2023 年 12 月８日
日本銀行決済機構局

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第２回会合の議事概要

１．開催要領

（日時）2023 年 11 月 21 日（火）14 時 00 分～16 時 00 分
（形式）対面形式及びＷｅｂ会議形式
（参加者）別紙のとおり

２．プレゼンテーション

株式会社ＮＴＴドコモ、他１社（社名非公表）より、プレゼンテーションが行われ、その後、参加者によるディスカッションが行われた。モデレータは、株式会社三菱ＵＦＪ銀行が担当した。概要は以下のとおり。

（１）既存の資金決済サービスの現状①（ＮＴＴドコモ）

―― 提供している資金決済サービスにおいて、ＫＹＣと当人認証に関連するユーザーアクションや実施状況の整理を行った。プレゼンテーション資料の要旨は別添を参照。

既存の資金決済サービスの現状整理として、ｄ払いにおける身元確認と当人認証に関して、説明を行う。 ｄ払いは、日本国内在住の個人のお客さまを対象として複数の決済機能を提供しており、お客さまがドコモの回線をお持ちであるかどうか、ｄ払いで身元確認をしているかどうかによって利用できる機能に差異を設けている。これらの確認のため、ｄ払いにおいては、エンドポイントデバイスから保有している社内共通の認証基盤と身元確認基盤を経由した上で、ｄ払いのシステムにアクセスをしている。共通基盤における確認の枠組みとして、当社では米国立標準技術研究所（ＮＩＳＴ）が定めたデジタルアイデンティティガイドラインを参考に、ドコモ版デジタルアイデンティティガイドラインとして、ビジネス環境を加味した身元確認保証レベルと当人認証保証レベルを策定している。このような統一のガイドラインをもとに、身元確認、当人認証の機能を社

内で共通化しており、ｄ払いにおいても同ガイドラインに基づき、実施している。

ｄ払いにおける身元確認は、ワ方式（公的個人認証・マイナンバーカードのＩＣチップ読み取り＋暗証番号）、ヘ方式（本人確認書類のＩＣチップ読み取り＋容貌の撮影）、ホ方式（本人確認書類の撮影＋容貌の撮影）を導入しており、それぞれメリットとデメリットが存在する。ワ方式は、マイナンバーカードのＩＣチップを用いるため偽造耐性が高く、本人確認書類および容貌の撮影が不要であること、即時審査が可能であることがメリットとなる。一方、マイナンバーカードの読み取り時には署名用電子証明書暗証番号が必要となり、申込者が記憶しておく必要があることがデメリットの１つとなる。ヘ方式は、マイナンバーカードの暗証番号は用いないが、マイナンバーカードに加え、運転免許証、または在留カードのＩＣチップが読み取り対象となり、利用可能な本人確認書類が増え、かつ申込者の容貌の撮影が必要となる。なお、ヘ方式でも、本人確認書類によってはワ方式同様に暗証番号が必要になる場合がある。ホ方式は、本人確認書類と申込者の容貌の２点を撮影することで申込みができるため、多くの人が対応できる点がメリット。しかし、本人確認書類の厚みを撮影することが難しい点や当該写真の審査は目検で行うことから身元確認の審査に時間がかかること等がデメリットになる。

ｄ払いにおける当人認証は、（ア）アプリログイン時・Ｗｅｂサイトにおける決済時、（イ）アプリやＷｅｂサイトにおけるクレジットカード登録時・決済時、（ウ）金融機関口座の登録時の大きく３パターンのユースケースがある。（ア）の認証時はお客さまのご契約や加盟店さまの取扱う商材により、認証方式を設定している。（イ）の認証時は、ＥＭＶ３－Ｄセキュアを必須としている。（ウ）の認証時は、ｄ払いでの身元確認が済んでいること、ｄ払いの身元確認情報と金融機関の情報が一致していること、金融機関のセキュリティレベルが当社の基準に則っていること、を確認することになる。

身元確認や当人認証は、年々悪意者による攻撃が高度化しており、脅威が高まっている。まずは、身元確認における課題を４点挙げる。１点目は偽造した本人確認書類を使った申込みへの対応、２点目は必要な暗証番号を覚えていないお客さまやＩＣチップを読み取る機能がないスマートフォンをお持ちのお客さまへの対応、３点目は審査において、本人確認書類の表記揺れや異体文字などによるお客さま情報の不一致によって即時審査ができない場合への対応、４点目は継続的な顧客管理によって身元確認コストが増加していること

