2023年11月1日

送金・決済分野におけるエンタープライズブロックチェーンの活用とセキュリティ等の課題

金融庁 総合政策局 フィンテック参事官室
林　敬祐

【講師紹介】

林　敬祐

金融庁 総合政策局フィンテック参事官室 課長補佐。弁護士（日本/NY州）。2018年からアンダーソン・毛利・友常法律事務所勤務。2022年から現職。ステーブルコインの仲介業者である電子決済手段等取引業者・電子決済等取扱業者の登録審査業務、暗号資産交換業者の監督業務、金融安定理事会（FSB）によるDeFi（分散型金融）の調査業務等に従事。

※講演・資料の内容は個人的な見解に基づくものであり、所属する組織とは一切関係ありません。

１．2022年改正資金決済法等の概要とデジタルマネー、ステーブルコインの整理

２．パーミッションレス型ブロックチェーン上で発行される暗号資産・ステーブルコインの取扱いに関するリスク

３．送金・決済分野におけるエンタープライズブロックチェーンの活用例と考えられるリスクや課題

安定的かつ効率的な資金決済制度の構築を図るための資金決済に関する法律等の一部を改正する法律（2023年６月施行）の概要

金融のデジタル化等に対応し、安定的かつ効率的な資金決済制度を構築する必要

○ 海外における電子的支払手段（いわゆるステーブルコイン（注））の発行・流通の増加
（注）利用者保護等に課題があるとの指摘

○ 銀行等における取引モニタリング等の更なる実効性向上の必要性の高まり（注）
（注）銀行界においてマネロン対応の共同化の動き

○ 高額で価値の電子的な移転が可能な前払式支払手段の広がり

電子決済手段等への対応

電子決済手段等取引業等の創設

○ 適切な**利用者保護等**を確保するとともに、分散台帳技術等を活用した**金融イノベーションに向けた取組み等を促進**

○ 電子決済手段等の発行者（銀行・信託会社等）と利用者との間に立ち、**以下の行為を行う仲介者**について、登録制を導入

［対象行為］➢ 電子決済手段の売買・交換、管理、媒介等
➢ 銀行等を代理して預金債権等の増減を行う行為
［参入要件］一定の財産的基礎、業務を適正かつ確実に遂行できる体制等
［規制内容］利用者への情報提供、体制整備義務等
［監　　督］報告、資料の提出命令、立入検査、業務改善命令等

【資金決済法第２条、第62条の３～第62条の24等】
【銀行法第２条、第52条の60の３～第52条の60の35等（信用金庫・信用組合の関連法も同様に措置）】

※ 電子決済手段；不特定の者に対して代価の弁済に使用すること等ができる通貨建資産であって、電子情報処理組織を用いて移転することができるもの等

※ 電子決済手段に該当する一定の信託受益権について金融商品取引法の適用対象から除外し、発行者となる信託会社等について資金決済法等の規律を適用
【金融商品取引法第２条等】【資金決済法第37条の２等】

※ 預金債権の増減を行う電子決済等取扱業者について、預金保険機構による報告、資料の提出命令、立入検査等に関する規定を整備　【預金保険法第37条等】

※ 仲介者たる電子決済手段等取引業者及び電子決済等取扱業者について、犯罪収益移転防止法の取引時確認義務等に関する規定を整備　【犯罪収益移転防止法第２条等】

銀行等による取引モニタリング等の共同化への対応

為替取引分析業の創設

○ 預金取扱金融機関等の委託を受けて、為替取引に関し、**以下の行為を共同化して実施する為替取引分析業者**について、**業務運営の質を確保**する観点から、許可制を導入　【資金決済法第２条、第63条の23～第63条の42等】

［対象行為］➢ 顧客の制裁対象者該当性の分析等（取引フィルタリング）
➢ 「疑わしい取引」該当性の分析等（取引モニタリング）
［参入要件］一定の財産的基礎、業務を適正かつ確実に遂行できる体制等
［規制内容］情報の適切な管理、体制整備義務等
［監　　督］報告、資料の提出命令、立入検査、業務改善命令等

高額電子移転可能型前払式支払手段への対応

○ **高額電子移転可能型前払式支払手段**の発行者について、不正利用の防止等を求める観点から、業務実施計画の届出、犯罪収益移転防止法の取引時確認義務等に関する規定を整備

※ 高額電子移転可能型前払式支払手段；電子情報処理組織を用いて高額の価値移転等を行うことができる第三者型前払式支払手段等　【資金決済法第３条、第11条の２等】【犯罪収益移転防止法第２条等】

デジタル・分散型金融への対応のあり方等に関する研究会」（第5回）2022年6月6日付金融庁「事務局説明資料」より抜粋

電子決済手段等への制度的対応

いわゆる法定通貨建てのステーブルコインの分類

【デジタルマネー類似型】

1 **法定通貨の価値と連動した価格（例：１コイン＝１円）で発行され、発行価格と同額で償還を約する**もの（及びこれに準ずるもの）

デジタルマネー（送金・決済の手段）として規律

【暗号資産型】

2 左記以外（アルゴリズムで価値の安定を試みるもの等）

暗号資産や金融商品として規律

1 【デジタルマネー類似型】（＝電子決済手段）等

発行者

銀行・資金移動業者

（注１）デジタルマネー類似型（＝電子決済手段）及び既存のデジタルマネー（預金・未達債務）の発行・償還は、為替取引に該当。
現行制度では、銀行・資金移動業者が行うこととされている。
（注２）発行者に係る規制の在り方は引き続き検討。

