Research Report

第一ライフ資産運用経済研究所
Daiichi Life Group

2026 年 11 月 9 日

なぜ暗号資産はハッキングされてもなくならないのか

～巨額流出が続いても消えない需要と、投資家が負うリスク～

資産運用調査部　主席研究員　柏村　祐

（要旨）

○　2026 年 10 月末に発生したバイナンスからの約 1 兆円規模の暗号資産流出事件は、市場のセキュリティリスクを改めて浮き彫りにした。しかし、これほどの巨額流出が頻発しても、暗号資産市場が崩壊・消滅する気配はない。

○　暗号資産が繰り返し盗まれる背景には、ブロックチェーンそのものの脆弱性だけでなく、秘密鍵やウォレット、アクセス権限など、「人間とシステムの接点」に存在する管理体制の脆弱性が攻撃者に狙われやすいという構造的な問題がある。

○　リスクが顕在化しても市場が消えない最大の理由は、市場内に確固たる資金需要が存在することにある。特にステーブルコインは、暗号資産取引の基軸として機能するだけでなく、新興国における米ドルへのアクセスや国際送金といった切実な「実需」に支えられている。

○　個人投資家にとっては、暗号資産を単なる投機対象としてではなく、代替資産としての可能性も評価しつつ、リスクの所在を正しく理解することが不可欠である。ハードウェアウォレットによる自己管理の徹底や、暗号資産 ETF の活用が実務上の対応策となる。

1. 史上最大の「1 兆円流出事件」が突きつける暗号資産市場の矛盾

2026 年 10 月 29 日、暗号資産市場を揺るがす過去最大規模のハッキング事件が発生した。世界最大の暗号資産取引所であるBinance（バイナンス）から、約 4 時間にわたって約 63 億ドル（約 1 兆円）相当の暗号資産が不正に流出した（一部の資産は数分のうちに移転された）。FBI（米連邦捜査局）は北朝鮮による犯行と発表しており、ブロックチェーン分析企業も北朝鮮系ハッカー集団の関与を指摘している。手口は、偽の求人面接を装ったマルウェアへの感染などを発端とし、取引所の資産管理インフラ（ホットウォレット）の権限を奪うという巧妙なものであったとされる。なお、11 月 3 日に公表されたバイナンスの調査報告によれば、今回の事件では内部の署名サービスやアクセス権限が悪用されており、秘密鍵そのものが漏洩した証拠は確認されていない。暗号資産市場では、これまでも幾度となく取引所へのハッキング事件が繰り返されてきた。しかし、今回の「1 兆円」という被害規模は過去のあらゆる事件を凌駕するものであり、暗号資産のセ

キュリティに対する不信感を一段と強める出来事となった。なお、バイナンスは流出資産の一部を凍結するとともに、顧客資産の補填を進めており、こうした取引所による損失吸収も、市場への信頼を維持するうえで重要な役割を果たしている。

ここで、多くの人が抱くであろう素朴な疑問がある。「これほどまでに巨額の資産が盗まれ、危険性が浮き彫りになっているにもかかわらず、なぜ暗号資産の市場は崩壊・消滅しないのか？」通常の金融商品であれば、これほどのセキュリティリスクが顕在化すれば、投資家が資金を引き揚げ、市場の機能が大きく損なわれる可能性がある。しかし現実には、事件直後こそ市場は動揺を見せたものの、暗号資産の取引が完全に停止したり、価値がゼロになったりする気配はない。それどころか、機関投資家の参入や新たな金融商品の組成など、市場は依然として拡大―傾向を維持しているようにも見える。この「頻発する巨額流出」と「消えない市場」という矛盾の正体は何なのだろうか。暗号資産は単なる危険な投機対象に過ぎないのか、それとも私たちが想像する以上に、グローバルな金融システムの中で確固たる「需要」を持ち始めているのだろうか。

本稿では、この矛盾を解き明かすため、マクロ的な視点と客観的なデータから暗号資産市場の実態に迫る。次章では、なぜ暗号資産が繰り返し盗まれるのかという「リスクの構造」を整理した上で、それでもなお世界中の資金を引きつけ続ける「需要の源泉」を紐解いていきたい。

