標準化部会
デジタルアイデンティティWG
活動報告2023

2023/06/07

WGリーダー　宮川　晃一
日本電気株式会社

概要

デジタルアイデンティティWGでは、2022年度様々なテーマで活動をしてきました。
　その中から、「特権ID管理ガイドライン」および「NZ政府が定めたID管理基準の考察」について成果物としてまとめることができましたので、その内容について概説いたします。

デジタルアイデンティティWGの紹介

活動の目的

「デジタルアイデンティティＷＧの目的」

本WGは“デジタルアイデンティティ”全般を広く議論する場として、
今年度で設立１８年目を迎えました。

本WGでは、デジタルアイデンティティの課題等について議論し、
導入指針や各種報告書の提示、執筆活動・セミナー・勉強会等での
啓蒙活動および普及促進、関連他団体との連携による市場活性化等を
目的として活動を行っています。

メンバー紹介：
https://www.jnsa.org/active/std_idm.html

これまでの活動

年	成果物等	WG名称
2005	WG設立	内部統制におけるアイデンティティ管理WG
2006	合宿実施（三浦マホロバツインズ）	
2007	内部統制における アイデンティティ管理解説書（第１版）	
2008	内部統制における アイデンティティ管理解説書（第２版）	
2009		
2010	クラウド環境における アイデンティティ管理ガイドライン （企業向け調査レポート）	セキュリティにおけるアイデンティティ管理WG
2011		
2012	改定新版　クラウド環境におけるアイデンティティ管理ガイドライン（書籍） エンタープライズ ロール管理解説書（第１版）	
2013	OpenID ConnectとSCIMの エンタープライズ利用ガイドライン	アイデンティティ管理WG
2014	エンタープライズ ロール管理解説書（第2版）	
2015	１０周年記念セミナー！ エンタープライズ ロール管理解説書（第3版）	
2016	エンタープライズにおける特権ID管理 解説書（第１版）	
2017	ID管理システム導入における現状把握チェックリスト（第１版） クロスボーダー時代のアイデンティティ管理セミナー!	
2018	内部統制における アイデンティティ管理解説書（第２版）	
2019	クレデンシャルの歴史（読み物）	
2020	Software Design 11月号特集（雑誌）	デジタルアイデンティティWG
2021	Enterprise Identity Day！ 標準化部会セミナー！	
2023	今さら聞けない暗号技術＆認証・認可（書籍） 改定新版　エンタープライズにおける特権ID管理ガイドライン（解説編） ミニウェビナー＆Youtube 「？？？とアイデンティティ」	

これまでの成果物

https://www.jnsa.org/result/digitalidentity/index.html

▶ ・2023/5/8

報告書 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==

▶ ・2023/3/31

報告書 【改定新版】特権ID管理ガイドライン　解説編

▶ ・2023/3/6

関連書籍発売 「Software Design　今さら聞けない認証・認可」が再編集されて別冊シリーズで発売されました。
技術評論社さんのページにリンクします。

▶ ・セミナー 2023/5/25開催　参加登録受付中

セミナー｜デジタルアイデンティティWGミニウェビナー「？？？とアイデンティティ」

2021/11/26

セミナー資料　2021年11月26日（金）開催
「Enterprise Identity Day　再考！！エンタープライズ・アイデンティティ～ゼロトラストセキュリティの礎を確立する～」

▶ ・執筆「Software Design」2020年11月号

特集1「今さら聞けない認証・認可ーセキュアなIAMを実現するために覚えておきたいこと」
技術評論社さんのページにリンクします。

▶ ・読み物 「クレデンシャルの歴史」

▶ ・報告書 「ID管理システム導入における現状把握チェックリスト（第１版）」

▶ ・出版書籍 「<改訂新版>クラウド環境におけるアイデンティティ管理ガイドライン」
Amazonにリンクします

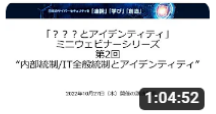
▶ ・報告書 「OpenID ConnectとSCIMのエンタープライズ利用ガイドライン」
（JNSAとOpenID Foundation Japanとの共同執筆）

