

# 豊島区



## 「庁内LANと校務LANの統合 セキュリティ強化と集中管理による効率化」



平成28年3月1日

政策経営部 情報管理課長  
高橋 邦夫

### 豊島区が校務と庁内とのネットワーク統合した背景

#### きっかけ

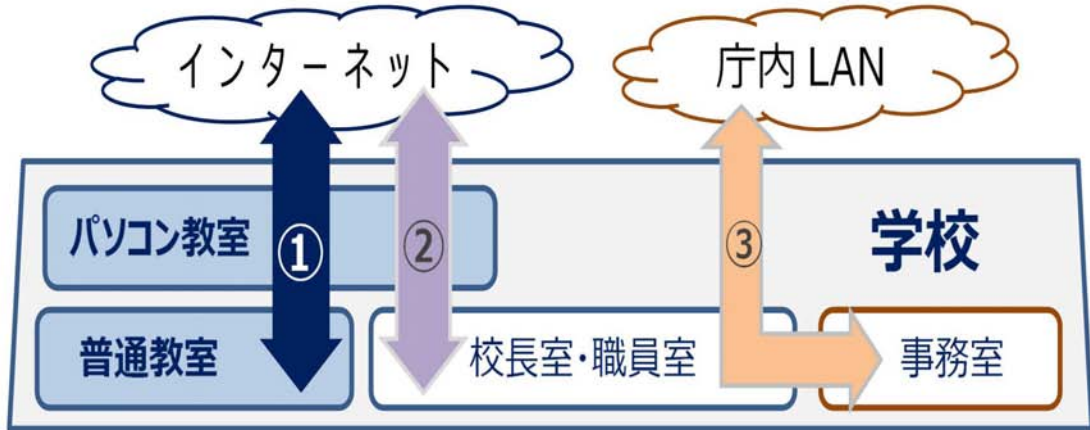
- ・教育ICT予算要求に対する財政部門の不信感(高額に見える)
- ・区長としては必要性は理解できるが、どうにか予算を抑えたい
- ・教育委員会担当者は現状の運用・管理業務で手一杯

#### 解決策

- ・区長部局システム担当者への下命
- ・教育委員会担当者をシステム部門兼務職員として任命
- ・システム部門のフォローアップ(基盤部分はシステム課調達)

# 豊島区立小中学校の平成25年度までの状況

## 学校のLAN環境（3種類のネットワーク）

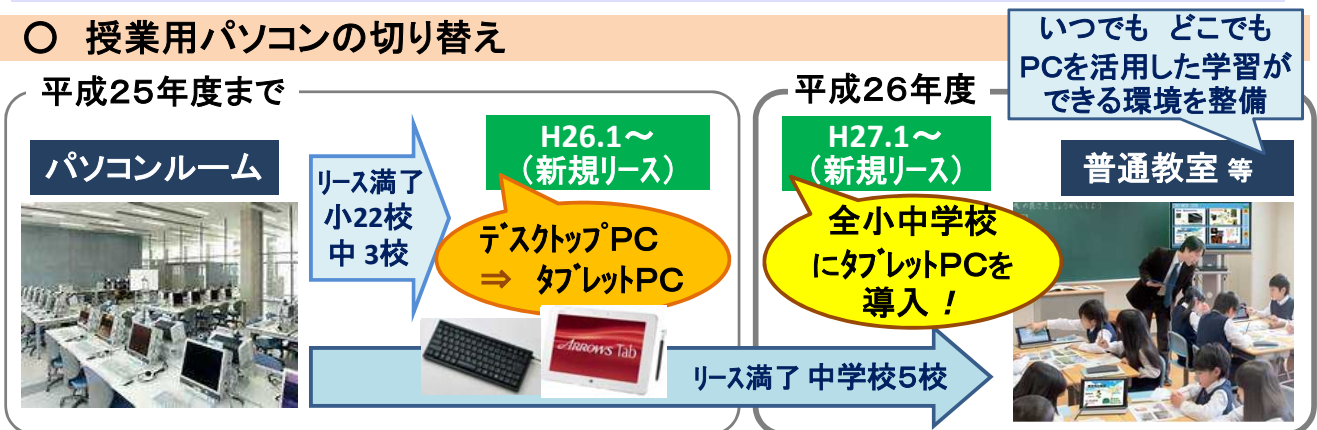


- ① … 学習用 LAN（児童・生徒が授業で使用）
- ② … 校務用 LAN（教職員が校務で使用）
- ③ … 庁内 LAN（校長・副校長・事務職員が教育委員会との事務処理等で使用）

