http://www.edu.pref.kagoshima.jp/ （通巻第1523号）

# 指導資料

鹿児島県総合教育センター

情報教育　第106号

―小，中，高，盲･聾･養護学校対象―

平成18年5月発行

## 学校における情報セキュリティの在り方

各学校においては，校内ネットワークの整備により，ファイルデータやデータベースなどの学校情報や生徒情報という情報資産を共有化し，校務の効率化が図られている。

しかしながら，デジタルデータが無防備な場合は，誰もがアクセス可能であり，データの取り込みも容易である。そのため，外部からのファイルの削除や変更を目的としたサーバ等への不正アクセスやコンピュータウィルスの浸入などにより情報資産は危険にさらされている。

また，情報を保存したメディアやパソコンなどの紛失，盗難などによる様々な想定外の個人情報漏洩問題が起きている。

さらに，人為的な攻撃だけでなく，地震や落雷などの自然災害も情報資産に対する安全性の脅威となっている。

このようなことから，学校においての校内ネットワーク上のトラブル等を未然に防ぐためのセキュリティ対策が喫緊の課題となっている。

そこで，本稿では，校内ネットワークに関する情報セキュリティの問題点とその対策及び学校における情報セキュリティポリシーについて具体的に述べる。

### 1　校内ネットワークの情報セキュリティ

情報セキュリティとは，「情報の漏洩防止（機密性）」，「情報やそれらの処理が正確であること（完全性）」，「許可された利用者がいつでもシステムにアクセスできること（可用性）」の3点を安全に維持することである。

このことを踏まえて，情報資産に対する様々な脅威について，その問題点と対策を述べる。

#### (1)　不正アクセス

正当なアクセス権を持たない者による不正な手段を使った学校内部の情報システムやコンピュータへのアクセスのことであり，個人情報や学校の機密情報等の漏洩，学校Web ページの改ざん・消去などの被害が生じる。

この対策としては，

ア　常時接続の場合には，ルータの持つファイヤウォール機能（コンピュータネットワークへ外部からの侵入を防ぐ機能）を有効にすることで，通信に必要な信号しか通さず不正なアクセスをブロックできる。同時にウィルス対策

ソフトやWindowsのサービスパックを使うことで，より強化することができる。

イ　ソフトウェアのアップデートを行ったり，修正プログラム等をインストールしたりすることでセキュリティホール（セキュリティ上問題となるソフトの弱点）をふさぐことも重要である。

今後の校内ネットワーク構築では，無線ＬＡＮでの構築も予想されるが，情報が無線上で学校内外へ流れる可能性もあるので有線ＬＡＮを使用する以上にセキュリティに配慮しなければならない。

(2)　コンピュータウィルス

パソコンにトラブルを起こすことを目的として作られたプログラムであり，感染すると情報システムの停止や破壊が起こる。最近では，Webページを見るだけで感染するものがある。

特に，電子メールの添付ファイル等安全性が確認できないものは，絶対に開かないようにすることが大切である。

対策としては，

ア　ウィルス対策ソフトの導入が不可欠である。万一感染した場合は対策ソフトで駆除や復元を行う。

イ　パソコンをリカバリーし，購入時の状態に戻すこと等で安全策を図ることができる。

(3)　生徒の過失や故意への対策

インターネットを利用したチャットや掲示板などよる誹謗・中傷などの書き込み，不適切なサイトの閲覧や校内サーバ等への不正アクセスなどがある。社会的・教育的影響が大きく児童生徒の日ごろの利用には注意しなければならない。

対策としては，

ア　ユーザ認証をさせてインターネットへアクセスさせることにより，ログ（履歴）を取りトラブルの対応に備えたり，プロバイダや各学校においてファイヤウォール機能を有効にし，二重にアクセス制限を行ったりすることが大切である。

イ　サーバを役割ごとに分けて，児童生徒が使用するパソコンは，校務処理のパソコンのサーバとＬＡＮを切り離しておくことが望ましい。

ウ　「利用上のきまり」等を作成して教室等へ掲示するなど注意を促し，タイミングをとらえて，情報モラルの指導を行うこと等が防止策として有効である。

(4)　職員の過失や故意への対策

教職員による誤操作，規定やモラルを無視した様々な出来事により，個人情報や機密情報等の漏洩等様々な事例が報告されている。場合によっては，被害者でなく加害者となるケースも増えている。これらのことから教職員においても，モラルと情報セキュリティ意識の向上が必要である。

ア　パスワード管理

パスワードについては，日常から管理に気を付け，パソコンの周りにはり付けるなどせず児童生徒の目に触れることのないようにしたい。パスワードは推測しにくいものとし，定期的に変更すべきであり，「アルファベット・数字・記号を

混ぜる」，「意味のある単語は使わない」などに留意して設定する必要がある。

イ　情報資産のバックアップ

操作のミスによるファイルの書き換え・削除，記録媒体の不良，落雷や停電によるデータのクラッシュ等の予期せぬ事態についての対策として，定期的にバックアップを行うことが推奨される。

その際，ソフトウェアを利用して自動的にバックアップをすれば，学校における情報管理担当者の定期的なデータバックアップ作業等に係る校務の軽減を図ることができる。経費面の負担を考えるとその機能を持つフリーソフトがあるので検討されたい。

【情報資産のバックアップの方法】

- 外付ハードディスクやＬＡＮ上におけるバックアップ用ドライブ活用
- ＵＳＢメモリ，ＣＤ，ＭＯ，ＤＶＤなどの外部媒体への保存
- インターネットサービスの利用
- 複数のハードディスクを内蔵させてのディスクのＲＡＩＤ化

