Microsoft

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４年３月改訂対応 ハンドブック

日本マイクロソフト株式会社

教育情報セキュリティポリシーに関するガイドラインの改訂ポイント（令和４年３月）

令和４年３月に文部科学省の教育情報セキュリティポリシーに関するガイドラインが改訂されました。
改訂の主なポイントは以下のとおりです。

改定ポイント 1

アクセス制御による対策の詳細な技術的対策の追記

アクセス制御による対策を講じたシステム構成を実現するために、校務用端末におけるセキュリティ対策（リスクベース認証、ふるまい検知、マルウェア対策、暗号化、SSO の有効性など）を追記

改定ポイント 2

「ネットワーク分離による対策」「アクセス制御による対策」を明確に記述

アクセス制御による対策を講じた場合
【校務用端末の使い分け】1台の端末で運用可能
【校務用端末の持ち出し】情報セキュリティ管理者の包括的承認による持ち出しを検討可能

詳しくはこちら▼

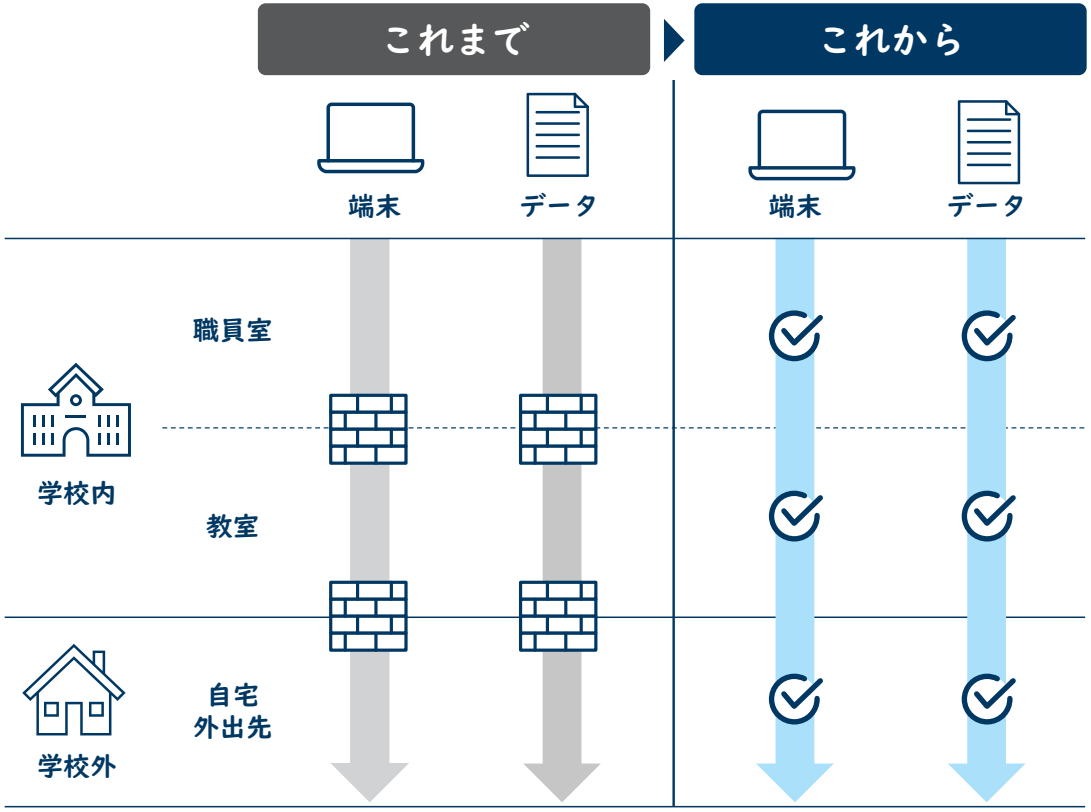
教育情報セキュリティポリシーに関するガイドライン（令和４年３月）改訂説明資料 (mext.go.jp)

本資料では、1で新たに追記された校務用端末のセキュリティ対策について説明します。

これらの対策はすべて Microsoft 365 A5 で実現できます。

アクセス制御によるセキュリティ対策を実施するメリット

「教育情報セキュリティポリシーガイドライン」の改訂に対応した環境では、
従来の境界型のネットワーク分離による利便性の制約から解放されます。
ゼロトラストセキュリティの考え方に基づいて、認証によるアクセス制御を前提とした構成にすれば、
いつでもどこでも安全に端末や情報を利用できるようになります。



