参考資料 3-2

平成 26 年度クラウド等の最先端情報通信技術を活用した学習・教育システムに関する実証別冊

学校情報管理ポリシーガイドブック(案)

2015 年 3 月

目 次

1. 本ガイドブックの位置づけ

学校情報管理ポリシーガイドブック（以下、本ガイドブックと記載）は、教育委員会や学校が、総務省が提供する教育・学習クラウドを活用する際に、情報セキュリティについて何を配慮すべきかを簡潔にまとめたものです。

本来であれば、教育・学習クラウドの活用が十分に進み、情報セキュリティ上の様々な課題が一通り出てきた段階で、各課題とその解決方法について整理して分かりやすく解説したものを本ガイドブックとすべきところですが、今年度は実証事業が開始されたばかりで、本格的な教育・学習クラウドの活用はこれからという状況であり、様々な課題を整理するにはもう少し時間がかかると思われます。

しかしながら、教育・学習クラウドの導入当初から出てきている大きな課題として、教育・学習クラウド利用時の情報セキュリティポリシーの変更の必要性と、各学校で実施される児童生徒の端末の持ち帰りと持込みにおけるセキュリティの配慮事項と情報セキュリティポリシーの変更の必要性が出てきており、これらは、今後、教育・学習クラウドを活用する予定がある教育員会や学校が必ず直面する課題であることから、これらの課題に絞って、どのように対応すべきかのノウハウを整理することは非常に有意義であると考えました。

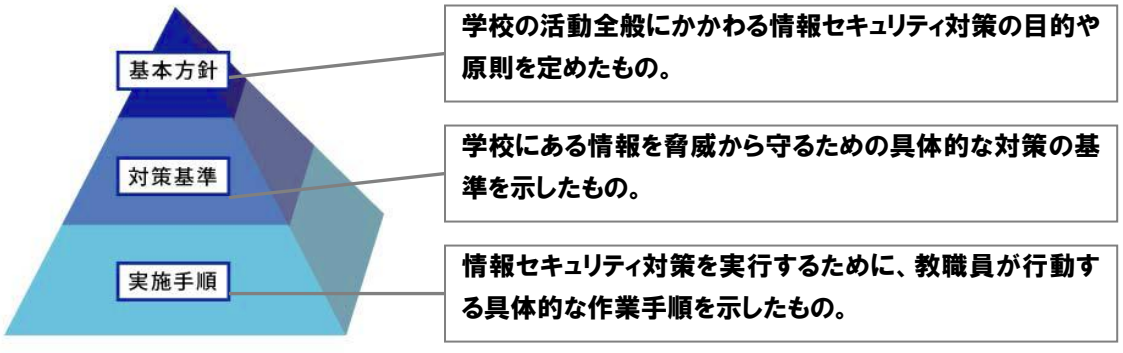
そこで、本ガイドブックでは、これらの 2 点に的を絞り、今後、教育・学習クラウドを導入する教育委員会や学校が課題に直面したときにどのように解決を図るかを検討する際の参考になるようにノウハウを整理してまとめました。

なお、本ガイドブックの作成にあたっては、実証地域の教育委員会にヒアリングを実施した内容を元にしてガイドブックの作成を行ったため、必ずしも全ての教育委員会や学校で参考となる内容にはなっていない箇所もあります。本事業で別途作成した情報セキュリティポリシーガイドラインでは、より幅広い教育委員会や学校の参考になるようにガイドラインを作成していますので、そちらも合わせてご参照いただければ、より一層、教育・学習クラウド導入時の情報セキュリティにおける配慮事項への理解が深まることが期待されます。

2. 情報セキュリティポリシーの概要と用語の定義

2.1 情報セキュリティポリシーの概要

一般的に、情報セキュリティポリシーは、「基本方針」「対策基準」「実施手順」の 3 つから構成されます。「基本方針」「対策基準」「実施手順」の概要は以下の通りです。



情報セキュリティポリシーの概要（出典:「教育の情報化に関する手引」（文部科学省））

「基本方針」「対策基準」の記載項目については、決まったものはありませんが、「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」（総務省）の項目例に従うことが一般的です。なお、教育・学習クラウドの導入及び児童生徒の端末の持ち帰り・持ち込みの実施に伴い、「基本方針」「対策基準」で変更の可能性がある項目は以下の下線の箇所です。

