茨城県教育研修センター

急速な情報化の進展が社会に変革をもたらし，パソコンや携帯電話などが広く普及していることにより，誰もが情報の受け手だけではなく送り手としての役割を担うようになっています。教職員自身も情報化社会の特性を理解した上で，新たな変化についての知識を得ながら柔軟に対応することが求められております。

そこで，本テキストを校内研修等で御活用いただき，情報セキュリティの正しい理解と対策を図っていただけるようお願いいたします。

情報セキュリティ校内研修資料

Contents

学校における情報セキュリティ対策

ネットワークに接続されたコンピュータが普及したことにより，コンピュータウイルス，不正アクセス，その他のハイテク犯罪が増加の一途をたどっている。これらのことから身を守るために，セキュリティ意識を高め，十分な注意を払わなければならない。当たり前の対策を当たり前にするといった心がけが大切である。

特に学校には，卒業生台帳や指導要録，成績一覧表，健康診断票等の公文書や児童生徒の住所録等の情報資産が数多く存在する。学校情報セキュリティとは，こうした学校の情報資産を情報の漏えい，改ざん，破壊，消失等の様々な危険から安全に守ることである。

※指導要録，指導要録の抄本又は写し及び出席簿のコンピュータ等による作成について

（平成 23 年茨城県教育庁義務教育課）

【演習１】　各自の情報セキュリティ対策について確認してみましょう。

No.	確認事項	チェック
1	定期的にＯＳのアップデートをしている	□
2	セキュリティソフトをインストールし，定義ファイルの更新を行っている	□
3	パスワードを付箋に書いてパソコンに貼るなど，人目につくところに記載していない	□
4	パスワードを分かりにくいものにして，定期的に変更している	□
5	無線ＬＡＮを利用するときは，その特性を理解し，適切に利用している	□
6	デジタルカメラ内に児童生徒の情報が残ったままになっていない	□
7	ＵＳＢメモリ等で個人情報を校外に持ち出すときは，管理職の許可を得ている	□
8	不審なメールを受信した場合には，送信者に確認後，メールを開くようにする	□
9	信頼できるWeb ページであるかをよく考え，危険なWeb ページには近づかない	□
10	不要な用紙（個人情報等が記載されているもの）は，シュレッダーで廃棄している	□

【演習２】　下のイラストは，学期末の職員室の様子です。先生たちが忙しく成績処理などを行っているようです。２人の先生は，席を離れているようです。学校情報セキュリティという観点で，問題点を考えてみましょう。（10 カ所）

①山積みで落ちそうな書類

②コーヒーカップ

③パソコンに貼られたふせん

④開きっぱなしの書類

⑤机の境界に積まれた書類

⑥ついたままのディスプレイ

⑦机に置かれたＵＳＢメモリ

⑧机に置かれた重要書類

⑨開きっぱなしの引出し

⑩中身がつまったごみ箱

出典：教育ネットワーク情報セキュリティ推進委員会

１　学校情報セキュリティの確保

ネットワークに接続されたパソコン，多種多様なメディア（媒体），サイバー犯罪による不正アクセス等から学校の情報資産を情報の漏えい，改ざん，破壊，消失等の様々な危険から安全に守ること。

教職員は，常に情報セキュリティを意識して，必要な知識を持ち，対策を考えなければならない。

２　個人情報の管理と情報漏えい

⑴ 個人情報とは

学校では，児童生徒個人に関する情報を扱っている。「個人情報」とは，生存する個人に関する情報であり，複数の情報（名前，住所等）で特定の個人を識別できる情報のことをいう。

⑵ 「個人情報」の種類と範囲

・学校が扱う情報のすべてが対象
・名簿（名前，住所，電話番号等），指導要録，健康診断票，成績一覧表，通知表，家庭環境調査票等（作成中のものも含む）
・個人が特定できる写真やビデオ

