学校情報セキュリティポリシー策定・運用のための

学校情報セキュリティ・ハンドブック解説書

＜改訂版＞

財団法人 コンピュータ教育開発センター

はじめに

急速に進展する情報化社会の負の側面として，コンピュータ・ウイルスへの感染や電子データの紛失などによる個人情報流出の事件・事故が相次いでいます。学校教育の現場も例外ではなく，児童生徒の重要な情報がファイル共有ソフトから漏れたり，情報を保存したパソコンが盗まれたり，大きな事件・事故も少なくありません。

学校は，そのような情報セキュリティに関するトラブル対策として，自らが持っている情報資産には何があるかを把握し，同時に，それら情報資産に対する脅威にどう備えるかも整理しておく必要があります。そして「学校情報セキュリティポリシー」にまとめて策定，実行していかなければならないでしょう。

財団法人コンピュータ教育開発センター（CEC）では，学校教育の現場における情報セキュリティの意識向上を図り，各学校が実効性のあるセキュリティポリシーを自ら策定できるようにするための施策を推進しています。平成17年度には，ポリシーの策定・運用までの手順を詳しく解説した『学校情報セキュリティ・ハンドブック』を発行しました。また，その後，全国の教育委員会や学校が『ハンドブック』を活用して，実際に情報セキュリティポリシーの策定・運用を試みる取り組みも行いました。そして，その取り組みの結果や『ハンドブック』への要望などを反映し，CECでは平成18年度に『学校情報セキュリティ・ハンドブック改訂版』をまとめています。

ここでは，第１章で『学校情報セキュリティ・ハンドブック改訂版』の内容を解説し，また第２章では，『ハンドブック』を活用して具体的な情報セキュリティポリシーの策定と運用を試みた教育委員会や学校からの現場報告をまとめていきます。さらに第３章では，教育委員会や学校が策定した情報セキュリティポリシーの例を掲載しています。教育現場における情報セキュリティ対策の向上に，ここで紹介する内容が一助となれば幸いです。

平成２０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

はじめに 1

第１章

『学校情報セキュリティ・ハンドブック改訂版』の解説 3

１．１　「学校情報セキュリティポリシー」の策定・運用に向けて 4

１．２　５段階の「学校情報セキュリティポリシー」策定手順 6

参考資料　学校情報セキュリティポリシーの「ひな形」 37

第２章

『学校情報セキュリティポリシー策定』取り組み事例 44

２．１　Ａ県教育委員会での取り組み事例 45

２．２　Ｂ県教育委員会での取り組み事例 52

２．３　Ｃ県教育委員会での取り組み事例 64

第３章

『学校情報セキュリティポリシー』例 69

３．１　セキュリティポリシー例（１）：基本方針・対策基準

３．２　セキュリティポリシー例（２）：対策基準

３．３　セキュリティポリシー例（３）：対策基準

３．４　セキュリティポリシー例（４）：対策基準

３．５　セキュリティポリシー例（５）：実施手順

３．６　セキュリティポリシー例（６）：基本方針・対策基準・実施手順

３．７　セキュリティポリシー例（７）：基本方針・対策基準

第１章

『学校情報セキュリティ・ハンドブック改訂版』の解説

１．１　「学校情報セキュリティポリシー」の策定・運用に向けて

１．２　５段階の「セキュリティポリシー」策定手順

１．１　「学校情報セキュリティポリシー」の策定・運用に向けて

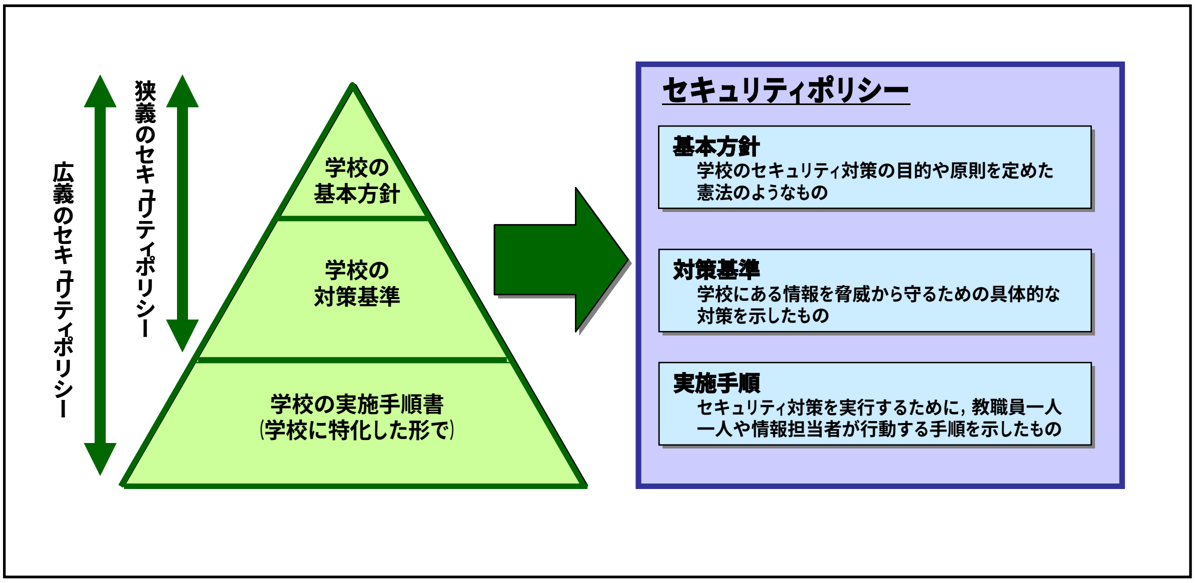
１．１．１　「情報セキュリティポリシー」とは

「情報セキュリティ」に関するさまざまなトラブルが，毎日のように新聞やテレビに取り上げられています。コンピュータ・ウイルスやパソコンの紛失・盗難などによる個人情報の流出トラブルは社会現象の一つといっても過言ではない状況ですが，最近では情報セキュリティの重要性が認識されるようにもなり，企業や自治体などで「情報セキュリティポリシー」の策定・運用に取り組む動きが出てきました。

情報セキュリティポリシーとは，組織の情報セキュリティに関する統一方針を示した文書であり，情報セキュリティを維持するためのさまざまな取り組みについて，包括的に規定された文書のことを言います。

一般的に，セキュリティポリシーは，「基本方針」「対策基準」「実施手順」の３階層の文書から構成されます。「基本方針」「対策基準」の２階層を狭義のセキュリティポリシー，「実施手順」を含めた３階層を広義のセキュリティポリシーと呼ぶこともあります。図表１．１　に，情報セキュリティポリシー文書体系を示します。

図表１．１　情報セキュリティポリシーの範囲



これらの３階層の文書の違いは，承認レベルや管理部門，または記述内容の具体性の違いによるものです。

記述内容の違いについて言えば,「基本方針」で定められた内容が，下位の「対策基準」「実施手順」の文書で具現化されることになります。また，承認レベルや管理部門の違いについて言うと,「基本方針」「対策基準」は組織の最終的な意思決定者である経営者レベルで承認されて，その管理を情報セキュリティの全社的な組織であるセキュリティ委員会などが担うケースが多く見られます。一方,「実施手順」は情報システムごと，あるいは部門ごとに作成・管理されるケースが多く，各部門の部門長が承認者となるのが一般的です。

１．１．２　『学校情報セキュリティ・ハンドブック』の発行・改訂へ

教育現場でも児童・生徒の個人情報が流出するなどのトラブルが頻発しており，上記のような情報セキュリティポリシーの策定・運用の重要性を指摘する声が増えています。しかし，ひとくちに情報セキュリティポリシーと言っても，企業のポリシーと学校のポリシーが全く同じというわけではありません。学校は，学校の特性に応じた情報セキュリティを前提として，ポリシーの策定・運用に取り組む必要があります。

財団法人コンピュータ教育開発センター（ＣＥＣ）は，平成１７年度に経済産業省から委託を受け,, 学校における情報セキュリティ対策とポリシー策定を支援する『学校情報セキュリティ・ハンドブック』を発行しました。学校にはどのような情報資産があるのか，それらに対する脅威には何があるかを分析し，そのセキュリティ対策をどうしたらいいか，わかりやすく整理しました。そのうえで，学校に相応しい「学校情報セキュリティポリシー」を策定・運用していく具体的な手順を示しました。

実際，この『学校情報セキュリティ・ハンドブック』を活用してポリシーの策定・運用に取り組んだ教育現場も多く,「セキュリティポリシーの文書体系の説明も掲載してほしい」などと，ハンドブックに対するご意見も寄せられています。

こうした利用者の方々のご意見やご要望を反映して，ＣＥＣでは平成１８年度に『学校情報セキュリティ・ハンドブック改訂版』を発行しています。平成１７年度版に比べて，できるだけポリシー策定の手順を簡易にし，また具体例も多く掲載して，学校が情報セキュリティポリシーの策定・運用に取り組みやすい内容に改訂しました。

『学校情報セキュリティ・ハンドブック改訂版』でも「基本方針」「対策基準」「実施手順」の３階層についてのセキュリティポリシー策定の方法を示しています。では，次から，学校情報セキュリティポリシーを策定する手順について,『ハンドブック改訂版』の内容をもとに，解説していきます。

１．２　５段階の「学校情報セキュリティポリシー」策定手順

１．２．１　【**STEP１**】から【**STEP５**】へと作業を進める

「学校情報セキュリティポリシー」を策定・運用するためには，具体的にどう作業を進めていけばいいでしょうか。『学校情報セキュリティ・ハンドブック改訂版』では，以下の５段階の手順を示しています。

- STEP１　問題意識の共有
- STEP２　情報資産の洗い出し
- STEP３　リスク対応策の検討
- STEP４　セキュリティポリシー作成
- STEP５　セキュリティポリシー運用

それぞれのSTEPのアウトプットは，次のSTEPのインプットにつながっていますから，全体の流れを意識しながら作業を進めていくことが大事です。

１．２．２　【**STEP１**】――学校内での「**問題意識**」の共有

情報セキュリティポリシー策定に向けた【STEP１】として「学校現場での問題意識の共有を行うこと」が重要となります。とはいえ，これはそう簡単なことではありません。すべての教職員の間で情報セキュリティの問題意識を共有するためには，学校内での体制整備が必要になり，また，最新のトラブル事例を常にアナウンスしたりして，危機感を共有しておくことも必要になります。また，【STEP１】では，セキュリティポリシー策定に向けた組織作りと実施計画作りも行います。以下に，いくつかポイントをまとめました。

（１）体制整備を工夫する

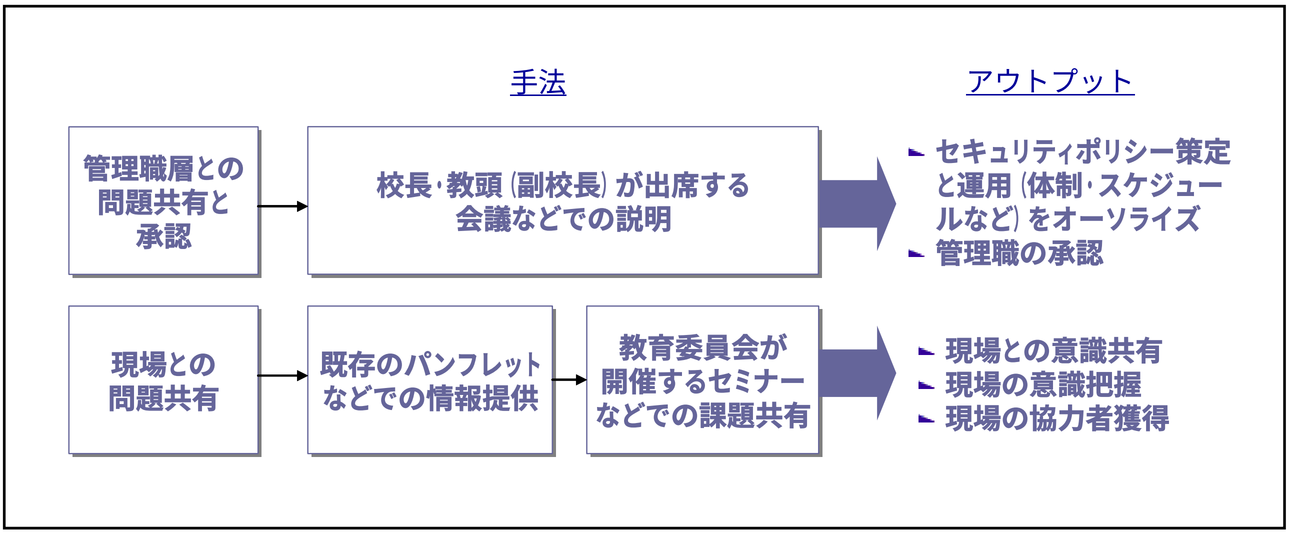
セキュリティポリシー策定に向けた組織作りでは，学校長などの管理職層及び学校現場での教職員を巻き込んでいくことが大事です。管理職層を巻き込む具体的な手法としては，校長会や教頭会など，校長や教頭（副校長）が出席する会議などでの説明が有効でしょう。また，現場の教職員を巻き込む手法としては，まずパンフレットなどで情報を共有し，その後，学校内でセミナーなどを開催すると有効です（次ページの図参照）。

最終的には学校独自でのポリシー策定と運用を目指していますが，所属する自治体の既存ポリシーや教育委員会が用意しているポリシーなどとの整合性が求められるため，教育委員会との連携による体制作りが現実的です。

ネットワークシステムの整備状況やＩＴ機器の整備・運用の形態の違いに左右される項目も多いため，教育委員会が中心になり学校の代表を含めたセキュリティポリシー策定委員会などを設置して実施するケースが多いようです。

その地域に大学がある場合，有識者として大学教授を委員に含める（または委員長になってもらう）と，共有知識も広がり活動もスムースに運びます。

図表１．２　ＳＴＥＰ１の手法とアウトプット



（２）実施スケジュールの確認

セキュリティポリシー策定委員会等を設置するなど体制整備を行った後は，具体的にいつまでに検討を進め，ポリシーを策定するのか，またいつから運用を開始するのか，実施スケジュールを確認することが必要です。

現在も学校現場に存在するリスクを回避するために，極力早めの対応を行うことが望ましいと言えるでしょう。

（３）最新事例を整理する

管理職層や現場の教職員の危機感を醸成するためには，他の地域で実際に起こった情報セキュリティに関するトラブル事例を整理して，共有することが最適でしょう。そうした他地域でのトラブル事例については，新聞記事やインターネット上の情報を検索するなどして，整理することができます。新聞記事などの主な検索サービスには，以下のような例があります。

日経テレコン 21(*)

http://telecom21.nikkei.co.jp/nt21/service/

Yahoo! JAPAN　新聞記事横断検索(*)

http://gsearch.news.yahoo.co.jp/gs?ty=g/

朝日新聞「聞蔵」(*)

http://www.asahi.com/information/db/index.html

警察庁　サイバー犯罪対策

http://www.npa.go.jp/cyber/

情報セキュリティ広場

http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku1.htm

Security NEXT

http://www.security-next.com/

INTERNET Watch

http://internet.watch.impress.co.jp/

独立行政法人情報処理推進機構　セキュリティセンター

http://www.ipa.go.jp/security/index.html

ニュース CNET Japan

http://japan.cnet.com/news/

*印のついたサイトは有料サービスで，記事を検索する場合は事前に手続きが必要です。

なお，これらを情報源として書類を作成・配布するときは，著作権法により情報の出所を明記する必要があります。

ｈｉｎｔ！

- 次 STEP 以降で，何をやるのかを確認しあう意味でも，委員会メンバーによる“ワークショップ”が有効です。
- ワークショップの事例概要は，ＣＥＣホームページ（http://www.cec.or.jp/CEC/）でも紹介しています。
- ワークショップの方法としては，参加者を４～６人程度のグループに分割し，グループ討論及び討論内容の発表を中心に，進めるのが有効です。
  ポリシー作成をグループ討論の中で進めるのは時間的に困難なので，ワークショップとしてはリスク対応策までに止め，ポリシー作成の考え方は講義の中で説明すると良いでしょう。

以下に，ワークショップの進行例を示します。発表時間は，グループ数によって違ってきますが，各グループの発表時間を２分程度とし，５グループを想定しています。

【　進行例　】

１３：００－１３：２０　①講義
１３：２０－１３：３０　②グループ分け及び自己紹介
１３：３０－１３：４０　③トラブル事例について
１３：４０－１４：０５　④学校の情報資産について
１４：０５－１４：２０　休憩
１４：２０－１４：５０　⑤脅威について
１４：５０－１５：１０　⑥リスクの評価について
１５：１０－１５：３０　⑦リスク対応策について
１５：３０－１６：００　⑧まとめ

【　ワークショップ内容例　】

①講義（２０分）

・「学校情報セキュリティ・ハンドブック」をテキストとして，セキュリティポリシー策定までの手順を説明します。

・ワークショップの進め方を説明します。

②グループ分け及び自己紹介（１０分）

・１グループ４～６人程度に分割します。
グループ内は，できるだけ同じ校種の人を集めると，後の討論をスムースに進めることができます。

・グループ内で自己紹介します。

・進行役，発表者を決めます。

③トラブル事例について（１０分）

・自校の情報トラブルをお互いに紹介することにより，問題意識を共有します。

④学校の情報資産について（２５分）

・各自に自校の情報資産をリストアップしてもらいます。（５分）

・グループ内討論を通して，グループとして情報資産のリストを作成し，資産の重要度の評価をします。（１０分）

・各グループが作成した情報資産リストを発表します。（１０分）

⑤脅威について（３０分）

・各自に，重要度の高い情報資産がさらされている脅威を洗い出してもらいます。（１０分）

・グループ内討論を通して，各自が洗い出した脅威をグループとしてまとめます。そのなかから，２つ程度の代表的な脅威を選定します。（１０分）

・各グループが選定した２つ程度の代表的な脅威について発表します。（１０分）

⑥リスクの評価について（２０分）

・グループ内討論を通して，選定した２つ程度の脅威それぞれについて，リスクのリスクの評価をします。（１０分）

・各グループがまとめたリスクの評価結果を発表します。（１０分）

⑦リスク対応策について（２０分）

・グループ内討論を通して，選定した２つ程度の脅威それぞれについて考えられる対応策案をリストアップし，その中で採用すべき対応策とその理由をまとめます。（１０分）

・各グループがまとめた対応策案を発表します。（１０分）

⑧まとめ（３０分）

・これまでのグループ討論を踏まえ，リスク対応策作成までの手順を再整理します。

・ポリシー策定の考え方を説明します。

・セキュリティポリシー運用について説明します。

１．２．３　【STEP２】——情報資産の洗い出しと重要性の評価

（１）情報資産とは

セキュリティポリシー策定委員会等が発足し，問題意識の共有が進むと，次の【STEP２】では，学校における情報資産の洗い出しと重要性の評価を行います。

情報資産とは，組織・団体にとって価値を有する情報そのものと，その情報を可用化（availability）する環境を指します。例えば企業では，企画，製品開発や営業の情報，顧客情報，知的財産などのデータベース，資料などが情報そのものであり，その情報を可用化する環境とは，ソフト面におけるアプリケーション，システムソフトウエア，ユーティリティや，ハード面におけるコンピュータ装置，通信装置，メディアなどを指します。

（２）情報資産の洗い出し

では，学校にはどのような情報資産があるでしょうか。上記の「情報を可用化する環境」は既に財産として管理されている場合がほとんどでしょう。ここでは学校にとって価値を有する情報そのものを，例えば図表１．３に示すように，「学籍関連」「生徒指導関連」「成績関連」「進路関連」「保健関連」「事務関連」などの観点から洗い出すのが望ましいと思います。

図表１．３　学校の情報資産洗い出し項目例

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

こうした学校の情報資産の洗い出しの作業は，セキュリティ策定委員会だけでは行えません。分掌や組織の役割などに沿って全員で取り組む工夫が必要です。実作業に際しては，例えば次ページに掲載したフォーマットを利用すると，効率よく進められるでしょう。

また既に管理文書一覧などが出来上がっている場合には，それを見直すなどの方法でも良いと思われます。学校規模にもよりますが，事例実績からみると１～２週間程度の工程を見込んでおくのが良いと思われます。

図表1．4　学校内の情報資産管理

情報資産		管理者	作成者	保存形態	公開の有無	公開の範囲	主な記載内容	重要度
種別	名称	分掌名･役職等		記録メディア 紙(手書，プリント)，CD，ＦＤ等	有 ○ 無 空欄	対象を記載 一般，校内，職員，等	資産内の項目名等	校内における重要度(大･中･小) 保存義務，他への影響等から評価
成績関連								

ｈｉｎｔ！

情報資産の洗い出しに際して，対象範囲をどうするかが疑問として投げかけられます。電子媒体も紙媒体も作業途中のデータも全てを対象にして整理するのが望ましいと思われます。これは困難ながら，そういうプロセスを全員参加で行うことによって情報セキュリティに対する意識向上を図れるとともに，自校の情報を全て整理できるという意味でも重要です。但し，相当な量になりますので，スケジュールや体力に合わせて，例えば電子媒体に限るというのも一つの方法です。

（３）重要度の評価

情報資産の重要度は，その情報が外部に漏れた場合や，消失した場合の影響度を考慮し，評価します。「情報を守る」という観点から，「大」「中」「小」の３段階に設定するのも有効でしょう。この評価の意味は，ポリシー策定までの検討を効率化するということです。膨大な量の全てについて，安全性確保の方法を考えなくても，重要なものについて対策が考えられれば，それによって，ほとんどカバーできると判断できるからです。従って，重要度の評価にあたって，絶対的基準というのは存在しません。あくまでも相対的な基準で重要度を設定してください。

また，ハンドブック改訂版で示したように，この段階で保存形態が「電子媒体」の資産をセキュリティポリシーの対象にすることによって，以降の検討の範囲を絞り込むことができます。委員会の体制や諸状況を勘案して判断してください。

参考までに，各学校における情報資産の重要度の設定基準例を，図表１．５に示します。

図表１．５　情報資産の重要度設定基準例

分類	Ａ県立養護学校での判断基準	Ａ県立高等学校での判断基準
大	・リサイクル，リユースされる情報，消えると困る情報かつ個人情報を含むもの，漏えいしてはならない情報	・個人情報または機密情報を含む情報
中	・リサイクル，リユースされる情報，消えると困る情報，漏えいしても支障のない情報	－
小	・消えてもよい情報，消されてもよい情報，リサイクル，リユースされな	・個人情報または機密情報を含まない情報

	い情報 ・公開されてもよい情報，一般公開されている情報 ・希望者又は一般に配布している情報，漏えいしても支障のない情報	

（出所）平成 18 年度 E スクエア・エボリューション成果発表会プログラムより

情報資産の重要度評価にあたっては，同じ名前の情報資産であっても，記入された内容によって重要度が異なるものも存在します。例えば，「児童生徒個票」では，保護者に配布する様式では，配布を前提としたものなので漏洩の脅威を恐れることはありませんが，必要に応じて変更していくので消えてしまうと困ることから重要度は「中」とすることが適当とも判断されます。個人情報が記入された後の「児童生徒個票」は，名前は変わりませんが，漏洩しては困ることから，重要度は「大」が適当と判断されます。

１．２．４　【STEP３】――リスク対応策の検討

情報資産の洗い出しと整理が進むと，【STEP３】ではリスク対応策の検討を行います。ここでは，セキュリティ上の脅威を洗い出し，その脅威に対するリスクの大きさを評価します。次いで，リスクの大きさに応じて対応策を検討し，具体的な対応策を決めていきます。

（１）脅威の洗い出しと評価

情報資産がどのような脅威にさらされるのかを洗い出します。

脅威とは，自然災害や機器障害，悪意のある行為など，情報の損失を発生させる直接の要因のことです。

一般的な学校における情報セキュリティの脅威例を図表１．６に示します。

図表１．６　情報セキュリティ脅威例

個人情報保護関連	情報消失関連
■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 ■ウィ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
業務停止関連	**情報モラル関連**
■学校内パソコン等のウィ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

脅威の洗い出しの作業を進めたら，今度はそれぞれの脅威の大きさについて評価していきます。「大」「中」「小」の３段階に評価する場合，大＝非常に危ない，中＝危険はある，小＝ほとんどない，という基準で評価できるでしょう。

評価の仕方には，次の方法があります。

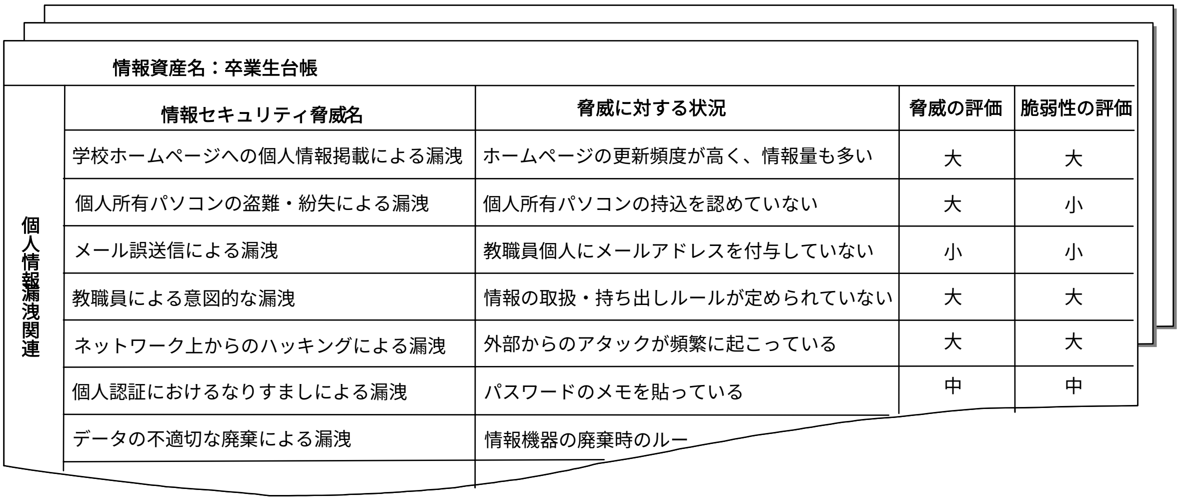
脅威の評価＝脅威の発生頻度×実際に発生した場合の被害の大きさ

脅威が頻繁に発生し，実際に発生したときの被害が大きいとなれば，脅威が大きい，ということになります。

次に脆弱性を評価します。脆弱性とは，学校が情報資産への脅威に対してどのくらい弱いかということを指します。まず脅威内容を明確にして，その脅威内容に対して学校の環境や体制がどのくらい弱いかを検討します。例えば情報資産をＵＳＢメモリで管理している場合，ＵＳＢメモリの持ち出しが可能な学校（ＵＳＢ管理体制が脆弱）の方が，持ち出しが禁止されている学校よりも脅威に直面する機会が増え，脆弱性の評価が高くなります。

図表１．７に，卒業生台帳についての情報セキュリティの脅威と脆弱性を評価した例を示します。

図表１．７　脅威と脆弱性の評価例



情報資産名：卒業生台帳

	情報セキュリティ脅威名	脅威に対する状況	脅威の評価	脆弱性の評価
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	ホームページの更新頻度が高く、情報量も多い	大	大
	個人所有パソコンの盗難・紛失による漏洩	個人所有パソコンの持込を認めていない	大	小
	メール誤送信による漏洩	教職員個人にメールアドレスを付与していない	小	小
	教職員による意図的な漏洩	情報の取扱・持ち出しルールが定められていない	大	大
	ネットワーク上からのハッキングによる漏洩	外部からのアタックが頻繁に起こっている	大	大
	個人認証におけるなりすましによる漏洩	パスワードのメモを貼っている	中	中
	データの不適切な廃棄による漏洩	情報機器の廃棄時のルー		

（２）リスクの評価

さらに，整理した学校の情報資産の重要度，脅威の評価結果，脆弱性の評価結果から，「リスク」の大きさを評価します。リスクとは，脅威によって情報資産が失われる可能性のことです。

一般的に

リスクの評価＝情報資産の重要度×脅威の評価×脆弱性の評価

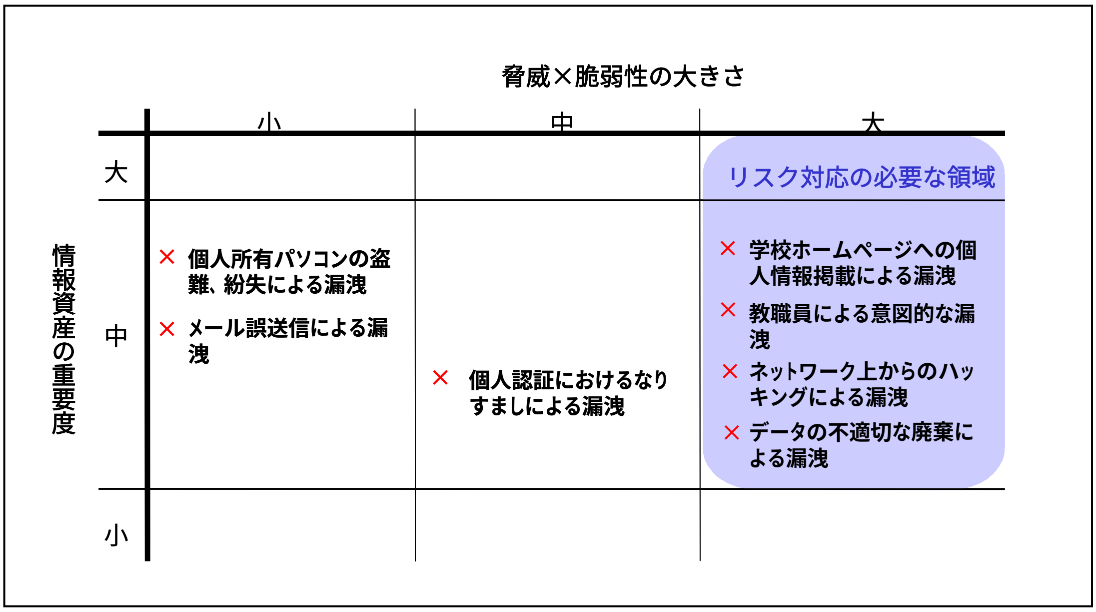
と言えます。

リスク評価の結果は，図表１．８のように表現できます。

例えば，卒業生台帳についてみれば，卒業台帳の情報資産の重要度は「中」であり，脅威の評価×脆弱性の評価の大きさが「大」のものを，対応が必要なリスクであるとします。言葉を換えれば，図において，リスク対応の必要な領域内にあるものが，リスク評価が「大」と言うことができます。

脅威の評価×脆弱性の評価の大きさは，機械的に計算できるものではありませんので，総合的に評価してください。

図表１．８　リスク評価の例



脅威×脆弱性の大きさ

情報資産の重要度

	小	中	大
大			リスク対応の必要な領域
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	× 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
小			

なお,「情報資産リスト」に脅威の評価，リスク評価を記入した表を「情報資産・リスクリスト」と呼んでいます。

『学校情報セキュリティ・ハンドブック改訂版』では，リスク評価作業を簡便化するために，前ステップにおいて検討すべき情報資産を重要度及び電子媒体に絞り込み，それをイメージしながら各脅威と脆弱性を合わせて評価するという方法を採用しています。

本来は，前ページにある卒業生台帳の例のように，すべての情報資産について脅威と脆弱性の大きさを評価し，情報資産の重要度と脅威・脆弱性の大きさからリスクの洗い出し・評価を行うことになります。

実際の検討にあたっては，図表１．９にあるワークシートなどを用いて，リスク評価を進めていきましょう。

この場合の評価の目的も,次工程であるリスク対応策をより効率的に行うためであり,大きいリスクへの対策によって，より小さいリスクへの対策もかなりカバーできると考えられます。更に小さいリスクに対しては，次工程で述べるように特別な対策は不要と判断しても問題ありません。

図表１．９　リスク評価ワークシート例

学校内の脅威の評価（情報資産名：　　　　　　　　　　）

	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

学校の情報資産ごとに,

1. 学校に想定される脅威をリストアップする。
2. 脅威の評価（大：非常に危ない　中：危険はある　小：ほとんどない）をする。
3. 評価判断の根拠を明らかにしておく。

リスク対応評価表（情報資産名：　　　　　　　　　　　）

	脅威×脆弱性の大きさ			
情報資産の重要度		小	中	大
	大			
	中			
	小			

学校の情報資産ごとに,

1. 資産の重要度・脅威の大きさをもとにマッピングする（大　中　小)。
2. 対応すべきリスクをしぼりこむ。

（３）リスク対応策の検討

重要な情報資産が洗い出され，セキュリティ上のリスクが洗い出されたら，対策を考え，意図的にリスクを減少させていく必要があります。

ａ）基本的対策の考え方

情報セキュリティの確保には，一般的に

- 技術的対策（環境面での対策）
- 管理的対策（運用面での対策）

の両面からの検討が必要であると言われます。

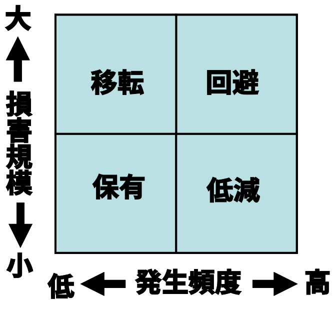
技術的対策はウイルス対策ソフトやファイアウォール，ネットワークなどハード・ソフトそのものの導入などを指し，管理的対策は，ＩＴ機器の利用者管理や運用体制，情報資産を扱うにあたって教員が守るべきルールなどを指します。『学校情報セキュリティ・ハンドブック改訂版』では，運用面での対策，環境面での対策と表現しています。

ｂ）対応策の考え方

リスク対応策には，「低減」「回避」「移転」「保有」といった考え方があります。これらは，情報資産に与える損害規模と脅威の発生頻度から，対応策を決定する考え方です。対応策を検討する際の参考にしてください。

図表１．１０　リスク対応の考え方

考え方		例
低減	脅威または脆弱性を小さくするなどの方法により，リスクを小さくする	パスワードを定期的に変更することにより，パスワードが盗まれたときのリスクを小さくする
回避	脅威そのものを取り除くことにより，リスクが発生する可能性をなくしてしまう	ノートパソコンの持ち出しを禁止することにより，外出先で紛失するリスクをなくす
移転	自校の抱えるリスクを他者に移し替える	自校で管理していたサーバを企業などに委託することにより，自校のリスクを移転する
保有	リスクがあっても，特に対応しない	小さなリスクまですべて対応することは現実的ではないので，対策しない



