

一般社団法人OpenIDファウンデーション・ジャパン  
KYCワーキンググループ

# 国内向けOpenID Connect for Identity Assuranceの普及と利便性向上に関する 検討レポート

次世代KYCレポート(Phase 5)

キーワード: eKYC, KYC, デジタル本人確認, 本人確認, 身元確認, 当人認証, OpenID Connect, OpenID Connect for Identity Assurance, Trust Framework, IAL, 身元確認保証レベル, AAL, 当人認証保証レベル, フェデレーション, 認証連携, トラストサービス

1. ご挨拶	2
2. はじめに	3
3. 国内向けIDA仕様の更なる普及のための検討	4
3.1. ユースケース分析結果から見えてきたこと	4
4. 検討結果の仕様への反映	6
4.1. 検討結果の国内向けIDA仕様への適用検討	6
4.2. 国内向けIDA仕様への反映	8
5. まとめ	13
6. Appendix	14
6.1. 過去検討の経緯	14
6.2. OpenID Connect for Identity Assurance最新動向	16
7. 用語集	17
8. 執筆者一覧	20

# 1. ご挨拶

2024年は、デジタルアイデンティティの分野において世界的に大きな変化と進展が見られた一年となりました。特に本ワーキンググループの対象領域である本人確認(KYC)においては、「OpenID Connect for Identity Assurance (IDA)」仕様の最終化という大きな節目を迎えました。

このIDA仕様の社会実装も急速に進んでおり、日本においてもデジタル庁が推進する法人認証基盤「GビズID」が本仕様に対応したことは、国際的にも注目を集める大きなニュースとなりました。一方で、不正に取得された携帯電話回線を用いた犯罪や、証券口座の乗っ取りなど、身元確認や当人認証の重要性が一層高まっていることも事実です。

こうした背景の中で、本ワーキンググループは2018年より継続して活動を行い、日本におけるOpenID Connect for Identity Assuranceの有効な活用に向けたプロファイルの策定などに取り組んできました。

近年では、Verifiable Credentialsやモバイル運転免許証(mdoc / mDL)など、身分証明書のデジタル化に関連する技術の社会実装も進んでおり、これらのデジタルクレデンシャルを活用したKYCの在り方についても、今後さらに議論と検討が求められています。実際に米国では、NISTのサイバーセキュリティセンター・オブ・エクセレンス(CCoE)が、デジタルクレデンシャルを活用したKYCの実証実験を金融機関と共に進めるなど、オンライン本人確認のデジタル化が世界的に加速しています。

我が国においても、こうしたグローバルな技術動向や標準化の流れを注視しながら、安全かつ信頼性の高いデジタル社会の構築を目指すことが重要です。OpenIDファウンデーション・ジャパンは、引き続き本ワーキンググループの活動を中心に、安心・安全なKYCの普及と標準化に向けて貢献してまいります。

本レポートが、業界関係者の皆さまにとって有益な知見を提供し、今後の取り組みの一助となれば幸いです。そして、関心をお持ちの皆さまには、ぜひ本ワーキンググループの活動にもご参加いただき、共により良いデジタル社会の実現を目指していただければと思います。

一般社団法人OpenIDファウンデーション・ジャパン  
代表理事 富士榮 尚寛

## 2. はじめに

本レポートは、OpenID ファウンデーション・ジャパンが主催する KYC ワーキンググループにて検討を行っている、「理想の KYC、次世代 KYC」について2022-2023年度に検討を行った結果をベースに取りまとめたレポートである。

本レポートでは、過去レポートで提案した「国内版OpenID Connect for Identity Assurance」(国内向けIDA仕様)に対して更なる普及、利便性向上を目的として、ユースケース分析、国内向けIDA仕様への反映を検討した経緯と内容をまとめたものである。

なお、「理想の KYC、次世代 KYC」については、Phase2 の活動結果として、2021年9月に「[次世代における KYC の方向性に関するレポート](#)」<sup>1</sup>、Phase3の活動成果として2022年12月に「[デジタル本人確認の国内での普及に向けたツール・ルールの検討レポート](#)」<sup>2</sup>を公開している。本レポートは、Phase 3 までの検討内容を踏まえた内容となっているため、過去検討内容については上記を参照されたい。また、過去の検討経緯については Appendix も合わせて参照されたい。

