自治体セキュリティ強靭化に関する調査報告
Survey report on strengthening local government information system

牧野 尚彦 [1)a)]、水越 一郎 [1)]、中西 晶 [2)]、上原 哲太郎 [3)]、後藤 厚宏 [1)]
Takahiko Makino, Ichiro Mizukoshi, Aki Nakanishi, Tetsutaro Uehara, Atsuhiro Goto

1 情報セキュリティ大学院大学 情報セキュリティ研究科
2 明治大学 経営学研究科　3 立命館大学 情報理工学科
a mgs175513@iisec.ac.jp

要旨: マイナンバー制度の導入によって、自治体における個人情報管理の重要性が高まっている。一方、2015年に日本年金機構において個人情報漏洩事件が発生した。これらの背景・事件を契機として、政府は自治体の情報セキュリティの抜本的強化を目的として、総合行政ネットワーク（LGWAN）とインターネットとの接続を断つとともに、自治体とインターネットの接続口を各都道府県で一本化する「自治体情報セキュリティクラウド」を導入した。
これらの施策によって、自治体の情報セキュリティは大幅に向上されたことが期待される。
この施策が実際にセキュリティを向上させたかどうか、また自治体職員の業務にどのような影響を与えたかの調査結果を報告する。

Abstract: Introduction of the national identification number system increased the importance of privacy control in the local governments. Besides, Japan Pension Service announced its personal information leakage incident in 2015. In response, Japanese government decided to urge all local governments to enhance their information security control by using the Local Government Wide Area Network (LGWAN), the network separation between the business terminals and internet, and "the local government information security cloud".
These means should have greatly improved information security in the local governments.
We hereby report the result of the survey which we carried out in order to find out whether the means really improved security and, on the other hand, how the day to day work of the staff at the local governments were affected.

キーワード: セキュリティ、自治体、インターネット分離、無害化
Keywords: Security, Local Government, Internet Separation、Sanitization

1. はじめに

2013 年 5 月にマイナンバー法案が成立・公布され、国の行政機関および地方自治体およびの行政機関において、住民情報の組織間連携の準備が進められることとなった。

その一方で、2015 年 5 月に日本年金機構における個人情報流出事案が発生したことを受け、総務省は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」を設置し、「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。 [1]

この報告書では、「三層の構えで万全の自治体情報セキュリティ対策の抜本的強化を」とし、以下の 3 つの対策を行うべきとした。

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 [1]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、ウイルスの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。

またこの対応期日を 2017 年 7 月の情報提供ネットワークシステムの稼働日として各自治体に対応を求め（後に 2017 年 7 月 18 日に決定）、そのための補助金として約 255 億円を予算措置し、そのほぼ全

[1] 総合行政ネットワーク（Local Government Wide Area Network）。地方公共団体の組織内ネットワーク（庁内 LAN）を相互に接続する行政専用の閉域網。各府省の庁内 LAN を相互に接続する「政府共通ネットワーク」とも相互接続している。

てを都道府県および市区町村に交付した。 [2]

全国の自治体職員は 2017 年 4 月時点で約 274 万人存在する [3] が、この 3 つの対策によってその多く[2]の業務環境が大きく変化したことになる。

この施策によって、全自治体の業務ネットワーク環境の情報セキュリティは大幅に向上されたと期待される。

この施策のうち、特に自治体職員の業務に大きな影響を与えたと考えられる「LGWAN 接続系とインターネット接続系の分割」に着目し、その概要と、期待される効果、副作用として発生している課題について論じる。

2. 施策の概要

2.1 ネットワーク分離

総務省が報告書において示した自治体ネットワーク再構成イメージ例では、従前は住基・税・国民健康保険等を扱う「基幹系」とその他の内部情報を取り扱う「情報系」の 2 系統のネットワークに分割され、情報系は LGWAN とインターネットの両方に接続されていた。

このうち「情報系」について、本施策によって、内部情報を取り扱う「LGWAN 接続系」と、Web サイトでの情報受発信や電子メール等を取り扱う「インターネット接続系」に分離するものとした。また、LGWAN 接続系とインターネット接続系の間の通信は原則禁止とし、無害化通信のみを許可するものとした。

