暗号資産関連業者における
サイバーセキュリティの課題と対策に関する研究調査

概要

2026年6月30日

合同会社デロイト トーマツ

暗号資産関連業者におけるサイバーセキュリティの課題と対策に関する研究調査 概要

■ 2017年度より毎年金融庁が実施するブロックチェーン「国際共同研究」プロジェクトでは、有識者と連携の上、分散型金融システムにおける技術リスク等についての研究調査が行われている。2025年度は、合同会社デロイト トーマツが委託を受け、**「暗号資産関連業者におけるサイバーセキュリティの課題と対策に関する研究調査」**をテーマに研究調査を実施。

■ 2026年 4 月に金融庁が公表した「暗号資産交換業等におけるサイバーセキュリティ強化に向けた取組方針」では、**①同プロジェクトの結果を暗号資産交換業者や情報共有機関等へ還元する**こと、**②国際的な場における議論の題材として提供することで国際的な連携の深化を図る**こと、**③事務ガイドラインにおけるサイバーセキュリティ水準の引上げの検討に活用する**ことが記載されている。

■ 同研究調査の構成は以下のとおり。

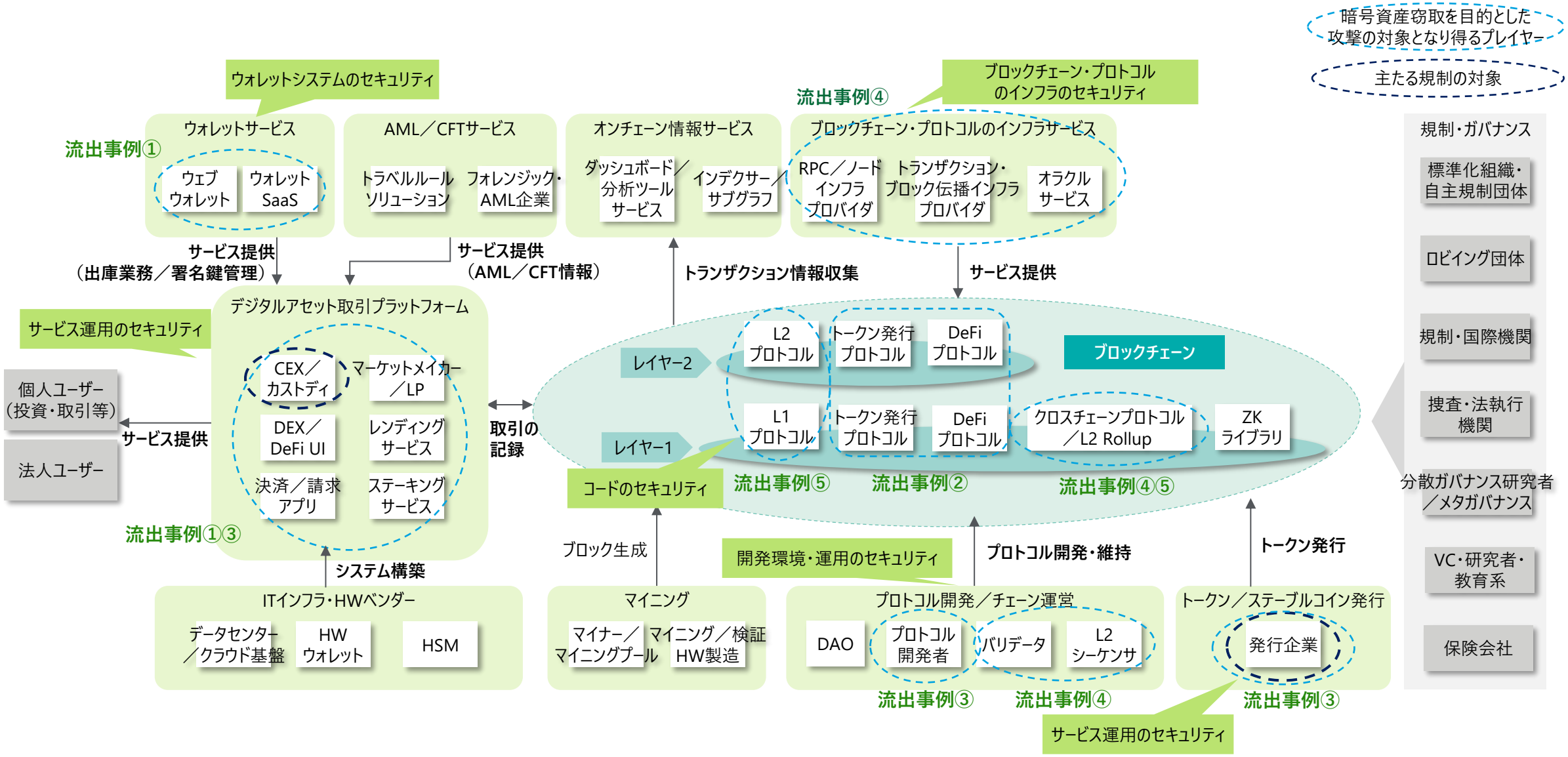
1. **暗号資産業界におけるサプライチェーンとそのリスクの把握**
   暗号資産業界における**サプライチェーン上の主要なプレイヤー**を整理。また、**交換業者（≒CEX）の出庫フローにおける攻撃対象**を整理。
2. **近年の国際的な流出事例の分析**
   被害額や攻撃手法の種類を踏まえて海外の代表的な流出事例を選定し、**攻撃プロセスと講じるべきだった対策**を整理。
3. **暗号資産特有リスクの分析と推奨事項**
   流出事例の分析で特定されたリスクを**国内外の既存のサイバーセキュリティに関するルールに照合**し、具体的な対策例を提示。