校務系・学習系を統合することで、
二重払いコストを削減可能

いつでもどこでも安全に使える
セキュリティ対策で、情報流出を防止

端末２台を行き来する不便さが解消され、
利活用が促進

校務系・学習系のデータ統合により、
深い教育を実現

お客様採用事例

※ Microsoft 365 E5 は政府機関向け、Microsoft 365 A5 は教育機関向けの同等機能製品です

文部科学省 様

文部科学省が、基盤ネットワークシステムの利便性・ 災害耐性の向上、セキュリティ強化を目的に「Microsoft 365 E5」と「Microsoft Azure」を全職員向けに展開

～中央省庁初のフルクラウド化～

文部科学省の全職員が利用する「文部科学省行政情報システム」に、利便性・災害耐性の向上、セキュリティ強化を目的にマイクロソフトのクラウドサービス「Microsoft 365 E5」と「Microsoft Azure」が、2022 年 1 月より稼働。

2017 年 1 月よりオンプレミスで稼働してきた「文部科学省行政情報システム」が更改時期を迎えたことを機に、職員の多様な働き方への対応や、業務効率の改善、非常時に影響を受けにくい耐災害性、セキュリティ強化を図ることを目的として構成を検討。結果、世界中の様々な業種の企業・組織で利用されている実績があることや、業務効率改善からセキュリティの担保まで包括的に実現できる点などが評価され、マイクロソフトのクラウドサービスが導入されました。

Microsoft 365 E5 の導入により、より高いレベルでセキュリティを担保しながら、利便性の向上と情報漏洩対策を実現、Microsoft Azure の導入により、運用管理の一元化による効率化や災害時における事業継続などが可能となります。

詳細はこちらから▶

鴻巣市教育委員会 様

鴻巣市が実現した教育 ICT 大改革

マイクロソフトの
ゼロトラストセキュリティで
先生の働く環境を整えてみたら・・
学校が変わりました

「用途に縛られない PC の活用が実現したことで、情報共有や協議、授業活用などが今まで以上に円滑に行えるようになり、教育の質の向上につながるものだと思います。」

「マイクロソフト ソリューションを包括的に導入することで、利用者が意識せずとも、未知の脅威にも対応した最新のセキュリティ対策が自動で施されている環境が 構築されるのです」

「Azure 上には、統合型校務支援システム、勤怠管理システム、採点支援システム等を構築。Azure を学術情報ネットワーク SINET 直結のクラウド サービスとして利用することで、高品質で安全なクラウド環境が実現されている点も大きな特徴です。

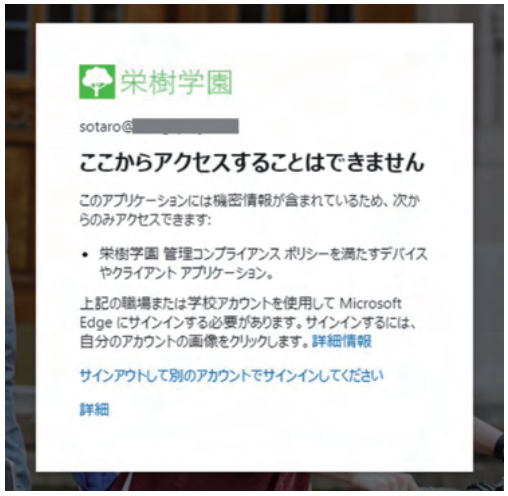
また、ファイル サーバーとして、Teams や OneDrive を活用することにより、IaaS を採用した際にコスト アップの要因となり得るストレージ問題も解決しています。」

詳細はこちらから▶

対策 1

不正アクセスへの対応
[リスクベース認証]

