学校情報セキュリティ推奨仕様

第 1.0 版

財団法人コンピュータ教育開発センター

平成 22 年 3 月 31 日

目次

はじめに

学校情報セキュリティ推奨仕様（以下，「本推奨仕様」という。）は，幼稚園，小学校，中学校，高等学校，特別支援学校等の教育現場（以下，「学校」という。）および教育委員会等の学校運営の主体となっている組織[1]（以下，「教育委員会等」という。）で扱われる児童・生徒，教職員ならびに臨時職員（以下，「教職員」という。），保護者，学校ボランティア等を含む学校関係者（以下，「学校関係者」という。）の電子化された個人情報（以下，「学校教育データ」という。）の漏えい防止に主眼をおいて，最低限導入されることが望まれるセキュリティ対策と，よりセキュリティを高めるために推奨される対策を明らかにしたものである。

学校で扱われる情報資産の中で最も高度なセキュリティが要求される情報資産は「学校教育データ」(p.3 参照)であり，その価値は児童・生徒や学校が異なろうと等価に扱われるべきものと考えられる。
学校における情報セキュリティの確保は，各自治体や教育委員会等あるいは個々の学校が主体となってリスク分析を行い，想定されるリスクを許容範囲内とするために必要と判断されたセキュリティ対策が導入されることで実現される。

しかしながら，重要な情報資産として扱われるべき「学校教育データ」が，十分なセキュリティの下におかれているケースもあればリスクの高い状態におかれているケースがあるのが実態である。こうした背景には，必ずしも情報資産の洗い出しやリスク分析が実施されていない，あるいは，リスク分析を実施しても，専門的な知見が得られないためにリスクを十分に低減するためにどのような対策を導入すべきかの適切な判断ができないという事情がある。

「教育の情報化」は，時間的・空間的制約から学びを解放し，学びの手段を拡大し，教育や校務の効率化だけでなく質を高める効果が期待できる。ところが，現状の意識，慣習，体制および技術では，これまでにない情報漏えいのリスクが顕在化している。今後，一学校内に限らず，学校間，地域間の電子データ交換へと発展する効果は大きいが，反面，情報漏えいリスクが高まることも懸念される。しかしながら，適正な対応をとることによって，そのリスクは格段に軽減できる。

本推奨仕様は，「学校教育データ」を扱う上で必要となるセキュリティ水準を確保するために実施することが推奨される対策（ベースラインセキュリティ）を要求事項として示したものである。本推奨仕様が達成されることで安心・安全な学校間のデータ連携が実現するだけでなく，安心・安全な情報環境が提供されることで教職員を情報漏えい事故から守り，快適な遠隔利用を可能とするなど，学校教育の改善に寄与することが期待される。

[1] 教育委員会ほか，教育センター，大学附属学校運営委員会・大学事務局，学校法人理事会等を指す

概要

学校情報セキュリティ推奨仕様は，学校教育データのセキュリティを強化し保護するため，さらにすべての学校教育に携わる組織に対する推奨仕様の周知・徹底を促進することを目的として作成した。

本推奨仕様では，学校教育に携わる組織および当事者を，その役割に応じて 3 種類に分け，「学校の管理者（教育委員会等および校長）編」，「教職員編」，「システムの開発，構築，運用者編」として，各々の役割に求められる要件をとりまとめている。

対象となる学校教育データ

次の表は，保護の対象となる児童・生徒，教職員および臨時職員（以下，「教職員」という。），保護者，学校ボランティア等を含む学校関係者（以下，「学校関係者」という。）のデータを含む，学校教育データの一般的な構成要素と各データ要素を保護する必要があるかどうかを示している。

	データ分類	データ要素	摘要
学校教育データ	基本データ	個人識別データ [1)]	学籍番号，教職員番号等
		氏名 [1)]	
		住所 [2)]	
		生年月日 [2)]	
		性別 [2)]	
	センシティブデータ [4)]	機微情報 [3)]	身体の特徴，傷病履歴等
		その他の要保護情報 [3)]	進路情報，成績等

1) これらのデータ要素のいずれか一方，あるいはその両方を含むデータを学校教育データとし，本推奨仕様における保護対象とする。
2) これらのデータ要素は，1)のデータとともに保有される場合は基本データに含まれる。
3) これらのデータ要素は，基本データとともに保有される場合は保護が必要である。この保護は，学校教育データ環境の全般的な保護に関する本推奨仕様の要件に従う。
4) センシティブデータのみによって個人が識別される恐れがある場合には，当該データが基本データを含まない場合においても学校教育データとみなすことがある。

適用範囲

本推奨仕様の要件は，すべての学校教育データ環境に適用される。すべての学校教育データ環境とは，学校教育データを保管・処理・伝送するシステムコンポーネントならびにネットワークコンポーネントから構成される。

システムコンポーネントは，サーバとアプリケーションから構成される。サーバには，Web サーバ，アプリケーションサーバ，データベースサーバ，認証サーバ，メールサーバ，プロキシサーバ，ネットワークタイムプロトコル（NTP）サーバ，ドメインネームシステム（DNS）サーバなどが含まれる。アプリケーションには，内部および外部（インターネット）アプリケーションなど，すべての市販およびカスタムアプリケーションが含まれる。ネットワークコンポーネントには，ファイアウォール，スイッチ，ルータ，無線アクセスポイント，ネットワーク機器，セキュリティ機器などが含まれる。