■ 本研究取り纏めに当たっての主なヒアリング先

- 有識者会議：京都大学・岩下直行名誉教授、米ジョージタウン大学・松尾真一郎研究教授
  日本銀行・デジタル庁がオブザーバー参加
- Japan Fintech Week2026期間中の当庁主催ラウンドテーブルにて、有識者から作成中の報告書へのフィードバックを収集
- 個別ヒアリング：Fireblocks、タレスDISジャパン株式会社、DFNSなどよりヒアリング実施

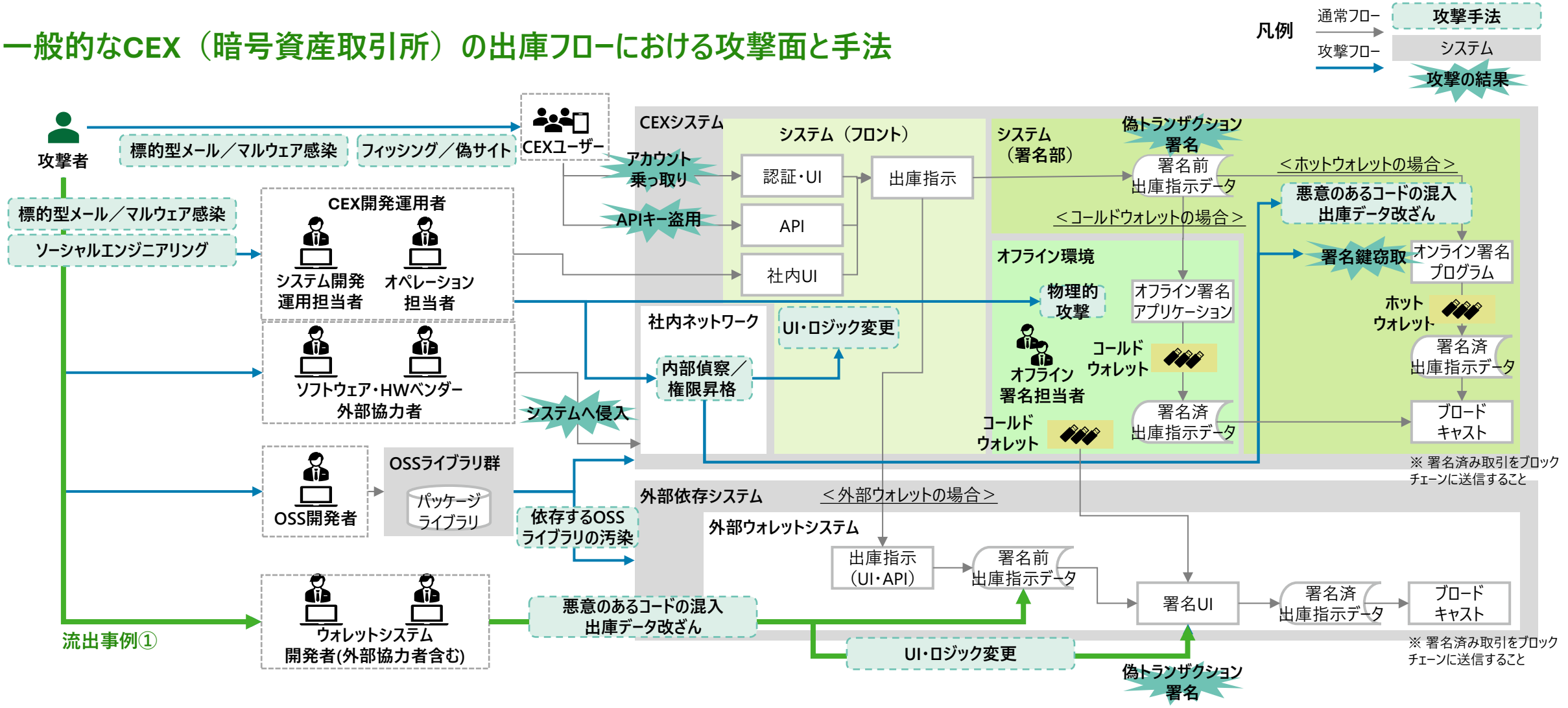
暗号資産業界におけるサプライチェーンとそのリスクの把握

暗号資産エコシステムに関わるプレイヤー俯瞰図



暗号資産業界におけるサプライチェーンとそのリスクの把握

一般的なCEX（暗号資産取引所）の出庫フローにおける攻撃面と手法



CEX開発運用者を経由する攻撃：CEX開発運用者へのソーシャルエンジニアリング等により社内ネットワークに侵入し、悪意のあるコードの混入、UI・ロジック変更、物理攻撃によってCEXシステムの中枢（出庫指示や署名等）を攻撃する手口
ソフトウェア・HWベンダー外部協力者を経由する攻撃：外部の開発協力者へのソーシャルエンジニアリング等により社内ネットワークに侵入し、悪意のあるコードの混入、UI・ロジック変更、物理攻撃によってCEXシステムの中枢を攻撃する手口
OSS（オープンソースソフトウェア）開発者を経由する攻撃：標的型メール等でOSS開発者を侵害し、OSSライブラリを汚染してCEXシステムまたは外部ウォレットシステム全体へ波及させる手口（※OSS: コードが公開されているソフトウェア／ライブラリ: 他のシステムから部品として使われるプログラム）
ウォレットシステム開発者を経由する攻撃：ウォレットシステム開発者へのソーシャルエンジニアリング等によりPCにマルウェアを感染させて外部ウォレットシステムへの接続権限を取得し、悪意のあるコード混入、UI・ロジック変更によって外部ウォレットシステムの中枢を攻撃する手口

