SP800-63-3A

- Digital Identity Guidelines
  - A: Enrollment and Identity Proofing

- 今回は、概略の説明になります。

Enrollment and Identity Proofing

- 必要なプロセスの整理と「強さ」の定義
  1. Resolution

     属性とエビデンスの収集

     ＊エビデンスについて「government issued photoID」といった具体的（すぎる）縛りがなくなった
  2. Validation

     属性、エビデンスの正当性チェック
  3. Verification

     属性、エビデンスの検証

Evidence = I.D.


入館証の掲示
お願い致します
六本木ファーストビル
Your I.D. Presentation
Requested
Roppongi First Building Co.,Ltd.

特にIAL

- レベルは1, 2, 3.
- プライバシーの観点から「minimum」を強調

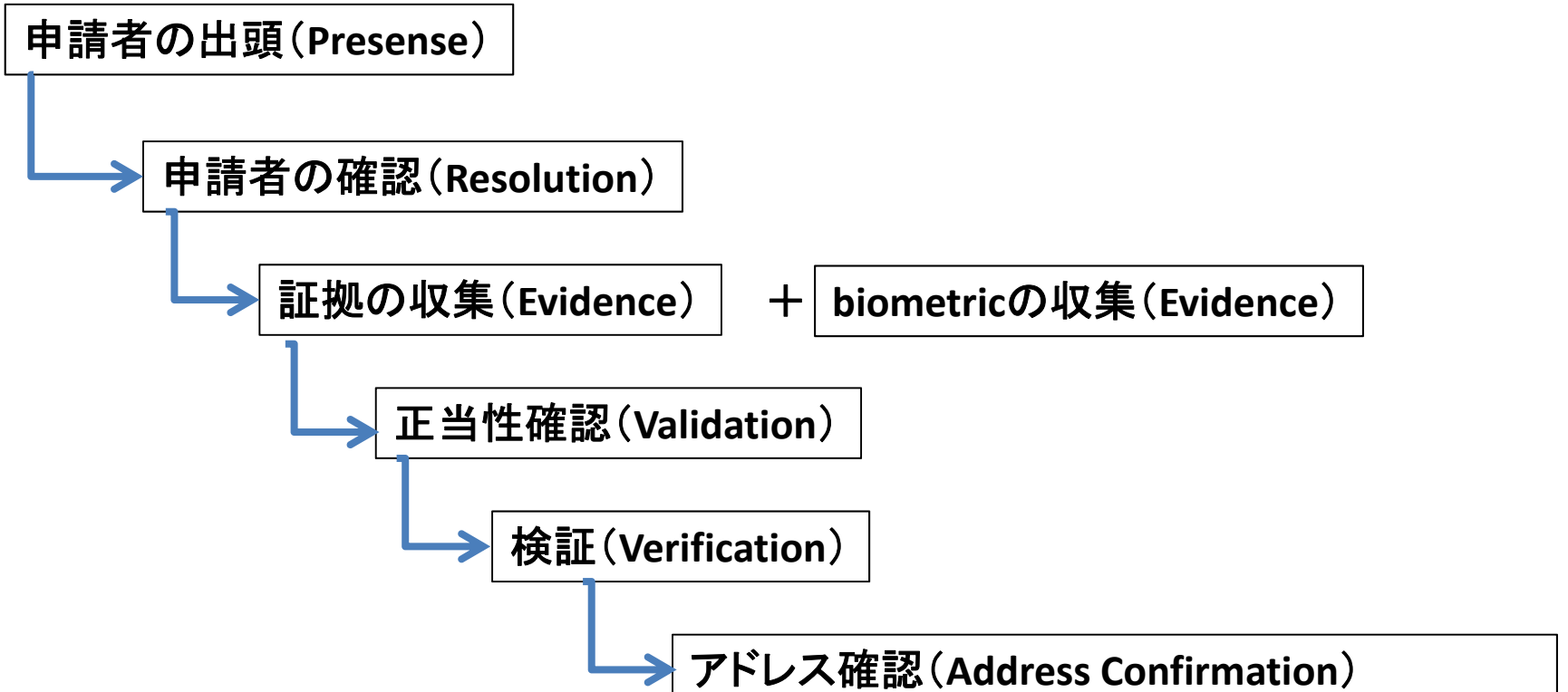
- エビデンス、正当性チェック、検証の「強さ」を定義して、一定の強さを要求する
  - Unacceptable/Weak/Fair/Strong/Superior
- 過去のインシデントの反省
  - 一定の強さを求めるところからKBV (Knowledge based verification) の追放