---

<sup>1</sup> <https://www.openid.or.jp/news/2021/09/kycwg.html>

<sup>2</sup> <https://www.openid.or.jp/news/2022/12/kycwg.html>

### 3. 国内向けIDA仕様の更なる普及のための検討

基本的な考えとして、法令等で本人確認について定めのないサービスにおいて、フェデレーションによる本人確認に必要なミニマム要件とは何かの検討から始めた。また、コンシューマ向けサービスにおいて、サービス提供をする際に何を求めるのか、意見を出し合った。例えば、料金さえ払ってもらえれば本人確認の必要はないサービスもあれば、リスクの低減や、特定の顧客層に限定したサービスを提供するため、本人確認が必要なサービスも存在する。今回の検討では後者を対象とし、実際のユースケースを想定しながら本人確認の目的や取得したい属性の整理、本人確認における課題の分析とその改善案の検討を行った。想定したユースケースについては、本人確認のニーズが見込める7つの業種に絞り込んで検討を行った。

#### 3.1. ユースケース分析結果から見えてきたこと

分析した内容をサマリーした結果が下記となる。

	項目	個人情報を取り扱う目的	本人確認書類で確認している属性	その他の手段で確認している属性	自己申告で取得している属性
1	スポーツ施設	<ul style="list-style-type: none"> <li>不正利用防止 (②)</li> <li>緊急時の連絡 (①)</li> <li>防犯目的 (①)</li> <li>営業情報の送付 (④)</li> </ul>	<ul style="list-style-type: none"> <li>氏名</li> <li>生年月日</li> </ul>	<ul style="list-style-type: none"> <li>電話番号(本人)</li> <li>メールアドレス</li> <li>在籍証明</li> </ul>	<ul style="list-style-type: none"> <li>住所</li> <li>性別</li> <li>電話番号(緊急連絡先)</li> </ul>
2	資格試験	<ul style="list-style-type: none"> <li>受験当日の本人確認 (②)</li> </ul>	<ul style="list-style-type: none"> <li>氏名</li> </ul>		<ul style="list-style-type: none"> <li>生年月日</li> <li>住所</li> <li>性別</li> <li>電話番号</li> </ul>
3	学習教材	<ul style="list-style-type: none"> <li>教材の発送</li> <li>成績管理</li> <li>支払先管理</li> <li>営業販促 (④)</li> </ul>			<ul style="list-style-type: none"> <li>氏名</li> <li>住所</li> <li>年齢</li> <li>電話番号</li> </ul>
4	チケット販売	<ul style="list-style-type: none"> <li>不正転売防止 (②)</li> </ul>	<ul style="list-style-type: none"> <li>氏名</li> <li>生年月日</li> <li>住所</li> </ul>	<ul style="list-style-type: none"> <li>電話番号</li> </ul>	<ul style="list-style-type: none"> <li>性別</li> </ul>
5	コンタクトセンター	<ul style="list-style-type: none"> <li>契約者と電話先ユーザーの一致確認 (②)</li> <li>なりすまし防止 (②)</li> <li>配送先・連絡先・支払い</li> </ul>			<ul style="list-style-type: none"> <li>氏名</li> <li>生年月日</li> <li>住所</li> </ul>

		情報の確認 ・申し込みの意思確認			
6	映画・居酒屋	・年齢判定 (③) ・顧客囲い込み (④)	・年齢情報 (生年月日)	・学生証明 (在籍証明)	・氏名 ・生年月日 ・住所 ・性別
7	カラオケ	・年齢判定 (③) ・顧客囲い込み (④)	・年齢情報 (生年月日)	・学生証明 (在籍証明) ・電話番号	

表 3-1 ユースケース分析結果

ユースケースの分析を行った結果、本人確認等によって個人情報を取得・検証する目的として

- ①防犯・顧客保護:不正行為者の特定や、事故等発生時の緊急連絡のため
- ②不正利用の防止:当人が授受すべきものを他人に授受させないため
- ③年齢制限:年齢制限があり、違法行為・条例違反にならないかの確認のため
- ④属性に基づくプロモーション:特定の年齢層(若年・高齢者等)や地域に対する利用促進施策のため

が挙げられることが多いことが確認できた。

上記目的のため、多くのユースケースにおいて氏名・住所・生年月日の確認・取得が行われているが、年齢や所属など享受資格の有無に係る身元確認においては在籍証明、また連絡先取得の観点においては住所に加えて電話番号を取得するケースが多いことがわかった。

課題として、年齢確認のような特定の年齢以上という情報だけで良いケースにおいても、生年月日以外の情報や生年月日自体の取得が行われておりプライバシー上の懸念があることや、電話番号や在籍証明といった追加の属性情報を要求するケースがあることが判明した。また、マイナンバーカードを利用した身元確認を行っている場合において、年齢情報のみが必要な場合においても基本4情報を取得しているケースがあることが判明した。