近年の流出事例及び暗号資産特有リスクの分析

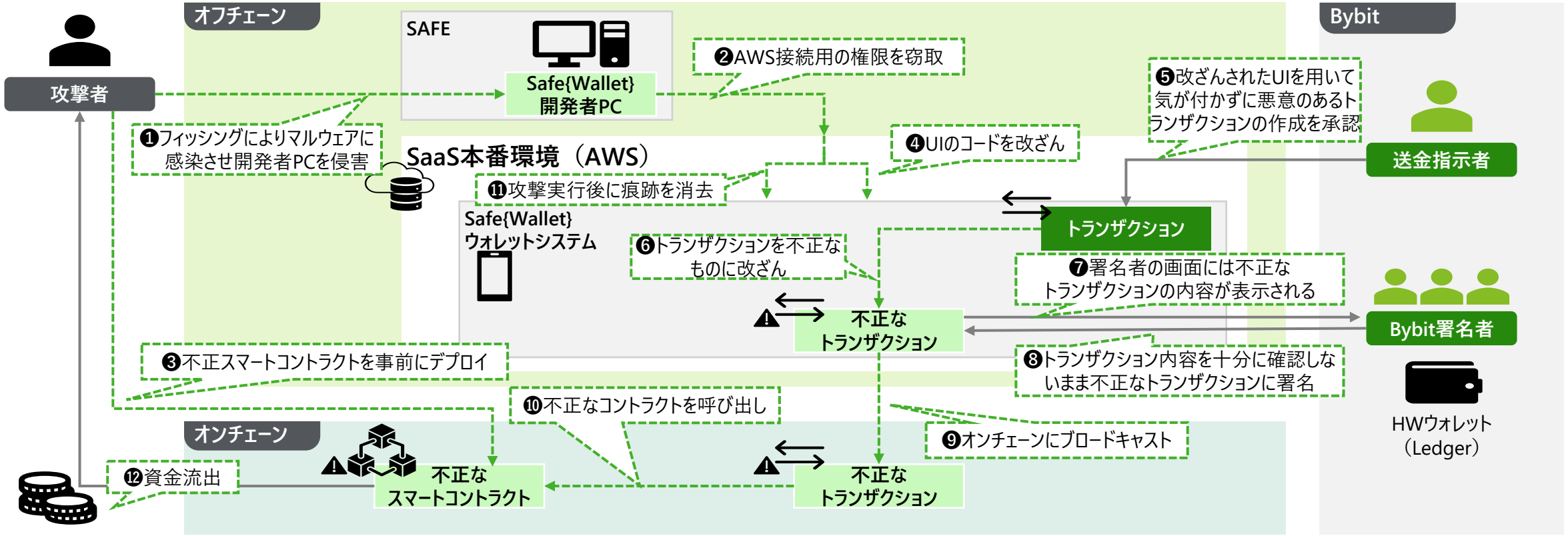
事例①: Bybit（委託先侵害・ブラインド署名）

攻撃の概要

■ 攻撃者は、Bybitが利用していた外部ウォレットサービス（Safe）に対して**ソーシャルエンジニアリング**を仕掛け、トランザクション生成のためのUIを改ざんした。その結果、Bybitの送金指示者は、改ざんされたUIを用いて不正なトランザクションの生成を承認した。また、Bybitの署名者が署名に用いるハードウェアウォレットには、不正なトランザクションの内容が表示されていたが、十分に確認されないまま署名した結果、不正なトランザクションが実行され、流出につながった。

事例分析より得られた経験

■ スマートコントラクトの取引内容を表示するウォレット画面は、人間にとって可読的ではない。そのため、**内容を十分に確認しないまま署名する「ブラインド署名」**が起こりやすい。Bybitの事例に限らず、交換業者による**ステーキングサービスの利用**等の際に、交換業者によるトランザクション送信先がスマートコントラクトとなる場合、「ブラインド署名」が起こるリスクに留意が必要となる。



