

# 学校現場の情報セキュリティ

## ～問題の本質を考える～



2016年7月1日  
公立大学法人会津大学  
特任教授  
山崎 文明  
fumiaki@u-aizu.ac.jp

## 加害者としての学校サイト

- メールアドレスや個人情報の漏えい
  - ✓ 本人がIDとパスワードを自由に設定できる本人登録型サイト
  - ✓ 安易なパスワード設定のため容易にクラッキングできるサイト
  - ✓ パスワードの強度に関する検査と変更勧告を行う必要がある
- 迷惑メール(Spam)/偽装メール(phishing)の発信基地
- ウイルスの拡散元
- サイバーテロへの負担
  - ✓ ホームページのテロ組織による利用
  - ✓ DDOS攻撃の発信元として利用される可能性
- ハッカー(クラッカー)の不正アクセスツールの格納庫
- 不正アクセスの身元隠蔽(踏み台)に利用される



ネットワーク社会の構成員としての社会的責任

# 学校ネットワークの実態

## n 軽視されがちな課題 見えないセキュリティの景色

- ✓ 実感されない被害
- ✓ 実感されない加害者責任意識

## n サーバーモンキーの実態

- ✓ 自分の仕事じゃないけど誰もやらない、誰も出来ないから俺がやる
- ✓ 俺はプロじゃないし、あくまでボランティアです
- ✓ そんな自分にまさか責任取れと言わないでしょ
- ✓ なんとか現状維持してるけど、評価は「好きでやってるだけでしょ」

## n 保護者のお力借りてます

- ✓ ドキュメントがないので引き継ぎは出来ません
- ✓ この線どこに繋がってるの

## n お金がないので

- ✓ ファイアーウォールも買えません



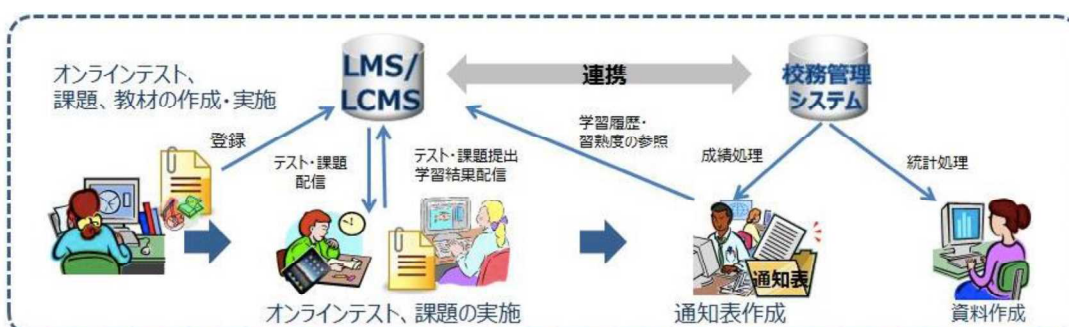
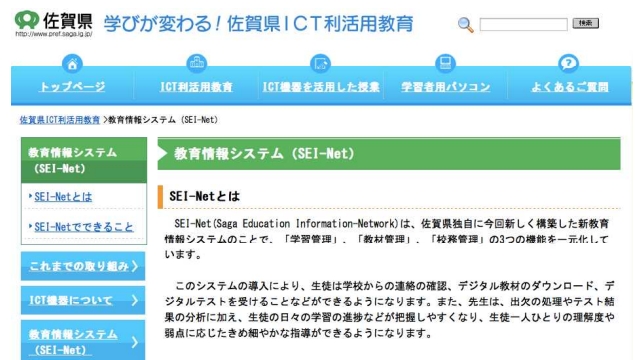
# 既に起こっている事件

## n セキュリティ事故・事件の経験が生かされない学校システム

- ✓ 十分認識されていないドメイン分割に必要性
- ✓ 放置されている脆弱性
- ✓ 売買・公開されているID、パスワード

## ■ これから発現する脅威

- ✓ ランサムウイルス感染



## 既に起こっている事件

### ■ 工業高校の個人情報流出問題で校長ら7人を訓告

卒業生304人の進路指導部内のパソコンに保存されていた氏名や成績、進路先、他校の卒業生3人の調査書の内容がインターネット上に流出した。

パソコンには教職員が使うパソコンとLANで接続されていたほか、生徒が使う教育用パソコンともLANで結ばれていた。そのため、生徒も自由に見ることができた。流出したデータは、自習中の男子生徒が自分のホームページに転送した情報だった。情報管理の責任者である校長と進路指導部の情報管理の責任者である男性教諭を文書による訓告。2人の教頭や総括事務長など5人の教職員を文書や口頭による訓告の処分とした。また、情報を転送した男子生徒に対しては、校長による指導が行われた。

