Empowered by Innovation NEC

地方公共団体におけるネットワークの考え方
～番号制度導入に向けて～

平成25年11月14日

NEC

公共ソリューション事業部

Agenda

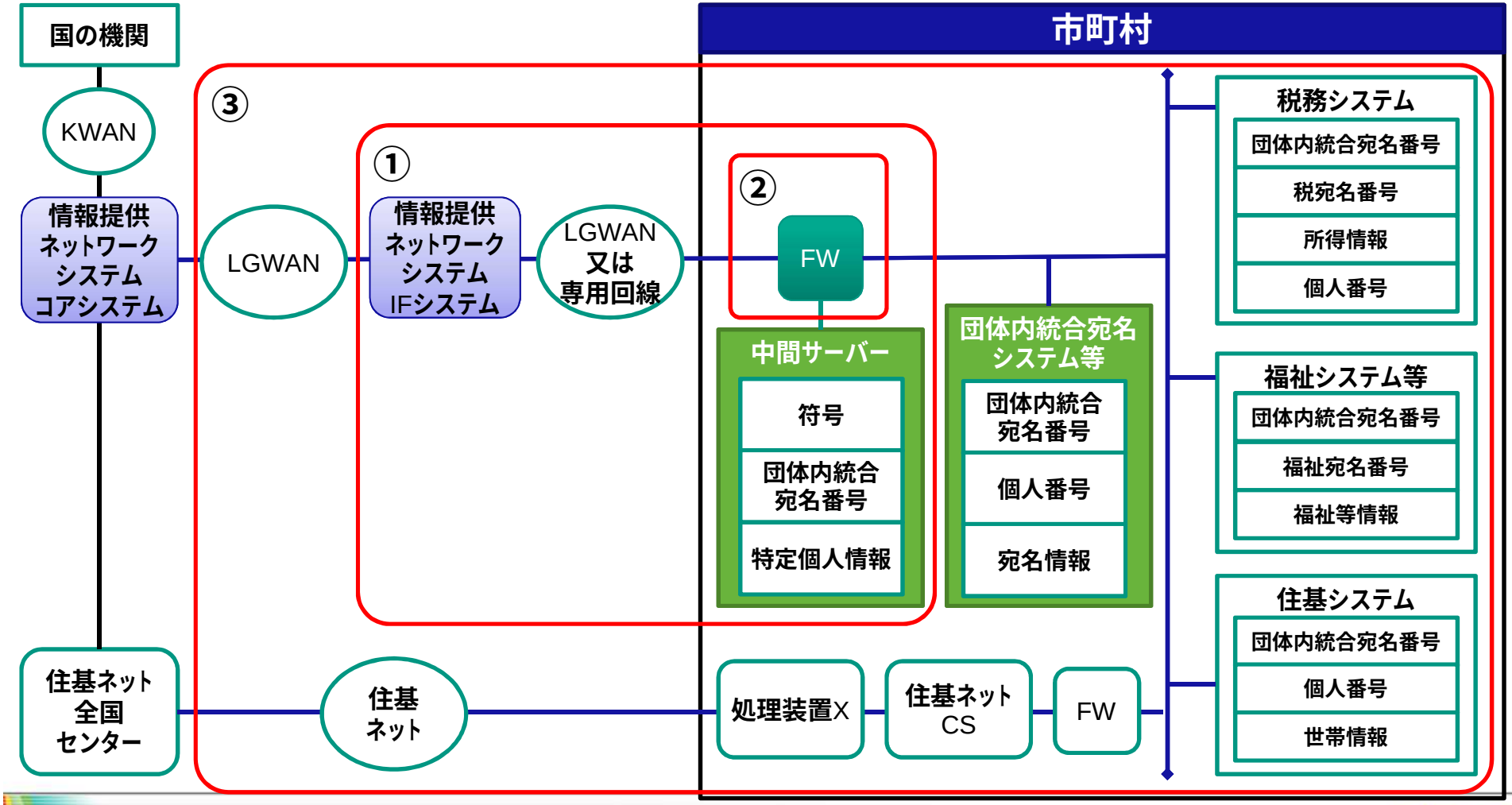
1. 総務省「地方公共団体における番号制度の導入ガイドライン」における
   ネットワークの記載事項
2. ネットワークの現状について
3. ネットワーク見直しのための検討事項
4. セキュリティ見直しのための検討事項
5. セキュリティ脅威とその対策

総務省「地方公共団体における番号制度の導入ガイドライン」におけるネットワークの記載事項

「地方公共団体における番号制度の導入ガイドライン」のモデル構成

出展：総務省「地方公共団体における番号制度の導入ガイドライン」

① 中間サーバーと情報提供ネットワークシステムを接続
② 中間サーバーと情報提供ネットワークシステムをFWで分離（LGWANの規定に伴う対応）
③ 庁内ネットワークを住基ネットとLGWAN双方に接続



地方公共団体における番号制度の導入準備について

出展：総務省「地方公共団体における番号制度の導入ガイドライン」より抜粋

- 情報提供ネットワークシステム（IFシステム）への接続に備えて、市町村内の庁内ネットワークの見直しを実施する。（平成27年度）
- 総合運用テストでは、各地方公共団体のシステムを情報提供ネットワークシステムに接続し、番号法に基づく情報提供／情報照会の一連の流れをテストする。（平成28年度）
- 一部の条例では、地域の独自性に基づく規定が定められているため、番号法における規定との間に整合性が取れていない場合は、条例改正等の検討を行う必要がある。
  - 外部提供に係る規定
  - オンライン結合の制限に係る規定
  - 電子計算機の結合の制限に関する条例の独自規定

