資料１

令和４年１月25日
トラストを確保したDX推進SWG（第４回）

事務局説明資料

デジタル庁

トラストを確保したDX推進SWGスケジュール

2021年12月末

- トラストスコープで集中的にニーズやユースケースを検討する範囲特定
- 電子化できる手続・取引の主要事例

2022年3月末

- トラスト実態調査分析結果に基づく対応検討
- Identificationのアシュアランスレベル整理
- トラストサービスのアシュアランスレベル整理

2022年6月末

- トラストポリシー基本方針
- ユースケース選定
- 報告書とりまとめ（日・英）

アウトライン

1. これまでの主な意見
2. Identificationアシュアランスレベルにおける海外の先行事例
3. Identificationアシュアランスレベル検討の進め方
4. トラストサービスのアシュアランスレベル

これまでの主な意見

トラストスコープの再整理

- 中小企業を巻き込むことが重要。
- トラストサービスの信頼できる運用に加えて、DFFTや包括的データ戦略のビジョンを踏まえたデータの信頼性等も考慮すべき

アシュアランスレベルの整理

- トラストサービスの通用性確保のため、公的手続き及び民民取引において必要なトラストサービスの統一的な基準を示すことが重要
- アシュアランスレベルはシンプルかつ明確なレベルを示すべき
- EUのみならず米国の状況も検討し、多様な国との相互認証を視野に入れる必要がある
- アシュアランスレベルの基準作りについて、認印相当等のアナログの世界とは異なる基準が必要ではないか
- サービスプロバイダの安全性やポータビリティ確保を含めたTAL(Trust Assurance Level)をアシュアランスレベルに含めることが重要
- レベルは、「手段」で分類するだけでなく、SP800-63-3Bに倣って、「脅威耐性」ベースで検討するべき
- プロセスだけでなく、IDやクレデンシャルを発行するオーソリティに相当するレベルについて議論することが必要
- 電子契約については、リスクと利便性を考慮して、本人性と完全性の確認において適切なレベルの電子署名等を利用することが必要

トラストポリシーの基本的考え方

- 裁判での文書の真正性は判例法理で形成されているため、裁判における安定性確保は、新法を作るより、解釈・運用の世界で対応するべき
- 法律としてトラスト技術を細かく書きこむと、社会の方が先に動いて法律が参照されないという事態になることに留意するべき
- 裁判における安定性は、トラストサービスの普及とセットで考えるべき
- 国内に限って使えるフレームワークにすると海外との取引に支障がでるので国際相互連携を確保した仕組みにするべき
- 電子署名法３条Q＆Aの「十分な水準の固有性」について、２要素認証以外にも例示があると利用者にとって分かりやすい

国の関与の在り方

- 法的インフラとして、eシールに関する法的根拠がないところがボトルネックになっている
- 国として、企業の事務手続きにトラストサービスを導入するためのインセンティブ設計を行うことが重要

Identificationのアシュアランスレベルにおける海外の先行事例

海外におけるIdentificationアシュアランスレベルの状況

定義カテゴリ	定義内容	各国の整備有無状況（内容の差異は存在）		
		eIDAS	NIST SP800-63	NZの Identification 管理基準
本人確認（IAL※1）	本人確認方法の確からしさをレベル分けする	✓	✓	✓
認証プロセス（AAL※1）	認証プロセスによって認証強度をレベル分けする	✓	✓	✓
トラストサービス事業者の運営条件	トラストサービスの提供元が信頼できる機関であるかどうかを定めた要件を満たすかどうかによってレベル分けする	✓	–	–
認証情報連携（FAL※1）	認証した情報を別機関に連携する際の連携方法の確からしさをレベル分けする	–	✓	✓
割当（Binding※2）	RP(Relying Party)が個人や組織といったエンティティをエンティティの情報に割り当てたり、エンティティを認証プロバイダーに割り当てるプロセスの堅牢性をレベル分けする	–	–	✓

