



iPadの管理と運用



環境のデザイン

ビジョンを達成するための
学習環境を構築する

目次

はじめに	3
空間的な学習活動の範囲	4
校内ネットワークからインターネットへのアクセス方式	6
ネットワーク環境におけるセキュリティ	13
OSおよびアプリの管理	17
関連資料	20

はじめに

生徒たちが想像し、思考したことを表現できる環境を実現するために

Appleは、優れたテクノロジーが多くの人の手に渡れば、世界を変えられると考えています。そのためには、すべての生徒がつながり、協働的、創造的で、パーソナルな、素晴らしい学習体験を構築することから始まります。これらの要素は、今日の世界、企業、そして革新的な学校に見られるのもので、学習のあり方を再考する上で基盤となる考え方です。

生徒たちを取り巻く学習環境は、めまぐるしく変化しました。学習者主体の探究的な学び、非常時におけるオンライン授業や分散登校、地域社会との関わり、教科書のデジタル化を含む、情報へのアクセス方法、業務の効率化に至るまで、教育の現場において、テクノロジーを活用して対応すべき項目はたくさんあります。変化が必要な時期は、ポジティブなインパクトを生み出す絶好の機会でもあり、学習環境を適切にデザインすることは、今まで以上に重要性を増しています。

この資料では、どのような環境、つまりインフラをデザインするかのヒントとなる考え方や、ベストプラクティスを紹介します。ITの面から実現したい学びを支えるためには、仕様書にどのように要件を記載するかが重要になるため、要件定義にフォーカスを当て、技術的なポイントを中心に話を進めていきます。

すべての生徒を情報につなげるということはつまり、「使いたい時に、使いたい場所で、発達段階に関係なく、準備の必要もなく、取り出したらすぐに」生徒や教職員のみなさんがiPadを使えるということになります。それを実現するには環境、つまりインフラ設計がとても重要です。そしてデザインしたい環境をベンダーやメーカーに伝える方法が仕様書であり、要件定義書になります。

次のページからは、いくつかの視点に分けてネットワーク環境を構成する要素や要件定義に必要なヒントを確認していきましょう。

空間的な学習活動の範囲

学習活動エリアの整理

はじめに生徒や教職員のみなさんが学習活動で利用するエリアという視点で確認していきましょう。生徒の学習活動エリアは主に、普通教室、特別支援学級、少人数教室を含む特別教室、体育館、運動場などの「校内」になります。小中一貫教育のケースや、校種をまたぐ交流などでは、小学校と中学校を一体とした「ブロック」が学習活動に含まれます。教職員の学習活動エリアは、普通教室、特別支援学級、少人数教室を含む特別教室、体育館、運動場に加え、校長室、職員室、事務室、保健室、特別教室の準備室なども「校内」に含まれます。教職員のみなさんも、「ブロック」での活動や、さらに校外学習下見や引率、出張や教科研究交流会などの「校外」での活動もあります。また、「校内」においても、教職員の校務業務の内容に応じて特に機微な情報を取り扱う作業エリアでは注意が必要になります。大切なことは、「いつでも、どこでも、誰にでも、すぐに」生徒や教職員のみなさんが端末を使える環境、つまりインフラをどこまでの範囲で実現するのが適切かを判断することです。そのために、以下の点を確認しておきましょう。

要件定義に向けて役立つヒント

学習エリアを把握する

まず、授業を行う教師のみなさんに、生徒にとって最適な学習活動エリアについてヒアリングを行いましょう。この時、教師のみなさんが成績や病歴などの機微情報を取り扱うエリアもあわせて確認してください。機微情報を取り扱うエリアの中で、生徒の利用エリアと重なる部分があれば、そのエリア内でも校務を止めない利用手段を計画する必要があります。例えば、生徒から目を離せない中、養護教諭が生徒のそばで校務に当たり機微情報を扱うことも考えられます。このようなケースについてもヒアリングし、把握しておきましょう。また、教室の用途変更が生じる可能性がある場合、最新の学校設営図を学校長に確認し、仕様書の変更相談をいつまで受け付けるのかを計画しておくことも重要です。



防災計画や公衆無線Wi-Fiを確認する

学校ごとに策定している防災計画における教室、特に災害フェーズに応じた特別教室の役割も確認しておきましょう。また、行政の危機管理担当からの補助金、あるいは社会貢献事業などで、教育委員会が把握していないアクセスポイントなどの通信機器が学校施設内に設置されているケースも考えられます。公衆無線Wi-FiがフリーWi-Fi化して電波を発出し続けると、昼夜問わず人が集まる場所になることも考えられるため、対象通信機器の設置の有無を確認してください。機器が設置されていることが判明した場合には、設置されている場所とLAN敷設経路を事前に把握し、ネットワーク設計時に考慮するようにしましょう。

校内ネットワークからインターネットへのアクセス方式

学習活動エリアで利用されるネットワーク構成の整理

次に、教室からインターネットへアクセスする経路について確認していきましょう。
公立学校でよく採用されているアクセス方法は以下の5つに分類できます。

1. センター集約方式 (拠点集約方式)
2. ローカルブレイクアウト方式 (インターネットブレイクアウト)
3. 学校直収方式 (拠点分散方式)
4. モバイル通信方式 (Cellular)
5. ハイブリッド方式

