電子データ化された証明書類を利用した身元確認手法の検討

石井 宏治, 坂根 栄作, 合田 憲人

国立情報学研究所

k_ishii@nii.ac.jp

A study of identity verification methods using identification documents on electronic media

Koji Ishii, Eisaku Sakane, Kento Aida

National Institute of Informatics

概要

コロナ禍を契機として急速に進展するデジタル化により学生証や在籍証明書などについても電子データ化されたものが見受けられるようになってきた。本稿ではスマートフォン上に表示する学生証や社員証および電子署名付きの在籍証明書等を利用して，所属組織を通じた身元確認をプラスチックカードや紙に印字されたものを利用する場合と同等以上のレベルで行う方法を検討する。

1　はじめに

学校や会社などが発行する学生証や社員証，在籍証明書といった書類は，発行元の組織が構成員の身分を認めるあるいは構成員の身分を第三者に対して保証するもので，これらを利用することで発行元の組織もしくは第三者は，発行対象者当人が発行元の組織に実在する特定の存在であることを確認（身元確認）することができる。

学生証や社員証，在籍証明書といった書類は，プラスチックカードや紙に印字されたものが一般的ではあるが，昨今のデジタル化の進展に伴い，電子データ化された学生証や在籍証明書などが見受けられるようになってきたことから，本稿ではスマートフォン上に表示する学生証や社員証および電子署名付きの在籍証明書等を利用して，所属組織を通じた身元確認を行う方法を検討する。

2　従来手法における課題

国立情報学研究所 (NII) では，産業界を含めた利用者層の幅広い共用計算環境基盤である革新的ハイパフォーマンス・コンピューティング・インフラ (High Performance Computing Infrastructure: HPCI [1]) における利用者の身元確認を行う手法として，利用者が所属する組織を通じて，つまり「どこそこのだれだれ」として確認する方法を確立している。 [2]

身元確認を物理的に対面しての実施およびテレビ会議を通じた遠隔で行う場合，身元識別の属性情報がプラスチックカードや紙に印字されたものを「身分証明書」として利用することを前提としているが，電子データ化された書類として，電子データ（PDF 形式）で原本を提出できる証明書類（以下「電子データ原本の証明書類」という），スマートフォン等に表示して使用する証明書類（以下「スマホ等に表示の証明書類」という）なども利用されて始めていることから，本節では電子データ化された証明書類を用いた身元確認の実施に係る課題等を整理する。

2.1　身元確認のための書類

我が国の官公庁が発行する旅券，運転免許証，個人番号カードなどは，いわゆる「身分証明書」として社会一般的に認知されており，個人の自己申告ならびに証明書類の記載事項の身元識別の属性情報を確認して当該本人が特定の存在であることを判断する「身元確認」に利用されている。身元確認の認証強度として求められるレベル（保証レベル）は，表 1 に掲げる身元確認保証レベル (Identity Assurance Level: IAL) として定義される。[3]

また，学生証や社員証，在籍証明書などは，学校や会社などが構成員の身分を認めるあるいは構成員の身分を第三者に対して保証する書類であることから，発行元の組織が信頼できる場合に限り「身分証明書」として機能すると考えられる。

表 1　身元確認保証レベル

保証レベル	定義
IAL1	特定の実在人物と結びつける必要はなく，自己申告による属性情報の登録でよい。
IAL2	身元識別の属性情報を遠隔もしくは対面にて確認する。
IAL3	特定の訓練を受けた担当者によって身元識別の属性情報を対面にて確認する。

2.1.1　公文書

旅券，運転免許証，個人番号カード（以下「公文書」という。）は，いずれも物理的な書類として存在するもので，プラスチックカードもしくは紙に身元識別の属性情報が印字されたものである。公文書は，書類様式が定まったものであることから公文書を用いて個人を身元確認する方法は汎用的なものとして確立されている。

2.1.2　各種組織が発行する証明書類

多種多様な組織が発行元となる学生証や社員証，在籍証明書などの構成員の身分を認めるあるいは構成員の身分を第三者に対して保証する書類（以下「証明書類」という。）は，発行元ごとに書類様式が異なるため，書類単位で記載事項を精査して身元確認に利用可能な書類であるかを判断する必要がある。