※1 SP800-63-3 におけるアシュアランスレベルの定義名を記載
※2 ニュージーランドのIdentification管理基準におけるアシュアランスレベルの定義名を記載

eIDAS：Electronic Identificationアシュアランスレベル

electronic identificationのアシュアランスレベルを３つのレベルに規定している。

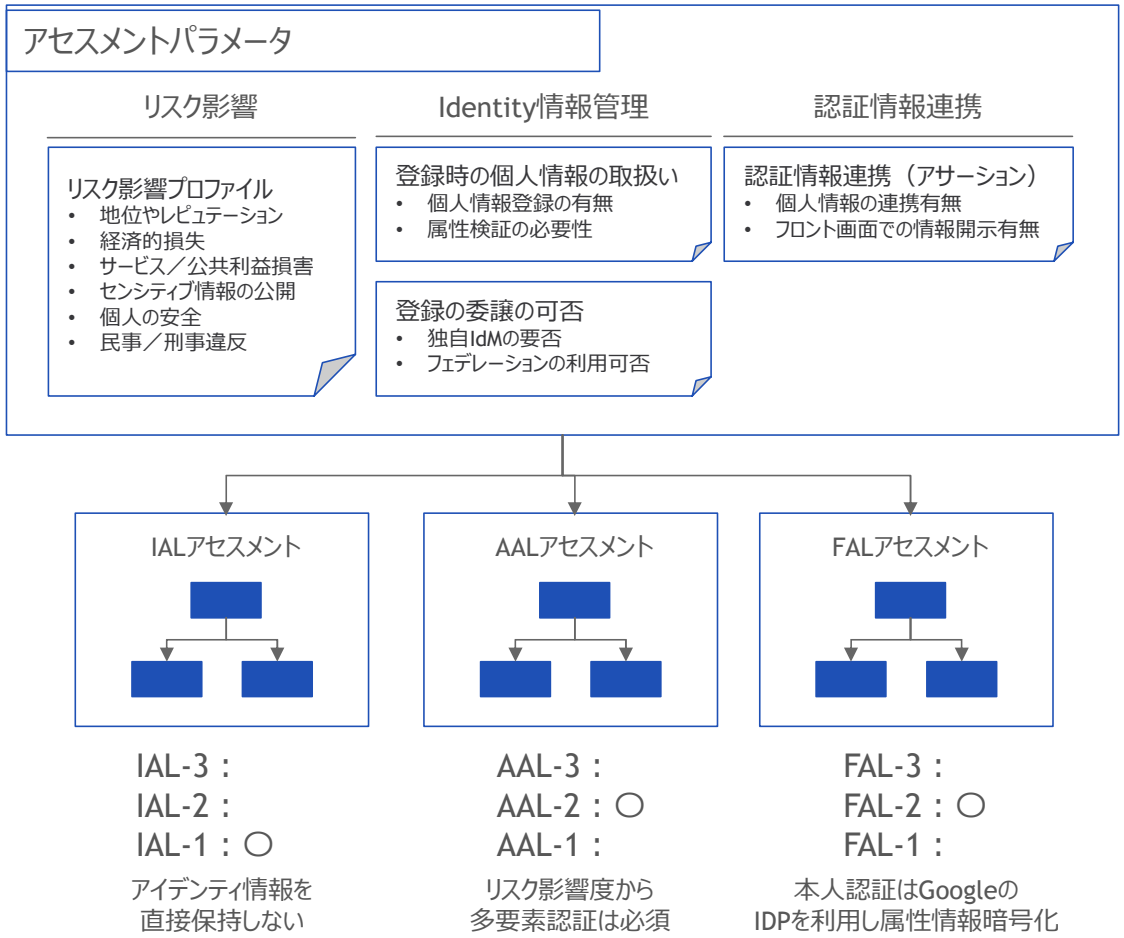
LoA	概要	具体例
Low	• 個人の身元に対して限定された程度の信頼度を提供。Identityの誤用又は改ざんリスクを減らすことを目的 • eIDAS仕様外の簡易なトラストサービス • トラストサービスプロバイダによって提供。事後監査が必要	サービスへの入会を、本人がウェブページを通じてセルフで行うケース。 本人性確認等は実施しない。
Substantial	• 個人の身元に対してSubstantialレベルの信頼度を提供。Identityの誤用又は改ざんのリスクを大幅に減らすことを目的 • 仕様に幅がある	サービスへの入会において、個人のアイデンティティ情報の提示が必須とするケース。 サービス利用時に、ユーザID／パスワード認証、および多要素認証（SMSへのワンタイムパスワード送付等）を必要とする。
High	• 個人の身元に対してSubstantialのアシュアランスレベルを備えた電子識別手段よりも高い信頼度を提供。Identityの誤用又は改ざん防止を目的 • 厳密に守るべき要件やポリシーが定められている • 適格トラストサービスプロバイダによって提供。定期的な監査が必要	サービスへの入会において、有人・対面による本人確認を必須とするケース。 サービス利用時の認証は、国民IDカード等スマートカードの利用を必要とする。

