スマートフォン等での決済サービス業務にかかるリスクマネジメント：本人認証のあり方に注目して

橋本（はしもと）　崇（たかし）

要　旨

日本におけるキャッシュレス決済比率が諸外国と比べると低い理由の 1 つとして、スマートフォン等を用いたキャッシュレス決済利用時におけるセキュリティやプライバシー保護面への人々の関心が高いことが挙げられている。キャッシュレス決済は信頼を基とする金融サービスであり、本人であることの認証や取引権限に関する認可の正確性は利用者からの信頼獲得の面で重要である。

本人認証等の正確性を高めるためのさまざまな技術的手法が提案されているが、利用者にとっての使い勝手や実装のためのコストを踏まえると、多くの手法をただ重畳的に適用すればよいものではない。また、各手法は利用者のパーソナル・データを利用するため、プライバシーへの配慮が必要である。この点、プライバシーに配慮しつつ効果的な本人認証等を行うには、プライバシー・バイ・デザインに則ったシステム開発が求められる。

そのような本人認証等に関する論点も踏まえつつ、決済サービス業者は発生しうる損失に備えることが必要である。その際、金融機関経営と同様、損失を期待損失と非期待損失に分けるというリスクマネジメントのアプローチが考えられる。デジタル技術は進歩が速いこともあり、決済サービス業者は、常に PDCA（Plan, Do, Check, Action）を行いつつ不断の安全性向上とサービス改善に取り組むことが期待される。

キーワード：　キャッシュレス決済、パーソナル・データ、プライバシー・バイ・デザイン、多要素認証、リスクマネジメント、PDCA

本稿の作成に当たっては、菊池浩明専任教授（明治大学）、廣川勝久元日本銀行金融研究所テクニカルアドバイザー、日本銀行の宇根正志氏、山田朝彦氏、千葉誠氏ほか各スタッフから有益なコメントを頂戴した。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

橋本　崇　日本銀行金融研究所企画役
（現決済機構局企画役、E-mail: takashi.hashimoto@boj.or.jp）

1. はじめに

店頭で物理的な現金（紙幣・硬貨）を使わずに行う決済、すなわちキャッシュレス決済に使用されるデバイスには、主にプラスチック・カード（磁気〈ストライプ〉カード、接触・非接触のICカード）と携帯電話がある。昨今、スマートフォンの普及が進むにつれ、携帯電話を用いたキャッシュレス決済、いわゆるモバイル決済が注目を浴びている。スマートフォンには磁気カードにはない高度な演算機能、メモリー機能、通信機能、さまざまなセンサー等が搭載されており[1]、これらを用いて決済時の認証機能を高め、セキュリティを強化できる。

スマートフォンを用いたキャッシュレス決済サービスを提供するアプリケーション（以下、キャッシュレス決済アプリ）が提供するのは、金融サービスである。金融サービスは、利用者からの信頼を基に成り立っている。換言すれば、キャッシュレス決済アプリは、一般のアプリ以上に利用者からの高い信頼の獲得が求められる。特に利用者本人であることの認証（Authentication）や認可（Authorization）における十分な安全性の確保が不可欠である。もっとも、やみくもに認証や認可の安全性を高めるだけでは、利便性・効率性といったユーザ体験（User Experience: UX）を損なう可能性がある。人間中心設計（Human-Centered Design: HCD）（International Organization for Standardization [2019]）という考え方のもと、感性品質の向上（黒須［2012］）を行う必要がある。

では、キャッシュレス決済において、個別の認証手段をどの程度重畳的に組み合わせるべきなのだろうか。この点は、必ずしも自明ではなく、サービス内容や各企業の置かれた環境、自己資本等の財務状況、その時点での技術レベル等さまざまな要素が影響する[2]。そのため、決済サービス業者は定期的にPDCA（Plan, Do, Check, Action）サイクルを実行し、当該業者が被りうる損害額を経営体力対比でコントロールするというリスクマネジメントが必要になる。

本稿では、キャッシュレス決済サービスの提供に当たって、安全性確保の観点からさまざまな本人認証の手段を検討するとともに、決済サービス業者のリスクマネジメント手法を検討したい。まず、2節では、スマートフォンやキャッシュレス決済アプリが取得しているパーソナル・データの種類を紹介する。3節では、パーソナル・データの保護を図るためのプライバシー・バイ・デザインの考え方を紹介する。4節では、キャッシュレス決済で考えられる具体的な認証方法を例示する。5

1 接触・非接触のICカードは、演算機能、メモリー機能、通信機能を搭載しているほか、指紋認証用のセンサーがカード上に搭載されたものも開発されている。

2 2019年7月、あるキャッシュレス決済サービスが不正アクセス被害を受けた際、利用者認証を2回に分けて行う「2段階認証」の不備への批判が聞かれたが（例えば、片渕［2019］参照）、本稿で述べるように、単に認証を2段階に変更するだけで安全性が自動的に向上するというものではない。

節では、決済サービス業者のリスクマネジメント方法を検討する。6 節は全体のまとめである。

2. スマートフォンやキャッシュレス決済アプリが取得しているパーソナル・データ

(1) 低いキャッシュレス比率

政府は、「未来投資戦略 2018」において、「今後 10 年間（2027 年 6 月まで）に、キャッシュレス決済比率を倍増し、4 割程度とすることを目指す」ことを明記し、キャッシュレス決済を推進している（内閣官房日本経済再生本部［2018］）。また、新型コロナウイルス感染症拡大を想定した「新しい生活様式」では、物理的な現金を用いない「電子決済の利用」をその実践例として示している（厚生労働省［2020］）。

現状、日本のキャッシュレス決済比率は 20％程度と諸外国と比べると低い（経済産業省［2018］）。日本でキャッシュレス決済が広く普及しない理由の 1 つとして、セキュリティや情報プライバシー保護面への人々の関心が高く、キャッシュレス決済が十分に信頼されていないことが指摘されている。特に、紛失や盗難時に他人になりすまして使い込まれるリスク等、認証面での安全性に不安を持つ人が多い（日本銀行決済機構局［2017］）。また、決済サービス業者が取得する利用者の決済データには、利用者個人との関係性が見出される「パーソナル・データ」が含まれるが[3]、総務省［2017a］によると、事業者にパーソナル・データを提供することに対する「不安」は、諸外国と比較して日本国民は特に大きい。

3 本稿では、個人情報、利用者情報、パーソナル・データを、以下の定義に従って使い分ける。
- 個人情報：生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）（個人情報保護法 第 2 条第 1 項）。
- 利用者情報：スマートフォンの利用者の識別に係る情報、利用者の通信サービス上の行動履歴に関する情報、利用者の状態に関する情報等、スマートフォンにおいてスマートフォンの利用者の情報と結びついた形で生成、利用又は蓄積されている情報（電話帳等の第三者に関する情報を含む）の総称（総務省［2017b］6 頁）。
- パーソナル・データ：個人情報に加え、個人情報との境界が曖昧なものを含む、個人と関係性が見出される広範囲の情報。個人の属性情報、移動・行動・購買履歴、ウェアラブル機器から収集された個人情報、特定の個人を識別できないように加工された人流情報、商品情報等を含む（総務省［2017a］53 頁）。

なお、読みやすさの観点から「利用者情報」で説明できた場合でも、前後の文脈等から、より広い概念を示す「パーソナル・データ」という言葉をあえて用いて説明している箇所がある。

(2) キャッシュレス決済における認証の必要性

キャッシュレス決済において、決済サービス業者は、決済指図を受け取った際に指図を行った人を特定し、その人の指図権限の有無を判断する必要がある。個人のアカウントについては、決済指図者が利用者本人あるいは指定代理人（法定後見人）等で、かつその決済指図の内容が正当かどうかを判断し、法人のアカウントについては、決済指図者がその法人の指名者（被権限移譲者）等であり、そのアカウントに対して決済指図を行う正当な権限者かどうかを判断する[4]。言い換えれば、決済指図を正当に行いうる人とその権限の同定を行う必要がある[5]。

決済指図を行った人とその人の持つ権限を識別する際は、その人のパーソナル・データを事前に蓄積し、その蓄積した情報と、決済指図の際に示された情報とを比較し、定められた条件を満たしているかを確認することで行われる。したがって、判断材料が多ければ多いほど、人や権限を正確に同定できる。

(3) 認証の手段とパーソナル・データの活用

最近のスマートフォンの高機能化等もあいまって、さまざまな本人確認方法が実用化されている。実務ではそれらの本人確認方法を組み合わせ、2 要素認証から多要素認証へとリスクに応じて複数の手段を組み合わせるリスクベース・アプローチが主流となってきている（金融情報システムセンター［2018］）[6]。また、これまでに受けた攻撃の経験も踏まえ、ログイン時の本人認証だけではなく、決済指図（振込先、金額等）が本人の意思に基づいていることを決済サービス業者が確認する取引認証も導入されてきた（鈴木・中山・古原［2013］、井澤・廣川［2015］）。

こうした過程でさまざまなパーソナル・データを活用した認証手段が考案されている。もっとも、パーソナル・データを認証に活用すると、決済サービス業者はそのデータを保有する必要が生じ、結果としてプライバシー保護の問題が生じる。認

4 決済アカウントとは、銀行であれば「口座」を指す。スマートフォン・アプリでの決済サービスでは、「ウォレット」等と呼ばれる。

5 同定とは、人を確認する「認証」と人や属性に対して権限を付与する「認可」との両方を正確に行うことを意味し、決済サービス提供に当たってはこれを行うことが不可欠である。

