http://www.edu.pref.kagoshima.jp/ （通巻第1662号）

指導資料

鹿児島県総合教育センター

情報教育 第118号

－小，中，高，特別支援学校対象－

平成22年４月発行

学校情報セキュリティポリシーの作成及び運用の在り方

情報化社会の進展に伴い，学校においても情報セキュリティに関する脅威（情報漏えいやウィルス感染等）が問題となっている。

文部科学省が調査した平成20年度「学校における教育の情報化の実態等に関する調査」結果（平成21年３月１日現在）によると，県内公立学校の情報セキュリティポリシーの策定・運用の状況は**図１**のとおりである。

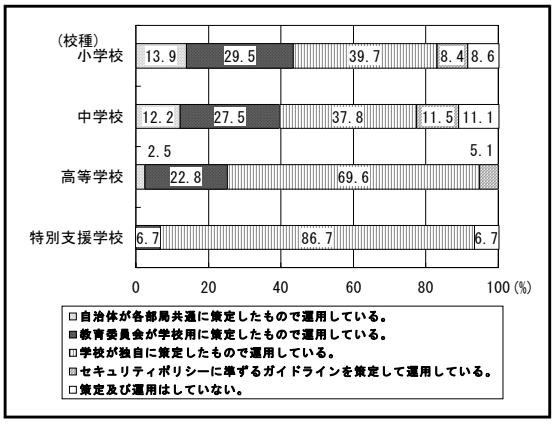


図１　情報セキュリティポリシー策定・運用の状況

どの校種でも，約９割以上の学校で情報セキュリティポリシーが運用されているが，情報セキュリティについての様々な脅威を未然に防いだり，職員の意識を向上させたりするには，その作成及び改善に全職員が主体的に関わることが大切である。そして，今後も更に各学校が実状に合わせた実効性の高い情報セキュリティポリシーに基づいた運用を行うことが重要となってくる。

そこで本稿では，学校情報セキュリティポリシーの作成及び運用の在り方について述べる。

１　学校における情報資産の管理の重要性

「情報資産」とは，学校で保有している情報全般と，それを扱うためのネットワーク及び情報機器等のことである。

教職員は，日ごろの教育活動や校務で，多くのデータや資料を作成し保有している。その中には児童生徒や卒業生，保護者等に関する多くの個人情報が含まれており，これらの情報を適切に管理するために，教職員一人一人が気を付けて行うことや，学校として決められた仕組みを作ることなど，様々な対策が必要となる。

情報セキュリティとは，「情報資産」を「漏えい」，「改ざん」，「破壊・消失」から守ることであり，学校の情報資産の管理の仕方を定めた「学校情報セキュリティポリシー」は，情報資産を教職員間で同じになるように取り扱い，組織として情報資産を守ることを目的としている。

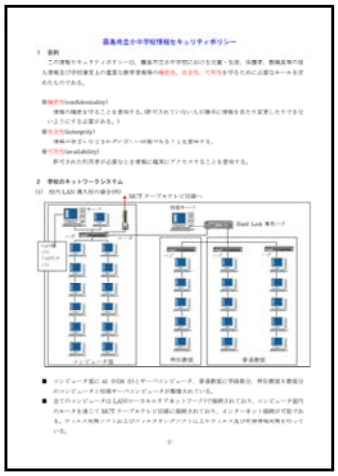
２　情報セキュリティポリシーの作成の在り方

情報セキュリティポリシーは，次の三つの構成で体系的にまとめ，文書化する。

○　**基本方針**
　セキュリティ対策の目的や原則などの基本方針
○　**対策基準**
　基本方針に基づいた具体的な遵守事項や対策基準
○　**実施手順**
　教職員が日ごろ守るべき項目をまとめた対策手順書