Source:eIDAS – The Ecosystem (EUROPEAN COMMISSION)(https://www.eid.as/), eIDAS Levels of Assurance (LoA) (Connecting Europe Facility)(https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+Assurance)

SP800-63-3：基本的な考え方

各事業者が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、適切なアシュアランスレベルを選択する基準を提示

アシュアランスレベルのアセスメントフロー



アセスメントの意義／効果

- **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マネージメントの実現**

  各サービス事業者が、サービスが取り扱うIdentityのリスク影響度を６カテゴリで定義し、規定された共通のアセスメントロジックによりアシュアランスレベルを個別に選択できるようにする。

  例）本来必要とされるレベル以上のアシュアランスを実現するため、コスト増大するようなケースを抑止する。

- **マイクロサービス化されたIdentity ソリューションへの対応**

  政府システムにおいてもIdentityソリューションは単一ベンダーが全機能を提供するモノリシックなものとは限らない。

  分散マイクロサービスによるアイデンティティ管理／認証連携を前提とするアシュアランスレベル選択を可能とする。

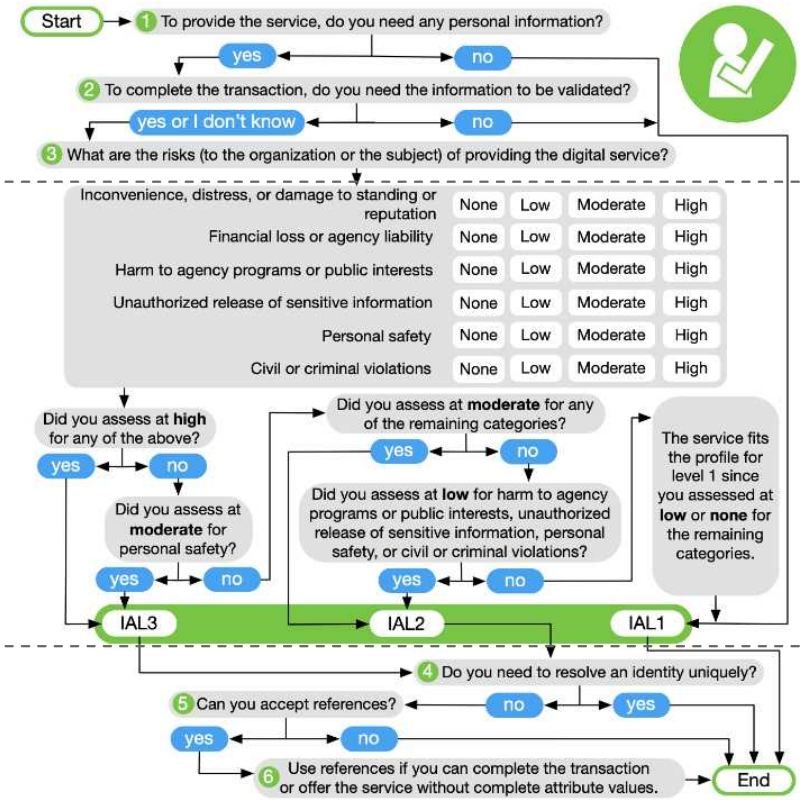
  例）Identity Management／認証はプラットフォーマーのIDP機能へ委譲（フェデレーション）する

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)等を元に作成

（参考）SP800-63-3：IALのアセスメントロジック

リスク影響度に加えて個人情報の取扱い有無やアイデンティティの独自管理の要否を加味し、LoAの選択肢を増やしている

IALのアセスメントフロー



アセスメントの要諦

- 個人情報の取扱い有無、属性情報等のバリデーション要否

  サービス登録時、個人情報の取扱いがない場合、ある場合も属性情報のバリデーションが必要ない場合はIAL1を許容する。

- リスク影響度に合わせたアシュアランスレベル決定
  - 6項目のうち一つでもHighがあればIAL-3相当
  - 上記以外で、個人の安全がModerateリスクがある場合IAL-3
  - 上記以外で 1 項目でもModerateがあればIAL-2
  - 上記以外で以下4項目でLowがあればIAL-2
    （サービス／公共利益損害、センシティブ情報の公開、個人の安全、民事／刑事違反）
  - 上記以外はIAL-1

