資料2

DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン

本人確認ガイドラインの改定に向けた有識者会議
令和6年度（2024年度）第1回

論点協議資料

令和6年9月　　デジタル庁　トラストタスクフォース

デジタル庁
Digital Agency

論点一覧

協議予定回	論点概要
第1回 /第2回	**論点1. NIST SP 800-63-4 2pdから反映を検討すべき事項について** • 2024年8月21日に公開された2nd public draft（2pd）での変更点を踏まえ、本人確認ガイドラインへの反映を検討すべき事項としてどのようなものがあるか。 （ウォレットモデル、新たなIALとRoles/Types、フィッシング耐性の強化、ウォレットを用いる場合の対策要件 等）
第2回	**論点2. フェデレーション保証レベル（仮称）と対策基準について** • NIST FALに相当するフェデレーション保証レベル（仮称）と対策基準をどのように定義すべきか。 （3段階のレベルが必要なのか、1段階や2段階でもよいのではないか、など）
	論点3. 身元確認において本人確認書類に求める対策基準について • 身元確認保証レベル3/2/1に対応する本人確認書類の要件（ICチップの有無、顔写真の有無など）は、我が国で普及している本人確認書類の種類等を踏まえてどのような要件をすべきか。 • 公平性確保等の観点から、ガイドラインにおいて代替手法の基準等を定義すべきか。
	論点4. スマートフォンに搭載された本人確認書類や資格証明等の扱いについて • 身元確認や当人認証において、スマートフォンに搭載された本人確認書類や資格証明情報等を扱う場合、どのようなリスクや留意事項、特有の対策基準等が考えられるか。

論点1. NIST SP 800-63-4 2pdから反映を検討すべき事項について

論点概要

- 2024年8月21日に公開されたSP 800-63-4 2nd public draft（2pd）では、initial public draft（ipd）から更に多数の変更が加えられた。
- 2pdでの変更点を踏まえ、本人確認ガイドラインへの反映を検討すべき事項としてどのような点が考えられるか、意見交換を実施いただきたい。

※ 本議論では2pdの改定内容を踏まえ、「本人確認ガイドラインの改定方針に、何をどのように反映すべきか」という観点からの議論をお願いいたします。

特に協議いただきたいポイント

- 次頁以降を参照ください。

特に議論いただきたい個別の論点

	2pdでの主な変更点	特に議論いただきたい個別論点
63-4 Base Volume	❶ ウォレットモデル（“ Federated Model With Subscriber-Controlled Wallet” ）	• 本人確認ガイドラインではどのようなウォレットモデルを定義すべきか。NISTモデルのどの点を参考とし、どの点を改良して取り込むべきか。
	❷ Risk Managementの見直し	• 「オンラインサービスの定義」「2種類のリスク」は反映すべきと考えられるが、「継続的評価のメトリクス」はどこまで参考とすべきか。
63A-4 Identity Proofing & Enrollment	❸ Identity Proofing Roles / Types	• 新たに追加されたRolesやTypesの枠組みは本人確認ガイドラインにも反映すべきと考えられる。反映時にどのような点を考慮すべきか。
	❹ IAL1の刷新とIAL2の見直し	• NIST IAL1のようにFAIR×1で受け入れられるレベルを設けるべきか。 • NIST IAL2のVerificationの緩和（住所へのコード送付）を反映すべきか。
63B-4 Authentication & Lifecycle Management	❺ AAL2のフィッシング耐性要件強化	• AAL2は「最低１つのフィッシング耐性認証オプションを提供しなければならない」と要件が強化された。本人確認ガイドラインに反映可能か。
	❻ ウォレットによるAuthentication	• 当人認証手法例の一つとしてガイドラインに掲載すべきか。掲載する場合、プライバシー面などどのような考慮事項が必要となるか。
63C-4 Federation & Assertions	❼ User-Controlled Walletの要件	• 本人確認ガイドラインにおいてWallet特有の要件（対策基準）をどこまで具体的に定義すべきか。NISTとの差をつけるべきポイントはあるか。
	❷ FALのRequirementsの一部変更	• 本人確認ガイドラインのフェデレーション保証レベルの要件をどのように調整すべきか。例えばFAL3に相当するレベルは必要なのか。

参考資料：2pd での主な変更点

63-4 Base Volume

2pd での主な変更点（63-4 Base Volume）

❶ Digital Identity Modelにウォレットモデルが追加

- “ Federated Digital Identity Model With Subscriber-Controlled Wallet” が新たに定義された
- あわせて、Federated Modelの図においてCSPがIdPから分離された

