

実践的な教育ネットワーク整備ガイド

<設計・運用編>



一般財団法人 全国地域情報化推進協会
アプリケーション委員会
教育ワーキンググループ

2016年3月

第0.9版（案）

目次

1.	はじめに	1
1.1.	本書の位置付け、読み方	1
1.2.	目指す姿	1
1.3.	前提条件	2
1.3.1.	対象校	2
1.3.2.	対象とする範囲	2
1.3.3.	想定する端末数	3
1.3.4.	検討するネットワーク機器類とセキュリティの考察範囲	3
1.4.	教育ネットワーク全体像イメージ	4
1.4.1.	ネットワークインフラストラクチャ	6
1.4.2.	授業支援系ネットワーク	7
1.4.3.	校務支援系ネットワーク	9
2.	構築に必要な設計要件	11
2.1.	構成要素の設計要件	11
2.1.1.	帯域(快適な利用に必要な考え方)	12
2.2.	無線LAN	14
2.2.1.	高速通信	14
2.2.2.	安定した通信接続	15
2.2.3.	セキュリティ対策	16
2.2.4.	状態把握、見える化	16
2.2.5.	技術的な仕様/機能の詳細解説	16
2.3.	有線LAN	21
2.3.1.	LANの広帯域化	21
2.3.2.	最適なトラフィック処理	21
2.3.3.	システム帯域管理	22
2.4.	WAN(自治体WAN、キャリア回線、インターネットVPN)	23
2.5.	データセンタ	24
2.6.	データの保存場所	25
2.7.	セキュリティ対策	26
2.7.1.	教育ネットワークにおけるセキュリティ対策の基本的な考え方	26
2.7.2.	教育ネットワークにおけるセキュリティ対策の基本的な要件	26
2.7.3.	セキュリティ対策と重要性の認識	29
3.	ネットワーク機器に要求される技術	31
3.1.	物理分離、論理分離、仮想化	31
3.2.	冗長化	31
3.2.1.	論理多重	32
3.3.	サービスの品質確保	32
3.3.1.	通信容量	33
3.4.	保守・交換容易性	34
4.	物理配線	35
4.1.	屋内配管・配線	35
4.1.1.	ルート調査	35
4.1.2.	ルート設計(光ファイバー)	35
4.1.3.	ルート設計(メタル)	35
4.1.4.	ルート設計(共通)	35

4.1.5.	準備工事(養生・搬入路の確保)	36
4.1.6.	配線工事留意点	36
4.1.7.	建設業法上の留意点	36
4.2.	無線	39
4.2.1.	設置場所	39
4.2.2.	干渉源、遮蔽物による影響	39
4.2.3.	アンテナ	39
4.2.4.	APの堅牢性	39
5.	運用に必要な要件	40
5.1.	アプリケーション・データの設置場所に必要な運用要件	40
5.1.1.	データセンタ、クラウドなど	40
5.2.	ネットワークの運用に必要な要件	40
5.2.1.	SLA	40
5.2.2.	システム状況の外部公開	42
5.2.3.	ヘルプデスク	42
5.2.4.	オンサイト保守	43
5.3.	教育利用者特有の運用要件	43
5.3.1.	システム委託事業者のアカウント管理	44
5.3.2.	ICT支援員	44
5.3.3.	PTAの利用	44
5.3.4.	学校の敷線管理	44
5.3.5.	教育委員会	44
5.3.6.	学校	44
5.3.7.	外部組織への業務委託	44
6.	利用シーンによるバリエーションの選択要件	45
6.1.	キャッシュサーバおよび学内専用サーバ設置検討	45
6.1.1.	デジタル教科書	45
6.1.2.	ファイルサーバ	45
6.2.	授業支援系ネットワークの利用シーン別検討事項	45
6.2.1.	環境準備	45
6.2.2.	一斉授業	46
6.2.3.	個別学習	46
6.3.	校務支援系ネットワークの利用シーン別検討事項	46
6.3.1.	校務支援システムの利用	46
6.4.	災害時避難場所として利用する場合	47
6.4.1.	無線LAN環境、インターネットアクセスの提供	47
7.	利用拡大に向けた留意事項および補強のポイント	48
7.1.	整備のシナリオに影響を与える事項	48
7.2.	ICT環境整備のパターン例	49
7.3.	整備の具体的な考え方	50
7.3.1.	ユースケースについての考え方	51
7.3.2.	ネットワークへの影響と構築上の留意点	53
7.4.	その他の留意事項	53
7.4.1.	可搬型無線LANについて	53
7.4.2.	防災拠点对応	53
7.5.	経年保存	54
8.	教育ネットワーク導入事例・活用事例	57

8.1.	古河市事例(セルラーモデル).....	57
8.1.1.	セルラーモデル導入メリット.....	57
8.1.2.	セルラーモデル導入の注意点.....	58
8.1.3.	苦労した点.....	58
8.1.4.	導入時の検討事項.....	58
8.1.5.	今後の課題.....	58
9.	付録.....	59
9.1.	用語集.....	59

本書について	目指す姿(1.2)	
	本書記述の前提条件(1.3)	
ICT環境構築	ネットワーク構築	全体像(1.4)
		帯域設計(2.1.1)
		無線LANの設計(2.2)
		有線LANの設計(2.3)
		WANの設計(2.4)
		データセンタについて(2.5)
	データ	データの保存場所(2.6)
	ネットワークセキュリティ(2.7)	考え方(2.7.1)
		分離(3.1)
	物理配線工事(4)	無線LAN(2.2.3)
学校内工事(4.1)		
通信機器への要求技術	分離(3.1)	
	冗長性(3.2)	
	無線LAN(2.2.5)	
ICT環境の運用	データ設置場所(5.1)	データセンタ、クラウド(5.1.1)
	ネットワーク運用(5.2)	SLA(5.2.1)
	ヘルプデスク(5.2.3)	
	教育ICT特有の運用(5.3)	委託業者の認証(5.3.1)
ICT支援員(5.3.2)		
教育独自の検討(5.3)	利用シーンでの追加検討(6)	整備手順
	ICT利用の範囲拡大(7)	拡大整備のパターン(7.2)
		経年利用と保存に関する規定(7.5)
	事例(8)	セルラーモデル(8.1)

1. はじめに

先行して始まった校務情報化にともなう職員室を中心とした環境整備に加え、近年の大きな流れとして教科指導における情報通信の利活用に取り組む自治体が増えている。また、学習記録データの活用や校務データの連携高度化なども模索され始めており、従来にも増して総合的な教育ICT環境整備へのニーズが高まってきている。

これらのムーブメントを背景として一般財団法人全国地域情報化推進協会(APPLIC)教育WGは、教育ICT環境整備の実践に必要となる情報の提供に取り組むこととしている。今回は、端末～クラウドまでを範囲としたネットワークに関する環境整備情報をまとめるものである。

1.1. 本書の位置付け、読み方

本書は、これから教育ネットワークを整備・運用する、および既に整備・運用しているが教育ネットワークの増強やセキュリティ強化を検討する自治体・教育委員会・学校関係者向けに、設計要件、ネットワーク構築要件、およびセキュリティ要件を記載する技術的な情報提供書となることを目指している。

自治体・教育委員会で仕様書の作成など調達を担当する組織や構築や運用を担当する事業者を主な読者とし、教育ネットワークの検討に必要な具体的な要件をまとめている。

例えばネットワークは、使用するアプリケーションが必要とするスペックやコンテンツのファイルサイズ、それらが格納される場所、端末からアプリケーションやコンテンツまでの回線速度、同時利用人数を考慮の上設計するが、設計したデータ量を超える場合や十分なネットワーク帯域を確保できない場合のキャッシュ機能導入など代替手段についても一部言及している。

1.2. 目指す姿

急速に進展する「ICTを活用した教育の情報化」の取組により、従来型のコンピュータ教室にはなかった新たな利活用シーンの実現や環境整備へのニーズがますます高まっている。

反面、無線LANで教育ネットワークに接続したタブレット端末から、授業の中でインターネットから配信される良質な動画を児童・生徒がそれぞれに視聴するなどの新たな利用シーンは、教育で利用するICT環境整備における様々な課題を顕在化させた。不安定な無線LANやスピードの遅いネットワークなどは、改善が必要とされる課題となっている。

特に、文部科学省の定める「教育のIT化に向けた環境整備4か年計画」¹のパンフレットで目標とする整備水準で、問題なく利用できるネットワーク環境の整備は急務となっている。

同時にICTの活用が進むにつれて、セキュリティ上脅威となる事象とそれに対する対策手段を講ずることが必須となっている。教職員や児童・生徒が安心・安全に利用し、運用するIT管理者の負担を極力軽減する教育ネットワークが必要である。

¹ 「教育のIT化に向けた環境整備4か年計画」パンフレット <http://jouhouka.mext.go.jp/school/pdf/2014ICT-panf.pdf>

「より効果的な授業を行うために 学校のICT環境を整備しましょう！ 教育のIT化に向けた環境整備4か年計画」

1.3. 前提条件

本書は、これから第一歩を踏み出そうとする自治体・教育委員会にもわかりやすく情報提供することを目指していることから、下記①～③を前提に各種情報を取りまとめている。

- ① 「教育のIT化に向けた環境整備4か年計画」パンフレットの目標水準で問題なく利用できること、をベースラインとして各種要件を取りまとめている。全校一人1台タブレットPCを利用する場合などは、本書の情報を参考に個別の検討が必要となる。
- ② セキュリティはそれぞれの自治体で定める指針に準ずる必要がある。セキュリティの専門部署へ事前に相談することをお勧めする。
- ③ 本書は小中学校での利用をイメージして記載されている。高等学校における利用で特別に留意が必要な部分のみ高等学校向けの情報として追記している。

1.3.1. 対象校

小学校、中学校、高等学校、特別支援学校を対象校としている。ただし、特に高等学校における専門科など、専門性が高くネットワークに特別な負担がかかることが想定される学校での利用に関しては個別の検討が必要である。

1.3.2. 対象とする範囲

いわゆる「授業」で利用するネットワーク(以下、授業支援系ネットワークと呼ぶ)と「校務」で利用するネットワーク(以下、校務支援系ネットワークと呼ぶ)を対象としている。

(1) ネットワーク範囲

端末～クラウド間を対象範囲としている。

(端末そのもの、およびクラウドそのものについては必要最小限の記載にとどめている)

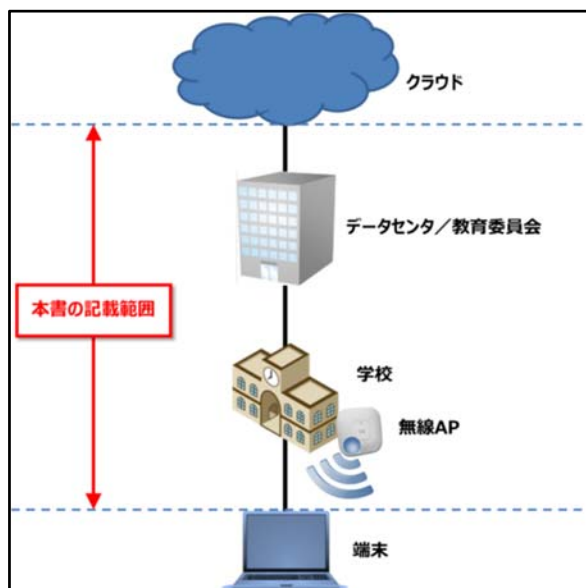


図 1-1 本書が対象とする範囲

(2) セキュリティ範囲

上記、ネットワークと同じ範囲を対象としている。

1.3.3. 想定する端末数

本書で記載する教育ネットワークは、1学校あたりの端末数および同時接続数が以下に示す台数を想定している。

「教育のIT化に向けた環境整備4か年計画」の整備水準を、以下と解釈。

83台 = 生徒端末40台 × 2教室 + 教師端末1台 × 2教室 + ICT支援員端末1台 × 1教室

端末数 …………… 約100台

同時接続数 …… 約100台

1.3.4. 検討するネットワーク機器類とセキュリティの考察範囲

教育ネットワークを構成する機器類毎にセキュリティ上考慮すべき管理項目と期待できるセキュリティ対策項目を下表に示す。本書では、これらの管理が教育ネットワークの運用部門においてなされることを前提として技術的な部分の記載を進めることとする。

表 1-1 機器別セキュリティ上考慮すべき項目

ネットワーク機器類	セキュリティ	侵入制限	持出し制限 データ漏洩	利用制限	対策実施手段の一例	校務支援系 ネットワーク	授業支援系 ネットワーク
サーバ (DC/クラウド)	利用履歴管理			●	認証等	●	●
	利用権限管理		●	●		●	●
	設定変更など管理者権限管理	●	●		管理ポリシー	●	●
ルータ	設定変更など管理者権限管理	●			管理ポリシー	●	●
コア/建屋/ フロアスイッチ	端末接続制限(持ちこみ端末)	●			[例：認証or証明書]	●	●
	設定変更など管理者権限管理	●		●	管理ポリシー	●	●
無線AP	端末接続制限(持ちこみ端末)	●		●	[例：認証or証明書]	●	●
	設定変更など管理者権限管理	●		●	管理ポリシー	●	●
WAN回線	盗聴防止		●		暗号化VPN	●	
	外部からの侵入	●			FW、IPS/IDS、WAFなど	●	●

1.4. 教育ネットワーク全体像イメージ

自治体によって名称や分け方が異なるケースもあるが、各学校や教育委員会では大まかに①授業、②校務、③行政事務の業務で利用するネットワークが必要とされている。これらは必要とされる通信量、それぞれの通信に含まれる情報内容、情報内容を扱うためのセキュリティレベルなどの通信特性が異なることから物理的もしくは論理的に別けて構成することが望ましく、本書では、それぞれの業務に対応したネットワークを下記名称で呼んでいる。

表 1-2 学校／教育委員会で必要とされるネットワーク

名称		概要と特徴
教育ネットワーク	①授業支援系ネットワーク	<ul style="list-style-type: none"> ・ 普通教室や特別教室でタブレット PC などを活用した授業で利用するネットワーク ・ 調べ学習に伴うインターネット接続や、デジタル教科書／教材などの視聴、授業支援システムでの活用など、利用用途は様々 ・ タブレット PC の一斉利用、動画教材の一斉視聴などバースト的に発生する通信にも安定して活用できることが求められる ・ 今後、授業における ICT の活用が更に推進されると考えられることから、利用シーンや利活用の度合い、展開する学校数などによる継続的なネットワーク強化と、それに柔軟に対応できる構成とすることが必要
	②校務支援系ネットワーク	<ul style="list-style-type: none"> ・ センターサーバ型の校務支援システムを代表とした校務事務で利用するネットワーク ・ 機微情報を扱うため求められるセキュリティレベルが高く、インターネットへのオープンな接続は許容していない ・ 校務支援システムの導入が進むにつれ、近年では職員室のみではなく普通教室からの利用ニーズも高まってきている
行政ネットワーク		<ul style="list-style-type: none"> ・ 行政事務で利用するネットワークの総称 ・ 行政事務で必要とされるセキュリティポリシーにて運用される ・ 使用する行政システム毎に更にネットワークが細分化されている場合もある

上記①および②を総称して「教育ネットワーク」と呼び、全体イメージと①②の分離構成イメージをそれぞれ図 1-3、図 1-2に掲載している。また後段で必要とされる技術的な要件や仕様を中心に記述していくが、①②それぞれに以下の点が重要なポイントになると考えられる。

- ① 授業支援系ネットワーク … 「無線 LAN」「ネットワーク帯域」「一次保存機能（キャッシュ）の配置」
- ② 校務支援系ネットワーク … 「セキュリティ確保」「校内 LAN」

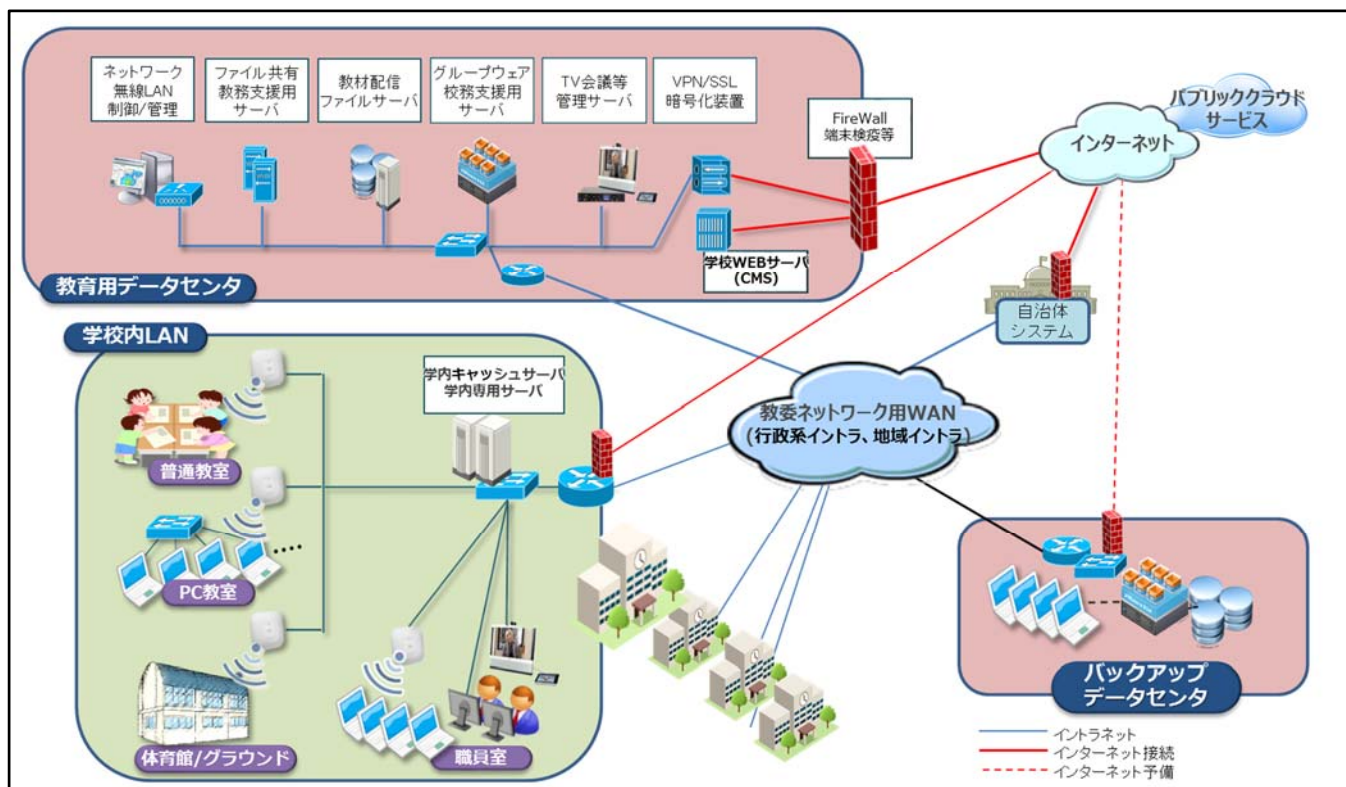


図 1-2 教育ネットワークの全体イメージ例

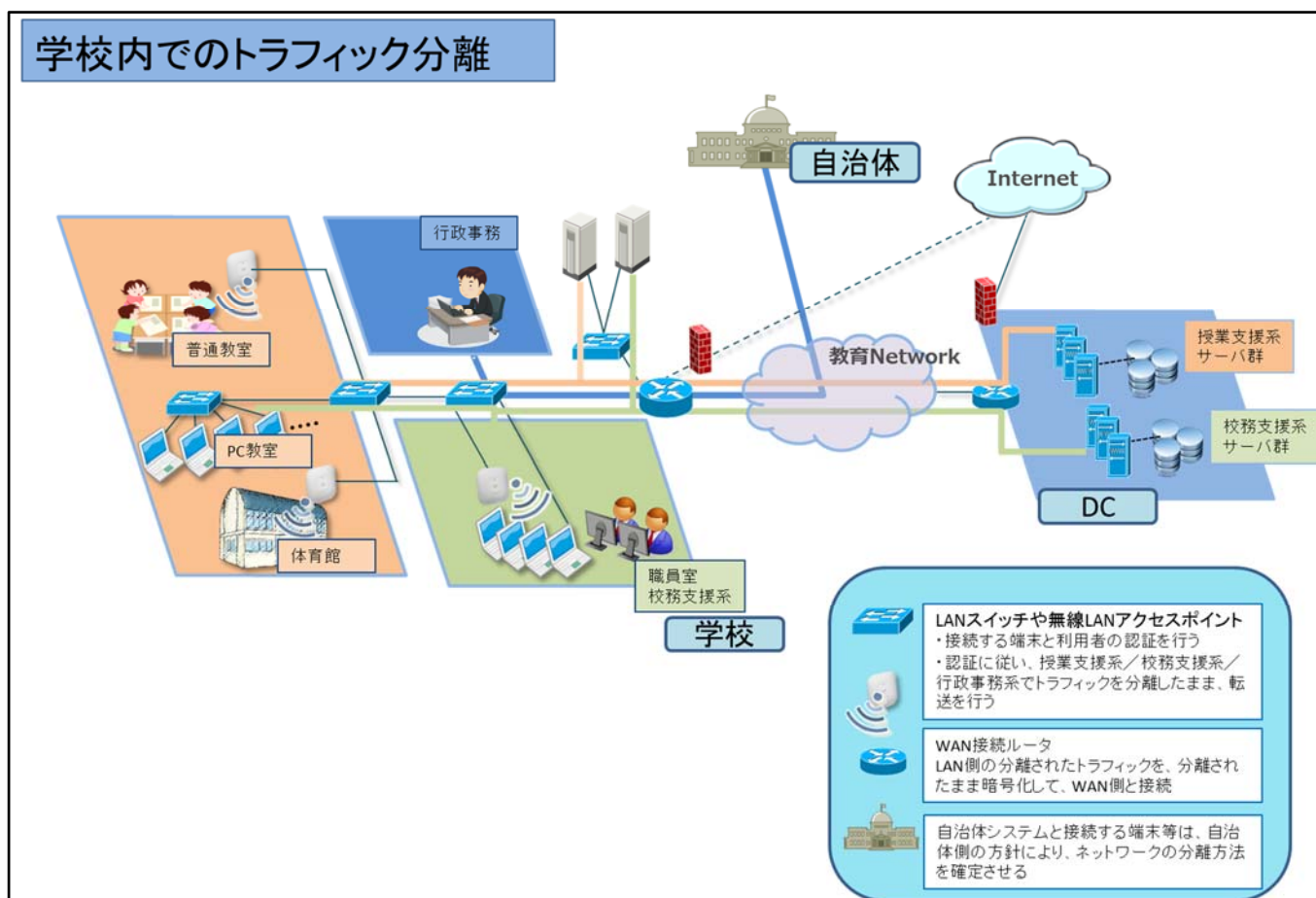


図 1-3 授業支援系ネットワークと校務支援系ネットワークの分離イメージ

1.4.1. ネットワークインフラストラクチャ

授業支援系／校務支援系ネットワークを支えるインフラストラクチャは下記の4つのケースが考えられるが、将来的な利活用計画や拠点(学校)数、および情報セキュリティポリシーなどから、情報システム部門や情報セキュリティ部門と連携しそれぞれの自治体毎に最適なインフラストラクチャを選択もしくは組合せて利用することが重要である。