### ■ 中学校で生徒が学内ネットワークに不正アクセス

生徒が学内のパソコンネットワークに不正にアクセスし、同級生ら約200人の名前や成績、住所などの個人情報を入手していた。生徒は学内のパソコンから校務用サーバーに、校長の名前をパスワードに使うことで侵入できることをみつけ、自分の携帯用音楽プレーヤーを接続してデータをコピー。一部を印刷して教頭に示した。本人は「管理の不十分さを指摘したかった」と話しているという。全教職員にパスワードを変更させたほか、生徒が校務用のサーバーにアクセスできないようにした。校長は「私のパスワード管理の不十分さが原因で、統括する者として責任を痛感している」保護者に陳謝した。

## 既に起こっている事件

### ■ 児童らの顔載ったHPのパスワードが流出

市立小学校のホームページに載せられた同小学校の5年生児童35人分の顔写真と氏名を閲覧するためのパスワードが、「ネットの掲示板に書き込まれている」と匿名の電話があり、個人情報が流出していることが分かった。同小学校は、以前キャンプで訪れた岐阜県内の地元小学校と交流を深めるため、顔写真と氏名をホームページに載せて見てもらい、5年生同士でメールを交換することなどを計画。同小学校は、顔写真などをホームページに掲載し、パスワードを設定した。パスワードは両校関係者が把握していたという。同小学校は、ホームページを閉鎖し、校長らが児童35人の自宅を訪れるなどして謝罪した。

### ■ 高校のHPから、435名分の個人情報流出

X高等学校は、同校のホームページから中学生ら435名分の個人情報が誤ってインターネットに流出したと発表した。流出した個人情報は、同校のHPで資料請求やオープンスクールの申し込みをした435人の氏名、年齢、住所、電話番号、中学校名、メールアドレスなど。HPに置いていたデータファイルを誤って閲覧可能な状態にしたため、特定の検索エンジンに登録され、申込者の氏名等の検索でヒットするようになっていたという。匿名の連絡を受けて発覚。直ちに閲覧できないよう対処したが、発覚するまでの約2週間に外部から100件以上のアクセス形跡があったという。

# 提言

---

- リスクマネジメントから脅威 (threats) マネジメントへ
  - ✓ セキュリティ格差 (価値観、予算不足、ITリテラシー)の是正
  - ✓ 校務ネットワークと教育ネットワークドメインの分割
- セキュリティ共通基盤の構築
  - ✓ 共通認証基盤 ID=マイナンバーや教員免許との連動 PW=ワンタイム
  - ✓ リモートアクセス環境の提供 (USBの使用禁止)
  - ✓ 丸ごと暗号化
  - ✓ 確実なデータ・バックアップ (データダイオードによる分離)
- 教職員負荷の軽減とベースライン・セキュリティの確保
  - ✓ プロキシサーバー/DNSサーバーのデータセンター集約
  - ✓ 使用アプリの登録制
  - ✓ 確実なパッチワーク (脆弱性の是正)
  - ✓ 固定パスワードの定期的強度検査orパスワード生成ツールの使用
  - ✓ 入力フィールドをとまなうホームページの更新時の確実な脆弱検査
- 全校メールサーバーのDMARC対応
  - ✓ メーリングリスト代替機能 (グループウェア/SNSなど) の提供

# 自治体と教育委員会の セキュリティポリシーのマネジメントにおける 現状とポリシーの見直し手順について

平成28年7月1日

三鷹市教育委員会 田島康義

Copyright(C) Mitaka City. All rights reserved.

## 三鷹市の紹介



### 三鷹市

- 人口 183,951人
- 世帯数 91,400世帯
- 男：90,108人
- 面積 16.42km<sup>2</sup>
- 女：93,843人
- (平成28年4月1日現在)
- 小学校 15校、中学校 7校 (平成28年6月1日現在)
- 児童・生徒数 通常11,498人 教育支援 168人 合計 11,666人

- 1 三鷹市での情報セキュリティの取組
- 2 その他の取組
- 3 三鷹市教育委員会での情報セキュリティの取組
- 4 今後の課題

## 三鷹市での情報セキュリティの取組

## 1-1 情報セキュリティの取組①（特徴）

### ○ 「心技体」の姿勢

三鷹市では原則職員一人にパソコンを配布し、ICTを活用した効率的な業務の遂行を実施しているが、セキュリティの確保と職員のICTリテラシーの向上は大きな課題として、**人材育成・技術的対応・組織的対応**の「心技体」の姿勢で取り組んでいる。

