教育クラウド調達ガイドブック

参考編

総務省
Ministry of Internal Affairs and Communications

教育クラウド調達ガイドブック　参考編

◆目　次

参考1 クラウドサービスとは

（1）クラウドサービスはなぜ生まれたか

「クラウド」とは「クラウド・コンピューティング」の略で、「インターネットを通じてソフトウェアやデータなどを利用するコンピュータの利用形態」のことをいいます。このクラウドを活かしたサービスがクラウドサービスです。

しかし、クラウドサービスの捉え方は人によって様々であり、「クラウド」とは何かを考えると、わかるようでわからない、まさに雲をつかむような話になりがちです。ここでは「クラウドサービスとは何か」について考えてみましょう。

例えば、クラウドサービスには使った分だけ課金する従量制課金など、クラウドならではの特長が存在しますが、どうしてそのようなことができるのでしょうか。そのカギは、クラウドを構成する技術を探ることで見えてきます。

①分散処理

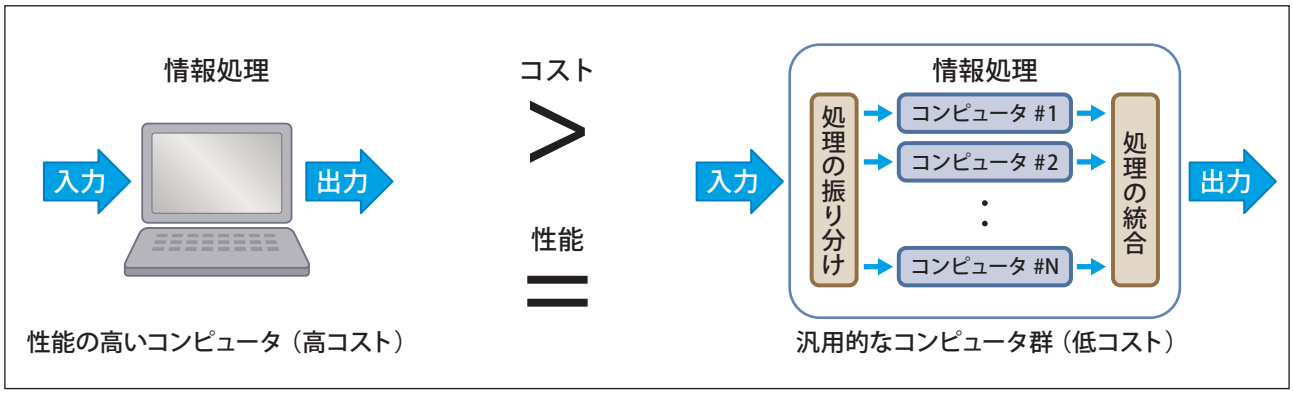
情報処理能力（性能）が高いコンピュータは一般的なコンピュータよりも高価になりますが、一般的なコンピュータでも複数台を動かして分散処理（並列運転）することで、トータルとしての情報処理能力を向上させる「分散処理」技術が存在します。

分散処理とは、情報処理を複数のコンピュータに振り分けることで処理能力を高める技術です。

処理性能を向上させる手段として、コンピュータ単体の能力アップから安価な汎用コンピュータを複数構成にすることで、情報処理能力の確保を質から量に置換し、高い処理能力を柔軟に提供することが可能です。

結果として、分散処理により、コストパフォーマンスの高い情報処理能力の確保が可能となります。

分散処理のイメージ



②仮想化

１台のコンピュータの処理能力は、通常の利用では持てる性能の数パーセント程度しか利用していないことが多く、余力のある状態となります。もし、物理的なコンピュータの処理能力を最大限に活用できれば非常に効率のよいシステムが構成できます。

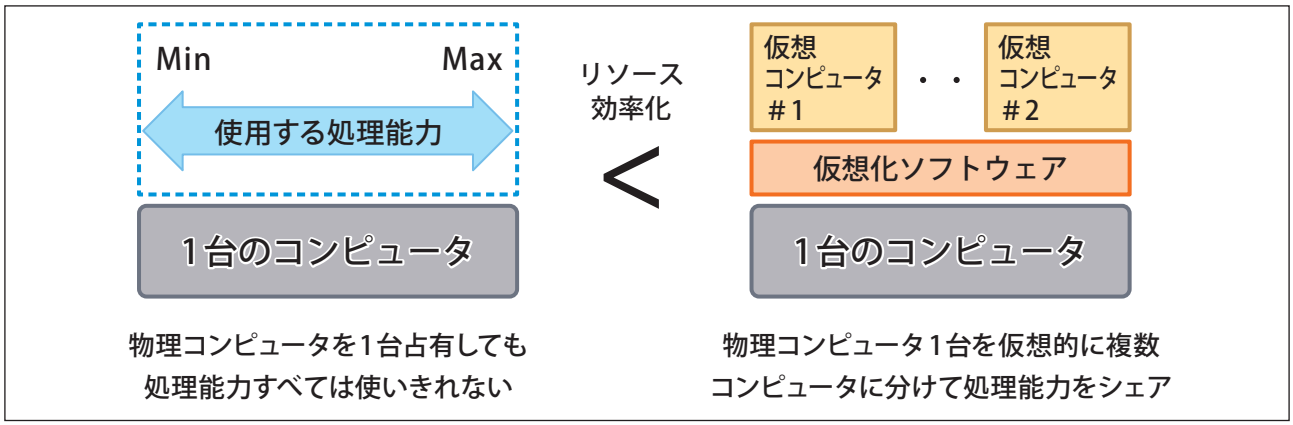
仮想化とは、1台のコンピュータ上に複数の仮想的なコンピュータを構成する技術のことです。これにより、コンピュータの処理能力を最大限に使うことが可能となります。

仮想化により、情報処理能力を確保するための手段として、物理的にコンピュータを毎回用意しなくても、コンピュータの処理能力で余っている部分を新たに割り当てることで、処理能力を確保することができるようになりました。

仮想化により、コストパフォーマンスを向上させることに加え、情報処理能力の提供を運用設定で用意することが可能となります。データを蓄えるストレージ[1]やルータ・スイッチ等のネットワーク機器といったハードウェアも仮想化が可能です。

1：ストレージとはデータの記憶装置で、コンピュータが利用するプログラムやデータなどを長期間に渡って固定的に保存する用途に用いられます。

仮想化のイメージ

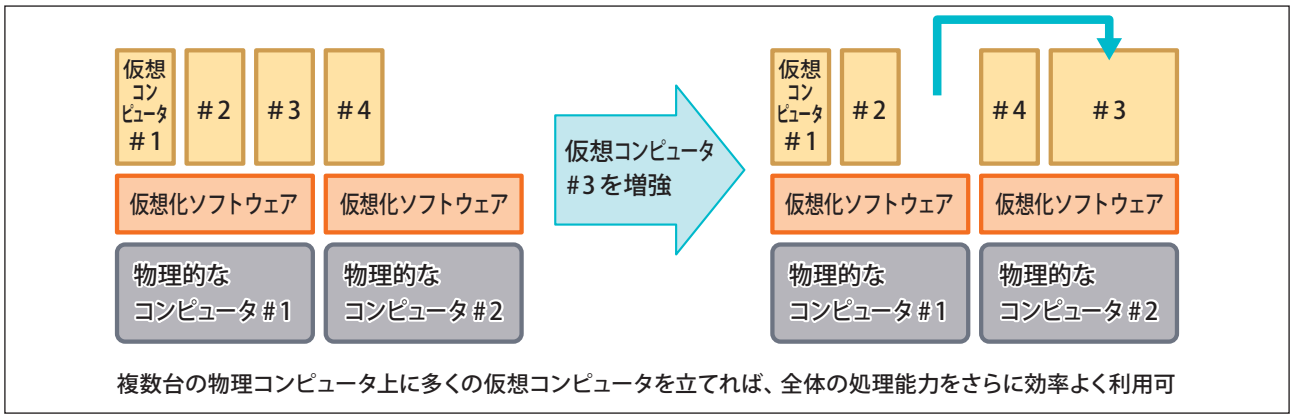


③運用技術

仮想化により、仮想コンピュータ上で稼動させるシステムに必要な情報処理能力に応じて、その能力を柔軟に割り当てることが可能となります。そのため、あらかじめ物理的なコンピュータを複数用意しておけば、物理的なコンピュータ全体の情報処理能力の余力を見ながら、運用設定で必要な能力を確保して仮想コンピュータを構成することが可能となります。

従来は必要な情報処理能力を確保するためには物理的なコンピュータの調達・構築が必要で、多くの準備期間と費用を要しましたが、仮想化を運用設定で実現する技術の進展により、必要な情報処理能力を迅速に提供することが可能となりました。さらに稼動中の仮想コンピュータを停止させずに他の物理的なコンピュータ上に移動させる「ライブマイグレーション」と呼ばれる技術も生み出され、より効率的で柔軟な情報処理能力確保が可能となっています。

仮想化のイメージ



④高速・常時接続型インターネットの普及

クラウド自体は、クラウド事業者が利用するデータセンター[2]において、クラウド利用者向けに情報処理能力を提供するものですので、クラウド利用者がサービスを受けるには、データセンターまで通信回線を用意する必要があります。その点では昨今、光ファイバに代表される高速・常時接続型のインターネット接続

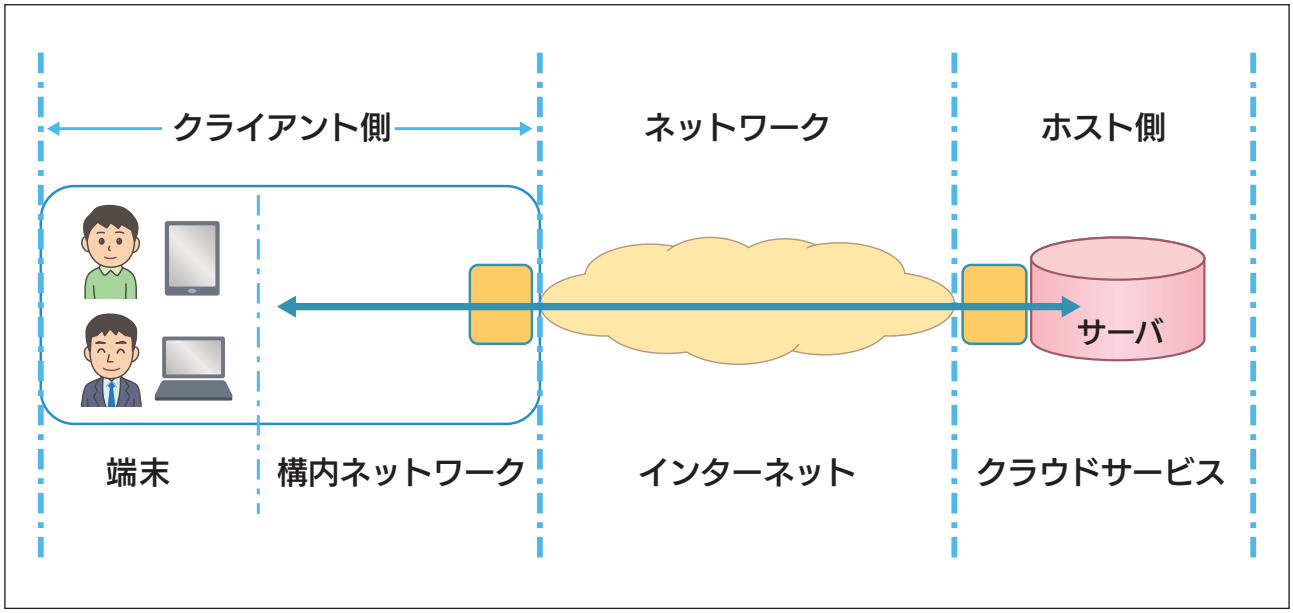
2：データセンターとは、外部へ機能やサービスを提供するためのサーバコンピュータなどを設置・運用するための施設です。構内には大量のコンピュータや通信装置、ケーブルなどがあり、これらが専用のラックに高密度に配置されています。

サービスが世界的に普及したため、クラウド利用者はインターネットを通信回線として用いて、全世界のデータセンターと常時接続できるようになりました。ネットショッピングやネット動画サービス等の世界的な普及は、クラウド環境と高速・常時接続型インターネットで支えられているといっても過言ではありません。

なお、情報セキュリティの観点から通信回線としてインターネットを用いずに、プライベート接続型[3]の回線サービスを利用する場合もあります。

3：プライベートネットワークとは、内部での通信のために用いられるコンピュータネットワークで、専用線、IP-VPN 等いくつかの種類があります。クラウド利用者のシステムとクラウドサービスを提供するデータセンター間で通信の傍受等の心配がない点が特徴です。

クラウド利用モデル

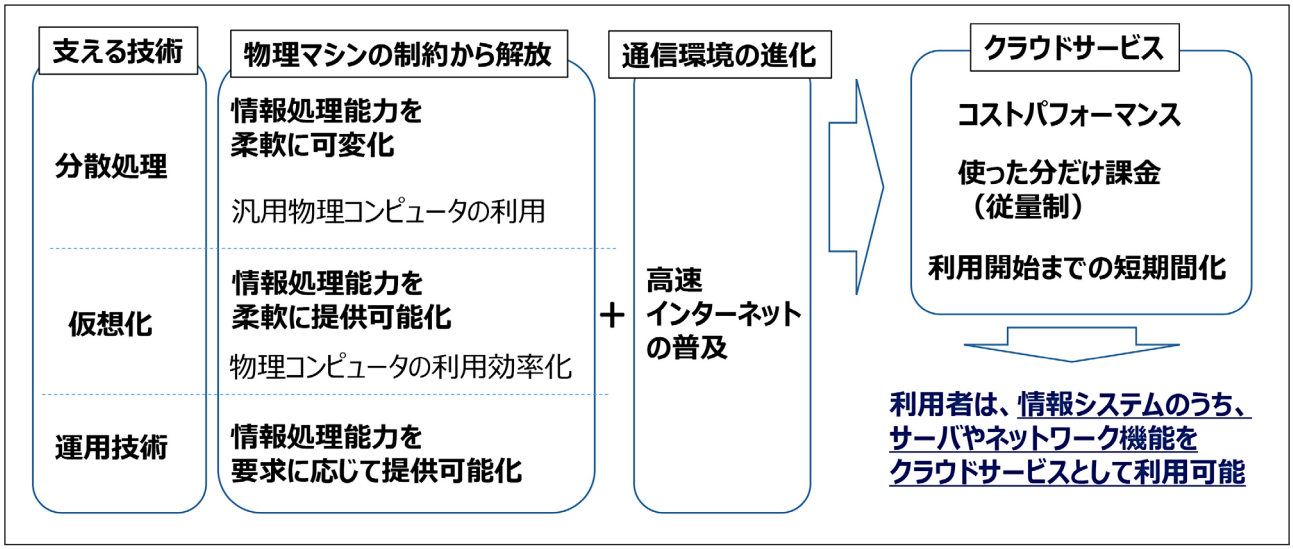


クラウドサービスとは、情報処理を行うホスト[4]側をサービス提供するものであり、利用者（クライアント）はネットワークを介してクラウドを利用します。

⑤クラウドサービスの特徴

クラウドサービスは、①～④で述べた技術や環境を組み合わせることで成り立っております。クラウドサービスの特長が生み出された流れを以下に示します。

クラウドサービスの特長が生み出された流れ



4：ホストとは、ネットワークを介して利用者からの要求に応えるためにサーバにネットワーク機能を含めたものです。クラウドサービスは、このホスト機能をサービスとして提供します。

（2）クラウドサービスの４つのメリット

前項に記した技術の組み合わせによって、情報処理能力を確保するために自前で物理的なコンピュータを用意することから解放され、情報処理能力をサービスとして利用することが可能となった点がクラウドサービスの本質と言えます。そこから、教育分野におけるクラウド活用の４つのメリット[5]が考えられます。

5：４つのメリットについては、本編「教育分野におけるクラウド活用とは～４つのメリット～」を参照ください。

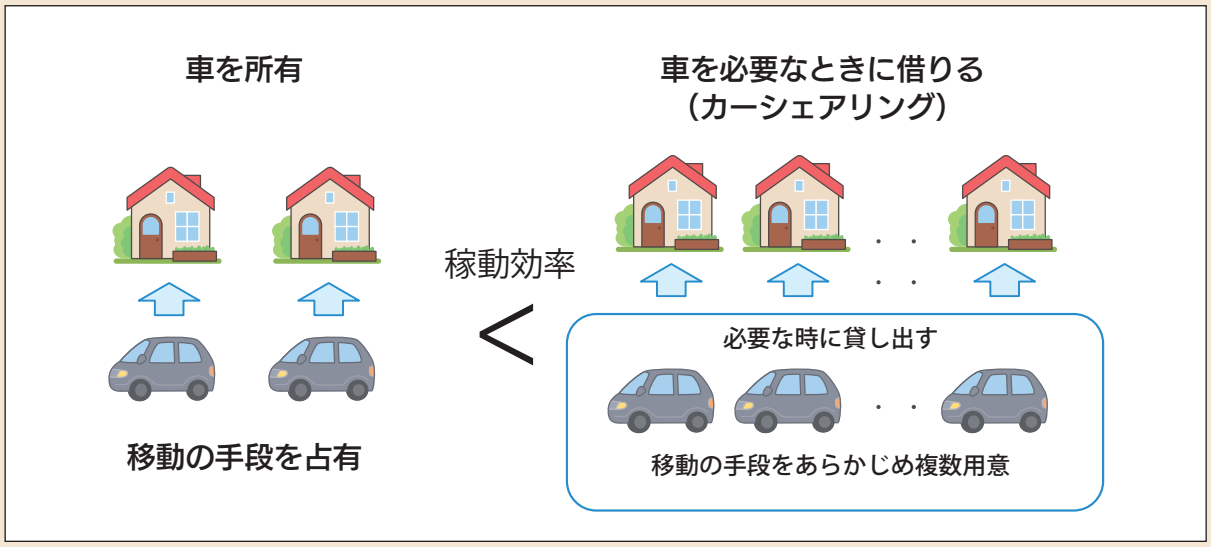
＜コラム＞　所有（占有）から利用へ

クラウドサービスの利用は、「サーバ[6]を核としたホスト機能を自前で構築して使うことから、外部の情報処理能力をサービスとして利用することへの価値の転換」と言えます。所有から利用への転換により、自前で行う行為がクラウド事業者に委ねる行為に変わります。

ただ、これは新しい概念ではなく、以前より類似事例が存在します。車に例えて考えてみましょう。車を所有するのは、いつでも乗ることができるようにするためですが、実際に車を使っている時間は限られているのではないでしょうか。あまり車を動かす機会のない人にとって、別に所有しなくても必要な時にすぐに車を借りられれば非常に便利で安上がりです。カーシェアリングは、複数の人が時間を分けて車を利用することで車の稼動率が上がり、利用料を支払うサービス形態です。このように、車の所有からシェアリングサービスに切り替えることで、車を所有することと同等の利便性を安価に調達できます。コンピュータについても、車と同様に考えることで、「所有から利用へ」のクラウドサービスの本質が垣間見えます。

6：サーバとは、サービスを提供するコンピュータです。利用者端末からの要求に対して情報や処理結果を提供する機能を果たす側のコンピュータやソフトウェアを指します。

所有から利用へ（※車にたとえた場合）



（3）クラウドのサービスモデル

クラウドが提供するサービス形態は「SaaS（サース、サーズ）」「PaaS（パース）」「IaaS（アイアース、イアース）」の 3 種類があります。サービス形態とは、どこまでをクラウド事業者が提供するか（ホスト機能のどこまでをクラウド事業者に任せるのか）の範囲から分類したものです。

クラウド事業者と利用者の役割分担（サービスモデル別）

<table>
<tr><th>レイヤ</th><th>オンプレミス</th><th>IaaS</th><th>PaaS</th><th>SaaS</th></tr>
<tr><td>データ利用</td><td rowspan="10">利用者</td><td rowspan="5">クラウド利用者</td><td rowspan="4">クラウド利用者</td><td>クラウド利用者</td></tr>
<tr><td>インタフェース</td><td rowspan="9">クラウド事業者</td></tr>
<tr><td>アプリケーション</td></tr>
<tr><td>バックアップ管理</td></tr>
<tr><td>ミドルウェア管理</td><td rowspan="6">クラウド事業者</td></tr>
<tr><td>OS管理</td></tr>
<tr><td>仮想マシン管理</td></tr>
<tr><td>仮想化ソフト管理</td></tr>
<tr><td>ハードウェア管理</td></tr>
<tr><td>ラック管理</td></tr>
<tr><td>物理施設/データセンタ</td></tr>
</table>

*オンプレミスとは、サーバ等のホスト機能を利用者が自前で構築する手段を指します

① SaaS（Software as a Service）

ソフトウェア（学校で利用するアプリケーションやコンテンツ）をサービスとして提供する形態です。例えば、校務分野では統合型校務支援サービス、授業・学習分野では教材配信、タブレット向けのデジタルドリルサービス、授業支援ソフトなどが考えられます。利用者側がインターネットにつながる環境があれば、そのまま利用することが可能です。

② PaaS（Platform as a Service）

プラットフォームをサービスとして提供する形態です。ここでのプラットフォームとは、クラウド利用者が利用したいアプリケーションを搭載すればすぐに利用できるように、ホスト機能のミドルウェアまでのレイヤ[7]を提供することを指します。

また、アプリケーションの開発環境としても利用できるため、開発目的で利用される場合も多いです。

③ IaaS（Infrastructure as a Service）

クラウド事業者がサーバやストレージ、ネットワークなどのハードウェアが提供する機能を提供するサービスです。ホスト機能のインフラ提供サービスと言えます。ホスティングサービスと類似していますが、ホスティングサービスは、コンピュータやネットワーク機器等の物理的なハードウェアをサービス提供するものですが、IaaS では、仮想化されたコンピュータやネットワーク機器等をサービス提供するところが異なります。

利用者は、IaaS 上に自前で OS、ミドルウェア、アプリケーションを用意して利用します。

クラウドサービスの種類により、クラウド事業者とクラウド利用者の役割分担が変わりますので、情報セキュリティの観点からは、どのサービスモデルを利用するかで責任範囲が変わることにご留意ください。

また、クラウド利用者とは、クラウドの実質的な利用者（教育委員会等）とクラウドの実質的な利用者から委託を受けて情報システムを構築・保守する事業者（ＳＩ事業者）に分けられます。

7：レイヤとは、ホストが果たすべき情報処理機能を階層構造化したものです。最も下位がコンピュータ等の機器保管場所等の物理層であり、その上位にハードウェア層、その上位にミドルウェア層、その上位にアプリケーション層といった形で情報処理機能を層別けした概念です。SaaS/PaaS/IaaS はどこまでのレイヤを提供するかで分類されます。

クラウド事業者と利用者の実態的な役割分担（サービスモデル別）

<table>
<tr><th>レイヤ</th><th>オンプレミス</th><th>IaaS</th><th>PaaS</th><th>SaaS</th></tr>
<tr><td>データ利用</td><td>利用者</td><td>クラウド利用者</td><td>クラウド利用者</td><td>クラウド利用者</td></tr>
<tr><td>インタフェース</td><td rowspan="9">SI事業者</td><td rowspan="5">SI事業者</td><td rowspan="3">SI事業者</td><td rowspan="9">クラウド事業者</td></tr>
<tr><td>アプリケーション</td></tr>
<tr><td>バックアップ管理</td></tr>
<tr><td>ミドルウェア管理</td><td rowspan="6">クラウド事業者</td></tr>
<tr><td>OS管理</td></tr>
<tr><td>仮想マシン管理</td></tr>
<tr><td>仮想化ソフト管理</td></tr>
<tr><td>ハードウェア管理</td></tr>
<tr><td>ラック管理</td></tr>
<tr><td>物理施設/データセンタ</td><td>建設系事業者</td></tr>
</table>

＜コラム＞　サプライチェーン

サプライチェーンとは、消費者に届くまでの調達、生産、流通を含む一連のビジネスプロセスを複数の企業が役割分担する複合的な供給形態を指します。クラウドサービスにおいては、SaaS 事業者の多くは、サービスを提供するインフラ基盤（ネットワークやハードウェアの機能）を IaaS 事業者から供給されています。この場合、インフラ基盤に関する情報セキュリティ対策は、SaaS 事業者が自ら実施するものではなく、IaaS 事業者に委託する形になります。

SaaS 事業者は IaaS を利用している場合でも、クラウド利用者に対して、クラウドサービス全体のセキュリティ対策の責任を負うに立場あります。そのため、SaaS 事業者は自ら実施するクラウド運用やセキュリティ対策と IaaS 側に委託する役割と責任の所在を明確にしておかないと、システム障害やセキュリティ事故時の調査等で支障が生じます。

クラウド利用者は、SaaS 事業者に対して、サプライチェーン構造と、委託先と情報セキュリティ対策をどのように分担しているかを確認することが必要です。

サプライチェーンの例

<table>
<tr><th>レイヤ</th><th>SaaS</th></tr>
<tr><td>データ利用</td><td>クラウド利用者</td></tr>
<tr><td>インタフェース</td><td rowspan="6">SaaS事業者
（自前提供）</td></tr>
<tr><td>アプリケーション</td></tr>
<tr><td>バックアップ管理</td></tr>
<tr><td>ミドルウェア管理</td></tr>
<tr><td>OS管理</td></tr>
<tr><td>仮想マシン管理</td></tr>
<tr><td>仮想化ソフト管理</td><td rowspan="4">SaaS事業者
（IaaSを利用）</td></tr>
<tr><td>ハードウェア管理</td></tr>
<tr><td>ラック管理</td></tr>
<tr><td>物理施設/データセンタ</td></tr>
</table>

