資料2-2

１人１台端末の円滑な利活用に関する調査協力者会議（第2回）

教育情報セキュリティの考え方について

2021年7月14日

合同会社KUコンサルティング　代表
（文部科学省ICT活用教育アドバイザー
文部科学省ガイドライン改訂検討会主査）
髙橋　邦夫

教育情報セキュリティポリシーガイドラインの目的

◆ 目的

- 児童生徒や外部の者等による不正アクセス防止等の十分な情報セキュリティ対策を講じることは、教師及び児童生徒が、安心して学校においてICTを活用できるようにするために必要不可欠。

- このことを踏まえ、**各教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考**とするものとして、『教育情報セキュリティポリシーに関するガイドライン』を策定した。（平成29年10月）

- ICT環境が常に進歩を遂げていることから、本ガイドラインについても、他機関の動向、技術的な進展等を踏まえつつ、随時見直しを行う。

地方公共団体における教育情報セキュリティの基本的な考え方

①組織体制を確立すること
- 情報セキュリティの責任体制の明確化
- 首長部局の情報政策担当部局との連携

②児童生徒による重要性の高い情報へのアクセスリスクへの対応を行うこと
- 情報の重要性の度合いごとに、取扱ルールを決定

③標的型および不特定多数を対象とした攻撃等のリスクへの対応を行うこと
- 学校ホームページや教職員によるメールの活用、さらには、学習活動におけるインターネットの活用等が行われていることから標的型及び不特定多数を対象とした攻撃等による脅威に対する対策を講ずること

④教育現場の実態を踏まえた情報セキュリティ対策を確立させること
- 教員が個人情報を外部に持ち出す際のルールの明確化
- 情報システムを教員が扱う際の、遵守すべきルールの整理

⑤教職員の情報セキュリティに関する意識の醸成を図ること
- 研修等の実施

⑥教職員の業務負担軽減及びICTを活用した多様な学習の実現を図ること
- 教育委員会が情報セキュリティの確保を主導することによる教員の業務負担の軽減
- 児童生徒の利用を前提とした、ICTを活用した学習活動への配慮

※ 情報セキュリティポリシーとは「組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書」のこと。

教育情報セキュリティポリシーガイドライン改訂の背景について

【平成29年10月】

- 各教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考とするものとして、『教育情報セキュリティポリシーに関するガイドライン』を策定。

【令和元年12月 ／ 第１回改訂】

- その後、GIGAスクール構想における「1人1台端末」及び「高速大容量の通信環境」を一体とした学校のICT環境整備の推進を受けて、教育情報セキュリティポリシーガイドラインについて改訂（１回目）を実施。

【令和３年５月 ／ 第２回改訂】

- 更に、令和２年に入り、コロナ禍においても子供たちの学びを保障する観点から、当初４年間で整備する予定であった計画を１年間に前倒して、１人１台端末環境の整備を加速させてきたところ。
- これらの急速な学校ICT環境整備の推進を踏まえ、**１人１台端末を活用するために必要な新たなセキュリティ対策**や**クラウドサービスの活用を前提としたネットワーク構成**等の課題に対応するため、**更なる改訂（２回目）を行う**こととする。

今回の改訂ポイント

① 端末整備推進に伴う新たなセキュリティ対策の充実

⇨ 1人1台の学習者用端末における学校内外での日常的な端末の活用や、クラウドサービス活用に向けたID管理などのセキュリティ対策の記述を充実

② 教育情報ネットワークの在り方を明確化

⇨ クラウドサービス活用に伴うセキュリティ対策を実現するため、過渡期としてのローカルブレイクアウト構成や、今後目指すべき校務系/学習系のネットワーク分離を必要としない構成の在り方を明確化

① 端末整備推進に伴う新たなセキュリティ対策

■ 1人1台端末の活用における新たなセキュリティ対策の追加

1人1台端末を利活用するにあたり、**クラウドサービスの日常的な活用**や、**利用するネットワーク・場所にとらわれない**セキュリティ対策が必要となる。そのため、下記の対策について**記述を充実。**

