ISOパネル第6回（2022年9月15日）

顧客識別と認証技術

― ISO 5158の概要と関連技術 ―

本文書の記載は十分注意しておりますが、国際標準の内容は原文にてご確認ください。本文書はISO 5158そのものの解説ではなく、参考情報です。一般的に使用されている言葉・用法と異なる場合があります。また、各組織の活動内容は、変更されている場合がありますので、ホームページ等にてご確認ください。

本日の説明内容

1. ISO/TC 68とは

2. ISO 5158　Mobile financial services — Customer identification guidelines

（モバイル金融サービス— 顧客識別ガイドライン）

① オンラインでの本人確認方法・確認結果の取り扱い

② 個人情報の保護とモバイル端末のセキュリティ

1.　ISO/TC 68とは

―　ISOおよびTC 68の概要　―

標準化とは

- 「**標準化**」とは、自由に放置すれば、多様化、複雑化、無秩序化する事柄を**少数化、単純化、秩序化すること**。
- 標準そのものは規制ではありません。

標準化の役割

- 消費者の利便性向上
- 効率性向上に伴う市場の拡大、取引コストの削減
- 標準の公開による、新しい技術の普及や産業の発展
- 製品・サービスの相互運用性の向上を通じたネットワーク効果
- 客観的な評価体制による、事業者への信頼性の確保

デジタル社会で注目

イノベーションとルールメイキング

法規制等の既存のルールはイノベーションの社会実装をそもそも想定していない

- イノベーションによる市場の創出には、新しいアーキテクチャと社会実装するための新たなルールの創造が必要

ISO専門委員会

—— 分野ごとに専門委員会（Technical Committee：TC）を設置

橙字：TC68国内委員会とのリエゾン先国内委員会

総会(General Assembly, GA)

理事会(Council)

技術管理評議会(TMB: Technical Management Board) ）

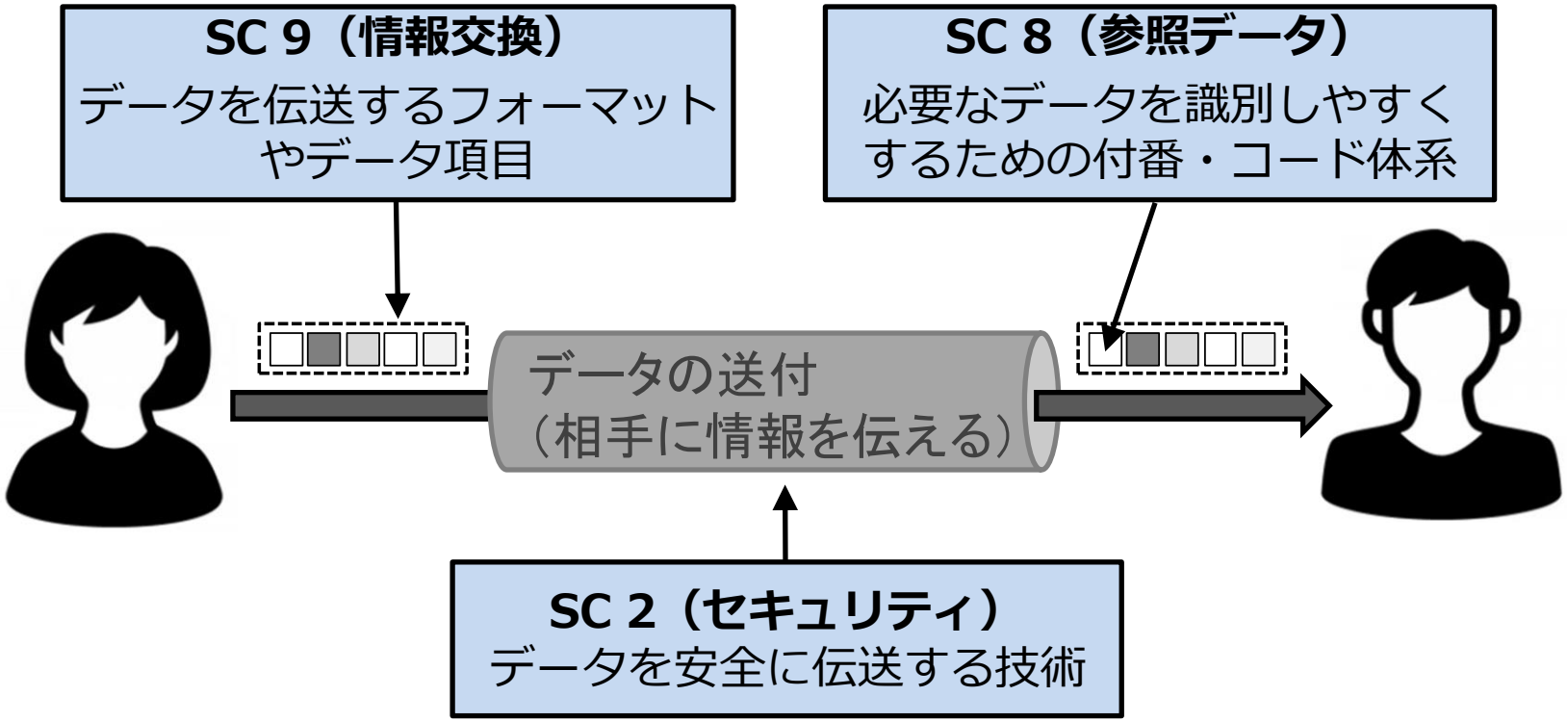
TC 1	ねじ
…	
TC 68	金融サービス（Financial Service）
…	
TC 207	環境管理(Environmental performance evaluation)
TC 251	アセットマネジメント(Asset Management)
TC 260	人事マネジメント（Human Resource Management）
TC 295	監査データサービス（Audit data services）
TC 307	ブロックチェーンと分散台帳技術（Blockchain and Distributed Ledger Technologies）
TC 322	持続可能なファイナンス（Sustainable Finance）
TC 323	循環型経済（Circular economy）
TC 324	シェアリングエコノミー（Sharing economy)
JTC 1	情報技術 <ISOとIECとの合同委員会>

SC 17	カード及び個人識別用セキュリティデバイス
SC 27	情報セキュリティ，サイバーセキュリティ及びプライバシー保護
SC 32	データ管理及び交換
SC 37	バイオメトリクス
SC 38	クラウドコンピューティングおよび分散プラットフォーム
SC 41	インターネット・オブ・シングスおよびデジタルツイン
SC 42	人工知能