＜情報セキュリティポリシー基本方針の項目例＞

1 目的
2 定義
3 対象とする脅威
4 適用範囲
5 教職員等の遵守義務
6 情報セキュリティ対策
7 情報セキュリティ監査及び自己点検の実施
8 情報セキュリティポリシーの見直し
9 情報セキュリティ対策基準の策定
10 情報セキュリティ実施手順の策定

＜情報セキュリティポリシー対策基準の項目例＞

1 対象範囲
2 組織体制
3 情報資産の分類と管理方法
4 物理的セキュリティ
5 人的セキュリティ
6 技術的セキュリティ
7 運用
8 評価・見直

また、実施手順につきましては、各自治体や教育委員会が独自に作成しており、特に一般的な記載の様式はありませんが、記載項目の一例として「学校における情報セキュリティについて」（文部科学省）の記載されている実施手順における主な記載事項と、実施手順の項目の中で変更の可能性がある項目を下線で示します。

＜情報セキュリティポリシー実施手順の項目例＞

１ 目的
２ 適用者
３ 用語の定義
４ 管理体制
５ 情報区分
６ 日常の留意事項
７ ネットワークの利用・管理
８ 緊急時及び障害発生時の対応
９ 情報セキュリティ研修等

（出典:「学校における情報セキュリティについて」（文部科学省））

なお、「基本方針」「対策基準」「実施手順」の各項目の詳細な記載方法については、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）及び「学校における情報セキュリティについて」（文部科学省）をご覧ください。

2.2 用語の定義

本ガイドブックで出てくる用語のうち、定義が曖昧なもの、分かりにくいものについて以下で説明します。

① 個人情報

一般的には、学校における個人情報は、生存する教職員、児童・生徒、保護者に関する情報で、その情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別できるものを指しますが、本ガイドブックでは、その中の児童・生徒の学習履歴に関連する個人情報を個人情報と記載します。

② 教育・学習クラウド

平成 26 年度クラウド等の最先端情報通信技術を活用した学習・教育システムに関する実証事業（総務省）にて各学校に提供されているクラウド環境を指します。

③ プライベートクラウド

自治体又は教育委員会、学校法人などが自らクラウドの環境を構築して、配下の学校等に対してサービスを提供する形態のクラウドを指します。

3. 教育・学習クラウド利用に際するセキュリティ上の留意事項

3.1 教育・学習クラウドを利用する際の情報セキュリティポリシーの変更

教育・学習クラウドを利用する場合に、教育委員会及び学校向けの既存の情報セキュリティポリシーを変更するか否かについては、教育・学習クラウドをどのように使うのか、教育委員会の所有しているクラウド環境がどのようになっているのか、によって異なってきます。

教育・学習クラウドの活用方法	教育委員会の既存のクラウド環境	情報セキュリティポリシーの変更必要性の有無
教材、学習履歴などの個人情報を含まない情報のみ保管	個人情報を含む校務情報を既存のプライベートクラウド環境で保管している	既存のプライベートクラウド上に個人情報を保管するように情報セキュリティポリシーが作成されているため、**情報セキュリティポリシーの変更は必要ない。**
	既存のクラウド環境は存在しない	教育・学習クラウドでは個人情報を活用せずに利用するため、情報セキュリティポリシーの変更は必要ない場合が多いが、**クラウドを活用することに関連してポリシーへの追記が必要になる場合がある。**
教材、学習履歴だけでなく個人情報を含む情報も保管	個人情報を含む校務情報を既存のプライベートクラウド環境で保管している	既存のクラウド環境とは異なる新たなクラウド環境に個人情報を保管するため、**情報セキュリティポリシーの変更が必要となる。**
	既存のクラウド環境は存在しない	クラウド環境に個人情報を保管することが想定されていない情報セキュリティポリシーとなっているため、**個人情報をクラウドでどのように扱うかのマンも含めて情報セキュリティポリシーの大幅な変更が必要となる。**

自治体又は教育委員会が所有する既存のプライベートクラウド環境上で個人情報を含む校務情報を扱っている場合は、情報セキュリティポリシーの変更を伴わずに教育・学習クラウドを活用できますが、既存のプライベートクラウドがない場合は、情報セキュリティポリシーの変更を行う必要があります。

