高等学校等における多様なICT端末の活用に関する導入・運用・活用に関するパンフレット

令和4年度　文部科学省委託
学校ネットワークの今後の在り方に関する実証研究
（高等学校における多様なICT端末の活用に関する実証研究事業）

兵庫県教育委員会

文部科学省

はじめに

(1) 現状と背景

現在、小学校や中学校等の義務教育段階の学校においては、GIGAスクール構想により1人1台端末や校内ネットワーク環境の整備が行われ、日常的なICT端末の活用による新たな学びの実現に向けた取組が進められています。

こうした中、高等学校においても、1人1台端末の環境を整備し、引き続き新たな学びを止めないことは、「誰一人取り残されない」デジタル社会の実現のためにも重要になっています。

高等学校の1人1台端末の整備は、各都道府県等において進められていますが、その整備方法は様々です。その中で、生徒が所有するICT端末を活用するBYOD（Bring Your Own Device）については、学校での多様なICT端末の活用における有効な選択肢の一つになり得るものと考えられます。

公立学校の教育現場においては、これまでICT端末は公費において同一機種を整備するのが通例であったため、それを支えるネットワーク環境の構成やセキュリティ対策についても、ICT端末が異なっても同じ考え方を適用することが可能でした。しかし、BYODの導入により一つの学校に多様なICT端末が混在し、同時に利用する環境が急速に進展する中で、それを支えるネットワーク環境の構成やセキュリティ対策については、ノウハウが蓄積されていない状況にあります。また、BYOD端末を活用する学習環境においては、同一端末で揃えられた学習環境では想定しえない課題に直面することも想定する必要があります。

(2) 実証研究の概要

本実証研究は、上述した背景に鑑み、高等学校におけるBYOD端末の活用を念頭においたネットワークやセキュリティ等の環境整備に関わる課題と、BYOD端末の活用が学習活動に与える影響等を評価・検証することを目的に、兵庫県教育委員会を実証地域として、「多様なICT端末を校内ネットワークで、安定的かつ安全に利用するための環境整備」と「多様なICT端末を学校で使用する場合における指導面・学習面の留意点」の2点について検証を進めました。 また、高等学校の生徒が1人1台端末を活用する際のポイントについても整理し、ガイドブックを作成しました。ガイドブックでは、以下の5章に分けて解説しています。本パンフレットは、その導入としてお使い頂くことを想定しています。

第1章　多様なICT端末の活用に向けた動きについて考察しました。
第2章　多様なICT端末環境におけるネットワーク構成についてポイントを整理しました。
第3章　多様なICT端末環境におけるセキュリティ対策についてポイントを整理しました。
第4章　多様なICT端末環境における指導上のトラブル対応についてポイントを整理しました。
第5章　多様なICT端末を活用した学びの充実についてポイントを整理しました。

(3) 実証校の概要

ICT端末の活用方法や活用場面は、学科・コースや学習内容、進路によって異なります。また、最適なネットワーク環境や端末利用に伴って生じるトラブル等は、学校規模や立地場所によって異なることも予想されます。そこで、今回の実証研究を進めるにあたっては、学校規模や学科、立地場所などが異なる3校を実証校としました。

学校名	学科	学級数	立地	BYOD端末	ICT整備
長田高校	普通科	24クラス	都市部	321台	【校内LAN】 ・全教室配線済 （Cat6a又はCat5e） 【無線LAN】 ・全普通・特別教室に整備 （5Ghz、2.4Ghz） 【大型提示装置】 ・全普通教室に整備
有馬高校	人と自然科 総合学科	18クラス	都市近郊	237台	
播磨農業高校	農業経営科 園芸科 畜産科	9クラス	中山間部	106台	

（注）上記の表は令和4年度現在の状況である。

(4) 端末の定義

本ガイドブックに記載のある端末名称の定義は以下のとおりとする。

名称	説明
BYOD端末	家庭で費用を負担し、購入された端末
1人1台端末	BYOD端末や公費整備による学習者用端末
学習者用端末	1人1台端末を含む各校に配備された教育用コンピュータ