クラウドにアクセスする際の認証（本人確認）にはユーザー名とパスワードを使うのが基本です。
ただし、ユーザー名・パスワードによる認証だけでは、その情報が第三者に漏洩してしまった場合に、なりすましを防ぐことができません。
悪意のある攻撃者が先生や生徒になりすまして、重要な情報を盗み取ったり、一括削除したりすることができてしまいます。
こうした攻撃を防ぐために「リスクベース認証」が役立ちます。これは、本人確認の際、ユーザー名・パスワードが正しくても、
何か「あやしい点」があれば、サインインをブロックしたり、多要素認証を求めたり、または、パスワード変更を求めたりする機能です。
たとえば、いつもと違う時間に、いつもと違う場所から、いつもと違う端末を使ってサインインの要求があった場合、ふだんと違う怪しい行動だと言えます。
また、たとえば、朝９時に日本からサインイン、朝９時半にアメリカからサインインが行われた場合、
同じ人によるサインインだとは考えにくいため、あやしいサインインだと言えます。
こういった「あやしいサインイン」を AI が自動的に見つけることで、セキュリティを高めることができます。
Azure Active Directory Premium P2 が提供するリスクベース認証を採用することでユーザーの利便性損なうことなく、不正アクセスを防止できます。



Session	日付	時刻	ユーザー	端末	アプリケーション	IP アドレス	場所
1	3-Mar	10:05	田中	iPhone 8	Teams	1.2.3.4	Tokyo, Japan
2	3-Mar	15:07	田中	iPhone 8	SharePoint	1.2.3.5	Tokyo, Japan
3	3-Mar	16:45	田中	Windows 10	Teams	2.2.2.1	Tokyo, Japan
4	4-Mar	10:23	田中	Windows 10	Word	2.2.2.1	Tokyo, Japan
5	4-Mar	2:04	田中	Linux	Sway	13.22.12.12	Seattle, US
6	5-Mar	11:30	田中	iPhone 8	Word	1.2.3.4	Tokyo, Japan

悪いように見える

- 田中さん は通常、朝 2 時にログインしない
- 田中さんが普段利用しないデバイス
- 不審な IP アドレス
- 田中さんが今までアメリカからログインした事はない

対策
2

外部攻撃から端末を守る
[ふるまい検知・マルウェア対策]

「アクセス制御による対策を行ったシステム」では、ネットワーク分離をしないため、教員や生徒が使用する端末がインターネットに接続されます。
これまでよりさらに、端末のマルウェア対策が重要になります。
マルウェアによる攻撃手法は巧妙化の一途をたどっており、新種のマルウェアが常に登場しています。
従来型のパターンファイルによる照合ではマルウェアを検出できないケースが増加しています。
このような状況を踏まえると、マルウェアが従来の対策をすり抜け、端末に侵入することを前提とした対策が必要になっていると言えます。
そのため、マルウェアが端末を攻撃する際に特有のふるまい（※）を検出する、ふるまい検知型の対策が必要になります。
（※ OS のセキュリティ設定を書き換える、インターネット上から追加のマルウェアをダウンロードする、など）
従来型とふるまい検知型の対策を併用することで、端末をインターネットに接続して利用する場合であっても、
より安全に利用することができるようになります。
なお、ふるまい検知型の対策では、次々と開発される新しい攻撃手法をどれだけ正確に識別できるかが鍵になります。
Microsoft Defender for Endpoint が提供するふるまい検知機能は、まったく新しい未知のマルウェアにも対応できるセキュリティです。