表 1-3 授業支援系／校務支援系ネットワークを支えるインフラストラクチャ

項番	ネットワークインフラストラクチャ	備考
①	教育ネットワーク専用のインフラストラクチャを利用	授業支援系ネットワークに見られる例
②	行政系ネットワークのインフラストラクチャを共同利用	校務支援系ネットワークに見られる例
③	情報ハイウェイのような地域イントラストラクチャをインフラストラクチャとして利用	高等学校で利用するネットワーク等に見られる例
④	インフラストラクチャは構成せず、商用回線で必要な拠点間を接続	比較的小規模自治体に見られる例

一般的に共通のインフラストラクチャに複数のネットワークを構成するほうがより経済性は高くなるが、セキュリティレベルや利用帯域が制限される場合もあることから、特にバースト性の高い授業支援系ネットワークはあらかじめ上表の①や④を選択肢として検討するなどの留意が必要である。

1.4.2. 授業支援系ネットワーク

下表は、授業支援系ネットワークの代表的な構成例である。将来の利活用計画や想定する利用シーン、学校数、共同利用の有無などから自治体に応じたネットワークを構成することが重要である。

表 1-4 授業支援系ネットワークの類型パターン

1	タイプパターン	特色	イメージ
1	イントラ型 (独自センタ設置)	<ul style="list-style-type: none"> ・教育委員会が独自に設置したデータセンタに必要な機能を格納 ・必要な資産を所有するオンプレミス型での整備 ・必要な機能はデータセンタに格納しているので、インターネット回線のボトルネックは発生しにくい ・セキュリティを一括してマネジメントが可能 ・集約効果の高い大規模自治体に適している ・柔軟な設備変更に課題がある（他システム等への影響の考慮が必要） 	
2	イントラ型 (クラウドセンタ利用)	<ul style="list-style-type: none"> ・インターネットから必要なサービスを利用、かつ、イントラネット経由で接続 ・資産を所有しないサービス利用型での整備 ・必要な機能はインターネットからサービスとして提供されるため、インターネット回線のボトルネックに注意が必要 ・インターネットを経由してクラウドセンタに接続するため、十分にセキュリティ対策を考慮する必要がある 	
3	個別接続型 (クラウドセンタ利用)	<ul style="list-style-type: none"> ・インターネットから必要なサービスを利用、かつ教育委員会・学校からそれぞれに接続 ・資産を所有しないサービス利用型での整備 ・必要な機能がインターネット経由で提供されるが分散して接続されるため、回線のボトルネックは発生しにくい ・教育委員会・学校毎で拠点単位のセキュリティ対策が必要 ・インターネットを経由してクラウドセンタに接続するため、十分にセキュリティ対策を考慮する必要がある ・スモールスタートができる 	
4	個別接続型 (インターネット接続のみ)	<ul style="list-style-type: none"> ・インターネットに接続しているがサービスなどの利用はない ・必要な機能を学校ごとに配置する必要がある（所有する資産を拠点ごとに配置するオンプレミス型での整備） ・分散してインターネットに接続されるため、回線のボトルネックは発生しにくい ・教育委員会・学校毎で拠点単位のセキュリティ対策が必要 ・スモールスタートができるが、拠点単位での運用保守が必要 	

表 1-5 授業支援系ネットワークの代表的な利用シーン

項目	概要				
環境準備	普通教室での使用に備えた環境準備				
	環境復元ソフトウェア				
	VDI				
	MDM				
	OSのアップデート				
	教材配布・授業準備				
	アプリケーションのインストール・アップデート				
一斉授業	クラス全員に課題・教員画面を配付・転送し、各自が検討して書込み・発表				
	教員による教材の提示 電子黒板、実物投影機等を用いた分かりやすい課題の提示 ※指導者用デジタル教科書の使用				
グループ学習	発表や話し合い…考えや作品を提示・交換しての発表や話し合い 協働での意見整理…複数の意見や考えを議論して整理 協働制作…グループでの分担や協力による作品の制作 クラス全体に課題を配付し、各自が検討して書込み・発表				
	<table border="1" data-bbox="323 909 1461 1005"> <tr> <td data-bbox="323 909 815 960">電子黒板と端末での利用</td> <td data-bbox="815 909 1461 960">ネットワークが校外に出る運用。グループで実施</td> </tr> <tr> <td data-bbox="323 960 815 1005"></td> <td data-bbox="815 960 1461 1005">ネットワークが校外に出ない運用。グループで実施</td> </tr> </table>	電子黒板と端末での利用	ネットワークが校外に出る運用。グループで実施		ネットワークが校外に出ない運用。グループで実施
	電子黒板と端末での利用	ネットワークが校外に出る運用。グループで実施			
		ネットワークが校外に出ない運用。グループで実施			
	<table border="1" data-bbox="323 1005 1461 1057"> <tr> <td data-bbox="323 1005 815 1057">写真・動画・作品アップロード</td> <td data-bbox="815 1005 1461 1057">グループ単位で成果物をアップロード</td> </tr> </table>	写真・動画・作品アップロード	グループ単位で成果物をアップロード		
	写真・動画・作品アップロード	グループ単位で成果物をアップロード			
	<table border="1" data-bbox="323 1057 1461 1153"> <tr> <td data-bbox="323 1057 815 1153">動画視聴</td> <td data-bbox="815 1057 1461 1153">YouTube, NHK for School等を使用しグループ単位で視聴</td> </tr> </table>	動画視聴	YouTube, NHK for School等を使用しグループ単位で視聴		
動画視聴	YouTube, NHK for School等を使用しグループ単位で視聴				
<table border="1" data-bbox="323 1153 1461 1205"> <tr> <td data-bbox="323 1153 815 1205">遠隔・協働学習（グループ・テレビ会議）</td> <td data-bbox="815 1153 1461 1205">遠隔地の離れたグループと協働学習</td> </tr> </table>	遠隔・協働学習（グループ・テレビ会議）	遠隔地の離れたグループと協働学習			
遠隔・協働学習（グループ・テレビ会議）	遠隔地の離れたグループと協働学習				
<table border="1" data-bbox="323 1205 1461 1240"> <tr> <td data-bbox="323 1205 815 1240">調べ学習</td> <td data-bbox="815 1205 1461 1240">インターネットを使用してグループで実施</td> </tr> </table>	調べ学習	インターネットを使用してグループで実施			
調べ学習	インターネットを使用してグループで実施				
個別学習	表現・制作…マルチメディアによる表現・制作 思考を深める学習…シミュレーション等を用いた考えを深める学習（英会話等） 調査活動…インターネット等による調査 個に応じる学習…一人一人の習熟の程度等に応じた学習（ドリル教材等） ※児童・生徒用デジタル教材所の使用				
	<table border="1" data-bbox="323 1471 1461 1568"> <tr> <td data-bbox="323 1471 815 1523">電子黒板と端末での利用</td> <td data-bbox="815 1471 1461 1523">ネットワークが校外に出る運用。児童・生徒それぞれが実施</td> </tr> <tr> <td data-bbox="323 1523 815 1568"></td> <td data-bbox="815 1523 1461 1568">ネットワークが校外に出ない運用。児童・生徒それぞれが実施</td> </tr> </table>	電子黒板と端末での利用	ネットワークが校外に出る運用。児童・生徒それぞれが実施		ネットワークが校外に出ない運用。児童・生徒それぞれが実施
	電子黒板と端末での利用	ネットワークが校外に出る運用。児童・生徒それぞれが実施			
		ネットワークが校外に出ない運用。児童・生徒それぞれが実施			
	<table border="1" data-bbox="323 1568 1461 1619"> <tr> <td data-bbox="323 1568 815 1619">写真・動画・作品アップロード</td> <td data-bbox="815 1568 1461 1619">個人単位で成果物をアップロード</td> </tr> </table>	写真・動画・作品アップロード	個人単位で成果物をアップロード		
	写真・動画・作品アップロード	個人単位で成果物をアップロード			
	<table border="1" data-bbox="323 1619 1461 1715"> <tr> <td data-bbox="323 1619 815 1715">動画視聴</td> <td data-bbox="815 1619 1461 1715">YouTube, NHK for School等を使用しお手本教材等を個人単位で視聴</td> </tr> </table>	動画視聴	YouTube, NHK for School等を使用しお手本教材等を個人単位で視聴		
動画視聴	YouTube, NHK for School等を使用しお手本教材等を個人単位で視聴				
<table border="1" data-bbox="323 1715 1461 1767"> <tr> <td data-bbox="323 1715 815 1767">遠隔・協働学習</td> <td data-bbox="815 1715 1461 1767">離れた児童・生徒と個人単位で協働学習</td> </tr> </table>	遠隔・協働学習	離れた児童・生徒と個人単位で協働学習			
遠隔・協働学習	離れた児童・生徒と個人単位で協働学習				
<table border="1" data-bbox="323 1767 1461 1818"> <tr> <td data-bbox="323 1767 815 1818">調べ学習</td> <td data-bbox="815 1767 1461 1818">インターネットを使用して児童・生徒それぞれが実施</td> </tr> </table>	調べ学習	インターネットを使用して児童・生徒それぞれが実施			
調べ学習	インターネットを使用して児童・生徒それぞれが実施				
<table border="1" data-bbox="323 1818 1461 1850"> <tr> <td data-bbox="323 1818 815 1850">ドリル学習</td> <td data-bbox="815 1818 1461 1850">ドリル教材等を児童・生徒それぞれが実施</td> </tr> </table>	ドリル学習	ドリル教材等を児童・生徒それぞれが実施			
ドリル学習	ドリル教材等を児童・生徒それぞれが実施				

1.4.3. 校務支援系ネットワーク

下表は、校務支援系ネットワークの代表的構成例である。求められるセキュリティ、学校数、共同利用の有無などから自治体に応じたネットワークを構成することが重要である。

表 1-6 校務支援系ネットワークの類型パターン

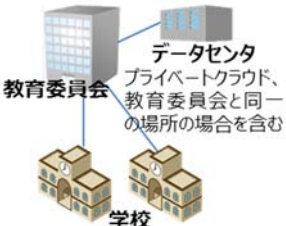
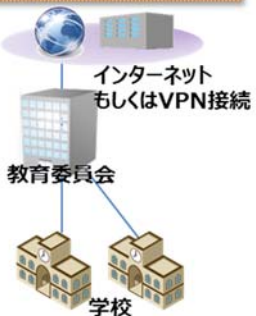
1	タイプパターン	特徴	イメージ
1	イントラ型 (独自センタ設置)	<ul style="list-style-type: none"> 教育イントラに直接接続する独自のデータセンタに校務支援システムをオンプレミス型での整備（資産を所有） インターネット回線のセキュリティ対策は不要、かつセキュリティを一括してマネジメントが可能 集約効果の高い大規模自治体に適している 	<p>教育イントラに直接接続するデータセンタにプライベートクラウドとして整備</p> 
2	イントラ型 (クラウドセンタ利用)	<ul style="list-style-type: none"> 資産は所有せず、校務支援システムをクラウドサービスとしてイントラネット経由で接続して利用 インターネットを経由してサービスを利用するため、VPN 接続で閉域性を高めるなど十分にセキュリティ対策を施す必要がある 	<p>校務クラウドサービスを教育インフラ経由で接続し利用</p> 
3	個別接続型 (クラウドセンタ利用)	<ul style="list-style-type: none"> 資産は所有せず、校務支援システムをクラウドサービスとして教育委員会・学校からそれぞれに接続して利用 教育委員会、学校ごとに拠点単位のセキュリティ対策が必要 インターネットを経由してサービスを利用するため、VPN 接続で閉域性を高めるなど十分にセキュリティ対策を施す必要がある スモールスタートができる 	<p>校務クラウドサービスを教育拠点それぞれから接続し利用</p> 
4	個別接続型 (インターネット接続のみ)	<ul style="list-style-type: none"> 校務支援システムを学校ごとに配置したサーバから利用し、ネットワーク化していないオンプレミス型の整備 教育委員会、学校ごとに拠点単位のセキュリティ対策が必要 スモールスタートができるが、拠点単位での運用保守が必要 	<p>学校毎に利用し、ネットワーク化していない</p> 

表 1-7 校務支援系ネットワークの代表的な利用シーン

項目	概要
環境準備	VDI
	OSアップデート
	アプリケーションのインストール・アップデート
校務処理	学期末における通知表の作成・印刷
	入試出願前における調査書等の作成・印刷
	年度末における指導要録等の作成・印刷 [※]

※校務処理の各種帳票の作成・印刷が最もネットワーク負荷がかかりそうだが、プリンタ出力自体がボトルネックといえる場合、ネットワーク帯域は問題とならない。

2. 構築に必要な設計要件

ICT環境を快適に利用する為、構築の段階で、流れるデータの量やデータの場所に応じた設計が必要となる。特に学校においては、児童・生徒の一斉利用などで、集中(バースト)的にデータが流れることがあるため、注意が必要となる。

- どのようなデータ(データ種類やサイズ)を利用するか
- どのくらいの端末台数が同時利用するか
- どのくらいの快適さ(表示速度など)を求めるか
- どこ(サーバの場所)にデータを置くか

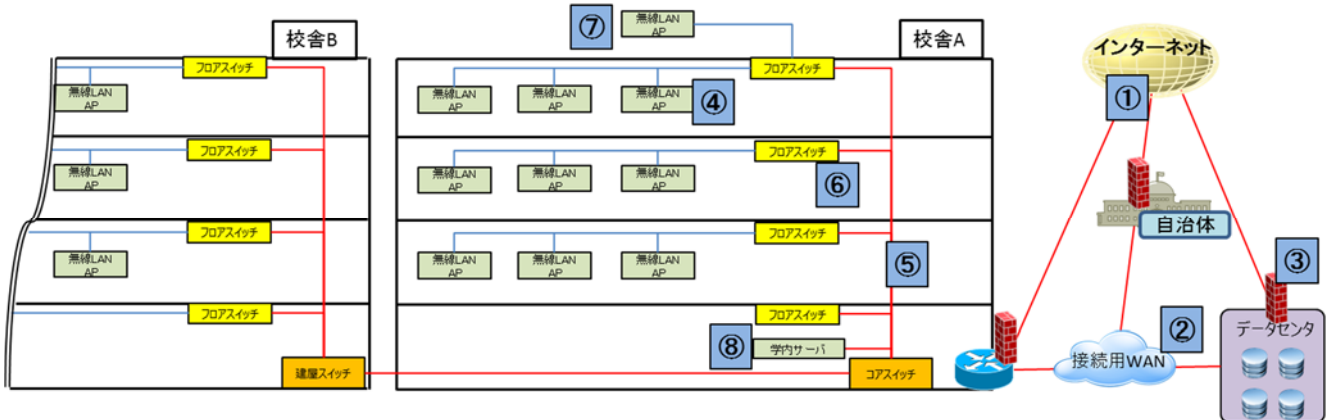
データの流れをあらかじめ想定しておくことで、必要となる機器のスペックや、契約する回線の帯域を仕様化しやすくなる。また、データ種類と利用者分類、インターネット接続の有無により、トラフィック分離などセキュリティへ要件や機器に求められる機能が異なってくるため、事前の検討が必要となる。

帯域やトラフィック分離の要件が整理されると、ICT環境を構成する、学校内の無線LAN、有線LANや、WAN接続、データセンタ (DC)、各所の物理的配線 のそれぞれに求められる要件が確定されていく。

単年度で最終形を導入するのではなく、数年ごとに規模を拡大していく整備計画の場合も、都度、上記要件がどのように変遷するかを予想の上で構築することを推奨する。

2.1. 構成要素の設計要件

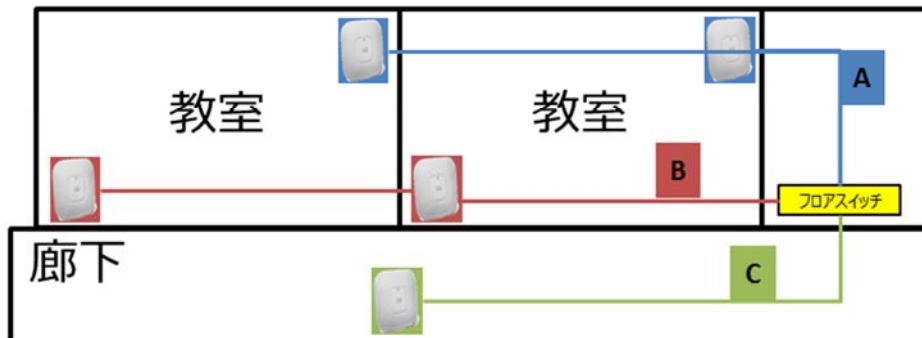
教育ICT環境を構築する要素、特に学校内LANについて、概略を図に示す。



①	インターネット接続	インターネットへの接続をどこから、どのように行うか	
②	施設間接続WAN	教育委員会や多くの学校の間など、施設をまたがるネットワーク	
③	インターネット接続セキュリティ	インターネット接続や、情報漏えいを未然に防ぐためのセキュリティ (端末セキュリティなどは含まず)	
④	無線LAN	多くの端末から利用する時の通信規格、アクセスポイント管理、注意点など	2.x.x
⑤	有線LAN配線	ICT機器を配線することを配慮されていない学校でLANを敷設する時の注意など	
⑥	フロアスイッチ	児童・生徒、教職員などが共有するLANで必要になる機能など	
⑦	屋外無線LAN	屋外で無線LANを利用する場合特有の注意点など	
⑧	学校内サーバ類	データの置場として、学校内で必要になるサーバ類	

図 2-1 学校内システム構成要素の概略図

教室での無線LANアクセスポイント(AP)の設置例
 教室の無線LANアクセスポイントをどのように配置するか、それぞれのメリットデメリット



設置パターン	メリット	デメリット
A + B 各教室2台設置	<ul style="list-style-type: none"> 細かい制御ができる機器の場合、接続性と快適性が高い 耐障害性も上がる 	<ul style="list-style-type: none"> 初期費用が高い
A + C 各教室1台 + バックアップ用廊下1台	<ul style="list-style-type: none"> 教室の1台に全生徒が接続するため、帯域不足になることは少ない 廊下 AP が予備で動くため耐障害性も高い 	<ul style="list-style-type: none"> 初期費用が高い 通常時、廊下 AP の利用頻度が低い
Aのみ 各教室1台設置	<ul style="list-style-type: none"> 費用的には抑えられる 	<ul style="list-style-type: none"> 教室の AP が故障した場合、交換まで利用できない
Cのみ 廊下1台 (2教室分で併用)	<ul style="list-style-type: none"> 費用的にはもっとも抑えられる 	<ul style="list-style-type: none"> 隣り合う教室での同時利用を避けるカリキュラムが必要など、運用への制限が出る可能性が高い

図 2-2 普通教室への無線APの設置例

2.1.1. 帯域 (快適な利用に必要な考え方)

下図は右にデータ保存場所(データセンターやクラウドなど)、左に利用端末を配置し、通信の途中で経由する機器や回線の想定帯域を視覚化したものである。

校内の有線LAN機器は、機器の中では比較的低価格であり、ネットワークの広帯域化を図りやすい。対して無線LANや、WAN、データセンター入口のWAN集約設計が実施されないと、そこがボトルネックになる可能性が高い上に、価格的にも影響度が高いため、十分な設計と管理が必要となる。