参考：「Bybit Incident Investigation Preliminary Report」（Verichains）_2026年1月時点

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

近年の流出事例及び暗号資産特有リスクの分析

事例②：Euler Finance（スマートコントラクトのコード脆弱性の悪用）

Euler Financeの仕組み

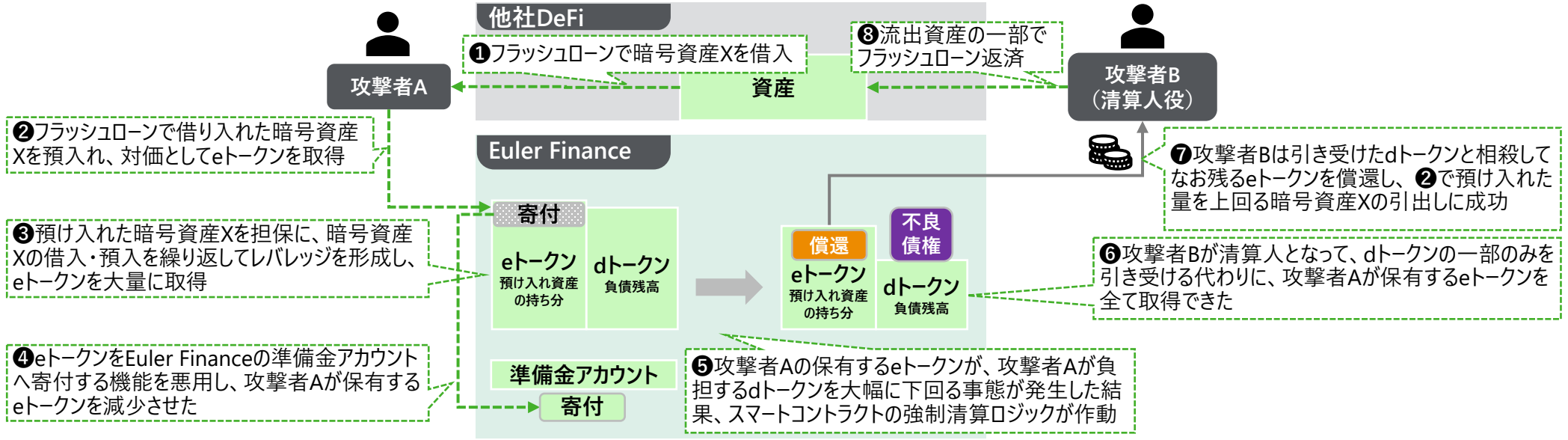
- Euler Finance（以下、Euler）は、ユーザーが暗号資産Xを預け入れると、その持ち分を表すeトークンを発行するDeFiプロトコルである。預け入れられた資産Xが他のユーザーに貸し出されることで発生する利息は、eトークンの価値に反映される。また、ユーザーがEulerから暗号資産Xを借り入れる場合には、返済義務を表すdトークンを引き受ける。Eulerでは、ユーザーが預け入れた資産Xを担保に暗号資産Xを借り入れ、その借り入れた資産Xを再び預け入れることで、レバレッジを形成できる。
- Eulerでは、ユーザーが保有するeトークンの価値が、ユーザーが負担するdトークンの価値に対して十分な余裕を持って上回っていない場合、プロトコル上、強制清算が発生する。強制清算においては、清算人は、ユーザーの債務を全て引き受ける代わりに、ユーザーのeトークンの一部を取得する。清算人は、取得したeトークンのうち、引き受けた返済義務の価値との差分をEulerに償還することで、利益を得ることができる。

攻撃の概要

- 攻撃者Aがフラッシュローンで借り入れた暗号資産XをEulerに預け入れ、借入と再預入を繰り返すことで大きなレバレッジポジションを形成した。
- 攻撃者Aは寄付機能を悪用し、自らが保有するeトークンを減少させた。これにより、eトークンの保有総額がdトークンの保有総額を大幅に下回るという、通常想定されていない状態が発生した結果、スマートコントラクトの強制清算ロジックが作動した。その結果、攻撃者Aと共謀する攻撃者Bが清算人となり、dトークンの一部のみを引き受ける代わりに、攻撃者Aが保有するeトークンを全て取得できた。Eulerには、攻撃者Bにより引き受けられなかったdトークンが不良債権として残り、Eulerが損失を負担することとなった。
- その後、引き受けたdトークンと相殺してなお残るeトークンが攻撃者の手元に残り、その償還によって、攻撃者Aが当初Eulerに預け入れた量を大きく上回る暗号資産Xの引き出しに成功した。

事例分析より得られた経験

- DeFiではスマートコントラクトのコードが資産管理のルールそのものとなるため、**スマートコントラクトのコードに脆弱性があると直接的な資産流出につながる**。
- 交換業者にDeFi等のスマートコントラクトと依存関係がある場合、その脆弱性は交換業者にも波及する可能性がある（**サプライチェーンリスク**）。



参考：「$197 Million Stolen: Euler Finance Flash Loan Attack Explained」（Chainalysis）2026年3月時点