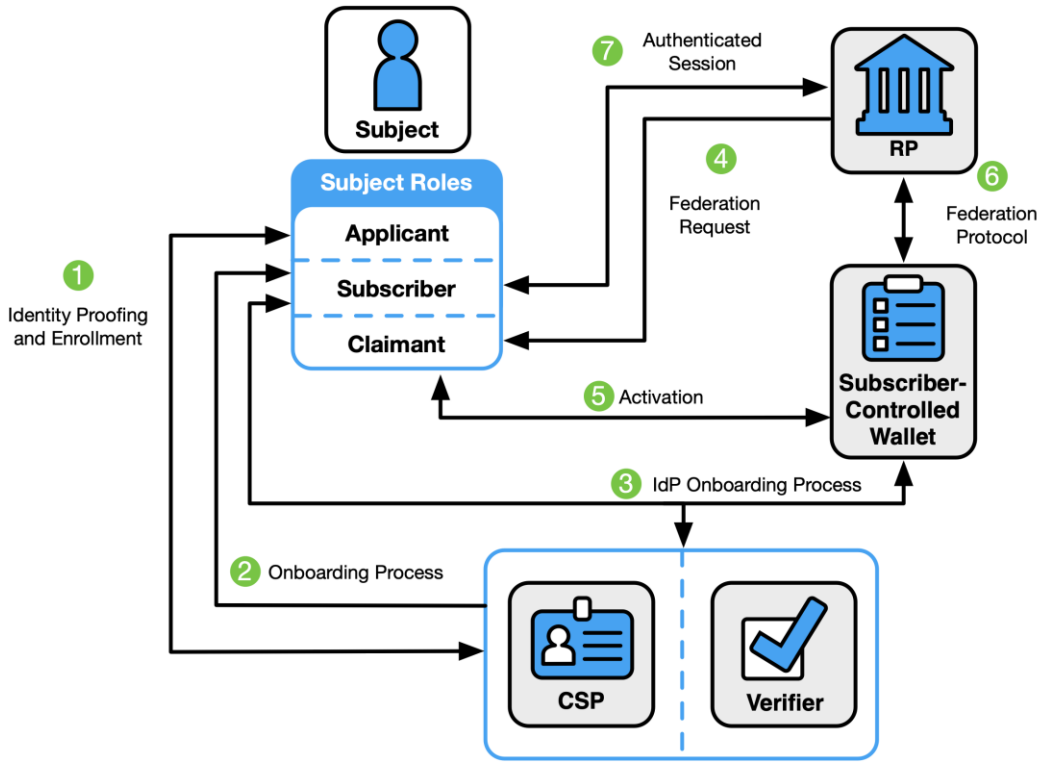
❷ Digital Identity Risk Managementプロセスの見直し

- リスクアセスメントの最初のステップに“Define the Online Service”が追加された
  （組織のミッション、適用される法的な要件、提供機能及びデータ、ユーザーグループの特定などの文書化）
- 2つの”Dimension”によるリスクの分類
- 3.5. Continuously Evaluate and Improveのメトリクス（測定指標）の要件が大幅に拡充
- 3.6. Redress（救済措置）が新規追加
- 3.8. Artificial Intelligence (AI) and Machine Learning (ML) in Identity Systemsが新規追加

論点協議資料
2pd での主な変更点（63-4 base volume）

“Federated Digital Identity Model With Subscriber-Controlled Wallet”

- ”Subscriber-Controlled Wallet”を用いたFederated Modelが新たに定義された。このモデルではCSPがIssuer、IdP（Wallet）がHolder、RPがVerifierに該当する（SP 800-63-4 2pdの説明文より）。
- ウォレットとの直接的な信頼関係を必要とせずに、RPがウォレットからのアサーションを受け入れられるモデルとして説明されている。



（図の出典：SP 800-63-4 2pd）

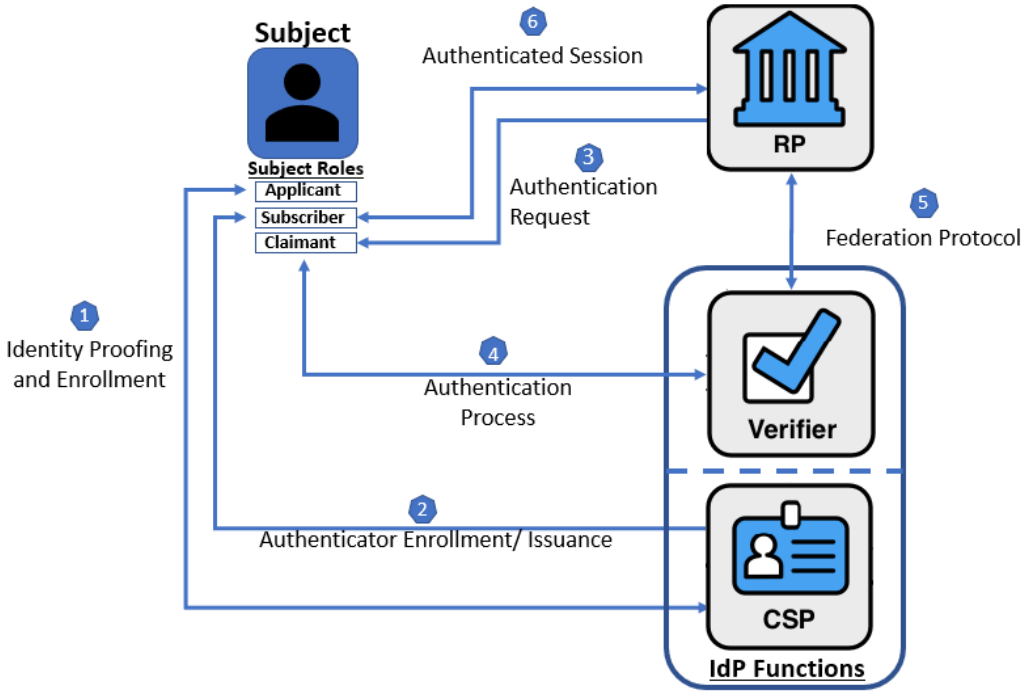
- **Step 1:** applicantは CSP の identity proofing and enrollmentプロセスに申請する。
- **Step 2:** identity proofingが成功すると、Applicantはオンボーディングプロセスを経て、subscriberとしてアイデンティティサービスに登録される。
- **Step 3:** CSP によって、 subscriber管理のウォレットがオンボーディングされる。
  - subscriberは CSP のオンボーディング機能に対して認証を行う。
  - subscriberはactivation factorを使用して、ウォレットを起動する。
  - ウォレットは、ウォレットが保持する鍵の証明を含んだリクエストを CSP に送信する。
  - CSPは、ウォレットのキーの参照とその他の追加属性を含む属性バンドルを作成する。
- **Step 4:** RPはクレームの認証を要求する。これにより、ウォレットへのfederated authenticationの要求がトリガーされる。
- **Step 5:** claimant は、subscriber管理ウォレットの所有と管理を証明する。
  - subscriberはactivation要素を使用してウォレットを起動する。
  - ウォレットは、 subscriberアカウント用に CSP が提供する属性バンドルを含むアサーションを作成する。
- **Step 6:** RP とウォレットはフェデレーションプロトコルを通じて通信する。ウォレットは、フェデレーションプロトコルを通じてアサーションとオプションで追加の属性を RP に提供する。RP はアサーションを検証し、RP におけるオンラインサービスのsubscriberのアイデンティティと属性に対する信頼性を確立する。RP は、 subscriberのfederated identity(仮名または非仮名)、IAL、AAL、FAL、およびその他の要素を使用して、承認の決定を行うことができる。
- **Step 7:** subscriberと RP の間で認証済みセッションが確立される。