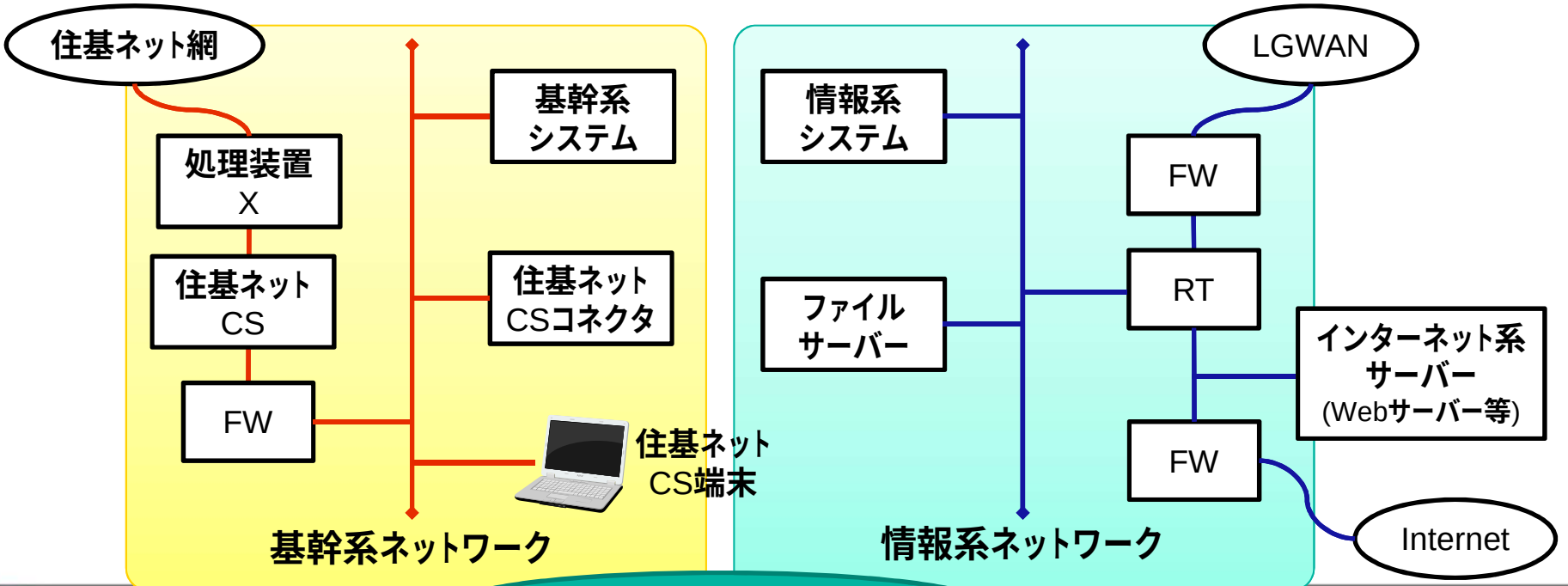
番号制度への対応にあたり、庁内ネットワークの見直しが必要

ネットワークの現状について

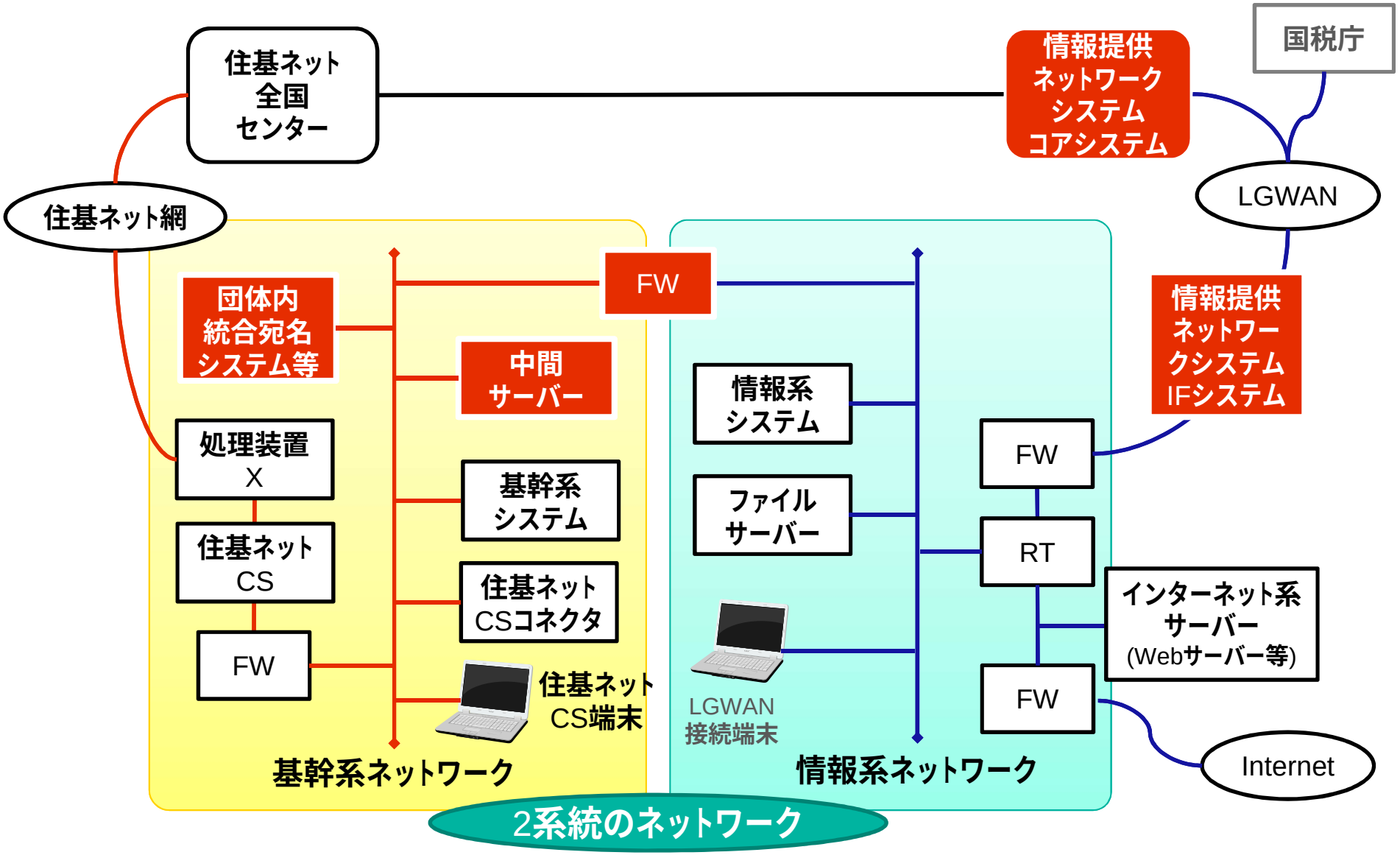
自治体ネットワークの一例

現状

- 住民サービス向けの基幹系システムを利用するための基幹系ネットワークと、情報系システムを利用するための情報系ネットワークの2つが存在。
- 基幹系ネットワークには本人確認情報を自治体間で連携させる住基ネットが接続。物理的に閉域網とすることでセキュリティを担保。
- 情報系ネットワークには自治体間で情報のやり取りを行うLGWANとInternetが接続。



