

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9月

第1.0版

目次

はじめに	1
本書について	1
本書における記載内容の前提条件	2
本書の使い方	5
1. 教育ネットワークの全体像	6
1.1. 教育ネットワークを支える情報基盤施設	7
1.2. 学校内ネットワーク(校内LAN)	7
1.2.1. 授業支援系ネットワーク	7
1.2.2. 校務支援系ネットワーク	11
1.3. データセンタ	13
1.3.1. データセンタの選択基準	14
1.4. アプリケーション・コンテンツ・データの格納先	14
1.4.1. データ保全のためのバックアップ	16
1.4.2. 機密保持のための特権ID管理	16
1.5. ネットワークの分離	17
2. 教育ネットワークの設計	19
2.1. 教育ネットワーク設計の要件	20
2.1.1. 利用時に遅延を生じない高速性	20
2.1.2. 利用したい時に利用できる安定性	21
2.1.3. 安心して使えるセキュリティ上の安全性	21
2.1.4. 通信に要求される通信帯域の算出	22
2.1.5. トラフィックが集中するデータセンタ出入り口の帯域	24
2.1.6. 学校内ネットワークのイメージ	24
2.1.7. 無線LAN	25
2.1.8. 有線LAN	31
2.1.9. WAN(自治体WAN、キャリア回線、インターネットVPN)	33
2.1.10. セキュリティ対策	34
3. 教育ネットワークの運用検討	42
3.1. 教育ネットワークの運用要件	42
3.1.1. ネットワークの品質確保	42
3.1.2. ヘルプデスク	45
3.1.3. オンサイト保守	45
3.1.4. SLA(サービスレベル契約)	46
3.2. 教育利用の特有シーンにおける運用要件	48
3.2.1. 環境準備	48
3.2.2. 一斉授業	49

3.2.3.	個別学習.....	49
3.2.4.	校務支援システムの利用.....	49
3.3.	教育委員会・学校における運用要件.....	50
3.3.1.	教育委員会・学校.....	50
3.3.2.	システム状況の外部公開への対応.....	51
3.3.3.	教育利用者特有の運用要件.....	51
3.4.	外部組織への業務委託.....	51
3.4.1.	運用方法の明確化.....	51
3.4.2.	システム委託事業者のアカウント管理.....	51
3.5.	ICT支援員.....	52
3.5.1.	ICT支援員の必要性.....	52
3.5.2.	ICT支援員の業務内容.....	52
3.5.3.	ICT支援員に求められる資質.....	53
3.6.	PTAのネットワーク利用.....	54
4.	学校内ネットワークの敷設.....	55
4.1.	無線LAN.....	55
4.1.1.	設置場所.....	55
4.1.2.	干渉源、遮蔽物による影響.....	55
4.1.3.	アンテナ.....	55
4.1.4.	アクセスポイントの堅牢性.....	56
4.2.	有線LAN.....	56
4.2.1.	ルート調査.....	56
4.2.2.	ルート設計と配線工事.....	56
参考	経年保存について.....	59
参考	無線ネットワークの技術的な仕様/機能の詳細解説.....	62
付録	用語集.....	66

はじめに

近年は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、教科指導におけるICTの利活用に取り組む自治体が増えている。同時に、学習記録データの利活用や校務データとの連携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な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。

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ではできなかった新たな利活用シーンの実現やそれを可能とする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に接続され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動画を視聴するなどの新たな利活用シーンは、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の利活用が進むにつれて、セキュリティ上の脅威となる事象への対策手段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。

本書について

本書は、これから教育ネットワークを整備・運用する、および整備・運用している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。

また、本書を記載するにあたっては、以下の情報を参考としている。特に本書に記載していない調達プロセスなどは参

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://johouka.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」

照されることをお勧めしたい。

- ・総務省 教育ICTの新しいスタイル クラウド導入ガイドブック2016

http://www.soumu.go.jp/main_content/000417631.pdf

- ・総務省 教育分野におけるクラウドを中心とした ICT環境構築のための調達ガイドブック

http://www.soumu.go.jp/main_content/000417632.pdf

- ・総務省 教育分野におけるクラウドを導入に対応する 情報セキュリティに関する手続きガイドブック

http://www.soumu.go.jp/main_content/000417633.pdf

- ・一般社団法人 日本教育情報化振興会 (JAPET&CEC) 学校の無線LAN導入・運用の手引きVer. 1.00

<http://www.japet.or.jp/jowlt6rz5-919/>

本書における記載内容の前提条件

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

<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。

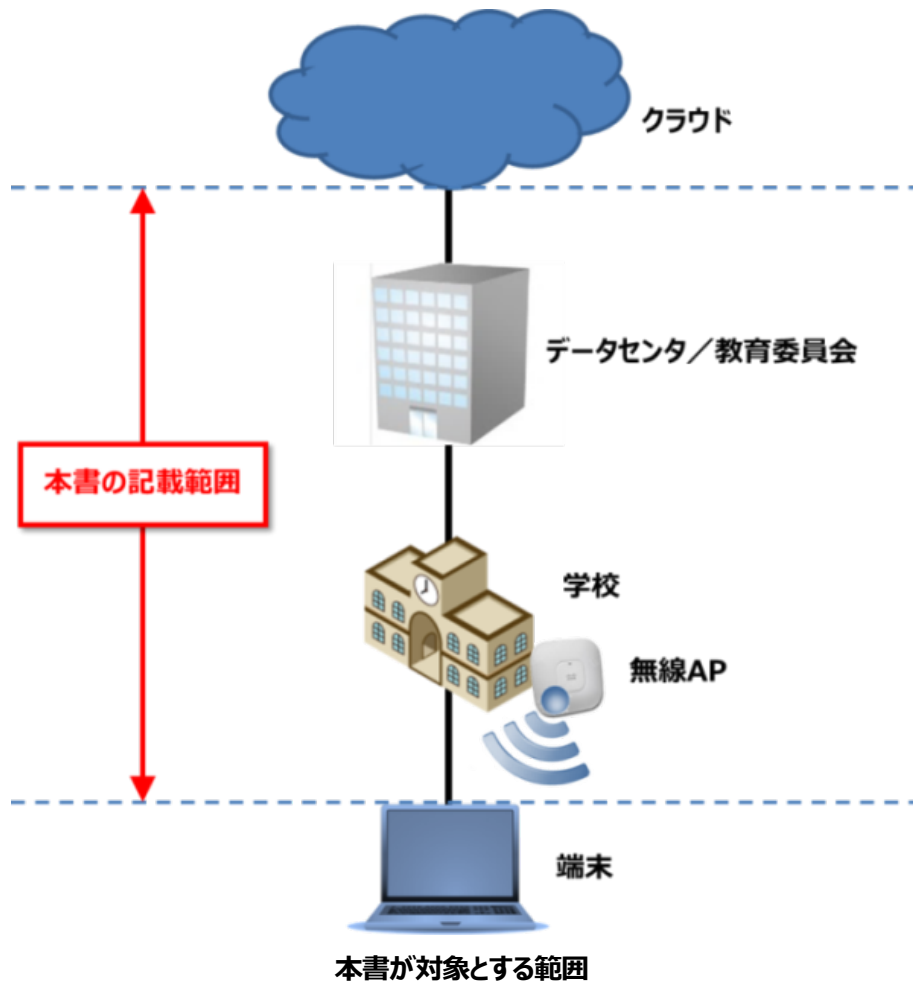
<対象範囲>

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。

- ・ ネットワーク範囲

端末～クラウド／インターネット間を対象範囲としている。

(端末そのもの、およびクラウド／インターネットそのものについては必要最小限の記載にとどめている)



・ 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。

<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(1頁注参照)を、以下と解釈。

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

端末数 …………… 約100台

同時接続数 …… 約100台

<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。

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	●	●
ファイアウォール 侵入防止装置	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 アクセスポイント	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	●	●

本書の使い方

本書では、主に、教育ネットワークとは何かを中心に1章で、教育ネットワークの設計に関する内容を2章、3章で、敷設に関する留意事項を4章で記載しており、教育ネットワークを整備する順を追った章立になっている。

本書の章立

章		概要
はじめに		本書の読者対象、位置付け、本書の記載する教育ネットワークの範囲や前提を記している。
1章	教育ネットワークの全体像	教育ネットワークとは何か、学校、データセンタ、クラウドという各要素を接続するネットワーク、また、実際に教育現場で必要となる利用シーンに基づいたネットワークの種類やネットワーク分類の仕方について紹介し、教育ネットワークの全体像を把握できるようにしている。
2章	教育ネットワークの設計	教育ネットワークの整備において、極めて重要となる“学校”にフォーカスをあて、学校内ネットワーク、学校の外部であるWANなどネットワーク設計に必要な要件・要点をまとめている。特に、最も課題意識の高い無線LANは詳しく記載している。
3章	教育ネットワークの運用検討	教育ネットワークを利用・運用する上で必要となる要件・要点をまとめている。クラウド利用におけるサービスレベル契約（SLA）やヘルプデスク・オンサイト保守などネットワーク整備のみでなく教育ICT整備でも含まれる内容も記載している。また、各授業シーンでの利用の工夫や教育委員会・学校で整備すべきルールや管理すべき事項も記載している。
4章	学校内ネットワークの敷設	学校内ネットワークを実際に整備する上で必要となる敷設・工事において、注意すべき点、学校環境特有の敷設上留意すべき内容を記載している。
参考		教育現場で使われている表簿類の経年保存、無線LAN技術の仕様・機能の詳細を記載。 データ保存の考え方や、無線LANの特性や機能を技術的に紹介し、把握の一助として必要に応じて参照いただきたい。
付録		用語集。 教育ネットワークや教育ICT整備において必要となる専門用語を中心に載せている。本書や他の教育ICT関連の資料を読む上で活用いただきたい。

1. 教育ネットワークの全体像

自治体によって名称や分け方が異なるケースもあるが、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る。これらは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、必要とされる通信量などの通信特性が異なることから用途別に別けて構成すること一般的である。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。

限られた予算を有効に活用しながら環境整備を進めるために、教育ネットワークも中期的な整備計画の一部としてあらかじめ位置づけておく必要がある。

表 1-1 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（従来の有線 LAN に加え無線 LAN の利用が重要） 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（ネットワーク帯域や一時保存機能（キャッシュ）利用の検討が必要） 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り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校内 LAN 経由で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」と呼ぶ。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、安心・安全な教育ネットワーク実現に向けて以下の点が重要なポイントとなる。

- 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」

1.1. 教育ネットワークを支える情報基盤施設

授業支援系／校務支援系ネットワークを支える情報基盤施設(インフラストラクチャ:以下インフラ)は下記の4つのケースが考えられる。情報システム部門や情報セキュリティ部門と連携し、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それぞれの自治体事情に見合ったインフラを選択する。

表 1-2 授業支援系／校務支援系ネットワークを支えるインフラ

項番	ネットワークインフラ	備考
①	教育ネットワーク専用のインフラを利用	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ネットワーク ² をインフラとして利用	高等学校で利用するネットワーク等に見られる例
④	独自インフラを構成せず、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。

1.2. 学校内ネットワーク（校内LAN）

学校内ネットワーク(以降、校内LANと呼ぶ)は、安心安全な教育ネットワーク利用を支える重要な構成要素の一つである。特に教室内でのタブレット端末などの利用を可能とする無線LANは、場合によっては授業の進行を直接左右するほど重要なポイントとなる。無線LANは、他にも教室WiFiや無線AP(アクセスポイント)などと表現されることもあるが、この無線LANと同義で使われることが多い。

無線LANは環境整備時に適切なハードウェア配置や利用のための設定が必要なことはもちろん、整備後も定期的な利用環境チェックや必要に応じた設定変更など、運用にも十分な配慮を施すことが安定した授業進行への近道といえる。このため、将来的に目指す利活用シーン、接続を予定する端末数の推移、機器の更改サイクルなどを勘案した中期的な整備運用計画を策定した上で整備仕様を決定することがポイントとなる。

1.2.1. 授業支援系ネットワーク

本章の冒頭で記載(表 1-1参照)する特徴をもつ授業支援系ネットワークは、学校(拠点)数・共同利用の有無・利活用や集約効果の度合い・必要とするセキュリティ・確保可能な予算規模・運用のための人材配置可否などから、どの様に整備するかを決定する。

これらのことから自治体毎に見合った検討を実施することが基本となるが、大まかには下表の4つの類型に分類することができる。一般的には、学校数が多く運用人材の配置も可能な自治体では「イントラネット型」、学校数が少なく人材配置

