学校情報セキュリティ・ハンドブック

～今日から始められるセキュリティポリシーの作り方～

財団法人 コンピュータ教育開発センター

はじめに

近年，情報化社会の進展に伴って毎日のように情報セキュリティに関する様々なトラブル事例が報じられています。この中には，学校で生じているトラブル事例も含まれています。パソコンの紛失・盗難による児童生徒の重要な情報の漏洩，ウイルス感染をはじめ，最近ではファイル共有ソフト（Winnyなど）による情報流出などについて耳にされた方も多いと思います。

こういった学校で生じるセキュリティに関するトラブル事例への対応としては，各学校でそれぞれ自らが持っている学校の情報としては何があるか，また，それらに対するリスクとしては何があるかを考え，そのリスクに如何に対応するかを整理し，「学校情報セキュリティポリシー」として策定・実行していくことが重要となります。しかしながら，企業などでは一般的に見られるようになっているセキュリティポリシーも学校現場ではあまり馴染みがないというのが実情だといえます。

このため，今回この冊子を作成しました。

この冊子の狙いは，学校における情報セキュリティ意識の向上を図ることと，学校現場に相応しいセキュリティポリシーの策定を提案し示すことです。その結果，より実効性の高い（実際に守り，運用できる）ポリシーの策定・運用が可能となる手助けになることをねらっています。また，この冊子の利用者は，校長・教頭（副校長）を含めた学校の全教職員としていますが，とりわけポリシー策定担当となる先生を意識してまとめています。さらに，多忙な教職員を対象にしていますので，極力，平易かつ簡潔な内容としています。

まずはこの冊子の内容を各学校現場で適用していただき，その上で更なるバージョン・アップを図っていきたいと考えています。皆様方のお意見ご提案を宜しくお願い致します。

平成18年３月

学校情報セキュリティ委員会　委員長　藤村　裕一

目　次

この冊子でできるようになること

自分が起こす危険性のある事故と，それを防止するための具体策がわかる！

・この冊子を読み，手順どおりに実施していくと，パソコンやネットワークの利用時の脅威や知らないうちに起こしてしまうかもしれない事故（個人情報の流出や学校のネットワークシステムなどに被害を及ぼしてしまうことなど）を知ることができます。

・あなたは，「自分は大丈夫！」と，思っているかもしれませんが，普段はとても優秀で誰からも信頼されている教職員が，個人情報流出などの事故を起こして，全国放送に取り上げられたり，懲戒処分を受けたりということが後を絶ちません。決して他人事ではないのです。また，自分自身の問題だけでなく，子供たちをリスクに晒す可能性があることも自覚する必要があります。

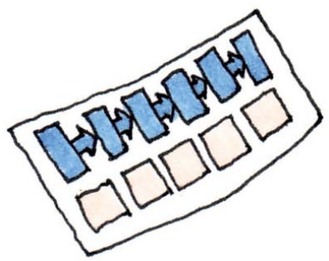
・「気を付ける」だけでは，情報セキュリティを守ることはできません。そのために，どうしたらよいのかを知り，即実践することが必要なのです。この冊子を読んで，学校情報セキュリティポリシーを作り，みんなで守っていけば，右の図のような事故を防ぐことができます。

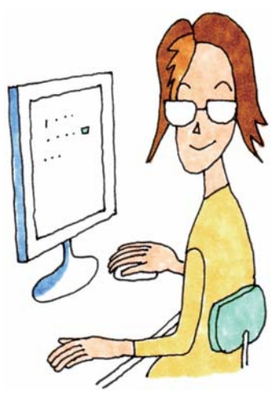
セキュリティポリシーの作成・運用の仕方がわかる！

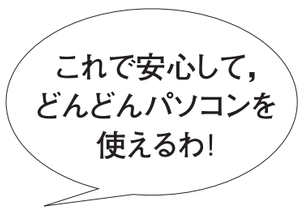
・学校現場でのセキュリティポリシーの作成の仕方が，事例を見ながらわかるようになります。この手順に従ってセキュリティポリシーを作成していくと，あなたの学校に合ったセキュリティポリシーができます（個人が守ること，学校全体として守ることもわかります）。

・作成されたセキュリティポリシーを関係者全員で遵守し，運用していけば，学校の情報セキュリティが確保され，授業や校務で安心してパソコンやネットワークを活用していくことができるようになります。

自校の
セキュリティポリシー





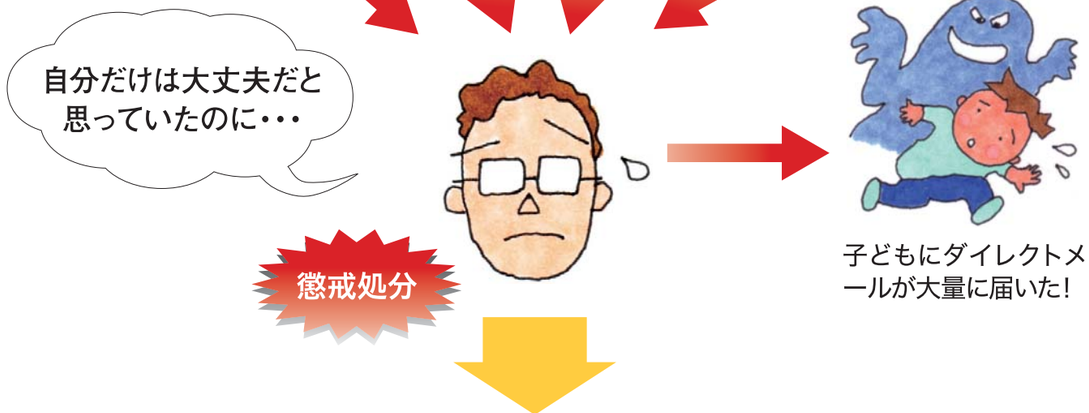


車上ねらいに，成績などの個人情報の入ったパソコンを盗まれた！

名簿などの情報が入ったＵＳＢメモリを，なくしてしまった！

通知票のデータや住所録などを，ファイル共有ソフト（Ｗｉｎｎｙなど）で，インターネット上に流出させ，回収不能になった！

ウイルスに感染した個人所有パソコンを，校内ＬＡＮに接続し，市のネットワーク全体を止めてしまった！



この冊子を読めば，情報セキュリティ確保の具体策がわかり，即，実践できます！

検討の進め方　～5段階のポリシー作成手順～

■セキュリティポリシー作成手順の全体像

・セキュリティポリシーの作成は以下の５段階の手順で行うのが理想的です。

・各ステップのアウトプットは次のステップのインプットにつながっています。全体の流れを意識しながら，検討を行いましょう。

step 1 問題意識の共有

●トラブル事例の共有を通じて情報取扱ルールの重要性やリスクについて教職員と意識を共有し，ポリシー作成計画の承認を得る

何をやるか

●情報トラブル事例

step 2 リスクなどの整理

●学校内の情報に関する重要情報資産やそのセキュリティ上の脅威を洗い出し，リスクの有無を整理する

何を守るか

●検討体制，実施スケジュール
●セキュリティポリシー作成に対するコンセンサス
●管理職の承認

●一般的な学校の情報資産リスト例
●一般的な学校の情報セキュリティ脅威例

step 3 リスク対応策の検討

●セキュリティ ィポリシーの元となる具体 的なリスク対応策を決定 する

どう 守るか

●学校内の情報資産管理表
●学校内の情報セキュリティ・リスクリスト

●セキュリティ ポリシーに記載されるリスク 対応例

step 4 ポリシー作成

●セキュリティポリシーを作成する

ポリシー完成

●リスクごとの対応策

●自治体のセキュリティポリシー
●個人情報保護条例
●セキュリティポリシーひな形
●セキュリティポリシーチェックシート

step 5 ポリシー運用

●作成したセキュリティポリシーを円滑に運用するための工夫を行う

運用サイクルを回す

●自校のセキュリティポリシー

●実施手順書
・作業手順書
・操作説明書　など

●改正版セキュリティポリシー

STEP1　：問題意識の共有をしましょう！

セキュリティポリシーの策定に当たっては，まず，問題意識の共有が重要となります。セキュリティポリシーの策定を始める際には，策定担当者だけでなく，実際にセキュリティポリシーを守ってもらう一般の教職員を上手に巻き込むことが重要になります。

1．1　過去に起こったトラブル事例から危機意識を共有しましょう

・このためには，他の地域で実際に起こったセキュリティに関連するトラブル事例を共有する方法が比較的多く見られます。

1．2　校長が出席する会議の場での報告や学校へのパンフレットの配布などを通じて周知しましょう

・教職員に対する周知の方法としては，学校においてトラブルに対する管理責任を負っている校長や教頭（副校長）の集まる場での定期的な報告，というスタイルを取るのが一般的です。

・また，教職員などに対する既存パンフレット配付や通知文書などの手法で広く問題の共有を図る手法も取られます。

1．3　一方的な情報発信だけでなく，巻き込み型の問題意識共有をしましょう

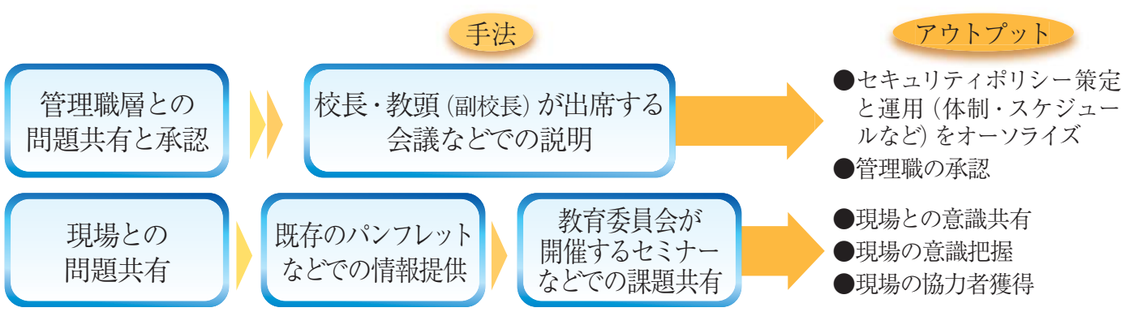
・一方的な情報発信だけでなく，トラブル事例を活用したグループ討議を行い，自分達の身近な問題に置き換えた議論を行なうことも有効です。

