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

次世代における**KYC**の方向性に関するレポート

2021年9月
第1.0版

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Phase2で取り上げた3テーマのうち、「理想のKYC、次世代KYC」についての検討をサブワーキンググループとして行い、その結果について取りまとめたレポートとなる。

このテーマでは、2020年1月に当団体にて公開した「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」で示唆した、理想のKYCに関する継続検討と、コロナ渦において変化するKYCというテーマで議論を行った結果として、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、といった点を改めて整理したものである。

ご挨拶

近年のインターネット上での重要取引の増加に伴い、より安全なAPI保護やデジタルアイデンティティの取り扱いへの関心が高まっています。OpenID Foundationでは Financial-grade API（FAPI）やOpenID Connect for Identity Assurance（OIDC4IDA）など、それらの要望に対応する技術標準の策定を進めてきています。OpenIDファウンデーション・ジャパンは日本国内における各種技術標準の普及・啓発活動を通じ、国内の各種事業者が効率的かつ効果的にビジネスを推進できることを目標としています。本ワーキンググループではKYCという文脈において、国際的な技術標準に加えて、国内の金融・通信事業者等の身元確認に関する従来の取り組みを取りまとめることを通じ、現在そして今後のKYCのあり方に関する議論・整理を続けてきました。本レポートは2020年に発表した「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」をさらに深堀する形で、会員企業の有識者の方々により一歩踏み込んだ議論を行い取りまとめたものとなっており、多様な業界において有用なレポートになると確信しています。ぜひ本レポートに目を通していただき、みなさまの事業へご活用いただければ幸いです。

最後に、議論への参加および執筆という形で多大なる貢献をいただいたWG構成員の方々に感謝を申し上げます。

2021年9月
OpenIDファウンデーション・ジャパン
代表理事／KYCワーキンググループ・リーダー　富士榮　尚寛

1. KYCワーキンググループの概要と目的

2019年1月よりOpenIDファウンデーション・ジャパン内のワーキンググループ゜として活動。本人確認・KYCの現状の課題の分析を通じて次世代KYCのあるべき姿、法令やガイドラインとして調整・整備すべき事項、およびOpenID Connect等のID連携標準が具備すべき機能の洗い出し・検討を行い、社会実装へつなげていくためのきっかけを作ることを目的として活動している。

2. 次世代KYCの検討

先にも述べたように、KYCワーキンググループでは「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」[1]において、KYCの現状について整理を改めて行うとともに、理想のKYCとはどういった要素を満たせるものか、いくつかの観点ごとに整理した。具体的な内容は上記レポートを参照してほしいが、観点ごとに整理した内容をまとめたものが理想のKYCのモデルとなりうるのではないか、という仮定を置いた。
ここでは、本人確認を行う主体と本人確認を行った結果を利用してサービスを提供する主体が明確に異なる場合、さらには両社の間に入ってアグリゲートを行うような主体が存在することが示唆されている。

表3-2. 理想の本人確認（KYC）に関する観点

	観点	課題	目指すべき姿
1	制度面	業界や法制度において本人確認に関する法制度ややり方がバラバラ	金融業界だけでなく、様々な業界において統一的な本人確認のガイドラインが制定されている
2	認知度	本人確認手法やKYC Providerについて認知度が低い	本人確認手法やKYC Providerに対してエンドユーザに対する認知・理解ができている
3	ユーザカバレッジ	日本国内において1社で日本の人口をカバーできるKYC Providerが存在しない。	複数の本人確認手法や適切なKYC Providerを提供し、日本の人口をカバーする
4	ユーザ体験（UI/UX）	エンドユーザのアクセス環境によって、提供される本人確認手法やKYC Providerが制限される	エンドユーザのアクセス環境（スマートフォン、パソコン）や利用状況（所持している本人確認書類、銀行口座、携帯電話など）により適切な本人確認手法を提供できる
5	セキュリティ	KYC Providerの当人認証のセキュリティによっては別人の本人確認がされてしまう 。	KYC Providerの当人確認（認証）の基準の標準化が必要
6	コスト	犯収法においては、最終的に人手での確認が必要なため、コストがかかる。	AI等の技術を利用し、本人確認のプロセスを完全に自動化することで、コストを下げる

図1-1 理想の本人確認に関する観点の抜粋

[1] https://www.openid.or.jp/news/oidfj_kycwg_report_20200123.pdf
OpenIDファウンデーション・ジャパン KYCワーキンググループ「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」

また、同時期に経済産業省が令和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」[2]においても、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、金融機関および通信キャリア等の身元確認APIの活用可能性について検討が進められてきた。ここでも本人確認の手法として通信キャリアや金融機関などの身元確認APIを活用することで、本人確認を別の主体に委任する形の方式が示されている。

