決済の未来フォーラム デジタル通貨分科会：中央銀行デジタル通貨を支える技術 ～CBDCに求められるセキュリティ～

2021年6月11日

セコム株式会社　IS研究所
コミュニケーションプラットフォームディビジョン
暗号・認証基盤グループ
佐藤　雅史

自己紹介

セコムIS研究所
Intelligent Systems Laboratory

- 電子署名・電子認証関連
  JNSA電子署名WG，日本トラストテクノロジー協議会(JT2A)，トラストサービス推進フォーラム(TSF)，OpenID Foundation Japan/KYC WG，JAHIS，JIIMA
- ブロックチェーン関連
  CGTF(Crypto-assets Governance Task Force)，ISO/TC 307 エキスパート/国内審議委員会 JWG4(セキュリティ)国内主査，JVCEA技術委員会委員
  書籍：「ブロックチェーン技術の未解決問題」，「Blockchain Gaps – From Myth to Real Life」，「ブロックチェーン技術の教科書」
- デジタル通貨関連
  デジタル通貨フォーラム ウォレットセキュリティ分科会幹事

セキュリティ？

守りたいもの

セキュリティ？

脅威

守りたいもの

脅威

セキュリティ？

脅威

対策

脅威

セキュリティ？

脅威

対策

脅威

セキュリティ？

脅威

対策

脅威

そもそも何のため？

セキュリティ？

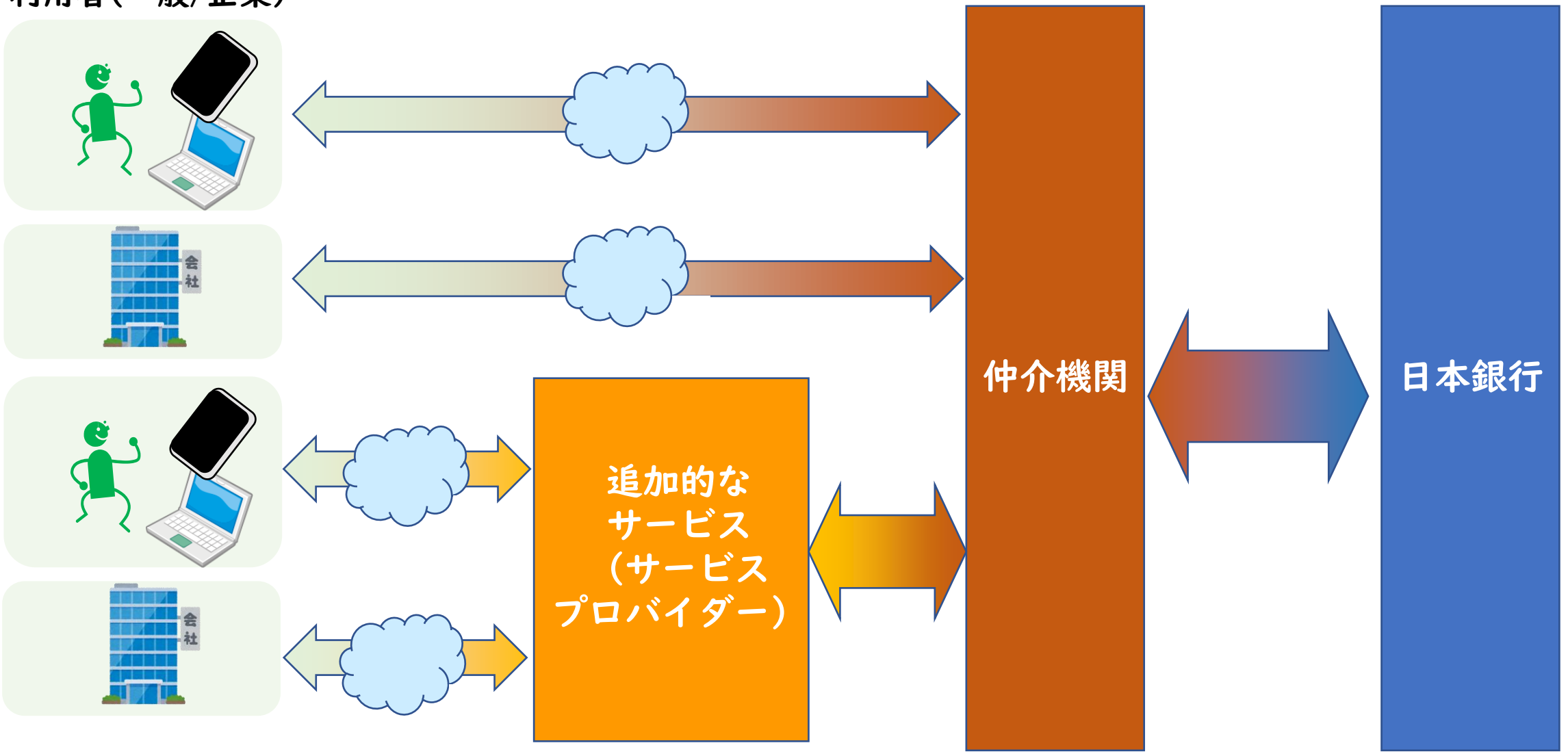
セキュリティは使うためのもの
安全・安心に利用を促進するもの

CBDCの発行形態モデル

※参考：中央銀行デジタル通貨に関する日本銀行の取り組み（2021/3/26 日本銀行決済機構局）

セコムIS研究所
Intelligent Systems Laboratory

利用者（一般/企業）

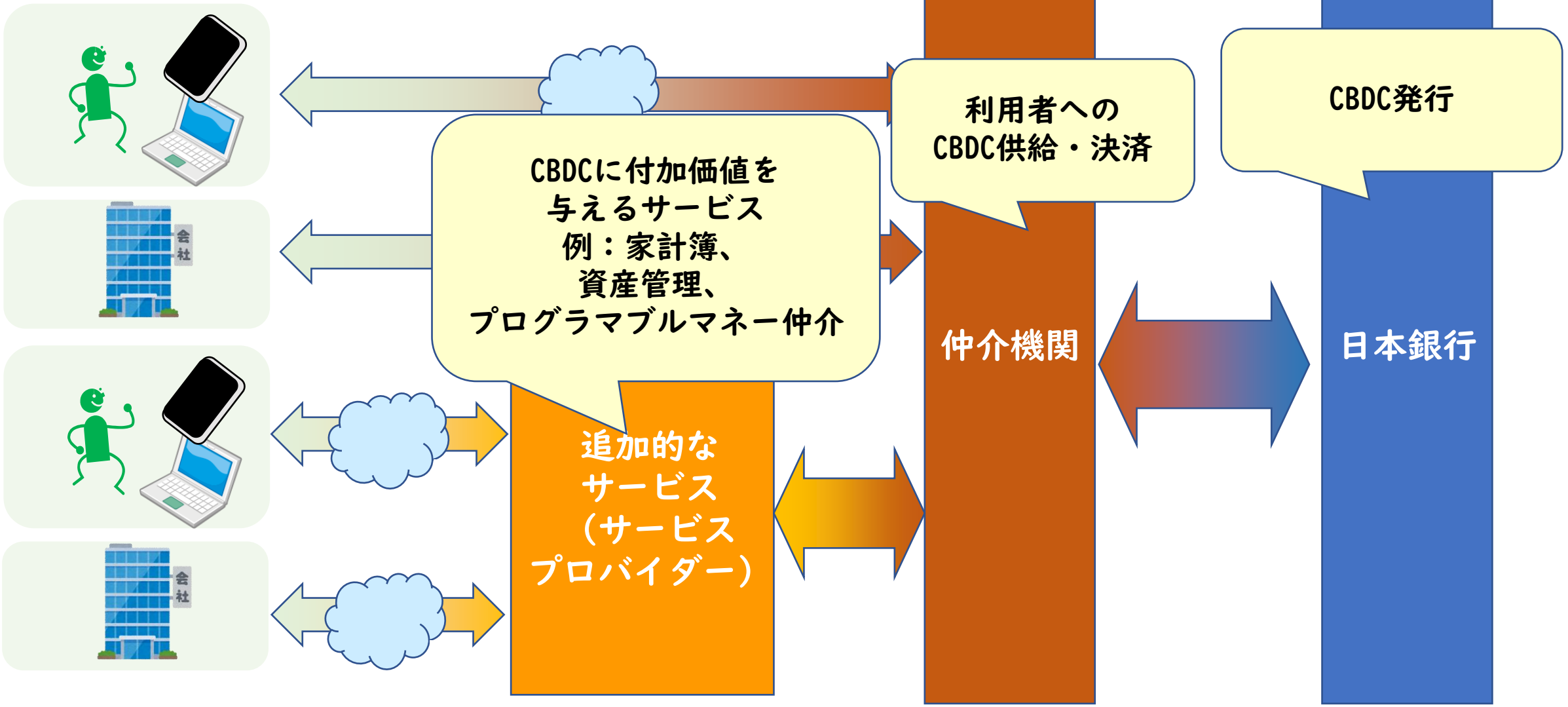