学校の管理者編

本編では，教育委員会等および校長をはじめとする学校の管理者の遵守事項について規定している。

1. 情報セキュリティのための組織

1.1. 教育委員会等ならびに校長は，学校内のセキュリティについて，次のことを実施すること。

(a) 学校の情報セキュリティ目標の共有
(b) 情報セキュリティ方針の明確化
(c) 各教職員の役割や責任の明確化
(d) 情報セキュリティに関する意識を維持するための計画策定

1.1.1. 次を実現するセキュリティポリシーを確立，維持および周知すること。

(a) 本推奨仕様のすべての要件に対応する。
(b) 脅威，脆弱性を特定し,1 年に 1 回のプロセスをリスク評価に含める。
(c) 1 年に 1 回の見直しを含め，環境の変化に合わせて更新する。

1.1.2. セキュリティに関する認識を高めるために，啓発活動を実施して，すべての教職員が学校教育データセキュリティの重要性を認識するようにすること。

(a) 赴任時および少なくとも 1 年に 1 回教職員を教育する。
(b) セキュリティポリシーおよび手順に目を通して理解したことについての同意を，少なくとも 1 年に 1 回教職員に求める。

1.1.3. 情報セキュリティにかかわる事件・事故対応計画（以下，「インシデント対応計画」という）を導入し，セキュリティ侵害に直ちに対応できるよう準備すること。

(a) セキュリティ侵害が発生した場合に実施されるインシデント対応計画を作成する。計画では，最低限，次の事項に対応する。
・関係機関への通知を含む，侵害が発生した場合の役割，責任および伝達と連絡に関する手続き
・具体的なインシデント対応手順
・復旧および継続手順
・データバックアッププロセス
・すべての重要なシステムコンポーネントを対象とした対応
・関係機関によるインシデント対応手順の遵守
(b) インシデント対応計画を少なくとも 1 年に 1 回試行する。
(c) 警告に 24 時間体制で対応できる担当者を指定する。
(d) セキュリティ侵害への対応を担当する管理職および担当者に適切なトレーニングを提供する。
(e) 侵入検知，侵入防止およびファイル完全性監視システムからの警告への対応演習を行う。
(f) 得られた教訓を踏まえてインシデント対応計画を変更および改善する。

1.2. 教育委員会等の内部および学校内に情報セキュリティに関する委員会を設置し，関係するセキュリティ情報を最新に保つために，専門家から情報セキュリティに関する助言を得るようにすること。

1.2.1. 新たに発見された脆弱性を特定するためのプロセスを確立すること（インターネット上で入手可能な警告サービスに加入するなど）。新たな脆弱性の問題に対処するために，設定を適正化すること。

2．情報資産

2.1. 学校内のすべての情報資産を洗い出し，その資産の重要度を記録した情報資産目録を作成すること。また，各々の情報資産の管理責任者を指定すること。

2.1.1. データの保管と廃棄に関するポリシーを作成すること。データ保管ポリシーにおいて，保管するデータ量と保管期間を，業務上，法令上，規則上必要な範囲に限定すること。保管期間を過ぎたデータは，少なくとも 1 年以内に廃棄されるようにすること。

3．教職員のセキュリティ

3.1. 学校教育データを取扱う者は，情報セキュリティに関する責任を記載した誓約書に同意・署名すること。

3.2. セキュリティ違反を犯した教職員には懲戒処分などの手続をとること。

3.3. すべての教職員の情報および情報処理施設に対するアクセス権は，雇用終了時および勤務校変更時に見直し，必要であれば削除すること。

4．ネットワークやソフトウェアの運用管理

4.1. セキュリティ確保のための操作手順を文書として作成すること。変更する場合は管理者である校長が認可すること。

4.1.1. 本推奨仕様と整合する日常的な運用上のセキュリティ実施手順を作成すること（例えばユーザアカウント保守手順，ログレビュー手順）。

4.1.2. 教職員に公開されている重要な技術（リモートアクセス，無線，リムーバルメディア，パソコン，携帯情報端末（PDA），電子メール，インターネットなど）の使用に関するガイドラインを作成して，すべての教職員にこれらの技術の適切な使用を徹底すること。

4.2. コンピュータやサーバ，周辺機器，ネットワーク等の設備およびシステムの変更については，担当者が記録，テスト，アセスメントなどを行い確実に管理すること。

4.2.1. システムコンポーネントへのすべての変更において，変更管理手順に従うこと。手順には次の事項を含めること。

(a) 変更が与える影響の文書化

(b) 適切な管理者による変更の承認
(c) 運用機能のテスト
(d) 回復手順

4.2.2. 外部および内部のペネトレーションテストを少なくとも構築時および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード，サブネットワークの追加， Web サーバの追加など）後に実行すること。これらのペネトレーションテストには次の事項を含めること。
(a) ネットワーク層のペネトレーションテスト
(b) アプリケーション層のペネトレーションテスト

4.3. 気づかれない状態で，利用者が情報資産に不正にアクセスできないように，担当者の職務および責任範囲を分割すること。

4.3.1. 教育委員会等内および学校内で，個人またはチームに次に示す情報セキュリティ管理責任を割り当てること。
(a) セキュリティポリシーおよび手順を確立，文書化および周知する。
(b) セキュリティに関する警告および情報を監視して分析し，該当する担当者に通知する。
(c) インシデントの対応および報告手順を確立，文書化および周知して，あらゆる状況をタイムリーかつ効果的に処理する。
(d) 追加，削除，変更を含め，ユーザアカウントを管理する。
(e) データへのすべてのアクセスを監視および管理する。