この内，損害規模の大きい“移転”，“回避”と，発生頻度の高い“低減”を中心に検討するのが一般的です。これらの検討において，費用に関係する項目やネットワーク及びＩＴ環境に深く関わる項目が予想されますので，対応策検討メンバーには，管理職やＩＴ担当などを加えておく必要があります。

また，具体的な対応策決定にあたっては

・教育，研修

・罰則の制定

について，考慮しておくことも大切です。

ｃ）対応策検討

リスクが大と評価された脅威（＝リスク名）について，重要と判断された情報資産をイメージしながら対応策を考え，採用する対応策を決定していきます。

リスク対応策検討シート記入例を図表１．１１に示します。

図表１．１１　リスク対応策検討シート記入例

リスク名		考えられる対応策	採用する対応策
個人情報保護関連	個人所有パソコンの盗難，紛失による漏洩	個人PCの持ち込み禁止 罰則規定を設ける	個人PCの持ち込み禁止
	USBメモリ等のメディアの盗難，紛失での漏洩	パスワード設定の義務づけ 暗号化の義務づけ 認証式のメディアの導入 持ち出し禁止の規定	パスワード設定の義務づけ 暗号化の義務づけ 認証式メディアを利用
	メールご送信による漏洩	フリーメールの利用制限 研修による扱いの徹底 添付のできないメールツールの採用	フリーメールの利用制限
	情報機器処分時のデータ消し忘れによる漏洩	廃棄時の扱いマニュアル作成 廃棄時のデータチェック	廃棄時の扱い手順を規定
	個人認証におけるなりすましによる漏洩	アカウント，パスワードの管理についての研修 生体認証の導入	アカウント，パスワードの管理義務を明確にする
	ディスプレー盗み見による漏洩	スクリーンセーバの導入 離籍時のロックシステム スクリーンフィルタによる視野角制限	離籍時のロックシステムを導入
	教職員による意図的な漏洩	研修の実施と義務づけ 罰則規定を設ける	悉皆研修を行い，その中で服務規程に触れる
情報消失関連の脅威	個人所有パソコンの盗難，紛失による喪失	個人PCの持ち込み禁止 罰則規定を設ける	個人PCの持ち込み禁止
	USBメモリ等のメディアの盗難，紛失での喪失	ファイルサーバ上でデータ管理	ファイルサーバ上でデータを一括管理する
	突然の電源断などによる情報喪失	UPSシステムの整備 データを置くファイルサーバの保護	UPSシステムの整備
	メディアの損傷などによる情報喪失	バックアップの実施	バックアップの実施
	誤消去等，人為的なトラブルによる情報消失	バックアップの世代管理 研修による扱いの徹底 ユーザ権限の設定	世代管理して，被害を最小限に止める
	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	バックアップの実施	バックアップの周期を短く
	保存ミスなど，データの取り扱い不全による情報消失	バックアップで保護 研修による扱いの徹底 ユーザの権限を細分化	ユーザの権限を細分化し，重要なファイルを守る。 バックアップの実施
業務停止関連	サーバ，システム等のダウンによる業務停止	サーバ等のシステムチェックを常時実施 ディスクのAlert装置の導入 バックアップ用のシステムを持つ	システムのチェックを定期的に実施
	停電による業務停止	UPSシステムの整備 発電システムを持つ	UPSシステムの整備
	システムの誤用など人為的ミスによる業務停止	基幹システムを扱えるユーザの限定 監視システムで，異常の検知	基幹システムを扱うユーザの限定 監視システムの導入
情報モラル関連	アカウントの不正利用	アカウント，パスワードの管理についての研修 生体認証の導入 罰則規定	アカウント，パスワードの管理についての研修 罰則規定を設ける

１．２．５　【STEP４】――セキュリティポリシーの作成

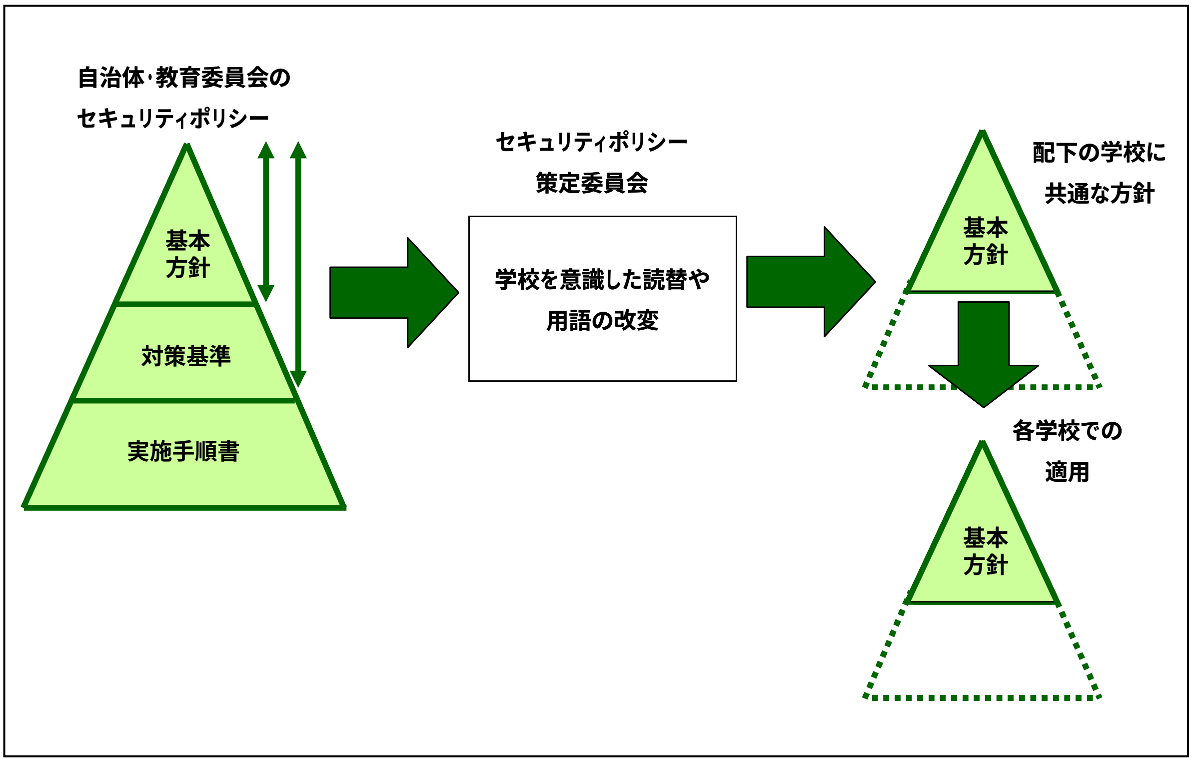
これまでの３段階で検討してきたリスク対応などをとりまとめて,【STEP４】では,いよいよ学校情報セキュリティポリシーの作成段階に入ります。

（１）基本方針の作成

ａ）取り組み方

情報セキュリティポリシーは,「１－１」項で説明したとおり,「基本方針」,「対策基準」,「実施手順」の３階層の文書から構成されています。一般に学校の情報機器（資産）は，自治体や教育委員会によって整備されることが多く，ネットワークを含めて，全システムの運用も学校単独で行われることは少ないと考えられます。従って，「基本方針」,「対策基準」は，自治体や教育委員会で設立した内容を参考にして，自校の実情に合わせて作成するのが適当と考えられます。図表１．１２に情報セキュリティポリシー作成の流れの例を示します。

図表１．１２　情報セキュリティポリシー作成の流れ（例）



ｂ）必要項目と例

情報セキュリティの確保に取り組むための管理策として，国際標準や，それをもとにしたＪＩＳ「情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範　JIS Q27002:2006」が制定されており，学校の上位に位置づけられる自治体や教育委員会の基本方針の多くも，これに沿った形で設定されていると思われます。実践規範として制定された JIS Q27002:2006 から，学校の情報セキュリティポリシー方針に必要と思われる項目を選び出し，学校向けの用語で表現しますと

＜必要項目＞

- ・目的
- ・学校の責務（管理責任の明確化，規程の整備，リスク分析・評価，条例・規則等の遵守）
- ・管理職及び各情報管理者の責務
- ・教職員の責務　　など

＜内容＞

- ・情報セキュリティ管理体制の整備（管理責任の明確化，義務及び責任）
- ・対策の規程整備（組織的な取り組みの明文化，対策実効化のしくみ）
- ・評価及び見直し　など

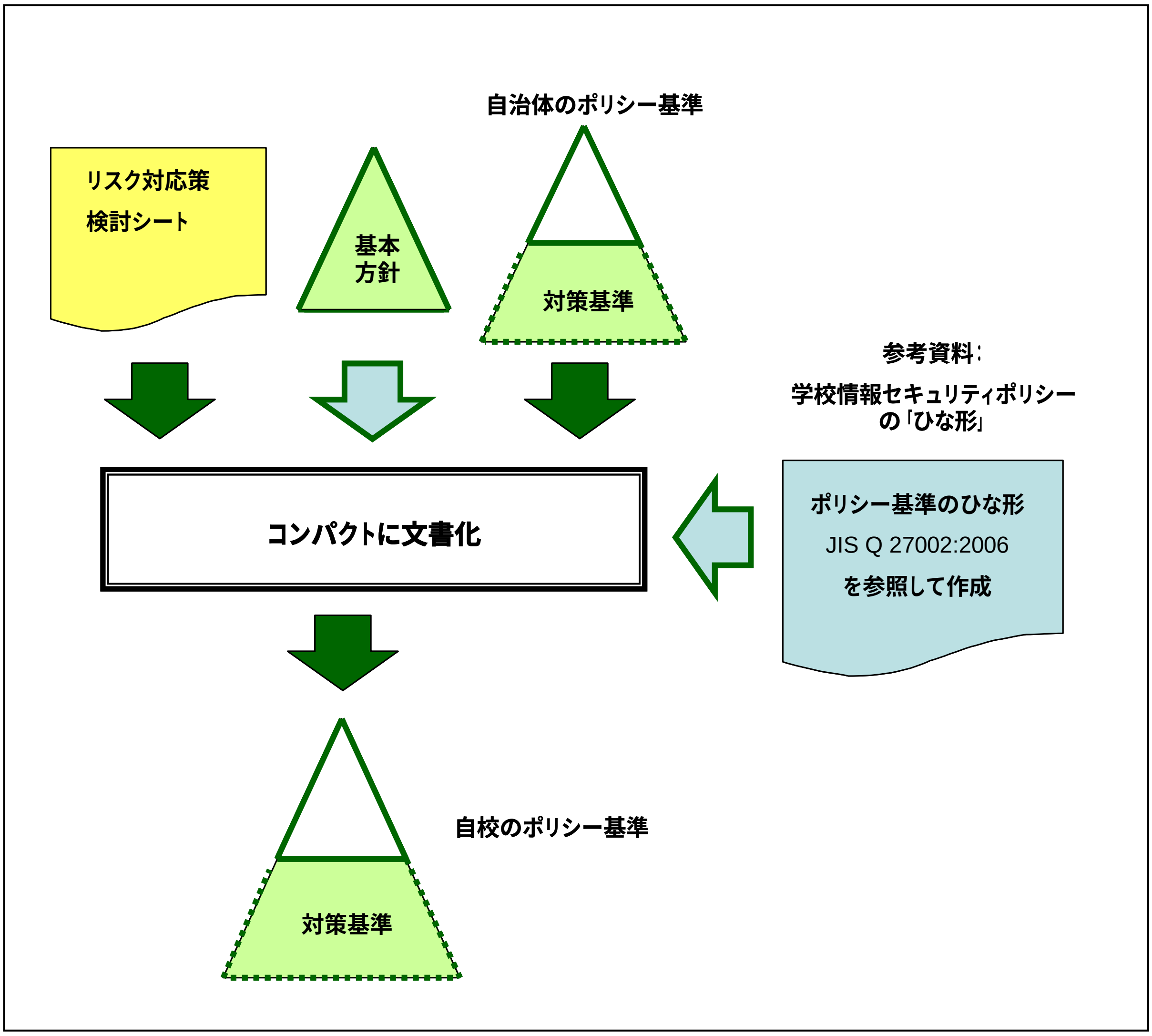
と，なります。

これをもとにした基本方針の例を，「２－４項　学校情報をセキュリティポリシー例（１)」に示します。

（２）対策基準の作成

【STEP３】で作成した「リスク対応策検討シート」と直前に作成した基本方針から，“学校はどのようなセキュリティ対策をとるのか”を規則の形に文書化します。自治体や教育委員会で既にポリシー基準が有る場合は，それを参照して作成しましょう。ここでは，セキュリティ管理の詳細な手順の記述は不要で，わかりやすく，できるだけ１対策１文で，表現するのが望ましいと言えます。

図表１．１３　情報セキュリティ対策基準のまとめ方例



ｈｉｎｔ！

教育委員会が中心にセキュリティポリシー策定委員会を運営している場合，「基本方針」，「対策基準」までを共通化するケースが多いようです。特に，教育ネットワークや事務処理のネットワークが教育センター中心にシステム化されている場合には，基準が共通化される方が望ましいと考えられます。

学校及び学校をとりまく情報システムの環境やその整備計画を勘案して適切な取り組み方を検討してください。

【STEP４】のセキュリティポリシー策定にあたっては，例えば図表１．１４に示すチェックリストを用いることも有効です（平成 17 年度版の『学校情報セキュリティ・ハンドブック』には掲載しています）。

なお，①～⑦の大項目は，「技術情報－セキュリティ技術－情報セキュリティマネジメントの実践のための規範　JIS Q 27002:2006　」の項目をもとに設定しております。

図表１．１４　セキュリティチェックリスト

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，通信事業者との連絡体制が構築されている（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等）。

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。また，重要度については，定期的に見直されている。

③教職員のセキュリティ

□情報セキュリティ確保のための各教職員の役割・責任がきちんと定められ，“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，ソフトウエ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，最悪の場合，懲戒処分の手続がとられるようになっている。

④ハードウエアや環境のセキュリティ

□コンピュータや周辺機器は，いじられたり，認められないアクセスがなされたりするようのないよう設置し，管理されている。

□重要情報が外部に漏洩しないよう，取扱に慎重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，ソフトウエアは，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エアの運用管理

□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。

□外部の請負業者の事業所内におけるデータの信用低下，損傷・喪失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新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エアの侵入を防止し，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エ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作成されている。

□電子メールの使用に際する明確な利用ルールが作成されている。

□ホームページ等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

□ソフトウエ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（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てください）。

上記のチェックリストに関して，学校現場として遵守する必要がないと判断される事項については削除するとともに，注力すべき項目については，一層具体的に内容を記述することで，セキュリティポリシーとして文章化していくことを目指します。

（3）実施手順書の作成

対策基準を実行するための具体的行動マニュアルに相当するものが実施手順書です。教育委員会を中心にしたセキュリティポリシー策定委員会が存在した場合においても各学校での事情や独自性から，各学校ごとに手順書を作成する場合が多いようです。

その場合も，管理職を含む学校内でのセキュリティ担当グループ（委員会）などで，全ての教職員が守れるような, わかりやすい現実的な手順を明文化することが重要です。

＜具体化のポイント＞
- ・誰が実施するかを明確にする。
- ・何を，どのようにするかを具体的に表現する。
- ・いつ実施するかを明確にする。
- ・パソコン操作方法などは，誰でも操作できるように図入りで説明する。
- ・許可や申請が必要な事項については，申請方法や申請書式を規定する。
- ・事故が発生した時の連絡先について明確にする。
- ・事故処理の記録，報告についての書式を作成する。

＜進め方のポイント＞
- ・すでに実施されている手順があれば，それを再整理する。
- ・手順を図示するなどの工夫をする。
- ・使用する帳票などは具体的な記入例を示す。

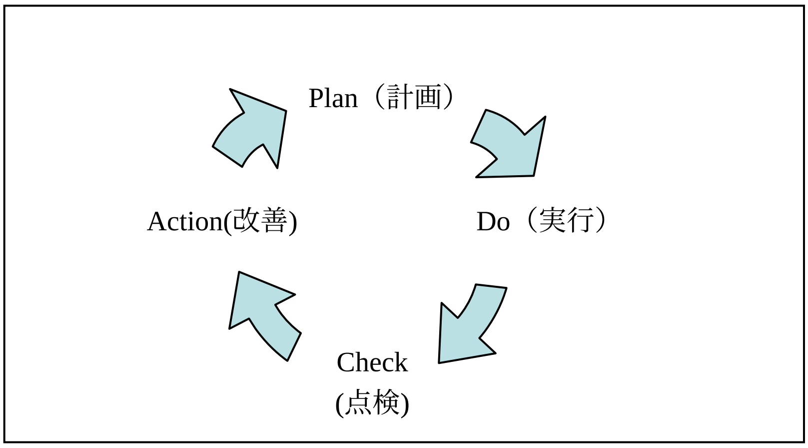
なお，一般教職員が守るべきセキュリティポリシーとしては,『学校情報セキュリティ・ハンドブック改訂版』の巻末に「ひな形」が掲載されていますが，管理者向けには以下の「ひな形」（平成 17 年版『学校情報セキュリティ・ハンドブック』の「ひな形Ａに相当）が参考になると思われます。

１．２．６　【STEP５】――セキュリティ対策の継続的な運用

セキュリティポリシーの策定は，目的ではなく，学校現場で安心・安全に情報資産を守っていくためのルール作りです。従って，日々の教育活動に携わる教職員の一人一人が，このルール（＝セキュリティ対策）について，十分認識し，それを厳守していく必要があります。

一般的に，このプロセスは，Ｐｌａｎ（計画）→Ｄｏ（実行）→Ｃｈｅｃｋ（点検）→Ａｃｔｉｏｎ（改善）という４つのステップをＰＤＣＡサイクルとして継続すること，と表現されます。

図表１．１５　ＰＤＣＡサイクル



① Ｐｌａｎ（計画）：セキュリティポリシーの策定
② Ｄｏ（実行）：機器やソフトウエアの導入・運用
③ Ｃｈｅｃｋ（点検）：状況把握と確認
④ Ａｃｔｉｏｎ（改善）：見直しとルールの改善

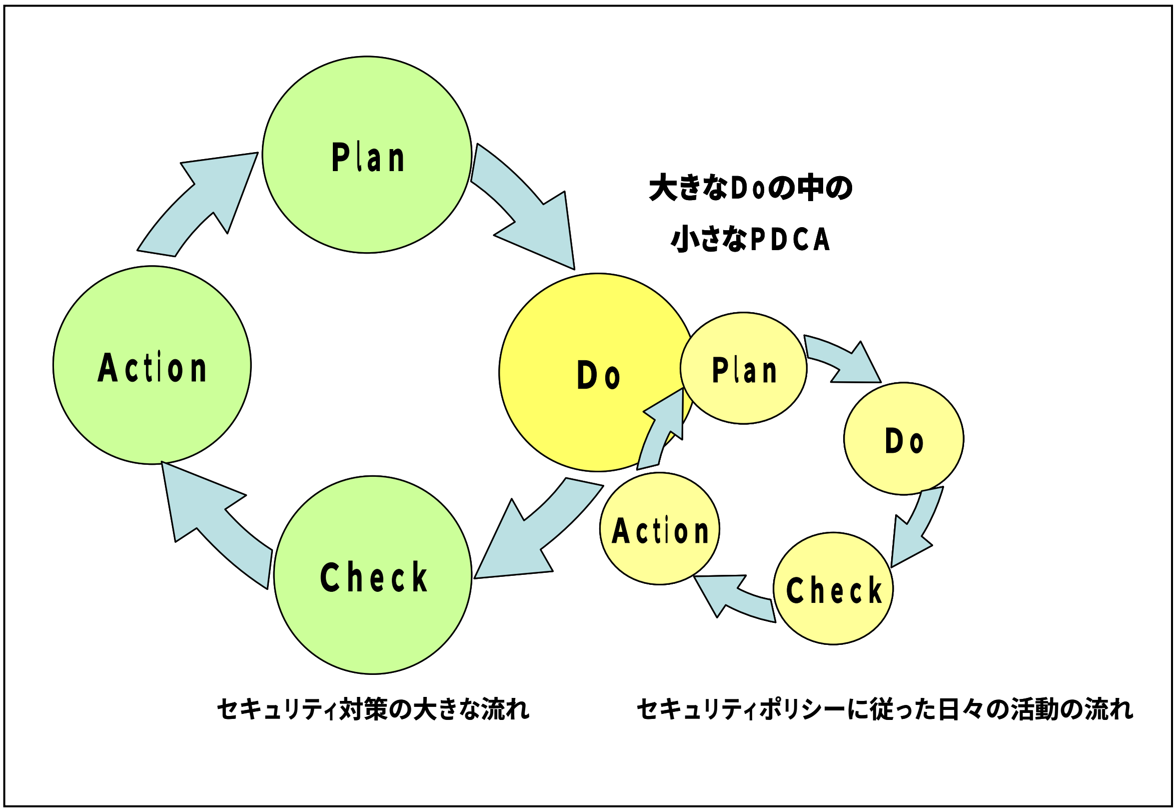
学校現場で考えた場合，上記の②Ｄｏでの機器やソフトウエアの導入・運用は，①Ｐｌａｎであるセキュリティポリシー策定内容に沿って行われることはなく，既存のシステム環境に沿って，ポリシーなどが考えられる，ということになります。

従って，②Ｄｏは，①で策定した「基本方針」，「対策基準」，「実施手順書」に従った日々の活動という風に考えれば良いでしょう。

また，「基本方針」，「対策基準」は，それほど頻繁に見直すという性格のものではありません。主として日々の活動マニュアルとも言える「実施手順書」及び「対策基準」の一部について，点検・改善していくことになります。

大きくセキュリティ対策のＰＤＣＡと，日々の活動でのＰＤＣＡとの関係は，次のように考えれば良いでしょう。

図表１．１６　セキュリティ対策の多重ループ

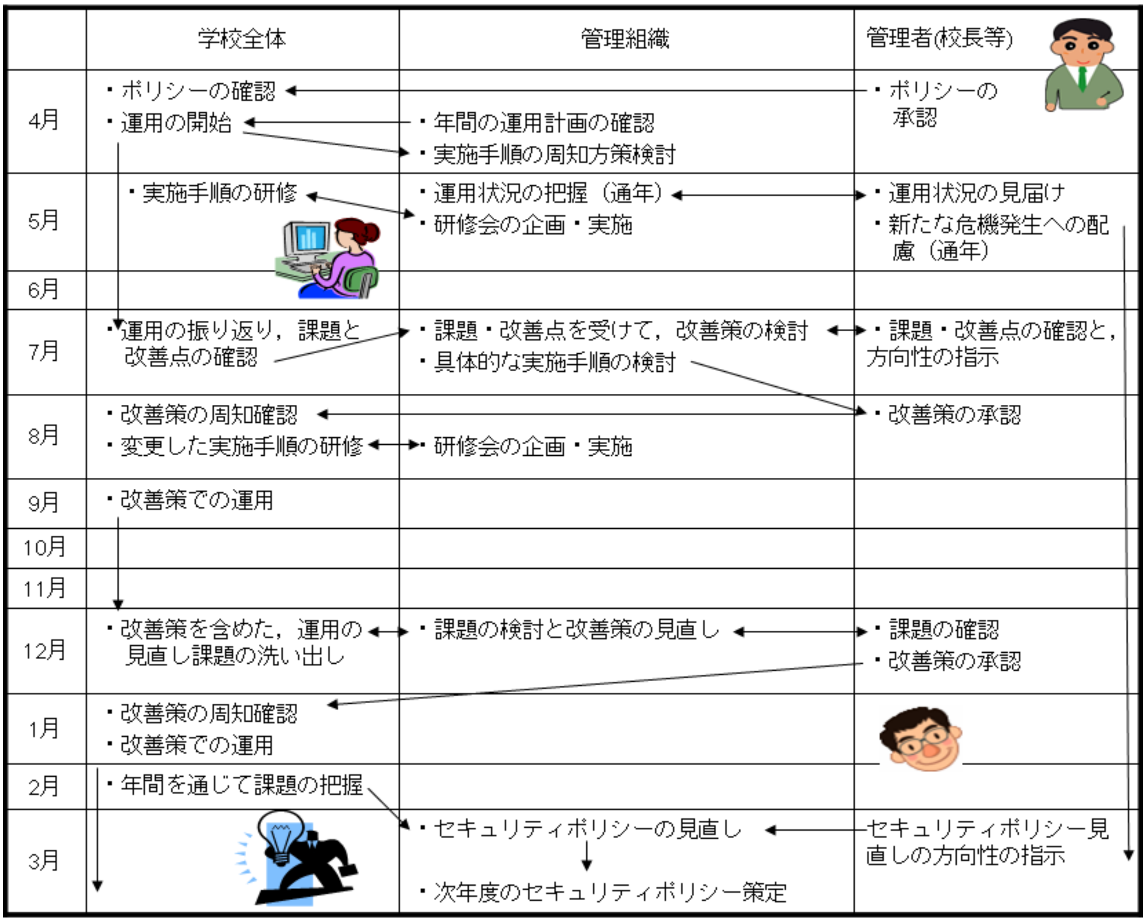


それでは，日々の活動の中でどのようにＰＤＣＡを回していけば良いでしょうか。

（１）運用計画の作成

学校には様々な行事がありますが，一般の組織と同様に１年サイクルで，重要な行事の時期が決まっていますので，それに沿った運用計画をたてると良いでしょう。

図表１．１７　情報セキュリティカレンダーの例



	学校全体	管理組織	管理者(校長等)
4月	・ポリシーの確認 ・運用の開始	・年間の運用計画の確認 ・実施手順の周知方策検討	・ポリシーの承認
5月	・実施手順の研修	・運用状況の把握（通年） ・研修会の企画・実施	・運用状況の見届け ・新たな危機発生への配慮（通年）
6月			
7月	・運用の振り返り，課題と改善点の確認	・課題・改善点を受けて，改善策の検討 ・具体的な実施手順の検討	・課題・改善点の確認と，方向性の指示
8月	・改善策の周知確認 ・変更した実施手順の研修	・研修会の企画・実施	・改善策の承認
9月	・改善策での運用		
10月			
11月			
12月	・改善策を含めた，運用の見直し課題の洗い出し	・課題の検討と改善策の見直し	・課題の確認 ・改善策の承認
1月	・改善策の周知確認 ・改善策での運用		
2月	・年間を通じて課題の把握		
3月		・セキュリティポリシーの見直し ・次年度のセキュリティポリシー策定	セキュリティポリシー見直しの方向性の指示

この中に含めておく内容のポイントは以下の通りです。

①実技研修を含む研修会の実施

作成したセキュリティポリシーは，教職員に配布し，同意を求めます。しかし，セキュリティポリシーは専門用語も多く，一般の教職員にはわかりにくいかもしれません。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」を説明するとともに，対策基準及び実施手順書を使って，具体的な操作を含む研修会を実施します。こうすることにより実効性を確保できます。

②重要な情報の定期的チェック

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回程度，定期的にチェックを行い，問題点の把握と改善に努めましょう。

③定期的見直しと改善

運用中に発生した問題を把握するとともに，教職員の意見も現場の声として

収集します。これらの情報をもとに，セキュリティポリシーが妥当かどうかを見直し，改善します。また，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。

変更した新しいセキュリティポリシーは，再度配布し，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。

見直し・改善の頻度については，セキュリティポリシーの運用をスタートした当初は，さまざまな問題を内包している可能性が高いと思います。例えば１学期間運用してみたところで，いったん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ていくと負担も少なくて済むと思います。また，最近の傾向として，転入してきた教職員が事故を起こしてしまうケースが非常に増えているので，転入者に対しては，運用の初年度と同様の研修を行っておく必要があるでしょう。

ｈｉｎｔ！

学校には個人情報を初めとする重要な情報が多くありますが，年間を通して，いつ，どんな情報を扱うのかを，年間の執務内容として情報セキュリティカレンダーにまとめておくと良いでしょう。

上越市教育委員会では,“ 個人情報の取扱い ”について，学校や幼稚園が執務の中で扱う情報と，扱いのポイントを月毎に整理して，まとめています。

（http://www.jecomite.jorne.ed.jp/kojin-joho/manual03.pdf）

これを参考に，自校の年間行事と執務内容，また重要情報の扱い方を整理してみてください。

（２）事故発生時の対応体制

最も避けなければならないのは，事故が発生したときに責任を問われることを恐れて報告も対処もしないでいることです。このようなことを避けるには,「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」といった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。

ここでのポイントは，事故やトラブルは防げるという発想から，事故やトラブルは必ず起きる，という前提で対応できる体制を考えることです。

（３）運用時のチェック項目

運用に際して事前に自校の状況を確認しておくことも重要です。簡単に行えるチェックリストを利用すれば便利です。この結果をもとに自校での対策が必要かどうかの検討や，手順書の不備についての改善を進めましょう。まだチェックリストそのものの改訂を行えるように結果を評価する機会を用意すれば更に効果的でしょう。

以下に，図表１．１８にチェックリストの例を示します。

図表１．１８　運用時チェックリストの例

- □　文章は，簡潔明瞭に記述され正確に理解されていますか。
- □　情報セキュリティポリシーに関する継続的改善活動を確実に実施する責任の所在が明確にされ定期的に委員会活動が行われていますか。
- □　情報セキュリティ事件･事故が発生した場合の初動対処の手順や緊急連絡先が周知されていることを確認するため定期的に訓練が行われていますか。
- □　情報セキュリティポリシーの有効性を定期的に確認するため, 定期的なリスク分析や自己点検，監査が実施されていますか。
- □　対策基準や実施手順書が情報化の進展や新たに採用された情報処理技術に適合するよう見直しが行われていますか。
- □　当校の情報セキュリティポリシーに整合した情報セキュリティに関する啓発･教育のための研修を定期的に行っていますか。
- □　対策基準を満たすために必要な予算措置は，行われていますか。
- □　情報セキュリティポリシーの要求事項が実際の業務や環境と乖離しており, 実践できず形骸化してしまっている要求事項はありませんか。
- □　情報セキュリティポリシーを浸透させるため率先して実践する担当者(ファシリテータ)は,各職場に適切に配置出来ていますか。

（４）セキュリティポリシー配付時の工夫

セキュリティポリシーを配付する時は，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。

最後に

情報セキュリティ確保のために
①ポリシー策定のプロセスが重要です。
②ポリシー策定後の運用のプロセスが重要です。

JIS Q 27002:2006 中項目	JIS Q 27002:2006 小項目	管理策	管理策の概要（一部抜粋，又は要約）
情報セキュリティ基本方針	5.1.1	情報セキュリティ基本方針文書	情報セキュリティ基本方針文書は，教育委員会によって承認され，全教職員に公表し，通知する。
	5.1.2	情報セキュリティ基本方針のレビュー	情報セキュリティ基本方針は，あらかじめ定められた間隔で，又は重大な変化が発生した場合に，それが引き続き適切妥当及び有効であることを確実にするためにレビューする。
内部組織	6.1.1	情報セキュリティに対する経営陣の責任	教育委員会は，情報セキュリティの責任に関する明りょうな方向付け，自らの関与の明示，責任の明確な割り当て及び承認を行なう。
	6.1.3	情報セキュリティ責任の割当て	全ての情報セキュリティ責任を，明確に定める。
	6.1.4	情報処理設備の認可プロセス	新しい情報処理設備に対する教育委員会による認可プロセスを定め，実施する。
	6.1.5	秘密保持契約	情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約をレビューする。
	6.1.6	関係当局との連絡	関係当局との適切な連絡体制を維持する。
	6.1.7	専門組織との連絡	情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。
	6.1.8	情報セキュリティの独立したレビュー	情報セキュリティ及びその実施のマネジメントに対する組織の取り組みについて，あらかじめ計画した間隔で，又はセキュリティの実施に重大な変化が生じた場合に，独立したレビューを実施する。
外部組織	6.2.1	外部組織に関係したリスクの識別	外部組織がかかわる業務からのリスクを識別し，外部組織にアクセスを許可する前に適切な管理策を実施する。
	6.2.3	第三者との契約におけるセキュリティ	学校の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げる。
資産に対する責任	7.1.1	資産目録	重要な資産すべての目録を作成・維持する。
	7.1.2	資産の管理責任者	資産のすべてについて，管理責任者を指定する。
情報の分類	7.2.1	分類の指針	学校に対しての価値，法的要求事項，及び重要度の観点から分類する。
	7.2.2	情報のラベル付け及び取扱い	学校として採用した分類体系に従って，情報のラベル付け及び取り扱いの手順を策定し，実施する。
雇用前	8.1.1	役割及び責任	学校の情報セキュリティ基本方針に従って，教職員，契約相手及び第三者の利用者のセキュリティの役割及びを定め，文書化する。
	8.1.3	雇用条件	教職員，契約相手及び第三者の利用者は，情報セキュリティに関する責任を記載した雇用契約書に同意し署名する。
雇用期間中	8.2.1	経営陣の責任	校長は，確立された方針及び手順に従ったセキュリティの適用を，教職員，契約相手及び第三者の利用者に要求する。
	8.2.2	情報セキュリティの意識向上，教育及び訓練	すべての教職員，関係する契約相手及び第三者の利用者は，職務に関連する教育・訓練を受ける。
	8.2.3	懲戒手続き	セキュリティ違反を犯した教職員に対する正式な懲戒手続きを備える。
雇用の終了又は変更	8.3.1	雇用の終了又は変更に関する責任	雇用の終了又は変更に関する責任を明確に定め，割り当てる。
	8.3.2	資産の返却	すべての教職員，関係する契約相手及び第三者の利用者は，雇用，契約，又は合意の終了時に，自らが所持する学校の資産すべてを

