学校情報セキュリティワークショップ

徳島県立総合教育センター
指導主事　大平　和哉
千葉県柏市立土南部小学校
教諭　西田　光昭

ー前提の確認ー
なぜ，学校情報セキュリティか

先生方を縛るためでなく

先生方が安心して
「校務の情報化」「授業の情報化」を
進めることができるように

学校改善，授業改善のため

先生方，子どもたちを守るため

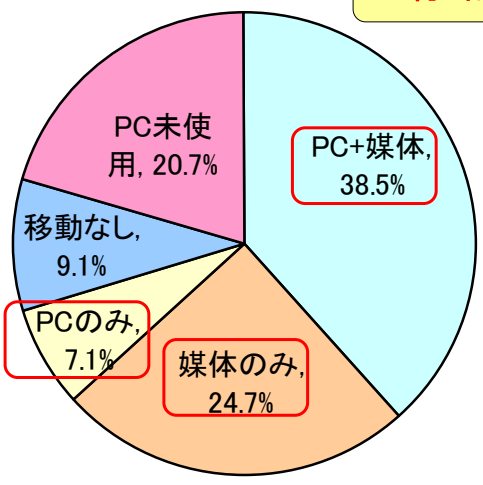
学校の情報セキュリティの現状（インスタント実態調査）

あなたの学校・地域の現状は？

- 情報セキュリティポリシー，実施手順を策定済み？
- 個人所有パソコンを自由に校内LANに接続？
- 記憶媒体や個人所有パソコンに，個人情報を記録し，学校・自宅・出張先間を持ち歩いている？
- パスワード設定・暗号化の状況は？
- コンピュータに詳しくない教員まで徹底している？

小・中・高教員の記憶媒体や個人所有パソコンの学校・自宅間での持ち歩き（札幌市）

約7割が持ち歩き

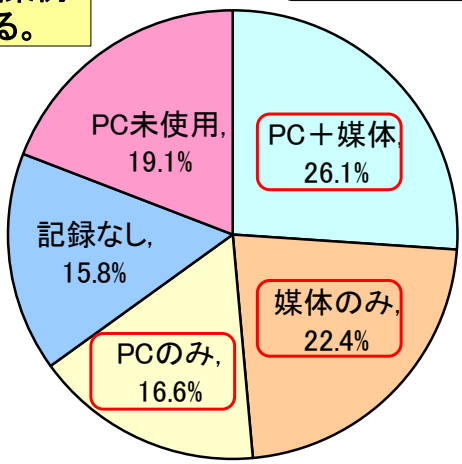


N=10,296
2005年8月

記憶媒体や個人所有パソコンに児童生徒や保護者等の個人情報が記録されているか（札幌市）

公立学校は，個人情報保護条例が適用される。

約6割が個人情報を電子化



学校における情報セキュリティの脅威

車上ねらいに，成績などの個人情報の入ったパソコンを盗まれた！

名簿などの情報が入ったUSBメモリを，なくしてしまった！

通知票のデータや住所録などをファイル共有ソフト(Winnyなど)で，インターネット上に流出させ，回収不能になった！

ウイルスに感染した個人所有パソコンを，校内ＬＡＮに接続し，市のネットワーク全体を止めてしまった！

子どもにダイレクトメールが大量に届いた！

情報セキュリティ確保のための対策が必要

学校における3つの課題

1．現場の教職員（管理職＋一般教職員）が，情報リスクを十分に自覚・認識していない。
→セキュリティポリシーがあっても，一般教職員にとって，存在していないのと同じ状況。参与の欠如による当事者意識の欠落
→学校の特殊性（指揮系統の曖昧さ，インセンティブ，サンクションなし）

2．学校における情報資産，情報リスクと脅威の分析が不十分
→具体的特定が不十分。しかも，情報資産の「オーナー」（所有者）と「オリジネータ」（入力者・作成者）が厳密に区別されていない。

3．小規模校では，実効性のあるセキュリティ対策が困難
→人的資源，学校向けテキスト等の各種支援が不足していること，ネットワーク管理・資金的裏付けの関係，教育委員会の関与
→最も重要な「実施手順書」（マニュアル）が作成がされず