4.4. 第三者が提供するサービス，報告および記録は，情報セキュリティの条件の遵守を確実にするため，常に監視し，レビューすること。

4.4.1. 学校教育データを業務委託先と共有する場合は，業務委託先を管理するための手順を確立し，維持すること。手順には，次の事項を含める。
(a) 業務委託先の一覧表を維持する。
(b) 学校教育データのセキュリティに対して業務委託先が責任を負うことに同意した，書面での契約を維持する。
(c) 契約前に調査を実施することを含め，業務委託先との契約に関する手順を確立する。
(d) 本推奨仕様の準拠状況について，業務委託先を監視する手順を維持する。

4.5. 情報管理者は，新しいシステムを受け入れるための要求事項および基準を明確にし，合意し，文書化し，試験すること。

4.6. ネットワーク管理者は，管理策を定めネットワークにおける情報のセキュリティ確保や無認可のアクセスからのネットワークの保護を確実に行うこと。

4.7. 情報処理設備の使用状況を監視する手順を確立し，監視活動の結果をレビューすること。

5．法令の遵守

5.1. 知的財産を保護するために，次の指針を考慮すること。

(a) 正規の製品を入手するために，ソフトウェアは知られた定評のある供給元を通して取得する。

(b) 許諾された最大利用数を越えない。

(c) その他，知的財産に関するものについては関係法令を遵守する。

5.2. 個人データおよび個人情報の保護に関する教育委員会等および学校の方針を確立して実施すること。

（学校の管理者編　以上）

教職員編

本編では，臨時職員を含む教職員の遵守事項について規定している。

1．情報資産

1.1． 情報資産目録を最新の状態に維持すること。

1.1.1．保管する学校教育データは最小限に抑える。データ保管ポリシーに従って，データの管理を行うこと。

1.2． ラベル付け等を行い，学校教育データを識別できるようにすること。

2．教職員のセキュリティ

2.1． 教職員は，学校のセキュリティポリシーに従って行動すること。また，認可されていないアクセス，認可されていない開示，改ざん，破壊または妨害から資産を保護すること。

2.1.1．個人識別データを表示する際は必要最低限にすること。

2.1.2．すべてのデータ保管場所（パソコン，USB 等の電子媒体，バックアップ媒体，ログを含む）で学校教育データの不正な閲覧を防止すること。

2.1.3．学校教育データを電子メール等で送信しないこと。

2.2． 学校教育データを取扱う者は，情報セキュリティに関する責任を記載した誓約書に同意・署名すること。

2.3． すべての教職員は，雇用終了時および勤務校変更時に，前もって支給されたソフトウェア，書類，設備のすべてを返却すること。

3．ハードウェアや環境のセキュリティ

3.1. コンピュータや周辺機器は，認可されていないアクセスを回避し，盗難・火災などのリスクを最小限に抑えるように設置し，管理すること。

3.2. 学校教育データが保管されている装置は，廃棄する前に物理的に破壊するか，または確実に上書きをしてデータを消去すること。

3.2.1. 次のように教務・校務または法令上の理由で不要になった学校教育データを含む媒体を破棄すること。
(a) 学校教育データを再現できないよう，ハードコピー資料を裁断，焼却または溶解する。
(b) 学校教育データを再現できないよう，電子媒体上の学校教育データを回復不能にする。

3.3. コンピュータやデータ，ソフトウェアは，指定場所から校長の認可なしには持ち出さないこと。持ち出し時および返却時には記録を残すこと。

3.3.1. 学校教育データが保管されたあらゆる種類の媒体の内部または外部での配布に関して，次の事項を定めること。
(a) 秘密であると識別できるように媒体を分類する。
(b) 安全な配達業者または正確に追跡できるその他の配送方法によって媒体を送付する。

4．アクセス制御

4.1. 教職員がパスワードの選択および使用を行う際には，「パスワードを秘密にしておく」「紙に記録して保管しない」「定期的に変更する」などの正しいセキュリティ慣行に従うこと。

4.1.1. すべてのシステムコンポーネントで，次のようにパスワード管理を確実に行うこと。
(a) グループ，共有，またはデフォルトのパスワードを使用しない。
(b) 少なくとも 90 日ごとにユーザパスワードを変更することが望ましい。
(c) 7 文字以上のパスワードを使用する。
(d) 数字と英文字の両方を含むパスワードを使用する。

4.2. 教職員が，コンピュータを用いる場合は，物理的保護，アクセス制御，暗号技術，バックアップおよびウィルス対策についての方針を定めた重要技術の使用ポリシーを遵守すること。

4.2.1. インターネットに直接接続するすべてのモバイル端末または教職員使用のコンピュータ、あるいはその両方で校内ネットワークへのアクセスに使用されるものに，パーソナルファイアウォールソフトウェアをインストールすること。

