暗号資産ウォレットの衝撃

～暗号資産取引所の破綻への備え～

ライフデザイン研究部 主席研究員 柏村 祐

1.大手暗号資産取引所の破綻

過日、グローバルに展開する暗号資産取引所が、日本の民事再生法に相当する米連邦破産法 11 条の適用を申請したと発表した。5 月に起きたアルゴリズムステーブルコイン TerraUSD の大幅下落に続き、今回大手暗号資産取引所が破綻したこともあり、暗号資産取引所および暗号資産に対する信頼が揺らいでいるようだ。2021 年 11 月に約 396 兆円におよんでいた暗号資産時価総額は、2022 年 11 月時点で約 117 兆円となっており、暗号資産市場の今後について当面見通せない状況が続くと考えられる。

今回の破綻が注目される理由として、暗号資産の価格下落に加え、利用者が取引所に預けている暗号資産を出金できない状況が発生し、預けている暗号資産の取り扱いがどのようになるのか懸念されている点が挙げられる。

暗号資産取引所で暗号資産を購入すると、その暗号資産は取引所が管理する暗号資産ウォレットに保管される。万一暗号資産取引所が破綻したり、ハッキングされた場合、取引所の機能は停止され、暗号資産の売買・出金ができなくなる。

日本においては、以前から暗号資産取引所の破綻やハッキング被害があるたびに、取引所に預けていた暗号資産が保全されるのか、どのように返還されるのか注目されてきた。そのため、過去に発生した事案を踏まえ、金融庁は、暗号資産の流出リスクへの対応や暗号資産取引所事業者の破綻時の対応について、利用者保護の観点に基づいた法整備を進めてきている。

そこで本稿では、暗号資産取引所の破綻に対する利用者の対応策の 1 つになりうる自己管理の暗号資産ウォレットの活用について概観する。

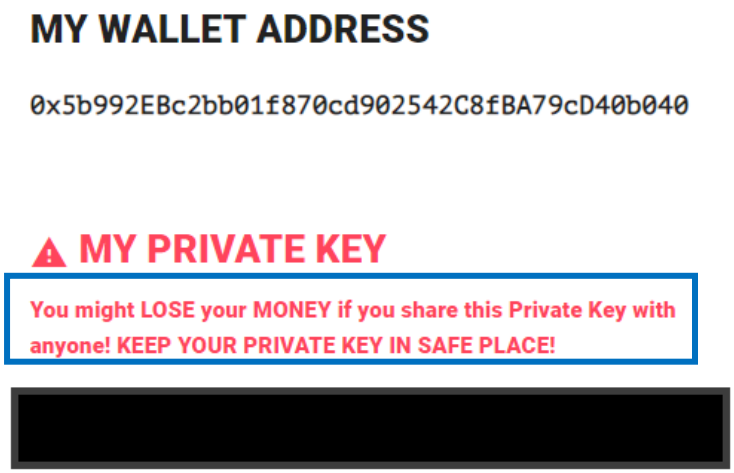
2.暗号資産ウォレットとは

暗号資産ウォレットとは、自分自身が保有する暗号資産を保管する場所を意味する。暗号資産ウォレットを構成する要素は、ウォレットアドレスと秘密鍵（ウォレットを開錠するための鍵）である。暗号資産ウォレットをインターネットバンクの預金口座に例えるならば、ウォレットアドレスは口座番号を意味し、秘密鍵はパスワードの位置づけとなる。

また、暗号資産ウォレットは、取引所内の暗号資産ウォレット（以下取引所ウォレット）と、自己管理の暗号資産ウォレット（以下マイウォレット）に分類される。取引所ウォレットは、暗号資産取引所内で管理される暗号資産ウォレットであるため、

秘密鍵は暗号資産取引所が管理する。一方、マイウォレットの場合、秘密鍵は利用者自身が管理する。秘密鍵を知っていれば誰でも暗号資産ウォレットを開錠することができるため、秘密鍵は安全な場所に保管することが推奨されている（図表 1 青枠）。

