情報セキュリティ対策強化に伴い、システム運用が大きく変わります

本年 7 月の番号制度の情報連携開始を前に、庁内システムのセキュリティ対策が強化され、各システムの運用方法が大きく変わります。国の自治体情報システム強靭性向上事業に基づくシステム構築や移行準備等を概ね完了し、操作習熟のための既存システムとの併用期間を経て、平成 29 年 6 月末までに順次、新システムへ切り替えていきます。

■国から求められている対策

①特に個人番号利用事務系からの個人情報流出の防止

・端末からの情報持ち出し不可設定

・2 要素認証の導入（端末やシステムのログインに複数の認証方法を使用）

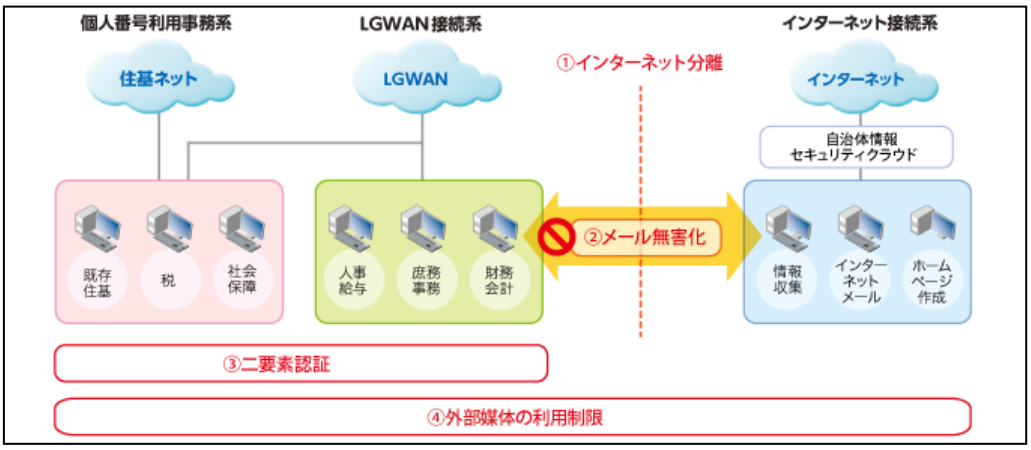
②LGWAN 接続系（国、地方公共団体系）とインターネット接続系の分離

・グループウェアを LGWAN 側用とインターネット側用に分割

・インターネットメールやファイルの無害化、画面転送方式によるインターネット接続

③県域単位で構築されるセキュリティクラウド（SC）への参加

・インターネット接続ルートを県 SC に集約、県 SC が通信等を 24 時間・365 日監視



■市の対策実施に伴う、システム運用の主な変更点

A）個人番号利用事務系の業務用端末からの情報持ち出し不可設定（①対策）

既に、業務用端末への外部記憶媒体（USB メモリ等）の接続を原則禁止しています。現在は業務上の必要に応じ、端末や媒体を限定して接続を許可していますが、セキュリティ対策上の必要があれば制限をさらに強化します。たとえば、媒体は情報政策室内の端末にしか接続できなくする等の方法について、システム事業者等と検討中です。