これを単純に物理端末のみで実装すると、インターネットと内部情報システムの両方を利用する必要がある職場ではネットワークや端末機が倍増してしまう。このため、実際にはインターネット接続系には物理端末を置かず、VDI（仮想デスクトップ環境）や SBC（サーバーベースドコンピューティング）といった技術を利用し、片方の端末環境を仮想化する方式が用いられる場合がある。

端末環境の仮想化において、LGWAN 接続系端末とインターネット接続系の仮想端末との間は画面・操作のみを転送する。これにより、仮にインターネット接続系の仮想環境がマルウェアに感染したとしても、LGWAN 接続系の情報資産が影響を受けることがないと考えられる。

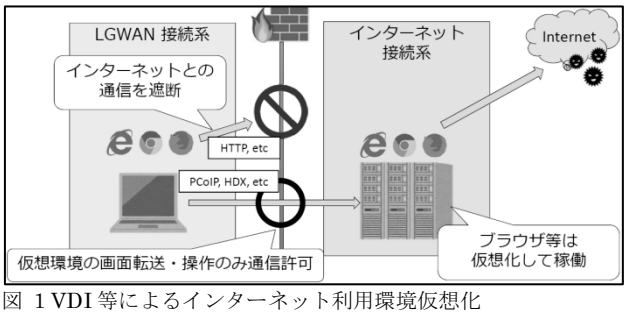

図 1 VDI 等によるインターネット利用環境仮想化

[2] 公営交通運転手等、業務上この 3 つのネットワークのいずれにも関わっていない職種も存在するため、全てではない。

2.2 ファイル無害化

インターネットから取得したファイルや電子メールに添付されたファイルを LGWAN 接続系に転送する必要がある場合は、ファイルに対して無害化処理を施す。

ファイル無害化システムが一般的なアンチウイルスと大きく異なる点は、悪性コードが存在しうる領域であれば、実際に悪性か否かにかかわらず一律削除または安全なデータに置き換える点である。

無害化システムとして提供されている製品は、大きく 2 種類の実装方式が存在する。

①ファイルを PDF や画像に変換するもの

②元の形式を保ったまま処理するもの

下図は後者のイメージを示したものである。

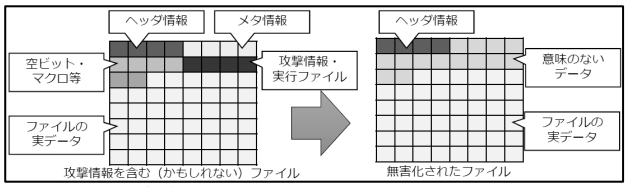

図 2 ファイル無害化イメージ

ファイル無害化システムのメリット・デメリットを以下の通り整理する。

メリットは、ファイル無害化処理では良性か悪性かを判断せずプログラムコードが一律削除されるため、偽陰性が理論上 0%となり、悪性コードが LGWAN 接続系に入り込む可能性がないと考えられることである。[3]

デメリットは、偽陽性も理論上 100%となり、どんな良性で必要なプログラムであろうと除去されることである。このほか、PDF や画像に変換するタイプの無害化処理が行われた場合、データの再編集ができなくなる。画像化した場合はテキストデータコピー・検索ができなくなるほか、視覚障害者が音声読み上げできなくなるといったアクセシビリティ上の問題も発生すると考えられる。また、ファイル形式毎に個別の処理が必要となるため、システムが対応していない形式に対しては何も処理することができず、無害であることを保証するためにはファイル自体を除去せざるを得ない。

3. 発生している課題

この施策はインターネットを通じた情報摂取攻撃への対策として大きな効果を生むと考えられる一方で、大きく安全面に倒したことにより様々な課題を生んでいる。

4.1 先行研究での指摘事項

吉田(2016)は、「ネットワークごとに使用する端末を使い分けたり、インターネットからダウンロードやメールに添付したファイルが他のネットワークに取り込めなくなったりという業務の非効率化にもつながる」と述べている。 [4]

