OpenID Connect for Identity Assurance Basic Profile with Scopes and UserInfo

OpenID ファウンデーション・ジャパン KYC WG

1. Introduction

本仕様は、OpenID Connect (OIDC) [OIDC] の仕組みを使い、身元確認済情報を連携するための OpenID Connect for Identity Assurance 1.0 (IDA)仕様群 のプロファイル並びに拡張仕様である。

IDA はできるだけ自由度を高めた形での仕様として標準化されており、様々な解釈ができることから、OP によってバラバラな実装になる可能性がある。

よって、本仕様では、実装が容易でかつ共通の認識をもつことができるように、日本国内での IDA 仕様の普及に向け、主なユースケースを分析し、最小公倍数的に利用できるミニマムなプロファイルとして作成した。

本仕様はある程度の身元確認レベルを担保しつつもなるべく簡単に身元確認済情報を取得したいというニーズを満たす、簡単な手法で身元確認済情報を提供する手段として作成したものである。

IDA は、属性値の要求に対して claims パラメータまたは scope パラメータのいずれかを利用できる仕様となっている。

IDA を用いた身元確認済属性の流通を促進するには、既存の OIDC を実装しているサービス提供事業者、身元確認情報の提供事業者の双方にとって可能な限り容易に実装できることが望ましい。そのため、既存の OIDC を実装している事業者が手軽に利用できる状態を実現することを目的とし、IDA 仕様のうち、身元確認済属性の要求には scope パラメータを用い、返却には UserInfo Endpoint で提供する方法を採用した。本仕様では、要求する身元確認済情報に合わせたプリセットとなる scope と、scope ごとに返却する身元確認済情報の一覧を定義し、それ以外は既存の OIDC から大きく変更しない形としている。

本仕様の scope のプリセット定義においては、シェアリングサービスなどのオンライン予約や、酒類購入時の年齢確認等において、ユーザ体験を損なうことなく身元確認を行えるようにすることなどを想定ユースケースとしている。

さらに、認証は成功したが、身元確認済みの属性情報を返却できないような場合に、その旨を連携するための方法として、`__response_metadata` を新たに定義した。この部分においては、既存の仕様からの拡張（Extension）となっている。

1.1. Terminology

本ドキュメントでは、下記の用語を用いる。

- **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
- **OIDC4IDA, IDA:** OpenID Connect for Identity Assurance 仕様群 の略称。以下の3つの仕様を総称する場合に利用する。
    - OpenID Connect for Identity Assurance 1.0 [IDA-Core]
    - OpenID Connect for Identity Assurance Claims Registration 1.0 [IDA-Claims]
    - OpenID Identity Assurance Schema Definition 1.0 [IDA-Schema]
- 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、本仕様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一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。
- クレーム: OpenID Connectにおけるclaim、個人の属性情報
- 検証済みクレーム: IDAにおける verified claim、特定のトラストフレームワークに則って正しさが検証されたクレーム

- トラストフレームワーク: 事業者間で本人確認済情報をやり取りする際に、受け取った情報を信頼する際の根拠となる取り決めや法的な枠組みのこと。特定の法律（犯罪収益移転防止法や携帯電話不正利用防止法等）や、事業者間の契約、NIST をはじめとするガイドラインなど。
- 犯収法, 犯罪収益移転防止法:
    - 犯罪による収益の移転防止に関する法律 [JP-AML]
    - 犯罪による収益の移転防止に関する法律施行令 [JP-AML-CAB]
    - 犯罪による収益の移転防止に関する法律施行規則 [JP-AML-RULE]
    - 金融機関等の取引時確認、取引記録等の保存、疑わしい取引の届出の義務など、資金洗浄及びテロ資金供与対策のための規制を定める法律。犯罪収益移転防止法とも呼称する。
- 携帯電話不正利用防止法:
    - 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律 [JP-MPIUPA]
    - 携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律施行規則 [JP-MPIUPA-RULE]
    - 振り込め詐欺など携帯電話を不正に利用した犯罪を防ぐための法律。
- **FAPI**: OAuth2.0 で提供される高いセキュリティが求められる API 向けのセキュリティプロファイルである、FAPI 2.0 Security Profile の略称 [FAPI2]
- **IAL**: Identity Assurance Level。身元確認保証レベル。NIST SP800-63A [NIST-SP-800-63a] で定義された身元確認レベル表現方法
- **AAL**: Authentication Assurance Level。当人認証保証レベル。NIST SP800-63B [NIST-SP-800-63b] で定義された当人認証レベル表現方法
- **OAuth 2.0:** サードパーティーアプリケーションによる HTTP サービスへの限定的なアクセスを可能にする認可フレームワーク
- **ID Token**: エンドユーザの認証に関するクレームを含んだセキュリティトークン。認証の結果、特定されたエンドユーザの識別子などの情報が含まれる。エンドユーザの属性情報が含まれることもある
- **Access Token:** OAuth 2.0（および OpenID Connect）において、保護されたリソースへアクセスするために使用されるクレデンシャル

2. Scope

本仕様は、OP と RP 間で検証済みクレームの流通を活性化すべく、日本国内向けの主要なユースケースを元に OpenID Connect for Identity Assurance の利用方法を定義したプロファイル及び拡張仕様（エクステンション）である。そのため、本仕様の範囲を超えた複雑な属性の要求や応答が必要な場合は、本仕様と合わせて OpenID Connect for Identity Assurance の仕様を利用して実装する（例: claims パラメータを利用した属性要求、など）こと。

法的側面 (責任を含む)、具体的な信頼の枠組み、または商業協定など、アイデンティティ保証のための完全なソリューションを展開するために必要な追加の側面は、本仕様の範囲外である。