² イントラネットワーク:一般に公開されたインターネットに対し、特定の組織内のみでの利用を目的としたネットワークの事

も困難な自治体は「個別接続型」となる場合が多い。

表 1-3 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
	イン트라ネットワーク型 (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自組織設置運用(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) 	
	イン트라ネットワーク型 (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 	
	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 	
	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 1-4 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		
	仮想デスクトップ(VDI : Virtual Desktop Infrastructure)		
	モバイル端末管理(MDM : Mobile Device Management)		
	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		
	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	
	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	
	動画視聴	YouTube, NHK for School等を使用しグループ単位で視聴	
	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	
	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		
	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	
	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	
	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	
	遠隔・協働学習	離れた児童・生徒と個人単位で協働学習	
	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	
ドリル学習	ドリル教材等を児童・生徒それぞれが実施		

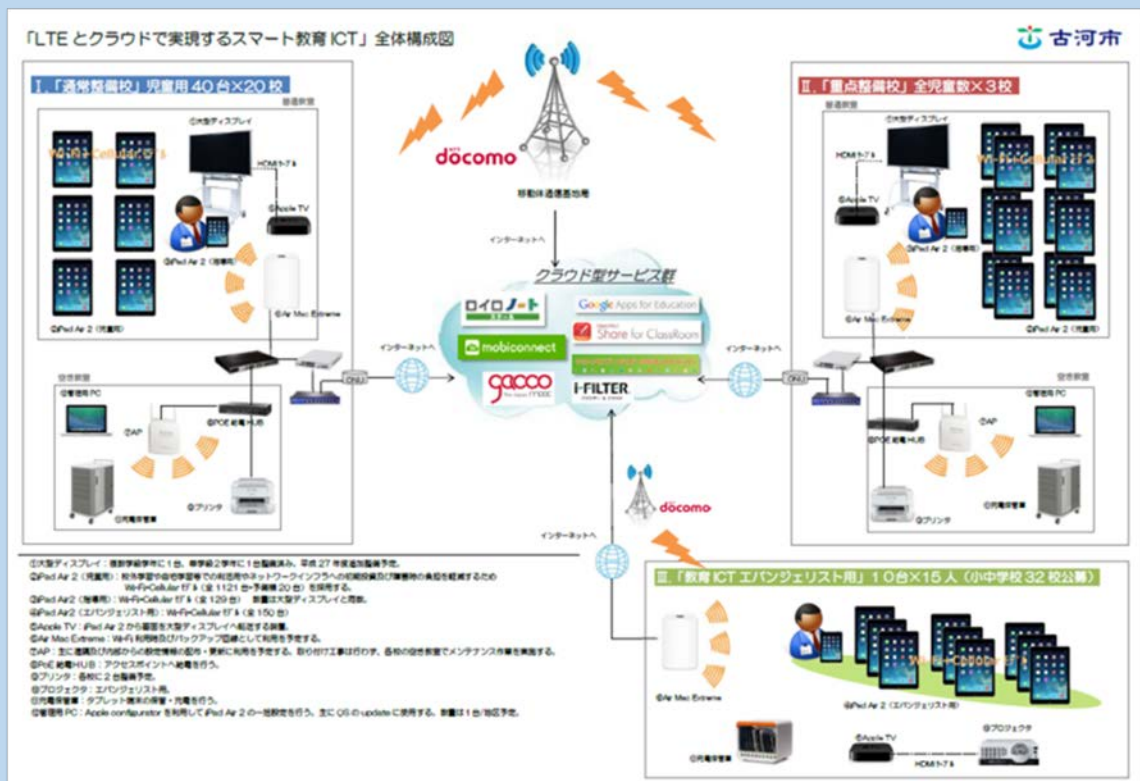
フルクラウド + セルラーモデル

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、校外学習や体育館、グラウンド等無線LAN環境の導入が難しい環境でも教育ICTが利用でき、いつでもどこでも学びの場となる。併せて、緊急避難所となる学校施設に、携帯通信会社のモバイル通信回線（LTE回線）を利用可能なタブレット端末を用意することで、災害時等、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の提供等のメリットがある。

ただ、タブレット端末毎の通信容量制限や数十台～数百台規模での一斉同時アクセスに対して通信基地局設備がトラフィックに耐えうるかどうか等注意が必要である。キャリア事業者への確認や検証の他、対策を検討し、学校内の無線LANの併用利用や運用方法の工夫が必要である。

古河市では、全システムをクラウド化し、全てのタブレット端末からLTE回線により接続して利用できる環境を整備している。

古河市の事例については、総務省「教育ICTの新しいスタイル クラウド導入ガイドブック2016」（http://www.soumu.go.jp/main_content/000417631.pdf）に詳しく記載されているので参照いただきたい。



1.2.2. 校務支援系ネットワーク

校務支援系ネットワークも授業支援系ネットワークと同様に自治体毎に見合った検討を実施するが、それほど高速・広帯域が必要とされない代わりにセキュリティが最も重要な要件となる。自治体毎のセキュリティ基準により「独自センタ設置」が必要な場合とクラウドセンタ利用が可能な場合はまちまちではあるが、クラウドセンタを利用する事例が増えている。

また、災害時の情報基盤整備の必要性の観点からも統合型校務支援システムの整備が推奨されていることから、今後、導入や更改を計画する場合は学校内設置型以外のネットワーク化された類型を検討すべきである。

表 1-5 校務支援系ネットワークの類型パターン

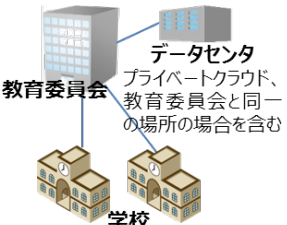
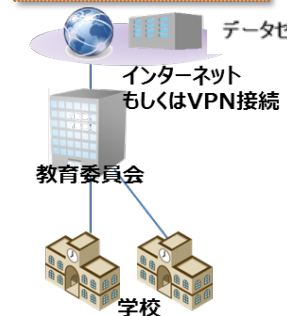
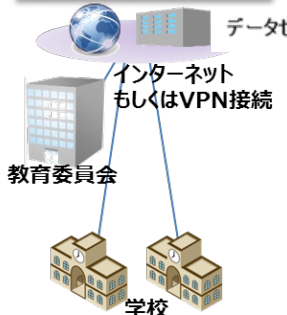

類型パターン	特色	イメージ
1 イントラネットワーク型 (独自センタ設置)	<ul style="list-style-type: none"> ・ 教育イントラに直接接続する独自のデータセンタに校務支援システムをオンプレミス型での整備（資産を所有） ・ インターネット回線への接続が無い、もしくはセンタでの制御を行うため、各校でのセキュリティ対策は不要、かつセキュリティを同一ポリシーでのマネジメントが可能 ・ 集約効果の高い大規模自治体に適している 	<p>教育イントラに直接接続するデータセンタにプライベートクラウドとして整備</p> 
2 イントラネットワーク型 (クラウドセンタ利用)	<ul 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ワーク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 学校内設置型	<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、校内ネットワークのみで利用し、学校間を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 1-6 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	仮想デスクトップ (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るが、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。

1.3. データセンタ

学校や教育委員会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構築することが必要となる。

自治体によって様子は異なるが、個人情報保護の観点より自治体外のロケーションや自庁施設外のセンタ設置が許可されていない場合がある。特に民間のデータセンタを活用する場合は、主管組織と連携し事前に制度上の整理を実施し、利用可能な状態とすることが必要である。

近年では独自センタは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たことから、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 1-7 センタ種別

種別	選択肢	特徴
独自センタ 設置	自前センタ (自治体サーバールーム含む)	<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ンシヤル費用が発生
クラウドセンタ 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 ・インシヤル費用は小さく、利用する期間のみのランニング費用が発生

1.3.1. データセンタの選択基準

サーバ群が設置されるデータセンタは、『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』など万全のデータ保全の仕組みで構築されている必要がある。

データセンタには、そのサービス継続性の指針として、下記のような基準があるため、利用するデータセンタが要求する基準に準じているか確認を行う(もしくは仕様書で指定する)。

- ・ 米国の民間団体 (Uptime Institute) が作成した「Tier」
- ・ 特定非営利活動法人日本データセンタ協会 (JDCC) による「データセンターファシリティスタンダード」

これらの指針を守った、データセンタ構築には、耐震建築物や電源設備等の初期費用と運用費用がかかる。つまり自前でのデータセンタ構築は、教育以外のシステムとの併用や、複数自治体での共用でサーバ数がある程度以上の規模が見込まれる時となる。

また、データセンタは、利用場所と一定の距離を置いた場所に設置されていることが多いことや、一か所にあるデータをバックアップしやすいため、災害発生時もデータ保全について安心して活用できるというメリットもある。

1.4. アプリケーション・コンテンツ・データの格納先

教育ネットワークにおけるアプリケーションやコンテンツ、データの代表的な格納先は、学校に設置されるサーバ(学校サーバ)、センタに格納されるサーバ(センタサーバ)、クラウドサービスとして提供されるサーバ機能(クラウドサーバ)の3ヶ所である。データを、どこに保存するかは、以下のような点を検討対象とする。

- ・ データの種別 (行政データ、個人情報、著作権等) と求められる機密度
- ・ 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密度

格納場所としては、それぞれ下表の特徴がある。

表 1-8 アプリケーション・コンテンツ・データの格納先と運用の特徴

種別	運用者	運用に関して
学校サーバ	各学校に維持管理担当者 教育委員会に主管理担当者	<ul style="list-style-type: none"> 学校サーバの維持管理が学校毎に必要。教職員が実施する場合の負担増や委託する場合の費用増につながっている 各学校に配置する維持管理担当者への、研修実施や手順書等マニュアル類の整備が必要 校内LANの範囲内で利用できるため、帯域が十分でない教育ネットワークの場合には有効 学校毎に設置するサーバのセキュリティ対策が必要
センタサーバ	教育委員会に主管理担当者	<ul style="list-style-type: none"> センタサーバの維持管理の自前実施が必要 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費用が発生
クラウドサーバ	教育委員会に主管理担当者	<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 イニシャル費用は小さく、利用する期間のみのランニング費用が発生

学校サーバと組み合わせる例もある。可能な限り学校以外(センタやクラウド)に格納することが望ましい。情報環境と費用のバランスだけだと、学校サーバはありうるが、業務プロセスの改善(BPR)まで視野に入れると学校サーバは避けたい選択肢である。

学校サーバは職員室やコンピュータ教室に設置されているケースが多いが、維持管理には専門的な知識が必要となることから教員の負担となる。

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。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、機密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。

例として、電子教材自体は機微情報が含まれておらず、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機微情報は、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。

1.4.1. データ保全のためのバックアップ

データの保全を考えると、データセンタの障害やシステム障害等でデータが消失した場合に備えて、定期的なバックアップを行う。バックアップ先には、オンラインストレージ対応と、媒体(DVDやテープ)での保管方法があり、復旧の速さが大きく異なる。費用面は、バックアップする情報量に影響される。

また、オンラインバックアップには、データのためのバックアップとサービス機能を含むバックアップがあるため、障害発生時の復旧希望時間により選択する。

データのためのバックアップとは、サービス復旧に緊急度はないが、消失してはいけないデータ。卒業生のデータや、毎日の業務で使用しないデータなどとなる。

サービス機能を含むバックアップとは、データセンタ喪失を含むシステム障害時でも、即時にサービス復旧を求められるシステムで構築する。毎日の業務で必須となる校務支援データやアプリケーションが対象となる。

また、遠距離のデータセンタをつなぐバックアップには広帯域が求められるため、一定期間でのフルバックアップと間を埋める短期的な差分バックアップを組み合わせ、データの最終変更時と復元データの差分をなるべく小さくする。

1.4.2. 機密保持のための特権ID管理

データセンタで保存されるデータについては、機密度を考慮の上、利用者グループごとの権限設定が必須となる。児童・生徒の端末から教職員やシステム管理者のデータが見えないようにするなどである。また、見落としがちなのは、データセンタ職員や、システム保守運用者から機微情報が閲覧できないようにすることである。

手法としては、いくつか考えられる。

- ・ 保存データの暗号化を行いその復号鍵は保守運用者に知らせない
- ・ システム保守運用者がシステムにログインする場合のID管理は、委託元の教育委員会で行い、誰がいつシステムにアクセスしたか証跡を管理する