### ○ ISO27001 (ISMS) の認証取得

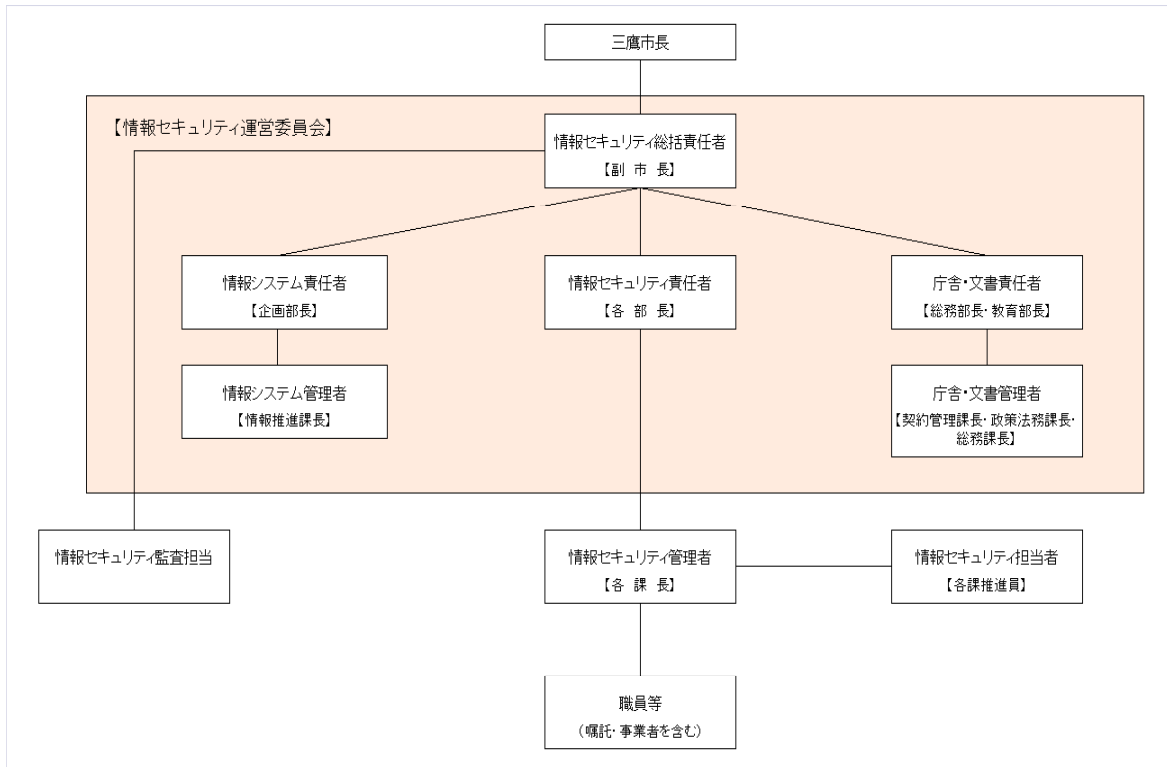
三鷹市では市民部を中心に11課で情報セキュリティマネジメントシステム（ISO/IEC27001:ISMS）の認証を取得し、国際規格に基づく運用を行っている。非認証取得課であっても、使用している業務システムはISMS認証取得課である企画部情報推進課がサーバー機器やネットワークを管理運用している。

なお、ISO27001 (ISMS) の非認証取得課においても特定個人情報保護評価を実施した課については、認証取得課と同様のルールを定め規程を作成した。

## 1-2 情報セキュリティの取組②（経過）

年度	トピック	動向
H14年度	・情報セキュリティポリシー策定 ・リスクアセスメント手法の基礎確立	準備
H15年度	・ISMS構築の取り組み開始 ・市民課、市政窓口、情報推進課で認証取得	事業開始
H16年度	・市民課から市民部全課に適用範囲拡大 ・市民税課、資産税課、納税課、保険課が認証取得	拡大
H18年度	・ISO27001への移行対応 ・政策法務課と契約管理課が認証取得	拡大
H20年度	・教育委員会総務課、学務課、指導課が認証取得 全庁11課で認証取得 ・情報セキュリティハンドブックの配布	拡大・更新
H21年度	・リスクアセスメント手法、内部監査手法の見直し ・全庁管理職を対象としたセキュリティ研修の実施	運用 見直し
H22年度	・全職員を対象とした情報セキュリティに関するアンケートの実施（以降毎年実施） ・「自治体セキュリティニュース」による啓発開始・情報セキュリティハンドブックの更新（第2版）	運用 底上げ
H23年度	・ISMS認証取得課以外への啓発 ・全庁セキュリティ点検（1年目）	運用 底上げ
H24年度	・更新審査 ・全庁セキュリティ点検（2年目）	運用 底上げ
H25年度	・ISMS認証取得課以外への啓発 ・研修の充実（外部職場、嘱託職員への啓発） ・全庁セキュリティ点検（最終年）	運用 底上げ
H26年度	・ISMS規格改訂に伴う移行審査	運用 見直し
H27年度	・情報セキュリティハンドブックの改訂（第3版） ・情報セキュリティポリシーの見直し検討	運用 見直し

## 1-3 情報セキュリティの取組③（推進体制）



Copyright(C) Mitaka City. All rights reserved.

