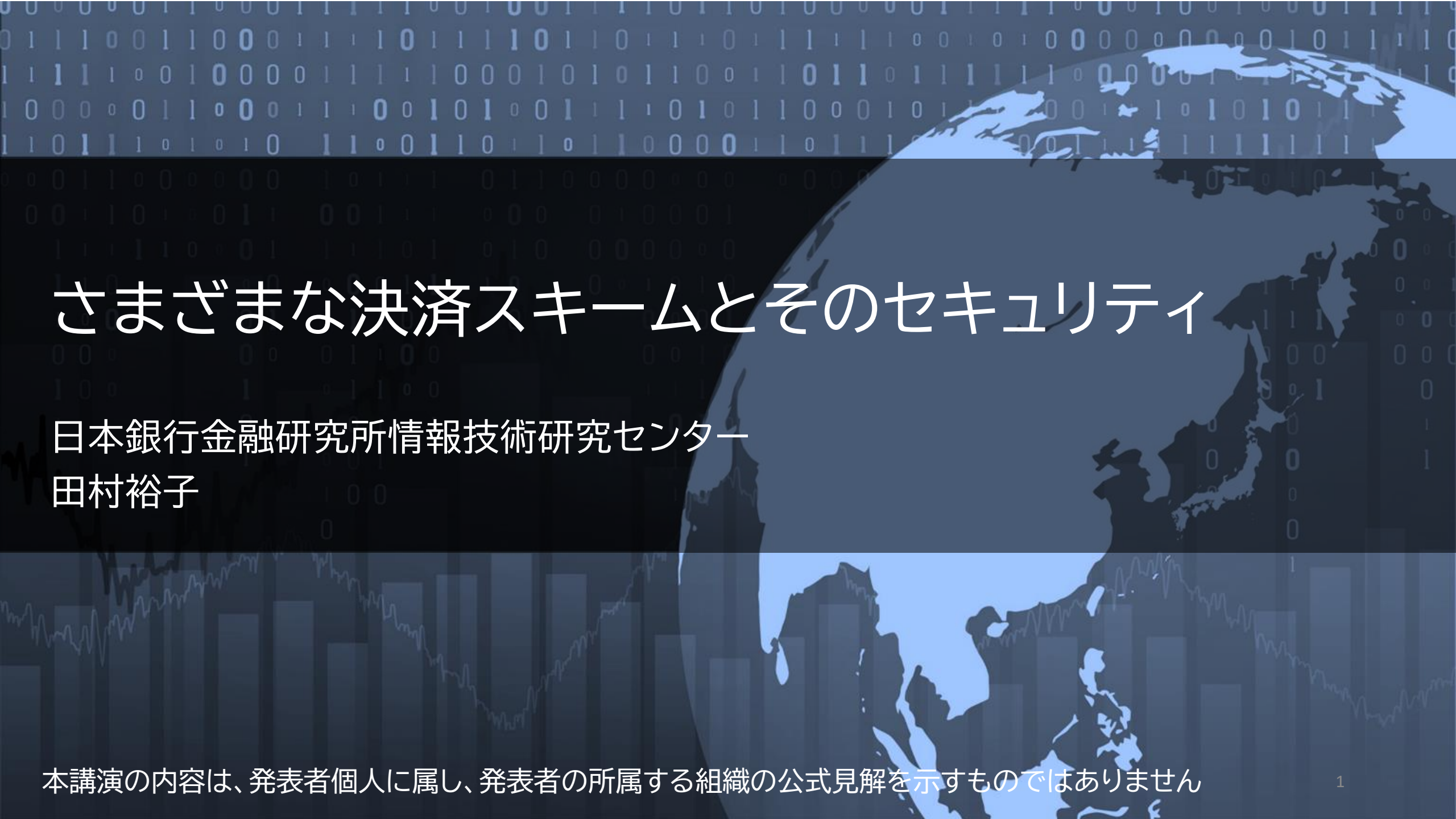
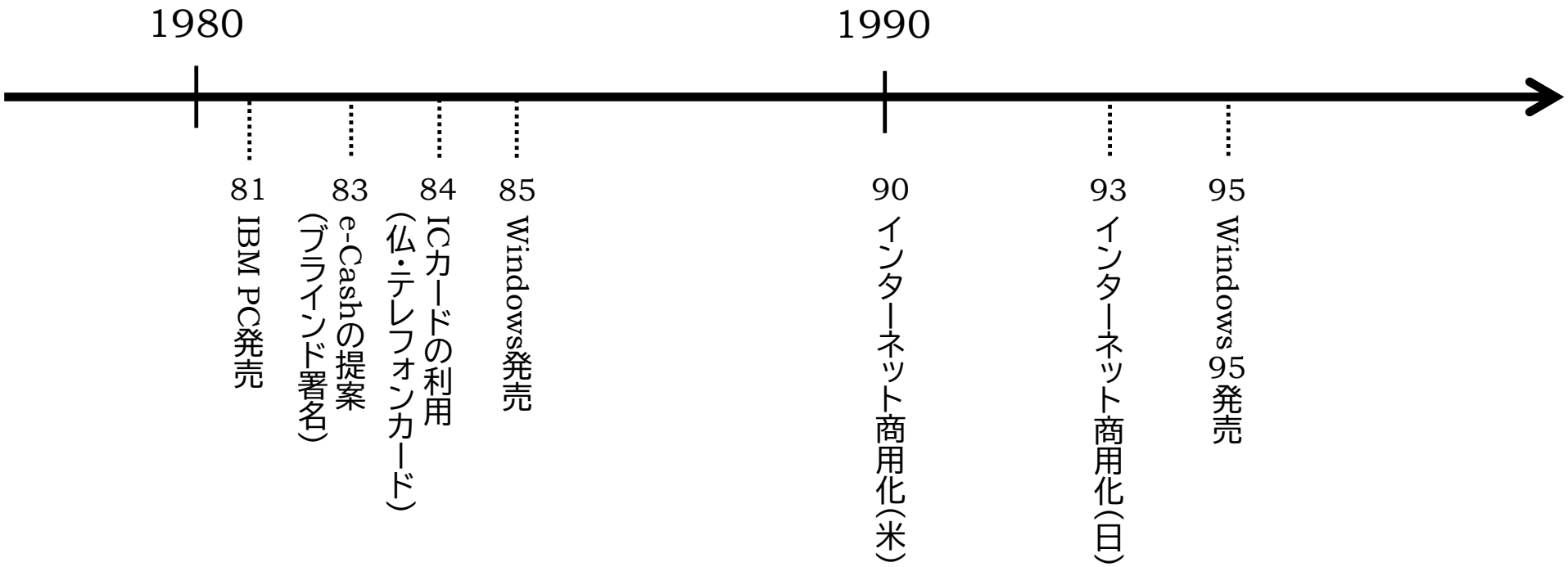


