応
般

コインチェック騒動
― 仮想通貨の安全性 ―

楠　正憲（Japan Digital Design（株））

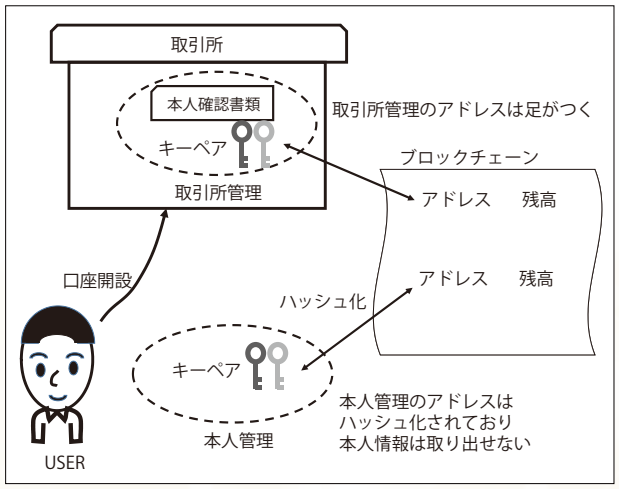
2018 年 1 月 26 日深夜，仮想通貨交換業者のコインチェック社が記者会見を行い，ブロックチェーン NEM 上で流通し同社の管理する仮想通貨 XEM の約 580 億円分が不正アクセスによって漏洩したと発表，翌 27 日に記者会見から発表までの加重平均価格（1XEM ＝ 88.x 円）にあたる約 460 億円を補償すると発表した．事件前 110 円前後で推移していた XEM 価格は事件を受けて 90 円弱まで下落し，補償の発表を受けて一時は事故前を超える 117 円台まで回復した．しかしながら本稿執筆時点で XEM 価格は 60 円以下の水準まで下落し，事件の原因や犯人は公表されていない．

流出した仮想通貨が戻ってくる可能性は低い

2014 年の Mt.Gox 事件（約 470 億円），2016 年の香港 Bitfinex 事件（777 億円），2017 年末の韓国 YouBit 事件（未公表，総資産の約 17%）など，これまで取引所への不正侵入によって仮想通貨が流出したケースはあるが，いずれのケースでも流出した仮想通貨は戻ってこなかった．

仮想通貨の動きそのものは公開されているブロックチェーンを通じて確認できるが，個々のアドレスの保有者を特定することは難しい．日本を含む多くの国の法規制で取引所で口座を開設するためには本人確認を必要としているため，法定通貨で仮想通貨を購入したり，仮想通貨を法定通貨に換金するには取引所に身元を明かす必要がある．

しかしながら仮想通貨のやりとりに必要なアドレスだけなら，手元で自由に作成できるキーペアと紐づいたハッシュなどの値で，身元を明かさず簡単に作成できる（図 -1）．アドレスごとに残高管理されている仮想通貨はキーペアを作成したアドレス所有者の持つ秘密鍵を使ってしか送金できず，捜査当局や破産管財人であってもアドレスを凍結することはできない．そのため資金の流れが公開されていて流出先のアドレスが分かっていても，被害者や捜査当局は手も足も出ない．これが犯罪に悪用されている



■図 -1　仮想通貨におけるキーペアとアドレス，ブロックチェーンの関係

口座番号さえ分かれば，捜査機関が職権に基づいて口座を凍結できる金融機関口座との大きな違いだ．

流出したコインの追跡と犯人の対抗策

仕様変更で流出そのものをなかったことにする「ハードフォーク」[☆1]という手段もあるが，NEM ブロックチェーンの仕様を管理する NEM 財団は，今回の流出にあたりコインチェック社が財団の推奨する署名を多重化するマルチシグと呼ばれる安全管理策をとっていなかったことを理由にハードフォークを行わない方針を表明し，流出した XEM を識別できるよう印をつけて，印のついた XEM の換金を取り扱わないよう仮想通貨取引所に呼びかけた．

犯人は追跡に対抗して，犯人を追跡している開発者や，NEM の多くを取り扱う仮想通貨取引所に対して印のついた NEM を送り付けて数多くのウォレットに印がついた状態をつくることで追跡を攪乱した．さらに発信元を突き止めることが難しい DarkNet 上で独自の仮想通貨販売サイトを立ち上げ，盗んだ NEM を割引価格でほかの仮想通貨と交換しはじめた．仮想通貨同士の取引は取引所を介した取引と違って本人確認情報と紐付いていないため足がつきにくく，DarkNet 上では発信元が分からずサイトの運営を差し止めることも難しい．そういった困難を乗り越えて，警察は盗まれた XEM と Litecoin とを交換した者を突き止め，事情を聞いているという．

☆1 ブロックチェーンの仕様変更にはソフトフォークとハードフォークがある．ソフトフォークとは採掘者のソフトウェアにしか影響しない仕様変更，ハードフォークとは利用者のウォレットにも影響する仕様変更を指す．特定の取引を無効にするためにハードフォークを用いた例には，2016 年に Ethereum のスマートコントラクトとして構築された仮想通貨ファンド The DAO の脆弱性を悪用して 50 億円以上相当（当時）の Ethereum が盗まれたことに対して，Ethereum が実施したハードフォークがある．このとき取引を無効化するハードフォークに反対するグループは Ethereum Classic に分裂して，それぞれに価格がつく事態となった．ハードフォークの中には仕様上の深刻な課題や脆弱性が見つかった場合，解決するために必要な仕様変更もあるが，開発者や採掘者によるハードフォークを野放図に認めると，発行主体にあたる運営者がいない，後から書き換えることができない，発行総額が決まっているといった仮想通貨の前提を掘り崩してしまうことが懸念される．