6 認証では複数の「要素」を組み合わせる多要素認証に意味があり、何回かの「段階」に分ける多段階認証を形式的に行っても、必ずしも精度の向上につながるわけではない。多段階認証を行っても同じ切り口で認証を行うのであれば、一般的にはセキュリティ強度の強化程度は限定的であるにもかかわらず、UX が低下することになり、システム設計上はマイナス評価となる。米国標準技術研究所（National Institute of Standards and Technology: NIST）発行規格や PCI DSS（Payment Card Industry Data Security Standard）等の多くの国際的な規格は、多要素認証を議論しており、多段階認証を議論しているものではない。

証の強化を図るためにより多くのパーソナル・データを保有しようとすると、求められるプライバシー保護もより複雑になる。今では、決済サービス業者にとってプライバシー保護は事業遂行上の重要な課題となっている。

この間、総務省では、スマートフォンの利用者情報の取扱いや活用の在り方について検討を進めてきた。2012 年以降、3 回にわたって「スマートフォン プライバシー イニシアティブ」という指針を提示し、国として利用者情報の適切な取扱いをアプリ業界等の関係事業者へ促している（総務省［2012, 2013, 2017b］）。

(4) キャッシュレス決済アプリが取得しうるパーソナル・データ

イ. スマートフォンが取得できる情報の種類

初めに、スマートフォンが技術的に取得できるパーソナル・データの種類について整理する[7]。

スマートフォンには、電話番号、メール・アドレス等連絡先の情報、通信履歴、ウェブ・ページの閲覧履歴、アプリの利用履歴、位置情報、写真や動画等、個人情報を含め、さまざまなパーソナル・データが蓄積される。総務省［2017b］によると、図表 1 に掲げるパーソナル・データがスマートフォンに蓄積されうる。アプリの設定等にも依存するが、アプリをインストールすると、これらのパーソナル・データの一部あるいは全部がアプリを通じて収集され、事業者はこれらのデータを取得できる。加えて、広告配信事業者等へ送信され、広告配信事業者等がそのデータを活用して、利用者の趣味・趣向に応じた広告の表示等に利用する場合もある（総務省［2012］）。

ロ. 決済サービス業者が取得できる情報

決済サービス業者は、図表 1 で掲げた一般的なスマートフォンが取得可能なパーソナル・データ以外に、決済業務から生じる以下のようなデータも取得できる[8]。

（イ） 決済自体に必要なデータ

決済金額、決済日時、決済相手、決済手段（カード、QR コード[9]、ウェブ上でのカード番号入力等）、決済場所（店舗名、POS〈Point of Sale〉番号等）等。

7 各国の法令や、国民のプライバシー意識、倫理感、関係する事業者の規約、アプリの設定等によって、各スマートフォンが取得している情報の種類が一律ではないことに留意を要する。

8 キャッシュレス決済には、法律や業界団体等によるルールがあり、データの取得、保存には一定の制約がある。例えば、クレジット・カード業界のセキュリティ基準である PCI DSS では、カード会員データへのアクセスは業務上必要な範囲内に制限しているほか、機密の認証データ（セキュリティ・コード等）の保存は禁じている。

9 QR コードの商標は株式会社デンソーウェーブの登録商標である。

図表１　スマートフォン上で取得されうるパーソナル・データ

区分	情報の種類	
利用者の識別にかかる情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジット・カード番号等の個人信用情報等
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報
	クッキー技術を用いて生成された識別情報	ウェブサイト訪問時、ウェブ・ブラウザを通じ一時的に端末に書込み記録されたデータ等
	契約者・端末固有 ID	OS が生成する ID、独自端末識別番号（Unique Device IDentifier: UDID）、加入者識別 ID（International Mobile Subscriber Identity: IMSI）、IC カード識別番号（Integrated Circuit Card ID: ICCID）、端末識別 ID（International Mobile Equipment Identifier: IMEI）、MAC アドレス（Media Access Control address）等 ※決済サービスの場合、近距離無線通信（Near Field Communication: NFC）の IC チップに付されている ID も活用している。
	広告 ID	IDFA（IDentification For Advertisers）、AdID（Advertising ID）
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴
	ウェブ・ページ上の行動履歴	利用者のウェブ・ページ上における閲覧履歴、購買履歴、検索履歴等の行動履歴
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等
	位置情報	GPS（Global Positioning System）機器によって計測される位置情報、基地局に送信される位置登録情報
	写真、動画等	スマートフォンに搭載されたカメラ等で撮影された写真、動画
第三者に関する情報	電話帳で管理されるデータ	氏名、電話番号、メール・アドレス等

資料：総務省［2017b］図表 1 を基に、筆者作成

（ロ）　決済に付随するデータ

一般的にキャッシュレス決済を行うだけでは購入品物や点数等のデータは取得できないが、店舗の POS システム等と連動させれば、そうしたデータを取得できる。オンライン・ショッピング・システムと連動させた場合は、検索ワードや、クリック商品等の動向を把握できる可能性が生じるほか、実店舗の場合でも、カメラや各種センサー等により、購入には至らなかったが手に取った商品等のデータを取得することも技術的には可能である。また、銀行振込み等の場合でも、EDI の仕組みを使えば[10]、例えばインボイス・データ等から支払請求の内容を把握できる可能性がある。

10 EDI（Electronic Data Interchange）とは、受発注に関して、支払企業から受取企業に伝達する電子的なメッセージ交換のこと。受発注、出荷、請求、支払い等、企業間での各種取引情報が交換される。日

ハ．スマートフォンが取得した情報の活用方法

総務省［2012］16頁によれば、一般的にスマートフォン・アプリによるパーソナル・データの活用方法は、大きく分けて①～④のようなものが想定されている。

① アプリがそれ自体のサービス提供のために用いる場合
② アプリ提供者が、アプリの利用状況等を把握することにより、今後のサービス開発や市場調査のために用いる場合
③ スマートフォンの位置情報あるいは契約者・端末固有ID等のパーソナル・データを情報収集事業者等が取得し、広告サービス等に活用する場合またはその他の市場調査等の情報分析等に活用する場合
④ 現段階では目的が明確ではないが、将来的な利用可能性等を見込んでパーソナル・データを取得する場合

キャッシュレス決済アプリでは、パーソナル・データの活用は、②、③のように市場調査や広告サービス等への活用といった、決済サービスに付随するビジネスとの関係で注目されやすいが、「①アプリがそれ自体のサービス提供のために用いる場合」も重要である。サービス提供の際の認証・認可にパーソナル・データを用いるほか、決済サービスに不可欠なマネー・ローンダリング対策（Anti-Money Laundering: AML）にも、パーソナル・データの活用は欠かせない。

(5) 法令順守と各種ルールの改訂への対応

決済サービス業者が取得情報を活用する際には、個人情報保護法等の各種法令の順守が求められる。サービス提供の際の認証や認可の行為、不正利用の検出、あるいはAML等を含め、個人情報の活用に当たっては、決済サービス業者はその利用目的について利用者から明確に同意を取り、適法状態にしておくことが必要である。なお、2017年に改正された個人情報保護法において、個人情報の定義が明確化された[11]。本節（4）で示したパーソナル・データのうち個人情報保護法の対象となる個人情報についての目的外利用は違法であり、留意が必要である。

プライバシーに関するルールは、日本での個人情報保護法だけなく、欧州での一般データ保護規則（General Data Protection Regulation: GDPR）、米カリフォルニア

本の銀行間決済ネットワークである全銀ネットでは、2018年12月からEDIが活用できるZEDI（全銀EDIシステム）の稼働を開始している（全国銀行協会［2020］）。

11 個人情報の定義の明確化として、①利活用に資するグレー・ゾーン解消のため、個人情報の定義に身体的特徴等が対象となることを明確化、②要配慮個人情報（本人の人種、信条、病歴等本人に対する不当な差別又は偏見が生じる可能性のある個人情報）の取得については、原則として本人同意を得ることの義務化が行われている（個人情報保護委員会事務局［2017］）。

州でのカリフォルニア消費者プライバシー法（The California Consumer Privacy Act: CCPA）等の法令のほか、国際標準や各種ガイドラインも適時改正を重ねている。例えば、ウェブサイト上でのクッキー利用に対し明示的な同意を求める動きが広がっている。一方、自分のパーソナル・データの提供先を利用者自身がコントロールする情報銀行等の動きもみられる。

こうした動向は、決済サービス業者のパーソナル・データ管理とその運用方法にも影響を与える。決済サービスの提供には、現行の各種法令やガイドラインに沿うことはもちろんのことであるが、それにとどまらず、利用者や社会全体が求めているサービスをデザインし、運営することが求められる[12]。

(6) パーソナル・データの扱い方にかかる利用者への説明

利用者からの信頼獲得のためには、単にデータの利用について同意を得るのみならず、データをどのように扱い活用しているかを利用者に説明し理解を得ることが欠かせない（寺田［2012］）[13]。

総務省は、事業者が自らの責任として、利用者への情報提供・周知啓発を推進し、利用者のリテラシー向上を図っていくことを求めている（総務省［2012, 2013］）。リテラシー向上については、アプリのデザインの中で、利用者がプライバシーの扱い方にかかる認識を深めていける仕掛けを用意することも 1 つのアイデアである。

また、利用者からの信頼の厚いサービスは、利用回数が多くなり、利用時間も伸びると考えられる。信頼性のバロメータという意味で、利用者のアプリへのアクセス回数や滞在時間を定期的に検証することが重要である。