3. Requirements

IDA の要件に加え、本仕様では次の要件を追加する。

- 属性情報のセットを新たに scope 名として定義する。
- RP が属性情報を要求する際は、scope を利用することとし、claims パラメータは利用しない。
- 属性情報の返却に、UserInfo Endpoint を利用することとし、ID Token を利用しない。
- UserInfo Endpoint におけるレスポンスは json 形式での返却をサポートすること。
- __response_metadataパラメータを利用してエラーを返却すること。

RP は、本仕様で定義された必要最低限のデータセットを選択することで、OP が採用する身元確認プロセスに関するデータセットを取得できる。

本仕様の基本的な考え方は、OP が事前に設定した身元確認情報のプリセットを RP が要求することで、あらかじめ設定された情報を取得するというものである。これにより RP はどのような身元確認情報を要求するかを OP が準備したプリセットから選択するだけでよく、自らどのような情報を取得すべきか細かく設定する必要がない。また、仕様に従ったプリセットを要求することで、データミニマイゼーションの観点から必要以上の情報を取得することも避けられる。OP は RP からの要求の内訳を都度個別に処理する必要がなくなり、必要最小限のデータセットのみを提供できる。

例えば、RP がとある規則に従って身元確認をしなければならない場合、IDA で身元確認情報を要求するときには、規則に則っていることを確認するための要求を細かく RP 側で指定する必要がある。本仕様の場合、予め規則に則ったプリセットを OP が用意していれば、RP はそのプリセットを要求するだけで規則に則った身元確認情報を取得できる。

技術的な観点としては、IDA の仕様に新たな scope の値を定義する。この scope の値は、身元確認情報のプリセットを定義する。

本仕様では、ID Token を利用して属性情報を取得するのではなく、UserInfo Endpoint を利用することと定義する。ID Token を用いて身元確認済み属性情報を提供する場合、ID Token に認証結果と身元確認済みの属性情報の両方が含まれることから、身元確認済みの属性情報が返却できないケースにおいて、RP が適切なエラーハンドリングを行いづらい可能性がある。また OP によっては、ログイン認証と身元確認済みの属性情報の提供機能を独立提供していたり、それ以外の複数の機能を提供している場合において、それぞれの機能で異なるビジネスモデルを採用している可能性があるため、API として独立して提供した方がシンプルなアーキテクチャになると考えられる。そのため本仕様では、認証結果と属性情報の提供を切り分けられるように UserInfo Endpoint を利用することとした。さらに、身元確認が行われていない場合は、エラーを返却する仕様を追加で定義した。

4. Defined Scope Values

本仕様では、OpenID Identity Assurance Schema Definition 1.0 [IDA-Schema] にて規定された Verified Claims 要素の下記の 2 つの Verification 要素、Claims 要素の各項目をプリセットする新たな scope を定義する。

- Verification 要素は、本人確認書類の確認プロセスに関するデータの JSON オブジェクトで、本人確認書類の発行者や確認プロセスに関する情報を含む。
- Claims 要素は、RP が身元確認をするための属性情報で、氏名・住所・生年月日等の情報を含む。

本仕様では、身元確認のユースケースによって、Verification 要素や Claims 要素を scope によってプリセットしている。

本仕様の基本となる scope は `jp_oidf_ida` で、厳密に身元確認は行っていないが、自己申告ではないレベルの属性情報がほしいなどのカジュアルな用途での利用を想定している。これは経済産業省が 2020 年に公開した「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」にある「中間強度の身元確認手法」にあるように、犯収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、犯収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た結果を取得するユースケースを想定しているためである。
どのような証跡や手続きで身元確認を行ったかの情報を取得したい場合、`jp_oidf_ida_with_evidence` の scope を利用する。`jp_oidf_ida` の scope に加えて、本人確認書類の種類や身元確認プロセスに関する情報を追加で取得することが出来る。

属性情報は不要だが、特定の年齢以上であること（または それ未満であること）を確認するための用途として `jp_oidf_ida_age_over_XX` を利用する。(XXには、日本で一般的に利用される、16, 18, 20 が利用できる。)この scope は、個人情報は必要ないため取得したくないが、契約行為や成人限定コンテンツの提供の判定が必要といったユースケースを想定している。

加えて、正確な電話番号を取得するため、`jp_oidf_ida_msisdn`の scope を利用することができる。このscopeは、通信キャリア等の、エンドユーザの正確な電話番号を保持しているOPが電話番号のみを返却する際に利用する。

以上6つのscopeは、`jp_oidf_ida_msisdn`を除いて、複数のscopeを同時に利用することは想定していない。`jp_oidf_ida_msisdn`以外のscopeが同時に利用された場合のOPの挙動は未定義とする。

項番	**Scope**値	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	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	電話番号	属性情報の発行元	通信キャリア等

5. Verified Claims

本仕様では、IDA にて規定された Verified Claims 要素について、特定の Verified Claims を返却する組み合わせのプロファイルを定義する。

5.1. General Requirements

5.1.1. Requesting Verified Claims

OpenID Connect for Identity Assurance 1.0 [IDA-Core] では、Verified Claims 要素の要求方法として Claims Parameter 及び scope の 2 種類の手法が規定されている。本仕様では、scope を用いた手法を利用し、Claims Parameter は利用しない。

5.1.2. Response Verified Claims

OpenID Connect for Identity Assurance 1.0 [IDA-Core] では、Verified Claims の返却方法として、ID Token に Claim を追加する手法、もしくは UserInfo Endpoint を利用した方法の 2 種類が規定されている。これは OpenID Connect Core [OIDC] に準拠した形となる。本仕様では、UserInfo Endpoint を用いた手法を利用し、ID Token に Verified Claims を含めないものとする。