⑶ 電子メールによる「個人情報」の流出

複数の人に電子メールを送信する際，「To」「Cc」「 Bcc」のいずれかを設定するが，使い分けをすることが大切である。

宛先に複数のメールアドレスを入力することで，同時に複数の相手にメールを送信することができる。しかし，宛先に入力した全てのメールアドレスが，受信者全員に表示されてしまうので，必要がある場合を除き，他の送信先のメールアドレスが分からないようにすることが重要である。

・To　（宛先）：正式な送信先のアドレスを入力
・Cc　（カーボンコピーの略）： 正式な宛先ではないが，参考に見てほしい場合に利用
・Bcc （ブラインドカーボンコピーの略）：ここに入力されたアドレスは，To や Cc の受信者には表示されない。

個人情報漏えいの結果・・・

個人情報を保有する組織への影響　→　事後対応に追われ業務に支障が出る

・信用失墜につながる
　保護者の間に自分の情報が悪用されるのではないかという不安が広がる。
・業務遂行に支障が出る
　クレームが増大し，対応(謝罪，再発防止等)をしなければならない。
　状況によりマスコミ対応が必要になる。
・実害が発生する
　裁判になれば，損害賠償・慰謝料請求に発展することがある。

実際に問題が発生する原因の多くは，取扱い担当者のちょっとした不注意や認識不足（管理ミス）

→ **ヒューマンエラー**

【対策】
□　個人情報の漏えいや消失等のないように，細心の注意を払う。
□　「当たり前の対策」を当たり前に行う。
　　例：会議で配付した個人データ資料は，終了後ただちに回収し，完全に破棄する。
□　重要な文書の破棄はシュレッダーを使用する。

個人情報の保護に関する法律（平成 15 年５月 30 日成立　平成 21 年６月５日改正）

（第３条）基本理念　個人の人格尊重の理念　→　**個人情報は，適正な取扱いが図られなければならない。**

・私立学校においては　→　**個人情報の保護に関する法律**
・国立大学法人附属学校においては　→　**独立行政法人等の保有する個人情報の保護に関する法律**
・公立学校においては　→　**各地方公共団体の個人情報保護条例等**

茨城県個人情報の保護に関する条例
（平成 17 年３月 24 日　茨城県条例第１号）

茨城県個人情報の保護に関する条例施行細則
（平成 17 年５月 30 日　茨城県教育委員会規則第 13 号）

学校における生徒等に関する個人情報の取扱いに係るガイドライン
（平成 17 年４月　茨城県教育委員会）

が適用される。

３　コンピュータの管理

仕事をしている最中に，席を離れることがある。そういった状況の中で悪意のある部外者が侵入して，重要な情報を盗み出したり，データを改ざんしたりしてしまうおそれがある。また，ノートＰＣやタブレットＰＣは携帯性があり，校外に持ち出す機会が多い。車内に置いたまま放置するようなことは絶対に避け，盗難には十分注意する必要がある。

【対策】
□　席を離れるときには，ディスプレイに表示されている情報を閉じる。
（Win キー  ＋　Ｌ）
□　パソコンのハードディスクには，原則として個人情報を保存しない。
□　パソコン等の盗難に気を付ける。
□　Windows 等のＯＳについては，常に更新情報を収集して，できる限り迅速にアップデートをする。
□　クライアントソフトの脆弱性を突いた攻撃への防御として，インストールされたソフトを最新のものにアップデートをする。

４　メディアの管理

ＵＳＢメモリ，外付けハードディスク，ＣＤ　Ｒ等といったメディアをきちんと管理することが大切である。また，それらが不要になった場合，内部のデータを消去しないまま処分してしまうことがないようにすることが重要である。

【対策】
□　重要な情報や個人情報が入っているメディアは，鍵のかかる場所に保管する。
□　パソコンやメディアを廃棄する場合は，データを完全に消去するか物理的に壊した後に廃棄する。
□　万一に備え，データのバックアップをする。
□　不用意に個人情報をコピーしたり，職場から持ち出したりしない。
□　重要なデータには，暗号化とパスワードの設定をする。
□　ＵＳＢメモリ等を外部で使用した後，職場のＰＣに接続する際には，最新のウイルス対策ソフトでスキャンする。

