連 載

官の情報システム研究部会報告（23）
第 23 回：マイナンバー制度及びセキュリティ強靭化対策が及ぼす自治体情報システムの影響について

吉田博一（よしだ　ひろかず）
大阪府立大学

本稿は，筆者の個人的見解であり，筆者が所属し，あるいは，関係する団体の見解とは無関係である．

1．はじめに

マイナンバー制度は申請手続き時の添付書類の省略やプッシュ型サービス等により住民の利便性の向上が期待されるとともに，地方自治体のシステムの仕組みを大きく変える可能性がある．

これまで自治体の情報システムは，個人情報保護等の観点から，個別の業務ごとに導入されてきた．同一自治体内の業務間のシステム連携を進めた事例はあるが，他の自治体との連携はなかった．

マイナンバー制度の運用に伴う情報連携では，個人番号に紐づく特定個人情報を保有する基幹系システムは他の自治体と情報提供や照会を行うためLGWAN 上に設置する中間サーバと接続する．そして，中間サーバを介して特定個人情報の情報提供や情報照会を行い，全国の地方自治体等とシステム間の連携ができるようになる．

ところが，2015 年 5 月に発生した日本年金機構における個人情報流出事案を受け，地方自治体における情報セキュリティに係る抜本的な対策を検討するため，学識経験者や国・地方自治体関係者からなる「自治体情報セキュリティ対策検討チーム」が設置され，「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」という報告書をまとめた．その中で地方自治体内のネットワークを，個人番号利用事務系と LGWAN 接続系とインターネット接続系の 3 層に分離することを求めた（総務省，2015a）．

この対策により，情報の漏洩を防ぐと共に，外部からの攻撃を防御する仕組みが構築される．その一方で，利用できる ASP サービスが制限され，ファイル転送等の操作が不可能になり利用できなくなった．

このような状況を踏まえ，自治体情報システムの現状と展望について論ずる．

2．マイナンバー制度における情報システム

2.1　マイナンバー制度の概要

マイナンバー制度は，複数の機関に存在する個人の情報が同一人の情報であるということの確認を行うための基盤で，社会保障・税制度の効率性・透明性を高め，国民にとって利便性の高い公平・公正な社会を実現するための社会基盤である（総務省，2014）．この制度により，複数の機関間において，同一人の情報を紐付けし，相互に活用する「情報連携」が可能となる．

地方自治体では，これらの仕組みを実現するために，図 1 の 4 つのシステム整備を行っている．

2.2　住基ネットと LGWAN との接続

これまで，住民基本台帳ネットワーク（以下，「住基ネット」と言う）に接続される住民登録等の基幹系システムは，LGWAN と接続せずに運用する団体が多かった．

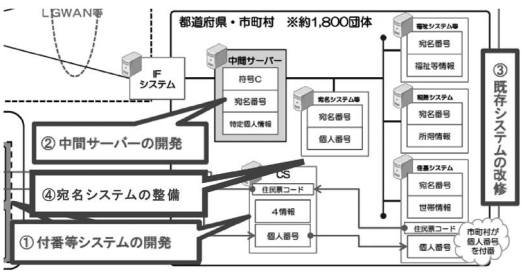

図 1　地方自治体で必要なシステム整備（（総務省，2014）加筆）

しかし，マイナンバー制度の運用に伴い，住基ネット上の基幹系システムは，個人番号に紐づく特定個人情報を提供・照会するため，LGWAN 上に設置する中間サーバと接続され，今後は，特定個人情報の情報提供や情報照会が行われるようになる．これをシステムアーキテクチャとしてまとめたのが，次の図 2 である．

