学校情報セキュリティ推奨仕様

解　　説　　書

- 項目別解説
- 評価内容
- 用語集

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 つに分け，「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。

【解説】

本解説書は，本推奨仕様の項目毎に【解説】として要件の概要を解説するとともに，本推奨仕様を利用する際の手引きとなる事項を記載している。また，本推奨仕様に遵守できているかどうかを評価するための最低限の確認事項を【評価項目】として記載している。あわせて用語解説を用語集として巻末に掲載している。

なお，本推奨仕様の策定に際しては，クレジットカード業界のセキュリティ基準である PCI(Payment Card Industry)データセキュリティ基準（PCI DSS）を参考にしている。PCI DSS は，クレジットカード番号を保護するうえでの必要な保護措置の最低水準を具体的に定めたクレジットカード業界の事実上の国際標準規格であり，PCI DSS に準拠していることを評価する仕組みにより業界全体としてのセキュリティ水準を確保することを目指している。このため，学校が遵守すべきセキュリティ基準に PCI DSS の要件を応用できれば，学校が学校教育データ等の重要情報に対して必須となる保護措置を具体的に示すことが可能となり，情報共有を必要とする別の学校等に対して実施すべき対策を求めやすくなる。さらに，全国の学校が同じ具体的な基準によってセキュリティ対策が実施されることにより，全国の学校全体のセキュリティ水準が確保されることが期待できる。

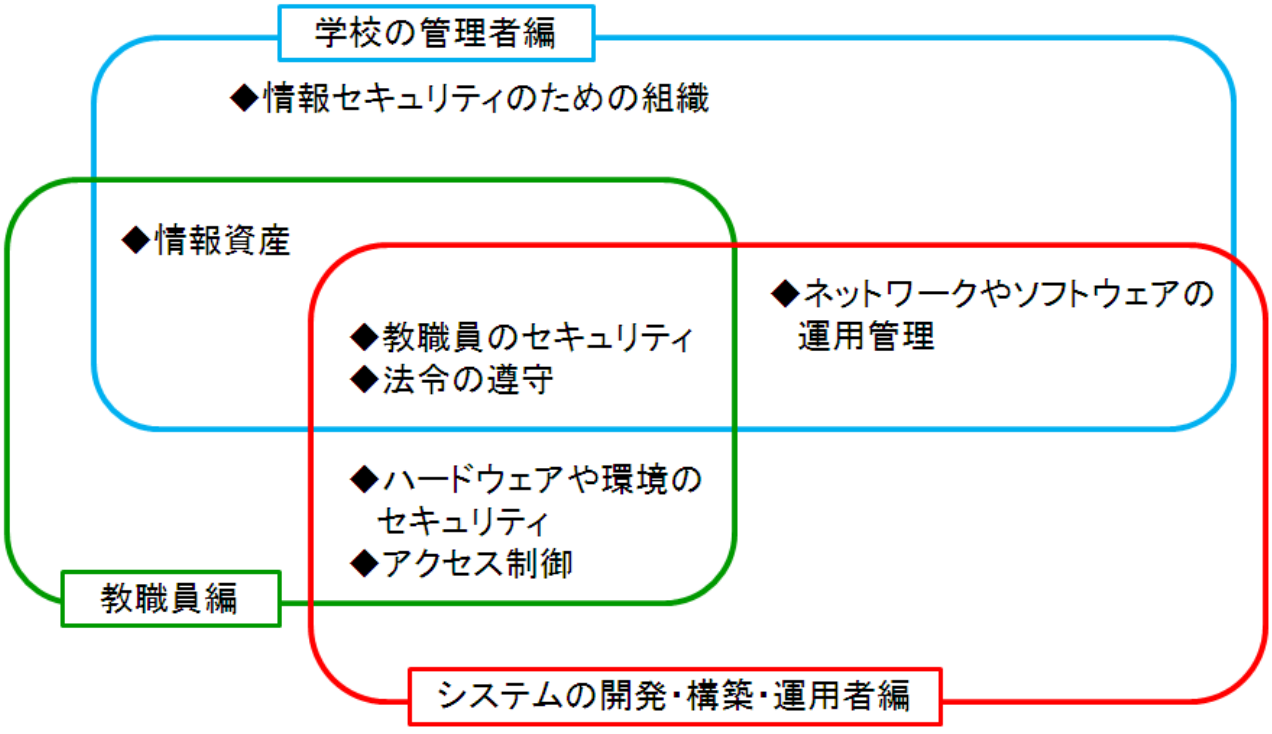

図 1.　本解説書の各編に含まれる内容

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。

【解説】

本推奨仕様において保護の対象となる学校教育データは，基本データとセンシティブデータ（特別に配慮が必要な情報）に大別される。基本データは，基本 4 情報（氏名，住所，生年月日，性別）に個人識別データを加えたものである。個人識別データは，これ単体では特に機密性の高いものではないが，個人識別データを紐付けることで，断片的な個人情報を統合化することが可能となる。今後，IT の利活用が促進されることにより，断片的な様々な個人情報がネットワーク上を流通することが予測される。このような状況の下では，個人を容易に紐付けることが可能となる識別情報の重要性が増すと考えられることから，本推奨仕様では個人識別データを学校教育データの重要なデータ要素と位置付けている。

なお，学校教育データは，個人情報保護法に準拠した取扱いが求められていることを認識する必要がある。

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。

【解説】

本推奨仕様は，学校教育データを保護することを目的としているため，本推奨仕様の適用範囲となるシステムコンポーネントは，学校教育データを保管・処理・伝送するものに限定される。このため，学校教育データを保管・処理・伝送しないシステムコンポーネントは，本推奨仕様の適用範囲から除外される。

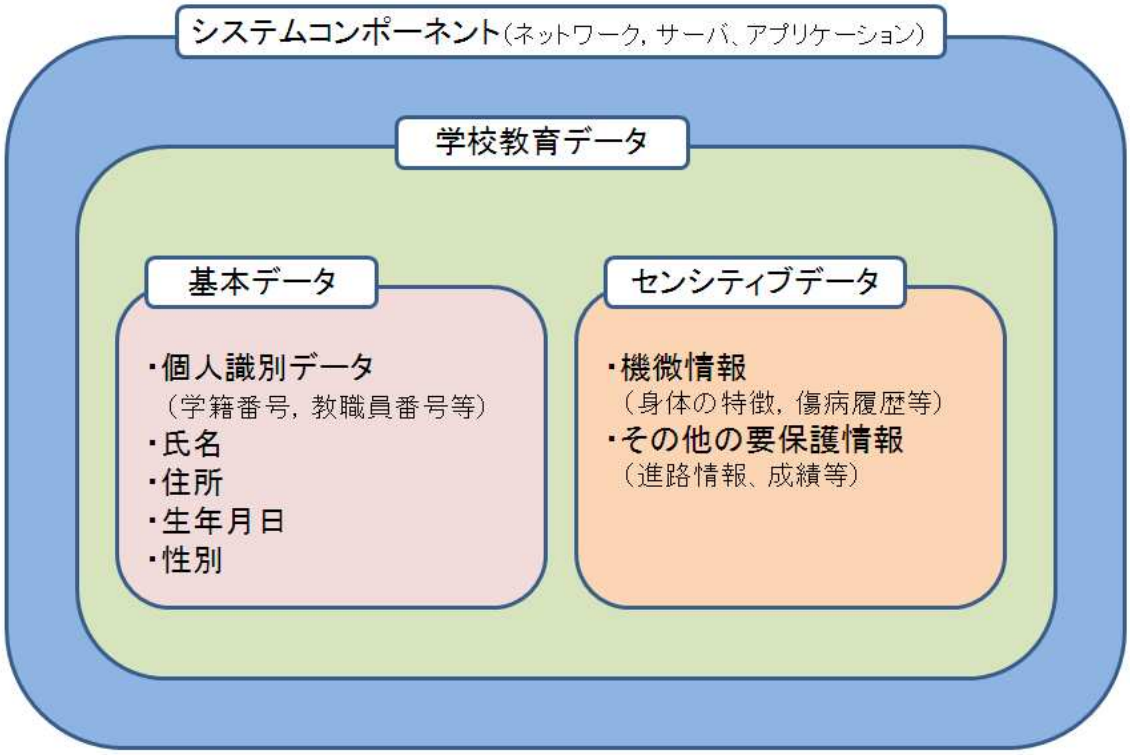

図 2.　学校情報セキュリティ推奨仕様の適用範囲

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。

【解説】

学校の管理者は，学校のセキュリティポリシーを確立し，これを周知するとともに常に最適な状態に維持することが求められる。

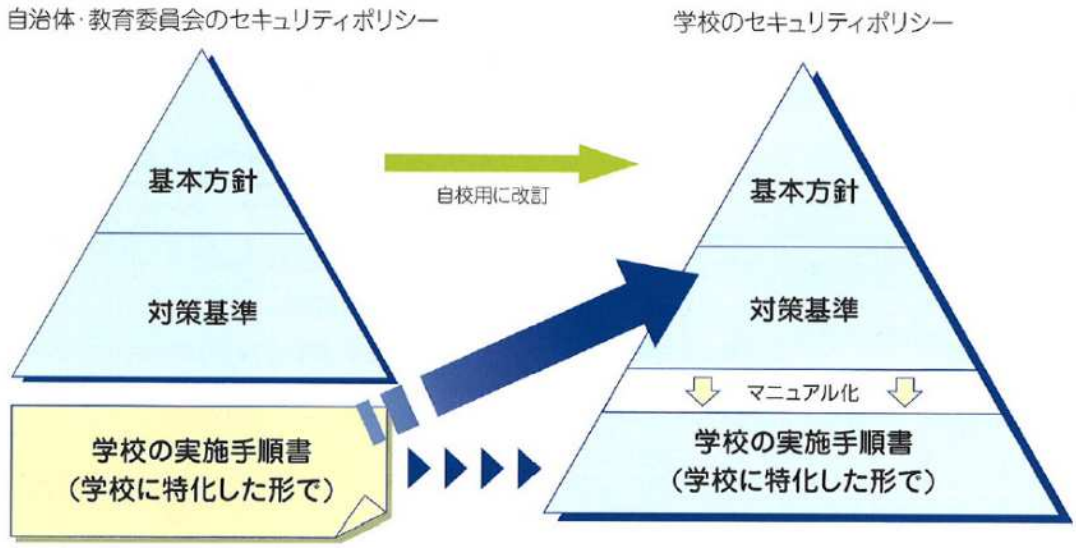

図 3．学校のセキュリティポリシーの策定イメージ

セキュリティポリシーには，本推奨仕様の要件をすべて盛り込み，具体的な対応策を対策基準もしくは実施手順書に記載する。また，ある時点ではセキュリティ対策が有効であっても，外部環境の変化により対策が陳腐化する恐れがある。セキュリティ対策が不備な状況になることを回避するためには，個々のセキュリティ対策において PDCA（Plan,Do,Check,Action）サイクルを確立し，適切な見直しや継続的な改善を図らなければならない。

【評価内容】

(1) セキュリティ基本方針・対策基準を調査し，関連するすべてのシステム利用者（業務委託先を含む）にセキュリティ基本方針・対策基準が公開，周知されていることを確認する。
(2) セキュリティ基本方針・対策基準が本推奨仕様のすべての要件に対応していることを確認する。

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。

【解説】

学校の管理者は，本推奨仕様の「教職員編」の要求事項を教職員が確実に実施するように研修と指導を行わなければならない。

すべての教職員が学校教育データを保護することの重要性を認識し，自らが所属する組織のセキュリティ基本方針・対策基準の内容を理解して行動できるようにするためには，適切な教育の実施が不可欠である。また，役割に応じた専門的な教育も必要となる。

【評価内容】

(1) すべての教職員向けに責任者に承認されたセキュリティ研修・啓発プログラムが存在することを確認する。
(2) セキュリティ研修・啓発プログラムによって，教職員の認知向上と教育を図る複数の方法（例えば，ポスター，通知，手引き，事例集，Web を用いた教育，研修会および他の推進資料）が提供されていることを確認する。
(3) 教職員が雇用時および最低 1 年に 1 回，セキュリティ研修に参加していることを確認する。

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。

【解説】

児童・生徒，教職員，学校関係者に関する機微な情報の漏えいなど，学校教育データにかかわるインシデント（事件・出来事）の発生がもたらす社会的影響は極めて大きい。また，最近では，情報システムへの依存度が高くなっており，システムにおけるインシデントの発生がそのまま教務あるいは校務の円滑な運営を阻害する問題

に発展する可能性がある。これを防ぐためには，インシデントが発生した際に影響を最小限に抑えるとともに，可能な限り迅速に業務を復旧できるようにしなければならない。このため，インシデント対応計画を事前に作成し，情報セキュリティにかかわる事件・事故に備えておく必要がある。

セキュリティ侵害が発生した際に迅速な対応を行うためには，事前に管理体制や対応手順を明確にしておくことが必要となる。また，インシデントのレベルによっては，関連組織への報告や届出も必要となる。インシデント対応計画に含めるべき事項について，次のようなものがある。

- インシデント対応に携わる関係者の役割と責務
- 具体的な発生事故を想定した対応手順
- 教務および校務の復旧手順および継続手順
- バックアップデータのリストア（データ復旧）手順
- 報告や届出を実施すべき関連組織の明確化と連絡方法
- インシデント対応計画を修正および展開するための体制

【評価内容】

事故対応計画および関連手順を調査し，次の項目が含まれていることを確認する。

- 必須項目として，セキュリティ侵害事象が発生した場合における役割，責務，コミュニケーションおよび関連組織（教育委員会，警察，独立行政法人情報処理推進機構（IPA）等）への即時報告，報道対応を含む情報連携方針
- 具体的なインシデント対応方針
- 業務復旧と事業継続のための手順
- データのバックアップ手順
- すべての重要なシステムコンポーネントを網羅し，対応していること
- 関連組織（教育委員会，警察，IPA 等）への通知，報道対応

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。

【解説】

アプリケーションシステムの多くの機能が，ベンダ（製品を販売する会社）が提供する既存の製品から構成されている。これら製品のベンダは，自製品の脆弱性が発見される度にセキュリティパッチ（脆弱性対策プログラム）を提供することで自製品の安全性を維持している。したがって，ベンダが提供するセキュリティパッチをできる限り早い時期に適用することで，システムの安全性を確保する必要があるため，ベンダが提供する自製品のセキュリティ情報に関するメーリングリストや，セキュリティ製品ベンダが提供するメーリングリストに参加するなどして，新しく見つかった脆弱性を認識することのできる体制を確立する必要がある。

また，メーリングリストに参加していながら，届いたメールを確認する体制が整っていないため脆弱性情報の把握漏れが発生した，というような事態を避けるため，収集したセキュリティ情報の中からシステムを構成する製品に関連する情報を確実に特定し，適切な判断のもとにセキュリティパッチを適用する保守・運用体制の整備が求められる。

これらの対応については，情報セキュリティに関する委員会を設置し，その委員会において専門家からの助言を得て対応できるようにすることが必要である。

【評価内容】

(1) 新しいセキュリティ脆弱性を特定するためのプロセスが確立され，機能していることを確認する。
(2) 新しいセキュリティ脆弱性情報を得るためのプロセスに，外部の情報源の使用や，新しい脆弱性問題が見つかったときのシステム設定基準の更新が含まれていることを確認する。

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。

【解説】

保管するデータは，データの保管と廃棄に関する基本方針・対策基準に従い，保管すべき情報，保管期間などを限定する必要がある。

【評価内容】

データの保管と廃棄に関する基本方針・対策基準と実施手順を入手し，以下の項目を確認する。

(1) 学校教育データの保管に関して，データ保管に関する法律上，規制上，業務上の要件が含まれていること。要件には，例えば「学校教育データは，X の期間，Y という業務上の理由で保管する必要がある」というように具体的な学校教育データの保管に関する記述が行われていること。
(2) 学校教育データに関して，法律上，規制上，業務上の必要性がなくなった場合の，データの廃棄に関する要件が含まれていること。
(3) 学校教育データのすべての保管範囲が含まれていること。
(4) 業務上の保管要件を超えて格納されている学校教育データを少なくとも 1 年毎に削除するための自動的なプロセス，もしくは格納された学校教育データが業務上の保管要件を超えていないかを確認するための少なくとも 1 年毎のレビュー実施要件が含まれていること。

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。

【解説】

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自らの責任を十分認識すべきである。このため，情報セキュリティに関する責任を果たすことについての記載がある誓約書に同意し，署名することは，学校教育データを取扱う者の認識を高めるうえで有効である。

【評価内容】

誓約書を入手し，以下の項目を確認する。

(1) 誓約書に情報セキュリティに関する責任が記載されていること。
(2) 学校教育データを取扱う者が，誓約書に同意したうえで署名していること。

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。

【解説】

懲戒処分などの手続きが存在することは，セキュリティ違反への教職員に対する抑止効果となり有効である。

【評価内容】

職務規定等を入手し，セキュリティ違反を犯した教職員に対する懲戒処分の手続きが記載されていることを確認する。

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。

【解説】

すべての情報および情報処理施設に対するアクセス管理を徹底するためには，利用者の登録に加えて，登録削除について管理が適切に行われなければならない。

【評価内容】

教職員の雇用終了時勤務校変更時の手続きにおいて，該当する情報が情報システムの利用者を管理する部署に通知される手順となっていること，あるいは雇用終了情報がシステム連携して削除処理等が行われることを確認する。

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）。

【解説】

ユーザアカウント（システム利用者登録情報）保守手順には，ユーザアカウントの生成，配布，変更および削除に関する実施手順の他に，無効なユーザアカウントが存在しないことを定期的に確認する実施手順が含まれることが望ましい。ログレビュー手順には，不正アクセスや攻撃の痕跡が発見された場合における対応手順が含まれることが望ましい。

【評価内容】

日常的な運用上のセキュリティ実施手順を調査する。実施手順がこの仕様に準拠し，各要件について管理手順および技術手順が規定されていることを確認する。

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，リムーバブルメディア，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。

【解説】

ガイドラインには，次の項目を記載することが必要である。

- 該当する技術を使用することについての管理責任者による明示的な承認
- 装置の使用時に必要となる認証手段（ユーザ名とパスワードによる認証，その他の認証手段）
- 装置およびアクセス権を持つ担当者のリスト
- 装置の所有者，連絡先，目的のラベル表示
- 許容される（または許可しない）技術の利用方法

【評価内容】

教職員に公開されている重要な技術の使用に関するガイドラインを調査し，ガイドラインが以下の項目を含んでいることを確認する。

(1) 装置を使用するための管理責任者による明示的な承認を求めていること。
(2) すべての装置の使用が，ユーザ名とパスワード，または他の認証手段（例：証明書，USB キー，IC カード，生体認証などのトークン）によって認証されていることが求められていること。