## 4. 検討結果の仕様への反映

### 4.1. 検討結果の国内向けIDA仕様への適用検討

前章までのユースケース分析・検討を踏まえて、過去検討を進めた国内向けIDA仕様に対してどのように反映していけるかを検討した。

IDA仕様とは、OpenID Foundationで策定された、OpenID Connect for Identity Assuranceをはじめとする3つの仕様を合わせた仕様群のことである。KYC WGでは、IDA仕様を国内で利用しやすくするためのプロフィールについて検討してきた。IDA仕様の詳細や、プロフィールの検討経緯については6章を参照されたい。

国内向けIDA仕様では、scopeの値を設定することで比較的容易に身元確認済み情報を取得できるような仕様として整理したが、今回の検討においても同様の考え方でユースケースの整理から取得する身元確認済み情報の追加のセットを整理している。

### verified\_claimsの構成

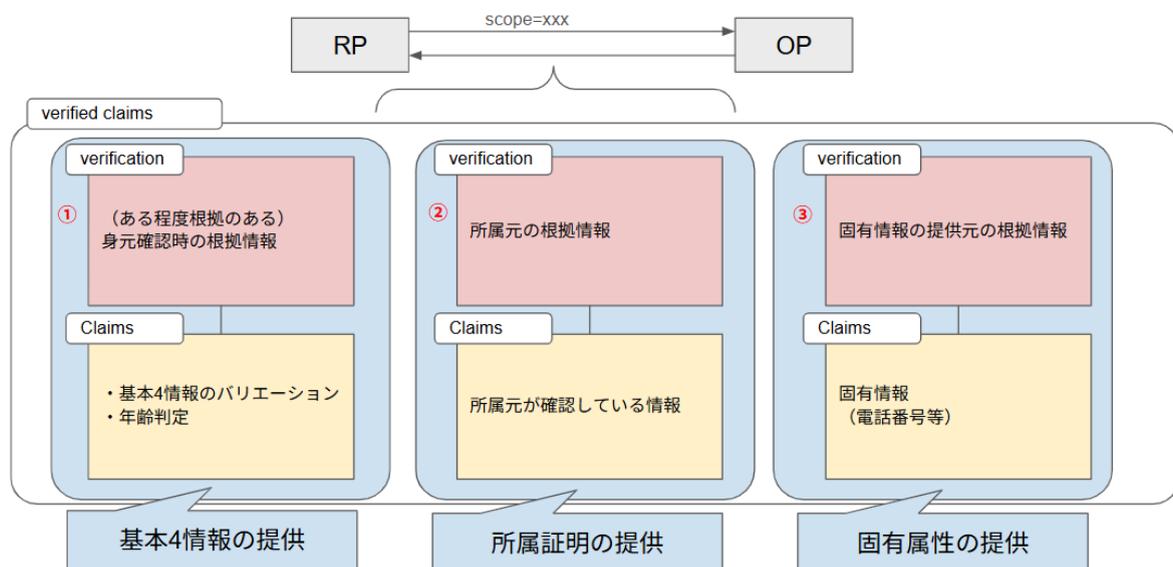


図 4-1 verified\_claimsの構成

図4-1は、IDA仕様の`verified_claims`のJSONの構成に今回の検討結果を反映したものを図で表現したものである。どのような身元確認結果を行ったかの根拠情報(`verification` 要素)と属性情報(`claims` 要素)を提供すべきかを整理した。

図 4-1の①②③はそれぞれ根拠情報と属性情報の組を示している。`verification` 要素でどういった根拠情報を提供すべきか、`claims` 要素でその時の属性情報として何を返却するのかを整理している。全体を一つの `verification` 要素と `claims` 要素で表現していないのは、それぞれ根拠となる情報が異なるためである。

①に関しては、国内向けIDA仕様として整理したものと同様のもので、法律に準拠しないまでもある程度根拠のある身元確認をしたということを根拠に、基本4情報をベースとした情報を提供する。

**verification** 要素としては、国内向けIDA仕様同様にある程度根拠のある身元確認を行ったという証跡を表現する。

**claims** 要素に関しては、ユースケースを踏まえ、基本4情報だけを提供するのではなく、バリエーションが必要と考えた。具体的には以下のようなClaimsのバリエーションが考えられると整理した。

#### 基本4情報ベース

・氏名・生年月日・住所  
年齢判定

- ・16 以上(例:労働基準法)
- ・18 以上(例:労働基準法・映倫 R18・成人)
- ・20 以上(例:酒・たばこ)

基本4情報のうち性別は明記されている本人確認書類が少ないこと、また本人確認の要素として必要とされるケースが少ないこともあり、国内向けIDA仕様での整理と同様に、提供する情報として氏名・生年月日・住所と整理している。