このマイナンバー制度の情報連携の仕組みを他の分野に応用することで，さまざまな自治体内や他自治体間等の情報連携が可能になると思われる．

2.3　統合宛名システムによる情報連携機能

他の団体と情報連携を図るのが統合宛名システムとなる．この統合宛名システムの機能は次のとおりである（総務省，2013）．

（1）宛名番号機能

新規に団体内統合宛名番号を付番する機能など．

（2）宛名番号付番機能

宛名情報を団体内統合宛名番号，個人番号と紐付けて保存し管理する．

（3）中間サーバ連携機能

中間サーバ又は中間端末からの要求に基づき団体内統合宛名番号に紐付く宛名情報等を通知する．

（4）既存システム連携機能

既存業務システムからの要求に基づき個人番号又は団体内統合宛名番号に紐付く宛名情報を通知する．

これらの機能を実現するために，統合宛名システムは，住基ネットや中間サーバ及び既存システムの間で付番や情報照会要求及び副本登録等を行い，サービスの連携を行う．

2.4　ESB の機能

SOA（Service Oriented Architecture）において，システム同士を疎結合させる ESB（Enterprise Service Bus: 異なる形式のサービスを用いる複数のアプリケーションを間接的に接続するための基盤）が存在する．

宗平（2014）は，EC システムについて「システム間連携に ESB を採用することにより，現在 API 連携で N 対 N となっている各モールとの連携について，各々が 1 対 1 対応で済み，お互いの仕様変更からの独立度を高める」アーキテクチャを提案した．

このアーキテクチャを応用し，統合宛名システムの仕組みをマイナンバー関連業務に限らず，自治体内の全システムと ESB を介して連携することで次のことが可能になる．基幹系パッケージやバックオフィス業務をカスタマイズなしのまま，独自業務部分についてはユーザ側で改変可能な独自なサービスとして独立させるシステム間連携が考えられる．これにより，法令改正等はパッケージ側でベンダーが対応したものを利用し，独自業務はユーザ側で自由に設定することができるようになる．また，この仕組みを複数の自治体が共同でクラウドサービスを使うことで，複数のパッケージシステムを利用した大規模自治体でも活用できる自治体クラウドが可能となると考えられる．図 3 に吉田（2016）によるシステムアーキテクチャによる応用例を示す．

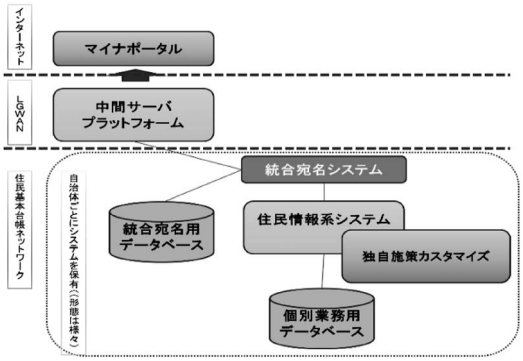

図 2　マイナンバー制度導入時の地方自治体の情報システムアーキテクチャ（吉田，2016）

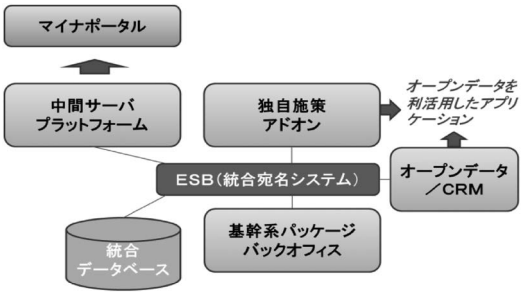

図 3　自治体情報システムアーキテクチャ（吉田，2016）

3. セキュリティ強靭化対策とその影響

3.1 三層の構えのセキュリティ強靭化対策

「はじめに」で述べたように，地方自治体における情報セキュリティに係る抜本的な対策を検討するために設置された「自治体情報セキュリティ対策検討チーム」が，2015年にまとめた報告が，「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」であった（総務省，2015a）．

これを受けて総務省が全国の地方自治体に示した対策が，図4のとおりとなる．

図4のように保有する個人情報が外部に漏れず外部からの攻撃を防御する仕組みが2017年4月までにほとんどの自治体で構築されることになる．

3.2 強靭化対策のネットワークごとの影響

この対策を徹底するため，総務省は2015年度に自治体情報セキュリティ強化対策事業255.0億円を予算措置した．内容は次の3つである（総務省，2015b）．

（1）個人番号利用事務系

端末からのデータ持出し設定不可や二要素認証を導入する．

他のネットワークと通信経路を徹底分離する．ただし，中間サーバやコンビニ交付用サーバ，クラウドセンターといったLGWAN経由での接続が必要となる場合等は，十分にセキュリティが確保された特定通信先と限定的な接続を可能とする．