JIS Q 27002:2006 中項目	JIS Q 27002:2006 小項目	管理策	管理策の概要（一部抜粋，又は要約）
			返却する。
	8.3.3	アクセス権の削除	すべての教職員,契約相手及び第三者の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除し，また変更に合わせて修正する。
セキュリティを保つべき領域	9.1.1	物理的セキュリティ境界	学校は，情報及び情報処理設備のある領域を保護するために，物理的セキュリティ境界（例：外壁，カードで制御した入口，有人の受付，等）を用いる。
	9.1.2	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を保つべき領域を保護する。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。
	9.1.3	オフィス，部屋及び施設のセキュリティ	オフィス，部屋及び施設のセキュリティを設計する。
	9.1.4	外部及び環境の脅威からの保護	火災，洪水，地震，爆発，暴力行為，その他の自然災害又は人為的災害による被害から保護する。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。
	9.1.5	セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する保護及び指針を設計する。
	9.1.6	一般の人の立寄り場所及び受渡場所	一般の人の立寄り場所（荷物受渡場所など）を管理し，可能なら，認可されていないアクセスを避けるために,情報処理施設から隔離する。
装置のセキュリティ	9.2.1	装置の設置及び保護	装置は,環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護する。
	9.2.2	サポートユーティリティ	装置は，サポートユーティリティの不具合による，停電，その他の故障から保護する。
	9.2.3	ケーブルの配線のセキュリティ	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受又は損傷から保護する。
	9.2.4	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，正しく保守する。
	9.2.5	構外にある装置のセキュリティ	構外にある装置に対しては,構内の作業とは異なるリスクを考慮に入れて，セキュリティを適用する。
	9.2.6	装置の安全な処分又は再利用	記憶媒体を内蔵した装置は,データ及びライセンス供与されたソフトウエアを消去する。
	9.2.7	資産の移動	装置，情報，又はソフトウエアは，事前の認可なしでは，構外に持ち出さない。
運用手順及び責任	10.1.1	操作手順書	操作手順は，文書化し維持していく。その操作手順は，必要とするすべての利用者に対して利用可能とする。
	10.1.2	変更管理	情報処理設備及びシステムの変更を管理する。
	10.1.3	職務の分割	職務及び責任範囲は，学校の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分割する。
	10.1.4	開発施設，試験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は，認可されていないアクセス又は変更によるリスクを低減するために，分離する。

JIS Q 27002:2006 中項目	JIS Q 27002:2006 小項目	管理策	管理策の概要（一部抜粋，又は要約）
第三者が提供するサービスの管理	10.2.1	第三者が提供するサービス	第三者が提供するサービスについて，セキュリティ管理策，提供サービスレベルが，第三者によって確実に実施，運用及び維持されるようにする。
	10.2.2	第三者が提供するサービスの監視及びレビュー	第三者が提供するサービス，報告及び記録を，常に監視し，レビューする。
	10.2.3	第三者が提供するサービスの変更に対する管理	サービス提供の変更を管理する
システムの計画作成及び受入れ	10.3.1	容量・能力の管理	要求されたシステム性能を満たすことを確実にするために,資源の利用を監視・調整し，将来必要とする容量・能力を予測する。
	10.3.2	システムの受入れ	新しい情報システム,及びその改訂･更新版の受入基準を確立し,開発中及びその受入れ前に適切な試験を実施する。
悪意のあるコード及びモバイルコードからの保護	10.4.1	悪意のあるコードに対する管理策	悪意のあるコードから保護するために，検出，予防及び回復のための管理策,並びに利用者に適切に意識させるための手順を実施する。
	10.4.2	モバイルコードに対する管理策	認可されたモバイルコードが,明瞭に定められたセキュリティ方針に従って動作することを確実にする環境設定を行なう。
バックアップ	10.5.1	情報のバックアップ	重要な情報及びソフトウエアのバックアップは,合意された方針に従って定期的に取得し，検査する。
ネットワークセキュリティ管理	10.6.1	ネットワーク管理策	ネットワークを用いた業務用システム及び業務用ソフトウエアのセキュリティを維持するために,ネットワークを適切に管理し制御する。
	10.6.2	ネットワークサービスのセキュリティ	すべてのネットワークサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項を特定する。
媒体の取扱い	10.7.1	取外し可能な媒体の管理	取り外し可能な媒体の管理のための手順を備える。
	10.7.2	媒体の処分	媒体が不要となった場合は，正式な手順を用いて，セキュリティを保ち，安全に処分する。
	10.7.3	情報の取扱い手順	情報の取り扱い及び保管についての手順を,認可されていない開示又は不正使用から保護するために，確立する。
	10.7.4	システム文書のセキュリティ	システム文書は，認可されていないアクセスからを保護する。
情報の交換	10.8.1	情報交換の方針及び手順	あらゆる形式の通信設備を利用した情報交換を保護するために,正式な交換方針，手順及び管理策を備える。
	10.8.2	情報交換に関する合意	学校と外部との間の情報及びソフトウエアの交換について,両者間で合意を取り交わす。
	10.8.3	配送中の物理的媒体	情報を格納した媒体は，配送の途中の認可されていないアクセス，不正使用又は破損から保護する。
	10.8.4	電子的メッセージ通信	電子メッセージ通信に含まれた情報を適切に保護する。
	10.8.5	業務用情報システム	業務用情報システムの相互接続と関連がある情報を保護するために，個別方針及び手順を策定し，実施する。
電子商取引サービス	10.9.1	電子商取引	公衆ネットワークを経由する電子商取引に含まれる情報は,不正行為,契約紛争,許可されていない開示及び改ざんから保護する。
	10.9.2	オンライン取引	オンライン取引に含まれる情報は，不完全な通信，誤った通信経路設定，認可されていないメッセージの変更，認可されていない開示，認可されていない複製または再生を未然に防止するために，保護する。
	10.9.3	公開情報	認可されていない変更を防止するために,公開システム上で利用

JIS Q 27002:2006 中項目	JIS Q 27002:2006 小項目	管理策	管理策の概要（一部抜粋，又は要約）
			可能な情報の完全性を保護する。
監視	10.10.1	監査ログ取得	利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを取得し，合意された期間保持する。
	10.10.2	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し，監視活動の結果をレビューする。
	10.10.3	ログ情報の保護	ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護する。
	10.10.4	実務管理者及び運用担当者の作業ログ	システムの実務管理者（情報管理者）及び運用担当者（情報担当教職員）の作業を記録する。
	10.10.5	障害のログ取得	障害のログを取得し，分析し，障害に対する適切な処置をとる。
	10.10.6	クロックの同期	学校又はセキュリティ領域内のすべての情報処理システム内のクロックは，合意された正確な時刻源と同期させる。
アクセス制御に対する業務上の要求事項	11.1.1	アクセス制御方針	アクセス制御方針は，アクセスについての業務上及びセキュリティ上の要求事項に基づいて確立し，文書化し，レビューする。
利用者アクセスの管理	11.2.1	利用者登録	すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者の登録・登録削除についての正式な手順を備える。
	11.2.2	特権管理	特権の割当て及び利用を制限し，管理する。
	11.2.3	利用者パスワードの管理	パスワードの割当ては，正式な管理プロセスによって管理する。
	11.2.4	利用者アクセス権のレビュー	教育委員会は，利用者のアクセス権を定められた間隔でレビューする。
利用者の責任	11.3.1	パスワードの利用	パスワードの選択及び利用時に，正しいセキュリティ慣行に従うことを，利用者に要求する。
	11.3.2	無人状態にある利用者装置	利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にする。
	11.3.3	クリアデスク・クリアスクリーン方針	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，並びに情報処理設備に対するクリアスクリーン方針を適用する。
ネットワークのアクセス制御	11.4.1	ネットワークサービスの利用についての方針	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。
	11.4.2	外部から接続する利用者の認証	遠隔利用者のアクセスを管理するために，適切な認証方法を利用する。
	11.4.3	ネットワークにおける装置の識別	特定の場所及び装置からの接続を認証するための手段として，自動の装置識別を考慮する。
	11.4.4	遠隔診断用及び環境設定用ポートの保護	診断用及び環境設定用ポートへの物理的及び論理的アクセスを制御する。
	11.4.5	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は，ネットワーク上，グループごとに分割する。
	11.4.6	ネットワークの接続制御	共有ネットワーク，特に，組織の境界を越えて広がっているネットワークについて，アクセス制御方針及び業務用ソフトウエアの要求事項に沿って，利用者のネットワーク接続能力を制限する。
	11.4.7	ネットワークルーティング制御	コンピュータの接続及び情報の流れが業務用ソフトウエ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，ルーティング制御の管理策をネットワークに対して実施する。
オペレーティングシステムのアクセス制御	11.5.1	セキュリティに配慮したログオン手順	オペレーティングシステムへのアクセスは，セキュリティに配慮したログオン手順によって制御する。
	11.5.2	利用者の識別及び認証	すべての利用者は，各個人の利用ごとに一意な識別子（利用者ID）を保有する。

JIS Q 27002:2006 中項目	JIS Q 27002:2006 小項目	管理策	管理策の概要（一部抜粋，又は要約）
	11.5.3	パスワード管理システム	パスワード管理システムは対話式とする。また，良質のパスワードを確実とする。
	11.5.4	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エアによる制御を無効にすることのできるユーティリティプログラムの使用を制限し，厳しく管理する。
	11.5.5	セッションのタイムアウト	一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する。
	11.5.6	接続時間の制限	リスクの高い業務用ソフトウエアに対しては，接続時間の制限を利用する。
業務用ソフトウエア及び情報のアクセス制御	11.6.1	情報へのアクセス制限	利用者及びサポート要員による情報及び業務用ソフトウエアシステム機能へのアクセスは，既定のアクセス制御方針に従って制限する。
	11.6.2	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は，専用の（隔離された）コンピュータ環境をもつ。
モバイルコンピューティング及びテレワーキング	11.7.1	モバイルのコンピューティング及び通信	モバイルコンピューティング設備･通信設備を用いた場合のリスクから保護するために，正式な方針を備え，適切なセキュリティ対策を採用する。
	11.7.2	テレワーキング	テレワーキングのための方針，運用計画及び手順を策定し，実施する。
情報システムのセキュリティ要求事項	12.1.1	セキュリティ要求事項の分析及び仕様化	新しい情報システム又は既存の情報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，セキュリティの管理策についての要求事項を仕様化する。
業務用ソフトウエアでの正確な処理	12.2.1	入力データの妥当性確認	業務用ソフトウエアに入力するデータは，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。
	12.2.2	内部処理の管理	情報の破壊を検出するために，妥当性確認の機能を業務用ソフトウエアに組み込む。
	12.2.3	メッセージの完全性	業務用ソフトウエアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要求事項を特定し，適切な管理方法を特定し，実装する。
	12.2.4	出力データの妥当性確認	業務用ソフトウエアからの出力データは，保存する情報の処理が正しく，適切であることを確実にするために，妥当性を確認する。
暗号による管理策	12.3.1	暗号による管理策の利用方針	情報を保護するための暗号による管理策の利用に関する方針を，策定し実施する。
	12.3.2	かぎ（鍵）管理	学校における暗号技術の利用を支持するために，かぎ管理を実施する。
システムファイルのセキュリティ	12.4.1	運用ソフトウエアの管理	運用システムにかかわるソフトウエアの導入を管理する手順を備える。
	12.4.2	システム試験データの保護	試験データは，注意深く選択し，保護し，管理する。
	12.4.3	プログラムソースコードへのアクセス制御	プログラムソースコードへのアクセスを制限する。
開発及びサポートプロセスにおけるセキュリティ	12.5.1	変更管理手順	変更の実施は，正式な変更管理手順の使用によって，管理する。
	12.5.2	オペレーティングシステム変更後の業務用ソフトウエアの技術的レビュー	オペレーティングシステムを変更するときは，学校の運用又はセキュリティに悪影響がないことを確実にするために，重要な業務用ソフトウエアをレビューし，試験する。
	12.5.3	パッケージソフトウエアの変更に対する制限	パッケージソフトウエアの変更は，抑止し，必要な変更だけに限る。

JIS Q 27002:2006 中項目	JIS Q 27002:2006 小項目	管理策	管理策の概要（一部抜粋，又は要約）
	12.5.4	情報の漏えい	情報の漏えいの可能性を抑止する。
	12.5.5	外部委託によるソフトウエア開発	教育委員会は，外部委託したソフトウエア開発を監督し，監視する。
技術的ぜい弱性管理	12.6.1	技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得する。また，そのようなぜい弱性に学校がさらされている状況を評価し，それと関連するリスクに対処するための適切な手段をとる。
情報セキュリティの事象及び弱点の報告	13.1.1	情報セキュリティ事象の報告	情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけすみやかに報告する。
	13.1.2	情報セキュリティ弱点の報告	すべての教職員，契約相手並びに第三者の情報システム及びサービスの利用者に，発見した又は疑いをもったセキュリティ弱点を，すべて記録し報告するように要求する。
情報セキュリティインシデントの管理及びその改善	13.2.1	責任及び手順	情報セキュリティインシデントに対する迅速，効果的で整然とした対応を確実にするために，責任体制及び手順を確立する。
	13.2.2	情報セキュリティインシデントからの学習	情報セキュリティインシデントの形態，規模及び費用を定量化し監視できるようにする仕組みを備える。
	13.2.3	証拠の収集	情報セキュリティインシデント後の事後処理が法的処置に及ぶ場合は，証拠を収集，保全及び提出する。
事業継続管理における情報セキュリティの側面	14.1.1	事業継続管理手続への情報セキュリティの組込み	学校全体を通じて事業継続のために，必要な情報セキュリティの要求事項を取り扱う，管理された手続きを，策定し維持する。
	14.1.2	事業継続及びリスクアセスメント	業務の中断を引き起こしうる事象は，そのような中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定する。
	14.1.3	情報セキュリティを組み込んだ事業継続計画の策定及び実施	重要な業務の中断又は不具合発生の後，運営を維持又は復旧するために，また，要求されたレベル及び情報の可用性を確実にするために，計画を策定し実施する。
	14.1.4	事業継続計画策定の枠組み	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，情報セキュリティ上の要求事項を矛盾なく取り扱うため，また，試験及び保守の優先順位を特定するために，一つの事業継続計画の枠組みを維持する。
	14.1.5	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で効果的なものであることを確実にするために，定めに従って試験・更新する。
法的要求事項の順守	15.1.1	適用法令の識別	各情報システム及び組織について，すべての関連する法令，規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取り組み方を，明確に定め，文書化し最新に保つ。
	15.1.2	知的財産権（ＩＰＲ）	知的財産権が存在する可能性があるものを利用するとき，及び権利関係のあるソフトウエア製品を利用するときは，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を導入する。
	15.1.3	組織の記録の保護	重要な記録は，消失，破壊及び改ざんから保護する。
	15.1.4	個人データ及び個人情報の保護	個人データ及び個人情報の保護は，関連する法令，規制，及び適用がある場合には，契約条項の中の要求に従って確実にする。
	15.1.5	情報処理施設の不正使用防止	認可されていない目的のための情報処理施設の利用は，阻止する。
	15.1.6	暗号化機能に対する規制	暗号化機能は，関連するすべての協定，法令及び規制を順守する。
セキュリティ方針及び標準の順守，並びに技術的順守	15.2.1	セキュリティ方針及び標準の順守	各分掌を代表する主任（主幹）は，セキュリティ方針及び標準類への順守を達成するために，自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にする。

JIS Q 27002:2006 中項目	JIS Q 27002:2006 小項目	管理策	管理策の概要（一部抜粋，又は要約）
	15.2.2	技術的順守点検	情報システムを，セキュリティ実施標準の順守に関して，定めに従って点検する。
情報システムの監査に対する考慮事項	15.3.1	情報システムの監査に対する管理策	運用システムの点検を伴う監査要求事項及び活動は,業務プロセスの中断のリスクを最小限に抑えるために，慎重に計画を立て，合意する。
	15.3.2	情報システムの監査ツールの保護	情報システムを監査するツールの不正使用又は悪用を防止するために，それらのツールへのアクセスは，抑制する。

第２章

『学校情報セキュリティポリシー策定』取り組み事例

２．１　Ａ県教育委員会での事例
２．２　Ｂ県教育委員会での事例
２．３　Ｃ県教育委員会での事例

本章の事例では，平成１７年度に作成された「学校情報セキュリティ・ハンドブック」を参照し，各学校あるいは教育委員会がセキュリティポリシー策定に取り組んだ具体的な内容を紹介しています。

２．１　Ａ県教育委員会での取り組み事例

２．１．１　学校情報セキュリティポリシー策定に取り組む背景

Ａ県では，県立学校（高等学校，特別支援学校）について，校内ＬＡＮの全校工事と，教員へのパソコン整備が行われることになっています。それをきっかけに，県立学校における教員のＩＣＴ（Information and Communication Technology）活用が確実に伸びることが予想され，情報セキュリティ対策が非常に重要な問題となるでしょう。

しかし現状では，インターネットや，校内ネットワークの利用は，各学校の自主的な判断に委ねられています。

このため，Ａ県教育委員会では，校内ネットワークも含めた「情報セキュリティポリシー」を策定するとともに，学校版の運用基準のひな型を策定し，各学校の教職員一人ひとりにその周知を図っていくことが急務となりました。そこで,『学校情報セキュリティ・ハンドブック』を活用して，情報セキュリティポリシー策定の取り組みを始めました。

２．１．２　　取り組みの概要とスケジュール

Ａ県教育委員会では，まず学校情報セキュリティの現況を把握するために，全校を対象にＩＣＴの利用状況や管理状況などを問うアンケートを実施しました。その後，平成１８年７月に「Ａ県立学校情報セキュリティ対策委員会」を設置。そして，実際に情報セキュリティポリシー策定を行う協力学校を，以下の３校に決めました。

- 県立 ア普通科高校
- 県立 イ職業学校
- 県立 ウ養護学校

その後，８月より対策委員会での協議を始め，上記の協力校３校には，情報資産の洗い出しから脅威への対応策までの過程をまとめた「情報セキュリティポリシー策定手順表」の作成を依頼するなどして，12 月に県立学校全体に適用するポリシー（Ａ県立学校情報セキュリティポリシー）の素案をまとめるに至りました。以下は，その経緯を一覧にした表です。

月	会議等名	内容
平成 18 年 7 月	情報化に関する調査	全校への調査 ・個人所有パソコンの利用状況 ・個人所有パソコンの管理状況 ・校内での利用規程の策定状況 ・ネットワーク担当者のスキル
7 月	Ａ県立学校情報セキュリティ対策委員会設置	委員構成 総務課，高等学校教育課，特別支援教育課 総合教育センター 高等学校（教諭）２名，養護学校（教諭）１名
8 月	第１回対策委員会	アンケート調査の結果報告 →学校の現状把握 協議内容 ・セキュリティポリシーの対象範囲 （紙媒体，学校独自のネットワークやスタンドアロンの取り扱い） ・個人所有パソコンの取り扱いについて ・校内ＬＡＮの管理方法 第２回委員会までの課題 ⇒（県教委）県立学校全体に適用するポリシーの素案を策定 （学校）情報資産の洗い出し，学校における脅威，脅威に対する対応策を行う
9 月	第２回対策委員会	報告 （学校）情報資産の洗い出し，学校における脅威，脅威に対する対応策 （県教委）県立学校全体に適用するポリシーの素案 協議内容 県立学校全体に適用するポリシーのうち，重要と思われる内容を検討 ・個人所有パソコンの利用制限

		・端末の登録・変更・抹消・管理（個人所有を含む） ・ソフトウエアのインストールの制限 ・校内ネットワークの拡張の制限 ・学校内での実務担当者の人数 第３回委員会までの課題 ⇒（県教委）県立学校全体に適用するポリシーの素案を策定
11 月	第３回対策委員会	協議内容 ・県立学校全体に適用するポリシーの内容確認 ・「学校情報セキュリティ・ハンドブック」への提案・意見 →12 月「学校情報セキュリティポリシー策定・運用事業」実施報告書で提出 第４回委員会までの課題 ⇒（学校）実施手順書を策定
平成 19 年 1 月	第４回対策委員会	協議内容 ・県立学校全体に適用するポリシーの内容確認 ・委員校で策定した実施手順書と県立学校全体に適用するポリシーとの整合性 ・全校で実施手順書をスムースに策定できるようにするための提案・意見
3 月	第５回対策委員会	協議内容 ・実施手順書の雛形について

なお，上記７月に実施したアンケート結果では，

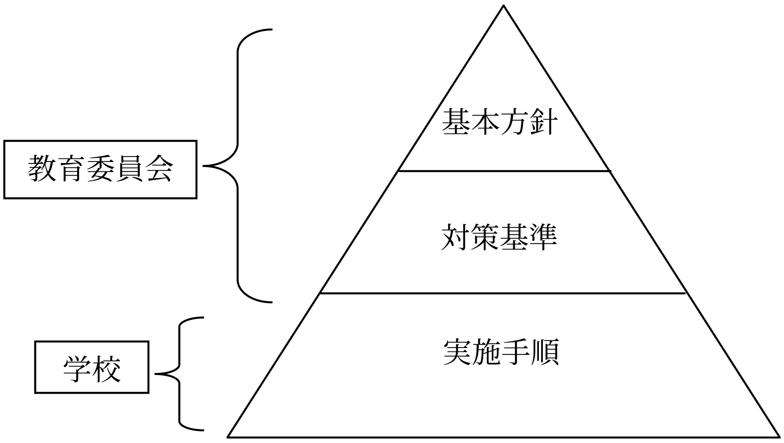
- 個人所有パソコンが約２人に１台程度利用（約 60%が Windows XP Home）
- 個人所有パソコンのネットワーク接続に対して管理をしていない　約 20%
- 校内での利用規程を定めていない　約 55%
- ネットワーク担当者がサーバを操作したことがない　約 50%

といった状況が明らかになりました。A県の学校情報セキュリティ対策委員会の

協議は，こうしたアンケート結果を踏まえたうえで進められました。

２．１．３　『学校情報セキュリティ・ハンドブック』の活用と課題

先述した「Ａ県立学校情報セキュリティポリシー」の素案をまとめるまでの経緯でも示したように，Ａ県では教育委員会が学校全体に対し統一的なポリシーを示し，学校はそのポリシーに沿った実施手順書を策定する，という方法で取り組みました。これは，Ａ県には 100 を超える学校があり，学校ごとにポリシーを策定して，県のポリシーと整合性をとる，という方法が困難と思えるからです。学校に対し統一的に示すべき内容については教育委員会より示し，その一方で教育委員会より統一的に示すことが困難な運用面については，各学校の実情（ネットワーク構成・端末・スキル・校種など）に応じて示す方法をとっているのです（下図参照）。



取り組みの協力校となった３校では，『学校情報セキュリティ・ハンドブック』の内容を活用し，「学校における情報セキュリティ脅威」と「リスク対応策」を作成しました。学校内にはどのような情報資産があるか，洗い出しを行い，その情報を守る必要性について「大」「中」「小」の３段階で重要度を示しました。また，脅威へのリスク対策の必要性についても「大」「中」「小」で重要度を示しました。

以下は協力校３校から，その作業報告の要約です。

〈県立 ア普通科高校〉

情報資産洗い出しの作業を，８月の職員打合せ(朝礼)の際，『セキュリティ・ハンドブック』（Ｐ８～Ｐ11）を印刷したものを用いてお願いした。校務運営委員会の際も教頭より主任に依頼した。

洗い出した情報の範囲は，文書作成に関わったデータまでを洗い出し，また将

来を考えて紙面データについてもできるだけ洗い出すこととした。

情報を守る必要性の判断基準は，基本的には各分掌で判断することとした。概ね個人情報を含むものが「大」となったが，その中の判断は難しく，判断基準が分掌ごとに委ねられていたため統一的な判断には至らなかった面もある。

対策の必要性の判断基準については，個人情報が含まれるものを「大」として，ネットワーク上にあるものも「大」とした。

作業を進める上で気づいたことは，判断基準を明確に示さないと，「大」「中」「小」を決定できないこと。洗い出しの考え方がまちまちなので，統一した考え方を示す必要があるということである。

〈県立 イ職業学校〉

８月，運営委員会にて各分掌主任に情報資産の洗い出しの作業を依頼した。『セキュリティ・ハンドブック』のコピー（抜粋）を各分掌主任に配布し，趣旨を説明後，情報資産の調査票の提出を教頭先生から依頼。８月の職員会にて周知し，各分掌に情報資産の調査票の提出を依頼している旨を，職員に教頭先生から報告した。

洗い出した情報の範囲は，各分掌で把握している文書のうち，電子媒体によって管理されているもの。及び，紙媒体で管理されているものであっても作成途上に電子媒体を使ったものとした。

情報を守る必要性の判断基準では，個人情報または機密情報を含む情報を「大」，個人情報または機密情報を含まない情報を「小」とし，対策の必要性の判断基準は，多くの職員が扱う情報は「大」とした。

判断基準を決定する作業が一番困難で，情報の管理媒体（ＭＯ・ＵＳＢメモリか，サーバ上か），情報をネットワーク接続したパソコン端末で扱うか否か，情報の管理者・管理場所が明確に決まっているか否かを判断基準に用いた。

〈県立 ウ養護学校〉

情報資産の洗い出し作業を個人情報保護委員会の中に位置付けて，集約する情報の範囲を「個人情報を含むもの」から「学校で取り扱うすべての情報」に拡大して取り組んだ。それに合わせるかたちで個人情報の取り扱いに関するガイドライン及びセキュリティについて文書を作成，８月に個人情報保護委員会で配布し，情報資産を洗い出す手順を説明した。洗い出しは，部主事と分掌主任を中心に行った。本作業を行うことを事前に連絡し，終日，効率よく作業を進めた。

作業は，ファイルサーバを開いてファイル名を確認，指定したエクセルシート内へ打ち込んでいくという方法が大半だった（同校では，情報資産は，あらかじめファイルサーバ内の決められたフォルダに保存するように義務付けられている）。この作業は，ファイルサーバ内のファイル名をＣＳＶファイルに集約して出力するスクリプトがあると便利だと感じた。洗い出す情報の範囲は，各部主事や各主任が保有している情報で，作成を終えたもの（完結したもののみ，メモは含まない）とした。

情報を守る必要性の判断基準は，以下のようにした。

「小」についての判断基準は，消えてもよい情報（消されてもよい情報）または，リサイクル（リユース）されない情報。公開されてもよい（一般公開されている）情報，希望者または一般に配布している情報も「小」の扱いとした。

「中」についての判断基準は，リサイクル（リユース）される情報，消えると困る情報であると決め，そうした情報の取り扱いはパスワードなし，暗号化なしで，ファイルサーバに保存（定期的にバックアップ）することとした。紙面については，一般のごみとして廃棄可，また持ち出し可とした。

「大」についてはリサイクル（リユース）される情報，消えると困る情報かつ個人情報を含むもの（公開されると困る情報）であると基準を決めた。取り扱い方法は，各ファイルについてはパスワード付きで保存し，持ち出す場合は暗号化する。個人情報については，データベースサーバに管理し，紙面については鍵のかかる金庫に保管することとした。持ち出し不可，盗み見，盗み聞きなどについても配慮を怠らないようにすること，盗難，紛失，情報漏えい時は教育委員会へ報告をすることとした。

対策の必要性の判断基準では，情報資産を個人所有の媒体やクライアントＰＣに保存して管理している場合と，個人情報を含む情報資産をファイルサーバで管理している場合を「大」とした。個人情報を含まない情報資産をファイルサーバで管理している場合（アクセス制限あり，ファイル単位で複写，変更，削除可能）を「中」とし，データベースサーバで情報資産を管理している場合（アクセス制限あり＝管理者のみ，ファイル単位で複写，変更，削除不可能）を「小」とした。

こうした作業を進める中で，校内で扱う情報資産は，①記入様式の作成（ワープロ），②様式に記入（手書き），③記入されたものを電子情報化（ワープロ，表計算，データベース）といった手順を踏んで作られることが多いということがわかった。これらの情報資産は，同じ情報資産名が付けられていても，記入された内容により，重要度が異なる。

例えば，「児童生徒個票」である。保護者に配布する様式は，ワープロで作られ，配布を前提としたものなので，漏洩の脅威はない。また，ほとんど変更すること

はないが，なくなっては困る（消失の脅威）ので，重要度は「中」となる。

個人情報が記入された後も「児童生徒個票」と，名前は変わらないが，漏洩しては困るので，重要度は「大」となる。収集した個人情報を電子情報化する場合も，ワープロや表計算で一覧表にまとめたり，データベースに入力したりと使いやすいように整理したものが該当し，漏えいしては困るので重要度は「大」となる。

これ以外にも，学級通信や学年通信など公開を前提とした情報がある。配布するまでは，なくなると困る情報なので重要度「中」。配布後は，役目を終えるので「小」となる。今回は，作成途中の情報は，洗い出しの範囲外としたので「小」とした。

２．１．４　学校情報セキュリティポリシーの策定

こうした協力校３校による情報資産の洗い出しや，脅威への対応策に関する報告を検討の材料として，Ａ県教育委員会では，県立学校全体に適用するセキュリティポリシーの策定へ向けて協議しました。個人所有のパソコンの利用制限や，ソフトウエアのインストールの制限など, 重要と思われる内容を中心に検討を重ねていき, セキュリティポリシーの策定を進めました。

２．１．５　今後のセキュリティポリシー実施の予定

上記の県立学校Ａ県立学校情報セキュリティポリシーは, 平成19年度中に施行する予定となっています。先に述べた協力校３校は，素案をもとにして実施手順を策定していきます。

また，平成19年度の早い時期にセキュリティポリシーに関する説明会も開き，全校に実施手順の策定を依頼する予定です。

なお，今回策定した学校情報セキュリティポリシーは，実効性を確保するため，学校の現状（ネットワーク構成・端末・スキル・校種など）を踏まえたものであり，今後，利用者やネットワーク担当者のスキルや意識の向上により，ポリシーを改善する余地は多く存在するでしょう。そのため利用者やネットワーク担当者のスキルや意識の向上を推し進めるとともに，その時々の学校の現状に合わせて，ポリシーもより強固にしていくことが，これからの課題と言えます。

２．２　Ｂ県教育委員会での取り組み事例

２．２．１　学校情報セキュリティポリシー策定に取り組む背景

Ｂ県の県立学校では，平成15年３月に，「県立学校校内ＬＡＮ概要及び利用にあたってのガイドライン」が示されたものの，具体的な情報セキュリティポリシーについては策定されていません。現在，県立学校の情報ネットワークの構築について検討中ですが，Ｂ県教育委員会として，県立学校におけるセキュリティポリシーの策定が喫緊の課題となっています。

また生徒情報などの情報資産の取扱いについて，一定のルール化は図られていますが，教員一人ひとりの情報セキュリティに関する意識は十分と言えない状況です。実際，情報処理業務の増大や校務用パソコンの不足を背景に，教員が個人のパソコンを家庭と学校の両方で使用しているケースや，ネットワークに接続しないでパソコンを使用している場合でも担当クラスの成績を処理しているケースが見られています。そうしたケースでは，個人情報漏洩の危険性が高いと言わざるを得ません。

このため，Ｂ県教育委員会では，『学校情報セキュリティ・ハンドブック』を活用して，統一された県立学校向け情報セキュリティポリシーを策定し，普及を図ることにしました。校内ＬＡＮ・校務ＬＡＮで整備されたパソコン・ネットワークについても，県立学校間で一定水準のセキュリティを確保するためにポリシーを策定し，情報資産の適正管理を図ります。

２．２．２　取り組みの概要とスケジュール

Ｂ県教育委員会では，平成 18 年７月５日，まず学校情報セキュリティポリシー策定委員会を設置しました（事務局＝Ｂ県教育委員会総務課）。策定委員会の構成員は，Ｂ県教育委員会総務課から２名，学校教育課２名，施設課１名，教職員課１名，総合教育センター２名のほかに，県立学校６校から２名ずつの代表者が加わり，合計 20 名。また，実際に『学校情報セキュリティ・ハンドブック』を活用してセキュリティポリシー策定を試みる協力校として，以下の県立学校６校に依頼しました。

- 県立　ア普通科高校
- 県立　イ普通科高校
- 県立　ウ総合学科高校

- 県立 エ商業高校
- 県立 オ養護学校
- 県立 カ定時制高校

その後，Ｂ県教育委員会では７月18日に第１回の学校情報セキュリティポリシー策定委員会を開催し，策定に向けて具体的な協議に入りました。９月20日から10月６日にかけては，上記の協力校６校の非常勤を除く教職員（教諭，実習助手，講師，栄養職員，寄宿舎職員）を対象に，情報セキュリティに関する意識調査のアンケートも実施しました。そして第１回と第２回の委員会の協議と，アンケートの実施結果を受けて同事務局がＢ県立学校情報セキュリティポリシーの原案を作成し，平成19年１月11日の第３回委員会での協議を経て「素案」が固まりました。以下に，同委員会の経緯をまとめました。

・第１回委員会（平成18年７月18日＝Ｂ県総合教育センター411研修室）

議題 ・委員会設置の趣旨について
　　 ・今年度の年間計画について
　　 ・情報資産の調査について
　　 ・その他

・第２回委員会（９月11日＝Ｂ県総合教育センターパソコン室）

議題 ・各学校における情報資産の確認
　　 ・リスク対応策の検討
　　 ・その他

・第３回委員会（平成19年１月11日＝Ｂ県総合教育センターパソコン室）
議題 ・Ｂ県立学校情報セキュリティポリシーについて
　　 ・実施手順書について
　　 ・その他

なお，その後，協力校６校では，学校情報セキュリティポリシー実施手順書を作成しているところです。

２．２．３　『セキュリティ・ハンドブック』の活用と課題

先述した取り組みのスケジュールの中でも示したように，Ｂ県教育委員会では協力校６校の非常勤を除く教職員を対象に，情報セキュリティに関するアンケートを実施しました。その結果をＢ県立学校情報セキュリティポリシーに反映させるのが目的であり，アンケートは合計 32 の質問から成っています。以下は，その質問内容と，協力校のうちの**県立ア普通科高校からの回答例**です。