への対応が挙げられる。こうした課題に対して、継続的にセキュリティ向上を図りつつ、なるべく自動化を進め、審査にかかる時間やコストを抑える必要があると考えている。

当人認証の課題は、リアルタイムフィッシングによる攻撃への対応であり、対策としてフィッシング耐性のある多要素認証の導入が必要となる。当社では、パスキー認証を導入しているが、ユーザーへの普及が課題と考えている。

これらを踏まえ、ＣＢＤＣを検討する上での論点は、①ユーザー対象範囲、②エンドポイントデバイス、③身元確認／当人認証保証レベル、④身元確認／当人認証のユーザーカバレッジ、⑤不正対策、⑥コストが挙げられる。①は、国内居住者に加えて訪日外国人や海外在住者を対象とするのか否か。②は、スマートフォンやＰＣ、カード型デバイス等のどのようなエンドポイントデバイスによる利用を想定するか。③は、お客さまにＣＢＤＣの機能を使えるようにするためにどの身元確認/当人認証保証レベルにすべきか。また、匿名を認めるのか等も検討する必要がある。④は、身元確認を行う場合、どの本人確認書類を利用して、どういった情報（氏名、生年月日、住所等）をもとに本人特定事項を確認するか。当人認証を行う場合、どのような認証手段（ＩＶＲ認証、ＳＭＳ認証、パスキー認証等）をもとに認証するか。⑤は、ＣＢＤＣサービス提供者の一部でもセキュリティホールがあるとサービス全体に影響がでる恐れがあることから、一定の水準を維持するための横断的なガイドラインを検討すべきか否か。例えば、身元確認であれば取り扱う本人確認書類の種類や、当人認証であればフィッシング耐性のある多要素認証を必須とするか否かといった点が一例として考えられる。⑥は、申込み時の身元確認、申込み後の継続的な顧客管理、当人認証における外部サービス（ＩＶＲ認証、ＳＭＳ認証、パスキー認証等）利用時等、一連のプロセスで様々に生じうるコストへの対応をどうすべきか。以上のようにＣＢＤＣを検討する上では様々な論点があると考えている。

（２）既存の資金決済サービスの現状②（社名非公表）

―― 提供している資金決済サービスにおいて、ＫＹＣと当人認証に関連するユーザーアクションや実施状況の整理を行った。

既存の資金決済サービスの現状整理として、提供中の資金決済サービス（バンキングアプリとインターネットバンキングサービス）、およびＫＹＣと認証認可の取り組みについて説明を行う。

当社は、日本国内居住者（含む外国籍）の個人ユーザー向けにバンキングアプリと、インターネットバンキングサービス（以下、ＩＢ）の２種類の資金決済サービスを提供している。サービスの利用には、普通預金口座の開設が必須となっており、バンキングアプリはスマートフォンでの提供、ＩＢはＰＣやスマートフォンにおけるＷｅｂブラウザベースの提供となっている。バンキングアプリは資金移動の機能を有しており、ＩＢはバンキングアプリの基礎となっているため、一部のアプリ固有機能を除き、より幅広な機能が利用できる。例えば、ＩＢには認可機能があり、ＩＢのログインＩＤとログインパスワードを用いることで電子決済等代行業者が提供する家計簿サービス等と連携することを可能としている。

前述のとおり、個人ユーザー向け資金決済サービスの利用には普通預金口座開設が必須であり、非対面で利用を開始するにはオンラインの口座開設サービスにて口座開設を行っていただく。この口座開設サービスでは、犯収法で定められている本人特定事項を入力いただき、身元確認にはホ方式を採用している。口座開設完了後に、バンキングアプリと預金口座を紐付けしていただく。

