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・活用に関するガイドブック

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）

兵庫県教育委員会

文部科学省

目 次

※ 本ガイドブックは、実証事業を通じて、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。

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ました。本書は実証研究のまとめを、以下の5章に分けて解説します。

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

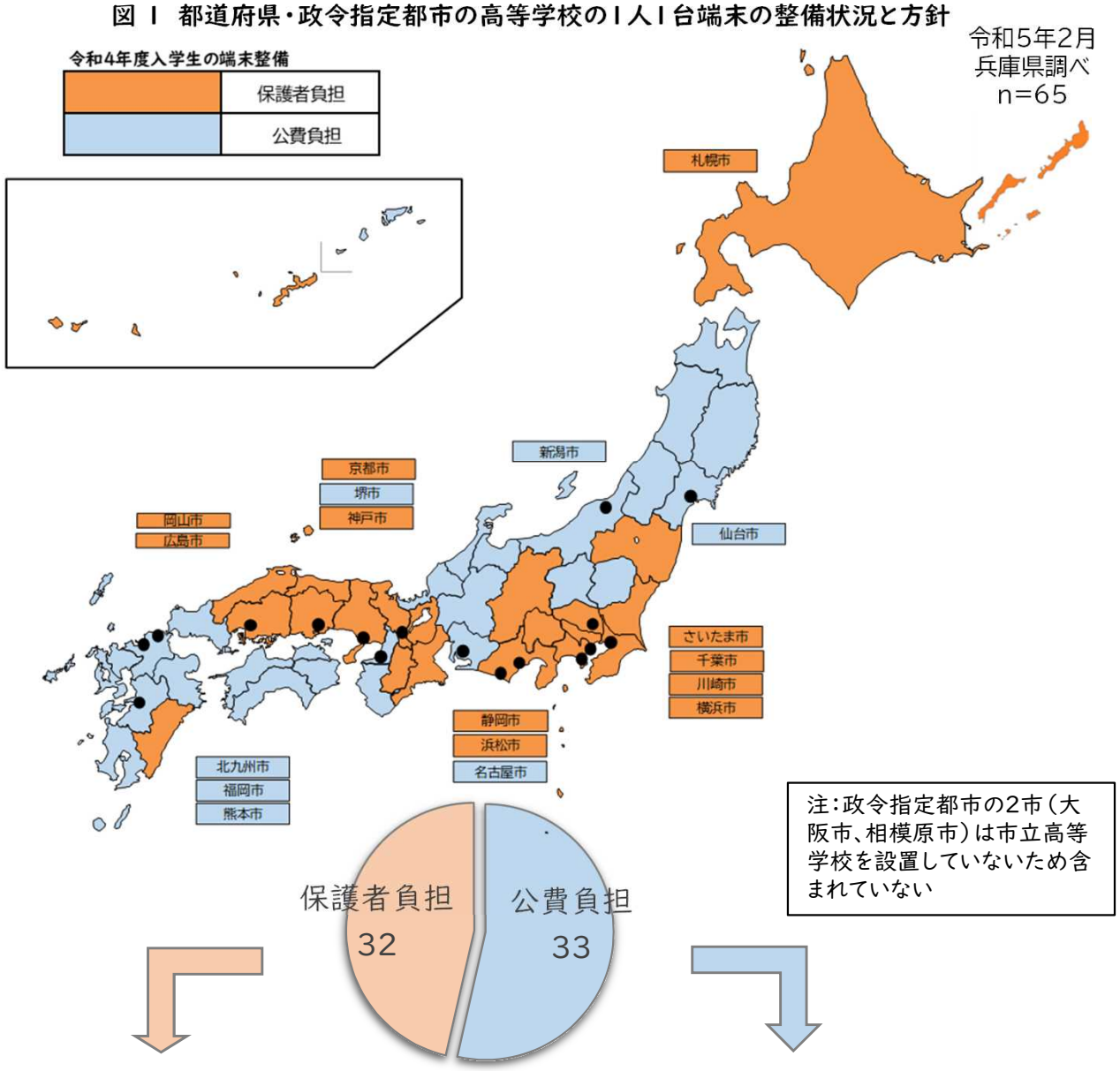
1 都道府県・政令指定都市の1人1台端末の整備状況と方針

高等学校の1人1台端末の整備には、主に、設置者が端末を用意し生徒がそれを使用する「公費負担」方法と、保護者が入学時に端末を用意する「保護者負担」方法があります。

令和4年度の入学生（高等学校）の1人1台端末の整備については、保護者負担とする自治体は32（21府県、11政令指定都市）あります。また、令和5年度以降は、保護者負担を検討している自治体や公費負担から保護者負担へ移行する自治体もあります。（兵庫県調べ）

文部科学省も、「GIGAスクール構想の最新の状況について、（令和3年3月19日）」において、高等学校段階の1人1台端末については、「BYODの推進も含めた高等学校等の設置者の取組を支援しつつ（後略）」としているように、今後は高等学校段階の1人1台端末については、保護者負担いわゆるBYODの導入が増えていくことが十分に予想されます。

図 1 都道府県・政令指定都市の高等学校の1人1台端末の整備状況と方針



引き続き保護者負担	30
R5新入生は保護者負担。R6新入生以降は検討中	1
R5新入生から公費負担	1

引き続き公費負担	17
R5新入生は公費負担。R6新入生以降は検討中	11
R5/R6新入生は公費負担。R7新入生以降は検討中	3
R8新入生から保護者負担	2

2 BYODによる1人1台端末整備の特徴

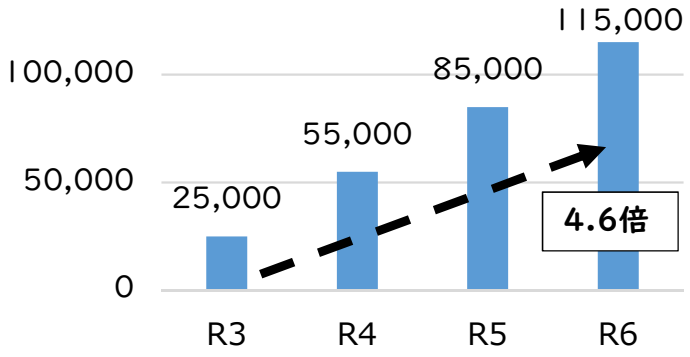
高等学校の1人1台端末をBYODにより整備するのは、公費負担による整備とは大きく異なります。本実証を通して、兵庫県では、BYODの特徴を、「多台数」、「多様」、「私物」の3つに整理しています。

① 「多台数」であること

今後全生徒が1人1台端末を所有すると、学習系ネットワークで利用する端末数が大きく増えることとなります。BYOD導入前（令和3年度）と比較すると、令和6年度は約4.6倍となることから、多台数の同時利用を考慮したネットワーク構成やセキュリティ対策が必要となります。

図2 兵庫県の県立高等学校の端末台数の推移（概数）

兵庫県では、令和4年度入学生よりBYODによる1人1台端末を年次進行で整備しています。令和6年度で、BYODによる全学年1人1台端末が実現します。



② 「多様」であること

BYODは、個人のICT端末を学校に持ち込んで使用するため、学習系ネットワークで利用するICT端末の種類（OSや機種）が多様化することとなります。

BYOD初年度（令和4年度）は、端末準備に伴う混乱の緩和や、円滑に授業を行うため等の理由により、学校推奨端末を設定している学校があり、その結果、大半の生徒が同じ端末を持つ学校が多くなっています。

今後、高等学校の1人1台端末が、より一般的になれば、学校においてICT端末の指定等をすることなく、生徒がより多様なICT端末を持ち込む方向に進んでいくことが予想されます。

表1 実証研究校の生徒が中学生の頃に所持していたコンピュータ・タブレットのOS

（n=210）

OS	割合
WindowsOS	34.8%
iPadOS	24.8%
ChromeOS	7.6%
その他OS（不明を含む）	32.8%

③ 「私物」であること

BYODは、各家庭にある個人のICT端末を学校でも使用することとなるため、ICT端末の所有者は生徒（又は家庭）であり、「私物」ということになります。

公費負担の整備の場合は、ICT端末の所有権は自治体または学校にあり、生徒はそれを借り受けて使用することとなるため、その使用内容や使用方法を限定することができました。一方、BYODは「私物」であるため、特に、学校の学習以外での使用の制限等、ICT端末を管理する方法や内容については配慮が必要です。

1 BYODの導入とローカルブレイクアウト※1

本章では、BYODの導入の際に必要なネットワーク構成の検討の進め方を解説します。

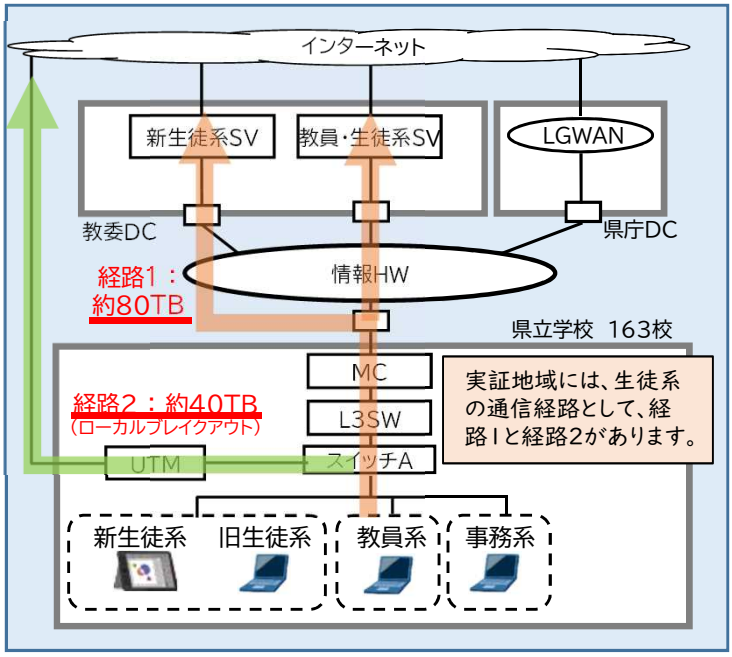
BYODの導入により、校内で使用する端末台数が増えるだけではなく、1人1人が端末を常時使用することとなるため、通信量は大きく増えます。そのため、兵庫県はこれまで、県立学校で使用する全ての生徒系、教員系の通信を、教育委員会のデータセンターに集約してインターネットに接続する構成（集約回線）でしたが、表2に示すとおりBYOD導入前において通信量の多かったソフトウェアを、集約回線から外部光回線へローカルブレイクアウト（図3-1緑）しました。OSのアップデートなど特定のサービスや宛先向けのトラフィックについては、ローカルブレイクアウトすることで、生徒系の通信だけでなく、教員系の通信についても安定化を図る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。