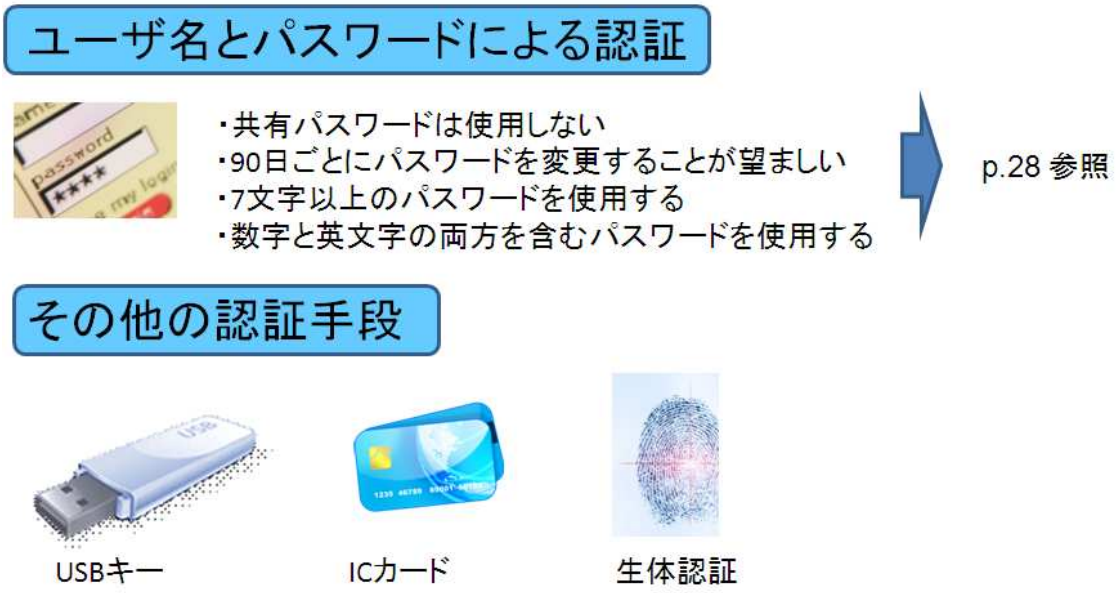

図 4.　情報システム（装置）の使用時に求められる認証手段

(3) すべての装置および装置の使用を許可されたすべての担当者のリストが含まれていること。
(4) 装置の所有者，連絡先，目的のラベル表示が求められていること。
(5) 許容される技術の用い方が含まれていること。
(6) 技術が許容されるネットワーク上の場所が含まれていること。
(7) 教育委員会等または校長が承認した製品のリストが求められていること。

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

【解説】

セキュリティパッチの適用，システム・ソフトウェアの設定変更，バグの修正，機能の追加を含むすべての変更は，変更管理手順に従って実施されなければならない。このため，学校教育データを扱うシステムにおいてすべての変更を安全かつ確実に実施するために，標準化された方法，実施手順を確立する必要がある。その実施手順には，以下に述べる要件が含まれていることが望ましい。

(a) 変更が与える影響の文書化
システムの変更を実施するにあたって，変更の適用範囲と，変更がシステムに与える影響の範囲，変更に伴うリスクが明確に文書化され，適切な関係者により評価されなければならない。

(b) 適切な管理者による変更の承認
評価された結果に事業上の正当性を加味し，変更作業の作業実施手順とともに，管理者による適切な承認を得なければならない。
(c) 運用機能のテスト
変更を適用した後，他の機能に悪影響を与えないか運用機能のテストを実施し，管理者による最終承認を得なければならない。
(d) 回復手順
変更の本番環境への適用時に失敗した場合の処置，回復する手順が明確にされ，作業実施手順書に記載されていなければならない。

以上に述べた変更管理プロセスが確実に適用されるよう，運用体制を整備し，変更管理プロセスを文書化して維持・管理する必要がある。

【評価内容】

(1) セキュリティパッチとソフトウェアの変更に関する変更管理実施手順を入手し，次の項目が要求されていることを確認する。
・利用者への影響に関する記述が，変更管理文書に含まれていること。
・管理者による適切な承認が存在すること。
・運用機能のテストが実施されていること。
・回復手順が用意されていること。
(2) システムコンポーネントのサンプルについて，各システムコンポーネントについて最新の変更／セキュリティパッチを調査し，それらの変更が関連する変更管理文書に基づくものかどうかを確認する。

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

【解説】

脆弱性検査がシステムの脆弱性の検出を目的としたテストであるのに対し，ペネトレーションテストは，発見された脆弱性に関して，更に攻撃者の視点からその脆弱性の有効性を判断し，システム全体としてのセキュリティ対策の有効性を評価することを目的としたテストである。日常的な運用としては，脆弱性検査で脆弱性の発見と修正対応というサイクルを実施することにより脆弱性管理を行う一方で,ペネトレーションテストにより,日々の検査では発見しきれない脆弱性の検出，万一の被害が発生した際の影響程度を測定したりすることが可能となる。

ペネトレーションテストの実施には，セキュリティ専業会社のサービスを利用することが多いと思われる。仮に自組織内で行うのであれば，インターネット上で入手可能なフリーのツール，ならびにペネトレーションテスト用の商用ツールを利用することで対応することも可能ではある。ただし，検査の実施には，システムに対する第三者的な視点，セキュリティに関する専門知識，攻撃者の視点などの要素が必要となるため，内部でペネトレーションテストの実施を計画する際は，内部で実施することの利点・欠点をよく検討する必要がある。

【評価内容】

(1) 最新のペネトレーションテストの結果を入手し，ペネトレーションテストが少なくとも 1 年に 1 回および環境の大きな変更の後に実施されていることを確認する。脆弱性が見つかった場合，修正され再テストが実施されていることを確認する。
(2) テストは，内部の適当な部署，または適当な外部の第三者によって実施されていることを確認する。適用可能であれば，組織として独立していることが望ましい。
(3) ネットワーク層を含むペネトレーションテストが実施されていることを確認する。このテストは，オペレーティングシステムや，ネットワーク機能を補助するコンポーネントを含まなければならない。
(4) アプリケーション層を含むペネトレーションテストが実施されていることを確認する。

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。

【解説】

セキュリティ基本方針･対策基準や他の文書において,これらの責務に関連する記述がされている必要がある。特に情報システムの構成要素に対しては，セキュリティ警告への対応，アカウント管理，アクセス制御といったシステムの運用に関する責務を明確に定めることが重要である。以下は，代表的な役割とその責務についてである。

(1) 管理責任者の役割
セキュリティ基本方針・対策基準は組織の部門を跨いで適用されるケースが多く，一般的にそれらの部門を統括する管理責任者がその責務を負うことが多い。このため，すべての関係者とシステム構成要素を対象としたセキュリティ基本方針・対策基準を確立する責務は，上席の管理責任者が担うものと考えられる。
(2) セキュリティ責任者の役割
個々のセキュリティ対策が適切かつ確実に実施されるようにする責務は，情報システムを統括するセキュリティ責任者が担うことが想定される。特に，セキュリティ事故への対応と報告手順を確立し，それらを迅速に取扱う責務はセキュリティ責任者が担うべき重要な責務の一つと考えられる。
(3) セキュリティ管理者の役割
具体的なシステムのセキュリティ設定や運用管理の実施は，セキュリティ管理者が責任を持つことになる。セキュリティ警告への対応，アカウント管理，アクセス制御などは，セキュリティ管理者が担うべき責務と考えられる。

(4) セキュリティ担当者の役割

セキュリティ担当者は前述のセキュリティ管理者の指示に基づいて，実際に設定や監視などの作業を行う責務を有する。

【評価内容】

セキュリティ基本方針・対策基準と実施手順を入手し，以下の項目についての責任が正式に割り当てられていることを確認する。

・セキュリティ基本方針・対策基準および実施手順の作成と周知
・セキュリティ警告の監視，分析および報告
・事故発生時の対応手順および報告手順の作成と配布
・ユーザアカウントの管理
・データに対するすべてのアクセスの監視と制御

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。

【解説】

自組織で適切なセキュリティ対策が施されていても，業務委託先等の外部のシステムで発生したインシデント（事件・出来事）の影響を受ける可能性がある。このため，学校教育データを業務委託先と共有する場合には，契約に盛り込むべき事項や管理の実施手順を事前に明確に定めることが必要となる。契約相手が自組織と同程度のセキュリティ水準を確保するよう求めるためには，セキュリティ上の要求事項を明確にし，契約の締結にあたり合意を得る必要がある。なお，以下の 3 点については外部委託において重要な事項であるため，あわせて確認することを勧める。

・委託先の選定基準に含まれるべき事項
・委託契約において契約書に盛り込むべき事項
・契約内容の遵守状況に関する確認事項

【評価内容】

学校教育データをサービスプロバイダ（例えば，バックアップテープ保管施設，Web ホスティング会社やセキュリティサービスプロバイダ等）と共有している場合には基本方針・対策基準と実施手順のレビュー，関連文書のレビューを行い，以下を確認する。

(1) サービスプロバイダの一覧が保持されていること。
(2) 学校教育データのセキュリティ維持の責任が，当該サービスプロバイダにあることを，当該サービスプロバイダが認める旨が明記されていること。
(3) 基本方針・対策基準と実施手順が文書化されており，すべてのサービスプロバイダとの契約前に適切な実務検証を実施することが含まれていること。
(4) サービスプロバイダの本推奨仕様遵守状況を監視するための運用手順について，当該サービスプロバイダ自らが検証していること。

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。

【解説】

学校の管理者には，システムの開発，構築，運用者が適切に業務を遂行していることを監督する責任がある。新しいシステムを受け入れる際に，受け入れの手続きが適切に実施されることを確認することは，学校の管理者として重要な責務である。

【評価内容】

新しいシステムを受け入れる際の実施手順等を入手し，以下を確認する。

(1) 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が明確になっていること。
(2) 新しいシステムを受け入れる際の実施手順等について，システムの開発，構築，運用者と学校の管理者が合意していること。
(3) 新しいシステムを受け入れる際に試験を行うことが記載されていること。

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。

【解説】

学校の管理者には，システムの運用者が適切に業務を遂行していることを監督する責任がある。システムの運用者が，ネットワークにおける情報のセキュリティを確保していることや，無認可のアクセスからのネットワークサービス保護を確実に行っていることを確認することは，学校の管理者として重要な責務である。

【評価内容】

ネットワーク管理に関する実施手順等を入手し，以下を確認する。

(1) ネットワークにおける情報のセキュリティ（例えば機器設定情報の保護等）を確保する管理策について規定していること。
(2) 無許可のアクセスからのネットワークサービス保護（例えばリモートアクセスの制限等）を確保する以下の管理策について規定していること。

・使用していない状態が一定時間続いた後のリモートアクセス接続の自動切断が求められていること。
・保守業務委託者用リモートアクセスは保守業務委託者が必要とする時のみ使用可能にし，使用後に直ちに使用不可能な状態にすることが求められていること。
・リモートアクセスを通じて遠隔より学校教育データにアクセスする場合，パソコン内の磁気ディスク装置やパソコンに外部接続されている各種記録装置，または USB メモリ等のリムーバブルメディアへ学校教育データを保管することの禁止が求められていること。

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。

【解説】

情報処理設備が適切に使用されていることを確認することは，学校の管理者として重要な責務である。学校の管理者は，情報処理設備の使用状況の監視について，システムの運用者が行う実施手順を確認するとともに，定期報告会等においてシステムの運用者が行う監視活動の結果をレビューする必要がある。

【評価内容】

以下を確認する。

(1) 情報処理設備の使用状況の監視に関する実施手順が整備されていること。
(2) 学校の管理者が，定期報告会等においてシステムの運用者が行う監視活動の結果をレビューしていること。

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。

【解説】

組織のすべての領域における情報セキュリティ活動には様々な法令が適用される。特に学校教育にかかわる活動においては，知的財産を保護するための法令の遵守は重要となる。

(1) 違法なソフトウェアの利用を防止するためには，定評のある供給元からソフトウェアを取得することが望ましい。
(2) ソフトウェアのライセンス契約に違反することは重大な法令違反である。
(3) 著作権を侵害するような行為は重大な法令違反である。

【評価内容】

職務規定等を入手し，知的財産を保護するための上記の指針について考慮した記述が記載されていることを確認する。また，教育実施の記録，業務従事者への周知事項の記録を入手し，これらの事項が業務従事者に周知されていることを確認する。

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。

【解説】

組織のすべての領域における情報セキュリティ活動には様々な法令が適用される。特に学校教育にかかわる活動においては，個人情報を保護するための法令の遵守は重要となる。

【評価内容】

個人情報の保護に関する方針が記載された文書（個人情報保護規程など）を入手し，個人情報を保護するための方針が確立していることを確認する。また，教育実施の記録，教職員への周知事項の記録を入手し，これらの方針が教職員に周知されていることを確認する。

（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。

【解説】

データの保護という観点において，最も有効な対応策は，必要としないデータは保管しないことである。また，保管するデータについても，データ保管ポリシーに従い，保管すべき情報，保管期間などを限定する必要がある。なお，データの廃棄を確実にするためには，例えばデータ消去ツールのような，専用の媒体処理装置の導入を検討すべきである。さらに，大量の媒体を処理する必要がある場合には，関連法令が適用される国内の専門業者に委託することも考慮すべきである。

【評価内容】

データの保管と廃棄に関する基本方針・対策基準と実施手順を入手し，以下の項目を確認する。

(1) 学校教育データの保管に関して，データ保管に関する法律上，規制上，業務上の要件が含まれていることを確認する。これには，具体的な学校教育データの保管に関する要件が含まれていること。（例：学校教育データは，X の期間，Y という業務上の理由で保管する必要がある）
(2) 学校教育データに関して，法律上，規制上，業務上の必要性がなくなった場合の，データの廃棄に関する要件が含まれていること。
(3) 学校教育データのすべての保管範囲が含まれていること。
(4) 業務上の保管要件を超えて格納されている学校教育データを少なくとも 1 年毎に削除するための自動的なプロセス，もしくは格納された学校教育データが業務上の保管要件を超えていないかを確認するための少なくとも 1 年毎のレビュー実施要件が含まれていること。

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。

【解説】

重要な情報資産は，その情報資産を取扱う者にとって，それが重要であることが一目でわかることが重要である。ラベル付けを行うことにより重要な情報資産が目立つことは，不正を誘発する恐れがあるとする意見もある。しかし，ラベル付けを行わないことによって重要な情報資産が放置されるリスクは，ラベル付けを行うことに伴うリスクより重大である。

【評価内容】

学校教育データが保管または記載された情報資産のサンプルを入手し，ラベル付け等の手段により，学校教育データを含んだものであることが識別できるようになっていることを確認する。

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。

【解説】

教職員は，個人識別データ，氏名等の個人を特定できる情報を表示する際は必要な範囲のみとすることが求められる。

また，システム開発を委託事業者に発注する等の場合には，個人識別データおよび氏名情報の表示を必要最低限にするように委託事業者に指示する。

【評価内容】

基本方針・対策基準文書の入手とレビューおよび個人識別データの表示（例えば，表示画面や各種の印刷物）の確認を行い，正当な業務上の理由がない限り，学校教育データを表示する際に個人を特定できないようになっていることを確認する。

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。

【解説】

学校教育データは個人情報保護法に準拠した取扱いが求められる。

したがって，学校教育データを保管する場合には，パスワード設定・データを暗号化するなどの対策を講ずることにより，不正な閲覧を防止することが必要となる。

注：「学校情報セキュリティ・ハンドブック」の P.6～7 “ パスワード設定・暗号化で盗難・紛失に備える ” を参照（「一太郎」他でのファイル読み取りパスワード設定方法を記述している）。
http://www.cec.or.jp/seculib/handbook/18ghjbs_5.pdf

【評価内容】

(1) 学校教育データが保管されたファイルのサンプルを入手し，パスワード設定・暗号化等の手段により，不正な閲覧が防止されていることを確認する。

(2) サンプリングした学校教育データベースの複数のテーブルあるいはファイルを調査し，個人識別データ，氏名等個人を特定できる情報が暗号化されていることを確認する。

ファイルの読み取りパスワード設定方法例
＜Microsoft Excel2007 ※場合＞

①  （Microsoft Office ボタン）をクリックし，「名前を付けて保存」をクリックします。
②「名前を付けて保存」ダイアログボックスで，「ツール」の「全般オプション」をクリックします。
③「読み取りパスワード」にパスワードを入力し，「OK」をクリックします。
④「パスワードの確認」にパスワードをもう一度入力し，「OK」をクリックします。
⑤「名前を付けて保存」ダイアログボックスで，「保存」をクリックします。

注：Word2007※も同様に読み取りパスワード設定が可能です。

※Excel2007 および Word2007 は，Microsoft 社の登録商標です。

図 5． ファイルの読み取りパスワードの設定例

(3) サンプリングしたリムーバブルメディア（例：外付け磁気ディスク装置，USB メモリ，CD-ROM）を調査し，個人識別データおよび氏名等の個人を特定できる情報が判読不可能な状態になっていることを確認する。
(4) パソコンのディスク暗号化をしている場合，暗号化されたファイルへのアクセスが，OS へのログオン認証とは別の認証が要求されるように実装されていることを確認する。（例えばパソコンの OS にログオンする前に暗号化されたファイルへのアクセスのための認証が必要になっている）
(5) パスワードは本推奨基準どおりに設定，運用されている，アクセスに必要な IC カード等が適切に管理されていることを確認する。
(6) 学校教育データをリムーバブルメディアに保管する場合には，すべての場所において暗号化する運用になっていることを確認する。
注：ディスク暗号化ではリムーバブルメディアを暗号化できないことがよくあるため，これらの媒体に保管されたデータは個別に暗号化を行う必要がある。

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。

【解説】

学校教育データは電子メールで学校外へ送信してはならない。

【評価内容】

(1) 学校教育データが電子メールやインスタントメッセージ等のメッセージングツールを通じて送信される場合，強力な暗号が使用されていることを確認する。
(2) 暗号化されていない学校教育データを，メッセージングツールを通じて送信しない旨を規定した基本方針・対策基準が存在することを確認する。

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。

【解説】

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自らの責任を十分認識すべきである。このため，情報セキュリティに関する責任を果たすことについての記載がある誓約書に同意し，署名することは，学校教育データを取扱う者の認識を高めるうえで有効である。