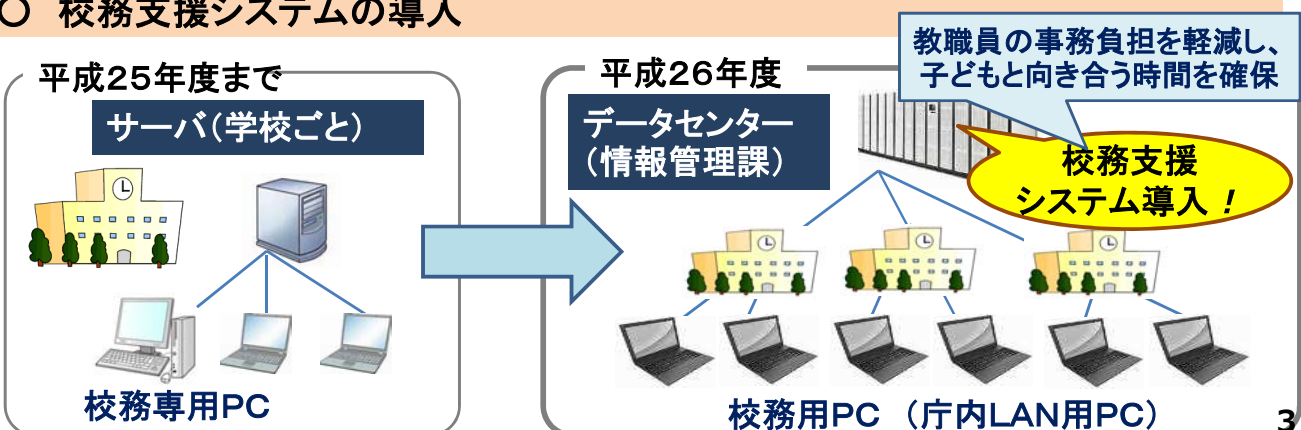
2

## 切り替えの方向性

### ○ 授業用パソコンの切り替え



### ○ 校務支援システムの導入



3

## 校務LANと授業用LAN統合の長所・短所

### メリット

- ・物理的に一元化が可能で、費用面・管理面が優れている
- ・職員室で作った教材を学習用パソコンに配付可能
- ・ネットからダウンロードした教材を両方で使える

### デメリット

- ・セキュリティレベルがあまりにも違う
- ・教師のデータに子どもからアクセス出来る危険性あり
- ・データを取り扱う教師のリテラシが高くない

4

## 庁内LAN・校務LAN統合の背景と要件

### 1. 教員側での独自運用

教員ユーザのPC利用として、USBメモリの利用など独自の運用が考えられる

### 2. ユーザー情報の管理元が異なる

教員情報と職員情報の管理元が異なるため、年次更新などメンテナンスのタイミングが異なる

### 3. 利用するシステムが異なる

メール関連、ファイル共有関連、校務支援システムなど、教員が利用するシステムが、職員側で利用するシステムとは異なる



### 既存のユーザー管理とは別の管理体制の必要性

既存のユーザー管理(ドメイン環境)に教員情報を含めるのではなく、教員用のドメインを新設し、ユーザ情報、グループ情報など、職員とは異なるセキュリティポリシーで管理することが、結果として運用負荷を下げることになる