表2 通信量が多いアプリケーションと集約回線の通信量（R2.12.1～R3.1.31）

生徒系			教員系		
ソフトウェア	通信量（TB）	経路	ソフトウェア	通信量（TB）	経路
MS. Windows.Update	22.97	1→2	HTTPS.BROWSER	15.44	1
YouTube	7.06	1	YouTube	10.74	1
Apple.Software. Update	5.76	1→2	Microsoft.Office. Update	8.42	1
HTTPS.BROWSER	3.54	1	MS. Windows.Update	8.31	1
Microsoft.Office. Online (Office365)	3.52	1→2	Google.Service (Google Workspace)	6.28	1→2
Apple.Store	1.93	1	HTTPS	6.11	1
Google.Cloud. Strage	1.88	1	Yahoo.Services	5.66	1
iCloud	1.33	1	Adobe.Web	5.24	1
Microsoft.Portal (Office365)	1.11	1→2	HTTP	5.01	1
Google.Service (GoogleWorkspace)	0.41	1→2	Microsoft.Portal (Office365)	1.75	1→2
OneDrive	0.40	1	HTTP.BROWSER	1.73	1

図3－1 実証地域（兵庫県）のネットワーク構成図



※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。

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。

実証校の有馬高校では、令和4年度のBYOD導入に合わせて、双方向型の学習を推進する上で、学習支援アプリの活用を始めたことから、データセンター経由（図3-1オレンジ）の通信量が増えました。（表3 赤枠①）

また、播磨農業高校は、令和4年度から家畜や果実・草花の生育・育成状況を記録・整理し、共有するため教育用クラウドサービスを活用したことから、ローカルブレイクアウト（図3-1緑）の通信量が増えました。（表3 赤枠②）」

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す。

表3 実証校の通信量

データセンターで集約する通信	ダウンロード		アップロード	
	R4通信量（Ave）	（R3比）	R4通信量（Ave）	（R3比）
① 有馬高校	2.07 Mbps	1.04 倍	0.40 Mbps	1.67 倍
播磨農業高校	2.73 Mbps	1.65 倍	0.27 Mbps	1.69 倍

ローカルブレイクアウトの通信	ダウンロード		アップロード	
	R4通信量（Ave）	（R3比）	R4通信量（Ave）	（R3比）
有馬高校	1.90 Mbps	1.41 倍	0.19 Mbps	0.90 倍
②播磨農業高校	1.66 Mbps	1.05 倍	1.00 Mbps	5.56 倍

調査期間	令和4年9月1日～11月30日
比較期間	令和3年9月1日～11月30日
対象となる通信	データセンターを経由する校内の通信 （図3-1オレンジ）（L3SW）の上記3ヶ月間の平均値 ローカルブレイクアウトの通信 （図3-1緑）（UTM）の上記3ヶ月間の平均値

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。

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3－2 実証地域（兵庫県）のネットワーク構成図

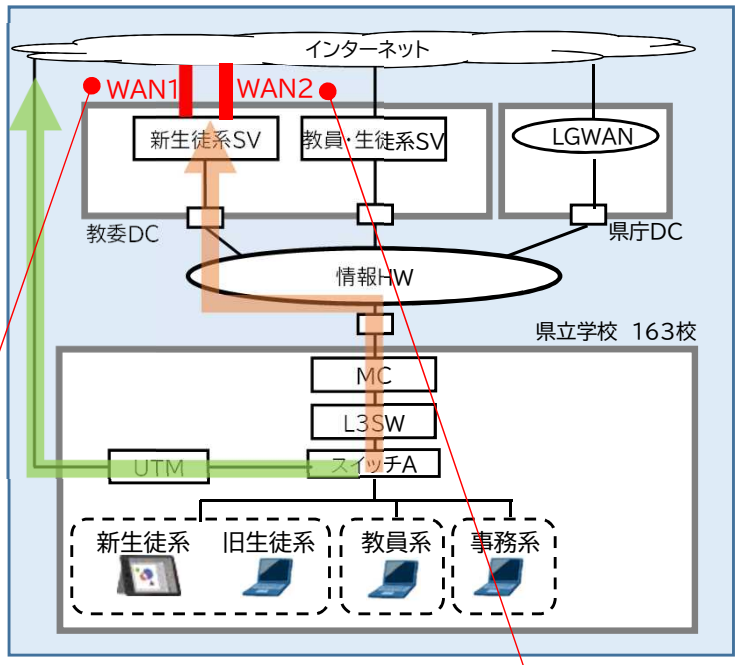
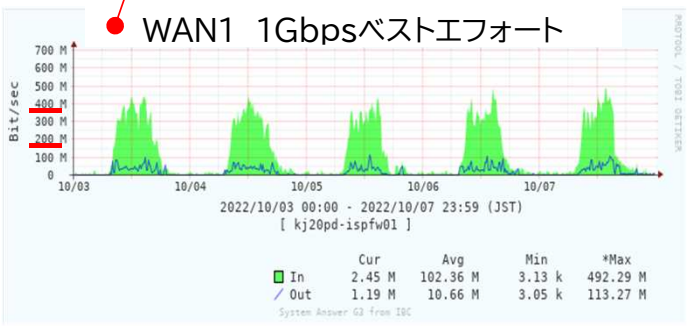
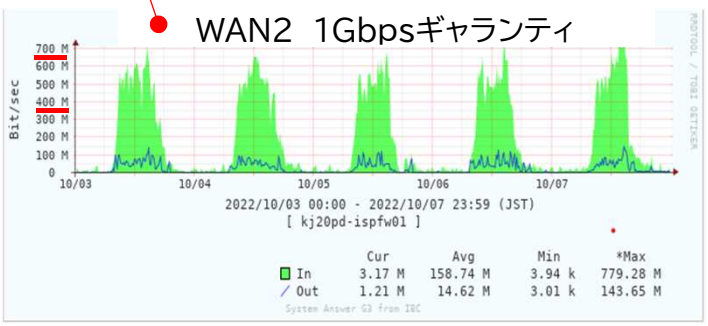


図4 実証地域（兵庫県）の集約回線の通信量





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。その年次進行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5 BYOD端末への動的IPアドレス払い出しの例（兵庫県）

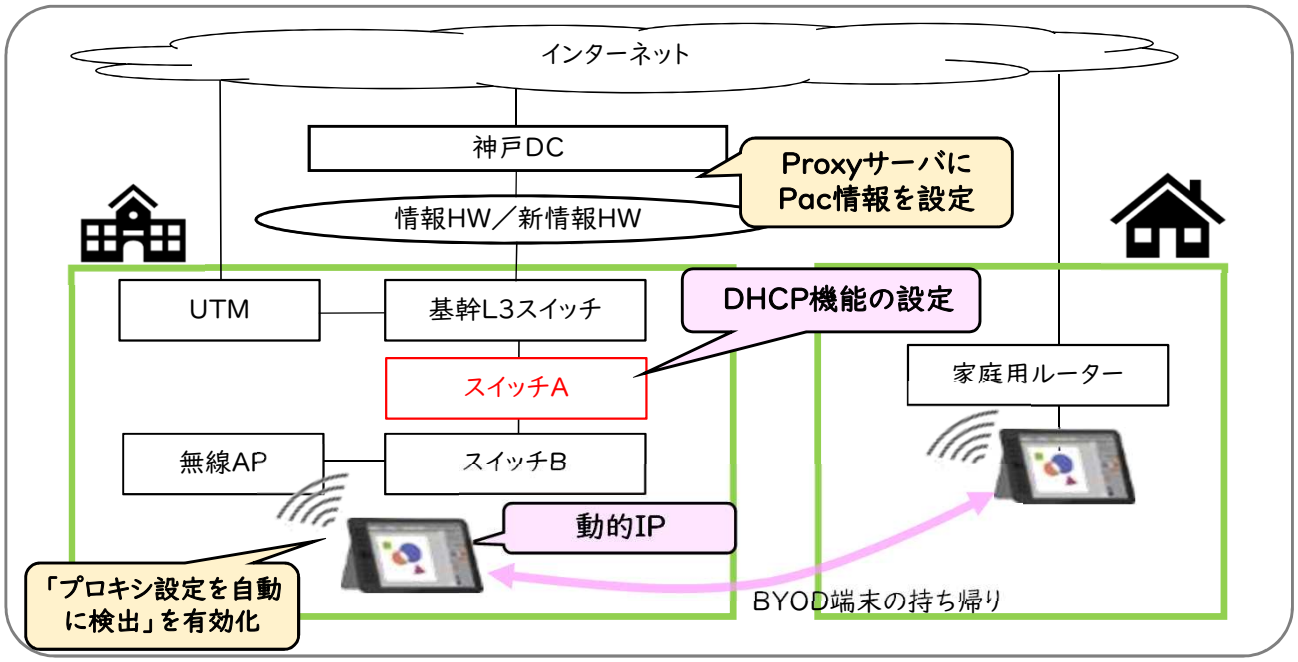


図6 IPアドレスの割当て範囲の例（兵庫県）

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4 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。