番号制度施行後の自治体ネットワークの一例

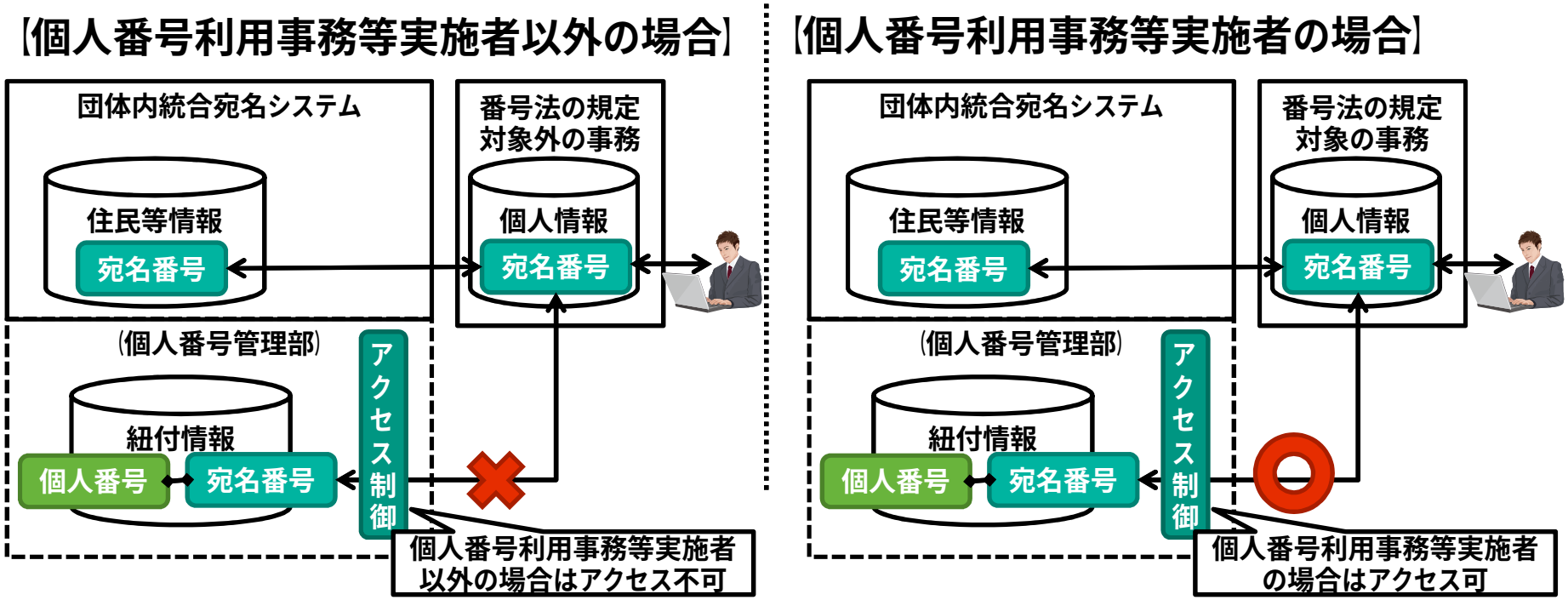


ネットワーク見直しのための検討事項

番号制度導入に必要な技術的措置

出展：総務省「地方公共団体における番号制度の導入ガイドライン」より抜粋

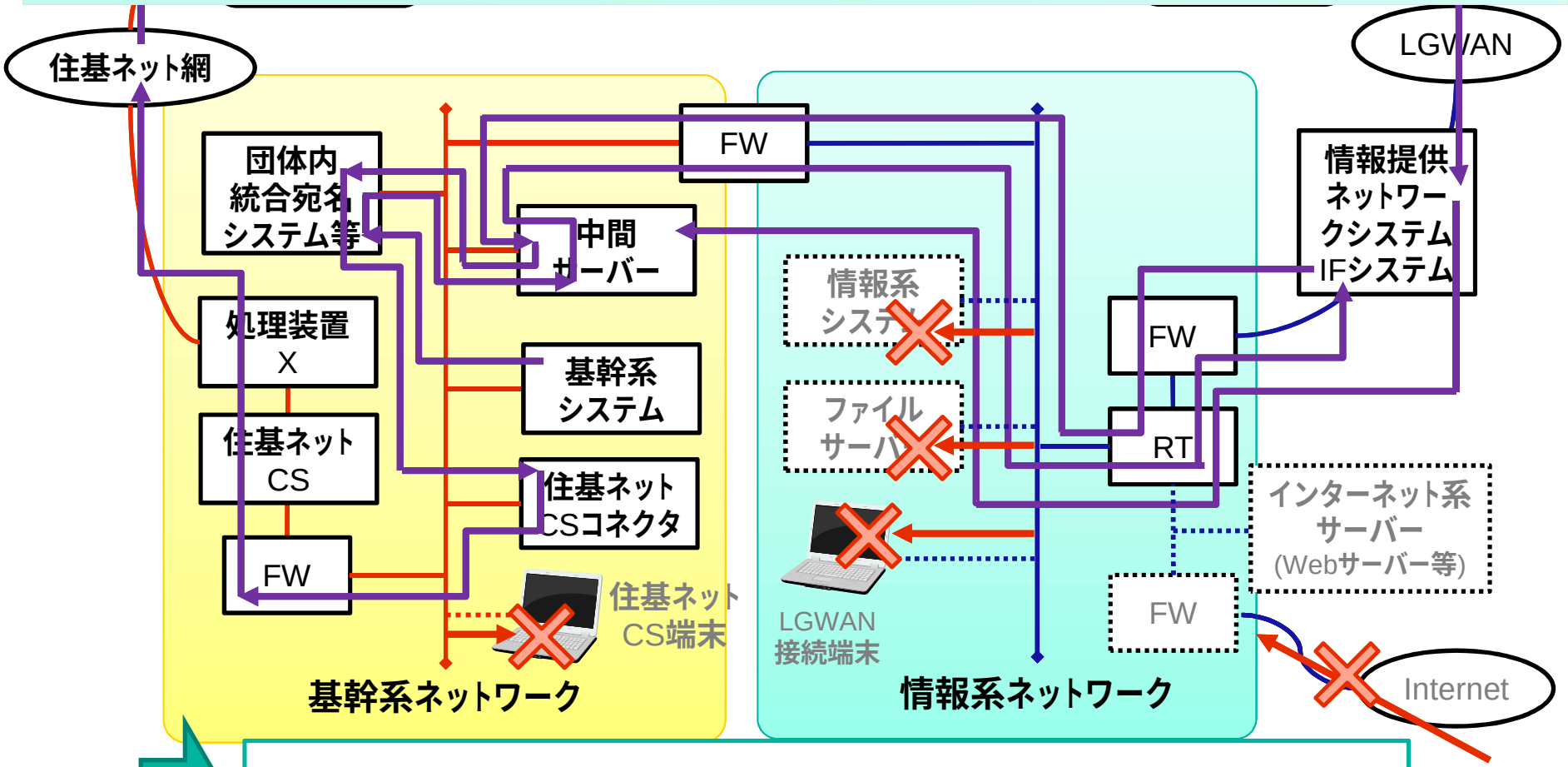
これらの情報システムの構築や改修に当たり、従来の個人情報ファイルと特定個人情報ファイルへのアクセスを識別し制御するためのデータ保持方法並びに当該個人番号利用事務等を実施する権限を持つ職員の認証及びアクセス制御等の技術的措置が必要となる。（第３章第３節1-②）



ネットワークのアクセス制御について検討が必要

符号取得時の情報の流れ方について

決められた機器間のみの通信経路を確立しなければならない。
許可されていない機器からのアクセスを制限しなければならない。



複雑なネットワークのアクセス制御が必要

ネットワークのアクセス制御にあたり必要な検討事項

「地方公共団体における番号制度の導入ガイドライン」記載事項

- アクセスできる職員を明確に定義し、その権限の管理やアクセス制御等の設定を正確に行う
- アクセスに係るログ等を定期的にチェックし、不正アクセス等の事実がないことを確認する
- 人事異動等を考慮し、アクセス権設定の正確性を維持できるようにする

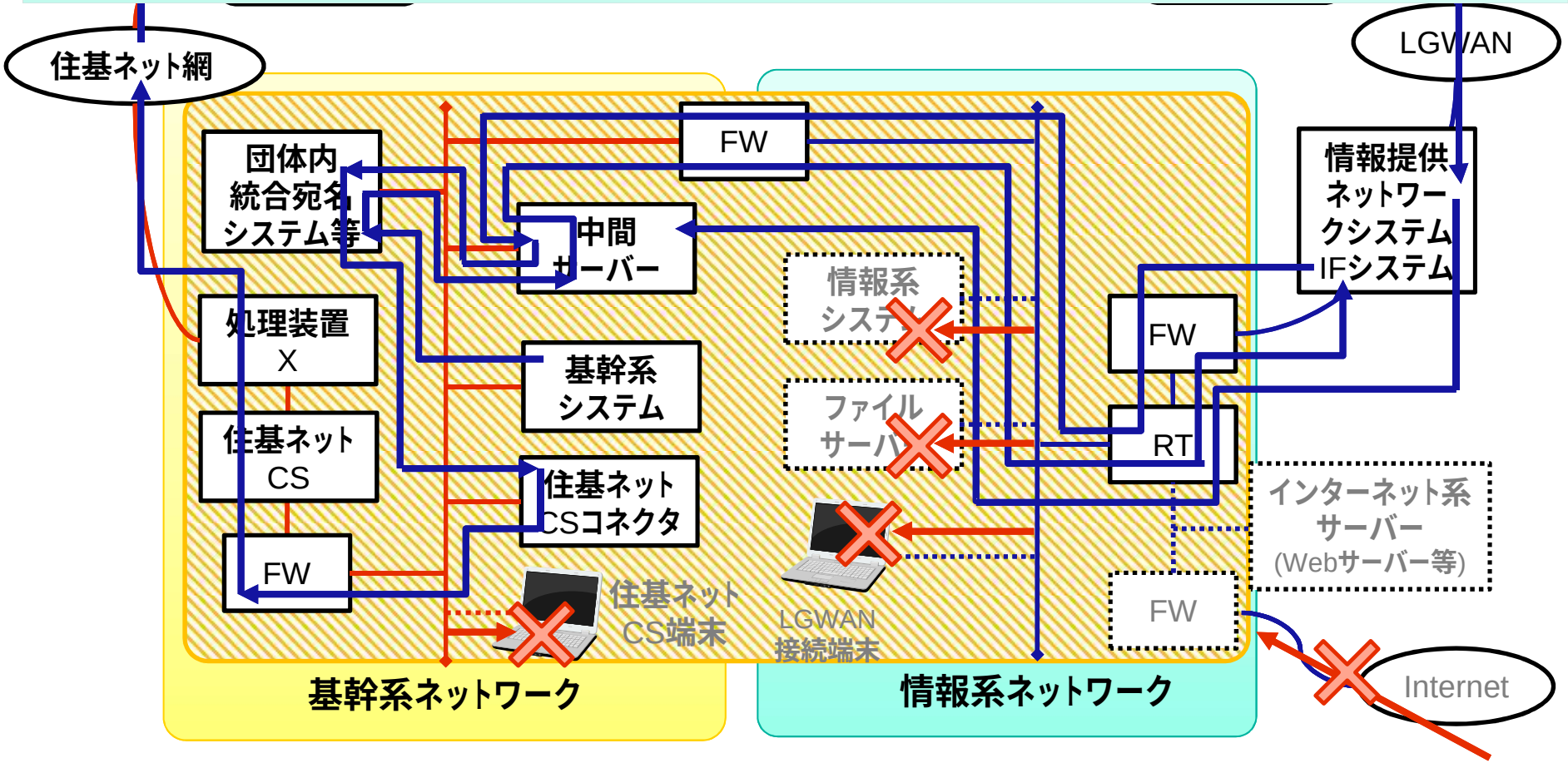
次世代ネットワークの技術を用いることで、アクセス制御をネットワークレベルで容易に実施することが可能。

