Vol.2019-IOT-44 No.44
2019/3/8

仮想通貨取引所におけるマルチシグネチャ対策調査と管理体制の検討

Investigation of multi-signature measures on the cryptocurrency exchange and its study of their management system

増山裕香[†1]　猪俣敦夫[†2]

概要：ここ数年，電子データ形式で取引される仮想通貨の取引が増え，それらの仮想通貨を円やドルなどの法定通貨及び別の仮想通貨と為替取引する仮想通貨取引所と呼ばれるサービスが増加している．しかしそれら仮想通貨取引所に対するハッキングにより，一年に数百億もの仮想通貨盗難被害が発生した．本稿は仮想通貨送受金に不可欠な秘密鍵の分散管理状況を調査し，調査結果より取引所の顧客資産の管理体制について考察する．

キーワード：仮想通貨取引所，秘密鍵，マルチシグネチャ

1. はじめに

仮想通貨とは紙幣や硬貨のような現物をもたず，電子データのみでやりとりされる通貨である．この電子データを構築するシステムとしてブロックチェーンという技術が使われている．この技術の導入により，非改ざん性，取引情報のトレーサビリティ，相互監視によるデータの整合性という 3 つの特徴が生まれ，通貨としての信頼性を獲得している．それらの仮想通貨を円やドルなどの法定通貨及び別の仮想通貨と為替取引する Web サービスが仮想通貨取引所である．しかしながら仮想通貨取引所を狙ったハッキングが相次いで発生しており，仮想通貨市場に大きな影響を与えている．朝日新聞は 2018 年 9 月 20 日，警察庁が発表した 2018 年上半期のデータで，仮想通貨ウォレットや交換所へのサイバー攻撃が 2017 年の同じ時期と比べ 3 倍になったと報じられており[1]，警察庁では，158 件のサイバー攻撃を通じ，605 億 300 万円（約 5 億 4000 万ドル）相当の仮想通貨が盗まれ，そのうち約 95%は仮想通貨取引所から盗まれたもので，約 5 億 1800 万ドルに及ぶと発表した．仮想通貨取引所がターゲットとなったハッキング事件を表 1 に示す．

時期	仮想通貨交換業者	被害額(時価)	要因
2014.2	Mt.GOX（日）	約470億円	不正アクセス・内部犯行
2015.1	BitStamp(英)	約5億円	従業員に対するフィッシング
2016.8	Bitfinex(香港)	約65億円	不正アクセス
2017.12	Youbit(韓)	約18億円	不正アクセス
2018.1	Zaif(日)	約10億円	WebAPIに対する不正アクセス
2018.1	CoinCheck(日)	約580億円	標的型メールによるマルウェア感染
2018.2	BitGrail(伊)	約181億円	不正アクセス
2018.9	Zaif(日)	約70億円	不明

表 1　仮想通貨取引所を狙ったハッキングの事例

2014 年の Mt．GOX 社のハッキング事件[2]を発端とし，2018 年 1 月には CoinCheck 社が過去最大規模となる約 580 億円[3], 同年 9 月にはコインビューロ社が運営する Zaif が約 70 億円もの被害総額をだした[4]．その事で金融庁による調査が入り，徐々に仮想通貨取引所のシステムセキュリティ運用状況が明らかになってきている[5]．　これら仮想通貨取引所のセキュリティ対策不足は急激な仮想通貨市場規模の拡大による仮想通貨交換業者の増加が一因といえる．図 1 に仮想通貨の市場流通合計額の推移を示す．

図 1　仮想通貨市場規模額の推移[6]

2017 年 4 月とピーク時の 2017 年 12 月の仮想通貨市場規模額を比較すると，最大で約 75 倍に増加している．このような市場規模の急成長に加えて FinTech の発展と仮想通貨による資金調達・クラウドファンディングの流行により，仮想通貨取引所の数は年々増加した．その結果図 2 に示すように 5 年間で約 5.5 倍に増加している．

一連の急激な開設の動きにより，多くの取引所は業務量に比べ，システム担当者が不足し，セキュリティに関しての対策を実施していなかった[5]．また，業界全体としてのルールの策定や法制度が間に合っていなかったといえる．