図表 1　秘密鍵を安全に保管するよう推薦するメッセージ



資料：MEW 社の口座より加工（黒塗り部分は秘密鍵情報）

取引所ウォレットとマイウォレットは、いずれも売買機能、入出金機能を備えている。大きな違いは、秘密鍵を取引所が管理するか、利用者自身が管理するかである。また、取引所ウォレットの開設は、銀行口座や証券口座と同様、暗号資産取引所が提供する取引所口座開設手順に従えば簡単に行うことができる。一方、マイウォレットの場合、利用者自身がマイウォレットを開設し、設定する作業が発生するため、秘密鍵の仕組みや暗号資産について一定の知識が求められる（図表 2）。

図表 2　取引所ウォレットとマイウォレットの比較

分類	機能	秘密鍵
取引所ウォレット	売買機能、入出金機能	取引所が管理
マイウォレット	売買機能、入出金機能	自分自身が管理

資料：筆者作成

仮に取引所において破綻やハッキングなどの重大な事象が発生した場合、秘密鍵を保有する暗号資産取引所は取引所の資産保全のために、出金停止処理を行うこともあるだろう。出金停止処理が行われると、利用者が取引所ウォレットから自分自身の暗号資産を取り出すことができないという事態が発生する。

一方、マイウォレットは、秘密鍵さえあればいつでも利用することが可能なので、暗号資産取引所の破綻やハッキングが発生しても利用者は影響を受けない。したがっ

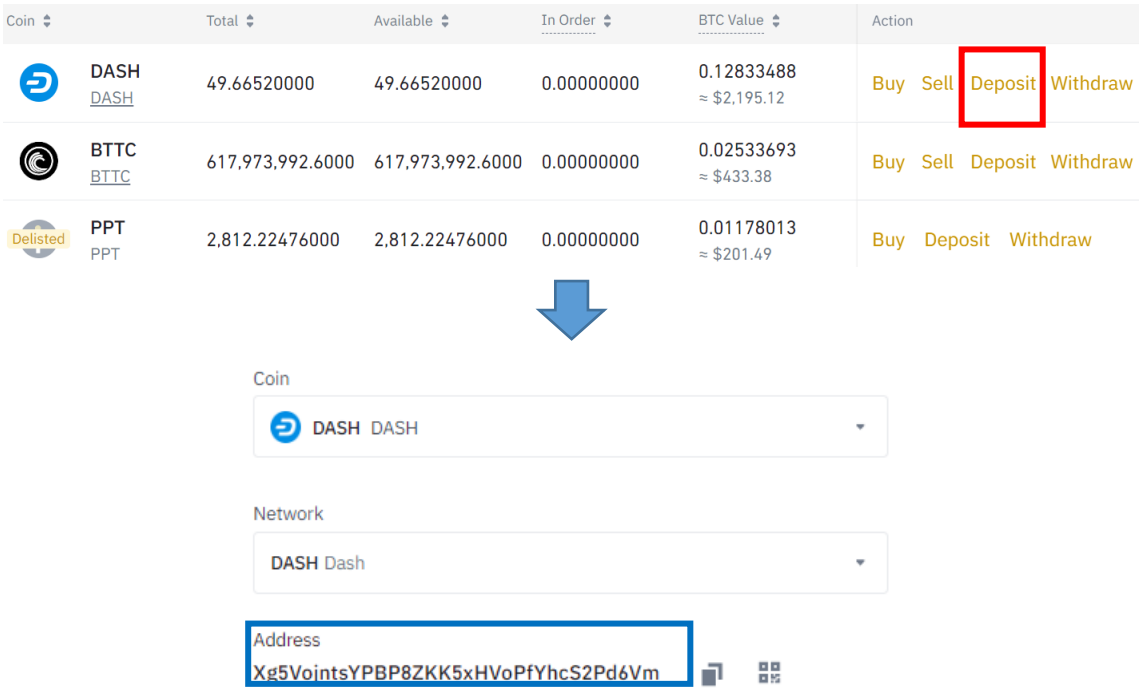
て、暗号資産取引所はあくまで暗号資産を取引する場として認識し、保有する暗号資産については、利用者自身がコントロールできるマイウォレットに保管しておくことも選択肢になるのではないだろうか。