さまざまな決済スキームとそのセキュリティ

日本銀行金融研究所情報技術研究センター
田村裕子

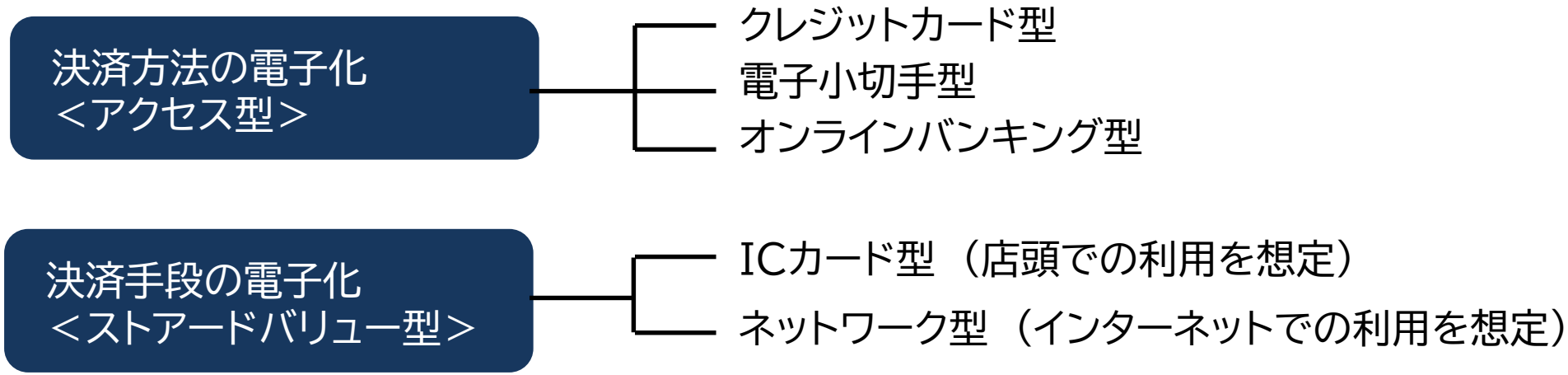
1. デジタル決済の黎明

- 1990年代、デジタル決済にかかる研究開発が盛んに
  - ✓「暗号技術」、「インターネット」、「ICカード」、「PC」の開発・普及が背景



1. デジタル決済の黎明～デジタル決済の種類

- デジタル決済にかかる研究開発は2種類（1990年代当時の分類*）
  - ✓ 決済方法の電子化： 既存の決済手段を前提に、そのアクセス方法をデジタル化したもの
  - ✓ 決済手段の電子化： 現金を代替する新たな電子的な手段を提供を目指したもの
- 国内外でさまざまな実証実験を実施



＊ 中山靖司、「実現せまる電子マネーの現状」、1998年2月

1. デジタル決済の黎明～国内での実証実験

		1995年以前	1996年	1997年	1998年以降
アクセス型	クレジットカード型	• ザ・サイバープラザ	• サイバーネットクラブ • Cyber Publishing Japan • カードレスカードシステム • アコシス	• スマートコマースジャパン • Smart Collar Club • バーチャルシティ構想 • エレクトロニック・マーケット・プレイス • Cyber Cash	ーー
	電子小切手型	ーー	ーー	• Smart Collar Club • サイバーコマースシティー • 日本IBM電子商取引実験	• 日立電子商取引実験
	オンライン・バンキング型	ーー	ーー	• 住友、富士、東京三菱 • 大垣共立、十六銀行 • ANSER-WEB	• 三和銀行
ストアードバリュー型	ICカード型	• 府中インテリジェントパーク • あすかるさんカード • テレコムセンタービル	• 東京ファッションタウン • Smart Island Consoritium • い～なちゃん／つれてってカード	• 早大生協実験 • Visa Cash・神戸実験 • 大学生協実験 • エレクトロニック・マーケット・プレイス・三鷹実験	• Visa Cash・渋谷実験 • 郵貯・大宮実験 **• スーパーキャッシュ**
	ネットワーク型	ーー	• Cyber Chip System	• NET-U • Ecash（野村総研DigiCash） • BitCash • ECN電子現金 • CyberCoin	**• インターネットキャッシュ**

（出典） 中山靖司、「実現せまる電子マネーの現状」、1998年2月

1. デジタル決済の黎明～国内での実証実験

- 日本銀行金融研究所は、1990年から「電子現金」の研究を開始。1995年よりNTT暗号研究開発チームと共同研究を実施
- 現金の電子化を目指したものであり、現金に見立てた電子データ（電子現金）のやり取りによって決済を完了させるもの
- 銀行から引き出した電子現金をICカードに格納し、ショッピングや個人間送金に利用

- 電子現金スキームに基づく大規模な実証実験：
  - ✓インターネットキャッシュ（1998-2000年）： オンライン決済の実証実験。4の金融機関と約1万人の参加者の協力のもと実施（サイバービジネス協議会、日本銀行も参画）
  - ✓スーパーキャッシュ（1999年-2000年）： 対面／オンライン決済の実証実験。24の金融機関、約1,000の店舗、約2.2万人の協力のもと実施（スーパーキャッシュ協議会）

1. デジタル決済の黎明～30年前の実証実験の様子

実証実験のオープニングセレモニー

Super Cash ロゴ

ICカードと残高を確認するためのデバイス

スーパーキャッシュで店頭決済
を行う様子

公衆電話を介して銀行からICカードに
スーパーキャッシュをチャージ可能

（出典） https://ascii.jp/elem/000/000/315/315560/

2. 電子現金スキームの再整理～モチベーション

- 現在広く普及しているキャッシュレス決済の多くは、**サービス事業者が決済を仲介**
  - ✓ ユーザから送金の指図を受けたサービス事業者がその内容を台帳に記載
- キャッシュレス決済のさらなる普及を想定した場合、サーバ・ネットワーク障害やサーバ処理性能が決済サービスに及ぼし得る影響について、より一層の考慮が必要ではないか

- 電子現金方式での送信処理は、**ユーザ二者間でのデータ通信に閉じる**ものであることから、サーバ・ネットワーク障害やサーバ処理性能への依存度の面から優位な可能性
- 現行技術を前提とすれば、どの程度のユーザビリティを確保し得るか

