ニュージーランド政府による “Identification Management Standards” に関する考察

==NIST SP800-63 “Digital Identity Guidelines”との比較結果等==

NPO日本ネットワークセキュリティ協会（JNSA)
標準化部会　デジタルアイデンティティWG

２０２３年５月8日　発行

留意事項

このレポートの利用に際しては、以下の条件を遵守してください。

このレポートに含まれる一切の内容に関する著作権は、レポート作成者に帰属し、日本の著作権法や国際条約などで保護されています。

著作権法上、認められた場合を除き、著作権者の許可なく、このレポートの全部又は一部を、複製、転載、販売、その他の二次利用行為を行うことを禁じます。

これに違反する行為を行った場合には、関係法令に基づき、民事、刑事を問わず法的責任を負うことがあります。

レポート作成者は、このレポートの内容の正確性、安全性、有用性等について、一切の保証を与えるものではありません。また、このレポートに含まれる情報及び内容の利用によって、直接・間接的に生じた損害について一切の責任を負わないものとします。

このレポートの使用に当たっては、以上にご同意いただいた上、ご自身の責任のもとご活用いただきますようお願いいたします。

また、レポート内の解説や和訳など全ての内容には、執筆者による独自の解釈を含んでいますのでご留意ください。

ご挨拶

本書は、2022年度デジタルアイデンティティWG内の「ドキュメントを読むサブWG」にて、ニュージーランド政府のID管理基準を定めたドキュメントを読み、約半年間に渡ってディスカッションを行った内容をまとめたものです。

デジタルアイデンティティに関する**主要なガイドラインについての概要**を知りたい方や世界の**電子政府の取り組みについて知りたい方**、**IDを取り扱うシステムの管理者、運用者、実装者**で、デジタルアイデンティティについて**「まず何から考えればよいか」の前提**を知りたい方を想定しています。
また、ニュージーランド（以下「NZ」と記載）の“Identification Management Standards”の概要を知りたい方にもご活用いただけるものとなっています。
本書を通して、少しでもデジタルアイデンティティへの理解を深め、アイデンティティ管理の適切な設計・導入・運用などにご活用いただけると幸いです。

本書の執筆にあたって執筆メンバーにご尽力をいただいたことに、この場をお借りして謝辞を申し上げます。

標準化部会　デジタルアイデンティティWGリーダー　宮川　晃一

目次

1．NZ Gov.
“Identification Management Standards”とは

New Zealand Government
Identification Management Standards

NZ Gov.“Identification Management Standards”

- 電子政府の取り組みを早くから推進してきた NZ 政府が定めた ID 管理基準
  ※ここでの “ID” は、”Identification”=本人の識別情報を指す

- 市民の ID の盗難、詐欺、プライバシーの損失を防ぐために必要なID管理手法について書かれている

- デジタルアイデンティティ界隈のバイブル的存在であるNIST SP800-63 と、一見すると似ている概念を取り入れているため、どんな新規性・特徴があるかについて読み解いてみた

本サブWGでは、システムにおけるデジタルアイデンティティの取り扱いに関する枠組みについて、
「NIST SP800-63 だけではない観点もある」という観点で、
NISTとNZの比較を実施し考察してみた

２．NZ Gov.
“Identification Management Standards “策定経緯

Digital Nations について

■Digital Nations とは？

- よりよい**デジタルガバメントの効率的で迅速な実現**を目的として、参画国が取り組みを共有、学習を進める組織。
- 2014年にエストニアなど 5カ国で D5 として発足し、参画国を増やして Digital Nations に改称。2022年12月時点で 10カ国が参画し、Identification Management Standards を公開している NZ も参画。

■Digital Nations におけるデジタルアイデンティティの扱われ方は？

- Digital Nations は「AI」「Data360」「デジタルガバナンス」「**デジタルアイデンティティ**」「持続的な政府情報技術」の 5テーマで WG を組成し活動を行っている
- デジタルアイデンティティWG は、「Digital Nations 加盟国において、**政府の DX のために健全なデジタルアイデンティティの概念と実装の利点を促進**し、**より良いサービスを一般市民に提供し、社会的成長を促進する**こと」を目的とし、WG 内で提起され優先順位付けされた議題に基づき、**加盟国間で知識と経験を共有**している

NZ Gov.“Identification Management Standards”の目的

- あらゆる**情報犯罪**（識別情報の盗難、詐欺、プライバシーの喪失等）**から市民を守るために必要なID管理**手法として策定

- 組織が**適切な“エンティティ”に関する適切な情報**を持っていることの保証を通じて情報犯罪を防ごうとしている

- 識別管理基準を所管する内務省（Department of Internal Affairs; DIA）が継続的な監視を担う

【参考】Digital Nations内のデジタルアイデンティティWGの取り組み概要

WGの目的に基づく活動

WGの目的に基づき各種活動を実施

- Digital Nations参画国のデジタルIDの取り組み状況の説明等の準備
- PoCデモをステアリングコミッティに提示・実演後、その他の国の住民に広く開示
- Digital Nations参画国のデジタルアイデンティティジャーニーを支援するための継続的な議論の促進

