Thu, 26 Oct 2017 14:16:51 +0000

**NIST 特別出版物 800-63A デジタル ID ガイドライン(翻訳版)**

*登録と身元情報の検証要件*



Paul A. Grassi James L. Fenton

**Privacy Authors:** Naomi B. Lefkovitz

Jamie M. Danker

**Usability Authors:** Yee-Yin Choong

Kristen K. Greene Mary F. Theofanos

この出版物は以下から無料で入手できる: https://doi.org/10.6028/NIST.SP.800-63a



**NIST 特別出版物 800-63A デジタル ID ガイドライン**

### 登録と身元情報の検証要件

Paul A. Grassi *Applied Cybersecurity Division Information Technology Laboratory*

James L. Fenton *Altmode Networks Los Altos, CA*

**Privacy Authors:** Naomi B. Lefkovitz

*Applied Cybersecurity Division Information Technology Laboratory*

Jamie M. Danker *National Protection and Programs Directorate Department of Homeland Security*

**Usability Authors:** Yee-Yin Choong Kristen K. Greene

*Information Access Division Information Technology Laboratory*

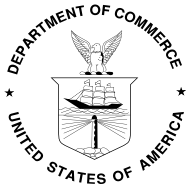
Mary F. Theofanos *Office of Data and Informatics Material Measurement Laboratory*

**翻訳者:** Nov Matake

*YAuth.jp LLC*

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-63a

2017年6月



米国商務省

*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology

*Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology*

### **権限**

この出版物は, 2014年の連邦情報セキュリティ現代化法 (Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283) の下で NIST がその法定責任に従って発展させた. NIST は, 連邦情報システムのための最小限の要件を含め, 情報セキュリティの標準およびガイドラインの発展に責任を負うが, その標準とガイドラインは, 全国的なセキュリティシステムにポリシー権限を行使する適切な連邦政府職員の明確な承認がなければ, そうしたシステムに適用されてはならない. このガイドラインは, 行政管理予算局 (OMB) の回状 A-130 の要件と一致している.

この出版物に記載されたいかなることも, 商務長官が法的権限の下で連邦機関に義務付け拘束力を持たせた標準とガイドラインに反駁するために用いられるべきではない. また, これらのガイドラインは, 商務長官, 行政管理予算局長官, またはその他の連邦職員の既存の権限を変更したりそれに取って代わったりするものと解釈されるべきではない. この出版物は, 非政府組織が自由意志に基づいて使用でき, 米国において著作権の対象にならない. しかしながら, 引用で出典として示されることが望ましい.

National Institute of Standards and Technology Special Publication 800-63-3 Natl. Inst. Stand. Technol. Spec. Publ. 800-63A, 45 pages (June 2017) CODEN: NSPUE2

この出版物は以下から無料で入手できる:

この文書では, 試験的な手順や概念を適切に記述する目的でいくつかの商業的なエンティティ, 装置, 材料を特定している場合がある. こうした特定は, NIST による推奨や支持を意味せず, そうしたエンティティ, 装置, 材料がその目的に対して最も有効であることを必ずしも意味していない.

この出版物では, 割り当てられた法的責任に応じてNIST が現在開発中の他の出版物を参照に挙げている場合がある。この出版物に含まれる情報は, 付属文書が完成する前でも連邦機関が概念と方法論も含めて使用する場合がある. したがって, 現在の要件, ガイドライン, 手順がある場合は, それぞれの出版物が完成するまでそれらが有効である.計画目的と移行目的に対し, 連邦機関は NIST によるこうした新しい出版物の発展に綿密に従うことを求めてもよい.

各機関は, パブリックコメントの期間中にすべての暫定版を調べ, NIST に意見を提示することが推奨される. 上記の他にもサイバーセキュリティに関する NIST の多くの出版物は, http://csrc.nist.gov/publicationsから入手できる.

<https://doi.org/10.6028/NIST.SP.800->

**この出版物に関する意見は** [**todig-comments@nist.gov**](mailto:todig-comments@nist.gov) **に提出される:**

すべての意見は, 情報公開法 (FOIA) の下で公表される.

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Email: [dig-comments@nist.gov](mailto:dig-comments@nist.gov)

## **コンピュータシステム技術に関するレポート**

国立標準技術研究所 (National Institute of Standards and Technology, NIST) の情報技術研究所 (Information Technology Laboratory ,ITL) は, 測定と標準に関する全国インフラのための技術的リーダーシップを示すことにより, 米国経済と福祉を促進する. ITL は, 情報技術の発展と生産的利用を押し進めるために, テスト, テスト方法, 参照データ, 概念検証の実装, テクニカル分析を開発している. ITL の責任には, 連邦システムの全国セキュリティ関連情報以外の経済的なセキュリティとプライバシーに対し, マネージメント, 行政, 技術, 物理上の標準とガイドラインの促進が含まれている. 特別出版物 800 シリーズは, 情報システムセキュリティにおける ITL の研究, ガイドライン, 社会福祉の支援努力と, 産業, 政府, 学術組織の共同作業に関するレポートである.

### **概要**

こうしたガイドラインは, デジタル身元識別情報 (ID) サービスを実施する連邦機関に技術要件を提供するもので, この目的に外れる標準の開発または使用を妨げる意図はない. このガイドラインのテーマは, デジタル認証で使用する身元情報の登録と検証である. 中心となるのは, 身元情報の検証として知られるプロセスである. このプロセスでは, 申請者は身元を確実に確認してくれる認証情報サービスプロバイダ (CSP) に申請者本人である証拠を提出する. これにより, CSP は実用的な身元情報保証レベルで身元確認を表明できる. この文書では, ３種類の身元情報保証レベルの技術的要件を定義する.この出版物は, NIST SP 800-63-2 に代わるものである.

## **キーワード**

認証; 認証情報サービスプロバイダ; 電子認証; デジタル認証; 電子認証情報; デジタル認証情報; 身元情報の検証; 連携

## **謝辞**

英国内閣府の Adam Cooper, Alastair Treharne, Julian White とカナダ財務委員会事務局の Tim Bouma を初めとする多くの方から貴重な意見を寄せてもらった。Kaitlin Boeckl は SP 800-63 のすべての巻で芸術的な図表を作成してくれた. また, Digital ID & Authentication Council of Canada (DIACC) の Joni Brennan, NIST のEllen Nadeau と Ben Piccarreta, Deloitte & Touche LLP の Danna Gabel O’Rourke を含めた多くの方々にお世話になった. これに加え, プライバシーに関する要件と考慮事項の発展に貢献してくれた連邦プライバシー委員会のデジタル認証タスクフォースの方々に特にお礼を申し上げる.

原文を執筆してくれた Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus のリーダーシップと革新的考え方に敬意を表したい. こうした方々のたゆまない努力がなければ, SP 800-63 を今日ある文書に発展させたすばらしい土台は築けなかったであろう. これに加え, プライバシーに関する要件と考慮事項の発展に貢献してくれた連邦プライバシー委員会のデジタル認証タスクフォースの方々に特にお礼を申し上げる.

## **表記法**

「SHALL(しなければならない)」および「SHALL NOT(してはならない)」という用語は, この出版物に厳密に従うことを要求しており, これから逸脱することは許されない.

「SHOULD(すべきである)」および「SHOULD NOT(すべきでない)」という用語は, いくつかある選択肢の中で特に適切なものとして１つが推奨されることを示しており, 他の選択肢については言及も除外もしない. または, ある行動方針が望ましいが必ずしも要求されないことを示す. または, (否定の意味では) ある可能性や行動方針を推奨しないが禁止もしないことを示す.

「MAY(してもよい)」および「NEED NOT(しなくてよい)」という用語は, 出版物の範囲において行動方針が許容できることを示す.

「CAN(できる)」および「CANNOT(できない)」という用語は, 物質的であれ, 物理的であれ, 必然的であれ, 可能性や能力があることを示し, 否定の意味では可能性や能力がないことを示す.

# 目次

**1 Purpose .................................................................................................................... 1**

**2 Introduction ............................................................................................................. 2**

2.1 Expected Outcomes of Identity Proofing .......................................................... 2

2.2 Identity保証Levels ................................................................................ 3

**3 Definitions and Abbreviations ............................................................................... 4**

**4 Identity保証Level Requirements ............................................................... 5**

4.1 Process Flow ................................................................................................... 5

4.2 General Requirements ..................................................................................... 6

4.3 Identity保証Level 1 ............................................................................... 8

4.4 Identity保証Level 2 ............................................................................... 8

4.4.1 IAL2 Conventional Proofing Requirements ........................................... 9

4.4.2 IAL2 信頼できる身元保証人 Proofing Requirements .................................... 11

4.5 Identity保証Level 3 ............................................................................. 11

4.5.1 決定 Requirements .................................................................... 11

4.5.2 Evidence 収集 Requirements ..................................................... 11

4.5.3 Validation Requirements ..................................................................... 11

4.5.4 Verification Requirements ................................................................... 12

4.5.5 Presence Requirements ...................................................................... 12

4.5.6 Address Confirmation .......................................................................... 12

4.5.7 Biometric 収集 ............................................................................. 12

4.5.8 Security Controls ................................................................................. 12

4.6 Enrollment Code ............................................................................................ 13

4.7 Summary of Requirements ............................................................................ 13

**5 Identity 決定, Validation, and Verification ................................................ 15**

5.1 Identity 決定 ......................................................................................... 15

5.2 Identity Evidence 収集 and Validation ................................................... 15

5.2.1 Identity Evidence Quality Requirements ............................................. 15

5.2.2 Validating Identity Evidence ................................................................ 18

5.3 Identity Verification ......................................................................................... 20

5.3.1 Identity Verification Methods ............................................................... 20

5.3.2 Knowledge-Based Verification Requirements ..................................... 21

5.3.3 In-Person Proofing Requirements ....................................................... 22

5.3.4 信頼できる身元保証人 Requirements ........................................................... 23

5.4 Binding Requirements .................................................................................... 23

**6 Derived Credentials .............................................................................................. 24**

**7 Threats and Security Considerations ................................................................. 25**

7.1 Threat Mitigation Strategies ........................................................................... 25

**8 Privacy Considerations ........................................................................................ 27**

8.1 収集 and Data Minimization ................................................................... 27

8.1.1 Social Security Numbers ..................................................................... 27

8.2 Notice and Consent ....................................................................................... 28

8.3 Processing Limitation ..................................................................................... 28

8.4 Redress .......................................................................................................... 29

8.5 Privacy Risk Assessment ............................................................................... 29

8.6 Agency Specific Privacy Compliance ............................................................. 29

**9 Usability Considerations ...................................................................................... 31**

9.1 General User Experience Considerations During Enrollment and Identity

Proofing .................................................................................................................. 32

9.2 Pre-Enrollment Preparation ........................................................................... 32

9.3 Enrollment Proofing Session .......................................................................... 34

9.4 Post-Enrollment ............................................................................................. 36

**10 References ............................................................................................................. 37**

10.1 General References ....................................................................................... 37

10.2 Standards ....................................................................................................... 38

10.3 NIST Special Publications .............................................................................. 38

**List of Figures**

Figure 4-1 The Identity Proofing User Journey ................................................................ 5

**List of Tables**

Table 2-1 Normative and Informative Sections of SP 800-63A ........................................ 2

Table 4-1 IAL Requirements Summary .......................................................................... 13

Table 5-1 Strengths of Identity Evidence ....................................................................... 17

Table 5-2 Validating Identity Evidence ........................................................................... 19

Table 5-3 Verifying Identity Evidence ............................................................................. 20

Table 7-1 Enrollment and Identity Proofing Threats ....................................................... 25

Table 7-2 Enrollment and Issuance Threat Mitigation Strategies ................................... 25

**正誤表**

この表は, 特別出版物 800-63A で加えられた変更の一覧である. 正誤表の更新には, 編集上または実質上の修正, 明確化, その他のマイナーな変更を含めることができる.

|  |  |  |  |
| --- | --- | --- | --- |
| **日付** | **種類** | **変更** | **場所** |
| **2017-12-01** | 編集上 | 文書全体で文法上の誤りを訂正 | N/A |
|  | 編集上 | ‘規範’ を ‘参考情報’ に変更 | 表 2-1 |
|  | 実質上 | ‘規範’ を ‘参考情報’ に変更 | セクション 4.1 |
|  | 編集上 | ‘規範’ を確認 | セクション 4.2 |
|  | 実質上 | 属性の所有に関する要件を明確化 | セクション 4.2 項目 4 |
|  | 実質上 | 要件で厳格性を引き下げ | セクション 4.3 |
|  | 実質上 | 要件を明確にして曖昧さを排除 | セクション 4.4 |
|  | 実質上 | 要件を明確化 | セクション 4.4.1.3 |
|  | 実質上 | 要件を明確にして曖昧さを排除 | セクション 4.4.1.6 |
|  | 実質上 | セクションを ‘参考情報’ に更新 | セクション 6 |
|  | 実質上 | タイトルを “処理制限” に変更, 用語の明確化, プライバシーの目的の説明を追加, 同意の明示を指定 | セクション 8.3 |
|  | 編集上 | 参照として NISTIR 8062 を追加 | セクション 10.1 |

# 目的

*このセクションは参考情報である.*

この文書では, リソースへのアクセスを希望する申請者に対して, 身元情報保証レベル (IAL) ごとに登録と身元情報の検証を行う要件をまとめる. こうした要件は, 加入者が本人であることを主張する際に証拠として提⽰する身元情報の受け⼊れ可能性, 確認, 検証について詳細に規定している. さらにこの文書は, 認証情報サービスプロバイダ (CSP) が登録記録を作成して維持し, 認証コード (CSP が発⾏するか加入者が提供) をそれに結び付ける CSP の責任についても詳しく述べる.