2.2　HPCI における身元確認

HPCI では，利用者の身元確認を大学や研究機関に設置の受付窓口（最寄りセンター）において保証レベル IAL2 として，物理的に対面しての実施ならびにテレビ会議を通じた遠隔で実施する際，学校や会社などの組織が発行する証明書類を利用する。

また身元確認の前提条件には以下に掲げる事項が設定されている。

1. 大学，研究機関や企業に所属する者が課題選定を経て HPCI の資源を利用することができる
2. 課題選定時に利用者の所属組織の同定を行う
3. 利用者の身元確認は，所属組織同定後に実施する

2.3　証明書類の要件

身元確認を受ける者（申請者）は，所属組織が発行元の顔写真付き証明書類を最寄りセンターに提示する必要がある。在籍証明書などでは顔写真が掲載されていない場合がある。顔写真のない証明書類を提示する場合には，申請者の顔写真付き公文書（運転免許証，旅券，個人番号カードなど）に記載の氏名との一致を最寄りセンターが確認することにより，当該証明書類を顔写真付きの証明書類と同等に扱う。

従来手法では，証明書類は以下のすべてを満たす場合に身元確認に利用できるものとしている。

1. 申請者の氏名と所属組織の名称が記載されていること。
2. 発行元の組織が本人の身分を認める旨の文言があること，あるいは本人の身分を第三者に対して保証していると判断できる記載があること。（「身分証」「学生証」「社員証」「職員証」「ID Card」「在籍証明書」など）
3. 在籍証明書やそれに相当する書類の場合は，以下のすべてを満たすこと。
   （a）本人が発行元の組織に所属していることを証明する書類であることが分かること
   （b）有効期間や有効期限の設定がない場合は，3 か月以内に発行されたものであること
   （c）発行元の組織の名称および印，あるいは発行者の氏名および印（もしくは署名）があること
4. 有効期限の設定がある書類の場合は，その期間内であること。
5. 手書きの文字がある場合は，判別可能な文字であること。
6. 名刺，入館証，労働条件通知書のいずれでもないこと。
7. 上記 2 を満たさない場合，証明書類として発行元が保証していることを確認できていること

2.4　課題

従来手法では，身元識別の属性情報がプラスチックカードや紙に印字された，つまり物理的に存在する証明書類を用いた確認を前提としており，電子データ化された証明書類の使用を想定していない。今後の更なるデジタル化の推進により学生証や社員証，在籍証明書などの証明書類の発行を電子データのみとする組織が現れることも否定できないため，申請者の身元確認における物理的に存在する証明書類の利用相当となる電子データ化された証明書類の利用方法の検討が課題となる。

電子データ化された証明書類を用いた身元確認の方法を検討するにあたり，以下に掲げる項目が要件とし

て挙げられる。

1. 申請者が所持する証明書類が電子データ化されたものであっても，身元確認に利用できるか否かを判断できること
2. 申請者が所持する電子データ化された証明書類に問題がないことを確認したうえで，人物の特定が可能であること

3　電子データ化された証明書類の利用

本節では，証明書類を用いた従来からの身元確認手法に対して，電子データ化された証明書類への対応を付け加えることを検討する。

3.1　物理的に存在する証明書類との比較

電子データ原本の証明書類の場合，電子データが原本であることから身元確認の際には証明書類のデータそのものを検証者に提出することが可能であり，これは紙に印字された在籍証明書などと同様である。検証者への提出に際しては，電子データであるため検証者が電子メールやオンラインストレージなどを介して受け取ることができれば比較的低コストで受け渡し可能といえる。一方，検証者に提示する際は，証明書類のデータをパソコンやスマートフォンなどのディバイス上に表示もしくは印刷したものを見せることになるため，紙に印字された在籍証明書など比べると準備に手間がかかるといえる。

スマホ等に表示の証明書類の場合，スマートフォン上で証明書類を表示することが前提となるため証明書類そのものを検証者に提出することはできない。提出を求められた場合，証明書類の原本の取り出しは不可能であることから証明書類の画面キャプチャーをファイル化あるいは印刷したものを写しとして提出することになる。提出する際に写しを利用することになるのはプラスチックカードに印字された学生証や社員証なども同様である。検証者に提示する際は，証明書類を表示した状態のスマートフォンを見せることになるためプラスチックカードに印字された学生証や社員証などと同様の手軽さといえる。