1.5. ネットワークの分離

授業支援系ネットワークと、校務支援系ネットワークは、それぞれの利用用途を要因とする通信特性の違い(特に校務支援システムで利用される情報の秘匿性)を考慮し、それぞれ専用のネットワークに分離して扱うことが必要である。ただし、設置する機器や配線を二重に整備するのは費用を大幅に押し上げる可能性があることから、仮想化技術に対応した機器を用いてネットワークを論理的に分離することが現実的である。

(詳細については2.1.10セキュリティ対策を参照)

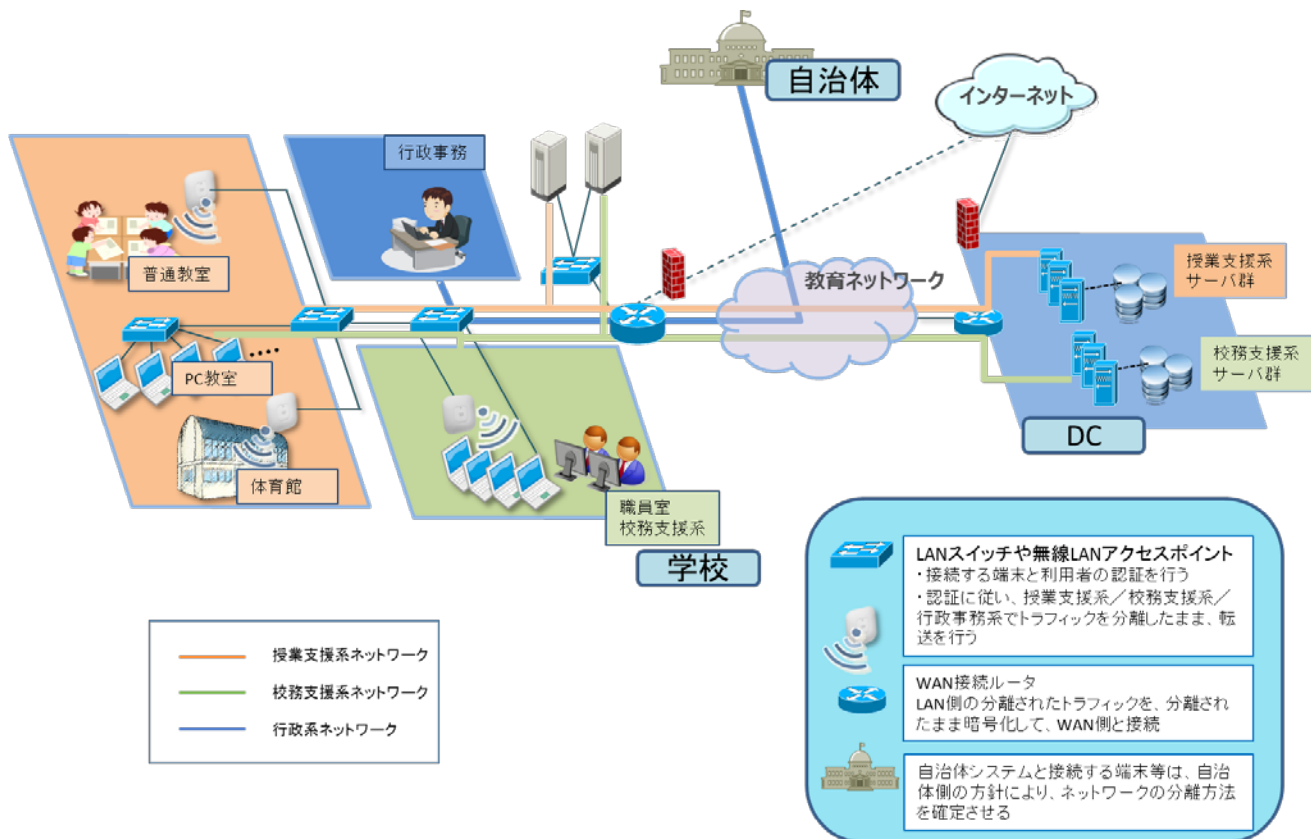


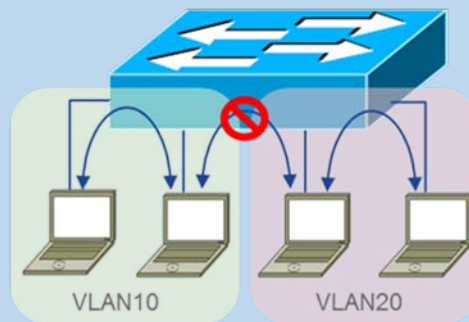
図 1-1 授業支援系ネットワークと校務支援系ネットワークの分離イメージ

VLANとVRF

授業支援系ネットワーク・校務支援系ネットワークを分離するために、以下の技術が利用される。

VLAN

一般的に、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を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。

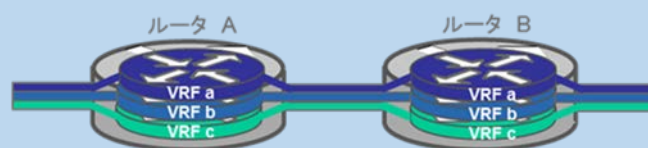


VLANによる論理分離

VRF

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。



VRFによる論理分離

2. 教育ネットワークの設計

本書で目指すのは、教育現場での「快適なネットワークの構築」であり、その時、重視されるのは、「利用時に遅延を生じない高速性」、「利用したい時に利用できる安定性」、「安心して使えるセキュリティ上の安全性」となる。

現在、インターネット技術を利用したネットワークは、一般家庭から、通信事業者のサービスまで、さまざまな組織に敷設され利用されている。もし、費用面を全く考慮しないのであれば、通信事業者が利用する通信機器やセキュリティ装置、広帯域回線を利用したネットワークを敷設することで快適なネットワークを構築することも可能ではある。もちろん、現実的な解決策ではない。

教育ネットワークの設計では、初期費用と運用費用を考慮しながら、実用に耐えうる快適なネットワークを設計するということであり、その時に通信のボトルネックを、できる限り排除し、設計することになる。

教育ネットワークの敷設にかかわる基本的な費用としては以下のようなものが想定されるが、本章では、構成設計にかかわる部分を中心に記述している。

表 2-1 想定される経費等

初期費用	構成設計費	当該教育委員会で必要とされる要件をもとにネットワーク全体の設計を行うため、要件が明確になっていないと冗長な構成で設計することになるため、他の費用にも影響する。
	機器部材費	利用帯域や端末数、要求される機能により価格は大きく変動する。
	設定費	使用する機材のメーカーが多い時や、使用する機能が複雑になると管理が煩雑になり設定費用も上昇する。
	工事費	工事する学校などの敷地面積や配管のしやすさ、経路の複雑さが影響する。
	設置費用	工事費と合算となることが多い。既存の設置場所の有無、電源の確保、校舎の構造などが影響するため、事前の現地調査は必須となる
運用費用	運用管理	ネットワークの状態監視などを委託した場合の費用。通信について本業ではない教職員が運用を行うのは、安定性に懸念がある。
	機器保守	1か所に集約された多数の機材の監視と各校に少数ずつ分散配置された機材の保守では、後者の方が移動効率も悪く費用も掛かる。本書では可能な限りデータセンタなどに機材を集約することを推奨する。
	回線等	必要に応じた回線での契約をするため、使用するアプリケーションの利用帯域を想定しておく。ここでも、要件が明確でないと費用を上昇させることになる。
	ライセンス月額利用	ネットワークにかかわる機器やソフトウェアは、買い取りの場合と、月額のライセンス払いのものがある。利用年数により、初期費用と運用費用の計算を行う必要がある。
	人件費	各種の運用関係を外部委託した場合と、職員が実施した場合の人件費の比較を行っておく。 教職員が運用を行う場合は、その教育費も計算する。

2.1. 教育ネットワーク設計の要件

教育ネットワークの設計に先立ち、教育ネットワークで何をするのかを明確にしておきたい。どのような教材を使い、どのような授業を行うのか、教職員が利用するシステムには何があるのか、動画は見るのか、屋外や自宅学習での利用、インターネットの利用などとなる。

利用目的が明確になったところで、2章の冒頭で記述した「利用時に遅延を生じない高速性」、「利用したい時に利用できる安定性」、「安心して使えるセキュリティ上の安全性」を設計する。その時、ラフでもよいので、想定している教育ネットワークの全体図を記述することで、各要件の整理に役立つ。

通信が集中してボトルネックになりそうな個所、障害が発生した時に影響の大きい機器や回線、外部アクセスやセキュリティ上、弱点になりそうなところの把握などである。

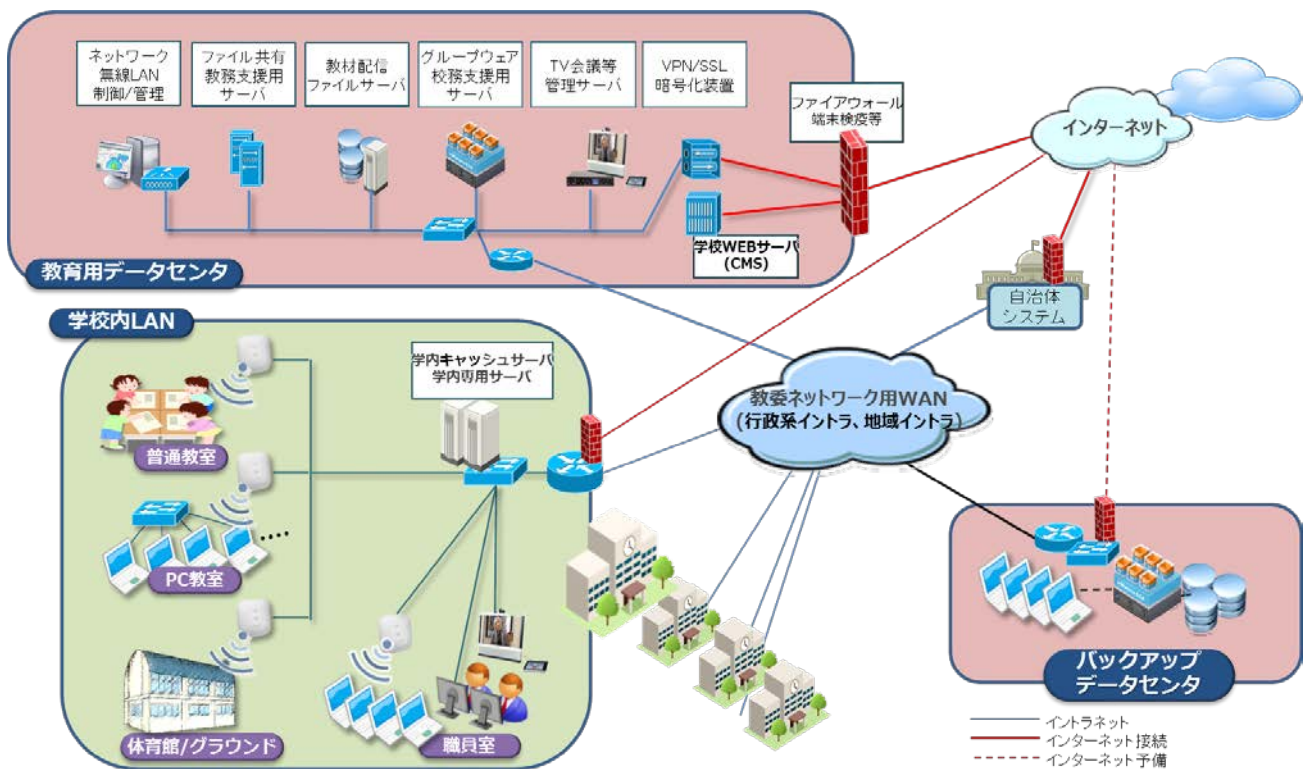


図 2-1 教育ネットワークの全体イメージ例

2.1.1. 利用時に遅延を生じない高速性

準備するネットワークを快適に利用し、ボトルネックが生じないためには、流れるデータの量とデータの場所に応じた設計が必要となる。特に学校において注意すべき点は、児童・生徒の人数である。学校という環境の特異点は、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ことであり、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

これらの要件と、データの流れをあらかじめ想定したうえで、ネットワークに求められる帯域の要件を確定し、ネットワークを構成する以下の要件を確定させる。

校内LANの構成、無線LANの構成、学校内サーバの設置、契約する回線の帯域、校外での利用方法。

2.1.2. 利用したい時に利用できる安定性

回線や配線、1台の機器の故障により教育ネットワークが利用できなくなることは、ICTに対する信頼性を失い、利用率の低下を招くことになる。上記「教育ネットワークの全体イメージ図」では、各機器等の二重化(冗長化)などは行っていないが、貴団体で想定した全体図から、冗長化を行ったほうがよい個所を選定していく。ただし、重要な機器や回線の二重化は、安定化をもたらすが、そのまま費用増となるため、注意が必要になる。