主な対策	概要
クラウドサービス利用における留意点	クラウドサービスの日常的な**活用に必要なネットワーク帯域の確保**や、**クラウドサービス利用における同時接続数**などの留意点を整理。また、クラウドサービス事業者において適切にセキュリティ対策を実施していることを確認するための**契約内容**及び**第三者認証**などの確認内容を充実
Webフィルタリング	児童生徒が端末を利用する際に、**不適切なウェブページの閲覧を防止するための対策**を整理（Webフィルタリングソフト、検索エンジンのセーフサーチ※1、セーフブラウジング※2）
マルウェア※3対策	児童生徒が自分専用の端末を活用する機会が増えることにより、インターネットなど外部からのリスクに直接晒される機会も増えることから、**端末におけるマルウェア対策**について整理
不正ソフトインストール防止	MDM※4などによる**不正ソフトウェアのインストール防止**、**セキュリティ設定の一元管理**、端末の盗難・紛失における**遠隔からの端末のロックやデータ消去などの対策**を整理
モラル教育	1人1台端末整備により、持ち帰り学習も推進することが想定されるため、学校のみならず**家庭で利用する際に保護者によるリテラシー教育の必要性**について追記。また、**学校と保護者の連絡体制を整備**することについて留意点を整理

※1 検索エンジンのセーフサーチ：検索エンジンの検索結果に不適切な情報が含まれる場合に表示させないようにする機能。
※2 セーフブラウジング：ウェブサイト閲覧時に不正なサイトであることが疑われる場合、利用者に対して警告を表示する機能。
※3 マルウェア：コンピュータウイルスなどのコンピュータの正常な利用を妨げたり、利用者やコンピュータに害を成す不正な動作を行うソフトウェアの総称。
※4 MDM (Mobile Device Management) ：「モバイル端末管理」とも呼ばれる端末を管理する仕組み。利用状況の管理、遠隔からの端末ロックなどの機能を有する。

文部科学省Webサイトに、上記※1～4に関するセキュリティ対策を含むOS事業者による端末の安心・安全な活用方法についての解説を掲載し、活用を促進。
https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/mext_01172.html

① 端末整備推進に伴う新たなセキュリティ対策

■1人1台端末及びクラウドサービス活用を前提とした1人1ID化に対する新たなセキュリティ対策の追加

児童生徒一人一人に個別のIDを付与することで、児童生徒の学びを蓄積し、教員やAIによるフィードバックが行われ、個別最適化された学びを提供することが期待できる。一方で、利用する学習用ツールやクラウド上のアプリケーションのID/パスワードに対して安全管理措置を講じなければならない。そのため、**1人1IDにおけるセキュリティ対策について、記述を充実。**

主な対策	概要
ID登録・変更・削除	1人1ID化することにより、**入学/転入、進級/進学、転出/卒業/退学時などのタイミングにおいて個々のID管理**を行うことが必要となるため、これらの管理について整理 こうした**ID管理を日常的に運用**する上で、必要に応じて事業者へ運用を依頼することも想定して**環境整備の段階から運用面を踏まえた準備**の必要性について整理。
多要素認証	CBT（Computer Based Testing：試験における工程を全てコンピュータ上で行う事）などの本人確認を厳格に行う必要がある場合には、ID/パスワードによる基本的な認証だけでなく、指紋/顔/ICカードなどの**複数の要素を組み合わせてなりすまし対策を行う多要素認証**の有効性について整理
シングルサインオン※1	利用するサービスが増加することにより、サービス利用時に都度ID/パスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になる場合の対処方法の一つとして、一度の認証により一定時間は各種サービスにアクセスが行える**シングルサインオンを用いた認証**の効率化について整理