CBDCの発行形態モデル

※参考：中央銀行デジタル通貨に関する日本銀行の取り組み（2021/3/26 日本銀行決済機構局）

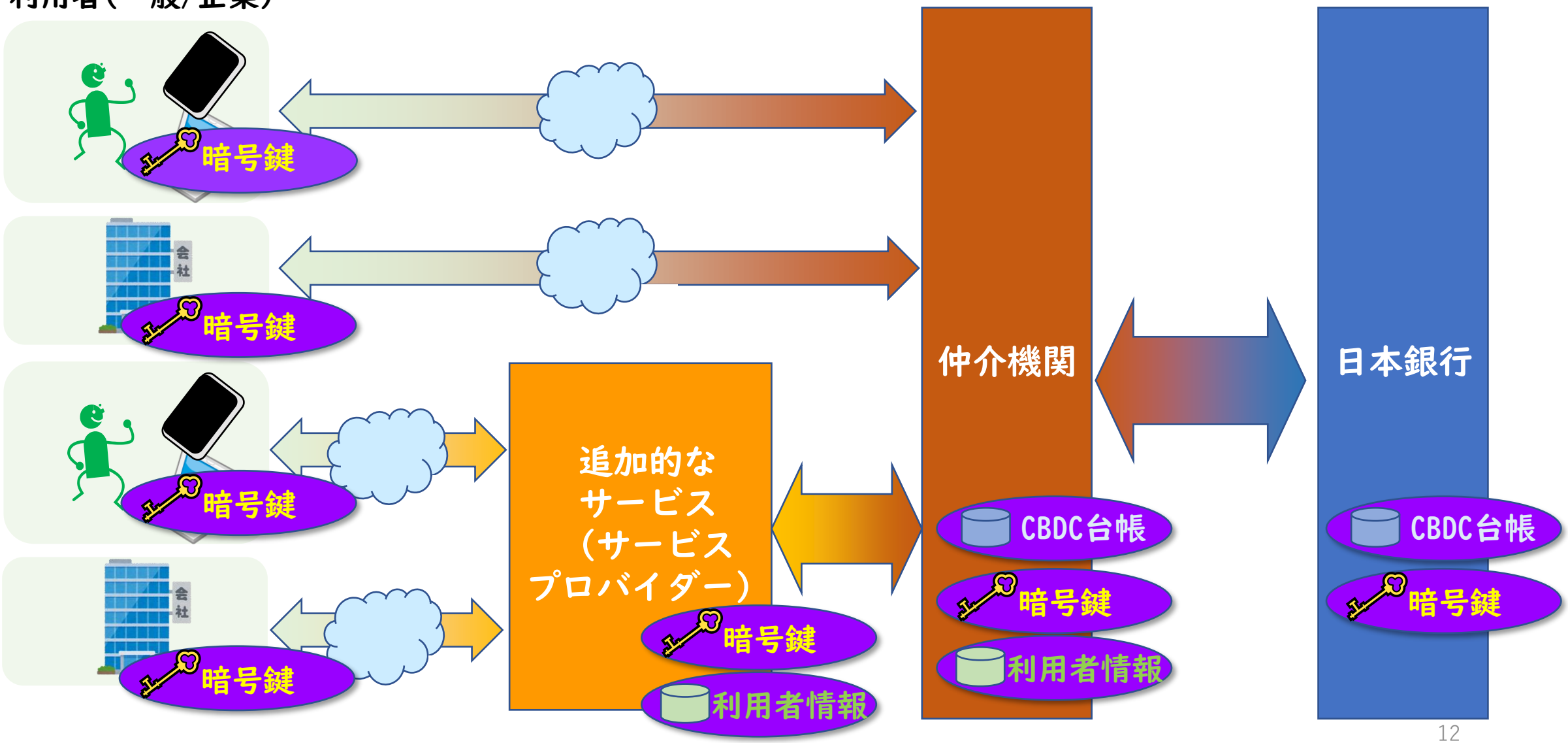
セコムIS研究所
Intelligent Systems Laboratory

利用者（一般/企業）



CBDCにおける守るべき資産とは？（例）

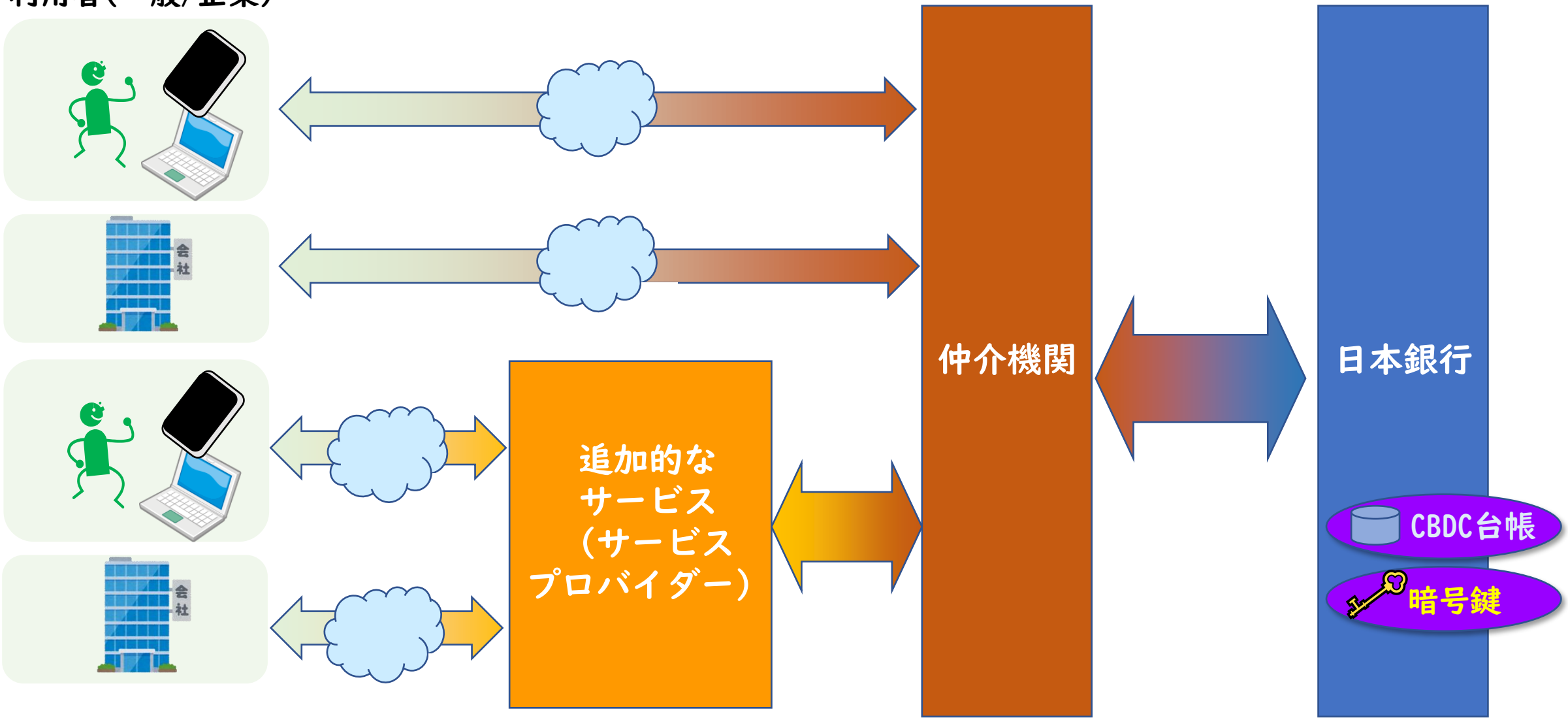
セコムIS研究所
Intelligent Systems Laboratory



CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory

利用者(一般/企業)



CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory

利用者(一般/企業)

追加的な
サービス
(サービス
プロバイダー)