- アイデンティティの独自管理の要否、Identityリファレンスの可否

  Identityの独自管理が不要で、他ソリューションへの参照情報が可能であればフェデレーションによるIdentity連携を推奨する。

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)

SP800-63-3：アシュアランスレベル定義

各事業者がリスク影響度や個人情報の取扱い有無等をもとに、ユーザーの身元情報、ユーザー認証、連携方法の確からしさからアシュアランスレベルが定義されている

定義内容	定義LoA	LoAの詳細	
ユーザ身元確認の確からしさ	IAL（Identity Assurance Level）SP 800-63A	IAL.1	身元確認不要、自己申告の登録でよい。メールアドレスの到達確認など
		IAL.2	識別に用いられる属性をリモートまたは対面で確認する必要あり
		IAL.3	識別属性を対面で確認する必要があり。検証担当者は有資格者
ユーザ認証の確からしさ	AAL（Authentication Assurance Level）SP 800-63B	AAL.1	1要素または2要素による認証
		AAL.2	2要素認証が必須。2要素目の認証手段はソフトウェアベースも可能
		AAL.3	2要素認証が必須。2要素目の認証手段はハードウェアベースが必須
連携方法の確からしさ	FAL（Federation Assurance Level）SP 800-63C	FAL.1	アサーション（RPに送るIdPでの認証結果データ）への署名
		FAL.2	FAL.1に加え、対象RPのみが復号可能な暗号化
		FAL.3	FAL.2に加え、Holder-of-Key アサーションの利用（ユーザごとの鍵とIdPが発行したアサーションを紐づけてRPに送り、RPはユーザがそのアサーションに紐づいた鍵を持っているか（ユーザの正当性）を確認）

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)

NZ政府Identification管理基準：基本的な考え方

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、適切なアシュアランスレベルを選択する基準を提示

アシュアランスレベルのアセスメントフロー

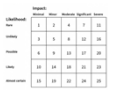
リスクの定義
影響度と発生確率の掛け算

リスク1：サービスまたはトランザクションのために誤った情報が提供される（改ざん）

ビジネス的な損失の影響度と発生可能性を5段階で評価
金銭的な損失または責任：影響度1 × 発生可能性1
機密情報の不正な公開：影響度2 × 発生可能性1
レピュテーションリスク：影響度1 × 発生可能性1
その他の損失または責任：影響度1 ×発生可能性1

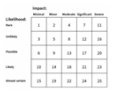
リスク2：サービスまたはトランザクションにおける情報または認証機関に、別の人が関連付けられる（なりすまし）
ビジネス的な損失の影響度と発生可能性を5段階で評価
金銭的な損失または責任：影響度3 × 発生可能性2
機密情報の不正な公開：影響度4 × 発生可能性3
レピュテーションリスク：影響度3 × 発生可能性3
その他の損失または責任：影響度2 ×発生可能性2

アセスメントロジック（マトリクス）
金銭的な損失または責任：リスクレベル1
機密情報の不正な公開：リスクレベル2
レピュテーションリスク：リスクレベル1
その他の損失または責任：リスクレベル1
最大値を取るため、リスクレベルは2



IAL-4：
IAL-3：
IAL-2：
IAL-1：〇

アセスメントロジック（マトリクス）
金銭的な損失または責任：リスクレベル13
機密情報の不正な公開：リスクレベル17
レピュテーションリスク：リスクレベル13
その他の損失または責任：リスクレベル5
最大値を取るため、リスクレベルは17