5

## また、相反する要件として

### 1. 職員と同様なセキュリティーレベルの追求

ベースとなるセキュリティーポリシーは原則職員側と同様にしたい

### 2. 利用システムの相互利用

校長、副校長は全庁ポータルなど職員側のシステムを利用する場合がある  
また、その逆に教育委員会職員が校務システムを共有する場合もある

### 3. インフラの統一

豊島区として、統一されたネットワーク認証、およびクライアントPCの管理システムを利用したい



## インフラ基盤の相互利用の必要性

教員を独自にドメインで管理すると、ベースセキュリティーポリシーの継承や、職員システムの利用をすることが難しくなる。

インフラ基盤は、現在運用しているものをそのまま利用して、追加のコストを抑える。

※インフラ基盤: ネットワーク認証系システム (RADIUSサーバ、証明書認証局)、PC管理システムなど

6

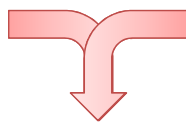
## 統合の方針

職員側とは別の管理体系

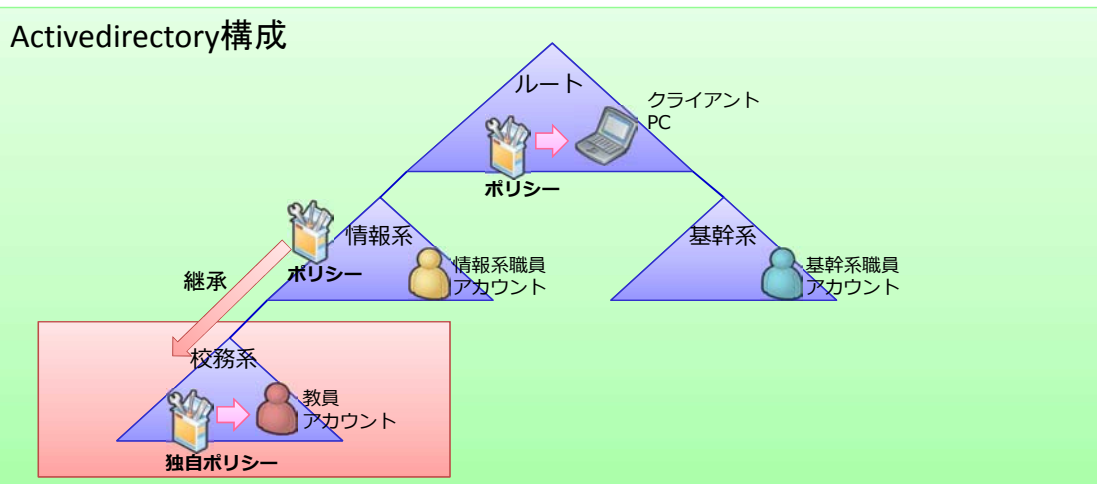
ユーザー管理  
システム利用管理

豊島区として統一した管理

セキュリティーの統一化  