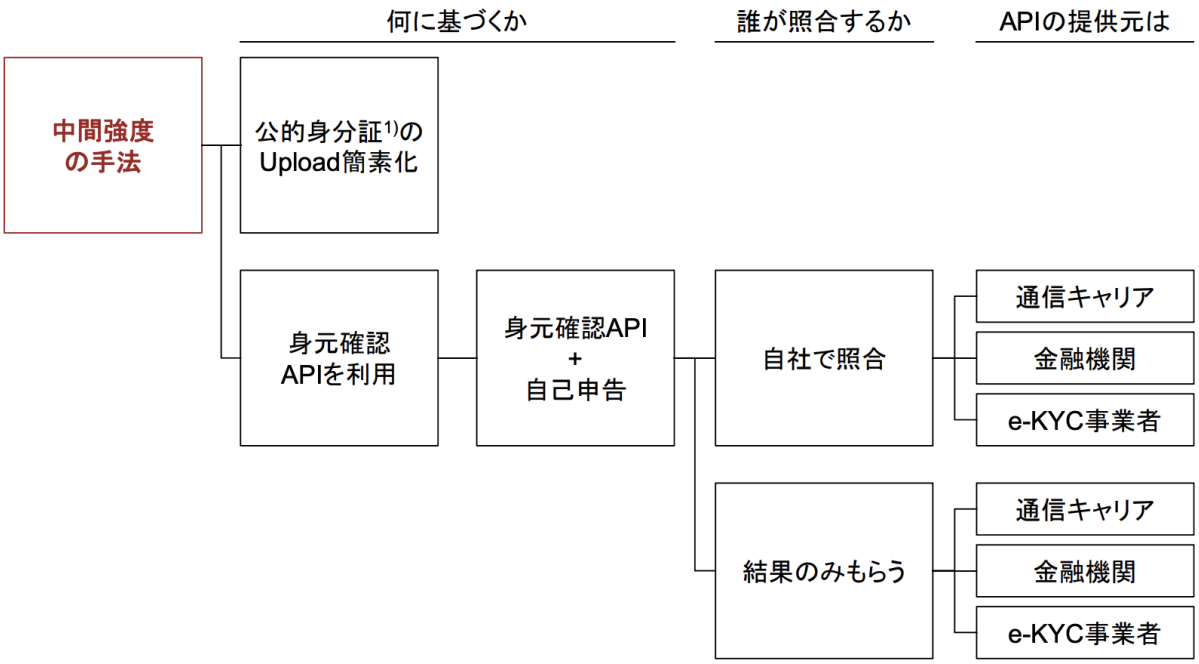

図1-2 中間強度の身元保証手法の整理資料抜粋

これまでの話の中で、KYC業務を行った主体とサービスを提供する主体が異なるようなユースケースが共通項として見えてくることから、将来的にこのような形か、あるいは近しいKYCのやり方が実現されうるのではないかと想定し、ベースとして検討を行った。

そこで利用できることが想定されるのが、API経由で本人確認済みの属性情報を連携することが可能な「OpenID Connect for Identity Assurance」（OIDC4IDA、あるいは単にIDA）とその関連仕様である。この仕様に関しては、前述した「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」でも触れられているが、すでに精度の高い顧客情報を持っている事業者から本人確認済み属性情報を提供して貰うことで、ユーザーと事業者の双方にとっての煩雑なプロセスを省略できることが期待される。

[2] https://www.meti.go.jp/press/2020/04/20200417002/20200417002-2.pdf
経済産業省「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）」

また、別の手法として自己主権型IDを用いる手段もある。GAFAを初めとするIDPがIDを発行してサービスを利用させる中央集権型のIDであることに対して、個人がIDを自ら発行し、利用したいサービスに提示して利用する自己主権型のIDである。 このような自己主権型のIDを実現できる仕様としてW3Cで策定されているのがDID[3](Decentralized Identifiers)とVerifiable Credentials[4]である。ユーザが自身で発行したID(DID)に対して必要な資格情報を証明したクレデンシャル(Vefiriable Credential)を発行してもらい、そのクレデンシャルを利用したいサービスに提示して、サービスの提供を受けるという形である。例えば、大学の在学証明のクレデンシャルをユーザ自らのDIDに紐づける形で大学(Issuer)から発行してもらい、そのクレデンシャルをユーザが在学証明を求められるサービス(Verifier)に対して提示する。こうすることで自身が大学に所属していることをサービスに対して証明することができ、学割などのサービスを受けることが可能になる。

KYCのケースとしては、本人確認済の事業者(Issuer)が発行した本人確認済み情報を含むクレデンシャルをユーザを介してサービス(Verifier)に提示することで、本人確認済みの情報を提供する手法も考えられる。本人確認済みの事業者とサービスを提供する事業者が異なるユースケースという意味では、実現できることはOpenID Connect for Identity Assuranceを活用する場合と近しいものになると考えられる。本WGでは主にOpenID Connect for Identity Assuranceをベースとして検討を実施しているが、DIDに関しても継続的に議論を実施していきたい。

[3] https://www.w3.org/TR/did-core/
[4] https://www.w3.org/TR/vc-data-model/

3. OpenID Connect for Identity Assuranceと関連技術

本章では、次世代KYCの検討に際して利用した仕様群について紹介する。

3-1. OpenID Connect for Identity Assurance

OpenID Connect for Identity Assurance[5](OIDC4IDA, IDA)は、OpenID Connect(OIDC)の拡張仕様であり、API経由でOpenID Provider(OP)からRelying Party(RP)に提供される属性情報に根拠情報を追加するものである。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本人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OpenID Connect for Identity Assurance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（evidence）を含めてRPに返却することが可能となっている。この仕様を、精度の高い顧客情報を持っている事業者が活用することで、RPに対して根拠を含めた属性情報が提供できることになる。

次の図はOpenID Connect for Identity Assuranceを利用したUserInfo Responseの一部の例である。返却する属性情報の根拠情報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。