返却する Verified Claims は、scope によって規定する。

5.2. "jp_oidf_ida" Scope Usage

この章では、`jp_oidf_ida` の scope を利用した Verified Claims の要求及び応答方法を規定する。

5.2.1. Request

RP は、`jp_oidf_ida` の Verified Claims を要求する際、OpenID Connect Core [OIDC] の Authorization Request における scope パラメータに、本仕様で定める scope を指定すること。`jp_oidf_ida_msisdn`を除いて、本仕様に定める scope を複数同時に指定してはならない。その他の仕様や独自に定義される scope との併用は可能である。

5.2.1.1. Requesting Scope

RP は、`jp_oidf_ida` の属性を要求する場合、以下の scope を利用すること。

- `jp_oidf_ida`

5.2.1.2. Authorization Request Example

以下に Authorization Request の例を示す。openid, email スコープに加えて、`jp_oidf_ida` スコープを認可要求している。

```
GET /authorize?
  response_type=code
  &scope=openid%20email%20jp_oidf_ida
  &client_id=s6BhdRkqt3
  &state=af0ifjsldkj
  &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb HTTP/1.1
 Host: server.example.com
```

5.2.2. Successful Response

Verified Claims は、OpenID Connect Core [OIDC] の UserInfo Endpoint を介して返却する。OP は下記の仕様に従い、UserInfo Response を返却すること。

5.2.2.1. Response Verified Claims

OP は `jp_oidf_ida` の scope が要求された際、以下の Verified Claims を返却すること。
各 Claim の詳細は、OpenID Identity Assurance Schema Definition 1.0 [IDA-Schema] の仕様に準ずる。

5.2.2.1.1. verification Element

- trust_framework: REQUIRED. 前提となるトラストフレームワークを示す文字列。本仕様内では、例示のために、`jp_oidf_ida` を利用する。どのようなトラストフレームワークを前提とするかは本仕様で定める範囲外となるため、指定する値は、本仕様を利用する関係者間にて事前に取り決めたルール（トラストフレームワーク）にて規定された値を利用すること。

5.2.2.1.2. claims Element

- name: REQUIRED. エンドユーザの氏名。名前の表現は多岐にわたることから、本仕様上では姓、名、ミドルネーム、旧姓等の記載内容や記載順序に関しては規定しない。同様に区切り文字も規定されないため、RP はこの文字列を機械的に区切ることを考慮しないこと。
- birthdate: REQUIRED. エンドユーザーの生年月日。ISO8601:2004 の YYYY-MM-DD 形式の文字列で返却すること。
- address/formatted: REQUIRED. エンドユーザの住所。住所の表現は多岐にわたり、画一的な表現方法がないことから、本仕様上では住所の詳細な記載内容に関しては規定しない。このクレームには郵便番号が含まれないことに注意。区切り文字も規定されないため、RP はこの文字列を機械的に区切ることを考慮しないこと。

5.2.2.2. UserInfo Response

OP は要求に合わせて UserInfo Response を返却する。
返却できない Claim が存在する場合、5.2.3. Error Response を参照してレスポンスを構築すること。

5.2.2.2.1. UserInfo Response Example

下記に UserInfo Response の例を示す。sub, email, email_verified に加えて、verified_claims のキーが追加される。

```
{
  "sub": "248289761001",
  "email": "taro@example.com",
  "email_verified": true,
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida"
    },
    "claims": {
      "name": "山田 太郎",
      "birthdate": "1956-01-28",
      "address": {
        "formatted": "東京都千代田区千代田1-1"
      }
    }
  }
}
```

5.2.3. Error Response

5.2.3.1. Authorization Response Error

RP は、ユーザーが Verified Claims の scope への同意を拒否する可能性を考慮しなければならない。要求した scope の全てに対してユーザーが同意しない場合、Authorization Error

Response で access_denied のエラーコードが返却される (RFC6749#section-4.1.2.1 参照のこと)。要求した scope の一部をユーザーが同意しない場合、Token Response にて同意された scope 一覧が必ず返却される。(RFC6749#section-3.3 参照のこと) そのため、RP は Token Response を検証し、要求した scope が含まれていることを必ず確認すること。

本仕様では、`jp_oidf_ida_msisdn`を除いて、本仕様で定める複数の scope を同時に利用することは許容しない。そのため OP は、Authorization Request にて本仕様に定める複数の scope を同時に認可要求された場合、Authorization Response にて invalid_scope のエラーレスポンスを返却してもよい (RFC6749#section-4.1.2.1 参照のこと)。

5.2.3.2. UserInfo Endpoint Response Error

OP は、Verified Claims を返却できない場合には、以下のように verified_claims 配下にエラー情報を含めたレスポンスを返却すること。Verified Claims を返却できない以外の理由でエラーが起こった場合、UserInfo Endpoint は OpenID Connect Core [OIDC]の Section 5 に示す Error Response を返却すること。

エラーレスポンスには、以下の要素を含まなければならない (MUST) 。

- error
  - REQUIRED. エラーコード。エラーコードの定義は下記参照。
- error_description
  - OPTIONAL. 人間が読める ASCII エンコードされたエラーの説明文.
- error_uri
  - OPTIONAL. エラーについての追加情報を含む Web ページの URI.