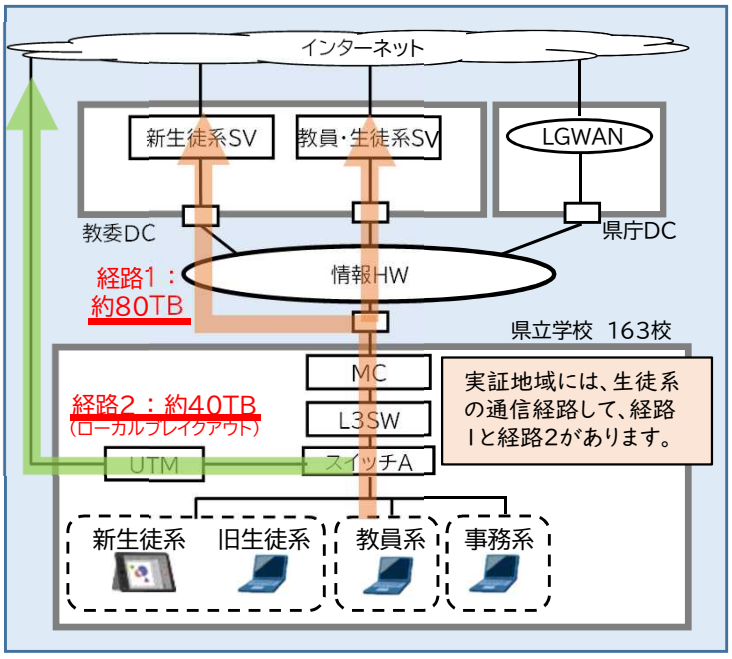
多様なICT端末環境におけるネットワーク構成

1 BYODの導入とローカルブレイクアウト※1

BYODの導入により、校内で使用する端末台数が増えるだけではなく、1人1人が端末を常時使用することとなるため、通信量は大きく増えます。そのため、兵庫県はこれまで、県立学校で使用する全ての生徒系、教員系の通信を、教育委員会のデータセンターに集約してインターネットに接続する構成（集約回線）でしたが、BYOD導入前において通信量の多かったソフトウェアを、集約回線から外部光回線へローカルブレイクアウト（図1-1緑）しました。OSのアップデートなど特定のサービスや宛先向けのトラフィックについては、ローカルブレイクアウトすることで、生徒系の通信だけでなく、教員系の通信についても安定化を図ることが期待できます。

兵庫県では、約3分の1の通信量をローカルブレイクアウトさせましたが、特に、OSのアップデートにかかる通信量は非常に多いため、ローカルブレイクアウトすることを推奨します。 また、教育用クラウドサービス※2の通信にも、セッション数※3が多いものがあります。そのため、クラウドサービスもローカルブレイクアウトすることで、授業中安定して利用することが期待できます。

図1－1　実証地域（兵庫県）のネットワーク構成図



2 BYODの導入に伴う通信量の変化

BYODの導入の前後で、どの程度通信量が増えるのか、各学校でアセスメントを実施するなどしてネットワークの現状を把握することが大切です。

高等学校では、学科やコースによって、BYOD端末の活用内容もそれぞれに異なります。それに応じて、通信量の増え方も異なっていることが伺えました。

ポイント①

標準的な学習ツールとして利用が多い教育用クラウドサービスの通信は、比較的セッション数が多いことから、積極的にローカルブレイクアウトを検討しましょう。

BYOD導入によって増える通信量は、1人1台端末の活用の仕方や内容に影響を受けるため、学校ごとに異なります。そのため、学校ごとに通信トラフィックを調査し、把握することが重要です。

※1 データセンターなどに設けられたインターネットとの接点を使わず、各拠点から直接アクセスするネットワーク構成

※2 教育向けに提供されているオンラインストレージやオンラインサービス。本実証地域では、Microsoft Office 365 for Educationや、Google Workspace for Educationを指す。

※3 端末とサーバー等において、同じタイミングで発生するアクセス開始から終了までの一連の通信数を示す。

3 BYODの導入と集約回線

兵庫県では通信の十分な帯域を確保するために、集約回線に1Gbpsベストエフォート1回線（WAN1）と1Gbps ギャランティ1回線(WAN2)の2回線の契約を行っています。

令和4年度現在、生徒が登校している時間帯では、WAN1は200Mbps～400Mbps程度、WAN2は400Mbps～700Mbps程度の通信量になっています。BYOD初年度では、通信が逼迫していることはありませんが、BYODが年次進行で導入されることにより、今後、通信量が増え、通信が逼迫することが予想されます。

図1－2 実証地域（兵庫県）のネットワーク構成図

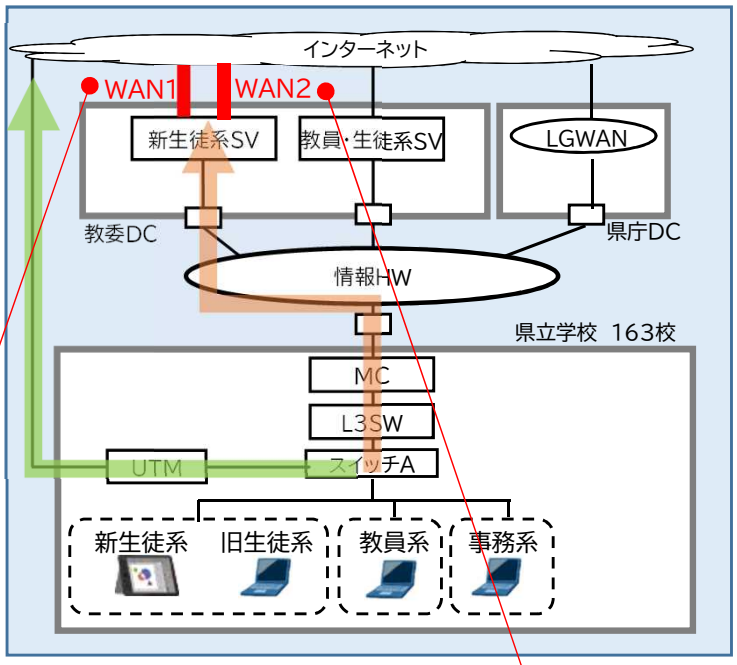
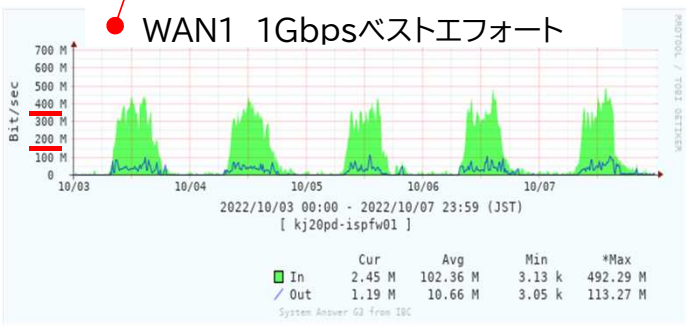
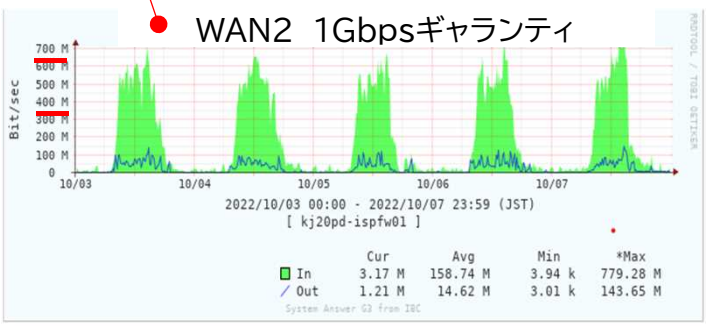