決済サービス業者は、事業者が利用者との接点を確保し、説明を丁寧に繰り返す等の地道な取組みを積み重ね、さまざまな年代・バックグラウンドからなる利用者が説明を十分に理解できるようにすることが必要である。そうした取組みが当該業者に対する利用者からの信頼につながることになる。

12 本稿での「デザイン」という用語は、黒須［2015］が述べるように、総合的な設計という意味で使用しており、必ずしもデザイナーの担当業務に限定したものではない。この点、経済産業省・特許庁［2018］1 頁では、「デザインは、企業が大切にしている価値、それを実現しようとする意志を表現する営みである。」と表現している。

13 総務省［2012］54 頁では、「アプリケーションがスマートフォンの中の利用者情報へアクセスを行い、利用者が自らの情報がどのように取得・利用されているのか十分理解することができなくなり、マルウェアやワンクリックウェア等も出現する中で利用者の不安感も高まっている状況である」と指摘し、そのうえで「スマートフォンにおける利用者情報を活用する関係事業者等は、利用者が個人情報やプライバシーの観点から安全・安心にサービスを活用できるように、利用者情報を適切に取り扱うとともに、利用者に対して分かりやすく透明性が高い説明を行い、その理解と有効な選択を促すことが求められている」と、利用者への周知啓発を推進する必要性を指摘している。

3. パーソナル・データのリスクマネジメント

キャッシュレス決済アプリがさまざまなパーソナル・データを活用する過程においては、2 節でみたように、各種データを法令に基づき適切に保護するとともに、その実態を利用者に理解浸透させる必要がある。そのための 1 つの方法として、プライバシー・バイ・デザインに則ったアプリの設計が考えられる。

(1) プライバシー・バイ・デザインに沿ったシステムの構築

パーソナル・データの収集・取扱いについて利用者からの納得を得る説明を行うための方策として、決済サービス業者がプライバシー・バイ・デザインというコンセプトに沿ったアプリの設計・開発を行うことが考えられる（総務省［2012, 2013］）。プライバシー・バイ・デザインとは、プライバシー保護のあらゆる側面にかかる施策をアプリのライフ・サイクルにおける企画段階から意識し、セキュリティ要件をあらかじめ設計・開発に適切に組み込むことである。これにより、利用者への説明が容易になって理解や信頼を得られやすくなると同時に、プライバシー保護の水準が向上することで、結果として利用者のみならず決済サービス業者にとっても有益である（Cavoukian [2011]、カブキアン［2012］）。

プライバシー・バイ・デザインは次の 7 つの基本原則からなる。

① 事後ではなく事前対策、救済ではなく予防
② プライバシーを初期設定すること
③ プライバシーを設計に組み込むこと
④ 十分な機能性（ゼロ・サムではなくポジティブ・サム）
⑤ 最初から最後までのライフサイクル全体を通じてのセキュリティ保護
⑥ 可視性と透明性、公開の維持
⑦ 利用者のプライバシーの尊重、利用者中心主義の維持

(2) プライバシー保護にかかるリスクマネジメント：PIA

キャッシュレス決済サービスのプライバシーにかかるリスク分析・評価を行う手法として、プライバシー影響調査（Privacy Impact Assessment: PIA）が提案さ

れている。PIA は、金融業界では比較的早くから議論されており、国際標準化機構（International Organization for Standardization: ISO）で金融サービスを担当する ISO/TC 68 において 2008 年に ISO 22307「金融サービスにおける PIA」という国際標準規格を制定している（International Organization for Standardization [2008]）。また、ISO 22307 のほかにも、ISO と国際電気標準会議（International Electrotechnical Commission: IEC）との共同委員会におけるセキュリティ技術担当部会である ISO/IEC JTC1/SC 27 が、2017 年に ISO/IEC 29134「PIA にかかるガイドライン」という国際標準規格を制定している（International Organization for Standardization and International Electrotechnical Commission [2017]）。

キャッシュレス決済のシステム構築においても、まず国際標準規格 ISO 22307 や ISO/IEC 29134 を基とした PIA プロセスを検討することが考えられる（瀬戸・長谷川［2020］、長谷川・中田・瀬戸［2019］）。個人情報の保護の評価については、個人情報保護委員会が「特定個人情報保護評価指針」（特定個人情報保護委員会［2014］）を公表しており、こうした指針も、プライバシーにかかるリスク分析・評価に有益である。

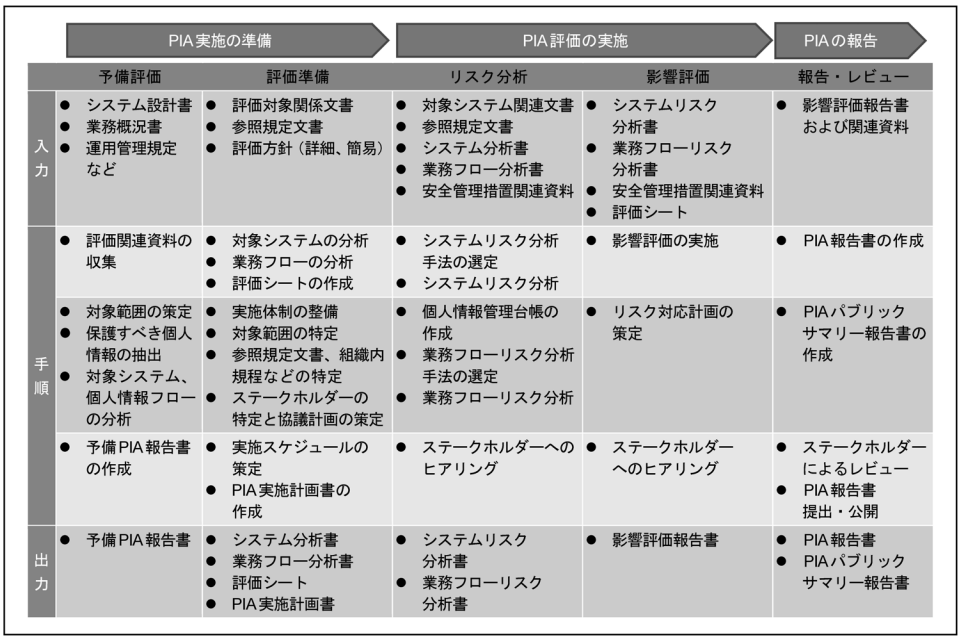
PIA はプライバシー情報を取り扱う事業者が「システム、事業、サービス等において、プライバシーへの影響を事前に評価し、プライバシーの侵害を防ぐために運用面、技術面での対策を講じる一連のプロセス」とされる（電子情報技術産業協会［2014］）。PIA の実施手順としては、①実施の準備をし、②プライバシー要件を洗い出し、③個人情報にかかる対象システムやデータ・フローを把握し、④リスクの分析や評価を行い、⑤評価結果をまとめるプロセスとなる（図表 2 参照）。

PIA 結果を受けて、個人のプライバシーへの影響を最小限とするために採りうる制度対応（a）と、プライバシー・個人情報保護のために実施可能な技術対応（b）等といった対応策の検討に進むことになる（カブキアン［2012］）。

（a）制度対応は主に組織の体制整備である。具体的には、顧客からのパーソナル・データの開示や削除請求への対応プロセスや顧客への選択肢の提示方法等、プライバシー保護にかかる業務プロセスを検討し、規程に明文化し、それに準拠した運用が実施されているかを確認するチェックシートの準備が必要となる。一方、（b）技術対応では、プライバシー保護強化技術（Privacy Enhancing Technology: PET）を検討し、アプリに実装していくことになる。PET とは暗号技術と認証技術、匿名化技術等を複合的に利用したものの総称である。PET の適用はプライバシーとセキュリティの双方への対策となり、システムの信頼性（安全性）とユーザの安心感を高めることができる（電子情報技術産業協会［2014］）。

サービス運用開始後は、（a）制度対応については、プライバシー保護の責任者は、チェックシートを基に定期的にパーソナル・データの保護状況を確認する。また、セキュリティやプライバシーにかかるデータ保護に関する意識の向上のためのセキュリティ教育も定期的に実施することが望まれる。加えて、定期的な内部監査

図表 2　ISO/IEC 29134 準拠の PIA 実施手順



資料：瀬戸・長谷川［2020］図 4.1

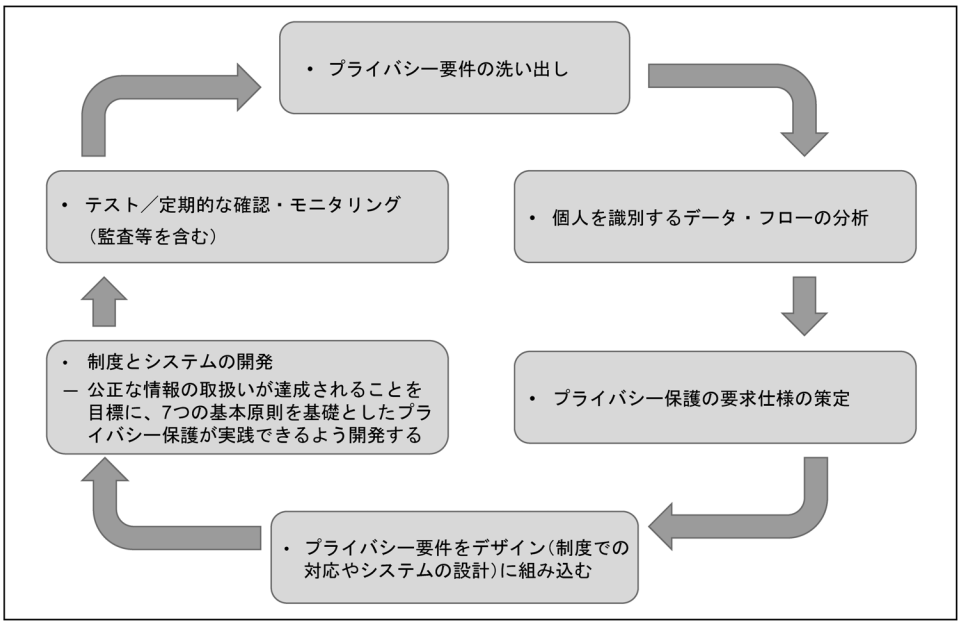
も要する。また、(b) 技術対応として、ログ解析を通じたモニタリングを行う必要がある。モニタリングに当たっては、特定のセキュリティ侵害やエラー検出時に管理者にアラートが自動的に通知されることが望まれる。モニタリングを通じて改善箇所を把握することで、プライバシー要件の十分性について再検証できる。