金融サービス分野の国際標準化（ISO/TC 68）

- **ISO/TC 68**は、ISOの金融サービス分野の国際標準化を担当する専門委員会。
- 日本銀行決済機構局は、**ISO/TC 68国内委員会事務局**を務めている。

ISO/TC 68の分科委員会（SC：Sub-Committee）



ISO/TC 68について（2022年9月時点）

米国

TC 68

AG 2：Standards Advisory Group (当局とのリエゾン)
AG 3:Best Practices（他のISO規格とのコンパチビリティ確認等）
AG 4：サステイナブルファイナンス
AG 5：デジタル通貨
SG 4：コミュニケーション
TAG 1: FinTech TAG
CAG:Strategic Leadership Group

日本

ISO 20022 RMG
金融メッセージの管理

Payment SEG　：資金決済
Securities SEG　：証券決済
Derivative SubSEG ：デリバディブ
Foreign Exchange SEG：外国為替
Trade SEG　：貿易金融
Cards and Related Retail Financial Services SEG
：カード決済
Cross SEG　：複数SEGの案件
Real-Time Payments Group
：即時決済
Technical Support Group
：技術サポート

英国

SC2
セキュリティ

WG 8 :PKI(公開鍵基盤)
WG11:暗号アルゴリズム
WG13:リテール決済の
セキュリティ（PIN等）
WG16:TPPのセキュリティ
WG17:デジタル通貨の
セキュリティ
WG18:顧客認証技術
（e-KYC）
WG19:バーコード決済の
セキュリティ

スイス

SC8
参照データ

WG 2：BPoS（金融商品説明項目）
WG 3：DTI（デジタルトークン識別子）
WG 7：NPI(自然人識別子)
WG10：FISN
（金融商品短縮名称・略称コード）
SG 5：DWI（デジタルウォーレット識別子）
CAG：Chair's Advisory Group

ISO 5158の
検討グループ

仏国

SC9
情報交換

WG1：セマンティック
モデル
WG3： ISO 8583と
ISO18245の改正
WG4: ISO 20022の改正
TG1：ATICA
（カード取引の
メッセージフォーマット）
AG1: ISO20022 RAの
オーバーサイト

2. ISO 5158　Mobile financial services — Customer identification guidelines

（モバイル金融サービス― 顧客識別ガイドライン）

ISO 5158は、

- 「要求事項」を含まない規格（shallが使われていない）
- 「認証制度」が設定されない規格

eKYCが着目される背景

- モバイル機器の普及に伴い、オンラインでの金融サービスの需要が急速に高まる。
- 本人確認は金融サービスを提供する上で、欠かすことができない業務。
- オンラインで本人確認（eKYCと呼ばれる）を正確に行うことは、利便性・効率性の観点から世界各国で金融サービス提供者にとっての重要な課題

ISO 5158の検討経緯

日付	出来事
2019年5月	eKYCの規格策定提案され、SC 2にSG 3を設置が決定。規格検討がスタート。中国がSG 3の主査を担当。
2020年6月	新規業務提案（NP）投票を実施。採択され、SC 2にWG 18を設置し、規格作成作業がスタート。中国が引き続きWG 18の主査を担当。
2020年9月	SG 3の解散を決定。
2022年2月	ドラフト案が完成し、DISステージに到達。ドラフト案の販売がスタート。

今回の発表内容

①　オンラインでの本人確認方法・確認結果の取り扱い

- 一般的なオンライン本人確認手順
- 本人確認の保証レベルにかかる評価方法
- 本人確認の評価方法のケーススタディ

②　個人情報の保護とモバイル端末のセキュリティ

- 顧客の個人情報保護
- モバイル機器のセキュリティに対する配慮

今回の発表内容

①　オンラインでの本人確認方法・確認結果の取り扱い

- 一般的なオンライン本人確認手順
- 本人確認の保証レベルにかかる評価方法
- 本人確認の評価方法のケーススタディ

②　個人情報の保護とモバイル端末のセキュリティ

- 顧客の個人情報保護
- モバイル機器のセキュリティに対する配慮

一般的なオンライン本人確認手順

属性とアイデンティティ

属性（Attribute）：

ある自然人が持つ特徴あるいは所有しているもの

(例)

- 生体固有の情報（顔の輪郭、指紋、虹彩など）
- 各自然人が選択して取得した情報
  （住所、電話番号など）
- 国家等が割り当てた情報（免許書番号など）
- 個人の行動情報（位置情報など）

アイデンティティ（Identity）：

属性の集合体

一般的なオンライン本人確認手順

オンラインで本人確認を行う際に用いる属性

ISO 5158では、 ISO 24366＜自然人識別子（NPI：Natural Person Identifier）のデータレコードを推奨。

- 地理的な位置（自宅の住所またはオフィスの住所）、雇用状況、緊急連絡先など属性の追加も考えられる。

自然人識別子（ISO 24366）が定める自然人の属性を示すデータレコード

注：ISO 24366”Natural Person Identifier”は、英数字15桁からなる自然人のID番号に関するISOの国際標準

データ要素	必須か否か
法律上の名前　― 名字	必須情報
法律上の名前　―ミドルネーム	オプション
法律上の名前―下の名前	必須情報
別名	オプション
別名の種類（定義に沿ったコードを入力）	オプション
誕生日	必須情報（例外あり）
産まれた国	必須情報（例外あり）
電話番号	オプション
電話番号の種類	必須情報（登録有の時）
電子メール	オプション
電子メールの種類	必須情報（登録有の時）

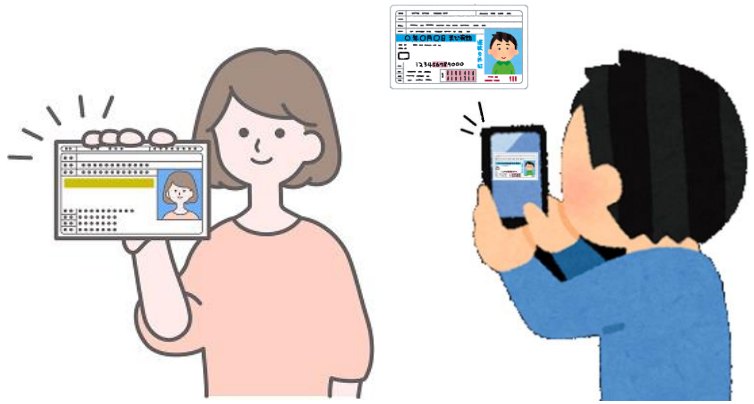
データ要素	必須か否か
国籍	必須情報
住所	必須情報
住所の種類	必須情報
法域（国家）が発行したID番号	必須情報
法域（国家）が発行したIDの種類	必須情報
IDを発行した法域(国家)	必須情報
性別	オプション
生体情報	オプション
情報のステータスを表すフラグ	必須情報
情報の変更理由	オプション
情報変更日	必須情報
確認フラグ	必須情報
確認にあたっての元情報	必須情報