2. 電子現金スキームの再整理～公表資料

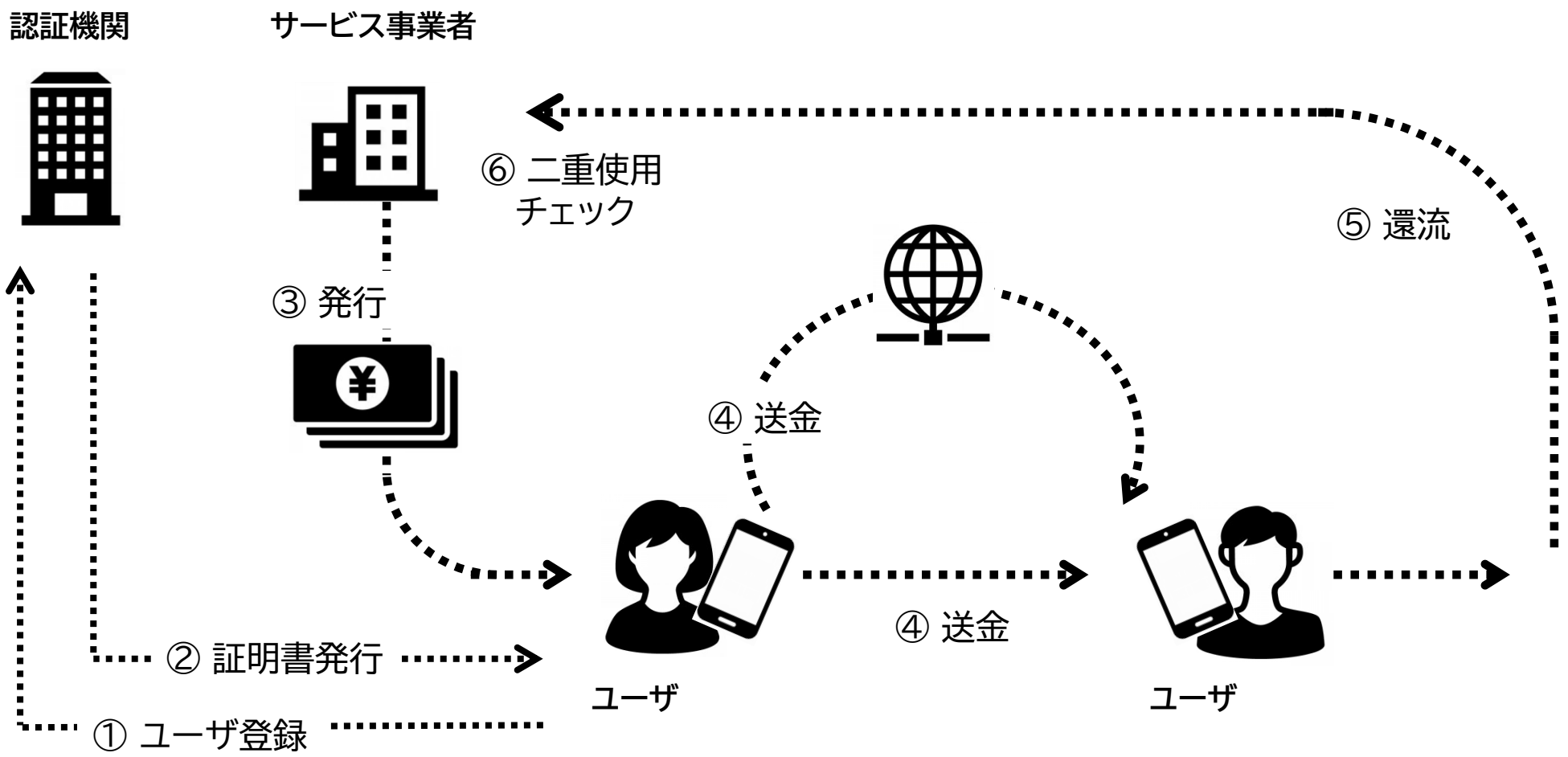
「台帳を用いない決済方式に関する技術面からの一考察」

金融研究所ディスカッションペーパー、2024-J-19

田村裕子、阿部正幸、奥田哲矢、津川天祐、宮澤俊之、山村和輝、
赤羽喜治、田口智貴、平栗勇人、増田博人、山田健斗

（台帳を用いた決済方式）

2. 電子現金スキームの再整理～基本スキーム



