資料2

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

本人確認ガイドラインの改定に向けた有識者会議
令和6年度（2024年度）第3回

ガイドライン改定案の妥当性に関する協議資料

令和6年12月　　デジタル庁　トラストタスクフォース

デジタル庁
Digital Agency

各回の検討テーマ（予定）

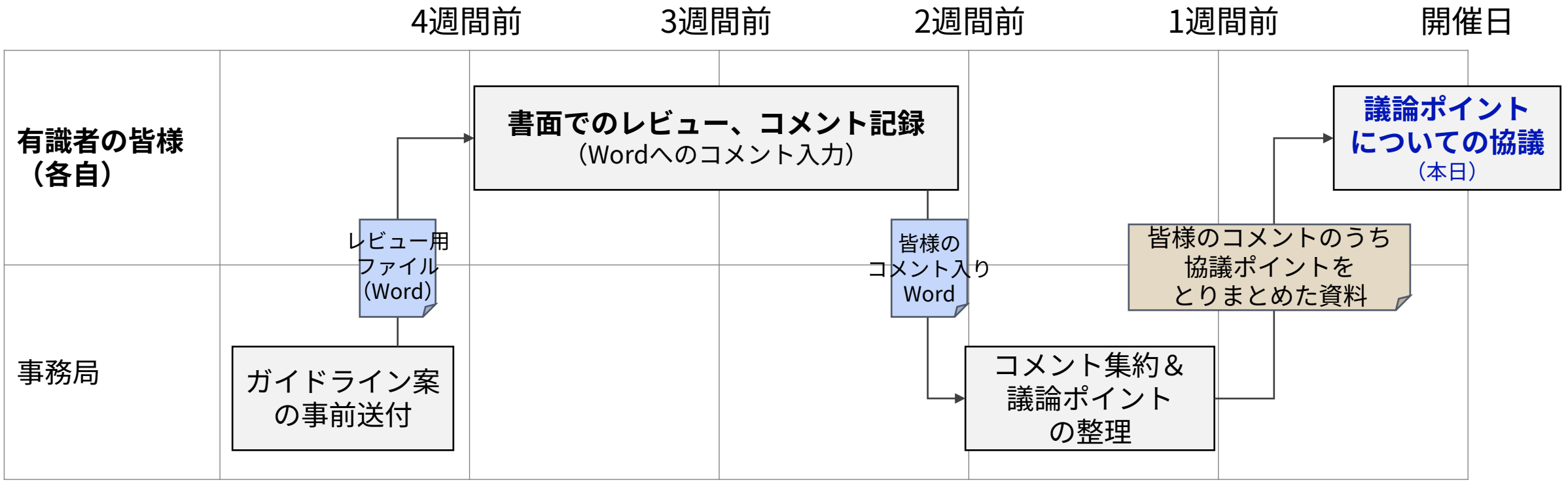
- 本日は「ガイドライン改定案の妥当性に関する協議」の第1回目として、作成中のガイドライン改定案の記載をご確認いただき、見直すべき記載、追加検討すべき論点などについてご議論をお願いします。

開催回	議題予定
第1回 令和6年9月17日（火） 18:00～20:00	• **開催要綱説明** • **ガイドライン改定に向けた論点協議（１）** – 論点1. NIST SP 800-63-4 2pdから反映を検討すべき事項について
第2回 令和6年11月5日（火） 18:00～20:00	• **ガイドライン改定に向けた論点協議（２）** – 論点2. 身元確認保証レベル１の位置づけと本人確認書類の対策基準について – 論点3. フェデレーション保証レベルと対策基準について
第3回 令和6年12月5日（木） 18:00～20:00	• **ガイドライン改定案の妥当性に関する協議（１）** – ガイドライン改定案に対するコメント、指摘、意見交換
第4回 令和7年1月16日（木） 18:00～20:00	• **ガイドライン改定案の妥当性に関する協議（２）** – ガイドライン改定案に対するコメント、指摘、意見交換
第5回 令和7年3月4日（火） 18:00～20:00	• **本人確認ガイドライン改定に向けた最終とりまとめ** – 最終とりまとめ（案）に対する意見交換、内容合意 – ガイドライン改定案の修正結果の確認

ガイドライン改定案の妥当性に関する協議の進め方について

- 委員の皆様におかれましては、ガイドライン改定案の事前レビューに対応いただき、ありがとうございました。
- 本資料では、皆様からいただいたコメントのうち特にご議論いただきたいポイントを抜粋・整理しておりますので、そのポイントを中心としたご議論やご助言をいただきたくお願いします。

※本資料内で抜粋していないコメントにつきましても、事務局にてガイドライン改定案への反映を検討いたします。



本人確認ガイドライン改定案の協議対象範囲

第3回会議におけるレビュー・協議の範囲

ガイドライン改定案の目次（現時点案）

1　はじめに
- 1.1　背景と目的（レビュー対象外）
- 1.2　適用対象（レビュー対象外）
- 1.3　位置づけ（レビュー対象外）
- 1.4　用語（レビュー対象外）
- 1.5　基本的な考え方

2　本人確認の枠組み
- 2.1　本人確認の基本的要素
- 2.2　本人確認モデル

3　本人確認における脅威と対策
- 3.1　身元確認（Identity Proofing）
- 3.2　当人認証（Authentication）
- 3.3　フェデレーション（Federation）

4　本人確認手法の検討方法（レビュー対象外）
- 4.1　本人確認に係るリスクの特定
- …

主なレビュー対象範囲

「1.5 基本的な考え方」
- 本ガイドラインに基づく検討にあたる基本的な考え方として、「1) 事業目的（ミッション）の遂行」、「2) 公平性」、「3) プライバシー」、「4) ユーザビリティ及びアクセシビリティ」及び「5) セキュリティ」の観点を解説

「2. 本人確認の枠組み」
- 身元確認、当人認証及びフェデレーションの目的、概要等の解説を追加
- 本人確認モデルとして「連携モデル（Federated Model）」及び「非連携モデル（Non-Federated Model）」を定義

「3. 本人確認における脅威と対策」
- 身元確認、当人認証及びフェデレーションのそれぞれについて、これまでの論点協議結果をもとに「1) 脅威と対策」、「2) プロセスと手法」、「3) 保証レベルと対策基準」を定義

※目次は2023年度の中間とりまとめ時点の案をベースに一部修正。
　また、別紙の記載は省略しています。

ガイドライン改定案に対するコメント、意見交換

- **1. はじめに**
- 2. 本人確認の枠組み
- 3. 本人確認における脅威と対策
  - 3.1. 身元確認
  - 3.2. 当人認証
  - 3.3. フェデレーション

ガイドライン改定案「1.5 基本的な考え方」

１．５　基本的な考え方

政府機関における本人確認は、単に高いセキュリティを確保すればよいというものではなく、公平性やプライバシーなど様々な観点を考慮した検討が必要となる。本ガイドラインに基づく検討は、以下に示す5つの観点を念頭において実施するものとする。

1)　事業目的（ミッション）の遂行

本人確認が障壁となって、対象手続が達成しようとする事業目的（ミッション）が阻害されてはならないと考える。

例えば、国民に対して緊急性の高い給付金を支給する手続において、必要以上に厳格で複雑な本人確認手法を求めてしまうと、それが申請の妨げとなり、本来遂行すべき「給付金を迅速に支給する」という事業目的を阻害してしまう恐れがある。

採用しようとする本人確認手法において事業目的の遂行を阻害する懸念がある場合には、代替手段や例外措置をあわせて検討する必要がある。

2)　公平性

当該手続が対象とする利用者について、その人種、国籍、文化、性別、年齢、住む地域などによらず、誰もが利用できる本人確認手法が必要であると考える。

例えば、肌の色によって認証精度に大きなばらつきが生じる認証手法は、その採用によって公平性が損なわれないか慎重な検討が必要である。また、外国語の氏名をもつ申請者は、氏名欄の設け方によっては自身の正確な情報を入力できず、申請が困難となるケースなどの考慮も必要である。

採用しようとする本人確認手法によって公平性の懸念が生じる場合には、代替手段や例外措置をあわせて検討する必要がある。

3)　プライバシー

本人確認においては個人に関する情報を取り扱うため、プライバシー保護についての留意が必要であると考える。

例えば、身元確認において申請者の情報入力を求める場合には、個人情報の収集目的を明示する、目的外の利用を行わないようにする、取り扱うデータを必要最小限に留めるなどといった、プライバシー保護の観点で必要な措置を検討する必要がある。

（前頁からの続き）

4)　ユーザビリティ及びアクセシビリティ

本人確認におけるユーザビリティやアクセシビリティが十分に考慮されていないと、申請者が誤った操作や入力をしてしまったり、手続きを途中で断念したりする原因にもなり、最終的には当該手続のミッション遂行、公平性、プライバシーなどにも影響を与えることになる。

本人確認手法の検討においては、当該手続の利用者の特性などを考慮したうえで、利用者が正しいことを行いやすく、間違ったことは行いにくくなるようなユーザビリティとアクセシビリティの確保が必要である。

5)　セキュリティ

セキュリティ強度の高い本人確認手法は、前述のミッション遂行、公平性、プライバシー、ユーザビリティ等の観点ではデメリットを抱えている場合がある。したがって、単にセキュリティ強度の高い本人確認手法を選べばよい訳ではなく、ミッション遂行、公平性、プライバシー、ユーザビリティ、アクセシビリティへの影響を考慮しつつ、当該手続におけるリスクに応じた適切な強度の手法選択が必要であると考える。

本ガイドラインでは、本人確認手法のセキュリティ強度の高低を「保証レベル」として段階的に定義する。保証レベルの基本的な位置づけは以下のとおりである。

表　1-2　保証レベルの基本的な位置づけ

保証レベル	保証レベルの位置づけ	該当する対象手続の考え方
レベル３	・ 極めて厳格な強度の保証レベル。 ・ 本人確認の失敗が申請者の生命に影響を与え得る場合など、リスクの影響度が極めて大きい場合に該当する。	ほとんどの対象手続は該当せず、ごく一部の例外的な対象手続のみが該当するレベルとして想定。
レベル２	・ 標準的な強度の保証レベル。 ・ 本人確認の失敗によるリスクの影響度が比較的大きい場合に該当する。	大多数の対象手続が該当するレベルとして想定。
レベル１	・ 簡易的な強度の保証レベル。 ・ 本人確認の失敗によるリスクの影響度が比較的小さい場合に該当する。	一部の低リスクの対象手続が該当するレベルとして想定。