新たな技術等の知識の共有

急速な発展を遂げるデジタルアイデンティティ領域で、WGが知識の共有をする上で重要な役割を担う

- ブロックチェーン
- DID
- 量子コンピューティング
- 信頼のベクトル
- ID のドメイン など

重要な課題への対応

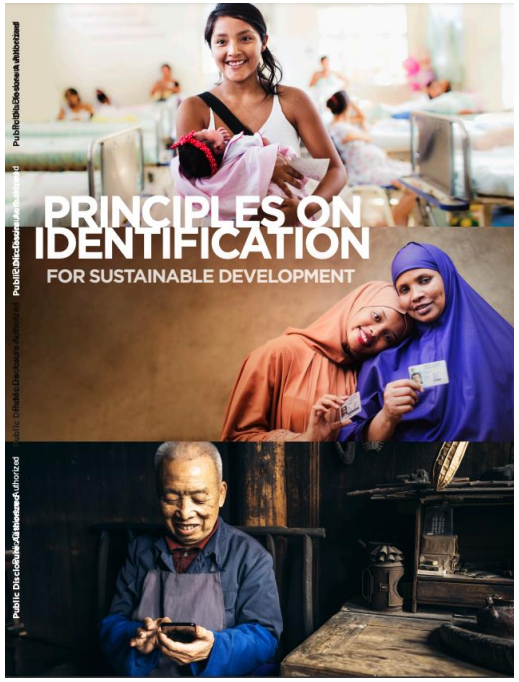
Digital Nations各国内の小グループで実践的なテストを実施し、その結果をDigital Nations他国に報告

- EUとの連携
  - EUと非EU諸国との連携の仕組みの理解
  - Digital Nations内でEUとの連携について議論
- 法人の識別
  - 法人(自然人に限らない)の識別方法の議論
  - 法人の識別方法の比較
- 国のスキームのマッピングに関する文書の準備
  - カナダとニュージーランドの取り組み
- 政府と民間でのデジタル認証情報活用
  - 政府のデジタル認証情報の民間利用の調査
  - 民間のデジタル認証情報の政府利用の調査

【参考】 Digital Nations内のデジタルアイデンティティWGの取り組み例

国境をまたぐ試み

国際的な枠組みづくりへの貢献



2018年：サミットで「**真のグローバルなデジタル市民を実現するために、国境を超えた政府サービスへのアクセスをフェデレートアプローチ(現在or新たな標準の採用を含む)で目指す**」という目標を確認

2021年：世界銀行のID4Dチームと協働し、25の国際団体と共に**Principles on Identification for Sustainable Developmentを承認**

【参考】 Digital Nations 加盟国

D5（2014年12月発足時の初期メンバ）				
エストニア	イスラエル	韓国	ニュージーランド	イギリス
				
				
カナダ	ウルグアイ	メキシコ	ポルトガル	デンマーク
2018年2月に2カ国が加わり D7 に		2018年11月にさらに2カ国加わり D9 に		2019年11月に加盟

【参考】Digital Nations各国のデジタルアイデンティティに関する取り組み

	エストニア	イスラエル	韓国	ニュージーランド	イギリス
国民ID	• Estonian personal identification code 国民識別コード (e-Residency digital identity card 国民番号カード)	• Mispar Zehut 国民識別番号 (Te'udat Zehut 国民番号カード)	• Resident registration number 住民登録番号	国民全員に共通附番されるものはない	• GOV.UK Verify 英国デジタルID
基準関連	ー	ID カード携帯および表示法(1982 年)	住民登録法(1962年)	Identification Management Standards(2016年)	UK digital identity & attributes trust framework alpha v2
備考	国内機能の整備を進める目的で導入された(2000年)	ー	• 政府や公的機関が発行する殆どの証明証に住民登録番号が記載されている	18歳以上であればKiwi Accessカードを申請可能	2016年から運用開始。民間IDと連携できる特徴があるが使い勝手がよくなくあまり普及せず。2023年4月までに閉鎖予定

【参考】Digital Nations 各国のデジタルアイデンティティに関する取り組み

	カナダ	ウルグアイ	メキシコ	ポルトガル	デンマーク
国民ID	国民全員に共通附番されるものはない	―	• Clave Única de Registro de Población 国民登録番号	• Civil Identification Number 市民識別番号 (Cartão de cidadão 市民カード)	• Det Centrale Personregister 個人識別番号
関連基準	• Guideline on Identity Assurance • Standard on Identity and Credential Assurance	―	―	―	市民登録法(1968年)
備考	12歳以上であれば、Social Insurance Number(社会保険番号)の申請が可能	―	―	―	行政関係からかかりつけ医等の民間の情報まで幅広く活用されている

３．NIST SP800-63-3との比較

5つの観点で比較してみた

比較観点

① ドキュメントの目的
② モデル
③ 定義されているもの
④ 定義から読み取れる内容
⑤ レベル分け

比較観点① ドキュメントの目的

比較観点① ドキュメントの目的（概要）

	NZ “Identification Management Standards”	NIST SP800-63-3
明示的な対象者	RP および、クレデンシャルプロバイダ（CP）の役割を果たす公的機関、民間企業	米国政府機関
対象	一般的なシステムへの要求事項	米国政府に入れるシステムの要求事項
概要	• 各事業者が**リスク影響度とリスク発生可能性**をインプットに、適切な Assurance Level を選択する基準を提示 • 想定される**リスクの定義、影響度、発生可能性**を段階評価 • ID に関する想定リスク（改ざんなど）に対し、影響度、発生可能性でパラメータ化	• **リスク影響度や個人情報の取扱い有無**等をインプットに、適切な Assurance Level を選択する基準を提示 • **フローチャート**でリスク影響度に合わせて Assurance Level が決定

