

自治体情報システム強靱性向上モデル 適用後の運用効率化対策

Improvement of Operational Efficiency After Enhancement of Resilience of Municipal Information System

● 千原章義 ● 千葉祐太郎 ● 野中謙佑

あらまし

総務省は、2016年1月の社会保障・税番号制度(マイナンバー制度)の稼働を見据え、インターネット上のセキュリティを強化する目的で「自治体情報システム強靱性向上モデル」の適用を各自治体に指示した。従来、自治体では情報系ネットワーク、基幹系ネットワークの二つのネットワークで業務運用が行われてきたが、自治体情報システム強靱性向上モデルの適用により情報系ネットワークがLGWAN(Local Government Wide Area Network: 総合行政ネットワーク)系とインターネット系に分離され、従来の基幹系ネットワーク(個人番号利用事務系に改称)と合わせて三つのネットワークで運用されることになった。その結果、運用の煩雑化・負荷増が顕著になってきている。

本稿では、こうしたネットワークの分離に対し、利便性を確保しながら自治体情報システム強靱性向上モデルを適用するためのポイントと、適用後に発生する運用負荷軽減の実現に向けた対策について解説する。

Abstract

In consideration of the start of operation of the Social Security and Tax Number System (My Number System) in January 2016, the Ministry of Internal Affairs and Communications announced that it would instruct the application of the “model for enhancing the resilience of municipal information systems” for the purpose of strengthening security on the Internet. Originally, municipalities have used two networks—information system and mission-critical system networks—for carrying out operations. By applying the model for enhancing the resilience of municipality information systems, the information system network has been separated into the Local Government Wide Area Network (LGWAN) and Internet system network, resulting in three networks used for operation. As a result, increased cumbersomeness and load of operation have become conspicuous. This paper describes points in dealing with the separation of networks by applying the model for enhancing the resilience of municipal information systems while ensuring convenience, and measures for reducing the operational load generated after the application.

ま え が き

2015年5月に日本年金機構の情報漏えい事案⁽¹⁾が発生し、社会保障・税番号制度（マイナンバー制度）の本稼働を控えていたこともあり、国民に不安が広がった。これを契機として、総務省からセキュリティ強化を狙いとした「三層の構え」に則った自治体情報システム強靱性向上モデル（以下、強靱性向上モデル）⁽²⁾適用が各自治体に指示⁽³⁾された。この三層の構えの主な要求事項は、インターネット上の脅威から国民の個人情報を守るために、庁内ネットワークを個人番号利用事務系、LGWAN（Local Government Wide Area Network：総合行政ネットワーク）系、インターネット系の三つに分離することである。また、個人番号利用事務系とLGWAN系との間の特定通信化、可搬媒体運用管理強化も求められた。

この発表が行われた時点では、一般的に庁内ネットワークは情報系・基幹系の二つで構成されており、強靱性向上モデルの適用により情報系ネットワークがインターネット系とLGWAN系に分離される。このため、各種サービスも分離されることになり、利便性低下対策という課題が発生した。

更に、総務省からの強靱性向上モデル適用指示の対処完了時期がマイナンバー制度の稼働を見据えて設定されたことで、短期間での対処完了を求められた。このため、各業務システムの運用方式が十分に検討されないままネットワークが分離されてしまい、新たな運用上の課題が発生した。

本稿では、強靱性向上モデルの要求事項を満たしながらもネットワークの分離影響を少なくするための対応方式と、強靱性向上モデル適用後の運用上の課題への対応方式について解説する。

強靱性向上対策に対する利便性維持のポイント

まえがきで述べた三層の構えは、総務省から発表された「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」⁽²⁾の中で、以下のように示されている。

(1) マイナンバー利用事務系（既存住基、税、社会保障など）においては、原則として他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導