（SP 800-63-4 2pdより機械翻訳）

参考：Federated Modelの図においてCSPがIdPから分離

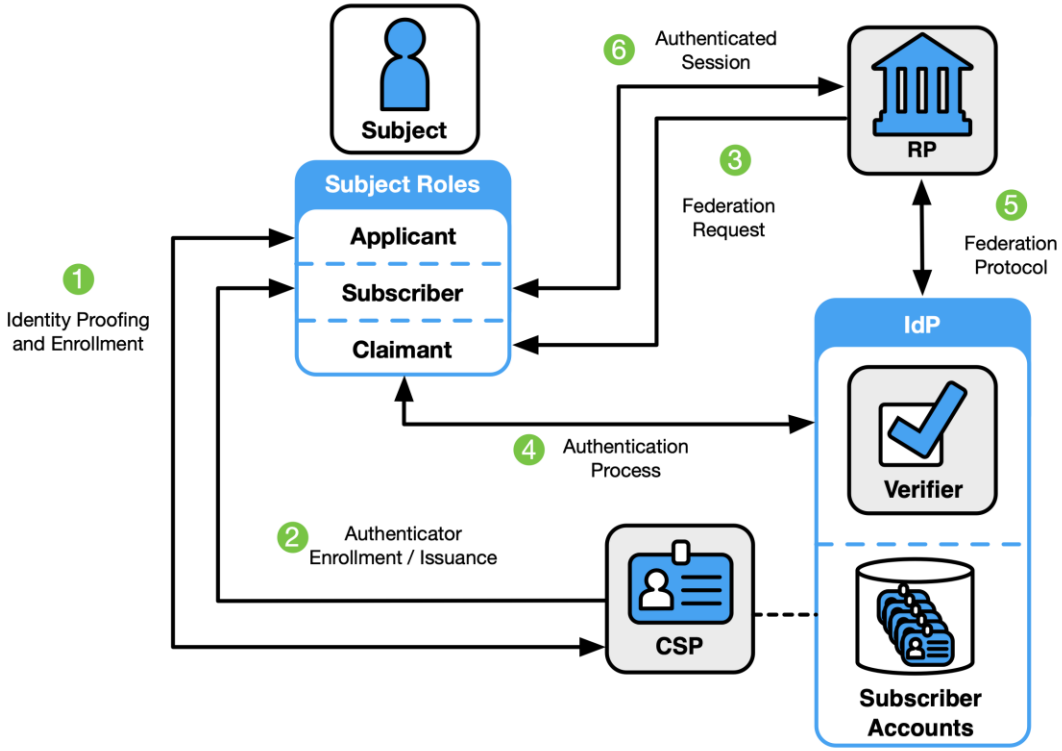
- Walletモデルの導入とあわせて、従来からあるFederated Modelの図が修正され、IdPの枠からCSPが分離された。

Initial public draft:



（図の出典：SP 800-63-4 ipd）

2nd public draft:

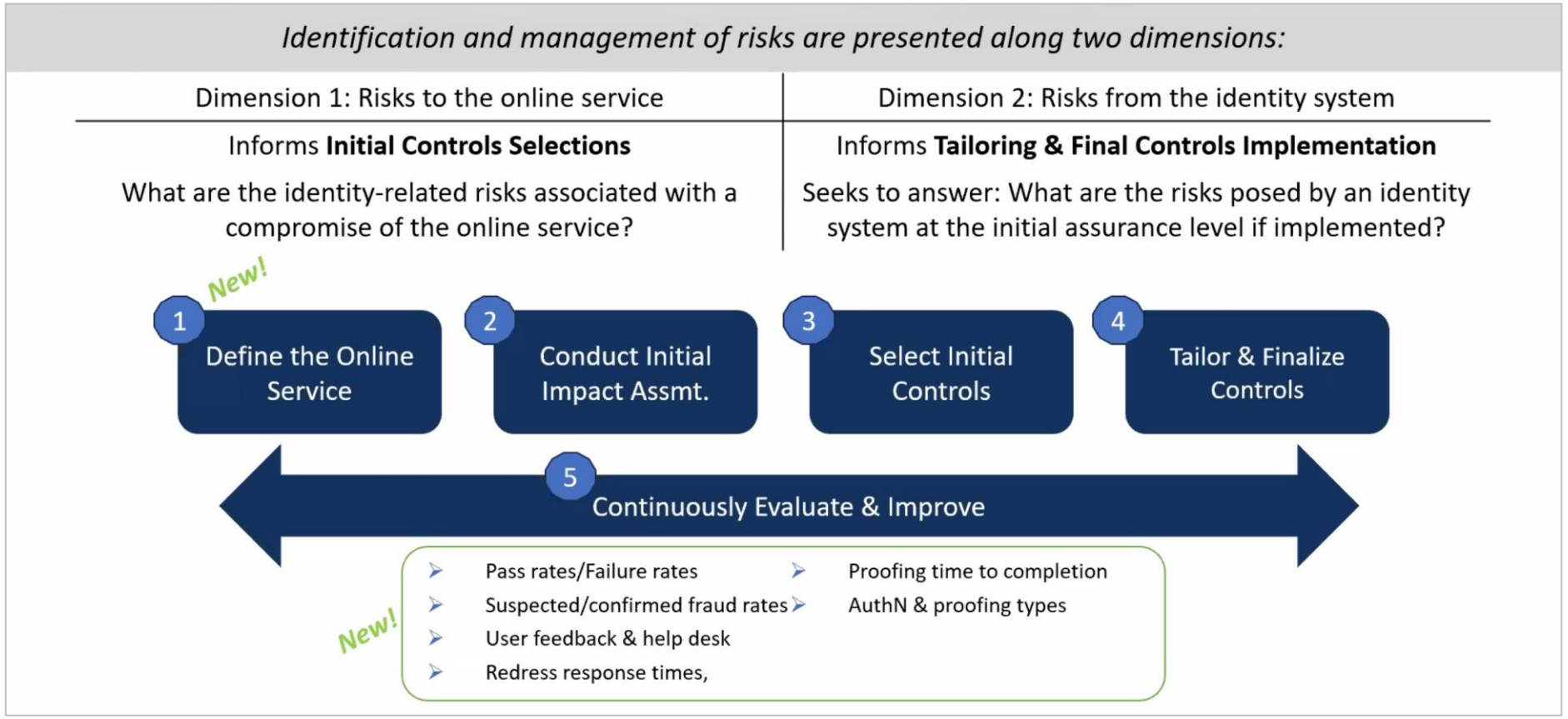


（図の出典：SP 800-63-4 2pd）

論点協議資料
2pd での主な変更点（63-4 base volume）

リスクマネジメントプロセスの見直し

- 2つのリスクDimensionが定義された（1st dimension: IDシステムに対するリスク、2nd dimension: IDシステムが引き起こすリスク）。
- リスクマネジメントの最初のステップとして「Define the Online Service」が追加された。また、Continuously Evaluate & Improveで収集すべきメトリクスが具体的に定義された。



出典：NIST Webinar Digital Identity Guidelines Update - Public Webinar（8/29）

参考資料：2pd での主な変更点

63A-4 Identity Proofing & Enrollment

2pd での主な変更点（63A-4 Identity Proofing & Enrollment）

❸ Identity Proofing Roles／Identity Proofing Typesの定義

- Identity proofing Rolesを定義するセクションが新設
  （Proofing Agent/Trusted Referee/Process Assistant/Applicant Reference など）
- Identity Proofing Typesについても同様にセクションが新設
  （Remote Unattended/Remote Attended/Onsite Attended/Onsite Unattended）

❹ IAL1の刷新とIAL2の見直し（新たなVerification方法の定義など）

- IAL1のRequirementsの全面的な見直し（NIST曰く”re-balancing”）
  （新たなIAL1は、FAIRなEvidenceのみでのidentity proofingが可能なレベルとして位置付けられた）
- IAL2でもconfirmation codeによるverification※が可能に
  （※エビデンスに紐づけられた検証済みアドレス（住所等）への確認コードの送付による検証）
- 新たなverification methodとして「Micro Transaction」が定義され、IAL1、IAL2で利用可能に
- IAL 0は削除

