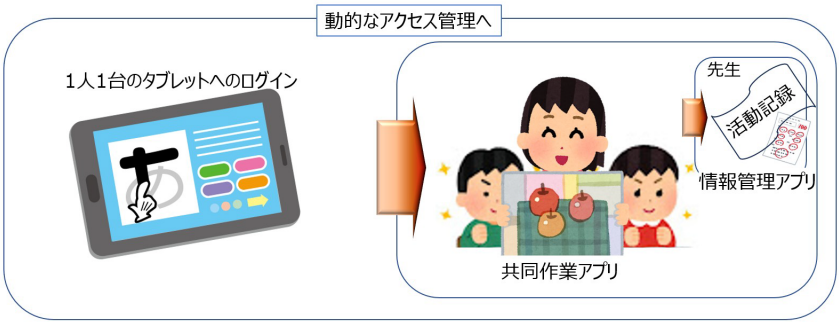
4 利用できるサービスに対応した管理

サービス毎にアクセス管理があります

従来は、静的なアクセス管理で役割や階層ごとに固定された権限管理でした



動的アクセス管理
ゼロトラストでは重要



サービスごと・役割ごと・活動ごとに異なるアクセス管理を行い、
「最小権限＋動的制御＋継続的検証」を実現

ゼロトラストでは、「状況（時間・場所・端末・利用状況）に応じて権限が変化する」考え方を取り入れて管理・運用します。

まず、授業に関してのシーンにおいて、①個人 ②共同 ③先生 の３つに分けて考えると基本がしっかり押さえられます。

その上で、②共同作業においてアクセス範囲が、班や教室などに限定し、作業内容を適切に守ります。

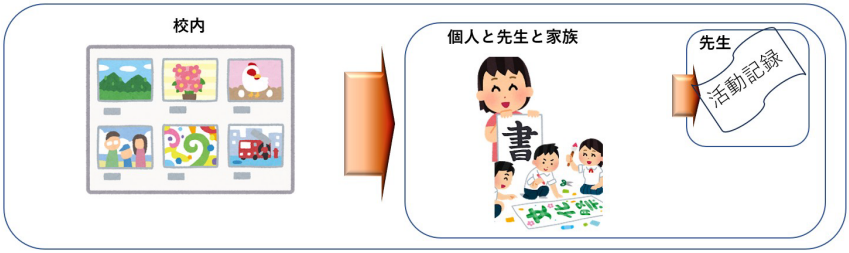
例えば、児童生徒の嫌がらせ的書き込みや、著作物へのいたずらを防ぐような範囲設定を考え、情報の開示範囲を動的に変更できる仕組みを加えた運用をすることが重要です。

また、③先生が扱う管理領域では、悪意のある侵入を防ぐために、「一度認証されたら安全」ではなく、利用中も継続的に正当性を検証し続ける機構を加えた運用をすることが重要です。

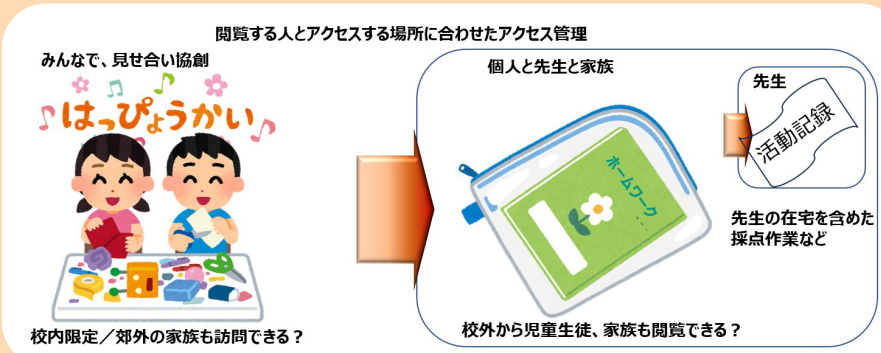
5 利用者の想定と場所を考えたアクセス管理

利用者の想定と扱う内容のレベルやアクセス場所を踏まえたアクセス管理が重要です。

閲覧する人とアクセスする場所に合わせて管理することが大切です。
（アクセスできるのは本人とクラスメイトまでなのか、家族を含むのか、アクセスする場所は校外を含むのかなどを考えて、従来も運用されてきました。）