出典：ISO 24366を参考に作成

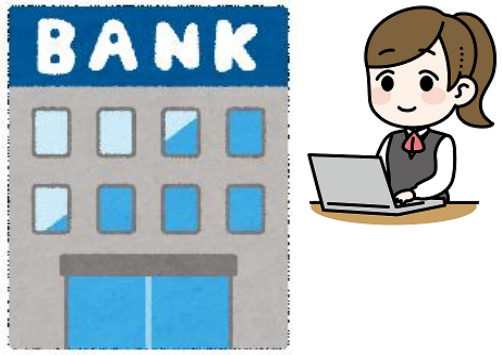
一般的なオンライン本人確認手順

初回登録時

属性情報と証拠の提示



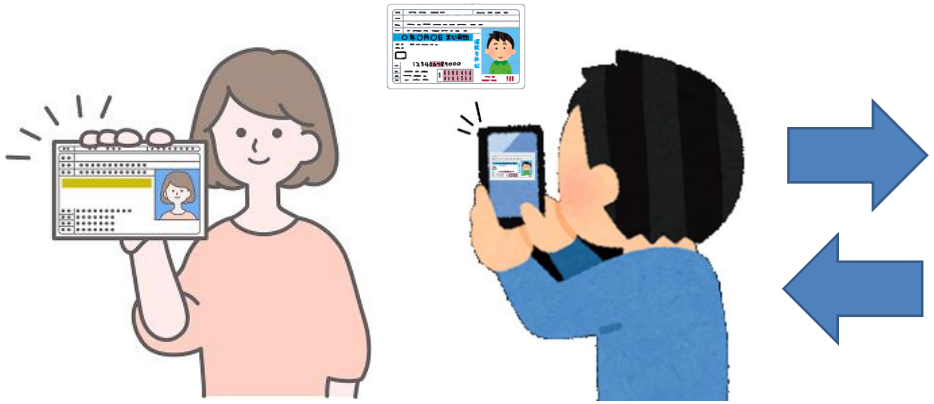
属性情報と証拠の確認



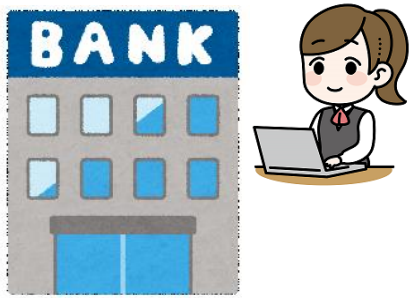
属性情報と証拠の保管

サービス利用時

属性情報と証拠の提示



属性情報と証拠の確認



本人確認結果に基づき
サービス提供

属性情報の照合

一般的なオンライン本人確認手順

▽　eKYCで用いられる顧客が提示する証拠の具体例

デジタル化された物的証拠	運転免許証やクレジットカードの顔写真など。
デジタル アイデンティティ	デジタル署名を生成することができるICカードなどに格納されたトークン、所有者の生体等の属性（指紋など）を含むデジタル証明書やソフトウェアなど。
オンライン上のアイデンティティ情報データベース	携帯電話会社の顧客データにアクセスするインターフェース、政府機関が運用するアイデンティティ情報オーソリティ（IIA：identity information authority）にアクセスするインターフェースなど

▽　生体認証の場合の顧客が提示する証拠の具体的手法

身分証明書のICチップに格納されている生体情報（クライアント照合）
サーバに保存されている生体情報（サーバー照合）

一般的なオンライン本人確認手順

本人確認のプロセス

顧客が、金融サービス提供者が求める「検証可能な属性」や「属性を裏付けられる証拠」を提示。

このとき以下の方法が考えられる：

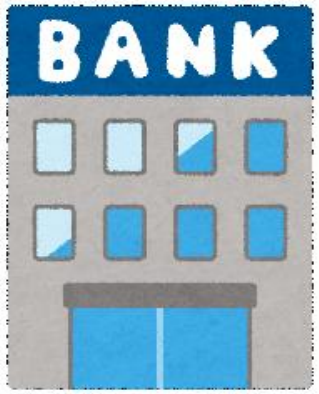
- 顧客に情報を提示してもらう方法。例：
  - ✓ 顧客に記入表を示し、名前や住所などの情報を文字で入力してもらう。
  - ✓ 顧客に自撮り写真（顔写真）をアップロードしてもらう。

- 属性を裏付ける証拠から判読する方法。例：
  - ✓ 顧客に、免許書等、IDカードの写真をアップロードしてもらう（その際、一定の偽造防止措置が施された機器を用いる）。
  - ✓ 顧客に特定属性を含むデジタルID文書（通常はデジタル署名付き）の提示してもらう。

- データベースから取得する方法。例：
  - ✓ 専門の第三者機関であるアイデンティティ情報プロバイダー（Identity information provider：IIP、認証・認可・属性情報を提供する業者）から属性を取得する。
  - ✓ ドメイン固有のアイデンティティ情報オーソリティ（Identity Information Authority：IIA、属性の妥当性や正当性を証明できるところ）から属性を取得する。

一般的なオンライン本人確認手順

本人確認のプロセス



金融サービス提供者は、あらゆる手段を用いて、顧客から提供された属性や証拠の真正性、有効性、適格性を検証。

金融サービス提供者は、あらゆる手段を用いて、顧客から提供された属性や証拠と顧客本人の関連性を検証。加えて、顧客が金融サービス提供者の提供するサービスに申し込む意思があることを検証。