こうした不断の改善プロセスを、継続的なリスクマネジメントに昇華させることが重要である。PIA の結果を踏まえて業務体制や PET が検討され、プライバシー保護が達成される仕組みが、プライバシー・バイ・デザインである（図表 3 参照）（カブキアン［2012］）。キャッシュレス決済サービスにおいては、プライバシー・バイ・デザインの考え方に基づき、パーソナル・データの保護にかかるリスクマネジメントを機能させる必要がある。

(3)　スマートフォン・アプリにおけるプライバシー保護の実現を図るうえでの課題

本節（2）ではプライバシー・バイ・デザインの総括的な考え方を整理したが、実際のアプリにおける具体的な実現手法については、さらなる検討を要する。

図表 3　プライバシー・バイ・デザインの適用フロー



資料：カブキアン［2012］38 頁の図表を基に、筆者作成

スマートフォンの開発は、アプリ開発者、通信キャリア、周辺機器ベンター、ファームウェア・ベンダー、OS ベンダー、端末ベンダー等、マルチベンダー構成になっている場合がある。各ベンダーが独自で十分なプライバシーが保護される設計を行ったとしても、各ベンダー間で十分な情報共有が行われなければ、結果的にプライバシー保護が不十分となる可能性がある。Gamba *et al.* [2020] では、一部のスマートフォンにおいて、工場出荷時にプリインストールされているアプリが悪用され、あるいは顧客の同意なしに、パーソナル・データが流出するリスクがあることを指摘している。また、磯部・坂本・葛野［2019］は、スマートフォンのプラットフォームに準備されている暗号鍵の管理機能をアプリが適切に使用できないケースがあることを報告している。また、工場出荷時点でリスクをコントロールできたとしても、一部のソフトウェアやハードウェアのアップデート（あるいはアップデートしないこと）によって認証機能が適切に実行されず、パーソナル・データが漏洩してしまう可能性も想定しうる。

スマートフォン・アプリ業者の場合、図表 2 で示した PIA 実施手順のうち、評価準備（特に、対象システムの分析、ステークホルダーの特定と協議計画の策定）、および、リスク分析（特に、システム・リスク分析）の実行が容易でない。特に「ステークホルダーへのヒアリング」は、関係者が多すぎたり、アプリの構成や相互依存性が複雑であったりし、情報を適切に入手・整理・分析できない可

能性が高い。プライバシー・データの取扱いについての設計情報等の開示や標準化手法の確立とその順守、プライバシー・マーク制度のような第三者評価機関での評価を、アプリの更新頻度に見合う形で徹底する等といった取組みを関係者すべてが行い、十分な透明性を確保することが、利用者からの信頼につながるであろう。

4. パーソナル・データの認証・認可での活用

プライバシー保護を含めてパーソナル・データの管理が適切に行われていることを前提に、本節ではパーソナル・データの活用としての認証・認可方法を考える。2節で述べたように、キャッシュレス決済のシステムにアクセスし取引を行う際には利用者の本人認証や取引認証を行う必要がある。その際のパーソナル・データを活用した認証手法例を紹介する[14]。なお、実際には、5節で説明するように、以下の認証手法の要素を複数組み合わせて適用するのが一般的である。

(1) 認証手法の例

① 利用者の所有する「もの」(所有物認証)

アプリ開発業者は端末の所有者と利用者が同一であることを前提に開発を行うため、スマートフォンを用いたキャッシュレス決済の場合、特定の「スマートフォン端末」そのものが、所有物認証として使われることが多い(この点、必要な場合には端末の所有者と利用者が一致しているという前提が維持されているかを確認する必要がある)。スマートフォン端末を認証するには、例えば、以下の方法がある。

- 利用者が事前に登録した端末のID番号を活用した認証
- ブラウザやアプリが持つクッキーや、アプリが生成し画面に表示したQRコードに埋め込んだ情報等を活用した認証[15]

14 法令や規約、スマートフォンの設計等により、個々の決済事業者にとって活用可能でない認証手段も含まれるほか、個々の認証・認可手段においても、精度の違い、なりすましの難易度、信ぴょう性等が異なることに留意を要する。また、一般論として、決済サービスを提供する業者の立場の違い(ハード製造者、オペレーティング・システム提供者、通信業者であるか否か等)によって、スマートフォン内に格納されている利用者情報の量や質(取得できた情報の正確さ等)に差異が生じる可能性がある点には留意が必要である。

15 QRコードを利用した認証方式では、時間によって表示されるQRコードが変化する動的QRコード

- NFC 対応等の機能を有する決済用 IC に埋め込まれた ID 番号[16] 等によって端末を特定することによる認証

② 利用者のみ知る情報（知識認証）

- パスワードや暗証番号[17]
- いわゆる「秘密の質問」[18]
- 生年月日や住所等の個人情報[19]

③ 利用者自身の生体情報（生体認証）

生体認証は、利用者が決済の際に示す所有物が、その利用者本人であることを正しく結びつけるために用いられることが多い。

（a）物理的生体認証（biophysical biometrics）

指紋、顔、虹彩、静脈パターン等、物理的な生体物を用いた認証（宇根［2016］）。なお、指紋は指紋センサー、顔、虹彩、静脈パターンはカメラを活用することで情報の取込みが可能である。

（b）生物力学的生体認証（biomechanical biometrics）

画面タッチの圧力やキーボード入力時のくせ等、筋肉・骨格・神経システム等の違いから生じる個人の「行動のくせ」を利用した認証。

④ 利用者の位置情報

（a）利用者が決済指図を行った地点に関する情報

スマートフォンの GPS 情報、接続中あるいは接続可能な Wi-Fi や携帯電話の基地局情報のほか、店舗の端末設置場所情報等によって、決済を指図した場所が特定できる。この位置情報を用いて、例えば決済指図を実

を生成したり、画面を点滅させたり、画面上に時刻を秒単位で表示することによって、画面コピーを他の端末へ送信する等によるなりすまし防止を図ることが可能であり、これによって、端末をその利用者が真に所有していることの証明になりうる。

16 NFC の IC チップや画面に表示した QR コードを決済端末にかざす行為は、スマートフォン端末の認証のためだけでなく、決済指図の意思表示も兼ねる場合が多い。

17 同じパスワードや暗証番号を複数の利用先で使いまわすようなケースも想定されるため、利用者以外もパスワードや暗証番号を知っている可能性を前提においた設計が必要である。

18 NIST の電子的認証に関するガイドライン第 3 版（National Institute of Standards and Technology [2017]）では、秘密の質問は文字数が少ないことが多く、強固ではない点といった理由から、これを使うべきでないとしている。

19 一般的にさまざまな用途・場所で取得されている生年月日や住所等の個人情報についても、パスワードや暗証番号同様、利用者以外も知っている可能性を前提においた設計が必要である。

店舗で行った場合、利用者（支払者）の位置と店舗の位置が一致しているか、短時間のうちに利用者が移動できない遠隔地で複数の決済指図が行われていないか等を判定できる。

また、IP アドレスは、利用者の国や接続先の事業者等を特定できるため、取引の正当性の判断に役立つ可能性がある。

(b) 利用者の行動パターンに関する情報

GPS 情報のほか Wi-Fi や携帯電話の基地局情報から、スマートフォンの位置と時刻を日々蓄積すると、利用者の行動履歴を把握できる。例えば、通勤・通学者の場合、定期的に同一時刻に出発し、同一交通手段で、同一の目的地に行くことから、位置情報に普段の行動パターンが現れる。こうした日常生活での行動パターンと端末の挙動が一致しているかどうかを認証に活用することがある。

⑤ 利用者のスマートフォンにインストール済のアプリ

(a) アプリの利用状況

アプリの利用状況のデータを日々蓄積し認証に活用することも考えられる。例えば、電車通勤者の場合、毎日ほぼ同時刻の通勤時に、同じアプリを同じ時間使うというパターンが現れやすい。このパターンと異なるアプリの使い方をした場合に、決済サービス業者が意図する利用者ではないと疑うことが可能となり、これを認証に活用することがある。

(b) インストールされているアプリの数や種別等

スマートフォンにインストールされているアプリの数や種別等が短期間に大きく変わることはないという経験則を本人確認に利用する。

⑥ 利用者の運動履歴

スマートフォン等から取得できる活動量（歩数計）やスマート・ウオッチ等から取得できる脈拍データのパターンを用いて、利用者の位置履歴やアプリ利用履歴と同様、認証に活用することがある。