５　パスワードの管理

パスワードが他人の手に渡って，パソコンの中にある重要な情報が漏えいしたり，データが改ざんされたりする危険性がある。ＩＤ，パスワードは厳重に管理することが大切である。

【対策】

強力なパスワードを設定（長さと複雑さが重要）

□　パスワードは，文字，数字，記号が組み合わされて，８文字以上が理想である。
※英字大小文字（26 種×２）＋数字（10 種）＋記号（約８種）　70 の８乗（８文字）
（≒約 576 兆通り）

□　自分の名前，誕生日やまたはそれに類似した情報についてのパスワードは使用しない。

□　定期的に変更する。

□　パスワードをＰＣに保存することや，オートコンプリート機能は使わない。
（特に共有ＰＣの場合）

６　ウイルス対策

ウイルス感染は，ＵＳＢメモリなど外部記憶媒体を経由することや電子メールからの感染，悪意のあるWebページを閲覧したことによる感染が大半を占めている。ウイルスに感染するとデータが破壊されたり，情報漏えいを引き起こしたりするものもある。インターネットからダウンロードしたファイルや電子メールの添付ファイルを開くときには注意が必要である。

ウイルスの主な侵入経路
- ＵＳＢメモリ等のメディアからの感染
- 電子メールからの感染
- 悪意のあるWebページを閲覧したことによる感染
- フリーソフト等のダウンロードによる感染

【対策】

□　ウイルス対策ソフトをパソコンに必ずインストールし，定期的に更新して，常に最新のパターンファイルにしておく。

□　セキュリティホールには，修正プログラム（セキュリティパッチ）をあてる。

□　不審な電子メールや添付ファイルは開かずに情報担当者へ連絡する。

□　不明なファイルはダウンロードしないようにする。

学校情報セキュリティの確保は「校務の情報化」を進める上で，特に留意しなければならない。「教育の情報化に関する手引」では，確保すべき学校情報セキュリティの内容として下記を挙げている。

(1) システム構成の基本
(2) １人１台のコンピュータの必要性
(3) 学校情報セキュリティポリシーの策定
(4) 校務用データファイルの保存の仕方
(5) 電子データの持ち出し

情報セキュリティについて教職員が持つべき知識

１　不審なWeb ページへの対応

Web ページの中には，アダルトサイトや暴力がからんだ有害なものが存在する。犯罪に関わるようなページは子供たちがトラブルに巻き込まれるおそれがある。また，個人情報を盗んで悪用したり，不正プログラムを送り込んでデータを盗んだり，ウイルスに感染させるといったわなが仕掛けられた悪質なものもある。子供たちにとって有害なページに対しては，フィルタリングソフトを導入し，アクセスできるサイトを限定することが大切である。

【対策】
- □　不審なWeb ページには近づかない。
- □　信頼できるWeb ページであるか，よく考える。
- □　フィルタリングソフトを導入する。

２　無線ＬＡＮ対策

無線ＬＡＮは，ネットワークケーブルを必要としないという手軽さを背景に年々普及している。しかし，適切なセキュリティ設定を行わないで使用すると，情報が盗まれる，情報の改ざん，漏えい，破壊などの被害を受ける可能性がある。最近では，無線ＬＡＮのアクセスポイントを求めて走り回るといったウォードライビングという行為が横行している。

【対策】

通信データを暗号化する安全度の高いセキュリティ機能を導入する。
- □　データを暗号化する。（ＷＰＡ，ＷＰＡ２等の設定）
- □　アクセスポイントを識別する名前（ＳＳＩＤ）を他の無線ＬＡＮ対応機器で表示できないように設定する。（ステルス機能）
- □　アクセスできる機器を制限する。（Ｍａｃアドレスフィルタリングの設定）

参考ＵＲＬ

「安心して無線ＬＡＮを利用するために」（総務省　平成 24 年 11 月）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/lan/pdf/lan_1.pdf