クライアントPC管理



この2つの要件を満足させることが目的



教員情報を既存ドメインで管理するのではなく、配下に設けた校務用のドメインにて管理運用することで実現している

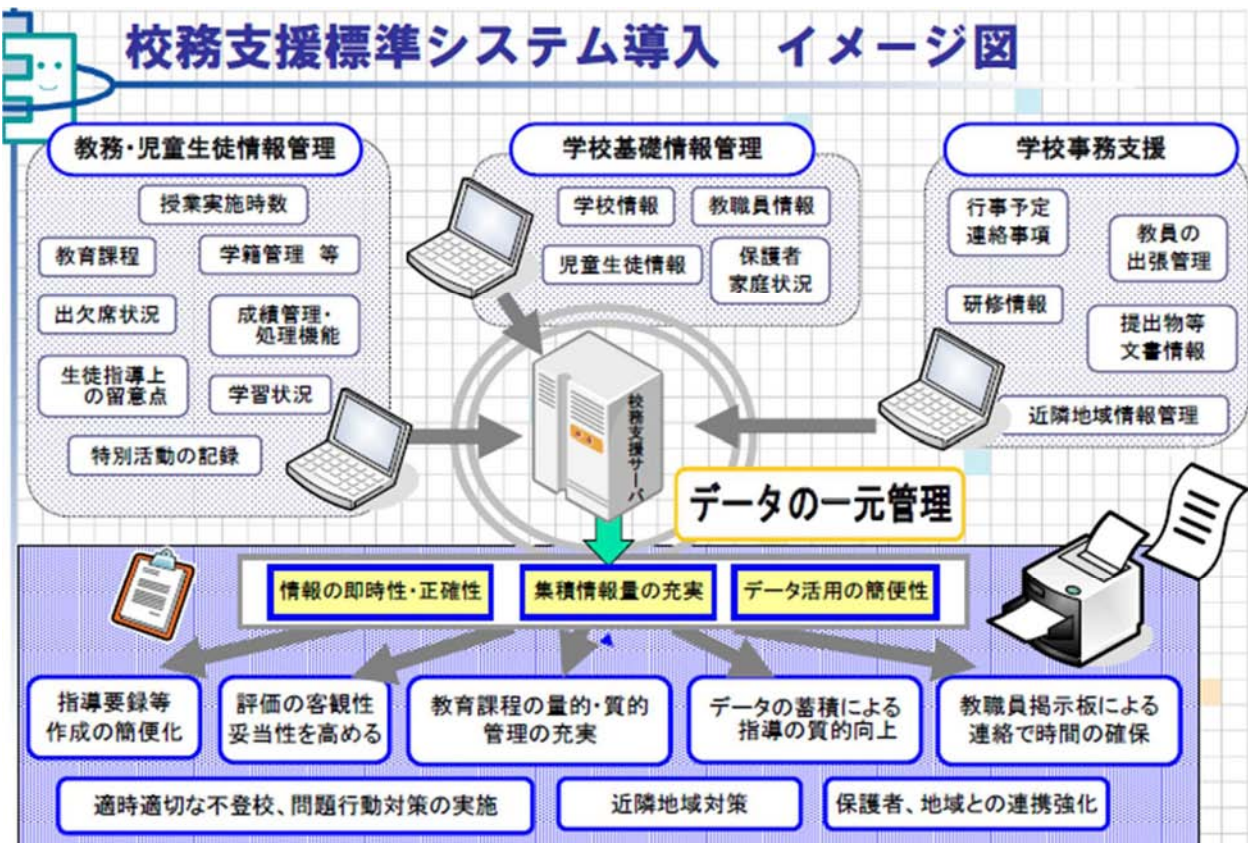
7

## 庁内LANと校務LANの連携

カテゴリ	概要
ユーザー（職員情報）の管理	庁内LANの職員情報管理システムと同等の教職員情報管理システムを構築 →庁内LANでの運用ノウハウを活用
データのやり取り	庁内LANと校務LANの間で、データのやり取りが出来る場所を準備 →これまでのUSBメモリでのデータのやり取りを排除し、セキュリティリスクを軽減
インターネット閲覧	校務LANのパソコンは、庁内LANのNWを介してインターネットを閲覧 →インターネット閲覧のルール（フィルタリング規則）は校務LAN独自のものを導入 校務ネットワーク独自で各校単位のプロバイダー接続（契約）は不要
プリンター（印刷環境）	庁内LANと同様に、ネットワーク経由のプリンタ環境を整備していく →事務環境の改善
上記以外のやり取り	原則禁止（論理的に分断された設定とする） →庁内の情報への教職員のアクセスや児童の個人情報への区職員のアクセスを排除し、セキュリティリスクを軽減