次世代ネットワークと従来ネットワークとの比較

	次世代ネットワーク (SDN)	従来ネットワーク (VLAN)
アクセスできる職員を明確に定義し、その権限の管理やアクセス制御等の設定を正確に行う	閉域網を必要に応じて作成。経路を可視化し、アクセス状況を確認可能。	経路制御は可能。経路の確認はログ等から確認。
アクセスに係るログ等を定期的にチェックし、不正アクセス等の事実がないことを確認する	ネットワーク上の通信をリアルタイムに確認可能。	各機器のログを集計することで確認。もしくは専用の可視化ツールの導入が必要。
人事異動等を考慮し、アクセス権設定の正確性を維持できるようにする	人事情報と連携したアクセス制御が可能。	―

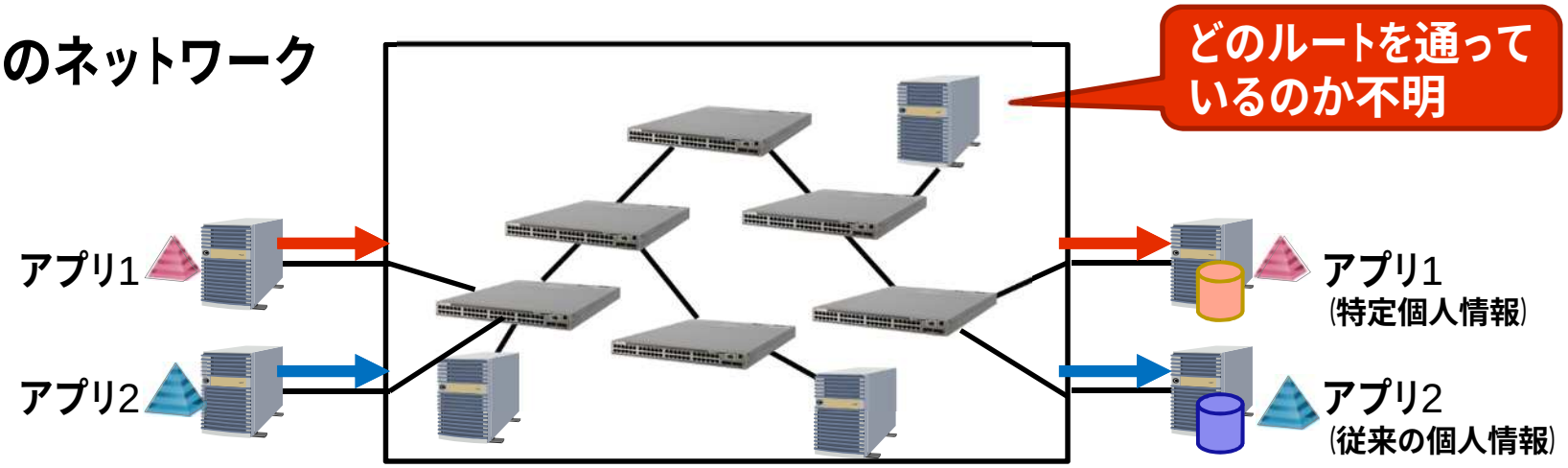
次世代ネットワーク技術によるアクセス制御

決められた機器以外は見えないネットワークが確立できます。
許可されていない機器からのアクセスを制限できます。

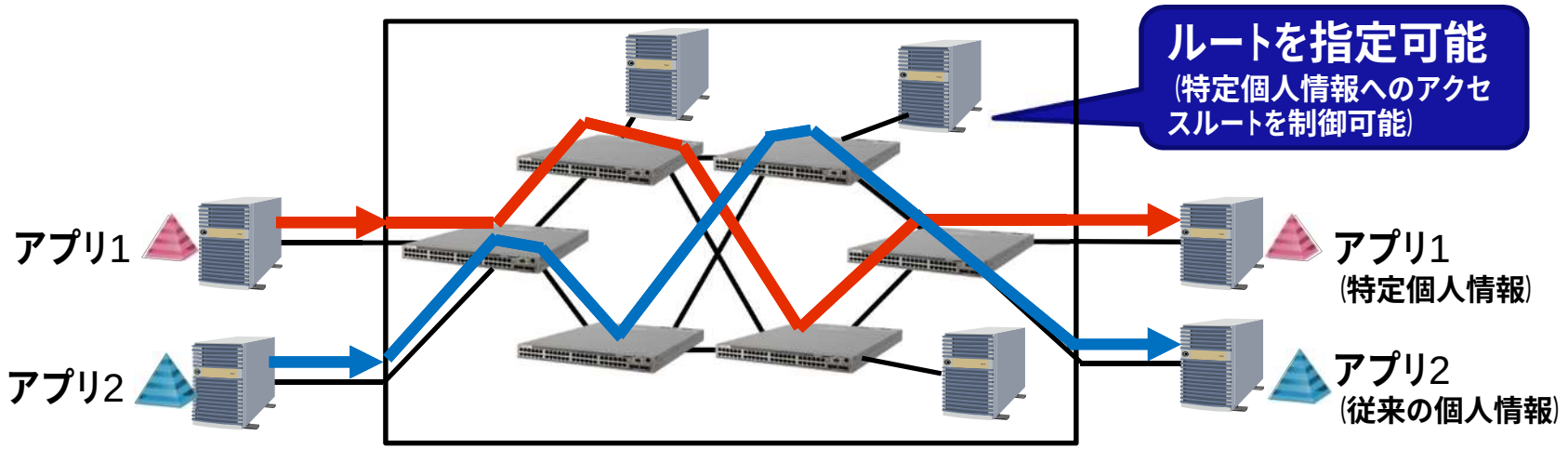


次世代ネットワーク技術（SDN）の活用

従来のネットワーク



次世代ネットワーク（SDN）



※SDNを採用したNECの次世代ネットワークソリューションが「ProgrammableFlow」です。

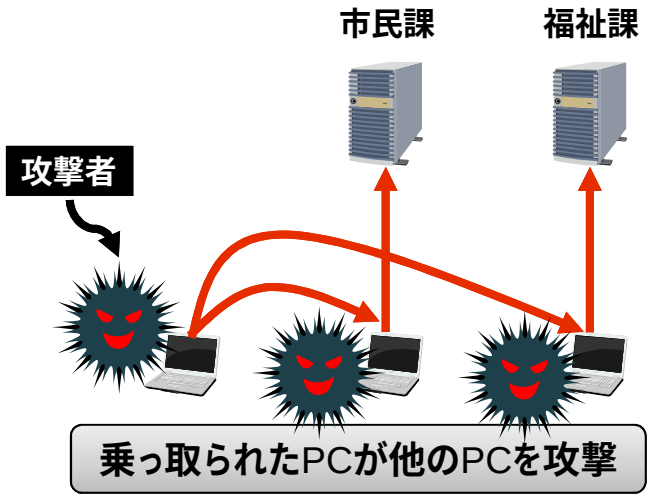
次世代ネットワーク技術の活用

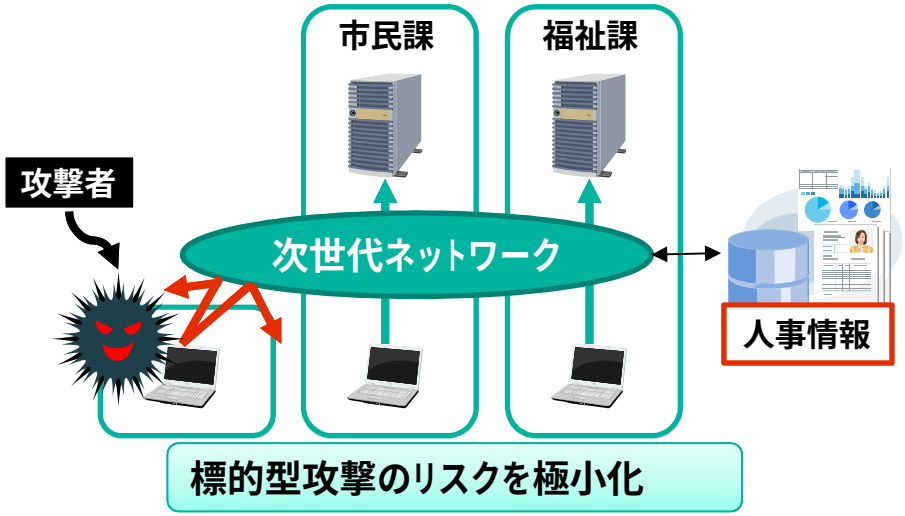
人事情報と連携したアクセス制御

- 人事情報を元にアクセス可能なサーバー・ネットワークを自動設定
- セキュリティ向上と運用コスト削減を実現

- 業務内容に基づいた情報管理の徹底が必要
- 人事異動時やオフィスレイアウト変更などに伴うネットワーク設定変更は煩雑。