① 対策の基本

感染しにくい状態にする

OS やアプリケーションを
最新のバージョンに更新

② 従来型の対策

使いまわしウイルスを排除

発見済みウイルス情報に基づき
端末に入り込んだウイルスを排除

指名手配型の対策

③ 現在必要な対策

AI が新しいウイルスを検知

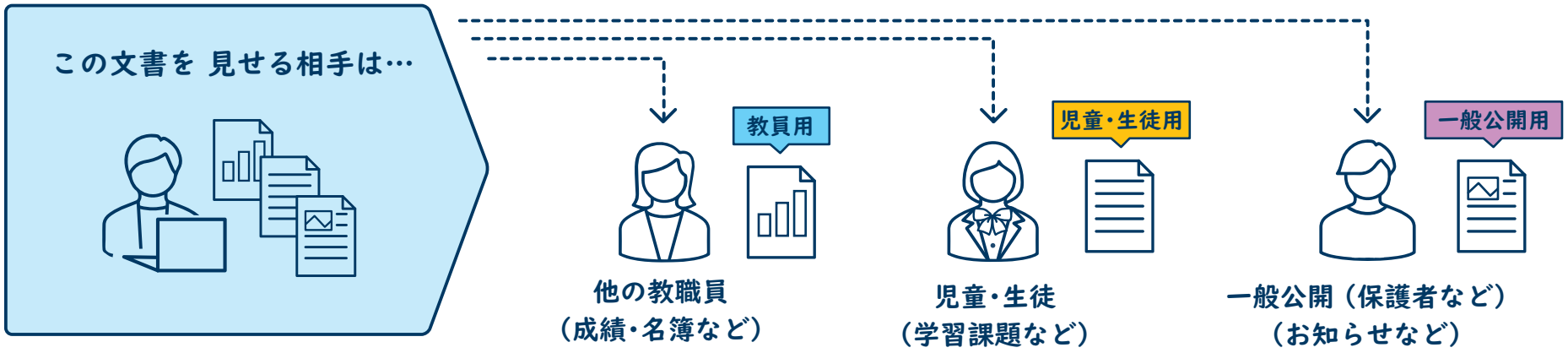
ウイルスによる怪しい動作を
自動で AI が検知し対処


職務質問型の対策

対策
3

情報漏洩対策
[ファイルの暗号化]

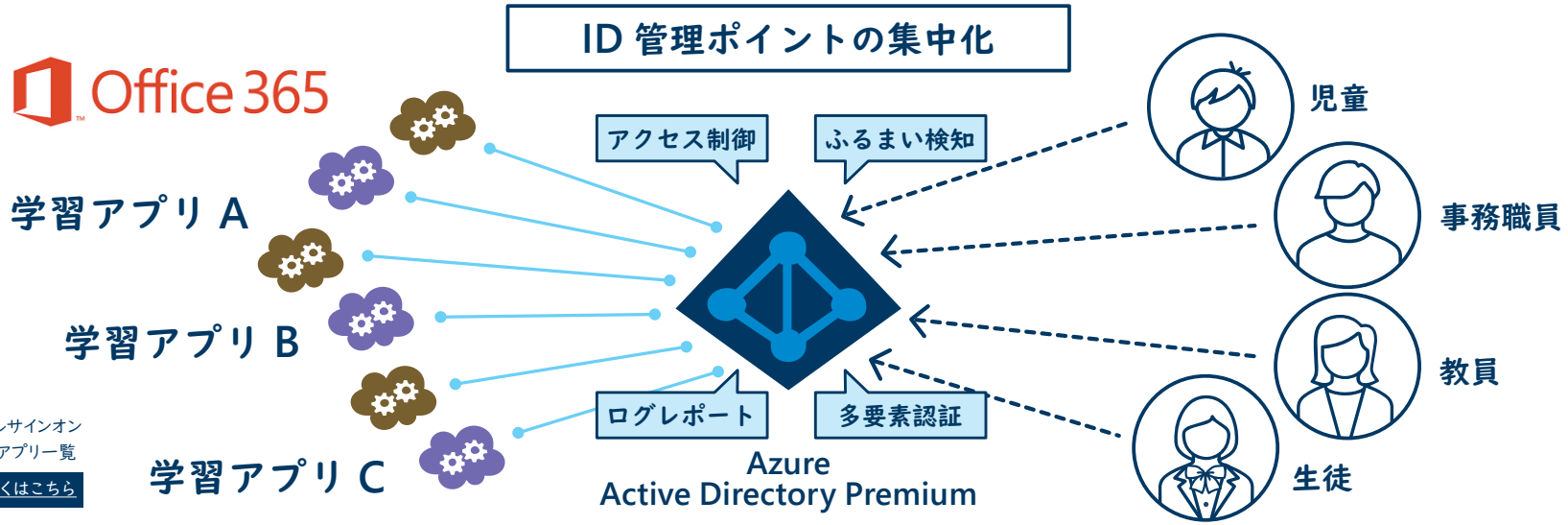
「アクセス制御による対策を行ったシステム」では、教員と生徒が同じネットワークを利用することになります。
学校内では、教員しか閲覧してはいけない資料（たとえば成績や進路に関する情報）を多く扱っており、
生徒がそれらの資料を閲覧できないようにすることが求められます。
そのために暗号化の技術、特に、ユーザー認証に基づいた暗号化の技術を利用することができます。
ユーザー認証に基づいた暗号化の技術を使えば、「教員は開くことができるが、教員以外は開けないように暗号化する」といったことが可能になります。
仮に生徒が開こうとしてもエラーになり、教員だけにとどめておくべき情報が生徒の目に触れることがありません。
また、仮にそのファイルを誤ってメールで外部に送信してしまった場合でも、外部の第三者はそれを開くことができません。
ファイルを保存した USB メモリーを紛失した場合も同様です。
この仕組みを正しく利用することにより、教員と生徒が同じネットワークを利用する環境であっても、
教員だけが知るべき情報が生徒に漏洩してしまうという事故を防ぐことができます。
Microsoft Information Protection を利用すれば、機密情報がどこに保存されていても、どこに移動しても、
それらの情報を検出、分類、保護ができます。
Microsoft Information Protection は意図しない共有を防止し、所有者の許可なく他人に機密情報を渡せないようになっています。



