APPLIC-0005_1-2014

教育クラウド整備ガイドブック

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

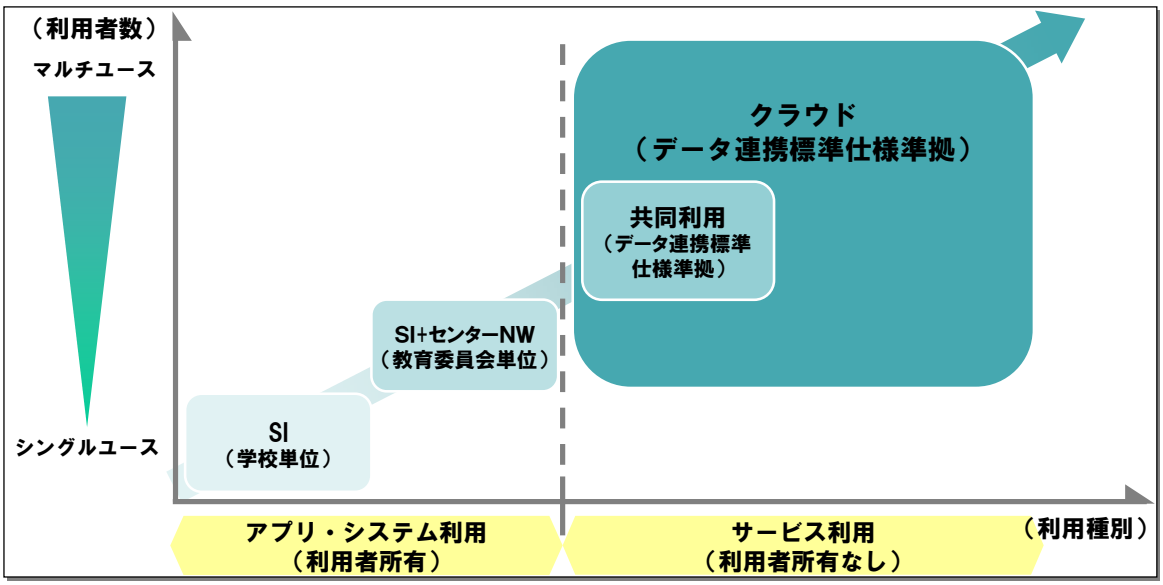
2014年3月
第1．0版

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。

教育分野におけるクラウド利用を考える場合、幼児教育や生涯学習など教育全般を視野にいれることが本来と考えられるが、ライフステージ全般に渡る検討が必要となることから、本書においては学校教育に範囲を限定し具体的な記述とするよう心がけた。

なお、教育分野のクラウド整備・導入状況について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ったり、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はあるが普及に向けて着実に検討が進められてい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。



目次

1. 教育クラウドの概要 1

1.1 教育クラウドの現在と今後の方向性 1
1.1.1 教育クラウドの必要性とメリット 1
1.1.2 現在進められている教育クラウドの整備状況 2
1.1.3 将来、教育クラウドが目指す方向性 3
1.1.4 省庁の教育クラウドに関連する政策 7
1.2 教育クラウドを構成する要素 15
1.2.1 認証 15
1.2.2 教育プラットフォーム 17
1.2.3 サービス(アプリケーション) 24
1.2.4 教育クラウドに付随する要素 25
1.2.5 教育クラウド利用にあたって留意を要する要素 29
1.3 クラウドの配置モデル 35

2. 教育クラウドの整備 37

2.1 想定する整備シナリオ 37
2.1.1 事前検討・利用条件 37
2.1.2 調達プロセス 37
2.2 整備計画の策定 38
2.3 推進計画 38
2.3.1 導入検討体制 38
2.3.2 運用実施体制 39
2.3.3 スケジュール 39
2.4 セキュリティに関する検討 40
2.5 利活用支援の検討項目 40
2.6 サービスレベル(SLA)の検討 41
2.7 クラウド運用の検討 42
2.7.1 情報セキュリティの確保 42
2.7.2 業務の効率化・標準化、事業継続性の確保 42
2.7.3 段階を踏んだ運用計画 43
2.7.4 ユーザ研修 44
2.7.5 運用・サポート体制 44
2.8 参考文献 45

3. セキュリティ 46

3.1 教育クラウドにおけるセキュリティ 46

3.1.1 概要 46
3.1.2 基本的な考え方 46
3.2 セキュリティポリシー 49
3.2.1 概要 49
3.2.2 セキュリティポリシーの適用パターン 49
3.3 セキュリティに関する検討事項 51
3.3.1 不正アクセス対策 51
3.3.2 データセンターのセキュリティ 51
3.3.3 サーバ、システム設計における情報セキュリティ 52
3.3.4 ネットワークのセキュリティ 53
3.3.5 クライアント PC のセキュリティ 56
3.3.6 データ持ち出しに関するセキュリティ 57
3.3.7 リモートアクセス 58
3.3.8 サービス事業者のセキュリティ要件 59
3.3.9 セキュリティ研修 61
3.3.10 学校現場のセキュリティ監査 61
3.4 参考文献 61
4. サービス調達 63
4.1 サービス調達 63
4.2 サービスレベル 64
5. 将来の課題 67
5.1 教育クラウドの整備に関する将来の課題 67

1. 教育クラウドの概要

1.1 教育クラウドの現在と今後の方向性

1.1.1 教育クラウドの必要性とメリット

教育クラウド関連の様々な政策を背景に、今後クラウドを活用した本格的な普及・展開がますます高まってくると予想される。日本教育工学振興会が平成 23 年度に実施した「教育コンピュータ等に関するアンケート調査（教育委員会 183 団体、公立小中学校 2,998 校）」でも「授業や補修・進学指導のために、教材コンテンツやデジタル教材、プリント教材、教員の自作教材等を広く地域内で共有できる仕組みを構築すべきである（教育クラウド化）」の質問に対して「強くそう思う」「そう思う」を合わせて 84.1%と高い数値となった。

それでは、教育センターや学校に配置されているサーバやアプリケーションをクラウド化した場合の利点はどのようなことがあるのか。以下にクラウド環境を利用するメリットを述べる。

（1） セキュリティ対策

学校は校務・授業に関する情報や保護者・地域に関する情報など数々の情報資産を保有している。特に校務に関する情報は、成績情報や生徒指導情報、個人情報などセンシティブな情報も存在する。クラウドを配置するデータセンターでは、サービスを中断することなく利用者から預かっている情報を安全に維持していくとともに、情報の流出や漏えい対策などの情報セキュリティ対策も求められるため『強固なセキュリティ対策』『システムの冗長化』『24 時間 365 日の監視体制』『UPS・自家発電設備設置』など、様々なセキュリティ対策やデータ保全の仕組みが施されている。

現在 ASPIC では、クラウドサービスを提供している事業者向けに情報開示の認定制度を行い、安全・信頼性に係る実施水準や状態に関する情報を定めることにより、利用者がサービスを比較・評価・選択するための認定制度を実施している。クラウドにおけるサービスの内容や品質は SLA（サービスレベルに関するサービス品質保証契約）に明記されており「契約書」という形で品質が保証されるため、利用者は機能とコストのバランスを考慮してサービスを選択することができる。

（2） サーバ維持管理（運用最適化）

学校では職員室やコンピュータ教室にサーバが設置されているケースが多いが、各学校でサーバを管理するには専門知識が必要となり、障害を未然に防ぐ対策や障害が起きた場合など運用面では大きな負担となる。クラウド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、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し、利用者がシステム管理の面で労力を費やさなくて済む点にあり、環境維持・管理などの作業負担から学校を解放することができる。

（3） 柔軟性・拡張性

クラウド環境では、サーバの性能（CPU・メモリ）や使用した割合（データ量や利用時間等）に応じて課金される仕組みが提供されている。そのため、段階的なサーバの増設や時期に応じてサーバ性能を強化できるため、年度ごとの学校数の増加や、高負荷がかかる時期にサーバ性能を強化することが可能である。例えば、校務システムの場合、モデル校での試験運用から始める場合や成績処理や要録作成時（期末や年度末等）など負荷が集中する場合にサーバ性能を強化することが可能となる。

教育の情報化を進める上で柔軟な導入計画の立案を可能とするとともに、運用期間や利用シーンの拡大に伴って必要となる大容量化にも極めて有効な対策となる。また、これらを通して教材や学習の記録などのデータの蓄積・共有や、学校～家庭間の共通的な利用などの将来的な利用シーンに備えることも考えられる。

（4） 共同利用によるコスト軽減

クラウド環境では自治体にまたがる共同利用が可能であることから、ハードウェア調達、システム更新、基礎的な運用などの費用が共同で調達されるとともに各年度の費用負担を平準化できるメリットがある。一方、サービスを共同で利用することから、業務や運用ルールの統一などの工夫も必要。

（5） BCP 対策

最近注目されているクラウド利用のメリットとして BCP 対策（業務継続計画）がある。クラウドを運営しているデータセンターでは耐震対策が十分にとられているほか、現地と距離を置いた場所に設置されていることが多いことから、データ保全についても安心して活用できる環境を用意できる。特に校務システム等で取り扱う成績情報や個人情報などのセンシティブ情報が多く存在することから、セキュリティ確保されたクラウド環境での運用が必要となる。

以上、教育クラウドの必要性とメリットについて簡潔に述べたが、インターネット回線を通じて利用するケースでは、不通になった場合利用することができない。また、現在の教育ネットワークの多くが学校から教育センターを通じてインターネット回線を利用するため、特に画像や動画など大容量のデータを取り扱う場合、ボトルネックになる可能性があるなどの留意も必要である。

1.1.2 現在進められている教育クラウドの整備状況

（1） 先進的な自治体における整備状況

教育クラウドの定義は現在も議論が続けられているところだが、既に先進的な自治体では工夫を凝らしながら様々な取組が進められている。

これら先進的な自治体では中期的な計画の中で、教育現場に提供するシステムをクラウドサービスとして利用する形態へと継続的な整備が進められており、自治体が整備したデータ

センターもしくは自治体エリア内の民間事業者が提供するデータセンターを活用する形で実現される例が多数を占めている。本書で後述するところの、いわゆるプライベートクラウドに相当する。

一方で、民間事業者が提供するサービスをそのまま利用する(いわゆる)パブリッククラウドや、プライベートクラウドに一部のパブリッククラウドから提供されるサービス（SaaS）を組合せたハイブリッドクラウドの活用も実例として出始めている。

（2） 一部で始まったパブリッククラウド活用への大きな流れ

教育の情報化に向けて、どのようにクラウドサービスを活用していくかはそれぞれの自治体における整備計画やポリシーによるところではあるが、従来からコンテンツマネジメントシステム（CMS）や緊急情報連絡網など個人情報を扱う必要のない機能のパブリッククラウド利用は存在したものの、個人情報を含む校務支援システムまでパブリッククラウド利用が始まっているところが近年の特徴的な動向といえる。

過去の整備計画との整合性や、自治体毎の個人情報の扱いやセキュリティポリシーにより進め方の違いはあるものの、個別に整備するクラウドからパブリッククラウド利用への大きな流れが始まっていると考えられる。

（3） 教育クラウド利用に向けた課題

一方で、このような流れが始まっている現時点だからこそ必要となってくるのは、将来的な教育クラウドの実現イメージや活用シーンによる方向性の共有と、現在進めている計画と将来イメージを摺り合わせながら、負の遺産化リスクを排除する計画見直しと考えられる。

APPLIC 教育 WG ではこのような必要性を踏まえ、本ガイドブックにおいて将来の教育クラウドのイメージを記載する試みを実施することとした。教育クラウドについては、今後も様々な議論がなされ本ガイドブックとは異なる方向性が提示されることも想定されるが、そのような議論の題材となることも含め記載を進めることを了承いただけることを望んでいる。

1.1.3 将来、教育クラウドが目指す方向性

ICT を活用した他の情報システムと同様、教育クラウドにおいても取得した情報の利活用とそれにより得られる結果を最大限教育現場にフィードバックすることで、利用者利便の最大化を目指す必要がある。

しかしながら、ここにはハードルも存在する。教育クラウドの全体像と利活用のイメージが共通認識化していない現時点においては当然のことも言えるが、教育クラウドの利用を通じて得られるログや履歴情報の活用は、どこまでが許容範囲か社会的なコンセンサスが得られるところまで議論されていない。また、番号制度導入後の教育分野における利活用に向けては、教育クラウドのイメージを再度検証する必要があると考えられる。

このような課題が存在することを認識しつつも、本書においては技術的な側面から教育クラウド

のイメージを描くこととした。ここで扱う教育クラウドは、より広く大きな括りのクラウド環境から、教育現場により貢献するための情報をフィードバックし、自治体の範囲を超えて如何に効率的かつ経済的に実現するかといったアプローチからの可視化を目指すものである。

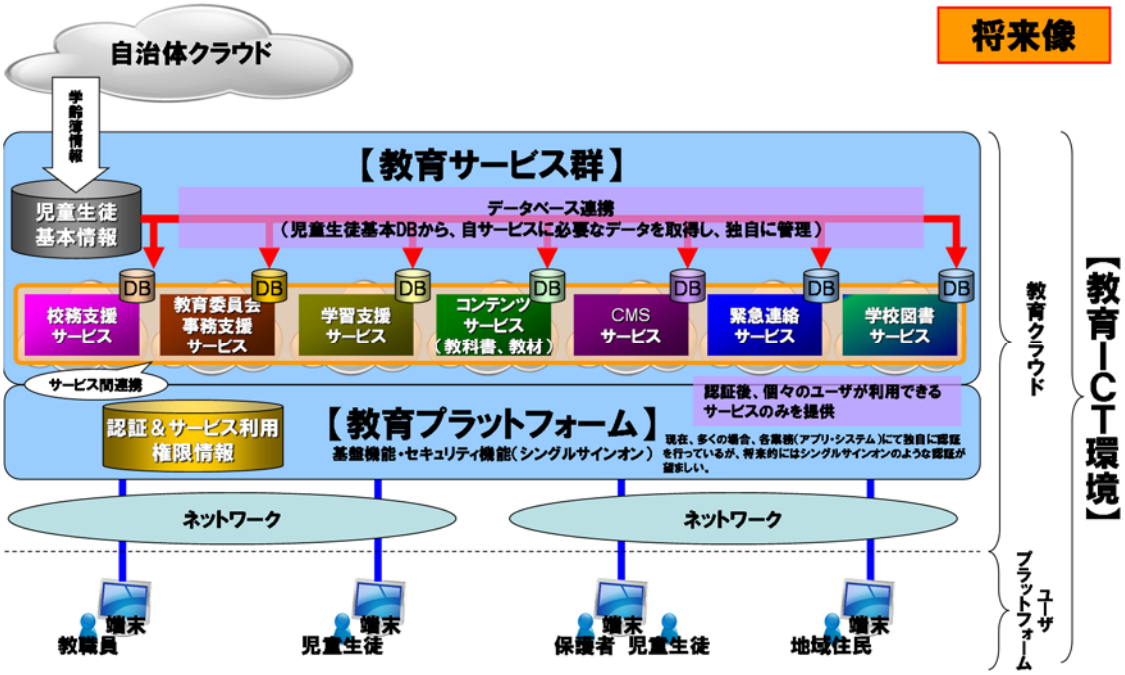
今後、各方面で交わされる活発な議論により、教育クラウドがより貢献度の高いモデルへと育っていくことを期待したい。

（1）教育クラウドの基礎的な要件

ここでは、現時点では実現されていない部分も含め教育クラウドの将来イメージを記載することとし、基礎的な要件と考えられるポイントを下記①～⑤の項目と仮定した。

① 利用者は学校（教育委員会を含む）の教職員、児童生徒、保護者（必要に応じて地域住民）
② 利用場所は学校（教育委員会を含む）、家庭、地域、など（いつでも、どこでも）
③ 将来、教育現場（家庭学習を含む）での利用が想定されるアプリケーションは、利用者にユニークな認証にて権限の範囲で全てが利用可能
④ それぞれのアプリケーションに保有する情報は、利用者をキーにして呼び出しもしくは名寄せが可能
⑤ 教育クラウドを構成する各機能が生成するログ情報は、必要に応じてビッグデータとしての活用が可能