エラーコードは下記のいずれかを利用すること。

- verified_claims_unavailable
  - 要求されたユーザーの身元確認が未実施の場合
- verified_claims_insufficient
  - OP の身元確認では取得・検証できていない Claim が存在する場合
  - 例えば、身元確認に利用した本人確認書類に記載がなかった属性を要求されている場合など
- verified_claims_other_error
  - その他の理由で返却できない場合

5.2.3.3. UserInfo Error Response Example

以下に、OP が Verified Claims を返却できない場合のレスポンス例を示す。trust_frameworkのみの最低限の verified_claims オブジェクトに、__response_metadata キーを追加し、エラー情報を記載すること。

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

```
          "trust_framework": "jp_oidf_ida"
      },
      "claims": {},
      "__response_metadata": {
         "error": "verified_claims_unavailable",
         "error_description": "<optional human-readable string>",
         "error_uri": "<optional uri with error description>"
    }
  }
}
```

5.3. "jp_oidf_ida_with_evidence" Scope Usage

この章では`jp_oidf_ida_with_evidence` の scope を利用した Verified Claims の要求及び応答方法を規定する。

5.3.1. Request

RP は、`jp_oidf_ida_with_evidence` の Verified Claims を要求する際、OpenID Connect Core [OIDC] の Authorization Request における scope パラメータに、本仕様で定める scope を指定すること。`jp_oidf_ida_msisdn`を除いて、本仕様に定める scope を複数同時に指定してはならない。その他の仕様や独自に定義される scope との併用は可能である。

5.3.1.1. Requesting Scope

RP は、`jp_oidf_ida_with_evidence` の属性を要求する場合、以下の scope を利用すること。

- `jp_oidf_ida_with_evidence`

5.3.1.2. Authorization Request Example

以下に Authorization Request の例を示す。openid, email スコープに加えて、`jp_oidf_ida_with_evidence` スコープを認可要求している。

```
GET /authorize?
  response_type=code
  &scope=openid%20email%20jp_oidf_ida_with_evidence
  &client_id=s6BhdRkqt3
  &state=af0ifjsldkj
  &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb HTTP/1.1
 Host: server.example.com
```

5.3.2. Successful Response

Verified Claims は、OpenID Connect Core [OIDC] の UserInfo Endpoint を介して返却する。OP は下記の仕様に従い、UserInfo Response を返却すること。

5.3.2.1. Response Verified Claims

OP は `jp_oidf_ida_with_evidence` の scope が要求された際、`jp_oidf_ida` の属性に加えて以下の Verified Claims を返却すること。各 Claim の詳細は、OpenID Identity Assurance Schema Definition 1.0 [IDA-Schema] の仕様に準ずる。

5.3.2.1.1. verification Element

- time: REQUIRED. 身元確認プロセスが行われた日時を表す文字列。ISO8601:2004 [ISO8601-2004] YYYY-MM-DDThh:mm[:ss]TZD 形式 のタイムスタンプ値を返すこと。

- evidence: REQUIRED. OP がエンドユーザーを身元確認するために使用した証跡に関する情報を含む JSON 配列。evidence 要素に含むプロパティは、evidence Element 参照のこと。

5.3.2.1.2. evidence Element

- type: 身元確認時に利用した本人確認書類の種類を表す値。以下の文字列のいずれかを返却すること。
    - document: 運転免許証やパスポートなど、物理的あるいは電子的な書類を用いて身元確認を行った場合
    - electric_record: OP 自身が情報源であるデータや、外部事業者の本人確認 API など OP がユーザー以外のソースから身元確認情報を取得した場合
    - electric_signature: 公的個人認証のように、電子証明書に基づいて身元確認を行った場合
- check_details: evidence に関連して行われたチェックを表す JSON 配列。type が document の場合必須。check_details 要素に含むプロパティは、check_details Element 参照のこと。

5.3.2.1.3. check_details Element

- check_method: 実行されたチェックを表す文字列。これには、ドキュメントの信頼性のチェックや、ID document に対するユーザーの生体認証の検証などのプロセスが含まれる。返却可能な値は Check Methods 参照。
- time: このドキュメントが検証された日時を表す文字列。ISO8601:2004 [ISO8601-2004] YYYY-MM-DDThh:mm[:ss]TZD 形式 のタイムスタンプ値を返すこと。
- document_details: 身元確認の実行に使用されたドキュメント（本人確認書類）を表す JSON オブジェクト。document_details 要素に含むプロパティは、document_details Element 参照のこと。

5.3.2.1.4. document_details Element

- type: 本人確認書類の種別を示す文字列。身元確認時に利用した本人確認書類の種別を表す文字列を返却する。例えば以下の通り。
    - 運転免許証: jp_drivers_license
    - 在留カード: jp_residency_card_for_foreigner
    - マイナンバーカード: jp_individual_number_card
    - 特別永住者証明書: jp_permanent_residency_card_for_foreigner
    - 健康保険証: jp_health_insurance_card
    - 住民基本台帳カード: jp_residency_card
    - パスポート: passport

5.3.2.2. UserInfo Response

OP は要求に合わせて UserInfo Response を返却する。返却できない Claim が存在する場合、5.3.3. Error Response を参照してレスポンスを構築すること。

5.3.2.2.1. UserInfo Response Example

下記に UserInfo Response の例を示す。sub, email, email_verified に加えて、verified_claims のキーが追加される。

```
{
  "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"
              }
            }
          ]
        }
      ]
    },
    "claims": {
      "name": "山田 太郎",
      "birthdate": "1956-01-28",
      "address": {
        "formatted#ja-Hani-JP": "東京都千代田区千代田1-1"
      }
    }
  }
}
```


5.3.3. Error Response

5.3.3.1. Authorization Response Error

RP は、ユーザーが Verified Claims の scope への同意を拒否する可能性を考慮しなければならない。要求した scope の全てに対してユーザーが同意しない場合、Authorization Error Response で access_denied のエラーコードが返却される ([RFC6749]#section-4.1.2.1 参照のこと)。要求した scope の一部をユーザーが同意しない場合、Token Response にて同意された scope 一覧が必ず返却される。([RFC6749]#section-3.3 参照のこと) そのため、RP は Token Response を検証し、要求した scope が含まれていることを必ず確認すること。[1]