選定のポイントとしては、下記のような箇所があるが、どこまで実施するかは、費用との調整となる。

- ・ 1か所の障害で影響範囲が大きいところ
- ・ 障害復旧に時間がかかってしまうところ
- ・ データ保存機器など障害があると復旧できないところ

冗長化等による安定化は、設計業者にとって教育独自な内容ではないため、有線LAN以外については本書では詳細を省く。

2.1.3. 安心して使えるセキュリティ上の安全性

教育ネットワークで利用されるデータ種類と利用者種別、インターネット接続の有無により、トラフィック分離や端末の接続制限、アンチウイルスなど、セキュリティ要件や機器に求められる機能が異なってくる。特に、教職員が利用する校務支援系に対しては、外部からの侵入、情報の漏えい、データの消去に対して対策が必要となる。

既存の教育ネットワークでセキュリティ上の課題となりそうなポイントをあげておく。

- ・ 教職員と児童生徒の端末間で自由な通信が可能になっている
- ・ 校内の無線LANの暗号化と認証が脆弱
- ・ 校内有線LANに端末を自由に接続できる
- ・ インターネットとの接続点のセキュリティがファイアウォールだけ

ネットワークの全体構成によっては、すべての対策を必要とはしないが、今後の設計で注意が求められる。必要となるセキュリティ技術については、「2.1.10 セキュリティ対策」にて後述する。

高速性、安定性、安全性について、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、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しやすくなる。

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。

2.1.4. 通信に要求される通信帯域の算出

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。

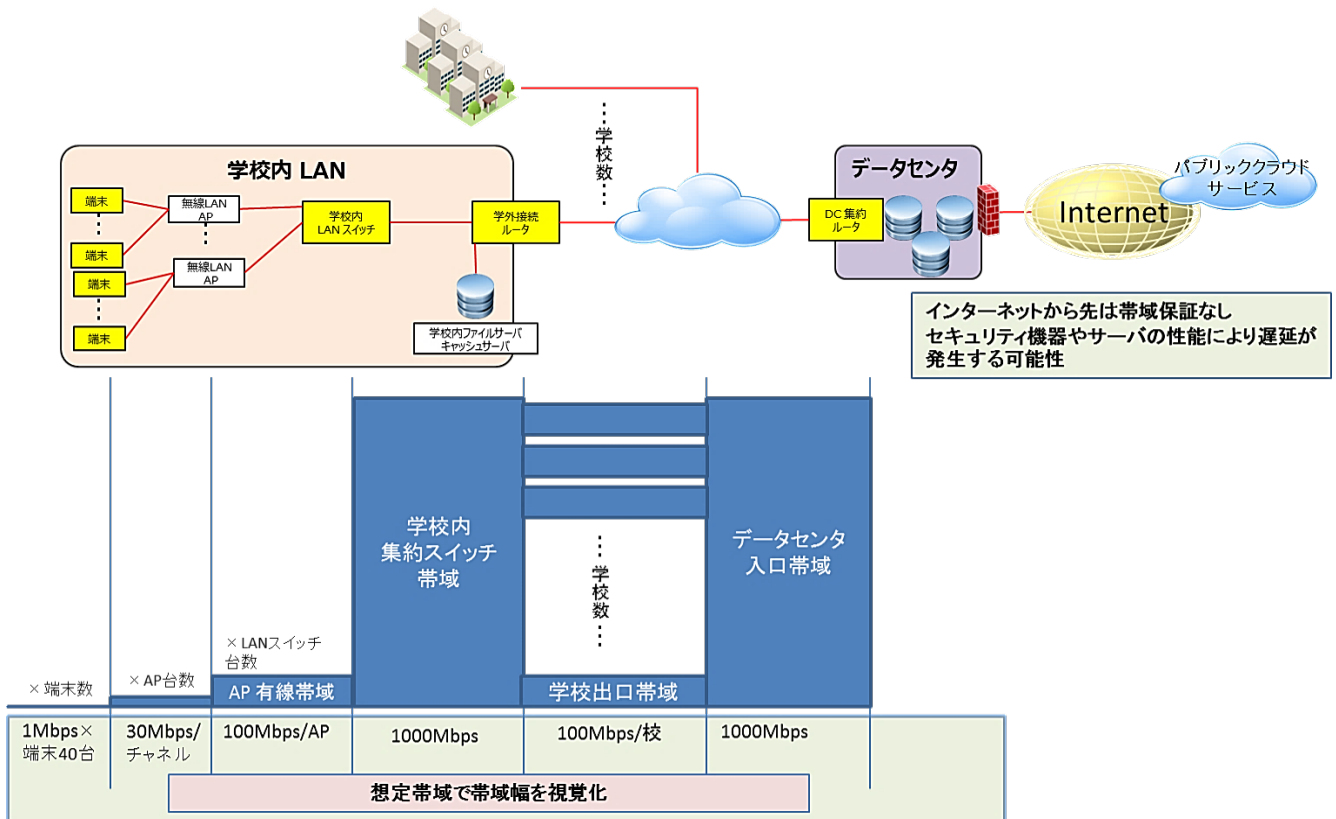


図 2-2 ネットワーク経路の帯域の違い

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収容点の帯域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。

無線LANは、製品により、無線の指向性や同時接続数の機能に違いがあり、単純な計算が実施できないため、通信の実行速度は製造メーカーから事前に情報を集める必要がある。

帯域について、特に、WANの広帯域化は毎月の回線利用料など価格的にも影響度が高いため、十分な設計が費用削減には必須である。

(1) 端末台数と利用する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のままであれば、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。

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

学外接続のWANの広帯域化は、サーバのセンタ化やクラウドの快適な利用には必須となる。ただし、毎月の回線費用増となり運用費用の増加を引き起こす可能性もある。

WANを狭帯域として、各種サーバ類を学校内に置いた場合には、数量の増える機器の購入費用、遠隔地の多数拠点の保守運用費用増などを計算し、WANを広帯域にした場合の費用比較を行ってみることも、全体把握に役立つ。

(2) 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。その場合、LANで広帯域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)などを置き、クラウドからWANを経由して同一ファイルを複数回ダウンロードしないようにすることができる。

帯域計算を行うときは、利用形態と費用、機器構成により削減できる点を考慮して検討を行う。過去の事例等では、最も通信帯域を消費する可能性があるのはデジタル教科書の更新と端末OSの更新である。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ことになるが、デジタル教科書のコンテンツやOSは、非常にサイズが大きいためである。この時も、夜間のうちに、学校に設置した「キャッシュサーバ」のコンテンツ配信機能でダウンロードし、端末への配信は、そこから行うようにすることで、WANの帯域ひっ迫を防止できる

(3) ファイルサーバ

児童・生徒が作成した課題、参考資料を、ファイルサーバへ蓄積し、授業で利用することがある。データセンタやクラウドのファイルサーバを利用した、WAN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場合、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もありえる。ただし、この場合は、サーバの管理をだれが行うのか、データが消えた場合にどうするのか等を事前に検討しておく必要がある。

※仮想デスクトップ(VDI)等を利用する場合、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ことが多い。目の前の端末で表示されるが、実データはWAN上を移動せず、クラウドの画面イメージの転送だけのためである。VDIを導入するときは、業者との間でデータの流れを確認し、帯域予測を行うとよい。

2.1.5. 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。

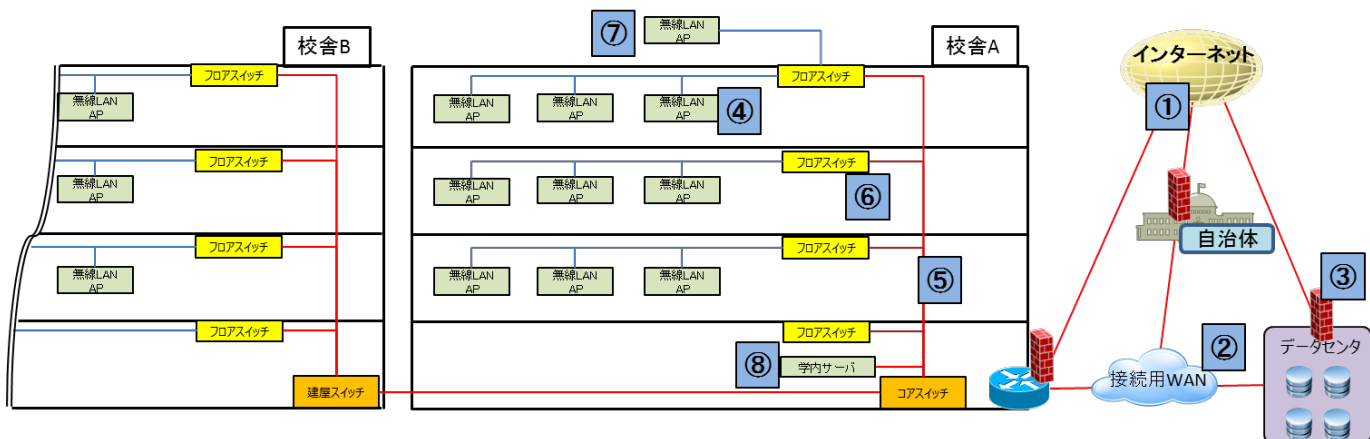
費用との関係から、最も過密な通信状態を想定した帯域確保を行わず、トラフィックの集中した時の、システム待ち時間が許容範囲に収まるかどうかで設計を行う。WEBの画面表示等であれば、数秒は許容されるし、動画再生でも、再生開始までの待ち時間が許容範囲であれば問題ない。ただし、音声通信やビデオ会議だと200msecの遅延が限界となる。

2.1.6. 学校内ネットワークのイメージ

学校内ネットワークを設計するとき、まず、校内のどこにネットワークのアクセスを準備するのか、どこが有線LANで敷設し、どこに無線LANでアクセスさせるかを視覚的に認識できる図や、必要なポートは一覧表などを作成し管理する。

- ネットワークのアクセスを準備する場所
職員室、普通教室、特別教室、コンピュータ教室、体育館、校庭、屋上など
- その場所に用意するアクセス方法（例：普通教室）
児童・生徒用の無線LANとIWB（電子黒板）用の有線LANポート
- その場所のネットワークに求められる要件
接続される端末数と想定帯域
利用者の種別（教員、職員、児童・生徒、災害時の周辺住民）

上記のような必要条件から、ネットワークの分離技術や認証に対する要件を確定



機器や部材	注意点など
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 校内無線LAN	児童・生徒等の多くの端末から利用される。通信規格、アクセスポイント管理、設置場所など
⑤ 校内有線LAN配線	ネットワーク配線することを配慮されていない校舎でLANを敷設する時の注意など
⑥ 校内LANスイッチ	無線LANの集線、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 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 2-3 学校内ネットワーク構成

2.1.7. 無線LAN

学校における無線LAN環境では、児童・生徒の多くの端末が、狭い教室で、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、同時利用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、教育ネットワークの無線LANで、最も重要になるのは、アクセスポイントへの同時接続数のサポートと、多くの端末からの同時通信でスループット低下や接続断が発生しないことである。安定した通信環境が提供されるべきである。

■無線LAN環境を導入する上で必要なポイント

・高速通信

使用する周波数帯の選択

通信規格の選択

・安定した通信環境

外的要因による影響の排除

DSF

セルの設計とアクセスポイントの教室設置・セキュリティ対策(セキュリティについては2.1.10にて記述)

盗聴や侵入への対策

・状態把握、見える化

無線LANの状態を目に見える形で監視する

(1) 高速通信

無線LANでは帯周波数帯(2.4GHzと5GHz)をいくつかのチャンネルに分割し、1つのチャンネルで、その瞬間に通信のために電波を出力してよいのは1台のみという通信方法をとっている。

同じチャンネルで接続される端末が増えるほど、端末あたりの割り当て時間が減ることになり、結果として各端末の通信速度が低下することになる。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あり、全員が同時に通信を行いたいような場面では、完了までに時間がかかってしまう傾向がある。費用を考慮した上ではあるが、なるべくチャンネル数の多い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を増し、授業中のダウンロードなどによる待ち時間を削減するようにする。