また、年齢判定のニーズも存在する<sup>3</sup>ことから、各法令等を参考に必要と思われるバリエーションも合わせて整理した。

②に関しては、ユーザの所属を表す情報を提供する。例えば、ユースケースとして学割の適用のため、大学に所属していることを証明する場合などに利用することを想定している。①では基本4情報をベースにその人が誰であるかを表現しているのに対して、②ではその人がどこに所属しているのか、を表現している。IDA仕様での表現を考えた場合、大学の学生データベースを根拠に身元確認を行った旨の情報を **verification** 要素に含めることは出来るが、「○○大学に所属している」ということを表現する Claims は標準では存在していない<sup>4</sup>。そのため、IDA仕様とは別に、Claims を定義する必要がある。ここまでユーザの所属情報をIDA仕様に適用する観点で検討したが、学生のユースケースを考えると、すべての学校がIDA仕様に対応ができるわけではない。大学であれば学認などのベースとなりうる仕組みがあるが、公立高校<sup>5</sup>などでは対応は難しく、一部の学生にし

<sup>3</sup> その他ニーズとして、民法上15歳以上で法的能力が認められるケースがあるが、民間において具体的なユースケースが想定できないため、対象外としている。

<sup>4</sup> 別の表現方法として、IDA仕様の拡張として検討されているAuthorityClaimsも検討したが、AuthorityClaimsは、何かを代表しての権限を持つ、といった意味合いを表現する仕様のため、大学を代表した学生である、とするのはニュアンスとしては異なることから、AuthorityClaimsを利用するのは正確ではないと判断した。

<sup>5</sup> 2025年よりデジタル庁が「教育分野の認証基盤の在り方に関する検討会」において初等中等教育における認証基盤のあり方の検討をすすめているが現時点で民間サービス等への利活用についての方向性は定まっていない。

<https://www.digital.go.jp/councils/education-authentication/d5c4a630-e234-4e5e-b14d-f64ef8666415>

か対応できないとなれば対応するメリットは薄い。また、オフラインでの所属確認としては、学生証等の目視確認がメインの確認手段でありIDA仕様を活用する必要性がない。オンラインでの需要は存在するもののIDA仕様を導入するほどのメリットを得ることは難しい。