6

## 1-4 情報セキュリティの取組④（研修・職員への周知）

### ①職員研修

- ・新入職員及び管理職となった職員への集合研修
- ・eラーニング（毎年100人程度が受講）

### ②情報セキュリティハンドブックの作成と配布

- ・セキュリティ8箇条（事例による説明とポイント）
- ・情報セキュリティに関する基本的説明

### ③全職員に対するセキュリティに関するアンケートの実施

- ・セキュリティ8箇条の理解度
- ・その他情報セキュリティに関すること
- ・研修の必要性を確認（H22～24）

### ④全職員へのセキュリティに関する情報提供

- ・自治体セキュリティニュース（J-LIS）の周知
- ・その他情報セキュリティに関する通知

### ⑤簡易版 I S M S 「全庁セキュリティ点検」の実施

- ・課長へのヒアリングと現場環境（職員へ）の確認
- ・セキュリティ8箇条の理解度
- ・その他情報セキュリティに関すること（H23～25）



### 情報セキュリティ8箇条

- 第1条 仕事のデータを持ち帰るべからず
- 第2条 パスワードはしっかりと管理すべし
- 第3条 外部記憶媒体の取扱いに注意すべし
- 第4条 職場のパソコンでは、業務と無関係なサイトは閲覧するべからず
- 第5条 離席の際には他人がパソコンを操作できないようにすべし
- 第6条 クリアデスクを心がけるべし
- 第7条 メールを送受信には細心の注意をするべし
- 第8条 コンピュータウィルスを意識すべし

Copyright(C) Mitaka City. All rights reserved.

7



### 2-1 個人情報保護条例①

#### ○ 個人情報保護条例

個人情報の開示請求等の権利の保障と個人情報の適正な取扱いについて必要な措置を講ずることにより、個人情報を保護し、市民の基本的人権を守る。

第8条で、電子計算組織の記録項目の設定、第13条で、個人別符号の制限、第26条、個人情報保護委員会の設置など

#### ○ 個人情報保護条例施行規則

個人情報保護条例の施行に必要な事項を定めたもの。

情報収集の手続き、目的外利用の条件、外部提供の手続き、外部提供の条件など

### 2-2 番号制度導入に伴う条例整備①

#### ○ 三鷹市個人情報保護条例 改正（その1）（H26.12）

平成26年第4回定例会で現行の一部改正を実施

委員会の調査審議事項に、特定個人情報保護評価に関することを加え市長が指名する委員3人以上をもって構成する部会において審議することとした。

⇒特定個人情報保護評価については、個人情報保護委員会の特定個人情報保護評価部会で第三者点検を行うこととした。

#### ○ 三鷹市特定個人情報保護条例 制定（H27.9）

・平成27年第3回定例会で特定個人情報保護に関する条例を制定

特定個人情報の保護に関しては、従来の個人情報保護条例を改正するのではなく、**新規条例を制定することとした。**

### 2-3 番号制度導入に伴う条例整備②

#### ○ 三鷹市特定個人情報保護条例の概要

番号法の規定に合わせて、市が保有する特定個人情報の適正な取扱いを確保するとともに、特定個人情報の開示請求の権利を保障することを目的として制定

##### 【主な規定】

- ◆ 特定個人情報の目的外利用の制限に関する規定
- ◆ 特定個人情報の提供の制限に関する規定
- ◆ 特定個人情報の開示請求等の請求者に任意代理人を認める。  
※運用に当たっては、本人からの委任の事実などを慎重に確認する。
- ◆ 特定個人情報を処理する事務を外部委託する場合に再委託を条件付きで認める。
- ◆ **特定個人情報保護評価の実施に関する規定**  
※番号法、特定個人情報保護委員会規則、同指針に基づいて評価を実施することを定める。

## その他の取り組み

### 2-4 番号制度導入に伴う条例整備③

#### ○ 三鷹市個人情報保護条例改正（その2）

平成27年第3回定例会で制定した三鷹市特定個人情報保護条例と取扱いを整合させるため現行の個人情報保護条例についても改正を行った。

##### 【主な改正事項】

- ◆ 個人情報の定義に「事業を営む個人の当該事業に関する情報」を追加
- ◆ 実施機関相互（市長部局⇔教育委員会等）における個人情報の授受を「提供」と位置付ける。
- ◆ 特定個人情報の開示請求等の請求者に任意代理人を認める。  
※運用に当たっては、本人からの委任の事実などを慎重に確認する
- ◆ 個人情報を処理する事務を外部委託する場合に再委託を条件付きで認める。
- ◆ その他、運用で実施していた内容を条例に定める など