今回の法的手当

信託会社

（注３）信託受益権を用いる仕組み。

【金融商品取引法第２条等】
【資金決済法第37条の２等】

※マネロン等対策を含め、発行者が自ら行うことは可能

銀行代理業者
電子決済等代行業者
金融サービス仲介業者

仲介者 今回の法的手当

電子決済手段等取引業者 等

※利用者保護やマネロン等対策の観点から必要な対応を行う

（注４）取引実態等が類似する暗号資産交換業の規制を参考。
（注５）マネロンリスクへの対応、発行者と仲介者の責任関係の明確化等を求める。 【資金決済法第２条、第62条の３～第62条の24等】
【銀行法第２条、第52条の60の３～第52条の60の35等（信用金庫・信用組合の関連法も同様に措置）】
【預金保険法第37条等】 【犯罪収益移転防止法第２条等】

2 【暗号資産型】

発行者

―

（注１）以は暗号資産型の一部について、発行者に開示規制等を導入する規制案を公表。
（注２）利用実態や諸外国の動向も踏まえ、日本においても規制の在り方について引き続き検討。

仲介者

暗号資産交換業者

（注３）金融商品取引法が適用される場合もある。

デジタル・分散型金融への対応のあり方等に関する研究会」（第5回）2022年６月６日付金融庁「事務局説明資料」より抜粋

デジタルマネー、ステーブルコインの整理

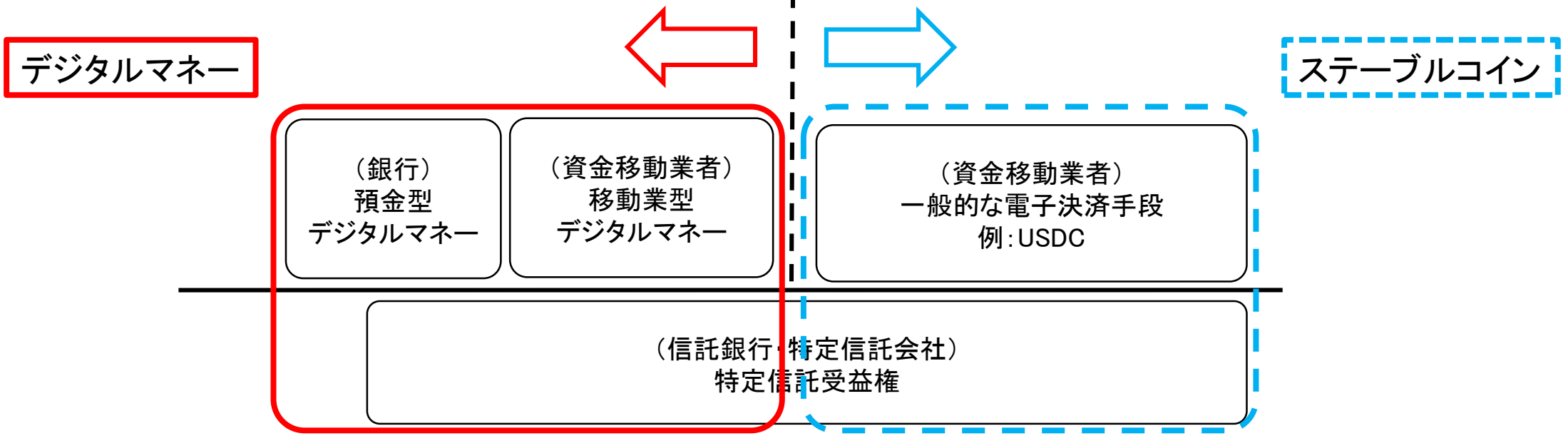
▶ 発行者が、本人確認（※）をした者にのみ移転を可能する技術的措置が講じられており、かつ、移転の都度発行者の承諾その他の関与が必要となる

例：
・パーミッションド型BC上のトークン
・パーミッションレス型BCを基盤としつつ、スマート・コントラクトにより登録されたアドレスにのみ移転可能とする機能等を用いて、移転先が本人確認済の者に限定されるトークン

※犯罪による収益の移転防止に関する法律に基づく取引時確認

▶ 左記の技術的措置等が講じられていない

例：一般的なパーミッションレス型BC上のトークン（本人確認をしない者同士の移転が可能なもの）



※本講演においては、エンタープライズブロックチェーン（パーミッションド型）はネットワークへの参加に管理者の許可が必要なもの（パーミッションレス型でもプロトコルの仕様等により、移転の都度発行者の承諾その他の関与が必要なものは、パーミッションド型に含める）を意味し、このブロックチェーン上に発行するものはデジタルマネー（左）、パブリックブロックチェーン（パーミッションレス型）はネットワークへの参加に制約のないものを意味し、このブロックチェーンに発行するものはステーブルコイン（右）を、それぞれ意味する。