- 確認後、顧客の属性情報はデータベースに登録
- 属性情報は継続的に維持管理（追加／削除／更新）する必要

今回の発表内容

①　オンラインでの本人確認方法・確認結果の取り扱い

- 一般的なオンライン本人確認手順
- 本人確認の保証レベルにかかる評価方法
- 本人確認の評価方法のケーススタディ

②　個人情報の保護とモバイル端末のセキュリティ

- 顧客の個人情報保護
- モバイル機器のセキュリティに対する配慮

本人確認の保証レベルにかかる評価方法

保証レベルの定義

保証レベル：顧客から提示された属性やその証拠を、本人と結びつけられている程度を示すベクトル

金融サービス提供者の顧客xの全体的な顧客本人であることの保証レベル（$\overrightarrow{AL\_IDx}$）：

$$\overrightarrow{AL\_IDx} = (ALu, ALe, ALp, ALw, ALr, \dots)$$

ベクトルの要素：

（1） ALu：アイデンティティの一意性

（2） ALe：アイデンティティと実在人物との対応

（3） ALp：提示された属性が顧客本人と一致する度合い

（4） ALw：サービスに申し込む意思

（5） ALr：顧客への連絡可能性

評価軸は5つに限られない
追加・削除も考えられる

金融サービス提供者が、顧客の提示した属性で顧客本人だと認識するのは、保証レベルの（$\overrightarrow{AL\_IDx}$）の値が、そのサービス提供者があらかじめ定めた閾値に該当するかどうかで判断

本人確認の保証レベルにかかる評価方法

（１）顧客を特定できる確率（*ALu*）の評価基準

*Alu*は、金融サービス提供者が顧客を特定できる情報の取得度合いを示す値

*ALu*値	状況	評価の基準
0	顧客を一意に特定できる保証がない	顧客は、登録やログインしなくてよい。
0を超え1未満	顧客を一意に特定できるかが不明確	サービスの提供に際して、顧客は、名前や位置など、一部の属性情報を提供している。
1	顧客を確実に一意に特定できる	サービスの提供に際して、顧客は、固有の属性（国民ID番号や生体情報など）、あるいは、複数の属性情報の組み合わせによって個人の特定が可能な情報を提供している。

出典：ISO 5158　Table1を参考に作成

本人確認の保証レベルにかかる評価方法

（２）顧客が提示する証拠の正確性（ALe）の評価基準

ALeは、顧客が提示する証拠の信頼度を示す確率。

ALe値	状況	評価の基準
0	信頼できない証拠	証拠が無効、 または、 証拠の発行者が、提供者のKYC方針に合致していない、もしくは、LoIP1(ISO/IEC TS 29003)、IAL1(NIST)と同等である。
0を超え0.9未満	部分的には信頼できる証拠	証拠の発行者が、 (a)①提供者のKYC方針に合致している、または、②LoIP2/3 (ISO/IEC TS 29003)、IAL2/3(NIST)と同等、 かつ、 (b)①リモートで検証可能な物的証拠の偽造防止策、または、②デジタルエビデンスの真正性・完全性を検証可能なデジタル署名などのセキュリティ手段を提供している。
0.9以上1未満	本物で有効な証拠	証拠の発行者が、 (a)①提供者のKYC方針に合致している、または、②LoIP2/3 (ISO/IEC TS 29003)、IAL2/3(NIST)と同等、 かつ、 (b)①デジタルエビデンスやアイデンティティ情報プロバイダー（IIP）からの情報が提供され、②デジタル署名やセキュアな通信プロトコルなどのセキュリティ手段で保護され、③失効チェックメカニズムで真正性・有効性も検証される 。

出典：ISO 5158　Table2を参考に作成

［参考］ ISO/IEC TS 29003・NISTでの本人確認強度

ISO/IEC TS 29003（Identity proofing：本人確認）による本人確認のレベル（LoIP： Levels of identity proofing）の定義

レベル	定義	属性確認	本人とIDとの結びつき確認
LoIP 1	本人であることの信頼度が低い（IDがコンテキスト内で一意であり、存在するとの仮定があり、かつ、申請者とIDとの結びつきがあるとの仮定がある）。	何の確認も行われていない。	何の確認も行われていない。
LoIP 2	本人であることの信頼度は中程度（IDはコンテキスト内で一意であり、存在することが中程度に立証されており、IDに対して何らかの拘束力がある）。	属性には裏付けとなる証拠が存在する。	本人とIDとの結びつきが1つの因子で確認された。
LoIP 3	本人であることの信頼度は高い（ID はコンテキスト内で一意であり、ID の存在 が強く立証されており、本人は ID に対して強い拘束力を持っている）。	属性には権威ある証拠が存在する。	本人とIDとの結びつきが2つ以上の要素を用いて確認された。

出典：European Union Agency for Cybersecurity(ENISA) “eIDAS COMPLIANT eID SOLUTIONS” Figure 4 を参考にISO/IEC TS 29003を参照しながら作成

米国立標準技術研究所（NIST）の「電子的認証に関するガイドライン(Electronic Authentication Guideline)」第3版(NIST SP 800-63-3)における、サービス提供者が行う本人確認の厳密さ、強度を示す IAL (Identity Assurance Level)

Lv.1	本人確認不要、自己申告での登録でよい。
Lv.2	サービス内容により、識別に用いられる属性をリモートまたは対面で確認する必要がある。
Lv.3	識別に用いられる属性を対面で確認し、確認書類の検証担当者は有資格者が行う必要がある。

出典：JIPDEC, ”NIST SP 800-63-3の概要と今回の改訂がもたらす影響”を参考にNIST SP 800-63-3を参照しながら作成

本人確認の保証レベルにかかる評価方法

（３）属性や証拠が顧客本人のものであることの保証レベル（*ALp*）の評価基準

*ALp*は、提示された属性や証拠が顧客本人のものである確率。

▽　属性や証拠が顧客本人のものであることを確認する方法

知識認証	支払履歴
生体認証	顔・指紋・声紋などでの認証
所持品認証	店舗等の物理的な場において、顧客が従業員に、パスポート、カード、または登録済みの電話などを提示して行う認証

本人確認の保証レベルにかかる評価方法

（３）属性や証拠が顧客本人のものであることの保証レベル（*ALp*）の評価基準

*ALp*は、提示された属性や証拠が顧客本人のものである確率。

*ALp*値	状況	評価の基準
0を超え 0.1未満	申請者が登録顧客である可能性は低い。	①知識ベース認証（例：支払履歴）、もしくは、②登録生体情報へのリスク等の管理策 がない生体認証。
0.1以上 0.9未満	申請者が登録顧客であることをある程度保証。	リスク管理措置 （例：支払履歴の場合は、申請の場所、操作習慣等の確認）を実施した知識ベース認証、登録生体情報への一定のリスク等の管理策 を実施した生体認証。
0.9以上 1未満	申請者が登録顧客である確度が高い。	対面での確認と同等の方法（例：登録生体情報への十分なリスク等の管理策 を実施した生体認証）。

出典：ISO 5158　Table3を参考に作成

[参考]様々な考え得る認証方法

注：実運用に当たっては法律等ルールへの準拠に留意

知識認証

所持品認証

生体認証

- 物理的生体認証（biophysical biometrics）：指紋、顔、虹彩、静脈パターンなど、物理的な生体物を用いた認証
- 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。