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

近年の流出事例及び暗号資産特有リスクの分析

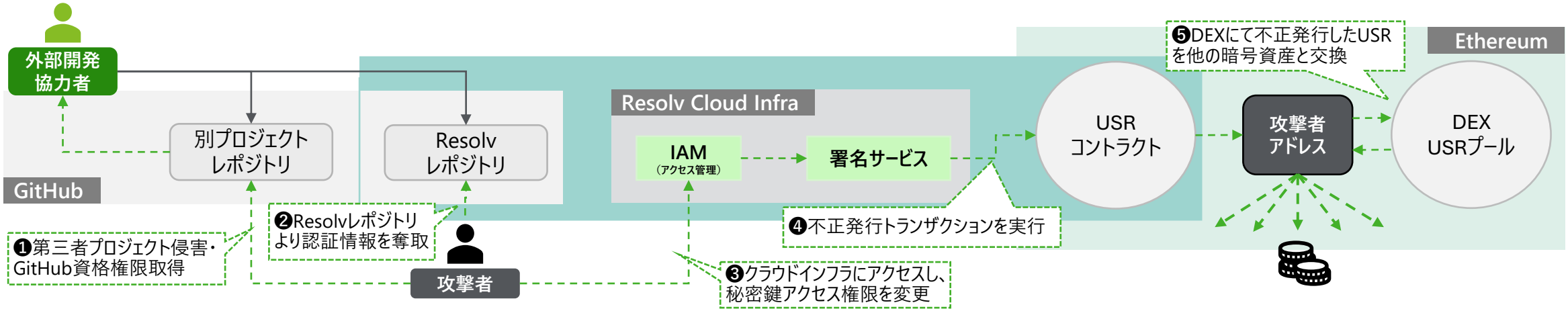
事例③: Resolv Protocol（不正発行）

攻撃の概要

- Resolvは暗号資産等（ETH、BTC、USDC等）を担保とする「ステーブルコイン」USRを発行するDeFiプロトコル。
- 攻撃者は、Resolvの外部開発協力者に**ソーシャルエンジニアリング**を仕掛けて、盗んだ資格情報を使ってResolvのクラウド環境に侵入し、「ステーブルコイン」発行用スマートコントラクトの署名権限を奪取した。その結果、裏付資産のない「ステーブルコイン」が不正に大量発行された。

事例分析より得られた経験

- ステーブルコイン発行用スマートコントラクトでは、発行権限の管理が極めて重要。
  署名権限の管理が不十分な場合、権限を奪われた攻撃者に**裏付資産のないステーブルコインを不正発行される可能性**がある。
- 不正発行されたステーブルコインが市場に流通すれば、**交換業者や利用者にも損失が波及**する。



【参考】Resolv Postmortem: March 22, 2026 Incident

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

近年の流出事例及び暗号資産特有リスクの分析

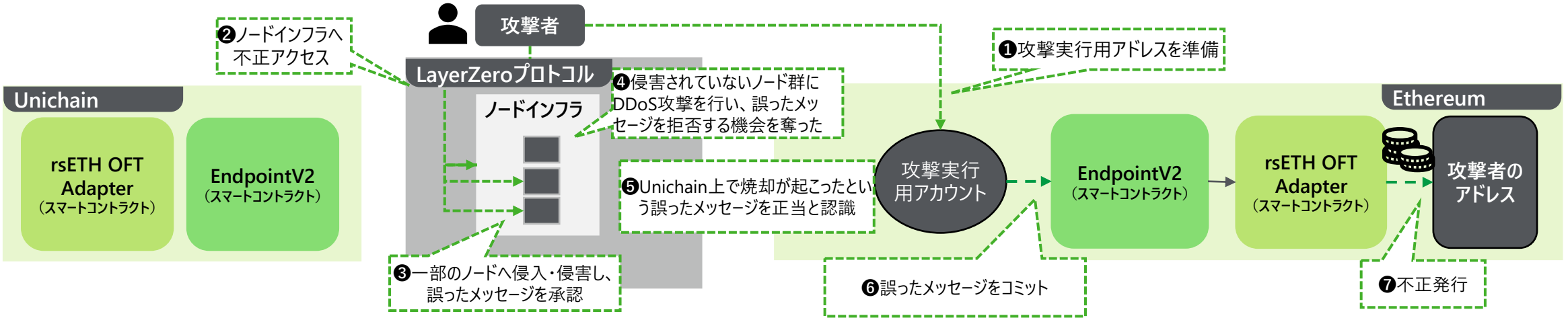
事例④: Kelp DAO/LayerZero（不正発行・クロスチェーンプロトコル脆弱性）