校外アクセスも考慮した管理



場所（校内・校外）によるアクセスリスクの違いがあります。校外からのアクセスでも多要素認証でのアクセスと持続的検証での運用管理が必要です。また扱う内容にも十分な注意が必要です。

学校の ICT 活用は、校内だけでなく、校外や家庭からもアクセスする機会が増えています。ゼロトラストの考え方では、「どこからアクセスしても安全であること」が求められます。

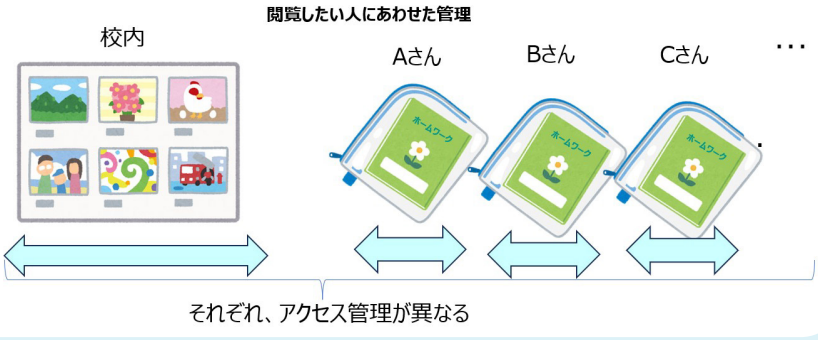
ホームワークなどでは家族が内容を見たり指導したりすることが想定されます。一方で、場合によっては、他の児童生徒の回答を勝手に書き換えようとする子どもが出てくる可能性もあります。また、デジタル教科書を自宅で開いて勉強したい子どもに対しては、その意欲を伸ばしてあげたいと考える大人も多いでしょう。

そのため、閲覧と書き込み権限を細かく管理し、デバイス管理とあわせて運用することで、子ども毎のホームワーク環境を適切に運用することが必要です。また、班ごとの共同作業では、その班で利用するサービスごとに招待と参加管理を行う方法を考えることも有効です。個人の ID を複数人で共用させることにはセキュリティ面で大きなリスクがあり避けるべきです。

さらに校外アクセスはインターネット上のリスクにさらされやすいため、特に厳格な認証や端末の健全性確認 (OS アップデート、ウィルス対策など) が必要です。学校ごとに、家族がアクセスできる情報範囲やパスワードの管理方法など、運用ルールを明確に定めることも大切となってきています。