▶ ・報告書 「エンタープライズにおける特権ID管理解説書（第１版）」

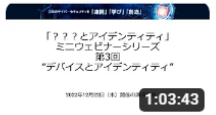
▶ ・報告書 「エンタープライズロール管理解説書（第３版）」

1 

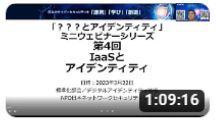
デジタルアイデンティティWGミニウェビナー第1回「ネットワークとアイデンティティ」
JNSA Channel・1173 回視聴・6 か月前

2 

デジタルアイデンティティWGミニウェビナー第2回「内部統制/IT全般統制とアイデンティティ」
JNSA Channel・459 回視聴・4 か月前

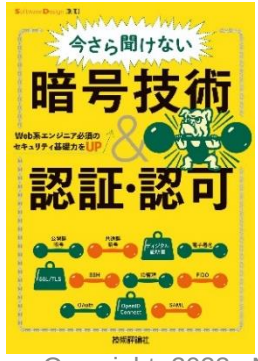
3 

デジタルアイデンティティWGミニウェビナー第3回「デバイスとアイデンティティ」
JNSA Channel・228 回視聴・3 か月前

4 

デジタルアイデンティティWGミニウェビナー第4回「IaaSとアイデンティティ」
JNSA Channel・162 回視聴・1 か月前

YouTube JP



昨年度の成果

昨年度やったこと-1

【テーマ】

１．ミニウェビナー開催　？？？とアイデンティティ　　全５回　　youtube 公開中

https://www.jnsa.org/seminar/digitalidentity/index.html

第1回2022年8月25日（木）16:00～17:00　テーマ：ネットワークとアイデンティティ

第2回2022年10月27日（木）16:00～17:00　テーマ：内部統制/IT全般統制とアイデンティティ

第3回2022年12月22日（木）16:00～17:00　テーマ：デバイスとアイデンティティ

第4回2023年2月22日（水）16:00～17:00　テーマ：IaaSとアイデンティティ

第5回2023年4月20日（木）　16:00～17:00　テーマ：自社運用システムとアイデンティティ

https://www.jnsa.org/seminar/digitalidentity/index.html

チャンネル登録とGood！
お願いします！

２．特権ID管理ガイドライン

【改定新版】特権ID管理ガイドライン　解説編公開

https://www.jnsa.org/result/digitalidentity/2022/index.html

３．標準化ドキュメントを読んでみる

NZ政府による“Identification Management Standards”に関する考察　公開

https://www.jnsa.org/result/digitalidentity/2023/idm1/index.html

本日解説

昨年度やったこと-2

４．ID管理技術勉強会

第１回目：認証連携　SAML/OIDC
第２回目：認可　OAuth
第３回目：当人認証　FIDO

５．ブレイクアウトセッション

第１回：各テーマごとの課題（初心者、エンプラ、当人認証、次世代）
第２回：次年度のテーマ検討（初心者、エンプラ、当人認証、次世代）

６．LT発表

新メンバーの方からそれぞれLT発表

７．各社ソリューション説明

TRUSTDOC様より

８．国際動向　UPDATE

ISO/IEC JTC 1/SC 27 WG5（アイデンティティ管理とプライバシー技術）

改定新版　特権ID管理ガイドライン（解説編）

はじめに

本書は2016年度に発行した、「エンタープライズにおける特権ID管理解説書（第１版）」について、これまでに多くのご意見やご指摘をいただいたものを反映すべく再度内容について検討を行い、新たな形で発行するものである。

今回の解説書は２部構成として、１部は「解説編」２部は「実践編」とした。
「解説編」では、特権ID管理の重要性や特権IDの捉え方、インシデント事例などを紹介した。
「実践編」では、実際に特権IDを行うための仕組みや運用方法について解説予定である。なお、「実践編」については現状未完成であるため、完成した際にはぜひ続けてご拝読いただきたい。

これから、特権ID管理を導入検討する人には、プロジェクトの推進の準備として、また、現在特権ID管理システムを導入中の人にとっては、現在のプロジェクトをよりよくするためのチェック・ヒント集として、ご活用していただけると考えている。

