Wed, 18 Oct 2017 06:55:32 +0000

**NIST 特別出版物 800-63**

**改訂版3 デジタル ID ガイドライン****（翻訳版）**



Paul A. Grassi

Michael E. Garcia

James L. Fenton

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.800-63-3





**NIST SP 800-63-3**

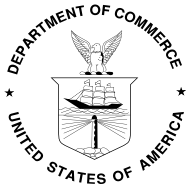
**デジタル ID ガイドライン**

|  |  |
| --- | --- |
| Paul A. Grassi  Michael E. Garcia  *Applied Cybersecurity Division*  *Information Technology Laboratory* | James L. Fenton  *Altmode Networks*  *Los Altos, CA* |
|  | **翻訳者:** Nov Matake  *YAuth.jp LLC* |

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.800-63-3

2017年 6 月



米国商務省

*Wilbur L. Ross, Jr., 長官*

国立標準技術研究所

*Kent Rochford, 代理所長, Commerce for Standards and Technology副長官*

## **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. 800-63-3, 73 pages (June 2017)

CODEN: NSPUE2

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.800-63-3>

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, 概念と方法論も含め, 付属文書が完成する前でも連邦機関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が有効である. 計画目的と移行目的に対しては, 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奨励される. 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.

**この出版物に関する意見の提出先**

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

すべての意見は, 情報公開法 (FOIA) の下で公表される.

## **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提供することにより, 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 ID（身元情報）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. こうしたガイドラインは, オープンなネットワークを介して政府の IT システムと対話するユーザー（従業員, 契約者, 民間人など）の身元情報の検証と認証をカバーする. こうしたガイドラインは, 身元情報の検証, 登録, 認証コード, 管理プロセス, 認証プロトコル, 連携, 関連するアサーションのそれぞれの分野の技術要件を明確にする. 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; 認証保証; 認証コード; アサーション; 認証情報サービスプロバイダ; デジタル認証; デジタル認証情報; 身元情報の検証; 連携; パスワード; PKI

## **謝辞**

SP 800-63 のすべての巻で芸術的な図表を作成してくれた Kaitlin Boeckl と, 貴重な意見を寄せてくれた 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 を初めとする多くの方々に感謝する.

これに加え, 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.

## **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.

# エグゼクティブサマリー

*このセクションは参考情報である.*

デジタル身元情報 (ID) とはある主体のオンライン上のペルソナであり, 単⼀の定義が国際的に広く議論されている. ペルソナという用語は, 主体がオンライン上で⾃⾝を多様に表現できるときに適切である. ある個⼈は, Eメール用にデジタル ID を持ち, パーソナルファイナンス⽤に別のデジタル ID を持つ場合がある. ある個⼈のラップトップは, 誰かの⾳楽ストリーミングサーバーにもなれば, 複雑な遺伝⼦計算を⾏う分散コンピュータネットワーク内の１つのワーカーボットにもなる. 利用状況を考えずしてすべてを満たす単⼀の定義に到達することは困難である.

法律上の身元情報としてのデジタル ID は, 社会と経済の領域で使用するデジタル ID の定義と機能をさらに複雑にする. デジタル ID は厄介である. ある⼈が⾃⾝の主張する⼈物であるということを - 特にリモートでデジタルサービスを通して - 証明する過程は, 攻撃者が誰かになりすます機会に満ちている. 『New Yorker』誌に載ったPeter Steinerの風刺漫画に描かれているとおり, “インターネットでは誰も君が⽝だと気づかない” のである. このガイドラインはオンライン固有の脆弱性に対する対策を提供する. そして, 低リスクのデジタルサービスにアクセスするときは “犬である” ことに不都合はないが, ⾼リスクのサービスでは, サービスにアクセスするデジタル ID が実際の主体の正当な代理であることを示す信頼レベルを必要とすることを認めそれを推奨している.

これらのガイドラインでは, デジタル ID は, オンライント上のトランザクションに関与する主体を⼀意に表現する. デジタル ID は, デジタルサービスの使用状況では常に⼀意となるが, すべての状況で主体を⼀意に識別する必要は必ずしもない. ⾔い換えれば, デジタルサービスへのアクセスは, 主体の実際の身元が明らかになることを意味しなくてもよい.

身元情報の検証は, 主体が主張する本人であることを確立する. デジタル認証は, デジタルサービスにアクセスしようとしている主体が, 主体のデジタル ID に関連付けられた１つ以上の正当な認証コードを管理していることを証明する. 繰り返し利用されるサービスにおいて, 認証に成功するということは, いまサービスにアクセスしている主体は以前にアクセスしていた主体と同⼀であることが適切なリスクに基づいて保証されたということである. デジタル ID のプロセスは, オープンなネットワークを介した個⼈の検証を伴い, 政府のデジタルサービスにアクセスする際はオープンなネットワークを介して個別の主体の認証を必ず伴うことから, 技術的課題をもたらす. デジタル ID を確⽴し使用するためのプロセスと技術は, なりすましやその他の攻撃のさまざまな機会と隣り合わせである.

これらの技術的なガイドラインは, NIST SP 800-63-2 に取って代わる. 各政府機関はこれらのガイドラインを⾃⾝のデジタルサービスのリスク評価と導入の⼀部として利⽤する. こうしたガイドラインは, 身元情報の保証を個別要素ごとに分離し, 認証の誤りがもたらす悪影響を軽減する方法を提供する. 連携していない (非連携) システムでは, 政府機関は*身元情報保証レベル (IAL)* と*認証コード保証レベル (AAL)* という2つの要素を⽤いる. 連携したシステムでは, 3番目の要素である*連携保証レベル (FAL)* を選択する.

これらのガイドラインでは, 保証レベル (LOA) という概念を実装固有の要件を駆使する単一の序数的指標として放棄する. 各機関は,適切な業務とプライバシーに関するリスク管理と役目の必要性を組み合せ, 個別の選択肢として IAL, AAL, FAL を選択する. 多くのシステムで IAL, AAL, FAL がそれぞれ同じレベル値になるとしてもそれは要件ではなく, 各機関はいかなるシステムでもこの値が同じであると想定すべきではない.

これらのガイドラインで詳しく説明している身元情報保証の構成要素は以下のとおりである.

* **IAL** は, 身元情報の検証プロセスに関係する.
* **AAL**は, 認証プロセスに関係する.
* **FAL** は, 連携した環境において認証情報と (妥当な場合は) 属性情報を証明書利用者 (RP) に伝達するのに使用されるアサーションの強度に関係する.

これらのカテゴリを分離することで, 各機関は身元情報に関するソリューションを柔軟に選択し, いかなる保証レベルにおいても身元識別情報システムの基本要素としてプライバシー強化⼿法を含める能力を⾼める. 例えば, これらのガイドラインでは, 強固なマルチファクタ認証コードを⽤いる場合でさえ, 匿名によるインタラクションを可能にするシナリオをサポートする. また, 連携した身元情報プロバイダ (IdP) に対して, データ問合わせに一連のオプションのサポートを要求することにより, 個人識別情報の拡散を最小限に抑制することを推奨している. 例えば, ⽣年⽉⽇全体ではなく, ある年齢より上かどうかを問い合わせる. 各機関の多くのユースケースでは, 個⼈の完全な識別が求められるが, これらのガイドラインでは, 完全な識別が必要な場合でも収集する個人情報をできる限り制限し, 可能な限り政府のデジタルサービスへの匿名アクセスを推奨する.

今⽇の環境では, 組織における身元情報ソリューションは単独のシステムやベンダーが全機能を提供するモノリシックである必要はない. 身元情報サービスのマーケットは細分化され, 組織や機関は標準ベースで組み込み可能な身元情報ソリューションを⽬的に合わせて採⽤することができる. こうしたことから, SP 800-63 は⼀連の文書に分割されている. 以降この文書⼀式を “ガイドライン” と呼び, 個々の文書を “巻” と呼ぶ. RP は SP 800-63 を使用することが要求される. それぞれの巻は, 機関が必要とする要素のサービスに応じて, 個別に⽤いてもよいし⼀体的に⽤いてもよい.

各巻はさまざまな標準化団体で規範または要件ベースとして国際的に認められた⽤語を採用している. ガイドラインで規範的表現を⽤いるときには, 分かりやすくするために⼤⽂字表記にしてある. 例えば, SHALL は必須要件を⽰し, SHOULD は推奨されるが必須ではない手法, 技術またはプロセスを⽰す. これらの⽤語の詳しい定義は, 各文書冒頭の「表記法」に説明してある.

ガイドラインは電子商取引などの連邦政府以外のアプリケーションに対して標準技術の開発・利⽤に⾔及することもあるが, 制限や制約を課すものではない.

ガイドラインは以下のような構成となっている.

**SP 800-63 デジタル ID のガイドライン** (この文書)

デジタルシステムで認証コード, 認証情報, アサーションを共に使用する⼀般的な身元識別情報フレームワークの概要と, 保証レベルを選択するリスクベースのプロセスについて述べる. *SP 800-63 には規範と参考情報の両方が含まれる.*

[**SP 800-63A 登録と身元情報の検証**](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.ja.html)

NIST SP 800-63-A では, 身元識別情報システムで申請者がどのように⾃⾝の身元情報を証明し,正当な加入者として登録されるのかについて説明する. この巻では, リモートと対⾯の両シナリオにおいて, リスク軽減の３種類のレベルで申請者が身元を証明し登録できるための要件をまとめる. *SP 800-63A には規範と参考情報の両方が含まれる.*

SP 800-63A は所定の IAL を満たす要件を決定する. 3種類の IAL は, 各機関のリスクプロファイルと, 攻撃者による不正な身元情報の主張が成功した場合の被害想定に基づいて, 各機関が選択できる選択肢を⽰す. 各 IAL は以下のとおりである.

**IAL1**: 申請者を特定の現実の身元情報と関連付ける必要はない. 認証プロセスに関連して提供されるいかなる属性も自己表明であるか, 自己表明であるはずである. (認証情報サービスプロバイダ (CSP) が RP に対して明示する属性も含む)

**IAL2**: 主張された身元情報が現実に存在することを裏付け, 申請者がその実在する身元情報に適切に関連付けられていることを検証できる証拠が必要になる. IAL2 ではリモートか対⾯での身元情報の検証のどちらかが必要となる. CSPは検証した属性を含む匿名の身元情報を用いて RP に属性を明示できる.

**IAL3**: 対⾯での身元情報の検証が要求される. 身元を識別する属性は, 訓練を受けた上で認可された CSP の担当者によって検証される必要がある. IAL2 と同様に, CSP は検証した属性を含む匿名の身元情報を用いて RP に属性を明示できる.

[**SP 800-63B 認証とライフサイクル管理**(sp800-63b.ja.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html)

繰り返し訪問されるサービスでは, 認証に成功することは現在サービスにアクセスしている主体は以前にアクセスしていた主体と同⼀であることが適切なリスクに基づいて保証されたことを示す. この信頼の堅牢性は AAL カテゴリによって記述される. NIST SP 800-63B では, １つまたはセットになったデジタルサービスにアクセスする個⼈が CSP に対してセキュアに認証できるプロセスについて説明する.*SP 800-63B には規範と参考情報の両方が含まれる.*

3種類の AAL は, 攻撃者が認証コードを⼿に入れて政府機関のシステムにアクセスした場合の被害想定と各機関のリスクプロファイルに基づいて, 各機関が選択できる一連の選択肢を定義する. 各 AAL は以下のとおりである.

**AAL1**: AAL1 では, 認証要求者が加入者のアカウントに結び付けられた認証コードを管理していることが, ある程度の確信度で保証される. AAL1 では, 利用可能な幅広い認証手段による単一ファクタかマルチファクタの認証コードが求められる. 認証を成功させるには, セキュアな認証プロトコルによって認証要求者が認証コードを保持し管理していることを証明する必要がある.

**AAL2**: AAL2 では, 認証要求者が加入者のアカウントに結び付けられた認証コードを管理していることが, ⾼い確信度で保証される. セキュアな認証プロトコルによって, 2つの異なる認証ファクタを所有し管理している証明が必要になる. AAL2 以上では, 承認済みの暗号化技術が要求される.

**AAL3**: AAL3 では, 認証要求者が加入者のアカウントに結び付けられた認証コードを管理していることが, ⾮常に⾼い確信度で保証される. AAL3の認証 は, 暗号プロトコルによる鍵の所有の証明に基づく. AAL3 の認証では, ハードウェアベースの認証コードと, 検証者に偽装耐性を提供する認証コードを使用しなければならない(SHALL).同⼀デバイスがこれらの要件の両方を満たしてもよい (MAY). AAL3 で認証するには, 認証要求者はセキュアな認証プロトコルによって2つの異なる認証ファクタを所有し管理していることを証明しなければならない(SHALL). 承認済みの暗号化技術が要求される.

[**SP 800-63C 連携とアサーション** (sp800-63c.ja.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.ja.html)

NIST SP 800-63C では,認証プロセスの結果と関連身元情報を機関のアプリケーションに伝送するために, 連携した身元情報アーキテクチャを使用する際の要件について説明する. さらに, 認証された正当な主体についての情報を共有する際のプライバシー強化⼿法と, 主体がデジタルサービスに対して匿名を維持できる強固なマルチファクタ認証 (MFA) の方法について述べる. *SP 800-63C には規範と参考情報の両方が含まれる.*

3種類の FAL は, 各機関によるリスクプロファイルと, 連携したトランザクションを攻撃者がコントロールする場合の被害想定に基づいて, 各機関が選択できる選択肢を⽰す. 各 FAL は以下のとおりである.

**FAL1**: 加入者は RP が ベアラアサーションを受け取ることを許容できる. アサーションは承認済みの暗号化技術を⽤いて IdP によって署名される.

**FAL2**: 上記に加え, アサーションは RP 以外が復号できないような承認済みの暗号化技術によって暗号化されなければならない.

**FAL3**: 加入者はアサーションの成果物自体に加え, アサーションで参照される暗号鍵の所有証明を提⽰する必要がある. アサーションは承認済みの暗号化技術を⽤いて IdP によって署名され, RP に対して暗号化される.

ガイドラインは, 各機関が構築または調達できる幅広い身元情報サービスのアーキテクチャについて関知しておらず, 機関が選択するアプローチとは無関係に適⽤できることを意図している. しかしながら,可能な場合は各機関が連携を⽤いることが推奨され, これにより, 連携したアーキテクチャを採⽤する際に IAL, AAL, FAL をうまく組み合わせる能力が単純化される. さらに, 連携は, 連邦政府の構成員が政府の貴重なデジタルサービスにアクセスする際のプライバシーを強化する能力の基盤となる。

**Table of Contents**

**Executive Summary iv**

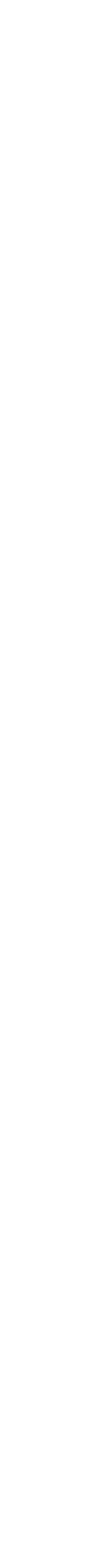
1. **Purpose 1**
2. **Introduction 2**
   1. Applicability 4
   2. Considerations, Other Requirements, and Flexibilities 5
   3. A Few Limitations 5
   4. How to 米国e this Suite of SPs 5
   5. Change History 6

2.5.1 SP 800-63-1 6

2.5.2 SP 800-63-2 6

2.5.3 SP 800-63-3 6

1. **Definitions and Abbreviations 8**
2. **デジタル 身元情報 Model 9**
   1. Overview 9
   2. Enrollment and 身元情報の検証 12
   3. 認証 and Lifecycle Management 12
      1. 認証コードs 12
      2. 認証情報s 14
      3. 認証 Process 14
   4. 連携 and アサーションs 14
      1. アサーションs 15
      2. Relying Parties 16
3. **デジタル 身元情報 Risk Management 17**
   1. Overview 17
   2. 保証レベルs 18
   3. Risk and Impacts 19
      1. Business Process vs. オンライン トランザクション 20
      2. Impacts per Category 21
   4. Risk Acceptance and Compensating Controls 22
   5. デジタル 身元情報 Acceptance 表明 23
   6. Migrating Identities 23



This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-63-3

1. **Selecting 保証レベルs 25**
   1. Selecting IAL 26
   2. Selecting AAL 29
   3. Selecting FAL 31
   4. Combining *x*ALs 33
2. **連携 Considerations 35**
3. **参考文献 36**
   1. General 参考文献 36
   2. Standards 37
   3. NIST Special Publications 37
   4. 連邦情報処理規格s 37

**List of Appendices**

**Appendix A— Definitions and Abbreviations 39**

* 1. Definitions 39
  2. Abbreviations 57

**List of Figures**

Figure 4-1 デジタル 身元情報 Model 10

Figure 6-1 Selecting IAL 27

Figure 6-2 Selecting AAL 30

Figure 6-3 Selecting FAL 32

**List of Tables**

Table 2-1 規範 and 参考情報 Sections of SP 800-63-3 4

Table 5-1 身元情報 保証レベルs 18

Table 5-2 認証コード 保証レベルs 19

Table 5-3 連携 保証レベルs 19

Table 6-1 Maximum Potential Impacts for Each 保証レベル 25

Table 6-2 Acceptable Combinations of IAL and AAL 34

**正誤表**

この表は, 特別出版物 800-63-3 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 | 用語 ‘cryptographic’ を AAL3 の説明から削除 | エグゼクティブサマリー |
|  | 編集上 | リスク管理フレームワークへの参照を更新 | セクション5 |
|  | 編集上 | xAL フローチャートの用語を訂正 | 図 6-1, 6-2, 6-3 |
|  | 編集上 | NISTIR 8062 を参照として追加 | セクション8.1 |
|  | 編集上 | 分離可能性, 管理可能性, プロセッシング, 予測可能性の定義を追加 | 付録 A |

# 目的

*このセクションは参考情報である.*

この推奨文書と付属文書である特別出版物 [(SP) 800-63A (sp800-63a.ja.html), SP 800-63B (sp800-63b.ja.html), SP 800-63C (sp800-63c.ja.html) は,デジタル認証の実装のための技術的ガイドラインを政府機関に提供する.](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.ja.html)

# はじめに

*このセクションは参考情報である.*

デジタル ID はオンライントランザクションに関与する主体を⼀意に表現する. デジタル ID は常にデジタルサービスのコンテキスト内で一意であるが, 必ずしもすべてのコンテキストで⼀意に主体を識別する必要はない. ⾔い換えれば,デジタルサービスにアクセスすることは, 主体の実際の身元情報が分かることを意味しなくてもよい. 身元情報の検証は, 主体が本人であるとする主張の正しさを確⽴する. デジタル認証は, デジタル ID を主張するために使用される1つ以上の認証コードの有効性を確定するプロセスである. 認証は, デジタルサービスにアクセスを試みる主体が認証に使用される技術の管理下にあることを確立する. 認証に成功すると, サービスにアクセスしている主体が以前にこのサービスにアクセスした主体と同⼀であることが, 適度なリスクベースで保証される. このプロセスにはオープンなネットワークを介した個人の検証がしばしば必要になる. そして, 主としてデジタル政府サービスにアクセスするためにはオープンなネットワークを介した個別の主体の認証が必要になるため, デジタル ID には技術的な課題を伴い, 本人であると不正に主張するなりすましやその他の攻撃のためのさまざまな機会がある.

