2025 年 4 月 28 日　全 7 頁

急速に広がる資格情報等のデジタル化

利用時に気をつけるポイントと求められるデジタルリテラシー

経済調査部　研究員　田邉 美穂

[要約]

■ 2025 年 3 月 24 日よりマイナンバーカードと運転免許証および運転経歴証明書の一体化が開始された。このように、クレデンシャル（特定の資格や権利を証明するための情報や証明書）のデジタル化を進めることで、デジタルサービスを利用した情報管理や本人確認、資格および権利証明等を可能とする取り組みは、近年急速に広がっている。

■ クレデンシャルのデジタル化が進む背景として、現在の一般的な手法（利用者が証明書等の画像ファイルや PDF ファイルを作成し、デジタルサービス上に添付してアップロードする手法等）が、デジタル環境に適していないことが挙げられる。これらはデジタル技術のメリットを十分に活かしきれていない結果、①真正性（本物であること）の確認が困難、②プライバシーの懸念、③手続きの煩雑さ、といった課題が生じている。

■ デジタル化されたクレデンシャルを利用したサービスの実用化は既に始まっている。その一方で、クレデンシャルをさまざまなサービスで横断的に利用するために必要となる相互運用性については、まだ検討段階にある。そのため、クレデンシャルのデジタル化は過渡期にあるといえる。

■ このような状況下で、デジタル化されたクレデンシャルを利用したサービスを実際に利用することになった場合、利用者自身がクレデンシャルを提示する目的を正しく理解し、利用するサービスを選択する力を身につけることが重要となる。新しい技術やサービスを適切に理解し、目的に応じた選択を行うことで、デジタルに最適化したクレデンシャルの利便性と安全性を最大限に活用することができるだろう。

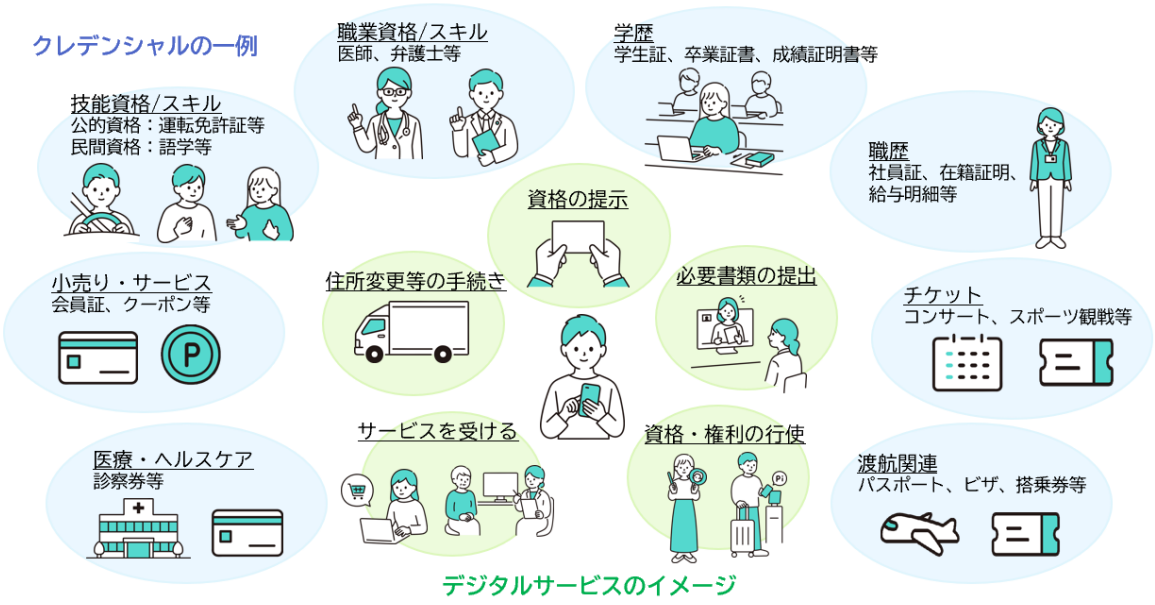
大和証券グループ　株式会社大和総研 丸の内オフィス　〒100-6756 東京都千代田区丸の内一丁目 9 番 1 号 グラントウキョウノースタワー

