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

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

次世代KYCレポート（Phase 3）

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, オープンAPI, FAPI, 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, 依拠による本人確認, トラストサービス, Trusted Web,

1. ご挨拶 2
2. はじめに 4
3. 次世代 KYC 検討の経緯 6
4. KYC の要件とツールとルール 8
5. KYC 実施時のルールの整理 9
5.1. RP、KP、CP 共通に求められること 9
5.2. RP 個別に求められること 10
5.3. KP 個別に求められること 11
5.4. CP 個別に求められること 12
6. KYC 実施時のツールの整理 14
6.1. 技術的な要件 14
6.2. システム構成 14
7. OpenID Foundation で策定している関連標準仕様の検討状況 17
7.1. OpenID Connect for Identity Assurance 17
7.2. Financial-grade API 19
7.3. OAuth2.0 Pushed Authorization Requests (PAR) 21
8. OpenID Connect for Identity Assurance (IDA 仕様) における国内向け仕様の検討 22
8.1. IDP における IDA 仕様の実装の注意点 23
8.2. IDA 仕様からの国内向けのミニマム仕様の検討 26
8.3. 国内向けミニマム仕様の Scope 定義 29
8.4. Scope 毎の返却 Claim の定義 34
9. まとめ 39
10. Appendix 41
10.1. 各レベルごとの verified_claims サンプル 41
11. 用語一覧 44
12. 執筆者一覧 47

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

1. ご挨拶

ここ数年、インターネット上における「トラスト」のレイヤの確立に向けた動きがグローバル、そして日本においても加速しています。例えば、米国 OpenID Foundation も全面的に協力し、インターネット上に信頼できるオーバーレイネットワークを構築することを目的として 2021 年 9 月に設立が発表された GAIN（Global Assured Identity Network）[1]、日本政府の取り組みとして内閣官房が主導しているTrusted Web推進協議会[2]など、幅広く「トラスト・信頼」とは何なのかが改めて問われている時代が到来しているということができます。これらの背景には金融犯罪やフェイクニュースなど業界を問わず「デジタル・アイデンティティの詐称」をベースとした事件や事故が日々発生し続けているということが挙げられます。

一般社団法人OpenIDファウンデーションジャパンでは 2019 年より電子取引における顧客確認を OpenID Connect の利活用により高度化するための取り組みとしてKYC ワーキンググループを立ち上げ、2020 年には「サービス事業者のための本人確認手続きに関する調査レポート[3]」、2021 年には「サービス事業者のための、継続的顧客確認(オンゴーイング KYC)に関する調査レポート、次世代における KYC の方向性に関するレポート[4]」を公開してきました。

本レポートは 2021 年に発表した次世代における KYC に方向性に関するレポートを更に深堀りし、現在 Implementer's draft の第4版となっており 2022 年中に最終版の出版を目標としている OpenID Connect を利用して KYC 済み顧客情報を安全に事業者間で伝達するためのプロファイルである OpenID Connect for Identity Assurance[5] を日本国内で利活用するためにはどのような対応が必要となるかを取りまとめているものです。先に述べた GAIN などの取り組みを含め、いよいよグローバルでは OpenID Connect の KYC への利活用が進んでいく中、事業者が国内からグローバルへ事業を拡大する上ではいち早くこれらの標準をフォローし実装していくことが益々重要になることが容易に想像がつきます。事業者の中で顧客情報の管理やトラストを考える実装者の方々が本レポートを手にとっていただき、より安全で実効性があるシステムの構築を進めていただけることを願います。

最後に、議論や執筆にご参加・貢献いただいたKYCワーキンググループの構成員の皆様に感謝を申し上げます。

---

[1] https://gainforum.org
[2] https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html
[3] https://www.openid.or.jp/news/2020/01/kycwg-report.html
[4] https://www.openid.or.jp/news/2021/09/kycwg.html
[5] https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

2022 年 11 月
OpenIDファウンデーションジャパン
代表理事　富士榮　尚寛

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

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の Phase3 で取り上げたテーマである、「理想の KYC、次世代 KYC」についての検討を行った結果について取りまとめたレポートである。

「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」[6]を公開している。Phase2 レポートでは、次世代の KYC に求められるものについての現状と今後に向けてどういったことを考えていくべきか、現在地点はどこか、といった点を整理した。

Phase3 の活動結果となる本レポートは、Phase2 の継続検討として、次世代に向けた KYC 実施時のルールとツールの整理と、それを踏まえて今後の普及に必要な OpenID Connect for Identity Assurance[7] (略称: OIDC4IDA、IDA、以降 IDA と記載)の国内向けのミニマム仕様の検討・整理を行った。

「ルール」とは、身元確認に関わる運用上の要件や契約上の取り決めに関する要件のこと、「ツール」とは、IDA や Claims Aggregation といった身元確認に関わる技術仕様などに関する要件のことである。

「ルール」には、主に当事者間の信頼関係の構築と適切な認証レベルを備える必要があること、「ツール」には、標準的なやり方で、必要最低限の情報を流通させることと、真正性の検証が行えることが必要であると考えた。

「ツール」としては、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を IDA の国内向けのミニマム仕様として検討することとした。検討の結果として、身元確認済情報のテンプレートを Scope で定義し、身元確認済情報を IDA 同様に返却すること以外は既存の OpenID Connect から大きく変更しない形の仕様を提案している。

身元確認済情報のプリセットとしての Scope を定義したことで、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利用しやすい仕様にしていくことができるのではないかと考えた。

---

[6] 次世代における KYC の方向性に関するレポート
https://www.openid.or.jp/news/next_generation_kyc_report.pdf

[7] OpenID Connect for Identity Assurance 1.0
https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

国内向けのミニマム仕様はまだ検討の段階であるが、Phase4 では仕様化を進め公開することで様々な事業者による採用が進み、将来的に日本国内のデジタル本人確認の実装が簡易になることを期待したい。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

3. 次世代 KYC 検討の経緯

KYC ワーキンググループ Phase2 の活動では、過去検討でまとめられた理想の KYC の内容を踏まえ、KYC を依拠するモデルを検討し、その結果としていくつかのモデルに整理した。

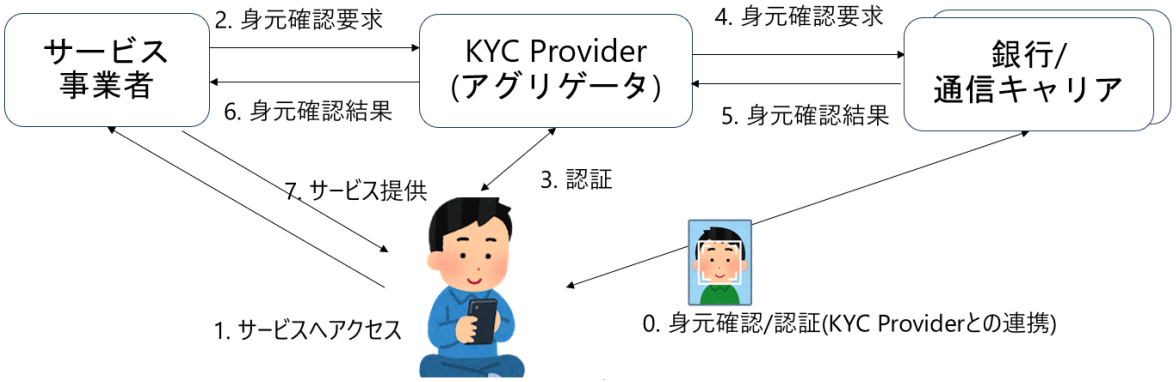

図3-1 理想の KYC 検討を踏まえた KYC 依拠モデル

また、一方で現実解としてサービス事業者がなぜ身元確認を必要とするのかという観点で目的と要件を整理し、それらを上記の KYC の依拠モデルに当てはめることで、サービス事業者（RP: Relying Party）、身元確認を実施した事業者（上図の銀行/通信キャリア。CP: Claims Provider）、それらを仲介する事業者（KP: KYC Provider）がそれぞれどのようなモチベーションでサービスを提供するのかを整理し、それぞれのアクターについての要件をとりまとめた。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

表3-1 各アクターにおける要件のカテゴリ(Phase2 検討時点)

要件	カテゴリ	キーワード
RP が KP に求める要件	IAL	依拠するために十分な種類のエビデンスの提供
	AAL	当人認証の強度
	FAL	改ざん防止
	プライバシー	取得データの最小化
	トラスト	データ提供者の信頼度など
RP が CP に求める要件	AAL	当人認証の強度
	プライバシー	取得データの最小化/ユーザ同意
	トラスト	データ提供者の信頼度など
KP が RP に求める要件	トラスト	トラストフレームワークにおける契約/ポリシー
KP が CP に求める要件	IAL	十分な種類のエビデンスの提供
	プライバシー	ユーザ同意
	トラスト	トラストフレームワークにおける契約/ポリシー
CP が RP に求める要件	AAL	当人認証の強度
	トラスト	相互の信頼性/トラストフレームワーク
CP が KP に求める要件	AAL	当人認証の強度
	トラスト	相互の信頼性/トラストフレームワーク/認定制度

Phase2 のレポートを一部修正。詳細は Phase2 レポート 6章を参照[8]のこと。

本レポートでは、Phase2 のレポートでまとめた要件をさらに細分化した。その結果を受け、KYC 依拠モデルの構成の整理や、実際に利用してもらうために必要な IDA 仕様の国内向けのミニマムな要件を整理した仕様の提案を行っている。

[8] 次世代における KYC の方向性に関するレポート
https://www.openid.or.jp/news/next_generation_kyc_report.pdf