比較観点① ドキュメントの目的（方向性）

	NZ “Identification Management Standards”	NIST SP800-63-3
記載の方向性	対象システム内部の実装要求事項ではなく、システムを利用する利用者、及び提供者側に対する要求事項を定義	対象システム内部の各種実装を行うにあたり実現すべき機能の要求レベルを定義
対象想定読者	対象システムを利用者に対して提供する管理者、運用者	対象システムを構築する実装者

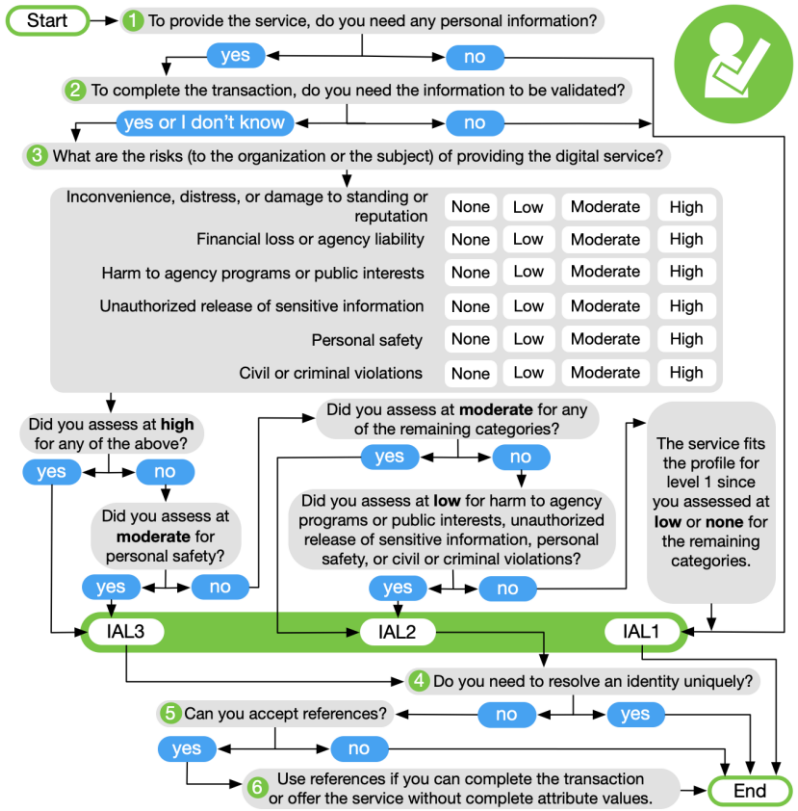
■ NZ、NISTの各ドキュメントについては、内容の記載よりドキュメントとしての目指している方向性が異なる

■ NZは、システム環境全般に対して、システムの実装やそのシステムを適切に動かすための管理、運用水準を定義

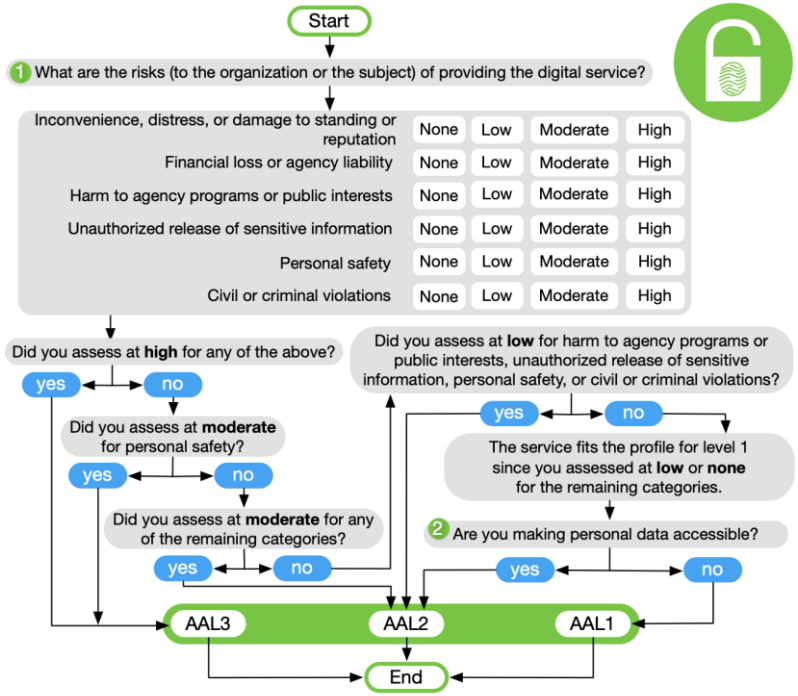
■ NISTは、前ページに記載の通り、米国政府に導入するためのシステム要求水準の定義を行っている