4.2.2．パソコンに，アンチウィルスソフトウェアを導入すること。

すべてのアンチウィルスソフトウェアは，すべての既知のタイプの悪意のあるソフトウェアに対して検知，駆除，保護が可能でなければならない。

4.2.3．すべてのアンチウィルスメカニズムが最新で，有効に実行されており，監査ログが生成できること。

5．法令の遵守

5.1．知的財産を保護するために，次の指針を考慮すること。

(a) ソフトウェアは知られた定評のある供給元を通して取得する。

(b) 書籍，記事，報告書またはその他の文書を違法に複写しない。

5.2．個人データおよび個人情報の保護に関する教育委員会等と学校の方針および法令を遵守すること。

（教職員編　以上）

システムの開発，構築，運用者編

本編では，
学校外部の業務受託者を含むシステムの開発，構築，運用者の遵守事項について規定している。

1．教職員のセキュリティ

1.1. 教職員は，学校の情報セキュリティ基本方針に従って行動すること。また，認可されていないアクセス，認可されていない開示，改ざん，破壊または妨害から資産を保護すること。

1.1.1. 個人識別データを表示する際は必要最低限にすること。

1.1.2. すべてのデータ保管場所（パソコン，USB 等の電子媒体，バックアップ媒体，ログを含む）では学校教育データを暗号化するとともに，不正な閲覧を防止すること。

1.1.3. 学校教育データの暗号化に使用される暗号鍵を漏えいと誤使用から保護すること。
- **(a) 暗号鍵へのアクセスを必要最小限の管理者に制限する。**
- **(b) 暗号鍵の保管場所を最小限にし，安全に保管する。**

1.1.4. 学校教育データの暗号化に使用される暗号鍵の管理プロセスおよび手順をすべて文書化し，実装すること。これには，次の事項を含むこと。
- **(a) 強力な暗号鍵の生成**
- **(b) 安全な暗号鍵の配布**
- **(c) 安全な暗号鍵の保管**
- **(d) 暗号鍵管理手順で，少なくとも年 1 回の定期的な暗号鍵の変更の要求**
- **(e) 古い暗号鍵または危険にさらされた疑いのある暗号鍵の破棄または取替**
- **(f) 暗号鍵の知識分割と二重管理**
- **(g) 暗号鍵の不正置換の防止**
- **(h) 暗号鍵管理者が自身の責務を理解し，それを受諾したことを示す書面への署名**

1.2. 学校教育データを取扱う者は，情報セキュリティに関する責任を記載した誓約書に同意・署名すること。

1.3. すべての教職員の情報および情報処理施設に対するアクセス権は，雇用終了時および勤務校変更時に見直し，必要であれば削除すること。

2. ハードウェアや環境のセキュリティ

2.1. コンピュータや周辺機器は，認可されていないアクセスを回避し，盗難・火災などのリスクを最小限に抑えるように設置し，管理すること。

2.1.1. 適切な施設入館管理を実施して，学校教育データ環境内のシステムへの物理アクセスを制限および監視すること。

(a) ビデオカメラやその他のアクセス管理設備を使用して,機密情報エリアへの個々の物理アクセスを監視する。収集されたデータを確認し，その他の記録と相関付ける。入退出に関する記録は、法令によって別途定められていない限り，少なくとも 3 カ月間保管する。

注: "機密情報エリア" とは，データセンタ，サーバルーム，学校教育データを保管，処理，または伝送するシステムが設置されているエリアのことである。

(b) 情報コンセントへの物理アクセスを制限する。

(c) 無線アクセスポイント，ゲートウェイおよびモバイル端末への物理アクセスを制限する。

2.1.2. 学校教育データにアクセス可能なエリアでは，教職員と訪問者を容易に区別できるような手順を開発すること。

2.1.3. すべての訪問者が次のように処理されることを確認すること。

(a) 学校教育データが処理または保管されているエリアに入る前に承認が行われる。

(b) 訪問者を教職員と区別する有効期限が設定されている物理トークン（バッジ，IC カードなど）が与えられる。

(c) 施設を出る前，または有効期限の切れる日に物理トークンを回収する。

2.1.4. 訪問者の行動の記録を保持すること。訪問者の名前，所属，物理アクセスを承認した教職員を記録すること。法令によって別途定められていない限り，この記録を少なくとも 3 カ月間保管すること。

2.2. 学校教育データが保管されている装置は，廃棄する前に物理的に破壊するか，または確実に上書きをしてデータを消去すること。

2.2.1. 次のように教務・校務または法令上の理由で不要になった学校教育データを含む媒体を破棄すること。

(a) 学校教育データを再現できないよう，ハードコピー資料を裁断，焼却，または溶解する。

(b) 学校教育データを再現できないよう，電子媒体上の学校教育データを回復不能にする。

2.3. コンピュータやデータ，ソフトウェアは，指定場所から校長の認可なしには持ち出さない。必要かつ適切な場合に限り，校長の許可を経て持ち出す。その際持ち出し時および返却時に記録を残すこと。