委員の皆さまよりいただいた主なコメント

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
1) 事業目的（ミッション）の遂行	採用しようとする本人確認手法において事業目的の遂行を阻害する懸念がある場合には、代替手段や例外措置をあわせて検討する必要がある。	未然に防ぐ観点に加え、後から追跡・検証する観点など、というような言い回しはどうか。
		事後の評価と取り消し等を含めないと、ハレーションを起こしそうです。2022年の熊本県立大のインシデントは今後ずっと引用されるでしょう。
2) 公平性	例えば、肌の色によって認証精度に大きなばらつきが生じる認証手法は、その採用によって公平性が損なわれないか慎重な検討が必要である。	生体認証は、後述でも「ただし、生体認証は他の認証要素と組み合わせて利用することを前提とし、単独の認証要素として利用することはできない」とあるとおり、まさに公平性の観点もあって、単独の認証要素としては利用されないことが既によく認識されています。そのため、公平性の説明例としては、生体認証の事例以外の事例を先に記す方が良いと思います。また、生体認証における公平性の確保については、肌の色の違いもさることながら、従事する職業によって指紋認証が使えない例なども理解されやすいと思います。
		実際の手法のイメージがしにくい気がします。年齢によって認証精度にばらつきが生じる認証方法、の方がイメージしやすい気がします。
		別の例が挙げられると良いのでは。たとえば障がい者とか。
	採用しようとする本人確認手法によって公平性の懸念が生じる場合には、代替手段や例外措置をあわせて検討する必要がある。	繰り返しですが、このため、生体認証は単独の認証要素として利用することはできない、望ましくなく、代替手段の提供が期待されているところであるため、公平性の確保の事例として、生体認証以外の例をあといくつか触れて、生体認証で単独の認証要素として利用することが望ましくないとされる理由もそこにある点を触れる方が、有用な記載となるように思われます。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3) プライバシー	...個人情報の収集目的を明示する、目的外の利用を行わないようにする、取り扱うデータを必要最小限に留めるなどといった、...	「取り扱うデータ」は、“取り扱う情報”又は“収集する情報”が良いと思います。
	例えば、身元確認において申請者の情報入力を求める場合には、個人情報の収集目的を明示する、目的外の利用を行わないようにする、取り扱うデータを必要最小限に留めるなどといった、プライバシー保護の観点で必要な措置を検討する必要がある。	どちらかというとここに記載の内容はプライバシー保護というよりも個人情報保護の観点で必要な措置だと思います。
4) ユーザビリティ及びアクセシビリティ	利用者が正しいことを行いやすく、間違ったことは行いにくくなるような...	OIDF-Jの翻訳にある「間違ったときに簡単に回復できるような」も入れてはいかがでしょう。
5) セキュリティ	セキュリティ強度の高い本人確認手法は、前述のミッション遂行、公平性、プライバシー、ユーザビリティ等の観点ではデメリットを抱えている場合がある。したがって、単にセキュリティ強度の高い本人確認手法を選べばよい訳ではなく、ミッション遂行、公平性、プライバシー、ユーザビリティ、アクセシビリティへの影響を考慮しつつ、当該手続におけるリスクに応じた適切な強度の手法選択が必要であると考える。	ユーザビリティ等の観点で緩和の方向性というのも判りますが、行政手続によっては、国の信用やナショナルセキュリティに係わるものもあることは留意した方が良いのではないでしょうか。対象の手続きによっては、セキュリティを優先すべきものもあると思うので、バランス良く書いていただきたいです。
		“セキュリティ強度の高低"という表現に少し違和感があります。現行版では「認証強度として求められるレベル（保証レベル）」と書かれていたので、そちらでいかがでしょう。
	表1-2 保証レベルの基本的な位置づけ	これは、ISO/IEC 29115 の Table 6-1 相当だが、Table 8-1 相当のものもあったほうが良いのではないか。
		書き方の問題だとは思うのですが、本人確認の保証レベルをここで包括的なものとして定めると、後続のIAL/AAL/FALのレベル分けと齟齬をきたしませんか？

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
5) セキュリティ（続き）	表1-2 保証レベルの基本的な位置づけ 保証レベル3 • 極めて厳格な強度の保証レベル。 • 本人確認の失敗が申請者の生命に影響を与え得る場合など、リスクの影響度が極めて大きい場合に該当する。	フェデレーションも含むことを考えると、単に「本人確認の失敗」とすると違和感がある。読み手が本人確認と聞いて、想像するものが曖昧、あるいは先入観をもってしまうため。
		本人に対するリスクは判りますが、国や社会のリスクはどのように考えられていますか。本人確認に失敗は「本人以外の人が本人と確認される」との解釈でよろしいでしょうか。 「本人を本人として確認するのに失敗した」リスクはここでは違うように受け止めています。
		改めて考えてみると、「行政手続きにおいて、失敗が申請者の生命に関わるような状況」がイマイチわかりません。民間であれば医療行為をする際に強固な本人確認が必要にも思いますが。 仮に生命に影響を与えうる（ので提供が必須の事業）であれば、ミッション遂行を考えれば厳格にする必要が無いように思います。 反対にマイナス影響が大きい場合（量刑など）も想定されるのでしょうか？
全般	政府機関における本人確認は、単に高いセキュリティを確保すればよいというものではなく、公平性やプライバシーなど様々な観点を考慮した検討が必要となる。本ガイドラインに基づく検討は、以下に示す5つの観点を念頭において実施するものとする。	後半に「影響度」に応じてアシュアランスレベルを選んでいるので、まずは、影響度を考えるが一番で、それに加えて、今の１）～５）を考えるのではないですか？「影響度」の話がないのは、後半と整合性が取れません。

特に協議いただきたいポイント

❶ 公平性への留意が求められる手法の例示について	• 複数の委員から「現在記載されている例は理解しにくく、別の例示とすべき」といった趣旨のコメントをいただいており、例示の修正を検討中です。 • より適切で理解しやすい例がありましたら、ご提案をお願いいたします。
❷ その他のご意見など	• 前述の記載案や委員コメント等に対して、追加のご意見・ご議論があればコメントをいただきたくお願いします。

ガイドライン改定案に対するコメント、意見交換

- 1. はじめに
- **2. 本人確認の枠組み**
- 3. 本人確認における脅威と対策
  - 3.1. 身元確認
  - 3.2. 当人認証
  - 3.3. フェデレーション

ガイドライン改定案「2. 本人確認の枠組み　―　2.1 本人確認の構成要素」

２．１　本人確認の構成要素

本ガイドラインでは、本人確認を「身元確認」、「当人認証」及び「フェデレーション」の3つの構成要素によって定義する。それぞれの構成要素の概要は次のとおりである。

表 2-1　本人確認の 3 つの構成要素の概要

構成要素	概要
身元確認 （Identity Proofing）	手続やサービスを利用しようとする申請者に対し、申請者の属性情報を収集することで、申請者を一意に識別すること
当人認証 （Authentication）	手続やサービスを利用しようとする者が、初回の利用時に登録された者と同一の人物であることを確認すること
フェデレーション （Federation）	身元確認及び当人認証の機能を提供する「ID プロバイダ」との連携によって、身元確認及び当人認証を実現すること

なお、必ずしも全ての構成要素を備える必要はない。例えば、初回の申請後、申請者が状況確認のためにシステムにログインすることが想定されない手続であれば、当人認証の機能は備えず、必要な場合には再度の身元確認を行う方針とすることもできる。

ガイドライン改定案「2. 本人確認の枠組み　―　2.2 本人確認モデル」

２．２　本人確認モデル

本人確認を実現するためのモデルとして、本ガイドラインでは「連携モデル（Federated Model）」と「非連携モデル（Non-Federated Model）」の2つのモデルを定義する。

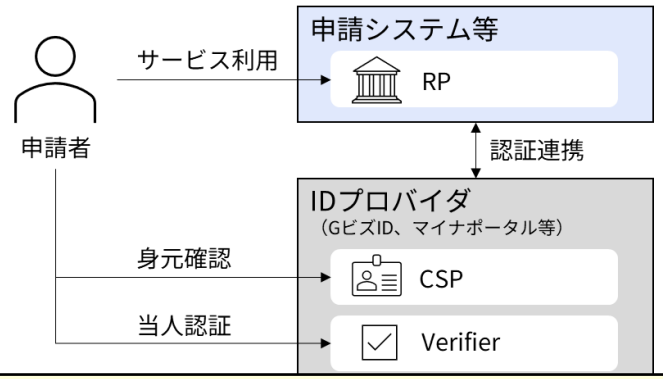
1)　連携モデル（Federated Model）

連携モデルは、IDプロバイダとのフェデレーションによって、身元確認や当人認証に関するアイデンティティ情報の連携を行うモデルである。

本モデルによって、IDプロバイダを複数システムで共用することができれば、対象手続それぞれが本人確認のための機能を重複して開発・運用することを避けることができ、利用者にとっても利便性の向上が期待できる。

また、自システムのみがIDプロバイダを利用する場合でも、IDプロバイダ機能とサービス提供機能が疎結合となることで、システムの拡張性や保守性の向上などのメリットが見込まれる。

本ガイドラインに基づく検討では、まずはこの連携モデルの採用を第一候補として検討することが望ましい。



注：上図はレビューのために2023年度の中間とりまとめの案を用いているが、
今後ガイドラインとして適切な用語・体裁を用いた図に差し替えを予定している。

表　2-2　連携モデルによるメリット

利用者側のメリット	サービス提供者側のメリット
・　身元確認が一度で済み、サービスごとに身元確認を行う手間が軽減される。 ・　当人認証において、サービスごとに別々の認証手法（パスワード等）を管理する必要がなくなり、同一の認証手法で複数のサービスを利用できる。	・　身元確認において、サービス提供者側で身元確認を行う負担が軽減される。 ・　当人認証に関するセキュリティ面の運用・管理の負担が軽減される。

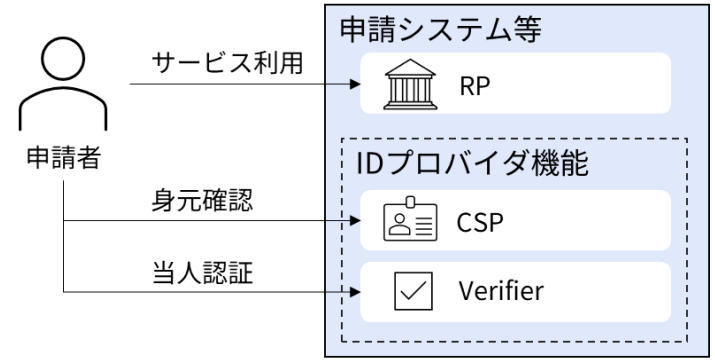
（前頁からの続き）

2)　非連携モデル（Non-Federated Model）

フェデレーション技術を用いず、本人確認に関する機能をサービス提供機能と一体となって実装するモデルである。

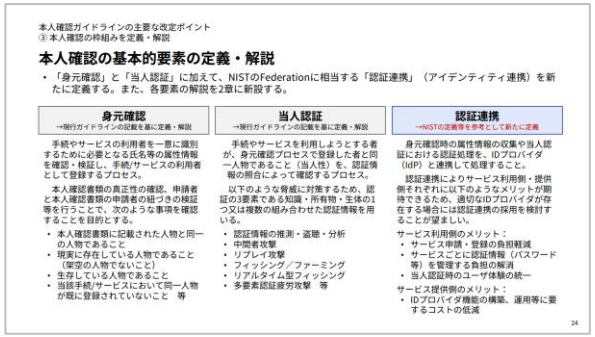
連携モデルと異なりIDプロバイダ機能を他システムと共同利用できないため、一般に構築・運用負担が高いモデルである。また、IDプロバイダ機能とサービス提供機能とが密結合となることで拡張性・保守性のデメリットも懸念される。