具体的に接続方法の特徴を見ていきましょう。

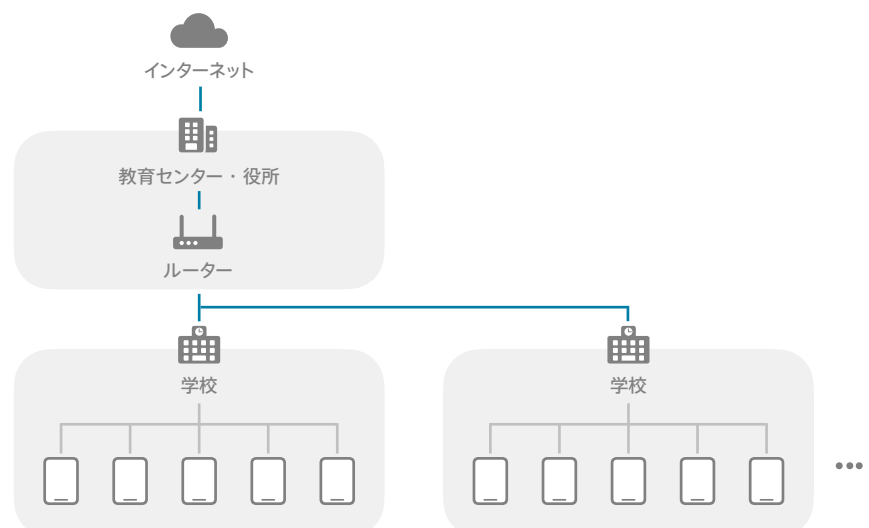
1. センター集約方式 (拠点集約方式)

センター集約方式 (拠点集約方式) とは、全教室のネットワークが校内のコンピュータ教室などに設置されているスイッチ類に集約され、役所や教育センターなどを経由し、インターネットに接続する方法です。この方式には、以下のようなメリットがあります。

- ・ 管理しやすい
- ・ どの学校のどの機器が正常に機能していないかなどを判断しやすい

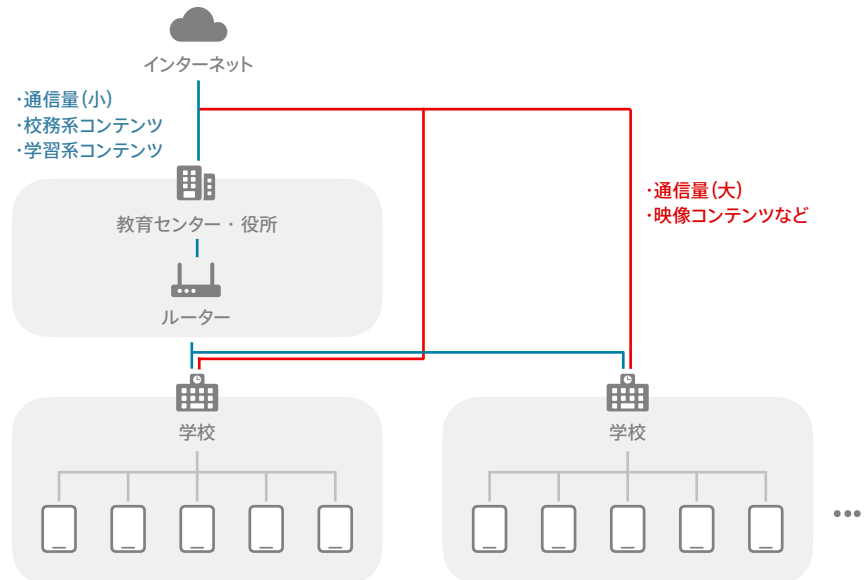
一方で、センター集約方式では、以下の点を考慮する必要があります。

- ・ 大容量アップデート (iPadOS、アプリ) を快適に行うための対策
- ・ 特定機器への集中アクセスや、通信速度の低下など、複数の学校へ広がるトラブルの影響
- ・ 複雑な構成の見直しなどの際にかかる時間と労力



2.ローカルブレイクアウト方式(インターネットブレイクアウト)

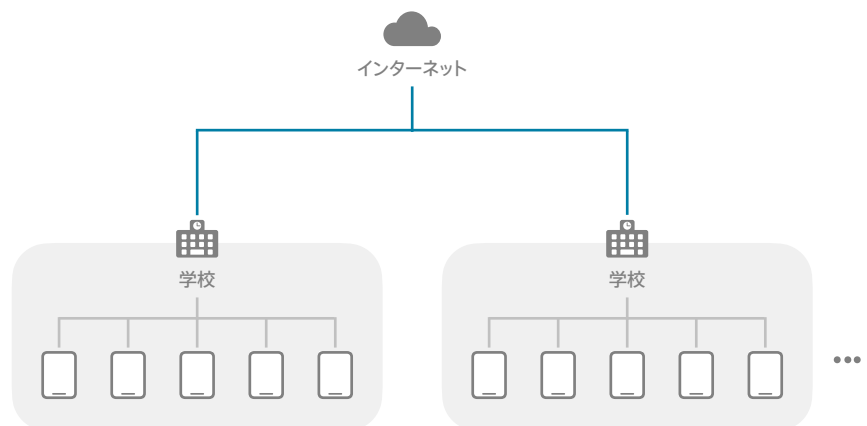
ローカルブレイクアウト方式(インターネットブレイクアウト)とは、センター集約方式(拠点集約方式)を取りつつ、通信量の大きい映像コンテンツなど、特定の通信やサービスは別のインターネット回線を使う方法です。この方式では、集約方式で集中するトラフィックの負荷を軽減できます。ただし、どの通信をブレイクアウトさせるかの検討と、学校の利用状況に応じた定期的なトラフィック量の確認、ブレイクアウトさせる通信の見直しが必要です。



