情報セキュリティと危機管理

柏崎市立教育センター　　学校経営講座
中山　博迪　　2008.6.4

情報化社会の特性

- 情報の量が飛躍的に増加、速さも瞬時
- 情報は回転寿司（情報活用の実践力）
- 情報のフラット化で社会が変化
- デジタル化された情報の可塑性
- 顔が見えないネット参加によるコミュニケーション
- 民主党指名争い　オバマ氏勝因(?)はネットの力

国の取組

・5年以内に世界最先端のＩＴ国家（e-Japan戦略　2001年）
・２００６年以降も世界最先端であり続ける(e-Japan戦略Ⅱ2003年)
・いつでも、どこでも、誰でもＩＴの恩恵を　（ＩＴ新改革戦略　2006年）

市の取組

・柏崎市における「教育の情報化」推進プラン
（ 2008年2月　策定）

人材育成

学校における教育の情報化

「教育の情報化」の目的

① 児童生徒の情報活用能力を育成する
② 校務の適正な執行と効率化を図る

情報活用能力の育成とは

① 情報活用の実践力
② 情報の科学的な理解
③ 情報社会に参画する態度
①、②、③をバランスよく育成すること

教員のＩＣＴ指導力の向上

①ＩＣＴ教育研修の充実
・教育の情報化を推進する教員の養成
②情報化を推進する校内体制の整備
・校内の情報化推進計画、情報管理規程等の整備
③校内研修の実施
・ＩＣＴを活用した授業実践
・児童生徒の情報モラルの育成
・学校における情報管理

学校における情報管理

「個人情報保護法」の基本理念と目的

2003年5月に成立、2005年4月より全面実施された。

基本理念

「個人の人格尊重」の理念のもとに慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。

目的

個人情報の有用性を配慮しつつ、個人の権利・利益を保護する。

・学校では、教育目標を達成するために、児童生徒等の氏名、住所、電話番号、成績及び健康状態等、非常に多くの個人情報を取り扱っている。教職員一人一人が、個人情報の取得・利用や保管方法など、個人情報の扱い方について正しい知識を身に付けることが大切である。

個人の権利・利益の保護に努める

学校内における個人情報

（校長室）

児童・生徒指導要録　卒業アルバム　卒業証書授与台帳　職員名簿　PTA役員名簿　同窓会名簿　教職員の人事関係の書類　教職員の勤務状況や教員評価に関する書類　児童生徒の個人情報が入ったUSBメモリー等の外部記憶媒体

（職員室）

家庭環境調査票　成績表・通知表　児童・生徒名簿　児童・生徒緊急連絡網　教育相談記録票　事故報告関係文書　健康保険証のコピー　職員出勤簿　職員緊急連絡網

各種アンケート　児童・生徒の学習記録

（保健室）

健康診断票　身体検査記録票　健康手帳

緊急時の保護者連絡先　カウンセリングノート

リスク　マネジメント（Risk　Management）

（危険が起こる前に危機的状況を回避する。起こったときに最小限に抑える）

- 危機対応マニアルの作成
- CMチームの編成
- CMの実施（問題対処、原因究明、説明責任）
- CM体制の見直し

クライシス　マネジメント（Crisis　Management）

（危機が起こったときに、これ以上悪くなることを回避する）

- 問題や事故への対処
- 事実関係の整理・原因の究明
- 説明責任の遂行（マスコミ対応、保護者対応など）

個人情報流出事例①

- ７月、Ｋ県Ｋ市の男性中学校教諭（２４）が、買い物のためにショッピンセンターに乗り付けたバイクのカギを抜き忘れ、買い物を終えて戻ったところ、バイクがなくなっていた。バイクのトランクに、生徒１１５名分の中間テスト結果の入ったＵＳＢメモリーが入っていた。
- この学校では、PC本体に個人情報等を記憶させないことにしており、備品のメモリーに記憶させ、校長室でまとめて保管していた。私物のメモリーに記憶させることも、外部に持ち出すことも禁止していた。

個人情報流出事例②

- 3月、Y県K市の中学校男性非常勤講師（24）が、内規に反しデータを自宅に持ち帰って成績処理をしていて、146人分の成績データがファイル交換ソフト「ウイニー」を介して流出した。
- 市教委の調査に対して、非常勤講師は「不注意で大変なことをしてしまった。認識が甘かった」と話しているという。市教委は、生徒や保護者に謝罪するとともに、男性への処分も検討する。