この推奨文書は,ネットワークを介した連邦システムに対して主体をデジタル認証するための技術的ガイドラインを提供する. また, 認証情報サービスプロバイダ (CSP), 検証者, 証明書利用者 (RP) 向けのガイドラインも提供する.

これらのガイドラインは, 適切なデジタル ID サービスを選択するためのリスク管理プロセスと, 身元情報, 認証コード, 連携のリスクに基づいたそれぞれの保証レベルの実装について詳しく説明する. ガイドラインのリスク評価ガイダンスは, *NIST リスク管理フレームワーク*[NIST RMF] とその構成要素である特別出版物を補完する. このガイドラインは各機関にさらなるリスク管理プロセスを規定するものではない. ガイドラインに含まれる要件は, すべての関連する RMF ライフサイクルフェーズを実⾏する際のデジタル ID のリスクに関する具体的なガイダンスを提供する.

デジタル認証は, 個⼈情報への不正アクセスのリスクを軽減してプライバシーの保護を支える. それと同時に, 身元情報の検証, 認証, 認可, 連携は個人情報の処理を伴うため, こうした機能はプライバシーに対してリスクを生み出すことになる. したがって, ガイドラインには, 潜在的に関連するプライバシーのリスクを軽減する助けとなるプライバシー要件と考慮事項が含まれる.

ガイドラインでは, 身元情報保証を個別の要素に分割することにより, 認証の誤りが引き起こす悪影響を軽減する. 連携していない (非連携) システムでは, 政府機関は*身元情報保証レベル (IAL)* と *認証コード保証レベル (AAL)* という2つの要素を⽤いる. 連携した (連携) システムには, 3番目の要素である*連携保証レベル (FAL)* が含まれる. セクション 5 のデジタル ID のリスク管理では, リスク評価プロセスの詳細について説明する. セクション 6 の保証レベルの選択では,政府機関のリスクに基づく適切な IAL, AAL, FAL の組合せの選択をサポートするために, リスク評価の結果と補足的な使用状況を組み合わせる.

ガイドラインは, 実装固有の要件を駆使する単一の序数的指標という文脈における複合の保証レベル (LOA) を考慮しておらず, それを推奨もしていない. 各機関は, ビジネス, セキュリティ, プライバシーのための適切なリスク管理をそれぞれの業務のニーズと組み合わせることにより, 個別の選択肢として IAL, AAL, FAL を選択する. 特にこの文書は, 各機関が以前に使用し, OMB M-04-04 に説明された４種類の LOA モデルを認めず, その代わりに各機関が実施している機能に応じて個別にレベルを選択するよう求めている. 多くのシステムで IAL, AAL, FAL がそれぞれ同じレベル値になるとしても, それは要件ではないため, 各機関はいかなるシステムやアプリケーションでもその値が同じであると想定すべきでもない.

これらのガイドラインで詳しく扱う身元情報保証の構成要素は以下のとおりである.

* **IAL** は, 身元情報の検証プロセスに関係する.
* **AAL**は, 認証プロセスに関係する.
* **FAL** は, 連携した環境において認証情報と (妥当な場合は) 属性情報を証明書利用者 (RP) に伝達するのに使用されるアサーションプロトコルに関係する.

SP 800-63 は以下のような⼀連の巻から構成される.

SP 800-63 *デジタル ID ガイドライン*: SP 800-63 では, リスク評価の⽅法論と, デジタルシステムで認証コード, 認証情報, アサーションをいっしょに利⽤する⼀般的な身元情報フレームワークの概要を説明する, そして保証レベルを選択するリスクベースのプロセスについて述べる. *SP 800-63 には規範と参考情報の両方が含まれる.*

SP 800-63A *登録と身元情報の検証*: NIST SP 800-63-A では, 身元識別情報システムで申請者がどのように⾃⾝の身元情報を証明して正当な加入者として登録されるのかについて説明する. そして, リモートと対⾯の両シナリオにおいて, リスク軽減の３種類のレベルで申請者が身元を証明して登録できるための要件をまとめる.

*SP 800-63A には規範と参考情報の両方が含まれる.*

SP 800-63B *認証とライフサイクル管理*: NIST SP 800-63B では, 個人がデジタルサービスまたはそのセットにアクセスするために CSP にセキュアに認証される方法を扱う. そして, 認証コードを身元情報に結び付けるプロセスについても説明する. *SP 800-63B には規範と参考情報の両方が含まれる.*

SP 800-63C *連携とアサーション*: NIST SP 800-63C では, 認証プロセスの結果と関連身元情報を機関のアプリケーションに伝送するために, 連携した身元情報アーキテクチャを使用する際の要件について説明する. さらに, 認証された正当な主体についての情報を共有する際のプライバシー強化⼿法と, 主体がデジタルサービスに対して匿名を維持できる強固なマルチファクタ認証 (MFA) の方法について述べる. *SP 800-63C には規範と参考情報の両方が含まれる.*

NIST では, ガイドラインの個々の巻が同時に改訂されないことを想定している. いかなる場合でも, それぞれの巻のもっとも新しい改訂版を使用すべきである (例えば, ある時点において SP 800-63A-1 と SP 800-63B-2 がそれぞれ最新の改訂版であれば, 改訂番号が一致しなくてもいっしょに使用すべきである). 適合性の矛盾によるリスクを最小限に抑えるため, 基本文献 (つまりSP 800- 63-3 ではなく SP 800-63) の参照は, 常にこの文書の最新バージョンを参照することを意味する.

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.

|  |  |
| --- | --- |
|  | **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. デジタル ID モデル | 参考情報 |
| 5. デジタル ID のリスク管理 | 規範 |
| 6. 保証レベルの選択 | 規範 |
| 7. 連携の考慮事項 | 参考情報 |
| 8. 参考文献 | 参考情報 |

## **適用性**

すべてのデジタルサービスが認証や身元情報の検証を必要とするわけではないが, このガイダンスはサービス対象 （市⺠, ビジネスパートナー, 政府機関など）とは無関係にデジタル身元情報や認証が必要なすべてのトランザクションに適⽤される.

このガイダンスが扱うトランザクションには, 44 U.S.C. § 3542(b)(2) で定義された国家安全保障システムに関連したトランザクションは含まれない. デジタルプロセスにさまざまな保証レベルが必要な民間組織や州政府, 地方自治体, 部族自治体は, 必要に応じてこうした標準の仕様を検討することができる.

これらのガイドラインは, 非政府関係者とやりとりする機関サービスを主に中心としており, 非政府関係者とは利便性を利用する市⺠や情報を共有する共同スペースを利用する民間部門のパートナーである. しかし, 機関の従業員や契約業者がアクセスする内部機関システムにも適⽤される. こうしたユーザーには, 主として個人検証 (Personal Identity Verification, PIV) カードや派⽣ PIV という, 政府が発⾏した正式な認証情報を保持していることが要求される. したがって [SP 800-63A (sp800-63a.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.html) と [SP 800-63B (sp800-63b.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html) は, FIPS 201 とそれに関連する特別出版物の要件と機関固有の指⽰に次ぐ⼆時的存在となる. しかしながら [SP 800-63C (sp800-63c.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.html) とリスクに基づく適切な FAL の選択は, 内部ユーザーの持つ認証情報タイプに関係なく適⽤される. 各機関は FAL を選択することにより, システムリスクに応じてアプリケーションを PIV で可能にする方法についてガイダンスに従って柔軟に対応できる.

## **考慮事項, その他の要件, 柔軟性**

各機関はここに指定されていない他のリスク軽減策と補完的管理策を採⽤してもよい. ただし採⽤するいかなる軽減策と補完的管理策も, 選択した保証レベルが意図したセキュリティとプライバシー保護を低下させないことを保証する必要がある. 各機関はデジタルサービスの機能を分割し, 機密性の低い機能をより低い認証保証レベルと身元情報保証レベルの下で提供することを検討してもよい.

各機関は, ⾃⾝のリスク分析を元に, 特定の利用状況では追加の措置を講じることが妥当であると判断してもよい. 特に, プライバシー要件と法的リスクにより, 追加の認証措置やその他のプロセス保護が適切となる場合がある. デジタル認証プロセスやデジタル認証システムを構築する際には, 各機関は *2002年の電子政府法のプライバシー規定に関する行政管理予算局*ガイダンス *(OMB Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002* [M-03-22] を参照すべきである. また, 特に 1) 検証の法的基準への準拠, 2) 否認防⽌の必要性に関連する法的リスクの追加情報は, 連邦機関のトランザクションにおける電子署名の使用 (*Use of Electronic Signatures in Federal Organization Transactions* [ESIG]) に説明されている.

これに加え, ガイドラインを導入する政府機関は, 2014年の連邦情報セキュリティ現代化法(FISMA), 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283 [FISMA] と, 関連する NIST 標準およびガイドラインに基づく法定責任に従わなくてはならない. FISMA は連邦政府機関に対し, 機関の業務と資産を⽀える情報とシステムを安全に保つために, 機関全体にわたるプログラムを開発, ⽂書化, 実装するよう指⽰している. これにはデジタル認証を⽀える IT システムのセキュリティの認証と認可 (Security Authorization and Accreditation, SA&A) が含まれる. NIST はガイドラインを導入する⾮連邦政府の主体に対し, デジタルシステムのセキュアな運⽤を確実にするために, 上記と同等な標準に従うことを推奨している.

## **数少ない制約**

デジタルアクセスに使用する一部の認証コードには, 物理的なアクセスの認証にも利⽤できるものもあるが, これらの技術的ガイドラインでは, 物理的アクセス（建物への⼊館など）の際の主体の認証は扱わない. さらに,ガイドラインのこの改訂版では, マシン対マシン（ルーター間など）認証と呼ばれるデバイス識別情報や, ⼀般的にモノのインターネット（IoT）と呼ばれる相互接続デバイスを明⽰的には扱わない. つまり, これらのガイドラインは, デバイスに適⽤できる可能性を残すために, 可能な限り⼀般的な主体について述べている. また⼈との認証プロトコルで使用するデバイスに認証コードを発⾏する固有の要件も除外している.

## **一連の特別出版物の利用方法**

身元情報サービスを提供するビジネスモデル, マーケットプレイス, 構成内容は, 初版の SP 800-63 が発表されてから劇的に変化している. 特に CSP はコンポーネント化され, 独⽴して運営・保有される複数のビジネス主体により構成できるようになった. さらに 身元情報の検証が必要ないケースでも, セキュリティ上強固な認証コードを利⽤することに⼤きなメリットがある. したがってこの改訂版では,こうした新しいモデルを促進し, 全体的なデジタル ID モデルでエンティティが提供する機能の特定の要件が容易に利用できるように, 800-63 の名前で⼀連の SP が作成された,.

## **改訂履歴**

### **2.5.1 SP 800-63-1**

NIST SP 800-63-1 は, 最新の認証コード (以降 “トークン” と呼ぶ) 技術を反映させ, ここで使われているデジタル ID アーキテクチャモデルの理解を深めるために NIST SP 800-63 を改訂して再構成した. CSP, 認証情報を伝えるプロトコル, デジタル ID モデルに実装されいる場合のアサーションに対して, 追加の (最⼩限の) 技術要件が規定された.

### **2.5.2 SP 800-63-2**

NIST SP 800-63-2 は SP 800-63-1 の限定的な更新であり, 実質的な変更はセクション 5 *登録と発行プロセス*のみであった. 改訂版の実質的な変更の意図は, 身元情報の検証プロセスにおいて専⾨的な認証情報の使⽤を促進し, レベル 3 のリモート登録で認証情報を発⾏するための記録上の住所に郵便を送る必要性を少なくすることにあった. セクション 5 のその他の変更は, 副次的な説明と明確化であった.

### **2.5.3 SP 800-63-3**

NIST SP 800-63-3 は SP 800-63-2 を再構成して⼤幅に更新した. SP 800-63-3 では, デジタル認証保証で個々の構成要素となる AAL, IAL, FAL が導⼊され, 認証の強度と主張された身元情報の信頼性を独⽴して処理する必要性の高まり (例えば, 強固な匿名認証)に応えている. このガイドラインには, リスク評価の⽅法論と IAL, AAL, FAL への適⽤が含まれる. SP 800-63-3 では, SP 800-63 がカバーするデジタル ID ガイダンス全体を, 認証 について述べた単⼀の文書から, (上述の個々の構成要素に個別に対処するために) SP 800-63-3 を最上位とする⼀連の4つの文書に分割した.

800-63-3 でのその他の変更点は以下のとおりである.

* 身元情報の検証と連携を範囲に含めていることを正しく⽰すために, そして,今後の改訂でデバイス識別情報やマシン間認証を含めるために範囲を拡大できるように, “デジタル ID ガイドライン” に改名した.
* アサーション技術におけるトークンの使用との混同を避けるため, トークンの代わりに*認証コード* という⽤語を⽤いるなど, ⽤語変更を⾏った.
* 認証とアサーションの要件を更新し, セキュリティ技術と脅威の進化を反映した.
* 検証者が長期シークレットを保管する際の要件を定めた.
* 身元情報の検証モデルを再構成した.
* 身元情報のリモート検証に関連する要件を更新した.
* 独⽴したチャネルとデバイスを “本人が持っているもの” として⽤いることを明確化した.
* 事前登録した知識トークン (認証コード) は, (時として⾮常に弱い) パスワードの特殊形態のため**削除**した.
* 認証コードの紛失や盗難時のアカウント回復に関する要件を定めた.
* アウトオブバンドの認証コード⽤の有効手段としての Eメールを**削除**した.
* 再認証とセッション管理に関する議論を深めた.
* 身元情報の連携に関する議論を深め, 連携の文脈でアサーションを再構成した.

# 定義と略語

⽤語の定義と略語については, すべて付録 A を参照.

# デジタル ID モデル

*このセクションは参考情報である.*

## **概要**

ガイドラインにおけるデジタル ID モデルは, 現時点で市場で調達可能な技術とアーキテクチャを反映している. 多数の主体に渡って認証情報発⾏と属性提供といったように機能を分離するさらに複雑なモデルも利用可能で, 一部のアプリケーションクラスではメリットをもたらす場合もある. この文書ではよりシンプルなモデルを採⽤するが, 各機関がこうした機能を分離することを妨げるものではない. さらに, CSP が実⾏する登録, 身元情報の検証, 発⾏プロセスの中には, しばしば登録局 (RA) や身元情報マネージャー (IM) として知られるエンティティに委託されるものもある. RA と CSP の関係は密接で, この関係の性質は, RA, IM, CSP　の間で異なる場合がある。こうしたタイプの関係性とその要件は, この文書の扱うところではない. したがって, CSP という用語は, RA と IM の機能も含む. 最後に, CSP がデジタル ID サービス以外のサービスを提供することもある. そういった状況では, ガイドラインに指定された要件は CSP としての機能にのみ適用され, その他のサービスには適用されない.

デジタル ID はオンライントランザクションに関与する主体を⼀意に表現する. 主体と実在する身元情報との関係を検証するプロセスは, *身元情報の検証*と呼ばれる. ガイドラインでは検証される主体を*申請者*と呼び, 検証プロセスを完了した申請者のことを*加入者*と呼ぶ.

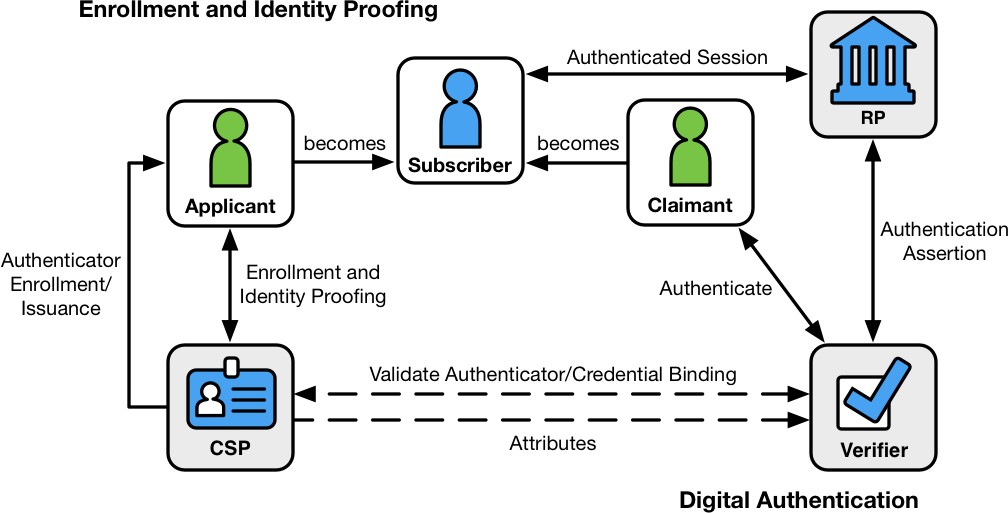
身元情報の検証の強度は IAL と呼ばれる序数的指標で表される. IAL1 では身元情報の検証は必要ない. したがって, 申請者が提供したどのような属性情報も自己表明であり, （それが CSP から RP に提供されたものだとしても）自己表明であるため検証されていないものとして扱う必要がある. IAL2 と IAL3 では, 身元情報の検証が必須となり, RP が CSP に対して, 検証済みの属性値, 検証済みの属性記述, 匿名識別子といった加入者情報の明示を要求することもある. これらの情報は RP が認証判定を⾏う際の材料となる. RP は IAL2 か IAL3 を必要とすることを決定できるが, 特定の属性のみを必須とすることもでき, そうすることで主体に対してある⼀定レベルの匿名性を確保することができる. このプライバシー強化アプローチは, 検証プロセスの強度を認証プロセスの強度から分離した成果である. さらに RP は 連携した身元情報アプローチを採⽤することもでき, その場合 RP は身元情報の検証, 属性の収集および保管をすべて CSP に任すことができる.

これらのガイドラインでは, 認証される主体を*認証要求者*と呼び, その身元情報を検証する主体を*検証者*と呼ぶ. 認証プロトコルを通して認証要求者が検証者に対して1つ以上の認証コードを保持・管理していることを⽴証すると, 検証者は認証要求者が正規の加入者であると検証できる. 検証者はこの加入者についてアサーションを RP に送る. この時加入者が匿名の場合もそうでない場合もある. アサーションには識別⼦が含まれ, 場合によっては⽒名や登録プロセスにおいて収集されたその他の属性など加入者に関する身元情報も含まれる. どういった情報を含むかは CSP のポリシーや RP のニーズ, 主体による属性 開示の同意などに依存する. 検証者も RP である場合, アサーションは暗黙的なものとなる. このとき RP は, 検証者から提供された認証済み情報を元に認証判定を⾏うことができる.