特定信託受益権は、その仕様によりデジタルマネー、ステーブルコインのいずれの特徴のものもあり得る。法律上は「電子決済手段」に該当する。

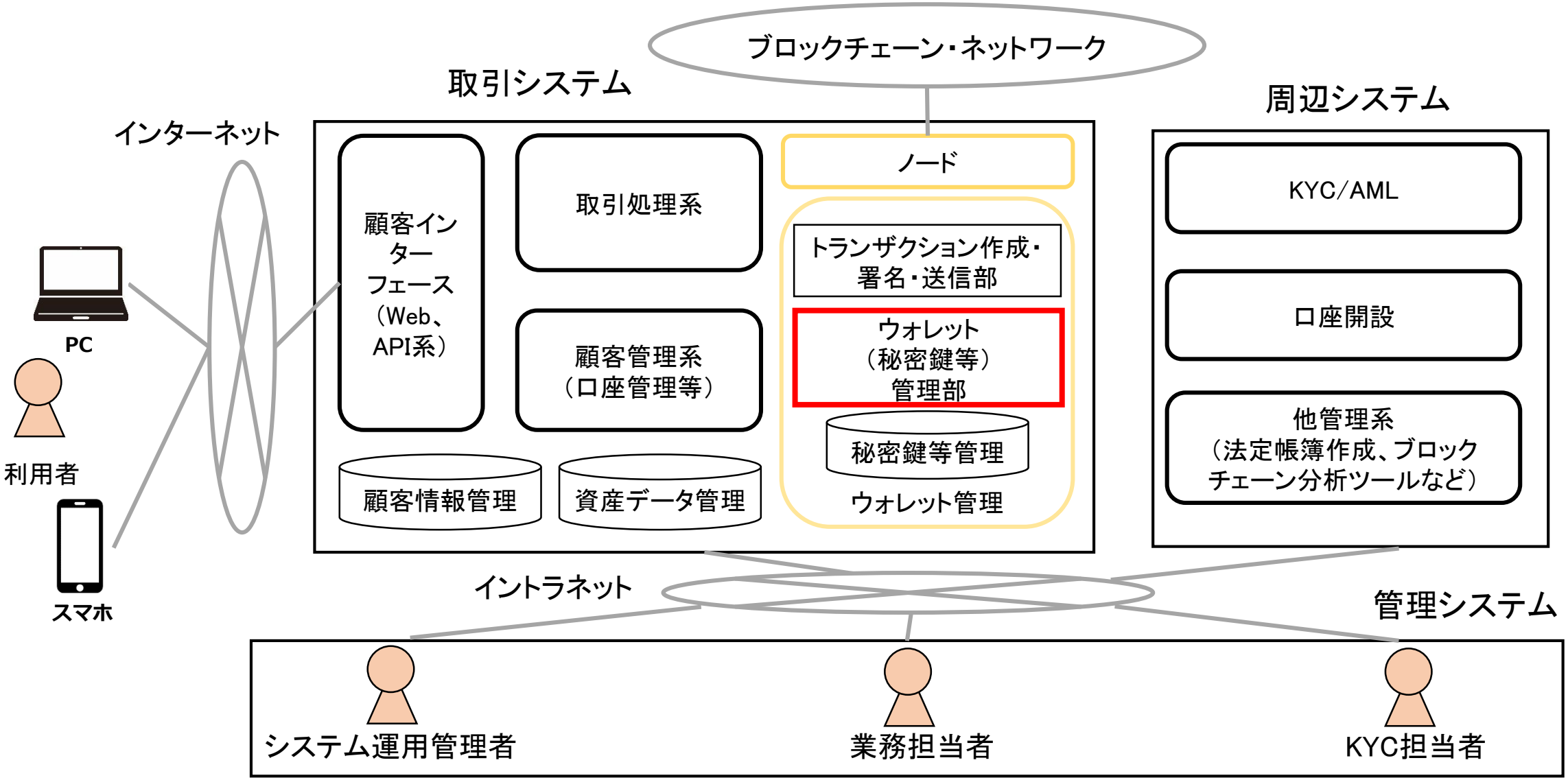
１．2022年改正資金決済法等の概要とデジタルマネー、ステーブルコインの整理

２．パーミッションレス型ブロックチェーン上で発行される暗号資産・ステーブルコインの取扱いに関するリスク

３．送金・決済分野におけるエンタープライズブロックチェーンの活用例と考えられるリスクや課題

暗号資産交換業者のシステム

・ノード（ブロックチェーンネットワークに接続するサーバや端末）を使って、暗号資産を移転するトランザクションを送信している。
・暗号資産の秘密鍵を管理するウォレットシステムを持つため、流出リスクに備えた高度なセキュリティ管理が求められる。



