Zaif からの仮想通貨流出
～仮想通貨交換業者はアンコントローラブル？～

応般

楠　正憲 | Japan Digital Design, Inc.

暗号通貨の流出が止まらない．直近の Zaif 事件を中心に，現状を報告する．2018 年 1 月末のコインチェックに続いて，2018 年 9 月 14 日夕刻にテックビューロ社の運営する仮想通貨交換所 Zaif から約 70 億円分の仮想通貨が流出した（表 -1）．今回は初めて被害が弁済できなくなる懸念があり，仮想通貨交換業者の信用を揺るがす問題となっている．

同社の発表によると 2018 年 9 月 17 日にサーバの異常を検知し，翌 18 日にはハッキングの被害が確認されたため，近畿財務局への報告と捜査機関への被害申告などを行った．今後は交換所を運営し，ホワイトボックスによる交換所システムを提供するフィスコの子会社を通じて，資本提携と 50 億円の金融支援などを検討する基本契約を締結したという．

今回の事件がコインチェック事件と大きく異なるのは，コインチェックが金融庁に登録していない「みなし事業者」だったのに対して，Zaif が改正資金決済法に基づいて登録された「登録仮想通貨交換業者」で，これまでに二度の業務改善命令を受けていたことだ．立入検査を実施し，業務改善命令を出していたにもかかわらず，事件を防ぐことはできなかった．

またコインチェックは自己資金で流出被害を全額補償したが，Zaif には十分な自己資金はなく，弁済にはフィスコからの金融支援が前提となる．当初のリリースでは 2018 年 9 月下旬のうちに支援が提供されることを前提として交渉を進めているとしていたが，本稿執筆時点（2018 年 10 月 1 日）で具体的な支援についての発表は行われていない．

■表 -1　Zaif から流出した主な仮想通貨（公表分）

仮想通貨	流出総額	うち顧客資産
Bitcoin	5966.1BTC（約 42.5 億円）	2723.4BTC（約 19.4 億円）
Bitcoin Cash	42327.1BCH（約 21 億円）	40360BCH（約 20 億円）
MONA	6236610.1MONA（約 6.7 億円）	5911859.3MONA（約 6.4 億円）

謎が多い事件発見までの経緯

一連の経緯で不可解なのは不正送金から発見・報告までに 4 日もかかっていることだ（表 -2）．資金決済法の事務ガイドラインでは日次での残高確認を求めており，適切にオペレーションが行われていれば 9 月 14 日中に不正送金を発見できたはずだ．

また，この流出によって 9 月 14 日夕刻から顧客からの仮想通貨の引き出し要求に応じられなくなったはずで，実際，9 月 15 日にはその旨のツイートが散見される．顧客からの出金要求に応じるための障害対応を行っていれば，やはり気付くことができたはずである．

自力での弁済が難しいほど多額の仮想通貨をホットウォレットに入れていたことも不可解だ．仮想通貨交換所の多くは預かり資産の大半を，不正アクセスだけでは詐取できない，ネットワークから分離されて入出金には手動の操作を要するコールドウォレットで管理している．

コインチェック事件では，流出した仮想通貨NEMが新しい電子署名方式を採用していたため，不正アクセスを受けても影響を受けないコールドウォレットの導入が間に合っていなかった．

今回流出したBitcoin他は管理手法が確立しており，多くの取引所がコールドウォレットで適切に管理している．経営を揺るがすほど多額の仮想通貨をホットウォレットに置いたままにするのは不自然だが，全資産に占めるホットウォレット，コールドウォレットの比率について，Zaifは明らかにしていない．

また救済を申し出ているフィスコが事件前の12日までにZaifのシステムから離脱し，翌13日にZaifが全部免責条項を削除する約款変更を行って，フィスコに提供していた仮想通貨の簡単売買サービスを一時停止していたことも憶測を呼んでいる．今回の不正送金と一連の動きに関連があるとすれば，内部犯行の可能性も疑われる．

相次ぐ仮想通貨の多額流出事件，今後の見通しは

MtGOX事件から数えて，仮想通貨交換業者から流出した仮想通貨は日本だけで優に1,000億円を超える（**表-3**）．現金の窃盗強奪事件 では50年前に起きた三億円事件が今なお語り継がれているが，今年は年に二度も三億円事件をはるかに超える規模の犯罪が起き，多額の資産が犯罪集団に渡ったことになる．

