DIGITAL DEVELOPMENT SYSTEMS

導入製品：Multi Authentication EVEMA

お客様導入事例　山形県 村山市役所 様

システムインテグレータ：株式会社 ハイテックシステム

次世代を見据えてマイナンバー利用事務系とLGWAN接続系の認証共通化を実践

～ Active Directory連携を活用したID管理で実務の利便性を大幅に向上 ～

山形県村山市では、三層の対策に対するシステム管理者の負担軽減、職員の利便性向上、そして次世代を見据えた認証共通化を実現するためEVEMAを導入されました。マイナンバーカードを活用するため、マイナンバーカード認証を中心に顔認証も取り入れた、パスワード不要な認証環境を構築しました。これにより職員のマイナンバーカード取得率は99%を達成。マイナンバーカード未取得者に配慮した認証環境も準備。セキュリティを確保しつつ利便性の向上も実現されました。Active Directory（以下、AD）連携を利用したユーザー管理の工夫や今後の展開についてお話を伺いました。

■ 複雑なユーザー管理からの解放と未来に向けた認証環境の構想

当時利用していた静脈認証システムは、ADと別々にユーザー管理が必要だったこと、Windowsの大型アップデートもPC毎に対応が必要など、とにかく運用に手間がかかることがシステム管理者として負担に感じていました。また、静脈認証自体の反応は良いのですが、デバイスが大きく運用に課題を感じていました。最終的に認証基盤はクラウドに移行して、ゼロトラストセキュリティを意識した環境にしたいという思いがありましたので、次期システムはそのための下地作りの第一歩として、マイナンバー利用事務系とLGWAN接続系でユーザー管理や認証を共通化し、とにかく職員自身によるパスワード管理を無くすことに重点を置くこととしました。
EVEMA導入の決め手は、職員の取得を推進していたマイナンバーカードを認証に利用できること、その認証には利用者証明用電子証明書を使うことでランニングコストが抑えられること、顔認証の精度が良かったこと、AD連携による管理者負担の軽減が図れることです。

■ マイナンバーカード認証を中心においたパスワード不要の認証環境を構築

職員には１人１台のノートPCを渡しています。三層の対策はαモデルで、マイナンバー利用事務系、LGWAN接続系で約400名がEVEMAを使用しています。ポリシーでは、ログインはマイナンバーカード認証を使用、ロック解除は顔認証を使用としており、認証方法はマイナンバー利用事務系もLGWAN接続系も同じとしました。具体的には、Windowsログオンはマイナンバーカード認証＋PIN、ロック解除は顔認証を用います。当市職員（学校を除く）のマイナンバーカード取得率は99%ですが、マイナンバーカード未取得の職員のPCは、ICカード認証＋顔認証を求める設定になっています。認証設定が違うため、該当職員は支給されたPC以外の他のPCにはログインできません。
業務アプリの認証は、IDマネージャーを利用し、グループウェアのログイン、セキュアブラウザに対しての認証でシングルサインオンに寄せた動きを付与しています。Microsoft Edgeで通常モードとIEモードは併用できないため、IEモードで動いている基幹システムは現在でもパスワードを使用していることが課題です。将来的に基幹システムがEdgeに対応したらシングルサインオンを実装したいと考えます。