3.学校直収方式(拠点分散方式)

学校直収方式(拠点分散方式)とは、全教室のネットワークが校内のコンピュータ教室などに設置されているスイッチ類に集約され、役所や教育センターなどを経由せずに、各学校から直接インターネットに接続する方法です。

学校単位で通信が集約されるため、トラブルが生じた際に影響が学校内に限定されるメリットがある反面、学校内の機器異常の発生を集中的に把握しづらくなるデメリットもあります。



4.モバイル通信方式(Cellular)

モバイル通信方式とは、校内の通信機器を経由せず、生徒の端末から通信事業者のインターネット回線に直接接続する方法です。この方式には、全学校の生徒数で1か月あたりの通信量をシェアできることに加え、以下のメリットもあります。

- ・生徒たちのあらゆる学習活動エリア(校外、ブロック、校内)で学習活動が可能
- ・生徒用端末から直接インターネットに通信できるため、校内のネットワークの整備負担が軽減される

ただし、OSや大容量アプリのアップデートを行うために、校内にWi-Fi環境の整備が必要かを検討しましょう。

5.ハイブリッド方式

ハイブリッド方式とは、上記の方式のいくつかを組み合わせで接続する方法です。ネットワーク分離により、教職員が利用する校務用端末はセンター集約方式を、生徒用端末はローカルブレイクアウト方式を併用する場合や、通信量が大きな映像コンテンツのみをローカルブレイクアウト方式にする場合があります。

接続方式ごとにメリット、デメリットがあるため、ハイブリット方式ではそれらを補い合うことが可能です。ただし、複数の方式を併用すると、管理工数と管理維持費がかかる点には注意が必要です。

💡要件を実現するためのヒント

校内アクセスポイントの設計と管理

Wi-Fiローミング

iPadを利用するにあたり、Wi-Fiローミングについての理解を深めておきましょう。生徒や教職員のみなさんは時限ごとに学習活動エリアを移動します。その際、教室を移動して前の時限とは異なるアプリやサービスを利用しても、複数のネットワーク機器が切り替わっていることを意識せずに利用することが可能です。このように、ネットワーク機器が切り替わり、自動的にインターネットにつながり続けることをWi-Fiローミングといいます。

iPadは次の条件に基づきローミングを行うタイミングを決定します。

- ・現在の信号強度インジケータ(RSSI)が-70dBmを超える
- ・新しいアクセスポイントのRSSIが現在のアクセスポイントよりも12dB強い(データを送受信していない場合)

※iPad第5世代以降を想定。

これらの値を考慮してネットワークを設計することにより、意図しないローミングの軽減が期待できます。

【参考】 [AppleデバイスでのWi-Fiローミングのサポート](#)

SSIDについて

SSIDは、定期的な変更を検討する必要はありません。SSID名などが表示されていることは問題視せず、セキュリティをきちんと設計すること、アクセスポイントのファームウェアをアップデートすることを重視してください。その際、必ずモデル検証校で確認を進めましょう。

教室などに無線機器を導入する場合

＜既設のアクセスポイント＞

校内でアクセスポイントなどを既設している場合は、無線環境の設定を確認しましょう。特にチャンネルの重複を自動回避できる仕組みで運用できているかをチェックし、実現できていない場合には再設計を行う必要があります。

＜周波数特性と電波干渉物＞

また、周波数特性、電波干渉物やDFS(W53、W56)を設計時に考慮することも必要です。2.4GHzと5GHzとの使い分けにおける利用方針を考慮し、2.4GHzの干渉物(Bluetoothマウス、キーボード、教師のみなさんが使う無線画面投影機器、電子レンジなど)を確認しておきましょう。

また、実際の教室をピックアップして簡易な空間サーベイランスの実施を推奨します。無線の強度確認を委員会で行いたい場合は、iPadでAirMacユーティリティアプリを使ってRSSI測定が可能です。サーベイランスの際に既設無線機器や隣接住居などの干渉の確認ができると、より精緻な設計が実現します。

防災Wi-Fiの導入がある場合

災害時用SSIDの通信先制限、時間制限の有無と方針を確認してください。また、教育用SSIDと災害時用SSID発出エリアも事前に把握しておきましょう。

IPアドレスの設計と管理

レンジごとのIPアドレスの用途を明確にする

IPアドレス体系、サブネットマスクは、両者をうまく利用したシンプルな構成をおすすめします。その際、iPadの台数だけではなく周辺機器、これから導入を検討したいネットワーク機器なども総数に考慮してください。