位置情報

- 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、店舗の端末設置場所）
- 利用者の行動パターンに関する情報（スマートフォンの位置と時刻を日々蓄積することでの利用者の行動履歴を把握）

購買履歴

利用者の過去の購買履歴

運動履歴

活動量（歩数計）やスマートウオッチ等の脈拍データなどのパターン

インストールアプリ

アプリの日々の利用状況、インストールされているアプリの数や種別等の変化

ライフスタイル認証

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

利用者の友人関係

過去の個人間送金の相手
SNSの友だち情報
スマートフォン内の電話帳情報等

参考：橋本崇、「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」、金融研究 第40巻第2号（2021年4月）
https://www.imes.boj.or.jp/research/abstracts/japanese/kk40-2-3.html

[参考] 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
意味	利用者の意思に基づいて行う認証	金融サービス提供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
主体	利用者本人（証明者）	金融サービス提供者（検証者）
認証方法	①「もの」（所有による認証） ②「情報」（記憶による認証） ③「生体情報」（生体認証） ⇒ 事業者が認証面での安全性を向上させる観点で、事業者の利用識別行為とて認証を行うことを検討する必要がある。	③ 生体情報 ④ 位置情報（スマホ） ⑤ インストールアプリ（スマホ） ⑥ 運動履歴（スマホ） ⑦ 利用者の過去購買履歴 ⑧ 利用者の友人関係 （個人間送金、SNS、電話帳） ⇒ ライフスタイル認証 ⇒ 揺らぎが生じる ⇒ 他の認証方法と合わせて活用することで安全
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（ある場合もある）

参考：橋本崇、「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」、金融研究 第40巻第2号（2021年4月）
https://www.imes.boj.or.jp/research/abstracts/japanese/kk40-2-3.html

本人確認の保証レベルにかかる評価方法

（４）サービスに申し込む顧客の意思確認の保証レベル（*ALw*）の評価基準

*ALw*は、金融サービス提供者が、申し込む顧客の意思や意図を正しく確認できているかを示す値。

具体的な顧客の意思の確認方法：

- 利用規約を読んでもらい同意を得る。
- 明示的に特定の書式に情報入力を求める。
- リモートビデオ会議にて、顧客に金融サービスに関する質問に答えてもらう。
- 店舗窓口、または訪問先で金融機関の従業員が直接立ち会い、質問する。

*ALw*値	状況	評価の基準
0を超え 0.1未満	申請者の意思を黙示的に確認。	取引条件の確認(チェックボックス等へのチェック)。
0.1以上 0.5未満	申請者の意思を明示的に確認。	明示的な記載による確認。
0.5以上 0.9未満	申請者と リアルタイムで会話し意思を確認。	遠隔ビデオ対話での個別の質問による確認。
0.9以上 1未満	物理的な確認。	窓口や訪問などで個別の質問を伴う物理的な確認。

出典：ISO 5158　Table4を参考に作成

本人確認の保証レベルにかかる評価方法

（５）顧客への連絡可能性（ALr）の評価基準

ALrは、金融サービス提供者が、必要なときに確実に顧客と連絡が取れる情報を取得しているかを示す値

―― 顧客の属性とは直接関係ないが、顧客の本人確認に関する全体的なリスク管理のために必要な情報

ALr値	状況	評価の基準
0	保証なし	物理的な住所、電話番号、電子メール、その他連絡先情報が未確認。
0を超え0.9未満	オンラインでの保証	①顧客が連絡先情報を提示し、 電話をかける、メールや携帯電話のワンタイムパスワードなどの手段で確認できる。②物理的な住所が身元証明書と照合できる。
0.9以上1未満	対面での保証	①顧客が物理的な住所を提示し、郵便などの手段で事実が確認できる。②従業員が顧客を直接訪問し確認できる。

出典：ISO 5158　Table5を参考に作成

今回の発表内容

①　オンラインでの本人確認方法・確認結果の取り扱い

- 一般的なオンライン本人確認手順
- 本人確認の保証レベルにかかる評価方法
- 本人確認の評価方法のケーススタディ

②　個人情報の保護とモバイル端末のセキュリティ

- 顧客の個人情報保護
- モバイル機器のセキュリティに対する配慮

本人確認の評価方法のケーススタディ

（１）中国の金融機関口座

中国の金融機関の口座では、本人確認の要件に応じて以下の3つ分類している

分類	KYC要件	制約事項	$\overrightarrow{AL_IDx}$の要素値での要件表記
I類	対面での確認	入金、出金、投資、送金、購入物の決済、請求書支払に利用可能。 口座残高や取引額に制限はない。	$ALu = 1$ $ALe \geqq 0.9$ $ALp \geqq 0.9$ $ALw \geqq 0.9$ $ALr \geqq 0$
II類	遠隔での確認可 同一の名前のＩ類銀行口座が必要。生体認証の利用を推奨。	入金、投資、購入物の決済、請求書支払に利用可能。 口座からの支払いは1日10,000元までの制限有。	$ALu = 1$ $ALe \geqq 0.9$ $ALp \geqq 0.1$ $ALw \geqq 0.1$ $ALr \geqq 0$
III類	遠隔での確認可。同一の名前のＩ類銀行口座からが必要。生体認証利用を推奨。	購入物の決済、請求書支払いに利用可能。 口座残高が1,000元未満の制限有。	$ALu = 1$ $ALe \geqq 0.9$ $ALp \geqq 0.1$ $ALw \geqq 0.1$ $ALr \geqq 0$

注：II類とIII類は、顧客が選択することによって分類が異なる。

出典：ISO 5158 Table B.1、Table B.2、および、白木 幹二「中国における個人預金口座開設の規制強化について」 、宋 良也「中国のネット専業銀行への取り組み－『百信銀行』について」 を参考に作成

本人確認の評価方法のケーススタディ

（2）マレーシアの決済サービス事業者の場合

マレーシアのペイメントアカウント（銀行以外の決済サービス事業者が、主に支払いを目的として使用するアカウント）の場合は、顧客確認（Customer Due Diligence：CDD）の状況に応じて2つの分類