【評価内容】

誓約書を入手し，学校教育データを取扱う者が，誓約書に同意したうえで署名していることを確認する。

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。

【解説】

ソフトウェア，書類，設備など，学校教育データが保管あるいは記載されている可能性のある重要な情報資産は，不要となった時点において確実に破棄することが必要である。一方で，雇用終了時および勤務校変更時に，すべての教職員に対して，重要な情報資産を破棄したことを確認することは困難である。このため，前もって支給されたソフトウェア，書類，設備のすべてを，雇用終了時および勤務校変更時に返却させる必要がある。

【評価内容】

以下の項目を確認する。

(1) 教職員の雇用終了時および勤務校変更時の手続きにおいて，返却すべきソフトウェア，書類，設備などが明確になっていること。
(2) 返却すべきソフトウェア，書類，設備などが確実に返却されたことを証明する資料（返却の事実を記載した記録など）が保管されていること。

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。

【解説】

不特定多数の者が往来するような場所，あるいは通常無人となるような場所に，コンピュータや周辺機器が放置されることは，不正利用あるいは盗難を回避するうえで望ましくない。また，コンピュータの冷却口を塞ぐような設置，漏電や火災事故の原因となるいわゆるタコ足配線などが行われることのないよう，設置方法を管理することが必要である。

【評価内容】

コンピュータや周辺機器の設置状況について，以下の項目を確認する。

(1) 不特定多数の者が往来するような場所，あるいは通常無人となるような場所に，コンピュータや周辺機器が放置されていないこと。
(2) コンピュータの冷却口を塞ぐような設置，漏電や火災事故の原因となるいわゆるタコ足配線などが行われていないこと。

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。

【解説】

媒体は，教務・校務または法令上の理由で不要になった場合，破壊や消去する必要がある。紙媒体の場合はクロスカット裁断，焼却，溶解する。電子媒体の場合は，裁断または破壊する。何らかの理由で裁断または破棄できない場合は，専用のデータ消去ツールを利用しデータを完全に消去する。自組織において実施する場合は，作業担当者のみならず責任者立会いの下で行う必要がある。破壊/消去作業が不十分だと情報が流出する可能性を残すため，厳重に監視する。業者サービスを利用する場合は，責任者が立会い可能な業者を選定する必要がある。業者自身は厳密に破壊/消去作業を行うとしているが，万一，不手際が発生した場合に備え，責任者の立会を行う必要がある。

【評価内容】

(1) 媒体の定期的な廃棄に関する基本方針・対策基準を調査し，学校教育データを含む媒体すべてが対象となっ

ていることと，次の項目を確認する。

- ハードコピーの資料が，再構成できないことを担保する合理的な根拠に基づき，クロスカット裁断，焼却，あるいはパルプ状に溶解されていること。
- 廃棄予定の情報が格納されたコンテナ（収納箱）を観察し，コンテナが安全であること。例えば，コンテナは，格納された媒体へのアクセスを防止するために鍵がかけられていること。

(2) 電子媒体に保管された学校教育データは，業界基準において定められた安全な消去方式に準拠したデータ消去ツールを用いて，あるいはその他の物理的媒体破壊（例えば，消磁）により，復元不可能な状態まで破壊されることを確認する。

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。

【解説】

学校教育データが含まれた書類やディスクなどは，持ち出しや持ち込み，運搬に際し，その記録が追跡できることが必要である。社外における運搬については，国内の大手配送業者や大手警備会社のサービスを利用する方法もある。運搬（配達）状況を確認できるサービスや，セキュリティ性の高い搬送サービスが提供されている。

【評価内容】

(1) 学校教育データを含む媒体の配布を管理するための基本方針・対策基準が存在し，その基本方針・対策基準が個人に配布されたものを含むすべての配布媒体をカバーしていることを確認する。
(2) 「機密」と判別できるよう，すべての媒体が分類されていることを確認する。
(3) 施設外に送られるすべての媒体は，記録が取られ，管理責任者による承認を受け，安全な配送機関，または追跡可能なその他の配送手段を使用して送付されることを確認する。

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。

【解説】

ユーザパスワードの管理は情報セキュリティの基本であり，不正に利用されることがないように，確実な管理を実施する必要がある。

【評価内容】

(1) システムコンポーネントのサンプルについて，ユーザ ID リストを調査し，以下の項目を確認する。
・デフォルトのユーザ ID およびデフォルトアカウントは，無効化もしくは削除されていること。
・システム管理や他の重要な機能に使用される共有 ID が存在しないこと。
・すべてのシステムコンポーネントの管理に共有 ID やデフォルト ID が使用されていないこと。
(2) パスワード基本方針・対策基準および実施手順を調査し，グループパスワードや共有パスワードが明示的に禁止されていることを確認する。
(3) システム管理者にインタビューを行い，たとえ求められても，グループパスワードや共有パスワードが付与されないことを確認する。
(4) システムコンポーネントのサンプルについて，システム設定を調査し，パスワードのパラメータ設定で少なくとも 90 日毎のパスワード変更が必要となっていることを確認する。
(5) システムコンポーネントのサンプルについて，システム設定を調査し，パスワードのパラメータ設定で最小 7 文字以上のパスワード長が必要となっていることを確認する。
(6) システムコンポーネントのサンプルについて，システム設定を調査し，パスワードのパラメータが，数字と英字の両方を含んだパスワードを求めるよう設定されていることを確認する。

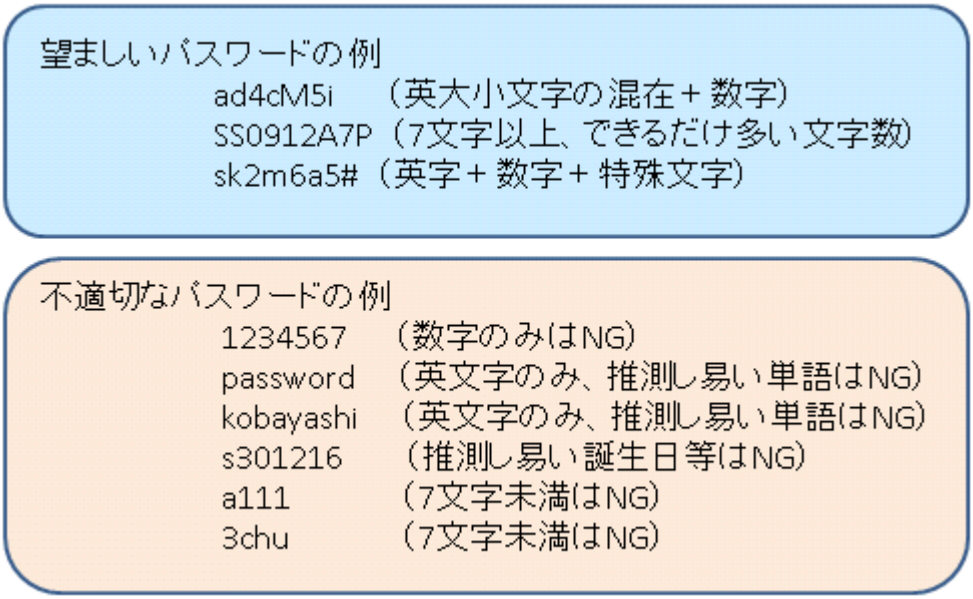

図 6.　望ましいパスワード／不適切なパスワードの例

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。

【解説】

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か，OS に付属のファイアウォール機能を利用し，有効に稼働させることにより，コンピュータ端末を不正侵入等の脅威から防御する。

【評価内容】

(1) インターネットに直接接続するモバイル端末（ノートパソコンや携帯電話など）や，教職員使用のコンピュータで，校内ネットワークへのアクセスに使用されるもの（例：教職員が使用するノートパソコン）にパーソナルファイアウォールソフトウェアが導入されており，正常に動作していることを確認する。

(2) パーソナルファイアウォールソフトウェアが組織の基準に基づき設定されており，モバイル端末の利用者によって変更されていないことを確認する。

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。

【解説】

サーバおよびこれに接続されるパソコンには，アンチウィルスソフトウェアを導入しなければならない。現在一般的にコンピュータウィルスと呼ばれているものには，ワーム，トロイの木馬，ボットなどがあり，その種類・攻撃手法が年々多種多様化してきている。また，コンピュータやインターネットの普及に伴いウィルスに対する脅威や被害が年々増加しており，ウィルス対策の必要性が非常に高まっている。

すべての既知のタイプのウィルスに代表される悪意のあるソフトウェア（例えば，トロイの木馬，ワーム，スパイウェア，アドウェア，ルートキット等）に対して検知，駆除，保護が可能とするためには，ベンダがサポート対象としているバージョンのアンチウィルスソフトウェアが導入され，それが有効になっていること，常に最新のウィルス定義ファイルに更新されていることが必要である。

【評価内容】

(1) 悪意あるソフトウェアによって影響を受けるすべての種類のオペレーティングシステムについて，システムコンポーネントのサンプルを調査し，アンチウィルスソフトウェアが導入されていることを確認する。
(2) 導入されているアンチウィルスソフトウェアは，最新のウィルス定義ファイルが適用されていることを確認する。

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。

【解説】

パッチの適用等により，アンチウィルスソフトウェアが最新の状態となっている必要がある。また，適切に実行されており，ウィルスの検知および駆除が実行されているとともに，監査ログを生成していることを確認する必要がある。

【評価内容】

すべてのアンチウィルスメカニズムが最新で，正常に稼動しており，監査ログが生成できることを確認するため，以下の項目を確認する。

(1) 基本方針・対策基準を入手およびレビューし，アンチウィルスソフトウェアおよびウィルス定義ファイルの更新が要求されていること。
(2) 悪意あるソフトウェアによって影響を受けるすべての種類のオペレーティングシステムについて，システムコンポーネントのサンプルを調査し，自動更新と定期スキャンが実施されていること。
(3) システムコンポーネントをサンプリングし，アンチウィルスソフトウェアのログの生成が有効になっており，ログが要件に従って保持されていること。

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。

【解説】

組織のすべての領域における情報セキュリティ活動には様々な法令が適用される。特に学校教育にかかわる活動においては，知的財産を保護するための法令の遵守は重要となる。

(1) 違法なソフトウェアの利用を防止するためには，定評のある供給元からソフトウェアを取得することが望ましい。

(2) 著作権を侵害するような行為は重大な法令違反である。

【評価内容】

知的財産権を保護することの重要性について，教職員が理解していることを確認する。

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と学校の方針および法令を遵守すること。

【解説】

組織のすべての領域における情報セキュリティ活動には様々な法令が適用される。特に学校教育にかかわる活動においては，個人情報を保護するための法令の遵守は重要となる。

【評価内容】

個人情報の保護に関する学校の方針を，教職員が遵守していることを確認する。

（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。

【解説】

アプリケーションシステムを開発する等において個人識別データおよび氏名等の個人を特定する情報を表示する場合には，その必要性について十分に検討し，それらの表示を必要最低限にする。

【評価内容】

基本方針・対策基準文書の入手とレビュー，個人識別データおよび氏名の表示（例えば，表示画面や各種の印刷物）の確認を行い，正当な業務上の理由がない限り，学校教育データを表示する際に個人を特定する情報がトランケーションまたはマスキングされていることを確認する。

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。

【解説】

学校教育データは個人情報保護法に準拠した取扱いが求められる。したがって，学校教育データを保管する場合には，データを暗号化するなどの対策を講ずることにより，不正な閲覧を防止することが必要となる。特に，学校教育データを含むバックアップ媒体およびログにおいては，対策漏れに注意する必要がある。

【評価内容】

(1) 保管データの保護に使われているシステムについて，ベンダ，システムやプロセスの種類，暗号化アルゴリズムなど（該当する場合）が記載された文書を入手し，レビューする。次の方法の１つにより，個人識別データおよび氏名等の個人を特定する情報が判読不可能な状態になっていることを確認する。
- SHA-1 などのワンウェイハッシュ化
- 関連する暗号鍵管理プロセスと手順を伴う，強力な暗号化

(2) サンプリングしたデータ保管場所内の複数のテーブルあるいはファイルを調査し，個人識別データおよび氏名等の個人を特定する情報が暗号化されている（すなわち，平文で格納されていない）ことを確認する。

(3) サンプリングした監査ログを調査し，個人識別データおよび氏名等の個人を特定する情報が暗号化され，安全な状態になっていることを確認する。

(4) ディスク暗号化を使用している場合，暗号化されたファイルシステムへの論理アクセスが，ネイティブな OS のメカニズムとは独立したメカニズムで実装されていることを確認する。（例えば，ローカル・ユーザ・アカウント・データベースを使用しない）

(5) リムーバブルメディアに記録された学校教育データは，すべて暗号化されていることを確認する。

注：ディスク暗号化ではリムーバブルメディアを暗号化できないことがよくあるため，これらの媒体に保管されたデータは個別に暗号化を行う必要がある。

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。

【解説】

運用の対象となるシステムにおいて使用される暗号鍵を適切に管理する必要がある。暗号鍵の管理は，「暗号鍵管理手順書」に基づいて行われなければならない。

【評価内容】

学校教育データの暗号化に使用されている暗号鍵を漏えいと不正使用から保護するため,次の項目を確認する。

(1) ユーザのアクセスリストを調査し，暗号鍵へのアクセスがごく少数の管理者に制限されていること。
(2) システム設定ファイルを調査し，暗号鍵が暗号化された状態で保管されていること，鍵暗号鍵がデータ暗号鍵と分けて保管されていること。

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

【解説】

暗号鍵管理手順書の策定に際しては，電子認証局において策定されている CPS（Certification Practice Statements ，認証業務運用規程）が参考になる。CPS は，電子認証サービスの約款のようなものであり，電子認証局（CA）が管理する各種の暗号鍵についての管理手順が記載されている。CPS のガイドラインは，RFC3647 として公表されている。CPS 自体は公開文書であるため，電子認証局の情報公開サイトにおいて入手可能である。また，暗号化，復号化に関しては，暗号鍵の管理が非常に重要となる。特に，公開鍵暗号方式の秘密鍵に関しては，悪意の第三者に漏えいした場合に，学校教育データの漏えい，改ざんなどを招くリスクが非常に高いため，暗号鍵の生成，保管，廃棄に至るライフサイクルを適切に管理する必要がある。

なお，暗号鍵の管理にはハードウェアセキュリティモジュール（HSM）の導入を推奨する。HSM は，より高いセキュリティを備えており，機器をこじ開けようとした場合に保管されている暗号鍵を破壊する機能や，複数の管理者が秘密鍵を分割して管理し，それぞれの役割を持った全員が揃わないと使用できないようにする機能などを持っている。

【評価内容】

学校教育データの暗号化に使用する暗号鍵の管理手順が存在することを確認する。さらに暗号鍵管理手順を調査し，次の項目を確認する。

(1) 強力な暗号鍵の生成が義務付けられていること。

(2) 暗号鍵の安全な配布が義務付けられていること。
(3) 暗号鍵の安全な保管が義務付けられていること。
(4) 定期的な暗号鍵の変更が義務付けられていること。暗号鍵変更手順が少なくとも年 1 回は行われていること。
(5) 古い暗号鍵を破棄することが義務付けられていること（例えば，暗号鍵の破棄および適切な失効）。
(6) セキュリティ侵害が発生あるいは疑われた場合における暗号鍵の交換要求について記述されていること。
(7) 暗号鍵の知識分割と二重管理が義務付けられていること（例えば，暗号鍵全体を再構築するには，2～3 人を必要とし，各自が暗号鍵の一部のみを知っている，あるいは HSM が導入され知識分割機能を使用している）。
(8) 暗号鍵の不正置換の防止が義務付けられていること。
(9) 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が義務付けられていること。

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。

【解説】

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自らの責任を十分認識すべきである。このため，情報セキュリティに関する責任を果たすことについての記載がある誓約書に同意し，署名することは，学校教育データを取扱う者の認識を高めるうえで有効である。

【評価内容】

誓約書を入手し，以下の項目を確認する。

(1) 誓約書に情報セキュリティに関する責任が記載されていること。
(2) 学校教育データを取扱う者が，誓約書に同意したうえで署名していること。

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。

【解説】

すべての情報および情報処理施設に対するアクセス管理を徹底するためには，利用者の登録に加えて，登録削除について管理が適切に行われなければならない。

【評価内容】

教職員の雇用終了時および勤務校変更時の手続きにおいて，該当する情報が情報システムの利用者を管理する部署に通知される手順となっていること，あるいは雇用終了情報がシステム連携して削除処理等が行われることを確認する。

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。

【解説】

学校教育データまたはそれを保管するシステムを保護するために，物理的なアクセス制限を実施することが求められている。施設への立ち入り管理については，訪問者を含むすべての入室者を適切に管理しなければならない。

訪問者を受け入れる会議室では，DHCP が有効になったネットワークポートがあってはならない。また，訪問者がアクティブな情報コンセントのあるエリアに入るときは，必ず案内者が同伴することが必要である。

【評価内容】

(1) コンピュータルーム，データセンタ，その他学校教育データ環境に含まれるシステムが存在する物理エリアについて，以下の物理セキュリティ管理が存在することを確認する。
・認証用バッジ，IC カード，鍵およびその他のデバイスによって物理アクセスが制限されていること。

(2) 重要なエリアの出入口を監視するためのビデオカメラ，または他のアクセス管理装置が存在することを確認する。ビデオカメラまたは他のアクセス管理装置は，不正改造または無効化に対して保護されていることを確認する。

(3) ビデオカメラまたは他のアクセス管理装置のデータは少なくとも 3 ヶ月間保管されているかを確認する。

(4) 情報コンセントが，許可を受けた教職員に必要な場合のみ有効化されることを確認する。

(5) 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が適切に制限されていることを確認する。

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。

【解説】

訪問者を教職員と区別し管理することは，物理的セキュリティの向上を図るうえで重要である。また，入退館あるいは入退室の記録は，物理監査証跡として保管しなければならない。

【評価内容】

(1) 教職員，訪問者にバッジを貸与するためのプロセスと手順を調査し，以下の項目が含まれていることを確認する。
・新規のバッジ貸与，アクセス要件の変更および離職した教職員や期限が切れた訪問者のバッジの返却
・バッジ管理システムへのアクセス制限
(2) 施設内の人々を観察し，教職員と訪問者を容易に区別できることを確認する。

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。

【解説】

学校教育データが処理または保守されているエリアでは，すべての訪問者を教職員と区別できるようにする必要がある。

【評価内容】

教職員／訪問者の管理が以下のとおり行われていることを確認する。

(1) 訪問者を観察し，訪問者のバッジの使用を確認する。データセンタへのアクセスを試み，訪問者のバッジでは，学校教育データを格納した物理エリアへは案内者の同伴なしには入れないこと。
(2) 教職員と訪問者のバッジを観察し，バッジにより，教職員と訪問者が明確に区別できることおよび訪問者のバッジに有効期限が設定されていること。
(3) 施設を出る訪問者を観察し，訪問者が退出時または有効期限切れ時にバッジの返却を求められること。