入等を図ることにより、住民（個人）情報の流出を徹底して防ぐこと。

(2) マイナンバーによる情報連携に活用されるLGWAN環境のセキュリティ確保に資するため、財務会計などLGWANを活用する業務用システムと、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こと。なお、両システム間で通信する場合には、ウイルス感染のない無害化通信を図ること（LGWAN接続系とインターネット接続系の分割）。

(3) インターネット接続系においては、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こと。

これによって、全国の自治体では、三層の構えのうち(3)によるインターネット接続口の集約を行い、(1)、(2)で実現されるシステム形態となる強靱性向上モデルを実装することとなった。

一方、総務省から発表された時点での一般的な自治体の庁内ネットワークは、住民の個人情報を取り扱う基幹系ネットワークと、LGWANやインターネットと接続し、基幹系以外の情報システムが接続される情報系ネットワークの二つで構成されていた。そのため、強靱性向上モデルを適用するためには、情報系ネットワークをLGWAN系とインターネット系に分離しなければならなかった。

ネットワークを分離しても、提供されていたサービスがいずれか一方のネットワーク上で継続していれば問題は発生しない。しかし、メールサービスについては、LGWANメールとインターネットメールをそれぞれのネットワークで提供する必要がある。このため、メールごとに端末を使い分けて運用する必要があり、職員の利便性を著しく低下させてしまうことが懸念された。メールは、言うまでもなく自治体と国・市民・業者をつなぐ重要なコミュニケーションツールである。今後もその重要度はますます高まるため、現在の利便性に近づけるための「ウイルス感染のない無害化通信」を実現することが最重要課題となった。

メールサービスにおけるウイルス感染対策とは、添付ファイルの無害化であると言える。これを実現するためには、利便性とセキュリティの確保度

合によって求められる機能が異なってくる。セキュリティを最優先するのであれば、添付ファイル内の情報を全てテキスト化する必要がある。しかし、図表などが含まれているものをテキスト化すると内容を解読できなくなり、逆に利便性を損ねてしまう。そのため、無害化したファイル中のデータの二次・三次加工までの利用といった一定程度の利便性の確保を目指した、マクロなどの有害機能を除去する機能がウイルス感染のない無害化通信のデファクトスタンダードとなっていく。

また、Web閲覧に関しては「自治体ICTリソースの全体最適に向けたアプローチ」⁽³⁾で解説されているとおり、VDI（Virtual Desktop Infrastructure：仮想デスクトップ基盤）をインターネット系ネットワークに配置することで、「画面情報のみのやり取りで行うウイルス感染のない無害化通信」の実現が可能となる。

これらを踏まえた強靱性向上モデルの要求事項

を反映したシステムイメージを図-1に示す。

強靱性向上モデル実現による運用への影響

総務省からの強靱性向上モデル適用の指示を受け、各自治体はその対応を進めた。対応時期がマイナンバー制度の稼働を見据えて設定されたことで、非常に短期間での対応完了が求められた。そのため、各業務システムの運用方式が十分に検討されないまま前章で述べたネットワークの分離が行われてしまい、新たな運用上の課題が発生した。

自治体では調達に公平性が求められており、特定のベンダーに集中することを回避するために、ほとんどの業務システムを個々に調達している。そのため、それぞれの業務システムを利用するためのユーザー情報（職員情報）もシステムごとに保持しているケースがほとんどである。一部の自治体業務システムでは、職員の人事異動に伴って発生する処理による運用負荷を軽減するため、業