※1 シングルサインオン：「SSO(Single Sign-On)」とも表記される。一度のユーザ認証で複数の異なるサービス認証と利用を可能にする仕組み。

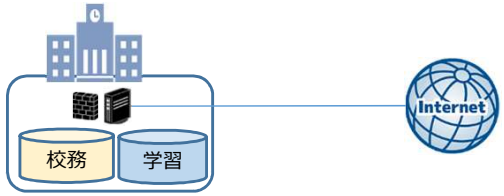
② 教育情報ネットワークの在り方について

■１人１台端末を利活用するにあたり、新たな教育情報ネットワークについて整理

現状のガイドラインに記載していない、一部の通信を直接インターネットへ接続する**ローカルブレイクアウト構成**及びクラウドサービス利活用を前提とし、**ネットワーク分離を必要としない認証によるアクセス制御を前提とした目指すべき構成を明確化。**

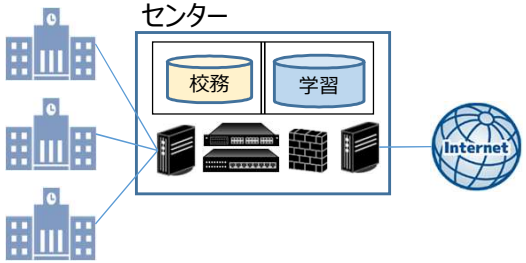
【 現状の構成 】

●学校からインターネット接続



細い回線を利用している場合がある。

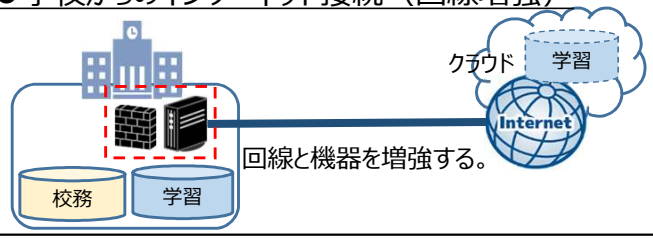
●センター集約接続



様々な個所でネットワークのボトルネックが生じ易い。

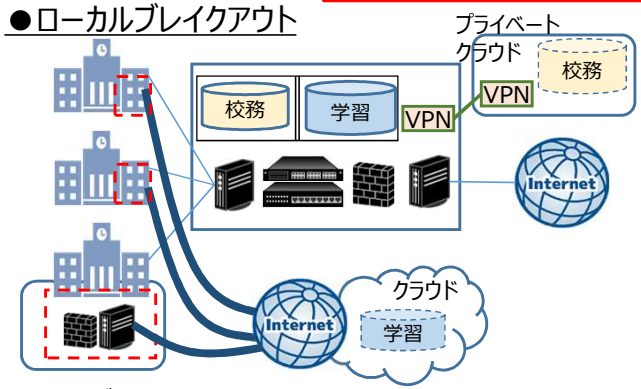
【 過渡期の構成 】

●学校からのインターネット接続（回線増強）



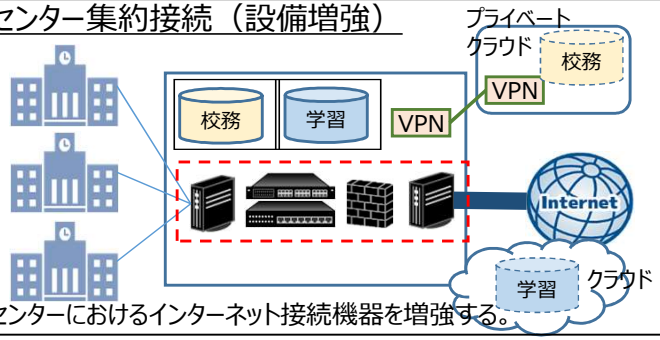
今回新たに追加した内容

●ローカルブレイクアウト



ローカルブレイクアウト構成をとることにより学校にあらたな機器が増えることや、直接インターネットへ接続する接続点が増えるため、これらのセキュリティ対策について整理

●センター集約接続（設備増強）

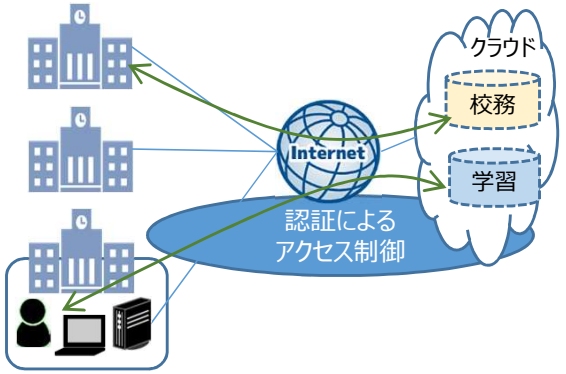


センターにおけるインターネット接続機器を増強する。

【 目指すべき構成 】

今回新たに追加した内容

●ネットワーク分離を必要としない
認証によるアクセス制限を前提とした構成



国や地方自治体全体の動きに合わせて、
教育委員会や学校も、極力設備を持たず、セキュリティ機器なども含めて、クラウド化し、最小限の機器のみ設置することで、利便性向上とコスト削減が可能

ネットワーク分離を必要とせず、端末やネットワークに依存することなく重要性の高い情報へのアクセスには多要素認証の導入や、学習者用端末を学校のアクセスポイントのみに接続を制限するなどの技術的対策、運用体制の整備などの人的セキュリティ対策を合わせて実施することで、十分なセキュリティを確保することが可能