【参考】NIST SP800-63-3 における Assurance Level の判定フロー

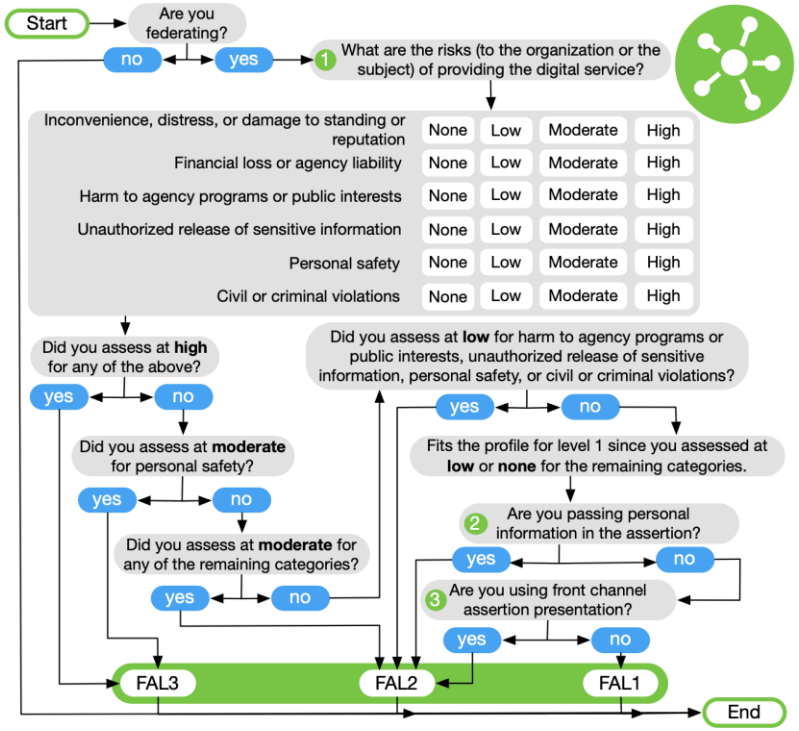
Identity Assurance Level



Authenticator Assurance Level



Federation Assurance Level



【参考】NZのドキュメントにおけるレベル評価

JNSA

リスクが顕在化した場合の重大度(Impact)を5段階で評価。

Minimum、 Minor、 Moderate、 Significant、 Severe

小 → 大

結果が発生する可能性(Likelihood)を5段階で評価。

低 → 高

Rare ：例外的な状況以外の防止管理が実施済
Unlikely：複数コントロールにより、限られた状況でのみ影響発生
Possible：防止策はあるが、状況により影響が発生する
Likely ：最小限、有効でない対策のため影響発生の可能性が高い
Almost certain：影響防止策が整っていない

Likelihood:	Impact: Minimal	Minor	Moderate	Significant	Severe
Rare	1	2	4	7	11
Unlikely	3	5	8	12	16
Possible	6	9	13	17	20
Likely	10	14	18	21	23
Almost certain	15	19	22	24	25

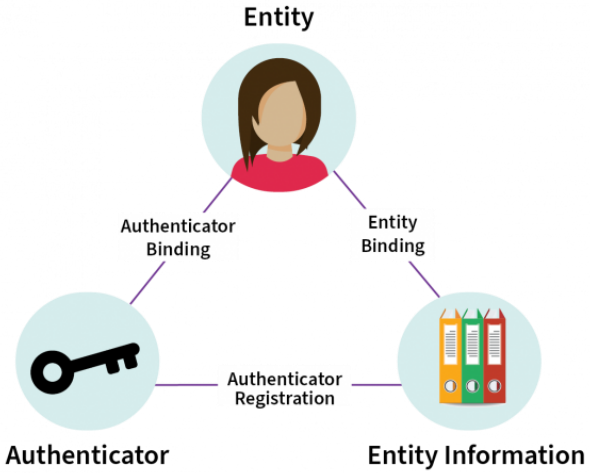
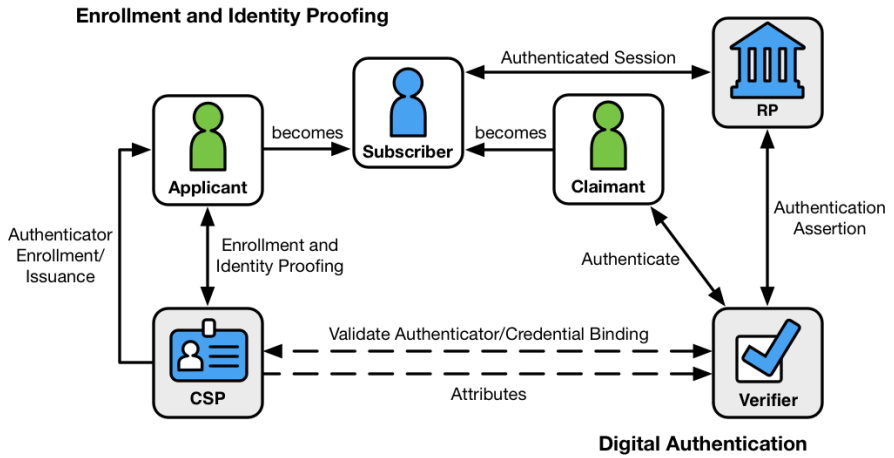
Plotted level for Risk 1	Plotted level for Risk 2	Strength of identification process
1–3	1–3	Negligible — Level 1
4-6	4-10	Low — Level 2
7-19	11-19	Moderate — Level 3
20-25	20-25	High – Level 4

重大度、発生可能性から適切なアシュアランスレベルを選択する基準を提示。
マトリクスによりリスクレベル(1～25)を判定し、そこからアシュアランスレベル(1～4)を判定。

比較観点② モデル

比較観点② モデル

JNSA

	NZ “Identification Management Standards”	NIST SP800-63-3
		
本人確認のレベル	Entity と Entity Information 間の結びつき強度を以て判別 ＝ **Entity Binding**	Applicant が利用する CSP (Credential Service Provider) の強度を以て判別
当人認証のレベル	Entity と Authenticator 間の結びつき強度を以て判別 ＝ **Authenticator Binding**	Claimant が利用する Verifier の認証強度を以て判別
考察	Entity の状態は定義せず、**各要素間の結びつき**強度を中心に定義	モデル内にエンティティの状態遷移（Subscriberへの移行）が含まれる