# はじめに

*このセクションは参考情報である.*

デジタル ID に関する課題の1つに, ⼀連のオンライン活動を単⼀の特定の主体と関連付けることがある. こうした関連付けが不要であるか望ましくない場合 (例えば匿名や仮名が求められるケース) もあれば, 実在する主体との関係性を確実に確⽴することが重要な場合もある. 医療情報の取得や⾦融取引の実⾏がその良い例である. また何らかの規制 (例えば 2001年の米国愛国者法の施行で規定された本人確認 (KYC) 要件) や, 危険度の高い行為 (例えば, ダムの放⽔率の変更) に対する責任の確⽴のために, そういった関連付けが必須となる場合もある.

さらに、証明書利用者 (RP) がトランザクションを実⾏する加入者について何かを知っているが, 実際の身元については知らないという状況が望ましい場合もある. 例えば, 国勢調査や選出議員への嘆願には, 加入者の⾃宅の郵便番号だけが分かる状態が望ましいかもしれない. どちらのケースでも, サービス提供のためには郵便番号がわかれば⼗分であり, 本人の基本的な身元情報を知ることは必要でないか望ましくない.

下の表は, この文書のどのセクションが規範であり, どのセクションが参考情報であるかを⽰している.

表 2-1 SP 800-63A の規範および参考情報セクション

|  |  |
| --- | --- |
| **セクション名** | **規範/参考情報** |
| 1. 目的 | 参考情報 |
| 2. はじめに | 参考情報 |
| 3. 定義と略語 | 参考情報 |
| 4. 身元情報保証レベルの要件 | 規範 |
| 5.身元情報の決定, 確認, 検証 | 規範 |
| 6. 導出した認証情報 | 規範 |
| 7. 脅威とセキュリティの考慮事項 | 参考情報 |
| 8. プライバシーの考慮事項 | 参考情報 |
| 9. ユーザビリティの考慮事項 | 参考情報 |
| 10. 参考文献 | 参考情報 |

# 身元情報の検証で予想される結果

主体の身元情報の検証には以下の結果が予想される.

* 主張された身元情報が, CSP がサービスを提供するユーザー層の中で単⼀で一意の身元情報になる.
* 提供されたすべての証拠が正しくて本物である (偽造や悪⽤されていない) ことを確認.
* 主張された身元情報が実際に存在することを確認.
* 主張された身元情報がその証拠を提⽰した実際の本人と関連していることを確認.

# 身元情報保証レベル

加盟者の身元情報に関する保証は, 以下の3つの IAL の1つを利⽤して記述される.

**IAL1**: 申請者を実在する特定の身元情報に結び付ける必要はない. 主体の活動に関連して提供されるどのような属性も自己表明であるか, 自己表明として扱うべきである (CSP が RP に表明する属性を含む). 自己表明された属性は確認も検証もされない.

**IAL2**: 主張された身元情報が実際に存在することを証拠が裏付け, 申請者が実在するその身元情報と適切に関連付けられていることを証拠が証明する. IAL2 ではリモートか対⾯での身元情報の検証が必要になる. CSP は検証済み属性を持つ匿名の身元情報をサポートしていれば, 属性を RP に表明することができよう. IAL2 をサポートする CSP は, ユーザーの同意があれば IAL1 のトランザクションを許可できる.

**IAL3**: 対⾯で身元情報の検証を必要とする. 識別に⽤いる属性は, 権限があり訓練を受けた CSP の代表者によって検証される必要がある. IAL2 と同様に, CSP は検証済み属性を持つ匿名の身元情報をサポートしていれば属性を RP に表明することができよう. IAL3 をサポートする CSP は, ユーザーの同意があれば IAL1 と IAL2 の身元情報属性を利用できる.

IAL2 と IAL3 では, CSP から RP に送信する属性の数やその提⽰⽅法を制限することで,連携環境での匿名性が実現できる. 例えば, RP が正確な誕⽣⽇以外の身元情報を必要としない場合, RP は加入者の誕⽣⽇のみを CSP に送らせるべきである. また可能であれば, RP は CSP に属性参照を要求すべきである. 例えば, 認証要求者が18歳以上かどうか知る必要がある場合, RP は完全な誕⽣⽇ではなく真偽値のみを要求すべきである. 逆に⾔えば, より低い保証レベルのトランザクションのためにより⾼い保証を提供する CSP を利⽤することは, ユーザーにとって有益になる場合がある. 例えば, ユーザーは IAL3 の身元情報を維持する場合でも, CSP を IAL2 や IAL1 のトランザクションに利⽤できるべきである.

個人は登録時に身元情報の検証プロセスを経ているため, CSP との個人的なやりとりに関するトランザクションは必ずしも匿名でない場合がある.

各 IAL の詳細な要件はセクション4 とセクション5 で述べる.

# 定義と略語

⽤語の定義と略語については, [SP 800-63 (sp800-63-3.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.html) 付録 A を参照.

# 身元情報保証レベルの要件

*このセクションには, 規範と参考情報の両方が含まれている.*

この文書では, 申請者が身元情報の検証と登録のプロセスを経る共通のパターンについて説明する. このプロセスでは, 身元情報の証拠と属性が収集され, 所定のユーザー層や状況の中で単一の身元情報が一意に決定され, 確認と検証が⾏われる. 最適な IAL の選択については [SP 800-63-3 (sp800-63-3.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.html) セクション 6.1 に説明がある. CSP はこうした属性を認証コードに結び付けることができる ([SP 800-63B (sp800-63b.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html) を参照).

身元情報の検証の唯⼀の⽬的は, 提示された確実性のレベルにおいて申請者が自ら主張する本人であることを保証することである. ここでは, 身元情報の検証に必要な最低限の属性の提⽰, 確認, 検証が⾏われる. 最低限として十分な属性のセットは多いため, CSP はプライバシーとユーザビリティのバランスを取り, デジタル ID の今後の利⽤に必要になる可能性のある属性を考慮した上で, 属性のセットを選択すべきである. 例えば, 必要最低限となる属性には以下を含めることができよう.

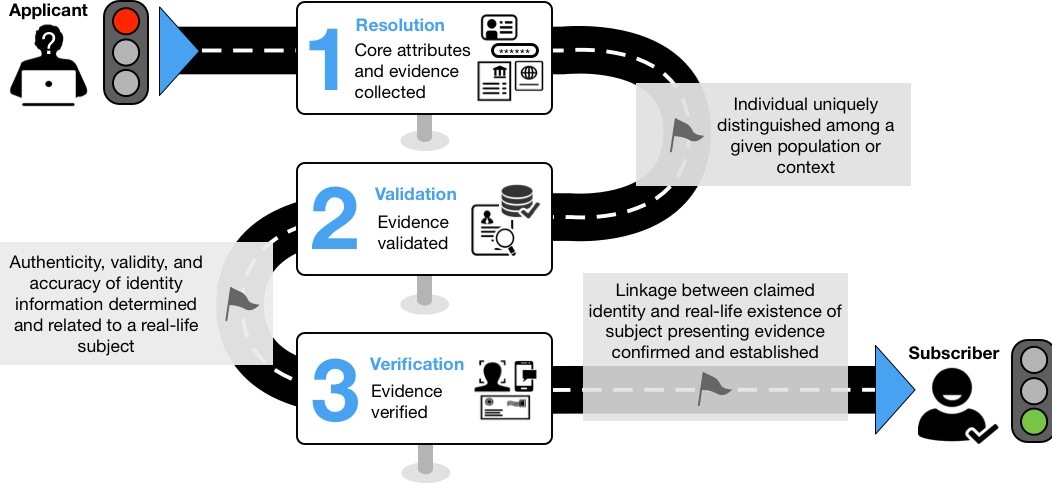
1. 氏名
2. 誕生日
3. 自宅の住所

またこの文書は,身元情報の検証以外の⽬的で利⽤される追加情報を収集する際の CSP に対する要件も⽰している.

## **プロセスの流れ**

*このセクションは規範である.*

図 4-1 は身元情報の検証と登録の基本的な流れの概略である.



##### 図 4-1 身元情報の検証におけるユーザーの扱い

（図の中）

申請者

１決定 基本的属性と証拠の収集

所定のユーザー層か状況の中で個人が一意に識別される.

２確認 証拠の確認

身元情報の信憑性, 有効性, 正確さが確定されて実在する主体に関連付けられる.

３検証 証拠の検証

主張された身元情報と証拠を提示した主体の実際の存在との関連付けが確認されて確立される.

以下では身元情報の検証プロセスで CSP と申請者がどのようなやりとりするのかを⽰す.

##### 決定

* 1. CSP は申請者から名前, 住所, 誕⽣⽇, Eメール, 電話番号などの PII を収集する.
  2. さらに CSP は, 運転免許証とパスポートなど 2種類の身元情報の証拠を収集する. 例えば CSP は, ラップトップのカメラを使って, こうした証拠の裏表を写真に取ることができる.

##### 確認

* 1. CSP は信頼元をチェックして 1a で提供された情報を確認する. CSP は申請者が提出した情報が信頼元の記録と一致していることを確定する.
  2. CSP は免許証とパスポートの画像をチェックし, 画像が修正されておらず, QR コードにエンコードされているデータが平⽂の情報と一致し, 識別番号が標準フォーマットに従っていることを確定する.
  3. CSP は免許証とパスポートの発行元に問い合せ, 情報が一致していることを確認する.

##### 検証

* 1. CSP は申請者に免許書とパスポートに一致した本人の写真を要求する.
  2. CSP は免許書とパスポートの写真を本人の写真と⽐較し, 一致していることを確定する.
  3. CSP は登録コードを申請者の確認済み電話番号に送り, 申請者は受け取った登録コードを CSP に提⽰する. CSP は両者が一致していることを確認し, 申請者が検証済み電話番号を所有して管理していることを検証する.
  4. 申請者は検証に成功する.

注意: 身元情報の検証プロセスは, 複数のサービスプロバイダが提供できる. 単一の組織, プロセス, 方法, 技術で検証プロセスのすべてのステップを実施することができるが, ここではそれを想定していない。

## **一般要件**

## *このセクションは規範である。*

IAL2 か IAL3 で身元情報を検証する CSP には, 以下の要件が課せられる.