３　不正アクセス

他人のＩＤやパスワードを無断で使用し不正アクセスをする行為，不正に侵入する行為，踏み台を使った侵入行為などを不正アクセスという。これらの行為は平成 12 年２月 13 日に施行された「不正アクセス行為の禁止等に関する法律」（不正アクセス防止法）で処罰の対象となる。また，他人のパスワードを許可なく第三者に教えることは不正アクセス行為を助長した行為となり，処罰の対象となる。セキュリティ侵害は，犯罪のこん跡が残りにくく，時間，場所の特定が非常に困難である。

【対策】
- □　管理的な対策を行う。
  - ・ウイルス対策ソフトやファイアウォールなどの技術的な対策や安全性，信頼性の確保をする。
  - ・パスワードの管理（なりすまし対策）や不要なときはパソコンの電源を切るなどのセキュリティ対策をする。
  - ・情報の保管等を厳重にしたり，立ち入り制限区域を設けたりする。
- □　情報セキュリティ意識の向上，ルールの策定とその遵守，一人一人の意識の向上といったことが大切である。

４　標的型メール

標的型メールとは，サイバー攻撃の一種で，攻撃や情報漏えいなどを目的として，企業や個人を対象に送りつけられる電子メールのことである。

特徴としては，電子メールを送りつける対象者を特定し，差出人として実在の人物を装う。電子メールの件名や添付ファイルの内容を業務内容と関連したものにする。メールの受信者が偽装に気付かずに添付ファイルを開いてしまうと，その中に組み込まれていた不正プログラムに感染することもある。

【標的型メールの例】

件名　：「【至急】○○教育研究会要項の送付について」
送信者：○○立□□学校　●名前●　　←　**実際に勤務している教職員の名前**
本文：
　○○立○○学校　○名前○　様

　○○立□□学校　●名前●です。標記の件につきましては，添付ファイルの通りです。至急ファイルを御確認の上，参加の有無について返信ください。

　以上，よろしくお願いいたします。

添付ファイル：○○教育研究会実施要項.exe
↑ワープロ文書ではなく不正プログラム
（ウイルス等）の実行ファイル

・標的型メール攻撃は，ひそかに流行しており，教職員自身もターゲットとして狙われる危険性がある。
・近年では実在の関係者や団体を装った内容のメールも確認されており，攻撃を受けていること自体に気付きにくいのが最大の特徴になっている。

【対策】
□　不審な電子メールを受信した場合には，送信者に確認（電話等で）後，電子メールを開くようにする。
□　普段やり取りのない人からの電子メールや差出人にそぐわない内容等，不自然さがある場合は注意する。

【校務用データファイルの管理について（管理職・情報教育担当）】

・　校務用データは，教職員が個々で保管するのではなくセキュリティの確保された安全なサーバを構築し，情報を一元管理することが望ましい。

・　データファイルの事故や消失に備えるためのデータのバックアップについても，情報漏えいを防ぐために，教職員が個々に行うのではなく，計画的に行う必要がある。

・　個人情報の持ち出しは極力避けなければならないが，例外的に校外に持ち出す場合は，データファイルを暗号化するなどの対策が必要となる。

情報セキュリティに関する参考資料

・学校情報セキュリティライブラリ
〔（財）コンピュータ教育開発センター〕http://www.cec.or.jp/seculib/

・ＩＰＡ 情報処理推進機構（Top ページ）http://www.ipa.go.jp/index.html

・映像で知る情報セキュリティ対策（動画）
〔ＩＰＡ 情報処理推進機構〕http://www.ipa.go.jp/security/keihatsu/videos/

・JPCERT コーディネーションセンター（システムの脆弱性に関する情報）
〔JPCERT〕http://www.jpcert.or.jp/

・安心インターネットライフ -ネット社会の７つの常識-
〔(財)マルチメディア振興センター〕http://www.e netcaravan.jp/pdf/newguide_1.pdf

・インターネットトラブル事例集（平成 26 年度版）
〔総務省〕http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho ka/jireishu.html

・警察庁セキュリティポータルサイト@police
〔警察庁〕http://www.npa.go.jp/cyberpolice/

・教育の情報化に関する手引
〔文部科学省〕http://www.mext.go.jp/a_menu/shotou/zyouhou/1259413.htm