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

4. KYC の要件とツールとルール

Phase2 で整理した各要件について、現実で運用していくためのより具体的な要件の検討を行うべく、Phase3 では「ルール」と「ツール」の二つの大きなカテゴリに分類し、整理した。

「ルール」では、身元確認に関わる運用上の要件や契約上の取り決めの観点を整理し、各事業者がどういった考え方で事業に身元確認を取り入れるべきか、最初の検討をする材料として利用できると考えた。

「ツール」では、技術的な観点で IDA や Claims aggregation といった身元確認の技術仕様に関連する要件を整理し、現在策定中の関連仕様を踏まえて整理していくことで、足りていない要件を可視化できると考えた。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

5. KYC 実施時のルールの整理

本 WG では、身元確認に関わる運用上の要件を整理した上で、要件を満たすために各々に求められる必要な契約上の取り決めを「ルール」として整理を行った。
その上で、Phase2 において理想の KYC モデルとして提起した、KYC の依拠モデルを運用していく上で、相互で合意した当事者間でのみサービスを提供することを前提とした場合に必要と想定されるルールの検討を行った。

5.1. RP、KP、CP 共通に求められること

- 相互に信頼関係を結んでいること
  KYC の依拠モデルでは、OpenID が元来想定しているような自由な情報流通ではなく、身元確認済みの属性情報をやり取りする事業者間で、契約などに基づく一定の信頼関係の構築が必要と考えられる。
  背景としては以下のような点が挙げられる。
  - 身元確認済みの属性情報を提供する KP/CP としては、不特定多数の RP に 身元確認済みの属性情報を提供するリスクは避けたい
  - 身元確認済みの属性情報を利用する RP としては、CP から取得する情報がどのように整理されて、KP から提供されるのかを事前に確認したい
- 適切な当人認証レベルを備えていること
  KYC で利用する情報は個人を特定する情報であり、取扱いには十分な注意が必要である。KYC の依拠モデルを考える際に、セキュリティに不備が生まれることは避けたい。特に KP や CP からすると、提供した個人情報が不正利用されてしまうことを避けたい。
  一連の依拠の流れの中で、どこか1箇所でも当人認証レベルが下がってしまうと、全体の当人認証レベル・身元確認レベルが下がってしまう。つまりは、一番レベルの低いところが、全体のレベルとなってしまう。
  そのため、依拠モデルに関わるすべてのアクターが、相互に取り決めたレベル以上の当人認証機能を具備し、不正利用が行われないような信頼関係を構築することが必要と考えられる。
- 異なる根拠法に基づく身元確認結果の相互運用が可能なこと
  CP が実施した身元確認に関する根拠法（例：犯罪収益移転防止法、携帯電話不正利用防止法、等）が RP の事業で求めているものと違う場合でも、相互運用でき

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

るようになることで、より多くの身元確認済みの属性情報の活用、依拠モデルの展開が可能となると考えている。

そのため、身元確認済みの属性情報の流通形式として、特定の根拠法に依存する形ではなく、汎用性のある形式での情報流通方式であることが求められる。

また、汎用的な情報流通形式としておくことで、将来的には現行の法制度では困難な、法規制のある事業・組織間での依拠の実現も可能となると考えられる。

現行の法制度では、根拠法が異なる場合（例: 犯罪収益移転防止法と携帯電話不正利用防止法）、法律ごとに要求される身元確認の内容や手法が定義されており、少しずつ内容が異なっている。一方で、身元確認の実際の行為としては同じようなものであることが多い。

現在の法律上は困難ではあるが、法律ごとに身元確認手法を定義するのではなく、身元確認手法を定義した上で各法律で参照することが出来ると、異なる根拠法に基づく身元確認結果間での相互運用性を持つことが可能となるため、今後の法改正等に期待したい。

5.2. RP 個別に求められること

- 取得した情報の利用用途を開示すること

  KP / CP からすると、保有している顧客の個人情報を提供することになり、身元確認以外の目的で提供した属性情報を使用されると、顧客の信頼を失う可能性がある。そのため、想定している用途以外で利用されることがないように、利用目的を把握しておきたい。

- 取得した情報を適切に管理できること

  KP / CP からすると、保有している顧客の個人情報を提供することになるため、仮に提供先で事故が起きた場合に、提供元のレピュテーションリスクになりうる。そのため、RP には顧客情報を守る体制が整っていることを要求したいと考えられる。RP の情報管理体制が適切であることを客観的に評価出来るようにするため、ISMS や Pマーク等の外部機関による認定を受けていることが望ましい。

- 必要な情報だけを要求、取得すること

  最小権限の原則に基づいて、RP は目的に必要な最小限の情報だけが要求できる状態であることが望ましい。例えば、年齢だけ必要な場合に、本人確認書類その

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

ものを要求してしまうと、RP は本来扱うことを想定していない個人情報を取得してしまうことになる。

5.3. KP 個別に求められること

- KP 自体の信頼性担保のため、内部統制に関する外部機関の認証を取得していること

  KP は CP から個人情報を預かり、また適切に RP へと提供することが求められることから、運用には高い信頼性が要求される。特に、RP へ提供される情報が KP によって改ざんされないか、という点を中心に、CP や RP は不安を持つことになる。そのため、国際認証の SOC (Service Organization Control) 等の内部統制に関する外部機関の認証を取得することで、その安全性を客観的に評価できる状況としておくことが望ましい。

- RP が、身元確認情報提供元の CP が明確にわかること

  KP が 複数の異なる CP から収集した属性情報を集約して RP へ引き渡す、というモデルも想定される。その際に、RP が信頼できる CP から受け取った情報のみを利用したり、あるいは CP がどのような方法で身元確認を行っているため信頼に足るかを判断する、といった信頼関係の構築が必要になるケースが想定される。

  そのため、各属性情報がどの CP から取得したものか、という情報を RP が判別できる状態にしておくことが望ましい。

- KP がアグリゲータとして十分な機能を有していること

  KP は CP を束ねて RP へ個人情報を提供するという役割（アグリゲータ）であり、RP へ単一のインターフェースで様々な CP の情報を提供できるべきである。そのためにも、KP が標準化された仕様への準拠（例えば IDA など）や認定制度、相互運用性テストを通過している状態であることが望ましい。

  補足として、アグリゲータの「集約」の役割として、カバレッジの提供（1つの CP だけでは、多くのユーザカバレッジが得られない場合に、複数の CP のどれか1つを選択可能とする）と、身元確認情報以外の追加情報の提供（1つの CP だけでは得られない、追加の属性情報を複数の CP から取得して提供する）という2つの役割が考えられる。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

5.4. CP 個別に求められること

- ユーザ同意の上で身元確認結果が提供されること

  CP の利用者の視点からした場合、提供した個人情報を無断で RP や KP に提供されることは望ましくない。例えば、OAuth や OpenID Connect の同意プロセスを用いるなどして、CP の保持する個人情報を RP や KP に提供することに対する同意を対話的にユーザから得る形とすることが望ましい。

- 事前に扱う情報について KP と CP 間で合意していること

  KP は予め CP がどういった属性情報を提供できるかを知っておくことで、RP からの要求に合わせて適切な CP へ誘導を行うことができる。そのため、KP に対してどういった属性情報を提供できるか、予め契約等で合意しておくことが望ましい。

- CP は KP/RP からの要求にあわせた情報を返却しないこと

  RP のサービスによっては、KP が CP に要求する属性情報が異なることが想定される。例えば、単なる年齢確認目的の場合であれば、基準となる年齢以上/以下を返却できればよい。また、郵送物を送りたい場合であれば氏名、住所といった身元確認を行っている属性情報そのものが必要となる。そのため、リクエストパラメータ等により、

  - 取得したい情報の条件を細かく指定できる
  - 取得したい属性情報や根拠法の指定に対応できる

  という状態であることが望ましい。

  加えて、KP/RP に対し、必要最低限の情報を返却し、要求以上の情報を返却しないことが望ましい。

- 情報の真正性（トラストアンカー）がわかること

  RP のサービス特性によっては、適用可能な身元確認方法が限定される可能性が想定される。そのため、CP はどういった方法（例：対面/オンライン、本人確認書類の種類など）で身元確認を行ったのかを提供できる状態としておくことが望ましい。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

6. KYC 実施時のツールの整理

5章では KYC の依拠モデルを運用していく際に必要と考えられるルールについて整理を行った。本章では、ルールに合わせて運用していくための技術的な要件、ツールに関する必要要件の整理を行った。

6.1. 技術的な要件

KYC の依拠モデルを実現する際に必要とされる技術的な要件は、下記が挙げられる。

- RP が（標準的なやり方で）身元確認された属性情報を受け取れること
- RP が（標準的なやり方で）身元確認の根拠を受け取れること
    - 本人確認書類の種類、発行日、有効期限など何かがわかること
    - CP にて身元確認をいつ/どのように行ったか、根拠法はなにか、等
- RP が必要最小限の情報だけ取得できること
    - RP がどの情報が必要かを指定できること
    - RP が本当に必要な情報しか要求しないこと
- CP から取得した情報が改ざんされてないことを証明できること

