

# 教育クラウド整備ガイドブック

一般財団 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

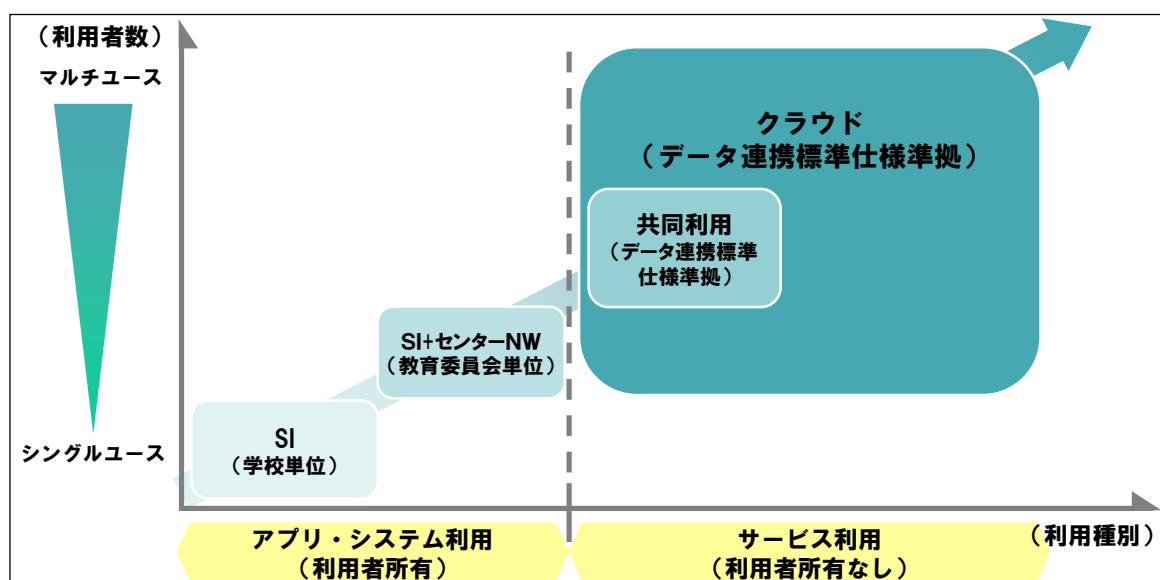
2013年3月  
第0.8版

## はじめに

公教育分野においては自治体業務と比較して標準化が進んでおらず、クラウドとは何か、どのようなメリットをもたらすものか、整備・導入時に留意すべきことは何か、調達者～事業者間の共通認識を形成など、クラウドサービスによる整備を推進するために整理・検討しなければならない事項が多い。一方で、平成 23 年に発生した未曾有の大震災を契機に、公的データ(教育分野においては指導要録や児童生徒の情報等)の電子化および保管や自治体業務の継続性確保の観点からもクラウド技術活用のメリットが再認識されている。並行して整備を進める教育情報アプリケーションユニット標準仕様(データ連携標準仕様)と同時に活用することで、本ガイドブックが自治体・教育委員会における教育分野のクラウドICT環境整備の一助となれば幸いである。

なお、教育分野のクラウド整備・導入状況について本年度ヒアリング調査を行った範囲では、実現に向けて検討中もしくは試行運用中であつたり、本格運用中ではあるもののクラウドサービスの要件を一部満たしていなかったりするなど、本格的な利活用例はまだ少数であり普及の前段階であることが判明している。今後も引き続き本ガイドブックの改版を通じて教育分野におけるクラウド技術活用の推進に資する所存であるが、同時に事業者が本格的にラインアップを整える際の参考資料としても活用いただきたい。

資料掲載URL [http://www.applc.or.jp/APPLIC-0005\\_1-2013.pdf](http://www.applc.or.jp/APPLIC-0005_1-2013.pdf)



## 【目次】

<b>1. 教育クラウドの概要</b>	<b>1</b>
1.1 ガイドブック(第 0.8 版)の位置付け	1
1.2 ガイドブックで対象とするクラウドの概要	2
1.3 教育クラウドが想定するアプリケーション	3
1.4 クラウドの配置モデル	3
1.5 クラウド利用の必要性和メリット	6
<b>2. 教育クラウドの整備</b>	<b>8</b>
2.1 想定する整備シナリオ	8
2.2 整備計画の策定	9
2.3 推進計画	9
2.4 セキュリティに関する検討	11
2.5 利活用支援の検討項目	11
2.6 サービスレベル (SLA) の検討	12
2.7 クラウド運用の検討	12
2.8 参考文献	15
<b>3. セキュリティ</b>	<b>16</b>
3.1 教育クラウドにおけるセキュリティ	16
3.2 セキュリティポリシー	19
3.3 セキュリティに関する検討事項	21
3.4 参考文献	32
<b>4. サービス調達</b>	<b>34</b>
4.1 サービス調達	34
4.2 サービスレベル	35
<b>5. アプリケーション毎の特徴と事例</b>	<b>38</b>
5.1 アプリケーション毎の特徴	38
5.2 事例	49
・ 北海道札幌市	
・ 福岡県北九州市	
・ 沖縄県宮古島市	
・ 東京都江戸川区	
・ 株式会社 HARP	
・ 静岡県富士市	
・ 千葉県千葉市	
・ 北海道札幌市	
<b>6. 今後の課題</b>	<b>69</b>
6.1 教育クラウドに関する今後の課題	69
6.2 本書の今後について	69
<b>7. 参考文献</b>	<b>70</b>

## 1. 教育クラウドの概要

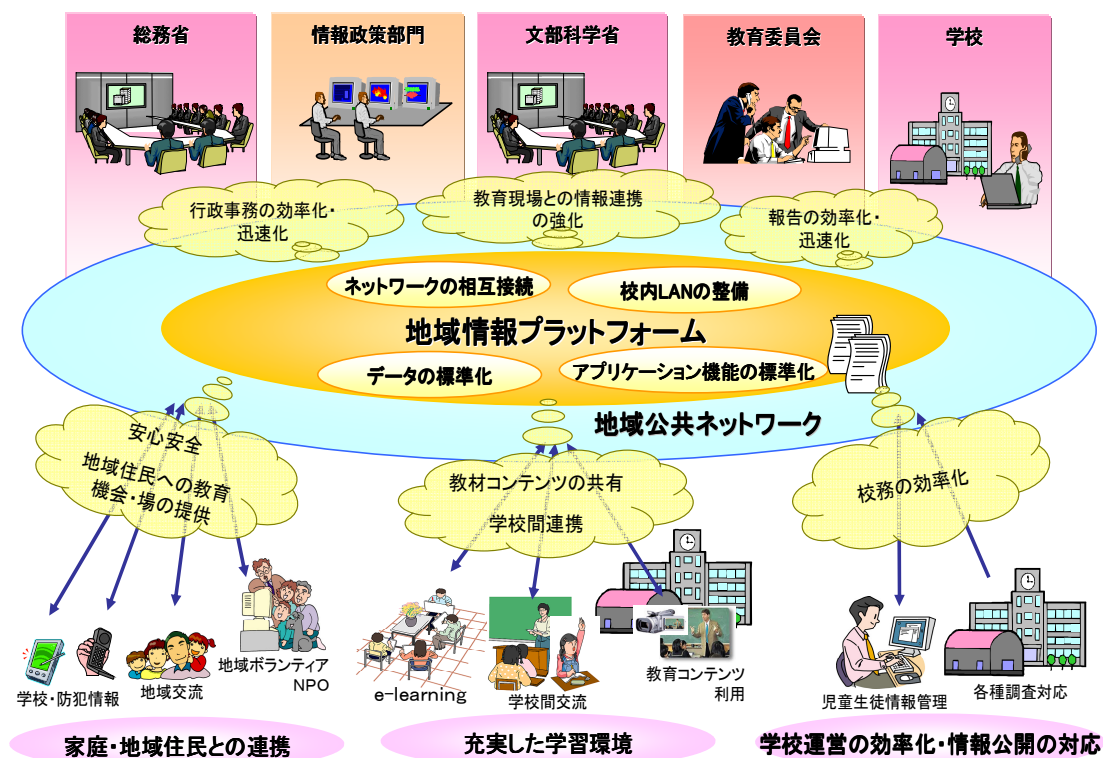
### 1.1 ガイドブック(第 0.8 版)の位置付け

教育クラウド整備ガイドブックは、地域情報プラットフォームに準拠した教育分野の公共アプリケーションを、昨今注目を集めているクラウド技術を活用して整備・導入するため、調達者となる自治体の視点からまとめたものである。具体的には、教育委員会の意志決定者、情報化担当部門および自治体の情報政策部門がクラウドサービスを取り入れる際に検討が必要な項目、整備の考え方、導入事例などを盛り込み、その特徴を活かして利活用が推進されることを目指している。

一般的にクラウドサービスは調達者、事業者ともに共通的なサービスイメージが十分に形成されておらず、教育利用においても研究に値する先進事例はまだまだ少ないのが現在の状況である。

また、本ガイドブックは、教育分野における公共アプリケーションとして利活用可能なクラウドサービスの充実に貢献することも必要と考えたことから、第 0.8 版として本格普及期前に編集することとした。よって、記述した内容は更なる見直し・充実が必須であり、特に以下の点については将来的な記載追加、見直しを想定している。

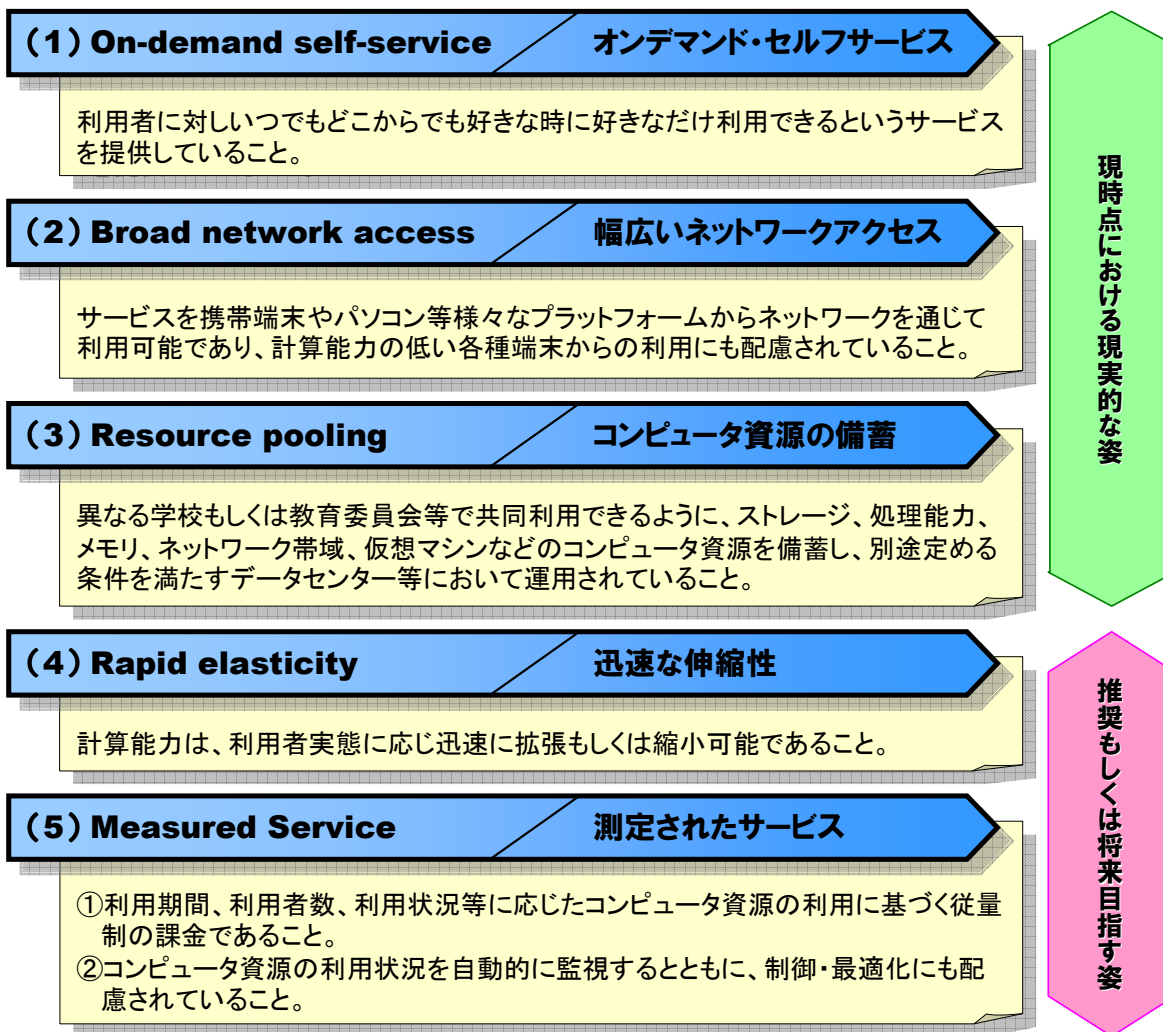
- ・ クラウド整備による効果について、実事例等から得られた知見等の記載
- ・ クラウド導入の調達仕様例、実事例等の記載
- ・ クラウド導入後のマネジメントノウハウに関する実事例等の記載
- ・ クラウド整備後の利用者サポートのあり方に関する方向性の記載





## 1.2 ガイドブックで対象とするクラウドの概要

本書で扱うクラウドは、NIST(アメリカ国立標準技術研究所)によるクラウドの定義である「5つの本質的特質」(下記)を有することを最終的な形態として定義している。なお、5つの本質的特質は比較的難解であるため、記載の趣旨を活かしつつ平易な表現とした。



たとえば、教育委員会が管轄内の学校を対象にクラウド整備を進める場合、物品やソフトウェアライセンスを購入して構築したシステムをデータセンターに格納することで、上記(1)(2)を満たすことは可能だが、(3)から(5)については従来型のシステム調達では実現が困難である。

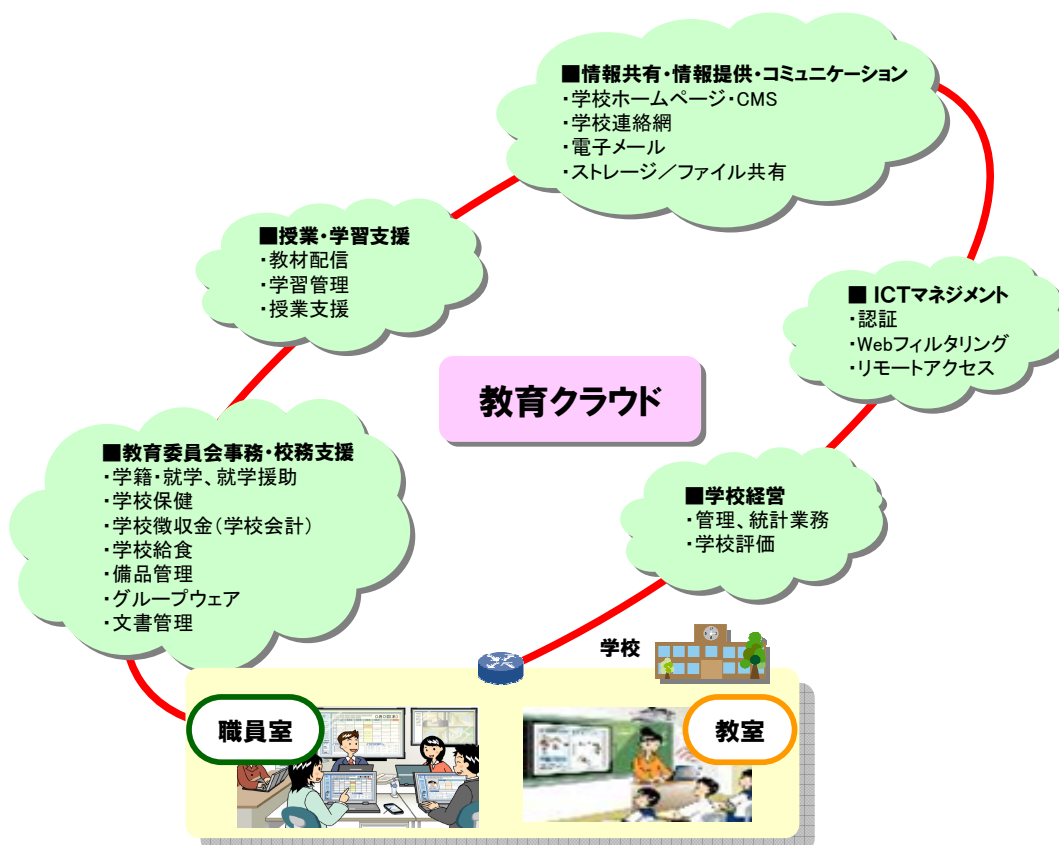
本来、利用者が計算資源の詳細を知らなくても使えるのがクラウド利用のメリットだが、現時点においては(1)から(5)の完璧な実現を求めるのではなく、利便性、セキュリティ、コストメリットをバランスよく享受できるクラウドサービスの利用が現実的と考えられる。

具体的には、(3)についてはサービス提供事業者が資産を保有することが必須条件、(5)①については推奨条件、(4)および(5)②については事業者側の提供要件として将来の実現を目指すのが当面ふさわしい。

### 1.3 教育クラウドが想定するアプリケーション

教育分野におけるクラウドは公教育のステークホルダーが利用するアプリケーションとして、業務支援(授業・学習支援、教育委員会事務・校務支援)、情報共有・情報提供・コミュニケーション、ICT マネジメント、学校経営等の機能を提供する。

以下に、教育クラウドによる提供が想定される具体的なアプリケーション名を例示する。



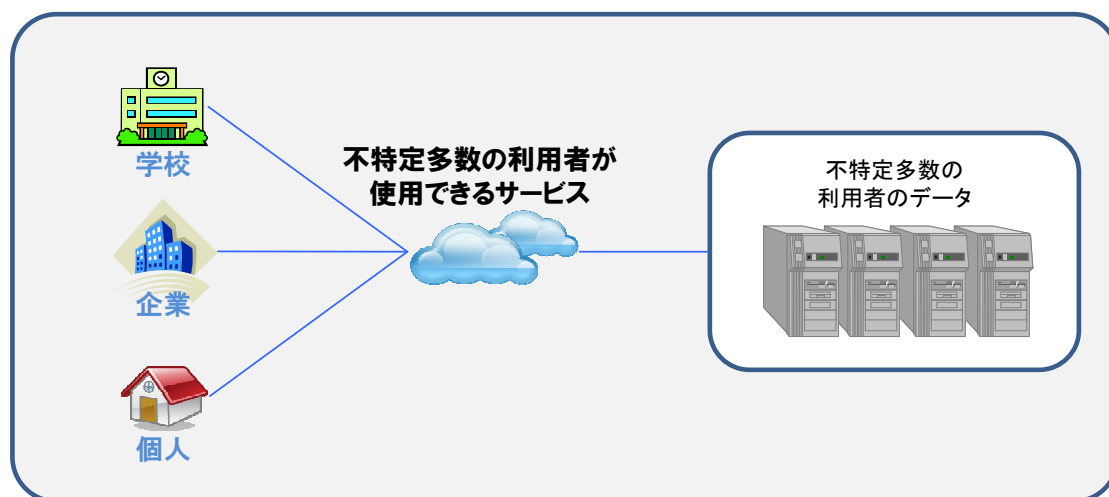
これらのアプリケーションで利用するデータには保護を要する広義の「センシティブデータ」(以下「センシティブデータ」と略する)が数多く存在する。それらの情報項目を抽出し、どのようにクラウド上に配置し保護するかについて、基本方針を事前に検討することが必要である。

### 1.4 クラウドの配置モデル

クラウドを運営する企業の多くは、サービスの継続性はもちろん、セキュリティ対策にも最大限の配慮をしているものの、不特定多数のユーザでサーバを共有するというクラウドに不安を感じる場合もある。しかし、クラウドの配置モデルによっていくつかの形態があるため、センシティブ情報の有無、個人情報保護審査会の意向を鑑み、利用するクラウドサービスによって使い分けることを推奨する。