③の固有情報の例としては、携帯電話番号がある。携帯電話事業者が発行元として提供することで信頼性の高い携帯電話番号の提供を想定している。

この場合、**verification** 要素は固有の属性情報の提供元が情報の発行元となるため、提供元が認証を行って本人を確認したと表現できる。

**claims** 要素は固有の属性情報を記載する形だが、①と同時に提供される場合にそれぞれの情報が同じ主体を示しているかを確認するために、氏名や生年月日、住所などを合わせて記載することが求められる可能性がある。

記載したように②③に関しては、公的な本人確認書類では提供できない属性情報を表現できるようなユースケースを検討したものである。

## 4.2. 国内向けIDA仕様への反映

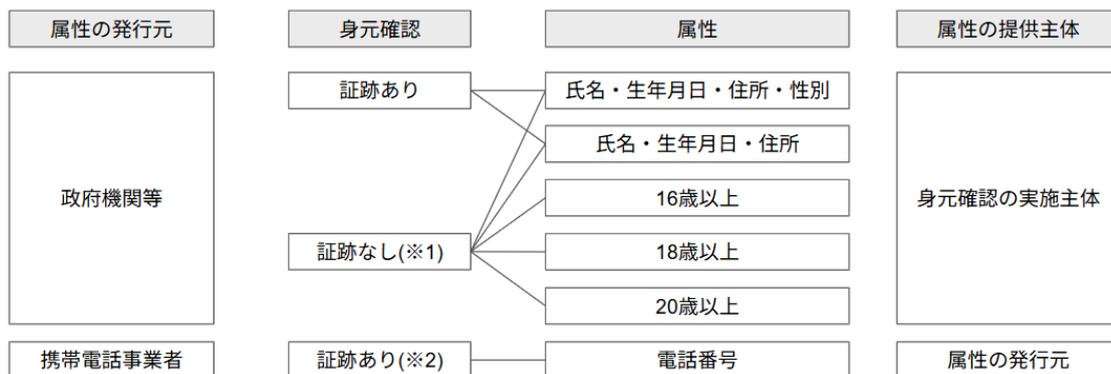
前章の検討結果をIDA仕様で表現する内容を整理すると、以下のようになる。

①については、過去整理した国内向け仕様に属性情報のバリエーションを持たせた形で再整理を実施する。

②については、ニーズはあるものの実現のハードルに対してメリットが十分得られない状況があることから、今回の整理では含めないこととする。

③については、固有の情報の提供元で認証することを **verification** 要素として、属性情報を提供することとする。

上記の内容を踏まえて、提供する根拠情報と属性情報のバリエーションを整理したものが以下の図である。



※1 何らかの身元確認はしているが、Verification要素としては不要  
 ※2 なんらか発行元としての本人確認をしていること（発行元での認証等）

図 4-2 提供する根拠情報と属性情報のバリエーション

基本4情報をベースとした身元確認を目的とする、属性情報の発行元が政府機関等（本人確認書類が、マイナンバーカードや運転免許証、在留カードなど）の場合、大きく分けて身元確認結果に証跡が必要な場合と、何らかの身元確認はしているがIDAの **verification** 要素としては不要とする場合の2パターンとした。過去のレポートで提案したレベル分けの考え方では4パターンに分けて整理していたが、そのうちの身元確認書類の画像データや有効期限内であることといった情報は身元確認結果のレコードとして保持しておらず、提供することが難しいことが見えてきたためである。また、属性情報として基本4情報（氏名、住所、生年月日、性別）のうち、性別を除いた3属性を基本とし、それとは別に年齢判定のバリエーションを設けている。性別に関しては本人確認書類に明記されて

いない場合が多いことから除外している。年齢判定のバリエーションに関しては、労働基準法(16歳以上、18歳以上)、映画倫理機構(R18等)、成人(18歳)、酒・たばこ(20歳以上)を基準にバリエーションを設けた。

また、属性情報の発行元が提供する情報として携帯電話事業者による携帯電話番号を設けた。これは、基本4情報以外の情報として提供するもので、携帯電話番号の発行元での確認結果(発行元での本人認証の情報等)を根拠情報として携帯電話番号を提供する形を想定している。

ここまでの整理結果から最終的に整理したScopeの種類は以下となる。

項番	Scope値	身元確認	属性情報	属性情報の提供主体	情報の発行元
1	jp_oidf_ida_with_evidence	証跡あり	氏名・生年月日・住所	身元確認の実施主体	公的機関等
2	jp_oidf_ida				
3	jp_oidf_ida_age_over_16		16歳以上		
4	jp_oidf_ida_age_over_18		18歳以上		
5	jp_oidf_ida_age_over_20		20歳以上		
6	jp_oidf_ida_msisdn	証跡なし <sup>6</sup>	携帯電話番号	属性情報の発行元	携帯電話事業者

表 4-1 scopeの種類

バリエーションそれぞれにscopeの値を設定しているが、項番6のscope(jp\_oidf\_ida\_msisdn)については携帯電話番号の真正性を証明するものであり、それ単独で要求する場合は身元確認としては利用できないことに注意が必要となる。

例として、項番1と6のscopeを要求された際のverified\_claimsを表現すると以下のようになる。

JSON

```
{
```

<sup>6</sup>

過去のレポートで整理したように、犯罪収益移転防止法などの法制度に記載されている公的身分の確認等ではなく、犯罪収益移転防止法などのレベル感までは求めないがそれなりに信頼度のある身元確認を実施していることを前提に証跡までは不要と整理。

デジタル本人確認の国内での普及に向けたツール・ルールの検討レポート

[https://www.openid.or.jp/news/nextgeneration\\_kyc\\_report\\_ph3.pdf](https://www.openid.or.jp/news/nextgeneration_kyc_report_ph3.pdf)

「8.3. 国内向けミニマム仕様の Scope 定義」を参照のこと

```

"sub": "248289761001",
"email": "taro@example.com",
"email_verified": true,
"verified_claims": [
  {
    "verification": {
      "trust_framework": "jp_oidf_ida",

      "time": "2023-01-23T01:23:45Z",
      "evidence": [
        {
          "type": "document",
          "check_details": [
            {
              "check_method": "vpip",
              "time": "2023-01-23T01:23:45Z",
              "document_details": {
                "type": "jp_individual_number_card",
                "date_of_issurance":
"2020-10-01T09:00:00Z",
                "date_of_expiry": "2030-01-28T08:59:59Z"
              }
            }
          ]
        }
      ]
    },
    "claims": {
      "name": "山田 太郎",
      "birthdate": "1956-01-28",
      "address": {
        "formatted": "東京都千代田区千代田1-1"
      }
    }
  },
  {
    "verification": {
      "trust_framework": "jp_oidf_ida",
      "time": "2023-01-23T01:23:45Z",
      "evidence": [
        {

```

```

        "type": "electronic_record"
      }
    ],
    "claims": {
      "msisdn": "819012345678"
    }
  }
]
}

```

この例は、マイナンバーカードを用いて対面で身元確認を行った根拠を基に氏名、住所、生年月日を取得すると同時に、携帯電話番号を発行した携帯電話事業者のアカウントで認証できたことを根拠に携帯電話番号を取得している。