対象手続にとって合理的な理由がある場合にのみ採用することが望ましい。



注：上図はレビューのために2023年度の中間とりまとめの案を用いているが、
今後ガイドラインとして適切な用語・体裁を用いた図に差し替えを予定している。

委員の皆さまよりいただいた主なコメント　―　2.1 本人確認の構成要素

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
２.１　本人確認の構成要素	表 2-1　本人確認の3つの構成要素の概要 全般	概要部分、中間取りまとめP.24（以下）のような記載の方が全体がわかりやすいのでしょうか。例えば、身元確認では「本人確認書類の真正性の確認、申請者と本人確認書類の申請者の紐づきの検証等を行うことで、次のような事項を確認することを目的とする・・・」等の記載があった方が、構成要素それぞれに対する理解が深まるかと思います。  本人確認ガイドラインの主要な改定ポイント ③本人確認の枠組みを定義・解説 **本人確認の基本的要素の定義・解説** ・「身元確認」と「当人認証」に加えて、NISTのFederationに相当する「認証連携」（アイデンティティ連携）を新たに定義する。また、各要素の解説を2章に新設する。 **身元確認** →現行ガイドラインの記載を基に定義・解説 手続やサービスの利用者を一意に識別するために必要となる氏名等の属性情報を確認・検証し、手続/サービスの利用者として登録するプロセス。 本人確認書類の真正性の確認、申請者と本人確認書類の申請者の紐づきの検証等を行うことで、次のような事項を確認することを目的とする。 ・本人確認書類に記載された人物と同一の人物であること ・現実に存在している人物であること（架空の人物でないこと） ・生存している人物であること ・当該手続/サービスにおいて同一人物が既に登録されていないこと　等 **当人認証** →現行ガイドラインの記載を基に定義・解説 手続やサービスを利用しようとする者が、身元確認プロセスで登録した者と同一人物であること（当人性）を、認証情報の照合によって確認するプロセス。 以下のような脅威に対策するため、認証の3要素である知識・所有物・生体の1つ又は複数の組み合わせた認証情報を用いる。 ・認証情報の推測・盗聴・分析 ・中間者攻撃 ・リプレイ攻撃 ・フィッシング／ファーミング ・リアルタイム型フィッシング ・多要素認証疲労攻撃　等 **認証連携** →NISTの定義等を参考として新たに定義 身元確認時の属性情報の収集や当人認証における認証処理を、IDプロバイダ（IdP）と連携して処理すること。 認証連携によりサービス利用側・提供側それぞれに以下のようなメリットが期待できるため、適切なIDプロバイダが存在する場合には認証連携の採用を検討することが望ましい。 サービス利用側のメリット： ・サービス申請・登録の負担軽減 ・サービスごとに認証情報（パスワード等）を管理する負担の解消 ・当人認証時のユーザ体験の統一 サービス提供側のメリット： ・IDプロバイダ機能の構築、運用等に要するコストの低減 24
	表 2-1　本人確認の3つの構成要素の概要 「身元確認（Identity Proofing）」 手続やサービスを利用しようとする申請者に対し、申請者の属性情報を収集することで、申請者を一意に識別すること	識別のみが目的に見えてしまうので、 https://www.openid.or.jp/news/kyc_guideline_v1.0.pdf の定義を参照してもらうと良いかと思います。 当人認証も同様にOIDF-Jのガイドラインの定義を記載した方が良い気がします。
	「フェデレーション（Federation）」 身元確認及び当人認証の機能を提供する「IDプロバイダ」との連携によって、身元確認及び当人認証を実現すること	身元確認や当人認証に関する結果を信頼する外部システムに依存すること。（あくまでRP目線ですが） ※もっとうまい言い回しがありそう。少なくともIdPと連携することで身元確認と当人認証を実施しているわけではないと思います。

委員の皆さまよりいただいた主なコメント　―　2.2 本人確認モデル

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2.2　本人確認モデル	本人確認を実現するためのモデルとして、本ガイドラインでは「連携モデル（Federated Model）」と「非連携モデル（Non-Federated Model）」の2つのモデルを定義する。	二つのモデルのメリット、デメリットを提示し、「連携モデル」のデメリットを補強するために必要な要件が示されていることも提示し、その結果として、なぜ「連携モデル」の採用を第一候補として検討するのが望ましいかの理由がわかりやすく、読者に腹落ちしやすいようにすることが望ましいと思います。
		連携モデルと非連携モデルと選択させるのであれば、メリットとデメリットの両方が必要だと思います。 つまり、デメリットも書きましょう。
		中間取りまとめP.26に記載の留意点も記載した方が良いかと思います。もしくはメリット・デメリットという形で表現した方がわかりやすいかと思います。　※非連携モデルも同様
	（モデルの名称について）	シンプルに"フェデレーション（又はテッド）モデル”、”非フェデレーション（又はテッド）モデル”でいかがでしょうか？
1)　連携モデル（Federated Model）	...本ガイドラインに基づく検討では、まずはこの連携モデルの採用を第一候補として検討することが望ましい。	利用できるIDプロバイダがある場合や、複数のシステムで本人確認をすることが想定される場合などIDPに括りだすケースの具体的表現を追加してはどうか。
		言い換えると「IdPを統合していくぞ」というメッセージを書いても良いのではないか。独自で作るのではなく、連携を前提として考えろ、というところまで。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　非連携モデル（Non-Federated Model）	フェデレーション技術を用いず、本人確認に関する機能をサービス提供機能と一体となって実装するモデルである。	本書のコンテキストでフェデーションを技術と捉えるのか、システムモデルと捉えるのかを統一した方が良いと思います。
	対象手続にとって合理的な理由がある場合にのみ採用することが望ましい。	「合理的な理由」の例示があった方が親切かと思います。

特に協議いただきたいポイント

❶ 連携モデル/非連携モデルのメリット・デメリットについて	• 皆様からのご指摘を踏まえ、連携モデル/非連携モデルのメリット・デメリットは改めて整理し、ガイドラインに明記する方針とします。 • 現在の記載案を踏まえ、特に言及しておくべきメリット・デメリットの観点についてご意見を伺いたくお願いします。

❷ モデルの名称について	• 今回の案では「連携モデル」、「非連携モデル」という名称を用いましたが、より適した名称の案があればご提案ください。
	  • 「非連携」という表現はネガティブな表現と捉えられる懸念があるか
	  • 機械翻訳の観点からは、直訳に近いモデル名が望ましいか、など

❸ その他のご意見など	• 前述の記載案や委員コメント等に対して、追加のご意見・ご議論があればコメントをいただきたくお願いします。

ガイドライン改定案に対するコメント、意見交換

- 1. はじめに
- 2. 本人確認の枠組み
- **3. 本人確認における脅威と対策**
  - **3.1. 身元確認**
  - 3.2. 当人認証
  - 3.3. フェデレーション

ガイドライン改定案「3.1. 身元確認（Identity Proofing）」

1) 身元確認における脅威と対策

３．１　身元確認（Identity Proofing）

（赤字：誤記訂正）

1)　身元確認における脅威と対策

身元確認では、以下に示すなりすましや不十分な識別等の脅威が想定される。このような脅威への対策として、本人確認書類が偽造・改ざんされていないことの検証や、申請者が確かに本人確認書類に記載の人物であることの検証を行う。

表　3-1　身元確認における主な脅威と対策

脅威	脅威の概要	脅威への対策
不十分な識別	申請情報の不足、誤り、表記揺れ等によって ・　同一人物であるにもかかわらず別人として扱い、重複した申請を受け付けてしまう ・　別の人物であるにもかかわらず同一の人物として扱ってしまい、別人の情報と紐づけてしまう	適切な収集手段によって、識別に必要な属性情報を正確に収集する
なりすまし	本人確認書類の偽造等によって、 ・　実在する別人になりすました者からの申請を受け付けてしまう ・　過去に存在していたが現在は生存していない人物になりすました者からの申請を受け付けてしまう ・　実在しない架空の人物になりすました者からの申請を受け付けてしまう	本人確認書類が偽造・改ざんされていないことを検証する ＋ 本人確認書類が確かに申請者のものであるかを検証する

2) 身元確認のプロセスと手法　―　ア　属性情報の収集（Resolution）

2） 身元確認のプロセスと手法

ア　属性情報の収集（Resolution）

申請者を一意に識別するための属性情報（氏名、生年月日、住所等）と、その証拠となる本人確認書類を申請者から収集する。

ここでは、特に前述する「不十分な識別」によるリスクを考慮する必要がある。収集する情報が不足していたり、不正確であったりすると、申請者を一意に識別できない原因となる。
そのため、属性情報の収集に当たっては、可能な限り収集した属性情報の誤記や表記揺れが発生しない方法による収集が望ましい。また、デジタルによる手法においては、当該情報を取り扱うシステムにおける異体字や外字の取扱いに関する仕様・制約に留意する必要がある。属性情報の収集に関する主な手法を以下に示す。

a）　本人確認書類から電子データを読み取る

本人確認書類に搭載されたICチップ等から、必要な属性情報を電子データとして読み取る方式。属性情報を電子データのまま取り扱うことができるため、誤記や表記揺れのリスク低減が期待できる。

また、「属性情報の収集」と「本人確認書類の検証」を同時に行うことができるため、ユーザビリティの面でもメリットがある。

b）　本人確認書類の券面からOCRで読み取る

本人確認書類の券面から、必要な属性情報をOCRで読み取る方式。人手作業での記入を求める方式と比べて誤記や表記揺れのリスク低減が期待できるが、OCRの読取精度によって一定のリスクは残存する。

c）　申請様式や申請フォームへの記入・入力を求める

紙、電子ファイル、入力フォームにより、申請様式への記入・入力を求める方式。
従来から広く用いられてきた手法であるが、人手作業による記入や入力を伴うため、誤記、表記揺れのリスクが想定される。

d）　IDプロバイダから取得する

（赤字：誤記訂正）

連携モデルでは、IDプロバイダに身元確認を依拠し、IDプロバイダから必要な属性情報を取得することもできる。この場合、後続の「本人確認書類の検証」や「申請者の検証」は実施済みのものとして取り扱うことができる。

ただし、IDプロバイダが有する属性情報がどの程度の正確性を有しているのか（どの程度の誤記や表記揺れ等のリスクを含んでいるのか）については、IDプロバイダが身元確認において採用している収集方法による。

2) 身元確認のプロセスと手法　―　イ　本人確認書類の検証（Evidence Validation）

イ　本人確認書類の検証（Evidence Validation）

身元確認におけるなりすまし等の不正を防ぐため、収集した本人確認書類に対して、それが偽造・改ざんされたものでないこと、有効期限超過や紛失等によって失効したものでないことを検証する。

主要な検証方法は以下のとおりである。検証方法によって偽造・改ざんへの耐性は大きく異なる。

a)　デジタル署名の検証

本人確認書類から取り出した電子データに付与されたデジタル署名を検証することで、データの発行元と、データが発行後に改ざんされていないことを検証する方法。

デジタル署名のもつ暗号学的な性質に基づき、厳密な検証が可能である。

b)　信頼できる情報源との照合

本人確認書類に一意に付番された番号等を用いて、本人確認書類の発行元が提供するデータベース等の信頼できる情報源に本人確認情報を照会し、本人確認書類に印字された内容と一致していることや、有効であることなどを確認する方法。