ＣＢＤＣの検討において、①身元確認方式のユーザビリティ、②ＡＭＬ取引モニタリング、③認証システムの３点は論点になると考えられる。

３．ディスカッション

（参加者）プレゼンタから説明のあったとおり、①身元確認方式のユーザビリティ、②ＡＭＬ取引モニタリング、③認証システムの３点は論点と考えられる。①については、ホ方式は各撮影で少なくとも数回の撮影を行うとともに、画像の読み取り精度に起因して撮り直しが必要となることもある。また、容貌の一致確認は人手が必要になっており、運用の負荷が相応にある。他方、ワ方式はホ方式に比べユーザーフレンドリーであるものの、マイナンバーカードを持ち歩いていない、電子署名用のパスワードを記憶していない、所有しているスマートフォンがＩＣチップ読み取りに対応していない、などの理由により、認証が完了しない問題が生じている。②は、不正の手口が更新されていくため、一定のタイミングで対策を講じるのではなく、不正対策を頻繁に実施できるような体制を整えておく必要があると考える。③は、システム移行が行われる際にユーザーに切り替え作業等が発生すると、ユーザー側と事業者側双方に相応の負荷がかかるため、

システム導入決定は将来性も加味して検討する必要があると考える。以上３点はＣＢＤＣの検討においても同様に課題となりうる。

（参加者）身元確認の保証レベルを検討するにあたっては、どの方式にどの程度のリスクがあるのかを認識する必要がある。

（事務局）セキュリティを向上させる対策を行うことで、ユーザビリティが低下する懸念が想定される。自社の取り組みだけでは閉じないこともあるかと思われるし、企業によっては対策を行うのに時間がかかる先もあるだろう。業界レベルでの働きかけが必要かもしれない。バランスを取るために苦労・工夫していることはあるか。

（参加者）セキュリティ向上によるユーザビリティ低下は課題と認識している。お客さまに求める作業を急速に変更することは混乱を招くため、変更に関する準備として、お客さまへの周知など、シナリオを描くことが必要。ガイドラインを守ればよいということにならないようサービスごとにお客さまに対して、移行後にどのようなＵＸになるかということも意識しながら、パスキー認証のようなセキュリティとＵＸが整っている技術を見極め、採用していくことが重要になると考えている。

（参加者）セキュリティとユーザビリティのバランスは同じく課題と認識しており、弊社では、定期的にユーザーとの座談会を実施し、直接声を聞いている。ユーザーの声をもとに、ユーザビリティの検討と合わせて、リスク管理部門と共に適切なセキュリティ水準を考え、アジャイル開発で実装に取り組み、機能の改善を図っている。

（参加者）プレゼンテーションにて説明のあったガイドラインのように、身元確認保証レベルや当人認証保証レベルを定め、リスクに応じて必要なレベルを判断し、そのレベルにあった認証方式を導入することは重要である。もっとも、実務上ではそもそもリスクをどう評価するか、実際に使う技術がどのレベルに適合しているかを評価することに、苦慮すると考えられる。ＣＢＤＣにおいては同様の問題がより顕著になることも考えられるため、ガイドラインを運用するにあたっての課題を知りたい。

（参加者）ガイドラインによってレベルを定めると、最高レベルのセキュリティを目指す傾向が強いことが課題の１つ。各サービスの内容や特性を理解し、何が

脅威となるかを把握したうえで、リスクに応じた対応を見極めることが必要と考えている。例えば当人認証においては、パスワードリスト型攻撃やリアルタイムフィッシングによる攻撃等に対して、対応できる認証方式は何か、といったことを考えることが重要と認識している。さらに不正対策としてはもっと幅広く脅威を考えて、それに対してどう対処していくかを考える必要がある。サービス部門とセキュリティ部門間でコミュニケーションを取り、議論をしながらバランスをどうとるのかが大事だと考えている。

（参加者）不正対策などセンシティブな部分であるために情報共有が難しい分野である。もっとも、社内ガイドラインでは説得力に欠くこともあるので、外部で公表されているガイドラインも参照しながら、脅威の実例やリスクのあり方を業界で共有し、身元確認や当人認証のレベル・技術・運用の適合性について議論していけるとよいと感じた。

（参加者）外部で公表されているガイドラインとしては、ＮＩＳＴによる「デジタルアイデンティティガイドライン」、デジタル庁による「行政手続きにおけるオンラインによる本人確認の手法に関するガイドライン」、ＯｐｅｎＩＤファウンデーション・ジャパンによる「民間事業者向けデジタル本人確認ガイドライン」などが参考になる。