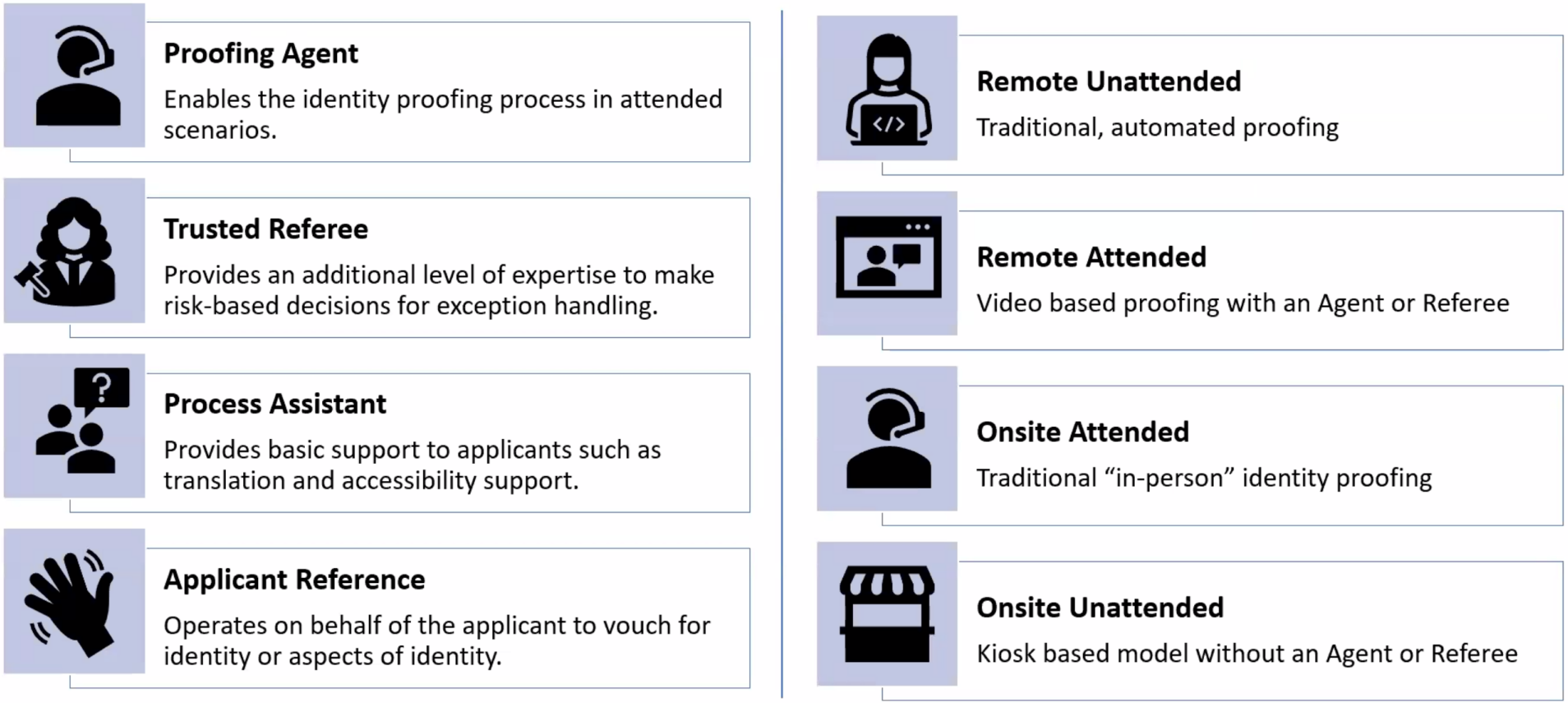
（参考）その他の変更点

- 「2.2 Core Attributes」のセクションが新設され、要件がより具体化された
- 6章の脅威に「Video or Image Injection Attack」が追加（ディープフェイク攻撃が例示された）

論点協議資料
2pd での主な変更点（63A-4 Identity Proofing & Enrollment）

Identity Proofing Roles／Identity Proofing Types

- Roles：Proofing AgentとProcess Assistantが新規定義
  （Trusted Referee/Applicant Referenceはipdにおいても定義あり）
- Types：リモート／オンサイトと、Attended／Unattendedの組み合わせで4タイプが定義
  （IALの各Requirementsでは、この４タイプ別に要求事項が整理されている）



出典：NIST Webinar Digital Identity Guidelines Update - Public Webinar（8/29）

論点協議資料
2pd での主な変更点（63A-4 Identity Proofing & Enrollment）

新たな IAL1のRequirements（概要）

- IALはEvidence要件が緩和されるなどして、FAIR×1点でも受入れられるレベルとなった。

項目（抜粋）	Requirements（要約）	主なポイント
Proofing Type	Remote/ Onsite、Unattended / Attendedのあらゆるタイプで提供可能。 • CSPはオプションとしてUnattended Remote identity proofingを提供しなければならない（SHALL） • CSPはオプションとしてRemote又はOnsiteのAttended identity proofingを最低1つは提供しなければならない（SHALL）	許容されるタイプだけでなく「オプションとして提供しなければならないタイプ」が定義された
Evidence Collection	• FAIR以上のエビデンス 1点 （オンサイトの場合は顔写真付きを使用すべき（SHOULD）とされている）	Ipdから緩和されFAIR 1点も受け入れられるレベルになった
Evidence Validation	以下のいずれか • デジタルセキュリティ機能（アサーション、データ上の署名等） • 物理的セキュリティ機能を検出できる自動スキャン技術 • Proofing agentによる目視検査（リアルタイム又は非同期プロセス） • Proofing agentによる物理的・触覚的な検査	自動スキャン技術について明記された
Verification	以下のいずれか • エビデンスに関連付けられた検証済みアドレスへの確認コード送付 • 検証済みの金融アカウント等に対するマイクロトランザクション • AAL2/FAL2以上の認証及びフェデレーションによる関連アカウントへのアクセス • 申請者の顔とEvidenceの顔画像との自動比較 • 申請者の顔とEvidence又は関連する記録上の顔写真との比較 • identity evidence(本人確認用証拠)またはその証拠に関連する権限のある記録に保存されている生体認証情報を、申請者が提供したサンプルと比較する。	Ipdと比べてマイクロトランザクション、自動比較技術がVerification手段として追加された

論点協議資料
2pd での主な変更点（63A-4 Identity Proofing & Enrollment）

IALの全体像

- IAL2のVerification手段に「検証済みアドレスへの確認コード送付」が追加された（ipdではIAL1のみ可だった）。
- 「マイクロトランザクション」が新たなVerification手段として定義され、IAL1、IAL2で利用可能となった。

項目（抜粋）	IAL1	IAL2	IAL3
Proofing Type	Remote/Onsite、 Unattended/Attendedの全パターン	IAL1と同じ	Onsite Attendedのみ ※従前のSupervised Remote Identity Proofingに相当する方法も「Onsite Attended」に含まれている。
Evidence Collection	FAIR以上のエビデンス 1点	SUPERIOR 1 点 又は FAIR 1点 + STRONG 1点	IAL2 と同じ
Attribute Collection	All Core Attributes	IAL1と同じ	All Core Attributes + Biometric Sample
Verification	以下のいずれか • 検証済みアドレスへの確認コード送付 • 検証済み金融口座等へのマイクロトランザクション送付 • AAL/FAL2以上による関連アカウントへのアクセスの実証 • 申請者とEvidenceの顔の比較（自動/対面/遠隔/非同期） • 記録された生体認証情報と申請者のサンプルとの比較	以下のいずれか • 検証済みアドレスへの確認コード送付 • 検証済み金融口座等へのマイクロトランザクション送付 • AAL/FAL2以上による関連アカウントへのアクセスの実証 • 申請者とEvidenceの顔の比較（自動/対面/遠隔/非同期） • 記録された生体認証情報と申請者のサンプルとの比較	以下のいずれか • 申請者とEvidenceの顔の比較（自動/対面/遠隔） • 信頼性の高い記録に保存されている生体認証情報と申請者のサンプルとの比較

