

今日のキーワード 『仮想通貨』を理解するシリーズ5

今年1月に、『仮想通貨』交換業者のコインチェック社で580億円相当の『仮想通貨』NEM（ネム）が流出し、問題になっています。金融庁は事件発覚後、コインチェック社に立ち入り検査を行ったほか、他の交換業者にも立ち入り検査を実施し、3月8日に業務停止を含む7社の行政処分を発表しました。このように『仮想通貨』については、交換業者のセキュリティの甘さや利用者保護の遅れが露呈しています。

ポイント1

ハッキングのリスクと利用者保護

おカネが全く返ってこないことも…

- 『仮想通貨』の基本的システムの「分散型台帳技術」は、データの改ざん等を防ぐ高度な技術を用いているため、ハッカーに崩された事例はほとんど無いようです。しかし、『仮想通貨』を売買するための交換業者のセキュリティが脆弱で、ハッカーはそこを徹底して突いてきています。
- 『仮想通貨』交換業者は、『仮想通貨』をコンピュータの「ウォレット」と呼ばれる口座で管理しています。常時ネット接続され売買に便利な「ホットウォレット」と、ネットから切り離され、安全性が高い「コールドウォレット」の2種類があります。『仮想通貨』送金時の暗証番号（「秘密鍵」）を一つとするか（シングルシグ）、複数とするか（マルチシグ）も重要なポイントです。コインチェック社はいずれも安全性が低い方を使っていた模様です。
- 交換業者が「コールドウォレット」で保存し、かつ、「マルチシグ」を使えば安全性が高まります。一方で、取引に時間がかかるようになり利便性が下がります。安全性を確保しつつ利用者の利便性を如何に維持するか、交換業者にとって、力を入れて取り組む経営課題となっています。
- なお、2017年に始まった改正資金決済法では、『仮想通貨』交換業者に『仮想通貨』と預り金のそれぞれについて、顧客と自社の資産を明確に分けて管理するよう義務付けています。ただし、銀行預金や株式では預金保険機構や証券保管振替機構によって顧客資産が守られていますが、『仮想通貨』の場合そういった仕組みがないため、登録業者であっても、倒産した場合に利用者に全資産が戻ってくる保証はないようです。



コールドウォレット？
ホットウォレット？

ポイント2

マネーロンダリングのリスク

気が付かずに、あなたが手を貸していることに…？

- 『仮想通貨』では、売買や送金した人物を明らかにすることなく取引を行う事も可能です。つまり匿名性があります。この特性を使ってマネーロンダリング（資金洗浄）に悪用される可能性があります。金融庁の検査では、一部の交換業者でマネーロンダリング対策がずさんな例が見つかったようです。
- 各国においてマネーロンダリングやテロ資金対策関連の規制は強化されてきています。『仮想通貨』の匿名性がこれらの規制に抵触することがあれば、『仮想通貨』の流通が制限されることもあり得ます。

※個別商品に言及していますが、当該商品を推奨するものではありません。

ここも チェック！

2018年3月9日 『仮想通貨』を理解するシリーズ4

2018年3月7日 『仮想通貨』を理解するシリーズ3

■当資料は、情報提供を目的として、三井住友アセットマネジメントが作成したものです。特定の投資信託、生命保険、株式、債券等の売買を推奨・勧誘するものではありません。■当資料に基づいて取られた投資行動の結果については、当社は責任を負いません。■当資料の内容は作成基準日現在のものであり、将来予告なく変更されることがあります。■当資料に市場環境等についてのデータ・分析等が含まれる場合、それらは過去の実績及び将来の予想であり、今後の市場環境等を保証するものではありません。■当資料は当社が信頼性が高いと判断した情報等に基づき作成しておりますが、その正確性・完全性を保証するものではありません。■当資料にインデックス・統計資料等が記載される場合、それらの知的所有権その他の一切の権利は、その発行者および許諾者に帰属します。■当資料に掲載されている写真がある場合、写真はイメージであり、本文とは関係ない場合があります。