分類	KYC要件	制約事項	$\overrightarrow{AL_IDx}$の要素値での要件表記
Non-CDD	必要なし	最大残高:5,000MYR 1回の取引上限:3,000MYR 購入物の決済のみ利用可（現金化は不可）	$ALu \geqq 0$ $ALe \geqq 0$ $ALp \geqq 0$ $ALw \geqq 0$ $ALr \geqq 0$
CDD	承認済身分証明書の提示と、氏名・識別番号・国籍・住所・携帯電話番号・誕生日・取引目的の情報提供	•送金可能 •為替取引可能 •現金化可能 ウォレット内の金額に上限あり （上限値は事業者が設定）	$ALu = 1$ $ALe > 0$ $ALp \geqq 0$ $ALw \geqq 0$ $ALr > 0$

出典：ISO 5158　TableB.3、TableB.4およびSTICPAY「海外送金ポリシー：マレーシア」を参考に作成

今回の発表内容

① オンラインでの本人確認方法・確認結果の取り扱い

- 一般的なオンライン本人確認手順
- 本人確認の保証レベルにかかる評価方法
- 本人確認の評価方法のケーススタディ

② 個人情報の保護とモバイル端末のセキュリティ

- 顧客の個人情報保護
- モバイル機器のセキュリティに対する配慮

顧客の個人情報保護とモバイル端末のセキュリティ

本人確認のプロセス　―　個人情報保護とセキュリティの重要性

① 属性情報と証拠の提示

属性情報と証拠の確認
② 真正性、有効性、適格性を検証
③ 顧客本人との関連性を検証

データの
照合・確認

扱う情報は
個人情報中心

個人情報保護策・セキュリティ対策は
eKYC運営の上でとても重要

顧客の個人情報保護

（１）一般的な個人情報保護

個人情報の扱いでは、ISO/IEC 29100（プライバシーフレームワーク）が掲げる原則に従う。

ISO/IEC 29100の定めている内容

- 個人識別可能情報の定義
- 一般的なプライバシーについての用語の規定
- 個人識別可能情報の処理に携わる者及びその役割の定義
- プライバシー安全対策要件の説明

▽　ISO/IEC 29100の定めるプライバシー安全対策要件（11項目）

- 同意と選択
- 目的の正当性と規定
- 収集の制限
- データ最小化
- 利用、保持、開示の制限
- 正確性と品質
- オープンさ、透明性、通知
- 個人の参加とアクセス
- 説明責任
- 情報セキュリティ
- プライバシー法令遵守

出典：JIPDEC、「プライバシーに関する国際標準化動向及びEDPB ガイドライン」、図表5を参考に作成

- この11の原則に基づいて事業者が、具体的なプライバシー技術の実装と利用、全体的なプライバシーマネジメント、外部委託したデータ処理のプライバシー管理策、プライバシーリスクアセスメントなど、詳細な個人情報保護の取り組みを定めて実施することを求めている。

顧客の個人情報保護

（２）生体情報の個人情報保護

- 生体情報は個人情報保護面で特に慎重な取り扱いが必要。
  - 生体情報は、通信途上での傍受・記録・改竄の可能性があり、異なるコンポーネント間で伝送するとシステムが脆弱になるリスクがある。

- 個人情報の扱いでは、ISO/IEC 24745（バイオメトリック情報の保護）の要求事項に従う。

- ISO/IEC 24745が提示する生体認証データの示す対象者のプライバシーを保護する対策方法
  - バイオメトリクス及びバイオメトリクス・システム・アプリケーション・モデルに固有の脅威と対策の分析手法
  - 生体参照情報（biometric reference：BR）とアイデンティティ参照情報（identity reference：IR）とを安全に結びつける際のセキュリティ要件
  - 生体参照情報の保管や比較の際に用いるバイオメトリクス・システム・アプリケーション・モデル
  - バイオメトリクス情報の処理中における個人のプライバシー保護に関するガイダンス

今回の発表内容

① オンラインでの本人確認方法・確認結果の取り扱い

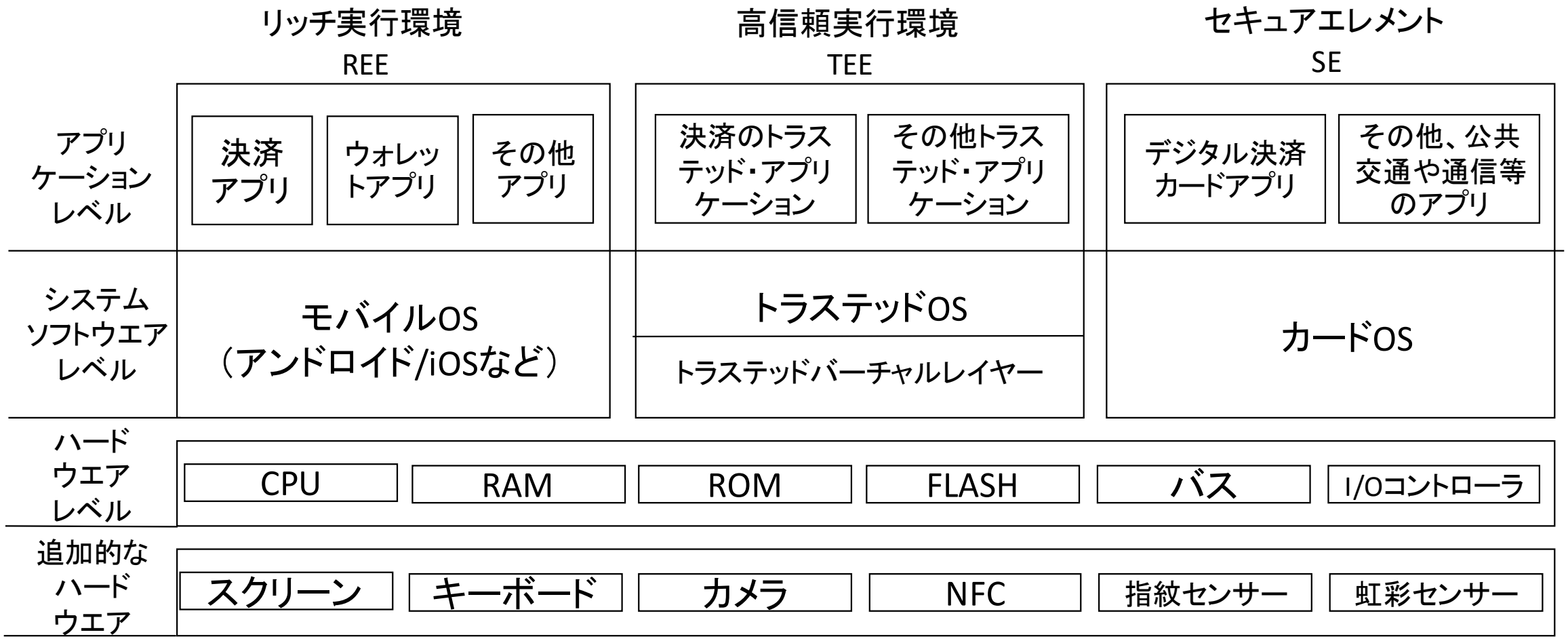
- 一般的なオンライン本人確認手順
- 本人確認の保証レベルにかかる評価方法
- 本人確認の評価方法のケーススタディ