・具体的には，「個人情報の持ち出しとリスク」などのテーマで事例を抽出して，このようなリスクを回避するにはどのような方策があるか？その方策を自分達が運用するとどのような問題が生じるか？などのポイントで議論し，参加者に身近な問題として意識させ，当事者意識を高めることが重要です。

1．4　セキュリティポリシー策定の計画を作り，管理者の承認を得ましょう

・このような議論を通じて教職員間で問題意識の共有を図り，情報セキュリティ委員会などセキュリティポリシーの検討体制やスケジュールを作って，セキュリティポリシー作成のコンセンサスや管理職の承認を得ることが必要です。

≪図表1　ＳＴＥＰ１の手法とアウトプット≫



近年よく起こっているトラブル事例は？

近年，学校で生じているセキュリティに関連するトラブル事例として，「個人情報漏洩・紛失」や「ウイルス感染」に関連するものが多く報告されています。最新の情報トラブル事例の収集には，各新聞社が提供しているホームページ上での記事検索などを活用するのが有効です。

≪図表2　近年の情報トラブル事例≫

	学　校	発生時期	内　容
校内での盗難・紛失	高等学校	2005年3月	学校内の金庫で書類とともに管理されていたフロッピーディスクが紛失した。出し入れをした間に紛失した可能性が高いという。フロッピーディスクには受験生 97 人分の氏名や生年月日，在籍校，成績など個人情報が含まれていた。
	高等学校	2005年4月	生徒指導室の机の上に置かれていた在校生 197 人分の数学の成績や卒業生 40 人分の各教科の成績などが保存されていたパソコンが盗まれた。
	中学校	2005年5月	男性教諭が職員室のパソコンに全校生徒の氏名・住所・電話番号・英語の成績などの個人情報が入った携帯型記録媒体（USB メモリ）を接続して作業後，そのまま帰宅。翌日出勤した際，紛失に気付いた。
	小学校	2005年10月	女性教諭が退勤する際，児童の個人情報が保存されていたノートパソコンを鞄ごと置き忘れた。翌朝，置き忘れに気付き，前日鞄を置き忘れたと思われる場所を捜索したが発見できなかった。
校外での盗難・紛失関連の事例	小学校	2004年12月	女性教諭が原付バイクで帰宅途中，前かごに入れておいた手提げかばんを背後から原付バイクできた男にひったくられた。かばんの中には担任クラスの全生徒の指導要録と調査書などが入っていた。
	高等学校	2004年12月	男性教諭が帰宅途中に飲酒し電車内で眠り，約2時間後に起きたときには，生徒の答案用紙と成績などを記録したMOディスク1枚が入ったかばんが紛失していた。
	中学校	2005年6月	女性教諭が帰宅途中，子供を迎えに寄った保育所に駐車したところ，自家用車の窓ガラスが割られ，車内に置いてあったノートパソコンをバッグごと盗まれた。そのパソコンには生徒の成績や保護者の名簿などの個人情報が保存されていた。
	養護学校	2005年9月	女性教諭が帰宅途中，薬店に駐車したところ，自家用車の窓ガラスが割られ，生徒３人分の指導内容が記録された記憶媒体（フラッシュメモリ）と教職員 17 人分及び生徒 79 人分の緊急連絡先が記載された書類が入ったバックを盗まれた。
	教育委員会	2005年9月	教職員課主幹の男性職員が，次年度採用の教員試験の受験者 1606 人や，県教委が指導力不足と認定した教員 175 人の氏名など，延べ 3202 人分の個人情報を記録したパソコンの記録媒体 (フラッシュメモリ)1 個を持ち出し，紛失した。
ウイルス関連	小学校	2005年6月	校務主任の教諭が全校児童 535 人分と教職員約 30 人分の個人情報を記録したメモリを自宅に持ち帰り，家族所有のパソコンにコピーしたところ，ウイルスに感染し，ファイル交換ソフト Winny を通じて名簿がインターネット上に流出した。
	小学校	2006年1月	男性教諭の私物パソコンから担任児童 36 人分の成績情報がインターネット上に流出した。ファイル交換ソフト Winny によるウイルス感染が原因とみられる。
その他	中学校	2005年4月	子供が通う中学校の指導方針に反感を持ったカメラマンの男性が，中学校から個人情報が入ったパソコンを盗み，インターネット上の掲示板に同校の中傷やパソコンから取り出した教員の個人情報を公開し，嫌がらせをした。
	教育委員会	2005年4月	公立小中学校の一部児童の情報が流出したことが，個人情報の買い取りを求める脅迫めいた電話により発覚した。流出したとみられる個人情報は，廃棄業者によって廃棄されたパソコンに保存されていたもので，生徒や保護者の氏名，住所，電話番号，成績など約 6000 名の個人情報が含まれていたという。

STEP 2：リスクや情報資産を整理しましょう!

問題意識の共有が進むと次に学校におけるリスクや情報資産の整理とそれに基づく情報セキュリティ・リスクリストの作成が重要となります。

情報資産や脅威の発見と，リスクの整理とは？

・リスクとは，情報資産が脅威にさらされることです。（正確には，脅威だけでは問題が生じることはなく，その組織・IT 環境などの持つ弱さ・不備などが加わって問題が生じることになりますが，ここではそういった弱さなども含めて脅威として呼ぶことにします）

・リスクを検討する際には，まず保護すべき重要情報資産を整理します。そして，その情報資産がどのような脅威にさらされているかを発見して整理することが必要です。そのためには，学校の業務に精通し，この問題に関心の強い教職員を巻き込んで議論をするのが有効です。

・重要情報資産に対する脅威の大きいことを，リスクが存在するとして，対応が必要かどうかを検討します。

《図表3　情報資産の整理とリスク対応策の流れ》

2．1　学校における情報資産の整理

・学校内に存在する文書や書類を洗い出し，分類・整理します。

・分類の方法など，学校毎に状況が異なる可能性がありますので，図表4に示した一般的な学校における情報資産リスト例を参考に，各学校の持つ情報を整理してみましょう。

《図表4：一般的な学校における情報資産リスト例》

学籍関連	生徒指導関連	成績関連
●学校沿革誌 ●卒業生台帳 ●同窓会名簿 ●学校要覧 ●教育計画 ●指導要録（学籍） ●指導要録（成績） ●指導要録抄本 ●出席簿 ●生徒名簿 ●転出入関係綴り	●在校生顔写真 ●家庭環境調査書 ●生徒住所録 ●生徒緊急連絡網 ●事故報告	●定期考査問題 ●成績一覧 ●定期考査得点通知 ●通知表
進路関連	**保健関連**	**事務関連**
●進路結果 ●進路指導カード ●入試成績 ●調査書 ●模試データ	●健康診断書 ●保健調査票 ●学校生活管理指導票 ●教育相談記録	●教職員履歴カード ●給与等支給明細書 ●学納金振替結果帳票

2．2　守るべき情報資産の絞り込み

・整理した自校に存在する情報資産の管理表を作成します。

・管理部署（管理者），保存形態，公開の有無，情報資産の重要度などを，図表5に示した学校内の情報資産管理表フォーマットの例を参考に，整理しましょう。

・重要度は，その情報が外部に漏れたり消失した場合の影響度も考慮し，資産としての重要性を3段階（大中小）程度に評価するのが有効です。

・重要度の評価の結果として，守るべき情報資産を絞り込みます。図表5に示した例では，重要度の大中の資産を守るべきものとして絞り込んでいます。どこまで絞るかは，学校の考え方にもよりますので，教職員間で話し合って決めてください。

以降の STEP では，守るべき情報資産として卒業生台帳を例に説明します。

《図表5：学校内の情報資産管理表フォーマットの例》

情報資産		管理者	保存形態	公開の有無	主な記載内容	公開の範囲	重要度	守るべき情報資産
学籍関連	学校沿革誌	教頭（副校長）	紙	○	創立日，歴代校長名　など	一般	小	
	卒業生台帳	教頭（副校長）	紙	×	氏名，住所，進学先　など		中	○
	同窓会名簿	教頭（副校長）	紙	×	氏名，住所，事務局，会長名 など		中	○
	学校要覧	教頭（副校長）	紙	○	教職員氏名　など	一般	小	
	出席簿	教頭（副校長）	紙	×		校内	大	○
	生徒名簿	教頭（副校長）	電子媒体	×				