具体的なユースケースとしては、とあるサービスが、携帯電話事業者から氏名、住所、生年月日、携帯電話番号を根拠情報とともに取得したいとする。この時、携帯電話事業者が本人確認情報を提供する際に、マイナンバーカードなどの身元確認結果を基に氏名、住所、生年月日を提供すると同時に、携帯電話事業者自体が提供する携帯電話番号を自身のサービスで認証できたことを根拠に提供する。このような形で、同じユーザを指しているがそれぞれ別の根拠情報をベースに属性情報を提供するような表現が可能となる。

一方で、scopeの値だけでは決定できない項目として、trust\_frameworkがある。trust\_frameworkはIDA仕様においては根拠情報を提供するOPがどのようなトラストフレームワークに則って身元確認を行ったのかを示すもので、例としては犯罪収益移転防止法やeIDAS、NIST SP800-63シリーズなどが想定されている。そのためscopeで身元確認の度合いや属性情報の種類を指定するにせよ、前提となるトラストフレームワークが何か、ということは規定する必要がある。

しかしながら、実際に情報を受け取る側のRPがOPと同じトラストフレームワークであることは規定されていない。

上記の例では、OPが"jp\_oidf\_ida"というトラストフレームワークで身元確認をしたことを示しており、RPはそのトラストフレームワークを信頼して結果を受け入れることが必要になる。そのため、実際に利用する際にはOPとRPがどのようなトラストフレームワークでやり取りができるかを規定することが重要となると考えられる。

本WGでは、IDA仕様を利用する際にどのようにトラストフレームワークを整理すればよいかを継続検討していきたい。

## 5. まとめ

本レポートでは、過去のレポートで提案した「国内版OpenID Connect for Identity Assurance」(国内向けIDA仕様)の更なる普及と利便性向上を目的とし、ユースケース分析および国内向けIDA仕様への反映を検討してきた。

具体的な検討内容として、まず法令等で本人確認について定めのないサービスにおいて、フェデレーションによる本人確認に必要なミニマム要件を検討した。コンシューマ向けサービスを対象とし、実際のユースケースを想定しながら本人確認の目的や取得したい属性情報の整理、本人確認における課題の分析とその改善案の検討を行った。

検討の結果、多くのユースケースにおいて基本4情報(氏名、生年月日、住所、性別)を取得している他、年齢や所属など享受資格の有無に係る確認においては在籍証明、また連絡先取得の観点においては住所に加えて電話番号を取得するケースが多いことがわかった。

これらのユースケース分析・検討を踏まえて、過去検討を進めた国内向けIDA仕様に対してどのように反映していけるかを検討した。

検討の結果、ユースケースに合わせたバリエーションの拡充を行った。年齢判定のバリエーションを利用頻度の高い16歳以上、18歳以上、20歳以上の3種類に増やし、また携帯電話番号を利用するケースが多いことが確認できたため、携帯電話番号についても返却できるように拡張を行った。携帯電話番号については、他の属性との併用を考慮し、scopeを同時に指定できるように変更を行った。

また、過去のレポートで提案していた本人確認書類の画像データや有効期限内であることといった情報は、フェデレーション先の事業者が身元確認結果のレコードとして保持しておらず、提供することが難しいことが見えてきたため、属性情報から削除した。

今後は、本レポートで得られた知見をもとに、国内向けIDA仕様の更なる普及に向けた検討を進めていくこととする。

## 6. Appendix

### 6.1. 過去検討の経緯

KYC ワーキンググループでは、Phase 1 の活動において、先行する海外事例について調査を行い、日本国内における今後の本人確認の理想像(次世代の目指すべき KYC の姿)について調査・検討を行った。

Phase 2 の活動においては、次世代の目指すべき KYC に求められる要件及び、OpenID Connect for Identity Assurance 1.0(以降、IDA)及び関連する仕様(主に分散/集約クレーム)を利用した社会実装の実現可能性の検討を行った。

Phase 3 の活動においては、次世代の目指すべき KYC モデルに関して、要件を「ツール」と「ルール」に分け改めて明確化を行った。また、日本国内で IDA 仕様を普及させるために、IDA のプロフィール仕様の検討に取り掛かった。

Phase 3 までの活動成果に関しては、各レポートを御一読いただきたい。

Phase 4, 5 では、Phase 3 までの活動を元にして、主に2つの検討活動を行った。

1つ目は Phase 3 から継続となる、IDA の日本国内向けプロフィール仕様の策定を行った。Phase 3 までの活動の中で、日本国内で IDA 仕様を普及させるためには、実装/利用が容易かつ、サービスや業界を超えた横断的な利用の出来るプロフィール仕様が求められると考えた。