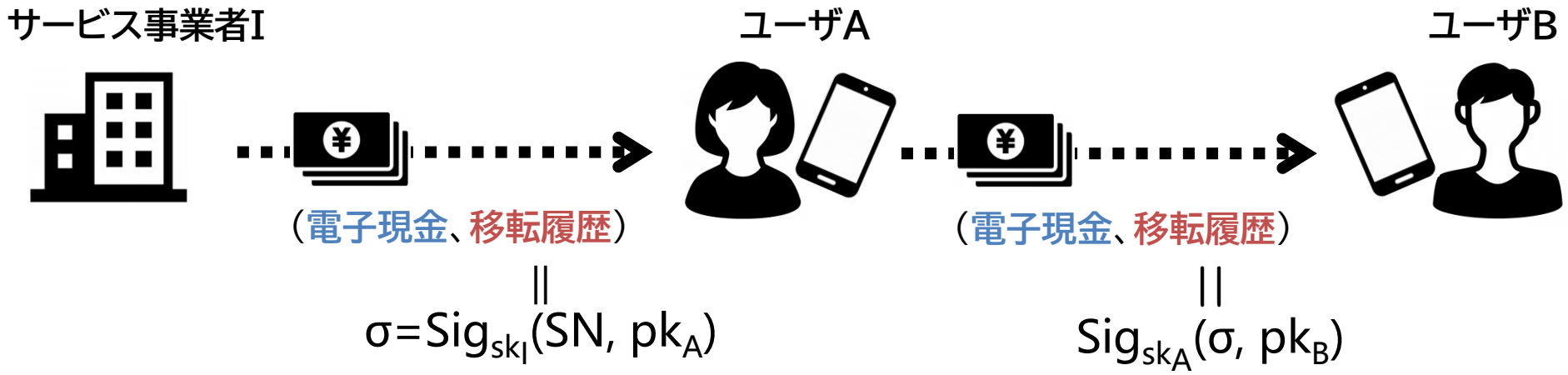
2. 電子現金スキームの再整理～電子現金の送受信

- **電子現金**の送受信は、その**移転履歴**とセットで行う（同じシリアルナンバSNを共有）

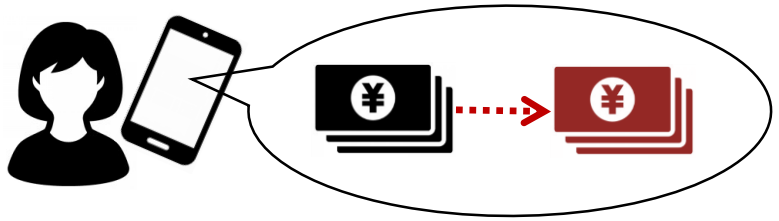
  電子現金： サービス事業者によるデジタル署名-- $Sig_{sk_I}(SN, 金額)$