〔組織体制について〕

Ｑ１：自分が取り扱う学校内の情報資産にはどのようなものがあるのか把握していますか？

全て把握している	だいたい把握している	把握していない
12.5%	64.6%	22.9%

Ｑ２：自分が取り扱う学校内の情報資産について，それぞれの情報資産の管理責任者が誰になっているか把握していますか？

全て把握している	だいたい把握している	把握していない
4.4%	50.0%	45.6%

〔教職員のセキュリティについて〕

Ｑ３：情報漏洩等の可能性がある事件や事故に遭遇した場合，連絡体制や対処法等について理解していますか？

はい	いいえ
27.7%	72.3%

Ｑ４：セキュリティ確保するための学校内の取り決めについて理解していますか？

はい（Ｑ５へ）	いいえ
50.0%	50.0%

Ｑ５：Ｑ４で「はい」と答えた方のみ答えてください。取り決めを実行していますか？

全て実行している	おおむね実行している	実行していない
12.5%	87.5%	0.0%

Ｑ６：見ず知らずの人が部屋を訪ねてきたときにどう対応しますか？

すぐ入れる	確認してから入れる	入れない
0.0%	83.0%	17.0%

Ｑ７：あなたはパソコンやインターネットで使用するパスワードを第三者に知られないように管理していますか？

はい	いいえ
97.9%	2.1%

Ｑ８：同じパスワードをどのくらい使っていますか？

１ヶ月未満	３ヶ月未満	６ヶ月未満	６ヶ月以上
0.0%	0.0%	9.1%	90.9%

Ｑ９：パソコンを使用し終わって席を立つ時には，必ずログオフあるいはシャットダウンを行っていますか？

いつも行っている	たまに忘れることもあるが意識している	行っていない
23.4%	29.8%	46.8%

Q10：個人所有のパソコンを学校内に持ち込んだことがありますか？

ある	ない
52.3%	47.7%

Q11：個人所有のパソコンを校内ＬＡＮ等の学校内ネットワークに繋いだことがありますか？

繋いだ	繋がなかった
4.2%	95.8%

〔パソコンの設定について〕

Q12：あなたはパソコンのファイル共有の設定方法を知っていますか？

はい	いいえ
22.9%	77.1%

Q13：ウインドウズアップデートについて知っていますか？

はい（Q14へ）	いいえ
47.8%	52.2%

Q14：Q13で「はい」と答えた方のみ答えてください。家庭のパソコンは定期的にウインドウズアップデートを実施していますか？

はい	いいえ
70.8%	29.2%

Q15：家庭のパソコンにウイルス対策ソフトを導入していますか？

はい（Q16へ）	いいえ
68.8%	31.2%

Q16：Q15で「はい」と答えた方のみ答えてください。今までに警告が出たことがありますか？

はい	いいえ
45.5%	54.5%

Q17：家庭のパソコンにスパイウェア対策ソフトを導入していますか？

はい（Q18へ）	いいえ
29.8%	70.2%

Q18：Q17で「はい」と答えた方のみ答えてください。今までに警告が出たことがありますか？

はい	いいえ
35.7%	64.3%

Q19：インターネットから，ダウンロードしたソフトウエアを個人のパソコンにインストールしたことがありますか？

ある	ない	わからない
48.9%	44.4%	6.7%

Q20：ウィニー等のファイル共有ソフトを家庭のパソコンで使っていますか？

はい	いいえ
０.０%	100.0%

〔データの取り扱いについて〕

Q21：ＵＳＢメモリやフロッピーディスク等にデータを入れて持ち歩いていますか？

はい（Q22へ）	いいえ
６９.６%	30.1%

Q22：Q21で「はい」と答えた方のみ答えてください。データにパスワードあるいは暗号化等のセキュリティ対策を行っていますか？

はい	いいえ
12.5%	87.5%

Q23：職務上の重要データや生徒の個人情報のデータ等をコピーして利用する場合，保存場所や保存回数などを自己管理し，必要に応じて削除等を行っていますか？

いつも行っている	たまに忘れることもあるが意識している	行っていない
42.6%	46.8%	10.6%

Q24：生徒の連絡先や成績等の個人情報が載っている手帳や資料などを，机上など第三者の目に触れるところに置きっ放しにしていませんか？

いつもしている	時々してしまう	していない
8.5%	44.7%	46.8%

Q25：家庭のパソコン及びハードディスク，ＣＤ等の記録メディアを廃棄するときに，データが漏洩しないように完全消去ソフト等を使ってデータを消去したり物理的に破壊したりするなど対策を行っていますか？

いつも行っている	たまに忘れることもあるが意識している	行っていない
46.8%	31.9%	21.3%

Q26：学校でパソコン等を使用して行う仕事は平均で１日に何時間くらいになりますか？

１時間未満	１～２時間	２～３時間	３時間以上
19.1%	51.1%	23.4%	６.４%

Q27：自宅でパソコン等を使用して行う仕事は平均で週に何日くらいになりますか？

１日	２日	３日	４日	５日	６日	７日
37.2%	20.9%	16.3%	7.0%	9.2%	4.7%	4.7%

Q28：自宅でパソコン等を使用して行う仕事は平均で１日に何時間くらいになりますか？

１時間未満	１～２時間	２～３時間	３時間以上
53.3%	37.8%	8.9%	０.０%

Q29：自宅でパソコン等を使用して行う仕事は主にどんな内容ですか？

教材研究	問題作成	成績処理	校務分掌の仕事	学年の仕事
26.0%	29.0%	４.０%	13.0%	4.0%

クラス担任の仕事	部活動の仕事	研修	その他
８.０%	6.0%	6.0%	4.0%

Q30：全教職員が，個人情報保護条例や情報セキュリティポリシーをよく理解し，遵守するためにはどんなことが必要かと思いますか？

・個々の規範意識の向上が必要
・ポイントを具体例で説明すると言った共通理解を図る現職教育・校内研修会が必要
・具体的内容が分かるようにすることが必要
・学校のパソコンを教職員全員分そろえ使用させ，ソフト・ハード的にセキュリティ対策をとり，使用方法を確認することが必要
・どんな問題（事故・事例）が起きているか知ることが必要
・分かり易いガイドライン・パンフレット等の作成をして，年度当初に全職員に周知を図る
・県立学校全部に対して一つのシステムで対応できる専門の組織をつくる必要がある（各学校に任せるのは無理）

- 入退室の管理を含め，独立したパソコン室の設置，机上以外に書類等の保管できる部屋の確保，専門管理者・オペレーターの雇用必要など
- 全員が個人パスワードを使用したり，個人の関係文書等の管轄・管理を全体で把握する必要
- 人権尊重について常に考える。セキュリティポリシー実施のための周辺整備，机の鍵，棚・収納庫等の整備を図る。

Q31：１週間（５日間）の勤務時間の内訳について，合計時間を0.5時間単位で記入して下さい。

授業	15.9時間	〔うちＰＣ処理0.3時間〕
教材研究	10.9時間	〔うちＰＣ処理3.3時間〕
校務分掌	7.9時間	〔うちＰＣ処理3.3時間〕
部活動	5.7時間	〔うちＰＣ処理0.3時間〕
会議・打合せ	2.3時間	〔うちＰＣ処理0.1時間〕
その他	4.7時間	〔うちＰＣ処理0.5時間〕

Q32：勤務時間内におけるＰＣ処理の内容について記入して下さい。

- 教材（プリント他）作成
- 問題作成
- 成績処理
- 会議資料等文書作成
- 生徒データの加工
- 校務分掌

アンケートの各32問に対する回答の割合は，その他の協力校（５校）においても同様の傾向を示しています。また協力校では，『学校情報セキュリティ・ハンドブック』の内容を活用し，それぞれに学校内の情報資産管理表を作成しています。それらもまたＢ県立学校情報セキュリティポリシーの検討資料としました。情報資産の洗い出しを行い，その情報を守る必要性について「大」「中」「小」の３段階で重要度を示しました。

以下は，協力校６校のうち，県立ア普通科高校の情報資産管理表（一部）です。

学校内の情報資産管理表

県立ア普通科高校

校務分掌	情報資産	管理部署	保存形態	保管場所	主な記載内容	PC処理	公開の範囲	重要度	守るべき情報資産	保存年限	備考
教務部	学則	教務部	紙	職員室ロッカー	学則		一般	小		常用	
教務部	教育計画	教務部	紙	職員室ロッカー	教育計画			大	○	3年	
教務部	学校要覧(配布用)	教務部	紙	職員室ロッカー	教育方針、教職員名簿等		一般	小		常用	
教務部	学校案内	教務部	紙	職員室ロッカー	教育方針、カリキュラム等		一般	小			
教務部	研究紀要「××」他報告書	教務部	紙	職員室ロッカー	色々な報告、研究内容		一般	小			
教務部	出席簿	教務部	紙	倉庫	出欠の記録			大	○	5年	
教務部	出席統計表	教務部	紙･電子媒体	校務LAN共有フォルダ他	各クラスの出席統計	○		中			
教務部	各年度のクラス担任･在籍数	教務部	紙･電子媒体	各教職員、担当教職員ロッカー等	変更時のクラス担任･在籍数	○		小			
教務部	転編入学関係綴り	教務部	紙	職員室ロッカー	考査結果等			大	○	5年	
教務部	学校日誌	教務部	紙	職員室ロッカー	行事記録等			小		3年	

こうした情報資産管理表の作業を実施していく過程において，その作業の効果と問題点が協力校６校それぞれで明らかになってきました。以下は，各校からの報告の要約です。

〈県立 ア普通科高校〉

ａ．実施した事による効果

・多様な情報資産があることを改めて認識した。

・情報資産の保護・管理の必要性，重要性を認識した。

ｂ．実施作業における問題点

・徹底した情報資産の洗い出しに関しては，各部署の協力が必要である。

・洗い出した情報資産の確認，及び係としてのフィードバックに務める。

・管理部署を確定しにくい情報資産がある。

・重要度の観点が大切である。

・洗い出しが的確であったかどうか不安な点がある。

・何を守るべき情報資産とするか，随時見直しの必要性がある。

〈県立 イ普通科高校〉

ａ．実施した事による効果

・文書やデータの所在が明らかになった。

・個人情報が含まれる情報資産が多いことが明らかになった。

・一部職員は「情報セキュリティ」の重要さが認知できた。

b．実施作業における問題点

・担当者で全て調査ではなく，各部でチェックという形式にならざるを得ない。

・個人所有のＰＣやＵＳＢメモリ等に保存されているデータまでは確認できていない。

・全職員への周知がなく「何でこんな事やるの？」という冷ややかな反応も。

・事務室で扱っている文書やデータには全く触れていない。

・ 情報資産の洗い出しは，実施手順書の一部に過ぎないのだから，ポリシーがおおむね策定した後でも良かったと思う。

〈県立 ウ総合科学科高校〉

a．実施した事による効果

・改めて学校に多くの情報が存在することを認識した。しかも，その情報の管理に曖昧なものが多く存在することが分かった。

b．実施作業における問題点

・複数の部にまたがる情報の扱いについて調整が難しいものがある。

・情報の持ち出し（流出）をどのように管理するか。情報の削除（保存期限の過ぎたものの破棄など）をどうしたらいいのか。学校の現場で判断するのは困難。

・情報をきちんと管理するためには物理的スペース（ファイルキャビネット等）や多数の校務専用コンピュータが絶対に必要。

〈県立 エ商業高校〉

a．実施した事による効果

・重要な情報資産の管理場所を特定するとともに，管理責任者を特定することができた。

b．実施作業における問題点

・各部の担当者以外，情報資産の量・種類・所在がわからず，洗い出し作業自体担当者に全て任せてしまう事になってしまった。

〈県立 オ養護学校〉

a．実施した事による効果

・学校情報資産の把握ができた。

・それらにより管理の徹底を図れるような体制が整った。

・校務分掌の職務分析と，保管帳簿の作成が容易にできるようになった。

b．実施作業における問題点

・職員間の意識の格差。

・策定内容や，手順書を見ると，学校裁量の部分が多いように感じる。

・今回の策定については，校内ＬＡＮのように，各校の独自性を出して行うことも必要かとは思うが，基準は県としての方針を表記して，運用に関しては各学校裁量という形にしていかなければと感じている。なぜなら，職員の定期異動を考えると，異動する学校間でやり方が異なるのはいかがなものかと思う（県の出先機関でもやり方は同様かと）。

・若い職員や，情報関係に明るい職員なら，順応性が早いが，苦手としている職員をはじめ，年配の方には学校間で相違する内容はいかがなものかと思う。また，語句の理解がそれぞれに異なることが理解の相違を生じているかと思う。「個人情報」の語句にしても，どこまでの範囲なのか，そういったことをしっかり踏まえた上で，研修にしろ，策定にしても行っていかなければならないと感じる。

〈県立 カ定時制高校〉

ａ．実施した事による効果

・情報資産の洗い出しによって，校務分掌上，どんな書類があり，重要なのかを再確認することができた。

・重要書類を，どのように管理することが大切なのかを，考える機会を設けることができた。

・職員の意識が高まったようである。

ｂ．実施作業における問題点

・ 各部で多忙なために，情報資産の洗い出し作業にかなりの時間を必要とした。

・書類については，今年度異動してきた人もあるので，どこにあるか，わからないこともあった。

２．２．４　学校情報セキュリティポリシーの策定

このような協力校６校による報告などを検討材料として，Ｂ県教育委員会では，県立学校に適用するセキュリティポリシーの策定へ向けて協議しました。

２．２．５　今後の予定と課題について

Ｂ県の県立学校のネットワーク環境は，平成19年度から県立学校間のイントラネット整備などによって改善されることが予想されています。学校情報セキュリティポリ

シーをより実効性を高めたものにするためには，イントラネットの整備内容を踏まえたうえで策定することが望ましいと言えます。そのようなハード面の状況は時間の経過とともに大きな違いが出てくることも予想されるので，それに合わせて学校情報セキュリティポリシーの内容も随時見直していくことが大事です。

Ｂ県教育委員会では，今回の取り組みの中で基本方針や対策基準の骨子が作成でき，また協力校においては情報セキュリティに関する職員の意識の改善が図れるなど，大きな成果を残すことができました。平成19年度には，県立学校間のネットワーク環境を踏まえ，今回の成果をもとにＢ県立学校情報セキュリティポリシーを策定することを計画しています。

２．３　Ｃ県教育委員会での取り組み事例

２．３．１　学校情報セキュリティポリシー策定に取り組む背景

Ｃ県では，県教育委員会が平成17年度末，県立学校と市町村県教育委員会に対し，ファイル共有ソフトの使用を禁止して個人情報漏洩の防止に努めるよう通知を出しており，また，県立学校への学校訪問を実施したり小・中学校の情報教育担当者会を開催したりして，情報セキュリティについての研修も実施しています。

しかし，Ｃ県の県立学校では，情報セキュリティポリシーを策定し，運用を行っている学校は少ない状況です。小・中学校においてもセキュリティ意識が低く，管理者アカウントをパスワードなしで使っている学校も多数見られます。

こうした状況は学校運営上大きな問題であり, 早急な情報セキュリティポリシーの策定が望まれることは言うまでもありません。

実効性のある学校情報セキュリティポリシーの運用を確保するには, 県教育委員会として必要な支援を行うことが大事です。そこで，Ｃ県教育委員会では，『学校情報セキュリティ・ハンドブック』を活用して，各校種・地域に対して情報セキュリティポリシーの策定と実質的運用が行われるまで支援を行うことになりました。

２．３．２　取り組みの概要とスケジュール

Ｃ県教育委員会では, まず, 以下の７つの学校･市町村教育委員会などに対して,『学校情報セキュリティ・ハンドブック』を活用しながら各校種・地域の実情に応じたセキュリティポリシーを策定するよう協力を依頼しました。

- ア市教育研究所
- イ市教育委員会
- ウ市教育委員会
- エ教育ネットワークセンター
- 町立オ小学校
- 県立カ養護高校
- 県立キ学校

そしてＣ県教育委員会は，上記の協力校・機関の代表者を委員とし，県内の教育大学の教授を委員長とする「Ｃ県学校情報セキュリティ検討委員会」を設置して，

各校種・地域に対し学校情報セキュリティポリシーの策定と実質的運用を支援するための体制を整えました。上記の７つの協力校・機関の取り組みの成果を「モデル」にして，県全域への普及を図ることにしたのです。

Ｃ県学校情報セキュリティ検討委員会は，平成18年７月28日の第１回協議から，12 月 15 日までに合計３回，情報提供，ワークショップ，実施報告，意見交換などを中心に協議を行いました。

２．３．３　『学校情報セキュリティ・ハンドブック』の活用と課題

先述した取り組みの概要でも示したように，Ｃ県教育委員会では，７つの協力校・機関に，各校種・地域の実態に応じて，『学校情報セキュリティ・ハンドブック』を活用しながらセキュリティポリシーを策定してもらう方法で取り組みを進めたので，策定方法や現段階までの実績についても各学校・機関で特徴的なものとなっています。以下は，各学校・機関の実施体制や実績，今後の予定をまとめた表です。

学校・機関	体制	実績	今後の予定
ア市教育研究所	教育研究所研究生１名，委嘱所員（小学校教諭）１名で研究	ポリシー試案（教職員用チェックリスト等）作成	学校全体で作成方法が検討できるよう協力校に研究を依頼し，各学校での作成に努める
イ市教育委員会	幼稚園（１園），小学校（１校），中学校（１校）に研究を依頼し，教育研究所（担当指導主事１名）と連携	各指定園・校においてポリシー作成中	市校長会，市園長会の承認を得て，市内各幼稚園・小・中学校でのポリシー作成
ウ市教育委員会	市内の３小学校に策定を依頼し，教育委員会（情報教育担当主査１名）と連携	ポリシー案を市内６小中学校で検討・修正し最終案作成	市教委としてのポリシー策定及び，市内各校でのポリシー策定と実践
エ教育ネットワークセンター	小学校１校を校内研修実施校として	計３回の校内研修でポリシー案作成	研修実施校を増やし，域内での枠組み

	依頼し，ネットワークセンターの担当者が校内研修に入り，策定		を検討するとともに，担当者会，情報視聴覚部会などを活用して研修を実施
町立オ小学校	校内企画委員会が，情報セキュリティポリシー策定委員会として機能	情報資産分類，運用規定策定	郡の校長会へ提案
県立カ養護学校	個人情報管理委員会の業務の中で，セキュリティポリシー策定･運用も検討	ポリシーの策定・試行	運用，見直し，改訂を実施するとともに，個人情報管理委員会による継続した審議，システム改善
県立キ高校	「セキュリティポリシー作成委員会」で原案作成，「情報セキュリティ委員会」で案の検討，「校務運営委員会」で決定	ポリシーの策定・試行	毎年，情報資産の洗い出しやポリシーの改訂を実施

各学校・機関の実績を見るとわかるように，いずれの学校・機関でもポリシーの完成・運用には，まだ至っていません。C県教育委員会で当初目的とした「モデル」の県全域への普及はこれからの課題です。しかし，『学校情報セキュリティ・ハンドブック』を活用する情報セキュリティポリシー策定の過程では，その啓発は確実に行われています。この取り組みを通じて得られたメリットとして，C県教育委員会は以下のような点を挙げています。

- 情報資産の洗い出しや，脅威・対策を考える際，いずれの学校でも全教員が何らかの形で関わっており，今まで関心が薄かった「情報セキュリティ」について共通理解が図れた。
- 当初研究を指定した学校以外にも働きかけるなど，学校間での広がりが見ら

れる。

- 地域の情報担当者会や教頭会で情報セキュリティに関する研修会を開催し，危機意識を喚起した。
- 地域の視聴覚情報部会でワークショップを実施するなど，作成方法についても啓発した。
- 指定校を決める際，市幼稚園長会，市教育用コンピュータ活用推進協議会，市中学校教育研究会視聴覚情報教育部会等と協議することにより，セキュリティポリシー策定の必要性をアピールした。
- 今後，協力いただいた市町村教育委員会では，地域の校長会，情報担当者会や教育研究会情報教育部会などをとおしてセキュリティポリシーの紹介・研修や作成依頼することを計画しており，地域での広がりが期待できる。

もちろん，このようなメリットばかりでなく，取り組みの中から諸課題も浮かび上がってきました。７つの協力校・機関から指摘があった課題を列挙してみます。

- ボトムアップからのアプローチとトップダウンのアプローチからポリシーが作成され，運用される事が重要。
- 地教委が年度途中から新たな研究活動を学校に依頼するのは難しい。
- 地教委において，異校種間で統一的に進める場合，環境・リテラシーの差は予想以上に問題となる。
- ポリシーを作成したメンバーが在籍しているときは緊張感を保てるが，時間がたつと薄れてしまう。
- 小規模校ではポリシーの業務に関わることでかなりの負担になる。
- 外部評価の必要性。
- 多くの教員が在籍し，情報資産の量も多い学校では全校を挙げての協力体制が必要。
- 学校では，教育という本来の職務に加えて，セキュリティ関連の業務を進めていかなければならず，細かい部分まではできないのが現状。
- 教職員に対して，情報に対する安全管理を企業並みに厳しく要求することは，現段階では難しい。将来的には，専任で関わる校務分掌（あるいは委員会）が設置されるべき。
- 紙の情報資産に偏りすぎる傾向があり，それを作るときのデータファイルが情報資産だと認識されていない。
- 既存のガイドラインやポリシーと整合性をとる必要がある。
- 補助簿など，日常持ち歩く情報資産についての意識が低い。

- 電子媒体と紙媒体両方のポリシーを同時に策定しようとすると労力と時間が足りない。
- 校舎改築のような場合，セキュリティレベルが下がる。
- ポリシー文例の紹介が有効。
- セキュリティ維持のための物品（ネット監視，保管庫など）が必要。
- 個人情報の意図的・組織的な消失に対する対策。
- 情報機器の整備が十分でない場合，検討が難しい。

７つの協力校･機関は, 学校情報に関するセキュリティポリシーを持っておらず, 今回の取り組みが作成の契機になりました。だだ，既存の情報機器使用マニュアルやガイドライン，個人情報保護規程などと整合性をとる必要もあるでしょう。Ｃ県教育委員会ではその点も大きな課題として捉えています。

２．３．４　学校情報セキュリティポリシーの策定

このようにＣ県教育委員会では，７つの協力校・機関に対して，それぞれの環境や実態に応じた学校情報セキュリティポリシーの策定を依頼しました。

２．３．５　今後のセキュリティポリシーの予定

上記のような協力校・機関が策定した学校情報セキュリティポリシーなどをもとにして，Ｃ県教育委員会では，これから全県域に向けて，各校種・地域の環境や運営体制に応じたセキュリティポリシーの普及を図ることにしています。

また，総合教育センターで毎年開催される情報教育担当者会などの機会も利用して，ワークショップを実施するなど普及・啓発に努めることにしています。さらに県立学校については，今回の取り組みの成果を参考にして，Ｃ県教育委員会として基本ポリシーの策定及びセキュリティポリシーの普及・啓発について検討していく方針です。

第３章

『学校情報セキュリティポリシー』例

３．１　セキュリティポリシー例（１）
３．２　セキュリティポリシー例（２）
３．３　セキュリティポリシー例（３）
３．４　セキュリティポリシー例（４）
３．５　セキュリティポリシー例（５）
３．６　セキュリティポリシー例（６）
３．７　セキュリティポリシー例（７）

本章では，教育委員会や学校が作成した情報セキュリティポリシーを紹介しています。それぞれの事例についてポリシーの範囲や詳細度等を記していますので，参考にしてください。

	対象	範囲	ページ数	詳細度	特徴
例（１）	学校	基本方針 対策基準	５	★☆☆	
例（２）	学校	対策基準	３	★☆☆	
例（３）	学校	対策基準	４	★☆☆	
例（４）	学校	対策基準	３	★☆☆	
例（５）	学校	実施手順	１３	★★☆	
例（６）	学校	基本方針 対策基準 実施手順	３６	★★★	申請書等 書式有
例（７）	教育委員会	基本方針 対策基準	２９	★★★	

詳細度：★が多いほど、詳細かつ具体的に記述しています。

３．１　セキュリティポリシー例（１）　：　基本方針・対策基準

○○学校情報セキュリティポリシー

第１章　基本方針

１．目的

教育活動の充実と効率的な校務処理を目指して情報化を推進するに当たり，児童及び保護者，教職員，その他地域住民等，本校関係者の個人情報をはじめとする情報資産を漏洩や改ざん，コンピュータ・ウイルスによるシステム障害などの脅威から守り，安心して児童が勉学に励むことができ，保護者ならびに地域住民から信頼される教育活動を実現するために総合的，体系的，継続的に情報セキュリティ対策を実施する。

２．学校の責務

（１）情報管理責任者の明確化

情報資産毎に情報作成者と情報管理責任者を区分して設定すると共に情報管理責任者の義務及び責任を明確化する。

（２）規程の整備

情報資産の安全を確保するために情報セキュリティに関する校内規程（情報セキュリティ基本方針，対策基準，実施手順書等，以下「情報セキュリティポリシー」という）を整備し，各校務分掌において遵守すべき事項を明らかにする。

（３）リスク分析・評価，情報セキュリティポリシーの見直し

情報化の進展や採用された情報処理技術等の環境変化に対応するため，定期的にリスクの分析と評価を行い，情報セキュリティポリシーの有効性を維持する。

（４）条例・規則等の遵守

情報セキュリティに関する各種条例，通知，情報セキュリティポリシーに関する研修を全教職員に定期的に対して実施し，周知徹底をはかる。

（５）情報セキュリティ向上委員会の設置

上記，各項の取り組みを確実なものとするため，校長を委員長とする「情報セキュリティ向上委員会」を設置し，情報セキュリティ対策の有効性を評価し，必要な改善策を継続的に実施する。

３．管理職及び情報管理責任者の責務

校長は，校長が任命した情報管理責任者の協力を得ながら，学校内における情報資

産及びシステム, ネットワークの円滑な利用とセキュリティを確保するために必要な対策を実施するとともに，教職員に対する意識啓発・教育のための研修を実施する。また，非常事態を想定した対応マニュアルを整備し，定期的に訓練を実施する。

4．教職員の責務

教職員は，校長が実施する情報セキュリティに関する研修を受け（転入者は，転入後速やかに情報セキュリティに関する規程及び実技研修を受けること), これら規程を遵守して情報の作成・管理・運用及び情報システムの利用を行うとともに，システム障害や外部者の不正接続，情報漏洩等を防止するために，使用が認められた機器のみを業務に利用するとともに，定期的に機器類，情報資産の点検を実施する。

また，これらの規程に違反した場合は所定の処分を受けるものとする。

第２章　ネットワーク及び情報機器等の運用管理

1．目的

機密保持及び情報資産の保護, 有効活用のために, 学校内ネットワーク及び情報機器の利用管理を行うことを目的とする。

2．対象者

学校内ネットワーク及び情報機器を利用するすべての教職員（非常勤教職員を含む）

3．利用範囲

ネットワーク及び情報機器の利用は，以下の利用ができる。

- 教職員の事務処理のための利用
- 教育活動のための利用
- 電子メールの利用
- ホームページの開設・更新・閲覧

4．利用できる端末

学校内で利用できる端末等は，以下の要件を満たすものでなければならない。

- 校長が認め，学校として管理するもの
- コンピュータ・ウイルス対策ソフトがインストールされているもの

- ファイル共有ソフト（Ｗｉｎｎｙ，Ｓｈａｒｅ等）をインストールされていないもの

５．電子メールの利用

電子メールの利用にあたっては，以下の内容を遵守すること。

- 電子メールの送受信にあたっては，職務の目的に限定すること。
- 個人情報や機密情報は，原則として電子メールを用いて送信しないこと。
- 電子メールの受信にあたっては，ウイスル対策基準に基づき，電子メール保護機能を有効にすること。
- 送信元不明のメールに添付されたファイル等，不審な添付ファイルを操作しないこと。
- ファイルを電子メールで送付するときは，ファイルのウイルス感染が無いことを確認すること。

６．ホームページの利用

ホームページの利用にあたっては，以下の内容を遵守すること。

- インターネットのアクセスにあたっては，職務の目的に限定すること。
- 職務上不必要なファイルやソフトウエア，不審なファイルをダウンロードしないこと。
- 必要なファイルやソフトウエアであっても，まずダウンロードし，ウイルスチェックを実施してから実行すること。
- パスワードをＷｅｂブラウザに記憶させないこと。
- アクセス制御されたＷｅｂサイトの閲覧時に離籍する場合は，Ｗｅｂブラウザを終了させること。

７．パスワード管理

利用者は，適切にパスワードを管理するため，以下の内容を遵守すること。

- パスワードは秘密にし，他の者に知られないようにすること。
- パスワードはメモしないこと。
- パスワードは，8 文字以上で記号を１ 文字以上含むこと。
- 一般に使われている単語など，他人に推測されやすいパスワードを使用しないこと。
- 設定されたパスワードは３ヶ月に一度以上更新すること。
- パスワードが他の者に知られた場合，又はそのおそれがある場合は，パスワードを速やかに変更すること。

- 過去に使用したパスワードを再利用しないこと。

第３章　情報の管理

１．目的

学校で扱うすべての情報資産について，その重要度に応じた管理を行い，情報の漏洩，改ざん，破壊を防止することを目的とする。

２．対象者

学校の情報資産を扱うすべての教職員（非常勤教職員を含む）

３．文書管理

個人情報や重要な情報が記載された文書は，情報セキュリティ事故の発生を未然に防止するために，以下の内容を遵守すること。

- 重要文書については，保管台帳を作成して管理すること。
- 重要文書を扱う者は，第三者の目に触れぬよう，鍵のかかる場所に保管し，鍵は容易に持ち出しが出来ない場所に保管すること。
- 重要文書が記述されている文書は，裏紙としての再利用を禁止すること。
- 重要文書を廃棄する場合は，焼却・裁断等，記載情報が判読できない形で廃棄すること。
- 職務時間内外を問わず，文書の放置をしないこと。
- プリンタ，複写機，ＦＡＸ機等から出力された文書を速やかに回収すること。

４．記憶媒体管理

個人情報や重要な情報の漏洩を未然に防ぐために，個人情報や重要な情報を格納した記憶媒体（ＵＳＢメモリ，ＭＯ，ＤＶＤ，ＨＤ，等）の管理について，以下の内容を遵守すること。

- 学校は，保管台帳を作成して記憶媒体を管理すること。
- 学校が管理する記憶媒体には，管理責任者，保存場所を記したラベルを貼ること。
- 重要な情報を格納した記憶媒体を管理責任者の許可なく校外へ持ち出さないこと。
- 職務時間内外を問わず，記憶媒体を放置しないこと。

- 重要な情報を格納した記憶媒体は，権限のない者が情報にアクセスできないように暗号化を行うか，媒体を鍵のかかる場所に保管すること。
- 記憶媒体を廃棄する場合は，再生できない方法で消去あるいは再生不可能な状態にしてから廃棄すること。

5．個人情報

個人情報の漏洩防止のため，以下の内容を遵守すること。

- 個人情報を含む情報，すべてのファイルにパスワードを設定し，また必要に応じてファイルまたはフォルダの暗号化を行うこと。
- 個人情報を扱う場合は，スタンドアロンで利用すること。
- 異動の場合は，個人情報を含むすべての情報について，情報を復元できないように消去すること。

第４章　雑則

1．報告

学校が開設したホームページの改ざん等,ネットワーク及び情報機器等の利用について違法な行為が発見した場合は，発見者は，ただちに校長及び情報管理責任者へ報告すること。

生徒等の個人情報の漏えい等が発生又は判明した場合は,ただちに校長へ報告すること。

３．２　セキュリティポリシー例（２）　：　対策基準

○○学校ネットワーク情報セキュリティポリシー

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「情報管理委員会」の設置を行う。

「情報管理委員会」では，以下のことを実施する。

（１）セキュリティ方針や，各教職員の責任の承認・見直し

（２）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

（３）セキュリティに関わる事件・事故の見直し・監視

（４）セキュリティを強化するための取り組みの提案・承認

・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，教育委員会への連絡体制を構築する。

２　情報資産

・情報管理委員会は，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。

３　教職員のセキュリティ

・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。

・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，ソフトウエ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。ソフトウエア誤動作の場合，教育委員会の認可を受けて，疑いのあるソフトウエアを除去する。

・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，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。

4　ハードウエアや環境のセキュリティ

・コンピュータや周辺機器は，盗難・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がないよう設置し，管理する。

・各教職員が，ノート型パソコンを用いるときには，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」「常に最新のウイルスパターンファイルを導入しておく」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。

・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，又は専用ソフト等により確実にデータを消去する。

・コンピュータやデータ，ソフトウエアは，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。

5　ネットワークやソフトウエアの運用管理

・情報管理委員会は，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。

・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。

・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。

・新しいソフトの導入にあたっては，情報管理委員会での検討後，校長の責任において導入する。（ただしファイル交換ソフトは認めない。）

・悪意のあるソフトウエアの侵入を防止し，検出するために，情報管理委員会は，OSのアップデートや対応ソフトのインストールなど，予防の措置を行う。

・極めて重要なデータやソフトウエアのバックアップは，各教職員が定期的に実施する。

・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う。

・情報管理委員会は，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。

・システムに関する文書を保護するために，情報管理委員会は，その管理策を策定する。

- 情報管理委員会は，電子メールの明確な利用ルールを作成する。
- ホームページ等を通じて情報を公開している場合，情報管理委員会は，その情報が改竄されていないか定期的に確認する。

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。
- 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。
- 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。
- 学校内のネットワークについては，共通ゾーン・教員ゾーンと児童・生徒ゾーンに，ネットワーク領域を分割する。また，情報管理委員会は，ネットワークごとにそれぞれの管理策を作成する。
- インターネットの利用については「インターネット教育利用要綱」に基づいて利用するものとする。

7　法令の遵守

- 全教職員が，個人情報保護条例や著作権をよく理解し，遵守する。

３．３　セキュリティポリシー例（３）　：　対策基準

○○市教育委員会学校ネットワーク情報セキュリティポリシー（案）

近年の，情報化社会の進展に伴い，情報漏えい・紛失，ウイルス感染等に関する様々な事件・事故が報じられています。これらの問題については学校現場においても例外ではなく，情報セキュリティに対するリスクは増大しています。この度，各学校現場においても有効な情報セキュリティポリシーの策定及び運用をお願いしたいと思いますが，大まかなガイドラインとして○○市教育委員会の情報セキュリティポリシー(案)を提示したいと思いますので，御協力ください。

１　セキュリティ確保にあたっての組織体制

①　学校内に，校長を責任者とする「情報セキュリティ委員会」(仮称)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，各教職員のユーザ名やパスワードの承認・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) セキュリティに関する事件・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

②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を行う。

③　市教育委員会内に，「情報セキュリティ委員会」(仮称)の設置を行う。

(a) 市教育委員会を事務局にし，各学校の代表者(管理職及び情報担当者)により構成する。
(b) 各学校の「情報セキュリティ委員会」に具体的なガイドラインの提示をする。
(c) セキュリティを維持・向上させるための各種設定の支援，ネットワークやウイルス対策の点検及び支援等を行う。

2　情報資産

①　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。

②　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。

3　教職員のセキュリティ

①　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。

②　外部の者が，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。

③　学校内でセキュリティに影響を及ぼす事件・事故が起きた場合や，ソフトウエ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市教育委員会学校課に報告する。

④　事件・事故や誤動作が発生した場合には，担当者が，その状況を文書または電子データにて記録するとともに，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。

4　ハードウエアや環境のセキュリティ

①　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。

②　重要情報が外部に漏えいしないよう，取扱い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。

③　コンピュータやデータ，ソフトウエアは，指定場所から校長の許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，校長の許可を得て持ち出しを認める。

5　ネットワークやソフトウエアの運用管理

①　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許可する。

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及びシステムの変更については，担当者が文書化して管理する。