†1 東京電機大学未来科学部情報メディア学科
†2 東京電機大学　教授

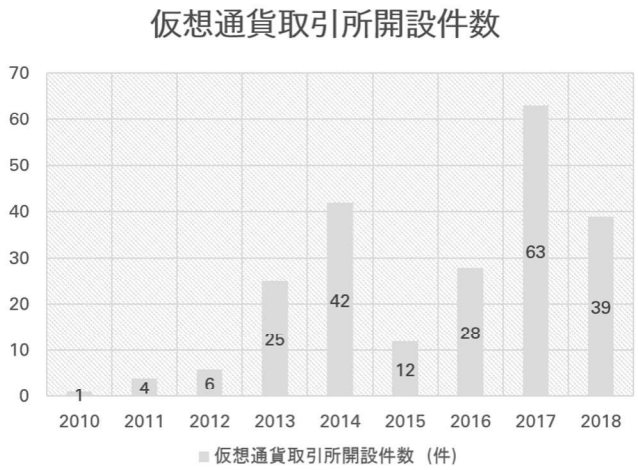

図 2　仮想通貨取引所開設件数[7]

これら仮想通貨取引所を狙ったハッキングの手口や被害規模は様々だが,多くの事件に共通することは取引所の「セキュリティ管理の脆弱性をついたもの」であるということである．これらの状況のもと，本論文では仮想通貨取引所サービス利用者の資産保護を目的とし，仮想通貨取引所が管理する仮想通貨において送金をするために必要な“秘密鍵”の保管状況について調査する．対象となる 2 種の仮想通貨の調査結果より取引所が取り組むべき安全な顧客資産管理について考察する．

2. 関連研究

仮想通貨取引所サービスのセキュリティを調査した既存調査として，須賀による研究が挙げられる[8]．この研究は仮想通貨取引所 Web サイトの SSL/TLS サーバを調査している．

2.1 関連研究内容

研究内容は金融庁登録の仮想通貨交換業者に記載の 16 業者[9]を調査したものであり，1 業者に対し 3 種類の Web ページの SSL/TLS サーバを調査し，評価している．
評価の指標は暗号化やプロトコルの脆弱性，コンテンツの不備，リダイレクト不備などを加味してランクをつけている (同論文の 3.2 章を参照) ．結論として Web ページの SSL/TLS サーバに課題があるサイトは 6 件，さらに早急に修正すべきサイトは 1 件存在した(2018 年 4 月 10 日時点).

2.2 関連研究の課題

関連研究は SSL/TLS サーバ設定の調査であったが，この設定は仮想通貨取引所を運営する Web サイトにおいて対策すべき必須要綱であると考える．しかし，それだけでは取引所の不正送金を防止できるとは言えず，マルウェアなどによるハッキングにより不正出金が起こる可能性が未だ存在する．業界で問われている対策は Web サイトの SSL/TLS サーバ設定のほかに，二段階認証，コールドウォレット，マルチシグネチャ，顧客資産の分別管理が必須であるという意見が多い[10]．そのなかでも本稿は取引所からの不正送金を防ぐという目的としてマルチシグネチャに注目し，仮想通貨取引所の保有するウォレットに関する認証を調査することで，仮想通貨取引サービスを利用する顧客の資産管理について考察する．

3. 仮想通貨の送金トランザクション

3.1 仮想通貨送金の認証

仮想通貨取引の送金認証は公開鍵暗号方式を用いる．仮想通貨取引を始める際に文字列がランダムに設定され，この文字列を秘密鍵とし，取引の証明書となる．この秘密鍵を元に計算して公開鍵を作り，公開鍵を元に計算してコインアドレスが作られる．公開鍵で暗号化されたデータは，その公開鍵に対応する秘密鍵でのみ復号が可能となる．また，秘密鍵で暗号化されたデータは，その秘密鍵に対応する公開鍵でのみ復号できる．反対に公開鍵を分析しても，秘密鍵を特定することはできず，同様に，コインアドレスから公開鍵を特定することはできない．

ビットコインを例にして送金の流れを説明する．銀行でいう口座番号に相当する，ビットコインアドレスという文字列を指定すれば，任意のアドレスに送金することができる．主な手順は以下のようになる．

1. 送金内容(トランザクションとよばれる)の記述
2. 送金内容を秘密鍵で電子署名
3. 公開鍵ともにトランザクションを送金リクエストとし，P2P ネットワークへ送信
4. 送金リクエストの検証作業
5. 検証が承認されればブロックに送金内容を追記

つまり，送金先のビットコインアドレスおよびトランザクションは外部から誰でも確認することができる．一方で署名に必要な秘密鍵を第三者に知られると保有する仮想通貨が別のアドレスに送金されてしまう可能性があるため，秘密鍵の流出は仮想通貨を失うことに直結する．