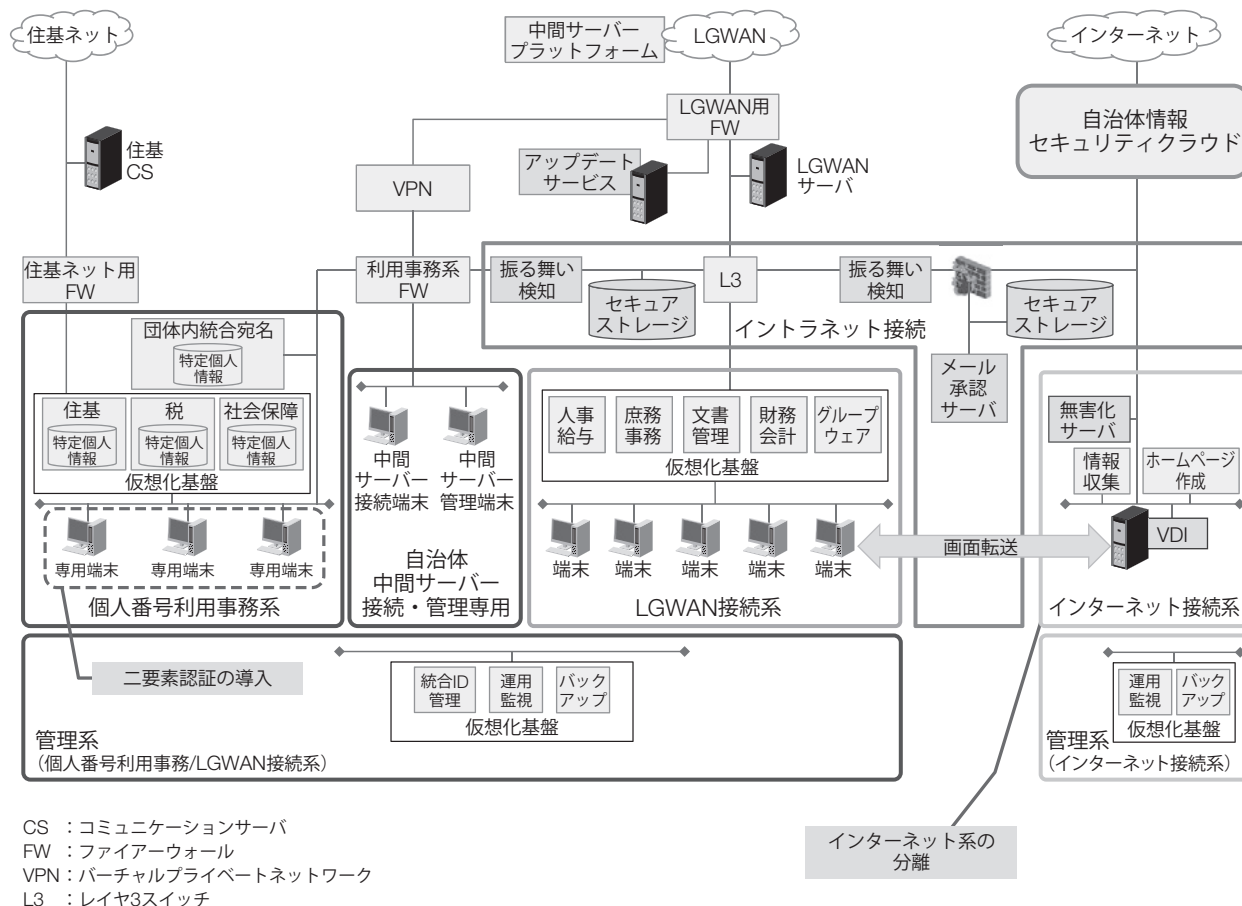


図-1 要求事項を反映したシステムイメージ

務処理によってアカウントを切り替える業務アカウントや、所属ごとに配付される所属アカウントを使用していた。

そのような中、今回の強靱性向上モデル適用の要求事項である個人番号利用事務系の二要素認証化によって処理を行う個人の特定が必須となった。このため、多くの自治体で従来から運用されていた業務アカウントや所属アカウントによる認証処理は利用できなくなった。これによって、実在の職員情報に基づくアクセス制限設定を業務システムごとに実施することが必要となり、特に年度末などの組織改編や人事異動が多い時期になると、アカウント情報更新の負荷は相当大きくなっていった。具体的には、業務システムごとにユーザー情報の属性や桁数、内容に違いがあることが多い。したがって、人事異動の処理を行うためには、人事システムから提供されたデータを基に桁数を揃えるためのゼロ埋めや、区分コードの変換といった「二次加工する一手間」をかけた上で、データを投入する必要があった。更に、業務システムの数が増加すると、上記の手間の積み重ねが大きくなり、作業工数を増大させることになる。