[5] https://openid.net/specs/openid-connect-4-identity-assurance-1_0-ID2.html


```
{
  "verified_claims":{
    "verification":{
      "trust_framework":"de_aml",
      "time":"2012-04-23T18:25Z",
      "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
      "evidence":[
        {
          "type":"id_document",
          "method":"pipp",
          "time": "2012-04-22T11:30Z",
          "document":{
            "type":"idcard",
            "issuer":{
              "name":"Stadt Augsburg",
              "country":"DE"
            },
            "number":"53554554",
            "date_of_issuance":"2010-03-23",
            "date_of_expiry":"2020-03-22"
          }
        }
      ]
    },
    "claims":{
      "given_name":"Max",
      "family_name":"Meier",
      "birthdate":"1956-01-28",
      "place_of_birth":{
        "country":"DE",
        "locality":"Musterstadt"
      },
      "nationalities":[
        "DE"
      ],
      "address":{
        "locality":"Maxstadt",
        "postal_code":"12344",
        "country":"DE",
        "street_address":"An der Sandd&#252;ne 22"
      }
    }
  }
}
```

図3-1 IDAの属性情報表現の例

また以下は、「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」においても記載されている内容であり、一部抜粋して紹介する。

OpenID Connectを利用することでサービス提供者は非常に簡単に顧客情報を取得できるようになる。しかし現状のOpenID Connectの仕様では、機能的な不足が否めない。例えば、UserInfoエンドポイントから住所を取得するケースにおいて、ただ住所が取れるだけでなく、取得日時やどのような証明情報から取得したのかなど、付帯的な情報も欲しいケースが当然考えられる。将来的な依拠が緩和された後の世界観を考えると、犯罪収益移転防止法（以下、犯収法）やeIDAS規制などにも対応できる必要があるだろう。

そのような厳格な本人確認性にも対応できる仕様として、新たに策定が進んでいるのがOpenID Connect for Identity Assuranceである。これは、マネーロンダリング防止法や電気通信法、テロ対策法、eIDASなどのような法律や規則を満たすことを目的に策定が進んでいる仕様で、現時点（2021年9月現在）の犯収法では他事業者による本人確認結果に依拠することは銀行依拠を除いて出来ないものの、他の法的要件や民間利用においての利用は十分に可能なものになると考えられる。

具体的には、OpenID Connect for Identity Assurance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予定だ。

- 本人確認プロセスに関する情報とその取得方法
- 本人確認済み情報の利用目的の通知と同意取得方法
- UserInfo Response として必要な属性の指定と必須属性の指定

これらの内容によって、RPはユーザーやOPに対して ①サービスが本人確認しなければならない属性の明示的な要求 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り、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本人確認を行ったかの取得が行えるようになる見込みだ。

3-2. 分散・集約クレーム

OpenID Connectの文脈では、属性情報を提供する主体がOPではないこともありうる。これはOpenID Connectのベースとなった認可プロトコルの OAuth2.0でも認可サーバとリソースサーバという形で分けて整理されている例が分かりやすい。

分散クレーム(aggregated claims)と集約クレーム(distributed claims)は仕様の名前ではなく、OpenID Connect仕様に記載されているClaimsの表現形式[6]である。いずれもOP以外のClaimsProvider（CP）から属性情報を返却する場合に用いられる表現形式となっている。

分散クレームは、属性情報を返却するCPへの参照情報をOPからRPに返却するための表現形式である。

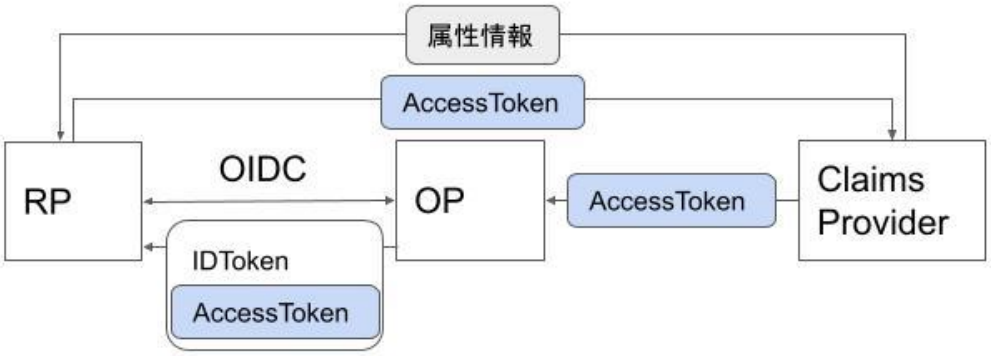

図3-2 分散クレーム図

上記はOPからRPに認証結果（IDToken）を返却する際に、CPへAPIアクセスするためのAccessTokenを含む手法である。RPはこのAccessTokenを使ってCPから属性情報を取得することが可能となる。また、別のやり方として、OPが発行したAccessTokenを使って、OPのUserinfo EndpointからCPにアクセスするための（CPがRPに対して提供する）AccessTokenを取得することも可能である。

一方で、集約クレームは、CPの属性情報をOPが集約してRPに返却するための表現形式である。

[6] https://openid.net/specs/openid-connect-core-1_0.html#AggregatedDistributedClaims

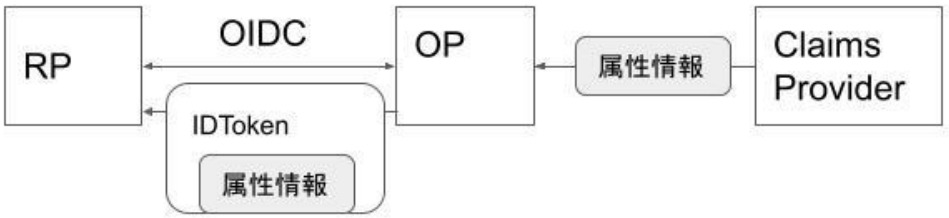

図3-3 集約クレーム図

分散クレームとは違い、RPがCPに直接アクセスすることはなく、OPがまとめて属性情報を返却する形となる。複数のCPからも集約して返却できるため、CPが複数の場合は集約クレームが有効に活用できる例といえる。