・使用する周波数帯の選択

5GHz帯

無線で使える周波数帯。5GHz帯の方が利用できるチャンネル数も多いため、狭い範囲に多くのアクセスポイントを配置する場合の設計が容易で、Wi-Fi通信を阻害する干渉減も少なく、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。

教育ネットワークでは、端末数が多いことや、隣り合う教室での同時利用を考慮すると、5GHz帯での無線LAN設

置を推奨する。

- ・ 利用可能なチャンネルは国や地域ごとに異なるが、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
- ・ W52, 53 が屋内利用のみ、W56 は屋内・屋外で利用が可能
- ・ 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）。

2.4GHz帯

- ・ Ch1～11 までの 11 チャンネルの中で、使用可能なのは、干渉しない最大 3 つのチャンネル
- ・ 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

・通信規格の選択

無線LANの通信規格は、1999年のIEEE802.11b以降、通信の高速化を図るため改定されてきた。新しい規格を利用すると高速通信を行えるが、利用する機材によって対応が可能か確認する必要がある。新規購入であれば、IEEE802.11n(5GHz)やIEEE802.11ac対応の機器を強く推奨する。

学内で利用する上で、古い機材(PCなど)が混在していると、古い機材に対する通信時間が長くなったり、複数の規格への対応が必要になったりするため、想定外の障害やデメリットが発生することがある。設置検証時に予定通りの速度が出ていない場合は無線LAN管理ツールなどで、無線を占有している端末の調査等を実施する。

表 2-2 無線LAN規格

	2.4G帯	5G帯
11Mbps (規格値)	IEEE802.11b (1999)	
54Mbps (規格値)	IEEE802.11g (2003)	IEEE802.11a (1999)
600Mbps (規格値)	IEEE802.11n (2009)	
6.9Gbps (規格値)		IEEE802.11ac (2014) (現行製品は最大規格値1.7Gbps)

※規格値は、理論最大値であり実行帯域とは異なる。() 内は策定年

IEEE802.11ac

2016年現在、最大規格値1.7Gbpsで通信可能な最新無線LAN規格。

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。

最大規格値は1台の機器が複数のチャンネルを使用した場合であり、複数台の機器が同時に利用できるわけではない。

(2) 安定した通信環境

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不安定になることがある。敷設後にそのようなことにならないために、「外的要因による影響の排除」、「セルデザイン」(アクセスポイント間のチャンネル干渉の排除)を設計時に実施しておく。

・ 外的要因による影響の排除

2.4GHz帯は、もともと通信に特化した周波数帯ではなかったため、無線LAN以外の製品での利用も多く、それら非無線LAN製品による干渉が多い。また、それらの2.4GHz利用は違法でもない。

2.4GHz帯で通信をしたり、その周波数帯にノイズを出す可能性がある製品には以下のようなものがある。

- ・ 許可されていないが設置された無線 LAN 機器
- ・ コードレスホンなどの近距離通信を目的とした機器
- ・ CT スキャンなどの医療機器
- ・ 電子レンジなど電磁調理器

これらの機器が近くにあると、無線LANはチャンネルを利用できずに、通信が不安定になるため、設置設計時に距離を離すか、これらの機器を遮蔽する。

5GHz帯は、無線LANが割り当てられる前に、レーダー利用周波数帯だったため、近隣にレーダーサイトがあると、影響を受ける。近隣にレーダーがない場合で最も影響が大きいのは、無許可設置の無線LAN機器や、アクセスポイント設定になった携帯電話である。

・ 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、初期の設定でDFSが動作する周波数帯は利用しないなど配慮する。

・セル³の設計とアクセスポイントの教室設置（アクセスポイント間のチャネル干渉の排除）

学校など、ある狭いエリアで複数アクセスポイントを同時に動作させ、数多くの端末が各アクセスポイント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1つのアクセスポイント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、1つのアクセスポイントに接続される端末が増えてしまい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であり、避けるべきデザインである。

従ってアクセスポイントの電波強度を下げ、教室あたり1つ以上のアクセスポイントを設置し、1つのアクセスポイントあたりの収容端末数を少なくする事が望まれる。

- ・ アクセスポイントの電波が届いても、端末が同じ距離の電波を飛ばせるとは限らず、片側通信になる可能性がある
- ・ 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る可能性が高まる
- ・ 下図のようにセルサイズが大きいと、アクセスポイントあたりの端末接続数が増えてしまい、端末の通信速度が下がる

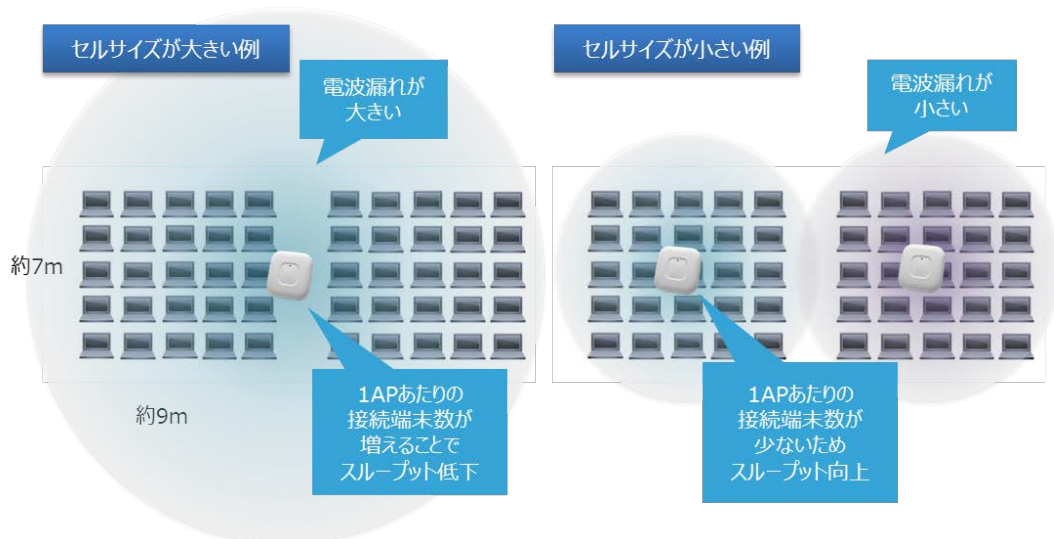
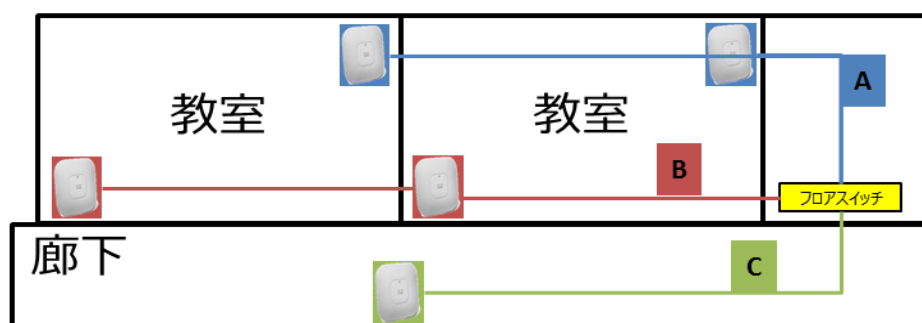


図 2-4 セルデザイン

上記のようなセルデザインを想定の上、各教室にどのようにアクセスポイントを設置するか設計する。

下図は、一般的な普通教室の配置をもとに、教室と廊下へのアクセスポイントの配置を図化したものである。また、それぞれの設置パターンでのメリット・デメリットを示した。教室の配置や校舎間の距離、隣の校舎を介した、上下階への反射など、他の要因も起こり得るが、基本的な設計の参照としていただきたい。

³ セル：1つのアクセスポイントから電波が届く範囲



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 廊下のアクセスポイント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、廊下のアクセスポイントの利用頻度が低い
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"> 教室のアクセスポイントが故障した場合、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 2-5 普通教室への無線アクセスポイントの設置例とメリット・デメリット

・ 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、アクセスポイント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。

・ 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。

・ 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。

・ 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。

・ 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。

(3) 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。最終的なアクセスポイントの設置場所を決めるには、現地でのサイトサーベイを行うことが望ましいが、環境が異なるとサイトサーベイ結果と実際の利用時とで異なる場合がある。

- ・ 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

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。）

(4) その他

- ・ 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

2.1.8. 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などして、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。

- 有線LAN環境を導入する上で必要なポイント
 - ・高速通信(LANの広帯域化)
 - 敷設する配線の選択 (ツイストペアとファイバ)
 - 通信が集中する箇所の広帯域製品の導入
 - ・ネットワークの安定化
 - 二重化(冗長化)などでの障害耐性の向上
 - リング構造での線路の冗長化
 - 論理分割技術等での障害の局所化
 - ・サービスの品質確保
 - ・セキュリティ対策 (セキュリティについては2.1.10にて記述)
 - 盗聴や侵入への対策
 - ・状態の把握、見える化
 - 有線LANの状態を目に見える形で監視する

(1) 高速通信 (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、短距離での1Gbps、ファイバーケーブルは1/10Gbps以上で利用されている。

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も可能になった。新規の通信機能については相対する機器での導入が必須となる。

表 2-3 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) ネットワークの安定化

・ 機器の二重化（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言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費用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。

・ 通信経路の冗長化

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配線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を行うことがある。しかし経路の冗長化は、配線のリング化(物理的なループ)が形成される。管理されないループはデータの回り込みなど障害の原因となるため、スパンニングツリーやルーティング技術で対応する(ここでは技術的な詳細は省く)

・ 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。

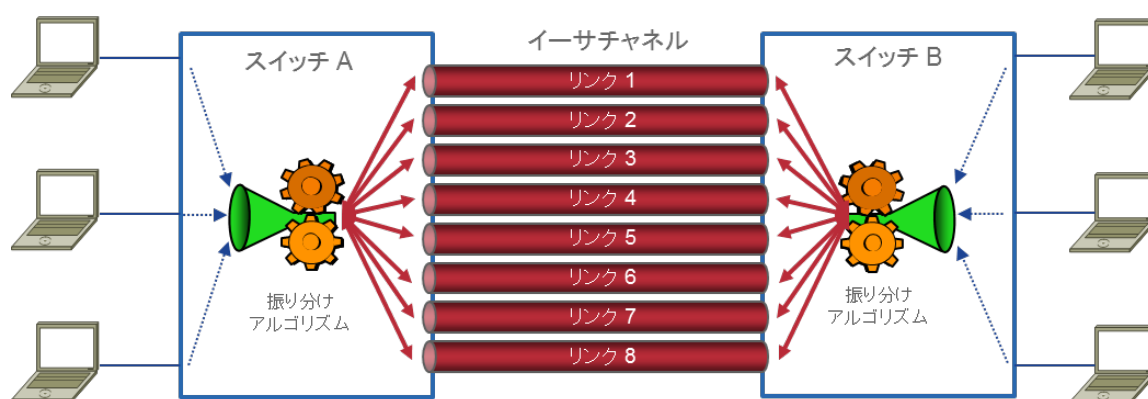


図 2-6 イーサチャネルによる多重化

(3) 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。

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。

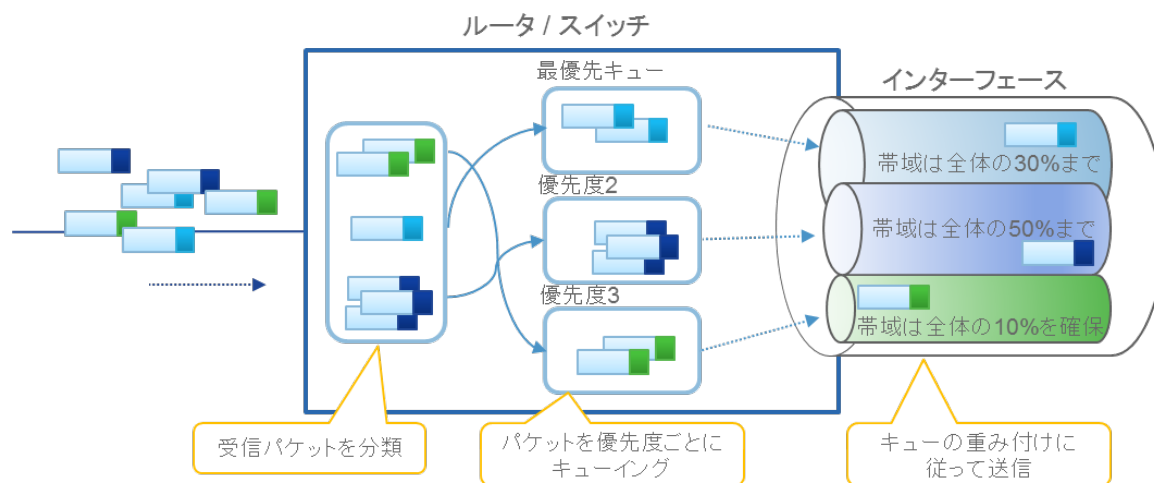


図 2-7 QoS 実行例

(4) 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。

2.1.9. 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。

外部の動画等の利用が想定される場合は、イントラネットワーク、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。

