資料2

令和５年度
本人確認ガイドラインの改定に向けた有識者会議
論点協議資料（第１回分）

令和5年10月　　トラストタスクフォース

デジタル庁
Digital Agency

論点一覧

論点一覧

協議予定回	大項目	論点の概要
第１回	**1. 身元確認保証レベルの見直し**	論点1-1.「身元確認保証レベル３」をNIST IAL3基準に見直すべきではないか
		論点1-2. リモート身元確認において生体情報の比較を必須とすべきか
		論点1-3.「身元確認保証レベル１」における登録コードの扱いをどうすべきか
	2. 当人認証保証レベルの見直し	論点2-1.「当人認証保証レベル２」においてフィッシング耐性を必須とすべきか
第２回	**3. マイナンバーカードを用いた本人確認の保証レベルについて**	論点3-1. マイナンバーカードを用いた各保証レベルはどのような位置づけとなるか（※NIST SP 800-63-4における保証レベル定義の見直し等を踏まえた位置づけの確認など）
		論点3-2. マイナンバーカード機能のスマートフォン搭載の保証レベルはどう整理できるか
	4. リスク評価プロセスの見直し	論点4-1. NISTの改定内容を本ガイドラインにも取り入れるべきではないか
		論点4-2. 適切なリスク評価を行うための検討支援や統制が必要ではないか

本資料中の用語・表記について

- NISTと本人確認ガイドラインとの類似用語を区別して議論できるよう、本資料中では以下の用語・表記を用いる。
- これら以外のNIST SP 800-63に関する用語等は原則として[OpenID Foundation Japanによる翻訳版]に準拠する。

用語・表記	本資料中の定義
本人確認ガイドライン ／本ガイドライン	改定検討中の「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン」のこと。 現行版のガイドラインのみを指す場合は「現行ガイドライン」のように表記する。
身元確認保証レベル 当人認証保証レベル 認証連携保証レベル	本人確認ガイドラインで定義する各保証レベルのこと。 NIST SP800-63のAssurance Levelとの混同を防ぐため、本資料中ではこのように日本語で表記する。 また、3種類の保証レベルをまとめて「本人確認保証レベル」と表記する。
NIST IAL NIST AAL NIST FAL	NIST SP800-63 Digital Identity Guidelinesで定義される各Assurance Levelのこと。 本人確認ガイドラインの保証レベルとの混同を防ぐため、明示的に「NIST xAL」と表記する。
対策基準	本人確認ガイドラインにおいて、各保証レベルにおいて求める対策の要求事項のこと。 NIST SP800-63 のRequirementsに相当。
妥当性確認（Validation）	NIST SP800-63A-4のValidationに相当する行為のこと。
検証（Verification）	NIST SP800-63A-4のVerificationに相当する行為のこと。
生体情報の比較 （Biometric comparison）	NIST SP800-63A-4のVerification時のRequirementsとして示される”Biometric Comparison”に相当する行為のこと。 証明書等のEvidenceに含まれる顔写真と、申請者の顔（リモートの場合は写真又はビデオ）を比較して、申請者と証明書とのバインディングを検証する。
登録コード （Enrollment code）	NIST SP800-63A-4のVerification時のRequirementsとして示される”Enrollment Code”のこと。 Validation済みの住所、電話番号、メールアドレス等に対して送信した登録コードによってVerificationを行う行為のこと。
フィッシング耐性 （Phishing resistant）	本資料中では特に明記しない限り、OTP等では防ぐことが難しいリアルタイムフィッシング攻撃に対する耐性のことを指す。

各論点の協議用資料（第１回）

1. 身元確認保証レベルの見直し

2. 当人認証保証レベルの見直し

3. マイナンバーカードを用いた本人確認の保証レベルについて

4. リスク評価プロセスの見直し

5. その他の個別論点

協議いただきたい論点

- NIST SP 800-63-4 ipdでのIALの見直しに伴い、本人確認ガイドラインの身元確認保証レベルについてもマイナンバーカード等の国内のインフラを踏まえた見直しを検討中。現時点の方針の妥当性を議論いただきたい。