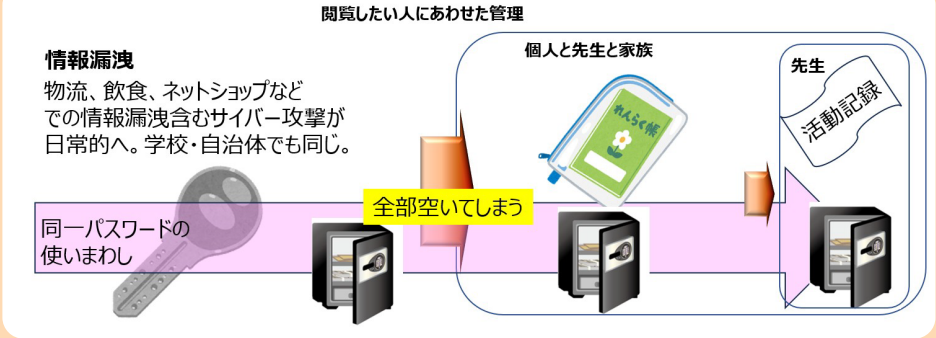
6 同一 ID/ パスワードの使いまわし

従来の学校では、物理的にアクセス管理が使う場所やノートや教室やプリントなどの媒体などで分かれていました。



悪意の攻撃
➡ 使い回しをしていないかを探る

見て欲しい範囲とみて欲しくない範囲がある



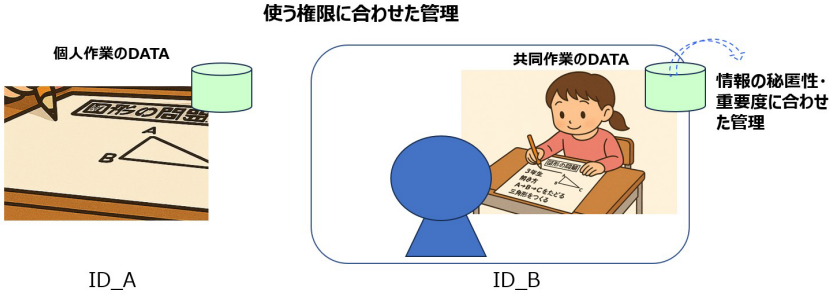
同じ ID/ パスワードを複数サービスで使うと、一つのサービスが漏洩した際に他のサービスにも不正アクセスのリスクが高まります。例えば、個人情報や重要なデータが一度に危険にさらされたりします。

悪意のある攻撃者は、利用者のID/パスワードを盗んだ後、それらを辞書として登録します。そして、同じ利用者が使っている他のサービスへの侵入をその ID/ パスワードで試みます。この辞書には、大文字や特殊文字などの組み合わせもその人毎に辞書化され、攻撃を仕掛けてきます。
ゼロトラストの考え方では、「ID が奪われることを前提」に設計し、被害を最小限に抑えることが重要です。
そのために、“利用者ごとにアクセスできる情報や利用サービスを最小限にする”、“想定外のアクセスのシステム監視をする”、“ID が奪われたことを想定した対応パターンの事前準備する” などをシステム運用として考える必要があります。

そのような工夫で、“ゼロトラストは「奪われる前提」で検討”することが求められています。

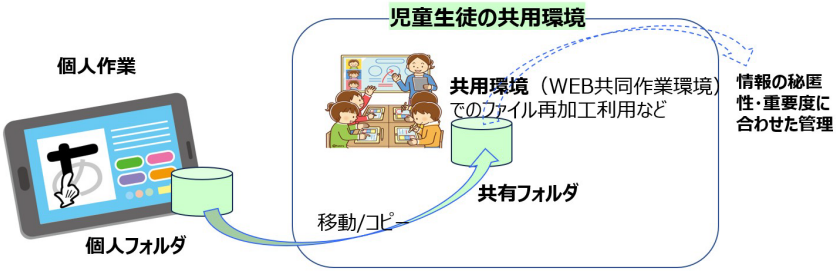
7 情報の共有と個人活動

情報の移動管理



データ自体も守る環境と運用が必要

個人 ID を共有せずに、個人・共同それぞれの作業が行える環境の管理が必要です。



個人 ID で管理されたデータに直接ログインさせず、共用の場所に移動またはコピーして利用する運用も可能です。このように、利用者の ID を起点としない運用手段も含め、ゼロトラストでは「データそのものを守る」ことも重要です。

情報資産は、セキュリティ侵害による影響度（被害の 大きさ）に応じて４段階に分類・仕分けし、その重要性に応じた対策を講じる必要があります。この考え方は文部科学省「情報セキュリティハンドブック」(令和７年３月) の図表１などで説明されています。