Table 4-1 IAL Requirements Summary

Requirement	IAL1	IAL2	IAL3
Presence	No requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No requirements	The minimum attributes necessary to accomplish identity resolution. KBV may be used for added confidence.	Same as IAL2.
Evidence	No identity evidence is collected	One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence, or One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	Two pieces of SUPERIOR evidence, or One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2.
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	SP 800-53 Moderate Baseline (or equivalent federal or industry standard).	SP 800-53 High Baseline (or equivalent federal or industry standard).

- プロセス

Security Controls (SP800-53 based)



アドレス　ー　電話　or 住所
（emailは当然廃止）

IAL 1

- Yahoo! ID相当（ここらへんがサービスのベースライン）

- （エビデンスを収集して）属性の有効性チェック、検証をしては「ならない」（申告されたとおりに処理すること）
- CSPは、サービス提供のために、申請者に、属性の自己申告を求めることは許容される
- IAL2, IAL3相当のCSPは、利用者が同意するのなら、IAL1のみを要求するRPにも対応すべきである（下位互換の保証）

IAL 2

- AAL2を要求するところはここらへんを要求することを想定する

- Superior またはStrongエビデンス（内部で発行機関とともに正当性チェックが可能な場合）

  OR

- Strongエビデンス2つ

  OR

- Strongエビデンス1つ＋Fairエビデンス1つ

エビデンスの強度

- FAIR：
  - Identity proofing processを通して発行機関がアイデンティティを確認している
  - 合理的な方法で配布されている
  - Unique ID or 写真、バイオメトリック　or KBVで検証
  - Integrityについての保証
  - reproduceについてのproprietary knowledge （偽造防止）

- Strong：　発行に際して
  - 文書による発行プロセス
  - 実世界の人間を「知っている」という合理的な信頼（belief）があること
  - 定期的な見直し
- 合理的な方法で配布されている
- Unique ID
- OfficialなFull name
- 写真 or biometric OR すでにあるIAL2にバインドされたAAL2を持っていること
- Integrityについての保証
- reproduceについてのproprietary knowledge（偽造防止）

- Superior:発行に際して
  - Strong+
  - 本人との結びつきについて高い確度を要求
  - 対面での本人確認
  - 正しく配布されていること
  - Unique ID
  - Officialなfull name
  - 写真 and biometric
  - …

Validation and Verification

- これにもいろいろありますが
- IAL2はStrongな方法で、IAL3はSuperiorな方法で
- Validation
  - Strong:真正性は「技術」を用いてチェック
  - Superior: 真正性は「trained personnel」による「技術」を用いたチェック
- Verification
  - Strong:物理的に検証（本人とエビデンスの顔写真の照合）
  - Superior:biometricを用いての検証

日本の話をしましょうか

- アメリカのFederal Serviceにシナリオは限定されています
- 日本の公的サービスの場合、また異なる「強さ」の基準があるでしょう
- 日本の民間サービスの場合、また異なる「強さ」の基準があるでしょう

- Superiorはパスポート一択でしょう（顔写真情報をbiometricと言うかはともかく）
- マイナンバーカードは？
- Strongは運転免許証がすぐおもいつきますが、いろいろ選択肢がありそうです（EG:JPの基準）

- で、戸籍謄（抄）本、住民票はどうなのだ、と。