これら①～⑤の要件を可能とする教育クラウドをイメージ化すると下図のとおり。システム的なアプローチから描いているため、今後、教育的な見地からも検証が必要。



（2） 利用者（教育委員会、教員、児童生徒、保護者、等）からみた教育クラウドの活用シーン

① 教育委員会、学校

- 従来、紙で学校保存していた各種情報が電子データとなりデータセンターに保存されることから、必要なセキュリティ対策を施すことで場所にとらわれない利用が可能。同時に災害および事業継続性の対策としても有効。
- データの利活用度合いが高まると同時に、統計処理などにも柔軟性が増すことで、業務の生産性向上が期待できる。
- データ連携を実現させることで、複数の業務アプリケーションにまたがる情報を名寄せし、学習者に多面的なフィードバックをするための指導情報を得ることができる。
- 蓄積した履歴を利用することで学習者のつまずきを発見し、その後のフォローアップに活かすことができる。
- 一人一人に応じた指導を実施するための情報取得が可能。

② 児童生徒（学習者）

- 教室に限定されない学びの機会と環境が得られる。
- 教室での一斉学習、教室外での個人学習の他、コラボレーションによる学びなどの学習スタイルの選択肢が拡大。
- 小中学校や高等学校などの学校種別や学年、居住地域などに捕らわれない、理解の進度に応じた学習を可能とするコンテンツが利用可能。
- 各種統計データにより自分自身の得意な部分や苦手な部分の把握をはじめ、学習進度や総合的な理解度を自己分析できる。
- 学校や地域に閉じないコミュニケーション機会の獲得。

③ 保護者、地域

- 校務情報の一部を利用することによる、学校内の様子や学習の実施状況など、校内における児童生徒の活動の共有。
- 学校～家庭・地域間コミュニケーションの活性化。
- 家庭にいながら、公平な学習サービスの提供を受けることができる。

（3） 教育クラウドイメージ実現に向けて更なる検討が必要な項目（制度・仕組・財政、技術、学校運営、地域・家庭、など）

① 制度・仕組・財政

- 自治体毎に点在する教育クラウドの成長シナリオ策定と実行に向けたプロセスの設計。
- 個人情報などのセキュリティを確保した上で可能とする各種データの基本利活用ポリシーの形成。

② 技術

- 教育クラウドに提供するサービスや基盤システムの必要最低限の仕様情報のオープン化。
- コンテンツやアプリケーション、ログデータや履歴情報の標準化の推進。

③ 学校運営

- 学校アセスメントなど運営オープン化に関する議論とコンセンサスの形成。
- 学校の見える化の進展に対応した業務プロセスの形成。

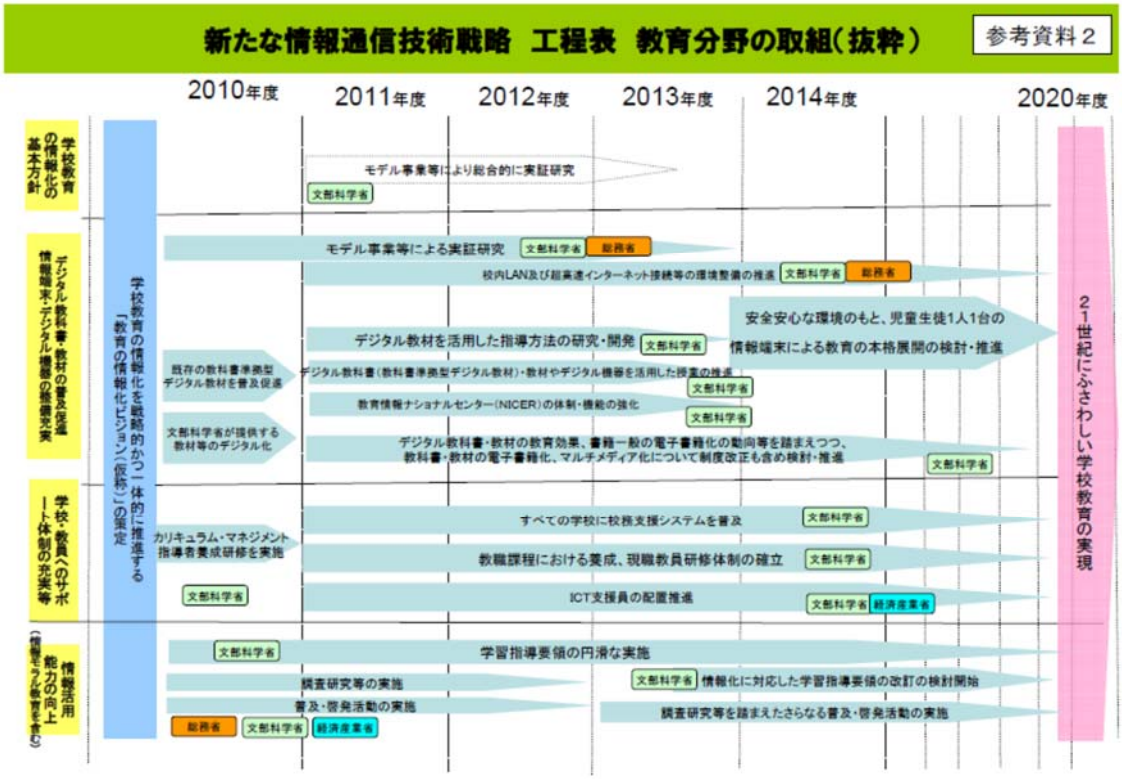
④ 地域･家庭

- 学校を支える（支援する）地域社会としての積極的な役割分担と理解。

検討が必要な項目は多数あるものの、教育クラウドは教育に新たなイノベーションをもたらす可能性を持っている。後述する「1.2　教育クラウドを構成する要素」では技術的なイメージを記載していく。

1.1.4　省庁の教育クラウドに関連する政策

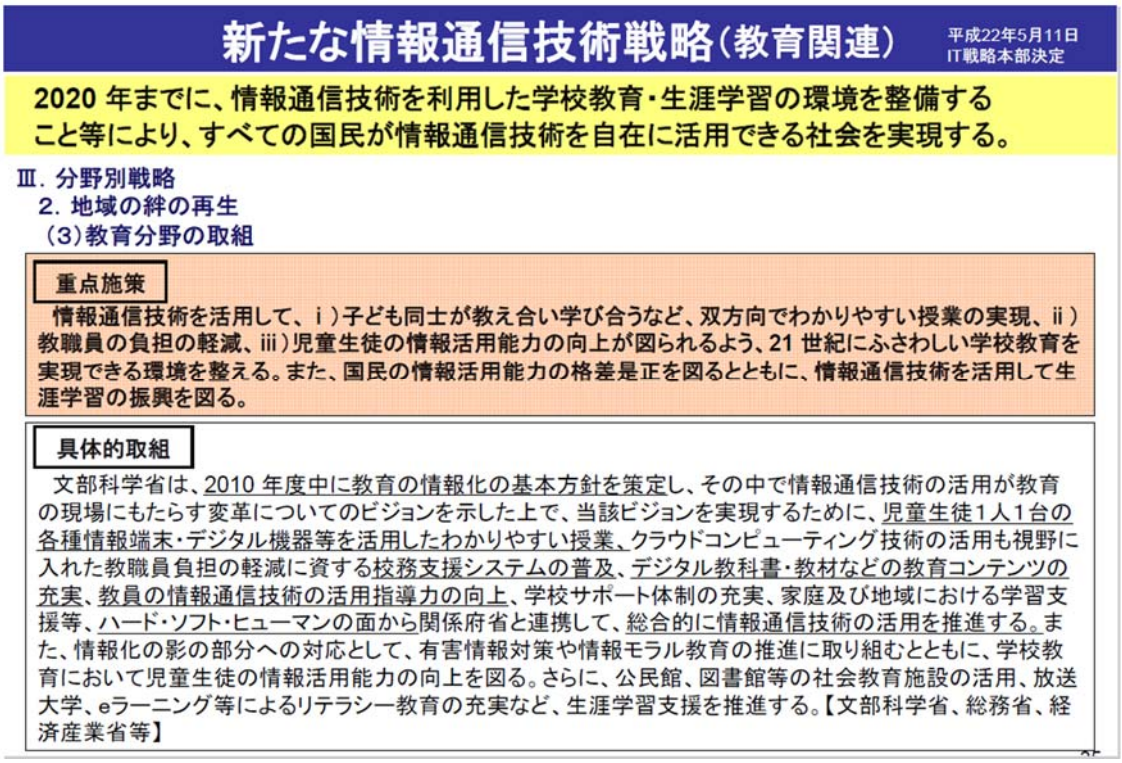
教育クラウドに関連する政策は2010年まで遡る。6月18日に閣議決定された新成長戦略において政府IT戦略本部が定めた新たな情報通信技術戦略工程表」の中では、2020年までに「児童生徒1人1台の情報端末の整備」や、「デジタル教科書・教材の導入」等が計画された。これを受けて各省庁では、教育クラウドに関する検討も開始された。



※IT 戦略本部「新たな情報通信技術戦略　工程表」（抜粋）より

（1） 新たな情報通信技術戦略（教育関連） 2010 年 5 月 11 日 IT 戦略本部

2010 年 5 月に IT 戦略本部より「2020 年までに、情報通信技術を利用した学校教育・生涯学習の環境を整備すること等により、すべての国民が情報通信技術を自在に活用できる社会を実現する」との戦略立案があり、具体的取組みとして「クラウドコンピューティング技術の活用も視野に入れた教職員負担の軽減に資する校務支援システムの普及・推進」について提言された。



新たな情報通信技術戦略（教育関連） 平成22年5月11日 IT戦略本部決定

2020 年までに、情報通信技術を利用した学校教育・生涯学習の環境を整備すること等により、すべての国民が情報通信技術を自在に活用できる社会を実現する。

Ⅲ. 分野別戦略
2. 地域の絆の再生
（3）教育分野の取組

重点施策

情報通信技術を活用して、ⅰ）子ども同士が教え合い学び合うなど、双方向でわかりやすい授業の実現、ⅱ）教職員の負担の軽減、ⅲ）児童生徒の情報活用能力の向上が図られるよう、21 世紀にふさわしい学校教育を実現できる環境を整える。また、国民の情報活用能力の格差是正を図るとともに、情報通信技術を活用して生涯学習の振興を図る。

具体的取組

文部科学省は、2010 年度中に教育の情報化の基本方針を策定し、その中で情報通信技術の活用が教育の現場にもたらす変革についてのビジョンを示した上で、当該ビジョンを実現するために、児童生徒1人1台の各種情報端末・デジタル機器等を活用したわかりやすい授業、クラウドコンピューティング技術の活用も視野に入れた教職員負担の軽減に資する校務支援システムの普及、デジタル教科書・教材などの教育コンテンツの充実、教員の情報通信技術の活用指導力の向上、学校サポート体制の充実、家庭及び地域における学習支援等、ハード・ソフト・ヒューマンの面から関係府省と連携して、総合的に情報通信技術の活用を推進する。また、情報化の影の部分への対応として、有害情報対策や情報モラル教育の推進に取り組むとともに、学校教育において児童生徒の情報活用能力の向上を図る。さらに、公民館、図書館等の社会教育施設の活用、放送大学、eラーニング等によるリテラシー教育の充実など、生涯学習支援を推進する。【文部科学省、総務省、経済産業省等】

※文部科学省「教育の情報化推進施策等について」より

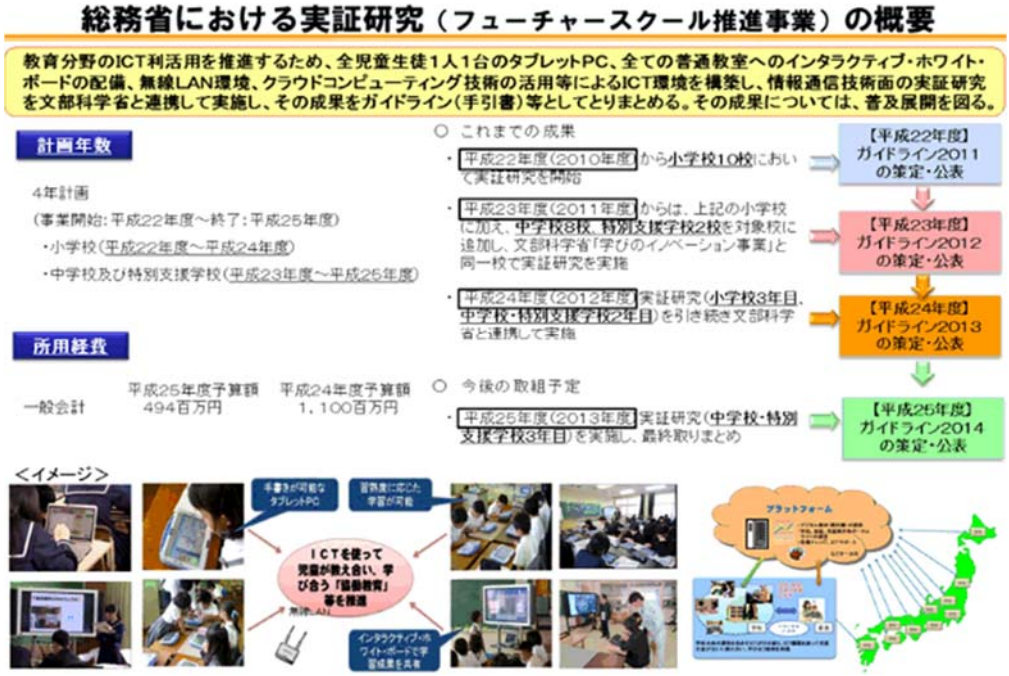
（2） 教育の情報化ビジョン　　2011 年 4 月　文部科学省

この戦略を受け、文部科学省では 2011 年 4 月に「教育の情報化ビジョン」を策定し、21 世紀にふさわしい学びと学校の創造を目指してクラウド時代に備えたソフト・ハード・ヒューマンの充実と学びのイノベーションに向けたビジョンが示され、校務の情報化においては、「クラウドコンピューティング技術の活用等」について試行的な取組みを行いつつ検証する旨が言及されている。

※文部科学省「教育の情報化ビジョン」より

（3） フューチャースクール推進事業　　2010 年～2013 年　総務省

総務省では、2010 年より小中学校における児童生徒 1 人 1 台の情報端末の整備を通じた各種実証実験を行う「フューチャースクール推進事業」が実施され、教育分野の ICT 利活用を推進するため、全児童生徒1人1台のタブレット PC、全ての普通教室へのインタラクティブ・ホワイト・ボードの整備、無線 LAN 環境、クラウドコンピューティングにおける技術の活用等による ICT 環境を構築し、情報通信技術面の実証研究を文部科学省と連携して行った（2010 年度：小学校 10 校、2011 年度中学校 8 校＋特別支援学校 2 校）。