2.3.1. 学校教育データが保管されたあらゆる種類の媒体の内部または外部での配布に関して，次の事項を含め，厳格な管理を維持すること。

(a) 秘密であると識別できるように媒体を分類する。

(b) 安全な配達業者または正確に追跡できるその他の配送方法によって媒体を送付する。

2.3.2. 安全なエリアから移動される学校教育データが保管されたすべての媒体を管理者が承認するようにすること。

3. ネットワークやソフトウェアの運用管理

3.1. セキュリティ確保のための操作手順を文書として作成すること。変更する場合は管理者である校長が認可すること。

3.1.1. 本推奨仕様と整合する日常的な運用上のセキュリティ手順を作成すること（例えばユーザアカウント保守手順，ログレビュー手順）。

3.2. コンピュータやサーバ，周辺機器，ネットワーク等の設備およびシステムの変更については，担当者が記録，テスト，アセスメントなどを行い確実に管理すること。

3.2.1. システムコンポーネントへのすべての変更において，変更管理手順に従うこと。手順には次の事項を含めること。
(a) 変更が与える影響の文書化
(b) 適切な管理者による変更の承認
(c) 運用機能のテスト
(d) 回復手順

3.2.2. 内部および外部ネットワークの脆弱性検査を少なくとも 3 ヵ月に一度，かつネットワークの大幅な変更（新しいシステムコンポーネントのインストール，ネットワーク構成の変更，ファイアウォール規則の変更，製品アップグレードなど）後に実行すること。

3.2.3. 外部および内部のペネトレーションテストを少なくとも構築時および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード，サブネットワークの追加， Web サーバの追加など）後に実行すること。これらのペネトレーションテストには次の事項を含めること。
(a) ネットワーク層のペネトレーションテスト
(b) アプリケーション層のペネトレーションテスト

3.3. 気づかれない状態で，利用者が情報資産に不正にアクセスできないように，担当者の職務および責任範囲を分割すること。

3.3.1. 個人またはチームに次に示す情報セキュリティ管理責任を割り当てること。
(a) セキュリティポリシーおよび手順を確立，文書化および周知する。
(b) セキュリティに関する警告および情報を監視して分析し，該当する担当者に通知する。
(c) インシデントの対応および報告手順を確立，文書化および周知して，あらゆる状況をタイムリーかつ効果的に処理する。
(d) 追加，削除，変更を含め，ユーザアカウントを管理する

(e) データへのすべてのアクセスを監視および管理する。

3.4. 第三者が提供するサービス，報告および記録は，情報セキュリティの条件の遵守を確実にするため，常に監視しレビューすること。

3.4.1. 共有ホスティングプロバイダは，各事業体のホストコンピュータ環境および学校教育データを保護すること。

3.5. すべての重要な情報およびソフトウェアの回復を確実にするために，バックアップ設備を備えること。

3.5.1. バックアップ媒体を安全な場所に保管すること（代替またはバックアップサイト，商用ストレージ施設などのオフサイト施設が望ましい）。保管場所のセキュリティを少なくとも 1 年に 1 回確認すること。

3.6. 情報管理者は，新しいシステムを受け入れるための要求事項および基準を明確にし，合意し，文書化し，試験すること。

3.6.1. システムをネットワーク上に導入する前に，ベンダ提供のデフォルト値を必ず変更すること（パスワード， SNMP コミュニティ文字列の変更，不必要なアカウントの削除など）。

3.6.2. すべてのシステムコンポーネントについて，設定基準を作成すること。この基準は，既知のセキュリティ脆弱性に対応しており，広く採用されているシステム強化のための基準等と矛盾しないこと。
(a) 1 つのサーバには，主要機能を 1 つだけ実装する。
(b) 安全性の低い不必要なサービスおよびプロトコルはすべて無効にする（デバイスの特定機能を実行するのに直接必要でないサービスおよびプロトコル）。
(c) 誤用を防止するようにシステムのセキュリティパラメータを設定する。
(d) スクリプト，ドライバ，機能，サブシステム，ファイルシステム，不要な Web サーバなど，不要な機能をすべて削除する。

3.7. ネットワークの管理者は，管理策を定め，ネットワークにおける情報のセキュリティ確保や，無認可のアクセスからのネットワークの保護を確実に行うこと。

3.7.1. すべてのシステムコンポーネントとソフトウェアに，ベンダ提供の最新セキュリティパッチを適用すること。重要なセキュリティパッチは，リリース後 1 カ月以内にインストールすること。

注: 組織は，パッチインストールの優先順位を付けるために，リスクに基づくアプローチの適用を検討できる。例えば，重要なインフラストラクチャ（一般に公開されているデバイス，システム，データベースなど）に重要性の低い内部デバイスよりも高い優先順位を付けることで，優先順位の高いシステムおよびデバイスは 1 カ月以内に対処し，重要性の低いシステムおよびデバイスは 3 カ月以内に対処するようにする。

3.7.2. 本推奨仕様 （安全な認証やロギングなど）に従い，業界のベストプラクティスに基づいてソフトウェアアプリケーションを開発し，ソフトウェア開発ライフサイクル全体を通して情報セキュリティを実現すること。これらのプロセスには，次の事項を含めること。

(a) 導入前にすべてのセキュリティパッチ，システムとソフトウェア構成の変更をテストする（次のテストが含まれるが，これらに限定されない）。

・すべての入力の検証（クロスサイトスクリプティング，インジェクションの不具合，悪意のあるファイル実行などを防止するため）

・適切なエラー処理の検証

・暗号化による安全な保管の検証

・安全な通信の検証

・適切な役割ベースのアクセス制御（Role-based Access Control（RBAC））の検証

(b) 開発/テスト環境と本番環境の分離

(c) 開発/テスト環境と本番環境での責務の分離

(d) テストまたは開発に本番環境データを使用しない

(e) 本番環境システムがアクティブになる前にテストデータとテストアカウントを削除する

(f) アプリケーションがアクティブになる前，または学校にリリースされる前に，カスタムアプリケーションアカウント，ユーザ ID，パスワードを削除する

(g) コーディングの脆弱性がないことを確認するために，本番または学校へのリリースの前に，カスタムコードをレビューする

注: このコードレビュー要件は，本推奨仕様で要求されるシステム開発ライフサイクルの一環として，すべてのカスタムコードに適用される。コードレビューは，知識を持つ校内技術担当者または第三者が実施できる。一般に公開されている Web アプリケーションは，実装後の脅威および脆弱性に対処するために，本推奨仕様に定義されている追加コントロールの対象となる。