⑦ 利用者の過去の購買履歴

利用者の過去の購買履歴を蓄積しておき、決済時に買った商品、金額、時刻、場所等のデータが、過去の履歴からかけ離れていないかチェックすることで、利用者が正しいかを推定できる。

⑧ 利用者の友人関係

過去の個人間送金の相手、SNS（Social Networking Service）に登録された友だち情報、スマートフォン内の電話帳情報等から交友関係の把握が可能である。この交友関係データを基に、ある支払指図が、正しい利用者からの指図で、かつ意図した支払先であるかを推定する材料とすることがある。

なお、④から⑧に挙げた認証方法例のうち、日常生活の行動パターンにかかる情報を利用した認証手段は「ライフスタイル認証」と呼ばれている（小林ほか［2016］）。スマートフォンの位置情報やインストール済アプリの情報、運動履歴等のログによって、端末所有者の日常生活の行動パターンを推測し、習慣化された行動パターンと異なる挙動を端末が示している場合に、決済サービス業者が正当な利用者ではないと疑うことが可能となるライフスタイル認証は、認証時にパスワード入力等の明示的な動作を必要としないことがメリットである。一方、ある程度長い期間にわたって情報を集積する必要であること、日常生活の行動パターンというプライバシー・データの保護が必要になること、人間の行動パターンを基にした認証であるため揺らぎが生じること等、既存の認証方式にはない性質があるため、他の認証方法と合わせて活用することで安全性を担保する必要がある。

将来的には、現行端末より性能の高いセンサーが搭載されたり、本人を認証する際の新たな技術が登場したりすることが想定される。また、社会基盤として信頼できる個人認証のあり方を模索する議論もあり（総務省［2018］）、こういった個人認証にかかる議論の結果をキャッシュレス決済の認証に活用することも考えられる[20]。また、スマートフォンのデータに限らず、SNS に投稿した場所や時刻、投稿された画像に映り込む景色から推定される位置情報、SNS 等に登録した学歴・職歴、配偶者の有無、家族の年齢といった SNS 利用者の個人情報、ウェブでの予約や検索履歴等から得られる情報、街中の監視カメラ等、理論上はさまざまな情報が本人を認証する手段として使われる可能性がある。

(2) 利用者の意思による認証と事業者の利用者識別行為

本節（1）①～⑧で掲げた認証手法には、イ）利用者の意思に基づいて行う認証（以下、利用者意思による認証）と、ロ）キャッシュレス決済事業者が利用者以外のなりすましを検出するために識別する行為（以下、事業者の利用者識別行為）の 2 種類がある（図表 4 参照）。上記の①（所有による認証）、②（記憶による認証）や

20 例えば、エストニアには公的に電子認証が行えるシステム（Electronic Identity〈eID〉System）がある。

図表 4　認証と識別の違い

	イ）利用者意思による認証	ロ）事業者の利用者識別行為
主体	利用者本人（証明する者）	キャッシュレス決済事業者（検証する者）
4節（1）の「認証方法の例」に掲げる番号	①、②、③の一部	③（イ）に含まれない部分）、④、⑤、⑥、⑦、⑧
要求条件	本人拒否率、他人受入率	識別（再現率、適合率）
本人同意	あり	なし（ある場合もあり）

一部の③（生体認証）は、イ）利用者意思による認証であるが、④～⑧（一部③も含む）は、ロ）事業者の利用者識別行為として使われる。キャッシュレス決済は利用者の同意が欠かせないサービスであることから、利用者意思による認証が欠かせない。そのうえで、事業者が認証面での安全性を向上させる観点で、事業者の利用者識別行為と組み合わせた認証を行うことを検討する必要がある。

事業者の利用者識別行為は、本人が意識しないうちに行われるケースがあるので、パーソナル・データ活用には留意が必要である。位置情報や通信履歴等を利用者の同意なく識別行為に用いることは、取得した情報の目的外使用に該当する可能性がある。また、事業者の利用者識別行為によって得られる結果の精度は、利用者意思による認証より低い可能性があるほか、利用者の意思が働いていない分、システムの攻撃への耐性も低い可能性がある。

5. キャッシュレス決済アプリの認証面での安全性向上とリスクマネジメント

先述のとおり、スマートフォンを用いたキャッシュレス決済の認証の場合、1つの強力な認証方法に頼るというよりは複数の認証手段を組み合わせ、攻撃の成功確率を下げることが一般的である。特にQRコードを用いた決済方式では、店舗に表示されたQRコードを第三者が貼り替え不正送金させる事件が発生している[21]（大熊・瀧田・森井［2018］）ほか、QRコード自体を細工して発見が容易でない偽装QRコードが生成できる（大熊・瀧田・森井［2018］）等、盗難等による利用者のなりすましのみならず、加盟店側でもなりすましが容易である等、脅威は大きい。このため複数の認証手段を組み合わせて、システム全体で安全性を確保することが必須である。

21 店舗側に表示されたQRコードを用いて決済を行う店舗提示型コード決済（Merchant Presented Mode: MPM）方式を対象とした攻撃方法。

もっとも、必要十分な安全性を確保するために[22]、どの認証手段をどの程度重畳的に多要素化を行い、セキュリティ・レベルをどの程度確保すべきなのかは自明ではない。認証手段の数を増やし、より多くの切り口から認証を行うほど安全性は向上するが、システム開発・維持管理のコストは増加する。また、設計の巧拙によるが、一般的には利用者の利便性である UX も損ねることにつながる。

そこで、以下では、必要十分な認証の要素の数と組合せについて、決済サービス業者自身が被りうる損失を測るリスクアセスメントの観点から検討する。ここでは、一例として、銀行等金融機関のミドル・オフィスで使われるリスク管理手法（日本銀行金融機構局［2005a, b］）を参考に、決済サービスにおけるリスクを定量化する方法を検討する。

リスクの評価・管理の手法は決済サービス業者の経営そのものである。キャッシュレス決済には、クレジット・カード、デビット・カード、前払式支払手段等の支払時期の違いや、磁気カード、IC カード、スマートフォン等のデバイスの違い等さまざまな種類があり、それぞれ対象とする脅威は異なるためマネジメント上の重点分野に違いが生じる。そのため、本稿で掲げるのはあくまで一例に過ぎない。

以下では、まず決済サービス業者におけるリスクアセスメント方法を検討する。次いで、アセスメント結果を踏まえて改善策を講じ、改めてアセスメントを行って実際に改善できているかを確認するリスクマネジメント・プロセスを検討する。

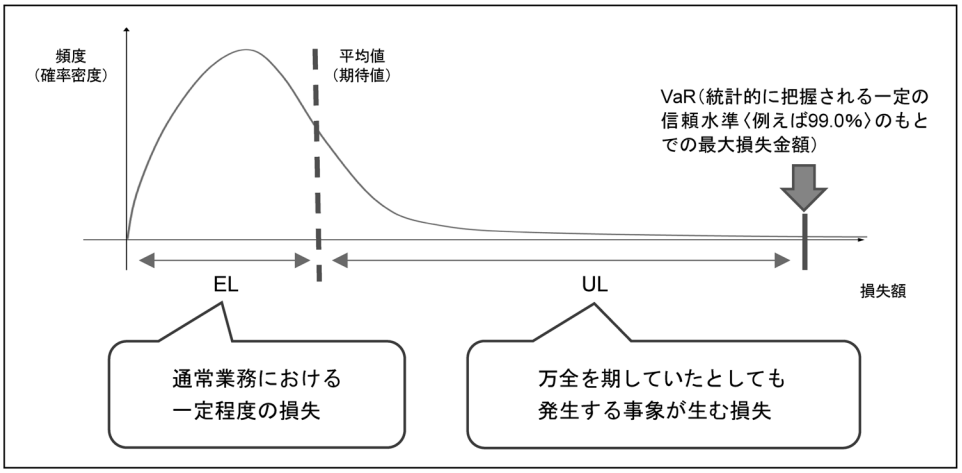
(1) 決済サービス事業に対するリスクアセスメントの特性

まず、事業者自身がサービス提供に伴う事業リスクを把握することが肝要である。

決済サービス事業が損失を被る確率を完全にゼロにすることは難しい。盗難カードや盗難スマートフォンが不正に利用され、決済サービス業者が損失を被ることがありうる。こういった損失は、1 件当たりは比較的少額であるが、一定程度の発生頻度があると考えられる。金融機関におけるリスクマネジメントに当てはめると、通常業務において一定程度発生が見込まれる損失額、すなわち期待損失（Expected Loss: EL）に当たる。金融機関の場合、EL が引当金の範囲内に抑えられる額になるようリスク量を制御している。

22 安全性について、本稿では個別の認証・認可手段をどの程度重畳的に行うべきか、その必要十分性について議論するが、認証・認可以外の安全性の観点にも留意する必要がある。例えば、情報セキュリティ・マネジメント一般については、ISO/IEC 27000 シリーズといった国際標準規格があり、情報セキュリティに関する管理の仕組み（情報セキュリティマネジメントシステム〈Information Security Management System: ISMS〉の確立、導入、運用、監視、レビュー、維持および改善するためのモデル）を提供している。

図表５　決済サービス業者の損失分布グラフの概念図



このほか、異例時等に発生する損失もある。例えば、コンピュータ・システムのバグによってサービスが停止するリスクがある。また、大規模地震等の天災やテロ・戦争によってシステムが破壊されるリスクもある。利用者向けの規約等に免責条項を入れていたとしても、仮にそれが業者側に不当に有利であるとの批判を受ければ、利用者への補償を余儀なくされることも考えられる。