※IAL1とIAL2のVerification手段は、概ね同様とみなせるが、実際の文書中の記載は細かな点に差異がある。

参考：Verification手段とIALとの関係

Verification手段		IAL1	IAL2	IAL3
a.	エビデンスに関連付けられた検証済みのアドレス(例えば、郵便宛先、電子メールアドレス、電話番号)に送信された確認コードを申請者が受け取ることができることを確認する	○	○	
b.	検証済みのアカウント(例えば、当座預金口座)に配信されたマイクロトランザクションの金額を申請者が受け取ることができることを確認する	○	○	
c.	AAL2/FAL2以上の認証及びフェデレーションによる関連アカウントへのアクセス	○	○	
d.	申請者の顔とEvidenceの顔画像との自動比較	○	○	○
e.	申請者の顔とEvidence又は関連する記録上の顔写真との比較（onsite attendedセッション：proofing agentとの対面）	○	○	○
f.	申請者の顔とEvidence又は関連する記録上の顔写真との比較（remote attended：proofing agentとのライブビデオ）	○	○	○
g.	申請者の顔とEvidence又は関連する記録上の顔写真との比較（非同期プロセス：proofing agentが別の時間に行う視覚的な比較）	○	○	
h	identity evidenceまたはその証拠に関連する権限のある記録に保存されている生体認証情報を、申請者が提供したサンプルと比較する。	○	○	
i	自動化された手段により、identity evidenceに保存されている、またはその証拠に関連する記録内の、顔以外の対象の生体認証情報を、申請者から提供された生体サンプルと比較する。		○	
j	本人確認用エビデンスまたはそのエビデンスに関連する信頼性の高い記録に保存されている生体情報を、申請者が提供したサンプルと比較する。			○

参考資料：2pd での主な変更点

63B-4 Authentication & Lifecycle Management

2pd での主な変更点（63B-4 Authentication & Lifecycle Management）

❺ Syncable Authenticatorの追加とAAL2のフィッシング耐性要件の強化

- Cryptographic authenticatorにパスキー等を想定したSyncable Authenticatorに関する記述が追記（4月頃に公開された63Bsup1の内容が取り込まれた。詳細はAppendix. Bに。）
- AAL2のフィッシング耐性要件が「最低１つのフィッシング耐性認証オプションを提供しなければならない」と強化された。

❷ウォレットによるAuthentication（Cryptographic Authenticatorとしてのウォレット）

- Cryptographic Authenticatorのdevice/softwareの区別がなくなり、user-controlled walletに関する記載が追加された（ただしwalletを利用する場合の詳細は63C-4を参照）

（参考）その他の変更点

- Account Recoveryの要件の見直し
- Session Managementの要件の見直し
- Reauthenticationの要件が若干緩和
- AitM resistance、Verifier-compromise resistanceが削除　等

Syncable Authenticator

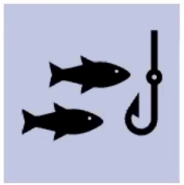
- 63Bsup1の内容を取り込み、 Multi-Factor Cryptographic Authenticationの一種としてSyncable Authenticatorsが定義された。 対応するAALは63Bsup1と同様に「最大でもAAL2」となる。

Syncable Authenticators:

- Are software or hardware cryptographic authenticators
- Where authentication keys can be cloned and exported to other storage
- To support the syncing of those keys to other authenticators (i.e., devices).

The draft guidance:

- Will provide requirements and considerations for use
- Confirm allowability at AAL2
- Reflect the content from the supplement



Phishing Resistant

Replay Resistant

Multi-factor (w/UV)

Since AAL3 still prohibits export of keys, the **maximum achievable** AAL for syncable authenticators **is AAL2**

出典：NIST Webinar Digital Identity Guidelines Update - Public Webinar（8/29）

論点協議資料
2pd での主な変更点（63B-4 Authentication & Lifecycle Management）

AAL2のフィッシング対策要件の強化

- AAL2のフィッシング耐性要件が「最低１つのフィッシング耐性認証オプションを提供しなければならない」（SHALL）と強化された。

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	• *Any AAL2 or AAL3 authenticator* • Password • Look-up secret • Out-of-band • SF OTP • SF cryptographic	• *Any AAL3 authenticator* • MF out-of-band • MF OTP • Password plus: * Look-up secret * Out-of-band * SF OTP	• MF cryptographic • SF cryptographic plus password
FIPS 140 Validation	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	• Level 3 physical security • Level 2 overall (MF cryptographic) • Level 1 overall (verifiers and SF cryptographic)
Reauthentication	30 days overall	24 hours overall 1 hour inactivity	12 hours overall 15 minutes of inactivity
Phishing Resistance	Not required	Recommended; must be available	Required
Replay Resistance	Not required	Required	Required
Authentication Intent	Not required	Recommended	Required