実効性のある学校に特化したセキュリティポリシー・実施手順書等策定のための支援（問題意識の共有，分析，具体化など）

情報セキュリティポリシーとは

■ 組織の情報セキュリティに関する方針を示した文書

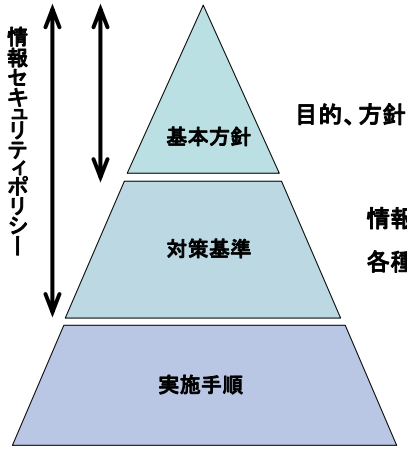
■ 情報セキュリティマネジメントを実践するための様々な取り組みを、包括的に規定する。

◎ 学校にとって守るべき情報は何か
◎ その情報のセキュリティ上の脅威やリスクを、どう管理すべきか

■ 組織全体の情報セキュリティポリシーは、情報セキュリティマネジメントの全ての活動に先立って策定する。

出展： 独立行政法人 情報処理推進機構 資料を編集

情報セキュリティポリシーの文書体系



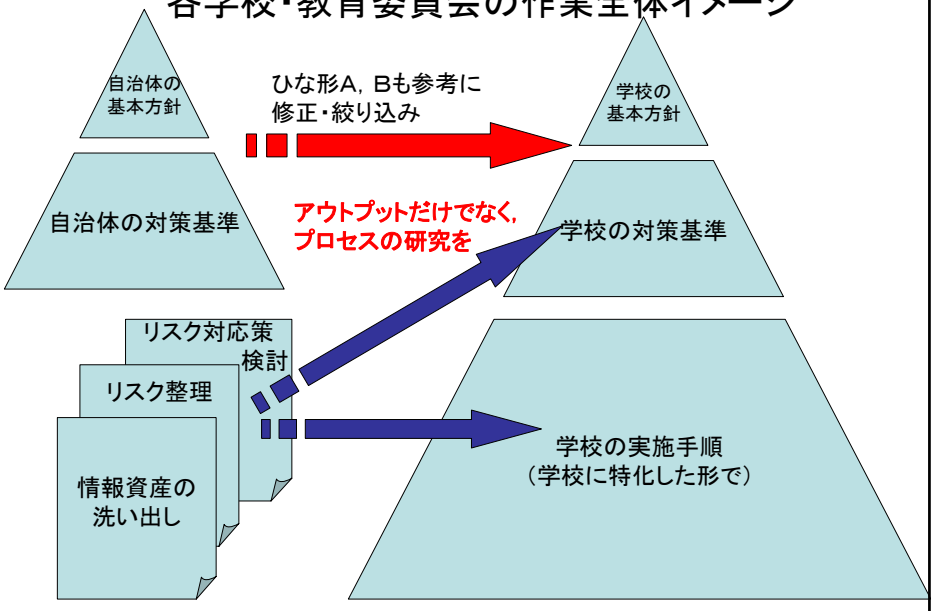
目的、方針、運用範囲、体制など、基本的事項

情報セキュリティ対策基準
各種ガイドライン

情報システム実施手順書
各種規程書
各種申請・届出用紙など

出展： 独立行政法人 情報処理推進機構　資料より

各学校・教育委員会の作業全体イメージ



各自の責任を自覚と学校情報セキュリティポリシーの策定

教職員は，被害者ではなく加害者になる
可能性が大きいことを自覚して

便利さは，危険と表裏一体
絶妙なバランス感覚が重要

甘くなりがちな現状を厳に戒めつつ，
業務に支障をきたさないための
「安全確保策」と「責任の所在の明確化」を

学校情報セキュリティポリシーの策定を！

学校に特化し，実効性を確保するための支援として『学校情報セキュリティハンドブック』を開発

JIS X5080 2002準拠

ワークショップの時間

- 開　始　14:40
  - 講義　20
- 自己紹介　15:00
- トラブル事例　15:10
  - グループ内でフリー
- 学校の情報資産　15:20
  - 個別に　5
  - 共同で　10
  - 発表　10
- 脅威　2つ　15:45
  - 個別に　10
  - 共同で　10
  - 発表　10

16:15(休憩)