また同じく吉田(2017)は、3 つの観点における実施事項とその課題を述べており、

[3] 無害化システム自身に脆弱性がある場合を除く

(1)複数ネットワークへの端末配備として「VDI や SBC 方式」を採用した場合、「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方式として「LGWAN-ASP（中略）サービスを利用」した場合「従来無償で利用したのが，有償となる」、「媒体を用いてサーバや端末ごとに個別で適用」した場合「アップデートごとに個別作業が必要」、
(3)ネットワーク間でのメールやファイルの受け渡しとして「メール内容を画像又はテキスト化して転送し閲覧」した場合「本文中の URL がハイパーリンクされない」「費用がかかる」、「無害化ツールを利用」した場合「ファイルの同一性を確保できない、費用がかかる、全種類のファイルには対応していない」等の課題を挙げている。

吉田の指摘は、大きく分類して「業務効率低下」と「経費増大」の 2 つの側面を取り上げている。 [5]

4.2 報道されている不具合事例

また、共同通信(2018)によれば、この施策の影響で「住民や民間業者からのメールや申請書類が届かないといったトラブル（中略）45 都道府県の 300 超の市区町村で業務に支障が出ていた」と報道されている。 [6]

ただしトラブルの内容は「問題のないメールや添付書類が、迷惑メールや安全性が疑わしいファイルと誤認され、自動的に削除される」とされており、一般的なウイルス・スパム対策の偽陽性に関するトラブルであるように読み取れる。

同じく共同通信によれば「突貫工事」「スケジュールありき」とされており [7]、この問題は導入初期の一過性のトラブルと考えられる。

4.3 ソフトウェア更新の不備

このほか本稿では、ソフトウェアのアップデートについて取り上げたい。

端末・サーバ機等で動作する OS やアプリケーション、アンチウイルス等の各種ソフトウェアは、最新の状態を保つためにインターネットから更新ファイルをダウンロードする必要があるが、ネットワークの分離によってそれができなくなる。

このため、特にメジャーな製品については、LGWAN 向けに更新ファイルを中継配信する LGWAN-ASP サービスが複数社から提供されている。

しかし LGWAN-ASP で更新ファイルが配信されている製品は一部に過ぎない。

以下の表は、地方公共団体情報システム機構が公開している ASP サービス一覧 [8]から「アップデート」または「配信」を含むものを確認した結果、サービスの存在を確認できたものとそうでなかったものを示したものである。

表 1 LGWAN-ASP での更新ファイル配信サービスの有無

	確認できた	確認できない
OS	Windows	macOS、Linux
アンチウイルス	Symantec 、TrendMicro、McAfee、ESET 、 Kaspersky 、Sophos	F-Secure、ClamAV
アプリケーション	Microsoft デスクトップアプリ	ジャストシステム、Adobe、Google、Mozilla、Microsoft ストアアプリ

OS とアンチウイルスに関しては、業務で幅広く利用されていると思われるものは概ねカバーされているが、アプリケーションに関しては非常にメジャーなものであっても対応されていない。このため、脅威が減っている一方でアプリケーションの脆弱性が放置され、新たなリスクが増大している恐れがある。

4. 実態調査・インタビュー

これまでの調査で、以下のような疑問点が上がってきた。

- インターネット分離は大きな効果があると思われるが、実際に効果が出ているか?
- セキュリティパッチを含めて何もかも遮断するのは妥当か? よりバランスの良いやり方があるのではないか?
- 自治体業務にどんな悪影響を与えているか? 住民サービスの低下などはないか?
- 利便性低下に伴いシャドー IT が増加し新たなセキュリティリスクを増大させていることはないか?
- セキュリティクラウド（都道府県での一本化）は本当に費用対効果が出ているのか?

以上のような疑問について、実態を把握するための最初の手がかりとして、複数の自治体のシステム管理者・エンドユーザーに対してそれぞれインタビューを実施した。

インタビュー対象は以下の通りで、2017 年 11 月から 2018 年 1 月にかけて行った。

- 都道府県（システム管理者）× 1
- 市区町村（システム管理者）× 2
- 市区町村（エンドユーザー）× 2

以下に、それぞれから聞き取った回答内容の一部を記載する。なお、回答者の団体の特定を防ぐ都合上、都道府県は全て「県」、市区町村は全て「市」と記載している。

5.1 システム管理者向けインタビューの回答

表 2 マルウェア関連インシデント発生量の変化

質問	回答
内部ネットワーク（LGWAN 接続系）におけるマルウェア検知量	A 市: 変わらない B 市: **下がった**
SOC から通報を受ける頻度	A 市: SOC を利用していなかったため比較できない B 市: どちらとも言えない