共通しているのは、認証主体のOPではなくCPから属性情報を取得するための表現形式であることであり、認証結果取得と属性情報取得を別々に行うことはOpenID Connect for Identity Assuranceと合わせて利用することが可能と想像できる。

3-3. Financial-grade API (FAPI)

FAPI [7](Financial-grade API) とは、OpenID Foundation FAPI WG[8]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、その用途の広さと自由度の高さとの引き換えに、設定の仕方次第で、セキュリティ上堅牢にも脆弱にもなり得る弱点が存在している。

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日に最終版が公開された。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。

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の利用を検討されるべきである。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 Connect

[7] https://openid.net/2021/03/12/fapi-1-0-part-1-and-part-2-are-now-final-specifications/
[8] https://openid.net/wg/fapi/

認定(Conformance Test)で必要とされる認可タイプの一部がFAPI認定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。

参考文献

https://hack.nikkei.com/blog/fapi_and_conformance_test/
https://qiita.com/TakahikoKawasaki/items/83c47c9830097dba2744

4.　理想のKYCモデルとユースケース

前述のとおり、KYC業務を行った主体とサービスを提供する主体が異なるユースケースを想定した理想のKYCの検討を行うにあたって、前章で説明したOpenID Connect for Identity Assuranceや関連する仕様（特に分散クレームと集約クレーム）をベースとしてモデルの検討を実施した。本章では検討した結果として本人確認を依拠するモデルを3つ紹介する。

4-1. 本人確認を依拠するモデル

本人確認主体とサービス提供主体が異なる場合のモデルは、OIDC4IDAを利用することで比較的分かりやすく実現できると考えられる。OIDC4IDAでは本人確認結果を表現することができるため、本人確認を行った主体がOpenID Provider（OP）、サービス提供主体がRelying Party（RP）として、本人確認を依拠することが可能となる。

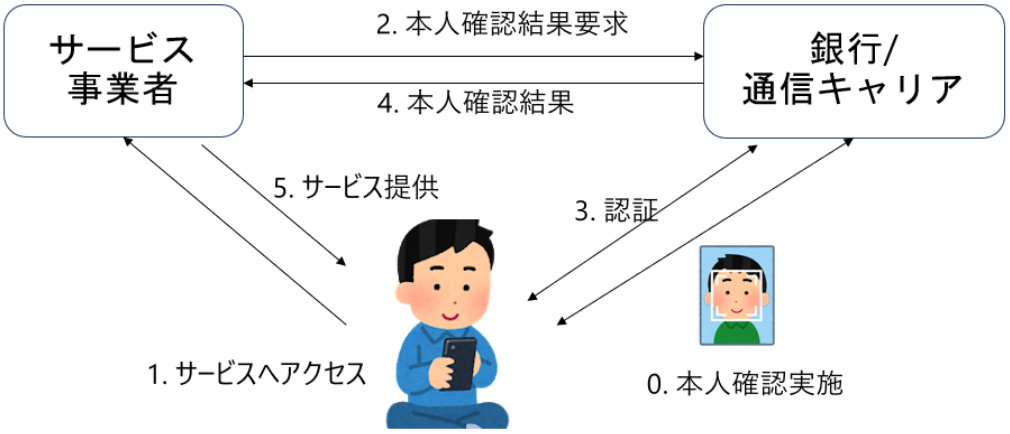

図4-1 本人確認依拠モデル

上図の例では、銀行や通信キャリアがOPとなりサービス事業者（RP）に対して本人確認結果を通知する。このモデルを実現すると、RP側は本人確認業務に関するコストを抑えることができ、また必要な本人確認属性情報だけを取得することが可能と考えられるため、不必要な情報を持つ必要がないというメリットが考えられる。

4-2. アグリゲータが存在するモデル

上のモデルのように、サービス提供主体(RP)と、KYC情報提供主体(OP)が存在するとした場合、OPが複数存在しうることがわかる。OPは自身で行った本人確認結果を本人の同意の元にRPに対して提供することになるが、OPが各々実施した「本人確認」は、各々が必要とする本人確認であり、必ずしも全く同じ本人確認ではない。例えば、OPが携帯電話の契約を伴う本人確認を行う事業者だったとすれば、携帯電話不正利用防止法に則った本人確認を行っていることになる。そのため、RPは自身がどういった本人確認結果を取得するべきか判断してOPから本人確認結果を取得しなければならない。OPがどういった本人確認を行っており、どういった項目を取得できるのかを判断して接続先OPを選定するのはRPにとっては負担が大きく、また、ユーザから見ても特定の本人確認手段だけでなく、複数の本人確認手段が提供されることが好ましい。こういった観点から、本人確認結果の流通をコントロールするアグリゲータが存在しうる想定のモデルを検討した。

下図は前節で紹介したモデルにKYC Provider（アグリゲータ）を追加したモデルである。このモデルの場合、銀行や通信キャリアといったKYC情報提供主体はClaimsProvider（CP）となり、ユーザの認証を行うOPの役割はKYC Providerが行うことになると考えられる。このような構成にすることで、サービス事業者は画一的なIFで本人確認情報を要求することができる。また、要求に応じたエビデンスを本人確認済みの事業者から取得する際に、適切な情報を適切な事業者から取得できるよう、アグリゲータがコントロールすることが可能となる。