比較観点③ 定義されているもの

定義の差分（IA）

	NZ “Identification Management Standards”		NIST SP800-63-3	
	正式名称	定義の概要	正式名称	定義の概要
IA	**Information** Assurance	• Entity [の本人特定事項などの] 情報の品質と正確さを確立するプロセスの堅牢性を意味する	**Identity** Assurance	• 個人の Identity を確信を持って決定するための Identity Proofing プロセスの頑強性 • IAL は潜在的 Identity Proofing エラーを軽減することを目的に選択される
主な内容	取り扱う情報に関する一定の信頼性を担保するための**運用上の手続き**や、システム稼働における**各種オペレーションの手続き**に関する要求事項の記載がされている		**システム内で扱うべき Digital Identity の信頼性**の要求、及びその信頼性を満たすためのデータのエビデンス要求事項の記載がある	
考察	**IT システム環境全般から見た** Identity Information **取得のプロセスや、その手続き**における信頼性担保の手法定義がされている		**情報システムから見た** Identity Information の取り扱い水準や**信頼性の根拠の定義**が記載されている	

定義の差分（BA）

	NZ “Identification Management Standards”		NIST SP800-63-3	
	正式名称	定義の概要	正式名称	定義の概要
BA	Binging Assurance	• Entity と Entity Information の紐づけ、及び/又は、Entity と Authenticator を紐づけるプロセスの堅牢性を意味する	―	―
主な内容	システムとリアルな Entity や 、Authenticator とリアルな Entity との**紐づけに関する信頼性**の定義や、実施すべき運用水準についての定義がされている		システム外で行われるリアルな Entity との紐づけに関する定義の記載はされていない	
考察	システムを利用する Entity とシステムをつなぐときの紐づけの信頼性の定義や、その信頼性を担保するための要求水準が定義されている		システム外で行われることに関しての定義については触れられていない	

定義の差分（AA）

JNSA

	NZ “Identification Management Standards”		NIST SP800-63-3	
	正式名称	定義の概要	正式名称	定義の概要
AA	**Authentication** Assurance	• Authenticator がその保有者 [本人] のみの管理下にあることを確保するプロセスの堅牢性を意味する	**Authenticator** Assurance	• Authentication プロセス自体、および Authenticator と特定個人の識別子の紐付けの頑強性 • AAL は Authentication エラーを軽減することを目的に選択される i.e., 本来正当でない偽の Claimant が正当なふりをして Credential を利用する
主な内容	Entity の**認証行為そのものに着目**し、認証行為そのものに対しての信頼性やなりすましの低減といった防御措置の要求水準について記載がされている		Entity の**認証に使われた手法そのもの信頼性**の定義や、システムによって要求すべき信頼性の要求事項の記載がある	
考察	IT システム環境全般から**認証プロセスのアクセス主体との紐づけの信頼性**の定義や**認証手法そのものの信頼性**の定義がされている		情報システムから見た、**認証時の手法の信頼性**の定義や、その信頼性を担保するための要求事項について定義がされている	

定義の差分（FA）

JNSA

	NZ “Identification Management Standards”		NIST SP800-63-3	
	正式名称	定義の概要	正式名称	定義の概要
FA	Federation Assurance	• 多くの場面で使用されるクレデンシャルの完全性（Integrity）、セキュリティ、及びプライバシーを維持するために実施されるべき追加手順を意味する	Federation Assurance	• Federation 時に Authentication および Attribute の情報をやり取りするための Assertion Protocol の頑強性. • すべての Digital システムが Federated Identity アーキテクチャを採用する訳ではないため, FAL はオプションである • FAL は Federation エラー (Identity Assertion が毀損するなど) を軽減することを目的に選択される.
主な内容	連携を行う際の**対象システムそのものの信頼性**や、**連携手続きそのものに関する要求事項**の記載がされている		他のシステムから受け取る各種 **Digital Identity 情報に関しての信頼性**の定義や、その信頼性を担保するためのシステム要求事項の記載がある	
考察	システム間連携を行うにあたり、**事業者間での連携の手続き**や、**事前確認すべき事項**の定義といった要件について定義がされている		システム間連携における、**データの信頼性の定義**や、その信頼性を保証するための**システム実装要件**について定義がされている	

比較観点④ 定義から読み取れる内容

比較観点④ 定義から読み取れる内容

- NZとNISTについて様々な角度からの比較を検討したが、難しいことが判明。理由は次の通り。

1. そもそも扱っているものが異なる
   例：NZのIASは「Information」だが、NISTのIALは「Identity」
   　　NZのAASは「Authentication」だが、NISTのAALは「Authenticator」

2. 片方にしか定義されていないものがある
   例：NZのBAS（Binding）、NISTにはBinding単体について記述した文書は無い

3. Level分けの個数が異なる
   例：NZは４段階だが、NISTは３段階

比較観点④ 定義から読み取れる内容

JNSA

- 前頁を踏まえ、（なかば強引に）NZとNISTの比較すると次の通り。

No.	項目	NZ	NIST	コメント
1	IAS/IAL	Information Assurance Standard • Level 1～4（4段階）	Identity Assurance Level • Level 1～3（3段階）	そもそも「Information」と「Identity」で保証対象が異なる
2	BAS	Binding Assurance Standard • Level 1～4（4段階）	（なし）	NISTには項目が無い
3	AAS/AAL	Authentication Assurance Standard • Level 1～4（4段階）	Authenticator Assurance Level • Level 1～3（3段階）	そもそも「Authentication」と「Authenticator」で保証対象が異なる
4	FAS/FAL	Federation Assurance Standard • Level 無し	Federation Assurance Level • Level 1～3（3段階）	NZにはLevelの分類が無い