# 三鷹市教育委員会での 情報セキュリティの取組

## 三鷹市教育委員会での情報セキュリティの取組

### 3-1 平成28年6月に学校情報セキュリティ基本方針を策定

#### ①策定したもの

1. 「三鷹市立学校情報セキュリティ基本方針」
2. 「三鷹市立学校情報セキュリティ対策基準」  
「三鷹市立学校情報セキュリティ対策実施手順」
  - 様式 1 学校情報資産取扱一覧表
  - 様式 5 研修等実施記録表
  - 様式 6 学校情報セキュリティ対策実施体制図
  - 様式 7 学校情報セキュリティ文書・記録一覧表
  - 様式 8 学校情報セキュリティ対策実施状況報告書
3. 学校情報取扱基準

#### ②学校に提出を求めたもの

各校における情報セキュリティ対策実施手順

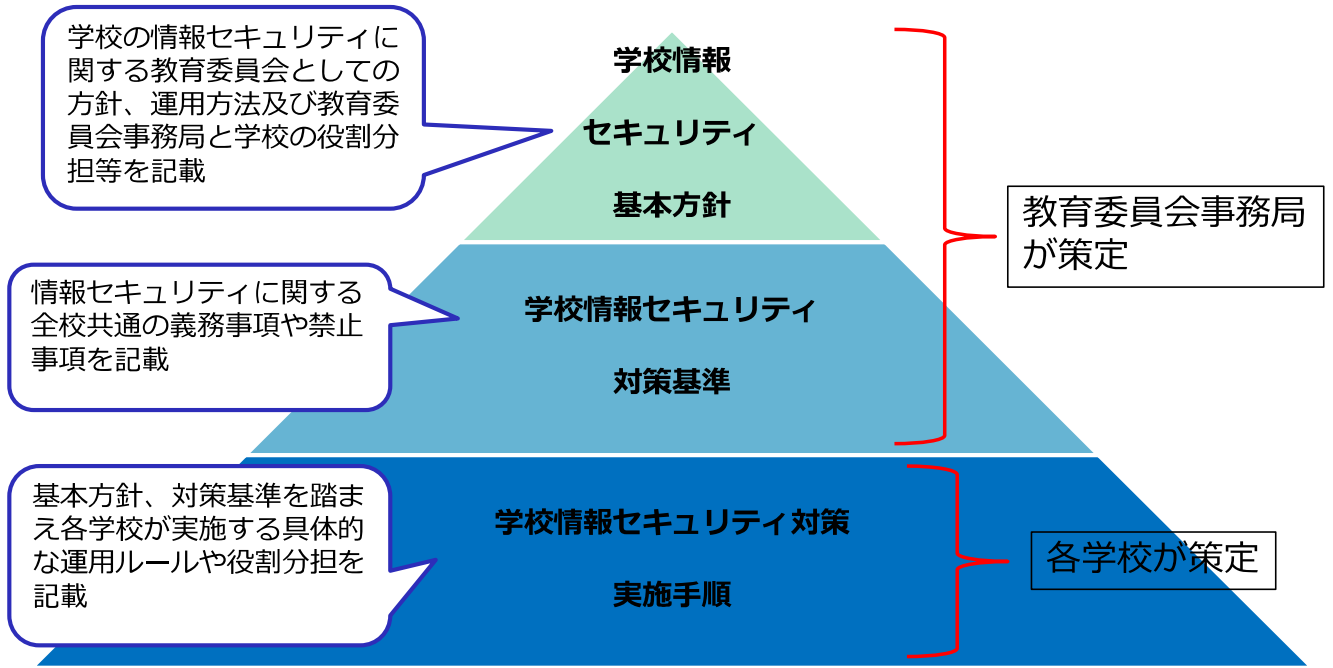
## 3-2 策定前の状況と課題

- 教育委員会事務局が策定し、学校に通知したものは次の3つ
  - 三鷹市公立小・中学校教育用コンピュータ及びインターネット取扱基準（平成15年1月）
  - 校務のために教職員が作成したデータの管理に関する運用指針（平成17年5月）
  - 三鷹市立学校における個人情報及び情報資産の適正な管理について（通知）（平成20年10月）
- 個々の規定が独立しており、**体系化されていないため分かりにくい。**
- 学校における情報セキュリティに関する事項について、**学校と教育委員会事務局の役割分担が不明確**
- 各学校が策定した「個人情報等安全管理基準」の運用状況を定期的に**チェックする仕組みがない。**
- 私物機器（タブレットPC及びスマートフォン等）の利用も**校長の許可があれば全て可**
- **教職員の遵守事項**が現在のICT技術動向、社会情勢及び教育ネットワークシステムの運用と乖離している。

