【セキュアな決済を支えるユーザーデバイス】

セキュアな IC チップを中心として

栗田 太郎

ソニー株式会社

2021 年 1 月 11 日

外出したときに現金を持っていなくても安心できる持ちもの（1/2）
【オフラインでも使うことができるものの例】

- ユニークなコードが（バーコード等として）印刷されたもの
  - 所有認証．バーコードであれば簡単に複製できてしまう
  - 利用者が運用者も含めてシステムを信頼するモデル

- セキュアな IC チップが搭載されたもの
  - 所有認証．複製は難しい
  - ものの中で何らかの安全な処理（認証・処理・情報の記憶等）を行うことができる
  - 知識認証や生態認証を組み込むこともできるが
    利便性が低くなったり，コストが高くなったりする

- セキュアな IC チップが搭載されたスマートフォン（以下スマホ）
  - 所有認証に加え、知識認証や生態認証を組み合わせることができる
  - アプリケーション（以下アプリ）を起動する必要がない．高速で動作する

→ シンプルなユーザインタフェース（UI）である．処理速度が速い

→ 何か（ネットワークトラブル，災害等）があったときにも動作する

→ ものを落としたとしても何らかの救済措置があることが多い

外出したときに現金を持っていなくても安心できる持ちもの（2/2）
【オンラインで使うものの例】

- スマホに一時的にしか使うことができない動的なコード（QR コード等）を表示するもの
- あるいは，スマホのアプリで（店舗等にある） QR コード等を読むもの
  - 所有認証・知識認証・生体認証等により守られる
  - 端末，スマホにはセキュアに管理しなければならない情報は（あまり）ない

- ネットサービスの利用時に，あるいはネットにある情報にアクセスするために ID・パスワードを入力するもの
  - パスワードはネット上にもあり，そこから情報が流出するかもしれない
  - メールのアカウントが乗っ取られるとパスワードの再発行がされてしまうかもしれない
  - 二段階認証とか二要素認証とかワンタイムパスワードとかいろいろある

- 手元に利用者しか知らない秘密鍵を用いるもの
  - アカウントベースではなく，所有認証＋知識認証（＋生体認証）となる
  - 鍵やパスワード（パスフレーズ）を紛失するとアクセスできなくなる
  - 鍵を管理する専用のデバイスがあるかもしれない

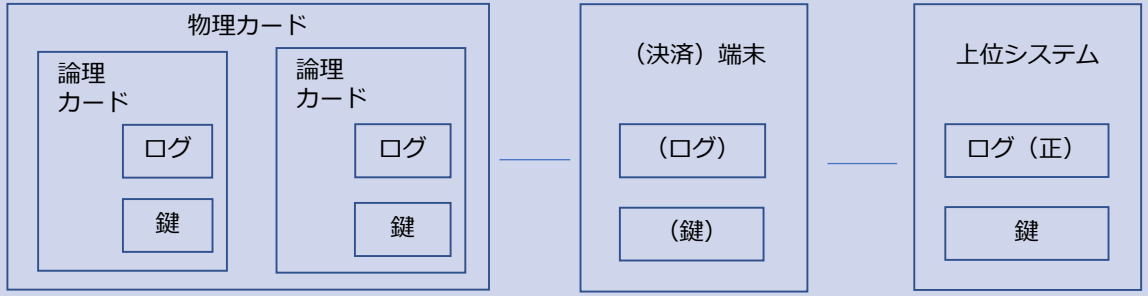
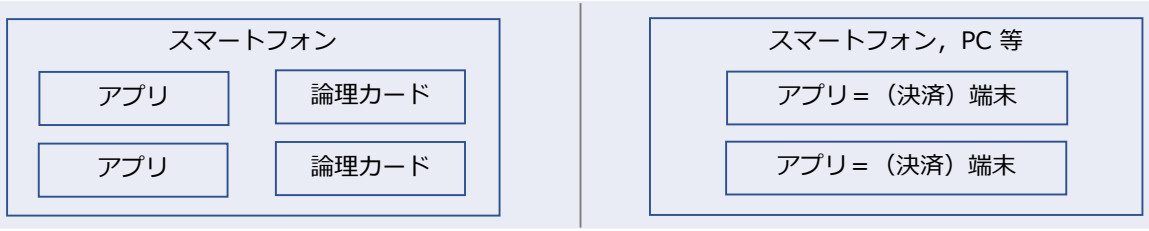
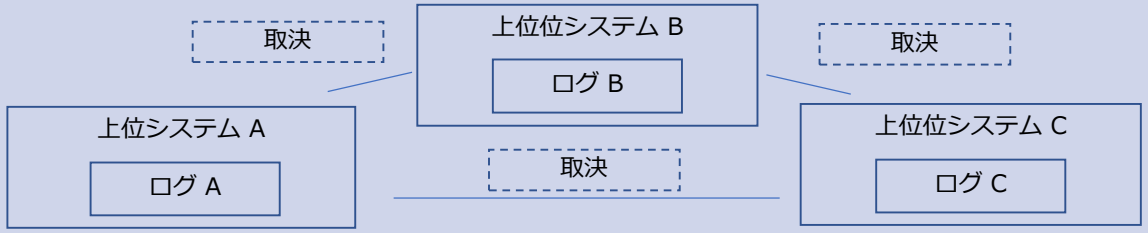
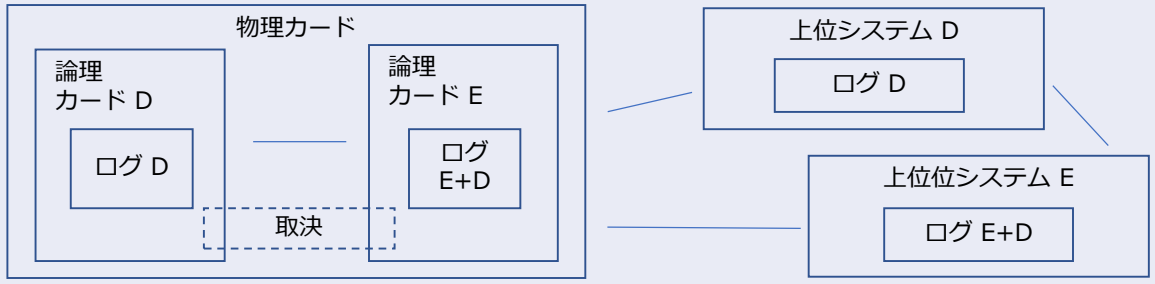
→ サービスの使い勝手はアプリの設計によるので様々である．開発者の視点ではセキュリティとのトレードオフになる

