「教職員の情報セキュリティ意識を高める校内研修パッケージ」の活用

―校内研修を担当する先生方へ―

本パッケージは，各チェックリストやワークシートから構成されています。短時間で実施できるワークショップ型研修により，セキュリティ意識を高めることができます。本パッケージについては，本書の他，下記URLにコンテンツを置いていますので，御活用ください。

http://www.edu-ctr.pref.okayama.jp/chousa/kiyou/h22/10-06pack/

平成23年２月
岡山県総合教育センター

はじめに

ー校内研修を担当する先生方へー

情報セキュリティの研修をワークショップ型で実施してみませんか？

情報セキュリティは，校務の情報化を進めるに当たって避けて通れない課題といえます。しかし，昨今，教職員が児童生徒の個人情報をＵＳＢメモリ等に保存し，学校から持ち出した際に紛失，盗難に遭った報道が後を絶ちません。

本パッケージでは，こうした学校から個人情報を持ち出す事例を中心に，セキュリティチェックリストや各種ワークシートをパッケージにしました。従来のトップダウン型や講義型の研修ではなく，小グループによるワークショップ型研修で御活用いただき，個々の教職員の情報セキュリティ意識を高めることをねらいとしています。是非，校内研修等にお役立てください。

本パッケージの活用に当たって

多忙な学校に短時間の研修でも活用可能

本パッケージのコンテンツは，以下の六つの章から構成されています。

Ⅰ　「セキュリティ・チェックリスト」（５分）
　　「セキュリティ・チェックリスト解説」（５～10分）
Ⅱ　「校内研修・導入編」（10分）
Ⅲ　「リスクマネジメント編」（１シート約20分×３）
Ⅳ　「クライシスマネジメント編」（20分）
Ⅴ　「研修の振り返り」（５～10分）
Ⅵ　「情報セキュリティ・参考Webページ」

約２時間の研修で順に活用することを想定していますが，研修の時間が十分に取れない場合，一つだけ取り上げて20～30分で活用することもできます。

【研修例１】４月：年度当初の職員会議後，ミニ研修として
- 「Ⅱ　校内研修・導入編」（10分）
- 「Ⅲ　リスクマネジメント編　ー学校から持ち出す時ー」（20分）

【研修例２】６月：職員会議内で１学期（前期）の成績処理に当たって
- 「Ⅲ　リスクマネジメント編　ー自宅で仕事をする時ー」（20分）

効果を上げる研修の進め方

チェックリストやワークシートは，記入用と解説用に分かれています。研修では，まず，各自で考えて記入した後，小グループや全体で発表や協議の時間を取ってください。そこで，セキュリティ意識の「違い」や新たな「気付き」を共有し，最後に解説用のシートで研修のまとめや振り返りをします。

【下記ＵＲＬからダウンロードして御活用ください】

http://www.edu-ctr.pref.okayama.jp/chousa/kiyou/h22/10-06pack/

※　本パッケージの著作権は岡山県総合教育センターに帰属しますが，一般的な情報セキュリティを想定して作成していますので，所管の教育委員会のセキュリティポリシーに応じ，内容を改編して御活用いただいても結構です。

Ⅰ セキュリティ・チェックリスト【５分】

☞研修例＝このチェックリストでは，正解を求めるのでなく，研修への意識付けとします。研修最初の５分程度で記入できます。時間がない場合，事前に配付しておく方法もあります。

以下の各項目について，できているものにチェック ☑ を入れましょう。

セキュリティ全般について

- □ １ 児童生徒の写真や作品は，本人と保護者の同意を得た上で利用している。
- □ ２ 仕事に関係のないWebページは見ていない。
- □ ３ 学校のコンピュータに無断でソフトウェアをインストールしていない。
- □ ４ 機密情報は電子メールで送っていない。
- □ ５ 機密情報を含む紙や記録媒体は，適切な方法で廃棄や削除をしている。
- □ ６ コンピュータのユーザーＩＤやパスワードは，他人に知られないよう管理している。
- □ ７ 電子メールを誤送信しないように注意している。
- □ ８ 離席時や帰宅時にコンピュータを不正操作されないための対策をしている。
- □ ９ コピーやプリンタの出力用紙は，直ちに回収している。
- □ 10 帰宅時には机上を片付けている。
- □ 11 ファイル共有ソフトは，自宅のコンピュータにもインストールしていない。

ＵＳＢメモリ等でデータを持ち出す際について

- □ 12 データを持ち出す際，決められた必要な手続きを知っている。
- □ 13 ＵＳＢメモリなどを持ち出す時には，常に携行している。
- □ 14 持ち出したデータは，パスワードが設定されているか暗号化されている。
- □ 15 ウイルス対策ソフトを自宅のコンピュータにもインストールしている。
- □ 16 ウイルス対策ソフトは，定期的に更新し，最新の状態にしている。
- □ 17 ＯＳ(Windows等)やソフトウェアは定期的に更新し，最新の状態にしている。
- □ 18 自宅で使用したデータは，自宅のコンピュータから必ず消去している。

セキュリティ・チェックリスト解説　【5～10分】

セキュリティ全般について

□　１　児童生徒の写真や作品は，本人と保護者の同意を得た上で利用している。

　児童生徒の個人情報の管理は大切です。学校新聞やWebページに顔写真や児童生徒の作品を掲載する際など，その扱いに注意する必要があります。

□　２　仕事に関係のないWebページは見ていない。

　悪意のあるWebページを閲覧しただけで，悪意のあるプログラムを実行される危険性があります。そのような被害に遭わないためにも，仕事上必要でないWebページの閲覧は避けるようにしましょう。