（4）クラウドの実装モデル

特定のユーザだけにクラウドを利用させるのか、多くのユーザが利用できるのかなどの利用機会の対象範囲（実装形態）によって、パブリッククラウド、プライベートクラウド、コミュニティクラウド、ハイブリッドクラウドの 4 つに分けられます。

①パブリッククラウド

名前のとおり、クラウドサービスを不特定多数の利用者が共同で利用する形態です。インターネット上には、メールサービスやストレージサービスなど登録するとすぐに利用できるサービスがありますが、これらはパブリッククラウドに相当します。

多くの利用者が共同で利用する形態のため、

（ア）定型的なサービス提供になりますので、クラウド利用者の個別カスタマイズ対応は原則困難です。

（イ）どこからでもアクセス可能な「インターネット」を通信回線として利用する形が一般的です。

授業・学習分野で提供されるデジタルドリルサービスやコンテンツ配信などは、多くの学校向けにサービス提供する形態ですので、原則パブリッククラウドモデルになります。

②プライベートクラウド

クラウドのプライベート利用になりますので、クラウド環境を特定のクラウド利用者に専用で利用させるサービスになります。スケールメリットを活かせる規模の大きな自治体等が利用するケースが多く、パブリッククラウドよりもカスタマイズ要望に沿ったサービス提供が可能な点があると考えられます。

③コミュニティクラウド

名前のとおり、コミュニティ（特定の共同体）としてクラウドを共同利用する形態です。パブリッククラウドでも複数利用者の共同利用形態ですが、パブリッククラウドでは不特定多数の利用者を前提としている点に対して、コミュニティクラウドでは共通の利用目的をもつ特定の共同体の専用使用である点が特徴です。教育分野では、パブリッククラウドとコミュニティクラウドの差がはっきりしない場合が多いと考えられます。パブリッククラウドは多数のユーザが利用する共用サービスを想起させますが、教育分野に限っては、クラウド利用のエンドユーザは教職員や児童生徒であり、用途もほぼ共通と考えられますので、コミュニティクラウド的な利用と言っていいでしょう。

例えば、県教育委員会が同県の市町村向けに統合型校務支援サービスを提供する場合は、コミュニティクラウドと言えます。

④ハイブリッドクラウド

パブリッククラウド、プライベートクラウド、コミュニティクラウドを組み合わせて利用する形態です。上記のクラウドモデルのなかで、コミュニティクラウド及びハイブリッドクラウドは、パブリッククラウドまたはプライベートクラウドの応用的な利用モデルですので、次の記載においては、パブリッククラウドとプライベートクラウドの 2 つのモデルについて記述します。

＜コラム＞　クラウドサービスモデル・実装モデルをオフィスにたとえた場合

クラウドサービスモデル・実装モデルについて、オフィスに例えて考えてみましょう。
情報システムの黎明期では、ホスト側を自前構築するオンプレミス型[8]が主流でした。これは、土地を所有（サーバ室を自前で建設）して、そこに建物を建てる（サーバ、ストレージ、ネットワーク機器等のハードウェア・ソフトウェアを自前構築）ことに例えられます。多くの自治体ではまだオンプレミス型が主流であり、庁舎のサーバ室にサーバ等の機器を自前で設置・運用しています。

クラウドサービスは、実際に土地を所有するわけではなく、建物を借りるケースに例えられます。次にあげる例では、ある土地に建物を建てることで４倍の床面積を確保することができました。

ここで、スペースの借り方は２種類あります。

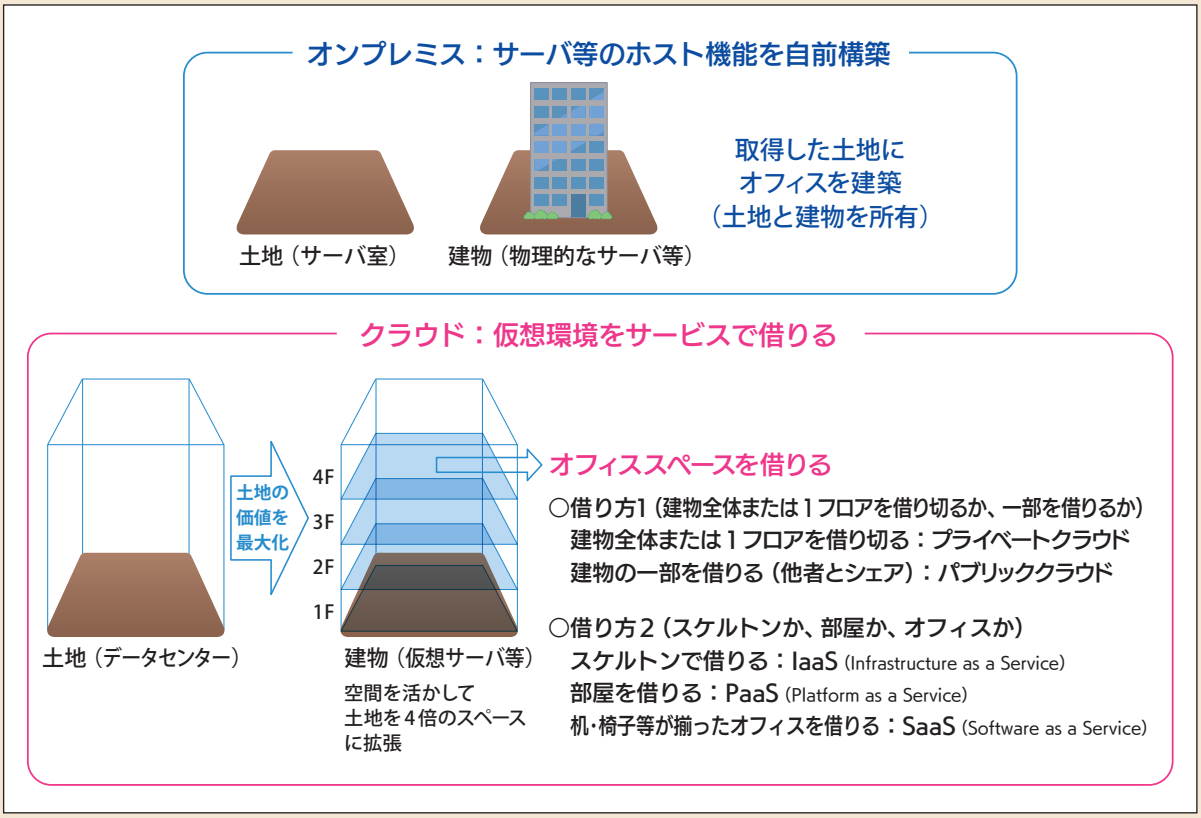
借り方の１つ目は、建物全体または１フロアを借り切る形か（プライベートクラウド）、建物の一部を借りて他者とシェアする形か（パブリッククラウド）です。これがクラウドの実装モデルの例えです。

借り方の２つ目は、どのような状態で部屋を借りるかです。内装も施されていないスケルトン状態で空間を借りて、自分でオフィスの内装や部屋の仕切りを設けて自由設計でオフィスを構えるケースが IaaS に例えられます。PaaS はオフィスの内装工事済の部屋を借りる形に例えられます。この場合は、机や椅子、書庫などを自前で調達すればオフィスとして使えます。SaaS は、机や椅子、書庫などが整っておりすぐにオフィスとして利用できる形で借りる形態に例えられます。

クラウドサービスモデルと実装モデルは独立した分類概念ですので、サービスモデルと実装モデルの組み合わせで様々なクラウドモデルが存在します。

8：オンプレミス型とは、ホスト機能（サーバ、ネットワーク接続機器等）を自前で構築する手法のことです。サーバも自分の場所の中に構築します。例えば自治体の場合であれば、市役所のサーバ室にサーバが設置される場合が該当します。

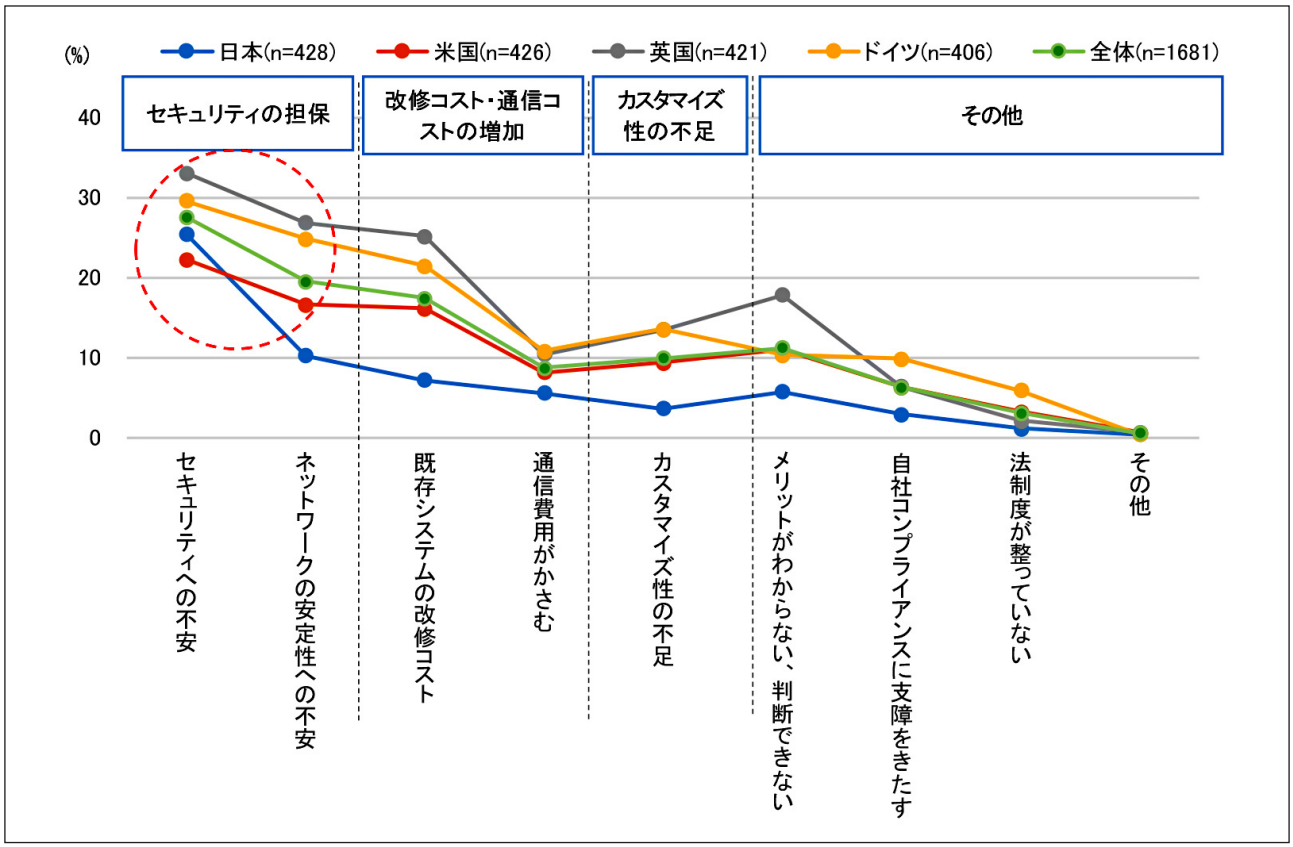
クラウドサービスモデル・実装モデルについて（※オフィスにたとえた場合）



（5）クラウドサービスの留意点

クラウドサービスは、前項で示したような特長を有していますが、一方で利用に慎重な見方があります。その要因としては、セキュリティへの不安が上がっています。

クラウドサービスの導入に対する課題の内容



※出典：「ＩＣＴによるイノベーションと新たなエコノミー形成に関する調査研究」図 2-35（平成 30 年版）（総務省）

①クラウドサービスならではの特性に起因する留意点

（ア）仮想化	クラウド利用者が利用する仮想環境を構成する物理環境に障害が発生した場合や、物理環境の老朽化等の理由により、仮想環境を別の物理環境に移設する場合があります。この物理環境の故障対応に伴い、ハードディスクの交換が行われる場合がありますが、データを消去しないまま交換を行うと、格納されたデータが流出するリスクがあります。
	利用する仮想環境の物理コンピュータ環境（利用者データの保管先）がどこにあるかについては、はっきりしない場合や海外のデータセンターに保管される場合があります。日本の法令が及ばない場所にデータセンターがある場合には、データ保護に支障をきたす場合がありますので、クラウドサービスを利用する場合には、データ保管先が日本の法令が及ぶかどうかを確認する必要があります。

（イ）マルチテナント	マルチテナントとはパブリッククラウドサービスにおいて、1つの仮想環境（アプリケーション、データベース）を多くの利用者が共用する形態のことです。この場合、特定の利用者の振る舞いが他の利用者に影響を与えるリスクがあります。利用者単位でデータベースを分離している場合は安全ですが、同じデータベースを多くの利用者が共用する場合などは、他利用者の影響を受けるリスクがあります。
	パブリッククラウドサービスでは多くの利用者に対して、均一なサービスを提供するため、利用者毎の個別対応は困難な場合が多いのが特徴です。例えば、利用者が直接セキュリティ監査を実施することが困難です。第三者の監査人による監査レポートをもって監査の証跡とする形態が一般的ですが、この形態がクラウド利用者の内部統制ルールに合わない場合があります。
（ウ）サプライチェーン	クラウドサービスは、サービス提供元のクラウド事業者内のみでサービス運営が完結している訳ではなく、サービスの開発・提供に関する一部業務を取引先や子会社等に外部委託していることがあります。このような場合、クラウドサービスのセキュリティレベルは、クラウドサービスを提供しているクラウド事業者単独でのセキュリティレベルだけでは決まらず、各関係者のセキュリティレベルにも依存します。そのため、どれだけクラウド事業者が堅牢なセキュリティ対策を実施していたとしても、外部委託したクラウド事業者側でセキュリティ事故が発生するリスクがあるため、委託先管理を適切に実施していないクラウド事業者には、サプライチェーンのリスクがあります。

＜コラム＞　サプライチェーンのたとえ

※サプライチェーンの詳細については、P8 のコラムを参照ください。

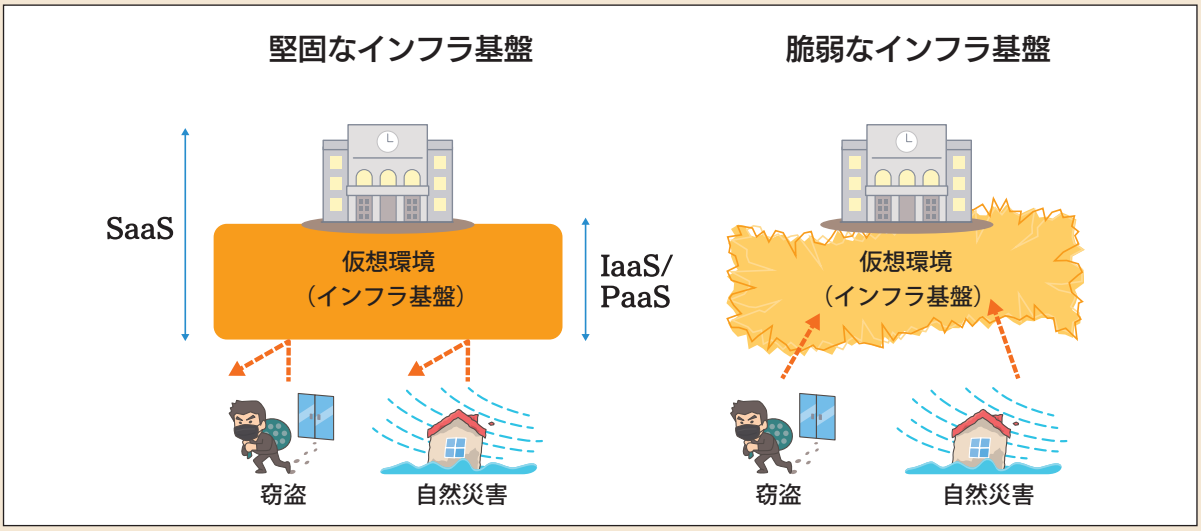
パブリッククラウドサービスの利用について、オフィスを調達する場合に例えてみましょう。

オフィスを土地と建物に分けると、建物を提供するのが SaaS パブリッククラウド事業者で、土地を提供するのが IaaS(PaaS) 事業者に例えることができます。建物は部屋数や間取りといった住み心地（サービス提供機能）や隣と遮音できているか（マルチテナントの安全性）は SaaS 事業者に問う内容と似ています。一方で、台風や地震などの自然災害リスク（データセンターの堅牢性）は、どのような土地に建物が建っているかに依存します。

例えば集合住宅を購入する際、どの土地にどんな建物が建っているか、土地と建物の両方を考えて検討するのではないでしょうか。クラウドサービスに例えると、土地がインフラ基盤を提供する IaaS(PaaS) 事業者であり、建物が SaaS 事業者に相当します。

よって SaaS 事業者に対しては、サービスの内容だけではなく、どのインフラ基盤を利用しているかを確認し、安全性を必ず確認することが必要です。

サプライチェーンのイメージ



＜コラム＞　海外の法規制例

アメリカの「愛国者法」では、政府や FBI は、裁判所の命令なしで国内のコンピュータやサーバ内のデータを調査することを可能としており、FBI が調査のため 2009 年に、あるデータセンターを差し押さえ、サーバを強制的に停止したため、このデータセンターを利用していた顧客がデータベースにアクセスできなくなる状態となりました。

この「愛国者法」はすでに廃止されていますが、日本の法令が及ばない海外にデータを保管する際には、長期間データが利用できない状態になるリスクがゼロではないことに留意が必要です。

留意点のひとつは、クラウド事業者の法人としての所在地とは別に、データセンター所在地により適用法令が決まりますので、クラウド利用者はデータ保管場所を事前に確認することが必要です。

留意点の２つ目は、各国でデータ保護に関わる規制や法令が公布されておりますので、日本の法令が及ばない海外にデータを保管する際には、最新の情報に基づいてリスクを確認することが望まれます。

②サービス利用型外部委託に起因する留意点

サービス利用型外部委託では、サービス提供条件は原則提供事業者側で定めるため、条件の中身を充分に確認する必要があります。特に SaaS・パブリッククラウドサービスは、多数の利用者向けに同一コンテンツやアプリケーション提供を想定しており、利用者はあらかじめ定められたサービス提供条件に原則沿った形で利用することになります。そのため、サービス利用者の内部統制[9]基準や情報セキュリティポリシーに沿ったセキュリティ運用を委託交渉しても難しい場合が考えられます。

その場合は、別の SaaS を選定するか、SaaS から IaaS(PaaS) に切り替えてアプリケーション等を自前で構築するか、利用者専用の環境を用意するプライベートクラウドやオンプレミス[10]でシステムを構築するなどの代替手段が考えられます。

以上のような状況を踏まえたうえで、複数の候補のなかで最も適した事業者のサービスを選定し、その提供ポリシーが利用者として受け入れ可能かを検討することになります。

（ア）自組織の情報セキュリティポリシー等との適合性

クラウド利用者による直接監査ができない、再委託先の管理状況が曖昧など、クラウド事業者のサービス提供ポリシーが自組織の情報セキュリティポリシーや個人情報保護法制を満たしてないリスクがあると考えられます。その場合は、情報セキュリティポリシーの見直しや個人情報保護法制をクリアする手続きを考える必要があります。

（イ）責任分界点・役割分担

契約や利用規約で示されるクラウド事業者の責任分界点が曖昧であると、クラウド利用者との役割分担上、セキュリティに関する一部の管理が行き届かなくなってしまい、必要なセキュリティ要件への不適合をもたらす場合があり得ます。

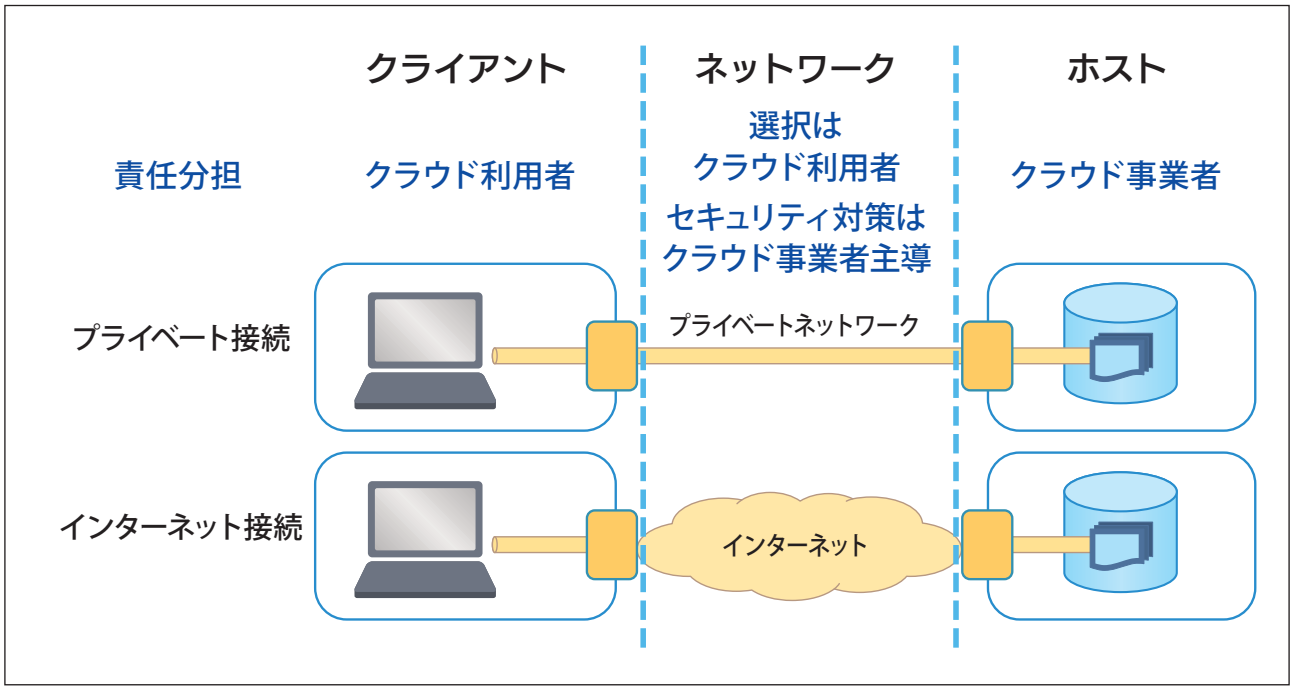
クラウド事業者側の責任分界点を確認して、クラウド利用者のセキュリティ対策との組み合わせで補完関係が築けるかを確認する必要があります。

ネットワークに対するセキュリティ確保について、クラウド事業者はクラウド利用者に対して説明責任があります。特にインターネット接続型では、通信経路上の暗号化施策が必須であるため、クラウド事業者が利用者にセキュリティ確保の機能を指示して、双方で合意する必要があります。

9：内部統制とは全職員が遵守すべき、組織内のルールや仕組みのことを言います。

10：オンプレミス型とは、ホスト機能（サーバ、ネットワーク接続機器等）を自前で構築する手法のことです。サーバも自分の場所の中に構築します。自治体の場合は、市役所のサーバ室にサーバが設置される場合が該当します。

クラウド利用者とクラウド事業者の責任分担



（ウ）ベンダロックイン

クラウド事業者のサービス仕様により、データフォーマットや処理方法等が限定され、他のクラウド事業者にデータを移行できないリスクがあります。ベンダロックインとは、一旦導入したクラウドサービスを簡単に移行できず囲い込まれることを意味します。

ベンダロックインを完全に避けることは難しいのですが、検討段階において、サービス終了後にはどのようなデータフォーマットで返却されるのかを確認しておくことが望ましいです。画像データの場合には圧縮保管される場合もありますので、注意が必要です。