攻撃の概要

- LayerZeroは、異なるブロックチェーン同士を接続し、メッセージを相互にやり取りできるようにするクロスチェーンプロトコル。
  チェーンA上でトークンXを焼却し、その情報をチェーンBへ伝達し、チェーンB上でトークンXを発行する仕組み。
- Kelpは、DeFiステーキングプロトコルで、ETHのステーキングを行うユーザーにrsETH（Kelpに預けられるETHに対する持分を表すトークン）を発行。
  複数のチェーン上でrsETHを流通させるため、LayerZeroを使用。
- 攻撃者は、Unichain上でrsETHが焼却されたように見せかける偽情報を作成して、Ethereumへその情報を伝達する役割を担うノードを誤認させた。
  その結果、実際にはUnichain上での正当な焼却処理が無いにも関わらず、Ethereum上で攻撃者のアドレスへ不正にrsETHが発行された。

事例分析より得られた経験

- クロスチェーンプロトコルのチェーン間の情報伝達に弱点があると、不正なトークンの発行につながる。
- 不正発行されたトークンが交換業者に流入する場合、不正発行されたトークンの価格が急落するなど、交換業者にとってもリスクとなり得る。
  また、当該トークンが裏付け資産がないにもかかわらず大量に不正発行され、DeFiレンディングプロトコルにて別トークン借入のための担保に使われる場合、価格下落や強制清算を通じて、**<u>DeFi市場全体に信用リスクが波及する可能性</u>**がある。



【参考】KelpDAO Incident Statement _2026年4月現在

※各事例に関して公表されている資料及び本報告書の執筆時点で入手可能な情報に基づき調査研究の目的から整理したもので、個別事案に関する責任の所在又は法的評価を示すものではありません

近年の流出事例及び暗号資産特有リスクの分析

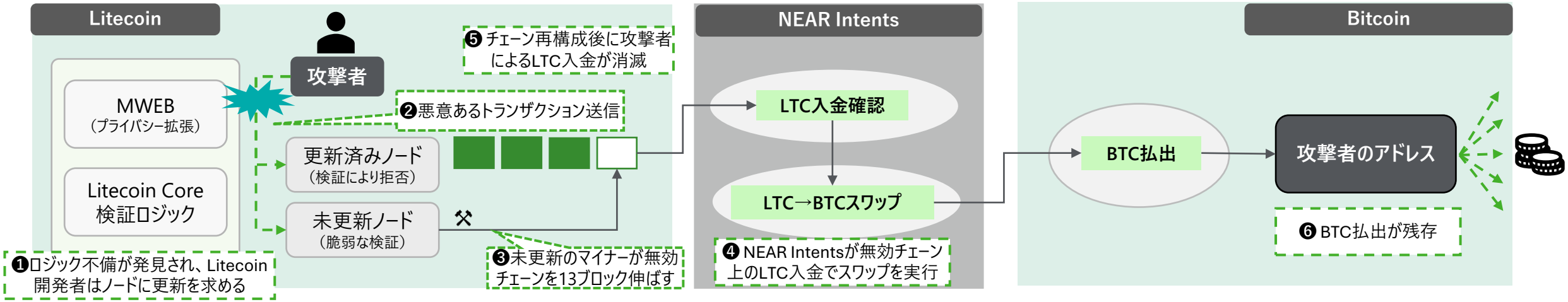
事例⑤: Litecoin（ブロックチェーン再構成）

攻撃の概要

- Near Intentsは、異なるブロックチェーン間でトークンの交換を可能にするクロスチェーンプロトコル。
- 攻撃者は、Litecoinチェーンで発生するブロックチェーンの分岐を悪用し、将来無効となる分岐チェーン上でNear IntentsへLTC（暗号資産）の入金を行った。
- Near IntentsはLTCの入金を確認済みと判断し、Bitcoin側で攻撃者にBTCを引き渡した。
- しかしその後、Litecoinチェーンの分岐が修正され、当初のLTCの入金は無効化された結果、攻撃者はLTCを支払わずにBTCだけを取得した。

事例分析より得られた経験

- ブロックチェーンでは、一度有効に見えた取引が後から無効になる場合がある（ブロックチェーンの再構成）。
  これは、複数のブロックが同時に生成され、後から一方のチェーンだけが正式なものとして採用されるためである。
- このブロックチェーンの仕組みを悪用されると、入金は後から取り消される一方で、出金された資産だけが持ち逃げされる可能性がある。
  交換業者は、運営ノードの分散度等、**ブロックチェーンごとの特性に応じて、出庫・入庫のトランザクションの最終性を評価する**必要がある。



【参考】Litecoin MWEB Security Incident Postmortem