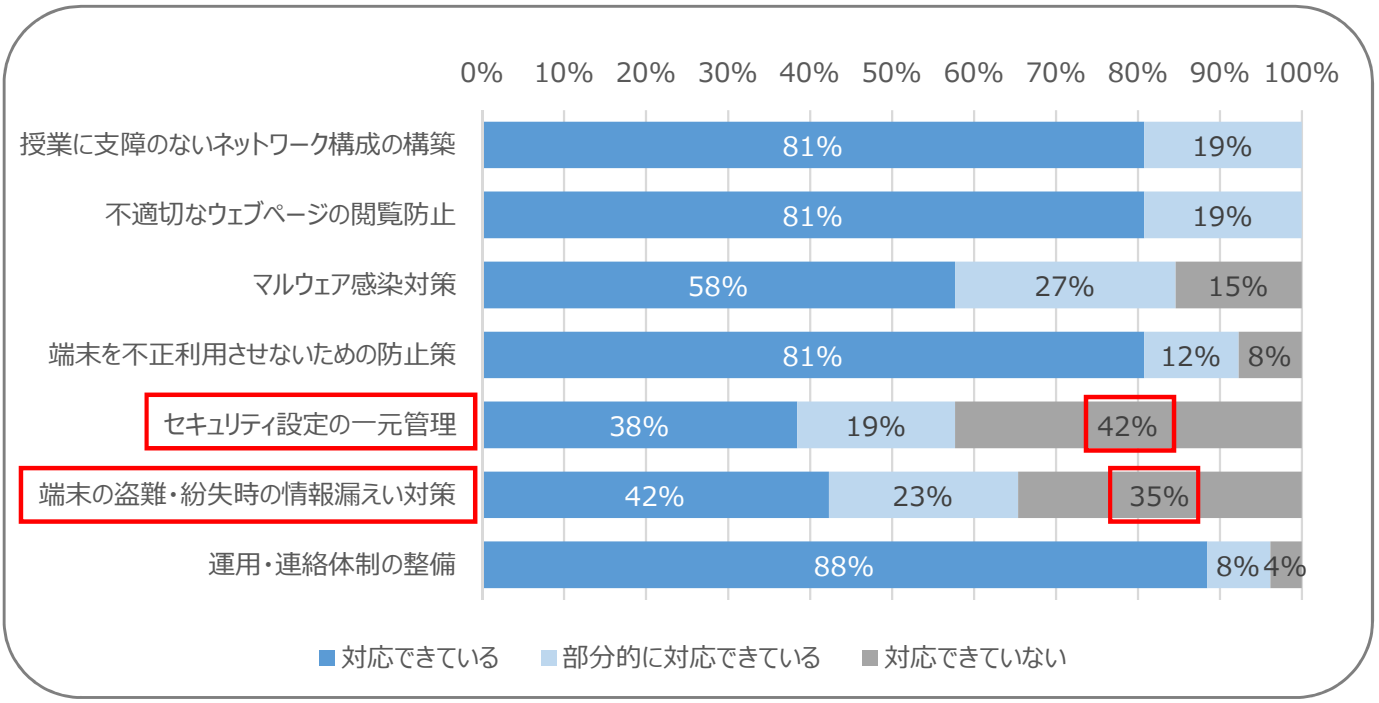
また、WindowsOSやChromeOSが混在する場合は、プロキシ設定の自動検出を有効化することで、学校や家庭で端末の設定変更することなく使用することが可能です。

Ⅰ BYODの導入時におけるセキュリティ対策

本章では、BYODの導入時のセキュリティ対策の検討の進め方を解説します。
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）においては、「BYODを行う際には、本ガイドラインを参考にしつつ自治体が整備する端末の環境と同等のセキュリティ対策を講じる必要がある。」とされています。
BYODを導入している自治体において、対応できていないセキュリティ対策として割合が高い項目は、「セキュリティ設定の一元管理」（42%）と、「端末の盗難・紛失時の情報漏えい対策」（35%）です。
なお、兵庫県では、BYOD導入に際して、学習者用端末の不適切なウェブページの閲覧防止、マルウェア感染対策や運用ルールの規定を追加するなど兵庫県教育情報セキュリティ対策基準を改訂し、「県立学校学習者用端末運用ルール」を参考に示した上で、各学校において運用ルールを策定することとしました。

図7 ガイドラインに例示された項目への対応状況（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）



《参考：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）において定められている7項目》

(1) 授業に支障のないネットワーク構成の選択（帯域や同時接続数など）
クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

(2) 不適切なウェブページの閲覧防止
児童生徒が端末を利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。
<対策例> ①フィルタリングソフト ②検索エンジンのセーフサーチ ③セーフブラウジング

(3) マルウェア感染対策
学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

(4) 端末を不正利用させないための防止策
端末のセキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

(5) セキュリティ設定の一元管理
児童生徒への端末配布後においても、端末のセキュリティ設定やOSアップデート、ウェブブラウザのアップデート、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。

(6) 端末の盗難・紛失時の情報漏洩対策
児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（データ消去）することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

(7) 運用・連絡体制の整備
学校内外での端末の運用ルールを制定し、インシデント時の連絡先や対応方法を各学校にて整理しなければならない。

コラム1

BYOD端末の運用ルールの見本（兵庫県の場合）

兵庫県では、オープンハイスクールや合格者説明会等において、生徒や保護者に対しBYODについて説明をしています。さらに、入学後、生徒に接続確認や端末の利用に当たっての運用ルールについてオリエンテーションを行った上で、BYOD端末を教育活動で活用しています。

県立○○学校学習者用端末運用ルール

兵庫県立○○学校

1 目的

本運用ルールは、本校において、生徒が使用する学習者用端末を校内ネットワークに接続して適切な活用を図ることを目的とする。

2 学習者用端末の定義

学習者用端末（以下「端末」という。）とは、授業時等に教員の指導のもと校内ネットワークに接続して使用する端末をさす。

3 利用期間

端末を校内ネットワークに接続して利用できる期間は、本校在学中に限る。

4 利用可能範囲

原則として学習活動や学校行事、生徒会活動や部活動などの教育活動に関係する内容であれば、Webブラウザによるインターネット閲覧、教育用クラウドサービス（以下「クラウド」という。）や学習活動等に関係するアプリの利用を認める。

5 利用上の注意

次の事項を守り適切な端末の利用に努めること。

(1) コンピュータウィルス等の有害なプログラムを使用または提供しないこと。
(2) 情報発信の際は、法令その他公序良俗に反しないよう内容を十分吟味すること。
(3) 誹謗中傷に当たる行為を行わないこと。
(4) 閲覧及びダウンロードした情報の著作権保護に注意すること。
(5) データ送受信の際には、ネットワークに過大な負担を与えないようデータ容量に注意すること。
(6) ネットワークの不具合等を認識したとき、速やかに教職員に報告すること。
(7) 端末の貸し借りはしないこと。
(8) 校内の電源を使用した充電はしないこと。
(9) その他、学校が禁止する、又は不適切と判断する行為を行わないこと。

6 利用の制限及び停止

県教育委員会及び学校は、前項に定める事項に違反、又は不適切な利用と認められる場合、校内での端末の利用やクラウドの利用を制限、又は停止することがある。

7 クラウド等のユーザーID及びパスワードの管理

(1) 利用者は、ユーザーID及びパスワードを他人に知られることがないよう、適切に管理すること。
(2) ユーザーID及びパスワードが漏えい、又はその可能性がある場合は、教職員に速やかに報告すること。
(3) 初期パスワード（仮パスワード）は必ず変更すること。
(4) パスワードは定期的に変更すること。

8 端末のセキュリティ対策

(1) 端末OSのバージョンはサポート期間内のものを使用すること。また、可能な範囲で最新版に更新していくよう努めること。
(2) 利用者は、端末にウイルス対策ソフトウェアを導入し、パターンファイルを常に最新の状態に更新しておくよう努めること。

9 ユーザーIDの廃止及び設定情報の削除

利用者は、休学、転学及び退学の場合、ユーザーID情報及びWi-Fiの設定情報を端末から削除すること。

2 実証研究におけるセキュリティ対策

ガイドラインに例示された7項目（P.10）のセキュリティ対策のうち、ガイドライン(3)（4）に対応するため「検疫システム」及び「認証システム」を、(5)（6）に対応するため「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に接続させるよう、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5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5 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。

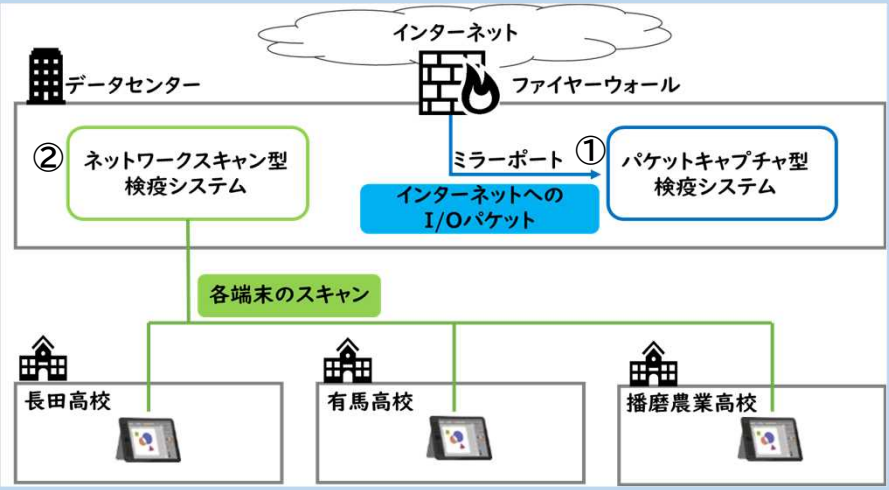
3 検疫システムの導入

学校のネットワークをウイルス感染などの脅威から守るために、接続するBYOD端末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へのアップデート等が適切に実行されていることが重要です。また、様々な種類の脅威からBYOD端末を守るため、到達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。セキュリティの観点から、安全なBYOD端末のみを校内ネットワークに接続するために端末の検疫を行う仕組を導入することが有効です。

検疫システムの概要

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、パケットキャプチャ型及びネットワークスキャン型の検疫システムを導入しました。

図8 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。

表6のとおり、実証校における検知調査の結果、危険度「高」の通信については、検出数は5件と少ないものの、「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出されました。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、教育現場における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。

表6 パケットキャプチャ型検疫システムの検知調査結果

調査対象 実証校3校
調査期間 令和5年2月8日～3月8日

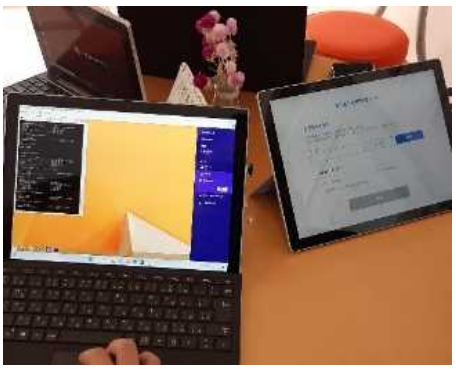
危険度	イベントの概要	総計
高	平文（暗号化されていない状態のデータ）でパスワード情報をやりとり	5
中	不正サイトで利用されるサイトへのアクセス	1,545
	新型コロナウィルスの情報サイトを騙った危険なサイトへのアクセス	49
	フィッシング等で利用されるURL短縮サービスの利用	3
	オンラインストレージサイトへのアクセス	2