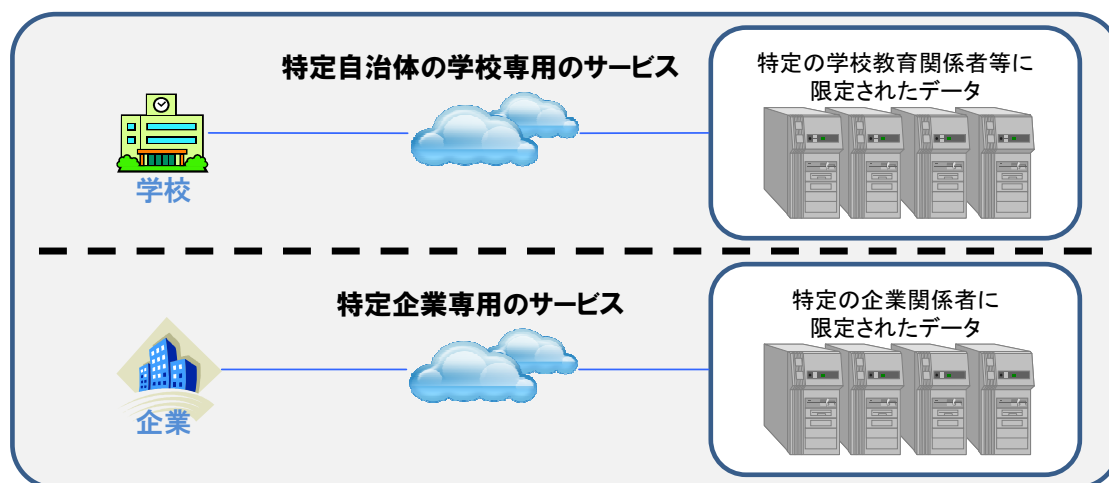
**a. パブリッククラウド:**

一般ユーザや企業等の不特定多数の産業体が利用可能であり、クラウドサービスを提供する組織により所有されるクラウド基盤。



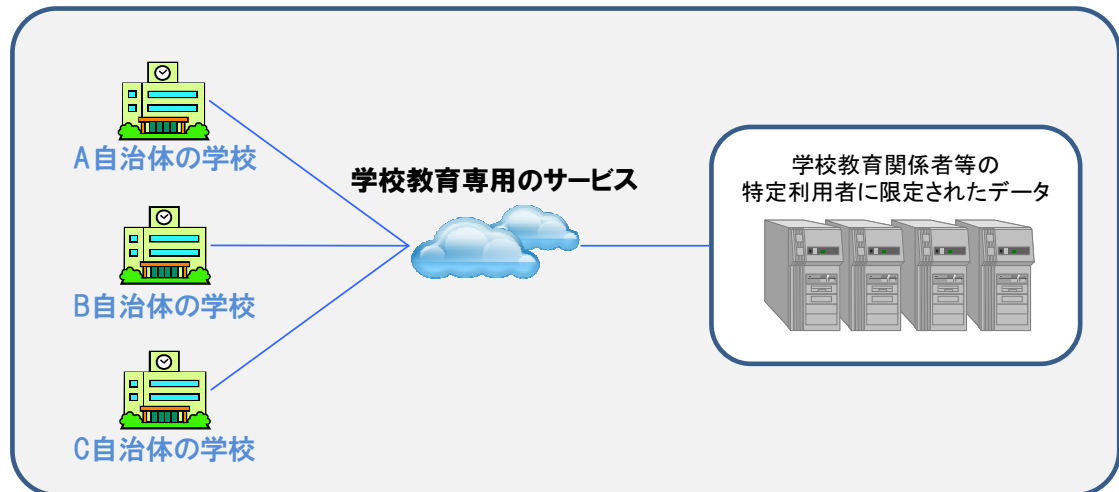
**b. プライベートクラウド:**

単一の特定組織によって運用されるクラウド基盤である。その特定組織あるいは第三者によって管理され、自社運用型と他社運用型がある。



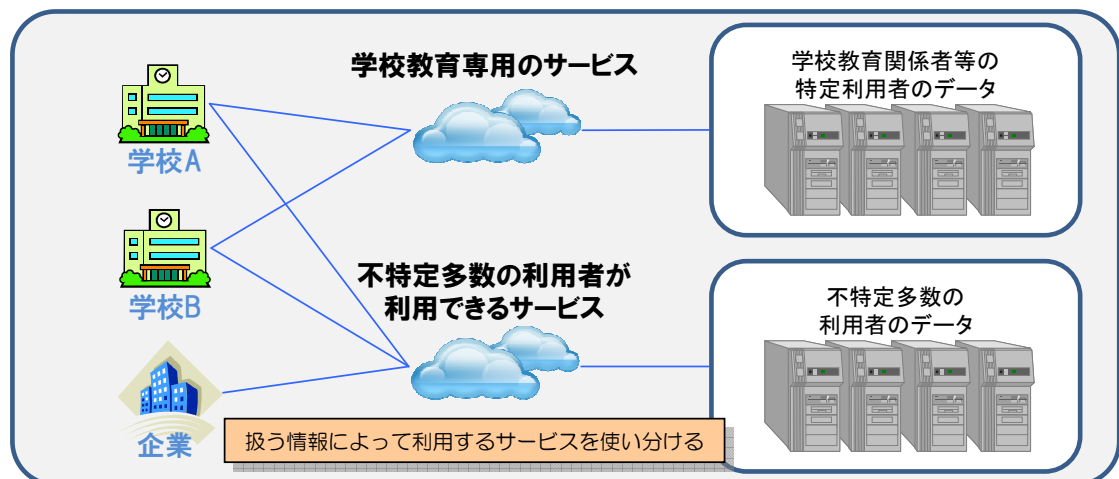
c. コミュニティクラウド:

複数の組織により共用されるクラウド基盤である。共通した利害関係(ミッション、セキュリティ要件、ポリシー、コンプライアンス検討)を持つ特定コミュニティをサポートするクラウド基盤。その組織群あるいは第三者によって管理され、自社運用型と他社運用型が存在する。



d. ハイブリッドクラウド:

2つ以上のクラウド(プライベート、コミュニティ、パブリック)サービスから構成されるクラウド基盤である。

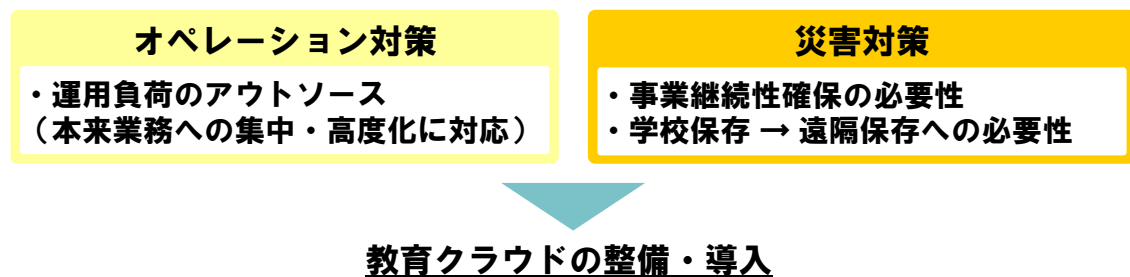


センシティブ情報を含む場合は、プライベートクラウド又はコミュニティクラウド、非センシティブ情報のみの場合は、パブリッククラウド、といった利用コストを鑑みた組み合わせを検討することが望ましい。しかしながら、クラウドサービスの信頼性、機密性は、上記の配置モデルで決まるものではなく、提供サービス内容、契約内容、提供事業者の信頼性によるものである。

## 1.5 クラウド利用の必要性とメリット

近年、ICTの利用環境は更に高度になっていく反面、利用者側にも高度な技術スキルを有する専門スタッフを必要とするなど管理・運用負担は無視できない問題となっている。また、震災を契機に公的データ(教育分野では指導要録や児童生徒の情報等)の電子化および保管や自治体業務の継続性確保が重要視されており、クラウドを上手く利用することでこれらの問題を解決できる可能性がある。

### ■教育情報化での課題

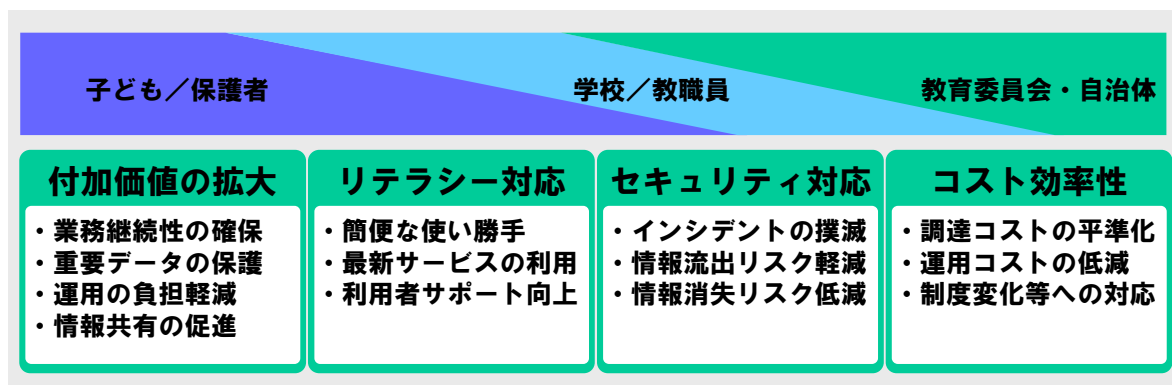


上記以外でクラウドを利用するメリットは、直接的には以下の2点が考えられる。

- ① ICT 整備に関するコストを複数の自治体・教育委員会で分担すること、あるいは設備や利用状況の効率化で、一自治体あたりの整備に必要なコストの低廉化が期待でき、既利用者がある場合はサービス運用に則ることで利活用を円滑に推進しやすい。
- ② 情報システムをデータセンターに集中化することで、システムの運用や資産管理なども集約することが可能となり、利用自治体・教育委員会の ICT マネジメントの負担を軽減し、全体的なセキュリティレベルの向上も期待できる。

また、クラウドのシステム構成やサービス内容にもよるが、以下のメリットも期待できる。システムの共同運用を企画する際あるいは事業者がクラウドを提供する際は、このようなメリットが享受できるようにすべきである。

- ① 個人情報や私物 PC や USB 等に保存して持ち出すことに起因する情報漏えい等は、ユーザーカル環境にデータを保存、複写できないようにする仕組みを利用可能とすることで防止できる。
- ② 予算の執行にあたり、サーバ等のハードウェアの製造、設置、設定等に要する時間を短縮し、必要なサービスを迅速に利用できる



一方、教育クラウドを整備する際には、以下の課題がある。

- ・ 独自の業務運用が行われている場合の業務標準化等の対処検討
- ・ 実利用に制約が生じないようレスポンスや故障修理時の対応など、サービスレベルの設定

## 2. 教育クラウドの整備

---

### 2.1 想定する整備シナリオ

#### 1) 事前検討・利用条件

- ・ 自治体、教育委員会の定める個人情報保護／セキュリティポリシーの観点から、クラウド利用の可能性と範囲を確認する。
- ・ 回線、ネットワーク等の利用環境調査を行い、クラウド利用の可否を確認すると共に調達範囲と予算を確定する。

#### 2) 調達プロセス

##### (1) 調達仕様の提示

- ・ 調達にあたり、まずは自治体・教育委員会から要求される機能やサービスの品質などを調達仕様書として提示することとなる。調達仕様書の提示にあたっては、業務の遂行に求められるサービスの品質を確認することが必要であり、不必要に高いサービス品質を要求するとその分利用料金に反映されることに留意する必要がある。

##### (2) サービス仕様・SLA の評価

- ・ サービス仕様はサービスの具体的な内容を定義したものであり、具体的に提供されるシステムや機能、運用にあたっての作業などが記載されたものである。
- ・ サービスの選択にあたっては、サービス仕様が調達仕様書に示した要件を満たしているかを確認するとともに、提案内容に調達仕様書に記載されていない優れたサービスや提案が含まれている場合の取扱いについて検討しておく必要がある。
- ・ SLA (Service Level Agreement) とはサービスを利用する際に、客観的にサービス品質を把握し、適正な運用管理を行うために事前に取り決めるものである。SLA の締結にあたってはコスト、実効性、責任範囲に注意することが必要である。

##### (3) 事業者の安全・信頼性評価

- ・ 自治体・教育委員会が事業者を評価選定するにあたり、参考とすべき既存の指針(報告書)などとして、7章に参考文献をまとめた。

##### (4) 契約の締結

- ・ 単一の事業者が単独でサービスを提供するもののほか、複数の事業者のサービスを組み合わせて一つのサービスとして提供するものもある。また、クラウドの利用にあたっては、クラウド事業者の他にもネットワーク事業者など様々な者が関係してくる。例えば、サービスに障害が発生した際の責任の所在などを明らかにするためには、契約の相手方であるクラウド事業者の責任範囲や関係各者との責任分界などについて、事前に十分に

確認しておく必要がある。

## 2.2 整備計画の策定

住民サービス向上や行政運営効率化などを目的として、自治体では総合的な情報化計画が策定されている。本書で扱う教育クラウドについても、全体の最適化を図るため情報化計画の中で明確に位置づけるべきである。教育クラウド整備で実現すること、その実現時期を明らかにし、実現に向けた予算化や環境整備、推進体制づくりを適切に実施していく必要がある。このような整備計画の策定作業を情報政策部門、教育委員会が連携して進めることによって、予算や要員等を効果的に配分することが可能となり、自治体全体でのセキュリティの維持、住民サービス向上などを図ることも期待できる。

## 2.3 推進計画

教育クラウド整備に関する体制として、導入を検討・実施する体制と運用を検討・実施する体制が必要となる。

### 1) 導入検討体制

- ・ 主体は教育委員会の ICT 施設整備部門および学校教育部門が考えられる。
- ・ 関与者としては、教育委員会外の部門として、
  - 情報企画部門: 全庁のセキュリティポリシーや情報システムの運用に関する内容
  - 総務広報部門: 個人情報保護に関する内容
  - 財務部門: サービス調達等に関わる内容などが考えられる。

### 2) 運用実施体制

以下 3 種の体制の相互調整を行う統括会議体

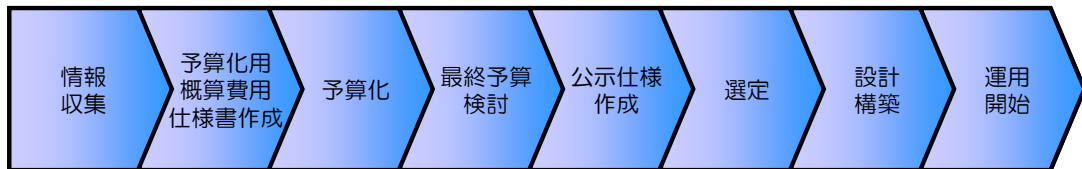
- ・ システム全体に関わる運用体制:  
教育委員会の ICT 施設整備部門および学校教育部門、第三者組織として情報企画部門等による監査を行う。
- ・ 校務などアプリケーションの運用改善に関わる体制:  
教育委員会の ICT 施設整備部門および学校教育部門に加え、学校現場の教育・事務・保健・給食等の代表者によるアプリケーションシステムの運用改善を検討する。
- ・ 学校でのシステム運用および情報セキュリティ管理に関わる体制:  
校長を学校 CIO とし、CIO 補佐官とともに学校の構成員すべてによる、システム運用及び情報セキュリティ管理の体制。特に情報セキュリティ管理に関しては、導入時の情報



資産棚卸、通常時の監査体制や緊急時のエスカレーションを実施する。

### 3) スケジュール

教育クラウド整備にあたり、予算化から導入までのイベントを示す。



#### (1) 情報収集

- ・ 文部科学省等の指針や見解等の情報収集
- ・ クラウド導入状況調査(他自治体利用状況、製品／サービス調査)
- ・ クラウド導入／運用に係る概算金額調査
- ・ 予算化
- ・ 概算費用をもとにした「仕様書」を作成し、財政部門との折衝、予算申請を行うケースもある。
- ・ 導入計画案作成
- ・ 予算申請

#### (2) 仕様検討／仕様書作成／選定

- ・ 調達対象・方法の記述
  - サービス調達に関連する規程整備など
- ・ アプリケーションに関する規定／選定
  - 帳票の取り扱いに関する文部科学省見解等の紹介
  - 業務の標準化の検討
  - 導入サービスの選定
    - 例) - 要求仕様を満たしているかどうか
    - 誰もが利用しやすい環境(使いやすい操作性)になっているか
    - システム／サービス間のデータ連携ができるか
- ・ セキュリティに関する規定
  - ネットワーク(LGWAN、VPC など)
  - データセンター(個人情報管理)
  - セキュリティ運用ルール(サーバ・NW、クライアントPC など)

#### (3) 導入

- ・ 導入スケジュール策定

- ・ 仕様書に基づく要件の確認

#### (4) 運用(マネジメント)

- ・ 管理者／利用者教育(研修)
- ・ 利活用サポート体制整備(ヘルプデスク、ICT 支援員等)
- ・ 継続的な活用事例の収集と運用の改善

また、教育クラウドの整備スケジュールを策定するにあたり、先行導入や段階的導入を実施し利用者の負担軽減を図ることも検討すべきである。

- ・ 先行的にモデル校に導入し、運用方法・ルールなどを検討
- ・ クラウドサービスの利用を段階的にすすめ、ICT 利活用促進策を検討

## 2.4 セキュリティに関する検討

クラウドサービスを利用するにあたり、センシティブデータの取り扱いを中心にセキュリティ対策を検討する必要がある。個人情報保護条例、自治体セキュリティポリシー、教育委員会のセキュリティポリシーとの整合を鑑み、どの範囲まで外部のクラウドサービスを利用するのかを検討する。場合によっては、セキュリティポリシーの見直しを行うことが必要になる。

## 2.5 利活用支援の検討項目

教育クラウドを整備もしくは、クラウドサービスを利用するにあたっては、これまでのシステム運用のように資産を有し運用管理するか否かは、コストを考える上で重要なポイントとなる。

公共施設を考えると、PFI という手法がある。我が国では、「民間資金等の活用による公共施設等の整備等の促進に関する法律」(PFI 法)が平成 11 年 7 月に制定され、平成 12 年 3 月に PFI の理念とその実現のための方法を示す「基本方針」が、民間資金等活用事業推進委員会(PFI 推進委員会)の議を経て、内閣総理大臣によって策定され、PFI 事業の枠組みが設けられた。PFI (Private Finance Initiative: プライベート・ファイナンス・イニシアティブ)とは、公共施設等の建設、維持管理、運営等を民間の資金、経営能力及び技術的能力を活用して行う手法である。PFI 事業では、民間事業者の経営上のノウハウや技術的能力を活用でき、また、事業全体のリスク管理が効率的に行われることや、設計・建設・維持管理・運営の全部又は一部を一体的に扱うことによる事業コストの削減が期待できる。これらにより、コストの削減、質の高い公共サービスの提供が期待され、現在、多くの公共施設がこの方式で建築、運営されている。

この PFI とは異なるが、サービス調達を行なうと、資産を持たず質の高いサービスを受け、管内のユーザにそのサービスを提供することが可能となる。

サービス調達におけるサービスの提供とは、物品(ハードウェア、ソフトウェア)ではなく、例えば、

1,000 人の教職員がグループウェアでメールを利用したいといったユーザ業務を提供することになる。調達されると、教職員には 1,000 人分のコンピュータシステムが配布され、サーバ類も設置運用されるが、これらは調達者側の資産ではなく、サービス提供者が有する資産で、ユーザである教職員は、それらで提供されるサービスを利用することになる。物品調達の場合は、機器構成表などを提供することになるが、サービス調達の場合はサービスカタログを提供することになる。

サービスカタログは、サービスを受けるユーザに、利用できるサービスは何かを明確に提示し、提供されるサービスを定義するものである。サービスカタログには通常、サービス名称や内容、特徴、適用範囲、連絡窓口や責任の所在、制約事項(サービスレベル範囲、提供時間など)などが記述される。

## 2.6 サービスレベル (SLA) の検討

近年、情報システムに関する業務の外部委託が増加するにつれ、情報システムの調達者からは「期待していた内容や品質のサービスがなかなか提供されない」という不満が、また、サービス提供者からは「仕様書や契約に含まれない過剰な要求をされる」という不満がよく聞かれる。これは、業務、サービス内容、提供範囲、サービス品質、料金体系等に関して、調達者とサービス提供者間の認識が異なることが大きな原因となっている。これらは問題が表面化して初めて認識の相違が明らかになり、トラブルへと発展する例が数多くみられる。このように、調達者とサービス提供者の間で認識のすれ違いが生じる要因は、そもそも形のある製品とは異なり、サービスはその評価を行うことがなかなか難しいにもかかわらず、契約の段階で業務の重要度・必要度に応じたサービスの内容や水準(レベル)が明確化されてないことにある。それに加えて、担当者それぞれによる思い込みや、担当者間の打合せの席での口約束、その内容の理解の違いなどがある。たとえ文書化されていたとしても、曖昧な表現で、双方が良いように判断していることなどにあると考えられる。

このような問題を避けるために、サービスレベルを明確に決めることが必要となる。サービスは、形のある製品に比べて内容が分かりづらく、特に長期間提供されるサービスの場合、「最初はよかったが、だんだんサービスの品質が悪くなった」「いい場合もあれば、悪い場合もある」といったことが多々ある。そこで、サービスレベルを数値によって明示し、定量的に定義することで、役割と責任の所在について“曖昧さ”を排除し、ルールを定めておくのが SLA(service level agreement: サービスレベル アグリーメント)である。

## 2.7 クラウド運用の検討

校務支援システムなどのクラウド運用にあたっては、下記 5 つの観点を十分に配慮しながらクラウド運用を行い、業務の標準化や段階的な運用計画を踏まえながら推進していくことが望ましい。

### (1) 情報セキュリティの確保

児童・生徒名簿や成績など個人情報等のセキュリティ確保は十分に考慮する必要がある。電子化により情報の一元管理や情報共有によるデータの有効活用ができるようになった反面、不特定多数からのデータの閲覧や個人情報を含むデータの持出が可能になるなどの懸念事項もでてきている。こういった面に対処するために、情報セキュリティの確保を下記の観点から十分に配慮する必要があるが、一方で運用のしやすさやコスト面にも関連してくるため、それらのバランスを保ちながら運用する必要がある。

- システム利用者に応じたセキュリティ確保
  - ✓ ID、パスワードによる利用者ごとの権限に応じたデータアクセス
  - ✓ 盗難や紛失の可能性のあるデバイスや周辺機器との接続防止
- クラウド環境における情報漏えいやデータ改ざんの防止

### (2) 業務の効率化・標準化、事業継続性の確保

クラウド運用のメリットとして、システムの標準化にあわせて業務の標準化や帳票等の統一化を行うことで、教職員の事務処理等の作業の効率化が可能となる。例えば学校現場では、今まで培ってきた各種帳票が散在するが、それを集約しパッケージ標準の帳票形式に近づけることでコスト効率化をはかることができる。また、クラウドセンターでは、耐震性やデータ保管の安全性が高いため、災害時等におけるデータ保管や公文書等の安全なバックアップなどの事業継続性を確保できることもメリットの 1 つと言える。

- 校務の情報化による業務環境の統一
  - ✓ 運用ルールの見直しによる各種事務の効率化と負荷軽減
  - ✓ 文書のデジタル化による作業の効率化
  - ✓ 各種帳票の統一化や標準化によるコスト効率化
- 指導要録や健康診断表等の公文書の安全な保管
  - ✓ 災害時等を含む事業継続性の確保
  - ✓ バックアップなどの安全なデータ保管

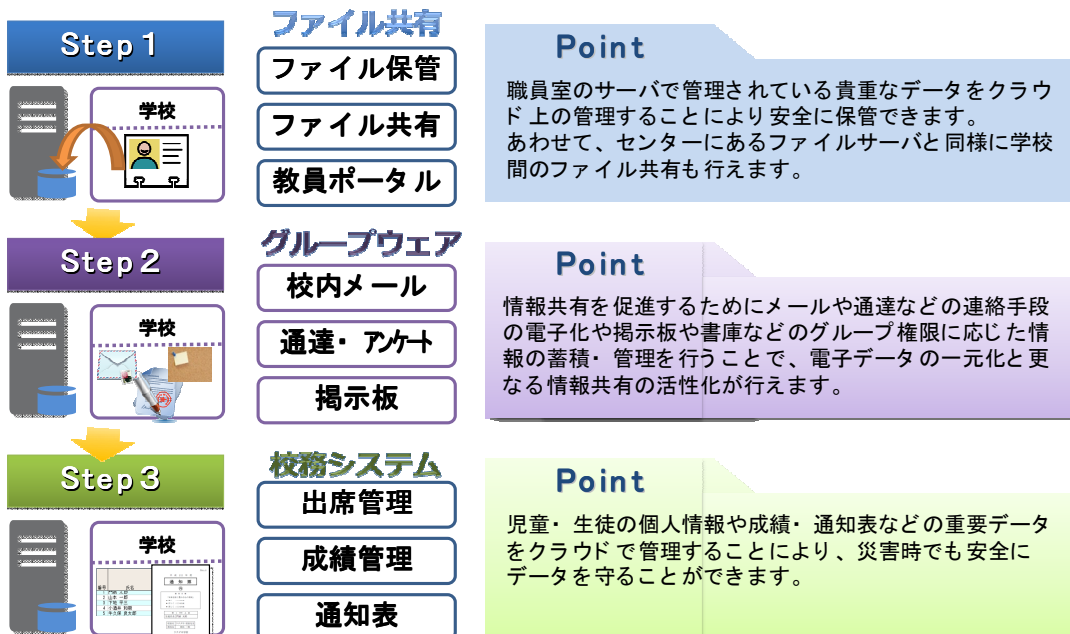
### (3) 段階を踏んだ運用計画

クラウド環境のメリットとして、機能単位のアプリケーション導入や CPU・メモリ・HDD 処理能力を用途に応じて拡張することなど学校の校務等の需要に合わせてクラウド環境を増設可能な仕組みを提供できる。その特性を利用し、クラウド運用にあたっては、はじめから 100%運用を目指すのではなく優先順位が高いものから段階に応じて普及させる方法や、モデル校スタートにより成果や効果、課題等を確認した上で段階的に全校に導入する方法などが実現できる。

- 段階的な校務支援システムの導入・運用
- モデル校スタートによる成果や効果、課題等の明確化

- 繁忙期や閑散期などに合わせたクラウド運用
- 終焉やシステム移行に伴う、データ移行や消去

## クラウド運用計画(例) ～段階的な活用推進～



### (4) ユーザ研修

クラウド環境を利用したユーザ研修では、クラウドを利用した即時性のある、かつ再利用可能な研修のほか、ICT 支援員の活用や集合研修等、現地でのユーザ研修も合わせたフォローアップを定期的 to 実施し、運用定着へ向けての予算措置等を鑑みながら利活用推進を実施していくことが望ましい。

- クラウド環境を利用したユーザ研修
  - ✓ e-Learning、オンラインマニュアル(動画等)
  - ✓ Web 会議、SNS などによる問合せや情報共有
- 現地でのユーザ研修
  - ✓ 訪問支援 (ICT 支援員)
  - ✓ 集合研修 (導入研修会、ステップアップ研修会・・・etc.)