認証により, 認証要求者が認証情報に関連付けられた認証コードを管理していることが確かめられ, 場合によっては加入者の属性値 (例えば, 加入者が市⺠であり, 特定の⼤学の学生であり, ある機関や組織から特定の番号やコードを割り当てられている) についても確認できる. 認証は認証要求者の認証やアクセス権限を確定しない. それは別の決定であり, このガイドラインの扱うところではない. RP は加入者の認証された身元情報と属性を他のファクタと組み合わせ, 認証を確定することができる. この一連の文書は, RP が加入者に対して認証を成功させるために追加情報を要求することを妨げるものではない.

認証プロセスの強度は AAL と呼ばれる序数的指標で表される. AAL1 では単一ファクタ認証が求められ, 幅広い種類の認証コードが利⽤できる. AAL2 ではより強固なセキュリティのために2種類の認証ファクタが要求される. 最⾼レベルの認証である AAL3 では, ハードウェアベースの認証コードと検証者なりすまし対策が要求される.

ここで扱われるデジタル ID モデルを構成するさまざまなエンティティとインタラクションを図 4-1 に⽰す.



（図の説明）

（上から下へ）

登録と身元情報の検証

認証されたセッション

**RP**

**申請者**

**加入者**

**認証要求者**

認定(becomes)

認定(becomes)

認証コード

登録/

発行

登録と

身元情報の検証

認証

認証アサーション

認証コード/認証情報の検証

属性

**検証者**

**デジタル認証**

#### 図 4-1 デジタル ID モデル

図の左側は, 登録, 認証情報発⾏, ライフサイクル管理活動と, 身元情報の検証と認証プロセスにおけるさまざまなステータスを⽰している. 通常は以下のような流れでインタラクションが⾏われる.

1. 申請者が登録プロセスを通して CSP に申請する.
2. CSP は申請者に対して身元情報の検証を⾏い, 検証に成功すると申請者は加入者になる.
3. 認証コードとそれに対応する認証情報が CSP と加入者の間で確定される.
4. CSP は, 認証情報とそのステータス, そして (少なくとも) 認証情報の有効期間内に収集された登録データを管理し, 加入者は⾃⾝の認証コードを管理する.

他の流れはこれほど⼀般的ではないが, 同様の機能要件を満たすと考えられよう.

図の右側は, 認証コードを利⽤してデジタル認証を⾏うエンティティとインタラクションを⽰している. 加入者は検証者に対して認証する必要がある場合に認証要求者と呼ばれる. ここでのインタラクションは以下のとおりである.

1. 認証要求者は認証プロトコルを通して認証コードを保持・管理していることを検証者に証明する.
2. 検証者は CSP と通信し, 加入者の身元情報をその認証コードに結び付けている認証情報を検証し, 任意で認証要求者の属性を取得する.
3. CSP または検証者は, 加入者に関するアサーションを RP に提供する. RP はアサーションに含まれる情報を利⽤して認証決定を⾏うことができる.
4. 加入者と RP の間で認証済みセッションが確⽴される.

すべての場合において, RP は認証要求者を認証する前に CSP に対して必要な属性を要求すべきである. さらに認証要求者は, アサーションの⽣成と送信の前に, 属性送信に同意を求められるべきである.

場合によっては, 検証者は認証を完了させるために CSP とリアルタイムで通信する必要はない (例えば., デジタル証明書を利⽤する場合). したがって, 検証者と CSP の間の点線はこれらの２つのエンティティの論理的なリンクを⽰している. 実装によっては, 検証者, RP, CSP の機能はこの図のように分離されている. しかし, こうした機能が同じプラットフォーム上に存在する場合, 各構成要素間のインタラクションは, 信頼できない共有ネットワーク経由のプロトコルではなく, 同⼀システム上で動作するアプリケーション間のローカルメッセージになる.

上述のとおり, CSP は⾃⾝が発⾏した認証情報に関するステータス情報を管理する. 一般的に CSP は認証情報を発⾏する時に管理期間を制限するために有効期限を割り当てる. ステータスを変更した時や認証情報の期限切れに近づいた時は, 認証情報は更新されたり再発⾏されたりするか, 無効化されて破棄される. 通常は加入者が⾃⾝の現存の期限切れしていない認証コードと認証情報を使って CSP に対して認証した上で, 新規の認証コードと認証情報の発⾏を依頼する. 加入者が有効期限切れや無効化処理が⾏われる前に認証コードと認証情報の再発⾏を依頼しない場合は, もう一度登録プロセスを繰り返して新規の認証コードと認証情報を取得することになる. または, CSP は有効期限後の猶予期間に依頼を受け付けることもできる.

## **登録と身元情報の検証**

規範上の要件は [SP 800-63A (sp800-63a.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.html) *登録と身元情報の検証*に示してある.

前のセクションでは, デジタル ID の概念モデルにおける参加者を紹介した. このセクションでは, 登録と身元情報の検証における参加者の関係と責任について詳しく説明する.

この段階で*申請者*と呼ばれる個⼈は, CSP に身元情報の検証を要求する. 申請者が検証されると, その個⼈は CSP の加入者と呼ばれる.

CSP は個々の加入者を一意に識別し, 加入者の認証情報を登録し, 加入者に発⾏された認証コードを追跡するメカニズムを確立する. 加入者は登録時に認証コードを受け取ったり, CSP が加入者のすでに所有している認証コードに加入者を結び付けたり, その後に必要となった段階で認証コードが⽣成されたりすることもある. 加入者は認証コードを管理し, 認証コードの有効性を保つために CSP のポリシーに従う義務がある. CSP は各加入者の登録の記録を管理し, 例えば認証コードの紛失や盗難の際にリカバリーできるようにする.

## **認証とライフサイクル管理**

規範の要件は [SP 800-63B (sp800-63b.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html), *認証とライフサイクル管理*に示してある.

### **認証コード**

認証システムの古典的パラダイムは, 3つのファクタを認証基盤にしている.

* 本人が知っていること（例えばパスワード）.
* 本人が持っているもの（例えばIDバッジや暗号鍵）.
* 本人の特徴であるもの（例えば指紋や他の生体認証データ）.

MFA は上記のファクタのうち１つ以上を使うことを意味する. 認証システムの強度は, そのシステムに組み込まれたファクタの数に⼤きく依存する. より多くのファクタを⽤いれば, 認証システムはそれだけ堅固になる. これらのガイドラインの⽬的においては, 認証システムが最高度のセキュリティ要件を満たすには, 2つのファクタを利⽤するのが適切である. セクション 5.1 で述べるように, 場所情報やデバイスの識別情報といったその他の種類の情報を RP や 検証者が使用し, 主張された身元情報のリスクを評価する場合もあるが, そうした情報は認証ファクタとは⾒なされない.

デジタル認証では, 認証要求者は CSP に登録されていて本人の証明に使用される１つ以上の認証コードを保持して管理する. 認証コードは 認証要求者が正規の加入者であることを証明するためのシークレットを含み, 認証要求者は １つ以上の認証コードを保持・管理していることをネットワーク経由でシステムやアプリケーションに対して認証する.

認証コードに含まれるシークレットは, 公開鍵のペア（非対称鍵）か共有シークレット（対称鍵）に基づいている. 公開鍵と関連するプライベート鍵が公開鍵のペアとなる. プライベート鍵は認証コード上に保存され, 認証要求者が認証コードを保持・管理していることの証明に使用される. 何らかの認証情報（一般的には個人鍵証明書）を通して認証要求者の個人鍵を知っている検証者は, 認証要求者が対応するプライベート鍵を含む認証コードを保持・管理していることを証明することで, 認証要求者の身元情報を検証するために認証プロトコルを使用することができる.

認証コード上に保存された共有シークレットは, 対称鍵か記憶されたシークレット (例えばパスワード や PIN) のどちらかになる. 上述の非対称鍵とは異なり, 加入者はこれらを検証者と共有する必要はない. 鍵とパスワードは両方とも同様のプロトコルで利⽤できるが, 加入者と関連付ける方法が⼤きく異なる. 対称鍵は⼀般的に加入者が管理するハードウェアやソフトウェア内に保存されるが, パスワードは加入者に記憶されることが想定されている. ほとんどのユーザーは覚えやすいか入力が簡単な短いパスワードを選ぶため, パスワードは一般的に 暗号鍵よりも短い. さらに, 乱数を⽤いてシステムが鍵を⽣成する場合と⽐べ, 覚えやすいパスワードを選択しようとするユーザーは, ⻑さの決まったパスワードの⾮常に⼩さなサブセットの中から選択することが多いため, その多くは似た値になりがちである. したがって, 暗号鍵がネットワークベースの類推攻撃が不可能なほど⼗分⻑いのに対し, ユーザーが選択するパスワードは, 特に何の防御策もない場合に脆弱である可能性がある.

この巻で扱う認証コードには必ずシークレットが含まれる. 従来の認証ファクタの中には, デジタル認証に直接には当てはまらないものもある. 例えば物理的な運転免許証は本人が持っているものであり, ⼈ (例えば警備員) の認証には便利であるが, それ⾃体はデジタル認証のための認証コードにはならない. 本人が知っていることに分類される認証ファクタも, 必ずしもシークレットではない. 認証要求者に対して本人だけが知っているであろう質問に答えるよう求める知識ベース認証も, デジタル認証で許容されるシークレットにならない. 生体認証もシークレットにならない. したがって, ガイドラインでは, 生体認証が物理的な認証コードに強固に関連付けられたときに限り, 生体認証の使用を認める.

デジタル認証システムは, 以下の2つの⽅法のどちらかで複数のファクタを含めることができる.

1. 複数のファクタが検証者に提⽰される仕組みがシステムに実装されている.
2. 検証者に提⽰されるシークレットを保護するために複数のファクタが使用できる.

例えば, 上記1は記憶シークレット (本人が知っていること) をアウトオブバンドのデバイス（本人が持っているもの）と組み合わせることで実現できる. 認証要求者を認証するために, 両⽅の認証コード出力値が検証者に提⽰される. 上記2は, 暗号鍵（認証コードシークレット）を含むハードウェア（認証コード）の部分があり, アクセスは指紋により保護される場合を考えるとよい. 生体認証と共に利⽤するときに暗号鍵は認証要求者を認証するための出力値を生成する.

上述のように, 生体認証を単一ファクタとして⽤いる場合, それ⾃体はデジタル認証に許容されるシークレットとはならないが, デジタル ID の認証においてはその利⽤箇所が存在する. 生体認証の特性は一意の個⼈の属性であり, 検証時に対⾯する⼈の身元情報を検証するために使用できる. 顔の特徴, 指紋, 虹彩パターン, 声紋などの 多くの生体認証特性が存在する. [SP 800-63A (sp800-63a.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.html) *登録と身元情報の検証* では, 登録プロセスで生体認証を収集し, 登録した加入者が登録を否認することを防⽌し, 不正な登録に関わる⼈物を特定することを推奨している.

### **認証情報**

先のセクションで述べたとおり, 認証情報は発⾏プロセスの一部として認証コードに加入者を識別⼦で結び付ける. 認証情報は CSP によって保管・管理されるが, 認証要求者が保持することもある. 認証要求者は認証コードを保持するが, 必ずしも認証情報を保管する必要はない. 例えば, ユーザーの属性を含むデータベースエントリーは, この文書の⽬的においては認証情報であると⾒なされるが, そのエントリーは検証者が保持する. X.509 公開鍵証明書は, 認証要求者が保持できる（実際に保持する場合が多い） 認証情報の古典的な例である.

### **認証プロセス**

認証プロセスは, 認証要求者が認証コードを保持し管理していることを検証者に⽰すところから始まる. ここでは認証コードは認証プロトコルを通して明示された身元情報に関連付けられている. 認証コードの保持と管理が一度でも⽰されていると, 検証者は 一般的にCSP とのインタラクションを通して, 認証情報が依然として有効であることを検証する.

認証プロトコルにおける検証者と認証要求者の間のやりとりの厳密な性質は, システムのセキュリティ全体を決定する際に極めて重要である. よく設計されたプロトコルは, 認証の最中とその後においてこうしたやりとりの完全性と機密性を保護することができ, 正当な検証者に偽装した攻撃者による被害を制限できる.

また, 検証者側で攻撃者が認証を試みる率を制限したり, 不正な試みを遅延させたりすることで, パスワードや PIN といったエントロピーの低いシークレットに対するオンラインの類推攻撃を軽減できる. オンラインの類推攻撃ではほとんどの試⾏が失敗することを前提にしているため, 一般的にその対策は失敗した試みを追跡することと回数を制限することになる.

検証者は機能的な役割であるが, CSP, RP またはその両⽅と合わせて実装されることが多い. 検証者が CSP から独⽴したエンティティである場合, 検証者は認証プロセスで加入者の認証コードのシークレットを知る手段がないことを保証するか, 検証者が CSP に保管されているシークレットに無制限にアクセスできないことを少なくとも保証することが一般的に望ましい.

## **連携とアサーション**

規範上の要件は [SP 800-63C (sp800-63c.html),](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.html) *連携とアサーション*に示してある.

全体として, SP 800-63 は連携した身元情報アーキテクチャを前提としていない. ガイドラインは市場に存在するモデルについては関知せず, 各機関は⾃⾝の要件に応じてデジタル認証スキームを導⼊できる. しかしながら, 単⼀の機関や RP が運営するサイロ化した多数の身元識別情報システムよりも, 身元情報の連携の⽅が望ましい.

連携したアーキテクチャには, 以下の他にも多くの利点がある.

* ユーザーエクスペリエンスが向上する. 例えば, 身元情報が一度証明されれば, 発⾏された認証情報を複数の RP に対して再利⽤できる.
* ユーザーと各機関の双⽅にとってコスト低減効果がある. （ユーザーにとっては認証コードの減少, 各機関にとっては情報技術インフラの縮⼩）
* 各機関が個人情報を保存する際に 収集, 保管, 処理, 法令遵守活動にかかる費用が不要となり, データが最低限に抑えられる.
* 各機関はサービスを提供するために匿名属性アサーションを利用し, クレームを含めた最⼩限の属性セットを要求できる.
* 各機関は身元情報の管理ではなく本来の業務に集中することができる.

以下のセクションでは, 各機関が連携した身元情報アーキテクチャを選択する場合の構成要素について説明する。

### **アサーション**

認証プロセスが完了すると, 検証者は認証結果を含んだアサーションを⽣成し RP に提供する. アサーションは検証者から RP に 認証プロセスの結果と, 随意ではあるが加入者に関する情報を伝えるために使用される. アサーションは直接 RP に送信されることも, 加入者を通して転送することもできるが, それはシステム設計と大きく関係する.

RP はアサーションの発行元, ⽣成⽇時, 有効期限, CSP と RP のポリシーとプロセスを管理するトラストフレームワークに基づいてアサーションを信頼する. 検証者はアサーションの完全性が確認できる⼿段を提供する責任を負う.

RP は発行元（検証者）を認証してアサーションの完全性を確認する義務を負う. 検証者が加入者を経由してアサーションを提供する場合は, 検証者はアサーションが変更できないような方法で完全性を保護しなければならない. しかし, 検証者が直接 RP と通信を⾏う場合は, 保護されたセッションを使用してアサーションの完全性を確保できる. オープンなネットワークを経由してアサーションを送信する場合は, 検証者は情報の機密性維持について信頼できる RP だけがアサーションに含まれる加入者に関する要注意情報を抽出できることを保証する責任を負う.

アサーションの例を以下に挙げる.

* セキュリティアサーションマークアップ言語（SAML）アサーションは, セキュリティアサーションを記述するためのマークアップ言語によって規定される. 検証者は SAML アサーションを使って認証要求者の身元情報に関するステートメントを RP に伝えることができる. SAMLアサーションにはデジタル署名が施されることもある.
* OpenID Connectクレームは, JavaScript Object Notation (JSON) を使ってセキュリティと場合によってはユーザーのクレームを記述するために規定される. JSON のユーザー情報クレームにはデジタル署名が施されることもある.
* Kerberos チケットは, Ticket-granting Authority が対称鍵ベースのカプセル化⽅式を利⽤して 2つの認証された主体にセッション鍵を発⾏することを可能にする.

### **証明書利用者 (RP)**

RP は, 認証プロトコルの結果を信頼し, オンライントランザクションを⾏うために加入者の身元情報か属性の確実性を確定する. RP は, 加入者の認証済み身元情報（匿名または実名）, IAL, AAL, FAL （FAL は アサーションプロトコルの強度を⽰す）およびその他のファクタを使用して認証を決定する. 検証者と RP は同じエンティティでも別々のエンティティでもよい. 両者が別々の場合, 通常 RP は検証者からアサーションを受け取る. RP は自ら信頼する検証者からアサーションが来たことを保証する. また, アサーションに含まれる個⼈の属性や有効期限などの追加情報を処理する. RP は 検証者によって提⽰されたアサーションが, IAL, AAL, FAL に関係なく RP の確⽴されたシステムアクセス基準を満たしているかどうかを最終的に判断する.

# デジタル ID リスク管理

*このセクションは規範である.*

このセクションおよび対応するリスク評価ガイダンス は, NIST リスク管理フレームワーク (RMF) とその構成要素である特別出版物を補完する. これは各機関にさらなるリスク管理プロセスを課すものではなく, ここに含まれる要件は, 各機関の RP がすべての関連する RMF ライフサイクルフェーズを実⾏する際に適⽤しなければならない (SHALL) デジタル ID のリスクに関連する具体的なガイダンスを提供する.

## **概要**

今⽇のデジタルサービスでは, 検証と認証コードと連携の各要件を１つにまとめると意図しない結果が⽣じ, 導入する組織に不必要な実装負担をかけることがある. 単⼀の包括的な LOA ではなく, デジタル認証の個々の構成要素ごとに認証失敗のリスクと影響を評価することにより, 機関は認証サービスの最も効率的なセットを提供することができる. これを達成するために, ガイドラインでは認証エラーはすべての要件を満たすシングルトンではないという立場に立つ.

この巻では, 機関が以下を回避する要件について説明する.

1. 身元情報の検証エラー (つまり, 偽の申請者が他人の身元情報を不正に主張する)
2. 認証エラー (つまり, 偽の認証要求者が他人の認証情報を不正に利⽤する)
3. 連携エラー (つまり, 身元情報のアサーションが改竄される)

身元情報の検証の失敗という観点からは, 潜在的に以下の2種類の影響がある.

1. 誤った主体にサービスを提供してしまうことによる影響. (例えば, 攻撃者は別人として検証される)
2. 過度の身元情報の検証による影響. (例えば, デジタルサービスを提供するために,必要以上に多くの個人情報を収集して保管してしまう)

そのため, 各機関は検証, 認証, 連携のエラーに関するリスクを個別に評価し, 各トランザクションに必要な保証レベルを確定しなければならない (SHALL).

RMF の全体的な適⽤を⽀援するため, セクション5.3 ではデジタル ID に固有の影響カテゴリを示している.