1. はじめに

2025 年 3 月 24 日よりマイナンバーカードと運転免許証および運転経歴証明書の一体化が開始された。オンラインで住所変更手続きや講習受講が可能になる等、運転免許証に関するデジタルサービスが利用できるようになったことで大きな話題となった。こうした際に重要になるのが、クレデンシャルという特定の資格や権利を証明するための情報や証明書である。クレデンシャルの種類は、運転免許証や医師・弁護士資格等の公的な資格を証明するものから、コンサートやスポーツ観戦チケット等のイベントへの参加権利、会員証やクーポン等の利用権利を証明するものまで多岐にわたる。このクレデンシャルのデジタル化を進めることで、デジタルサービスを利用した情報管理や本人確認、資格および権利証明等を可能とする取り組みは、近年急速に広がっている（図表 1）。

前回のレポート[1]では、デジタル ID（オンラインで個人を特定/証明するための識別子、属性情報およびクレデンシャルの集合）の管理方法や課題について整理した。その中で、デジタル ID の一部であるデジタル証明書をはじめとしたクレデンシャルのデジタル化について、既に実用化が始まっていることを述べた。今回のレポートでは、このクレデンシャルのデジタル化に着目し、直近の動向や実用化が進む今だからこそ気をつけるべきポイントについて整理する。

図表 1　クレデンシャルのデジタル化のイメージ



（出所）大和総研作成（イラストはソコスト（https://soco-st.com/））

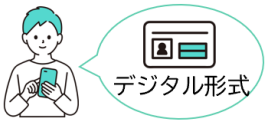
[1] 田邉美穂[2024]「デジタル化が進む個人情報はこれからどのように管理するべきか：自己主権型アイデンティティ（SSI）の課題と未来」大和総研レポート（2025 年 4 月 1 日）

2. クレデンシャルのデジタル化が進む背景と現状

アナログ手法を単純に電子化するだけではデジタル技術のメリットを十分活かせない

今までアナログ（対面）で行ってきた手続きやサービスのデジタル化が進み、デジタルサービス上でクレデンシャルを提示する機会も増えてきた。現在一般的に多く利用されているのは、利用者が証明書等の画像ファイルや PDF ファイルを作成し、デジタルサービス上に添付してアップロードする手法である。しかし、この手法は、従来の対面で行っていたクレデンシャル確認作業の流れを、そのまま電子化したものにすぎない。そのため、デジタル技術が持つメリットを十分に活かしきれておらず、そこにはいくつかの課題が存在する（図表 2）。

図表 2　クレデンシャルのデジタル化が進む背景

	現在一般的な手法  画像撮影・PDF化	クレデンシャルのデジタル化  デジタル形式
真正性（※）の確認が困難 （※）本物であること	クレデンシャルの複製にあたるため • 改ざん/偽造が容易 • 真正性の確認が難しい	デジタルに最適化することで • 改ざん/偽造が難しい仕組みが構築可能 • 真正性の確認が容易
プライバシーの懸念	提示方法等がサービスごとに異なるため • サービス提供側の行っている セキュリティ対策に依存	デジタルに最適化することで • 暗号化技術等、高いセキュリティ対策が 実現可能
手続きの煩雑さ	利用するサービスにあわせて、 提示するクレデンシャルの準備が必要	提示するクレデンシャルの準備から確認 までの全ての手続きがデジタル上で完結

（出所）大和総研作成（イラストはソコスト（https://soco-st.com/））

1 つ目の課題：真正性（本物であること）の確認が困難

先述の現在一般的に多く利用されている手法で用いる画像ファイルや PDF ファイルは容易に改ざんされる可能性がある。その結果、偽造された証明書が提出されるリスクは増大する。手動確認や機械的チェックを行っても提出されたファイルから改ざんを検出し、真正性の確認をすることは容易ではない。