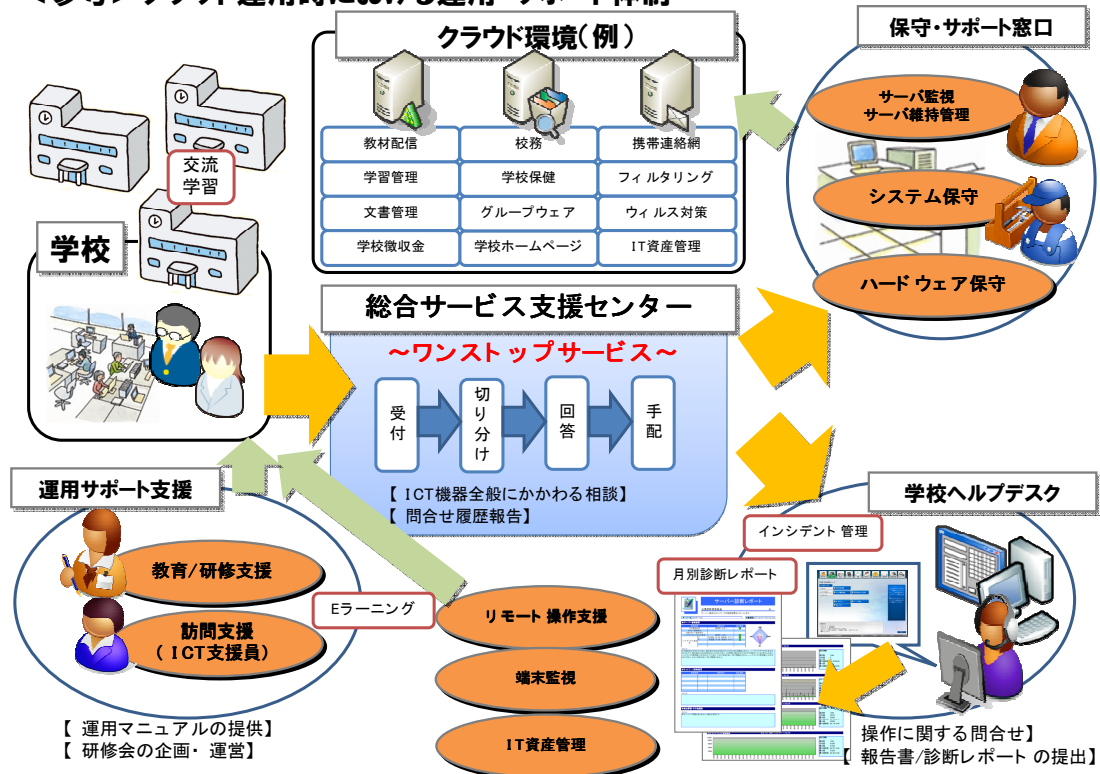
### (5) 運用・サポート体制

教員の負担感を軽減するため情報を一元管理するサポート体制を構築するとともに、サーバやクライアント PC を安全かつ最適な状態で維持・管理していくことが必要である。

- 窓口の一元化による情報の集約と、質問内容の切分けや進捗状況の管理を行うワンストップサービスの提供
- クラウドサーバを安全かつ最適な状態で保持するための仕組み

- ✓ サーバの監視を常時実施し、サーバの攻撃や情報漏えいなどを防止
- ✓ 個人情報や成績・通知表などの重要データを安全に保管
- クライアント PC を最適な問題なく維持管理
  - ✓ ウィルス対策など最新の状態で保持
  - ✓ IT 資産管理

### ＜参考＞クラウド運用時における運用・サポート体制



## 2.8 参考文献

- ◆ 日本教育工学振興会 (JAPET) <http://www.japet.or.jp/>
  - ・「校務情報化の現状と今後の在り方に関する研究」  
<http://www2.japet.or.jp/komuict/>
  - ・「パンフレット:校務の情報化を推進しよう！」  
[http://www2.japet.or.jp/komuict/dl\\_pamphlet.html](http://www2.japet.or.jp/komuict/dl_pamphlet.html)
- ◆ 総務省、特定非営利活動法人 ASP・SaaS・クラウド コンソーシアム (ASPIC)
  - ・「校務分野における ASP・SaaS 事業者向けガイドライン」  
[http://www.soumu.go.jp/menu\\_news/s-news/01ryutsu02\\_01000004.html](http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_01000004.html)

## 3. セキュリティ

---

### 3.1 教育クラウドにおけるセキュリティ

#### 3.1.1 概要

クラウドコンピューティング利用の最大のメリットは、システム機器の管理やアプリケーションの運用、そしてセキュリティ対策等の多くの部分を、サービス提供側に集約できることにあり、サービス利用者(教育クラウドの場合、多くは教職員)は、多くのシステム知識習得と管理労力から解放されることにある。

一般的な「情報システムのセキュリティ」については、さまざまな研究成果や調査報告が発表されているが、多くは非常に広い範囲のセキュリティ、とくに情報分類と使用される技術に関して記述される事が多い。また、本来、セキュリティは、利用する団体の特性と所有する情報資産により、考慮すべき点や対応策も異なるが、これらの、広範な要因（アプリケーション、サーバ・クライアントPCのOS、ネットワーク、利用者のセキュリティモラル、運用管理、ウィルス、セキュリティ事故発生時の対応、情報の分類等）に対する記述の多さと、さまざまな技術用語が、各団体(特に、セキュリティ専門技術員を置くことができない団体)で情報セキュリティポリシーの策定や、情報システムの構築、利用者への教育、セキュリティ事故発生時の対応等の障壁となっていることが多い。

しかし、実際のクラウドコンピューティングにおいては、サービス利用者が、情報システムで起こりうる全てのセキュリティ事故の詳細やその対策、対抗技術を深く理解する必要はなく、自分が関与する部分についてのモラルと知識を持てば、セキュリティリスクをある程度低減させることができる。

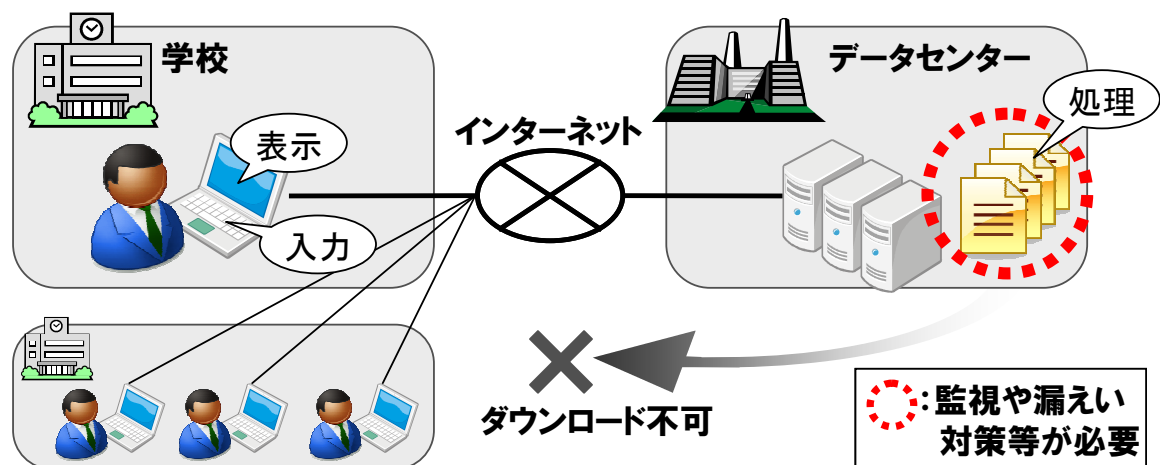
本ガイドブックでは、なるべく教育クラウドの構築と利用を行う上での考え方や、留意点に限定して記述することにより、クラウド利用上のセキュリティの理解を容易にしたい。

#### 3.1.2 基本的な考え方

クラウドサービスのセキュリティは、「どのようなデータ」が、「実際にどこで」、「誰によって」処理されるかによって、設計と対策の容易度が、かわってくる。

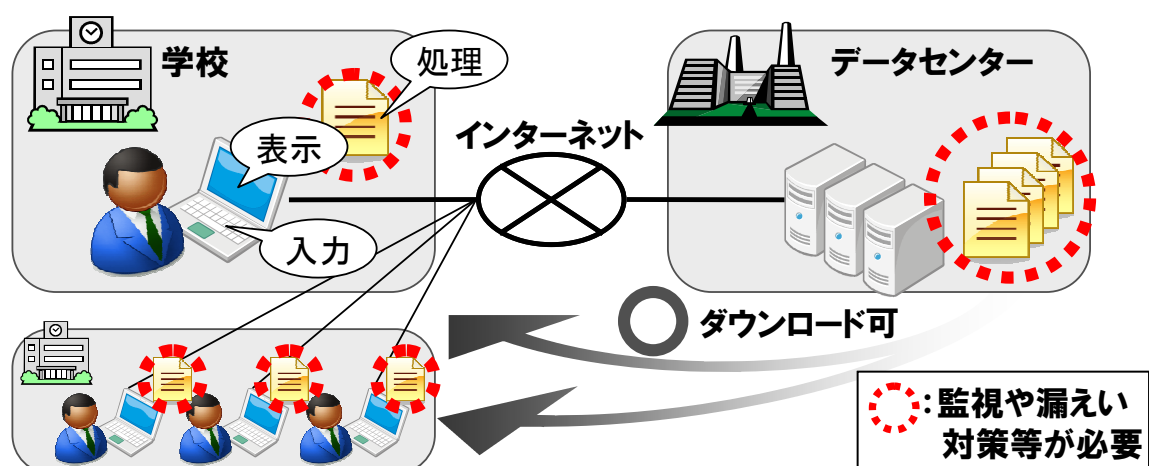
##### ◆ 例1

- ・ 利用者はクラウドに Web 経由でアクセスする
- ・ センシティブデータは、全てクラウドのサーバ上で処理
- ・ 利用者はデータの閲覧と操作は行えるが、クライアント PC へのダウンロード、コピーはできない



◆ 例 2

- ・ 利用者はクラウドに Web 経由でアクセスする
- ・ センシティブデータは、クラウドのサーバ上で処理
- ・ 利用者は、クライアント PC へのデータダウンロードもコピーも可能



例 1 と例 2 の違いは、クライアント PC へのデータのダウンロードができるかどうかでしかないが、例 2 では、「センシティブデータ」を、「利用者のクライアント PC」で、「利用者」によって処理できている。

例 2 の場合、利用者は、「情報漏えい(盗難、メディアでの持ち出し、紛失)」、「コンピュータのウィルス対策(マルウェア、OS/アプリのセキュリティパッチ)」、「クライアント PC の物理セキュリティ(盗難、紛失)」、「情報の再利用規定(センシティブデータの取り扱い)」について理解し、利用者自身が十分な対策を実施する必要がある。

つまり、例 2 のようなクラウドサービスは、利用者(教職員)への十分なセキュリティ教育が行われていなければならない、途端に管理負荷が増えることになる。また、「センシティブデータ」の実体がネットワーク上を通過することから、通信経路(校内 LAN や WAN)の暗号化は、より強固なものが



必須となる。

決して良い事とは言えないが、例1でデータセンター側のウィルス対策や外部からの攻撃耐性が確実なものであれば、教職員のクライアントPCがウィルス感染しても、サーバ側に感染する経路がないため、システムへの影響は微細なものになる。

このように、センシティブデータの実体を、なるべく教育クラウドのサービス側(通常はデータセンター)に集約することで、クライアントPCサイドからの情報持ち出しや、クライアントPC盗難等でのセキュリティ事故は、起きる可能性が非常に低くなるといえる。

加えて、例1、例2ともに、クラウドサービス提供側における外部からの攻撃や不正アクセスに対する対策は必要であるが、数か所のデータセンターサイドでの集中したセキュリティ対策／管理と、多数の学校と教職員への対策では、費用と労力に大きな差がある。

すなわち、教育クラウドのセキュリティを考える場合、クラウドサービスの提供者と、サービスの利用者で分割し、利用者(クライアントPC)側が、保持(処理)できる実データを減らすことで、全体のセキュリティ設計の労力と費用を削減することができる。

なお、実データがクライアントPC上に存在しないというのは、ファイルやデータベースのクエリーのような、実体のあるデータの固まりで存在しないだけであり、クライアントPCのWeb画面上では、閲覧編集が可能であるべきである。

また、セキュリティを設計するうえで、「セキュリティ強度とコストと利便性」のバランスは、非常に難しい。コストに関しては、初期導入コストだけではなく、監視とセキュリティ事故対応のための運用コストも含まれる。

たとえば、パスワード漏えいに対する対策として、定期的なパスワード変更がある。

- ・ 3か月に1回の変更では不安な担当者が、週に1回のパスワード変更ポリシーを設定すると、一見セキュリティ強度が高くなり、コストへの影響も少なく見えるが、当然、利用者の利便性は下がり、パスワードを覚えられない利用者がパスワードを付箋紙でPCにはるという、本末転倒な事態も起こりえる。
- ・ OneTimePassword(OTP)を導入すれば、毎回パスワードが異なるため、漏えいの危険性は下がり、利便性への影響も少ないが、コストはその分上がることになる。(ただし、OTPの導入により、リモートアクセスが利用できるようになれば、コストと利便性は相殺されるとも考えられる。)

これらバランスを、データの重要度と、漏えい時の影響で勘案する必要があるが、各団体での基本ポリシーの違いもあり、設計が難しくなっている。また、どのくらいでパスワード変更すれば、漏えい事故にならないのかは、定期的にログを解析する必要があるが、そのためには、管理用のログ機材と、解析のためのコストが発生する。

以上のようなセキュリティに対する不安と設計の難しさが、ICT導入の妨げになることもあるが、「どのようなデータ」が、「実際にどこで」、「誰によって」処理されるか、を整理することが大事である。

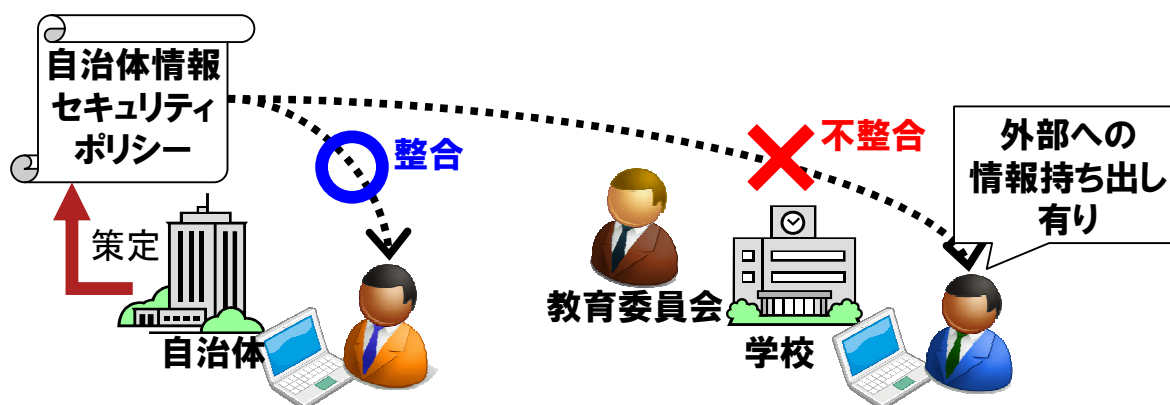
## 3.2 セキュリティポリシー

### 3.2.1 概要

情報セキュリティポリシーに基づいたセキュリティ対策の実施を徹底するためには、情報セキュリティポリシーに記載されている対策が業務実態に即していることが不可欠である。（総務省「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」参照のこと。）

既に、多くの自治体において、情報セキュリティポリシーが策定されており、各自治体の教育委員会は自治体の情報セキュリティポリシーの適用範囲内となっているケースが見られる。

しかし、自治体・教育委員会の情報セキュリティポリシーは、自治体の一般職員の業務を中心に記載されており、学校教職員の業務実態に即した内容となっていない場合がある。



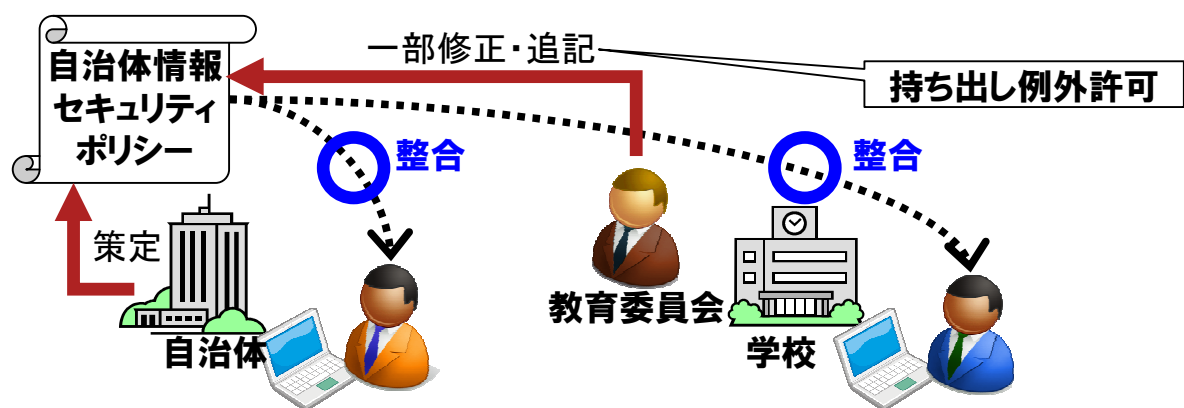
上記のような理由から、教育クラウドの利用形態や管理主体を考慮し、自治体の情報セキュリティポリシーを一部改訂した上で準拠する、または教育委員会で新たに情報セキュリティポリシーを策定するといった対応が必要となる。

### 3.2.2 セキュリティポリシーの適用パターン

#### (1) 既存の自治体策定の情報セキュリティポリシーに準拠する場合

自治体クラウドの一部を利用する場合や、教育クラウドを自治体が主管する場合は、既存の自治体情報セキュリティポリシーに準拠することが考えられる。自治体情報セキュリティポリシーの記載と学校教職員の業務実態に乖離がある部分については、例外的に学校教職員が実施すべき対策を追記する等の工夫が必要である。

また、既存の記載内容への追記にあたっては、自治体情報セキュリティポリシーの主管課や文書法務課等、関係組織に対し十分調整を行う必要がある。



(2) 教育委員会独自の情報セキュリティポリシーを策定する場合

教育委員会にて独自に教育クラウドを構築・管理する場合は、情報セキュリティポリシーについても独自で策定することが望ましい。この場合は、既存の自治体情報セキュリティポリシーに加え、以下のような公的機関によるガイドライン等が参考文献として有効である。

- ・財団法人 コンピュータ教育開発センター「学校情報セキュリティポリシー策定・運用のための学校情報セキュリティ・ハンドブック解説書」

また、策定にあたっては、既存の自治体情報セキュリティポリシーや個人情報保護条例等、他の規程との齟齬が発生しないよう、関係組織に対し十分調整を行う必要がある。



### 3.3 セキュリティに関する検討事項

#### 3.3.1 不正アクセス対策

不正アクセスを防止するためには、ファイアウォール、プロキシサーバ、データ/ネットワークの暗号化、認証技術による利用者確認、不正侵入検知システム(IDS) 等さまざまなシステムへの対策についての検討が必要である。