③　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。

④　悪意のあるソフトウエアの侵入を防止し，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。

⑤　極めて重要なデータやソフトウエアのバックアップは，各教職員が定期的に実施する。

⑥　ネットワーク管理者（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，無許可のアクセスからの保護を確実に行う。

⑦　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盛り込む。

⑧　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。

⑨　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，防止方法を定める。

6　アクセスの制御

①　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」「紙に記録して保存しない」「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。

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。

③　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。

7　法令の遵守

①　ソフトウエ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」などの管理策を策定する。

②　全教職員が，個人情報保護条例をよく理解し，遵守する。

③　コンピュータ(学校用)やデータ，ソフトウエアは，指定場所から校長の許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，校長の許可を得て持ち出しを認める。

３．４　セキュリティポリシー例（４）　：　対策基準

○○学校情報セキュリティポリシー

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「個人情報管理委員会」の設置を行う。
- 「個人情報管理委員会」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
- 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などとの連絡体制を構築する。

② 情報資産

- 個人情報管理委員会は，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管理責任者を明示する。
- 個人情報管理委員会は，学校内の情報を分類し，重要度を，大・中・小の三段階に決定する。また，重要性については，定期的に見直す。

③ 教職員のセキュリティ

- 個人情報管理委員会は，セキュリティ確保のための各教職員の役割・責任を明確にする。“ 職務規程 ” にも取り入れる。
- 外部利用者（保護者，公開講座開催時，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。
- 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，ソフトウエ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県総合教育センターと教育委員会に報告する。ソフトウエア誤動作の場合，県総合教育センター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エ

アを除去する。

- 事件・事故や誤動作が生じた場合には，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。
- 学校のセキュリティルールに違反した教職員には，校長が厳重な指導を行うとともに，職務命令違反で県教育委員会より懲戒処分などの手続きが取られる。

④ ハードウエ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しないよう設置し，管理する。
- 情報を廃棄，又は消去する場合，重要情報が外部に漏洩しないよう，取り扱いに注意を要する。USB メモリやフロッピーディスクなどに入っているデータを消去する場合，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。
- コンピュータやデータ，ソフトウエアは，指定場所から校長の認可なしに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。
- 学校施設の外部公開時（運動会，学校祭など）には，重要なデータを保管してある場所が教職員によって管理できない場合は必ず施錠する。

⑤ 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ために,「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ついての研修を実施する。
- 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。
- 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。
- 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，個人情報管理委員会は，ネットワークごとにそれぞれの管理策を作成する。
- 学校の教職員は，各個人ごとに利用者 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。

- 各教職員が，個人の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,「パスワードを設定する」「最新のウィルスソフトを導入する」「ファイル交換ソフトは使用しない」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。

⑥ 法令の遵守

- ソフトウエア製品などの著作権を遵守するため，個人情報管理委員会は,「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。
- 全教職員は情報モラルを身につけ，掲示板への荒らし行為や不正アクセスなどを許さない態度を養い，各児童生徒にも指導する。
- 全教職員が，個人情報保護条例をよく理解し，遵守する。

３．５　セキュリティポリシー例（５）　：　実施手順

教育用ネットワークの運用管理に係るセキュリティ対策実施手順

教育用ネットワークの運用管理に係るセキュリティ対策実施手順とは，教育用ネットワーク管理に係るセキュリティレベルの維持，向上を目的として，別に定めるもののほか，運用管理の手順をより具体的に定めることを目的とする。

１　用語の定義

(1)　教育用ネットワーク

○○市教育用ネットワーク並びにサーバ及びコンピュータ等を活用したシステムをいう。

(2)　情報セキュリティ

情報資産の機密の保持，正確性及び安全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(3)　情報セキュリティポリシー

情報セキュリティ基本方針及び対策基準，実施手順を総称して，情報セキュリティポリシーという。

(4)　記録媒体

情報を記録したフロッピーディスク，CD,MO，DVD及び磁気テープその他取り外し可能な記録媒体をいう。

２　適用範囲

教育用ネットワークを管理，運用及び利用するすべての職員，非常勤職員，臨時職員及び外部委託事業者について適用する。

３　管理体制

(1)　教育用ネットワークのセキュリティ管理は，次に掲げる体制とする。

ア　教育用ネットワーク管理者

教育用ネットワークの適正な運用及び管理を行う為，教育用ネットワーク管理者を設置し，教育センター所長をもってこれに充てる。

イ　利用責任者

教育用ネットワークの適正な利用を確保する為，利用者の所属する学校園に利用責任者を設置し，所属長をもってこれに充てる。

ウ　運用担当者

教育用ネットワークの運用を担当する職員を運用担当者という。

エ　利用者

教育用ネットワークを利用する職員，非常勤職員及び臨時職員を利用者という。

4　人的セキュリティ

(1)　役割及び責任

ア　教育用ネットワーク管理者

(ｱ)　教育用ネットワーク管理者は，ネットワークに係る開発，変更及び運用等を行う。

(ｲ)　教育用ネットワーク管理者は，セキュリティ対策実施手順等の作成，維持及び管理を行う。

(ｳ)　教育用ネットワーク管理者は，セキュリティ対策実施手順等に定められている事項について運用担当者及び利用者に実施及び遵守させること。

(ｴ)　教育用ネットワーク管理者は，運用担当者及び利用者に対し，教育用ネットワークに関する教育，指導，助言及び指示を行う。

イ　利用責任者

(ｱ)　利用責任者は，利用者に対して情報セキュリティに関する教育，指導，助言及び指示を行うこと。

(ｲ)　利用責任者は，使用する教育用ネットワークコンピュータや記録媒体について，第三者に使用させること又は許可なく情報を閲覧させることがないようにすること。

(ｳ)　利用責任者は，非常勤職員及び臨時職員の雇用時に必ずセキュリティ対策実施手順等のうち，非常勤職員及び臨時職員が守るべき内容を理解させ，また実施及び遵守させること。

ウ　運用担当者

(ｱ)　運用担当者は，セキュリティ対策実施手順等に定められている事項を遵守すること。

(ｲ)　運用担当者は，教育用ネットワークに係る情報セキュリティ対策について不明な点，遵守することが困難な点等については，速やかに教育用ネットワーク管理者に相談し，指示等に従うこと。

(ｳ)　運用担当者は，教育用ネットワーク管理者の指導，助言及び指示に従い，システムの開発，変更及び運用等の作業を行うこと。

(ｴ)　運用担当者は，教育用ネットワーク管理者の許可を得ず，システム機器や端末機器等を学校園外に持ち出さないこと。

(ｵ)　運用担当者は，異動，退職等により業務を離れる場合には，知り得た情報を他に漏らさないこと。

エ　利用者

(ｱ)　利用者は，セキュリティ対策実施手順等に定められている事項を遵守すること。

(ｲ)　利用者は，情報セキュリティ対策について不明な点，遵守することが困難な点等については，速やかに利用責任者に相談し，指示等に従うこと。

(ｳ)　利用者は，教育用ネットワーク管理者の許可を得ず，コンピュータ機器やネットワーク機器等を学校園外に持ち出さないこと。

(ｴ)　利用者は，異動，退職等により業務を離れる場合には，知り得た情報を他に漏らさないこと。

(2)　外部委託に関する管理

ア　データ入力・データ保管を外部に委託す場合は，下記事項を明記した契約を締結するか，又は覚書を取りかわすこと。

(ｱ)　データの受払い及び搬送に関する事項

(ｲ)　委託先におけるデータの保管及び廃棄に関する事項

(ｳ)　その他データの保護に関し必要な事項

(3)　データの管理

ア　運用担当者及び利用者は，教育用ネットワークで作成した個人情報等の重要情報が含まれるデータは，サーバ内に長時間保存しておかず記録媒体に保存し，耐火金庫及び施錠可能なロッカーで盗難のないよう保管すること。

イ　運用担当者及び利用者は，個人情報等の重要な情報の入ったデータ（以下「重要情報」という。）を記録媒体等で校内に持ち出す場合は，事前に所属長等の許可を得ること。

ウ　利用者は，重要情報が記録された記録媒体かどうか確認できない場合には，重要情報を記録されているものとして取り扱うこと。

エ　重要情報が記録された記録媒体を送付する場合は，職員又は守秘義務を明記した契約を締結した外部委託事業者に行わせるとともに，記録媒体は施錠可能な十分な強度を持つ外箱等に収容して送ること。

オ　重要情報が記録された記録媒体の廃棄は，所属長の許可を得ることとし，記録媒体を物理的に破壊するか又は専用のソフトウエアを使って消去することにより，いかなる方法によっても情報を復元できないようにすること。

(4)　教育

教育用ネットワーク管理者は，情報セキュリティを維持するために必要な操作方法や情報モラル（含情報セキュリティ）に関する教育を運用担当者及び利用

者に対して年に一回以上計画的に行うこと。

(5)　事故及び欠陥に対する報告

ア　運用担当者及び利用者は，情報セキュリティに関する事故，システム上の欠陥及び誤動作を発見した場合には下記の観点で状況把握し，教育用ネットワーク管理者及び利用責任者に報告し，指示に従い，対応方法を速やかに実施すること。

(ｱ)　事故等の真偽

(ｲ)　事故等を発見した日時

(ｳ)　被害の拡大範囲。

(ｴ)　被害内容

(ｵ)　被害原因

(ｶ)　対応方法

イ　利用責任者は，必要に応じ報告のあった事故等について教育用ネットワーク管理者に報告すること。

ウ　教育用ネットワーク管理者は，これらの事故等を分析し，再発防止の為の情報として記録を保存すること。また，必要に応じて部長又は教育長に報告を行うこと。

エ　教育用ネットワーク管理者は，これらの事故等への対応が完了した後，再発防止計画書を作成すること。

オ　教育用ネットワーク管理者及び利用責任者は，再発防止計画書を運用担当者及び利用者に周知し，適切に実施するように指導すること。

(6)　校務に利用するための管理職，養護教諭及び職員が使用するデスクトップ及びノート型コンピュータの取扱いについて

ア　ログオン時に使用するUSBセキュリティキーは，帰宅時には，鍵の掛かるロッカー等に保管しておくこと。

イ　必ず各個人の「ユーザ名とパスワード」を使用してログオンし，使用すること。

ウ　長時間席を離れる時は，コンピュータの電源を切ると共に，コンピュータからセキュリティキーを抜いておくこと。

エ　スクリーンセイバーは，規定値では15分で動作し，復帰時には，パスワード入力を必須とした設定にすること。

オ　ノート型コンピュータについては，席を離れる時は，蓋を閉めて表示内容が第三者に見えないように注意すること。

(7)　パスワードの管理

ア　教育用ネットワーク新規利用者は，パスワードを教育用ネットワーク管理者に申請すること。

イ　学校間及び市外への移動及び退職等によりパスワードを使用しなくなった場合は，教育用ネットワーク管理者に申請すること

ウ　パスワードは，使用者が責任を持って管理すること。

エ　パスワードは，英数半角６文字以上とすること。

オ　一般に使われている単語や本人の趣味，プライベートなどから，他人に推測されやすいパスワードを使用しないこと。

カ　パスワードは，一年に一回以上更新すること。

キ　パスワードは，不用意に口外したり，メモを作成したりしないこと。

ク　過去に一度使用したパスワードを連続でなくとも使用しないこと。

5　物理的セキュリティ

(1)　情報システム等

ア　機器の取付け等

(ｱ)　ネットワーク及びシステムの取付けを行う場合は，火災，水害，埃，振動，温度，湿度等の影響を可能な限り排除した場所に設置すること。

(ｲ)　ネットワーク及びシステムの取付けを行う場合は，落下や損傷の防止の為に，適切な固定等の措置をすること。

(ｳ)　ネットワーク及びシステムの設置位置については，不正な操作が実施しにくく，不用意な間違いや見落としなどの操作ミスが起こりにくいように配慮すること。

イ　電源設備

(ｱ)　電源設備は，耐震，耐火，耐水などの防災対策を実施する。

(ｲ)　電源設備は，負荷容量に対し十分な余裕をもつこと。

(ｳ)　電源設備には，避雷設備を設置すること。

(ｴ)　教育用ネットワーク関連機器の電源は，過電流，漏電等による機器への障害に対する保護措置を取る。

(ｵ)　教育用ネットワーク関連機器の電源は，空調機やコピー機等の負荷変動の激しい機器との共用をさけること。

(ｶ)　教育用ネットワークのサーバ関連機器の電源は，無停電装置等を設置すること。

ウ　空調設備

(ｱ)　コンピュータ室の空調設備は，コンピュータ室専用とする。

(ｲ)　空調設備は，耐震処置を講じる。

(ｳ)　空調設備は，システム機器を適切に運転する為に十分な温度・湿度の調整能力を確保する。

エ　配線

(ｱ)　配線は，損傷や回線の傍受又は損傷等を受けることがないよう，保護用の電線管・カバーの使用や，敷設経路に対する配慮などの対策を行うこと。

(ｲ)　電源ケーブルと干渉を受け易い通信ケーブルとは分離すること。

6　技術的セキュリティ

(1)教育用ネットワーク及びコンピュータの管理

ア　アクセス記録の取得等

教育用ネットワーク管理者は，システムのアクセス記録の取得等に対し，次に掲げる措置を講じること。

(ｱ)　アクセス記録は，３ヵ月さかのぼって解析できるよう保存又は保管し，必要に応じて分析を行うこと。

(ｲ)　アクセス記録は，教育用ネットワーク管理者権限がなければアクセスが行えないようにシステムの設定を行うこと。

イ　システム管理記録の作成と管理

教育用ネットワーク管理者は，ネットワーク及び所管するシステムにおいて行ったシステム変更作業等の記録を作成し，適切に管理すること。

ウ　障害記録

教育用ネットワーク管理者は，ネットワーク及び所管するシステムの障害に対する処理又は問題等に対し，次に掲げる措置を講じること。

(ｱ)　システムの構築時には，ハードウエア又はソフトウエアの障害時の対応に備え，システムに障害ログを記録するようにセットアップを行うこと。

(ｲ)　障害時の処理作業においては，障害発生時の障害ログ，障害発生時の作業状況，復旧への作業内容等を，障害記録として記録すること。

(ｳ)　障害記録は，再発防止の為の情報として保管すること。

(ｴ)　障害記録の保管場所は，業務上必要とする者のみが閲覧できる場所とすること。

(ｵ)　障害回復後には，確認等の適正な措置を講じること。

エ　システム仕様書の管理等

教育用ネットワーク管理者は，システム仕様書(以下「仕様書」という。)の管理等に対し，次に掲げる措置を講じること。

(ｱ)　システムの開発を行った場合は，システムの仕様書を整備すること。

(ｲ)　システムの仕様変更等の処理を行った場合は，仕様書の内容を変更し，最新の状態にしておくこと。

(ｳ)　仕様書は，業務上必要とする者のみが閲覧できる場所に保管すること。また，システムの構築及び変更等の作業を外部に委託した場合は，当該外部委託事業者に守秘義務を課すこと。

オ　機器の管理

教育用ネットワーク管理者は，機器の管理に対し，次に掲げる措置を講じること。

(ｱ)　ネットワーク及び所管するシステムのハードウエア構成について，機器名，型番，設置場所，管理者，購入方法等を整理し，これらをハードウエア管理情報として保管すること。

(ｲ)　ネットワーク及び所管するシステムのハードウエアを追加，更新，変更等の作業を行った場合は，ハードウエア管理情報の内容を変更し，最新の状態にしておくこと。

(ｳ)　ハードウエア管理情報は，業務上必要とする者のみが閲覧できる場所に保管すること。また，システムの構築及び変更等の作業を外部に委託した場合は，当該外部委託事業者に守秘義務を課すこと。

カ　ソフトウエアの管理

教育用ネットワーク管理者は，ソフトウエアの管理に対し，次に掲げる措置を講じること。

(ｱ)　システムのソフトウエア構成について，製品名，バージョン，利用機器，ライセンス数，購入方法等を整理し，これらをソフトウエア管理情報として保管すること。

(ｲ)　システムのソフトウエアを追加，更新，変更等の作業を行った場合は，ソフトウエア管理情報の内容を変更し，最新の状態にしておくこと。

(ｳ)　システムのソフトウエアを追加，更新，変更等の作業を行った場合は，ソフトウエアのインストール手順又はバージョンアップ手順について記録し，保管を行うこと。

(ｴ)　ソフトウエア管理情報は，業務上必要とする者のみが閲覧できる場所に保管すること。また，システムの構築及び変更等の作業を外部に委託した場合は，当該外部委託事業者に守秘義務を課すこと。

キ　バックアップ

教育用ネットワーク管理者は，障害時の復旧作業に必要なデータのバックアップについては，次に掲げる措置を講じること。

(ｱ)　バックアップは，磁気テープ又は磁気ディスク等の媒体で行うこと。

(ｲ)　障害発生時に備え，復旧作業に必要なシステム稼動環境のバックアップは少なくとも６ヶ月に一度は実施すること。

(ｳ)　日常的に業務で使用する学校園のサーバデータのバックアップは，毎日行うこと。

(ｴ)　バックアップに使用した媒体は，耐火金庫又は旋錠等のできるロッカーへ保管すること。

(ｵ)　バックアップに使用した媒体の破棄については，物理的に破壊したり，特殊なソフトウエアによってデータを消去する等の作業を行った上で廃棄すること。

ク　電子メール

(ｱ)　新規利用者は，別紙によりメールアドレス登録申請書を教育用ネットワーク管理者に提出すること。

(ｲ)　市外への転勤及び退職時は，メールアドレス廃止申請書を教育用ネットワーク管理者に届けること。

(ｳ)　利用者は，メールの自動転送機能を用いて，業務上不必要な者へ職場のメールを転送しないこと。また，チェーンメールや不審なメールを他者に転送しないこと。

(ｴ)　利用者は，個人情報の入ったメールの送信については別紙（＊１）によること。

(ｵ)　利用者は，差出人が不明又は不自然なファイルが添付されたメールを受信した場合は，直ちにそのメールを削除すること。

ケ　電子署名及び暗号化

(ｱ)　外部に送るデータが完全であることを担保することが必要な場合には，定められた電子署名方法又は暗号化方法を使用して送信すること。

(ｲ)　暗号化については，所定の方法を使用すること。

コ　業務目的以外の使用の禁止

(ｱ)　利用者は，業務上必要のない情報を検索，表示，保存又は印刷しないこと。

サ　無許可ソフトウエアの導入等の禁止

利用者は，無許可でソフトウエアの導入を行うこと。ただし，業務上の必要から，ソフトウエアの導入を希望する場合は，事前に教育用ネットワーク管理者と協議し承認を受けること。

シ　機器構成の変更の禁止

(ｱ)　利用者は，システムの機器について改造又は機器の増設及び交換を行うこと。

(ｲ)　利用者は，システムの機器について業務を遂行する為に機器の増設及び交換を行う必要がある場合には，教育用ネットワーク管理者と協議し承認を受けること。

ス　個人が所有するパソコン機器等の接続禁止

利用者は，個人が所有するコンピュータ機器等を教育用ネットワークに接続しないこと。

(2)　アクセス制御

ア　利用者登録

(ｱ)　利用者の登録，変更，抹消等は，利用者から教育用ネットワーク管理者に対する申請により行うこと。

(ｲ)　教育用ネットワーク管理者は，利用者からの申請を受けた場合には，業務上必要なシステムの利用権限(以下「アカウント」という。)の設定を行うこと。

(ｳ)　教育用ネットワーク管理者は，申請を受けた利用者のアカウントに対して，必要最小限のアクセス権限を与えること。

(ｴ)　教育用ネットワーク管理者は，利用者及び運用担当者がシステムの不正利用が行えないように，アカウントを利用したシステム利用制限を行えるよう，システムの構築を行うこと。

(ｵ)　教育用ネットワーク管理者は，システムへのアカウント登録，変更，削除等の作業は，教育用ネットワーク管理者権限がなければ行えないようにシステムの設定を行うこと。

(ｶ)　利用責任者は，利用者の人事異動又は退職等によりアカウントが不必要となった場合は，速やかに教育用ネットワーク管理者に連絡すること。

(ｷ)　教育用ネットワーク管理者は，利用者の人事異動又は退職等によりアカウントが不必要となった場合は，速やかに削除，停止等の作業を行うこと。

イ　ネットワークにおけるアクセス制御

教育用ネットワーク管理者は，ネットワークサービスを使用する権限を有しない利用者が当該サービスにアクセスできないよう，必要な措置を講じること。

ウ　強制的な経路制御

教育用ネットワーク管理者は，不正アクセスを防止するため，適切なネットワーク経路制御を施すこと。

エ　パスワード等の管理

教育用ネットワーク管理者は，ネットワーク及びシステムに係るサービスのユーザ名（ID）及びパスワード等を厳重かつ適切に管理すること。

(3)　システムの開発，導入及び保守等

ア　システムの開発及び導入

(ｱ)　教育用ネットワーク管理者は，システムのソフトウエアを開発又は導入する場合並びに機器を導入する場合は，情報セキュリティ確保の上で問題がないかどうか，確認すること。

(ｲ)　教育用ネットワーク管理者は，新たにシステムを導入する際には，既に稼働しているシステムに接続する前に十分な試験を行うこと。

イ　ソフトウエアの保守及び更新

(ｱ)　教育用ネットワーク管理者は，情報セキュリティに重大な影響を及ぼすソフトウエアについては，適切な保守が行われるようにするとともに，その不具合に対する修正等については，速やかな対応を行うこと。

(ｲ)　システムのソフトウエアの更新等については，不具合及び他のシステムとの相性の確認を行い，計画的に実施すること。

ウ　機器の廃棄及び修理

ハードウエアの廃棄及び修理を行うとき，次に掲げる措置を講じること。

(ｱ)　機器の廃棄を行う場合には，物理的に破壊したり，特殊なソフトウエアによってデータを消去したりした上で廃棄すること。また，これらの作業が困難で撤去及び運搬を外部に委託した場合は，当該外部委託事業者に守秘義務を課すこと。

(ｲ)　機器の修理を行う場合で，外部の業者に修理させる場合は，修理を委託する業者と守秘義務を明記した契約を締結すること。

(4)　コンピュータ・ウイルス対策

ア　外部のネットワークから受信したファイルは，ファイアウォールレベルでコンピュータ・ウイルス（以下「ウイルス」という。）のチェックを行い，システムへの侵入を防止すること。

イ　外部のネットワークへ送信するファイルは，ファイアウォールレベルでウイルスのチェックを行い，外部へのウイルス拡散を防止すること。

ウ　教育用ネットワーク管理者は，次に掲げる事項を実施すること。

(ｱ)　サーバ及び必要な機器にウイルス対策ソフトを導入すること。

(ｲ)　ウイルス情報について利用者に対する注意喚起を行うこと。

(ｳ)　常時ウイルスに関する情報収集に努めることこと。

(ｴ)　ウイルスチェック用のパターンファイルは常に最新のものを適用すること。

エ　利用者及び運用担当者は，次に掲げる事項を遵守すること。

(ｱ)　外部からデータ又はソフトウエアを取り入れる場合は，必ずウイルスチ

ェックを行うこと。

(ｲ)　ウイルスチェックの実行を途中で止めないこと。

(ｳ)　教育用ネットワーク管理者が提供するウイルス情報を確認すること。

(5)　不正アクセス対策

ア　教育用ネットワーク管理者は，セキュリティホール等の情報収集に努め，メーカー等から修正プログラムの提供があり次第，速やかに対応するとともに，その修正履歴を記録，保存すること。

イ　教育用ネットワーク管理者は，不正アクセスを検出又は探知できるよう，適切な対応に努めること。

ウ　教育用ネットワーク管理者管理者は，外部ネットワークより不正アクセスがあった場合には，システムの停止等の必要な措置を講じること。

エ　教育用ネットワーク管理者は，重要なシステムの設定に係るファイル等について定期的に当該ファイルの改ざんの有無を検査すること。

オ　利用者による不正アクセスがあった場合，教育用ネットワーク管理者は利用責任者に通知し，利用者のシステム利用停止又は使用方法の改善，再発防止の対策等の処置を求めること。

(6)　セキュリティ情報の収集

教育用ネットワーク管理者は，国，関係団体及び民間事業者から情報セキュリティに関する情報を適宜収集し，利用者に通知するとともに，情報セキュリティ対策上必要な措置を講じること。

7　運用

(1)　ネットワーク及びシステムの監視

教育用ネットワーク管理者は，常にネットワーク及び所管するシステムの監視を行うとともに，重要情報の侵害に対して注意を払うこと。

(2)　セキュリティ対策実施手順等の遵守状況の確認

ア　利用責任者は，セキュリティ対策実施手順等が遵守されているかどうかについて，また問題が発生していないかについて常に確認を行い，問題が発生していた場合には速やかに教育用ネットワーク管理者に報告を行うこと。

イ　教育用ネットワーク管理者は，システムの運用がセキュリティ対策実施手順等を遵守しているかどうかについて，また問題が発生していないかについて定期的に確認を行い，問題が発生していた場合には，速やかに問題を回避する為の処置を行うこと。

ウ　利用者は，セキュリティ対策実施手順等の違反が発生した場合は，速やかに利用責任者に報告を行い，利用責任者は教育用ネットワーク管理者に報告を行

うこと。

(3)　侵害時の対応

重要情報への侵害が発生した場合又は侵害のおそれがある場合における連絡，証拠保全，被害拡大の防止，侵害の調査及び復旧等の必要な措置を迅速かつ円滑に実施し，再発防止の措置を講じる為，緊急時対応計画を次のとおり定める。

ア　連絡先

○○

イ　侵害への対応

(ｱ)　運用担当者及び利用者は，教育用ネットワーク管理者及び利用責任者に報告を行い，指示を仰ぎ，侵害への対応を行うこと。

(ｲ)　利用責任者は，教育用ネットワーク管理者に報告を行い，侵害への対応を行うこと。

(ｳ)　教育用ネットワーク管理者は，侵害が与える影響の大きさに応じて，部長及び教育長に報告を行い，指示を仰ぐとともに関係機関へ連絡を行うこと。

(ｴ)　教育用ネットワーク管理者は，次に掲げる侵害が発生し，重要情報の防護の為に必要な場合は，システムを停止すること。

ａ　異常なアクセスが継続しているとき，又は不正アクセスが判明したとき。

ｂ　システムの運用に著しい支障をきたす攻撃が続いているとき。

ｃ　コンピュータ・ウイルス等不正プログラムがネットワーク経由で拡がっているとき。

ｄ　コンピュータ・ウイルス等不正プログラムが重要情報に深刻な被害を及ぼしているとき。

ｅ　災害等により電源を供給することが危険又は困難なとき。

ｆ　その他，情報資産に係る重大な被害が想定されるとき。

(ｵ)　教育用ネットワーク管理者は，侵害に係る証拠保全の実施及び再発防止の暫定措置を講じるとともに，速やかに侵害に対する復旧措置を講じ，それらの措置を記録すること。

(ｶ)　教育用ネットワーク管理者は，復旧等侵害に係る対応措置について，部長に報告を行うこと。

ウ　侵害の調査

(ｱ)　教育用ネットワーク管理者は，次に掲げる項目について，調査すること。

ａ　侵害の内容

ｂ　侵害が発生した原因

ｃ　確認した被害及び影響範囲

(ｲ)　教育用ネットワーク管理者は，調査した内容について，部長に報告を行うこと。

エ　再発防止の措置

(ｱ)　教育用ネットワーク管理者は，必要な再発防止の措置を講じること。

(ｲ)　教育用ネットワーク管理者は，再発防止の措置の内容について部長に報告を行うこと。

８　法令等の遵守

利用者は，職務の遂行において使用する重要情報について，次に掲げる法令等を遵守すること。

(1)　不正アクセス行為の禁止等に関する法律(平成１１年法律第１２８号)

(2)　著作権法(昭和４５年法律第４８号)

(3)　○○市個人情報保護条例

９　評価及び見直し等

(1)　監査

教育用ネットワーク管理者は，情報セキュリティについて監査を定期的に行うこと。

(2)　見直し

ア　教育用ネットワーク管理者は，新たに必要な対策が発生した場合又は自主点検の結果を踏まえ，情報セキュリティポリシーの実効性を評価して見直しが必要となる事象が発生した場合は，部長に報告を行うこと。

イ　教育用ネットワーク管理者は，新たに必要な対策が発生した場合は，セキュリティ対策実施手順等の見直しを行うこと。

１０　その他

この実施手順に定めるもののほか，情報セキュリティ対策に関して必要な事項は，教育用ネットワーク管理者が別に定めること。

＊１：別紙は，本事例の中では省略しています。

３．６　セキュリティポリシー例（６）　：　基本方針・対策基準・実施手順

○○県立学校情報セキュリティポリシー

目　　次

第１章　総則

第１条（目的）
第２条（用語の定義）
第３条（教育企画室の職務）
第４条（総合教育センターの職務）
第５条（管理責任者の職務）
第６条（情報化推進者の職務）
第７条（ネットワーク担当者の職務）
第８条（職員の責務）
第９条（情報化推進委員会の設置）
第１０条（実施手順）

第２章　ネットワーク及び情報機器等の運用管理

第１１条（利用内容）
第１２条（学校内で利用できるサーバ及び端末等）
第１３条（県教育委員会が整備したもの以外の情報機器等の登録及び管理等）
第１４条（県教育委員会が整備したもの以外の情報機器等に係るソフトのインストール）
第１５条（県教育委員会が整備した情報機器等の機器構成の変更）
第１６条（学校内ネットワークの拡張）
第１７条（無線回線の利用）
第１８条（不正アクセス対策）
第１９条（ウイルス対策）
第２０条（パスワードの管理）
第２１条（ファイルの共有）
第２２条（メールの利用）
第２３条（情報機器等及び記録媒体の管理）

第３章　ネットワーク及び情報機器等における電子的情報の管理

第２４条（情報の分類）
第２５条（重要な情報の取り扱い）
第２６条（情報の持ち出しの禁止）
第２７条（個人情報の取り扱い）
第２８条（校務処理等における留意点）

第４章　雑則

第２９条（事故等を発見した時の措置）
第３０条（遵守状況の調査及び指導等）
第３１条（違反行為等への対応）
第３２条（県ポリシー等の準用）
附　則

第１章　総則

（目的）

第１条　このポリシーは，○○県立高等学校及び○○県立特別支援学校（以下「学校」という。）におけるネットワーク及び情報機器等の利用に係る運用管理並びに電子的情報の管理について必要な事項を定め，学校における学習活動等を支援し，本県における教育の情報化を推進するとともに，情報セキュリティの確保に資することを目的とする。

（用語の定義）

第２条　このポリシーにおいて次の各号に掲げる用語の定義は，当該各号に定めるところによる。

⑴　職員　学校の教職員（非常勤職員を含む。）をいう。

⑵　ネットワーク　○○県行政情報通信ネットワーク以外の学校内に整備されているネットワークをいう（インターネットに接続しているかは問わない。）。

⑶　情報機器等　サーバ，パーソナル・コンピュータ（以下「パソコン」という。）及びプリンタ等の情報処理を行う機器並びにルータ（ファイアウォールを含む。），ハブ等のデータ通信を行う機器をいう。

⑷　端末等　ネットワークに接続して利用するパソコン及びスタンドアローンで利用するパソコンをいう。

⑸　利用者　情報機器等を利用する者をいう（幼児，児童及び生徒（以下「生徒等」という。）を含む。）。

⑹　メールアカウント　メールを送受信するための個人情報及び権限をいう（メールアドレスを含む。）。

⑺　ユーザーＩＤ　利用者及び所属等に与えられる利用者識別のための文字列をいう。

⑻　パスワード　利用者の情報保護のため，ユーザーＩＤごとに設定する暗証用文字列をいう。

⑼　インストール　ソフトウェア（以下「ソフト」という。）を情報機器等に導入することをいう。

⑽　ウイルス　プログラムやデータに対して意図的に何らかの被害を及ぼすように作られたプログラムであり，自己伝染機能，潜伏機能及び発病機能のいずれかの機能を有するものをいう。

⑾　ＭＡＣアドレス　機器固有情報等の識別コードをいう。

⑿　記録媒体　ハードディスク，フロッピーディスク，ＭＯ，ＣＤ等，データを記録しておくための装置（紙媒体を除く。）をいう。

⒀　ネットサーバ　各学校に設置されている○○県教育情報通信ネットワークのサーバをいう。

２　前項で規定する用語の他，このポリシーで使用する用語は，○○県情報セキュリティポリシー（平成△年△月△日策定），○○県教育情報通信ネットワーク運営管理規程（平成△年△月△日策定。以下「管理規程」という。）及び○○県教育情報通信ネットワークセキュリティポリシー（データセンタ）（平成△年△月△日策定）（これらを総称して以下「県ポリシー等」という。）で使用する用語の例による。

（教育企画室の職務）

第３条　総務課教育企画室（以下「教育企画室」という。）は，次の職務を行う。

⑴　本県における教育の情報化，ネットワーク及び情報機器等の利用に係る運用管理並びに電子的情報の管理について総括すること。

⑵　このポリシーの運用管理に関すること。

（総合教育センターの職務）

第４条　総合教育センターは，教育の情報化，ネットワーク及び情報機器等の利用に係る運用管理並びに電子的情報の管理について，次の職務を行う。

⑴　教育企画室及び学校に対する技術的な助言及び支援に関すること。

⑵　学校で対応できない障害への対応及び障害の除去に関すること。

（管理責任者の職務）

第５条　管理規程第○条に規定する管理責任者は，管理規程別表で定める職務の他，学校内での利用に関して次の職務を行う。

⑴　学校内の情報化に関する企画及び推進に関すること。

⑵　ネットワーク及び情報機器等の利用に係る総括的な運用管理に関すること。

⑶　学校内の電子的情報の管理を総括すること。

⑷　職員の情報化に係る啓発，研修及び訓練に関すること。

２　管理責任者は，学校内の教員から情報化推進者を１名選任するものとする。

３　管理責任者は，管理規程別表の規定にかかわらず，学校内の教員から２名以上の者をネットワーク担当者として選任するものとする。

４　管理責任者は，前２項の規定により選任した情報化推進者及びネットワーク担当者について，別に定める方法により教育企画室へ報告するものとする。

（情報化推進者の職務）

第６条　前条第２項に規定する情報化推進者は, 学校内での利用に関して次の職務を行う。

⑴　管理責任者の職務を補佐すること。

⑵　管理責任者の指示に基づき，学校内の情報化，ネットワーク及び情報機器等の利用並びに電子的情報の管理について，ネットワーク担当者に対して具体的な指導及び助言を行うこと。

