教育分野におけるクラウド導入に対応する

情報セキュリティに関する手続きガイドブック

総務省
Ministry of Internal Affairs and Communications

― 目次 ―

はじめに

① 本ガイドブックの背景

教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック（以下、「本ガイドブック」）は、総務省「クラウド導入ガイドブック２０１６」（以下、「導入ガイドブック」）の別冊版として、主に情報セキュリティに関する手続きについてまとめたものです。

本ガイドブックは、クラウドを中心とした ICT 環境を導入する際の情報セキュリティに関する手続き上の留意点等を整理しています。

なお、本ガイドブックの内容については、最新の情報を総務省ホームページ「教育情報化の推進」に追加掲載していきますので、適宜ご参照ください。

http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/sendou.html

本ガイドブックの作成にあたっては以下を参照しています。

本ガイドブック作成にあたっての参照資料

名称	発行元※	発行年月
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[1]	総務省	平成 27 年　3 月
地方公共団体における情報資産のリスク分析・評価に関する手引き[2]	総務省	平成 21 年　3 月
学校情報セキュリティ・ハンドブック ～今日から始められるセキュリティポリシーの作り方～	財団法人コンピュータ教育開発センター	平成 19 年　3 月
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[3]	財団法人コンピュータ教育開発センター	平成 20 年　3 月
政府機関の情報セキュリティ対策のための統一基準（平成２６年度版）[4]	内閣官房情報セキュリティセンター	平成 26 年　5 月
新たな自治体情報セキュリティ対策の抜本的強化に向けて[5]	総務省	平成 27 年 11 月
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）2014（中学校・特別支援学校版）[6]	総務省	平成 26 年　4 月
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　セキュリティ要件ガイドブック[7]	総務省	平成 27 年　3 月

※発行元の名称は発行時の名称

[1] http://www.soumu.go.jp/denshijiti/jyouhou_policy/
[2] http://www.soumu.go.jp/main_content/000013970.pdf
[3] http://www.cec.or.jp/seculib/handbook/kaisekai.pdf
[4] http://www.nisc.go.jp/active/general/pdf/kihan26.pdf
[5] http://www.soumu.go.jp/main_content/000387560.pdf
[6] http://www.soumu.go.jp/main_content/000285283.pdf
[7] http://www.soumu.go.jp/main_content/000372875.pdf

学校においてクラウドサービスを導入するにあたっては、従来、各自治体が所有するサーバーに保存していた個人情報等を、クラウドサービス事業者のサーバーに置くことになるため、個人情報保護条例や情報セキュリティポリシー等、既存の法令や規定との整合性をとる必要があります。本ガイドブックでは、それらの法令や規定と整合性をとりながら、クラウドサービスの活用を進めるための手順について記載します。

② 本ガイドブックで取り扱う課題

本ガイドブックの作成にあたり、全国の都道府県及び市区町村教育委員会にアンケート調査を実施しました[8]。

その調査結果によると、各自治体が「個人情報」と「自治体のネットワークや情報セキュリティポリシーとの整合性」について課題に感じていることがわかりました。

本ガイドブックは、自治体が抱える以下のような課題に対し解決のヒントとなる情報を提示することを目的としています。

（a）クラウドで個人情報を扱うにはどうしたらよいか？

各自治体の個人情報保護条例や情報セキュリティポリシー等に照らして、サービス利用可否の検討や、必要な手続きを確認する必要があります。

先行自治体へのヒアリングでは、「児童生徒が利用するクラウドサービスには個人情報を含めないようにして、個人情報保護条例が利用の妨げとならないようにする」という回答が多く見られました。

ただし、校務に関しては機微情報が含まれるため、いずれの自治体も慎重に手続きを進めています。個人情報保護審査会への付議など必要な手続きを経るという回答の他、パブリッククラウドではなくプライベートクラウドに保存するという回答も多く見られました。

詳細は第２章を参照してください。

（b）自治体ネットワークとの整合性はどう考えるとよいか？

各自治体がネットワークの強靭化に向けた検討を始めています。

先行自治体へのヒアリングでは、学校ネットワークについては、引き続き学校に特化したネットワークで情報セキュリティ対策も含め進めていくとしている場合と、いずれ自治体のネットワークに集約化していきたいとしている場合に分かれました。

いずれにせよ、自治体ネットワークの在り方については首長部局で検討途中という場合が多く、今後の動向に注意する必要があります。

詳細は第２章を参照してください。

[8] 紙媒体でアンケート調査を実施し、計 849 件の回答を得ました（回収率 47.6%）。

（c）自治体の情報セキュリティポリシーが厳格で、ICT 活用の障壁とならないか？

先行自治体では、特に児童生徒が使う学習系ネットワークに関し、ネットワークが独立していたり、取り扱う情報資産が行政系とは大きく異なっていたりしたため、教育委員会にある程度の権限が委譲されていたり、教育委員会で行政部局と独立した情報セキュリティポリシーを持っていたりする場合が多くありました。

詳細は第２章で示しますが、クラウドを中心とした ICT 環境の構築に伴い、活用とセキュリティとのバランスを図る等の観点から情報セキュリティポリシーの改定を行った自治体も多くあります。

③ 情報収集の重要性

情報セキュリティを巡る状況は、刻々と変化しています。情報セキュリティに関するトラブルのニュースも後を絶ちません。「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成２７年９月成立）」等、法令への対応も必要となります。クラウドサービスの導入を行う等、教育委員会や学校における情報システムに変化があった場合にも、とるべき情報セキュリティ対策は変わってきます。

このため、日頃からニュース等で情報セキュリティに関する最新情報を収集して危機に備えたり、時代に合うよう情報セキュリティポリシーの見直しを行ったりしていくことが重要です。関連する Web サイトを、以下に紹介しますので、適宜ご活用ください。なお、これらを参考に資料を作成する場合は、情報の出所を明記する等、著作権に注意してください。

- 内閣サイバーセキュリティセンター（NISC）
  http://www.nisc.go.jp/
- 独立行政法人情報処理推進機構（IPA）　情報セキュリティ
  https://www.ipa.go.jp/security/
- 警察庁　サイバー犯罪対策
  https://www.npa.go.jp/cyber/
- 一般社団法人 JPCERT コーディネーションセンター
  http://www.jpcert.or.jp/

第１章　クラウド導入のプロセスと情報セキュリティに係る手続き

1.1 調達の各プロセスと情報セキュリティに関する手続きの関係

クラウドを中心とした ICT 環境調達のための流れは大きく「準備段階」→「計画段階」→「調達段階」→「運用段階」の４段階に分かれます。

調達における各段階

本ガイドブックでは、次章以降これらの各段階における情報セキュリティに関する手続きについて記載します。情報セキュリティに関する手続きについて、以下に各段階及びプロセスのポイントを示します。

各段階及びプロセスにおける情報セキュリティに関する手続きのポイント

段階	プロセス	ポイント
1.準備段階	情報収集	・導入を想定するクラウドサービス上で取り扱う情報資産の想定 ・個人情報保護と情報セキュリティポリシーについて順守すべき規定等の確認 ・自治体のネットワークポリシーの確認
2.計画段階	ICT 環境の検討	・取り扱う情報資産を洗い出し、個人情報保護や、その他取り扱う情報資産に応じた手続きを実施 ・ICT 機器やネットワーク、クラウドサービスの情報セキュリティ上の要件について、情報セキュリティポリシーや自治体のネットワークポリシーと整合性をとれるよう検討
	仕様作成	・調達仕様の作成における情報セキュリティ要件の盛り込み
3.調達段階	整備	・適切な情報セキュリティ対策が施されているかの確認
4.運用段階	運用（活用）	・情報セキュリティに関するルールやマニュアルの見直し・周知 ・情報セキュリティ対策の実施状況、ルール順守状況の定期的な確認 ・インシデント発生時の対応、緊急時対応、再発防止策の検討

教育委員会や学校は、児童生徒の成績情報やその他の機微情報など、様々な情報を保有しています。クラウドサービスを利用するにあたっては、情報をクラウドサービス事業者のサーバー上に置くこととなる場合があります。そのため、クラウド上で利用するデータ（情報資産）を具体的に想定し、個人情報保護条例や情報セキュリティポリシー、自治体のネットワークポリシーに照らして、サービス利用可否の検討や必要な手続きを踏む必要があります。

第2章　情報セキュリティ手続きにおける「準備段階」の留意点

準備段階では、クラウドを中心としたICT環境の導入に向けた情報収集を主に行います。

2.1 教育用コンテンツに関する情報収集

準備段階では、導入の候補となる教育用コンテンツの情報収集を行うこととなりますが、その際、機能面だけではなく、当該コンテンツを活用するうえでどのような情報を登録する必要があるのかも確認します。セキュリティに関する既存の法令や規定との整合性を検討するうえで、教育用コンテンツ上で扱う情報について具体的に想定できている必要があります。

例えば、ある教育用コンテンツでユーザー登録に必要な情報は以下のとおりです。このような登録情報は、教育用コンテンツにより異なります。

教育用コンテンツでのユーザー登録に必要な項目例

分類	登録項目
教員用アカウント	姓・名
	学年・クラス
	eメールアドレス
	ユーザー名
	パスワード
児童生徒用アカウント	姓・名
	学年・クラス
	パスワード