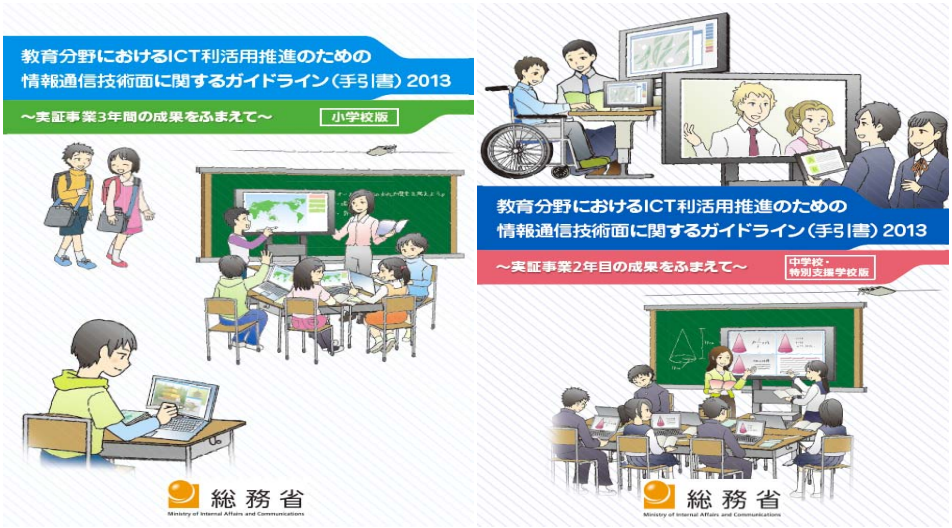


※総務省　フューチャースクール推進事業 HP より

（4）教育分野にける ICT 利活用推進のための情報通信技術面に関するガイドライン（手引書）2013

2013 年 4 月　総務省

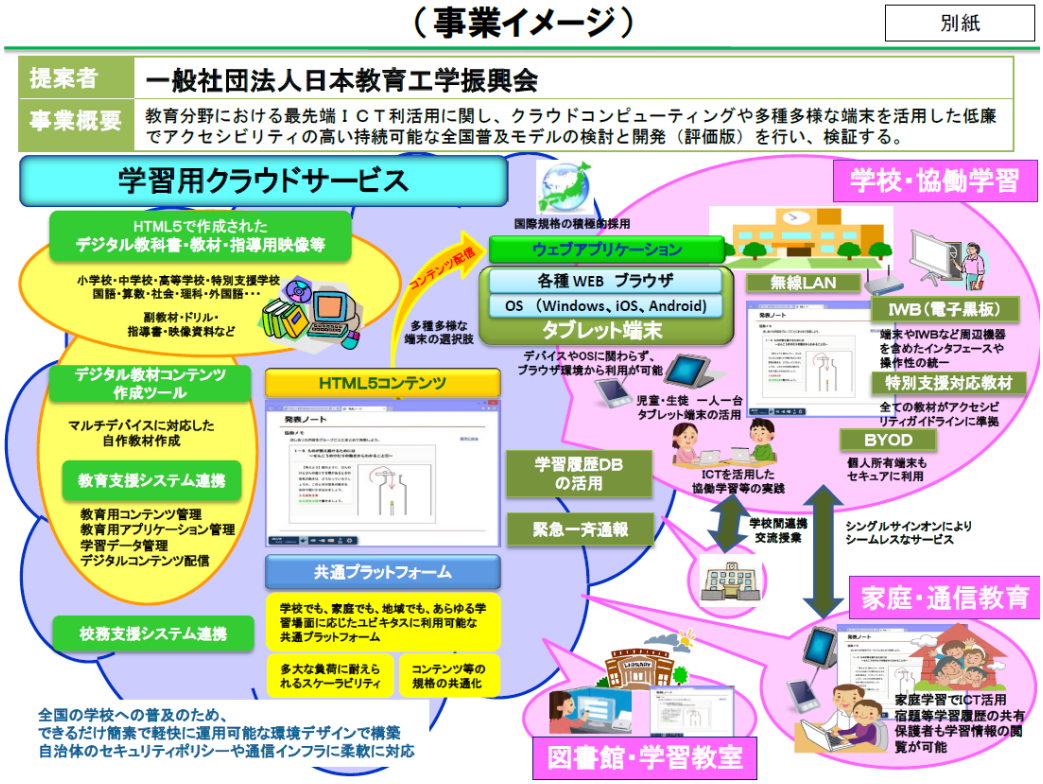
総務省が、これまでの「フューチャースクール推進事業」の成果を踏まえ、学校現場における ICT 環境の構築や運用、利活用の際の情報通信技術面に関わるポイントや留意点について、教育関係者の具体的な取組や地方自治体の導入の参考となるとともに、導入のきっかけとなるように、「小学校版」及び「中学校・特別支援学校版」のガイドラインをそれぞれ策定した。このガイドラインは 2014 年度も刊行される予定であり、「学校現場におけるクラウドコンピューティング技術活用に関する要件の整理」や「将来におけるクラウド活用にむけた課題・解決策」についても議論されている。



※総務省　「教育分野における ICT 利活用推進のための情報技術面に関するガイドライン（手引書）2013」より

（5） 教育分野における最先端 ICT 利活用に関する調査研究　　総務省

これまでの実証研究（フューチャースクール推進事業）で判明した運用上の対応では解決できない課題について、技術的な解決を図るとともに、本格的な普及・展開を見据えて、クラウドコンピューティング技術を最大限活用し、学校と家庭がシームレスでつながる教育・学習環境の構築に向けた調査研究が開始され、一般社団法人）日本教育工学振興会が主体となり調査研究がすすめられている。



※総務省 「教育分野における最先端 ICT 利活用に関する調査研究」」より

（6） 教育振興基本計画　　2013 年 6 月 14 日閣議決定

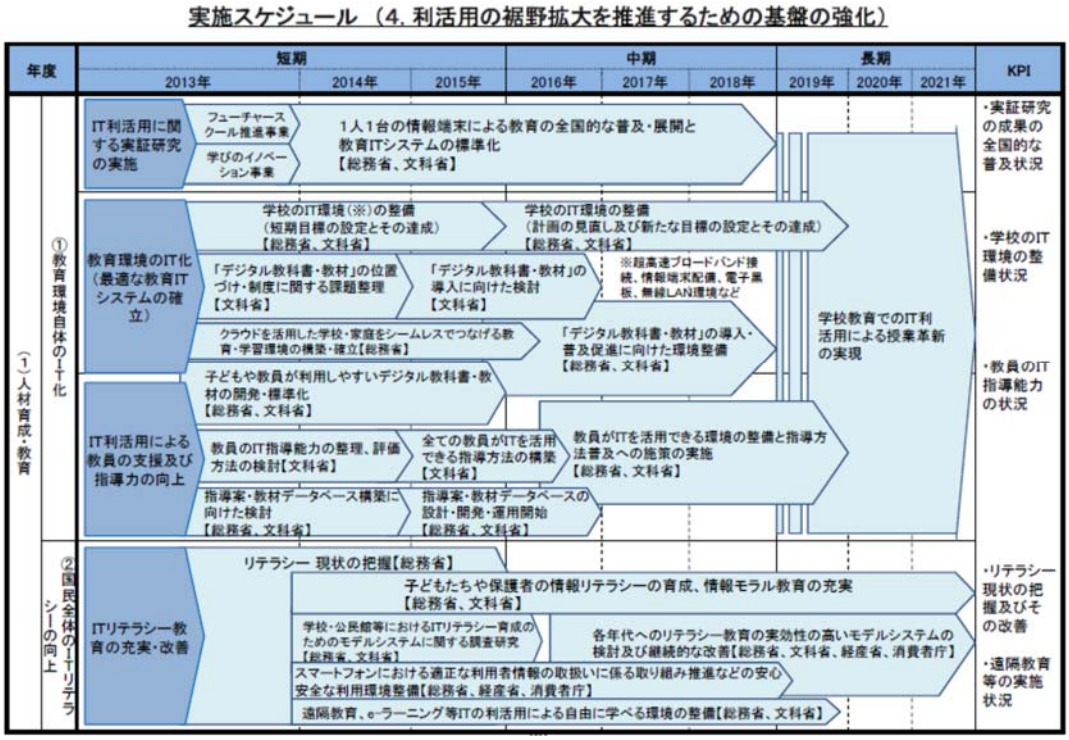
平成 25 年 6 月 14 日に第 2 期の教育振興基本計画が策定され、各学校間や、学校教育と職業生活等との円滑な接続を重視し、「社会を生き抜く力の養成」など、生涯の各段階を貫く4つの教育の方向性が示された。その基本政策25の中で「良好で質の高い学びを実現する教育環境の整備の中で教材等の教育環境の充実」が提言され、教育クラウドの導入を想定した記載がされている。

（記載内容）

- 教育用コンピュータ1台当たりの児童生徒数3．6人（※），教材整備指針に基づく電子黒板・実物投影機の整備，　超高速インターネット接続率及び無線LAN整備率100％，校務用コンピュータ教員1人1台の整備を目指すとともに，地方公共団体に対し，教育クラウドの導入やICT支援員・学校CIOの配置を促す。

（7） 世界最先端 IT 国家創造宣言　　2013 年 6 月 14 日閣議決定

IT 総合戦略本部では、未来を創造する国家ビジョンとして「世界最先端 IT 国家創造宣言」（平成 25 年 6 月 14 日閣議決定）を策定、人材育成・教育面として教育環境の IT 化を促進し、「2015 年度末までに、クラウドを活用した学校・家庭をシームレスでつなげる教育・学習環境を構築、確立する。」との目標が掲げられている。



※IT 総合戦略本部 「世界最先端 IT 国家創造宣言工程表」より

1.2 教育クラウドを構成する要素

1.2.1 認証

教育クラウドのプラットフォームを検討するにあたり、従来の閉じられたネットワーク、学校を中心とした制限された利用環境ではなく、家庭等、学校外でも学習ができる利用環境及び利用者についても教職員や児童生徒だけではなく保護者やボランティア団体や地域住民等も含め検討する必要がある。また現在の校務や教育サービスも多様になり、多くの企業がサービスを提供することが想定される。また利用する機器は単一の OS や機種、形状に制限することができず、多様な機器に対応するシステムが想定される。

これらの環境における認証に求められる機能及び課題は次の通りと想定している。

（1） 教育サービス提供

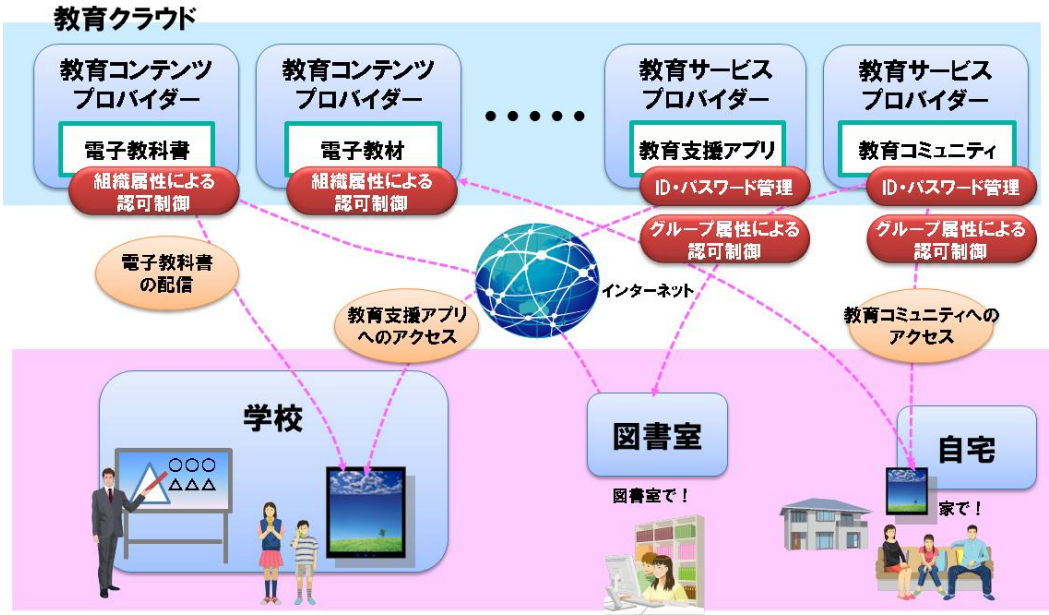
教育クラウドからの教育サービス提供は学校外部、もしくは教育委員会ネットワークの外部からのサービス利用を想定した利用者の権限管理が重要となる。一般的な商用サービスでは、個人毎に権限管理されているが、現在のコンテンツの許諾やサービス提供、契約の単位から教育委員会、学校、学年単位などの組織の利用許諾を許可できる認証が現実的と考える。さらにそのコンテンツやサービスの利用状況の確認及びサービス自体を保護者が利用することも想定される。その際の児童生徒と保護者の関連性の紐づけなどが課題となる。

（2） 学習データの蓄積

教育クラウドで教育サービスを提供し、児童生徒一人一人の学習データ（学習履歴や成果物）の蓄積を行うためには、個人ごとの各アプリケーションやサービスで学習したデータと認証とを紐づける必要がなる。また学習データは児童生徒自身だけではなく、教職員や保護者のアクセスも想定する必要がある。そのためには、教育サービスを提供している企業が児童生徒、教職員、保護者の各個人の認証情報と属性を管理するとともに、年次の異動処理や家庭等の異動が発生した際の処理を行う必要がある。

（3） 協働学習を想定したグルーピング

教育クラウドでは協働学習を想定したグルーピングを柔軟に行う必要がある。児童生徒がクラス単位はもちろんのことクラス内外のグループ単位、更に学校を超えた形で、様々な教育コンテンツや教育データを共有して学習するための権限管理が必要になる。しかしそのためには個人属性やグループ属性を各組織や企業が行うことが必要となり、煩雑な対応が必要となる。



教育クラウドに必要となる認証機能

以上を踏まえ、今後の教育クラウドに必要な認証基盤は次のような機能が必要となる考えられる。

1. 学校外での利用を前提とする認証基盤
2. 教職員、児童生徒だけではなく、保護者や地域住民も含めた認証
3. 低学年の児童生徒も想定したユーザビリティ(顔認証等)
4. 多種多様な情報端末に対応した認証
5. さまざまなサービスに対応したシングルサインオン
6. 学習履歴データと児童生徒、保護者、教職員との紐づけ管理
7. 学校現場での児童生徒のグルーピング管理
8. 児童生徒・教職員・保護者を含めた異動処理

また以上の機能のを達成するにあたって、自治体の限られたコストで実現する必要があるため、管理機能及び運用コストを抑えるようなシステムが必要となる。

今後求められる認証基盤

従来の市町村単位のプライベートクラウドにおいては、クラウドサービスの契約者と提供範囲が同じであるため(例:ある自治体が契約したプライベートクラウドはその自治体の学校にのみサービスを提供する)、提供されるサービスやコンテンツの契約や異動処理等はその自治体向けにカスタマイズし、自治体内だけに通用するルールにのっとって運用が可能である。

またパブリッククラウドにおいても、パブリッククラウド提供者があらかじめ用意するサービスやコンテンツのみ利用し、パブリッククラウドのルールに従って運用可能であれば大きな問題にならな

い。

しかし、いずれにおいても今後出現するであろうインターネット上の様々な教育サービスを活用するにあたって、独自の認証基盤を構築すると認証連携や個人情報の取り扱いなどで個別カスタマイズの発生やそもそも連携できないなどの問題が出てくる可能性がある。

またサービス提供者においても、各利用自治体にあわせた認証方法や個人情報の取り扱いに対応せざるを得ず、運用負担の増加やコストの増加を招く可能性がある。

これら今後増加するであろう教育サービスを低コストかつ不必要な個人情報を外部に出すことなく利用できる先行事例として考えられるのは、大学における認証フェデレーション（学認）が想定される。

大学においては、電子ジャーナルをはじめとして様々なクラウドサービスを利用している。その認証は大学のキャンパスネットの IP による制御や ID によるログイン管理方式を取っているが、学校外からのアクセスができないや、複数の ID パスワードを利用する必要があり、学生の利便性が落ちていた。その解決として、国立情報学研究所（NII）が中心となり学校の認証基盤を活用した認証フェデレーションとよばれるものを構築した。認証フェデレーションは SAML 等の認証技術を利用して、フェデレーション運営組織が定めるポリシーによって各大学の認証基盤（IdP）と各サービス提供者（SP）が信頼関係を結んでいくものである。信頼関係が構築されると利用者は学校で利用している ID、パスワードを利用し、学外の教育サービスをシームレスに活用することができる。さらにサービス提供者側も学生等の ID、パスワードを個別に管理することなくサービス提供を行うことができるので、運用管理コストを削減することが可能になる。

初等中等教育においても、英国等の教育クラウドで同様の認証基盤が採用されている。

日本においても、今後このような初等中等における教育クラウド向け認証フェデレーションの構築・運用が必要と考えられるが、そのためにはポリシー策定を含む運用ルールの管理組織の在り方など検討すべき事項は多い。これらは今後の検討課題となるであろう。