（ネットワーク担当者の職務）

第７条　管理規程第○条に規定するネットワーク担当者は, 管理規程別表で定める職務の他，学校内での利用に関して次の職務を行う。

⑴　学校内の情報化, ネットワーク及び情報機器等の利用並びに電子的情報の管理に関する職員への指導に関すること。

⑵　障害時における連絡及び一次対応に関すること。

⑶　その他，情報化推進者の指導及び助言に基づく職務を行うこと。

（職員の責務）

第８条　職員は，このポリシー及び県ポリシー等の趣旨を十分に理解し，遵守しなければならない。

２　職員は，ネットワーク及び情報機器等を，私的に利用してはならない。

（情報化推進委員会の設置）

第９条　各学校に，管理責任者を委員長とする情報化推進委員会を設置するものとする。

２　委員には，情報化推進者，ネットワーク担当者，各学校で定める生徒の個人情報管理･運用規程により設置された個人情報管理責任者及び○○県教育委員会個人情報保護事務取扱要領（平成△年△月△日策定）に規定する個人情報保護主任者の他，管理責任者が選任する者をもって充てる。

３　情報化推進委員会は，次の事項を実施する。

⑴　学校内の情報化に関する企画及び推進について具体的な検討を行うこと。

⑵　学校内におけるネットワーク及び情報機器等の利用に係る運用管理並びに電子的情報の管理の具体的な手順（以下「実施手順」という。）を策定すること。

⑶　実施手順の運用状況について審議し，必要に応じて実施手順の見直しを行うこと。

（実施手順）

第１０条　前条第３項第２号の規定により情報化推進委員会が策定することとされる実施手順には，次の各号に掲げる事項を定めるものとする。

⑴　第１３条から第１６条及び第２６条に規定する許可の手順

⑵　第１８条第２号，第１９条第２項第５号，第２７条第２項及び第２９条に規定する報告の手順

⑶　第２３条に規定する情報機器等の具体的な管理方法

⑷　第２４条第１項に規定する情報分類の方法

⑸　第２５条に規定する重要な情報の具体的な取り扱い方法

⑹　メールアカウント，ユーザーＩＤ及びパスワードの管理方法

⑺　その他このポリシー及び県ポリシー等の規定を実施するために必要な事項

第２章　ネットワーク及び情報機器等の運用管理

（利用内容）

第１１条　ネットワーク及び情報機器等は，次の用途で利用することができる。

⑴　学校教育活動を行うための利用

⑵　校務を処理するための利用

⑶　総務事務入力のための利用

（学校内で利用できるサーバ及び端末等）

第１２条　学校内で利用できるサーバ及び端末等は，次の各号のいずれの要件も満たすものでなければならない。

⑴　県が管理するものであること。

⑵　ウイルス対策ソフトがインストールされていること。ただし，Ｗｉｎｄｏｗｓ系ＯＳ以外のＯＳを利用したサーバ及び端末等で，有効なウイルス対策ソフトが存在しない場合は，これによらないことができる。

⑶　ファイル交換ソフト（Ｗｉｎｎｙ，Ｓｈａｒｅ等，インターネットを介して不特定多数のコンピュータの間でファイルを共有するソフトをいう。），著作権法（昭和４５年法律第４８号。以下「著作権法」という。）に違反するおそれがあるソフト又は特定のサーバに負荷を与えるソフトがインストールされていないこと。

２　県が管理しないサーバ及び端末等（以下「個人所有端末等」という。）については，前項第２号及び第３号の要件を満たし，かつ，次条第１項に規定する管理責任者の許可を得た場合に限り，学校内で利用することができる。

３　個人所有端末等は，ネットワークに接続してはならない。ただし，管理規程第○条

に規定する統括管理者（教育長）が許可した場合には，接続することができる。

４　次条第１項に規定する管理責任者の許可を得た者は，前項ただし書に規定する統括管理者の許可を得たものとみなす。

５　学校内で利用する個人所有端末等の所有者は，当該端末等が本条第１項第２号及び第３号の要件を満たすことを証明する責を負うものとする。

（県教育委員会が整備したもの以外の情報機器等の登録及び管理等）

第１３条　個人所有端末等及び学校が独自に整備した情報機器等の登録，変更又は抹消を行う場合は，個人所有端末等については所有者が，学校が独自に整備した情報機器等についてはネットワーク担当者が，設置場所，有線・無線の別，機種，ＭＡＣアドレス，ＯＳバージョン，通信関係ソフト，セキュリティ対策，登載する主なアプリケーション・ソフト並びに接続するネットワークの区分及び導入方法等（以下「機器情報」という。）を記載した情報機器等利用申請書（様式１）により，管理責任者に申請して，その許可を得なければならない。

２　管理責任者は，前項に規定する許可をした場合は，当該許可を受けた情報機器等に学校内で番号（以下「機器番号」という。）を割り振り，機器番号を情報機器等の見やすい場所に貼付するとともに，機器情報及び機器番号を管理するため，情報機器台帳（様式２）を作成するものとする。

３　第１項の申請に係る許可の通知は，前項に規定する情報機器台帳に申請内容を記載し，当該情報機器等に機器番号を貼付することにより行うものとする。

４　情報機器台帳は，施錠が可能な場所に保管する等，取り扱いに注意しなければならない。

５　管理責任者は，毎年４月末日現在の機器情報及び機器番号が記録された情報機器台帳の写しを，５月末日までに教育企画室長に提出するものとする。

（県教育委員会が整備したもの以外の情報機器等に係るソフトのインストール）

第１４条　前条により許可を得た個人所有端末等及び学校が独自に整備した情報機器等へ新たにソフトを追加インストールする場合は，個人所有端末等は所有者が，それ以外の端末等はネットワーク担当者が，ソフトインストール申請書（様式３）を管理責任者に提出して，その許可を得なければならない。

２　前項の申請に係る管理責任者の許可の通知は，情報機器台帳に申請内容を記載し，その旨を申請者に伝達することにより行うものとする。

３　申請者が第１項の許可を受けてインストールしたソフトの保守及び管理は，当該申請者が行うものとする。

（県教育委員会が整備した情報機器等の機器構成の変更）

第１５条　県教育委員会が整備した情報機器等のハードウェア及びソフトの構成は，原則として変更してはならない。ただし，学校教育活動及び校務上の理由により変更する必要がある場合，管理責任者は，情報機器等機器構成変更申請書（様式４）を教育企画室長に提出して，その許可を得なければならない。

２　前項の申請があった場合，教育企画室長は，必要に応じて関係課と調整し，許可することが適当であると認めたときは，その旨を情報機器等機器構成変更許可書（様式５）により管理責任者に通知するものとする。

（学校内ネットワークの拡張）

第１６条　学校内におけるネットワークの拡張は，学校教育活動及び校務上必要な場合において，あらかじめ教育企画室長の許可を得た上で行うことができる。

２　前項に規定する教育企画室長の許可を得ようとする場合，管理責任者は，拡張する配線状況を記載した系統図，ネットワークの利用者区分，利用するＩＰアドレス並びにハブ等機器の機種及び仕様等を記載したネットワーク拡張申請書（様式６）を教育企画室長に提出するものとする。

３　教育企画室長は，第１項に規定する許可をした場合は，その旨をネットワーク拡張許可書（様式７）により管理責任者に通知するものとする。

（無線回線の利用）

第１７条　学校内で無線回線を利用する場合は，次の措置を講じるものとする。

⑴　接続しようとする端末等を，ＭＡＣアドレスで自動的に判別する等の措置を，情報機器等に講じること。

⑵　可能な限り高いレベルの暗号化の措置を講じ，暗号化キーは厳重に管理すること。

（不正アクセス対策）

第１８条　ネットワーク担当者は，不正アクセスを防止するため，次の措置を講じるものとする。

⑴　総合教育センター等から提供されたセキュリティホールに関する情報をもとに，メーカー等から提供される修正プログラム等を速やかに適用すること。

⑵　ネットワーク内の情報機器等からの不正アクセスが発見された場合，直ちに総合教育センターに報告し，情報機器等の切断及び不正アクセスを行った者の特定等，適切な処置を求めること。

（ウイルス対策）

第１９条　ネットワーク担当者は，ウイルスに関する情報の収集に努め，職員に対して最新の情報を提供するとともに，適切なウイルス対策を講じるよう指導するものとする。

２　サーバ及び端末等を利用する職員は，ウイルス対策を行うため，次の措置を講じるものとする。

⑴　サーバ及び端末等において，定期的なウイルスチェックを行うこと。

⑵　ウイルス対策ソフトは，常に有効な状態に保つとともに，ウイルスチェックに用いるパターンファイルが最新のものであることを確認すること。

⑶　ネットワーク担当者が提供するウイルス情報に常に留意すること。

⑷　メールにファイルを添付して送信する場合又は外部から持ち込まれた記録媒体を利用する場合は，あらかじめウイルスチェックを行うこと。

⑸　サーバ及び端末等がウイルスに感染していることが判明した場合には，直ちにネットワークから切断した上で，ネットワーク担当者に報告し，その指示に従って適切な措置を講じること。

（パスワードの管理）

第２０条　パスワードは相当の文字数とし，文字列は他の者が推測しにくいものでなければならない。

２　ネットワーク担当者は，適切にパスワードを管理するため，次の措置を講じるものとする。

⑴　パスワードを新規に発行する場合は，仮のパスワードを発行し，ログイン後，直ちに職員にパスワードを変更させること。

⑵　必要に応じてパスワードの設定状況を調査し，不適正な使用を行っている職員には，速やかに是正させること。

⑶　パスワードを保管するファイルは，利用者以外の者が入手できないように暗号化を施す等，適切に管理すること。

３　利用者は，適切にパスワードを管理するため，次の措置を講じるものとする。

⑴　パスワードは秘密にし，他の者に知られないようにすること。

⑵　パスワードが他の者に知られた場合，又はそのおそれがある場合は，パスワードを速やかに変更すること。

⑶　過去に使用したパスワードを再利用しないこと。

（ファイルの共有）

第２１条　ネットワーク担当者は，学校内でファイル共有を行う場合は，パスワードや

アクセス権限を設定するなど，ファイルを利用する権限のある者だけが利用できる仕組みを策定するものとする。

（メールの利用）

第２２条　利用者は，次の事項に留意してメールを利用するものとする。

⑴　メールの自動転送機能は，業務上特に必要な場合を除いて，利用しないこと。

⑵　メールアカウントは，総合教育センターが発行したもの又はネットワーク担当者がネットサーバで発行したもののみを利用すること。

（情報機器等及び記録媒体の管理）

第２３条　管理責任者は，情報機器等及び記録媒体の管理にあたっては，各部屋の施錠等，盗難防止のための措置を講じなければならない。

２　利用者は，使用する情報機器等及び記録媒体について，他の者が無断で使用，又は情報を閲覧することのないよう適切に管理しなければならない。

第３章　ネットワーク及び情報機器等における電子的情報の管理

（情報の分類）

第２４条　情報化推進委員会は，実施手順に定める方法により，学校が保有する電子的情報（以下「情報」という。）をその重要度に応じて分類するものとする。

２　生徒等の個人情報は，重要度が高い情報（以下「重要な情報」という。）に分類するものとする。

（重要な情報の取り扱い）

第２５条　利用者は，重要な情報を，次のとおり取り扱うものとする。

⑴　バックアップを定期的に行うこと。

⑵　暗号化，ユーザーＩＤ，パスワードの設定等，情報を利用する権限のある者だけが利用できるよう必要な措置を講じること。

⑶　重要な情報を記録した記録媒体は，施錠が可能な場所に保管すること。

⑷　重要な情報を記録した記録媒体は，保存期間満了後に廃棄するとともに，廃棄する場合は，当該情報を復元できないように消去し，又は記録媒体を破砕すること。

⑸　情報機器等を外部の者に修理させる場合は，重要な情報を復元できないように消去するものとする。ただし，消去できない場合は，当該外部の者に対して守秘義務を課した上で，修理させること。

⑹　情報機器等を賃借期間の満了に伴い外部の者に返却する場合は，重要な情報を復

元できないように消去するものとする。ただし，消去できない場合は，当該外部の者に対して守秘義務を課した上で，当該情報を復元できないように消去させ，又は当該情報を記録した媒体を破砕させること。

⑺　情報機器等を廃棄する場合には，重要な情報を復元できないように消去するものとする。ただし，消去できない場合は，廃棄を依頼する者に対して守秘義務を課した上で，当該情報を復元できないように消去させ，又は当該情報を記録した媒体を破砕させること。

（情報の持ち出しの禁止）

第２６条　全ての情報を，学校外へ持ち出さないこと。ただし，持ち出しをしないことにより職務の遂行に支障をきたすとして，管理責任者又は管理責任者が指名した者（以下「管理責任者等」という。）の許可を得た場合を除く。なお，重要な情報の持ち出し許可は，重要情報持ち出し管理票（様式８）を管理責任者等に提出して，その許可を得なければならない。

２　管理責任者等は，前項の許可を受けようとする者が，次の事項を遵守することを確認したうえで，許可を行うものとする。

⑴　持ち出す情報は，必要最小限にすること。

⑵　寄り道など，申請した持ち出し先以外の場所に情報を持ち出す行為やパソコン及び記録媒体の放置をしないこと。

⑶　申請したパソコン又は記録媒体以外に情報をコピーしないこと。

⑷　パソコンを起動したまま放置して，他の者に使用されることのないこと。

⑸　作業は，パソコンをネットワークから切り離した状態で行うこと。

⑹　持ち出した情報は，以下の条件を満たすパソコンで取り扱うこと。

ア　ウイルス対策ソフトがインストールされ，かつ，定義ファイル(パターンファイル)が最新の状態に保たれているパソコンであること。

イ　ファイル交換ソフト又は著作権法に違反するおそれがあるソフトがインストールされていないパソコンであること。また，家族に対しても，職員が作業に使用するパソコンにファイル交換ソフトをインストールしないよう周知すること。

ウ　ユーザーＩＤ・パスワードを設定したパソコンであること。

エ　Ｍｉｃｒｏｓｏｆｔ　Ｕｐｄａｔｅが定期的に実施され，ＯＳが最新の状態に保たれたパソコンであること（Ｗｉｎｄｏｗｓ系ＯＳを利用したパソコンの場合)。

⑺　持ち出しに使用したパソコン又は記録媒体を学校に持ち帰った時は，ウイルスチェックを行うこと。

３　管理責任者等は，学校外での作業完了後，速やかに情報の持ち帰りを確認すること。

（個人情報の取り扱い）

第２７条　利用者は，○○県個人情報保護条例（平成△年○○県条例第○号）の趣旨を十分に理解するとともに，特に次の事項に留意し，個人情報漏えい防止に努めなければならない。

⑴　個人情報を取り扱う場合は，当該個人情報の重要度に応じたアクセス権限を設けること。

⑵　個人情報を含む情報については，全てのファイルにパスワードを設定するとともに，必要に応じてファイル又はフォルダの暗号化を行うこと。

⑶　異動又は退職をする場合は，個人情報を含む全ての情報（後任者に引継ぐ必要がある情報を除く。）について，情報を復元できないように消去すること。

２　生徒等の個人情報の漏えい等が発生又は判明した場合については，平成△年△月△日付け×××××通知に従い，ただちに教育企画室へ報告すること。

（校務処理等における留意点）

第２８条　管理責任者は，職員が校務等，生徒等に閲覧されてはいけない情報を取り扱う端末等について，ユーザーＩＤ及びパスワードによる管理をしなければならない。

２　職員は，生徒等が利用するネットワークでは，生徒等に閲覧されてはいけない情報を取り扱ってはならない。

第４章　雑則

（事故等を発見した時の措置）

第２９条　ネットワーク及び情報機器等の利用について，事故，障害又は違反行為若しくは違反の疑いのある行為が発見された場合，ネットワーク担当者は，その内容に応じて，ただちに総合教育センター又は教育企画室へ報告し，その指示に従って必要な措置を講じなければならない。

（遵守状況の調査及び指導等）

第３０条　管理責任者は，このポリシー及び実施手順の遵守状況を定期的に確認し，遵守されていない事項については速やかに必要な措置を講じなければならない。

２　教育企画室長は，各学校におけるこのポリシーの遵守状況を把握するため，必要な調査を実施し，又は管理責任者に対して報告を求めることができる。

３　教育企画室長は，前項に規定する調査又は報告に基づき，管理責任者に対して必要な指導を行い，又は必要な措置を講じることができる。

（違反行為等への対応）

第３１条　教育企画室長は, このポリシーに規定する事項又は教育企画室長の指示に違反する行為を行った職員がある場合は, 当該職員のネットワーク及び情報機器等の利用を停止することができる。

２　教育企画室長は, 前項に規定する利用の停止を行う場合は, その旨をネットワーク及び情報機器等利用停止通知書（様式９）により当該職員及び当該職員が所属する学校の長に通知するものとする。

（県ポリシー等の準用）

第３２条　このポリシーに定めるものの他, 教育の情報化, ネットワーク及び情報機器等の利用に係る運用管理並びに情報セキュリティ対策に関しては, 県ポリシー等及び教育企画室長が別に定める規定によるものとする。

附　則

（施行期日）

１　このポリシーは, 平成△年△月△日から施行する。

様式１（第１３条関係）

情報機器等利用申請書

（個人所有端末等及び学校が独自に整備した情報機器等）

年　　月　　日

（管理責任者）
所属の長　殿

（申請者氏名）

次のとおり情報機器等を利用したいので申請します。

申　請　の　別		□新規　□変更　□抹消
機器	設置場所	
	有線・無線の別	□有線　□無線　□両方
	機　　種	□ｻｰﾊﾞ　□ﾊﾟｿｺﾝ　□ﾌﾟﾘﾝﾀ　□その他（　　　　）
	MAC ｱﾄﾞﾚｽ	
通信	OS ﾊﾞｰｼﾞｮﾝ	
	通信関係ｿﾌﾄ（ﾒｰﾙ・ﾌﾞﾗｳｻﾞ等）	
ｾｷｭﾘﾃｨ対策		(1) ｺﾝﾋﾟｭｰﾀｳｲﾙｽ対策ｿﾌﾄ（ﾊﾞｰｼﾞｮﾝまで） (2) その他
搭載する主なｱﾌﾟﾘｹｰｼｮﾝ・ｿﾌﾄ（ｵﾌｨｽ等）		
接続するﾈｯﾄﾜｰｸ		□職員用ﾈｯﾄﾜｰｸ　□生徒用ﾈｯﾄﾜｰｸ　□ｽﾀﾞﾝﾄﾞｱﾛﾝ
導入方法		□学校購入　□学校賃借　□個人所有　□その他（　　　　）
機器の利用者		□氏名（　　　　　　　）　□共同　□生徒等

備考　必要に応じてﾈｯﾄﾜｰｸ構成図を添付すること。

※個人所有端末等の場合，下記の事項について記入・押印のうえ申請すること。

上記の端末等は，次の要件を満たします。

□　ウイルス対策ソフトがインストールされている。

□　ファイル交換ソフト，著作権法に違反するおそれがあるソフト又は特定のサーバに負荷を与えるソフトがインストールされていない。

職・氏名　　　　　　　　　　　　印

様式２（第１３条関係）

取 扱 注 意

情報機器台帳

（個人所有端末等及び学校が独自に整備した情報機器等）

学校名

項目			1	2	3	4	5	6	7	8	9	10
機器番号（学校が任意に割り振ること）												
ｱﾄﾞﾚｽ等	ＩＰｱﾄﾞﾚｽ											
	ｻﾌﾞﾈｯﾄﾏｽｸ											
	ﾃﾞﾌｫﾙﾄｹﾞｰﾄｳｪｲ											
機器	設置場所											
	有線・無線の別											
	機種	（ｻｰﾊﾞ･ﾊﾟｿｺﾝ･ﾌﾟﾘﾝﾀ･その他）										
	MACｱﾄﾞﾚｽ											
通信	OSﾊﾞｰｼﾞｮﾝ											
	通信関係ｿﾌﾄ（ﾒｰﾙ･ﾌﾞﾗｳｻﾞ等）											
ｾｷｭﾘﾃｨ対策		ｺﾝﾋﾟｭｰﾀｳｲﾙｽ対策ｿﾌﾄ（ﾊﾞｰｼﾞｮﾝまで）										
		その他										
搭載する主なｱﾌﾟﾘｹｰｼｮﾝ･ｿﾌﾄ（ｵﾌｨｽ等）												
接続するﾈｯﾄﾜｰｸ		（職員用ﾈｯﾄﾜｰｸ・生徒用ﾈｯﾄﾜｰｸ･ｽﾀﾝﾄﾞｱﾛﾝ）										
導入方法		（県購入・県賃借・個人所有・その他）										
機器の利用者		利用者が１人に特定されている場合は氏名、共同利用の場合は「共同」、生徒等が利用する場合は「生徒等」と記入										

様式３（第１４条関係）

ソフトインストール申請書

（個人所有端末等及び学校が独自に整備した情報機器等）

年　　月　　日

（管理責任者）
所属の長　殿

（申請者氏名）

次のとおり使用許可を受けた情報機器等にソフトを追加インストールしたいので申請します。

機器番号	
インストールするソフト	
インストールを必要とする理由	

様式４（第１５条関係）

情報機器等機器構成変更申請書

（県教委が整備した情報機器等）

年　　月　　日

総務課教育企画室長　殿

（管理責任者）
所属の長

次のとおり情報機器等の機器構成を変更したいので申請します。

機器番号	
機器構成の変更内容	
変更を必要とする理由	

備考　必要に応じてカタログ等を添付すること。

様式５（第１５条関係）

情報機器等機器構成変更許可書

（県教委が整備した情報機器等）

年　　月　　日

（管理責任者）
所属の長　殿

総務課教育企画室長

年　　月　　日付けで申請のありました，機器構成の変更について，次のとおり許可します。

許可の内容	許可する機器構成	□全て許可　□一部許可　□許可せず （一部許可する場合，許可する機器構成） （許可しない理由）

様式６（第１６条関係）

ネットワーク拡張申請書

年　　月　　日

総務課教育企画室長　殿

（管理責任者）
所属の長

次のとおりネットワークを拡張したいので申請します。

拡張する配線状況がわかる系統図	〔以下の内容を明記すること。 ﾈｯﾄﾜｰｸ（職員用・生徒用）の区分，IP ｱﾄﾞﾚｽ，ﾈｯﾄﾜｰｸ機器（ﾊﾌﾞ・ﾙｰﾀ・ｱｸｾｽﾎﾟｲﾝﾄ等）〕※必要に応じ別紙とする。
接続にあたっての安全対策（無線を利用する場合は必ず記入）	〔不正アクセス対策，暗号化等〕
拡張の目的	
施工する者	□業者　□職員
添付資料	・ﾊﾌﾞ・ﾙｰﾀ・ｱｸｾｽﾎﾟｲﾝﾄ等ﾈｯﾄﾜｰｸ機器のｶﾀﾛｸﾞ

様式７（第１６条関係）

ネットワーク拡張許可書

年　　月　　日

（管理責任者）
　所属の長　殿

総務課教育企画室長

　　　年　　月　　日付けで申請のありました，ネットワークの拡張について，次のとおり許可します。

許可の条件	安全対策	
	特　記	

様式８（第２６条関係）

平成　　年　　月　　日

重要情報持ち出し管理票

持ち出す者の職・氏名		
持ち出し先		
持ち出すファイルの一覧 （欄が不足するときは別紙にする）		
持ち出しに使用するパソコン・記録媒体		パソコン・フロッピー・MO・その他 （　　　　　　　　　）
持ち出しを必要とする理由 （具体的に記入）		
使用するパソコンの状況	インターネット接続の有無	あり　・　なし （作業中はネットワークから切断すること）
	家庭内ＬＡＮ接続の有無	あり　・　なし （作業中はネットワークから切断すること）
持ち出し日		年　　月　　日
返却予定日		年　　月　　日

重要情報を持ち出すにあたり，以下の事項を遵守します。

(1)　持ち出す情報は，必要最小限にすること。
(2)　寄り道など，申請した持ち出し先以外の場所に情報を持ち出す行為やパソコン及び記録媒体の放置をしないこと。
(3)　申請したパソコン又は記録媒体以外に情報をコピーしないこと。
(4)　パソコンを起動したまま放置して，他の者に使用されることのないこと。
(5)　作業は，パソコンをネットワークから切り離した状態で行うこと。
(6)　持ち出した情報は，以下の条件を満たすパソコンで取り扱うこと。
ア　ウイルス対策ソフトがインストールされ，かつ，定義ファイル(パターンファイル)が最新の状態に保たれているパソコンであること。
イ　ファイル交換ソフト又は著作権法に違反するおそれがあるソフトがインストールされていないパソコンであること。（家族に対しても，職員が作業に使用するパソコンにファイル交換ソフトをインストールしないよう周知すること。）
ウ　ユーザーＩＤ・パスワードを設定したパソコンであること。
エ　Ｍｉｃｒｏｓｏｆｔ　Ｕｐｄａｔｅが定期的に実施され，ＯＳ等が最新の状態に保たれたパソコンであること（Ｗｉｎｄｏｗｓ系ＯＳを利用したパソコンの場合)。
(7)　持ち出しに使用したパソコン又は記録媒体を学校に持ち帰った時は，ウイルスチェックを行うこと。

職・氏名　　　　　　　印

		管理責任者等許可・確認印	
		持ち出し許可	返却確認
持ち出し日	年　　月　　日		
返　却　日	年　　月　　日		

様式９（その１）（第３１条関係）

ネットワーク及び情報機器等利用停止通知書

（所属長あて）

年　　月　　日

所属の長　殿

総務課教育企画室長

下記のとおり，貴校職員　　　　　　　　　のネットワーク及び情報機器等の利用を停止する。

記

１　ネットワーク及び情報機器等の利用を停止する期間

年　　月　　日　　時　　分から

年　　月　　日　　時　　分まで

（停止事由が終了するまで）

２　ネットワーク及び情報機器等の利用を停止する範囲

３　ネットワーク及び情報機器等の利用を停止する事由

様式９（その２）（第３１条関係）

ネットワーク及び情報機器等利用停止通知書

（職員あて）

年　　月　　日

様

総務課教育企画室長

下記のとおり，ネットワーク及び情報機器等の利用を停止する。

記

１　ネットワーク及び情報機器等の利用を停止する期間
　　年　　月　　日　　時　　分から
　　年　　月　　日　　時　　分まで
　（停止事由が終了するまで）

２　ネットワーク及び情報機器等の利用を停止する範囲

３　ネットワーク及び情報機器等の利用を停止する事由

○○学校情報セキュリティ実施手順

※（　）は県立学校情報セキュリティポリシー関係条文

Ⅰ 体　　制

1　情報化推進委員会（第９条関係）

（1）「○○学校情報化推進委員会」を設置する。

（2）構成員

役　職	職名・氏名
管理責任者	校長　○○
情報化推進者	○○（教務・情報など）主任　○○
ネットワーク担当者	教諭　○○，教諭　○○
個人情報管理責任者	教頭　○○
個人情報保護主任者	事務長　○○
ホームページ担当者	教諭　○○，教諭　○○

（管理責任者，情報化推進者，ネットワーク担当者，個人情報管理責任者，個人情報保護主任者以外にも，必要に応じて構成員を加えましょう。）

（3）活動内容

月日	内容
○月○旬	第○回会議 今年度の活動について
○月○旬	職員研修 ○○学校情報セキュリティ実施手順の説明
○月○旬	職員研修 暗号化，パスワードの設定について操作研修 ファイル共有ソフトやウィルスの確認について操作研修 端末及び個人所有パソコンの取り扱いについて
○月○旬	第○回会議

○月○旬	情報資産重要度の評価と管理方法の徹底 ○○学校情報セキュリティ手順の見直しについて 新規採用者，異動者への説明

Ⅱ　情報機器・ネットワークの管理

1　利用する端末の登録・変更又は抹消，ソフトウェアのインストール（第12,13,14条関係）

（1）承認ルート

ア　個人所有の場合

申請者→ネットワーク担当者→情報化推進者→部主事（特別支援学校の場合）→教頭→管理責任者（最終決裁）→ネットワーク担当者（情報機器台帳の整備・機器番号の貼付）

イ　個人所有以外の場合

ネットワーク担当者→情報化推進者→部主事（特別支援学校の場合）→教頭→管理責任者（最終決裁）→ネットワーク担当者（情報機器台帳の整備・機器番号の貼付）

※ネットワーク担当者以外の利用者が変更希望等のある場合でも，申請はネットワーク担当者が行う。

（2）サーバ及び端末の利用を許可する際の確認事項

ア　ウィルス対策ソフトがインストールされていること

ネットワーク担当者が，画面によりインストール状況を確認する。

なお，フリーソフトのウィルス対策ソフトについては，申請の都度協議を行う。

イ　ファイル共有ソフトがインストールされていないこと

下記のどちらかの方法により，ファイル共有ソフトがインストールされていないことを，申請者が明らかにする。

①　シマンテックのWinny検索ツールにより検索した結果の画面を出力して添付する。

http://www.symantec.com/region/jp/winny/winny_tools.html

②　アンラボ社のWinny Share検索ツール，ウィニーシールド for Companyにより検索した結果をメールで○○@△△.ed.jpへ転送する。

http://www.ahnlab.co.jp/download/index.asp

ウ　著作権法上違法なソフトがインストールされていないこと

ライセンスがフリーであるソフト以外については，ライセンスの有無をライセンス証書などにより，ネットワーク担当者が確認する。

エ　特定のサーバに負荷がかかるソフトがインストールされていないこと

ネットワーク担当者は，「プログラムの追加及び削除」等の画面によりインストールの有無を確認する。

（特定のサーバに負荷がかかるソフトの例）

① インターネット上のサーバを自動巡回して画像ファイルを自動ダウンロード収集するソフトウェア

Rydia http://www.yasuoka-yoshiharu.net/Computer/Rydia.html

② １時間で10000個以上の画像や動画を自動収集するソフトウェア

WebFCS http://hw001.gate01.com/kzsoft/

③ 株価自動収集分析Excelマクロ

SwingingStar
http://www.vector.co.jp/soft/mac/business/se423148.html

オ　インストールしても問題がないソフトについて

次のソフトについては，様式３「ソフトインストール申請書」にライセンス証書の写し等の添付があり，著作権法上違法でない場合については，申請書の提出とともに認めるものとする。

オフィス, 一太郎, 三四郎, 花子, ホームページビルダー, STUDIO8, Lhaca,
周辺機器のドライバー・・・・など

（３）ソフトのインストール・保守・管理

インストール・保守・管理は申請者が行うものとする。

２　県教育委員会が整備した情報機器等の変更（第15条関係）

（１）承認ルート

ネットワーク担当者→情報化推進者→部主事（特別支援学校の場合）→教頭→管理責任者→総務課教育企画室→管理責任者→ネットワーク担当者（情報機器台帳の整備・機器番号の貼付）

※ネットワーク担当者以外の利用者が変更の希望がある場合でも，申請はネットワーク担当者が行う。

（２）抹消の場合の注意

リース期間が満了することに伴う返却や，更新や故障に伴う廃棄の際には，情報機器台帳の該当項目を削除する。

※廃棄の際には，整備した関係課と事前に調整してください。

３　校内ネットワークの拡張（第 16 条関係）

（１）承認ルート

ネットワーク担当者→情報化推進者→部主事（特別支援学校の場合）→教頭→管理責任者→総務課教育企画室（最終決裁）→管理責任者→ネットワーク担当者

※ネットワーク担当者以外の利用者が変更希望等のある場合でも，申請はネットワーク担当者が行う。

（２）工事・設定

ネットワーク担当者が立会いを行う。

パスワードが必要な場合は，ネットワーク担当者が設定する。

４　情報機器・記録媒体の管理（第 23 条，第 25 条第１項（３）関係）

情報機器及び記録媒体については，下記の表のとおり管理者を置き，管理を行う。

（１）部屋ごとで管理する場合

部屋名	管理者
職員室	教頭　○○
パソコン教室	ネットワーク担当者　○○
・・・	・・・

（２）分掌ごとで管理する場合

分掌名	管理者
教務	教務主任　○○
生徒指導	生徒指導主事　○○
・・・	・・・

Ⅲ　情報資産の管理

１　情報資産の洗い出し（第 24 条，第 25 条第１項（３）関係）

（１）スケジュール

月　日	内　容
○月○旬	職員会議で，情報化推進者が説明を行う。

○月○旬 ～○月○旬	全教員が，各自利用しているファイルに基づいて，情報の洗い出しを行う。
○月○旬	情報化推進委員会が情報資産ごとに重要度などを評価し，適切な管理方法を検討する。
○月○旬	情報資産ごとの管理方法をまとめ，配布する。

（２）重要度の基準

分類	分類基準
重要度Ａ	秘密を要する情報資産 生徒等の個人情報を含む情報資産
重要度Ｂ	重要度Ａ又はＣ以外の情報資産
重要度Ｃ	直ちに一般公表や配布することを前提としている情報資産

（３）利用できる者の制限を行う基準

重要度Ａについては，ＩＤにより利用できる者の制限を必ず行う。

（４）暗号化の要否の基準

重要度Ａについては暗号化を必ず行う。

※第 27 条において「個人情報を含む情報については，必要に応じてファイル又はフォルダの暗号化を行う」とありますが，「○○県情報セキュリティポリシー」第○条において「重要性Ａの情報資産については，暗号化，パスワードの設定，個人情報の匿名化，アクセス制限等，厳重に管理すること」となっていますので，基本的には重要度Ａの情報資産については，暗号化を行うようにしてください。

（５）パスワード設定の要否の基準

重要度Ａについてはパスワードを必ず設定する。

（６）情報機器（記録媒体を含む）の取り扱いの基準

ア　重要度Ａの情報資産が保存されている記録媒体は，施錠して保管する。

イ　重要度Ａの情報資産は，個人所有の情報機器（記録媒体を含む）には保存しない。

※個人所有の情報機器に保存を行うと，所有者の情報と業務の情報とが混在する可能性があります。そのことから，許可を得ていない個人情報まで持ち帰ることにつながります。

個人所有の情報機器への情報の保存については，各学校で適切な基準を策定していただくようお願いいたします。

（７）情報資産の洗い出しの回数

最低年１回は行うこととし，洗い出し後に追加された情報資産については，上記基準をもとに情報化推進委員会において適宜分類を行うものとする。

２　ユーザーＩＤ・アクセス制限（第 21 条，第 25 条第１項(２)，第 27 条第１項(１)，第 28 条第１項関係）

ファイル共有をする場合(第 21 条),重要な情報を取り扱う場合(第 25 条第 1 項(2)),個人情報を取り扱う場合（第 27 条第１項(1)），生徒等に閲覧されてはいけない情報を扱う端末等（第 28 条第１項）には，ユーザーＩＤ及びパスワードにより管理をする。