1. 身元情報の検証は, サービスや利益を得るための適格性や資格を決定するために実施してはならない (SHALL NOT).
2. PII の収集は, 主張された身元情報の存在確認に必要な情報と, そして, 身元情報の決定, 確認, 検証のために証拠を提⽰している申請者と主張された身元情報との関連付けに必要な情報を, 最⼩限に制限しなければならない (SHALL). この PII には, 身元情報の証拠を信頼元と関連付けて, RP が認証決定に使用する属性を含めてもよい(MAY).
3. CSP は, 身元情報の検証に必要な属性の記録を収集して保持する⽬的について, 申請者に明確に知らせなければならない(SHALL). これには, 身元情報の検証プロセスを完了するためにこうした属性が任意なのか必須なのかや, 属性を提供しない場合の結果を含む.
4. CSP は, 身元情報の検証, 認証, 属性アサーション (これらをまとめて “身元情報サービス”と言う), 関連する不正行為の防止, 法律や法的手続きの遵守以外の⽬的で属性を処理する場合は, 追加処理によるプライバシーのリスクに釣り合った予測可能性と管理可能性を維持するための措置を講じなければならない (SHALL). 措置には, 明確な通知の提供, 加入者の同意の取得, 属性の選択的使用または開示を含めてもよい (MAY). 同意措置を利用する場合, CSP は追加処理の同意を身元情報サービスの条件にしてはならない (SHALL NOT).
5. CSP は,身元情報から生じる申請者からの苦情や問題を是正する手段を提供しなければならない (SHALL). そうした手段は, 申請者が容易に見つけて利用できなければならない (SHALL). CSP は苦情や問題の解決に対する手段の有効性を評価しなければならない (SHALL).
6. 身元情報の検証と登録のプロセスは, 適⽤可能な書⾯によるポリシー, または身元情報を検証するための特定の手順を規定した*実施規定*に従って実施されなければならない (SHALL). *実施規定*には,申請者が正しく登録されない検証エラーを CSP がどのように処理するか詳しく記した制御情報が含まれなければならない (SHALL). 例えば, 許容されるリトライ回数, 代わりの検証⽅法 (リモートが失敗した場合の対⾯など), 異常検知時の不正対策などである.
7. CSP は, 申請者の身元情報の検証に用いたすべての手順の記録を監査ログも含めて管理しなければならない (SHALL). そして, 検証プロセスで提⽰された身元情報の証拠の種類を記録しなければならない (SHALL). CSP は, プライバシーとセキュリティに関するリスク評価を含めたリスク管理プロセスを実施し, 以下を確定しなければならない (SHALL).
   1. ここで指定されている必須要件の他に申請者の身元情報を検証するために取り入れるステップ.
   2. CSP が検証の記録として管理する生体認証情報, 画像, スキャン, 身元情報の証拠のその他のコピーを含む PII (注意: 特定の連邦政府要件が適用される場合もある)
   3. これらの記録の保管スケジュール. (注意: CSP は適⽤可能な法律, 規制, 政策に基づく特定の保管ポリシーの対象になる場合がある. これには適⽤可能な場合の国立公文書館 (NARA) の記録保管スケジュールも含まれる)
8. 登録プロセスの一部として収集されたすべての PII は, 機密性, 完全性, 情報源の帰属を保証するために保護されなければならない (SHALL).
9. 検証のトラザクション全体は, 第三者が関与するものも含め, 認証済み保護チャネルで実施されなければならない (SHALL).
10. CSP は, 追加の不正防止策がここで規定される必須要件に代わるものでない限り, 不正防⽌策 (例えば, 位置情報の検査, 申請者のデバイス特性の調査, ⾏動特性の評価[, 社会保障庁の死亡記録 (DMF)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.html#dmf) などの統計記録の確認) を⽤いて検証の信頼性を向上させるべきである (SHOULD). CSP は, 不正防止策を講じる際に, こうした対策に対してプライバシーのリスク評価を行わなければならない (SHALL). こうした評価には, プライバシーリスク軽減策 (例えば, リスクの許容や移転, 制限付き保持, 使⽤制限, 通知), その他の技術的対策 (暗号化など), 上記 4.2(7) のそれぞれの要件の文書化が含まれなければならない (SHALL).
11. CSP が身元情報の検証および登録プロセスを終える場合, CSP は PII を含む要注意情報の完全な廃棄または破棄, または保管期間中の不正なアクセスからの保護に責任を負わなければならない (SHALL).
12. CSP が政府機関であっても⺠間プロバイダーであっても, 検証サービスの提供または利⽤には以下の要件が適⽤される.

d. CSP はプライバシー上級担当者 (SAOP) と協議し,身元情報の検証を実施するための PII 収集にプライバシー法の要件が適用されるかどうかを判断するための分析を実施しなければならない (SHALL).

e. CSP は, 該当する場合はそうした収集をカバーするために, 記録通知システム (SORN) を公開しなければならない (SHALL).

f. CSP は SAOP と協議し, 身元情報の検証を実施するための PII 収にが 2002 年電子政府法の要件が適用されるかどうかを判断するための分析を実施しなければならない (SHALL).

g. CSP は, 該当する場合はそうした収集をカバーするために, プライバシー影響評価 (PIA) を公開しなければならない (SHALL).

1. CSP は, 身元情報の決定に必要ない限り, そして身元情報の決定がその他の属性または属性組み合わせによって実現不可能でない限り, 社会保障番号 (SSN) を収集すべきでない (SHOULD NOT).

## **身元情報保証レベル 1**

*このセクションは規範である.*

IAL1 のみをサポートする CSP は, 属性を確認したり検証したりしてはならない (SHALL NOT).

1. CSP はサービス提供のために申請者に自己表明属性を要求してもしなくてもよい (MAY).
2. IAL2 や IAL3 の CSP は, ユーザーの同意があれば, IAL1 のみ必要とする RP をサポートすべきである (SHOULD).

## **身元情報保証レベル 2**

*このセクションは規範である.*

IAL2 では**リモート**または**対⾯**での身元情報の検証を許可している. IAL2 は, 利用者を増やし, 誤検出 (検証にパスできなかった正式な申請者) を減らし, 悪意ある申請者による不正な身元情報の提⽰を可能な限り検出するため, 広範囲で許容できる身元情報の検証テクニックをサポートする.

CSP はセクション4.4.1 の要件に従って優先的に検証を実施しなければならない (SHALL). CSP はサービスを提供するユーザー層に応じて, セクション4.4.2 に従って補足的に身元情報を検証してもよい (MAY).

#### **I AL2 の従来の検証要件**

#### 以下のセクションでは, 決定, 証拠, 収集, 確認, 検証, 提示のための要件を説明する. また, 生体情報の収集とセキュリティ管理策についても説明する.

* + - 1. **決定要件**

PII の収集は, 所定の文脈において一意の身元情報を決定するために必要最低限の範囲に限定されなければならない (SHALL). これにはデータ問い合わせの助けとなる属性の収集を含めてもよい (MAY). ⼀般的な決定要件はセクション5.1 を参照.

#### **証拠の収集要件**

CSP は以下を申請者から収集しなければならない (SHALL).

* + - * 1. 証拠の発行元が自らの検証イベントにおいて, “優” または “強” な証拠を2つ以上の形で収集して主張された身元情報を確認しており, **かつ** CSP が発行元と直接その証拠を確認した場合は, “優” か “強” の証拠の1つ. **または**
        2. “強” の証拠を2つ. **または**
        3. “強” の証拠を1つと “適” の証拠を2つ.

許容可能な身元情報の証拠についての詳細は, セクション5.2.1 身元情報の証拠の品質要件を参照.

#### **確認要件**

CSP は, 提示された証拠と同じ強度が達成できるプロセスでそれぞれの証拠を確認しなければならない (SHALL). 例えば “強” の証拠の2つの形が提⽰された場合は, それぞれを “強” な強度で確認する.

身元情報の証拠の確認についての詳細は, セクション5.2.2 身元情報の証拠の確認を参照.

#### **検証要件**

CSP は身元情報の証拠を以下のように検証しなければならない (SHALL).

* + - * 1. 最低でも, 申請者と身元情報の証拠 の結び付けは, 強度 “強” を達成できるプロセスによって検証されなければならない.
        2. 知識ベース検証 (KBV) は, 対⾯ (物理的または監視されたリモート) の身元情報検証に利⽤してはならない (SHALL NOT).

身元情報の証拠の検証についての詳細は, セクション5.3 身元情報の検証を参照.

#### **対面要件**

CSP は対⾯またはリモートによる身元情報の検証をサポートしなければならない (SHALL). CSP は両⽅を提供すべきである (SHOULD).

#### **住所の確認**

* + - * 1. 住所を確認できる有効な記録は, 発行元か信頼元のものでなければならない (SHALL).
        2. CSP は記録上の住所を確認しなければならない (SHALL). CSP は, 提⽰された有効な身元情報の証拠 のいずれかに記載された住所の確認を通して, 記録上の住所を確認すべきである (SHOULD). CSP は, 申請者が提供したいかなる有効な身元情報の証拠にも記載されていない情報の確認を通して, 記録上の住所を確認してもよい (MAY).
        3. 記録時に確認しなかった自己表明の住所データは, 確認に⽤いてはならない (SHALL NOT).

##### CSP が対⾯検証 (物理的または監視されたリモート) を実施する場合

CSP は確認された記録上の住所に検証の通知を送るべきである (SHOULD).

加入者と認証コードの結び付けが後⽇発⽣する場合は, CSP は登録コードを直接加入者に提供してもよい (MAY).

登録コードは最⼤7⽇間有効でなければならない (SHALL).

##### CSP がリモート検証 (監視なし) を実施する場合

CSP は申請者に対して確認された記録上の住所に登録コードを送付しなければならない (SHALL).

申請者は身元情報の検証プロセスを完了するために有効な登録コードを提⽰しなければならない (SHALL)

CSP は記録で確認した郵送先に登録コードを送付すべきである (SHOULD). CSP は, 記録で確認済みであれば, 携帯電話 (SMS や⾳声), 固定電話, Eメール に登録コードを送信してもよい (MAY).

登録コードが認証ファクタとしての⽤途も兼ねている場合は, ⼀度使用したらリセットされなければならない (SHALL).

登録コードの最大有効期限は, 以下でなければならない (SHALL).

i. 地続きの州内で記録上の郵便宛先に送る場合は10日間

ii. 地続きの州外で記録上の郵便宛先に送る場合は30日間

iii. 記録上の電話に送る場合 (SMS か音声) は10分間

iv. 記録上の Eメールアドレスに送る場合は24時間

CSP は, 登録コードと検証通知が異なる記録上の住所に送信されることを保証しなければならない (SHALL). 例えば, 記録で確認した電話番号に登録コードを送信するならば, 検証通知は, 記録で確認した郵便住所や, 確認および検証済みの運転免許証のような証拠に記載された郵便住所に送られる.

注意: 郵送先は, 登録コードと通知を含めたあらゆる連絡物を送る際に優先される方法である.しかし, これらのガイドラインでは, 確認された記録上の住所が物理的であってもデジタルであってもそれをサポートする.

#### **生体認証情報の収集**

[CSP は否認防⽌や再検証を⽬的として生体認証情報を収集してもよい (MAY). 生体認証情報の収集に関する詳細は SP 800- 63B,セクション5.2.3 (sp800-63b.html#biometric\_use) を参照.](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use)

#### **セキュリティ管理策**

CSP は, SP 800-53 やそれに相当する連邦政府標準 (例えば FEDRAMP) または業界標準に定められた中または高レベルのセキュリティ管理策の中から, 管理の強化を含め適切に調整したセキュリティ管理策を採⽤しなければならない (SHALL). CSP は, *影響が中レベル*のシステムやそれに相当する最小限の保証関連管理が十分であることを保証しなければならない (SHALL).

#### **IAL2 信頼できる身元保証人の検証要件**

個⼈がセクション4.4.1 に規定された身元情報の証拠要件を満たすことができない場合, 機関は信頼できる⾝元保証⼈を申請者の身元情報の検証に参加させてもよい (MAY).

## **身元情報保証レベル 3**

*このセクションは規範である.*

IAL3 では IAL2 で要求される手順がさらに厳格化され, 強度の⾼い別の証拠の提供が求められるほか, なりすましや不正やその他の重大なダメージから身元情報と RP を保護する特定の追加プロセス (生体認証情報の利⽤を含む) も求められる. 生体認証情報は, 不正なまたは重複した登録を検出するために利⽤され, 認証情報への結び付けを再確⽴する⼿段としても利⽤される. これに加え, IAL3 での身元情報の検証は対⾯ (監視されたリモートを含む) で実施される. 詳細はセクション5.3.3 を参照.

#### **決定要件**

PII の収集は, 所定の文脈において一意の身元情報を決定するために必要最低限の範囲に限定されなければならない (SHALL). これにはデータ問い合わせの助けとなる属性の収集を含めてもよい (MAY). ⼀般的な決定要件はセクション5.1 を参照.