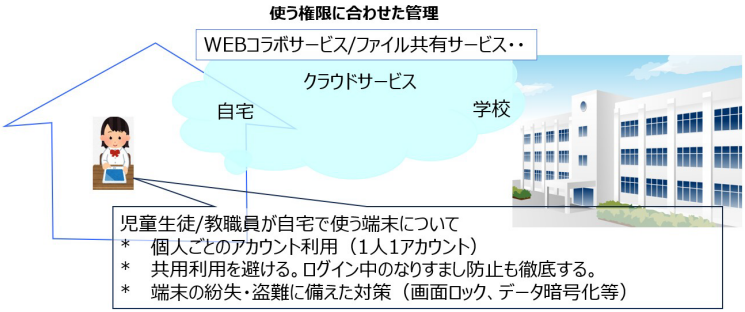
同ハンドブックでは、情報資産を重要性をⅠからⅣの ４ 段階に分類しています。最も高い重要性Ⅰは、情報が侵害された場合に甚大な被害が想定され、学校もしくは特定個人が著しく不利益を被る情報であり、要配慮個人情報を含むもの等としています。最も低い重要性Ⅳは、セキュリティ侵害が発生しても学校事務及び教育活動の実施にほとんど影響を及ぼさない情報 としています。

また、重要度だけでなく機密性・完全性・可用性の侵害の影響度を考慮することも記載されています。

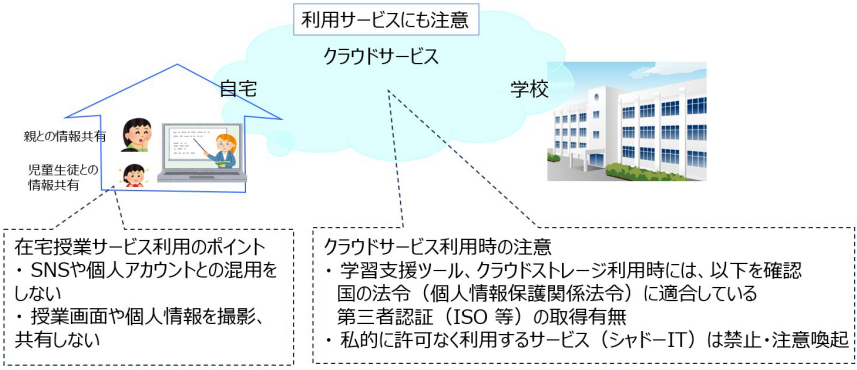
こうした考え方から、例えば保護者の参加確認などは、学校システムと分離された参加確認アプリなどを使うことも一つの方法です。

8 在宅授業での ID 管理

在宅授業・学習は、例外的な対応ではなく、前提として考えることが文部科学省「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７年３月）に示されています。
https://www.mext.go.jp/content/20250325-mxt_jogai01-100003157_1.pdf



児童生徒の活動拡大
＋
サービス利用

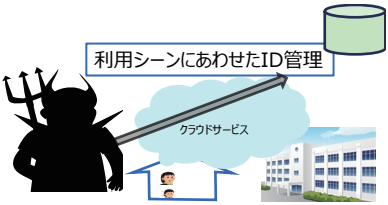


学校外からのアクセスは、インターネット上の悪意にさらされるリスクが高まります。その悪意のある攻撃側が最初の標的とするのが ID 情報になっています。

そのため、成績・個人情報など重要情報（重要性分類 II 以上）へのアクセスでは、多要素認証（MFA）の利用が望まれています。

ただし、児童生徒の場合は、①パスワードの適切管理②誤入力時のロック③十分な複雑性④アクセスできるデータの最小化 を前提に「ID 及びパスワードでの認証」も許容される記載になっています。