1.2.2 教育プラットフォーム

教育クラウドのプラットフォームを構築する場合の前提として以下のクラウド基礎技術の検討が必要である。

① 仮想化技術
② 自動化技術
③ クラウド連携技術
④ 業務サービスの見える化技術

教育クラウド特有の検討内容としては、以下の観点からの考慮も必要となる。

① サービス提供規模の大小に応じた柔軟なクラウドサービス
② 個人所有の情報端末の利用を前提とした安心安全な利用環境
③ コンテンツ等の秘匿化、個人情報及び著作権の保護
④ 学習記録・履歴の一元管理とデータの多目的利用を実現する情報供給基盤

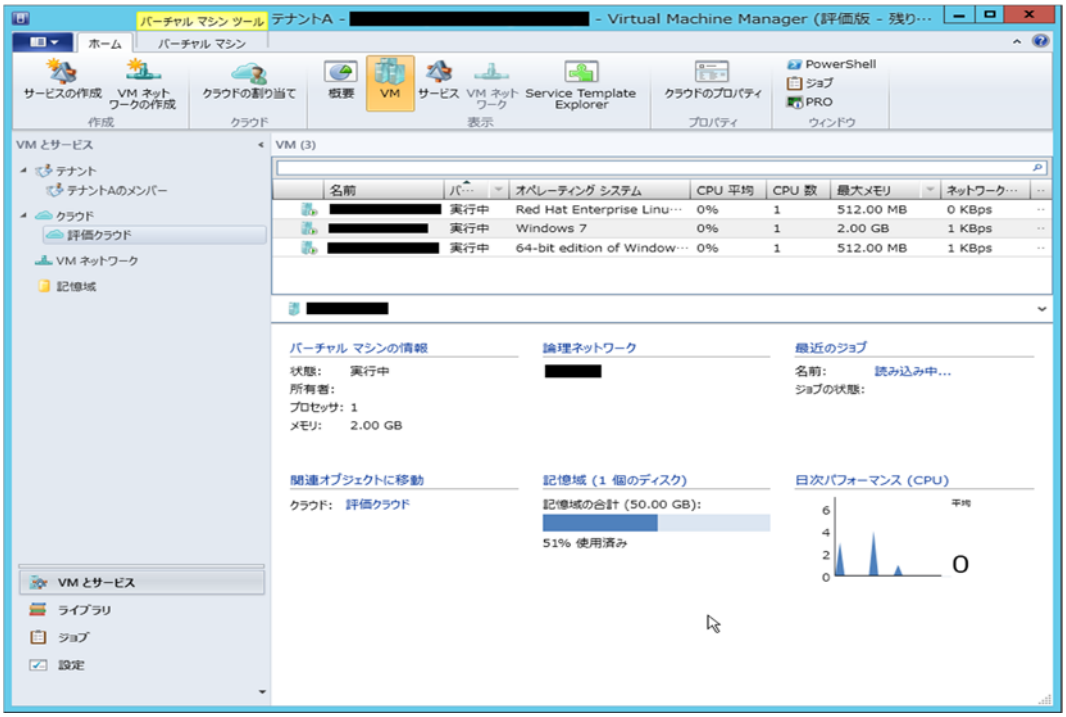
（1） クラウド基礎技術

① 仮想化技術

仮想化技術により、1台の物理サーバ上で複数台の独立した仮想サーバを動作させられるようになった。そのため、複数の異なるシステムで物理サーバのリソースを共有することが有効に活用できる。

一方、仮想サーバへのシステムの割当て方によっては、リソース不足や余剰が発生するリスクも生じる。運用管理者は、リソースを十分活用するために、物理サーバに対する仮想サーバの割当て方を適切に制御しなければならない。このリソース管理は、仮想化により生じた新たな管理作業である。

この管理作業を容易にするため、サーバー・ストレージ・ネットワークといったハードウェアリソースをプール化し、使用状況や空き状況を見える化し、必要なときに必要なだけリソースを割り当てるツールが必要である。



仮想マシンの使用状況

② 自動化技術

仮想サーバに対するミドルウェアのインストール作業やパラメータ設定作業の作業負荷軽減には、あらかじめアプリケーションの動作に必要となる複数台のサーバー・ネットワーク・ミドルウェア構成とそれぞれの設定情報の雛形をあらかじめ作っておき、利用者が要求した際に自動的に必要な仮想イメージが載った複数台の仮想サーバのセットが得られるようにするのが自動配備の技術である。利用者は、必要なときにテンプレートを選択するだけで、いつでも自動的に必要な仮想サーバ一式を得られるようになる。

クラウド化により、利用していた様々なシステムを集約化すると、隠れていた運用負荷が集中し、運用管理者の負担を増大する。

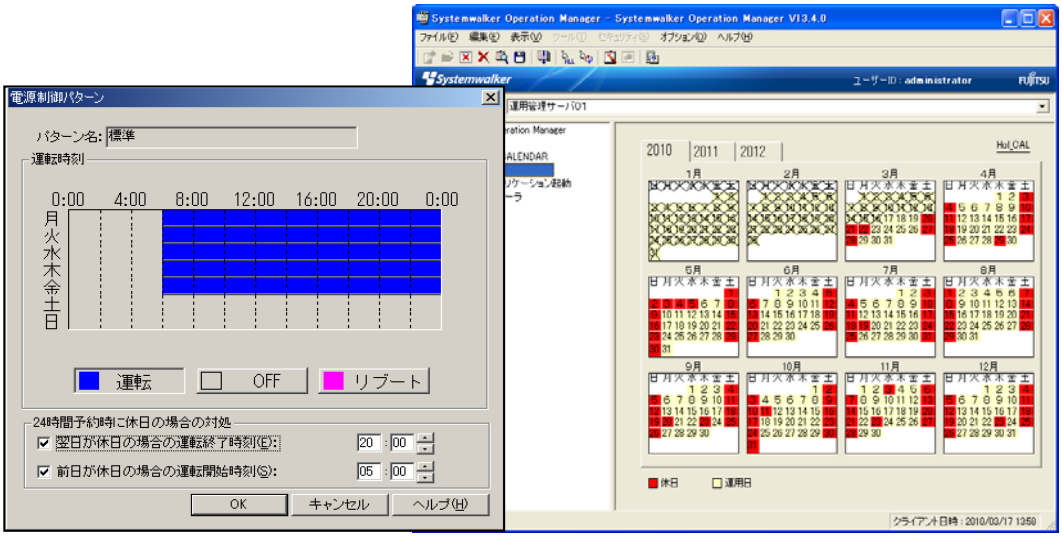
例えば ICT システムの基本的操作である起動手順を考えてみると、以下のような流れになる。

a. 仮想サーバの起動
b. OS とミドルウェアの起動
c. 起動確認
d. 業務アプリケーションの起動
e. 正常動作確認
f. 利用者への公開

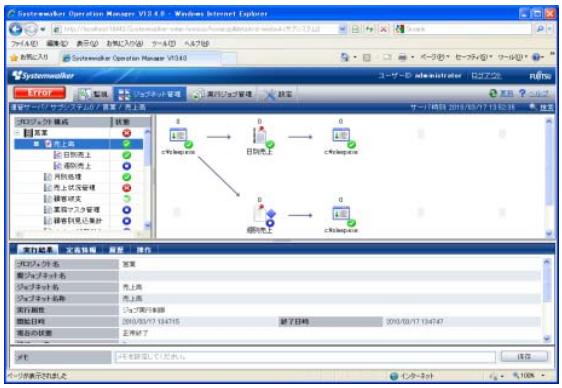
また、途中の操作で異常が検知された場合は、以下の操作を中断し、関係者へ通報するなどの考慮も必要となる。

自動運用機能は、a.～f.のような、サーバ・ネットワーク機器へのコマンド投入、結果の照合、管理者への承認・確認依頼、関係者へのメール送信操作などの複数の対象への操作を作業フローとして定義し、自動実行する機能が必要となる。これにより、作業の効率化に加え人的操作ミスや操作記録の保存が可能になる。

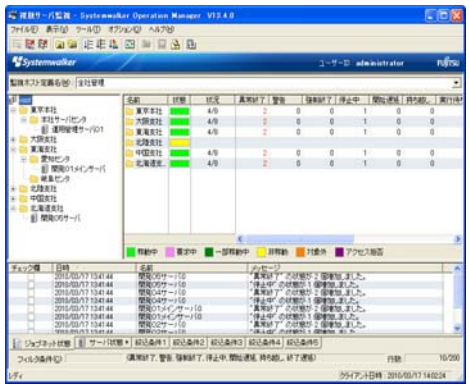
通常のクラウドでは、定期バックアップなども利用者責任となるため費用面の検討とともに、自動化の検討も必要である。



自動実行(ジョブスケジュール)



自動バックアップ



システム全体の監視画面

③ クラウド連携技術

クラウドの構成を考えると、フロント系の業務はパブリッククラウドで提供され、バックエンド系の業務はプライベートクラウドやオンプレミスで提供される場合がある。それぞれの業務間で同じマスターを利用する場合には連携が必要となる。

この連携を実現するためには、以下の技術が必要となる

a. フロント統合

パブリッククラウド・プライベートクラウド・オンプレミス上に散在した業務アプリケーションやサービスの操作を、一つに統合した操作画面から利用することにより、業務担当者の操作性を向上させ、効率良く業務を遂行できるようにする技術。

b. データ統合

各種マスター類などの業務データをパブリッククラウド・プライベートクラウド・オンプレミスに提供して活用したり、蓄積されたデータを活用できるようにする技術。

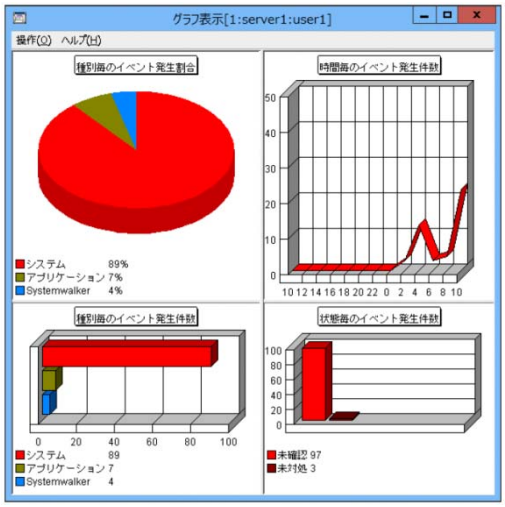
c. プロセス統合

業務アプリケーションとクラウドサービスを連携させた業務プロセスの構築、申請や承認といった人間の判断を必要とする作業を連携させた業務プロセスを構築することで業務全体の統制を実現する技術。

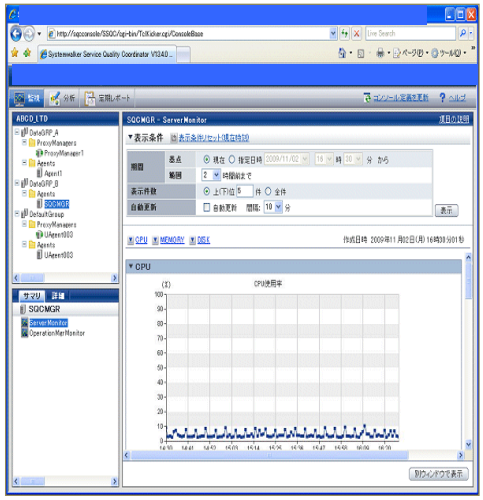
④ 業務サービスの見える化技術

ハードウェアリソースが仮想化により共有化され、必要に応じて貸し出されるようになると、サーバー・ストレージなどのハードウェアの調達コストを特定の業務システムに固定的に割当てられなくなり、業務システムごとの ICT インフラコストの算出が難しくなる。

そのため、クラウド導入では、業務システムが使用したリソース量と時間の把握ができるサービスカタログが必要となる。サービスカタログは、提供されているサービスの一覧、システム構成を確認・操作するセルフマネジメント機能、借用・返却申請の承認フロー、リソース利用量の見える化機能から構成される。



システムの稼働状態



リソース使用状況

（2） 教育クラウド特有の検討内容

① サービス提供規模の大小に応じた柔軟なクラウドサービス

(i) 利用者端末一斉接続に耐えるクラウド環境

児童生徒用の端末台数の増加に対応し、クラウド環境への多数の端末の一斉接続や同一の教材データの一斉利用に対応できるよう、サーバ性能・メモリ容量・ネットワーク性能等を柔軟に対応できるよう設計する必要がある。

また、利用者端末の増加に伴い、端末のシステムメンテナンスを従来のような人手によるものでは対応しきれなくなるため、自動化機能を備える必要がある。

(ii) 学校・家庭からの接続に対応するネットワーク環境

家庭学習の推進のため児童生徒端末を家庭に持ち帰り利用する場合には、学校、家庭それぞれの環境に応じたネットワーク接続を実現する必要がある。家庭からのネットワーク接続の有無への対応や学校での利用環境と家庭での利用環境を分離して、環境にあった利用内容を安心安全に実現する機能が必要となる。

(iii) 既設の校内サーバを不要とする運用環境

業務システムの安全性確保やセキュリティ確保のためには、学校内にサーバを設置するのではなく、校内サーバの果たしている役割をクラウド上に移行する必要がある。また、クラウド連携技術により、業務システム間連携をスムーズに実現する利点もある。このためにはネットワーク性能等の向上、クラウドから提供する運用管理サービスの整理、運用ポリシーの構築が求められる。

② 個人所有の情報端末の利用を前提とした安心安全な利用環境

利用者端末を保護者が購入して学校で利用するBYOD(Bring your own device)が始まっている。これに対応するためには以下の機能の実現が求められる。

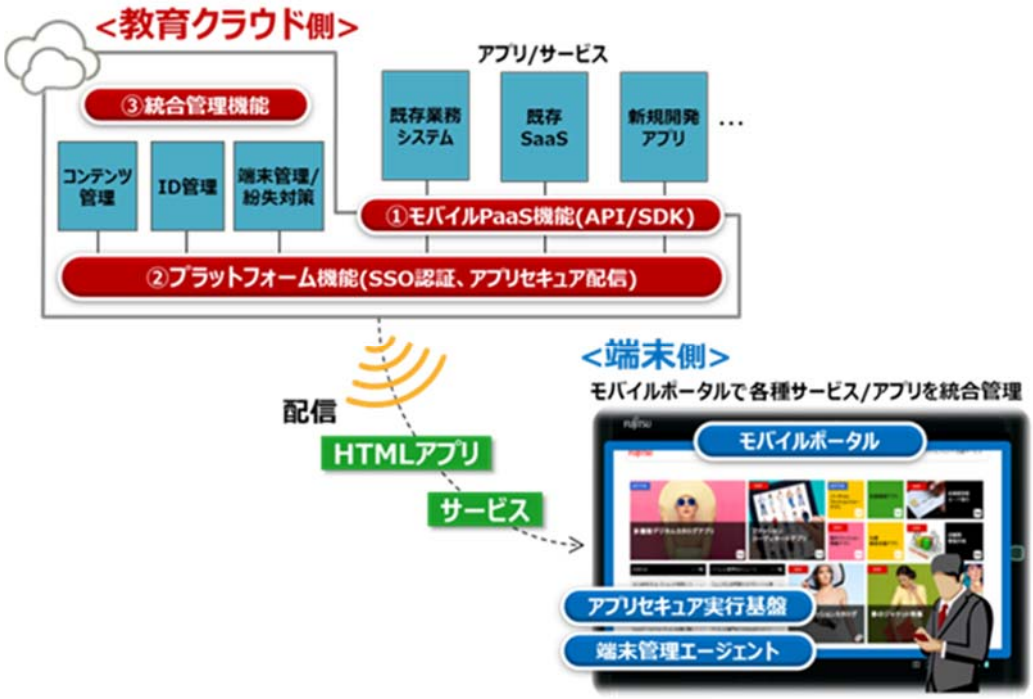
(i) 教育外のアプリケーション(ゲーム等)、インターネット(有害サイト等)など目的外の利用をクラウド側で制限