B）個人番号利用事務系への二要素認証の導入（①対策）

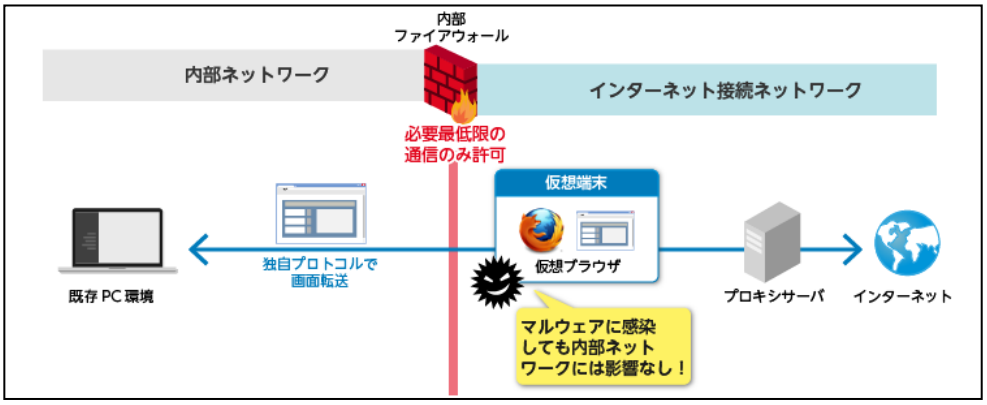
端末の起動やシステムへのログインにおいて、従前は指紋またはパスワードのいずれか

一つによる認証でしたが、なりすまし等による不正アクセスを防止するため、個人番号利用事務系システムには生体認証（指紋）と IC カード認証の二重認証を導入します。端末起動時、システムログイン時のいずれにおいても指紋と IC カードの両方で認証します。システム操作者を適切に管理し、不正アクセスを防止するには、操作開始時のログインと操作終了後のログアウトの徹底が重要です。

C）事務用端末のインターネット接続方法の変更（②対策）

インターネット分離後、事務用端末（一人一台パソコン、マスタパソコン等）は LGWAN 接続系の端末となるため、直接インターネットへは接続できなくなります。

事務用端末からのインターネット接続は、画面転送方式によるインターネット接続環境から行います。分離されたネットワークに接続することで動作が重くなり、ウェブサイト画面を印刷するには印刷イメージ PDF ファイルを LGWAN 側へ取り込む必要が生じるなど、従前に比べ時間や手間がかかるようになります。また、同時接続数に制限があるため、無操作で一定時間が経過するとインターネット接続を切断する仕組みになっており、インターネットメールの送信作業中やインターネットサービスの利用中においては注意が必要です。なお、当該環境では正常に表示、動作しないウェブサイト等もあり、そのような場合は別途対応を検討します。



D）インターネット用グループウェアの構築（②対策）

インターネット分離後、現行のグループウェアは LGWAN 用となり、インターネットメールが受信できなくなることから、インターネット用グループウェアを新たに構築しています。市民や事業者等とメールの送受信を行うときは、インターネット用を使用します。インターネット用グループウェアは、上記 C)のインターネット接続環境から起動します。一方、庁内メール、国や地方公共団体とのメールは、LGWAN 用グループウェアで送受信を行います。LGWAN 用からインターネット側（市民や事業者等）へメールを送信することはできません。送信ミス等による情報漏えい防止のため、送信メールに添付ファイルがあるときは強制的に圧縮され、解凍パスワードを設定することが求められます。

E）メール添付ファイル、ダウンロードファイルの無害化処理（②対策）

インターネット分離により、市民や事業者等から送付されたメールの添付ファイルやウェブサイトからダウンロードしたファイルは、そのままでは利用できません。事務処理上、インターネット側から LGWAN 側へファイルを取り込む必要があるときは、ファイル無害化装置を通してファイル無害化処理を行います。無害化処理が可能なファイルの種類には制限があり、無害化できないファイルは LGWAN 側へ取り込めないため、インターネット側で作業を完結する必要があります。LGWAN 側からインターネット側へファイルを出す際は、所属長等の承認が求められます。