本テーマの論点	現時点での方針
1-1.「身元確認保証レベル３」はNIST IAL3基準に見直すべきではないか • 現行の本人確認ガイドラインにおいては「マイナンバーカードの署名用電子証明書」による身元確認などを「レベル３」として扱っているが、これはNISTが定義するIAL3の基準とは乖離がある。 • 今後も国内独自の「レベル３」を継続するか、それともNISTとの相互運用性等を考慮してレベル３の扱いを見直すべきか検討が必要。	**レベル３はNIST IAL3相当に見直す** • 将来的なPIV制度での活用、NISTとの相互運用性確保などを見据え、レベル３の対策要件はNIST IAL3相当となるように見直する。 • 一般の行政手続は該当しない「真に厳格な本人確認が必要な場合のレベル」として位置付ける。
1-2. リモート身元確認において生体情報の比較を必須とすべきか • 対面での身元確認では通常「申請者の顔と、身分証明書等の顔写真との比較」が行われるが、現在の本人確認ガイドラインでは、リモート身元確認での顔の比較は求めていない。 • 他方、NISTではIAL1～3のいずれにおいても顔などの生体情報の比較（Biometric Comparison）によるVerificationが求められている。国内の基準を今後も継続することが妥当であるのか、検討が必要。	**生体情報比較は必須としない** • マイナンバーカードでは各APの知識認証によってリモート身元確認時のなりすましリスクを低減できる。 • これを踏まえ、国内の基準においては生体情報比較は必須とはせず、暗証番号のない身分証明書を用いる場合など、リスクに応じて求める基準とする。
1-3.「身元確認保証レベル１」の登録コードの扱いをどう考えるべきか • NIST SP 800-63-4 Draft版のIAL1では、身元確認時の生体情報の比較に代わる手段として、「確認済みの住所、電話番号、メールアドレス等に対する登録コード送信」による認証が認められている。（IAL2、IAL3では登録コードの使用は不可。） • 本人確認ガイドラインの身元確認保証レベル１においても同様に登録コードの使用を認めるべきか。国内での登録コードのユースケースや強度から考慮すべき事項はないか。	**方針未定（本会議で議論いただきたい）** • NISTのように登録コードによるVerificationを認めることが、国内における身元確認保証レベルの「レベル１」と「レベル２」の違いとして本当に適当なのか継続検討中。

「身元確認保証レベル３」の厳格化

- 現行ガイドラインの身元確認保証レベル３の対策基準は、NIST IAL3の要求事項とは異なる点も多い。
- 政府機関における個人アイデンティティの検証（Personal Identity Verification）や経済安全保障関連等において本ガイドラインの保証レベルが参照される可能性や、NISTとの相互運用性の観点を考慮し、レベル３はNIST IAL3相当の「真に厳格な身元確認が必要な場合の保証レベル」として厳格化することを検討中。

身元確認保証レベル３の対策基準の見直し（案）

対策基準項目	対策基準の見直し案（赤字：主な変更点）
身元確認の実施環境 （Presence）	対面を原則 リモートの場合はNISTの” Supervised Remote Identity Proofing” 相当の監視環境下
必要な 身分証明書 （Evidence）	公的な顔写真付きの身分証を２つ以上（仮） ※ 数量についてはマイナンバーカードの身分証の一元化方針も踏まえながら今後も継続検討する。
身分証明書の妥当性確認 （Validation）	• 券面の目視検査（対面の場合） • 耐タンパ性ICチップによる偽造の検知＋デジタル署名の検証による完全性の確認（デジタルエビデンスの場合）
身分証明書と申請者の紐づきの検証 （Verification）	申請者の顔と身分証の顔写真の比較
生体情報の収集 （Biometric Collection）	生体情報（顔、指紋等）の情報を収集・記録する

身元確認保証レベル３の考え方

一般の行政手続は該当しないレベルとして定義

- レベル３は対面での身元確認又は監視環境下でのリモート身元確認を必要とする、真に厳格なレベルとして定義する。
- 該当する行政手続は一部の特殊なケースに限られ、本ガイドラインで扱う行政手続の多くはレベル３には該当しないことを想定している。

将来的な活用を見据える

- NISTのPIV制度ではIAL3相当の身元確認が求められている。我が国においても将来的に国内版PIV制度を整備しようとする際、身元確認保証レベル３を参照する可能性があることを考慮してレベル３の基準を厳格化する。
- 同様に、セキュリティクリアランス制度等での活用可能性も考えられるため、NIST IAL3との相互運用性はできる限り確保する対策基準とする。