3.2　証明書類要件の拡張

電子データ原本の証明書類およびスマホ等に表示の証明書類が身元確認に利用できるか否かを判断するためには，前述の証明書類の記載事項の要件を満たすことを確認することは従来手法と同様に必須の事項である。

電子データ化された書類の場合，プラスチックカードや押印等のある紙の書類と比較して証明書類らしきものを捏造することは容易であることから，発行元の組織が本人性を担保していることが確認できること，例えば以下のような場合に利用可能な証明書類として取り扱う。

電子データ原本の証明書類の場合：

- 証明書類に電子署名が付与されており，署名者が書類を発行する責任を有している者であることを確認できること

スマホ等に表示の証明書類の場合：

1. 証明書類をスマホ等に表示して利用することを認めている発行元の組織公式の Web サイトが存在すること
2. 証明書類を表示するアプリケーションが発行元の組織公式のものであること
3. 証明書類を表示するアプリケーションの利用規約に証明書類として利用できることが記載されていること

3.3　身元確認手順

HPCI の身元確認は以下の二通りの方法で実施しているので，それぞれの方法に電子データ化された証明書類への対応を付加した手順を説明する。

1. 最寄りセンターの窓口にて対面
2. 最寄りセンターとのテレビ会議を通じて遠隔

3.3.1　物理的に対面して行う場合

■事前準備　申請者は，最寄りセンターに出向く際は，日時を調整のうえ訪問する。身元確認に電子データ原本の証明書類を使用する場合，電子署名の妥当性確認は最寄りセンターではなく NII の担当者が実施することから確認までに時間を要することもあるため訪問日時の調整時に電子メールで最寄りセンターに事前送付する。なお，スマホ等に表示の証明書類については，写しの事前送付の必要は無い。

最寄りセンターの担当者は，申請者からの訪問日時の調整依頼に電子データ原本の証明書類が含まれている場合，電子メールの発信元の氏名とメールアドレスが課題に登録されている申請者の情報と一致すること確認したうえで，電子署名を含む証明書類の記載事項の内容の確認を行っておく。

■最寄りセンターへの訪問　申請者は，持参した対面認証申請書を最寄りセンターへ対面にて提出すると共に，自らの所属組織が発行する証明書類を提示する。

表 2　物理的に対面して行う場合

身元確認に利用する書類	事前送付する書類	窓口に提示する書類
物理的に存在する証明書類	なし	物理的に存在する証明書類
電子データ原本の証明書類	電子データ原本の証明書類	電子データ原本の証明書類もしくは印刷したもの
スマホ等に表示の証明書類	なし	スマホ等に表示の証明書類

表 3　テレビ会議を通じた遠隔で行う場合

身元確認に利用する書類	事前送付する書類	テレビ会議上で提示する書類
物理的に存在する証明書類	物理的に存在する証明書類の写し	物理的に存在する証明書類
電子データ原本の証明書類	電子データ原本の証明書類	電子データ原本の証明書類もしくは印刷したもの
スマホ等に表示の証明書類	スマホ等に表示の証明書類の写し	スマホ等に表示の証明書類

電子データ原本の証明書類の場合，原本を各種ディバイス上に表示もしくは印刷したものを提示する。

スマホ等に表示の証明書類の場合，証明書類全体が確認できるように提示する。

■申請者の身元確認　身元確認の検証者である最寄りセンターの担当者は，以下に掲げる事項の全てを対面で確認することで，申請者が提示した証明書類に問題がないことを確認し，人物を特定する。

1. 証明書類の顔写真が申請者本人であること
2. 証明書類に記載の氏名が対面認証申請書に記載の氏名と一致すること
3. 証明書類に記載の氏名および所属組織が課題に登録されている申請者の情報と一致すること

電子データ原本の証明書類の場合，最寄りセンターの窓口で当該証明書類をパソコン等に表示してもらうか，紙に印刷したものを持参して貰い，事前送付された証明書類との突合せを行う。