また、登録時以外にも、教育用コンテンツの活用を進めるうえで、以下のような情報が事業者のサーバー上に保存される可能性があります。

教育用コンテンツ利用中に保存される可能性がある情報例

情報	説明
成績情報	・問題への解答した結果の履歴が、成績情報のような形で保存される場合がある。
個人情報	・ユーザー情報を登録しなかった場合でも、児童生徒の書き込みにより保存される場合がある。 ・写真を登録する場合、顔が写りこむ場合がある。
その他の情報	・児童生徒の思想・信条に関する情報等が保存される場合がある。

さらに、これらの情報は、利用者である教育委員会や学校、児童生徒自身が利用する場合の他、クラウドサービス事業者が自社のサービスの利用傾向を知る等の目的で利用する場合も想定されます。クラウドサービス事業者が情報をどのように扱い、どのような目的で利用することがあり得るのかもあわせて確認します。

2.2 法令やポリシーに関する情報収集

クラウドサービスを利用するにあたり、個人情報保護に関する法令と、情報セキュリティポリシーについて確認する必要があります。また、自治体のネットワークに関するポリシーとの整合性についても検討が必要になります。

本節では、クラウドサービス導入の準備段階として、それらの法令等を確認するポイントについて記載します。

（1）個人情報保護に関する法令

教育委員会や学校においては、保護者や児童生徒等の個人情報を取り扱う観点で、個人情報保護条例の対象となり得ます。また、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等、条例等で定められた手続きを経る必要があります。準備段階での確認の観点例を以下に示します。

個人情報保護に関する法令確認の観点例

項目	確認内容
a）適用される法令	・適用される個人情報保護条例はどのような内容か（条文を入手）。
b）取り扱うための手続き	・個人情報保護審査会等、どこに対し、どの段階で、どのような手続きを行うことになっているか。

a）適用される法令の確認

個人情報に関する法体系としては、まず個人情報保護委員会の所管する「個人情報の保護に関する法律（個人情報保護法）（平成２７年９月改正）」が前提となっています。

「個人情報保護法」は、基本理念や国及び地方公共団体の責務・個人情報保護施策等に関する基本方針の部分（１～３章）と、民間の事業者における個人情報の取り扱いのルールを定めた部分（４章～７章）から成り、クラウドサービス事業者や、私立学校を設置する学校法人等の民間事業者にはこの法律が適用されます。また、公立学校には当該学校を設置する自治体の個人情報保護条例[9]が、国立大学法人等が設置する学校には「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」が適用されます。

b）個人情報を取り扱うための手続きに関する確認

個人情報保護条例の中には、個人情報を取り扱う場合の手続きが義務づけられている場合が多くあります。個人情報保護審査会や、首長または特定部局への届け出や承認を求められる場合があるため、それら手続きの方法について確認しておきます。

[9] 個人情報保護条例の中には、公的分野における個人情報の取り扱いに関する各種規定に加え、事業者の一般的責務等に関する規定や、地方公共団体の施策への協力に関する規定等を設けている場合もあります。

（2）情報セキュリティポリシーの確認

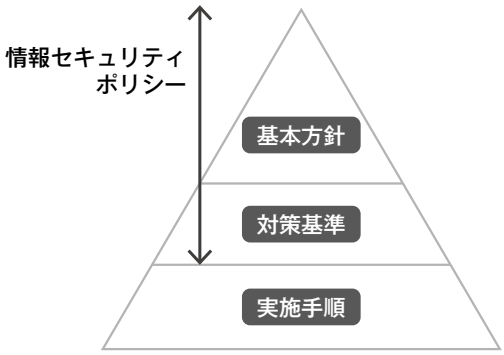
クラウドサービスを利用するにあたっては、情報セキュリティポリシーとの整合性も重要となります。そのため、準拠すべき情報セキュリティポリシーについても、準備段階で確認しておきます。確認の観点は、導入しようとするクラウドサービスによって異なりますが、以下に例を示します。

情報セキュリティポリシー確認の観点例

項目	確認内容
a）準拠するポリシー	・教育委員会や学校が準拠すべき情報セキュリティポリシーは存在するか。 ・教育委員会や学校の権限範囲はどのようになっているか。 ・「実施手順」の追加策定等、個別に求められる項目はあるか。
b）体制	・情報セキュリティに関する推進体制や権限範囲はどのようになっているか。
c）ポリシーの想定	・対象は教職員のみか、児童生徒等も含むか。 ・無線 LAN が敷設可能か、可搬端末（タブレット等）の利用が想定されているか。 ・クラウドサービスの利用が想定されているか。想定されている場合、校務系/学習系いずれが想定されているか。
d）情報資産（データ）の取り扱い	・情報の区分（重要度等）や管理手続きはどのようになっているか。 ・区分に応じて必要な手続きがあるか。 例）条例で定められた個人情報保護審査会、保存場所や件数の申請　等

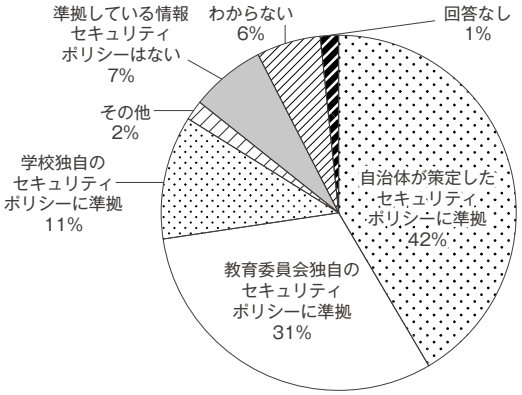
a）準拠する情報セキュリティポリシーの確認

情報セキュリティポリシーは、一般に、情報セキュリティに対する基本的な考え方を定める「基本方針」、基本方針に基づいて情報セキュリティ対策の基準を定める「対策基準」から構成されます。また、「対策基準」を満たすための具体的な運用手順等を定めた「実施手順」が別途あります。



教育委員会や学校においては、自治体の情報セキュリティポリシーに準拠し実施手順のみを策定する場合の他、教育委員会が主体となって所管の学校まで含めた情報セキュリティポリシーと実施手順を策定する場合等が考えられます。まずは、自治体の情報セキュリティポリシーを所管する部局（情報政策課等）に相談し、準拠すべき情報セキュリティポリシーを確認します。

なお、前述のアンケート調査では、学校が準拠している情報セキュリティポリシーについて「自治体が策定したセキュリティポリシーに準拠している。」という回答が最も多く（42%）、次いで「教育委員会独自のセキュリティポリシーに準拠している。」（31%）となっていました。



学校が準拠している情報セキュリティポリシー

また、情報セキュリティポリシー（「基本方針」「対策基準」）が既に定められている場合でも、クラウドサービス等の追加のシステムを導入する場合には、個別に「実施手順」や「管理規定」等の詳細を策定することが求められる場合もあります。そのため、教育委員会や学校が追加で手順等を策定する必要があるかをあわせて確認しておきます。

【事例　佐賀県立中原特別支援学校】

ICT の活用に関する委員会が、情報セキュリティポリシーとの整合性をとりながら推進

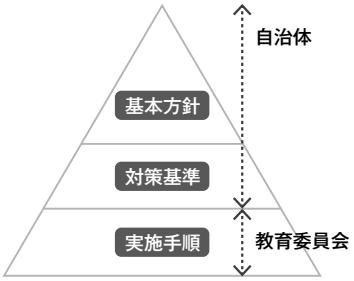
佐賀県では、県の情報セキュリティポリシーに基づき、各学校で実施手順および実施マニュアルを作成することになっています。中原特別支援学校では、「情報教育部」を組織して、実施手順・実施マニュアルの策定や見直しを行っています。情報教育部は、特別支援教育領域（病弱、肢体不自由、知的）、小学部・中学部の各教員が参加して主に ICT の活用推進を行う組織ですが、あわせて情報セキュリティに関する活動も行うことで、ルールと活用の整合性をとりながらクラウドの活用を進めています。

【事例　札幌市教育委員会】

札幌市の情報セキュリティポリシーに基づき、クラウドサービス毎に「ガイドライン」と「利用手順」を作成

札幌市教育委員会では、モデル校でクラウドサービスを活用していますが、情報セキュリティポリシーに関する進め方について細かく検証しています。クラウドサービスの導入毎に、機能や取り扱う情報、運用体制等を定める「ガイドライン」と、学校長や教頭、利用者の責任範囲や情報セキュリティ対策を定める「利用手順」を作成しています。目次例は以下です。

アプリケーションＡを利用した情報共有に関するガイドライン
1．本ガイドラインの目的
2．情報共有の定義
3．アプリケーションＡの利用にあたっての基本原則
4．利用する機能について
5．取り扱う情報について
6．運用体制について
7．効果の検証等について



アプリケーションＡ利用手順
1．目的および適用範囲
2．実施体制と責務
3．情報資産の特定
4．人的セキュリティ対策
5．情報セキュリティ対策の遵守義務
6．技術面及び運用面における情報セキュリティ対策

b）体制の確認

情報セキュリティポリシーでは、情報セキュリティ対策を推進するための体制が定められています。

「政府機関の情報セキュリティ対策のための統一基準（平成２６年度版）[10]」においては、情報セキュリティに対する統一的な窓口として、専門的な知識や適正を有するものを含むCSIRT[11]の設置が必要とされています。そのようなチームの有無や、誰がどのような責任や権限を持っているのか確認しておく必要があります。

次頁に情報セキュリティ対策における関係者の役割例を示します。

[10] http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf

[11] Computer Security Incident Response Team の略で、情報セキュリティインシデントに対応するための専門チームのことです。