暗号資産交換業者におけるセキュリティリスクの要因の例

【パブリックブロックチェーン特有の要因】

・秘密鍵の窃取による暗号資産の不正流出。

・取引手数料の高騰によるブロックチェーン上の送金処理の遅延。

【システム的要因】

・リスト型攻撃により二要素認証未設定の利用者のアカウントからの暗号資産の不正流出。

・フィッシングメール、DDoS攻撃等。

【管理面・人為的要因（外部委託先管理を含む）】

・設定・作業ミス、リリース作業ミスによるサービス等の利用不可。

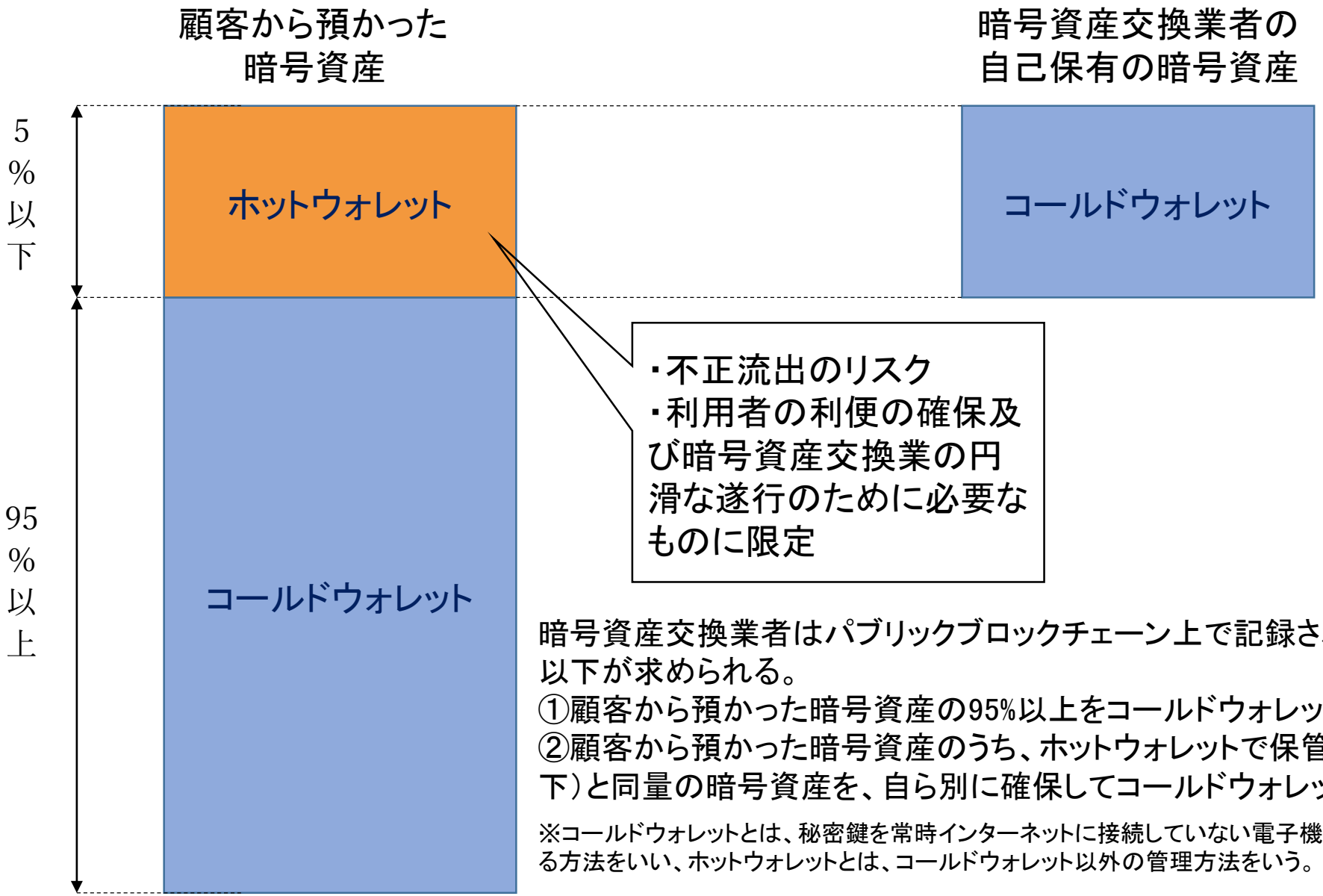
・委託先や外部サービスの障害の影響によるサービス等の利用不可。

暗号資産交換業者のサイバーセキュリティ事件

年月	事案	概要
2018年1月	コインチェック社事件	2018年1月26日、利用者から預託を受けた約580億円分の暗号資産NEMが外部からの不正アクセスにより流出。外部の者が、(a) 従業員の端末にマルウェアを感染させ、外部ネットワークから当該従業員の端末経由で当社のネットワークに不正にアクセスをし、遠隔操作ツールによりコインチェック社のNEMのサーバ上で通信傍受を行いNEMの秘密鍵を窃取したうえ、(b) 窃取したNEMの秘密鍵を使用して外部の不審通信先にNEMを不正送金したものと推定されている。 ※当時の法律上、コールドウォレットでの保管義務はなく、コインチェック社は暗号資産を全てホットウォレットに保管していた。
2018年9月	テックビューロ社事件	2018年9月14日、テックビューロ社が運営する取引所Zaifから約70億円分（顧客分が約45億円、自己保有分は約25億円）の暗号資産が流出。同年9月17日にサーバ異常を検知し、翌18日にハッキング被害が確認された。 ※外部から最後の不正アクセスを受けたのは2018年9月14日午後7時頃であったのに対し、それを検知したのが約3日後の同年9月17日で時間を要している。
2019年7月	ビットポイント社事件	2019年7月11日、ビットポイント社がホットウォレットに保管していた約30.2億円分（顧客預かり分が約20.6億円、自己保有分が約9.6億円）の暗号資産が外部からの秘密鍵の窃取・不正使用により流出。当社のウォレットサーバに作成されたバックドア型ウィルスにより、ホットウォレットの秘密鍵の窃取・不正使用がなされたものと考えられている。対顧客サービスのアクセス経路、執務エリアからの不正侵入の痕跡は見当たらなかったが、保守系サーバがハッキングされ不正侵入され、秘密鍵が盗取された可能性がある。 ※バックドア型ウィルスとは、コンピュータに外部から侵入しやすいように「バックドア」と呼ばれる裏口を作成するタイプのウィルスをいう。 ※コールドウォレットへの95%保管の義務づけに係る改正資金決済法は2019年5月31日に成立し、2020年5月1日に施行。本件は、改正法成立後、施行前に起きたもので、コールドウォレットへの対応の準備が求められる間に発生した事件。