(ii) 学校・家庭、それぞれの利用環境にあった端末管理サービスをクラウド側から提供

これらの機能を実現するためには、シンクライアント技術やエージェント技術の採用を検討する必要がある。

シンクライアントには、ネットワークブート方式・サーバーベース方式・ブレードPC方式・仮想PC方式などがあるが、広帯域のネットワークと高性能のサーバ性能・OSやアプリケーションのライセンス費用などの課題もある。

最近では端末の高性能低価格化を反映して、端末にエージェントを配置し、クラウドと通信して動作制限や運用管理を行う方法が注目されている。



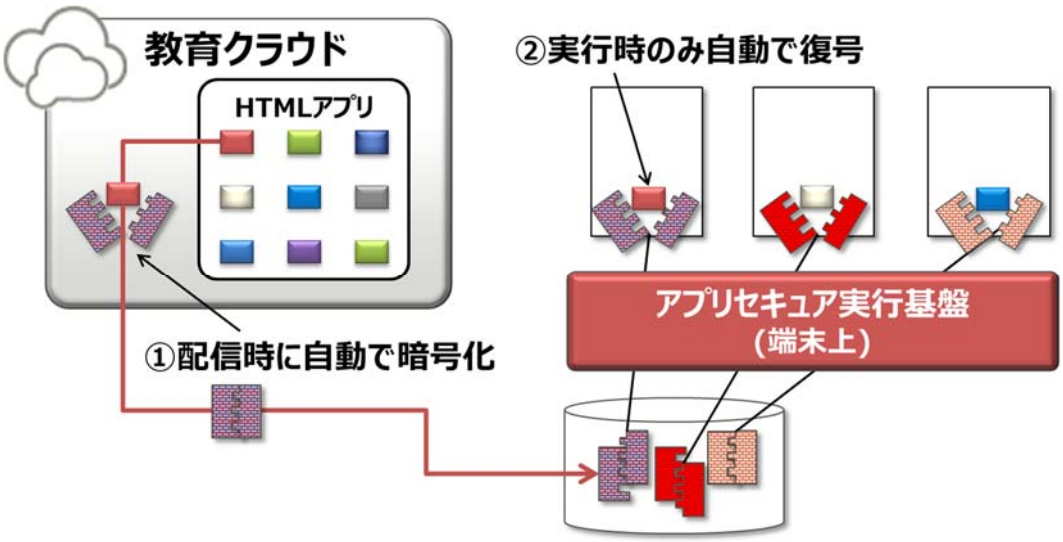
クラウドを利用することのメリットの一つには現地（学校）での ICT 関連の作業・工事を極小化できることがある。現地（学校）では端末だけを用意すれば、教育に必要な機能は全てクラウドから提供されることが理想的と考えられる。しかし、一方で、端末の管理・マネジメントのためには何らかのソフトウェアやエージェントを端末へ導入した方が望ましいケースも考えられる。

想定される運用を考慮しつつ、現地（学校）での負荷を増やさないよう、クラウドサービスの利用、ソフトウェアやエージェントの端末導入を考慮すべきと考えられる。

③ コンテンツ等の秘匿化、個人情報及び著作権の保護

コンテンツ提供者の権利を護り、利用者の個人情報の保護を実現するためには教育クラウドに以下の機能が必要となる。

(i) 上り・下りの双方向の通信における保護
(ii) コンテンツ／成績情報の改竄防止、保護



④　学習記録・履歴の一元管理とデータの多目的利用を実現する情報供給基盤

教育クラウドの利用により、各種情報の多目的利用が実現できる。このため以下の機能の実現に向けた検討が望まれる。

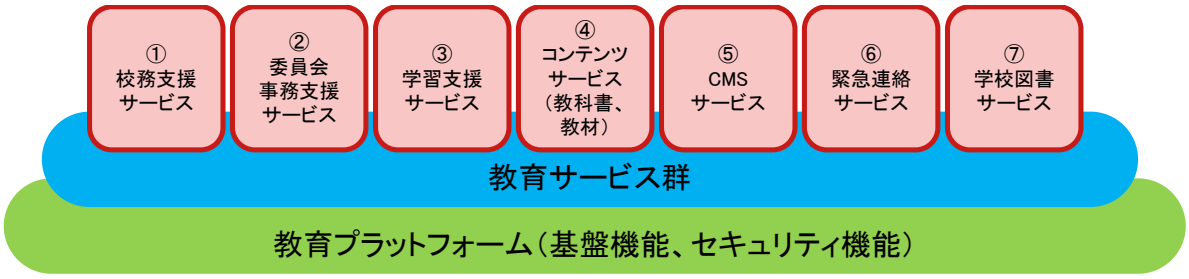
(i)　利用者個人が作成したコンテンツ・データのクラウド上での集約・蓄積の方法

(ii)　コンテンツ・データの参照権限

1.2.3　サービス(アプリケーション)

教育クラウドの構成要素としては、大きく「教育プラットフォーム」と「教育サービス群」に分類できる。

「教育プラットフォーム」は、教育クラウドを利用する前提となる基盤(ID 管理、ファイルサービス)やセキュリティ対策を指す。また、「教育サービス群」とは、校務、学校教育、教育委員会事務を支援するためのサービス群となる。



① 校務支援サービス

学校教員の事務（校務）を支援するサービス。主な構成要素としては、情報共有機能、成績処理機能、保健管理機能、備品管理等が挙げられる。

② 委員会事務支援サービス

学齢簿、就学援助、徴収金管理等の事務に係るサービス。

③ 学習支援サービス

コンピュータ教室での授業において授業支援を行うサービス。教員機から生徒機をコントロールする機能、ファイル配付・回収等の機能がある。

④ コンテンツサービス（教科書、教材）

授業や授業の準備等において電子化された教科書や補助教材類を利用できるサービス。

※電子教科書等の場合には、児童生徒が一斉にクラウド環境にアクセスすることから、教育委員会の規模に応じて、例えば学校に負荷分散するための Proxy サーバの設置等も含めて考慮することが望ましい。

⑤ CMS サービス

学校現場が保護者や地域住民へ情報発信していくうえで、ウェブページを簡易に作成できる仕組みを提供するサービス。

⑥ 緊急連絡サービス

学校が保護者に対して緊急時や災害時等に情報発信を行うサービス。

※先行自治体においては、SaaS 型のサービスを利用している自治体もある。

⑦ 学校図書サービス

学校図書館における図書業務を支援するサービス。

これらのサービス群は、センシティブデータの有無などにより必要とするセキュリティレベルが異なることから、それぞれに応じたプラットフォーム機能と組み合わせることが必要。

1.2.4 教育クラウドに付随する要素

1.2.4.1 ネットワーク

これまで、学校に導入されたネットワークは、教育委員会や自治体から（出先機関へ）のネットワーク延長であり、自治体側のポリシーに沿って構築されている場合が多かった。ここ数年の電子黒板の普及などにより、普通教室への校内 LAN の整備も 80%を超えてきているが、生

徒全員が端末を利用するために必要となる無線 LAN の整備率は 25%未満となっている。以下のようなネットワーク利用・運用をしている学校も多いのではないだろうか。

教育クラウドに関連するネットワークには、クラウド側の DC 内 SAN、学校内 LAN、DC−学校間 WAN、家庭の Internet からの接続等、様々な接続があるが、教育クラウド特有の点について記述する。

（1）学校内

- ネットワークは自治体のセキュリティポリシーにより有線 LAN で構築
- 端末は、教職員 PC とコンピュータ教室の数十台、フロアで共有する NotePC
- ファイルサーバは学内に設置
- 職員室とコンピュータ教室は VLAN で分割してルータで接続制限
- 職員室/学校　内の LAN ポートは、接続認証などのセキュリティは無し
  （もしくは IP アドレス、MAC アドレス認証）
- 個人管理ではなくアプリケーションごとの　アカウント名／パスワード
- 無線 LAN は利用禁止
- ネットワークは地域で一括導入されるが、管理運用は学校単位

今後の学校ネットワークでは、「校務全般の ICT 化」、「児童生徒全員の ICT 端末利用」、「教育クラウドの導入」に向けた要求事項への対応が望まれる。考えられるものとしては以下の点があげられる。

① 学校独自のセキュリティポリシー
② 全教室で常時ネットワークが利用できること（無線も含む）
③ 全児童生徒が端末を利用しても逼迫しない帯域の確保（学内、WAN、IDC）
④ 学内の端末同士の接続の自由度（IWB とタブレットなど）
⑤ 教職員、児童生徒、災害時の住民／自治体職員　等への接続の提供
⑥ 学内ネットワークへの持ち込み端末接続の制限
⑦ 学外からの校務情報のアクセス
⑧ 誰が、どのデータに、いつ、どこからアクセスしているのかの把握
⑨ 管理運用の常時実施と学外へのアウトソース

②、③であれば、下記のような点に注意が必要となる。特に補講制度のない初等中等教育現場では、ネットワーク障害によって授業ができない状況は、避けるべきである。

- **学内の無線 LAN の AP 設置場所**

  教室で同時に使用する端末の数とトラフィックから、1 教室をいくつの無線 AP でカバーするか、また教室設置の AP が故障した場合にどのようにバックアップするかを考慮す

る。

例えば、教室に AP1 台、2 教室をカバーできる廊下部に 1 台など。また、体育館、校庭などもネットワークサポート範囲にする場合は、耐衝撃性のあるケースに収容するとか、屋外周波数で運用するなど、注意が必要である。

無線 LAN の電波伝搬には、教室壁や防煙壁の材質に影響を受けるため、事前の現地調査を行うことで、AP 設置後の通信障害発生を抑えることができる。

・ **端末台数と利用アプリケーションから WAN の帯域計算**

私用する端末、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 XXbps 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。

（10MB×8bit） ÷ 100Mbps ＝ 0.8sec

もし、1 クラス 32 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、全員の画像が表示終わるには 25.6 秒以上となってしまう。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。

（10MB×8bit×32） ÷ 100Mbps ＝ 25.6sec

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

・ **トラフィックが集中する IDC の帯域**

学校を複数収容する DC 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を考慮する

⑤, ⑥であれば、通常時の学校運営で、ネットワークに接続された端末が、まず、接続を許可されるのか、排除すべきか、さらに端末同士の通信を許可するかの管理がある。また災害時に避難場所となる場合は、住民や自治体職員にどのようにネットワークを提供するかを考慮する必要が出てくる。

⑦, ⑧は、統合された個人認証でなければ、実現できない。

これらのネットワークを学校職員で管理運用することは難しく、教育 ICT の利用で、教育

の充実や教員の業務効率化を図るべきにもかかわらず、管理が教職員への負荷になっては、本末転倒となってしまう。教育クラウドの導入に当たっては、⑨の項目については、学内ネットワークの管理運用も教育クラウド基盤として(学内にはユーザしかいない状況に)すべきである。

(2)学外(地域 WAN)接続形

現在の学校から外部への接続には、下記のようにいくつかのパターンがあり、また、回線についても、光専用線、プロバイダ FTTH、CATV ADSL など回線速度もその SLA も統一性はない。自治体 WAN で利用している回線も考慮の上、(1)で述べたような、WAN ネットワークに求められる帯域とコスト、クラウド DC との接続形態により選択をする。

接続先	教育委員会	Internet 接続
	教育委員会 WAN	学校から直接
	自治体 WAN	教育委員会経由
	InternetVPN	自治体ネットワーク経由

今後の教育クラウドの構築に当たっては、その必要帯域計算の上、一定以上の帯域の保障を求められることから、光回線の利用と、秘匿データも多くなることから、教育委員会への接続が、利便性が高く、現実的である。

1.2.4.2 HTML5

W3C(World Wide Web Consortium:WWW で利用される技術の標準化を進める民間団体)では、最新の HTML 言語である HTML5 を 2014 年度に勧告することを目指すと表明している。(平成 24 年 情報通信白書 第1部2章2節(2)「コラム HTML5 について」、http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc122220.html)

HTML5 はウェブページでの情報の表現に加え、ウェブブラウザのみでアプリケーションが動作する。HTML5 は Web 標準技術であるため、インターネットや一般書籍での情報収集が比較的容易である。また、視覚効果や非同期処理に関する OSS(Open-source software)の各種部品が公開されている点も利用しやすい。現在はアニメーションや動画再生には Adobe Flash や Silverlight が補完的に利用されているが、将来的には HTML5 の動画再生機能を活用する方向になる。

現在のウェブブラウザは最終勧告を前に、一部の機能の取り込みをしている状態だが、正式な仕様が公開されれば、各ウェブブラウザがフル機能をサポートし、互換性のあるものになると考えられている。これにより、様々な端末で HTML5 対応の教材やアプリケーションが共通して使える可能性が出てくる。

また、HTML5 では、データをローカルに保存することができるため、通信状態の不安定な無

線 LAN の環境や、通信環境の無い家庭や校外の環境でも、HTML5 アプリケーションの活用が可能となる。

今後の課題は、

- HTML5 の動作には、CPU・メモリ・グラフィックスがある程度以上の性能が必要
- ローカルに保存されたデータや通信上のデータは、そのままでは著作権保護ができないため、なんらかの秘匿化技術の採用が教材や各種教育アプリケーションの普及には必要

などが考えられるが、様々な端末の画面サイズ・解像度で利用者にとって使いやすいユーザインターフェースが実現できるかも重要な観点である。

1.2.5 教育クラウド利用にあたって留意を要する要素

教育クラウドの検討にあたっては、Web の新たなアーキテクチャーの採用や端末等の導入形態の新しい変化に着目する必要がある。最新技術の採用により教育への ICT の新たな活用が期待される。

現在の学校の環境で、コンピュータ教室での端末利用から普通教室での1人1台環境での利用への移行を考えると、様々な課題と制約がある。現状では、普通教室での1人1台を整備する場合には充分に検討しておく必要がある。(後述　端末の項参照)

1.2.5.1 端末等

ICT の分野では、企業や自治体・各種団体で活用されている業務システム用の PC 端末に加え、スマートフォンに代表される個人用の情報端末の普及が急速に進んでいる。

教育の情報化では、各種教科をわかり易く教え、協働的な教育を実現することに加え、情報に関する教育や情報の安心安全な取扱いに関する教育が求められている。

このため、総務省のフューチャースクール推進事業では、企業や自治体・各種団体で活用されている PC に加え、個人用のタブレット入力機能などを持つ、タブレット PC を採用している。

教育クラウドで実現される教育には、教科書教材や創作のための各種ツールの活用に加え、企業や自治体・各種団体での ICT 活用に対応できるための基本的操作の習得や社会での ICT 活用のための安全教育(いわゆる情報モラル教育)が求められる。

単なる情報の消費に止まらず、新たな創作や企業等で利用されている各種ツールを活用し、実際に仕事に就くときには更に数段進んだ ICT 環境を活用できるようにするための情報端末を選択する必要がある。

また、最近は無線 LAN の活用が進んでいるが、飲食店や公共施設などそれほど多くない人数で個々のニーズに従い無線 LAN を使う場合と、学校での多数の端末を一斉に使う使い方は全く異なっている。このような条件を考慮せず安易に施設整備すると様々な問題が発生する。

一人一台を目指した端末の整備には、従来の端末導入の数倍～数十倍に及ぶ台数の導

入・運用・維持・メンテナンスが必要となり、教育クラウドと連携した自動化が重要となる。これらの内容を明らかにするため、以下に端末の要件等を記載する。

1)タブレット PC の技術的要件

総務省の「教育分野における ICT 利活用推進のための情報通信技術面に関するガイドライン(手引書)2013　小学校版」では、3 年間の実証実験を終えて、端末の要件について触れている。

http://www.soumu.go.jp/main_content/000218505.pdf

＜手引書　92 ページより＞

タブレット PC に関する技術的要件のポイントを以下に示します。

［ 安定動作や起動時間 ］

・ 使用中にフリーズすることなく安定して動作すること
・ 安定した高速接続が可能な無線 LAN が利用できること
・ 日中はスリープ運用が多い点に照らし、スリープからの復帰時間が約 30 秒以内であること