※センター集約接続構成などの既存構成の見直しを行う際には、利便性・セキュリティ構成・コストなどを考慮して今後のネットワーク構成を検討することが重要

その他の改訂内容について①

■情報資産の「持ち出し」「外部送信」ついて内容を適正化

情報資産の「持ち出し制限」「外部送信」により利活用の弊害になっているケースがあったが、今後のデータ活用促進に向けて見直し

情報資産の分類		情報資産の取扱例		
重要性分類	定義	組織外部への持ち出し制限*	端末制限	情報の組織外部への送信**
Ⅰ	セキュリティ侵害が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。	真にやむを得ない場合に限り情報セキュリティ管理者の判断で持ち出しを可	支給以外の端末での作業の原則禁止	暗号化、パスワード設定を行う
Ⅳ	影響をほとんど及ぼさない。			

【改訂内容】
本ガイドラインに準拠していることを確認した上で業務遂行上必要な場合には、情報セキュリティ管理者の判断で持ち出しを可

⇒　従来の表現では実質禁止と捉えられているケースもあったため、今後のデータ活用に向けて、ガイドラインに準拠していることを前提としたうえで、利活用が可能となるよう表現を適正化。

【改訂内容】
（クラウドストレージなどの）限定されたアクセスの措置がとられていること

⇒　データ送信においては限定されたアクセス措置をとることができるクラウドストレージなどの利用を利用することを想定。
今般、電子メールにより添付ファイルを送信する際に、パスワード付きファイルを送信し、2通目にパスワードを送付する方法は推奨されない対策となるためこの方法を見直し。

その他の改訂内容について②

■クラウドサービス活用における個人情報保護に関する確認事項について追加

今般の法改正により、地方公共団体の個人情報保護制度について、全国的な共通ルールを規定し、公的部門を含めて全体の所管を個人情報保護委員会に一元化することとになった（施行は令和５年春頃が見込まれる。）。改正法においては、いわゆる「オンライン結合制限」に相当する規定は設けず、今後その解釈が示される安全管理措置や利用・提供の制限に係る規定等により、個人情報の安全性を確保することとされている。

しかしながら、**現状の地方公共団体における個人情報の取り扱いに関しては、地方公共団体ごとに定められた個人情報保護条例に準拠**する必要があり、クラウドサービスを活用して個人情報を取り扱う場合には、個人情報保護審議会へ諮問答申を得ることが必要な自治体も多い。