AAL/BAL-4：
AAL/BAL-3：〇
AAL/BAL-2：
AAL/BAL-1：

アセスメントの意義／効果

- 想定されるリスクが定義されている
  Identificationに関する想定リスク（改ざん／なりすまし等）が定義されており、各リスク発生時のビジネス／セキュリティの影響度がパラメータ化されている
- 発生確率が考慮されており、リスク影響度の発生期待値を見たより現実的なリスクアセスメントとなっている
  リスク影響度とリスク発生可能性をそれぞれ5段階で評価することで、適切なアシュアランスレベルを精度を高く選択できる。（発生確率も見ることで、ほぼ起こりえないリスクに対してコスト高なアシュアランスレベルを選択しないよう工夫されている。）
- バインディング
  人を身元確認のための情報や認証プロバイダーのユーザーID/PASS等の認証子に関連付けるプロセスを指す。なりすましリスクの低減に加えて、本人情報の鮮度／整合性を担保することを目指す

Source: Identification management (digital.govt.nz)(https://www.digital.govt.nz/standards-and-guidance/identification-management/)等を元に作成

NZ政府Identification管理基準：リスク及びアシュアランスレベル

リスク影響度とリスク発生可能性をレベル分けし、マトリクス表を用いて総合的にリスクレベルとアシュアランスレベルを判断

リスク影響度とリスク発生可能性のレベル分け

ビジネス的な損失の影響度と発生可能性を5段階のレベルで評価

ビジネス的な損失

- 金銭的な損失または責任
- 機密情報の不正な公開
- レピュテーションリスク
- その他の損失または責任

リスク影響度

- Minimal
- Minor
- Moderate
- Significant
- Severe

リスク発生可能性

- Rare
- Unlikely
- Possible
- Likely
- Almost certain

マトリクス表によるリスクレベル評価

以下のマトリクス表を基に、各ビジネス的な損失のリスクレベルを評価

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

リスクレベルによるアシュアランスレベル評価

算出されたリスクレベルの最大値及び以下の表を基に、アシュアランスレベルを評価

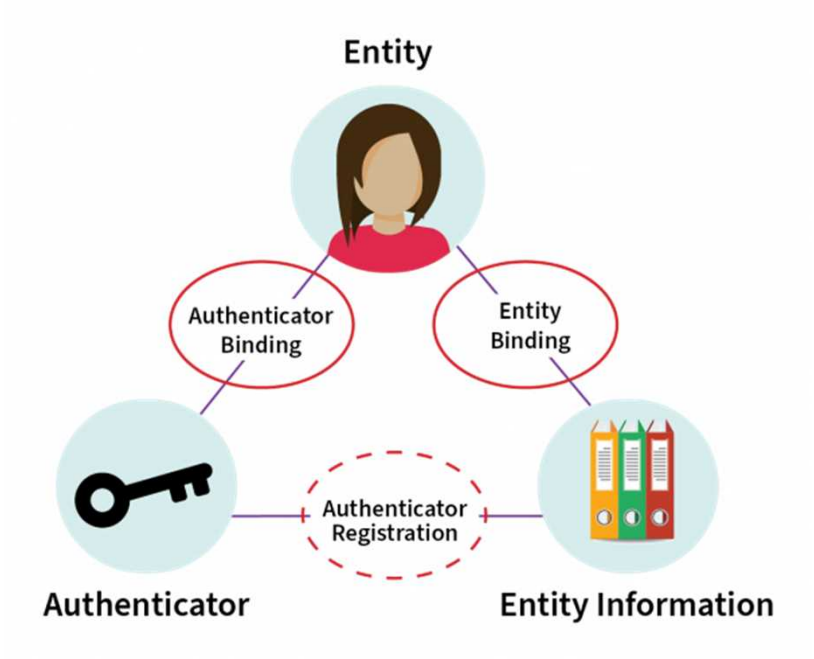
リスク1	リスク2	対応するアシュアランスレベル
1–3	1–3	Negligible — Level 1
4-6	4-10	Low — Level 2
7-19	11-19	Moderate — Level 3
20-25	20-25	High – Level 4

Source: Identification management (digital.govt.nz)(https://www.digital.govt.nz/standards-and-guidance/identification-management/)

（参考）NZ政府Identification管理基準：バインディング

人を正当な情報及び認証子に関連付けるプロセスを指し、なりすましリスクを考察するための概念

バインディングイメージ図



バインディングとは？

- 概要
  Entity（人）をEntity Information（本人確認書類から読み取れる個人情報など）に関連付けたり、EntityをAuthenticator（認証プロバイダーなど）に関連付けるプロセスを意味する
  バインディングには、認証と同様に、知識要素、所有要素、生体要素が使用される