仲介機関

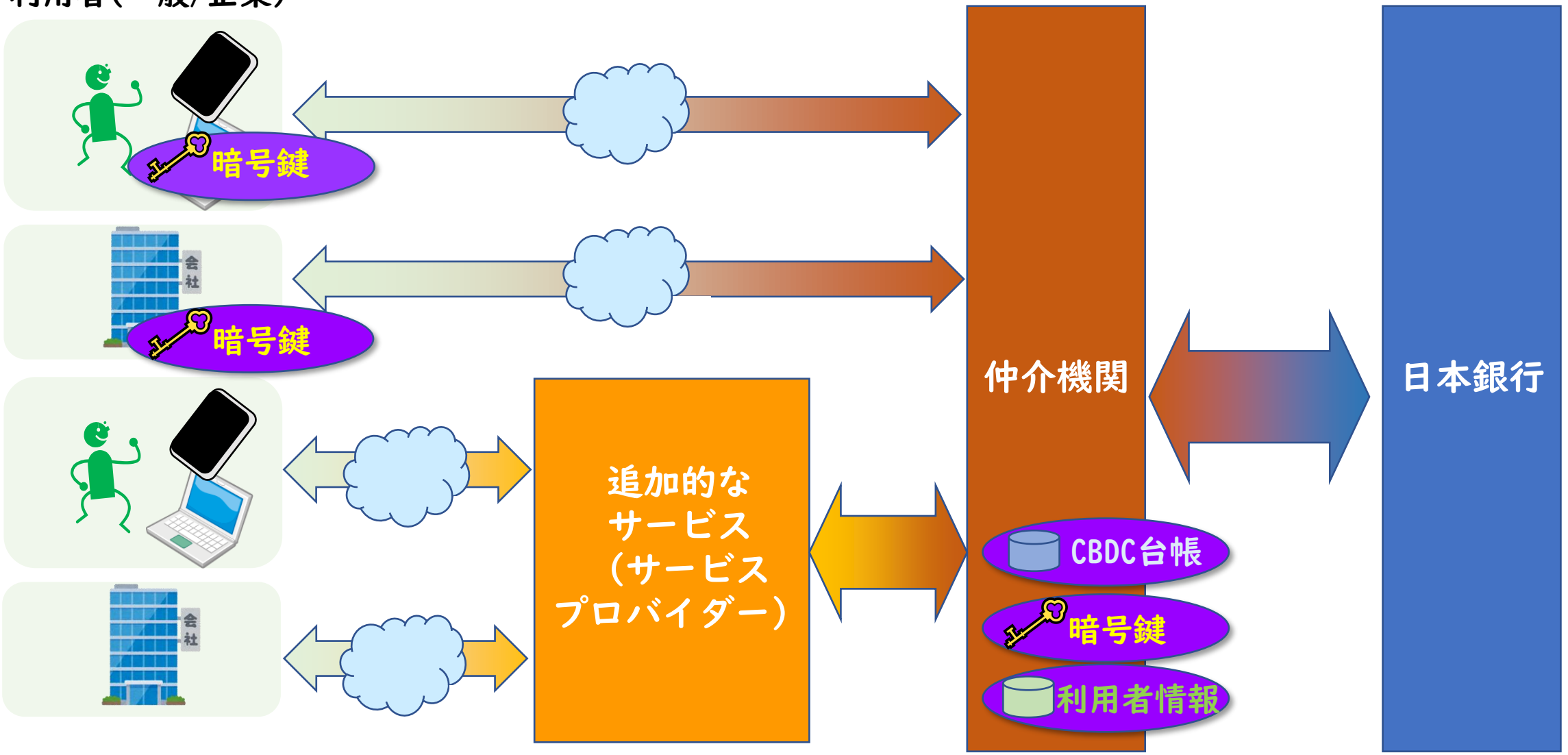
日本銀行

【日本銀行】
セキュリティマネージメント
(サイバー/物理の安全策含む)
・セキュリティ体制
・システム管理策
・台帳情報管理策
・暗号鍵管理策
など

【日本銀行-仲介機関間】
・ネットワーク管理策
・システム間認証
・CBDC発行・還収プロトコル安全性

CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory



CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory

利用者(一般/企業)

【仲介機関-利用者】
・ネットワーク管理策
・CBDC送受プロトコル安全性
・Webサイト/Webアプリ安全性,真正性(認証)
・利用者の本人確認
・利用者の認証
など

【仲介機関-サービスプロバイダー】
・ネットワーク管理策
・システム間認証
・ CBDC送受プロトコル/API安全性
など

追加的なサービス(サービスプロバイダー)

仲介機関

日本銀行

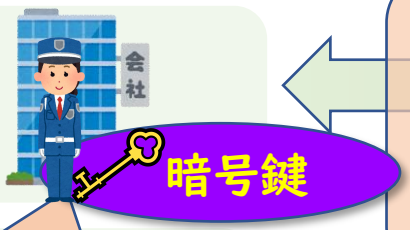
【仲介機関】
セキュリティマネージメント
(サイバー/物理の安全策含む)
・セキュリティ体制
・システムの安全策
・台帳情報管理策
・利用者情報管理策
・暗号鍵管理策
など

CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory

利用者(一般/企業)

【仲介機関提供アプリ】
・スマホアプリ安全性,
真正性
・認証クレデンシャル(暗号鍵)管理
など



【仲介機関-サービスプロバイダー】
・ネットワーク管理策
・システム間認証
・ CBDC送受プロトコル/API安全性
など

【利用企業】
・認証クレデンシャル(暗号鍵)管理
・仲介機関の認証,安全な利用方法
など

追加的な
サービス
(サービス
プロバイダー)