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。



検疫の様子

表7 検査内容としきい値

検査内容	しきい値
OS種別／バージョンの判定	メーカーサポート切れのOS（EOS：End of Sales）
ポートスキャン(侵入経路探索)	不要ポートの開閉状況（侵入可能な経路がある等）
脆弱性検査(Emotet等)	脆弱性あり

iPhone、iPad及びMicrosoft Windows全般にEOS（End of Sales）で異常を検知したBYOD端末が135台中11台存在していました。また、Windows端末については、MS17-010の脆弱性が検知されており、ランサムウェアとして有名なWannaCryに感染する可能性があることがわかりました。

表8 ネットワークスキャン型検疫システムの検知結果

調査対象 実証校3校
調査期間 令和5年2月8日～3月8日

校名	対象BYOD	正常	異常	総計	異常理由
A高校	iPhone or iPad	1		1	EOSバージョン
	Microsoft Windows 8.1		2	2	WannaCry感染可能（MS17-010脆弱性）
	Windows10 or 11	24		24	
B高校	iPhone or iPad	4		4	EOSバージョン
	Mac OS X 10.4		2	2	
	Microsoft Windows 7 Home		1	1	WannaCry感染可能（MS17-010脆弱性）
	Microsoft Windows 8.1		4	4	
	Windows10 or 11	18		18	
C高校	Microsoft Windows 8.1		2	2	
	Windows10 or 11	77		77	
合　計		124	11	135	

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。

4 認証システムの導入

BYODを導入した場合は、端末が多様化し、かつ、端末の種類は年度毎に流動的であるため、ネットワーク認証として、ユーザー認証の重要性が高いと考えられます。

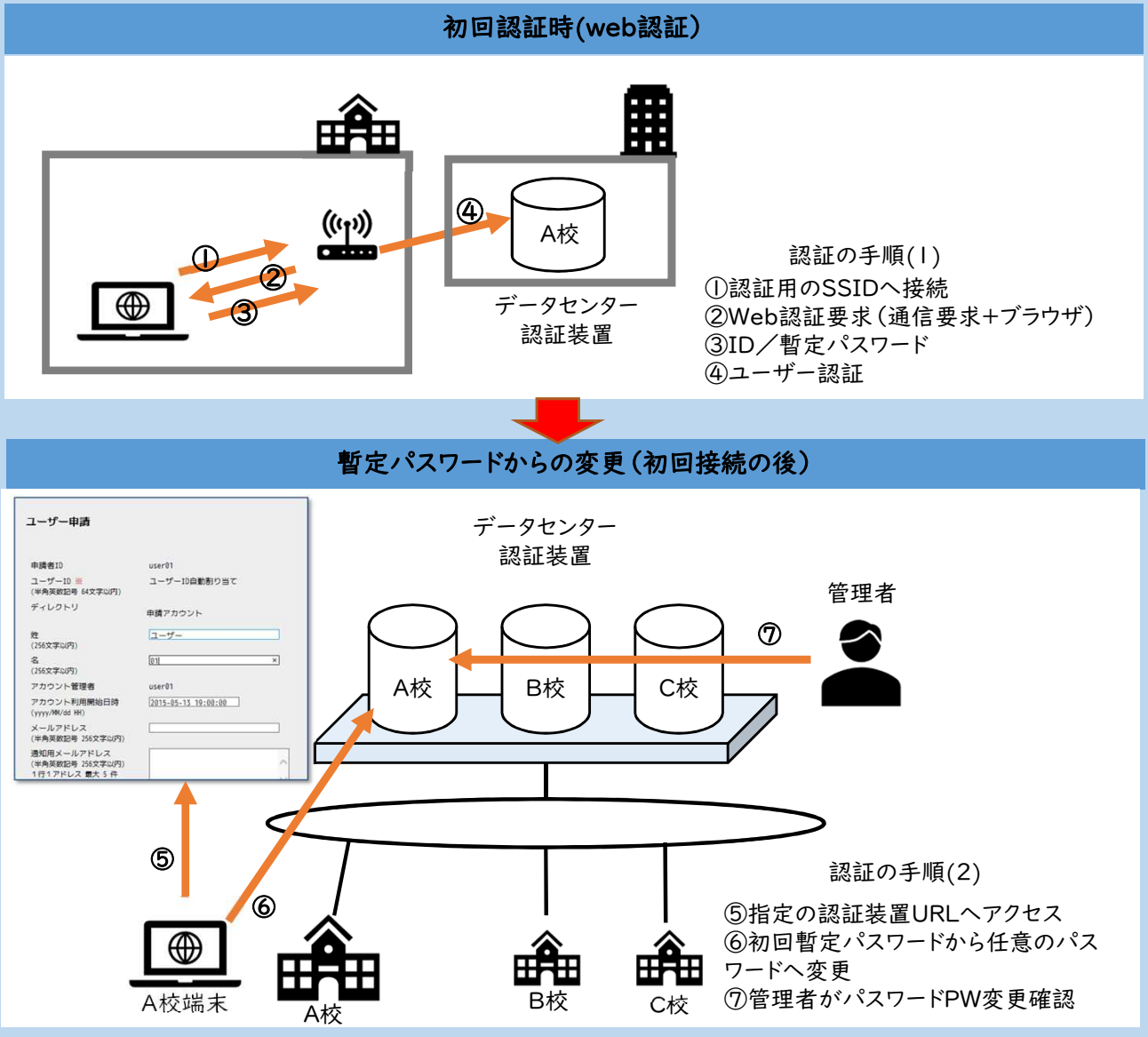
校内には、重要性の高い情報資産があるとともに、利用者の安全も確保する必要があるため、校内ネットワークを利用できる人物や端末、利用者の権限については、明確に範囲を限定する必要があります。

認証システムの実証概要

初回認証時は全生徒共通の暫定パスワードでログインしますが、セキュリティ向上と他人のアカウントでのログインを防ぐため、認証を完了した生徒は自分で任意のパスワードへと変更を行う設定としました。

実証校アンケート（P.20）では、生徒がIDやパスワードを忘れることを心配する教員が多い（77.4%）ことから、各学校の管理者が、生徒のパスワード変更状況を確認できるとともに、パスワードを忘れた生徒のパスワードを強制的に変更できる仕組としました。

図9 認証システムの概要



認証システムの選定ポイント

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9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。

また、認証システムを設置する場所は、主に以下表10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。

表9 認証方式

	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。

表10 認証装置の設置場所

	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。

5　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。

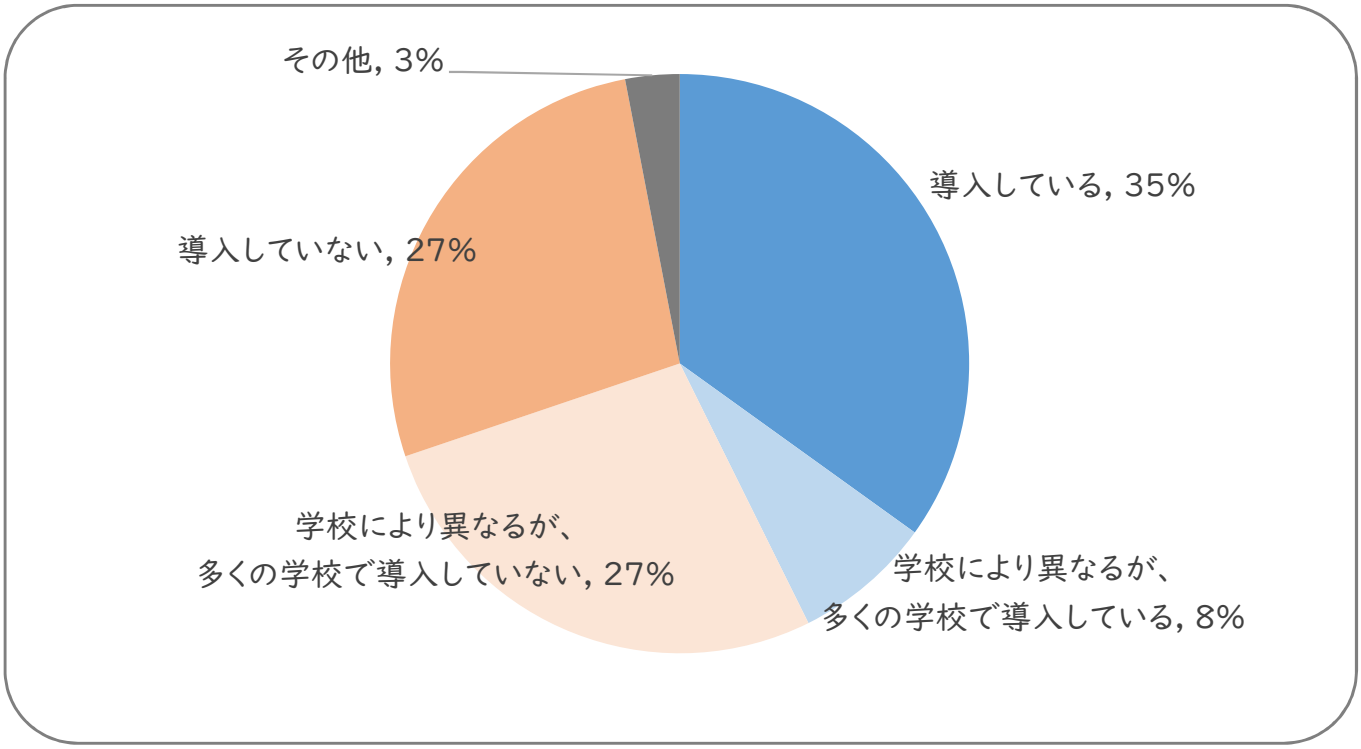
MDMにより見込めるセキュリティ面での効果は、主に以下のとおりです。

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10　保護者負担の端末におけるMDMの導入状況（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