#### **証拠の収集要件**

CSP は以下を申請者から収集しなければならない (SHALL).

1. 2つの “優” の証拠. **または**
2. “強” の証拠の発行元が, その身元情報の検証イベントにおいて, “優” か “強” の証拠を2つ以上の形で収集して主張された身元情報を確認しており, **かつ** CSP が発行元と直接その証拠を確認した場合は, “優” の証拠１つと “強” の証拠を1つ. **または**
3. “強” の証拠を2つと “適” の証拠を1つ.

許容可能な身元情報の証拠についての詳細は, セクション5.2.1 身元情報の証拠の品質要件を参照

#### **確認要件**

CSP は身元情報の証拠を以下のように確認しなければならない (SHALL).

それぞれの証拠は, 提⽰された証拠と同じ強度に到達できるプロセスによって確認されなければならない. 例えば “強” な身元情報の証拠 が２つの形で提⽰された場合は, それぞれは “強” な強度で確認される.

身元情報の証拠の検証についての詳細は, セクション5.2.2 身元情報の証拠の検証を参照

#### **検証要件**

CSP は身元情報の証拠を以下のように検証しなければならない (SHALL)

1. 最低でも, 申請者と身元情報の証拠 の結び付けは, 強度 “優” を達成できるプロセスによって検証されなければならない.
2. 知識ベース検証 (KBV) は, 対⾯ (物理的または監視されたリモート) の身元情報検証に利⽤してはならない (SHALL NOT).

許容可能な身元情報の証拠についての詳細は, セクション5.3 身元情報の検証を参照

#### **面前要件**

CSP は身元情報の検証の全ステップを申請者と対⾯で実施しなければならない (SHALL). 詳細はセクション5.3.3 を参照.

#### **住所の確認**

1. CSP は記録上の住所を確認しなければならない (SHALL). CSP は, 提⽰された有効な身元情報の証拠 のいずれかに記載された住所の確認を通じて, 記録上の住所を確認すべきである (SHOULD). CSP は, 申請者が提供したいかなる有効な身元情報の証拠 にも記載されていない情報の確認を通して記録上の住所を確認してもよい (MAY).
2. 自己表明された住所データを確認に⽤いてはならない (SHALL NOT).
3. 検証の通知は確認された記録上の住所に送らなければならない (SHALL).
4. 加入者と認証コードの結び付けが後⽇発⽣する場合は, CSP は登録コードを直接加入者に提供してもよい (MAY). 登録コードは最⼤7⽇間有効でなければならない (SHALL).

#### **生体認証情報の収集**

CSP は否認防⽌や再検証を⽬的として, 検証時に生体サンプルを収集して記録しなければならない (SHALL). 生体認証情報の収集に関する詳細は [SP 800-63B,セクション5.2.3 (sp800-63b.html#biometric\_use)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use) を参照.

#### **セキュリティ管理策**

CSP は, SP 800-53 やそれに相当する連邦政府標準 (例えば FEDRAMP) または業界標準に定められた高レベルのセキュリティ管理策の中から, 管理の強化を含め適切に調整したセキュリティ管理策を採⽤しなければならない (SHALL). CSP は, *影響が高レベル*のシステムやそれに相当する最小限の保証関連管理が十分であることを保証しなければならない (SHALL).

## **登録コード**

*このセクションは規範である.*

登録コードにより, CSP は申請者が記録上の住所を管理していることを確認できるほか, 申請者は登録の記録との結び付けを再構築できる. 結び付けは, 元の身元情報の検証のトランザクションと同じセッションで完了する必要はない (NEED NOT).

登録コードは以下の１つで構成されなければならない (SHALL).

1. 最低でも６⽂字の英数字かそれに相当するエントロピーを持つもの. 例えば, 承認された乱数⽣成器を使って⽣成されたコードや, 物理ハードウェア認証コードのシリアル番号.
2. ランダムな６⽂字の英数字と同じかそれ以上のエントロピーを持つデータを含む, QR コードなどの機械可読光学ラベル.

## **要件のまとめ**

*このセクションは参考情報である.*

表 4-1 に各身元情報保証レベルの要件をまとめる.

##### 表 4-1 IAL 要件のまとめ

|  |  |  |  |
| --- | --- | --- | --- |
| **要件** | **IAL1** | **IAL2** | **IAL3** |
| 対面 | 要件なし | 対⾯および監視なしのリモート | 対⾯および監視ありのリモート |
| 決定 | 要件なし | * 身元情報の決定に最小限必要な属性. * KBV により信頼を⾼めてもよい. | IAL2 と同じ |
| 証拠 | どのような証拠も収集されない | * 元の証拠の強度と発行元が実施した確認に応じて, “優” か”強” な１つの証拠, または * 2つの “強” の証拠, または * 1つの “強” の証拠と2つの “適” の証拠. | * 2つの “優” の証拠, または * 元の証拠の強度と発行元が実施した確認に応じて, 1つの “優” と１つの “強” の証拠, または * 2つの “強” の証拠と1つの “適” の証拠. |
| 確認 | 確認なし | 提示された証拠と同じ強度のプロセスでそれぞれの証拠を確認しなければならない. | IAL2 と同じ |
| 検証 | 検証なし | “強” の強度が達成できるプロセスによって検証する. | “優” の強度が達成できるプロセスによって検証する. |
| 住所の確認 | 要件なし | 必須. 登録コードを任意の記録上の住所に送付する. 通知を登録コードとは別の手段で送付する. | 必須. 検証の通知を郵送先住所に送付する. |
| 生体認証情報の収集 | なし | 任意 | 必須 |
| セキュリティ管理策 | N/A | * SP 800-53 * 中レベル (またはそれ相当の連邦 / 業界標準). | * SP 800-53 * 高レベル (またはそれ相当の連邦 / 業界標準). |

1. **身元情報の決定, 確認, 検証**

*このセクションは規範である.*

このセクションでは, 身元情報と提⽰された身元情報の証拠の決定, 確認, 検証に関する要件を⽰す. これらの要件は, 主張された身元情報が CSP に登録しようとしている主体の実際の身元情報であることを確実にし, 登録された多数の個⼈に影響するどのような攻撃も, システムが保護しているリソースの価値に時間の上からも費用の上からも見合わないようにすることを確実にする.

## **身元情報の決定**

身元情報の決定の目標は, ある個⼈を所定のユーザー層や文脈一意に区別することである. 効率的に身元情報を決定するには, 個人を特定するのに必要な属性の最⼩セットを使用する. これは CSP による身元情報の検証プロセス全体に潜在的な不正の初期検出を含めるための重⼤な出発点となるが, それだけでは決して完全で有効な検証トランザクションにならない.

1. 検証プロセスで利⽤される情報の完全⼀致は達成が困難である. CSP は, 複数の証拠, 発行元, 信頼元を通して, 個人情報とその他の関連する検証データの違いを調べるために適切な照合アルゴリズムを⽤いてもよい (MAY). 使⽤する照合アルゴリズムとルールは, 一般に向けてまたは少なくとも関連する利益共同体に向けて公開されるべきである (SHOULD). 例えば, ⽂書化されたポリシーやセクション4.2 で⾔及されている*実施規定*にそれらを含めることができる.
2. KBV (知識ベース認証とも呼ばれる) は, 公開データベースから得られる情報に対して申請者の知識をテストすることにより, 主張された身元情報を検証するために使⽤されてきた. CSP は主張された一意の身元情報を決定するために KBV を使用してもよい (MAY).

## **身元情報証拠の収集と確認**

身元情報の確認の目標は, もっとも適切な身元情報の証拠 (例えばパスポートや運転免許証) を申請者から収集し, その信憑性, 有効性, 正確性を確定することである. 身元情報の確認は, 身元情報の適切な証拠の収集, それが本物で有効であることの確認, 証拠に含まれるデータが正当, 最新かつ実在する主体に関連していることの確認という３つのステップから成る.

#### **身元情報証拠の品質要件**

このセクションでは, 身元情報の検証段階で収集する証拠 の品質要件について述べる.

表 5-1 には, 正当な身元情報を確⽴するために収集する証拠について, “許容不可” から “優” までの強度を列挙する. 特に記載がない限り, 所定の強度を達成するために, 証拠は少なくともここに列挙されたすべての品質を満たさなければならない (SHALL).

##### 表 5-1 身元情報の証拠の強度

|  |  |
| --- | --- |
| **強度** | **身元情報の証拠の品質** |
| 許容不可 | 許容可能な身元情報の証拠ではない. |
| 弱 | * 証拠の発行元が身元情報を検証していない. * 証拠の発⾏プロセスで, 証拠が申請者の手に渡ったことが当然のように想定できる. * 証拠が以下を含む. * 証拠⾃体かそれに関係する⼈物を⼀意に識別できる少なくとも1つの参照番号. **または** * 関係する⼈物の写真か生体認証テンプレート (様式は問わない). |
| 適 | * 証拠の発行元が, 主張された身元情報の検証プロセスを通じて確認している. * 証拠の発⾏プロセスで, 証拠に関係する⼈物の手に証拠が渡ったことが当然のように想定できる. * 証拠が以下を満たす.   + 証拠⾃体かそれに関係する⼈物を⼀意に識別できる少なくとも1つの参照番号を含む. **または**   + 関連付けられた⼈物の写真か生体認証テンプレート (様式は問わない) を含む. **または**   + KBV を通じて所有権を確認できる. * 証拠にデジタル情報が含まれる場合, その情報は認可された暗号方法か固有の方法, またはその両⽅により保護され, そうした方法により情報の完全性が保証され, 主張された発行元の信憑性が確認できる. * 証拠に物理セキュリティ機能が含まれる場合, それを再現するために固有の知識が必要になる. * 発行された証拠の有効期限が切れていない. |
| 強 | * 証拠の発行元が, 本人の実際の身元情報を知っていることに適切な確信を持てるように⽂書化された⼿続きを通して, 主張された身元情報を確認している. このような⼿続きは, 規制当局または公的に責任がある機関によって定期的に監督される. 例えば, 2001年愛国者法や, 2003年公正かつ正確な信用取引法 (FACTA) のセクション 114 に定められたレッドフラグルールに対処するために作成された顧客識別プログラム (CIP) ガイドラインである. * 証拠の発⾏プロセスで, 証拠がそれに関係する主体の手に渡ったことが保証される. * 証拠に関係する⼈物を⼀意に識別できる少なくとも1つの参照番号が含まれる. * 証拠に記載された氏名は, 当⼈が発⾏時点において正式に知られている名前でなければならない. 仮名, 別名, イニシャルは許容されない.   + 発行された証拠は, 関係する⼈物の写真か生体認証 テンプレート (様式は問わない) を含む. **または**   + 申請者が, 少なくとも IAL2 の身元情報に結びづいた AAL2 の認証コードかそれに相当するものを保持していることを証明している. * 証拠にデジタル情報が含まれる場合, その情報は認可された暗号方法か固有の方法, またはその両⽅により保護され, そうした方法により情報の完全性が保証され, 主張された発行元の信憑性が確認できる. * 証拠に物理セキュリティ機能が含まれる場合, それを再現するための固有の知識と固有の技術が必要になる. * 証拠の有効期限が切れていない. |
| 優 | * 証拠の発行元が, 主体の実際の身元情報を知っていることに高い確信を持てるように⽂書化された⼿続きを通じて, 主張された身元情報を確認している. このような⼿続きは, 規制当局または公的に責任がある機関によって定期的に監督される. * 発行元は申請者を視覚的に識別し, 当⼈の存在確認のためのさらなるチェックを⾏なっている. * 証拠の発⾏プロセスで, 証拠がそれに関係する人物の手に渡ったことが保証される. * 証拠に関係する⼈物を⼀意に識別できる少なくとも1つの参照番号が含まれる. * 証拠に記載された氏名は, 当⼈が発⾏時点において正式に知られている名前でなければならない. 仮名, 別名, イニシャルは許容されない. * 証拠は, それに関係する⼈物の写真を含む. * 証拠は, それに関係する⼈物の生体認証テンプレート (様式は問わない) を含む. * 証拠はデジタル情報を含みｚ |

* + 1. **身元情報の証拠の確認**

CSP はひとたび身元情報の証拠を取得すると, 証拠とその関連情報の正確さ, 信憑性, 完全性を信頼元に照会し, 提⽰された証拠に対して以下を確定する.