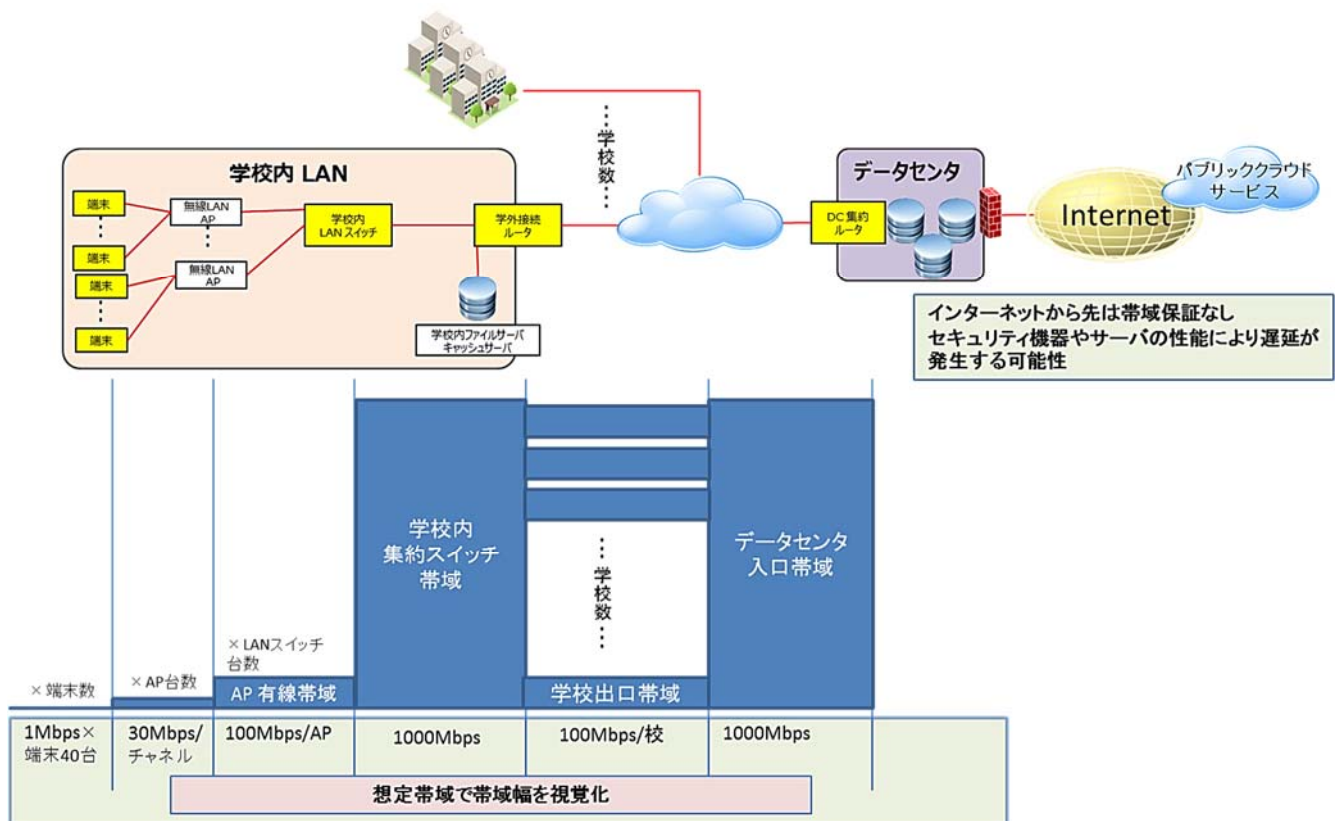


図 2-3 ネットワーク経路の帯域の違い

(1) 端末台数と利用アプリケーションからWANの帯域計算

使用する端末、OS、アプリケーション、クラウドの形態、データ種、ユーザの数により必要となる帯域は異なるため、一概に何bps以上あればよいと言えない。

例) 100Mbps (bit/sec) の回線帯域があり、10MB (Byte=8bit) のデータを転送する場合、0.8秒以上かかる。

$$(10\text{MB} \times 8\text{bit}) \div 100\text{Mbps} = 0.8\text{sec}$$

もし、1クラス40名、全員端末、10MBの画像データを教員の指示で一斉に参照した場合で、回線帯域が100Mbpsのみであれば、全員の端末で画像表示が完了するには32秒以上が必要となる。このような時間ロスで授業の進行を妨げる事は、ICT利活用の本意ではない。

$$(10\text{MB} \times 8\text{bit} \times 40) \div 100\text{Mbps} = 32\text{sec}$$

学校内有線LANの広帯域化は、学内機器の更新費用で、それほどのコスト高とはなり難いが、学外接続のWANの広帯域化は、回線費用となり運用コストの高額化を引き起こす可能性がある。例えば、LANを利用できる学内にメンテナンスの必要ないキャッシュサーバ(Proxyサーバなど)を置くと、クラウドから同一ファイルを複数回ダウンロードしないようにできる。帯域計算を行うときは、利用形態とコスト、機器構成を考慮して行うとよい。

(2) トラフィックが集中するデータセンタ出入り口の帯域

学校を複数収容するデータセンタには、学校接続用の帯域に加えて、バックアップセンターへの接続分、自治体ネットワークとの接続分があり、単純に加算すれば、広帯域での契約が必要となる。事前に同時接続数や、利用時間帯から必要な帯域を考慮する

2.2. 無線LAN

学校における無線LAN環境は、多くの端末が同時接続し、同時に通信を行う点が企業や公衆無線LANと異なる点である。また、教育コンテンツ等、同時通信するアプリケーションが映像の場合、より広帯域・安定性が求められる。よって、アクセスポイントへの同時接続数だけでなく、多くの端末が同時に通信を行っても大幅なスループット低下や接続断が発生しない、安定した通信環境が提供されるべきである。

以下に無線LAN環境を導入する上で必要なポイントを解説する。

- ・ 高速通信
- ・ 安定した通信環境
- ・ セキュリティ対策
- ・ 状態把握、見える化

2.2.1. 高速通信

無線LANはひとつのアクセスポイントに接続される端末が増えるほど、端末あたりの通信速度が低下するという特性がある。これは、同時通信が発生しやすい学校の環境においては特に重要で、全員がひとつのファイルをダウンロードするまで非常に時間がかかる傾向がある。そのため、コストを考慮した上でなるべく最新規格へ対応し通信速度を高めておくことで、端末個々の通信速度も増すため、授業中のダウンロードなどによる待ち時間を削減することができる。

(1) 5GHz帯

無線で使える周波数帯のひとつで、もうひとつは2.4GHz帯と呼ばれる。5GHz帯の方が利用できるチャンネル数も多く、設計が容易で、Wi-Fi通信を阻害する干渉減が少なくきれいな環境であるといったメリットがある。一方、一部レーダーと利用周波数帯が重なるため、検知後にチャンネルを切り替える機能(DFS 後述)をアクセスポイントに搭載させる必要がある。

(2) 802.11ac

最大規格値1.7Gbpsの最新無線LAN規格である。IEEE802.11nで導入されたMIMO (Multi-Input Multi-Output) と呼ばれる複数アンテナを同時に利用する技術や通信チャンネルを複数束ねるチャンネルボンディングをより強化するなど、IEEE802.11n (最大規格値600Mbps)からさらに高速化した。

現在、通信速度が1Gbpsを超えるアクセスポイントも多くあり、端末側もIEEE802.11acに対応したものが増えている。今後IEEE802.11ac対応の製品が主流になると予測される。

2.2.2. 安定した通信接続

無線LANは誰でも利用可能なライセンス不要の周波数帯を利用しているため、周辺環境に影響され通信が途切れたり遅くなったりと通信が不安定になることがある。そのため、外的要因による影響を受けにくくする機能、自動的な回復機能や電波の設計がとても重要である。また、多くの端末の同時通信に耐えられる製品を用意することが安定性にもつながるので考慮が必要である。

高速通信で説明したMIMOは複数アンテナを同時利用することで安定性も向上するため、コスト面を考慮する必要はあるがアンテナ数は多いほうが望ましい。無線LAN通信を不安定にさせる干渉には無線LAN同士の干渉と、非無線LAN製品(電子レンジなど)による干渉があるため、この両方の影響を見える化し、端末接続への影響を考慮しながら回避する方法があるべきである。また、映像を同時配信する場合にも画像が乱れにくい仕組みがあることが望ましい。

(1) 同時接続・同時通信

同時接続(アソシエーション)と同時通信は異なり、接続はできても通信できない場合があるため、AP単体の性能はひとつの考慮すべきポイントである。少なくとも、ひとつの教室で利用する端末数で同時接続ができ、授業に支障がないレベルの通信速度が全端末で保てるかどうかは重要なポイントである。

(2) セルデザイン

学校などある一定のエリアでひとつのシステムとして複数APを同時に動作させ、数多くの端末が各APに接続されることが想定される場合、電波がより遠くへ飛ぶことは望ましくない。電波がより遠くへ飛ぶことにより1APでカバーできる範囲が広がることは一見良いように思われるが、1APに接続される端末が増え通信速度が極端に下がるリスクや、干渉により通信が不安定になるリスクが増えるため避けるべきデザインである。従って1教室あたりに1以上のAP設置が望まれる。

(3) チャンネルと出力の自動切り替え

無線LAN環境は常時周辺環境の影響を受け、また周辺環境は一定ではないため、無線LAN環境も常に一定の状況を保つことは難しい。環境の変化により無線LAN機器、または非無線LAN機器による干渉の影響を受けた場合に、自動的にチャンネルを切り替える、または出力を変更することにより悪化した状態から自動的に回復する機能が必要である。この際、チャンネル切り替えにより端末の通信が切断される可能性があるため、この自動化そのものが安定性を欠くことにならないよう配慮が必要である。

(4) 授業支援系アプリケーションへの対応

映像を利用する場合、通信量が増え、通信の安定性が映像の乱れの有無に直結するため、データ通信以上に注意が必要である。不要なトラフィックをなるべく流さないことで全体の通信を圧迫しない機能が必要である。

(5) DFS

DFSとは、無線LANが利用している周波数帯と重なる周波数帯を利用するレーダーを検知し、検知した場合は無線LAN側がチャンネル変更を行う機能である。そのため、レーダーが多く検知されるエリアにおいてはDFSが動作する周波数帯は利用しないなど配慮が必要である。

(6) 干渉対策

干渉対策には、チャンネルと出力の自動切り替えによる回避策とともに、システム全体に対する影響度を把握するため見える化も重要である。特に、干渉となる非無線LAN機器の場合は、どのような端末なのか、どのくらいの数がある

のか、また無線LAN環境にどれほどの影響を与えているのか等、視覚的に分かる仕組みがあれば、トラブルが発生した際にもユーザに都度状況を確認することなく迅速な対応が可能となる。

(7) 物理的な設置場所

電波は周波数が低いと回り込みやすいという特性があるため、壁などの障害物が多い環境では2.4G帯では電波が届く箇所でも5G帯は電波が届かない可能性があるため、アクセスポイントの設置場所が重要になる。

詳細は2.4.2無線 設置場所による注意点を参照すること。

2.2.3. セキュリティ対策

無線LAN接続では認証と暗号化が必須要件である。特にIEEE802.11nやIEEE802.11acの暗号化では最も強固なAESを利用しなければ、11n、11acで規定する速度で通信できない(AES以外を利用すると、11g/aの速度で通信する)。また、不正APの見える化などいくつか注意すべき点もあるが、詳細については「2.7 セキュリティ対策」を参照すること。

2.2.4. 状態把握、見える化

無線LANは電波であるため、目に見えない点が問題解決を難しくさせる。そのため、電波環境、干渉源などの周囲の影響度、端末の状況を常に一目でわかるような状態にしておくべきである。また、常時監視することや迅速な現地への人員配置は難しいため、ある程度自動化に任せられる仕組みなども配慮すべきである。

電波がエリアのどこに届いているかを把握することや、電波が届いていてもその電波が干渉源などで使えない状況になっていないか視覚的に分かると、対応が早くなる。また、ユーザに通信できないと言われた時に、何が問題かを把握し、その情報を提供できる仕組みがあると望ましい。

2.2.5. 技術的な仕様/機能の詳細解説

(1) 802.11ac

最初の規格であるIEEE802.11は1997年に標準化されたが、2Mbps程度でありメーカー間の相互互換性がなかったために広く普及されることはなかった。

次に最大11Mbpsまで拡張されたIEEE802.11bが1999年に標準化された。これは2.4G帯を利用し、IEEE802.11と下位互換性を持たせた規格である。

同じ時期に5G帯を利用する最大54MbpsのIEEE802.11aも標準化されたが、製品は2002年以降に登場した。また、当時日本で使用されていた5G帯の中心周波数は国際標準と異なっていたが、2005年以降国際標準へ変更され移行期間を経て、現在は国際標準規格のみが利用可能である。

IEEE802.11bの上位互換であるIEEE802.11gは2003年に標準化され、IEEE802.11aと同じ最大54Mbpsをサポートする。

IEEE802.11nは2.4G帯/5G帯の周波数帯を利用するため、IEEE802.11a/b/gとの下位互換性があり最大600Mbpsをサポートする規格である。2006年にドラフト1.0、2007年にドラフト2.0、2009年に正式規格となったが、2007年のドラフト2.0の頃から製品が登場し、それらがそのまま利用できるような形で正式規格となった。

最新規格であるIEEE802.11acは5G帯を利用して理論的には最大6.9Gbpsの通信が可能である。現在登場している製品は最大帯域が1.7Gbpsであり、同じ5G帯を利用するIEEE802.11a/nとの下位互換性がある。

IEEE802.11n以降、複数のアンテナで送受信を行うMIMO(Multiple Input Multiple Output)技術が採用され、高速化に加えて安定性が向上する傾向にある。

表 2-1 無線LAN規格

	2.4G帯	5G帯
11Mbps (規格値)	IEEE802.11b	
54Mbps (規格値)	IEEE802.11g	IEEE802.11a
600Mbps (規格値)	IEEE802.11n	
6.9Gbps (規格値)		IEEE802.11ac (現行製品は最大規格値1.7Gbps)

※規格値は実行帯域とは異なる

2.4GHz帯

- ・ Ch1～11 までの 11 チャンネルの中で干渉しない最大 3 つのチャンネルを利用可能
- ・ 利用可能なチャンネル数が少ないため、セル設計が難しい
- ・ 干渉源となる非 Wi-Fi デバイスが多いため、無線 LAN 環境は不安定になりやすい
- ・ 屋内・屋外ともに利用可能

5GHz帯

- ・ 利用可能なチャンネルは国や地域ごとに異なる
- ・ 日本では下記チャンネルが利用可能
W52 (Ch36, 40, 44, 48)
W53 (Ch52, 56, 60, 64)
W56 (Ch100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140)
- ・ 利用可能なチャンネルが最大 19 あるため、セル設計が容易
- ・ W52, 53 が屋内利用のみ、W56 は屋内・屋外で利用可能
- ・ W53, 56 は DFS (Dynamic Frequency Selection) というレーダー回避機能の実装が必須になっているため、レーダーが多数検知される場所での利用は注意が必要である（例：海の近く、空港の近く等）。

(2) DFS

- ① レーダー検知後、他のチャンネルへ切り替えが必要
- ② 他のチャンネル(W53, 56)へ移動した場合、1 分スキャンした後に利用可能
- ③ レーダーを検知したチャンネルは、検知後 30 分利用不可

(3) 同時接続・同時通信

無線LANは原則1対1の通信が基本のため、APに複数端末が接続されるとフレーム衝突を防止するため、CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)により時間をずらして通信する仕組みを採用している。そのため、アクセスポイントに接続される端末が増えるほど通信するまでの待機時間が増え、個別端末における実行スループットが落ちる。このCSMA/CAのルールにより、接続端末数が増えれば増えるほど1台あたりのスループットは落ちる傾向にあるため、以下の項目への考慮が必要である。

- ① 100 台の同時接続(アソシエーション)が可能
- ② 100 台同時の通信が発生しても、大幅なスループットダウンがない
- ③ 100 同時通信時の接続断がない、あるいはより少ない

(4) 端末の仕様に依存しない高速化機能

利用する端末は学校により異なる可能性があるため、通信の高速化の検討は下記のような端末側の仕様に依存しない機能であることが望ましい。

(5) ビームフォーミング

複数のアンテナからの電波の重ね合わせで、特定の方向への電波強度を変更する技術である。

IEEE802.11g/a/n/acのどの端末でも高速化を実現することが可能で、特に11acでは、最も高データレートで通信できる範囲が狭いため、ビームフォーミング機能により電波到達エリアを調整することがメリットとなる。

ビームフォーミングは、電波が飛ぶ範囲を広げる技術ではなく、高速通信できるエリアを絞って距離をかせぐ技術である。

干渉の有無によってチャンネルボンディング のチャンネル幅を自動で切り替える機能

干渉があり、チャンネルを変更すると他のAPへの影響が及ぶ。帯域幅を減らすことで、他に管理しているAPに影響せず、かつ干渉の軽減も行える点がメリットである。

無線APのCPU・メモリ強化

IEEE802.11acはIEEE802.11nに比べて1,500 byteの packets長で秒間あたりのパケット処理数が2.5倍以上になるため、APのラジオごとのCPU、メモリの強化がされていることが望ましい。

(6) セルデザイン

複数端末が接続される学校の環境において、セルサイズ(電波が届く範囲)は小さくすること。理由は下記の通りである。

- ・ AP の電波がより遠くまで届くことが可能でも、端末が同じ距離の電波を飛ばせるとは限らないため、片側通信になる可能性を避ける
- ・ セルサイズを小さくすることで、1APあたりの端末接続数を減らせるため、より高スループットが得られる
- ・ 電波が飛びすぎ想定外のエリアに電波が漏れることにより、干渉源の影響を受け、スループットの低下や安定性が下がることを防ぐことが必要

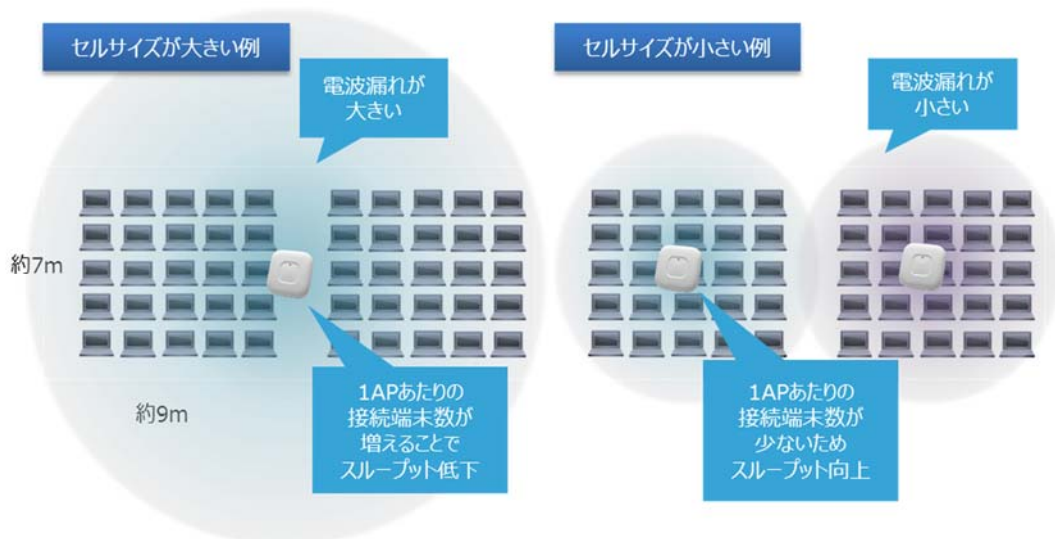


図 2-4 セルデザイン

利用周波数帯は、干渉源が少ないことや、利用可能チャンネルが19ありセル設計が容易であることから、5G帯を推奨する。

5G帯を使うIEEE規格は802.11a/n/acがあるが、IEEE802.11acの利用を推奨する。なぜなら、最新の規格で最速であり、映像など大容量スループットを求めるアプリケーションなどの新規導入が容易になることや、例えば現在端末がIEEE802.11ac非対応端末があるとしても、下位互換性があるため11aや11nの端末も接続可能だからである。

IEEE802.11gやIEEE802.11nの2.4G帯のみ利用可能な端末もある可能性があるため、2.4G帯と5G帯が同時に利用可能なアクセスポイントを選択すべきである。

(7) 授業支援系アプリケーションへの対応

マルチキャストは、映像を再生していないなどの理由で受け取る必要のない端末にもパケットを送信するため、無駄なトラフィックが流れてネットワーク全体が遅くなる傾向にある。学校ではマルチキャストを利用したビデオの同時利用が想定されることから、映像の乱れが発生しないよう無線LANにおけるマルチキャストへの配慮が必要である。

具体的には、無線LAN区間ではユニキャストに変換し、余計なトラフィックを流さない仕組みや、マルチキャストをユニキャストに変換する対応をアクセスポイントで実施することで、コントローラ-AP間の有線区間はマルチキャストのまま帯域を圧迫させないことが必要である。



図 2-5 無線LANでのマルチキャスト画像配信

(8) 干渉対策

無線LANは免許不要の周波数帯であるため誰でも利用可能である。そのため、Wi-Fiおよび非Wi-Fiの干渉源対策が重要であり、下記の実装が必要である。

- ① システム内の AP 同士の電波干渉および不正 AP による電波干渉を検知し、自動的に出力調整およびチャンネル切り替えにより干渉を回避する
- ② 電子レンジなどの非 Wi-Fi 波による干渉源を検知し、それが何であるかを特定し、可能であればこれらを排除するまたは避けるため位置や影響範囲を特定できるようにしておく。また、この機能が AP の負荷となり通常の通信のスループットに影響しないことが重要である。具体的には、以下のような機能である。

- ・ ハードウェアで高速かつ正確に干渉源を検知
- ・ 何が干渉しているか自動で判別し、干渉源の影響度を数値化
- ・ 干渉源の位置を特定干渉源の影響度、無線占有率を総合的に評価
- ・ 影響度が高い場合は他のチャンネルへ切り替え、影響度がそれ程でもない場合はそのまま判断

③ チャンネル切り替えが発生した時に、その理由がわかること。この情報を基に、レーダー検知が多ければ利用するチャンネルの見直しを行うなどの対策が可能になる

(9) 状態把握、見える化

電波は目に見えないため、自動化してシステムが自動回復する仕組みを備えたり、視覚的に見える化を実現したりする事により、状況確認やトラブルの早期解決ができるようにしておく必要がある。周辺環境も含めて電波環境は常時変化するため、履歴取得可能な状況が望まれる。

- ・ APの故障などにより電波が届かない範囲ができた場合、他APが出力を上げてカバーする、干渉などの理由で出力を下げる、チャンネルを切り替えることを自動的に行うこと
- ・ 設定変更した際に自動的にアーカイブできるようにし、世代管理ができること
- ・ 自動でメーカー推奨の設定内容が機器に設定されること
- ・ 電波の届いているエリアがマップ上でわかるようにして、電波が届いていないまたは弱い箇所を把握可能なことが望ましい
- ・ 無線 LAN 環境が良好な状態かどうかを数値やマップで把握することにより、電波は届いているが干渉などの理由により通信が途切れる、遅いなどの早期トラブル対応が可能なが望ましい