- 実施タイミング
  バインディングは、主には登録時だが、それだけではなく、エンティティ情報の存続期間中のさまざまな時点で実行される
  - Entity InformationがEntityに紐ついていない時（出生登録、割り当てられていないプリペイドカードなど）
  - 新しいAuthenticatorを追加する時
  - BindingのAssurance Level を上げる時
  - Entity Informationが漏洩している可能性があり、再紐付けが必要な時

- Assurance Levelの表現意義
  バインディングのAssurance Levelを定義することで、主には登録時の身元確認のなりすましに加え、上記のユースケースにおけるEntityとInformation、Authenticatorとの関連付けるへのリスク低減の強弱を表現する

Source: https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/binding-assurance-standard/

NZ政府Identification管理基準：アシュアランス要素の規定

定義内容	定義	LoAの詳細	
情報エビデンスの確からしさ	Information Assurance	IAL.1	エビデンスはエンティティの自己主張である
		IAL.2	エビデンスは信頼できるソースのコピーの一部を参照している
		IAL.3	エビデンスは信頼できるソースのコピーであり、品質・有効性が保証されている
		IAL.4	エビデンスは信頼できるソースそのものであり、品質・有効性が保証されている
エンティティ紐付けの確からしさ	Binding Assurance	BAL.1	バインディングのための情報が提供されているが条件はなし＋整合性の維持
		BAL.2	1要素以上の認証子をバインディングに使用＋整合性の維持
		BAL.3	2要素以上の認証子をバインディングに使用＋整合性の維持や不正対策技術等の要件
		BAL.4	生体要素含む2要素以上のバインディングを紐付けに使用＋整合性の維持や不正対策技術等の要件
ユーザ認証の確からしさ	Authentication Assurance	AAL.1	1要素認証
		AAL.2	1要素認証＋認証子保有者の義務に関する規約の発行義務等の要件
		AAL.3	生体要素を含む1要素認証、または2要素認証
		AAL.4	生体要素を含む2要素認証
認証情報連携の確からしさ	Federation Assurance	なし	

Source: Identification Management Standards (**https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/**)を元に作成

Identificationアシュアランスレベル検討の進め方

トラスト確保のニーズが確認された主なユースケース

Source: 個人アンケート調査/企業アンケート調査

Identificationのアシュアランスレベルの整理を進める上での留意点

- アシュアランスレベルの整理が必要となる理由
  - リスクと利便性を考慮した適切なサービスの選択
  - デジタル完結におけるオンラインでのアナログの世界とは異なる基準の必要性 等
- 技術動向の変化
  - クラウドやスマートデバイスの普及　等
- アシュアランスレベルの整理における基準
  - 個人の安全や経済的損失等へのリスク　等
- アシュアランスレベル実装の在り方

Identificationに関するアシュアランスレベルでの論点案

1. 身元確認や認証プロセスのレベルの議論において、基本的考え方はどうあるべきか？

2. 身元確認や認証プロセスのレベルの議論において、昨今の技術動向を踏まえて考慮すべきユースケースはどのようなものか？

3. 身元確認や認証プロセスに加えて、認証情報連携やバインディングの基準について考慮すべきか？

（参考）IALで考慮すべき事例

IAL	身元確認方法		身元確認におけるリスク軽減パターン[1]	
	Identifier	確認方法	正当な身元確認証明を第三者に不正に利用されてしまうリスク	身元確認証明が偽造され、なりすまし利用されてしまうリスク
IAL-3	信頼できる機関により電子的に身元証明可能なもの	対面で確認	◎	◎
	発行元保証されている身元証明可能なもの	対面での有資格者による確認	◎	◎
		対面相当オンライン(eKYC[2])	○?	○?
	発行元保証されている身元証明可能なもの	オンライン登録後対面で確認	○	△
IAL-2	信頼できる機関により電子的に身元証明可能なもの	非対面で確認	×	○
	発行元保証されている身元証明可能なもの		×	△
	–	犯収法eKYC	○	○?
IAL-1	身元確認のない自己表明可能なもの	身元確認なし	×	×

eKYCのアシュアランスレベルはどう考えるか?