表 2-4 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

2.1.10. セキュリティ対策

(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

インターネットの高度利用とセキュリティの確保を両立したICT環境の構築には高度な知識を要する。データの配置、クラウドの利用、データセンタとの接続方法、端末の種類やアプリケーション、利用者のセキュリティ知識レベルなどによって対策方法が異なるためである。本書でも唯一のシステム構成を提示することが困難であるため、現在のセキュリティ対策の基本的な考え方と、そこで利用される機器について記述する。

2016年7月に開催された「2020年代に向けた教育の情報化に関する懇談会（第5回）」において、「教育情報セキュリティのための緊急提言」が行われた。

今後の教育ICTにおけるセキュリティのあり方を再検討することになるが、セキュリティの基本として、本書の解説が有効と考える。

参考：

文部科学省「2020年代に向けた教育の情報化に関する懇談会（第5回）」

http://www.mext.go.jp/a_menu/shotou/zyouhou/1375322.htm

文部科学省「教育情報セキュリティのための緊急提言」（2016.7月）

http://www.mext.go.jp/component/a_menu/education/detail/_icsFiles/afeldfile/2016/08/09/1375325_02_1.pdf

リスク低減に対する考え方

まず、セキュリティ対策では、リスクを完全除去する方法と、リスクを低減する方法がある。

リスクを完全に除去できることが最もよいが、費用や利便性の観点からの検討を行う。そこに残るリスクについて、リスクを低減するための方策を検討する。

例えば、教職員が成績の管理を行う校務支援系の端末をインターネット等外部接続と分離することで、セキュリティ上のリスクを大幅に減少又は取り除くことができる。しかし、校務支援系システムには、利便性の要求から以下のようなポイントで外部接続する可能性があり、その場合のリスクを低減する対策をとる必要がでてくることになる。

表 2-5 現場要望と対応するリスク

校務支援系端末のリスク	現場から要求される利便性	必要となる検討すべき対策
インターネット利用	校務支援系端末でメールの確認をしたい	外部からの侵入防御、 メールセキュリティ、 添付ファイルの無害化、 VDIでの仮想アクセス WEBアクセスのチェックなど
USBメモリ等外部デバイス	教職員間でファイルを共有したい 外部のファイルを持ち込みたい	USB経由ファイルのウイルスチェック機能、 USBメモリの紛失対策、 機密データの持ち出し防止
持ち込み端末の利用	自宅の端末を利用したい、 システム管理者が持ち込む端末	端末の隔離検閲機能、 接続端末認証

多層防御の考え方

インターネットが一般開放された当時(1993年)と異なり、組織の境界を防御するだけではセキュリティ確保を行えないというのが、現在の一般的な考え方である。そのため複数のポイントで様々な手法を用いてセキュリティ事故発生の確率を下げていき、重大事故が発生しないようにするのが、多層防御やEnt to Endセキュリティといわれる手法となる。

教育ICTにおける多層防御の前提は、利用者グループとデータ重要度に応じて、分離、多層化したネットワークを構築し、各ネットワーク間にセキュリティポリシーに対応した対策を行うこととなる。

「1. 教育ネットワークの全体像」にも記載があるが、教育ネットワークにおいては、情報の重要度から最低以下のネットワークに分離されることが考えられる。もちろん必要に応じてこれ以上の分離もあり得る。

- ・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授業支援系ネットワーク
- ・成績情報に代表される機微情報を扱う校務支援系ネットワーク(職員室のみでなく普通教室からも安全に利用することを前提に構築されることが望まれる。)
- ・教職員が、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)

これらのネットワークを分離し、ネットワーク間の不正侵入を防御し、それでも侵入された場合の対策を講じることで多層防御によるセキュリティの確保を行う。

なお、端末やアプリケーションを含めたセキュリティについては「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。

表 2-6多層防御のステップ

実施する対策	考慮する要素や想定する脅威	利用される機器や機能
組織やデータ重要度でグループ化	データの機微度 利用者の属性(教職員、児童・生徒、システム管理者など)	利用者確認、属性の確認のための認証(そのレベルにより生体認証や二要素認証)
グループ間に境界を設けて分離	学内とインターネット 校務支援系と授業支援系	ファイアウォール、VLAN、VRFなどの分離技術、
内側に侵入する攻撃への対応 (外部からの侵入対策)	物理的な侵入(有線LANや無線LAN侵入) ネットワーク経由の直接侵入、マルウェアやワーム(メール添付、WEBアクセス時、USBメモリ経由、ソフトウェア埋め込みなど)、児童・生徒の校務支援系への侵入	接続認証、二要素認証、ファイアウォール、IPS/IDS、メールセキュリティ、WEBフィルタリング、サンドボックス、Proxyサーバなど、侵入経路と手法により設置場所と機能が選択される
侵入された場合の対応 (脅威の可視化・拡大防止と機密データの改ざん、漏えい防止)	権限を持たないユーザによるファイルアクセス、データ改ざん、データ持ち出し、感染端末の拡散	サーバ機能、システム監視、ログ分析、端末セキュリティなど
組織内の攻撃	職員によるデータ持ち出し、外部システム管理者のデータ持ち出し、閲覧、改ざん	システム監視、ログ分析、特権ID管理など

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る。

(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 2-7 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

(3) 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。

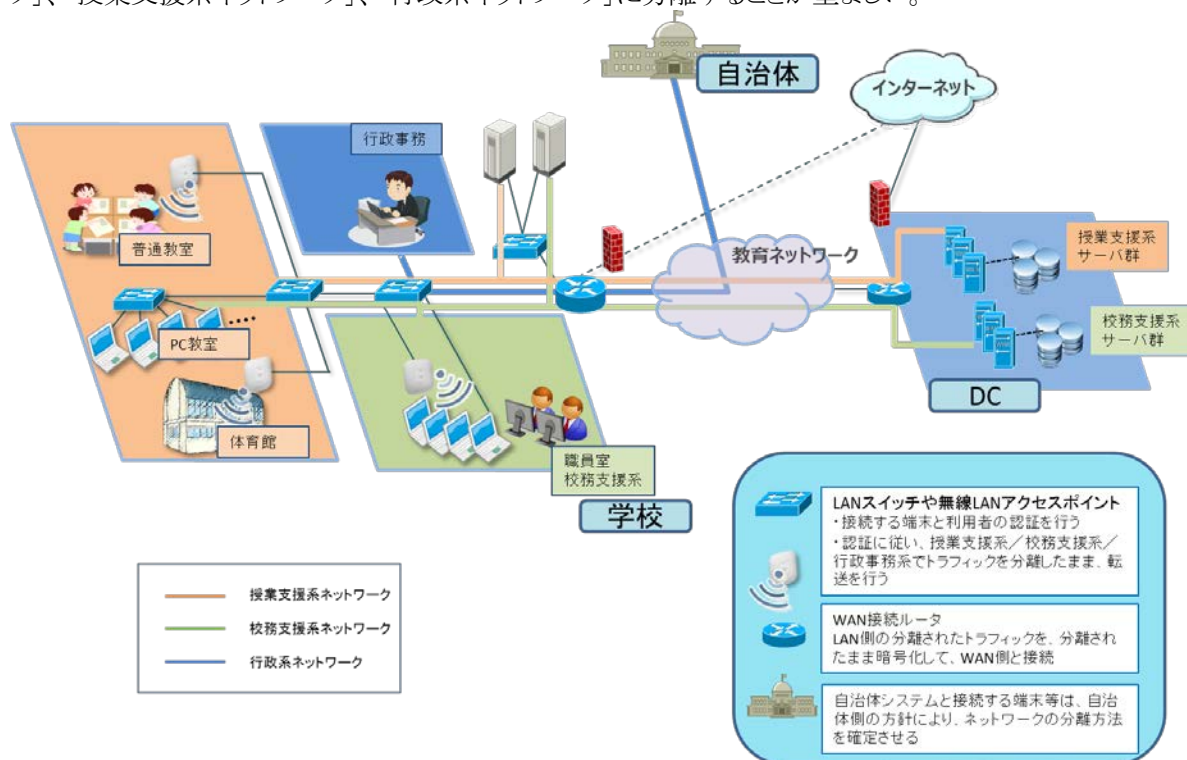


図1-1授業支援系ネットワークと校務支援系ネットワークの分離イメージ

① 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⁴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」利用端末はサブリカントを採用の事
- ・ 「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 インターネット接続部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⁵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 2-8 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検知と防御	ファイアウォール、IDS/IPS、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 ⁶ 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

⁴ 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

⁵ 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

⁶ 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。

- ・ 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

(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⁷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⁸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

③ 無線 LAN におけるセキュリティ要件

不用意な設定をされた無線LANは、第三者から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に侵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が望まれる。特に認証に関して、ID/パスワードのみの利用では、パスワード漏えいにより簡単に侵入を許してしまうため注意が必要となる。校務支援系ネットワークへのアクセスには、生体認証、二要素認証、端末証明書の利用を推奨する。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

⁷ 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

⁸ 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

討の参考となる。

(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⁹（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。

(4) 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。

(5) 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

⁹ ESSIDについては、アクセスポイント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

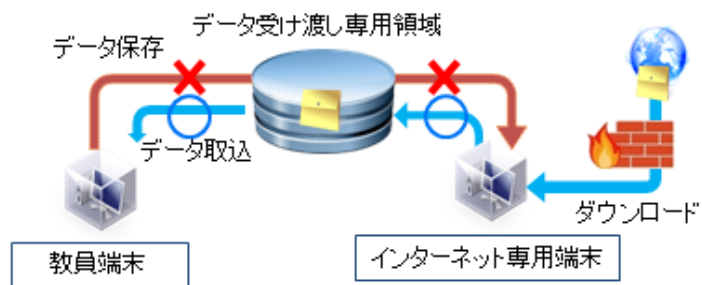


図 2-8 データ受け渡し領域のモデル例

- ・ 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 データの受け渡し 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. 教育ネットワークの運用検討

教育ネットワークを長年にわたり快適に安定的に活用するためには、運用について事前に検討を行う必要がある。初期のネットワーク敷設のみを行い、そのあとは専門知識を持たない現場の教職員に運用を期待しても、教育を受けていないため、無理がある。

例えば、ネットワーク障害発生時や、帯域不足に陥った場合の状況解析などは、専用のツールや専門知識がないと対応ができず、障害が長期化してしまい、その間、教育のICT利用は滞ってしまう。結果として、教育でのICT利用が敬遠されてしまう事となる。

3.1. 教育ネットワークの運用要件

教育ネットワークの運用を設計するとき、監視装置など専用のシステムを使った状態の把握と見える化、機器の異常や障害を検知した場合の交換の容易性などシステムの設計、利用者として障害が認められるときのヘルプデスクやオンサイト保守などの人的サポートと、多面的な設計で運用の安定化を図る。また、費用高になることが多いが、教育ネットワークや校務支援システムのサービス時間やサポートレベルを、納入業者に確約してもらう方法として、SLAの条項を入れることもある。運用については、すべて費用に影響する要件となるが、教職員で対応する場合の教育費用等との兼ね合いで、どこまでを外部委託するのかを検討する。教職員が教育に専念するために、可能な限り外部委託することを推奨する。

注意点として、ネットワーク状態の見える化を行わずに、ヘルプデスクを設置しても、何も情報がないまま対応することになり、専門家であっても障害解決の時間短縮にはならない。

■ ネットワークの品質確保

- ・ネットワークの状態の見える化
ネットワーク機器や通信の状態把握
- ・保守交換容易性
サービス停止に影響する障害機器の交換
- ・サービスレベル契約(SLA)
サービスのレベルでの契約
- ・ヘルプデスク
障害時の専門家への問い合わせ
- ・オンサイト保守
機器の現地での交換等

3.1.1. ネットワークの品質確保

ネットワークの品質を確保するためには、現在何が起きているのかを把握(見える化)する必要がある。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、回線の状態を把握することで、初期の対処と解決策の発見を早め、早期に解決する為である。