この方法を採用できる手続等は多くないが、発行元が有する情報を直接取得できるため、厳密な検証が可能である。

c)　対面での券面の検査

対面での手続において、本人確認書類の券面を物理的（視覚的・触覚的）に検査することで、偽造・改ざんがされていないことを検証する方法。

この手法による検証の強度は、検査を行う環境（照明の明るさ等）、検査に利用できる道具、本人確認書類の偽造対策技術（ホログラムやパールインキ等の印刷技術等）の有無、検査を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。

d)　非対面での券面の検査

カメラによる画像・動画の撮影、複合機等による複写・スキャン等によって、本人確認書類の券面を非対面で検証する方法。

手法により強度の差はあるが、この手法による精巧な偽造・改ざんの検知は難しく、対面の場合と比べて検証の強度は著しく低くなる。

2) 身元確認のプロセスと手法　―　ウ　申請者の検証（Verification）

ウ　申請者の検証（Verification）

「本人確認書類の検証」によって本人確認書類が真正かつ有効であることを確認できた場合においても、正規の本人確認書類が盗難や貸し借りによって悪用されるリスクがある。そのため、本人確認書類が確かに申請者のものであるかを検証する必要がある。

主な検証方法は以下のとおりである。検証方法によって検知可能な攻撃や強度が異なる点に留意が必要である。

a)　対面での容貌比較

対面において、本人確認書類に含まれる顔写真と申請者の容貌とを見比べ、同一の人物であることを検証する方法。

この検証の強度は、検証を行う環境（照明の明るさ等）、検証時の条件（帽子やマスク等の着脱等）、本人確認書類の顔写真の精度、検証を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。

b)　非対面での容貌比較

オンラインでの手続において、カメラで撮影された映像・画像等が観察することで、本人確認書類に含まれる顔写真と申請者の容貌とを見比べ、同一の人物であることを検証する方法。

この検証の強度は、カメラでの撮影を行う環境（照明の明るさ等）、カメラの解像度、本人確認書類の顔写真の精度、検査を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。顔照合技術等を用いて検査担当者を介さずに行う場合は、当該技術の精度によっても左右される。

また、カメラに偽の映像・画像を流し込む、通信途中にデータを差し替える、AI技術等を用いてリアルタイムに加工するなど、この手法特有の攻撃への対策検討が必要となる。

c)　認証機能による認証

ICチップを備える本人確認書類、スマートフォンに搭載された本人確認書類等において、それらが備える暗証番号や生体認証等の認証機能を利用して申請者を検証する方法。

この検証の強度は、認証に用いる要素、認証機能の精度や仕様等に左右されるが、検証の環境や担当者の技能等に左右されにくく、一定の強度が期待できる。

本人確認書類の持ち主と攻撃者が結託し、本人確認書類と暗証番号が攻撃者に共有された場合などには、この方法では検知できない点に留意が必要である。

d)　確認コードの送付による検証

本人確認書類に記載された住所等の連絡先に対して「確認コード（4桁の番号等）」を送付し、申請者がそのコードを入力できることをもって申請者と本人確認書類との紐づきを検証する方法。

この方法は、顔写真を含まない本人確認書類であっても住所等の連絡先の記載があれば検証を実施できる利点がある。ただし、確認コードを郵送する場合は身元確認をその場で完結できない点に留意が必要である。

この検証の強度は確認コードの送達手段等に依存するが、検証の環境や担当者の技能等に左右されにくく、対面・オンラインのいずれにおいても一定の強度が期待できる。

本人確認書類の持ち主と攻撃者が結託し、本人確認書類とともに確認コードが攻撃者に共有された場合には、この方法では検知できない点に留意が必要である。

なお、本人確認書類に紐づかない連絡先に確認コードを送付しても「検証」の意味を果たさない点に留意が必要である。

3)　身元確認保証レベルと対策基準

- 「3)　身元確認保証レベルと対策基準」については、第2回有識者会議での議論結果を踏まえ保証レベル全体を見直し中であるため、第4回会議にて修正方針とともに議論を行う方針とします。
- 今回いただいたコメントについても、第4回会議においてとりまとめます。

委員の皆さまよりいただいた主なコメント　―　3.1. 身元確認

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
1)　身元確認における脅威と対策	目次の流れ	先に2)のプロセスの説明があって、1)脅威と対策の流れの方が良いのではないでしょうか。
	身元確認では、以下に示すなりすましや不十分な失敗等の脅威が想定される。このような脅威への対策として、本人確認書類が偽造・改ざんされていないことの検証や、申請者が確かに本人確認書類に記載の人物であることの検証を行う。	「本人確認書類」というワードは市政で一般的であるものの、他の部分との表記揺れを生じるので「身元確認書類」にする可能性を考えたい。
	表 3-1　身元確認における主な脅威と対策 「不十分な識別」	わかりにくい言葉という印象です。"重複登録 または 別の人物との紐付け”もしくは"誤登録"でいかがでしょう。
		「本人であるにも関わらず申請を受け付けない。」は別のリスクとして出てきますが、ここでは対象外とするとしても、何処かに記載が必要と思います。追加情報により本人を正しく確認して救うためのプロセスは別にあっても良いと思います。
	表 3-1　身元確認における主な脅威と対策 「なりすまし」 本人確認書類の偽造等によって...	盗難、貸し借りも明記した方がよりイメージできると思います。
	表 3-1　身元確認における主な脅威と対策 「不十分な識別」と「なりすまし」	この脅威の順番を入れ替えた方が理解しやすいと思います。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　身元確認のプロセスと手法	全般	身元確認を完了させるためには、ア→イ→ウのプロセスがあり、それぞれこのような目的のためにこのようなことをします、というような全体の説明文章（又は図）があった方が良いと思います。 もしくは、当人認証やアカウント復帰を含めたアイデンティティライフサイクルを図示し、その中で”身元確認はこの部分”という説明でも良いかと思います。
		どういうポリシーのもとで作られたどの属性を集めるかというプロセスが抜けている。これらに対する文書化の要求も落ちている。
ア　属性情報の収集（Resolution）	ア　属性情報の収集（Resolution） ... また、デジタルによる手法においては、当該情報を取り扱うシステムにおける異体字や外字の取扱いに関する仕様・制約に留意する必要がある。属性情報の収集に関する主な手法を以下に示す。	外国出身者の場合、母国語での発音とそれに基づく表記と、日本語でのカタカナ表記に差異が出るとか、揺れが生じるなどの事態もあり得るかと、今更ながら思いました。
	a)　本人確認書類から電子データを読み取る ...また、「属性情報の収集」と「本人確認書類の検証」を同時に行うことができるため、ユーザビリティの面でもメリットがある。	利用者目線ですと「本人確認書類の検証」はRP側のタスクなので、必ずしも同時に行う事がメリットとは言い切れない印象です。 もちろん、その他の手法と比べてやり直しがほぼ発生しない、という意味でのメリットはあると思います。
		JPKI・ワ方式では署名を伴い、単にICチップから属性情報を収集し、かつ本人確認書類の検証を同時に行っているためユーザビリティにメリットがあるとは言い難い面があり、この文については削除を含めて検討した方が良いと感じました。
	b)　本人確認書類の券面からOCRで読み取る	券面偽造のリスクを書くべきでは？この先には、券面偽造のリスクも書いてあったと思います。
	d)　IDプロバイダから取得する 連携モデルでは、IDプロバイダに身元確認を依拠し、...	依拠という言葉によって過去に民間企業等でのインシデントが発生しているので、概要を説明する部分でも、フェデレーションの際に両社で合意すべきIAL/AAL/FALの話は触れておきたい。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
イ　本人確認書類の検証（Evidence Validation）	イ　本人確認書類の検証（Evidence Validation） 全般	実施場所と検証方法を分けて記載してはいかがでしょうか。表3-3で初めて実施場所の概念が出てきており、実施場所も保証レベルを決定する条件になっていますので説明が必要かと思います。 ※Verificationも同様 -4で追加された、Remote Unattended/Attended、Onsite Unattended/Attendedなども踏まえて記載するとより明確になると思います。
	b)　信頼できる情報源との照合 …この方法を採用できる手続等は多くないが、発行元が有する情報を直接取得できるため、厳密な検証が可能である。	公的個人認証の有効性確認を行える手続きはどんどん増えている印象です。むしろこの方法を採用できる”本人確認書類”が多くないのではないでしょうか。
	c)　対面での券面の検査 …この手法による検証の強度は、検査を行う環境（照明の明るさ等）、検査に利用できる道具、本人確認書類の偽造対策技術（ホログラムやパールインキ等の印刷技術等）の有無、検査を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。	それに伴ってIdentity documentの種類や強度、枚数の議論が出てくると承知しており、現状はそこに対する議論が十分ではない認識。左右されるのは事実として、それだけの記載は運用者側にとって困るので、ではどうするのか、どう考えて使うのか補足したい。 ※「d) 非対面での券面の検査」についても同様のコメント
	d)　非対面での券面の検査 …手法により強度の差はあるが、この手法による精巧な偽造・改ざんの検知は難しく、対面の場合と比べて検証の強度は著しく低くなる。	カメラによる撮影と比べ、複写（コピー）は現物でないことから信頼性が一段下がると思われます（とはいえ、日本ではまだ残っている）。表現が難しいですが分けて記載するか、一段下がることを明記してはいかがでしょうか。
		「著しく」とまで書くべきか。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
ウ　申請者の検証（Verification）	a)　対面での容貌比較 対面において、本人確認書類に含まれる顔写真と申請者の容貌とを見比べ、同一の人物であることを検証する方法。	本人確認書類は、Validate済みである必要があることを明記したい。
	c)　認証機能による認証	必ずしも認証機能とはいえない。券面の正しさだけを確認するIFがついていて認証機能がないICカードがあった通して、デジタルには真正性を確認できるので。
		特に、生体認証は、 ・本人排他率 ・他人受入率 を解説してあげた方がいいかと思います。
	d)　確認コードの送付による検証 …本人確認書類の持ち主と攻撃者が結託し、本人確認書類とともに確認コードが攻撃者に共有された場合には、この方法では検知できない点に留意が必要である。	本人限定受取郵便への言及は不要でしょうか。想定リスクとして結託が記載されているが、空き家問題や郵便物窃取の想定リスクと照らして複数のレベルにわたって考慮できる内容と考える。ここは議論が十分になされていないという認識。
		郵送の場合は本人限定郵便などを使ってより確実に本人へ到達することを求めることも記載できると良いと思います。
		昔、電子署名法の議論では、攻撃者がなりすまして、申請し、確認コードを郵便受けから盗むのは比較的簡単ではないかという議論がありました。そのため、転送禁止の郵便物に限定した覚えがあります。結託でないレベルの攻撃が必要かも。
		保証レベル2より弱い、だったと思うので表現を工夫（今の表現だと、担当者の技能等に左右される2E,2Dより強そう）。
	なお、本人確認書類に紐づかない連絡先に確認コードを送付しても「検証」の意味を果たさない点に留意が必要である。	現在の記載は、メアドやSMSを除外できているように思う。 一方で、キャリア（連絡先を確実に把握）が実施するSMSやSIMなどまで除外されそうで、どこまで書くか悩ましい。