また、今後予想される新たな業務通信の追加に対しても考慮が必要である。前述のアカウント運用を例に挙げると、職員情報を管理する人事システムはLGWANネットワークに配置されている。このため、個人番号利用事務系に業務システムが追加されるたびに、フィルタリングを追加するファイアーウォール運用の煩雑化・コスト増加に加えて、通信制御ポリシーの複雑化といった運用上の課題が発生する。

運用上の課題回避への取り組み

従来、組織改正や人事異動に伴う職員情報や所属情報の連携システムへのデータ配信～更新処理は、ほとんどが人手で行われている。また自動化されていたとしても、特定の作業のみが動作するバッチ処理で構成されていることが多く、環境変化に対する柔軟性がなかった。更に、人事情報という側面から、実際の異動直前まで業務システムにデータが提供されないケースが多い。そのため、短期間で多数の業務システム用データの作成とその反映・確認をしなければならず、常に時間不足

と戦いながら運用を行ってきた。これを回避するためには、人事システムから提供される職員情報や所属情報を一元管理して、職員・所属情報を誰でもメンテナンスできるようにし、かつ各業務システムに合わせた形式に変換してデータを配信する処理を完全に自動化する以外に手がない。

そのため、前述した通信制御ポリシーの複雑化を回避しつつ、個人番号利用事務系システムへ職員情報を配信するためには、図-2に示すデータ蓄積変換機能を実装することが必要不可欠であると考えた。この機能は、LGWAN系ネットワークで発生する職員情報を個人番号利用事務系ネットワークに接続するシステムごとにデータ変換した上で、各業務サーバに配信するものである。このデータ蓄積変換機能の実装により、時間不足で間に合わなくなるというリスクを回避できるだけでなく、業務システム追加に伴うフィルタリング運用の煩雑化・複雑化も回避できる。

マイナンバーの本格利用時代に向けた考察

今回の強靱性向上モデル適用への対応は、マイナンバー制度の運用開始に起因している部分が多い。国は、マイナンバーの利用範囲の拡大を検討しており⁽⁴⁾、今後新たな業務システムが次々に個人番号利用事務系システムに追加されることが予想される。一方、自治体側も従来からの住民サービスを組み合わせた新たなサービスの提供を目指している。このため、個人番号利用事務系ネットワークに接続する業務システムは、業務間の連動性をより高める必要が出てくると予想される。

つまり、マイナンバーが本格的に利用される時代になると、システムを横断した業務処理がこれまで以上に多数発生することが予想され、自治体職員が使いやすいポータルシステムの導入が必須になると考えられる。

また、自治体は新たな住民サービスの提供を模索している。この新たな住民サービスを実現するためには、従来からの業務システムの情報に加え、追加された新たな業務システムの情報を組み合わせ、よりきめ細かい住民の特性・傾向の分析ニーズが高まることが予想される。いわゆるBI (Business Intelligence) ツールを使用した、エンドユーザー独自の分析機能である。