例えば霧島市は「学校情報セキュリティポリシー」を次のように示している。

＜霧島市小中学校情報セキュリティポリシー＞



（クリックすると拡大されます）

このように，学校で作成する際は自治体や教育委員会の示したものに基づき，自校の実状に合わせる方法がある(図2)。

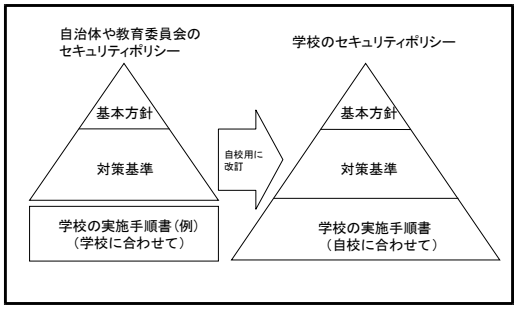


図２　教育委員会・各学校の作成イメージ

図３に，情報セキュリティポリシーの作成手順を示す。

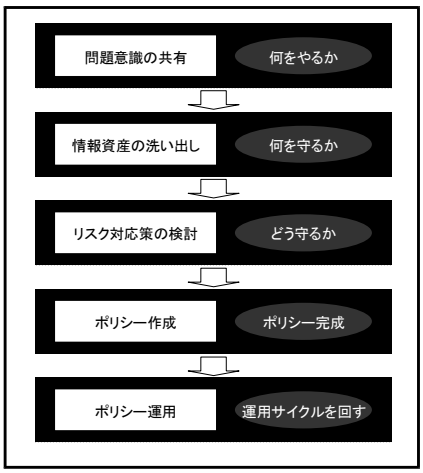


図３　情報セキュリティポリシー作成手順

(1) 問題意識の共有

個人情報漏えいやウィルス感染など，セキュリティに関する問題の事例を挙げ，情報セキュリティポリシーの重要性を職員間で共有する。

(2) 情報資産の洗い出し

学校を運営するために必要な情報について，誰が，どこに，どのような形で所有しているのかを洗い出し，整理する。

(3) リスク対応策の検討

情報資産の重要度，情報資産がさらされている脅威，脅威に対する脆弱性の観点からリスクの大きさを評価し，リスクに対する具体的な対応策を検討する。

(4) ポリシー作成

自校の教育目標や学校運営の方針及びネットワーク環境等に基づいたセキュリティポリシーを作成する。

(5) ポリシー運用

計画的に運用し，実効性及び事故発生時の対応等について定期的に見直し，改善を行う。

３　情報セキュリティポリシーの運用の在り方

情報セキュリティポリシーの目標を達成するためには，導入時に職員研修を実施し共通理解を図ったり，運用時の問題点を把握し，セキュリティポリシーの妥当性の見直し，改善を行う運用サイクルを継続したりしていくことが必要となる（**図４**）。

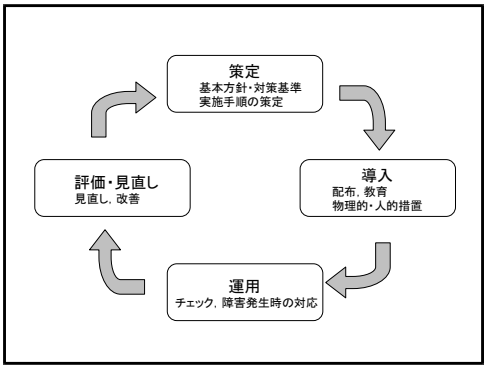


図４　セキュリティポリシー運用のサイクル

(1) 運用計画

学校全体や管理者(校長)や管理する係が行うことを月ごとに示した運用計画を作成し，その中にセキュリティポリシーの見直しと改善を盛り込む。その際，以下のようなチェックリストを基に，改善すべき項目については再検討する。

○　情報セキュリティポリシー運用時のチェックリスト例

□　文章は簡潔明瞭に記述され，正確に理解できるか。
□　責任の所在は明確か。
□　定期的な情報資産のリスク評価や自己点検，監査を実施しているか。
□　見直しが定期的に行われているか。
□　情報セキュリティに関する職員研修を行っているか。
□　対策規準を満たすために必要な予算措置を行っているか。
□　実践できずに形骸化している事項はないか。
□　担当者を適切に配置しているか。

(2) 職員研修の実施

作成したセキュリティポリシーを，すべての職員に配布し，同意を求める。その際，情報セキュリティの必要性を分かりやすく説明したり，対策基準及び実施手順に沿った具体的な操作を含む研修を実施したりする。

(3) 定期的なチェック

個人情報の管理やウィ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定期的にチェックを行い，問題点の把握と改善に努める。

(4) 事故発生時の体制づくり

ウィルス感染や情報漏えい等の事故が発生したときに，報告や対処が遅れることは最も避けなければならない。そのためには，事故を起こした場合に，速やかに報告できる体制作りをしておくことも重要である。

(5) 定期的な見直しと改善

運用中に発生した問題を把握するとともに，教職員の意見も収集する。これらの情報を基に，セキュリティポリシーが妥当かどうかを見直し，改善する。

変更したセキュリティポリシーは再度配布し，同意を求め，運用する。

４　情報セキュリティポリシーの実効性を高める取組

学校における運用の具体的な取組について，霧島市立青葉小学校の実践例を基に述べる。

(1) 職員の共通理解を図る取組

青葉小学校では，情報セキュリティポリシーを冊子にして年度始めに全職員に配布し，その中で示した実施手順に基づいた職員研修を通して共通理解を図っている。以下に学校情報セキュリティポリシーを示す。

