【講演レポート】第99回JIPDECセミナー

今考えるべき、「KYC」とは

JIPDEC
プライバシーマーク推進センター　主任　　紅谷　昭光

本セッションでは、コロナ禍におけるWeb会議の増加、キャッシュレス化、ショッピングサイト利用の増加等、生活・ビジネスにおけるあらゆる場面でオンライン化が進む中でサービス提供者及び利用者が留意すべき基本的な部分をお伝えします。

オンライン化の普及が進む要因とさらなる普及に必要なこと

生産性向上が日本の共通課題

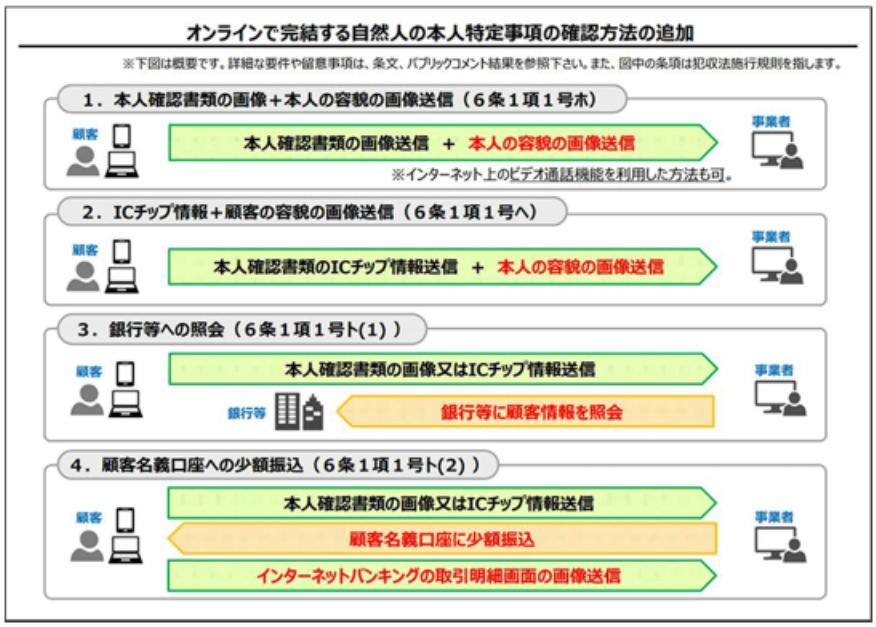
テレワークやキャッシュレス決済等オンライン化普及の要因として、新型コロナウィルスのまん延やキャッシュレス・ポイント還元事業の開始などが挙げられます。しかし、これらはきっかけに過ぎず、人口減少・少子高齢化、さらに生産年齢（15～65歳）人口が減少する中で、如何に生産性を向上させるかが共通課題となっていることがオンライン化を加速させていると考えられます。

本人確認（KYC）

オンラインサービスが普及する一方で、サービス利用時の「セキュリティ対策」と「本人確認」が重要なポイントとなります。ここでは、特に「本人確認（=KYCと定義）」について説明します。

KYC（Know Your Customer：ノー ユア カスタマー）」は、ユーザ当人の実在性の確認を行う「身元確認」と、ユーザの行為を確認する「当人認証」の二つで構成されており、中でもオンライン上での本人確認を意味する言葉は「eKYC」と呼ばれます。

なお、狭義では、2018年11月に金融庁が策定した犯罪による収益の移転防止に関する法律施行規則で、「オンラインで完結する自然人の本人特定事項の確認方法の追加」として、次の4つのeKYCの手法が示されています。



出典:「オンラインで完結する自然人の本人特定事項の確認方法の追加」（金融庁）

19

身元確認と当人認証

身元確認とは、ユーザが実在する特定の存在であることを確認する行為のことをいい、ユーザが身分証明書と自己申請（顔写真）を郵送・アップロードするなどして、サービス事業者が内容を確認できた時点でユーザ登録が完了する流れです。

当人認証とは、ユーザが実際にサービスを利用していることを確認する行為のことで、具体的には、ユーザIDやパスワードをサービス事業者側に提示し、その内容が確認できれば認証される流れとなっています。

身元確認と当人認証にはNISTが制定する「SP 800-63-3」によるレベル分けがあり、以下の通り１から３にそれぞれ定義されています。

身元確認の保証レベル（IAL：Identity Assurance Level）

・レベル1：確認不要で自己申告での登録が可能なため、信用度がほとんどない。
・レベル2：遠隔または対面で確認するため、信用度が相当程度ある。
・レベル3：有資格者による対面での確認が必要なため、信用度は非常に高い。

当人認証の保証レベル（AAL：Authenticator Assurance Level）

・レベル1：認証情報の3要素（知識・所持・生体情報）のうち、単要素または複数要素を使うことにより、信用度がある程度ある。
・レベル2：3要素のうち、IDパスワード+ワンタイムパスワードなど複数要素を使うことにより、当人認証の信用度が相当程度ある。

レベル3：2要素認証が必要、かつ2要素目の認証手段は耐タンパ性※1を有するハードウェアを用いることで信用度が非常に高い。具体的には、PIN+ICカード+マイナンバーカードなどがある。

※1：コンピュータシステム、情報処理技術の内部構造の解析のしにくさ、見破られにくさのこと

IAL・AALの設定の重要性

サービス内容に応じたIAL・AALレベルの設定

本人確認を要するサービスを提供する事業者は、サービス内容に応じてIAL、AALの設定を行う必要があります。ともに、まずはどういった情報を取り扱うのか、また取り扱う情報の検証が必要なのかを見極め、そこから考えうるリスクを洗い出したうえで導き出されたレベルに合わせた実装を行う必要があります。

参考：NIST SP 800-63-3の概要と今回の改訂がもたらす影響（https://www.jipdec.or.jp/library/report/20171127.html）

事例：ドコモ口座を悪用した不正出金

ユーザは地銀に口座を持っていただけなのに、不正に出金される被害にあってしまった事象ですが、これはユーザと地方銀行のやりとりにおいて、口座番号、口座名義等の「知識情報」のみによる本人確認しか実施されていなかった事が直接的な問題点として挙げられます。さらには、非ドコモユーザはメールアドレスのみでドコモ口座の開設が可能だったことも要因のひとつです。

この事象における根本的な原因は、資金移動が起こりうる取引ではIAL・AALのレベル２以上が求められるところ、レベルの選択が間違っていたところにありました。

まとめ

KYCにおいては、身元確認と当人認証が重要な要素であり、それぞれのレベルを理解したうえでサービス設計を行う必要があります。また、 サービスを利用する側、提供する側ともに取り扱う情報等に応じたリスクを理解した上で実装方法を選択することが求められています。

一般財団法人日本情報経済社会推進協会（JIPDEC）
プライバシーマーク推進センター　主任
紅谷　昭光

2014年JIPDEC入社
オープンデータ活用推進事業、G空間情報活用推進事業、JCAN証明書活用推進事業等に従事した後、 OpenID ファウンデーション・ジャパン KYCワーキンググループに参画。
2019年10月より現職。プライバシーマーク推進センターにて、各種基準策定、事故対応業務等に携わる。

本内容は、2020年11月20日に開催された第99回JIPDECセミナー「ビジネスモデル変革に伴うなりすましリスク対応－オンライン本人認証となりすまし対策」講演内容を取りまとめたものです。