また、IPアドレスはレンジごとに用途を明確にしておきましょう。特に各教室に設置するICT機器でWi-Fiを利用する場合、管理するIPアドレスが増えるため、IPアドレスが不足しないよう計画、設計することが必要です。

学校行事も考慮する

年間教育計画や行事を想定し、IPアドレスやアクセスポイントのSSIDの設計に反映させましょう。具体的には、生徒と教職員のみなさんをネットワーク上で分けるのか同一にするのか、周辺機器や管理デバイスのネットワークが必要かなどを検討してください。ネットワークを分ける場合、それぞれのアクセスポリシーを設定するかの検討も必要です。

DHCPを利用する場合

DHCPを利用する際は、サーバをどこに設置し、どのような単位(学校、ブロック、建物、フロア)でiPadやApple TVなどの周辺機器を管理するかを検討します。MACアドレスに基づいてユニークに割り当てIPアドレスを定義し、MACアドレス予約を利用することで、問題の切り分けやトラフィック分析を行う際に、端末の特定がしやすくなります。なお、Padはプライバシーを守るため、MACアドレスをランダム化します。この機能はMDMを使って無効にすることもできます。

リース時間

DHCPのリース時間にも注意が必要です。通常、生徒のiPadを接続する教育用SSIDでは、DHCPリース時間は8時間程度にします。公開授業研究会や保護者が来校し、校内のWi-Fiを利用するような行事では、ゲスト用SSIDを発出し、リース時間は行事の内容によって設計してください。多くの場合、1時間から2時間を目安にします。

プロキシサーバあるいはクラウドプロキシを利用する場合

プロキシの特性を理解し、目的と運用方針を明確に整理しておきましょう。特に、プロキシは「代理応答」である点には注意が必要です。代理応答の際に証明書を差し替える場合（SSLインスペクションを行う場合）には、iPadOSやアプリのダウンロードなどで問題が発生します。

セキュリティ面は向上するものの、オンプレミス、クラウド型を問わず、パフォーマンスを見極めることも重要です。モデル校で実証を行い、事前に検証しておくことを推奨します。その際、運用開始後の設定変更のしやすさもあわせて確認しておきましょう。

年度更新作業の効率化を通信機器の設計時に検討

卒業生から回収したiPadを初期化した後、iPadを再設定するにはまずインターネットに接続する必要があります。iPadOS 17以降では、MDM（デバイス管理サービス）からのリモートワイプによる初期化の実行時にコマンドにWi-Fi構成プロファイルを含め、自動でWi-Fi設定を行うことができます（MDMが対応している場合）。ローカルワイプでは、それぞれのデバイス上での操作が必要になるため、リモートワイプを利用することをおすすめします。それぞれのiPad上からローカルワイプによる初期化を行う場合、iPad内に保持されているWi-Fiのプロファイルも初期化されるため、初期化後の初回使用時に校内のWi-Fiに接続する必要があります。MDMからWi-Fi構成プロファイルが配信されると、校内ネットワークに接続できるようになり、そのあとのほとんどの更新作業は自動で行えます。

この初回Wi-Fi接続を校内で行うためには、アクセスポイントの設計、設定を工夫し、年度更新作業時だけ発出するWi-Fi SSID、あるいは防災対策用のWi-Fi SSIDの利用の検討が必要です。これらのSSIDは暗号化キー（パスワード）なしにしておき、インターネット通信可能な宛先を絞り込み用途を限定することでセキュリティを担保します。最低限、以下の宛先にアクセスできる必要があります。

- ・ Appleサーバ群（17.0.0.0/8宛）
- ・ MDMへの登録に必要な宛先ホスト名あるいはIPアドレス

これらを活用すれば、業者の修理などから返却された未設定のiPadも教職員や支援員のみなさんが初期設定して利用可能な状態にすることができます。

アプリ単位での通信可視化

次世代ファイアウォールや統合脅威管理（UTM）製品など、アプリの通信を可視化し、インターネットサービスへの通信を制御可能な機器が導入されている場合や、学校から「アプリが起動しない」、「不安定」などの相談を受けた場合、IT担当者は以下の手順で初期切り分けと操作を行うことができます。

1. 通信流量を確認
2. 必要に応じて通信の帯域幅を変更
3. アプリが利用する通信ポートの確認、変更
4. 送信元IPアドレスと宛先IPアドレスとの確認、通信許可

センター集約方式(拠点集約方式)

ネットワークリソースやIPリソース効率よりも、生徒たちの学習活動エリアを重視し、校内、ブロック、校外のどこで学習活動するかをヒアリング、設計、検討することが大切です。これらを効率良く実現するには、以下のポイントを確認しておきましょう。