3.暗号資産ウォレットの実際

ここからは、実際に運営されている取引所ウォレットとマイウォレットの利用方法を確認してみよう。まず、暗号資産取引所で取引所ウォレットを確認するには、各暗号資産取引所が認めたID(メールアドレスやSNSアカウント)とパスワードを入力し、取引所にログインする必要がある。利用者がウォレットアドレスを確認する必要が生じるケースは、自分が利用している暗号資産取引所の取引所ウォレットへの入金や取引所ウォレットから出金する場合に限られる。たとえば、取引所ウォレットに暗号資産を入金してもらいたい場合、暗号資産のウォレットアドレスを確認し、暗号資産を送付してもらいたい第三者にウォレットアドレスを伝えればよい。一方、保有する暗号資産を第三者に出金したい場合、送付先となるウォレットアドレスを入力し送金ボタンを押せば、自分自身の取引所ウォレットから暗号資産を送ることができる。

筆者が実際に取引を行っている暗号資産取引所では、ログインすると現在の暗号資産の資産管理画面が表示される。暗号資産ごとに、売買する機能、入出金する機能が準備されている。取引所ウォレットのウォレットアドレスを確認するには、該当する暗号資産の入金機能画面に遷移すればよい。たとえば、ある暗号資産の入金機能（Deposit機能）を起動させれば（図表3上段赤枠）、当該暗号資産のウォレットアドレスが「Xg5VojntsYPBP8ZKK5xHVoPfYhcS2Pd6Vm」であることがわかる(図表3下段青枠)。暗号資産取引所では、それぞれの暗号資産毎にウォレットアドレスが用意されている。

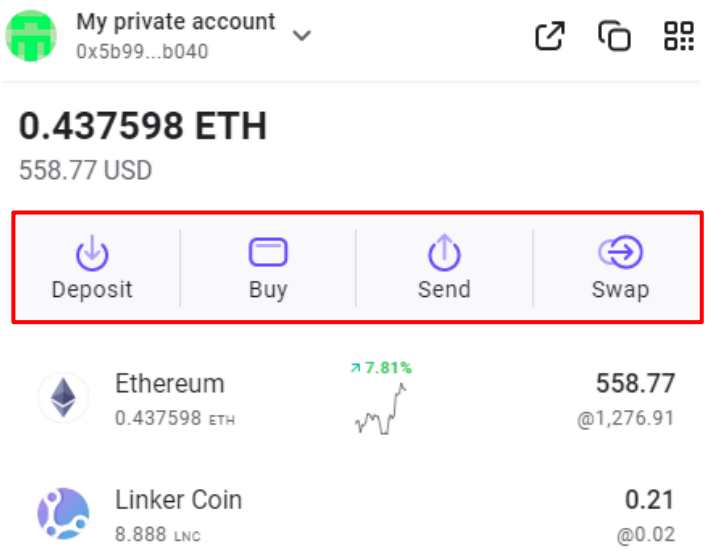
図表 3　取引所ウォレットの概要



資料：BINANCE 社の口座より作成

次に、暗号資産ウォレットの別類型であるマイウォレットをみていく。マイウォレットは、ブラウザーまたはスマートフォンのアプリで設定し利用することができる。マイウォレットを利用するには、利用者が管理する秘密鍵を使い開錠する。実際に筆者が保有する秘密鍵を利用してマイウォレットを開錠してみると、保有暗号資産の状況は、マイウォレット上のダッシュボードで確認することができる。また、マイウォレット上では、暗号資産を売買する機能や入出金機能が備えられている（図表 4 赤枠）。暗号資産の売買機能や入出金機能が装備されているマイウォレットは、暗号資産取引所で展開される取引所ウォレットと比べ機能面での遜色はない。

図表 4　マイウォレットの概要



資料：enkrypt 社の筆者口座より作成

4.突然破綻する暗号資産取引所に対する備え

先述の通り、マイウォレットは取引所ウォレットと異なり、暗号資産取引所の破綻やハッキングが発生しても利用者は影響を受けない。したがって、暗号資産取引所はあくまで暗号資産を取引する場として認識し、保有する暗号資産については、利用者自身がコントロールできるマイウォレットに保管しておくことも一案である。

ただし、マイウォレットの場合、悪意の第三者に秘密鍵を知られてしまうと、暗号資産ウォレットは開錠され暗号資産を盗まれてしまう。そのため、秘密鍵は誰にもしられないように厳格に保管しておく必要がある。

暗号資産ウォレットについては、取引所ウォレットの方が広く知られているが、利用者自身が管理するマイウォレットも進化を続けている。すでに暗号資産を保有している人も、今後暗号資産を取引する人も、暗号資産をどのように保有していくかを考える上で、マイウォレットの進化を踏まえ、その活用を視野に入れてよいのではないだろうか。