



厳格な本人確認強化策が業務効率と 職員のセキュリティ意識向上を後押し

～ 認証方式を自由に組み合わせ、セキュリティレベルに応じた納得の本人確認環境を構築 ～

高知市では、急速なデジタル化に伴う情報漏えいなどのリスク対策として、全職員約4,700名を対象にPC利用時の本人認証強化としてEVE MAを導入されました。マイナンバーカードの利用促進、代理認証機能とマスク顔認証での円滑な窓口業務、シングルサインオン（以下、SSO）を利用した業務効率向上、そしてLGWAN接続系に多要素認証を導入したことによる職員の変化など、EVE MAがもたらした効果についてお話を伺いました。

■ 情報漏えい対策にLGWAN接続系にも厳格な本人認証を取り入れたい

自治体強化時に導入した以前の認証システムは、必要とされるセキュリティレベルに応じた認証が手のひら静脈認証しかなく、別途購入する認証機器も高額であることが課題と感じていました。また、急速なデジタル化に伴う情報漏えいなどのリスク対策も課題でしたので、マイナンバー利用事務系だけでなく、LGWAN接続系への多要素認証導入も重要でした。そこで今回の認証システム更改では、三層分離された庁内ネットワーク利用時、庁内でのモバイル端末利用時、テレワークでのモバイル端末利用時などPCの利用シーンと、取り扱う情報の重要度に応じて最適な認証方式を自由に選択できること、その上で本人認証強化を実現することを目指しました。

システム更改のプロポーザルを実施し、高知電子計算センター（以下KCC）様の提案は本市が求めるさまざまな認証方式に対応していたこと、ネットワークなどPCの使用用途に応じた柔軟な対応ができることを評価しました。特に重視したのはマイナンバーカード認証でした。また、窓口共有端末に対応する代理認証機能、テレワークで利用する仮想端末への対応、SSOも加点ポイントでした。

■ マイナンバーカード認証、顔認証などセキュリティレベルと利便性を熟慮した認証選択

庁内ネットワークはマイナンバー利用事務系、LGWAN接続系、テレワーク系の3つに分かれており、今回それぞれのPC認証にEVE MAを適用しました。

マイナンバー利用事務系は、手のひら静脈を利用した認証から、顔認証とパスワード認証の多要素認証へ変更し、約1,600名が利用しています。高いセキュリティレベルの生体認証でありながら手軽であること、PC内蔵カメラを利用できるため、認証用機器購入費用を抑えられることが顔認証選定のポイントでした。

全職員約4,700名が利用するLGWAN接続系端末は、本人確認を厳格化するためICカード認証とパスワード認証の多要素認証に変更しました。ICカードはマイナンバーカード、もしくは職員が必ず所有する庁舎入退用ICカードを選択できるようにしています。また同じLGWAN接続系でも、管理職が所持するモバイルPCは、会議室など移動先での利用の負担にならないよう、顔認証とパスワード認証の多要素認証としました。

テレワーク用端末も顔認証とパスワード認証の多要素認証を採用しました。テレワークは昨年度（令和3年度）から本格化し、緊急時でも行政機能の維持をするために各課に最低1台専用端末を用意しています。庁外へ持ち出したテレワーク用端末は顔認証とパスワード認証で起動し、その後専用のテレワークシステムへ接続するための認証を経てLGWANへ接続し利用して



います。テレワークで可能なのはLGWAN系業務に限定となりますが、セキュアな環境を用意できたと考えています。またEVE MA導入に合わせ、全職員のパスワードポリシーの厳格化も実施いたしました。

■ 代理認証とSSOで利便性と業務効率アップ。職員からも高評価のマスク顔認証

職員から評価が高いのは、EVE MAの代理認証機能とSSOです。代理認証は、複数人で利用するマイナンバー利用事務系の共有端末で使用しています。これまでは共有端末利用者が業務終了時にWindowsをログオフし、次の担当が業務開始時に再度ログオンするというルールで運用していたため、交代に時間がかかり、窓口で来庁者をお待たせすることもありました。しかし、代理認証は利用者交代時のログオフ・ログオンが不要で、システムも途切れることなく次の担当にスムーズに引き継ぎできるので、来庁者をお待たせすることがなくなりました。システム管理者としては、代理認証時も個人を特定認証するのでセキュリティを担保している点も安心できるポイントです。

また、マイナンバー利用事務系はマスク顔も認証できる高精度顔認証を採用したので、新型コロナウイルス感染が収束していない現状、認証時にマスクを外す必要がなく来庁者を不快にすることが無いことも職員が評価しているポイントです。性能面では、高精度顔認証はとにかく認証精度が高く、認証時間も利用者が不安になるほど一瞬で終わること、色付きマスクや少し斜めからの認証も問題なく、認証にかかる時間が確実に短縮できています。夕方や休日出勤時など通常と光源が違う環境では認証がうまくいかないとの相談もありますが、認証しやすい状況を職員に案内するようにしています。

SSOは、全庁で日々利用するグループウェアや文書管理システム、出勤簿管理の庶務事務システムのログインなど9種類をあらかじめ設定して職員に提供しました。何度も認証をする必要がないため、業務効率も向上し職員は利便性を感じています。

■ 多要素認証導入で職員の情報セキュリティに対する意識向上が最大の効果

今回の導入で一番大きかったのは、LGWAN接続系に多要素認証を導入したことです。セキュリティポリシーが異なる小中学校など一部を除いて、市長以下、幹部職員も含めほぼ全職員が、通常業務で多要素認証に触れるようになりました。多要素認証の導入に合わせ、パスワードポリシーを強化しましたが、以前に比べパスワード忘却によるリセット依頼も少なくなりましたので、職員がパスワードを適切に管理していると思われれます。職員の情報セキュリティに対する意識向上が図られたと考えています。

■ マイナンバーカードや顔認証の本人確認の仕組みを最大限利用したい

現在一定数の職員がマイナンバーカードを利用していますが、取得率はまだ低いと感じています。普段の利用でマイナンバーカードの利便さや本人認証の明確さを実感してもらうことで、取得者を増やしたいため、詳細はお話しできませんが、LGWAN接続系の認証でマイナンバーカードとICカードで差をつける工夫をしています。庁内でもマイナンバーカード利用促進の動きがあることと、マイナンバーカードの証明書機能のスマホ搭載を国が予定していることから、今後マイナンバーカード認証を利用する職員が増えることを期待しています。職員のマイナンバーカード利用を広めるため、スマホ搭載が固まってきた際にはDDSからの利用提案が欲しいです。

また、顔認証も利用範囲を広げ、出退勤なども一元管理できるのが理想です。

日々の運用はKCCにサポートいただき、DDSには新しい機能の情報共有をいただいて導入を検討したいと考えます。



※ 記載の内容は2022年8月現在のものです。内容は予告無く変更する場合があります。 ※ 記載の社名、および製品名は、各社の商標または登録商標です。 202303_D220840_3



株式会社 ディー・ディー・エス
<https://www.dds.co.jp/ja/>

本社：〒460-0002 名古屋市中区丸の内三丁目6番41号 DDSビル7F
TEL：052-955-6600（代表） FAX：052-955-6610
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14F
TEL：03-6712-3561（営業本部） FAX：03-6712-8762