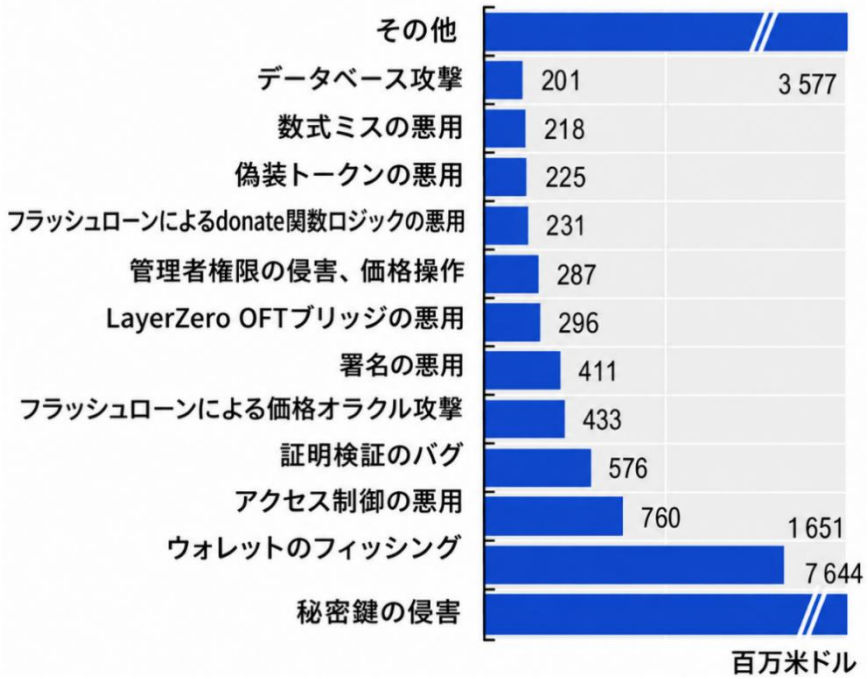
2. 巨額流出が続いても消えない暗号資産の需要とリスク構造

(1) 狙われる秘密鍵とウォレット

暗号資産市場では、取引所や投資家から巨額の資産が流出するハッキング事件が後を絶たない。こうした事件が繰り返される背景には、ブロックチェーンそのものへの攻撃だけでなく、秘密鍵やウォレット、アクセス権限など、その周辺にある管理体制の脆弱性が攻撃者に狙われやすいという構造的な問題がある。

OECD（経済協力開発機構）が2026年6月に公表した「Asia Capital Markets Report 2026」によれば、暗号資産のサイバーセキュリティインシデントによる被害は甚大である。資料1は、2016年から2026年にかけて発生したハッキングの手法別被害額を示している。これを見ると、最も被害が大きいのは「秘密鍵の侵害」であり、その被害額は76.44億ドルに上る。次いで「ウォレットのフィッシング」が16.51億ドルとなっている。暗号資産の所有権は暗号技術によって守られているが、それを操作するための「秘密鍵」がオンライン環境（ホットウォレットなど）に晒されていれば、悪意のある第三者による不正アクセスを許すおそれがある。近年ではAIを用いた巧妙なフィッシング詐欺なども増加していると指摘されており、投資家や取引所の管理の隙を突く攻撃が高度化している。つまり、暗号資産の流出リスクは、システムの中核よりもむしろ、「人間とシステムの接点」である秘密鍵やウォレットの管理といった人的・運用上の部分に集中しているのである。

資料１　暗号資産のハッキング被害は秘密鍵の侵害とフィッシングに集中している



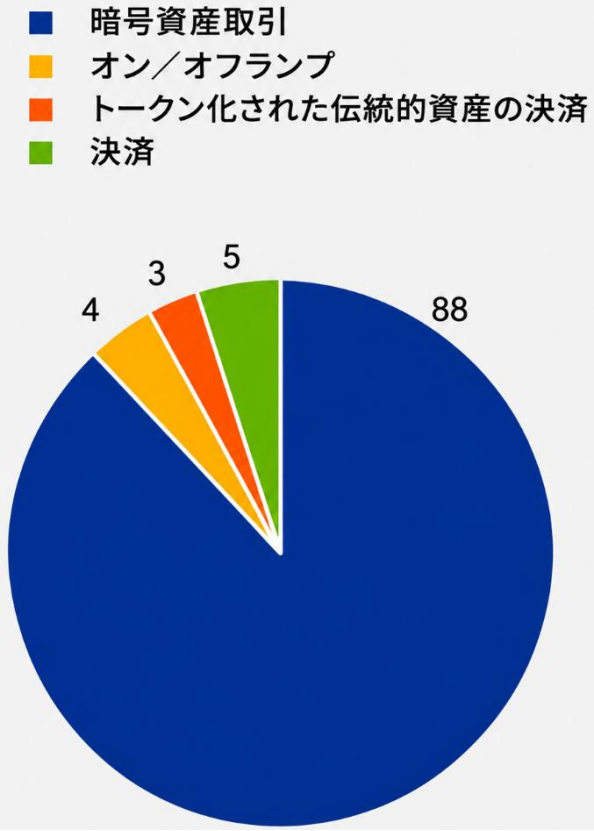
（注）2016 年から 2026 年におけるハッキング手法別の被害額（百万ドル）。秘密鍵の侵害が 76.44 億ドル、ウォレットのフィッシングが 16.51 億ドルと突出している。2026 年のデータは同年通年の集計ではなく、同年 10 月のバイナンス事件は含まれていない。
（出所）OECD, “Asia Capital Markets Report 2026”をもとに第一ライフ資産運用経済研究所作成