6.2. システム構成

上記の技術要件を満たすシステム構成として、3つの多段構成のパターンを検討した。

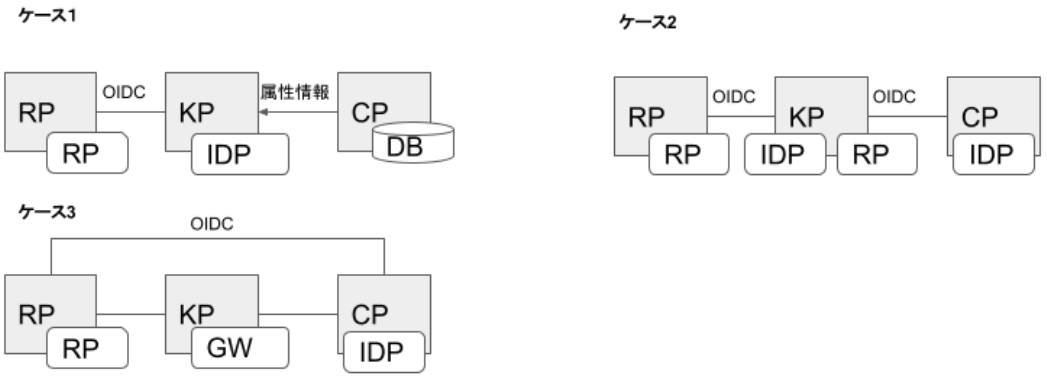

図6-1 KYC 依拠モデルの想定パターン

表6-1 KYC 依拠モデルのケース分類

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

ケース1	● CP は任意のプロトコルで、KP に属性情報を提供する ● KP は CP をデータソースとする OpenID Connect の IDP として動作する ● RP と KP 間は OpenID Connect で連携する
ケース2	● CP は OpenID Connect の IDP として動作する ● KP は CP に対し、OpenID Connect の RP として動作しつつ、RP に対し、OpenID Connect の IDP として動作する ● KP と CP がそれぞれ IDP として動作する。同意取得は KP で実施 ● KP がユーザに引き渡す CP の情報をコントロールする ● RP - KP 間、KP - CP 間でそれぞれ独立した認証プロバイダとして動作する形で、2段階のフェデレーションのような形を想定
ケース3	● CP は OpenID Connect の IDP として動作し、同意取得も行う ● KP は要求された情報に応じて、適切な CP を提示する ○ Discovery Service のように振る舞う形を想定 ○ イメージは、学術認証フェデレーション（学認）が認証時に接続する大学一覧を表示する様にユーザが使用する CP を一覧から選択する形態

ケース1およびケース3は、システム構成は実質的に2者間の属性情報連携となる。

そのため、ケース1およびケース3は IDA を利用することで、現時点では技術要件を満たしていると考えられる。

ただし、ケース1では、CP が KP に提供した属性情報の真正性は、KP が担保する形となる。

ケース2においても、IDA を利用することは可能である。しかし、CP が複数存在するケースかつ、KP が CP から受け取った属性情報を選択的に RP へと返却する場合、CP の署名付きで渡すことが出来ず、RP が CP の検証を行うことが出来ない（KP までしか信頼できない）という課題がある。複数の CP から属性情報を集めるユースケースは、現在策定

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

中の OpenID Connect Claims Aggregation 仕様[9]や、W3C で策定された Verifiable Credentials[10] を活用することで課題の解決が期待される。
また、KP が存在するモデルにおいては、ユーザーは CP の数だけ事前に認証認可が必要であり、UX 上煩雑であることが想定されるため、今後の検討課題である。

[9] OpenID Connect Claims Aggregation Draft 02
https://openid.net/specs/openid-connect-claims-aggregation-1_0.html
[10] あるエンティティに関する属性情報を、検証可能な方式で表現するデータモデルである。W3C で仕様定義されている。https://www.w3.org/TR/vc-data-model/

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

7. OpenID Foundation で策定している関連標準仕様の検討状況

6章では、KYC の依拠モデルを運用していく際に、IDA を利用することで、技術要件を満たすことが確認できた。

そこで、改めて IDA 並びに IDA で言及されているセキュリティプロファイルとしての Financial-grade API の最新の検討状況の確認を行った。

本章では、2020年1月に発行した、「サービス事業者のための、本人確認手続き（KYC）に関する調査レポート　第1.0版[11]」並びに、2021年9月に発行した、「次世代における KYC の方向性に関するレポート　第1.0版[12]」の内容を元に、最新の検討状況について追記した。

7.1. 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 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

[11] サービス事業者のための、本人確認手続き（KYC）に関する調査レポート
https://www.openid.or.jp/news/oidfj_kycwg_report_20200123.pdf
[12] 次世代における KYC の方向性に関するレポート
https://www.openid.or.jp/news/next_generation_kyc_report.pdf

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

- 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 は2022年10月に 4th Implementer's Draft ステータスとなっている。現在、Final バージョン公開に向けて、最終的な実装者からのコメントの募集、修正、確認作業を実施中である。

次の図は IDA を利用したリクエストとレスポンスの例である。

レスポンスについては、JSON の verified_claims 要素で表現され、本人確認プロセスの中で検証済みの属性情報(claims 要素)の他に根拠情報(verification 要素)を合わせて返却することで、属性情報がどのような根拠によって確認されたものかを証明することができる。

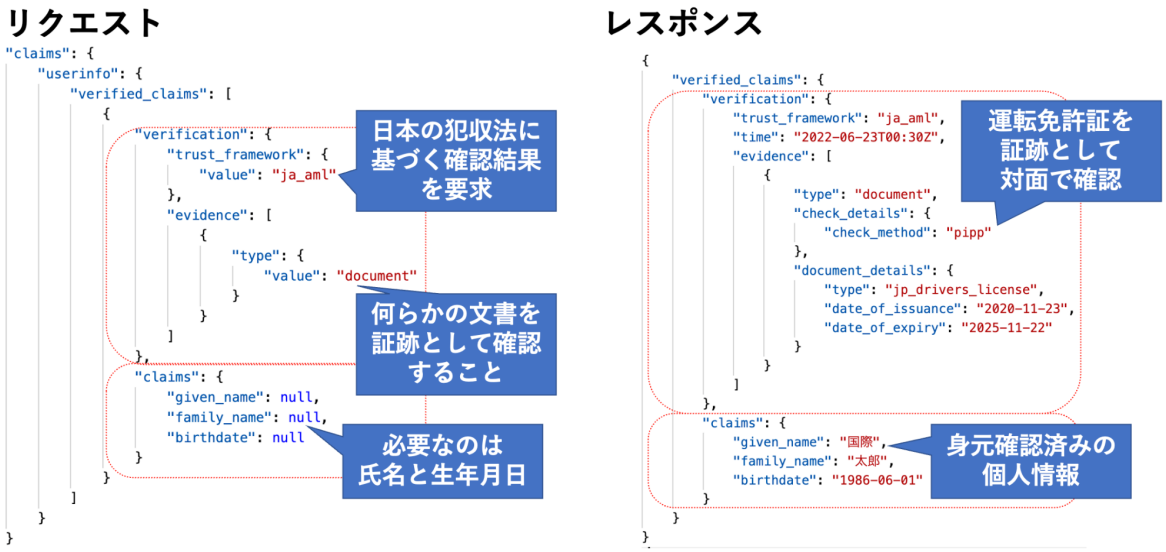

図7-1 OpenID Connect for Identity Assurance におけるリクエストとレスポンスの例

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

また、リクエストについては、上記のように Authorization Request 時に必要な情報の詳細を Claims Parameter として記載し、必要最小限の個人情報のみ取得)することが望ましい(データ最小化の原則)。

別の手段としては、提供元(OP)が規定した定型的な情報セットを scope として記載することも可能となっている。ただし、その際にはデータ最小化の原則に留意すべきである。例えば、提供先(RP)が必要と考えられる最低限の情報セットを複数 scope として用意するなどが考えられる。(例として第8章を参照のこと)

7.2. Financial-grade API

FAPI (Financial-grade API) とは、OpenID Foundation FAPI WG で策定されている、OAuth 2.0 のセキュリティプロファイルである。OAuth 2.0 はあらゆる分野において広く利用されている API の認可フレームワークだが、その用途の広さや自由度の高さと引き換えに、特定のユースケースに対応するためには追加のセキュリティ対策などを施す必要がある。

Fintech の台頭をきっかけに、金融 API を安全に使うための共通な枠組みの必要性から、英国の Open Banking で策定された API プロファイルをベースに標準化されたものが、FAPI である。策定の経緯からも分かるとおり、FAPI は金融 API での利用を念頭に置いているものの、金融レベルの安全性が求められる、あらゆるユースケースに適用されることを目指している。そのため、FAPI の正式名称も、Financal API ではなく、Financial-grade API と命名された。加えて、金融目的であるとの誤解を防ぐため、Financial という単語すら名称から取り外す検討もされている。

API のセキュリティ観点には、情報の漏洩を防ぐ観点と、それに加えて、情報の改ざんを防ぐ観点(否認防止性)があり、前者は Part 1: Baseline Security Profile として、後者を必要とするユースケースには Part 2: Advanced Security Profile として、2つのプロファイルが策定されることとなった。

前述の通り、FAPI は OAuth 2.0 を安全に使うためのセキュリティプロファイル であり、安全性を高めるための設定一覧を提示している。例えば、Part1 においては、ベアラトークン の禁止(スマホアプリ等の public クライアントを除く)、暗号アルゴリズムの最低ビット数の指定、認可サーバの接続先などの情報は OpenID Discovery を利用して取得することなどが規定され、Part2 では、Part1 に加え、public クライアントの禁止、リクエスト、レスポ

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

ンスの署名必須化などが規定されている。それら規定は簡潔に箇条書きで記載されており、チェックリストのように活用することができる。

上記2つのプロファイルは、FAPI 1.0 として、2021年3月12日に最終版[13]が公開された。

FAPI は、策定のベースとなった英国 Open Banking をはじめとして、オーストラリア、ブラジルにおける Open Banking、Open Data の取り組みにおける API セキュリティ標準として（一部各国のニーズにカスタマイズされながら）利用されている。また、北米や EU、中東などでも採用の検討が進んでいる。日本においても、一部企業や金融機関で FAPI の採用が見られるほか、「オープン API のあり方に関する検討会報告書[14]」の中で、「同団体(OpenID Foundation)において OAuth2.0 の標準仕様が定められた場合には、各銀行において同仕様への準拠や準拠に向けた方針等が検討されることが望ましい」とあることから、今後採用にむけた動きが加速することが期待される。

