NECが考える無線LAN対策イメージ図

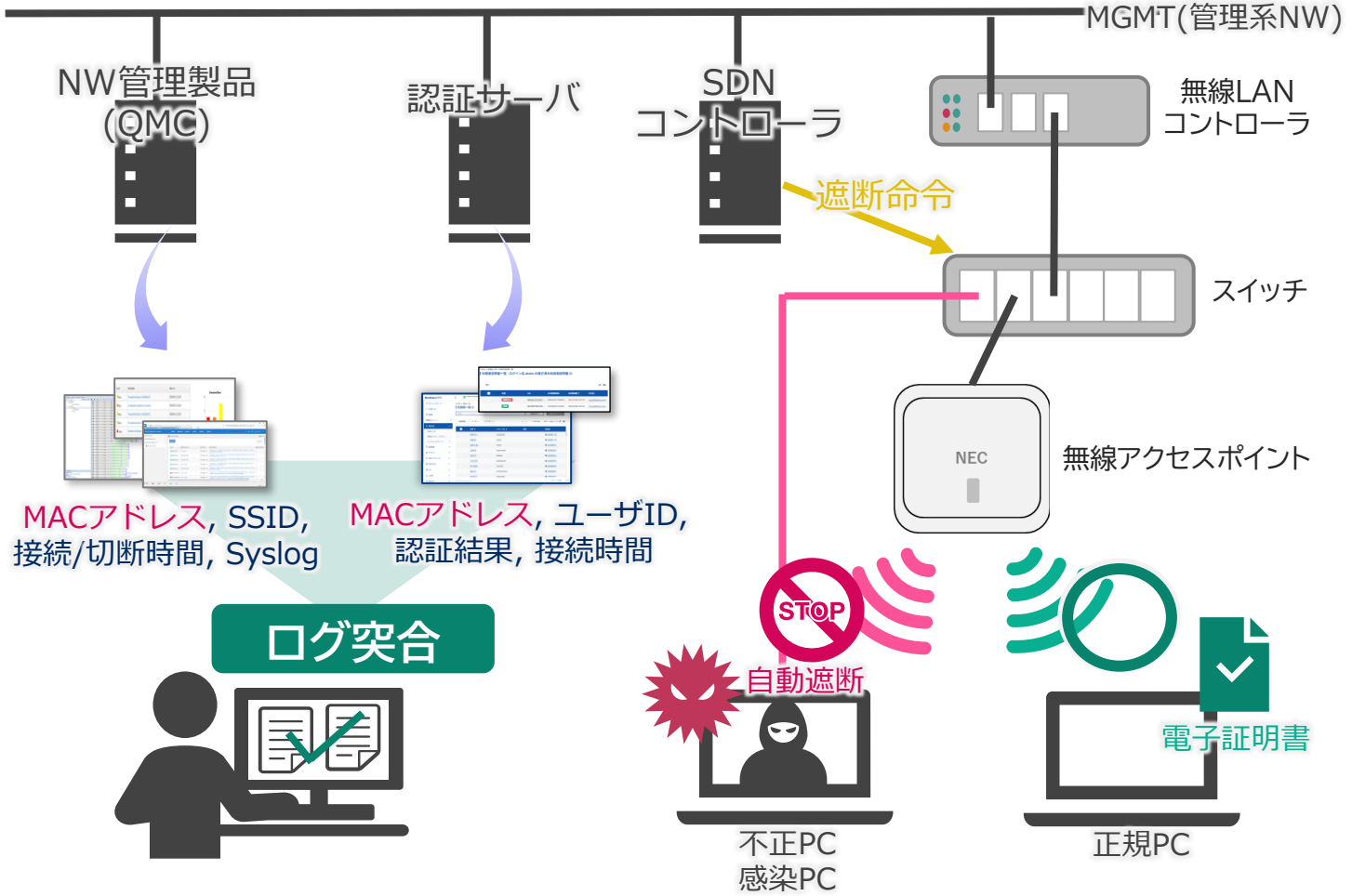
端末のアクセスログ
端末の認証・認可
WPA2またはWPA3
認証サーバのログ収集
ユーザ認証・認可
不正な挙動をする端末の自動遮断