特に協議いただきたいポイント

❶ 脅威とプロセスの記載順について	• 「1) 身元確認における脅威と対策」と「2) 身元確認のプロセスと手法」は逆順でもよいのでは、というご意見を踏まえ、ガイドラインとして望ましい記載順や、脅威をプロセスより先に書く場合の留意点などについてご議論をお願いします。
❷ 様々な要因によって強度に幅の生じる手法の解説について	• 例えば券面の検査における照明の明るさ、検査に利用できる道具、本人確認書類の偽造対策技術の有無、検査を担当する者の経験・技能、マニュアルや訓練の有無など、このガイドラインでどこまで踏み込んで記載すべきか、ご議論をお願いします。
❸ 各種手法に対する各種コメントについての議論	• 「非対面での券面の検査」を、カメラ越しとコピー提出で定義し分けるべきか。 • 「確認コードの送付による検証」における郵送のリスク（窃取、空き家問題）をどこまで想定すべきか。
❹ その他のご意見など	• その他、追加のご意見・ご議論があればコメントをいただきたくお願いします。
❺ 「本人確認書類」という用語の置き換えについて （時間があれば）	• 「本人確認書類」ではなく「身元確認書類」と書くべきでは、というご意見がございました。ガイドラインとして望ましい用語についてご議論をお願いします。 （時間がない場合は、別途の議論テーマとさせていただきます。）

ガイドライン改定案に対するコメント、意見交換

- 1. はじめに
- 2. 本人確認の枠組み
- **3. 本人確認における脅威と対策**
  - 3.1. 身元確認
  - **3.2. 当人認証**
  - 3.3. フェデレーション

ガイドライン改定案「3.2. 当人認証（Authentication）」

1) 当人認証における脅威と対策

３．２　当人認証（Authentication）

1)　当人認証における脅威と対策

当人認証では、パスワード等に代表される認証情報の推測、漏えい、窃取等によるなりすましが主な脅威となる。

また、利用者が認証情報を紛失・喪失した際のアカウント回復手続においても、第三者がアカウント回復手続を悪用してアカウントを乗っ取る攻撃を想定し、適切な対策を講じる必要がある。

表　3-8　当人認証における主な脅威と対策

脅威	脅威の概要	脅威への対策
なりすまし	認証情報の推測、漏洩、窃取、複製等によって、第三者が本人になりすまして不正にログインする	複数の認証要素を組み合わせた多要素認証の採用する、攻撃への耐性を有する認証技術の採用する
アカウントの乗っ取り	アカウント回復手続を悪用し、第三者が本人になりすましてアカウントの認証情報を再設定する	適切なアカウント回復手続の設計

2) 当人認証のプロセスと手法　―　ア　認証情報（Authenticator）

2）当人認証のプロセスと手法

当人認証における認証情報には、「認証の3要素」と呼ばれる「知識」、「所有物」及び「生体」が用いられる。当人認証では、これらのうち1つ又は複数の要素を組み合わせて利用する。ただし、生体認証は他の認証要素と組み合わせて利用することを前提とし、単独の認証要素として利用することはできない。

a）　パスワード

パスワードは、オンラインサービスにおいて最も普及している知識認証の一つである。推測攻撃への対策として、設定可能な最小の桁数を制御したり、推測されやすいパスワードの設定を禁止したりするなどして、一定の複雑性を確保することが必要である。

しかしながら、利用者が複数サービスでパスワードを使い回すことが少なくなく、他サービスから漏洩したパスワードによって不正アクセスを受けるリスクがある。また、フィッシング攻撃によってパスワードを窃取される攻撃に対しても脆弱である。こうしたリスクはユーザの行動に依存する部分があるため、パスワードのみでの根本的な対策は難しい。

b）　アクティベーションコード

アクティベーションコードは、一般に4～6桁の数字などで構成される認証情報であり、知識認証の一種である。「PIN（Personal Identification Number）」や「暗証番号」などと呼ばれることもある。

本ガイドラインでは、機器やICカード等のデバイスに紐づけられ、認証時にデバイス外に送信されることがなく、デジタル証明書などの他の認証要素との組み合わせによって多要素認証を実現するものを「アクティベーションコード」として定義する。アクティベーションコードを単独の認証情報として用いることは想定していない。

c）　ICカード等に格納されたデジタル証明書

ICカード、スマートフォン、USB接続型セキュリティキー等に格納したデジタル証明書により、所有物認証を行うものを指す。代表例として、マイナンバーカードに格納された公的個人認証（利用者証明用電子証明書）がある。

アクティベーションコードや生体認証と組み合わせることで、多要素認証を実現する方式も多い。

通常、デジタル証明書はデバイスから外部に取り出すことはできない仕組みとなっているが、複数のデバイス間でデジタル証明書を同期できる技術も存在する。

（次頁へ続く）

2) 当人認証のプロセスと手法　―　ア　認証情報（Authenticator）

（前頁からの続き）

d)　ワンタイムパスワード

一回限りのパスワードを生成して認証する方式。デバイス等の所有物に紐づくものは所有物認証に該当し、代表例としてスマートフォン用のTOTP（Time-based One-Time Password）アプリ、物理的なワンタイムパスワード専用デバイス（ハードウェアトークン）、携帯電話番号を使ったSMSへのワンタイムパスワード送信などがある。

ワンタイムパスワードは多要素認証の一要素として用いられることが多いが、リアルタイム中継型のフィッシング攻撃への耐性は有さないことに留意が必要である。

SMSを用いてワンタイムパスワードを送信する方式は、SIMスワッピング攻撃により利用者が携帯電話番号を不正に奪取されるリスク、第三者によってSMS認証の代行が行われるリスク、携帯電話番号の再割り当てが行われるリスク等があるため、採用に当たってはこれらのリスクを受容できるか個別のリスク評価が必要である。

電子メールアドレスに対してワンタイムパスワードを送信する方式は、電子メールへのアクセスがパスワードに依存している場合が多くパスワードと同時に侵害される可能性があることや、メールの送信経路中で傍受されるリスクがあること等を踏まえ、採用に当たってはこれらのリスクを受容できるか個別のリスク評価が必要である。

e)　スマートフォン等による生体認証

生体認証機能を搭載したスマートフォン、PCにおいては、格納したデジタル証明書をアクティベーションするために生体認証を利用できるものがある。これを認証情報として利用する場合、所有物認証＋生体認証による多要素認証として扱うことができる。

f)　セキュリティキー等に搭載された生体認証

デジタル証明書を格納するための認証用セキュリティキーには、アクティベーション用に生体認証機能を備えるものもある。ICカードについても同様に生体認証機能を備えるものがある。これらを利用する場合、所有物認証＋生体認証による多要素認証として扱うことができる。

2) 当人認証のプロセスと手法　―　イ　想定脅威と対策例

イ　想定脅威と対策例

a)　オンライン推測攻撃

攻撃者がサービスに繰り返しログインを試行するなどして認証情報を推測しようとする攻撃。パスワード特有の脅威である。

対策例として、パスワードの複雑性の確保、一定時間あたりの認証回数の制限、知識以外の認証要素の採用等がある。

b)　オフライン推測攻撃

攻撃者が何らかの方法で取得したパスワード等のハッシュ値を用いて、オフライン環境でパスワードの推測を行う攻撃。パスワード特有の脅威である。

対策例として、パスワードの複雑性の確保、ソルト等の対策技術の導入、知識以外の認証要素の採用等がある。

c)　使い回されたパスワードの漏えい

他サービスから漏洩したIDとパスワードを使ってログインを試行するなどして認証情報を推測しようとする攻撃。パスワード特有の脅威である。

対策例として、他サービスで使いまわしにくいIDの採用、知識以外の認証要素の採用等がある。

d)　リプレイ攻撃

攻撃者が認証に関する通信を盗聴し、同じ内容を再度送信してなりすましを行う攻撃。

対策例として、サーバ認証及び通信の暗号化、チャレンジレスポンス方式の採用、nonceの導入、ワンタイムパスワードの採用等がある。

（赤字：誤記訂正）

e)　フィッシング攻撃

攻撃者が利用者を偽のサイトに誘導し、パスワード等の認証情報を窃取・中継する攻撃。

対策例として、サービスと認証情報とを紐づけられる技術（FIDO等）の採用、クライアント認証等がある。

なお、窃取された認証情報をリアルタイムに中継されるタイプの攻撃に対して、ワンタイムパスワードは対策として機能しない点に留意が必要である。

f)　秘密鍵の不正な取り出し・複製

秘密鍵が格納されたデバイスやアカウントに対して不正なアクセスや解析を行い、秘密鍵の窃取や複製を行おうとする攻撃。

対策例として、耐タンパ性を有するハードウェア等の利用、暗号鍵の安全な管理を目的とした仕組みの採用、秘密鍵の複製・同期・バックアップの禁止等が考えられる。

2) 当人認証のプロセスと手法　―　ウ　アカウントの回復（Account Recovery）

ウ　アカウントの回復（Account Recovery）

アカウント回復の代表的な手法は以下のとおりである。

a)　身元確認の再実施

初回登録時と同様の身元確認を再度実施する方式。初回登録時と同様の身元確認を行うことで、アカウントの回復特有の手続きに起因する脆弱性を生みにくいが、利用者にとっての利便性が低下する場合がある。

なお、身元確認において「本人確認書類の紛失時の例外措置」を設けている場合でも、アカウント回復においては例外措置を適用不可とすべきである。

b)　リカバリーコードの事前発行

アカウントの登録時にリカバリー専用のコードを発行しておき、アカウント回復が必要となった際にリカバリーコードの入力を求める方式。

リカバリーコードは登録時にのみ発行されるため、攻撃者が能動的にリカバリーコードを不正入手できる機会が少なく、比較的強度が高い方式であるが、利用者はリカバリー用コードを適切に保管しておく必要がある。

c)　リカバリーコードの必要時発行

利用者の求めに応じて、利用者の連絡先（住所、電子メール、携帯電話番号等）に対してリカバリーコードを送信し、入力を求める方式。

利用者はリカバリー用コードを保管する必要がないが、攻撃者が電子メールアカウントの乗っ取り等を経由してリカバリーコードを不正に発行・窃取する攻撃への考慮が必要である。

d)　予備の認証情報の登録

予備の認証情報（例えば、セキュリティキーに格納されたデジタル証明書など）をあらかじめ登録しておくという手法も考えられる。

複数の認証情報の保証レベルや脅威耐性の差がリスクに繋がる恐れがある点に留意が必要である。

3) 当人認証保証レベルと対策基準

ア　当人認証保証レベルの位置づけ

当人認証の保証レベルは、以下の３段階で定義する。

表 3-9　当人認証保証レベルの定義

当人認証保証レベル	保証レベルの位置づけと概要
レベル3	[位置づけ] ・　極めて厳格なレベル。当人認証が失敗したとき、組織活動に致命的な影響が及ぶ、利用者の生命や財産に致命的な影響が及ぶなど、リスク顕在化時の影響度が極めて高い、一部の対象手続のみが該当するレベルとして想定。 [対策基準の概要] ・　認証の3要素のうち2要素以上を用いる。 ・　全ての利用者が、フィッシング攻撃への耐性を有する認証情報を利用する。 ・　耐タンパ技術等により電子的な複製攻撃への耐性を有し、かつ他のデバイスと同期・共有されない認証要素を含む
レベル2A	[位置づけ] ・　高い強度の当人確認 を行うレベル。当人認証に関するリスクの高い対象手続が該当するレベルとして想定。 [対策基準の概要] ・　認証の3要素のうち、2要素以上を用いる。 ・　利用者が希望する場合には、フィッシング攻撃への耐性をもつ認証要素を利用可能とすることを必須とする。
レベル2B	[位置づけ] ・　標準的な強度の当人確認を行うレベル。当人認証に関するリスクが標準的な対象手続が該当するレベルとして想定。 [対策基準の概要] ・　認証の3要素のうち、2要素以上を用いる。
レベル1	[位置づけ] ・　簡易的な当人認証を認めるレベル。リスク影響度が比較的 低い対象手続が該当するレベルとして想定。 [対策基準の概要] ・　認証の3要素のうち、「知識」又は「所有」のいずれか1 要素による認証を行う