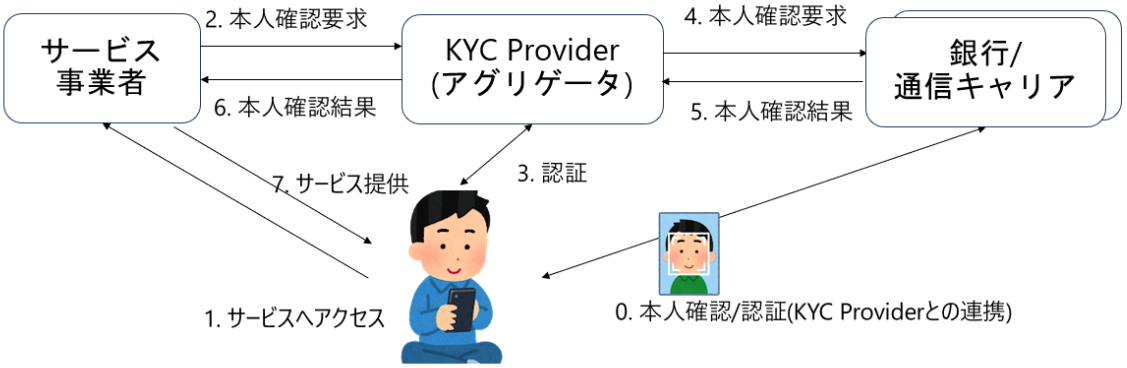

図4-2 アグリゲータを含む本人確認依拠モデル

このモデルをコンポーネントで分割すると次のようになる。

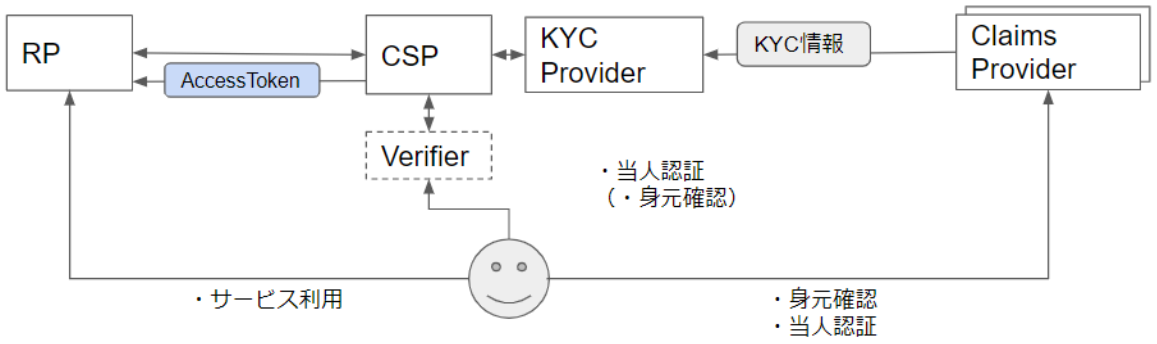

図4-3 本人確認依拠モデルコンポーネント図

表4-1 本人確認依拠モデルの登場人物

アクター	説明	備考
KYC Provider	KYC情報を仲介するProvider。 TrustAnchorのKYC情報を仲介し、RPに対して提供するアグリゲータ。 自身がTrustAnchorとなることもある。	
Claims Provider	属性情報を提供する主体。 ユーザの身元確認（本人確認）を実施し、本人確認情報を保持している。	銀行や通信キャリアなどの本人確認を行っている事業者を想定
RP	Relying Party。 本人確認結果を利用して、ユーザに対してサービス提供を行う主体。	サービス提供事業者
CSP	Credential Service Provider。 ユーザのクレデンシャルを発行する主体。 KYC Providerと連動してKYC情報を提供するためのクレデンシャルをRPに対して発行する。	CSP+VerifierでOPとして振る舞う
Verifier	ユーザ認証を行う主体。 ユーザから提示されたAuthenticatorを検証する。	

上記のモデルを想定したとき、3-2で紹介したOpenID Connectの仕組みを踏まえて考えると2つの方法が考えられる。

4-2-1. 分散クレームを用いたモデル

一つ目の方法は分散クレームを用いる方法である。分散クレームは先に紹介したように、属性情報を返却するCPへの参照情報をOPからRPに返却するための表現形式である。

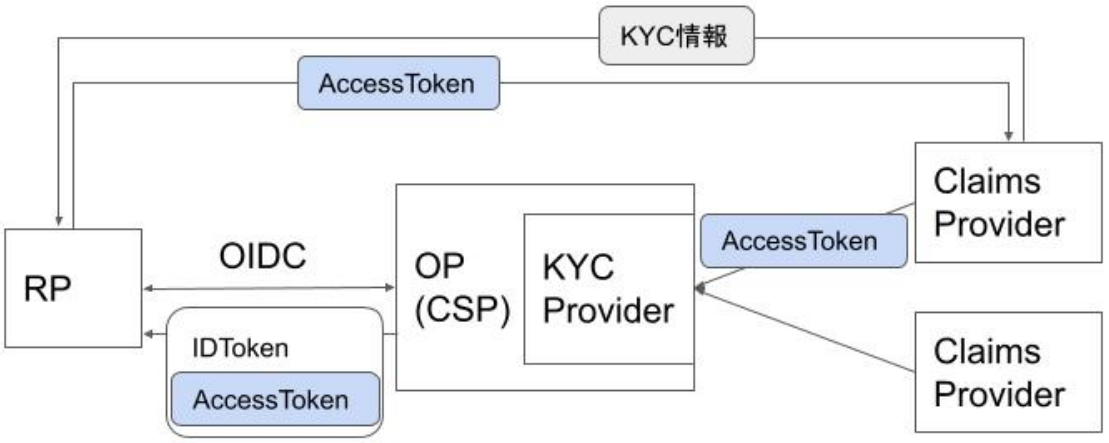

図4-4 分散クレームを利用した本人確認依拠モデルのコンポーネント図

具体的には、OpenID ConnectでOPからRPに返却されるIDTokenにCPにアクセスするためのAccessToken[9]を埋め込んで返却する。RPは取得したAccessTokenを用いて、直接CPのAPIにアクセスし、IDAに準拠したKYC情報を取得することができる。