教育委員会では、自治体の情報セキュリティポリシーを流用している場合が多いこと、自治体の情報セキュリティポリシーによる様々な縛りが発生する場合があること（例：自治体の外にはサーバを設置できない、無線 LAN の利用は禁止など）、情報セキュリティポリシーの作成や変更を教育委員会のみで実施することは困難であること、などから、教育・学習クラウドを導入する際は、自治体の情報政策関連の部署と密に連携をしながら進めることが望ましいです。

ポイント

＜教育・学習クラウドを利用する際の情報セキュリティポリシーの変更＞

- 自治体又は教育委員会が所有する既存のプライベートクラウド環境上で個人情報を含む校務情報を扱っている場合は、情報セキュリティポリシーの変更を伴わない、教育・学習クラウドと既存のプライベートクラウドを連携させる方法が最もスムーズに教育・学習クラウドを活用できる方法です。

- 既存のプライベートクラウドがない場合は、クラウド環境でどのような情報をどのように扱うかを明確にした上で、情報セキュリティポリシーの変更を行う必要があります。

- 教育・学習クラウドの導入の際は、自治体の情報政策関連の部署と密に連携をしながら進めることが望ましいです。

コラム

- セキュリティポリシーでは、教育委員会や学校で扱っている情報を重要度に応じて 3～5 の分類（情報区分）に分けていることが一般的です。この情報区分ごとに、どのように情報を取り扱うか（例：校外への持ち出しは禁止）を定めています。

- セキュリティポリシー上では、情報を保管する媒体の扱いについて必ずしも記載されているとは限りません。情報区分ごとにどの媒体で情報を扱えるかを記載することは理想的ではありますが、ポリシーの見直しが頻繁に必要となる可能性が高くなります。例えば、プライベートクラウドは校内と同様と定義することによって、「校外への持ち出しは禁止」に当たらないと解釈する方法もあります。

3.2　クラウド間連携

3.1 で既に説明した通り、自治体又は教育委員会が所有するクラウドが既にある場合は、教育・学習クラウド上では個人情報を扱わないことで、情報セキュリティポリシーの変更なしに教育・学習クラウドを利用することが可能となります。この場合は、既存クラウドと教育・学習クラウドを連携させ、学習履歴等の情報を個人と紐付けることによって活用する必要があります。

具体的な方法の一つとして、個人を特定できない関連付けのための情報を、既存クラウドと教育・学習クラウドの両者で保有する方法があります。こうすることによって、教育・学習クラウドの情報のみを見ただけでは、どれが誰の情報かが特定できませんが、既存クラウド側で関連付け情報を介して個人を特定することによって、学習履歴などの情報を利活用することが可能となります。

このように、教育・学習クラウドだけを見ただけでは個人を特定できず、既存クラウドと連携することによって個人を特定できるような何らかの方法を用いることで、情報セキュリティポリシーの変更なしにスムーズに教育・学習クラウドを利用することが可能となります。

ポイント

＜クラウド間連携を行う場合のポイント＞

- 自治体又は教育委員会が所有するクラウドが既にある場合は、教育・学習クラウド上では個人情報を扱わないかたちでクラウド間で情報を連携させ、情報セキュリティポリシーの変更なしにスムーズに教育・学習クラウドを利用することが可能となります。

- クラウド間連携を実現するには、個人を特定できない関連付けのための情報を、既存クラウドと教育・学習クラウドの両者で保有して、既存クラウド側で個人情報との紐付けを行うことで情報の利活用を行う必要があります。

4. 児童生徒の端末の持ち帰り、持込みでのセキュリティ上の留意事項

4.1 児童生徒の端末の持ち帰りの際のセキュリティ上の留意事項

児童生徒の端末の持ち帰りについては、テスト前や長期休み期間中など、学習効果が期待できる時期に限定的に実施されています。しかしながら、端末の持ち帰りを実施する際の課題は多く、気軽に持ち帰りを実施できていないのが実情です。児童生徒の端末の持ち帰りを実施する際のセキュリティ上の課題は以下の通りです。

- **様々なネットワーク環境が存在する児童生徒の家庭にて、専門知識なしに持ち帰り端末を簡単かつ安全に接続できる環境をどのように提供するか**
- **自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか**
- **端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか**

各課題に対する対応は各実証地域の学校にて試行錯誤しながら実施しているところで、今後の技術の進歩によって新たな対応方法が出てくる可能性もありますが、現時点で、一定の効果が得られている対応策は以下の通りです。