対策
4

利便性高・セキュリティ高
[シングルサインオンの有効性]

教育におけるクラウド サービスの利活用が進むにつれ、教育現場で使われるクラウド サービスの数が増えていくと考えられます。
それに伴い、課題になるのが ID とパスワードの管理です。
教員や児童生徒から見ればサービスに応じて複数の ID とパスワードを使い分けるのは至難の業です。
また、複数のパスワードを記憶するのが面倒なために、安易なパスワードを設定したり、
パスワードを人目につきやすい場所にメモしておいたりといった、セキュリティを低下させる行為につながりがちです。
それを防ぐため、ひとつの ID・ひとつのパスワードで複数のクラウド サービスを利用できるようにするのがシングル サインオン (SSO) です。
これにより、教員や生徒は一つのパスワードだけを覚えればよくなります。
この仕組みのもう一つの利点は、ユーザー認証（本人確認）を一箇所で行うようになるため、
そこに強固なセキュリティ対策（多要素認証やリスクベース認証）を施すことで SSO 対象のすべてのクラウド サービスの
セキュリティを向上させることができる点です。さらに、教員の退職や他県等への異動、生徒の卒業の際に、一箇所で ID を無効化するだけで、
SSO 対象のクラウド サービスすべてがその ID では利用できなくなる点も重要です。