現在の社会において、スマートフォンを用いたキャッシュレス決済サービスは、社会的基盤を成す金融サービスである。決済サービス業者は、万全を期したつもりでも発生しうるリスクが顕現した場合に発生する損失額、すなわち非期待損失（Unexpected Loss: UL）が自己資本の範囲内に抑えられるようリスク量を制御することが必要である。

以上の EL および UL の議論を踏まえると、概念的には決済サービスの損失分布の形状は、日本銀行金融機構局［2005a, b］に示されている金融機関の信用リスクやオペレーショナル・リスクがもたらす損失と類似した、図表 5 のような形のグラフになると考えられる。このグラフの形状については、本節（2）以降で検討したい。

(2)　リスク量の測定方法

決済サービス業者のリスク量を評価する手法は、現在のところ一般化されていない。ここでは銀行等金融機関の信用リスク管理（日本銀行金融機構局［2005a］、家田・丸茂・吉羽［2000］）およびオペレーショナル・リスク管理（日本銀行金融機構局［2005b］）の手法を参考にして、決済サービス業者の損失分布グラフの形状を

検討したい。なお、計量化手法は、解析的に行うもの、シミュレーションによるものがあるほか、シミュレーションには、パラメトリック（特定の統計的な分布形を想定し、その分布に従う数値データをシミュレーションに用いる）やノンパラメトリック（特定の分布形を想定せず、実データをそのままシミュレーションに用いる）等、さまざまな手法が存在する。以下では、実データを活用したシミュレーション手法を例として取り上げる。

リスク量を測定するに当たって、まず、リスク要素（損失発生率、損失発生時の損失額）の推計が必要となる。決済サービス業者の場合は、主なリスクとして、①なりすまし等の不正利用によって発生し損失を被るリスクや、②事務ミスやシステム障害等によって発生しうるリスク等が考えられる。

イ．なりすまし等の不正利用によって発生しうる損失

暗証番号を求められることなくカードをタッチするだけで決済が完了するケースにおいて、仮に認証方式がカードの所有だけである場合、盗難・紛失等による第三者の不正利用が容易に起こりうる。また、店舗掲示型 QR コード決済では、店舗に掲示してある QR コードの上から不正な QR コードを貼り付けるといった事案が発生している（大熊・瀧田・森井［2018］）。こうした場合の利用者の損害に対して、決済サービス業者が補償し、その結果損失を被るケースが考えられる。

こうした損失のリスク量は、貸出債権のデフォルトの考え方を参考にすれば、信用リスク管理の手法を応用して計測できると考えられる。信用リスク管理では、個々の債務者や取引を信用度等に応じて分類・管理する内部格付制度を導入することが多い。決済サービスの場合でも、例えば、顧客のロイヤリティに応じて定められるステージや利用者の属性（職業、年齢、利用期間等）等で顧客をセグメント分けし、ある顧客セグメントにおける全取引数のうちの不正な取引数の割合を求めれば、不正取引割合（信用リスク管理の手法におけるデフォルト率〈Probability of Default: PD〉に該当）が算出できる。また、セグメントごとの不正取引時の補填額のデータを集めることで、デフォルト時エクスポージャー（Exposure at Default: EAD）に該当する不正取引 1 件当たりの補償額を抽出できる[23]。さらにはセグメントごとの相関も計測可能である。

こうして計算した不正取引割合、不正取引時の補償額、セグメント間の相関等を入力情報として、モンテカルロ・シミュレーションを行えば、不正利用の補償等によって発生する損失額にかかる分布を描くことができる（実際のシミュレーションの実施方法については、例えば、肥後［2007］を参照）。

23 金融機関の信用リスク管理において 1 つのリスク要素となるデフォルト時損失率（Loss Given Default: LGD。LGD は「1 – 回収率」で計算できる。）については、決済サービスの場合、一般的に担保等は取得しておらず、デフォルト時における他の回収策が用意されていないことが多いことから「LGD = 1」を想定している。

ロ．オペレーション上のリスクから発生しうる損失

なりすまし以外にも、システムのバグや天災等によってシステムが停止することに伴う損失やプログラム更新時等のオペレーション上の手続きミス、内部不正等のリスクから発生しうる損失もある。こうしたオペレーション上の損害から発生するリスク量の計測にはオペレーショナル・リスク管理における計量化手法が応用できる。オペレーショナル・リスクとは、例えばバーゼル規制では「事務事故、システム障害、不正行為等で損失が生じるリスク」のことを意味している（金融庁・日本銀行［2018］）。

ただ、一般的には障害やオペレーションが原因で損害が発生するケースはまれであり、データが不十分な場合も多い。そのため、オペレーショナル・リスクを計量化する具体的な手法としては、「損失分布手法」を用いることが考えられる。すなわち、「一定期間当たりの損失事例発生件数（ポアソン分布等を用いる場合が多い）」と「1 件当たりの損失金額（ある分布を仮定するパラメトリック手法や過去データを活用するノンパラメトリック手法がある）」を用いて、モンテカルロ・シミュレーションによって「1 年間の累積損失金額分布」を作成し、その「1 年間の累積損失金額分布」の VaR（統計的に把握される一定の信頼水準〈例えば 99.0％〉のもとでの最大損失金額）を算出し、それを「オペレーショナル・リスク量」とする方法である（日本銀行金融機構局［2005b］）。

ハ．決済サービス業者の統合リスク量

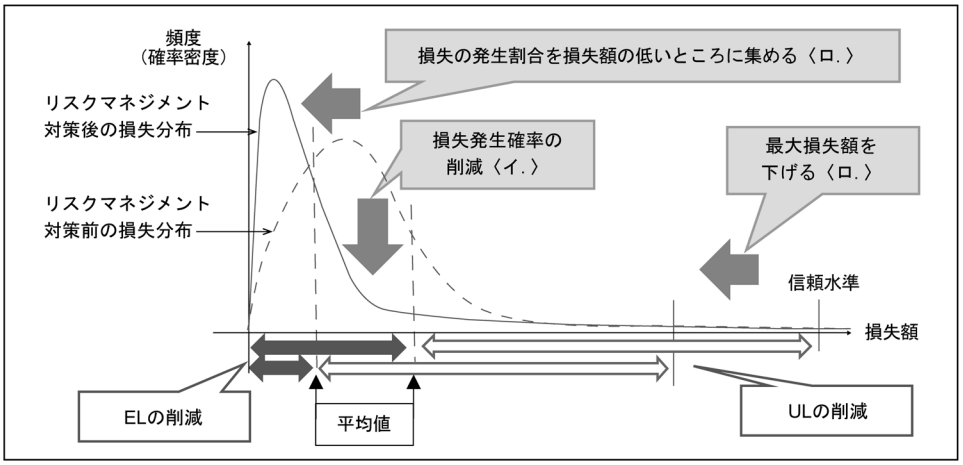
仮に決済サービス業者の損失の多くが、①利用者の認証の失敗による不正利用の補償等によって発生した損失と、②オペレーション上発生する損失である場合は、①と②の損失分布を合算したものが全体の損失分布となる。合算する際、最悪の事態が同時発生することを想定するか（相関係数 1 を想定）、何らかのリスク分散効果を勘案するか（相関係数が 1 未満と想定）によって、合算方法は異なりうる。また、事業者の風評リスク等、その他のリスク量も勘案したうえで、決済サービス業者全体の統合リスクを把握していくこととなる。

(3) リスク対応策の実施とその際の留意点

決済サービス業者にとってのリスクマネジメントは、要すれば、損失が発生する確率を小さくし、損失額を下げ、EL（事業を行う中で一定期間内に平均的に発生が見込まれる損失額）を引当金でカバーできる範囲にし、UL（決済サービス提供に伴う潜在的な損失額）を自己資本の範囲内に抑えることである。

損失が発生する確率を小さくし、損失額を下げるということは、縦軸に損失発生確率、横軸に損失額を取った損失分布グラフで示せば、図表 6 に示すように損失額

図表６　リスク管理した結果描かれる損失分布グラフ



が低いところの頻度をできるだけ高くすることになる。

そこで、以下では損失発生確率を小さくし、損失額を下げるための方法を考察したい。

イ．損失発生確率の削減

損失発生確率を小さくするには、（イ）個人認証の精度を向上させて個人認証における誤認識の確率を下げる、あるいは、（ロ）システムを攻撃されにくくする、という方法が考えられる。

（イ）　個人認証の精度向上

スマートフォンは磁気（ストライプ）カードと比較すると認証の切り口が多い。そのもとで認証手段を組み合わせることにより他人受入率（False Acceptance Rate: FAR）を減らすことができる[24]。

もっとも、認証の切り口や手法、実装方法の違い等によって、精度の違いやなりすましの容易度、データの信ぴょう性が異なる。端末の特定では、①端末に物理的に書き込まれた改変不可能なデータの参照、②セキュア・エレメントの活用、③ユーザが通常の使用ではアクセスできない領域の活用、④クッキーのように誰でもいつでも削除可能な領域への格納等、データの格納場所や格納方法によって、例えばマルウェアに対する耐性等が変わり、ひいては認証精度が変わる（宇根・廣川［2017］）。

端末に搭載された IC チップに物理的に書き込まれた ID や通信業者が管理して

24　一般に FAR を減少させると、本人拒否率（False Rejection Rate: FRR）は増大するというトレードオフの関係にあり、ユーザビリティの観点で留意が必要である。