現在、FAPI WG では、利便性と相互接続性を向上させた FAPI 2.0 の策定に現在取り組んでいる。

FAPI2.0 では、仕様のオプション（選択肢）を減らすことで相互運用性の向上を図っており、またブラウザを経由せずに許諾内容などのパラメータを事前にサーバ間で取り交わす Pushed Authorization Request [15](PAR)の必須化によりセキュリティの向上を図っている。加えて、Grant Management[16] という新しい仕様を追加することにより、今までは IDP 側でしか許認可の状態を変更できなかったものを、RP 側で変更をリクエストできるようになり、特に1つの RP で多数の IDP に接続する、家計簿サービスのようなユースケースにおいて、ユーザの利便性を向上させている。

IDA では、重要な個人情報を授受するユースケースも想定される。IDA 仕様としては FAPI の利用は必須とはされていないが、ユースケースに沿った、安全なプロファイルを選定することとしている。とはいえ、特に理由がない限り、まずは FAPI の利用を検討するべきである。なお、IDA において FAPI を利用する場合には、セキュリティ制約上、OpenID

---

[13] Financial-grade API Security Profile 1.0 - Part 1: Baseline
https://openid.net/specs/openid-financial-api-part-1-1_0.html
Part 2: Advanced
https://openid.net/specs/openid-financial-api-part-2-1_0.html

[14] オープン API のあり方に関する検討会報告書 2017 年3月 16 日 オープン API のあり方に関する検討会（事務局:一般社団法人 全国銀行協会）
https://www.zenginkyo.or.jp/fileadmin/res/news/news290316_2.pdf

[15] RFC 9126 OAuth 2.0 Pushed Authorization Requests
https://www.rfc-editor.org/rfc/rfc9126.html

[16] Grant Management for OAuth 2.0
https://openid.net/specs/fapi-grant-management.html

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

Connect 認定(Conformance Test)で必要とされる認可タイプの一部が FAPI 認定[17]では認められないため、両認定を同時に満たすことはできない点に留意すべきである。

7.3. OAuth2.0 Pushed Authorization Requests (PAR)

Pushed Authorization Request (PAR) とは、OAuth2.0 の拡張仕様で、RP が直接 IDP に対してリクエスト内容を事前に伝達させることができる。既存の OAuth2.0 ないし OIDC でも、request-uri という形で、リクエスト内容を uri 形式で指定することができたが、具体的に RP と IDP 間でどのようにリクエスト内容を伝達するかについて仕様化されていなかったものを、PAR で仕様化したものである。

RP と IDP 間で直接リクエスト内容が通信され、さらにその際に両者で認証が可能である点と、通常の認証・認可リクエストと異なりユーザ（ブラウザ）から見える URL 内にリクエスト内容が含まれないことから、情報漏洩や改ざんの恐れがない。

さらに、IDA における Claims Parameter など、リクエストパラメータ内に複雑な内容を含むと、リクエストが長大になってしまうが、PAR によってそれを防ぐことができる。

[17] Conformance Testing for FAPI Read/Write and FAPI1Advanced-Final OPs
https://openid.net/certification/fapi_op_testing/

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

8. OpenID Connect for Identity Assurance (IDA 仕様) における国内向け仕様の検討

ここまで各種要件を整理してきた中で、今後、国内向けに IDA 仕様を採用するにあたり、実装が容易でかつ共通の認識をもつ必要があることがわかってきた。理由として、IDA 仕様は、できるだけ自由度を高めた形での仕様として標準化が進められており様々な解釈ができることから、IDP によってバラバラな実装になる可能性があるためである。

例えば、IDA 仕様の面では、次のようなことが考えられる。

- どの属性情報が返却できるか、IDP によって異なる可能性がある。
- 身元確認済みの属性情報がどのように claim として表現されるか、IDP によって異なる可能性がある。(姓名の項目が分かれている・分かれていない、住所の項目が分かれている・分かれていないなど)
- evidence として必要な属性情報を IDP によっては提供できない可能性がある。(本人確認書類の有効期限など)

加えて、IDA 仕様の実装にあたっては、下記のような課題が挙げられる。

- サービスや業界によっては本人確認に関する法制度・ガイドラインがないため、RP が何を基準として身元確認済みの属性情報を取得・利用すべきかを判断できない。

そこで、KYC WG では、IDA 仕様の詳細を確認し、IDP における IDA 仕様の実装の注意点と上記を踏まえて国内で利用しやすい IDA のミニマムな仕様を検討した。

なお、以降においては3章から6章にかけて検討してきた CP、KP、RP の多段モデルは考慮せず、RP と IDP のシンプルなモデルとして検討している。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

8.1. IDP における IDA 仕様の実装の注意点

IDP における IDA 仕様の実装の注意点の検討に先立ち、IDA 仕様における OpenID Connect のシーケンス図を作成し、実装に必要な内容がないか確認した。なお、シーケンス図は OpenID Connect の Authorization Code フローに基づいて記載をしている。(図 8-1参照)

注意点として大きなポイントとしては、下記の2点である。

1. Authorization Request 時に必要な属性情報を指定する方法として Claims Parameter[18] または scope を選択できること
2. verified_claims 要素の返却方法として、ID Token と UserInfo Endpoint を選択できること

また、それ以外の項目については表8-1で整理した。

まず、Authorization Request において、現行の実装として、IDP は OpenID Connect を提供するにあたり、Scope 単位で提供する属性情報を管理し、かつユーザへの同意を Scope 単位でグループ化して実施しているケースが多いのではとの意見があった。Claims Parameter の場合、Claim 単位でのユーザの同意管理の仕組みを作り直す必要が出てくる。そのため、Claims Parameter が必須となってしまうと、IDP が属性情報提供の単位を Claims Parameter にて Claim 単位で管理しなおすように設計を見直す必要があり、対応するのは簡単ではないため、Scope 単位での属性情報の要求を行う方が良いと判断した。

次に、verified_claims 要素の取得方法について、ID Token と UserInfo Endpoint のどちらで取得すると良いのか検討した。ID Token は、IDP としてログイン機能を提供する際に、sub や iss などにてユーザ識別子を提供している。また、ID Token の真正性確認のため RP にてトークン検証をしている。しかしながら、IDP はログイン機能を無償で提供し、属性情報は UserInfo もしくはそれに類似する API で有償で提供しているケースが多い。そのため、verified_claims 要素で取得する属性情報は UserInfo Endpoint で提供した方が良いと判断した。

[18] Claims Parameter については、下記を参照
https://openid.net/specs/openid-connect-core-1_0.html#ClaimsParameter