3.2 秘密鍵の保管手法

送金に必要な秘密鍵はウォレットと呼ばれるプログラムやデバイスに保管される．ウォレットには 2 種類あり，ホットウォレットとコールドウォレットに分けられ，大きな違いは保管形態がオンラインであるかオフラインであるかの違いである．それに伴う特徴としてホットウォレットは送受金が簡単であり，運用管理コストが安いというメリットがあるが，一方で不正アクセスにより外部ネットワークからのハッキングに合うリスクがある．仮想通貨取引所で不正送金が起きたウォレットはほとんどがホットウォレットで，秘密鍵をネットワークから隔離することはセキュリ

ティ管理の視点で見ると必須である．また，仮想通貨はトランザクションの署名に複数の秘密鍵による認証を行うことが可能であり，これをマルチシグネチャ(以降マルチシグ)と呼ぶ．マルチシグの特徴として，一つの秘密鍵で署名を行う通常のシングルシグに比べてセキュリティが高く，秘密鍵紛失時に対応しやすいなどのメリットがある．しかし，デメリットとしてそれぞれの秘密鍵を設定し，多くの場合それらを別々に保存しなければならない．また，秘密鍵を利用する際も複数回認証しなければならないことが多い．さらにシングルシグに比べ複数の秘密鍵を利用する複雑な機能のため，設定や送金に追加手数料がかかる場合が多い．以上のことから運用管理の点とコストの点で難があるため，仮想通貨取引所としてはマルチシグを採用していない業社も存在し，仮想通貨盗難のリスクがマルチシグ対応の取引所に比べると高いといえる．

3.3 Bitcoin と NEM の送金アルゴリズム

本稿で調査する仮想通貨ウォレットは BitCoin と NEM であるため 2 つの仮想通貨プロトコル独自要素について述べる．

3.3.1 Bitcoin の送金スクリプト

Bitcoin の送金認証過程はトランザクションが保有するスクリプトから見ることができる．トランザクションは bitcoin ネットワークにブロードキャストされるので誰でも見ることが可能であり，過去全ての取引を確認することができる．一つのトランザクションはトランザクションインプットとトランザクションアウトプットを保有する[11]．トランザクションインプットには“scriptSig”というオブジェクトがあり，送信者のデジタル署名と公開鍵を記述した Unlocking Script がある．Unlocking Script はアウトプットの使用条件を満たすスクリプトであり，後述する Locking Script が解錠されたことを証明する．対してトランザクションアウトプットには”scriptPubkey”というオブジェクトがあり，送信者の Bitcoin アドレスを含めたビットコインをロックするためのスクリプトを Locking Script として保持している．スクリプトによる認証は Locking Script と Unlocking Script は 2 つ繋げて一つのプログラムになる性質を利用し，取引の認証を行う．スクリプトの実行結果が TRUE であれば LockingScript と UnlockingScript は対であるとみなし，ブロックチェーンに記述する．

送金スクリプトによってスクリプトの記述形式が異なる[12]．それぞれの記述方法は”scriptPubkey”内の “type” に記述される．それぞれの送金スクリプトの情報を表 2 に示す．

送金スクリプト	type	シングルシグ	マルチシグ
P2PKH	pubkeyhash	○	×
P2SH	scripthash	○	○
Multi-Signature	multisig	×	○
P2WPKH	witness_v0_keyhash	○	×
P2WSH	witness_v0_scripthash	○	○

表 2 スクリプト形式の特徴

P2PKH は現在の Bitcoin で最も使われている形式である．P2PKH 形式の”scriptPubkey”および “scriptSig” は以下のようになる．

```
scriptPubkey : OP_DUP OP_HASH160 <PubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubkey>
```

認証は，”scriptPubkey”と “scriptSig” を連結させ，連結したスクリプトを，左から順番にスタックに移動していき，実行していくことで電子署名と公開鍵を使ってアンロックする．P2PKH では認証に必要な sig は 1 つなのでシングルシグとなる．

Multi-Signature はマルチサインスクリプトの形式であり，n 個の公開鍵から m 個の署名でアンロックすることを記述する．n と m は 1 から 15 まで(n<=m）可能である．Multi-Signature 形式の”scriptPubkey”および “scriptSig” は以下のようになる．

```
scriptPubkey : <m> <A pubkey> [B pubkey] [C
pubkey．．．] <n> OP_CHECKMULTISIG
scriptSig: OP_0 <A sig> [B sig] [C sig．．．]
```

Multi-Signature の問題点としては公開鍵のハッシュや公開鍵をそれぞれ n 個分スクリプトに記載しなくてはならないためスクリプトの肥大化によるトランザクション手数料の高騰が課題である[13].