* 本物で正確であり, 偽造や捏造されていない.
* 正確な情報が含まれている..
* 実在する主体に関する情報が含まれている.

表 5-2 は, 検証セッションで提⽰された証拠とそこに含まれる情報を確認するために CSP が実施する身元情報の確認 について, “許容不可” から “優” までの強度を列挙する.

##### 表 5-2 身元情報の証拠の確認

|  |  |
| --- | --- |
| **強度** | **CSP が実施する方法** |
| 許容不可 | * 証拠が確認されていないか確認に失敗した. |
| 弱 | * 証拠から得られるすべての詳細な個⼈情報は,信頼元が保有または公開している情報と⽐較して正当性が確認された. |
| 適 | * 証拠に含まれる属性は, 発行元か信頼元が保有または公開している情報と⽐較して正当性が確認された. **または** * 物理セキュリティ機能の完全性と証拠が改竄や不正な変更を受けていないことを確認する適切な技術によって, 証拠が本物であることが確認された. **または** * 訓練を受けた担当者により証拠が本物であると確認された. **または** * 暗号論的セキュリティ機能の完全性を確認することにより, 証拠が本物であると確認された. |
| 強 | * 以下のように証拠が本物であると確認された.   + 適切な技術を使用し, 物理セキュリティ機能の完全性と証拠が改竄や不正な変更を受けていないことを確認した. **または**   + 訓練を受けた担当者と適切な技術によって, 物理セキュリティ機能の完全性が確認され, 証拠が改竄や不正な変更を受けていないことを確認した. **または**   + 暗号論的セキュリティ機能の完全性を確認した. * すべての詳細な個⼈情報と詳細な証拠は,発行元か信頼元が保有または公開している情報と⽐較して正当性が確認された. |
| 優 | * 訓練を受けた担当者と, 物理的で暗号論的セキュリティ機能の完全性を含めた適切な技術によって,証拠が本物であることを確認した. * 証拠から得られるすべての詳細な個⼈情報と詳細な証拠は,発行元か信頼元が保有または公開している情報と⽐較して正当性が確認された. |

証拠を確認する担当者の訓練に関する要件は, CSP または RP のポリシー, ガイドラインまたは要件に基づかなければならない (SHALL).

## **身元情報の検証**

身元情報の検証の目標は, 主張された身元情報と, 証拠を提⽰する実際に存在する主体との関連付けを確認して確⽴することである.

#### 身元情報の検証方法

表 5-3 は, 身元情報の検証強度を達成するために必要な検証⼿段の詳しい説明である. CSP は, 身元情報の検証に KBV を利⽤する場合は,セクション5.3.2 の要件に従わなければならない (SHALL).

##### 表 5-3 身元情報の証拠の検証

|  |  |
| --- | --- |
| **強度** | **身元情報の検証方法** |
| 許容不可 | 証拠は検証されていないか, 検証に失敗した. 申請者が主張された身元情報の所有者であることが確認できない. |
| 弱 | 申請者が主張された身元情報を裏付けるために提出された証拠へのアクセス権限を持っていることが確認された. |
| 適 | * 申請者が主張された身元情報の所有者であることが, 以下のように確認された.   + KBV. 詳細はセクション 5.3.2. を参照. **または**   + 主張された身元情報を裏付けるために提⽰された最も強力な証拠と申請者の物理的⽐較.リモートによる物理的な⽐較は[, [SP 800-63B,セクション5.2.3.] (sp800-63b.html#biometric\_use)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use) のすべての要件に従わなければならない (SHALL). **または**   + [申請者の生体認証情報と身元情報の証拠の⽐較. リモートで実施した生体認証上の⽐較は, [SP 800-63B,セクション 5.2.3.] (sp800-63b.html#biometric\_use) のすべての要件に従わなければならない(SHALL).](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use) |
| 強 | * 申請者 が 主張された身元情報の所有者であることが, 以下のように確認された. * 適切な技術を使用し, 主張された身元情報を裏付けるために提⽰された証拠の中で最も強力なものと写真との[物理⽐較. リモートによる生体認証上の比較は, [SP 800-63B,セクション5.2.3.] (sp800-63b.html#biometric\_use) のすべての要件に従わなければならない (SHALL).](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use) **または** * 適切な技術を使用し, 主張された身元情報を裏付けるために提⽰された証拠の中で最も強力なものと申請者の生体認証上の比較. [リモートで実施した生体認証上の比較は, [SP 800-63B,セクション5.2.3.] (sp800-63b.html#biometric\_use) のすべての要件に従わなければならない (SHALL).](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use) |
| 優 | 申請者が主張された身元情報の所有者であることが, 主張された身元情報を裏付けるために提⽰された証拠の中で最も強力な証拠との申請者の生体認証上の比較より確認された. リモートで実施した生体認証上の比較は[, [SP 800-63B,セクション5.2.3.] (sp800-63b.html#biometric\_use)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use) のすべての要件に従わなければならない (SHALL). |

* + 1. **知識ベース検証の要件**

IAL2 の身元情報の検証には以下の要件が適⽤される. KBV を身元情報の決定に⽤いる場合の制約は何もない.

1. CSP は, 身元情報について確認した1つ以上の証拠に対して, KBV を⽤いて申請者の身元情報検証を⾏なってはならない (SHALL NOT).
2. CSP は, KBV プロセスを開始するのに必要な情報を含めるために, 申請者と信頼元だけが知っていると予測される情報だけを使⽤しなければならない (SHALL). ⾃由に取得可能な情報, パブリックドメインで料金を支払えば⼿に⼊る情報, ブラックマーケットで⼿に⼊る情報は使⽤してはならない (SHALL NOT).
3. CSP は, 決定と確認が完了した身元情報に対して, KBV 以外の別の検証プロセスを利⽤できるようにしなければならない (SHALL).
4. CSP は, CSP が参加していた最近のトランザクション履歴に関する知識を検証してから KBV を実施すべきである (SHOULD). CSP は, トランザクション情報が最低限20ビットのエントロピーを持つことを保証しなければならない (SHALL). 例えば, 最⼩のエントロピー要件を満たすには, 申請者に自分の銀⾏⼝座に対して少額預金の金額と取引番号の照合を求めることができる. この例では全桁数は７桁以上になる.
5. CSP は, 申請者が主張された身元情報の所有者であることを⽰すための質問を行って KBV を実⾏しても良い (MAY). しかしその場合は以下の要件が適用される.
   1. KBV は複数の信頼元に基づくべきである (SHOULD).
   2. CSP は最低限4つの質問を⾏い, それぞれの正解をもって KBV ステップの成功としなければならない(SHALL).
   3. CSP は⾃由回答⽅式の KBV 質問を⾏うべきである (SHOULD). 選択式質問でもよいが (MAY), その場合は各質問に4つ以上の選択肢を⽤意しなければならない (SHALL).
   4. CSP は KBV を完了するために申請者に2度の試⾏を許すべきである (SHOULD). 3回以上の試⾏を許可してはならない (SHALL NOT).
   5. CSP は質問ごとに2分間の無反応状態があれば KBV セッションをタイムアウトさせなければならない(SHALL). セッションがタイムアウトした場合は失敗と見なし, KBV プロセス全体を繰り返さなければならない (SHALL).
   6. CSP は KBV の⼤部分を陽動となる質問にしてはならない (SHALL NOT). (つまり, "上記以外" が正解となるような質問)
   7. CSP は同じ KBV 質問を後の試⾏で尋ねるべきではない (SHOULD NOT).
   8. CSP は, 単⼀のセッションまたは失敗後のセッションにおいて, 後の KBV 質問に役⽴つ情報を提供するような質問をしてはならない (SHALL NOT).
   9. CSP は正解が変わらない KBV 質問を利⽤してはならない (SHALL NOT). (例 "始めて購入した自動車は何ですか?")
   10. CSP は, いかなる KBV 質問も,申請者がまだ提⽰していない PII や, KBV セッション中の他の情報と組み合わせて特定の個⼈の識別につながるような個人情報を漏洩させることのないことを保証しなければならない (SHALL).

#### **対面検証の要件**

IAL3 の対⾯検証には, 以下の2つの⽅法がある.

担当者の監視下で行われる申請者との物理的対応.

セッション 5.3.3.2 にある特別な要件に基づいた, 担当者の監視下で行われる申請者とのリモート対応.

#### **一般要件**

* + - * 1. CSP は, 不⾃然な材料の存在を調べるために, 検証プロセスの一部として担当者に生体認証サンプル (指や 顔) を確認させなければならない (SHALL).
        2. CSP は, 生体情報が他の主体ではなくその申請者から収集されたことが保証される⽅法で生体情報を収集しなければならない (SHALL). 生体認証の実施には, [SP 800-63B,セクション5.2.3 (sp800-63b.html#biometric\_use)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#biometric_use) の要件がすべて適用される.

#### **監視下のリモート対面検証の要件**

CSP は,リモート検証プロセスを採⽤し, 対⾯と同等レベルの信頼性とセキュリティを実現することもできる. 以下の要件により, 申請者が CSP と物理的に同じ場所にいる対⾯処理と, 申請者がリモートの場合の処理との比較ができる.

監視下のリモート身元情報の検証と登録の処理は, セクション4.6 に⽰した IAL3 での確認および検証要件に加えて, 以下の要件に従わなければならない (SHALL).

* + - * 1. CSP は,申請者がその場から離れてはならない (SHALL NOT) 検証セッション全体を監視しなければならない (SHALL). 例えば, 申請者の継続的な⾼解像度ビデオ伝送.
        2. CSP は,身元情報の検証セッション全体を通じて, 申請者と共にリモート担当者をリアルタイムで参加させなければならない (SHALL).
        3. CSP は,身元情報の検証セッション全体を通じて, 申請者が⾏ったすべてのアクションがリモート担当者にはっきりと⾒えるようにしなければならない (SHALL).
        4. CSP は, 証拠に対するすべてのデジタル検証 (例えばチップやワイヤレス技術を使用) が, 統合されたスキャナーやセンサーで実⾏されるようにしなければならない (SHALL).
        5. CSP は潜在的な不正を検出してリモート検証セッションを正しく実⾏するため, 担当者に訓練プログラムを受けさせなければならない (SHALL).
        6. CSP は, 環境に応じて物理的改竄の検出策と対抗策を適切に施さなければならない (SHALL). 例えば, 制限されたエリアや信頼できる個⼈によって監視されているエリアにあるキオスクは, ショッピングモールのコンコースなどの半公開エリアにあるキオスクよりも, 改竄検出の必要性は低い.
        7. CSP は, すべての通信が相互認証されて保護されたチャネルで⾏われることを確実にしなければならない (SHALL).

#### **5.3.4 信頼できる身元保証人の要件**

1. CSP は, 公証人や法的保護者, 医療専⾨家, 後⾒⼈, 法定代理⼈, 訓練を受け承認されたか認定された個人を, 適切な法律, 規則, 機関のポリシーに従って,申請者の⾝元を保証したりその代理⼈を務めたりする信頼できる身元保証人として利用してもよい (MAY). CSP はリモートと対⾯のどちらのプロセスでも, 信頼できる身元保証人を利用してもよい (MAY).
2. CSP は, 信頼できる身元保証人の確定と, 保証人としての資格が維持される期間について, 資格の取り消しや⼀時停⽌といったあらゆる制約も含めたポリシーと⼿順を明⽂化しなければならない (SHALL).
3. CSP は,申請者を検証した同じ IAL で信頼できる身元保証人を検証しなければならない (SHALL). また CSP は, 信頼できる身元保証人と申請者を結び付けるのに必要な最低限の証拠を確定しなければならない (SHALL).
4. CSP は,セクション4.4.1 の要件を満たすことを目標として, 上記1で指定された書面のポリシーに定義されたように定期的に加入者を再検証すべきである (SHOULD).