いる電話番号といった偽装しにくいデータもあれば、位置情報やSNS上の情報等偽装しやすいデータもある。また、ライフスタイル認証のように、ライフスタイルが変化した場合の認証精度の低下や、ライフスタイルを判別するに足る十分な認証データが確保できていない期間はそもそも認証できない等の制約がある手法もある（小林ほか［2016］）。このほか、「利用者の過去の購買履歴」を用いて認証する手法は、基本的には人工知能を用いたビッグ・データ解析によって行われるため、認証能力は人工知能システムの学習状況等に左右される。したがって、実務上は、決済サービス業者自身が試行錯誤を行いながら、認証精度を必要十分なレベルにまで向上させる必要があろう。

また、仮に4節で紹介した個人認証の基盤を決済サービス業者が活用するにしても、その認証基盤の信頼度を決済サービス業者自身が見極めることが大切である。必要に応じて、そうした個人認証の基盤を活用した認証と事業者自身の認証を組み合わせることも検討する必要があろう。

（ロ） 攻撃への対策

一般的に、セキュリティ・レベルの低いシステムは攻撃されやすく、セキュリティ・レベルの高いシステムは攻撃されにくい。そのため、システム側にファイヤーウォール等を導入することにより攻撃されにくくすることが考えられる。また、早期に攻撃への対策を取れる体制を整備しておくことによって、攻撃されにくくすることもできる。このほか、スマートフォン側での対策もある。例えば、アプリにウイルス対策機能を組み込んだり、不正アプリがインストールされていないかのチェック機能を導入したり、スマートフォンがいわゆる「脱獄（スマートフォンの製品に対して業者等が設定している制限事項を規約に反して解除する行為）」されていないかをモニターしたりする等の対策を講じることで、攻撃に対する耐性を高めることができる。

また、利用者の属性によっても攻撃されやすさが変わる。例えば、互いに顔が見えるコミュニティ内のみで通用するローカル通貨のように、相互監視可能な、限られた範囲のみで提供されるサービスの場合、攻撃者がすぐに特定され、決済サービス業者からペナルティが課されると攻撃者自身が不利益を被るため、攻撃しようとする者が現れにくくなり、結果的に攻撃されにくいシステムとなる場合がある。

ロ．リスク顕現時の損失額の削減

リスクマネジメントのもう1つの方向として、損失額の削減がある。提供する決済サービスのビジネスモデルにも影響するが、例えば1回当たりの決済金額に上限を設けたり、1人当たりの決済回数を制限したりすれば[25]、損失額は削減できる。

25 これらの取り組みを行うことで、攻撃者にとっては手間の割に得られるリターンが小さくなるため、攻撃へのインセンティブを低下させられる効果も期待できる。

(4) 対策効果の測定

リスク量をより削減するには、例えば認証精度の向上であれば、4節で掲げた認証を重畳的に組み合わせる必要がある。しかしながら、その適切な組み合わせ方は自明ではない。精度の向上度合いは認証の観点の組み合わせによって異なると考えられ、実際のところテストしてみないと、どの程度精度向上に寄与するのかは把握できない。

本節（3）の整理に基づき行った対策の効果をテストするには、過去のデータをテスト・データとして、対策を講じる前と後との損失発生確率と損失額の関係をグラフ描画し、対策後のグラフが対策前と比較して、左へ移動していること、および、移動幅が意図する程度に生じている（図表6において対策前が点線グラフ、対策後が実線グラフになる）ことを確認する必要がある。そのうえで、損失分布を改めてグラフに描画し、ELが引当金でカバーできること、ULが自己資本の範囲内で賄える額に抑えられることを確認する。その結果、さらなるリスク量の削減が必要な場合は、追加的に認証の切り口を増やして認証精度の向上を図ったり、あるいは攻撃を受けにくいシステムに変更したりする等して対策を講じ、決済サービス業者自身が、事業で生じるリスクをマネジメント可能な範囲に抑える必要がある。

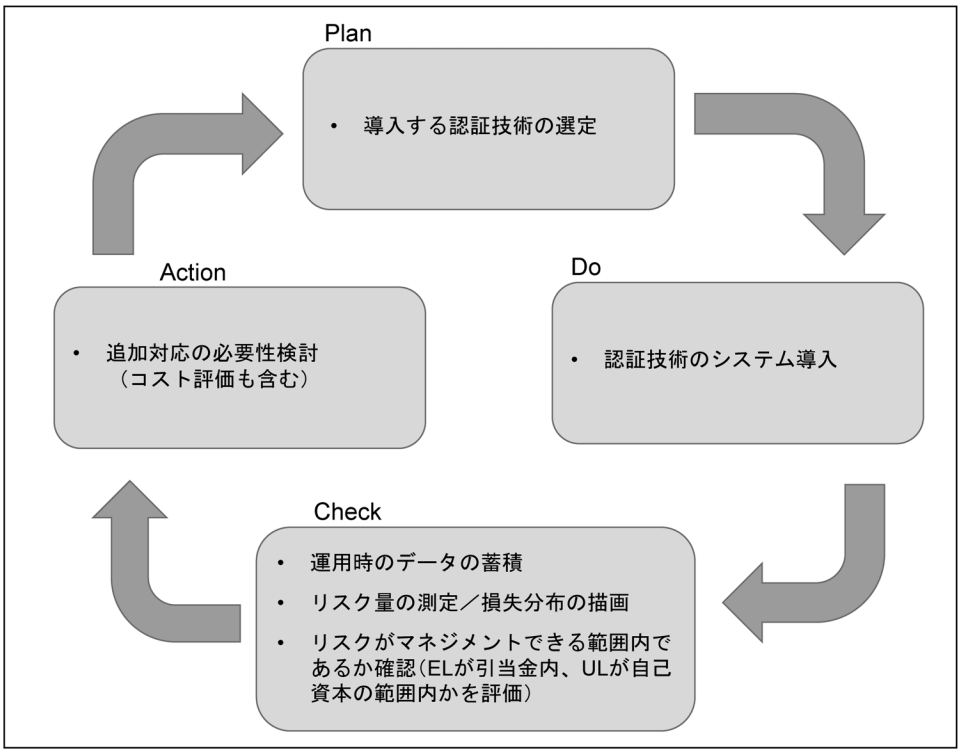
(5) コストの評価

損失発生確率を削減すべく個人認証の精度を高めるためには、それだけ多くのシステムの構築コストやランニング・コストが発生する。攻撃されにくいシステムであると評価できる場合は、自社がリスクテイクできる範囲内でシステム側やスマートフォン側での攻撃対策の一部をあえて省くことで、システム構築や運用に要する費用を抑えることも、経営判断として考えられる。

また、利用者が認証に要する手間も利便性の低下というコスト要因となる。例えば、何度も利用者の記憶を尋ねる質問を行うと、利用者はサービス利用に対しわずらわしさを感じ、サービスを利用しなくなってしまう（例えば、インターネット・ショッピングにおける「かご落ち」の状態となる[26]）。ただ、その一方で、利用者にあえて認証行為を行わせることによって、利用者に認証が適切に行われているという安心感を与え、サービス全体のコスト・パフォーマンスが最適化される場合もある。換言すれば、ユーザ・インターフェース（User Interface: UI）やUXの仕様も1つのコスト評価対象項目であるといえよう。

26 かご落ちとは、インターネット上のショッピング・サイト等で、利用者が商品を選択し、ショッピング・カートに入れたにもかかわらず、途中で買い物を中断してしまうこと。

図表 7　リスクに応じた認証精度の確保に向けた PDCA サイクル



このほか、保険を活用したリスクヘッジも活用されている。しかしながら、全リスクを保険でヘッジすることは難しい。なぜなら、本来、保険会社は、決済サービス業者よりも情報劣位にあるため、保険会社はその分のリスクプレミアムを保険料に上乗せしていると考えられるためである。

(6)　継続的な評価の実施

中長期的には決済ビジネスやシステムが置かれている環境も変化するため、決済サービス業者は PDCA サイクルを回し、リスクに応じた対策がなされているかを不断に把握する必要がある（図表 7）（廣川［2010］、宇根・沖野［2020］）。

キャッシュレス決済サービスの安全性向上のためには、こうした PDCA を通じたセキュリティ強化が欠かせない。認証精度の向上を図ろうとしても、当初の設計段階から将来のシステムのセキュリティ面での拡張性に配慮しておかないと、精度の向上は簡単にはいかない。プライバシー保護同様、情報セキュリティを企画・設

計段階から確保するための方策であるセキュリティ・バイ・デザインに則った設計が重要になる（内閣官房内閣サイバーセキュリティセンター［2019］）。

6. 終わりに ― キャッシュレス決済は「信頼」を基とする金融サービス ―

キャッシュレス決済アプリは、「信頼」を基とする金融サービスを提供している。通常のアプリ以上に、利用者からの高い信頼の獲得が求められる。十分な資本の確保とそれに裏付けされたシステムの認証にかかる安全性の確保が必要である。

こうした課題への対応となる鍵は、円滑な PDCA サイクルの継続である。不具合をすぐに修正し、直ちに利用者へのサービス向上につなげる迅速な対応が求められる。それぞれのスタッフが持ち場で迅速かつ適切に判断し、実行するという組織・文化の醸成が必要になろう。