目次-1

目次-2

情報システムにおける特権IDとは

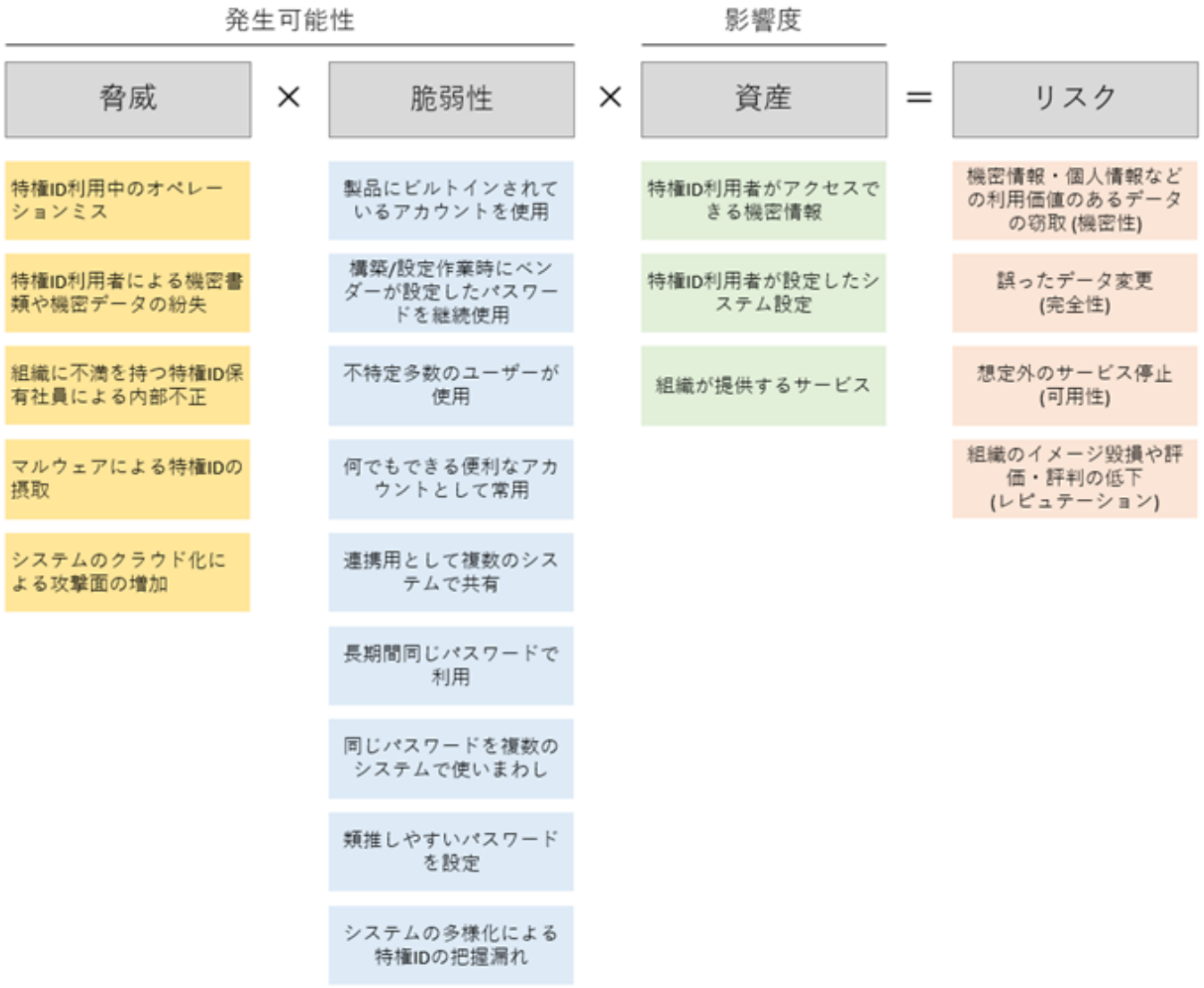
情報システムにおける権限とは、システム内のリソースやファイルへのアクセス権やプログラムの実行権、他のユーザーやプロセス等とのデータの共有権限などが考えられる。それらの権限に対して、一般のユーザーより特別に与えられる優越的な権利が、情報システムにおける特権となる。
※欧米では「特権アクセス管理（PAM）」と呼ばれることが多い。

種別	利用目的	保持する権限
一般ID	通常業務で使用	通常業務で使用する必要最低限の権限
特権ID	特別な操作が必要な業務で使用	全ての権限（全権）、あるいは全権に準ずる権限（高権限）