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。

【解説】

訪問者のログは必ずしも電子データである必要はなく，入室記録簿のように，紙面に記録したものでも有効である。

【評価内容】

(1) 学校教育データが格納または伝送されるコンピュータルームやデータセンタへの物理アクセスについて，訪問者ログが記録されていることを確認する。
(2) ログは，訪問者の氏名，勤務先，物理アクセスを許可した教職員を含んでおり，少なくとも 3 ケ月間保管されていることを確認する。

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。

【解説】

媒体は，業務上または法律上不要になった場合，破壊や消去する必要がある。紙媒体の場合はクロスカット裁断，焼却，溶解する。電子媒体の場合は，データを消去，裁断，または破壊する。学校にて実施する場合は，作業担当者のみならず責任者立会いの下で行う必要がある。破壊/消去作業が不十分だと情報が流出する可能性を残すため，厳重に監視する。業者サービスを利用する場合は，学校の責任者が立会い可能な業者を選定する必要がある。業者自身は厳密に破壊/消去作業を行うとしているが，万一，不手際が発生した場合に備え，学校責任者の立会を行う必要がある。

【評価内容】

(1) 媒体の定期的な廃棄に関する基本方針・対策基準を調査し，学校教育データを含む媒体すべてが対象となっていることと，次の項目を確認する。
・ハードコピーの資料が，再構成できないことを担保する合理的な根拠に基づき，クロスカット裁断，焼却，あるいはパルプ状に溶解されていること。
・廃棄予定の情報が格納されたコンテナを観察し，コンテナが安全であること。例えば，コンテナは，格納された媒体へのアクセスを防止するために鍵がかけられていること。
(2) 電子媒体に保管された学校教育データは，業界基準において定められた安全な消去方式に準拠したワイプ・プログラムを用いて，あるいはその他の物理的媒体破壊（例えば，消磁）により，復元不可能な状態まで破壊されることを確認する。

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。

【解説】

学校教育データが含まれた書類やディスクなどは，持ち出しや持ち込み，運搬に際し，その記録が追跡できることが必要である。組織外における運搬については，国内の大手配送業者や大手警備会社のサービスを利用する方法もある。運搬（配達）状況を確認できるサービスや，セキュリティ性の高い搬送サービスが提供されている。

【評価内容】

(1) 学校教育データを含む媒体の配布を管理するための基本方針・対策基準が存在し，その基本方針・対策基準が個人に配布されたものを含むすべての配布媒体をカバーしていることを確認する。
(2) 「機密」と判別できるよう，すべての媒体が分類されていることを確認する。
(3) 施設外に送られるすべての媒体は，記録が取られ，管理責任者による承認を受け，安全な配送機関，または

追跡可能なその他の配送手段を使用して送付されることを確認する。

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。

【解説】

学校教育データが保管されたすべての媒体を安全なエリア外に持ち出す場合には，適切な管理者がこれを承認する。

特に媒体が個人に配布される場合には，厳密に運用する必要がある。

【評価内容】

学校教育データが記録されたすべての媒体について，直近数日分の持ち出し記録をサンプリングして，適切な管理責任者の承認が存在することを確認する。

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）。

【解説】

ユーザアカウント保守手順には，ユーザアカウントの生成，配布，変更および削除に関する手順の他に，無効なユーザアカウントが存在しないことを定期的に確認する手順が含まれることが必要である。また，ログレビュー手順には，不正アクセスや攻撃の痕跡が発見された場合における対応手順が含まれることが必要である。

【評価内容】

日常的な運用上のセキュリティ手順を調査する。実施手順がこの仕様に準拠し，各要件について管理および技術手順が規定されていることを確認する。

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

【解説】

変更管理手順に含める事項については，次のとおり。

(a) 変更が与える影響の文書化
システムコンポーネントの変更を実施する際に，この変更が与える影響について，特に利用者に与える影響について文書化し，明確にしておく必要がある。
(b) 適切な管理者による変更の承認
文書化された変更の影響を含め，システムコンポーネントの変更の実施について管理者が内容を確認し，承認する。
(c) 運用機能のテスト
システムコンポーネントの変更に伴い，運用機能（監視機能，監視手順あるいは保守手順等）も変更になる場合には，変更を実施する前に机上テスト等を行い，有効に機能することを事前に確認する。
(d) 回復手順
変更を実施した結果が当初の計画と異なる場合には，管理者の判断で原状回復を行う。このときの回復手順については，文書化することが望ましい。

【評価内容】

システムコンポーネントのサンプルについて，各システムコンポーネントについて最新の変更／セキュリティパッチを調査し，それらの変更が関連する変更管理手順に基づくものかどうかを確認する。

・変更が与える影響に関する記述が，変更管理文書に含まれていること。
・管理者による適切な承認が存在すること。
・運用機能のテストが実施されていること。
・回復手順が用意されていること。

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。

【解説】

脆弱性検査には，通常自動検査ツールが使用される。自動検査ツールは，設定した調査対象の機器に対してポートスキャンを実施し，対象システム上で提供されるサービスを特定する。その上で特定されたサービスに対して，実際に脆弱性が存在するかどうか確認するために実際の攻撃パケットを送信するテストを行う。テスト対象からの応答内容により最終的に脆弱性の存在を判断する。ペネトレーションテストと異なり，脆弱性検査は，テストの目的が脆弱性の有無を判定することにあるため，脆弱性の利用による二次的な被害内容およびそのシステムが持つ脆弱性の影響度などに関して判断することは行なわれない。

【評価内容】

(1) 内部ネットワーク，ホストコンピュータ，アプリケーションに対する過去 4 回の 3 ヵ月脆弱性検査の出力を調査し，学校教育データ環境内の装置のセキュリティテストが定期的に実行されていることを確認する。脆弱性を対策した後に実施するスキャンプロセスにおいて，良好な結果が得られるまで対策とスキャンが続行されていることを確認する。
　　注：ネットワーク変更に伴う外部スキャンと内部スキャンは，知識を持った校内スタッフあるいは第三者が行うことも可能である。
(2) 外部スキャンが 3 ヵ月毎に実行されていることを確認する。

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

【解説】

脆弱性検査がシステムの脆弱性の検出を目的としたテストであるのに対し，ペネトレーションテストは，発見された脆弱性に関して，更に攻撃者の視点からその脆弱性の有効性を判断し，システム全体としてのセキュリティ対策の有効性を評価することを目的としたテストとなっている。日常的な運用としては，脆弱性検査で脆弱性の発見と修正対応というサイクルを実施することにより脆弱性管理を行う一方で，ペネトレーションテストにより，日々の検査では発見しきれない脆弱性の検出，万一の被害が発生した際の影響程度を測定したりすることが

可能となる。

ペネトレーションテストの実施には，セキュリティ専業会社のサービスを利用することが多いと思われる。仮に自組織内で行うのであれば，インターネット上で入手可能なフリーのツール，ならびにペネトレーションテスト用の商用ツールを利用することで対応することも可能ではある。ただし，検査の実施には，システムに対する第三者的な視点，セキュリティに関する専門知識，攻撃者の視点などの要素が必要となるため，内部でペネトレーションテストの実施を計画する際は，内部で実施することの利点・欠点をよく検討する必要がある。

【評価内容】

(1) 最新のペネトレーションテストの結果を入手し，ペネトレーションテストが少なくとも 1 年に 1 回および環境の大きな変更の後に実施されていることを確認する。脆弱性が見つかった場合，修正され再テストが実施されていることを確認する。
(2) テストは，内部の適当な部署，または適当な外部の第三者によって実施されていることを確認する。適用可能であれば，組織として独立していることが望ましい。
(3) ネットワーク層を含むペネトレーションテストが実施されていることを確認する。このテストは，オペレーティングシステムとともに，ネットワーク機能を補助するコンポーネントを含まなければならない。
(4) アプリケーション層を含むペネトレーションテストが実施されていることを確認する。

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。

【解説】

セキュリティ基本方針･対策基準や他の文書において,これらの責務に関連する記述がされている必要がある。特に情報システムの構成要素に対しては，セキュリティ警告への対応，アカウント管理，アクセス制御といったシステムの運用に関する責務を明確に定めることが重要である。以下は，代表的な役割とその責務についてである。

(1) 管理責任者の役割
セキュリティ基本方針・対策基準は組織の部門を跨いで適用されるケースが多く，一般的にそれらの部門を統括する管理責任者がその責務を負うことが多い。このため，すべての関係者とシステム構成要素を対象としたセキュリティ基本方針・対策基準を確立する責務は，上席の管理責任者が担うものと考えられる。
(2) セキュリティ責任者の役割
個々のセキュリティ対策が適切かつ確実に実施されるようにする責務は，情報システムを統括するセキュリティ責任者が担うことが想定される。特にセキュリティ事故への対応と報告手順を確立し，それらを迅速に取扱う責務はセキュリティ責任者が担うべき重要な責務の一つと考えられる。
(3) セキュリティ管理者の役割
具体的なシステムのセキュリティ設定や運用管理の実施は，セキュリティ管理者が責任を持つことになる。

セキュリティ警告への対応，アカウント管理，アクセス制御などは，セキュリティ管理者が担うべき責務と考えられる。

(4) セキュリティ担当者の役割

セキュリティ担当者は前述のセキュリティ管理者の指示に基づいて，実際に設定や監視などの作業を行う責務を有する。

【評価内容】

(1) セキュリティに精通した管理責任者に，情報セキュリティマネジメントの責務が正式に割り当てられていることを確認する。

(2) セキュリティ基本方針・対策基準と実施手順を調査し，以下の情報セキュリティの責務が特定され，正式に割り当てられていることを確認する。

- セキュリティ基本方針・対策基準および実施手順の確立と周知の責任が正式に割り当てられていること。
- 適切な情報セキュリティ管理者および学校の管理者に対して，セキュリティ警告の監視と分析，情報の配布における責任が割り当てられていること。
- セキュリティ事故対応および報告手順の作成と配布が正式に割り当てられていること。
- ユーザアカウントと認証管理の管理責任が正式に割り当てられていること。
- データに対するすべてのアクセスの監視と制御の責任が正式に割り当てられていること。

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。

【解説】

ホスティングプロバイダとは，各種のサービスを提供するサービスプロバイダの１つで，学校などの事業体のホストコンピュータやデータの管理サービスを提供する事業体のことである。ホスティングプロバイダは複数の事業体と契約している場合があるため，特にこのような要件を規定し，サービス提供先のそれぞれの事業体のホストコンピュータ環境やデータの保護を求めている。

【評価内容】

ホスティングプロバイダがサービス提供先である学校などの事業体のホストコンピュータ環境およびデータを保護していることを確認する。

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。

【解説】

参照頻度が少ないデータの場合は，組織外に保管する方法もある。大手倉庫業者などで機密文書などの保管サービスを実施しているので，それらを利用する事も検討する。文書保管や磁気テープ類保管，光ディスク保管サービスなどを実施している。また，バックアップ媒体は，上記の様な倉庫やデータセンタに保管する事が必要である。災害が発生した際の対策としても非常に有効である。よって，保管場所を選定する際は，防火対策や地震

対策が施されているか否かを確認する必要がある。

【評価内容】

最低 1 年に 1 回施設を訪問し，バックアップ媒体が安全に保管されていることを確認する。

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）。

【解説】

一般に，ベンダは，ユーザが製品を購入後に最新機能などの様々な機能を早く簡単に使用できるようにするため，デフォルト設定(初期状態)で多くの機能を予め使用可能な状態にしている。その結果として，デフォルト設定ではセキュリティレベルが低くなっていることがある。また，デフォルト設定情報やアカウント情報は，ベンダ提供のマニュアルやインターネットなどにより取得が容易である。このため，セキュリティを確保するためには，前節のファイアウォールなどのネットワーク構築，運用上のセキュリティ対策に加えて，機器自体についてもセキュリティ対策を行わなければならない。

機器ごとにデフォルトの状態からセキュリティを確立する作業は，要塞化，あるいは，セキュリティ・ハードニング(Security Hardening)と呼ばれている。要塞化の作業が完了するまでの間は，システムをネットワークに接続することを禁じなければならない。要塞化の設定には，OS，機器およびアプリケーションソフトウェアの製品のタイプごと，バージョンごとに異なる設定が多くある。

【評価内容】

(1) システムコンポーネント，重要なサーバ，無線アクセスポイントのサンプルを選択し，システム管理者の協力を得てデフォルトアカウントとパスワードを使用してデバイスへのログオンを試み，ログオンできないことを確認する。(デフォルトのアカウント／パスワードはベンダ提供のマニュアルやインターネット上の資料で調べる)

(2) 無線ネットワーク環境のベンダのデフォルト設定について，次の項目を確認する。また，すべての無線ネットワークにおいて，強力な暗号技術（例えば，AES）が実装されていることを確認する。

- 暗号鍵がインストール時のデフォルト値から変更されている。また，暗号鍵に関する情報を持つ人物が退職または異動する際には，その都度暗号鍵が変更される。
- 無線デバイスの SNMP コミュニティ文字列が，デフォルト値から変更されている。
- アクセスポイントのパスワード／パスフレーズがデフォルト値から変更されている。
- 無線ネットワークにおける認証および伝送において強力な暗号を維持（例えば，WPA/WPA2）するために，無線デバイスのファームウェアが更新されている。
- その他，セキュリティに関連する無線ベンダによるデフォルト値から変更されている。

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。

【解説】

システム設定基準とは，基本的にすべての機器設定に関する標準的な設定について定めた文書である。システム設定基準の策定により，組織内の機器ごとのセキュリティに高低のバラツキがないように管理ができるようになり，脆弱性を減らす効果が高く重要である。システム設定基準の項目例を以下に示す。

(1) アカウント関連
- デフォルトパスワードの変更
- 不要なアカウントの削除
- ユーザ権限の最小化
- 強固なパスワードの設定

(2) サービス関連
- 不要なサービスの停止
- Web，DNS，SNMP などサービス固有のセキュリティ設定
- デフォルトでインストールされるアプリケーションの削除
- サービスごとのサーバ機器の導入

(3) ファイルシステム関連
- パーティションの設定
- ファイルアクセス権の設定

(4) セキュリティパッチの適用
(5) ロギングの設定
(6) 管理用通信の暗号化
(7) ウィルス対策
(8) 無線 LAN のセキュリティ対策

【評価内容】

(1) すべての種類のシステムコンポーネントのシステム設定基準を調査し，システム設定基準が SANS，NIST など業界で承認されているシステム強化基準と一致していることを確認する。
(2) システム設定基準に，次の項目が含まれていることを確認する。
- 新しいシステムを設定する際に，システム設定基準が適用されること。
- １つのサーバにつき主要機能が１つだけ実装されること（例えば，Web サーバ，データベースサーバおよび DNS は，別々のサーバに実装されていなければならない）。
- 不要な，もしくは安全でないサービスやプロトコルを無効にすること，サービスの適切な使用の根拠が示され，文書化すること（例：FTP が使用されていない，もしくは SSH，その他の技術によって暗号化されている）。
- システムコンポーネントに関する一般的なセキュリティパラメータ設定が実施されること。

(3) システムコンポーネントのサンプルを選択し，一般的なセキュリティパラメータが適切に設定されていることを確認する。
(4) システムコンポーネントのサンプルを選択し，不要な機能（例：スクリプト，ドライバ，機能，サブシステム，ファイルシステムなど）がすべて取り除かれていることを確認する。また，有効になっている機能のみ存在し，すべて文書化され，セキュアに設定されていることを確認する。

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。

【解説】

アプリケーションシステムの多くの機能は,サードパーティベンダが提供する既存の製品から構成されている。それらの製品には，Web サーバ，アプリケーションサーバ，データベースなどがあるが，これらはどれも頻繁に脆弱性が発見されており，また，より一般的な利用者の多い製品ほど脆弱性が多く発見され攻撃目標となりやすい。これら製品のベンダは，自製品の脆弱性が発見される度にセキュリティパッチを提供することで自製品の安全性を維持している。学校教育データ環境下にあるすべての製品について，ベンダが提供するセキュリティパッチの存在を常に把握し，できる限り早い時期(遅くともリリース後 1 カ月以内)に適用することで，システムの安全性を確保しなければならない。

【評価内容】

(1) システムコンポーネントおよび関連したソフトウェアのサンプルを調査し，各システムに導入されたセキュリティパッチのリストと，ベンダから提供されている最新のセキュリティパッチのリストを比較して，最新のセキュリティパッチが導入されていることを確認する。
(2) セキュリティパッチの導入に関する基本方針・対策基準を調査し，優先度の高いすべての新しいセキュリティパッチを，1 ヶ月以内に導入することが要求されていることを確認する。

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。

【解説】

ソフトウェアアプリケーションを開発するにあたって，開発ライフサイクル全体を通じて情報セキュリティを徹底することが求められる。分析・設計フェーズから実装・テストフェーズを経て保守・運用フェーズへ至る開発ライフサイクルにおける情報セキュリティは特別なことを求められているわけではなく，一般的なシステム開発における情報セキュリティの原則・慣例に従えばよい。例えば，セキュリティパッチの適用やソフトウェアの設定変更前に必ずテストを実施しなければならない，開発環境・テスト環境・本番環境を物理的・論理的に分離しなければならない，といったことはその一例である。

【評価内容】

(1) ソフトウェア開発プロセスを記述した文書を入手し，開発プロセスが業界標準に基づいたもので，開発ライフサイクル全体を通じてセキュリティが含まれており，ソフトウェアアプリケーションが本推奨仕様の規定に従って開発されていることを確認する。

(2) ソフトウェア開発プロセス文書の調査，ソフトウェア開発者へのインタビュー，関連データ（ネットワーク構成文書，本番およびテスト環境データ，その他）のレビューを行い，次の項目を確認する。

・すべての変更（パッチを含む）が，本番環境への配置前にテストされていること。

・すべての入力の評価が実施されていること（クロスサイトスクリプティング，インジェクション攻撃，悪意あるファイルの実行等）。

・適切なエラー処理の評価が実施されていること。

・暗号化による安全な保管の評価が実施されていること。

・安全な通信の評価が実施されていること。

・適切な役割ベースのアクセス制御(RBAC) の評価が実施されていること。
・テスト／開発環境は本番環境から分離され，分離を強制するためのアクセス制御が施されていること。
・テスト／開発環境の担当者と本番環境の担当者について，職務の分離が行われていること。
・テスト／開発環境で使用されるデータを調査し，本番環境データがテストおよび開発目的で使用されていないこと，または使用前に安全な状態になっていること。
・本番システムを稼動させる前に，テストデータおよびテストアカウントが取り除かれていること。
・カスタムアプリケーションのアカウント，ユーザ ID，パスワードが，システムの実稼動前，もしくは顧客へのリリース前に取り除かれていること。