2 つ目の課題：プライバシーの懸念

クレデンシャルには個人情報が含まれていることが多い。画像ファイルや PDF ファイルの送信時や保存時に適切なセキュリティ対策（暗号化や保護等）がされていない場合、情報漏洩のリスクがある。

3 つ目の課題：手続きの煩雑さ

クレデンシャル提示側は、証明書のスキャンや撮影、ファイル形式の変換といったアナログ由来の手作業をデジタルデバイス上で行うことで、手間と時間がかかるケースがある。またクレ

デンシャル受領側も、提示された多様な形式のファイルを個別に確認する必要がある。このように、デジタル環境でありながら目視確認の煩雑さや、機械による画像認識の精度限界に起因する確認作業の困難さがボトルネックとなっている。

デジタル環境に適した仕組みを検討することで、課題解消が期待できる

これら 3 つの課題の原因は、現状クレデンシャルの大半が対面利用を想定としたアナログ形式のままであることであろう。それにより、現在一般的に多く利用されている手法が、アナログとデジタルの環境の違いにうまく対応できていない。そのため、以下のようにクレデンシャルをデジタル化し、デジタル環境に適した仕組みを検討することで課題の解消が期待できる。

1 つ目の真正性の担保に関しては、デジタル署名等の技術を利用することで、クレデンシャルが信頼できる機関から発行されたものであることや、改ざんされていないことがデジタル上で確認できるようになる。2 つ目のプライバシーの懸念に関しては、暗号化技術やブロックチェーン技術等の利用により改ざんが困難な仕組みを構築することや高いセキュリティ対策を実現することが可能だ。また、クレデンシャルのデジタル化の手法によっては、必要な情報に限って提示することも可能となる。3 つ目の手続きの煩雑さに関しても、提示するクレデンシャルの準備から確認までの全ての手続きが、デジタルに最適化されたプロセスで処理できれば、課題解消が期待できる。

日本におけるクレデンシャルのデジタル化に関する取り組みは活発化している

クレデンシャルのデジタル化を推進する取り組みは、近年日本では政府や民間企業を問わず、活発化している。特に政府の取り組みをみると、2025 年 3 月だけでもデジタル庁を中心に多くの取り組みが行われている。例を挙げると、クレデンシャルのデジタル化の実現手法として注目されている VC/VDC（Verifiable Credential、検証可能なクレデンシャル）の活用に向け、適切な運用ルールや社会実装に向けた課題を議論する「Verifiable Credential（VC/VDC）の活用におけるガバナンスに関する有識者会議」[2]が設置された。ほかにも、クレデンシャルとマイナンバーを組み合わせた実証実験やデモンストレーション[3]も複数行われている（図表 3）。

[2] デジタル庁ウェブサイト、「Verifiable Credential（VC/VDC）の活用におけるガバナンスに関する有識者会議」

[3] デジタル庁ウェブサイト、「穂坂デジタル副大臣が『マイナンバーカード機能のスマートフォン搭載を活用したセルフレジ年齢確認デモンストレーション』の視察を行いました」（2025 年 3 月 18 日）および 「岸デジタル大臣政務官が『マイナンバーカード利活用：在学資格証明デジタル化実証実験』に関する共同発表会登壇・デモンストレーション視察を行いました」（2025 年 3 月 28 日）、「穂坂デジタル副大臣が『ライブイベントにおけるチケット不正転売防止・業務効率化実証実験』の視察を行いました」（2025 年 4 月 4 日）

図表 3　デジタル庁が実施したクレデンシャルのデジタル化に関する実証実験等（2025 年 3 月）

セルフレジ年齢確認デモンストレーション

公開日：2025年3月18日

① セルフレジで年齢確認対象商品を読み取る
② レジ画面の指示に従い、デジタルIDウォレットからマイナンバーカードを開く
③ 要求された情報の提供を承認（例：20歳以上であること）
④ 20歳以上であることの確認が完了、支払手続きへ