（参加者）現状は業種や企業によって認証レベルが相違しており、認証のガイドラインの文書化有無の違いもある認識。今後、ＣＢＤＣを検討する上では、ある程度共通の目線を仲介機関で持つべきか、あるいは各社によるべきなのか、ご意見を伺いたい。

（参加者）2018 年の改正銀行法の際に、銀行が提供する参照系ＡＰＩの接続は、ＩＤとパスワードの代わりにトークンを利用することで共通認識が図りやすかった。一方、銀行が提供する更新系ＡＰＩの接続では、使途や送金先によってリスクの度合いが大きく異なるにもかかわらず、セキュアな取引を念頭においた一律の対応を行っているため、特に実際にはリスク度合いが低いユースケースにおいて、ＵＸと認証レベルの目線が合わないと感じた。こうした事例から、各社の目線を合わせるための標準化は難易度が高いと感じているが、欧州など海外の事例も参考にしながら、制度や何らかのフレームワークを定めていけるとよいだろうと考えている。

（参加者）議論する中では、ＣＢＤＣを誰が使えるか、利用金額、利用使途をど

うするかは大きなポイント。身元確認は、不正にアカウントが作成されるリスクへの対策であり、当人認証は、身元確認済のアカウントに本人以外の第三者が不正にアクセスするリスクへの対策と理解している。その上で２点申し上げる。

①身元確認について。少額の前払式支払手段とは異なり、銀行口座の開設は犯収法上の特定取引に該当するため、それに紐づく取引はレベル分けせずに、犯収法に準拠する。仮に、ＣＢＤＣが銀行口座同様のリスクを内包している取引を行うことになれば、現行法をもとに考えると、犯収法による本人確認と同水準か、もしくは、それ以上に厳格化せざるをえないと思われる。したがって、ＣＢＤＣがどのレベルで身元確認を求めるかを議論するためには、保有や移転できる金額や使途について、どの程度自由度を許容するのか定義する必要があるのではないかと考えている。

②当人認証について。ＳＭＳ認証は広く使われているが、通信キャリア事業者が保有している電話回線に対して、他の事業者が認証に利用するリスクと、コスト負担は課題と考えている。例えば、ＳＩＭスワップにより電話番号が乗っ取られその番号を用いて他の事業者の当人認証が突破された場合の責任の所在が明確ではないと思われる。理想論は各事業者が自ら管理可能な認証システムを持つことかもしれないが、社会的なコストが大きすぎるため、責任の所在も含めて、どこかに認証システムを集約して誰かが持つという議論もする必要があるかもしれないと考えている。

この他の話題として、ワンタイムパスワード等の生成に利用される物理的なトークンは発行体が取り扱いをコントロールできるが、スマートフォン内のアプリを用いて同パスワードを生成し、取引する際は、スマートフォンでは、機種変更など発行体がコントロールできない事象が発生する。スマートフォンの機種変更時の当人認証が電話番号の認証だけで済むならば、スマートフォン内のアプリによる認証強度は電話番号を用いた認証と同一となってしまう。これはＣＢＤＣの議論からは外れるかもしれないが、当人認証におけるリスクであり課題と認識している。

悪意者は、犯罪行為で得られる経済的な利益がその労力とバランスするまで攻撃手段を過激化する傾向にあるため、当人認証のレベルについて、金額や使途等も含めてどこまでのセキュリティを求めるべきかという議論はすべきであると考えている。

（参加者）ここまでの議論を踏まえると、認証とユーザビリティについて、仲介機関である程度共通の目線をガイドラインのような形で持つように設計されることが民間事業者にとっては望ましいと理解したが、日本銀行の見解はあるか。

（事務局）ＣＢＤＣは現時点で発行が決まっていないが、ＣＢＤＣを含めてデジタル社会に適応する決済システムを将来提供していく上での、重要なテーマの１つと理解した。

（参加者）身元確認の手法について、ホ方式とワ方式の例が出てきていたが、ト方式を使うことでユーザビリティの改善と保証レベルの引き上げが実現できるかと考えている。

（参加者）実例としてト方式を採用しているケースは少ないと感じているが、利便性が向上する方式と理解した。

（参加者）現状における認証のレベルとユーザビリティは事業者ごとに一定の差異がある。今はサービスの内容というのは当然事業者ごとに違うため、各社ごとのポリシーに沿うことで問題ないが、ＣＢＤＣの場合は、仲介機関ごとに共通するポリシーを作るのか、あるいは作らないのか。作るのであれば、金額・使途によって目線をどのように設定するのか、論点として提示された。また、認証やＫＹＣにおけるコスト負担についても問題提起された。次回以降の会合で、この論点も含めて継続議論してはどうか。