（エ） サービス提供の継続性

クラウド事業者の経営不振や経営方針変更などに起因して、一方的にサービスを停止する場合があります。

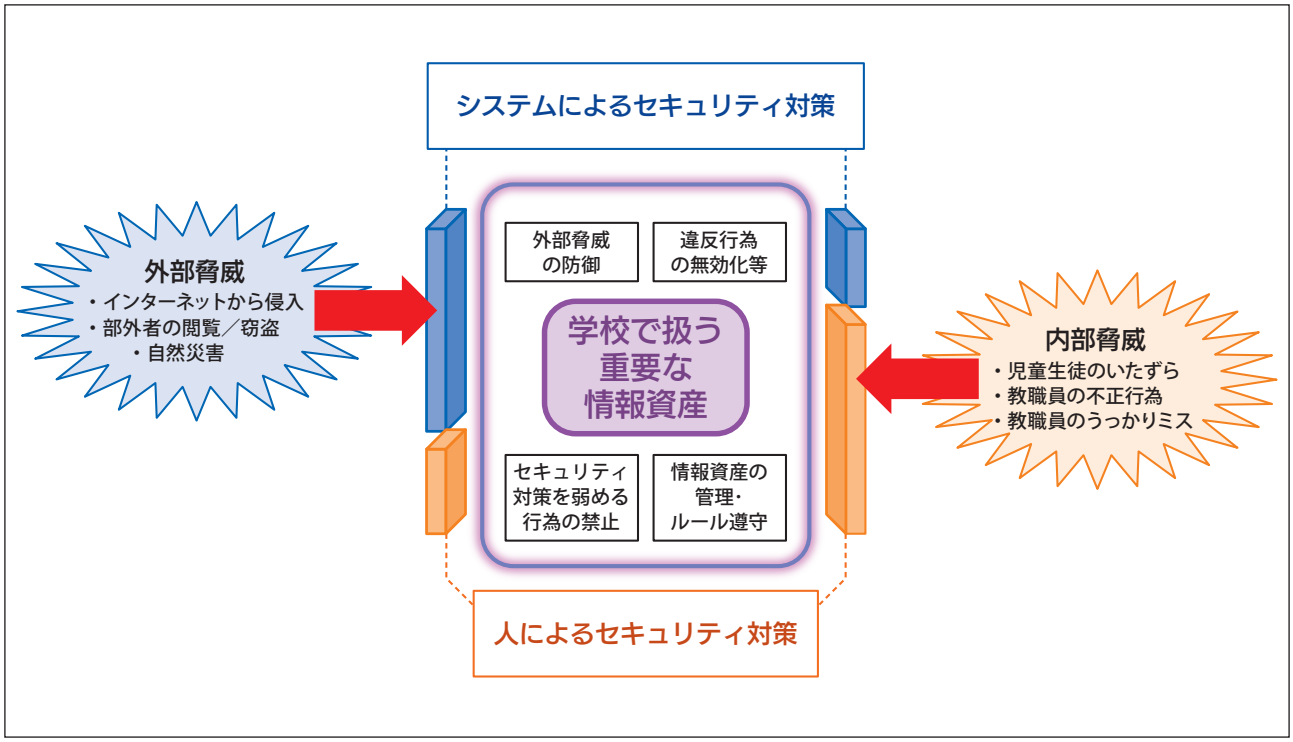
クラウド事業者選定の際には、その点を充分に留意したうえで、サービス停止リスクに対しては、契約のなかで「サービス停止の〇〇ヶ月前に通告する義務」を課すなどを織り込むことが考えられます。

参考2 教育情報セキュリティの基本

（1）情報セキュリティ対策の概念

情報セキュリティ対策の概念を示します。情報セキュリティ対策は、システムによる守り方（システム面での対策）と人による守り方（人的面での対策）の合わせ技で機能します。その双方を規定するものが「情報セキュリティポリシー」です。

情報セキュリティ対策の概念



情報セキュリティ対策がシステム面と人的面の合わせ技である以上、互いに補完関係にあり、システム面の対策が不充分な場合には、人的面の対策で埋め合わせることになります。

なお、システム面の対策として、情報資産を取り扱う者が不正利用できないようにガードし、内部脅威の抑止効果を高める側面もあります。同様に、システムを扱う者がシステム面のセキュリティレベルを下げないように人的対策（抑止ルール）で縛る側面もあります。

システム面と人的面の対策は、システム面が前提条件であり、人的面が補完条件と考えることもできます。情報資産を取り扱う教職員の立場からは、人的面のセキュリティ対策は、業務上の制約になる場合があるため、なるべくシステム面での対策を厚くして、人に課すセキュリティ対策を軽くするというケースも考えられます。

（2）情報資産の分類

「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）では、情報資産の分類を重要性に基づき 4 種に分類する考え方となっており、重要性分類は、セキュリティ侵害時の影響度でクラス分けされています。

自治体の情報資産の分類の考え方は、首長部局の考え方を準用しているケースが多く、必ずしもガイドラインに沿っていない場合もありますが、重要なのは、分類定義が実際に使えるものになっているかです。

例えば、重要性の基準が抽象的ですと、学校で分類する際に判断にばらつきがでます。また、個人情報を全て重要な情報に定義してしまうと、学習系情報が授業・学習のなかで利用するうえで、自由に見せ合うことが困難になるなど、大きな制約[11]になります。

情報資産の分類は情報セキュリティの要です。学校の情報が、どの分類に属するかははっきりさせて台帳管理[12]することが求められます。

11：児童生徒が授業や学習活動を通して生成する学習系情報には個人情報が含まれると考えてください。例えば、作文には友人の氏名が記載される場合がありますし、写真や動画を撮影した場合には児童生徒の顔やゼッケンといった個人情報が映り込むことは起こり得ます。

12：情報資産の管理台帳を整備することをお勧めします。情報資産ごとに、重要性分類・保存期限・保存場所・管理担当者・外部持ち出し制限（禁止・学校管理者の個別許諾要・制限なし等）を決めておくことが重要です。

情報資産の重要性分類

	重要性分類	セキュリティ侵害が及ぼす影響	情報資産の例	取り扱い
学校で管理が必要な情報 重要な情報	Ⅰ 機密性３ 完全性２Ｂ 可用性２Ｂ	教職員又は児童生徒の生命・財産・プライバシー等へ重大な影響を及ぼす	指導要録原本	特に許された教職員のみが扱える
学校で管理が必要な情報 重要な情報	Ⅱ 機密性２Ｂ 完全性２Ｂ 可用性２Ｂ	学校事務及び教育活動の実施に重大な影響を及ぼす	機微な校務情報名簿類	教職員のみが扱える（校務分掌等で扱える範囲は限定）
学校で管理が必要な情報 次に重要な情報	Ⅲ 機密性２Ａ 完全性２Ａ 可用性２Ａ	学校事務及び教育活動の実施に軽微な影響を及ぼす	学習系情報（ﾜｰｸｼｰﾄ、作品等）	授業・学習の中では自由に使うが、外部には漏らさない
守らなくてもほとんど影響ない情報	Ⅳ 機密性１ 完全性１ 可用性１	影響をほとんど及ぼさない	作成教材、行事予定・・	規定なし

※「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）を元に作成

①重要な情報（重要性分類Ⅰ及びⅡ）

重要な情報は、「機密性」が高いため、外部への情報漏えいに対して必要充分な防御が求められます。同様に「完全性」が高いため、情報の改ざんや滅失に対しても必要充分な防御が求められます。「可用性」とは利用したいときにいつでも利用できることを担保することです。学校での校務事務は、毎日行われるもので、「可用性」も高く、信頼性の高いシステムの維持が求められます。

※なお、「機密性」とは情報が漏えいしない状態を保つこと、「完全性」とは情報が改ざんされないよう元の状態を保つこと、「可用性」とは情報がいつでも利用できる状態を保つことを意味します。

重要な情報のほとんどは、「機微な校務系情報」です。ここで「機微な」という言葉は、児童生徒の成績情報や保健観察情報（病歴を含む）、学籍情報（家族構成、児童生徒保護者の職業等）といった、他者に知られると当該児童生徒にとって深刻な問題や支障をきたすプライバシー情報のことです。このような情報を学校のなかで取り扱うため、充分なセキュリティの確保が必要となります。

また、業務分類の視点から、「校務系情報」、「学習系情報」に区分することもできます。

重要性分類と業務分類の関係性

重要性分類の考え方	重要性分類（※）	業務分類	
		校務系情報	学習系情報
重要な情報資産 （機微な校務系情報）	Ⅰ、Ⅱ	多数含まれる	なし
次に重要な情報資産 （学習系情報）	Ⅲ	含まれる	多数含まれる
守らなくてもほとんど影響のない情報資産 （過去の行事案内、自作教材等）	Ⅳ	含まれる	含まれる

※「教育情報セキュリティポリシーに関するガイドライン」（文部科学省）参照

重要な情報資産（重要性分類）は機微な校務系情報（業務分類）とほぼ同じ集合になります。校務系情報はすべてが重要な情報であるわけではなく、教職員向けの研修資料、過去の行事案内等は、外部漏えい、改ざんが行われてもほとんど影響がない[13]ため、考え方次第では重要性分類Ⅳになります。

以降の解説において、重要性分類よりも、業務分類のほうがわかりやすい場合もありますので、機微な校務系情報と重要な情報と同じであると思ってください。

重要な情報は、高い「機密性」「完全性」を求められますので、外部漏えいや改ざんに対して充分な防御が必要です。そのため、取り扱う人を制限します。すなわち、重要な情報とは許可された教職員だけが取り扱える情報になります。

このように、情報資産の分類によって、取り扱い、外部持ち出し、保管、廃棄等情報の管理を規定する礎になることを理解ください。

②次に重要な情報（重要性分類Ⅲ）

「次に重要な情報」とは、セキュリティ侵害時に、重要な情報ほど深刻な影響はないものの、「軽微な影響」がある定義です。なお個人情報が含まれる場合は、個人情報保護法制により、「個人情報の安全管理義務」が生じますので、安全に管理しなければなりません。

「次に重要な情報」の典型的な例が、「学習系情報」です。「学習系情報」とは、子どもたちが、パソコンやタブレットを使って作成した作品・作文や書き込んだワークシート、動画や写真が該当します。

「学習系情報」には、個人情報を含むことが避けられないため、個人情報保護法の安全管理義務が生じます。そのため、学校の外に流出しないようシステム面の防御と、取り扱いでの配慮が求められます。

「教育情報セキュリティポリシーに関するガイドライン」（文部科学省）では、重要性分類Ⅲの管理について、重要性分類Ⅰ、Ⅱよりも緩和しています。

例えば、外部持ち出しの許可については、包括的許可で良いこととし、記録を残すことまで求めていません。

また、インターネット接続環境での情報資産の保管についても、「暗号化等の保護措置」を求めていません。

学校の実情から教職員の負担を考慮して、セキュリティ運用管理の手間を軽くしています。

文部科学省がガイドラインを自治体情報セキュリティガイドラインと別に制定した主な理由は、学校には児童生徒が存在し、彼らが生成する学習系情報について、現場の実情に沿った形で「情報資産の分類と管理」を規定しなければ、学習系情報も「重要な情報」扱いとなるため、自由な授業・学習活動を妨げることを考慮したことも背景のひとつです。

13：どの情報がどの分類に属するかは自治体判断になりますので、ここでは例として認識ください。

③守らなくてもほとんど影響のない情報（重要性分類Ⅳ）

守らなくてもほとんど影響のない情報は、セキュリティ管理をしなくても構わない情報です。公開を前提としているもので改ざんの影響がほとんどないもの（過去の行事案内等）や教員が作成するプリントや提示教材、教員の研修教材（個人情報が含まれず、一般的な情報）が該当[14]します。

但し、守らなくてもほとんど影響のない情報と思っていても、他者の著作権を二次利用しているケースでは、勝手に外部に提供・公開することは著作権違反になる場合があります。また、児童生徒の顔写真などを勝手に公開することは、「個人情報保護条例の違反」や「肖像権の侵害」になりますので、どちらも事前に承諾が必要なことにはご留意ください。

14：どの情報がどの分類に属するかは自治体判断になりますので、ここでは例として認識ください。

（3）情報資産の管理とセキュリティ対策

情報資産の管理体系は、重要性分類によって異なります。

身近な例として、自宅における物の管理で考えてみましょう。例えば、現金、キャッシュカード、印鑑、預金通帳と雑誌や新聞、チラシなどは重要性が異なることは明らかです。おそらく現金、キャッシュカード、印鑑、預金通帳などは、鍵のかかる場所に保管するでしょう（慎重な人なら、定期預金通帳や印鑑を銀行の貸金庫に保管するかもしれません）。しかし雑誌や新聞、チラシはテーブルなどに放置していませんか？これは、無意識のうちに、紛失・盗難を意識して、大事なものかどうかで保管方法に差をつけている行為です。

情報資産の管理もこれと同じ思想です。つまり、重要な情報であればあるほど、外部流出、改ざんなどのセキュリティ侵害を受けにくい対策を講じて厳重に管理します。
そのため、情報資産の重要度に応じた管理方法が必要になります。

①重要な情報資産（重要性分類Ⅰ、Ⅱ）の管理

機微な校務系情報に代表される重要な情報資産は、許可された教職員のみが取り扱い可能ですので、許可された教職員は、業務のなかで、自分以外の者に対して、この情報が閲覧や取り扱いができないようにガードすることが求められます。また、ルールとして、この情報に対して、児童生徒や外部から学校に訪問した人（外部委託業者、親御さん等）のアクセスを禁止し、学校からの外部持ち出しを禁止 (必要な場合は許可制にして、記録を残す) することが必要です。

上記の安全管理措置が「情報資産の管理」の本質です。

②次に重要な情報資産（重要性分類Ⅲ）の管理

学習系情報に代表される「次に重要な情報」の管理方法は、「重要な情報」と比較して、「保管」で情報資産への暗号化等は求められず、「情報資産の外部持ち出しルール」では、教育情報セキュリティ管理者の個別許可と持ち出し記録義務は不要で、「包括的許可」の適用が可となり、運用が緩和されます。

＜コラム＞　情報資産の管理とセキュリティ対策

情報資産の管理は、取り扱い・外部持ち出し・保管に大別され、その情報セキュリティ対策は、人的な管理とシステムによる管理に大別されます。情報資産全体の管理規定をまとめましたので、ご覧ください。

情報セキュリティ対策とは、情報資産を管理するために必要な具体的な行為です。

ア　人的な管理

取り扱い、外部持ち出しは人的な管理となります。人的な管理として、ルールを策定して組織的にセキュリティを確保する「組織体制作り」と、情報資産を取り扱う個人に求められる「人的セキュリティ対策」が必要になります。

イ　システムによる管理

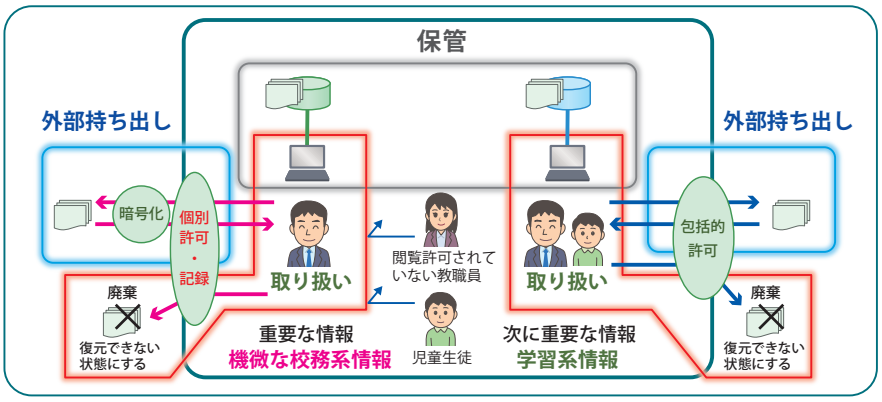
保管については、外部脅威・内部脅威から情報資産を守ることが求められます。情報資産を保管するうえで、窃盗、自然災害から守る「物理的セキュリティ対策」、インターネット上の悪意のある外部脅威の侵入を監視し、防御する等の「技術的セキュリティ対策」、「運用」が必要になります。

各セキュリティ対策とは、情報資産を管理するための具体的な方策であり、これらの合わせ技でセキュリティが確保される構図です。

情報資産の管理種別

情報資産の管理

- 取り扱い　→　職員室・事務室において他者に見せない
- 外部持ち出し　→　学校外への持ち出す際の情報資産と利用ツールの制限
- 保管　→　どの情報をどの場所に保管しているかの現況把握
安全管理措置（パスワード設定、暗号化）
- 廃棄　→　復元できない状態にして廃棄



情報資産の管理規定

分　類	重要性分類から導かれる特性	管　理			保存先
		取り扱い	外部持ち出し	保管（対策方法）	
機微な校務系情報 （重要性分類Ⅱ以上）	・許可された教職員のみが扱える情報 ・児童生徒が見られない情報 ・学校の外に出せない情報	・本人以外に見られない、盗まれない、他人に伝えないよう配慮	・学校の外に持ち出す場合には、セキュリティ管理者の個別許可が必要 ・誰が何を持ち出したか記録を残す ※持ち出せない情報もあり	・インターネット接続システムから隔離する ・インターネット接続システムに保管する必要がある場合は、パスワード、暗号化等の保護措置を講ずる ・学校に保管せず、教育委員会が一元集約管理	自治体のルールに則る
学習系情報 （重要性分類Ⅲ）	・児童生徒と教員が学習の中で扱う情報 ・学校の外に出せない情報	・部外者に見られない、盗まれないよう配慮	・学校の外に持ち出す場合には、セキュリティ管理者が包括的に許可	・インターネット接続ポイントを教育委員会が集約し、外部脅威からの防御・監視を強化 ・インターネット接続できる学校設置サーバに保管可 ※暗号化等の保護措置は求めない	
守らなくてもほとんど影響ない情報 （重要性分類Ⅳ）	特に規定しない				

（4）教職員が遵守すべき人的セキュリティ対策

ここでは、情報を取り扱う立場の教職員に守っていただきたい事項を記します。

①情報資産の取り扱いにおける「他者からの秘密保持義務」

機微な校務系情報は、許可された教職員のみ取り扱えるものです。そのため、他者に対して秘密を保持することが必要です。

（ア）目に入る状態にしない	・重要書類を机上に放置しない ・パソコン画面に重要な情報が表示されたまま放置しない ・ID・パスワードが書かれたメモを机上など目につくところに貼付しない
（イ）盗める状態にしない	・重要なデータや ID・パスワード情報にパスワードをかけないままパソコンやサーバに保存しない ・端末収納ラックは施錠をする。扉を開けっ放しにしない ・重要書類をそのままゴミ箱に廃棄しない ・USB メモリ、CD-ROM など記録媒体を破壊しないまま廃棄しない
（ウ）話題に出さない	・秘密にすべき情報は話題にしてはいけない（特に移動中や宴席では気を付けてください）

②情報資産の外部持ち出し

学校の外に情報資産を持ち出す行為は最もセキュリティ事故が多発する危険な行為ですので、充分注意ください。

（ア）管理者から許可を得る	・成績情報など機微な校務系情報の外部持ち出しは学校管理者の許可が必要です
（イ）USB メモリの扱いに注意する（私物使用の禁止等）	・持ち帰るときは立ち寄り禁止 ・セキュリティ機能を使う（パスワード設定・暗号化）
（ウ）情報にパスワードをかける	・外部メールの本文に個人情報を記載しない ・外部メールで個人情報を送信するとき、添付ファイルにパスワードをかける
（エ）個人向け WEB サービス[15]を勝手に利用しない	・無断での利用は禁止（学校のルールに従う） ・成績情報など機微な個人情報は送信・保存禁止 ・電子データにはパスワードをかける

15：個人向け WEB サービスは、文部科学省「教育情報セキュリティポリシーに関するガイドライン」のなかで、「1.9.4 約款による外部サービス」と定義され、取り扱いについて規定されています。WEB で同意すれば使える外部メール、ファイルストレージサービス等のことを指します。

③マルウェアを持ち込まない

マルウェアとはコンピュータの正常な利用を妨げたり、利用者に害を及ぼしたりする悪意のあるソフトウェアのことです。マルウェア感染を誘発する危険な行為について充分注意ください。

※詳しくは、参考 4（6）を参照ください。

④児童生徒への情報セキュリティ指導

児童生徒も授業・学習系システムを利用する立場ですので、情報セキュリティの基本について知ってもらう必要があります。

（ア）情報資産の外部持ち出し	・学校外にモバイル端末・USB メモリ等を持ち出すときは、担任の許可が必要
（イ）コンピュータウイルス感染予防	・未承認の個人 PC・モバイル端末等を学校の情報システムに接続してはいけない ・未承認の個人 USB メモリ等を PC・モバイル端末等に接続してはいけない ・無許可で端末等のソフトウェアに関するセキュリティ機能の設定変更をしてはいけない ・端末の動作異常時はすぐに担任に報告する
（ウ）ID・パスワード管理	・自分のＩＤは、他人に利用させてはいけない （共用利用の場合は、共用ＩＤ利用者以外に利用させてはいけない） ・パスワードを他人に知られないようにする

⑤マルウェア感染時の対応

例えば以下のような症状があれば、マルウェア感染が疑われますので、教育情報セキュリティ管理者に緊急報告してください。

また、感染が疑われる端末はネットワークからすみやかに分離する必要があります。有線ケーブル利用の場合は、ＬＡＮコネクタを外してください。無線ＬＡＮ利用の場合は、無線をＯＦＦ設定してください。なお、端末は専門家による解析が必要ですので、電源を落とさないままにしてください。

（ア）パソコンの挙動が不自然	・再起動を繰り返す ・インターネット接続、切断を繰り返す ・パソコンの動きが遅い、フリーズ、強制終了する ・セキュリティソフトが動かない、アップデートできない ・大量の迷惑メール受信
（イ）だれかに勝手に操作されている	・立ち上げ時の画面表示が変わった ・ファイルが消えた、場所が変わった ・関係ないサイトや広告、メッセージが勝手に表示 ・知らないソフトが入っている、増えている

参考3 クラウドサービス利用における セキュリティ確保の考え方

（1）クラウドサービスのセキュリティをどう確保するか

クラウドサービスについてはいくつかの特長がありますが、主にセキュリティ面の不安が払しょくされず、クラウドサービス利用を躊躇する自治体もあると考えられます[16]。

では、どうしたらセキュリティの不安を払しょくできるのでしょうか。そのためには、クラウド事業者及びサービスを選定する際に、２つの側面からリスクの可視化・洗い出しをする必要があります。

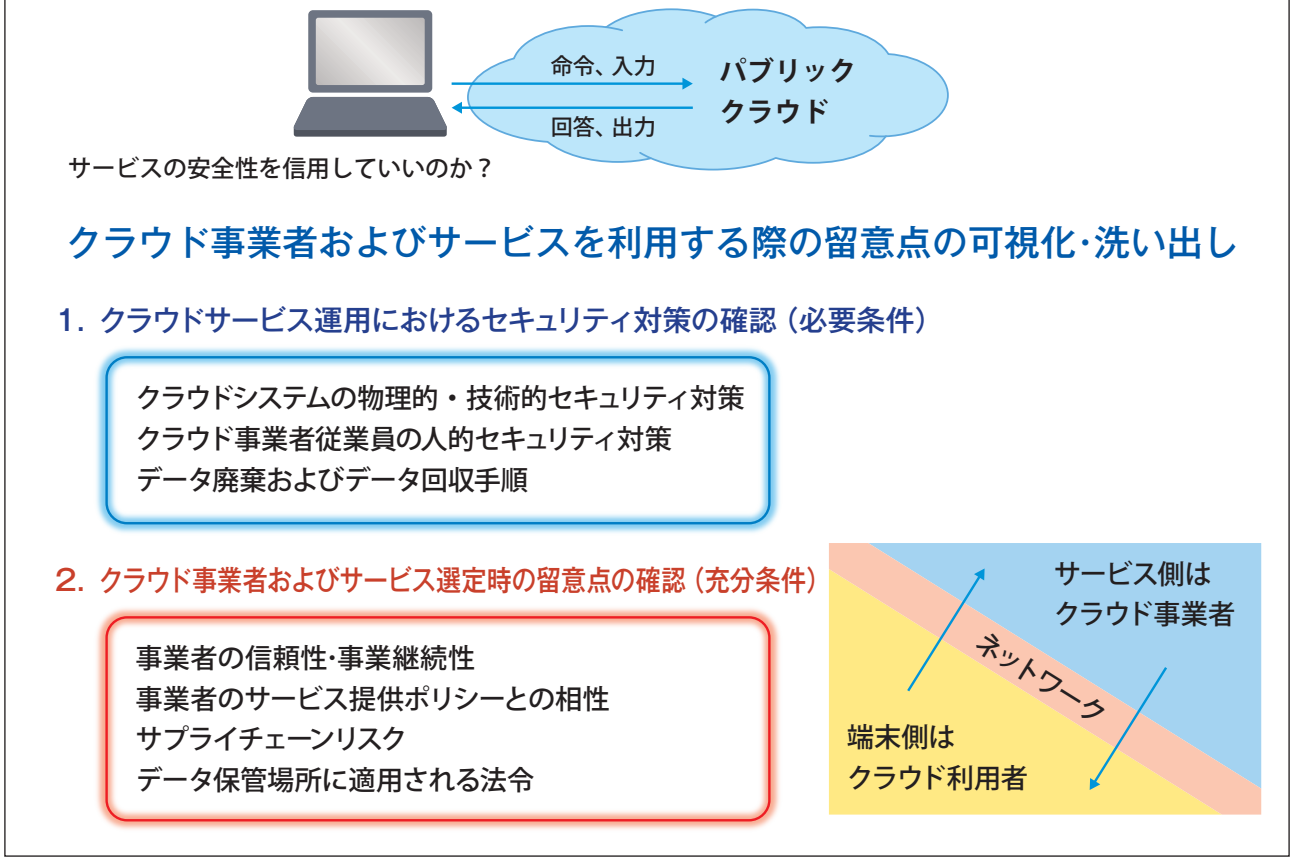
１つ目は、クラウドサービスの運用でどのようなセキュリティ対策が講じられているかを確認することです。外部委託先においても、しっかりとしたセキュリティ対策を講じる必要があります。

２つ目は、クラウド事業者やサービスへの信頼性や提供ポリシーが、クラウド利用者にとって受け入れられるかどうかのリスク評価を行うことです。例えば、セキュリティ対策をしっかり講じているクラウド事業者であっても、突然サービスを停止する危険性がある場合や、セキュリティ事故が発覚した際にまったく協力してくれない場合には、そのようなサービスを選択することは難しいと考えられます。

「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）のクラウドサービス利用におけるセキュリティ規定（参考資料 1.9 章）は、クラウドサービス運用におけるセキュリティ対策を確認する規定と、事業者ポリシーや内在リスクを確認する規定から成っています。