(3) 基本方針・対策基準を入手およびレビューし，内部のアプリケーションにおけるカスタム・アプリケーション・コードのすべての変更について，（手動あるいは自動のプロセスを用いた）以下に示すようなレビューを必要としていることを確認する。
・コードの変更は，コードレビューおよびセキュア・コーディングの手法に関する知識を持った開発者以外の者によってレビューされている。
・リリース前に適切な修正が実装されている。
・コードレビューの結果が，リリース前に責任者によってレビューされ承認されている。

(4) 基本方針・対策基準を入手およびレビューし，Web アプリケーションにおけるすべてのカスタム・アプリケーション・コードの変更について，（手動あるいは自動のプロセスを用いた）以下に示すようなレビューを必要としていることを確認する。
・コードの変更は，コードレビューおよびセキュア・コーディングの手法に関する知識を持った開発者以外の者によってレビューされている。
・Open Web Application Security Project Guide 等に示されるセキュア・コーディング・ガイドラインに従ってコーディングされている。
・リリース前に適切な修正が実装されている。
・コードレビューの結果が，リリース前に責任者によってレビューされ承認されている。

(5) 最近のカスタムコードの変更をサンプリングし，カスタム・アプリケーション・コードがレビューされていることを確認する。

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。

【解説】

「Open Web Application Security Project(OWASP)」は，安全な Web アプリケーションの開発を支援するドキュメントの提供や，Web アプリケーションの安全性の評価基準の整備を行なっている非営利団体である。OWASP では，安全な Web アプリケーション構築のガイドラインを開示しており，その中で Web アプリケーションの基本的な仕組みから，Web 特有の脆弱性と，その脆弱性を防止するコーディング技術に至るまで具体的に述べている。Web アプリケーションを開発する際には，最低限，本ガイドライン記載の脆弱性については対処されていなければならない。安全なコーディングのガイドラインとしては，IPA セキュリティセンターが提供している IPA/ISEC セキュア・プログラミング講座も有効である。OWASP のガイドラインに比べ，より開発者の視点で記述されており，開発言語ごとの脆弱性と安全な実装について，より細かく具体的に説明している。実際に開発を行なう際に良い指針となる。

【評価内容】

(1) すべての Web アプリケーションのソフトウェア開発プロセスを入手しレビューする。このプロセスにおいて，開発者には安全なコーディング技術に関するトレーニングが義務付けられており，OWASP ガイドライン（http://www.owasp.org）などに基づいていることを確認する。
(2) サンプリングした開発者にインタビューを実施して，セキュア・コーディングの知識を有していることについての証跡を入手する。
(3) Web ベースアプリケーションについて，以下の脆弱性が存在しないことをチェックするプロセスが存在することを確認する。
- クロスサイトスクリプティング（XSS）（取り込まれる前のパラメータをすべて評価する）
- SQL インジェクションに代表されるインジェクション攻撃（ユーザがコマンドやクエリーの意味を改変できないことを確認する）
- 悪意あるファイルの実行（アプリケーションがユーザから送信されたファイル名やファイル自体を受付けないことを確認する）
- 安全でないオブジェクトの直接参照（ユーザに対して内部オブジェクトを直接参照させない）
- クロスサイトリクエストフォージェリ（CSRF）（ブラウザが自動的に提示した認定信任（クレデンシャル Credential）やトークンに応答しない）
- 意図しない情報開示と不適切なエラー処理（エラーメッセージやその他の方法による意図しない情報開示を防止する）
- 完全でない認証およびセッション管理（ユーザを適切に認証し，アカウント証明やセッション・トークンを保護する）
- 安全でない暗号保管（暗号に関する欠陥を防御する）
- 安全でない通信（すべての認証および重要情報に関する通信を適切に暗号化する）
- URL アクセス制限の不備（すべての URL におけるプレゼンテーション層のアクセス制御等，一貫した強化対策を実施する）

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。

【解説】

ソースコードレビューは，①各種ガイドラインに従った安全なコーディング作法が適切に実装されている，②対象とするアプリケーションに脆弱性が含まれない，といった項目について，アプリケーションのソースコードを逐次確認することにより，ソースコードの安全性を直接確認する手法である。

Web アプリケーションファイアウォール（頭文字をとって「WAF」と呼ばれる場合がある）は，ネットワークファイアウォールでは防ぎきれないアプリケーション層の攻撃から，Web サイトを守るための製品である。ネットワークファイアウォールの背後に配置され，かつ Web サーバや Web アプリケーションサーバの前に配置される。

【評価内容】

公開された Web アプリケーションについて，次のいずれかの手法がとられていることを確認する。

(1) 以下に示す条件で，公開された Web アプリケーションのレビューを実施している（セキュリティ評価ツールあるいは評価手法を用いた手動または自動のアプリケーション脆弱性検査を採用している）。
- 少なくとも 1 年に 1 回実施している。
- すべての変更の後に実施している。
- アプリケーション・セキュリティを専門とする組織によって実施されている。
- 脆弱性がすべて修正されている。
- 修正後にアプリケーションが再評価されている。

(2) Web ベースの攻撃を検出および予防するために，公開された Web アプリケーションの前に Web アプリケーションファイアウォールが導入されている。

注：「アプリケーション・セキュリティを専門とする組織」は，レビューを実施する者がアプリケーション・セキュリティに精通し，開発チームとの独立性が保たれていれば，第三者組織でも内部組織でも構わない。

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。

【解説】

権限の付与に関する実施手順において，特に管理権限を持つユーザへの権限付与について，審査および承認の手順について明記すべきである。

【評価内容】

システムコンポーネントの監査証跡が有効で，アクティブであることを確認する。

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

【解説】

各システムコンポーネントにおいては，セキュリティ事件・事故の原因究明を可能にするため，次のイベントのログを記録することが求められる。

(a) 学校教育データに対してアクセスした記録
(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操作の記録
(c) ログ等の監査証跡に対してアクセスした記録
(d) 許可されていない操作の実行を試みた記録
(e) システムコンポーネントへのアクセスにおいて利用者の識別と認証機能が正常に機能していることの記録

(f) ログを初期化した記録
(g) 実行ファイルや各種設定等，システムレベルのオブジェクトを作成あるいは削除した記録

【評価内容】

インタビュー，監査ログの調査，監査ログ設定の調査を行い，以下の項目の確認を実施する。

(1) 学校教育データに対する，すべての個人ユーザアクセスが記録されていること。
(2) ルート権限または管理権限を持つ個人が行ったすべての操作が記録されていること。
(3) すべての監査証跡へのアクセスが記録されていること。
(4) 無効な論理的アクセス試行が記録されていること。
(5) 識別および認証メカニズムの使用が記録されていること。
(6) 監査ログの初期化が記録されていること。
(7) システムレベルのオブジェクトの作成と削除が記録されていること。

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

【解説】

各イベントにおいて取得するログは，セキュリティ事件・事故の原因究明を可能にするため，次の項目の情報を含むことが求められる。

(a) イベントを実行した個人を識別する情報
(b) 前述したイベントの種類
(c) イベントが実行された日付と時刻
(d) イベントが実行されたか否かを示す情報
(e) イベントの実行命令が発生したシステムコンポーネントあるいはプロセス等を示す情報
(f) イベントの実行によって影響を受ける対象となるエンティティ（データ，システムコンポーネント，リソース等）を示す情報

【評価内容】

個々の監査可能なイベントについて，以下を確認する

(1) ユーザ ID がログ情報に含まれること。
(2) イベントの種類がログ情報に含まれること。
(3) 日付と時刻がログ情報に含まれること。
(4) 成功または失敗の表示がログ情報に含まれること。
(5) イベントの起点がログ情報に含まれること。
(6) 影響を受けたデータ，システムコンポーネント，リソースの識別子または名称がログ情報に含まれること。

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。

【解説】

一般的に，障害の解析，セキュリティインシデントの分析，ユーザ活動の追跡作業などのログ解析を実施する際は，ログを時系列に並べ調査する手法がとられる。そのため，ログに記録される時刻が正確であることは必須とされている。時刻同期に関しては，一般的に NTP(Network Time Protocol)による仕組みが構築される。NTP は DNS などのネットワークプロトコルと同様，効率性と負荷分散の観点から階層構造をとり，階層化のレベルをストラタム（Stratum）と表現する。組織に正確な時刻源（ストラタム０），もしくはストラタム０を参照する NTP サーバ（ストラタム１）を構築して，そのサーバを中心に管理範囲内の機器に対して，時刻情報を配信する構成である。

【評価内容】

組織内で正しい時刻を入手および配布するためのプロセスおよびシステムコンポーネントのサンプルについて，時刻に関連したシステムパラメータ設定を調査する。以下の項目が実施手順に含まれ，実装されていることを確認する。

(1) 安定しているバージョンの NTP または類似する技術が，時刻同期に使用されていること。
(2) すべての内部サーバが外部ソースからの時刻信号を受信していないこと（2～3 の中央タイムサーバが外部からの時刻信号（特殊ラジオ，GPS 衛星，その他の国際標準時刻や UTC（以前の GMT））からを直接受信して正確な時刻を保持し内部サーバと時刻を共有していること）。
(3) タイムサーバが NTP による時刻同期を行うために，外部ホストコンピュータが指定されていること（悪意ある個人による時刻変更を防止するために）。この時刻更新は，共通鍵方式により暗号化され，NTP サーバからの配信を受ける機器の IP アドレスを特定するアクセス制御リストが作成されていることが望ましい（内部のタイムサーバが承認なく利用されることを防止するため）。

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。

【解説】

ログに基づき警告を発報するシステム（自動監視ツール）の利用で実現することができる。不正アクセスが実施される場合にはアクセス回数が増加することから，生成されたログのファイル容量を毎日比較観察する，拒絶したイベント数をモニタする等も有効である。

【評価内容】

(1) セキュリティ基本方針・対策基準と実施手順を調査し，セキュリティログの最低 1 日 1 回のレビューと，例外発生時のフォローアップが求められていることを確認する。
(2) すべてのシステムコンポーネントに対して，定期的なログのレビューが行われていることを確認する。

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。

【解説】

無線 LAN を使用しているか否かにかかわらず，無許可で設置された不正な無線アクセスポイントが存在していないことを確認するために，定期テストを実施する。

【評価内容】

(1) すべての無線デバイスを識別するために，無線アナライザを使用した調査を最低 3 ヵ月に 1 回実施しているか，または無線 IDS/IPS を導入していることを確認する。
(2) 無線 IDS/IPS を導入している場合には，担当者に発報する設定となっていることを確認する。
(3) 組織のインシデント対応計画において，認証されていない無線デバイスが検出された場合の対応方法について記載されていることを確認する。

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。

【解説】

学校教育データが記録された媒体は，紙媒体を含めて物理的に厳重に保護された保管をおこなう。また，バックアップ媒体は安全なオフサイト施設に保管する事が望ましい。さらに配送についての追跡・管理も求められている。学校教育データの廃棄を確実にするためには，データ消去ツールのような専用の媒体処理装置の導入を検討すべきである。大量の媒体を処理する必要がある場合には，専門業者に委託することも考慮すべきである。このような情報・データの保護・管理に関しては，データの保管と廃棄に関する基本方針・対策基準に基づいて対応すること。

【評価内容】

学校教育データの保護手順が，紙および電子媒体（コンピュータ，リムーバブルメディア，ネットワークおよび通信用ハードウェア，通信回線を含む）の物理的保護に関する管理策を含んでいることを確認する。

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。

【解説】

媒体保管の最も基本的な方法は，施錠可能な金庫やキャビネット，あるいは専用の室を設けてそこに保管する方法である。さらにセキュリティレベルを高めたい場合は，これらの鍵を鍵管理装置にて管理する方法もある。鍵管理装置自体の開閉はテンキーや ID カードで行うことが可能であり，ID カード使用の場合は使用履歴（ログ）が残るため，鍵紛失の際にもログを基に最終使用者を特定できる。入退室管理に連動可能な鍵管理装置もあり，イベントログをサーバで閲覧する事や,ネットワークに接続されている場合は E-mail で管理者のパソコンや携帯電話にログを飛ばす事も可能である。

【評価内容】

(1) ハードコピーや電子媒体の保管および保守の管理に関する基本方針・対策基準を入手し，その基本方針・対策基準によって定期的な媒体の在庫管理が求められていることを確認する。
(2) 媒体の在庫管理記録を調査し，在庫の管理が最低 1 年に 1 回以上定期的に実行されていることを確認する。

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。

【解説】

ルータの構成情報が記録されたファイルは，不正に閲覧あるいは持ち出しされないよう保護する必要がある。また,このファイルに記録された構成情報は,対象となるルータの設定状況と合致したものでなければならない。

【評価内容】

ルータ設定ファイルがセキュアであり，同期していることを確認する。例えば，ランニングコンフィグファイル（実行中の設定ファイル）とスタートアップコンフィグファイル（リブート時に実行される設定ファイル）は，同じ安全な設定である必要がある。

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。

【解説】

コンソール管理アクセスとは，端末を機器に直接接続して操作する業務アクセスのことであり，非コンソール管理アクセスとは，同様の操作をネットワーク経由で行う業務アクセスのことである。すべての非コンソール管理アクセスを暗号化することを求めている。このため，例えば TELNET を使用したアクセスは，暗号化を実施していないためにこの要件を満たすことができない。また，管理対象となる機器が多数となる場合には，専用のコンソールサーバを設置することも考慮すべきである。

【評価内容】

システムコンポーネントのサンプルを選択し，非コンソール管理アクセスが暗号化されていることを，以下の項目に従って確認する。

(1) 各サンプルシステム上の管理者操作ログを見て，管理者パスワードが送信される前に，強力な暗号手段が利用されていること。
(2) システム上のサービスおよび設定ファイルを検証し，TELNET などのリモートログインコマンドが内部で利用不可能になっていること。
(3) Web ベース管理インターフェイスへの管理アクセスが強力な暗号によって暗号化されていること。

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。

【解説】

伝送経路を保護するための各種製品の導入が必要となる。特に，無線ネットワークを通じて学校教育データを伝送する場合には注意が必要である。

【評価内容】

(1) 学校教育データが公衆ネットワークで送受信される場合，すべて暗号化手法（例：SSL/TLS，IPsec）が使用されていることを確認する。
- データの伝送に強力な暗号化が使用されていること。
- SSL の場合：
  - サーバに適用されたパッチが最新版であること。
  - ブラウザのユニバーサルリソースロケータ（URL）に HTTPS と表示されていること。
  - URL に HTTPS と表示されていないときは，学校教育データが要求されないこと。
- 受信時のトランザクションのサンプルを選択し，学校教育データが伝送時に暗号化されていること。
- 信頼された SSL/TLS の暗号鍵／証明書のみを受付けていること。
- 使用中の暗号化手法について，適切な強度が実装されていること（例：ベンダの推奨やベストプラクティスを調べる）。

(2) 学校教育データを伝送する，もしく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ついて，認証と伝送経路の保護のために，例えば，IEEE 802.11i のような業界標準技術を採用していることを確認する。

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。

【解説】

ファイル完全性監視ツールの動作チューニングを行うには，対象システムの把握，理解が必須である。特に導入初期においては，誤検知が多く発生することがあるため，十分な運用期間を定めて検知設定チューニングの期間をおくことが必要である。

【評価内容】

学校教育データ環境において，システム設定と監視対象ファイル，監視活動の記録を調査し，ファイル完全性監視製品が導入されていることを確認する。監視すべきファイルを以下に例示する。

- システム実行ファイル
- アプリケーション実行ファイル
- 設定および設定値ファイル
- 集中保管された履歴ファイル，アーカイブファイル，ログファイル，監査証跡ファイル

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。

【解説】

攻撃者による不正侵入が発生した際，攻撃の証拠隠蔽のためにログは確実に改ざんされるものと考えた方がよい。ログはシステムの運用状況に加え，攻撃の証跡を残す重要な記録でもあるため，様々なセキュリティ基準，ガイドラインでは，ログ自身が重要情報として扱われ，高度なセキュリティ対策の実施が要求されている。ログの保護の基本的なセキュリティ対策は，ログへのアクセス制御の強化である。しかしながら，システムに侵入した攻撃者が管理権限を取得している場合，アクセス制御の強化は意味をなさない。むしろ，リアルタイムでシステム外への保管（バックアップ）する仕組みとシステム上でのログファイルの改ざん検知と管理者への通知の仕組みを構築しておく対策が有効である。

ファイル完全性監視ソフトウェアを利用する場合，ログ自体が常に書き換えられる性質のものであるため設定を正しく行わないと正確な改ざん検知はできない。同ソフトウェアを導入する場合，十分な調整期間をおき，対象範囲の絞込みと同時に対象ファイルに対する動作概要を理解した上での設定を実施することが重要となる。チューニング作業を行わずにシステム導入をしてしまうと誤検出（フォールス・ポジティブ「検出しすぎ」，フォールスネガティブ「検知すべきものを見落とす」）が大量発生し，アラートへの対応ではなく識別に追われる状態となってしまう。

【評価内容】

監査証跡が安全であることを，以下の項目から確認する。

- 業務上必要な担当者のみが監査証跡ファイルにアクセス可能であること。
- 最新の監査証跡ファイルが，アクセス制御，物理的分離，ネットワーク分離などによって，改ざんから保護されていること。
- 最新の監査証跡ファイルが，集中ログサーバまたは改ざんが難しい媒体に直ちにバックアップされること。
- 外部に晒された機能（例えば，無線，ファイアウォール，DNS，メール）が出力するログが，安全な内部の集中サーバまたは媒体に直接出力されるか，またはコピーされていること。
- システム設定や監視ファイルおよび監視活動を調査し，ログに対して，ファイル完全性監視もしくは変更検知ソフトウェアが使用されていること。

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）。

【解説】

システムコンポーネントのログファイルは，1 年間以上保持する。また，3 カ月間は，インシデントが発生した際の調査に即時に利用できるような状態を維持しておく。なお，ログの保管期間は，法令やガイドラインに準拠していなければならない。

【評価内容】

(1) セキュリティ基本方針・対策基準および実施手順を調査し，監査ログの保管ポリシーが含まれており，最低 1 年間の保管が求められていることを確認する。
(2) 監査ログは，最低 1 年間利用可能であり，最低 3 ヶ月間は分析の必要性が生じた際に速やかにリストアすることが可能であることを確認する。