P2SH 形式のスクリプトは”scriptPubkey”を 20 バイトのハッシュ値にしたものを置き換え，ハッシュ変換前を Redeem Script，変換後を含めたスクリプトを Locking Script とする形式である．P2SH 形式のスクリプトは三種あり，以下のようになる．

```
Redeem script : OP_2 <A pubkey> <B pubkey> <C pubkey>
OP_3 OP_CHECKMULTISIG
scriptPubkey : OP_HASH160 <Hash160(redeemScript)>
OP_EQUAL
scriptSig: OP_0 <A sig> <C sig> <redeemScript>
```

”scriptPubkey”にはハッシュ化された RedeemScript が格納されており，RedeemScript には P2PKH や Multi-Signature 形式のスクリプトを記述することができる．そのことからシングルシグ，マルチシグどちらにも対応しており，マルチシグの場合，スクリプトが冗長にならないという利点がある．また，P2SH にはもう一つ利点があり， Script hash をアドレスとして使うことができる点である． これを P2SH

アドレスと呼ぶ．Redeem Script の 20byte hash を Base58Check でエンコードしたもので，ちょうど Bitcoin Address と同じ見た目をしており，アドレスは必ず 3 から始まるという特徴がある．そのことから，スクリプトがアドレスとして実装されることで，送り主と送り主のウォレットは P2SH 形式の送金システムの設計に関して特別な実装をする必要がない事が大きなメリットである．

P2WPKH，P2WSH は Segwit と呼ばれる技術を利用したスクリプト形式で，取引データの改ざんへの対策と，ブロックチェーンのスケーラビリティ問題を解決するために実装されている[14]．Segwit は“scriptSig”をトランザクションから分離し，別の領域に保管する．この領域を witness と呼ぶ．P2WPKH は以下のように記述される．

```
witness          : <signature> <pubkey>
scriptSig        : (empty)
scriptPubKey : 0    <PubKeyHash>
```

P2WPKH の<PubKeyHash>は，<pubkey>を RIPEMD-160 によりハッシュ化した 20 バイトの値になる．

また，P2WSH は以下のように記述される．

```
witness          : 0 <signature1> <1 <pubkey1> <pubkey2> 2
CHECKMULTISIG>
scriptSig        : (empty)
scriptPubKey : 0    <PubKeyHash>
```

P2WSH の<PubKeyHash>は redeemScript を SHA-256 によりハッシュ化した 32 バイトの値になる．

3.3.2 NEM の送金スクリプト

NEM はプロトコルレベルでマルチシグの設定機能が備わっており，API などを用いて手軽にマルチシグに対応させることができる．Bitcoin でいう Bitcoin アドレスは NEM の場合アカウントと呼ばれる．

NEM のトランザクションには NEM アカウント間の送金スクリプトとは別に,「アカウントをマルチシグアカウントに変更する」ためのトランザクションが存在する[15]．NEM でマルチシグを用いるためには，通常のトランザクション(シングルシグ)を複数人で署名し，マルチシグ変更トランザクションを送信することで，アカウントをマルチシグアカウントへと変更することができる．このトランザクションには連署人の情報が入っており，その数は最大で 32 となる．NEM トランザクションは P2P ネットワークのリソースを消費するため，各トランザクションに手数料が設定されている． 手数料はトランザクションの種類とパラメータによって決まるため，マルチシグにすると運用コストが高くなってしまう点が欠点である．アカウントごとのマルチシグ対応状況はネットワークにブロードキャストされた” account data”から参照することが可能である[16].

4. 調査

仮想通貨取引所の運営サイトでは実施しているセキュリティ対策について説明しているが，その内容は非常に漠然ており,“どの仮想通貨に”や“所有するウォレットの割合”など,具体的な対策について書かれているサイトは少ない．実際に, 金融庁の取引所調査レポート[17]によると, 多数の業者でセキュリティ対策があいまいになっている現状があり，それに加えて発生したシステム障害への対応が不適切であるとの指摘もあった．そのため，それらのサイトの記述に関して信頼性は低いといわざるを得ない．

今回の調査では取引所が所有するウォレットのマルチシグ状況をそれぞれのブロックチェーンデータから解析する．対象とする通貨は BitCoin と NEM を用いる．この 2 つを調査する理由としては, 流通量が比較的多いこと(Bitcoin は 1 位，NEM は 14 位[7]), 後述するマルチシグの実装が判別できるためである．