- 巧妙化する標的型攻撃による情報漏えいリスクの増大。

- 人事情報と連動し、人事異動時のアクセス権変更漏れを防止
- 標的型攻撃や情報漏えいなどイントラネット内部のセキュリティリスクに対応
- 人事異動やオフィスレイアウト変更に伴う設定変更が不要



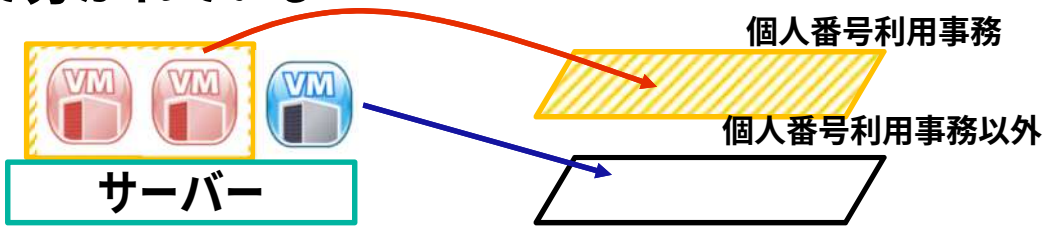


次世代ネットワーク技術の活用

個人番号利用事務と個人番号利用事務でない事務が混在するサーバーのアクセス制御

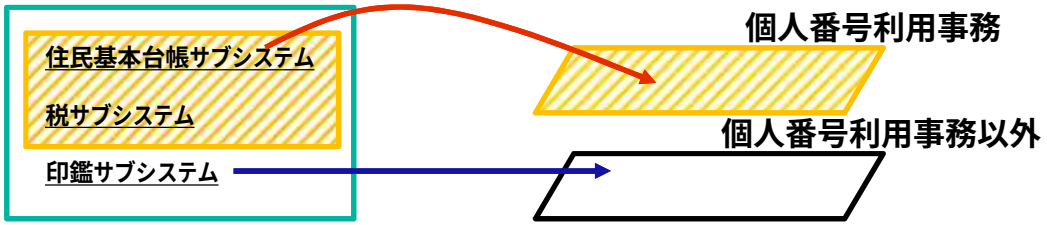
- 事務処理システムが仮想マシンで分かれている

  ⇒ 仮想マシンのIPアドレス毎にアクセス制御が可能



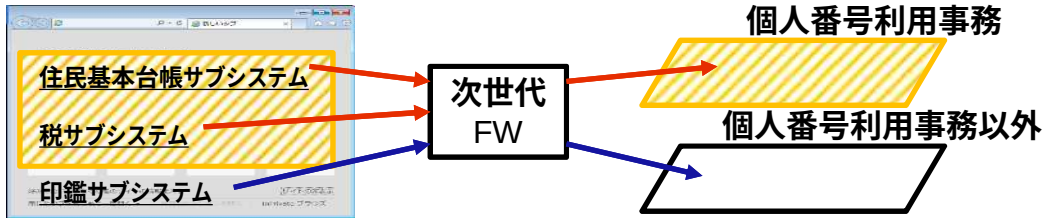
- 事務処理システムがC/Sシステム

  ⇒ アプリケーションのポート番号を分けることでアクセス制御が可能



- 事務処理システムがWebシステム

  ⇒ 次世代FWを導入することでアクセス制御が可能

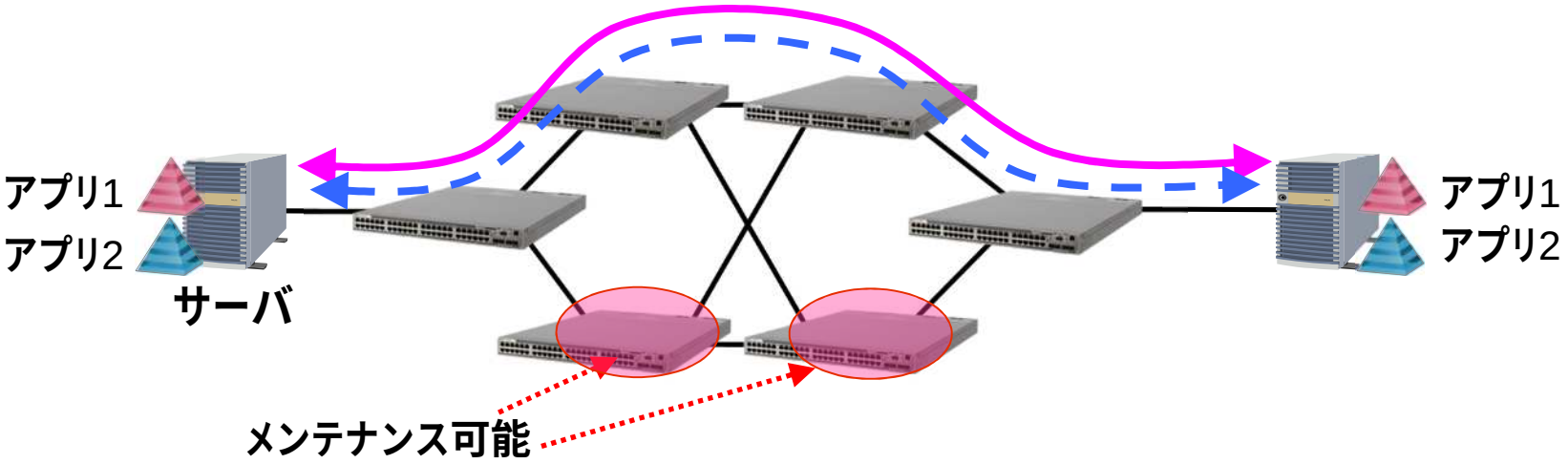


次世代ネットワーク技術の活用による副次的なメリット

情報提供／情報照会のための止まらないネットワークの構築が可能

- 開庁時間の延長や休日開庁などでメンテナンス時間が取れない
- 他自治体からの情報参照を考慮したメンテナンス計画が必要

ネットワーク機器のメンテナンスを平日業務時間内に実施することが可能。



セキュリティ見直しのための検討事項

番号制度によるセキュリティ強化の必要性について

- 番号制度により外部を含めた複数システムにまたがる情報流通が行われることとなります。
- 個人情報を保護するため、情報管理やセキュリティ対策の強化が重要となります。