3) 当人認証保証レベルと対策基準

イ　当人認証保証レベルの対策基準

当人認証の各保証レベルの対策基準は以下のとおりである。

表　3-10　当人認証保証レベルの対策基準（認証情報）

脅威	当人認証保証レベル			
	3	2A	2B	1
a.　オンライン推測攻撃	○	○	○	○
b.　オフライン推測攻撃	○	○	○	○
c.　使い回されたパスワードの漏えい	○	○	○	—
d.　リプレイ攻撃	○	○	○	—
e.　フィッシング攻撃への耐性	○	○ ※1	—	—
f.　秘密鍵の不正な取り出し・複製	○	—	—	—

※1：全ての利用者にフィッシング攻撃への耐性を求めることは必須としないが、希望する利用者がフィッシング耐性を有する方式を利用可能であることを必須とする

表　3-11　当人認証保証レベルの対策基準（アカウント回復）

アカウント回復手続	当人認証保証レベル			
	3	2A	2B	1
a.　身元確認の再実施				
b.　リカバリーコードの事前発行				
c.　リカバリーコードの必要時発行				
d.　予備の認証情報の登録				

アカウント回復の対策基準については現在検討中。

委員の皆さまよりいただいた主なコメント　—　3.2. 当人認証

1) 当人認証における脅威と対策

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
1) 当人認証における脅威と対策	Authenticatorの訳語について	"認証器"でしょうか。ただ、読む側がイメージできない可能性がありますので、"認証情報"でも良いかと思います。
		認証情報(Authenticator)だと資格情報(Credential)やCookie/Passwordなど様々なものが思い浮かぶことが懸念されるため、NISTのrev2からrev3の変化でAuthenticatorという言葉が導入された際に私が選択した認証器という表現を推します。認証子もありますが、一般的には難しいように思います。
		認証器に慣れてしまっているので認証器の方が良いかと思いますが、正しい訳とも思いませんので、いっそのこと認証手段くらいにしてしまっても良いかと思います。
		NIIでは「認証器」と言っています。
	文書構成：脅威と対策の整理方法について	直接的なAuthenticatorではなく一般論にはなりますが、認証の3要素ごとに想定される脅威を記載してはいかがでしょうか。（800-63B-4の6.1冒頭のイメージ） ア：で定義されているAuthenticatorは組み合わせがあり、その組み合わせによっても脅威耐性が変わため、脅威と整理をするのは難しい印象です。800-63B-4にならってア：の中でフィッシング耐性の有無を記載するのも良いかと思います。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
1) 当人認証における対策と脅威（続き）	表 3-8　当人認証における主な脅威と対策 ★事務局からのレビュー依頼ポイント ・「推測攻撃」、「フィッシング攻撃」など、もっと具体的な粒度で記載すべきか？	記載すべきと思います。
		ちょっとざっくりし過ぎでは？と思います。
		曖昧さ回避のため、複数の脅威内容が想像できるような粒度の記述は避けるのが良いと考えます。
		1.1 3.) で「フィッシング対策の強化」に触れてあり、昨今の状況から「フィッシング攻撃」は主な脅威として記載は必須のように思います。
		認証情報の推測、漏洩、窃取（詐取）等による「なりすまし」が主な脅威で、結果的にどんな好ましくない、望ましくない、起こってはいけない事象が発生するかにまで踏み込んでおくことで、理解が進むように思います。 「不正決済、不正送金、個人（法人）情報漏洩、ランサムウェアなどによる攻撃、その他」など。 これらを防ぐため、当人認証の保証レベルを高めることが期待されており、近年では推察、漏洩にも増して窃取（詐取）すなわちフィッシング攻撃による被害が増えていることから、フィッシング耐性のある多要素認証（パスキーなど）が必要とされている、NIST SP800-63-4Bでもその必要性が明確に記されるようになったということを反映していくことが望ましいと考えます。
		攻撃手法（は陳腐化しやすい、新しいものが出やすい）と脅威の対応関係などを別冊にするのはどうか。
		攻撃者が申請者になりすますケースと、攻撃者が申請者を誘導するフィッシングのケースは分けて書いた方が良いと思います。（対策が異なるため）
		３.2のイの内容に合わせるべきでは。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
1) 当人認証における対策と脅威（続き）	表 3-8　当人認証における主な脅威と対策 「アカウントの乗っ取り」	これも"なりすまし"の一種だと思われますので、シーンで分けるとわかりやすいかもしれません。
		アカウント回復手続きと、最初の身分証明書を発行するための本人確認の手続きは、似ているところがあると思います。運転免許証、パスポートを所持していない人がマイナンバーカードを紛失し再発行申請を行うための手続きが一番厄介で、写真で本人と紐づけが出来る民間証明書の活用なども考えていく必要があるのではないでしょうか。
		アカウントの乗っ取りも、上記（上では5点提示）に並ぶ一つの事象と思います。実際のところ、不正決済・不正送金などをしている瞬間は乗っ取りが行われているわけですが、その後住所などを戻して立ち去るケースもあり、乗っ取りという表現だけでは不十分に感じられます。
		認証器のエンロールのプロセスについても記載できると良いと思います。ID登録時に認証器を登録させることでEntityとAuthenticatorのバインディングを強めることが重要だと思います。

委員の皆さまよりいただいた主なコメント　—　3.2. 当人認証

2) 当人認証のプロセスと手法　ア　認証情報(Authenticator)

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　当人認証のプロセスと手法 ア　認証情報(Authenticator)	ア　認証情報(Authenticator) 当人認証における認証情報には、「認証の3要素」と呼ばれる「知識」、「所有物」及び「生体」が用いられる。当人認証では、これらのうち1つ又は複数の要素を組み合わせて利用する。 ただし、生体認証は他の認証要素と組み合わせて利用することを前提とし、単独の認証要素として利用することはできない。	もはや認証の３要素にこだわるのはやめたほうが良いのではないか。わるい３要素はだめなので。むしろ、どの脅威を潰しているかで議論したほうが良い。良い１要素は悪い３要素を凌ぐ。
		生体情報は確かに、知識情報、所持情報とレベル感の違いはあると思いますが、程度問題の違いで、ここまで言い切れるか？また、純粋に「生体認証を単独で使う」想定がリーズナブルか確認が必要かも。
	b)　アクティベーションコード アクティベーションコードは、一般に4～6桁の数字などで構成される認証情報であり、...	4-6桁ぐらいのOOBによる認証コード送付と混同するので、単に知識認証と記載するのではなく、事前に登録した、というような補足があるとよい。
	...アクティベーションコードを単独の認証情報として用いることは想定していない。	マイナンバーカードの利用者証明用電子証明書のユースケースで、これを用いて正しく署名ができること（もちろん署名検証が正しくでき電子証明書が有効であること）をもって、ログイン可とするものがある。ので、（これが単独の認証情報として用いているのか、は悩ましいが、）想定していないとまではいかないのかも。 もうちょっと広げると、認証時にデバイス外に送信されることがない、というのは、そうできるように追求したからであって、だから（単独の）認証情報に用いることができない、との帰結にはならないのではないか。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　当人認証のプロセスと手法 ア　認証情報(Authenticator)（続き）	c)　ICカード等に格納されたデジタル証明書	デジタル証明書の形式であることは必須ではないと認識しています。わかりやすさのために表記することは理解できるので、少なくとも暗号理論的に共有シークレットではない方式であるということに触れつつ「等」とするのが良いのではないでしょうか。
		ここは電子証明書が良いのでは。（用語のところでもコメント）
		ソフトウェアトークンは考えないのでしょうか。
	d)　ワンタイムパスワード 一回限りのパスワードを生成して認証する方式。デバイス等の所有物に紐づくものは所有物認証に該当し、代表例としてスマートフォン用のTOTP（Time-based One-Time Password）アプリ、物理的なワンタイムパスワード専用デバイス（ハードウェアトークン）、携帯電話番号を使ったSMSへのワンタイムパスワード送信などがある。	こちらを先に記載したほうが理解促進のためには良いと思います。TOTPにはシェアードシークレットが利用されている点は補足したうえで、フィッシング耐性と絡めて語るのが良いかと思います。
		「SMS」は、RCSを考慮し“SMS等”としておきたいです。 ※以降も同様
		ワンタイムパスワードは、あくまでもパスワードの一種であるため、「パスワード」に近いところに配置することで、前後関係から直感的に理解されやすくなると感じました。
	...ワンタイムパスワードは多要素認証の一要素として用いられることが多いが、リアルタイム中継型のフィッシング攻撃への耐性は有さないことに留意が必要である。	ワンタイムパスワードは、あくまでもパスワードの一種であり、認証の3要素に照らし合わせたとき、同じ知識要素であるため、特に我が国ではパスワードとOTPを多要素認証と呼ばず、二段階認証と呼ぶことが多い望ましい文化があると思います。他方、欧米では多要素認証（MFA）と呼び、アップルも国内でMFA、多要素認証と呼んでいます。そして、欧米ではわざわざAnti-phishing MFAが重要だという言い方をしています。ここでは「二段階認証の2段階目として用いられることが多い」などにしてはどうでしょうか。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　当人認証のプロセスと手法 ア　認証情報 (Authenticator)（続き）	... SMSを用いてワンタイムパスワードを送信する方式は、SIMスワッピング攻撃により利用者が携帯電話番号を不正に奪取されるリスク、第三者によってSMS認証の代行が行われるリスク、携帯電話番号の再割り当てが行われるリスク等があるため、採用に当たってはこれらのリスクを受容できるか個別のリスク評価が必要である。	中国のサービスで、SMSによる導通確認を突破するために簡単に誰かのSMS番号を利用できるサービスが登場してきています。ボランティアと称してサービスを提供しています。お小遣い稼ぎでSMS番号を貸しているようなケースに該当します。
	...電子メールアドレスに対してワンタイムパスワードを送信する方式は、電子メールへのアクセスがパスワードに依存している場合が多くパスワードと同時に侵害される可能性があることや、メールの送信経路中で傍受されるリスクがあること等を踏まえ、採用に当たってはこれらのリスクを受容できるか個別のリスク評価が必要である。	電子メールは所有物とみなさないことを明記してはいかがでしょう。
		単なる解説のみでなく、SMS OTP > メールOTP で強度が違うことを述べると良いと思いました。 そのあと、その上の文、SMS OTPだろうがメールOTPだろうが、フィッシング攻撃への耐性を有しないことに留意が必要であるということを述べるのが良いと思います。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　当人認証のプロセスと手法 ア　認証情報(Authenticator)（続き）	e)　スマートフォン等による生体認証 生体認証機能を搭載したスマートフォン、PCにおいては、格納したデジタル証明書をアクティベーションするために生体認証を利用できるものがある。これを認証情報として利用する場合、所有物認証＋生体認証による多要素認証として扱うことができる。	端末のロックを解除する行為は一要素とみなさない、という記載を入れてはいかがでしょう。
		NISTで定番の記述ですが、スマホ自体のロックが１要素にカウントできない点、何回同じ要素を使ってもそれは本書では１要素としてカウントされる点は言及しても良いかと思います。また、取引前の異なるPWでの認証（ここのコメントではないですが）の効果については一定認められるものの、互いに素である必要があるという点も触れる候補と思いました。 ただ、スマホ自体のロックをポリシーで強制しているような場合も想定したり、アプリで必ずロック解除を入れているような場合にどう記載するかは一度合意しておくと良いと思いました。
		「国民を詐欺から守る総合政策」に「パスキーの推進」が盛り込まれましたので、具体的な例としてFIDO認証、パスキーのことに触れることで、わかりやすくなると思います。
	f)　セキュリティキー等に搭載された生体認証 デジタル証明書を格納するための認証用セキュリティキーには、アクティベーション用に生体認証機能を備えるものもある。ICカードについても同様に生体認証機能を備えるものがある。これらを利用する場合、所有物認証＋生体認証による多要素認証として扱うことができる。	Authentication intentは認証要素ではないが意思確認として重要である点は、近接性などと合わせてどこかで触れられると良さそうです。
		この説明はLocal Mode を話している。Remote Modeも必要ではないでしょうか。 Local Mode に関しては、Activation Code の類型として取り扱うべきだと思います。
		FIDOの具体製品などを考えるとe)の生体認証と同じ書き方でいいのか。製品によっては、生物であることを確認はしていますが、個々の生体情報（いわゆる特徴点）を確認していないと思います。