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。

【解説】

一般的に侵入検知（防止）システムには，システムごとに専用の管理ツールが存在する。システムの監視は原則的に専用の管理ツールを使って行うことになる。管理ツールはシステムの監視の用途のほか，システムの設定や監視装置に適用するポリシー管理やシグネチャ管理の機能も提供する。ポリシー・シグネチャ管理を行うために，専用の管理ツールは必須である。しかしながら全体としての監視環境を考慮すれば，侵入検知システムのほかにログ監視システムなども存在することになり，結果として複数の監視用システムに対しての監視が必要となるため効率的ではない。統合ログ管理ツールの中には，侵入検知システムのセキュリティ警告情報も扱えるツールもあるので，統合管理ツールを利用することで運用コストの低減を図ることができる可能性がある。

【評価内容】

(1) ネットワーク侵入検知システム（IDS）あるいは侵入阻止システム（IPS）が導入されており，これによって学校教育データ環境内におけるネットワークトラフィックがすべて監視されていることを確認する。
(2) IDS および／または IPS について，危殆化の可能性がある場合は担当者に警告するようになっていることを確認する。
(3) IDS/IPS の設定を調査し，IDS/IPS がベンダの指示に従って設定，保守，更新され，最適に保護されていることを確認する。

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. 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。

【解説】

ユーザを認証する際に用いるパスワードは，システムに保管する場合にはすべて暗号化しなければならない。

【評価内容】

システムコンポーネントのサンプルについてパスワードファイルを調査し，パスワードが伝送時および保管時において判読不可能であることを確認する。

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。

【解説】

すべてのシステムコンポーネント上において,適切なユーザ認証とパスワード管理を徹底しなければならない。特にパスワードの管理方法については，具体的な項目が詳細に規定されている。このため，大規模なシステムの場合には,ID 管理のための製品を導入することも考慮すべきである。 ここで述べているパスワード使用手順は，すべての教職員を対象としている。教職員を監督する責任者は，ここに記載されたパスワード使用手順をすべての教職員に遵守させなければならない。尚，システム担当者のパスワードには更なる堅牢さが求められることから，システム担当者向けのパスワード使用手順は，別途策定することも検討すべきである。

【評価内容】

(1) 管理者および一般ユーザのユーザ ID のサンプルを選択する。それぞれのユーザが，セキュリティ基本方針・対策基準に従って認証されることを確認するため，次の項目を確認する。

・管理者 ID の認証フォームを入手し，認証フォーム（例：指定された特権を持っている，すべての署名が

記入されている等）に従って認証が実施されていることを確認する。
・選択したユーザ ID を，認証フォームからシステムまで追跡し，認証フォームに従って認証が実施されていることを確認する。

(2) パスワード使用手順を調査およびセキュリティ担当者を観察し，電話，電子メール，ウェブ，またはその他の非対面方法でパスワードのリセット要求があった際は，パスワードリセット前にユーザが正しく識別されていることを確認する。

(3) パスワード使用手順を調査およびセキュリティ担当者を観察し，新規ユーザに対する初回パスワードがそれぞれのユーザに対して異なる値に設定され，初回使用後，直ちに変更されていることを確認する。

(4) 過去 6 ケ月以内に離職した教職員のサンプルを選択し，現在のユーザアクセスリストをレビューして，ID が無効もしくは削除されていることを確認する。

(5) 90 日を越える期間で休眠状態のアカウントは，消去するか無効化していることを確認する。

(6) ベンダがシステムコンポーネントの保守に使用するアカウントが非アクティブで，ベンダが必要とするときだけ有効にされ，使用中は監視されることを確認する。

(7) サンプル ID のユーザにインタビューを行い，ユーザがパスワード使用手順および基本方針・対策基準を理解していることを確認する。

(8) システムコンポーネントのサンプルについて，ユーザ ID リストを調査し，以下の項目を確認する。
・デフォルトのユーザ ID およびアカウントは，無効化もしくは削除されていること。
・システム管理や他の重要な機能に使用される共有 ID が存在しないこと。
・すべてのシステムコンポーネントの管理に共有 ID やデフォルト ID が使用されていないこと。

(9) パスワードの使用に関する基本方針・対策基準および実施手順を調査し，グループパスワードや共有パスワードが明示的に禁止されていることを確認する。

(10) システム管理者にインタビューを行い，たとえ求められてもグループパスワードや共有パスワードが付与されないことを確認する。

(11) １要素認証が使用されている場合は，システムコンポーネントのサンプルについてシステム設定を調査し，パスワードのパラメータ設定で少なくとも 90 日毎のパスワード変更が必要となっていることを確認する。

(12) システムコンポーネントのサンプルについてシステム設定を調査し，パスワードのパラメータ設定で最小 7 文字以上のパスワード長が必要となっていることを確認する。

(13) システムコンポーネントのサンプルについてシステム設定を調査し，パスワードのパラメータが数字と英字の両方を含んだパスワードを求めるよう設定されていることを確認する。

(14) １要素認証が使用されている場合は，システムコンポーネントのサンプルについてシステム設定を調査し，パスワードのパラメータが新しいパスワードが直近 4 回使用されたものと同じであってはならないことを求めるよう設定されていることを確認する。

(15) システムコンポーネントのサンプルについてシステム設定を調査し，システム／セッションが未稼働である場合にタイムアウトするまでの時間が 15 分以下に設定されていることを確認する。

(16) データベースとアプリケーションの設定を調査し，ユーザ認証とデータベースアクセスについて以下が含まれていることを確認する。
・すべてのユーザアクセスが認証されたものであること。
・データベースに対するすべてのユーザアクセス，ユーザからの要求，ユーザの実行処理（例えば，移動，コピー，削除）がプログラムを介したものに限定されている（例えば，ストアードプロシージャを介している）こと。
・データベースに対する直接のアクセスあるいは要求は，データベース管理者のみに限定すること。

(17) アプリケーションの ID はそのアプリケーションの利用のみに限定されていることを確認するために，データベース・アプリケーションと関連するアプリケーションの ID を調査する。

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。

【解説】

情報システムは，正当な権限を持たない利用者によって不正に利用されることがないように確実な管理を実施する必要がある。

ユーザ ID 認証の試行は連続で最大 6 回までとし,それ以上は試行拒否する設定により不正なアクセスを排除する。

【評価内容】

システムコンポーネントのサンプルについて，最大 6 回の試行後にユーザ ID をロックアウトする設定となっていることを確認する（１要素認証の場合)。

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。

【解説】

情報システムは，正当な権限を持たない利用者によって不正に利用されることがないように確実な管理を実施する必要がある。

ロックアウトされたユーザ ID を再び有効にするまでのロックアウト時間は最短で 30 分とするか，または管理者が有効にするまでとする。

【評価内容】

システムコンポーネントのサンプルについて，ロックアウトの時間が 30 分以上の設定となっている，または管理者がユーザ ID を有効にするまでとなっていることを確認する。

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

【解説】

必要のないアカウントが放置されることは大きなリスクとなる。このため，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ために，権限の抹消手順についても権限の付与に関する実施手順に明記し徹底することが求められる。

【評価内容】

データ管理に関する基本方針・対策基準を入手し，次の項目が含まれていることを確認する。

(1) 特権ユーザ ID に関するアクセス権限は，職務の実行に必要な最小限の特権に制限されること。
(2) 特権の付与は，個々の担当者の業務区分と職務分掌に基づいて実施されること（「役割に基づくアクセス制御」，あるいは「RBAC」と呼ばれる）。
(3) すべての特権アクセスの権限付与が，責任者により署名された任命書により行われること。
(4) 自動化されたアクセス管理システムが実装されること。

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

【解説】

誤った権限の付与は大きなリスクとなる。このため，権限の付与に関する実施手順に明記し適切な権限付与の実施を徹底する。

【評価内容】

システム設定とマニュアルを調べて，アクセス制御が実施され，かつ次の項目が含まれていることを確認する。

(1) すべてのシステムコンポーネントにおいて，アクセス制御システムが機能していること。
(2) アクセス制御システムが，職種と職能に基づく個人への特権の付与を制限するように設定されていること。
(3) アクセス制御システムが，デフォルトで「すべてを拒否」の設定となっていること。
注：一部のアクセス制御システムは，デフォルトで「すべてを許可」に設定されており，個別に拒否するためのルールを記述しないかぎり，または記述するまでは，アクセスが許可されてしまう。

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。

【解説】

ネットワークへのリモートアクセスについては，２要素認証が要求されている。２要素認証の例としては，利用者が認識しているパスワードと，利用者が所持しているトークンデバイスあるいは電子証明書を組み合わせて用いる場合がある。

【評価内容】

すべてのリモートアクセスについて２要素認証が使用されていることを確認するため，担当者（例：アドミニストレータ）がネットワークにリモートから接続する様子を観察し，パスワードおよび別の認証手段（スマートカード，トークン PIN など）の両方が要求されていることを確認する。

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

【解説】

ファイアウォール設定基準は，最新のネットワーク図，業務に必要なサービス／ポートのリストおよびルータの設定基準を含まなければならない。

【評価内容】

(1) ファイアウォールおよびルータ設定基準を入手および検査し，ルールセットが少なくとも 6 ヵ月ごとに見直されていることを確認する。

(2) すべてのネットワーク接続とファイアウォールまたはルータの設定変更に関するテストおよび承認の実施手順が存在することを確認する。

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。

【解説】

インターネットを代表とする信頼できないネットワークと学校教育データ環境のシステムコンポーネントを接続する場合には，ファイアウォールを設置してトラフィックを制限する。信頼できないネットワークには無線ネットワークも含まれる。

ファイアウォールの構成情報が記録されたファイルは，不正に閲覧あるいは持ち出しされないよう保護する必要がある。また，このファイルに記録された構成情報は，対象となるルータの設定状況と合致したものでなければならない。

【評価内容】

信頼できないネットワークと，学校教育データ環境にあるシステムコンポーネントとの間の接続を制限するため，ファイアウォールおよびルータの設定について，次の項目を確認する。

(1) インバウンドおよびアウトバウンドトラフィックが，学校教育データ環境にとって必要なものに限られており，なおかつ文書化されていること。
(2) 例えば，明確に「すべてを拒否」するか，あるいは許可するものを明示することによって，他のすべてのインバウンドおよびアウトバウンドトラフィックを限定して拒否する設定になっていること。

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。

【解説】

ファイアウォールの構築に際しては，ネットワークの適切なセグメンテーションの実施に基づき，DMZ とサーバの配置を決定する必要がある。組織には，一般に，Web，メール，DNS など外部に公開するサービスがある。外部に公開するサービスを内部ネットワークに設置すると，万が一そのサービスが不正侵入されて乗っ取られた場合にそこを踏み台にして内部ネットワークのホストコンピュータに侵入されてしまうことになる。このような侵入を防止するために外部と内部の中間的なセキュリティ領域を設ける。その領域を DMZ(DeMilitarized Zone，非武装地帯)と呼ぶ。外部に公開するサーバは DMZ に設置し，仮にそのサーバが不正侵入されて乗っ取られても，DMZ と内部の間のファイアウォールが内部ネットワークへの被害の拡大を防止する。

インターネットと内部ネットワークの間について直接の通信を禁止するために DMZ の導入が求められている。学校教育データを保管するシステムコンポーネントが設置されるネットワーク領域は，外部ネットワークからのアクセスが禁じなければならない。DMZ を導入することで外部ネットワークから接続を許さない領域を「内部ネットワーク」として，外部ネットワークから接続を許す領域を「DMZ」として定義することができる。「内部ネットワーク」に対して直接自由にアクセスできないネットワーク領域は，校内システムといえども「外部ネットワーク」として分類される。更に，内部ネットワークからの DMZ 宛ての通信についても制限を設けるよう定めている。

【評価内容】

インターネットとシステムコンポーネントの間の直接アクセスが存在しないことを明らかにするために，以下に示すファイアウォールおよびルータの設定を検査する。システムコンポーネントには，インターネット上のチョーク・ルータ，DMZ のルータとファイアウォール，DMZ における学校教育データセグメント，エッジ・ルータ，内部の学校教育データネットワークセグメントが含まれる。

(1) DMZ の実装において，インバウンドとアウトバウンドトラフィックが，学校教育データ環境において必要なプロトコルのみに制限されていることを確認する。
(2) インターネットからの受信トラフィックの宛先が，DMZ 内の IP アドレス宛てに制限されていることを確認する。
(3) インターネットと学校教育データ環境との間で，インバウンドおよびアウトバウンドトラフィック経路が存在しないことを確認する。
(4) 内部アドレスがインターネットから DMZ 内へ通過できないことを確認する。
(5) 学校教育データ環境からインターネットへのアウトバウンドトラフィックが DMZ 内の IP アドレスに制限されていることを確認する。
(6) ファイアウォールにおいて，ステートフルインスペクション(動的パケットフィルタリング)が有効になっている事を確認する(確立した接続のみ許可され，以前に確立した接続が存在する場合のみ通信が許可されること。すべての TCP ポートに対して ”syn reset ” か ”syn ack ” をセットしたパケットをポートスキャナで送りレスポンスがあった場合は，以前に確立した接続がないにもかかわらずそのパケットは許可されていることになる)。
(7) DMZ から分離された内部ネットワーク領域にデータベースが配置されていることを確認する。
(8) 上記のファイアウォールおよびルータのサンプルを選択し，NAT もしくはその他の RFC 1918 アドレス空間を実装するための技術を利用して，内部ネットワークからインターネットへの IP アドレスのブロードキャストが制限されていることを確認する（IP マスカレード)。

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。

【解説】

システムコンポーネントにおいて利用者個人を識別することが可能となるように，すべてのユーザには個別の ID を割り当てなければならない。共有 ID を使用して個別のユーザ名（ID）を与えないと，ファイルごとのアクセス履歴を調査するときに，個人の特定が不可能になる。リモート・サイトからのメンテナンスのために業者に渡すメンテナンス用の ID や，OS 既定の管理者アカウントなどについても考慮する必要がある。
IC カード等のアクセス認証用デバイスの共用も許されない。

【評価内容】

システムコンポーネントもしくは学校教育データへアクセスするすべてのユーザに対して，一意のユーザ ID が付与されていることを確認する。

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）

【解説】

２要素認証とは，パスワードまたはパスフレーズの認証に加えてもう一種類の方式を追加することで認証を強化することを意図している。追加の方式には，トークンデバイス，スマートカード，生体認証，公開鍵方式などが含まれる。

【評価内容】

すべてのユーザを認証する際に一意な ID を割り当てることに加えて，追加の認証（例：パスワード）を実施していることを確認するため，以下の項目を確認する。

・システムコンポーネントごとに使用されている認証方法を記述した文書が存在すること。
・各認証方法について，それぞれのシステムコンポーネントについて認証を観察し，上記の文書に記述された認証方法に従って認証が実行されていること。

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。

【解説】

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し有効に稼働させることにより，コンピュータ端末を不正侵入等の脅威から防御する。

【評価内容】

(1) インターネットに直接接続するモバイル端末や，教職員使用のコンピュータで校内ネットワークへのアクセスに使用されるもの（例：教職員が使用するノートパソコン）にパーソナルファイアウォールソフトウェアが導入されており，正常に動作していることを確認する。
(2) パーソナルファイアウォールソフトウェアが組織の基準に基づき設定されており，モバイル端末の利用者によって変更されていないことを確認する。

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。

【解説】

一般に，ベンダは，ユーザが製品を購入後に最新機能などの様々な機能を早く簡単に使用できるようにするた

め，デフォルト設定(初期状態)で多くの機能を予め使用可能な状態にしている。その結果として，デフォルト設定ではセキュリティレベルが低くなっていることがある。また，デフォルト設定情報やアカウント情報は，ベンダ提供のマニュアルやインターネットなどにより取得が容易である。このため，セキュリティを確保するためには，前節のファイアウォールなどのネットワーク構築，運用上のセキュリティ対策に加えて，機器自体についてもセキュリティ対策を行わなければならない。

【評価内容】

無線ネットワーク環境のベンダのデフォルト設定について，次の項目を確認する。また，すべての無線ネットワークにおいて，強力な暗号技術（例えば，AES）が実装されていることを確認する。

- 暗号鍵がインストール時のデフォルト値から変更されている。また，暗号鍵に関する情報を持つ人物が退職または異動する際には，その都度暗号鍵が変更される。
- 無線デバイスの SNMP コミュニティ文字列が，デフォルト値から変更されている。
- アクセスポイントのパスワード／パスフレーズがデフォルト値から変更されている。
- 無線ネットワークにおける認証および伝送において強力な暗号を維持（例えば，WPA/WPA2）するために，無線デバイスのファームウェアが更新されている。
- その他，セキュリティに関連する無線ベンダによるデフォルト値から変更されている。

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。

【解説】

ウィルスに代表される多くの悪意のあるソフトウェア（例えば，トロイの木馬，ワーム，スパイウェア，アドウェア，ルートキット等）は，教職員の電子メール操作やインターネット上の Web サイト閲覧によって校内システムに侵入する場合が多い。校内システムを悪意のあるソフトウェアから保護するためには，教職員の使用するパソコンおよびサーバには，悪意のある様々な形態のソフトウェアを検知・除去・防護できるアンチウィルスソフトウェアを導入し,つねに最新の状態に更新しておく必要がある。ウィルス対策でもっとも基本となる対策は，使用するコンピュータ上でウィルス対策を行うことである。ウィルスが活動するコンピュータ上でウィルスの検出・駆除・削除を行うことにより，ウィルス被害の発信源となる原因を絶やすという考え方である。また，システム内で使用している共有ファイルサーバ，グループウェアサーバなどはウィルスに感染するとその利用者に対して被害が拡散してしまう可能性があるため，ウィルス対策が必要になる。

【評価内容】

(1) 悪意あるソフトウェアによって影響を受けるすべての種類のオペレーティングシステムについて，システムコンポーネントのサンプルを調査し，アンチウィルスソフトウェアが導入されていることを確認する。
(2) アンチウィルスソフトウェアは，すべての既知の悪意あるソフトウェアに対して，検知，駆除を行い，システムコンポーネントを保護していることを確認する。

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。

【解説】

アンチウィルスソフトウェアが最新のバージョンであるとともに,最新のパターンファイルが適用されており，

ウィルスの検知，隔離および駆除が適切に実施されるようにする。また，ソフトウェアが有効に実行されていることを確認するために，監査ログが作成できることが求められる。

【評価内容】

すべてのアンチウィルスメカニズムが最新で，正常に稼動しており，監査ログが生成できることを確認するため，以下の項目を確認する。

(1) 基本方針・対策基準にアンチウィルスソフトウェアおよびパターンファイルの更新が要求されていること。
(2) ソフトウェアのインストールによって，自動更新と定期スキャンの設定が有効になっていること。
(3) 悪意あるソフトウェアによって影響を受けるすべての種類のオペレーティングシステムについて，システムコンポーネントのサンプルを調査し，自動更新と定期スキャンが実施されていること。
(4) システムコンポーネントをサンプリングし，アンチウィルスソフトウェアのログの生成が有効になっており，ログが過去 1 年間分保持されていること。