□　３　学校のコンピュータに無断でソフトウェアをインストールしていない。

　Webページでダウンロードしたり，外から持ち込んだりしたソフトウェアは，安全性の検証ができていないことがあります。どうしてもそのソフトウェアが必要な場合，ネットワークから切り離した環境で動作確認をし，管理者の許可を得てから使用するようにしましょう。

□　４　機密情報は電子メールで送っていない。

　電子メールは複数のサーバーを経由して相手先に届くため，他人が情報を入手してしまう危険性があります。また，メールは一般的に暗号化もされていません。
　機密情報を電子メールで送信することは，避けるようにしましょう。

□　５　機密情報を含む紙や記録媒体は，適切な方法で廃棄や削除をしている。

　何気なく捨てているゴミの中にも，個人情報が含まれていることがあります。機密情報を含む紙は，情報が漏えいしないようにシュレッダーなどで処分しましょう。また，記録媒体については，データを完全消去するソフトウェアなどを利用して，情報が漏えいしないようにしましょう。

□　6 コンピュータのユーザーＩＤやパスワードは，他人に知られないよう管理している。

ユーザーIDとパスワードは，その人を識別する重要な情報です。これらの情報が他人の目に付きやすいところにあると，なりすまし（他人のIDやパスワードを盗み，その人のふりをしてネットワーク上で活動すること）をされるなど，大きな問題を引き起こす危険性があります。IDとパスワードは暗記するか，自分しか分からないところに記録しておくようにしましょう。

□　7 電子メールを誤送信しないように注意している。

電子メールは，一旦送信すると取り消すことができません。宛先は手入力か，アドレス帳をクリックして選ぶ形で入力しますが，必ず送信前に正しいアドレスであることを確認するようにしましょう。
また，メーリングリストから送られてきたメールについて，単純に「返信」した場合，そのメーリングリスト加入者全員に情報が届くので注意が必要です。

□　8 離席時や帰宅時にコンピュータを不正操作されないための対策をしている。

ちょっと席を離れた間に，作業の内容を盗み見されたり，勝手にコンピュータを操作されたりすることがないよう，コンピュータにパスワードロックをかけるなどの対策を施すようにしましょう。

□　9 コピーやプリンタの出力用紙は，直ちに回収している。

離れた場所にあるプリンタに出力した書類は，ついつい取りに行くのを忘れることがあります。多数の人の目に触れる場所に，各種の情報資産をさらすことがないように心がけましょう。

□　10 帰宅時には机上を片付けている。

紛失や盗難を防ぐためにも，帰宅時には机上を片付け，機密文書については，鍵のかかるところに保管するようにしましょう。

□　11 ファイル共有ソフトは，自宅のコンピュータにもインストールしていない。

ファイル共有ソフトを通じた情報漏えいは社会問題化しており，政府等による共有ソフト自体の不使用の呼びかけがなされています。

ＵＳＢメモリ等でデータを持ち出す際について

□　12 データを持ち出す際，決められた必要な手続きを知っている。

　データを持ち出すことで，情報漏えいの危険性が高まります。しかし，仕事上どうしてもデータを持ち出さなければならないこともあります。その際に，学校でどのような手続きが必要なのか，日頃から確認しておきましょう。

□　13 ＵＳＢメモリなどを持ち出す時には，常に携行している。

　持ち出したデータは，盗難に遭ったり，紛失したりしないようにするためにも，常に携行するようにしましょう。

□　14 持ち出したデータは，パスワードが設定されているか暗号化されている。

　万一，持ち出したＵＳＢメモリ等を紛失した場合，大切なデータが簡単に漏えいしないようにするためにも，データを暗号化し，パスワードを入力しないと読み取りができない状態で保存しておきましょう。

□　15 ウイルス対策ソフトを自宅のコンピュータにもインストールしている。

　コンピュータウイルスは，インターネットや電子メール，ＵＳＢメモリ等，いろいろな経路で侵入してきます。データを持ち帰り，使用する際には自宅のコンピュータにも，必ずウイルス対策ソフトをインストールするようにしましょう。

□　16 ウイルス対策ソフトは，定期的に更新し，最新の状態にしている。

　日々，新しいコンピュータウィルスが出現しています。それに対応するためにも，ウイルス対策ソフトは定期的に更新し，新しいコンピュータウイルスの侵入を防ぐようにしましょう。

□　17 ＯＳ(Windows等)やソフトウェアは定期的に更新し，最新の状態にしている。

　コンピュータウイルスは，ＯＳやソフトウェアのプログラムのセキュリティホール（脆弱性）につけ込み，コンピュータに被害をもたらします。定期的にＯＳやソフトウェアを更新し，脆弱性に対処するようにしましょう。