1. 検証者が誤認してしまう(正当なものを不当、不当なものを正当だと判断)するレベルは、有資格者 = eKYC > それ以外の手法と仮定
2. リアルタイムでの写真撮影や動画での確認等、不正利用防止のためにリアルタイム性を担保された証拠の提出が必須である仕組みをeKYCと想定

（参考）AALで考慮すべき事例

AAL	認証プロセス	想定リスク及び各本人確認方法によるリスク軽減是非	
AAL-3	多要素認証 (含む耐タンパー性を持つハードウェアトークン)	複数要素	◎
AAL-2	多要素認証	複数要素	○
AAL-1	一要素認証	単要素	×
AAL-0	認証なし	無し	×

耐タンパー性を持つハードウェアトークンの多様化により、認証プロセスの定義の詳細化や変更が必要になるか？

Note: SP800-63BのAAL.3における認証は、ハードウェアベースの認証機に加え検証者との認証済み保護チャネルを構築することで検証者なりすまし攻撃への耐性を求められており、その内容を参考に記載。

トラストサービスのアシュアランスレベルにおける主な論点案

1 アシュアランスレベルの基準

- トラストサービスのアシュアランスレベルに関して、どのような基準が考えられるか
- 考慮すべき要素（トラストレベルの担保、国際的な通用性、ユーザーへのわかりやすさ等）
- 具体的なユースケースにおける検討

2 機動性の確保

- 技術進化に対応した柔軟な見直しが求められる中、機動性の確保するための考え方
- トラストアシュアランスレベルの策定/運営の在り方

（参考）構成員・オブザーバー

構成員

手塚　悟	慶應義塾大学環境情報学部　教授 (主査)
濱口　総志	慶應義塾大学SFC研究所　上席所員
宮内　宏	宮内・水町IT法律事務所　弁護士
林　達也	LocationMind株式会社　取締役
宮村　和谷	PwCあらた有限責任監査法人　パートナー
太田　洋	西村あさひ法律事務所　パートナー弁護士
崎村 夏彦	東京デジタルアイディアーズ株式会社　主席研究員
佐古 和恵	早稲田大学　基幹理工学部情報理工学科　教授

その他関係行政機関

総務省	サイバーセキュリティ統括官付参事官
法務省	民事局商事課長
経済産業省	商務情報政策局サイバーセキュリティ課長

オブザーバー

伊地知　理	一般財団法人日本データ通信協会　情報通信セキュリティ本部 タイムビジネス認定センター長
佐藤　創一	一般社団法人新経済連盟　政策部長
西山　晃	電子認証局会議　特別会員（フューチャー・トラスト・ラボ　代表）
山内　徹	一般財団法人日本情報経済社会推進協会 常務理事・デジタルトラスト評価センター長
若目田　光生	一般社団法人日本経済団体連合会 デジタルエコノミー 推進委員会企画部会 データ戦略 WG 主査
太田　大州	デジタルトラスト協議会　渉外部会長
小川　博久	日本トラストテクノロジー協議会　運営委員長 兼株式会社三菱総合研究所　デジタル・イノベーション本部 サイバー・セキュリティ戦略グループ　主任研究員
柴田　孝一	セイコーソリューションズ株式会社　DXサービス企画統括部　担当部長 兼トラストサービス推進フォーラム　企画運営部会　部会長
袖山　喜久造	ＳＫＪ総合税理士事務所　所長・税理士
中武　浩史	Global Legal Entity Identifier Foundation (GLEIF) 日本オフィス　代表
小松　博明	有限責任あずさ監査法人 東京ＩＴ監査部　パートナー
中須　祐二	SAPジャパン株式会社　政府渉外　バイスプレジデント
小倉　隆幸	シヤチハタ株式会社 システム法人営業部　部長
島岡　政基	セコム株式会社IS研究所　主任研究員
佐藤　帯刀	クラウド型電子署名サービス協議会　協議会事務局
三澤　伴暁	PwCあらた有限責任監査法人　パートナー
小川　幹夫	全国銀行協会　事務・決済システム部長
豊島　一清	DigitalBCG Japan　Managing Director
野崎　英司	金融庁　監督局　総務課長
田中　彰子	厚生労働省 医政局 研究開発振興課 医療情報技術推進室長
杉　眞里子	独立行政法人情報処理推進機構（IPA）デジタルアーキテクチャ・デザインセンター（DADC） インキュベーションラボ　デジタル本人確認プロジェクトチーム　プロジェクトリーダー（事務局）