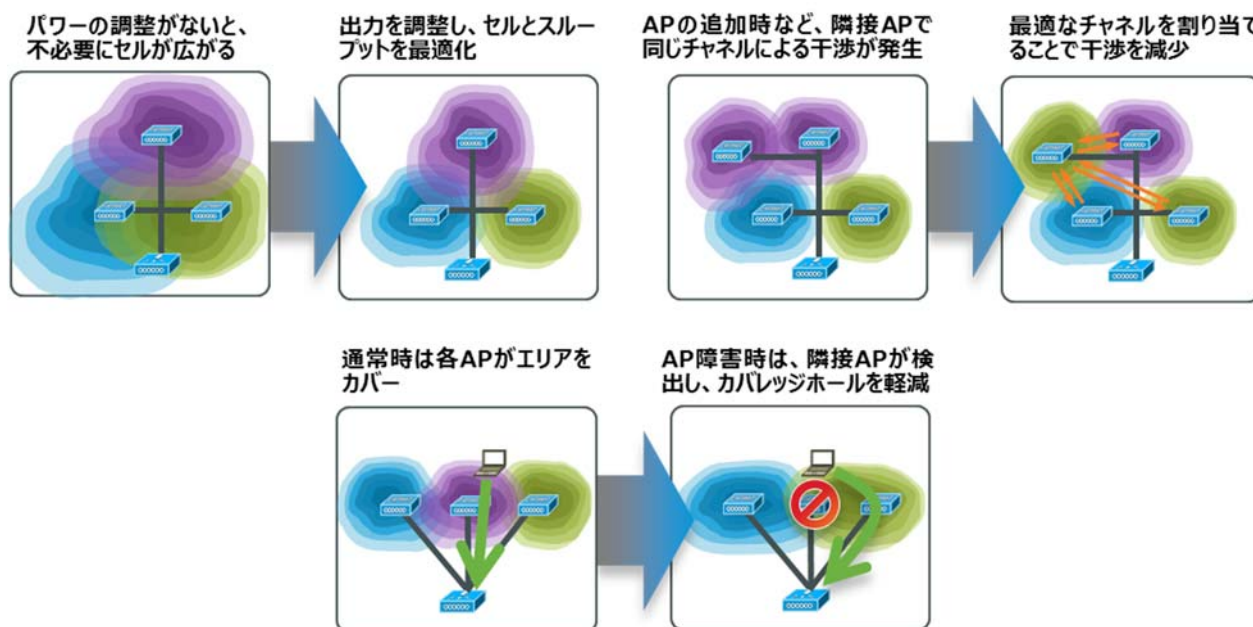


図 2-6 無線LANの電波環境変化への追従

2.3. 有線LAN

インターネットや教育において映像配信や様々なアプリケーションを利用する場合、有線LANの広帯域化が必要である。また単純に広帯域化するだけでなく、トラフィック負荷の高い動画コンテンツ等はキャッシュサーバを利用し、校内でキャッシュすることで、ネットワークシステム全体で効率よく利用/運用する設計が重要である。その各要素について記載する。

2.3.1. LANの広帯域化

一般的なLAN環境では安価なツイストペアケーブルと長距離の伝送に適した光ファイバーが利用されている。ケーブル種別により利用できる回線速度の規格があり、通常ツイストペアケーブルは100Mbps(古いケースでは10Mbps)か1Gbps、ファイバーケーブルは1/10Gbpsで利用されている。

昨今の端末の広帯域化によってフロアスイッチから建屋スイッチにおいても1Gbpsを超える帯域が必要になってきている。

この区間はツイストペアケーブルが利用されていることも多く、ファイバーケーブルへの工事費用が一つの課題となっていたが、新たにマルチギガビットなどNBase-T準拠の技術が出来たことによってカテゴリ5e以上のツイストペアケーブルで2.5/5Gbpsと言った広帯域の利用が可能になった。

表 2-2 LANで利用されるケーブル種別と通信規格

ケーブル種別	ツイストペアケーブル			ファイバーケーブル
	CAT5e カテゴリ 5e	CAT6 カテゴリ 6	CAT7 カテゴリ 7	シングルモード/マルチモード
主な通信規格	10BASE-T 100BASE-TX 1000BASE-T NBase-T	10BASE-T 100BASE-TX 1000BASE-T 1000BASE-TX NBase-T	10BASE-T 100BASE-TX 1000BASE-T 1000BASE-TX 10GBASE-T	1000BASE-SX 1000BASE-LX 10GBASE-SR 10GBASE-LX4

2.3.2. 最適なトラフィック処理

(1) ネットワークセグメンテーションの物理分離/論理分離

ネットワークシステムの中では様々なセグメンテーション手法が用いられている。物理的な手法では階層化などネットワークデザインによってトラフィックの流れや運用の効率化を行い、論理的な手法ではVLANなど各種技術や機能によって物理環境内部を論理的にグループによって分けることが可能となる。

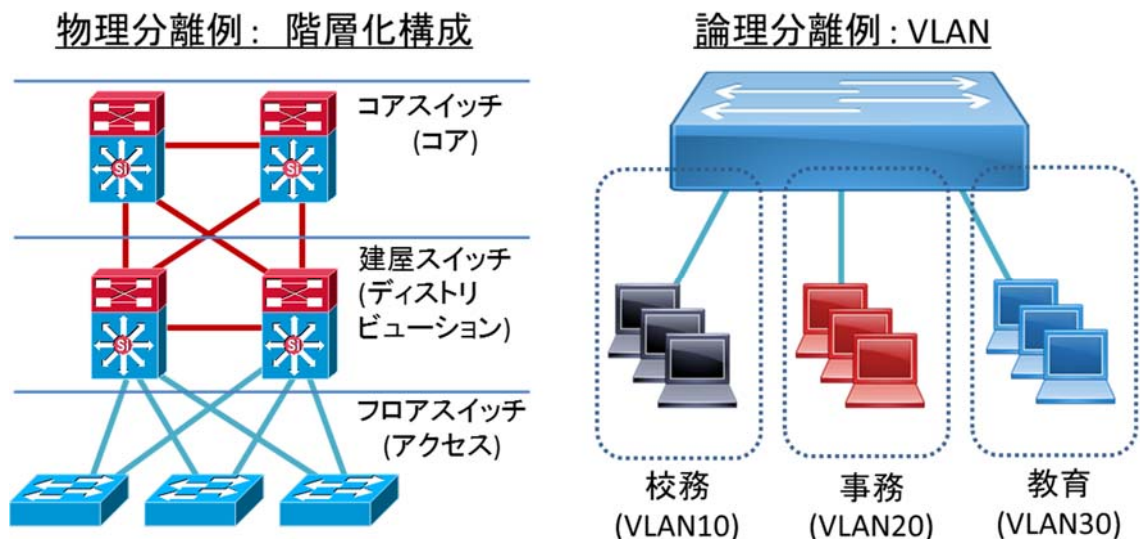


図 2-7 ネットワークセグメンテーションの物理分離/論理分離

(2) 冗長化/負荷分散

ネットワーク機器に障害が発生した場合においても利用者が引き続き通信できる別の経路を用意することは重要である。通常建屋やコアスイッチなど集約ポイントの機器を複数台設置することによって冗長化を行う。

冗長化により経路が複数になった時、一方のみ利用しもう一方は障害時のみ利用するといった最大トラフィック量を一定にして設計する場合と、通常は両方の経路を分散して使い障害時はトラフィック量が半分になる場合といったように運用ポリシーやコストにあわせて最適な設計を考える必要がある。

また、冗長構成において機器に障害があった場合、もともとの経路情報などを素早く引き継いだり、管理ポイントを削減したりすることは管理/運用の面でも重要であり様々な機能によって提供されている。

(3) トラフィック多重化

複数の回線で接続することによってネットワーク機器間を冗長化し分散処理による広帯域を提供する様々な多重化技術がある。一般的に双方の機器が同じ技術で接続されている必要があり、様々な標準化プロトコルが提供されている。

(4) サービスの品質確保

広帯域化された端末によって、より上流の建屋スイッチやコアスイッチで処理できるトラフィック量を超える場合がある。そのためトラフィックの集約点となるネットワーク機器においては、重要なサービスやビデオなど遅延の影響を受けやすいサービスのトラフィックを優先的に転送する技術が必要になる。

2.3.3. システム帯域管理

通常状態の把握や予兆検知のため、校内LANのネットワーク機器状態や流れているトラフィックといった様々な見える化を行うことが必要となる。この見える化は有線ネットワーク機器と無線ネットワーク機器、そしてトラフィックの見える化を単一の管理ツールで行うことが望ましい。

(1) 見える化

見える化の必要性は通信断や遅延等、トラブルがあった場合にネットワーク機器及び、トラフィックの状態をあらかじめ把握しておくことで、一時対処を早め、早期に解決する為のものである。

・ ネットワーク機器の見える化

機器の状態監視はネットワーク機器の死活監視から始まり、CPU利用率、メモリ利用率、インターフェイス利用率といった状態監視があげられる。また機器のシリアル番号といったインベントリ情報もこの項目に必要な要素となる。

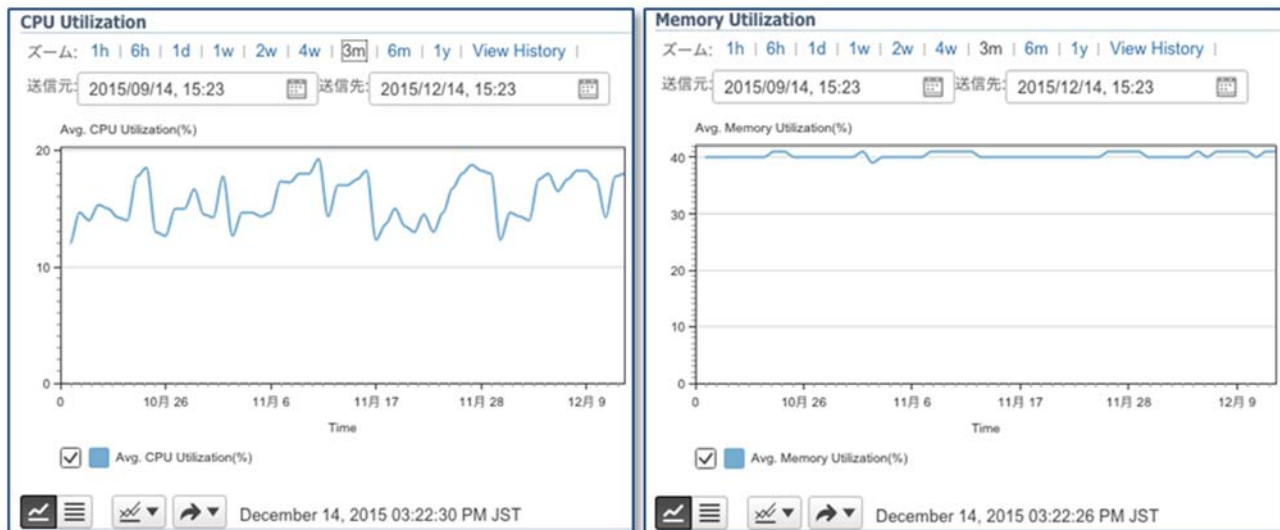


図 2-8 CPU/メモリ使用率 出力サンプル

・ 流れているトラフィックの見える化

ネットワークに流れるトラフィックが複雑になり、原因解決のためにもトラフィックの見える化が必須となってきている。これらの情報は、WAN帯域の契約や次期校内LANの設計、またセキュリティ対策でも利用できる。

また、通常時でも回線帯域とトラフィック種別を把握することで、ビデオトラフィックを優先的に転送、必要無いトラフィックを制御する等、効率的の運用する為の設計が可能になる。

2.4. WAN（自治体WAN、キャリア回線、インターネットVPN）

前述のネットワークインフラストラクチャで分類したケースのうち教育ネットワーク専用のインフラストラクチャを構成する場合、もしくは学校個別にインターネットや拠点間を接続する場合は、WANを選択する必要がある。行政系ネットワークや地域イントラを利用する場合は、教育ネットワークのWANとして必要な帯域をそれぞれのネットワーク主管部門と調整する必要がある。

次表はWANの選択肢一覧となるが、利用者数(端末数)・利用シーン・利用頻度(同時接続数)などの見通しから中期的な利用に耐えられる余裕を持つておくことが必要となる。

表 2-3 教育ネットワークWAN種別

種別	選択肢	特徴
自前WAN	行政系ネットワーク、地域イントラ利用	<ul style="list-style-type: none"> ・割り勘効果が高く、経済性に優れる ・通信帯域の制限や、セキュリティポリシーによる利用シーンの制約を事前に主管組織と相談しておくことが必要
キャリアサービス	帯域保障回線利用	<ul style="list-style-type: none"> ・必要な通信帯域が保障されるため、安定した利用シーンの実現が可能 ・回線トラブルに対して手厚いサポートが期待でき、SLAが準備されているサービスが多い ・比較的高価となる傾向
	一部帯域保障回線利用	<ul style="list-style-type: none"> ・帯域保障とベストエフォートの中間的な回線サービス ・保障部分に対してSLAが準備される ・想定する利用シーンとサービススペックが合致するか事前の確認が必要
	ベストエフォート回線利用	<ul style="list-style-type: none"> ・経済性に優れ、手軽に利用開始できることから、まず着手（スモールスタート）に適する ・無線LAN（Wi-Fi）まで提供されるサービスも用意されている ・帯域は保障されないため、利用シーンに応じてスペックアップが必要 ・故障回復などSLAは提供されない
その他（参考）	モバイル回線利用	<ul style="list-style-type: none"> ・端末から直接インターネット接続するため利用場所にとらわれず自由度が高い ・想定する利用シーンに対して十分な十分な通信帯域が確保できるか、事前にサービス提供キャリアとの相談や検証が必要

2.5. データセンタ

自治体内で共通的に利用する統合型校務支援システムや共有ファイルサーバ、シンクライアントシステムなどを導入する場合は教育ネットワーク内にこれらを格納するセンタを設置することが必要となる。

特に民間のデータセンタを活用する場合は、個人情報保護の観点より自治体によっては自治体外のロケーションや自庁施設外の設置が許可されていない場合もあることから、主管組織と連携し利用可能となるよう制度上の整理を事前に実施しておくことが必要。また、近年ではセンタを設置せずクラウドから提供されるサービスを活用することも現実的な手段となってきていることから、将来的なクラウド利用の可能性も含めて教育ネットワークの構築やセンタの設置を計画する必要がある。

次表はセンタの種別と特徴を記載する。

表 2-4 センタ種別

種別	選択肢	特徴
センタ設置	自前センタ (自治体サーバーーム含む)	<ul style="list-style-type: none"> ・制度の変更などが不要な場合が多い ・格納したセンタ設備の管理・運用・保守の自前実施が必要 ・将来的なスペースの確保など関連組織と事前の調整が必要
	民間データセンタ	<ul style="list-style-type: none"> ・専用の管理・運用・保守人員を配置しており、人材も含めフルアウトソースが可能 ・設置場所が自治体外となる場合が多いが、自治体の出先機関に位置づけるなどの例もある ・センタ設備導入にあたってイニシャルコストが発生
クラウド利用	各種サービス利用	<ul style="list-style-type: none"> ・管理・運用・保守はサービスの一部として提供側で実施される ・特別な人員の配置は不要なため、サービスを調達するだけで運用スタートが可能 ・機微情報を扱う場合、利用可否など関連組織への事前相談が必要 ・イニシャルコストは小さく、利用する期間のみのランニングコストが発生

2.6. データの保存場所

授業支援系、校務支援系で取り扱われるデータを、どこに保存するかは、以下のような点が検討対象となる。

- ・ データの機微度（行政データ、個人情報、著作権）と求められる機微度
- ・ 利用者（職員、教員、児童・生徒）の種別、人数、利用場所
- ・ 取り扱うデータのサイズと途中のネットワーク帯域
- ・ 途中経路でのネットワークの分離要件とその機微度

利用可能なファイルサーバの例としては、

- ・ 学校内サーバ
- ・ 教育用データセンタ内、サーバ（複数校共有サーバ、もしくは、各学校専用サーバ）
- ・ インターネット上のクラウドに存在するサーバ（教育専用、もしくは、一般との共有サーバ）

これまで、組織内性善説(自組織内で、違法な行為を行う者はいないという考え方)から、機微データは組織内に置くことがよいとされてきたが、ICTのセキュリティ確保の複雑さや、ICT技術者不在という点から、専門の管理者がいるデータセンタや、クラウドでそれぞれを担保してもらうという考え方が増えてきている。

その場合も、委託先のデータ流出などの防止策として、管理ログの第三者による監視など、事前の対策は必要となる。

例として、電子教材自体は機微度が低く、データサイズが大きく、複数名が一斉にダウンロードする場合があります。WAN帯域の逼迫と動作遅延を引き起こす。このような場合、セキュリティレベルは低いですが利用者に近いところにサーバがある方が利便性は高い。

逆に、児童・生徒の成績データや、個人データにかかわるデータは、機微度が高いため、サーバ自体の管理や物理セキュリティが考慮された場所に設置される必要がある。

2.7. セキュリティ対策

2.7.1. 教育ネットワークにおけるセキュリティ対策の基本的な考え方

「1.4 教育ネットワーク全体像イメージ」にも記載がある通り、教育ネットワークを整備するに当たって取り扱う情報の重要性を考慮してネットワークを分離することが考えられる。

特に、学校で取り扱う情報においては、成績情報に代表される機微情報があることからインターネットや他のネットワークから分離し、機微情報専用のネットワーク(以下「校務支援系ネットワーク」という)を整備し、職員室のみでなく普通教室からの利用にも考慮することが望まれる。

さらに、教育ネットワークには、授業で児童・生徒が情報端末を活用して調べ学習に伴うインターネット接続や、デジタル教科書、動画教材の視聴などに活用するためのネットワーク(以下「授業支援系ネットワーク」という)の整備も不可欠となる。

また、教職員(主に校長先生、教頭先生)の方々が、行政業務に利用するためのネットワーク(以下「行政系ネットワーク」という)の整備も必要となる。

なお、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を始め様々なセキュリティ対策に関するガイドライン等が発行されていることから、本書では、ネットワークにおけるセキュリティ対策に主眼をおいて記載することにする。

一般に、学校用ホームページは校務として扱われるが、機微データの保存を主目的とするサーバとは異なるため、本書では授業支援系ネットワークでの取り扱いと同等と考えている

2.7.2. 教育ネットワークにおけるセキュリティ対策の基本的な要件

教育ネットワークは、「授業支援系ネットワーク」、「校務支援系ネットワーク」、「行政系ネットワーク」に大きく分類されそれぞれの特性を以下の表の通りとなる。

表 2-5 各ネットワークの特性とその利用者

ネットワーク名		想定利用者	ネットワークの特性
教育ネットワーク	授業支援系ネットワーク	教職員 児童・生徒	インターネットへの接続可、ただし、教職員、児童・生徒がアクセスできるWebサイトをフィルタリングすること ※仮想技術等を採用し倫理的に分離、または、児童・生徒からのアクセスを制御することで校務支援系ネットワークとの併用は可能
	校務支援系ネットワーク	教職員	インターネットとの接続禁止 他のネットワークとの接続を制限 ※仮想技術等を採用し論理的に分離することで授業支援系ネットワークとの併用は可能
行政ネットワーク		教職員	授業支援系ネットワーク、校務支援系ネットワークとの接続不可

(1) 教育ネットワークにおけるセキュリティ対策

学校間を繋ぐ基幹ネットワークとなる教育ネットワークは、その取り扱う情報の特性を考慮して「校務支援系ネットワーク」、「授業支援系ネットワーク」、「行政系ネットワーク」に分離することが望ましい。

① 教育ネットワークにおけるセキュリティ要件

教育ネットワークにおけるセキュリティ対策の要件について下記に記載する。調達する自治体・教育委員会および導入事業者は、これらの要件を踏まえてセキュリティ対策の検討を行うものとする。

- ・ 教育ネットワークは教職員が実務（成績情報、出欠席など）を行うための「校務支援系ネットワーク」と、調べ学習やデジタル教科書、動画教材などインターネット接続し、授業で利用するための「授業支援系ネットワーク」、行政業務を行うための「行政系ネットワーク」の接続は分離すること
- ・ 各ネットワークのネットワークセグメントは分離すること
- ・ ネットワークに接続する機器を特定するため、MACアドレスやサブリカント²を採用しネットワーク上で機器を識別・認証を可能とすること
- ・ 「校務支援系ネットワーク」、「授業支援系ネットワーク」、「行政系ネットワーク」との各ネットワークの物理的な接続箇所には、ファイアウォールやルータを配備し、ネットワーク分離を行うこと
- ・ 教育ネットワークに接続する機器のウイルス対策ソフトウェアやセキュリティパッチは最新のパターンファイルの更新と適用状況を管理できること

② インターネットのセキュリティ要件

インターネットのセキュリティ対策については、昨今の標的型攻撃³に代表される新たな脅威に対応すべく総合的な対策の導入が望まれる。

インターネットセキュリティとして必要となる新たな脅威に対応すべく総合的なセキュリティ対策の例について以下の表に示す。

表 2-6 総合的対策の例

対策方針	対策の具体例
システムへの入口と経路での防御	ファイアウォール、IPS/IDS、サンドボックス機能等
脆弱性対策	ウイルス対策ソフトウェアのパターンファイルの更新、セキュリティパッチの適用等
標的型攻撃ルートでの対策	スパムメール ⁴ 対策、Webフィルタ等
ウイルス活動の阻害および抑止（出口対策）	Proxyサーバ
アクセス制御	認証、アクセス制御、IDたな卸し、特権IDの厳密な管理
情報の暗号化	重要なデータの暗号化
システム監視、ログ分析	インターネット環境ログ、サーバログ等
管理統制およびコンテンジェンシープラン	ポリシーの徹底、復旧計画、専門家による監視サービス

※参考:IPA「標的型攻撃/新しいタイプの攻撃の 実態と対策」より

(ア) ファイアウォール要件

- ・ インターネットとの接続口にはファイアウォールを設置して通信を制限すること
- ・ ファイアウォール等の装置は、不正な通信に対して検知できる機能があること
- ・ ファイアウォール等の装置は、不正な通信に対して自動的にその通信を制限できる機能があること

(イ) Proxyサーバ要件

- ・ Proxyサーバのログ分析できる事が望ましい
- ・ 業務時間外や、深夜、早朝のWebアクセスがないか監視できる事が望ましい

² サブリカントとは、無線LANの端末認証・暗号化の手順を定めた用語で、認証サーバに対して認証を求める端末や、認証サーバとのやり取りの手順を実装したソフトウェアのこと