比較観点④ 定義から読み取れる内容

- 前頁を踏まえ、（なかば強引に）NZとNISTの比較すると次の通り。
  - 赤枠部分を次ページ以降で比較

No.	項目	NZ	NIST	コメント
1	IAS/IAL	Information Assurance Standard • Level 1～4（4段階）	Identity Assurance Level • Level 1～3（3段階）	そもそも「Information」と「Identity」で保証対象が異なる
2	BAS	Binding Assurance Standard • Level 1～4（4段階）	（なし）	NISTには項目が無い
3	AAS/AAL	Authentication Assurance Standard • Level 1～4（4段階）	Authenticator Assurance Level • Level 1～3（3段階）	そもそも「Authentication」と「Authenticator」で保証対象が異なる
4	FAS/FAL	Federation Assurance Standard • Level 無し	Federation Assurance Level • Level 1～3（3段階）	NZにはLevelの分類が無い

比較観点④ 定義から読み取れる内容

JNSA

- NZ-IAS vs NIST-IAL

No.	項目	要求事項	
		NZ	NIST
1	Level 1	• RPはエンティティを証拠として用いるべきである。 • RPはそのエンティティを証拠して受け入れなければならない。	• 対面不要 • 収集しない/検証しない • ベースライン無し
2	Level 2	• RPは、少なくとも作成時に権威あるソースのコピーを参照した証拠を選択すべきである。 • RPは証拠を「額面通り」に受け取らなければならない。	• 対面および監視無しのリモート • SUPERIORまたはSTRONGなもの１つ/STRONGの強度を達成するプロセスで検証済 • SP 800-53中程度のベースライン
3	Level 3	• RPは、少なくとも権威のあるソースのコピーである証拠を選択しなければならない。 • RPは証拠を「額面通り」に受け取らなければならない。 • RPは詐欺対策技術を適用すべきである。	• 対面および監視付きのリモート • SUPERIORなもの２つ/SUPERIORの強度を達成するプロセスで検証済 • SP 800-53高のベースライン
4	Level 4	• RPは、権威ある情報源であるか、または権威ある情報源と連続的に同期したリンクを持つエビデンスを選択しなければならない。 • 信頼できる通信チャネルを介してシステム的に識別され、アクセスされる証拠に基づいて品質を設定しなければならない。 • RPは詐欺技術的対策を適用しなければならない。	（存在しない）

比較観点④ 定義から読み取れる内容

JNSA

- NZ-AAS vs NIST-AAL

No.	項目	要求事項	
		NZ	NIST
1	Level 1	• 1つの認証要素 • 知識認証は4文字以上の複雑さ	• 1つまたは2つの認証要素 • 30日に1回は再認証
2	Level 2	• 1つの認証要素 • 知識認証は12文字以上の複雑さ	• 2つの異なる認証要素 • 12時間に1回は再認証（非活動30分で再認証） • リプレイ耐性が必要
3	Level 3	• 2つの異なる認証要素 • 知識認証は4文字以上の複雑さ • 認証の連続失敗を制限	• 2つの異なる認証要素（ハードウェアベース） • 12時間に1回は再認証（非活動15分で再認証） • リプレイ耐性が必要
4	Level 4	• 2つの異なる認証要素 • 知識認証は12文字以上の複雑さ • 認証の連続失敗を制限 • プレゼンテーション攻撃（生体情報のなりすまし攻撃）に90%以上の耐性	（存在しない）

比較観点④ 定義から読み取れる内容

JNSA

- 【参考】NIST SP800-63 における Strength of Evidence

No.	Type of Evidence	Strength
1	US Passport	SUPERIOR
2	Foreign e-Passport	SUPERIOR
3	REAL ID cards（運転免許証のようなもの）	STRONG+
4	Enhanced ID cards（持つことのできる人がUS Citizenに限定。一部国向けにはパスポート代わりとして利用可能）	STRONG+
5	Permanent Resident Card（永住者カード）	STRONG
6	Native American Tribal Photo Identification Card（ネイティブアメリカン部族の写真付き身分証明書）	STRONG
7	Utility account statement（学生証：顔写真付き）	FAIR
8	Credit/debit card and account statement（公共料金明細）	FAIR
9	US Social Security Card（社会保障カード）	WEAK
10	Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal（出生証明書の原本）	WEAK

JNSA

比較観点⑤ レベル分け

レベルの違い

		Information Assurance (IA)	Binding Assurance (BA)	Authentication Assurance (AA)
特徴		高いレベルほど 権威的源泉との関連の強さや 不正対策が求められる	高いレベルほど 本人の身体との関連の強さや 不正対策が求められる	高いレベルほど 複数の認証要素の利用に加え 各認証要素の強度が求められる
		対面確認の重要性は さほど強調されていない	生体認証は 本人との Binding が最も高い 認証器という観点に立脚	Lv4 では現行のNISTに先行し プレゼンテーション攻撃耐性を 必須化
参考	NIST	ー	他人受入率の高さゆえ生体認証 の単独利用を禁止する	ー