ポイント
現在デジタル庁で進めている
マイナンバーカード機能のスマートフォン搭載の活用可能性を検証

在学資格証明デジタル化実証実験

公開日：2025年3月28日

① 学術機関と連携し、利用者（大学生）にデジタル在学証明書をVCで発行
② 検証機関（交通機関）のサービス上で、VCを利用し学割の適用を受けたチケットを購入

ポイント
在学証明以外の資格情報（成績証明や卒業証明等）の利用や、文教分野の他
様々な利用シーンの拡大をにらみ技術検証を行っている

ライブイベントにおけるチケット不正転売防止・業務効率化実証実験

公開日：2025年4月4日

① 抽選申込時にマイナンバーカード＋顔登録し、認証済みアカウント作成
② 認証済みアカウントのみ抽選を実施し、当選者に対して登録された顔情報と紐づいたQRコードを発行
③ 入場時「QRコード＋顔」を会場設置端末で読み取り、チケット保有者の本人確認を実施

ポイント
昨年度に引き続き、不正転売防止・本人確認業務の効率化を図り、社会実装に繋げることを目的に実施
サブアカウントでの複数申込・購入防止やなりすまし入場防止の効果が期待される

（注）一番下の「ライブイベントにおけるチケット不正転売防止・業務効率化実証実験」について、
公開日は 2025 年 4 月 4 日だが、実際の視察は 3 月中（3/21 および 3/29）に行われている。
（出所）各種資料（脚注 3）より大和総研作成（イラストはソコスト（https://soco-st.com/））

3. デジタル化されたクレデンシャルを利用する場面で気をつけること

クレデンシャルを提示する目的を正しく理解することが重要

デジタル化されたクレデンシャルを利用したサービスの実用化は既に始まっている。このようなクレデンシャルはさまざまなサービスで横断的に利用できることが理想だ。しかし、そのために必要となる相互運用性の実現に向けた、使用技術の標準化や法整備等はまだ検討段階にある。このことから、クレデンシャルのデジタル化は現在過渡期にあるといえるだろう。このような状況下でも、クレデンシャルのデジタル化を利用したサービスは徐々に増えつつある現状を踏まえると、これらのサービスを利用する機会も今後増えていくと思われる。

このようなサービスを利用する際には、利用者自身がクレデンシャルを提示する目的を正しく理解することが重要だ。先述の通り、公的資格の証明やイベントへの参加権利等、クレデンシャルの種類は多岐にわたる（前掲図表 1 参照）。したがって、クレデンシャルを提示する目的によっては、クレデンシャルの提示とあわせて厳密な本人確認が必要になる場合もあれば、クレデンシャルの提示のみで足りる場合も考えられる。そのため、利用者が提供する情報の範囲やサービスに求められる機能が適切かを判断する上で、クレデンシャルを提示する目的の理解が重要となる。