2．3　脅威の洗い出し

・絞り込んだ守るべき情報資産ごとに，情報セキュリティ上の脅威を洗い出します。

・自校の脅威を，図表6に示した一般的な学校における情報セキュリティ脅威例を参考に洗い出してください。脅威になるか否かは，学校の環境によっても異なってきます。

《図表6:一般的な学校における情報セキュリティ脅威例》

個人情報漏洩関連の脅威	情報消失関連の脅威
●個人所有パソコンの盗難，紛失による漏洩 ●USBメモリ等のメディアの盗難，紛失での個人情報漏洩 ●学校ホームページへの個人情報掲載による漏洩 ●メール誤送信による漏洩 ●学校内パソコンのウィルスやスパイウェア感染による漏洩 ●情報機器処分時のデータ消し忘れによる漏洩 ●ネットワーク上からのハッキングによる漏洩 ●個人認証におけるなりすましによる漏洩 ●児童生徒によるネットワーク侵入による漏洩 ●ディスプレイ盗み見による漏洩 ●教職員による意図的な漏洩 ●データの不適切な廃棄による漏洩 ●委託業者などによる情報の漏洩 ●不用意なネットワークサービスの利用による情報の漏洩 ●バックアップデータの不適切な扱いによる情報の漏洩 ●学校施設の外部公開による情報の漏洩 ●無線 LAN を利用したアクセスによる情報の漏洩	●個人所有パソコンの盗難，紛失による情報消失 ●USBメモリー等のメディアの盗難，紛失による情報消失 ●ウイルス感染による情報消失 ●突然の電源断による情報消失 ●メディアの損傷などによる情報消失 ●パソコン・サーバの盗難，紛失による情報消失 ●誤消去等，人為的なトラブルによる情報消失 ●ディスク障害などハードウェアトラブルによる情報消失 ●保存ミスなどデータの扱い不全による情報消失
業務停止に至る脅威	**情報モラルに関する脅威**
●学校内パソコン等のウイルス感染による業務停止 ●サーバ，システム等のダウンによる業務停止 ●ネットワークへのアタックによる業務停止 ●停電による業務停止 ●システムの誤用など人為的ミスによる業務停止	●有害サイトへのアクセス ●ソフトの不正コピー，インストール ●児童生徒によるデータの持ち出し ●掲示板・チャット等への荒らし行為 ●ファイル交換ソフトなどの違法利用 ●アカウントの不正利用

2．4　脅威の評価

・守るべき情報資産の一つ一つに対して洗い出した脅威の大きさを，図表7に示した学校内の脅威の評価の例を参考に3段階（大中小）に評価しておきます。頻繁に発生し実際に発生したときの被害が大きいことが，脅威が大きいということになります。図表7の例では，卒業生台帳についての情報セキュリティ脅威を評価しています。

《図表7:学校内の脅威の評価の例:卒業生台帳の例》

情報資産名：卒業生台帳

	情報セキュリティ脅威名	脅威の評価	脅威の評価判断の根拠
個人情報漏洩関連	学校ホームページへの個人情報掲載による漏洩	大	ホームページの更新頻度が高く，情報量も多いため
	個人所有パソコンの盗難，紛失による漏洩	小	個人所有パソコンの持込を認めていないため
	メール誤送信による漏洩	小	教職員個人にメールアドレスを付与していないため
	教職員による意図的な漏洩	大	情報の取扱・持ち出しルールが定められていないため
	ネットワーク上からのハッキングによる漏洩	大	外部からのアタックが頻繁に起こっているため
	データの不適切な廃棄による漏洩	大	情報機器の廃棄時のルールが明確でないため
	個人認証におけるなりすましによる漏洩	中	

2．5　リスク対応の必要な領域の特定

・守るべき情報資産が絞り込まれ，その情報資産に対する脅威が評価されると，対応が必要かどうかの検討に入ります。

・STEP 2．2で絞り込んだ「守るべき情報資産」の重要度と，STEP 2．4で評価した「自校の脅威」の大きさとから，リスク対応の必要性を検討します。この検討に当たっては図表8のリスク対応評価表の例を活用すると有効です。

・「守るべき情報資産」の重要度（図表5）と，その資産への「自校の脅威」の大きさ（図表7）から，資産ごとの脅威を図表8にプロットしてみましょう。図表8の例では，資産の重要度が大または中で，脅威の大きさが大の領域内のものを，リスクが存在するとして，対応が必要であると整理しています。対応すべき範囲は，学校のIT環境により異なりますので，必要に応じて，ネットワーク管理を委託している業者や機器の導入・設定業者に確認をすることも必要です。

《図表8:リスク対応評価表の例:卒業生台帳の例》

図表5より　　図表7より

情報資産の重要度 ＼ 脅威の大きさ	小	中	大
大			**リスク対応の必要な領域** ✕学校ホームページへの個人情報掲載による漏洩 ✕教職員による意図的な漏洩 ✕ネットワーク上からのハッキングによる漏洩 ✕データの不適切な廃棄による漏洩
中	✕個人所有パソコンの盗難，紛失による漏洩 ✕メール誤送信による漏洩	✕個人認証におけるなりすましによる漏洩	
小			

2．6　情報セキュリティ・リスクリストの作成

・図表8で示したリスク対応の必要性の検討結果を元に，自校にとってのリスクを整理します。

・自校にとってのリスク整理に当たっては，図表9に示した学校内の情報セキュリティ・リスクリストの作成が有効です。

・情報セキュリティ・リスクリストでは，図表8でリスク対応が必要な領域内の脅威と守るべき情報資産を一覧表にします。この結果は恒常的なものではないので，1 学期間の運用後見直し，その後は年1回など定期的に見直すと良いでしょう。

《図表9:学校内の情報セキュリティ・リスクリストの例》

	守るべき情報資産 ＼ 情報セキュリティ脅威名	学籍関連		
		卒業生台帳	同窓会名簿	出席簿
個人情報漏洩関連	学校ホームページへの掲載による漏洩	リスク有		
	教職員による意図的な漏洩	リスク有		リスク有
	ネットワーク上からのハッキングによる漏洩	リスク有		リスク有
	データの不適切な廃棄による漏洩	リスク有		リスク有
	個人認証におけるなりすましによる漏洩		リスク有	

STEP3：リスク対応策を考えましょう！

情報セキュリティ・リスクリストの作成のあとはそれぞれのリスクに応じたリスク対応策を検討することになります。

リスク対応策とは？

・リスク対応策とは，リスクが実際のトラブルとして顕在化しないように防ぐ施策を言います。

・リスク対応策には，情報資産を扱うにあたって教員が守るべきルールなどの運用面での対策と，ウイルス対策など業務で使用するパソコンやネットワークなどの機器に対する環境面での対策の二つがあります。

・教育委員会や学校ごとの事情も踏まえて，運用面と環境面を組み合わせながらリスク対応策を作成します。

リスク対応策の実効性にはレベルがある

・一般的に対応策の実効性にもレベルが存在します。対応策の裏づけ（前提条件）が希薄であると対応策が無意味になる可能性があります。

・例えば教員個人が所有しているパソコンの校内ネットワーク接続や情報の持ち出しを認めるか否かは，学校の事情により異なります。

・現状を踏まえつつ，出来る限り対応策の実効性を上げる努力をする必要があります。

3.1　リスク対応策を検討してみましょう

・STEP ２．６で作成した情報セキュリティ・リスクリストから，対応が必要なリスクに対して，対応方針を決定します。

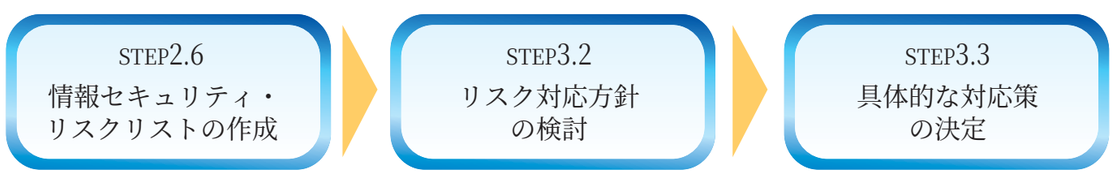
・対応の方針が決まった段階で，具体的な対応策の検討に入ります。この段階では具体的なネットワーク構成などを意識しながら対応策を決定します。

ITに詳しい教員や管理職を交えて検討してみましょう

・検討にはＩＴに関する知見があって関心のある教員を巻き込むのが望ましいでしょう。また，学校内の業務に精通した管理職又は管理職経験者を加える必要があります。

・検討の中では，必要に応じて教育委員会（または教育庁）の情報関連セクションとの意見交換を行いましょう。策定する対応策が全体の対応策と不整合を起こす可能性があります。

≪図表10:リスク対応方策の検討ステップ≫



3.2　リスク対応方針の検討

・STEP ２．６で作成した図表９の学校内の情報セキュリティ・リスクリストから，対応の必要なリスクに対して，運用面と環境面の両方から対応方針を検討します。一つのリスクに対し，運用面の対応が必要なもの，環境面の対応が必要なもの，両方の対応が必要なものがあります。

3.3　具体的な対応策の決定

・STEP ３．２のリスク対応方針の検討に基づき，具体的な対応策を検討します。図表１１にリスク対応策例を示しますので参考にしてください。

≪図表11:リスク対応策例≫

個人情報保護関連	情報消失関連
●情報の持ち出しに対する管理者の許可制度導入 ●情報の持ち出し･返却の記録義務化 ●パソコンの利用制限の設定 ●ハードディスクやフロッピーの物理的破壊または完全消去 ソフトによる情報の抹消 ●外部業者との個人情報保護義務を課した契約締結 ●ホームページの情報改ざん対策の実施 ●パスワードの発行	●重要データ･ソフトウェアのバックアップ
業務停止関連	**情報モラル関連**
●ウイルス対応ソフトのインストール ●ネットワーク管理者と管理策の明確化	●著作権に関する運用ルールの策定 ●電子メール使用ルールの策定 ●パスワードの適正管理のためのルール策定 ●サイトへのアクセス制限の実施

・自校のリスク対応策を，図表１２に示した「リスク対応策検討シートの例」を参考に作成しましょう。ここでは脅威の内容を軸としてリスク整理を行っています。情報資産やリスクごとに対応策は複数想定されるので，教育委員会や学校毎の事情を踏まえて選択していく必要があります。

・以下に示した対応策例以外にも，自分達で考えつくものを議論してみましょう。

≪図表12:リスク対応策検討シートの例≫

	リスク名	採用するリスク対応策	採用の理由
個人情報保護関連	学校ホームページへの個人情報掲載による漏洩	掲載可能な情報の明確化	ホームページの活用とセキュリティを両立させるため
	教職員による意図的な漏洩	懲戒処分の決定	処分の明確化による抑止
	ネットワーク上からのハッキングによる漏洩	管理者の設置と管理策の策定	ハッキング防止の必要性
	データの不適切な廃棄による漏洩	廃棄手順の明確化と廃棄業者との契約見直し	手順の明確化によるリスク回避
	個人認証におけるなりすましによる漏洩		