※　RAID 化：データを分割し，複数のディスクに書くことで保存の信頼度を高めること。

## 2　情報セキュリティポリシーについて

### (1)　情報セキュリティポリシー

情報の取扱いについては，これまで個人のモラル等に任されていたが，情報化社会の中で，今までに予想できなかった様々な問題が起きている。

これからの学校においては情報管理の視点から，取扱いに関する「ガイドライン」（情報セキュリティポリシー）を作成し，いかなる事態にも対応できる態勢作りが必要である。

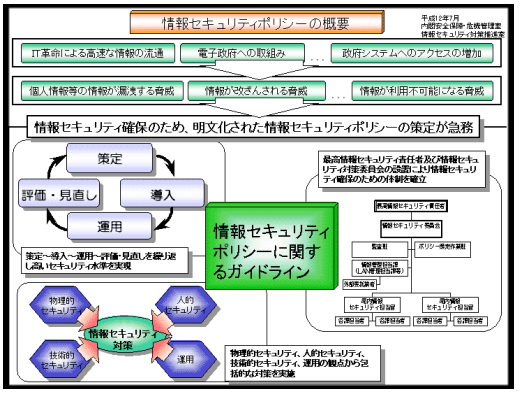


図１　情報セキュリティポリシーの概要
（出典：情報セキュリティ対策推進室）
（図をクリックすると拡大されます）

### (2)　情報セキュリティポリシーの作成

セキュリティポリシーを作成する目的は，学校の情報資産をセキュリティ上の脅威から守ることである。導入や運用を通して，教職員等の情報セキュリティに対する意識の向上や保護者等への信頼性の向上といったメリットも考えられる。

【作成上の留意点】

ア　学校として意思統一され，明文化したポリシーを策定すること。

イ　情報資産の重要度を分類，評価して，守るべき情報資産の内容に応じた情報セキュリティ対策を取ること。

ウ　「策定」，「導入」，「運用」，「評価」を一つの実施サイクルとし，サイクルを止めることなく実施すること。

エ　「評価」，「見直し」の手法として，情報セキュリティ全般に関するネットワークやサーバの情報セキュリティ監査を取り入れること。

## 3　情報セキュリティポリシーの作成例

各学校においては，情報セキュリティの必要性は理解されているが，情報資産の管理についての規程を示している学校はあまり多くない。そこで，学校における「情報セキュリティポリシー」の作成例を示す。

### ○○○学校情報セキュリティポリシー（例）

**1　情報セキュリティの基本方針**

児童（生徒），保護者，教職員などの個人情報及び学校運営上の重要な教育情報を保護して適切に管理・運用するためのルールを定める。

**2　対象者**

情報セキュリティポリシーの対象は，本校の教職員等とする。

**3　組織・態勢**

(1)　学校長は，すべての情報セキュリティに関する権限及び責任を負う。
(2)　職員は，本情報セキュリティポリシーの内容を遵守しなければならない。
(3)　校務分掌又は委員会において情報セキュリティ担当者を置く。
(4)　職員は，異動・退職などの場合には，知り得た情報を学校外で漏らしてはならない。
(5)　新任者には，情報セキュリティの研修会を行う。
(6)　システムで使用するパスワードは，他人に推測されにくいものとし，その管理は十分に行う。

**4　情報機器・ネットワーク管理**

(1)　情報セキュリティ担当者は，サーバ等の管理を行い共有フォルダのバックアップを定期的に行う。
(2)　個人のパソコンをネットワークに接続する際は，学校長の許可を得る。
(3)　使用するパソコンにソフトウェアをインストールする場合やメモリ等を増設する場合は，情報セキュリティ担当者の許可を得る。
(4)　校務処理を行う個人機器には，ウィルス対策ソフトをインストールする。
(5)　不正アクセス等を防止するため，情報システムを利用するすべての者は，適切なるパスワードの管理を行わなければならない。
(6)　インターネットの利用や電子メールの利用については，教育活動に限定する。

**5　個人情報の保護**

(1)　学校及び自宅において，校務や児童（生徒）の個人情報を扱うパソコンにはファイル交換ソフトをインストールしない。
(2)　児童（生徒）に関する指導記録，名簿，成績などのデータをコピー又は印刷し，校外へ持ち出さない。

**6　運用**

(1)　管理職及び情報セキュリティ担当者は，本ポリシーが適切に遵守されているか確認する。また，重大なポリシー違反が明らかになった場合は，緊急時対応計画に基づいて，迅速に対応を行う。
(2)　緊急時の対応については，管理職に連絡する。また，情報セキュリティ担当者は，原因の特定，被害や影響の範囲の把握，経過の記録などを行い，被害が拡大しないようネットワークを停止し，業者へ連絡するなどの対応を行う。

**7　評価・監査・見直し**

本ポリシーは，常に実態との相違等を評価し，監査を行う。また，その結果，必要な場合は見直し及び更新を行う。

情報セキュリティ対策を施すことは，教職員はもとより，児童生徒もセキュリティについての正しい知識と対応を身に付けることになり，情報化社会で生きていくための情報モラルの育成につながる。是非，各学校でも積極的に取り組んでいただきたい。

【参考文献】　村上今雄・野間俊彦著『学校の情報セキュリティ』　ぎょうせい　平成17年11月



（情報教育研修課）