16：参考１（５）を参照ください。

セキュリティの不安を解消するために何をすべきか？



（2）クラウドにおける各種評価・認証制度

クラウドサービスのリスクや留意点に対して、クラウド事業者がどう対策を講じているかについては、事業者内部の取り組みであり、一般的に利用者に公表されていません。

しかし、クラウド利用を検討する立場からは、クラウド事業者がどのようにリスクや留意点に対して対策を講じているかを含めて、クラウド事業者の信頼性や内在リスクを確認・検証しないままクラウドサービスを利用することは危険です。そのための「クラウド事業者及びサービス選定リスクを把握するうえで何を確認すべきか」について、「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）1.9 にて規定しています。

クラウド事業者自らの安全性・信頼性に関わる対策状況を第三者が評価し、安全性・信頼性が確認された場合には認定する制度が存在します。具体的には、以下のような認証制度があります。

＜認証制度の例＞

ア　ISO/IEC 27017 による認証取得
　　https://isms.jp/ismscls/lst/ind/index.html
イ　米国 FedRAMP
　　https://marketplace.fedramp.gov/#/products?status=Compliant
ウ　AICPA SOC2（日本公認会計士協会 IT7 号）
エ　AICPA SOC3 SysTrust/WebTrsuts ）（日本公認会計士協会 IT2 号）
オ　JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
　　http://jcispa.jasa.jp/cs_mark_co/cs_gold_mark_co/
カ　ISO /IEC 27018 による認証取得 クラウドサービスにおける個人情報の取扱い

※出典：「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）

いずれかの認証制度の認証を取得することで、情報セキュリティのマネジメントが適切に行われている目安になると考えられます。ただし、認証取得事業者であれば問題なしとして、それだけで採用を判断することは早尚です。クラウド利用者の環境（システム、遵守法令等）は様々ですので、クラウドサービスとの相性があります。クラウド利用者は、自らの環境に照らし合わせて「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）の「クラウドサービスの利用」規定に基づき確認を行い、サービスの採用可否を個別判断することが望ましいといえます。

なお、認証取得したクラウド事業者は大手の IaaS(PaaS) 事業者が多く、SaaS 事業者で取得している例は限られると考えられます。その場合でも SaaS 事業者が、認証取得した IaaS（PaaS）事業者を利用している場合は、IaaS（PaaS）に関する情報セキュリティのマネジメントは適切に行われていると考えられます。

（3）「教育情報セキュリティポリシーに関するガイドライン」におけるクラウドサービス利用規定

「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）では、クラウドならではの特性に起因する留意点や、SaaS・パブリッククラウドのような定型サービスを外部委託先として利用する場合の制約条件等を考慮して、クラウドサービス利用に関して、1.9.2 項と 1.9.3 項に個別規定が記載されています。この規定に共通する考え方を解説します[17]。

①クラウドサービスに求められる情報セキュリティ対策（1.9.2 項）

クラウドサービスを提供する情報システムの情報セキュリティ対策は、システム所有者であるクラウド事業者の権限と責任範囲となりますので、クラウド利用者はクラウドサービス側のセキュリティ対策の多くをクラウド事業者に委ねる構造になります。そのため、クラウド事業者が講じる情報セキュリティ対策を、クラウド利用者が検証する形で安全性を確認する形になります。

「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）では、クラウドを利用す

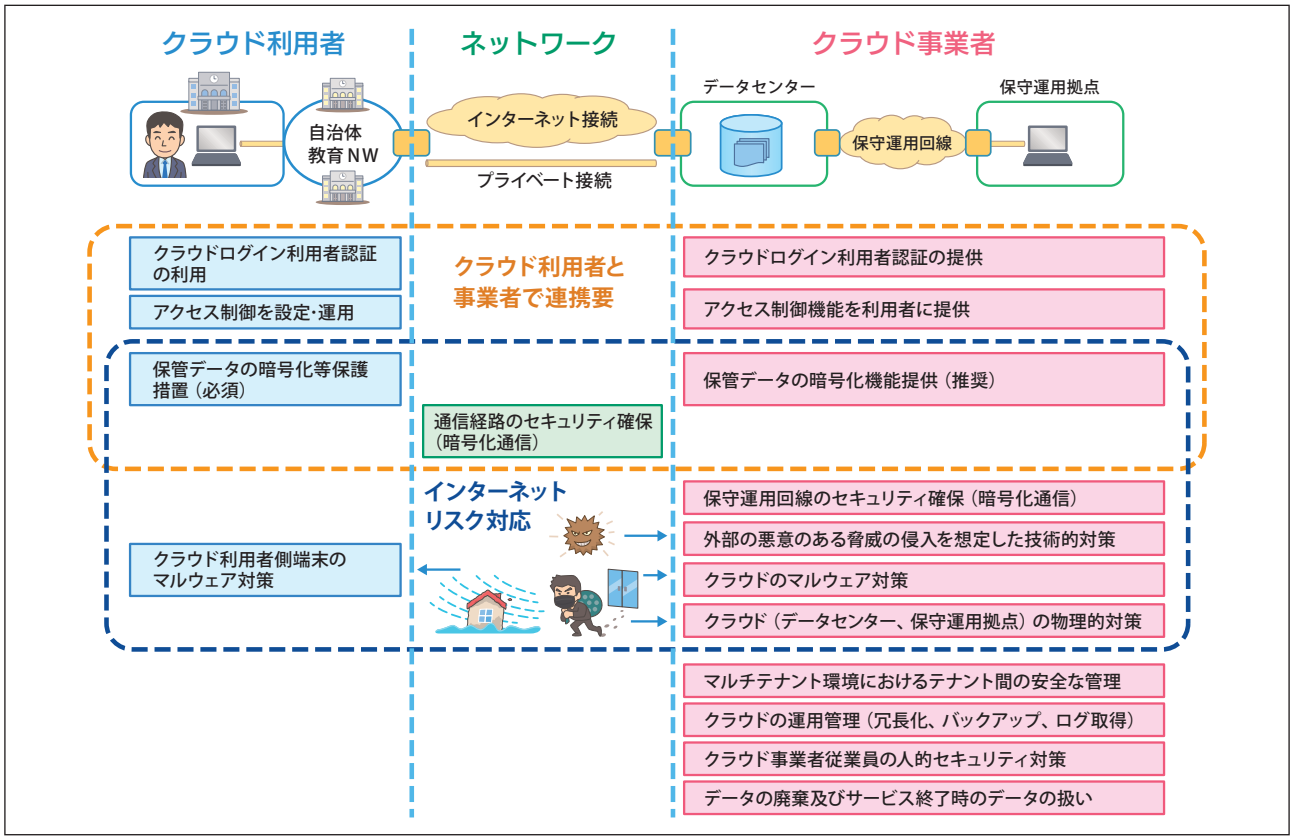
17：本編第３章（５）①、参考１（５）も参照ください。また、個別規定の詳細については、「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）1.9 を参照ください。

るシステム全体の視点から情報セキュリティを確保するために必要な項目を洗い出しており、クラウドを利用する側に求められる規定も含まれています。例えば、マルウェア対策は、クラウド利用者側、事業者側に共通して必要なことです。

この場合のように、クラウドサービスに求められる情報セキュリティ対策の一部にはクラウド利用者側が講ずべき対策も含まれることに留意願います。

なお、ガイドラインの規定は、校務系システムと学習系システムの両方を想定しているため、インターネット接続形態で重要な情報資産を取り扱う最もセキュリティリスクの高いケースまで想定しています。

クラウドサービス運用における情報セキュリティ対策



＜コラム＞　クラウドサービスでのデータ廃棄に関する安全性確保

教職員が扱う校務系・学習系情報は保存期限が設定されていると考えられます。保存期限を過ぎたデータを残置することは、情報セキュリティの観点からはリスクですので、保存期限を過ぎた情報は速やかな廃棄が必要です。クラウドサービスが仮想環境で情報処理をしている以上、データを物理的に保管しているサーバの所在地を特定することが難しい場合があります。そのため、２つの課題が生じます。その対応策も含めて、下記に記します。

●ハードディスク等の物理交換によりデータが流出したとしても現場を押さえられない

クラウドサービスを提供する物理環境の保守・運用はクラウド事業者に任せていますので、老朽化等でデータが格納されたまま物理ストレージ[18]が撤去されることがあり得ます。本リスクに対しては、物理ストレージから保管データが漏えいしないように物理ストレージ自体に暗号化することが必須となります。ここでの暗号化は、保管データ自体を暗号化するわけではなく、物理ストレージからデータを取り出せないようにする手段のことです。

●データ消去をクラウド利用者が直接確認する手段がない

仮想環境でデータを消去しても、物理サーバのどこかに残っているリスクはないかと不安になる場合があると考えられます。校務系情報のように重要な情報はバックアップが求められますので、バックアップデータも当然消去対象になります。これらのデータが完全に消去されたかについては、クラウド利用者は物理サーバ上で直接確認する手段がないのが現状です。そこで、クラウド事業者が確実に該当データを消去した証として、「データ廃棄証明」を提出させることで、確実に該当データが消去されたと判断する方法があります。

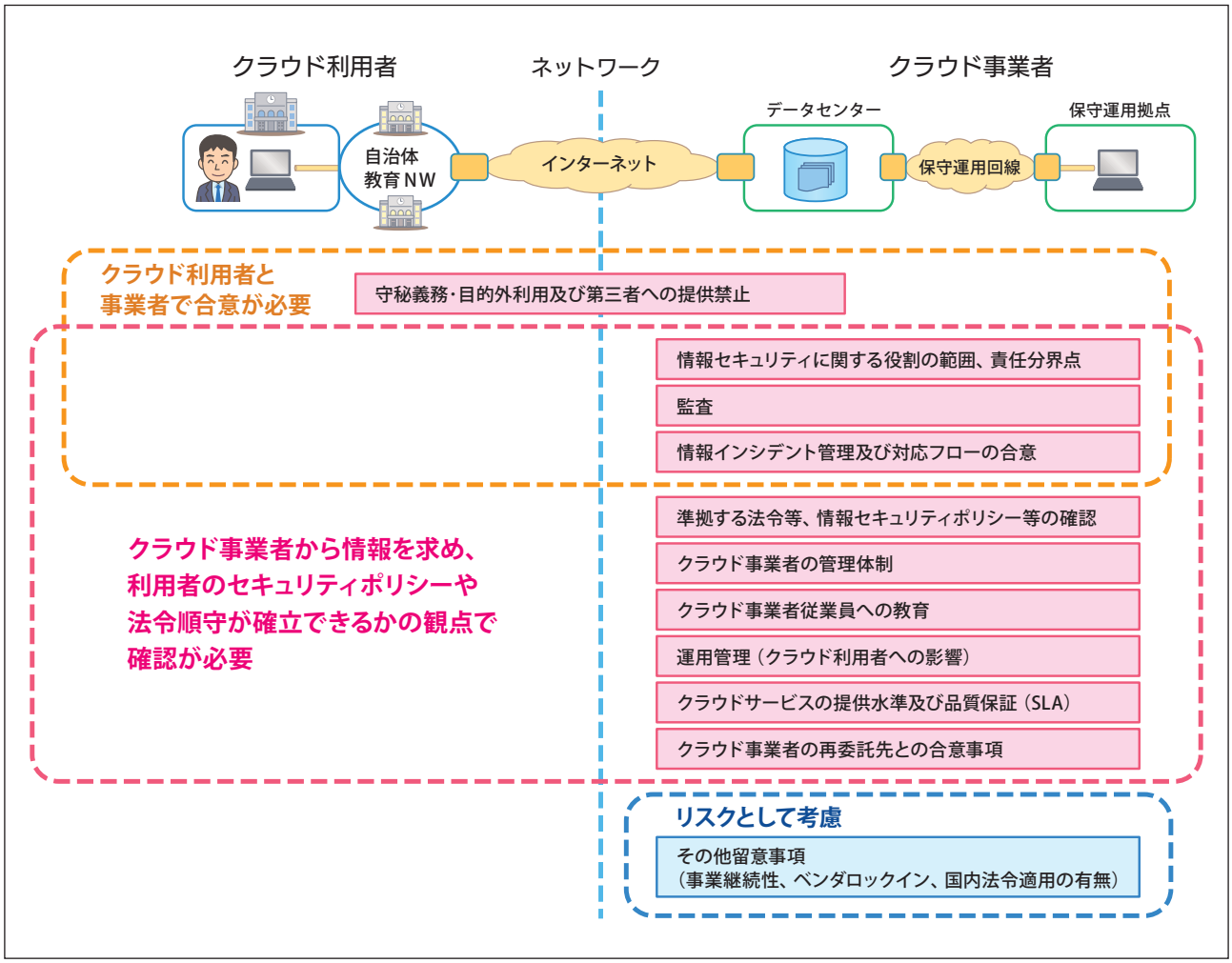
18：ストレージとは、情報を保管する外部記録媒体

②クラウド事業者およびサービス選定リスクの確認（1.9.3 項）

クラウドサービス利用における安全性担保のためには、クラウド事業者が実施する情報セキュリティ対策に加えて、クラウドサービス提供ポリシーがクラウド利用者のセキュリティポリシーや内部統制に求められる事項に適合するか、クラウド事業者として適切にサービス提供できる管理体制を有しているか等を確認する必要があります。

「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）では、セキュリティ確保の観点を点検して、10 項目を抽出し規定しています。

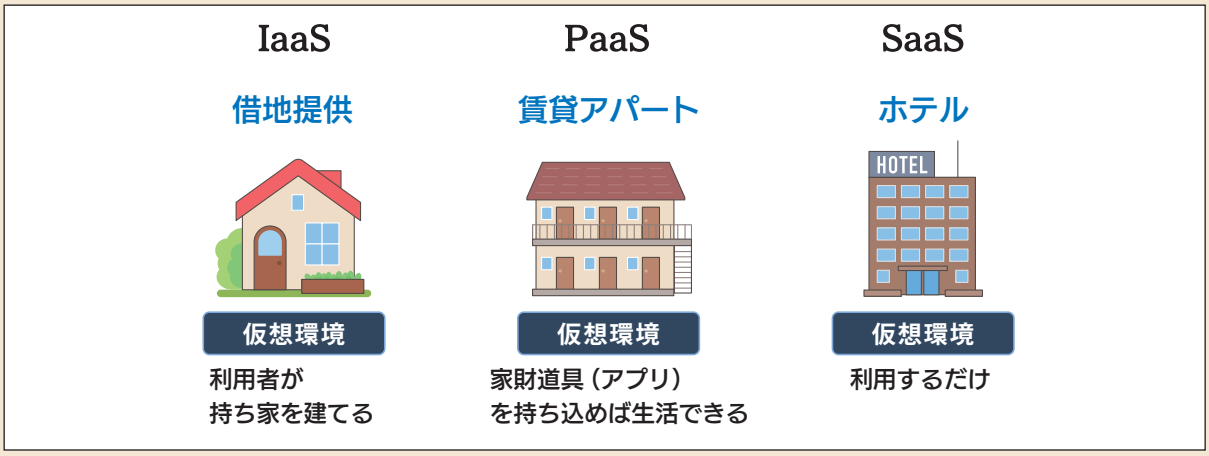
パブリッククラウド事業者のサービス提供に係るポリシー等に関する事



＜コラム＞　SaaS・パブリッククラウドは定型サービス型

クラウドサービス利用モデルを住居に例えた場合を示します。IaaS は仮想環境上に注文住宅を建てるようなもので、IaaS という借地の上に自由な間取りの注文住宅を建設できます。PaaS の場合も部屋を借りるだけで、家財道具は利用者が持ち込みます。SaaS になると、ホテルのように家財道具もベッドもすべて揃っており、利用するだけでいい便利な点がメリットです。しかし逆の視点で見ると、SaaS は備え付けの家具や什器を利用していただく前提でサービスを提供しており、原則利用者による家財道具の持ち込みを許容していません。SaaS 利用では、利用者は SaaS 事業者が提供する定型サービスを利用することが前提であり、ベッドを変えてほしいなど個別要望には対応しないのが原則です。もし、個別要望を叶えたい場合には、自分で家財道具を持ち込む IaaS や PaaS を利用することが現実的だと考えられます。

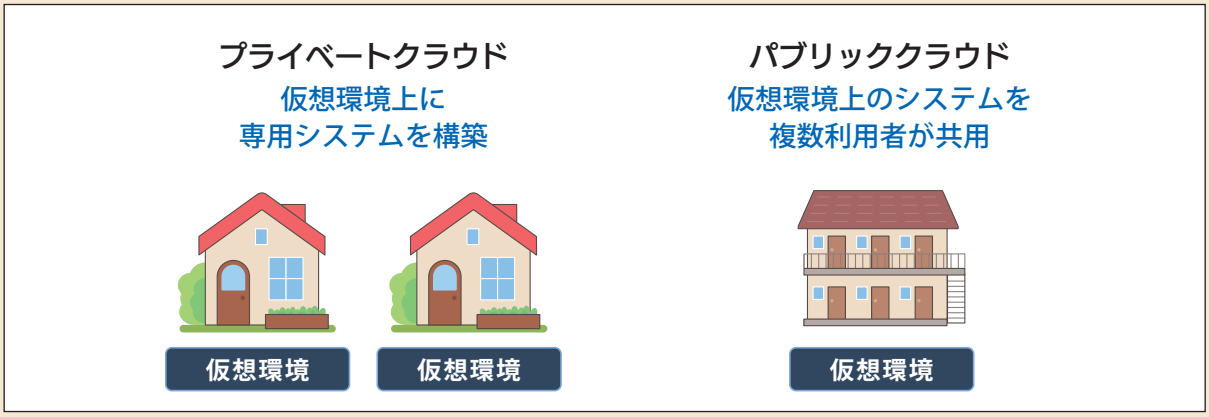
クラウドサービス利用モデルについて（※住居にたとえた場合）



次に、クラウド実装モデルについて考えてみます。プライベートクラウドは、仮想環境を占有しますので、その環境上に自由にシステムを構築できます。借地に好きな間取りの注文住宅を建てる例に例えられます。一方で、パブリッククラウドの場合は仮想環境に複数の利用者を収容しますので、アパートのように専用の住居ではありますが、他利用者と隣り合わせの生活となり、間取りの変更にも一定の制約があります。

以上の例に例えられるように、パブリッククラウドの場合は、定型的なサービスの利用を前提として提供されます。

クラウド実装モデルの比喩例



（4）約款による外部サービス利用の留意点

①約款による外部サービスとは

有料、無料に関わらず、個人を対象にインターネット上に掲示された約款へ同意し、簡易なアカウントの登録により当該機能を即時利用可能なサービスは「約款による外部サービス」です。

約款とは、定式化された契約条項の総体で、サービス規約とも称されます。電気通信サービスや郵便、運送サービス等多数の定型的な契約を結ぶ事業者に利用されており、世の中に広く普及しています。なおここで取り上げる「約款による外部サービス」とは、下記のサービスに限定しています。

（ア）インターネット上で
（イ）不特定多数の個人を対象に
（ウ）約款を提示して同意した個人に対して
（エ）簡易なアカウントの登録（メールアドレス、氏名等）をすれば
（オ）機能（電子メール、ファイルストレージ、グループウェア等）が使える

これらのＷＥＢサービスは、便利な反面、情報セキュリティ面での裏付けを確認できないことが多く、利用にあたりセキュリティリスクが残るため、利用できる範囲を制限し、対策を講じたうえで利用する必要が

あります。なお、学校や教育委員会が個別に契約締結するサービスは約款型であっても「約款による外部サービス」には該当しません。

②約款による外部サービスを利用するリスク

「約款による外部サービス」を利用する場合は、約款で提示した条件の範囲内でのサービス利用となり、特別な条件を加える等、個別契約を締結することが困難な場合が一般的です。

このようなサービスを利用する場合の主なリスクとして下記が想定されます。利用者は、提示された約款の範囲で利用の可否判断が求められることになりますが、リスクを十分踏まえた上で利用を判断し、セキュリティ対策を適切に講ずる必要があります。

（ア）利用者データの取り扱いについてのセキュリティ遵守事項が保証されない可能性	知りえた情報の秘密保持義務、目的外利用の禁止、無許可での第三者への提供の禁止、安全な廃棄手順等が約款に示されていない場合があります。
（イ）知的財産権の扱い	利用者データの知的財産権がサービス提供者側に帰属することを前提にサービス提供する場合があります。
（ウ）セキュリティ事故調査協力が確約されていない可能性	セキュリティ事故調査等においては、利用者の当該サービスへのアクセス記録が必要になるが、利用者の求めに応じてアクセス記録を提供する等、利用者の事故対応に協力することが約款に示されていない場合があります。
（エ）該当サービスに対する情報セキュリティ対策が不明な場合がある	当該サービスについて、人的・物理的・技術的セキュリティ対策等が約款に示されていないため、利用者データ保管における安全管理措置が不明な場合があります。
（オ）一方的な利用規約の変更・サービス停止の可能性	約款や利用規約が予告なく一方的に変更されたり、サービス停止したりする可能性があります。

③約款による外部サービスを利用する際の留意点

「約款による外部サービス」のリスクを考えて、安全性が確認できる範囲でしか利用しないことが基本的な考え方です。

（ア）機密性の高い情報を扱わない

学校のなかでしか扱えない機密性の高い情報を「約款による外部サービス」を利用して外部に持ち出したり、学校外部のクラウドサービスに蓄積したりすることは、外部漏えいや情報消失リスクがありますので、重要性の低い情報資産（万が一、セキュリティ侵害が発生しても軽微なレベルである情報）に留めることが必要です。

（イ）教職員個人が勝手に利用しない

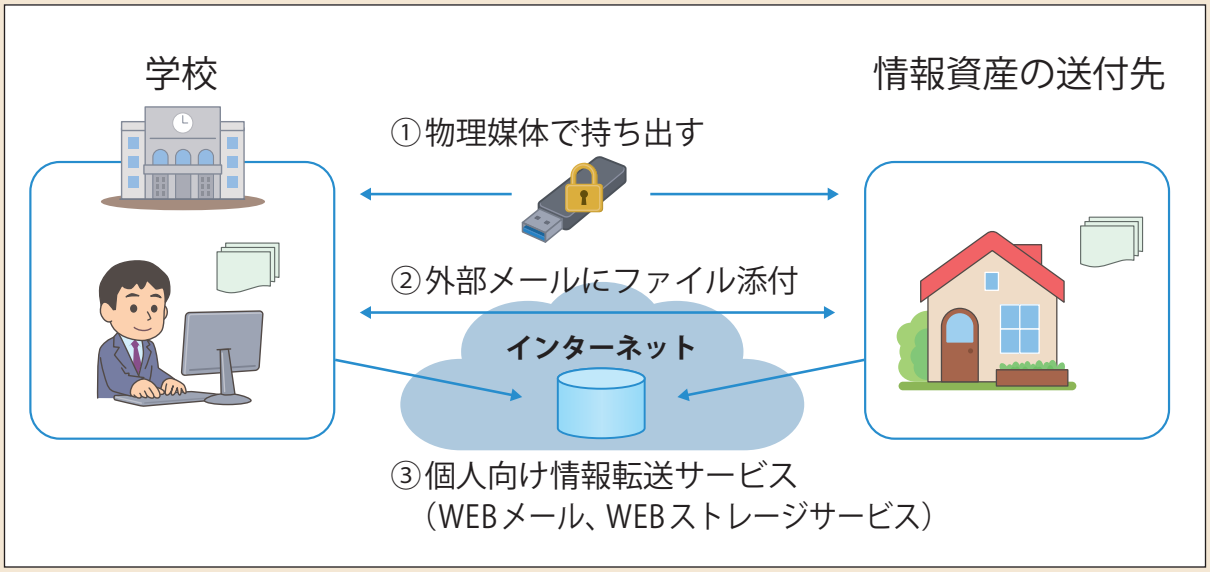
教職員等が学校において、個人的に契約した約款によるメールサービスやストレージサービスを無断で利用することは、学校の情報セキュリティ管理をすり抜ける行為に相当します。情報資産の重要性によっては外部漏えい事案に相当するため、教育情報セキュリティ管理者（校長等）はこのような事態を避ける必要があります。

なお、一概に利用を禁止するものではなく、どうしても使用する場合は約款内容をふまえて残存するリスクに照らして、利用規定を整備し、教育委員会や学校が契約したサービスのみを教職員等に提供することにより、教職員等の私的利用を禁止し、情報セキュリティ管理者が教職員等の利用を把握できる状態にすることが重要です。

＜コラム＞　「約款による外部サービス」を利用した情報の外部持ち出しの危険性

学校の情報を外部に持ち出すツールとしては３種の方法があります。
① USB メモリのような物理媒体による持ち出しで、最も普及している方法と言えます。
②外部メールにファイル添付して送付する方法です。
③個人が契約した WEB メールや WEB ストレージサービスを利用する方法です。
このうち、③が「約款による外部サービス」を利用した情報の外部持ち出しに該当します。
重要な情報は、本来は学校の外に教職員が無断で持ち出してはいけない情報になります。そのため、教育情報セキュリティ管理者（校長等）の個別許可を得て持ち出すルールが必要です。
①においては USB メモリ及び持ち出す情報（持ち帰った場合も含めて）を記録管理します。②は送受信記録が残ります。③については、学校では管理できない方法を用いて、教職員個人が無断で情報を持ち出すことになりますので、意図的な情報漏えいに相当します。
そのため、教職員が個人で契約した「約款による外部サービス」を利用せず、学校や教育委員会が契約したサービスのみを利用することで、情報の外部持ち出しを学校が管理できる形にすることが必要です。