シングルサインオン
対応のアプリ一覧
◀詳しくはこちら

Microsoft 365 A5 のメリット

改訂により重視されるようになった機能も含め、

ガイドラインに沿った構成を実現するための製品をセットで提供します

費用面

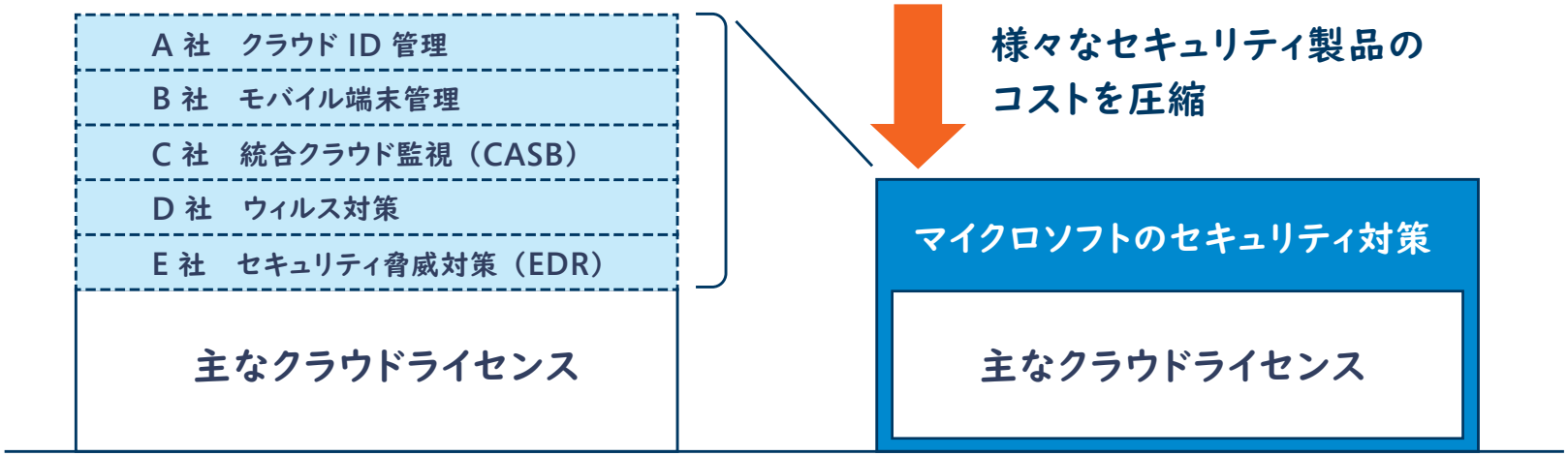
セット価格だから、
積みあがるセキュリティ製品コストを
圧縮可能

管理・運用面

管理・サポート窓口がすべて一元化でき、
シンプルな設計になるので
効率的

セキュリティ面

各機能が連携して動くことで、
業界トップレベルの
セキュリティ対策を実現



Microsoft 365 A5 でご利用いただける機能

機能	説明	これらの対策はすべて Microsoft 365 A5 に含まれる 以下の製品 / 機能で実現できます。 製品名
リスクベース認証	「あやしいサインイン」を自動的に検出し、サインインをブロックする、 多要素認証を要求する、パスワード変更を要求するなどの対処を行う	・Azure Active Directory Plan 2
ふるまい検知・端末のマルウェア対策	端末が未知のマルウェアに感染しても、マルウェアが端末を攻撃しようとする 振る舞いを検出し、駆除・復旧の処理を行う	・Microsoft Defender for Endpoint
ファイルの暗号化	情報資産を分類し、各ファイルを閲覧すべきユーザーだけがそのファイルを 開けるようにする（教員専用のファイルを児童・生徒が開けないようにする、など）	・Azure Information Protection Plan 1
シングル サインオン（SSO）	一回のユーザー認証で複数のクラウド サービスを利用できるようにする	・Azure Active Directory Plan 1
なりすましや不正アクセスの防止	ユーザー名・パスワード以外の手段で本人確認を強化したり（多要素認証）、 想定しない場所や端末からの利用をブロックしたりする（条件付きアクセス）	・Azure Active Directory Plan 1
端末管理	端末に一括して設定を適用したり、アプリを配信したりする	・Azure Active Directory Plan 1
クラウドからの情報流出防止	クラウド サービスを経由して外部に機密情報が漏洩することを防ぐ	・Microsoft Defender for Cloud Apps ・Insider Risk Management ・Office 365 Data Loss Prevention ・Endpoint Data Loss Prevention ・Communication Data Loss Prevention
端末からの情報流出防止	端末の紛失・盗難などの際に外部に機密情報が漏洩することを防ぐ、 また、操作ミスや意図的な操作により端末から機密情報を外部に流出させる行為を防ぐ	・BitLocker ・Microsoft Intune ・Endpoint Data Loss Prevention
メール経由のマルウェア対策・ フィッシング対策	メールの添付ファイルに対するサンドボックス型のマルウェア対策および メール本文や Office 文書に記載されている URL によるフィッシングの防止	・Exchange Online ・Microsoft Defender for Office 365

Microsoft

お客様事例　続々公開中！

先生が働きやすい環境を整えてみたら…
詳しくはこちら >>>

教員たちで実現した学校 ICT 革命
データを統合して真の探究的な学びの環境を構築
詳しくはこちら >>>

鴻巣市が実現した教育 ICT 環境大変革の軌跡
詳しくはこちら >>>

文部科学省が基盤ネットワークシステムの利便性および
災害耐性の向上、セキュリティ強化を目的として、
「Microsoft 365 E5」と「Microsoft Azure」を全職員向けに展開
詳しくはこちら >>>

関連記事

［ICT 教育ニュース掲載］
元教員とひも解く ～「文科省のガイドライン改定」で
大幅に変わる ICT 環境の姿とは？
詳しくはこちら >>>

［ICT 教育ニュース掲載］
GIGA スクールあるある「先生！パソコンが遅くて
調べものが進みません」にどう対処すればいい？
詳しくはこちら >>>

教育機関ご担当者様向け GIGA スクールお問い合わせ窓口

0120-933-308

受付時間：9:00-17:30 月曜日～金曜日（祝祭日、年末年始、マイクロソフト休業日を除く）

詳しくはこちら >>>

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