４．次回予定

次回の会合は 12 月 11 日（月）に開催予定。

以　上

別紙

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第２回会合参加者

（参加者）※五十音・アルファベット順
株式会社イオン銀行
セコム株式会社
ソニー株式会社
大日本印刷株式会社
株式会社千葉銀行
日本電気株式会社
日本マイクロソフト株式会社
日立チャネルソリューションズ株式会社
フェリカネットワークス株式会社
株式会社野村総合研究所
株式会社ふくおかフィナンシャルグループ
株式会社マネーフォワード
株式会社みずほ銀行
株式会社三井住友銀行
株式会社三菱ＵＦＪ銀行
株式会社ゆうちょ銀行
株式会社りそなホールディングス
ＮＲＩセキュアテクノロジーズ株式会社
株式会社ＮＴＴドコモ
ＰａｙＰａｙ株式会社

（事務局）
日本銀行

CBDCフォーラム WG3 第2回

d払いにおける
身元確認(KYC)と当人認証について

2023年11月21日

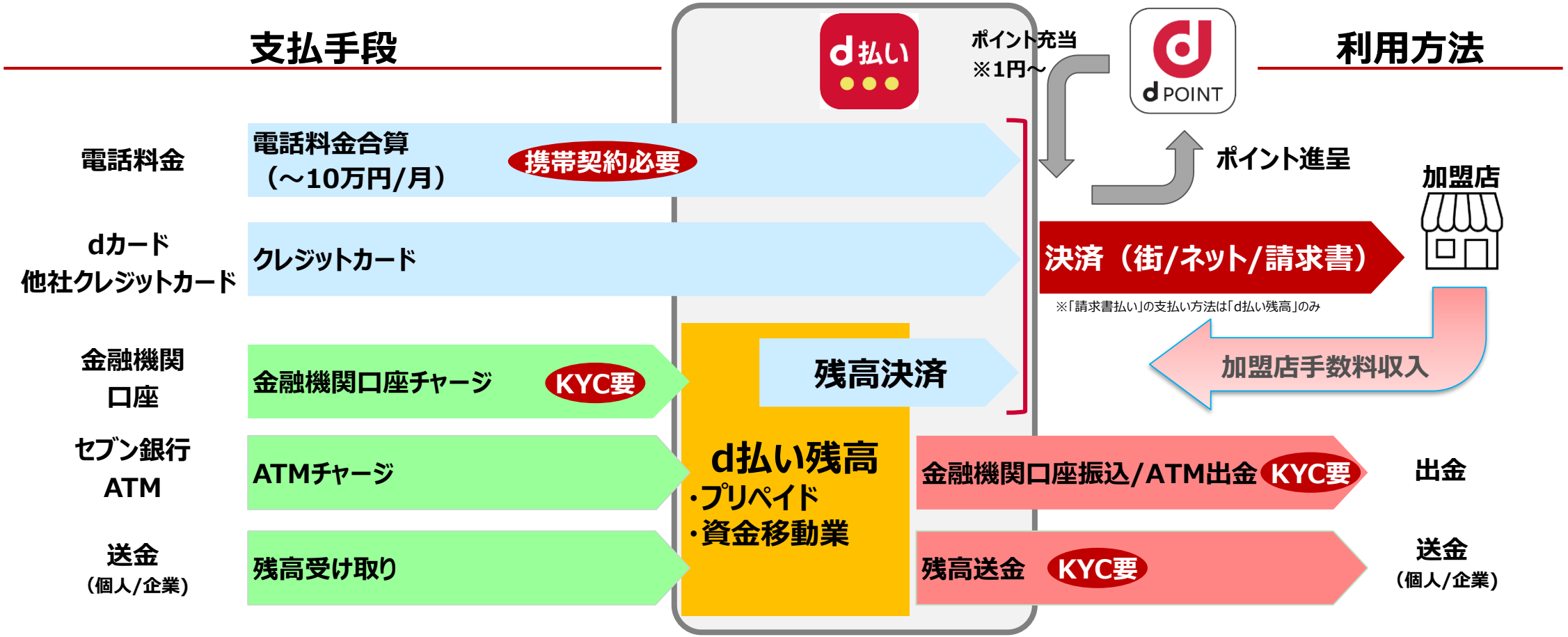
株式会社NTTドコモ

d払いとは

- 「d払い」は、日々のお買物に便利な機能とあんしん・安全のセキュリティ、サポートがそろった決済サービス
- 街やネットのお店での支払いでdポイントがたまる・つかえるだけでなく、「請求書払い」や「送金」といった決済関連機能や、「dポイント投資」や「dスマホローン」といった金融サービスとの連携など、お客さまの生活に寄り添ったさまざまな機能やサービスを提供

d払いの提供機能

- d払いは、日本国内在住の個人のお客さまが対象で、ドコモの回線をお持ちでない方もご利用できる
- 街のお店(d払いアプリ) やネットのお店(d払いネット)での決済でdポイントがたまり、1ポイント1円として利用できる
- 設定可能な支払い方法は、電話料金合算、dカード／他社クレジットカード、d払い残高