キャッシュレス決済の利用者を増やすためには、ただ UI や UX が優れた利便性の高いサービスを提供すればよいというものではない。携帯電話を用いたキャッシュレス決済は発展途上国において普及が進んでいるが、その大きな主因は、既存のインフラが十分でないところに、携帯電話を用いたキャッシュレス決済という利便性が高く UX の優れたサービスが登場したからである。ただ、発展途上国のキャッシュレス決済サービスが先進国のサービスと比較して、必ずしもセキュリティ・レベルが高いわけではなく、単に代替手段が少ないことによって使われているにすぎない面もある。実際、インフラが整っている米国やドイツでは、キャッシュレス決済の普及率は高くない（日本銀行決済機構局［2017］）。安全性が伴って初めて利用者増が伴うものであり、日本のようなインフラが充実した国ではなおのことである。利便性の高さは利用者を増やす必要条件にはなるものの、十分条件ではない。

キャッシュレス決済は、デジタル・トランスフォーメーション（Digital Transformation: DX）の一部であり、究極的にはデザイン経営（経済産業省・特許庁［2018］）といったデジタル社会に対応した経営の在り方に直結する。定期的に PDCA サイクルを実行し、潜在的な損失額が経営体力に見合う状態であることを確認するというリスクマネジメントを通じて、持続可能で安定的なキャッシュレス決済サービスの提供が行われることを期待したい。

参考文献

家田　明・丸茂幸平・吉羽要直、「与信ポートフォリオにおける信用リスクの簡便な算出方法」、『金融研究』第 19 巻別冊第 2 号、日本銀行金融研究所、2000 年、109～144 頁

井澤秀益・廣川勝久、「IC カード利用システムにおいて新たに顕現化した Pre-play attack とその対策」、『金融研究』第 34 巻第 4 号、日本銀行金融研究所、2015 年、53～78 頁

磯部光平・坂本一仁・葛野弘樹、「ハードウェアベース暗号鍵管理に関する日本向け Android プラットフォームの調査」、『コンピュータセキュリティシンポジウム 2019 論文集』、情報処理学会、2019 年、1140～1147 頁

宇根正志、「生体認証システムにおける人工物を用いた攻撃に対するセキュリティ評価手法の確立に向けて」、『金融研究』第 35 巻第 4 号、日本銀行金融研究所、2016 年、55～90 頁

――――・沖野健一、「多様化するリテール取引システムのセキュリティ：ビジネスリスク管理に焦点を当てて」、『金融研究』第 39 巻第 4 号、日本銀行金融研究所、2020 年、1～24 頁

――――・廣川勝久、「モバイル端末による金融サービスの安全性を高めるために：セキュア・エレメント等の活用」、金融研究所ディスカッション・ペーパー No. 2017-J-15、日本銀行金融研究所、2017 年

大熊浩也・瀧田　愼・森井昌克、「悪性サイトに誘導する QR コードの存在とそれを利用した偽造攻撃」、『電子情報通信学会技術研究報告』第 118 巻第 109 号、電子情報通信学会、2018 年、33～38 頁

片渕陽平、「『7pay』不正ログイン被害で話題『二段階認証』とは？」、ITmedia NEWS、2019 年（https://www.itmedia.co.jp/news/articles/1907/04/news116.html、2021 年 1 月 7 日）

カブキアン、アン、堀部政男・日本情報経済社会推進協会編、『プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流』、日経 BP 社、 2012 年

金融情報システムセンター、『金融機関等コンピュータシステムの安全対策基準・解説書（第 9 版）』、2018 年

金融庁・日本銀行、「バーゼル III の最終化について」、金融庁、2018 年（https://www.fsa.go.jp/inter/bis/20171208-1/02.pdf、2021 年 1 月 7 日）

黒須正明、「ユーザエクスペリエンスにおける感性情報処理」、『放送大学研究年報』第 30 号、放送大学、2012 年、93～109 頁

――――、「『UX が拓く新しいデザインの世界』特集号について」、『デジタルプラクティス』第 6 巻第 4 号（2015 年 10 月号）、情報処理学会、2015 年、247～248 頁

経済産業省、「キャッシュレス・ビジョン」、経済産業省、2018 年（https://www.meti.

go.jp/press/2018/04/20180411001/20180411001-1.pdf、2021 年 1 月 7 日）
――――・特許庁、「『デザイン経営』宣言」、経済産業省、2018 年（https://www.meti.go.jp/press/2018/05/20180523002/20180523002-1.pdf、2021 年 1 月 7 日）
厚生労働省、「新型コロナウイルスを想定した『新しい生活様式』の実践例を公表しました」、厚生労働省、2020 年（http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000121431_newlifestyle.html、2021 年 1 月 7 日）
個人情報保護委員会事務局、「改正個人情報保護法の基本」、個人情報保護委員会、2017 年（https://www.ppc.go.jp/files/pdf/1706_kihon.pdf、2021 年 1 月 7 日）
小林良輔・疋田敏朗・鈴木宏哉・山口利恵、「行動センシングログを元にしたライフスタイル認証の提案」、『コンピュータセキュリティシンポジウム 2016 論文集』2016(2)、情報処理学会、2016 年、1284～1290 頁
鈴木雅貴・中山靖司・古原和邦、「インターネット・バンキングに対する Man-in-the-Browser 攻撃への対策『取引認証』の安全性評価」、『金融研究』第 32 巻第 3 号、日本銀行金融研究所、2013 年、51～76 頁
瀬戸洋一・長谷川久美、『ISO/IEC 29134 対応 プライバシー影響評価実施マニュアル』、日科技連出版社、2020 年
全国銀行協会、「ZEDI（全銀 EDI システム）」、2020 年、全国銀行協会（https://www.zenginkyo.or.jp/abstract/efforts/smooth/xml/、2021 年 1 月 7 日）
総務省、「スマートフォン プライバシー イニシアティブ―利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション―」、総務省、2012 年（http://www.soumu.go.jp/main_content/000171225.pdf、2021 年 1 月 7 日）
――――、「スマートフォン プライバシー イニシアティブ II ～アプリケーションの第三者検証の在り方～」、総務省、2013 年（https://www.soumu.go.jp/main_content/000358528.pdf、2021 年 1 月 7 日）
――――、『情報通信白書 平成 29 年版』、総務省、2017 年 a
――――、「スマートフォン プライバシー イニシアティブ III」、総務省、2017 年 b（http://www.soumu.go.jp/main_content/000495608.pdf、2021 年 1 月 7 日）
――――、「Society 5.0 を見据えた個人認証基盤のあり方について（報告）」、総務省、2018 年（http://www.soumu.go.jp/main_content/000560721.pdf、2021 年 1 月 7 日）
寺田眞治、『アプリビジネスで転ばないためのスマートフォンプライバシーの基礎知識』、インプレス R&D、2012 年
電子情報技術産業協会、「情報セキュリティ調査報告書」、2014 年（https://home.jeita.or.jp/upload_file/20180126155926_wxHqlf80F9.pdf、2021 年 1 月 7 日）
特定個人情報保護委員会 、「特定個人情報保護評価指針」、特定個人情報保護委員会、2014 年（https://www.ppc.go.jp/files/pdf/shishin.pdf、2021 年 1 月 7 日）
内閣官房内閣サイバーセキュリティセンター、「情報システムに係る政府調達にお

けるセキュリティ要件策定マニュアル」、内閣官房内閣サイバーセキュリティーセンター、2019 年（https://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf、2021 年 1 月 7 日）

内閣官房日本経済再生本部、「未来投資戦略 2018―『Society 5.0』『データ駆動型社会』への変革―具体的施策」、内閣官房内閣広報室、2018 年（https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_d2.pdf、2021 年 2 月 24 日）

日本銀行金融機構局、「内部格付制度に基づく信用リスク管理の高度化」、リスク管理高度化と金融機関経営に関するペーパーシリーズ、日本銀行金融機構局、2005 年 a

――――、「オペレーショナル・リスク管理の高度化」、リスク管理高度化と金融機関経営に関するペーパーシリーズ、日本銀行金融機構局、2005 年 b

日本銀行決済機構局、「モバイル決済の現状と課題」、決済システムレポート別冊シリーズ、日本銀行決済機構局、2017 年

長谷川久美・中田亮太郎・瀬戸洋一、「ISO/IEC 29134:2017 適合のプライバシー影響評価実施マニュアルの開発」、『日本セキュリティ・マネジメント学会誌』 第 32 巻第 3 号、日本セキュリティ・マネジメント学会、2019 年、35～43 頁

肥後秀明、「信用リスク計量モデルの基礎と応用」、日本銀行金融機構局金融高度化センター、2007 年（https://www.boj.or.jp/announcements/release_2007/data/fsc0703c3.pdf、2021 年 1 月 7 日）

廣川勝久、「非接触インタフェース経由取引の技術とビジネスリスク管理の課題」、『金融研究』 第 29 巻 4 号、日本銀行金融研究所、2010 年、79～106 頁

Cavoukian, Ann, “Privacy by Design, The 7 Foundational Principles,” 2011（https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf、2021 年 1 月 7 日）.

Gamba, Julien, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, and Narseo Vallina-Rodriguez, “An Analysis of Pre-installed Android Software,” Proceedings of 41st IEEE Symposium on Security and Privacy, IEEE, 2020.

International Organization for Standardization, “ISO 22307:2008, Financial Services—Privacy Impact Assessment,” International Organization for Standardization, 2008.

――――, and International Electrotechnical Commission, “ISO/IEC 29134:2017, Information Technology—Security Techniques—Guidelines for Privacy Impact Assessment,” International Organization for Standardization, 2017.

――――,“ISO 9241-210:2019, Ergonomics of Human-system Interaction—Part 210: Human-centred Design for Interactive Systems,” International Organization for Standardization, 2019.

National Institute of Standards and Technology, “NIST Special Publication 800-63-3 Digi-

tal Identity Guidelines," National Institute of Standards and Technology, 2017.