(1) ネットワーク機器の見える化

まずは接続構成をトポロジー図として俯瞰的に把握し、それぞれの機器の状態監視は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内容があげられる。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。

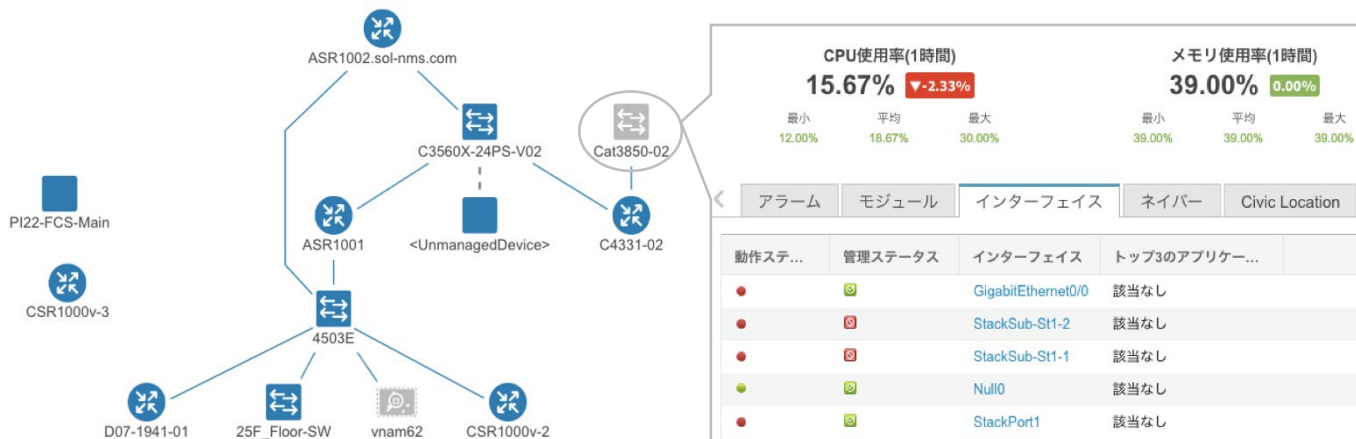


図 3-1 トポロジー図と接続デバイスのCPU/メモリ使用率 出力サンプル

(2) 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。

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。

・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。

・流れているトラフィック情報の詳細を把握

管理情報ベース(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が、より詳細な情報取得のため、ネットワーク機器によっては、フロー解析技術を利用することが可能である。フロー解析技術には、NetflowやSflowなどの名称がついており、下記の情報を見ることができる。

- ・ 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

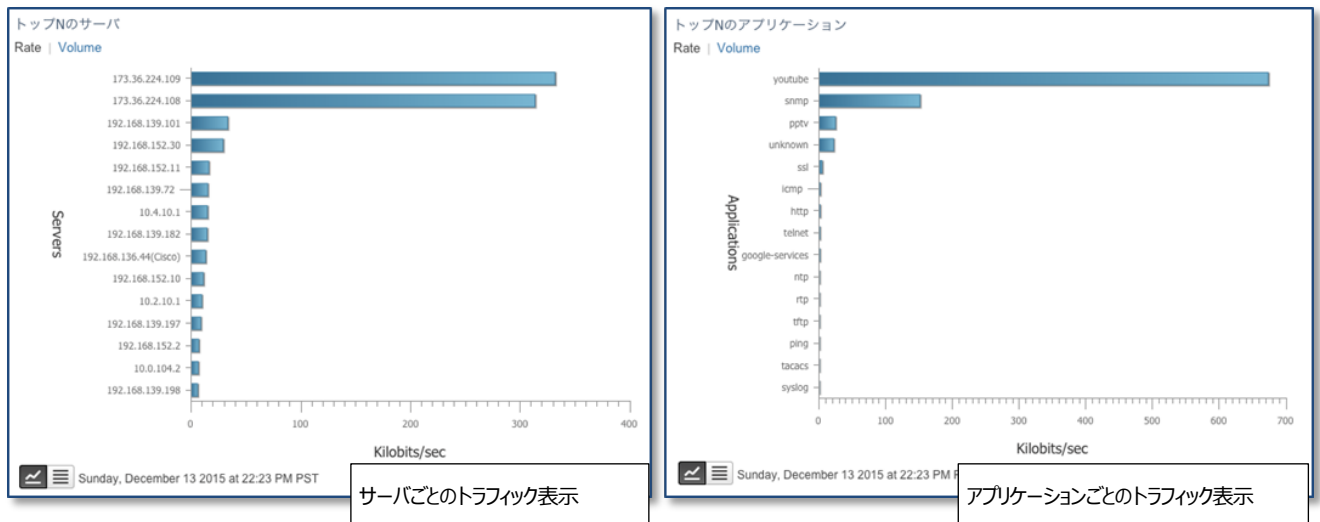


図 3-2 外部管理ツールによるトラフィック可視化のサンプル

(3) 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 箇所を確認できる GUI やツールなど
- ・ 電波環境やトラフィックの履歴管理
- ・ アクセスポイントを管理するコントローラの冗長性
- ・ アクセスポイントが故障した場合に、他のアクセスポイントで電波エリアをカバーできる出力の自動調整

3.1.2. 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¹⁰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、一次対処を行わせることも検討する。

(3) インシデント¹¹ (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。

3.1.3. 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。

¹⁰ エスカレーション:より上級の対応部署や人員に上申する事

¹¹ インシデント:事象、事故などの意味。ICTでは、障害やセキュリティ事故を指すことが多い

(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。

3.1.4. SLA(サービスレベル契約)

(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、校務支援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 3-1 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

3.2. 教育利用の特有シーンにおける運用要件

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。また、校務支援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。

3.2.1. 環境準備

・ 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。

・ 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。

・ 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。

3.2.2. 一斉授業

- **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。無線アクセスポイントを利用するため、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。

- **児童・生徒全員の一斉操作の運用検討**

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。

3.2.3. 個別学習

- **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授業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。

3.2.4. 校務支援システムの利用

- **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。

- **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。

- **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。

3.3. 教育委員会・学校における運用要件

教育ICTのネットワークを利用・運用するためには、教育委員会のみではなく、学校、調達部門、情報システム部門、施設部門などと連携し、運用ルールの作成や共通理解を推進することで、教育ICT環境の足回りであるネットワークを“常に使える状態”を維持でることが肝要である。

また、学校のネットワーク状況やシステム利用状況を教育委員会や自治体の関連部門が参照するため、学校外への公開が必要となるのが、セキュリティトラブルや不正利用対策の観点で公開方法や運用ルールを検討する必要がある。

3.3.1. 教育委員会・学校

教育ネットワーク全体を運営するために、各学校における運営体制、各学校と連携するため教育委員会での体制作りを行うことが不可欠である。ここでは、運営に必要な要件をまとめる。

表 3-2 教育委員会・学校における運用に必要な要件

組織	要点	内容
教育委員会	把握しやすいシステム	学校のCIO（最高情報責任者）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。
	運用作業と運用権限	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。
	セキュリティ監査など訓練 体制の継続的な見直し	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。
	学校の敷線管理	学校にネットワークを整備すると、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、学校のネットワークを維持・管理するため、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である。特に、施設部門が教育委員会以外にある場合、連携を充分にとり、資料の最新化に留意する。
学校	学校内の体制作り	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。

3.3.2. システム状況の外部公開への対応

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。たとえば、ネットワークの障害通知、負荷状態の把握、未許可の無線LAN端末の発見などを目的に参照などが挙げられる。

学校の運用状況を把握するためには、学校の情報を教育委員会や情報システム部門などに公開するために、経路を用意する必要がある。この経路からの不正侵入に対策する必要がある。たとえば、経路の入口・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。

3.3.3. 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など、調達する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次節以降に示す。

3.4. 外部組織への業務委託

教育ネットワークを利用・運用する上で、要所毎にその専門的な知識や技術が必要となる。外部専門組織に対して業務委託を行うことで解決に図るが多い。効率よく効果的に教育ネットワークを利用するため、その運用方法を明確にすることは不可欠である。

3.4.1. 運用方法の明確化

外部組織に対して業務委託を行なう場合、教育委員会は、契約に基づく各種運用方法を明確にし、学校に対し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	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
機器等	機器の障害や破損の場合の対応ルール 等
その他	その他の委託内容のルール 等

3.4.2. 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、システムの標準のID(デフォルト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。これを実施することで、いつ・どこで・誰が・何を操作したかをシステムの記録として自動的に記録でき、セキュリティインシデント時における影響範囲などに寄与でき、また、不正利用の抑止にもなる。

3.5. ICT支援員

教育ネットワークの活用は、学校現場にゆだねられているが、多くの学校ではICTに関する知識や経験の無さから、有効に活用されていないことが多く見受けられる。一方で、導入後の活用率を上げることは、自治体担当者の責務でもあり、ICTの専門スタッフとして学校にICT支援員を配置する自治体が増えてきている。一般に、教育委員会・業者・ICT支援員・学校間における契約～サービス提供の流れは以下のとおりである。

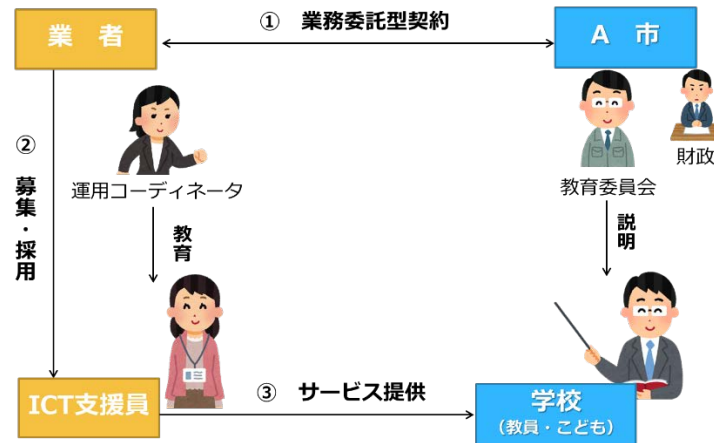


図 3-3 ICT支援員によるサービス提供の流れ (例)

3.5.1. ICT支援員の必要性

中央教育審議会においても社会の変化に伴う指導内容の変化に学校や教員だけが対応するのでは十分に解決できない課題が増えてきていることに対し、「チームとしての学校の在り方と今後の改善方策について(答申)」の中で、「国・教育委員会は、ICT活用のスキルを持った専門人材等の確保、活用を図りつつ、ICT支援員を養成し、学校への配置の充実を図る」という具体的な改善方策が述べられている。

http://www.mext.go.jp/b_menu/shingi/chukyo/chukyo0/toushin/attach/1366271.htm

平成25年度に一般社団法人日本教育情報化振興会が実施したアンケートでは、「授業でのICT活用、校務支援システムの導入などで、ICT支援員の必要性が高まっている」に対して「強くそう思う・そう思う」と回答した教育委員会は全体の約90%となっており、その必要性は自治体担当者がもっとも感じているところかと思受けられる。

http://www.japet.or.jp/index.php?action=pages_view_main&active_action=journal_view_main_detail&post_id=788&comment_flag=1&block_id=1053#_1053

3.5.2. ICT支援員の業務内容

教育ネットワークの整備にあたり、ICT支援員の業務範囲をどこまでにするか、ということは非常に難しいである。前提条件として、業務内容を依頼する前に教育委員会(学校)、業者、ICT支援員の間で、学校環境やデータの取扱い等に関して、自治体ポリシーに準じた守秘義務(誓約書)等を交わすなどの仕組みが必要である。ICT支援員の業務内容や実際の活動については、以下のとおりである(文部科学省「学校のICT化のサポート体制の在り方について」(H20.7)および「学びの場.com」(<http://www.manabinoba.com>)より抜粋)。

- ・ **機器・ソフトウェアの設定や操作**

授業や研修の開始前に機器やソフトウェアを設定したり、授業中や研修中に操作したりする。また、校務に必要なソフトウェアの設定を行う。

- ・ **機器・ソフトウェアの設定や操作の説明**

授業や研修に向けて、あらかじめ、機器・ソフトウェアの設定方法や操作方法を教員や研修講師(情報主任等)に説明する。また、授業中に、児童生徒が使う機器・ソフトウェアの操作方法について説明するなど、教員の指導を支援する。校務で使用するソフトウェアの設定方法や操作方法を教員に説明する。