リスク評価は, 身元情報の検証, 認証, 連携の各プロセスによってリスクを軽減すべき範囲を確定する. こうした確定は, リスクの特定につながる技術を求めるのでははなく, 適⽤可能な技術とリスク軽減対策の適切な選択につながる. 機関が全体的なリスク評価を終え, 身元情報の検証, 認証, (妥当な場合は) 連携に対して保証レベルを選択し, それぞれの保証レベルを満たすために採⽤するプロセスと技術を選定すると, 機関は SP 800-53A IA-1 a.1 に 従 い “デジタル ID の許容表明” を確定しなければならない (SHALL). セクション5.5 に “デジタル ID の許容表明” に必要なコンテンツを詳しく説明する.

## **保証レベル**

機関の RP はリスクに基づき以下の個々の保証レベルを選択しなければならない (SHALL).

* IAL: 個⼈の身元情報を確信を持って確定するための, 身元情報の検証プロセスの頑強性. IAL は潜在的な身元情報の検証 エラーを減少させることを⽬的として選択される.
* AAL: 認証プロセス⾃体と, 認証コードと特定の個⼈識別⼦の結び付けの頑強性. AAL は認証エラー （つまり,偽の認証要求者が他人の認証情報を不正に使用）を減少させることを⽬的として選択される.
* FAL: 連携時に認証と（妥当な場合は）属性情報を RP に伝えるために使用するアサーションプロトコルの頑強性. すべてのデジタルシステムが連携した身元情報アーキテクチャとは限らないとき FAL はオプションである. FAL は潜在的な連携エラー（身元情報アサーションの改竄）を減少させることを⽬的に選択される.

身元情報, 認証コード, 連携の各保証レベルの概要は以下のとおりである.

**表 5-1 身元情報の保証レベル**

|  |
| --- |
| **身元情報の保証レベル** |
| **IAL1:** 属性 がある場合それらは自己表明である. または自己表明として扱われるべきである. |
| [**IAL2:** リモートか対⾯での身元情報の検証が必須となる.識別に⽤いられる属性に関しては, 少なくとも SP 800- 63A (sp800-63a.html) の手順に従い, 対⾯またはリモートで検証されている必要がある.](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.html) |
| **IAL3:** 対⾯での身元情報の検証が必須となる. 識別に⽤いられる属性に関しては, [SP 800-63A (sp800-63a.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.html) に説明してあるように, 認可された CSP の担当者が書類審査で検証しなければならない. |

#### 表5-2 認証コードの保証レベル

|  |
| --- |
| **認証コードの保証レベル** |
| **AAL1:** 認証要求者が加入者に対して登録された認証コードを管理していることがある程度保証される.  AAL1 では, 利用可能な幅広い認証技術を使用する単一ファクタ認証が必須である. 認証を成功させるには, 認証要求者がセキュアな認証プロトコルを通して認証コードを保持・管理していることを証明する必要がある. |
| **AAL2:** 認証要求者が加入者に対して登録された認証コードを管理していることが⾼い確信度で保証される.２つの異なる認証ファクタを保持・管理していることをセキュアな認証プロトコルを通して証明する必要がある. AAL2 以上では, 承認済み暗号化技術も必要になる. |
| **AAL3:** 認証要求者が加入者に対して登録された認証コードを管理していることが, ⾮常に⾼い確信度で保証される. AAL3 の 認証 は, 暗号プロトコルによる鍵所有の証明に基づいている. AAL3 は AAL2 と似ているが, 検証者のなりすましに対抗する “ハードな” 暗号認証コードも必要になる. |

**表 5-3 連携の保証レベル**

|  |
| --- |
| **連携の保証レベル** |
| **FAL1:** RP は 身元情報プロバイダ (IdP) からベアラアサーションを受け取ることができる. IdP は承認済みの 暗号化技術 を使ってアサーションに署名しなければならない. |
| **FAL2:** RP のみが復号できるように承認済みの暗号化技術を使ってアサーションを暗号化する要件が加わる. |
| **FAL3:** 加入者がアサーションとアサーションの成果物自体で参照される暗号鍵を保持していることを証明する必要がある. アサーションは承認済みの暗号化技術を使って署名され, RP に対して暗号化されなければならない. |

総称的にあるいは⼀括的に説明する場合は, IAL, AAL, FAL を **xAL** と表記する.

## **リスクと影響**

このセクションでは, IAL, AAL, FAL を決定するために使用する影響カテゴリについて詳しく述べる.

潜在的な影響カテゴリ: 明示された身元情報について適切な保証レベルを決定するために, 各機関は潜在リスクを評価し, その影響を最⼩限に抑える⼿段を特定しなければならない (SHALL).

より深刻な悪影響が予想される認証, 検証,連携のエラーには, より⾼い保証レベルが求められる. ビジネスプロセス, ポリシー, 技術がリスク軽減に役⽴つ可能性がある.

被害と影響のカテゴリは次のとおりである.

1. 不便, 苦痛, または社会的地位や評判の低下.
2. 経済的損失または機関の負債.
3. 機関のプログラムや公共利益への損害.
4. 要注意情報の無許可の公開.
5. 個⼈の安全.
6. ⺠事または刑事上の違反.

デジタルトランザクションに要求される保証レベルは, 連邦情報処理規格 (FIPS) 199 [FIPS 199] に示された潜在的影響度を利⽤し, 上記のカテゴリごとの潜在的影響を評価して確定できる.

潜在的影響度には, 以下の3つの値がある.

1. 影響度低
2. 影響度中
3. 影響度高

### **ビジネスプロセス対オンライントランザクション**

保証レベルの確定は, デジタルシステムの⼀部をなすトランザクションにのみ基づく. オンライントランザクションは, オフライン処理や完全にセグメント化されたシステム上でのオンライン処理を必要とする完全なビジネスプロセスとは等価でないこともある. 適切な保証レベルの選択において, 機関は提供する便益性やサービスに関連するビジネスプロセス全体の評価ではなく, デジタルサービスを通して提供しているオンライントランザクションに関連するリスクを評価すべきである. 例えばオンラインアンケートでは個人情報が収集されることがあるが, 情報提供者は保存された情報をオンラインで決して利用できない. このような場合, バックエンドシステムで注意深く情報を保護することは重要だが, システムや関連する利益にアクセスする目的で情報を提供するユーザーの身元情報を検証したり認証したりする必要はない. オンライントランザクションはデータの提出処理に過ぎない. ビジネスプロセス全体ではかなりのデータ検証が必要となる可能性があるが, 正規の⼈物が情報を提出したかどうかを知る必要はない. このシナリオでは, 身元情報のどのような検証も認証も必要としない.

機関がオンライントランザクションの要件ではなくビジネスプロセス全体を評価した場合にリスク評価が変わりうるその他の事例としては, 公開人材募集の履歴書を受け付けるデジタルサービスが挙げられる. このユースケースでは, デジタルサービスは個⼈が他⼈に代わって履歴書を提出することを許可し (少なくとも個人が提出することを制限しない), その後にサイトに再訪した時にさまざまな⽬的のために履歴書にアクセスすることを許可する. 履歴書の情報はユーザーが後のセッションで利用でき,個人情報が含まれることがあることから, 個人情報がユーザーの自己表明であったとしても, 機関は MFA が必要な AAL を選択する必要がある. この場合, [EO 13681] の要件が適⽤され, アプリケーションは少なくとも AAL2 で提供されなければならない. しかしながら 身元情報の検証要件は依然として明確でない. 履歴書を審査し最終的に雇⽤して研修を行うビジネスプロセス全体では, 膨大な身元情報の検証が必要になる. 機関は採⽤を決定するとき, 求⼈情報への応募者が実際にオンライン提出された履歴書の主体であるという⾼レベルの確信が必要となる. しかしこのレベルの検証はオンラインでの履歴書提出には必要ではない. 身元情報の検証はトランザクションのデジタルな部分を完了させるためには必要ではない. 提出者に対して身元情報の検証を⾏うと, デジタルの求職ポータルによる採⽤プロセスでこうした情報がまったく必要ないとき, 過剰に個人情報を収集してしまうこともあるため, オンラインシステムに必要以上にリスクを生み出し, ユーザビリティを低下させる恐れがある. したがって, 最も適切な IAL は1となろう. オンライントランザクションを完了するにはユーザーの身元情報の検証は不要である. オンラインポータル⾃体に対するこの決定は, 偽の提出者が採用されることがないよう,ビジネスプロセス全体に対して一見すると明確に見える身元情報の検証要件と無関係である.

### **カテゴリごとの影響**

このセクションでは被害のカテゴリごとに潜在的影響を定義する. IAL, AAL, FAL (連携した身元情報を許容または評価する場合) の保証レベルは個別に評価しなければならない (SHALL).

|  |
| --- |
| 注意: 身元識別情報システムのエラーがカテゴリに測定可能な結果を及ぼさなければ, 影響はない. |

*不便, 苦痛, 社会的地位や評判の低下に関する潜在的影響:*

低: 最悪でも, 任意の主体に対する, 限定的かつ短期間の不便, 苦痛, 困難.

中: 最悪でも, 任意の主体に対する, かなりの短期間または限定的な⻑期間の不便, 苦痛, または社会的地位や評判の低下.

高: 任意の主体に対する, 重⼤またはかなりの⻑期的な不便, 苦痛, または社会的地位や評判の低下. 一般的にこれは特に深刻な影響を及ぼすか, 多くの個⼈に影響を及ぼす可能性のある状況を想定したレベルである.

*経済的損失に関する潜在的影響:*

低: 最悪でも, 任意の主体に対する, 些細なまたは軽微な経済的損失または機関の負債.

中: 最悪でも, 任意の主体に対する, 相当な経済的損失または機関の負債.

高: 任意の主体に対する, 重⼤または致命的な経済的損失または機関の負債.

*機関のプログラムや公共利益の損害に関する潜在的影響:*

低: 最悪でも, 組織の運⽤や資産, 公共利益への限定的な悪影響. 限定的な悪影響の例としては, (i) ⼀定範囲と期間にわたる, 業務遂⾏能⼒の低下による組織の主要機能の処理効率の低下, (ii) 組織の資産または公益への軽微な損害, がある.

中: 最悪でも, 組織の運⽤や資産, 公共利益への相当な悪影響. 相当な悪影響の例としては, (i) ⼀定範囲と期間にわたる, ミッション遂⾏能⼒の著しい低下による組織の主要機能の処理効率の著しい低下, (ii) 組織の資産または公益への著しい損害, がある.

高: 組織の運⽤や資産, 公共利益への重⼤または致命的な悪影響. 重⼤または致命的な悪影響の例としては, (i) ⼀定範囲と期間にわたる, ミッション遂⾏能⼒の重⼤な低下や喪失による組織の主要機能の処理不能, (ii) 組織の資産または公益への深刻な損害, がある.

*要注意情報の無許可公開に関する潜在的影響:*

低: 最悪でも, FIPS 199 で定義されたような低インパクトの機密性の喪失をもたらす, 認可されていない主体に対して個人情報や, 米国政府にとって重要なあるいは商業的に注意を要する情報の限定的公開.

中: 最悪でも, FIPS 199 で定義されたような中インパクトの機密性の喪失をもたらす, 認可されていない主体に対して個人情報や, 米国政府にとって重要なあるいは商業的に注意を要する情報の公開.

高: FIPS 199 で定義されたような⾼インパクトの機密性の喪失をもたらす, 認可されていない主体に対して個人情報や, 米国政府にとって重要なあるいは商業的に注意を要する情報の公開.

*個⼈の安全に関する潜在的影響:*

低: 最悪でも, 治療を必要としない軽傷.

中: 最悪でも, 軽傷に対する中程度のリスク, または治療を必要とする怪我に対する限定的なリスク.

高: 重⼤な傷害または死亡に対するリスク.

*⺠事または刑事上の違反に関する潜在的影響:*

低: 最悪でも, 通常は執⾏の対象とはならない種類の⺠事または刑事上の違反のリスク.

中: 最悪でも, 執⾏の対象となりうる⺠事または刑事上の違反のリスク.

高: 執⾏計画にとって特に重要な⺠事または刑事上の違反のリスク

## **リスク許容と代替統制**

一連の SP 800-63 は保証レベルに基づいたデジタル ID サービスに対して基本要件を指定している. 各機関はこれらのガイドラインの要件に従って身元情報サービスを実装すべきであり (SHOULD), システムをさらにセキュアにしてプライバシー保護を強化するために追加の技法や技術を検討すべきである (SHOULD).

各機関は, 業務, リスク許容範囲, 既存のビジネスプロセス, 特定の⼈々への特別な考慮事項に基づき, そしてこれらのガイドラインに記載されているのと同様の緩和策を実現するためのデータの可⽤性に基づき, または組織固有のその他の能⼒に応じて, 評価された xAL に対して NIST が推奨するガイダンスに代わる対策を講じてもよい (MAY).

適⽤可能な SP 800-63 要件が完全には実装されていない場合, 各機関は代替統制を含めるために, 選択した任意の代替策の⽐較可能性を⽰さなければならない (SHALL). 例えば, 国家情報パートナーシップ (National Information Assurance Partnership, NIAP) の保護プロファイルが FIPS 要件と同等またはより強固である場合, 機関は FIPS の代わりにその保護プロファイルを選択してもよい. つまり, 機関は⾃⾝の能⼒に基づいて評価した xAL を変更してはならないが (SHALL NOT), SP 800-63 の要件に明記されていない⼿段によりリスクを軽減する能⼒に基づいてソリューションの実装を調整してもよい (MAY). 機関は規範要件から逸脱する正当な理由と, 採⽤する代替統制の詳細の両方を文書化する⼿順を導入しなければならない (SHALL).

このガイダンスは認証エラーと身元情報の検証エラーに関するリスクのみを扱う. NIST SP 800-30 の情報技術システムのリスク管理ガイド [SP 800-30] は, 連邦政府システムにおいてリスクを管理する⼀般的⽅法論を推奨している.

## **デジタル ID の許容表明**

各機関は SA＆A を達成するために必要な既存の要件にこの情報を含めるべきである (SHOULD).

表明には, 最低限以下の情報を含めなければならない (SHALL).

1. 評価済 xAL.
2. 実装済 xAL.
3. 実装済 xAL が評価済 xAL と異なる場合は, その根拠.
4. 適⽤可能な 800-63 要件が完全には実装されていない場合, 代替制御の⽐較可能性.
5. 連携した身元情報を採⽤していない場合は, その根拠.

## **身元情報の移行**

これらのガイドラインは改訂されるため, CSP はユーザーに影響する要件の変更を考慮しなければならない (SHALL). ユーザーに影響しない場合もあれば, CSP はユーザーに移⾏⼿続を要求する場合もある. 例えば, 改訂後の最初のログイン時に, CSP は新しい IAL 要件に従うためにユーザーに追加の⾝元証明を要求することもある. これは CSP, CSP を利⽤する RP, 業務, 対象ユーザーに関連したリスクベースの決定でなければならない(SHALL). 以下の考慮点は, 機関が要件変更の影響を検討するガイドとしてのみ役立つ.

1. RP が身元情報関連の詐欺を被っている場合は, 移⾏が有益な可能性がある. そうでなければ移⾏は付加価値ではなくなる.
2. 新しくより強固な, または利用がより簡単な認証の選択肢が個別の AAL に追加されれば, CSP は新しい認証コードを発⾏したり, ユーザーがすでに持っている認証コードを登録させたりすることが可能になる.
3. 連携の要件は, ユーザーに影響を与える場合も与えない場合もある. 例えば, 同意要件やインフラ要件により, インフラやプロトコルの更新が必要になることもある.
4. xAL の追加や削除は移⾏を必要としないかもしれないが, RP に対して変更が必要かどうかを決定するために新規のリスク評価が必要になろう.

このガイダンスは, いかなる移⾏も必要であるとは規定しておらず, 改訂版が公表されたときに検討するとだけに留めている. リスク許容範囲とミッションに基づく最良のアプローチの決定は, CSP と RP の判断に委ねられる.

# 保証レベルの選択

*このセクションは規範である.*

リスク評価の結果は最適なレベルを選択する際の第⼀要因になる. このセクションでは, リスク評価の結果をリスクと無関係なその他の要因と合わせて適用し, 最も有益な xAL を選択する方法について説明する.

最初に, 以下の表 6-1 に示したようにリスク評価の影響プロファイルをそれぞれの保証レベルに関連する影響プロファイルと⽐較する. 必要な保証レベルを決定するには, リスク評価で分析されたすべてのカテゴリに対して, その影響プロファイルが潜在的影響に合致または超越する最も低いレベルを見つける必要がある.

#### 表 6-1 各認証レベルにとって最大の潜在的影響

|  |  |  |  |
| --- | --- | --- | --- |
|  | **保証レベル** | | |
| **影響カテゴリ** | **1** | **2** | **3** |
| 不便, 苦痛, または社会的地位や評判の低下 | 低 | 中 | 高 |
| 経済的損失または機関の負債 | 低 | 中 | 高 |
| 機関のプログラムや公共利益への損害 | N/A | 低/中 | 高 |
| 要注意情報の無許可公開 | N/A | 低/中 | 高 |
| 個⼈の安全 | N/A | 低 | 中/高 |
| ⺠事または刑事上の違反 | N/A | 低/中 | 高 |

リスクを分析するにあたり, 機関は認証失敗の予測される直接的・間接的結果をすべて考慮しなければならない (SHALL). これには, １回以上の失敗や単一以上の人や組織に及ぼす損害の可能性を含む, 潜在的な影響の定義には, 意味が文脈に依存する “重大” や “軽微” のような相対的な⽤語がいくつか含まれる. 機関はこうした被害の相対的重要性を決定するために, 影響を受ける⼈やエンティティの性質と状況を考慮すべきである (SHOULD). 機関は時間の経過と共にこうした問題で実践的な経験を得るため, これらの⽤語の意味はより明確になろう. 機関のプログラムやその他の公共利益への被害の分析は状況に大きく依存するため, 機関はこうした問題を注意深く考慮すべきである (SHOULD).

IAL, AAL, FAL の保証レベルはそれぞれ異なる可能性がある. 例えばある機関が, ユーザーが保健情報 (PHI) の形式で個人情報を提出する “健康管理” アプリケーションを構築したとする. EO 13681 には “デジタルアプリケーションを通して市⺠に個人データのアクセスを可能にする全機関は, 認証の複数のファクタの使用を求める” ことを要求すると定められており, 機関は AAL2 か AAL3 で MFA を実装する必要がある.

また EO 13681 は, 個人情報が公開される場合, 各機関が “必要に応じて有効な身元情報の検証プロセス” を使用することを要求している. これは (必要な AAL に合致するよう) IAL2 や IAL3 での検証が必要であるということを意味しない. 上記の例では, 機関のシステムはユーザーの実際の身元情報を知る必要がない場合がある. このケースでは, “有効な検証プロセス” とは検証を⼀切⾏わないこととなり, 機関は IAL1 を選択することになろう. これにより, 健康管理システムのユーザーは匿名状態でいることができる.