② 個人情報の保護とモバイル端末のセキュリティ

- 顧客の個人情報保護
- モバイル機器のセキュリティに対する配慮

モバイル機器のセキュリティに対する配慮

- モバイル機器のどの環境にどのアプリケーションを実行させるべきかの整理

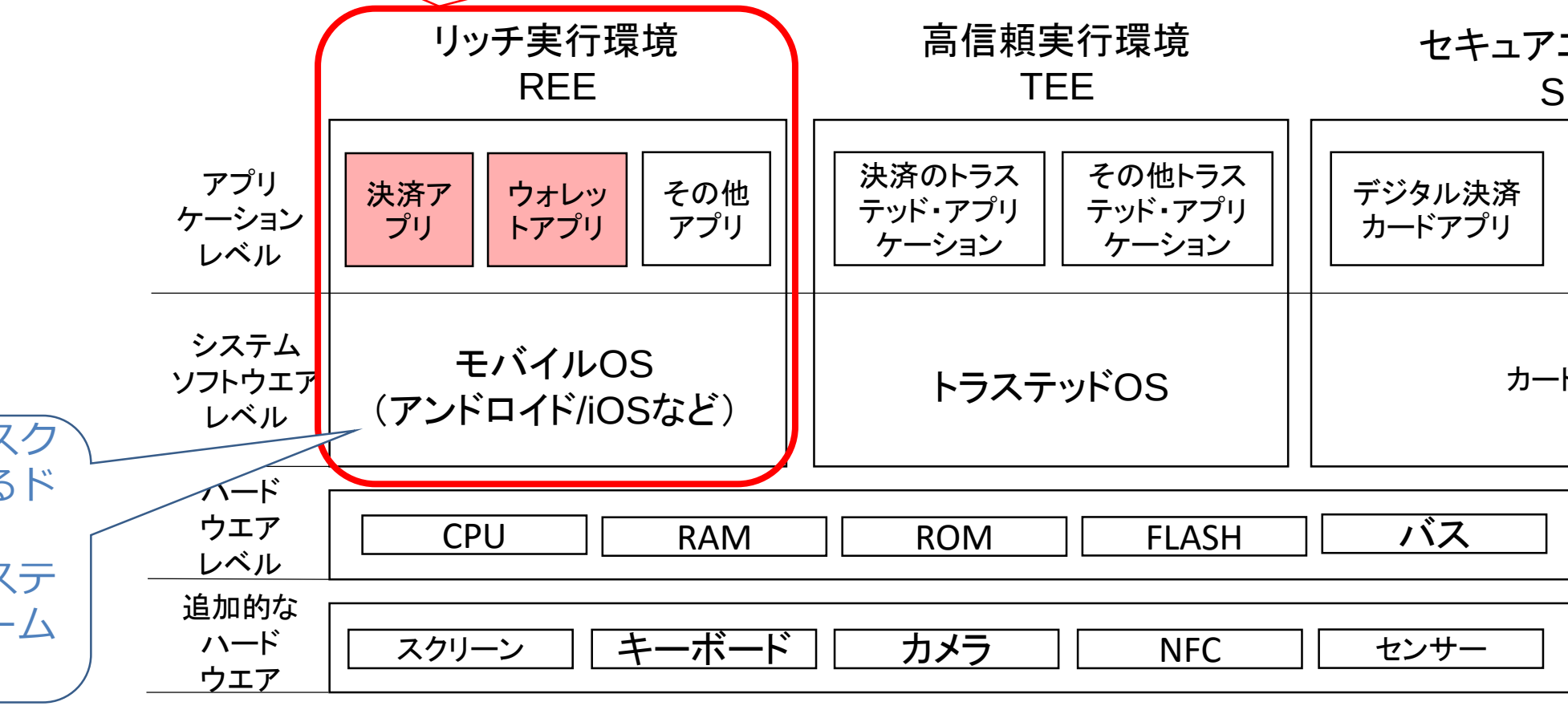


出典：ISO 5158　FigureA.1

モバイル機器のセキュリティに対する配慮

（１）REE（リッチ実行環境：Rich Execution Environment）

REE:一般的なアプリを実行



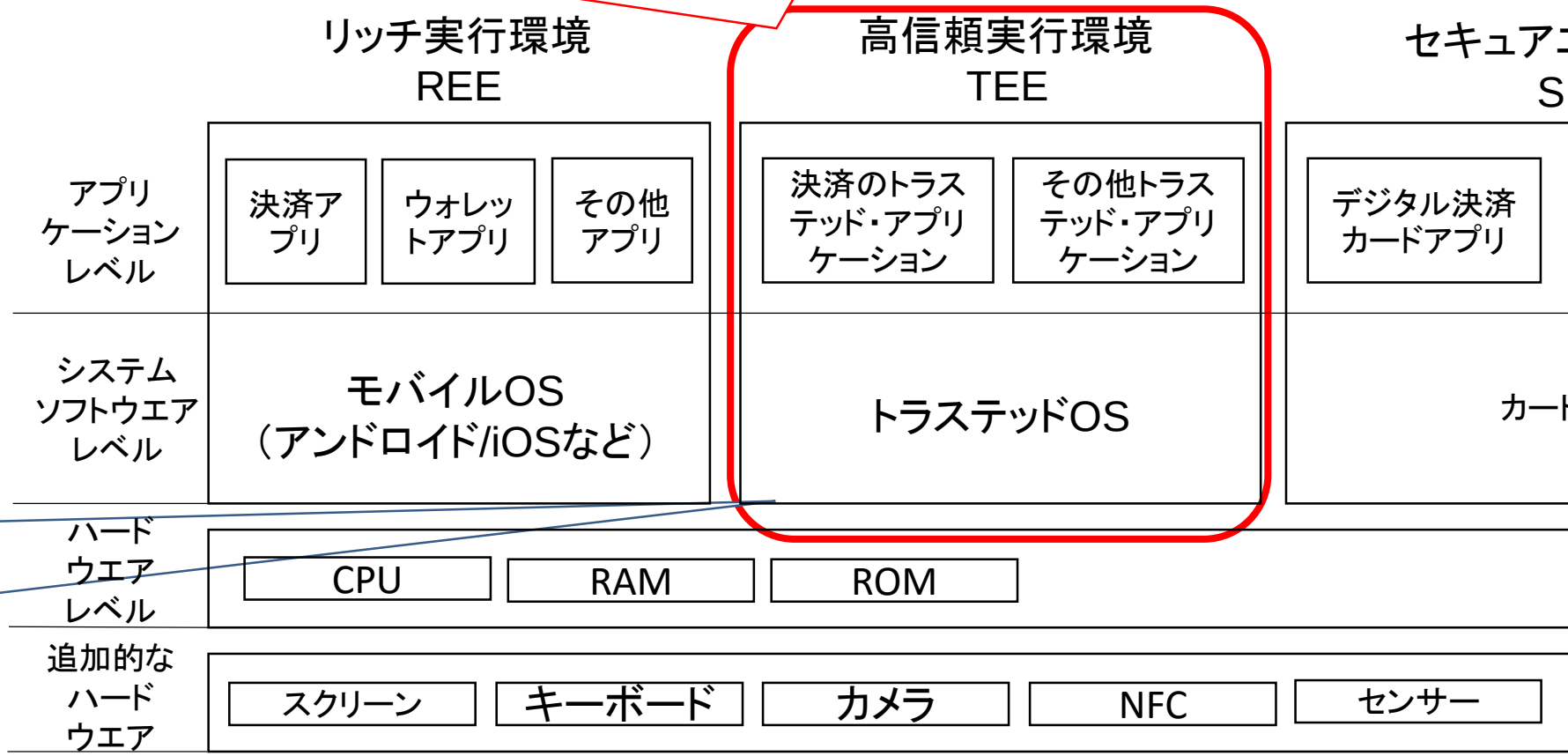
カメラ、USB、タッチスクリーンなどを動作させるドライバー
アプリを動作させるシステムサービスや管理フレームワークの実行

出典：ISO 5158　FigureA.1を参考に作成

モバイル機器のセキュリティに対する配慮

（２）TEE（高信頼実行環境：Trusted Execution Environment）

TEE:指紋認証、支払い、ID認証など重要な
金融サービス機能を提供するアプリを実行



①認証の実行、
②秘密鍵の操作、
