ブロックチェーンセキュリティ最前線

仮想通貨取引所に代表されるブロックチェーン関連ビジネスが盛り上がりを見せている一方で、セキュリティに問題があり、被害を受けるケースも増えている。ブロックチェーンを活用したシステムを開発する場合は、攻撃者視点にたち、多層防御を取り入れた上での、アーキテクチャや運用設計のリスクベースによる評価が必要である。

ブロックチェーン関連ビジネスが盛り上がりを見せている一方で、セキュリティに問題があり、被害を受けるケースも増えている。ブロックチェーンのセキュリティでは、秘密鍵[1)]を如何に守るかが重要なため、最近よくマルチシグやコールドウォレットを採用すべきと言われるが、単に採用すれば安心という論調は間違いである。また、ブロックチェーンのセキュリティはこれらがすべてではない。ブロックチェーンのセキュリティは如何にあるべきか、以下で解説する。

マルチシグ採用時の注意点

マルチシグとは所有権の移動に複数の秘密鍵を必要とする方式で、一般的にセキュリティレベルが高い。マルチシグでは、N個の秘密鍵のうちM個の秘密鍵が必要な場合、M-of-Nと表現され、1つの秘密鍵が盗まれてもM-of-NのM個の秘密鍵が盗まれなければ安全である。しかし、同一サーバ上にM個の秘密鍵を保管し、サーバが侵害されれば、M個の秘密鍵はすべて盗まれてしまう。また、保管を分散させているのが同一ネットワークセグメント上のサーバである場合、1つのサーバが侵害されてしまえば、そこを起点に他のサーバも侵害され、結局はM個の秘密鍵が窃取されてしまう可能性も高い。サーバは侵害される前提にたち、秘密鍵はネットワークセグメントレベルで分散しておく等の対策が望ましい。

また、内部犯行にも留意しなければならない。適切に分散しても、担当者がM個の秘密鍵すべてにアクセス可能では問題である。そのため運用設計も重要になる。ブロックチェーンは一定の匿名性が保たれていることから、内部犯行であっても足のつく可能性はそれほど高くなく、内部犯行の敷居も低いと考えた方が良い。

なお、秘密鍵の分散や担当者のアクセスコントロールという観点は、秘密鍵のバックアップサイトや、DR（ディザスタリカバリ）サイトでも同様に必要である。

コールドウォレット採用時の注意点

ウォレットとは秘密鍵を格納する箱のようなものである。コールドウォレットとはオフライン環境下にあるウォレットを指す。ホットウォレットはオンライン環境下にある。コールドウォレットを利用する場合は外部犯行の難易度は高くなるが、内部の犯行はそれほど難しくない。ペーパーウォレット[2)]にせよ、ハードウェアウォレット（以下H/W）にせよ、コールドウォレットにアクセスできる担当者は容易に不正送金が可能である。そのため、コールドウォレットを採用する場合においても、マルチシグを組み合わせて保管を分散することが望ましい。

ホットウォレットも注意点は同様だが、ここで悩ましい問題なのが、マルチシグを採用していないブロックチェーンプラットフォームの場合である。例えば、プラットフォームの1つであるEthereumではマルチシグが採用されていない。Ethereumでは、スマートコントラクト[3)]と呼ばれるブロックチェーン上で実行可能なプログラムで、実質的にマルチシグ同様の実装をすることは可能であるが、当該コンセプトのもとで作られたParityと呼ばれるマルチシグウォレットのスマートコントラクトに脆弱性があったため、2017年には多額の仮想通貨が盗まれた。Ethereum上のスマートコントラクトは誰でもアクセス可能であり、常に攻撃のリスク

NOTE

1) 仮想通貨の所有権は秘密鍵によって証明される。所有権を移す際は、移動を表すトランザクションを生成して、秘密鍵で署名を行い、ネットワークに伝搬する。
2) 秘密鍵を紙に印刷したもの。
3) スマートコントラクトとスマートコントラクトのセキュリティについては以下の書籍が詳しい。「堅牢なスマートコントラクト開発のためのブロックチェーン［技術］入門」田篭 照博、技術評論社。
4) 秘密鍵は乱数だが、その乱数を生成する種のようなもの。

に晒されている。この場合、攻撃ポイントはスマートコントラクトのみ、つまりシングルポイントになってしまうので、リスクとしてはマルチシグを採用しないのと同等か、またはそれ以上と筆者は考える。

鍵管理で気にすべきことは他にもある。例えば、ウォレットには決定性ウォレットと呼ばれる、1つのシード[4]から複数の秘密鍵を生成することが可能な方式がある。H/Wの場合は、紛失時や故障時に備えて当該シードに該当する、ニモニックコードと呼ばれるバックアップを控えておくことで秘密鍵が復元可能となる。そのため、ニモニックコードに関してもコールドウォレットと同様のセキュリティが求められるのである。

なおH/Wでは、秘密鍵が専用のハードウェアに格納され外に出ることはないため秘密鍵の漏洩リスクは極めて低いが、H/Wを接続するPC端末がオンライン環境下にある場合は、マルウェアによってクリップボード内のアドレスを攻撃者のアドレスに書き換えられるなどのリスクもあり、オフライン環境下での利用が推奨される。

重要なのは鍵管理だけではない

確かに、ブロックチェーンにおいて、最も気にすべきは鍵管理であると筆者も考える。しかし、鍵管理観点で堅牢だからOKというのは間違いである。提供するサービスを実現するためのWebアプリケーション、サーバ、ネットワークなどを含め、全体を俯瞰した上で堅牢性を担保しなければならない。秘密鍵が盗まれずとも、不正送金等に繋がる可能性はあるためである。

例えば、ブロックチェーンの公式クライアントソフトはコマンドを叩くことで利用するが、その際JSON-RPCと呼ばれるHTTPベースのサービスが提供されていることが多く、HTTPで命令を送ることも可能である。しかし、JSON-RPCは一般的に、外部に公開する用途ではなく、ローカルホストや想定されたIPからのアクセスのみに制限すべきである。にも関わらず、JSON-RPCをユーザ向けWebサービスから直接呼び出すアーキテクチャであったり、意図せず公開している場合は、JSON-RPC経由の命令で不正送金を許してしまう可能性もある。すでに、ブロックチェーンのJSON-RPCポートを探索する動きは見られており、公開した場合は攻撃されると思った方がよい。他にも、サーバを侵害して、すべての送金先を攻撃者のアドレスに変更する不正なクライアントソフトで公式クライアントソフトを置き換えれば、秘密鍵がなくても不正送金は成立してしまう。

「マルチシグを採用している」「コールドウォレットを採用している」といった単一の側面だけ見て、セキュリティを評価するのは極めて危険である。鍵管理周りはプラクティスも整備されてきており、そのプラクティスに乗るべきだが、それが意図する背景や本質を理解しなければセキュリティレベルは上がらない。また、提供するサービスのシステム/ビジネス要件に応じてアーキテクチャや運用は変わるが、全体を俯瞰した上で、攻撃者視点に立ち、リスクベースで評価する必要がある点を強調しておく。鍵管理に加え、従来のアプリケーション同様にリスク分析やセキュリティ対策は必要なのである。

Writer's Profile

田篭 照博 Teruhiro Tagomori
NRIセキュアテクノロジーズ
セキュリティエンジニア
専門はブロックチェーンセキュリティ
focus@nri.co.jp