8

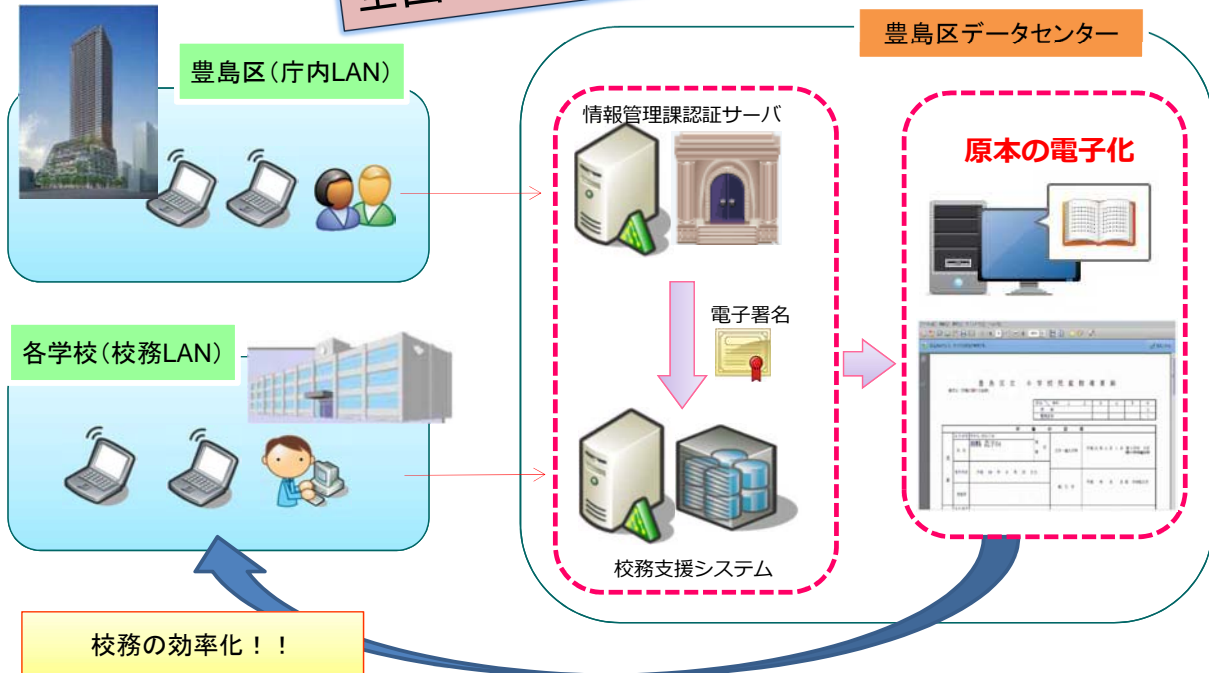
## 校務支援システムの選定は教育委員会



9

## 副次的効果・指導要録原本の電子化

全国で2例目。首長部局との連携では初！



10

## 総務省が打ち出した自治体情報セキュリティ強靱策

新たな自治体情報セキュリティ対策の抜本的強化に向けて

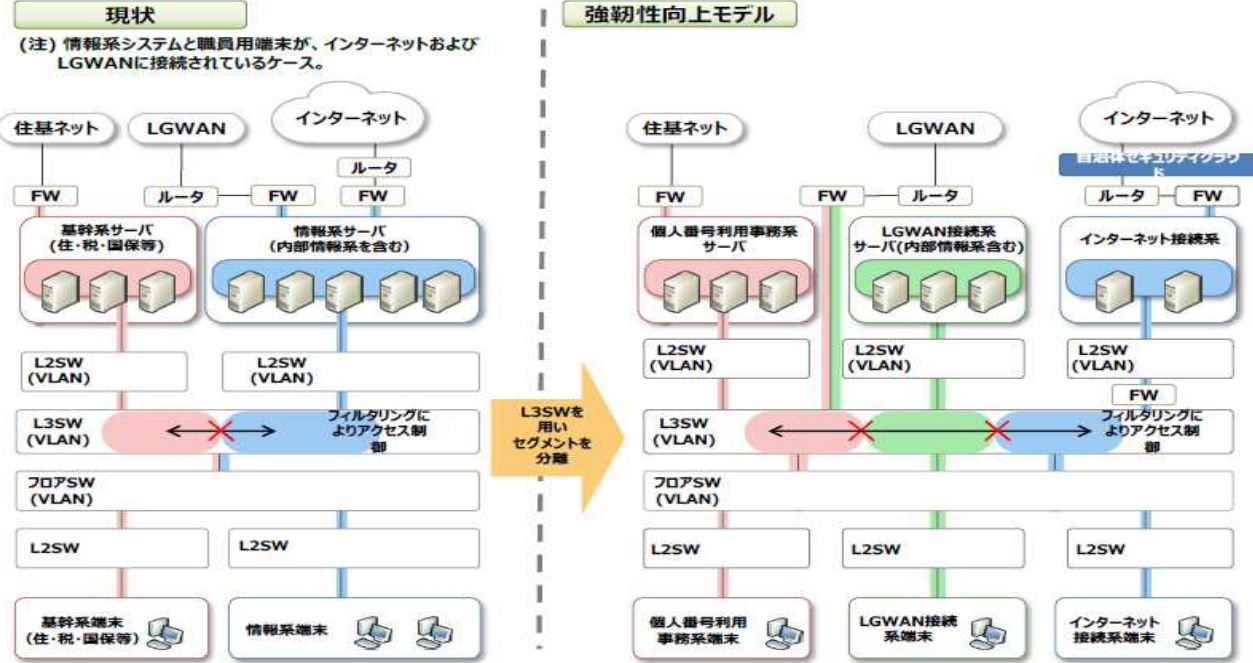
「システム全体の強靱性の向上」確保のための『三層の構え』

1. 住民（個人）情報の流出を徹底して防ぐ
  - ◆ マイナンバー利用事務系においては、他の領域との通信をできないようにする。
  - ◆ 端末からの情報持ち出しをできない設定をする。
  - ◆ 端末への二要素認証を導入する。
2. LGWAN接続系とインターネット接続系の分割