クレデンシャルを提示する目的と利用するサービスに相違がないか確認も必要

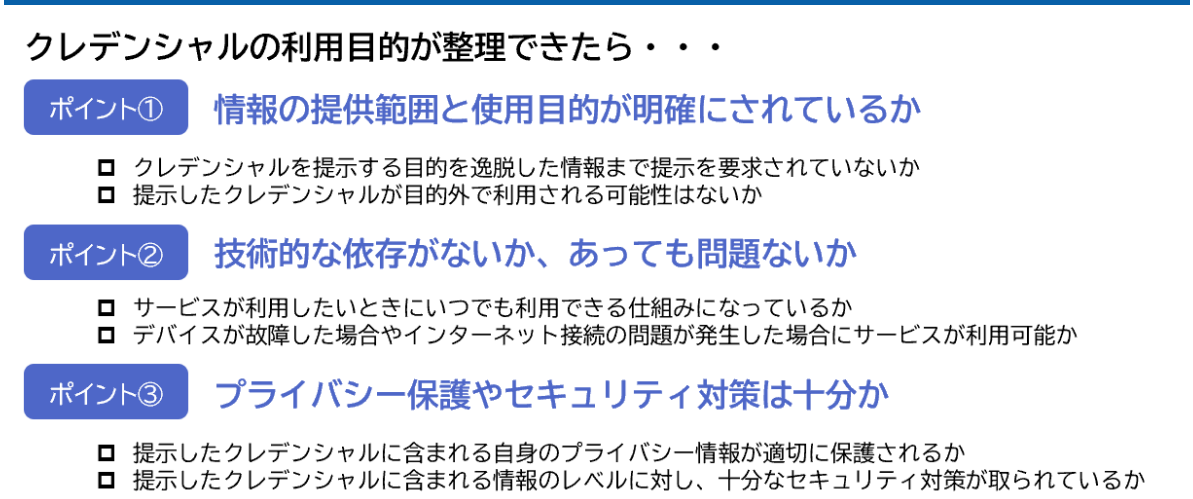
クレデンシャルを提示する目的が整理できたら、次に利用するサービスに問題がないかの確認も行う必要がある。そのためのポイントは大きく 3 つに分けられる（図表 4）。

1 つ目は、利用するサービスにおいて、情報の提供範囲と使用目的が明確にされているかを確認することである。利用者はクレデンシャルを提示する目的を逸脱した情報まで提示を要求されていないか、また提示した情報が目的外で利用されないか等を慎重に確認する必要がある。一方で、サービス提供者には、これらの情報を明瞭に説明する責任がある。特に、デジタル化されたクレデンシャルに不慣れな利用者が多い現時点では、提示方法や提示した情報を視覚的に把握しやすいインターフェースを提供する等、丁寧なサポートが求められる。

2 つ目は、技術的な依存がないか、あっても問題がないかを確認することである。利用者は、デバイスが故障した場合やインターネット接続の問題が発生した場合にサービスが利用可能かどうかを確認する必要がある。ただし、クレデンシャルを提示する目的によっては即時性が不要の場合もあり、目的に応じたサービス要件を満たしているか、適切な判断が求められる。一方で、サービス提供者にとって代替手段を検討することは、デジタルデバイド[4]への対応にも関連するため、これらの事態に対する準備と検討は必須となる。

3 つ目は、利用するサービスのプライバシー保護やセキュリティ対策は十分かを確認することである。利用者は、自身のプライバシーが適切に保護されるか、セキュリティ対策が十分かどうかを、提示するクレデンシャルに含まれる情報のレベルにあわせて判断する必要がある。例えば厳密な本人確認が必要になる場合は、提示するクレデンシャルも個人情報を多く含むものになる可能性が高いため、高度なセキュリティ対策が求められる。一方で、サービス提供者はプライバシー保護やセキュリティ対策を適切に実施し、利用者に対して責任を明確に説明する必要がある。

図表 4　デジタル化されたクレデンシャルを利用する場面で気をつけること



（出所）大和総研作成

[4] デジタルデバイド（デジタル格差）とは、デジタル技術やデジタルサービスの利用能力の違いによって生じる社会的な格差のことを指す。

このように、デジタル技術の進展に伴い、サービスもデジタルに適用した形へ変化していく。この結果、クレデンシャルのようにこれまで物理的にしか存在していなかったものも、デジタル形式に移行していくことが十分に予期できる。新しい技術やサービスを過渡期だからと忌避するのではなく、利用者自身で判断する力（リテラシー）を身につけ、積極的に利用していくことが重要だ。今回提起したポイントは、難しく見えるかもしれないが、いずれもデジタルリテラシーの基本に相当する。新しい技術やサービスを適切に理解し、目的に応じた選択を行うことで、デジタル化したクレデンシャルの利便性と安全性を最大限に活用することができるだろう。

以上