情報の外部持ち出しツール



参考4 クラウド利用型システムにおけるセキュリティ対策の考え方

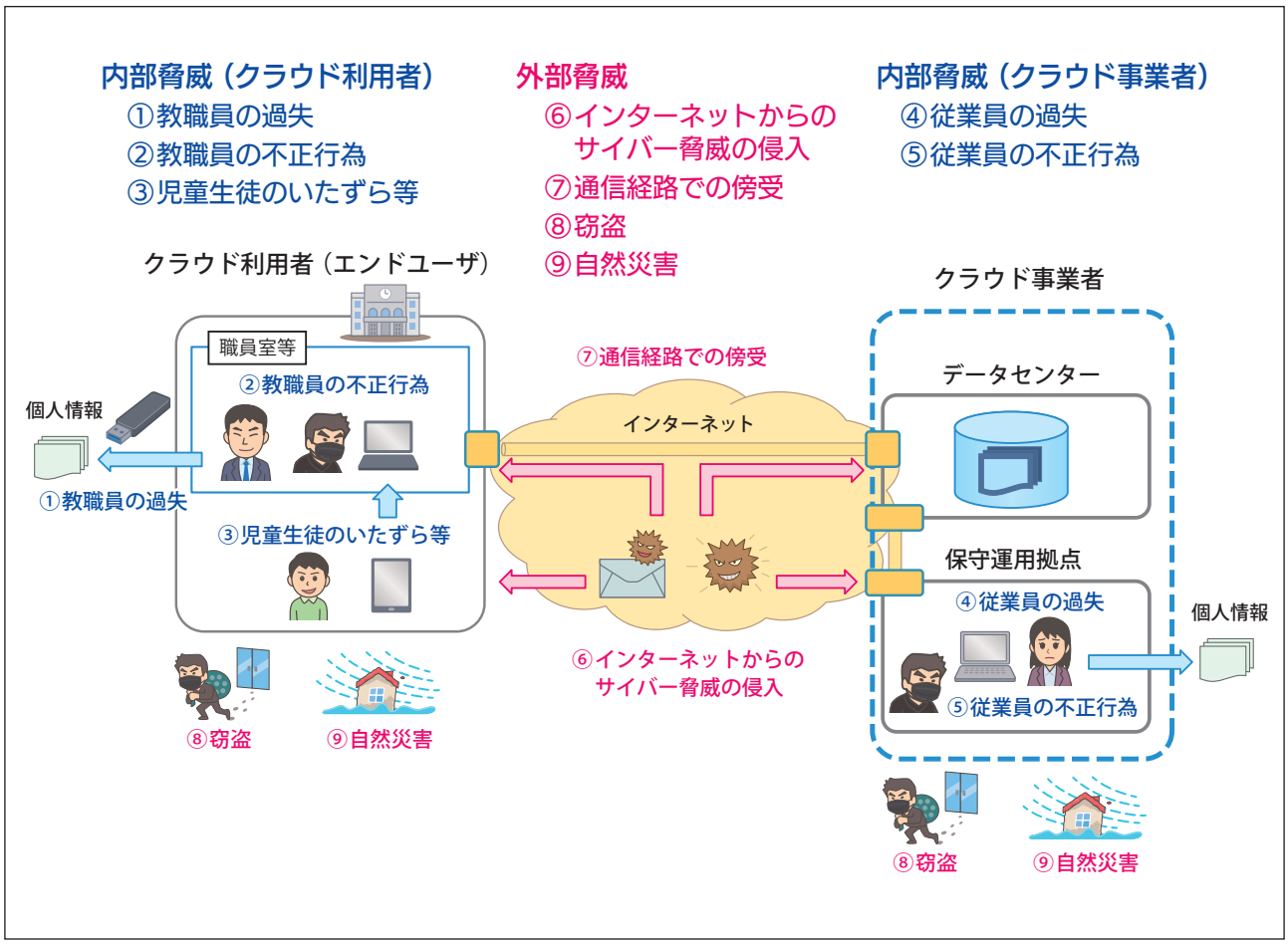
（1）クラウドサービス利用を想定したセキュリティ脅威の洗い出し

ここでは、クラウドサービスを利用する場合に、どのようなセキュリティ脅威が存在するかを整理します。

システムや人に求められるセキュリティ対策の検討は、どのような脅威を想定するところから始まります。セキュリティ脅威は、内部脅威と外部脅威に大別されます。

クラウド利用者の内部脅威とは、主に教職員による過失や不正行為を意味し、事故件数が多数を占めるため、最も注意が必要な脅威です。クラウド事業者の内部脅威とは、クラウド側に預けた情報に対して、クラウド事業者従業員が運用を誤って削除したり、不正アクセスまたは持ち出したりする場合が相当します。また、外部脅威は、窃盗や自然災害等の物理的な脅威と、インターネットからのサイバー脅威に大別されます。

教育クラウドモデルにおけるセキュリティ脅威



クラウド利用者の内部脅威	①教職員の過失	外部への情報持ち出しにおいて USB メモリを紛失したり、メールを誤送信したり、誤ってデータを削除したり、重要な情報を机上に放置したりするようなケースです。
	②教職員の不正行為	教職員は情報にアクセスする権限を持つため、アクセス可能な情報の不正持ち出しや改ざんを意図的に実行されるケースです。
	③児童生徒のいたずら等	児童生徒が教職員しかアクセスできない校務系情報にアクセスする場合などが相当します。ケースとしては、職員室で教員不在時に机上に放置された情報を盗み見する場合や、教室から学習者用端末で校務系システムに侵入して校務系情報を不正閲覧する等が想定されます。
クラウド事業者の内部脅威	④従業員の過失	クラウドサービスは、オペレーションミスでクラウド利用者の仮想環境が消失することなどもあるため、従業員には高度なスキルが求められます。
	⑤従業員の不正利用	SaaS 事業者は原則クラウド利用者データにアクセスできますので、不正アクセスが可能な立場です。これはクラウドに限らず、オンプレミスでも外部委託事業者にサーバの運用保守を任せている場合も同様です。
外部脅威	⑥インターネットからのサイバー脅威の侵入	学校で保管する情報を狙って、悪意のある攻撃者がサイバー攻撃を仕掛けるケースです。ここで注意いただきたいのは、サイバー攻撃を受ける危険性は、クラウド利用者とクラウド事業者の双方です。そのため、クラウド利用者とクラウド事業者双方で、サイバー攻撃に対する対策が必要になります。
	⑦通信経路での傍受	インターネットを通信回線として利用する場合には通信内容を傍受される場合があります。校内で無線 LAN を利用する場合も同様です。
	⑧窃盗	学校で、端末等の窃盗事件が毎年発生しています。外部から無理やり学校に侵入して窃盗を起こすケースもありますが、学校には多くの外部の者が出入りしますので、その際に窃盗が起きる場合もあります。
	⑨自然災害	大規模地震や風水害により、学校で保管する情報が破壊・散逸することがあります。2011 年の東日本大震災では、学校で金庫に保管していた指導要録等重要な情報が海に流失する痛ましい事故が発生しました。

＜コラム＞　クラウドサービス利用におけるセキュリティ脅威

セキュリティ脅威のうち、クラウドサービス利用の観点から見ると、クラウド事業者従業員の不正行為や過失行為も内部脅威のひとつといえます。

なお、インターネットを通信経路として利用する場合の留意点として下記 2 点が挙げられます。

①インターネットからのサイバー脅威の侵入を想定する必要がある（クラウド事業者とクラウド利用者の双方）

②通信経路において情報の傍受対策を講じる必要がある

リスクとしてはクラウド事業者側にもセキュリティ脅威が存在する前提で対策を講じる必要があります。

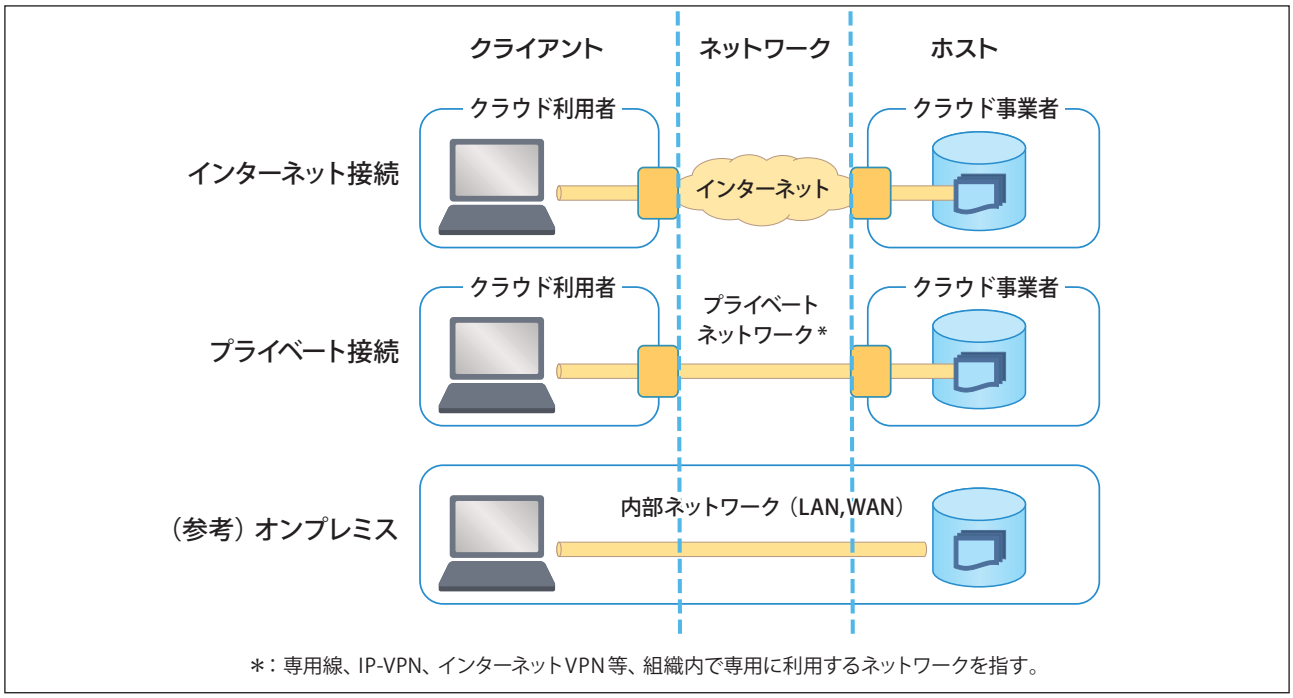
※具体的なセキュリティ対策については、参考 4（4）を参照ください。

※利用者が行う対策については、詳しくは、参考 2（4）を参照ください。

（2）システム構成から見た情報セキュリティの留意点

クラウドサービスモデルやネットワーク種別の組み合わせに対して、留意点を整理します。システムの基本構成を示します。

クラウド利用型システムの基本構成



＊：専用線、IP-VPN、インターネットVPN等、組織内で専用に利用するネットワークを指す。

①クライアント側：システム構成によらず自前構築となります。
②ネットワーク：プライベートネットワーク構成と、インターネット接続の２種に分かれ、プライベートネットワーク接続ではインターネット環境から分離する目的で利用します。
③ホスト側：クラウドモデル（SaaS/PaaS/IaaS、パブリッククラウド / プライベートクラウド）のバリエーションがあります。

＜コラム＞　情報システムの構成バリエーション

クラウドサービスは、仮想環境をサービス提供するものですが、古くから物理環境をサービス提供する形態が存在しています。コロケーションはデータセンターの場所レンタル、ホスティングは、データセンター内の物理環境のサービス提供です。コロケーション・ホスティングともにクライアント側とデータセンターの間をネットワークで接続して、情報システムを構成します。

情報システム構成についてそのバリエーションを比較してみました。　ホスト側を自前で構築するオンプレミスから、最大限自前構築領域を軽くする SaaS 利用までのバリエーションがあります。

情報システムをクライアント（端末、構内ネットワーク）、ネットワーク、ホスト（サーバ等）に分解して、オンプレミスから SaaS までを比較すると下記のことが読み取れます。

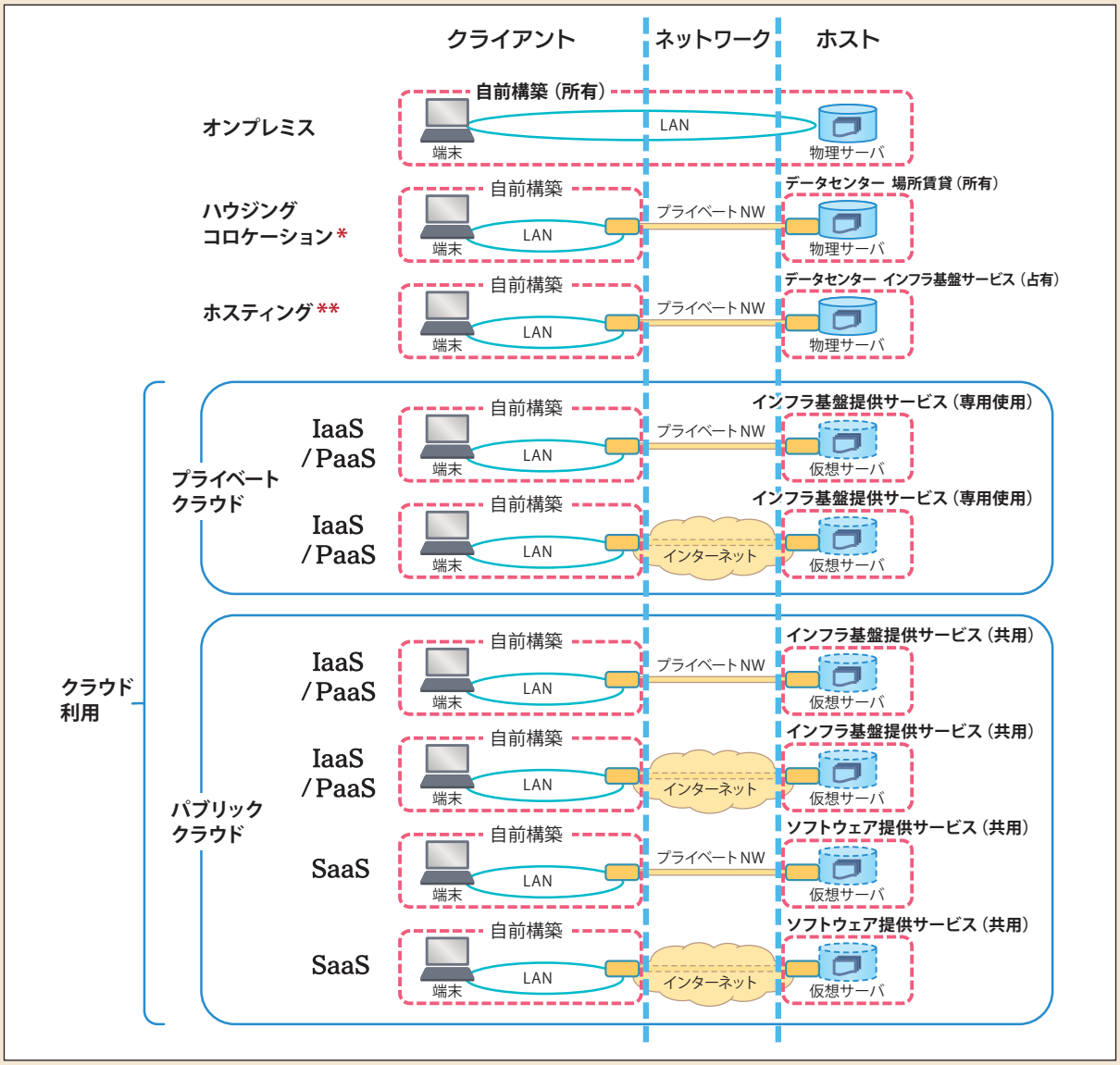
（ア）オンプレミスを除き、クライアントとホストは外部ネットワークを介して接続する構成
（イ）クラウドを利用するのはホスト側のみ（クラウドモデルとは、ホスト側を構成するバリエーション）
（ウ）外部ネットワークは、インターネット利用とプライベート利用に大別できる
（エ）クライアント側は、システム構成によらず自前構築となる

以上から、クラウド利用の観点はホスト側をどう構成するかであり、クラウドモデルの選択はホスト側の構成についての論点です。

学習系システムのように、多様なサイトにアクセスする前提の場合はインターネット利用が前提になりますが、校務系システム（狭義）のように特定のサーバだけにアクセスする場合は、インターネットを利用しない構成も可能です。

プライベートネットワークを利用するケースの多くは、情報セキュリティ強化の観点から、インターネットからのサイバー脅威を排除するために、インターネットから遮断されたイントラ型システムを構成する目的で選択されます。

システム構成のバリエーション（オンプレミスからクラウドまで）



＊　：ハウジングとは、通信回線などの設備が整った施設内で通信機器やコンピュータなどの設置場所を顧客に貸与するサービス。顧客は自ら利用する機器を持ち込んでインターネットに接続し、システムを運用する。コロケーションとは、所有者や運用者が異なる設備や機器を同じ施設にまとめて設置するサービス。そのような共同の設置場所を指すこともある。

＊＊：ホスティングとは、ホスティングサービスとは、専用の施設内に設置されたサーバコンピュータを、インターネットを通じて顧客に貸与するサービス。顧客は借り受けたコンピュータに必要なソフトウェアやデータを導入して運用する。

（3）クラウドサービスの構成から見た留意点の整理

ここは、3 種のクラウドモデルについての留意点[19]を解説します。

①ネットワークモデル

留意点として最も重要なのがネットワークモデル（構成）です。ネットワークモデルとは、プライベートネットワークと称する専用の通信回線と、インターネットを通信回線として利用する 2 種が存在します。

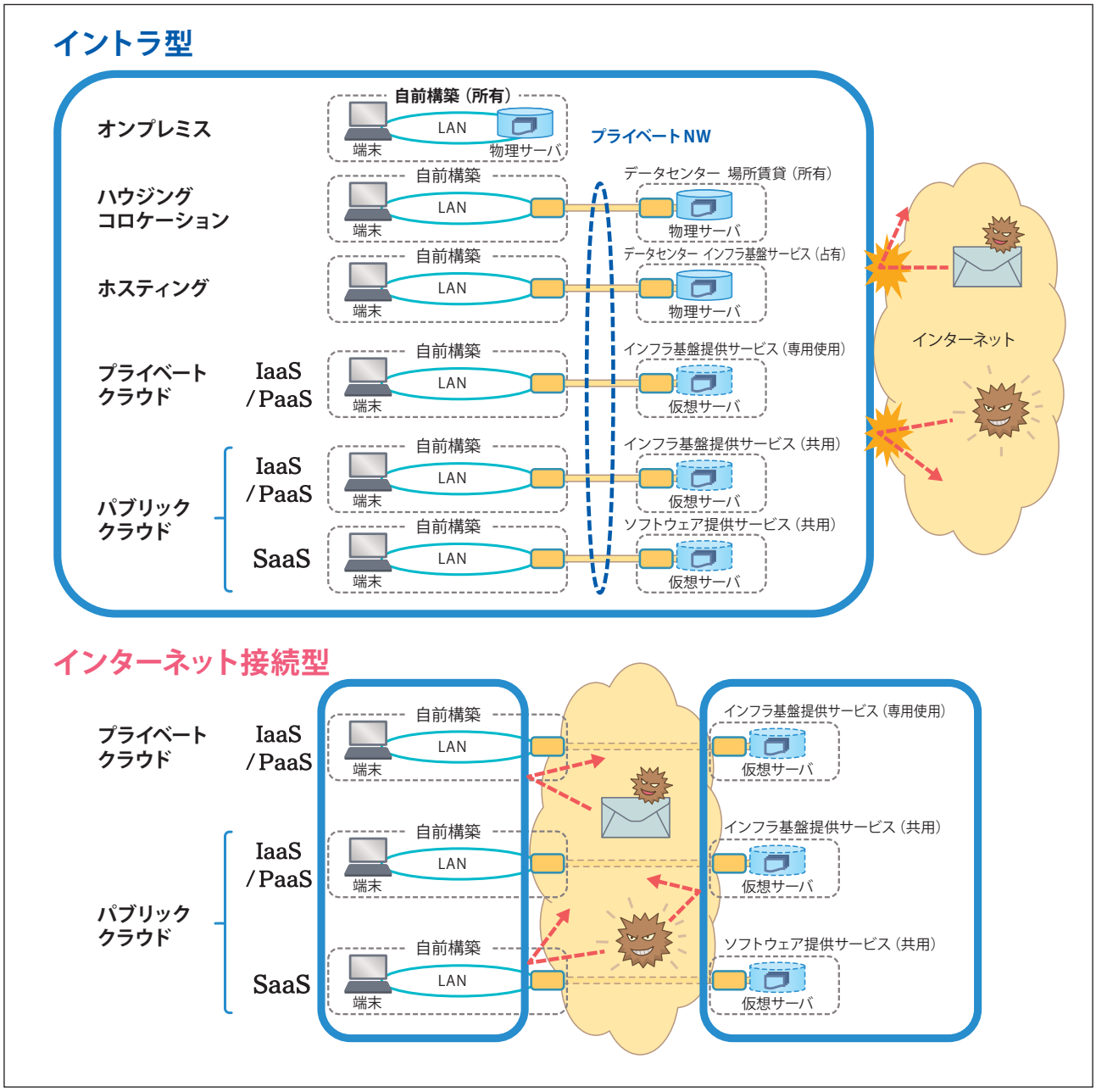
プライベートネットワーク接続ではインターネット環境から分離された形でシステムを構成できますので、インターネットからのサイバー脅威に対して、物理的に対策が講じられる構成です。一方で、インターネットを通信経路とする構成では、クライアント及びホスト両方にインターネットからのサイバー脅威に晒されますので、そのための防御対策が必要になります。

そのため、システム構成別セキュリティリスクを論じるうえで、インターネットからのサイバー脅威への対策が重要で、検討初期にどちらのネットワークモデルを選定するかについて検討する必要があります。

なおネットワークモデルについては、クラウドサービス利用ではなくても当てはまる一般論です。

19：参考 1 （5）にもクラウドサービスの留意点が記載されていますので参照ください。

ネットワークモデル



②クラウドの実装モデル

クラウド実装モデルによってセキュリティリスクにどのような差があるかについて考えてみましょう。

プライベートクラウドでは、クラウド事業者が仮想環境をクラウド利用者専用に提供しますので、提供された仮想環境を他者が侵害するリスクはありません。しかし、仮想環境の設定ミスや土台である物理環境に障害が発生した場合においては影響を受けます。パブリッククラウドでは、クラウド事業者の仮想環境を複数の利用者が共用しますので、マルチテナントに関するリスクが生じます。

③クラウドのサービスモデル

SaaS ／ PaaS ／ IaaS による提供形態でセキュリティリスクにどのような差があるかについて考えてみましょう。ここでは、SaaS と IaaS(PaaS) を分けて捉えるといいでしょう。

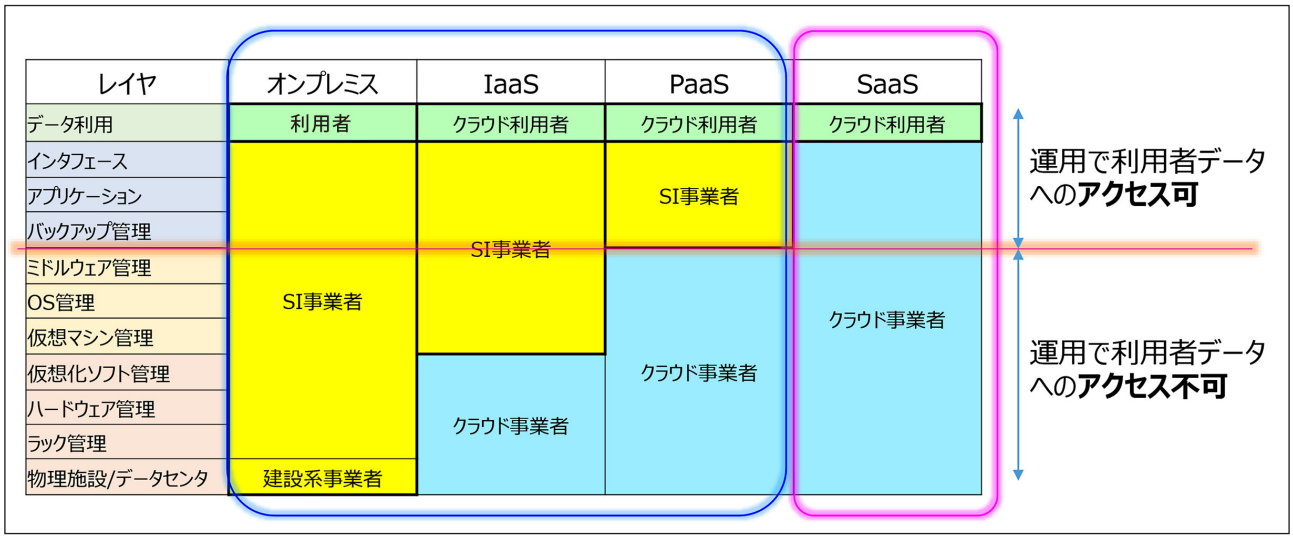
（ア） クラウド事業者とクラウド利用者の役割分担（責任範囲）

クラウドに預けたデータにアクセスできるかどうかの視点では、SaaS はアクセス可能ですが、IaaS（PaaS）では直接アクセスできる立場にはありません。

クラウドサービスの安全性を確保するなかで、クラウド事業者がクラウド利用者データにアクセス可能かどうか

は重要なポイントです。SaaS 利用ではクラウド事業者の運用における安全性確保に気に留める必要があります。IaaS・PaaS では SI 事業者による運用の安全性確保がポイントになります。SI 事業者の運用の安全性確保が重要である観点では、IaaS・PaaS 利用はオンプレミスとさほど違いがないと言えます。