セキュリティポリシーへの反映を意識してリスク毎の対応策を明確にすると共に，各対策を採用した理由も明確にする必要があります！

STEP4:ポリシーを作成しましょう！

さて，ここでは，いよいよセキュリティポリシーの作成段階に入ります。

4.1　セキュリティポリシーを作成してみましょう

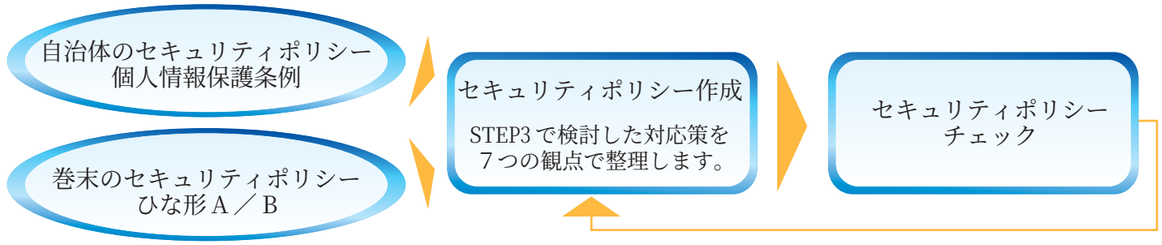
・STEP 3までで検討してきた“リスク”への“対応方策”をとりまとめ，自分たちの学校の「セキュリティポリシー」として整理しましょう。
・既存のポリシーや県・市のポリシーとの整合性確認も必要です。
・整理にあたっては，以下の７つの観点で整理するのが適切です。

①組織体制　④ハードウェアや環境のセキュリティ　⑦法令の遵守
②情報資産　⑤ネットワークやソフトウェアの運用管理
③教職員のセキュリティ　⑥アクセスの制御

※セキュリティポリシーの一つの「ひな形」として，巻末に標準的な学校において教職員が策定・遵守すべきポリシー案を整理しましたので，参考にしてください。

4.2　セキュリティポリシーチェックをしてみましょう

自治体のポリシー，個人情報保護条例との整合性が必要です。



ひな形Aは学校に必要な項目をほぼ網羅しています。ひな形Bは最低限必要な項目を整理しています。

作成したセキュリティポリシーを下のリストを使ってチェックしましょう。
チェックがつかなかった項目は，自校で対策が必要か再検討しましょう。

＜セキュリティポリシ ーのチェックシート＞

①組織体制
□学校内に，校長を責任者とする「情報セキュリティ委員会」が設置されている。
□セキュリティの事件・事故が発生した場合に，適切な処置が素早く取られるように，教育委員会や，情報サービスの提供事業者，通信事業者などとの連絡体制が構築されている。

②情報資産
□学校内の情報資産を洗い出し，情報資産目録が作成されている。情報資産目録には，それぞれの情報資産の現在の所在場所，管理責任者が明示されている
□学校内の情報を分類し，重要度に応じたラベル付けがされている。重要性については，定期的に見直されている。

③教職員のセキュリティ
□セキュリティ確保のための各教職員の役割・責任が定められ，“職務規程”にも取り入れられている。
□外部利用者（臨時職員や請負業者などを含む）が，学校内のパソコンやサーバにアクセスできないようにしている。どうしてもアクセスすることが必要な場合には，その者が十分に信用できる人物かを見極めた上で校長がアクセスを許可している。
□学校内でセキュリティに影響を及ぼす事件・事故が起こった場合や，ソフトウェアの誤動作が発生した場合には，校長を通じて，できるだけ速やかに教育委員会に報告している。
□事件・事故や誤動作が発生した場合には，担当者が，その状況を書面又は電子データにて記録するともに，類似の事件・事故の再発につながらないよう，学校内でその情報を確実に共有している。
□学校のセキュリティルールに違反した教職員には懲戒処分などの手続がとられるルールになっている。

④ハードウェアや環境のセキュリティ
□コンピュータや周辺機器は，破壊されたり認められないアクセスがなされたりすることのないよう設置し，管理されている。
□重要情報が外部に漏洩しないよう，取扱に注意を要するハードディスクやフロッピーディスクなどは，各教職員が，物理的に破壊するか，又は確実に上書きをしてデータを消去している。
□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してはならないルールとなっている。

⑤ネットワークやソフトウェアの運用管理
□セキュリティ確保のための操作手順が，正式な文書として作成され，遵守されている。
□コンピュータやサーバ，周辺機器，ネットワークなどの設備及びシステムの変更については，担当者が文書化して確実に管理されている。
□迅速，効果的，かつ，整然とした対処を確実に行えるよう，セキュリティ事件・事故管理の責任及び手順が確立されている。

⑤ネットワークやソフトウェアの運用管理(続き)
□外部の請負業者が事業所内でデータを損傷・喪失するといったリスクを回避するよう，請負業者と適切な管理策を同意し，契約に組み入れられている。
□新しい情報システムの導入や更改にあたっての受入れの基準が確立され，受入れ前に適切な試験が実施されている。
□悪意のあるソフトウェアの侵入を防止し，検出するために，対応ソフトのインストールなど，予防の措置が行われている。
□極めて重要なデータやソフトウェアのバックアップは，各教職員が定期的に実施している。
□ネットワークの管理者（＝情報担当教職員）は，管理策を定め，ネットワークにおけるデータのセキュリティ確保や，無認可のアクセスからの保護を確実に行っている。
□フロッピーディスクやUSBメモリなど取り外し可能なメディアや，印刷された文書の管理手順が作成されている。
□システムに関する文書を保護するための管理策が策定されている。
□電子メールの明確な利用ルールが作成されている。
□ホームページなどを通じて情報を公開している場合，その情報が改竄されないよう，防止方策が定められている。

⑥アクセスの制御
□各教職員が，「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っている。
□ネットワークの管理者は，ファイルサーバなどの無人運転の装置が，不正に利用されないような保護対策を確実に行っている。
□学校内のコンピュータからは，使用することが特別に認可されたネットワークサービスへのみ，アクセスできる環境が設定されている。
□学校内のネットワークについては，教員用と児童・生徒用など，ネットワーク領域が分割され，ネットワークごとにそれぞれの管理策が作成されている。
□学校の教職員は，各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なっている。
□各教職員が，ノート型パソコンや携帯電話など，移動型の機器を用いるときには，「無人の状態で放置せず引き出しに入れて施錠する」「最新のウイルスワクチンを導入する」など，業務情報のセキュリティが危険にさらされないような防御策が確実に実行されている。

⑦法令の遵守
□ソフトウェア製品などの著作権を遵守するため，「ルールの策定・公表」「財産登録簿の維持管理」「ルール違反をした教職員に対して懲戒措置をとる意志通知」などの管理策が策定されている。
□全教職員が，個人情報保護条例をよく理解し，遵守している。

STEP5　：実際に運用してみましょう！

最後に，作成したセキュリティポリシーを実際に運用して，その結果をセキュリティポリシーの見直し･改善につなげることが重要となります。

配付時の工夫

5．1　「実施手順書」の作成を

・作成したセキュリティポリシーをベースに，見やすさ・わかりやすさを重視した「実施手順書」を作成しましょう。実施手順書は，セキュリティポリシーを実施する際に，具体的に何をどのように実施するかを示したもので，作業手順書やチェックシートなどの各書式，ファイルへのパスワード設定の仕方など具体的な操作を含む「操作説明書」などが含まれます。
（操作説明書の例は次ページ：「今すぐできる情報セキュリティ向上対策」を参照してください）

教職員に配付する際には，いつでも参照できる工夫を

・セキュリティポリシー全体は，管理職（校長・教頭（副校長））と情報担当の教員，事務職員がいつでも参照できるように，ファイルに綴じるなどして持っているようにしましょう。しまい込まれ，どこにしまったのか分からなくなるようでは意味がありません。そこで，以下のような工夫も考えてみましょう。

①厚手のA３（もしくはB４）裏表印刷をして，他の書類と区別しやすくする。

②ラミネートでコーティングし，つるすためのひもを付けて，パソコンや机の横にぶら下げたり，本棚に差し込んでおいたりできるようにする。

③職務規程や年間行事計画などを１冊の「年間運営計画」に製本している地域・学校では，その中に綴じ込み，いつでも参照できるようにする。

5．2　配付と同時に実技研修を含む研修会を実施する

・セキュリティポリシーは専門用語も多く，一般の教職員には何をどうしていいか分からないということが考えられます。そこで，セキュリティポリシーの各条項がなぜ必要なのかの説明に加え，「操作説明書」などを使い，具体的な操作を含む研修会を実施すると，より実効性を確保できます。

・その際，一般の教職員からの質問を受け，内容について十分納得，理解してもらえるようにしましょう。

同意書の提出を求めることが，意識を高めるために非常に重要

・ただ，配付するだけでは，一般の職員会議の文書と同じ扱いを受けてしまいます。そこで，職務規程に準ずる重要なもので，「自分に責任がある」ということを自覚してもらうために，署名・捺印した同意書を提出してもらうようにしましょう。

・同意しない教職員には，校長・教頭から理由の聴取・注意をしてもらいましょう。

運用する際の留意点

5．3　重要な情報については，定期的なチェックも

・成績や就学援助，住所録などの個人情報の管理や，ウイルス対策などの重要事項については，情報セキュリティ委員会などで年１回など，定期的にチェックを行い，問題点の把握，改善に努めましょう。

5．4　事故発生時に素早く報告できる雰囲気と体制作りを

・万が一事故が発生した場合，責任を問われることを恐れて，事故に関する報告を行わず適切な対処もしないでいることが，最も避けなければならないことです。そのためには，セキュリティポリシーを遵守した上での事故については，責任を問わないというようなこともあらかじめ周知しておく必要があります。また，セキュリティポリシーに違反して事故を起こした場合にも，事故を秘匿した場合には厳罰に処し，速やかに報告・対処した場合には，その対応を考慮するなど，素早い報告・相談をしやすい雰囲気を作っておくことも重要です。さらに事故発生時の報告・相談の窓口や，報告手順，対応組織・対応マニュアルなど，体制作りもしておくと安心です。

