総務省策定「地方公共団体における情報セキュリティポリシーに関するガイドライン」最新版の準拠をめざす！

自治体の既存システムに“後付け”できるログイン管理セキュリティ

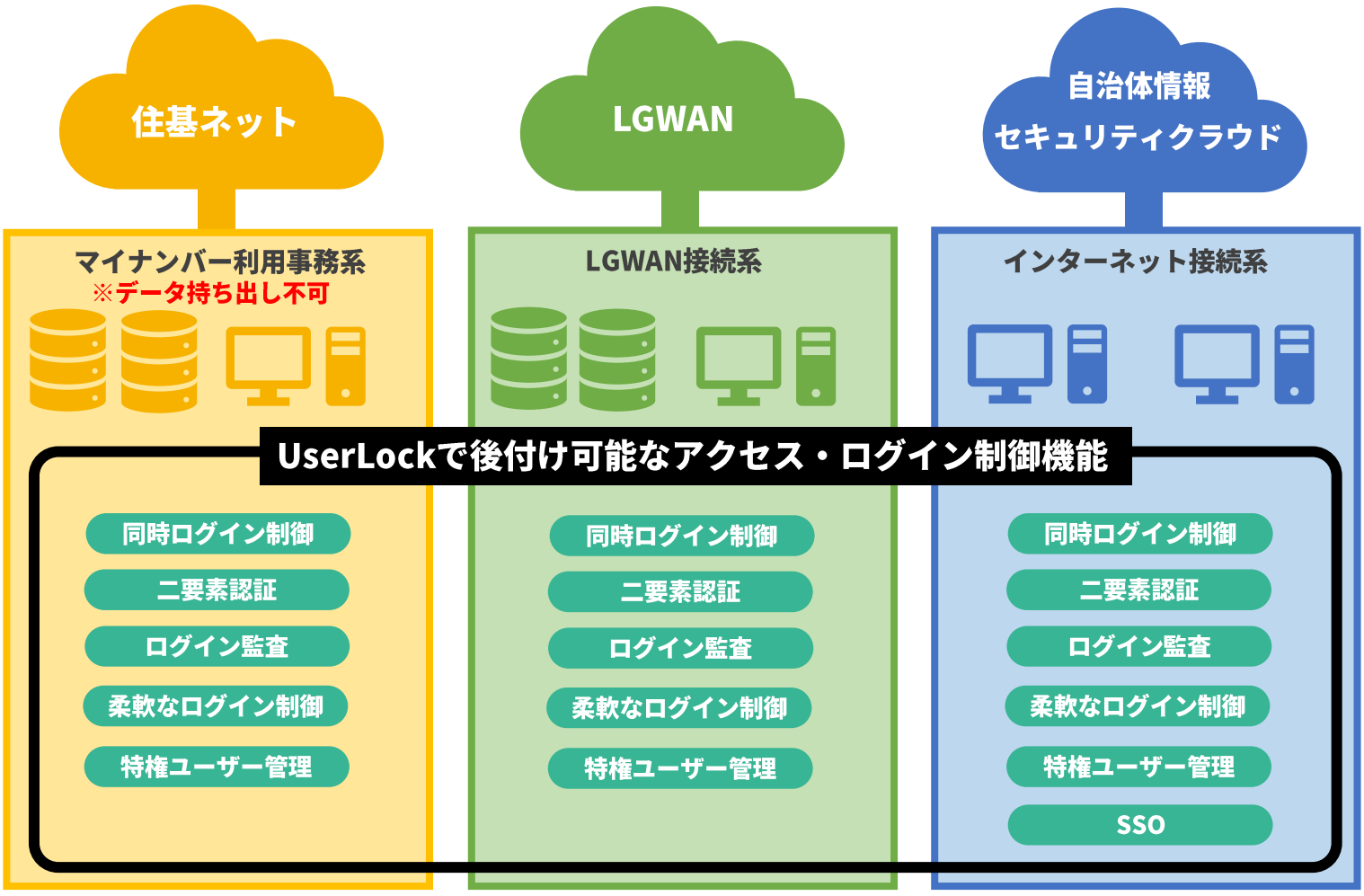
▶ ゼロトラストセキュリティで重要な内部対策

重要な情報資産を保管している各自治体様では、情報セキュリティ強化に努められていると思いますが、最新のサイバーセキュリティは「ネットワーク外部、内部を問わず、常に脅威にさらされている」という“ゼロトラスト”の観点で考える必要があります。ウィルスソフトやUTMなど外部からの攻撃には対策をされていて、昨今話題の“なりすまし”や、実は情報流出が一番多い“内部不正”などの内部対策は進んでいないというケースが多くなっています。