個人情報流出事例③

- 4月、M県T市の中学校男性教諭（24）が、卒業生174人の個人情報などを保存していた個人用USBメモリーを紛失した。
- 教諭は校長に無断で、個人情報をUSBメモリーに保存、買い物に訪れたショッピングセンターを出た後、ズボンのポケットに入れていたUSBメモリーがなくなっているのに気付いた。

個人情報流出事例④

- 3月 、F県I市の県立高校の女性養護教諭（54）の自宅から全校生徒約1000人の健康診断の結果と2年間分の保健室日誌の入ったパソコンが盗まれた。同養護教諭が家族旅行から帰宅した際、自宅1階の居間の窓が開いており、テーブルに置いたパソコンが盗まれているのに気付いたという。
- 同校は、「生徒の個人情報の持ち出しは禁じられており、誠に遺憾。生徒や保護者に申し訳ない」と話している。

個人情報流出事例⑤

- 6月、I県N市の小学校女性教諭（23）が児童の情報を無断で持ち帰り、自宅のパソコンに入れたファイル交換ソフト「ウイニー」を経由して、インターネット上に流出した。
- 女性教諭は昨年度、複数回にわたり、校長の許可を得ずに情報が保存されたUSBメモリーを自宅に持ち帰り、成績処理などの作業を行っていた。同年12月にウィニーをパソコンに入れたという。

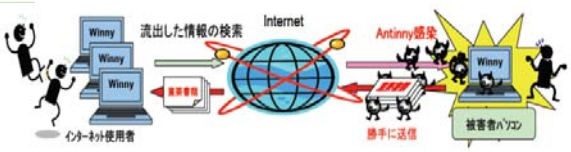
ウイニーによる流出

・ウイニーとは

インターネットに接続したパソコンどうしで音楽や画像などのデータを交換し合うファイル交換ソフト。（2002年に登場）

・アンチニーとは

パソコン上のファイルを勝手にインターネット上に流出させるコンピュータウイルス。（暴露ウイルスの一種で2003年に登場）



ウイニーによる流出（典型的なパターン）

パソコン（データ）を家に持ち帰る

↓

インターネットに接続する
（ウイニーウイルスに感染）

↓

情報流出！！

情報セキュリティポリシーの概要

柏崎市教育委員会

「セキュリティポリシー」とは何か？

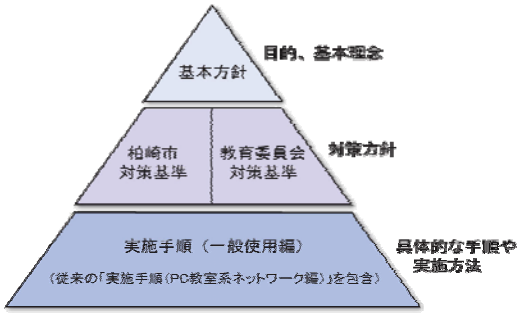
- **一般的には**
  - 情報の目的外利用や外部からの侵入、機密漏洩などを防止するための方針を定めたもの。
- **柏崎市における情報セキュリティポリシー**
  - 柏崎市が所掌する情報資産に関するセキュリティ対策について、総合的、体系的、具体的にとりまとめたもの。
  - 柏崎市全体のセキュリティポリシーと教育委員会独自に定めた部分がある。

なぜ今厳しいルールが必要か

- **世の中では**
  - アナログ（紙）→デジタル（電子データ）という社会の流れ
  - あらゆる組織におけるネットワーク化の推進
  - 情報漏洩などの事件が年々増加している現実
  - 県教委からも個人情報の流出には懲戒処分を含む厳罰を持って臨むとの厳しい通知が出ている(H19　5/10)
- **市内の教育機関では**
  - セキュリティ対策の必要性に対する認識不足
  - ウィルス感染やパソコン盗難事例