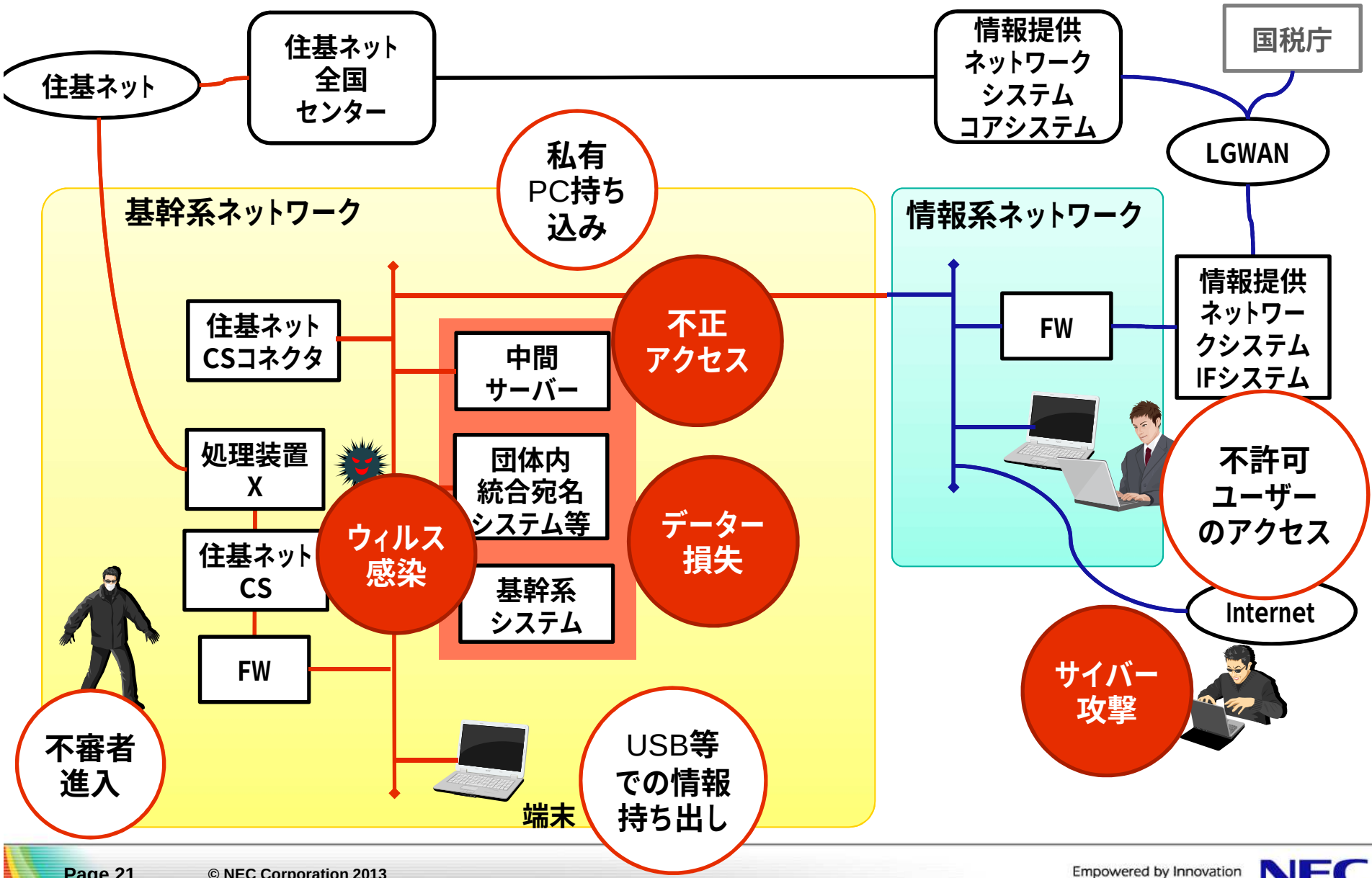
考えられる脅威

- 個人情報を盗み出すために、サイバー攻撃や標的型メール攻撃が増える。
- 個人情報を直接取り扱わない部署の脆弱性を踏み台に庁内への侵入が行われる。
- ソーシャルエンジニアリングによって、機微な情報を取得しようとする。

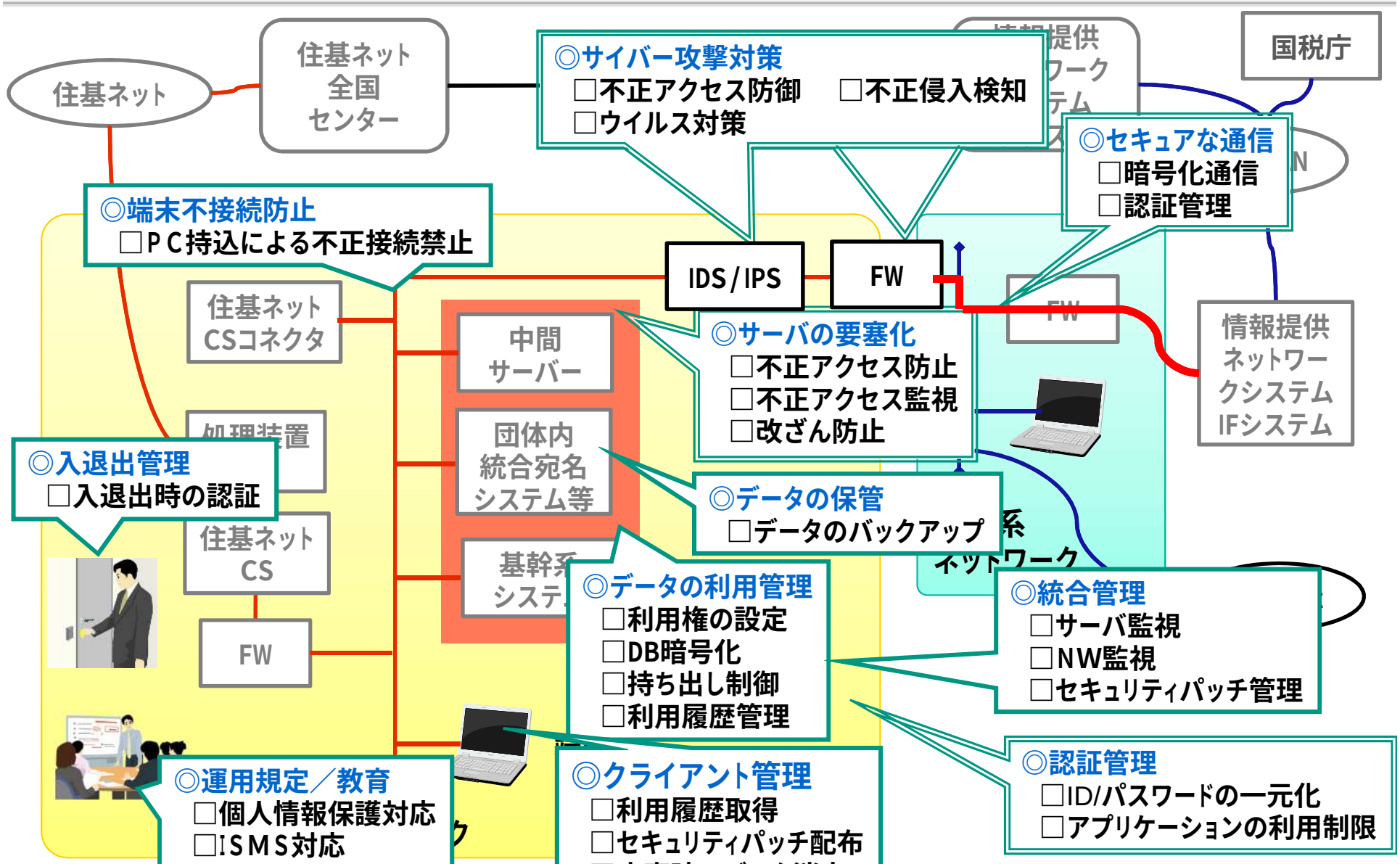
重点対策

- セキュリティパッチの適用やウィルス対策ソフトの適正利用などの、基本的なセキュリティ対策の徹底が必要。
- 巧妙化する攻撃の兆候を察知し、それを防ぐための多層防御対策が必要。
- 情報漏えいを未然に防ぐため、データーの暗号化やアクセスログの管理が必要。
- 継続的に全庁的な情報セキュリティの底上げが必要。