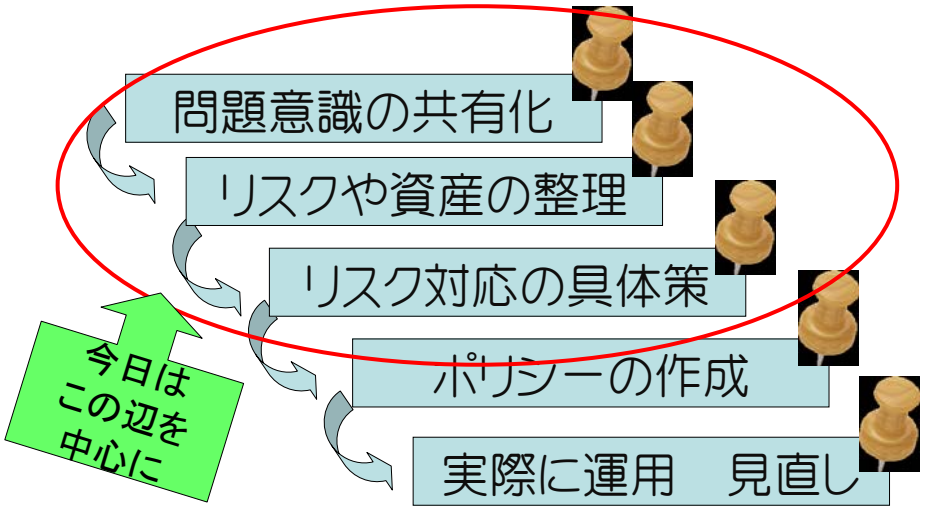
- 脅威のマッピング　16:30
  - 共同で　10
- リスクリストの作成　16:40
  - 共同で　10
  - 発表　10
- リスク対応策の作成 17:00
  - 共同で　10
  - 発表　10
- まとめ　17:20
- 終　了　17:40

自己紹介　グループ内で

・所属　名前　など　・学校の環境等

・特に成績関係の扱い方　※リーダー（発表者）の決定

5つのステップ



多くのトラブル事例

問題意識の共有化

- 校内での紛失・盗難
- 校外での紛失・盗難
- ウィルスの影響
- 部外者による漏洩

懲戒処分の指針

千葉県

問題意識の共有化

- **個人情報の紛失、盗難**
  - 児童、生徒等に係る重要な個人情報を、重大な過失により、紛失し又は盗難に遭った職員は、**減給又は戒告**とする。
- **コンピュータの不適正使用**
  - 職場のコンピュータをその職務に関連しない不適正な目的で使用し、公務の運営に支障を生じさせた職員は、**減給又は戒告**とする
- **指導監督不適正**
  - 部下職員が懲戒処分を受ける等した場合で、管理監督者としての指導監督に適正を欠いていた職員は、**減給又は戒告**とする。
- **非行の隠ぺい、黙認**
  - 部下職員の非違行為を知得したにもかかわらず、その事実を隠ぺいし、又は黙認した職員は、**停職又は減給**とする。

http://www.pref.chiba.jp/kyouiku/kyousou/tyoukaisisin/sisin.html

具体的なトラブル事例（1）

校内での盗難・紛失

高等学校	2005年3月	学校内の金庫で書類とともに管理されていたフロッピーディスクが紛失した。出し入れをした間に紛失した可能性が高いという。フロッピーディスクには受験生97人分の氏名や生年月日，在籍校，成績など個人情報が含まれていた。
高等学校	2005年4月	生徒指導室の机の上に置かれていた在校生197人分の数学の成績や卒業生40人分の各教科の成績などが保存されていたパソコンが盗まれた。
中学校	2005年5月	男性教諭が職員室のパソコンに全校生徒の氏名・住所・電話番号・英語の成績などの個人情報が入った携帯型記録媒体（USBメモリ）を接続して作業後，そのまま帰宅。翌日出勤した際，紛失に気付いた。
小学校	2005年10月	女性教諭が退勤する際，児童の個人情報が保存されていたノートパソコンを鞄ごと置き忘れた。翌朝，置き忘れに気付き，前日鞄を置き忘れたと思われる場所を捜索したが発見できなかった。