本仕様では、`jp_oidf_ida_msisdn`を除いて、本仕様で定める複数の scope を同時に利用することは許容しない。そのため OP は、Authorization Request にて本仕様に定める複数の

[1] ミニマムディスクロージャーの観点から、RP は、真に必要な個人情報だけを要求すべきである。よって、OP は、個人情報の個別の項目毎に開示の許諾を得る必要は無い。すなわち、ユーザが Verified Claims の開示に許諾をしたかどうかは、当該 scope の許諾が得られたかどうかで判断できる。

scope を同時に認可要求された場合、Authorization Response にて invalid_scope のエラーレスポンスを返却してもよい ([RFC6749]#section-4.1.2.1 参照のこと)。

5.3.3.2. UserInfo Endpoint Response Error

OP は、Verified Claims を返却できない場合には、以下のように verified_claims 配下にエラー情報を含めたレスポンスを返却すること。Verified Claims を返却できない以外の理由でエラーが起こった場合、UserInfo Endpoint は OpenID Connect Core [OIDC]の Section 5 に示す Error Response を返却すること。

エラーレスポンスには、以下の要素を含まなければならない (MUST) 。

- error
  - REQUIRED. エラーコード。エラーコードの定義は下記参照。
- error_description
  - OPTIONAL. 人間が読める ASCII エンコードされたエラーの説明文.
- error_uri
  - OPTIONAL. エラーについての追加情報を含む WebページのURI.

エラーコードは下記のいずれかを利用すること。

- verified_claims_unavailable
  - 要求されたユーザーの身元確認が未実施の場合
- verified_claims_insufficient
  - OP の身元確認では取得・検証できていない Claim が存在する場合
  - 例えば、身元確認に利用した本人確認書類の記録が存在しない場合など
- verified_claims_other_error
  - その他の理由で返却できない場合

5.3.3.3. UserInfo Error Response Example

以下に、OP が Verified Claims を返却できない場合のレスポンス例を示す。trust_frameworkのみの最低限の verified_claims オプジェクトに、__response_metadata キーを追加し、エラー情報を記載すること。

```
{
  "sub": "248289761001",
  "email": "taro@example.com",
  "email_verified": true,
  "verified_claims": {
    "verification": {
          "trust_framework": "jp_oidf_ida"
      },
      "claims": {},
      "__response_metadata": {
          "error": "verified_claims_unavailable",
          "error_description": "<optional human-readable string>",
          "error_uri": "<optional uri with error description>"
    }
  }
}
```

5.4. "jp_oidf_ida_age_over_XX" Scope Usage

この章では、`jp_oidf_ida_age_over_16`, `jp_oidf_ida_age_over_18`, `jp_oidf_ida_age_over_20` の scope を利用した Verified Claims の要求及び応答方法を規定する。

5.4.1. Request

RP は、`jp_oidf_ida_age_over_XX` の Verified Claims を要求する際、OpenID Connect Core [OIDC] の Authorization Request における scope パラメータに、本仕様で定める scope を指定すること。`jp_oidf_ida_msisdn`を除いて、本仕様に定める scope を複数同時に指定してはならない。その他の仕様や独自に定義される scope との併用は可能である。

5.4.1.1. Requesting Scope

RP は、`jp_oidf_ida_age_over_XX` の属性を要求する場合、以下の scope のいずれか1つ、かつ1つのみを利用すること。

- `jp_oidf_ida_age_over_16`
- `jp_oidf_ida_age_over_18`
- `jp_oidf_ida_age_over_20`

5.5.1.1.1. Authorization Request Example

以下に Authorization Request の例を示す。openidスコープに加えて、`jp_oidf_ida_age_over_18` スコープを認可要求している。

```
GET /authorize?
  response_type=code
  &scope=openid%20jp_oidf_ida_age_over_18
  &client_id=s6BhdRkqt3
  &state=af0ifjsldkj
  &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb HTTP/1.1
 Host: server.example.com
```

5.4.2. Successful Response

Verified Claims は、OpenID Connect Core [OIDC] の UserInfo Endpoint を介して返却する。OP は下記の仕様に従い、UserInfo Response を返却すること。

5.4.2.1. Response Verified Claims

OP は `jp_oidf_ida_age_over_XX` の scope が要求された際、以下の Verified Claims を返却すること。各 Claim の詳細は、OpenID Identity Assurance Schema Definition 1.0 [IDA-Schema] に準ずる。

5.4.2.1.1. verification Element

- trust_framework: REQUIRED. 前提となるトラストフレームワークを示す文字列。本仕様内では、例示のために、`jp_oidf_ida` を利用する。どのようなトラストフレームワークを前提とするかは本仕様で定める範囲外となるため、指定する値は、本仕様を利用する関係者間にて事前に取り決めたルール（トラストフレームワーク）にて規定された値を利用すること。

5.4.2.1.2. claims Element

以下のいずれか1つ、かつ1つのみを返却すること。RPの要求したscopeに一致する年齢を返却すること（REQUIRED)

- ::age_16_or_over: 16 歳以上かどうかを表す boolean 値。
- ::age_18_or_over: 18 歳以上かどうかを表す boolean 値。
- ::age_20_or_over: 20 歳以上かどうかを表す boolean 値。

5.4.2.2. UserInfo Response

OP は要求に合わせて UserInfo Response を返却する。返却できない Claim が存在する場合、5.4.3. Error Response を参照してレスポンスを構築すること。