4.1 調査手法

4.1.1 Bitcoin アドレスのマルチシグ調査手法

調査対象とするウォレットは Bitcoin Rich List[18]と WalletExplorer[19]を参照し，12 件の取引所を調査した．なお,本稿は取引所の優劣をつけることが目的ではない為取引所名は匿名とする．3.3.1 節でも述べた通り，Bitcoin アドレスは送金スクリプト形式によってマルチシグの対応状況とスクリプトの記述方法が異なるため，以下のような手順で調査する．

1 取引所のタグ情報がついているウォレットで balance (所有額)が 0.01BTC 以上のウォレットを“所有ウォレット数”にカウント．
2 所有するウォレットのうち，balance が多く，入出金が定期的なものを“保管用ウォレット”，所有額が多く，入出金が 1 日に数十件であるものを”取引用ウォレット”と分類．
3 ウォレットのトランザクションをオンラインデータ[20]から検索．
4 ”scriptPubkey”内の”type”を API[21]から調査．
  4.1 “pubkeyhash”の場合シングルシグと判定．
  4.2 “Multi-Signature”の場合”scriptPubkey”を確認し，マルチシグの N of M を判定．
  4.3 ”scripthash”の場合は”scriptPubkey”の RedeemScript を API[22]から調査．
  4.4 それ以外なら”witness”の文字列を調査．

4.1.2 NEM アカウントのマルチシグ調査手法

調査対象のアカウントは NEM Rich List[23]を参照し，5 件の取引所を調査した．3.3.2 節で述べた通り，NEM アカウントのマルチシグ対応状況は” account data”を参照する

ことから手順は以下のようになる．

1 NEM アカウントの”account data”を API[16]より参照．
2 戻り値”meta”内の” "cosignatoryOf""を確認．空ならコールドウォレット，そうでなければホットウォレットと判別．
3 ホットウォレットの場合，”account”の”multisigInfo”を確認．
4 ”multisigInfo”に値が書いてあれば．” minCosignatories” (N)と，"cosignatoriesCount"(M)の数値をマルチシグ(N ofM)と判定．

5. 調査結果

5.1 Bitcoin アドレスの調査結果

表 3 に取引所ごとのウォレットの”scriptPubkey”およびマルチシグの N of M を示す．残高は小数点第三位切り捨ての値を表記している．各種ウォレットのアドレスは先頭 3 文字まで記載している．残高額および所有ウォレット数は 2018 年 12 月 16 日時点での値である．

取引所	保管用ｳｫﾚｯﾄ	残高(BTC)	scriptPubKey	保管用ｳｫﾚｯﾄ No	取引用ｳｫﾚｯﾄ	残高(BTC)	scriptPubKey	取引用ｳｫﾚｯﾄ No	所有ｳｫﾚｯﾄ数
A	3D2… 16r…	138,660.86 107203.07	P2SH P2PKH	3 of 6 シングルシグ	1Kr…	3,362.61	P2PKH	シングルシグ	6
B	34x… 3Qj…	41,454.93 10,088.00	P2SH	シングルシグ	1ND…	8,854.16	P2PKH	シングルシグ	939
C	3Cb…	108,134.65	P2SH	3 of 5	1EV… 19u…	1004.13 0	P2PKH	シングルシグ	1653
D	1EE…	88.03	P2PKH	シングルシグ	3Aj… 3Jf…	36.73 165.67	P2SH	2 of 3 シングルシグ	2196
E	1An… 14e…	23227.61 22,211.16	P2PKH	シングルシグ	1Kd…	9,707.12	P2PKH	シングルシグ	65
F	3Nx…	107,848.28	P2SH	3 of 5	38f… 3G1… 3CQ…	321.27 22.61 236.85	P2SH	2 of 3 2 of 3 シングルシグ	534
G	336…	30,624.55	P2SH	2 of 4	bc1… bc1…	2,903.52 1,316.11	P2WPKH	シングルシグ	48
H	なし	– –		–	17A… 12c…	5,604.00 28.88	P2PKH	シングルシグ	5616
I	33t…	200.01	P2SH	シングルシグ	3Js… 35C…	63.31 479.69	P2SH	シングルシグ	212
J	16r…	107,203.07	P2PKH	シングルシグ	1N5… 14c… 1PC…	1,156.81 1,165.62 889.75	P2PKH	シングルシグ	312
K	3L7…	61.82	P2SH	シングルシグ	35B… 34v…	1.35 1.61	P2SH	シングルシグ	2444
L	392… 342… 3JX…	1263.21 1197.25 384.03	P2SH	シングルシグ	39h… 17a…	144.55 1953.17	P2SH P2PKH	シングルシグ	1336