図2 実証地域（兵庫県）の集約回線の通信量





ポイント②

BYODが年次進行で導入されることにより、学習者用端末の台数や通信量が年毎に増えます。その年次変更による変化を見据えたネットワーク構成の設計・見直しが必要です。

4 校内ネットワーク利用時におけるBYOD端末の設定

BYOD端末に固定IPアドレスを設定すると、毎年、新入生の端末の設定変更が必要になるとともに、その端末がWindows端末またはChrome端末の場合は、異なるネットワークに接続する度に設定変更が必要となります。そのため、BYOD端末には動的IPアドレスを払い出すことが有効です。

また、プロキシの適用範囲はOSによって異なります。WindowsOSとChromeOSについては、プロキシを利用する場合は、その切替えが必要になります。BYOD端末は、毎日持ち帰ることから、学校においても、家庭においても、生徒が、毎回端末の設定変更等を行わなくても使用できるよう、プロキシの自動切替え機能を利用することが有効です。

図3 BYOD端末への動的IPアドレス払い出しの例（兵庫県）

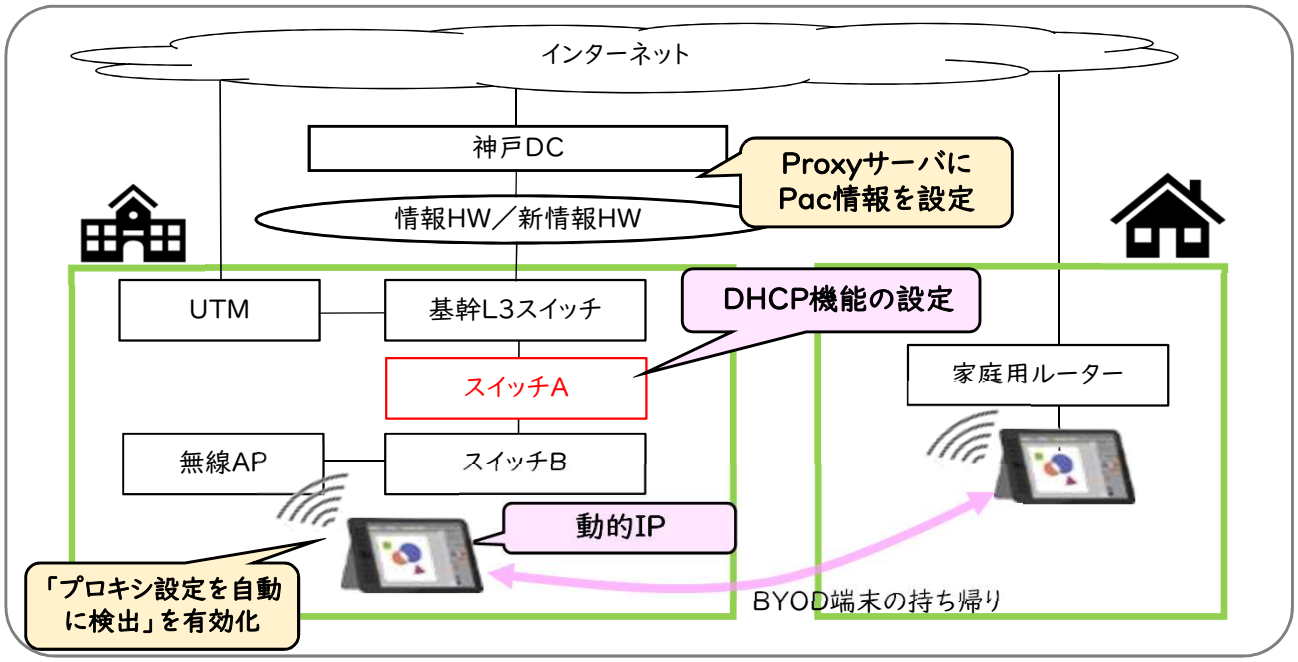


図4 IPアドレスの割当て範囲の例（兵庫県）

第3ｵｸﾃｯﾄﾞ	152	153	154	155	156	157	158	159
	固定	固定	DHCP	DHCP	DHCP	DHCP	固定	固定

公費整備端末や周辺機器が利用するレンジ　BYOD端末が利用するレンジ　公費整備端末や周辺機器が利用するレンジ

表1 プロキシの適用範囲

OS	プロキシ設定
Windows OS	OS全体にプロキシ設定が適用される
iPad OS	SSID毎にプロキシを設定する
Chrome OS	①OS全体にプロキシ設定が適用される ②Chromeのみプロキシ設定を適用する

ポイント③

BYOD端末のIPアドレスを動的に払い出すことで、IPアドレスを節約できますが、BYODが年次進行で導入されることに合わせて、払い出し状況を把握し、IPアドレスが枯渇しないよう留意する必要があります。

また、WindowsOSやChromeOSが混在する場合は、プロキシ設定の自動検出を有効化することで、学校や家庭で端末の設定変更することなく使用することが可能です。

Ⅰ 実証研究におけるセキュリティ対策

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（令和4年3月版）（以下、「ガイドライン」という。）」に例示されたセキュリティ対策に対応するため「検疫システム」及び「認証システム」「MDMによる一元管理」を導入し、本実証研究を行いました。