① 様々なネットワーク環境が存在する児童生徒の家庭にて、専門知識なしに持ち帰り端末を簡単かつ安全に接続できる環境をどのように提供するか

児童生徒の家庭でのネットワーク接続環境については、千差万別の環境が存在していることが想定されることから、端末側の設定のみで簡単かつ安全な接続に対応することは容易ではないと考えられます。そこで、モバイルルータも合わせて持ち帰らせることで、ネットワークへの接続も学校側で制御できるようにすることが効果的な対応策です。

なお、ネットワーク環境が存在しない児童生徒の家庭も一定割合で存在することから、家庭環境の違いを児童生徒に感じさせずに済む効果もあります。

② 自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか

端末に、児童生徒が閲覧することが好ましくないサイトへのアクセスをブロックするフィルタリングソフトウェアを導入し、自宅で児童生徒がインターネットを閲覧する際に、全てのサイトに自由にアクセスすることを防ぐことができます。なお、①でモバイルルータを導入した場合は、フィルタリングの機能を持ったモバイルルータを導入すれば、新たにソフトウェアを導入する必要がなくなります。

③ 端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか

児童生徒が端末を持ち帰る際に、端末上の個人情報等を削除し、教材やドリルなどを保存した持ち帰り専用の環境に入れ替えた上で児童生徒に渡し、端末を持ち帰り後に学校に持っ

てきた際には、校内で利用する環境を復元する運用を行うことで、万が一、児童生徒が端末を紛失したり盗難にあったりした場合でも、個人情報等の重要度の高い情報の流出を防ぐことができます。

ポイント

＜児童生徒の端末の持ち帰りの際のセキュリティ上の留意事項＞

- 児童生徒が端末を持ち帰る際は、家庭でのネットワーク接続とインターネットの閲覧について、学校側で制御が行える環境を提供する必要があります。
- 端末上に個人情報が存在する場合は、持ち帰り時の端末設定と学校内での端末設定の内容を入れ替えることで、情報漏えいを防ぐことができます。
- 新たな技術の出現によって対応策が変わってくるため、定期的にベンダーなどから情報収集を行い、新たな対応策の導入について検討を行うことが必要です。

コラム

- 端末環境の入れ替えは、毎回、手動で運用を行っていると大変であることから、専用のツールなどで自動化を図ることも合わせて検討する必要があります。

4.2　児童生徒の端末の持込みの際のセキュリティ上の留意事項

児童生徒の端末の持込みについては、児童生徒が購入した端末を学校の授業で活用することから、常時、持込みが行われることになります。また、家庭のネットワーク環境からインターネットの閲覧は許しており、インターネット経由で佐賀県がクラウドにて提供している学習系コンテンツにもアクセスすることができます。しかし、児童生徒が家庭にあるさまざまな端末を自由に持ち込むものではなく、備品として児童生徒が自ら購入した端末を持ち込んでいる関係で端末は全て同機種であり、会社等で一般的に行われている個人端末の持込みとは特徴が異なっています。こうした環境での児童生徒の端末の持込みを実施する際のセキュリティ上の課題は以下の通りです。

- **児童生徒の端末を校内ネットワークに安全に接続する環境をどのように提供するのか**
- **自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか**
- **端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか**

各課題に対する対応は各学校にて試行錯誤しながら実施しているところで、今後の技術の進歩によって新たな対応方法が出てくる可能性もありますが、現時点で、一定の効果が得られている対応策は以下の通りです。

①　児童生徒の端末を校内ネットワークに安全に接続する環境をどのように提供するのか

児童生徒が購入した端末を受け取る前に、学校側で環境設定などを行い、端末の機能に制御をかけることで、児童生徒が備品として購入した端末のみしか校内ネットワークに接続できず、更に、接続後も学習系ネットワークのみに接続が可能で、校務系のネットワークには接続ができないように制御が可能となります。また、アプリケーションのインストールを禁止し、事前の環境設定でウィルス対策ソフトの設定を行うことで、児童生徒の端末が家庭のネットワーク環境でウィスルに感染するのを防ぐことが可能となります。

②　自宅で児童生徒が安全にインターネットに繋げられる環境をどのように提供するか

学校側の事前の環境設定の際に、端末に、児童生徒が閲覧することが好ましくないサイトへのアクセスをブロックするフィルタリングソフトウェアを導入し、自宅で児童生徒がインターネットを閲覧する際に、全てのサイトに自由にアクセスすることを防ぐことができます。