- ・ **機器・ソフトウェアや教材等の紹介と活用の助言**

授業や研修に使用する機器・ソフトウェアやデジタル教材について情報を収集し紹介するとともに、それらの効果的な活用方法や指導案・指導計画づくりについて教員に助言する。

- ・ **情報モラルに関する教材や事例等の紹介と活用の助言**

情報モラルに関する教材や事例、対処法等について情報を収集し紹介するとともに、それらの効果的な活用方法や指導案・指導計画づくりについて教員に助言する。

インターネット上の有害情報等の問題については、情報サービスの変化・多様化や、その中で児童生徒がこれまでなかったような被害に遭うケースの出現も考えられることから、最新の情報をもつICT支援員の役割は重要である。

- ・ **デジタル教材作成等の支援**

授業や研修に向けて、あらかじめ、必要なデジタル教材について教員の依頼を受けて作成する。

- ・ **機器の簡単なメンテナンス**

授業や研修、校務に使用する機器やソフトウェアの簡単な調整・保守を行い、トラブル時には故障箇所の切り分けや保守管理業者への連絡を行う。

http://www.mext.go.jp/b_menu/houdou/20/07/08072301/001/004.htm

また、「先生と教育行政のためのICT教育環境ハンドブック2016」(一般社団法人 日本教育情報化振興会)の中で、「ICT機器が故障したときの修理や、システム障害の復旧をICT支援員が行うことは、基本的にできません。ICT支援員とは別にICT機器やシステムを導入した業者と保守契約を結んでおく必要があります。」とある通り、ICT支援員が行うのはSE,CEが行うような業務とは異なるので注意が必要である。

3.5.3. ICT支援員に求められる資質

ICT支援員は、先生や子ども達と接する機会が多いため、これらを加味すると、スキル面よりも人物面に関する資質が重

要となってくる。

■ 人物面における資質（例）

- | | |
|-----------|---------------|
| ・明るい人 | ・ルールやマナーが守れる人 |
| ・子ども好きな人 | ・公平性を持った人 |
| ・即応性を持った人 | ・礼儀正しい人 |
| ・向上心のある人 | ・目的意識のある人 など |
-

一方、スキル面の資質を担保する資格として、「ICT支援員能力認定試験」や「教育情報化コーディネータ」といったものがあり、特にICT支援員を管理・教育する人材については、「教育情報化コーディネータ2～3級」の資格を求める自治体が増えてきている。こうした管理者が、ICT支援員に対して事前の教育や配置後のOJT、定期的な研修などを実施し、支援員を育成できる業者であることも大切である。

3.6. PTAのネットワーク利用

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。

4. 学校内ネットワークの敷設

施設内にネットワークを敷設する上で、学校において課題になりやすいポイントを掲載しておく。無線LANであれば、アクセスポイントの設置個所と個数について、有線LANについては、児童・生徒への安全配慮と配管等でのネットワークの保全となる。また、参考として、調査から施工までを順番に参考写真・参考図を使い解説する。

4.1. 無線LAN

4.1.1. 設置場所

無線LANの電波の広がりを考慮して設置場所を決めることになるが、アクセスポイントと端末の間に人間の体が入り込まない方が、不安定要素が少なくなる。また、アクセスポイントが手に届きやすい場所に設置されていると、児童・生徒のいたずら等、余計なリスクを発生させるため避けるようにする。

- **設置推奨場所**

- 天井（表側）
- 壁の高い位置（3メートルほど）

- **設置非推奨場所**

- 天井裏や床下
- 足元に近い位置
- 屋内用のアクセスポイントを屋外に設置すること

4.1.2. 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性質があるため、これらの影響を考慮してアクセスポイントを設定する。

1つのアクセスポイントで複数教室をカバーする場合は、廊下への設置も検討対象となるが、廊下との壁面の素材や、金属メッシュの有無を把握しておく。

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、可能な限り実利用に近い環境で実施することを推奨する。

4.1.3. 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にすることもできる。人が通常より密集するエリアでは、セルサイズをさらに小さくする高密度用途のアンテナ、体育館など設置場所の天井が高い場合にセルを小さくする場合は、下向きに指向性の強いアンテナを選択する。

同じアクセスポイントでも、オプションでアンテナの種類を選択できるものもあるため、利用場所によって業者に確認を行う。

4.1.4. アクセスポイントの堅牢性

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。特に体育館や、校庭への設置では、機器の物損が発生しやすいため、ガードの設置、耐候性の高いケースを利用する。

4.2. 有線LAN

学校内の有線LANの設置について、問題になるのは、学校内の配管の取り回しや電源の確保となる。

情報通信用の配管や配線を想定していない校舎においては、天井裏や床下を利用できなかつたり、校舎間の配線経路がないなど、企業で実施している工事手法が利用できないため、余計な経費が掛かる場合がある。

また、壁の貫通なども建物図面の不備から手間がかかる可能性があるため注意が必要となる。電源については、端末を含め、使用する機器の消費電力が学校の電力容量を超えないか、事前に計算を行う必要がある。

4.2.1. 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）の要否を確認する。

(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) 機器設置場所確認

LANスイッチや無線機器(アクセスポイント)の設置場所を確認する。むき出しでの設置は故障や破壊の可能性を高めるため、普段利用しない部屋へのラックでの設置などの可能性も検討する。

4.2.2. ルート設計と配線工事

校舎間等の屋外区間の配線は、來外を避けるため、必ず耐光性の光ファイバーケーブルを使用する。

屋内区間のLANケーブルはUTPケーブル(カテゴリー6以上)を使用することが多いが、LANケーブル布線距離が100メートル以上の場合、電源を確保の上中継器を設置するか、光ファイバーを使用する。

ケーブル敷設距離に関しては、2点間の直線距離ではなく、ケーブル長である。迂回配線など、距離は思いのほか長くなるため、注意が必要になる。

一般に光ファイバーの方が、収容するLANスイッチも含めて費用がかかるが、規定の距離を超えるUTPケーブルは不安定な通信となり、原因不明の障害の原因になるため、注意が必要である。

工事で使用するケーブルは、既存敷設されている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方が、追加工事の場合などに、混乱を生まない。

(1) 配線工事の留意点

- ・ 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。また校舎の施工時期によっては、アスベストの有無を事前に確認する必要がある
- ・ 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

下記に天井裏や床下配管ができない場合の屋内配管工事の作業例を挙げる。

右の配管の例で、児童・生徒が行き来する場所のばあい、緩衝剤での保護など、安全配慮が必須となる。

左の例では、高さがあるため安全配慮への課題は少ないが、逆に学校イベントで工作物を固定するために使用されてしまったり想定以上の荷重をかけられて破壊してしまう可能性がある。



図 4-1 配管工事イメージ

(2) 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。最近では、耐震工事の関係で、躯体に補強が入っていることがある、耐震補強骨材近辺のコア抜きには、十分に注意する

参考 経年保存について

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、「2.1.10 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。

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。

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。

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。

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		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	
教務	教育計画(学校・学年・学級経営案)	5年	会計	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		就学援助関係	10年	
	児童・生徒名簿・入学児童生徒名簿	5年	旅費	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		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	安全	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
電子文書の特性として、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。

参考 無線ネットワークの技術的な仕様/機能の詳細解説

• IEEE802.11ac

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。

• DFSの動作

- ① レーダー検知後、他のチャネルへ切り替えが必要
- ② 他のチャネル(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ネルは、検知後30分利用不可

• 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、アクセスポイント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

- **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。

- **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アクセスポイントへの影響が及ぶ。帯域幅を減らすことで、他に管理しているアクセスポイントに影響せず、かつ干渉の軽減も行える点がメリットである。

無線アクセスポイントのCPU・メモリ強化

IEEE802.11acはIEEE802.11nに比べて1,500 byteのパケット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、アクセスポイントのラジオごとのCPU、メモリの強化がされていることが望ましい。

- **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。

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。

- **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 - アクセスポイント間の有線区間はマルチキャストのままでも帯域を圧迫させないことが必要である。



・ 干渉対策

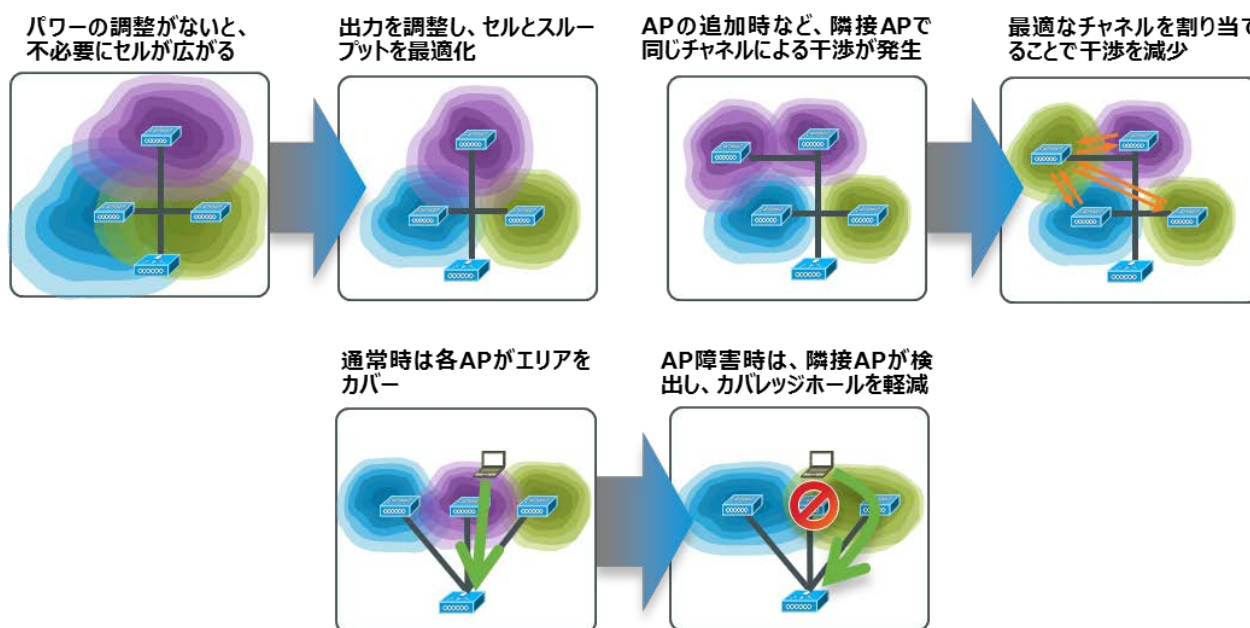
無線LANは免許不要の周波数帯であるため誰でも利用可能である。そのため、Wi-Fiおよび非Wi-Fiの干渉源対策が重要であり、下記の実装が必要である。

- ① システム内のアクセスポイント同士の電波干渉および不正アクセスポイント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、この機能がアクセスポイント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

・ 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。

- アクセスポイントの故障などにより電波が届かない範囲ができた場合、他のアクセスポイント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



無線LANの電波環境変化への追従

• ネットワークの冗長化回避技術（スパンニングツリー、ルーティング）

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ンニングツリー（STP）である。スパンニングツリーは、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、スパン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。

付録 用語集

用語	意味
FW	[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
IDS/IPS	[Intrusion Detection System] [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（IDS）と防御（IPS）を行う装置。
MDM	モバイル端末管理 [Mobile Device Management] 支配下にある端末の状態監視、アプリケーション配布、ネットワーク利用度などを監視するシステムを指すが、製品により実現する機能は異なる。教育においてタブレットの統一管理を行う場合に利用する。
MIB 管理情報ベース	[Management information base] ICT機器の内部情報を外部監視装置から取得するために、内部で保持しているデータベース規格
VDI	仮想デスクトップ[Virtual Desktop Infrastructure] 実際の処理をDCなどの仮想サーバ上で行い、利用者はキー入力と画面出力の転送にてサービスを受ける。利用者の目の前の端末では、アプリケーションやデータも存在しないためセキュリティ対策が行いやすい
VPN	[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の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は帯域保証されないため、接続速度の保証はない。
WAF	[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	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確認のためつけられる。
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
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
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
クラウド	[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
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)
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
サーバ	何らかのサービスを提供しているコンピュータ
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
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。
セキュリティ	[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。サーバ室の施設などの物理セキュリティも含まれる。
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。
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。
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
ポリシー	方針、基本規定の事
ルータ	ネットワークで、経路決定している機器
可動式コンピュータ	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
教育ICT環境	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。
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
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。
校務情報化	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。
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
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
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。
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。
無線AP	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
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