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

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 remote identity vetting with a live view of video meeting system

Koji Ishii, Eisaku Sakane, Kento Aida

National Institute of Informatics

概要

新型コロナウイルス感染症対策として，職場に出勤することなく在宅での勤務を行う対応を採った組織は少なくない。対人間の物理的な距離を取ることによって人が互いに密接な接触を行う機会を減少させる方策が推奨される状況下においては，人と人が互いに対面して行うことを前提とした身元確認の実施は困難である。本稿では，対人間の物理的距離に囚われないテレビ会議システム等のライブビューを通じた対面相当の遠隔での身元確認の手法を検討する。

1 はじめに

令和 2 年 4 月 7 日に発出（同月 16 日に実施地域が日本全国に拡大）された新型コロナウイルス感染症対策のための特別措置法に基づく緊急事態宣言を受けての不要不急の外出の自粛が要請されたことにより，職場に出勤することなく在宅での勤務を行う対応を採った組織は少なくない。また緊急事態宣言が解除となった後も継続して在宅での勤務を行う組織もある。令和 2 年 9 月現在，国立情報学研究所 (NII) においても，日々の業務は原則在宅で実施し，職場への出勤は必要に応じて最低限の人員および回数で行う対応を継続している状況である。

対人間の物理的な距離を取ることによって人が互いに密接な接触を行う機会を減少させる方策が推奨される状況下では，人と人が互いに対面して行うことを前提とした身元確認の実施は困難であることから，本稿では対人間の物理的距離に囚われることなく実施可能な対面相当の遠隔身元確認の手法として，テレビ会議システムの利用を検討する。

2 物理的に対面して行う身元確認の課題

本節では，物理的に対面して実施する身元確認の例として，共用計算環境の利用者の確認を想定モデルに，人が互いに密接な接触を行う機会を減少させる方策が推奨される状況下において職場に出勤することはできず在宅で勤務する場合など，利用者と身元確認を行う検証者が物理的に対面することが困難な際の身元確認の実施に係る課題等を整理する。

2.1 本人確認の要素としての身元確認

本人確認は，「架空の人物でないこと」（実在性），「他人への成りすましでないこと」（同一性）を担保する行為で，「身元確認」と「当人認証」に整理される。前者は，個人の自己申告ならびに身分証明書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確認する。この際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。また後者では，「知識情報」（パスワードなど）・「所持情報」（ハードウェアトークンなど）・「生体情報」（指紋など）のいずれかもしくは組み合わせて用いることで，当該本人が実際に行っている行為であることを確認する。[1]

本稿では，前者の「身元確認」を対象に論じる。

2.2 想定モデルの対面認証

ここでは，共用計算環境の利用者の身元確認を大学や研究機関に設置の受付窓口（利用者受付）において，保証レベル IAL2 として，物理的に対面して実施すること（対面認証）を想定モデルとする。

また対面認証の前提条件として，以下に掲げる事項を設定する。

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。

1. 共用計算環境の資源は，大学・研究機関や企業に所属する者が課題選定を経て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. 対面認証は利用者の所属組織同定後に実施する

■利用者受付への訪問　対面認証を受ける者（申請者）は，持参した対面認証申請書を利用者受付へ対面にて提出すると共に，自身の所属組織が発行する身分証明書（社員証や学生証など）を提示する。なお申請者が利用者受付に出向く際は，日時を調整のうえ訪問する必要がある。

■申請者の身元確認　身元確認の検証者である利用者受付の担当者は，以下に掲げる事項の全てを対面で確認することで，申請者が提示した身分証明書に問題がないことを確認し，人物を特定する。

1. 身分証明書の顔写真が申請者本人であること
2. 身分証明書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. 身分証明書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

身元確認できた申請者の身分証明書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。身分証明書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身分証明書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。

■顔写真のない身分証明書　対面認証で利用する身分証明書は，さまざま組織から発行されるものであるため，顔写真が掲載されていない場合（在籍証明書など）がある。顔写真のない身分証明書が提示された場合には，申請者の顔写真付き公文書（運転免許証，旅券など）に記載の氏名との一致を利用者受付が確認することにより，当該身分証明書を顔写真付きの身分証と同等に扱う。また顔写真付き公文書については，利用者受付での確認にのみ使用することとし，複写して保管する必要はない。

2.3　課題

利用者受付を運営する組織において，職場に出勤することなく在宅で勤務することを原則とするといった状況である場合，対面認証の実施は困難である。また申請者からみて利用者受付が遠隔地である場合，例えば対面認証のためだけに出張が必要になるなどであれば，利用者受付に出向いて対面認証を受けること自体が高いハードルと言える。