(2) 暗号資産市場を支える取引需要

これほどまでにハッキングや詐欺の被害が繰り返され、リスクが顕在化しているにもかかわらず、暗号資産市場が消滅しないのはなぜだろうか。その最大の要因は、市場の内部に、巨額の流出事件が発生しても失われない資金需要が存在していることにある。その需要の構造を読み解く鍵となるのが、法定通貨と価値が連動する「ステーブルコイン」の存在である。

ECB（欧州中央銀行）が 2026 年 6 月に公表したレポート「From money market funds to stablecoins」は、ステーブルコインの用途を分析している。資料 2 の円グラフが示す通り、ステーブルコインの用途の圧倒的多数である 88%が「暗号資産取引」に用いられている。次いで「決済」が 5%、「オン／オフランプ（ステーブルコインウォレットと暗号資産取引所間の資金移動）」が 4%、「トークン化された伝統的資産の決済」が 3%となっている。このデータは、暗号資産市場が自己増殖的なエコシステムを形成していることを示唆している。投資家は、価格変動の激しい暗号資産を売買する際、いちいち法定通貨に戻すのではなく、価値が安定したステーブルコインを資金の退避先や取引の基軸通貨として利用している。つまり、暗号資産市場には、ステーブルコインを介して暗号資産を売買し、資金を移動させる大きな取引需要が存在している。市場内部でこの需要が回り続けている限り、巨額の流出事件が起きても取引そのものが止まることは考えにくい。

資料 2 ステーブルコインの用途は暗号資産取引が圧倒的多数を占める



（注）ステーブルコインの用途別構成比（%）。暗号資産取引が 88%を占め、市場内の資金移動の基軸となっている。
（出所）ECB, “From money market funds to stablecoins”をもとに第一ライフ資産運用経済研究所作成

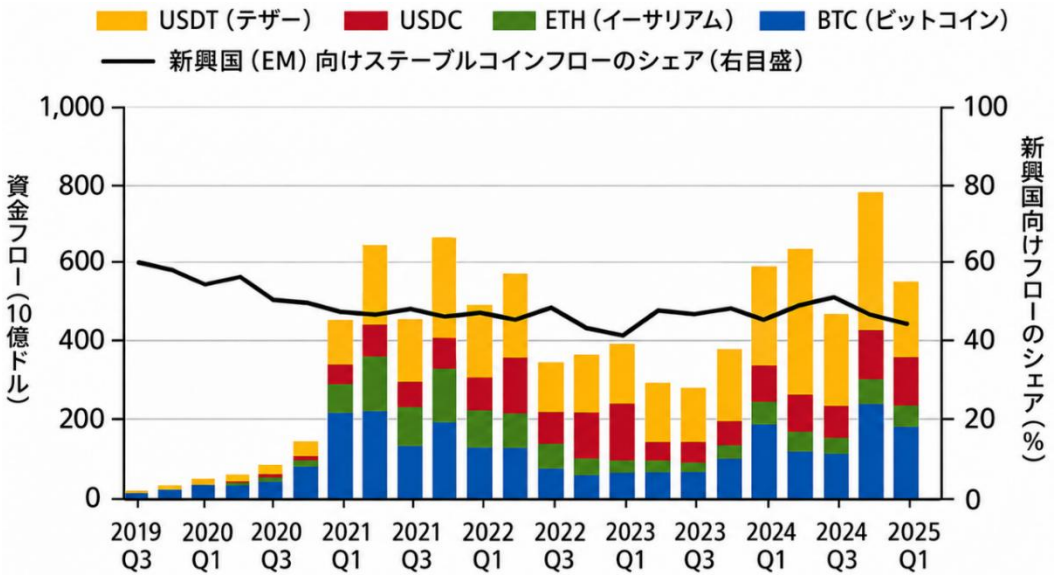
(3) 新興国における実需と米ドルへのアクセス

暗号資産の需要を「先進国の投資家による投機」だけで片付けることはできない。視野をグローバルに広げると、新興国を中心とする実需の存在が浮かび上がる。

IMF（国際通貨基金）が 2026 年 4 月に公表した「Global Financial Stability Report」は、暗号資産を通じた国境を越えた資金移動の急増を指摘している。資料 3 は、暗号資産別の国際移転額の推移を示したものである。代表的なドル連動型ステーブルコインであるUSDT（テザー）とUSDCの四半期ごとの国際移転総額は、2020 年初頭の約 120 億ドルから、2025 年初頭には約 3,160 億ドルへと、わずか 5 年で約 26 倍に急増している。この増加の背景には、新興国特有の事情がある。自国通貨のインフレ率が高く為替変動が激しい国や、厳格な資本規制が存在する国において、人々は資産保全の手段を求めている。そうした環境下では、ステーブルコインは事実上の「米ドルへのアクセス手段」として機能する。また、伝統的な金融インフラが未発達な地域では、安価で迅速な「国際送金や海外からの送金受取の手段」としても重宝されている。