急がれる仮想通貨交換業者の安全対策基準

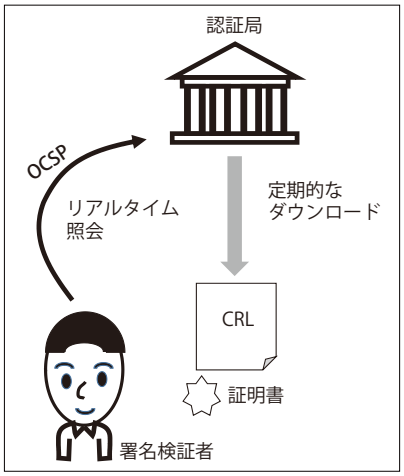
2016 年 テロリスト等に対する資産凍結のための多国間枠組み FATF（金融活動作業部会）が仮想通貨取引所に対して，口座開設にあたっては本人確認を義務付けるよう勧告したことを受けて，2017 年 4 月に改正資金決済法が施行され，仮想通貨交換業者の法律的な位置づけが明確となった．この改正では FATF 勧告を遵守するため仮想通貨や仮想通貨交換業者については規定したが，インサイダー取引の禁止やコインを新規発行する場合の情報開示といった投資家保護のための規律は不十分で，詐欺まがいのコイン発行や投資勧誘が少なからず行われているのが実情だ．

そして 2017 年 9 月までに仮想通貨交換業者として登録を申請した事業者は，正式に登録されるまでの間みなし事業者として事業を継続できることとなった．コインチェック社は 2017 年 9 月に登録を申請したものの，匿名性の高い Monero，Zcash，DASH といった仮想通貨を取り扱っていたことから登録は難航し，みなし事業者として営業を続けている中で流出事件が起きた．

仮想通貨交換業者の安全対策について金融庁は事務ガイドラインを発出しているほか，認定自主規制機関を認定できるが，仮想通貨交換業者の業界団体をめぐっては日本ブロックチェーン協会と日本仮想通貨事業者協会が併存しており一本化に難航したことから，金融庁は認定を行わず，統合へ向けた働きかけを続けていた．そうした環境にあって仮想通貨交換業者について，技術的な安全対策基準が定まらず，事業者によってセキュリティ水準がまちまちな状況が続いている．

PKI アプリケーションよりも難しい仮想通貨の鍵管理

仮想通貨における送金とは，技術的には送金指示



■図 -2　CRL と OCSP

に対するディジタル署名である．ディジタル署名に使うキーペアは直接そのアドレスと結びついている．PKI（公開鍵暗号基盤 Public Key Infrastructure）では漏洩などによって鍵が危殆化した場合，廃止鍵リストに掲載したり，OCSP（図 -2）[☆2]で鍵の有効性について応答することで，鍵を無効にすることができる．ところが仮想通貨の場合，残高や入出金のキーとなるアドレスがキーペアと直接的に結びついているため，鍵を破棄することは，すなわちそのアドレスと紐づいた残高そのものを動かせなくなることを意味する．一般的な PKI アプリケーションと異なり，鍵を破棄することが想定されていないのである．

さらに一般的な PKI アプリケーションでは成熟して幅広いハードウェアやミドルウェアに対応している RSA や ECDSA（Elliptic Curve Digital Signature Algorithm，楕円曲線ディジタル署名アルゴリズム）といった署名アルゴリズムを用いるケースが多いが，仮想通貨やブロックチェーンでは EdDSA（Edwards-curve Digital Signature Algorithm, エドワーズ曲線ディジタル署名アルゴリズム）など新しいアルゴリズムを積極的に採用する傾向にある．これは歴史的に鍵管理に対して無頓着で，軍や金融機関のような鍵管理に厳密な組織からの要求を受けてこなかったこと，新しいアルゴリズムを採用すること自体がほかのブロックチェーンに対する差別化要素と考えられていることが背景にある．

体系的な脅威分析が必要

仮想通貨取引所をめぐっては国際的にも頻繁に高額な漏洩事故が発生しているが，中でも日本の被害額は世界最大で，流出した仮想通貨が犯罪や反社会的勢力に悪用された可能性も考えられる．仮想通貨や交換業者の法的な位置づけが明確化された中で，社会的責任はこれまで以上に高まっている．仮想通貨交換業者の安全性を高めてさらなる事故を防止するためには，仮想通貨業界の社会的責任を問うだけでなく，我々は情報処理に携わる者として，これまで蓄積してきた情報セキュリティの知見に基づいて仮想通貨そのものや仮想通貨取引所の業務について体系的な脅威分析を行い，情報セキュリティ・マネジメントシステムを確立する必要があるのではないか．

（2018 年 2 月 9 日受付）

楠　正憲（正会員）　masanori.kusunoki@japan-d2.com
マイクロソフト，ヤフーなどを経て 2017 年より現職．2011 年から内閣官房 番号制度推進管理補佐官としてマイナンバー制度を支える情報システムの構築に従事．OpenID Foundation Japan 代表理事，ISO/TC307 ブロックチェーンと分散台帳技術にかかわる専門委員会 国内委員会 委員長，日本ブロックチェーン協会 アドバイザー．

☆2　OCSP：Online Certificate Status Protocol（OCSP）は，RFC 6960 で規定された公開鍵証明書の失効状態を取得するための通信プロトコルである．インターネット標準トラック上にある．元々 X.509 の公開鍵証明書は，鍵の無効化を CRL（廃止鍵リスト）と呼ばれるファイルで管理していたが，この方法では CRL を取得した後に無効化された鍵を正しく検証できないため，問合せ時点で鍵が無効化されていないか照会する方法として OCSP が開発された．