これらの状況から，対人間の物理的距離に囚われることなく，遠隔での身元確認を行うための手法の検討が課題となる。対面認証に相当する遠隔での身元確認の手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. 利用者受付と申請者の双方の物理的距離に関わらず実施できること
2. 申請者が所持する身分証明書に問題がないことを確認したうえで，人物の特定ができること

3　テレビ会議を通じた遠隔での確認手法

本節では，対人間の物理的距離による問題への対処として，距離的制約のないテレビ会議システムを通じて対面相当の身元確認を遠隔でも行える手法を検討する。

ここで検討するテレビ会議のライブビューによる遠隔での身元確認の手法は，新型コロナウイルス感染症が世界的拡大となる以前，IGTF(Interoperable Global Trust Federation) [2] における平成 28 年 4 月の NII からの問題提起と時を同じくして EUGridPMA(EU Policy Management Authority for Grid Authentication in e-Science) にて議論が始まった手法 [3] をベースにしたもので，次のとおりである。

■テレビ会議システム　利用者受付の担当者および申請者の双方が職場ではない場所から参加することも考慮しておく必要があることから，利用するテレビ会議システムは，任意の場所から指定のミーティングに参加が可能かつ接続用のソフトウェアが入手し易いものであることが望ましいため，Webex，Zoom，

BlueJeans などを想定している。

■関係者　遠隔での実施であっても基本的な枠組みに変更は無い。テレビ会議を通じた身元確認においても，利用者受付とのやり取りを行うのは申請者に限定する。

■申請・事前予約　申請者は，利用者受付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，申請者自身の身分証明書の写しと対面認証申請書を電子メールで利用者受付に提出する。

利用者受付の担当者は，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。参加するための URL やミーティング ID 等は使い回さず毎回変更するなど，第三者の介入の発生等がないように取り扱いに留意する。

利用者受付の担当者は，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. 身分証明書の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. 身分証明書の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。

利用者受付の担当者は，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。

利用者受付の担当者は，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. 事前に提出された身分証明書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身分証明書を照合し，同一のものであること
4. 身分証明書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，申請者に身分証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。

また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身分証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。

利用者受付の担当者は，申請者の身元確認の実施後の追跡ができるように，以下に掲げる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利用者受付に提出された対面認証申請書ならびに身分証明書の写し
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，テレビ会議のライブビューを通じて利用者の身元確認を遠隔で行うことは，2.3 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

利用者受付の担当者と申請者のやり取りは，職場宛の架電，FAX 送信，郵送等では行わず，電子メールおよびテレビ会議システムのみを介して行うため，仮に利用者受付の担当者と申請者の双方が職場以外の場所に滞在している場合であっても，物理的距離に関わらず身元確認を行うことができると言える。ただし，時差のある国外とのやり取りである場合は双方で都合がつく時間帯での実施のために調整することも考慮する必要がある。

4.2　要件 2

利用者受付の担当者は，申請者に対して以下に掲げる事項をテレビ会議中に尋ね，回答内容の全てに誤

りがないことを確認することで，テレビ会議のライブビュー上の人物のライブネス判定を行う。

1. 申請者から事前に提出された対面認証申請書に基づく基本情報
2. 非定型で機械的な対応が困難な質問

利用者受付の担当者は，以下に掲げる事項の全てをそれぞれ照合することで，申請者が所持する身分証明書に問題がないことを確認する。

1. テレビ会議の開催前:
   （a）身分証明書の写しに記載の氏名と対面認証申請書に記載の氏名
   （b）身分証明書の写しに記載の氏名および所属組織と課題に登録されている申請者の氏名および所属組織
2. テレビ会議のライブビュー上:
   （a）事前に提出された身分証明書の写しと申請者が提示する身分証明書
   （b）申請者が提示する身分証明書の顔写真と申請者自身

これらのことから，テレビ会議システムを通じた遠隔での確認であっても，申請者の人物を特定することは可能と言える。

5　本稿提案手法以外の手法

本節では，本稿提案手法のベースとなった EUGridPMA が提案するテレビ会議を通じた遠隔での身元確認手法ならびに本稿提案手法との相違点の説明に加えて，NII で確立したテレビ会議システムに依らないオンラインでの対面相当の身元確認手法を紹介する。