※　以上はホームページ、報道等の公表されている情報に基づき作成。

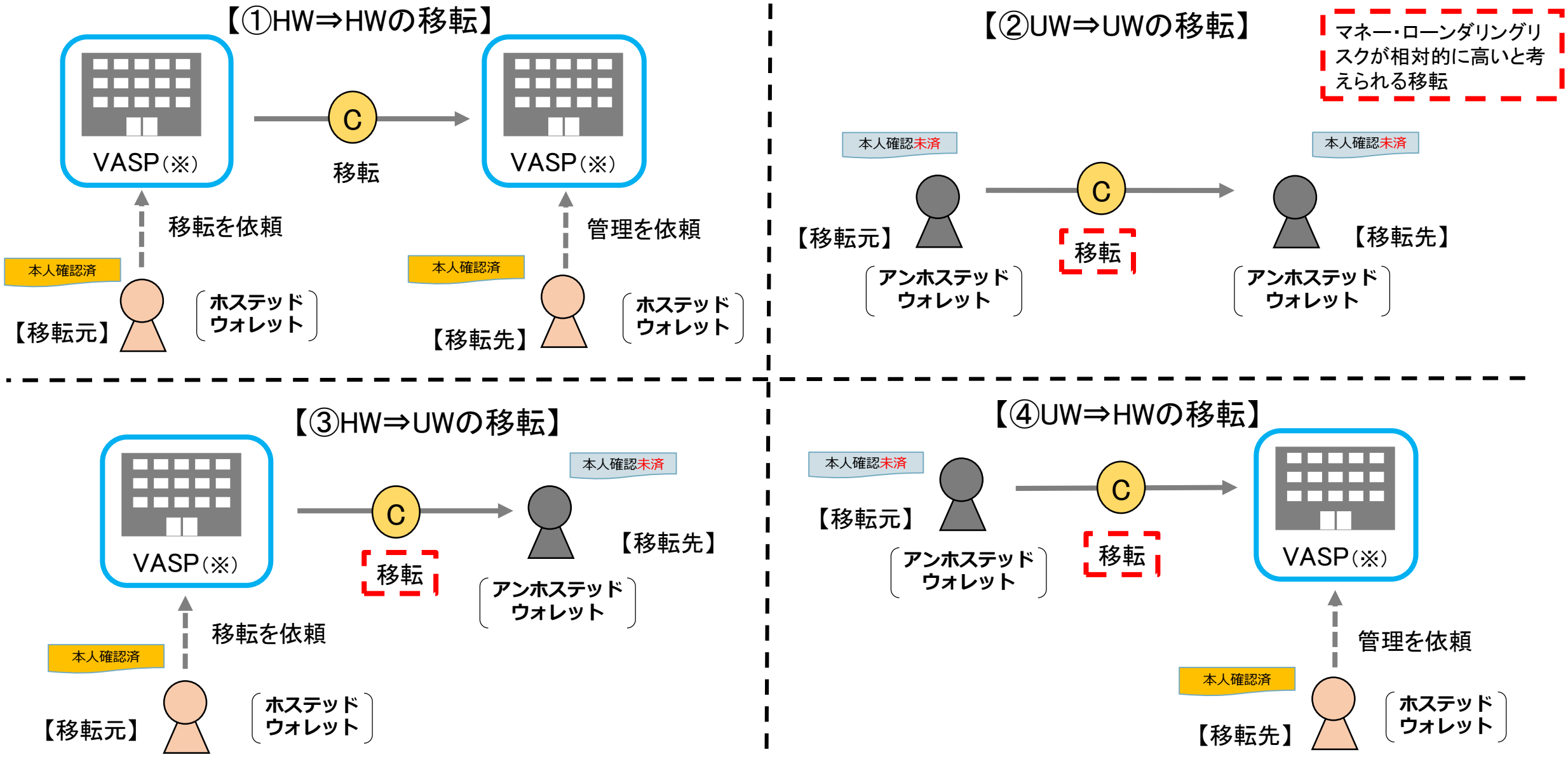
暗号資産交換業者のコールドウォレット規制



暗号資産交換業者はパブリックブロックチェーン上で記録されることを前提に以下が求められる。
①顧客から預かった暗号資産の95%以上をコールドウォレットで保管。
②顧客から預かった暗号資産のうち、ホットウォレットで保管するもの（5%以下）と同量の暗号資産を、自ら別に確保してコールドウォレットで保管。

※コールドウォレットとは、秘密鍵を常時インターネットに接続していない電子機器等に記録して管理する方法をいい、ホットウォレットとは、コールドウォレット以外の管理方法をいう。

パブリックブロックチェーン上のステーブルコインの移転の類型とマネー・ローンダリングリスク



※電子決済手段等取引業者を指す。UWの移転に係る取扱いをする際には、UWに関する移転元・移転先の情報収集、リスク分析等が求められる。

金融機関（特に銀行）がパブリックブロックチェーン（パーミッションレス型）上のステーブルコインを保有する上で考えられるリスク

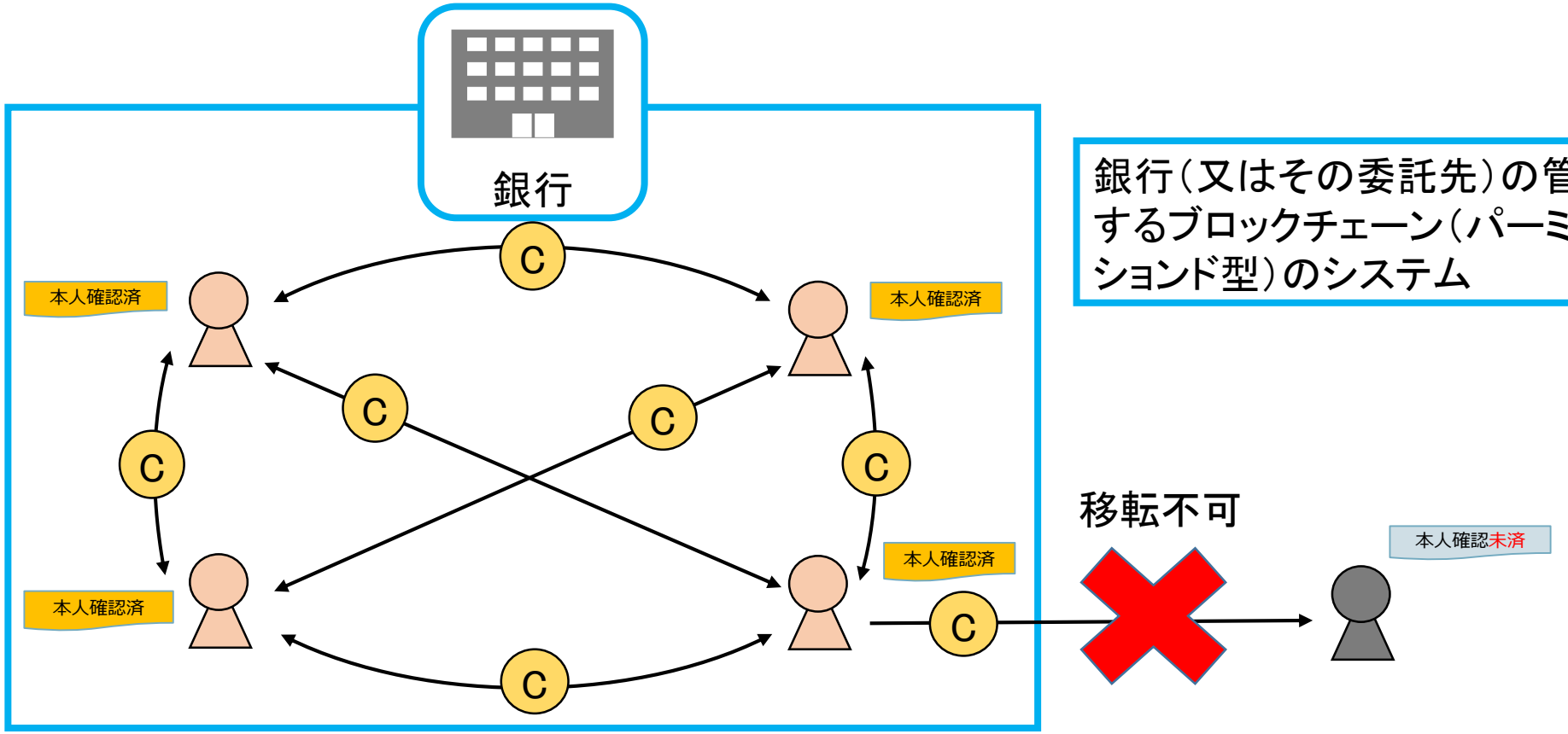
リスクの分類	内容
①システムリスク	システム上の誤作動、サイバー攻撃などのリスクがある。また、秘密鍵の不正流用により外部にステーブルコインが流出するリスクもある。
②マネー・ローンダリングリスク	パブリックブロックチェーン（パーミッションレス型）においては、誰でも参加が可能なため不正な取引に利用されるリスクがある。また、秘匿性の高い仕様のチェーンにおいては、取引の追跡が困難となる。
③価値変動リスク	法律上、保有者による償還のための裏付資産が確保されることから、理論上は価値変動がほとんどない又はあるとしても小さいと考えられる。
④レピュテーショナル・リスク	ステーブルコインに関する以上のリスクが顕在化することで、銀行のレピュテーションが低下するリスクが認められる。