実効性のあるルール作りが必要

情報セキュリティポリシーの構成



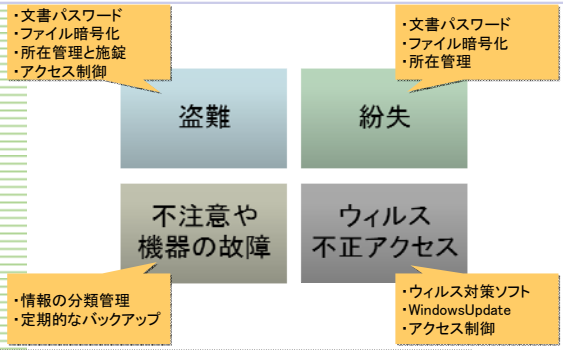
柏崎市の組織・体制について

- **情報セキュリティ最高責任者（歌代教育次長）**
  - 総括的な意思決定と、責任を負う。
- **情報セキュリティ委員会**
  - セキュリティポリシーの策定および重要事項の決定を行う。
- **システム管理責任者（矢沢指導主事）**
  - 情報システムの管理および情報セキュリティに関する総括的な対応にあたる。
- **情報セキュリティ責任者（各学校の校長）**
  - 各学校の校長がその任にあたり、総括的な意思決定と、当該教育機関内、他の組織および個人に対する責任を負う。
- **システム管理者（各学校の担当者）**
  - 各学校内における情報システム管理および情報セキュリティに関する総括的な対応にあたる。

重要なことは

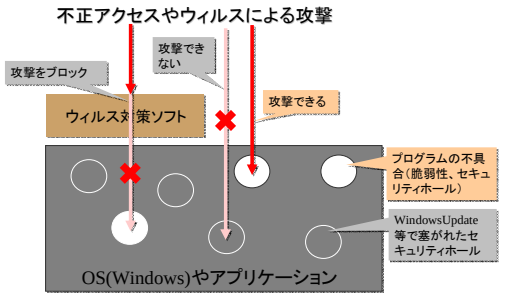
- **個人情報の安全な管理**
  - 一般企業に比べて、はるかに機密性の高い情報を扱っているという意識が必要
- **児童生徒の情報活用能力の育成**
  - 情報モラルの育成も含めた取組を
- **教育の情報化への対応**
  - 業務の効率化、授業の改善
- **適切かつ安全な情報提供**
  - 学校ホームページの役割の再確認を
- **ネットワーク社会の一員として他の利用者に迷惑をかけないための意識**
  - 1人の不注意が市全体のネットワークに影響を与えることになる事を忘れずに

リスクの分析と対策 ―情報資産を何から守るか―



25

WindowsUpdateやウィルス対策ソフトの役割



26

セキュリティポリシーの概要(1)

- **情報の分類と管理**
  - 「公開」と「非公開」に区別して管理
  - 「非公開」情報には文書パスワードを設定
    - 毎年4月にパスワードを変更して届出
    - だれでもが開ける形で保存しないこと
  - ネットワークの区別
    - PC教室系では「非公開」情報を扱わない

27

セキュリティポリシーの概要(2)

- **物理的セキュリティ**
  - 施錠可能な部屋で管理するなどの盗難対策が必要
  - 機器の所在管理を徹底する
    - どの機器がどこにあるか（様式2-2-3　公用情報機器管理表）
  - 個人所有PCは使い方によって許可が必要
    - 教務室系ネットワークに接続する場合
      （WindowsUpdateやウィルス対策ソフトの適切な利用が必須）
    - 「非公開」情報を扱うことがある場合

28

セキュリティポリシーの概要(3)

- **人的セキュリティ**
  - 組織・体制と役割
    - **各学校におけるセキュリティ責任者は校長**
    - 担当者まかせとならないように
  - 教育・研修の重要性
    - 校内研修や教育センターにおける研修などを活用して定期的な意識づけを
  - 事故・障害の報告
    - メール等でウィルスが検出されても感染しなければ報告の必要はない（不安な場合は連絡を）
    - ウィルス感染や情報漏洩の発生時は定められたルートで報告を

29

セキュリティポリシーの概要(4)

- **技術的セキュリティ**
  - 公用PCの構成変更には許可が必要
    - 周辺機器の接続、ソフトウェアのインストール
  - 日常的なセキュリティ管理（WindowsUpdateなど）
    - **教務室系で使用している公用PCはシステム管理者を中心に学校で対応する**
    - PC教室系で使用している公用PCは原則業者が定期点検時に対応している
  - アクセス制御
    - パスワードのメモを人目につく場所に置かない
    - ログインしないと使えないようにする
    - 教務室系ネットワークは毎年4月にパスワードを変更して届出
    - ログイン状態で長時間放置しない

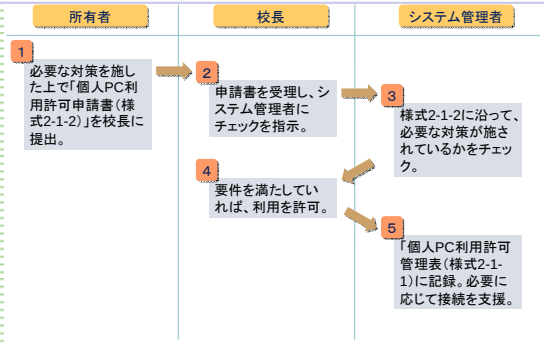
30

セキュリティポリシーの概要(5)