■ 検疫システムの導入

検疫システムとは、ウイルス対策ソフトのインストール及び最新のパターンファイル適用、OSやソフトウェアの最新バージョンアップデートなどが適切に実行されているかを検査し、安全なBYOD端末のみを校内ネットワーク接続させるよう、端末の検疫を行う仕組です。検疫システムの機能は以下表2のとおりです。しかしながら、これらの機能を全部満たすことは技術的、費用的にも困難であることから、本実証研究では検疫システムの機能のうち、検査のみを実施する検疫システムを導入しました。

また、様々な種類の脅威からBYOD端末を守るため、通過するパケットを解析することで、さらに安全性の向上を図りました。

表2 検疫システムの機能

機 能	内 容
検 査	接続する機器を検疫システムへ誘導し、マルウェアの感染、ウイルス対策ソフトの導入、OS更新状況を検査する。
隔 離	検査された機器を検疫用のネットワークに分離し、内部ネットワークと分離する。
治 療	特定された問題に対処し、必要に応じてウイルスやマルウェアの削除を行う。
再検査	修正された機器を再検査して、問題が解決された場合は、内部ネットワークに接続させる。

■ 認証システムの導入

認証システムとは、校内の情報資産を守るため、校内ネットワークを利用できる人物や端末、利用者権限を明確に範囲を限定し、接続を許可する仕組です。認証方法には、ID/PASS認証、証明書認証、MACアドレス認証の大きく3つの認証方法があります。本実証研究では、導入の容易さと生徒の利便性及び各校の管理者の負荷を考え、「ID/PASS認証」を実施しました。

■ MDM（モバイルデバイスマネジメント）による一元管理

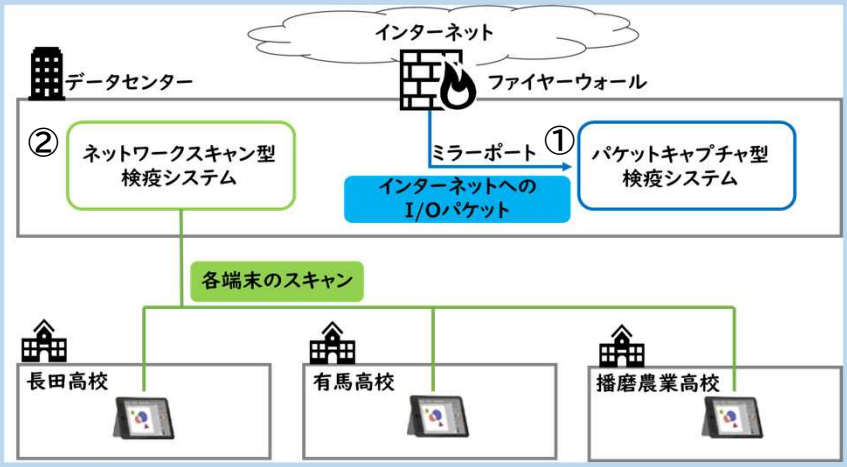
MDM（モバイルデバイスマネジメント）とは、学校におけるBYOD端末をはじめとしたモバイル端末のシステム設定などを、統合的・効率的に管理する手法、またそれを実現するソフトウェアや情報システムなどの仕組のことです。

ガイドラインでは、端末のセキュリティ設定やOSやソフトウェアのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましいため、MDM等によりセキュリティ制御を行うことが推奨されていることから、本実証研究でもMDMを用いて、多様な端末のセキュリティ対策状況を維持しました。