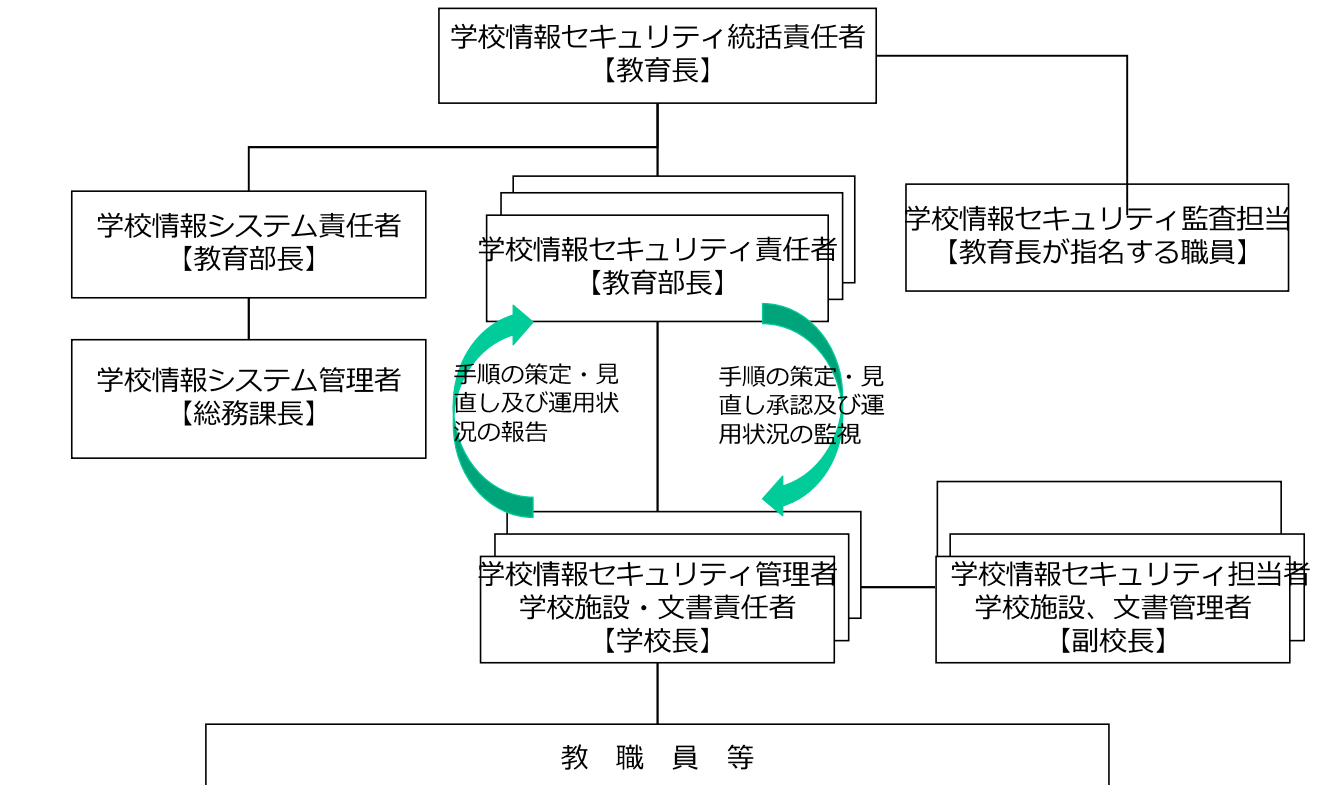
## 3-3 課題解決に向けた取組

- ① 現行の規定類を、現在のICT技術動向、社会情勢及び教育ネットワークシステムの運用を踏まえ、三鷹市のISMSの運用を参考に「三鷹市立学校情報セキュリティ基本方針」として再構成  
→**規定類の体系化による情報の整理**
- ② 学校における情報セキュリティに関する事項について、学校と教育委員会事務局の役割分担を明確化  
→**教育委員会全体で取り組む体制の整備**
- ③ 各学校の情報セキュリティに関する運用状況を定期的にチェックする仕組みの導入  
→**策定したルールの有名無実化の予防**
- ④ 現在のICT技術動向、社会情勢及び教育ネットワークシステムの運用を踏まえた教職員の遵守事項の見直しと校長裁量範囲の明確化  
→**グレーゾーン減少による情報セキュリティリスク低減**