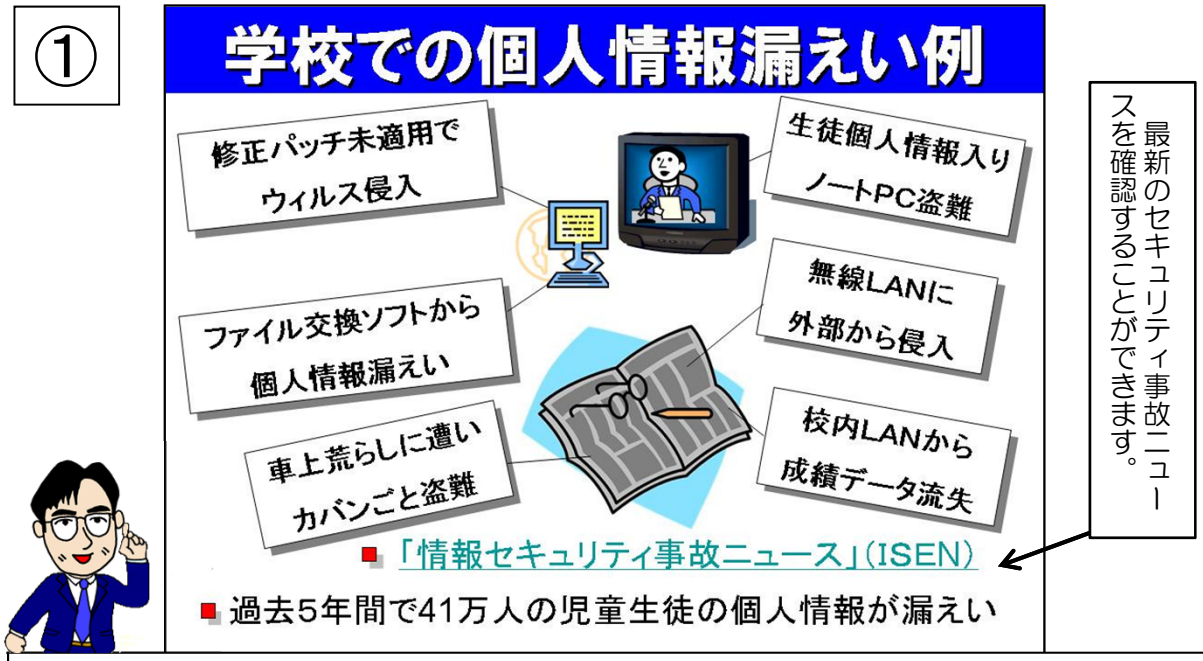
□　18 自宅で使用したデータは，自宅のコンピュータから必ず消去している。

　自宅のコンピュータにデータをコピーして作業した場合，そのファイルを必ず完全に消去して，データの漏えい・拡散を防ぐようにしましょう。

Ⅱ 校内研修・導入編 【10分】

☞研修例＝研修の導入として10分程度，情報セキュリティに関する基本的なお話をします。このスライドのダウンロード先は以下です。
http://www.edu-ctr.pref.okayama.jp/chousa/kiyou/h22/10-06pack/

①



「情報セキュリティ」に関する研修を始めます。御存じのように，新聞やテレビ，インターネットなどで児童生徒の個人情報の紛失や漏えいの報道が絶えません。「ＩＳＥＮ（教育ネットワーク情報セキュリティ推進委員会）」のWebページによると，ほぼ５日に１校の割合で全国のどこかの学校が個人情報の紛失や漏えいを起こしています。2004～2009年度の過去６年間で，41万人の児童生徒の個人情報が漏えいしています。これは倉敷市の人口とほぼ同じです。

②

個人情報とは何でしょう？

第一章　総則

（定義）
第二条　この法律において「個人情報」とは，生存する個人に関する情報であって，当該情報に含まれる 氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合 することができ，それにより特定の個人を識別することができることとなるものを含む。）をいう。

引用：「個人情報の保護に関する法律（平成一五年五月三十日法律第五十七号）」

「個人情報」とは何でしょうか？「個人情報の保護に関する法律」によると，「氏名，生年月日その他の記述等により特定の個人を識別することができるもの」とされています。携帯電話番号やメールアドレスなども，氏名やその他の情報と照合できれば，個人情報となります。このような情報も保護する必要があります。

③ 学校が管理する個人情報の例

＜氏名により管理されているもの＞

・学籍関係（指導要録，進学先資料，卒業証書関係台帳など）
・教務関係（指導要録，家庭環境調査票，成績考査に関するもの，健康診断票など）
・職員関係（職員名簿，履歴書，出勤簿，健康診断票，勤務評定など）
・　その他（同窓会名簿，児童生徒の答案，作文など）

＜時系列により管理されているもの＞

・学校日誌，保健日誌，学校医執務記録簿，教育相談日誌，職員会議録，事故等報告書

USBメモリの普及とリスク

先生方が扱う「個人情報」を具体的に見ていきましょう。まず，「氏名により管理されているもの」や「時系列により管理されているもの」があります。
近年，安価で容量が大きく，しかも手軽なＵＳＢメモリが普及してきたことで，こうしたデータを学校から持ち出し，その際に紛失や漏えいにつながるケースが多くなっています。

④ 個人情報データ紛失の報道例

20xx年〇月△日

〇〇市教育委員会は，市内〇学校の教諭が生徒の成績などを記録した私物のUSBメモリを紛失したと発表した。

市教委によると、教諭は学校側の許可を得ず，生徒の名簿やテストの点数を私物のUSBメモリに保存し，自宅に持ち帰ろうとしたが，車上荒らしに遭い，カバンごと紛失してしまった。

20xx年〇月△日
〇〇市教育委員会　記者発表資料要約

これは個人情報データ紛失を取り上げた典型的な報道例です。
こうした記事を読むと，教員は車上荒らしの被害者としてよりも，「学校側の許可を得ず」に勝手に個人情報を持ち出し，児童生徒の個人情報を漏えいさせた加害者として書かれていることが分かります。

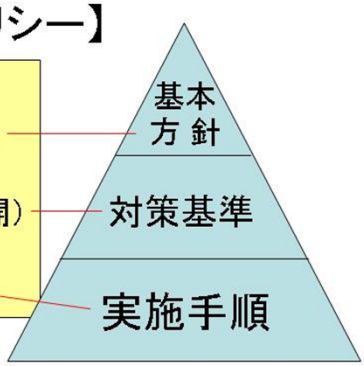
⑤

個人情報の扱いに関する指針

文部科学省（H18.4.21）
「学校における個人情報の持出し等による漏えい等の防止について（通知）」http://www.mext.go.jp/b_menu/koukai/kojin/info/001.htm