▶ 内部対策で重要なアクセス・ログイン制御

内部対策として効果的に安全性を高めるためには何が有効なのでしょうか。結局、不正を行うのは“人”であるということを踏まえると、“アクセス・ログイン制御”が課題を解決するためのキーポイントとなります。
しかし、いくらアクセス・ログイン制御が重要でも、そのためにシステムを大きく変更しなければならないとなると、導入は難しくなります。 既存のWindows Active Directoryに連携するログイン管理ツール“UserLock”であれば、三層分離モデルで構築された自治体のネットワークにも簡単に“後付け”が可能になります。

▶ 三層分離に“後付け”できるUserLock



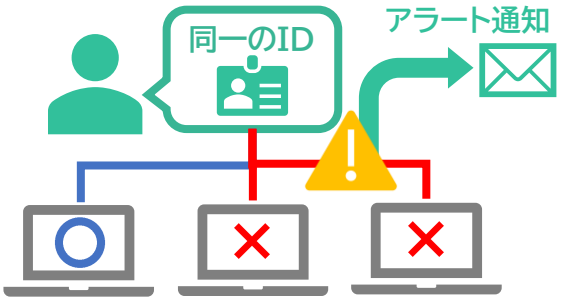
三層分離における運用面での課題をUserLockで解決

▶ 課題その1

職員間でアカウント情報を共有して使い回ししていたり、生体認証の認証端末のバックアップとして、1つのIDとパスワードを共有している場合、実際に誰がどのアカウントでログインしているのかわかりません。
このような場合、もし職員以外のなりすましによる不正アクセスがあっても防止するどころか、発見することも難しくなります。

▶ UserLockで解決

複数の端末で同時にログインした場合、検知と制御を行うことが可能です。アカウント情報の使い回しの防止だけでなく、なりすまし対策にも有効です。
さらに不正利用検知した場合、システム管理者、職員自身のアカウントにもアラートを通知することで素早い検知と対応を実現します。

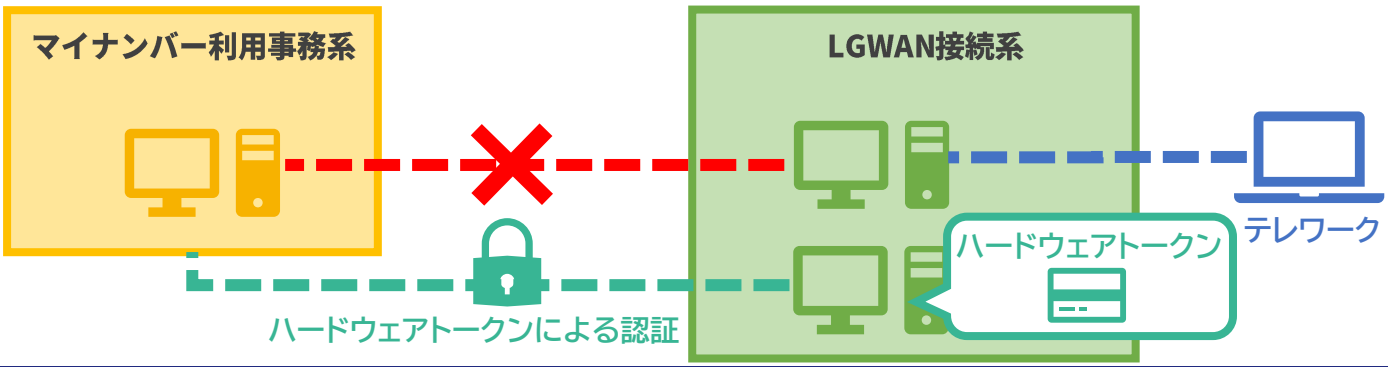


▶ 課題その2

クローズド環境であるマイナンバー利用事務系は、データ持ち出しが禁止されており、テレワーク時にアクセスできないように規定されています。しかし、システム構成によってはテレワーク時にLGWAN接続系端末を踏み台にすると、アクセスが可能となってしまいます。

▶ UserLockで解決

マイナンバー利用事務系にログインする場合には、UserLockでハードウェアトークンによる二要素認証を実装、ハードウェアトークンを庁内で保管することにより、庁内からのみアクセス可能にします。



OCEANBRIDGE
つかえるITを、世界から。

株式会社オーシャンブリッジ
〒107-0051 東京都港区元赤坂1-5-12　住友不動産元赤坂ビル7F
Web : https://www.oceanbridge.jp/
Email : userlock@oceanbridge.jp