5.1　EUGridPMA 提案手法との比較

EUGridPMA が提案するテレビ会議を通じた遠隔での身元確認における関係者は利用者受付と申請者であり，本稿提案手法との違いはない。

テレビ会議開催前に行う手順は次のとおりである。

利用者受付の担当者は，テレビ会議を通じた身元確認を依頼の申請者に対して，テレビ会議時に使用する登録用文書の様式を申請者の情報として登録されているメールアドレス宛てに送付する。

申請者は，利用者受付から送付された登録用文書の様式をテレビ会議までに印刷して準備しておく。また自身の顔写真付き身分証明書の写しを電子メールにて利用者受付へ提出する。

続いて，テレビ会議の開始後の手順は次のとおりである。

利用者受付の担当者は，申請者にテレビ会議開催中に提供する固有の情報（使い捨てのランダムな値: nonce）を伝える。

申請者は，伝えられた nonce を含めて，利用者受付の担当者から目視できる状態で登録用文書に自著した後，電子データ化して利用者受付へ電子メールで返信する。

利用者受付の担当者は，テレビ会議のライブビュー上の申請者自身の顔と身分証明書の顔写真がほぼ同じ大きさで映る状態を画像で保存する。また以下に掲げる事項を全て確認することで申請者の人物を特定する。

1. 返信された登録用文書の電子データの内容がテレビ会議のライブビュー上で申請者が自著した内容と一致すること
2. 電子データとして返信された登録用文書に記載された nonce が正しいこと
3. 事前に提出された身分証明書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身分証明書を照合し，同一のものであること
4. 身分証明書の顔写真が申請者本人であること

上記の EUGridPMA の提案手法では，nonce のやり取りに基づいてテレビ会議のライブビュー上の人物のライブネス判定を行うが，nonce を記入した登録用文書をテレビ会議中に電子データ化したうえで電子メールで返信するという煩雑な手続きを必要としている。

本稿提案手法では，煩雑な nonce のやり取りに関する手順を置き換える形で，テレビ会議のライブビュー上の人物とリアルタイムのコミュニケーションを行うということが相違点ではあるが，要件 2 に関する評価で述べたとおり，ライブネス判定は可能であると考えられる。

5.2　テレビ会議システムに依らずオンラインで行う確認手法

NII では，身元確認保証レベルが対面相当以上の IGTF 認定認証局が発行する証明書を持つ申請者に限定するものではあるが，テレビ会議システムに依らないオンラインでの身元確認手法を確立しており，平成 30 年 4 月の APGridPMA(Asia Pacific Grid Policy Management Authority) [4] Face-to-face Meeting にて報告を行っている。

このオンラインでの手法における身元確認の関係者は以下に掲げる三者である。

1. 申請者
2. Identity Management System (IdM)
3. 認証局

申請者は，本稿提案手法と同様に身元確認の対象者である。IdM は，申請者の身元確認を対面相当の保証レベルで行う機関である。認証局は，IdM と同等の対面相当の保証レベルで利用者の身元確認を行う機関で，その身元確認保証レベルに基づいて利用者向けに電子証明書の発行を行う。また認証局は，申請者に対して電子証明書を発行済みであることを前提条件とする。

身元確認の手順の概要は次のとおりである。

IdM は，電子証明書を用いて申請者を認証した後，電子証明書の記載事項をキーに照合対象の認証局に照会する。

認証局は，当該申請者に IdM からの照会の正当性を確認したうえで，IdM に回答する。

IdM は，照会結果に基づき登録データの照合を完了する。

この手法は，身元確認保証レベルが同等以上の IGTF 認定認証局が発行する電子証明書を持つ申請者に限定するものではあるが，対面相当の身元確認保証レベルに基づいて発行された電子証明書を信用することでオンラインでの身元確認を行う。またこのオンラインでの手法は，対人間の物理的な距離的制約を受けないことに加えて，関係者間の時差による実施時間帯の制約を伴わないものとなっている。

6 おわりに

本稿では，身元確認の申請者とその検証者である利用者受付の担当者の双方の物理的距離に囚われることなく実施可能なテレビ会議のライブビューによる遠隔での対面相当の身元確認の手法を報告した。今回検討した手法は想定モデルに限定せず，汎用的な身元確認に応用できるものでもあり，皆様の課題解決のお役に立てれば幸いである。

また今回検討した手法は，APGirdPMA での議論の俎上に載せることに加えて，EUGridPMA をはじめとする IGTF コミュニティへも共有を行う予定である。

参考文献

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

[2] IGTF: Interoperable Global Trust Federation, http://www.igtf.net/

[3] Vetting Model Guidelines, http://wiki.eugridpma.org/Main/VettingModelGuidelines

[4] Asia Pacific Grid Policy Management Authority, http://www.apgridpma.org/