情報セキュリティ対策推進のための役割例

名称	役割
最高情報セキュリティ責任者（CISO[12]）	CSIRT の責任者であり、情報セキュリティの推進体制が機能するよう管理する。情報資産の管理や情報セキュリティについて権限と責任を有する。
統括情報セキュリティ管理者	CISO の直属で、ネットワークや情報システムに関する権限と責任を有する。
情報セキュリティ管理者	組織毎に設置され、所管する組織の情報セキュリティについて権限と責任を有する。
情報システム管理者	個々の情報システムおよび、情報システムに対する情報セキュリティに関する権限と責任を有する。情報システム管理者の下に、情報システム担当者を置く場合もある。

なお、これらのチームや役割については、自治体や情報セキュリティポリシーの策定主体等、状況に応じて様々な形態があり得ます。例えば CISO については、自治体で情報セキュリティポリシーを策定している場合は副市長等、学校毎に策定している場合は学校長等というように、策定主体によって充てられる者が異なってきます。

c）情報セキュリティポリシーが想定する環境の確認

特に自治体で各部局共通の「対策基準」や「実施手順」が策定されている場合、必ずしも学校で児童生徒が学習を行うことを想定した内容になっているとは限りません。例えば、職員室での端末等の利用のみを想定しており、教室での利用を想定していない場合も考えられます。また、学校を対象としていても、校務系のネットワークのみが対象である場合もあります。

情報セキュリティポリシーによって記載箇所や内容は異なりますが、特に確認しておくべき点に関する記載例を以下に示します。

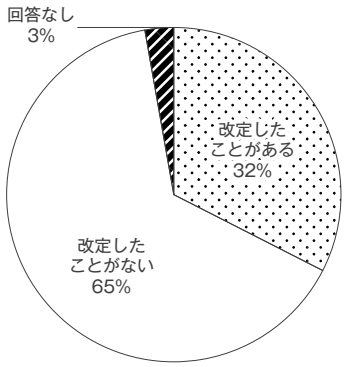
情報セキュリティポリシーの中の記載例

確認内容	記載例
無線 LAN	・統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。
ICT 機器	・モバイル端末については、使用時以外において施錠管理等の物理的措置を講じなければならない。 ・電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
クラウドサービス	・庁舎の敷地外にサーバー等の機器を設置する場合、最高情報責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。 ・サービスの利用終了時には、機器内部の記憶装置からすべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

[12] Chief Information Security Officer の略です。

また、既存の情報セキュリティポリシーでは無線 LAN やクラウドサービス等の利用が想定されていない場合があります。そのような場合には、必要に応じて関係部局（情報政策部門、情報セキュリティ委員会等）と連絡を取り、改定の働きかけをすることも検討する必要があります。

アンケート調査では、準拠している情報セキュリティポリシーがあると回答した教育委員会のうち 32%が、「情報セキュリティポリシーを改定したことがある」と答えました。



情報セキュリティポリシーを改定したことがあるか

クラウドを中心とした ICT 環境に係る項目の改定を行った自治体について、主な改定内容は以下のとおりです。

ICT 環境に係る情報セキュリティポリシーの改定内容例

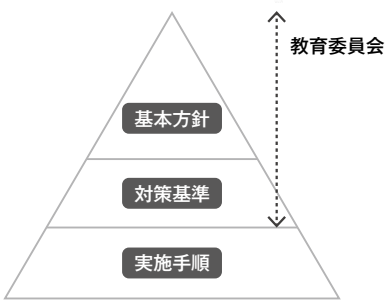
分類	内容
個人情報	・個人情報を含むファイルの保存方法について、パスワードの設定の規則を追加した。 ・情報資産を外部提供する際に、自治体の個人情報保護条例等の規定に抵触しないことを確認する義務を追加した。 ・学校ホームページに写真等をアップロードする場合の個人情報保護や同意の取得についての項目を改定した。
無線 LAN	・教育用パソコン（タブレット端末を含む）の使用に限り、無線 LAN の使用を認めた。 ・タブレット端末導入にあわせて、無線 LAN を授業用ネットワークのみで認め、無線 LAN アクセスポイントの情報セキュリティ機能要件を明記した。 ・学校内で無線 LAN を利用する場合に必要な情報セキュリティについて定めた。
ICT 機器	・タブレット端末の利用規定を追加した。 ・タブレット端末の利用上の注意事項と、情報モラル教育について追記した。 ・教職員の情報機器の取扱いに関する事項を追記した。 ・ICT 機器の管理（施錠できる保管庫等への格納）に関して記載した。
クラウドサービス	・クラウドサービスのような外部サービスの利用、委託先の管理、ネットワーク（公衆通信網）の利用、支給品以外の個人所有のスマートフォンなどの端末等やソーシャルメディアサービスの業務利用、情報セキュリティインシデント対策体制の強化について追記した。 ・クラウドサービスを利用する場合の基準について追記した。 ・クラウドサービスへの無断登録（保存）の禁止事項を追記した。

【事例　古河市教育委員会】

学習系のクラウドサービス利用にともない、教育委員会で独自に情報セキュリティポリシーを策定

古河市教育委員会では、市の情報セキュリティポリシーとは別に、教育委員会と学校を対象とした情報セキュリティポリシーを策定しています。古河市の情報セキュリティポリシーは、機微情報を扱う教職員の校務分野を想定しており、児童生徒が学習サービスを活用するうえではより柔軟なポリシーが必要と考えたためです。

なお、実施手順については初めから細かく定めると制約が多くなるため、導入後に実態を踏まえて徐々に整備していくこととしました。



d）情報資産（データ）の取り扱いに関する確認

情報セキュリティポリシーに基づいた情報資産の区分の考え方や管理方法についても、確認しておく必要があります。一定の基準で重要度等の区分が定められており、いずれの重要度であるかによって、保存場所等の管理方法が決められている場合があるからです。

例えば、情報資産のリストと重要度の区分が以下のように定められている場合、「管理番号００５のテスト問題について、保存場所を職員室からクラウドサービス事業者のサーバー上に変更する」のであれば、首長部局への保管場所の変更の申請が必要です。このような情報資産に関するルールと手続きを確認しておきます。実際の定義や手続きは自治体により異なるため、各情報セキュリティポリシーに従い適切な対応を行う必要があります。

既存の情報資産リストの例

管理番号	情報資産	管理者	保存形態	保存場所	公開対象	区分
001	学校要覧	教頭	データ	サーバー	一般	1
002	教育計画	教務主任	データ	サーバー	一般	1
003	指導要録	指導課	紙	鍵付きロッカー	教員	3
004	生徒名簿	教頭	データ	サーバー	校内	2
005	テスト問題	教務主任	紙	職員室	校内	2
	…	…	…	…	…	…

重要度の区分例

区分	定義	取り扱いルール
３	情報の漏えい、改ざん、破壊等により、教職員、児童生徒、保護者等の財産またはプライバシーに著しい影響があるもの、または業務に深刻な影響を及ぼすもの	インターネット経由で扱わない。保管場所と件数を申請する。
２	情報の漏えい、改ざん、破壊等により、業務に重大な影響を及ぼすもの	保管場所と件数を申請する。
１	区分３・２以外のもの	-

なお、上記重要度区分のように「インターネット経由で扱わない」等、ネットワーク上での取り扱いについて禁止事項がある場合でも、業務の適正な遂行等のために例外措置が認められる場合が多くあります。運用上どのような場合に例外措置が認められ得るのか、手続きを含めて確認しておきます。

