IIMAの目　公益財団法人 国際通貨研究所

2018 年 9 月 28 日

最近発生した仮想通貨流出事件で思うこと

公益財団法人　国際通貨研究所
経済調査部　主任研究員　志波　和幸

9 月 20 日に、仮想通貨交換業者「テックビューロ社」は、同社が運営する仮想通貨取引所 Zaif（ザイフ）が外部からの不正アクセスを受け、管理していた仮想通貨（3 種類）計約 70 億円相当（そのうち約 45 億円相当分が顧客資産）が不正に流出したと発表した[1]。今年本邦で起きた仮想通貨の大規模（10 億円以上）の不正流出は、今年 1 月のコインチェック社での NEM 流出事件（約 580 億円相当）以来 2 度目である。

流出金額がコインチェック社と比べ桁が 1 つ小さい 100 億円未満の規模にとどまったことや、テックビューロ社が顧客に対する補填を即時公表したこともあり、メディアで続報を取り上げていない。その一方、流出原因の詳細について同社から未だ発表がない。

そうしたなか、今回の事件の問題点及び課題について、一部筆者の推測を含めつつ、以下 4 点を指摘したい。

１．「システムの堅牢性強化」と「ホットウォレット」との融合の難しさ

本邦の仮想通貨取引所は、「仮想通貨と法定通貨（円）との交換」業務に加え、「顧客資産（仮想通貨と法定通貨ともに）の預かり」業務を行っている。換言すると、仮想通貨取引所は顧客に対して「貸金庫」を提供するとともに、入出金の際それを開くための「鍵」を預かり、厳重に管理する責任を負っている（図 1）。

Zaif では、顧客の入出金に即時に対応するべく、「ホットウォレット」形式で顧客の仮想通貨の大部分を保管・管理していた。「ホットウォレット」を簡潔に述べると、本来ならば取引所は玄関に門番を配備し、顧客が取引所内で管理している預かり資産を「貸金庫」から入出庫する都度、①本人確認の実施、②「鍵」の手交、③玄関を開く、作業をするべきところ（これを「コールドウォレット」という）、それでは時間がかかるため、玄関を常時開放するとともに、本人確認と「鍵」の手交を簡略化した方法である（図 2）。

しかし、それが同社の「利用リスクと『Zaif』のセキュリティ体制について」[2]の「①

[1] 事件の詳細及び Zaif の対応については、2018 年 9 月 20 日「仮想通貨の入出金停止に関するご報告、及び弊社対応について（テックビューロ株式会社）」をご参照。
[2] https://corp.zaif.jp/security/をご参照。

預かり暗号通貨管理の強化」と「③システムインフラの堅牢性強化」に記載している態勢に見合うものであったのか、疑問が残る。

２．「顧客資産」と「取引所資産」との分別管理が出来ていたか？

冒頭の通り、今般「顧客からの預かり分（約 45 億円）」とともに「取引所の資産（約 25 億円）」が流出した。テックビューロ社からは今般の流出事件で被害にあった顧客数は公表されていないが、外部から不正アクセスを受けたのは 9 月 14 日の午後 5 時ごろから 7 時ごろにかけての僅か 2 時間であったという報告を鑑みると、ハッカーは、個々の顧客の「金庫」を開いて仮想通貨を奪取したのではなく、Zaif が「顧客と取引所の資産を総合管理している『財布』」から一斉に奪取した可能性が高い（図 3）。因みに、コインチェック社事件も同様の方法で顧客資産が流出した。

このことがテックビューロ社の「利用リスクと『Zaif』のセキュリティ体制について」の「④お客様預かり金の分離」を履行していたのか、今後の発表が待たれる。

３．不正アクセス検知の遅さ

前述の通り、外部から最後の不正アクセスを受けたのは 9 月 14 日の午後 7 時ごろであったが、その異常を検知したのが 3 日後の 9 月 17 日と時間を要している。これは 1 月のコインチェック社での流出事件で異常を検知したのが、最後の不正取引（1 月 26 日午前 8 時 26 分）の 3 時間後（午前 11 時 25 分）と比べても大変遅い。このことから同社の「利用リスクと『Zaif』のセキュリティ体制について」の「⑤リスク管理やセキュリティ対策の強化（欧米型の数理モデルによる不正検知の導入）」が有効に機能していたか疑わしい。

４．金融庁の監督人材不足

当該流出事件を受け、9 月 25 日に金融庁はテックビューロ社に対し 3 度目の業務改善命令を出状した。

【表 1】テックビューロ社宛て業務改善命令項目

(1)	流出事案の事実関係及び原因の究明（責任の所在の明確化を含む）並びに再発防止策の策定・実行
(2)	顧客被害の拡大防止
(3)	顧客被害に対する対応
(4)	3 月 8 日付業務改善命令[3]及び 6 月 22 日付業務改善命令[4]の内容について、流出事案を踏まえて、具体的かつ実効的な改善計画の見直し及び実行
(5)	上記(1)から(4)までについて、平成 30 年 9 月 27 日（木）までに、書面で報告