なお、在宅利用でも学校内と同じく、利用停止やパスワード変更などの事故対応をあらかじめ用意します。

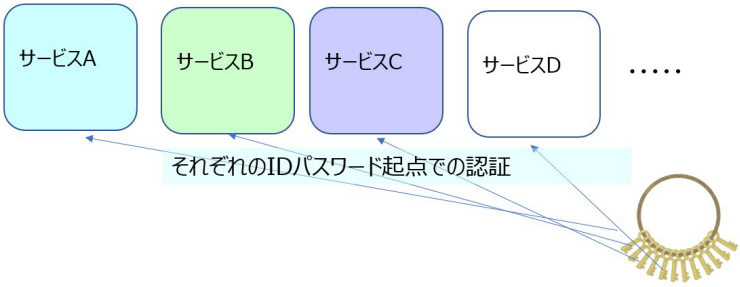


9 生体情報などを使う認証

様々なサービスへのアクセス管理は運用負荷が高い

使う権限にあわせた管理

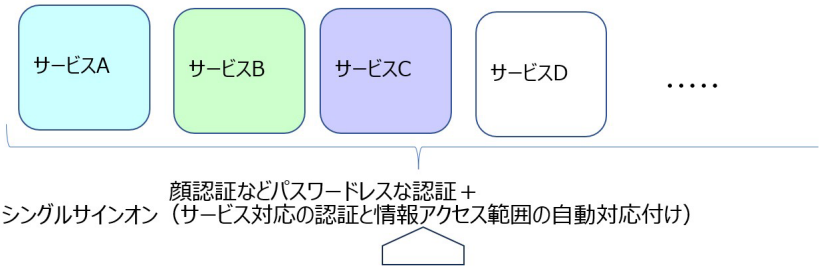
児童生徒に、これに入ると時はこれ、このサービスを使う時の子機は別のこれ‥ は大変



アクセス権管理も重要

見て欲しい範囲とみて欲しくない範囲がある

使う権限にあわせた管理



最近のパソコン、タブレット、スマートフォンは、生体情報認証で認証管理が可能です。
さらに、生体情報を活用し、パスワードを使わないログイン方式（例：パスキー）も可能です。

近年では様々なデバイスで顔認証が利用できるようになっています。これを活用することで多要素認証やパスワードレス認証への道が広がります。

WIndows11での顔認証
＝＞顔認識

iOS(26)での顔認証
＝＞Face ID

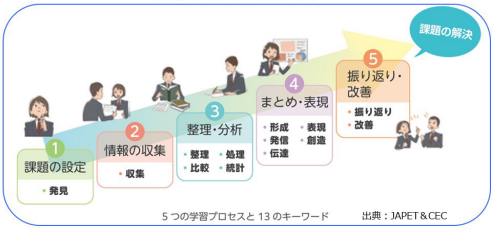
Androidでの顔認証
＝＞顔認証

生体認証を含むパスワードレス認証はゼロトラストの“入口対策”の一部です。認証後も継続的な検証・動的なアクセス制御・多層防御がセキュリティ対策として不可欠となっています。
生体情報も活用した多要素認証で、パスキーと呼ばれるパスワードレス認証によるログイン方式の利用も広がっています。

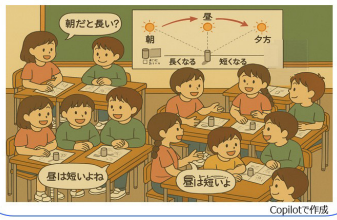
10 各位を伸ばすセキュアなサービス活用

予測困難な時代に対応し、たくましく生きる力を持つ子どもの育成が求められています。
そのためには、主体的に関わり、他者と協働しながら、自らの可能性を発揮できることが重要指針となります。

課題発見、解決力



協働、コンセンサス力



セキュアなICT活用力

セキュアに ICT を使いこなす

「**知識の習得**」の教育から＋「**未来を創る力の育成**」にシフト

セキュアなICT活用力

セキュアな環境で ICT を活用し、「未来を作る力」が伸びて行くことが期待されています。

こうした ICT 利用では、ID/ パスワード管理が利用開始時の重要な要素となっています。この点に関して NIST（米国国立標準技術研究所）はパスワード作成に関する最新のガイドライン「NIST SP 800-63 Digital Identity Guidelines」を示しています。

この 2025 年版ガイドラインでは、「定期的なパスワード変更は不要」と今回の改定前から示されており、さらに「特殊文字や大文字などを混ぜる規定も不要」としています。