端末だけでなくユーザ認証を行い、マイナンバー利用事務系利用者を識別して管理
暗号化だけでなく、感染PCの自動遮断により、インシデント対応を強化

NECが考える対策

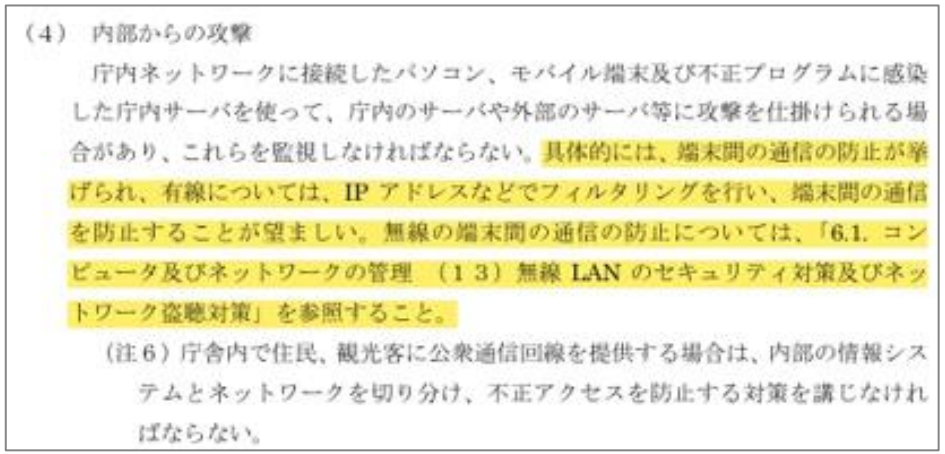
・上記に加え、認証サーバのログを確認
⇒QMCと認証サーバのMACアドレスを突合し、誰か（ユーザID）を識別

・有線/無線：自動遮断
⇒インシデント初動対応の自動化により、二次感染被害を最小化。
管理者不在の時間帯も対応できて安全。



マイナンバー利用事務系における無線LAN対策ポイント

BluStellar



（4） 内部からの攻撃

庁内ネットワークに接続したパソコン、モバイル端末及び不正プログラムに感染した庁内サーバを使って、庁内のサーバや外部のサーバ等に攻撃を仕掛けられる場合があり、これらを監視しなければならない。具体的には、端末間の通信の防止が挙げられ、有線については、IP アドレスなどでフィルタリングを行い、端末間の通信を防止することが望ましい。無線の端末間の通信の防止については、「6.1. コンピュータ及びネットワークの管理 （13）無線 LAN のセキュリティ対策及びネットワーク盗聴対策」を参照すること。

（注6）庁舎内で住民、観光客に公衆通信回線を提供する場合は、内部の情報システムとネットワークを切り分け、不正アクセスを防止する対策を講じなければならない。

地方公共団体における情報セキュリティポリシーに関するガイドライン3月改定版
https://www.soumu.go.jp/main content/001001336.pdf

P253に添付pngのハイライト部分の追加がありました。

➢ ガイドライン（NW）に記載の対策

あくまで対策例であり、どこまで対策を実施するか自治体様との協議が必要です

対策項目	推奨対策例
端末のアクセスログ	QX Management Center
端末認証・認可	NetAttest EPS ap（RADIUS認証サーバ）
WPA2またはWPA3	QX-Wシリーズ（アクセスポイント）
アップデート	運用にて対応

➢ NECが考える追加の対策

運用項目	推奨対策例
認証サーバのログ収集	NetAttest EPS ap（RADIUS認証サーバ）
ユーザ認証・認可	
不正な挙動をする端末の自動遮断	Network Operation Engine
GUIによるNW管理（無線含む）	NEC 無線可視化ソリューション
アップデート（集中管理）	QX Management Center＆QX-Wシリーズ