そのため、クラウドサービスにて個人情報を取り扱う際に**個人情報保護審議会に諮る上で整理すべき主な項目例を整理。**

項目例
(1) クラウド活用の目的
(2) システムの対象範囲
(3) 本人(保護者)同意の要否
(4) セキュリティリスクに対する技術的対策
(5) インシデント発生時の責任分界点の明確化（クラウド事業者側の体制含む）
(6) クラウド事業者の二次利用に対する対策※
(7) クラウド事業者の第三者認証取得の有無

なお、上述のとおり個人情報保護条例は自治体ごと規定されており、個人情報保護審議会への諮問の要否及び、求められる項目はそれぞれ異なるため、確認が必要。

【参考：自治体の事例】 ※上記（1）～（7）のうち、以下の項目がそれぞれ必要

・A自治体：(1)目的、(4)技術的対策、(5) 責任分界点明確化、(7)第三者認証、(その他)管轄裁判所/準拠法
・B自治体：(1)目的、(2)対象範囲、(4)技術的対策、(6)事業者の二次利用に対する対策
・C自治体：(1)目的、(4)技術的対策、(7)第三者認証
・D自治体：(2)対象範囲、(3)保護者同意、(6)事業者の二次利用に対する対策、(7)第三者認証

※ クラウドサービス事業者が、同意なく学習ログなどの情報資産を利用しないよう、その対策についても確認が必要。

「教育情報セキュリティポリシーに関するガイドライン」の全般的な内容

■クラウドサービス活用における第三者認証

クラウドサービスを利用する場合は、扱う情報資産の重要性に応じた情報セキュリティ対策が講じられていることを利用者側が確認することが重要。クラウド事業者の選定においても、求める内容に応じた認証規格を参考にすることで、クラウド事業者の責務と対策を履行できる能力を持ち、情報セキュリティの確保等が適切に行われていると判断することが可能である。これらの取得・準拠の状況を踏まえ、クラウドサービスのセキュリティ対策・内容等を確認していくことが、円滑な導入に有効である。

＜認証制度の例＞

・ISO/IEC 27001(情報セキュリティマネジメントシステム)
・ISO/IEC 27002(情報セキュリティマネジメントシステム)
・ISO/IEC 27014(情報セキュリティガバナンス)
・ISO/IEC 27017(クラウドサービスの情報セキュリティ)
https://isms.jp/isms-cls/lst/ind/index.html
・ISO/IEC 27018（クラウドサービスにおける個人情報の取扱い）
・米国FedRAMP
https://marketplace.fedramp.gov/#/products?status=Compliant
・AICPA SOC2（日本公認会計士協会 IT7号）
・AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会 IT2号）
・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/
・ASP・SaaS安全・信頼性に係る情報開示認定

■クラウドサービス提供元のセキュリティ確認

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ものだけでなく、インフラ基盤をIaaS事業者から供給を受けて、アプリケーションをSaaSとして提供する事業者も存在する。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、SaaS事業者が適切なセキュリティレベルを確保していることを確認する必要がある。（IaaS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、SaaS事業者の委託作業の中でセキュリティインシデントが発生すると、データの流出が発生したり、データにアクセスできなくなったりする可能性がある。）

また、その確認作業においては、クラウドサービスの情報セキュリティの実態を、クラウド利用者自らが詳細に調査することは困難であることから、第三者による認証や各クラウドサービス事業者が提供している監査報告書を利用することが重要である。

地方公共団体の個人情報保護制度の在り方（改正の方向性）

＜地方公共団体の個人情報保護制度に求められるもの＞

1　社会全体のデジタル化に対応した「個人情報保護」と「データ流通」の両立

※ いわゆる「２０００個問題」
①団体ごとの規定・運用の相違が、データ流通の支障となりうること
②条例がないなど、求められる保護水準を満たさない団体があること
等への問題提起がなされている