このようなシステムへの対策を実施するためには、インターネットに接続する情報システム機器やクラウドサービスを含む Web アプリケーション等の調達にあたって、十分なセキュリティ要件を設定し、これを実現するための機能を有する製品を選定する必要がある。(セキュリティ要件の設定にあたっては、総務省「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」、財団法人地方自治情報センター「地方公共団体における情報システムセキュリティ要求仕様モデルプラン(Web アプリケーション)」参考のこと。)

また、前述のような脅威への対策だけでなく、日々発見されるセキュリティホールに対する対策が必要である。これについては、OS やミドルウェアの脆弱性のセキュリティ診断を、納入時だけでなく保守等のタイミングで継続的かつ定期的の実施し、セキュリティパッチの適用を行う必要がある。

セキュリティ診断については、公的セキュリティ認証や第三者によるセキュリティ診断結果を活用することも推奨する。

ただし、セキュリティパッチの適用にあたっては、作業によってシステムの継続利用に支障がないよう、サービス提供事業者と十分協議した上で作業を実施する必要がある。

#### 3.3.2 データセンターのセキュリティ

データセンターではシステムを稼働させるための基盤(サーバ、CPU、ストレージ等)に関するサービスをネットワーク経由で受けることができる、ハードウェアのメンテナンスや障害対応等もすべて任せることができるといった利点がある。

これに加え、セキュリティ対策や事業継続の観点におけるデータセンター利用のメリットも大きい。データセンターは設置されるシステムの保護に特化した建物であるため、入退室管理や機密性等、物理的対策が強固な構造となっており、震災や火災、水害等の災害対策や有事の際の非常時電源対策等、庁舎や校舎にはない安全性を確保することが可能である。

このようなデータセンター利用のメリットを最大限に得るためには、教育クラウドの選定にあたって、以下のような項目について検討することが望ましい。なお、記載していない項目の洗い出しについては、「IaaS・PaaS の安全・信頼性に係る情報開示指針」(総務省)等も参考にできる。

主たる検討項目	検討内容例
サーバの保守	定期保守の頻度、間隔
耐震対策	施設の耐震等級、設置機器の転倒対策
入退室管理	データセンターの入退室管理
監視	設置場所の監視方法
床面耐荷重	フロアの積載荷重
電源	非常時電源対策

これらのサービスを利用する場合には利用前に設置場所へ赴き、要求した仕様や条件に合致しているか確認することが望ましい。またセンシティブデータを保存するデータセンターは、日本国内に存在することが望ましい。これは、サーバが設置されている国の法規制が適用されることから、データセンター事業者、またはその利用者が訴訟や捜査の対象になった際に、捜査機関によるサーバの差し押えが発生し、預託したデータの機密性、可用性が損なわれる可能性があるためである。このようなリスクは事前に回避しておくことが望ましい。

### 3.3.3 サーバ、システム設計における情報セキュリティ

サーバのシステム設計を行う場合、いくつかの面から検討を行う必要があるが、サーバの不正アクセスやウィルス対策等は、クラウドサービスでも通常のサーバ同様に、OS、アプリケーションへのセキュリティ対策は必須となる。

また、アプリケーションのサービス提供を受ける場合、ユーザで利用できる機能の範囲を明確にし、アクセスできる情報への制限をかける必要がある。併せて、管理者権限を誰が保有するかといった検討も必要である。

主たる検討項目	検討内容例
利用するアプリケーション	利用者毎に利用できる機能や画面の範囲
利用権限	利用者に与える登録、更新、閲覧の権限の範囲
管理者権限	管理者権限の制限

#### (1) 仮想化による問題

クラウドシステムの場合、サーバは仮想化されることが通常であり、1台の物理サーバで、複数の仮想サーバとして動作したり、逆に複数の物理サーバで1台の仮想サーバとして動作する。複数の物理サーバが、別のデータセンターに存在しながらクラウドサービスを提供している可能性もあるため、教育クラウドのデータが、どの範囲のサーバを利用しているのか（データがどこで処理されているのか）を把握しておく必要がある。

#### (2) サーバの物理的なセキュリティ

通常、データセンターは入退室管理の仕組みを有している。クラウドモデルでは、データセンター内に出入りする要員が複数存在するが、どのような人物が出入りするのかを管理し、どのような場合であってもサーバが物理的に保全される必要がある。

#### (3) サーバ管理上のセキュリティ

サーバの管理者であっても、データに容易にアクセスすることは望ましくない。サーバへ管理者としてのログインにも管理者個人を特定するための認証をかけることや、別のサーバでアクセスログを管理する仕組みとなっていることが望ましい。

### 3.3.4 ネットワークのセキュリティ

教育クラウドにおけるネットワークには、データセンター、教育委員会、学校、それらをつなぐ WAN 回線等がある。

センシティブデータの取り扱いにあたっては、すべての場所で暗号化されていれば、確かに安全性は高まるが、暗号化には(ハードウェア処理にしても)処理遅延が発生することを考慮しなければならない。この処理遅延によって、教育クラウドの使い勝手が悪くなるようでは、教育クラウド利用目的が十分果たされているとは言えない。処理遅延を最小限に止めるために、暗号化すべき箇所、暗号化以外のセキュリティ対策によるカバー等を検討する必要がある。

#### (1) データセンター内

データセンター内のサーバ間接続の場合、データセンターの物理的なセキュリティや、外部からの攻撃に対するセキュリティ対策が十分であれば、暗号化の必要性は低くなり、膨大なデータのやり取りに暗号化遅延が影響することもなくなる。

#### (2) WAN 回線

WAN 回線と学校内のネットワークは、関係者以外が介在する可能性が高いため、必要に応じて暗号化が必要になる。

この場合、暗号化・復号を繰り返さない設計とすることが、レスポンスの良い教育クラウドを構築するにあたって重要なポイントとなる。校務支援についていえば、WAN 回線のみの暗号化ではなく、データセンターの出口で暗号化し、教職員の利用するクライアント PC で復号できれば、遅延は最小に抑えられ、なおかつセキュリティリスクも低減することができる。

このように、セキュリティについては、局部的に技術を導入するのではなく、データの流れと脅威の有無によって、対策をとることが有効になる。

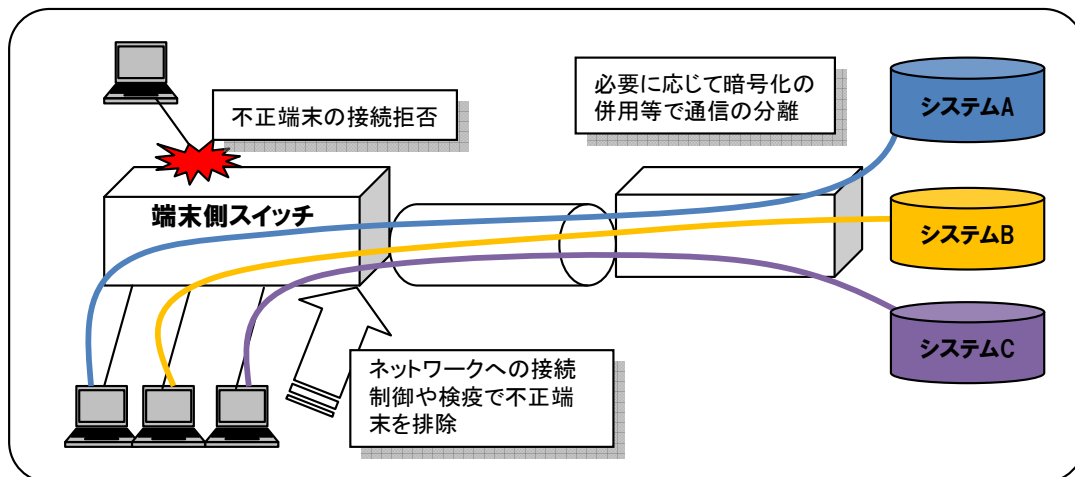
#### (3) LAN(学校内・教育委員会内)

学校内の LAN の利用においても、様々なセキュリティレベルのシステム情報が LAN を利

用するため、ネットワーク(トラフィック)の分離は必須要件となる。

たとえば、児童生徒が利用する教育コンテンツ、センシティブデータを扱う校務支援システム、会計システム(必要に応じて PTA への開放や、災害時の避難場所となった場合の災害情報等)である。

LANは実際のデータを保持するわけではないため、LAN 設計で注意すべき点は、盗聴と侵入であり、技術的には、LAN 内でのトラフィック分離と LAN への接続セキュリティとなる。



トラフィックの分離技術には多くの方式が存在するが、利用頻度の高い VLAN (IEEE802.1Q) の場合、ネットワーク機器で論理的な分離はしているが、流れているデータは加工されていないため、経路にあるネットワーク機器に接続できれば、盗聴は容易である。

ただし、ネットワーク機器への接続セキュリティ(LAN 接続認証や検疫ネットワーク)と組み合わせ合わせた場合は、侵入の危険度を下げることができ、なおかつ盗聴に対する耐性も高くなるため、十分な運用に耐えるようになる。

現在、業務用に販売されているネットワーク機器では、接続のセキュリティを高めるための技術(標準規定であれば IEEE802.1X 等)が搭載されている物も多い。これらを考慮して設計された LAN であれば、校内のどこからでも、各種データの取り扱いが可能になり、利便性も向上する。

#### (4) 無線 LAN

学校内では、無線 LAN の利用で利便性の向上が図れることも多いが、LAN の項でも述べたように、盗聴と侵入に対する不安から、無線 LAN はセキュリティ上問題があるという認識が現在でも存在している。

しかし、現在の無線 LAN では、解読に時間のかかる暗号化と認証の組み合わせにより、セキュリティを考慮しない設定の有線 LAN より安全性は向上している。接続認証と暗号化については、IPA 等の最新の情報を参照し、その時点で安全といわれる組み合わせを選択す

べきである。(IPA「無線 LAN 利用環境のための運用上のセキュリティ対策」(<http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/411.html>) 参照のこと。)

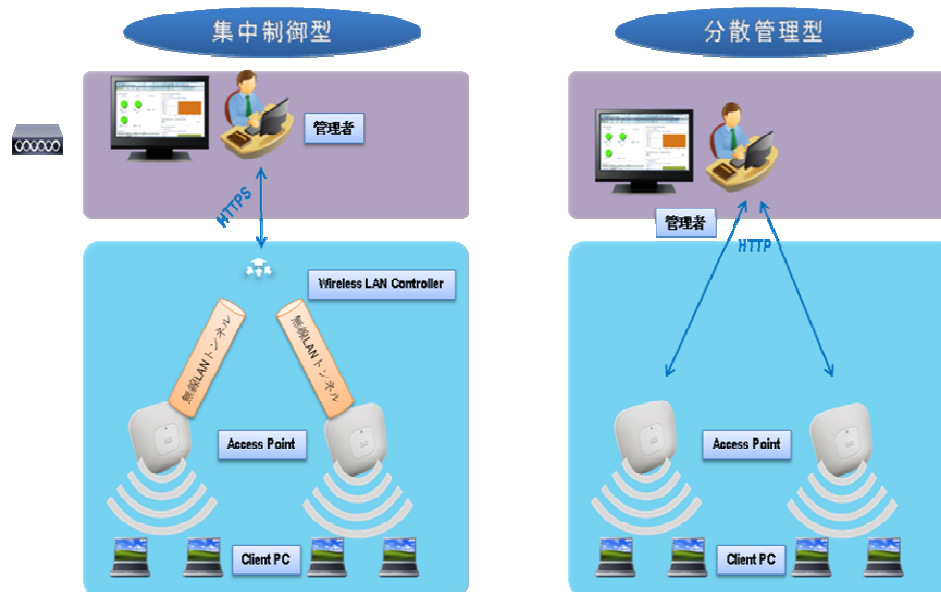
本ガイド記述時点では、接続認証では IEEE802.1X、暗号化は WPA2-PSK(AES)以上を推奨する。重要なデータを利用するクライアント PC においては、電子証明書や OTP (OneTimePaaword)の同時利用を推奨する。

暗号化利用についての注意としては、アクセスポイントが、指定する暗号方式に対応したハードウェアを搭載して、通信速度の低下を招かないようにすることである。

また、無線 LAN の課題としては、情報システム利用者が、管理者の許可を得ずに設置する不正アクセスポイントが、大きな問題となる。情報漏えいや侵入のセキュリティ事故は、十分なセキュリティ対策を行わない無線アクセスポイントを不注意に設置したことにより、発生することが多く、システム管理者も、管理外の機器のため、発見が遅れることも多い。

これらに対する対策も考慮した設計を行うべきである。

現在販売されている無線 LAN のタイプには、個別のアクセスポイントを設定して設置するものと、集中管理サーバで無線の設定や認証を管理するものがある。



企業等では、多数のアクセスポイントを、運用する必要があるが、分離型アクセスポイント設置でおきる、設定ミス、接続認証変更時の作業負荷、セキュリティ事故発生時のログ管理等も煩雑になり、結果的に運用コストが高くなることから、集中管理型を利用することが多くなっている。集中管理により認証方法や暗号キー管理や、設定の一括変更で、セキュリティを向上しており、不正アクセスポイントの発見機能を持つものもある。

教育クラウドを利用するネットワークにおいても、セキュリティポリシーの統一運用や、セキュリティ事故の早期発見、故障機器の交換の負荷軽減の面で有効である。



### 3.3.5 クライアント PC のセキュリティ

3.1 でも述べたが、センシティブデータの実体(ファイルやデータの固まりでの保存)をクライアント PC で取り扱うかどうか、クライアント PC のサーバへのアクセス形態によって、クライアント PC に求められるセキュリティは異なってくる。

教育クラウドを構築するに当たっては、なるべくクライアント PC で、実データの取り扱いを、行わないことを推奨する。

実データの取り扱いをしないとしても、クライアント PC においては、本人認証と、ネットワークへのアクセス認証は、確実に実施する。

#### (1) 本人認証

クラウドサービスにアクセスする場合には、利用者を個別管理する必要があり、また、本人であることを確認するための認証を行う必要がある。教育クラウドのサービス利用者に求められる、セキュリティ要素として最重要となるのが、本人認証情報の秘匿管理である。どのような堅牢なシステムを構築しても、ID とパスワードの流用や流出があれば、利用者詐称は防ぎきれない。この点は、利用者のモラル教育が絶対に必要であり、運用ポリシーの罰則等の規程も求められる。

本人認証方式を決定する上で、ID とパスワードの組み合わせだけでは、他人に知られた場合、簡単に不正アクセスされてしまうため、本人確認としては不十分となることがある。とくにリモートアクセス等、場所やクライアント PC の限定等で、セキュリティを担保できない場合である。

その場合、物理的な認証(USB トークンや IC カード等)、生体認証(指紋、静脈等)等と、組み合わせることにより、パスワードを知られた場合や、物理的な認証キーを落とした場合でも対策をとる時間を得ることができる。

また、利用者の個人認証ではなく、クライアント PC 等の機器自体に電子証明書を組み込むことで、教育クラウドにアクセスする認証の精度は、さらに高まる。

ただし、ユーザがログインする際に認証の手間が増えることと、導入コストが上がることを考慮し、検討を行うことが望ましく、認証の組み合わせは、教育クラウド利用のセキュリティリスクと、相対させることも有効である。

例えば、部屋の入口にセキュリティロックがあり、部外者のアクセスの可能性が低い、教育委員会の執務室であれば、クライアント PC に証明書を入れた上で、ID、パスワード認証で接続可能とする等である(この場合、最初の証明書インストールの手間だけで、通常業務では、入力の手間は増えない)。

学校のネットワークに、本人認証を基にしたアクセス制御を入れることで、無許可のクライアント PC 経由でのアクセスも防ぐことが可能になる。

また、本人認証は、利用する各システム(自治体システム、教育クラウド、教育用コンテンツ等)毎に ID、パスワードが異なる可能性があり、アクセスするシステムが多数の場合に、管

理が複雑になり、結果 ID、パスワードを PC にメモしたり、テキストファイルで保存したりすることのないよう注意が必要になる。

このような場合は統合認証システム等を利用して、シングルサインオンを可能にできると、利用者の利便性は高まる。

### 3.3.6 データ持ち出しに関するセキュリティ

教育クラウドのリモート利用が可能になる以前では、校務は教職員のクライアント PC 上でのデータ処理が主であり、自宅等での業務継続には、データを何らかの形で持ち出す必要があった。しかし、データ持ち出しによる、データ紛失、自宅 PC からのウィルス感染等、セキュリティのリスクは非常に高まる。これは、「3.1.3 セキュリティの基本的な考え」で述べた、“「どのようなデータ」が、「実際にどこで」、「誰によって」処理されるか”において、“実データが、自宅 PC 等で、教職員により処理される”ため、発生している。

自宅 PC 等、管理すべきクライアント PC 数の増大や、管理の徹底が実施しにくいことから、データの持ち出しは行うべきではなく、持ち出しをしなくてもシステムを操作できるように教育クラウドを設計するべきである。

それでも、データの持ち出しを許可する場合、

- ・ 自宅 PC のアンチウィルスが最新であるかのチェック機能
- ・ 持ち出しする媒体(USB や DVD 等のメディア)が紛失や盗難にあっても容易に解読できないように暗号化されているか
- ・ 個人メールアドレスへデータ転送される場合に、必ず暗号化しているかのチェック

上記のようなチェック機構が、必須となり、導入すべきセキュリティシステム機器やアプリケーションが増え、それに伴い、管理コストも増大する。

#### (1) 出力データ

多くの校務支援システムは、表計算用データや印刷用帳票の出力機能を利用できる。そのため出力されるセンシティブデータは、出力内容、保存場所の制限等の取り扱いに配慮するべきである。

クライアント PC サイドでセンシティブデータの一括印刷が可能となれば、印刷物は情報システムの手を離れて、それ以降を管理することは不可能になってしまうためである。クライアント PC で印刷可能な情報は、サービス利用者の権限で閲覧できる情報内で、印刷物にしても影響範囲が限定されるように、規定する。

教育クラウドを利用しながら、学校のプリンターでの印刷を行う場合、プリントサーバ機能を使用することで可能になる。その場合、本人が物理的にプリンターまで行って ID カードや ID 認証を入力して印刷するような本人認証の組み合わせを利用することで、印刷物の混在や盗み見からの情報漏えい等は、防ぐことができる。

### 3.3.7 リモートアクセス

クラウドサービスを自宅等組織外(校外)から利用する場合は「どのようなデータ」が、「実際にどこで」、「誰によって」処理されるかを明確にする。

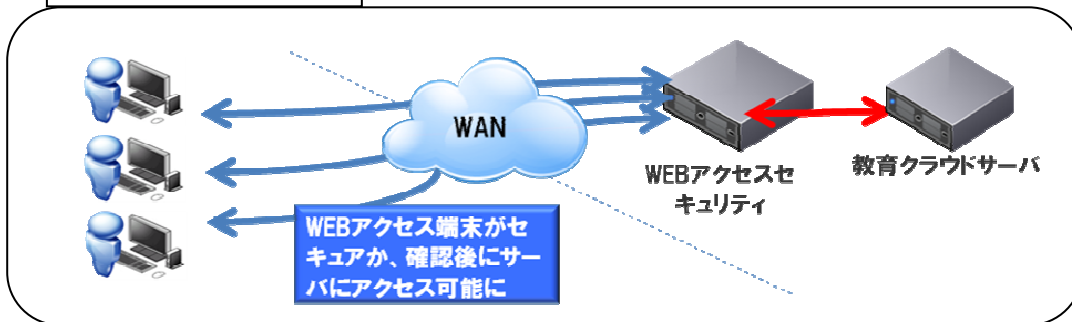
「3.3.6 データ持ち出しに関するセキュリティ」でも記述したが、実データが自宅 PC 上で処理されるのは、管理すべきクライアント PC の台数やクライアント PC の種類の事情からも、セキュリティの維持には不向きである。なるべくクラウドのセンター側でデータ処理を行い、リモートアクセスに使用する機器は Web の画面としての操作や、シンクライアントの画面操作に限定するほうが、セキュリティを維持しやすい。

Web 接続でアクセスを許可する場合は、センター側で攻撃に対応するための Web アクセスセキュリティ機器の設置を行うべきである。また、リモート接続してくる機器自体の安全性を確認する場合は、リモート接続してきた機器をまずは隔離セグメントに接続し、クライアント PC の OS のセキュリティパッチ、アンチウイルスソフトのバージョン、セキュリティ設定を確認し、規定されたレベルに達していると判断できた場合に、その先のシステムへの接続を許可する機能等が有効である。

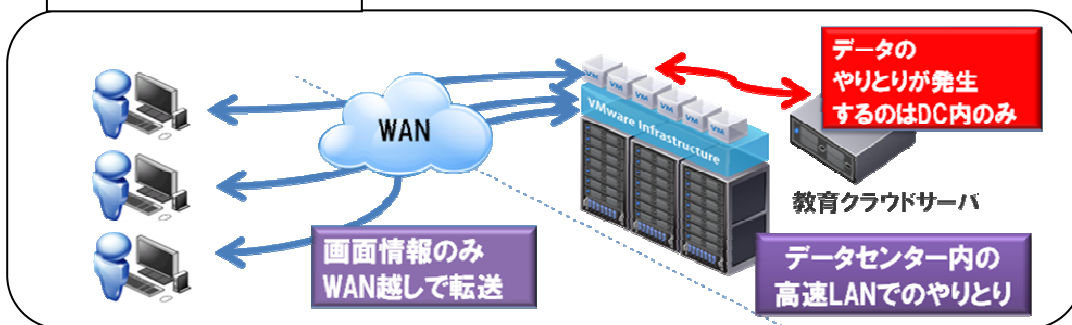
シンクライアントには、いくつかの種類があるが、VDI(Virtual Desktop Infrastructure)の場合、教育クラウド側に、教職員のクライアント PC の代替となる仮想端末(実際はデスクトップ OS)があり、リモートアクセスする自宅 PC は、この仮想端末の画面とキー入力を操作することで、教育クラウドを利用する形態になる。