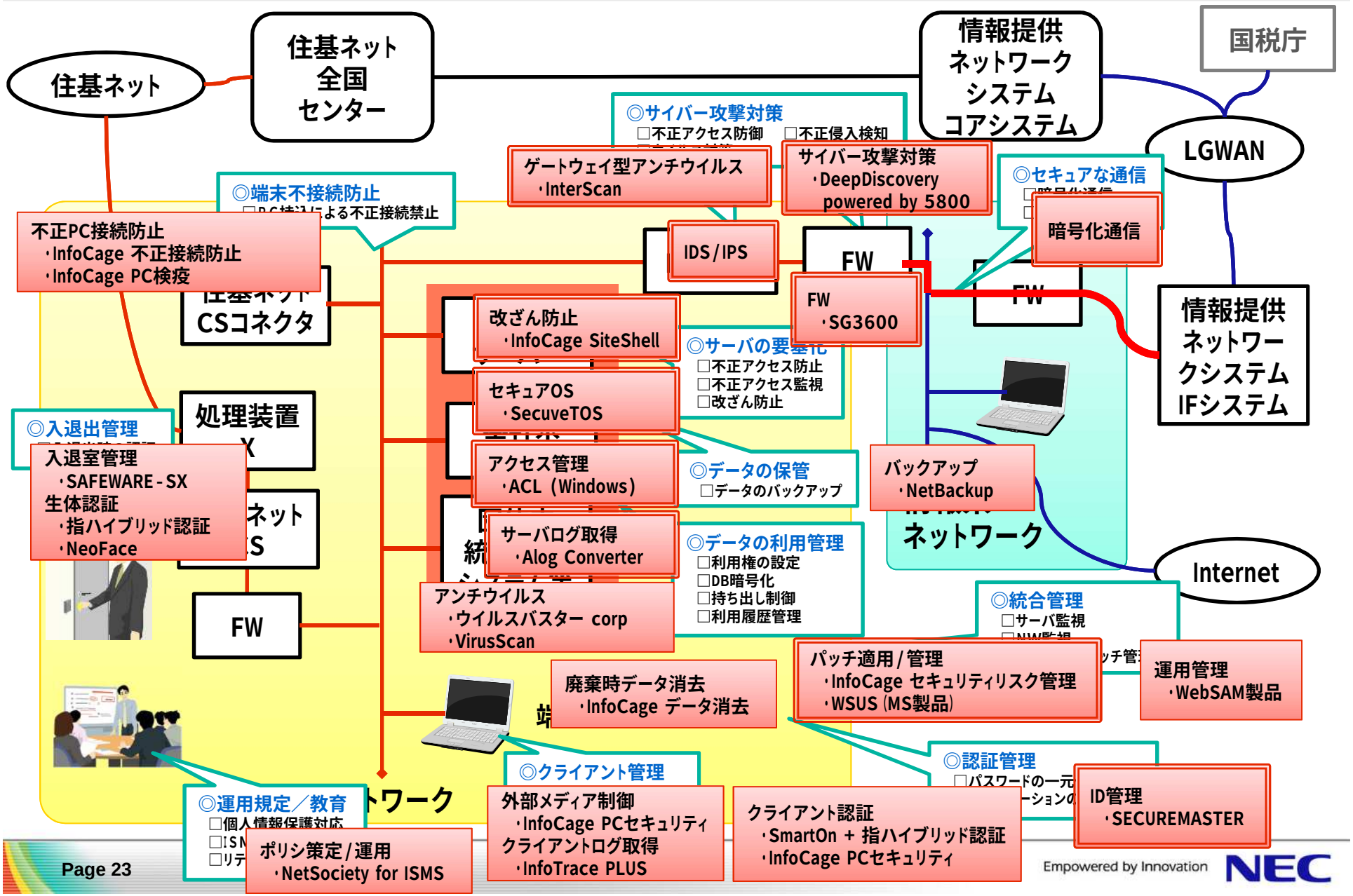
番号制度施行後に考えられる脅威



セキュリティ対策例



セキュリティ対策製品

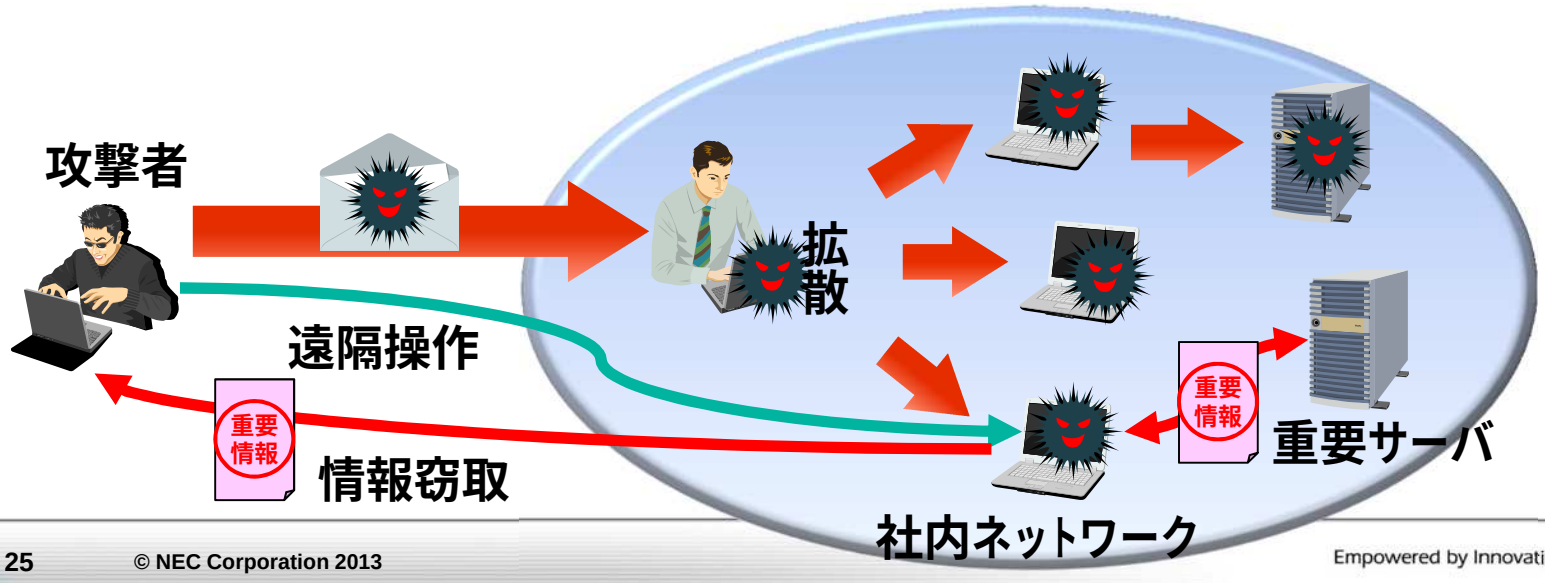


セキュリティ脅威とその対策

新たなサイバー攻撃「標的型攻撃」

新しいサイバー攻撃「標的型攻撃」とは？

- 近年話題となっている大手総合重機メーカーや公的機関へのサイバー攻撃に類する攻撃。
- ソーシャルネットワークを利用し、**送信者を巧みに詐称**して侵入。
- **情報窃取・システム破壊**を目的とし、**特定の人物・企業・業界**を攻撃。
- 攻撃の過程でマルウェア（不正プログラム）を利用。
  - 従来のパターンマッチング方式の対策（IPSや**アンチウイルスソフト**）**では検知が困難**。
- 攻撃者は、**外部からマルウェアの遠隔操作**を行い目的を達成。
- マルウェアを感染させるために、なりすましメールや改ざんしたWebを利用。



