



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

続編

～ Active Directory連携を活用したID管理と高精度な失効確認の実現 ～

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を導入しています。認証基盤はクラウドへの移行とゼロトラストセキュリティを意識した環境を目指しており、その第一歩として職員のマイナンバーカード（取得率99%を達成）を活用した認証環境を構築しました。

具体的には、Windowsログオンはマイナンバーカード認証（利用者証明用電子証明書を使用）とPINを用い、ロック解除には利便性を重視した顔認証を取り入れています。また、EVEMAの導入により、AD連携を活用したID管理を通じて、システム管理者の負担軽減を図りつつ、アクセス権の管理も実装しています。

前回の取材から約1年半。この間マイナンバーカード認証の運用改善に積極的に取り組まれ、より一層高度化した運用を実現されました。新たに取組まれた課題や改善方法についてお話を伺いました。

■ 実運用における改善を実施。失効確認の高度化と現在の課題

マイナンバーカードを認証の主軸とすることで、職員によるパスワード管理の負荷は解消されましたが、セキュリティを確保しつつ利便性を向上させるため、認証の核となる利用者証明書の失効確認については、実運用の中でさらなる高度化を図りました。

1. 失効確認方式の変更(CRLからOCSPへ)

導入後、村山市では、マイナンバーカードの利用者証明用電子証明書の失効確認を、従来のCRL (Certification Revocation List: 証明書失効リスト) 提供方式から、よりリアルタイムな確認が可能なOCSP (Online Certificate Status Protocol) レスポンド方式へ変更しました。

この変更により、失効確認の仕組みは以下のように進化しました。

変更前：インターネット接続系から日次で失効リストを取得し確認する方式。

変更後：LGWAN接続系を通じて、認証の都度、地方認証プラットフォームへのリアルタイム確認ができる仕様へと変更。

また、従来のCRL提供方式では、マイナンバーカードの利用者証明用電子証明書が更新された際や、紛失などで失効した際に、都度EVEMA側での再登録が必要でした。OCSP方式への切り替えにより、利用者証明用電子証明書の新旧情報の紐づけが可能となり、認証時にEVEMAの登録情報を自動で更新できるようになりました。

このOCSP方式への切り替えにより、より厳格で即時性の高いセキュリティが確立し、認証環境の信頼性が向上しました。また、更新時の利便性も高まったことで、運用効率の大幅な改善にもつながっています。



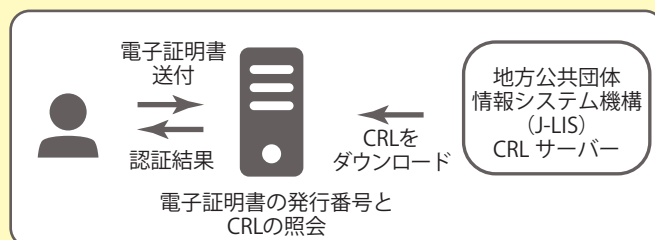
2. 現在の運用課題

失効確認の高度化を進める一方で、現在の運用には時間的な制約が残っています。地方認証プラットフォームは窓口での利用を想定されて構築されたものであるため、夜間の利用が制限されています。このため、夜間帯に認証が必要な場合は、OCSPレスポнда方式が利用できず、一時的にCRL方式に切り替えて確認を行う必要があります。当市としては、地方認証プラットフォームでの失効確認が24時間利用可能となることを期待しつつ、インターネット接続系での利用も想定し、JPKIでのOCSP方式による失効確認への対応も検討をしていきたいです。

電子証明書の有効性確認の方式は、「CRL提供方式」と「OCSPレスポнда方式」の2種類があります。

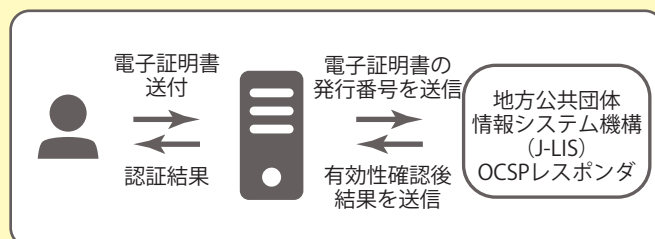
CRL提供方式

CRLとは、電子証明書の失効情報の一覧です。CRL提供方式とは、この一覧を定期的（1日1回等）に取得する方式です。J-LISから提供されるCRLは、1日単位で更新されており、これをダウンロードして、電子証明書の発行番号と照合することで、電子証明書の有効性を確認しています。CRL提供方式はオフラインでも確認できることが特徴です。



OCSPレスポнда方式

OCSPとは、電子証明書の有効性を確認するための通信プロトコルです。OCSPレスポнда方式とは、特定の電子証明書の有効性の照会について、「OCSPレスポнда」と呼ばれる応答用サーバから個別に回答する方式です。OCSPレスポндаには、失効情報が保存されており、15分単位で更新されています。OCSPレスポндаは、失効情報とサービス利用者の電子証明書の発行番号を照合し、有効性を確認します。OCSPレスポнда方式はリアルタイムに確認できることが特徴です。



参照：<https://www.digital.go.jp/policies/mynumber/private-business/jpki-introduction>

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

今回の対応は、当市からの要望により、DDSにて迅速に対応いただきました。マイナンバーカードの職員からの普及といった目的も、取得率99%を達成しており、一定の効果を発揮しています。職員のPCはEVEMAの運用開始と同時期に入れ替わっており、「パスワードを入力することがなくなった」「マイナポータルやマイナ保険証の利用時のPIN忘れがなくなった」という狙った効果も既に出ています。

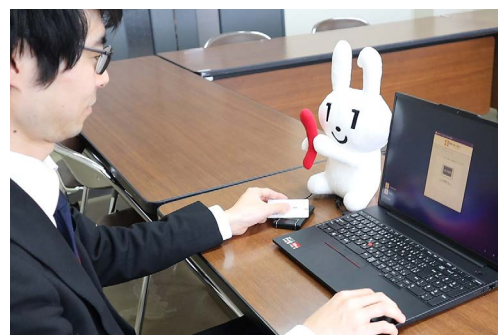
マイナンバーカードのスマートフォン搭載（電子証明書機能や券面記載情報をスマートフォンに移し、スマホ単体で本人確認や電子署名を行う仕組み）も始まっており、カードを持ち歩かなくとも、スマートフォンをかざして利用できるようになることを期待しています。また今後は、オンプレミス環境からEntra IDを使用したクラウドベースへの移行など、

次世代を見据えた課題が残ります。EVEMAであれば、仮にマイナンバーカードの仕様が変わり、PINなしで利用できるようになったとしても、顔認証との二要素認証に簡単に変更できる柔軟性があります。DDSには、引き続き自治体が考える理想のセキュリティ像の実現に向けたソリューション提案を期待しています。

※ 記載の内容は取材時（2025年11月）のものです。内容は予告無く変更する場合があります。

※ EVEMAは株式会社ディー・ディー・エスの登録商標です。その他記載の社名、および製品名は、各社の商標または登録商標です。

202511_D250860



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

本社：〒160-0023 東京都新宿区西新宿6-12-1 パークウエストビル 8F
TEL：03-6821-1630（代表） FAX：03-5321-5566

名古屋支社：〒450-0002 愛知県名古屋市中村区名駅3-9-6 アルティメイト名駅2nd 8F
TEL：052-955-6600（代表） FAX：052-583-7800

