自治体初の安心マーク導入と DMARC 対応

上島町役場
総務部　広報情報課　情報推進係
元森　龍太　氏

はじめに（上島町のご紹介）

上島町は、半径 200 キロメートルで神戸市と下関市を結ぶ瀬戸内海のほぼ中央に位置し、愛媛県の東北部、広島県境に浮かぶ 7 つの有人島と、18 の無人島からなる全部離島の町。サイクリングが盛んである。町のマスコットキャラクターは、上島町内に古くから住まう海の神様をモチーフとした「かみりん」。

自治体のセキュリティ動向について

国や地方自治体は、平成 29 年 7 月から開始されるマイナンバーの本格利用、すなわち、情報提供ネットワークシステムによる情報連携を控えている。こうしたなか、平成 27 年 6 月に日本年金機構による情報流出事案が発生したことを受け、地方自治体の情報セキュリティに係る抜本的な対策を検討するため、総務省に自治体情報セキュリティ対策検討チームが設置された。その後平成 27 年 12 月 25 日付け総行情第 77 号「新たな自治体情報セキュリティ対策の抜本的強化について」で、総務大臣から全自治体に対し、セキュリティ対策についての通知があった。

その主な内容としては、マイナンバー利用事務系では端末からの情報持ち出し不可設定等を行い住民情報の流出を徹底して防止すること、マイナンバーによる情報連携に活用される LGWAN（総合行政ネットワーク。自治体同士を繋ぐ専用のネットワークであり、マイナンバーの他団体との情報連携もこのネットワークを利用する）環境のセキュリティ確保のため LGWAN 接続系とインターネット接続系を分割すること、都道府県と市区町村が協力して自治体情報セキュリティクラウドを構築し高度な情報セキュリティ対策を講じること、というものである。またこれとあわせて、総務省から全国地方自治体に対し、自治体情報システム強靭性の向上の実施の要請と、補助金の支給が行われた。

自治体情報システム強靭性の向上で求められる対応

マイナンバー利用事務系については、マイナンバー利用事務系端末について二要素認証を施したうえで、インターネットへの接続は不許可とし、プリンターも共有しないといった、完全に閉じたネットワークにする対応を行っている。

一方、その他の情報系端末では、現在、インターネット、E メール、LGWAN 上のサイト、LGWAN メールを利用することができるが、自治体情報システム強靭性向上対応では、LGWAN 系ネットワークとインターネットを完全に分離させることが求められている。現時点では、LGWAN でのやりとりは自

治体同士でのやりとりが主な方法であり、その他、他市町村の例規を見る際等にはインターネットを利用するし、業者とのデータ・文書のやりとりには E メールを利用している。またシステム的なところでは、たとえば WSUS やウイルス定義ファイルのアップデートなどはインターネットに接続しないとできないので、これらを完全に分離するとなると、業務へのインパクトがかなり大きいと考えられる。また、現在、各自治体で ISP に契約してそれぞれでインターネット接続しているのを、今後は都道府県ごとにインターネット接続を統合し、SOC 等の高度なセキュリティ対策を施すことも求められている。この対応をセキュリティクラウドと呼んでいるが、こちらもあわせて対応を検討しているところである。

なお具体的な対応として、まずメールは、LGWAN 側からインターネットへの送信は行うことができ、インターネットから LGWAN への受信は、無害化処理（テキストデータ・添付ファイルの削除）を行えば可能である。インターネット閲覧については、専用端末を置くか VDI・リモートデスクトップなど、間接的ならよいということになっている。また、例えば設計書や仕様書等のやりとりにおいて、インターネット上で取得したファイルを LGWAN 上に持ってくるような場合は、マクロの削除や PDF を画像ベースのデータにする等の無害化処理を施せば可能であるということになっている。

DKIM＆DMARC、安心マークの導入について

以前より、地方公共団体情報システム機構（J-LIS、当時は LASDEC）から、メールに SPF を採用するよう要請があった。せっかく導入するならばということで、SPF 以外にもメールに適用できる技術をあわせて検討していたところ、DKIM にたどり着いた。DKIM の導入は難しいと考えていたが、実際には SPF とあわせて簡単に設定することができ、スムーズに導入した。また SPF と DKIM の導入をふまえて、メール発信元が本物であることを明示できる「安心マーク」を導入、さらにその後 DMARC の導入にも至った。安心マークの導入は地方自治体初であり、今年 10 月にニュースリリースも行っている（ https://www.jipdec.or.jp/topics/news/u71kba0000005qd9-att/20161014.pdf ）。

DKIM は、実質 1～2 日で設定完了した。大まかな流れとしては、1.パッケージを入れる（OpenDKIM）、2.秘密鍵・公開鍵を作る（ドメイン認証で OK）、3.DNS の設定、4.Postfix の設定（数行で OK）、5.動作確認、というものである。また DMARC は、DKIM と SPF の設定を行っていれば、DNS にレコード登録するだけでよいので、簡単に導入できた印象だ。

今後、自治体セキュリティクラウドでは、インターネット接続を県で 1 本化することになる。これはつまりメールも出口を一本化することになるため、もし DKIM・DMARC の設定をそこで行えば「県内自治体すべてが対応」ということになり、もっとこうした技術の普及につながるのではないかと考えている。