- ・ 各教室内、あるいは教室付近の既設アクセスポイントの性能
- ・ 校内のケーブル敷設時期、敷設経路と規格 (Cat5、Cat5e、Cat6など)
- ・ PoEスイッチの配置場所と性能※
- ・ 校内のどの教室にLANケーブルとスイッチが集約されているかの図面と、集約しているスイッチの性能
- ・ 回線業者により、学校から役所、教育センターまで通信している通信方式と帯域などの契約
- ・ 学校内設置端末数と帯域から計算した、おおよその端末通信流量
- ・ 役所、教育センター内のスイッチやファイアウォールなどの構成
- ・ オンプレミス型サーバとの接続をどのスイッチ類が制御しているか
- ・ それぞれのスイッチの役割と性能 (長年の運用においてスイッチ類が階層化、多段構成になっている場合があるため。スイッチ類の必要性、新しい技術の導入を検討し、コスト削減を見込んだ構成も再検討)
- ・ 役所、教育センターのファイアウォールからインターネット回線へ接続する方式と帯域
- ・ 教育委員会が所有するグローバルIPアドレスの数と契約内容
- ・ 学校で集約しているスイッチから役所、教育センターへ接続されず回線業者局舎を経由、集約している場合には、その経路と通信方式、帯域など

※PoEスイッチは、アクセスポイントへの電源供給と電波減衰しないよう増幅機能も担います。

ローカルブレイクアウト、拠点分散方式

ローカルブレイクアウト、拠点分散方式の場合でも、ネットワークリソースやIPリソース効率よりも生徒たちの学習活動エリアを重視し、校内、ブロック、校外のどこで学習活動するかをヒアリング、設計、検討してください。ローカルブレイクアウト、拠点分散方式の場合、以下のポイントを確認しておきましょう。

- ・ 各教室内あるいは教室付近の既設アクセスポイントの性能
- ・ 校内のケーブル敷設時期、敷設経路と規格
- ・ PoEスイッチの配置場所と性能
- ・ 校内のどの教室にLANケーブルとスイッチが集約されているかの図面と、集約しているスイッチの性能
- ・ 学校からのインターネット接続方式や回線数、帯域などの契約
- ・ 学校内設置端末数と帯域から計算した、おおよその端末通信流量
- ・ 各学校拠点にグローバルIPアドレスが払い出されるのか、またその有無に関わらず必要性の検討

モバイル通信方式(Cellular)

モバイル通信方式は、クラウドでの集約管理がしやすいものの、事前に何を集約し管理するかを設計しておく必要があります。

また、モバイル通信方式を採用する場合には、OSなどの大容量アップデートを校内で行えるようにするために、校内Wi-Fiネットワークとコンテンツキャッシュの導入を推奨します。校内でOSや大容量アプリのアップデートを行う場合は、特定の教室に無線環境を整備しましょう。その際、以下の点を事前に検討してください。

検討事項

- ・ 生徒用iPadのアップデートを効率良く進めるための手順
- ・ 学校規模に応じたWi-Fi設置教室数
- ・ OSのメジャーアップグレード、およびマイナーアップデートの適用タイミング

また、生徒の家庭でOSやアプリのアップデートを行う場合、以下の点を検討してください。

- ・ 保護者への承諾と手順策定
- ・ Wi-Fi環境がない家庭への対策
- ・ 生徒用iPadのアップデートを効率良く進めるための手順

モバイル通信方式では、学校内の通信機器が正常に動作しているかの管理は不要ですが、障害発生時の切り分けフローと通信業者、教育委員会、学校担当者の確認、連絡方法は事前に検討しておきましょう。また、生徒が利用する1か月あたりの通信量総量の計算もあわせて行ってください。

ハイブリッド方式

既存のネットワークを温存しなければならず、結果的にハイブリッド方式での運用となるケースも想定されます。それぞれの利用目的を整理し、中長期的な期間でどのように集約、維持していくのかの方針を検討しておきましょう。定期的に新しい技術の導入を検討し、集約、維持の方法を見直すことも必要です。

ネットワーク環境におけるセキュリティ

以前と比べるとセキュリティに対する考え方には大きな変化が見られ、インフラ設計者にも大胆な意識改革が求められています。

GIGAスクール構想初年度には、生徒のクラウドサービス利用やデータ保管場所などが各自自治体で検討され、決定した方針のもと運用が進められてきました。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」でもクラウドサービスの利用についての方針が示されており、このような運用を後押しする内容となっています。

また、適切な環境で適切な認証を行い、校務の機能ごとにアクセスコントロールができるインフラをデザインすれば、教職員のみなさんによるiPadでの校務が視野に入ってきます。iPadを使って協働的、創造的でパーソナルな、素晴らしい学習体験を構築するのみにとどまらず、教職員のみなさんがセキュリティリスクを意識することなく校務を行うことが可能になれば、校務の負荷を解放することにつながります。

生徒や教職員のみなさんが安心して安全に学習活動ができる環境をデザインするために、セキュリティをいくつかの視点から整理していきましょう。「iPadでアプリを起動し、校内ネットワーク(モバイル通信を含む)を経由してインターネットに接続し、サービスにアクセスする」という授業シーンをもとに分類すると、以下のようになります。

1. iPadやアプリのセキュリティ
2. 校内ネットワークのセキュリティ
3. 校内ネットワークからインターネットに接続するセキュリティ
4. 利用サービスでのセキュリティ

特に3と4は技術的なポイントも重要ですが、自治体として学習活動における利便性とセキュリティのバランスをどのようにとるかを考慮し、目的と運用ルールを明確にすることが重要になります。

【参考】 [Appleプラットフォームのセキュリティ](#)