【セキュリティポリシー】

＜県立の学校の例＞
- 県情報セキュリティ基本方針（公開）
- 県情報セキュリティ対策基準（非公開）
- 各学校の実施手順（非公開）

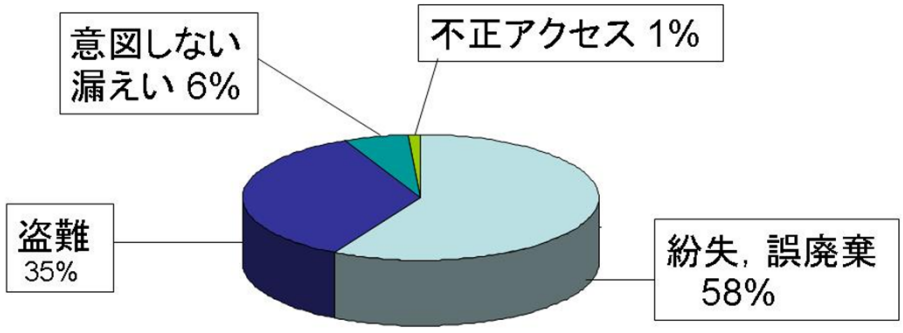


個人情報の扱いに関する指針として，文部科学省は平成18年４月に，「学校における個人情報の持出し等による漏えい等の防止について」という通知を出しています。
一般的にセキュリティに関する行動の指針となるのは，セキュリティポリシーと呼ばれるもので，県立学校では，県が策定した「基本方針」，「対策基準」に従い，この下に各学校が具体的な「実施手順」を策定します。

⑥

個人情報漏えいの要因

2009年1月～12月



情報セキュリティ事故情報まとめ（ISEN）

昨年度と一昨年度のデータが詳細にまとめられています。

こうした指針やポリシーがあるにもかかわらず，個人情報の漏えいが繰り返し起きています。教育機関における個人情報漏えいで一番多い要因は「紛失，誤廃棄」で，２番目の「盗難」と合わせ，人為的なミスが全体の９割以上を占めます。
こうしたことから，今日の研修では，情報セキュリティの知識やセキュリティリスクに対する適切な対応を身に付けていただきたいと思います。