クラウドサービスモデルによる特性の違い



（イ）サプライチェーンに関するリスク

多くの SaaS 事業者は、そのインフラ基盤を IaaS（PaaS）事業者から供給されておりますので、サプライチェーンに関して留意する必要があります。

④クラウド構成別セキュリティリスクのまとめ

以上のとおり、クラウド構成別セキュリティリスクは以下のように整理できます。

クラウド構成別セキュリティリスクのまとめ

クラウドモデル	バリエーション	たとえ	セキュリティリスク
ネットワークモデル	プライベート NW 接続／インターネット接続	専用道／一般道	インターネット上からのサイバー脅威侵入
クラウドの実装モデル	プライベートクラウド／パブリッククラウド	戸建住宅／集合住宅	マルチテナント
クラウドサービスモデル	SaaS ／ PaaS ／ IaaS	スケルトン（内装、仕切り未仕上げ）／部屋／家具付き部屋	・SaaS 事業者はデータに ・サプライチェーン アクセス可

クラウド構成別セキュリティリスクについて①から③まで概観してきましたが、セキュリティ対策を講じる場合には、もうひとつ大事なことがあります。それは、どのような情報資産を前提にクラウドサービスを利用するかです。

校務系システムのように、機微な個人情報を含む場合は、万が一セキュリティ侵害を受けると重大な影響がありますので、厳重なセキュリティ対策が求められます。学習系システムで学習系情報（機微な個人情報を含まないもの）を管理する場合には、そこまで厳しい要件を求められませんので、取り扱う情報資産の重要性を加味して、セキュリティ対策を検討することが必要です。

そのため、クラウドサービス活用においては前提条件を 4 項目揃えてリスクを確認する必要があると考えられます。

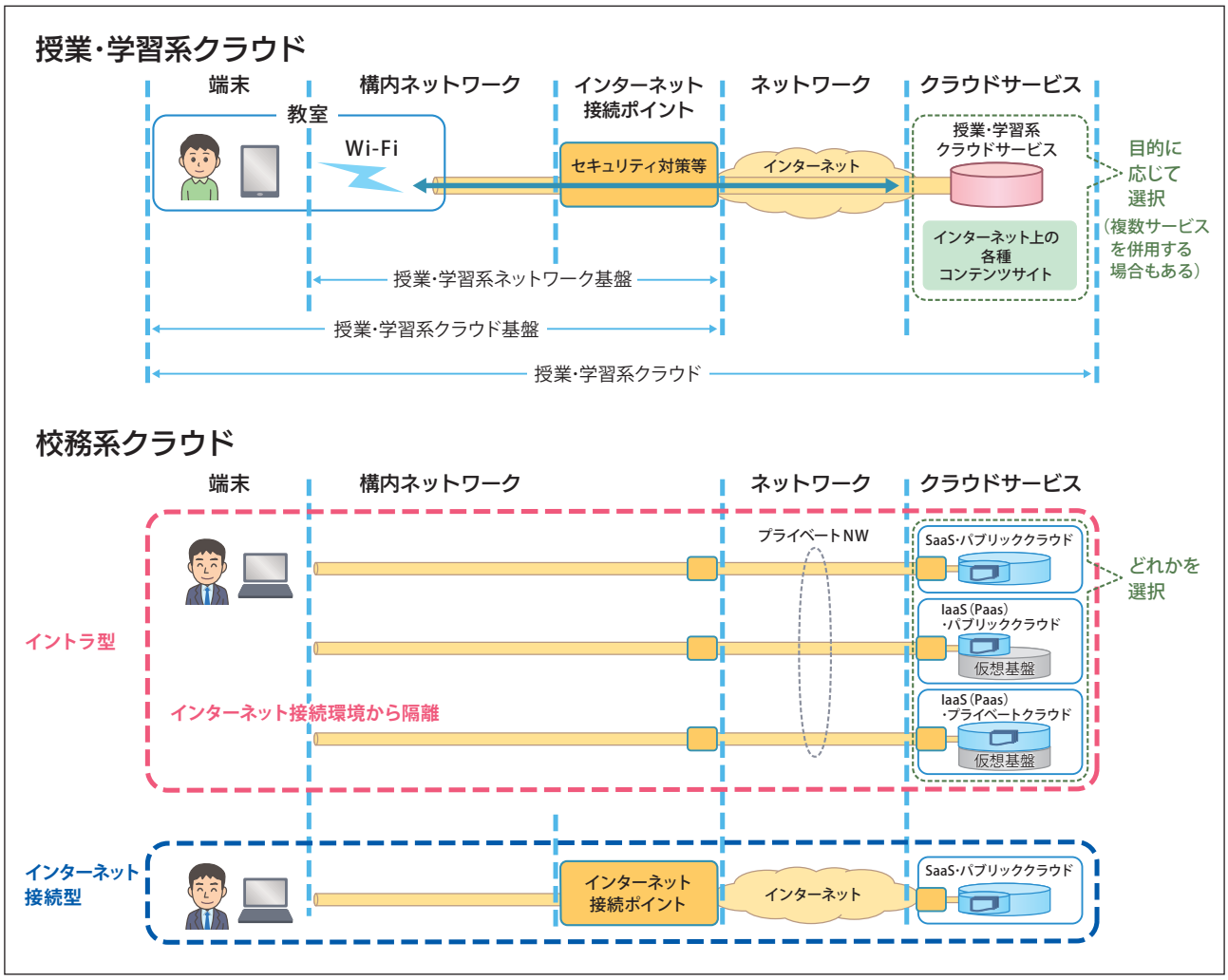
（ア） 扱う情報の重要性分類

（イ）イントラ型、インターネット接続型のどちらを選択するか（ネットワークモデル）
（ウ）仮想環境を占有するか、共用するか（クラウド実装モデル）
（エ）仮想環境の借り方（SaaS/PaaS/IaaS）（クラウドサービスモデル）

⑤教育分野におけるクラウドモデル

上記で触れたクラウドモデルを教育分野におけるクラウドモデルとして、授業・学習系クラウド、校務系クラウドに整理すると以下のようになります。

クラウドサービスモデルによる特性の違い



（ア）授業・学習系クラウド：インターネット接続・SaaS・パブリッククラウド利用型学習系システム

デジタルドリルサービス、授業支援サービス等学習系サービスはほとんどが、インターネット接続・SaaS・パブリッククラウド利用型と考えられます。さらには、学校での学習と家庭学習両方を想定したサービスが多く、インターネット接続を前提としたサービスになります。

（イ）校務系クラウド[20]（イントラ型）

端末、ネットワーク、サーバ等（クラウド）のすべてをインターネット接続環境から隔離する形でインターネットからのサイバー脅威の侵入を遮断する方式です。クラウドサービスのモデル選定により下記の 3 種などが考えられます。

（A）プライベートネットワーク接続・SaaS・パブリッククラウド型校務系システム
（B）プライベートネットワーク接続・IaaS(PaaS)・パブリッククラウド型校務系システム
（C）プライベートネットワーク接続・IaaS(PaaS)・プライベートクラウド型校務系システム

このなかでは、コスト面から SaaS・パブリッククラウド利用が最も一般的です。

20：校務系クラウドとは、校務系システムのホスト側をクラウドサービスを利用して構築するものです。

（ウ）校務系クラウド（インターネット接続型）

インターネットを通信回線として利用する形で校務系システムを構築する方式です。インターネットを通信回線として利用することで複数の自治体向けサービスを提供するものです。

（4）インターネットリスクに対する対策

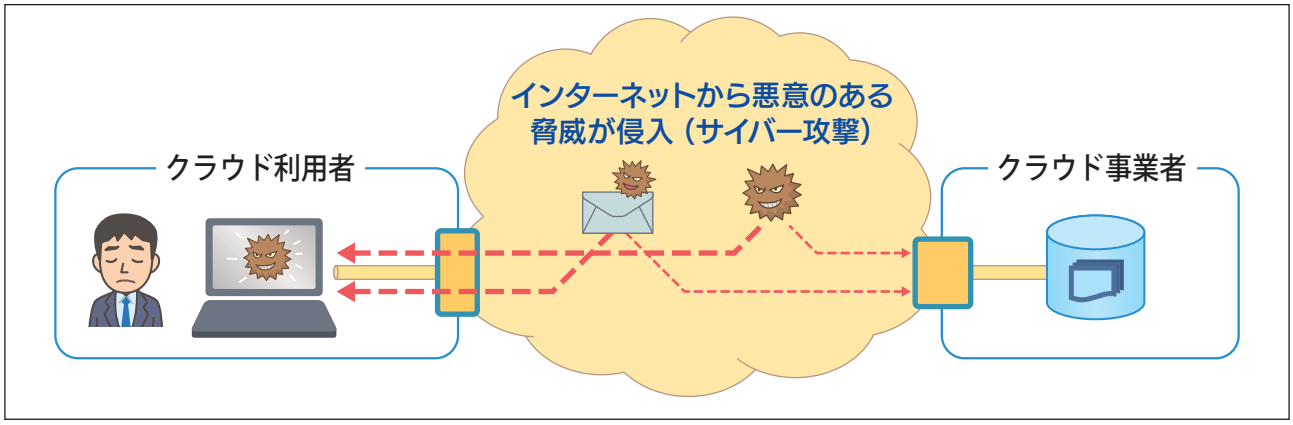
①インターネットリスク

まず、インターネットを通信回線として利用する学習系クラウドやインターネット接続型校務クラウドのセキュリティリスクについて解説します。

インターネット接続型システムに共通する最大の課題が、インターネットからのサイバー脅威が情報システム内に侵入し、サーバや端末を攻撃する、いわゆる「サイバー攻撃」対策です。インターネットに接続するすべての情報システムはインターネットからのサイバー攻撃に晒される「インターネットリスク」を負っています。このインターネットリスクは、クラウドサービス利用であってもなくても変わるものではありません。

クラウドサービス利用におけるインターネットリスクの構造を示します。インターネットリスクは、クラウド事業者にもクラウド利用者にも存在します。

インターネットリスク



そのため、クラウド事業者側システムにマルウェアが侵入することを防ぐ必要がありますが、クラウド利用者の端末にマルウェアが侵入して、クラウドに保管されているデータが利用者の端末経由で侵害される危険性もあります。

攻撃の手口としては、主に 2 つあります。

（ア）サーバや端末を攻撃	サーバや端末といったコンピュータのセキュリティ面で弱い部分を狙ってコンピュータ内部に侵入し攻撃を行う場合で、利用者としては、インターネット接続境界における監視やサイバー脅威の侵入検知・防御機能が必要です。また端末ではウイルス対策ソフトや OS を常に最新にしておくことが求められます。
（イ）利用者を標的とした攻撃	標的型メール攻撃が代表的なもので、主にはメールを利用して言葉巧みに添付ファイルを開封させたり、マルウェアを仕込んだサイトにアクセスさせたりするよう誘導します。騙された利用者は、自端末にマルウェアが仕込まれ、本人が気づかないまま攻撃者から遠隔操作されて、自端末を経由して情報漏えいや改ざんされる等の手口です。人間を標的にする手口は、システムでの防御が困難である場合が多く、100% の防御ができない前提で対策を講じる必要があります。

以上のようなインターネットリスクをどう防御するかが、インターネット接続型システムの最大課題です。この課題は、学習系システムでも校務系システムでも同様ですが、特に校務系システムでは機微な個人情報を大量に扱うため、より厳密なセキュリティ対策が求められます。

＜コラム＞　マルウェア感染の怖さ

マルウェアとは「悪意をもったソフトウェア」のことで、マルウェア感染経路は複数あります。

マルウェア感染経路

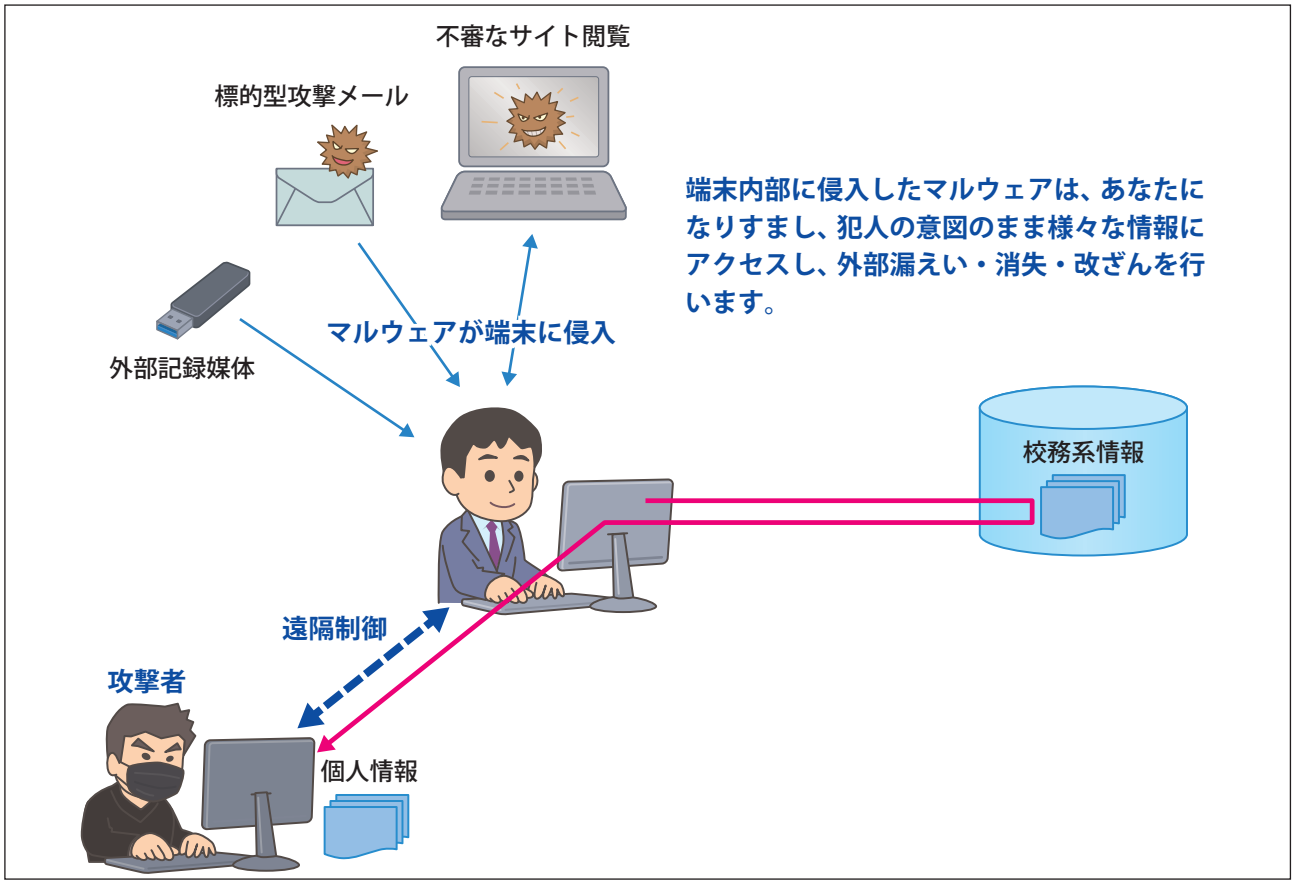
（ア）標的型攻撃メール	標的型攻撃メールとは、マルウェアを仕込んだ添付ファイルやサイト URL をメールと一緒に送り、その脅威となるプログラムを展開することでウイルスや不正プログラムを強制インストール（感染）させます。この標的型攻撃メールは、取引がある企業を装い安全なメールだと思い込ませる方法が増えています。このような偽装をされていることが多くなっているため、特に注意が必要です。
（イ）外部記録媒体	外部記録媒体を端末に接続することで、マルウェア感染する場合があります。教育現場では、教職員が自宅で業務を行う場合に USB メモリを利用して情報を持ち出す場合があります。もし、教職員の自宅パソコンがマルウェア感染していたとしたら、持ち出した USB メモリを媒介して、学校の校務用端末にマルウェア感染する危険性があります。
（ウ）不審なサイトの閲覧	不審なサイトを閲覧する危険性として、マルウェア感染を目的としたサイトに誘導される場合があります。標的型攻撃メールにも、特定のサイトに誘導し、マルウェア感染させる手口があります。

②マルウェアの動き

マルウェア感染した端末はどうなるのでしょうか。端末にマルウェアが感染した場合は、マルウェアを送り込んだ攻撃者の意図に従って動きます。すでに端末のなかに侵入済なので、端末ログインの利用者認証は突破され、端末に電源が入っている間は、端末の正規な利用者に成り代わって動作します。

そのため、正規端末からのアクセスであっても、厳密には正規な利用者からのアクセスとは言い切れないところがあります。よって、クラウドログイン時には、パスワードなどで利用者本人の真正性を確認するこ

マルウェア感染によるセキュリティ侵害例



とが必要になります。しかし、正規端末からのクラウドログイン時に、正規の利用者による入力パスワードをマルウェアが感知できた場合には、クラウドログインも突破されてしまいます。

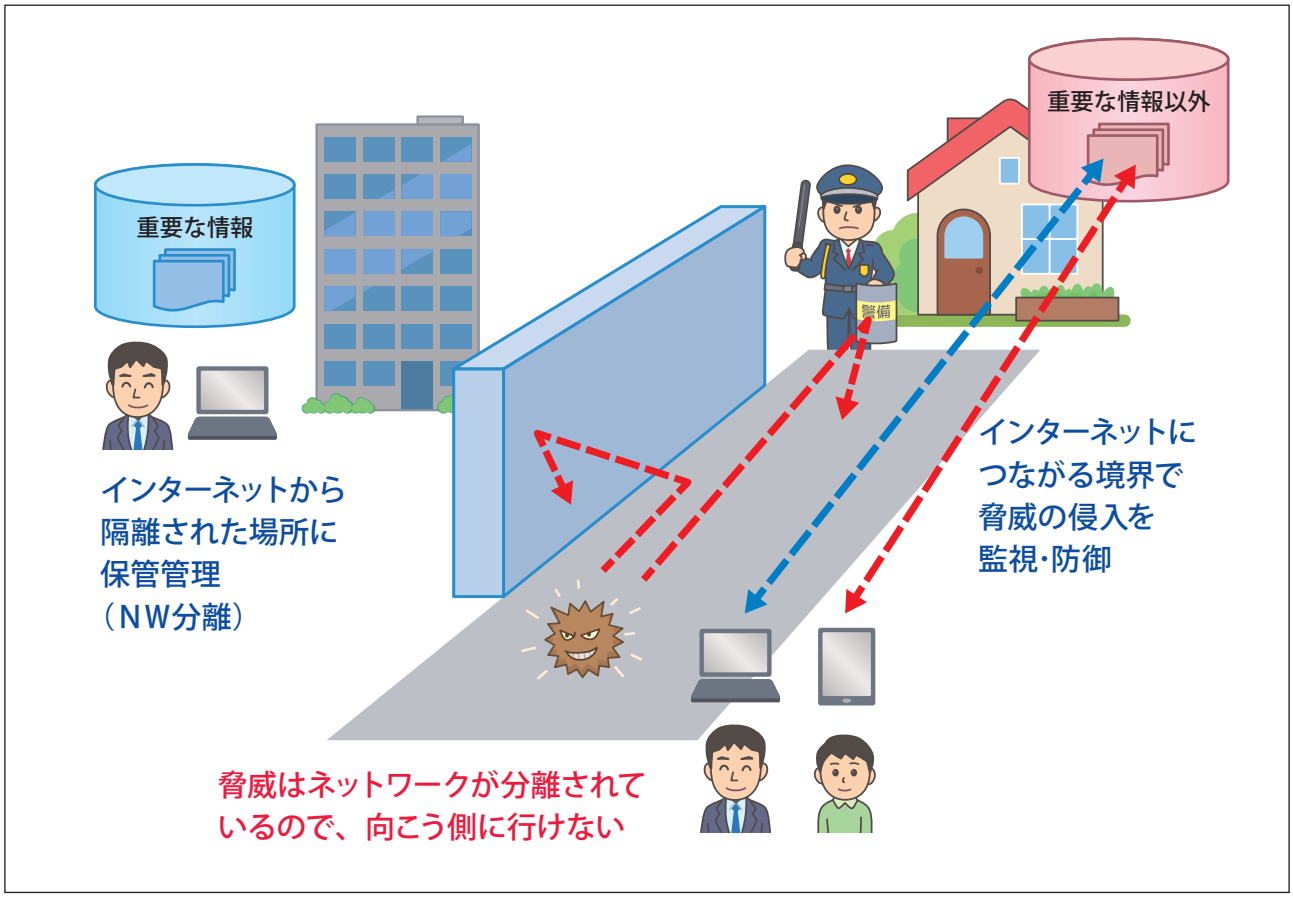
この場合の対策として、クラウド側から別のメディアによってワンタイムパスワードを送付する方法が有効です。例えば、教職員のスマホにクラウドログインパスワードが送付される場合には、正規端末にひそむマルウェアにはこのパスワードを知る手立てがありません。このケースでは、本人の真正性が認証された形でログインすることになります。また、入力されるパスワードは毎回変わるため、マルウェアが記憶したとしても、クラウドへのログインはできないこととなります。しかし、攻撃者は利用者認証の弱い部分を突く新たな方法を次々と考えるため、防御する側もそれに合わせて対応を行う必要があります。

③ネットワーク分離

ここでは、インターネットからのサイバー脅威の侵入に対して、どのようにセキュリティ確保を講じるかについて、２つの考え方を比較してみましょう。

最初に、インターネットからのサイバー脅威に対する対策の考え方を以下に示します。考え方は、インターネットとつながらないようにすることでサイバー脅威の侵入を防ぐことです。イントラ型クラウドは、この考え方を踏襲しており、インターネットの脅威が情報システム内部に侵入しないように、インターネットから通信経路を切り離した閉域（イントラネット）システムです。

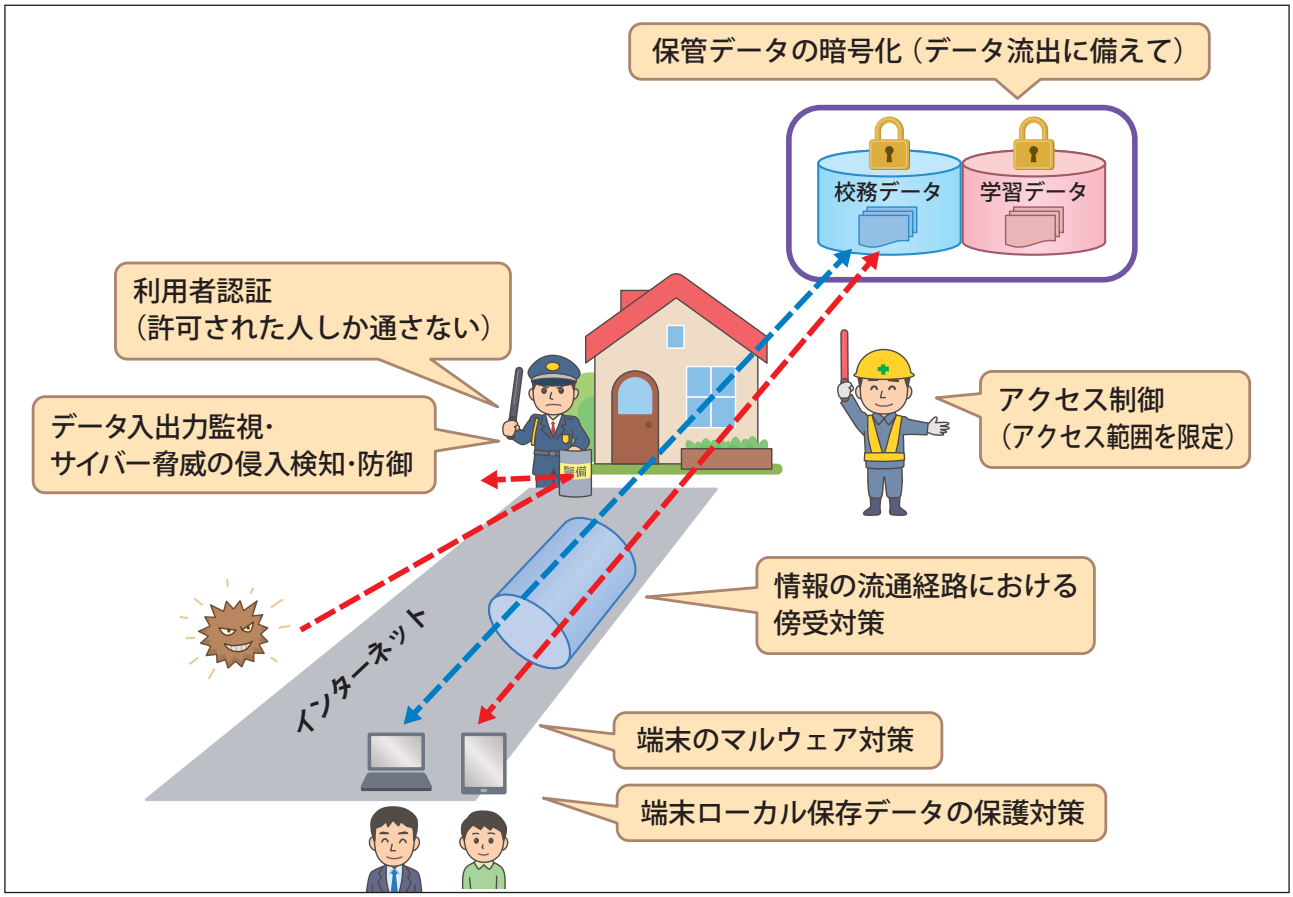
ネットワーク分離イメージ（※一般道にたとえた場合）



④インターネット接続型クラウドにおけるセキュリティ確保

では、インターネット接続を前提とする校務系の SaaS 利用ではどのようにインターネットからのサイバー脅威の侵入を防ぐのでしょうか。考え方としては、ネットワーク分離する方法で防ぐことはできませんので、複数の対策の合わせ技で防ぐアプローチになります。