【仲介機関-利用者】
・ネットワーク管理策
・CBDC送受プロトコル安全性
・Webサイト/Webアプリ安全性,真正性(認証)
・利用者の本人確認
・利用者の認証
など

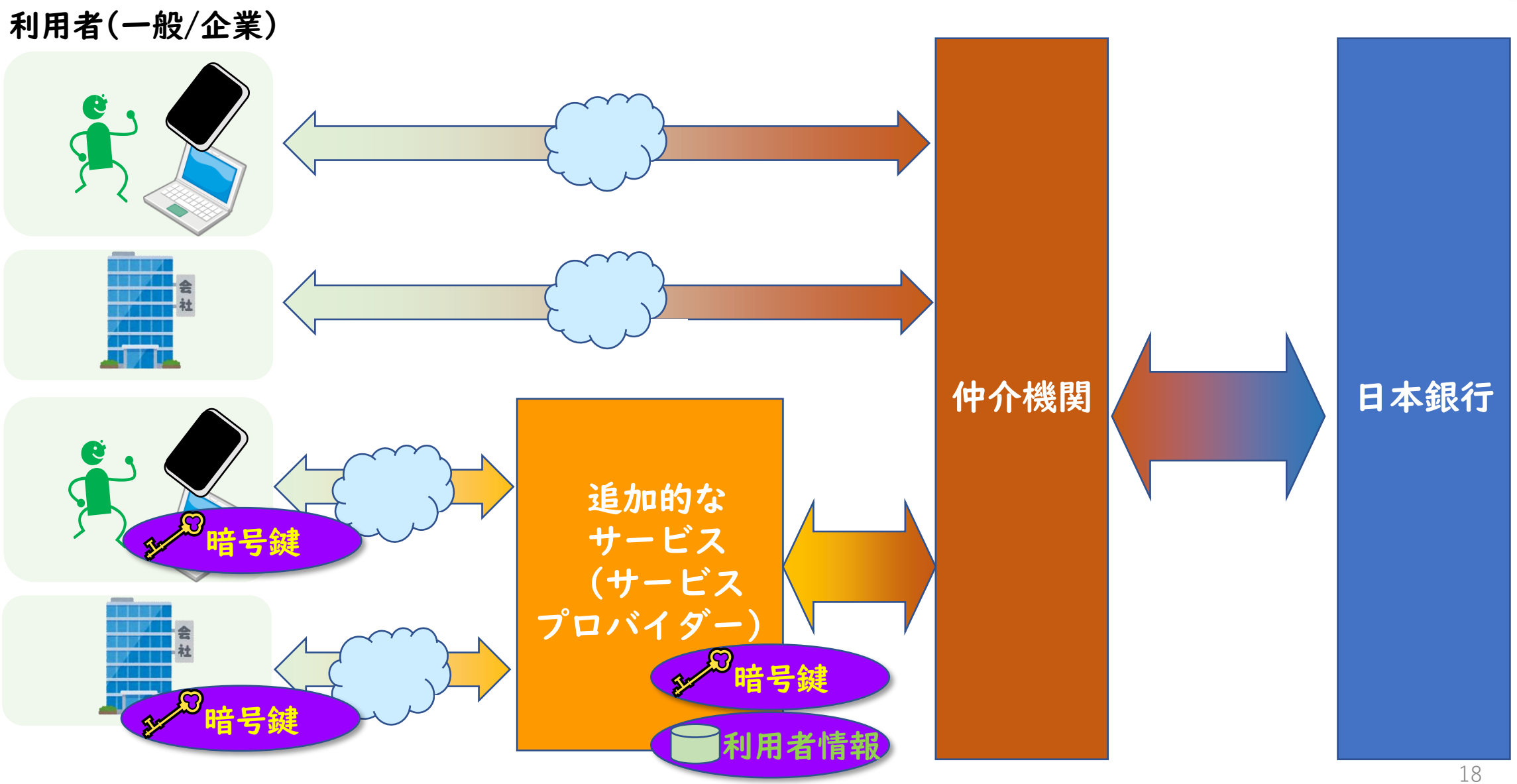
仲介機関

【仲介機関】
セキュリティマネージメント
(サイバー/物理の安全策含む)
・セキュリティ体制
・システム管理策
・台帳情報管理策
・利用者情報管理策
・暗号鍵
など