（３）自治体のネットワークに関するポリシーの確認

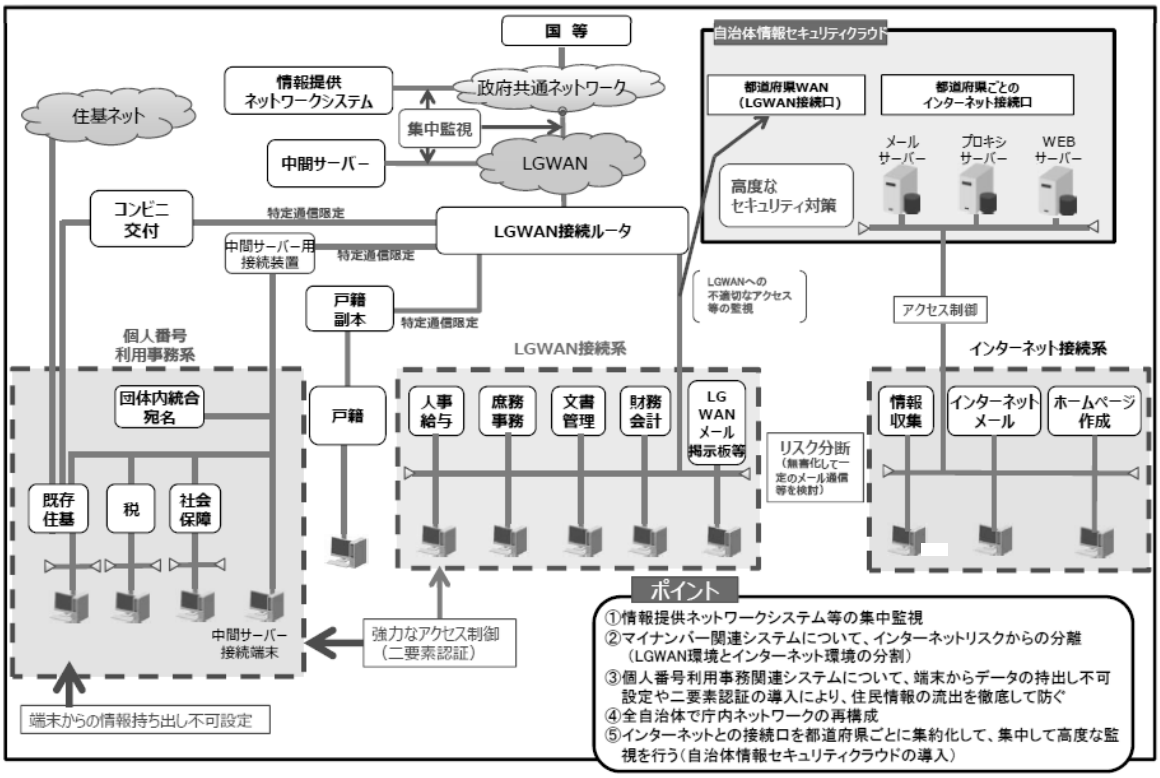
総務省の「新たな自治体情報セキュリティ対策の抜本的強化に向けて」では、

① マイナンバー利用事務系では、端末からの情報持ち出し不可設定等を図り、住民情報流出を徹底して防止すること
② マイナンバーによる情報連携に活用される LGWAN 環境のセキュリティ確保に資するため、LGWAN 接続系とインターネット接続系を分割すること
③ 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度な情報セキュリティ対策を講じること

との、三層からなる対策を講じることにより、早急に各自治体の情報セキュリティ対策の抜本的強化を図ることをお願いしています。総務省が示した「自治体セキュリティクラウド」のイメージは、次頁のとおりです。

自治体情報セキュリティクラウドイメージ

（総務省「新たな自治体情報セキュリティ対策の抜本的強化に向けて」より）



これらのネットワークの見直しの流れにおいて、学校のネットワークをどう位置付けるかは自治体により異なります。広域ネットワーク等で学校に特化したネットワークを敷設しており、当面は情報セキュリティ対策も含め独立して進めるとしている場合と、自治体ネットワークのルールづくりや整備を進めており、学校もいずれ整合性をとりたいとしている場合があるようです。

いずれにせよ、現時点ではまだ首長部局で検討している段階の自治体がほとんどであり、その動向にも注意しつつ、今後のネットワーク構成について検討する必要があります。

【事例　京都府】

自治体情報システム強靭性向上モデルに対応するものの、教育情報ネットワークは自治体情報セキュリティクラウドに含めず

京都府には、自治体が利用している行政系ネットワークの他に、学校の学習系ネットワークおよび校務系ネットワークから構成される教育情報ネットワーク「京都みらいネット」があります。行政系のネットワークに関しては、マイナンバーを想定して情報セキュリティ対策の強化を進めていますが、「京都みらいネット」については業務の性質、その規模の大きさ等から見て、行政系ネットワークとは分けて対策を立てる必要があると考えており、セキュリティクラウドには含めない方針を打ち出しています。

なお、「京都みらいネット」内の学習系ネットワークおよび校務系ネットワークについては、論理的にネットワークの分割を行うとともに、セキュリティクラウドと同等の対策を行って、情報セキュリティを担保しています。

第３章　情報セキュリティ手続きにおける「計画段階」の留意点

計画段階では、実際に導入する ICT 機器やネットワーク、教育用コンテンツの具体的な要件を定めますが、それらの要件については、準備段階で確認した法令やポリシーに対し整合性がとれたものである必要があります。

3.1 クラウド上で取り扱う情報資産の洗い出し

準備段階で教育用コンテンツの仕様と、順守すべき法令等を確認した結果を踏まえ、クラウドサービス上で取り扱いたい情報資産（データ）について整理します。

この段階では、「個人情報を取り扱うのか」「どのような区分（重要度等）の情報資産（データ）を取り扱うのか」が大きなポイントとなります。

（１）個人情報の取り扱いについて

準備段階で個人情報に関連する法令を確認した結果、クラウドサービス上で個人情報を扱えることが判明した場合には、個人情報保護審査会への付議等、必要な手続きを進めます。

クラウドサービス上で個人情報を扱えない場合は、何らかの対応を検討する必要があります。

例えば、個人情報に該当しない情報のみをクラウド上で扱うことが考えられます。情報収集の段階で、教育用コンテンツに「氏名」を登録する必要があることがわかったとしても、登録内容を工夫して「個人情報に該当しない」とみなしている例もあります。

【事例】クラウドサービス導入自治体・導入校での個人情報に関する解釈例

例 1）【個人情報は扱わない】各人のデータ保管場所としてのみクラウドを使う

市立札幌開成中等教育学校では、教育用コンテンツの利用にあたっては、児童生徒が学習に使った素材や成果物作成の過程のみを、生徒自身がクラウド上に保存しています。成果物は印刷して提出することし、学習系のネットワーク上で成績評価は行いません。このようにして、「クラウド上で個人情報を扱わない」と整理し、自治体の情報セキュリティポリシーにおける「インターネット上では個人情報を扱わないこと」とする規定の整合性をとっています。

例 2）【個人情報は扱わない】紐づけ情報のない状態でクラウドを使う

新地町では、クラウド上には ID のみを登録しています。児童生徒数が少ないため、ID がどの生徒に紐づくかという情報は教員の記憶のみで管理し、クラウド上で個人情報は扱っていないとしています。

また同志社中学校・高等学校では、クラウド上のユーザー登録をニックネームで行い、紐づけ情報を持たないことで、個人情報は扱っていないとしています。

例 3）【個人情報を扱う】個人情報が自治体内にあるとみなし、クラウドを使う

柏市では、クラウド上のメールサービスの利用にあたり、個人情報保護条例に抵触しないかどうか行政課に確認しました。

柏市の情報セキュリティポリシーでは、個人情報を保存するサーバーは市内に設置する必要がありますが、対象となったメールサービスはセキュリティに十分配慮した環境下で運営され、外部流出等の恐れがないため、個人情報が自治体内にあると見なされ、導入に至りました。

例 4）【個人情報を扱う】自治体の手続きを実施してクラウドを使う

姫路市では、校務のクラウドサービス利用にあたり、市が保管している個人情報の目録を管理する市政情報センターに対し、学校内に保管していた個人情報の保存場所を変更する旨の届け出を提出しました。

【事例　奈良県教育委員会】

個人情報保護に関する弾力的な対応

奈良県教育委員会では、原則論上は、個人情報は有線の校務系ネットワークでのみ扱えるようになっています。しかし、例えば学校行事の写真を校務系ネットワークにしか置けないとなると、写真印刷のインターネット発注や卒業アルバム作成を行うことができません。そのため、首長部局との協議を踏まえて、「一時的な共有のための取り扱いは、十分注意して取り扱う」としています。十分注意して取り扱うことで、個人情報保護条例を踏まえているという考え方です。

（2）個人情報以外の情報資産の取り扱いについて

個人情報以外の情報資産（データ）に関しても、どのような解釈でどのような情報を取り扱うのか検討し、準備段階で確認した手続きを進める必要があります。そのため、情報セキュリティポリシー等で定められている情報の区分等に沿って、情報資産の扱いがどのように変わるのか検討します。

3.2 クラウドを中心としたICT環境に関するリスクの洗い出し

法令等を確認した結果、特に規定がない場合であっても、クラウドを中心としたICT環境に関するリスクの洗い出しを行い、情報セキュリティ対策の検討を行うことは非常に重要です。情報セキュリティ対策については「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）2014（中学校・特別支援学校版）」等に記載された内容が参考となります。

端末をインターネットに接続し、教育クラウドサービス等を活用することを念頭においた場合の、リスクと対策例を以下に示します。

情報セキュリティに関するリスクと対策例

項目	リスク	対策
物理的	校舎内で端末等を盗難される恐れがある。	・放課後、充電保管庫を施錠する。 ・警備会社等による警備を強化する。
	学校外で盗難・置き忘れが起こる恐れがある。	・身体にかけられる専用持ち出し袋を使う。 ・貸し出し手続きを決め、意識づけする。
	盗難・置き忘れにより、端末を不正利用される恐れがある。	・ログイン認証を行う。 ・MDMツールで現在地確認を行えるようにする。 ・遠隔操作で、端末のロック・データ削除を行えるようにする。
人的	情報の持ち出しやソーシャルエンジニアリング[13]が起こる恐れがある。	・情報の取り扱いルールを徹底する。
	公共の場での閲覧によりショルダーハッキングされる恐れがある。	・他者が画面を覗き見ることができる場所で、重要な情報を閲覧しないことを徹底する。
ウイルス感染	ウイルスに感染する恐れがある。	・ウイルス対策システムを導入する。 ・ウイルス対策状況（OSやウイルス定義ファイルのバージョン等）を確認できるツールを導入する。
	端末に接続されたUSBメモリ等からウイルスに感染する恐れがある。	・許可されたUSBメモリ以外の使用を禁止する（感染ルートを減らす）。
	フリーソフトからウイルスに感染する恐れがある。	・フリーソフトの利用を制限する。
	Webサイトやメールからウイルスに感染する恐れがある。	・メールの添付ファイルやURLに注意する旨の研修を行う。
不正接続・不正侵入	サーバーや共有フォルダに不正アクセスされる恐れがある。	・各データへのアクセス権限を適切に設定する。
	外部から、校内ネットワークに不正アクセスされる恐れがある。	・ファイアウォールや侵入検知システムを導入する。
	外部から、無線LANに不正アクセスされる恐れがある。	・許可された端末以外、無線LANに接続できないようにする。
	ネットワーク上の情報が盗聴される恐れがある。	・通信の暗号化を行う。
	ネットワーク機器の脆弱性を狙って攻撃される恐れがある。	・脆弱性対策ファームウェアの適用を行う。
クラウドサービス事業者	クラウドサービスの脆弱性を狙って攻撃される恐れがある。	・OSやソフトウェアのセキュリティパッチの適用を行う。
	従業員により情報の持ち出しが起こる恐れがある。	・各データへのアクセス権限を適切に設定する。 ・保存データの暗号化を行う。 ・その他、持ち出し禁止の研修等を行う。