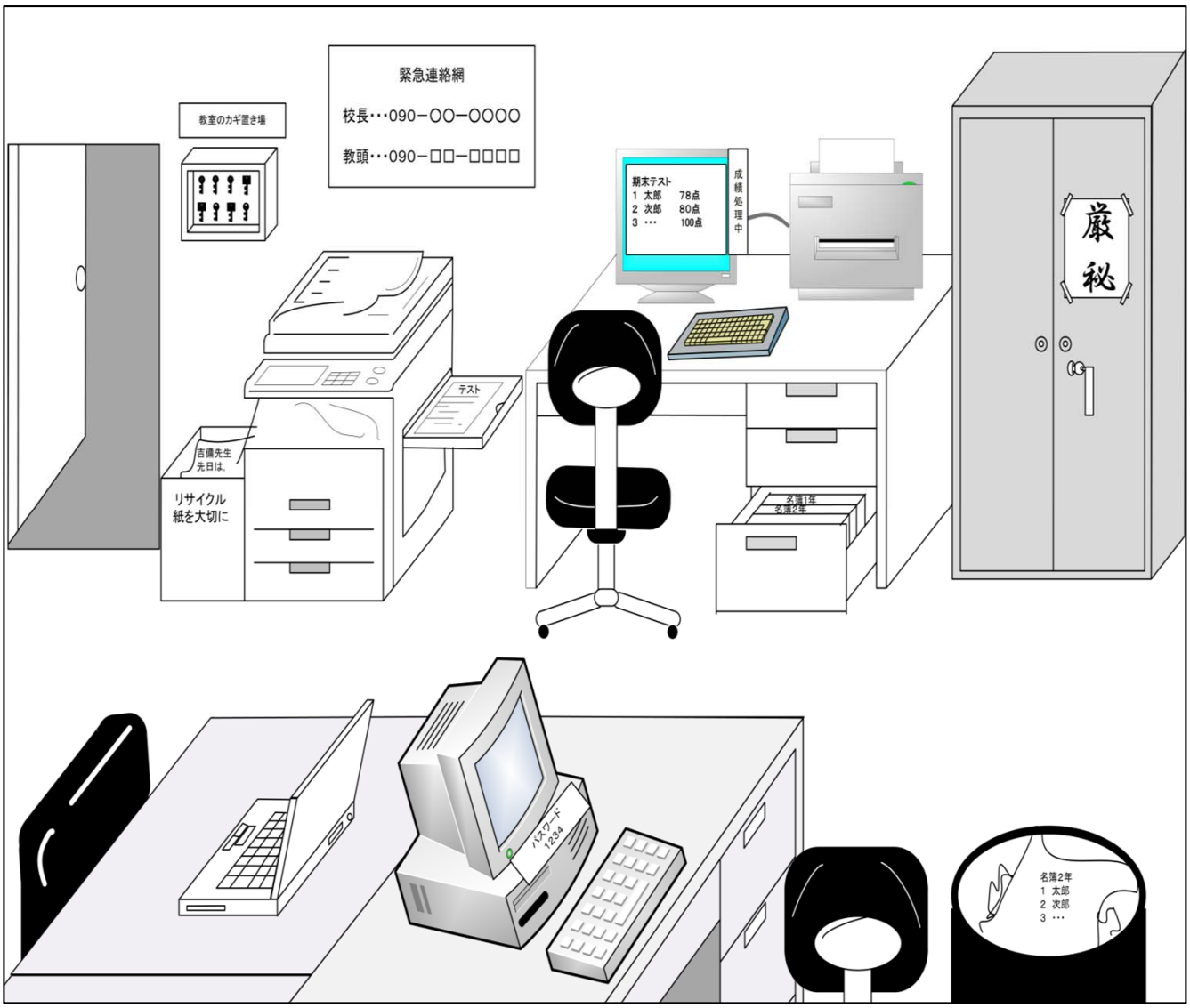
Ⅲ リスクマネジメント編 【１シート20分】

☞研修例＝各自記入５分＋グループ協議７分＋全体共有７分

ワークシート①　職員室で

授業時間帯の職員室です。情報セキュリティ上，リスク（危険箇所）はどこにあるでしょうか？

まず，各自でリスクが考えられる箇所に印を付けましょう（５分）。その後，小グループや全体で発表し，リスクに対する考えを共有しましょう。



ワークシート①の解答例と解説

職員室で

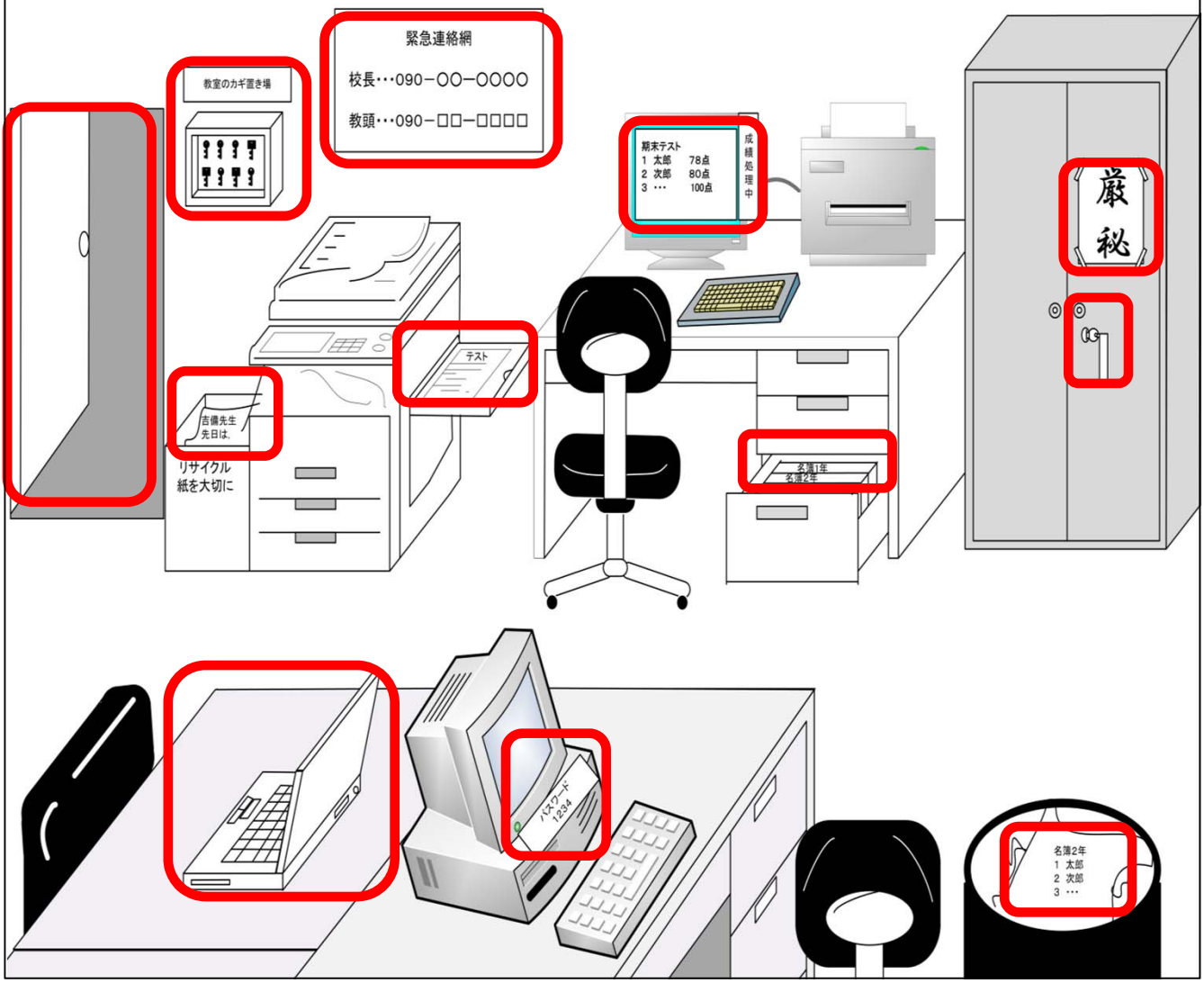
授業時間帯の職員室です。情報セキュリティ上，リスク（危険箇所）はどこにあるでしょうか？
まず，各自でリスクが考えられる箇所に印を付けましょう（５分）。その後，小グループや全体で発表し，リスクに対する考えを共有しましょう。