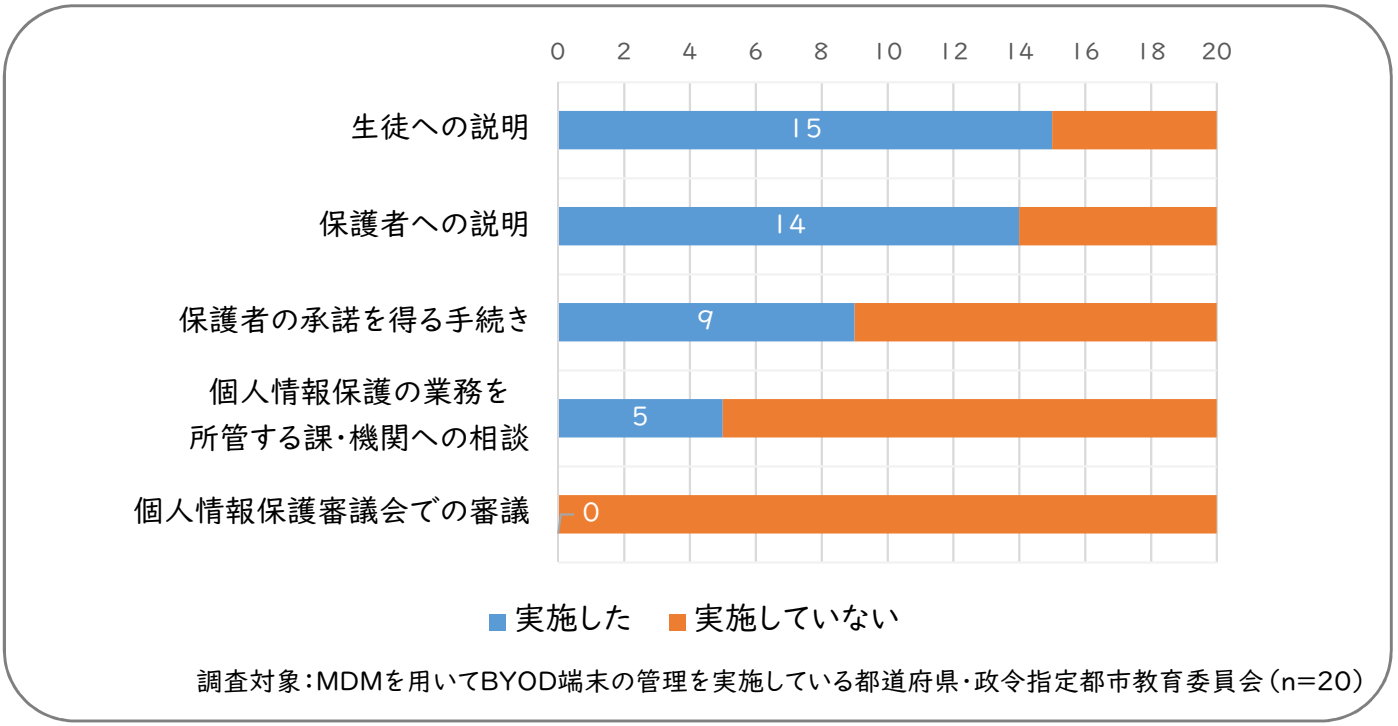
全ての生徒に自身のBYOD端末のセキュリティ対策を適切に行わせるのは難しく、かつ、その指導も難しいことから、MDM等によって、多様な端末のセキュリティ対策状況を維持することが有効です。

6 BYOD端末と個人情報の管理

BYODを導入する場合、生徒の端末は家庭の所有物（私物）であるため、MDMで管理を行う場合は、利用目的を明確化（端末をどうやって管理するか、どこまで管理するか）するとともに、MDMで収集される端末情報（管理するために収集される情報はどのようなものがあるか）を明確化し、所有者である生徒・保護者に説明することが必要です。

都道府県・政令市において、BYOD端末を管理するにあたり実施した手続きについてアンケート調査を実施しました（図11）。

図11 MDMを用いてBYOD端末を管理するために、実施した手続き（令和5年2月）



調査対象：MDMを用いてBYOD端末の管理を実施している都道府県・政令指定都市教育委員会（n=20）

兵庫県では、BYOD端末の所有者である生徒・保護者に入学説明会で案内するなど、利用するMDM名とその目的、県・学校が収集する情報を文書にまとめ、理解を得る手続きを行っています。

兵庫県において県・学校がMDMで閲覧ができる情報は以下のとおりです。MDMで閲覧できる情報について、個人情報保護の業務を所管する課へ相談を行い、「個人情報」には該当しないと確認したことから、個人情報保護審議会では審議していません。

県・学校が閲覧できる情報	県・学校が閲覧できない情報
・端末のモデル（例：Dynabook K60） ・端末の製造元（例：Dynabook） ・OSとそのバージョン（例：iOS12.0.1） ・アプリの情報（アプリ名、バージョン、サイズ等） ・端末名 ・端末のシリアル番号	・通話履歴、Web閲覧履歴 ・電子メール、テキストメッセージ ・連絡先、予定表 ・パスワード ・画像 ・位置情報　など

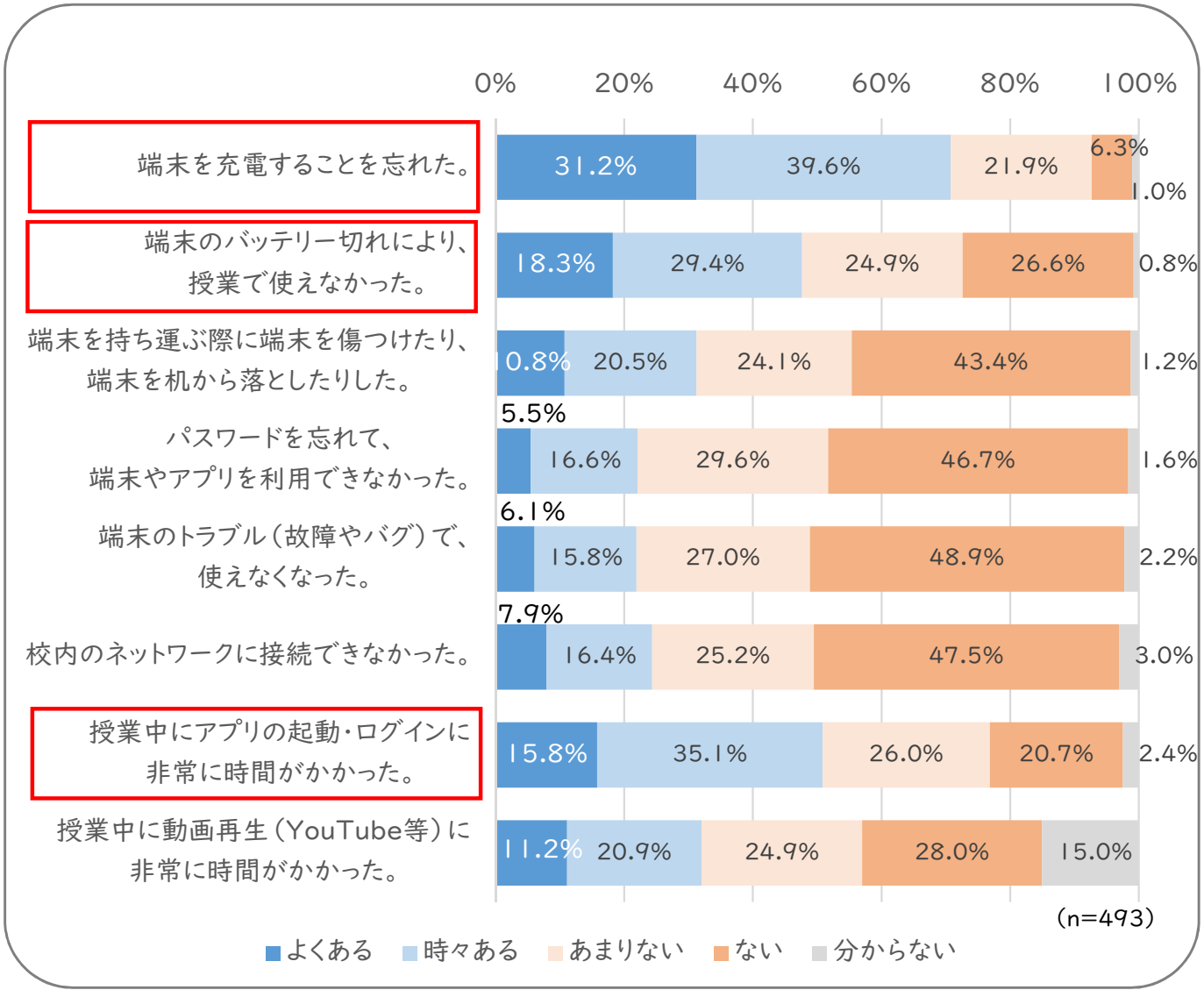
1 生徒が経験したBYOD端末に関するトラブル

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経験を持つ（50.9%）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。