１．2022年改正資金決済法等の概要とデジタルマネー、ステーブルコインの整理

２．パーミッションレス型ブロックチェーン上で発行される暗号資産・ステーブルコインの取扱いに関するリスク

３．送金・決済分野におけるエンタープライズブロックチェーンの活用例と考えられるリスクや課題

エンタープライズブロックチェーン（パーミッションド型）上のデジタルマネー



※エンタープライズブロックチェーンは、特定の企業や企業群が、各参加者やチェーン上のトークンの移転や記録を管理することができるブロックチェーン（パーミッションド型）を指します。

国内におけるブロックチェーン技術を用いたデジタルマネー等に関するプロジェクトの例

プロジェクト名 （関連主体）	概要	台帳
Progmat （三菱UFJ信託銀行等）	株式会社Progmatが管理するプラットフォームのブロックチェーン上で、ステーブルコインの発行を希望する各事業者の委託に基づき、発行主体となる各信託銀行がステーブルコインを発行し、決済等のためにブロックチェーン上を移転する。また、同プラットフォーム上では、セキュリティ・トークン（デジタル有価証券）やユーティリティトークン（NFT等）などのデジタル資産とステーブルコインによるDvP（Delivery vs Payment）決済をすることも想定している。	Corda等 （パーミッションレス。一部パーミッションドもあり）
デジタル通貨フォーラム （ディーカレットDCP等）	民間銀行が預金としてデジタル通貨DCJPYを、ディーカレットDCPが提供するプラットフォームのブロックチェーン上に発行し、送金・決済等のために用いる。また、事業者が同プラットフォーム上にセキュリティ・トークン（デジタル有価証券）、NFTなどのデジタル資産を発行し、DCJPYとのDvP決済をすることも想定している。	ハイパーレジャーベース （パーミッションド）
珠洲トチツーカ （北國銀行、Digital Platformer、珠洲市等）	北國銀行、Digital Platformer、石川県珠洲市等が共同で連携し、珠洲市が発行するポイント「珠洲トチポ」や北國銀行が発行するステーブルコイン（注：デジタルマネー）「珠洲トチカ」をブロックチェーン上で発行し、珠洲市にある加盟店で決済手段として用いることを想定している。	SHIKI （パーミッションド）
ステーブルコイン実証実験 （G.U.Technologies等）	G.U.Technologies、東京きらぼしフィナンシャルグループ、Minna no Ginko、四国銀行は、バリデーターが日本企業であるJapan Open Chainのブロックチェーン上で、ステーブルコイン（注：デジタルマネー）の発行や送金を行う実証実験を開始した。	Japan Open Chain （パーミッションド）