☑ チェックポイント

□　下の枠囲みの12箇所がチェックできた。
※　また，この他にもセキュリティリスクが潜んでいると考えた箇所があれば，書き加えてみましょう。

□　グループや全体協議で，他者とのセキュリティ意識の違いに気付いた。

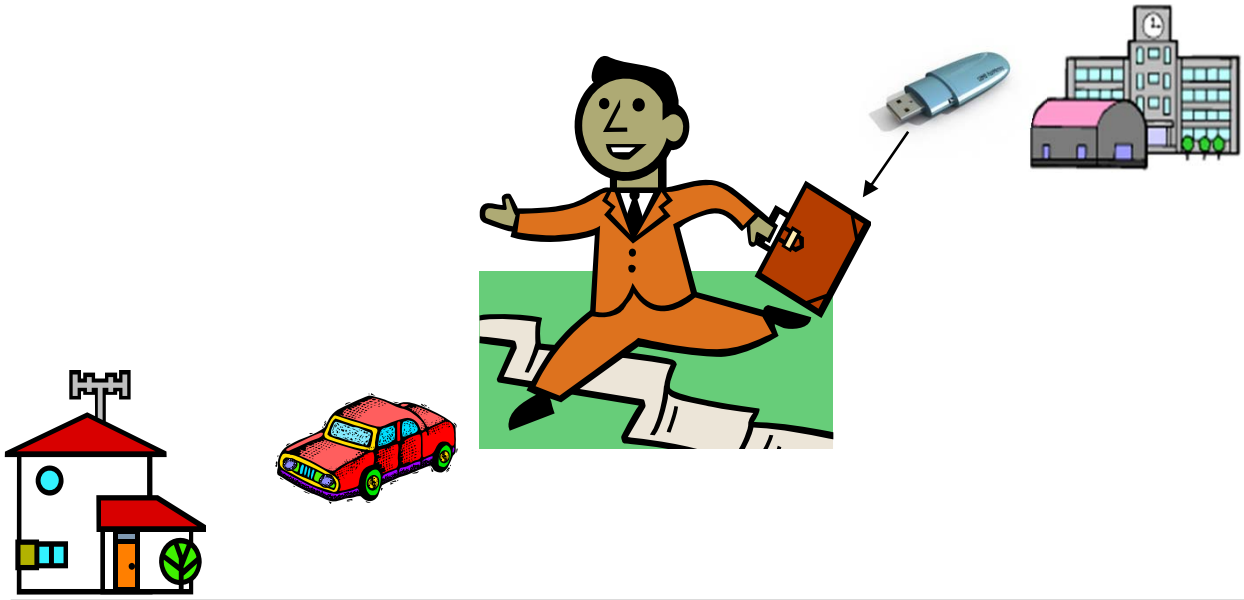
□　グループや全体協議で，セキュリティリスクに対する考えを共有できた。



ワークシート②　学校から持ち出す時

☞研修例＝各自記入5分＋グループ協議7分＋全体共有7分（1シート約20分）

Ａ先生の学校では，最も扱いに留意すべきレベルにある通知票やテスト結果等のデータは原則，学校からの持ち出しは禁止されています。ただし，やむを得ない場合，校内で定めた手続きや留意事項を守ることで許可されています。
本日，こうしたデータをやむなく持ち出すＡ先生，学校から家に持ち帰るまでの間，どんなことに気を付ければよいでしょうか？自分の学校での持ち出しに関する手順の流れや取り扱い上の留意事項等を基に，箇条書きでまとめてみましょう。



ワークシート②の解答例と解説

学校から持ち出す時

Ａ先生の学校では，最も扱いに留意すべきレベルにある通知票やテスト結果等のデータは原則，学校からの持ち出しは禁止されています。ただし，やむを得ない場合，校内で定めた手続きや留意事項を守ることで許可されています。
本日，こうしたデータをやむなく持ち出すＡ先生，学校から家に持ち帰るまでの間，どんなことに気を付ければよいでしょうか？自分の学校での持ち出しに関する手順の流れや取り扱い上の留意事項等を基に，箇条書きでまとめてみましょう。

☑ チェックポイント

次のような点を挙げているかチェックしましょう。

□　情報管理者（学校長等）の許可を得たり，持ち出し簿に記録をしたりするなどの具体的な手順やルールを守ること。

□　持ち出すデータにパスワードや暗号化など漏えい防止対策をすること。

□　自宅に直帰することが望ましいこと。どうしても途中下車が必要な場合，常にデータを携行すること。

□　学校外（自宅等）で使うコンピュータについても，校内で利用するコンピュータと同様なセキュリティが施されていること。
　例　ウィルス対策ソフトの導入，ＯＳのアップデート（最新の状態に更新）等

□　万一，情報の紛失や漏えいが起きた際にはどう対応するかなど手順の確認をすること。

☞　ＵＳＢメモリを自宅から学校に持ち帰る際も，同様な注意が必要です。

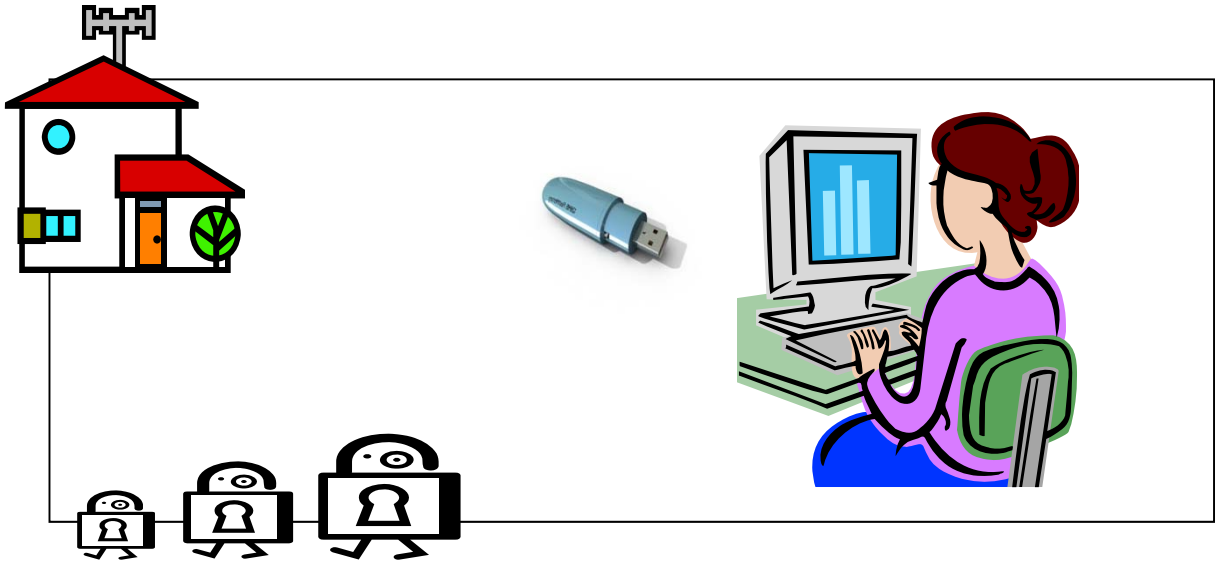
☞　個人情報を持ち出した時に，紛失や漏えいが頻繁に起きていることから，定期的に職員会議等で全体への周知を図るとともに，毎年，短時間でもセキュリティに関する校内研修を実施することが望まれます。