委員の皆さまよりいただいた主なコメント　―　3.2. 当人認証

2) 当人認証のプロセスと手法　イ　想定脅威と対策例

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　当人認証のプロセスと手法 イ　想定脅威と対策例	全般	疲労攻撃のことが触れられていないと思いました。（プッシュ通知が頻繁に届き、確認を怠るようになり、最終的には複数選択でさえ適当に選択して、まれに当たって認証が通過してしまう、など）
		認証時とリカバリー時だけを取り扱っていて、発行時他が入っていません。（これまで議論もされていませんが…。） 良し悪しはありますが、ISO/IEC 29115 の10.2を見てみるとクレデンシャル管理における脅威がリストされているので参考になると思います。 ちなみに、ライフサイクルには、Credential creation, activation, suspension, recovery, use, archiving, deleting のようなフェーズがあるはず。
		窃盗、盗聴が抜けている。ちなみにNISTでは、 Theft/Duplication/Eavesdropping/Offline Cracking /Side-Channel Attack/Phishing/Social Engineering /Online Guessing/Endpoint Compromise /Unauthorized Binding/Latent Keys/Proliferation of Keys /Key Transfer Security/Insider Threats が挙げられています。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2)　当人認証のプロセスと手法 イ　想定脅威と対策例 （続き）	c)　使い回されたパスワードの漏えい 他サービスから漏洩したIDとパスワードを使ってログインを試行するなどして認証情報を推測しようとする攻撃。パスワード特有の脅威である。対策例として、他サービスで使いまわしにくいIDの採用、知識以外の認証要素の採用等がある。	IDではなくパスワードではないでしょうか。 また、この対策は行政機関側でできるものでしょうか。（注意喚起の文言を表示するぐらいはできるのでしょうが）
	e)　フィッシング攻撃 攻撃者が利用者を偽のサイトに誘導し、パスワード等の認証情報を窃取・中継する攻撃。 対策例として、サービスと認証情報とを紐づけられる技術（FIDO等）の採用、クライアント認証等がある。 なお、窃取された認証情報をリアルタイムに中継されるタイプの攻撃に対して、ワンタイムパスワードは対策として機能しない点に留意が必要である。	確認コードを転送しろ系のフィッシングについても考慮したいところです。フィッシング対策協議会の文書に日本向きの適切な分類ワーディングがある可能性。
		サービスと認証情報とを紐づけるだけではフィッシング対策にならないように思います。「クライアント認証」ということばもそれが指し示すことが不明瞭で、フィッシング対策にならないように思います。この節は、修正が必要だと思います。
	f)　秘密鍵の不正な取り出し・複製 秘密鍵が格納されたデバイスやアカウントに対して不正なアクセスや解析を行い、秘密鍵の窃取や複製を行おうとする攻撃。 対策例として、耐タンパ性を有するハードウェア等の利用、暗号鍵の安全な管理を目的とした仕組みの採用、秘密鍵の複製・同期・バックアップの禁止等が考えられる。	狙い撃ちや１つのカギを攻略することで様々な対象に対してオペレーションが可能になるようなシステムの認証については、秘密鍵の取り出しについては、個人認証用のAuthenticatorの盗難＆かぎ取り出しのインパクトに対して、レベルが広くなるというような考え方は添えておきたいところ。逆にフィッシングはマス向けに大量に実施して誰か引っかかれば良い、というアプローチがしやすい点も言及したい。
		そのとおりなのですが、このガイドラインの読者が直接実行できる対策ではないので、どのような選択をするとこの対策につながるのかという解説が付記されるのが望ましいと思いました。 耐タンパ性を有するハードウェアの利用とは何かなどについても、もう少し補足が必要と思いました。（用語一覧のところが充実すれば、それでよいかもしれません）

委員の皆さまよりいただいた主なコメント　―　3.2. 当人認証

2) 当人認証のプロセスと手法　ウ　アカウントの回復（Account Recovery）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
2) 当人認証のプロセスと手法 ウ　アカウントの回復（Account Recovery）	全般	この b)～ d)と、 a)のレベル感が一段違う気がします。 b)～d)は、「身元確認のための準備作業」と思われる内容が記載され、その方法として3つがある、という感じかなと思いました。
	a)　身元確認の再実施 初回登録時と同様の身元確認を再度実施する方式。初回登録時と同様の身元確認を行うことで、アカウントの回復特有の手続きに起因する脆弱性を生みにくいが、利用者にとっての利便性が低下する場合がある。 なお、身元確認において「本人確認書類の紛失時の例外措置」を設けている場合でも、アカウント回復においては例外措置を適用不可とすべきである。	「アカウント回復においては例外措置を適用不可とすべき」 →ミッションの遂行を阻害しないでしょうか。
		（利便性の低下について）デメリットとして理解しますが、大きなメリットがあります。メリットとデメリットをフェアに記載すべきではないでしょうか。
		適用不可とするのは、良いですが、適用不可の場合、どう対応すればいいか、ここでなくていいと思いますが、記載してください。職員の方は、適用不可というとできないで思考停止する場合もあるので、使えませんという答えにならないようしてください。
	c)　リカバリーコードの必要時発行	連絡先の乗っ取り（電子メールであればアカウント乗っ取り、居住地住所であれば郵便物窃取など）というような表記がより望ましい。
	d)　予備の認証情報の登録 予備の認証情報（例えば、セキュリティキーに格納されたデジタル証明書など）をあらかじめ登録しておくという手法も考えられる。 複数の認証情報の保証レベルや脅威耐性の差がリスクに繋がる恐れがある点に留意が必要である。	ここで最も記載すべき事項は、そんなに複数の手段が実質的な選択肢として存在しうるのか、という点だと認識しています。
		この方式は有効です。これについてもメリットとデメリットをフェアに記載できると良いと思います。
	その他	行政サービスを前提とするなら、申請者が亡くなった場合の回復手段についてもどこかで触れておけるとより良いかと思います。

委員の皆さまよりいただいた主なコメント　―　3.2. 当人認証

3)　当人認証保証レベルと対策基準

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3)　当人認証保証レベルと対策基準	ア　当人認証保証レベルの位置づけ 表 3-9　当人認証保証レベルの定義	（各レベルの）想定手段をある程度記載しておくのがよいのでは。
		対策基準を対策基準表に抜き出して番号を与えた方が良い。それを後のレベルの表3-10にマッピングする。そうすることによって繰り返しが減る。
	表 3-9　当人認証保証レベルの定義 当人認証が失敗したとき、...	「失敗」は間違った人を本人と認証してしまったケースの想定で良いですよね。認証失敗というと本人が失敗したようにも受け取れます。 例えば「当人認証が失敗して本人以外が手続き等を行う事により・・・」のような書き方は如何でしょうか。
	表 3-9　当人認証保証レベルの定義 レベル2A 利用者が希望する場合には、フィッシング攻撃への耐性をもつ認証要素を利用可能とすることを必須とする。	レベル2Aのフィッシング耐性の要件は、議論はあると思いますが、将来を見据えたガイドラインとして、良い契機になると思います。
		民間での適用を前提とした際、FIDOメンバー目線ではAgreeですが、事業者目線では現実的にどこまでの事業者が対応できるのか？という点は課題になる認識です。 おそらく第二地銀くらいではほぼ対応できないのではないかと想像しますが、「必須」なのか「推奨」なのかは政治的な判断にもなるので、NISTが2nd PDの記載で民間側も行けそうな感覚を持っているのかは気になるところです。
	表 3-9　当人認証保証レベルの定義 レベル1	特別な理由がある場合に限って利用すべき、ぐらい踏み込んでも良いのでは。（行政分野なので）

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3)　当人認証保証レベルと対策基準（続き）	表 3-9　当人認証保証レベルの定義 レベル1 「認証の3要素のうち、「知識」又は「所有」のいずれか1要素による認証を行う。」	生体なしは、前に書いてあるのは理解していますが、本当にダメにするのか。 程度の違いだとすると生体はなしとするのか。
		この定義では、いわゆるSMS OTPを使った二段階認証はレベル1に分類されます。念のための議論は必要かと思います。
	表 3-10　当人認証保証レベルの対策基準（認証情報）	表中の◯ ー を書くのではなく、Control 番号を書いたほうが良いのでは。

特に協議いただきたいポイント

❶ 認証の3要素について	• 「もはや認証の3要素にこだわるのはやめてはどうか」とのご意見については、事務局としては前向きに反映を試みたいと考えております。この方針について、委員の皆さまで意見交換をいただきたくお願いします。
❷ 電子メールOTPの扱いについて	• このガイドラインにおいて電子メールOTPをどのように扱うか。「メールアドレスは所有物ではない」とした場合、単独で利用された場合、パスワードと組み合わされた場合の位置づけを、どのように示すべきかについてご意見を伺わせてください。
❸ アカウントリカバリ―に関する記載について	• 今回の案では、NISTの2pdでの動向も踏まえ、昨年度までに議論できていなかったアカウントリカバリ―に関する記載案を作成しています。内容の妥当性、過不足などについてご意見を伺いたくお願いします。
❹ 当人認証保証レベル2Aにおけるフィッシング耐性要件について	• レベル2Aにおいて、NIST 2pdと同様に「希望する利用者がフィッシング耐性のある手段を利用可能とすること」といった要件を設けることについて、意見交換をいただきたくお願いします。
❺ その他のご意見など	• その他、追加のご意見・ご議論があればコメントをいただきたくお願いします。
❻ Authenticatorの訳語について（時間があれば）	• Authenticatorの望ましい訳語について、ご議論をお願いします。 （時間がない場合は、別途の議論テーマとさせていただきます。）