表 3 管理者の業務負担の変化

質問	回答
新たなシステム利用に関する調整・問い合わせ対応等で業務負担増	A 市・B 市:**あり**

インシデントが減って業務負担減	A 市: なし B 市: **あり** X 県: **頻度は増えた**が短時間で状況把握できた**トータルでは楽に**なった

表 4 経費

質問	回答
補助金は足りたか? 一般財源からどのぐらい補填したか?	C 市: **補助金の 3 倍**はかかった D 市: **補助金約 3 千万に対し**て**一般財源から 1 億以上**出した

表 5 エンドユーザーからの声の有無

質問	回答
安心して仕事できるようになった	A 市: なし B 市: **あり**
システムの利便性が悪い	A 市・B 市: **あり**
システムの応答が遅い	A 市: なし B 市: **あり**
システムが不安定	A 市・B 市: **あり**

以上から、少ないサンプルながらもセキュリティ向上効果が見られること、その一方で利便性に関するエンドユーザーからの苦情が複数の団体で上がっていることがわかる。

5.2 エンドユーザー向けインタビューの回答

Q PC を使う仕事のしかたは変わったか A 「手順」という意味ではとても変わった。例えば**仮想ブラウザの起動に 3〜40 秒**かかる。ダウンロードしたファイルは無害化によって**全て PDF 変換**される。
Q どのぐらいで慣れたか A 操作自体は半月で慣れたが、**全て PDF 化されることには 8 ヶ月経った今も慣れない**。
Q 安全性は向上したと思うか A **ウイルス付きメールが来なくなった**。
Q 今回の変化をどのように感じているか A1 良い点: **安全性は格段に向上**した。 悪い点: **ロスタイムが非常に多くなった**。例えば**仮想ブラウザが短時間でセッションタイムアウト**し、**再接続に 3〜40 秒**かかる。 ダウンロードファイルの**無害化処理に 3 分〜3 時間**近く待つ。**PDF を印刷して手で入力している職員も**いる。 A2 仮想ブラウザの動作が遅い、**インターネットの調べ物は私物のスマホでやっている**人もいる。 **Thunderbird** を使っていて時々**「更新できません」という旨の警告が出る**のが気になる。

安全性の向上はエンドユーザー側でも感じられているが、利便性・業務効率が著しく下がっていることや、また、一部のアプリケーションで更新が止まっていることがうかがえる。

5. まとめ

全国自治体において行われたセキュリティ強化のうち、特にインターネット分離については、インターネットからの攻撃（特に情報窃取）に対して大いに有効と考えられる。

しかし、これは大きく安全側に倒した施策であり、様々な課題も生んでいる。課題は大きく以下の 2 種類に分けられる。

①大規模な変更をスケジュール優先で強行したことによるシステム障害（一過性）

②インターネット接続性がないことによる利便性や業務効率の低下、セキュリティパッチ適用不可など（継続的・本質的）

また、複数の市区町村において、交付された補助金の約 3〜4 倍の経費がかかっていた実態が明らかになった。

6. 今後の予定

今回は対面インタビューによって調査を行った。有意義な情報を聞き取ることができたが、サンプル数としてまだ少ない。今後も自治体システム管理者への調査、エンドユーザーへの調査を、それぞれ範囲を広げて継続したい。

そのうえで、各団体での課題意識や構成例をもとに、安全性と実用性のバランスの取れた構成を模索・提案したい。

7 参考文献

[1] 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,” 2015.

[2] 総務省, “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,” 2016.

[3] 総務省, “平成 29 年地方公共団体定員管理調査結果の概要,” 2017.

[4] 吉田博一, “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,” 2016.

[5] 吉田博一, “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,” 2017.

[6] 共同通信, “300自治体事務トラブル メール、申請書類届かず サイバー対策で副作用,” *47 行政ジャーナル,* 8 1 2018.

[7] 共同通信, “【深掘り】〜情報セキュリティー強化でトラブル〜 解決策見えず、自治体困惑 「突貫工事」が裏目に,” *47 行政ジャーナル,* 8 1 2018.

[8] 地方公共団体情報システム機構, “LGWAN-ASP サービスリスト,” [オンライン]. Available: https://www.j-lis.go.jp/lgwan/asp/servicelist/cms_15764241.html. [アクセス日: 29 1 2018].