³ 標的型攻撃メールを受信し、開封したことで未知のマルウェアに感染し、内部情報がインターネットに流出した事案をいう

⁴ スパムメールとは、迷惑メールのことでトロイの木馬、ウイルス、ワーム、スパイウェア、フィッシング攻撃の媒介として使われることもあり、ウェブサイトへのリンクも含まれることがあります。

(ウ) Webフィルタリング要件

- ・ 教職員や児童・生徒がインターネット閲覧する際に安全に利用できるためのアクセス制御機能があること
- ・ アクセス元のクライアント端末をIPアドレス、認証サーバに登録されたアカウント名で識別できること
- ・ 独自に定義したURL、および URLリストを反映させられることがこと
- ・ Webサイトへのアクセス制限時には、警告画面を表示できること
- ・ 常に最新のURLフィルタリングリストが配信できること
- ・ 全てのアクセス記録を保存でき、後から追跡可能なこと

(エ) サンドボックス機能要件

- ・ 標的型攻撃を検知するため、サンドボックス⁵機能で仮想的に端末と同様の環境を用意でき、マルウェアの可能性が高いプログラムの動作を自動的に検証できること
- ・ 標的型メールに代表されるインターネットメールの添付ファイルについて、マルウェア検知できる機能があること
- ・ 内部の端末がマルウェアに感染した恐れがある場合に、特定のインターネットサーバ（攻撃サーバ）とのインターネット通信（情報漏えいの恐れ）を検出できること
- ・ マルウェア⁶に感染した内部端末の特定ができること
- ・ 特定のインターネット上の不信な外部サーバとのインターネット通信（情報漏えいの恐れ）を検出した場合に、その通信を切断できること

(オ) インターネット環境ログ

- ・ 内部の端末がマルウェアに感染した恐れがある場合に、特定のインターネットサーバ（攻撃サーバ）とのインターネット通信（情報漏えいの恐れ）を検出できること
- ・ インターネットの通信ログについては、許可ログも含めて取得すること
- ・ Proxyサーバで取得できるアクセスログ、Webフィルタリングのブロックログ、サンドボックスで取得できる不審な外部サーバとの通信ログ等の必要なログ情報を取得すること
- ・ インターネット環境のログは、1年以上保管できること
- ・ インターネット環境のログは、外部からの攻撃を考慮して適切なエリアで保管すること

(2) 無線LAN導入時の留意事項

「授業支援系ネットワーク」については、無線LANの導入が想定される。一方で無線LANは、第三者からの通信が盗聴される可能性や、学校が管理していない機器が校内の無線LANに進入してくる可能性があるため、その利用にあたっては認証や暗号化技術等の複合的なセキュリティ対策の実施により安全な環境の整備が望まれる。

① 無線LANにおけるセキュリティ要件

無線LANにおけるセキュリティ対策の要件について下記に記載する。なお、日本教育情報化振興会より「学校の無線LAN導入・運用の手引き」が発行されているため、導入検討の参考となる。

⁵ サンドボックスとは、保護された領域で外部から受取ったプログラムやアプリケーションを動作させることで、システムが不正に操作されることを防ぐセキュリティモデルの事です

⁶ マルウェアとは、ウイルス、ワーム、トロイの木馬を含む悪意あるプログラムの総称であり、電子メール（標的型攻撃メール）、Webサイト、P2P通信、個人USBなどで感染する事が多くシステムの脆弱性を悪用し侵入して、目立たないように活動を試み、他コンピュータへの感染、破壊活動を行ったり、情報を外部に漏洩させたりする有害なソフトウェアの事です

(ア) 無線LANの要件

- ・ 教室等に設置される無線LAN機器は、児童・生徒が届かない高さの場所に設置すること
- ・ 最新の無線LAN規格（IEEE802.11シリーズ）に対応している機器を選定すること
- ・ 接続する端末とアクセスポイントの暗号方式はAES暗号方式を採用すること
- ・ 無線LANに端末を接続する場合には、サブリカントを用いたネットワーク認証をすること
- ・ アクセスポイントのESSIDは表示設定とする⁷（但し、安易に利用者や場所、セキュリティ設定が想定できるようなESSIDの設定を行わないこと）
- ・ アクセスポイントは接続する機器を限定すること
- ・ アクセスポイントの設定、接続状況等を確認できるようにすること。
- ・ 無線LANソフトウェアのバージョン、認証や暗号化の方式については最新の技術動向を踏まえて定期的に見直しすること
- ・ 許可していないアクセスポイントの設置を検知できること。
- ・ 無線LANのアクセスポイント同士の干渉を防止すること。

2.7.3. セキュリティ対策と重要性の認識

新たな脅威への対応やインターネットから情報漏えいを防止するためには、ネットワークを細分化することになる。一方でネットワークを細分化したことで利用者の負担が増加するという意見もある。セキュリティ教育・啓発を通じた利用者の理解を深めると共に、情報連携や共有をネットワーク間で安全に実現する手法の導入も不可欠となる。

(1) 教育ネットワークの分離における留意事項

教育ネットワークを分離することで、「授業支援系ネットワーク」で教員が教材や調べた情報を他のネットワークで活用する手法として「論理的に制限されたデータの受け渡し領域の設置」と「USBメモリ等の外部装置活用」が考えられる。これらの利用に当たってのセキュリティ要求事項例を示す。

① データの受け渡し

- ・ インターネット経由で教材をダウンロードし校務で利用したい場合に、データ受け渡し専用領域を用意すること
- ・ コンピュータウイルス／マルウェア検疫を経てダウンロードした校務用教材を、受け渡し専用領域にのみ保存可能とすること
- ・ 専用領域へのアクセスは「データの読み込み可能とし、データの書き込み（保存）は不可とする設定」とすること

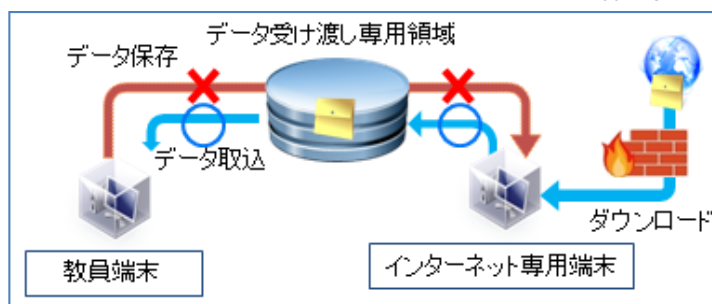


図 2-9 データ受け渡し領域のモデル例

⁷ ESSIDについては、AP側で表示非表示の選択がある。非表示にした場合、端末が、自身に設定されたESSIDを探す動作から結果的に脆弱性を高めてしまう観点から、表示設定を要件に入れている

- ・ データの受け渡し領域は利用者ごとにアクセス制限ができること
- ・ データの受け渡し領域は暗号化できること
- ・ データの受け渡し領域は指定したタイミングで自動的に保存データを削除できること

② USBメモリ等の外部装置

- ・ 校務支援系ネットワークではUSBメモリ等の外部装置は利用しないこと
- ・ 校務支援系ネットワークでUSBメモリ等の外部装置は利用しなければならない場合には、特定の権限者に限定して一時的に利用させること。利用後には、速やかに利用を禁止できること
- ・ 「授業支援系ネットワーク」、「行政系ネットワーク」で利用できるはUSBメモリ等の外部装置は特定できること
- ・ USBメモリ等の外部装置の利用状況をログとして記録できること。
- ・ USBメモリ等の外部装置は暗号化すること。

3. ネットワーク機器に要求される技術

3.1. 物理分離、論理分離、仮想化

一般的に、同じスイッチにつながる端末は同一のネットワークに所属する。ここで同一のネットワークとは、同一のネットワークアドレスを持つグループ(レイヤ2、ブロードキャストドメイン)を意味する。VLANは、1台のスイッチ上に異なるネットワークに属する端末の接続を可能にする技術である。スイッチ上では、VLANは番号で識別され同じVLANに属する端末間は通信が可能であり、異なるVLANに属する端末と通信を行うためにはルーティングが必要となる。この機能を利用することによって同一の物理接続の上に流れるトラフィックを論理的に分離し、仮想的なネットワークをつくることができる。

また、1つの物理的なルータを論理的に複数台のルータに分割できる機能としてVRFがある。VRFを利用すると1台のルータで複数の仮想的なルータを構成することができる。それぞれの仮想ルータにおけるルーティングテーブルは独立し、基本的にVRFをまたぐ転送はできない。

通常、LAN内においてネットワークアドレス(IPアドレス)は重複することはできない。しかし、部門毎に構築されたネットワークの統合などを行う際にはIPアドレス体系が重複してしまうことがある。そのような場合にVRFを利用することでアドレス体系を変更することなくネットワークを統合することが可能となる。

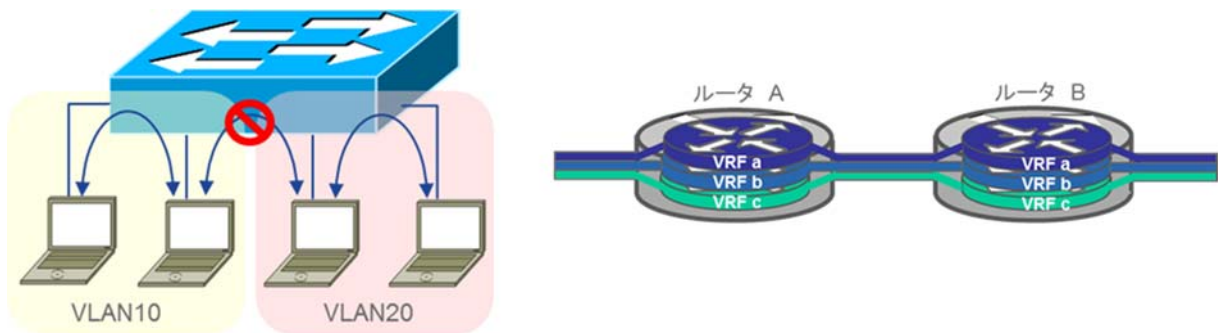


図 3-1 VLAN, VRFによる論理分離

3.2. 冗長化

ネットワークを構築するにあたっては、装置の故障や装置間を接続するリンクに何らかの障害が発生した際にも通信を継続するために通信経路の冗長化は必要不可欠である。しかし経路を冗長化すれば必ず物理的にはループが形成される。

レイヤ2ネットワークではループが発生するとイーサネットフレームは其中で無限にブリッジされ続け、その結果いわゆるストーム(ブロードキャストストーム)が発生し、正常な通信を行うことができない。このような状態になることを防ぐための機能がスパニングツリー(STP)である。スパニングツリーは、ネットワークのループ状態を検出し、必要な箇所のインターフェイスをブロッキング状態(リンクが上がっていてもデータ通信が行えない状態)とすることでループを防止する。通信を行っているリンクに障害があった場合には、スパニングツリーはループのない状態を保ちつつブロッキング状態となっているポートにてその状態を解除することにより通信を継続させる。

IPネットワークにおいては、ネットワークの経路情報管理する手法としてルーティングプロトコル(RIP,EIGRP, OSPFなど)を使用し、ルータが経路情報を自動的に学習するダイナミックルーティングがある。ダイナミックルーティングでは経路情報は動的に学習され、宛先となるネットワークに対し複数の経路がある場合には、トラフィックの転送に最適な経路を選択する。ネットワークの更新をダイナミックに反映できるため、利用中の経路が使用不能となった場合には、その情報を反映し適切な迂回路の選択を行い、通信を継続させる。

3.2.1. 論理多重

装置間に接続する複数の物理インターフェイスを論理的に1本に束ねて利用することを可能とする機能がイーサチャネル(リングアグリゲーション)である。イーサチャネルの効果は、大きく2つあり1つ目は束ねた本数に比例して帯域幅が増大すること、もう1つには高信頼化が挙げられる。イーサチャネルを構成する物理リンクに障害があった場合には、短時間で障害を検知して、該当するリンクを避けるように振り分けアルゴリズムを調整するこれによりスパンニングツリーやルーティングプロトコルのレベルには影響を及ぼさずに傷害に対処して通信を継続することが可能となっている。

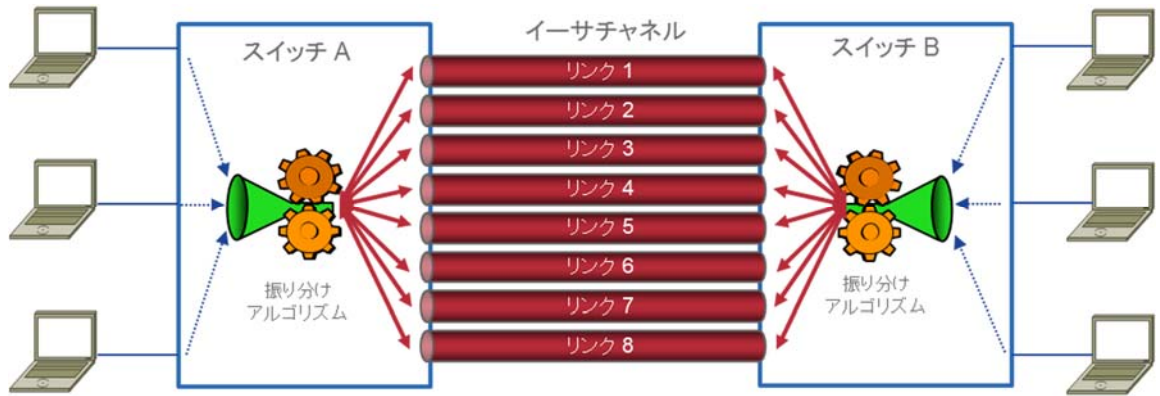


図 3-2 イーサチャネルによる多重化

3.3. サービスの品質確保

IPやイーサネットのサービスの品質を確保するために、優先制御や帯域制御といったQoS技術が用いられる。

優先制御は、パケットやフレームの種類に応じて優先順位をつけ、その順位に従ってルータやスイッチが送信を実行する機能である。帯域制御には、パケットやフレームの種類ごとに帯域を割り当てる“帯域保障”と“帯域制限”の2種類がある。前者は特定の優先度のトラフィックがそのインターフェイスにおいて輻輳時でも利用可能となる帯域を保障する。後者はトラフィックが利用可能な上限値を決め、当該トラフィックによる帯域占有を防ぐ。

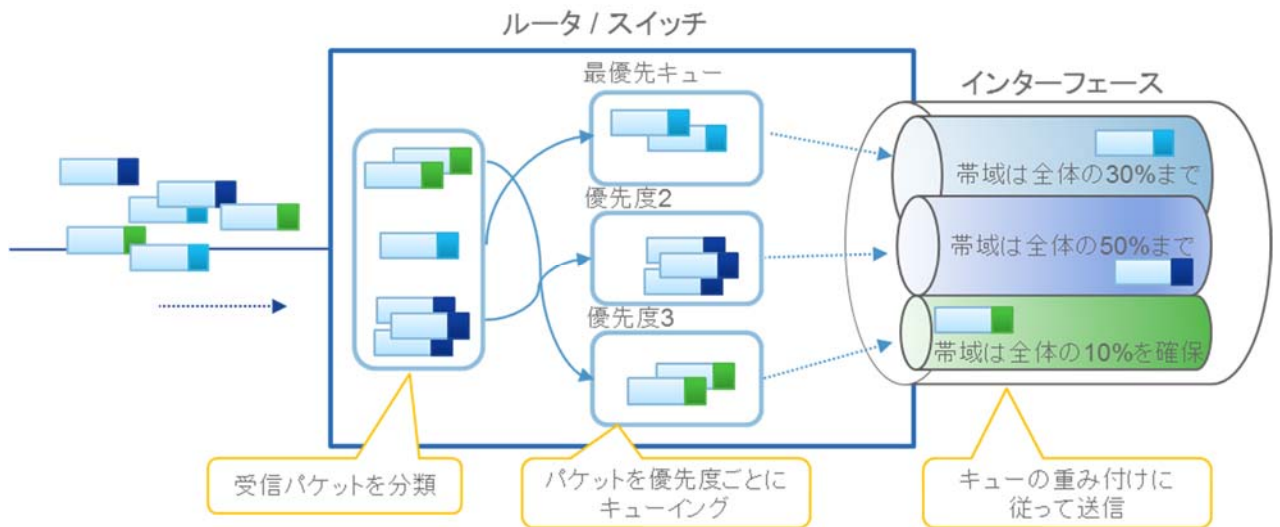


図 3-3 QoS 実行例

3.3.1. 通信容量

トラフィックの見える化として以下2つの方法があげられる。

(1) インターフェイス帯域の把握

ネットワーク機器の各インターフェイスにおいて、どの程度の帯域を利用しているかを把握する。ネットワーク機器に実装されているMIBと呼ばれる情報を利用し、外部管理ツールがこの情報を取得する。

(2) 流れているトラフィック情報の詳細を把握

MIBでは、インターフェイス毎の帯域のみ見える化ができる。より詳細な情報取得のため、ネットワーク機器に実装されているNetFlowと呼ばれる技術を利用することが望ましい。

- ・ 誰が (どのようなクライアント)
- ・ どこへ (どのようなアプリケーションやサーバ)
- ・ どのようなトラフィックを (L5 や L7 レイヤ)
- ・ どれくらい 等

これらの統計情報を収集するとき、偏りをなくすために流れているトラフィックをサンプリングではなく流れているトラフィックの全てで統計情報を測定可能なネットワーク機器を利用することが必須となる。

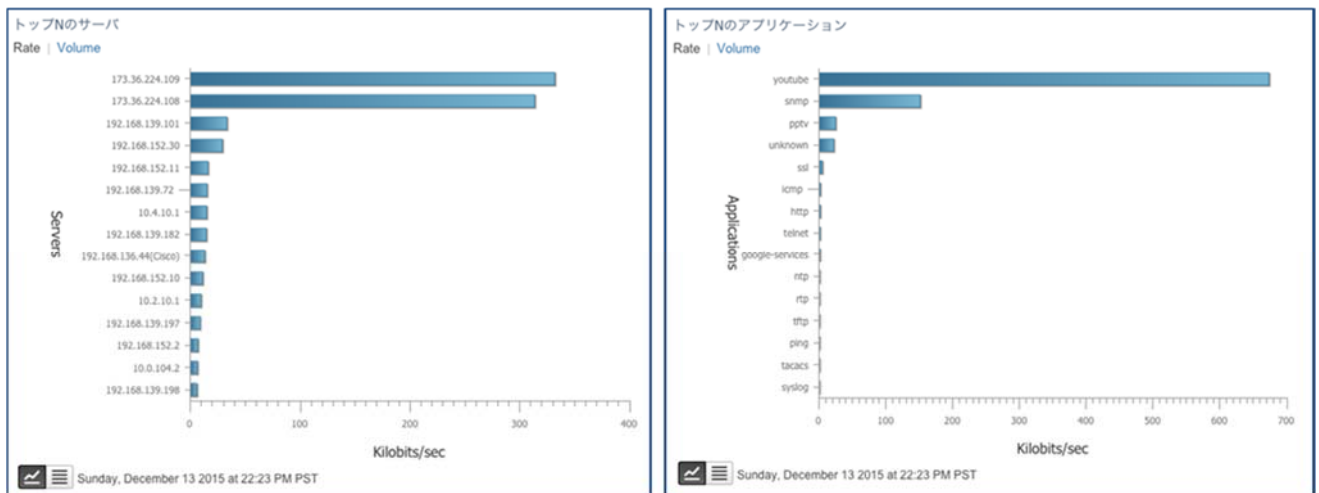


図 3-4 外部管理ツールによるトラフィック可視化のサンプル

3.4. 保守・交換容易性

新規機器導入時や故障交換時を考慮し、初期ネットワーク機器への設定投入の簡素化、そして動作中ネットワーク機器の設定変更の簡素化を考慮する必要がある。

また、これらの設定投入/変更はネットワーク機器個別の専門知識を持たない人でも作業が行えるよう、簡単なGUIを利用した方法が望ましい。

初期設定の投入	複数台のネットワーク機器に対して、同じ手順により設定情報を投入することで作業を効率化する。
ネットワーク機器の設定変更	機器個別や複数機器への一括設定変更が可能な柔軟性のある外部管理ツールを導入する必要がある。
設定情報の世代管理	機器へ設定変更を行った場合、設定変更を行った外部管理ツールが自動で変更情報を収集し世代管理を行う。
故障交換時の設定変更	世代管理を行っている場合、最新の設定情報を利用し簡単にその設定情報を交換機器へ投入することが可能となる。
資産管理	利用しているネットワーク機器のシリアル番号といった機器固有の資産情報を外部管理ツールで一元管理する必要がある。故障交換時はシリアル番号が自動で更新される。

無線LANにおける保守は、干渉源が移動可能なもの（モバイルルータなど）である、特定の時間しか使われない（電子レンジ）など、周辺環境が常時動的に変化するため、システムも自動的にそれらの変化に対応し、全体が一括で把握できる状態にするべきである。

また、製品故障による対策も必要である。具体的には以下である。

- ・ 干渉が発生した場合のチャンネルの自動切換え、出力の自動調節
- ・ システム全体の無線 LAN 環境が 1 箇所で確認できる GUI やツールなど
- ・ 電波環境やトラフィックの履歴管理
- ・ AP を管理するコントローラの冗長性
- ・ AP が故障した場合に、他 AP が電波エリアをカバーできる出力の自動調整

4. 物理配線

教育ネットワークを構築していく上で、実際の校内における屋内配管・配線について、調査段階から施工段階までを順番に参考写真・参考図を使い解説する。

4.1. 屋内配管・配線

4.1.1. ルート調査

(1) 天井、壁状況（ダクト等）確認

物理配線を効率的に敷設できるルートを確認するため天井、壁状況を調査して、天井板の有無やダクトや配管の利用可否や躯体（構造体のコンクリート）に対するコア抜き（床や壁に円筒形の穴を開けること）の可否を確認する。

(2) MDFやEPS等の場所確認

屋外から引き込む電話回線や通信回線をまとめて収容し管理する主配線盤（MDF：Main Distributing Frame）の設置場所、MDFから分岐された配線を各階や各室にて受ける中間配線盤（IDF）の設置場所、並びに各階を縦につなぐ配管設備（EPS：Electric Pipe Space / Shaft）の設置場所の確認を行う。