表 3 取引所ごとのウォレット調査結果

5.1.1 Bitcoin アドレスの調査考察

調査結果をもとに 3 つの観点から管理状況を考察する．取引所ごとに 3 つの評価点を表 4 に示す．

取引所	①	②	③
A	△	×	○
B	×	×	○
C	△	○	○
D	△	○	×
E	×	×	×
F	○	○	○
G	△	○	○
H	×	○	×
I	×	○	×
J	×	○	○
K	×	○	○
L	×	○	×

評価点①”マルチシグ対応”
○:保管用，取引所ウォレットいずれもマルチシグに対応．
△: 保管用，取引所ウォレットどちらかがマルチシグに対応．
×: 全てのウォレットマルチシグに非対応．
評価点②"分散管理"
取引用アドレスの複数運用の有無
評価点③""取引用ウォレット額の妥当性
取引用ウォレットが保有額の2割で管理されているかの可否

表 4 3 つの要素によるウォレット管理評価

①のマルチシグ対応の観点であるが，○に該当する取引所は 1 件のみであった．取引所ウォレットは頻繁に取引が行われるためホットウォレットの可能性が高く過去のハッキングと似た事例が起こる恐れがある．さらに内部犯行やシステムエラーなどの意図しない送金を防ぐことが難しいため，外部からの認証を強化しているとしても実装すべきである．

次に②の分散管理の観点について考察する．取引所アドレスを単独で運用していた取引所は 3 件存在した．また，保管用ウォレットを持たずにすべてのコインを取引用ウォレットで管理する取引所も見受けられた．このような集中管理は万が一,不正送金時のリカバリーや補償の観点から改善の必要がある．

最後に③の取引用ウォレット額の妥当性について考察する．この項目で×に当てはまった取引所は 5 件あった．運用上，取引用のウォレットはホットウォレットの可能性が高く， 外部ハッキングにより不正送金に遭いやすい．仮想通貨取引業の自主規制団体である一般社団法人日本仮想通貨交換業協会(JVCEA)の自主規制ルールでもホットウォレットでの保管は 2 割以内とされている[24]ことから．長期的な保管は保管用ウォレットかつオフラインで保管することが望ましい．

5.2 NEM アカウントの調査結果

NEM アカウントを調査した取引所は 5 件である．いずれの取引所に関してはウォレットにタグが付いているものを調査している．取引所ごとの所有するアカウントのコールドウォレット状況，もしくはマルチシグ状況を表 5 に示す．各種アカウントのアドレスは先頭 3 文字まで記載している．NEM 残高は 2018 年 12 月 16 日時点の値であり，小数点第三位切り捨ての値を表記している．

取引所名	NEMアカウント	NEM残高	コールドウォレット	N of M
α	NCE…	690,325,265.81	○	—
β	ND2…	298,449,317.41	○	—
γ	NBZ…	222,438,832.49	×	シングルシグ
δ	NDB…	220,443,887.26	○	—
α(取引用)	NAG…	66,277,365.07	×	2 of 3
ε	NBR…	6,955,503.00	○	—

表 5 NEM を取引するアカウントの調査結果

5.2.1 NEM アカウントの調査考察

5 件中 1 件がホットウォレットの状態，さらにシングルシグの状態で運用していたため，ハッキングのリスクは高いと考える．しかしながら大半の取引所がコールドウォレットかマルチシグの対策を行っており，安全性は全体的に高い．これらの対策実施は過去のハッキングからの危機意識の高まりにより，実装が進んだのではないかと考える．

6. 調査から見えてきた課題

本稿は取引所が保有する仮想通貨のウォレットについての調査を行った．調査の結果としてはいくつかの観点で取引所が行うべき対策はまだ存在する，という結論であり．特に Bitcoin においては未だセキュリティインシデントの脅威に対応しきれていないといえる結果となった．5.1.1 節で考察したことから，①に対する対応としては技術面の実装，②と③は取引所全体の管理体制を見直す必要があると考える．