具体的なトラブル事例（2）

校外での盗難・紛失

小学校	2004年12月	女性教諭が原付バイクで帰宅途中，前かごに入れておいた手提げかばんを背後から原付バイクできた男にひったくられた。かばんの中には担任クラスの全生徒の指導要録と調査書などが入っていた。
高等学校	2004年12月	男性教諭が帰宅途中に飲酒し電車内で眠り，約2時間後に起きたときには，生徒の答案用紙と成績などを記録したMOディスク1枚が入ったかばんが紛失していた。
中学校	2005年6月	女性教諭が帰宅途中，子供を迎えに寄った保育所に駐車したところ，自家用車の窓ガラスが割られ，車内に置いてあったノートパソコンをバッグごと盗まれた。そのパソコンには生徒の成績や保護者の名簿などの個人情報が保存されていた。
養護学校	2005年9月	女性教諭が帰宅途中，薬店に駐車したところ，自家用車の窓ガラスが割られ，生徒3人分の指導内容が記録された記憶媒体（フラッシュメモリ）と教職員17人分及び生徒79人分の緊急連絡先が記載された書類が入ったバックを盗まれた。
教育委員会	2005年9月	教職員課主幹の男性職員が，次年度採用の教員試験の受験者1606人や，県教委が指導力不足と認定した教員175人の氏名など，延べ3202人分の個人情報を記録したパソコンの記録媒体(フラッシュメモリ)1個を持ち出し，紛失した。

具体的なトラブル事例（3）

ウイルス関連、他

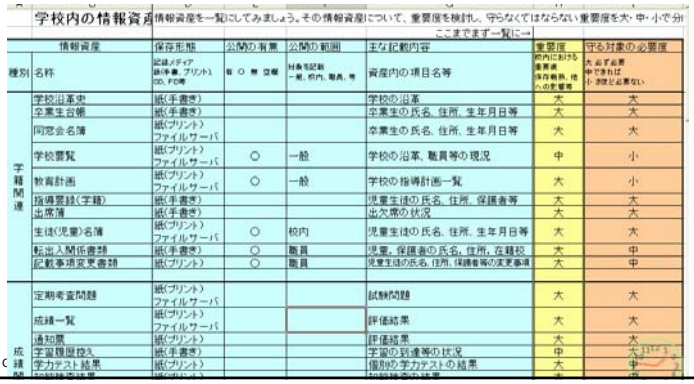
小学校	2005年6月	校務主任の教諭が全校児童535人分と教職員約30人分の個人情報を記録したメモリを自宅に持ち帰り，家族所有のパソコンにコピーしたところ，ウイルスに感染し，ファイル交換ソフトWinnyを通じて名簿がインターネット上に流出した。
小学校	2006年1月	男性教諭の私物パソコンから担任児童36人分の成績情報がインターネット上に流出した。ファイル交換ソフトWinnyによるウイルス感染が原因とみられる。
中学校	2005年4月	子供が通う中学校の指導方針に反感を持ったカメラマンの男性が，中学校から個人情報が入ったパソコンを盗み，インターネット上の掲示板に同校の中傷やパソコンから取り出した教員の個人情報を公開し，嫌がらせをした。
教育委員会	2005年4月	公立小中学校の一部児童の情報が流出したことが，個人情報の買い取りを求める脅迫めいた電話により発覚した。流出したとみられる個人情報は，廃棄業者によって廃棄されたパソコンに保存されていたもので，生徒や保護者の氏名，住所，電話番号，成績など約6000名の個人情報が含まれていたという。