また、MDFやEPSの利用可否を確認する。

(3) 無線機器設置場所確認

無線機器（アクセスポイント）の設置場所を確認する。

(4) 電源系統の確認

電源系統・配線の状況、利用可否を確認する。

4.1.2. ルート設計（光ファイバー）

- ・ 校舎間等の屋外区間の配線は光ファイバーケーブルを使用する

4.1.3. ルート設計（メタル）

- ・ 屋内区間の LAN ケーブルは UTP ケーブル（カテゴリ6以上）を使用する
- ・ LAN ケーブル布線距離が 100 メートル以上の場合は、中継器を設置すると共に、電源を確保する
- ・ 既存ケーブルとは色を区別し、同一システム内は色を統一する

4.1.4. ルート設計（共通）

- ・ 中継器（収納ボックス）の収容スペースを確保する
- ・ MDF（回線引き込み終端装置）の設置場所を確認・確保する
- ・ 工事図面を設計した上で物理配線工事を実施する

4.1.5. 準備工事（養生・搬入路の確保）

- ・ 建物、既設機器等に損傷を与えぬことと作業上危険と思われる箇所にはあらかじめ防護処置を施す



図 4-1 搬入路

4.1.6. 配線工事留意点

- ・ コア抜き等工事を実施する前に非破壊内部検査を実施する事。また、アスベストの有無を事前に確認する
- ・ 各種ケーブル間の離隔距離を保つ
- ・ LAN ケーブルと電力用および照明用ケーブルの離隔距離は、50mm(2インチ)以上とすることが望ましい（米国規格 ANSI/TIA/EIA-569-A）
- ・ 建物の図面確認を行う
- ・ 防火区画を配線する際は建築基準法を配慮する
- ・ ケーブルの両端にはタグを付ける
- ・ 十分なケーブル余長を確保する
- ・ 配線後の導通試験を実施する

4.1.7. 建設業法上の留意点

- ・ 建設業法に基づき、主任技術者または監理技術者を配置する
<工事イメージ>

(1) 屋内配管工事作業イメージ



図 4-2 配管工事イメージ

(2) 配管の支持方法・支持間隔

下記の支持方法・支持間隔を標準とする。

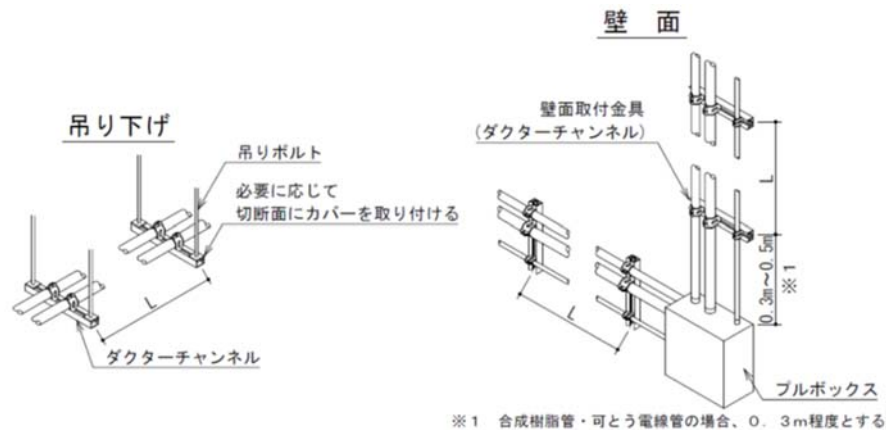


図 4-3 配管の支持方法・指示間隔

(3) 配管の曲げ

曲げ形状は各金属管の規格に定められたノーマルバンド(直角に曲げた配管)を標準とする。標準以外の曲げ形状とする場合は、曲げ半径は配管内径の 6倍以上とする。

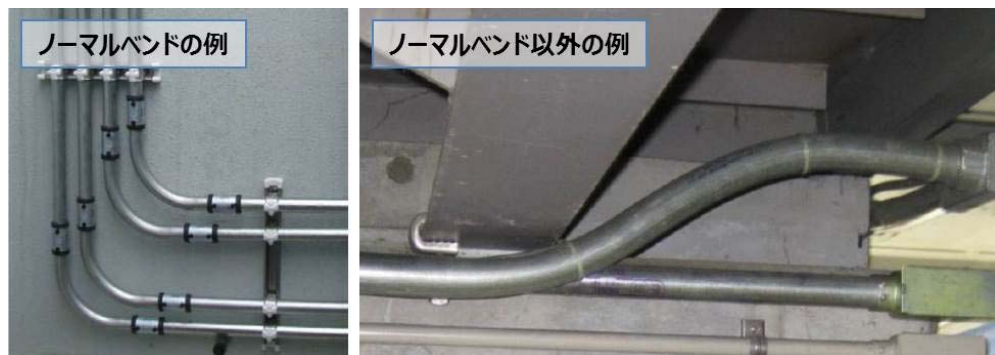


図 4-4 配管の曲げ

(4) 配管のアース

導通しないカップリングや可とう管部分、プルボックスとの接続部等には、アースクランプを取付け、電気的接続が途切れないようにする。

使用するアース線は、IV線(G)を標準とし、接続経路やブレーカの定格電流等に応じて適切な太さのものを選定する。

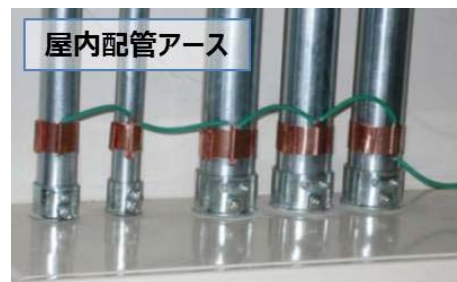
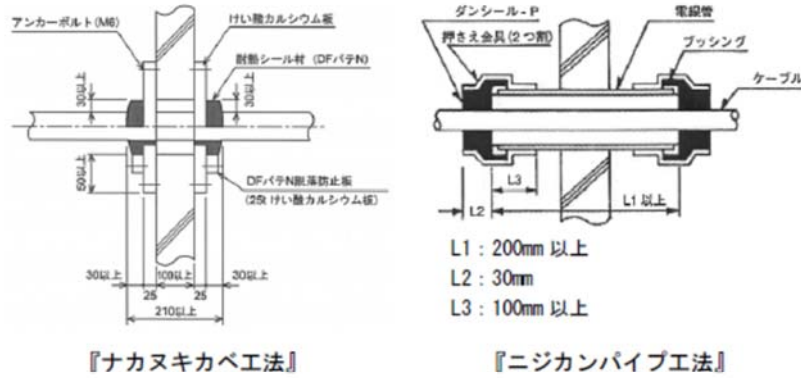


図 4-5 配管のアース

(5) コア抜き貫通部防火措置

配電管その他の管が防火区画を形成する床、壁を貫通する場合は、それらの管と防火区画との隙間をモルタル等の不燃材料で埋め、防火区画から1m以内の管(両側)を不燃材料で造らなければならない。(建築基準法施行令第112条第15項、第129条の2の5第1項第7号)

その他、国土交通大臣の認定を受けた防火措置工法(防火時間は最長1時間)で処理することも出来る。



認定工法による防火措置を実施する際、使用材料の品質管理と適正な施工を確保するため右記の「工法表示ラベル」を使用する。



図 4-6 工法の一例

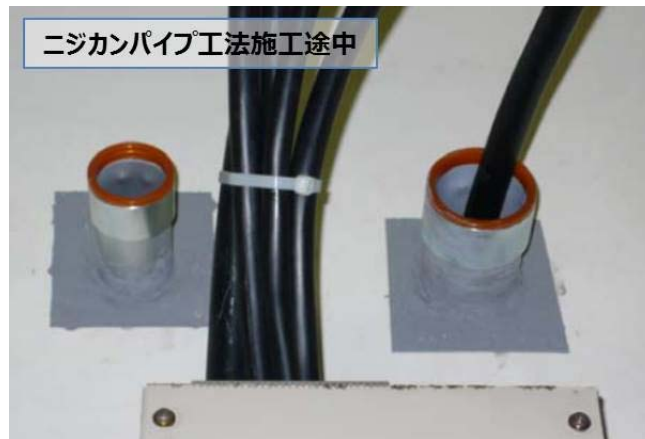


図 4-7 コア抜き貫通部防火

4.2. 無線

802.11acは5G帯を利用するため、障害物が少ない見晴らしの良い場所に設置することが望ましい。最終的なAP設置場所を決めるには、現地でのサイトサーベイが必要である。サイトサーベイの注意点を以下に示す。

- ・ 机・椅子などが教室にある通常利用環境に近い状態で行うこと
- ・ 人も電波を減衰させる原因となるので、可能であれば人がいる状態が望ましい

4.2.1. 設置場所

(1) 設置推奨場所

- ・ 天井(表側)
- ・ 壁の高い位置(3メートルほど)

(2) 設置非推奨場所

- ・ 天井裏や床下
- ・ 足元に近い位置
- ・ 屋内用 AP を屋外に設置すること

4.2.2. 干渉源、遮蔽物による影響

- ・ 金属やコンクリート、レンガは電波を遮蔽するため、これらの影響が少ない箇所に AP を設定する必要がある
- ・ 1つの AP で複数教室をカバーする場合は、廊下に設置するなどの検討が必要な場合がある
- ・ 建物のガラスや人、空気中の水分などでも電波は減衰する(弱くなる)。そのため、サイトサーベイは、実利用に近い環境で実施する必要がある

4.2.3. アンテナ

- ・ 壁に設置する場合は指向性のパッチアンテナなどを利用して電波が効率良くカバーされるよう考慮する
- ・ 講堂など人が通常より密集するエリアで無線LANを提供する場合、セルサイズをさらに小さくする高密度用途のアンテナを使用し、さらに高密度Wi-Fiな環境でも安定した通信を提供すること

4.2.4. APの堅牢性

アクセスポイントは通常人が見える位置に設置することが多い。そのため、子供が誤って物をぶつけても壊れにくい堅牢性を考慮すること。

5. 運用に必要な要件

5.1. アプリケーション・データの設置場所に必要な運用要件

アプリケーションやデータの設置場所に求められる運用要件について記述する。

想定される設置場所は、学校内サーバ、データセンタ、クラウド(パブリック/プライベート)となるが、学校では職員室やコンピュータ教室にサーバが設置されているケースが多いが、サーバを管理するには専門知識が必要となり、その業務が教員の負担となる。

データセンタやクラウド環境の場合、専任担当者による維持管理やサービス提供者によるバックアップサービスが提供されていることも多いため、教員の作業負担を軽減することができるが、教職員以外の管理に対してセキュリティ上の考慮が必要となる。

5.1.1. データセンタ、クラウドなど

サーバ群は、通常堅牢なデータセンタで管理されており、『強固なセキュリティ対策』『システムの二重化』『24時間365日の監視体制』『耐震対策』『UPS・自家発電設備設置』など強固なセキュリティ対策や万全のデータ保全の仕組みが構築されている。

そのため利用者が高セキュリティの環境を用意できるほか、安定した電源の供給や空調設備等の提供を行う必要がない。また災害時の場合、現地と距離を置いた場所に設置されていることが多いことから、データ保全についても安心して活用できる環境を用意できる。

5.2. ネットワークの運用に必要な要件

5.2.1. SLA

(1) サービスレベル管理

利用者(教育委員会、学校関係者、および保護者・地域住民等)が日常的に安心して業務遂行およびサービス利用できる必要がある。

そのため、校務システムおよびネットワークシステムのサービスレベルを定義し、委託者と受託者が責任を持ってその品質を維持することが必要である。

表 5-1 サービスレベル管理

サービスレベル項目（例）		内容（例）	基準値（例）
システムの可用性	稼働時間	全体サービス提供時間	平日8:00～20:00 (計画停止は除く)
	稼働率 (ネットワークに関する障害は除く)	全体サービス提供時間のうち、実際に利用可能な時間の割合	99.9%以上 (サービス時間に対する割合)
	計画停止	定期点検、修正モジュール適用等で計画的にシステムを停止する時間 (緊急度の高い修正モジュール適用の場合は除く)	月10時間以内 (開庁日6:00～24:00を除く)
サービスデスクからのエスカレーション受付・対応	受付時間	平日（土・日・祝祭日・年末年始を除く）の8:00から18:00まで	電話応答率 90%以上 問題解決率 90%以上 (24時間以内)
サービス運用	データセンタ内障害対応	復旧するまでの平均時間	4時間以内
	障害の復旧予定時刻の報告	障害報告受付から教育委員会に対する復旧予定時間を報告するまでの時間	2時間以内

(2) SLA維持のための監視業務およびヘルプデスク

SLAを維持するためのネットワークおよびサーバ機器等の死活、負荷、障害、性能などの状況と各種セキュリティの維持管理を適正に行う必要がある。

また、教育委員会および学校が本来の業務に従事できるようにヘルプデスクにて構成管理を含む管理業務および利用者からの依頼に基づく変更管理を迅速かつ正確に行うことが求められる。

① 監視業務

監視業務の対象は下記の通りである。ただし、受託者の提供するサービスによって、さらに必要となる監視要件は責任もって対応する必要がある。

- ・ ネットワーク死活監視
- ・ 負荷監視
- ・ セキュリティ監視
- ・ 障害監視
- ・ 性能監視

② ヘルプデスク

ヘルプデスクの業務要件として下記の対応を行うこと。ただし、受託者の提供するサービスによって、さらに必要となるヘルプデスク業務は責任を持って対応する必要がある。

- ・ ID 管理
- ・ 構成管理
- ・ 各サービスのポリシー変更受付、対応
- ・ 各サービスのログ調査、報告
- ・ 資産情報管理
- ・ 各種通知、情報配信

5.2.2. システム状況の外部公開

教育ICTのネットワークやサーバの運用状況を、教育委員会側や、自治体の情報システム側で参照する場合がある。

例えば、ネットワークの障害通知や、負荷状態を把握する、許可されていない無線LAN端末の発見など、このような場合、情報公開するための経路からの侵入(入口出口でのファイアウォール等による監視、盗聴(途中経路での暗号化など)への対応を行う。

また、情報の閲覧には、公開を許可された職員であるかどうかの認証は必須であり、誰がいつ閲覧したかの履歴は一定期間保存することで、利用者への抑止力にもなる。

5.2.3. ヘルプデスク

学校現場におけるネットワーク運用の特長として、ネットワーク専任の対応者がおらず、トラブルが発生した場合、障害検知、一次切り分け、対処方法などが難しいと想定される。

そのため、下記のようなフォローをヘルプデスクで実施することにより円滑なネットワーク運用を実施し、授業や校務などの業務に支障がないよう、十分配慮が必要である。

(1) トラブル時の一次対応及び切り分け

現場教員からの問合せ等に対し、一次切り分けを行い、回答可能なものはその場で対処する。不可能なものはエスカレーションフローに則って各メーカー、ベンダー、SE/CEにエスカレーションを実施する。

(2) リモート保守を含む操作問合せの対応

一次切り分けを円滑に実施するために、現象の切り分け、確認、PC操作を含む対応を行うなど、きめ細やかなフォローをする必要がある。また、必要に応じて、セキュアな通信環境下でのリモート接続を許可し、一次対応を行わせることも検討する。

(3) インシデント (QA履歴) 管理

ネットワークが起因するトラブルに関して、校内・教育イントラ内、インターネット回線などを切り分け、日々発生する問合せへの対応を記録させる。併せて、定期的な報告書を作成させることにより、次年度予算化の検討材料とする。

(4) 土日祝日対応・サービス提供時間の延長

学校では授業参観日等、土曜日に授業がある場合もあり、また夕方の児童・生徒の帰宅後によりやく教員業務が

行えるなどのケースが想定される。このような利用を想定し期間や時間延長を検討する必要がある。

(5) 運用支援（追加アプリ・ドライバ等のインストール作業代行(管理者権限での処理代行)

日々の運用の中で、パソコンやタブレットへ新たにアプリケーションやドライバを追加インストールが必要となることが考えられる。追加インストール作業は、基本的に管理者権限が必要であり、先生方にてインストールすることを禁止している場合がある。その場合は、ヘルプデスクによるインストール代行等の運用支援を契約することも検討する必要がある。

5.2.4. オンサイト保守

学校現場におけるネットワークトラブル等の障害に関して、授業や校務での利用ができなくなるケースに対し、緊急で対応する必要がある。これらを円滑に行うため、下記のような保守契約を検討する必要がある。

(1) ハードウェア障害対応

サーバ機器をはじめ、パソコンやタブレット、ネットワーク機器等のオンサイト保守を契約すると、機器の早期復旧が見込まれる。オンサイト保守は通常のセンドバック等の通常保守と比べ、金額が高くなるため、必要有無については、各機器障害発生時の影響度について取りまとめ、影響度が高いものから優先度をつけ、優先度順にオンサイト保守を検討する。

(2) ネットワーク障害対応

現場におけるネットワークトラブルは、授業の中断や業務の中断が発生するため、ネットワーク保守ベンダーによるオンサイト保守を結ぶことを推奨する。

(3) ヘルプデスクでは対処が出来ない、難易度、ボリュームの作業実施依頼

ヘルプデスクによる運用支援では、難易度が高い作業および非常にボリュームがある作業について、契約することは難しい。よって、これら作業が発生することが見込まれる場合は、オンサイトでの作業依頼を検討する必要がある。

(4) オンサイト保守対象範囲の確定

オンサイト保守契約を結ぶにあたり、ベンダーとの間で対象範囲を明確にすることが重要となる。保守契約を結ぶ際には、対象範囲を书面化し、双方認識合わせを必ず行う。

(5) オンサイト保守対象範囲外の対応方針

上記、保守範囲を明確化する際には、併せて、オンサイト保守範囲外の事項についても取りまとめ、障害が発生した際の対応方針についても検討しておく必要がある。

5.3. 教育利用者特有の運用要件

ネットワーク・端末・周辺機器の調達や、授業支援・校務支援等のシステム調達の部門が分かれる場合があるため、学校現場での運用に配慮する必要がある。

また、学校ネットワークを利用する利用者は、教職員、児童・生徒が中心となるが、それ以外にもシステム委託事業者、ICT支援員等も想定されることから、学校固有の要件に関する注意事項を下記に示す。

5.3.1. システム委託事業者のアカウント管理

システム委託事業者が、学校ネットワークに導入されている機器の運用保守に携わるため、その権限の管理については厳密に実施することが望まれる。具体的には、システム標準のIDを廃止し、作業者毎にIDを付与すると共に、操作の記録を取得することが考えられる。

5.3.2. ICT支援員

情報端末を利活用した授業の実施にあたってICT支援員が学校に配備されている機器を利用する場合がある。この場合に備えて、ICT支援員に必要な権限を検討して、その権限に適したアクセス制御を設定することになる。特に、ICT支援員が成績情報等の重要な情報にアクセス出来ない設定とする。

5.3.3. PTAの利用

PTA活動の一環で学校ネットワークの機器を保護者が利用する場合が想定される。この場合に備えてPTAが利用する機器は限定すると共に、学校ネットワークとして実施しているウイルス対策やデータの保全や不要なデータの削除等の対策の徹底を依頼する。

学校ネットワークは、重要なネットワークとなることから保護者が機器等を増設しないように技術的な制限も検討が必要となる。また、保護者が学校にデータを持ち込む場合には、ウイルスチェックを義務付ける必要もある。

5.3.4. 学校の敷線管理

学校ネットワークを整備すると、学校に電源配線や物理的なネットワーク配線されることになる。

今後、学校ネットワークを維持するため、これらの配電図、配管図、配線図等の設計図書を工事事業者に納品を求め自治体・教育委員会で一括管理することが不可欠となる。特に、施設部門が教育委員会以外にある場合、連携を充分とり、資料の最新化に留意する必要がある。

5.3.5. 教育委員会

- ・ 学校のCIOである校長が全体像を把握できるよう、調達各部門では連携してシステム全体を取りまとめる必要がある
- ・ アカウント管理等、システムの運用に関する権限の設定・変更等の運用をどの部門が行い、運用に必要な作業は誰が行なうかを決定し、公開する必要がある
- ・ 学校と連携し、セキュリティ監査や各種の訓練の企画など、運用体制の強化や見直しのための活動を行なう必要がある

5.3.6. 学校

機器やシステムの性格により、学校での担当者は別になることがあるが、校務分掌に位置づけることで明確にし、相互の協力体制をとる必要がある。

5.3.7. 外部組織への業務委託

教育委員会は、外部組織に対して業務委託を行なう場合、契約に基づく各種運用方法を明確にし、学校に運用を依頼する必要がある。

- ・ ICT支援員：作業内容の範囲・巡回頻度・学校内の依頼ルール 等
- ・ コールセンター：問い合わせ内容の範囲・コールは学校担当者からか各教員からか等のルール 等
- ・ 機器障害や破損の場合の対応ルール 等
- ・ その他の委託内容のルール 等

6. 利用シーンによるバリエーションの選択要件

ネットワークに要求される要件は利用用途により変化します。よって、この章では、利用シーン別の要件および検討事項を洗い出す。

また、前段では、データセンタもしくはクラウドサービスを利用する場合に検討が必要となるキャッシュサーバや学内専用サーバについて記述する。

6.1. キャッシュサーバおよび学内専用サーバ設置検討

データセンタもしくはクラウドサービスを利用する場合、各学校のアクセスがデータセンタ/クラウドサービスに集中するため、十分なネットワーク速度が得られない場合が想定される。

よって、利用頻度が高く、ネットワークに負荷が掛かる下記のシステムについては、学校単位もしくはデータセンタ内にサーバを設置することを検討する。

6.1.1. デジタル教科書

更新があるたびにインターネットからコンテンツをダウンロードする必要がある。デジタル教科書のコンテンツは、非常に容量が大きいので、夜のうちに、データセンタ内もしくは学校単位に「キャッシュサーバ」というクライアントへのコンテンツ配信サーバを設置することを検討する。