### 3-4 基本方針の構成



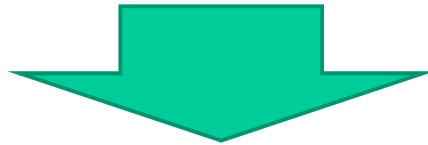
### 3-5 学校と教育委員会事務局の役割分担



3-6 チェック機能

**【策定前】**

- 平成20年度に指導課より、各学校に「個人情報等安全管理基準」の策定と校内研修の実施を通知
- 上記基準の運用と研修実施は各学校に委任



**【策定後】**

学校長に次の各項目の実施を義務付け

- ① 毎年4月中に教職員等向け研修実施（新規任用の教職員等に対しては着任時に実施）
- ② 年1回の手順見直しの検討
- ③ ①及び②の**実施状況の記録と、教育部長への報告（年度毎）**

3-7 私物機器の利用に関する校長の裁量を限定

**【策定前】**

次の行為も、**「校長の許可」があれば全て可**

- 校務・授業等における私物機器の利用
- 校内機器への私物機器の接続



**【策定後】**

次の場合以外は**不可（校長が許可してもNG）**

- ① 他自治体から転入してきた教職員が、それまで使用していた教材等のファイルをファイルサーバに保存する場合
- ② 校内における外部講師による講演会等で、外部講師が持ち込んだプレゼンテーション資料を使用する場合
- ③ 学校運営協議会委員等が作成した資料を校内のパソコンで修正したり、印刷する場合

### 3-8 教職員の遵守事項の見直し

#### 1. 教職員の遵守事項として、次の項目を新たに追加

- ① 教職員の義務に関する一般規定（地方公務員法第34条、三鷹市個人情報保護条例第3条第3項及び基本方針に基づく、適切な情報セキュリティ管理の継続的な実施の義務付け）の追加
- ② 私物機器・媒体の利用禁止
- ③ クリアデスクを始めとする整理整頓の徹底
- ④ ID及びパスワードの他人への貸与等の「なりすまし行為」の禁止
- ⑤ 「Gmail」及び「Yahoo!メール」等のwebメールサービスの利用禁止
- ⑥ 「Dropbox」、「Googleドライブ」及び「OneDrive」等のストレージサービスの利用禁止
- ⑦ ソフトウェアの無断インストールの禁止
- ⑧ 業務上必要のない送信先への電子メール送信禁止
- ⑨ 複数人に電子メールを送信する場合における原則宛先「bcc」設定の義務付け
- ⑩ 学校・学園ホームページ及び三鷹SchoolSNS上への教職員等及び児童・生徒の画像及び動画の本人が特定可能な状態での掲載禁止（本人（児童・生徒にあっては保護者）が事前に同意した場合を除く。）

20

### 三鷹市教育委員会での情報セキュリティの取組

#### 2 教職員の遵守事項を「情報セキュリティ遵守事項」として一覧化

##### 【三鷹市立学校情報セキュリティ遵守事項】

- 1 学校が保有する情報は、「原則外部への持ち出し禁止（メール送信も禁止）」
- 2 上記の情報のうち、三鷹市立学校情報セキュリティ対策基準別表に定める分類S-1に該当する情報資産は、「絶対に持ち出し禁止」※1、「指定場所以外への保存禁止」、「メール送信の禁止」
- 3 三鷹市及び三鷹市教育委員会が配置している「機器（※2）の持ち出し禁止」
- 4 業務上の目的で、電子ファイル・記録媒体（※3）等の情報資産を校外へ持ち出す場合は、「事前に書類の提出及び校長の許可が必要」※3、「電子ファイルにはパスワードを設定」、「パスワードと記録媒体（※4）を一緒に携帯しない」、「校長の許可の下、記録媒体（※4）を外部に持ち出す場合は、記録媒体（※4）を入れるかばんなどを身体から離さない」
- 5 私物の機器（※5）・記録媒体（※4）は、「校務・授業等での使用（校内の機器（※2）への接続を含む。）禁止」
- 6 三鷹市立学校情報セキュリティ対策基準別表に定める分類S-1に該当する情報資産は、「S-1とS-1以外を分けて保管・管理」、「児童・生徒も使用するフォルダでの作業は禁止」
- 7 業務に関係のないインターネット上のウェブサイトへのアクセス禁止
- 8 webメールサービス（Gmail、Yahoo!メール及びhotmail等）の利用禁止
- 9 インターネット上のストレージサービス（Dropbox、Googleドライブ及びOneDrive等）の利用禁止
- 10 業務上必要のない送信先への電子メールの送信禁止
- 11 学校・学園ホームページ及び三鷹SchoolSNS上への、児童・生徒の本人が特定可能な画像及び動画掲載の原則禁止（※6）