2　個人情報保護に関する国際的な制度調和と我が国の成長戦略への整合

例）・EUにおけるGDPR（一般データ保護規則）十分性認定
・G20大阪首脳宣言におけるDFFT（信頼ある自由なデータ流通）

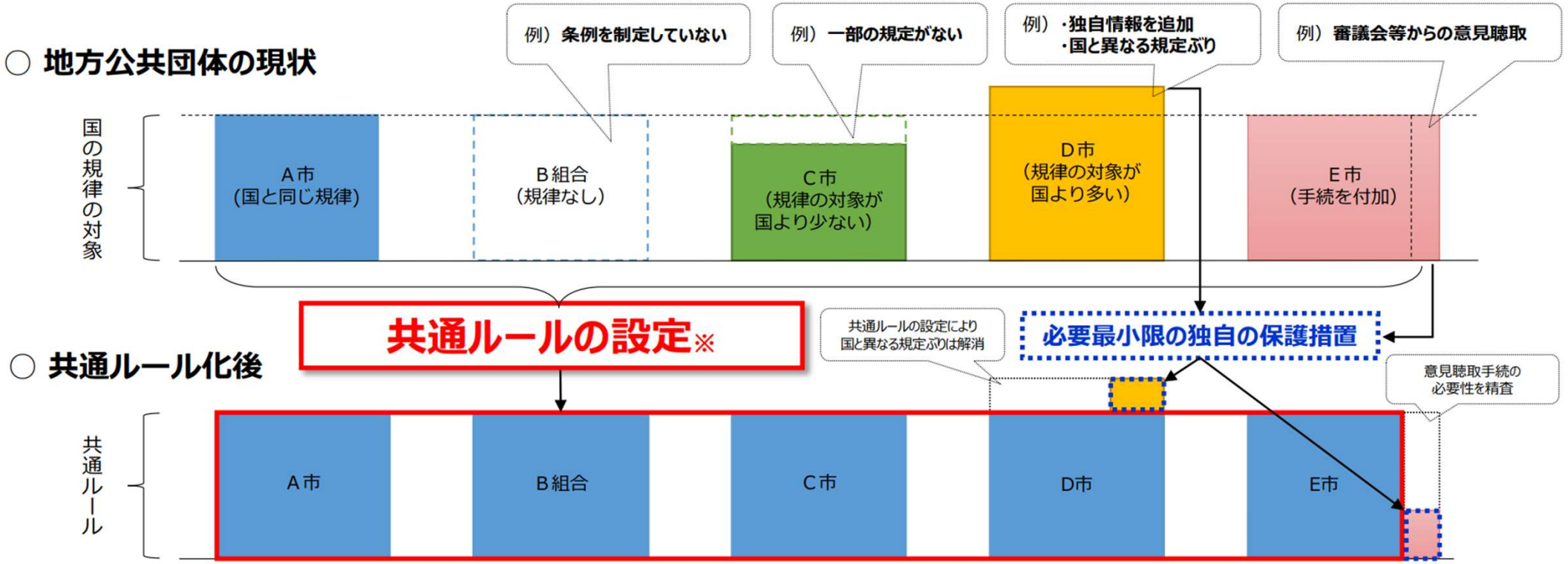
＜改正の方向性＞

○　「個人情報保護」と「データ流通」の両立に必要な全国的な共通ルールを法律で設定

○　法律の的確な運用を確保するため、国がガイドラインを策定

○　その上で、法律の範囲内で、必要最小限の独自の保護措置を許容　⇒条例を個人情報保護委員会に届出

例）・「条例要配慮個人情報」として保護する情報を規定
・個人情報の適切な取扱いを確保するため、特に必要な場合に限り審議会等からの意見聴取手続を規定



（内閣官房「個人情報保護制度の見直しに関する最終報告（概要）」（令和２年12月　個人情報保護制度の見直しに関するタスクフォース）より引用）

主な質問について

■主な質問について

質問	回答
学習系システムにて個人情報を扱って良いのか。	児童生徒が学習活動を通して生み出す学習系情報の中にも、氏名、性別、学年といった属性情報を置くことは自然なことであり、様々な学習系ツールの利用場面も含めて、これらの属性情報について学習系システムの中において扱うことを一義的に禁止するものではない。活用場面等に応じて、実態に即した形で運用すること。例えば学習活動において、動画や写真等を取り扱う際には、適切なアクセス権限を設定すること。
ログは個人情報に該当するのか。	個人情報は一般的に「個人に関する情報であること」「特定の個人を識別できること」であり、取得するログが一概に個人情報に該当するかどうかを断定はできない。個人情報の取り扱いについては各自治体の個人情報保護条例に準拠する必要があるため、必要に応じて個人情報担当へ確認すること。
多要素認証は必須か。	校務の情報を取り扱う端末においては多要素認証を求めているが、学習者用端末においてはCBTなど厳格な本人確認が求められる場合において有効であると考えている。
教員のテレワーク等の情報漏えい対策はどうすれば良いか。	端末側にデータを保存しない運用を徹底する。もしくは、端末側にデータを保存するのであれば端末に対する「ウイルス対策」、「暗号化対策」、「ふるまい検知の対策」、「フィルタリング」などの対策を想定している。
データの授受についてはメール利用が前提となるのか。	適切なアクセス権限を設定したクラウドストレージによるデータ授受でも問題ない。