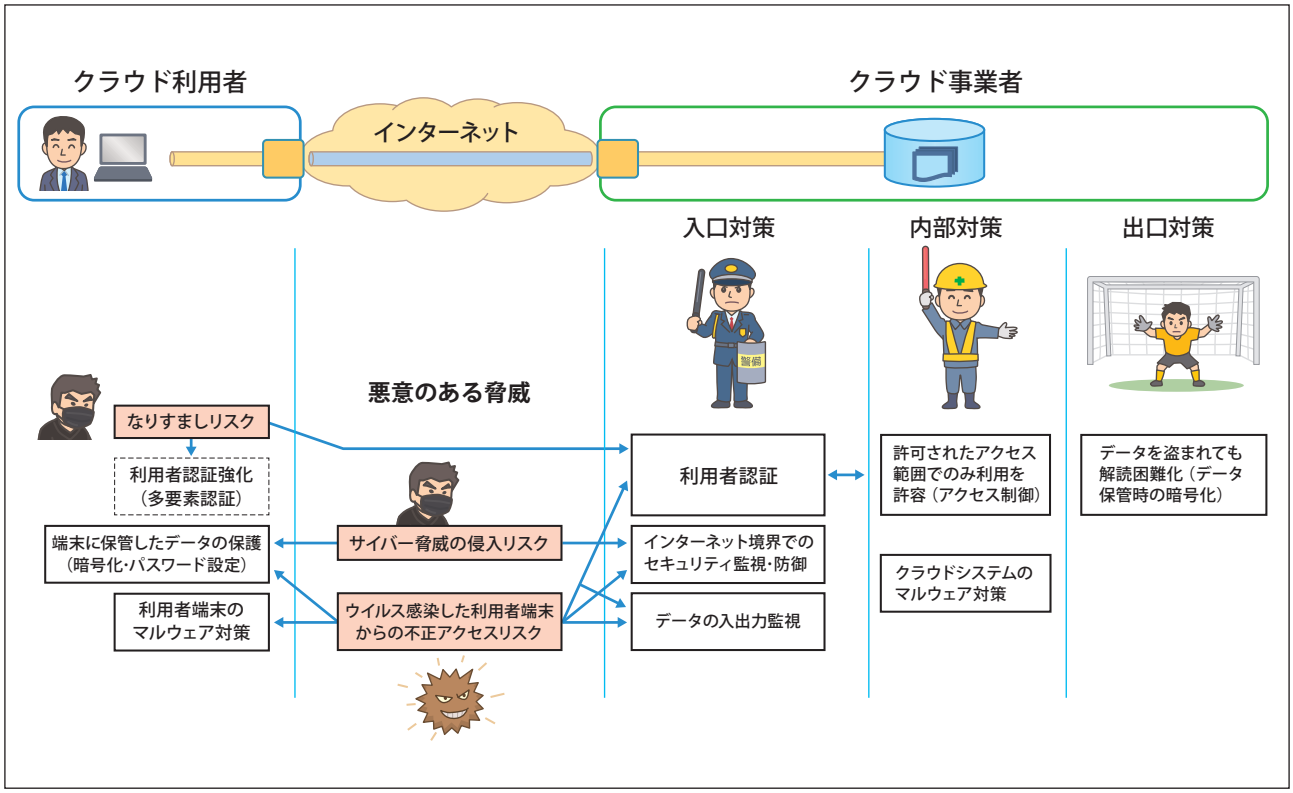
インターネット接続型クラウドでのセキュリティ確保イメージ（※一般道にたとえた場合）



⑤インターネットからのサイバー脅威に対するクラウド利用型システムのセキュリティ対策

まず、インターネット接続型クラウドを前提にクラウドシステム側の対策から見ていきましょう。

インターネット接続型クラウドにおける技術的セキュリティ対策



（ア） クラウドシステム入口対策

クラウドシステムはインターネットと接続していますのでインターネット接続境界にて監視等を行い、正規なアクセスは中に入れ、疑わしいアクセスは中に入れない措置が必要になります。そのためには、下記の入り口対策が求められます。

（A）利用者認証

許可された人しか中に通さないために必要な措置です。利用者認証方式としては、ＩＤ・パスワードによる記憶認証が一般的ですが、数字やアルファベッドの組み合わせのため、総当たり攻撃（ブルートフォースアタックと言います）や、利用者のＩＤ・パスワード管理が不徹底で他者に知られるなどの弱点があります。ＩＤ・パスワードが破られると、システム側は正規な利用者として認識しますので、利用者のアクセス権限の範囲で自由に情報を閲覧・複製することができます。

利用者認証強化の方策としては、異なる方式による利用者認証を複数組み合わせる多要素認証が有効です。記憶認証（ＩＤ・パスワード）に生体認証（顔や指紋、生体認証静脈等本人しか持ち合わせない身体的特徴）または物理認証（ＩＣカードなど）を組み合わせることで、格段に認証レベルが向上します。

ここでは、クラウドにログインするための利用者認証について取り上げていますが、利用者の端末ログインにおいても同じことが言えます。

まずは、利用者の端末ログインの段階で利用者認証の強化が必要で、多要素認証を検討されているケースも多いと考えられます。

クラウドログインにおいては、さらにワンタイムパスワード等端末ログインとは別の方式の利用者認証を組み合わせることが有効です。

多要素認証

認証要素	認証手段	概要	例
要素A	記憶	本人だけが知っている情報	パスワード
要素B	生体	本人だけに備わっている特徴	静脈、顔、指紋、網膜、虹彩
要素C	物理	本人だけが持っているモノ	ICカード、USBキー、トークン

複数要素認証
・要素の異なる認証を複数組み合わせた認証

二要素認証の例
要素A+要素B
要素A+要素C
要素B+要素C

※出典：「教育情報セキュリティポリシーに関するガイドライン　ハンドブック」（平成 29 年版）（文部科学省）

（B）サイバー脅威の侵入を検出・防御する技術的セキュリティ対策

クラウドシステムの入口対策として、インターネット上のサイバー脅威の侵入を検知して防御する仕組みが必要です。そのためには、以下のような点に留意し、インターネット境界でのセキュリティゲートウェイ機能として装備することが重要です。

・クラウド利用者が利用するＩＰアドレスに限定して中に入れる	ファイヤーウォールにおける設定
・通信データの常時監視（不信なデータ送受信をチェック）	マルウェアによる不正アクセスでは、教職員が働いていない時間帯や教職員がアクセスするはずのないサーバにアクセスするなどの不審な挙動が起こりえます。そのような不審な挙動を検知するセキュリティソリューションも登場しています。
・脅威の侵入を検知して防御する仕組み	侵入検知システム（IDS）、侵入防止システム（IPS）

（イ）　クラウドシステム内部対策

　サイバー脅威が侵入した場合に、その被害を最小限度に留めるための対策です。

クラウドシステムを直接攻撃するタイプの脅威は入口対策で食い止められる場合が多いのですが、利用者端末がマルウェア感染して、利用者になりすましてクラウドシステムに侵入する場合などは入口対策を突破される危険性が高く、その場合は、利用者がアクセス権限をもつエリアに脅威がフリーパスで侵入可能です。

(A) アクセス制御	ここで被害を最小限度に抑止する方法がアクセス制御です。アクセス制御とは、アクセス権限のある範囲ではアクセス可能とし、権限のない範囲ではアクセスできないように制御することを言います。 なりすまし利用者やマルウェア感染した端末が遠隔操作されてクラウドシステム内部に侵入した場合でも、アクセス制御が適正に設定されていれば、アクセス可能な範囲が限定されます。 ただし、攻撃者もそのことがわかっていますので、アクセス権限の広い運用保守拠点の端末や学校管理者の端末が標的となりうることに注意ください。
(B) サーバ及び端末へのマルウェア対策	クラウドシステムを構成するサーバ及び運用管理端末にマルウェアが侵入した場合に備えて、ウイルス対策ソフトの導入等の対策を講じる必要があります。 （なおマルウェア対策は、クラウドに関係なく必要な対策となります。）

（ウ）　クラウドシステム出口対策

　出口対策とは、守るべきデータが外部に漏えいすることを前提にした対策です。データが外部漏えいしてもすぐに解読できないように保管するデータ自体に暗号化することが原理的には有効です。

（A）クラウドに保管するデータの暗号化

　クラウドに保管するデータの暗号化をクラウド事業者側で行うケースとクラウド利用者側で行うケースを対比してみました。

●ケース１：クラウド事業者側で暗号化

　クラウド事業者側で暗号化することはクラウド利用者からは自前の暗号化運用作業が不要となります。

　ただ、利用者端末がＷＥＢブラウザ機能を利用して通信処理を行っているため、復号化機能を端末側に持たせることが難しく、クラウド側で復号化して端末に転送する形になります。データ送受信のたびに暗号化・復号化処理することはクラウドシステムの負荷となり、一定程度処理能力がダウンする可能性もあります。

　また、クラウドシステムに直接脅威が侵入して保管データを持ち出す場合には、アプリケーションやデータベースにアクセスし、アプリケーション上に格納した復号キーも同時に流出するリスクがあり、原理どおりには有効性を発揮できないリスクがあります。

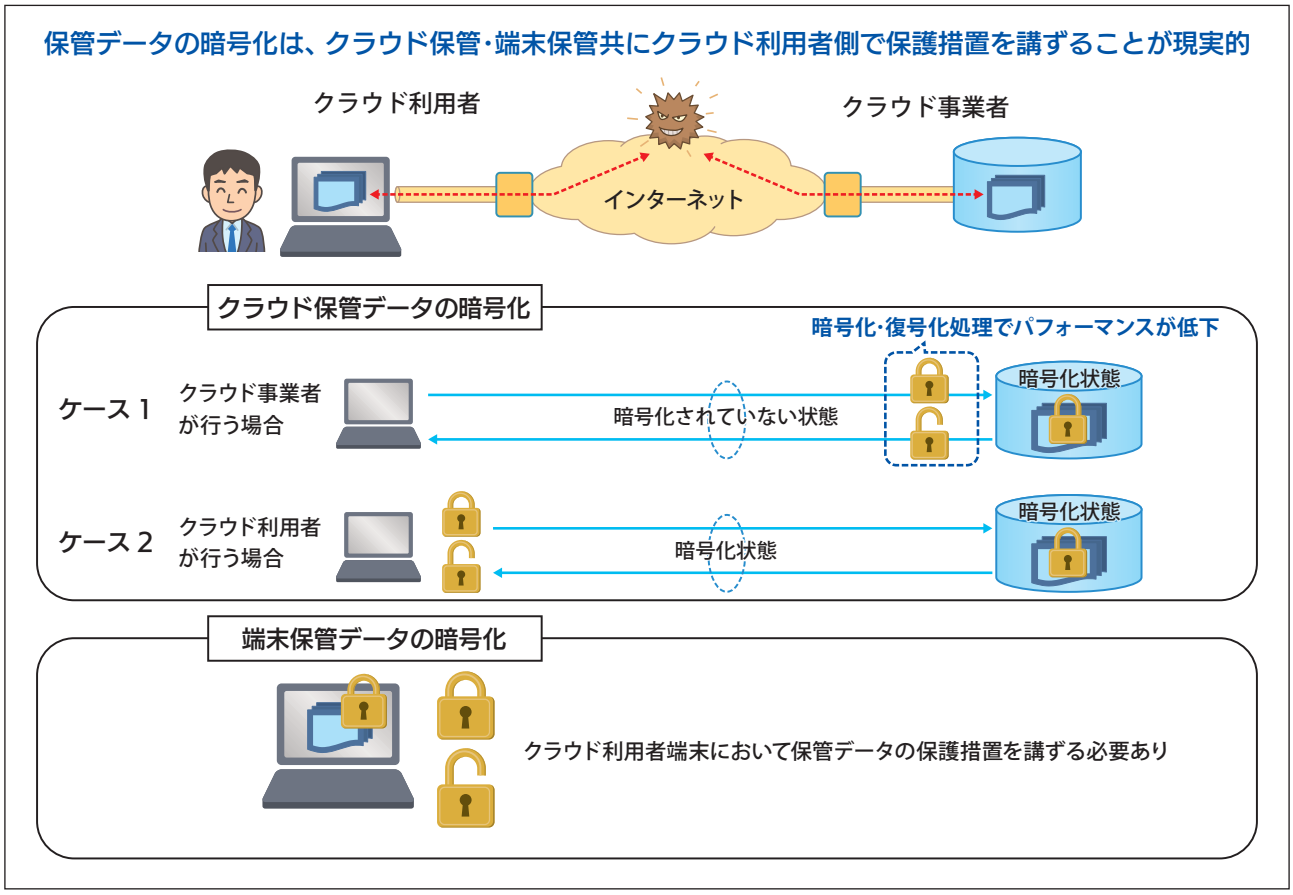
●ケース２：クラウド利用者側で暗号化

　暗号化・復号化処理を利用者端末で行うことができれば、通信経路を含めて暗号化される点で有利です。ただし、自動的に暗号化されるソリューション等を導入する場合のコスト負担などの課題が残ります。

　別の方法として利用するデータファイルにパスワードをかけてクラウド保存するなどのアプローチが考えられます。この場合には、出口対策としては有効ですが、利用者自身にパスワード設定の負担をかけます。

　以上のようにケース1、２とも一長一短があります。クラウド利用者側での自動暗号・復号化がセキュリティ対策としては望ましいのですが、コスト、教職員の手間、安全対策としての信頼性の総合判断になります。

保管データの暗号化



（B）端末に保管するデータの暗号化

機微な校務系情報など重要な情報を端末に保管することは避けることが望ましいと考えられますが、校務で作業中の成績処理データ等を一時保管するニーズが存在します。学校の事情から、端末に重要な情報を保管する場合には、利用者側で必ず暗号化またはファイルパスワード設定が必要になります。

⑥通信経路における傍受対策

通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置が求められます。

インターネット接続型クラウドでは、クラウド利用者のインターネット境界から当該クラウドサービスを提供する情報システムまでの通信経路としてインターネットを利用しますので、通信の暗号化等安全性を確保するために必要な保護措置を講じる必要があります。

一般的には、SSL（Secure Socket Layer）通信が使われます。この方式はインターネット上で個人情報を扱う場合やショッピングでの決済行為を安全に行うための暗号化方式として広く普及しています。サーバと端末の WEB ブラウザ間で、通信が発生する毎に、公開鍵・共通鍵による暗号方式が利用されます。

SSL 通信は、端末とサーバ間で情報のやり取りが発生する都度に通信経路を設定する形式であり、端末とサーバ間であらかじめ通信回線を固定的に用意しておくプライベートネットワークとは異なります。

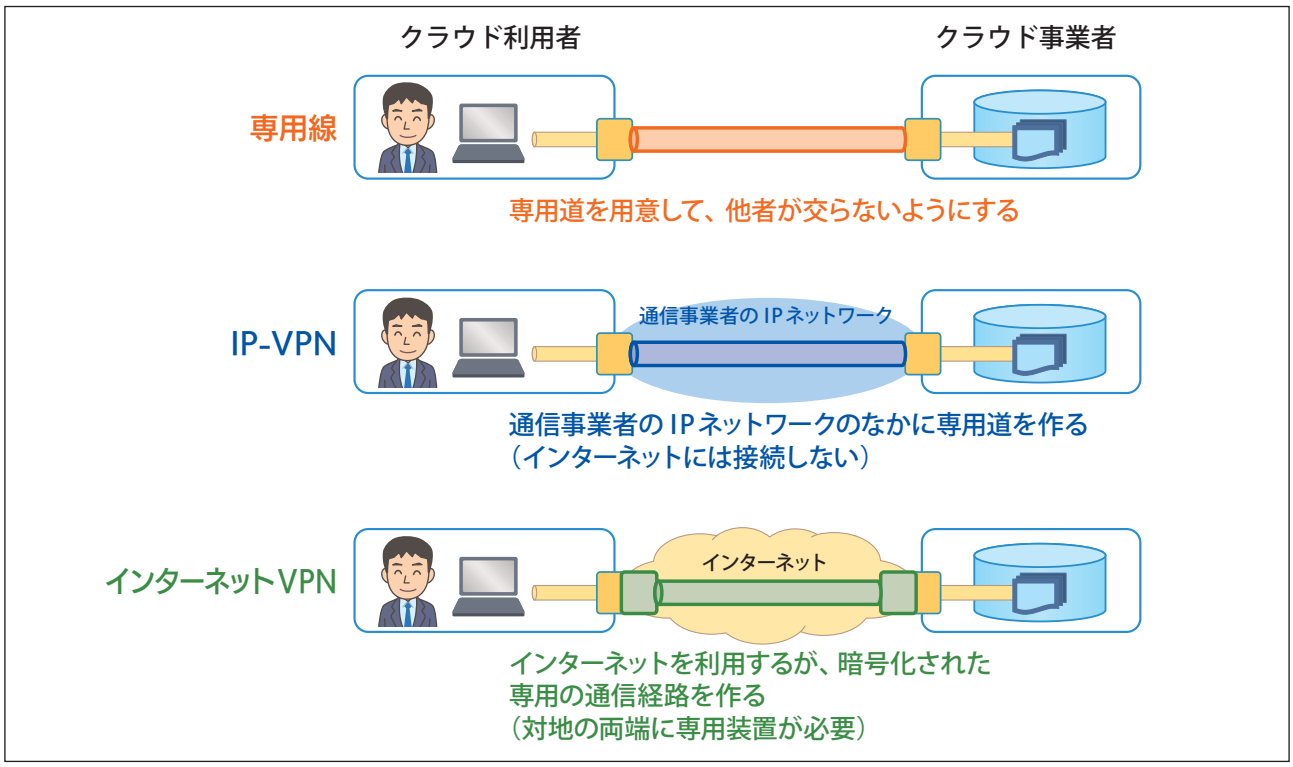
イントラ型クラウドで利用されるプライベートネットワークでは、専用線、IP-VPN,IP-SEC といった方式が用いられます。専用線は他の回線とは交わらない最もセキュリティの高い回線ですが、相対的にコスト高です。IP-VPN は通信会社の IP ネットワーク内で暗号化通信しますので、インターネットの中に情報を流通させない点でセキュリティレベルの高い回線です。

インターネット VPN は、IP-SEC と称する暗号化通信プロトコルを用いて、インターネットの中に暗号化された専用の通信経路を形成する方式です。なお、インターネット VPN を形成するためには、送受信する

双方に専用の装置が必要になります。

これらプライベートネットワークは、対地（入口と出口の 2 箇所）が固定された 1 対 1 の通信経路上にあらかじめ必要な保護措置が講じられている点が、SSL 通信と異なる部分です。

プライベートネットワーク



また、学校のなかで無線LANを利用する場合にも、通信中の電波を傍受されるリスクがあります。そのため、充分な暗号強度をもった無線 LAN 方式を採用する必要があります。

⑦インターネットからのサイバー脅威に対するクラウド利用者側でのセキュリティ対策

インターネット接続型クラウド利用では、インターネットからのサイバー脅威がクラウド利用者側の情報システムに侵入することに備えたセキュリティ対策が必要です。

考え方は、⑤クラウド利用型システムのセキュリティ対策と同じになります。

（ア）入口対策	インターネット接続境界において、脅威の侵入を検知し、防御する対策が必要になります。
（イ）内部対策	端末やサーバに対するマルウェア対策が必要です。
（ウ）出口対策	学校の端末やサーバに重要な情報資産を保管する場合には、保管データの暗号化が重要になります。

（5）物理的セキュリティ対策

外部からのセキュリティ脅威のなかで、自然災害や窃盗に対しては物理的に守ることになります。

クラウド事業者側のデータセンター及び保守運用拠点、クラウド利用者側の拠点（学校等）が守る対象になります。

①クラウド事業者側の物理的セキュリティ対策

クラウド事業者側の物理的なセキュリティ対策がどのように講じられ、どのくらい安全かについては委託先の権限と責任ですが、クラウド利用者として確認しておく必要があります。

（ア）データセンターの物理的対策	クラウド事業者のデータセンター内のサーバにはクラウド利用者のデータが保管されますので、自然災害や外部からの不審者の侵入などの脅威に対して物理的にガードします。 以下の 2 点が求められます。 ・安全なサーバの管理（冗長化、予備電源の設置、定期保守等） ・データセンターとして堅牢な構造（耐震・耐水・耐湿・停電対策等）及び入退室管理
（イ）保守運用拠点の物理的対策	クラウド事業者の保守運用拠点はデータセンターとは別のロケーションにあり、通信回線で結ばれている場合があります。SaaS 保守運用拠点における運用管理端末は、数多くのクラウド利用者データにアクセス可能なため、外部脅威から狙われやすく、データセンター同様に保守運用拠点に求められる堅牢な構造（耐震・耐水・耐湿・停電対策等）及び入退室管理は重要です。

②クラウド利用者側の拠点（学校等）の物理的セキュリティ対策[21]

学校に存在する重要な情報資産を保管する際は、物理的な観点では以下の点で注意が必要です。

21：「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省） 1.4 物理的セキュリティで規定されています。

（ア）端末（外部記録媒体を含む）	端末（外部記録媒体を含む）に重要な情報資産が保管されている場合に盗難被害に合うと、重要な情報資産の外部漏えい事案になりますので、端末の盗難対策（デスクトップ端末はワイヤーロック、モバイル型端末・外部記録媒体は施錠保管）の徹底が必要です。
（イ）サーバ	学校への校務系サーバの設置は、自然災害や窃盗に対して必ずしも盤石とはいえず、セキュリティリスクが高く、運用負担が多い形態と言えます。 多くの学校は避難所になり、堅牢な建物構造ですが、サーバ設置を目的に各種セキュリティ対策が講じられているデータセンターのようなセキュアな環境ではありません。また、多くの人が出入りするため、サーバ設置場所への入退室管理等、学校の運用負担が大きいのが実情です。

（6）内部脅威に対する対策

①クラウド事業者側内部脅威

クラウド事業者従業員の不正行為や過失行為がクラウド事業者側内部脅威になります。どちらも人的な脅威ですので、クラウド事業者の人的なセキュリティ確保について確認する必要があります。

クラウド事業者従業員は高度な運用管理を行う立場であり、運用を間違えるとクラウド利用者の仮想環境が消滅するリスクもあります。また、SaaS 事業者は利用者データにアクセス可能な立場であることから、不正アクセス等を抑止するための人的セキュリティ対策を遵守する必要があります。

（ア）クラウド事業者従業員の人的セキュリティ対策	以下 3 点について、ルール化することをクラウド事業者に求めることが必要です。 （A）クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守 （B）ID 及びパスワードその他の利用者認証に必要な情報及び媒体の適切な管理 （C）業務に関わるクラウド事業者従業員に対して秘密保持義務を課すこと
（イ）クラウド事業者従業員への教育	従業員に対して個人情報保護等の関係法令、守秘義務等、業務遂行に必要な知識、意識向上のための適切な教育及び訓練を実施し、充分な知識とセキュリティ意識を醸成することをクラウド事業者に求めることが必要です。

②クラウド利用者側内部脅威

人的なセキュリティ確保[22]については、クラウド事業者の人的なセキュリティ確保と変わりませんが、学校には児童生徒が存在するため、児童生徒にまつわる対策について配慮する必要があります。