身元確認保証レベル２における「生体情報比較」の考え方

- 身元確認保証レベル２は現行ガイドラインの対策基準から大きく変更しない。
- NISTでは生体情報比較（申請者と身分証の顔写真との比較など）が求められているが、国内では広く普及したマイナンバーカードでは知識認証が利用可能であることを踏まえ、知識認証によってなりすましリスクを低減できている場合には生体情報比較は必須としない方針。

身元確認保証レベル２の対策基準の見直し（案）

対策基準項目	対策基準の見直し案（赤字：主な変更点）
身元確認の実施環境 （Presence）	対面又はリモート
必要な 身分証明書 （Evidence）	公的な顔写真付きの身分証を１つ以上
身分証明書の妥当性確認 （Validation）	• 券面の目視検査（対面の場合） • 耐タンパ性ICチップによる偽造の検知＋デジタル署名の検証による完全性の確認 （デジタルエビデンスの場合）
身分証明書と申請者の紐づきの検証 （Verification）	対面の場合： • 申請者の顔と身分証の顔写真の比較 リモートの場合： • 暗証番号等の知識認証による確認 • 又は、申請者の写真/動画と身分証の顔写真の比較

身元確認保証レベル２の考え方

多くの行政手続が該当する保証レベルとして定義

- レベル２は、大多数の行政手続が該当するレベルとして想定。
- 対策基準は全面的に見直すものの、結果としては現行ガイドラインのレベル２をほぼ踏襲する位置づけのレベル定義となる。

「生体情報比較」を必須としないことの考え方

- 米国で普及している身分証明書には暗証番号を利用可能なものが少なく、盗難等によって容易になりすましができてしまうため、NIST IALでは生体情報比較を必須としていると解釈できる。
- 他方、我が国ではマイナンバーカードが広く普及しており、リモート身元確認においても暗証番号による知識認証を行うことで、申請者と身分証明書の紐づきを確認できる。カメラで容貌を撮影する方式よりもユーザビリティに優れると考えられるため、この手法を基本として考え、知識認証を利用できない場合には生体情報比較を求める対策基準とする。
- この基準に照らし合わせると、犯罪収益移転防止法の「ホ」に相当する方式は「知識認証による紐づきを確認できないため、生体情報比較によって紐づきを確認している」という解釈ができるようになる。

「身元確認保証レベル１」の登録コードの扱い

- NIST IAL2とIAL1の差を参考とし、登録コードによる検証を認める「身元確認保証レベル１」を新設する。登録コードは妥当性確認済みの住所、電話番号、メールアドレス等に送信することを想定している。
- ただし、国内の郵送や電話番号の信頼性等を考慮した場合、この登録コードの有無がレベル２とレベル１の差として妥当であるのかについては検討の余地が残っており、現在も継続検討中。

身元確認保証レベル１の対策基準の見直し（案）

対策基準項目	対策基準の見直し案（赤字：主な変更点）
身元確認の実施環境 （Presence）	対面又はリモート
必要な 身分証明書 （Evidence）	公的な顔写真付きの身分証を１つ
身分証明書の妥当性確認 （Validation）	• 券面の目視検査（対面の場合） • 耐タンパ性ICチップによる偽造の検知＋デジタル署名の検証による完全性の確認 （デジタルエビデンスの場合）
身分証明書と申請者の紐づきの検証 （Verification）	対面の場合： • 申請者の顔と身分証の顔写真の比較 リモートの場合： • 暗証番号等の知識認証による確認 • 又は、申請者の写真/動画と身分証の顔写真の比較 • 又は、登録コードによる認証

身元確認保証レベル１の考え方

登録コードによるVerificationを認めるレベルとして設定

- NISTのIAL2に対するIAL1の主な差異である「登録コード（Enrollment Code）によるVerification」を参考とし、本ガイドラインにおいても登録コードによる検証を認めるレベル１の策定を検討中。

保証レベル２と１の差としての妥当性

- 国内のデジタル化の方針、郵送の信頼性等を考慮したとき、登録コードによる紐づきの検証を認めることがレベル２とレベル１の差異として妥当であるのかについては現在も検討中。

住所以外の登録コード送信先について

- 身分証明書との紐づきを確認することが目的であるため、登録コードは身分証明書等によって妥当性を確認できた宛先に送信する必要がある。
- 住所については妥当性確認が可能であるが、電話番号、メールアドレスについては現状妥当性確認できるケースはあまり想定されないのではないか。