  移転履歴： 前の移転履歴・送金先ユーザの公開鍵に対する送金元ユーザのデジタル署名

  ――― 移転履歴の検証により、「正当な保有者による送信である」ことがわかる



2. 電子現金スキームの再整理～二重使用への対策



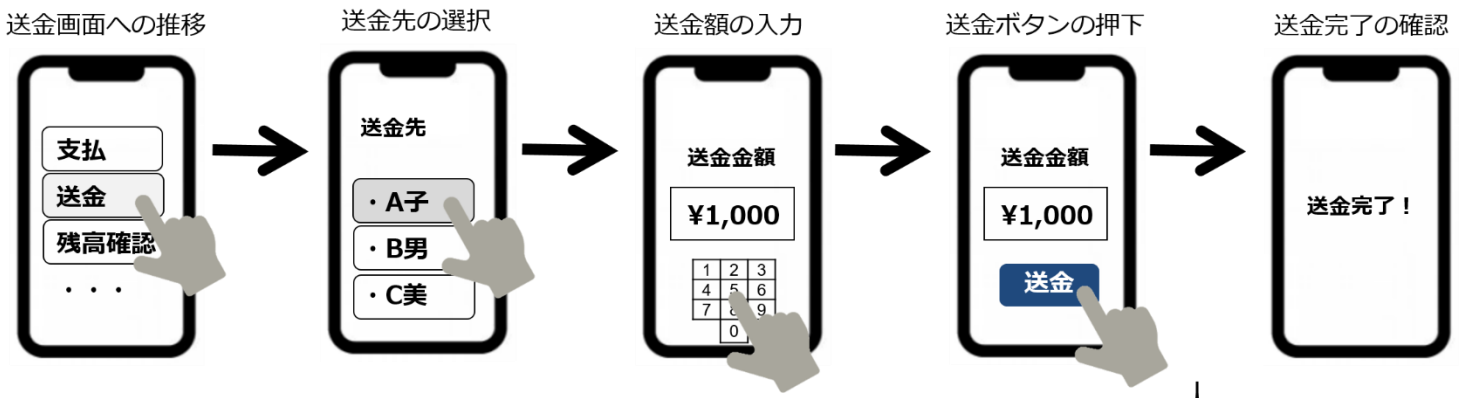
電子現金を複製して使用（二重使用）

→ 秘密鍵を用いた処理（移転履歴の更新）を不正に実行できないよう、耐タンパーデバイスの使用を義務付け

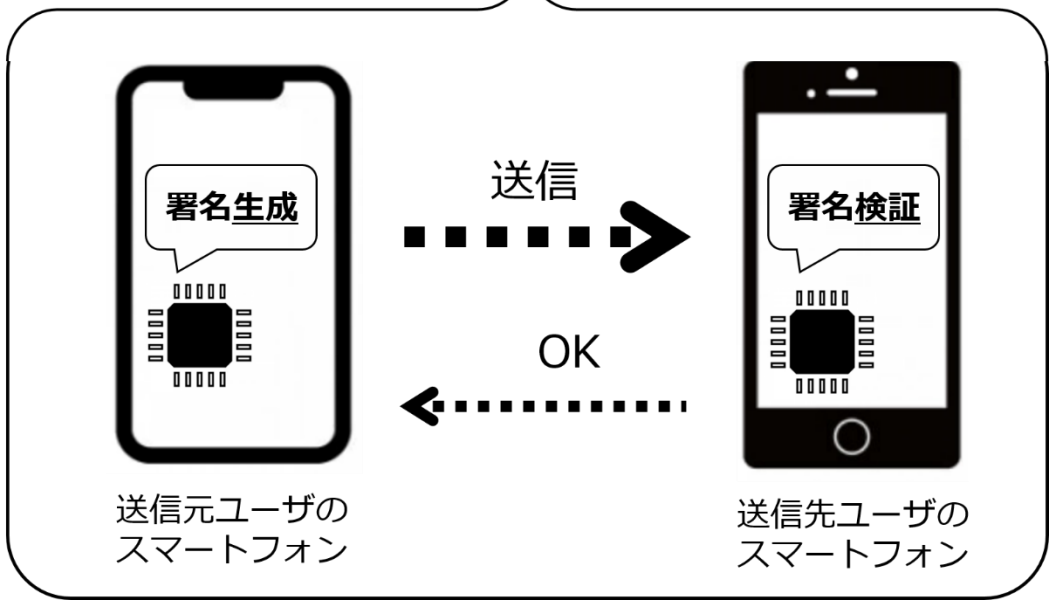
ただし・・・

- 安定したサービス提供のためには、将来的なデバイスの**耐タンパ性の低下への備え**も必要
- 電子現金スキームでは、**事後的な二重使用検知**機能を付与することで二重使用を抑止
  - ✓ 電子現金の還流時、同じシリアルナンバーをもつ電子現金があれば、移転履歴の確認によって、二重使用者を特定可能