このように分散クレームを用いることで、OPを経由することなくKYC情報を提供することが可能になる。一方で、AccessTokenはOPを経由して提供することになることから、特定のRPからのみアクセスできるようAccessTokenを制限するなど、AccessTokenの扱いには注意が必要である。

4-2-2. 集約クレームを用いたモデル

もう一つの方法は集約クレームを用いる方法である。集約クレームはCPの属性情報をOPが集約してRPに返却するための表現形式である。

[9] OPにアクセスするためのAccessTokenは別に存在する（図中では表現していない）

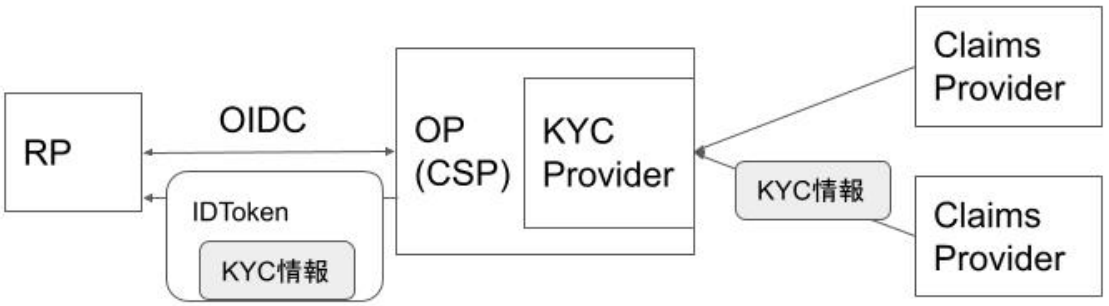

図4-5 集約クレームを利用した本人確認依拠モデルのコンポーネント図

こちらのユースケースは、CPから取得したKYC情報をOPが発行するIDTokenに埋め込んでRPに返却するフローとなる。

集約クレームではKYC情報がOP(KYC Provider)を経由してRPに渡されることになる。そのため、分散クレームと違いRPはOPから必要なすべてのKYC情報を取得することができ、APIアクセスの手間を省くことが可能となる。一方で、KYC情報が必ずOPを経由することになる。

5.　現実的な社会実装ケースの検討

上記3つのユースケースモデルについて、いずれの場合も銀行およびキャリアへの依拠モデルに近い事になるが、実際に運用される様々な社会実装ケースをこちらに当てはめようとすると、それだけでは様々な課題がある。 例えば実際のユースケースにおいては、RPとKYC Providerは業務委託関係にあることが多いため、契約書ベースで考えるとRPとKYC Providerは一心同体の存在であると考えて良いだろう。また、図の右側にある銀行およびキャリアからKYC Providerの連携と、KYC ProviderからRPへの連携の2つの時系列は、必ずしも一続きではない場合が多いと言える。

さらに、例えば犯罪収益移転防止法 第六条 ト(1)の要件を考えた場合、銀行およびキャリアから連携された基本3情報をRPから来る本人確認情報と突合確認（以下、マッチング）をするところまでが、一般的にはKYC Providerのサービス提供範囲となる。つまり、このサービス提供範囲についてはKYC Providerが独自で決めることができるので、どの社会実装ケースにも対応する一般化したものを作るのに適しているとは言えない。

よってここからは、それぞれのモデルが日本国内においてワークする社会実装ケースを逆引きする形で紹介する。

例えば海外の事例として、マッチング結果共有のサービスを2つ使えば本人確認が完了するというケースがある。この場合、RPが申請情報をKYC Providerに投げ、それに対してKYC Providerが何かしらの方法でマッチング結果を返すという流れとなる。もしくは、OpenID Connectを通じてユーザー情報連携のみを行い、RP側で申請情報とマッチングするという流れも想定される。このユースケースモデルは、犯収法をはじめとする既存の規制業種では定義されていないので、現状では利用することができないのだが、出会い系サイト規制法（正式名称：インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律）の識別符号付与業務のみは例外的に可能となっている。同法では、年齢確認をユーザーがサービスを利用する度に行うか、もしくは年齢確認が完了したユーザーにIDとパスワードを付与して、ユーザーがサービスを利用する際にこの識別符号を入力してログインすることが義務付けられている。このIDとパスワードのことを「識別符号」としており、ユーザビリティの観点から前者で設計されているサービスは実質的におらず、ほぼ全てのインターネット異性紹介事業は、後者の識別符号によるログイン確認で設計されている。よってユーザー情報のみ連携する場合においては、現状では、出会い系サイト規制法に準じた「年齢確認」義務が発生するインターネット異性紹介事業における活用が期待される。