４．参考文献

参考文献

p.6, 他	New Zealand Government “Identification Management Standards”	https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/
p.8	Digital Nations	https://www.leadingdigitalgovs.org/
p.9	TRUSTDOCK “ニュージーランド政府発表の「新アイデンティティ管理基準」における IAL ポイントを読み解く”	https://biz.trustdock.io/column/nz_ims
p.10	Digital Nations “Thematic Working Groups”	https://www.leadingdigitalgovs.org/working-groups
p.11	RINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT: TOWARD THE DIGITAL AGE	https://www.idprinciples.org/
p.13, 14	アクセンチュア株式会社 “諸外国における共通番号制度を活用した行政手続のワンスオンリーに関する取組等の調査研究”	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/f8a3c045-6c82-4abf-b0bf-cf18bdb79c38/bbf9c127/20220512_policies_mynumber_report_02.pdf

参考文献（続き）

p.13, 14	Microsoft “機密情報の種類のエンティティ定義”	https://learn.microsoft.com/ja-jp/microsoft-365/compliance/sensitive-information-type-entity-definitions?view=o365-worldwide
p.13	Teudat Zehut – Israeli Identification	https://www.nbn.org.il/life-in-israel/government-services/teudat-zehut-israeli-identification/
p.13	NZ “Kiwi Access Card”	https://kiwiaccess.co.nz/
p.13	Guidance GOV.UK Verify	https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
p.14	Government of Canada “Guideline on Identity Assurance”	https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30678&section=html
p.18, 他	NIST SP800-63-3 “Digital Identity Guidelines”	https://pages.nist.gov/800-63-3/sp800-63-3.html
p.34	IPA “サービスに応じたデジタル本人確認ガイドラインの検討”	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/093e09a7-2ffe-4a41-971a-5c0dcfd3c0b3/20220125_meeting_trust_dx_02.pdf

5． Appendix.

Information Assurance (IA) のレベル定義

IAレベル	要件	要求されるコントロール（レベルごとに差分があるもののみ抜粋）
4	情報の正確性	• **権威的源泉または権威的源泉と継続的に同期したリンクを持つ証拠**を使用しなければならない
	証拠の質	• **信頼できる通信チャネルを介してシステム的に識別され、アクセスされる証拠**に基づいて品質を設定しなければならない
	証跡の状態確認	• 証跡のステータス (一時停止、取消等) により証跡を使用できなくするため、証跡発行者または同等のサービスプロバイダーに**登録されたステータスを確認しなければならない**
	詐欺対策技術	• **詐欺（fraud）対策技術を適用しなければならない**
3	情報の正確性	• 少なくとも**権威的源泉のコピーを証拠**として使用しなければならない
	証拠の質	• **手動で特定された証拠**に基づいて品質を決定しなければならず、また、**再現するために独自の知識を必要とする物理的な機能**を含まなければならない
	証跡の状態確認	• 証跡のステータス (一時停止、取消等) により証跡を使用できなくするため、証跡発行者または同等のサービスプロバイダーに**登録されたステータスを確認すべき**である
	詐欺対策技術	• **詐欺（fraud）対策技術を適用すべき**である
2	情報の正確性	• **権威的源泉の作成したコピーを参照した証拠**を選択すべきである
	証拠の質	• 証拠を**額面通りに**受け取らなければならない
1	情報の正確性	• そのエンティティを証拠として用いるべきである
	証拠の質	• そのエンティティを証拠として受け入れなければならない

Binding Assurance (BA) のレベル定義

BAレベル	要件	要求されるコントロール（レベルごとに差分があるもののみ抜粋）
4	バインディング手法の選択	• 認証保証要件に準拠した**生体認証要素を知識または所持要素のいずれかで使用**、または同等以上の保証レベルの既存の認証器または資格情報を使用しなければならない
	詐欺対策技術	• **詐欺（fraud）対策技術を適用しなければならない**
	状態の再確認	• 認証イベントに生体認証要素が含まれていない限り、必要なBAのレベルと一致していることを5年に1度は再テストして確認しなければならない
	侵害の確認	• 認証器の発行者または同等のサービスプロバイダーとともに**侵害を確認しなければならない**
3	バインディング手法の選択	• **少なくとも2つのバインディング要素**、または同等以上の保証レベルの既存の認証器または資格情報を使用しなければならない
	詐欺対策技術	• **詐欺（fraud）対策技術を適用すべき**である
	状態の再確認	• 認証イベントに生体認証要素が含まれていない限り、**必要なBAのレベルと一致していることを5年に1度は再テストして確認しなければならない**
	侵害の確認	• 認証器の発行者または同等のサービスプロバイダーとともに**侵害を確認すべき**である
2	バインディング手法の選択	• **少なくとも1つのバインディング要素**、または同等以上の保証レベルの既存の認証器または資格情報を使用しなければならない
	状態の再確認	• 必要なBAのレベルと一致していることを5年に1度は再テストして確認すべきである
1	状態の再確認	• 必要なBAのレベルと一致していることを5年に1度は再テストして確認すべきである