6.1.2. ファイルサーバ

課題、参考資料を、ファイルサーバへ蓄積しておき、授業で利用することは多々ある。データセンタやクラウドでもファイルサーバを設置することは可能だが、インターネット越しのアクセスでは、十分なパフォーマンスを得られない可能性があるため、ファイルサーバ機能を持たせた「学内専用サーバ」を学校単位で設置することを検討する。

上記以外のシステムでも、利用者、利用頻度、コンテンツのデータ容量の大きさ等を考慮の上、必要に応じて、サーバを校内ネットワーク内に設置することを検討する。

※VDI等を利用する等で、データのやり取りがデータセンタもしくはクラウドサービス内で完結する場合は、この限りではない。

6.2. 授業支援系ネットワークの利用シーン別検討事項

授業でタブレット端末を利用することを想定し、授業の環境準備、一斉授業、個別学習の利用シーンを想定した検討事項を記述する。

6.2.1. 環境準備

(1) 環境復元ソフトウェア検討

児童・生徒が利用した個人データを端末内に残さないことを目的に、環境復元ソフトウェアを導入することを検討する。

(2) 端末の自動更新タイミング検討

端末脆弱性対策のため、定期的にOS/アプリケーションのアップデートを実施する。ただし、自動更新時はネットワークに負荷がかかり、且つ端末も利用できなくなる可能性がある。

よって、タイミングについては、日中に更新することは難しく、夜間もしくは休日に自動更新が掛かるようにシステムを構成する必要がある。

各学校のインターネットアクセスが、データセンターやクラウドサービスを経由する場合は、各学校のアップデートタイミングをずらすなど考慮する。

(3) 教材配布等による情報教育ネットワークから校務支援系ネットワークへのアクセス方法の検討

教材配布用データを先生が校務支援系ネットワーク内のファイルサーバに保存した場合、授業で利用するためには情報教育ネットワークから校務支援系ネットワークにアクセスし、教材を配布する必要がある。

通常、情報教育ネットワークから校務支援系ネットワークへのアクセスは許可しない。よって、情報教育、校務支援系ネットワーク間の通信を許可する端末を電子黒板用端末のみに制限する等検討する。

校務支援系ネットワークにアクセス可能な端末については、児童・生徒から簡単に利用されないような仕組みが必要となる。例えば、児童・生徒のアカウントではログイン出来ないようにする等認証ルールが必要となる。

6.2.2. 一斉授業

(1) 児童・生徒全員への一斉配布/回収の運用検討

一斉授業でクラス全員に課題配布や回収を行うことが想定される。無線APを利用するため、大きいサイズのファイルの一斉配布/回収時は時間が掛かることを想定した準備を行う必要がある。併せて、大きいサイズのファイルの一斉配布/回収を想定し、QoS等を利用した帯域制御を行う等、ネットワークに負荷がかからない設計もしくは運用を検討する。

(2) 児童・生徒全員の斉操作の運用検討

一斉授業で児童・生徒全員による動画閲覧、インターネット閲覧等を行う場合、ネットワークに負荷がかかることが想定される。よって、QoS等を利用した帯域制御を行う等、ネットワークに負荷がかからない設計もしくは運用を検討する。

6.2.3. 個別学習

(1) 授業外利用の運用検討

端末を授業外で利用するもしくは持ち帰りを想定する場合、利用者を特定する下記のような仕組みを導入することをお勧めする。

- ・ 認証の多重化(2要素ログイン)
- ・ 利用方式の限定(USBキーの有無によるシステムへのアクセス)

また、端末の持ち出しが難しい場合もあるため、VDI等のリモート接続を利用し、家庭の端末からでもセキュアに校務支援系ネットワークを利用可能なソリューションも検討する。

6.3. 校務支援系ネットワークの利用シーン別検討事項

校務システムをタブレット端末で利用することを想定した検討事項を記述する。

6.3.1. 校務支援システムの利用

(1) 校務支援系ネットワーク接続端末検討

校務支援システムを利用する端末は、よりセキュアなネットワーク内で利用する必要がある。よって、認証の

多重化等、利用者を限定する仕組みを導入することを検討し、且つ、校務支援系ネットワークへの接続可能な端末を制限する仕組みを検討する。また、データの持ち帰り等についてもセキュリティポリシーを取り決め、内容次第によっては、USBメモリ利用禁止等の仕組みを検討することも必要となる。

(2) 校務支援システム利用者制限の検討

児童・生徒の個人データを取り扱う校務支援システムは、利用するユーザを限定し、ユーザを特定する仕組みを導入する必要がある。ユーザを限定/特定する仕組みとしては、認証の多重化やアプリケーション内でのユーザ権限設定による、利用範囲の限定を検討する必要がある。

(3) 年度末の指導要録等の作成・印刷

年度末、指導要録等を作成し、印刷する際、印刷が集中すると、ネットワークの負荷が非常に高くなることが懸念される。よって、負荷を軽減させるために、印刷のタイミングをずらす等の運用が必要となる。また、タイミングをずらす等の運用が出来ない場合は、校務支援用端末を有線で接続する、プリントサーバを経由せず、直接印刷を行う、プリントサーバを校内に設置する等の検討が必要となる。

6.4. 災害時避難場所として利用する場合

6.4.1. 無線LAN環境、インターネットアクセスの提供

一般向けのインターネットアクセス用の無線LANを提供するためには、セキュリティの観点から無線LAN区間からインターネットに出るルータまでの有線区間まで一貫して学校のネットワークと論理的に分離されている必要がある。

また、学校で利用するSSID以外に別途SSIDをあらかじめ用意しておき、緊急時にすぐにオンにできるようにしておく必要がある。

また、開放する通信については、学校のシステムに入れないように分離する必要があるが、分離の考え方については、「3.1 物理分離、論理分離、仮想化」を参照したうえで、事前設定すること。

7. 利用拡大に向けた留意事項および補強のポイント

現在の学校におけるICT環境の整備状況は以下のとおりとなっている。

- ・ 教育用コンピュータ1台当たりの児童・生徒数 6.4人
- ・ 電子黒板・実物投影機の整備 総学級数の7%
- ・ 超高速インターネット接続率 82%、無線LAN整備率 27.2%
- ・ 校務用コンピュータ 教員1人1台：113.9%
⇒84台/校（100）

ただし、地方公共団体間の差異が拡大している。

第2期教育振興基本計画で目標とされている水準として以下が提示されている。

（文部科学省発行パンフレットより）

- ・ 教育用コンピュータ1台当たりの児童・生徒数 3.6人
 - ◇ コンピュータ教室 40台
 - ◇ 各普通教室1台、特別教室6台
 - ◇ 設置場所を限定しない可動式コンピュータ 40台
- ・ 電子黒板・実物投影機の整備（1学級当たり1台）
- ・ 超高速インターネット接続率及び無線LAN整備率 100%
- ・ 校務用コンピュータ 教員1人1台
⇒123台/校（146）

また、先進的な地域やモデル校などでは、児童・生徒1人1台の導入を想定
⇒379台/校（451）

7.1. 整備のシナリオに影響を与える事項

フェーズ	現行	3.6人/台	1人1台
整備台数	84台/校	123台/校	379台/校
指数	100	146	451

端末台数の増加に伴い、学校からの回線は、最近では、1Gbpsなどの回線の採用や複数の回線の引き込みをしている場合もある。

特に、動画サイトの活用を考える場合には、タイムアウトになる前に動画データを読み込むだけのネットワーク性能の確保や、キャッシュサーバの活用などを必要がある。

セキュリティの観点では、BYOD⁸の場合を含め、利用者以外の端末接続の排除や、利用者端末の状態を把握してネッ

⁸ *BYOD: Bring Your Own Deviceの略。私物の情報端末を一定の条件下で活用することを言います。この場合、私物の情報端末を安全安心に接続できる十分なネットワークや授業環境の整備と情報端末で利用できるシステムの整備が必要となります。公立学校では佐賀県教育庁がBYODの本格事例。

トワーク接続の可否を判断する検疫ネットワークなど、安心安全に活用できる検討が必要になる。

校外での端末利用を考える場合には、Wi-Fiルータの利用や無線WANのポートを持つ端末を利用したLTE/4Gなどを検討する必要がある。反転授業などで使う場合には、回線機能を必要としない場合もあるので、利用目的とコストのバランスに配慮する必要がある。

7.2. ICT環境整備のパターン例

文部科学省のICT環境整備パターン例では、以下が例示されている。

- ・ モデル校設置型
- ・ 均等整備型
- ・ 教員用機器先行整備型
- ・ 教員配備型
- ・ 全校一斉整備型

教育用PC、教員用PC/電子黒板/プロジェクタ、無線LAN環境、校内LAN/インターネット接続、サポート体制に関する留意事項が示されている。

ICT環境整備のパターン例と整備における留意点～各地を視察させていただいて感じたこと～
7

整備パターン例

モデル校設置型

数校をモデル校（研究校・実証校）として先行して整備を行い、実証成果を踏まえて他校に展開

均等整備型

地域内の全校で同時に整備を徐々に展開

教員用機器先行整備型

教員の授業用機器を先行して整備

教員配備型

地域内の教員に複数台のタブレットPCを配備し、徐々に対象教員を増加

全校一斉整備型

地域内の全校で一斉に整備

※上記パターンを組み合わせる段階的に整備するパターンもある。
 (例) モデル校設置型→均等整備型
 (例) モデル校設置型→教員用機器先行整備型→均等整備型

教育分野におけるICT活用推進のための情報通信技術面に関するガイドライン（手引書）—総務省—



2013年
小学校版



2014年
中学校
特別支援学校版



「ICT教育環境整備ハンドブック」
2015年版
(日本教育情報化振興会発行)

整備における留意点

教育用PC（児童生徒用タブレットPC）

- 屋外や雨天時での使用、持ち帰り時の衝撃（自転車で乗せての登下校等）、持ち歩き時の落下等を考慮した設計
- 授業中のフリーズの回避（児童生徒は反応が遅ければ何度もタッチする）
- 異なる児童生徒が1台のPCを使用することを想定したログイン方法、データ保存（フォルダの構成）及び管理方法等の確立
- 1日の授業時間（6～8時間）を考慮した連続駆動時間の確保
- 電源容量の確保及び電源コンセントの設置
- カメラ機能を多用している事例が多い

無線LAN環境

- 「同じ時間帯に」、「学校内で」、「同時に数十名、数百名が通信」を行うことを想定したアクセスポイントの設置
- 学校外からの電波の飛び込みへの対処

教員用PC/電子黒板・プロジェクタ

- 電子黒板やプロジェクタへの簡単な接続（特に教科担任制の場合は、毎時間、異なる教員が異なるPCを接続する必要がある）
- 黒板との併用方法に応じた電子黒板・プロジェクタの設置
- 電子黒板の場合、遮光カーテン等映り込み防止策が必要な場合あり

校内LAN/インターネット接続

- ネットワーク構成を把握した上で、活用したい授業内容に応じた回線速度の確保（特に動画視聴を念頭に置く場合）
- フィルタリング措置の徹底及びフィルタリング設定変更方法の周知

サポート体制

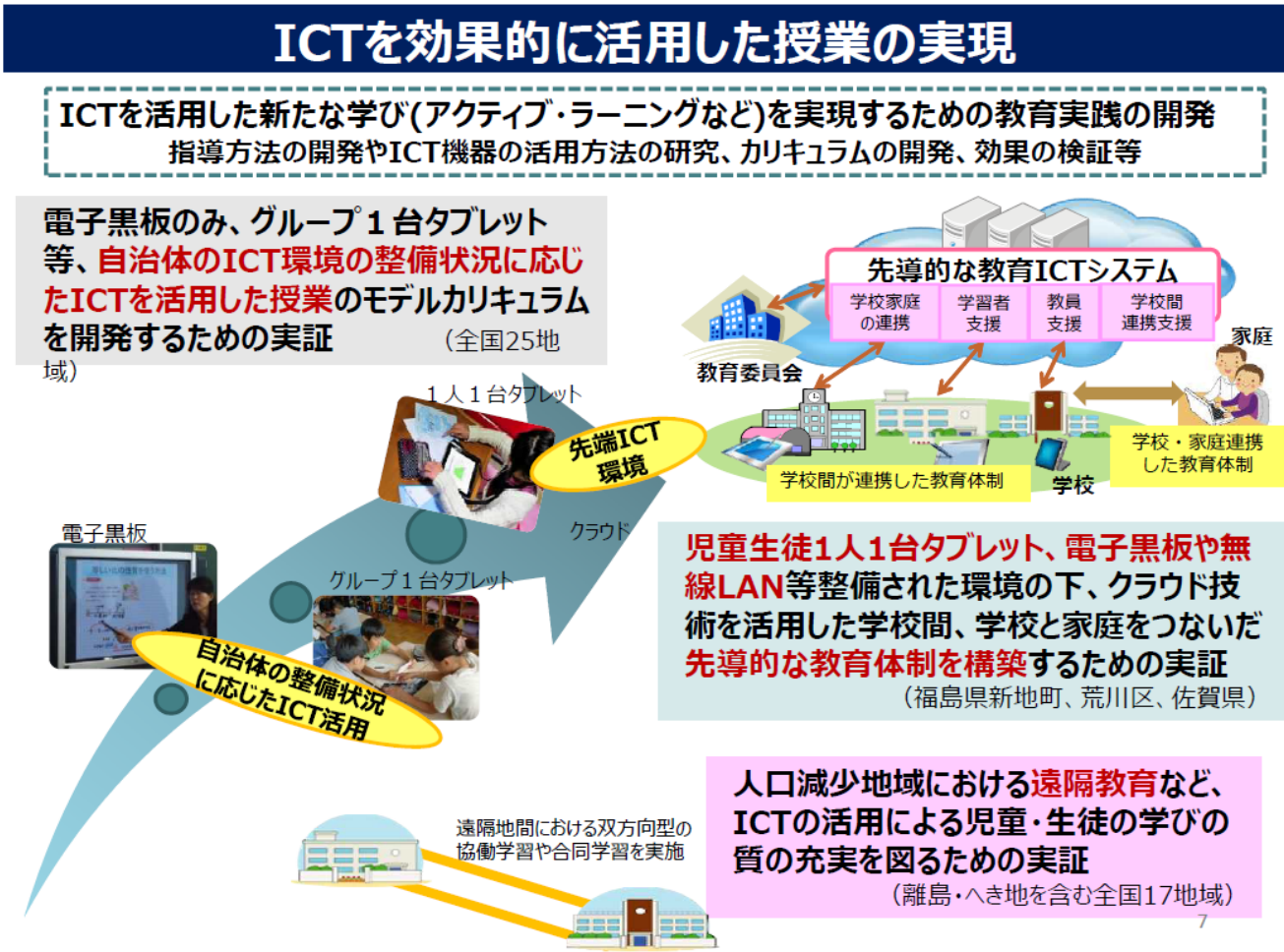
- 機器、ネットワーク、サーバー等のトラブル、備品（タッチペン等）交換への対応（授業は止められない）
- ICT支援員の派遣やサポートセンターの充実

文部科学省発表資料より

また、ICTを効果的に活用した授業の実現を目的に、ICTを活用した新たな学び(アクティブ・ラーニングなど)を実現するための教育実践の開発するため、指導方法の開発やICT機器の活用方法の研究、カリキュラムの開発、効果の検証等が施策として行なわれている。

- ・ 自治体の ICT 環境の整備状況に応じた ICT を活用した授業のモデルカリキュラム開発
- ・ 人口減少地域での遠隔教育など ICT 活用による学びの質の充実を図るための実証
- ・ 児童・生徒 1 人 1 台タブレット、電子黒板や無線 LAN 環境での先導的な教育体制実証

が例示されている。



文部科学省発表資料より

7.3. 整備の具体的な考え方

「学校の無線LAN導入・運用の手引きVer. 1.00」(一般社団法人 日本教育情報化振興会(JAPET&CEC)教育の情報化政策検討委員会 学校の無線LAN導入・運用の手引き作成WG)のユースケースの整理が参考となる。

<http://www.japet.or.jp/jowl6rz5-919/>

7.3.1. ユースケースについての考え方

(1) ユースケースの整理

実現したい学習場면을、

- ・使用イメージ：先生一人の使用と、クラス全員の使用
- ・運用イメージ：学校だけで運用、自治体／教育委員会の管理者が運用の組み合わせで考える。

		運用イメージ		想定される学習場面
		学校で運用	教育委員会／自治体で運用	
使用イメージ	先生もしくは複数人で共有して普通教室で使用	ユースケース (1-a)	ユースケース (1-b)	【一斉学習】 教員による教材の提示 電子黒板、実物投影機等を用いた分かりやすい課題の提示 ※指導者用デジタル教科書の使用 【協働学習】 発表や話し合い 考えや作品を提示・交換しての発表や話し合い 協働での意見整理 複数の意見や考えを議論して整理 協働制作 グループでの分担や協力による作品の制作 学校の壁を越えた学習 遠隔地の学校等との交流
	先生、児童生徒全員が普通教室で使用	ユースケース (2-a)	ユースケース (2-b)	【個別学習】 個に応じた学習 一人一人の習熟の程度などに応じた学習（ドリル教材等） 調査活動 インターネット等による調査 思考を深める学習 シミュレーション等を用いた考えを深める学習（英会話等） 表現・制作 マルチメディアによる表現・制作 ※児童生徒用デジタル教科書の使用

a：学校で運用…教育委員会／自治体が学校の校内LANを監視・管理していない

b：教育委員会／自治体で運用…教育委員会／自治体が学校の校内LANを監視・管理している

図 7-1 ユースケースの整理

(2) 段階的整備の考え方

トライアル校と地域全体、コンピュータ教室のタブレット化・グループに1台分の台数整備・クラスで一人一台分の台数整備でシナリオを考える。

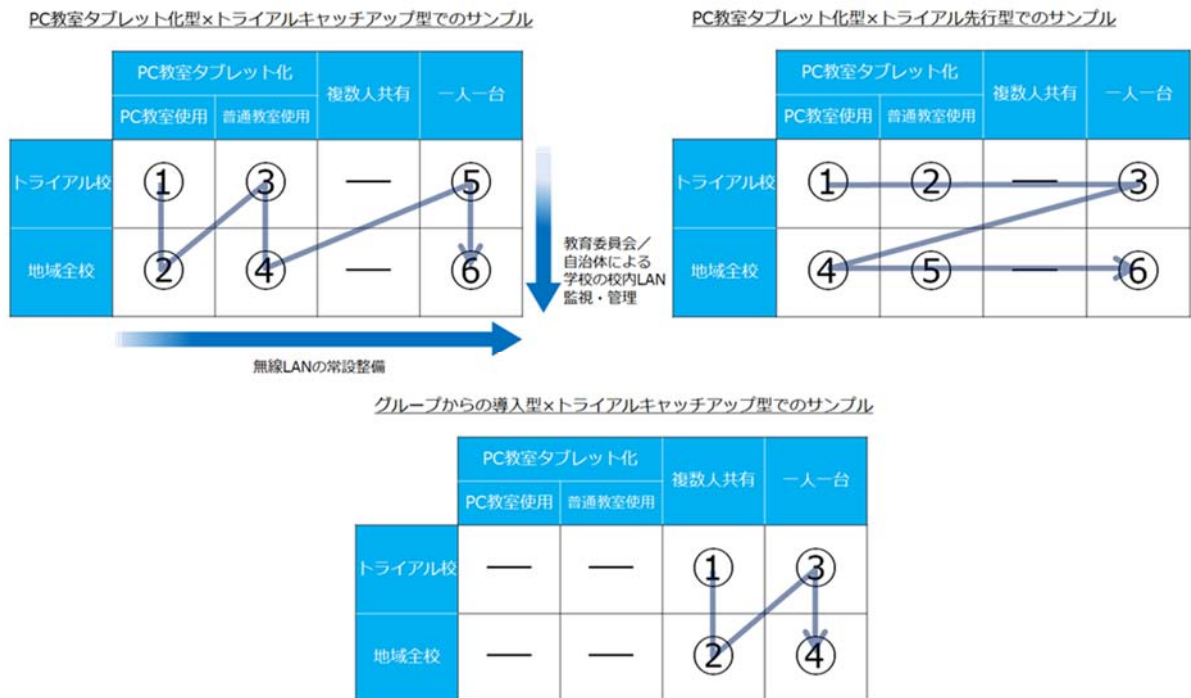


図 7-2 段階的整備の整理

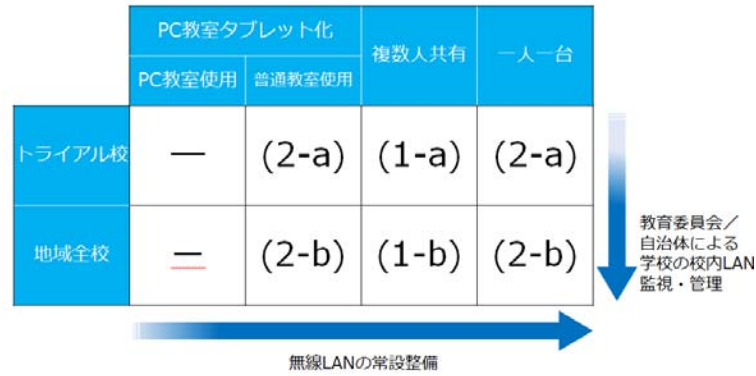


図 7-3 ユースケースと段階的整備

・ シナリオサンプル ㉑ <グループからの導入型>

- Step. 1…コンピュータ教室の設備とは別に複数人共有用のタブレットPCを導入
- Step. 2…可搬型無線LAN設備を導入（普通教室で使用する際は可搬型無線LAN設備をその都度移動）
- Step. 3…普通教室に無線LANを整備（数人共有用のタブレットPCを常時普通教室で使用可能に）
- Step. 4…追加のタブレットPCを導入（常時一人一台タブレットPCが利用可能に）

・ シナリオサンプル ㉒ <コンピュータ教室タブレット化型>

- Step. 1…コンピュータ教室の設備更新にあわせてコンピュータ教室にタブレットPCを導入
- Step. 2…可搬型無線LAN設備を導入（普通教室で使用する際は可搬型無線LAN設備をその都度移動）
- Step. 3…普通教室に無線LANを整備（コンピュータ教室タブレットPCを常時普通教室でも使用可能に）
- Step. 4…追加のタブレットPCを導入（常時一人一台タブレットPCが利用可能に）