スマホ等に表示の証明書類の場合，最寄りセンターの窓口ではスマートフォン上に表示した証明書類を提示してもらう。

身元確認できた申請者の証明書類の記載事項がある面の全てを複写して保管することで事後の追跡可能性を確保する。証明書類に第三者への開示が不適当な記載事項が存在する場合，非該当面に記載の属性情報のみで人物を特定できる場合に限り証明書類として使用できることとし，複写は非該当面のみで良いこととする。

電子データ原本の証明書類の場合，原本が事前に提出されているので複写の必要はない。

スマホ等に表示の証明書類の場合，証明書類全体が含まれるように撮影するなどして写しを採取する。

3.3.2　テレビ会議を通じた遠隔で行う場合

■申請・事前予約　申請者は，最寄りセンターに対して身元確認のためのテレビ会議の実施を依頼する。この時，申請者自身の証明書類の写しと対面認証申請書を電子メールで最寄りセンターに提出する。

電子データ原本の証明書類の場合，原本を提出する。

スマホ等に表示の証明書類の場合，証明書類の画面をキャプチャーするなどして写しを採取する。

最寄りセンターの担当者は，テレビ会議実施依頼の電子メールの発信元の氏名とメールアドレスが課題に登録されている申請者の情報と一致すること確認したうえで，身元確認を行う日時を申請者と調整する。また身元確認の手続きの検証に動画を利用する目的でテレビ会議を録画することへの同意も得ておく。テレビ会議をスケジュールする際は申請者単位にテレビ会議を用意する。第三者の介入の発生等がないようにミーティング URL 等の取り扱いに留意する。

最寄りセンターの担当者は，以下に掲げる事項をテレビ会議の開催前に確認しておく。

1. 証明書類（写し）に記載の氏名が対面認証申請書に記載の氏名と一致すること
2. 証明書類（写し）に記載の氏名および所属組織が課題に登録されている申請者の氏名および所属組織と一致すること

■申請者の身元確認　申請者は，指定日時に任意の場所からテレビ会議に参加する。

最寄りセンターの担当者は，テレビ会議を始める際に身元確認手続きの検証に動画を利用する目的で録画をすることを申請者に伝え，了承を得たうえで録画を開始する。

最寄りセンターの担当者は，テレビ会議において以

下に掲げる事項の全てを確認することで，申請者を特定する。

1. 事前に提出された対面認証申請書に基づき，いくつかの基本情報に関する質問を申請者に対して行い，申請者の回答内容に誤りがないこと
2. 非定型で機械的な対応が困難な質問を申請者に対して行い，申請者の回答内容に誤りがないこと
3. 事前に提出された証明書類の写しとテレビ会議のライブビュー上で申請者が提示する証明書類を照合し，同一のものであること
4. 証明書類の顔写真が申請者本人であること

テレビ会議のライブビュー上では，申請者に証明書類明書の表裏両面を提示して貰い記載事項を確認するが，第三者への開示が不適当な面が存在する書類であることを申請者が申し出た場合，開示可能な面に記載の属性情報のみで人物を特定できるか確認する。

電子データ原本の証明書類の場合，原本を各種ディバイス上に表示した状態でカメラ越しに提示が難しい場合は印刷したものを提示することで良い。

スマホ等に表示の証明書類の場合，証明書類を表示するアプリケーション上で証明書類の記載事項が確認できるように提示する。

上記の確認に加えて，テレビ会議のライブビュー上の申請者自身の顔と証明書類の顔写真がほぼ同じ大きさかつ同時に映る状態で画像を採取する。画像が正常に採取できていることが確認できた後であれば，テレビ会議の録画は破棄しても差し支えないが，テレビ会議中に保存した画像に不備がある場合は録画から切り出して画像として保管する。

すべての確認が完了した後，手続き終了の旨を申請者に告げ，テレビ会議を終了する。

最寄りセンターの担当者は，申請者の身元確認の実施後の追跡ができるように，以下の全てを参照できる状態で保存しておく。

1. 申請者からのテレビ会議の実施依頼時に電子メールにて最寄りセンターに提出された対面認証申請書ならびに証明書類（写し）
2. テレビ会議のライブビュー上の申請者の顔と身分証の顔写真がほぼ同じ大きさで同時に写った状態の画像
3. 審査結果等の記録