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。

【解説】

組織のすべての領域における情報セキュリティ活動には様々な法令が適用される。特に学校教育にかかわる活動においては，知的財産を保護するための法令の遵守は重要となる。

(1) 違法なソフトウェアの利用を防止するためには，定評のある供給元からソフトウェアを取得することが望ましい。
(2) ソフトウェアのライセンス契約に違反することは重大な法令違反である。
(3) 著作権を侵害するような行為は重大な法令違反である。

【評価内容】

職務規定等を入手し，知的財産を保護するための上記の指針について考慮した記述が記載されていることを確認する。また，教育実施の記録，業務従事者への周知事項の記録を入手し，これらの事項が業務従事者に周知されていることを確認する。

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。

【解説】

組織のすべての領域における情報セキュリティ活動には様々な法令が適用される。特に学校教育にかかわる活動においては，個人情報を保護するための法令の遵守は重要となる。

【評価内容】

個人情報の保護に関する方針が記載された文書（個人情報保護規程など）を入手し，個人情報を保護するための方針が確立していることを確認する。また，教育実施の記録，業務従事者への周知事項の記録を入手し，これらの方針が業務従事者に周知されていることを確認する。

（システムの開発，構築，運用者編　以上）

用語集　「学校の管理者編」および「教職員編」

	用語	解説	出現ページ
あ	アカウント管理	ユーザ ID の管理	15,43,44
	悪意のあるソフトウェア/マルウェア	コンピュータに侵入し，害を与えるように設計されたソフトウェア。例として，ウィルス，ワーム，トロイ（またはトロイの木馬），スパイウェア，アドウェア，ルートキットなどがある	30,67
	アクセス管理	コンピュータの利用，ハードディスクなどに保管された電子情報，あるいは接続された周辺機器などの利用を管理すること	11,36,37,62
	アクセス権	コンピュータの利用者に与えられた権限，ハードディスクなどに保管された電子情報，あるいは接続された周辺機器などを利用する権限	11,12,36,46,61
	アクセス制御	情報を保管する機器または情報処理を行う機器の使用やアプリケーションの使用を承認された利用者のみに制限する仕組み	15,28,29,43,44,48,49,50,53,57,59,61,62,66
	アップグレード	ソフトウェアを最新版に更新すること	14,42
	アドウェア	ユーザの画面に強制的に広告を表示させるプログラム	30,67
	アプリケーション	OS との対比で使われるソフトウェアの類別の一つで，市販のソフトウェアおよび独自に開発したソフトウェア	4,9,14,15,34,42,43,45,46,47,48,49,50,51,56,60
	アプリケーションシステム	アプリケーションを構成するシステム	9,34,47
	アプリケーション層	データ通信の仕組みを説明するモデルの内で，ネットワーク経由での送受信を行なうプログラムとユーザとの入出力を行なうプログラムの間の通信部分のこと	14,15,42,43,50
	暗号化	特定の文字列データ（暗号鍵）を用いて，情報を変換すること	23,24,25,34,35,46,48,50,53,55,56,59,66

	暗号技術／暗号化技術	暗号化を行うために必要となる技術。例えばハッシュ関数や非対称鍵暗号などがある	29,45,66,67
	アンチウィルスプログラム/ソフトウェア	ウィルスをはじめとするさまざまな形式の悪意のあるソフトウェア（「マルウェア」とも呼ばれる）を検出，除去し，これらのソフトウェアからコンピュータを保護するプログラム（ソフトウェア）	30,67,68
	アンチウィルスメカニズム	アンチウィルスプログラム／ソフトウェアを含むコンピュータウィルス対策機能。コンピュータウィルスを検出・除去するための一連の仕組み	30,67,68
	インシデント	事件や事故	7,8,15,16,43,53,54,58
	インフラストラクチャ	システムを有効に機能させるために基盤として必要となる設備	14,42,47
	ウィルス	電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラム	29,30,46,66,67,68
	ウィルス定義ファイル	ウィルスの特徴が記録されているデータベースファイル。ウィルス対策ソフトがウィルスを発見するために使われる	30
	オペレーティングシステム/OS	すべての動作の管理と調整およびコンピュータリソースの共有を行うコンピュータシステムのソフトウェア。オペレーティングシステムの例として，Microsoft Windows，Mac OS，Linux および Unix などがある	14,15,24,29,30,34,42,43,45,65,67,68

	用語	解説	出現ページ
か	カスタムアプリケーション	市販されているアプリケーションではなく,利用者の要求に基づいて独自に開発されたアプリケーションのこと	4,48,49
	監査ログ	「監査証跡」とも呼ばれる。システムの動作状況アクティビティの時系列の記録。データが正しく処理されたことの調査を可能にする十分な証跡（証拠）を提供する	30,34,51,52,58,67,68
	監視	停電，警報，または他の事前定義イベントが発生した場合に，担当者に警告するために,継続的にコンピュータまたはネットワークリソースを監督するシステムまたはプロセス	7,15,16,17,18,26,37,39,41,43,44,53,56,57,58,60
	キー/暗号鍵	暗号化技術では，キーは，プレーンテキスト（暗号化されていないテキスト）を暗号化テキストに変換する際に暗号化アルゴリズムの出力を決定する値。一般に，キーの長さによって，任意のメッセージでテキストを復号化する難しさが決まる	12,34,35,36,45,56,66,67
	脅威	情報または情報処理リソースが意図的または偶発的に失われたり，変更されたり，公開されたり，アクセス不能になったり，または影響を受けたりして，組織の損失を招く原因となる状態または行為	6,29,30,48,50,66

	強力な暗号／強力な暗号技術	業界で認められたテスト済のアルゴリズムに，十分なキーの長さと適切なキー管理の実践が伴った暗号化技術。暗号化技術とは，データを保護する技法で，暗号化（復号可能）とハッシング（復号不能な「一方向」）の両方が含まれる。業界で認められたテスト済のハッシングアルゴリズムの例として，SHA-1 が挙げられます。業界で認められたテスト済の暗号化の標準およびアルゴリズムの例として，AES（128 ビット以上），TDES（最小倍長キー），RSA（1024 ビット以上），ECC（160 ビット以上）および ElGamal（1024 ビット以上）が挙げられる。詳細については，NIST Special Publication 800-57（http://csrc.nist.gov/publications/）を参照	25,34,35,36,45,46,55,56,59,66,67
	共有 ID	コンピュータの複数の利用者間で共有して利用しているユーザ ID	28,60,65
	共有パスワード	コンピュータの複数の利用者間で共有して利用しているパスワード	28,60
	グループパスワード	グループにおいて共用利用しているパスワード	28,60
	クロスカット裁断	一定間隔ごとに縦横に裁断する機能を使った処理	26,27,39
	攻撃	他のコンピュータに不正アクセスを行い，ダメージを与えようとする行動	12,14,30,41,42,43,47,48,50,51,57
	コンテナ	収納箱	27,39

	用語	解説	出現ページ
さ	サーバ	他のコンピュータに通信処理，ファイル記憶域，印刷機器へのアクセスなどのサービスを提供するコンピュータ。サーバには，Web，データベース，アプリケーション，認証，DNS，メール，プロキシ，NTP などがある	4,13,14,30,37,41,42,45,46,47,50,53,54,55,56,57,64,67
	サービスプロバイダ	学校教育データの処理，保管，伝送に直接関わる事業体。これには，学校教育データのセキュリティを制御する，または学校教育データのセキュリティに影響を与えうるサービスを提供する会社も含まれる。例として，マネージドファイアウォール，IDS およびその他のサービスを提供するマネージドサービスプロバイダや，ホスティングプロバイダなどの事業体が挙げられる	16,17,44
	サブネットワーク	部門ネットワーク。全体のネットワークと区別するために用いる	14,42

	サンプリング	抽出すること	23,24,30,34,40,49,50,68
	システムコンポーネント	学校教育データ環境に組み込まれている，またはこれに接続するすべてのネットワークコンポーネント，サーバ，またはアプリケーションを指す	4,7,8,13,14,28,30,41,42,45,46,47,51,52,53,55,58,59,60,61,62,63,64,65,66,67,68
	システム設定	システムを稼働させるために決められた値など	9,28,35,46,47,56,57,60,62
	システム・ソフトウェア	システムを構成するソフトウェア	13
	消磁	磁気を消去すること	27,39
	使用ポリシー	使用するための基本的な考え方や方針	29
	商用ツール	市販されているプログラム	14,43
	情報処理設備	情報を処理するための装置およびこれらの装置を維持・管理するための施設や設備	18,57
	侵害	「データ侵害」または「データ違反」とも呼ばれる。コンピュータシステムへの侵入があり，学校教育データの不正な開示/盗難，変更，または破壊が疑われること	7,8,19,31,36,58,69
	スイッチ	通信パケットの交換(スイッチング)機能を持った通信装置	4
	スパイウェア	悪意のあるソフトウェアの一種で，コンピュータ内部からインターネットに対して，ハードディスクに記録されている情報などを不正に送り出すソフトウェア	30,67
	脆弱性	悪意のあるユーザに利用されて，システムへの侵入およびシステムの完全性の侵害を許してしまう，システム上の弱点	6,9,14,15,42,43,46,47,48,49,50,51
	脆弱性検査	システムに存在している脆弱性を検出すること	14,42,51
	セキュリティ事故／セキュリティインシデント	情報管理やシステム運用に関する，保安上の脅威となる現象や事案	15,43,44,53

	セキュリティ警告	情報セキュリティが脅かされる虞がる事を告げ知らせること	15,16,43,44,58
	セキュリティサービスプロバイダ	情報セキュリティに関するサービスを提供する事業者	16
	セキュリティ侵害	情報セキュリティが脅かされること	7,8,36
	セキュリティ脆弱性	情報セキュリティにおける脅威となる行為に利用できる可能性のある，システム上の欠陥や仕様上の問題点	9,46,50
	セキュリティ責任者	組織のセキュリティ関連業務の最高責任者	15,43,44
	セキュリティ設定	情報セキュリティにかかわる設定	15,44,46,66
	セキュリティパッチ	プログラムに脆弱性やセキュリティホールなどが発見された際に，それらの問題を修正するためのプログラム	9,13,14,42,46,47,48
	セキュリティポリシー	学校の基本方針，対策基準，学校に特化した形での実施手順書を記載した文書の総称	6,7,15,23,43
	センシティブデータ	学校教育データの内，身体の特徴や傷病履歴等の機微情報，あるいは進路情報や成績等の要保護情報を含むデータ	3

	用語	解説	出現ページ
た	担保	「保証する」という意味	27,39
	ディスク暗号化	ファイル単位ではなく磁気ディスク全体を暗号化すること	24,34
	データベース	容易に抽出できるように，情報を整理および管理するための構造化された形式。簡易なデータベースの例として，テーブルやスプレッドシートが挙げられる	4,23,34,47,60,64,65
	手順／手順書	ポリシーを説明したもので，ポリシーの実行方法および実装方法を示す	6,7,8,10,11,12,13,14,15,16,17,18,22,28,34,35,36,37,38,41,42,43,44,51,53,54,57,58,59,60,61,63

	デフォルトアカウント	システムを最初に使用する際，初期アクセスを可能にするために，システム，アプリケーション，またはデバイスで事前に定義されているログインアカウント	28,45
	テーブル	リレーショナルデータベースにおけるデータ保管の単位	23,34
	トークン	動的な認証または２要素認証を実行するハードウェアまたはソフトウェア	12,38,50,62,66
	ドメインネームシステム/DNS	インターネットなどネットワーク上の分散データベースに，ドメイン名に関連する情報を格納するシステム	4,46,47,53,57,64
	トロイ/トロイの木馬	正体を偽ってコンピュータへ侵入し，データ消去やファイルの外部送信，他のコンピュータへの攻撃などを行なうプログラム	30,67

	用語	解説	出現ページ
な	認証	個人，デバイス，またはプロセスが本人（またはその物）であることを検証するプロセス	4,12,13,24,35,37,44,46,48,50,51,52,54,56,59,60,61,62,65,66,67
	ネットワーク	リソース（CPU，メモリ，ハードディスク等）を共有するために，複数台のコンピュータを互いに接続した状態のことを指す	3,4,12,13,14,15,17,29,37,41,42,43,45,46,47,48,50,53,54,55,56,57,58,62,63,64,65,66,67
	ネットワークコンポーネント	ネットワークを構成するすべての機器のこと。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，その他のセキュリティ機器などが含まれる	4,63
	ネットワークサービス保護	ネットワークに関係するサービスを適切に維持すること	17
	ネットワーク層	データ通信の仕組みを説明する階層モデルの内で，ネットワーク同士の通信をおこなうための方式を定めた部分のこと	14,15,42,43

	ネットワークタイムプロトコル/NTP	コンピュータシステムの時計を,ネットワーク経由で同期するためのプロトコル	4,53

	用語	解説	出現ページ
は	媒体	USB メモリや磁気テープなど，情報の記録をおこなうためのもので，紙も含まれる	22,23,24,26,27,34,39,40,45,54,55,57
	バグ	コンピュータプログラムに含まれる誤りや不具合のこと	13
	パスワード/パスフレーズ	コンピュータの利用者を認証するための文字列	12,23,24,28,29,45,46,48,49,55,59,60,62,66,67
	パーソナルファイアウォールソフトウェア	主に個人利用のパーソナルコンピュータにインストールすることによって,外部からの侵入を検知あるいは遮断するためのソフトウェア	29,66
	バックアップ	コンピュータに保管されたデータやプログラムを,破損などの事態に備えて別の記憶媒体に保管すること	7,8,16,23,29,34,45,54,57,58,66
	パッチ	機能を追加したり，不具合を修正したりする，既存のソフトウェアのアップデートプログラム	9,13,14,30,42,46,47,48,56
	ハードコピー	複写した印刷物	26,27,39,55
	パラメータ設定	設定値を入力すること	28,47,53,60
	ファイアウォール	組織内のコンピュータネットワークに対して,外部から侵入されるのを防ぐための仕組みを備えたコンピュータまたはソフトウェア	4,29,42,45,50,51,57,63,64,65,66,67
	ファイル完全性監視	コンピュータ上の特定のファイルを監視して,内容が変更された場合にそれを検出すること。重要なファイルが変更された場合には該当するセキュリティ担当者に警告を送信される	7,56,57
	不正アクセス	あるコンピュータへの正規のアクセス権を持たない人が,ソフトウェアの不具合などを悪用してアクセス権を取得し,不正にコンピュータを利用する，あるいは試みること	12,41,53
	不正侵入	悪意のある第三者が,学校や個人のコンピュータに不正にアクセスし，そのコンピュータを操作すること	29,57,64,66

	フリーのツール	無償で提供されているプログラム	14,43
	プロキシサーバ	内部ネットワークとインターネットの境にあって,「代理」としてインターネットとの接続を行なうコンピュータ	4
	プロセス	手順あるいは過程	6,7,9,10,14,22,34,35,38,42,48,49,50,51,52,53,63
	プロトコル	ネットワーク内で使用される,合意された通信方式。ネットワーク上で処理を実行する際にコンピュータ製品が従うべき,ルールや手順を説明した仕様	4,46,47,53,56,63,65
	ペネトレーションテスト	コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで,システムを実際に攻撃して侵入を試みる手法	14,15,42,43
	ベンダ	製品を販売する会社。製品のメーカーや販売代理店のこと。ある特定の企業の製品だけでシステムを構築することを「シングルベンダ」,複数の企業の製品を組み合わせてシステムを構築することを「マルチベンダ」という	9,30,34,45,46,47,56,58,59,60,66,67
	ボット	「ロボット」の略称で,インターネット経由の命令によって遠隔操作を行うコンピュータプログラム群	30
	ポリシー	許容できるコンピューティングリソースの使用およびセキュリティの実践を管理し,操作手順の開発を指導する,組織全体にわたるルール	6,7,10,15,22,23,29,43,58,59

	用語	解説	出現ページ
ま	無線アクセスポイント／ワイヤレスアクセスポイント	無線通信機器を無線ネットワークに接続できるようにする装置。ワイヤレスアクセスポイント自体は有線ネットワークに接続されており,ネットワーク上において無線通信機器と有線通信機器のデータを中継する	4,37,45,54
	メッセージングツール	キー入力による短いメッセージを交互にやり取りすることにより,コミュニケーションを図る仕組み	25
	メーリングリスト	複数の人に同じメールを配送できる仕組み	9
	モバイルコンピュータ／モバイル端末	持ち運ぶことを前提としたノートパソコンなど	29,37,66

	用語	解説	出現ページ
や	ユーザ ID リスト	利用者 ID（ユーザ名）の一覧表	28,60
	ユーザアカウント	コンピュータの利用者(ユーザ)を識別するための標識となる文字列。ネットワーク上の「身分」や「戸籍」に当たる。一般にはユーザアカウントは「ユーザ名」と「パスワード」を核として，このほかに環境設定や利用権限などの情報も含んでいる	12,15,16,41,43,44,59
	ユーザパスワード	利用者（ユーザアカウント）のパスワード	28,59

	用語	解説	出現ページ
ら	リスク	危険性。情報セキュリティにおけるリスクとは，情報システムと，そこで扱われるデータの保全を脅かす危険のこと。コンピュータウィルス，不正アクセスなどの外的脅威はもとより，セキュリティホールやシステムの不具合，人的ミス，組織としての危機管理体制，職員のモラルなども含まれる	1,6,13,22,26,35,37,47,61,62
	リスク分析/評価	情報資産および情報資産に対する脅威を識別し，事故が発生した場合の影響の大きさを分析し，現在実施している対策が十分なものかを評価すること	1,6
	リストア	破損したシステムやディスク，データベースなどを復旧すること	8,58
	リムーバブルメディア	記憶装置からディスクを取り外し，交換して使用できる装置または媒体	12,18,24,34,54
	リモートアクセス	遠隔地からサーバ等に接続すること	12,17,18,62
	ルータ	ネットワーク上を流れるデータを他のネットワークに中継する機器	4,55,63,64,65
	ルートキット	悪意のあるソフトウェアの一種で，許可なしにインストールされた場合，その存在を隠して，コンピュータシステムの管理者レベルの制御を奪い取る	30,67
	ログレビュー	サーバ等のログデータの内容を確認すること	12,41

	用語	解説	出現ページ
わ	ワーム	自己増殖を繰り返しながら不正活動を行なうコンピュータプログラム	30,67

	用語	解説	出現ページ
A-G	DNS	「ドメインネームシステム（Domain Name System）」または「ドメインネームサーバ（Domain Name Server）」の頭字語。インターネットなどネットワーク上の分散データベースに，ドメイン名に関連する情報を格納するシステム	4,46,47,53,57,64

