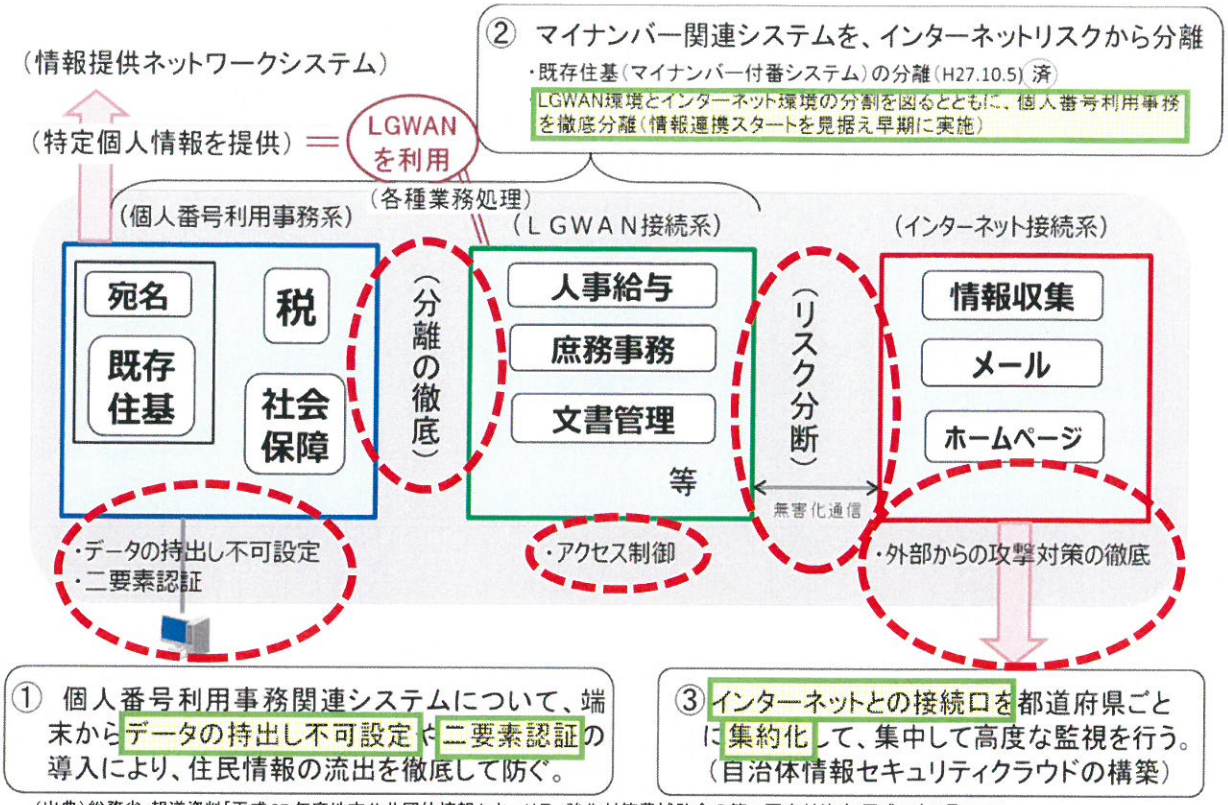
①自治体情報セキュリティ強化対策事業：
無害化と分離・リスク分断で感染前提のいたちごっこに決別

資料3



（出典）総務省・報道資料「平成27年度地方公共団体情報セキュリティ強化対策費補助金の第１回交付決定(平成28年3月8日)」
（出典）日経コンピュータ「特集:無害化と分離-標的型攻撃の防ぎ方-」(2016年2月4日号)
（出典）日経新聞夕刊「マイナンバー安全対策『万全』自治体2割 準備不足浮き彫りに」(2016年2月4日)

②重要インフラへのサイバー攻撃：制御システムへの脅威と脆弱性

発生年	名称	概要
2000	上下水処理場への不正アクセス	豪Maroochy市の上下水処理場のシステムに元従業員が不正アクセスを行い、システムを誤動作させることで、汚水が公園や河川に流れ出した。
2003	原発監視制御システムのマルウェア感染	米Davis-Besse原子力発電所の監視制御システムにマルウェア（SQL Slammer）が感染、一部システムが数時間にわたって停止した。
2006	交通信号制御システムへの不正アクセス	米Los Angels市の交通監視センターの信号制御システムに対して元職員が不正アクセスを行い、交通信号を止めたことで、渋滞が発生した。
2008	クレジット決済会社への不正アクセス	英The Royal Bank of Scotland傘下のクレジット決済会社のコンピュータに東欧の犯罪者集団が不正アクセスしクレジットカードデータを窃取。日本を含む世界各国のATM2,100台から約8億円を盗んだ。
2010	Stuxnetによるイラン核施設へのサイバー攻撃	マルウェア（Stuxnet）を用いたイランの核施設を標的とした攻撃。施設の遠心分離機が稼働不能に陥ったとされる。
2013	韓国の銀行や放送局へのサイバー攻撃	韓国の銀行や放送局を狙ったサイバー攻撃により、ATMやインターネットバンキングが停止する等の影響があった。

普段は存在しない経路がつながる時…

USBメモリ
- USBメモリからのウイルス感染事例は頻繁に発生しています
- しかしながら、USBポートは運用上なくすことは不可能なことが多く、メンテナンス上も不可欠です

操作端末の入れ替え/保守用端末の管理
- 操作端末は、汎用パソコンであることが一般的であり、入れ替え時にウイルス感染していた端末から被害が発生しています
- システムに接続する保守用端末が原因となるケースもあります

被害事例の原因の多くは、こういった基本的な部分にあります。

リモートメンテナンス回線
- リモートメンテナンス回線の先の端末からの不正アクセス・ウイルス混入が発生しています

内部犯行・工業用無線LAN等
- 内部犯行者は物理セキュリティはすり抜けます
- 工業用無線LANからの侵入事例もあります
- PCのIDやパスワードの共通化、メモ書きの貼り付けなどは、悪用されやすい、危険な運用です

脅威は外部からだけでなく…

（出典）国会図書館『情報通信技術の進展とサイバーセキュリティ』
http://dl.ndl.go.jp/view/download/digidepo_9111024_po_20140300.pdf?contentNo=1)
（出典）独立行政法人情報処理推進機構『重大な経営課題となる制御システムのセキュリティ』https://www.ipa.go.jp/files/000044733.pdf