学習系・校務系含めて、直ぐに目指すべき構成にシステムを更改しなければならないのか。また、いつまでに実現すれば良いのか。	センター集約接続構成などの既存構成の見直しを行う際には、利便性・セキュリティ構成・コストなどを考慮して今後のネットワーク構成を検討することが重要。

チェックリストとの関連について

■GIGA スクール構想 本格運用時チェックリスト（情報セキュリティ関連）

	チェック項目	意見
A管理運用	⑥ セキュリティ問題やネット利用に関するトラブルが発生した際の問合せ先、相談先を、教職員・保護者・児童生徒にわかるように示しているか	**とても大事なことである。 首長部局のCSIRT（セキュリティ対策チーム）にPOC（連絡窓口）という機能があるように、教育委員会内部でもトラブルの早期発見・早期対応が出来るよう、相談先を決めて、関係者全員に周知すべきである**
Bクラウド利用	②セキュリティポリシーや個人情報の取扱いなどが、クラウドサービスの利用に適したものになっているか	**個人情報保護条例との兼ね合いで、利用が進められない自治体もある 首長部局の担当者と相談の上、教育現場に負担のない利用ルールを考えるべきである**
	③１人１アカウント（ID）の命名規則を定め、発行し、パスワードとともに児童生徒に配付しているか	**相変わらず「〇年△組×番」の規則でＩＤを割り振ってしまうきらいがある。進級や場合によっては自治体内転校であっても使い続けられる規則とすべき また、SSO（シングルサインオン）ツールは利便性の観点より導入を検討して頂きたい**
	⑤セキュリティ機器や無線アクセスポイントなどのネットワーク機器を、端末の円滑な活用を妨げることがないように導入・設定しているか	**様々な機器やサービスをやみ雲に追加すると、管理の支障となるばかりか、トラブルが起きた際の解決に時間が掛かることとなる。運用管理の頭を取る事業者を決めて、追加の際には事業者の意見を参考にする**
	⑥複数クラスの児童生徒が同時活用しても、学校からインターネットへの接続に支障はないか	**「教育情報セキュリティポリシーに関するガイドライン」の第2回改訂で追加されたローカルブレイクアウトを検討することや、ネットワーク環境を常に監視し、専門的知見を入れつつ、良好な環境を目指すことが重要である**
追加	「Ｅ組織・支援体制」に「自治体（学校設置者）の情報化担当者と意思疎通が図れているか」	**個人情報保護制度は改正されたが、施行は令和５年春頃が見込まれるため、現状の個人情報の取り扱いに関しては、地方公共団体ごとに定められた個人情報保護条例に準拠する必要がある。そのため、現時点から首長部局の担当者と情報交換を行う必要があると考える**