※　以上はホームページ、報道等の公表されている情報に基づき作成。

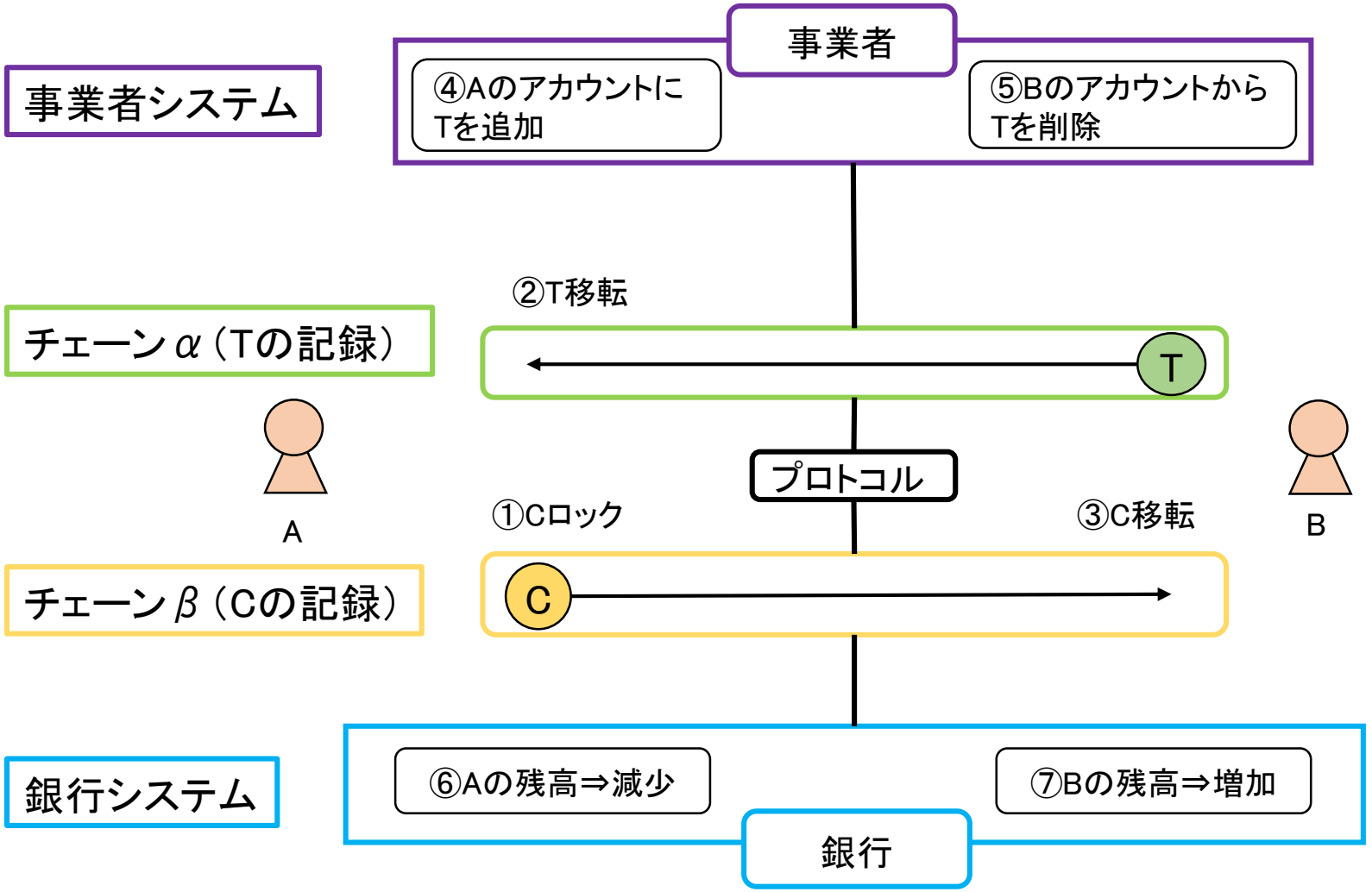
海外におけるブロックチェーン技術を用いたデジタルマネー等に関するプロジェクトの例

プロジェクト名 （関連主体）	概要	台帳（レジャー）	法域
欧州投資銀行債 （欧州投資銀行、ゴールドマン・サックス、BNPパリバ、HSBC、RBCキャピタル・マーケッツ等）	欧州投資銀行は、2022年11月、1億ユーロのデジタル債をプライベートチェーン上で発行し、ゴールドマン・サックスのトークンプラットフォームであるGS DAP™上に発行。現金の分散型台帳はフランス銀行の提供するもので、実験的にCBDCを用いて、DvP(Delivery vs Payment)決済がなされた。なお、投資家への情報提供の目的でパブリック・ブロックチェーンを用いる。ソシエテ・ジェネラル証券サービシーズ、ゴールドマン・サックス・バンク・ヨーロッパが投資家に、カストディ業者、アカウント管理者としてサービスを提供した。	GS DAP™ （パーミッショんド）	ルクセンブルク
JPM コイン （Onyx、JPモルガン等）	JPM コインはブロックチェーン上に記録される預金で、決済ネットワークと預金アカウントとして機能する。企業間の決済に用いられ、PvP（Payment vs Payment）決済と将来的にはDvP決済の流動性提供を行う予定。2020年に正式にローンチし、最初は米ドルの取引に用いられていたが、最近ユーロの取引にも用いられるようになった。	Quorum （パーミッショんド）	米国、EU
Regulated Liability Network （ニューヨーク連邦銀行等）	ニューヨーク連邦銀行を含む金融セクターが12週間の概念実証に参加し、各金融機関で共有された台帳上に記録されるトークン型預金と中央銀行デジタル通貨（CBDC）を用いて、国内の決済及びクロスボーダーの決済の実験を行い、決済の効率性等の有用性を発見した一方で、実際に導入する上で、新たなインフラの投資が必要であること、スケーラビリティのためにネッティングの運用が必要などの課題も発見した。	SETL （パーミッショんド）	米国
Brazilian Digital Real (DREX) （ブラジル中央銀行等）	ブラジル中央銀行が、ブラジル国債、トークン型預金、ホールセールCBDCを含む様々な種類の資産をトークン化することを企図したプロジェクトで、金融資産とCBDC・トークン型預金のDvP決済の円滑化とコスト減少を図る。本プロジェクトを通じて、個人が金融市場に参加することを容易にすることと、民間セクターが金融サービスのイノベーションを起こすプラットフォームを提供することを目的とする。	Hyperledger Besu （パーミッショんド）	ブラジル
Bakong （カンボジア国立銀行、ソラミツ等）	カンボジア国立銀行が主導し、紙幣や小切手による決済の割合が多いカンボジアにおいて、決済の効率性や成長する経済を支えること等を目的として、2020年10月デジタルマネーであるBakongがプライベートチェーン上で発行された。主にリテール決済に用いられるが、銀行間の大口決済にも利用可能となっている。	Hyperledger Iroha （パーミッショんド）	カンボジア