- d払い残高の開設、金融機関口座からのチャージや送金・請求書払いをご利用する際、お客さまの身元確認を実施



ドコモ版デジタルアイデンティティガイドラインについて

- ドコモでは、米国立標準技術研究所（NIST）が定めるデジタルアイデンティティガイドラインを参考に、ビジネス環境を加味しドコモ版デジタルアイデンティティガイドラインとして **身元確認保証レベル(dIAL)、当人認証保証レベル(dAAL)** を策定
  IAL: Identity Assurance Level　　AAL: Authenticator Assurance Level
- d払いでは、本ガイドラインに基づき、d払いの身元確認(KYC)および当人認証の方式を定めている

d払い 対象範囲

ドコモ版デジタルアイデンティティガイドライン		NIST デジタルアイデンティティガイドライン SP 800-63A-3	
dIAL3	犯罪者収益移転防止法などの金融ビジネスの法的要件での身元確認手法を満たすレベル（例：マイナンバーカードでの公的個人認証）	**IAL3**	認定従業員による対面か監視下の遠隔での存在確認と、本人確認書類の有効性および所持の強固な確認
dIAL2	SMSの送達確認を必要とし、同一者による大量作成を防ぎつつ、自己申告でアカウントを作成できるレベル	**IAL2**	対面ないし非監視下の遠隔での存在確認と、本人確認書類の有効性および所持のある程度強固な確認
dIAL1	身元確認も伴わず、自己申告でサービスを提供するレベル	**IAL1**	自己申告

d払い 対象範囲

ドコモ版デジタルアイデンティティガイドライン		NIST デジタルアイデンティティガイドライン SP 800-63B-3	
dAAL3	フィッシングを防ぐ効果の高い多要素認証レベル	**AAL3**	ハードウェアの認証器利用と、検証者側のなりすまし耐性のある多要素認証
dAAL2	２段階での認証レベル	**AAL2**	多要素認証
dAAL1	単一要素での認証レベル	**AAL1**	単一要素認証