日本銀行

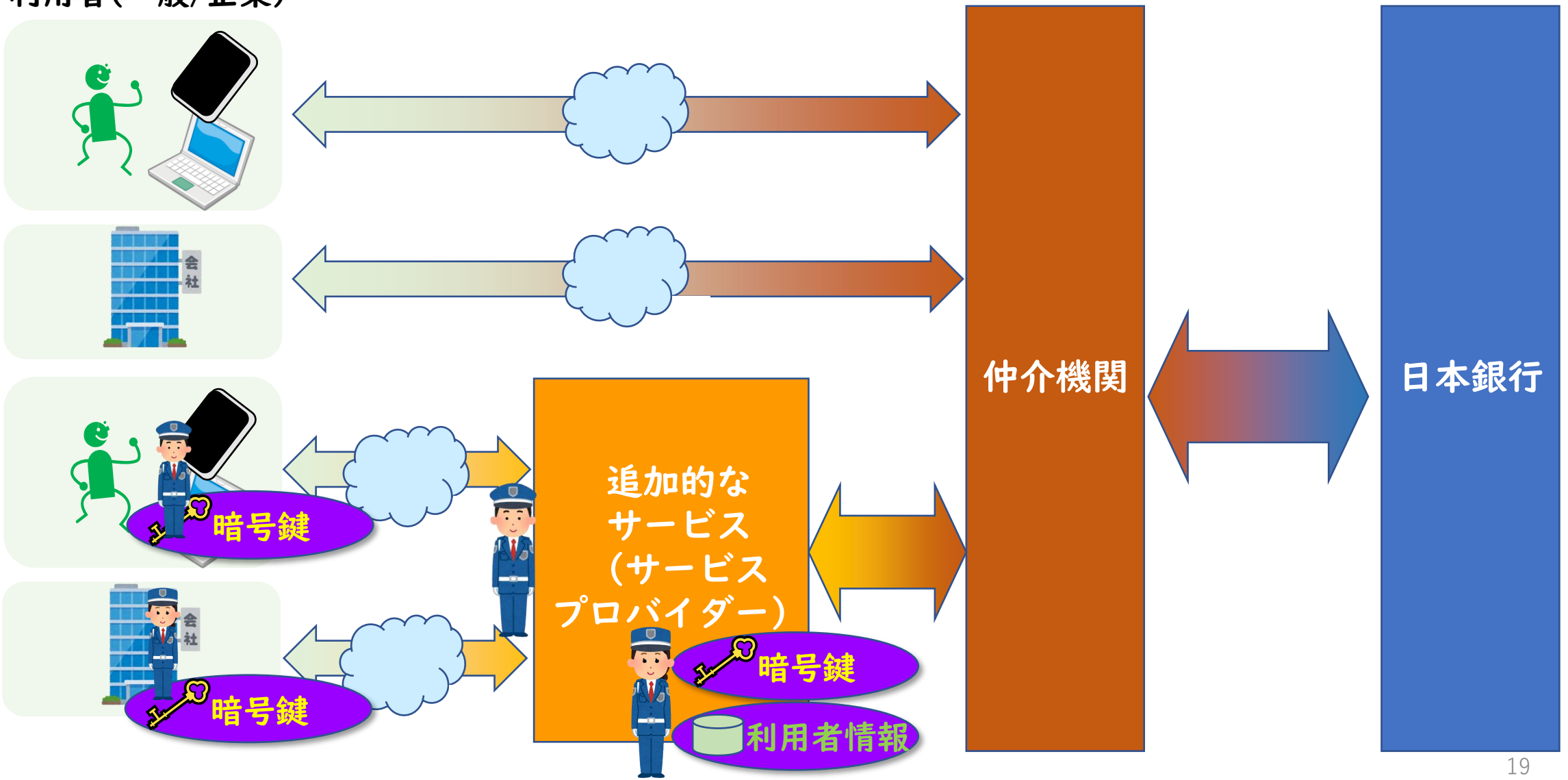
CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory



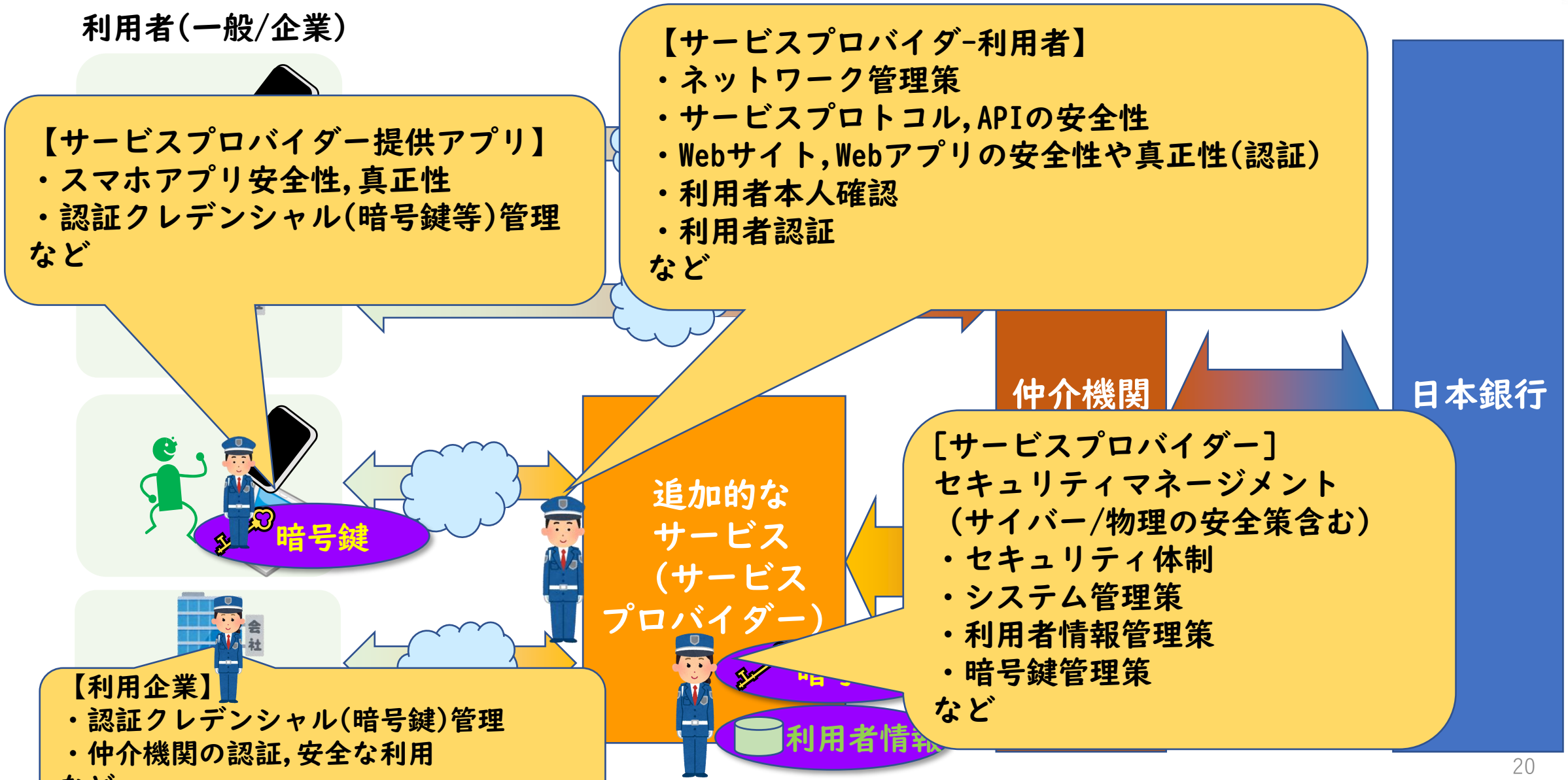
CBDCを取り巻く系全体のセキュリティ（例）

セコムIS研究所
Intelligent Systems Laboratory



CBDCを取り巻く系全体のセキュリティ(例)

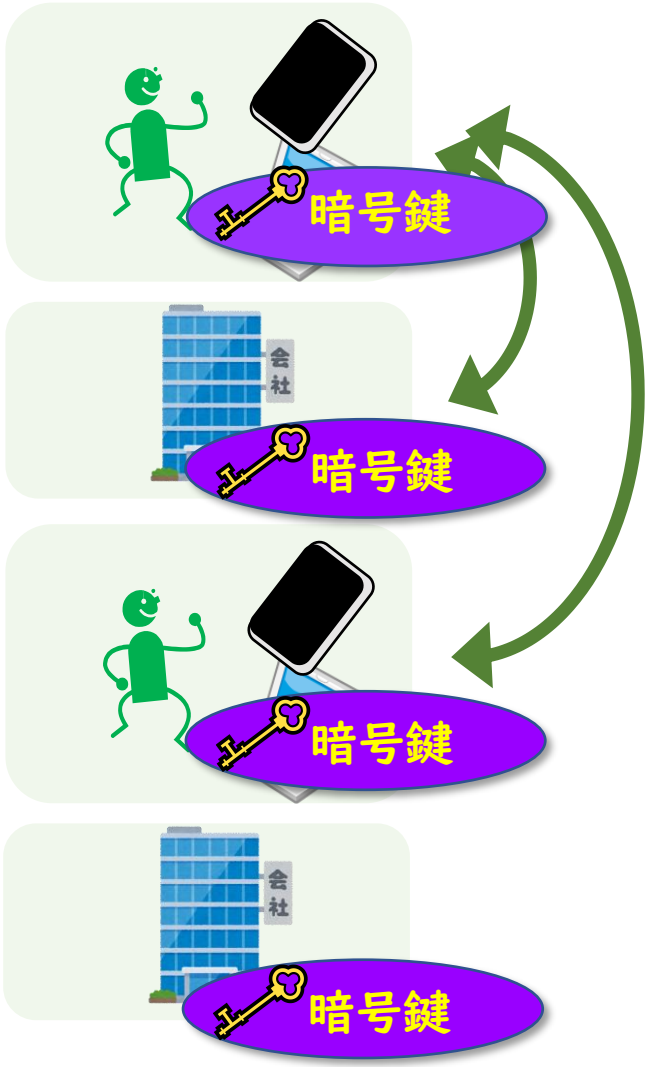
セコムIS研究所
Intelligent Systems Laboratory



CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory

利用者(一般/企業)



追加的なサービス(サービスプロバイダー)

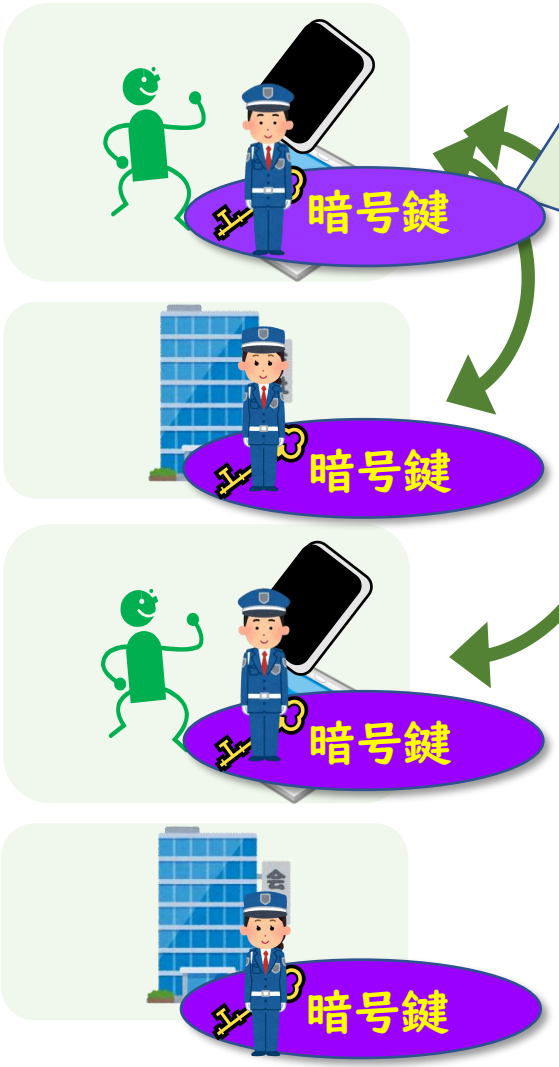
仲介機関

日本銀行

CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory

利用者(一般/企業)



【オフライン利用】
・CBDC送受プロトコル(オフライン)の安全性
・オフラインアプリ安全性・真正性
・CBDC管理の安全性
・認証クレデンシャル(暗号鍵等)管理の安全性

追加的な
サービス
(サービス
プロバイダー)