・ シナリオサンプル ㉓ <トライアルキャッチアップ型>

- Step. 1…トライアル校で複数人共有のタブレットPCを導入
- Step. 2…地域全校で複数人共有のタブレットPCを導入
- Step. 3…トライアル校で一人一台用のタブレットPCを導入
- Step. 4…地域全校で一人一台用のタブレットPCを導入

・ シナリオサンプル ㉔ <トライアル先行型>

- Step. 1…トライアル校で複数人共有のタブレットPCを導入
- Step. 2…トライアル校で一人一台用のタブレットPCを導入
- Step. 3…地域全校で複数人共有のタブレットPCを導入
- Step. 4…地域全校で一人一台用のタブレットPCを導入

・ シナリオサンプル ㉕ <全校導入型>

- Step. 1…地域全校で複数人共有のタブレットPCを導入
- Step. 2…地域全校で一人一台用のタブレットPCを導入

7.3.2. ネットワークへの影響と構築上の留意点

(1) 校内LANの構築および再構築の検討

端末最数の拡大が想定される場合は、校内LAN(有線)は最低でも100Mbps以上、可能であれば1Gbpsで整備する必要がある。

(2) イン트라ネット、インターネットへの出口の再構築の検討

外部の動画等の利用が想定される場合は、イントラネット、インターネットへの出口回線は、最低でも100Mbps以上、可能であれば1Gbpsで整備する必要がある。

(3) 無線LANアクセスポイントの仕様の検討

- ・ 一人一台の導入がシナリオにある場合は、各教室へのアクセスポイント常設が必要
- ・ グループ1台の場合にも、将来常設の可能性のある倍には、常設に耐えられる仕様のアクセスポイントの選択が必要
- ・ 導入するアクセスポイントは基本的な機能に加え、複数アクセスポイント管理・チャンネル管理・チャンネル制御・OSのアップグレード・送信出力管理・不正なアクセスポイント検知・不正なクライアント検知・クライアントのチャンネル帯域制御・冗長性・干渉源の特定・ローミングなどの機能の検討が必要になる

7.4. その他の留意事項

7.4.1. 可搬型無線LANについて

トライアルにおいては、可搬型無線LANを利用し、知見を蓄積することは有効だが、可搬型無線LANを都度設置することは、常設無線LANの場合と比較して授業運営に追加の時間を要してしまうこと、システムの安定性が低いことは否めない。

早期の段階(普通教室への展開時)に常設無線LANを導入することを推奨する。
(※政府目標においても2017年度までの整備が掲げられている。)

7.4.2. 防災拠点対応

体育館や校庭等でも無線LAN環境を整備することで、より自由で魅力的な授業を実現することが可能となる。体育館や校庭等では普通教室、コンピュータ教室と異なり空間が広いため、普通教室、コンピュータ教室とは異なった無線LANの設計が必要である。

また、被災時には、無線LAN接続を被災者へ開放できるように予め検討しておく(設定変更パターンや運用ケースを考慮しておく)ことも重要なポイントである。

7.5. 経年保存

学校で取り扱う情報は多岐にわたっており、個人情報を含むデータも多い。保存にあたっては、「2.7 セキュリティ対策」が必要である。

多くの情報、表簿類には、保存年限が法的に定められている。

第二十八条 学校において備えなければならない表簿は、概ね次のとおりとする。

- 一 学校に関係のある法令
- 二 学則、日課表、教科用図書配当表、学校医執務記録簿、学校歯科医執務記録簿、学校薬剤師執務記録簿及び学校日誌
- 三 職員の名簿、履歴書、出勤簿並びに担任学級、担任の教科又は科目及び時間表
- 四 指導要録、その写し及び抄本並びに出席簿及び健康診断に関する表簿
- 五 入学者の選抜及び成績考査に関する表簿
- 六 資産原簿、出納簿及び経費の予算決算についての帳簿並びに図書機械器具、標本、模型等の教具の目録
- 七 往復文書処理簿

2 前項の表簿（第二十四条第二項の抄本又は写しを除く。）は、別に定めるもののほか、五年間保存しなければならない。ただし、指導要録及びその写しのうち入学、卒業等の学籍に関する記録については、その保存期間は、二十年間とする。

学校教育法施行規則には、学校に備えなければならない表簿として以下のように示されている。

上記に記載されているもの以外にも、各自治体(教育委員会)で独自に永年保存、長期保存、30年保存、1年保存等と定められている表簿が多々存在する。参考例を次表に示す。

保存にあたっては、帳票・表簿の形式でPDFのようなファイルを校務用サーバで保存し、プリントアウトしたものを原本として保存するといった方法や、電子署名を埋め込むことで、原本を電子化する方法などがある。

表 7-1 諸表簿等の保存年限（参考例）

区分	表簿等名称	保存年限	区分	表簿等名称	保存年限
総務	学校沿革史	永年	統計調査	学校基本調査	10年
	学校(校務)日誌	永年		学校教員統計調査	5年
	職員会議記録	5年		地方教育費調査	5年
	校務分掌表	1年		例規通達	永年
	行事予定表	1年	保健	保健日誌	5年
	文書受理簿・発送簿	5年		児童生徒健康診断票・歯科検査票	5年
	出勤簿	5年		学校医・学校歯科医・学校薬剤師執務記録簿	5年
	諸届簿(休暇簿等)	5年		日本体育学校健康センター掛金加入同意書・掛金納入書	5年
切手・電話使用簿	1年	会計	学校保健センター災害報告書控 災害給付金通知書・給付金受払簿	5年	
事務引継書	5年		予防接種児童生徒名簿	5年	
教育計画(学校・学年・学級経営案)	5年		職員健康診断書	5年	
教育課程関係(実施届、実施状況報告書等)	5年		市会計関係	5年	
学級編成関係	5年	旅費	就学援助関係	10年	
児童・生徒名簿・入学児童生徒名簿	5年		出張命令簿	5年	
児童・生徒調査著(家庭環境調査書等)	5年		旅行命令依頼簿	5年	
行事記録(入学式・卒業証書授与式・修学旅行・運動会等)	5年		復命書	3年	
指導要録及び写し(学籍)	20年	給食	自家用車公用使用承認申出書	5年	
指導要録及び写し(指導に関する記録)	5年		給食費徴収簿	5年	
指導要録抄本	5年		給食日誌	5年	
出席簿	5年		給食献立表	5年	
転学に関する書類	5年	安全	給食物資受払簿	5年	
日課表・週時程表	5年		給食実施記録簿	5年	
成績関係書類	5年		学校給食検食簿	5年	
学習成績一覧表	5年		安全点検簿・安全関係書類	1年	
進路指導に関する書類	5年	給与	給与支給明細書	5年	
知能検査・学力検査	5年		教員特殊業務手当	5年	
担任学級・担任の教科または科目及び時間表	5年		諸手当認定簿	5年	
図書台帳	永年		時間外勤務命令簿	5年	
児童生徒賞罰録	永年	福利	給与台帳	5年	
諸証明書交付台帳	5年		児童手当認定簿	5年	
学割証発行台帳	5年	公務災害	公務災害関係書類	永年	
安全指導に関する書類	5年				
教育実習関係	1年				
教科用図書関係	5年				
副読本等教材使用関係	5年				
理科薬品管理簿	5年				

指導要録の電子データでの保存に関しては、文部科学省より現行制度上でも問題ないことが示されている。
文部科学省のURL http://www.mext.go.jp/b_menu/shingi/chukyo/chukyo3/043/siryu/attach/1285299.htm

参考事例

東京都豊島区では、区として文書の電子化を行っており、教育委員会・学校も同様で、完全電子化を進めている。統合型校務支援システムを導入し、指導要録、健康診断票も電子化している。原本の電子化にあたっては、豊島区の認証局が発行した電子署名を埋め込むことで対応している。児童・生徒が区内で転校(異動)する場合は、電子データが転校先の学校に送られ、区外に転校(異動)する場合は、プリントアウトし、原本に相違ないことを示した鑑文を付けて転校先の学校に送付している。

○原本性保障

表簿類の保存にあたっては、複製防止や改ざん防止の手段を講じ、原本性保障を行なう必要がある。
原本性を脅かす脅威としては以下のようなことが考えられる。

1. 故意による改ざん(過失を含む)

故意により電子文書の書き換え、消去、削除等が行なわれること。また、過失、誤操作等により、結果

的に電子文書の一部もしくは全部が削除されること。

2. コンピュータウイルスによる破壊・消去
コンピュータウイルスがシステムに侵入し、保存されている電子文書を消去したり、システム自体を破壊すること。
3. 原本と抄本・謄本が混在することによる唯一性の欠如
電子文書の特長として、同一の複製が容易に作成できるため、同じ文書が複数存在することとなった場合に、それらが混同されてしまうこと。原本と謄本・抄本が明確に区別されていない状況も同様。
4. システム障害による内容の消失
予期せぬ災害や停電、システムダウン等により、電子文書が消失・変化すること。また、システム機器が故障したり、破壊されるなどして電子文書が利用できなくなること。
5. 記録媒体の経年劣化
長期間保存することで、ディスク等が劣化すること。
6. 管理の責任やその権限の管理や権限の不明確
電子文書の管理や保存を行なう責任や権限を明確にせず、電子文書の信頼性が保たれなくなること。

上記のような脅威を払拭するには、文書管理の運用規定を明確に定め、IDとパスワードを利用した識別認証だけでなく、もう一種類のなんらかの方式を加えて二要素認証とし、バックアップシステムを導入(可能であれば遠隔地にてバックアップ)する等の対策が必要である。

○保存年限終了後の対応

表簿に定められたそれぞれの保存年限が過ぎたものに関しては、適宜、削除(廃棄)を行なわなければならない。削除(廃棄)にあたっては各自治体の基準に従って作業を行う必要がある。尚、謄本・抄本・写しも同時に削除が必要となるので、留意が必要である。しかしながら、校務関連のデータに関しては、廃棄・削除に関して明確な指針が公的な機関から示されていない。今後、表簿類の電子保存がますます広がるので、早急な対応が望まれる。

8. 教育ネットワーク導入事例・活用事例

ネットワークの導入の事例はこれまでも多く紹介されている。ここでは、特徴的なセルラーモデルの導入事例を紹介し、合せて、ネットワークの活用事例を紹介する。

8.1. 古河市事例(セルラーモデル)

古河市では、全システムのクラウド化、および全タブレット端末のLTE(4G)化により、「LTEとクラウドで実現するスマート教育ICT」を実現した。

下記の図の通り、iPadセルラーモデル約1,500台を小学校23校に配布し、授業への利活用を進めることができた。

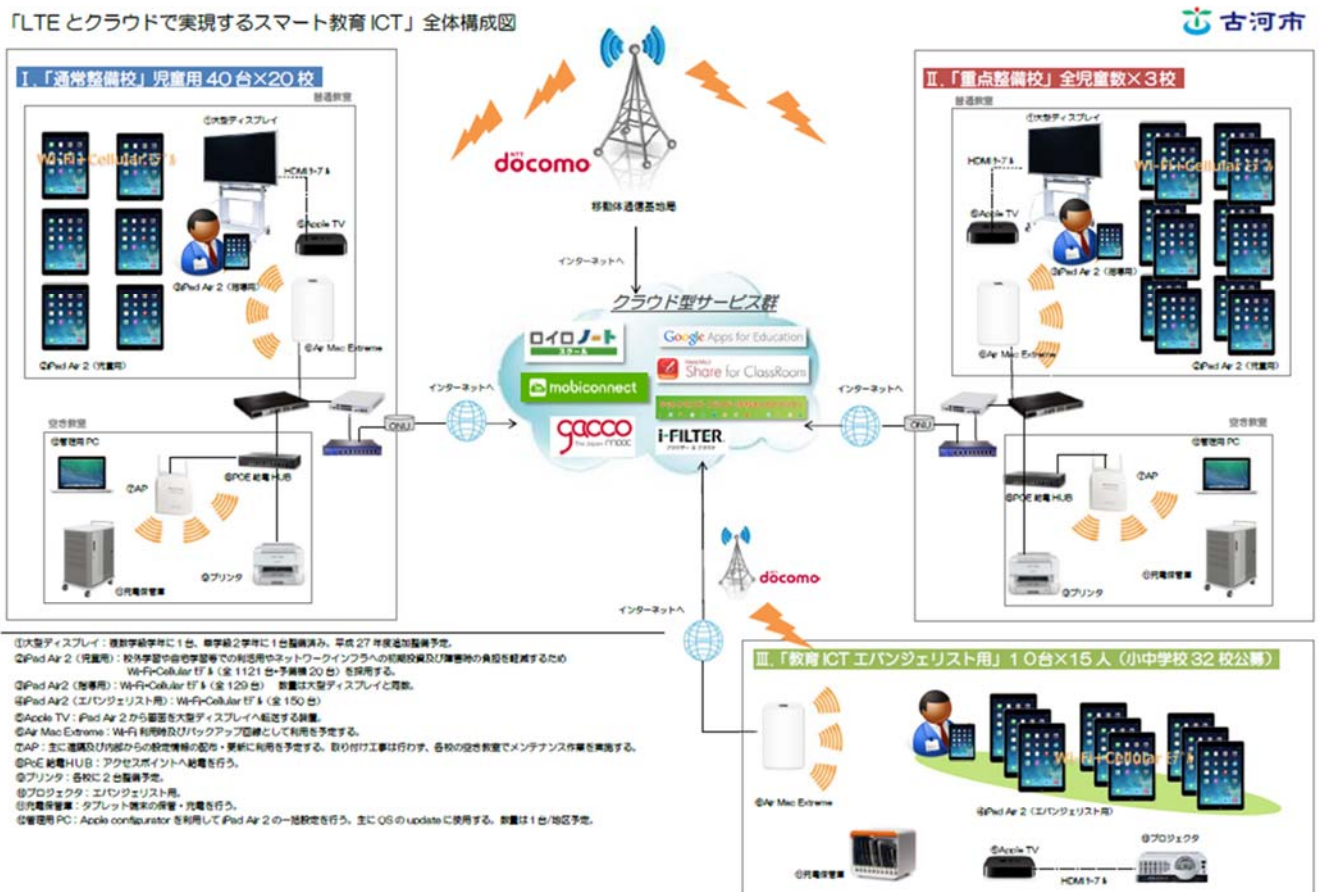


図 8-1 LETとクラウドで実現するスマート教育ICT全体構成図

8.1.1. セルラーモデル導入メリット

セルラーモデルタブレット端末を導入することにより、Wi-Fi環境の有無にとらわれることなく、いつでもどこでもタブレット端末を活用した教育ICT環境を提供することが可能となった。

セルラーモデルタブレット端末は、一般消費者と同様の通信環境を利用するため、通信品質の信頼性が高く、安定した運用が可能であり、授業においては、校外学習や体育館、グラウンド等Wi-Fiの導入が難しい環境での学習では真価を発揮し、いつでもどこでも学びの場となるため、指導する先生の創造力を縛ることなく、授業を展開することが可能となった。例えば、野外での観察で、見つけた生き物、建物のリアルタイム検索に活用し、校外での観察記録を、すぐにクラウドで共有することが可能となる。

併せて、緊急避難所となる学校施設に、常時LTE回線を利用可能なタブレット端末を用意することができ、災害時等、非常時の情報収集や情報発信、テザリング機能を用いた一時的な公衆無線LANの提供等が可能となる。

8.1.2. セルラーモデル導入の注意点

一般的にセルラーモデルタブレット端末は、端末毎に通信容量制限があり、サイズの大きいファイルのやり取りや、アプリケーションインストール/アップデート等のデータダウンロードを実施する際は、機器の仕様等により、LTE回線でまかなうことができない場合がある。併せて、数十台～数百台規模での一斉同時アクセスを想定していないため、最寄りの通信基地局設備がトラフィックに耐えうるかどうかは、キャリア事業者への確認や検証が必要となる。場合によっては、基地局やアンテナ増設を検討する必要もある。

8.1.3. 苦労した点

MDMを利用してiPad展開を行ったが、アプリケーションの展開が出来ず、導入するアプリケーションを都度設定する必要があり、非常に時間がかかった。また、iOSアップデートのためにWi-Fi環境を利用する必要があったが、必要最低限のインターネット回線しか準備していなかったため、アップデートに非常に時間がかかった。

8.1.4. 導入時の検討事項

契約によって、導入端末数が増えると、セルラーモデルタブレット端末よりもWi-Fiモデルの方がコストメリットを出せる場合がある。よって、導入検討時には、セルラーモデルのみではなく、Wi-Fiモデルについても、検討が必要となる。

また、完全にLTE回線のみでの運用は現状では難しいため、有線もしくはWi-Fi環境もメンテナンス時に利用することを想定し、運用に耐えうるインターネット回線を各学校に準備することをお勧めする。

8.1.5. 今後の課題

今後は、多様なクラウドサービスを利用することとなるため、共通認証基盤の整備が必要不可欠となるため、利用するクラウドサービスを共通ポリシーでアカウント構成する等、可能な限り管理者に負担がかからない運用を検討していく必要がある。

また、セルラーモデルタブレット端末は、小規模導入においてメリットを出せると考えられるが、まだ導入事例も少なく、運用も始まったばかりである。よって、技術面や運用面において、現段階では整理しきれていない部分もあると考えられる。

9. 付録

9.1. 用語集

用語	読み等	意味
校務情報化	こうむじょうほうか	従来紙で行ってきた学校業務を電子化する事。本書では特に児童生徒の教育にかかわる部分を指す。
教育ICT環境	きょういICTかんきょう	教育ICT化を実現するためのシステム環境。ネットワークやサーバ、セキュリティ、端末などを含む。
クラウド	くらうど [Cloud Computing]	おもにインターネット上にある資源(データやアプリケーション)からサービスを受ける形態
教育ネットワーク		ICT環境の中で、機器間を接続するLAN、WAN、インターネット接続等の事
セキュリティ	せきゅりてい [Information Security]	保安。 可用性(必要なとき使える)、機密性(アクセス権の有無確認など)、完全性(改ざんされないなど)、の3点を維持する事を目的とする。特に外部侵入、データ漏えいなどによる被害からシステムを守る。サーバ室の施錠などの物理セキュリティも含まれる。
可動式コンピュータ	かどうしきこんぴゅーた	ノートPC、タブレットPC、スレートPCのような持ち運びを想定した端末
アプリケーション		利用者にある目的の情報処理を提供するソフトウェア
コンテンツ		本書の中では、アプリケーションが利用するデジタルデータを指す(画像データや帳票データ)
キャッシュ		データが流れる途中でデータを保存する仕組み。本書ではネットワークの途中に配置してデータ転送の効率化を図る装置を指す
コンピュータ教室		一般的にPC教室、コンピュータ室といわれるPC学習を行う特別室
無線LAN		通信メディアとして無線を利用して構築した近接ネットワーク。IEEE802.11で規定される
タブレット端末		可動式コンピュータのうち板状の端末全般こと。スレート端末ともいう。IOS(iPad)、Android、Windows RTなどのOSを使ったものが主流。
校務支援システム		教職員のメール、掲示板などのグループウェアや、児童・生徒の成績管理など校務にかかわるアプリケーション。製品により含まれる機能はことなる。
授業支援アプリケーション		ICTを利用した授業で利用するアプリケーション。ドリ

		ル学習、画像視聴、端末間情報共有など、多岐にわたる
データセンタ		通信機器やデータを集約して管理するために作られた施設。無停電電源、耐震性、通信経路、物理セキュリティなどによりレベル分けされている。
ポリシー		方針、基本規定の事
認証		対象の正当性を確認する事。本書の中では特記しない限り利用者の本人認証を指す。ユーザ名パスワードが一般的だが、生体認証(指紋、網膜、顔)や、ID(カード等)も増えている。
認可		認証が本人確認であるのに対し、データ等のリソースへのアクセス権限の管理は認可で行う。年度末の担当変更時など認証は変更ないが、認可設定を変えることになる。
インターネット		IP技術を使ったネットワークの集合体。ウェブやメールなどインターネット上のアプリケーションを指すこともある。
イントラネットワーク		IP技術を使い特定の団体内で構築されたネットワーク。インターネットとの区別として使われる
スループット		データ転送速度など単位時間当たりの処理速度。帯域のように経路の処理速度や、端末が転送処理できるデータ量など場合により意味合いが異なることがある。
帯域		その通信経路が単位時間に転送できるデータ量。ネットワークでは、bps(bit per sec : 1秒当たり転送bit数)が使われる
ネットワーク		本書の場合、通信機器により構築された通信網を指す。学校内などの狭域で構築されているものをLAN、拠点間を接続するものをWANとしている
サーバ		何らかのサービスを提供しているコンピュータ
ルータ		ネットワークで、経路決定している機器
スイッチ		ハードウェア処理によりデータ転送している機器。ルータ機能を持つか持たないかで、L3スイッチ、L2スイッチなどがある
無線AP	むせんえーぴー	有線LANに接続するための無線接続機器。複数の端末が同時にアクセスすることが多いためアクセスポイントと呼ばれる
VPN	ぶいぴーえぬ [Virtual Private Network]	複数の利用者が利用する公衆ネットワーク上で、暗号化技術により仮想的に専用線的ネットワークを構築する技術。ただし、インターネット上の場合には帯

		域保証されないため、接続の保証はない。
FW	ふあいあうおーる [Fire Wall]	防火壁。他のネットワークとの境界で、侵入などを食い止めるための装置。製品により防御機能が異なるため機能の確認が必要
IPS	あいぴーえす [Intrusion Prevention System]	侵入防止装置。FWと同じようにネットワーク境界に置き侵入に特化して検知と対策を行う装置。
WAF	わふ [Web Application Firewall]	通常のFWが通信プロトコル中心の防御なのに対し、WEBサーバアプリケーションやサービスを狙った攻撃に対するFW。WEBサーバがインターネットに公開されていることから攻撃対象になりやすいため特化した製品となっている。
Wi-Fi	わいふあい	Wi-Fi Allianceという団体が、無線LAN製品の相互接続性を確認し認定を行った製品に付けられるマーク。無線LAN規格はIEEE802.11で規定されているが、メーカー間の接続性保証のためつけられる。