- **評価・見直し**
  - 情報セキュリティ監査
    - 毎年2月頃、セキュリティチェックを実施している
  - セキュリティ委員会の招集
    - 毎年少なくとも1回招集している(3月頃)
    - 必要に応じて招集
  - ポリシーの見直し
    - 現状のポリシーも完成形ではない
    - 運用実態や利用者の意見等により変更も

31

個人PC利用許可の手順



32

システム管理者の主な業務と提出書類

4月
- 文書パスワードの変更、提出。
- 教務室系先生用パスワードの変更、提出(LANDISKはKASIXに依頼して変更)。
- 個人PC利用許可のチェックと「個人PC利用許可管理表(様式2-1-1)」の維持(届出不要)。
- 個人PCの教務室ネットワークへの接続支援(KASIXに支援を依頼してもよい)。

2月
- セキュリティチェックの取りまとめ、提出。

3月
- セキュリティ委員会への参加。

定期・随時
- 教務室系公用PCのセキュリティ対策と教職員への適切な対策の周知。
- 重要な情報の定期的なバックアップ。
- USBメモリ型暗号化キー(Hardlockey)の管理。
- 公用PCへのソフトウェアのインストール、周辺機器の追加などは「情報機器構成変更申請書(様式2-2-1)」を提出して許可を得てから。
- 機器のトラブルや、ウィルス感染等のトラブル発生時の対処。

33

ウィルスの進入経路を知る

- CD-ROMやFD、外部機器から
  - 雑誌の付録や市販のソフトからの感染例も
  - 学校にある古いFDはとても危険
- 電子メールから
  - 添付ファイルを開かなくても感染する場合も
  - メール本文のリンクをクリックだけでも危険な場合も
- ホームページから
  - 開いただけでそこに埋め込まれたウィルスに感染する場合も
- LANから
  - 1台でも感染したPCがあると全体に影響を及ぼす
- 不正アクセス
  - インターネット経由で直接攻撃を受け、PCを乗っ取られる場合も

ウイルスに感染した場合の処置

- コンピュータの使用を停止し、システム管理者の指示を仰ぐ。
- 最新のウイルス対策ソフトで検査を行い、ウイルス名を特定する。
- ウイルスに合った適切な駆除を行う。
- データが破壊されたときは、バックアップから復旧する。
- 最新のウイルス対策ソフトでもう一度検査を行う。
- 再発防止の予防策を講じる。

全ての利用者が行うべき対策(1)

- **ウィルス対策ソフトを正しく使う**
  - インストールしただけでは効果は薄い。最新の状態を保つことが重要。
  - ウィルスの侵入経路は様々。ネットワークにつながなくても必要である。
- **脆弱性(セキュリティホール)をふさぐ**
  - 定期的にWindowsUpdate,OfficeUpdateを実行して、ウィルスや不正アクセスの入り口をふさぐ。
  - 脆弱性が公開された後のすばやい対応が重要。
- **電子メールソフトを正しく設定する**
  - プレビューは表示されないように設定する。
  - HTML形式のメールは送らない。

36

全ての利用者が行うべき対策(2)

- **非公開情報を扱うときは**
  - 盗難や紛失への十分な注意を。（学校内も安全とは言えない）
  - 非公開情報はパソコン内に保持しないのがベスト。
  - 自宅ではインターネットに接続できない状態で。
  - 配布済みのUSBメモリ型暗号化キーを活用する。

- **Winnyなどのファイル交換ソフトを使わない**
  - 個人情報漏洩事件の多くが、このタイプのソフトウェアを利用していたことに起因する。

37

全ての利用者が行うべき対策(3)

- **メディアやPCの廃棄に注意**
  - ファイル削除や初期化をしただけではデータは消えない。物理的な破壊がベストだが、データを確実に消去するソフトを利用するのも有効。
- **最後は個人個人の意識改革が重要**
  - 学校で扱う個人情報は学校のものではない。児童生徒や保護者などから預かっているもの。
  - 努力しなければ情報資産は守れない。
  - やりすぎというくらいの予防措置が必要。
  - 被害にあってからでは取り返しがつかない。
  - パソコンの利用者にとって適切なウィルス対策は義務である。