仮想端末が実際の教育クラウドの処理を行い、仮想端末とリモート端末との間では、画面データとキー入力データのみが、やり取りされるため、リモート端末からのウィルスやメール等の実データのやり取りは、発生せず、セキュリティの管理機器を削減することができる。

#### Web によるアクセス



#### VDI によるアクセス



### 3.3.8 サービス事業者のセキュリティ要件

教育クラウドの整備にあたっては、サービス事業者への委託が前提となる。しかし近年、自治体・教育委員会において、情報システムのサービス事業者（委託事業者）による情報漏えい事件が後を絶たない。システムだけでなく、これを提供するサービス事業者についても、セキュリティ要件を十分検討し、管理する必要がある。

総務省『「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書』においては、委託事業者の管理における以下のような枠組みが提示されている。

- ・ 要件の伝達
- ・ 委託事業者の選定
- ・ 委託事業者との契約
- ・ 実施状況の確認

教育クラウドにおけるセキュリティレベルの確保においても、これらの観点に基づいてサービス事業者を管理することが有効である。

#### (1) 要件の伝達

サービス事業者の選定に先立つ情報収集、調達仕様書や入札説明会等においては、セキュリティ要件の明確化と伝達が重要である。学校が保有する様々なセンシティブデータの

取り扱い等を明示し、サービス事業者がセキュリティ要件を十分理解した上で提案できるよう、情報提供を行う必要がある。

## (2) 委託事業者の選定

利用するクラウドサービスを提供するサービス事業者が安心・安全にサービスを供給できるかという点は、サービス事業者選定における重要な基準の一つとなる。特に、最初に契約を締結する前は、サービスの提供に対して日頃どのような対策を実施している事業者かわからないことが多い。そのため、公的な認証を取得しているかを確認することにより、求めるサービスが安心・安全なものか事前にある程度確認できる。クラウドサービスに関係する公的認証には次のようなものがあげられる。

名称	対象	内容
ISO27001 (ISMS)	セキュリティ対策	組織においてセキュリティ対策を維持する仕組みを構築し、維持しているか。
ISO20000 (ITSMS)	IT サービスマネジメント	組織が顧客の求める品質レベルの IT サービスを安定的に供給する仕組みを構築し、維持しているか。
プライバシーマーク	個人情報	組織が個人情報を基準に沿って適切に取り扱っているか。

利用するクラウドサービス、保存する情報の範囲等を踏まえて検討し、選定基準として考慮することが望まれる。

## (3) 委託事業者との契約

選定したサービス事業者との契約にあたっては、業務を処理する場所や業務従事者の特定、データの適切な管理、再委託の制限について、書面にて取り決めを取り交わすことが望まれる。

## (4) 実施状況の確認

利用中でも引き続きシステムが安全・安心に利用できるものなのか、監査を行い確認することが望まれる。

監査の実施にあたっては、ユーザが実施することだけでなく、利害関係のない第三の事業者にも委託することも考えられる。特に次の表における技術的な監査については、地方公共団体自ら実施できる態勢を整備していることは少ないといえる。

分類		実施内容
運用面の監査		契約書、仕様書、自らの情報セキュリティポリシー等に基づき、システムの運用がされているか、聞き取り調査、現物確認、等により実施。
技術的な監査	ネットワーク脆弱性検査	外部からの様々な脅威を想定し、サーバやネットワーク機器等に対し実際に攻撃を行うことで、不正アクセスやサービス停止の脆弱性がないかを確認。
	Web アプリケーション検査	利用している Web ページ(ホームページ等)に対して実際に攻撃を行うことで、不正アクセスやサービス停止の脆弱性がないかを確認。

### 3.3.9 セキュリティ研修

情報セキュリティポリシーによってセキュリティに関するルールを取り決め、システム対策によってシステムの脆弱性や外部からの脅威に備えたとしても、ルールやシステムを活用するのはあくまで利用者の学校教職員であり、利用者が正しくルールを遵守し、適切にシステムを利用しなければ、情報漏えいを防ぐことはできない。策定した情報セキュリティポリシー、構築したシステムの利用方法等について、学校教職員に対し、周知徹底する必要がある。

また、管理職である学校長および副校長へのセキュリティ研修にあたっては、自身が遵守すべきセキュリティ対策の学習だけでなく、管理下の一般教職員のセキュリティ対策の実施状況を管理するための視点を研修内容に追加する必要がある。

具体的には、セキュリティに関わる一般教職員からの申請の承認や、情報セキュリティ事故発生時の教育委員会への報告等が挙げられる。この点についても、教育クラウドの仕組みに応じた運用に基づいて、具体的な手順等を含めてわかりやすい教育内容となるよう努める必要がある。

このような研修を効果的に実施するためには、多忙な学校教職員の業務の妨げとならないよう、関係組織と調整の上、予め適切な研修計画を立案することが重要である。

例えば、実施時期については夏季休業等に設定する、実施場所については学校のパソコン教室を利用し、近隣の学校に勤務する教職員を対象に集まってもらい、自席で学習できる e ラーニングシステムを利用する等の工夫が有効である。

### 3.3.10 学校現場のセキュリティ監査

教育クラウドの利用にあたっては、学校現場における情報漏えいの可能性もあることから、自治

体・教育委員会が学校に対し定期的に情報セキュリティ監査を行い、運用面においてもセキュリティ対策が十分に実施されていることを確認するのが望ましい。

### 3.4 参考文献

◆内閣官房情報セキュリティセンター(NISC) <http://www.nisc.go.jp/index.html>

情報セキュリティ政策の基本戦略を決定し遂行するため、機関省庁の横断的なセキュリティ基準の作成等を行っている機関。教育クラウドへの直接の関係は少ないが、文部科学省や総務省等、監督官庁のセキュリティに関して参考となる。

◆独立行政法人情報処理推進機構(IPA) <http://www.ipa.go.jp/>

セキュリティを含む ICT に関する多くの情報を提供している。図表を多用し、参照しやすいものが多い。

- ・「クラウドコンピューティングのセキュリティその意味と社会的重要性の考察」

<http://www.ipa.go.jp/about/technicalwatch/20120424.html>

クラウドコンピューティングのセキュリティ全般についてのレポート「2. クラウドコンピューティングのセキュリティに関する主たる関心事」、「6. IPA におけるクラウドコンピューティングのセキュリティへの取り組みの今後の方向性」等は、プライベートクラウドを構築する場合や、クラウド業者を選定するときの参考となる。また、セキュリティ監査のポイントの参考資料としても有効である。

- ・「2012 年版 10 大脅威 変化・増大する脅威！」

<http://www.ipa.go.jp/security/vuln/10threats2012.html>

世の中でどのようなセキュリティ事故が起きているかの最新レポート。

インシデントの傾向を把握して、何に注意してセキュリティ設計を行うかの参考となる。

- ・「情報漏えい発生時の対応ポイント」

<http://www.ipa.go.jp/security/awareness/johorouei/>

教育クラウドでも、もっとも起こりえる「情報漏えい」が発生した場合の対応のポイントが記載されている。情報漏えい時に何を行うべきかを取り決める参考になる。

◆日本教育工学振興会(JAPET) <http://www.japet.or.jp/>

教育情報システム等について、教育現場の視点の研究資料を多数掲載している。

- ・「ICT教育環境整備ハンドブック」2012 年版

[http://www.japet.or.jp/jo12yfxe8-475/#\\_475](http://www.japet.or.jp/jo12yfxe8-475/#_475)

教育現場での ICT 利用全般についての資料である。

◆財団法人コンピュータ教育開発センター(CEC) <http://www.cec.or.jp/CEC/>

・「学校情報セキュリティ・ハンドブック改訂版」解説書

<http://www.cec.or.jp/seculib/index.html>

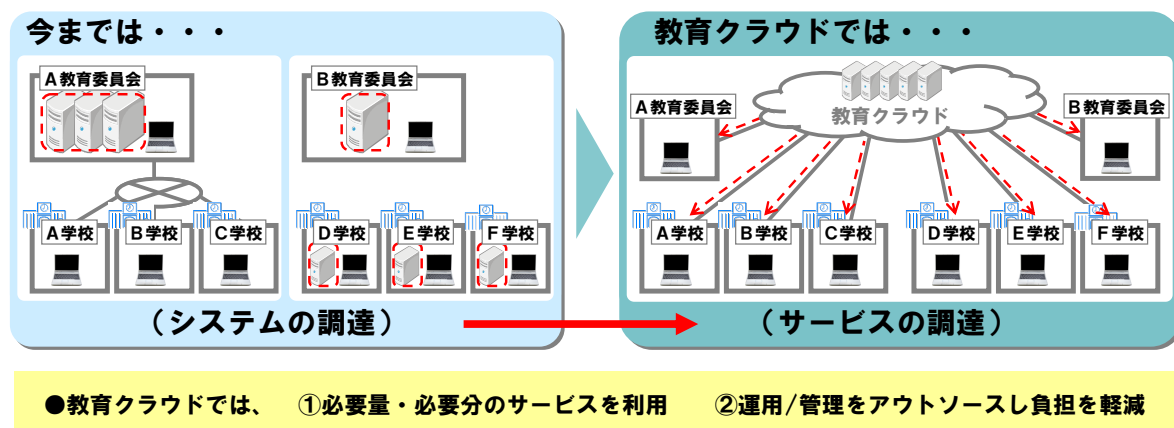
平成 18 年版のため、技術情報については更新が必要となるが、情報資産の洗い出し方法やフォーマット等の参考資料として有効であり、作業の効率化が図れる。



## 4. サービス調達

### 4.1 サービス調達

教育クラウドを整備もしくは、クラウドサービスを利用するにあたっては、これまでのシステム運用のように資産を有し運用管理するか否かは、コストを考える上で重要なポイントとなる。



サービス調達におけるサービスの提供とは、物品（ハードウェア、ソフトウェア）ではなく、例えば、1,000 人の教職員がグループウェアでメールを利用したいといったユーザ業務を提供することになる。調達されると、教職員には 1,000 人分のコンピュータシステムが配布され、サーバ類も設置運用されるが、これらは調達者側の資産ではなく、サービス提供者が有する資産で、ユーザである教職員は提供されるサービスを利用することになる。物品調達の場合は、機器構成表などを提供することになるが、サービス調達の場合はサービスカタログを提供することになる。

サービスカタログは、サービスを受けるユーザに、利用できるサービスは何かを明確に提示し、提供されるサービスを定義するものである。サービスカタログには通常、サービス名称や内容、特徴、適用範囲、連絡窓口や責任の所在、制約事項（サービスレベル範囲、提供時間など）などが記述される。

参考記述例：

上記の例に挙げた 1,000 人の教職員がグループウェアでメールを利用したいといったユーザ業務の場合、実現するには様々な機能が必要となるが、その中にフィルタリングサービスが含まれることが考えられる。その一つのウィルス対策では、以下のような内容が記される。サービスカタログには機能ごとに一覧で記載されることになる。

機能(サービス)名称	ウィルス対策
概要	専用アプライアンスにより高速で透過的なウィルス・スパイウェア対策を、負荷分散を行なって耐障害性に優れたサービスを提供します。
詳細	アンチウィルス製品と連携することで、プロキシサーバを経由するトラフィック上のウィルスやワーム等に感染した Web サイトへの接続をブロックします。
サービス利用者	教育委員会事務局、常勤職員、非常勤職員、児童生徒
サービス提供範囲	教育系ネットワーク、図書館、児童館
サービス提供時間	24 時間／365 日

サービスの提供形式には、SaaS のようなマルチテナント型や、個別アウトソース型(プライベートクラウド)などが考えられ、複数の方式の組み合わせもある。これらのサービス調達のメリットとしては以下の 4 つが考えられる。

- ・ 費用対効果が出しやすい
- ・ 業務に即した仕様書が作成できる(システムの詳細な知識は不要)
- ・ セキュリティ対策
- ・ 機器の構成や製品のバージョン等を把握する必要がない

## 4.2 サービスレベル

ここで取り上げるサービスレベルは、サービス提供者から調達者に対して提供されるサービスのレベルであり、サービスの可用性や納期など利用者の立場から意味のある項目で評価される。また、サービスレベルを評価する際には、客観的で制御・測定が可能であり、調達者とサービス提供者の間で合意できる内容を定義する。

独立行政法人情報処理推進機構の「情報システムに係る政府調達へのSLA導入ガイドライン」には以下のような例が記載されている。

例えば、次のような要件を持つシステムがあると仮定する。

- ① 利用者に対して、1日あたり24時間・365日、提供者が運用するサーバから、オンラインでサービスを行う必要がある
- ② 利用者の業務上の必要性から、利用者が操作してからシステムが応答するまでの時間(応答時間)は、3秒以内である必要がある
- ③ 前日の入力を夜間にバッチ処理し、委託者が指定する場所に、毎日朝9時までに帳票を届ける必要がある

このような場合、それぞれの要件に対して、次のようなサービスレベルを設定することになる。サービスレベル達成に必要なリソースや費用は、システム稼働環境、業務データ量、ピーク時、

ユーザ数等の条件によって異なる可能性が高いので、サービスレベルはこれらの前提条件を明確にした上で設定する必要がある。

① サーバ可用性

予定された稼働時間のうち、どのくらいの間、正常に利用できたかをサービスレベルとして設定する。

例えば、1,000時間の計画稼働時間のうち、1時間だけ、サーバがダウンして、システムが利用できなかった場合には、サーバ可用性は、 $99.9\% \{ (1 - (1/1,000)) \times 100 \}$ となる。

② 基準応答時間達成率

利用者からの操作に対するシステムの応答時間を計測し、そのうち、基準応答時間である3秒以内にどの程度応答できたかを、サービスレベルとして設定する。

例えば、1,000回の操作のうち、2回だけ3秒以上かかったとすると、基準応答時間達成率は、 $99.8\% \{ (1 - (2/1,000)) \times 100 \}$ である。

ただし、端末レベルでの日常的な応答時間の計測が技術的に困難な場合、システムの内部応答時間により代用することができる。

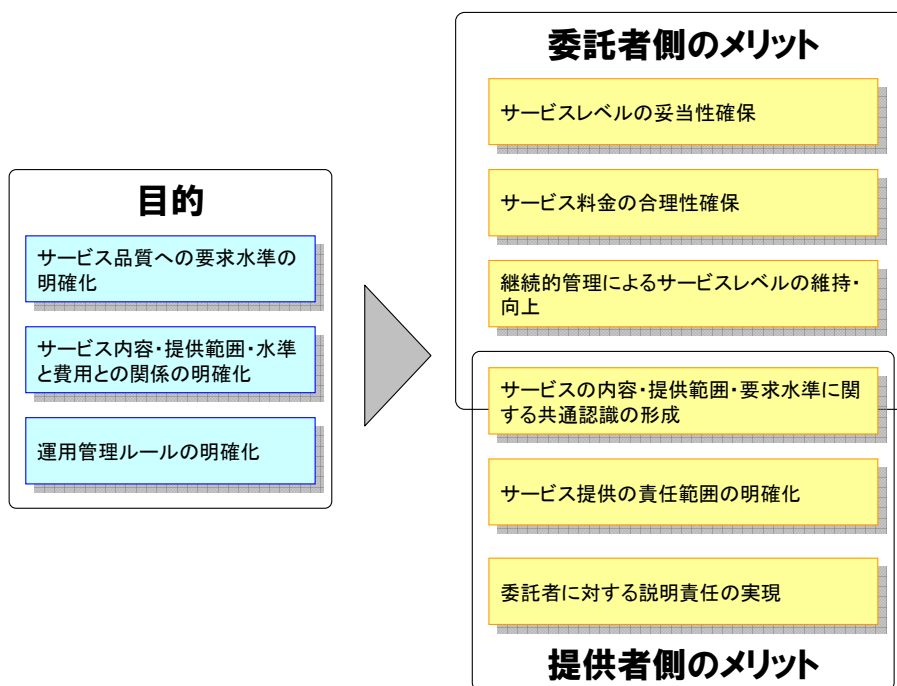
③ 帳票デリバリ時間遵守率

指定された各拠点に対して、内容を間違いなく出力した帳票を、指定時間の午前9時までに配達できた比率を、サービスレベルとして設定する。

例えば、365日のうち、1日だけ守ることができなかった場合は、帳票デリバリ時間遵守率は、 $99.7\% \{ (1 - (1/365)) \times 100 \}$ となる。

SLA によって、調達者にとっては支払いの対価としてどのようなサービスがどれだけ提供されるのかが事前に明確になり、機能とコストのバランスを考慮して適切なサービスを選択することが可能になる。一方、サービス提供者にとっては、事前に想定していなかった“サービス”の要求や、SLA で取り決めた以上の品質を求められることを防ぎ、ビジネスのコスト構造をはっきりさせることができる。

SLA には多くのメリットがあると考えられるが、独立行政法人情報処理推進機構の「情報システムに係る政府調達への SLA 導入ガイドライン」では、下図のようにメリットを示している。共通のメリットとして、調達者とサービス提供者との間の共通認識のもとで、SLM を行うことができるようになる。さらに、調達者側は、適切なサービスレベルを確保することができ、サービス提供者側は、契約したサービスを適切に提供していることを調達者側に説明することができるようになる。



独立行政法人情報処理推進機構：情報システムに係る政府調達へのSLA導入ガイドラインより

図 SLAの目的と委託者・提供者のメリット

SLAは単に契約時に取り交わすばかりではなく、適宜、見直しが必要となる。そのために継続的なモニタリングが大切となる。SLAは最初から調達者側、サービス提供者双方にとって最適な内容とすることは非常に困難であり、定期的に見直すことが望ましい。こうした活動をSLM(service level management: サービスレベル管理)といい、双方の利益の為に必要である。

## 5. アプリケーション毎の特徴と事例

### 5.1 アプリケーション毎の特徴

教育現場において活用されるアプリケーションは、センシティブデータの有無や利活用支援の度合い、運用や SLA 必要性の強弱などにより、前述したクラウドの配置モデルとの親和性が異なる。現時点で保有するアプリケーションのみではなく、将来的に利用を予定しているアプリケーションも含めクラウド整備計画を策定しておくことが望ましい。

【活用アプリケーションとクラウドの種別例】

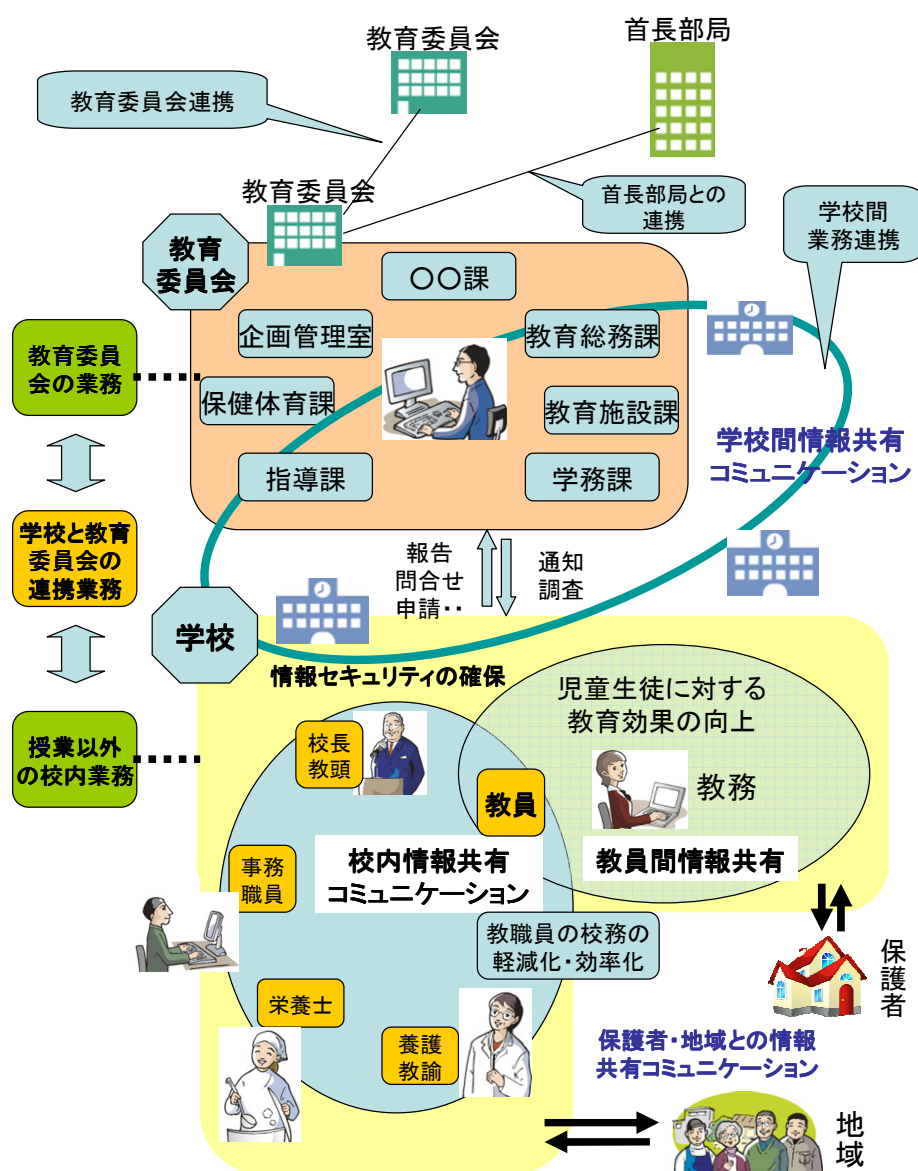
種別	a. パブリッククラウド	b. プライベートクラウド	c. コミュニティクラウド	d. ハイブリッドクラウド
校務支援システム	△	○	○※1	○※1
グループウェア	○	○	○	○
CMS	○	○	○	○
学校連絡網システム	○	△	△	○※2

※1: 参加自治体間の合意が必要

※2: d. ハイブリッドクラウドは a～c の複合形態であることから基本的に全て○となる

### 5.1.1 校務支援システム

校務支援システムの「校務」の定義は、一般社団法人日本教育工学会 (JAPET) が、文部科学省の委嘱研究「校務情報化の現状と今後の在り方に関する調査研究」を基に考えるが、範囲が広いのでここでは、センシティブデータを取り扱う“校務”に関して記述する。