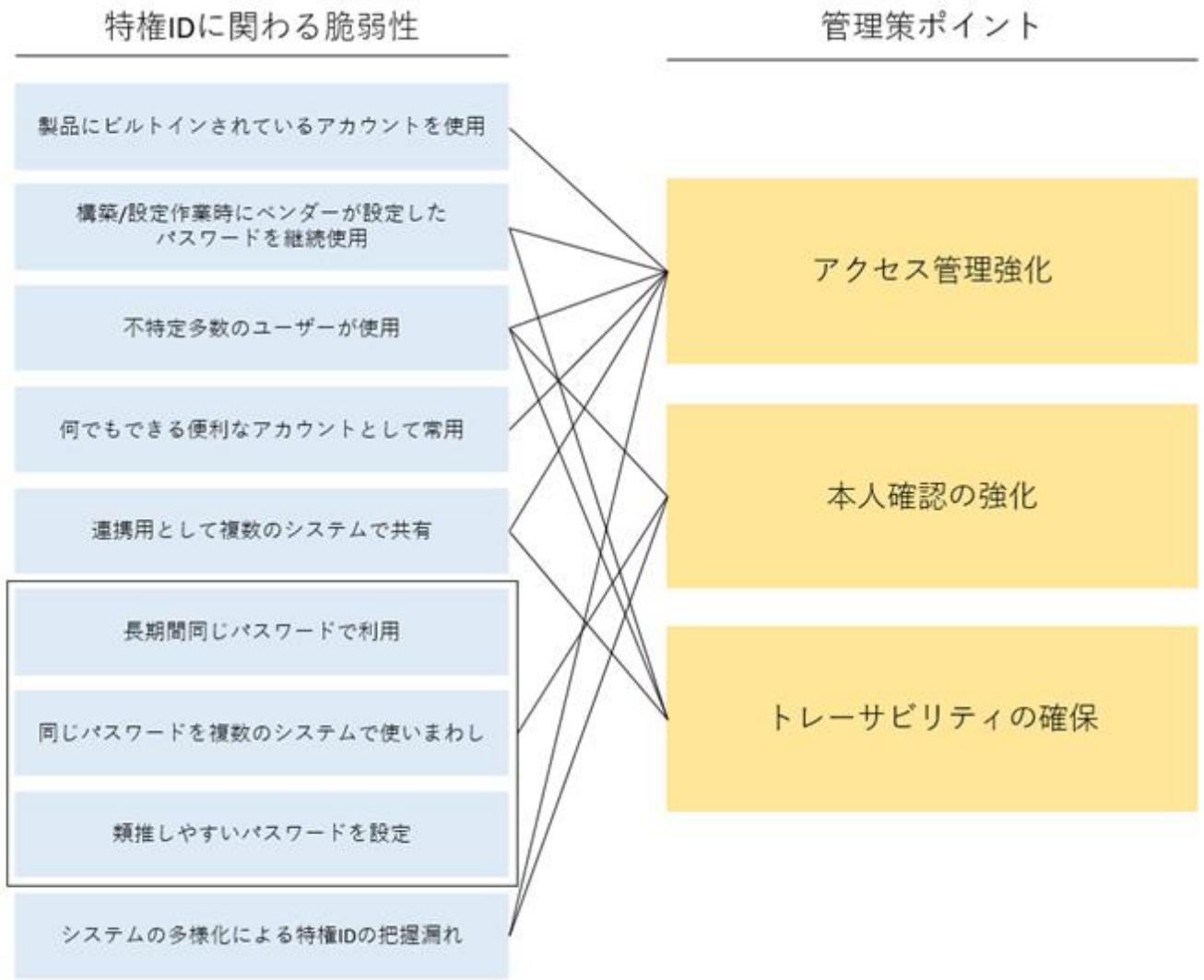
特権IDの例

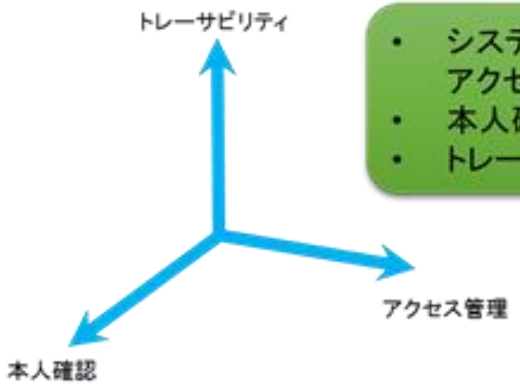
特権ID	説明
root/Administrator	Linux/Windows等のOSやハイパーバイザにおいて、あらゆる操作に対する権限を持つ　※ビルトイン管理者アカウントともいう
Administratorsグループに所属するID	Windows OSにおいて、あらゆる操作に対する権限を持つ
Windows Server Operators、Windows Account Operators、Backup Operatorsのようなグループに所属するID	Windows OSにおいて、特定の機能を利用する場合に必要な操作に対する権限を持つ（アカウント管理権限、バックアップ権限など）
sa	Microsoft SQL Server（データベース）において、あらゆる操作に対する権限を持つ
SYS、SYSTEM、SYSADMINなどのグループに所属するID	Oracle Database（データベース）において、あらゆる操作に対する権限、あるいは特定の機能を利用する場合に必要な操作に対する権限を持つ（バックアップ権限など）
enableコマンドによる特権行使	ネットワーク機器において、あらゆる操作に対する権限を持つ（enableコマンドを使用することで、通常モードから特権モードに移行する）
AWS、Azure、GCP等のクラウドサービス登録時のメールアドレス	当該クラウドサービスにおいて、あらゆる操作に対する権限を持つ
アプリケーションの管理者ID （アプライアンスを含む）	アプライアンスやアプリケーションにおいてあらゆる、操作に対する権限を持つ

特権ID固有リスクの整理



特権IDの管理策ポイント