参考：「学校における個人情報の持出し等による漏えい等の防止について（文部科学省）」
http://www.mext.go.jp/b_menu/koukai/kojin/info/001.htm

ワークシート③ 自宅で仕事をする時

☞研修例＝各自記入5分＋グループ協議7分＋全体共有7分（1シート約20分）

　B先生はこの日，どうしても早く帰らなければいけない用事があったので，所定の届けを出して成績データの入ったＵＳＢメモリを持ち帰りました。
　B先生は家に着きました。自宅での用事が終わると，B先生は自宅のコンピュータに向かい，成績処理の作業を始めました。さて，この時，セキュリティ上，どんなことに気を付けなければならないでしょうか？



ワークシート③の解答例と解説

自宅で仕事をする時

Ｂ先生はこの日，どうしても早く帰らなければいけない用事があったので，所定の届けを出して成績データの入ったＵＳＢメモリを持ち帰りました。
Ｂ先生は家に着きました。自宅での用事が終わると，Ｂ先生は自宅のコンピュータに向かい，成績処理の作業を始めました。さて，この時，セキュリティ上，どんなことに気を付けなければならないでしょうか？

☑ チェックポイント

次のような点を挙げているかチェックしましょう。

□　自宅のＰＣにもウィルス対策ソフトがインストールされていること。

□　自宅のＰＣでもＯＳやソフトウェアがアップデート（最新の状態に更新）されていること。

□　自宅のＰＣにも，ファイル交換ソフトはインストールしていないこと。
※　家族で共有しているコンピュータの場合，家族の誰かがファイル交換ソフトをインストールしたり，使用したりしていないか確認しましょう。本人が知らないうちに，ファイル交換ソフトを経由して情報漏えいしたケースがあります。

□　自宅からデータを電子メールやＦＡＸでデータ送信することについては十分，留意すること。
※　電子メールやＦＡＸ等で送信してよいデータかどうかの検討，判断が必要です。
※　もし利用する場合，送り先を間違えて，全く知らない他人に情報が漏えいしてしまわないよう，送り先を十分確認しましょう。

□　自宅でも，重要なファイルを開いたまま，席を離れないこと。

□　自宅のＰＣにファイルをコピーした場合，必ずファイルを完全削除すること。

□　自宅のプリンタで印刷した場合，用紙の管理やシュレッダー等の処分をすること。

□　持ち出したＵＳＢメモリ等を返却する際，データを完全消去すること。

□　自宅での保管場所も，鍵がかかる場所など，データの管理に留意すること。
※ 情報セキュリティ事故ニュース（ISEN　http://school-security.jp/leak/）によると，平成22年4月から9月末までの6か月間に，学校の個人情報の紛失や漏えいが47件報告されていますが，そのうち自宅での紛失，盗難が５件となっています。

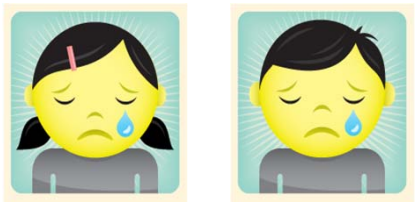
参考：「漏れたら大変！個人情報」（独立行政法人　情報処理推進機構セキュリティセンター）
http://www.ipa.go.jp/security/kojinjoho/user.html

Ⅳ クライシスマネジメント編

☞研修例＝各自記入５分＋グループ協議７分＋全体共有７分（１シート約20分）

ワークシート④ USBメモリの紛失

〇月△日，Ｃ先生は所定の手続きに従ってテストの得点データが入ったＵＳＢメモリをカバンに入れ，校外に持ち出しました。しかし，途中，買い物に立ち寄った際，車内にカバンを放置し，買い物の後，カバンごと紛失していることに気付きました。
この後，Ｃ先生は具体的にどうすればよいのでしょう？また，その後，学校はどのように動き，対応すればよいのでしょうか？



【まずＣ先生がとるべき行動として考えられること】

【次に学校が動き，対応すべき内容として考えられること】

ワークシート④の解答例と解説

USBメモリの紛失

○月△日，C先生は所定の手続きに従ってテストの得点データが入ったＵＳＢメモリをカバンに入れ，校外に持ち出しました。しかし，途中，買い物に立ち寄った際，車内にカバンを放置し，買い物の後，カバンごと紛失していることに気付きました。
この後，C先生は具体的にどうすればよいのでしょう？また，その後，学校はどのように動き，対応すればよいのでしょうか？