  - ◆ LGWANを活用する業務システムとWeb閲覧やインターネットメールなどのシステムとの通信経路を分割する。
  - ◆ システム間で通信する場合には、ウィルス感染のない無害化通信を図る。
3. 自治体情報セキュリティクラウドの構築
  - ◆ インターネット接続系は、都道府県と市区町村が協力して、インターネット接続口を集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講じる。

11

# 総務省が打ち出した自治体情報セキュリティ強靱策

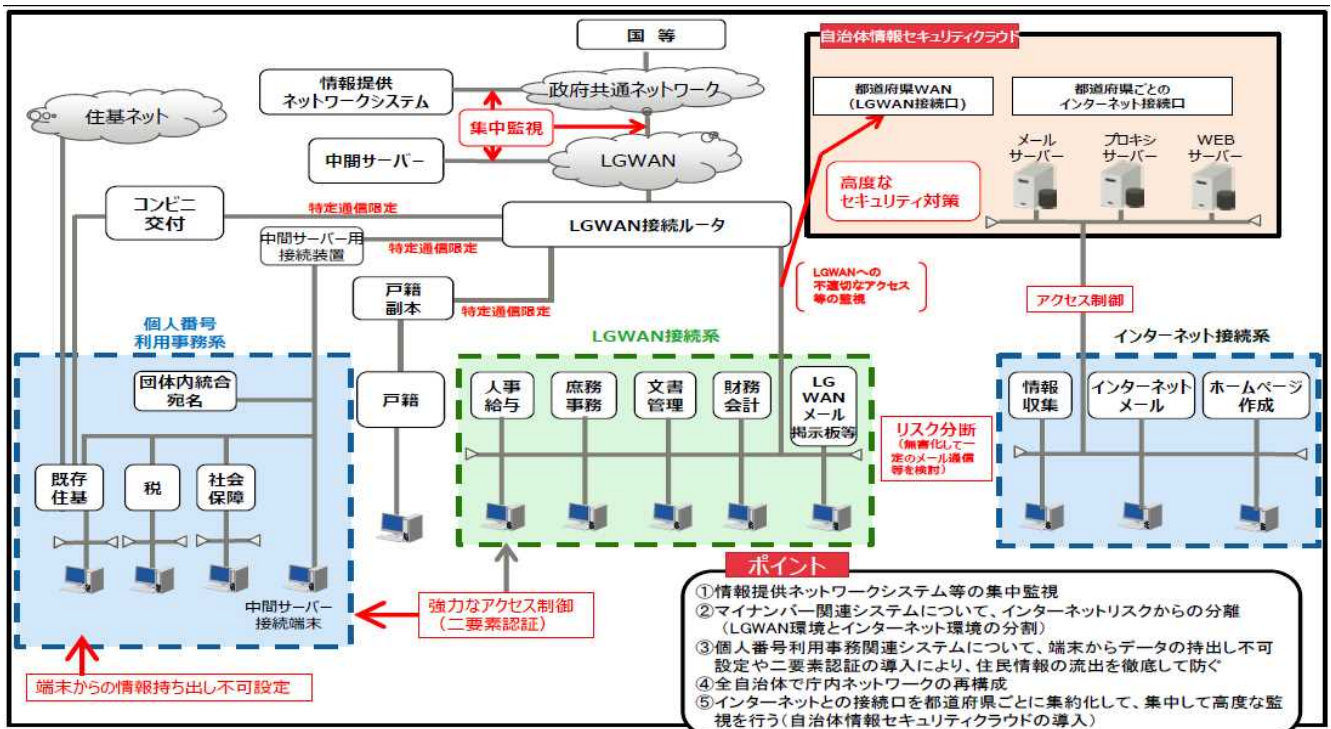
LGWAN環境とインターネット環境を分割し、「個人番号利用事務系」、「LGWAN接続系」、「インターネット接続系」でネットワークとシステムを分類し、その後、端末を適切に通信制御する。