学校の情報資産

リスクや資産の整理

- **児童・生徒・保護者の個人情報**
- **学校を運営するために欠かせない情報**

成績関連



学校内の情報資産一覧にしてみましょう。その情報資産について、重要度を検討し、守らなくてはならない重要度を大・中・小で分

種別	名称	保存形態	公開の有無	公開の範囲	主な記載内容	重要度	守る対象の必要度
学籍関連	学校沿革史	紙(手書き)			学校の沿革	大	大
	卒業生台帳	紙(手書き)			卒業生の氏名、住所、生年月日等	大	大
	同窓会名簿	紙(プリント) ファイルサーバ			卒業生の氏名、住所、生年月日等	大	大
	学校要覧	紙(プリント) ファイルサーバ	○	一般	学校の沿革、職員等の現況	中	小
	教育計画	紙(プリント) ファイルサーバ	○	一般	学校の指導計画一覧	大	小
	指導要録(学籍)	紙(手書き)			児童生徒の氏名、住所、保護者等	大	大
	出席簿	紙(手書き)			出欠席の状況	大	大
	生徒(児童)名簿	紙(プリント) ファイルサーバ	○	校内	児童生徒の氏名、住所、生年月日等	大	大
	転出入関係書類	紙(手書き)	○	職員	児童、保護者の氏名、住所、在籍校	大	中
	記載事項変更書類	紙(プリント)	○	職員	児童生徒の氏名、住所、保護者等の変更事項	大	中
成績関連	定期考査問題	紙(プリント) ファイルサーバ			試験問題	大	大
	成績一覧	紙(プリント) ファイルサーバ			評価結果	大	大
	通知票	紙(プリント)			評価結果	大	大
	学習理解控え	紙(手書き)			学習の到達等の状況	中	大
	学力テスト結果	紙(プリント)			個別の学力テストの結果	大	中

学校における脅威

リスクや資産の整理

- 1つの資産について
- 学校に想定される脅威をリストアップする。
- 脅威の評価をする。
  （大：非常に危ない　中：危険はある　小：ほとんどない）
- 評価判断の根拠を明らかにしておく

特色の異なるもの

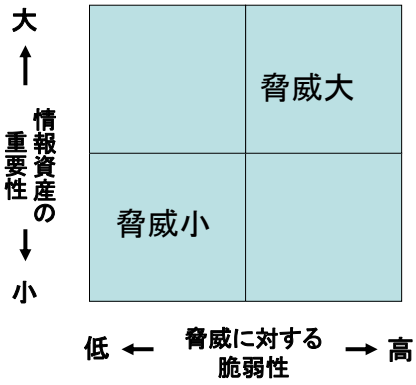
学校内の脅威の評価（情報資産名：

情報セキュリティ脅威名	脅威の評価	脅威の評価判断の根拠

脅威の評価

脅威評価法（例1）

情報資産の重要性と、脅威に対する脆弱性から評価する方法



脅威:

情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因

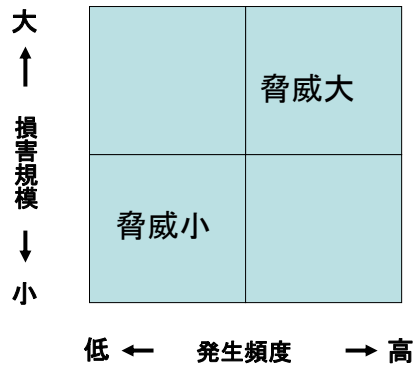
脆弱性:

脅威に対してどのくらい弱いかということ

脅威の評価

脅威評価法（例2）

発生した場合の損害規模と、予想される発生頻度から評価する方法



何を　何から　守るか

リスクや資産の整理

1. 1つの資産について
2. 資産の重要度・驚異の大きさを元にマッピングする。(大　中　小)
3. 対応すべきリスクをしぼりこむ。

リスク対応評価表（情報資産名：　　）

重要度は変わらない	情報資産の重要度	脅威の大きさ 小	中	大
	大			リスク大
	中			
	小	リスク小		

リスクを一覧にする

リスクや資産の整理

- 資産に対する脅威から
- リスクをまとめる

学校内の情報セキュリティ・リスクリスト(成績関連)

守るべき情報資産 / 情報セキュリティ脅威名	資産名		
個人所有パソコンの盗難，紛失による漏洩			
学校内パソコンのウィルスやスパイウェアによる漏洩			
無線LANを利用したアクセスによる情報の漏洩			

どのように守るか

リスク対応の具体策

1. リスクへの対応策を、リストアップする。
2. 対応策を選び、決定する。
3. 理由をはっきりとさせる

成績関連

	リスク対応策	想定されるリスクへの対応策をあげ、実際に採用する対応策を決定します。	
	リスク名	考えられる対応策	採用する対応策
個人情報保護	個人所有パソコンの盗難，紛失による漏洩	個人PCの持ち込み禁止 罰則規定を設ける	個人PCの持ち込み禁止
	USBメモリ等のメディアの盗難，紛失での漏洩	暗号化の義務づけ 認証式のメディアの導入 持ち出し禁止の規定	暗号化の義務づけ 認証式メディアを利用
	学校Webページへの個人情報掲載による漏洩	学校WebへのFTPアカウントの管理 公開のチェック	FTPアカウントの管理
	メールご送信による漏洩	フリーメールの利用制限 研修による扱いの徹底 添付のできないメールツールの採用	フリーメールの利用制限
	情報機器処分時のデータ消し忘れによる漏洩	廃棄時の扱いマニュアル作成 廃棄時のデータチェック	廃棄時の扱い手順を規定
	個人認証におけるなりすましによる漏洩	アカウントの管理についての研修 生体認証の導入	アカウントの管理義務を明確にする