Deep Discovery powered by Express5800
標的型攻撃対策アプライアンス

プラットフォームセキュリティ
標的型攻撃対策

＜製品概要＞
標的型攻撃などで利用される新型ウイルスの感染端末を検知・可視化。エンジニアによる脅威分析・感染時復旧支援サービスもご提供。

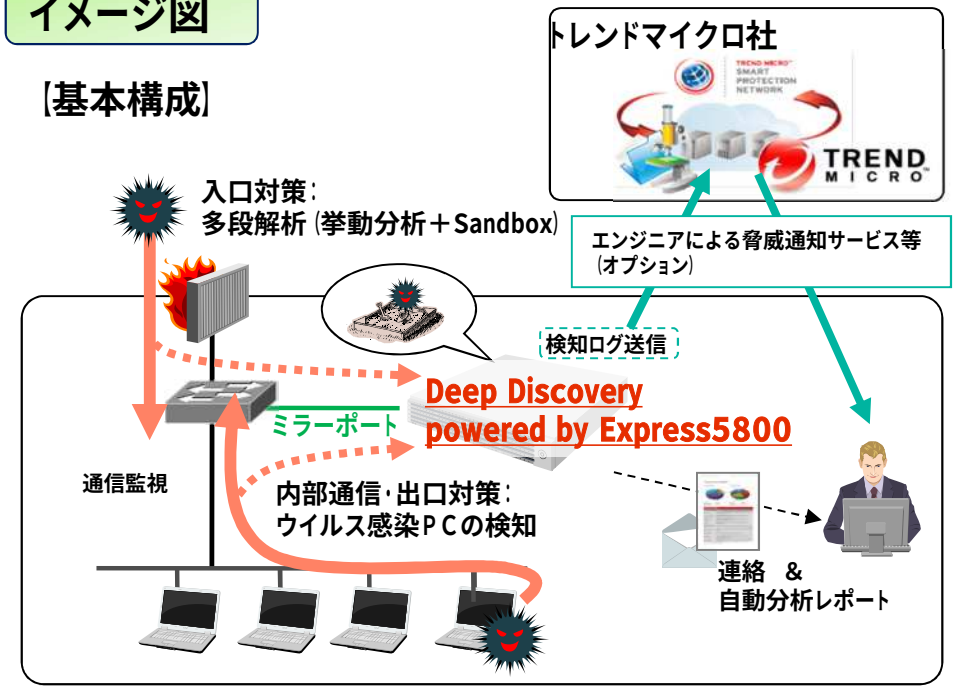
＜導入効果と機能＞
●新型ウイルスの検知（入口対策）
- 従来のパターンファイルだけでは検知できない新型ウイルスを複数のロジックによる挙動分析（静的解析）と、仮想環境（Sandbox）による動的解析の多段解析で検知。

●ウイルス感染PCを検知（内部通信・出口対策）
- ウイルスの特徴ある通信・挙動や接続先を分析することで、ウイルスに感染したPCを脅威として検知し、ネットワークの感染状況を管理者へ通知。

●脅威の可視化・分析レポート
- 通信をリアルタイムに分析、脅威として可視化し、日次・週次・月次で分析レポートを自動生成します。
- 脅威の詳細についてはローカライズされた脅威詳細Webコンソールで詳細分析が可能です。
- また、エンジニアによる脅威分析・感染時復旧支援等をご提供（オプション）。

●最新のV3.5をリリース
- Webコンソールのローカライズや監視プロトコルの指定や既知ファイルのSandbox解析の省略等チューニング性が向上。

イメージ図
【基本構成】



NEC優位性
- Express5800でアプライアンス化。トレンドマイクロ製（Dell筐体）に搭載した同製品と比べHW保守性、運用性が向上。
- NEC独自で、HWスペックと価格を抑えた「ミドルレンジ版（通常版）」や、内部通信・出口対策に特化し一部機能を省いた「NS版」をラインナップ。

動作環境：
アプライアンスであり、動作環境（HW/SW）は一括提供。

アクセス管理の課題

アクセス管理に要求される事項

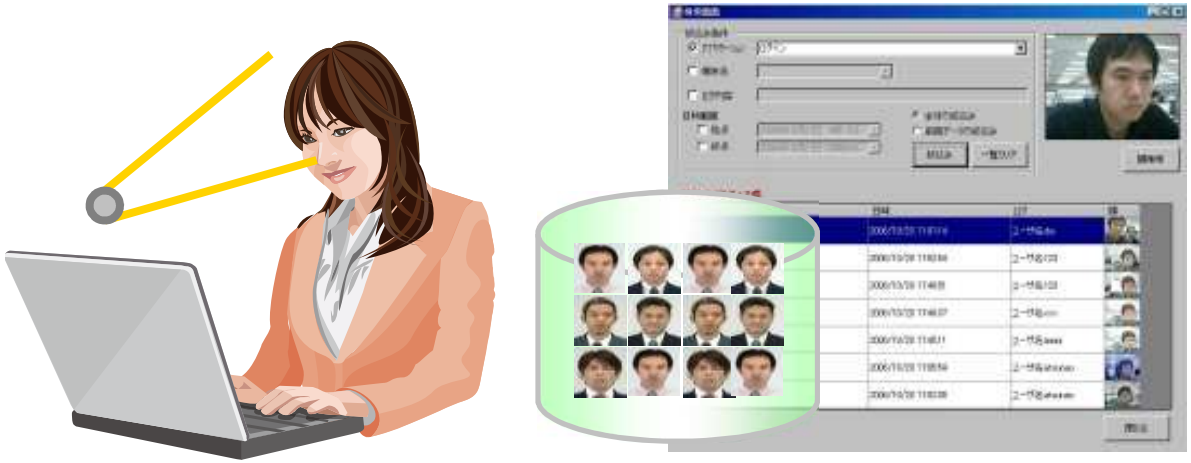
- 職員一人ひとりにIDを付与し、情報の機密性に応じたアクセス制限の実施が必要
- PC利用時には自身のIDで常にログオンすることが必要

遵守できない場合の問題点

- 問題が発生した際に、ログ情報から状況の把握が困難となる。
- 特定個人情報へのアクセスが認められているのかを情報へのアクセス時や監査時に確認できない。

顔認証によるアクセス管理ソリューション

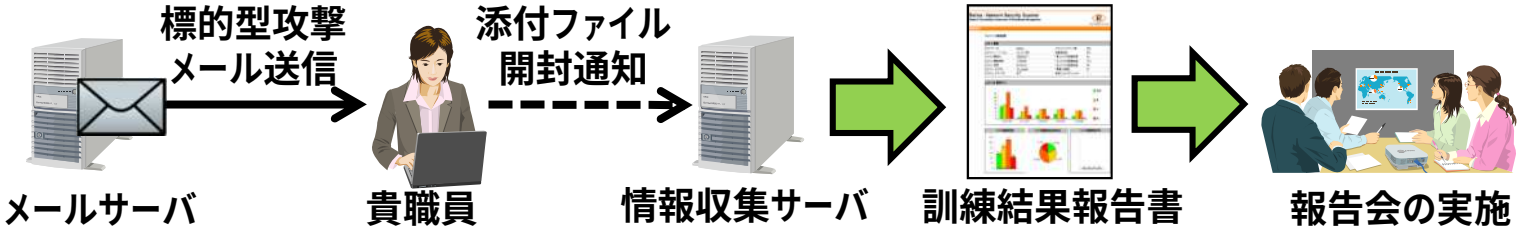
- 機密性の高い機微な情報を含む画面利用時に、Webカメラで利用者の顔認証を行うことで、機密性の高い情報の漏洩リスクを格段に軽減。
- 顔認証方式を用いることで、機密性にあわせたアクセス管理を自動認証にて実現。
- システム起動時のみの認証ではなく、システム利用中の継続的な認証が可能となり、大幅にセキュリティを向上。
- ＰＣの操作履歴を顔画像共にログ保存。不正利用を効果的に抑止。



情報セキュリティコンサルティングの一例

標的型攻撃メール対応訓練サービス

- 擬似的な標的型攻撃メールを各従業員のメールアドレスに送信し、添付ファイルの開封状況を報告します。
- 報告後に従業員に対して種明かしと注意喚起を行なっていただきます。



情報セキュリティ内部監査支援サービス

- 情報セキュリティポリシーに則って、情報セキュリティに係わる活動が行われているか監査します。
- 情報セキュリティポリシーと情報セキュリティ管理基準（経済産業省）などから個別管理基準を作成し、監査計画を立案します。
- 文書・記録の閲覧、インタビュー、現地調査（観察・再実施等）の監査技法を使用して監査を実施し、監査報告書を作成します。
- 監査の結果、不適合と判断された事項については具体的な助言を行います。

NECグループビジョン2017

人と地球にやさしい情報社会を
イノベーションで実現する
グローバルリーディングカンパニー

Empowered by Innovation