③REE、SE、および外部デバイスとの安全な通信・アクセス制御を実行

出典：ISO 5158　FigureA.1を参考に作成

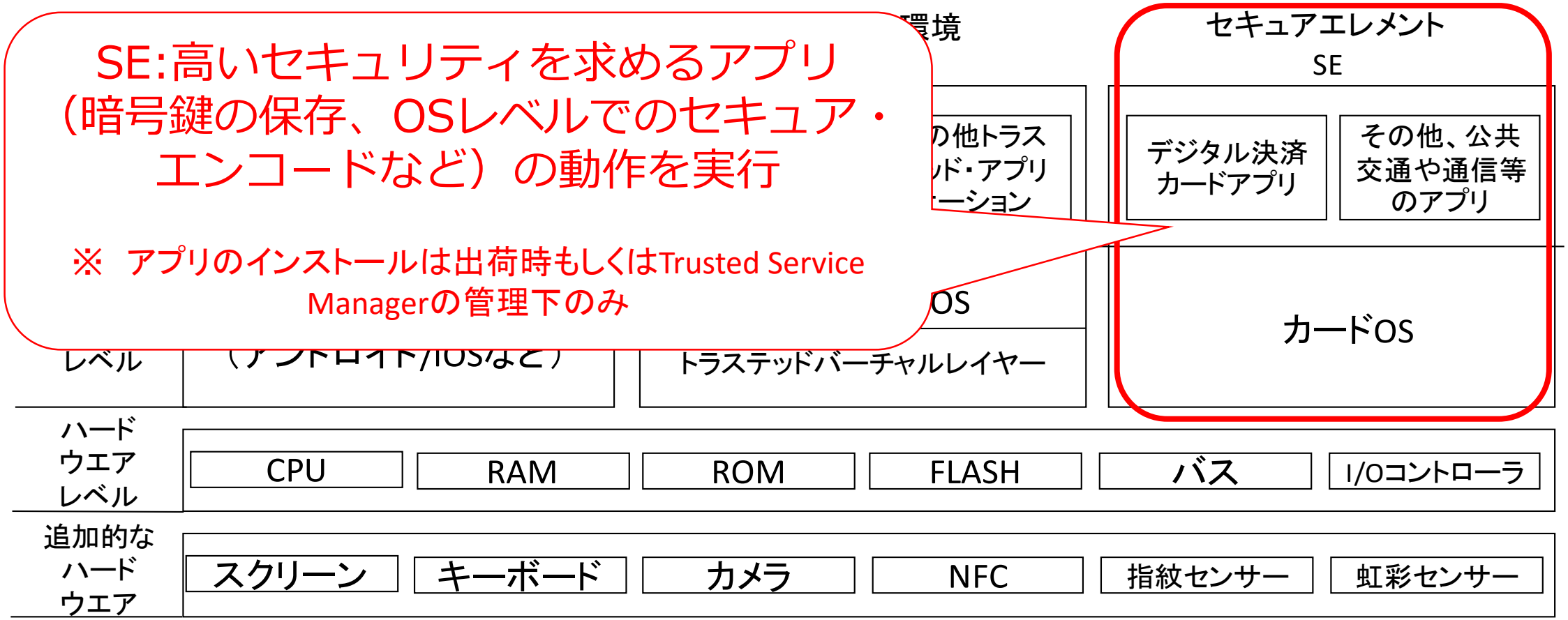
モバイル機器のセキュリティに対する配慮

（３）SE（セキュアエレメント：Secure Element）

SEは、信頼できる機関が定めたルールやセキュリティ要件に従って、アプリケーションやその機密データ、暗号データ（暗号鍵など）を安全に保持することができる耐タンパ性のあるプラットフォーム

SE:高いセキュリティを求めるアプリ（暗号鍵の保存、OSレベルでのセキュア・エンコードなど）の動作を実行

※ アプリのインストールは出荷時もしくはTrusted Service Managerの管理下のみ



出典：ISO 5158　FigureA.1を参考に作成

ISO/TC 68 国内委員会

ISO/TC 68国内委員会事務局（日本銀行決済機構局）

E-mail：iso-tc68@boj.or.jp

03-3277-2150
03-3277-1483 （事務局直通）

https://www.boj.or.jp/paym/iso/index.htm/