UserInfo Response の形式に関する仕様は、OpenID Connect Core [OIDC] の Section 5.3.2 を参照すること。

5.4.2.2.1. UserInfo Response Example

下記に UserInfo Response の例を示す。subに加えて、verified_claims のキーが追加される。

```
{
  "sub": "248289761001",
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida",
    },
    "claims": {
      "::age_18_or_over": true
    }
  }
}
```

5.4.3. Error Response

5.4.3.1. Authorization Response Error

RP は、ユーザーが Verified Claims の scope への同意を拒否する可能性を考慮しなければならない。要求した scope の全てに対してユーザーが同意しない場合、Authorization Error Response で access_denied のエラーコードが返却される ([RFC6749]#section-4.1.2.1 参照のこと）。要求した scope の一部をユーザーが同意しない場合、Token Response にて同意された scope 一覧が必ず返却される。([RFC6749]#section-3.3 参照のこと) そのため、RP は Token Response を検証し、要求した scope が含まれていることを必ず確認すること。

本仕様では、`jp_oidf_ida_msisdn`を除いて、本仕様で定める複数の scope を同時に利用することは許容しない。そのため OP は、Authorization Request にて本仕様に定める複数の scope を同時に認可要求された場合、Authorization Response にて invalid_scope のエラーレスポンスを返却してもよい ([RFC6749]#section-4.1.2.1 参照のこと)。

5.4.3.2. UserInfo Endpoint Response Error

OP は、Verified Claims を返却できない場合には、以下のように verified_claims 配下にエラー情報を含めたレスポンスを返却すること。Verified Claims を返却できない以外の理由でエラーが起こった場合、UserInfo Endpoint は OpenID Connect Core [OIDC]の Section 5 に示す Error Response を返却すること。

エラーレスポンスには、以下の要素を含まなければならない (MUST) 。

- error
  - REQUIRED. エラーコード。エラーコードの定義は下記参照。
- error_description
  - OPTIONAL. 人間が読める ASCII エンコードされたエラーの説明文.
- error_uri
  - OPTIONAL. エラーについての追加情報を含む Web ページの URI.

エラーコードは下記のいずれかを利用すること。

- verified_claims_unavailable
  - 要求されたユーザーが身元確認が未実施の場合
- verified_claims_insufficient
  - OP の身元確認では取得・検証できていない Claim が存在する場合
  - 例えば、本人確認書類に生年月日が存在しない場合など
- verified_claims_other_error
  - その他の理由で返却できない場合

5.4.3.3. UserInfo Error Response Example

以下に、OP が Verified Claims を返却できない場合のレスポンス例を示す。trust_frameworkのみの最低限の verified_claims オブジェクトに、__response_metadata キーを追加し、エラー情報を記載すること。

```
{
  "sub": "248289761001",
  "verified_claims": {
     "verification": {
          "trust_framework": "jp_oidf_ida"
     },
     "claims": {},
     "__response_metadata": {
        "error": "verified_claims_unavailable",
        "error_description": "<optional human-readable string>",
        "error_uri": "<optional uri with error description>"
      }
  }
```

```
}
```

5.5. "jp_oidf_ida_msisdn" Scope Usage

この章では、`jp_oidf_ida_msisdn` の scope を利用した Verified Claims の要求及び応答方法を規定する。

5.5.1. Request

RP は、`jp_oidf_ida_msisdn` の Verified Claims を要求する際、OpenID Connect Core [OIDC] の Authorization Request における scope パラメータに、本仕様で定める scope を指定すること。1つに限り、本仕様に定める 他のscope を複数同時に指定することができる。その他の仕様や独自に定義される scope との併用は可能である。複数指定した場合のレスポンス例は Appendix 参照のこと。

5.5.1.1. Requesting Scope

RP は、`jp_oidf_ida_msisdn` の属性を要求する場合、以下の scope を利用すること。

- `jp_oidf_ida_msisdn`

5.5.1.2. Authorization Request Example

以下に Authorization Request の例を示す。openid, email スコープに加えて、`jp_oidf_ida_msisdn` スコープを認可要求している。

```
GET /authorize?
  response_type=code
  &scope=openid%20email%20jp_oidf_ida_msisdn
  &client_id=s6BhdRkqt3
  &state=af0ifjsldkj
  &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb HTTP/1.1
 Host: server.example.com
```

5.5.2. Successful Response

Verified Claims は、OpenID Connect Core [OIDC] の UserInfo Endpoint を介して返却する。OP は下記の仕様に従い、UserInfo Response を返却すること。

5.5.2.1. Response Verified Claims

OP は `jp_oidf_ida_msisdn` の scope が要求された際、以下の Verified Claims を返却すること。
各 Claim の詳細は、OpenID Identity Assurance Schema Definition 1.0 [IDA-Schema]の仕様に準ずる。

5.5.2.1.1. verification Element

- trust_framework: REQUIRED. 前提となるトラストフレームワークを示す文字列。本仕様内では、例示のために、`jp_oidf_ida` を利用する。どのようなトラストフレームワークを前提とするかは本仕様で定める範囲外となるため、指定する値は、本仕様を利用する関係者間にて事前に取り決めたルール（トラストフレームワーク）にて規定された値を利用すること。
- time: REQUIRED. 身元確認プロセスが行われた日時を表す文字列。ISO8601:2004 [ISO8601-2004] YYYY-MM-DDThh:mm[:ss]TZD 形式 のタイムスタンプ値を返すこと。
- evidence: REQUIRED. OP がエンドユーザーの ID を個別の JSON オブジェクトとして検証するために使用した証跡に関する情報を含む JSON 配列。evidence 要素に含むプロパティは、evidence Element 参照のこと。