見直し･改善

5．5　定期的に見直し，改善を（セキュリティポリシー運用のサイクル化）

・セキュリティポリシーの同意を求めた際や運用していく中で，問題点を指摘する教職員がいる場合はその意見や理由を現場の声として収集します。また，実際に運用する中で発生した問題も把握します。収集した情報をもとに，現在運用しているセキュリティポリシーが妥当かどうかを見直し，変更が必要な場合は，改善します。さらに，組織の変更や法令の改正などによっても，変更が必要になることもあります。その後，改訂した新しいセキュリティポリシーを配付し，再度同意を求め，運用していきます。このようなセキュリティポリシー運用のサイクル化が，より実効性があり適切なセキュリティポリシーを策定していくために必要です。

・ただ押し付けるだけでは，「同意はするが規定を守らない」という教職員を増やしてしまうことにつながります。それを防ぐためにも，教職員の意見を柔軟に聞きつつ，しっかりとした理念をもって，どれを反映させ，どれを却下するかを判断しましょう。

最初は早めに見直し，その後は年１回程度

・最初は，様々な問題を内包している可能性が高いため，１学期間運用してみて，一旦見直しをかけるといいでしょう。その後は，年１回など定期的に見直ししていくと負担もかかりません。

・転入してきた教職員が事故を起こす事例が非常に増えています。そこで，初年度と同様の研修を，転入者を対象に，年度当初，転入時に行うことも重要です。

その際，一般の教職員からの質問を受け，内容について十分納得，理解してもらえるようにしましょう。

参考:今すぐできる情報セキュリティ向上対策

パスワード設定･暗号化で盗難･紛失に備える

最近非常に増えている車上荒らしによるパソコンの盗難や，ＵＳＢメモリの紛失。成績や住所録などの個人情報などが入っていても，パスワードの設定やデータの暗号化をしておけば，盗み見されたり，流出したりする可能性を低くすることが出来ます。そこで，以下の設定を必ず行うように

■学校のパソコンはもちろん，個人所有のパソコンにもパスワード設定を

・他人による利用や，盗み見防止のために，学校の教育用パソコンや事務用パソコンすべてにパスワードを設定しましょう。

・個人所有パソコンにも，以下の方法で必ず起動時のパスワード設定をしましょう。以下はWindows の例です。

● Windows2000 の場合

①「スタート」ボタンをクリックし，「設定」メニューから「コントロールパネル」を選択します。
②表示されたアイコンの中の「ユーザとパスワード」をクリックし，必要な設定を行います。

● WindowsXP の場合

①「スタート」ボタンをクリックし，「設定」メニューから「コントロールパネル」を選択します。
②表示されたアイコンの中の「ユーザアカウント」をクリックし，必要な設定を行います。

■個人情報･重要情報ファイルにも，パスワード設定を

・成績や住所録などの個人情報，その他の部外秘の重要情報には，ファイルの一つ一つにパスワードを設定するようにしましょう。これにより，万が一パソコン本体を盗まれたり，ＵＳＢメモリを紛失したりしても，盗み見することが困難になります。以下に，具体例を示します。

●一太郎２００４ファイルの場合

①「ファイル」メニューの「名前を付けて保存」を選択します。
②ファイル名を入力し，文書を保存するドライブ･フォルダ，保存形式を選択します。
③「詳細」をクリックします。
④「パスワード設定」をクリックし，パスワードを入力します。
⑤「ＯＫ」をクリックし，名前を付けて保存ダイアログボックスに戻ります。
⑥「ＯＫ」をクリックすると，確認パスワードダイアログボックスが表示されます。
⑦「確認パスワード」に，設定したパスワードをもう一度入力します。
⑧「ＯＫ」をクリックします。

●Word２００３ファイルの場合

①「ファイル」メニューの「名前を付けて保存」を選択します。
②「ファイル名をつけて保存」ダイアログボックスで，「ツール」メニューの「セキュリティオプション」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「保存」をクリックします。

■ファイル･フォルダの暗号化を（Windows XPの場合）

①暗号化するファイルまたはフォルダを右クリックし，「プロパティ」 をクリックします。

②「全般」タブで，「詳細設定」をクリックします。
③「内容を暗号化してデータをセキュリティで保護する」チェックボックスをオンにし

ウイルス対策ソフトの導入と基本ソフトのアップデートを

■すべてのパソコンにウイルス対策ソフトを導入し，アップデートを頻繁に

・学校のパソコンはもちろん，個人所有のパソコンにも必ずウイルス対策ソフトを導入するようにしましょう。万が一ウイルスに感染すると，パソコン内のデータが消失したりするだけでなく，学校や市町村の教育用ネットワークを停止させたり，それにつながるパソコンに次々とウイルスを広げたりすることがあります。また，最近では，パソコン内の情報をインターネット上に流出させるウイルス，スパイウェアもありますので，大変危険です。

・ウイルス対策ソフトを導入していても，最新版にアップデートしていなければ，新しいウイルスやスパイウェアに対応できませんので，頻繁にアップデートを行いましょう。

・無料で利用できるウイルス対策ソフトもありますので，使用許諾条件などに十分注意すれば利用することができます。

■基本ソフトのアップデートの定期的実行を

・Windows などの基本ソフトには，セキュリティホールと呼ばれる，安全上の欠陥がよく見つかります。そこで，Windows Update（「スタート」→「すべてのプログラム」で表示されます）などを実行して，定期的にその危険をなくすようにしましょう。また，「自動アップデート」を設定しておくと，自動的にその作業をさせることもできます。

リース返却，売却時には，データの完全消去を

■フォーマットでは消えないデータを，完全消去してから，返却･売却を

・パソコンを返却，売却する際に，「ハードディスクのフォーマットをすれば，データが消えて安心！」と思っている方も多いようですが，フォーマットでは，データは完全に消去されません。データ復元ソフトを使うと，簡単にデータを復元され，情報の流出につながります。

・そこで，パソコンの返却，売却時には，下記サイトなどからデータの完全消去ソフトを入手し（市販のものもあります），必ず個人情報・重要情報を完全に削除するようにしてください。

Eraser（英語版）…　非常に強力な消去方法を採用したソフトで，以下のサイトの画面左の「Download」からダウンロードできます。
http://www.tolvanen.com/eraser/

ファイル共有ソフト（Winnyなど）は利用しない

■ファイル共有ソフトの利用は危険がいっぱい

・近年，テレビや新聞などをにぎわせている情報流出の原因の多くが，ファイル共有ソフト（Winny など）によるもの。流出した情報は，回収不能となり，取り返しがつかなくなりますので，絶対に利用しないようにしましょう。

情報セキュリティポリシーのひな形（A）[1/3]