図12 BYOD端末に関するトラブルの経験（実証校生徒アンケート）



ポイント⑧

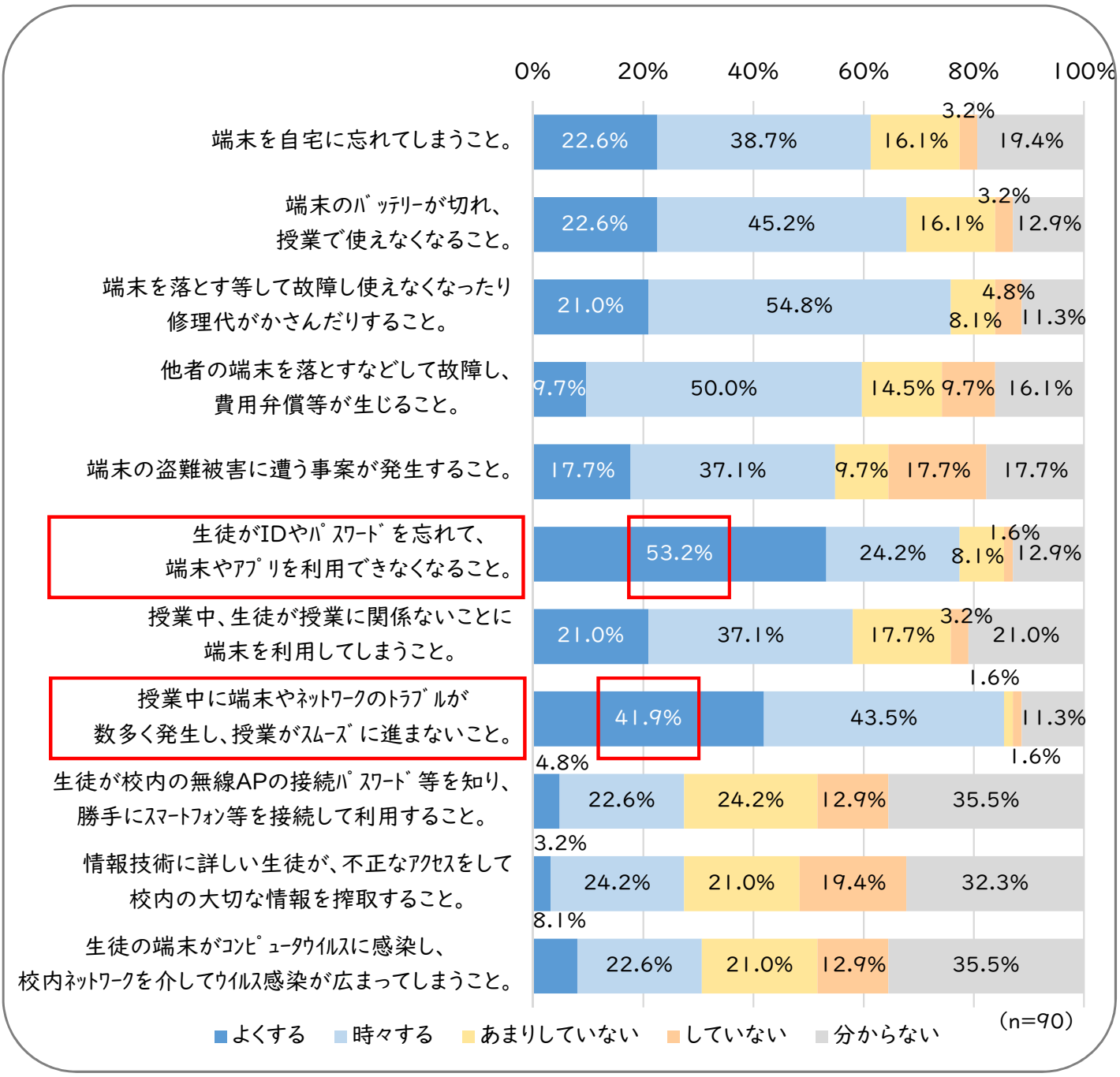
教育DXを見据え、学習ツールとしてのBYOD端末を、教員主導ではなく、生徒自身が自由に使いこなすことで、生徒主体のICT活用を進めることができます。

※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。

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。

図13 BYOD端末に関するトラブルが発生することを心配しているか（実証校教員アンケート）



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。

※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

3 トラブルを未然に防止するための知識・技能

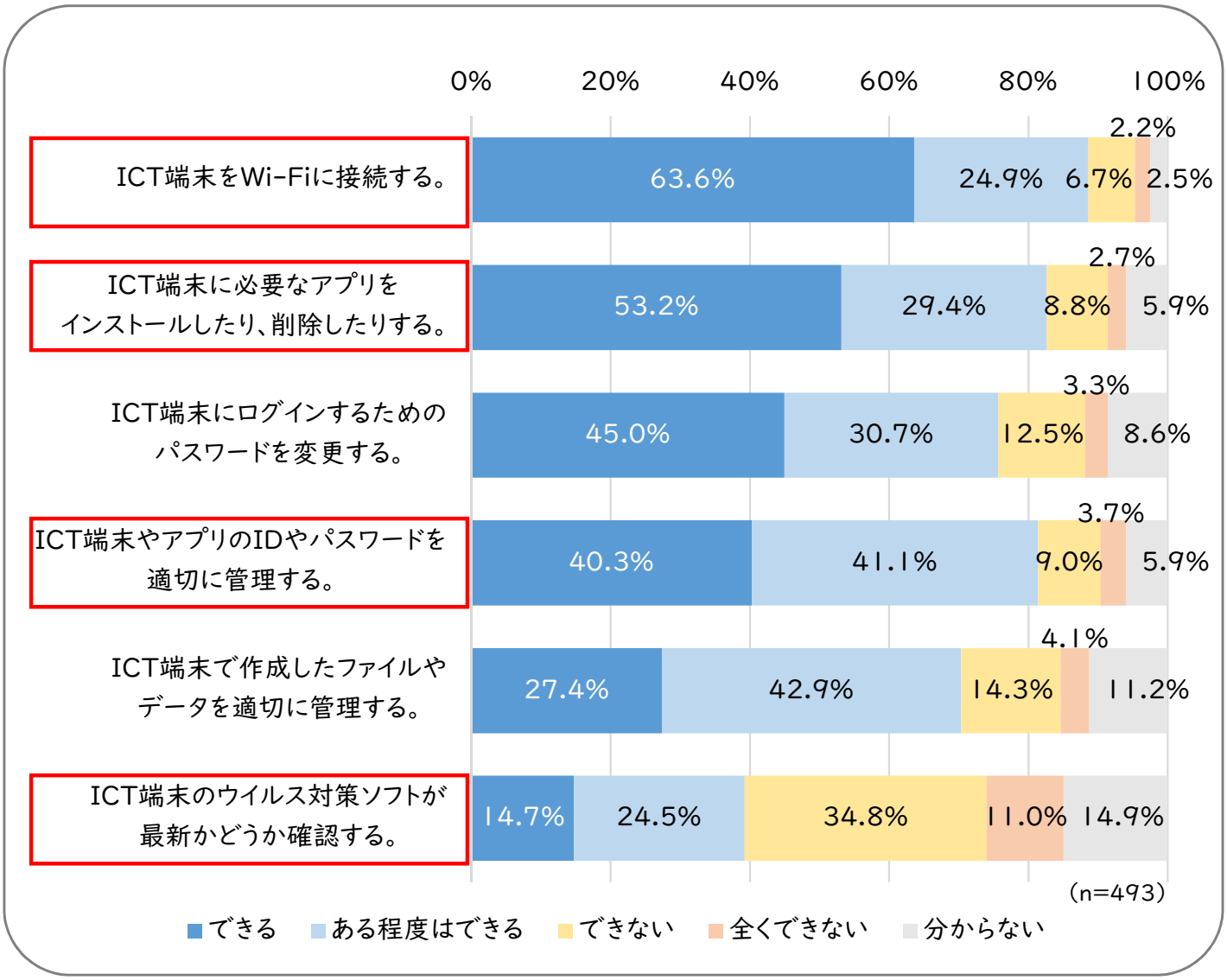
BYOD端末は「私物」であることから、日々の管理は生徒自身が行います。管理が不十分な場合は、トラブルに直結します。

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。

図14 BYOD端末の管理スキル（実証校生徒アンケート）



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 BYOD端末の導入・活用・運用に関するルール作り

端末活用に伴うトラブルを防ぐには、端末使用に関するルールを決めておくことが大切です。

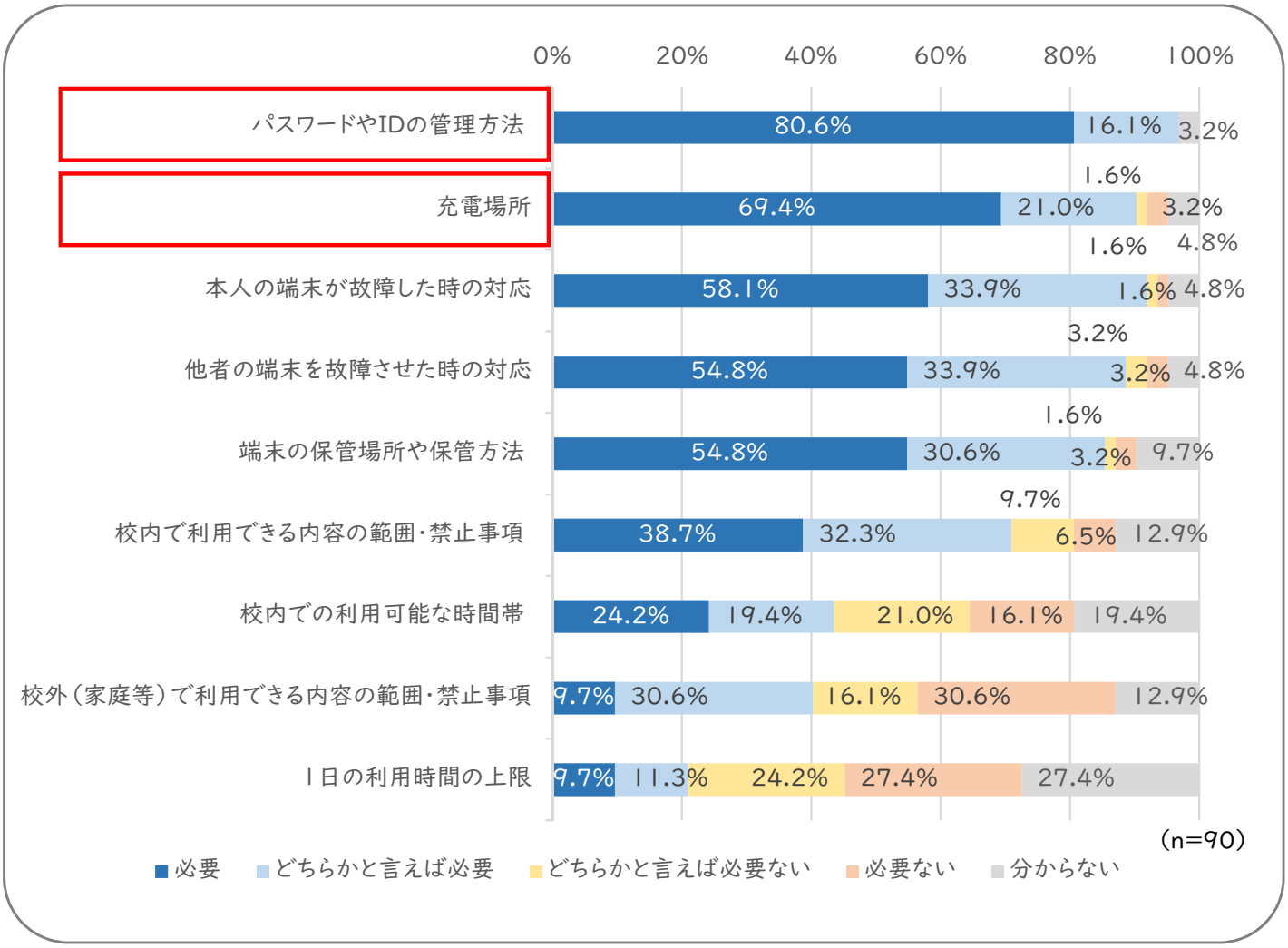
実証校の教員に、BYOD端末にはどのような運用ルールが必要であるかを尋ねました。「必要」及び「どちらかと言えば必要」と回答した教員の割合では、「パスワードやIDの管理方法」に関するルール（96.7%）や「充電場所」に関するルール（90.4%）が必要と考える教員が多いです。また、BYOD端末が故障したとき、故障させたときについてもルールを決めておくほうがよいと考える教員は多いです。