#### **5.3.4.1 未成年者に対する追加要件**

1. CSP は, 児童のオンライン上のプライバシー保護を定めた 1998年の法律 (COPPA) と該当する場合はその他の法律を遵守することを保証するために, 身元情報の検証の証拠要件を満たすことができない未成年者の扱いについて法的制約を特に考慮しなければならない (SHALL).
2. 13歳以下の児童に関しては, CSP は COPPA とその他の法律の下で別の配慮が必要になるため, CSP は該当する場合に準拠を保証しなければならない (SHALL).
3. CSP は, このセクションの別の箇所で述べたように, 未成年の申請者の信頼できる身元保証人として, 親か法定成⼈後⾒⼈を関与させるべきである (SHOULD).

## **5.4 結び付け要件**

認証コードと加入者の結び付けについては[, 800-63B (sp800-63b.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html) Section 6.1 認証コードの結び付けを参照.

# 導出した認証情報

*このセクションは参考情報である.*

認証情報の導出 (derived) は, 個⼈が⾃⾝の所有する1つ以上の認証コードに結び付けられた身元情報レコード (つまり認証情報) の正当な主体であることを CSP に対して証明するプロセスに基づいている. 個⼈に対して既存の身元情報の検証済みレコードや認証情報に結び付いた新たな認証コードを取得することを考える CSP は, このプロセスを利⽤することができる.身元情報の検証プロセスを繰り返す回数を最小限にすることは個⼈と CSP のメリットになる. 元の検証済みのデジタル ID にすでに結び付いている認証コードの保持証明と, その認証コードを使った認証の成功をもって, 身元情報の導出は達成される.

このセクションにおける導出の定義では, ある鍵から別の鍵を導出するなど, 認証コードが暗号論的に一次的認証コードに結び付いていることは意味*しない*. むしろ, すでに検証した身元情報に結び付いた認証コードを使った認証が成功したことに基づき, 不必要な身元情報の検証を繰り返すことなく新たに発行することにより認証コードを導出させることができる.

身元情報の導出を⾏うユースケースとしては, 以下の2つがある.

1. *認証要求者*が, PIV スマートカードを所有するための制限と権限の範囲内だけで利⽤する目的で, ⾃⾝の身元情報レコードに結び付いている導出された PIV を取得しようとする. *このユースケースについては SP 800-157, 導出した身元情報検証 (PIV) 認証情報のガイドラインを参照*
2. *申請者*が, 事前に関係性を持たない CSP との間で認証情報を確⽴しようとする. 例えば, 申請者がある CSP から別の CSP に移⾏しようとしたり, 新たな CSP から個別の認証コードを別⽬的 (基本的なブラウジングに対する⾦融取引など) で得ようとしたりすることが考えられる. *このユースケースについては,セクション5.2 にある受け⼊れ可能な身元情報の証拠に関する記述を参考.*

上で述べたように, PIV から導出される認証情報に関する要件はすべて SP 800-157 に記載されている. 2つめのユースケースに関しては, 本ガイドラインは物理的な身元情報の証拠とデジタルな身元情報の証拠の区別をつけない. したがって, 最初の CSP が⽣成した認証コードやアサーションがセクション5 の要件を満たせば, それらを IAL2 や IAL3 の身元情報の証拠 として利⽤することもできる. さらに, デジタルな身元情報の証拠を提⽰した結果として発⾏された認証コードに対しては[, SP 800-63B (sp800-63b.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html) の要件が適用される.

# 脅威とセキュリティの考慮事項

*このセクションは参考情報である.*

登録プロセスの脅威には, なりすましと, インフラ提供者に対する不正アクセスや提供者⾃⾝の不正⾏為, という2つのカテゴリが⼀般的に存在する. インフラに対する脅威は従来のコンピュータセキュリティ管理策 (侵⼊防⽌, 記録保持, 独⽴監査など) により対応可能でありこの文書の範囲外であるため, このセクションではなりすましの脅威に焦点を当てる. セキュリティ管理策に関する詳細は SP 800-53 *連邦情報システムおよび機関に推奨されるセキュリティおよびプライバシー管理*を参照.

登録プロセスにおける脅威としては, なりすましに加え, 身元情報の検証, 認証コードの結び付け, 認証情報の発⾏の各段階における通信メカニズムに対する脅威がある. 表 7-1 に登録と身元情報の検証に関連する脅威をまとめる.

##### 表 7-1登録と身元情報の検証に関する脅威

|  |  |  |
| --- | --- | --- |
| **アクティビティ** | **脅威/攻撃** | **例** |
| 登録 | 身元情報の検証証拠の偽造 | 申請者が偽造した運転免許証を利⽤して不正な身元情報を主張する. |
| 他⼈の身元情報の不正利⽤ | 申請者が他⼈のパスポートを利⽤する. |
| 登録の否認 | 加入者が CSP に登録していないと主張する. |

* 1. **脅威の軽減方針**

登録における脅威は, なりすましを困難にしたり, なりすましの検出率を向上させたりすることで抑制できる. この推奨対策では, 主になりすましを困難にする⼿法について扱うが, 誰がなりすましを⾏なったかを証明するのに役⽴つ⼿段と⼿順も説明する. 各レベルにおいて, 主張された身元情報が存在すること,申請者が主張された身元情報の所有者であること,申請者が後⽇登録を否認できないことを確実にする⽅法が採⽤される.保証レベルが上がるにつれ, 偶発的, 組織的, 内部的ななりすましに対する抵抗⼒が⾼まる. 表 7-2 に登録および発⾏プロセスにおける脅威への対策に関する方針をまとめる.

##### 表 7-2 登録および発行に対する脅威の軽減方針

|  |  |  |  |
| --- | --- | --- | --- |
| **アクティビティ** | **脅威/攻撃** | **軽減方針** | **規範の参照** |
| 登録 | 身元情報の検証証拠の偽造 | CSP は提⽰された証拠の物理セキュリティ機能を確認する. | 4.4.1.3, 4.5.3, 5.2.2 |
|  |  | CSP は証拠発⾏元やその他の信頼元に対して証拠に記載された個⼈の詳細を確認する. | 4.4.1.3, 4.5.3, 4.5.6, 5.2.2 |
|  | 他⼈の 身元情報の不正利⽤ | CSP は証拠発⾏元やその他の信頼元から取得した情報と照らし合わせて申請者の身元情報の証拠と生体認証情報を検証する. | 4.4.1.7, 4.5.7, 5.3 |
|  |  | 申請者が提供した⾮政府機関発⾏の書類 (申請者名義で申請者の現住所が記載された電気代の請求書や, クレジットカードの請求書など) を検証し,申請者の身元情報の信頼度を⾼める. | 4.4.1.7, 4.5.7, 5.3 |
|  | 登録の否認 | CSP は加入者の生体認証情報を保存する. | 4.4.1.7, 4.5.7 |

1. **プライバシーの考慮事項**

*このセクションは参考情報である.*

以下のプライバシーに関する考慮事項は,セクション4.2 の 一般 要件に関する情報を提供する.

* 1. **収集とデータの最小化**

セクション 4.2 の要件 2 は, 身元情報に関する決定, 確認,検証に適⽤可能な最良事例に基づいて, 主張された身元情報の存在確認と申請者との関連付けに必要な PII に限って収集を許可している. 不必要な PII を収集すると, 身元情報の検証に利⽤されない情報がどうして収集されているのかについて混乱が⽣じる. これは権利侵害や余計な懸念につながり,申請者の信頼を損ねる可能性がある. さらに, PII を保持すると不正アクセスや不正利⽤に対して脆弱になる可能性もある. データの最⼩化により PII の量を減らしてこうしたリスクを軽減することは,身元情報の検証プロセスにおける信頼を高める.

#### **社会保障番号 (SSN)**

セクション 4.2 の要件 13 では, 身元情報の決定が SSN 以外の属性や属性の組み合わせによって達成できないときのように SSN が身元情報の決定に必要でない限り, CSP が SSN を収集することを許可していない. SSN への過度な信頼は誤⽤を招き, なりすましなどにより申請者に損害を与える. しかし, 連邦政府機関の RP にとっては, SSN によって加入者を既存の記録に関連付けることができ, 身元情報が決定できるケースもある. したがって, この文書は SSN の役割を識別⼦として捉え, その利⽤に関して適切な許可を与える.

注意: より高レベルの IAL での証拠要件は, SSN や社会保障カードを許容可能な身元情報の証拠として使用することを排除している.

身元情報の検証⽬的で SSN を収集する前に, 各組織は SSN を収集する際の法的義務, 第三者のプロセスやシステムとの相互運⽤性のために SSN を利⽤する必要性, または運⽤要件を考慮する必要がある. 運⽤要件は, システムやプロセス, 形式がコストや許容できないリスクレベルが原因で変更できないことによって提示できる. なお, 運⽤上の必要性は, 使い勝⼿や変更を望まないという理由によって正当化されるものではない.

連邦政府機関に対する [行政命令 (EO) 9397] (#9397) の初期の要件では, 職員, 取引関係にある個⼈または取引関係にある他組織に属する個⼈を識別する主要⼿段として SSN の使用を指定していたが、この要件は削除された. したがって, 行政命令 9397 は SSN 収集を必要と定めた唯一の出典として引用することはできない.

連邦政府機関は, 行政管理予算局の方針に従って SSN の収集および不必要な利⽤を抑制する義務を考慮に⼊れ, SSN を収集するあらゆる決定を見直す必要がある.

## **通知と同意**

[セクション 4.2 の要件 3](https://openid-foundation-japan.github.io/800-63-3-final/4.2-r3) では, 身元情報の検証に必要な属性の収集と記録管理の⽬的を, 属性が身元情報の検証処理を完了させるために必須か否かや,属性を提供しなかった場合の影響を含め, CSP が収集時に申請者に明⽰的に通知するよう求めている.

効果的な通知を⾏うには, ユーザーエクスペリエンスのデザイン標準と研究, そして収集により発⽣する可能性のあるプライバシーリスクの評価を考慮することが重要になる. 属性が収集される理由や, 収集された情報が他のデータソースと組み合わされるかどうかなどに関して申請者が不正確な推測を⾏うことなどを含め, さまざまな要素を考慮すべきである. 効果的な通知は, 申請者が読んだり理解したりしそうもない複雑で法に固執したプライバシーポリシーや一般規約へ導く単なる指針では決してない.

## **処理の制限**

セクション 4.2 の要件 4 は, 身元情報の検証, 認証, 認可, 属性アサーション, これらに関連する不正の軽減以外の目的で属性を処理することから生じるプライバシーリスクと同一基準の予測可能性 (PII と情報システムによるその処理について, 個人と所有者と処理担当者が確実に予測できること) と管理可能性 (変更, 削除, 選択的公開を含め, PII をきめ細かく管理できること) の目標を維持するための措置を講じること, または, 法律や法的手続きを遵守するための措置を講じることを CSP に求めている[NISTIR8062].

CSP には, 身元情報ではないサービスを加入者に提供することを含め, 属性処理に対してさまざまな業務上の目的がある. しかし, 身元情報サービス以外の目的で属性を処理することは, 個人がその追加処理を予測していないか気にしないときにプライバシーリスクを生じさせる. CSP は, 追加処理から生じるプライバシーリスクと同一基準の適切な措置を決めることができる. 例えば, 適用可能な法律, 規制またはポリシーがない場合, 加入者が依頼した身元情報に関係しないサービスを提供するために属性を処理するとき, 通知によって加入者がその処理について確実に推定できることを助ける場合もあろうが (予測可能性), 明確な同意を得る必要はない場合もある. 属性のその他の処理は, 明示的な同意の取得や, 特定の属性の使用や公開を加入者がさらに細かく管理できること (管理可能性) を求める別のプライバシーリスクをもたらす場合もある. 加入者の同意には意味があることが必要である. したがって, CSP が同意を利用するとき, 追加利用を加入者が受け入れることを身元情報サービスを提供する条件にすることはできない.

提案する処理が, 許可された処理や適切なプライバシーリスク軽減措置の範囲外かどうかについて疑問がある場合は, SAOP に意見を求めなければならない.

## **8.4. 救済**

セクション 4.2 の要件 5 は, 身元情報の検証によって⽣じる申請者の苦情や問題に関する効果的な救済⼿段を提供し, その⼿段を申請者が容易に見つけて利用できることを CSP に規定している.

プライバシー保護法は, 記録システムを管理する連邦政府の CSP に対して, 申請者が自分の記録にアクセスし, 正しくない場合は訂正できる⼿順に従うことを求めている. あらゆるプライバシー保護法声明書には, 申請者にアクセスや訂正の方法について指示を与える適⽤可能な SORN への参照を含めるべきである. 連邦政府以外の CSP は, 情報源となる第三者の連絡先を含め, 上記と同等の⼿順を⽤意すべ きである.