5.5.2.1.2. evidence Element

- type: 身元確認時に利用した本人確認書類の種類を表す値。以下の文字列を返却すること。
    - electric_record: OP 自身が情報源であるデータや、外部事業者の本人確認 API など OP がユーザー以外のソースから身元確認情報を取得した場合を表す。

5.5.2.1.3. claims Element

- msisdn: REQUIRED. エンドユーザの電話番号。OpenID Connect for Identity Assurance Claims Registration 1.0 [IDA-Claims] に従って表現されたエンドユーザーの携帯電話番号。

5.5.2.2. UserInfo Response

OP は要求に合わせて UserInfo Response を返却する。
返却できない Claim が存在する場合、5.5.3. Error Response を参照してレスポンスを構築すること。

5.5.2.2.1. UserInfo Response Example

下記に UserInfo Response の例を示す。sub, email, email_verified に加えて、verified_claims のキーが追加される。

```
{
  "sub": "248289761001",
  "email": "taro@example.com",
  "email_verified": true,
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida"
      "evidence":{
          "type": "electric_record"
        }
    },
    "claims": {
```

```
    "msisdn": "819012345678"
   }
  }
}
```

5.5.3. Error Response

5.5.3.1. Authorization Response Error

RP は、ユーザーが Verified Claims の scope への同意を拒否する可能性を考慮しなければならない。要求した scope の全てに対してユーザーが同意しない場合、Authorization Error Response で access_denied のエラーコードが返却される ([RFC6749]#section-4.1.2.1 参照のこと)。要求した scope の一部をユーザーが同意しない場合、Token Response にて同意された scope 一覧が必ず返却される。([RFC6749]#section-3.3 参照のこと) そのため、RP は Token Response を検証し、要求した scope が含まれていることを必ず確認すること。

本仕様では、1つに限り、`jp_oidf_ida_msisdn`に加えて本仕様で定める他の scope を同時に利用することを許容する。

5.5.3.2. UserInfo Endpoint Response Error

OP は、Verified Claims を返却できない場合には、以下のように verified_claims 配下にエラー情報を含めたレスポンスを返却すること。Verified Claims を返却できない以外の理由でエラーが起こった場合、UserInfo Endpoint は OpenID Connect Core [OIDC]の Section 5 に示す Error Response を返却すること。

当仕様で定義する scope を複数指定した場合には、どれか1つの scope に対応する claim を返却できない場合には、一律エラーとすること。

エラーレスポンスには、以下の要素を含まなければならない (MUST) 。

- error
    - REQUIRED. エラーコード。エラーコードの定義は下記参照。
- error_description
    - OPTIONAL. 人間が読める ASCII エンコードされたエラーの説明文.
- error_uri
    - OPTIONAL. エラーについての追加情報を含む Web ページの URI.

エラーコードは下記のいずれかを利用すること。

- verified_claims_unavailable
    - 要求されたユーザーの身元確認が未実施の場合
- verified_claims_insufficient
    - OP の身元確認では取得・検証できていない Claim が存在する場合
    - 例えば、要求されたユーザの正確な電話番号を保持していない場合など
- verified_claims_other_error
    - その他の理由で返却できない場合

5.5.3.3. UserInfo Error Response Example

以下に、OP が Verified Claims を返却できない場合のレスポンス例を示す。trust_frameworkのみの最低限の verified_claims オブジェクトに、__response_metadata キーを追加し、エラー情報を記載すること。

```
{
  "sub": "248289761001",
  "email": "taro@example.com",
  "email_verified": true,
  "verified_claims": {
     "verification": {
         "trust_framework": "jp_oidf_ida"
     },
     "claims": {},
     "__response_metadata": {
       "error": "verified_claims_insufficient",
       "error_description": "msisdn is not available",
       "error_uri": "<optional uri with error description>"
     }
   }
}
```

6. Privacy Consideration

本仕様では個人情報が授受されるため、個人情報保護の観点から OP はエンドユーザに対して RP へ身元確認済情報を提供する旨の同意を取得しなければならない。また、同意を取得する際には、利用目的を明示して同意を取得し、取得した目的と異なる用途で情報を利用してはならない。更に、情報漏洩を防ぐために、Security Considerations を参照し、適切なセキュリティレベルを設定しなければならない。

データミニマイゼーションの観点から、RP は、必要最低限の情報を scope で求めなければならない。同様に、OP は、本仕様の定義外の方法により別途要求された場合を除き、scope として求められた以上の情報を返却してはならない。

また、民間事業者におけるベストプラクティスについては、民間事業者向けデジタル本人確認ガイドライン[OIDFJ-eKYC-guideline] 第 6 章に詳しい。

7. Security Considerations

OP は、自身が取り扱う個人情報に合わせた適切なセキュリティレベルを設定し、それを満たす当人認証をユーザに求めなければならない。同様に、RP は、自身の求める個人情報の精度（本人詐称の可能性）に応じて、多要素認証など、適切な当人認証保証レベルを OP に求めなければならない。ここで RP から OP に適切な当人認証保証レベルを求める方法は、本仕様のスコープ外とする。

なお、NIST SP 800-63B-4 [NIST-SP-800-63b] Section 2によると、個人情報をオンラインで利用可能とする米国政府機関は、AAL2 以上の当人認証を求めなければならないとある。

scope をフロントチャネルで送信する (OAuth 2.0 Pushed Authorization Requests [RFC9126] や signed request を使わない) 場合、悪意者により変更される可能性がある。よって RP は、受領した Verified Claims の内容を確認して、自身が求めた scope に対応する情報であることを常に確認すること。