［ 重さ ］

・ タブレット PC の重さは約 1kg を目安とし、軽量で児童にも持ち運びやすいこと

［ 画面サイズ ］

・ コンテンツの見やすさ、文字の判別のしやすさ等を踏まえ、10～12 インチ前後のものとすること

［ 文字入力 ］

・ ペンで文字や図形等を滑らかに記入することができること。また、ペン先以外の部分に誤反応を起こさないこと
・ 特に高学年の場合、キーボード機能を有していること

［ バッテリー ］

・ 1 日の授業時間分(約 6～8 時間程度)バッテリーが持続すること
・ 授業中のバッテリー不足に備えて、あらかじめ大容量のバッテリーをつけたり、予備バッテリーを準備する等の措置を講ずること

［ 堅牢性 ］

・ 教室間移動の際や落下による破損を想定し、筐体は耐久性や堅牢性に配慮した設計であること。また、破損した場合には、予備機による対応ができるようにすること

［ その他 ］

・ カメラ機能を有すること(タブレット PC の画面上部に自分を撮影するために内蔵されているカメラ(以下、「インカメラ」という。)や、児童が被写体を画面で確認しながら撮影できるよう、画面の外側に備えられたカメラ(以下、「アウトカメラ」という。)等)

＜引用終了＞

2) 普通教室でのタブレット PC 利用とコンピュータ教室の従来の機器との差異

a)電源がバッテリー駆動

・コンピュータ教室では、ノート型 PC やタブレット PC を利用していても、AC 電源での運用となりバッテリーは利用されない場合が多い。普通教室で利用する場合はバッテリー運用となるので、利用方法の検討が必要となる。

・バッテリー駆動であるため、時間の経過とともに電力が消耗するので、使用時間・残容量に留 意する必要がある。

・バッテリーは消耗品であり、充放電を繰り返すと充電容量が減少する。ノート型PCでよく使われている「リチウムイオン」バッテリーは 300～500 回程度で、タブレットPCで採用されはじめている「リチウムポリマー」バッテリーは 800～1000 回程度の充放電で寿命となり、交換が必要となる。

b)無線 LAN

・無線 LAN の安定性を阻害する要因として、各種の電波干渉がある。学校内であれば、電子レンジや Bluetooth 対応の各種機器・デジタルフォン、住宅地であれば、各種の無線LANルータ、工場地帯であれば電力設備など様々な雑音源がある。また、5GHz帯の無線LANでは衛星通信等の公共社会通信設備の電波を受信すると停波し、別の電波帯への変更を行う仕様となっている。これらの影響を受けると、無線LANの利用が困難となる。

・無線 LAN は周辺のアクセスポイント等をスキャンするので、モバイルルーターやルータ機能を持ったスマートフォンなどが多数ある場合、通信状態が不安定になる。

・様々な理由で無線 LAN が切断された場合、利用するアプリケーションがそれを感知し適切な対応を行う必要がある。

c) Bluetooth

・Bluetooth でキーボードやマウスを利用する場合、多数の端末があると、どの端末とどの周辺機器がペアかを外部から判断できるようにする必要がある。また、ペアリングが外れた場合の再設定が必要な場合がある。

d)照明等の環境

・コンピュータ教室では、採光や照明設備が整備されており、反射等による不具合が解消されているが、普通教室では配慮されていない場合がある。

タブレット PC は机の上で平面に置く場合が多く、照明や陽光の反射を避ける工夫が求められる。また、グループ学習での利用では、複数方向から画面を見ることになるので、視野角の広い液晶画面が求められる。通常の液晶は左右方向が上下方向より視野角が広いのに対し、最新の液晶では上下・左右両方向に視野角の広いものもあらわれている。

3)端末の OS について

a)現在学校に導入されている端末の OS

学校における教育の情報化の実態等に関する調査 平成24年度 調査結果

http://www.e-stat.go.jp/SG1/estat/GL08020103.do?_toGL08020103_&tclassID=000001050381&cycleCode=0&requestSender=dsearch

（3）教育用コンピュータのOS別台数

学校種	教育用コンピュータ台数(再掲)	Windows 8	割合	Windows 7	割合	Windows Vista	割合	Windows XP	割合	その他のWindows(2000,NT,Me,98,95等)	割合
	A	B	B／A	C	C／A	D	D／A	E	E／A	F	F／A
	台	台	%	台	%	台	%	台	%	台	%
小学校	890,349	28,750	3.2%	355,936	40.0%	188,208	21.1%	297,832	33.5%	10,856	1.2%
中学校	502,379	16,086	3.2%	216,256	43.0%	105,805	21.1%	154,820	30.8%	5,113	1.0%
高等学校	474,706	14,136	3.0%	159,207	33.5%	131,158	27.6%	146,228	30.8%	16,278	3.4%
専門学科・総合学科 単独及び 複数学科設置校	314,512	8,918	2.8%	101,771	32.4%	79,843	25.4%	103,158	32.8%	14,435	4.6%
中等教育学校	2,926	3	0.1%	1,322	45.2%	1,010	34.5%	560	19.1%	6	0.2%
特別支援学校	35,043	577	1.6%	11,879	33.9%	9,452	27.0%	10,772	30.7%	636	1.8%
合計	1,905,403	59,552	3.1%	744,600	39.1%	435,633	22.9%	610,212	32.0%	32,889	1.7%

学校種	教育用コンピュータ台数(再掲)	Mac OS	割合	iOS	割合	Andorid	割合	その他のOS（Linux等）	割合
	A	B	B／A	C	C／A	D	D／A	E	E／A
	台	台	%	台	%	台	%	台	%
小学校	890,349	3,054	0.3%	3,392	0.4%	809	0.1%	1,512	0.2%
中学校	502,379	1,688	0.3%	1,876	0.4%	223	0.0%	512	0.1%
高等学校	474,706	3,786	0.8%	1,375	0.3%	614	0.1%	1,924	0.4%
専門学科・総合学科 単独及び 複数学科設置校	314,512	3,308	1.1%	871	0.3%	570	0.2%	1,638	0.5%
中等教育学校	2,926	5	0.2%	20	0.7%	0	0.0%	0	0.0%
特別支援学校	35,043	178	0.5%	1,434	4.1%	50	0.1%	65	0.2%
合計	1,905,403	8,711	0.5%	8,097	0.4%	1,696	0.1%	4,013	0.2%

b)OS の種別による特性

・マルチタスク OS では、アプリケーションを実行している状態で、バックグラウンドで通信処理ができ、リアルタイムに、先生の画面を生徒に送信したり、生徒の画面をモニタリングしたり、生徒の操作を停止させたりする、コンピュータ教室で利用されている授業支援システムが構築できる。

これに対し、シングルタスクの OS では、画面転送が実現できないため、生徒用端末のアプリケーションが送信用データを作成し表示用の PC などに送信し、そこでアプリケーションで画面を再生して表示する必要があり、特定のアプリケーションでしか対応できない場合がある。

・OS によっては、画面表示が画面サイズによって正確に表示されない場合があるので利用するアプリケーションの確認が必要である。

・OS の種類によっては、短いサイクル（2～3 年）で新たな OS が提供され、従来のハードウェ

アでは動作できなくなる場合がある。
また、新 OS 上では新しいアプリケーションのみがサポートされ、古いアプリケーションが利用できなくなる場合があるので留意が必要である。
OS 自体のセキュリティパッチの提供期間が利用用途に合致しているかの確認も必要となる。
また、通常の利用の場合、利用者に直接アップデート実施の可否が問われる。この場合、利用者がそれぞれにアップデートを実施してしまい、端末の環境がそれぞれ異なり、一時的に管理ができなくなるリスクが生じる。このような状況に対応するため、運用管理での考慮が必要になる。

・セキュリティ面で校内 LAN への端末接続を管理している場合、端末を接続する場合の認証機能や管理機能が端末の OS で提供されているかどうかの確認が必要。

4）情報端末の運用管理

a)アプリケーションの購入・インストール

・個人利用を前提に提供されている情報端末では、アプリケーションの購入にクレジットカードが必要になり、また、一台一台を各端末からアプリケーションのインストールが必要になる場合がある。公立学校ではクレジットカードの作成や、一台一台アプリケーションをインストールするのは困難な場合が多い。
自治体のルールに適したアプリケーションの提供方法が求められる。

b)各種パッチの適用

・セキュリティパッチやウィルスパターンのダウンロードや適用が授業中に行われると、授業運用が困難になる。適切なタイミングでの運用管理が行われる必要がある。

c)設定変更などへの対応

・教員の転勤や生徒の入学/卒業/進級/転入学など利用者の変更に伴う設定の変更や、ネットワークやアプリケーションの設定変更などを、大量の端末に作業する場合、人手のみで行っていると、作業工数・作業費用が高くなる場合がある。このため、大量端末の設定作業の自動化の仕組みが必要となる。

5）その他

a)タブレット PC のペンについて

・タブレット PC のタッチパネル機能には、指などでの操作ができる静電容量方式と、精細なペン操作ができる電磁誘導方式のデジタイザが採用されたものがある。電磁誘導方式のデジタイザは通常、静電容量方式も同時に搭載している。
電磁誘導方式のデジタイザは、長文の手書き入力やデザイン画の作成等に利用される場合が多く、業務としてペンを活用する場合はこの方式が採用される。
静電容量方式のペンも提供されているが、指の代わりにポインティングするのには使えるが、ペンを利用していても、画面に手が触れると認識されるため、長文の手書き文字入力などには利用できない。
ペンが使えるとしてもどのタイプが利用目的に合致するかを充分留意する必要がある。

b)アプリケーションの利用方法について

・個人利用を主に設計された情報端末は、スマートフォンなどと同様にゲームやゲームのアイテム、音楽データ、書籍データを購入して楽しむことを目的としている。このため、アプリケーションもブラウザ・音楽／書籍ビューワー・簡単なメール機能を中心に提供され、本格的なワープロや表計算・プレゼンテーション用のアプリケーションは提供されず、作成したデータを見たり、一部変更する機能が提供されれる場合が多い。

情報端末を報告書や論文、本格的なプレゼンテーション作成に活用しようという場合には目的とアプリケーションの機能を確認する必要がある。

c)外部インタフェース

・タブレット PC では従来の PC で採用されていた外部インタフェースが変わっている場合が多い。タブレット PC では、映像系では HDMI の採用が多く、従来のプロジェクタに用意されている VGA のインタフェースはほとんどなく、通信系では有線 LAN のインタフェースもほとんどなく無線 LAN の利用が一般的である。
場合によっては、拡張クレードルや変換ケーブルが用意され、旧来の PC のインターフェイスが利用できるものもある。

1.2.5.2 BYOD

スマートフォンやタブレット PC などの携帯端末の性能や機能の向上と普及により、企業などでは、個人保有の端末を業務でどう活用するかという観点で BYOD（Bring your own device）の採用が始まっている。

教育分野においても、大学等での学生コンピュータの利用や私立学校での個人持ちコンピュータの活用が既に多くの事例がある。

大学等での BYOD では、構内での無線LAN接続や履修登録・各種の学生ポータルに加え、大学で契約した電子ジャーナルや電子書籍等の利用などほとんどの作業が個人所有端末から利用できるようになっている。

最近では、公立学校でも保護者負担による1人1台コンピュータの活用を始める例も出てきている。

学校での利用を考えると、学校で必要なアプリケーションやサービスを活用できるような仕組みをどう構築し、教育に有用な道具として利用するかが課題となる。

また、家庭での利用においても、学校での教育利用の延長としてどう活用するかを検討すべきである。この場合、前述の HTML5 に加え、情報秘匿機能を付加した、ローカルデータの活用が各種教材の利用に有効ではないだろうか。

1.3　クラウドの配置モデル

教育クラウドが想定するアプリケーションクラウドサービスとは、利用者からみて、サービスがクラウド（ネットワーク）の先に存在していてその実態を意識する必要はないものであるが、実態は、要件に応じて設計された DC へのサービスとデータの配置である。

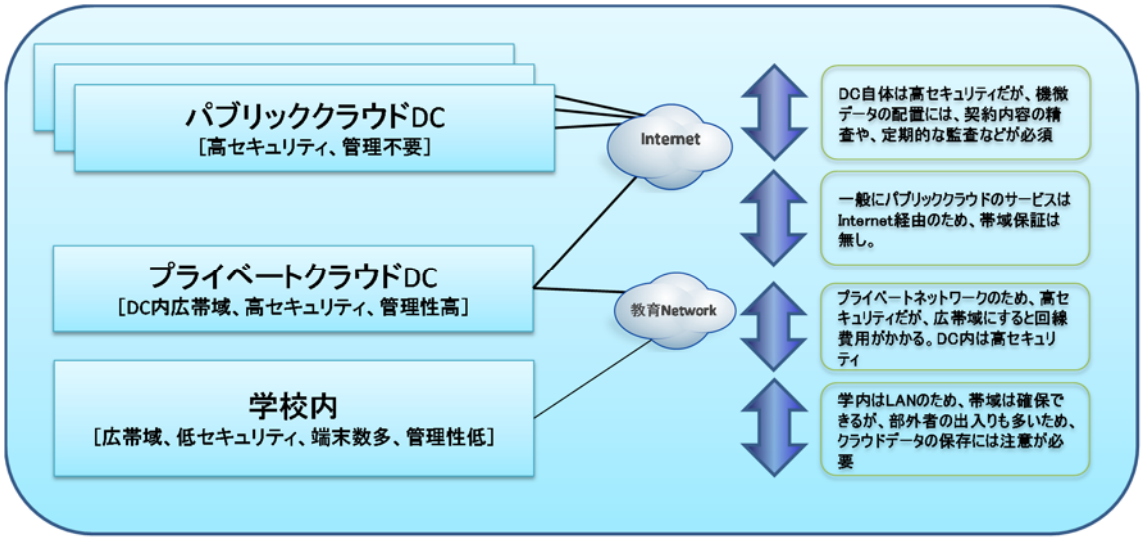
教育クラウドの設計を行う時、データの「セキュリティ（秘匿性の高さ）」、「データサイズ」「ユーザ数と使用頻度」「回線帯域のコスト」などを想定の上、どの DC に何のデータを置くかにより、配置モデルは変わってくる。

例えば、電子教材自体は秘匿性が低く、データサイズが大きく、複数名が一斉に利用するため、もし電子教材などをすべてクラウド上に置いた場合、児童生徒が授業のたびにダウンロードする必要があり、WAN 帯域の逼迫と動作遅延を引き起こす。

そのため、電子教材は、端末へのインストール保存も可能と判断できるが、教材への書き込みデータやテスト回答データは、個人に紐付いた学習履歴となるため、どこに保存すべきか事前に確定しておく必要がある。

また、成績データのような秘匿性を高くすべきデータは、教員の PC や学内サーバに置けば、情報漏えいの原因になりやすいが、幸いなことに秘匿性の高いデータの1レコードサイズは、大きくないことが多いため、これらのデータはプライベートクラウド（自治体内 DC、もしくはセキュリティ要件をクリアする民間 DC）への配置が可能である。

民間事業者が提供するパブリッククラウドや、プライベートクラウドに一部のパブリッククラウドから提供されるサービスを組合せたハイブリッドクラウドでの利用を行う場合、要件にあった DC の組み合わせを選択することで、遅延の少ないクラウドサービスを利用することができる。



この時の課題は、現在の校務、教材などのアプリケーションが、データの種別によって保存場所を分割保存する機能を持っているか。また、DC に置いたデータを複数名で利用した時の排他処理ができるかにより、教育クラウドでの利活用に影響を及ぼす。この他にも、DR や BCP のための

データのバックアップ手法も考慮する必要がある。DC 間接続などは、既存の DC 技術により設計されるが、バックアップ DC を同一自治体内に作るのか、災害時にも影響を受けにくい遠隔地と相互バックアップなどで行うのか。バックアップは、データ保存だけか、サービス提供機能も持たせるのかなどにより、コストとサービスのレベルは異なる。

・秘匿性低 ： アプリケーション、教材、公開可能データなど
・秘匿性中 ： 学習成果物、写真など公開はしないが漏えいしても影響の少ないもの
・秘匿性高 ： 成績、病歴等個人情報が含まれるもの