OSアップデートやウィルス対策ソフトのパターンファイルの更新等においてもインターネットと接続できない．

（2）LGWAN接続系

インターネット接続系の通信回線と分割し，LGWANメールやLGWAN-ASP等の特定通信と限定的に接続する．

直接インターネットと接続できない．ただし，インターネットへのメール発信とインターネット接続系にてHTMLメールのテキスト化や添付ファイルの削除が行われた受信メールの取込み等無害化された通信のみインターネット接続は可．

（3）インターネット接続系

インターネットとの接続口を都道府県ごとに集約化して，集中して高度な監視を行う（自治体情報セキュリティクラウドの導入）．

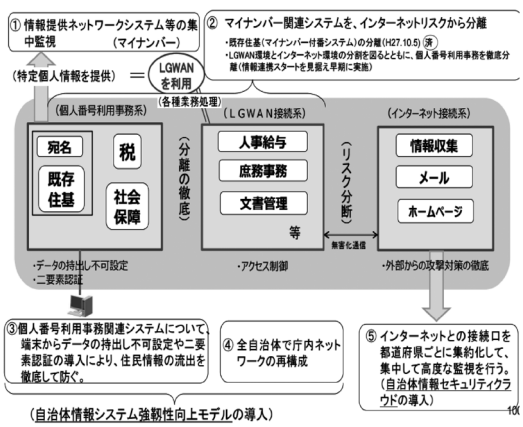

図4 自治体情報セキュリティに係る攻撃リスク等低減のための抜本的対策の概要（総務省，2017）

3.3 強靭化対策の影響に対する業務上の対応

ネットワークごとに対策がとられることになるが，業務的に住民対象の業務も財務関係等の内部事務も一人の人が行うことが大半であり，次のような対応の検討が進んでいる（吉田，2017）．

（1）複数ネットワークへの端末配備

個人番号利用事務系とLGWAN系，インターネット接続系の3つに分離する．これにより，一人の人間が3つの業務を行う場合，3台の端末を各々の回線に接続して設置することになる．

実際このように設置している団体もあるが，費用やスペース的に難しく，おおむね次のような対策を講じている．

1-1 インターネット接続端末を業務上必要な箇所にのみ配置する．

（課題）Web閲覧が行いにくい．常時見ているわけではないので，インターネットメールが届いてもすぐに確認できない．

1-2 VDI（Virtual Desktop Infrastructure）やSBC（Server Based Computing）方式といったデスクトップ仮想化技術を用い，LGWAN系とインターネット接続系の端末を物理的に1台の端末でネットワーク接続を切り替えて利用する．

（課題）端末設置スペースは減るが，ライセンス

料が必要となる．

(2) ソフトウェアのアップデート

従来，インターネット経由で無償入手していたソフトウェアの更新プログラムが，ネットワークから分離された個人番号利用事務系やLGWAN接続系では利用できない．

2-1 LGWAN-ASPによりベンダーが提供するソフトウェアアップデートサービスを利用する．

（課題）従来無償で利用したのが，有償となる．

2-2 アップデートプログラムをダウンロードした媒体を用いてサーバや端末ごとに個別で適用する．

（課題）アップデートごとに個別作業が必要となる．

2-3 情報ハイウェイでLGWANも収容している場合はアップデートプログラムの配信サーバを構築する．

（課題）配信サーバの構築費が必要で，情報ハイウェイがない都道府県もある．

2-4 平成29年度総務省予算要求案に盛り込まれているマイナンバー利用事務系やLGWAN接続系の端末へのアップデートファイルの提供を利用する．

（課題）総務省の2017年度の事業となり，内容については現段階では不明．

(3) ネットワーク間でのメールやファイルの受け渡し

LGWAN系とインターネット接続系が分離されているため，インターネットメールの添付ファイルを直接LGWAN系で受信することができず，ネットワーク間でのファイルのやり取りができない．

3-1 メール内容を画像又はテキスト化して転送し閲覧する．データのダウンロードは行わない．

（課題）添付ファイルが全く利用できない．メール本文中のURLがハイパーリンクされない．

3-2 メールの添付ファイルや電子申請・媒体持込ファイルからマクロやスクリプト等危険因子を除去するセキュリティクラウドやLGWAN-ASP，ファイル交換サーバにおける無害化ツールを利用する．