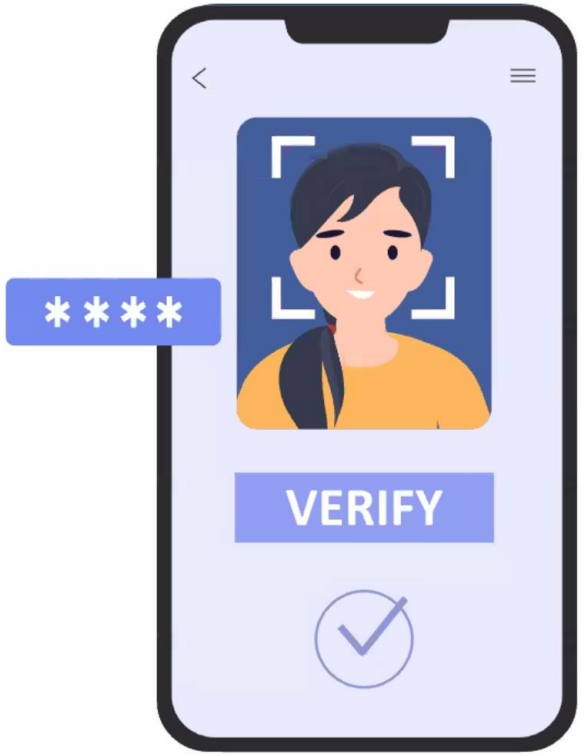
Fig. 1. Summary of requirements by AAL

Verifiers **SHALL** offer at least one phishing-resistant authentication option at AAL2, as described in Sec. 3.2.5.
Verifiersは、セクション3.2.5に記載されているように、AAL2において少なくとも1つのフィッシング耐性を有する認証オプションを提供しなければならない。
Federal agencies **SHALL** require their staff, contractors, and partners to use phishing-resistant authentication to access federal information systems.
連邦機関は、職員、請負業者、およびパートナーに対し、連邦情報システムにアクセスする際にフィッシング対策認証を使用することを義務付けるものとする。
In all cases, verifiers **SHOULD** encourage the use of phishing-resistant authentication at AAL2 whenever practical since phishing is a significant threat vector.
フィッシングは重大な脅威のベクトルであるため、すべてのケースにおいて、verifiersは、実用的な場合には常に、AAL2においてフィッシング対策認証の使用を奨励すべきである。

（出典：SP 800-63B-4 2pd 青字部分は機械翻訳）

Digital Wallets for AuthN（1/2）

- Multi-Factor Cryptographic Authenticationの一種として「 Usage With Subscriber-Controlled Wallets 」が新たに定義された。



Authentication with subscriber-controlled wallets

- Multi-factor cryptographic authentication
- Must use an activation factor to unlock the wallet
- Authentication process must use a federation protocol following -63C to present the credential

- ***SHOULD*** use platform APIs when available
- Cross-device flows must establish proximity between authenticator and the user’s endpoint

出典：NIST Webinar Digital Identity Guidelines Update - Public Webinar（8/29）

Digital Wallets for AuthN（2/2）

（該当箇所の翻訳文）

3.1.7.3. Usage With Subscriber-Controlled Wallets

multi-factor cryptographic authenticationの特別なケースでの使用法は、[SP800-63C]のセクション5で説明されているsubscriber-controlled walletsである。claimantがまずactivation factorを使用してwalletのロックを解除した後、authentication processでは[SP800-63C]で詳細に説明されているようにfederation protocolが使用される。federation protocolのアサーション内容および提示要件は、cryptographic authenticatorsに求められるセキュリティ特性を提供する。そのため、subscriber-controlled walletsは、activation factorとwalletによって生成されたアサーションの提示および検証を通じて、multi-factor authenticatorsとみなすことができる。

秘密鍵へのアクセスにはactivation factorが必要である。authenticator activation secretsは、セクション3.2.10の要件を満たさなければならない。生体認証のactivation factorは、連続した認証失敗の回数制限を含め、セクション3.2.3の要件を満たさなければならない。認証処理の直後に、activationに使用されたパスワードまたは生体認証サンプル、および生体認証サンプルから派生したすべての生体認証データはゼロクリア(消去)されなければならない。

subscriber-controlled walletsを使用するauthentication processesは、[SP800-63C]の第5項で詳述されているfederation processとともに使用しなければならない。subscriber-controlled walletsによって生成された署名付きaudience-restricted assertionsは、詐称RPに提示されたassertionが正当なRPによって使用されるのを防ぐため、フィッシング対策として有効であると考えられる。walletからの有効な署名またはaudience restrictionを欠くassertionは、フィッシング対策として有効であるとはみなされない。

（SP 800-63B-4 2pdより機械翻訳）

参考資料：2pd での主な変更点

63C-4 Federation & Assertions

2pd での主な変更点（63C-4 Federation & Assertions）

❼ User-Controlled Walletの要件が定義

- ウォレットに関する要件は「5. Subscriber-Controlled Wallets」として、以下の構成の章が新設された。
  - 5.1. Wallet Activation
  - 5.2. Federation Transaction
  - 5.3. Trust Agreements
  - 5.4. Provisioning the Subscriber-Controlled Wallet
  - 5.5. Discovery and Registration
  - 5.6. Authentication and Attribute Disclosure
  - 5.7. Assertion Requests
  - 5.7. Assertion Contents
  - 5.9. Assertion Contents
  - 5.10. Assertion Validation
  - 5.11. RP Subscriber Accounts

❽ FALのRequirementsの一部変更

- ”Audience Restriction”が追加されるなど、FALのRequirementsの表が一部変更された。

（参考）ドキュメント構成の全面的な改定

- 63Cは章レベルで全面改定された。ページ数は49ページ（-3）→ 87ページ（-4 ipd）→135ページ（-4 2pd）に。
- 共通の要件が「3. Common Federation Requirements」に定義され、従来のFederated Modelの要件は「4. General-Purpose IdPs」に整理された

論点協議資料
2pd での主な変更点（63C-4 Federation & Assertions）

目次構成の全面的な改定（Ipdから2pdへの目次構成の変化）

- 63C-4の目次構成はipdから全面的に見直された。従前のFederated Modelを想定した要件は「3. Common Federation Requirements」と「4. General-Purpose IdPs」に再編されている。

2pdの目次（主要部分を抜粋）

3. Common Federation Requirements
（一部のみ抜粋）
3.4. Trust Agreements
3.6. Authentication and Attribute Disclosure
3.7. RP Subscriber Accounts
3.11. Identity Attributes
3.12. Assertion Protection
…

4. General-Purpose IdPs
4.1. IdP Account Provisioning
4.2. Federation Transaction
4.3. Trust Agreements
4.4. Discovery and Registration
4.5. Subscriber Authentication at the IdP
4.6. Authentication and Attribute Disclosure
4.7. Reauthentication and Session Requirements in Federated Environments
4.8. Shared Signaling
4.9. Assertion Contents
4.10. Assertion Request
4.11. Assertion Presentation

