別紙

項目	主な意見の内容	文部科学省の考え方
組織体制	教育情報システム担当者は校務分掌として担当を職員から配置すると記載されているが、業務負荷の軽減と質の向上を目的として、外部人材(例えば ICT 支援員)に業務を委託するなどの措置をとれるように記載をいただきたい。	御指摘を踏まえ、2.2(6)の(解説)に(注10)を追記し、外部人材の活用の可能性についても言及いたします。
物理的セキュリティ	地方や小さな自治体ではサーバ設置や管理に関して情報不足から水準以上の対策を行うことが難しい場合があるため、セキュリティ対策を一定レベルの水準で実施するには、専門業者のデータセンターやクラウドサービスを用いることも有用だと考える。	本ガイドライン全体を通して、データセンターやクラウドサービスを使うことは否定していません。利用については、各自治体において御判断いただきたいと考えています。
	二要素認証の例として指紋認証のみが記載されているが、本人認証を厳密に行うことが本来の意図であり、特定の認証方式に限定するような表現は望ましくないと考える。	御指摘を踏まえ、2.4.4④を修正いたします。
	日常的に機微な情報を取り扱うこと、庁舎と比較し、学校は第三者が立ち入り易い環境にあることなどを踏まえ二要素認証の実施について、推奨事項となっているが、必須にすべき。	本ガイドラインにおいては地方公共団体の実態等も踏まえ、二要素認証の導入は必須事項とはしておりません。
	学習者用端末についてもモバイル端末と同様に持ち出しが可能となるため、校務用端末と同様の、二要素認証や遠隔消去機能などのセキュリティ対策がとれる端末を選択することとすべきと考える。	学習系システムは、機微情報が保管される校務系システムから論理的又は物理的に分離することを前提としているため、学習用端末への二要素認証や遠隔消去機能の導入は、推奨事項としても記載しておりません。
人的セキュリティ	パスワードを定期的に変更することで、むしろセキュリティが低下するという懸念もある。	パスワードの定期的変更の是非については専門家の中でも見解が異なっていることから、引き続き、自治体におけるパスワードの運用実態及び技術的動向等も勘案しながら、必要に応じて見直しを行うこととします。

技術的セキュリティ	近年のサイバー攻撃は複雑、巧妙化しており、パターンファイルによる不正プログラム対策ソフトウェアでは検知出来ない攻撃が頻発しているため、感染原因や感染範囲の特定を迅速に行うことが出来るソフトウェアを導入する必要がある点についても、追記すべき。	御指摘を踏まえ、2.6.4.（解説)(1)（注 3)を追記いたします。
外部サービスの利用	クラウドサービスを活用する際に、セキュリティレベルが確保されているか判断することは難しいため、明確な判断基準を示してはどうか。	インターネットを介したクラウドサービスの利用における留意点については、文部科学省が平成29～31年度に、総務省と連携して実施することとしている「次世代学校支援モデル構築事業」において検討し、本ガイドラインの記述に反映する予定です。
その他	情報セキュリティの対策が重要なのは、疑いないが、セキュリティ確保を無制限で取り組んでは、費用が掛かり過ぎるため、クラウド化の推奨など、価格低減につながる具体策を明確に出していただきたい。	本ガイドラインの対策事項については、各自治体において標準的に対策することが望まれる事項と、各自治体において、必要性の有無を検討し、必要性が認められる時に選択的に実施することが望まれる「推奨事項」に区別して記載しています。 また、物理的セキュリティや技術的セキュリティ等の一部の対策事項については、ソフトウェアの調達等が新たに必要となる場合も考えられますが、クラウドサービスの活用を含め、具体的にどのような手段（商品、サービス等）を活用するかは、各自治体の判断に委ねられています。 各自治体においては、本ガイドラインを参考にしつつ、各自治体の実態も踏まえながら、適切な手段（商品、サービス等）の活用をご検討いただければと思います。