また、OpenID Connect for Identity Assuranceで本人確認結果を連携して受け入れる流れについて考えた場合、先ほどRPとKYC Providerは業務委託関係にあるとお伝えしたが、厳密には「請負」の関係になると考えた方が実態に即している。この場合、犯収法ベースの法律においてはRPは直接KYCをしなければならない立て付けとなるが、KYC Providerとしては正当な本人確認プロセス・認証手段・連携方法を根拠として結果を受け入れ、直接KYCをしなくても良いようにする必要がある。つまり、既存の規制法をこれに準じて改正することが、実装における根本的な課題となる。

一方で、例えばこれが厳格な本人確認用途ではなく、法定要件ではない任意の年齢確認等を実施するサービスの場合は、IDTokenでKYC情報を返却する方法そのままの仕様で実装することが期待できる。実際、OpenID Foundation内のeKYC & Identity Assurance WGにおいても、「該当者の年齢が○○歳より上か下か」という議論がなされている状況だ。この場合、RPはユーザーにいちいち申請情報の記入をさせないことになるので、RPに記載した申請情報とKYC結果として送られるユーザー情報の突合確認をする必要がなく、PRとユーザーの双方にとってUX改善の大きなチャンスでもあると言えるだろう。

6.　市中における実際のKYC

前章で述べた通り、現状で犯罪収益移転防止法などの業法を前提に考えた場合、理想のKYCモデルは社会実装にそのまま適するものではない。

一方で、先に述べたように将来的にKYCを依拠するようなユースケースが予見されていることもあり、その間にはギャップが存在する。KYC情報を利用したい事業者は何を目的としてKYCを行おうとしているのか、また、その目的のためにハードルとなることは何か。そういった内容を再整理することで見えてくる、社会実装や業法にとらわれない本来満たすべきKYCの要件について改めて議論を行った。

KYCの要件が見えてくることで、その要件は市中の制度や技術で補うことができるのか、それとも全く新しい技術や考え方が必要なのかを整理することにつながり、KYCに置ける現在地と将来どうなっていくべきかが見えてくると考えられる。

6-1. サービス事業者におけるKYCの目的

本来満たすべきKYCの要件を抽出するにあたって、市中における現在の依拠のユースケースをモデルケースとして、業法などに囚われずサービス事業者が本人確認を実施したい本来の目的を整理した。ユースケースにおいて、何を目的として本人確認を実施しているのか、本人確認で依拠する場合に必要な情報はどんなものか、適切な依拠先はどこが考えられるのか。これらを整理したのが次の表である。

表6-1 市中の本人確認依拠ユースケースとその目的

	ユースケース	業界・事業者	KYCの目的	依拠する場合に欲しい情報	（理想像）依拠してよいか	適正な依拠先はどこか
1	身分証アップロードの代替	タバコ	未成年への販売防止	年齢が20歳以上であるかどうか	よい	なるべく多くの国民が利用しているサービス
2		インターネット異性紹介業	18歳未満を性犯罪などから保護	年齢が18歳以上であるかどうか	よい	・なるべく多くの国民が利用しているサービス ・年齢の確認ができているサービス
3	アカウント登録	フリマアプリ	・取引相手への信頼感の醸成による取引の活性化	・正当な（偽造されてない）公的身分証かどうか？	一定の条件下では良い	公的な身分証でKYCを実施している機関

			・決済方法によっては反社チェックが必須	・氏名/生年月日/住所/電話番号など		
4		シェアリングエコノミー	・取引相手が実在する人なのか ・取引相手が不正、双方の犯罪の抑止	・サービスによって異なる？ （住所/連絡先/氏名/年齢など）	よい	公的身分証での本人確認を行い、住所情報を定期的に確認している機関（顧客の登録した住所で行うサービスなどでは必要）
5	圧着ハガキの代替	金融機関	新規登録やパスワード再発行時の本人確認用途（＝転送不要郵便で実在する住所を確認） →住所に居住する人にサービスを提供する	その住所に今住んでいるかどうか	住所がリーチできるものであればよい	犯収法に基づいて本人確認を行っている、他の金融機関
6		電気・ガス会社	新規登録やパスワード再発行時の本人確認用途（＝転送不要郵便で実在する住所を確認） サービスの提供場所＝住所	その住所に今住んでいるかどうか	住所がリーチできるものであればよい	住所情報を定期的に確認している事業者
7	電話番号・メールアドレス存在確認の代替	会員登録が必要なサービス	・当人性の精度向上 ・ビジネスリスクの低減（反社チェック、支払い能力保証）	氏名/生年月日/住所など	よい	疎通確認を定期的に行えている事業者
8	2段階認証の代替	金融機関（地銀）	金融機関として適切な確認を行っていることの担保	-	一定の条件下ではよい	IAL・AALが適切な機関
9	コールセンターへの電話での本人確	コールセンターサービス事業者	電話口の顧客が本人かどうかを確認したいので知識認証	氏名/生年月日など	よい	・当人認証が可能な機関 ・（属性情報を必要とするなら）属性情報の真正性を確認している機関

	認					
10	携帯電話契約	携帯キャリア	振り込め詐欺などに携帯電話番号を悪用されることを防止	本人が追跡できる情報	よい	同等の確認を行っている携帯キャリア/銀行など
11	馬券購入	賭博	馬券を購入できる年齢かどうか (ギャンブル可能な分別があるか)	年齢が20歳以上であるかどうか	よい	年齢の確認ができているサービス
12	(身分証アップロードの代替)	レンタカー	・免許の種類、有効期限 ・運転免許証の住所が現住所であるか	・運転免許証の有効性(不正に作成されたものでないか) ・現住所	よい	直近の免許証情報を保持している事業者など
13	研修受講	研修機関	・申請者本人であるか ・受講要件(年齢、職歴など)に適合しているか	年齢、職歴などの受講要件	よい	・資格監督機関 ・求人サービス
14	第三者審査	審査機関	・申請者、申請会社の実在性 ・部外者(コンサルなど)が関与してないか	・申請会社の実在性 ・申請者、担当者が所属しているか	よい	・認証監督機関 ・入札元(国、自治体、民間企業)