38

不審な添付ファイルや迷惑メールの取り扱い

- **不審なメールの添付ファイル**
  - 基本的には開かない
- **ユーザーの気を引くような添付ファイル**
  （ファイル名を工夫することによりユーザーを引きつけ感染させることが目的）
- **例:「(お宝)秘蔵写真集」（W32/Antinny）**
  - そのまま捨てる

- **迷惑（spam）メール**
  - そのまま捨てる
- **身に覚えのない架空請求メール**
  - 関係機関に相談、警察に届出
- **デマメール、チェーンメール**
  - ➔ 無視して、転送しない

最後に「これだけは全職員で徹底しよう！」

- ウイルス対策ソフトを正しく使う
  （日々の更新を正しく行う　常時監視機能をOffにしない）
- ソフトウエアのセキュリティホールをふさぐ
  （定期的にMicrosoft　Updateなどを行う）
- 電子メールを正しく使う
  （不審なタイトルのメールは開かない　不用意に添付ファイルを開かない　送受信はテキスト形式にする）
- 個人情報を含むデータの取り扱いに気をつける
  （パスワードを付けるか、暗号化する　WinnyやShareなどのファイル交換ソフトは使わない）

個人情報の安全管理のための取組(参考例)

- 個人情報等の取り扱いに関する校内研修
- 個人情報流出等に備えた危機管理マニュアルの整備
- 個人情報保護方針を内外へ示す
- 個人情報の取り扱いに関する保護者への通知・許諾等
- 個人所有パソコンの使用、安全管理等

危機管理マニュアルの策定(参考例)

個人情報の流出等、緊急対応が必要な場合に備えて、全職員による共通理解の徹底を図る必要がある。

(1)危機管理対策チームのメンバーの選定
(2)事故発生時の報告・連絡手順
(3)対応窓口の一本化
(4)事実調査
(5)原因究明
(6)今後の対応
- 今後の方針
- 児童生徒・保護者への謝罪・説明
- 公表

個人情報保護の方針(参考例)

個人情報の保護について、学校としてどのように取り組むかの基本的な姿勢を内外に示す。

個人情報保護の方針

本校では、個人情報の重要性を認識し、･･･保護に努めます。

1. 個人情報の取得について
2. 個人情報の利用についいて
3. 個人情報の第三者への提供について

校内に掲示する

個人所有パソコンの利用規程について(参考例)

校内における個人所有パソコンの利用規程

1. ファイル交換ソフトがインストールされてる個人所有パソコンを校内での利用は禁止する。
2. 校内で個人所有パソコンを使用する場合は、校長に届け出る。
3. 個人所有パソコンを校内LANへの接続する場合は、校長の許可を得る。
4. 個人所有パソコンを校内LANへの接続を許可する場合は、ウイルス定義ファイルがインストールされ常に最新であることを条件とする。
5. 個人情報等を含む校務のデータについては、外部記憶媒体に保存、管理し、個人所有パソコンのハードディスクへの保存は禁止する。
6. 個人所有パソコンを自宅へ持ち帰るなど、学校外へ持ち出す場合は、校長へ届け出る。

個人情報保護のチェックシート(参考例)

- 柏崎市等の「セキュリティポリシー」の内容を理解しているか。
- 自校のデジタル化された個人情報にどのようなものがあるか把握しているか。
- デジタル化された個人情報を校外等に持ち出す際に、職員は確実に校長の許可を得ているか。
- デジタル化された個人情報の保管場所がきちんと定められており、施錠等の防犯対策が講じられているか。
- 自校のHPを定期的に確認している。またHPの更新について、担当者から連絡を受け、承認しているか。
- 自校の児童生徒への情報モラル育成のための指導がどのような場面で行われているか理解しているか。

学校内の個人情報のチェックシート(参考例)

- 校務分掌として、管理者が明確に決まっているか。
- 管理簿があり、管理場所、責任者等が明確になっているか。
- 金庫等カギのかかる場所に保管すべきものは、厳重に保管されているか。またこれらの資料を持ち出す際の規定が決まっており、遵守されているか。
- 利用目的以外で利用されていることはないか。

個人情報等の漏えい防止規定(参考例)

○○小学校個人情報等の漏えい防止規定

・ウイニーを導入したパソコンを使用しない。
・パソコンに導入しているウィルス定義ファイルが最新である。
・個人情報等を個人所有パソコンのハードディスクに保存しない。
・個人所有パソコンについて校内規程を策定する。

上記規程を全職員に周知徹底する。

大変お疲れ様でした