2. 電子現金スキームの再整理～電子現金処理にかかる時間

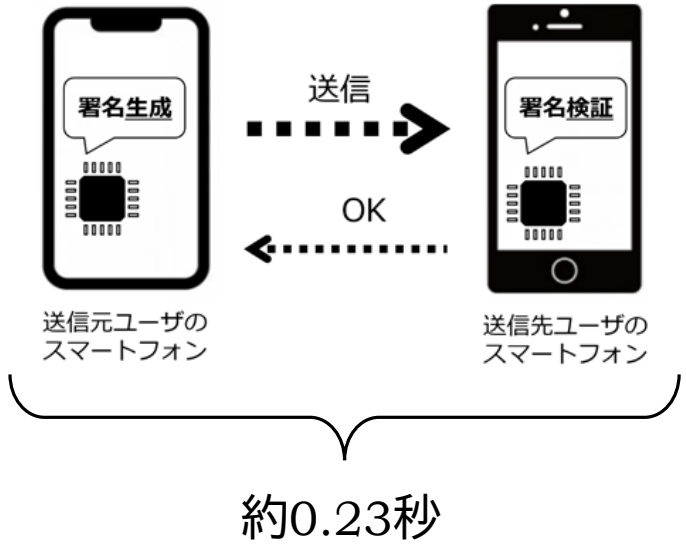


送信時の**署名生成**(移転履歴の更新)と
データの送信がボトルネック



2. 電子現金スキームの再整理～実機検証の結果

- 100枚の電子現金を送付するとき‥
  - ✓ 現行のeSEによる署名生成は**35ミリ秒**
  - ✓ 送金先における署名検証に同程度かかったとしても、**合計約70ミリ秒**
  - ✓ 送金元から送金先へは、Wi-Fi Directであれば**160ミリ秒**
  - ✓ 取引レスポンス時間は**約230ミリ秒（0.23秒）**と概算可能



2. 電子現金スキームの再整理～効率化に向けた検討

ディスカッションペーパーでは、以下についても考察を実施

- 送信時における署名生成回数の削減（送信時の効率化）
- 取引時における通信回数の削減（変動額面方式）
- 送信時における公開鍵更新頻度の削減（ゼロ知識証明を使用したプライバシー強化）