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

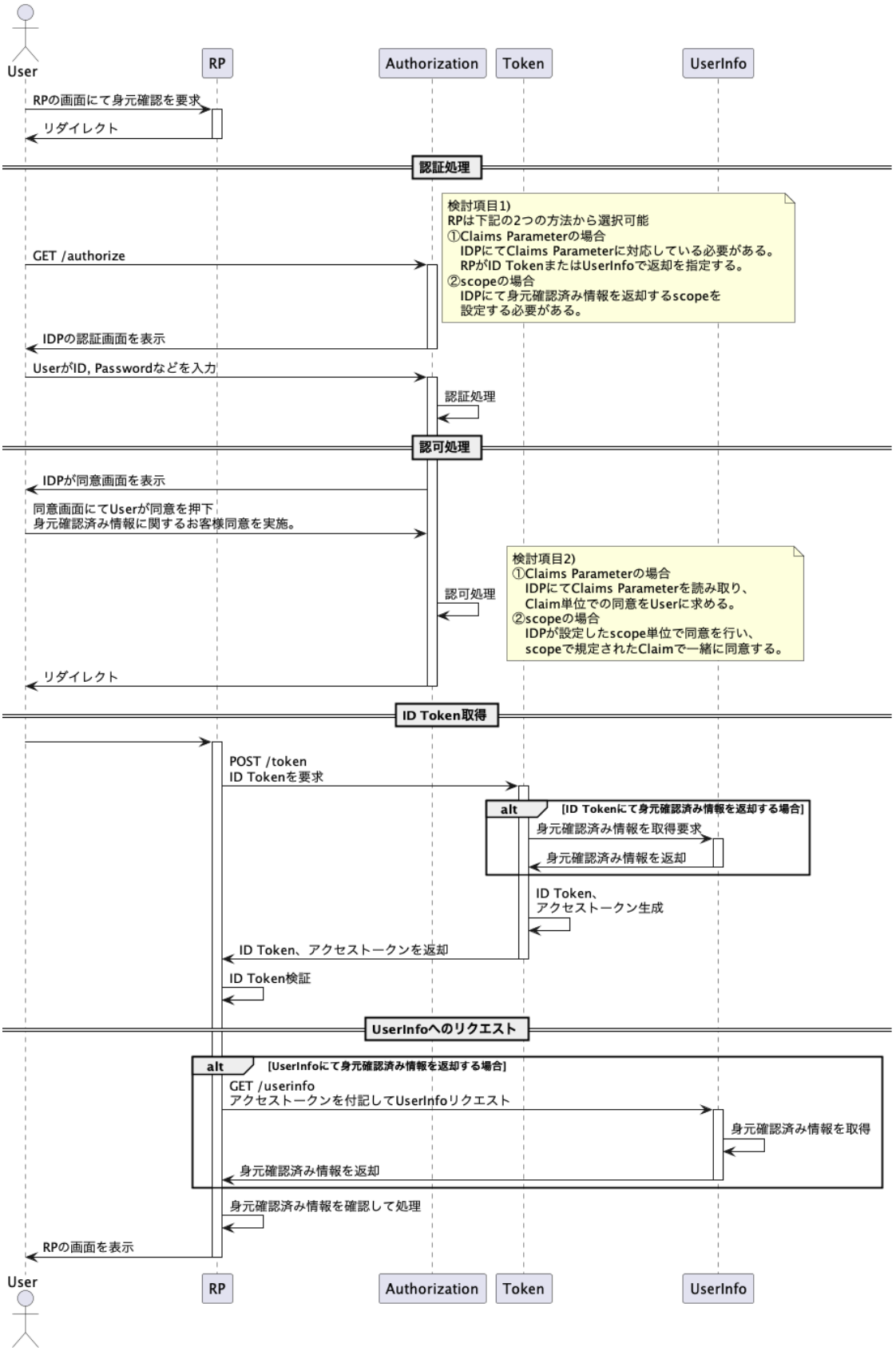

図8-1 OpenID Connect for Identity Assurance シーケンスと検討項目

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

表8-1 OpenID Connect for Identity Assurance 実装時の注意点

	IDA の実装の注意点	詳細
1	Authorization Request の方法をどれにするか？	RP は下記の2つの方法から選択可能 ① Claims Parameter の場合 IDP にて Claims Parameter に対応している必要がある。 RP が ID Token または UserInfo Endpoint で返却を指定する。 ② scope の場合 IDP にて身元確認済みの属性情報を返却する scope を設定する必要がある。
2	ユーザへの同意の単位はどうするか？	① Claims Parameter の場合 IDP にて Claims Parameter を読み取り、Claim 単位での同意をユーザに求める。 ② scope の場合 IDP が設定した scope 単位で同意を行い、scope で定義された Claim 全てを一緒に同意する。
3	verified_claims 要素の取得方法をどれにするか？	① Claims Parameter の場合 ID Token で取得するのか、UserInfo で取得するのかを RP で指定可能。IDP 側で Claims Parameter を読み取り、対応する必要あり。 ② scope の場合 IDP により ID Token、UserInfo のどちらで返却するのか規定している。
4	本人確認書類の verification 要素に必要な項目は何か？	verification 要素には、IDP がアカウントに対し身元確認を行った時の、本人確認書類の根拠情報（有効期限など）や身元確認方法（対面など）が返却できる。 RP によって、どの情報が必要になるのか選択する必要がある。
5	身元確認するための claims 要素の項目は何か？	国内の法律等で定められている本人特定事項としては、「氏名」「生年月日」「住所」であるが、OpenID Connect には同じような項目が複数ある。 （例：name、given_name、family_name など） また、日本語の場合、漢字・カナへの対応も必要。
6	準正常エラー時の挙動はどうするのか？	IDP にて身元確認を未実施のユーザなどの対象外ユーザである場合にどのようなエラーを返却するべきか IDA では記述が定まっていない。 例： ・IDP が提供できない claim は応答から削除する ・要件に合致しないデータの場合は、verified_claims 要素全体を省略する ・HTTP エラーで返却する
7	課金のタイミング	IDP が有償で身元確認済みの属性情報を提供する場合、どのタイミングで課金をするのか規定がない。 ID Token では IDP としてログイン機能を提供しているケースではログインの度に課金が発生する可能性がある。 UserInfo により、認証と属性情報の切り分けが可能になる。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

8.2. IDA 仕様からの国内向けのミニマム仕様の検討

IDA 仕様の実装の注意点を考慮し、すでに OpenID Connect を提供している IDP に対して開発負荷の少ない仕様について検討を進めた。

国内向けのミニマム仕様の基本方針としては下記の通り。

- IDA 仕様としての Authorizaion Request を scope で行い、身元確認済みの属性情報の提供・同意を scope にて管理する。
- verified_claims 要素の取得方法は、UserInfo Endpoint で返却する。

scope を用いることのメリットは3点ある。

1. RP にとって必要な身元確認のレベルを scope で表現することができるため、サービスのために必要な情報を RP が個々に検討して取得せずとも、事前に整理された身元確認済みの属性情報を取得できる点である。
2. IDP が身元確認済みの属性情報を提供するためのユーザの同意の単位を scope 単位で管理することができる。IDP としては、Claim 毎に同意の管理をする必要がなくなり管理が楽になる。また、アクセストークンに紐づく Claim についても Scope 単位で管理できる。
3. IDP が身元確認済みの属性情報を有償で提供する場合、scope の単位で課金対象の判別をすることができるためである。Claim 単位となった場合、Claim 単位で価格を設定するのかなどの検討をする必要がある。

また、UserInfo Endpoint を利用することで、認証と身元確認済み属性の提供の切り分けがしやすくなり、エラーハンドリング（準正常等）や課金の対応がしやすくなる。ID Token では、認証時のエラーとの切り分けや、ログインの度に課金をするべきなのかどうかを判断して実装する必要が出てくる。

また、scope の詳細について、標準を考慮し詳細を8.3章に記載する。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

表8-2 OpenID Connect for Identity Assurance ミニマム実装案

	ミニマム実装案	詳細
1	Authorization Request の方法をどれにするか？	scope にて設定。KYC WG にて検討した scope 名にて定義する。
2	ユーザへの同意の単位はどうするか？	scope にて同意を行う。scope で規定された Claim 全て一緒に同意する。
3	verified_claims の取得方法をどれにするか？	UserInfo にて取得する。準正常エラーや課金のタイミングを考慮すると、ID Token ではなく UserInfo にて取得する方が良いと判断。
4	本人確認書類の verification 要素に必要な項目は何か？	8.3章の scope 定義にて詳細説明。
5	身元確認するための claims 要素の項目は何か？	8.3章の scope 定義にて詳細説明。
6	準正常エラー時の挙動はどうするのか？	今後の継続検討課題とはなるが、Claim の削除や HTTP エラーではなく、JSON の返却項目としてエラーを表現することが望ましい。
7	課金のタイミング	Userinfo に対するトランザクションにて課金。 無償で属性情報を提供している UserInfo API がある場合は、別 API として切り出す等の検討が必要。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

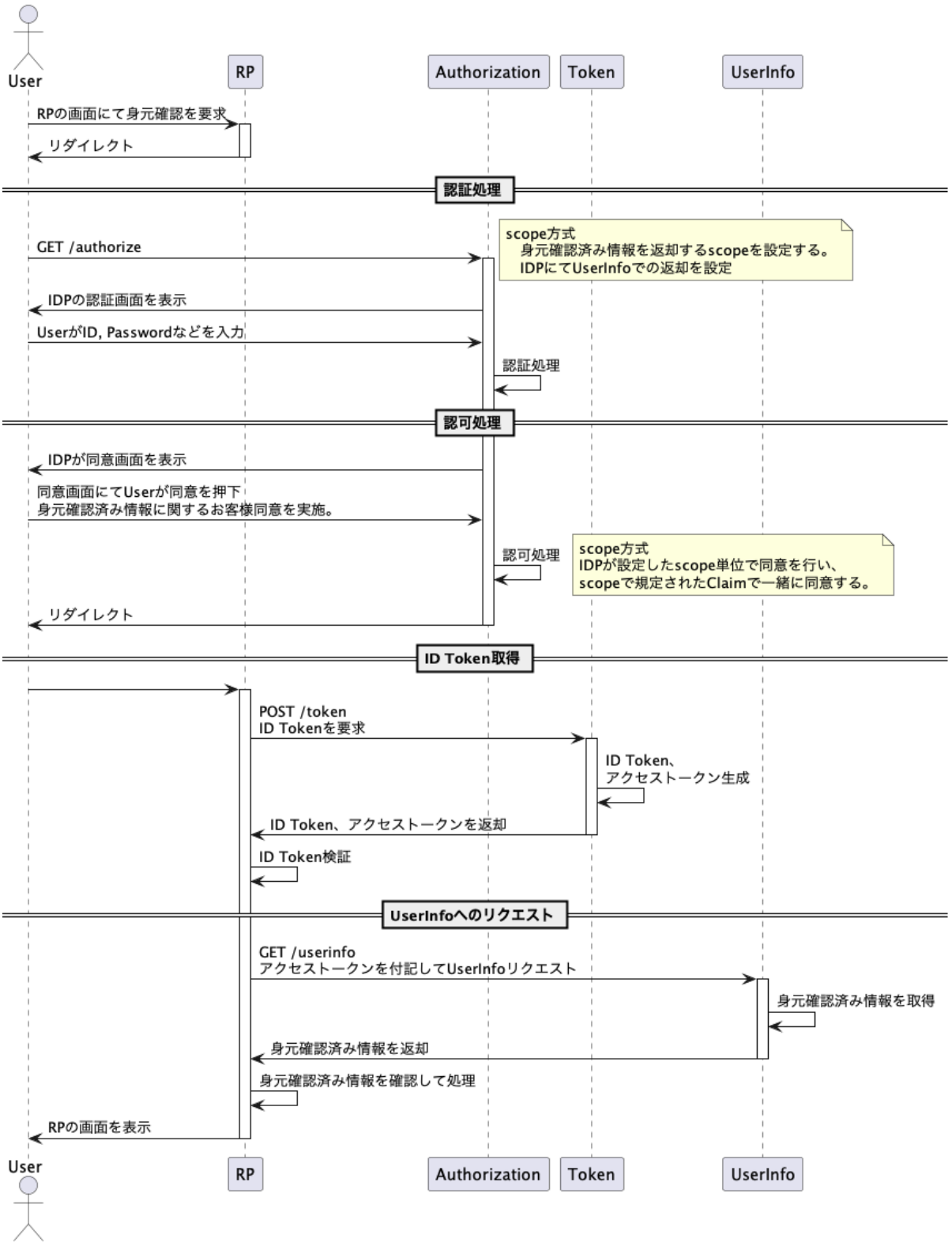

図8-2 OpenID Connect for Identity Assurance ミニマム実装案シーケンス

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

8.3. 国内向けミニマム仕様の Scope 定義

前項で取り上げたように IDA の国内向けのミニマム仕様を定義するにあたり、Scope の定義が必要となる。

Scope の値とそれに紐づく身元確認済みの属性情報を定めるにあたって、何の単位で取り決めるのか、どの程度のバリエーションが必要なのか、何の値を返却すべきかなど、事業者にとって使いやすい枠組みとできるかを検討した。