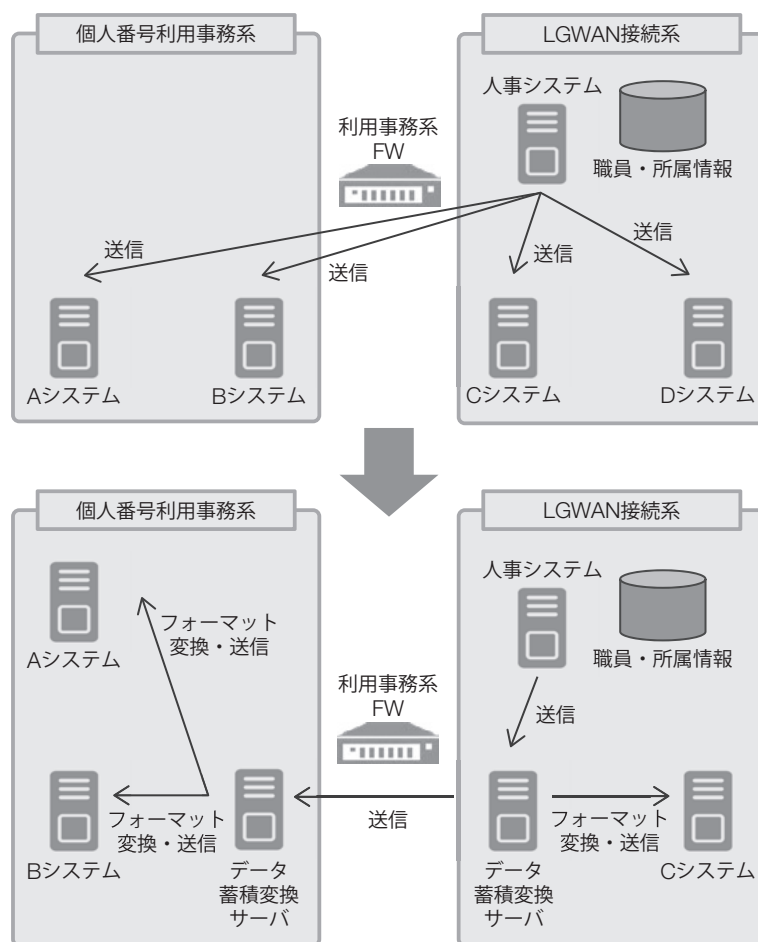


図-2 データ蓄積変換機能方式の概要

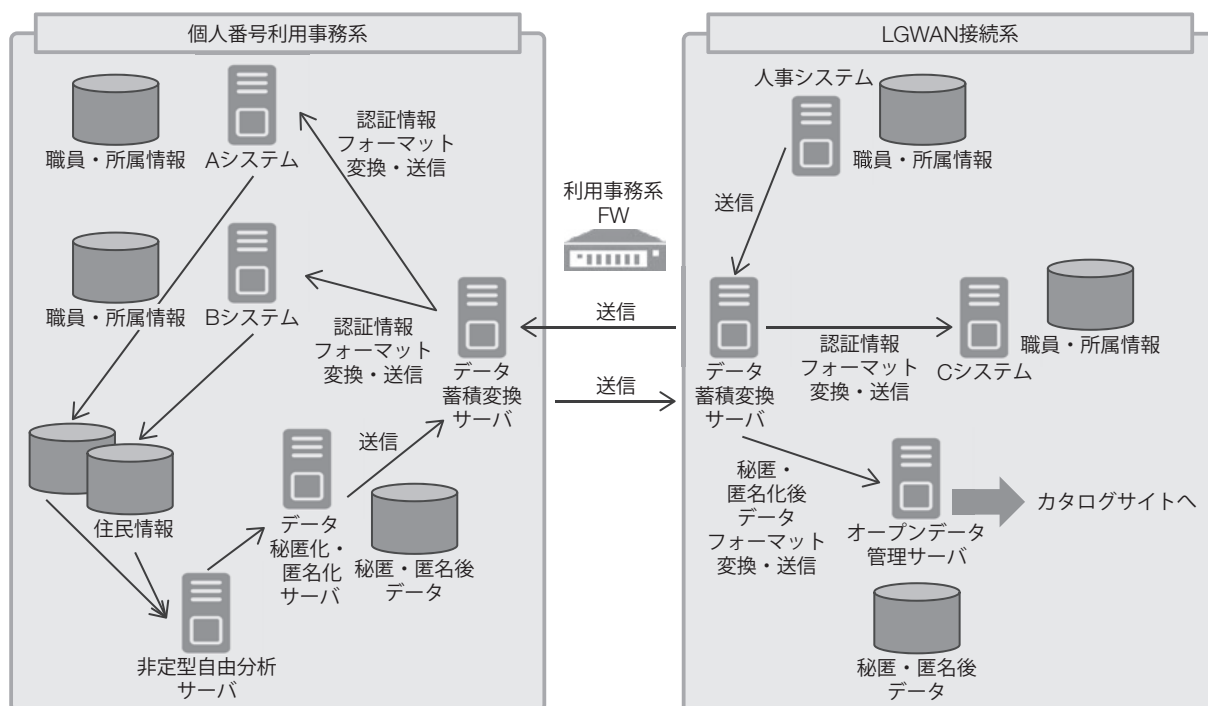


図-3 データ秘匿化・匿名化機能の実装方式

更に、新たに導入される業務システムで発生する住民情報の量や属性が充実してくると、次は地域産業活性化に向けた官民によるデータ活用時代が訪れると予想される。いわゆる「オープンデータ戦略」である。オープンデータの利用を実現するためには、住民（個人）情報の流出を徹底して防ぐ必要があり、個人情報の秘匿化・匿名化は必要不可欠な機能である。そのため、前述のデータ蓄積変換機能において、個人情報の秘匿化・匿名化機能を追加実装できるように機能を分割する必要がある（図-3）。このデータ蓄積変換機能とデータ秘匿化・匿名化機能を組み合わせたソリューションによって、オープンデータの利用を実現するプラットフォームへと段階的に拡張できると考える。

む す び

本稿では、総務省の強靱性向上モデル要件における運用上の影響に加えて、マイナンバー制度の本格的な運用が開始された後の富士通が考える新たなソリューションの方向性について考察した。外部環境が新制度の施行や法改正などに伴って変化した場合、当然お客様の要件も変化する。ベンダーとしては、環境の変化を理由に手をこまねいているわけにはいかず、何らかの対策を施さなければならない。

例えば、マイナンバー制度の本格運用前に、日本年金機構の情報漏えい問題のような外部環境の変化が発生した場合には、お客様の要件が変化する可能性もゼロではない。その対策としては、変化を先読みし、世の中の動向を注視しつつ、お客様の要件を整理して、迅速に対応していくことが重要である。

富士通は、今後も環境の変化を注視し続け、未来を予測しながら、タイムリーにお客様に貢献できるシステムを継続的に提供することで、お客様のビジネスの成功に貢献していく。

参考文献