校内で利用できる内容の範囲・禁止事項についても、ルールを決めておきたいという考えを持つ教員も、一定数います。校内では、学習に必要な範囲で使用するなどの制限をかけることはやむを得ないと考えられます。

しかし、校外での使用については、「私物」であるため、塾や自分の趣味などに使用することもあります。BYOD端末の利用に関する制限や禁止事項を決めるばかりではなく、生徒のICT活用を推進する視点で、学校全体で協議して決めていくことが必要です。

BYOD端末の利用範囲や禁止事項については、やみくもに制限をかけるのではなく、情報モラル教育を着実に実施し、生徒の積極的かつ主体的なICT活用を推進するように検討しましょう。

図15 BYOD端末に必要なルール（実証校教員アンケート）



5 BYOD端末導入までの年間スケジュール

第4章の1～4を踏まえて、BYOD導入にあたっては、校内に検討委員会等を設置し、計画的に進める体制を構築することが望ましいです。

兵庫県では組織した検討委員会を中心に、まず、BYOD端末の活用方針を決め、次に、その学びを実現するために必要なスペックなどをまとめた学校推奨端末の仕様を決めました。最後に、端末の運用ルールを決めています。

また、オープン・ハイスクールにおいて、ICT端末を用いた授業を公開するなど、1人1台端末を用いた新たな学びの推進について、生徒や保護者の関心を高め、理解を得る取組も必要です。

新年度、すべての生徒が無理なく端末等を準備できるよう配慮し、端末を用いた教育活動を開始する時期を決める必要があります。まずは、端末の使用にあたっての注意事項等に関するオリエンテーションを行い、その後、本格的に教育活動へ活用していくのが有効です。

表11 BYOD導入までの標準的な手続きや流れの例

月	校内組織	保護者・生徒	業者 （学校斡旋する場合）
4～6	検討委員会の設置 活用方針の検討 学校推奨端末の仕様の検討		
7～8	学校推奨端末の仕様の決定 導入方法（契約・支払い方法等）の決定	オープン・ハイスクール等にて、保護者・生徒に説明	
9～12	運用ルールの決定	オープン・ハイスクール等にて、保護者・生徒に説明	業者選定 （1～2ヶ月程度）
1～2		学校ホームページ等に合格後の必要な手続き等を公表	業者と申込み方法や受け渡し方法の協議 （1ヶ月程度）
3	設定情報の作成 合格者説明会の開催		（必要に応じて）設定情報を学校から受け取り、端末のキッティング
新年度 4～5 （※）	接続確認 使用オリエンテーション	手順書に従い、初期設定	学校に納品

コラム2

トラブル対応のヒント

実証校の学校長と担当者に、多様なICT端末に関連して発生するトラブルへの対応方策について、インタビューしました。

実証校の先生からは、「生徒から端末やアプリの操作について質問があった際に、OSや機種が異なると、自分の端末とは、ボタン配置や画面、レイアウトが変わるので、対応する自信がない」という声が聞かれました。BYODとなり、OSや機種が多様化する中で、自分で対応することに不安を抱く教員は多くいます。苦手な教員をサポートできる体制づくりは、活用推進の大切なポイントになります。

当たり前にICT端末を使う若手教員のノウハウを発信していくことが最も近道と考えて、若手教員15名で組織したICT委員会を設置し、効果的な活用方法について研究しています。若手教員ができるところから丁寧に教えてくれるので、学校全体がICT活用推進の方向へ動き出していることを実感しています。

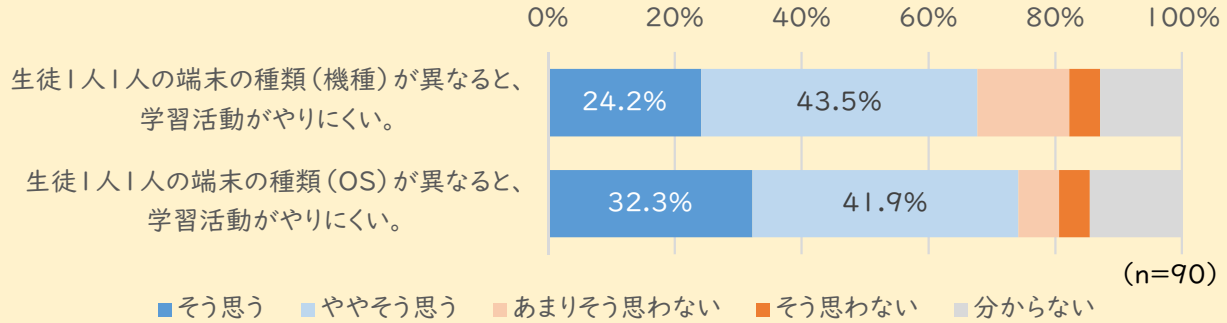
兵庫県立有馬高等学校
校長　萩原　健吉氏

兵庫県立有馬高等学校
教諭　増井　貴明氏

ICT端末が使いやすくなり、使用頻度が高まったことに比例してトラブルも多く起きるようになりました。校内に授業トラブルの支援チームのような存在を広げていくようにしています。

また、一度起こったトラブルは、その解決策をまとめ、共有するようにしています。これは効果的だと感じています。

図16　ICT端末の多様化について（実証校教員アンケート）



コラム3

BYOD導入期のポイント

実証校の学校長と担当者に、BYODを導入する際のポイントについて、インタビューしました。

BYOD導入期には、端末の活用方針を決め、それに見合ったスペックを提示し、端末の使用ルールを定め、学校説明会で生徒・保護者に説明をする流れとなります。その際、担当者任せにするのではなく、校内にBYODに関するチームを組織するなど、学校全体で取り組む体制づくりがポイントになります。

兵庫県立長田高等学校
校長　山根　尚氏

学校説明会において、BYODに関する質問コーナーを設置しました。中学校において1人1台端末を使った学びを経験し、それが効果的だと感じている保護者は多くいます。そのため、BYOD導入については、特に心配する声はありませんでした。

BYOD端末の活用を円滑に進めるためには、学校の特色にあわせて、職員全体で、「このように生徒に学ばせたい」や「関わっていきたい」ということを、じっくり話し合うことが大切です。

兵庫県立播磨農業高等学校
教諭　長生　達也氏

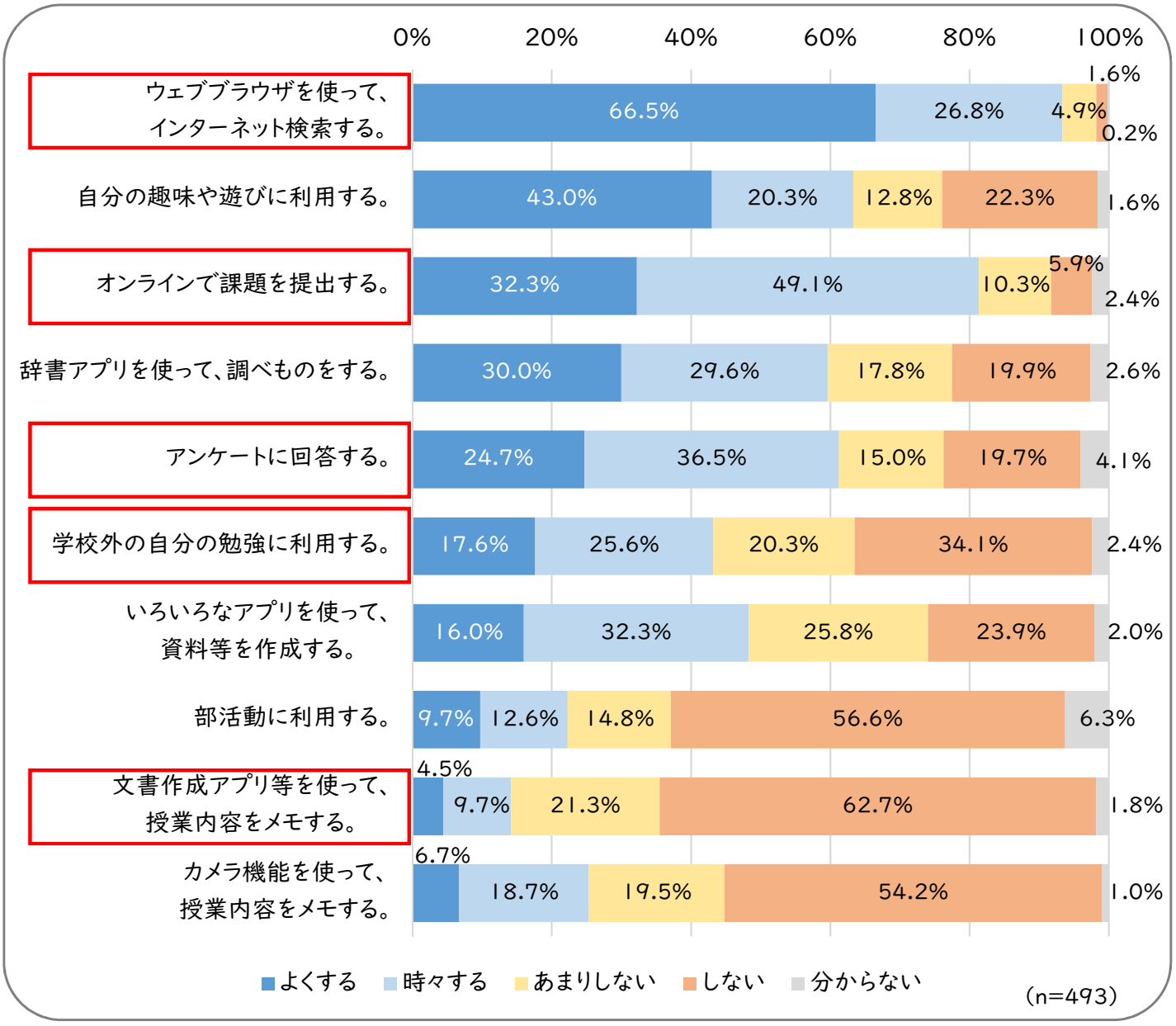
校内に、端末の仕様選定をするBYOD委員会を設置しました。チームで対応することで、困ったことを共有できました。教科担当に頼るのではなく、チームを組んで端末活用を進めていくことが大切だと感じています。