[13] 情報通信技術を用いずに、人間の心理的な隙をついて情報を盗み出す方法のことを言います。

項目	リスク	対策
児童生徒の安心・安全	児童生徒が適切でない（暴力的等）Web サイトを閲覧する恐れがある。	・フィルタリングの設定を行う。
	児童生徒が深夜等、過度に端末等を利用する恐れがある。	・決められた時間以外は端末を使えないよう設定を行う。 ・利用時間に関わるルールを徹底する。

特にクラウドを中心とした ICT 環境を導入するにあたっては、以下のような点に留意が必要です。

（1）端末等の機器について

クラウドを中心とした ICT 環境の導入にあたっては、タブレット等の持ち運び可能な端末を導入することが多いと考えられます。

そのため、端末の盗難対策としての充電保管庫の施錠管理や、端末の紛失を予防するための対策を検討します。

【事例　草津市】

充電保管庫について、日中は解放、夜間は施錠管理

草津市内の小学校では、充電保管庫の運用は学校毎に異なっており、日中は充電保管庫に鍵をかけていない学校もあります。そのような学校では、朝の授業開始前や雨の日の休み時間等に児童が自由に端末を利用しています。放課後以降は、台数や充電の状況を確認したうえで、施錠管理しています。

【事例　新地町】

持ち帰り袋で破損・紛失対策

新地町では、両手が空くよう、肩や首から下げられる持ち帰り袋を利用し、紛失や破損の対策としています。

持ち帰り袋の使用例（新地町）

なお、MDM ツール等の導入により、現在地の確認や、遠隔での端末ロック、データ削除など、端末の紛失後に適切に対応することが可能となります。

（2）教員や児童生徒への研修

クラウドを中心とした ICT 環境を活用するうえで、どれだけ端末やネットワークの情報セキュリティ対策を行ったとしても、教員や児童生徒によって情報が漏えいする可能性が残ります。

そのため、ルールの策定や、そのルールについて研修等で周知徹底することが非常に重要です。教職員や児童生徒に対するルールづくりや研修については、第４章で詳述します。

（3）ネットワークに関する設計

クラウドサービスの利用にあたっては、インターネット経由で接続することとなります。学習系ネットワークをインターネット接続する場合、ネットワーク経由でのウイルス感染や、不正侵入のリスクが高くなります。

そのため、ウイルス対策やファイアウォールの設置等を検討します。

なお、端末の OS の脆弱性パッチや、端末に導入したウイルス対策ソフトウェアのウイルス定義ファイルは、常に最新のものにしておくことが必要です。MDM ツールの一部や資産管理ツール等により、それらのバージョンを一元管理できる場合もありますので、あわせて検討しておきましょう。

また、特に無線 LAN の導入にあたっては、外部から持ち込まれた機器が勝手にネットワークに接続されないよう、ネットワークへの機器の接続制限を行うことが有効です。接続制限を行う方法としては、ネットワーク機器に設定を行い、事前に登録された端末しか接続できないようにしたり、本人認証を行ったりといった方法があります。

（4）認証

端末やクラウドサービスを利用する場合の認証については、安全性と使い勝手の両面で検討する必要があります。

本人認証に関しては、一般的なパスワードを使う方式の他、USB メモリがなければ端末やソフトウェアが使えないようにする方式等があります。認証は一般に、パスワードを覚える等の「知識情報」、USB メモリ等の鍵となる物品を持っている等の「所持情報」、指紋や虹彩等の「生体情報」で行われ、複数種類・複数回を組み合せた方がより強固であると言われています。どの程度守るべき情報か、運用上の手間はどの程度許容できるか等の条件から、最適な認証方法を選択します。

【事例】児童生徒が使うタブレット等の端末のパスワード管理例

例１）端末にログインする際の認証のみ

奈良県立畝傍高等学校では、端末へのログインのみでクラウドサービスを利用できるようシングルサインオンを実現しています。ログイン時に毎回生徒が ID やパスワードを入力する必要がなく、簡単にクラウドサービスを利用することができます。

例２）児童生徒がパスワードを入力

柏市の学校では端末を共有で使用しており、クラウドサービス利用時のパスワードを都度、児童生徒が入力しています。小学校 1 年生の児童については、当初アルファベットが入力できないのではという懸念があり、キーボードに書いてあるカナでパスワードを伝えていましたが、アルファベットでも特に問題ないことがわかったため、すべて児童生徒自身で入力しています。

例３）教員が使う端末のパスワードについて、USB 認証で教員の負担軽減＋情報セキュリティ強化

柏市教育委員会では、教職員に配布している PC の起動時には、USB 認証が必要です。USB メモリがなければ PC を起動することはできません。また、USB メモリの他に「PIN（Personal Identification Number）コード」と呼ばれる文字列を入力することが必要です。

USB メモリの「所持情報」と、PIN コードによる「知識情報」の２要素による認証で情報セキュリティを強化する一方、パスワードより平易な PIN コードを用いることで、教員の負荷軽減も同時に実現しています。

【コラム】パスワードの重要性

独立行政法人 情報処理推進機構 （IPA）が定期的に発表している「コンピューターウイルス・不正アクセスの届出状況および相談状況」によると、届出があった不正アクセスは、なりすましによる被害が最も多い状況が続いています。

なりすましが起こりやすいパスワードは、「自分に関連した情報が含まれていて、推測しやすいもの」、「短かったり、辞書に載っていたりするような単語を使った単純なもの」、「複数の Web サイトで使いまわしているもの」だと言われています。

特にパブリッククラウドを活用する場合、不正アクセスを行う攻撃者はどこにいるかわかりません。ネットワークを経由して、世界中から攻撃されることがあります。不正アクセスを受けた場合、クラウド上にあるデータやネットワーク上を通るデータが漏えいしたり、改ざんされたりといった被害が考えられます。

また、児童生徒間でアカウントが推測しやすい状態になっていたため、友達のアカウントでログインしてしまったという事例もあります。

このようなことを防ぐためには、パスワードの文字種をシステム上で制限するような技術的な対策の他、教員や児童生徒に対する研修をあわせて行うことも有効です。

（5）児童生徒の安心・安全を守るための対策

ウイルス感染や不正侵入等の一般的な情報セキュリティ対策の他、学校現場においては児童生徒の安心・安全を守るための対策もあわせて検討する必要があります。

＜フィルタリング＞

学校における Web サイトの閲覧制限（フィルタリング）に関しては、業務や授業に関係のない Web サイトの閲覧を禁止するだけでなく、インターネットを通じたトラブルから児童生徒を保護する目的もあります。

フィルタリングをあらかじめ設定することで、有害なコンテンツや不適切なサイトの閲覧を制限でき、コンピューターウイルスへの感染リスクだけでなく、不当な高額請求や迷惑メール等を受けるリスクが減少します。

なお、フィルタリングを行う対象については、以下のような方法で指定します。

代表的なフィルタリング対象の指定方法

方式	説明
URL フィルタリング	Web サイトの URL を指定する。
コンテンツフィルタリング	キーワードやカテゴリの指定等、Web サイトのコンテンツの内容を指定する。

これらの方式により、閲覧できるものを指定するホワイトリストか、禁止するものを指定するブラックリストにより制御を行います。

ホワイトリストを採用する場合には、指定したサイトしか閲覧できないため、調べ学習で自由にインターネット検索を行う場合に目的のWebサイトが閲覧できない等の影響がないか注意する必要があります。

また、フィルタリングの設定は万能ではなく、特に最新のショッキングなニュースや動画等に対応しきれない場合もあります。追加の設定要望を随時保守業者に伝えたり、児童生徒への情報モラル教育により不要な検索を避けたりする等の配慮も並行して必要です。

なお、フィルタリングは従来、ネットワーク上に機器を置くことが一般的でしたが、近年ではクラウドサービスでの提供も行われています。

【事例　古河市教育委員会】

専用 Web ブラウザーとクラウドサービス型フィルタリングで見られるサイトを制限

古河市教育委員会では、児童生徒からタブレット端末上の標準 Web ブラウザーが見られないようにしたうえで、専用 Web ブラウザーとクラウド型フィルタリングサービスを使っています。

しかし、利用している教育用コンテンツの中に専用 Web ブラウザーを経由しない通信を行うものがあり、フィルタリングがかからない場合があるという課題を抱えています。そのため、今後は通信キャリアが提供するフィルタリングサービスと組み合わせることでの対応を計画しています。