CSP は,申請者が⾃⾝の身元情報を確⽴して登録プロセスをオンラインで完結できない場合に, 明確なプロセスを補うための代替方法 (可能であれば, カスタマーサービスセンターでの対⾯⼿続きなど) を提供するべきである.

注意: 身元情報の検証プロセスに失敗する場合は, CSP は申請者に対処法を通知すべきであるが, 登録に失敗した理由の詳細を通知すべきではない (例えば, “手元にある記録の1つにSSN が一致しない” ). そうしないと, 不正な申請者が PII の正確さについてさらに知識を得ることになる.

## **プライバシーリスクの評価**

セクション 4.2 の要件 7 および 10 は, CSP にプライバシーリスクの評価を規定している. CSP は評価の際に以下を考慮すべきである.

1. CSP が取るアクション (追加の検証ステップや記録保持など) が, 侵害や情報への不正アクセスなど申請者にとっての問題となる可能性.
2. 発⽣した問題の影響. CSP は, リスクの許容, 軽減, 共有など, 識別したプライバシーリスクへのあらゆる対応を正当化できるようにすべきである. 申請者の同意は, リスクを共有する形態の⼀例と見なすべきである. したがって申請者が共有されたリスクを評価し許容できると合理的に推測できる場合のみ,申請者の同意を使⽤すべきである.

## **機関特定のプライバシー準拠**

セクション 4.2 の要件 12 は, 連邦機関の CSP に対する特定の準拠義務について述べている. 機関の SAOP をデジタル認証システムの開発初期段階から関与させることは, プライバシーリスクの評価/軽減と準拠義務の助言 (身元情報の検証のための PII 収集が, プライバシー影響評価を実施するための1974 年プライバシー法 [Privacy Act] や 2002年電子政府法 [E-Gov] の要件の対象になるのかどうかなど) の上で非常に重要である. 例えば, 身元情報の検証に関しては, プライバシー法の要件が適⽤され, 身元情報の検証に必要な PII やその他の属性の収集と保持の理由から, プライバシー法において新規または既存の記録システムによる対応が求められる可能性がある.

SAOP は同様に PIA が必要かどうかを決める際に機関を⽀援できる. これらの考慮事項は,身元情報の検証のためだけにプライバシー法において SORN や PIA を開発するための要件として読まれるべきではない. 多くの場合,デジタル認証プロセス全体を網羅する PIA と SORN を計画したり, 機関がオンラインアクセスを確⽴しているプログラムやメリットについて議論するさらに広範で計画的な PIA の⼀部としてデジタル認証プロセスを含めたりすることが, もっとも理にかなっていよう.

デジタル認証には多くの構成要素があることから, SAOP に各要素を認識し理解させることが重要である. 例えば, Data Use Agreements (データ使用合意書) や Computer Matching Agreements (コンピュータ致合意書) などの検証サービスを提供したり利⽤したりする機関にその他のプライバシー要件が適用できる場合がある. SAOP は機関にどの追加要件を適⽤するのか決定する際に⽀援を⾏なうことができる. さらにデジタル認証の個々の要素を完全に理解することで, SAOP は準拠プロセスかその他の⼿段を通してプライバシーリスクを⼊念に評価し, 緩和することができる.

# ユーザビリティの考慮事項

*このセクションは参考情報である.*

このセクションでは, 登録と身元情報の検証に関連するユーザビリティの考慮事項を実装者に周知させることを⽬的とする (認証コードの通常利用と断続的イベントに関するユーザビリティの考慮事項については [SP 800-63B,セクション10 (sp800-63b.html#sec10)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#sec10) を参照).

ISO/IEC 9241-11 はユーザビリティを “特定のユーザーが特定の利⽤状況において, 有効性, 効率性, 満足感を持って特定の⽬的を達成するために製品を利⽤できる程度” と定義している. この定義は, 有効性, 効率性, 満⾜感を達成するために必要な要素として, ユーザー, ⽬標, 利⽤状況に着⽬している. ユーザビリティを達成するには, カギとなるこれらの要素を考慮した全体的なアプローチが必要である.

登録と身元情報の検証におけるユーザビリティの包括的な目標は, ユーザーの負担 (費やす時間やフラストレーションなど) や登録における煩わしさ (完了までのステップ数と追跡すべき情報の量) を最⼩化し, スムーズではっきりした登録プロセスを促進することである. この目標を達成するには, 組織はまずユーザーについて詳しく知る必要がある.

登録プロセスと検証プロセスでは, ユーザーがアクセスするオンラインサービスと所定の CSP とのやりとりのための段階が設定されている. 最初の印象が悪いとその後の操作に影響するため, 組織はプロセス全体を通じて肯定的なユーザーエクスペリエンスを促進する必要がある.

ユーザビリティは断続的なやり方で達成できるものではない. 登録プロセスと検証プロセスについてユーザビリティ評価を⾏うことは⾮常に重要である. 代表的なユーザー, 現実的な目標とタスク, 適切な利⽤状況の下でユーザビリティを評価することが大切である. こうしたプロセスでは, ユーザーが正しいことをするのは簡単にし, 間違ったことをするのは難しくし,そして 間違っても簡単にやり直せるように設計して実装すべきである.

ユーザー視点では, 登録と身元情報検証には, 登録の事前準備, 登録と検証セッション, 登録の完了後アクションという３つの主要なステップがある. これらのステップは単⼀のセッションで済むこともあれば, かなり時間が経ってから発生することもある (数⽇から数週間).

ステップごとの一般的なユーザビリティの考慮事項については, 以下のサブセクションで述べる.

**前提**

このセクションでは, “ユーザー” は “申請者” または “加入者” を意味する.

ユーザーの視点からガイドラインと考慮事項を説明する.

アクセシビリティはユーザビリティとは異なり, この文書の扱う範囲ではない. セクション 508 は情報技術の障壁を排除するために策定され, 情報技術を使った電子的な公開コンテンツに障害者がアクセスできるようにすることを連邦機関に求めている. アクセシビリティのガイドラインについてはセクション 508 の法律と標準を参照.

## **登録と身元情報検証における一般的なユーザーエクスペリエンスの考慮事項**

このサブセクションでは, 登録プロセスの全ステップに渡って適⽤可能なユーザビリティの考慮事項について述べる. 各ステップに固有な考慮事項は, セクション 9.2 ～ 9.4 を参照.

* ユーザーにフラストレーションを感じさせないために, 登録に必要なプロセスを合理化し, 各ステップを可能な限り分かりやすく簡単にする.
* 技術的な⽀援が受けられる場所と方法を明確に伝える. 例えば, オンラインセルフサービス機能へのリンクや, ヘルプデスクサポートのチャット機能や電話番号を提供する. 理想的には, 外部の介⼊なしにユーザー⾃⾝が疑問を解決できるように⼗分な情報を提供するべきである.
* 誰が何の⽬的でデータを収集するのかを明確に説明する. また, データがたどる経路, 特に保管される場所も⽰す.
* 提出するすべての情報が使⽤できることを保証する.

すべてのユーザーに提⽰する資料 (データ収集通知や記⼊用紙) について, 情報デザインの適切な慣例に従う.

資料を一般的に第6学年から第8学年の識字レベルの平易な⾔葉で記述し, 技術的な専⾨⽤語は避ける. 能動態と会話体を使用し, 重要点を論理的に順序⽴て, 混乱を避けるため同義語ではなく同⼀語を繰り返し使⽤し, 読みやすくするために必要に応じて箇条書きや番号などを利⽤する.

フォントのスタイル, サイズ, ⾊, 周囲の背景とのコントラストなどのテキストの読みやすさを考慮する. 最もコントラスト⽐が⾼いのは⽩地に⿊である. ユーザーの視⼒は⼈それぞれであるため, テキストの可読性は重要である. 読みにくいテキストは, ユーザーの誤認や⼊⼒エラーにつながる (記⼊用紙に記入する場合など).

電⼦的な資料にはサンセリフフォント, 紙の資料にはセリフフォントを使⽤する.

可能であれば, 混同しやすい⽂字 (⽂字 “O” と数字 “0” など) を明確に区別できないフォントは避ける. これは特に登録コードにおいて重要である.

テキストがディスプレイに収まる限り, 最⼩フォントサイズを12ポイントにする.

* 代表的なユーザーに対して各ステップのユーザビリティ評価を⾏う. ユーザビリティ評価においては, 現実的な目標とタスクを定め, 適切な利⽤状況を設定する.

## **登録の事前準備**

このセクションでは, 登録セッションでユーザーが困難を感じてフラストレーションを溜めることがないように,登録の事前準備を容易にする効果的なアプローチについて述べる. ユーザーが登録セッションにできる限り準備していることは,登録と身元情報検証のプロセス全体の成功とユーザビリティにとって⾮常に重要である.

そうした準備は, ユーザーが必要な情報 (必要な提出書類など) を適切な時間内に利⽤可能な形式で受け取れる場合にのみ可能になる. これには, 身元情報のどの証拠が必要になるかを正確にユーザーに伝えることが含まれる. ユーザーは IAL についてまたは身元情報の証拠が “適”, “強”, “優” のどれに当てはまるかなどについては⼀切知る必要はないが, 組織は特定のシステムにアクセスするためにどの IAL が必要かを知っている必要がある.

ユーザーが登録プロセスを進めるかどうか, そしてそのセッションに何が必要になるかについて, 情報に基づいた判断を下せるようにするために, ユーザーに以下の項⽬を提供する.

* 各ステップで何が予測されるかなど, プロセス全体についての情報.
* ユーザーが計画を⽴てられるようにするための, 予測される時間枠についての明確な説明.
* ユーザーが登録価値を理解できるようにするための, 身元情報の検証の必要性とメリットに関する説明.
* 登録料⾦が発⽣する場合は, その額と⽀払い⽅法についての情報. さまざまな⽀払い⽅法を用意すれば, ユーザーは好みの⽅法を選ぶことができる.
* 登録セッションの対面が物理的なのか, それともリモートチャネル経由なのか, そしてどちらかが選択できるのかといった情報. 利⽤できるセッションの選択肢に関する情報だけを提供する.
* ユーザーが場所を選べるかどうかに関する情報と, 物理的またはリモートチャネル経由の対⾯セッションに必要な場所情報. ユーザーは身元情報の証拠の紛失や盗難の恐れが高まるとして, 特定の公共空間 (銀⾏に対してスーパーマーケットなど) に証拠を持っていくのをためらう場合があることに注意が必要である.
* リモートセッション に対する技術要件 (インターネットのアクセス要件など) に関する情報.
* 待ち時間を最⼩限にするための, 物理的またはリモートチャネル経由の対⾯セッションの予約. 予約なしでもできる場合は, 予約がないと待ち時間が⻑くなる可能性があることをユーザーに明確に伝える.
* 登録セッションの予約, リマインダー, 予約の変更に関する⽅法について明確な⼿順を伝える.
* 予約についてリマインダーを用意し, ユーザーが好みの方式 (郵便, ボイスメール, Eメール, テキストメッセージなど) を指定できるようにする. ユーザーには, ⽇付, 時刻, 場所, 必要な証拠の説明などの情報が必要である.
* 利⽤可能で必要な身元情報の証拠と属性のどれが任意でどれが必須であるかという情報と, 完全な証拠⼀式を提供しない場合の結果についての情報. ユーザーはそれぞれの証拠の要件 (例えば出⽣証明書には捺印が必要) を含めた特定の組み合わせについて知る必要がある. 必要な証拠を取得することが困難な場合もあるため, これは特に重要である.
* 可能であれば, 必要な証拠の取得を容易にするツールを導入する.
* 未成年や特殊な配慮が必要な⼈々に対する特別な要件をユーザーに知らせる. 例えば, 公証⼈, 法定後⾒⼈, 本⼈の代理権を法的に証明できるその他の個⼈など, 信頼できる身元保証人を利⽤する場合に必要な情報 (詳細はセクション 5.3.4 を参照).
* 記入用紙が必要な場合
* 登録セッションの開始前とその最中に記⼊用紙を提⽰する. プリンターの使用をユーザーに要求しない.
* ユーザーが記入する情報量を最小限にする. 記入事項が多いとユーザーはフラストレーションを感じて間違いを犯しやすくなる. 可能であれば事前に記入された用紙を使用する.