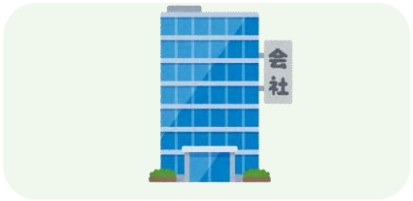
仲介機関

日本銀行

CBDCを取り巻く系全体のセキュリティ(例)

セコムIS研究所
Intelligent Systems Laboratory

利用者(一般/企業)



【全体】
・フィッシング対策
・アンチマネーロンダリング,テロ資金供与対策
・プライバシー保護
など

仲介機関

追加的なサービス(サービスプロバイダー)

日本銀行

セキュリティ関連の基準も沢山…

セコムIS研究所
Intelligent Systems Laboratory

- FISC安全対策基準
- PCI/DSS
- 金融庁各種ガイドライン
- ISO/IEC 27001/27002等の情報セキュリティマネージメントシステム関連規格
- FISC API接続チェックリスト
- Financial-grade API (FAPI)
- NIST SP800-63 Digital Identity Guidelines

などなど

誰が何のために何を守るのか？前提となるシステムは何か？などによって
行うべき対策やその重要度も変わる。

様々な既存の基準は参考になると考えられるが、それらの目的や前提が
あることを理解する必要がある。

CBDCではどんな前提で何を守らなければいけないのか？

CBDCを考える上でのある観点

セコムIS研究所
Intelligent Systems Laboratory

- **相互運用性とセキュリティ**
  仲介機関やサービスプロバイダーなど複数の主体にまたがって利用可能であることが求められる。
  セキュリティの差異による問題あるいは相互運用性のみを重視したセキュリティの低下は望ましくない。
  基準が求められる。
- **暗号鍵管理の重要性**
  暗号鍵管理は利用者側、仲介機関、サービスプロバイダーの重要なポイントとなりえる。
  特にオフラインを想定した場合に利用者デバイス側の暗号鍵管理（ウォレット）に留意する必要がある。
  暗号鍵の生成、利用、失効、廃棄、復旧などのライフサイクルを考える必要がある。
- **移行可能性**
  CBDCのプロトコルの移行、対応アプリケーションの移行、サポートするデバイスなどの環境。
  特に暗号アルゴリズム、暗号鍵サイズの移行を念頭に置いた設計や運用が必要である。
  CBDCの場合、より多くの利害関係者に及ぶ可能性がある。
- **保証レベル**
  サービスに応じたリスク評価と適切なセキュリティレベル。扱う金額や頻度、脅威の可能性、補償方法なども検討ポイントとなる。保証レベルを考慮したセキュリティ基準など。
- **プライバシーとAML/CFT**
  利用者のプライバシー保護とAML/CFTをどう両立していくか？

CBDCを考える上でのある観点

セコムIS研究所
Intelligent Systems Laboratory

本フォーラムの別セッションのテーマ
「標準化」や「ユニバーサルアクセス」
にも関連する項目が絡み合っている

- **相互運用性とセキュリティ**
  仲介機関やサービスプロバイダーなど複
  セキュリティの差異による問題あるいは
  基準が求められる。
- **暗号鍵管理の重要性**
  暗号鍵管理は利用者側、仲介機関、サービスプロバイダーの重要なポイントとなりえる。
  特にオフラインを想定した場合に利用者デバイス側の暗号鍵管理（ウォレット）に留意する必要がある。
  暗号鍵の生成、利用、失効、廃棄、復旧などのライフサイクルを考える必要がある。
- **移行可能性**
  CBDCのプロトコルの移行、対応アプリケーションの移行、サポートするデバイスなどの環境。
  特に暗号アルゴリズム、暗号鍵サイズの移行を念頭に置いた設計や運用が必要である。
  CBDCの場合、より多くの利害関係者に及ぶ可能性がある。
- **保証レベル**
  サービスに応じたリスク評価と適切なセキュリティレベル。扱う金額や頻度、脅威の可能性、補償方法なども検討ポイントとなる。保証レベルを考慮したセキュリティ基準など。
- **プライバシーとAML/CFT**
  利用者のプライバシー保護とAML/CFTをどう両立していくか？

CBDCを考える上でのある観点

セコムIS研究所
Intelligent Systems Laboratory

- **相互運用性とセキュリティ**
  仲介機関やサービスプロバイダーなど複数の主体にまたがって利用可能であることが求められる。
  セキュリティの差異による問題あるいは相互運用性のみを重視したセキュリティの低下は望ましくない。
  基準が求められる。
- **暗号鍵管理の重要性**
  暗号鍵管理は利用者側、仲介機関、サー
  特にオフラインを想定した場合に利用者
  暗号鍵の生成、利用、失効、廃棄、復旧

参考：
日本銀行ディスカッションペーパー 「スマートフォン等のスマート・デバイスにおけるセキュリティ：プラットフォーム化によるリスクの現状と展望」(2020-J-17, 2020年12月)

- **移行可能性**
  CBDCのプロトコルの移行、対応アプリケーションの移行、サポートするデバイスなどの環境。
  特に暗号アルゴリズム、暗号鍵サイズの移行を念頭に置いた設計や運用が必要である。
  CBDCの場合、より多くの利害関係者に及ぶ可能性がある。
- **保証レベル**
  サービスに応じたリスク評価と適切なセキュリティレベル。扱う金額や頻度、脅威の可能性、補償方法なども検討ポイントとなる。保証レベルを考慮したセキュリティ基準など。
- **プライバシーとAML/CFT**
  利用者のプライバシー保護とAML/CFTをどう両立していくか？

セコムIS研究所
Intelligent Systems Laboratory

ご清聴ありがとうございました