ユーザーが匿名であるにもかかわらず, 機関はそれでも認証に AAL2 か AAL3 を選択するべきである. 悪意ある人物がユーザーのアカウントを攻撃して PHI にアクセスできる恐れがあるからである.

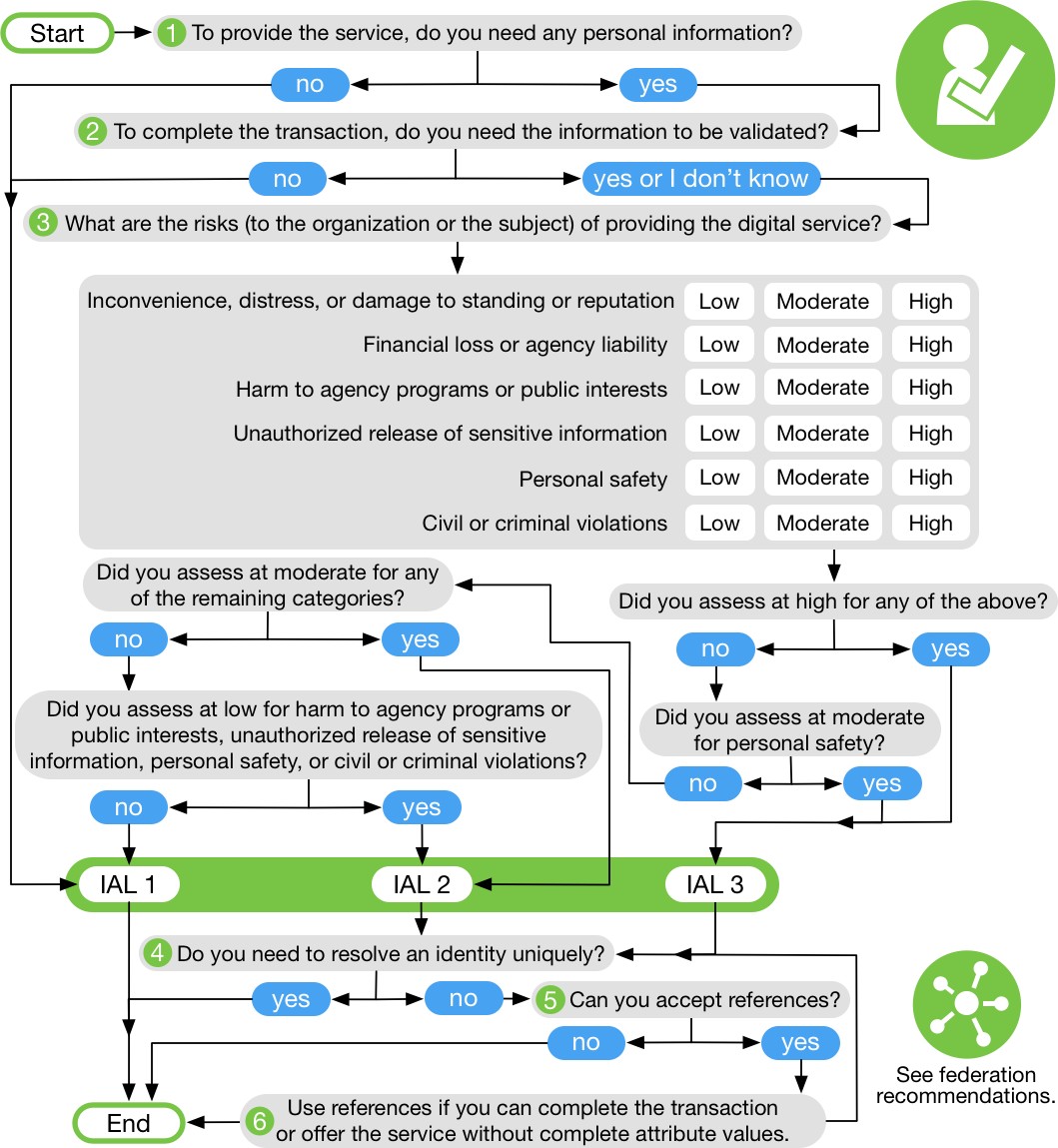
注意: 機関は上の表で求められているよりも高い保証レベル を受け入れることができる. 例えば, 連携したトランザクション では, アプリケーションが IAL2 で評価される場合に IAL3 の身元情報を受け⼊れることができる. これは認証コードに対しても同様であり, より低い認証コード要件のある RP でさらに強固な認証コードを使用できる. ただし, RP はこうしたことが CSP によってプライバシーが適切に保護されている連携シナリオだけで発⽣することを保証しなければならない. この場合, RP が要求し加入者が認可した属性だけが RP に提供され, 余計な個人情報が認証情報やアサーションから漏れることがないようにしなければならない. 詳細は SP 800-63C のプライバシーの考慮事項(sp800-63c.html#privacy) を参照.

注意: 単⼀のアプリケーションで異なる IAL, AAL, FAL を設定できるということは, この文書がもはや総合的な LOA という概念をサポートしていないという事実から導き出される. LOA を決定するための “low watermark” アプローチはもはや適用されない. IAL1 かつ AAL2 のアプリケーションを, IAL2 かつ AAL2 のアプリケーションよりセキュアでないとかプライバシー強度が低いとみなすべきではない. これらのアプリケーションの差は, 必要とされる検証の程度だけであり, それそれのアプリケーションのセキュリティとプライバシーには影響しないかもしれない. とは言っても,機関が誤った xAL を選択すると, セキュリティとプライバシーに⼤きな影響を及ぼす可能性がある.

* 1. **IAL の選択**

図 6-1 に⽰す IAL の決定⽊は, リスク評価の結果と身元情報の検証サービスに関する追加の考慮事項を組み合わせ, 各機関がデジタルサービスの提供に最適な身元情報の検証要件を決定する助けとなる.

L の選択は, デジタルサービス提供者が自分自身を検証しなければならないことを意味しない. 機関が連携できるかどうかはセクション 7 で詳しく説明する

.

#### 図 6-1 IAL の選択

#### スタート　1. サービスを提供するために, 個人情報が必要ですか？

#### いいえ はい

#### ２．トランザクションを完了するために, 情報の検証が必要ですか？

#### いいえ はい,またはわかりません

#### 3. デジタルサービスを提供する (組織または主体の) リスクは何ですか？

#### 不便, 苦痛, または社会的地位や評判の低下 低 中 高

#### 経済的損失または機関の負債 低 中 高

#### 機関のプログラムや公共利益への損害 低 中 高

#### 要注意情報の無許可公開 低 中 高

#### 個⼈の安全 低 中 高

#### ⺠事または刑事上の違反 低 中 高

#### （左側）

#### 残りのカテゴリに対して “低” で評価したときサービスはレベル1のプロファイルに一致します. または, どのカテゴリに対しても影響はありません.

#### （中央）

#### 残りのどのカテゴリも “中” で評価しましたか？

#### いいえ はい

#### 機関のプログラムや公共利益への損害, 要注意情報の無許可公開, 個⼈の安全, ⺠事または刑事上の違反に対して“低”で評価しましたか？

#### いいえ はい

#### （右側）

#### 上のいずれも “高” で評価しましたか？

#### いいえ はい

#### 個人の安全を “中” で評価しましたか？

#### いいえ はい

#### ４．個人識別情報を一意に特定する必要がありますか？

#### はい いいえ

#### ５．参照情報を許容できますか？

#### いいえ はい

#### ６．トランザクションを完了できる場合は参照情報を使用するか, 完全な属性値なしでサービスを提供します.

#### 連携推奨事項を参照してください.

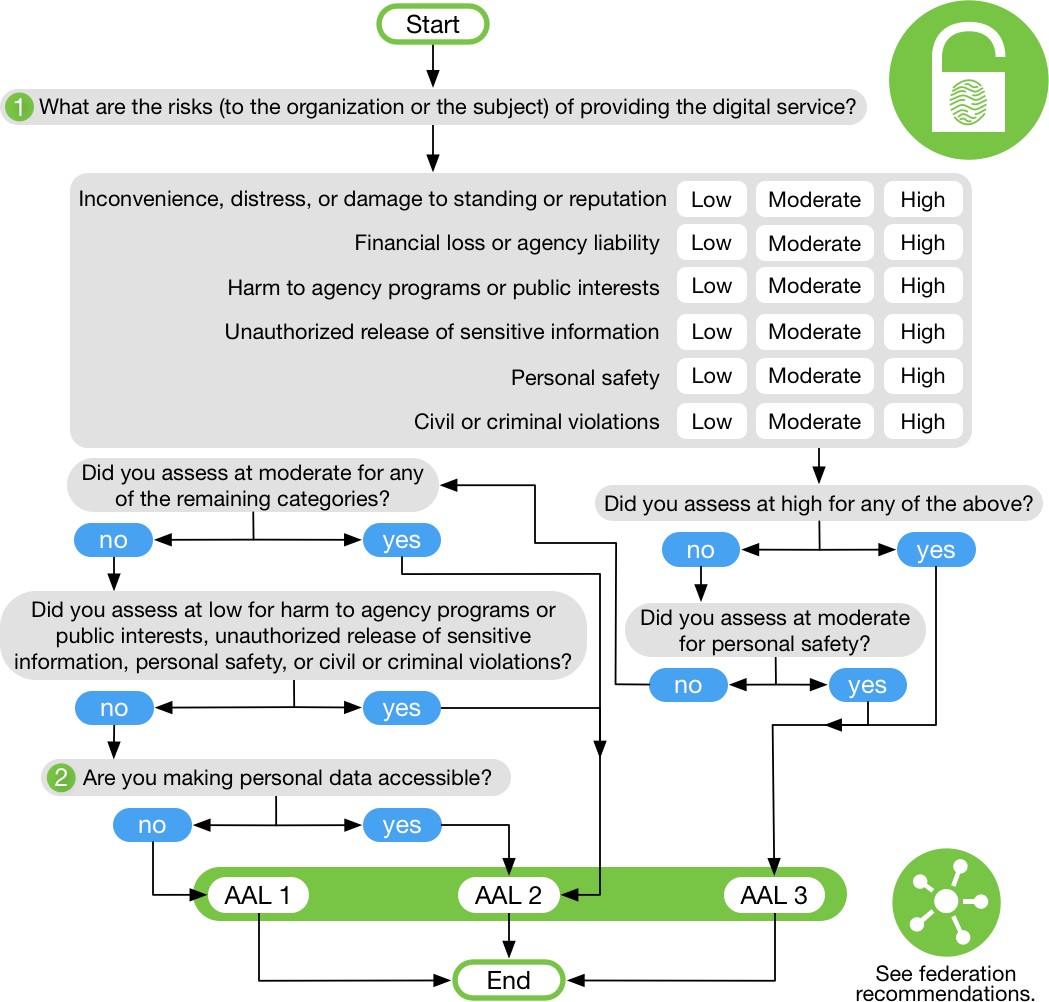
|  |
| --- |
| **1. サービスを提供するために, 個人情報が必要ですか？** |
| 最初にこの問いに答えることで, リスク評価 と IAL 選択を簡略できる. サービスがデジタルトランザクションを実⾏するのにどのような個人情報も必要としない場合, システムは IAL1 で運⽤できる. |
| ２．トランザクションを完了するために, 情報の検証が必要ですか？ |
| 個人情報が必要であれば, 確認して検証した属性が必要かどうか, または自己表明の属性が許容できるかどうかを RP は確定する必要がある. 確認して検証した属性が１つでも必要な場合は, IAL2 か IAL3 で検証した属性を受け⼊れる必要があろう. 自己表明の属性だけでデジタルサービスが提供できれば, IAL 選択は IAL1 に簡略できる. |
| 3. デジタルサービスを提供する（組織または主体の）リスクは何ですか？ |
| この段階では, 機関はある程度の検証が必要であることは理解している. ステップ 3 は, IAL2 と IAL3 のどちらが最適な選択かを決定するために, 身元情報の検証に失敗した際の潜在的影響に着⽬している. 機関が直面する可能性のある主な検証失敗は, 偽造された身元情報を本物として受け⼊れてしまうことである. これによりサービスや利益を間違った⼈物や不適格な⼈物に提供してしまうことになる. さらに, 検証が必要ない場合の検証や必要以上に多くの情報を収集する場合はそれ⾃体がリスクとなる. したがって必要がないのに検証した属性を取得することも, 身元情報の検証の失敗であるとみなされる. このステップでは, サービス提供に個人情報が必要ないことを理解した上で機関がステップ 1 と 2 に誤って回答していないかどうかを確認すべきである. リスクは組織からの観点とユーザーに対する観点から検討すべきである. というのは, 一方が悪影響を受けない場合でも, もう一方が大きな被害を受ける可能性があるためである. 機関のリスク管理プロセスはこのステップから開始されるべきである. |
| ４．個人識別情報を一意に特定する必要がありますか？ |
| ステップ 4 では, 機関が要求する個人情報が最終的に一意の身元情報の特定につながるかどうかを決定する. ⾔い換えると, 機関はデジタルサービスにアクセスする主体の完全な身元情報を知る必要があり, 確認されて検証された属性が少しはあったとしても, 匿名アクセスは不可能である. 機関が主体を一意に確認する必要がある場合, IAL 選択プロセスを終了できる. しかし, 機関はステップ 5 が価値あるものかどうか検討すべきである. クレームの受け⼊れにより, 必要以上の個人情報の収集と保存から発生するリスクを軽減できるからである. |
| ５．参照情報を許容できますか？ |
| ステップ 5 の要点は, デジタルサービスが完全な属性値へのアクセスなしに提供可能かどうかにある. これはすべての属性 がクレームとして渡されなければならないという意味ではないが, 機関が必要と見なす個⼈属性をそれぞれ検討し, クレームとして十分な属性と完全性が必要な属性を識別することを組織に要求する. 連携環境ではデジタルサービスの提供者は最初に属性情報を管理しないため, クレームの受け取りに最適である. アプリケーションがすべての必要な身元情報の検証を実⾏する場合は, すべての値はすでにデジタルサービス提供者の管理下にあるため, クレームは意味がない可能性もある. |
| **６．トランザクションを完了できる場合は 参照情報を使用するか, 完全な属性値なしでサービスを提供します** |
| ステップ 6 にたどり着いた場合はクレームを使用すべきである. このステップでは, デジタルサービスの提供に完全な属性値は必要ないことが確定されているため, デジタルサービスは連携した属性記述を 1 つ（または複数）の CSPから受け取るのに最適であると判断される. |

|  |
| --- |
| 注意: 機関は最適な検証プロセスを選択する際に, ⾃⾝のサービス対象のユーザー層も考慮すべきである. IAL 選択の機能ではなくても, ある種の検証プロセスは一部のユーザー層にとって他のプロセスより適切である場合がある. この種の分析で対象ユーザー層の検証成功率が最も高くなれば, 機関の利益となろう. |

* 1. **AAL の選択**

図 6-2 に⽰す AAL の決定⽊は, リスク評価の結果と認証に関する追加の考慮事項を組み合わせ, 各機関がデジタルサービスの提供に最適な認証要件を決定する助けとなる.

AAL の選択は, デジタルサービス提供者⾃⾝が認証コードを発⾏しなければならないことを意味しない. 機関が連携できるかどうかは セクション 7 で詳しく説明する.



#### 図 6-2 AAL の選択

#### 1. デジタルサービスを提供する (組織または主体の) リスクは何ですか？

#### 不便, 苦痛, または社会的地位や評判の低下 低 中 高

#### 経済的損失または機関の負債 低 中 高

#### 機関のプログラムや公共利益への損害 低 中 高

#### 要注意情報の無許可公開 低 中 高

#### 個⼈の安全 低 中 高

#### ⺠事または刑事上の違反 低 中 高

#### （左側）

#### 機関のプログラムや公共利益への損害, 要注意情報の無許可公開, 個⼈の安全, ⺠事または刑事上の違反に対して“低”で評価しましたか？

#### いいえ はい

#### 2. 個人データをアクセス可能にしていますか?

#### いいえ はい

#### （右側）

#### 上のいずれも “高” で評価しましたか？

#### いいえ はい

#### 個人の安全を “中” で評価しましたか？

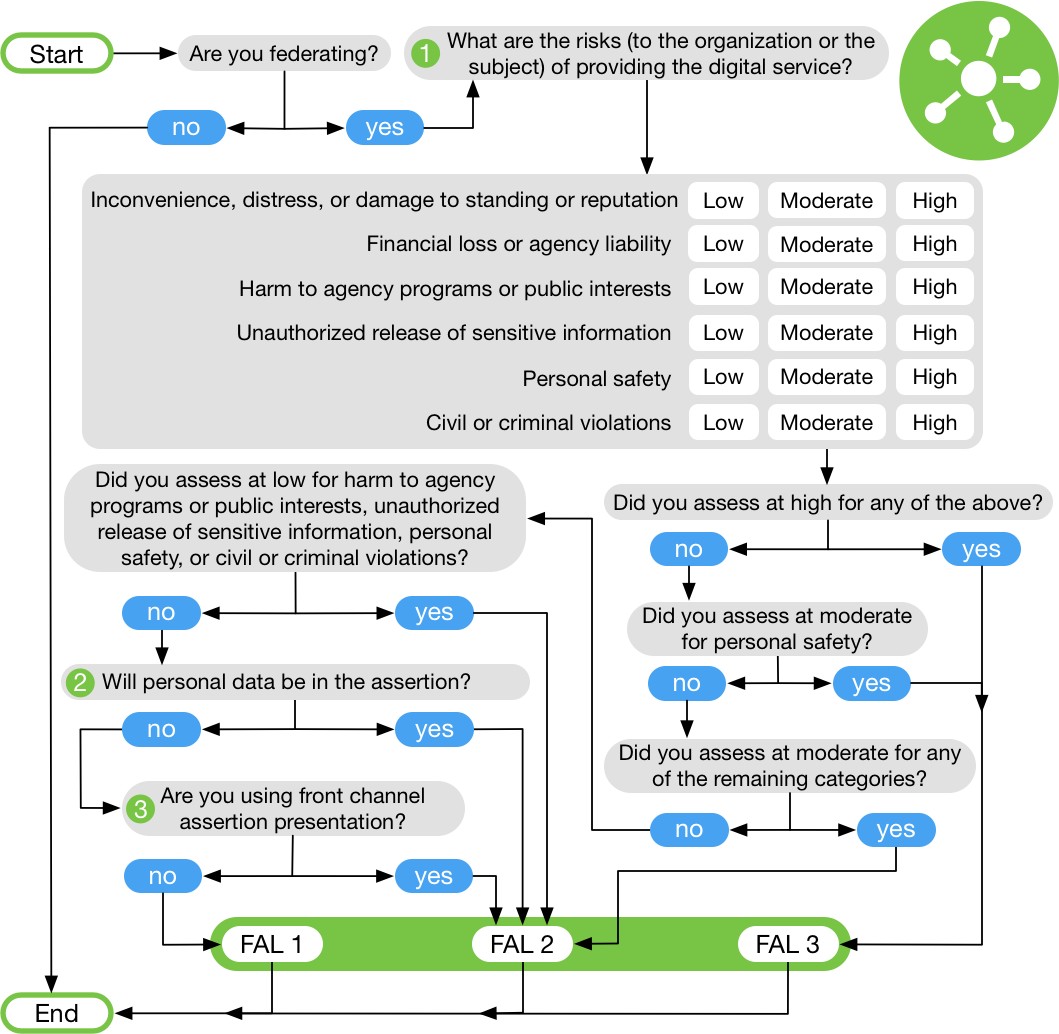
#### いいえ はい

#### 連携推奨事項を参照してください.

|  |
| --- |
| 1. デジタルサービスを提供する (組織または主体の) リスクは何ですか？ |
| ステップ 1 では認証失敗の潜在的影響に着⽬する. 言い換えると, 認可されていないユーザーが１つ以上の正規アカウントにアクセスしたら何が起こるかということである. リスクは組織からの観点とユーザーに対する観点から検討すべきである. というのは, 一方が悪影響を受けない場合でも, もう一方が大きな被害を受ける可能性があるためである. 機関のリスク管理プロセスはこのステップから開始されるべきである. |
| 2. 個人データをアクセス可能にしていますか? |
| 個人情報がオンラインで利用できるときに MFA が必要となる. この決定⽊の他のパスではすでに MFA が必要な AAL が確定しているため,個人情報に関して問われるのはこの段階のみとなる. とはいえ, リスク評価を実施するとき, すべての AAL で個人情報の公開について検討すべきである. このステップで重要な点は,個人情報がオンラインで利用できない場合, AAL2 以上を要求するために個人情報を確認して検証する必要はないということである. 個人情報が自己表明であっても, 公開にはMFA によるアカウント保護が必要である. 自己表明情報は偽造が可能だが, ほとんどのユーザーはデジタルサービスの恩恵を受けるため正しい情報を提供するであろう. したがって, 自己表明データは適切に保護されなければならない. |

* 1. **FAL の選択**

図 6-3 に⽰す FAL の決定⽊は, リスク評価の結果と連携に関する追加の考慮事項を組み合わせ, 各機関がデジタルサービスの提供に最適な要件を決定する助けとなる.