☑ チェックポイント

次のような点を挙げているかチェックしましょう。

【まずC先生がとるべき行動として考えられること】

□ 学校長等の情報管理者に紛失した情報と暗号化，パスワードの有無等を報告すること。

□ 紛失場所（鉄道やバス会社，店舗等の窓口等）に早急に届け出ること。

□ 警察に届け出ること。
※ カバンの中身やＵＳＢメモリの形態（メーカー，色，形），もし分かればＵＳＢメモリの製造番号等も伝えましょう。

【次に学校が動き，対応すべき内容として考えられること】

□ 校内に対策委員会を設けて内部での検討，外部との窓口を一本化すること。

□ 管轄の教育委員会に届け出て助言を受け，連携しながら対応を図ること。

□ 予想される二次被害への対応をすること。
例 IDやパスワードが含まれていれば，関係するシステムへのアクセスを制御する。

□ 個人情報が含まれ漏えいの恐れがある場合，本人や保護者への通知と謝罪を行うこと。規模や影響が大きい場合，緊急の生徒集会や保護者会で，経緯説明と謝罪を行うこと。

□ 再発防止のために，実施手順の見直しと遵守を行うこと。

□ 報告について対策委員会等で内部評価し，隠ぺい工作が起こらないよう配慮すること。

☞ 情報漏えい後の対応５原則は次のとおりです。
１ 被害拡大防止・二次被害防止・再発防止の原則
２ 事実確認と情報の一元管理の原則
３ 透明性・開示の原則（組織の透明性を確保し情報を開示する姿勢）
４ チームワークの原則（経営，広報，技術，法律など様々な要素を考慮し組織対応）
５ 備えあれば憂いなしの原則

☞ 日頃から危機管理に向けた体制やチームづくりをしましょう。万一の際に，統一した見解や素早い対応が取れない場合，更なる信用失墜につながります。

参考：「情報漏えい発生時の対応ポイント集」（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/kojinjoho/user.html

研修の振り返り　【５～10分】

☞研修例＝各自記入５分程度。研修時間があればグループや全体での発表を

◇　今回の情報セキュリティ研修を振り返って，次の１～３の各問いにお答えください。

１　共感できたこと，気を付けたいと思ったことはどんなことですか。

２　疑問に思ったことがあれば，記入してください。

３　情報セキュリティについて，更に知りたいことがあれば，記入してください。

◇　今回の研修について，４～７は該当する選択肢に〇を付け，８には研修の感想を自由に書いてください。

＜選択肢＞　a：そう思う　b：おおむねそう思う　c：余りそう思わない　d：そう思わない

４　研修テーマについて事前の関心は高い方でしたか。　a　b　c　d

５　今日の研修の内容は適当でしたか。　a　b　c　d

６　今日の研修の方法は適切でしたか。　a　b　c　d

７　今日の研修の成果は生かせますか。　a　b　c　d

８

Ⅵ 情報セキュリティ 参考Webページ

◆ 文部科学省Webページ

□ 学校における個人情報の持出し等による漏えい等の防止について（通知）
http://www.mext.go.jp/b_menu/koukai/kojin/info/001.htm

□ 情報の漏えい等の防止についての関連情報
http://www.mext.go.jp/b_menu/koukai/kojin/info.htm

◆ ＩＰＡ（独立行政法人 情報処理推進機構セキュリティセンター）

□ 情報セキュリティ緊急対策情報 http://www.ipa.go.jp/security/

□ ５分でできる情報セキュリティポイント学習
～事例で学ぶ中小企業のためのセキュリティ対策～
http://www.ipa.go.jp/security/vuln/5mins_point/

◆ ＩＳＥＮ（教育ネットワーク情報セキュリティ推進委員会）

□ 学校情報セキュリティお役立ちWeb 今日もワンステップ！
http://www.school-security.jp/

◆ CEC（財団法人 コンピュータ教育開発センター）

□ 学校情報セキュリティライブラリー
□ 学校情報セキュリティ・ハンドブック改訂版（平成18年度）
http://www.cec.or.jp/seculib/index.html

◆ 岡山県Webページ

□ 岡山県セキュリティポリシー
http://www.pref.okayama.jp/soshiki/detail.html?lif_id=1071

お　わ　り　に

本パッケージは，学校における日常の具体的な場面を幾つか取り上げることで，実感を持ちながら，情報セキュリティの意識を高めていくことをねらいとしています。また，研修の中で発表や協議を通して共有したことは，各学校が実施手順を検討，作成する上でも役立つものと考えています。

なお，各学校での実施手順作成の具体的な方法については，CEC（財団法人コンピュータ教育開発センター）のWebページ（http://www.cec.or.jp/seculib/）を御参照ください。

最後に，情報セキュリティに関する基本的な考え方をまとめました。

- セキュリティに完璧はない。
- セキュリティと利便性はトレードオフである。
- セキュリティの常識は変化する。
- セキュリティの基本は「人」である。
- 鎖の強さは最も弱い環で決まる。

The strength of the chain is in the weakest link.

こうしたことからも，毎年，教職員が入れ替わる学校においては，定期的に情報セキュリティに関する研修を行い，共通理解を図ることが強く望まれます。

「教職員の情報セキュリティ意識を高める校内研修パッケージ」の活用
研究協力委員会

研究協力委員
佐藤　裕之　　高梁市立高梁小学校主幹教諭
赤木陽一郎　　高梁市立高梁中学校教諭

山内　隆彦　　岡山県総合教育センター情報教育部長
小林　朝雄　　岡山県総合教育センター情報教育部指導主事
西村　能昌　　岡山県総合教育センター情報教育部指導主事

平成23年２月発行
編集兼発行所　岡山県総合教育センター

〒716-1241 岡山県加賀郡吉備中央町吉川7545-11
TEL　（0866）56-9101　FAX　（0866）56-9107
URL　http://www.edu-ctr.pref.okayama.jp/
E-MAIL　kyoikuse@pref.okayama.lg.jp

お問い合わせ　情報教育部　TEL　（0866）56-9127