【事例　新地町立駒ケ嶺小学校】

学校内でのみ利用する端末と、持ち帰り用端末で異なるフィルタリング設定を実施

５・６年生分のタブレット端末を共有で使用しており、「2 セット分」として学校で管理しています。このうち 1 セット分のみが、持ち帰り学習に対応しています。

持ち帰り学習を行える端末については、特定の教育用コンテンツのみにしかアクセスできないようなフィルタリング設定を行い、自由なインターネット検索を制限しています。

＜端末の利用制限＞

特に持ち帰り学習を行う場合に、児童生徒が端末の利用に熱中してしまい、利用が長時間におよんだり、深夜におよんだりといった課題が生じる場合があります。

対策として、「夜９時以降は使わない」「インターネットやゲームで遊ばない（利用を教育用コンテンツに制限する）」等の制限を児童生徒と約束する他、技術的に対策を行うことも可能です。

例えば、MDM ツールの一部機能や専用ツール等で時間制限を設けたり、持ち帰り学習の際は特定の教育用コンテンツ以外に接続できないようフィルタリングの設定を切り替えたりする方法もあります。

＜端末に保存されるデータの制限＞

児童生徒間で端末を共有する場合には、お互いに情報を見えないようにする工夫が必要です。児童生徒ごとにアカウントを設定する方法や、端末内に情報を保存しない方法、授業が終わったらデータを自動的に削除するシステムを導入する方法等が考えられます。

また、個人専用の端末であっても、教職員や児童生徒がソフトウェアを自由に導入することを許可すると、コンピューターウイルス等の侵入の可能性が高まり、不正にコピーしたソフトウェアや、ライセンス違反のソフトウェアが導入される可能性も生じるため、自由なソフトウェアの導入を制限する等の配慮が必要です。

さらに、近年では電子メールサービスや、写真やデータをクラウド上に保存するオンラインストレージサービス等のクラウドサービスを、個人が家庭等において利用する機会も増えてきました。例えば個人でアカウントを取得したフリーメールやオンラインストレージサービスを教育委員会や学校で自由に使えるようにすると、外部への不正な情報流出に繋がる可能性があります。ルールの徹底やフィルタリングの対象にすることを検討する等、注意が必要です。

【事例　古河市教育委員会】

タブレット端末へのアプリケーション追加は教育委員会と保守業者で管理し、教員や児童生徒は追加できない運用を実施

古河市教育委員会では、MDM による端末管理に加え、アプリケーションを追加するために使う管理用のアカウント（パスワード）を教育委員会が管理しています。

アプリケーションの追加は教育委員会から保守事業者に依頼して行うことで、許可しないアプリケーションが勝手に追加されることを防いでいます。

3.3　リスクおよび情報セキュリティポリシーを踏まえた仕様書の作成

前述のリスクおよび情報セキュリティ対策、情報セキュリティポリシーを踏まえ、クラウドを中心とした ICT 環境の仕様書を作成します。本節では、教育用コンテンツの導入にあたりクラウドサービス事業者に向けた仕様書を作成することを想定して、情報セキュリティに関する仕様策定について述べます。

（1）情報セキュリティに関する要求仕様の作成

利用する教育用コンテンツの選定にあたっては、情報セキュリティポリシーに沿った事業者、情報セキュリティ対策を適切に行っている事業者のコンテンツを選定することが必須となります。

「地方公共団体における情報セキュリティポリシーにおけるガイドライン」（平成２７年３月改定　総務省）では、外部委託の際に配慮する項目例として以下が示されています。

外部委託の際に配慮する項目例

- 外部委託事業者に提供する情報の、委託事業者における目的外使用の禁止
- 外部委託事業者における情報セキュリティ対策の実施内容及び管理体制
- 外部委託事業の実施にあたり、外部委託事業者の組織又はその従業員、再委託事業者、若しくはその他の者による意図せざる変更が加えられないための管理体制
- 外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属
- 専門性（情報セキュリティに係る資格・研修実績等）
- 実績及び国籍に関する情報提供
- 情報セキュリティ要件の適切な実装
- 情報セキュリティの観点に基づく試験の実施
- 情報セキュリティインシデントへの対処方法
- 情報セキュリティ対策、その他の契約の履行状況の確認方法
- 情報セキュリティ対策の履行が不十分な場合の対処方法

また、「政府機関の情報セキュリティ対策のための統一基準（平成２６年度版）」においては、パブリッククラウド等の外部サービスを利用する際に、統括情報セキュリティ管理者が委託先の選定基準を整備することが定められています。選定基準の観点を以下に示します。

情報セキュリティに関する外部委託先の選定基準の観点例

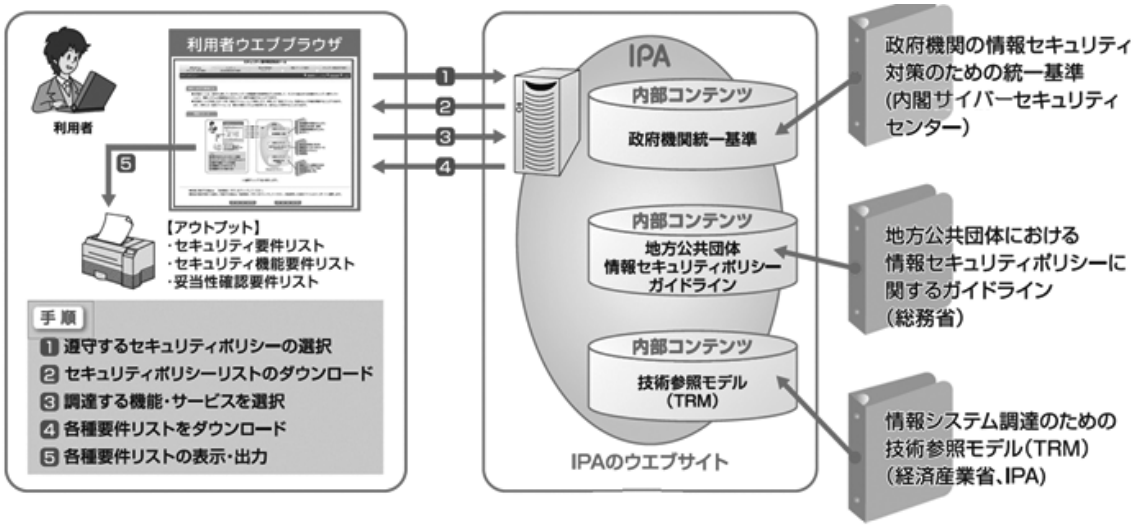
分類	評価項目例
自治体の状況にあわせた指標	a）情報セキュリティポリシーと整合性がとれるか
客観的指標	b）情報資産に関する規格の認証を受けているか c）定期的な脆弱性検査を行っているか

a）情報セキュリティポリシーとの整合性に関する仕様の作成について

情報セキュリティポリシーで定められた情報セキュリティ対策等について、実際にクラウドサービス事業者が順守すべき具体的要件として整理し、仕様書等に記載する必要があります。

なお、独立行政法人 情報処理推進機構 （IPA）が公開している「セキュリティ要件確認支援ツール[14]」を利用すると、順守すべき情報セキュリティポリシーから、クラウドサービスの利用にあたっての具体的要件例を洗い出すことができます。

IPA セキュリティ要件確認ツールのイメージ



（IPA「セキュリティ要件確認支援ツール」より）

b）情報資産の取り扱いに関する規格等について

クラウドサービス事業者が情報資産を適切に取り扱っているか確認する方法のひとつとして、第三者認証があります。関連する規格等を以下に示します。

情報資産に関連する国内および国際的な標準規格

規格	説明
ISO/IEC 27001	情報セキュリティマネジメントシステム（ISMS）の国際規格
ISMS/JIS Q 27001	上記 ISO/IEC27001 に基づいた国内規格
ISO/IEC 27017	クラウドサービスの提供及び利用のための情報セキュリティ管理策の国際規格
JIS Q 15001	個人情報保護マネジメントシステムの国内規格
プライバシーマーク	上記 JIS Q 15001 に適合し、個人情報保護の体制を整備している事業者を一般法人日本情報経済社会推進協会（JIPDEC）が認定する制度

これらの規格において、情報資産を適切に取り扱うための計画だけでなく、計画の実施状況や達成状況の確認が定められています。事業者が PDCA サイクルに基づいて継続的に見直しを行っているかどうか等を判断する一つの基準となります。

[14] https://isec-sras.ipa.go.jp/

c）脆弱性検査について

脆弱性検査を行い適切な対応を行うことで、脆弱性を狙った攻撃によって情報資産が漏えい・改ざんされるリスクを低減することができます。そのため、事業者に定期的な脆弱性検査を求めることが推奨されます。

脆弱性検査には、いくつかの種類や方法があり、ネットワークや Web アプリケーション（クラウドサービス）を対象としたものもあります。Web アプリケーションに関しては、事業者の開発したアプリケーションそのもののほか、サーバーの OS やミドルウェア等も含めて検査を行います。

d）仕様書に関する留意点

前述の通り、仕様書の作成にあたっては、情報セキュリティポリシーとの整合性を加味して検討する必要がありますが、広く一般に提供されているクラウドサービスを利用する場合には、個別の要望にあわせた仕様変更が行えない場合があります。

その場合には、統括情報セキュリティ管理者等が策定したクラウドサービス事業者の選定基準を元に、クラウドサービス事業者が開示している SLA（サービスレベル契約）や、利用規約やプライバシーポリシーといったホワイトペーパー等を確認したうえで、情報セキュリティポリシーに適合するかどうか確認する必要があります。