（出所）国際通貨研究所作成

この(4)に記載している「3 月 8 日付業務改善命令」（つまり 1 度目のもの）は、改善項目の 1 つとして「実効性あるシステムリスク管理態勢の構築」とともに、「改善計画

[3] https://www.fsa.go.jp/news/30/virtual_currency/20180308-3.html をご参照。
[4] https://www.fsa.go.jp/news/30/virtual_currency/20180622_06.html をご参照。

書の提出及び 1 ヵ月毎の進捗・実施状況の報告」を挙げていた。

しかしながら、今般の流出事件を鑑みると、テックビューロ社が構築した管理態勢が不十分であったことと同時に、その監督者である金融庁もそれを指摘するだけの組織の組成が出来ていなかった、そして現在も出来ていないものと思料する。

奇しくも、9 月 12 日に開催された「仮想通貨交換業等に関する研究会（第 5 回）」で、一部のメンバーから金融庁内の仮想通貨のモニタリング人員数について質問があり、これに対し金融庁から、現時点でその専任者は 30 名であること。そして、モニタリングを更に強化するべく、次年度の予算にその増員を申請中の旨の回答があった。

仮想通貨は、ナカモトサトシ氏が 2009 年 1 月にビットコインの運用サーバー第 1 号を立ち上げてからまだ 10 年も経っておらず、他の金融商品と比べると大変若い市場である。従って、投資家・取引所・監督当局が想定していなかった事件が今後も起ころう。投資家及び仮想通貨への投資に興味をもっている方は、その市場が成熟するにはまだ時間がかかるということを念頭に置くべきである。

【表 2】各市場の発生時期

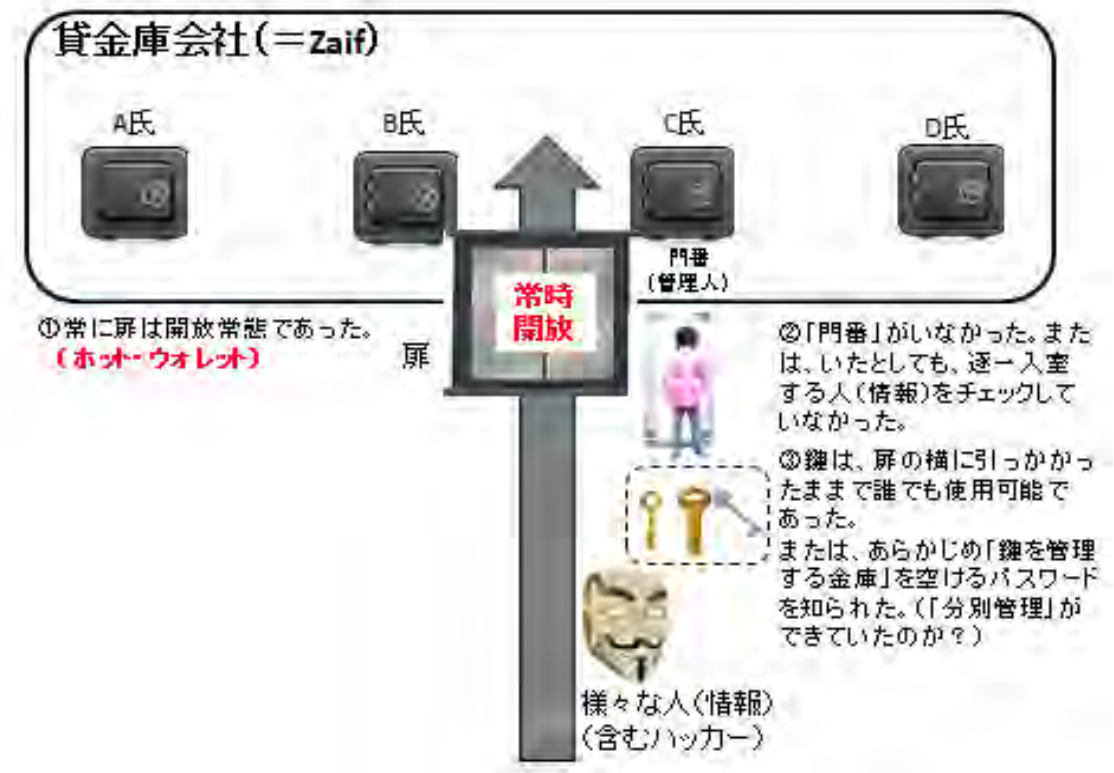
債券市場	12 世紀~13 世紀 ヴェネチアをはじめとしたイタリア北部の都市国家で、政府が債券を発行
株式市場	1602 年 オランダ東インド会社（VOC）
デリバティブ市場	1730 年代 徳川吉宗の命により大岡越前守が大阪（堂島）に米の先物市場を整備
外国為替市場 （変動相場制）	1973 年 金=ドル本位制、スミソニアン体制崩壊後
仮想通貨	2009 年 ビットコイン誕生

（出所）国際通貨研究所作成

以　上

【図１】仮想通貨交換業者に対し一般的に求められる仮想通貨の管理手法

【図 2】Zaif の仮想通貨の管理手法（その 1）（筆者推測）



【図 3】Zaif の仮想通貨の管理手法（その 2）（筆者推測）