IDA 仕様は諸外国において OP と RP 間で信頼関係がない状態においても動的に身元確認済み属性の流通を行えるように設計されているため、受け渡しする証跡や身元確認プロセスに関する情報が充実していたり、受け渡しする属性を要求する方法の設計が自由度の高いものになっている。一方、日本国内における身元確認の現実として、個人情報保護の観点等から事前に企業間の契約を締結することが標準的であり、その契約が流通させる情報の信頼の源泉となっている。また既に OpenID Connect の実装を行っている OP/RP が多数存在するため、既存の実装からの変更量が少ないほうが早く普及するのではないかと考えた。

これらの事情を加味し、身元確認済み情報のテンプレートを Scope で定義し、UserInfo Endpoint から返却されるように IDA 仕様の使用方法を制限する形で、日本国内向けのプロフィール仕様の策定を行った。

策定した国内向けプロフィールは、本レポートと合わせて公開しているため、御一読いただきたい。

2つ目は、日本国内における主要な身元確認のユースケース整理を行い、先述の国内向け IDA プロフィール仕様を適用可能かの分析・検討を行った。Phase 3 以前のレポートでも触れている通り、経済産業省が令和2年4月に発表した「オンラインサービスにおける身元確認手法の整理に関する検討報告書」において、中間強度の手法(適度に簡易で信頼性のある手法)としての、金融機関および携帯電話事業者等の身元確認APIの活用可能性について指摘されている。国内向けの IDA プロフィール仕様はこの中間強度での身元確認を主なユースケースとしているため、各業界の既存の身元確認業務に対して適用可能かを分析・検討し、プロフィールに求められる要件の検討を行った。

検討結果については、本レポートの5・6章にて紹介する。



## 6.2. OpenID Connect for Identity Assurance最新動向

前回レポートの通り、OpenID Connect for Identity Assurance (IDA) は、OpenID Connect (OIDC)の拡張仕様であり、API 経由で OpenID Provider (OP) から RP に提供される属性情報と、根拠情報を併せて提供するものである。OIDC で氏名、住所、電話番号、生年月日といった属性情報を提供する仕組みはある一方で、提供された氏名や住所などが、ユーザの自己申告に基づくものなのか、あるいは運転免許証などを提示し身元確認を行った結果として登録されたものなのかはわからない。

この問題に対応するのが IDA である。提供される属性情報が、何を根拠に、いつ、どのようなチェックを受けて確認されたものかといった根拠情報を含めて RP に返却することが可能となっている。これにより身元確認済みの顧客情報を持っている事業者が標準に準拠した形で、RP に対して根拠を含め情報提供できることになる。

具体的には、OIDC と IDA を利用することで、主に以下のようなことが標準化される。

- 身元確認プロセスに関する情報とその取得(リクエスト)方法
- 身元確認済みの属性情報の利用目的の通知と同意取得方法
- ID Token または UserInfo Response の返却内容に必要な属性情報の指定と必須属性情報の指定

これらの内容によって、RP はユーザや OP に対して ①サービスが身元確認しなければならない属性情報の明示的な要求、②ユーザに属性情報の利用目的の説明と同意の取得を行うことができるようになる。

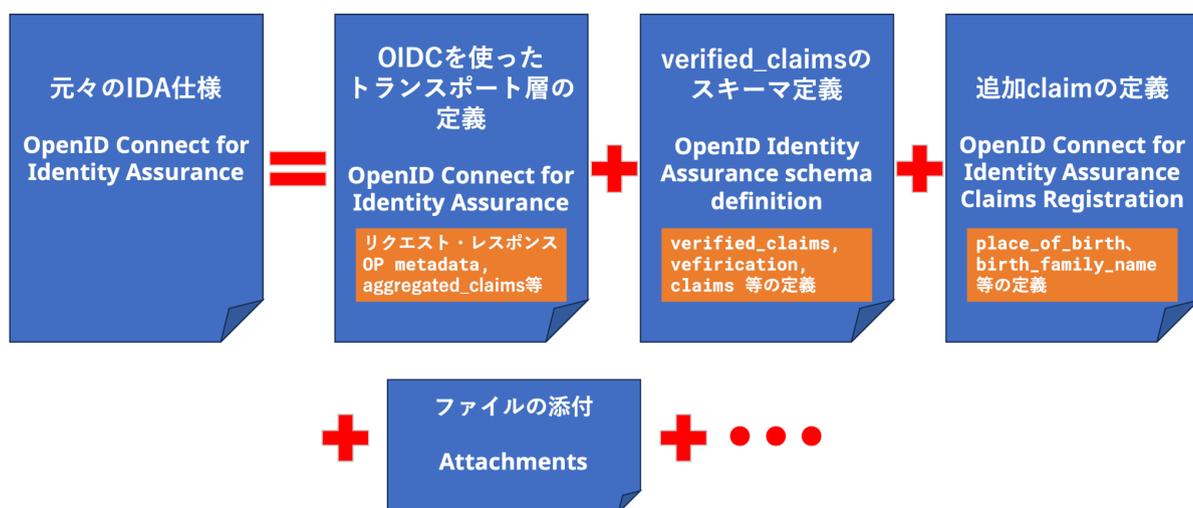
また、OP からの情報取得については、①自身のサービスで必要な最小限の個人情報の取得(データ最小化/データミニマイゼーション原則の達成) ②どのようなレベルや本人確認書類に基づいて身元確認を行ったかの取得が行えるようになる。