#### (1) クラウドモデル

多くの自治体が個人情報保護には慎重であり、現時点ではパブリッククラウドはかなり難しく、大半がプライベートクラウドとなっている。先進自治体の調査でも、最初からプライベートクラウドを目指したわけではなく、結果的にプライベートクラウドになったというところが少なからずある。

個人情報保護条例、セキュリティポリシーが許せば、宮古島市様の事例のような運用も可能である。

## (2) セキュリティ

サーバを何処に設置するか、クライアント(教職員用コンピュータ)を通常のコンピュータにするか、シンクライアントにするかでセキュリティで検討しなければならないポイントが異なってくる。

### ①サーバ

- ・民間のデータセンターを利用する場合

以下のような項目を検討した上で、データセンターを選定する必要がある。選定に当たっては事業者からの報告だけではなく、設置場所に足を運んで実際に確認することが重要である。

主たる検討項目	検討内容例
サーバの保守	定期保守の頻度、間隔
耐震対策	施設の耐震等級、設置機器の転倒対策
入退室管理	データセンターの入退室管理
監視	設置場所の監視方法
床面耐荷重	フロアの積載荷重
電源	非常時電源対策

- ・自治体・教育委員会内にサーバを設置する場合

上記と基本は同様であるが、民間のデータセンターと同様の基準では難しいと考えられるので、首長部局の情報政策部門と十分な調整が必要となる。

- バックアップサーバを設置(検討)する自治体・教育委員会が増えているが、その場合も検討項目は同じで、設置場所に足を運んで実際に確認することは必要である。

### ②教員用コンピュータ

教員用コンピュータにデータを保存できるようにするか否かで対応は大きく異なる。シンクライアントコンピュータにする場合は、セキュリティの設定は一括での設定が可能となるが、通常のコンピュータの場合は、利用者の協力は必須となるので、セキュリティ研修の徹底が必要となる。

- ・検討項目(i) 出力データ

多くの校務支援システムは、表計算用データや印刷用帳票の出力機能を利用する。そのため出力されるセンシティブデータは、出力内容、保存場所の制限等の取り扱いに配慮することが望ましい。

- ・検討項目(ii) 本人認証

クラウドサービスにアクセスする場合には、認証を行う必要がある。ID とパスワードの組み合わせだけでなく、物理的な認証(USB トークンや IC カード等)、生体認証(指紋、静脈等)、電子証明書の組み合わせにより、他人による詐称のリスクを大幅に低減できる。

本人認証のシステムを導入することで、他人の詐称リスクを低減することは可能になるが、ユーザがログインする際に認証の手間が増えることと、導入コストが上がることを考慮し、導入の検討を行うことが望ましい。

また、権限設定と合わせての検討も必要である。

・検討項目(iii) 校外からのアクセス

クラウドサービスを校外から利用する場合は、本人認証、利用できる機能の制限、PC へのデータ保存の可否を十分に検討することが望ましい。

③不正アクセス対策

セキュリティ強化には、さまざまなシステム対策が必要である。ファイアウォール、プロキシサーバ、データ/ネットワークの暗号化、認証技術による用者確認、不正侵入検知システム(IDS) 等を施すだけでなく、日々発見されるセキュリティホールに対する対策が必要である。また、パッチの適用の判断とテスト作業、次々に現れる侵入手口への対策検討が要求される。これらをユーザが評価するためには、同等の知識が必要になるため、公的セキュリティ認証や第三者によるセキュリティ診断結果を活用することも推奨する。

(3) 利活用支援

校務支援システムの運用にあたっては、サポート体制と研修の充実が必要である。学校業務の特性で、年度当初や学期末に業務が集中する。ヘルプデスク等での電話等での対応だけではなく、支援員が直接学校に出向いて支援できる体制も必要である。研修は悉皆が基本で、あるが、学校数が多い場合は、必ずしもタイムリーな研修とはならないので、スケジュール管理などで工夫が必要となる。

(4) SLA

SLA の設定に当たっては、ネットワーク環境、ユーザ数を考慮の上、導入業者との綿密な打合せが必要となるが、実際の運用開始後の見直しがより必要で、業務が集中する時期の状況を良く見極める必要がある。見直しを行うことで、運用に見合った SLA とすることが可能となる。

(5) 運用

システム運用にあたっては、教職員の負担をできる限り軽減するためにも保守・メンテナンスと合わせてアウトソーシングが望ましい。近年、セキュリティ対応など運用上求められる技術レベルが高度化・複雑化しており、安心できる専門の業者の選定が重要である。



### 5.1.2 グループウェア

ネットワークに接続されたコンピュータを利用して教職員が互いに情報の交換や共有、またスケジュール管理等の業務に利用される機能を有し、業務の効率化を目指すシステムである。業務に必要な様々な機能が一つに統合されてユーザにサービスを提供する。主な機能としては、電子メール、電子掲示板、スケジュール管理、施設予約、ファイル共有などがある。

#### (1) クラウドモデル

必ずしもセンシティブな情報を取り扱うシステムではないので、様々なクラウドモデルが考えられる。ASP サービスでの利用も考えられる。

#### (2) セキュリティ

校務支援システムと同様の検討が必要で、特に利用者の認証が重要である。

外部へのメール機能がある場合には、添付ファイルがある場合に管理職の承認がないと送信できないような機能の有無も検討が必要である。

#### (3) 利活用支援

グループウェアには特に難しい機能や操作があるわけではないので、ヘルプデスクを設置し、伝達研修を実施することで対応できる。活用促進にあたっては、管理職が率先しスケジュール管理や電子承認を使用することが必要で、管理職研修が重要である。

#### (4) SLA

メールシステムやファイル共有の機能は停止すると業務に大きな支障が発生するので、稼働時間や稼働率に関しては、十分な検討が必要である。レスポンスタイムなどもポイントであるが、ネットワーク環境やユーザ数によって異なるので、運用開始後の見直しが必要である。

#### (5) 運用

稼働監視やセキュリティ対策を十分に行う体制を整備する必要がある。またユーザ研修や運用支援面では、その活用促進を目的としてユーザ研修会や学校ヘルプデスクなどの操作問合せ環境を整備する必要がある。

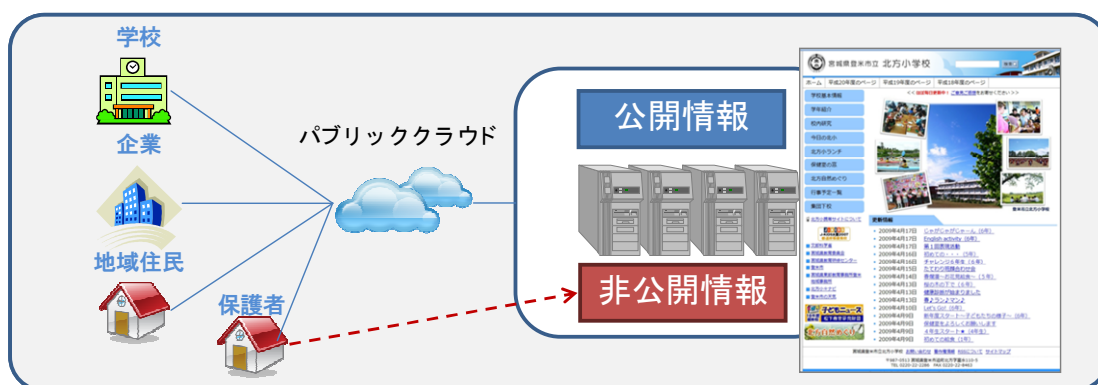
### 5.1.3 学校ホームページ管理システム(コンテンツ・マネジメントシステム:CMS)

教員1人1台 PC など学校の ICT 環境の整備に伴い、学校ホームページを活用した保護者や地域への情報発信が益々重要となってきた。学校ホームページ管理システム(CMS)は、学校現場が教育方針や教育体制、子供たちの活動の様子や成果などを保護者や地域住民等に情報発信していく上で、多くの教員が簡単に手際よく安全に情報発信できる仕組みを提供するものである。



#### (1) クラウドモデル

学校ホームページ管理システムは保護者、地域住民、第3者など不特定多数の利用者が幅広く閲覧する仕組みを提供するシステムである。従ってクラウドモデルとしては、パブリッククラウドが前提であるが、ホームページのコンテンツ内容によってはその他のクラウドモデルで運用される場合がある。例えば学校として日々公開する情報はパブリック上に配置するが、児童・生徒の写真や一般には公開されない情報については、特定のメンバーだけが閲覧できる専用ページを設けたり、プライベートクラウド上に設置したりするなど情報の種類によって分別される。



## (2) セキュリティ

学校から発信する情報として、情報の種類や内容によってセンシティブに取り扱わなければデータが存在する。一般的に学校から発信される学校基本情報や学校行事等については公開情報として幅広く公開をすることは望ましいが、個人として特定できる写真や遠足等の帰りの時間等のセンシティブデータについては、閲覧者を制限するなどの注意が必要である。

### (ア) 一般・地域住民への公開データ(ノンセンシティブデータ)

- ✓ 「学校情報」「研究・学校評価」などの学校基本情報
- ✓ 「学校・学年行事」「クラブや部活動」「校外活動・外部交流」などの学校行事

### (イ) 保護者が閲覧できるデータ(センシティブデータ)

- ✓ 児童・生徒など個人情報として特定できるデータ(写真等)
- ✓ 遠足や運動会などの連絡などの催事連絡

## (3) 利活用支援

### ➤ 概要

学校ホームページ管理システム(コンテンツ・マネジメントシステム)

### ➤ 詳細

各学校のホームページを学校単位で各教員が作成できる仕組みや保護者や地域住民などに対して幅広くホームページを閲覧できる仕組みをクラウド上に提供する。

### ➤ サービス利用者

教育委員会事務局、常勤職員、非常勤職員、児童生徒および保護者、地域住民

### ➤ サービス提供範囲

一般公開

### ➤ サービス提供時間

24 時間／365 日

## (4) SLA

学校ホームページ管理システム(CMS)の SLA としては、稼働中のアクセス状況を可視化できる仕組みのほか、万が一に備えてアクセスログを採取できる状態を提供しなければならない。また、教育クラウドでは、学校ホームページのアクセスが集中する時期に CPU やメモリなどの処理能力を高められるメリットもあるため、年間アクセス状況を睨んだ設計も可能である。

### (ウ) CMS 稼働中のアクセス状況やアクセスログ

- ✓ 学校ホームページのアクセス状況(遷移)
- ✓ 不正アタックなどに対するアクセスログ

(エ) 閲覧が多い時期の高負荷対応

✓ 入試時期や学校イベント時期

(5) 運用

学校ホームページ管理システム(CMS)のクラウド運用としては、24時間／365日のサービス提供が必須という観点から稼働監視やセキュリティ対策を十分に行い、外部攻撃や Web 改竄などの防止にあたらなければならない。またユーザ研修や運用支援面では、各教員が日々の活動を簡単に情報発信することが重要であり、その活用促進を目的としてユーザ研修会や学校ヘルプデスクなどの操作問合せ環境を整備する必要がある。

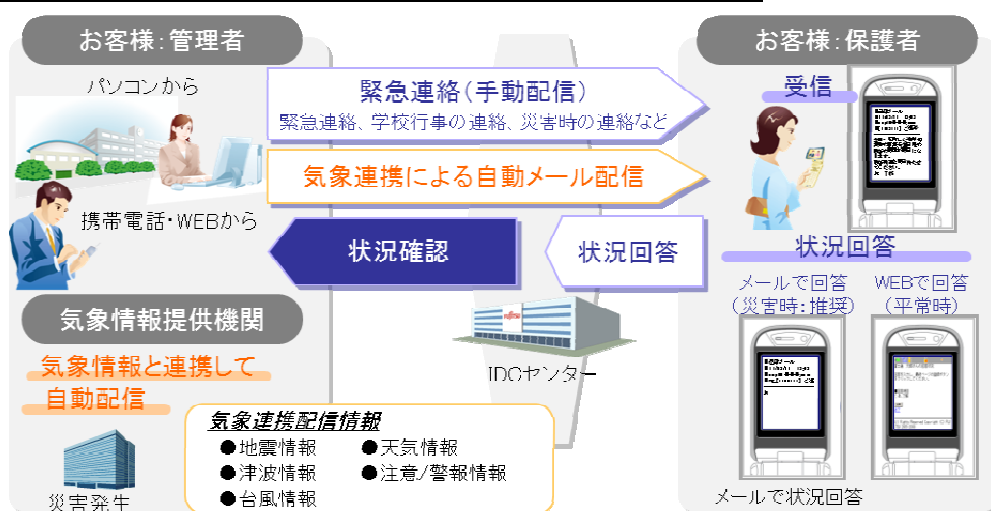
### 5.1.4 学校連絡網サービス

現代ではライフスタイルが変化し、留守宅が多く電話連絡網では連絡が行き届かなくなっている。

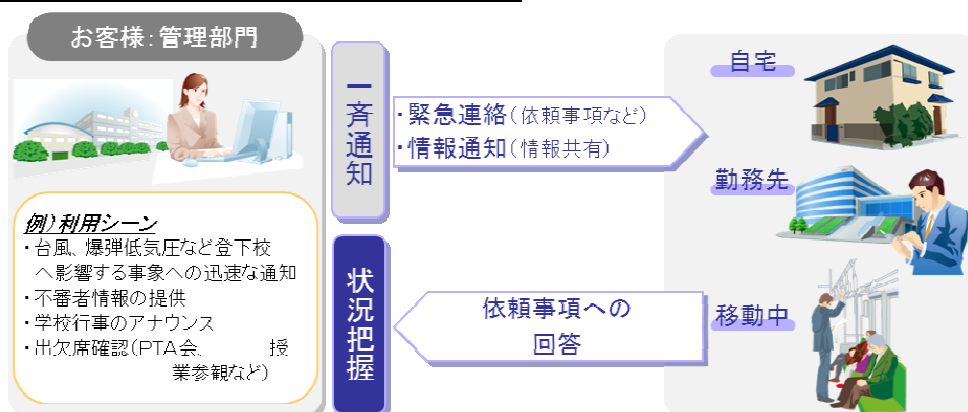
学校連絡網サービスでは世帯普及率 90%を超えた携帯電話と SaaS サービスを活用し、メールで教育委員会及び学校から保護者への連絡事項を一斉に伝達することができる。

活用例として、不審者情報提供や緊急時連絡、さらに保護者からの回答が必要な学校行事の出欠確認やインフルエンザ流行時の確認作業にも利用されている。

#### ■サービス利用イメージ(メール配信から状況回答)



#### ■急な連絡事項や行事のアナウンス



### (1) クラウドモデル

一般的に、複数の携帯キャリアに対応し、かつキャリアによる発信規制を回避して多数の携帯メールを遅延なく一斉に送信するためには、専用の設備が必要となる。

更には、最も価値を発揮する災害時における利用を想定する場合、災害に備える構造を持ったデータセンターでの運用が必要。

これらの点からも、災害に対して十分なインフラを活用したパブリッククラウドサービスが適していると考えられる。

### (2) セキュリティ

- ・ インターネットを利用する際は、SSL 通信(または同程度の通信)を使用すること
- ・ ログイン後も、セキュリティ確保のため、無操作時で一定時間経過後に自動的にセッションが切断されること
- ・ 不正利用防止のため、パスワードの連続間違いで、ログイン ID をロックする機能を有すること
- ・ 高度なデータセンターを利用し、高セキュリティを有すること
  - (A) 24 時間 365 日監視体制であること
  - (B) 登録された個人情報外部へ漏洩しないように、つぎの対策を講じていること
    - ・ 生体認証(手のひら静脈認証)／RFID タグによる入退室管理
    - ・ サーバ室入り口は共連れ防止対応＋金属探知機
    - ・ 人位置管理情報管理システム
    - ・ 生体認証(手のひら静脈認証)と連携したラック鍵管理システム
  - (C) 首都直下型地震の影響を受けにくい場所に開設されたデータセンターで運用していること
  - (D) 設置する施設は耐震構造等の地震に対する対策を講じていること
  - (E) 電力供給が途絶えた場合に備え大容量の蓄電池や自家発電装置等を備えていること
  - (F) プライバシーマーク及び ISO27001 (ISMS)を認証取得していること

### (3) 利活用支援

#### ①学校連絡網サービス概要

教職員および保護者の登録した携帯電話に一斉若しくはグループ毎にメール送信を行うとともに、アンケートへの返信・自動集計により安否確認等を実施する。

#### ②サービス利用者

教職員、保護者、教育委員会事務局

#### ③サービス提供範囲

一般には非公開

④サービス提供時間

24 時間/365 日(システムメンテナンス時間は除く)

⑤問い合わせ対応

メール受付 24 時間 365 日、電話窓口は平日 9～17 時

(4) SLA

- ・ サービス運用、メンテナンスに関する取り決めが必要。
- ・ インターネット上の通信障害、携帯電話事業者の通信規制および、気象情報提供機関からの情報提供等の条件設定が必要。
- ・ エンドユーザは、ID/パスワード/URL 情報の使用および管理に責任を持つ必要がある。

(5) 運用

- ・ メールによる一斉連絡を実現するためには、携帯電話等のアドレスの変更をエンドユーザから簡易に登録・修正する機能が必要。
- ・ 情報発信者の負担軽減のためには、予め行事などのアナウンスメールや定期的にメールするスケジュール送信する自動送信機能が必要。
- ・ アンケートでの活用には、メール受信した際に状況回答する機能および職員、保護者が回答してきた状況を自動でとりまとめ、パソコン、携帯電話から確認できる集計機能が必要。
- ・ 緊急時の情報提供者の負担軽減のため、気象情報や災害発生時に連動してメールする自動送信機能が望ましい。

## 5.2 事例

### 5.2.1 北海道札幌市

札幌市教育委員会は全市統一の校務支援システム導入により、業務効率化と教育の質の向上を目指しています。

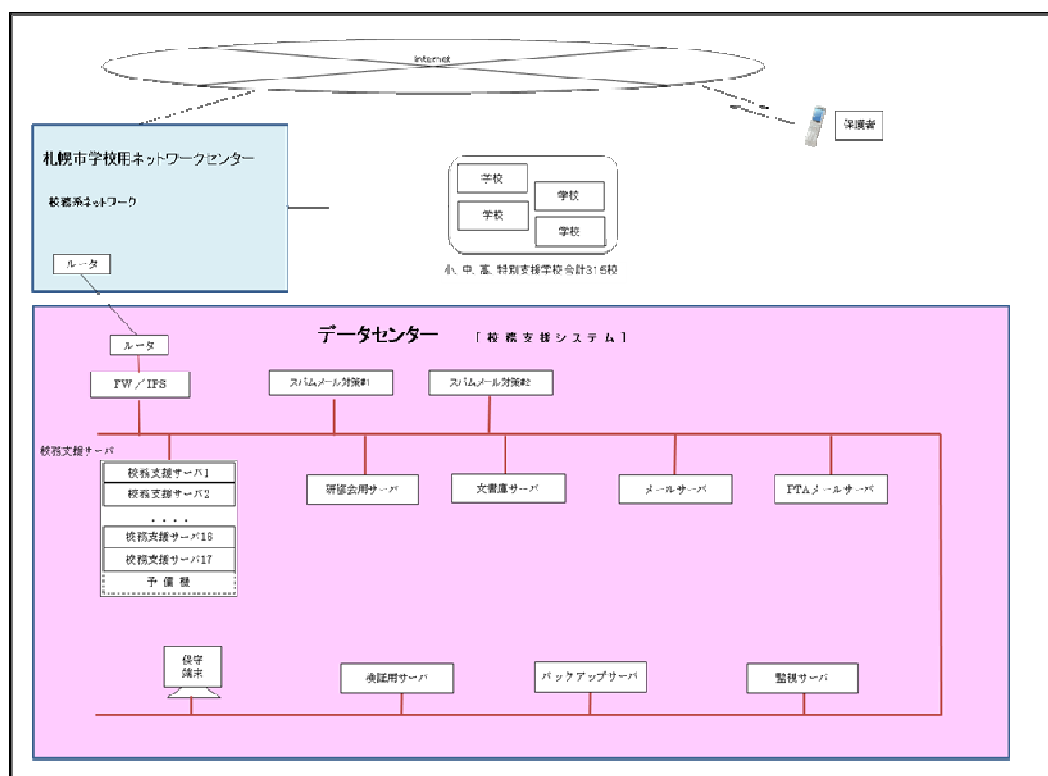
サービス調達・クラウド型の採用・「教育情報アプリケーションユニット標準仕様 V1.0」採用・研修の充実・ヘルプデスクの採用など、最新の取り組みを進めています。

#### (1) 校務支援システム導入の背景と目的

札幌市教育委員会は、

- ・文部科学省は「教育情報化ビジョン」施策にて「校務情報化」を2020年までに全ての学校で整備することが決められていること。
- ・教職員の業務量増大による慢性的な時間外勤務などによる疲弊感の解消を行い、教師が子どもと向き合うための時間を確保することが急務とされていること。
- ・先生ひとり一台の校務用パソコン整備および校務用ネットワークを2009年度に実現し、これを利用した市内の全学校に統一的な校務支援システム導入の要望が強くなっていること。

を背景に校務支援システムの導入を進めています。



札幌市 校務支援システム ネットワーク概要



校務用パソコンが導入された各学校では、校務支援のために、プログラムの得意な教員が Excel のマクロなどを組んで利用していましたが、その教員が異動してしまうとマクロなどのメンテナンスができないなどの問題が発生しており、全市で統一的なシステムの導入が求められていました。

統一的な校務支援システムを導入することで、通知表や指導要録などへの転記作業の軽減や転記ミスの防止などが期待されます。

校務支援システム導入の目的として以下の3点があげられています。

- ・学校現場の業務負担の軽減、セキュリティの強化

教職員の事務処理の大幅な効率化により生み出される時間や労力を児童生徒と向き合う時間の充実、授業準備・研究の充実など教育の本来の目的のために振り向ける。さらに、統一したシステム導入により、業務標準化・長期保存義務のある指導要録や健康診断票の電子化・各種帳票の統一化・ペーパーレス化・各種事務の簡素効率化と負担軽減を図る。また、学校のサーバセンターへデータベースを移行することで、学校での運用管理業務の軽減を図るとともに、強固なセキュリティ対策を講じることができる。