2. 教育クラウドの整備

2.1 想定する整備シナリオ

2.1.1 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。

2.1.2 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、以下に参考文献をまとめた。

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）

（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。

2.3.1 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。

2.3.2　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

（1）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。

（2）校務などアプリケーションの運用改善に関わる体制

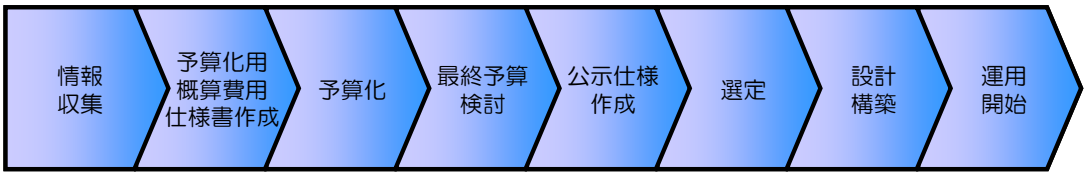
教育委員会の ICT 施設整備部門および学校教育部門に加え、学校現場の教育・事務・保健・給食等の代表者によるアプリケーションシステムの運用改善を検討する。

（3）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。

2.3.3　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、サービス提供業者が有する資産で、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、サービス提供業者からは「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業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業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。

2.7.1 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。

（1） 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

（2） 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

2.7.2 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。

（1） 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

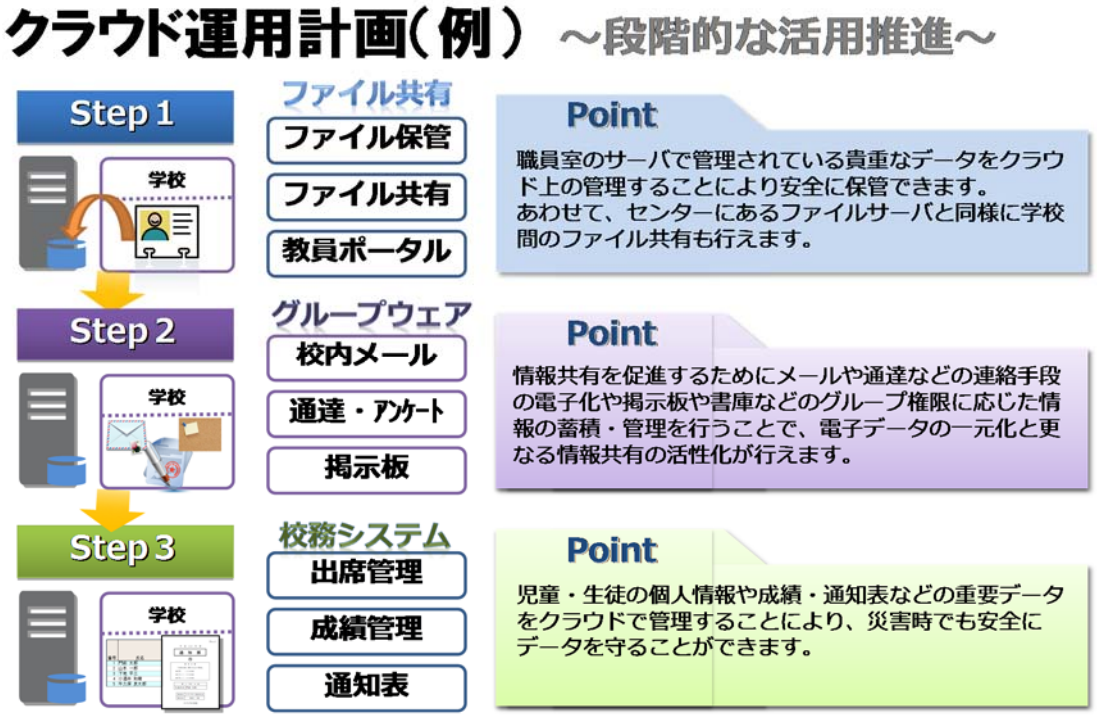
（2） 指導要録や健康診断表等の公文書の安全な保管

- 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

2.7.3 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。

（1） 段階的な校務支援システムの導入・運用
（2） モデル校スタートによる成果や効果、課題等の明確化
（3） 繁忙期や閑散期などに合わせたクラウド運用
（4） 終焉やシステム移行に伴う、データ移行や消去



2.7.4 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に実施し、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。

（1） 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

（2） 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など）

2.7.5 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。

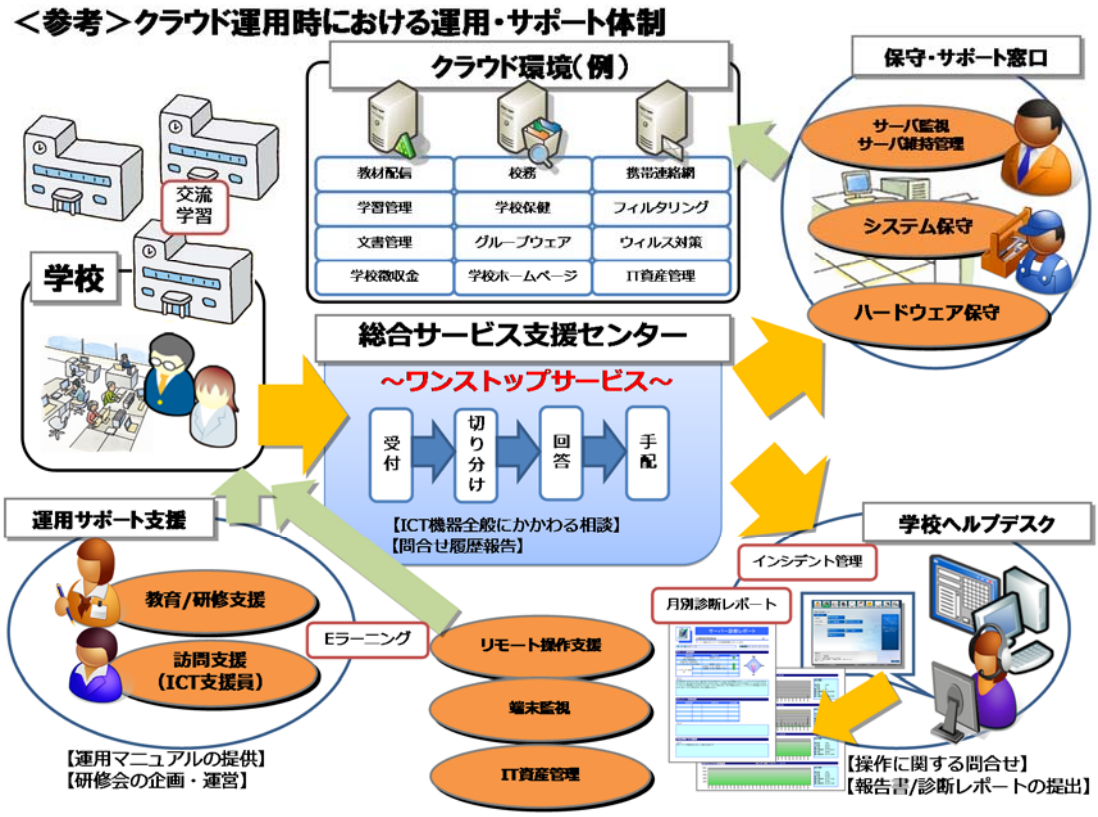
（1） 窓口の一元化による情報の集約と、質問内容の切分けや進捗状況の管理を行うワンストップサービスの提供

（2） 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、サーバのアタック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

（3） 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



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

◆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

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

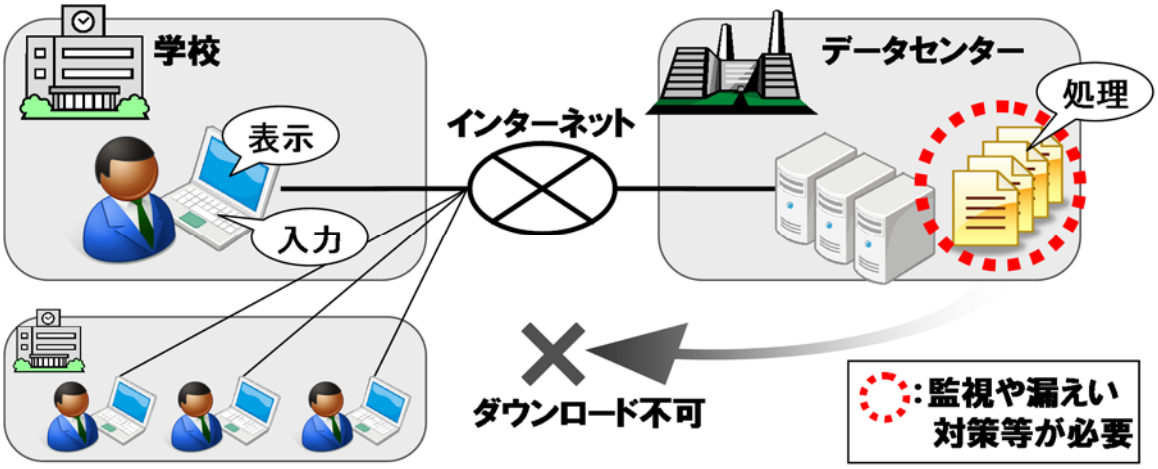
クラウドサービスのセキュリティは、「どのようなデータ」が、「実際にどこで」、「誰によって」処理されるかによって、設計と対策の容易度が、かわってくる。

◆ 例1

・利用者はクラウドに Web 経由でアクセスする

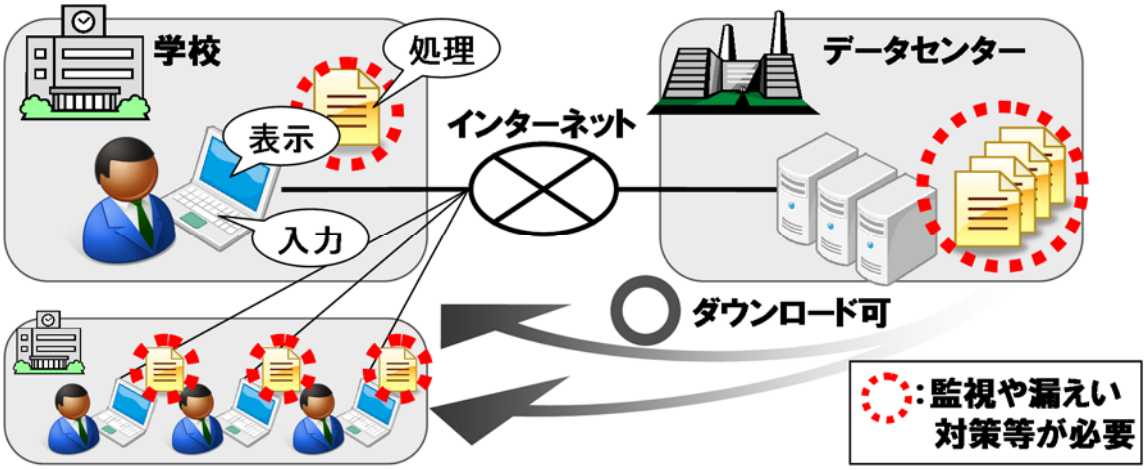
・センシティブデータは、全てクラウドのサーバ上で処理

・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ず、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。

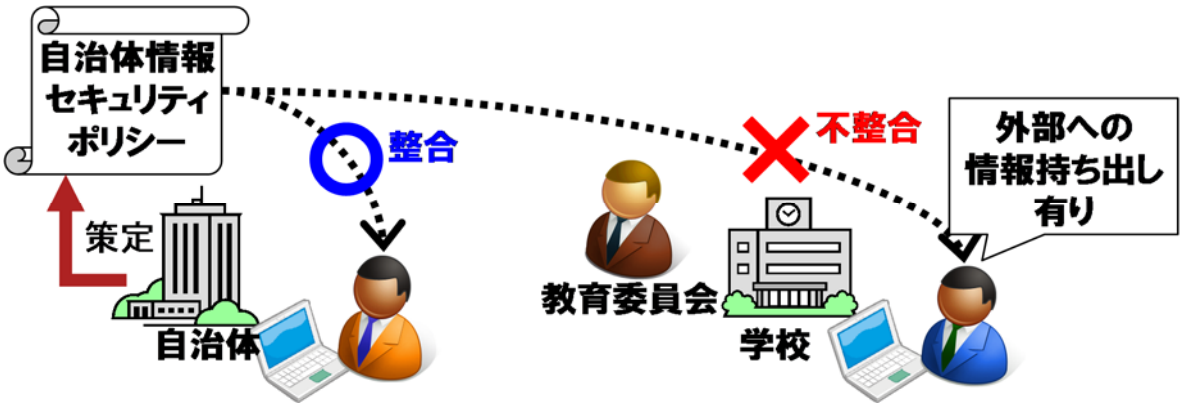
3.2 セキュリティポリシー

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。



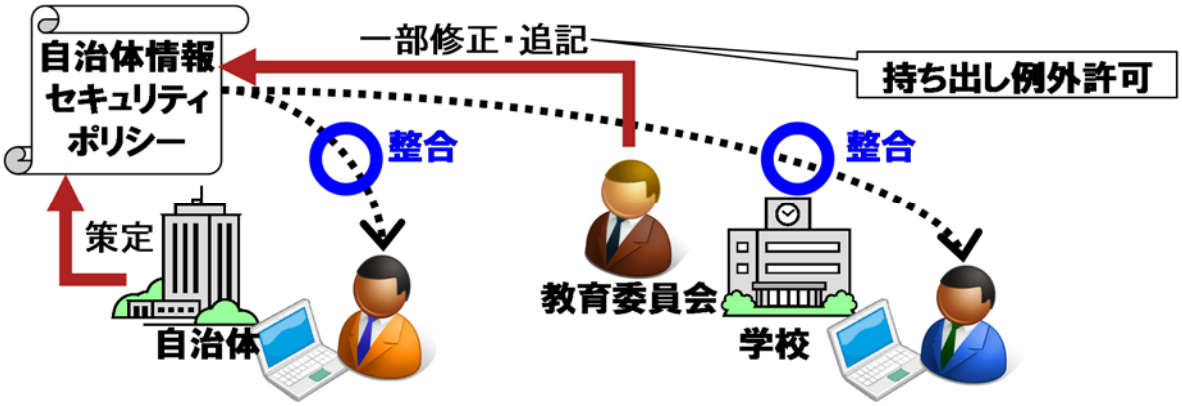
上記のような理由から、教育クラウドの利用形態や管理主体を考慮し、自治体の情報セキュリティポリシーを一部改訂した上で準拠する、または教育委員会で新たに情報セキュリティポリシーを策定するといった対応が必要となる。

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に実施し、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したりする。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。

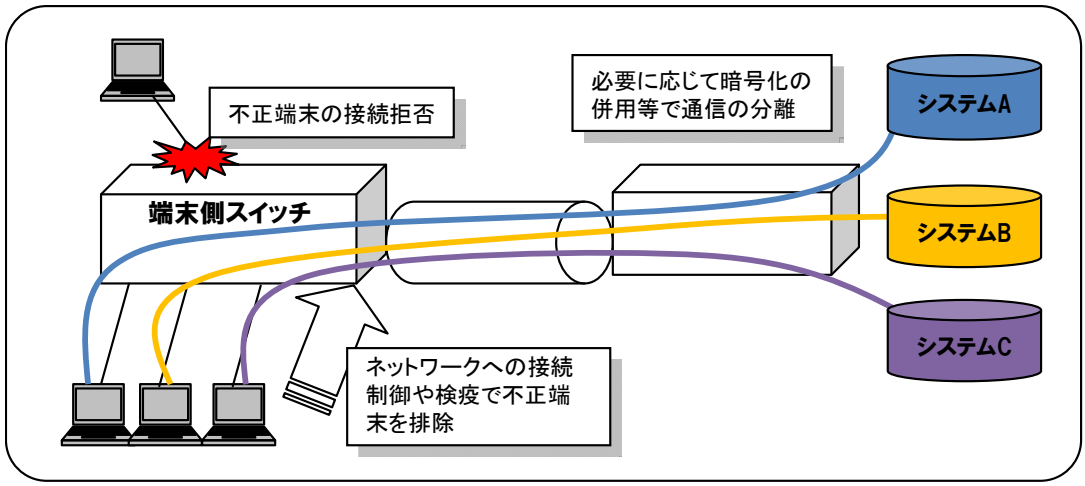
(3)LAN(学校内・教育委員会内)