Authentication Assurance (AA) のレベル定義 1

AAレベル	要件	要求されるコントロール（レベルごとに差分があるもののみ抜粋）
4	認証器の所有者の正しい行動の確保	• 認証器の所有者に義務を説明する条件を発行しなければならない • 認証器の所有者が義務を思い出すための定期的な連絡を行わなければいけない • **生体要素を含む2つの異なる認証要素**を実装することにより、認証器の共有を制限しなければいけない • 認証の連続失敗は30回までに制限し、**アカウントを無効化しなければならない**
	所有要素の不正利用防止	• **生体要素と組み合わせる**ことにより、取得された所有要素の使用を防がなければならない
	知識要素の推測からの保護	• **知識要素は12文字以上または少なくとも3種以上の文字種の中から7文字以上などと同等の複雑さとしなければならない** • **同じ文字の反復等を禁止することにより、容易に推測可能な知識要素の生成を制限しなければならない** • 失敗した試行を5回に制限し、それ以上の認証試行を最低30分間禁止しなければならない • **生体要素と組み合わせる**ことにより、推測された知識要素の使用を防がなければならない
	知識要素の開示の防止	• **生体要素と組み合わせる**ことにより、開示された知識要素の使用をふせがなければならない
	所有と生体要素のなりすましからの保護	• 所持要素に関する物理的でないチャレンジに対して予測不可能な動的応答を使用し、応答有効時間を最大10分またはメッセージング遅延がほとんど存在しない場合は1分に制限しなければならない • 生体認証チャレンジのスプーフィングに対処しなければならない • **プレゼンテーション攻撃に対して90%以上の耐性を持たなければならない**
	生体要素の他人受入率の管理	• **系統的な比較**により、生体認証比較の誤検知の発生を減らさなければならない • **異なる認証要素と組み合わせることにより、生体要素の確率的性質から保護しなければならない**

Authentication Assurance (AA) のレベル定義 2

AAレベル	要件	要求されるコントロール（レベルごとに差分があるもののみ抜粋）
3	認証器の所有者の正しい行動の確保	• 認証器の所有者に義務を説明する条件を発行しなければならない • 認証器の所有者が義務を思い出すための定期的な連絡を行わなければいけない • **2つの異なる認証要素**を実装することにより、認証器の共有を制限しなければいけない • **認証の連続失敗は30回までに制限し、アカウントを無効化すべきである**
	所有要素の不正利用防止	• **異なる認証要素と組み合わせる**ことにより、取得された所有要素の使用を防がなければならない
	知識要素の推測からの保護	• **知識要素は最低4文字の数字またはスワイプポイントの照合などと同等の複雑さとしなければならない** • **同じ文字の反復等を禁止することにより、容易に推測可能な知識要素の生成を制限すべきである** • 失敗した試行を5回に制限し、それ以上の認証試行を最低30分間禁止しなければならない • **異なる認証要素と組み合わせる**ことにより、推測された知識要素の使用を防がなければならない
	知識要素の開示の防止	• **異なる認証要素と組み合わせることにより、開示された知識要素の使用を防がなければならない**
	所有と生体要素のなりすましからの保護	• 所持要素に関する物理的でないチャレンジに対して予測不可能な動的応答を使用し、応答有効時間を最大10分またはメッセージング遅延がほとんど存在しない場合は1分に制限しなければならない • 生体認証チャレンジのスプーフィングに対処しなければならない
	生体要素の他人受入率の管理	• **いずれかの方法により、生体認証比較の誤検知の発生を減らさなければならない** • **手動比較の場合は、異なる認証要素と組み合わせることにより、生体要素の確率的性質から保護しなければならない**

Authentication Assurance (AA) のレベル定義 3

AAレベル	要件	要求されるコントロール（レベルごとに差分があるもののみ抜粋）
2	認証器の所有者の正しい行動の確保	• **認証器の所有者に義務を説明する条件を発行しなければならない** • **認証器の所有者が義務を思い出すための定期的な連絡を行わなければいけない**
	知識要素の推測からの保護	• **知識要素は12文字以上、または少なくとも3種以上の文字種の中から7文字以上と同等レベルの複雑さとしなければならない** • **同じ文字の反復等を禁止することにより、容易に推測可能な知識要素の生成を制限しなければならない** • **失敗した試行を5回に制限し、それ以上の認証試行を最低30分間禁止しなければならない**
	所有と生体要素のなりすましからの保護	• **所持要素に関する物理的でないチャレンジに対して予測不可能な動的応答を使用し、応答有効時間を最大10分またはメッセージング遅延がほとんど存在しない場合は1分に制限しなければならない** • **生体認証チャレンジのスプーフィングに対処しなければならない**
1	認証器の所有者の正しい行動の確保	• 認証器の所有者に義務を説明する条件を発行すべきである • 認証器の所有者が義務を思い出すための定期的な連絡を行ってもよい
	知識要素の推測からの保護	• 知識要素は最低4文字の数字またはスワイプポイントの照合などと同等の複雑さとしなければならない • 同じ文字の反復等を禁止することにより、容易に推測可能な知識要素の生成を制限すべきである • 失敗した試行を10回に制限し、それ以上の認証試行を最低15分間禁止すべきである
	所有と生体要素のなりすましからの保護	• 所持要素に関する物理的でないチャレンジに対して予測不可能な動的応答を使用し、応答有効時間を最大10分またはメッセージング遅延がほとんど存在しない場合は1分に制限してもよい • 生体認証チャレンジのスプーフィングに対処してもよい

6．執筆メンバー

■検討・執筆メンバー（順不同）　（ドキュメントを読むサブSWG)

株式会社NTTデータ	宍戸 りさ　（サブWGリーダー）
TIS株式会社	斎藤 知明
NECソリューションイノベータ株式会社	相馬 一洋
株式会社TRUSTDOCK	竹位 和也
株式会社リクルート	西村 宗晃
伊藤忠テクノソリューションズ株式会社	花井 杏夏
日本電信電話株式会社	星野 亮
日本ビジネスシステムズ株式会社	見上 昌成

■本WGの活動内容およびメンバーは以下の紹介ページを参照いただきたい。

【デジタルアイデンティティWG紹介ページ】 https://www.jnsa.org/active/std_idm.html