→ セキュアにおこなわければならない処理はクラウド上で行い，スマホ・PC 側は認証と UI が中心になる

→ マルチクライアントはできたり，できなかったりする

→ 可用性（いつでも使うことができるかどうか）はスマホの電池と通信に依存する（お店側も同様）

セキュアな IC チップが搭載されたもののシステムの構成パターン（青字: 特長・緑字: 課題）

システムの構成（概略図）	説明
	・セキュアな演算機能を持つカードと（決済）端末が相互に認証し，決済（処理）が行われる（一般には，利用者の代金債務が消滅する） ・記録（ログ）はカードと端末に残り，これが上位システムにいつか伝わり，上位システムにある記録が正となる ・情報はいつか伝わればよいので，オフラインでも決済できる．利用者の視点では，いつでも短い時間で（リアルタイムに）決済できる．サービス提供者としては，有事に対応することもできる ・（たとえば落とした）カードを利用停止にすることもできるが，オフラインの場合は，遅れての停止通知，運用対処となる
	・「カード」と「端末」にはさまざまなバリエーションがある ・カードと同様に，スマートフォンもバッテリがなくてもカードとして動作する（厳密には異なる） ・スマートフォンをカードとして利用する場合，アプリを起動しなくても利用できる ・スマートフォン，PC 等を端末にすることもできる
	・上位システム間は，リアルタイム，または，後れて連携する ・システムは各者が責任を持って構築・運用しており，これが重層的になって System of systems のセキュリティが成り立つ ・システム間連携は，リアルタイムの合意形成というよりは事前の約束に基づく連絡のようなものであり，基本的には他者からの情報（処理の結果）を信頼する必要がある．また，このとき必ずしもフラットな関係にはならない
	カード内で，複数の論理カードにある情報が事前の取り決めに基づきリアルタイムに連携され，その後遅れてシステムに情報が伝搬・確定（たとえば不正がないことを確認）することもできる．これにより，システム間連携をリアルタイムに行うこともできる

セキュアな IC チップが搭載されたものの ISO 25010 システムの品質モデル等に基づく整理（青字: 特長・緑字: 課題）

ISO 25010 品質特性	副特性の一部	説明
機能適合性	・機能正確性	各セキュリティ演算器の正確性と，複数者による記録の突合により成り立つ
性能効率性	・時間効率性 ・資源効率性 ・容量満足性	・オフラインでも利用できるので即座に処理できる ・資源や容量が少なくても動作する ・システムに複数あるセキュリティ演算器の計算結果を信じるモデルであり（監査はできる），計算コストが低い
互換性	・共存性 ・相互運用性	・プラットフォームの仕様と，端末の検定等によって成り立つ ・システムとその要素を複数者が開発・検証することにより接続性が向上する
使用性	・習得性 ・運用操作性 ・アクセシビリティ	・「カード」はシンプルで使いやすい ・スマートフォンをカードと同様に簡単に取り扱うことができる ・アプリや端末，Web サービス等が連動すると分かりづらくなる
信頼性	・成熟性 ・可用性 ・障害許容性（耐故障性） ・回復性	・アトミック性があり，処理は確実に行われることが保証される ・一方で，無線の場合，「処理未了」が生じる可能性がある（処理は行われている） ・様々な運用形態により信頼性を実現する．オフラインでも動作する
・保守性 ・移植性	・モジュール性 ・置換性	・オープンな，規格化された仕様である ・複数者で開発・運用・維持している