- システム組み込みまたはオプション機能による
  アクセス管理強化（権限最小化）
- 本人確認の強化
- トレーサビリティの確保

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

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

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

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

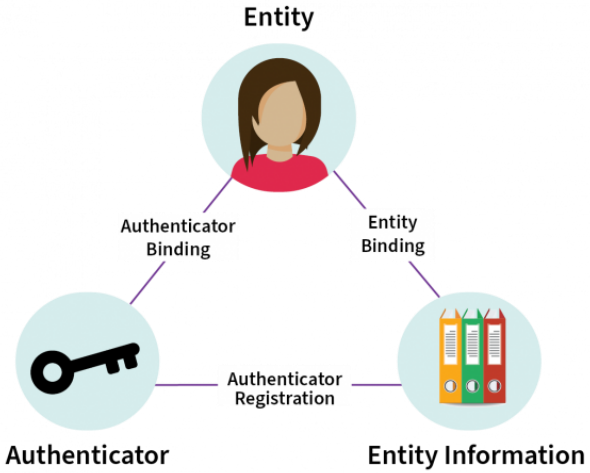
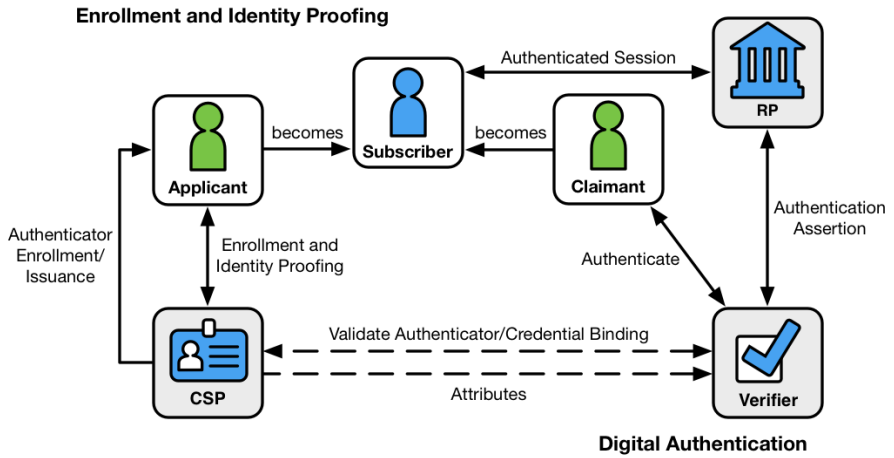
■ NZ、NISTの各ドキュメントについては、内容の記載よりドキュメントとしての目指している方向性が異なる

■ 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

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

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）

	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

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）

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	―	他人受入率の高さゆえ生体認証 の単独利用を禁止する	―

ご意見、お問合せ、WG参加等

事務局まで