#### 図 6-3 FAL の選択

#### 連携していますか？

#### いいえ はい

#### 1. デジタルサービスを提供する (組織または主体の) リスクは何ですか？

#### 不便, 苦痛, または社会的地位や評判の低下 低 中 高

#### 経済的損失または機関の負債 低 中 高

#### 機関のプログラムや公共利益への損害 低 中 高

#### 要注意情報の無許可公開 低 中 高

#### 個⼈の安全 低 中 高

#### ⺠事または刑事上の違反 低 中 高

#### （左側）

#### 機関のプログラムや公共利益への損害, 要注意情報の無許可公開, 個⼈の安全, ⺠事または刑事上の違反に対して“低”で評価しましたか？

#### いいえ はい

#### 残りのカテゴリに対して “低” で評価したときサービスはレベル1のプロファイルに一致します. または, どのカテゴリに対しても影響はありません.

#### 2. 個人データをアクセス可能にしていますか?

#### いいえ はい

#### 3. フロントチャネルのアサーション提示を使用していますか？

#### いいえ はい

#### （右側）

#### 上のいずれも “高” で評価しましたか？

#### いいえ はい

#### 個人の安全を “中” で評価しましたか？

#### いいえ はい

#### 残りのカテゴリのいずれも “中” で評価しましたか？

#### いいえ はい

#### 連携推奨事項を参照してください.

|  |
| --- |
| 1. デジタルサービスを提供する（組織または主体の）リスクは何ですか？ |
| ステップ 1 では連携失敗の潜在的影響に着⽬する. 言い換えると, 認可されていないユーザーが１つ以上の正規アカウントにアクセスしたら何が起こるかということである. こうした危険の例としては, アサーションのリプレイによるなりすまし, ブラウザを介したアサーション情報の漏洩がある. リスクは組織からの観点と加入者に対する観点から検討すべきである. というのは, 一方が悪影響を受けない場合でも, もう一方が大きな被害を受ける可能性があるためである. 機関のリスク管理プロセスはこのステップから開始されるべきである. |
| **2. 個人情報はアサーションに含まれていますか？** |
| 個人情報が アサーションで渡されるときは FAL2 が必須となる. リスク評価を実施するとき, すべての FAL で個人情報の公開について考慮すべきである. アサーションに個人情報が含まれる場合は, FAL1 のオーディエンス要件と暗号化要件では個人情報の公開を防ぐには不⼗分であるため, FAL2 以上が必要である. 自己表明の個人情報でも公開には FAL2 によるアサーション保護が必要である. 自己表明情報は偽造できるとしても, ほとんどのユーザーはデジタルサービスの恩恵を受けるため正しい情報を提供しよう. しかし, 認可された API を呼び出して RP が個人情報を利用できる場合には, それらの情報は アサーション⾃体に含める必要はない.アサーションには個人情報がもう含まれないため, 暗号化は必要なく このFAL の要件も適⽤されない. |
| 3. フロントチャネルのアサーション提示を使用していますか？ |
| RP は, より⾼度なプライバシーとセキュリティ保護を実現するため, 可能であれば [SP 800-63C のセクション 7.1](sp800-63c.html#back-channel) に示されたバックチャネルでの提⽰⽅式を⽤いるべきである. この⽅式では加入者はアサーション⾃体ではなくアサーション参照のみを扱うため, アサーションに含まれる属性やその他の要注意情報が加入者のブラウザやその他のプログラムに漏洩する可能性は低くなる. RP は アサーション参照を直接 IdP に提⽰するため, IdP はこのステップで RP を識別して認証することもできる. さらに, RP は認証済み保護チャネル経由でアサーションを IdP から直接読み込むため, 攻撃者が RP に対してアサーションを挿入する可能性も低くなる. |

すべての FAL において, アサーションには, 署名, 有効期限, オーディエンス制限, [SP 800-63C (sp800-63c.html#assertions)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.html#assertions) に列挙されたその他の要件を含む基本的な保護対策が必要である. これらの要件を合わせた対策により, 認可されていない主体はアサーションを作成したり変更したりできなくなり, 別のシステム向けに作成されたアサーションを RP が受け⼊れることもなくなる.

## **xAL の組み合わせ**

このガイドラインは各 xAL を相互に⼀致させなくても選択できるモデルを紹介する. １つのシステムに対して異なる xAL の選択肢が存在するが, 多くの場合すべての xAL に同じレベルが適⽤されよう.

異なる xAL の組み合わせが可能となったことにより各機関には⼤きな柔軟性がもたらされたが, 個⼈から収集するデータの性質とそのデータを保護する認証コードの性質から, すべての組み合わせが可能なわけではない. 個人情報が MFA で保護されることを保証するために, IAL と AAL の有効な組み合わせを表 6-2 に示す.

#### 表 6-2 IAL と AAL の許容可能な組み合わせ

|  |  |  |  |
| --- | --- | --- | --- |
|  | **AAL1** | **AAL2** | **AAL3** |
| **IAL1: 個人情報なし** | 可能 | 可能 | 可能 |
| **IAL1: 個人情報あり** | **NO** | 可能 | 可能 |
| **IAL2** | **NO** | 可能 | 可能 |
| **IAL3** | **NO** | 可能 | 可能 |

|  |
| --- |
| 注意: 行政命令 13681 [EO 13681] によると, 個人情報が自己表明で未検証であっても, 個人データの公開には MFA による保護が必須である. 個人データにアクセスできないトランザクションでは, より強力な認証の選択肢をユーザーに提供することが推奨されていても, AAL1 での認証が発生する場合がある. さらに, IAL1 では個⼈情報ではないデータを自己表明するもできるが, その場合は AAL1 を許容できる. |

1. **連携の考慮事項**

*このセクションは参考情報である.*

このガイドラインと付随する巻は, 各機関が選択する認証および身元情報検証のアーキテクチャに関して関知しない. しかし, 機関や個別のアプリケーションに対してローカルで身元情報サービスを構築するよりも, 連携を利⽤した⽅がより効率的で効果的になるシナリオが存在する. 連携が利⽤可能であれば有望な選択肢として検討できるシナリオを以下のリストにまとめる. このリストは連携とローカルの身元情報アーキテクチャの経済的メリットやデメリットを考慮していない.

認証コードを連携させるケース:

1. 潜在的ユーザーが必要な AAL 以上を満たす認証コードをすでに持っている.
2. 想定できるすべてのユーザーコミュニティをカバーするために, 認証情報フォームの複数のファクタが必要である.
3. 認証管理をサポートするインフラ（例えば, アカウント回復, 認証コード発⾏, ヘルプデスク）が機関にない.
4. RP 実装を変更せずに, 基本的な認証コードの追加や更新を長期的にできるようにしたい.
5. サポートすべき複数の環境がある. 連携プロトコルはネットワークベースであり, 幅広いプラットフォームと⾔語で実装できる.
6. 潜在的ユーザーが複数のコミュニティーに所属し, それぞれが独⾃に身元情報インフラを持っている.

属性を連携させるケース:

1. 関係者がサービスにアクセスするには, 匿名性が必須, 必要, 実現可能または重要である.
2. サービスへのアクセスには, 部分的な属性リストのみが必要である.
3. サービスへのアクセスには, 少なくとも1つだけの属性記述が必要である.
4. 機関は必要な属性の権限ある情報元や発⾏元ではない.
5. 属性は (アクセスを決定するときなどの) ⼀時的な利⽤のためだけに必要であり, 機関はデータをローカルで保存する必要はない.

# 参考文献

*このセクションは参考情報である.*

## **General 参考文献**

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

[eIDAS] European Union, *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, July 23, 2014,

[available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2014.257.01.0073.01.ENG (http://eur-lex.europa.eu/legal- content/EN/TXT/?uri=uriserv:OJ.L\_.2014.257.01.0073.01.ENG).](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG)

[EO 13681] Executive Order 13681, *Improving the Security of Consumer Financial トランザクションs*, October 17, 2014, available at: [https://www.federalregister.gov/d/2014-25439 (https://www.federalregister.gov/d/2014-25439)](https://www.federalregister.gov/d/2014-25439).

[ESIG] Federal CIO Council, *米国e of Electronic Signatures in Federal Organization トランザクションs*, January 25, 2013, available at: [https://cio.gov/wp-content/uploads/downloads/2014/03/米国e\_of\_ESignatures\_in\_Federal\_Agency\_トランザクションs\_v1-0\_20130125.pdf (https://cio.gov/wp-content/uploads/downloads/2014/03/米国e\_of\_ESignatures\_in\_Federal\_Agency\_トランザクションs\_v1-0\_20130125.pdf)](https://cio.gov/wp-content/uploads/downloads/2014/03/Use_of_ESignatures_in_Federal_Agency_Transactions_v1-0_20130125.pdf).

[[FISMA] *Federal Information Security Modernization Act of 2014*, available at: https://www.congress.gov/bill/113th-congress/senate- bill/2521 (https://www.congress.gov/bill/113th-congress/senate-bill/2521).](https://www.congress.gov/bill/113th-congress/senate-bill/2521)

[GPG 44] UK Cabinet Office, Good Practice Guide 44, *認証 and 認証情報s for 米国e with HMG オンライン Services*, Aug米国t 8, 2016, [available at: https://www.ncsc.gov.uk/guidance/認証-and-認証情報s-米国e-hmg-オンライン-services-gpg-44 (https://www.ncsc.gov.uk/guidance/認証-and-認証情報s-米国e-hmg-オンライン-services-gpg-44).](https://www.ncsc.gov.uk/guidance/authentication-and-credentials-use-hmg-online-services-gpg-44)

[GPG 45] UK Cabinet Office, Good Practice Guide 45, *身元情報の検証 and verification of an individual*, November 3, 2014, available at: [https://www.gov.uk/government/publications/身元情報の検証-and-verification-of-an-individual (https://www.gov.uk/government/publications/身元情報の検証-and-verification-of-an-individual)](https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual).

[HSPD-12] Department of Homeland Security, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard* [*for Federal Employees and Contractors*, Aug米国t 27, 2004, available at: https://www.dhs.gov/homeland-security-presidential-directive-12 (https://www.dhs.gov/homeland-security-presidential-directive-12).](https://www.dhs.gov/homeland-security-presidential-directive-12)

[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://georgewb米国h-whiteho米国e.archives.gov/omb/memoranda/m03-22.html (https://georgewb米国h- whitehouse.archives.gov/omb/memoranda/m03-22.html).](https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html)

[M-04-04] OMB Memorandum M-04-04, *E-認証 Guidance for Federal Agencies*, December 16, 2003, available at: [https://georgewb米国h-whiteho米国e.archives.gov/omb/memoranda/fy04/m04-04.pdf (https://georgewb米国h- whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf).](https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf)

[NSTIC] *National Strategy for Tr米国ted Identities in Cyberspace*, April 2011, available at: [https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf (https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf).](https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf)

[[NIST RMF] Risk Management Framework Overview, available at http://csrc.nist.gov/groups/SMA/fisma/framework.html (http://csrc.nist.gov/groups/SMA/fisma/framework.html).](http://csrc.nist.gov/groups/SMA/fisma/framework.html)

[RSDOPS] UK Cabinet Office, Good Practice Guide 43, *Requirements for Secure Delivery of オンライン Public Services (RSDOPS)*, November [3, 2014, available at: https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-オンライン-public-services (https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-オンライン-public-services).](https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services)

[Steiner] Steiner, Peter. “On the インターネット, nobody knows you’re a dog”, *The New Yorker*, July 5, 1993.

[[STORK 2.0] European Union, *Secure 身元情報 acrOss boRders linKed 2.0*, 2014, available at: https://www.eid-stork2.eu/ (https://www.eid- stork2.eu/).](https://www.eid-stork2.eu/)

## **Standards**

[BCP 195] Sheffer, Y., Holz, R., and P. Saint-Andre, *Recommendations for Secure 米国e of Transport Layer Security (TLS) and Datagram* [*Transport Layer Security (DTLS)*, BCP 195, RFC 7525,DOI 10.17487/RFC7525, May 2015, https://doi.org/10.17487/RFC7525 (https://doi.org/10.17487/RFC7525).](https://doi.org/10.17487/RFC7525)

[[Canada] Government of Canada, *Standard on 身元情報 and 認証情報 Assurance*, February 1, 2013, available at: https://www.tbs- sct.gc.ca/pol/doc-eng.aspx?id=26776 (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776).](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776)

[ISO 9241-11] International Standards Organization, ISO/IEC 9241-11 *Ergonomic requirements for office work with visual display terminals* [*(VDTs) — Part 11: Guidance on 米国ability*, March 1998, available at: https://www.iso.org/standard/16883.html (https://www.iso.org/standard/16883.html).](https://www.iso.org/standard/16883.html)

[ISO 29003] International Standards Organization, ISO/IEC DTS 29003 *Information technology — Security techniques — 身元情報の検証*.

[ISO 29115] International Standards Organization, ISO/IEC 29115 *Information technology — Security techniques — Entity 認証* [*assurance framework*, April 1, 2013, available at: http://www.iso.org/iso/home/store/catalogue\_tc/catalogue\_detail.htm?csnumber=45138 (http://www.iso.org/iso/home/store/catalogue\_tc/catalogue\_detail.htm?csnumber=45138).](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138)

[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore, *OpenID Connect Core 1.0 incorporating errata set 1*, [November, 2014, available at: https://openid.net/specs/openid-connect-core-1\_0.html (https://openid.net/specs/openid-connect-core- 1\_0.html).](https://openid.net/specs/openid-connect-core-1_0.html)

## **NIST Special Publications**

[NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html (http://csrc.nist.gov/publications/nistpubs/index.html). The following publications may be of particular](http://csrc.nist.gov/publications/nistpubs/index.html) interest to those implementing systems of applications requiring デジタル 認証.

[SP 800-30] NIST Special Publication 800-30 Revision 1, *Guide for Conducting リスク評価s*, September 2012, [https://doi.org/10.6028/NIST.SP.800-30r1 (https://doi.org/10.6028/NIST.SP.800-30r1).](https://doi.org/10.6028/NIST.SP.800-30r1)

[SP 800-37] NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information* [*Systems, A Security Life Cycle Approach*, February 2010 (updated June 5, 2014), https://doi.org/10.6028/NIST.SP.800-37r1 (https://doi.org/10.6028/NIST.SP.800-37r1).](https://doi.org/10.6028/NIST.SP.800-37r1)

[SP 800-52] NIST Special Publication 800-52 Revision 1, \*Guidelines for the Selection, Configuration, and 米国e of Transport Layer Security (TLS) Implementations, April 2014, [http://dx.doi.org/10.6028/NIST.SP.800-52r1 (http://dx.doi.org/10.6028/NIST.SP.800-52r1).](http://dx.doi.org/10.6028/NIST.SP.800-52r1)

[SP 800-53A] NIST Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and* [*Organizations, Building Effective Assessment Plans*, December 2014 (updated December 18, 2014), https://doi.org/10.6028/NIST.SP.800- 53Ar4 (https://doi.org/10.6028/NIST.SP.800-53Ar4).](https://doi.org/10.6028/NIST.SP.800-53Ar4)

## **連邦情報処理規格**

[FIPS 199] 連邦情報処理規格 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, [https://doi.org/10.6028/NIST.FIPS.199 (https://doi.org/10.6028/NIST.FIPS.199).](https://doi.org/10.6028/NIST.FIPS.199)

[FIPS 201] 連邦情報処理規格 Publication 201-2, *Personal 身元情報 Verification (PIV) of Federal Employees and Contractors*, Aug米国t 2013, [http://dx.doi.org/10.6028/NIST.FIPS.201-2 (http://dx.doi.org/10.6028/NIST.FIPS.201-2)](http://dx.doi.org/10.6028/NIST.FIPS.201-2).

# 付録 A—定義と略語

*このセクションは規範である.*

## **定義**

認証分野で使われる⽤語は幅広く, 多くの⽤語の定義は SP 800-63 の旧版と整合性を保っているものの, いくつかは今回の改訂で変更されている. 一貫した単一の定義を欠く⽤語が多いため, この文書で用語がどのように定義されているのか注意を払う必要がある.

### **Access**

### アクセス

オンラインのデジタルサービスの1つ以上の個別機能に接続すること.

### **Active Attack**

### 積極的攻撃

認証プロトコルに対する攻撃で, 攻撃者は認証要求者, 認証情報サービスプロバイダ (CSP), 検証者, 証明書利用者 (RP) に対してデータを送信する. 積極的攻撃の例としては, 中間者攻撃 (MitM), なりすまし, セッションハイジャックがある.

### **Address of Record**

### 記録上の住所

許可された手順に沿って個⼈が情報を受け取ることができる, 有効で検証済みの (物理的または電子的) 場所情報.

### **Applicant**

### 申請者

登録と身元情報の検証を受ける主体.

### **Approved Cryptography**

### 承認済み暗号化技術

連邦情報処理規格 (FIPS) の承認または NIST の推奨を受けており, FIPS または NIST 推奨事項に (1) 指定されているか, (2) 採⽤されているアルゴリズムまたは技術.