身元確認保証レベルと対策基準の見直し（案）

対策基準項目	対策基準の見直し方針（赤字：現行ガイドラインからの主な変更点）		
	身元確認保証レベル１ →新設扱い （現行のレベル１（身元確認なし）は「レベル０」となる）	身元確認保証レベル２ →大きな変更なし	身元確認保証レベル３ →NISTにあわせて厳格化
身元確認の実施環境 （Presence）	対面又はリモート	対面又はリモート	対面を原則 リモートの場合：NISTの”Supervised Remote Identity Proofing” 相当の監視環境下を条件とする
必要な 身分証明書 （Evidence）	公的な顔写真付きの身分証を１つ	公的な顔写真付きの身分証を１つ	公的な顔写真付きの身分証を２つ以上（仮） ※ ただし身分証明書の点数については、マイナンバーカードの身分証の一元化方針も踏まえながら今後も継続検討する。
身分証明書の 妥当性確認 （Validation）	• 券面の目視検査（対面の場合） • 耐タンパ性ICチップによる偽造の検知＋デジタル署名の検証による完全性の確認（デジタルエビデンスの場合）	• 券面の目視検査（対面の場合） • 耐タンパ性ICチップによる偽造の検知＋デジタル署名の検証による完全性の確認（デジタルエビデンスの場合）	• 券面の目視検査（対面の場合） • 耐タンパ性ICチップによる偽造の検知＋デジタル署名の検証による完全性の確認（デジタルエビデンスの場合）
身分証明書と申請者の紐づきの検証 （Verification）	対面の場合： • 申請者の顔と身分証の顔写真の比較 リモートの場合： • 暗証番号等の知識認証による確認 • 又は、申請者の写真/動画と身分証の顔写真の比較 • 又は、登録コードによる認証	対面の場合： • 申請者の顔と身分証の顔写真の比較 リモートの場合： • 暗証番号等の知識認証による確認 • 又は、申請者の写真/動画と身分証の顔写真の比較	申請者の顔と身分証の顔写真の比較 （対面、監視環境下リモートのいずれも）
生体情報の収集 （Biometric Collection）	なし	なし	生体情報（顔、指紋等）の情報を収集・記録する

目次

協議いただきたい論点

- NIST SP 800-63-4 ipdにおいてAALのRequirementsとして追加されたPhishing resistance（フィッシング耐性）をどのように反映すべきかが主な論点。NISTではAAL3で必須、AAL2で推奨、AAL1で不要となっている。
- 今後のパスキー等の普及動向も踏まえつつ、改定方針の妥当性について協議いただきたい。

本テーマの論点

2-1. 当人認証保証レベル２のフィッシング耐性を「必須」にできないか

- Phishing resistanceについては、NIST IAL2では「Recommended（推奨）」となっているが、昨今のフィッシングの脅威動向を踏まえると「必須」にすることが望ましいと考えられる。
- 国内の行政手続で採用され得る手法、民間で普及している手法等を踏まえ、本人確認ガイドラインの当人認証保証レベル２においてはフィッシング耐性要件を「必須」とすることを検討できないか。

現時点での方針

レベル２の要件はNISTと同じく「推奨」とする。

- 国内で普及している当人認証手法を踏まえると、レベル２においてフィッシング耐性を「必須」とした場合、採用できる手法が極めて限られてしまうため、レベル２のフィッシング耐性要件は必須としない方針とする。
- ただし、本ガイドラインの改定タイミングまでにパスキー等の新たな認証手法が普及する可能性も考慮し、今後の動向を注視する。

対策可能な脅威に応じて手法例を示すことで、リスクに応じた手法を選択できるようにする。

- 要件としては必須としないが、レベル2に該当する手法を脅威に応じてカテゴリ分けして手法例として提示する。これにより、各行政手続がフィッシング等の脅威によるリスクに応じて適切な手法を選択できるようにする。

フィッシング耐性を有する当人認証手法の例

- 現時点で普及している当人認証手法を踏まえると、レベル２においてフィッシング耐性を必須とした場合、行政手続において採用できる手法が極めて限定的になってしまうことが懸念される。