5. Subscriber-Controlled Wallets（後述）

ipdの目次（主要部分を抜粋）

5. Federation
5.1. Trust Agreements
5.2. Registration
5.3. Authentication and Attribute Disclosure
5.4. RP Subscriber Accounts
5.5. Privacy Requirements
5.6. Reauthentication and Session Requirements in Federation Environments

6. Assertions
6.1. Assertion Binding
6.2. Assertion Protection
6.3. Identity APIs

7. Assertion Presentation
7.1. Back-Channel Presentation
7.2. Front-Channel Presentation
7.3. Protecting Information

※上記の対応関係の矢印は一例。網羅的な関係を示すものではない。

論点協議資料
2pd での主な変更点（63C-4 Federation & Assertions）

User-Controlled Walletの要件（5. Subscriber-Controlled Wallets）

2pd 目次	概要
5.1. Wallet Activation	WalletのActivationに関する要求事項（activation factorの要求など）
5.2. Federation Transaction	WalletをIdPとした場合のフェデレーショントランザクション（シーケンス図）の説明
5.3. Trust Agreements	Walletを使用する場合にRPとCSPとの間で必要となるtrust agreementの要求事項、ウォレットによる連携の実行時に必要となる要求事項（RPが要求する属性セット、その目的、必要とするxALの開示など）
5.4. Provisioning the Subscriber-Controlled Wallet	CSPによるWalletのプロビジョニングの際の要求事項（認証からattribute bundleの発行までの手順） Walletのデプロビジョニング（停止、廃止）の手段の提供に関する要求事項
5.5. Discovery and Registration	フェデレーショントランザクションを開始する際の、Attribute bundleに署名された公開鍵の取得方法等についての要求事項
5.6. Authentication and Attribute Disclosure	選択的属性開示手段の提供（SHOULD）や、不正確な属性値に関する苦情や是正のためのメカニズムについて
5.7. Assertion Requests	RPがアサーションリクエストに含めるべき内容 （RPの識別子、nonce、要求する属性セットとその使用目的など）
5.8. Assertion Contents	Walletがアサーションに含めるべき内容、アサーションに含まれるAttributes Bundleに含めるべき内容 （CSPが発行したAttribute Bundle、アサーション発行者の識別子、RPの識別子、タイムスタンプ、nonceなど）
5.9. Assertion Presentation	アサーションを提示する際の要求事項（authenticated protected channelの使用、nonceの検証、PIIが含まれる場合の暗号化、XSS対策やアサーションインジェクション対策など）
5.10. Assertion Validation	RPが受け取ったアサーションを検証する際の要求事項（発行者、時間、Audience restriction、nonceなどの検証）
5.11. RP Subscriber Accounts	RP側のSubscriber Accountsの管理等に関する要件 （※Walletでは、just-in-time又はephemeralなプロビジョニングモデルのみ使用可能とされている）

論点協議資料
2pd での主な変更点（63C-4 Federation & Assertions）

FAL Requirementsが一部変更

- FALの表には「Audience Restriction」が追加された。その他にも細かな要件や用語も変更されている。

Requirement	FAL1	FAL2	FAL3
Audience Restriction ※2pdから追加	Multiple RPs allowed per assertion, Single RP per assertion recommended	Single RP per assertion	Single RP per assertion
Injection Protection	Recommended for all transactions	Required; transaction begins at the RP	Required; transaction begins at the RP
Trust Agreement Establishment	Subscriber-driven or A priori	A priori	A priori
Identifier and Key Establishment ※従前の「Registration」を置き換える形	Dynamic or Static	Dynamic or Static	Static
Presentation	Bearer Assertion	Bearer Assertion	Holder-of-Key Assertion or Bound Authenticator ※従前のBound Authenticatorから2種類の定義に詳細化された

論点協議資料
2pd での主な変更点（63C-4 Federation & Assertions）

参考：3. Common Federation Requirementsの概要

2pd 目次	概要
3.1. Roles	Credential Service Provider (CSP) 、Identity Provider (IdP) 、Relying Party (RP)に関する概要説明
3.2. Functions	Trust Agreement Management、Authorized Party、Proxied Federationに関する概要説明 Fulfilling Roles and Functions of a Federation Model の概要説明
3.3. Federated Identifiers	PPI（Pairwise Pseudonymous Identifiers）に関する要求事項
3.4. Trust Agreements	Trust Agreementsの各モデル（2者間、多者間）の概要説明と要求事項、Redress要件
3.5. Identifiers and Cryptographic Key Management for CSPs, IdPs, and RPs	Key Rotation、Cryptographic Key Storage、Software Attestationsに関する要求事項
3.6. Authentication and Attribute Disclosure	IdPからRPへのsubscriber attributesの受け渡しに関する要求事項
3.7. RP Subscriber Accounts	RPがローカルに保持するsubscriberのレコードに関する要求事項
3.8. Authenticated Sessions at the RP	RPとSubscriberとの間のauthenticated sessionを確立するための要求事項
3.9. Privacy Requirements	プライバシー面の考慮事項と、IdP、RP又はその両方に求められる要求事項
3.10. Security Controls	インジェクション攻撃対策、サブスクライバー情報の保護・保管についての要求事項
3.11. Identity Attributes	Subscriber-Controlled Walletで使用される”Attributes Bundle”、従前のIdentity APIsに関する要求事項
3.12. Assertion Protection	アサーションの偽造、再利用などの攻撃に対する対策要件
3.13. Bearer Assertions	bearer assertionの概要説明
3.14. Holder-of-Key Assertions	FAL3で求められるHolder-of-Key Assertionsの概要説明と要求事項
3.15. Bound Authenticators	FAL3で求められるBound Authenticatorsの概要説明と要求事項
3.16. RP Requirements for Processing Holder-of-Key Assertions and Bound Authenticators	Holder-of-Key Assertions および Bound Authenticators に関するRPでの処理要件

デジタル庁

Digital Agency