## インターネットと個人情報との分離の徹底

12

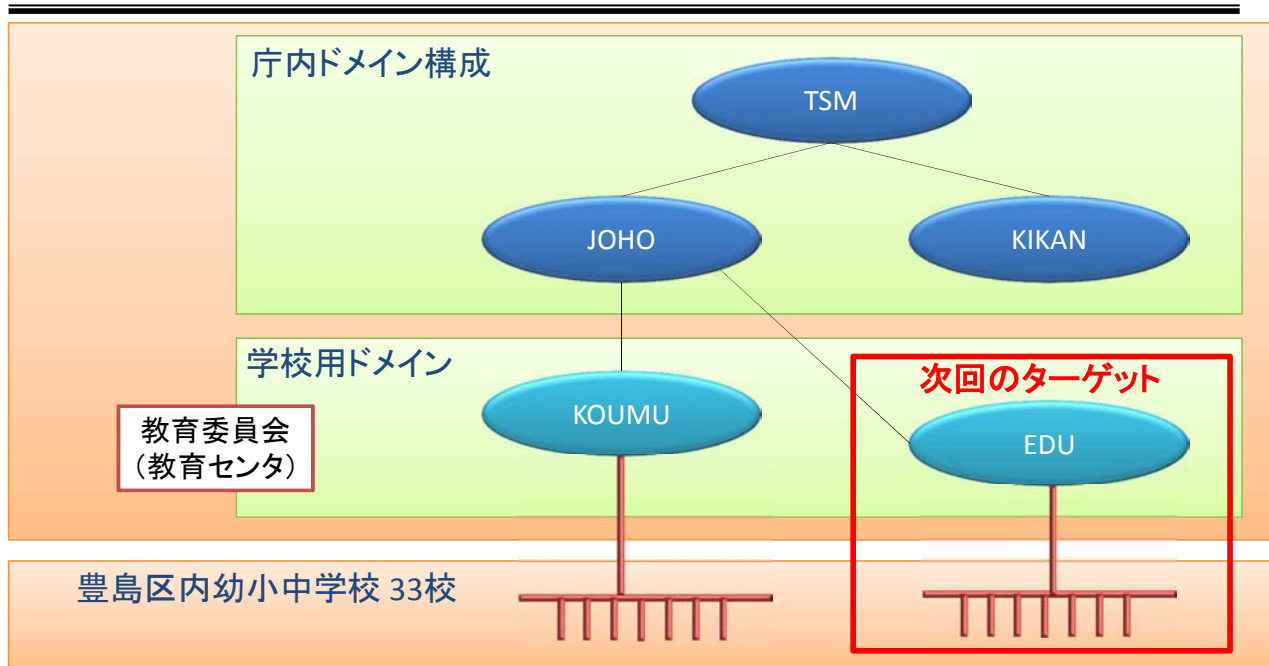
# 総務省が打ち出した自治体情報セキュリティ強靱策



## 首長部局の仕組みを利用してインターネットのリスクを最小化

13

## 将来は授業用ネットワークも一元化



- 学校用ドメイン(ネットワーク)の統合の目的
  - 教師・生徒情報の一元管理
  - PC管理の効率化(資産管理の一元化)
  - 情報共有の向上

現在は教育委員会管理の無線ネットワークも一元化する

14

## 豊島区での無線LANサービス(職員用と来訪者用)

(職員用)

- ・5GHz帯での通信
- ・一般のスマートフォンでは認識されない
- ・IEEE802.1xのEAP-TLS方式で接続制限
- ・接続後にPCの検疫を行い、パッチを強制適用

地域情報化と教育情報化を同時に実現可能



1台のアクセスポイントで職員用と来訪者用無線LANを管理

(来訪者用)

- ・2.4GHz帯での通信
- ・職員用と物理的には同一で論理分割されたNW
- ・センタースイッチから先は物理的にも分割
- ・エリアWi-Fiとして、豊島区のWi-Fiグループに参加



15