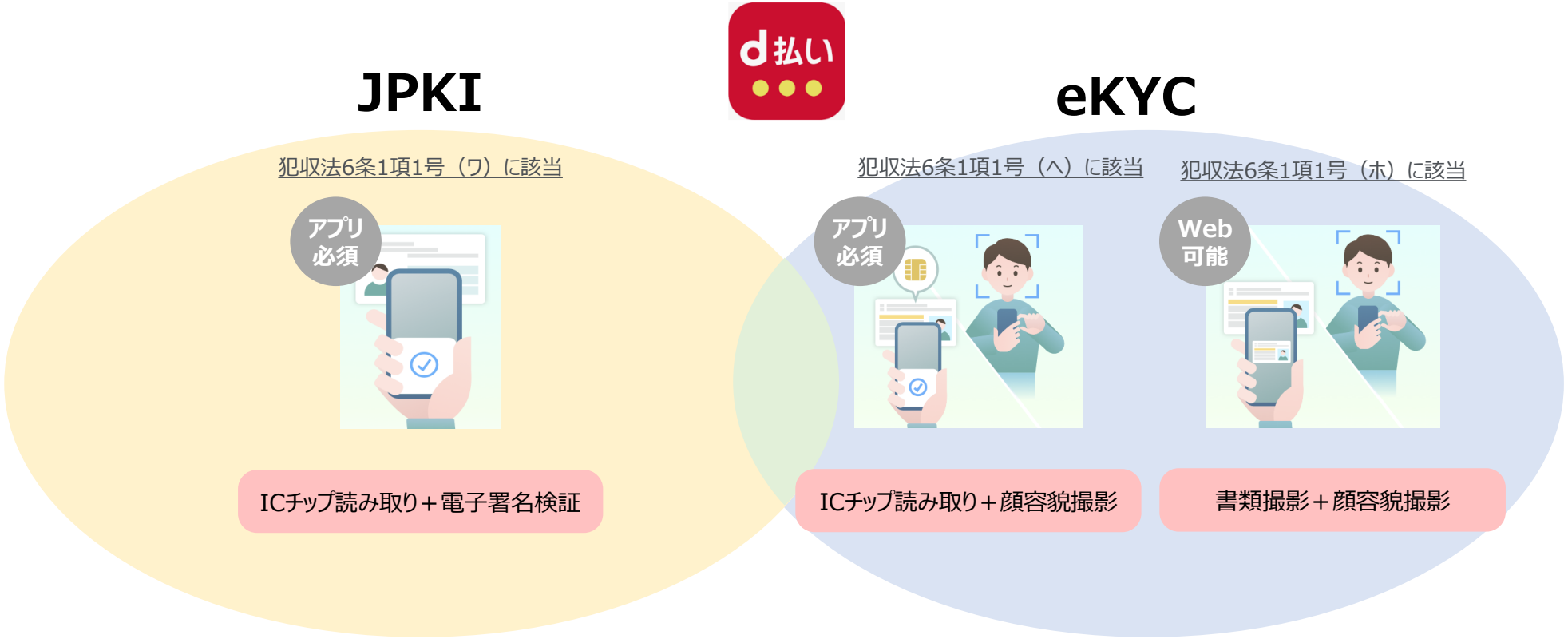
d払いにおける身元確認（KYC）について

- お客さまがお持ちのさまざまな本人確認書類に対応するため、さまざまな身元確認方法を提供
- 23年9月より、❷ **ICチップを利用した身元確認(eKYC へ方式)**を導入
- ドコモでは、身元確認機能の基盤化を推進しており、d払いも基盤機能を利用している

	❶ 公的個人認証（JPKI・ワ方式）	❷ ICチップを利用した身元確認（eKYC へ方式）	❸ 写真撮影で身元確認（eKYC ホ方式）
必要手順	マイナンバーカードのICチップ読取 ＋署名用電子証明書の暗証番号	本人確認書類のICチップ読取 ＋容貌の撮影	本人確認書類の撮影 ＋容貌の撮影
本人確認書類	マイナンバーカード	マイナンバーカード、運転免許証、在留カード	マイナンバーカード、運転免許証、運転経歴証明書、在留カード
提供時期	2022年3月	2023年9月	2020年8月
メリット	•本人確認書類および容貌の撮影が不要 •即時での身元確認の審査完了 •本人確認書類のICチップ読み取るため、偽造耐性が高い	•マイナンバーカードは券面情報のみで本人確認可能で暗証番号が不要 •最短即時での身元確認の審査完了 •本人確認書類のICチップ読み取るため、偽造耐性が高い	•対象の本人確認書類とスマートフォンを所持していれば、申請可能
デメリット	•署名用電子証明書の暗証番号（6~16桁の英数字）の記憶が必要 •身元確認用途では若干オーバースペック •ICチップを読み取りできるスマートフォンが必要	•運転免許証の暗証番号2組（4桁の数字）の記憶が必要 •容貌の撮影が必要なこと •ICチップを読み取りできるスマートフォンが必要	•本人確認書類の厚み撮影といった難しい撮影や容貌の撮影が必要なこと •身元確認の審査に時間がかかる