3.7.3. すべての Web アプリケーション（内部，外部，アプリケーションへの Web 管理アクセス）を「Open Web Application Security Project Guide」 などの安全なコーディングガイドラインに基づいて開発すること。

3.7.4. 一般公開されている Web アプリケーションは，常時，新しい脅威と脆弱性に対処し，次に示すいずれかの手法によって既知の攻撃から保護すること。

(a) 一般公開されている Web アプリケーションは，アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって，少なくとも年 1 回および何らかの変更を加えた後にレビューする。

(b) 一般公開されている Web アプリケーションの手前に，Web アプリケーションファイアウォールをインストールする。

3.7.5. システムコンポーネントへのすべてのアクセス（特に，ルートなどの管理者権限を使用して行われたアクセス）を各ユーザにリンクするプロセスを確立すること。

3.7.6. 次に示すイベントを再現するためにすべてのシステムコンポーネントの自動監査証跡を実装すること。

(a) 学校教育データへのすべての個人アクセス

(b) ルート権限または管理権限を持つ個人によって行われたすべてのアクション
(c) すべての監査証跡へのアクセス
(d) 無効な論理アクセス試行
(e) 識別および認証メカニズムの使用
(f) 監査ログの初期化
(g) システムレベルオブジェクトの作成および削除

3.7.7. イベントごとに，すべてのシステムコンポーネントについて少なくとも次の監査証跡を記録すること。
(a) ユーザ識別
(b) イベントの種類
(c) 日付と時刻
(d) 成功または失敗を示す情報
(e) イベントの発生元
(f) 影響を受けるデータ，システムコンポーネントまたはリソースの ID または名前

3.7.8. すべての重要なシステムクロックおよび時刻を同期すること。

3.7.9. 少なくとも日に一度，すべてのシステムコンポーネントのログを確認することが望ましい。

3.7.10. 無線アナライザを少なくとも 3 ヵ月に一度使用して，または使用中のすべての無線デバイスを識別するための無線 IDS/IPS を導入して，無線アクセスポイントの存在をテストすること。

3.8. 取り外し可能な媒体について，不要になった媒体が再利用可能なときは，それに格納している内容を回復不能とすること。また不要になった媒体の措置のすべてについて認可を要求し，記録を保管すること。

3.8.1. 学校教育データを含むすべての紙および電子媒体を物理的にセキュリティで保護すること。

3.8.2. 学校教育データを含む媒体の保管およびアクセスに関して厳格な管理を維持すること。
すべての媒体の在庫ログを適切に保持し，少なくとも 1 年に 1 回媒体の在庫調査を実施すること。

3.9. システム文書を保護するために，セキュリティを保って保管する。また，システム文書へのアクセスは，最小限に抑え，当該業務の管理者が認可すること。

3.9.1. ルータ構成ファイルをセキュリティ保護および同期化すること。

3.10. 電子的メッセージ通信のセキュリティのために，認可されていないアクセス，改ざんまたはサービス妨害から保護すること。

3.10.1. すべてのコンソール以外の管理アクセスを暗号化すること。Web ベースの管理やその他のコンソール以外の管理アクセスについては，SSH，VPN，または SSL/TLS などの技術を使用すること。

3.10.2. オープンな公共ネットワーク経由で学校教育データを伝送する場合，強力な暗号化と SSL/TLS または IPsec などのセキュリティプロトコルを使用すること。
学校教育データを伝送する，または学校教育データ環境に接続している無線ネットワークには，広く採用されている標準技術（IEEE 802.11i など）を使用して，認証および伝送用に強力な暗号化を実装すること。

3.10.3. ファイル完全性監視ツールを導入して重要なシステムファイル，構成ファイル，またはコンテンツファイルの不正な変更を担当者に警告し，重要なファイルの比較を少なくとも週に一度実行するようにソフトウェアを構成すること。

3.11. 情報処理設備の使用状況を監視する手順を確立し，監視活動の結果をレビューすること。

3.11.1. 変更できないよう，監査証跡をセキュリティで保護すること。
(a) 監査証跡の表示を業務上必要とする管理者，担当者のみに制限する。
(b) 監査証跡ファイルを不正な変更から保護する。
(c) 監査証跡ファイルを変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。
(d) 外部に公開されている Web サーバ等のログを内部 LAN 上のログサーバに書き込む。
(e) ログに対してファイル完全性監視または変更検出ソフトウェアを使用して，既存のログデータを変更すると警告が生成されるようにする。

3.11.2. 監査証跡の履歴を少なくとも 1 年間保持すること。少なくとも 3 カ月はすぐに分析できる状態にしておくこと（オンライン，アーカイブ，バックアップから復元可能など）。