### **Assertion**

### アサーション

検証者から証明書利用者 (RP) に対して送られる, 加入者の身元情報を含んだステートメント. アサーションには検証済み属性を含めることもできる.

### **Assertion Reference**

### アサーション参照

アサーションと関連付けて⽣成されるデータオブジェクトで, 検証者を識別するとともに, 検証者が所有する完全なアサーションへのポインタを含む.

### **Asymmetric Keys**

### 非対称鍵

公開鍵とプライベート鍵から成る２種類の関連した鍵. 暗号化と復号, 署名⽣成と署名検証など, 補完的な処理の実行に⽤いられる.

### **Attack**

### 攻撃

認可されていないエンティティが, 検証者や RP をだまして加入者本人であると信じ込ませようとする試み.

### **Attacker**

### 攻撃者

システムを危険にさらすために悪意をもって行動する主体で, 部内者も含む.

### **Attribute**

### 属性

⼈や物に与えられた性質や特徴.

### **Attribute Bundle**

### 属性バンドル

パッケージ化された属性の集合で, 一般的にアサーションに含まれる. 属性バンドル により, RP は最も関連性の高い必要な属性を IdP から簡単に受け取ることができる. 属性バンドルは OpenID Connect のスコープ [OpenID Connect Core 1.0] と同義.

### **Attribute Reference**

### 属性参照

必ずしも身元情報を含まず, 書式に関係なく加入者のプロパティを明示するステートメント. 例えば “誕生日” という属性に対しては, 記述は “18歳以上” や “12月生まれ” などにできる.

### **Attribute Value**

### 属性値

書式に関係なく加入者のプロパティを明示する完全なステートメント. 例えば “誕生日” という属性に対しては, “12/1/1980” や “December 1, 1980” などを値にできる.

### **Authenticate**

### 認証する

認証を参照.

### **Authenticated Protected Channel**

### 認証済み保護チャネル

承認された暗号化技術を⽤いて暗号化された通信チャネルで, 接続元（クライアント）は接続先（サーバー）を認証している. 認証済み保護チャネルは機密性を保護して MitM を防ぎ, ユーザーの認証プロセスでよく使用されている. 例としては, 接続先が提⽰した証明書を接続元が検証するトランスポートレイヤセキュリティ (TLS) [BCP 195] がある. 特に指定がない限り, 認証済み保護チャネルではサーバーがクライアントを認証する必要はない. サーバーの認証は, サーバーを個別に用いるのではなく, 多くの場合信頼されたルート機関で終わる証明書チェーンで完了する.

### **Authentication**

### 認証

ユーザー, プロセス, デバイスなどの身元情報を検証すること. 多くの場合, システムリソースへのアクセスを許可する際の前提条件となる.

### **Authentication Factor**

### 認証ファクタ

*本人が知っていること*, *本人が持っているもの, 本人の特徴によるもの*という3種類の認証ファクタがある. すべての認証コードには1つ以上の認証ファクタがある.

### **Authentication Intent**

### 認証意図

ユーザーが認証フローに関わることを要求するプロセスを含めることにより. 認証要求者が認証または再認証する意図を確認するプロセス. 認証コードによっては, 認証意図をその処理の⼀部として設定することもあれば（例えば OTP デバイス）, ボタンを押させるなどといった特定のステップを要求するものもある. 認証意図は,加入者が知らない間にエンドポイントで攻撃者を認証させるプロキシとしてマルウェアが使用されるケースに対抗する措置となる.

### **Authentication Protocol**

### 認証プロトコル

認証要求者と検証者の間でやりとりされる定義された⼀連のメッセージで, 認証要求者が自らの身元情報を確立するために１つ以上の正規の認証コードを所有し管理していることを立証する. そして, 必要に応じて, 認証要求者が意図した検証者と通信していることを立証する.

### **Authentication Protocol Run**

### 認証プロトコル実行

認証要求者と検証者との間で交わされる, 認証（または認証失敗）に至るメッセージ交換.

### **Authentication Secret**

### 認証シークレット

認証プロトコルにおいて攻撃者が加入者になりすますために利⽤できる可能性のあるシークレット値の総称.

認証シークレットは*短期認証シークレット*と*長期認証シークレット*に分類することができ, 前者は攻撃者が限定的な期間のみ利⽤可能なもの, 後者は⼿動でリセットされるまで攻撃者が加入者になりすますことができるものを指す. 認証コードシークレットは長期認証シークレットの代表例であり, 認証コード出⼒値は認証コードシークレットと異なると, ⼀般的には短期認証シークレットになる.

### **Authenticator**

### 認証コード認証要求者が所有し管理するもの（典型的な例としては暗号モジュールやパスワード）で, 認証要求者の身元情報を認証するために⽤いられる. SP 800-63 の旧版では*トークン*と呼ばれていた.

### **Authenticator Assurance Level (AAL)**

### 認証コード保証レベル (AAL)

認証プロセスの強度を⽰すカテゴリ.

### **Authenticator Output**

### 認証コード出力値

認証コードによって⽣成される出⼒値. 要求に応じて正当な認証コード出力値を⽣成できることは, 認証要求者が認証コードを所有し管理していることを証明する. 検証者へ送信されるプロトコルメッセージは認証コード出力値によって異なるが,メッセージに明⽰的に出力値が含まれることもそうでないこともある.

### **Authenticator Secret**

### 認証コードシークレット

認証コードに含まれるシークレット値.

### **Authenticator Type**

### 認証コードタイプ

共通の特徴を持つ認証コードのカテゴリ. 単⼀の認証ファクタを持つタイプと, 2つの認証ファクタを持つタイプがある.

### **Authenticity**

### 信憑性

データが意図された情報源から得られたことを示すプロパティ.

### **Authoritative Source**

### 信頼元

発行元の正確な情報にアクセスできるか, その検証済みコピーを所有しているエンティティ. これにより身元情報の検証で申請者の提出した身元情報の証明の有効性をCSP が確認できる. 発行元が信頼元になることもある. 多くの場合, 信頼元は, 身元情報の検証フェーズの前に, エージェントや CSP のポリシー決定によって確定される.

### **Authorize**

### 認可する

アクセスを許可するための決定. 通常は主体の属性を評価して⾃動的に判断される.

### **Back-Channel Communication**

### バックチャネル通信

ブラウザなどを介したリダイレクトを使用せずにダイレクト接続に依存する2つのシステム間の通信（標準プロトコルレベルのプロキシを許可）. HTTP のリクエストとレスポンスを使用して実現される.

### **Bearer Assertion**

### ベアラアサーション

主体が身元情報を証明するために提⽰するアサーションで, アサーションを保有していること⾃体がアサーション持参⼈（ベアラ）の身元情報の十分な証明となる.

### **Binding**

### 結び付け

加入者の身元情報と認証コードまたは所定の加入者セッションの間の関連付け.

### **Biometrics**

### 生体認証

個⼈の⾏動や⽣体情報に基づいて個⼈を⾃動認識すること.

### **Challenge-Response Protocol**

### チャレンジ/レスポンスプロトコル

検証者が認証要求者に対してチャレンジ（通常はランダム値やノンス）を送信し, 認証要求者はそれをシークレットと結合（チャレンジと共有シークレットを⼀緒にハッシュするか, チャレンジにプライベート鍵による処理を適用）してレスポンスを⽣成し, 検証者に送り返すための認証プロトコル. 検証者は認証要求者が⽣成したレスポンスを自分だけで検証（チャレンジと共有シークレットのハッシュを再計算してレスポンスと⽐較するか, レスポンスに対して公開鍵による処理を実施）し, 認証要求者がシークレットを所有し管理していることを確認できる.

### **Claimant**

### 認証要求者

1つ以上の認証プロトコルを用いて身元情報が検証される主体.

### **Claimed Address**

### 主張された住所

主体が⾃分に到達可能であると主張する物理的場所で, 個人の居住地の住所が含まれるが, 郵便の届く住所を含めることもできる.

例えば, 米国に居住する外国籍パスポートの所持者は, 身元情報の検証プロセスで住所を提供する必要がある. その場合の住所は, “記録上の住所” ではなく “主張された住所” になろう.

### **Claimed Identity**

### 主張された身元情報

申請者による未検証で未確認な属性の申告.

### **Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)**

Web フォームを使用しているのが⼈間か⾃動化されたエージェントかを区別するためにフォームに追加する対話的な機能. 一般的に, 歪んだ画像や⾳声に対応するテキストの⼊⼒を要求する.

### **Credential**

### 認証情報

１つまたは複数の識別⼦を使用して, 加入者が所有し管理している少なくとも１つの認証コードにその身元情報と（任意の）追加属性を厳密に結び付けたオブジェクトまたはデータ構造.

⼀般的に, 認証情報の使用は, 加入者が認証情報を保持していることを想定しているが, このガイドラインでは, 加入者の認証コードと身元情報の結び付けを確⽴する CSP が保持する電⼦レコードも指す.

### **Credential Service Provider (CSP)**

### 認証情報サービスプロバイダ (CSP)

加入者の認証コードを発⾏または登録し, 加入者に電⼦的な認証情報を発⾏する信頼されたエンティティ. CSP は独⽴した第三者であることも, 自ら使用するために認証情報を発行することもある.

### **Cross-site Request Forgery (CSRF)**

### クロスサイトリクエストフォージェリ (CSRF)

RP に対して認証されている加入者がセキュアなセッションを通して攻撃者の Web サイトに接続すると発⽣する攻撃で, 加⼊者は知らない間に好ましくないアクションを RP 上で実⾏してしまう.

例えば, ある銀⾏のサイトが CSRF 攻撃に対して脆弱である場合, 加入者は Web メールの悪意あるリンク先を参照するだけで, 銀⾏に接続された別のブラウザウィンドウで知らないうちに多額の資⾦移動を許可してしまう可能性がある.

### **Cross-site Scripting (XSS)**

### クロスサイトスクリプティング (XSS)

攻撃者が不正なコードを Web サイトに挿入できる脆弱性. こうしたスクリプトはターゲットの Web サイトで⽣成されるスクリプト権限を取得するため, Web サイトとクライアント間のデータ転送の機密性と完全性を侵害する. Web サイトが脆弱な場合, ユーザーが⼊⼒したデータを実行できないようにサニタイズが実行されずにリクエストや入力フォームからデータが表示される.

### **Cryptographic Authenticator**

### 暗号認証コード

暗号鍵をシークレットとする認証コード.

### **Cryptographic Key**

### 暗号鍵

復号, 暗号化, 署名⽣成, 署名検証などの暗号処理を管理するために⽤いられる値. これらのガイドラインでは, NIST SP 800-57 Part 1 の表 2 にある最低限の要件を満たさなければならない.

非対称鍵と対称鍵も参照.

### **Cryptographic Module**

### 暗号モジュール

ハードウェア, ソフトウェアそして/またはファームウェアのセットで, 承認されたセキュリティ機能（暗号アルゴリズムと鍵⽣成を含む）を実装するもの.

### **Data Integrity**

### データの完全性

認可されていないエンティティによってデータが変更されていないというプロパティ.

### **Derived Credential**

### 導出した認証情報

事前に発⾏された認証情報に関連付けられた認証コードを所有/管理している証明に基づいて発⾏される認証情報. これにより, 身元情報の検証プロセスを繰り返す必要がなくなる.

### **Digital Authentication**

### デジタル認証

情報システムに電子的に提示されるユーザーの身元情報の信頼性を確⽴するプロセス. SP 800-63 の旧版では *電子認証 (Electronic* *Authentication)* と呼ばれていた.

### **Digital Signature**

### デジタル署名

プライベート鍵を⽤いてデータにデジタル署名を⾏い, 公開鍵を⽤いて署名検証を⾏う, 対称鍵による操作. デジタル署名は信憑性の保護, 完全性の保護, 否認の防⽌を提供するが, 機密性の保護は提供しない.

**Disassociability**

非関連付け性

NISTIR8062 に基づき, システムの運用要件を超えて個人やデバイスを関連付けることなくPII やイベントを処理できること.

### **Diversionary**

### 陽動

KBV で提供されたすべての答えが正しくなく, 申請者に “上記以外” といった選択肢を与えるような多項選択式質問.

### **Eavesdropping Attack**

### 盗聴攻撃

攻撃者が認証プロトコルを受動的に傍受し, その後の積極的攻撃で認証要求者になりすますための情報を入手する攻撃.

### **Electronic Authentication (E-Authentication)**

### 電子認証（E-認証）

*デジタル認証を* 参照.

### **Enrollment**

### 登録

申請者が CSP の加入者となるために申し込み, CSP がその身元情報を検証するプロセス.

### **Entropy**

### エントロピー

攻撃者がシークレット値を突き止める際の不確実性の尺度. エントロピーは通常ビットで表現される. *n* ビットの エントロピーを持つ値は, 一様に分散した*n* ビットの乱数値と同等の不確実性を持つ.

### **Federal Information Processing Standard (FIPS)**

### 連邦情報処理規格 (FIPS)

米国商務省は, 情報技術管理改革法（Information Technology Management Reform Act（一般法104-106））に 基 づき, 標準技術研究所 (National Institute of Standards and Technology, NIST) が連邦政府機関のコンピュータシステムのために開発する標準およびガイドラインを承認している. これらの標準とガイドラインは NIST によって FIPS として発⾏され, 政府機関で横断的に使われている. セキュリティや相互運⽤性といった強制⼒のある連邦政府の要求事項がある場合と, 許容可能な業界標準やソリューションが存在しない場合に, NIST は FIPS を開発する. 詳細については参考資料を参照.

FIPS 文書は FIPS ホームページ ([http://www.nist.gov/itl/fips.cfm)](http://www.nist.gov/itl/fips.cfm)%20) から入手できる.

### **Federation**

### 連携

⼀連のネットワークシステム間で身元情報と認証情報の譲渡を許可するプロセス.

### **Federation Assurance Level (FAL)**

### 連携保証レベル (FAL)

認証情報と属性情報（妥当な場合）を RP に伝達するために連携で使用するアサーションプロトコルを記述するカテゴリ.

### **Federation Proxy**

### 連携プロキシ

IdP のセットに対して論理的に RP として動作し, RP のセットに対して論理的に IdP として動作する, 2つのシステムを単一のコンポーネントでブリッジするコンポーネント. “ブローカー” と呼ばれることもある.

### **Front-Channel Communication**

### フロントチャネル通信

ブラウザなどを介して 2つのシステム間でリダイレクトを⽤いて⾏われる通信. これはメッセージ受信者がホストする URL に HTTPクエリパラメータを追加することで実現される.

### **Hash Function**

### ハッシュ関数

任意⻑のビット列を固定⻑のビット列に変換する関数. 承認されたハッシュ関数は以下のプロパティを満たす.

⼀⽅向性 - 事前に指定された任意の出⼒になるどのような⼊⼒も特定することが計算上困難である.

衝突困難性 - 同じ出⼒となる任意の2つの異なる⼊⼒を特定することが計算上困難である.

### **Identity**

### 身元情報

特定の文脈において, 主体を一意に記述する属性または属性 のセット.

### **Identity Assurance Level (IAL)**

### 身元情報保証レベル (IAL)

申請者が主張する身元情報が本物であることの信頼度を示すカテゴリ.

### **Identity Evidence**

### 身元情報の証拠

申請者が主張する身元情報を裏付けるために提出する情報または書類. 証拠となるものは物理的存在（例えば免許証）のことも, デジタルな存在（例えば CSP が申請者を認証した上で作成して発⾏したアサーション）のこともある.

### **Identity Proofing**

### 身元情報の検証

CSP が個人に関する情報を収集, 確認, 検証するプロセス.

### **Identity Provider (IdP)**

### 身元情報プロバイダ (IdP)

加入者の主要な認証情報を管理し, その情報に由来するアサーションを発⾏する主体. この文書シリーズでは, 一般に CSP として論じる.

### **Issuing Source**

### 発行元

身元情報の証拠として利⽤できるデータやデジタルな証拠（アサーションなど）や, 紙の書類の生成に責任を負う権限機関.

### **Kerberos**

### ケルベロス

MIT で開発され幅広く利⽤されている認証プロトコル. “古典的” なケルベロスでは, ユーザーは秘密のパスワードをキー配布センター (KDC) で共有する. ユーザー Alice はユーザー Bob と通信するため KDC に対して認証し, KDC は認証に使用する “チケット” を Bob に発⾏する.

詳細は [SP 800-63C (sp800-63c.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.html) セクション 11.2 を参照.

### **Knowledge-Based Verification (KBV)**

### 知識ベース検証 (KBV)

主張された身元情報と関連付けられている個人情報の知識に基づいて身元情報を検証する⽅法. 知識ベース認証 (KBA) や知識ベースプルーフィング (KBP) とも呼ばれる.

### **Manageability**

### 管理可能性

### NISTIR8062 に基づいた, 個人を特定できる情報の変更, 削除, 選択的開示を含めたきめ細かい管理を提供する能力.

### **Man-in-the-Middle Attack (MitM)**

### 中間者攻撃 (MitM)

通信する2つの主体の間に攻撃者が割り込み, データを傍受したり改竄したりする攻撃. 攻撃者は, 認証関連では認証要求者と検証者の間に, 登録関連では登録者と CSP の間に, 認証コード結び付け関連では加入者と CSP の間に割り込む.

### **Memorized Secret**

### 記憶シークレット

加入者が記憶するか記憶できることを前提とした, ⽂字列からなる認証コードのタイプ. 加入者は*知っていること*を認証プロセスの一部として利⽤できる.

### **Message Authentication Code (MAC)**

### メッセージ認証コード (MAC)

データの偶発的変更と意図的変更を検知するために対称鍵を使用する, 暗号理論に基づくデータのチェックサム. MAC は 信憑性と完全性の保護を⾏うが, 否認防⽌は⾏わない.

### **Mobile Code**

### モバイルコード

一般的に提供元から別のコンピュータシステムに転送されて実⾏されるコード. 転送は多くの場合ネットワークを介するが (例えば, Web ページに埋め込まれた JavaScript) が, 物理的なメディアを介することもある.

### **Multi-Factor**

### マルチファクタ

認証のために１つ以上の明確な認証ファクタを要求する認証システムや認証コードの特性. マルチファクタは, １つ以上のファクタを提供する単⼀の認証コードを⽤いてもよいし, 異なるファクタを提供する複数の認証コードを組み合わせてもよい.

３種類の認証ファクタは, *本人が知っていること, 本人が持っているもの, 本人の特徴によるもの*である.

### **Multi-Factor Authentication (MFA)**

### マルチファクタ認証 (MFA)

認証のために１つ以上の明確な認証ファクタ を要求する認証システム. マルチファクタ認証は単⼀のマルチファクタ認証コードを⽤いてもよいし, 異なるファクタを提供する複数の認証コードを組み合わせてもよい.

３種類の認証ファクタは, *本人が知っていること, 本人が持っているもの, 本人の特徴によるもの*である.