ガイドライン改定案に対するコメント、意見交換

- 1. はじめに
- 2. 本人確認の枠組み
- **3. 本人確認における脅威と対策**
  - 3.1. 身元確認
  - 3.2. 当人認証
  - **3.3. フェデレーション**

ガイドライン改定案「3.3. フェデレーション（Federation）」

1) フェデレーションにおける脅威と対策

1)　フェデレーションにおける脅威と対策

フェデレーションにおける主な脅威として、IDプロバイダとRPとの間で保証レベルの齟齬が生じてしまうことで、RPが本来必要な身元確認・当人認証が実施されなくなる脅威が挙げられる。また、連携に用いられるアサーションの窃取、偽造、改ざん等によるアサーションインジェクション攻撃についても対策が必要となる。

表　3-11　フェデレーションにおける主な脅威と対策

脅威	脅威の概要	脅威への対策
IDプロバイダと RP の間の保証レベルの齟齬	IDプロバイダが実施する身元確認・当人認証の保証レベルと、RPが必要とする身元確認・当人認証の保証レベルに差異があり、なりすまし等の攻撃につながる	IDプロバイダとの信頼関係の確立
アサーションインジェクション攻撃	IDプロバイダから RP に対して発行されるアサーションの窃取・偽造・改ざん・再利用などにより、不正なアサーションをRPに注入される	安全な連携のための設定・登録、 基準を満たしたアサーションによる連携

2) フェデレーションのプロセスと手法

2)　フェデレーションのプロセスと手法

　フェデレーションを実現するためには、IDプロバイダとRP間の事前調整、合意、登録処理などのプロセスが必要となる。その上で、適切なアサーションによる連携を行う必要がある。

ア　IDプロバイダとの信頼関係の確立（Trust Agreements）

　IDプロバイダとRPとの間で、フェデレーションにおいて連携する属性情報や保証レベル等の条件を事前に調整し、合意・確立するプロセスである。

　なお、信頼関係の確立を必要時に動的に行う方式も存在するが、本ガイドラインでは事前に行う方式のみを扱う。

イ　安全な連携のための設定・登録（Registration）

　フェデレーションによるIDプロバイダとRPとの間で安全な連携を実施するために必要となる、設定・登録等の処理を行うプロセスである。ドメイン名やURIの設定、暗号鍵の交換と登録処理等が該当する。

　なお、設定・登録を必要時に動的に行う方式も存在するが、本ガイドラインでは事前に行う方式のみを扱う。

ウ　基準を満たしたアサーションによる連携（Assertion）

　IDプロバイダとRPとの連携においては、「アサーション」と呼ばれるデータの授受を行う。フェデレーションの実装においては、偽のアサーションの提示、アサーションの改ざん等のアサーションインジェクション攻撃を想定した対策が必要となる。

3) フェデレーションのプロセスと手法

3)　フェデレーション保証レベルと対策基準

本ガイドラインにおいては、フェデレーションの段階的な保証レベルは定義せず、一律の対策基準を定義する。

ア　フェデレーションに係る対策基準

a)　IDプロバイダとの信頼関係の確立に関する対策基準

RPは、IDプロバイダとの連携にあたり、フェデレーションに必要な条件等についてIDプロバイダと合意し、文書化して管理する。最低限合意すべき事項を以下に示す。この内容は定期的に見直すものとする。

表　3-12　信頼関係の確立において合意すべき事項

No.	大項目	合意すべき事項
1	ID プロバイダから RP へ連携する属性情報	・ 属性情報名 ・ 属性情報の概要 ・ 各属性情報を連携する目的
2	ID プロバイダによる本人確認の保証レベル	・ ID プロバイダが実施する身元確認の保証レベル及びその根拠（採用されている身元確認手法等） ・ ID プロバイダが実施する当人認証の保証レベル及びその根拠（採用されている当人認証手法等）
3	RP が必要とする保証レベル	・ RP が必要とする身元確認の保証レベル ・ RP が必要とする当人認証の保証レベル
4	ID プロバイダと RP との間で共有するシグナル	・ 共有シグナルの利用有無 ・ 共有シグナルの送信契機とするイベント（アカウントの停止、アカウントの侵害の疑い、アカウントの属性情報の変更、対応可能な保証レベルの変更等） ・ 共有シグナルに含まれる情報
5	安全な連携のための設定・登録事項	・ 連携に使用するプロトコル ・ ID プロバイダと RP との間で安全な連携を確立するために必要となる事前の設定・登録事項（ID プロバイダ及び RP の識別子、暗号鍵等） ・ 暗号鍵の更新期間、更新プロセス等

b)　安全な連携のための設定・登録に関する対策基準

IDプロバイダとRPの間の連携を安全に行うため、IDプロバイダ及びRPのそれぞれにおいて、「信頼関係の確立」においてIDプロバイダと合意した内容に基づき、連携に必要となる識別子や暗号鍵の設定・登録を行う。

3) フェデレーションのプロセスと手法

c)　アサーションに関する対策基準

IDプロバイダとRPとの間の連携は、アサーションによって行われる必要がある。アサーションに関して最低限満たすべき対策基準を以下に示す。

なお、IDプロバイダとの連携方式、連携に用いるネットワーク、採用するプロトコルの仕様等に応じて脅威と対策が異なるため、システムの構築時において想定される脅威とリスクを分析し、必要な対策を講じること。

表　3-13　アサーションに関する対策基準

No.	分類	対策基準
1	基本事項	フェデレーションによる連携は、ID プロバイダが RP に対してアサーションを発行することによって行うこと。
2	トランザクションの開始	フェデレーションによる連携のトランザクションは RP から開始すること。 ただし、連携がイントラネット内のみでの行われる場合など、アサーションインジェクションの脅威が低いとみなせる環境下においては、トランザクションを ID プロバイダから開始する方式としてもよい。
3	アサーションのリクエスト	アサーションのリクエストには、少なくとも以下を含めること。 ・　RP の識別子 ・　ノンス（nonce）
4	アサーションに含める情報	アサーションには、少なくとも以下の情報を含めること。 ・　アサーションが適用される利用者の識別子 ・　発行元 ID プロバイダの識別子 ・　発行先 RP の識別子 ・　発行日時 ・　アサーションの有効期限 ・　アサーションの識別子 ・　ID プロバイダが利用者を最後に認証した日時 ・　リクエストに含まれていたノンス（nonce） ・　ID プロバイダによるデジタル署名 加えて、必要に応じて、以下の情報を含めることを検討すること。 ・　当該アサーションに関する保証レベル ・　当人認証に用いられた認証情報の分類
5	RPによるアサーションの検証	RP は、ID プロバイダから受信したアサーションに対して、少なくとも以下の検証を行うこと。 ・　アサーションが偽造・改ざんされていないこと ・　想定する IDプロバイダから発行されたものであり、他の ID プロバイダから発行されたものでないこと ・　自身に向けて発行されたものであり、他の RP に向けて発行されたものでないこと ・　有効期限内であること
6	その他の脅威への対策	ID プロバイダとの連携方式、連携に用いるネットワーク、採用するプロトコルの仕様等に応じて想定される脅威とリスクを分析し、必要な対策を講じること。

委員の皆さまよりいただいた主なコメント　―　3.3. フェデレーション

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
３.３　フェデレーション（Federation）	全般	フェデレーションは一律の対策基準で良いように思いました。 考慮すべきこと、は記載されていますが、どう選ぶのか、選択肢があるのか、について内容を盛っていけると良いのではないかと思います。 自治体の視点で眺めると、民間IdPと連携済みのケースはあるので、こういうものをどう捉えたら良いのか、本ガイドラインの埒外である、よりは材料が提供できると良いな、と考えます。
		3.1や3.2と完全並立でなくていいのではないか。「フェデレーションに関する留意事項」ぐらいでも良いのではないか。メリハリをつけるべきと思います。 留意事項にすることにより、「3)　フェデレーション保証レベルと対策基準」の部分の記載は、不要になるかと思います。
		PIVを意識したHoK（Holder-of-Key）の記述をどう反映させるかは一度もんだほうが良さそうですね。
2)　フェデレーションのプロセスと手法	ア　IDプロバイダとの信頼関係の確立（Trust Agreements）	”信頼関係の確立”を読み手がイメージできるのか少し疑問があります。日本的には"条件および仕様の合意”でいかがでしょう。
		信頼関係の確立は結果なので、その過程に至るまでに必要な歩合意形成のプロセスと定期的な見直し（監査）について触れると良いかと思います。
	ウ　基準を満たしたアサーションによる連携（Assertion）	今の説明では、アサーションが唐突。 「アサーションインジェクション攻撃への対応」ぐらいにすれば、抽象化して、説明できるのではないか。

（前頁からの続き）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3)　フェデレーション保証レベルと対策基準	a)　IDプロバイダとの信頼関係の確立に関する対策基準 RPは、IDプロバイダとの連携にあたり、フェデレーションに必要な条件等についてIDプロバイダと合意し、文書化して管理する。最低限合意すべき事項を以下に示す。この内容は定期的に見直すものとする。	合意事項の見直しに加えて、実際に合意した内容に従って運営されているかどうかの確認を定期的に行うことも記載しておいた方が良いと思います。
	a)　IDプロバイダとの信頼関係の確立に関する対策基準 表 3-12　信頼関係の確立において合意すべき事項 No.1「IDプロバイダからRPへ連携する属性情報」	同一性の確認のために照合するか(など連携において追加の制限を貸すかどうか)どうか、もドコモ口座事件を踏まえると考慮したいところです。
	c)　アサーションに関する対策基準 表 3-14	身元確認、当人認証のように想定脅威に対する対策基準という書き方は難しいのでしょうか。
		技術依存することが想定されるので、別紙にして、必要であれば、マイナーチェンジで修正するような内容ではないか。本文レベルではない気がします。

特に協議いただきたいポイント

❶ フェデレーションに関する対策基準の記載粒度について	• 現在の記載案は、フェデレーションプロトコルの仕様を抽象化しただけの記載となっている箇所が多く、ガイドラインとして適切であるかやや疑義が残っています。 • 「フェデレーションについては対策基準ではなく考慮事項に留めるべきでは」といったご意見も踏まえ、ガイドラインとして定義すべき範囲、粒度についてご意見を伺いたくお願いします。
❷ “federation”の訳語について	• 昨年度までにいただいたご意見を踏まえ、「認証連携」ではなく「フェデレーション」という表記に変更いたしました。 • この訳語についてのご意見、ご懸念、別案があれば提案いただきたくお願いします。 （別案：「アイデンティティ連携」「ID連携」など）
❸ PIV等での活用等を見据えた記載方法	• 将来的にHoK（Holder-of-Key）などが必要となるユースケースが出てくることを見据えた場合のガイドラインの記載方法などについて、ご意見があればいただきたくお願いします。 （将来的な拡張も見越しつつ、今回は参考情報として存在を示す程度とする、等）
❹ その他のご意見など	• その他、追加のご意見・ご議論があればコメントをいただきたくお願いします。

デジタル庁

Digital Agency