なお，ユーザーＩＤについては，ネットワーク担当者が割り振った上で，情報資産ごとに適切なアクセス権の制限を行う。

（ユーザーＩＤとアクセス権の設定例）

情報資産	ユーザーＩＤ	グループ	利用者	アクセス権	
				読み込み	書き込み
成績一覧表	kyomu	教務部	教務部全員	○	○
健康診断結果	hoken01	保健部	養護教諭, 保健主事	○	○
・・・	・・・	・・・	・・・	・・・	・・・

３　パスワード（第 20 条，第 21 条，第 25 条第１項(２)，第 27 条第１項(２)，第 28 条第１項関係）

（１）パスワードの設定基準

パスワードは，８文字以上でアルファベットと非アルファベットを組み合わせたものとする。

（２）パスワードの発行方法

ネットワーク担当者は，仮のパスワードを利用者に発行し，利用者に直ちに変更させるようにする。

４　バックアップ（第 25 条第１項(１)関係）

情報の分類によりバックアップを必要とする場合は，下記のとおり行うものとする。また，バックアップをした職員の氏名，日時，ファイル名を記入したバックアップ記録簿を各学校で作成するなど，バックアップの管理を明らかにしておくこと。

（バックアップ対象情報機器）

情報機器	担当者	周期	バックアップ先
○○室のファイルサーバ	ネットワーク担当者	１ヶ月	○○室内のＭＯ
・・・	・・・		・・・

（バックアップ記録簿）

バックアップ年月日	担当者	バックアップファイル名	バックアップ先
平成○年○月○日	・・・	・・・	・・・

５　修理・リース満了・廃棄時のデータ消去(第 25 条第１項(4)(5)(6)(7)関係)

（１）県有備品のデータの消去は，情報企画課よりソフト（DELETE　MASTER（Media Vision 社製））を借り，復元できないように消去する。

（２）個人所有パソコンやフラッシュメモリについては，各個人がＨＤＤ消去ソフト（フリーソフト「Eraser」（http://www.tolvanen.com/eraser/）など）を使用して，完全に消去するように全教員に年 1 回通知する。

（３）物的に破壊するときは，シュレッダ等で粉砕する。

（４）重要度Ａ及びＢの情報を含む記録媒体，及び情報機器に関して，修理，リース満了による返却, 及び廃棄をするときは, 別添の書類を契約時に添付する。（参考資料を参照のこと。）

６　情報の持ち出し（第 26 条）

（１）持ち出しの承認方法

ア　重要度Ａ・Ｂの情報を持ち出す場合

様式８「重要情報持ち出し管理票」により承認を得ること。

イ　重要度Ｃの情報を持ち出す場合

様式８「重要情報持ち出し管理票」，又は口頭により承認を得ること。

※○○県情報セキュリティポリシー第１８条(5)に,「重要性Ｂ以上の情報を記録した記録媒体の持ち出し許可は，記録に残る形で行うこと。」とある。上記の例は，これにより重要度Ｃの情報を持ち出す場合は口頭でも可としたが，簡易な台帳等に記入することを必須としても問題ありません。

（２）承認ルート

ア「重要情報持ち出し管理票」の場合

申請者→教頭→管理責任者（管理責任者が不在の場合は○○とする）

イ　口頭の場合

申請者→教頭→管理責任者（管理責任者が不在の場合は○○とする）

（３）記録媒体の持ち出し方法

○○室にある決められた記録媒体を利用する。用務が終わった後は情報を記録媒体から完全に削除した後，管理責任者等の確認を受け，元の場所に返却する。

※記録媒体については，可能な限り，暗号化やパスワードを容易に設定できるＵＳＢメモリに限定してください。

（４）返却の際の確認方法

「重要情報持ち出し管理票」にある遵守事項が守られたかを，管理責任者（管理責任者が不在の場合は○○）は，本人に口頭で確認をする。

Ⅳ　もしもの時

１　不正アクセス（第18条第１項(２)関係）

（１）不正アクセスが見つかった場合は，速やかにネットワーク担当者に連絡する。

（２）中継しているＨＵＢの電源を切る。

（３）ネットワーク担当者は，全ての情報機器をネットワークから外す。

（４）ネットワーク担当者は，管理責任者及び総合教育センターへ連絡する。

（５）ネットワーク担当者は，総合教育センターと調整して不正アクセスの原因を究明する。

※　生徒等の個人情報の漏えい等が発生又は判明した場合は，管理責任者はただちに教育企画室へ報告する

２　ウィルスの感染（第19条関係）

（１）ウィルスの感染が見つかった場合は，速やかにネットワーク担当者に連絡する。

（２）中継しているＨＵＢの電源を切る。

（３）ネットワーク担当者は，全ての情報機器をネットワークから外す。

（４）ネットワーク担当者は，管理責任者に連絡する。

（５）全ての端末でウィルスの駆除を行う。

（６）ウィルスの影響が外部にも及んでいる可能性がある場合は，ネットワーク担当者は，総合教育センターに連絡し，調整しながら対応する。

※　生徒等の個人情報の漏えい等が発生又は判明した場合は，管理責任者はただちに教育企画室へ報告する。

３　事故，障害又は違反行為（第 29 条関係）

（１）事故，障害又は違反行為が見つかった場合は，速やかにネットワーク担当者に連絡する。

（２）ネットワーク担当者は，管理責任者に連絡する。

（３）ネットワーク担当者は，総合教育センターへ連絡する。

（４）ネットワーク担当者は，総合教育センターと調整しながら対応を行う。

※　事故, 障害又は違反行為が重大な場合については, 教育企画室にも連絡を行う。

※　生徒等の個人情報の漏えい等が発生又は判明した場合は，管理責任者はただちに教育企画室へ報告する。

Ⅴ　その他

１　無線の利用（第 17 条関係）

（１）設定の基準

ア　暗号化キーの設定：ＷＥＰ

イ　なりすまし対策：ＭＡＣアドレスフィルタリング，ＳＳＩＤのａｎｙ接続拒否

（２）設定の手順

無線の利用が許可された場合は，ネットワーク担当者が端末の設定を行い，暗号化キー等の無線の設定内容は，漏れないようにする。

（３）設定内容の保管

暗号化キーを含む無線の設定内容については，暗号化して事務室内の金庫に保管する。

２　ウィルス対策（第 19 条第 1 項）

ネットワーク担当者は，緊急性の高いウィルスに関する情報を収集した際には，全利用者に周知をする。

なお，それ以外のウィルスに関する情報については，〇〇室に掲示，広報をする。

３　メールアカウントの発行（第 22 条）

（１）メールアカウントの承認ルート

ア　校内のネットサーバで発行するアカウント

申請者→ネットワーク担当者→情報化推進者→部主事（特別支援学校の場合）→教頭→管理責任者（最終決裁）→ネットワーク担当者

イ　総合教育センターで発行するアカウント（※年１回４月に申請）

申請者→ネットワーク担当者→情報化推進者→部主事（特別支援学校の場合）→教頭→管理責任者→総合教育センター（最終決裁）→管理責任者→ネットワーク担当者

（２）メールアカウントの管理

ネットワーク担当者は，メールアカウントと利用者の対応表（総合教育センター発行分は除く）を作成し，暗号化して事務室内の金庫に保管する。

ネットワーク担当者は，毎年４月中に，転勤等異動によるアカウントの追加・削除を行う。

４　遵守状況の確認・措置（第 30 条第 1 項）

県立学校情報セキュリティポリシーが守られていない利用者がいる場合，ネットワーク担当者は管理責任者に報告する。

管理責任者は，その利用者に対して適切に指導するとともに遵守状況の改善がなされるまで，その利用者に対してネットワーク及び情報機器等の利用を停止することができる。

参考資料

情報セキュリティに関する特約条項（例）

（総則）

第1条　この特約は，この特約が添付される契約（以下「本契約」という。）と一体をなす。

（機密の保持等）

第2条　乙は，本契約に係る業務の遂行にあたって，直接又は間接に知り得た一切の情報について，甲の許可なく業務遂行の目的以外の目的に使用し，又は第三者に提供してはならない。本契約の　終了後においても同様とする。

2　乙は，本契約に係る業務遂行にあたって入手した資料，データ，記録媒体等について，常に適正な管理を行うとともに，特に個人情報等の重要な情報について，暗号化，パスワードの設定，個人情報の匿名化，アクセス制限等，厳重に管理し，使用しない場合には，施錠ができる書庫等に保管しなければならない。

3　乙は，本契約に係る業務の遂行にあたって，甲又は甲の関係者から提供された資料，データ，情報機器，各種ソフトウェア，記録媒体等について，庁外若しくは社外へ持ち出し，若しくは第三者に提供し（以上，電子メールの送信を含む。），又は業務遂行の目的以外の目的で，資料，データ等の複写若しくは複製を行ってはならない。ただし，あらかじめ甲の承認を得た場合はこの限りでない。なお，その場合にあっても，乙は，情報漏えい防止のための万全の措置を講じなければならない。

（再委託時の特約条項遵守）

第3条　乙は，甲の承認を得て他に事務を再委託する場合は，再委託先の事業者にこの特約条項を　遵守させなければならない。

（ネットワーク，情報システム等の使用）

第4条　乙は，本契約に係る業務遂行にあたって，甲の管理するネットワークに乙の情報機器を接続し，又は甲の管理する情報システムの端末を利用する場合は，あらかじめ甲の指示に従い必要な事務　手続きを行わなければならない。

2　乙は，第1項のネットワークに接続した情報機器又は情報システムの端末について，業務遂行の目的以外の目的で利用してはならない。

3　乙は，第1項のネットワークに接続した情報機器について，甲の定める利用基準に従って適正な使用を行うとともに，特に第三者に使用させないよう適切に管理しなければならない。ただし，あらかじめ甲の承認を得て第三者に使用させる場合は，この限りでない。

4　乙は，第1項のネットワークに接続した情報機器について，前項に定めるものの他，情報セキュリティを確保するための必要な安全対策を講じなければならない。

5　甲は，乙が前項までの規定に違反した場合には，ネットワークからの情報機器の切断，情報システムの利用停止等の措置をとることができる。この場合において，乙の業務の円滑な遂行に支障が生じることがあっても，甲はその責任を負わない。

（資料等の返還等）

第5条　乙が本契約による業務を遂行するために，甲から提供を受けた資料，データ，情報機器，各種ソフトウェア，記録媒体等は，業務完了後直ちに甲に返還するものとする。ただし，甲が別に指示したときは当該方法によるものとする。

（再委託先事業者からの回収）

第6条　乙が，甲から提供を受けた資料，データ，情報機器，各種ソフトウェア，記録媒体等について，甲の承認を得て再委託先の事業者に提供した場合は，乙は，甲の指示により回収するものとする。

（違反時の報告等）

第7条　乙は，この特約条項に違反する行為が発生した場合，又は発生するおそれがあると認められる場合は，速やかに甲にその旨を報告し，その指示に従わなければならない。

（立ち入り検査）

第8条　甲は，この特約条項の遵守状況の確認のため，乙又は再委託先の事業者に対して立ち入り検査を行うことができる。

（情報セキュリティの確保）

第9条　甲は，本契約に係る乙の業務遂行にあたって，前条までに定めるものの他，必要に応じて，〇〇県における情報セキュリティを確保する上で必要な対策を実施するよう指示することができ，乙はこれに従わなければならない。

実施手順策定　チェックリスト

別添２

項　目			県立学校情報セキュリティポリシーに該当する条文
体制	情報化推進委員会	構成員	第９条
		活動内容	
情報機器・ネットワークの管理	端末の登録・変更・抹消	承認ルート	第１２条、第１３条
	ソフトのインストール	承認ルート	第１２条、第１４条
	県教委が整備した機器の変更	承認ルート	第１５条
	校内ネットワークの拡張	承認ルート	第１６条
	情報機器・記録媒体の管理	情報機器の管理方法	第２３条、第２５条第1項(3)
情報資産の管理	情報の分類	情報の分類を行う方法（分担等）	第２４条
		情報の分類を行う期日	
	ユーザーＩＤ・アクセス権限	ユーザーＩＤの割り振りとアクセス権限の設定	第２１条、第２５条第1項(2)、第２７条第1項(1)、第２８条第1項
	パスワード	パスワードの設定基準	第２０条、第２１条、第２５条第1項(2)、第２７条第1項(2)、第２８条第1項
		パスワードの発行方法	
	バックアップ	バックアップの管理方法	第２５条第1項(1)
	修理・リース満了・廃棄時のデータ消去	廃棄の手続き	第２５条第1項(4)、(7)
		修理の手続き	第２５条第1項(5)
		リース満了に伴う返却の手続き	第２５条第1項(6)
	情報の持ち出し	持ち出しの承認方法、承認ルート	第２６条
		持ち出し・返却の方法、返却の確認方法	
もしもの時	不正アクセス対策	不正アクセスが発見された時の対処	第１８条第1項(2)
	ウィルスの感染	ウィルスが発見された時の対処	第１９条第2項(5)
	個人情報漏洩	個人情報が漏洩した時の対処	第２７条第2項
	事故・障害・違反行為の報告	事故・障害・違反行為が発見された時の対処	第２９条
その他	無線の利用	無線のセキュリティ条件	第１７条
		無線の設定を行う職員の明確化	
		無線設定の保管方法	
	ウィルス対策	ウィルスに関する情報の周知方法	第１９条第1項
	メールの利用	メールアカウント発行の承認ルート	第２２条
		メールアカウントの管理方法	
	遵守状況の確認・措置	遵守状況の確認・措置の方法	第３０条第1項

３．７　セキュリティポリシー例（７）　：　基本方針・対策基準

○市教育委員会情報セキュリティポリシー

目次

第１　情報セキュリティ基本方針
１　○市教育委員会情報セキュリティポリシーの目的
２　用語の定義
（１）電子情報
（２）情報システム
（３）○市イントラネット
（４）○市教育委員会イントラネット
（５）情報資産
（６）情報セキュリティ
３　適用範囲
４　情報セキュリティの基本方針
（１）組織及び体制
（２）電子情報の分類及び管理
（３）物理的セキュリティ対策
（４）人的セキュリティ対策
（５）技術的セキュリティ対策
（６）情報システムの監視等
（７）法令遵守
（８）情報セキュリティに関する違反への対応
（９）評価及び改定
（10）その他
５　情報セキュリティガイドライン等の策定

第２　情報セキュリティ対策基準
１　組織及び体制
（１）ＣＩＯ（高度情報化推進統括責任者）
（２）ＣＩＳＯ（情報セキュリティ統括責任者）

（3）教育ＣＩＯ（教育委員会高度情報化推進統括責任者）
（4）教育ＣＩＳＯ（教育委員会情報セキュリティ統括責任者）
（5）情報セキュリティ統括者
（6）情報システム管理者
（7）情報システム業務責任者
（8）情報セキュリティ担当者
2　電子情報の分類及び管理
（1）電子情報が記録されたファイルの分類
（2）ファイルの管理責任
（3）ファイル等の管理方法
3　物理的セキュリティ対策
（1）本委員会の基幹的なコンピュータ，基幹的なサーバ等
（2）事務局職員及び教職員のパソコン
4　人的セキュリティ対策
（1）役割及び責任
（2）本ポリシーの周知について
（3）事故，欠陥等への対応
（4）パスワードの管理
（5）非常勤職員，臨時的任用職員，講師，非常勤講師及び助手の本ポリシーの遵守等
5　技術的セキュリティ対策
（1）情報システムの管理
（2）アクセス制御
（3）情報システムの開発，導入，保守等
（4）コンピュータウィルス対策
（5）不正アクセス対策
（6）セキュリティ情報の収集
6　情報システムの監視等
（1）情報システムの監視
（2）本ポリシーの遵守状況の確認
（3）緊急時対応措置
7　法令遵守
8　情報セキュリティに関する違反への対応
9　評価及び改定
（1）監査

（2）点検

（3）情報セキュリティポリシーの改定

10　その他

第１　情報セキュリティ基本方針

１　〇市教育委員会情報セキュリティポリシーの目的

〇市教育委員会情報セキュリティポリシー（以下「本ポリシー」という。）は，〇市教育委員会（以下「本委員会」という。）における継続的かつ安定的な教育行政事務の実施を確保するとともに，市民及び児童・生徒の安全，安心及び信頼の下に委員会事務局，教育委員会の所管する教育機関及び学校・園の情報化を進めるため，本委員会が保有する情報資産（以下「情報資産」という。）に関し，適切なセキュリティ水準を達成するよう情報セキュリティ対策を総合的, 体系的及び具体的に定めることを目的とする。

なお〇市は，情報セキュリティに関する様々な問題を解決するため，その対策を総合的, 体系的及び具体的に定めた〇市情報セキュリティポリシーを策定しているが, 本ポリシーは, その理念及び表意されているものに基づき策定するものである。

２　用語の定義

本ポリシーの用語の定義は，次のとおりとする。

（1）電子情報

電磁的に蓄積し，及び流通しているすべての情報

（2）情報システム

ハードウェア(注１)，ソフトウェア(注2)，ネットワーク(注3)及び記録媒体（フロッピーディスク(注4)，MO(注5)，CD(注6)等をいう。以下同じ。）で構成されるものであって，これら全体で業務処理を行うもの。

（3）〇市イントラネット（以下「市役所イントラネット」という。）

本市の情報システムの一つであり, 情報通信基盤として本市が整備したネット

ワーク, 当該ネットワークに接続したサーバ(注7)及びパーソナルコンピュータ（個人が占有し, 小規模の利用に供する小型のコンピュータをいう。以下「パソコン」という。）のうち，市長部局の情報担当課が管理するもの。

（4）〇市教育委員会イントラネット（以下「イントラネット」という。）

本市教育委員会の情報システムの一つであり, 情報通信基盤として本市教育委員会が整備したネットワーク, 当該ネットワークに接続したサーバ及びパソコンのうち，教育委員会ネットワークセンター（仮称）が管理するもの。

（5）情報資産

電子情報，情報システム並びに情報システムの開発，運用及び保守のためのすべての資料

（6）情報セキュリティ

電子情報の機密性（許可を受けた者だけが電子情報を利用することができる状態をいう。以下同じ。），完全性（電子情報を利用することについて許可を受けた者が電子情報を正しく利用する状態及び不正なアクセス(注8)により電子情報が改ざんされることがない状態をいう。以下同じ。）及び可用性（電子情報を利用することについて許可を受けた者が，電子情報を，必要なときにいつでも利用することができる状態をいう。以下同じ。）を維持すること。

3　適用範囲

本ポリシーは，教育委員会事務局及び教育委員会の所管する教育機関の職員（教員籍職員，非常勤職員及び臨時的任用職員を含む。以下「事務局職員」という。）及び学校・園における教員及び職員（講師，非常勤講師，助手，非常勤職員及び臨時的任用職員を含む。以下「教職員」という。）に適用する。

4　情報セキュリティの基本方針

本委員会においては，情報資産をあらゆる脅威から守るため，次の事項を内容とする情報セキュリティ対策基準を定める。

また，事務局職員及び教職員は，本ポリシーを尊重し，及び遵守しなければならない。

（1）組織及び体制

情報セキュリティを確保するため, 情報セキュリティ対策を推進する組織及び体制を定める。

（2）電子情報の分類及び管理

本委員会の情報システム（以下「情報システム」という。）において取り扱う電子情報について，重要なものを重点的に管理する考え方から，重要度に応じ，電子情報が記録されたファイル（注9）の分類並びに当該ファイルの管理責任及び管理方法を定める。

（３）物理的セキュリティ対策

情報システムを設置する施設への不正な立入りを防止し，事務局，教育委員会の所管する教育機関及び学校・園の情報資産をその損傷，妨害等から保護するために，物理的な対策を定める。

（４）人的セキュリティ対策

情報セキュリティに関する役割及び責任，事務局職員及び教職員に本ポリシーの内容を周知する方法，事故，欠陥等への対応等について必要な対策を定める。

（５）技術的セキュリティ対策

事務局，教育委員会の所管する教育機関及び学校・園の情報資産を外部からの不正なアクセス等から保護するため，事務局，教育委員会の所管する教育機関及び学校・園の情報資産へのアクセスの制御，ネットワークの管理等について必要な対策を定める。

（６）情報システムの監視等

本ポリシーの実効性を確保するため，又は不正にアクセスが行われること及びそれにより本委員会以外の情報システムにも被害が発生することを防ぐため，情報システムの監視，本ポリシーの遵守状況の確認に関し必要な事項を定める。また，緊急事態が発生した場合に迅速な対応を行うため，緊急時対応措置を定める。

（７）法令遵守

事務局職員及び教職員に関連する法令等の遵守について定める。

（８）情報セキュリティに関する違反への対応

本ポリシーに違反した事務局職員及び教職員については，その重大性及び発生した事件の状況に応じて懲戒処分等の対象となり得ることを定める。

（９）評価及び改定

本ポリシーの実効性の評価及び改定に必要な事項を定める。

（10）その他

（１）から（９）までに定めるもののほか，情報セキュリティに関し必要な事項を定める。

５　情報セキュリティガイドライン等の策定

本ポリシーに定めるもののほか，本ポリシーの具体的な実施手順に関しては，情

報セキュリティガイドライン及び実施マニュアル・手順書等を別途定めるものとする。

第２　情報セキュリティ対策基準

１　組織及び体制

（１）ＣＩＯ（高度情報化推進統括責任者）

ＣＩＯを置き，ＣＩＯは，○市情報政策監をもって充てる。

（２）ＣＩＳＯ（情報セキュリティ統括責任者）

ＣＩＳＯを置き，ＣＩＳＯは，○市服務監をもって充てる。

（３）教育ＣＩＯ（教育委員会高度情報化推進統括責任者）

教育ＣＩＯを置き，教育ＣＩＯは，総務部長をもって充てる。

（４）教育ＣＩＳＯ（教育委員会情報セキュリティ統括責任者）

教育ＣＩＳＯを置き，教育ＣＩＳＯは，総務部長をもって充てる。

（５）情報セキュリティ統括者

情報セキュリティ統括者を置き，情報セキュリティ統括者は，情報担当課長をもって充てる。

（６）情報システム管理者

情報システム管理者を置き，情報システム管理者は，情報担当副課長をもって充てる。

（７）情報システム業務責任者

情報システムの構築及び運用に係る業務を主管する学校・園（○市立小学校条例，○市立中学校条例，○市立高等学校条例，○市立養護学校条例及び○市立幼稚園条例に定める小学校，中学校，高等学校，養護学校及び幼稚園をいう。以下同じ。），課等（○市教育委員会通則第○条に規定する課及び課のない室（センターを含む。）並びに○市例規集第○編第○類第○章第○節及び第○章に規定する施設の課をいう。以下同じ。）に，情報システム業務責任者を置き，情報システム業務責任者は，当該学校・園，課等の長をもって充てる。

（８）情報セキュリティ担当者

情報システムを利用する学校・園，課等に，情報セキュリティ担当者を置き，情報セキュリティ担当者は，当該学校・園，課等の長をもって充てる。

２　電子情報の分類及び管理

（１）電子情報が記録されたファイルの分類

情報セキュリティ担当者は，電子情報が記録されたファイル（以下「ファイル」

という。）について，各々の電子情報の機密性，完全性及び可用性を踏まえ，重要性の分類を行うものとする。

＜重要性の分類＞

Ⅰ　○市情報公開条例第○条第○号，第○号本文又は第○号から○号までのいずれかに該当するファイルのうち，業務上当該ファイルを必要とする者のみが取り扱うことを認められているもの

Ⅱ　○市情報公開条例第○条第○号，第○号本文又は第○号から第○号までのいずれかに該当するファイルのうち，Ⅰ以外のもの

Ⅲ　Ⅰ及びⅡ以外のファイルのうち，業務上重要なもの

Ⅳ　Ⅰ，Ⅱ及びⅢ以外のファイル

（２）ファイルの管理責任

ファイルを作成し，編集し，又は取得した課等は，当該ファイルを管理する責任を有する。ただし，特別の定めがあるときは，この限りでない。

（３）ファイル等の管理方法

ア　ファイルの分類の表示

情報セキュリティ担当者は，情報システムで取り扱う記録媒体に，ファイルの重要性の分類を表示する等，適切な管理を行わなければならない。

イ　ファイルの管理及び取扱い

（ア）情報セキュリティ担当者は，ファイルの重要性の分類に応じ，当該ファイルを取り扱うことができる事務局職員及び教職員の範囲を定めなければならない。

（イ）事務局職員及び教職員は，情報セキュリティ統括者の許可を受けたときを除き，重要性の分類Ⅰ又はⅡに属するファイル（以下「非公開ファイル」という。）をメールにより外部に送信してはならない。

ウ　記録媒体の管理

（ア）事務局職員及び教職員は，情報セキュリティ統括者の許可を受けたときを除き，非公開ファイルが保存された記録媒体を外部に持ち出してはならない。

（イ）事務局職員及び教職員は，ファイルが保存された記録媒体を外部に持ち出すときは，適切な方法で記録を行なう等により，適切に管理しなければならない。

（ウ）事務局職員及び教職員は，非公開ファイルが保存された記録媒体を施錠可能な場所に保管する等，情報セキュリティを確保するために必要な措置を講じなければならない。

（エ）事務局職員及び教職員は，非公開ファイルが保存された記録媒体を郵送し，又は自動車等の交通手段により輸送するときは，郵送中又は輸送中の電子情報の漏えい，記録媒体の破損等を防止するため，記録媒体を物理的に保護するた

めに必要な措置を講じなければならない。

エ　記録媒体の廃棄

（ア）事務局職員及び教職員は，ファイルが保存された記録媒体が不要となったときは，当該記録媒体に保存されたファイルを復元することができないような方法を講じて消去したうえ，廃棄しなければならない。

（イ）事務局職員及び教職員は，非公開ファイルが保存された記録媒体を廃棄するときは，情報セキュリティ統括者の許可を受けなければならない。この場合において，事務局職員及び教職員は，当該記録媒体の廃棄処理の日時及び内容並びに当該廃棄処理を行った担当者を記録しなければならない。

3　物理的セキュリティ対策

（１）本委員会の基幹的なコンピュータ，基幹的なサーバ等（以下「基幹的なコンピュータ等」という。）

ア　情報システム室の管理

（ア）情報システムの基幹的なコンピュータ等を設置し，並びに当該情報システムの管理及び運用を行うための執務室（以下「情報システム室」という。）は，外部からの侵入が容易にできない場所に配置されなければならない。

（イ）情報システム室から外部に通じるすべてのドアは，カードチェック機器（ＩＣカード（注10）により入室する者を識別することができる機能を有する機器をいう。），監視カメラ，警報装置等により，情報システム管理者から入室の許可を受けていない者の入室を防止することができるものとしなければならない。

（ウ）情報システム室には，監視設備を設置しなければならない。

（エ）情報システム室にある機器等には，耐震対策及び防火措置を講じなければならない。

（オ）情報システム室の入退室管理

ａ　情報システム室に入室することができる者は，情報システム管理者から入室の許可を受けた者のみとし，当該者が情報システム室に入室し，又は情報システム室から退室するときは，その旨を適切な方法で記録しなければならない。

ｂ　情報システム室に入室する者は，身分証明書等を携帯し，必要に応じ，これを提示しなければならない。

（カ）情報システム室への機器等の搬入

契約により機器等の搬入を認められた委託業者が情報システム室へ機器等

を搬入するときは，情報システム管理者の指名する事務局職員及び教職員は，あらかじめ，当該機器等を設置することにより既存の情報システムに悪影響が生じないことを確認するとともに，当該委託業者に同行する等の措置を講じなければならない。

イ　基幹的なコンピュータ等の取付け等

（ア）基幹的なコンピュータ等は，火災，水，ほこり，振動，温度，湿度等による影響を可能な限り排除した場所に設置し，容易に取り外すことができないよう固定する等，必要な措置を講じなければならない。

（イ）情報システム管理者は，契約により操作を認められた委託業者以外の者が基幹的なコンピュータ等を操作することができないよう，使用者のＩＤ（注11）（以下「使用者ＩＤ」という。）及びパスワード（注12）を設定する等の措置を講じなければならない。

（ウ）情報システム管理者は，基幹的なコンピュータ等の取付けに当たっては，ディスプレイ，配線等から放射される電磁波により電子情報が外部に漏えいすることがないよう必要な措置を講じなければならない。

ウ　電源

（ア）情報システム管理者は，基幹的なコンピュータ等の電源に，機器を適切に停止するまでの間に必要な電力を供給し得る予備電源を備え付けなければならない。

（イ）情報システム管理者は，落雷等による過電流等により基幹的なコンピュータ等が停止することを防ぐため，基幹的なコンピュータ等の電源に必要な措置を講じなければならない。

エ　配線等

（ア）情報システム管理者及び情報システム業務責任者は，配線に，電子情報の傍受，損傷等を防止するために必要な措置を講じなければならない。

（イ）情報システム管理者及び情報システム業務責任者は，契約により工事を認められた委託業者以外の第三者が配線を変更し，及び追加等が行なえないような措置を講じなければならない。

（ウ）情報システム管理者及び情報システム業務責任者は，事務局職員及び教職員に無線を利用して電子情報を送信させ，又は受信させるときは，電子情報の傍受，損傷等を防止するため，ＭＡＣ（注13）アドレス及びＩＰ（注14）アドレスによりパソコンを特定すること，事務局職員及び教職員に当該電子情報を暗号化させること等の措置を講じなければならない。

オ　外部の施設に設置する基幹的なコンピュータ等

情報システム管理者は，基幹的なコンピュータ等を委託業者の施設等の外部の施設に設置するときは，情報セキュリティ統括者の許可を受けなければならない。また，情報セキュリティ統括者は，定期的に，外部の施設に設置された基幹的なコンピュータ等の情報セキュリティの確保の状況を確認しなければならない。

（２）事務局職員及び教職員のパソコン

ア　事務局職員及び教職員は，情報セキュリティ担当者の許可を受けたときを除き，パソコンを執務室の外に持ち出してはならない。

イ　情報セキュリティ担当者は，事務局職員及び教職員が外部に持ち出すパソコンの使用方法を定めるとともに，適切な方法で記録する等，適切に管理しなければならない。

ウ　情報セキュリティ担当者は，事務局職員及び教職員が使用するパソコンについて，盗難防止のために必要な措置を講じなければならない。

エ　情報システム管理者及び情報システム業務責任者は，事務局職員及び教職員が使用するパソコンについて，ディスプレイ，配線等から放射される電磁波により電子情報が外部に漏えいすることがないよう必要な措置を講じなければならない。

４　人的セキュリティ対策

（１）役割及び責任

ア　ＣＩＯ

ＣＩＯは，〇市情報セキュリティポリシー実施の最高責任者であり，情報セキュリティを確保するため，教育 CIO を指導，監督する。

イ　ＣＩＳＯ

ＣＩＳＯは，〇市情報セキュリティポリシーの実施状況を継続的に監視し，必要に応じて，ＣＩＯに対し，情報セキュリティに関する勧告を行う。

ウ　教育ＣＩＯ

教育ＣＩＯは，本ポリシー実施の教育委員会における最高責任者であり，情報セキュリティを確保するため，情報システム管理者を指導，監督する。

エ　教育ＣＩＳＯ

教育ＣＩＳＯは，本ポリシーの実施状況を継続的に監視し，必要に応じて，教育ＣＩＯに対し，情報セキュリティに関する勧告を行う。

オ　情報セキュリティ統括者

情報セキュリティ統括者は，情報システムの情報セキュリティを確保するた

め, 情報システム管理者及び情報システム業務責任者を指導, 監督するとともに, 本ポリシーの遵守に関する意見の集約並びに事務局職員及び教職員に対する教育，訓練，助言，指示等を行う。

カ　情報システム管理者

情報システムの統括管理者であり, 情報システムの情報セキュリティを確保するため, 情報システム業務責任者を指導, 監督するとともに, 当該情報システムの運用状況を定期的に情報セキュリティ統括者に報告する。

キ　情報システム業務責任者

自らが構築及び運用に係る業務を主管する情報システム（イントラネットを除く。）を統括管理し，情報セキュリティを確保するため，事務局職員及び教職員が当該情報システムの電子情報を適切に利用するよう指導，監督する。

ク　情報セキュリティ担当者

所管する課, 学校･園の事務局職員及び教職員に本ポリシーを遵守させるため, 当該事務局職員及び教職員を指導，監督する。

ケ　事務局職員及び教職員等

（ア）情報セキュリティ対策の遵守義務

ａ　事務局職員及び教職員は，本ポリシー，情報セキュリティガイドライン及び実施マニュアル･手順書等に定められている事項を遵守しなければならない。

ｂ　事務局職員及び教職員は，情報セキュリティ対策について不明な点，遵守することが困難な点等があるときは, 速やかに情報セキュリティ担当者に相談し，問題の解決を図らなければならない。

（イ）外部委託に関する管理

情報システム管理者及び情報システム業務責任者は, 情報システムの開発及び保守を外部に委託するときは，委託業者（委託業者が再委託をする事業者を含む。）が本ポリシーを遵守すること，委託業者が本ポリシーを遵守しなかったときの措置及び委託業者が本市に損害を与えたときは損害賠償責任を負うことを契約書に記載し, 当該委託業者の本ポリシーの遵守を徹底しなければならない。

（ウ）その他

事務局職員及び教職員は，使用するパソコン及び記録媒体について，第三者が許可を受けずに使用すること及びこれらに記録されている電子情報を閲覧することがないよう必要な措置を講じなければならない。

（２）本ポリシーの周知について

情報セキュリティ統括者は，事務局職員及び教職員に対し，本ポリシー，及

び本ポリシーの実施方法を周知しなければならない。

（3）事故，欠陥等への対応

ア　事務局職員及び教職員は，情報システム及び情報セキュリティに関する事故，システム上の欠陥及び誤動作等を察知，発見したときは，直ちに情報セキュリティ担当者に報告しなければならない。