＜青葉小学校の情報セキュリティポリシー＞

青葉小学校の情報セキュリティーポリシー

1　目的

この情報セキュリティーポリシーは，国分市立青葉小学校における児童，保護者，教職員等の個人情報及び学校運営上の重要な教育情報等の機密性，完全性，可用性を守るために必要なルール全般のことである。なお，「国分市立小・中学校情報教育及び校内 LAN の運用に関する規程」及び「国分市立小中学校情報セキュリティーポリシー(案)」に基づき作成するものとする。

◇ 機密性（confidentiality）・・・情報の機密を守ることを意味する。（許可されていない人が勝手に情報を見たり変更したりできないようにする必要がある。）

◇完全性（intergrity）・・・・・・情報が改ざんなどされず正しい状態であることを意味する。

◇可用性（availability）・・・・・・許可された利用者が必要なとき情報に確実にアクセスすることを意味する。

2　学校のネットワークシステム

○コンピュータ室・・41台のコンピュータ
　1台のサーバコンピュータ
○普通教室・・・・・24台のコンピュータ
○特別教室・・・・・　6台のコンピュータ（校長室，保健室，特別支援教室，少人数指導室，図書室，音楽室）
　1台の統括サーバ（校長室）

※上記のコンピュータは，平成16年度に国分市教育委員会が設置したものである。
※ 上記のコンピュータはＬＡＮ（10-BASE-T/100-TX）で接続されており，コンピュータ室内のルータを通して，ＮＴＴケーブルテレビ回線に接続されており，インターネット接続が可能である。ウィルス対策ソフト及びフィルタリングソフトによりウィルス対策及び有害情報対策を行っている。
※ 上記のコンピュータには，グループウェアソフトがインストールされており，校内でイントラネット形式での情報通信が可能である。
※ 校務サーバには，USB 認証システム HardLock 専用ハブを通じてすべてコンピュータが接続されており，USB 認証キーを利用した場合のみ，校務サーバに接続して，個人情報や教育情報へアクセスできる。

○職員室・・・・・・1台のコンピュータ（2000server）
○体育室・・・・・・1台のコンピュータ（XP）
○会議室・・・・・・1台のコンピュータ（2000pro）
○家庭科準備室・・・1台のコンピュータ（2000pro）
○コンピュータ室・・1台のコンピュータ（XP）
○理科室・・・・・・1台のコンピュータ（2000pro）

※ 上記のコンピュータは，平成16年度以前に，学校予算の中から購入して設置したものと，「リサイクル PC」として無償でいただいたものであり，校務で活用していく必要上，教育委員会に申請して，校内LANに接続できるようにする（申請，教育委員会に許可申請をする）

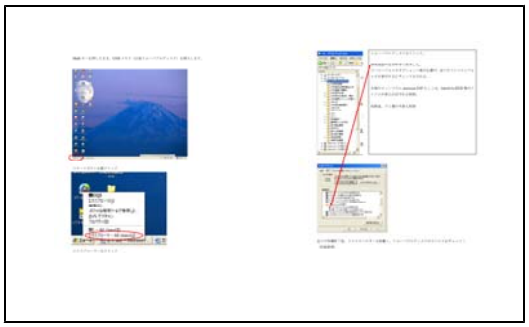
-1-

（クリックすると拡大されます）

(2) 最新情報の提供

不正侵入やウィルス感染については，常に新しい手法や種類に関する情報を共有するため，定期的に最新情報に基づいた資料を作成し，配布している。以下にＵＳＢメモリを介して感染するウィルスへの対策文書の例を示す。

＜ＵＳＢメモリを介して感染するウィルスへの対策を示した文書例＞



（クリックすると拡大します）

(3) 職員の意識向上の取組

作成した資料は配布するだけでなく，職員室に掲示したり，コンピュータ等の近くに置いたりするなど，常に職員が閲覧できるようにし，情報セキュリティに対する意識の向上を図っている。

また，校内ＬＡＮの共有サーバを利用した情報共有の取組などの工夫も行っている。

情報セキュリティに関する最新の情報を閲覧することができるWebサイトの例を以下に示す。これらのサイトを参考に，情報漏えいの事例やウィルス被害の最新動向などを参考にしていただきたい。

○　鹿児島県総合教育センターWebサイト
　学校の教育情報化推進に役立つﾘﾝｸ集
　http://www.edu.pref.kagoshima.jp/infomation/rink/top.html
○　コンピュータ教育開発センター
　http://www.cec.or.jp/CEC/
○　情報処理推進機構
　http://www.ipa.go.jp/
○　学校情報セキュリティサイト
　http://www.school-security.jp/

また，情報セキュリティやウィルス対策に関することについては指導資料（通巻第1523号，1603号，1626号）でも述べているので参考にしていただきたい。

〔参考文献〕

○　文部科学省「教育の情報化に関する手引」
平成21年３月
○　コンピュータ教育開発センター「学校情報セキュリティ・ハンドブック(改訂版)」平成19年３月

（情報教育研修課）