ただし、文字数については、多要素認証を利用しない場合は 15 文字以上、多要素認証を利用する場合は 8 文字以上と記載されています。

また、パスワードの定期変更ではなく、侵害事案発生時の速やかな対応を重視しています。アカウント回復のための手段も、ID/ パスワードと同じ知的要素だけとなる登録時の質問 (秘密の質問など) は推奨されず、URL の送信や他のデバイスなどへの通知、回復コードの利用等、多要素となるような工夫が求められています。

このようにセキュリティ認証管理に関する最新動向を踏まえつつ、サービスも最新を調べて、児童生徒がさらに成長できるように工夫して行くことが求められています。

加えて、パスキーなどのパスワードを入力しなくてよい多要素認証の利用も、児童生徒の手間を減らせることから、今後さらに広がっていくことでしょう、

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関して、ID/ パスワード管理でのお役立ち情報を整理してみました。
セキュアな端末を使いつつ、一人一台端末でのツールも使いつつの創造や合意形成を経験していく学びはとても大切です。

ID/ パスワードから、多要素認証で、かつ、米国標準技術研究所（NIST）など海外含むセキュリティ事情の更新を踏まえたセキュリティ活用を、ゼロトラストの考え方の 5 本の柱を ID 管理含めて運用し、そうした取組を通じて、前例のない課題へと立ち向かえる児童生徒が生き生きと将来を担えることを皆さまと共に願っています。

今回の内容は基本的な考え方の整理ですが、インターネットにつないで、学校から自宅までの場所を問わない学びの経験の場の提供への一助となれば幸いです。

最後に、一般社団法人日本教育情報化振興会（JAPET＆CEC）様、モバイルコンピューティング推進コンソーシアム（MCPC）の会員様他、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

本書は、
『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」～』の続編となります。
また、ネットワークの安定稼働に関する情報も各種提供しております。
ネットワークの活用にあたり、確認したい事項がある場合など、ご参考としていただけますと幸いです。

「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」～」（PDF 58.7MB）

学校自治体向け通信技術「無線 LAN 導入後のお役立ち情報」（PDF 11MB）

「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）

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：教育課程企画特別部会における論点整理
https://www.mext.go.jp/b_menu/shingi/chukyo/chukyo3/004/gaiyou/mext_00010.html

文部科学省：総合的な学習（探究）の時間：文科省　小中高の 3 つ掲載
https://www.mext.go.jp/a_menu/shotou/sougou/main14_a2.htm

独立行政法人教職員支援機構：「探究的な学習の過程」の方法論
https://www.nits.go.jp/materials/practical/files/008_001.pdf

文部科学省：次期教育振興基本計画について（答申）（中教審第 241 号）
https://www.mext.go.jp/b_menu/shingi/chukyo/chukyo0/toushin/1412985_00005.htm

Microsoft 社：Bing（Edge）用 Copilot
https://learn.microsoft.com/ja-jp/copilot/edge/

Microsoft 社：Bing AI を使用して知識の世界を活用する | Microsoft Learn
https://learn.microsoft.com/ja-jp/shows/ai-show/ai-show-bing-web-search-api

Microsoft 社：Azure で AI ソリューションを開発するための計画と準備 - Training | Microsoft Learn
https://learn.microsoft.com/ja-jp/training/modules/prepare-azure-ai-development/

Microsoft 社：Microsoft 365 Copilot Chat の概要 | Microsoft Learn
https://learn.microsoft.com/ja-jp/copilot/overview

Microsoft 社：テレワーク・自宅学習 お役立ち情報 - Microsoft atLife
https://www.microsoft.com/ja-jp/atlife/

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）
	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 2026 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 ソリューションを追求し、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。

（2026 年 3 月現在　会員会社数 172 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-20260302.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
～ゼロトラストの基本“ログイン /ID 管理”～
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　2026 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

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/