IDA 仕様は、WGの設立された2020年1月から、4th Implementers Draftが承認された2022年10月まで1本の仕様として作られてきたが、より広く利用されることを目的に、4つの仕様に分割され、2024年10月にFinal仕様として公開された。

具体的には、IDA仕様で定義されている“verified\_claims”のスキーマを、OpenID 以外のプロトコル(具体的にはVerifiable Credentials)でも利用したいという要望を受け、スキーマ定義を切り出すこととした。

同様に、新たに定義した身元確認のための claim 定義 (nationality, place\_of\_birth, msisdn等)、さらには、身分確認書類などのファイルを別途送付するための Attachment仕様も、IDA枠内に限らずOIDC文脈全般で使うことができるので、別仕様として切り出すこととした。

仕様を分割するという外形的には比較的大きな変更を行っているものの、内容については、4th Impremerter's Draft と比較し、normative (規範的: 実装に影響する) な変更では無いということで、新たなImpremerter's Draftを発行せず、直接仕様群をFinal化している。



IDA仕様群の概要については前回レポートを参照されたい。また、OpenIDファウンデーション・ジャパン KYC WGの有志メンバーで、当最終仕様案の日本語訳作業を実施したので、あわせて参照されたい。

## 7. 用語集

- **OpenID Connect:** OAuth2.0 にアイデンティティレイヤを追加した、アイデンティティを安全に流通させるための認証連携の仕組みを定義した仕様
- **OIDC:** OpenID Connect の略称
- **IDA:** OpenID Connect for Identity Assurance 1.0, OpenID Connect for Identity Assurance Claims Registration 1.0, OpenID Identity Assurance Schema 1.0 を総称した略称
- **本人確認:** 申請者の実在性や当人性を確認する行為のこと。本レポートでは、本人確認を「身元確認」、「当人認証」及び「フェデレーション」の3つの要素によって定義する。なお、本人確認という言葉は多義的に用いられる言葉であるため、本レポートでの定義と対象手続の根拠法等での定義が異なる場合があることに留意すること。個人が本人であることを確認する手続き。
- **身元確認:** 申請者を一意に識別するとともに、実在性を確認すること。具体的には、申請者の属性情報を収集することで申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認する。
- **当人認証:** 申請者の当人性を確認すること。具体的には、対象手続を利用しようとする者が、身元確認時に登録された者と同じの人物であることを、申請者と紐づけて登録した認証器を用いて確認する。
- **フェデレーション:** 身元確認や当人認証を、他者に依拠して実現すること。
- **OP (OpenID Provider):** OpenID Connect を利用したフェデレーションによる連携を行うモデル(連携モデル)において、申請者に対する身元確認や当人認証を行い、その結果に関する情報をRPへと連携する主体のこと。
- **RP (Relying Party):** 連携モデルにおいて、身元確認や当人認証をIDプロバイダに依拠する主体のこと。
- **属性情報:** ある主体が備えている性質や特徴に関する情報。例えば、氏名、生年月日、住所など。
- **本人確認書類:** 身元確認において、申請者が主張する属性情報の証拠として用いる書類。マイナンバーカードや運転免許証などの物理的な本人確認書類のほか、スマートフォンに格納されたデジタル証明書なども本人確認書類になり得る。
- **基本4情報:** 氏名、生年月日、住所、性別の4つの基本的な個人情報。



## 8. 執筆者一覧

執筆メンバ(所属50音順)

所属	氏名
株式会社NTTドコモ	栗山 盛行
株式会社オプティム	菊池 佑
KDDI株式会社	小畑 雅人
KDDI株式会社	小岩井 航介
ソフトバンク株式会社	作田 宗臣

執筆協力メンバ(所属50音順)

所属	氏名
株式会社メルカリ	狩野 達也
TOPPANエッジ株式会社	後藤 聡
他、KYC WG 次世代サブWGメンバー	

問い合わせ先

OpenIDファウンデーション・ジャパン事務局  
contact@openid.or.jp