- ・情報の共有、活用による教育の質の向上

児童生徒の日常の様子・特性などを、学級担任だけでなく複数の教職員が情報入力し、情報共有することで、個々人の情報を組織的に把握し、よりきめ細やかな教育に寄与できる。

また、蓄積されたデータにより、様々なノウハウの教員間の共有・学校内・学校間での分析・研究を実現し、個々の教師力の向上、学校力の向上を図る。

- ・全国標準仕様の意義

総務省・文部科学省が進める地域情報・教育情報の全国標準化に準拠したシステムを導入することにより、将来的に市外の転出入処理業務を円滑にし、システム利用料の低減化・サービス提供所を変更した場合のデータ移行の容易性を確保する。

特にセキュリティ面では、

- ・教育用パソコンと校務用パソコンは別に用意しているおり、教育用ネットワークと校務用ネットワークも分離されている。
- ・ネットワークへのログインの仕組みと校務支援システム利用のID・パスワードの利用で、安全性を確保する。
- ・校務支援システムの入力はサーバみに格納され、パソコンのローカルには保存できないようにする。
- ・市の学校に統一のセキュリティポリシーが設定されており、必要に応じて改定を続けている。

など、重要な情報を護るための様々な取組がされています。

## (2) 導入規模とスケジュール

札幌市教育委員会の学校は、小学校 206 校・中学校 99 校・高等学校 8 校・特別支援学校 4 校の計 317 校、児童生徒 14 万 5 千人超・教職員約 9 千人超の規模です。

開発スケジュールとしては、

- ・2012 年 3 月 調達を実施。
- ・2012 年 9 月 パイロット校(小 20 校、中 10 校、高 2 校、特別 1 校の計 33 校)にて導入開始。
- ・2013 年 4 月 全校で導入開始。

## (3) 校務支援システム調達の特長

今回の校務支援システム調達の特長として、  
契約形態としては、

- ・2012 年 9 月～2019 年 3 月までの 6 年度にわたるサービス利用料契約。

システム導入の仕様としては、

- ・クラウド型のシステム方式であり、総務省の「校務分野における ASP・SaaS 事業者向けガイドライン」を遵守したものであること。
- ・データセンターは国内に所在することとし、バックアップを行った副本をデータセンターの設置場所以外の市町村に保管することとしています。
- ・校務用端末のブラウザで動作するシステムであること。
- ・一般財団法人全国地域情報化推進協会(APPLIC)が策定した「地域情報プラットフォーム標準仕様書」と「教育情報アプリケーションユニット標準仕様 V1.0」に完全準拠し、「準拠登録・相互接続確認製品マーク(オレンジマーク)」を 2012 年度末までに受けていること。

があげられます。また、

- ・システム導入時の研修 1 万 5 千人超、翌年度 2 千人、以降 4 年間各年度 6 百人超を予定。
  - ・教職員などからの問い合わせ対応窓口として「ヘルプデスク(サポートセンター)」の設置。
- など、導入後の安全安心な利用のための手立てもとられています。

クラウド型システムを採用した理由としては、市全体としてシステムを運用する人員が減るなか、大規模なシステムを内部で運用することは現実的ではないとの考えで、外部の専門家に任せることを選択したものです。

具体的な機能仕様については、約 1 年間かけて、それぞれの管理職や学校種や職種のメンバーで検討チームを作り仕様作成を行ったとのこと。

今後調達される自治体には、十分な時間をかけることを勧めたいと考えています。

仕様化作業のなかでは、いくつかの業務ルールを見直し業務改善を図っています。

2012 年 4 月に教育委員会全体の ICT を推進する学校 ICT 推進担当部門が新設され、今回の校務支援システムもこの部門にて運営されます。

## 5.2.2 福岡県北九州市

北九州市教育委員会は、平成 17 年度からネットワークをプライベートクラウドに順次移行し、平成 20 年度に完了した。校務システムに関しては、市内小中特別支援学校約 200 校で、平成 24 年 4 月より稼働している。

### (1) 教育委員会の体制

教育委員会学務部学事課に校務支援システム担当係があり人員は 2 名。

実際の IDC は、ネットワーク運用管理と共に民間業者に委託している。学校のサーバ、パソコンの重要な設定事項なども保守業者が行い、学校側が作業することはない。同様にヘルプデスクも設置し、繁忙期には増員するなどうまく運用されている。

### (2) ネットワーク関連

物理的に 1 回線で、セッションを分けている。実際には、事務系、校務系、教育系の 3 種。すべて有線 LAN で接続。(北九州市は無線 LAN によるネットワーク接続を認めていない。) 教室には、教育系情報コンセントのみ、校務系は事務室、職員室、校長室、保健室のみ。保健室は、本来教育系のみとしていたが現場からの要望が強く、MAC アドレス認証で校務系も使えるようになっている。将来は、普通教室も同様の切り替えが可能なように、今年度から準備を行っている。

### (3) セキュリティ関連

教育系、校務系は、IP 認証＋ユーザ認証の 2 重認証。情報コンセントは L3 スイッチで分離しており、校務系情報コンセントに校務系として登録されている端末で、かつ、校務系ユーザのログインでないと接続できない。データはすべて IDC のサーバに収められている。

校務用ネットワークはリモートアクセスを認めていない。私物 PC、私物 USB メモリは持ち込み禁止。学校においては持ち出し用の USB 購入を許可しているが、教育委員会に導入協議を申請し、許可を得る必要がある。自動暗号化＋パスワードロックがかかる USB メモリだけを購入許可対象としている。

本年度に本格稼働した校務システムの導入もあり、セキュリティの意識は高くなっている。

### (4) 校務システム関連

これまで、学校にはグループウェアもメールもない状況だったので、導入への期待は大きく、当初から部分導入ではなく 100% 導入を目指した。ゼロからのスタートだったので、首長部局の説得もやりやすかったと考える。

北九州市には区単位で校長会があり、その上位組織として校長会長会がある。その中に帳票委員会があり、そこで全ての帳票が決定されるので、全市内で帳票は統一されている。しかしながら、導入したパッケージのカスタマイズは少なからず必要であった。

本年4月から全校で本格稼働し、初めての通知表作成・出力の際は、教育委員会としても体制を整えたが、特に障害は無かった。

#### (5) 調達に関して

IDC 関係の調達仕様書には、専門的な項目名も出ているが、基本的には計画時の大きな目的として、200 校、20,000 台をマックスとして使うにあたって、セキュリティを確保し、サービスを円滑に行えるサービスを提案書でいただき審査の形態。技術的なことはわからないので、アウトソーシングしている。IDC センターの運営は任せるが、これだけ是可以できるようにしたいという書き方をしている。ヘルプデスク業務も含め、人員体制も円滑を調達条件としているので、適宜時期、時間で増員、減員されている。

校務支援システムも同様に、こういう機能・処理・帳票が必要という文言で条件を出し、提案書を出してもらって審査とした。仕様書作成にあたっては、検討委員会を設置し、その下に教員 50 名の作業部会を設置し、各業務主管課がそれぞれに関して責任を持つかたちで、実質 8 ヶ月で仕様書を作成した。現在もその作業部会は残っており、改善や普及に関する課題を検討している。

##### ※サービス調達成功のポイント

- ・できるところ、できないところ、何のために行うのかを見失わないこと。
- ・学校をどうしたいかを明確にすれば、おのずと誰に協力を得ないといけないか、誰が主体とといけないかがわかる。

#### (6) 研修に関して

全体説明会は校務支援システム担当係が、全管理職を対象に定期的を実施。基本的にすべて校内研修で、管理職が主催し、趣旨説明を行い、操作説明等は ICT サポーターが実施。ICT サポーターは各校月 3 回、年間 36 回巡回が原則であるが、各校の事情にあわせ、月によって回数の変更が可能。

#### (7) 校務システム導入の効果

まだ、1 年たっていないので、全体は把握できていないが、文書管理機能の導入で、そのままだま回覧やメール添付、担当者の回答を電子決済とするなどでペーパーレス化は劇的に進んだ。行政行為に関わるもの意外はすべて帳票から公印を廃止し、電子保管も進んでいる。

#### (8) 課題

現在、教室で出欠の入力などができない環境なので、将来的にできるようにすることで考えている。現場にもそのように伝えている。公印は廃止したが、指導要録の様式 1 には担任印が必要。様式 1 の取り扱いを検討中である。

(9) まとめ

教育委員会学務部学事課校務支援システム担当係を中心に、各担当所管課、校長会が協力して推進している。導入委員会が解散せず、改善や利用促進の要として活動継続。サービス調達は目的を明確にし、業者との調整を重ね、サポート・保守も充実させ成功に導いた。

## 5.2.3 沖縄県宮古島市

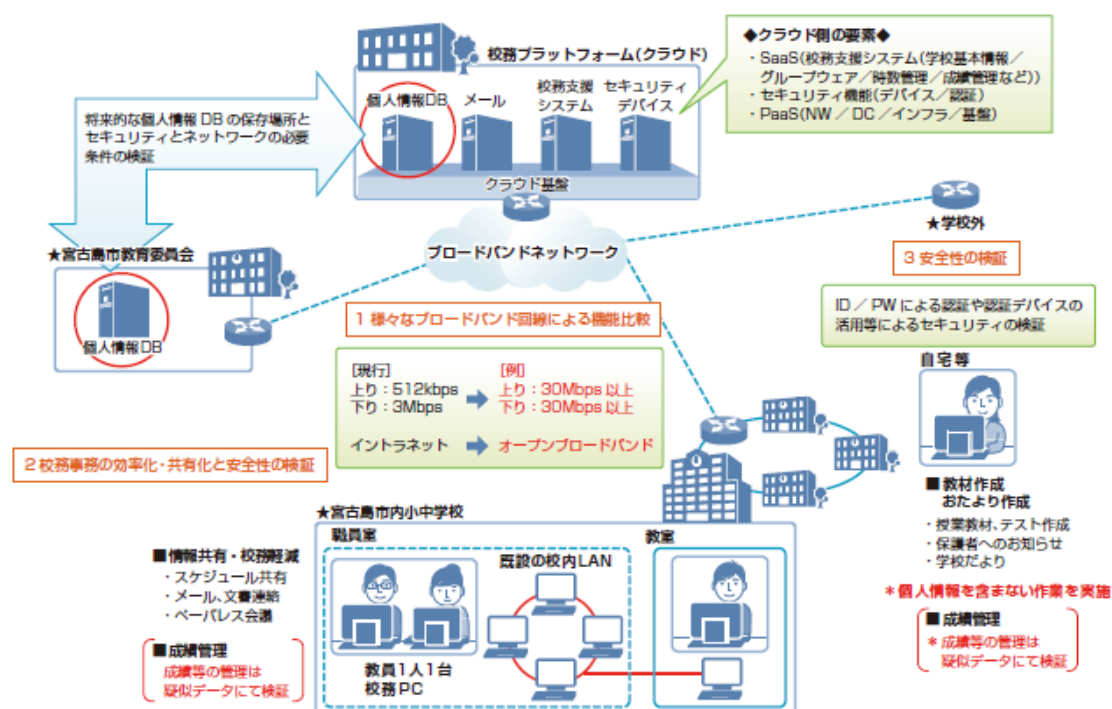
〔概要〕教育分野でも活用が広がりはじめたクラウド

教育の ICT 化は全国で様々な取組みが実施されており、創意工夫の積み重ねによりますます広がりを見せています。近年では災害対策の観点からもクラウドの活用が注目されており、教育分野においてもトライアルが実施されたり、実際に採用される例もではじめています。ICT 環境整備を進める上でも有効な選択肢の一つになっていくものと考えられます。

〔コラム1〕校務クラウド実証実験からはじめた校務情報化の取組

数多くの島が連なる沖縄県のほぼ中央に位置し、豊かな心を育てる学校教育の充実を掲げて、ICT を活用した最先端の教育環境の実現を目指す宮古島市。大小 6 つの島々に海を隔てて 36 校の小中学校が分布していることから、文書の受け渡し等の連絡調整が難しく、結果的に情報の共有や全体の連携が課題となっていました。

平成 22 年 4 月には市内小中学校教職員全員に 1 人一台の校務用 PC を整備すると共に、これらを活用して以前より抱えている課題の解消や、校務情報化を進め教師が子どもと向き合う時間を更に拡大させることに取組んでいました。この取組みを加速させるきっかけとなったのは、平成 22 年 10 月より開始された総務省の実証実験「ブロードバンド・オープンモデルによる地域課題解決支援システムの検証(小・中学教員の事務軽減支援)」への参加でした。

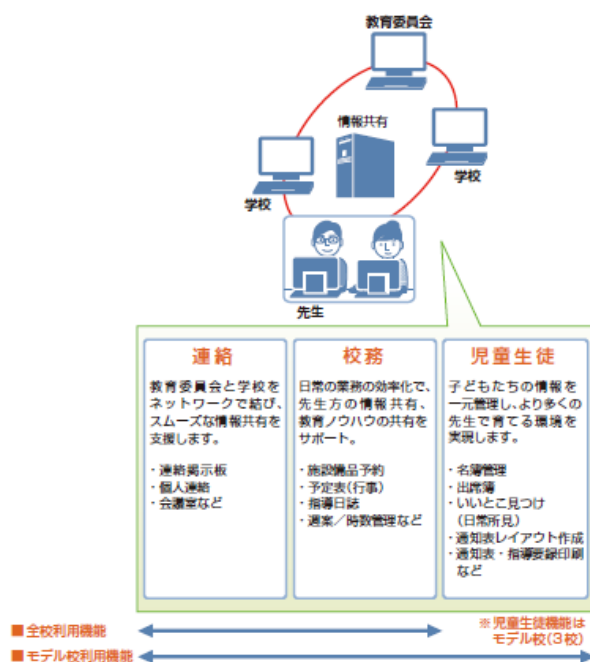


●実証実験の構成イメージ

「ブロードバンド・オープンモデル」とは、行政、教育、医療などの分野における業務用アプリケーションに関して、ハードウェアやソフトウェアを地方公共団体が自ら所有することなく、セキュリティが確保された環境のもとでブロードバンド回線を介して外部サービスを積極的に活用し、効率的に業務を遂行しようというもの。平成 23 年 3 月末までの約 6 カ月間、「ブロードバンド・オープンモデル」を教育用途に用いながら、実証実験を通じて宮古島市の教育現場や地域の抱える課題の解決を目指してきました。

「風は南から」を合言葉にモデル校の一つとなった南小学校をはじめ、教育委員会と各学校が一丸となって取組んだのがクラウドにより提供される校務支援システムの活用です。クラウド技術とブロードバンド回線を用いることで、自前でシステムを構築するより少ない予算で導入することができ、更にはシステムを管理するための人材を必要としないメリットもありました。

実証実験では教職員による検討会を立上げ、この校務支援システムの活用や運用の改善を積極的に進めてきましたが、継続的にシステムを利用することで校務作業負担の軽減が期待される結果を得ることができ、総務省の平成 24 年度情報通信白書の事例でも取り上げられています。宮古島市ではこの結果をうけて実証実験後も正式にクラウド技術を活用した校務支援システムを採用し、現在も活用を進めています。



●実証実験中の校務支援システム機能

こうした経緯から校務情報化を進めてきた結果、天候の影響などにより特に大変だった海を隔てた島への文書の受け渡しなどはリアルタイムにやり取りできるようになり、周知・共有事項や研修会の案内なども連絡(掲示板)機能を利用することで徹底でき校務に関する手間が削減できてき

ています。インフルエンザ発生件数の情報共有にも効果的です。

その他、教育委員会には「最初は戸惑ったが、楽になった」という教員の声も寄せられており、指導教官や教員同士の学校を超えた横のつながりや、情報共有をきっかけとした教科毎のコミュニケーションの促進にも効果が現れており教科研究や授業研究に反映されてきています。

また、今後も経過を注目していきたいと考えているのは教材やノウハウの活用です。書庫機能を活用してこれら情報の蓄積が始まっていますが、教材やノウハウの有効活用とコミュニケーションの活性化による相乗効果で校務情報化のメリットを更に引出すことができるのではと期待しています。

今後は、指導要録作成や成績管理など活用範囲の拡大を検討会で議論していく計画ですが、子どもと向き合う時間の拡大に向けて着実に前進してきていると言えそうです。

#### 〔コラム2〕フューチャースクール推進事業による学校 ICT 環境と教育クラウドの活用

宮古島市では前述の校務情報化とともに授業における ICT 活用にも取り組んでいます。以前より ICT 機器や校内 LAN、インターネットなど情報教育の環境整備を進めると同時に、コンピュータ活用指導方法や情報機器の効果的な活用方法の教員研修機会を拡充することで情報教育に強い学校づくりを推進してきましたが、平成 23 年度からは総務省「フューチャースクール推進事業」および文部科学省「学びのイノベーション事業」にも参加しています。



フューチャースクール推進事業の実証校となった下地中学校では、全生徒・全職員に 1 人一台のタブレット型パソコン・全普通教室に電子黒板・校舎全域で利用可能な無線 LAN・学校から利用可能な教育クラウドを配置し、教育活動全般で活用できる ICT 環境の整備を行いました。また、市内の学校現場に精通した ICT 支援員が教員の授業をサポートすることで、ICT 機器の良さを生かした「楽しい授業」「わかる授業」の構築を目指しています。

特に、下地中学校では「ICT 機器の効果的活用を通しての言語活動の充実を図る授業の工夫・改善に関する課題の抽出・分析」を独自のテーマとして取り組んでおり、教育活動において ICT



を効果的に運用し生徒の興味関心を高めることで、発表などプレゼンテーション能力の向上にも力を入れています。

生徒を対象に実施したアンケート結果では、「友達の考え方や意見を知って学びが深まったか」という設問に対して「大変そう思う」「少しそう思う」と回答した生徒が 75%に達しており、学習効果の向上や言語活動の充実に有用性があることが確認できましたが、アンケートまでの実践期間も短かったことから継続的な取組みを続けていきます。

教育クラウドはこの運用を支える役割を担っています。学校の教員同士、他実証校の教員や ICT 支援員と、学校と保護者間で教材共有・お知らせ・学校行事・アンケートなどの情報共有・連携をサポートするコミュニケーションサイトとなっており、家庭のパソコンや携帯電話等からもインターネット経由で接続できます。その他、インターネット接続や Web フィルタリングなどのサービスも教育クラウドが提供しています。

その他、宮古島市下地中学校における平成23年度のフューチャースクール推進事業に関する成果は、総務省のホームページに掲載されています。今後、宮古島市教育委員会では本事業で実現している情報環境を、段階的に市内各校に広げていかれないか検討を進める予定です。



教育クラウドの提供する機能(サンプル)

## 5.2.4 東京都江戸川区

江戸川区は公立小中学校数 106 校、児童生徒数が東京 23 区では最も多い大規模自治体である。ICT による校務の改善計画をスタートさせたのは平成 20 年度。当時、教育の情報化を進める国の基本方針への対応、教員の多忙解消に加え、7 割近くの教員が私物のコンピュータで事務作業を行っていた状況もあり、情報セキュリティ面でもシステム整備が急務となっていた。

そのような状況の中、江戸川区は 2,700 名の全教員に PC を配布するとともに、江戸川区外にあるデータセンターに学校 LAN 用サーバ設置し、そこに児童生徒の学籍管理、出欠管理、成績管理までトータルに行えるパッケージ型のセンター版校務支援システムを構築した。江戸川区はその面積の 7 割以上が海拔 0m 地帯にあり、洪水などの被害により、学校が作成し、保存が 20 年にも及ぶ書類が消失する危険性なども問題視されてきたが、このクラウド型の校務支援システムを構築することによって、そのリスクも極めて小さなものにすることができた。

さらに平成 21 年度からは ASP サービスによる学校ホームページ作成システムも順次導入に踏み切った。以前はホームページの担当者により学校により、その内容や更新頻度に大きな差があったが、今では、その差も徐々に小さくなってきているという。また、ASP サービスであるので、学校や教育委員会は、サーバ保守などからは解放され、コンテンツの充実のみに注力すればよい環境が整っている。

### 1. 校務支援サービス

#### (1) 導入までの流れ

導入は以下のようなスケジュールで行われた。なお、指導要録、調査書、出席簿、健康診断票等の公簿は、都内、区内統一の小式を校務支援システムで出力できるようにカスタマイズを行っている。通知表に関しては、全校オリジナルのレイアウトのため、1 校ずつヒアリングを行い、学校個別のカスタマイズを行っている。

平成 20 年度	平成 21 年度	平成 22 年度
校務支援システムの導入。 グループウェア機能を小・中学校 全校で運用開始。	モデル校 <sup>※1</sup> にて、通知表作成とデータ管理を校務支援システムにて運用開始。	全校 <sup>※2</sup> で、通知表、指導要録、調査書、保健関連の各帳票作成とデータ管理を校務支援システムで運用開始。

※1: 小学校 13 校、中学校 8 校

※2: 小学校 73 校、中学校 33 校、但し、夜間中学校を除く

#### (2) 導入の成果(利用者からのヒアリング結果:抜粋)

- ・「校務支援システムでの通知表作成になれてしまうと、手書きの通知表がとても大変だと感じた。」(江戸川区から、他地区に異動になった先生からのご意見)
- ・「今まで通知表を手書きで作成していたが、校務支援システムを使った通知表作成は効率的だ。一度入力したデータを様々な帳票に反映させることができるため、同じ内容を何度

も記入する必要がない。」(他地区から江戸川区に異動してきた先生からのご意見)

- ・「電子データだと、管理職のチェック後の修正が非常に楽だ。手書きの時は、わずかな修正でもとても大変だった。」(管理職の先生からのご意見)

### (3) セキュリティについて

- ・通知表を電子化したことで、通知表の紛失事故は激減した。万が一生徒が通知表を紛失しても、電子データで保存している場合はすぐに再配布ができる。
- ・電子データに関してはプライベートクラウドで一括管理をし、データの校外への持ち出しについては指紋認証 USB を利用している。

## 2. 学校ホームページ作成支援システム(学校 CMS)

### (1) 導入までの流れ

導入は以下のようなスケジュールで行われた。

平成 21 年度	平成 22 年度	平成 24 年度
幼稚園 5 園が、一般のホームページ作成ソフトによる作成から、学校 CMS に移行。	小・中モデル校※ <sup>1</sup> が、一般のホームページ作成ソフトによる作成から、学校 CMS に移行。	江戸川区幼稚園、小・中学校全校が、一般のホームページ作成ソフトによる作成から、学校 CMS に移行完了。