💡 要件を実現するためのヒント

校内ネットワークのセキュリティ

1. 必要な認証の種類と目的の整理

端末ユーザー認証、校内アクセスポイントへの暗号化と認証、利用しているサービスへの認証はすべて個別に必要と考え、すべての暗号化や認証の仕組みと役割を明確にしておきましょう。

2. Wi-Fiのセキュリティ

校内のアクセスポイント、SSIDを利用する際は、最新のセキュリティ(WPA3)に対応したアクセスポイントなどの導入を検討してください。必要なセキュリティプロトコルを検討し、不要なSSIDは発出ししないような設計にする必要があります。その際、年間の学習活動や災害時なども考慮に入れた上で、オペレーションや担当者を策定し、要件に含めておきましょう。なお、SSIDの非表示、ステルスを利用しても、セキュリティが高まることにはつながりません。

また、生徒たちが学習活動で利用するエリアによりWi-Fiの特性は異なるため、適切な周波数帯とチャンネルの設計が必要です。アクセスポイントを効率良く管理できるシステムの導入もあわせて検討してください。

3. 生徒用端末、管理用機器、周辺機器の整理

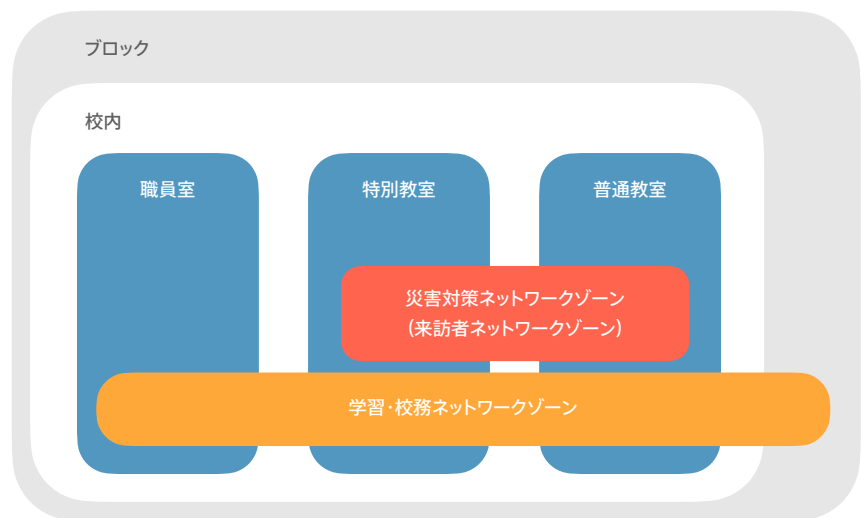
セグメント

各機器を、用途別に年間計画や行事に沿って整理しておきましょう。ブロードキャスト、コリジョンなどによるネットワーク自身への負荷リスクを軽減するために、セグメント(VLAN)を複数用意し、それぞれの利用目的を検討しておきます。この時、セグメントを増やしすぎると管理工数が増えるため、セキュリティの観点から、大きく「生徒用セグメント」「教職員用セグメント」「周辺機器用セグメント」「管理機器通信用セグメント」などに分けて整理しましょう。

また、あらゆる通信が同一セグメント内を通過するのではなく通信用途に分けることで、検証校テストや運用開始後のトラブルを局所的に抑えることができます。そのセグメントの通信をポリシーで管理すると、より安全性が高まります。ゼロトラストのようにセグメントを分けず、異なる手法でセキュリティを担保することも可能です。

ゾーニング

管理、運用面からゾーニングは可能な限り1つとし、生徒の学習活動エリアと教職員の校務エリアを想定しつつ、その中で複数のセグメント、レイヤー構成を検討します。その場合、複数のセグメント間での通信別アクセスコントロールポリシーを検討してください。アクセスコントロールポリシーは、教育委員会の職員や指導主事でも変更可能な手順を検討することで、緊急トラブル時や急ぎの授業、行事への早期対応が可能になります。



4. 1～3のトータルコストとリスク管理を誰がどこまで行うかの方針を検討

自治体職員、指導主事、教職員、ICT支援員、契約先ベンダー、学校への迅速な対応を誰がどこまで行うかの方針の決定と、フローの策定も重要なプロセスです。すべての項目に対し、担当者、タイミング、連絡フロー、許可をする責任者、共有先などの計画をあらかじめ決めておきましょう。

5. 校内ネットワークからインターネットに接続するセキュリティ

「[教育情報セキュリティポリシーに関するガイドライン](#)」の情報資産の分類を行います。その際、生徒の学習活動の妨げにならないような考慮が必要です。また、教職員の校務を止めず、負荷を軽減できるか、どのように情報資産を活用し守るかもあわせて検討してください。

生徒の学習活動の妨げにならないかという観点からよく議論されるのが、調べ学習でのウェブフィルタリングの強度です。「絶対に有害なサイトは見せないこと」を目指すのではなく、指導主事や教師のみなさんと協議しながら指導方針、指導計画を定め、それに即したフィルタリング導入の必要性やアクセス方法を検討するようにしましょう。