今回の調査では一部の仮想通貨の調査であったが，調査に挙げた取引所は Bitcoin，NEM 以外にも様々な通貨を取り扱っており，それぞれの仮想通貨に対するセキュリティ対策は異なる．それらの対策を取引所ごとに行うだけでは業務量の負担が多く，万全な顧客資産の保護には繋がらない．そのため，仮想通貨交換業者は管理体制を充実・強化させることが求められる．現在(2018 年 12 月)の法律上では，仮想通貨交換業者の規模や特性からみて，利用者保護の面で直接的な問題がないと認められた場合にはセキュリティ対策をとらなくても仮想通貨法違反にはならない．しかし金融庁に登録済みの仮想通貨交換業者 16 社[9]により 2018 年 3 月 1 日に新しく認定自主規制団体である JVCEA の設立合意に至り，自主規制を進める方向に業界全体が向かっている．そのことから取引所ごとの保守・運用・監査の取組みと併せて，金融庁と金融庁認可の仮想通貨交換業団体である JVCEA が今後も積極的に規制ルールを確立し，業界においての資産管理体制の枠組み作りを行っていくことが，セキュリティインシデント脅威に対抗する現実的な対策であると考える．そこで本稿はウォレットのデータを用いて JVCEA を中心とした取引所間の相互監視体制を提案する．

7. ウォレット運用ルールの提案

現状，金融庁登録の仮想通貨交換業者はすべて JVCEA の会員である[9][25]ことに加え，現在金融庁に「みなし事業者」とされている業者も JVCEA に第二種会員として登録されているため，JVCEA を中心として，各ウォレット運用管理ルールを定めることにより事実上取引所の相互監視が可能になると考える．今回の調査を踏まえ，JVCEA が策定すべき運用管理ルールの提案を以下に記載する．また，本稿で述べるルールは Bitcoin と NEM に適用される．

自主規制ルールとして JVCEA 会員はウォレット運用状況を JVCEA に開示するものとする．

・開示情報

1. 顧客との取引に用いる全ての保管用および取引用ウォレットのアドレス
2. サービスとして運用している全ての仮想通貨資産額
3. 上記のウォレットの資産所有者(顧客の資産と自己の資産を区別して管理することが義務づけられている(内閣府令資金決済に関する法律第六十三条の十一)[26]ため)

・開示ウォレットのルール(ルール実装適用有無の判定方法を(判別)として示す)

① 保管用ウォレットはコールドウォレット
(判別)開示情報 1，2，3 からは判定できないので複数の会員からの監査が必要である．

② 取引用ウォレットは全体の 2 割以下の資金を保管
(判別)開示情報 1 の取引用ウォレット残高が開示情報 2 の 2 割以下であることを確認する．

③ 取引用ウォレットのマルチシグ実装義務づけ
(判別)開示情報 1 の取引用ウォレットのマルチシグ実装を確認する．

④ 取引用ウォレットは最低 2 つ以上で運用
(判別) 開示情報 1 の取引用ウォレットの数を確認する．

JVCEA はこれら開示情報を随時仮想通貨のブロードキャストされたブロックチェーンデータよりモニタリングし，開示ウォレットルール①～④のいずれかが適用されていないと判別できる場合はその交換業者に対して状況の説明と是正勧告を行う．

8. おわりに

6 章で述べた実装の課題があるため，各取引所の保管用と取引用ウォレットの把握，および相互監視を行うシステムモデルの構築は急務である．実際に金融庁の会合でも仮想通貨交換業者から仮想通貨の管理業務を分離し，専門機関による管理体制を確保するという案は論じられている[25]が，専門機関において仮想通貨を集中管理する場合，各仮想通貨交換業者にて分散管理を行う場合と比較して流出リスクは低減するのか，専門機関に集約されることでかえってリスクが増大しないかといった問題点が指摘されている．それに対して本稿 7 章で述べた提案ルールにおいては，あくまでアドレスのみの開示にとどまるため，上記の専門機関の役割にあたる JVCEA が仮想通貨を流出させるということがない．仮想通貨資産の入出金は各交換業者が最終責任をもって取り扱いつつ，JVCEA が各取引所の管理体制を牽制できる，という利点があると考える．しかし，持続可能な組織運営として監視のコストは誰が負担をするのか，JVCEA の信頼性をどのように評価するかなど，情報工学で解決でき得る領域を超えた新たな懸念が生じる．そのことから，これらの提案ルールを実際に運用するためにはさらなる検討の必要があると考える．多角的な側面において，仮想通貨交換業会の運用管理体制のシステムモデル構築は今後の課題であり，法学，金融工学，情報工学全ての分野において取り組むべき領域であると考える．