2 検疫システムの導入

本実証研究では、経費面の問題を解決するために、オープンソースを利用して、教育情報ネットワークに接続するBYOD端末のOSバージョン、ウイルスパターンファイル、インストールされたソフトウェアを接続時に検疫し、ソフトウェアによる脆弱性の防止を図るシステムについて、①パケットキャプチャ型及び②ネットワークスキャン型を導入しました。

図5 実証した検疫システムの概要図



① パケットキャプチャ型検疫システム

パケットキャプチャ型検疫システムとは、通信ネットワークや回線を流れるデータを捕獲（capture）して、危険度の解析や集計などを行う検疫システムです。

実証校における検知調査の結果、検出数は少ないものの、「暗号化されていない状態でインターネットに対するパスワード情報のやりとり」といった危険度の高い通信が検知されました。また、「フィッシングサイト等の不正・危険なサイトへのアクセス」も多く検知されており、教育現場において大きなリスクがある通信が多いことが明らかになりました。

ポイント④

日々の通信には、平文（暗号化されていない状態のデータ）でパスワード情報をやりとりなど危険度の高い通信や、不正・危険なサイトへのアクセスが一定数発生することを想定し、全てのパケットを検査するパケットキャプチャ型の検疫が有効です。

② ネットワークスキャン型検疫システム

ネットワークスキャン型検疫システムとは、ネットワークに接続した検疫用端末とBYOD端末をWi-Fi通信で接続した上で、BYOD端末の検査を１台ずつ実行する仕組のものです。

なお、本実証研究では、端末の安全性を確認するため、生徒自身が検疫端末を操作して行う想定で、生徒が一人ずつ順番に検疫を行いました。また、BYOD端末の検査までを行うものとし、問題がある端末を隔離したり治療したりすることは行なっていません。検査の結果異常のあった端末は所有者である生徒自身がOSのバージョンアップやファイヤーウォールの設定等の対応を行いました。

ポイント⑤

学校ネットワークに接続するBYOD端末の中には、脆弱性がある場合が想定されるため、校内ネットワークに接続を試みる全ての端末を検査するためのネットワークスキャン型検疫システムを導入することが有効です。

3 認証システムの導入

① 認証方式

認証システムを導入する際には、認証方式を検討する必要があります。認証方式には、主に以下表の3つがあり、セキュリティ強度や運用管理のしやすさを基に検討することになります。

MACアドレス認証は、導入が容易ですが、MACアドレスが毎回ランダムに発行されるOSもあるため、BYODを導入する際には、注意が必要です。兵庫県では、ID/PASS認証を採用しました。

	証明書認証 (EAP-TLS)	ID/PASS認証 (EAP-PEAP)	MACアドレス認証
セキュリティ強度	◎	○	△
運用管理のしやすさ	△	○	△
メリット	・証明書をインストールされた端末のみアクセス可能なため、セキュリティ強度が高い。	・証明書発行管理が不要である（ユーザー管理が軽い）。 ・年度毎のユーザーの棚卸しが容易である。 ・現状NW設定の変更が少ない。	・ユーザーの認証負担が軽い(ID/PASS入力不要)。 ・現行のNW設定の変更が少ない。
デメリット	・証明書を配布する必要がある（配布用SSID、VLANの作成、メールによる配布等）。 ・証明書管理が必要である。 ・人の認証が出来ない。	・ID/PASSを知っていればどの端末からでもアクセス可能になる。	・MACアドレスは偽装することが可能である。 ・iOS/Androidデバイス等ではMACアドレスが可変する。 ・MACアドレスの収集・削除が必要である。

② 認証装置の設置場所

認証システムを設置する場所は、主に以下表の3つが想定され、運用管理のしやすさや障害への耐性、導入コストのバランスから検討する必要があります。兵庫県では、プライベートクラウド型（集中管理型）を採用しました。

	パブリッククラウド型	プライベートクラウド型 （集中管理型）	オンプレミス型 （学校設置型）
運用管理のしやすさ	◎	○	△
耐障害性	○	○	△
セキュリティ	△	○	○
メリット	・遠隔による対応が可能である。 ・ユーザー数の拡張が容易である。	・遠隔による対応が可能である。 ・外部からのアクセスできない。	・外部からアクセスされにくい。 ・校内回線切断時にも認証可能である。
デメリット	・外部からアクセス可能である。 ・個人情報をクラウド保存できる。 ・校内回線切断時には認証できない。	・製品により筐体毎に管理台数に上限がある。 ・学校回線切断時には認証できない。	・各学校に設置するため、経費がかかる。 ・冗長構成には機器を増やす必要がある。

ポイント⑥

多様な端末が混在するBYODでは、MACアドレスが可変する端末が存在することから、MACアドレス認証では対応できない端末も存在するため、証明書認証、もしくはID・パスワード認証が有効です。

4　MDM（モバイルデバイスマネジメント）による一元管理

前述したようにガイドラインでは、端末のセキュリティ設定をはじめ、OSやソフトウェアのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましいため、MDM（モバイルデバイスマネジメント）等によりセキュリティ制御を行うことが推奨されています。