## **登録検証セッション**

ユーザビリティに関して登録セッションに固有の考慮事項は 以下のとおりである.

* ユーザーに登録セッションの⼿順についてセッション開始時に確認する. ユーザーが事前の準備段階以降も手順を覚えていると想定しない. 登録セッションが事前準備の直後に開始されない場合, 検証と登録にかかる一般的な時間をはっきりと確認させることが特に重要である.
* 物理的な対面またはリモートチャネル経由の対⾯の予定を変更できるようにする.
* ユーザーが登録セッションを進めるのに必要な身元情報の証拠を用意していることを確実にするために,利⽤できる必要な証拠のチェックリストを提供する. 妥当な場合は登録コードを含める.
* どの情報が破棄され, 後続セッションがあればどの情報がそのために保管され, どの証拠が今後のセッションを完了させるために必要となるかをユーザーに通知する. 理想的には, ユーザーは身元情報の検証セッションを途中で終了するかどうかを選択できる.
* 先の身元情報検証の経験からユーザーはすでに何らかを想定している可能性があるため,登録セッション の結果に関するユーザーの想定を考慮する (例えば, 運転免許証を対⾯で受け取る, パスポートを郵送で受け取る).
* 登録セッションが完了するとユーザーは認証コードをすぐに受け取るのかどうか, 対面で受け取る場合に予約が必要か, 郵便で受け取るのか, そしてそれがいつになるのかについて明確にする.
* 登録セッションでは, CSP がどのデータを記録に残すかなど, 身元情報の検証時にユーザーに明⽰的に通知するためのいくつかの要件がある (通知要件の詳細についてはセクション 4.2 とセクション 8 を参照). CSP がユーザーに追加属性について同意を求めたり,属性を身元情報の検証, 認証, 認可, 属性アサーション以外の⽬的で利⽤することに同意を求めたりする場合, そういった⾏為がユーザーの予期しないことであったり不快感を与える可能性について CSP はセクション 4.2 の要件 (5) に従う. ユーザーがそれらに対してメリットを感じず, リスクが増えると考える場合, ユーザーは同意することやプロセスを進めることに躊躇する場合がある. 追加要件に関して, ユーザーに明確な通知を⾏う.
* ユーザビリティの視点からは, KBV は⾮常に問題が多いため使用を避ける. ⼈間の記憶⼒には限界があるため, KBV はエラーを引き起こしやすくユーザーはフラストレーションを感じやすい. KBV を使用する場合は, ユーザビリティに関して以下を考慮する.
* ユーザーが正しく回答できるよう, KBV の質問には関連性と文脈を持たせるべきである.
* KBV の質問は明確な⾔い回しにする. あいまいな表現はユーザーを混乱させる. 例えば, 社会保障給付金口座の残⾼について質問する場合, 給付金の変動を考慮し期間を明確に指定する.
* KBV の質問をする前に, ユーザーに以下を知らせる
* 許容される試⾏回数と残りの試⾏回数.
* KBV の質問が次の試⾏で変化すること.
* KBV セッション中, タイムアウトになる前にタイムアウトが近いことを警告する.

登録コードを発⾏する場合.

* 登録コードが送られることを, その到着予想時期, コードの有効期限, 送付⽅法 (郵送, SMS, 固定電話, Eメールなど) とともに事前にユーザーに通知する.
* 登録コードを送付するとき, その使用⼿順と有効期限の説明を添える. 特にセクション 4.4.1.6 にあるように, 有効期限が短い場合にこの情報は特に重要である.
* QR コードなどの機械可読光学ラベルを発⾏する場合 (セクション 4.6. を参照), スキャン方法についての情報も添える (利⽤できる QR コードアプリなど).
* 登録コードの期限が切れたり使⽤前に紛失したりすると, 登録ロセスを再び繰り返す必要があることをユーザーに知らせる.
* すべてのユーザーがこのレベルの技術を使えるわけではないため, 代替オプションをユーザーに提供する.ユーザーはこのアプローチに必要な技術を持っていない場合がある.
* 登録セッションの終了時.
* 登録が完了した場合は, ユーザーに完了した登録に関する確認と次のステップに関する情報を送る (認証コードを受け取る時期と場所, 郵送の場合の到着時など).
* 登録が途中で終了した (ユーザーが完全な身元情報の証拠セットを持っていなかった, ユーザーがプロセスを中断した, セッションがタイムアウトしたなど) 場合は, ユーザーに以下を伝える.
* どの情報が破棄されるか.
* 後続セッションがあれば, そのためにどの情報が保持されるか.
* 情報はどれくらいの期間が保持されるか.
* 今後のセッションでどの身元情報の証拠を提示する必要があるか.
* 登録が失敗した場合は, 代替の登録セッションについて明確な説明を提供する. 例えば,リモート検証を完了できないユーザーに物理的な対⾯による検証を提供する.
* ユーザーが登録セッション中に認証コードを受け取る場合は, 認証コードの使用と保管に関する情報を伝える. 例えば, 使用⼿順 (特に初回の使用や初期化に特別な要件がある場合), 有効期限, 保護⽅法, 紛失や盗難の際の対応⽅法を含めることができる.

物理的な対⾯とリモートチャネル経由の登録セッションによる対⾯のどちらにおいても, ユーザビリティの補足的な考慮事項が適⽤される.

* 登録セッション開始時に, 担当者や係員は⾃⾝の役割をユーザーに説明する (セッションを通してユーザーを手助けするのか, 見守るだけで必要な時だけ介入するのかなど).
* 登録セッション開始時に, セッション中に席を離れてはならないことと, 行動はセッションを通して目で確認されなければならないことをユーザーに伝える.
* 登録セッション中に生体認証情報を収集する場合は, その収集プロセスを完了する方法についてユーザーに明確に説明する. この方法はプロセス直前に説明することが最も望ましい. その場にいる担当者が修正できる⼝頭による説明が最も効果的である (生体認証センサーがどこにあるか, いつ開始されるか, どのようにセンサーを使用すべきか, いつ収集が完了するかなど).
* 身元情報のリモート検証はオンラインで⾏われるため, ⼀般的な Web 上のユーザビリティ原則に従う. 以下に例を挙げる.
* 登録プロセスを通してユーザーを手助けできるようなユーザーインタフェースを設計する.
* ユーザーが記憶しなければならないことを減らす.
* インタフェースに⼀貫性を持たせる.
* 順次ステップには明確にラベルをつける.
* 開始ポイントを明確にする.
* 多様なプラットフォームやデバイスサイズをサポートするように設計する.
* ナビゲーションに⼀貫性を持たせ, 見つけやすくて辿りやすいものにする.

## **登録後**

登録後とは, 登録直後で認証コードの通常利⽤前のステップを指す (認証コードの通常利⽤と断続的イベントに関するユーザビリティの考慮事項については[, SP800-63B (sp800-63b.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html) Section 10.1-10.3 を参照). 先に述べたように, ユーザーは登録セッション終了時に認証コードの配送 (または受け取り) ⼿段に関して知らされている.

登録後に関するユーザビリティの考慮事項には以下がある.

* 認証コードが到着するまでの待ち時間を最短化する. 待ち時間が短いほど, ユーザーは情報システムとサービスに早くアクセスできる.
* 認証コードを受け取るために物理的な場所に出向く必要があるかどうかを知らせる. 先に述べた予約とリマインダーに関するユーザビリティの考慮事項はここでも適⽤される.
* 認証コードと共にその使用と管理に関する情報も提供する. 認証コードの使用⼿順 (特に初回の使用や初期化に特別な要件がある場合), 有効期限, 保護⽅法, 紛失や盗難の際の対応⽅法などを含めることができる.

# 参考文献

*このセクションは参考情報である.*

## **一般**

[A-130] OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016, available at: [https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf%20) .

[COPPA] *Children’s Online Privacy Protection Act of 1998 (“COPPA”)*, 15 U.S.C. 6501-6505, 16 CFR Part 312, available at: https://www.law.cornell.edu/uscode/text/15/chapter-91.

[EO 9397] Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, November 22, 1943, available at: https://www.ssa.gov/foia/html/EO9397.htm.

[DMF] National Technical Information Service, *Social Security Death Master File*, available at: https://www.ssdmf.com/Library/InfoManage/Guide.asp?FolderID=1.

[E-Gov] *E-Government Act of 2002* (includes FISMA) (P.L. 107-347), December 2002, available at: http://www.gpo.gov/fdsys/pkg/PLAW- 107publ347/pdf/PLAW-107publ347.pdf .

[FBCACP] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.30, October 5, 2016, available at: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA\_CP.pdf.

[FBCASUP] *FBCA Supplementary Antecedent, In-Person Definition*, July 16, 2009.

[FEDRAMP] General Services Administration, *Federal Risk and Authorization Management Program*, available at: https://www.fedramp.gov/.

[GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing *and verification of an individual*, November 3, 2014, available at: https://www.gov.uk/government/publications/Identity-proofing-and-verification-of-an-individual.

[M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html.

[M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, available at: https://georgewbush- whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf

[Privacy Act] *Privacy Act of 1974* (P.L. 93-579), December 1974, available at: https://www.justice.gov/opcl/privacy-act-1974.

[Red Flags Rule] 15 U.S.C. 1681m(e)(4), Pub. L. 111-319, 124 Stat. 3457, *Fair and Accurate Credit Transaction Act of 2003*, December 18, 2010, available at: https://www.ftc.gov/sites/default/files/documents/federal\_register\_notices/identity-theft-red-flags-and-address-discrepancies-under-Fair- and-accurate-credit-transactions-act/071109redflags.pdf.

[Section 508] Section 508 Law and Related Laws and Policies (January 30, 2017), available at: https://www.section508.gov/content/learn/laws-and- policies.

## **標準**

[Canada] Government of Canada, *Guideline on Identity Assurance*, available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML.

[ISO 9241-11] International Standards Organization, ISO/IEC 9241-11 *Ergonomic requirements for office work with visual display terminals (VDTs)*

*— Part 11: Guidance on usability*[, March 1998, available at: https://www.iso.org/standard/16883.html](https://www.iso.org/standard/16883.html) .

## **NIST 特別出版物**

NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html. The following publications may be of particular interest to those implementing systems of applications requiring e-authentication.

[SP 800-53] NIST Special Publication 800-53 Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), https://doi.org/10.6028/NIST.SP.800-53r4.

[SP 800-63-3] NIST Special Publication 800-63-3, *Digital* *Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

[SP 800-63B] NIST Special Publication 800-63B, *Digital* *Identity Guidelines: Authentication and Lifecycle Management*, June 2017, <https://doi.org/10.6028/NIST.SP.800-63b.>

[SP 800-63C] NIST Special Publication 800-63C, *Digital* *Identity Guidelines: Assertions and Federation*, June 2017, <https://doi.org/10.6028/NIST.SP.800-63c>.

[SP 800-157] NIST Special Publication 800-157, *Guidelines for Derived Personal* *Identity Verificatio (PIV) Credentials*, December 2014, <http://dx.doi.org/10.6028/NIST.SP.800-157.>

[Privacy Policy (http://www.nist.gov/public\_affairs/privacy.cfm#privpolicy)](file:///C:\Users\shiokawa\AppData\Local\Temp\B2Temp\Attach\Privacy%20Policy%20(http:\www.nist.gov\public_affairs\privacy.cfm#privpolicy) ) | [Security Notice (http://www.nist.gov/public\_affairs/privacy.cfm#secnot)](file:///C:\Users\shiokawa\AppData\Local\Temp\B2Temp\Attach\Security%20Notice%20(http:\www.nist.gov\public_affairs\privacy.cfm#secnot) ) | [Accessibility Statement (http://www](http://www.nist.gov/public_affairs/privacy.cfm#accesstate)[.nist.gov/public\_affairs/privacy.cfm#accesstate) | Send feedback (https://github.com/openid-foundation- japan/800-63-3-final/issues/)](https://github.com/openid-foundation-japan/800-63-3-final/issues/) [ (/800-63-3-final/comment\_help.html)](https://openid-foundation-japan.github.io/800-63-3-final/comment_help.html)