【事例　市立札幌開成中等教育学校】

学校の要望を満たすクラウドサービス選定を教育委員会がサポート

札幌開成中等教育学校では、新規に導入したいクラウドサービスがある場合、市の所定の手続きに従います。事業者が提示するホワイトペーパー等で、情報セキュリティポリシーと齟齬がないことが確認できないと導入できません。

札幌市の場合、クラウドサービスの導入については、同市の情報セキュリティポリシー上、外部サーバーの利用として位置づけられます。このため、同市が管理するサーバーの情報セキュリティ対策と同程度の対策が施されるなど、安全性が担保されていることを規約等で確認できることが求められます。同市では、サービス提供事業者のプライバシーポリシーやサービス利用規約、個人情報の取り扱い規定等から、情報セキュリティ対策の状況を確認することにより、最高情報セキュリティ責任者よりクラウドサービスの利用承認を得ています。

また、学校からクラウドサービスの名称指定で要望があったとしても、必要なセキュリティ対策が施されていない場合には、札幌市教育委員会がサポートして同様のことを行えるサービスで代替できないか、一緒に検討するようにしています。

（2）クラウド導入にあたっての仕様書作成上の留意点

情報セキュリティポリシーに配慮して仕様書上で記載される情報セキュリティ対策のうち、自前サーバー（オンプレミス）を利用する場合とクラウドサービスを利用する場合で、考え方に相違が生じる可能性のある項目について以下に示します。

クラウド導入にあたり留意が必要な情報セキュリティ対策例

情報セキュリティ対策	目的
a）入退室や機器の物理的な管理	侵入等による情報漏えいや改ざんの予防
b）機器の冗長化、定期的な点検	故障等によるサービス停止の予防
c）機器の廃棄、データの廃棄	情報漏えいの予防
d）アクセス記録やメンテナンス記録の保存	不正アクセスの抑止や検知 不正アクセス発生後の原因究明
e）研修等の実施	事業者の従業員等による情報漏えいや改ざんの抑止

a）入退室や機器の物理的な管理

入退室の管理や機器の施錠等について、情報セキュリティポリシーで定められている場合があります。

クラウドサービスを利用する場合には、機器がクラウドサービス事業者のデータセンター内に置かれています。そのためデータセンターへの入退室管理や機器の管理については事業者の役割となり、情報セキュリティポリシーに適合する管理を行うことについて、仕様に明記する必要があります。

b）機器の冗長化、定期的な点検

故障に備えて複数台の機器を置く冗長化や、機器の定期的な点検・修理等に関しても、クラウドサービス事業者の役割となります。

そのため、点検結果について定期的に報告を求めること等を検討し、仕様に盛り込みます。

c）機器の廃棄、データの廃棄

情報セキュリティポリシー上に、USB メモリやハードディスク等の記憶媒体の廃棄を想定した項目がある場合があります。

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のサーバー上のディスクにデータが保存されることとなるため、サービス利用を終了する場合のデータ消去の可否と、データ廃棄の方法の観点から留意が必要です。

廃棄の方法については、データが保存されたディスク等が事業者の資産であるため、物理的な破壊や磁気的な破壊は難しいことがあります。情報セキュリティポリシーで物理的な廃棄に対応が限定されていないかを確認したうえで、クラウドサービス事業者にデータ消去ソフトウェアの利用が可能か確認したり、復元可能性について説明を求めたりする等の注意が必要です。

d）アクセス記録やメンテナンス記録の保存

情報セキュリティポリシーで、情報システムへのアクセス記録（ログ）や、メンテナンス作業記録を残しておくことが求められている場合があります。そのような記録は不正アクセスの検出や、情報漏えい時の調査、情報システムのトラブルの原因調査等に利用するため、改ざんされないよう保管する必要があります。

クラウドサービスを導入するにあたっては、クラウドサービス事業者における記録の保管状況について確認する必要があります。

e）研修等の実施

情報セキュリティポリシーで、クラウドサービス事業者等、委託先の事業者内で研修を行うことについて規定されている場合があります。自治体の情報セキュリティポリシーの周知徹底をクラウドサービス事業者に求める等の場合には、要求仕様に盛り込みます。

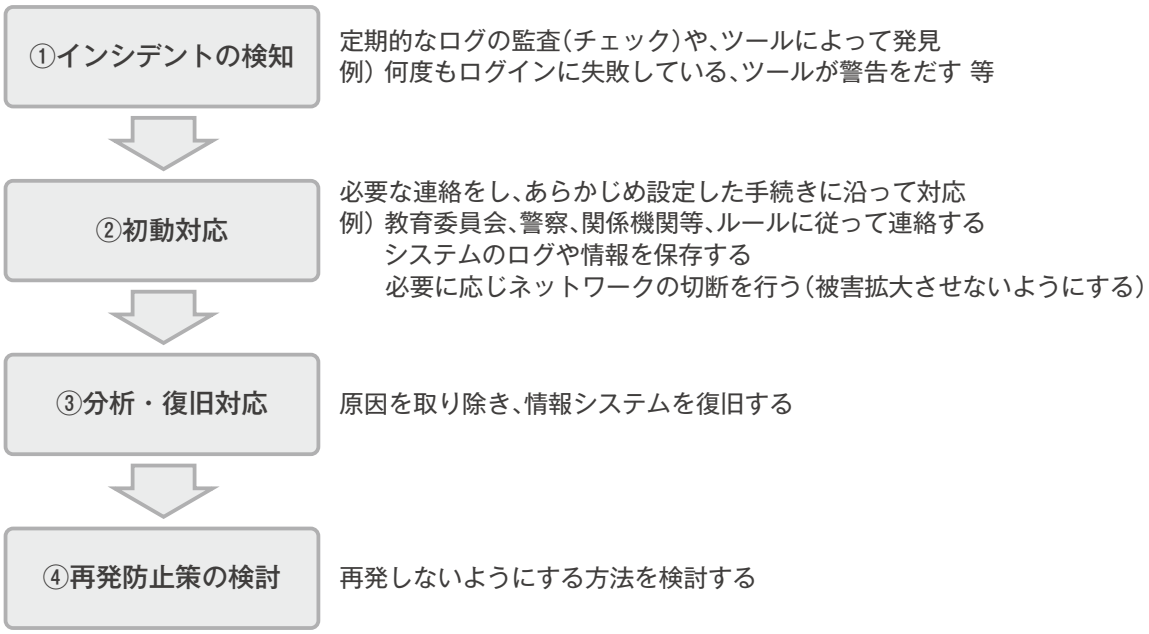
第４章　情報セキュリティに関する手続きにおける「運用段階」の留意点

運用段階で実際にクラウドを中心とした ICT 環境を活用していくにあたっては、情報セキュリティに関する運用方法をあらかじめ決めた上で、そのとおりに運用されているかどうか継続的に確認する必要があります。

4.1 緊急時対応計画の整備

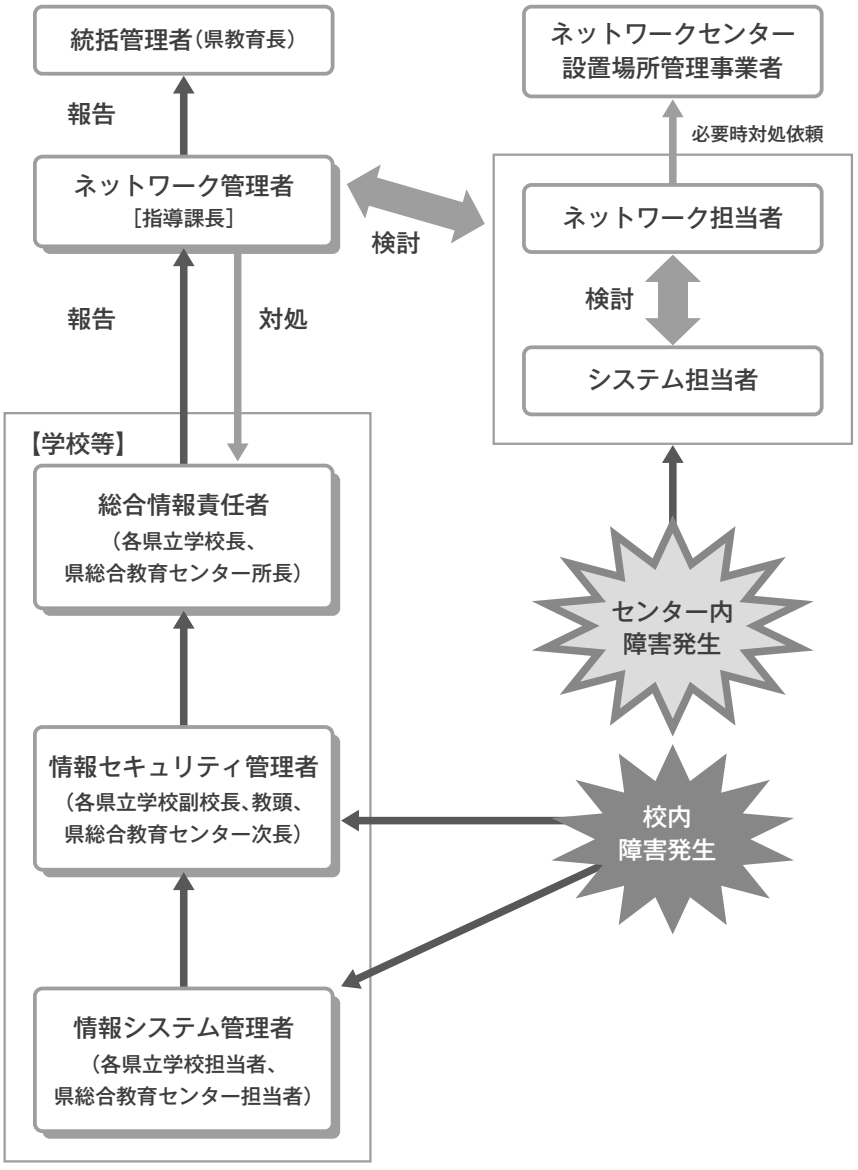
各種の情報セキュリティ対策を行ったとしても、情報資産を脅かすような出来事（インシデント）が発生する可能性があります。そのような場合に備え、「緊急時対応計画」を事前に策定しておくことが重要です。一般に、情報セキュリティポリシーの中で、すでに以下のようなフローが既定されていると想定されるため、整合性をとりながら、クラウドサービス事業者との連絡体制等についてあらかじめ定めておきます。