### **Multi-Factor Authenticator**

### マルチファクタ認証コード

１つ以上の明確な認証ファクタを提供する認証コード. 例としてはデバイスをアクティベートするのに必要な生体認証センサーを備えた暗号認証デバイスがある.

### **Network**

### ネットワーク

オープンな通信媒体でインターネットがその代表例. ネットワークは認証要求者とその他の関係者の間でメッセージを伝達するために⽤いられる. 特に明記しない限りセキュリティを前提としていないため, 主体（認証要求者, 検証者, CSP, RP など）間のいずれの地点においてもオープンであり, 積極的攻撃（なりすまし, 中間者攻撃, セッションハイジャックなど）と受動的攻撃（盗聴など）を受けやすいことが想定される.

### **Nonce**

### ノンス

セキュリティプロトコルで利⽤され, 同じキーによる繰り返しを許さない値. 例えば, チャレンジ/レスポンス認証プロトコルでチャレンジとして使用されるノンスは, 認証キーが変更されるまで繰り返されてはならない (SHALL NOT). そうしないと, リプレイ攻撃を許す可能性がある. ノンスをチャレンジとして利⽤することは, チャレンジをランダムにすることとは異なる要件である.ノンスは必ずしも予測不可能である必要はないからである.

### **Offline Attack**

### オフライン攻撃

攻撃者が自ら選択したシステム内で解析できるデータを入手する攻撃で, 一般的には, 認証ロトコルのやりとりを盗聴したり, システムに侵⼊してセキュリティファイルを盗んだりする.

### **Online Attack**

### オンライン攻撃

認証プロトコルに対する攻撃で, 攻撃者は正当な検証者に対して認証要求者になりすますか, 認証チャネルを積極的に改竄する.

### **Online Guessing Attack**

### オンライン類推攻撃

攻撃者が認証コード出力の取りうる値を類推してログオンを繰り返し試みる攻撃.

### **Pairwise Pseudonymous Identifier**

### ペア匿名識別子

CSP がそれぞれ特定の RP に対して⽣成する, 不透明で推測不可能な加入者の識別⼦. この識別⼦を知っていて使用できるのは. 単一のペアとなる CSP と RP だけである.

### **Passive Attack**

### 受動的攻撃

認証プロトコルに対する攻撃で, 認証要求者と検証者の間をネットワーク経由でやり取りされるデータが傍受されるが, 改竄はされない（つまり盗聴）.

### **Passphrase**

### パスフレーズ

認証要求者が⾃⾝の身元情報を認証するのに使用する, 単語列や⽂字列からなる記憶シークレット. 使用についてはパスワードと同じであるが, セキュリティを強化するためにパスワードよりも長い場合が多い.

### **Password**

### パスワード

*記憶シークレットを*参照.

### **Personal Data**

### 個人データ

*個人を特定できる情報を*参照.

### **Personal Identification Number (PIN)**

### 暗証番号 (PIN)

通常は10進数の数値のみで構成される記憶シークレット.

### **Personal Information**

### 個人情報

*個人を特定できる情報* 参照.

### Personally Identifiable Information (PII)

### 個人を特定できる情報 (PII)

OMB Circular A-130 で定義されているように, 個人を特定できる情報とは. 個⼈の身元情報を識別したり追跡したりするために⽤いることができる情報である. こうした情報は単体のものもあれば, 特定の個⼈に関連付けられているか関連付けが可能なその他の情報と組み合わせたものもある.

### **Pharming**

### ファーミング

DNS（ドメイン名システム）のようなインフラサービスを侵害して, 加入者を偽の検証者/RP へ誘導し, 機密情報の開示, 有害なソフトウェアのダウンロード, 詐欺行為の加担などを加入者にさせる攻撃.

### **Phishing**

### フィッシング

加入者を（主に Eメールを通して）偽の検証者/RP に誘導し, 本物の検証者/RP に対してその加入者になりすますために情報を騙し取る攻撃.

### **Possession and Control of an Authenticator**

### 認証コードの所有と管理

認証プロトコルで認証コードをアクティベートして利⽤する能⼒.

### **Practice Statement**

### 実施規定

認証プロセスの当事者（CSP や検証者）が従う実施内容を正式に表明した⽂書. 通常, 当事者のポリシーと実施内容が記述されており, 法的拘束⼒を持たせることができる.

**Predictability**

予測可能性

NISTIR8062: PII と, 情報システムによる PII の処理に関して, 個人, 所有者, 処理者が確実に予測できること.

### **Private Credentials**

### プライベート認証情報

内容が認証コードの改竄に使用できるため, CSP が開示できない認証情報.

### **Private Key**

### プライベート鍵

デジタル署名や復号に使用する非対称鍵ペアのシークレットな部分.

**Processing**

処理

NISTIR8062: PII の収集, 保有, 記録, 生成, 変更, 使用, 開示, 破棄を含むがそれに限定されない, PII に実施される操作または一連の操作.

### **Presentation Attack**

### プレゼンテーション攻撃

生体認証システムの運⽤妨害を⽬的とする, 生体認証データ読取りサブシステムに対するなりすまし.

### **Presentation Attack Detection (PAD)**

### プレゼンテーション攻撃検知 (PAD)

プレゼンテーション攻撃の⾃動判定. 生体検知と呼ばれるプレゼンテーション攻撃の判定方法のサブセットは, 解剖学的特徴や不随意または随意的反応を測定して分析し, 生体認証サンプルがその時点で⽣体から直接読み取られているかどうかを判定する.

### **Protected Session**

### 保護されたセッション

2人の参加者間でやりとりされるメッセージを, セッションキーと呼ばれる共有シークレットのセットを⽤いて暗号化して完全性を保護するセッション.

このセッションで参加者がセッションキーの他に1つ以上の認証コードを所有していることを証明し, もう⼀⽅の参加者がその認証コードに関連付けられた身元情報を検証できる場合, 参加者は*認証されている*と言われる. 両方の参加者が認証される場合, 保護されたセッションは*相互認証されている*と言われる.

### **Protected Session**

### 保護されたセッション

認証されて保護されたチャネルで確⽴されたセッション.

### **Pseudonym**

### 匿名

正式名以外の名前.

### **Pseudonymity**

### 匿名性

主体の識別に匿名を⽤いること.

### **Pseudonymous Identifier**

### 匿名識別子

RP は加入者について何も推測できないが, 加入者の主張する身元情報に複数のやりとりを関連付けることができる, 意味はないが単一の番号.

### **Public Credentials**

### 公開認証情報

認証コードを改竄しない方法で結び付けを記述する認証情報.

### **Public Key**

### 公開鍵

署名の検証やデータの暗号化に使用する, 非対象鍵ペアの公開部分.

### **Public Key Certificate**

### 公開鍵証明書

加入者の識別⼦を公開鍵と結び付ける認証局 (CA) のプライベート鍵によりデジタル署名されて発行されるデジタル文書で, この証明書で識別される加入者だけがプライベート鍵を管理して利用することを示す. [[RFC 5280] (sp800-63b.ja.html#RFC5280)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html#RFC5280) も参照.

### **Public Key Infrastructure (PKI)**

### 公開鍵基盤(PKI)

証明書と公開鍵/プライベート鍵のペアを管理する⽬的で利⽤される, ポリシー, プロセス, サーバープラットフォーム, ソフトウェア, ワークステーションなどのセットで, 公開鍵証明書の発⾏, 管理, 失効が処理できる.

### **Re-authentication**

### 再認証

使用が延長されたセッションにおいて, 加入者が引き続き存在して認証を受ける意思があることを確認するプロセス.

### **Registration**

### 登録

登録 (Enrollment)を参照.

### **Relying Party (RP)**

### 証明書利用者 (RP)

加入者の認証コードと認証情報や, 認証要求者の身元情報に関する検証者のアサーションを信頼して, 一般的にトランザクションを処理したり情報やシステムへのアクセスを許可したりするエンティティ.

### **Remote**

### リモート

（*リモート認証 やリモートトランザクションといった文脈において）* 単⼀組織によるセキュリティ管理策ではエンドツーエンドで確実な保護ができないネットワーク接続デバイス間の情報交換.

### **Replay Attack**

### リプレイ攻撃

攻撃者が事前に入手した（正当な認証要求者と検証者との間の）メッセージを, 検証者に対して認証要求者（またはその逆）になりすますために再送する攻撃.

### **Replay Resistance**

### リプレイ耐性

リプレイ攻撃に対抗するための認証プロセスの特性. 一般的には, 特定の認証にのみ有効な認証コード出力値を使用する.

### **Restricted**

### 制限付き

不正な受け入れの補足的なリスクを関連付けて追加要件を要求する認証コードのタイプ, クラス, インスタンス.

### **Risk Assessment**

### リスク評価

システムの運⽤に起因する, 組織の運営（業務, 機能, イメージ, 評判を含む）, 組織の資産, 個⼈, 他の組織に対するリスクを, 特定, 推定, 優先順位付けするプロセス. これはリスク管理の⼀部であり, 脅威/脆弱性分析を行い, 計画済みか実施中のセキュリティ管理によりリスク軽減を考察する. リスク分析と同義.

### **Risk Management**

### リスク管理

組織の運営（業務, 機能, イメージ, 評判を含む）, 組織の資産, 個⼈, 他の組織に対する情報セキュリティのリスクを管理するプログラムと補助的プロセスで, (i) リスク関連活動の状況を確立し, (ii) リスクを評価し, (iii)リスクが確定されれば即座に対応し, (iv) 継続的にリスクをモニタリングする活動を含む.

### Salt

### ソルト

暗号プロセスで⽤いられる秘密でない値で, 通常１つのインスタンスの計算結果を攻撃者が再利⽤できないことを確実にするために使用する.

### **Secure Sockets Layer (SSL)**

### セキュアソケットレイヤ (SSL)

*トランスポートレイヤセキュリティ(TLS)* を参照.

### **Session**

### セッション

加入者とエンドポイントである RP または CSP の間の継続的な対話で, 認証イベントにより開始され,セッション終了イベントにより終了する. セッションは, RP や CSP に対して加入者のソフトウェア（ブラウザ, アプリケーション, OS）が加入者の認証情報 の代わりとして提⽰することができるセッションシークレットの使用によって関連付けられる.

### **Session Hijack Attack**

### セッションハイジャック攻撃

認証要求者と検証者の間で認証のやりとりが確立したのち, 攻撃者が両者の間に割り込む攻撃. 攻撃者は検証者に対して加入者 を装ったり, 加入者に対して検証者のふりをしたりして, セッション中のデータ交換をコントロールできる. 攻撃者は, 認証要求者と RP の間のセッションも同様に攻撃できる.

### **Shared Secret**

### 共有シークレット

加入者と検証者が知っていて認証で使用されるシークレット.

### **Side-Channel Attack**

### サイドチャネル攻撃

物理的な暗号システムからの情報漏洩によって可能となる攻撃. 攻撃に悪用される特性は, タイミング, 消費電⼒, 電磁波放出, ⾳響放射が考えられる.

### **Single-Factor**

### 単一ファクタ

認証のために単⼀の認証ファクタ（本人が知っていること, 本人が持っているもの, 本人の特徴であるもの）だけを要求する認証システムや認証コードの特性.

### **Social Engineering**

### ソーシャルエンジニアリング

⼈をだまして要注意情報を開示させたり, 不正にアクセス権を入手したり, ⼈を信頼させた上で詐欺を働く行為.

### **Special Publication (SP)**

### 特別出版物 (SP)

NIST が発⾏する出版物の⼀形態. 特に SP 800 シリーズは, コンピュータセキュリティ分野における情報技術研究所 (Information Technology Laboratory, ITL) の研究活動, ガイドライン, 公共福祉のための⽀援活動と, 産業・政府・学術組織との共同作業のレポートである.

### **Subject**

### 主体

⼈, 組織, デバイス, ハードウェア, ネットワーク, ソフトウェア, サービスなど.

### **Subscriber**

### 加入者

CSP から認証情報や認証コードを受け取っている主体.

### **Symmetric Key**

### 対称鍵

暗号化と復号の両方の処理に使用される暗号鍵で, 例えば暗号化と復号やメッセージ認証コードの生成と検証に使用される.

### **Token**

### トークン

認証コードを参照.

### **Token Authenticator**

### トークン認証コード

認証コード出力値を参照.

### **Token Secret**

### トークンシークレット

認証コードシークレットを参照.

### **Transaction**

### トランザクション

ビジネスやプログラムの⽬標を⽀援するシステムとユーザーの間の個別のイベント. 政府のデジタルシステムではトランザクションの複数のカテゴリやタイプを持たせることができ, デジタルの身元情報のリスク評価全体で個別の分析を要求することができる.

### **Transport Layer Security (TLS)**

### トランスポートレイヤセキュリティ(TLS)

ブラウザや Web サーバーに広く実装されている認証およびセキュリティプロトコルで [RFC 5246] に定義されている. TLS はより古い SSL プロトコルと似ており, 実質的に TLS1.0 は SSL version 3.1 といえる. TLS 実装の選択と使用のためのガイドラインである NIST SP 800-52 [SP 800-52] は, 政府のアプリケーションでどのように TLS を使用すべきかを定めている.

### **Trust Anchor**

### トラストアンカー

信頼された他のエンティティ（例えば公開鍵証明書）によって保証されるのではなく, ハードウェアやソフトウェエアに直接埋め込まれていたり, アウトオブバンドな手段によりセキュアに提供されたりすることで信頼される公開鍵や対称鍵を指す.そのスコープを制限する名称やポリシー制約を持たせることもできる.

### **Usability**

### ユーザビリティ

ISO/IEC 9241-11: 製品の特定の利用において, 特定のユーザーが製品を効果的, 効率的かつ⼗分に特定の⽬的を果たすために利⽤できる範囲.

### **Verifier**

### 検証者

認証プロトコルを利⽤して, 認証要求者が1つまたは2つの認証コードを所有し管理していることを検証し, 認証要求者の身元情報を検証するエンティティ. 認証コードと身元情報をリンクした認証情報を検証者が確認してそのステータスをチェックする必要がある場合もある.

### **Verifier Impersonation**

### 検証者なりすまし

一般的に, 正規の検証者に対して加入者を装うために使用できる情報を入手する目的で攻撃者が認証プロトコルで検証者になりすますシナリオ. SP 800-63 の旧版では, 検証者なりすましに耐性を持つ認証プロトコルは, “強力なMitM 耐性 (strongly MitM resistant)” として説明されていた.

**Supervised Remote Proofing**

監視リモート検証

個人識別情報に関してリモートセッションを物理的で直接的な検証プロセスと等しいと見なすことができる十分な信頼性を提供する物理的, 技術的, 手続き的措置を使用する, 個人識別情報のリモート検証プロセス

### **Weakly Bound Credentials**

### 結び付きの弱い認証情報

認証情報を無効化することなく変更できる⽅法で加入者と結び付けられた認証情報.

### **Zeroize**

### ゼロ埋め

データを破壊し復元できないようにするために, ゼロ値のビットだけで構成されるデータで記憶域を上書きすること. これとよく対比される削除とは, データそのものを破壊するのではなくファイルシステム上のデータへの参照を単に破壊することである.

### **Zero-Knowledge Password Protocol**

### ゼロ知識パスワードプロトコル

認証要求者が検証者にパスワードを提示しなくても本人であることを証明できる, パスワードベースの認証プロトコル. 例として, EKE, SPEKE, SRP がある.

## **略語**

これらのガイドラインで選択されている略語を以下に定義する.

|  |  |
| --- | --- |
| **略語** | **用語** |
| ABAC | 属性ベースのアクセスコントロール |
| AAL | 認証コード保証レベル |
| AS | 認証サーバー |
| CAPTCHA | Completely Automated Public Turing test to tell Computer and Humans Apart |
| CSP | 認証情報サービスプロバイダ |
| CSRF | クロスサイトリクエストフォージェリ |
| XSS | クロスサイトスクリプティング |
| DNS | ドメイン名システム |
| EO | 行政命令 |
| FACT Act | 2003年信用取引の公正・適性化に関する法律 |
| FAL | 連携保証レベル |
| FEDRAMP | リスクと認証に関する連邦マネージメントプログラム |
| FMR | 偽一致率 |
| FNMR | 偽不一致率 |
| FIPS | 連邦情報処理規格 |
| FISMA | 連邦情報セキュリティ現代化法 |
| IAL | 身元情報保証レベル |
| IM | 身元情報マネージャ |
| IdP | 身元情報プロバイダ |
| IoT | モノのインターネット |
| ISO/IEC | 国際標準化機構/国際電気標準会議 |
| JOSE | JSON Object Signing and Encryption |
| JSON | JavaScript オブジェクト記法 |
| JWT | JSON Web トークン |
| KBA | 知識ベース認証 |
| KBV | 知識ベース検証 |
| KDC | キー配布センター |
| LOA | 保証レベル |
| MAC | メッセージ認証コード |
| MitM | 中間者 |
| MitMA | 中間者攻撃 |
| MFA | マルチファクタ認証 |
| N/A | 適用なし |
| NARA | 米国国立公文書記録管理局 |
| OMB | 米国行政管理予算局 |
| OTP | ワンタイムパスワード |
| PAD | プレゼンテーション攻撃検知 |
| PHI | 個人健康情報 |
| PIA | プライバシー影響評価 |
| PII | 個人を特定できる情報 |
| PIN | 暗証番号 |
| PKI | 公開鍵基盤 |
| PL | 公法 |
| PSTN | 公衆回線網 |
| RA | 登録局 |
| RMF | リスク管理フレームワーク |
| RP | 証明書利用者 |
| SA&A | Security Authorization & Accreditation |
| SAML | セキュリティアサーションマークアップ言語 (Security Assertion Markup Language) |
| SAOP | プライバシー上級責任者 (Senior Agency Official for Privacy) |
| SSL | セキュアソケットレイヤ |
| SMS | ショートメッセージサービス |
| SP | 特別出版物 |
| SORN | 記録システム通知 (System of Records Notice) |
| TEE | 信頼された実行環境 (Trusted Execution Environment) |
| TGS | チケット発行サーバー |
| TGT | チケット発行チケット |
| TLS | トランスポートレイヤセキュリティ |
| TPM | 信頼プラットフォームモジュール |
| VOIP | ボイスオーバー IP |

[Privacy Policy (http://www.nist.gov/public\_affairs/privacy.cfm#privpolicy) | Security Notice (http://www.nist.gov/public\_affairs/privacy.cfm#secnot) |](http://www.nist.gov/public_affairs/privacy.cfm#secnot) Access[ibility Statemett (http://www.nist.gov/public\_affairs/privacy.cfm#Accesstate)](file:///C:\Users\shiokawa\AppData\Local\Temp\B2Temp\Attach\ibility%20Statemett%20(http:\www.nist.gov\public_affairs\privacy.cfm#Accesstate))

| [Send feedback (https://github.com/米国nistgov/800-63-3/issues/)](https://github.com/usnistgov/800-63-3/issues/) [ (/800-63-3/comment\_help.html)](https://openid-foundation-japan.github.io/800-63-3/comment_help.html)