参考文献

[1] 朝日新聞デジタル,“コインチェック,580 億円分の仮想通貨流出　社長謝罪”,https://www.asahi.com/articles/ASL1V7WCML1VULFA03Z.html,2018 年 12 月 16 日参照

[2] 日本経済新聞，マウントゴックス破綻　ビットコイン 114 億円消失，https://www.nikkei.com/article/DGXNASGC2802C_Y4A220C1MM8000/,2018 年 12 月 16 日参照

[3] 朝日新聞デジタル，コインチェック，５８０億円分の仮想通貨流出　社長謝罪，https://www.asahi.com/articles/ASL1V7WCML1VULFA03Z.html,2018 年 12 月 16 日参照

[4] 日本経済新聞,「Zaif」のテックビューロ 仮想通貨 67 億円分流出,https://www.nikkei.com/article/DGXMZO3555502020092018MM0000,2018 年 12 月 16 日参照

[5] 金融庁，仮想通貨交換業者等の検査・モニタリング　中間とりまとめの公表について　https://www.fsa.go.jp/news/30/virtual_currency/20180810.html,2018 年 12 月 16 日参照

[6] CoinMarketCap，BitcoinCharts，https://coinmarketcap.com/currencies/bitcoin/,2018 年 12 月 16 日参照

[7] CoinMarketCap，Top 100 Cryptocurrencies by Market Capitalization，https://coinmarketcap.com，2018 年 12 月 16 日参照

[8] 須賀 祐治，“仮想通貨交換業者が提供する Web サイトに関する一考察,”2018-CSEC-81, no.8, pp.1-7, 2018.

[9] 金融庁，仮想通貨交換業者一覧,https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.xls,2018 年 12 月 16 日参照

[10] GMO コイン,セキュリティ・顧客資産管理,https://coin.z.com/jp/corp/about/security/,2018 年 12 月 16 日参照

[11] P2SH と Multisig,http://blog.bruwbird.com/p2shtomultisig/,2018 年 12 月 16 日参照

[12] アンドレアス・M.アントノプロス／著　今井崇也／訳　鳩貝淳一郎／訳,”ビットコインとブロックチェーンー暗号通貨を支える技術ー”,2016 年 7 月出版

[13] Bitcoin,”Bitcoin Developer Guide”，https://bitcoin.org/en/developer-guide#standard-transactions，2018 年 12 月 16 日参照

[14] Bitcoin Core,”Segregated Witness Benefits”,https://bitcoincore.org/en/2016/01/26/segwit-benef,2018 年 12 月 16 日参照

[15] GitBook,マルチシグ関連トランザクション,http://nemmanual.net/NEM_Technical_reference_JA/Transactions/4.3.html,2018 年 12 月 16 日参照

[16] 3.1.2 Requesting the account data，NEM NIS API Documentation，Version 1.22,https://nemproject.github.io/#requesting-the-account-data，2018 年 12 月 16 日参照

[17] 金融庁，仮想通貨交換業者等の検査・モニタリング中間とりまとめの公表について，p.9~10③ システムリスク管理，2018 年 12 月 16 日参照

[18] “Bitcoin Rich List”,https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html，2018 年 12 月 16 日参照

[19] “walletexplorer”，https://www.walletexplorer.com/，2018 年 12 月 16 日参照

[20] “blockchain”，https://www.blockchain.com/ja/，2018 年 12 月 16 日参照

[21] Chainquery，http://chainquery.com/bitcoin-api/getrawtransaction，2018 年 12 月 16 日参照

[22] QBit Ninja,”api.qbit.ninja for MainNet”，https://qbitninja.docs.apiary.io/，2018 年 12 月 16 日参照

[23] NEM Rich List，https://nemnodes.org/richlist/，2018 年 12 月 16 日参照

[24] JVCEA,”利用者財産の管理に関する規則ガイドライン”,https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/jvcea-guideline-6.pdf,2018 年 12 月 16 日参照

[25] JVCEA,”会員紹介”，https://jvcea.or.jp/member/,2019 年 1 月 11 日参照

[26] 日本法令索引,”資金決済に関する法律　第六十三条の十一”，http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=421AC0000000059_20180601_429AC0000000049&openerCode=1#436，2019 年 1 月 11 日参照

[27] 金融庁，「仮想通貨交換業等に関する研究会」（第６回）議事録，https://www.fsa.go.jp/news/30/singi/20181003-2.html,2018 年 12 月 16 日参照