セキュリティ等に関係する規格	セキュリティ等の副特性・要件等	説明
ISO 25010	機密性 (Confidentiality)	・偏在する演算器のセキュリティにより守る ・上位システムのセキュリティにより守る
	・インテグリティ (Integrity) ・責任追跡性 (Accountability)	・改ざんに対しては暗号技術で守る ・記録（ログ）を集めることにより全てを把握する ・記録を確認・監査する
	・否認防止性 (Non-repudiation) ・正真性 (Authenticity)	・所有認証・知識認証・生体認証等により守る ・利用者について，所有認証の場合，本人認証が難しい ・スマートフォンの場合，利用機種のセキュリティに依存する
ISO 15408	セキュリティ機能要件	システムの一部の静的な仕様と実装・テストに対して，第三者評価・認証の規格・制度に基づき，目標や仕様・検証項目等を定め，これが専門家により評価・認証される
	セキュリティ保証要件	システムの開発と運用，環境についても規格に従い文書化，評価される
その他	暗号アルゴリズム	システム全体に脆弱性がないことの証明は難しい
	プライバシ	利用者が，運用者が法律や約款を守ることを信じるモデルである

現行システムの特長と課題

【特長】

- 利用者と攻撃者が物理的にアクセスできるものはセキュアな演算器により守られる
- 様々な構成や利用の形態がある
- 処理速度が速い（急がない処理は後から行う．取り消しもできる）
- 分かりやすく使いやすいユーザインタフェースである
- オフラインでも利用できる（たとえば故障や災害に強い）
- スマートフォンのアプリの起動が不要である
- ハードウェアとエコシステムによるセキュリティと安心感がある
- 環境負荷が低い
- セキュリティの第三者評価・認証や，機能・通信の互換性の検定に関する枠組みがある

【課題】

- 利便性とのトレードオフで本人認証が難しい．スマートフォンのセキュリティに依存している
- スマートフォンのアプリケーションや Web サービス，（店舗等の）端末等と連動すると，利用方法が統一されず，使いづらいと感じる利用者もいる
- 利用者にとってサービス提供者のシステムはブラックボックスであり，利用者がサービス提供者を信頼するモデルである（利用者にとって契約の履行の確認のコストが高い）
- 利用者にとって取り決めが分かりづらい．様々な形の契約をリアルタイムに合意形成することができない
- 利用者のプライバシの取り扱いはサービス提供者の考え方やシステム運用による
- 暗号アルゴリズムや運用を含めて，システム全体を品質保証し続けることは難しい

[付録] サービスに対する要求事項?

【利用者が求めるもの?】

[？] 安全な場所に情報がある（自分の情報が守られる）

[？] 安全な場所で処理がされている

[〇] 所有している人が使うことができる．セキュリティを強くできる

[〇] 処理をしたときに何が行われるのかが理解しやすく，
また，理解している

[△] 何が行われたのかを後から確認しやすい

[△] 落としても失われるものがない

[？] 信頼できる人が安全なものだと言っている

[〇] みなが使っている，なんとなく安心・安全である

[〇] 使いやすい．いつでも使うことができる．決済に時間がかからない

[〇] 便利である．（とくにコロナ禍において）清潔である

[◎] お得である．効率化できる

→ 利用者にとっては利便性と安心感，「お得である」ことが重要である

【提供者が求めるもの?】

[〇] 安全な場所に情報がある（システムの重要情報全体が守られる）

[〇] 安全な場所で処理がされている

[△] 利用者本人だけが利用できるサービスは他者が
使うことができないようにしたい

[〇] 利用者に安心感をお持ちいただきたい

[〇] 利用者にお問い合わせいただく回数を減らしたい

[〇] 安全性を第三者に追認してもらうことで説明した
（説明責任を果たしたい．身の潔白を証明したい）

[◎] 提供者のエコシステムの中でサービスを使って欲しい
このためにサービスを差異化したい

→ 提供者側は変わりゆく価値の提供と提供スピードとセキュリティのバランスが重要になる

→ 「当たり前品質」だけではなくて「魅力的品質」を競う

【凡例】[〇]: おそらく求めている
[△]: おそらくそれほどは求めていない
[？]: 求めても求めていなくもない?