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。)

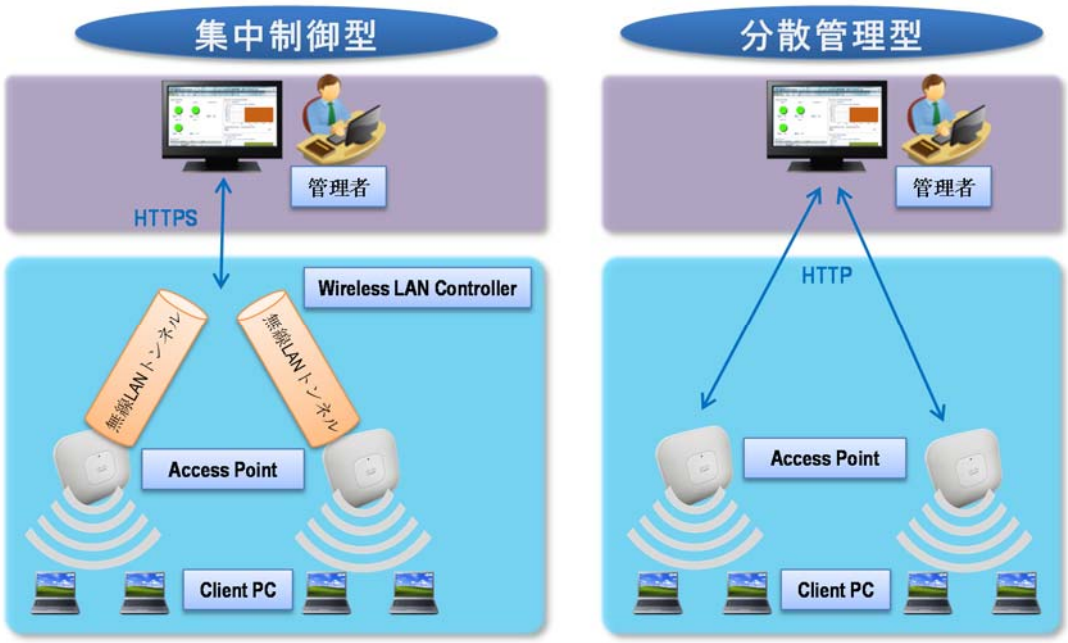
本ガイド記述時点では、接続認証では IEEE802.1X、暗号化は WPA2-PSK(AES)以上を推奨する。最重要なデータを利用するクライアント PC においては、電子証明書や OTP (OneTimePaaword)の同時利用を推奨する。

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

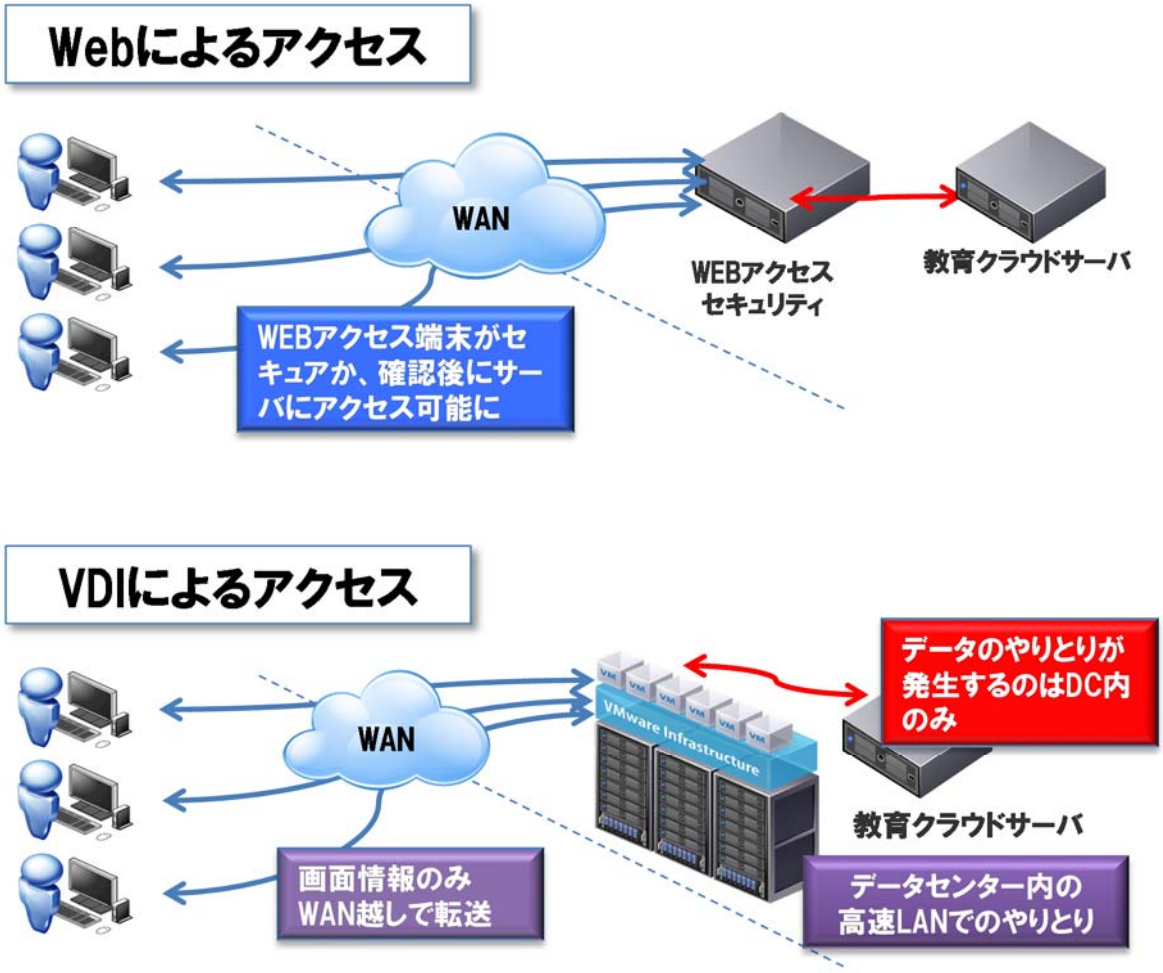
クラウドサービスを自宅等組織外（校外）から利用する場合は「どのようなデータ」が、「実際にどこで」、「誰によって」処理されるかを明確にする。

「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。



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う、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

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」

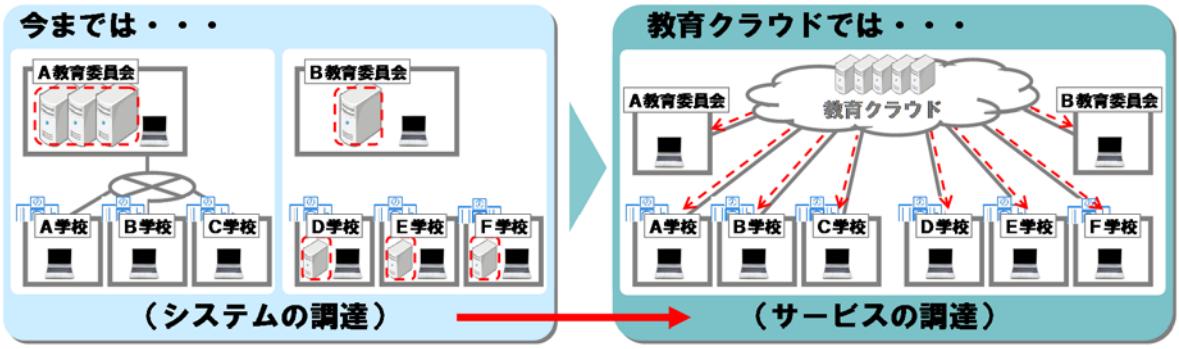
http://www.cec.or.jp/seculib/index.html

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。



●教育クラウドでは、　①必要量・必要分のサービスを利用　　②運用/管理をアウトソースし負担を軽減

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、サービス提供業者が有する資産で、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。調達側が必要量・必要分のサービスを利用し、これまで調達者側が行っていた運用・管理をサービス提供業者に任せ負担を軽減することができる。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となるリソースや費用は、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)}×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)}×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。

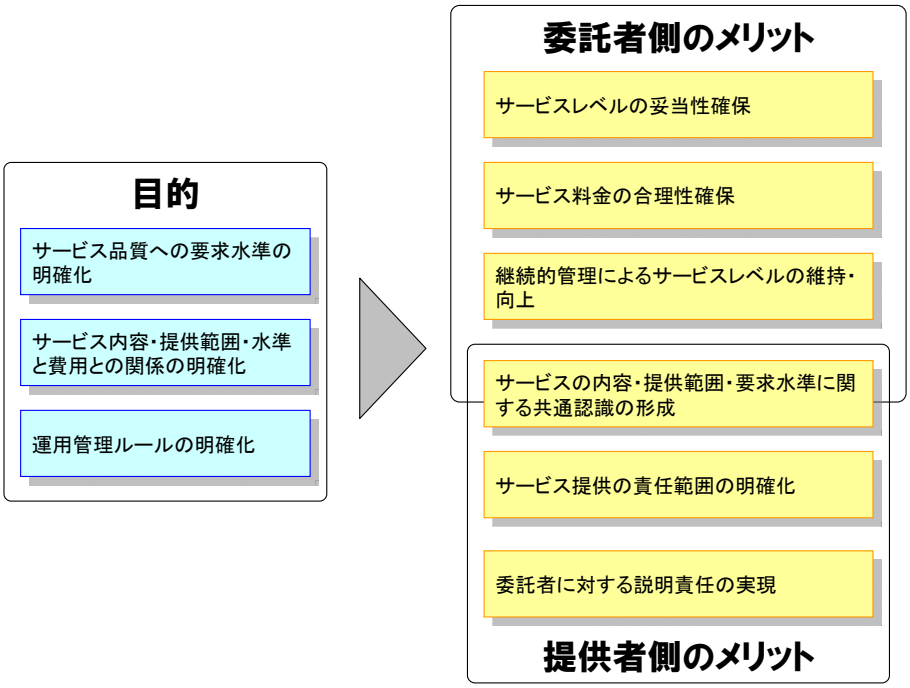
③ 帳票デリバリ時間遵守率

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)}×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. 将来の課題

5.1 教育クラウドの整備に関する将来の課題

(1) 自治体クラウドとの関係

規模の大きな自治体では、教育委員会が独自にプライベートクラウドを構築しているケースが多い。一方、自治体の首長部局では、規模の大小にかかわらず独自にプライベートクラウドを構築したり共同利用型のクラウドを活用している。教育委員会と自治体の首長部局が共同でクラウド化を推進しているところはほとんどない状況である。自治体の財政状況も厳しい中で、一つの自治体が行政系のクラウドと教育クラウドの 2 つを持つのは非効率と判断されてもおかしくない。

教育クラウドを利用する児童・生徒・保護者は、もともとその自治体の住民なので、自治体クラウドと教育クラウドを一つにまとめる方向を後押しする施策が望まれる。番号制度が導入されれば、住民情報の利用や、医療情報との連携も考えられ、就学援助や予防接種の履歴活用など業務の効率化の促進やメリットは非常に大きいと予想される。

(2) データ連携

教育クラウド内でのデータ連携に関しては、同じ校務支援システムや共通の LMS の利用で大きな問題は発生しないと考えられるが、児童・生徒の転校などでクラウド間でのデータをやり取りする場合の、データ連携に関してはまだ取り決めが無い状況である。クラウド間でのデータ連携に関する標準化も望まれるところである。また、自治体行政には総合行政ネットワーク(LGWAN:Local Government Wide Area Network)があり、セキュアなネットワーク環境が確立されているが、教育や医療に特化した LGWAN に相当するようなネットワークはまだ整備されていない。現状の総合行政ネットワーク(LGWAN)を、教育でも利用できるようにするのか、教育や医療関係用に新たにセキュアなネットワークを構築する等の検討が必要だと考えられる。

(3) 認証基盤

教育クラウドの利用者は、教育委員会および教育委員会事務局職員、自治体職員、教職員、児童・生徒、保護者、ボランティア団体、地域住民等多岐にわたる。利用者ごとにアクセスできる領域やデータ、利用できるサービスは異なることになる。一方、保護者の立場で考えると、大学生、高校生、中学生の 3 人の子どもがいた場合、3 つの教育クラウドに別々にログインすることになる。システムが複雑化し、セキュリティへの要求が高まると利用者にとって使いにくい状況が発生する。それを防ぐために、国としての共通統合認証基盤の構築が望まれる。番号制度の導入でユニークな ID が国民に与えられるので、生体認証となんらかの認証の組み合わせで共通の認証基盤が構築されれば、利用者は 1 度のログイン認証で、複数のクラウド、サービスを利用できるようにすることは可能である。特定の自治体や1ベンダーが認証基盤を構築してもメリットが少ないため、国としての共通統合認証基盤の構築が望まれる。

(4) 学習履歴

①LMS（Learning Management System）の標準化

今後、教育クラウドを利用する児童・生徒が、学習の履歴を保存するという活用がが進むものと考えられる。現状、市販、流通している LMS は標準化されておらず、特定の教材に特化した製品が大半である。児童・生徒が転校や進学をしても履歴を移動し活用できるようにするには、LMS の標準化が必要である。そのためには、指導要領や年間指導計画のコード化等も必要で、近々に活用が広まることが予想される学習者用デジタル教科書の標準化も必要になると考えられる。また、学習履歴は成績と密接な関係があるので、校務システムとの連携に関しても標準化が必要となる。

②ストレージの考え方、帯域確保

児童・生徒の学習履歴データを、どこに保存するのか、何年間保存するか等も検討が必要である。一人の児童（生徒）が、どこで躓いたかを見るには過去のデータは必要であろう。何年前まで遡る必要があるかは、システム側の都合ではなく、指導する教員（学校）側の判断に委ねられるものと考える。また、ポートフォリオ的な活用を考えた場合、児童・生徒の図工や美術の作品を写真に撮って保存、家庭科や音楽、体育などでも写真や動画での保存等は考えられる。学校の特性を考えると、授業の終わりに一斉に写真を撮って保存という状況が発生する。

ストレージの容量、ネットワーク回線の帯域は十分考慮が必要である。写真や動画の保存にあたっては、いきなり教育クラウドのサーバに置くのではなく、学習者端末に一時的に置くか、学校のサーバに保存するなどの運用上の工夫が必要になるであろう。現状、規模の小さな自治体では、自治体のネットワーク回線を教委員会（学校）が利用しているところも多いので、帯域に関しては他の業務に支障が無いよう十分な検討が必要である。

③暗号化

個人情報となる学習履歴に関して、暗号化等の処理が必要か否かは、教育クラウドや校務システムの考え方にも影響されるものと考えられるが、校務システムとも合わせて何らかの指針が必要になるものと考えられる。

④公開の範囲

学習履歴に関しては、すべてオープンにする必要はないと考えられるが、児童・生徒本人や保護者が、家庭から確認できるようにすべきであろう。公開にあたって自治体ごとでばらつきの無いよう、学習履歴公開の指針も検討が必要であろう。

(5) 生涯学習への対応

教育クラウドと言った場合、社会教育、生涯学習も対象となる。学校教育の場合は利用者も限定しやすいが、社会教育、生涯学習に利用者を広げた場合、セキュリティや個人認証への新たな対応が必要となる。

(6) 外字

学習者や教職員の情報を取り扱うに当たって、外字の統一が必要である。

学校間や自治体間でデータのやり取りを行なう場合、外字が含まれていると不都合が生じる。IPA（独立行政法人 情報処理振興機構）が行政機関向けの文字情報基盤を公開しているが、外字を 100%カバーには至っておらず、国としての統一が図られたわけではない。番号制度の導入で、情報の参照・流通は確実に増えると考えられ、異なった外字コードの存在は大きな経済的損失である。国としての早急な外字統一が望まれる。