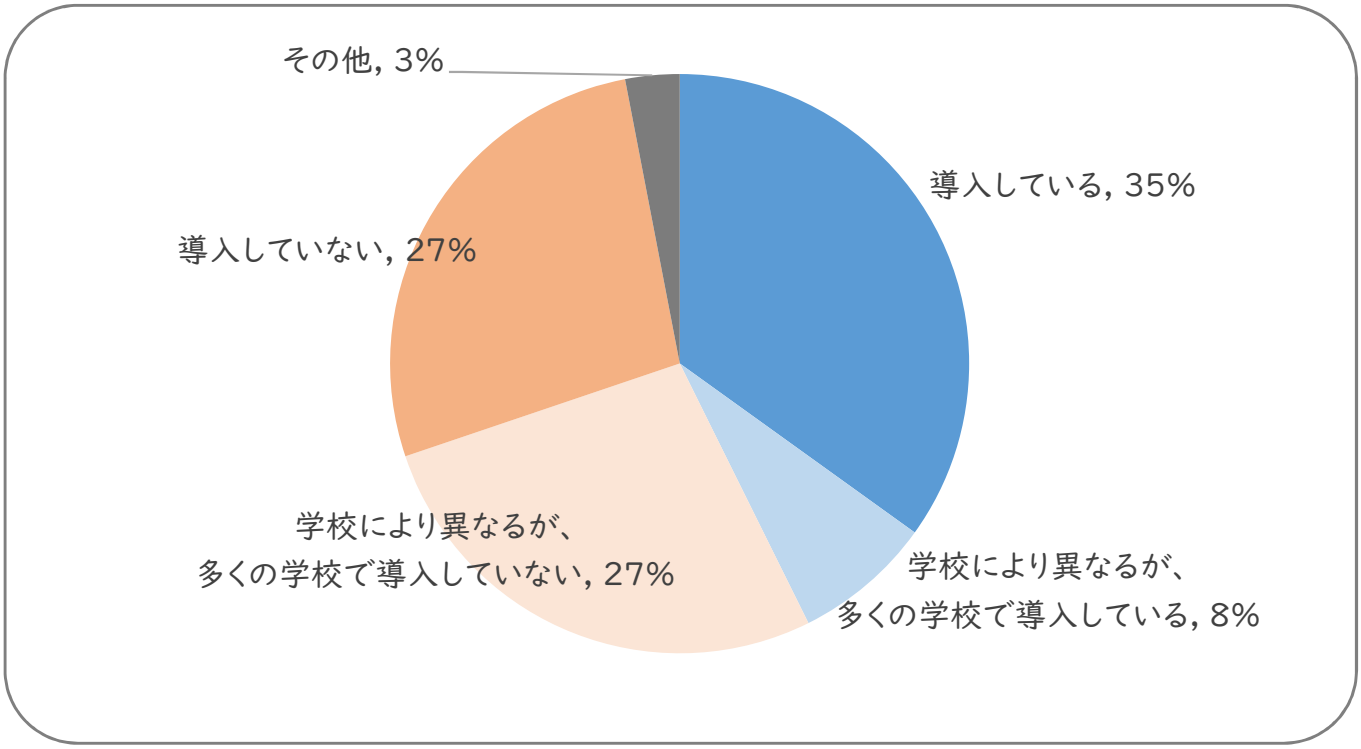
MDMにより見込めるセキュリティ面での効果は、主に以下のとおりです。

〇標準的なセキュリティ対策ソフトの設定を、一律に保つことができ、脆弱な端末を減らすことができます。（例）リアルタイム監視や、メールのスキャン、マルウェアのスキャン　等

〇端末の紛失・盗難時に、遠隔操作でロックやワイプ（消去）することで第三者による不正操作や情報漏洩を防ぐことができます。

図6　保護者負担の端末におけるMDM導入状況（令和5年2月）

調査対象：BYODを実施している都道府県・政令指定都市教育委員会（n=32）



ポイント⑦

全ての生徒に自身のBYOD端末のセキュリティ対策を適切に行わせるのは難しく、かつ、その指導も難しいことから、MDM等によって、多様な端末のセキュリティ対策状況を維持することが有効です。

第4章 多様なICT端末環境における指導上のトラブル対応

1 生徒が経験したBYOD端末に関するトラブル

本章では実証研究において、BYOD端末を使用する中で、実際に経験したトラブルに基づく、対応方策をまとめました。

生徒が経験したBYOD端末に関するトラブル（「よくある」及び「時々ある」と回答した生徒の割合）では、毎日持ち帰るため家庭で充電することを忘れた(70.8%)、又は、充電が不十分なために学校で端末を使用できなかった（47.7%）という経験を持つ生徒が多くいました。

また、ログイン時やアプリケーション起動時に、非常に時間がかかった（50.9%）経験を持つ生徒も多くいました。実証校の通信トラフィックを調べると、慢性的に帯域不足が生じているということはありませんでした。教員の指示の下、一斉に起動、一斉にアクセスという使用により、一時的に通信トラフィックが急増しバーストトラフィック※4していることも一因として考えられます。