兵庫県立長田高等学校
教諭　黒地　美有氏

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。

図17 普段のICT端末の活用（実証校生徒アンケート）



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。

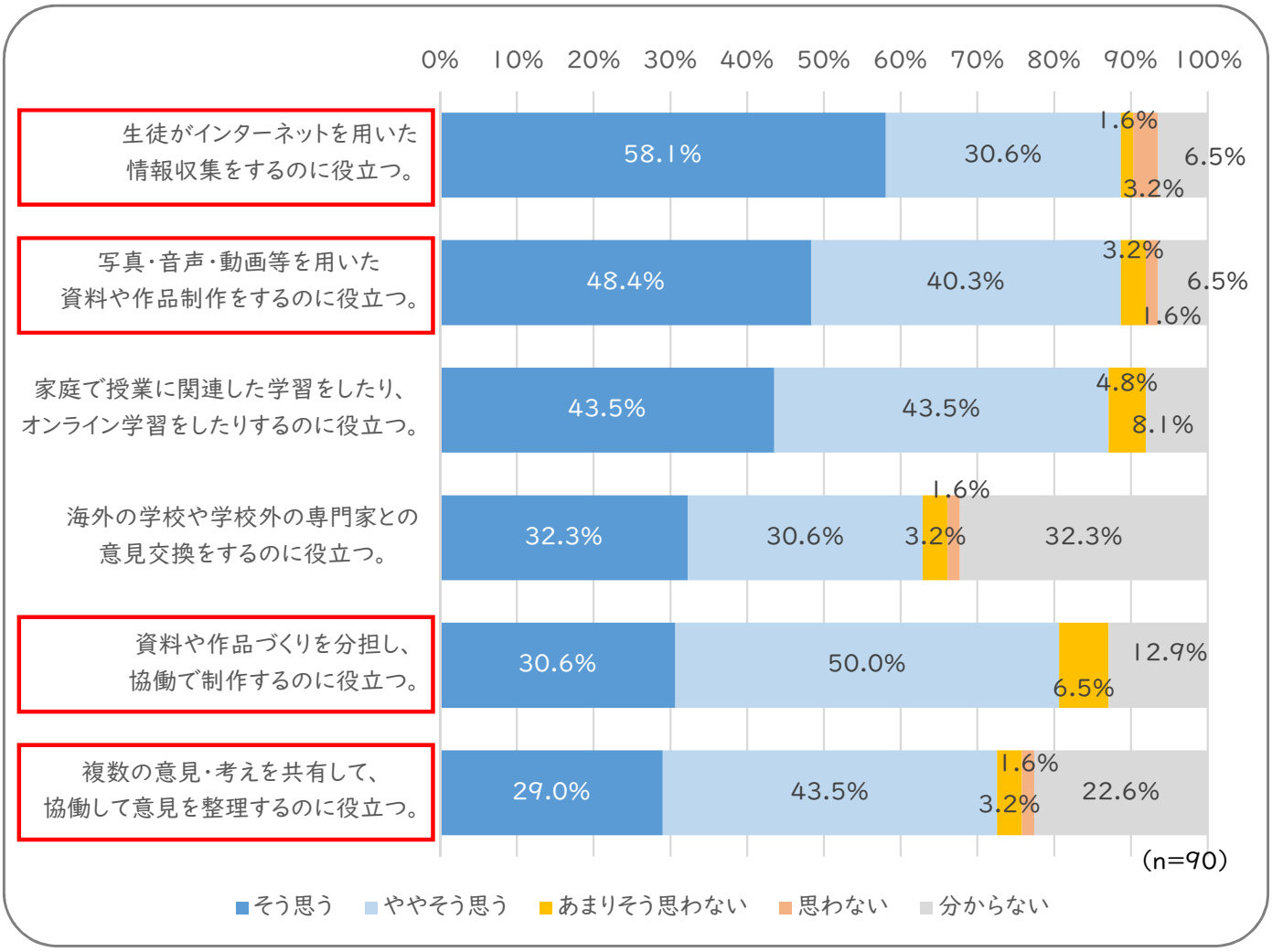
BYOD端末が役立つと回答した割合（「そう思う」及び「ややそう思う」と回答した教員の割合）が多かったのは、インターネットを用いた情報収集（88.7%）や、写真・音声・動画を用いた資料作成（88.7%）、家庭でのオンライン学習（87.0%）でした。

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。

図18 BYOD端末はどのような学習に役立つか（実証校教員アンケート）



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。

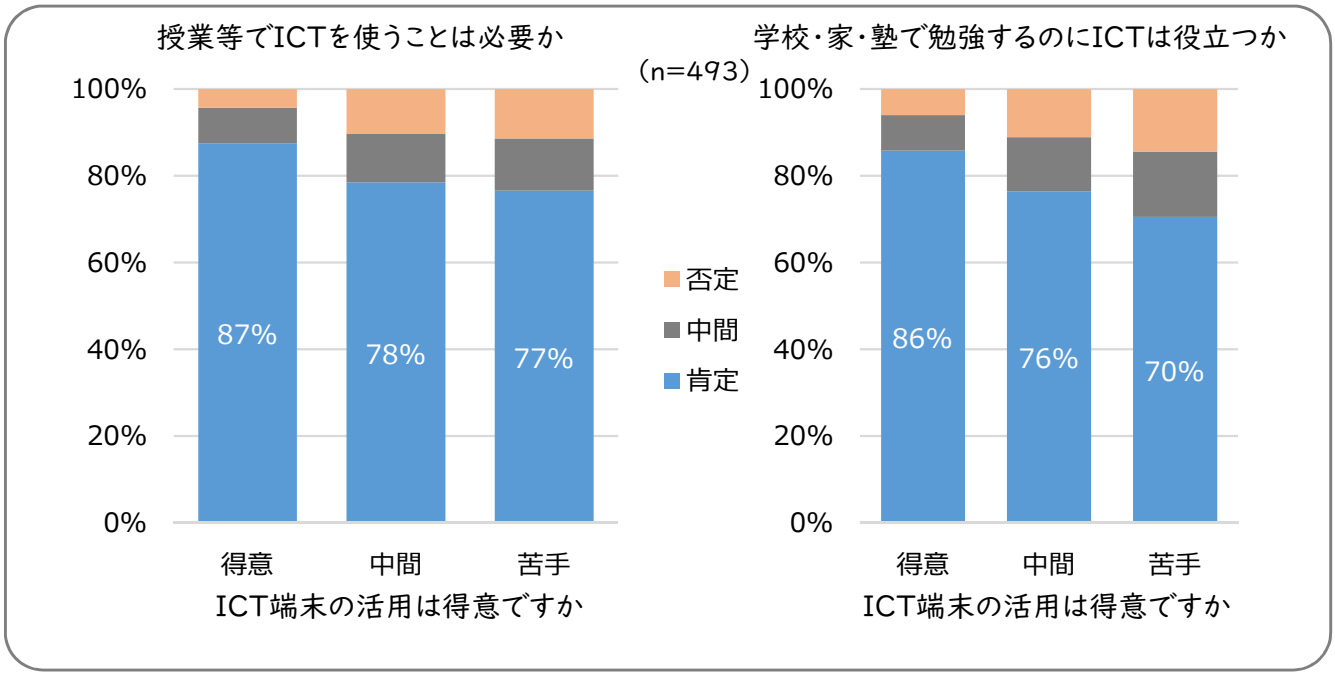
また、クラウドサービス内のワープロや表計算などのいわゆるOfficeアプリと、コミュニケーションアプリやオンライン会議アプリを組み合わせることで、他者との情報共有や協働での意見整理などが容易に行えるため、協働的な学びが円滑に実施できます。

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。

図19 BYOD端末はどのような学習に役立つか（実証校生徒アンケート）



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。

コラム4

多様なICT端末の教育的効果

実証校の学校長に、多様なICT端末を活用した学習による教育的効果と、今後の展開について、インタビューしました。

兵庫県立有馬高等学校
校長　萩原　健吉氏

生徒全員が日々の教育活動の中において、ICT端末をツールとして自由自在に活用できるように指導しています。
急速に進展する学校ICT改革の波に、乗り遅れないよう、家庭でもICT端末を使って、自ら考え、自ら学ぶスタイルを早急に確立することが重要です。知識・技能の定着を図るとともに、社会の様々な場面で活用できる力を身につけさせたいと考えています。

真に求められる「農作物」をつくるためには、勘ではなくデータ活用が必要です。常にそのような学習活動を取り入れた授業や課題研究を進めるようにしています。
また、他者と協働して取り組む「新しい農業」を目指して、問題発見・解決や協同的な問題解決に必要な思考力・判断力・表現力を育成したいと考えています。

兵庫県立播磨農業高等学校
校長　藤岡　文博氏

兵庫県立長田高等学校
校長　山根　尚氏

探究活動をするには、1人1台端末は非常に有効です。探究活動を進める過程において、生徒自ら大学や研究機関にアプローチして、オンラインで事前に質問を投げかける姿もあります。1人1台端末を用いて、高いレベルでの学習活動が実施できています。激しい変化が起きる時代に、主体的に学習に取り組む態度を育てたいと考えています。

第2章　多様なICT端末環境におけるネットワーク構成の検証

■ 安定した通信環境を実現するために検討すべきポイント

・ 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）→P.7

・ 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）→P.7

・ 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）→P.8

■ 学校でも家庭でもICT端末を用いるために検討すべきポイント

・ 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）→P.9

・ 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）→P.9

第3章　多様なICT端末環境におけるセキュリティ対策の検証

■ 不正・脆弱なICT端末の接続を防ぐために検討すべきポイント

・ 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）→P.13

・ 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）→P.14

・ 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）→P.16

■ 端末のセキュリティ設定を一元管理するために検討すべきポイント

・ 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）→P.17

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

■ BYOD端末を学校で使用する場合の指導上のポイント

・ 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）→P.19

・ 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）→P.20

・ 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）→P.21

第5章　多様なICT端末を活用した学びの充実

■ BYOD端末を活用した個別最適な学びと協働的な学びの充実のポイント

・ 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）→P.26

・ 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）→P.27

・ 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）→P.28

※　本ガイドブックは、実証事業を通じて、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・活用に関するガイドブック

（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