リスク対応

4種類のリスク対応

大 ↑ 損害規模 ↓ 小	低 ← 発生頻度 → 高	
	リスクの移転	リスクの回避
	リスクの保有	リスクの低減

リスクの低減

脅威を小さくする、または脆弱性を小さくするなどの方法により、リスク小さくすること。

例えば、パスワードを定期的に変更することを徹底すれば、パスワードが盗まれるリスクは小さくなる。

リスクの回避

脅威そのものを取り除くことにより、リスクの発生可能性をなくしてしまうこと。

例えば、ノートパソコンの持ち出しを禁止すれば、紛失のリスクはなくなる。

リスクの移転

自社の抱えるリスクを他者に移し替えること。

例えば、業務を委託する、保険に加入するなど。

リスクの保有

リスクの存在を認識しながらも、特段の対応を取らないこと。

小さなリスクまですべてに対応することは現実的でなく、リスクを保有することもリスク対策のひとつである。

出展： 個人情報保護士試験完全対策（あさ出版） を参照

情報セキュリティ向上策

リスク対応の具体策

- パスワード設定
  - 学校のパソコン
  - 個人のパソコン
- ファイルにパスワード設定
- ファイルやフォルダの暗号化
- ウィルス対策ソフトの利用とアップデート
- OSのアップデート