※　以上はホームページ、報道等の公表されている情報に基づき作成。

エンタープライズブロックチェーン（パーミッションド型）上で考えられるデジタルマネーを用いた決済の場面①

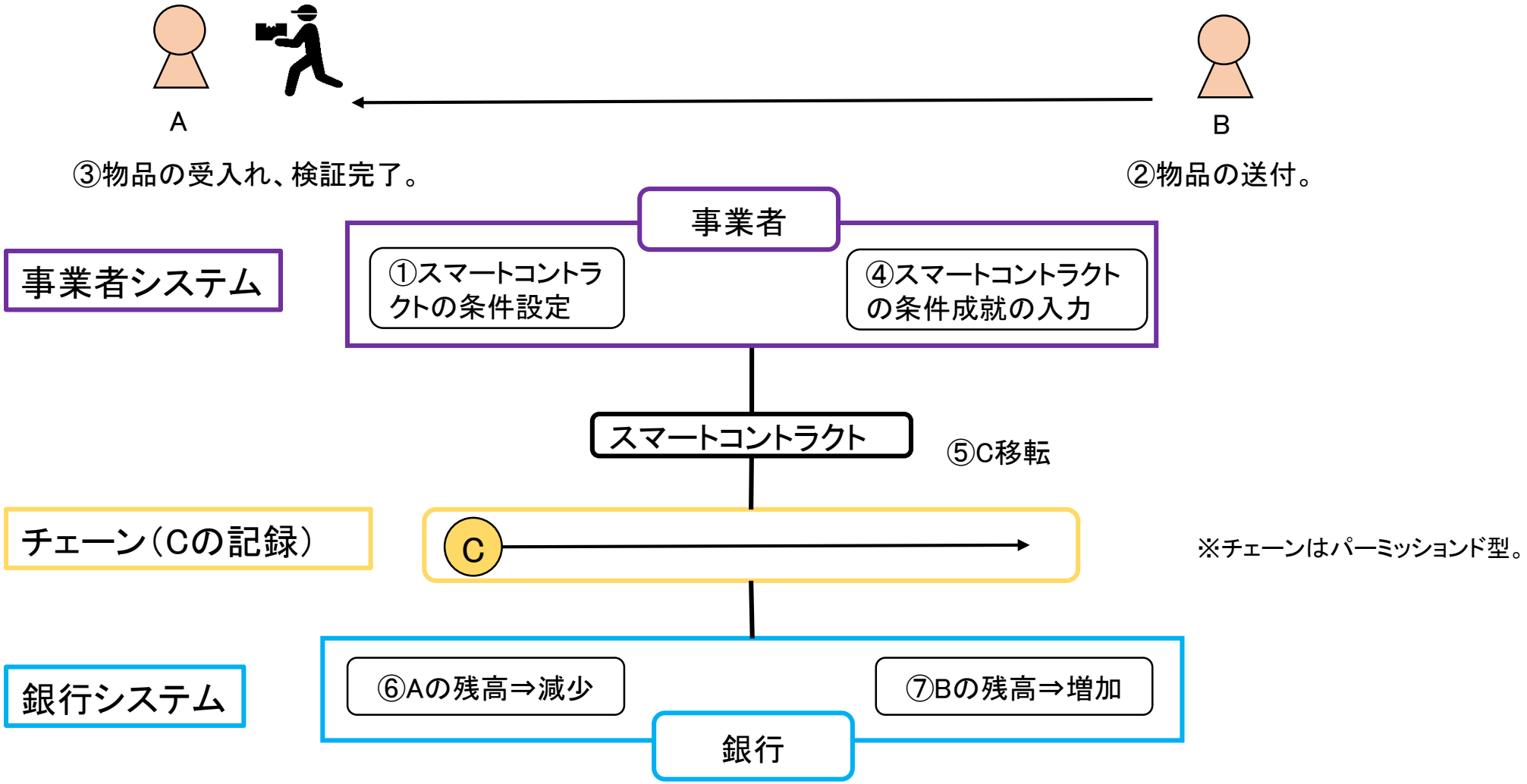
AがBからT（トークン）を購入し、C（デジタルマネー）で支払う、DvP（Delivery vs Payment）決済の場面。トークンの記録は事業者が、デジタルマネーの記録は銀行がそれぞれ管理。



※T（トークン）は、暗号資産、NFT、セキュリティ・トークン（デジタル有価証券）、他のデジタルマネー等が想定される。
チェーンαはパーミッションレス型・パーミッションド型の両方あり得る。
チェーンβはパーミッションド型。

エンタープライズブロックチェーン（パーミッションド型）上で考えられるデジタルマネーを用いた決済の場面②

AがBから物品を購入し、Bからその納入を受けてAの検証が完了したことをもって、AからBにC（デジタルマネー）を支払う場面。
スマートコントラクトに関する条件の設定・入力を事業者側で行い、デジタルマネーの記録は銀行が管理。



決済・送金分野におけるエンタープライズブロックチェーンで考えられるリスクや課題

ブロックチェーン特有の課題	
相互運用性	DvP決済、PvP決済等の異なるブロックチェーン間の決済を同時に行う場合の技術的課題。
スケーラビリティ	多くの決済・送金を処理するにはグロス決済だけではなく、ネッティング決済の運用の検討、セカンドレイヤーによる処理の効率化等が必要となり得る。
費用	ブロックチェーンのシステムや機器等の新しい導入や新しい人材の育成・採用が必要で、システム導入費・人件費がかかる。
スマートコントラクトの脆弱性	プラットフォームに組み込まれるスマートコントラクトに不備が生じると取引・決済に支障が生じる。またスマートコントラクトの脆弱性を突いた攻撃を受けるおそれ。
オラクル（情報）	ブロックチェーン外の情報（オラクル）を踏まえて、取引・決済を実行する場合はその正確性を担保する必要。また、オラクル自体が悪意のある攻撃を受け、不適切な情報により取引・決済が実行される可能性。
パブリックBCの特性	パブリックブロックチェーンを用いる場合は秘密鍵の不正利用によるブロックチェーン上のトークンの流出のおそれ。
システム一般の課題	
・ソフトウェア障害（プログラム誤り等）。 ・DDoS攻撃、標的型メール等のプログラム脆弱性を突いた攻撃。 ・リスト型攻撃、フィッシング、不正アクセス、マルウェア等の感染。	

ご清聴ありがとうございました。