ポイント⑧

教育DXを見据え、学習ツールとしてのBYOD端末を、教員主導ではなく、生徒自身が自由に使いこなすことで、生徒主体のICT活用を進めることができます。

2 教員が不安に感じるBYOD端末に関するトラブル

教員が心配するトラブルとして多い（「よくする」と回答した教員の割合）のは、生徒のID・パスワード忘れ（53.2%）や、通信回線の帯域不足ネットトラブル等による授業の停滞（41.9%）があります。教育用クラウドサービスのアカウントや、学習支援アプリのアカウントなど、個々の生徒に配布するアカウントの種類や量が増えると、生徒の管理が複雑になります。シングルサインオン※5の利用など、ユーザー認証の仕組みを工夫し、生徒が使いやすい環境とすることが重要になります。

ポイント⑨

生徒に配布するアカウントの種類と量が増えると、生徒がID・パスワードを忘れるトラブルが起きやすくなるため、シングルサインオンの活用など、ユーザー認証の仕組みを工夫しましょう。

3 トラブルを未然に防止するための知識・技能

BYOD端末は「私物」であることから、日々の管理は生徒自身が行います。管理が不十分な場合は、トラブルに直結します。

アンケート（「できる」及び「ある程度はできる」と回答した生徒の割合）によると、BYOD端末をWi-Fiに接続（88.5%）したり、アプリをインストール・アンインストールしたりする（82.6%）ことは、多くの生徒が自分でできるようです。

また、教員アンケートでは多くの教員が心配している「生徒のID・パスワードの管理」についても、多くの生徒が、適切に管理している（81.4%）と回答しています。

一方、BYOD端末のウイルス対策アプリが最新であるかを確認することができる生徒は少なく（39.2%）、情報活用の実践力として、生徒が自身のBYOD端末を管理する知識や技能を高めていくことが大切です。

ポイント⑩

ウイルス対策ソフトやOSが更新されていないBYOD端末が多く存在する可能性があります。危険性のある端末を検知し、隔離・治療する検疫システムが有効です。

※4 バーストトラフィックとは、ある通信回線やネットワークなどに、一時的に大量のデータが流れること。
※5 シングルサインオンとは、1度のユーザー認証によって複数のアプリケーションやクラウドサービスなどの利用が可能になる仕組

多様なICT端末を活用した学びの充実

1 BYOD端末を用いた学習活動の実際

BYOD端末をどのように活用しているか、実証校の生徒にアンケート調査をしました。
普段のICT端末の活用の場面（「よくする」及び「時々する」と回答した生徒の割合）で多かったのは、「ウェブブラウザを使って、インターネット検索する（93.3%）」でした。「オンラインで課題を提出する（81.4%）」や、「アンケートに回答する（61.2%）」など、オンラインでの学習支援での活用も増えています。
一方で、「学校外の自分の勉強に利用する（43.2%）」「文書作成アプリ等を使って、授業内容をメモする（14.2%）」は低率であることから、生徒自身が日常的にツールとして端末を使用できるように、学習活動における指導上の工夫や改善が求められます。

ポイント⑪

教師の指示に基づいて使用するだけではなく、授業において生徒自身がBYOD端末を日常的に学習ツールとして使用できるようにすることが重要です。

2 BYOD端末を用いた学習への具体的な活用

BYOD端末の活用に取り組む実証校の教員に、どのような学習にBYOD端末は役立つかを尋ねました。
BYOD端末が役立つと回答した割合（「そう思う」及び「ややそう思う」と回答した教員の割合）が多かったのは、インターネットを用いた情報収集（88.7%）や、写真・音声・動画を用いた資料作成（88.7%）、家庭でのオンライン学習（87.0%）でした。
一方、資料や作品を協働で制作すること（80.6%）や、協働して意見を整理すること（72.5%）は、それらに比べると低い結果となりました。
協働での意見整理や協働制作などの協働的な学びについては、生徒が個々に取り組む調べ学習や資料作成などの学習活動に比べて、BYOD端末を活用した取組が遅れていると考えられます。
教育用クラウドサービスはそのような取組を行うのに有効な上、端末のOS等に依存せずブラウザ上で利用できるため、導入しやすいアプリケーションです。教育用クラウドサービスのアカウントを全生徒・全教員に付与することで、他者との情報共有など容易にできます。1人1台端末環境下において協働的な学びを実現するため、積極的に利用することが求められます。

ポイント⑫

教育用クラウドサービスのアカウントを全生徒・全教員に付与することで、コミュニケーション環境を容易に構築することができます。
また、クラウドサービス内のワープロや表計算などのいわゆるOfficeアプリと、コミュニケーションアプリやオンライン会議アプリを組み合わせることで、他者との情報共有や協働での意見整理などが容易に行えるため、協働的な学びが円滑に実施できます。

3 BYOD端末の活用スキルとICTの活用姿勢との関連

「ICT端末を活用することは得意であるか」という項目と、「授業でICTを使うことは必要か」及び「学校・家・塾で勉強するのにICTは役立つか」という項目のクロス集計結果を見ると、ICT端末の活用が得意な生徒の方が、苦手な生徒よりも、ICTを授業や自身の勉強に活用する意欲が高いことがわかります。
ICT端末の活用を支える基本的な知識や技能としての情報活用能力を育成できるよう、あらゆる教科等においてICT端末の活用に取り組むことが重要です。