- (1) 日本年金機構における不正アクセスによる情報流出
事案検証委員会：検証報告書（要約版）。
<http://www.nenkin.go.jp/oshirase/topics/2015/0104.files/G.pdf>
- (2) 総務省：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。

http://www.soumu.go.jp/main_content/000387560.pdf

- (3) 森永景介：自治体ICTリソースの全体最適に向けたアプローチ。Fujitsu, Vol.65, No.6, p.49-55(2014).
<http://img.jp.fujitsu.com/downloads/jp/jmag/vol65-6/paper04.pdf>

- (4) 内閣官房：マイナンバー制度の概要と最新動向について。

[http://activeictjapan.com/pdf/20150909/](http://activeictjapan.com/pdf/20150909/jimin_it-toku_document2_20150909.pdf)

[jimin_it-toku_document2_20150909.pdf](http://activeictjapan.com/pdf/20150909/jimin_it-toku_document2_20150909.pdf)

著者紹介



千原章義（ちはら あきよし）

行政システム事業本部
事業戦略統括部
自治体向け業務ソリューションのアプリケーション基盤企画・開発に従事。



千葉祐太郎（ちば ゆうたろう）

行政システム事業本部
事業戦略統括部
自治体向け共通基盤ソリューションのパッケージ開発および保守に従事。



野中謙佑（のなか けんすけ）

政策渉外室
執筆当時、自治体情報システム強靱性向上モデルの対応に従事。現在はICT政策、ビジネス環境整備・ビジネス市場拡大に向けて渉外活動に従事。