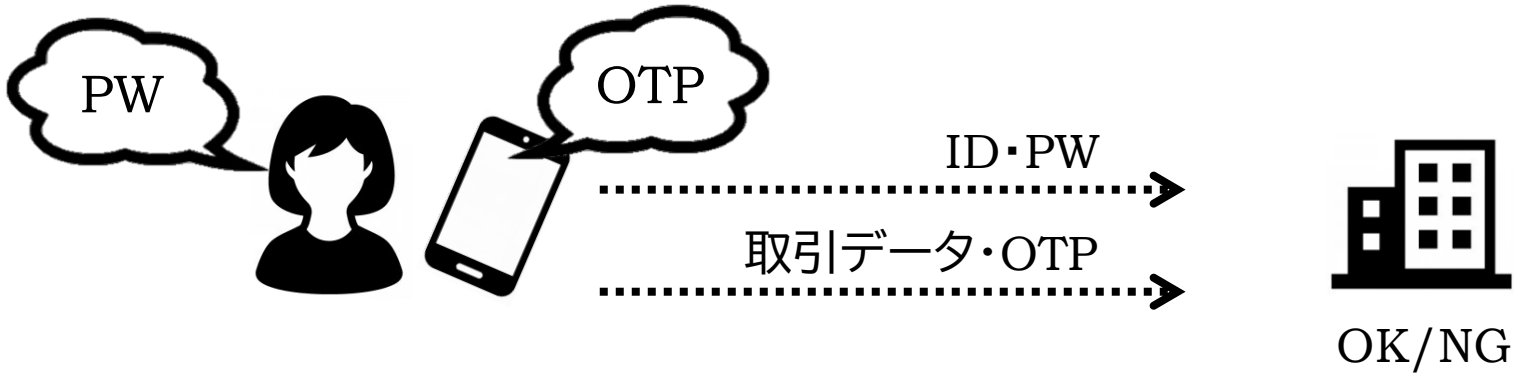
3. 決済スキームのセキュリティ～身近な決済

クレジットカード決済、インターネットバンキング、コード決済

- 台帳ですべての取引を管理
- 不整合な取引は、サービス事業者によって排除可能
- アカウントにログインした者が取引を実施可能

難しい

→ なりすましによる不正送金を防止するには、PWやOTPの漏洩を防止する必要

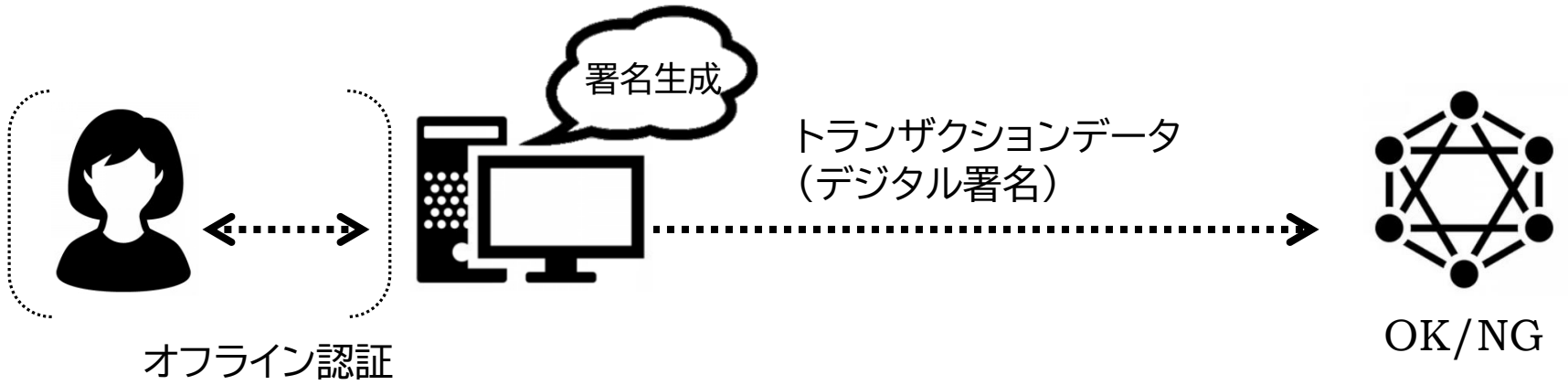


3. 決済スキームのセキュリティ～暗号資産

暗号資産

- 台帳ですべての取引を管理
- 不整合な取引は、参加者による検証（マイナー）によって排除可能
- 暗号資産に対応する鍵で署名を生成した者が取引を実施可能

→ 不正送金を防止するには、本人だけが署名生成できる仕組みが必要