（課題）無害化前後のファイルの同一性が確保できない．費用がかかる．全種類のファイルには対応していない．

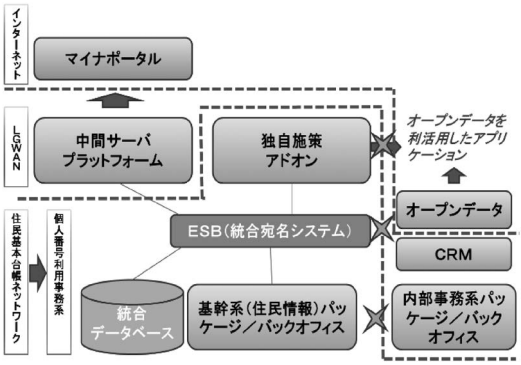

図5 強靭化対策を単純に実施した場合の地方自治体の情報システムのアーキテクチャ（吉田，2016）

3-3 ウィルス対策ソフトやサンドボックス等によりウィルスチェックを行ったものを媒体により受け渡しする．

（課題）媒体へのファイル格納や媒体の持ち運び・媒体からファイルへの落とし込みの手間がかかる．個人番号利用事務端末はデータの持出し不可設定を行っており，原則媒体の利用はできない．

3.4 セキュリティ強靭化対策による情報連携の影響

2.4節で述べたESBを応用した情報連携については，これらのセキュリティ強靭化対策により，ネットワークを超えての端末の利用制限やネットワーク間でのシステム連携ができなくなり，図5のようにESBを介して複数のネットワークでシステム間連携を行うことが困難となった．

4. おわりに

セキュリティ強靭化対策後もネットワーク間の特定通信を許可することによりESBの応用が可能と考える．実現すると大規模自治体も含めたASPサービス利用型の自治体クラウドやオープンガバメント／オープンデータ導入の促進が期待できる．

参考文献

総務省（2013）「地方公共団体における番号制度の導入ガイドライン平成25年8月」．

総務省（2014）「マイナンバー制度について」，個人番号を活用した今後の行政サービスのあり方に関する研究会（第 1 回）資料 2, http://www.soumu.go.jp/main_content/000314021.pdf（2017 年 4 月 4 日）
総務省（2015a）「自治体情報セキュリティ対策検討チーム」http://www.soumu.go.jp/main_sosiki/kenkyu/jichitaijyouhou_security/（2017 年 4 月 4 日）
総務省（2015b）「平成 27 年度総務省所管　補正予算（案）の 概 要」http://www.soumu.go.jp/main_content/000391075.pdf（2017 年 4 月 4 日）
総務省（2017）「地域の元気創造プラットフォーム，地域経済好循環推進プロジェクト，地域経済好循環拡大推進会議（全国連絡会）の開催，3. 地方公共団体の情報セキュリティ，自治体クラウドについて」https://www.chiikinogennki.soumu.go.jp/chiiki/files/koujyunnkann160226-03.pdf（2017 年 4 月 4 日）
宗平順己（2014）「EC システムの成熟度とアーキテクチャ」，経営情報学会 2014 年秋季全国研究発表大会
吉田博一（2016）「マイナンバー制度及びセキュリティ強靭化対策後における自治体情報システムアーキテクチャについて」経営情報学会 2016 年秋季全国研究発表大会
吉田博一（2017）「マイナンバー制度及びセキュリティ強靭化対策が及ぼす自治体情報システムの展望について」経営情報学会 2017 年春季全国研究発表大会

略歴

吉田博一（よしだ　ひろかず）

1983 年京都大学大学院工学研究科数理工学専攻修士課程修了，2010 年摂南大学大学院経営情報学研究科博士後期課程修了，博士（経営情報学）．

1983 年大阪府入庁以降．庶務事務・病院・土木・インターネット・電子調達・図書館・防災・税務等大規模情報システムの開発・再構築，マイナンバー・自治体クラウド・セキュリティクラウド関係のシステム整備・市町村との調整業務に携わる．

一時期，摂南大学経営学部非常勤講師も勤める．

現在は大阪府立大学新法人設立準備室システム担当課長代理．