③　端末の盗難、紛失時に重要度の高い情報の流出をどのように防ぐのか

学校側の事前の環境設定の際に、端末管理ツールを導入して、管理サーバよりリモートにて端末を管理し、第三者による端末操作を防止することで、端末の盗難・紛失時の情報漏えいを防止できます。更に、端末内の情報を暗号化することで、情報漏えいの防止を強化できます。

ポイント

＜児童生徒の端末の持ち込の際のセキュリティ上の留意事項＞

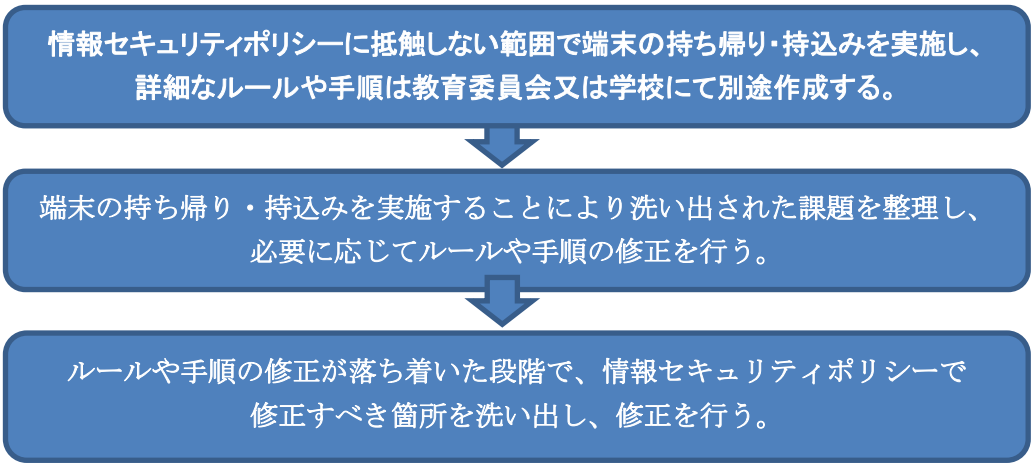
- 児童生徒に端末を渡す前に、端末に対してセキュリティ上の各種設定を施すこと、アプリケーションのインストールを禁止することなど、学校側で端末の制御がある程度行えるようにする必要があります。
- 端末上に情報の漏えいの防止は、端末のリモート管理と端末上の情報の暗号化の 2 つの技術的対策を施すことで、情報漏えいを防ぐことができます。
- 新たな技術の出現によって対応策が変わってくるため、定期的にベンダーなどから情報収集を行い、新たな対応策の導入について検討を行うことが必要です。

コラム

- 児童生徒が所有する端末であるにも関わらず、学校側で様々な制限を設けていることについては、保護者の理解が必須となります。保護者へのパンフレットの配布、説明会の開催など、理解を得られるように様々な周知活動を行うことが重要です。
- 端末を児童生徒が購入することに関しては、義務教育ではない高校では、教科書を児童生徒が購入しているなど、備品の購入に関して理解が得られやすい環境であることから、小中学校よりは導入が容易であるかもしれません。

4.3　児童生徒の端末の持ち帰り・持込みの実施による情報セキュリティポリシーの変更

児童生徒の端末の持ち帰り、持込みについては、これまでに学校で行われていた情報端末の活用とは大きく異なり、学校の情報機器を校外に持ち出す、学校の情報機器でないものを校内に持ち込むという情報機器の校内校外の移動が頻繁に発生することから、校内に固定された情報端末の扱いを前提とした既存の情報セキュリティポリシーでは対応が難しくなってきています。しかしながら、情報セキュリティポリシーの変更には時間がかかることから、当面の対応として以下のような手順で進めながら、将来的には、情報セキュリティポリシーを改定することが望ましいです。



ポイント

＜児童生徒の端末の持ち帰り・持込みの実施による情報セキュリティポリシーの変更＞

- 児童生徒の端末の持ち帰り、持込みは、これまでの情報セキュリティポリシーでは対応できない可能性が高く、変更に向けた検討が必要です。
- 児童生徒の端末の持ち帰り、持込みについては、当面は情報セキュリティポリシーに抵触しない範囲内で実施し、詳細にルール等については別途作成して周知します。
- 児童生徒の端末の持ち帰り、持込みで明らかになった課題を整理し、その結果を反映するかたちで情報セキュリティポリシーの変更を行います。