ハンドブック　P18-19

暗号化による保護

リスク対応の具体策

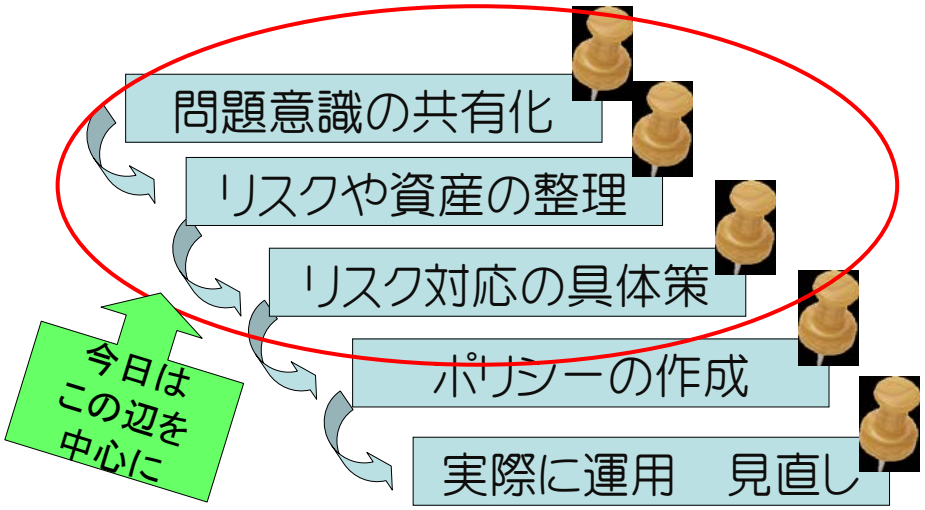
何もなし

パスワード

パスワード
＋
暗号化

同じようなUSBメモリでも

5つのステップ

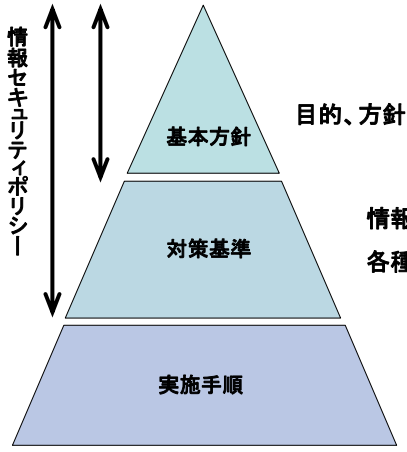


文章にする

ポリシーの作成

- 何について、どのように守るか
- しなくてはいけないことは何か
- してはいけないことは何か
- 例外はあるのか

情報セキュリティポリシーの文書体系



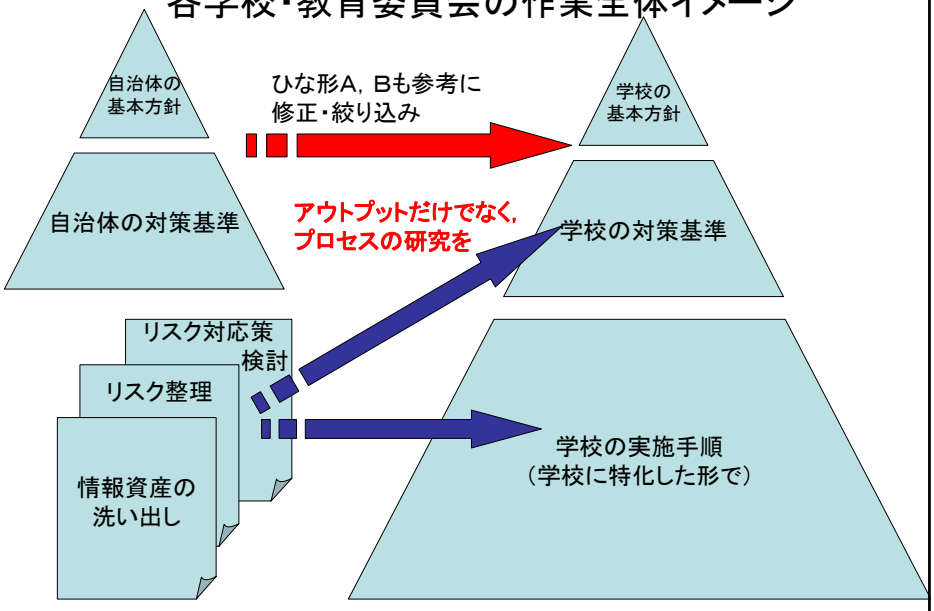
目的、方針、運用範囲、体制など、基本的事項

情報セキュリティ対策基準
各種ガイドライン

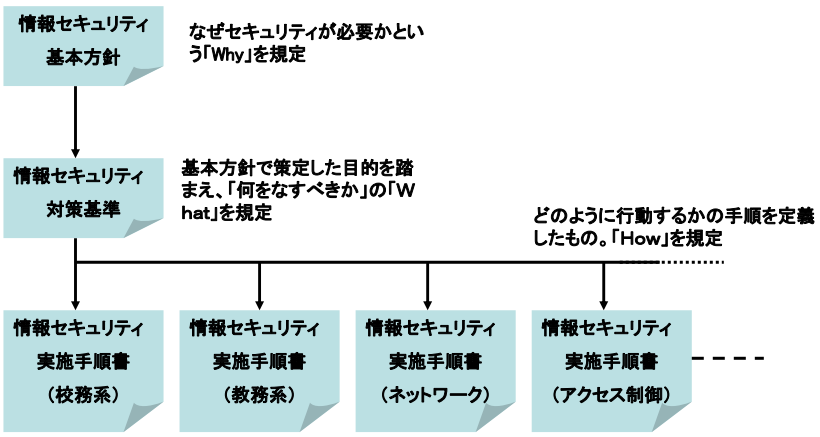
情報システム実施手順書
各種規程書
各種申請・届出用紙など

出展： 独立行政法人 情報処理推進機構　資料より

各学校・教育委員会の作業全体イメージ



情報セキュリティポリシーの構成例



出展：　独立行政法人 情報処理推進機構　資料　を編集

作るだけではダメ

実際に運用　見直し

- 運用しながら見直し
  - 初回は早めに　　数ヶ月
- 教職員が理解できるように
  - 研修
  - 実施手順書
    - » マニュアル
    - » ガイドブック

学校の情報セキュリティポリシーに従う

The strength of the chain is in the weakest link.
鎖の強さは，最も弱い環で決まる。

ポリシーに反する人が一人でもいると・・・！
【×0（かけるゼロ）の恐怖】

参考：IPA情報セキュリティの基礎

今後の展開

①各地の優れた事例の収集と共有

②『学校情報セキュリティハンドブック』
の改善
（帳票や手順の改善を含む）