Token Endpoint 並びに UserInfo Endpoint は、例えば、下記のような方法を用いて、不正なアクセスから保護することを推奨する。

- （レベル高）専用線や VPN を利用して、client のみからアクセス可能とする。
- （レベル高）FAPI 2.0 Security Profile [FAPI2] に定義された holder bound acess token を実装すること
    - MTLS as described in [RFC8705]
    - DPoP as described in [RFC9449]
- （レベル中）JWT を使ったクライアント認証を実施する [RFC7523]
- （レベル低）client の接続元 IP アドレスを限定させる。
- （レベル低）access token の他に、client-secret や API キーを用いて client を認証する。

なお、[FAPI2] を適用することで、上記レベル高の要求を満たすことができるだけでなく、グローバルな相互運用性が向上すること、また、型式証明によりセキュリティが担保されていることから、可能な限り [FAPI2] を適用することが望ましい。

8. Normative References

[OIDC] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0 incorporating errata set 2", 8 November 2014, <https://openid.net/specs/openid-connect-core-1_0.html>.

[IDA-Core] Lodderstedt, T., Fett, D., Haine, M., Pulido, A., Lehmann, K., and K. Koiwai, "OpenID Connect for Identity Assurance 1.0", 1 October 2024, <https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html>.

[IDA-Claims] Lodderstedt, T., Fett, D., Haine, M., Pulido, A., Lehmann, K., and K. Koiwai, "OpenID Connect for Identity Assurance Claims Registration 1.0", 1 October 2024, <https://openid.net/specs/openid-connect-4-ida-claims-1_0.html>.

[IDA-Schema] Lodderstedt, T., Fett, D., Haine, M., Pulido, A., Lehmann, K., and K. Koiwai, "OpenID Identity Assurance Schema Definition 1.0", 1 October 2024, <https://openid.net/specs/openid-ida-verified-claims-1_0-final.html>.

[ISO8601-2004] ISO, "ISO 8601. Data elements and interchange formats - Information interchange - Representation of dates and times", <https://www.iso.org/iso/catalogue_detail?csnumber=40874>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

9. Informative References

[JP-AML] 日本国, "犯罪による収益の移転防止に関する法律" , 2025年6月1日施行, <https://laws.e-gov.go.jp/law/419AC0000000022/>

[JP-AML-CAB] 日本国, "犯罪による収益の移転防止に関する法律施行令" , 2025年5月15日施行, <https://laws.e-gov.go.jp/law/420CO0000000020/>

[JP-AML-RULE] 日本国, "犯罪による収益の移転防止に関する法律施行規則", 2025年6月24日施行 , <https://laws.e-gov.go.jp/law/420M60000F5A001/>

[JP-MPIUPA] 日本国, "携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律", 2025年6月1日施行, <https://laws.e-gov.go.jp/law/417AC1000000031>

[JP-MPIUPA-RULE]日本国, "携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律施行規則", 2025年6月24日施行, <https://laws.e-gov.go.jp/law/417M60000008167/>

[NIST-SP-800-63a] Temoshok, D., Abruzzi, C., Choong, Y., Fenton, J. L., Galluzzo, R., LaSalle, C., Lefkovitz, N., Regenscheid, A., and M. Vachino, "NIST SP 800-63A-4 Digital Identity Guidelines: Identity Proofing and Enrollment", July 2025, <https://doi.org/10.6028/NIST.SP.800-63A-4>

[NIST-SP-800-63b] Temoshok, D., Fenton, J. L., Choong, Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., and J.P. Richer, "NIST SP 800-63B-4 Digital Identity Guidelines: Authentication and Authenticator Management", July 2025, <https://doi.org/10.6028/NIST.SP.800-63b-4>

[RFC8705] Campbell, B., Bradley, J., Sakimura, N., and T. Lodderstedt, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens", RFC 8705, DOI 10.17487/RFC8705, February 2020, <https://www.rfc-editor.org/info/rfc8705>.

[RFC9449] Fett, D., Campbell, B., Bradley, J., Lodderstedt, T., Jones, M., and D. Waite, "OAuth 2.0 Demonstrating Proof of Possession (DPoP)", RFC 9449, DOI 10.17487/RFC9449, September 2023, <https://www.rfc-editor.org/info/rfc9449>.
[RFC7523] Jones, M., Campbell, B., and C. Mortimore, "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants," RFC 7523, DOI 10.17487/RFC7523, May 2015, <https://www.rfc-editor.org/info/rfc7523>.
[OIDFJ-eKYC-guideline] OpenIDファウンデーション・ジャパン, "民間事業者向けデジタル本人確認ガイドライン", 2023年3月，<https://www.openid.or.jp/news/kyc_guideline_v1.0.pdf>
[RFC9126] Lodderstedt, T., Campbell, B., Sakimura, N., Tonge, D., and F. Skokan, "OAuth 2.0 Pushed Authorization Requests", RFC 9126, DOI 10.17487/RFC9126, September 2021, <https://www.rfc-editor.org/info/rfc9126>.
[FAPI2] Fett, D., Tonge, D., and J. Heenan, "FAPI 2.0 Security Profile", 22 February 2025, <https://openid.net/specs/fapi-security-profile-2_0-final.html>

10. Appendix

10.1. 複数のscopeを指定された場合のレスポンス例

本仕様では、`jp_oidf_ida_msisdn`と、それ以外のscope の2つを組み合わせて同時に要求することができる。
`jp_oidf_ida_with_evidence`と`jp_oidf_ida_msisdn`の2つのscopeを要求された際のレスポンスを以下に例示する。

```
{
  "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"
    }
  }
 ]
}
```