Scope の値としてまず考えられるのは、犯罪収益移転防止法(犯収法)などのトラストフレームワークの枠組みを指定する、あるいは、エビデンス（本人確認書類等）を指定することである。

前者は、RP がトラストフレームワークに準拠した身元確認を行った属性情報を取得することができる。そして、IDP はトラストフレームワークで規定された身元確認済みの属性情報を返却すればよい。ただし、現状の法制度では、サービスを提供する事業者自身が身元確認を行う必要があると規定されている。例えば、犯収法に規定された身元確認を行った事業者からの身元確認済みの属性情報の提供を受けただけでサービスを展開できるとはならないのが現状である。結果的に犯収法などトラストフレームワークの名称をこの Scope に適用すると、その法制度を満たすことができるという誤解を招きかねない。

後者は、何の本人確認書類を確認したかは分かるが、トラストフレームワークが問われないため身元確認の基準が明確でない。そのため、期待した基準に則って取得された身元確認済みの属性情報を取得できない可能性がある。

このように既存の法制度をベースとしたトラストフレームワークやエビデンスそのものを Scope の値とするよりも、国内向けのユースケースを想定し新たに Scope の値を考案するほうが有用であるのではないかと考えた。

そこで次に検討したのが、NIST SP800-63-3[19] で規定されている IAL（Identity Assurance Level）におけるレベルの粒度に合わせる形での定義である。国内向けのユースケースとしては、身元確認のレベルを定義し、必要なレベル感の身元確認済みの属性情報を取得できる形が事業者にとっては扱いやすいと考えられる。そこで、Scope で要求する属性情報をレベルごとに定義する形を想定した。

NIST SP800-63-3 で定義されている IAL を簡潔に整理すると以下のようになる（分かりやすさ優先のため正確ではないことに注意）。

[19] NIST SP800-63-3
https://pages.nist.gov/800-63-3/

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

表8-3 IAL の定義

IAL1	自己申告による身元確認（≒事業者での身元確認未実施）
IAL2	リモート、あるいは対面での身元確認
IAL3	対面による身元確認（有資格者による書類確認必須）

今回の用途を考えると、IAL1 は身元確認未実施であることから、IDA に定義される verified_claims 要素ではないと考えられる。また、そうした場合、実質 IAL2 及び 3 のみを Scope の定義対象とすると、表現できる幅がかなり狭まってしまう。そのため、IAL をそのまま当てはめる形では Scope 値のレベル感を表現する用途には合わないことがわかった。

国内向けとしては、用途に沿った形でレベル分けを行い、それに沿った形の Scope の値とそれに紐づく属性情報を用意したほうが良いと考えられる。ただし、細分化しすぎても利用しにくくなるため、ある程度包括した範囲での定義とするのが良いと考えた。

上記を踏まえ、KYC WG では以下の項目で Scope のレベル感を整理した。

表8-4 Scope のレベル定義における評価項目

依拠元（IDP）の確認内容	依拠元（IDP）で何に則って身元確認を実施したのか
依拠元（IDP）の身元確認手法	依拠元（IDP）の身元確認は対面での実施か非対面での実施か
依拠元（IDP）のエビデンスの有効期限	依拠元（IDP）で身元確認を行った際のエビデンスは有効期限内かどうか
依拠先（RP）に提供する証跡	どういった証跡が必要か
依拠先（RP）に提供する属性情報	依拠先（RP）に返却する属性情報は何か

これらの検討から、国内向け IDA の Scope の値として、身元確認のレベルとその際に返却される証跡・属性情報を整理したものが表8-3である。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

表8-5 国内向け IDA における Scope の定義

scope 名	レベル	依拠元の確認内容	依拠元の本人確認手法	依拠元のエビデンスの有効期限	証跡	属性情報
jp_oidf_ida_2022_high_unexpired_with_attachments	AA	犯収法レベル相当	対面・非対面	期限内必須	文書画像 確認プロセス 確認者 確認日（エビデンスの確認日＋全体プロセスの完了日）	氏名 住所 生年月日
jp_oidf_ida_2022_high_unexpired	A	犯収法レベル相当	対面・非対面	期限内必須	確認プロセス 確認者 確認日（エビデンスの確認日＋全体プロセスの完了日）	氏名 住所 生年月日
jp_oidf_ida_2022_high	B	犯収法レベル相当	対面・非対面	特になし	確認プロセス 確認者 確認日（エビデンスの確認日＋全体プロセスの完了日）	氏名 住所 生年月日
jp_oidf_ida_2022_medium	C	適度に簡易で信頼性のある KYC	対面・非対面	特になし	特になし	氏名 住所 生年月日
jp_oidf_ida_2022_medium_age_over_18	D	適度に簡易で信頼性のある KYC	対面・非対面	特になし	特になし	匿名情報 18歳以上か未満か[20]

[20] 事業者の要求に応じて、18歳以上だけでなく、16歳、20歳以上などの定義を追加することも可能だが、複数定義を同時提供することにより細かい年齢情報を提供しないよう留意すること。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

例えば、厳密な身元確認を行った結果を取得したいのであれば、AA レベルの Scope（jp_oidf_ida_2022_high_unexpired_with_attachments）を要求することで、犯収法レベル（先にも記載した通り、一部の例外を除き、犯収法に則って身元確認した結果を取得した事業者がそのまま犯収法に則ったとすることはできないためここでは犯収法「レベル」という記載にしている）の身元確認を行った事業者から、身元確認を行ったユーザの属性情報（氏名、住所、生年月日）とその身元確認時を行った際の証跡の情報（有効期限内のエビデンスの文書画像、確認プロセス、確認者、確認日）を取得することが可能となる。

文書画像などの情報までは必要ない（取得したくない）等であれば、Aレベルの Scope で要求することができる。さらに依拠元が身元確認した際のエビデンスの有効期限も問わないような場合は、Bレベルの Scope を用いればよい。

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あればCレベルの Scope が利用できる。
さらに属性情報は不要だが18歳以上を確認するなどの用途のためDレベルを設定した。

なお、Cレベル以下では、表中に記載の依拠元の身元確認内容を「適度に簡易で信頼性のある」と記載している。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[21]」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。

一方、ここまで検討してきた中で残った検討課題もある。

レベルを分けすぎると逆に不便になる可能性があることを踏まえて、代表的な利用と考えられる上記の分け方としたが、検討中にはこれ以外にも複数の案があった。例えば、軍事用や B2B の研究機関などで利用される用途として、AAの内容に加え、対面での身元確認が必須、確認者が信頼のできる機関などを設定する案や、身元確認実施有無のフラグのみを返却する案などが挙げられていた。レベルの表現に関しては様々なユースケースがあると思われることから、今後も継続検討に取り組んでいく。

また、AレベルとBレベルの差分はエビデンスの有効期限だが、身元確認に利用されるエビデンスのうち、例えば、住民票や保険証（の一部）に関しては有効期限が明確に記載されていないものもある。これらはAレベルの条件を満たさないものと整理している。住民票

[21]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（要約版）
https://www.meti.go.jp/press/2020/04/20200417002/20200417002-2.pdf

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

は発行後6か月間有効とする旨を犯収法や携帯電話不正利用防止法などには記載されているが、事業者によって異なる基準であることから、IDP が保証するレベル感としては表現が難しい。また、一部の保険証に関しては所有していること＝有効であるということになり、明確な有効期限が存在しない。これらのエビデンスの整理も必要であると認識している。

加えて、IDP が複数のエビデンスを用いて身元確認を行っていた場合にレベルをどう判断して返却するかについても明確でないところもあるため、継続して整理していきたい。

上記のような残った課題に関しては、継続検討を行っていく予定である。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

8.4. Scope 毎の返却 Claim の定義

IDA で定義された OP から RP に返却される身元確認済みの属性情報は7章で説明したように verified_claims 要素として表現され、OpenID Conecct 仕様の userInfo Endpoint にて返却される[22]。verified_claims 要素は verification 要素と claims 要素に分かれており、verification 要素ではどのような身元確認を実施したのかを表現し、claims 要素ではその確認を経て実際に提供される属性情報が表現される。
以下の表に簡単な概要を記載した。

表8-6 verified_claims 要素に含まれる項目の概要

項目名			内容
verified_claims			
	verification		検証プロセスに関するデータを含むオブジェクト ・検証の基準となるトラストフレームワーク、またレベル感は何か ・どのようなプロセスでいつ検証されたのか ・検証された証拠(evidence)の情報（後述） といった情報が含まれる
		evidence	検証するために必要なエビデンスに関する情報を含む JSON 配列 検証されたエビデンスの情報と、それがいつどこでどのように確認されたか といった情報が含まれる
	claims		エンドユーザの確認済み属性情報を含むオブジェクト 実際に返却されるユーザの属性情報が含まれる （氏名、生年月日、住所）