情報セキュリティポリシーにおける緊急時対応の一般的な例



【事例】緊急時対応計画の例

千葉県では、千葉県学校情報ネットワーク運用要領の中で、障害発生個所毎に、連絡担当者等の緊急時対応フローを規定しています。



(千葉県学校情報ネットワーク運用要領を元に加工)

4.2 研修の実施

ICT 機器やネットワーク、教育用コンテンツの活用にあたっては、利用者である教員や児童生徒が自ら情報漏えい等を行わないよう、情報セキュリティを確保するための実施手順を整備し、周知徹底する必要があります。次頁に周知徹底が必要な項目の例を示します。

周知徹底が必要な項目の例

分類	項目	内容例
情報セキュリティポリシー	体制、役割	・CSIRT、CISO 等の体制と役割 ・各教職員の義務や責任
	情報資産の区分と、区分に応じた取り扱い	・情報資産の重要度等の区分 ・情報の持ち出しルール
	個人情報の取り扱い	・個人情報の取り扱いルール
	緊急時対応	・端末紛失時等の連絡体制
ICT 環境に関するルール	ウイルス対策	・OS のアップデートやウイルス対策ソフトの利用に関する呼びかけ
	ソフトウェアインストール	・ソフトウェアインストールのルールや注意事項
	端末の持ち出し	・端末の持ち出しの手続きと手順
	機器やコンテンツの使い方	・ネットワークへの接続方法 ・端末の起動・終了の方法 ・教育用コンテンツの機能や使い方
	その他の注意項目	・各種の順守事項、禁止事項、推奨事項等 ・クラウドのストレージサービスやメールサービスの個人利用に伴うルール
情報モラル	ソーシャルエンジニアリング	・パスワードの管理についての注意事項 ・不審なメールに対する注意事項（標的型メール攻撃対策[15]） ・シュレッダーの利用
	SNS 利用	・書き込みに関するルール

また、このような項目に関しては、クラウドを中心とした ICT 環境の導入時の他、継続的に情報セキュリティ意識の向上を図っていくことが重要です。その方法やタイミングの例は以下のとおりです。

セキュリティ意識の向上のための取組例

方法	タイミング	内容例
研修	ICT 機器や教育用コンテンツの導入時、追加時	・ICT 機器や教育用コンテンツの使い方と、情報セキュリティの留意点に関する説明をあわせて実施
	定期的な実施（1 年に 1 回等）、または教職員のライフステージに応じた実施（1 年目、3 年目等）	・特に重要なルールや手続きの再確認 ・ルールや対策の見直しを行った項目の共有 ・最新の情報セキュリティ対策情報の共有
	教職員の異動時	・学校特有の情報の共有
	違反やインシデント発生時	・再発防止のためのルールや手続きの再確認
e ラーニング	定期的な実施（1 年に 1 回等）、または教職員のライフステージに応じた実施	・特に重要なルールや手続きの再確認 ・ルールや対策の見直しを行った項目の共有 ・最新の情報セキュリティ対策の共有
チェックリスト	定期的な実施	・チェックリストの配布によるルール等の順守状況の確認
小冊子	定期的な実施	・ICT 機器や教育用コンテンツの使い方をあわせて、ハンドブック形式で作成・配布

15 特定の組織に対し特定の目的のために行う攻撃を「標的型攻撃」と言います。標的型メール攻撃では、メール本文の URL や添付ファイルを開くことでウイルスに感染させ、情報漏えいに繋がる場合があります。

【事例　姫路市教育委員会】

教員向け研修にセキュリティ研修を組込

姫路市の教育委員会では、教員の５年目研修・10 年目研修・15 年目研修の中で情報セキュリティに関する研修を行っています。また、管理職は、市長部局の管理職と同じ情報セキュリティのｅラーニング学習を行うこととしており、市の情報セキュリティ研修とも連携しています。

【事例　新地町教育委員会】

各学校の代表の教員に「ネットアドバイザー養成講座」を実施し各学校には教員が展開

新地町教育委員会では、夏休みに各学校の教員 2～3 名を集め、「ネットアドバイザー養成講座」を行いました。

教員がネットアドバイザーになるための内容で、情報モラルに関して参加教員が各人で生徒向け・保護者向け・教員向けの講座資料をまとめました。お互いに作成したものを共有し、それぞれの学校で役立てています。

【事例　同志社中学校・高等学校】

生徒全員に「ネットワーク利用の手引き」を配布

同志社中学校・高等学校では、すべての生徒に「ネットワーク利用の手引き」という冊子を配布し、端末やネットワーク利用に関する利用手順の他、ルールやマナーについても周知しています。

目次

【事例　千葉県立袖ヶ浦高等学校】

生徒自身がルールづくりを行う

千葉県立袖ヶ浦高等学校では、学校が定める正式なルールの他に、授業の一環として生徒が自主的なルールを考えています。

禁止事項を並べ立てるような内容ではなく、望ましい使い方について考えるものです。生徒自身が考えることで、守ろうという意識づけにつなげています。

4.3 情報セキュリティに関する監査

情報セキュリティポリシーで情報セキュリティ監査について定められている場合には、それに従って進めます。

クラウドサービスを利用するにあたって、特に定期的に確認すべき項目例を以下に示します。なお、問題があった場合には CISO（最高情報セキュリティ責任者）に報告したうえで、是正措置を検討します。

特に定期的に確認すべき項目例

対象	項目例
事業者	・アクセスログ等の定期的な確認 ・情報セキュリティ対策機器の検知状況の確認 ・定期的な脆弱性診断の実施状況の確認
教育委員会・学校	・情報セキュリティポリシーや実施手順等の順守状況の確認

4.4 著作権等

クラウドサービスの利用にあたっては、著作権や肖像権への配慮が必要となります。

（1）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、法令の順守に向け、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。

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、トラブルになる可能性
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可能性
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、トラブルとなる可能性

【事例　新地町立駒ケ嶺小学校】

素材利用にあたってのルールを児童に徹底

新地町立駒ケ嶺小学校では、写真にコメントを付けるような授業を積極的に取り入れていますが、あわせて、低学年の時から自分のものと他人のものを分けて他人のものを尊重するような指導に取組んでいます。

具体的には「自分で撮影した写真か、特定の教育用コンテンツで提供されている写真（契約上、利用可能なもの）しか使ってはいけない」というルールを徹底しています。

【事例　市立札幌開成中等学校】

成果物作成のための素材をクラウドサービス上に保存

札幌開成中等教育学校では、クラウドサービス上に生徒の成果物を作成する過程での素材を保存することがありますが、成果物そのものを保存することはありません。

また、成果物には、出典を明示するよう徹底しています。

（2）肖像権

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ることは、大きなメリットとして評価されています。

また、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。

このような場合に、児童生徒を特定し得る写真を公開する等の場合には、肖像権への配慮が必要です。

【事例　古河市立古河第五小学校】

入学時および都度の同意取得を実施

古河市立第五小学校では、従前から ICT やクラウドサービスの活用について先進的な取組をしており、事例の発信を多くしています。そのため、入学時にホームページ等への顔写真の掲載に関し同意を得るとともに、必要に応じて再度同意を取得しています。同意を得られない児童生徒に関しては、掲載しないようにしています。

【事例　千葉県立袖ヶ浦高等学校】

入学時に承諾書を取得

千葉県立袖ヶ浦高等学校情報コミュニケーション科では、入学時に肖像権等に関する承諾書の提出をするよう、入学前の保護者説明会でお願いしています。

学校長および学科長の名義で「生徒の肖像権等の取り扱いの承諾について（お願い）」文書を保護者に配付し、外部からの問い合わせや取材の依頼が多く授業風景の撮影が行われることと、インターネットを含む各種メディア等に生徒の写真・氏名・著作物が掲載されることについて説明を行ったうえで、学校長宛てに以下のような承諾書を提出するよう依頼し、必要に応じて実際の運用時に再度、本人・保護者に確認を行っています。

年　　月　　日

千葉県立袖ヶ浦高等学校長　様

承 諾 書

情報コミュニケーション科在籍中の取材，広報活動等に関して，各種メディア（書籍，雑誌，Ｗｅｂページ等）に生徒の写真，氏名，課題作品等が掲載されることを承諾いたします。ただし，内容が教育活動の紹介，研究等，適切な用途であるものに限ります。

生徒名＿＿＿＿＿＿＿＿＿＿＿＿＿＿

保護者名＿＿＿＿＿＿＿＿＿＿＿＿印

なお、承諾書に関しては、他に生徒の肖像権に特化した例や、著作権に特化した例もあります。