※<sup>1</sup>: 小学校 6 校、中学校 3 校

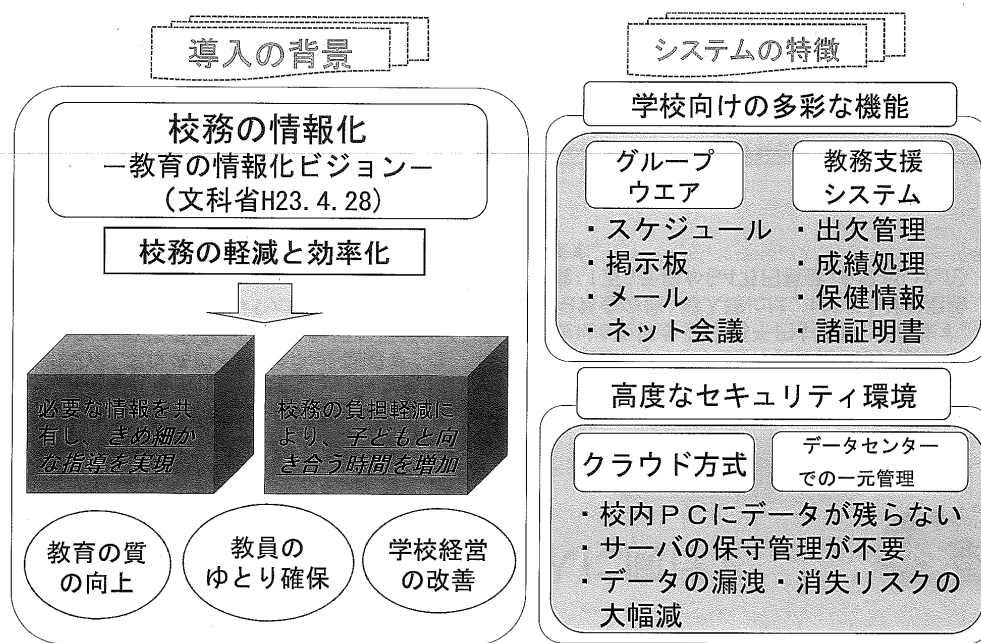
### (2) 今後の展望

- ・区の方針である、「開かれた学校」にするためのツールとして、学校ホームページを活用していきたい。既に、「学校応援団」、「PTA」等のページで、地域との交流をホームページで紹介している学校が多数あるが、こういった取り組みをより広げていきたい。そのためには管理職、特に校長先生の意識が重要であるが、徐々に校長先生方の意識も変わりつつあると感じる。

## 5.2.5 株式会社 HARP

平成 21 年 10 月から教務支援システムとグループウェアを併せもつアプリケーションを ASP-SaaS 方式で構築し運用を開始。

### 北海道公立学校校務支援システム



1

#### (1) 本格運用予定

##### (ア) 開始時期

- ・ 平成 24 年 4 月 1 日

##### (イ) 利用見込み

- ・ 平成 24 年:市町村立学校 100 校程度、道立学校 270 校
- ・ ユーザ数 17,000 名と想定
- ・ 平成 25 年度以降については、北海道教育委員会で別途調査を予定

##### (ウ) 契約形態

- ・ 利用校を管轄する教育委員会で構成する協議会を設置し、協議会から HARP 運用保守業務を委託予定
- ・ 協議会において情報セキュリティに関する要綱等を定め、運用保守業者はその要綱等を順守
- ・ 北海道教育委員会において毎年度、翌年の導入希望を調査
- ・ 利用校増に向け、平成 24 年度以降も説明会等を実施予定

## (2) 構築の基本方針

### (ア) 業務処理要領抜粋

- ・ 教職員の業務量縮減を図る観点で、児童生徒の成績情報等を一括管理・処理・共有する校務支援システムを構築
- ・ 公立の小学校・中学校・高等学校・特別支援学校・中等教育学校の利用校に対し、クラウド方式でサービス提供
- ・ 児童生徒の個人情報扱うものであることから、強固なセキュリティを実現
- ・ 効率的で安定したシステムの構築を図るとともに、オープンソースのソフトウェアを活用して廉価で導入・運用
- ・ 校務支援システムは、グループウェアと教務支援システムで構成

## (3) 課題等

### (ア) 外字対応

- ・ 指導要録に記載する氏名と住民票記載の正確な漢字氏名との関係

### (イ) 共通化

- ・ 共通システムにおいて学校独自性が尊重されている通知表への対応

### (ウ) データバックアップ

- ・ 震災などによるデータ消失を防ぐため、複数拠点でのバックアップデータ保管

### (エ) XML 対応

- ・ APPLIC 標準(XML)の外部インターフェース対応

### (オ) 指導要録の電子化

- ・ 公的個人認証(LGPKI)などを利用した認証方法の決定および環境の整備  
※指導要録の電子化に係る全国的なルール化が望まれる(認証局など)

## (4) 提言等

### (ア) 全道統一の公立学校校務支援システムの導入・運用に係る財源措置

個々の学校でのシステムの導入には、インシャルコストが発生するとともに、ランニングコストの負担の必要がある。また、システムの導入の前提条件として、教員 1 人 1 台パソコンの整備、校内 LAN 環境の整備、教員 1 人 1 台パソコンの整備を促進するとともに、システム導入経費、システム運用経費に係る財源措置が必要。

### (イ) 公立学校校務支援システム導入に係る環境整備

道においては、学校や児童生徒に関する様々な情報をデジタル化し、教職員間で共有するシステムを構築することにより、教職員の事務負担を大幅に軽減するとともに、子どもの育ちを教職員全体で見守るきめ細やかや充実を図ることを目的に、「北海道公立学校校務支援システム」を平成 24 年度から全道規模で導入する取組みを進めている。県域全体での導入は全国初となる見通しであり、他の自治体等にも有益なデータを提供できると考えている。

### (ウ) 自治体の導入状況・意見を勘案した指導要録等の標準化の検討

## 5.2.6 静岡県富士市

富士市教育委員会は、平成 23 年度に市内小学校 27 校、中学校 16 校の校務用 PC 1,200 台を全て仮想シンクライアント化し、かつ、教員用ポータル・グループウェア、校務支援システムを整備。サーバ仮想化、デスクトップ仮想化、アプリケーション仮想化を行い、セキュリティ対策とユーザ環境の統一を図りながら、自宅での利用も可能にするなど利便性にも十分配慮したシステムを推進している。

### (1) 導入目的

#### (ア) 子どもと向き合う時間の創出

- ・ 情報の共有／活用
- ・ 校務アプリケーションの導入

#### (イ) 安心・安全なしくみの導入

- ・ シンクライアント方式の採用
- ・ USB メモリ等でのデータ持出しを不要に
- ・ 家庭からも利用可能に

#### (ウ) 省スペース／省エネルギー

- ・ 1,200 台の仮想デスクトップを 3 ラックに収容

### (2) 校務支援システムでの期待と成果

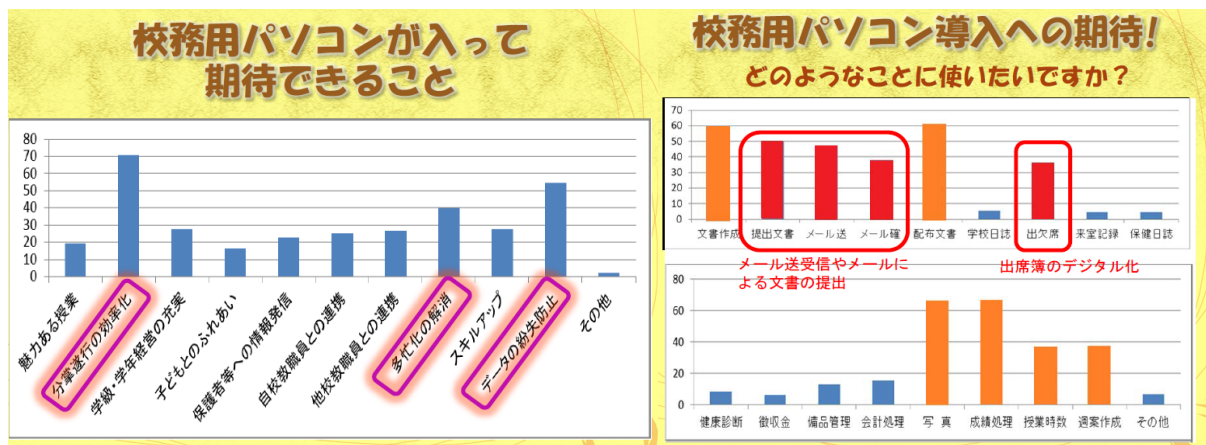
#### (ア) 校務支援システム導入への期待(教員アンケート結果より)

##### 【業務面での期待】

- ・ 分掌遂行の効率化
- ・ 多忙化の解消
- ・ データの紛失防止

##### 【利活用面での期待】

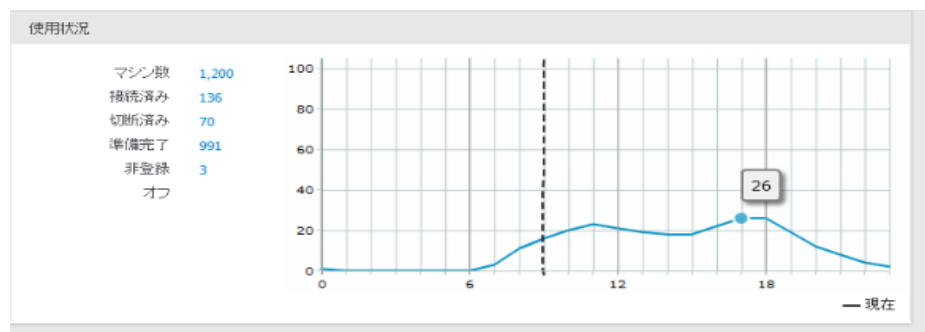
- ・ メール送受信やメールによる文書の提出
- ・ 出席簿のデジタル化



## (イ) 校務支援システムの使用状況と成果

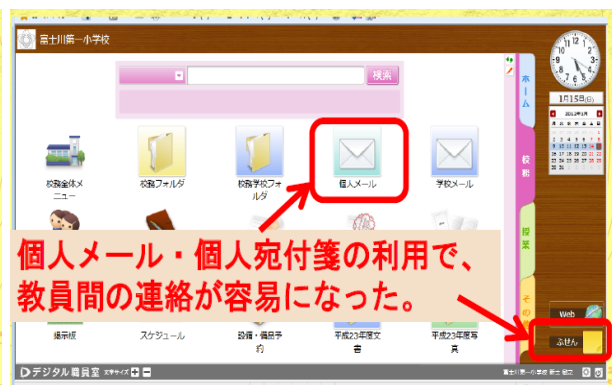
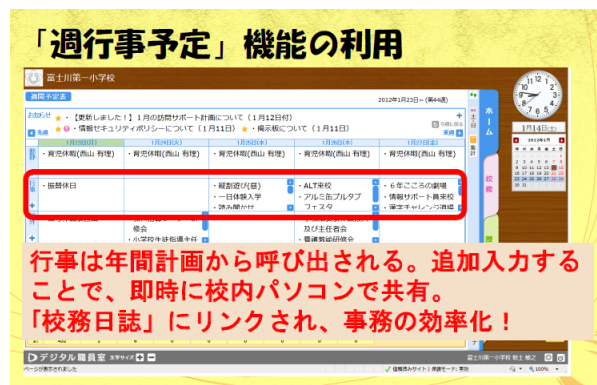
### 【使用状況】

- ・ 自宅からのリモートアクセスは、学校が始まる前日が多い(始まる前日は 100 前後のアクセス)
- ・ 校内での接続情報は 1,700 人強(ピークは午後 4～6 時台)



### 【利活用面での成果】

- ・ ペーパーレス化
  - 朝の打ち合わせを掲示板で
  - 職員会議資料をパソコン画面上で確認
  - 文書保存フォルダ指定 で共有化
- ・ 提出文書作成の効率化
  - 校務フォルダに雛形
  - 提出用フォルダの作成
  - 教員ポータルにボタンを設定



### (3) 今後の課題

- ・ より使いやすいシステムに
  - － 運用方法の確定
  - － 活用状況の調査・変更に向けての調整
  - － 機能・操作等の研修・サポート体制
- ・ 教員のセキュリティ意識向上
  - － セキュリティポリシーの見直し・通達
  - － データ、ID・パスワード等の管理



## 5.2.7 千葉県千葉市

千葉市教育委員会は、平成 22 年度に市内小中特別支援学校 176 校の教職員と児童生徒の学習用に 8,000 台のパソコンを新たに導入し、政令都市として初となる大規模なシンクライアントシステム「Cabinet (キャビネット) 統合システム」を構築した。

Cabinet: Chiba-city Abundant Information Net-work for Education and Trainig

### (1) Cabinet の運用のための組織

情報システム管理者 (教育長: 教育 CIO)、情報システム副管理者 (学校教育部長)、  
情報システム責任者 (教育センター所長)

#### 【学校】

Cabinet 利用責任者 (校長: 学校 CIO)、Cabinet 取扱責任者 (利用責任者が所属職員から指名)、教育メディア主任、ホームページ担当者

#### 【教育委員会】

教育センター: 情報教育部門: 担当指導主事 4 名

### (2) 機器整備状況

小学校: 117 校、中学校: 57 校、特別支援学校: 2 校

児童生徒数: 76,856 人、教員数: 4,344 人 (H23.5 現在)

教育用 PC: 8,015 台

### (3) 学習システムと校務システムで期待する導入効果

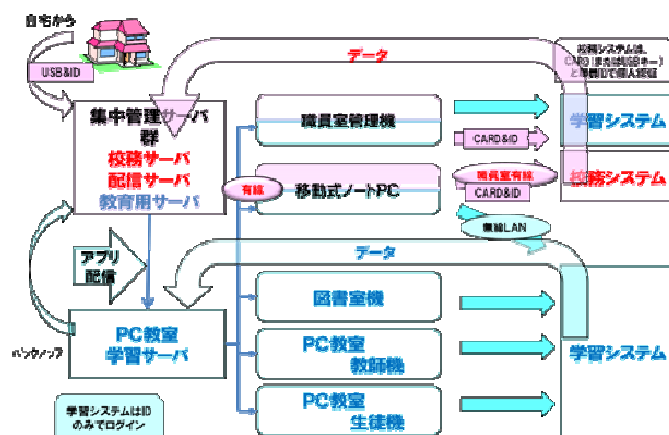
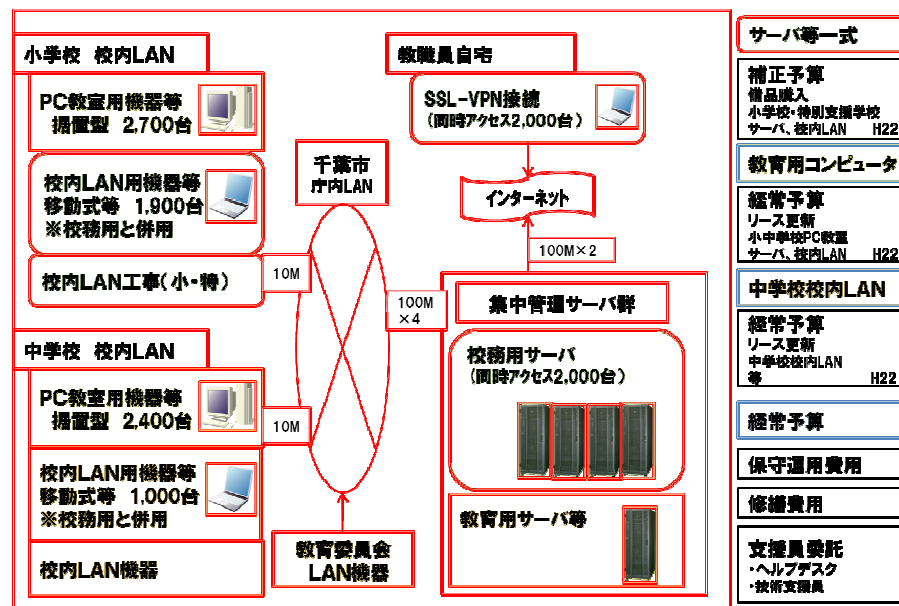
#### < 学習システム >

- これまでの、PC 教室での調べ学習・ドリル型の学習に加え、普通教室等での教材提示や発表、理解の深化のために ICT 機器を利用することで教育的効果が期待できる。
- デジタルコンテンツ (指導用デジタル教科書等) を電子黒板や大型 TV に拡大して利用できる。

#### < 校務システム >

- 校務用システムは、児童生徒の重要度の高い個人情報进行处理する。
  - 高いセキュリティ性
  - ー 児童・生徒が偶然に個人情報を見るリスクの低減 (職員室で有線利用)
  - ー 自宅から接続する場合のセキュリティ性の向上 → 画面情報のみに限定
- 業務内容の標準化が進めば、情報共有や効率化が進む。

#### (4) Cabinet 統合システム全体構成図



#### (5) アプリケーション配信システム

- ・利用頻度が高くないソフトは、経費節減のためにライセンス数を設定し、センターからの配信方式を採用。サーバ上で動作し、Web イメージで利用できるため、端末へのインストール不要。8,000 台に対して 200 ライセンスで運用。

#### (6) 研修の状況(平成 23 年度)

##### ①基礎研修(指定) 3 講座 6 組

- ・情報セキュリティ研修(管理職×2 回)、電子黒板研修(研究主任、メディア主任それぞれ 1 回、計 2 回)、Cabinet 校務システム操作研修(教務主任×1 回:2 グループ)

##### ②専門研修(希望) 9 講座 20 組

- ・情報モラル教育の進め方、学校ホームページ作成、学習探検ナビ、教育用統合ソフ

ト、Office、画像処理、動画教材作成 等

③その他研修(指定) Cabinet 取扱講習(各校取扱責任者×1回)

④出前講座(要請)

- ・Cabinet を利用した学習指導(5校)、校務システムの活用(12校)
- ・要請状況(6校:H23年12月現在受付数)

⑤休日講座(希望)

- ・ICT を活用した資料づくり、電子黒板活用

(7)課題

- ・校務システムの操作法研修の実施が年度途中であったため、システム内に整備した校務支援ソフトは一部の学校から利用を始めている。  
今後、研修等を通じ、176校全校での利用を推進していく。

(8)まとめ

- ・PC環境を仮想PCで提供することにより、OSパッチやシステムエンハンス、復元等のメンテナンスの運用が容易である。
- ・校務用と学習用を別の仮想PCにすることでハードを2台用意せず、1台の学習用PCで厳重にセキュリティを確保することができ、個人情報の漏えいを防ぐシステムとなっている。
- ・自宅PCからUSBキーのみで、校務用仮想PCへのSSL-VPN接続が可能となり、安全に利用することができる。
- ・アプリケーション配信システムを使い、高価な画像動画編集用ソフトを必要な時のみ利用できる。
- ・本内容は、教育クラウドで必要とされる仮想化技術で大規模な環境で活用しており、本格運用での成果を期待したい。

## 6. 今後の課題

---

### 6.1 教育クラウドに関する今後の課題

教育クラウドについては利用者、提供者ともにさまざまな課題があり、まさに発展の緒についたばかりと言える。今後も普及および技術面、運用面の進展によりさらに検討が必要な事項が出てくると思われるが、以下に現時点で見通せる課題を簡単にまとめる。

#### <主に利用(調達)者の課題>

- ✓ 全庁のクラウド化動向把握、全体最適化に向けた調整等の連携
- ✓ クラウドの適用業務の選定および適用に向けた業務の見直し
- ✓ クラウド導入に向けた調達手続きの確認・整備
- ✓ コスト負担ルール、サービスレベル設定、利用者としてのマネジメントノウハウの蓄積
- ✓ クラウド整備により得られる具体的な効果等の蓄積・情報共有

#### <主に提供(事業)者の課題>

- ✓ 使用量変動への柔軟な対応を含むコンピュータ資源の有効活用の仕組み整備
- ✓ スマートフォン・タブレット等、多様化する端末環境への迅速・適切な対応
- ✓ 取り扱う情報種類にふさわしいセキュリティの仕組み整備

#### <利用者・提供者共通の課題>

- ✓ 利用者を支援し、活用度を高める仕組みづくり
- ✓ 運用の共通化等、トータルコストを低減する取組
- ✓ クラウド間の連携など可用性を必要な範囲で維持するための検討。なお、これは災害時の業務継続などにも有効な対策となる。
- ✓ 適用業務に合わせた課金体系の検討・合意
- ✓ 利用者として校務に関する帳票類の標準化、および提供者としてデータ連携の標準化(教育情報アプリケーションユニット標準仕様の普及)

いずれの課題も簡単に解決可能なものではなく、先行的なモデル的取組とその中で積み重ねた知見の共有をもとに、より良い形を創り上げていく必要がある。

### 6.2 本書の今後について

前項の課題認識をもとに、本書についても今後さらに先行的な事例の調査やディスカッションを通じて、教育クラウドの導入を推進すべく検討を深めていくことが必要。しかしながら、クラウドの活用が普及期の前段であることを踏まえ関係する多くの方に理解を広めるための内容として普及に資するものとして再編集することで中間のまとめを行うこととしたい。

## 7. 参考文献

---

1. 「公共 IT におけるアウトソーシングに関するガイドライン」(総務省)
2. 「ASP・SaaS の安全・信頼性に係る情報開示指針」(総務省)
3. 「ASP・SaaS の安全・信頼性に係る情報開示認定制度」(財団法人マルチメディア振興センター)
4. 「ASP・SaaS における情報セキュリティ対策ガイドライン」(総務省)
5. 「総合行政ネットワーク ASP ガイドライン」(総合行政ネットワーク運営協議会)
6. 「SaaS 向け SLA ガイドライン」(経済産業省)
7. 「データセンターの安全・信頼性に係る情報開示指針」(総務省)
8. 「情報システムに係る政府調達への SLA 導入ガイドライン」(独立行政法人情報処理推進機構)

Copyright ©一般財団法人全国地域情報化推進協会 2012-2013 All rights reserved.