（ア） 児童生徒による重要な情報へのアクセス禁止

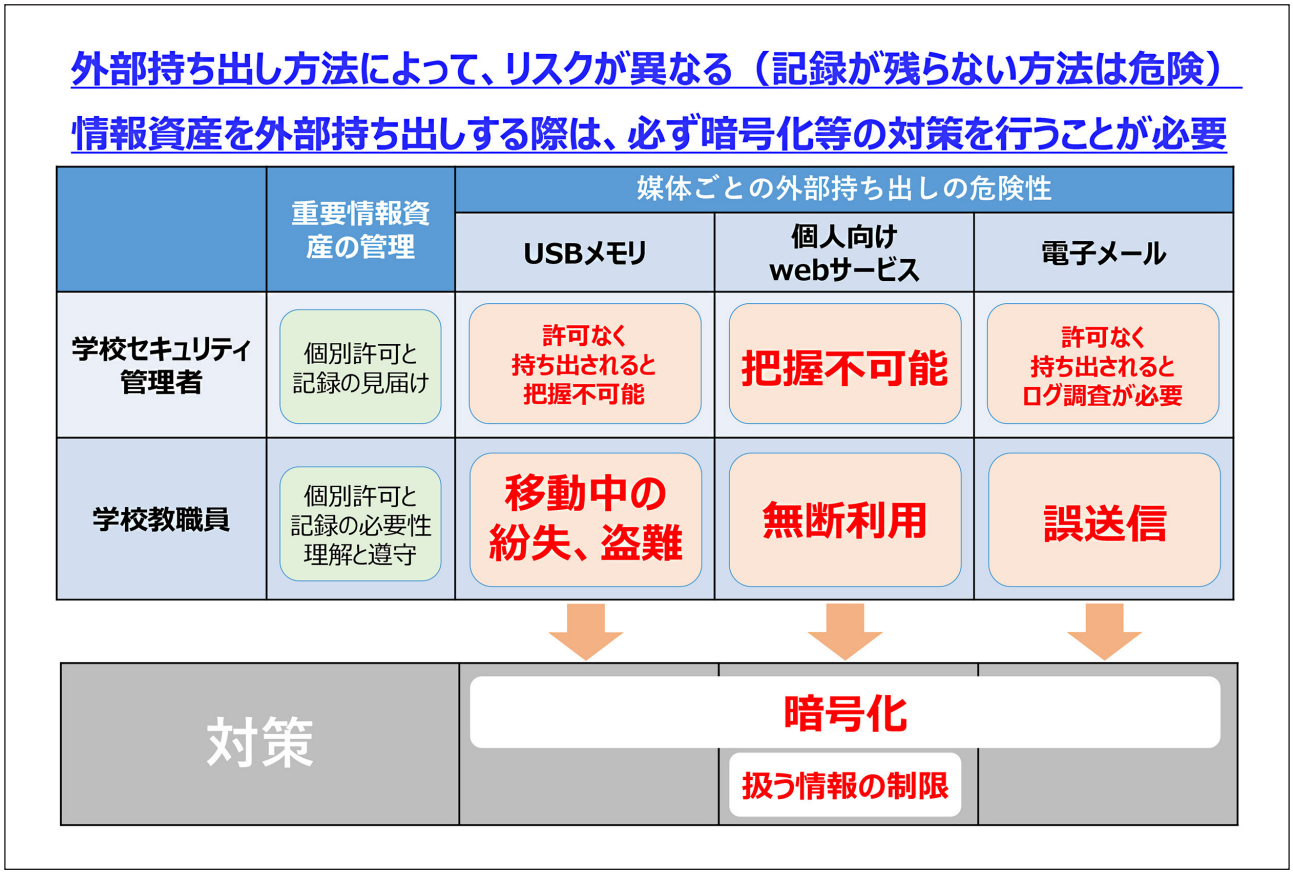
児童生徒が機微な校務系情報へアクセス・閲覧することは避けなければなりません。児童生徒の機微な情報への接する可能性として、職員室における教職員のデスクに放置された書類やパソコン画面を、たまたま見てしまうケースが想定されます。職員室のデスクを整理し、クリーンデスク・クリーンオフィスを徹底する必要があります。教室で校務事務を行う場合は注意が必要です。

（イ） 重要な情報資産の外部持ち出し

重要な情報資産を外部持ち出しする行為は、セキュリティレベルが大きく下がります。さらに、重要な情報資産の外部持ち出し行為は、教育情報セキュリティ管理者（校長等）の個別許可等、自治体の教育情報セキュリティポリシーに基づく手続きが必要となります。

22：「教育情報セキュリティポリシーに関するガイドライン（令和元年版）」（文部科学省）1.5 人的セキュリティで規定されています。

情報資産の外部持ち出しの危険性



（ウ） マルウェアを学校に持ち込まない

マルウェアが学校に侵入するルートは主に 7 つあり、大きく 2 種類に分けられます。

（A）教職員や児童生徒がマルウェアを学校に持ち込むルート

①標的型攻撃メール	（4）①（イ）に示したように、インターネットリスクとして、教職員を標的にしたマルウェア感染の危険性があります。標的型攻撃の備えとして、少しでも不自然なメールや送信元に心当たりのないメールを不用意に開封しないことが求められますので、危険性とその対応について教職員への徹底が求められます。
②私物の端末や外部記録媒体の業務利用	私物のパソコン等を学校のネットワークに接続することは非常に危険です。私物端末がマルウェア感染している場合には、学校のネットワークを介して接続されているコンピュータにも感染するリスクがあります。私物の USB メモリを学校の正規端末に接続する場合も、同様に危険です。 やむを得ず私物端末や USB メモリを業務利用する場合には、ウイルス対策ソフト等でマルウェア感染していないことを確認したうえで、利用することが求められます。
③無許可での外部ソフトウェアのダウンロード	インターネット上で魅力的なソフトウェアを発見しても、すぐにダウンロードすることは危険です。該当ソフトウェアにマルウェアが仕込まれている場合があるからです。教職員は必ず、教育情報セキュリティ管理者（校長等）の事前許可をとってから、安全性を確認のうえ、ソフトウェアダウンロードすることが求められます。
④業務に関係ない不審なサイトへのアクセス	インターネット上のサイトのなかには、意図的にマルウェア感染させる目的のものが存在します。不審なサイトにアクセスしないことが求められます。安全が確認されたサイトにしかアクセスできないように、アクセス先を制限するコンテンツフィルタリングを設定することが大切です。

（B）セキュリティ対策レベルを下げる３つの感染ルート

※セキュリティ対策が施されたシステム環境に教職員や児童生徒が手を加えて、セキュリティレベルを低下させる行為を指します。勝手にシステムの設定を変更することができないよう制限をかける等の対策を行うことが重要です。

⑤端末のウイルス対策ソフトや OS の更新停止	端末のウイルス対策ソフトや OS（Windows 等のコンピュータを動かす基本ソフト）の更新を意図的に止めてしまうことは、セキュリティレベルを最新の状態に保てずに、マルウェアを侵入させやすくする禁止行為です。
⑥端末のセキュリティ設定の変更	端末には最適なセキュリティ設定が施されています。例えば、外部のソフトウェアダウンロードがセキュリティ設定上不可の場合に、設定レベルを落としてダウンロードできる場合があります。このような行為は意図的にマルウェアを侵入させやすくする禁止行為です。
⑦無許可での機器の改造・増設・交換	端末やネットワーク機器を無許可で機器改造・増設・交換する行為は、セキュリティ設定が変わってマルウェアを侵入させやすくする行為です。必ず、事前許可を取る必要があります。

参考5 クラウド利用に関連する法制度

（1）個人情報保護法制

①各対象者が確認すべき法令

児童生徒や保護者等の個人情報を適正に取り扱うためは、個人情報保護に関する法令について確認を行い、必要な手続きを行わなければなりません。

個人情報保護に関する法令は、以下の表のように、対象者によって確認すべきものが異なります。

各対象者が確認すべき法律

対象者	確認すべき法律
公立学校	各自治体の「個人情報保護条例」
国立学校	「独立行政法人等の保有する個人情報の保護に関する法律」
私立学校	「個人情報保護法（個人情報の保護に関する法律）」4～7章

※「個人情報保護に関する法律・ガイドラインの体系イメージ」（個人情報保護委員会）（https://www.ppc.go.jp/files/pdf/personal_framework.pdf）を元に作成

個人情報の具体的な取扱いについては、各団体が対象となる法令をそれぞれ確認した上で、必要な手続きを講じる必要があります。該当する法律について、個別に確認するようにしましょう。

対象者に応じた確認すべき内容について、②～⑤に示します。

②公立学校・国立学校・私立学校が共通して確認すべきこと

個人情報保護法令が保護の対象とする個人情報の定義は、各法令によって異なります。しかしながら、公立、私立、国立の別を問わず、各学校では個人情報保護の取り組みがなされているはずであり、適用される法令に関する解説なども参照して理解を深めてください。ここでは、各法令に共通するごく基本的なことを説明します。

個人情報には、単体（集合）でそれ自体が個人情報になるものと、そのような個人情報と結びつくことによって個人情報になるものがあります。前者については、例えば、氏名と直接紐付いている情報は個人情報に該当しますし、氏名を削除していたとしても、住所と勤務先の組み合わせにより個人が識別可能な場合も、個人情報に当たります。顔写真等についても、それ自体で個人が識別できてしまうため、個人情報に当たります。重要なのは後者、すなわち、それ（ら）自体が個人情報になるもの（前者）と結びつくことによって個人情報になるものがあることです。例えば、人のネクタイの色や購買履歴は、それだけでは個人情報になりませんが、特定の人の氏名等とむすびつくことによって個人情報となるのです。

「郵便番号は個人情報ですか？」という質問には、すぐに答えることはできません。なぜなら、郵便番号がそれ自体で個人情報でないことは明らかですが、「〇〇さんの郵便番号」という形で個人に紐づいていれば、個人情報となるからです。

※詳しくは「個人情報の保護に関する法律についてのガイドライン（通則編）」（個人情報保護委員会）を参照ください。

＜コラム＞　個人情報保護法の見直し状況

個人情報保護法は、3年ごとに見直しを行うものと定められています。本書は 2017 年版の個人情報保護法を基に執筆しております。法律は常に更新されていくため、最新の情報を確認するようにしましょう。

※詳しくは、「個人情報保護委員会」サイト（https://www.ppc.go.jp/）を参照ください。

③公立学校が確認すべきこと

※詳しくは、各自治体の「個人情報保護条例」を参照ください。

個人情報保護条例は、自治体によってそれぞれ内容が異なるため、該当する自治体のものを個別に確認する必要があります。特に、個人情報を取り扱う情報システムを導入する場合には、個人情報保護審査会への諮問や、首長または特定部局への届け出・承認等、条例等で定められた手続きを得る必要があるため、注意が必要です。

個人情報保護条例において確認すべき主なポイントと、手続きについて確認すべき主なポイントの例を、以下に記載します。詳しくは、各自治体の個人情報保護条例を必ず個別に確認するようにしてください。

個人情報保護条例において確認すべき主なポイント（例）

確認ポイント	確認内容
（ア）収集の制限について	個人情報の収集に関わる制限について確認する。
（イ）利用の制限について	個人情報の利用に関わる制限について確認する。
（ウ）外部提供の制限について	保有する個人情報を外部へ提供する場合の制限（本人の同意や同意なしで提供できる等）について確認する。
（エ）電子計算機の結合（オンライン結合）の制限について	保有する個人情報の電子計算機処理をするにあたって、実施機関（教育委員会）以外のものとの間における電気通信による電子計算機の結合の制限について確認する。
（オ）委託に関する制限について	保有する個人情報を外部に委託する際の制限について確認する。
（カ）適正管理の原則について	保有する個人情報の適正管理について確認する。

個人情報保護にまつわる手続きについて確認すべき主なポイント（例）

確認ポイント	必要な手続き
前提条件の確認	・データ取得時の根拠法令の確認 ・統計的な活用に関する確認 ・実施期間に関する確認 ・他の法令について確認
利用目的の確認	・個人情報取扱事務名の把握 ・事務に記載されている利用目的の確認 ・目的の範囲内かどうかの判断 ・目的外利用に係る該当条項の確認 ・目的外利用が可能かどうかの判断 ・利用条件等の検討
庁内手続きの確認	・個人情報保護審査会等 ・答申・庁内稟議等 ・事前通知 ・利用目的の明示 ・同意書による確認
データの入手・共有方法の確認	・データの入手方法の確認 ・データの共有方法の確認 ・適正管理 ・開示・訂正・利用停止請求
提供先・委託先の確認	・提供先の確認 ・委託事業者との責任分界 ・委託先の管理に関する設定・委託先管理体制・監督指導に関する記載
その他対応の確認	・情報漏えい時の対応 ・研修・育成（教員向け・児童生徒向け） ・監査・管理

④国立学校が確認すべきこと

国立学校が確認すべき主なポイントについて、以下に記載いたします。

※詳しくは、「独立行政法人等の保有する個人情報の保護に関する法律」を参照ください。

なお国立大学法人では、個人情報の適切な管理のための措置に関する規則等を、各々整備しているケースがあります。その場合は、そちらの管理規程についても参照するようにしましょう。

確認すべき主なポイント

確認ポイント	確認内容
（ア）利用目的の明示について	あらかじめ本人（保護者）に対してその利用目的を明示する必要があるため、その方法について確認する。
（イ）安全確保の措置について	適切な管理のために必要な措置を講じる必要があるため、その方法について確認する。
（ウ）利用及び提供の制限について	利用目的以外の目的のために保有個人情報を自ら利用又は提供するために、必要となる以下の条件のどれかを満たしているかどうか確認する。 ・本人の同意（保護者の同意）を得る場合 ・本人に提供する場合 ・学術研究の目的のために保有個人情報を提供する場合 ・本人以外の者に提供することが明らかに本人の利益になる場合 ・その他保有個人情報を提供することについて特別の理由のある場合

⑤私立学校が確認すべきこと

私立学校が確認すべき主なポイントについて、以下に記載します。

※詳しくは、「個人情報保護法」4～7章を参照ください。

確認すべき主なポイント

確認ポイント	確認内容
（ア）個人情報の利用目的について	利用目的をできる限り具体的に特定するため、その方法について確認する。 （「学習支援を行うため」等のあいまいな特定を避ける） ※なお利用目的を変更する場合には、本人の同意[23]が必要。
（イ）個人情報の取得について	要配慮個人情報を取得する際は、あらかじめ本人の同意を得る必要があるため、その方法について確認する。 （未成年の場合は、保護者等から同意を得ることとなる）
（ウ）個人データ[24]の管理について	適切な安全管理措置、従業者の監督、委託先の監督の義務を果たす必要があるため、その方法について確認する。
（エ）個人データの第三者への提供について	あらかじめ本人の同意を得ないで、個人データを第三者に提供しないよう配慮する。（ただし例外措置があるため、第三者提供を行う場合は、その内容について確認する）
（オ）保有個人データ[25]に関する事項の公表等、保有個人データの開示・訂正等・利用停止等について	保有個人データの利用目的及びその取扱いに関する苦情の申出先等について、本人の知り得る状態に置くよう配慮する。
（カ）個人情報の取扱いに関する苦情処理について	個人情報の取扱いに関する苦情を本人（保護者）から受けた際、その適切かつ迅速な処理を行うための体制の整備を行う。

23：法律実務の観点からは、一般に、児童生徒の全員から一律に同意を取得し、個々の児童生徒が事実上拒否できない場合には、同意が無効となる可能性があることに留意することが必要であると考えられます。

24：個人情報データベース等を構成する個人情報をいう。（個人情報保護法第2条6項）

25：個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は1年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。（個人情報保護法第2条7項）

⑥クラウドサービス事業者に守らせるべきこと

クラウドサービスを利用するに際して、例えば個人情報保護法上の委託先の監督義務（第 22 条）を負わないためには、クラウドサービス事業者が個人データを取り扱わないこととなっている必要があります。個人データを取り扱わないこととなっている場合とは、契約条項によって当該クラウドサービス事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられます（個人情報保護委員会 Q&A5-33）。

クラウドサービス事業者がクラウドサービス事業者の独自の目的（広告利用、サービス改善、アルゴリズム強化等）で個人データを利用することが想定される場合には、個人データの第三者提供（個人情報保護法第 23 条 1 項）となり、利用方法の如何によっては児童生徒のプライバシー侵害となりうるので注意が必要です。

クラウドサービス事業者について委託先の監督義務を負わない場合でも、学校自身の安全管理措置として、適切なセキュリティレベルを有する事業者やサービスを選択することが求められます（個人情報保護法第 20 条）。

（2）著作権

クラウドサービスの利用にあたっては、クラウドサービス事業者が提供したドリル等について、ライセンスの範囲を超えて複製利用する場合など、著作権の侵害によるトラブルが起こる可能性があります。

著作権者に許諾を得るなど、法令の遵守に向け、あらかじめルールづくりや研修、情報モラル教育を行う等、教員と児童生徒それぞれに対し、適切な対応を図ることが重要です。

なお、音楽等の特定の教科については、取り扱っている題材そのものに著作権が存在しており、学校内のみでの保存が義務付けられているものもあります。

クラウドサービスの利用にともない著作権侵害の可能性がある状況（例）

共有の例	メリット	懸念される状況
他の教員が作成した教材を共有する	良い教材を取り入れたり、授業の準備を省力化したりすることが可能となる	勝手に改変して利用するなど、トラブルになるリスク
他の児童生徒が作成した成果物を見る	児童生徒による相互評価等が可能となる	他の児童生徒の成果物を盗用するリスク
インターネット上のコンテンツを活用して教材や成果物を作る	教材や成果物の内容が充実し、説得力が高まる	著作権者に許諾を得ずに利用するなど、トラブルとなるリスク

（3）肖像権

肖像権とは、自分の写真や絵の使用に関する権利のことを指し、例えば自分の写真や絵を承諾なしに公開されることを拒否することができます。

※出典：「国民のための情報セキュリティサイト」（総務省）

近年、ホームページ作成や保護者との連絡等を手軽に行えるようなクラウドサービスを利用する学校が増えています。修学旅行等の校外学習の際に児童生徒の様子をホームページにアップロードすることで、保護者にリアルタイムに子供の様子を伝えられたり、ＩＣＴを利用した授業の実践事例として、具体的な写真を校外に公開するような場合もあります。

このような場面で、児童生徒を特定し得る写真などを公開する場合には、個人情報保護に関する配慮だけではなく、肖像権への配慮も必要です。

参考6 クラウド活用効果検証例

（1）授業・学習系システムにおける効果検証例

授業・学習系システム導入による効果検証の例として、活用頻度と活用効果を確認する場合を示します。教職員等へのアンケート調査により傾向を確認する方法も考えられます。

観点としては、活用頻度（Input）と活用した結果としての効果（Output）があります。

①活用頻度の把握

（ア）誰が	どの教員が（who）
（イ）どのようなツールで	端末とコンテンツまたはアプリケーション（what）
（ウ）どこで（活用場面）	コンテンツの拡大提示 / タブレットによる個別学習 / タブレットを活用した協働学習等（where）
（エ）どのくらい使ったか（活用頻度）	毎日 / 週に数回 / 週に 1 回 / 月に数回 / 月に 1 回 / 使わない（How much）
（オ）利用を促進するうえでの課題	ツール不足 / ネットワークの帯域不足 / 教員のリテラシー不足 / 準備時間の不足等
（カ）利用しない理由（利用しない教員向け）	効果が期待できない / 活用スキルがない等

②活用効果の把握

（ア）誰が	どの教員が（who）
（イ）どのようなツールで	端末とコンテンツまたはアプリケーション（what）
（ウ）どこで（活用場面）	コンテンツの拡大提示 / タブレットによる個別学習 / タブレットを活用した協働学習等（where）
（エ）どのような効果を感じたか	興味関心の喚起 / 思考力の向上 / 表現力の向上 / コミュニケーションの活性化等（How much）

（2）校務系システムにおける効果検証例

統合型校務支援システム導入による効果検証の例として、教職員の校務負担軽減による時間削減効果を確認する場合を示します。

①目標設定

校務支援システムの導入においては、ツールが新しくなることに加え、校務にかかる運用ルールが自治体で統一され、これまでと校務処理が変更になるため、教職員が新しい校務運用に慣れるまでには一定の時間を要することから、導入 2 年目以降において効果検証を行うことが現実的です。

※具体的な削減目安時間については、「統合型校務支援システムの導入のための手引き」（文部科学省）1.3.1 章を参照ください。

②効果検証の考え方

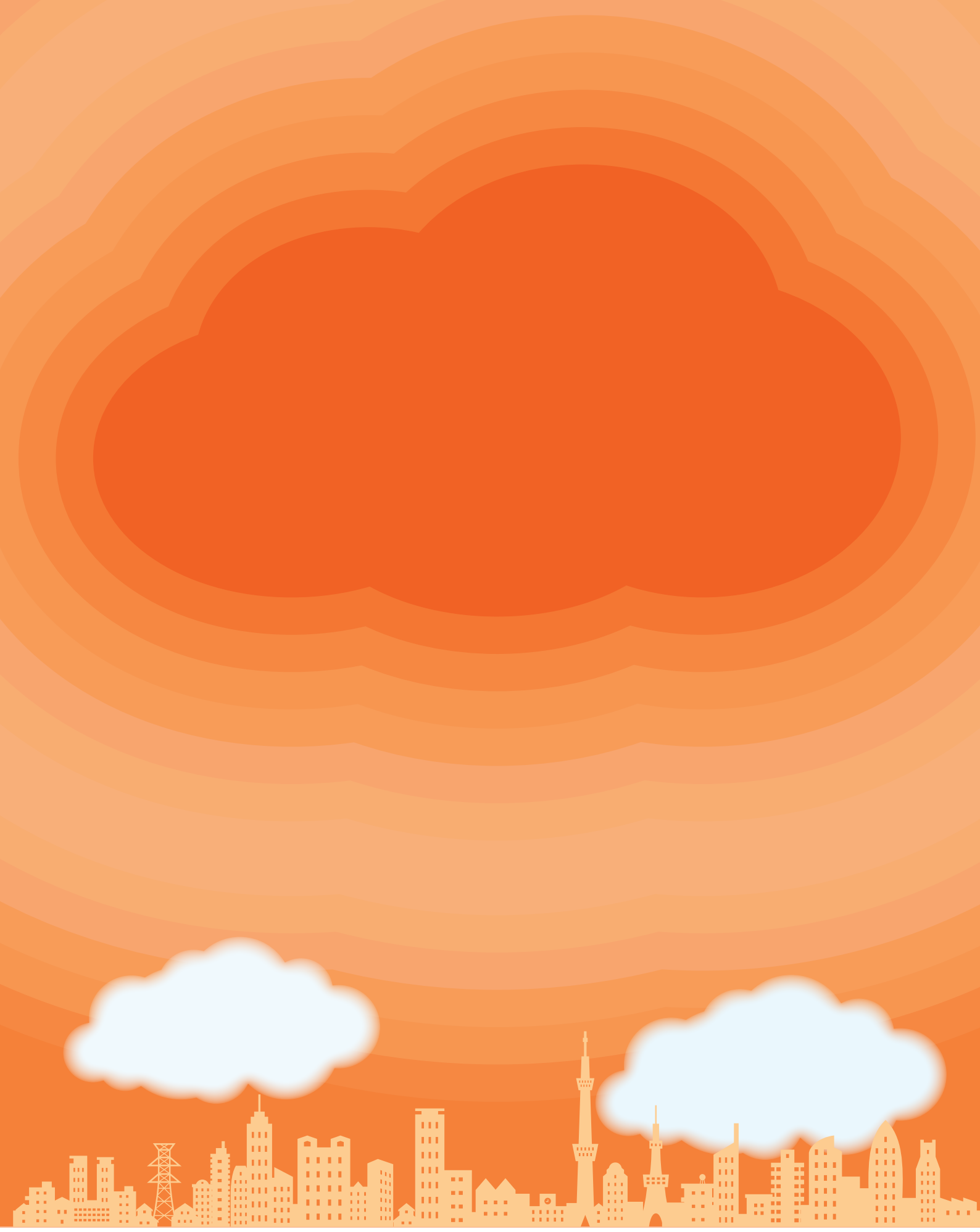
効果検証を検討するうえで、教職員への意識調査が考えられます。

例えば、校務負担の軽減による時間削減効果（量的）と負担感の削減（質的）の 2 つの観点から意識調査を行うことなどが考えられます。意識調査は、校務全般、統合型校務支援システムによる事務作業の省力化効果、グループウェアを導入する場合はコミュニケーション等の業務効率化効果の 3 つのカテゴリーで実施することなどが考えられます。

定量化の方法としては、例えば 5 択選択形式にて、○○になった（5 点）、やや○○になった（4 点）、変わらない（3 点）、やや○○にならない（2 点）、○○にならない（1 点）と点数づけを行うことなどが考えられます。その場合、「上位 2 択のポジティブ回答比率」「5 択回答の平均値」の 2 つの指標で定量化します。

校務負担軽減による時間削減に関する意識調査項目例

カテゴリー	校務項目	回答対象者	期待効果	設問の観点	
				量　的	質　的
全般	校務効率化	全員	時間削減	【週単位での時間削減の量】 30 分未満 /30 ～ 60 分未満 /60 ～ 90 分未満 /90 ～ 120 分未満 /120 ～ 150 分未満 /150 ～ 180 分未満 /180 ～ 210 分未満 /210 ～ 240 分未満 /240 分以上	【校務全般の感じ方】 負担感が減った / やや減った / 変わらない / やや増えた / 増えた
統合型校務支援システム関連	学籍管理	一般教員	稼働量減 / 負担感減	【稼働量】 稼働が減った / やや稼働が減った / 変わらない / やや稼働が増えた / 稼働が増えた	【負担感】 楽になった / やや楽になった / 変わらない / やや負担が増えた / 負担が増えた
	出欠管理	クラス担任	〃	〃	〃
	健康観察（毎朝） 健康観察集計表	養護教諭	〃	〃	〃
	成績処理	一般教員	〃	〃	〃
	成績一覧表作成	クラス担任	〃	〃	〃
	通信表作成	クラス担任	〃	〃	〃
	指導要録作成	クラス担任	〃	〃	v
グループウェア関連	会議時間・情報共有	全員	情報共有で会議時間を短縮	【情報共有による会議時間の変化】 会議の時間が減った / 変わらない 【週単位での時間削減の量】 10 分未満 /10 ～ 20 分未満 /20 ～ 30 分未満 /30 ～ 40 分未満 /40 ～ 50 分未満 /50 分以上	【会議時間が短縮された新しい情報共有形態について】 情報共有は強化された / やや強化された / 変わらない / やや低下した / 低下した
	紙媒体使用	全員	量の低減 / 負担感減	【紙使用の量】 変わらない /10% 未満 /10 ～ 20% 未満 /20 ～ 30% 未満 /30% 以上	【負担感】 コピー稼働が減って楽になった / やや楽になった / 変わらない / やや負担が増えた / 負担が増えた



【発行年】　2020 年 3 月
【発行元】　総務省 情報流通行政局 情報流通振興課 情報活用支援室
〒 100-8926 東京都千代田区霞が関 2-1-2　TEL：03-5253-5685　FAX：03-5253-5752
【総務省 教育の情報化推進ページ】　https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/index.html
【制作元】　エヌ・ティ・ティラーニングシステムズ株式会社