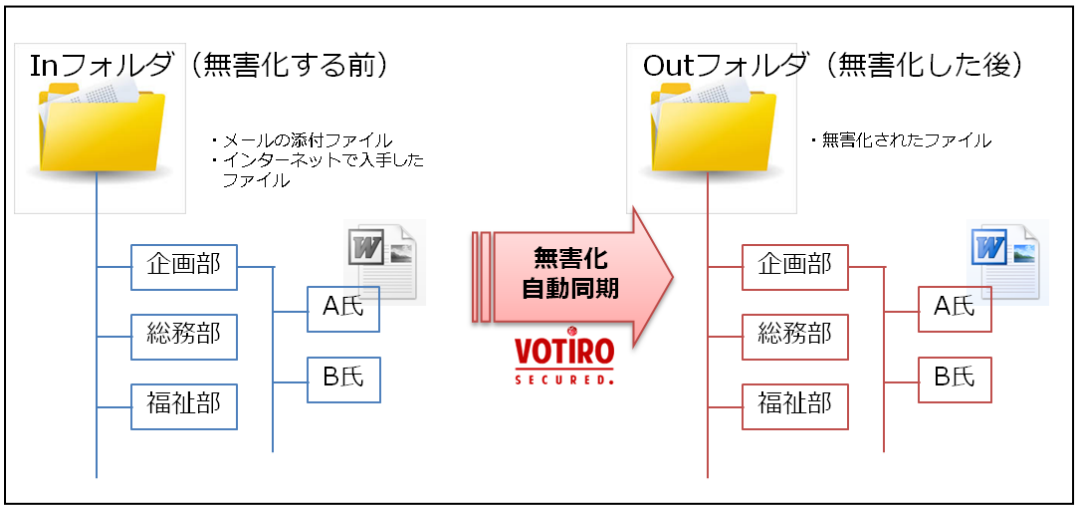
※無害化処理が可能なファイル

Microsoft Office：Excel,Word,PowerPoint

Adobe Acrobat：pdf

画像ファイル：bmp,gif,wmf,emf,png,jpg,jpeg,tiff,tif

圧縮ファイル：zip,cab,tar,rar,7z,gz



F）事務用端末への外部媒体接続の禁止（②対策）

上記 E）のインターネットからのファイル取り込みの規制に準じ、事務用端末（一人一台パソコン、マスタパソコン等）に外部媒体を接続することを禁止します。すでに使用許可をしている USB メモリ等も接続できなくなります。市民や事業者等との間で外部媒体を介してファイル授受をするときは、各所に配置される「データ取り込み・取り出し専用パソコン」を使用してください。外部媒体ファイルの取り込み等の際は、メール添付ファイルやダウンロードファイルの場合と同様に、ファイル無害化処理を行います。

G）県セキュリティクラウドによる通信状況等の監視（③対策）

「桑名市ホームページ」「桑名市議会ホームページ」「オープンデータポータルサイト」「文化財ホームページ」「桑名市グループウェア」へのインターネット接続は、県セキュリティ

クラウドを経由して行います。県セキュリティクラウドでは、セキュリティ・オペレーション・センター（SOC）が通信状況等を 24 時間・365 日監視しており、不正アクセスや不審な通信等を検知したときは、各市町へ通報する仕組みになっています。県から各ウェブサイトに対するサイバー攻撃の通報があった際は情報政策室で初動対応を実施しますが、状況次第で各ウェブサイト運営課の担当者を招集する場合があります。関係各課においては招集に備え、担当者や事業者との緊急連絡体制を構築しておくよう留意してください。

H）事務用端末での議会中継の閲覧を完全規制

申請により閲覧規制を解除している議会中継のインターネット閲覧は、議会運営上の必要な場合を除き、完全に規制します。議会中継等の動画配信は通信環境に負荷がかかり、インターネットを利用する他の業務に悪影響を及ぼしかねないからです。セキュリティ強化対策実施後は、理事者控室のモニターで傍聴する等により対応してください。議会事務局によると、6 月以降は議会中継のスマートフォン閲覧も可能となっていますので、その利用も検討してください。

I）部長級以上職員のインターネット閲覧規制を一般職員同様に強化

部長級以上職員のインターネット閲覧規制は一般職員に比べて緩和されていましたが、セキュリティ強化対策の一環として、一般職員同様の規制を行うように改めます。これにより、従前は閲覧できていた犯罪、暴力、麻薬、掲示板、SNS、ブログ、宗教、金融・投資情報、芸能等のウェブカテゴリが閲覧できなくなります。業務上、規制対象になっているウェブサイトを閲覧する必要があるときは、解除申請により対象を特定して規制を解除します。