3.11.3. 侵入検知システムや侵入防止システムを使用して，学校教育データ環境内のすべてのトラフィックを監視し，侵害の疑いがある場合は担当者に警告すること。すべての侵入検知および防止エンジンを最新状態に保つこと。

4. アクセス制御

4.1. 教職員がパスワードの選択および使用を行う際には，「パスワードを秘密にしておく」「紙に記録して保管しない」「定期的に変更する」などの正しいセキュリティ慣行に従うこと。

4.1.1. 強力な暗号化を使用して，すべてのシステムコンポーネントでの伝送および保管中のすべてのパスワードを読み取り不能にすること。

4.1.2. すべてのシステムコンポーネントで，次に示すように，教職員および管理者に対して適切なユーザ認証とパスワード管理を確実に行うこと。
(a) ユーザ ID，資格情報およびその他の識別子オブジェクトの追加，削除，変更を管理する。
(b) パスワードのリセットを実行する前にユーザ ID を確認する。
(c) 初期パスワードをユーザごとに異なる値に設定し，初回使用後に直ちに変更する。
(d) 少なくとも 90 日ごとに利用履歴のないユーザアカウントを無効化する。

(e) リモート保守のためにベンダが使用するアカウントは，必要な期間のみ有効にする。
(f) パスワード使用手順およびポリシーを学校教育データにアクセスできるすべてのユーザに伝達する。
(g) グループ，共有，またはデフォルトのアカウントおよびパスワードを使用しない。
(h) 少なくとも 90 日ごとにユーザパスワードを変更することが望ましい。
(i) パスワードに 7 文字以上が含まれることを要求する。
(j) 数字と英文字の両方を含むパスワードを使用する。
(k) ユーザが新しいパスワードを送信する際，最後に使用した 4 つのパスワードと同じものを使用できないようにする。ただし，２要素認証の場合はこの限りではない。

4.2. 利用者は，実行していた処理が終わった時点で，接続を切る。パソコンまたは端末は，利用していない場合，キーロック等によってセキュリティを保つこと。

4.2.1. 最大 6 回の試行後にユーザ ID をロックアウトして，アクセス試行の繰り返しを制限すること。

4.2.2. ロックアウトの期間を最小 30 分または管理者がユーザ ID を有効にするまでに設定すること。

4.3. 利用することを特別に認可したサービスへのアクセスだけを利用者に提供すること。

4.3.1. システムコンポーネントと学校教育データへのアクセスを業務上必要な人に限定すること。アクセス制限には次の事項を含めること。
(a) 特権ユーザ ID に関するアクセス権が,職務の実行に必要な最小限の特権に制限されていること
(b) 特権の付与は，個人の職種と職能に基づくこと
(c) 管理職により署名され，必要な特権を特定する承認フォームが要求される
(d) 自動アクセス制御システムを実装する

4.3.2. 複数のユーザを持つシステムコンポーネントに対して，ユーザの必要な範囲に基づいてアクセスを制限し，特に許可されていない限り「すべてを拒否」に設定した，アクセス制御システムを確立すること。アクセス制御システムには次の事項を含めること。
(a) すべてのシステムコンポーネントを対象に含む
(b) 職種と職能に基づく，個人への特権の付与
(c) デフォルトでは「すべてを拒否」の設定

4.4. 遠隔利用者のアクセスを管理するために，暗号に基づく技術など適切な認証方法を利用すること。

4.4.1. 教職員，管理者および第三者によるネットワークへのリモートアクセス（ネットワーク外部からのネットワークレベルアクセス）には ２要素認証を組み込むこと。RADIUS（Remote Authentication and Dial-In Service），TACACS（Terminal Access Controller Access Control System）とトークン，または VPN（SSL/TLS または IPsec ベース）と個々の証明書などの技術を使用すること。

4.5. 学校内のネットワークについては，教職員用と児童・生徒用など，ネットワーク領域を分割すること。また，ネットワークごとにそれぞれの管理策を作成すること。

4.5.1. 次の事項を含むファイアウォールおよびルータ構成基準を確立すること。

(a) すべてのネットワーク接続およびファイアウォール/ルータ構成への変更を承認およびテストするプロセス

(b) 無線ネットワークを含む学校教育データへのすべての接続を示す最新ネットワーク図

(c) インターネット接続および DMZ（demilitarized zone） と内部ネットワークゾーンとの間のファイアウォール要件

(d) ネットワークコンポーネントの論理的管理のためのグループ，役割，責任に関する記述

(e) 使用が許可されているすべてのサービス，プロトコル，ポートの文書化および使用が許可されている業務上の理由（安全でないとみなされているプロトコルに実装されているセキュリティ機能の文書化など）

(f) ファイアウォールおよびルータのルールセットは少なくとも 6 カ月ごとにレビューすること

4.5.2. 信頼できないネットワークと学校教育データ環境内のすべてのシステムコンポーネントとの接続を制限するファイアウォール構成を構築すること。

注: 「信頼できないネットワーク」とは，レビュー対象の事業体に属するネットワーク外のネットワーク，または事業体の制御または管理が及ばないネットワーク、あるいはその両方のことである。