今回の事件はコインチェック事件を受けた各社のセキュリティ対応が一段落して，マネックス証券傘下で再建を目指していたコインチェックを仮想通貨交換業者として登録して，積滞している登録申請の審査に着手しようという矢先に起きた．登録を行って業務改善命令を受けていた業者が事故を起こしたことで，コインチェックを含めて登録申請を行っている各社の審査は遠のくことになるのではないか．

■表-2　Zaifからの仮想通貨流出についての時系列で見た流れ

9月12日	フィスコ仮想通貨取引所がZaifからカイカ の提供するシステムに移行
9月13日	Zaifが約款から全部免責条項を削除する改訂 フィスコがZaifから提供を受けていた簡単売買サービスを停止
9月14日17：33	Zaifから Bitcoin Cash, Bitcoin の不正送金がはじまる
9月14日17：39	Zaifから Monacoin の不正送金がはじまる
9月14日18：54	Zaifから約70億円相当の仮想通貨の不正送金が完了
9月15日3：10	利用者が「昨日の夕方から Bitcoin，Monacoin の出金ができない」旨ツイート
9月15日10：00	Zaifから不正送金された Bitcoin の資金洗浄が大規模化
9月17日	テックビューロがサーバの異常を検知 Zaifが流出した Bitcoin，BitcoinCash，Monacoin の入出金を停止
9月18日11:48	Zaif公式Twitter「顧客資産の安全を確認」とツイート
9月18日午後	テックビューロが不正アクセス被害の発生を把握 テックビューロが近畿財務局に不正送金被害を報告 金融庁がテックビューロに資金決済法に基づく報告聴取命令
9月19日	フィスコが取締役会を開きテックビューロの支援を行うことを決定 テックビューロが大阪府警西署に仮想通貨不正送金の被害を申告 フィスコとテックビューロの間で金融支援等を検討する基本契約を締結 カイカ（フィスコにシステムを提供する仮想通貨交換所システム構築業者）がテックビューロにセキュリティ向上の技術提供の基本契約を締結
9月20日深夜	テックビューロが不正アクセスを受け仮想通貨の入出金を停止したと発表

残念ながら今のところ仮想通貨の安全な管理手法は確立していない．銀行のダイレクトバンキングをはじめとした既存の金融機関においては，振込額の上限設定や多要素認証の確実な利用などのリスク管理が強化されて，不正送金被害の抑え込みに成功しつつあるが，仮想通貨ではオンライン上で青天井の金額を不正送金できることから，今後も国内外の攻撃者の標的となることが懸念される．

とはいえ Zaif における仮想通貨の管理が適切であったかというと，ホットウォレットに多額の仮想通貨を入れていたこと，それらが流出して 4 日間も気付かなかったことを見てもずさんであったことは明らかだ．事業者を信用できない，被害の迅速な報告が見込めないとなると，規制当局が直接モニタリングすることの必要性が増すことも考えられる．

今回，初めて被害が弁済できなくなる懸念があることも，仮想通貨交換業者の信用を揺るがす問題だ．仮想通貨は金庫の中にある現金と違って，ウォレット残高はブロックチェーンでリアルタイムに把握できる．個社の監視体制がずさんということになると，各社の仮想通貨ウォレットのアドレスを業界団体と規制当局で共有して，相互に監視することも検討すべきではないか．業界団体でホットウォレットに置く仮想通貨の比率上限を決める動きがあるようだが，流出額を自前で弁済できないといった事態を防止するためには，確実に被害を弁済できるよう，業者に要求する財務体質を見直す動きも出てくるのではないか．

（2018 年 10 月 1 日受付）

■表 -3　仮想通貨交換所の主な仮想通貨流出事案

起きた時期	流出元	流出した金額
2014 年 2 月	MtGOX - 日本	約 470 億円
2016 年 8 月	Bitfinex - 香港	約 65 億円
2017 年 11 月	Thether トークン - 米国	約 50 億円
2017 年 12 月	Youbit - 韓国	約 18 億円
2017 年 12 月	NiceHash - スロベニア	約 68 億円
2018 年 1 月	CoinCheck - 日本	約 580 億円
2018 年 2 月	BitGrail - イタリア	約 181 億円
2018 年 9 月	Zaif - 日本	約 70 億円

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．