【参考】ドコモでは、身元確認機能の基盤化を推進

d払いで提供している身元確認機能を dアカウントとして基盤化し、ドコモ内のサービスで共通利用を推進



d アカウント

身元確認手段はJPKI・eKYCをあわせて導入することも可能

d払いにおける当人認証について

- d払いアプリ（街でのQRコード決済）、d払いネット（ネット加盟店での決済）の認証のタイミングは異なる
  - d払いアプリへのログイン時、d払いネットでの決済時
  - d払いへのクレジットカード登録、d払いの支払い方法がクレジットーカード決済時
  - 金融機関口座を登録時

ログイン時・決済時

お客さまのご契約や加盟店様の取扱う商材により、認証手段を設定

	利用可能な認証手段
高	フィッシングを防ぐ効果の高い 多要素認証レベル
中	２段階での認証レベル

【d払いアプリ】
•d払いアプリのログイン時

【d払いネット】
•お支払いの都度決済時
•継続的なお支払いの登録時に認証

クレジットカード登録時・決済時

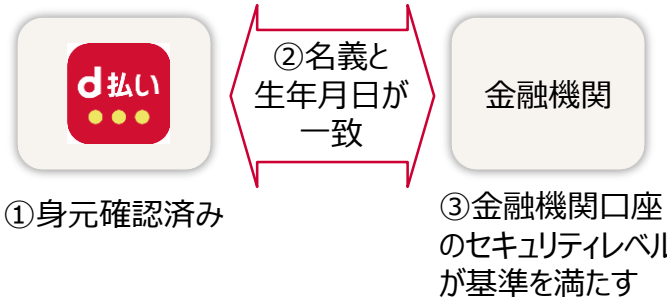
EMV 3-Dセキュア認証を実施し、
クレジットカードの利用状況に応じ、
チャレンジ認証が表示

【d払いアプリ】
•クレジットカードの新規登録時
•支払い方法をクレジットカードへ変更時

【d払いネット】
•お支払いの都度決済時
•支払い方法をクレジットカードへ変更時

金融機関口座の登録時

金融機関口座の登録には、3つの条件が必要



① d払いが身元確認済み
② 金融機関口座の名義と一致していること
③ 金融機関口座のセキュリティレベルがドコモの基準に則っていること

WG3における論点

カテゴリ		CBDCシステム論点	
対象	対象ユーザ	誰を対象とするか？	• 国内在住・海外在住、訪日外国人など誰を対象とするか？
	エンドポイントデバイス	何の端末を対象とするか？	• スマートフォンアプリ、PC、カード型デバイスなど、どの端末への提供するのか？
身元確認	身元確認保証レベル	匿名でサービス提供するか？ どの身元確認手段を利用するのか？	• 無記名や自己申告で登録するユーザを許容するのか？ • 全員を身元確認する場合、どの身元確認手段を採用するのか？
	ユーザカバレッジ	どの本人確認書類を対象とするのか？	• マイナンバーカード、運転免許証、在留カード、パスポートなど、どれを選択するのか？ • 本人確認書類で対象ユーザをカバーできるのか？
	本人特定事項	氏名・カナ・生年月日・住所・性別・本人画像の何の情報で身元確認をするのか？	• 本人確認書類によって本人特定事項がない可能性がある • 表記ゆれ・異体字による自動化ができないことがある
	不正対策	偽造本人確認書類への対策をどうするか？	• ICチップ読み取り方式は堅牢だが、ICチップを読み取るスマートフォンが必要 • 提供主体が多い場合、ガイドライン等の対応が必要になる
	コスト	身元確認のコストを誰が負担するのか？	• 口座開設時のコストだけでなく、継続的顧客管理でもコストが発生する
当人認証	当人認証保証レベル	どの認証手段までを必須とするのか？	• フィッシング耐性のある多要素認証を必須とするか？
	ユーザカバレッジ	どの認証手段を対象とするのか？	• IVR認証(固定・携帯)、SMS（携帯のみ）、ハードウェアトークン（配布が必要）、パスキー認証（インストールや設定必要）などの認証手段
	不正対策	高度化する不正手口への対処	• 提供主体が多い場合、ガイドライン等の対応が必要になる
	コスト	認証にかかるコストは誰が負担をするか？	• IVR認証やSMSは1通ごと、ハードウェアトークンは端末代金、パスキー認証はライセンス当のコストが発生する