ポイント⑬

ICT端末の積極的な活用姿勢と、端末活用スキルには関係性があると考えられます。
情報活用能力の実践力として、基本的な端末活用スキルを高めるための手立てを考える必要があります。

まとめ　多様なICT端末を校内ネットワークで、安定的かつ安全に利用するための環境整備

第2章　多様なICT端末環境におけるネットワーク構成

- 標準的な学習ツールとして利用が多い教育用クラウドサービスの通信は、比較的セッション数が多いことから、積極的にローカルブレイクアウトを検討する必要がある。（ポイント①）
- 高等学校は、学科等により学習者用端末を用いた学習活動の内容が大きく異なるので、BYOD導入による通信量の増加幅は、学校毎に異なる。そのため、学校毎に通信トラフィックを調査し、適切に把握することが必要となる。（ポイント①）
- BYODの年次進行での導入により、学習者用端末の台数や通信量が年毎に増える。その変化を見据えたネットワーク構成の設計・見直しが必要となる。（ポイント②）
- BYOD端末のIPアドレスを動的に払い出すことで、IPアドレスを節約できるが、BYODの年次進行に合わせて、払い出し状況を把握し、IPアドレスが枯渇しないよう留意する必要がある。（ポイント③）
- WindowsOSやChromeOSが混在する場合は、プロキシ設定の自動検出を有効化することで、学校や家庭で端末の設定変更することなく利用することが可能となる。（ポイント③）

第3章　多様なICT端末環境におけるセキュリティ対策

- 日々の通信には、パスワードの平文通信などの危険度の高い通信や、不正・危険なサイトへのアクセスが一定数発生することを想定し、全てのパケットを検査するパケットキャプチャ型の検疫が有効である。（ポイント④）
- 学校ネットワークに接続するBYOD端末の中には、脆弱性がある場合が想定されるため、校内ネットワークに接続を試みる全ての端末を検査するためのネットワークスキャン型の検疫が有効である。（ポイント⑤）
- 多様な端末が混在する場合は、MACアドレス認証では対応できない端末も存在するため、証明書認証、もしくはID・パスワード認証が有効である。（ポイント⑥）
- 全ての生徒に自身のBYOD端末のセキュリティ対策を適切に行わせるのは難しく、かつ、多様な端末がある場合は、その指導も難しい。MDM等によって、多様な端末のセキュリティ対策状況を維持することが有効な手立てである。（ポイント⑦）

まとめ　多様なICT端末を学校で使用する場合における指導面・学習面の留意点

第4章　多様なICT端末環境における指導上のトラブル対応

- 教育DXを見据え、学習ツールとしてのBYOD端末を、教員主導ではなく、生徒自身が自由に端末を使用できるようにし、生徒主体のICT活用を進めることが重要である。（ポイント⑧）
- 生徒に配布するアカウントの種類や量が増えると、生徒がID・パスワードを覚えきれず、授業中に円滑にBYOD端末を使用できなくなるといったトラブルが起きやすくなる。シングルサインオンの利用など、ユーザー認証の仕組みを工夫することが重要である。（ポイント⑨）
- BYOD端末は、生徒自身が端末を管理するため、ウイルス対策ソフトやOSが適切に更新されていない端末が一定数存在することが予想される。端末の管理方法に関する指導とともに、危険性のある端末を検知し、隔離・治療する検疫システムの導入が有効である。（ポイント⑩）

第5章　多様なICT端末を活用した学びの充実

- 教師の指示に基づいて使用するだけではなく、授業において生徒自身がBYOD端末を日常的に学習ツールとして使用できるようにすることが重要である。（ポイント⑪）
- 教育用クラウドサービス内のワープロや表計算などのいわゆるOfficeアプリと、コミュニケーションアプリやオンライン会議アプリを組み合わせることで、他者との情報共有や協働での意見整理などが容易に行えるため協働的な学びが円滑に実施できる。（ポイント⑫）
- ICT端末の積極的な活用姿勢と、端末活用スキルには関係性があると考えられる。情報活用の実践力として、基本的な端末活用スキルを高めるための手立てを考える必要がある。（ポイント⑬）

※　本パンフレットは、実証研究を通じて、兵庫県の現行のネットワーク環境を前提とした場合におけるセキュリティ対策等を取りまとめたものです。なお、各自治体のネットワークの状況や技術の進展等により取りうるセキュリティ対策は異なることも想定されます。

学校ネットワークの今後の在り方に関する実証研究
（高等学校等における多様なICT端末の活用に関する実証研究事業）
事業推進委員会（敬称略）

黒田　昌克	神戸女子大学文学部教育学科准教授
津川　誠司	グローバルセキュリティエキスパート株式会社顧問
福井　昌則	徳島大学高等教育研究センター准教授

令和4年度　文部科学省委託
学校ネットワークの今後の在り方に関する実証研究
（高等学校等における多様なICT端末の活用に関する実証研究事業）

高等学校等における多様なICT端末の活用に関する
導入・運用・活用に関するパンフレット
（令和5年3月）

兵庫県教育委員会
神戸市中央区下山手通5－10－1