教育的配慮をしつつ生徒たちの学習活動の道筋を作り、学習活動を阻害するノイズを減らすための活用を考えることが大切です。対応方針とフィルタリング、チューニングは必ず生じる作業のため、どれくらいの時間で変更でき、どれくらいの負担がかかるかを把握しておきましょう。

6. フィルタリングと監視

フィルタリング

フィルタリングにおいては、まず目的と運用方針を整理しましょう。過度なフィルタリングは、iPadやインターネットのレスポンスに影響を与えます。有害サイトの閲覧制限と学習活動の両立を前提に、生徒たちの学習活動において一定のノイズを減らす役割として捉え、授業や指導の中での対応も検討してください。

一定のフィルタリングを施す場合には、クラウドベースのフィルタリングソリューションによるセーフサーチの強制や、カテゴリ単位でのフィルタリングを活用しましょう。その際、通信速度やレスポンスへの影響が少ないもの、生徒の学習活動を阻害しないものを選定基準にします。

【参考】 [iPadの管理と運用 持ち帰り学習](#) (6～7ページ)

監視ツール

監視ツールの目的と運用方針を明確に整理しておくことも大切です。通信内容を監視、収集するツールの導入は一般的ではなく、生徒のプライバシー保護が困難になります。

利活用への障害にもなるため、教育機関では推奨されるべきではありません。SSLインスペクションなどで通信内容を取得することにより、生徒たちが何をしているかを詳細に把握することもでき、場合によっては犯人探しのような使い方もできてしまいます。そのため、監視ツールを利用する場合には、収集するデータの正しい理解と収集目的、収集データ運用方針の策定および関係者への説明が欠かせません。

7. 利用サービスでのセキュリティ

プライバシーポリシーの確認

利用するサービスのプライバシーポリシーで、生徒のデータがどのように取り扱われるのかを確認しましょう。また、使用するサービス以外の目的で生徒のデータが利用されないことを確認してください。サービス、クラウド基盤の安全性は、以下を基準に判断します。

- ・ 第三者機関認証 (ISO/IEC 27001、27018など) を取得、維持しているか
- ・ クラウド基盤の可用性、冗長性、完全性への対応

また、情報セキュリティインシデントへの対応策の確認とフローの策定も必要です。

パスワードの管理

小学校ではIDとパスワードの運用に工夫が必要です。例えば、サービスアクセス時にIDとパスワードをキーチェーンで記憶させると、生徒の学習活動に負荷をかけずセキュリティを担保することができます。また、発達段階に応じて、一定の強度を持ったパスワードを利用することも重要になります。

中等教育では、生徒が主体的にどのようにパスワードを管理していくか、授業でどのように実践していくかを検討してください。

教職員のみなさんが使うサービスでは、Touch IDのほかに、追加認証用アプリ、多要素認証デバイスなどにより、機微レベルの高い情報を含むサービスへのアクセスを制御することも検討します。

OSおよびアプリの管理

端末などを管理するシステムの選定

MDMの比較検討

各社それぞれに特徴があるため、内容を比較検討してから導入すべきMDMを選定しましょう。MDM選定の意思決定に役立つ基準をいくつか紹介します。

- ・ 宣言型デバイス管理への対応
- ・ 必要な機能への対応
- ・ 最新OSおよび新機能の迅速な対応
- ・ 管理対象となるデバイスのサポート
- ・ Apple School Managerへの対応
- ・ アプリカタログの提供
- ・ ベンダーのサポートおよびトレーニング
- ・ 試用版

ソリューションによっては、無料トライアルを提供している場合があります。可能であれば購入前に必ず試し、実現したいことが簡単に実装できそうかを確認しましょう。例えば、アプリを削除できないようにMDMで設定することにより、生徒が誤ってアプリを削除してしまうことを防ぐことができます。

【参考】 [Appleプラットフォーム導入：デバイス管理サービスを選択する](#)

OSバージョンの管理

iPadOSメジャーアップグレードについての対策

iPadOSのメジャーアップグレードでは、利用している周辺機器やアプリの対応に時間がかかるケースがあるため、これらの対応を確認したあとでメジャーアップグレードを実施するように調整が必要です。

OSアップデート延期の設定

OSのアップデートは最大90日間（デフォルト値は30日間）、延期することが可能です。Appleでは、セキュリティを担保するために、OS、アプリともに可能な限り最新の状態に保つことを推奨しています。

メジャーアップグレードの時期には延期の長さを60～90日に設定しましょう。そのあと、利用している周辺機器やアプリの対応確認が済み次第、延期の長さを通常時に戻します。自治体内でモデル検証校を指定し、利用している周辺機器や主に利用しているアプリの動作検証を行うことを推奨します。

生徒の家庭でアップデートを行う場合

家庭でOSやアプリのアップデートを行う場合には、保護者への承諾と手順策定の検討が必要です。また、Wi-Fi環境がない家庭があることも想定し、その対策を検討しておきましょう。

【参考】 [iPadの管理と運用 OSアップデート](#)

コンテンツキャッシュの活用

モバイル通信方式の場合であっても、特定の教室にWi-Fiネットワークを敷設し、コンテンツキャッシュを導入することを推奨します。学校の規模に応じてWi-Fi設置教室数を検討してください。