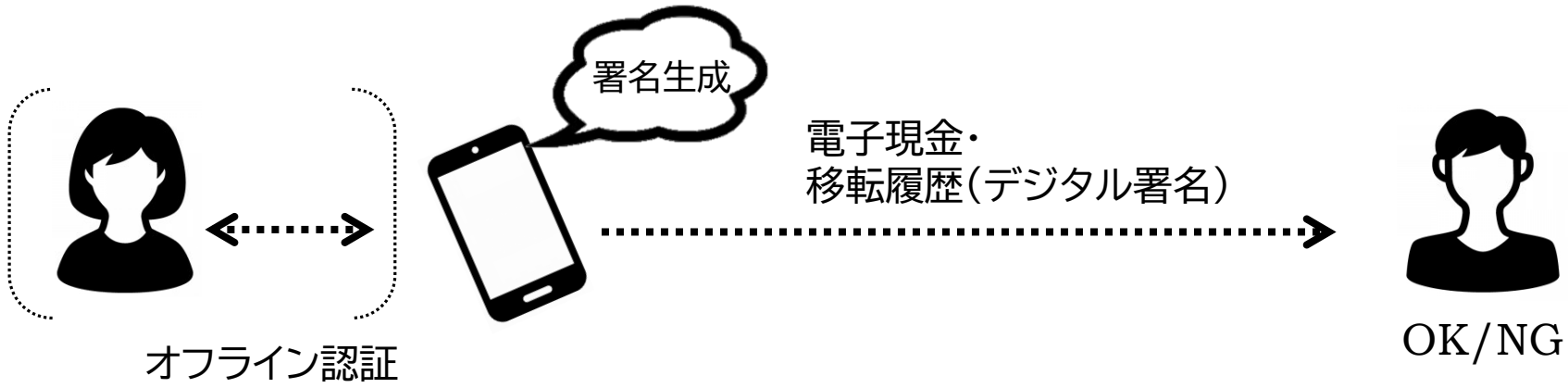


3. 決済スキームのセキュリティ～電子現金

電子現金

- 不整合な取引は、受信者による検証によって排除可能
- 送信者による不正は、デバイスの耐タンパー性と事後的な二重使用検知によって排除可能
- 電子現金に対応する鍵で署名を生成した者が取引を実施可能

→ 不正送金を防止するには、本人だけが署名生成できる仕組みが必要



まとめ

- 電子現金スキームを再整理するとともに、実機検証を実施することで、高いユーザビリティを確保できる可能性を確認
- ただし、法律や制度、実運用等、社会実装に向けた実現可能性は検討の対象外

- 電子現金では、暗号資産と同様、第三者による署名生成を防止するセキュリティ対策が必要。もっとも、ウォレットを使用しさえすれば安全に取引できるわけではないことに留意