4　評価

本節では，利用者の身元確認に電子データ化された証明書類を利用することは，2.4 で挙げた要件を満たしているか等の確認を行う。

4.1　要件 1

電子データ化された証明書類の場合も必要となる記載事項は，プラスチックカードや紙に印字された物理的に存在する証明書類の場合と変わらないことから，同要件を満たすことを要求している。また，電子データ化された証明書類の発行元の組織が本人性を担保していることが確認できることも利用可能な証明書類としての要件に設定している。

電子データ原本の証明書類については，証明書類の発行元の組織が本人性を担保していることが確認できる例として「証明書類に電子署名が付与されており，署名者が書類を発行する責任を有している者であることを確認できること」を挙げているが，Adobe Acrobat を使用するとメールアドレスと名前を設定するだけで PDF ファイルに電子署名を付与することが可能となるため，実際の運用においては，例えば「署名は組織の発行した証明書に基づくものであること」のような詳細条件の検討が今後の課題となる。書類を発行する責任を有している者であることを確認できる電子署名が付けば，書類の真贋はひとまず PKIX(Public-Key Infrastructure using X.509) に依拠することができることから書類の真贋に限れば，電子データ原本の証明書類の方が物理的に存在する証明書類よりも優れている。

スマホ等に表示の証明書類の場合に証明書類の発行元の組織が本人性を担保していることが確認できる例として挙げている「証明書類をスマホ等に表示して利用することを認めている発行元の組織公式の Web サイトが存在すること」については，実際に申請者がスマホ等に表示して提示する証明書類が発行元の組織が認めている証明書類そのものであるかを実運用において確認する詳細条件の検討が今後の課題となる。一方「証明書類を表示するアプリケーションが発行元の組織公式のものであること」もしくは「証明書類を表示するアプリケーションの利用規約に証明書類として利用できることが記載されていること」については，スマートフォンの公式アプリケーションストア（Apple の App Store および Google Play ストア）を介して申請者が提示するアプリケーションを起動してもらうことで，いわゆる「野良アプリ」ではないこととともに

に確認する。スマホ等に表示の証明書類については，発行元の組織が信頼できる場合に限り機能するという点は物理的に存在する証明書類相当と考えられる。

4.2 要件 2

物理的に対面して行う場合，最寄りセンターの窓口にて提示された証明書類の記載事項を確認し，顔写真と申請者を見比べることで人物の特定する。（表 2）

電子データ化された証明書類のうち，電子データ原本の証明書類の場合は電子署名の署名者が書類を発行する責任を有している者であるの確認を課しているため事前送付を追加している。スマホ等に表示の証明書類の場合は，物理的に存在する証明書類の場合と同様に最寄りセンターの窓口にて提示してもらい確認する。

テレビ会議を通じた遠隔で行う場合，事前に提出された証明書類の記載事項を確認したうえで，テレビ会議のライブビュー上で提示された証明書類との突合せおよび顔写真と申請者を見比べることで人物の特定する。（表 3）

電子データ原本の証明書類の場合，原本を事前に提出してもらったうえで，テレビ会議では原本を各種ディバイス上に表示もしくは印刷したものを提示してもらう。

スマホ等に表示の証明書類の場合，画面をキャプチャーするなどして採取した写しを事前に提出してもらったうえで，テレビ会議では証明書類を表示するアプリケーション上で証明書類の記載事項が確認できるように提示してもらう。

これらのことから，電子データ化された証明書類を利用する場合も物理的に存在する証明書類を利用する場合相当での申請者の身元確認は可能と言える。

5 おわりに

本稿では，電子データ化された証明書類を用いた身元確認の手法を報告した。今回検討した手法は HPCI に限定せず，汎用的な身元確認にも応用できるものであり，皆様の課題解決のお役に立てれば幸いである。

参考文献

[1] 革新的ハイパフォーマンス・コンピューティング・インフラ（HPCI）について, https://www.mext.go.jp/a_menu/kaihatu/jouhou/hpci/1307375.htm

[2] 石井宏治, 坂根栄作, 合田憲人, “テレビ会議システムのライブビューによる遠隔での身元確認手法の検討”, 大学 ICT 推進協議会 2020 年度 年次大会論文集, 2020

[3] NIST Special Publication 800-63 Revision 3, https://pages.nist.gov/800-63-3/sp800-63-3.html