また、大容量アップデートの際のダウンロードトラフィックの影響を低減するためにも、校内ネットワークにコンテンツキャッシュを導入することを推奨します。

【参考】 [iPadの管理と運用 コンテンツキャッシュ](#)

アプリの管理

アプリの提供の仕方や管理も、環境をデザインするための重要な要素です。アプリと管理ツールをどのように整理し、要件として検討すれば、生徒や教師のみなさんが使いやすい学習活動につながるかを見ていきましょう。

要件を実現するためのヒント

一般のiPadユーザーは、iPadにインストールされているApp Storeからアプリを選択しインストールを行います。この時、アプリのライセンスはApple Accountに割り当てられます。

一方、教育機関が購入しMDMに登録されたiPadの場合は、MDMからアプリを配布できます。ユーザーがApp Storeからアプリをインストールする必要はありません。MDM管理者はアプリを強制的にインストールすることもできますし、後述の組織内アプリカタログにアプリを登録しておくことで、必要に応じてユーザーがアプリをインストールすることもできます。

アプリ配布の考慮事項

<初期(強制)導入アプリと任意導入アプリの分類>

初期導入アプリは必ず利用するものに限定し、必要最低限になるようにしてください。これにより修理後の再キッティングや年度更新の作業効率を上げることができます。

初期導入アプリのうち、組織内アプリカタログ、フィルタリングアプリなどiPadを利用するために最低限必要なアプリは、ユーザーが手動で削除することがないよう、「削除不可」オプションを設定して配布してください。

<学習活動エリアを意識したアプリの特性を把握>

発達段階を考慮して、主に使うアプリは自治体が選定することが必要です。アプリの中には、インターネットへの接続が不要なもの、常にインターネットの接続が必要なもの、一時的にインターネットの接続が必要となるものの3種類があります。それぞれのアプリがどのタイプに該当するのかを事前に把握しておきましょう。学校のどの場所で学習をするかも関わるため、可能な限りアプリの詳細情報を確認してください。

<アプリの選定方針>

指導主事、教師のみなさんが中心になってアプリを選定することで、授業での操作説明のしやすさにつながり、より安心して利用できるようになります。

＜学校からのアプリ追加申請フロー＞

事前に、学校から教育委員会にアプリの追加を申請するプロセスを策定し、教育委員会内でアプリのライセンスを管理する担当者を決めておくなど、計画的に進めるためのフローを策定しておきましょう。

学校からのリクエストごとに都度インストール対応を行うことはせず、教育委員会が事前に用意したアプリカタログで対応できるかを指導計画とともに聞き取り、案内してください。

また、アプリの購入を将来的に学校やブロック単位でできるような設計の検討も大切です。Apple School Managerでは場所単位でライセンスが蓄積されるため、場所、ユーザー、権限の設定を計画、検討する必要があります。Apple School ManagerとMDMの担当者を決め、手順書を作成し、説明を行いましょう。

このようなフローを検討することは、将来的に教育委員会の担当者の作業負担を軽減することにつながります。

＜組織内アプリカタログの活用＞

発達段階に応じてアプリを検討していくと、たくさんのアプリが候補に上がり、教科も考慮に入れると100から200ほどになることもあります。それらのアプリのインストール時には、MDMベンダーが提供しているアプリカタログを活用しましょう。

アプリカタログでは、App Store内から管理者が指定したアプリのみをカタログ化し、iPadユーザーが必要に応じてインストールすることが可能です。特定の学年、教科、活動の間だけ利用するアプリなど、一部のiPadユーザのみが利用するアプリの配布に適しています。

MDMベンダーによっては、アプリカタログの中でアプリのカテゴリをセットして分類することも可能です。アプリカタログを活用すれば、ユーザーが任意のタイミングでインストールや削除を手動で行えるため、iPadのストレージ容量不足にも対応できます。

＜特別な支援を要する生徒向けの個別アプリ管理＞

特別支援学校や学級では、管理対象外の個人iPadを購入し、保護者のみなさんが作成した一般のApple Accountを用いて運用するケースもあります。

＜アプリライセンス資産の所有権＞

アプリは、導入時も含め自治体側で一括購入するため、教育委員会の資産となります。Apple School ManagerとMDMを利用すると、転出した生徒や卒業生が使っていたアプリライセンスを、新しい生徒用として再利用することが可能です。

有償のアプリを学級費など保護者負担で運用する場合は、卒業や転出後はアプリが使えなくなることなど、事前に留意点を保護者のみなさんに伝えておくとい良いでしょう。

関連資料

「AppleデバイスでのWi-Fiローミングのサポート」

support.apple.com/ja-jp/HT203068

「Wi-FiルーターとWi-Fiアクセスポイントの推奨設定」

support.apple.com/ja-jp/102766

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」

next.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

「Appleプラットフォームのセキュリティ」

support.apple.com/ja-jp/guide/security

「iPadの管理と運用 持ち帰り学習」

apple.co/takingipadhome_JA

「Appleプラットフォーム導入 - デバイス管理サービスを選択する」

support.apple.com/ja-jp/guide/deployment/dep1d7afa557

「iPadの管理と運用 OSアップデート」

apple.co/osupdate_JA

「iPadの管理と運用 コンテンツキャッシング」

apple.co/contentcaching_JA