事業者が本人確認に求めるものとして、以下のような目的が見えてくる。

- 名前や住所のような代わる値を扱っている場合、適度に最新の情報に更新される情報が取得できる
- 生年月日を保持しており、今現在の年齢を知ることができる
- 情報のベースとなる本人確認書類は何かがわかる(何を担保としているか)
- 資格保有の有無の確認
- 情報にある程度マスクをかけた情報取得(何歳以上など)

6-2. 本人確認における要件

では、6-1で整理した各ユースケースの目的から見えてくる要件とはどういったものがあるのか。図4-2,図4-3で示したIDAをベースとしたKYCモデルを前提に、それぞれのアクター間(サービス事業者＝RP、アグリゲータ＝KYC Provider(KP)、本人確認済事業者＝Claims Provider(CP))で相互に必要になる機能要件を洗い出し、大まかなカテゴリに分類した。

なお、ここでのKPは図4-3で示した、KYC Provider、CSP、Verifierの機能を合わせ持つアクターとする。

表6-2 アクターの要件のカテゴリ

要件	カテゴリ	キーワード
RPがKPに求める要件	IAL	依拠してよいか/ エビデンスの種類
	AAL	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	認証の粒度感
	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	エビデンスの種類
	プライバシー	ユーザ認可
	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	認証の粒度感
	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	認証の粒度感
	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

似通ったカテゴリが多くあるが、RPがKPに求めるものは最終的にCPに求めるものであったり、アクター双方で同様の要求を行っているためである。

全体としては、トラストの議論がある。本人確認情報の流通を行う目的で信頼関係や取得した情報の利用用途など、契約やポリシーにおいてどこまで枠組みとして築いていけばよいのか。信頼の枠組みをどう形成していくのかという議論を行っている。

また、RP, KP, CPと3者が関わってくることから、相互の認証レベルや本人確認レベルをお互いにどう担保していけばよいのかという議論もある。例えば、CPの認証レベルや本人確認プロセスがいくらしっかりしていても、KPの認証レベルが低ければ、全体としてのセキュリティは非常に低レベルになってしまう。そのようにフレームワーク全体として認証や本人確認のレベル感を担保していくか、また、その表現方法をどう揃えていくかなどの整理も必要であると考えられる。

本レポートではカテゴリ分けまでを行ったが、さらに今後も継続議論していき、カテゴリ分けした要件の詳細化、既存の技術でどこまで解決できるのか、今後必要となってくるものは何か、といった点の検討と議論を進めていく予定である。

7. まとめ

ここまで整理してきたように、OpenID Connect for Identity Assuranceを初めとした関連仕様を活用することで、本人確認の将来的な手法の変化にもある程度対応することが可能なのではないかと考えられる。もちろん継続議論の必要はあり、これらの仕様でも対応できないような要件が存在しうる可能性もあるし、本人の依拠という手段が犯罪収益移転防止法や携帯電話不正利用防止法などを初めとした業法でどこまでこのような手法が可能になるのか、といった問題もある。

一方でこれらの仕様があることで可能となる手段も増えることも考えられ、コロナ渦において、eKYC化を加速せざるを得ない状況を踏まえると、本人確認業務とサービス提供を分離していくことが、一つの手段となりうるのではないだろうか。

OpenID Foundation Japanではこれらのプロトコルを念頭に置きつつ、次世代KYCに向けてどういった要素が必要になるのかを詳らかにし、次世代のKYCのあるべき姿に向けた議論を継続していくこととしたい。

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	身元確認、Identity Proofingとも呼称する。 信頼できる機関が発行した本人確認書類を確認すること（真正性確認を含む）
eKYC	eKYCとはelectronic Know Your Customerの略。 本書では、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。 代表的な例としては、平成30年11月の犯収法の改正により、犯収法施行規則第6条第1項第1号に記載をされた本人特定事項の確認方法のうち、郵送不要の新手法にホ・ヘ・トの方法などがある。
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	本人確認情報を提供するプロバイダ。 本人確認を行った主体を指すことが多いが、本書では主にKYC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本人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
IAL	Identity Assurance Level。 NIST SP800-63 で定義された本人確認レベル表現方法
AAL	Authentication Assurance Level。 NIST SP800-63 で定義された認証レベル表現方法
FAL	Federation Assurance Level。 NIST SP800-63 で定義された認証連携レベルの表現方法

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
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

執筆者一覧

執筆メンバ（所属50音順）

所属	氏名
KDDI株式会社	小岩井　航介
ソフトバンク株式会社	作田　宗臣
株式会社TRUSTDOCK	菊池　梓

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
株式会社NTTドコモ	栗山　盛行
株式会社NTTドコモ	松岡　洋平
株式会社オージス総研	金井　敦
株式会社オプティム	菊池　佑
オープンソース・ソリューション・テクノロジ株式会社	今井　啓
KDDI株式会社	小畑　雅人
株式会社ジェーシービー	間下　公照
株式会社DataSign	坂本　一仁
一般財団法人日本情報経済社会推進協会	紅谷　昭光
楽天株式会社	板倉　景子
株式会社Liquid	池田　雄一郎

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