JIS X 5080:2002 大項目	JIS X 5080:2002 中項目	JIS X 5080:2002 小項目 詳細管理策	詳細管理策の概要（一部抜粋,又は要約）
3.セキュリティ基本方針	3.1 情報セキュリティ基本方針	3.1.1 情報セキュリティ基本方針文書	基本方針文書は，教育委員会によって承認され，適当な手段で，全教職員に公表し，通知する。
		3.1.2 見直し及び評価	基本方針には，定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者 （＝情報セキュリティ委員会の委員長） を明記する。
4.組織のセキュリティ	4.1 情報セキュリティ基盤	4.1.1 情報セキュリティ運営委員会	セキュリティを主導するための明瞭な方向付け及び教育委員会による目に見える形での支持を確実にするために，運営委員会 （＝情報セキュリティ委員会） を設置する。
		4.1.3 情報セキュリティ責任の割当て	個々の資産の保護に対する責任及び特定のセキュリティ手続の実施に対する責任を，明確に定める。
		4.1.4 情報処理設備の認可手続	新しい情報処理設備に対する教育委員会による認可手続を確立する。
		4.1.5 専門家による情報セキュリティの助言	経験を積んだ情報セキュリティの専門家 （＝教育委員会） による助言を受けることができる体制を構築する。
		4.1.6 組織間の協力	セキュリティの事件・事故の場合，適切な処置が素早く取られ，助言が得られることを確実にするために，教育委員会，情報サービス提供者及び通信事業者との適切な関係を維持する。
		4.1.7 情報セキュリティの他者によるレビュー	情報セキュリティ基本方針文書には，情報セキュリティの基本方針及び責任を記述する。 学校の行動が基本方針を適切に反映し，基本方針が実行可能及び有効であることを保証するために，情報セキュリティ基本方針の実施を監査人がレビューする。
	4.2 第三者によるアクセスのセキュリティ	4.2.1 第三者のアクセスから生じるリスクの識別	物理的アクセスと論理的アクセスを区別し，第三者へのアクセス制限を明確にする。
		4.2.2 第三者との契約書に記載するセキュリティ要求事項	正式な契約に基づいて，学校の情報処理施設への第三者アクセスに関わる取り決めを行う。
	4.3 外部委託	4.3.1 外部委託契約におけるセキュリティ要求事項	情報システム，ネットワーク，デスクトップ環境等について，外部委託を行う場合は，情報セキュリティに対する要求事項を契約に定める。
5.資産の分類及び管理	5.1 資産に対する責任	5.1.1 資産目録	情報資産目録を作成しておく。
	5.2 情報の指針	5.2.1 分類の指針	情報を分類し，重要度に応じたラベル付けを行う。 また，重要性は時間が経つと変化することにも留意する。
		5.2.2 情報のラベル付け及び取扱い	学校として体系化した情報の分類及びラベル付けについて決めておく。 次に，「a) 複製」「b) 保存」「c) 郵便，ファクシミリ及び電子メールによる伝達」「d) 移動電話，音声メール，留守番電話を含め，言葉による伝達」「e） 破棄」 に至るまで，情報が保護されるように手順も指定する。 物理的なラベル付けだけでなく，電子的データに対するラベル付けについても考慮する。
6.人的セキュリティ	6.1 職務定義及び雇用におけるセキュリティ	6.1.1 セキュリティを職責に含めること	情報セキュリティ基本方針で定義された役割・責任を，“職務規程” などの内部文書にも明記する。
		6.1.2 要員審査及びその個別方針	外部利用者 （臨時職員や請負業者等を含む） が情報処理設備にアクセスしないようにする。 また，重要情報にアクセスすることが必要な場合には，その者に対して信用調査も行う。
		6.1.3 機密保持契約	教職員は，雇用条件の一部として常に，秘密保持契約・守秘義務契約の契約書に署名する。
		6.1.4 雇用条件	雇用条件に，情報セキュリティに対する教職員の責任について明記する。
	6.2 利用者の訓練	6.2.1 情報セキュリティの教育及び訓練	学校の基本方針及び手順について，学校のすべての教職員及び関係する外部利用者を適切に教育するとともに，定期的に更新教育を行う。
	6.3 セキュリティ事件・事故及び誤動作への対処	6.3.1 セキュリティ事件・事故の報告	セキュリティに影響を及ぼす事件・事故は，適切な連絡経路をとおして，できるだけ速やかに報告する。 事件・事故の正式な報告手順を，事件・事故への対処手順とともに確立し，その報告を受けたならば直ちに取るべき措置に着手する。
		6.3.2 セキュリティの弱点の報告	システム若しくはサービスのセキュリティの弱点，又はそれらへの脅威に気づいた場合若しくは疑いをもった場合に，情報サービスの利用者に対して，注意を払い，かつ，報告するように要求する。
		6.3.3 ソフトウェアの誤動作の報告	ソフトウェア誤動作を報告する手順を確立する。 また，利用者は，疑いのあるソフトウェアの除去を認可なしに試みない。
		6.3.4 事件・事故からの学習	事件・事故及び誤動作の種類，規模並びに費用の定量化及び監視を可能とする仕組みを準備する。 また，この仕組みから得られる情報を，事件・事故の再発若しくは影響の大きい事件・事故又は誤動作を識別するために用いる。
		6.3.5 懲戒手続	学校のセキュリティ基本方針及び手順に違反した教職員に対する，正式な懲戒手続を準備する。
7.物理的及び環境的セキュリティ	7.1 セキュリティが保たれた領域	7.1.1 物理的セキュリティ境界	学校は，情報処理設備を含む領域を保護するために，いくつかのセキュリティ境界 （例：外壁，カードで制御した入口，有人の受付，等） を設置する。
		7.1.2 物理的入退管理策	認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によってセキュリティの保たれた領域を保護する。 具体的には，①訪問者の監視や立入許可の要求 （入退の日付・時刻の記録），②情報処理設備へのアクセス管理 （暗証番号付きの磁気カード等），③目に見える何らかの形状をした身分証明の着用要求，④セキュリティが保たれた領域へのアクセス権の定期的な見直し・更新，等の管理策を考慮する。
		7.1.3 オフィス，部屋及び施設のセキュリティ	セキュリティが保たれた領域の選択及び設計においては，火災，洪水，爆発，騒擾，その他の自然又は人為的災害による損害の可能性を考慮する。 具体的には，①主要な設備は一般の人のアクセスが避けられる場所に設置，②建物は目立たせずその用途を示す表示は最低限とする，③複写機・ファクシミリといった支援機能・装置は領域内の適切な場所に設置，④要員が不在のときは扉及び窓に施錠，等々の管理策を考慮する。
		7.1.4 セキュリティが保たれた領域での作業	セキュリティが保たれた領域において部外者が行う作業に関するものだけでなく，そこで作業する要員又は部外者そのものについての管理策を含める。
		7.1.5 受渡し場所の隔離	品物を受渡しする場合について管理を行い，可能ならば，認可されていないアクセスを回避するために，情報処理設備から隔離する。
	7.2 装置のセキュリティ	7.2.1 装置の設置及び保護	装置は，環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置又は保護する。
		7.2.2 電源	装置は，停電，その他の電源異常から保護する。
		7.2.3 ケーブルの配線のセキュリティ	データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は，傍受又は損傷から保護する。
		7.2.4 装置の保守	装置についての継続的な可用性及び完全性の維持を確実とするために，装置の保守を正しく実施する。
		7.2.5 事業敷地外における装置のセキュリティ	所有権に関係なく，学校の敷地外で情報処理のために装置を使用する場合は，各分掌を代表する主任 （主幹） が認可する。
		7.2.6 装置の安全な処分又は再使用	取扱に慎重を要する情報を保持する記憶装置は，標準の削除機能を用いるよりも物理的に破壊するか，又は確実に上書きする。
	7.3 その他の管理策	7.3.1 クリアデスク及びクリアスクリーンの個別方針	書類及び取り外し可能な記憶媒体に対するクリアデスク方針の適用，並びに情報処理設備に対するクリアスクリーン方針の適用を行う。
		7.3.2 資産の移動	装置，情報又はソフトウェアは指定場所から無認可では持ち出し出来ないようにする。 必要かつ適切ならば，持ち出し時及び返却時に記録を残す。
8.通信及び運用管理	8.1 運用手順及び責任	8.1.1 操作手順書	セキュリティ個別方針によって明確化した操作手順は，文書化し維持していく。 操作手順は，正式な文書として取り扱い，変更の場合は各分掌を代表する主任 （主幹） によって認可する。
		8.1.2 運用変更管理	情報処理設備及びシステムの変更について文書化して管理する。
		8.1.3 事件・事故管理手順	セキュリティ事件・事故に対して，迅速，効果的，かつ，整然とした対処を確実に行うことができるように，事件・事故管理の責任及び手順を確立する。

情報セキュリティポリシーのひな形（A）[2/3]

JIS X 5080:2002 大項目	JIS X 5080:2002 中項目	JIS X 5080:2002 小項目	詳細管理策	詳細管理策の概要（一部抜粋,又は要約）
8.通信及び運用管理	8.1 運用手順及び責任	8.1.4	職務の分離	情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために，ある種の職種若しくは責任領域の管理又は実行の分離を行う。
		8.1.5	開発施設及び運用施設の分離	開発施設，試験施設及び運用施設を分離することは，それぞれが本来もつ役割を明確に分けるうえで重要である。 ソフトウェアの開発から運用の段階への移行についての規則は，明確に定め，文書化する。
		8.1.6	外部委託による施設管理	情報処理施設を管理するために外部の請負業者を利用することは，請負業者の事業所内におけるデータの信用低下，損傷又は喪失といった，セキュリティに影響を与える可能性をもたらすこともある。 これらのリスクはあらかじめ識別し，そのうえで適切な管理策を請負業者の同意を得て契約に組み入れる。
	8.2 システムの計画作成及び受入れ	8.2.1	容量・能力の計画作成	十分な処理能力及び記憶容量が利用できることを確実にするために，容量・能力の需要を監視して，将来必要とされる容量・能力を予測する。
		8.2.2	システムの受入れ	新しい情報システム，改訂版及び更新版の受入基準を確立し，その受入れ前に適切な試験を実施する。
	8.3 悪意のあるソフトウェアからの保護	8.3.1	悪意のあるソフトウェアに対する管理策	悪意のあるソフトウェアの侵入を防止し，検出するために予防の措置を行う。
	8.4 システムの維持管理	8.4.1	情報のバックアップ	極めて重要な業務情報及びソフトウェアのバックアップは，定期的に取得する。
		8.4.2	運用の記録	運用担当者は，自分の作業の記録を継続する。
		8.4.3	障害記録	障害については報告を行い，是正措置をとる。
	8.5 ネットワークの管理	8.5.1	ネットワークの管理策	ネットワークの管理者 （＝情報担当教職員）は，ネットワークにおけるデータのセキュリティを確保するとともに，ネットワークに接続したサービスを無認可のアクセスから保護することを確実にするために，管理策を実施する。
	8.6 媒体の取扱い及びセキュリティ	8.6.1	コンピュータの取外し可能な付属媒体の管理	コンピュータの取り外し可能な附属媒体 （例えば，テープ，ディスク，カセット） 及び印刷された文書の管理手順を作成する。
		8.6.2	媒体の処分	媒体が不要となった場合は，安全，かつ，確実に処分する。 媒体の安全な処分のための，正式な手順を確立する。
		8.6.3	情報の取扱い手順	認可されていない露呈又は誤用から情報を保護するために，情報の取り扱い及び保管についての手順を確立する。
		8.6.4	システムに関する文書のセキュリティ	認可されていないアクセスからシステムに関する文書を保護するために，管理策を策定する。
	8.7 情報及びソフトウェアの交換	8.7.1	情報及びソフトウェアの交換契約	組織間の情報及びソフトウェアの交換がある場合には，正式な契約として合意を取り交わす。
		8.7.2	配送中の媒体のセキュリティ	情報は，物理的な配送の途中で，認可されていないアクセス，誤用又は改竄に対する弱点をさらすことがある。 事業所間で配送されるコンピュータ媒体を保護するために，管理策を適用する。
		8.7.3	電子商取引のセキュリティ	電子商取引をネットワーク上の多くの脅威から保護するための管理策を適用する。（例：SSL，SET 等）
		8.7.4	電子メールのセキュリティ	電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮する。 また，学校は電子メールの使用に際して明確な個別方針を作成する。
		8.7.5	電子オフィスシステムのセキュリティ	オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために，個別方針及び手引きを作成し，導入する。
		8.7.6	公開されているシステム	情報を公開している学校は，その情報の改竄によって評判が傷つくことがあるので，これを防止するために，電子的に公開した情報の完全性を保護するように注意する。
		8.7.7	情報交換のその他の方式	音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために，適切な手順及び管理策を策定する。
9.システム監査ツールの保護	9.1 システム監査ツールの保護	9.1.1	アクセス制御方針	アクセス制御についての業務上の要求事項を定義し，文書化する。 また，アクセス制御の規則を定める際には，a) 常に遵守しなければならない規則と選択的又は条件的規則とを区別，b) “明確に許可していなければ原則的に禁止する” という前提に基づいた規則設定，等々の事項に注意する。
	9.2 システム監査ツールの保護	9.2.1	利用者登録	複数の利用者をもつすべての情報システム及びサービスについて，それらへのアクセスを許可するための，正規の利用者登録及び登録削除の手続を策定する。
		9.2.2	特権管理	特権 （利用者をシステム又は業務用ソフトウェアの管理策に優先させることを可能とする複数の利用者を持つ情報システムの特質又は機能） の割当て及び使用を制限し，管理する。
		9.2.3	利用者のパスワードの管理	パスワードの割当ては，正規の管理手続によって統制する。
		9.2.4	利用者のアクセス権の見直し	データ及び情報サービスへのアクセスに対する有効な管理を維持するため，教育委員会は，利用者のアクセス権を見直す正規の手順を，定期的に実施する。
	9.3 利用者の責任	9.3.1	パスワードの使用	利用者は，パスワードの選択及び使用に際して，正しいセキュリティ慣行に従う。
		9.3.2	利用者領域にある無人運転の装置	利用者は，無人運転の装置が適切な保護対策を備えていることを確実にする。
	9.4 ネットワークのアクセス制御	9.4.1	ネットワークサービスの使用についての個別方針	利用者には，使用することが特別に認可されたネットワークサービスへの直接のアクセスだけを提供する。
		9.4.2	指定された接続経路	利用者端末からコンピュータサービスまでの経路は，管理が必要となることがあるため，通常，経路の異なる接続点において幾つかの制御を実施する。 その選択の幅を予め定めることによって，ネットワークの各点における経路設定の選択肢を制限する。
		9.4.3	外部から接続する利用者の認証	遠隔地からの利用者のアクセスには認証を行う。
		9.4.4	ノードの認証	遠隔コンピュータシステムへの接続は，認証により利用可能とする。 このことは，その接続が学校のセキュリティ管理外であるネットワークを用いる場合に，特に重要である。
		9.4.5	遠隔診断用ポートの保護	診断用ポートへのアクセスは，セキュリティを保つように制御する。
		9.4.6	ネットワークの領域分割	情報サービス，利用者及び情報システムのグループを分離するためには，ネットワークごとにそれぞれの管理策を作成する。
		9.4.7	ネットワークの接続制御	共有ネットワーク，特に，組織の境界を超えて広がっているネットワークについてのアクセス制御方針の要求事項では，利用者の接続の可能性を制限する制御策の組み込みが必要とされることもある。
		9.4.8	ネットワーク経路を指定した制御	共有ネットワーク，特に，組織の境界を超えて広がっているネットワークには，コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために，経路指定の制御策の組み込みが必要なこともある。
		9.4.9	ネットワークサービスのセキュリティ	ネットワークサービスを使用する学校は，使用するすべてのサービスのセキュリティの特質について，明確な説明を受けることを確実にする。
	9.5 オペレーティングシステムのアクセス制御	9.5.1	自動の端末識別	特定の場所及び携帯装置への接続を認証するために，自動の端末識別を行う。
		9.5.2	端末のログオン手順	情報サービスへのアクセスは，安全なログオン手続を経て達成するものとする。
		9.5.3	利用者の識別及び認証	すべての利用者は，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，各個人の利用ごとに一意な識別子 （利用者 ID） を保有するものとする。
		9.5.4	パスワード管理システム	質の良いパスワードであることを確実にするために，パスワード管理システムは有効な対話的機能を提供する。
		9.5.5	システムユーティリティの使用	システム及び業務用ソフトウェアの制御を無効にすることのできる一つ以上のユーティリティプログラムについて，それらの使用を制限し，厳しく管理する。