この verified_claims 要素としての表現に前章で整理した各レベルを当てはめ、どのような項目が必要になってくるのかを改めて整理した。

例として、AAレベルの verified_claims 要素を可視化したものが以下である。

[22] IDA の仕様上は IDToken に含む形でも返却できるが、7章で説明したように本検討では userInfo Endpoint から返却されると整理

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

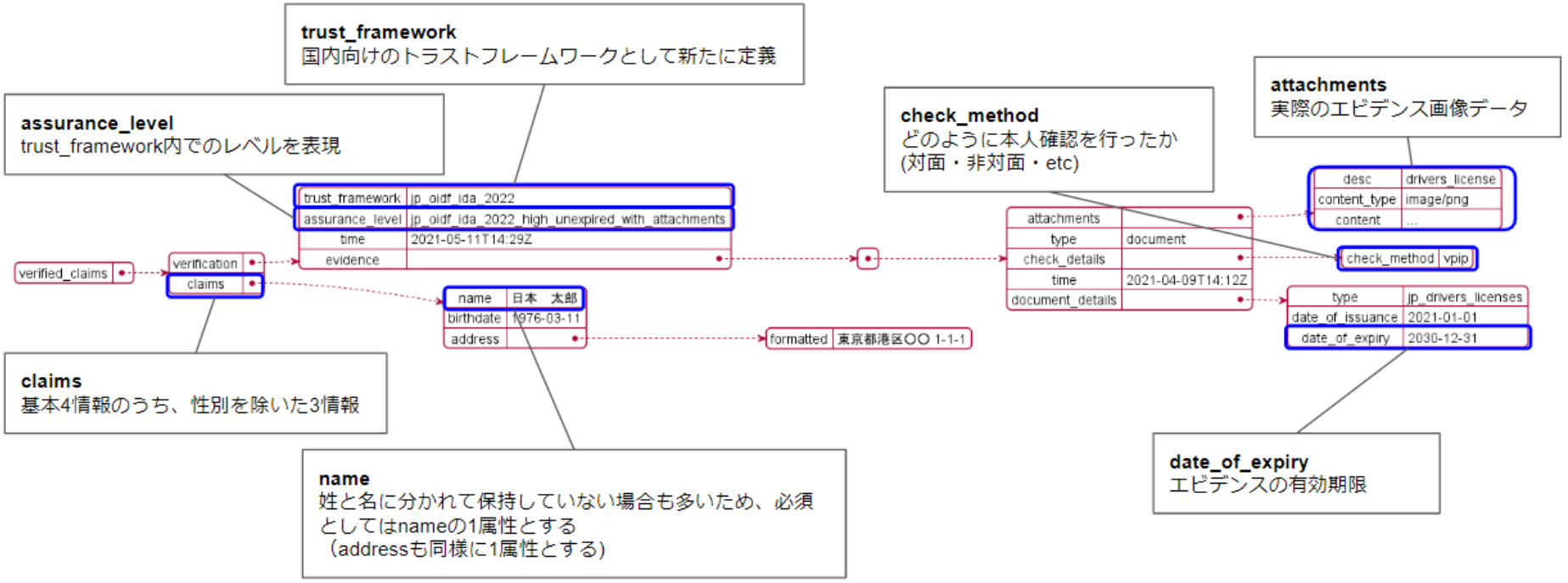

図8-3 verified_claims 要素の可視化

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

verification 要素に目を向けると、まず trust_framework 要素と assurance_level 要素がある。これは準拠するトラストフレームワークとそのレベルを示しており、今回定義した値を設定すると、以下のようになる。

```
"trust_framework": "jp_oidf_ida_2022",
"assurance_level": "jp_oidf_ida_2022_high_unexpired_with_attachments",
```

また、time 要素については、この身元確認プロセスが実施された日時を示している。

evidence 要素には、検証するために必要なエビデンスが含まれている。type 要素はどの種類(document、electronic_record、vouch、utility_bill、electronic_signature)のエビデンスなのかを示しており、種類により要素が異なる。今回は document のみとしているが、これは国内で利用する場合、券面を提示して身元確認することがほとんどであるためである。

attachments 要素が実際の本人確認書類の画像データ（例えば、運転免許証の券面画像など）となり、AAレベルでは必要な要素となる。check_method の値はどのような手法で本人確認書類を検証したかを示す値であり、具体的な値は IDA の Wiki[23] で定義されている。evidence 要素の time 要素は本人確認書類等自体が検証された日時を示し、前述した time 要素とは異なる。

document_details 要素は、証跡となる本人確認書類自体の詳細情報を示す要素である。AAレベルとAレベルでは本人確認書類の有効期限に言及するため、date_of_expiry 要素が必須となる。

ここまでの evidence 要素を JSON で表現したものが以下となる。

```
"evidence": [
        {
          "attachments":{
              "desc":"drivers_license",
              "content_type":"image/png",
              "content":"..."
          },
          "type": "document",
          "check_details": {
            "check_method": "vpip"
          },
          "time": "2021-04-09T14:12Z",
          "document_details": {
            "type": "jp_drivers_licenses",
            "date_of_issuance": "2021-01-01",
            "date_of_expiry": "2030-12-31"
          }
```

[23] https://bitbucket.org/openid/ekyc-ida/wiki/identifiers

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

claims 要素は verification 要素で検証された身元確認済みの属性情報が記載される。構造は verifiation 要素と比較すると単純で属性情報が同階層で記載されるだけである。

一方で課題となったのはどの属性情報の返却を必須とするかである。IDA では、従来の OpenID Connect で定義されている claim に加え、ユーザーの出生地を表す place_of_birth や国籍を表す nationalities などの claim が追加で定義されている。

今回は、身元確認を行った結果の属性情報として、本人特定事項でよく利用される氏名、生年月日、住所を各レベル（Dレベルを除く）で必須属性情報とした。また、氏名と住所はフォーマットが様々であり、事業者によって保有の仕方が異なっていることが想像される。例えば、名前であれば、姓と名が別カラムのケース、姓と名が同一カラムで間に半角スペース・全角スペースが入っているケース、入っていないケースといったバリエーションがある。また、外国人であればミドルネームも存在する。住所はさらにバリエーションがあり、郵便番号、国名、都道府県、市町村、番地、通り、マンション名などの様々なカラムの組み合わせが考えられる。

一方で、仕様に目を向けてみると、OpenID Connect に定義されているフォーマットでも、名前と姓と名、旧姓やミドルネーム、さらには敬称や通称など、様々なフォーマットがある。住所に関しても細かくカラムが分かれている。

これらの課題を整理して標準化を行うことは現実的ではないため、汎用性を重視する形で、住所に関しては address 要素の formatted 要素に、名前に関しては name 要素で、それぞれデータフォーマットに関する細かい定義は行わず返却するよう整理した。

claims 要素の表現は以下のような形となる。

```
"claims": {
     "name": "日本　太郎",
     "birthdate": "1976-03-11",
     "address": {
       "formatted":"東京都港区○○ 1-1-1"
     }
   }
```

また、Dレベルで定義した claim はCレベル同様、ある程度の身元確認を実施されていて、年齢確認だけを行いたいニーズに対応する形で定義しており、18歳以上かどうかだけを確認するものである。

最終的に整理した各レベルにおける必須 claim の詳細は別紙1を参照してほしいが、例として最低限必要なAAレベルの verified_claims 要素は次のように表現できる。なお、