	用語	解説	出現ページ
H-N	ID	特定のユーザまたはアプリケーションの識別子	28,48,49,52,54,59,60,61,65,66
	IPA	独立行政法人　情報処理推進機構（Information-technology Promotion Agency,Japan） のこと http://www.ipa.go.jp/	8,49
	NTP	「ネットワークタイムプロトコル（Network Time Protocol）」の頭字語。コンピュータシステムの時計を同期するためのプロトコル	4,53

	用語	解説	出現ページ
O-Z	PCI データセキュリティ基準／PCI DSS	Payment Card Industry Data Security Standard の頭字語。VISA やJCBなどクレジットカードの国際ブランド5社が共同策定したカード情報保護のためのセキュリティ基準。準拠すればカード情報の漏えい防止につながる。情報セキュリティの認証基準としてはISMS（情報セキュリティマネジメントシステム）などが先行して普及しているが，PCI DSS はクレジットカード情報の保護に特化した，より具体的な基準である	2
	Web サーバ	Web クライアントからの HTTP 要求を受け入れて，HTTP 応答（一般に Web ページ）を提供するプログラムが組み込まれたコンピュータ	4,14,42,46,47,50,57
	Web ホスティング会社	Web サービスの提供を行っている事業者	16

用語集　「システムの開発，構築，運用者編」

	用語	解説	出現ページ
あ	アーカイブファイル	文書ファイルやプログラムなどを一つにまとめたファイル	56
	アカウント･データベース	利用者 ID のデータベース	34
	アクティブ	使用状態にすること。使用可能状態にあること	37,48,51,60
	暗号化アルゴリズム	暗号化を行うための一連の数学的な手順	34
	暗号鍵	暗号化および復号化するときに用いるデータのこと	34,35,36,45,56,66,67
	安全でないプロトコル/サービス/ポート	セキュリティ上の問題があるプロトコル，サービス，またはポートのこと。例えば，FTP はネットワーク上で暗号化せずにパスワードを送信してしまうため，インターネットで利用する場合には安全ではない	47,63
	インジェクション	注入攻撃。SQL インジェクション	48,50
	エッジ・ルータ	あるネットワークと別のネットワークの境界に位置するルータ	65

	用語	解説	出現ページ
か	監査証跡ファイル	監査ログが記録されたファイル	56,57
	強力な暗号／強力な暗号技術	業界で認められたテスト済のアルゴリズムに，十分なキーの長さと適切なキー管理の実践が伴った暗号化技術。暗号化技術とは，データを保護する技法で，暗号化（復号可能）とハッシング（復号不能な「一方向」）の両方が含まれる。業界で認められたテスト済のハッシングアルゴリズムの例として，SHA-1 が挙げられる。業界で認められたテスト済の暗号化の標準およびアルゴリズムの例として，AES（128 ビット以上），TDES（最小倍長キー），RSA（1024 ビット以上），ECC（160 ビット以上）および ElGamal（1024 ビット以上）が挙げられる。詳細については，NIST Special Publication 800-57（http://csrc.nist.gov/publications/）を参照	25,34,35,36,45,46,55,56,59,66,67
	強力な暗号鍵	上記の暗号技術で用いられる暗号鍵。 暗号鍵の長さが長くなるほど，バリエーションが多くなり，暗号の強度も「強い」と言える。暗号鍵のバリエーションを十分増やせば，総当たり攻撃による解読は現実的に不可能になる	35,36

	クレデンシャル	信任状，証明書	50
	クロスサイトスクリプティング／XSS	ソフトウェアのセキュリティホールの一つで,Web サイトの訪問者の入力をそのまま画面に表示する掲示板などのプログラムが，悪意のあるコードを訪問者のブラウザに送ってしまう脆弱性のこと	48,50
	クロスサイトリクエストフォージェリ／CSRF	Web サイトにスクリプトや自動転送(HTTP リダイレクト)を仕込むことによって，閲覧者に意図せず別の Web サイト上で何らかの操作(掲示板への書き込みなど)を行なわせる攻撃手法	50
	ゲートウェイ	ネットワーク上で，媒体やプロトコルが異なるデータを相互に変換して通信を可能にする機器	37
	公共ネットワーク	公衆にデータ伝送サービスを提供する目的で，通信プロバイダによって運用されるネットワーク。公共ネットワーク上でデータを伝送する場合，伝送中にデータが傍受，変更，または宛先が転換される可能性がある	56
	コンソール	ネットワーク環境で，サーバまたはメインフレームコンピュータへのアクセスまたは制御を行うための画面およびキーボード	55

	用語	解説	出現ページ
さ	サードパーティベンダ	既存のハードウェア／ソフトウェア製品に対して，新しい機能を提供するベンダの総称	47
	システム実行ファイル	システムを稼働されるために必要となるアプリケーションファイル	56
	情報コンセント	建物内部に情報配線(LAN など)が敷設された学校などで，情報通信機器をネットワークに接続するために壁などに用意された接続口(ソケット)のこと。どこでも手軽に情報ネットワークに接続できる点を，電気のコンセントになぞらえてこのように呼ぶ	37
	信頼できないネットワーク	組織に属するネットワーク外のネットワークおよび組織の制御または管理が及ばないネットワーク	63,64
	ステートフルインスペクション	「動的パケットフィルタリング」とも呼ばれる。通信パケットを追跡して強力なセキュリティを提供する，ファイアウォールの機能。適切な応答（「確立された接続」）の着信パケットのみが，ファイアウォールの通過を許可される	64,65
	ストアードプロシージャ	Stored Procedure　データベースに対する一連の処理手順を一つのプログラムにまとめ，データベース管理システムに保存したもの	60
	スマートカード	「チップカード」または「IC カード（Integrated Circuit Card)」とも呼ばれる。集積回路を埋め込んだカードの一種。回路は「チップ」とも呼ばれ，磁気ストライプデータと同等のデータおよびその他のデータを含むカードデータが収録されている	62,66
	責務の分離	異なる担当者間で職務の工程を分離して,1 人の担当者がプロセスを破滅させることがないようにすること	48
	設定値ファイル	設定値を記録したファイル	56

	用語	解説	出現ページ
た	知識分割	2 つ以上の事業体が別々にキーコンポーネントを持っており,個々の知識では暗号鍵を生成できないようにした状態を指す	35,36
	チョーク・ルータ	内部ネットワークと DMZ の境界に置くルータ。パケットフィルタリングによるネットワークアクセス制御を行う	65
	デフォルトパスワード	システム，アプリケーション，またはデバイスで事前定義されているシステム管理アカウントまたはサービスアカウントのパスワード。一般に，デフォルトアカウントと関連付けられる。デフォルトアカウントおよびデフォルトパスワードは，公開され広く知られているため，容易に推測できてしまう	46
	動的パケットフィルタリング	「ステートフルインスペクション」を参照	64,65
	トランケーション	一部の文字列を除いて非表示にすること	34

	用語	解説	出現ページ
な	二重管理	2 人以上の管理者に権限を分担することにより,機密性の高い機能や情報を保護する手法	35,36
	２要素認証	例えば IC カードと ID・パスワードというように,利用者に固有な二つの要素により確実に認証すること。２要素認証の場合，異なる性質を持つ有効な認証方法を組み合わせることが必要で，パスワードを 2 つ入力させただけでは２要素認証とはいえない	59,62,66

	用語	解説	出現ページ
は	ハッシュ（ハッシング）	元のデータから一定の長さの文字列を生成するハッシュ関数によって，平文（暗号化されていない通常のデータ）を暗号化されたデータに変換すること。ハッシュ関数によって生成されたデータはダイジェストと呼ばれ，異なる元データから同一のダイジェストが生成される可能性は非常に低いと言われている。そこで,2 つのデータが同一のものであることを確認する必要がある際に，ハッシュ関数が利用される。元データのサイズが大きい場合でも，短いダイジェストを比較するだけで済み,高速にデータの同一性を証明できるため,電子署名などで利用されている	34
	平文	暗号化されていないデータ	34

	ファイル完全性監視	データファイルが不正に改変されていないかを監視すること	7,56,57
	ファイルシステム	データファイルを管理するためのシステム	34,46,47
	ブロードキャスト	ネットワーク内で，不特定多数の相手に向かってデータを送信すること	65
	ペネトレーションテスト	コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで，システムを実際に攻撃して侵入を試みる手法	14,15,42,43
	ホスティングプロバイダ	システムの構築，運用，保守や障害時の対応まで，システムの管理を一括して請け負う事業者	44
	ホスト/ホストコンピュータ	コンピュータのソフトウェアが配置されている，メインコンピュータのハードウェア	42,44,53,64

	用語	解説	出現ページ
ま	マスキング	データを非表示にして保護すること	34
	無線ネットワーク/ワイヤレスネットワーク	回線への物理的接続なしで，コンピュータを接続するネットワーク	45,46,56,63,66,67

	用語	解説	出現ページ
ら	履歴ファイル	履歴データが記録されたファイル	56
	論理アクセス	アプリケーションあるいはデータに対する，インターフェースを介した認証に基づくユーザアクセス	34,51

	用語	解説	出現ページ
わ	ワイプ・プログラム	回復することができないようにデータを消去するためのプログラム	39
	ワンウェイハッシュ	ハッシュ関数による一方向の（逆変換ができない）データ変換	34

	用語	解説	出現ページ
A-G	AES	Advanced Encryption Standard の略。米国政府が政府内の標準として策定した暗号化規格のこと。高い強度を持ちながら，暗号化/復号化処理を高速に実行できることが特徴。	45,67
	CPS	Certification Practice Statement 認証局運用規定。認証局（CA）が電子証明書を発行する際の運用規定やその目的などを記したドキュメント。対外的に公表する。CA のサービス詳細や認証ポリシーなどの文書から参照させる。CPS の目次フォーマットは RFC2527 で提案されている	35
	DMZ	「Demilitarized Zone（非武装地帯）」の略語。組織の内部プライベートネットワークへの追加のセキュリティ層となる，物理または論理サブネットワークまたはコンピュータホスト。DMZ はインターネットと組織の内部ネットワークの間に新たなネットワークセキュリティ層を追加し，外部の者が内部ネットワーク全体ではなく，DMZ 内のデバイスにのみ直接アクセスできるようにする	63,64,65
	FTP	「ファイル転送プロトコル（File Transfer Protocol）」の頭字語。インターネットなどの公共ネットワークを介して，コンピュータ間でデータを転送するネットワークプロトコル。パスワードやファイル内容が平文で保護されずに送信されるため，FTP は一般に安全でないプロトコルと考えられている。FTP は，SSH などの技術を使用することで安全に実装できる	47

	用語	解説	出現ページ
H-N	HSM	「HSM(Hardware Signing Module) 」の頭字語。 暗号鍵を生成および管理するハードウェア機器であり，暗号鍵を安全な方法で作成し，暗号鍵の強度を設定できる。管理に関する機能も有する	35,36
	HTTPS	「Hypertext Transfer Protocol over Secure Socket Layer（Secure Socket Layer を経由するハイパーテキスト転送プロトコル）」の頭字語。World Wide Web 上で認証および暗号化された通信を提供する，セキュリティ保護された HTTP。Web ベースのログインなど，セキュリティが問題となる通信のために設計されている	56

	IDS	「侵入検知システム（Intrusion Detection System)」の頭字語。ネットワークまたはシステムへの侵入の試みを識別し，警告するソフトウェアまたはハードウェア。イベントを監視してセンサーに対する警告および制御を行うコンソール，センサーによってログ記録されたイベントをデータベースに記録する中央エンジンなど，セキュリティイベントを生成するセンサーで構成されている。検知されたセキュリティイベントに対して，システムのルールを使用して警告を生成する	54,58
	IP	「インターネットプロトコル（Internet Protocol)」の頭字語。パケットをルーティングするためのアドレス情報および一部の制御情報を含む，ネットワーク層のプロトコル。IP は，インターネットプロトコルスイートの主要なネットワーク層プロトコルである	53,64,65
	IP アドレス	「インターネットプロトコルアドレス（Internet Protocol Address)」とも呼ばれる。インターネット上で特定のコンピュータを一意に識別する数値コード	53,64,65
	IPS	「侵入防止システム（Intrusion Prevention System)」の頭字語。IDS は侵入の試みを検知するが，IPS はさらに侵入の試みをブロックする	54,58
	IPsec	「Internet Protocol Security（インターネットプロトコルセキュリティ)」の頭字語。すべての IP パケットを暗号化または認証（あるいはその両方）を行い，IP 通信をセキュリティ保護するための規格。IPsec は，ネットワーク層でセキュリティを提供する	56,62
	IP マスカレード	インターネットに接続された企業などで，一つのグローバルな IP アドレスを複数のコンピュータで共有する技術。組織内でのみ通用する IP アドレス(ローカルアドレス)と，インターネット上のアドレス(グローバルアドレス)を透過的に相互変換することにより実現される	64,65
	LAN	「ローカルエリアネットワーク（Local Area Network)」の頭字語。一般に建物または建物群など，狭い領域を対象とするコンピュータネットワークを指す	46,54,57
	NAT	「ネットワークアドレス変換（Network Address Translation)」の頭字語。ネットワークマスカレードまたは IP マスカレードと呼ばれている。あるネットワーク内で使用されている IP アドレスを，別のネットワーク内で認識されている別の IP アドレスに変更する	64,65
	NIST	National Institute of Standards and Technology 「(米国)標準技術局」の略。連邦政府の機関で，工業技術の標準化を支援している。1988 年に NBS(National Bureau of Standards)が改組して誕生した。連邦政府の標準暗号を制定する機関として有名	46

	用語	解説	出現ページ
O-U	OWASP	「Open Web Application Security Project」の頭字語。アプリケーションソフトウェアのセキュリティを向上させるために，2004 年に設立された非営利団体。OWASP は，Web アプリケーションの最も危険な脆弱性を一覧表示した，OWASP トップ 10 を発表した（http://www.owasp.org を参照）	49,50
	PAT	「ポートアドレス変換（Port Address Translation）」の頭字語で，「ネットワークアドレスポート変換」とも呼ばれる。ポート番号も変換する NAT の種類	64
	RADIUS	「Remote Authentication Dial-In User Service」の略語。RADIUS サーバに渡されたユーザ名やパスワードなどの情報が正しいかどうかを確認して，システムへのアクセスを許可する，認証/アカウンティングシステム	62
	RBAC	「役割ベースアクセス制御（Role-based Access Control）」の頭字語。特定の承認されたユーザのアクセスを，職責に基づいて制限する制御手法	48,49,62
	RFC	インターネットに関する技術の標準を定める団体である IETF(Internet Engineering Task Force)が正式に発行する文書	35,64,65
	SANS	SysAdmin, Audit, Network, Security Institute 米国において，政府系機関，一般企業，大学などの教育機関を対象に，情報セキュリティの調査・研究・教育を行うことを目的として 1989 年に設立された情報セキュリティ専門の民間団体。数々のセキュリティ関連の書籍を出版しているほか，セキュリティ・アラート情報を提供している	46
	SNMP	「簡易ネットワーク管理プロトコル（Simple Network Management Protocol）」の頭字語。管理者がすべきあらゆる状況に関して，ネットワーク接続デバイスの監視をサポートする	45,46,66,67
	SNMP コミュニティ文字列	SNMP で情報取得のために用いられる文字列。このコミュニティ文字列がデフォルトや慣習的に使用される文字列となっていることが，ペネトレーションテスト中に発見されることが非常に多い	45,46,66,67

	SHA-1	Secure Hash Algorithm 1 認証やデジタル署名などに使われるハッシュ関数(要約関数)のひとつ。2 の 64 乗ビット以下の原文から 160 ビットの「ハッシュ値」を生成し，通信経路の両端で比較することで，通信途中で原文が改ざんされていないかを検出することができる。計算方法には初期値敏感性の不可逆な一方向関数を含むため，ハッシュ値は擬似的な乱数のような値をとり，これをもとに原文を再現することはできない。また，同じハッシュ値を生成する別のメッセージを作成することも極めて困難である。1995 年に米国標準技術局(NIST)によってアメリカ政府の標準ハッシュ関数として採用された。インターネット上で安全に通信を行なうための IPsec などに応用されている	34
	SQL	「Structured Query Language」の頭字語。リレーションシップデータベースマネジメントシステムでのデータの作成，変更，抽出に使用するコンピュータ言語	50
	SQL インジェクション	データベース駆動型 Web サイトでの攻撃の形式。悪意のあるユーザが，インターネットに接続されたシステム上で安全でないコードを利用して，不正な SQL コマンドを実行する。SQL インジェクション攻撃は，通常はデータを入手できないデータベースから情報を盗むため，またはデータベースをホストしているコンピュータを介して組織のホストコンピュータにアクセスするために使用される	50
	SSH	主に UNIX コンピュータで利用される，ネットワークを介して別のコンピュータにログインしたり，遠隔地のマシンでコマンドを実行したり，他のマシンへファイルを移動したりするためプログラム。ネットワーク上を流れるデータは暗号化されるため，インターネット経由でも一連の操作を安全に行なうことができる	47,55
	SSL	「Secure Sockets Layer」の頭字語。Web ブラウザと Web サーバ間のチャネルを暗号化して，チャネル上を伝送されるデータのプライバシーと信頼性を確保するために確立された業界標準	55,56,62
	TACACS	「Terminal Access Controller Access Control System」の頭字語。リモートアクセスサーバと認証サーバ間で通信するネットワークで，ネットワークへのユーザアクセス権を決定するために使用される，一般的なリモート認証プロトコル	62
	TCP	「Transmission Control Protocol」の頭字語。インターネットの基本的な通信言語またはプロトコル	65
	TELNET	「Telephone Network Protocol」の略語。一般に，ネットワーク上のデバイスに，ユーザ主導のコマンドラインログインセッションを提供する。ユーザ資格証明は平文で伝送される	55
	TLS	「Transport Layer Security」の頭字語。通信を行う 2 つのアプリケーション間で，データ機密性とデータ整合性を実現するために設計されている。TLS は SSL の後継	55,56,62

	用語	解説	出現ページ
V-Z	VPN	「仮想プライベートネットワーク（Virtual Private Network）」の頭字語。一部の接続が，物理回線による直接接続ではなく，インターネットなどの大規模ネットワーク内の仮想回線で行われるコンピュータネットワーク。この場合，仮想ネットワークのエンドポイントは，大規模ネットワークをトンネリングする。通常のアプリケーションでは公共のインターネットを介してセキュリティ保護された通信が行われるが，VPN は認証またはコンテンツの暗号化など強力なセキュリティ機能を使用する場合と使用しない場合がある	55,62

●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　　千葉大学教育学部附属中学校

●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　解説書

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/