情報セキュリティポリシーのひな形（A）[3/3]

JIS X 5080:2002 大項目	JIS X 5080:2002 中項目	JIS X 5080:2002 小項目 詳細管理策	詳細管理策の概要（一部抜粋,又は要約）
9.システム監査ツールの保護	9.5 オペレーティングシステムのアクセス制御	9.5.7 端末のタイムアウト機能	リスクの高い場所にあるか，又はリスクの高いシステムで用いられている端末が活動停止状態にある場合，認可されていない者によるアクセスを防止するために，一定の活動停止時間の経過後，その端末は遮断されるようにする。
		9.5.8 接続時間の制約	リスクの高い業務用ソフトウェアに対しては，接続時間の制限によって，追加のセキュリティを確保する。
	9.6 業務用ソフトウェアのアクセス制御	9.6.1 情報へのアクセス制限	支援要員を含め，業務用システムの利用者は，既定のアクセス制御方針に従い，個々の業務用ソフトウェアの要求事項に基づき，また，学校の情報アクセス方針に合わせて，情報及び業務用システム機能へのアクセスを許す。
		9.6.2 取扱いに慎重を要するシステムの隔離	取扱に慎重を要するシステムには，専用の（隔離された）情報システムを設置する。
	9.7 システムアクセス及びシステム使用状況の監視	9.7.1 事象の記録	例外事項，その他のセキュリティに関連した事象を記録した監査記録を作成して，将来の調査及びアクセス制御の監視を補うために，合意された期間保存する。
		9.7.2 システム使用状況の監視	情報処理設備の使用状況を監視する手順を確立する。監視の結果は定期的に見直す。
		9.7.3 コンピュータ内の時計の同期	監査記録は，調査のために，又は法律若しくは懲戒にかかわる場合の証拠として要求されることがあるので，監査記録の正確さを保証するためにコンピュータの時計を常に正しく設定しておく。
	9.8 移動型計算処理及び遠隔作業	9.8.1 移動型計算処理	移動型計算処理（ノートPC等）の設備を用いるとき，業務情報のセキュリティが危険にさらされないような防御を確実にするために，特別な注意を払う。
		9.8.2 遠隔作業	装置及び情報の盗難，認可されていない情報の漏洩，遠隔地から学校の内部システムへの認可されていないアクセス，設備の誤用などの脅威に対して，遠隔作業の場所に適切な保護が整っている状態とする。
10.システムの開発及び保守	10.1 システムのセキュリティ要求事項	10.1.1 セキュリティ要求事項の分析及び明示	新しいシステム又は既存のシステムの改善に関する業務上の要求事項を記述した文書では，管理策についての要求事項を明記する。
	10.2 業務用システムのセキュリティ	10.2.1 入力データの妥当性確認	業務用システムに入力されるデータは，正確で適切であることを確実にするために，その妥当性を確認する。
		10.2.2 内部処理の管理	改竄を検出するために，妥当性の検査をシステムに組み込む。
		10.2.3 メッセージ認証	重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に，メッセージ認証を適用する。
		10.2.4 出力データの妥当性確認	業務用システムからの出力データについては，保存された情報の処理がシステム環境に対して正しく，適切に行われていることを確実にするために，妥当性を確認する。
	10.3 暗号による管理策	10.3.1 暗号による管理策の使用に関する個別方針	リスクアセスメント及び管理策の選択の一部として，暗号技術を用いた解決策が適切であるかどうかに関して決断を下す。
		10.3.2 暗号化	暗号化は，情報の機密性を保護するために用いることができる技術であり，取扱いに慎重を要する又は重要な情報の保護のために採用する。
		10.3.3 ディジタル署名	電子文書の真正性及び完全性を保護する手段として，ディジタル署名の活用を検討する。
		10.3.4 否認防止サービス	事象（契約など）又は動作（支払いなど）が起こったか，起こらなかったかの紛争の解決が必要である場合には，否認防止サービスを用いる。
		10.3.5 かぎ管理	暗号かぎの管理は，暗号技術の効果的な使用のために不可欠である。
	10.4 システムファイルのセキュリティ	10.4.1 運用ソフトウェアの管理	運用システムでのソフトウェアの実行を，管理する。
		10.4.2 システム試験データの保護	試験データは保護し，管理する。
		10.4.3 プログラムソースライブラリへのアクセス制御	コンピュータプログラムが破壊される危険性を軽減するために，プログラムソースライブラリへのアクセス全体にわたって，厳しい管理を維持する。
	10.5 開発及び支援過程におけるセキュリティ	10.5.1 変更管理手順	情報システムに対する破壊の危険性を最小限に抑えるために，変更の実施は厳しく管理する。
		10.5.2 オペレーティングシステムの変更の技術的レビュー	定期的にオペレーティングシステムを変更する。
		10.5.3 パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更は行わないようにする。
		10.5.4 隠れチャネル及びトロイの木馬	隠れチャネル又はトロイの木馬に対する対応策を考慮する。
		10.5.5 外部委託によるソフトウェア開発	ソフトウェア開発を外部委託する場合，外注内容の明確化，権利関係の取り決め，開発過程における進捗管理，納入物の十分な検収，確認作業を重視する。
11.事業継続管理	11.1 事業継続管理の種々の面	11.1.1 事業継続管理手続	学校全体を通じて事業継続のための活動を展開し，かつ，維持するための管理された手続を整える。
		11.1.2 事業継続及び影響分析	事業継続のための活動は，業務手続の中断を引き起こし得る事象，例えば，装置の故障，洪水及び火災を特定することから始める。その後，それらの障害の影響を判断するために，リスクマネジメントを行う。これら両活動の実施には，事業資源及び手続の管理者（＝各分掌を代表する主任）が全面的に関与する。このアセスメントは，すべての業務手続を検討するものであり，情報処理施設に限定しない。
		11.1.3 継続計画の作成及び実施	重要な業務手続の中断又は障害の後，事業運営を維持又は要求される時間内に復旧させるための計画を立てる。
		11.1.4 事業継続計画作成のための枠組み	全ての計画が整合したものになることを確実にするため，また，試験及び保守の優先順位を明確にするために，一つの事業継続計画の枠組みを維持する。
		11.1.5 事業継続計画の試験，維持及び再評価	事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために，定期的に試験する。
12.適合性	12.1 法的要求事項への適合	12.1.1 適用法令の識別	各情報システムについて，すべての関連する法令，規則及び契約上の要求事項を，明確に定め，文書化する。これらの要求事項に適合する特定の管理策，及び個々の責任も同様に明確に定め，文書化する。
		12.1.2 知的所有権（IPR）	著作権及びソフトウェアの著作権を遵守するための管理策を考慮する。
		12.1.3 組織の記録の保護	学校の重要な記録は，消失，破壊及び改竄から保護する。
		12.1.4 データの保護及び個人情報の保護	個人情報の保護について規定した，又は個人情報をデータ化している場合のそのデータの取扱について規定した法律に適合するために，適切な管理構造の下で管理・統制を行う。
		12.1.5 情報処理施設の誤用の防止	学校の情報処理施設の使用は，各分掌を代表する主任（主幹）が認可する。
		12.1.6 暗号による管理策の規制	国によっては，暗号による管理策へのアクセス又はその使用を統制するために，協定，法律，規制，又はその他の手段を実行している。
		12.1.7 証拠の収集	人又は学校に対する措置を支援するには，十分な証拠を持っていなければならない。
	12.2 セキュリティ基本方針及び技術適合のレビュー	12.2.1 セキュリティ基本方針との適合	各分掌を代表する主任（主幹）は，自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にする。さらに，学校内のすべての範囲について，セキュリティ基本方針及び標準類に適合することを確実にするために，定期的な見直しを考慮する。
		12.2.2 技術適合の検査	情報システムは，セキュリティ実行標準と適合していることを定期的に検査する。
	12.3 システム監査の考慮事項	12.3.1 システム監査管理策	監査要求事項，及び，運用システムの検査を含む監査活動は，業務手続の中断のリスクを最小限に抑えるように，慎重に計画を立て，合意する。
		12.3.2 システム監査ツールの保護	システム監査ツール，すなわち，ソフトウェア又はデータファイルへのアクセスは，誤用又は悪用を防止するために保護する。