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

データ最小化の観点から、必須としているもの以外の claim は返却しないほうが望ましい。

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida_2022",
      "assurance_level":
"jp_oidf_ida_2022_high_unexpired_with_attachments",
      "time": "2021-05-11T14:29Z",
      "evidence": [
        {
          "attachments":{
              "desc":"drivers_license",
              "content_type":"image/png",
              "content":"..."
          },
          "type": "document",
          "check_details": {
            "check_method": "vpip"
          },
          "time": "2021-04-09T14:12Z",
          "document_details": {
            "type": "jp_drivers_licenses",
            "date_of_issuance": "2021-01-01",
            "date_of_expiry": "2030-12-31"
          }
        }
      ]
    },
    "claims": {
      "name": "日本　太郎",
      "birthdate": "1976-03-11",
      "address": {
        "formatted":"東京都港区○○ 1-1-1"
      }
    }
  }
}
```

このようにして各レベルの verified_claims 要素を定義したことで、必要最低限の身元確認情報を Scope で表現することができ、IDA の利便性を高めることができると考える。参考までに各レベルの verified_claims 要素の JSON サンプルは Appendix に記載した。

9. まとめ

「理想の KYC、次世代 KYC」というテーマで継続して議論していく中で、Phase2 で整理した要件と理想の KYC モデルに関して、「ルール」と「ツール」に分けて改めて検討してきた。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

「ルール」に関しては、身元確認を行いたい事業者のモチベーションと理想の KYC から始めた検討の結果として、身元確認に関わる運用上の要件や契約上の取り決めの観点をある程度明確化できたと考えられる。

現行の国内法では、犯収法や携帯電話不正利用防止法の要件を満たす本人確認サービスは提供できない状況ではあるが、経産省の「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」で中間強度の身元確認手法のあり方として提言されているように、事業者としては、法令による定めが無くても、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み情報を取得したいというニーズも確実に存在する。

「ツール」に関しては、検討した結果、本人確認事業者からの属性情報の提供方法は、IDA を始めとした標準仕様を利用することで技術的な要件を満たすことがわかった。IDA の仕様は EU 圏での eIDAS 準拠での利用も想定されたものであり、多様な表現が可能であることから、IDA をベースに検討していくことが望ましいといえる。他方、理想の KYC モデルで示した多段構成となる際にはステークホルダーが多く、システム構成が複雑になることが見えてきた。特に、複数の CP から属性情報を集めるユースケースにおいては、現在の IDA 仕様だけでは考慮しきれていない点も確認できた。

以上から、KYC WG では、IDA を用いた複数のステークホルダーが絡む複雑なシステム構成を検討するよりも先に、IDA の国内向けミニマム仕様として、RP と IDP のみのシンプルな構成で身元確認済情報を提供する手段を検討することとした。今後 IDA の普及の過程でステークホルダーが増えたとしても受け入れられるのではないかと考えたからである。

国内向け仕様は身元確認済み情報のテンプレートを Scope で定義し、UserInfo Endpoint から返却される身元確認済み情報以外は、既存の OpenID Connect から大きく変更しない形の仕様を提案している。このように OIDC と同じ流れで、また身元確認済み情報のプリセットとしての Scope を定義したことで、サービス提供事業者、本人確認情報の提供事業者の双方にとって利用しやすい仕様にしていくことができるのではないかと考えた。

本レポートで記載してきたように、利用のしやすさも含めての理想の KYC モデルであり、その点、国内向けの IDA 仕様という発想で方向性を定められたことは有意義だったと考える。ただし、方向性は定まったものの、まだ課題も多々残っているところでもある。

しかし、身元確認済みの属性情報を持つ事業者の新規ビジネスを広げること、現状身元確認を行っていない事業者が安価で手軽に身元確認を行う上で有用であるため、理想の KYC モデルと国内向けの IDA の仕様という両面で継続して議論していくこととしたい。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

10. Appendix

10.1. 各レベルごとの verified_claims サンプル

- AAレベルの verified_claims サンプル

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida_2022",
      "assurance_level":
"jp_oidf_ida_2022_high_unexpired_with_attachments",
      "time": "2021-05-11T14:29Z",
      "evidence": [
        {
          "attachments":{
              "desc":"drivers_license",
              "content_type":"image/png",
              "content":"..."
          },
          "type": "document",
          "check_details": {
            "check_method": "vpip"
          },
          "time": "2021-04-09T14:12Z",
          "document_details": {
            "type": "jp_drivers_licenses",
            "date_of_issuance": "2021-01-01",
            "date_of_expiry": "2030-12-31"
          }
        }
      ]
    },
    "claims": {
      "name": "日本　太郎",
      "birthdate": "1976-03-11",
      "address": {
        "formatted":"東京都港区oo 1-1-1"
      }
    }
  }
}
```

- Aレベルの verified_claims サンプル

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida_2022",
      "assurance_level": "jp_oidf_ida_2022_high_unexpired",
      "time": "2021-05-11T14:29Z",
      "evidence": [
```

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

```
        {
          "type": "document",
          "check_details": {
            "check_method": "vpip"
          },
          "time": "2021-04-09T14:12Z",
          "document_details": {
            "type": "jp_drivers_licenses",
            "date_of_issuance": "2021-01-01",
            "date_of_expiry": "2030-12-31"
          }
        }
      ]
    },
    "claims": {
      "name": "日本　太郎",
      "birthdate": "1976-03-11",
      "address": {
        "formatted":"東京都港区oo 1-1-1"
      }
    }
  }
}
```

- Bレベルの verified_claims サンプル

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida_2022",
      "assurance_level": "jp_oidf_ida_2022_high",
      "time": "2021-05-11T14:29Z",
      "evidence": [
        {
          "type": "document",
          "check_details": {
            "check_method": "vpip"
          },
          "time": "2021-04-09T14:12Z",
          "document_details": {
            "type": "jp_drivers_licenses"
          }
        }
      ]
    },
    "claims": {
      "name": "日本　太郎",
      "birthdate": "1976-03-11",
      "address": {
        "formatted":"東京都港区oo 1-1-1"
      }
    }
  }
}
```

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

- Cレベルの verified_claims サンプル

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida_2022",
      "assurance_level": "jp_oidf_ida_2022_medimum",
      "time": "2021-05-11T14:29Z",
    },
    "claims": {
      "name": "日本　太郎",
      "birthdate": "1976-03-11",
      "address": {
        "formatted":"東京都港区oo 1-1-1"
      }
    }
  }
}
```

- Dレベルの verified_claims サンプル

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "jp_oidf_ida_2022",
      "assurance_level": "jp_oidf_ida_2022_medimum_anonymous",
      "time": "2021-05-11T14:29Z",
    },
    "claims": {
      "::age_18_or_over": true[24]
    }
  }
}
```

[24] “::age_18_or_over” と、冒頭にコロンを2つ付与しているのは、IDP で定義した派生クレームを表す。OpenID Connect Advanced Syntax for Claims (ASC) 仕様として、現在検討されている。
https://bitbucket.org/openid/ekyc-ida/src/master/openid-advanced-syntax-for-claims.md

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

11. 用語一覧

本書で用いた用語について解説する。

用語	意味/正式名称
KYC	顧客確認、Know Your Customer の略称。 本書ではお客様を知るための行為を総称して KYC と定義する
本人確認	本人確認は「身元確認」と「当人認証」の組み合わせによって構成される。
身元確認	信頼できる機関が発行した本人確認書類にて登録する氏名・住所・生年月日などの属性情報が正しいことを確かめること（真正性確認を含む） Identity Proofing とも呼称する。
当人認証	利用者がその当人が作業していることを認証要素（記憶・所持・生体）により確かめること
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。
本人確認書類	本人を確認するために公的機関から発行された証明書・書類の総称。 運転免許証、日本国パスポート、マイナンバーカード、住民票、健康保険証、在留カードなど
本人特定事項	本人確認書類の属性情報（氏名、生年月日、住所、有効期限、顔写真など）から本人と特定するための情報を指す。法律によって確認する情報が異なるケースがある。
身元確認手法	本人特定事項の確認方法のことを指します。例としては、犯収法施行規則第6条第1項第1号や、携帯電話不正利用防止法第3条第1項、電子署名法施行規則第5条などに記載されている確認方法などがあげられる。
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[25] ・犯罪による収益の移転防止に関する法律施行令[26] ・犯罪による収益の移転防止に関する法律施行規則[27] 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[28]

[25] https://elaws.e-gov.go.jp/document?lawid=419AC0000000022
[26] https://elaws.e-gov.go.jp/document?lawid=420CO0000000020
[27] https://elaws.e-gov.go.jp/document?lawid=420M60000f5a001
[28] https://elaws.e-gov.go.jp/document?lawid=417AC1000000031

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

	・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[29] 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。
デジタル本人確認	電子的＝オンラインでお客様の本人確認をする行為を指す。 本レポートでは、API 連携によって身元確認済み情報の提供（依拠）による手法を主として指している。 一般的には容貌の撮影などを用いた手法（eKYC と呼ばれることが多い）も含む。
ID 連携	認証連携と呼ばれることもある。SAML や OpenID Connect により実現される RP と IDP/OP の間での ID 情報の連携（フェデレーション）を指す
KYC Provider	身元確認情報を提供するプロバイダ。 身元確認を行った主体を指すことが多いが、本書では主に身元確認済みの属性情報を扱うアグリゲータとして記載している
RP	OpenID Connect における Relying Party
OP	OpenID Provider。OpenID Connect における IDP の呼称
IDP	Identity Provider。アイデンティティ情報を RP へ提供する
Claims Provider	エンティティについてのクレーム（属性情報）を返却する Provider。本レポート上ではユーザの身元確認情報を返却するアクターを示している場合が多い
KP	KYC Provider の略称
CP	Claims Provider の略称
OIDC4IDA, IDA	OpenID Connect for Identity Assurance の略称
FAPI	Financial-Grade API Security Profile の略称
IAL	Identity Assurance Level。当人認証保証レベル。 NIST SP800-63A[30] で定義された身元確認レベル表現方法
AAL	Authentication Assurance Level。身元確認保証レベル NIST SP800-63B[31] で定義された当人認証レベル表現方法
FAL	Federation Assurance Level。 NIST SP800-63C[32] で定義された認証連携レベルの表現方法

[29] https://elaws.e-gov.go.jp/document?lawid=417M60000008167
[30] https://pages.nist.gov/800-63-3/sp800-63a.html
[31] https://pages.nist.gov/800-63-3/sp800-63b.html
[32] https://pages.nist.gov/800-63-3/sp800-63c.html

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

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
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
IDToken	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
AccessToken	OAuth2.0（および OpenID Connect）において、保護されたリソースにアクセスするために使用されるクレデンシャル
Verifiable Credentials	あるエンティティに関する属性情報を、検証可能な方式で表現するデータモデル。W3C で仕様定義されている。

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved

12. 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	小岩井　航介
ソフトバンク株式会社	作田　宗臣

サブワーキンググループメンバ（所属50音順）

所属	氏名
伊藤忠テクノソリューションズ株式会社	寺岡　卓也
エクスジェン・ネットワークス株式会社	李　伝民
NTTテクノクロス株式会社	久米田　博
株式会社NTTドコモ	松岡　洋平
株式会社NTTドコモ	松井　利樹
株式会社TRUSTDOCK	肥後　彰秀
KDDI株式会社	小畑　雅人
Japan Digital Design 株式会社	前川　沙美
株式会社 DataSign	池永　武史
一般財団法人日本情報経済社会推進協会	松下　尚史
日本電気株式会社	宮川　晃一
日本電気株式会社	飯田　憲司
富士通株式会社	西口　由美
富士通株式会社	小倉　孝夫
楽天株式会社	板倉　景子

Copyright (c) 2022 OpenID Foundation Japan All Rights Reserved