イ　情報セキュリティ担当者は，アにより報告があった事故等について，情報システム業務責任者に報告しなければならない。

ウ　情報システム業務責任者は，イにより報告があった事故等について，情報システム管理者に報告しなければならない。

エ　情報システム管理者は，イ又はウにより報告があった事故等について，情報セキュリティ統括者に報告し，その指示に従い，必要な措置を講じなければならない。

オ　情報セキュリティ統括者は，エにより報告があった事故等について，その重要性に応じ，教育ＣＩＯ及び教育ＣＩＳＯに報告し，教育ＣＩＯの指示を受けなければならない。

カ　教育ＣＩＯは，エにより報告があった事故等について，その重要性に応じ，ＣＩＯ及びＣＩＳＯに報告し，ＣＩＯの指示を受けなければならない。

キ　情報セキュリティ統括者は，事故等の再発防止のため，エにより報告があった事故等を分析し，当該事故等に関し適切な方法で記録を作成しなければならない。

（4）パスワードの管理

事務局職員及び教職員は，パソコン等を使用する際に必要な自己のパスワード（以下「事務局職員及び教職員のパスワード」という。）に関し，次の事項を遵守しなければならない。

ア　事務局職員及び教職員のパスワードを秘密にし，事務局職員及び教職員のパスワードの照会等に一切応じないこと。

イ　事務局職員及び教職員のパスワードを記録したメモ等を第三者が容易に発見することができる場所に保管しないこと。

ウ　事務局職員及び教職員のパスワードは，十分な長さとし，事務局職員及び教職員のパスワードの文字列は，推測し難いものとすること。

エ　事務局職員及び教職員のパスワードは，定期的に，又はアクセスの回数に応じて変更し，古い事務局職員及び教職員のパスワードを再利用しないこと。

オ　複数の情報システムを取り扱う事務局職員及び教職員は，事務局職員及び教職員のパスワードを情報システム間で共有しないこと。

カ　５（２）キ（イ）により情報セキュリティ統括者から付与された仮の事務局職

員及び教職員のパスワードは，速やかに変更すること。

ク　事務局職員及び教職員のパスワードを他の事務局職員及び教職員と共有しないこと。

（５）非常勤職員，臨時的任用職員，講師，非常勤講師及び助手の本ポリシーの遵守等

ア　情報セキュリティ担当者は，非常勤職員，臨時的任用職員，講師，非常勤講師及び助手に対し，その任用の際，本ポリシーのうち非常勤職員，臨時的任用職員，講師，非常勤講師及び助手が守るべき内容を理解させ，及び遵守させなければならない。

イ　情報セキュリティ担当者は，非常勤職員，臨時的任用職員，講師，非常勤講師及び助手に対し，その任用の際，必要に応じ，本ポリシーを遵守する旨の誓約書に署名することを求めなければならない。

５　技術的セキュリティ対策

（１）情報システムの管理

ア　アクセス記録の取得

（ア）情報システム管理者は，基幹的な情報システムのアクセス記録（使用者ＩＤ，ＩＰアドレス，利用した情報システム，利用日時等を記録したデータをいう。以下同じ。），アクセスに失敗したことを記録したデータ及び不正アクセスの有無の調査の結果を記録したデータを取得し，それらのデータのチェックを行わなければならない。

（イ）情報システム管理者は，（ア）により取得したデータを，盗難，改ざん等が行われることのないよう安全な状態で保管しなければならない。保管期間は，３箇月間を目安とする。

イ　情報システム管理記録

（ア）情報システム管理者及び情報システム業務責任者は，情報システムのハードウェアの構成，ソフトウェアの構成及びネットワークの構成を把握し，構成図を作成しなければならない。

（イ）情報システム管理者及び情報システム業務責任者は，情報システムのハードウェア等の構成を変更するときは，事前に情報セキュリティ面での問題がないかを調査，分析し，情報セキュリティ統括者の承認を受けなければならない。情報セキュリティ統括者は，情報システムのハードウェア等の構成の変更により生じるセキュリティ面での影響を審査し，承認又は不承認を決定する。

（ウ）情報システム管理者及び情報システム業務責任者は，情報システムのハードウェア等の構成の変更を構成図に反映し，構成図を常時，最新の状態に維持す

るとともに, 最新の構成図を情報セキュリティ統括者に報告しなければならない。

ウ　障害の記録

情報システム管理者及び情報システム業務責任者は, 情報システムに生じた障害の記録を管理し, 障害の原因の究明並びに再発防止策の立案及び実施に努めるとともに, 当該記録を適宜, 情報セキュリティ統括者に報告しなければならない。

エ　情報システムに係るシステム仕様書等の管理

情報システム管理者及び情報システム業務責任者は, 情報システムに係るシステム仕様書及びイ（ア）により作成した構成図を，業務上それらを必要とする事務局職員及び教職員以外の事務局職員及び教職員が閲覧することができないように保管しなければならない。

オ　情報システムに関する情報及びソフトウェアの交換

情報システム管理者及び情報システム業務責任者は，課等の間において，情報システムに関する情報及びソフトウェアを交換するときは，あらかじめ，その取扱いに関する事項を定め, 情報セキュリティ統括者の許可を受けなければならない。

カ　バックアップ(注15)

情報システム管理者，情報システム業務責任者及び情報セキュリティ担当者は，情報システムで取り扱う電子情報について，定期的にバックアップを行い，漏えい，改ざん，紛失等がないよう安全な方法で保管しなければならない。

キ　電子メール

（ア）情報システム管理者は，外部からのメールを外部に転送すること（メールの中継処理）を不可能とする等，事務局，教育委員会の所管する教育機関及び学校・園の情報システムに悪影響を与えないような設定を施さなければならない。

（イ）事務局職員及び教職員は，メールの自動転送（受信したメールを指定した相手に自動的に送信することをいう。）の機能を用いて，メールを外部に転送してはならない。

ク　外部の者が利用することができる情報システム

情報システム管理者及び情報システム業務責任者は, 外部の者が利用することができる情報システムについて，必要に応じネットワークを分ける等, 特に強固な情報セキュリティ対策を講じなければならない。

ケ　情報システムに入力し，又は情報システムから出力された電子情報の管理

（ア）情報システム管理者及び情報システム業務責任者は，情報システムに入力する電子情報に，誤り又は改ざんがないかを確認するために必要な措置を講じな

ければならない。

（イ）情報システム管理者，情報システム業務責任者及び情報セキュリティ担当者は，情報システムから出力された電子情報を，その機密性，完全性及び可用性に応じ，漏えい，改ざん，紛失等がないよう安全な方法で保管しなければならない。情報システムから出力された電子情報を廃棄するときは，その重要性の分類に応じ，当該電子情報を復元できないよう消去し，又は当該電子情報が印字された紙等の裁断，溶解等の処理を行わなければならない。

コ　暗号化

情報システム管理者及び情報システム業務責任者は, 情報システムで取り扱う電子情報の重要性の分類に応じ, 情報システム内及び通信経路上の電子情報を暗号化しなければならない。

サ　業務目的以外の使用禁止

事務局職員及び教職員は, 情報システムを業務上の目的以外の目的に使用してはならない。

シ　無許可ソフトウェアの導入禁止

事務局職員及び教職員は，パソコンに対し，情報システム管理者及び情報システム業務責任者が指定したもの以外で, 許可を受けていないソフトウェアを導入してはならない。

ス　機器構成の変更

事務局職員及び教職員は, 情報システム管理者及び情報システム業務責任者の許可を受けたときを除き，パソコンを改造し，パソコンに機器を増設し，又はパソコンの機器を交換してはならない。

（２）アクセス制御

ア　使用者登録等

情報セキュリティ統括者は，使用用者の登録，登録の変更及び登録の抹消，登録情報の管理，異動し，若しくは出向した事務局職員及び教職員又は退職した事務局職員及び教職員の使用者ＩＤの取扱い等に関する事項を定めなければならない。

イ　情報システムのイントラネットへの接続

（ア）情報システム業務責任者は，情報システムの新規構築等により，当該情報システムを新たにイントラネットに接続する必要が生じたときは, 情報システム管理者の承認を受けなければならない。

（イ）情報システム管理者は，承認を受けずに，又は承認を受けたものとは異なる状態で, 情報システムがイントラネットに接続されていることを発見したときは，当該情報システムを切断することができる。

ウ　外部からのアクセス制御

（ア）情報セキュリティ統括者は，外部アクセスサーバ（外部からのアクセスを本ネットワーク内に配信するためのサーバをいう。以下同じ。）に対してのみ，外部からアクセスをすることを許可することとし，外部アクセスサーバ以外の情報システムへ直接アクセスをすることを許可してはならない。

　また，情報セキュリティ統括者は，外部アクセスサーバに対して外部からアクセスをすることを許可するときは，使用者ＩＤ，パスワード等により，当該アクセスをする者を識別することができるようにする等の措置を講じなければならない。

（イ）モバイル(注16)のパソコン等により外部から情報システムにアクセスをすることは，当分の間，禁止する。ただし学校･園において児童・生徒が所有し，システム構成の機器として授業等に用いるパソコンは除く。

エ　情報システムの外部ネットワークへの接続

（ア）情報システム管理者及び情報システム業務責任者は，情報システムをインターネット等の外部ネットワーク（以下「外部ネットワーク」という。）に接続するときは，当該外部ネットワークのハードウェアの構成，ソフトウェアの構成及びネットワークの構成を詳細に検討し，情報システムに悪影響が生じないことを確認したうえで，情報セキュリティ統括者の許可を受けなければならない。情報セキュリティ統括者は，情報システムを外部ネットワークに接続する必要性及び危険性を検討し，接続の許可又は不許可を決定する。

（イ）情報システム管理者及び情報システム業務責任者は，外部ネットワークを情報セキュリティ統括者の適切な管理の下で利用し，外部からのアクセスについての管理を徹底しなければならない。

（ウ）情報システム管理者及び情報システム業務責任者は，情報システムを外部ネットワークに接続するときは，当該外部ネットワークの瑕疵（かし）により，電子情報の漏えい，破損及び改ざん，情報システムの停止等の業務への悪影響が生じたときに対処するため，当該外部ネットワークの管理責任者の損害賠償責任に関する規定を契約に定めなければならない。

（エ）情報システム管理者及び情報システム業務責任者は，接続した外部ネットワークのセキュリティに問題があり，情報資産に悪影響が生じるおそれがあるときは，情報セキュリティ統括者の判断に従い，速やかに当該外部ネットワークを切断しなければならない。

（オ）情報システム管理者は，イントラネットと外部ネットワークとの接続点に，必要に応じて保護回路(注17)又はそれと同等の機能を有するものを設置し，アクセス

を制限しなければならない。

（カ）情報システム管理者及び情報システム業務責任者は，情報システムを外部ネットワークに接続するときは，電子情報を暗号化して送信し，又は受信すること，情報システムと切り離された独立のパソコン等を用いること等の措置を講じなければならない。

オ　自動識別

情報システム管理者は，MACアドレスによりアクセスをすることができるかを自動的に判別することができる基幹的なコンピュータ等及びパソコンを配備しなければならない。

カ　ログイン(注18)手順

情報セキュリティ統括者は，ログインの試行回数の制限，アクセスタイムアウト(注19)の設定等，事務局職員及び教職員がログインをする手順を定めなければならない。

キ　パスワードの管理方法

（ア）情報セキュリティ統括者は，事務局職員及び教職員が事務局職員及び教職員のパスワードを知られることがなく，かつ，当該事務局職員及び教職員のみが事務局職員及び教職員のパスワードを変更することができるシステムを整備しなければならない。

（イ）情報セキュリティ統括者は，事務局職員及び教職員のパスワードを管理する仕組みに関する情報を厳重に管理しなければならない。事務局職員及び教職員に事務局職員及び教職員のパスワードを付与するときは，あらかじめ仮の事務局職員及び教職員のパスワードを付与し，速やかに仮の事務局職員及び教職員のパスワードを変更させるようにしなければならない。

（ウ）情報システム管理者及び情報システム業務責任者は，事務局職員及び教職員のパスワードの変更を行わない事務局職員及び教職員に対し，事務局職員及び教職員のパスワードを変更するよう勧告し，事務局職員及び教職員が当該勧告に従わないときは，速やかに当該事務局職員及び教職員のアクセスをする権利を停止しなければならない。

（エ）情報システム管理者及び情報システム業務責任者は，当該事務局職員及び教職員から事務局職員及び教職員のパスワードを変更する旨の申出があったときは，当該事務局職員及び教職員に対し，アクセスをする権利を再度付与するものとする。

（オ）情報システム管理者，及び情報システム業務責任者は，事務局職員及び教職員のパスワードを第三者に読まれることのないよう暗号化をする等，事務局職員及び教職員のパスワードを取り扱う方法を定めなければならない。

（3）情報システムの開発，導入，保守等

ア　ソフトウェアの開発等

（ア）情報セキュリティ統括者は，ソフトウェアの開発，変更及び運用についての手順及び基準を明らかにしなければならない。

（イ）情報セキュリティ統括者は，機器及びソフトウェアの導入，保守及び撤去についての手順及び基準を明らかにしなければならない。

（ウ）情報システム管理者及び情報システム業務責任者は，機器及びソフトウェアの購入等をしようとするときは，当該機器及びソフトウェアに情報セキュリティ面での問題がないかを確認しなければならない。

イ　情報システムの変更等の際の履歴の記録

情報システム管理者及び情報システム業務責任者は，情報システムのハードウェア等の構成の変更，廃棄等をしたときは，当該情報システムの設定，構成等の履歴を記録しなければならない。

ウ　情報システムの開発

（ア）情報セキュリティ統括者は，情報システムの開発時又は保守時の事故及び不正行為を防止するため，情報システムの開発又は保守に関する次の事項を定めなければならない。

ａ　責任者及び監督者

ｂ　作業者及び作業範囲

ｃ　開発又は保守をする情報システムの(注20)ソースコードの提出義務

ｄ　開発又は保守の作業の記録の提出義務

ｅ　開発又は保守の際に情報セキュリティ面で問題となるおそれがある(注21)ＯＳ，(注22)ミドルウェア及び(注23)アプリケーションソフトの使用の禁止に関する事項

（イ）情報システム管理者及び情報システム業務責任者は，情報システムの開発時又は保守時の事故及び不正行為の対策のため，次の事項を実施しなければならない。

ａ　開発又は保守に伴う事故及び不正行為に係る危険性の分析

ｂ　開発又は保守をする情報システムと既存の情報システムとの分離

ｃ　開発又は保守の際のアクセスの制限

ｄ　機器の搬出入の規制

ｅ　定められた場所へのマニュアル等の保管

ｆ　開発又は保守の終了後における当該開発又は保守を行った者の使用者ＩＤ，パスワード等の抹消，回収

エ　情報システムの導入

（ア）情報システム管理者及び情報システム業務責任者は，新たな情報システムを

導入するときは，既に稼動している情報システムに接続する前に，十分な試験を行わなければならない。

（イ）情報システム管理者及び情報システム業務責任者は，試験用に使用したデータを複製したもの及び試験の結果についての資料の写しを情報セキュリティ統括者に提出するとともに，当該データ及び資料を厳重に保管しなければならない。

オ　ソフトウェアの保守及び更新

情報システム管理者及び情報システム業務責任者は，ソフトウェアを更新し，又は修正(注24)プログラムを導入するときは，ソフトウェア又は修正プログラムに不具合がないことを確認しなければならない。

情報システム管理者及び情報システム業務責任者は，情報セキュリティに重大な影響を及ぼす不具合に対しては，修正プログラムを実行する等により速やかな対応を行わなければならない。

カ　システムの委託業者に関する規定

（ア）情報システム管理者及び情報システム業務責任者は，新たな情報システムの開発を外部の事業者に委託するときは，当該事業者に対し，情報システムの仕様が分かる報告書を提出させなければならない。

（イ）情報システム開発に係る業務の委託を受けた事業者が当該業務を再委託するときは，当該委託業務に係る事務を担当する課等の長は，再委託を受ける事業者の経営状況等により，当該事業者が契約を履行することができるかを確認するとともに，委託契約に，当該情報システムを導入する前に行う検査の項目を定めなければならない。

（ウ）情報システム管理者及び情報システム業務責任者は，情報システムの開発を信頼のおける事業者に委託するため，委託契約に基づく作業に従事する者に必要な資格等を定めなければならない。

（エ）情報システム管理者及び情報システム業務責任者は，情報システムの開発の作業中に，当該開発に係る委託契約に基づく作業に従事する者に身分証明書の提示を求め，契約に定められた資格を有する者であるかを確認しなければならない。

情報システム管理者及び情報システム業務責任者は，委託契約に，当該契約に基づく作業を実施するに当たり知り得た事項を第三者に漏らしてはならない旨の規定（以下「秘密の保持に関する規定」という。）を設けなければならない。

キ　機器の修理及び廃棄

（ア）情報システム管理者，情報システム業務責任者及び情報セキュリティ担当者

は, 記憶媒体が含まれる機器を外部の事業者に修理させ, 又は廃棄するときは, あらかじめ, 記憶媒体に保存された電子情報を消去しなければならない。

（イ）情報システム管理者, 情報システム業務責任者及び情報セキュリティ担当者は, 記憶媒体が含まれる機器を外部の事業者に修理させる場合において, 記憶媒体に保存された電子情報を消去することが困難であるときは, 当該修理に係る契約に, 秘密の保持に関する規定を設けなければならない。また, 情報システム管理者, 情報システム業務責任者及び情報セキュリティ担当者は, 記憶媒体が含まれる機器を廃棄する場合において, 記憶媒体に保存された電子情報を消去することが困難であるときは, 当該機器を復元不可能な状態にしなければならない。

（４）コンピュータウィルス対策

ア　情報システム管理者及び情報システム業務責任者は, 外部ネットワークから受信したファイルについて, ファイアウォール(注25)においてウィルスチェック(注26)を行うことにより, 情報システムにウィルスが侵入することを防止しなければならない。

イ　情報システム管理者及び情報システム業務責任者は, 外部にウィルスが拡大することを防止するため, 事務局職員及び教職員が外部ネットワークへ送信するファイルについて, ウィルスチェックを行うことができる機能を備えたパソコンを配備しなければならない。

ウ　情報システム管理者及び情報システム業務責任者は, 次の事項を実施しなければならない。

（ア）事務局職員及び教職員に対し, ウィルス情報についての注意を喚起すること。

（イ）常時, ウィルスに関する情報の収集に努めること。

（ウ）ウィルスチェック用のパターンファイル(注27)を常に最新のものに更新すること。

エ　事務局職員及び教職員は, 次の事項を遵守しなければならない。

（ア）外部からデータ又はソフトウェアを取り入れるときは, 必ずウィルスチェックを行うこと。

（イ）添付ファイルがあるメールを送信し, 又は受信するときは, 必ずウィルスチェックを行うこと。

（ウ）差出人が不明なメール又は不自然に添付されたファイルを速やかに削除すること。

（エ）ウィルスチェックの実行を途中で止めないこと。

（オ）情報システム管理者及び情報システム業務責任者が提供するウィルス情報を常に確認すること。

（５）不正アクセス対策

ア　情報システム管理者及び情報システム業務責任者は, 次の事項を実施しなければ

ばならない。

（ア）使用を終了した通信回線又は使用される予定がない通信回線を長時間使用しない状態で放置しないこと。

（イ）(注28)セキュリティホールの発見に努めるとともに，ハードウェア及びソフトウェアのメーカー等から修正プログラムの提供があったときは，速やかに当該修正プログラムを実行すること。

（ウ）業者によるセキュリティに関するＯＳ等のサポート期間が終了したパソコン等は，速やかにＯＳを入れかえる等の処置を施すこと。ただし，学校・園において児童・生徒が利用するネットワークに接続しているパソコンで，ウイルスチェックソフトのサポートが継続しているものを除く。

（エ）不正アクセスによる(注29)ウェブページの書換えを確実に防止するために，ウェブページの書換えが当該ウェブページの書換えに係る事務を担当する事務局職員及び教職員により行われたものであるか否かにかかわりなく，ウェブページの書換えを検出する設定を施すこと。

（オ）情報システムの設定に係るファイル等について，定期的に改ざんの有無を検査すること。

イ　情報システム管理者及び情報システム業務責任者は，不正アクセスにより情報システムが何らかの被害を受けるおそれがあり，かつ，当該不正アクセスが不正アクセス行為の禁止等に関する法律に違反する等，犯罪行為に当たる可能性があるときは，当該不正アクセスの記録に努めるとともに，関係機関との連携を密にすることにより情報の収集に努めなければならない。

ウ　情報システム管理者及び情報システム業務責任者は，事務局職員及び教職員による不正アクセスがあったときは，当該事務局職員及び教職員が所属する課等の情報セキュリティ担当者に通知し，適切な処置を講じるよう求めなければならない。

（６）セキュリティ情報の収集

情報セキュリティ統括者は，情報セキュリティに関する情報を収集し，情報システムについて，情報セキュリティ対策上必要な措置を講じなければならない。

６　情報システムの監視等

（１）情報システムの監視

ア　情報セキュリティ統括者は，次のとおり，情報システムの監視を行わなければならない。

（ア）外部と常時接続する情報システムについては，ネットワーク侵入監視装置を設置することにより，２４時間監視を行わなければならない。

（イ）（ア）の情報システム以外の情報システムについては，(注30)アクセスコントロール等を行い，異常な運用等の監視を行わなければならない。

イ　情報セキュリティ統括者は，アの監視により得られた結果を記録したデータについては，消去及び改ざんを防止するための措置を講じるとともに，安全な場所に保管しなければならない。

ウ　情報セキュリティ統括者は，アクセス記録，メールその他の個人のプライバシーに係る情報を閲覧するとき（法令に定めがある場合を除く。）は，教育ＣＩＯの許可を受けなければならない。

（２）本ポリシーの遵守状況の確認

ア　情報セキュリティ統括者，情報システム管理者及び情報システム業務責任者は，本ポリシーの遵守状況及び違反の発生状況について，常に確認を行わなければならない。

イ　事務局職員及び教職員は，本ポリシーに違反する事実を発見したときは，直ちに情報セキュリティ担当者に報告しなければならない。

ウ　情報セキュリティ担当者は，イにより報告があった違反の事実について，情報システム業務責任者に報告しなければならない。

エ　情報システム業務責任者は，ウにより報告があった違反の事実について，情報システム管理者に報告しなければならない。

オ　情報システム管理者は，ウ又はエにより報告があった違反の事実について，情報セキュリティ統括者に報告しなければならない。情報セキュリティ統括者は，当該違反が直ちに情報セキュリティに重大な影響を及ぼすと認めるときは，（３）の緊急時対応措置に従い，（３）イ（ア）の連絡を行わなければならない。

カ　情報セキュリティ統括者は，情報システムの設定が本ポリシーを遵守したものとなっているか，及び当該設定により問題が発生していないかを定期的に確認しなければならない。

（３）緊急時対応措置

情報資産が侵害される事態が生じた場合における連絡，証拠保全，被害拡大の防止，情報システムの復旧等の措置を迅速かつ円滑に実施し，及び当該事件の再発を防止するため，次のとおり，緊急時対応措置を定める。

ア　事件の調査

（ア）事務局職員及び教職員は，外部からの不正アクセス等，本市の情報資産の情報セキュリティが侵害される事件を発見したときは，当該事件の内容，発生原因と想定される行為並びに確認した被害及び影響の範囲を速やかに情報セキュリティ担当者に報告しなければならない。

（イ）情報セキュリティ担当者は，（ア）により報告があった事件を情報システム

業務責任者に報告しなければならない。

（ウ）情報システム業務責任者は，（イ）により報告があった事件を情報システム管理者に報告しなければならない。

（エ）情報システム管理者は，（イ）又は（ウ）により報告があった事件の詳細な調査を行うとともに，当該事件を情報セキュリティ統括者に報告しなければならない。

イ　事件への対処

次の者は，情報資産が侵害される各種の事件に対処するため，次の項目を実施しなければならない。

（ア）情報セキュリティ統括者は，次の各場合に応じ，それぞれに定める連絡先に連絡すること。

・多くの市民に重大な被害が生じるおそれがあるとき

ＣＩＯ，ＣＩＳＯ，教育長，教育ＣＩＯ，教育ＣＩＳＯ並びに影響が考えられる市民及び法人

・不正アクセスその他犯罪があると思料するとき，又は情報システムを経由して外部の情報システムに被害を与えるおそれがあるとき

ＣＩＯ，ＣＩＳＯ，教育長，教育ＣＩＯ，教育ＣＩＳＯ

・市役所イントラネットに被害を与えるおそれがあるとき

ＣＩＯ，ＣＩＳＯ，教育長，教育ＣＩＯ，教育ＣＩＳＯ，市役所イントラネット管理者

・情報システムに関する被害が発生したとき

情報システム管理者，情報システム業務責任者及び必要と認められる業者等

・その他の情報資産に係る被害が発生したとき

関係部署等

（イ）情報セキュリティ統括者は，次の事件が発生し，情報資産の防護のために情報システムを切断せざるを得ないときには，教育ＣＩＯの許可を受けること。ただし，当該情報資産の被害の拡大を防止するため，情報システムを直ちに切断する必要があるときは，情報システムの切断の後に教育ＣＩＯにその旨を報告することをもって足りる。

・情報システムに著しい支障を来す被害が継続して発生しているとき。

・不正アクセスが継続しているとき。

・コンピュータウィルス等の不正プログラムが情報システムを経由して広がっているとき。

・コンピュータウィルス等の不正プログラムが情報資産に深刻な被害を及ぼしているとき。

・災害等により電源を供給することが危険なとき，又は困難なとき。

・その他の情報資産に係る重大な被害が発生したとき。

（ウ）情報システム管理者及び情報システム業務責任者は，情報資産が侵害された事件についての情報システムのアクセス記録を保存すること。

（エ）情報システム管理者及び情報システム業務責任者は，情報資産が侵害された事件に対処した経過を記録すること。

（オ）情報システム管理者及び情報システム業務責任者は，情報資産が侵害された事件についての証拠の保全を実施するとともに，再発防止の暫定措置を講じること。

（カ）情報システム管理者及び情報システム業務責任者は，情報資産が侵害された事件の再発防止の暫定措置を講じた後，情報セキュリティ統括者の許可を受けて，情報システムを復旧すること。

ウ　再発防止の措置

（ア）情報セキュリティ統括者は，情報資産が侵害された事件に係るリスクの分析を実施し，本ポリシー，情報セキュリティガイドライン及び実施マニュアル・手順書等の改善に係る再発防止計画を策定し，教育ＣＩＯの承認を受けなければならない。

（イ）教育ＣＩＯは，（ア）により承認した再発防止計画を教育ＣＩＳＯに報告しなければならない。

教育ＣＩＳＯは，再発防止計画が不十分であると判断したときは，教育ＣＩＯに是正の勧告を行う。

エ　その他

上記のほか，緊急時の対応に関し必要な事項は，情報セキュリティガイドライン及び実施マニュアル・手順書等において定めるものとする。

7　法令遵守

事務局職員及び教職員は，職務の遂行において使用する情報資産に関し，次の法令及び関連する法令等を遵守しなければならない。

（１）不正アクセス行為の禁止等に関する法律

（２）著作権法

（３）○市個人情報保護条例

8　情報セキュリティに関する違反への対応

情報システム管理者，情報システム業務責任者及び情報セキュリティ担当者は，事務局職員及び教職員が本ポリシーに違反したときは，直ちに情報セキュリティ統

括者に報告しなければならない。

情報セキュリティ統括者は，情報セキュリティ担当者に対し，当該事務局職員及び教職員に是正を求めるよう指示しなければならない。

情報セキュリティ担当者は，当該事務局職員及び教職員に対し，是正を指示するとともに，総務課に報告しなければならない。

事務局職員及び教職員の本ポリシーに違反する行為については，その重大性及び発生した事件の状況に応じて懲戒処分等の対象とし，悪質な場合には刑事告発を行う。

9　評価及び改定

（1）監査

本ポリシーの実施に関し，教育ＣＩＳＯが指名する者による監査を定期的に行うものとする。

（2）点検

情報セキュリティ統括者は，本ポリシーに沿った情報セキュリティ対策の実施状況について事務局職員及び教職員にアンケート等を行うとともに，自己点検を行わなければならない。

（3）情報セキュリティポリシーの改定

教育ＣＩＳＯは，本ポリシーを是正する必要があると認めるときは，教育ＣＩＯに対し，当該是正する必要がある部分を改定するよう勧告する。教育ＣＩＯは，教育ＣＩＳＯによる勧告を受けたときは，速やかに本ポリシーを改定しなければならない。

10　その他

（1）既に制定されている電子計算機処理データ保護管理規程については，本ポリシーに包含されるものとする。

（2）情報セキュリティ統括者は，情報システムのうち，１から９までの基準によらなくても十分な情報セキュリティが確保され得ると認めるものについて，教育ＣＩＯの承認を受けて，別に情報セキュリティ対策に関する基準を定めることができる。

（3）教育ＣＩＯは，（２）により情報セキュリティ統括者が定めようとする基準について承認したときは，当該基準を教育ＣＩＳＯに報告しなければならない。

（4）教育ＣＩＳＯは，（３）により教育ＣＩＯから報告を受けた基準が不十分であると判断したときは，教育ＣＩＯに対し，当該基準の是正を求めるよう勧告を行う。

（５）（２）により定めた情報セキュリティ対策に関する基準を変更するときについても，（２）から（４）までに準じた取扱いをすることとする。

（注１）ハードウェア

　トランジスター，集積回路等から組み立てたコンピュータ（電子計算機をいう。以下同じ。）自体を記憶媒体に保存されたプログラム（ソフトウェア）と区別して呼ぶ語

（注２）ソフトウェア

　コンピュータを作動させるためのプログラム，マニュアル等

（注３）ネットワーク

　コンピュータとコンピュータを接続する電気通信回路網。電子情報を伝送する。

（注４）フロッピーディスク

　磁性体を塗った薄い円盤状のデータの記憶媒体。通常は，プラスチックなどの四角形のカバーにより守られ，携帯性に優れている。

（注５）MO（マグネット・オプティカル）

　光磁気ディスク。レーザー光線で記録部分に熱を加え，磁界を変化させてデータを記録する装置

（注６）ＣＤ（コンパクト・ディスク）

　音楽用のデジタルデータを記録し，及び再生するために，考案され，及び規格化されたデジタルオーディオディスク。これをコンピュータなどで利用可能なデジタルデータの記録媒体として応用したものがＣＤ－ＲＯＭ。

（注７）サーバ

　ネットワークの中心となるコンピュータ。ネットワーク上のファイルを共有し，ネットワークに接続している使用者が当該ファイルを使うことができるようにするファイルサーバ，ネットワーク上のプリンタを管理するプリントサーバ，メールの送受信を行うメールサーバ等がある。

（注8）アクセス

①　電話回線，ケーブル等のネットワークを通じ，他のコンピュータに接続すること。

②　他のコンピュータに接続した後，当該コンピュータに記録されているプログラムやデータを読み取ったり，編集したりすること。

（注9）ファイル

　ワープロソフトで作った文書，ペイントソフトで描いたグラフィック等

のプログラムやデータの単位。プログラムやデータは，すべてこのファイルという単位で，ハードディスク，フロッピーディスク等の記録媒体に保存され，管理されている。

（注 10）ＩＣカード

プラスチックカードに集積回路を埋め込んだもの。暗証番号等により使用者を識別することができる。

（注 11）ＩＤ（Identification の略）

識別記号のことで，ネットワークを通じてコンピュータに接続する者を識別するために利用されるものをいう。パソコン通信では，数字やアルファベットなどを組み合わせた記号が使われる。

（注 12）パスワード

アクセスをするため，コンピュータの認証を受けるときに，ＩＤと共に入力する文字列。パスワードは，使用者しか知らないので，使用者本人がアクセスをしていることを認証することができる。

（注 13）ＭＡＣアドレス（メディア・アクセス・コントロール・アドレス）

コンピュータを識別するためにコンピュータ自体に設定されるアドレス。世界に一つしかない。

（注 14）ＩＰアドレス（インターネット・プロトコル・アドレス）

インターネットに接続するコンピュータを識別するためのアドレス。インターネットに接続するコンピュータにはすべてこのアドレスが割り振られる。

（注 15）バックアップ

事故等に備えて，あらかじめプログラム又はファイルを複製しておくこと。

（注 16）モバイル

「可動性の」,「移動性の」という意味

（注 17）保護回路

情報システムへのアクセスを制御するコンピュータ

（注 18）ログイン

他のコンピュータに接続した後，当該コンピュータに記録されているファイルを取り扱うために当該ファイルに接続すること。

（注８）①の意味でのアクセス　→　ログイン　→（注８）②の意味でのアクセスとなる。

（注 19）アクセスタイムアウト

一定時間内にコンピュータへの接続が完了しないときに，自動的に接続

処理を終了させること。

（注 20）ソースコード

プログラミング言語（コンピュータが読み取ることができる言語）で記述されたプログラムのこと。コンピュータは，ソースコードに従って，プログラムを実行する。

（注 21）ＯＳ

ファイルの管理，メモリの管理，入出力の管理，使用者がパソコンを操作するためのプログラム（ユーザインターフェース）の提供などを行う基本ソフトウェア

（注 22）ミドルウェア

ＯＳとアプリケーションの中間に位置するソフトウェアのことで，アプリケーションにサービスを提供する。

（注 23）アプリケーションソフト

コンピュータを使って，文書，表及びデータベースを作るなど，それぞれの目的を実現するためのソフトウェア

（注 24）修正プログラム

アプリケーションのプログラムを部分的に修正する実行ファイル

（注 25）ファイアウォール

インターネット等の外部のネットワークから内部のネットワークに不正にアクセスが行われること及び内部のネットワークにウィルスが進入することを防止するため，内部のネットワークと外部のネットワークの間に設置されるハードウェア及びソフトウェア又は当該防止の機能のこと。

（注 26）ウィルスチェック

コンピュータウィルスを発見し，及び除去すること。

（注 27）パターンファイル

ウィルス対策のためのソフトがウィルスを検索し，及び駆除するために参考とするファイルのこと。様々なウィルスの特徴が記され，新しいウィルスが見つかる度に，ウィルス対策のためのソフトのメーカーがパターンファイルを更新することで新種のウィルスに対処する。

（注 28）セキュリティホール

ネットワーク及び情報システムにおけるセキュリティの欠陥

（注 29）ウェブページ

インターネット上にある情報提供サービスで，一般的にホームページといわれるもの。インターネット・エクスプローラ，ネットスケープ・ナビゲータ等のインターネットブラウザを使うことで，文書，画像等が含まれ

るページとして見ることができる。

（注 30）アクセスコントロール

　コンピュータの使用者を識別する機能（ＩＤ，パスワード等）を使って，アクセスを管理すること。

学校情報セキュリティポリシー策定・運用のための

学校情報セキュリティ・ハンドブック解説書＜改訂版＞

平成20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/