（注）ISOの改訂にあわせ,2006年5月にJIS X 5080の改訂版である「JIS Q 27002:2006」が発行される予定だが,今回の本表は「JIS X 5080:2002」をベースに整理した。

情報セキュリティポリシーのひな形（B）［1/2］

一般教職員向け　セキュリティポリシーのひな形	JIS X 5080:2002 項番
①セキュリティ確保にあたっての組織体制	
・学校内に，校長を責任者とする「情報セキュリティ委員会」の設置を行う。 「情報セキュリティ委員会」では，以下のことを実施する。 (a) セキュリティ方針や，各教職員の責任の承認・見直し (b) 重要な情報が重大な脅威にさらされていないかの継続的監視 (c) セキュリティに関わる事件・事故の見直し・監視 (d) セキュリティを強化するための取り組みの提案・承認	4.1.1
・セキュリティの事件・事故が発生した場合に，適切な処置が素早く取られるように，教育委員会や，情報サービスの提供事業者，通信事業者などとの連絡体制を構築する。具体的には，電話連絡表の作成・掲示，定期的なコミュニケーション機会の設定などを行う。	4.1.6
②情報資産	
・情報セキュリティ委員会は，学校内の情報資産を洗い出し，情報資産目録を作成する。情報資産目録には，それぞれの情報資産の現在の所在場所，管理責任者を明示する。	5.1.1
・情報セキュリティ委員会は，学校内の情報を分類し，重要度に応じたラベル付けを行う。また，重要性については，定期的に見直す。	5.2.1
③教職員のセキュリティ	
・情報セキュリティ委員会は，セキュリティ確保のための各教職員の役割・責任をきちんと定め，“職務規程”にも取り入れる。	6.1.1
・外部利用者（臨時職員や請負業者等を含む）が，学校内のパソコンやサーバにアクセスできないようにする。どうしてもアクセスすることが必要な場合には，その者が十分に信用できる人物かを見極めた上で校長がアクセスを許可する。	6.1.2
・学校内でセキュリティに影響を及ぼす事件・事故が起こった場合や，ソフトウェアの誤動作が発生した場合には，校長を通じて，できるだけ速やかに教育委員会に報告する。ソフトウェア誤動作の場合，教育委員会又は校内の情報担当の認可を受けて，疑いのあるソフトウェアを除去する。	6.3.1
・事件・事故や誤動作が発生した場合には，担当者が，その状況を書面又は電子データにて記録するともに，次に類似の事件・事故の再発につながらないよう，学校内でその情報を確実に共有する。	6.3.4
・学校のセキュリティルールに違反した教職員には懲戒処分などの手続をとる。	6.3.5
④ハードウェアや環境のセキュリティ	
・コンピュータや周辺機器は，破壊されたり認められないアクセスがなされたりすることのないよう設置し，管理する。	7.2.1
・重要情報が外部に漏洩しないよう，取扱に注意を要するハードディスクやフロッピーディスクなどは，各教職員が，物理的に破壊するか，又は確実に上書きをしてデータを消去する。	7.2.6
・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してはならない。必要かつ適切な場合に限り，校長の許可を経て，持ち出し時及び返却時に記録を残すものとする。	7.3.2
⑤ネットワークやソフトウェアの運用管理	
・情報セキュリティ委員会は，セキュリティ確保のための操作手順を，正式な文書として作成し，遵守する。変更の場合は管理者である校長によって認可する。	8.1.1
・コンピュータやサーバ，周辺機器，ネットワーク等の設備及びシステムの変更については，担当者が文書化して確実に管理する。	8.1.2
・セキュリティ事件・事故管理の責任及び手順を確立し，迅速，効果的，かつ，整然とした対処を確実に行うことができるようにする。	8.1.3
・外部の請負業者を利用する場合，請負業者が事業所内でデータを損傷・喪失するといったリスクを回避するよう，情報セキュリティ委員会が，請負業者と適切な管理策を同意し契約に組み入れる。	8.1.6
・新しい情報システムの導入や更改にあたっては，情報セキュリティ委員会が受入れの基準を確立しておくとともに，受入れ前に適切な試験を実施する。	8.2.2

情報セキュリティポリシーのひな形（B）［2/2］

一般教職員向け　セキュリティポリシーのひな形	JIS X 5080:2002 項番
・悪意のあるソフトウェアの侵入を防止し，検出するために，情報セキュリティ委員会は，対応ソフトのインストールなど，予防の措置を行う。	8.3.1
・極めて重要なデータやソフトウェアのバックアップは，各教職員が定期的に実施する。	8.4.1
・ネットワークの管理者（＝情報担当教職員）は，管理策を定め，ネットワークにおけるデータのセキュリティ確保や，無認可のアクセスからの保護を確実に行う。	8.5.1
・情報セキュリティ委員会は，フロッピーディスクやUSBメモリなど取り外し可能なメディアや，印刷された文書の管理手順を作成する。管理手順には，廃棄のときの文書化についても必ず盛り込む。	8.6.1
・システムに関する文書を保護するために，情報セキュリティ委員会は，その管理策を策定する。	8.6.4
・情報セキュリティ委員会は，電子メールの明確な利用ルールを作成する。	8.7.4
・ホームページ等を通じて情報を公開している場合，情報セキュリティ委員会は，その情報が改竄されないよう，防止方策を定める。	8.7.6
⑥アクセスの制御	
・各教職員がパスワードの選択及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。	9.3.1
・ネットワークの管理者は，ファイルサーバ等の無人運転の装置が，不正に利用されないような保護対策を確実に行う。	9.3.2
・学校内のコンピュータからは，使用することが特別に認可されたネットワークサービスへのみ，アクセスできる環境を設定する。	9.4.1
・学校内のネットワークについては，教員用と児童・生徒用など，ネットワーク領域を分割する。また，情報セキュリティ委員会は，ネットワークごとにそれぞれの管理策を作成する。	9.4.6
・学校の教職員は，各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。	9.5.3
・各教職員が，ノート型パソコンや携帯電話など，移動型の機器を用いるときには，例えば「無人の状態で放置せず引き出しに入れて施錠する」「最新のウイルスワクチンを導入する」など，業務情報のセキュリティが危険にさらされないような防御策を確実に実行する。	9.8.1
⑦法令の遵守	
・ソフトウェア製品などの著作権を遵守するため，情報セキュリティ委員会は，「ルールの策定・公表」「財産登録簿の維持管理」「ルール違反をした教職員に対して懲戒措置をとる意志通知」などの管理策を策定する。	12.1.2
・全教職員が，個人情報保護条例をよく理解し，遵守する。（私立学校は個人情報保護法，国立大学附属学校は独立行政法人等個人情報保護法に置き換える）	12.1.4

執筆　学校情報セキュリティ委員会（敬称略，五十音順）

委員長：
藤村　裕一　鳴門教育大学

委　員：
井上　　勝　八千代松陰中学・高等学校
加藤　　敏　東京都品川区荏原第六中学校
小泉　力一　尚美学園大学
西田　光昭　千葉県柏市立土南部小学校
松方　　純　国立情報学研究所
松本　博幸　千葉県印西市立大森小学校
山崎　文明　ネットワンシステムズ株式会社
和氣　正典　東京都品川区教育委員会

オブザーバ：
大西　尊久　文部科学省
上原　　智　経済産業省
菊田　真希　経済産業省

事務局：
吉本　孝一　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
小山内 好博　財団法人コンピュータ教育開発センター
三ｒ　冨査雄　株式会社野村総合研究所
福田　隆之　株式会社野村総合研究所

学校情報セキュリティ・ハンドブック
～今日から始められるセキュリティポリシーの作り方～

平成18年3月31日発行

著作権者　経済産業省
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/