(a) 着信および発信トラフィックを学校教育データ環境に必要なトラフィックに制限する。

(b) ルータ構成ファイルをセキュリティ保護および同期化する。

(c) すべての無線ネットワークと学校教育データ環境の間に境界ファイアウォールをインストールし，無線ネットワーク環境から学校教育データ環境へのすべてのトラフィックを拒否または業務上必要な場合は制御するようにファイアウォールを構成する。

4.5.3. インターネットと学校教育データ環境内のすべてのシステムコンポーネント間の，直接的なパブリックアクセスを禁止すること。

(a) DMZ を実装し，着信および発信トラフィックを，学校教育データ環境に必要なトラフィックに制限する。

(b) 着信インターネットトラフィックを DMZ 内の IP アドレスに制限する。

(c) インターネットと学校教育データ環境間トラフィックの，すべての直接経路（着信/発信）を使用不可にする。

(d) インターネットから DMZ 内へ通過できる内部インターネットアドレスを禁止する。

(e) 学校教育データ環境からインターネットへの発信トラフィックが，DMZ 内の IP アドレスにのみアクセス可能なように制限する。

(f) 動的パケットフィルタリングとも呼ばれるステートフルインスペクションを実装する（ネットワーク内へは，「確立された」接続のみ許可される）。

(g) DMZ から分離された内部ネットワークゾーンに，データベースを配置する。

(h) RFC 1918 アドレス領域を使用して，IP マスカレードを実装し，内部アドレスが変換されインターネット上で露出することを防ぐ。ポート アドレス変換（PAT）などのネットワークアドレス変換（NAT）技術を使用する。

4.6. 教職員は，個人ごとにユニークな利用者 ID を保有し，その活動が誰の責任によるものかを後で追跡できるようにすること。また，利用者の同一性を検証するために，適切な認証技術を選択すること。

4.6.1. システムコンポーネントまたは学校教育データへのアクセスを許可する前に，すべてのユーザに個別の ID を割り当てること。

4.6.2. 個別の ID の割り当てに加え，次の方法の少なくとも 1 つを使用してすべてのユーザを認証すること。
・パスワードまたはパスフレーズ
・２要素認証（トークンデバイス，スマートカード，生体認証，公開鍵など）

4.7. 教職員が，コンピュータを用いる場合は，物理的保護，アクセス制御，暗号技術，バックアップおよびウィルス対策についての方針を定め，適切なセキュリティ対策を採用すること。

4.7.1. インターネットに直接接続するすべてのモバイル端末または教職員使用のコンピュータ、あるいはその両方で，校内ネットワークへのアクセスに使用されるものに，パーソナルファイアウォールソフトウェアをインストールすること。

4.7.2. 学校教育データ環境に接続されている，または学校教育データを伝送する無線ネットワーク環境の場合，無線ネットワークベンダのデフォルト値を変更すること。これには，デフォルトの無線ネットワーク暗号鍵，パスワード，SNMP コミュニティ文字列が含まれる（ただし，これらに限定されない）。認証および伝送のために，強力な暗号化技術の無線デバイスセキュリティ設定が有効になっていることを確認すること。

4.7.3. 悪意のあるソフトウェアの影響を受けやすいすべてのシステム（特にパソコンとサーバ）に，アンチウィルスソフトウェアを導入すること。
すべてのアンチウィルスプログラムは，すべての既知のタイプの悪意のあるソフトウェアに対して検知，駆除，保護が可能でなければならない。

4.7.4. すべてのアンチウィルスメカニズムが最新で，有効に実行されており，監査ログが生成できること。

5．法令の遵守

5.1. 知的財産を保護するために，次の指針を考慮すること。
(a) ソフトウェアは知られた定評のある供給元を通して取得する。
(b) 許諾された最大利用数を越えて使用しない。
(c) 書籍，記事，報告書またはその他の文書を複写しない。

5.2. 個人データおよび個人情報の保護に関する学校の方針を確立して実施すること。

（システムの開発，構築，運用者編　以上）

●執筆　　「教員のＩＴ利用環境整備の調査研究」検討委員会（敬称略,五十音順）

●委員長：
中川　正樹　　東京農工大学

●副委員長：
山崎　文明　　ビジネスアシュアランス株式会社

●委員：
赤倉　貴子　　東京理科大学
榎本　竜ニ　　東京都立江東商業高等学校
大澤　一郎　　独立行政法人　産業技術総合研究所
梶本　佳照　　三木市立教育センター
来住　伸子　　津田塾大学
曽田　耕一　　上越地域学校教育支援センター
豊田　祥一　　ビジネスアシュアランス株式会社
藤村　裕一　　鳴門教育大学
三宅　健次　　千葉大学教育学部付属中学校

●事務局：
鶴田　雅文　　財団法人　コンピュータ教育開発センター
木島　令己　　財団法人　コンピュータ教育開発センター
山中　計一　　財団法人　コンピュータ教育開発センター
藤本　康雄　　財団法人　コンピュータ教育開発センター
小関　佳彦　　財団法人　コンピュータ教育開発センター
鈴木　健司　　財団法人　コンピュータ教育開発センター

学校情報セキュリティ推奨仕様

平成 22 年 3 月 31 日発行

著作権者　財団法人コンピュータ教育開発センター（ＣＥＣ）
発　　行　財団法人コンピュータ教育開発センター（ＣＥＣ）
〒108-0072　東京都港区白金 1-27-6
TEL　03-5423-5911（代表）　FAX 03-5423-5916
URL http://www.cec.or.jp/CEC/