導入事例：山形県 村山市役所 様

Multi Authentication
EVEMA

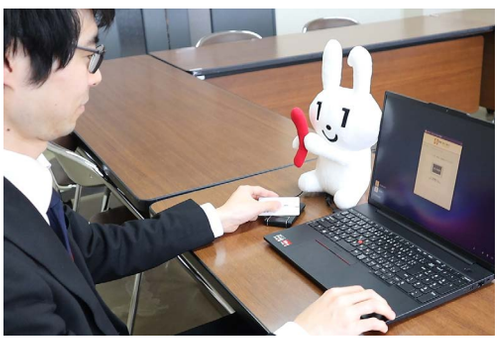
■ セキュリティを確保しつつ利便性も重視。実務に即した認証環境を提供

LGWAN 接続系がメイン業務の職員は、マイナンバー利用事務系に入れないよう、グループポリシーで制限をかけています。AD で LGWAN 接続系を利用するグループ、マイナンバー利用事務系を利用するグループを作り、さらにその中に課ごとにグループを作成し管理しています。認証方法は共通化しつつも、AD 連携を利用してアクセス権の管理も実装できています。その一方で、LGWAN 接続系がメイン業務の部署であっても、業務上マイナンバー利用事務系への接続が必要な部署には、EVEMA の代理認証でマイナンバー利用事務系へ接続ができる PC を課ごとに 1 台用意しています。マイナンバー利用事務系の管理設定に課ごとに使える共通 ID とグループを用意し 1 対 N 認証で運用しています。この設定が可能であることも EVEMA の良いところだと思っています。
また、EVEMA の顔認証は PC 内蔵カメラで利用できるのも良いところです。職員は、朝 PC を立ち上げる時に IC カードリーダーを接続しますが、PC を持ち歩かない職員は接続したままで、持ち歩く時はリーダーを抜いていきます。そのため、ロック解除は利便性を重視し顔認証にしています。利用場面で認証を使い分けできるのも EVEMA の良いところです。
職員がマイナンバーカードを忘れた場合は、リモート接続して管理者が代わりにテンポラリーパスワードを用いてログインをしています。その後は通常通り顔認証でロック解除です。セキュリティ面から考えると例え管理者であっても利用者の ID を使用するのはよくないと考えているのでこの運用としました。

■ マイナンバーカード更新対応が今後の課題

EVEMA の運用開始と同時期に PC も入れ替えました。職員は PC が変わったため認証方法も変更したという認識だと思います。認証に必要なマイナンバーカードの登録と顔認証の登録は、管理者 3 名で全部署（施設）を訪問し 1 ヶ月で実施しました。登録作業は、 1 人 2 分程度ですが、職員にマイナンバーカードを持ち歩く習慣がなかったり PIN を忘れていたりなどで、登録作業が滞ることはありました。学校も事務職と教務主任、教頭、校長の登録を実施しました。
PC が変わり、パスワードを入力することがなくなったため狙った効果はある程度出たと思います。
一方マイナンバーカードの利用者証明用電子証明書が 5 年に 1 回更新となることは懸念事項です。 5 年以内に全職員の更新時期が必ずやってくるため、その対策も考えないといけませんが、マイナンバーカードの PPID（Pairwise Pseudonymous Identifier）が活かせるようになるのが理想です。仮にマイナンバーカードが利用者証明用電子証明書を PIN なしで利用できるようになったとしても、マイナンバーカード認証＋顔認証の二要素認証にするなど、EVEMA なら認証要素を簡単に変更できるのも良いところだと思います。

■ 自治体が理想とするセキュリティ像に応えるソリューション提案に期待



当市ではテレワークの仕組みはあるのですが思ったほど利用されていません。今後の普及を考えると仮想業務サーバーを立てるなど、テレワーク環境の構築も必要でその時はセキュリティ対策も考えないといけません。また、管理者業務の引き継ぎの観点ではドメイン全体の設定を一覧でレポートできる機能があると助かります。
現在はオンプレで運用していますが、将来的にはクラウドベースでEntra IDを使用し、Microsoft 365を使うことは避けられないと考えます。そのような場合でもEntra IDの仕組みにある二要素認証を使用するのか、それともクラウド認証を使用するのか、他社にはできないDDSならではの提案を期待しています。また、実際に現場がかかえているリスクや課題を認識した上で、自治体が考える理想のセキュリティ像の実現に応えられるようなソリューションも期待しています。

202404_D240350

DIGITAL DEVELOPMENT SYSTEMS

株式会社 ディー・ディー・エス
https://www.dds.co.jp/ja/
本　　社：〒450-0002　名古屋市中村区名駅三丁目9番6号 アルティメイト名駅2nd 8F
TEL：052-955-6600（代表）　FAX：052-583-7800
東京支社：〒108-0075　東京都港区港南二丁目16番1号 品川イーストワンタワー7F
TEL：03-6894-4098（代表）　FAX：03-6894-4099

地方創生 SDGs 官民連携プラットフォーム
私たちは持続可能な開発目標（SDGs）を支援しています。

TW100 Telework Pioneer

お問い合わせ