※1 法令に定めのある場合を除く。※2 テレビ、プロジェクター、実物投影機、パソコン（タブレット端末を含む。）、プリンタ、各教室の情報コンセント、スイッチングハブ、その他校内の全ての機器が対象 ※3 校外への持ち出しに当たっては、1使用目的 2内容 3作業場所・方法 4使用期間 5作業後の扱い等について事前に確認した上で許可とする。※4 ICボイスレコーダー、デジタル（ビデオ）カメラ、パソコン（タブレット端末を含む。）、メモリーカード、USBメモリ、フロッピーディスク、CD/DVD-R等、データ記録可能なものは全て対象 ※5 ICボイスレコーダー、デジタル（ビデオ）カメラ、パソコン（タブレット端末を含む。）、スマートフォン、ガラケー、外付けHDD、NAS、プリンタ、無線ルーター、スイッチングハブ、その他学校資産でないものは全て対象 ※6 保護者が事前に同意した場合を除く。

### 3-9 学校情報取扱基準一覧の分類の見直し

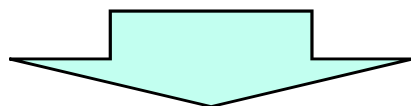
策定前 東京都立学校の分類を基に作成

S-1 原則持出禁止

(プライバシー性が高い情報並びに指導要録や成績一覧表などは持出禁止)

S-2 持出す都度、校長等の承認を得る

S-3 包括的承認 (上記以外は全て可)



策定後 持出可に対して明確化 (記載がないものは、管理職に協議、相談)

S-1 法令に定めのある場合を除いて持出禁止

S-2 校長、副校長の承認を得た場合を除いて持出禁止

S-3 持出可 (配布、公開されてもよい校務情報)

学園・学校・学年・学級だより学校行事のしおり、卒業アルバムなど

(個人情報についてはS-2の扱い)

S-4 持出可 (配布、公開されてもよい校務情報)

授業用教材、教材研究資料など

### 3-10 三鷹市の I S M S 規定と教育委員会の規定の違い

三鷹市 I S M S の規定

**I S M S 文書で以下の項目を規定**

1. 目的
2. 対象
3. 情報
4. 管理体制  
三鷹市長が定める。情報セキュリティ委員会を設置
5. 情報の管理及びリスク評価
6. 情報の取扱い
7. 業務委託契約
8. 監視
9. 監査
10. 報告
11. 事業継続管理
12. 職員研修
13. 保険
14. 関連法規等の順守
15. 違反行為に対する処分
16. 基本方針の見直し

教育委員会で新たに定めた規定

**学校が運用・順守するために負担にならない範囲で規定**

1. 目的
2. 対象
3. 情報
4. 管理体制  
教育長が定める。情報セキュリティ委員会は設置しない。
5. 情報の管理 **学校の負担を考慮してリスク評価はしない。**
6. 情報の取扱い
7. **業務委託契約の規定は、学校で委託契約をしないため、規定しない。**
8. 監視
9. 監査 **内部、外部監査は実施しない。**
10. 報告
11. **事業継続管理の規定は、I S M S 認証を取得しないため規定しない。**
12. 職員研修
13. **保険の規定は、I S M S 認証を取得しないため規定しない。**
14. 関連法規等の順守
15. 違反行為に対する処分
16. 基本方針の見直し



## 今後の課題

### 今後の課題

#### 4-1 今後の課題

##### ① 教職員の意識改革

校長、副校長の管理職が教職員に対してどこまで情報セキュリティの重要性について、教育、徹底できるか

(教職員は東京都の職員であるため、サービス規程等も東京都)

**セキュリティを守る(維持)するのは人**

##### ② 情報セキュリティの運用

学校情報資産一覧表の更新、研修の実施、各種記録(使用記録、持出記録など)、事故等発生報告書など、**適切な運用を継続的な実施**

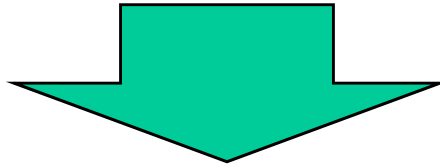
##### ③ 教育委員会内での情報共有

教育課程・学習指導、教職員人事、研修などを行う部署(指導課)とシステム構築・運用する部署との連携が重要  
学校との情報共有がポイント

### 4-2 国に期待すること

#### 自治体の現状

- ・セキュリティポリシー作成後、見直しがされない  
新しい技術、脅威への技術的対応が困難
- ・セキュリティポリシーの見直しの手順がそもそもない  
人材がない（セキュリティポリシーがよくわからない）



#### あるといいな

- ・自治体規模、セキュリティ対策の内容など選択によるポリシー作成、リスク評価、運用できるケース分けされた雛形の提供
- ・雛形の定期的な見直し

ご清聴ありがとうございました。