NIST AAL		主要な当人認証手法 （括弧内：SP 800-63B-4のAuthenticator Type）	行政手続における留意事項等
NIST AAL3 （HWベース多要素）	フィッシング耐性あり （注１）	生体認証でアクティベートされるFIDOセキュリティキー （Multi-Factor Cryptographic Devices）	• 物理デバイスの準備が必要であるため不特定多数が利用する行政手続では採用しにくい
		PINでアクティベートするスマートカードによる証明書認証 （Multi-Factor Cryptographic Devices）	
NIST AAL2 （多要素）		生体認証でアクティベートされるFIDO認証（パスキー含む） （Multi-Factor Cryptographic Software）	• フィッシング耐性を備えるAAL2として有力な実現方式となり得ると期待できるが普及動向への考慮が必要
		生体認証でアクティベートされるAuthenticatorアプリによる証明書認証 （Multi-Factor Cryptographic Software）	• 証明書の配付が必要となるため不特定多数が利用する行政手続では採用しにくい
		パスワード ＋ 端末にインストールされた証明書認証 （Memorized Secret + Single-Factor Cryptographic Software）	• 証明書の配付が必要となるため不特定多数が利用する行政手続では採用しにくい
	フィッシング耐性なし	パスワード ＋ Authenticatorアプリでのプッシュ通知・番号選択等 （Memorized Secret + Out-of-Band Devices）	
		パスワード ＋ AuthenticatorアプリでのTOTP （Memorized Secret + Single-Factor OTP Device）	
		パスワード ＋ SMS認証コード （Memorized Secret + Out-of-Band Devices）	
NIST AAL1 （単要素）		パスワードのみ （Memorized Secret ）	

（注１）最終的なフィッシング耐性の有無は、上記の認証器の種別だけでなくバックチャネルの実装（相互認証の有無等）にも依存する点に留意。

2. 当人認証保証レベルの見直し
2-1. 当人認証保証レベル２のフィッシング耐性を「必須」にできないか

脅威に応じた手法例の提示（案）

- 同じ保証レベル２に該当する手法であっても対策可能な脅威が異なることをガイドライン中の参考情報として示すことで、行政手続ごとのリスクに応じた手法を選択できるようにすべきではないか。

脅威に応じた認証手法の分類イメージ（参考：CISA Implementing Phishing-Resistant MFA）

認証手法例	多要素認証に対する脅威			概要説明
	リアルタイムフィッシング	多要素認証疲労攻撃 ※Fatigue Attack	SIMスワップ、SS7脆弱性	
フィッシング耐性多要素認証 • FIDO認証 • 電子証明書によるPKIベース認証	✓	✓	✓	• フィッシング耐性を有する認証手法。 • 当人認証レベル２に該当する手続では、これらのようなフィッシング耐性を有する手法の採用を推奨する。
モバイルアプリ認証 • Authenticatorアプリ等によるワンタイムパスワード • Authenticatorアプリへのプッシュ通知による番号選択	—	✓	✓	• フィッシングへの耐性のない認証手法。疲労攻撃やSIMスワップには耐性がある。 • 当該手続におけるフィッシングリスクを評価したうえで、リスクを受容できる場合や代替手段で対策できる場合などには採用を検討する。
モバイルアプリ認証（番号照合無し） • Authenticatorアプリへのプッシュ通知（番号の選択や入力がないもの）	—	—	✓	• フィッシングへの耐性がないうえ、疲労攻撃への耐性も有さない認証手法。原則として採用すべきではない。
SMS認証 • SMSによる認証コード通知	—	—	—	• フィッシング、疲労攻撃、SIMスワップのいずれの耐性も有さない認証手法。原則として採用すべきではない。

見直し後の当人認証保証レベル（案）一覧

対策基準項目		対策基準の見直し方針 （赤字：現行ガイドラインからの主な変更点）		
		当人認証保証レベル１	当人認証保証レベル２	当人認証保証レベル３
認証要素		単要素	２要素	耐タンパ性が確保された ハードウェアトークンを含む２要素
脅威への耐性	オンライン上の推測 （※辞書攻撃など）	必須		
	盗聴による認証情報の取得	必須		
	セッションハイジャック	必須		
	中間者攻撃	必須		
	リプレイ攻撃	不要	必須	
	フィッシング	不要	推奨	必須

デジタル庁

Digital Agency