このように、暗号資産市場には投機的・投資的な取引需要に加え、新興国における米ドルへのアクセスや国際送金などの実需も存在している。こうした複数の需要が重なり合っていることが、ハッキングリスクを抱えながらも市場が存続する背景の一つと考えられる。

資料 3　USDT・USDC の国際移転額は 5 年間で約 26 倍に急増



（注）暗号資産別の国際移転額（10 億ドル、左軸）および新興国（EM）向けステーブルコインフローのシェア（%、右軸）の推移。
　　USDT および USDC の移転額が 2020 年以降急増している。
（出所）IMF, “Global Financial Stability Report (April 2026)”をもとに第一ライフ資産運用経済研究所作成

3. 個人投資家はどう向き合うべきか～「実需」の評価と「自己管理」の徹底～

第 2 章で見てきたように、暗号資産市場は単なる投機マネーの遊び場ではなく、ステーブルコインを基軸とした強固な取引需要と、新興国における資産保全や送金の実需にも支えられている。後者は、従来の金融システムを補完する役割を担いつつある。この視点に立てば、個人投資家にとっても、暗号資産を「実体のない危険なバブル」と安易に切り捨てることは適切ではない。暗号資産をポートフォリオの一部に組み入れることは選択肢の一つとなりうるが、その際には価格変動の大きさに加え、伝統的な株式や債券との相関が市場環境によって変化する可能性にも十分注意する必要がある。

ここで重要なのは、投資に際してリスクの所在を正確に把握することである。バイナンスの 1 兆円流出事件や、過去 10 年間のハッキング被害のデータが物語るように、暗号資産のサイバーセキュリティ上の重大なリスクは、ブロックチェーン技術そのものだけでなく、取引所のホットウォレットや投資家自身による秘密鍵の管理など、「人間とシステムの接点」に存在する脆弱性にもある。サイバー攻撃が AI も駆使して極めて高度化・巧妙化する環境下において、中央集権的な暗号資産取引所に多額の資産を預けっぱなしにすることは、常にカウンターパーティリスクを抱え続けることを意味する。こうしたリスク構造を踏まえ、個人投資家が暗号資産に向き合うための実務的な対応策は、大きく 2 つ挙げられる。

第一に、暗号資産の現物を直接保有する場合には、「自己管理（セルフカストディ）」を選択肢の一つとして検討することである。暗号資産の秘密鍵をインターネットから切り離して管理できる専用機器（ハードウェアウォレット）を活用し、秘密鍵を自らの責任で厳重に管理する。これ

により、取引所への資産預託に伴うハッキングリスクを低減できる一方、秘密鍵の紛失やフィッシングなど、自己管理に固有のリスクには引き続き注意が必要である。

第二に、秘密鍵の自己管理に不安や負担を感じる場合には、海外市場で取引される「暗号資産ETF（上場投資信託)」などの関連商品を活用する方法も考えられる。こうした商品では、裏付けとなる暗号資産の保管（カストディ）を専門機関が担うため、投資家自身が秘密鍵を直接管理する必要はない。ただし、保管機関への依存や商品自体の価格変動リスクなどがなくなるわけではなく、日本国内での取扱状況や投資可能な商品にも留意する必要がある。

暗号資産は「危険だから一切触れない」という段階を過ぎ、グローバルな資金需要を持つ新たな資産クラスへと成長しつつある。だからこそ、これからの個人投資家には、ニュースの表面的な印象に流されるのではなく、「何が本当のリスクなのか」を冷静に見極め、適切な防衛策を講じた上で市場に参加するかどうかも含め、慎重に判断する姿勢が求められている。

以　上

【参考文献】

・OECD (2026) “Asia Capital Markets Report 2026”
・ECB (2026) “From money market funds to stablecoins”
・IMF (2026) “Global Financial Stability Report (April 2026)”
・Binance (2026) “29 October 2026 Binance Security Incident: Initial Findings and Response Update”, November 3
・FBI (2026) “North Korea Responsible for $6 Billion+ Binance Attack”, October 31

本資料は情報提供を目的として作成されたものであり、投資勧誘を目的としたものではありません。作成時点で、第一ライフ資産運用経済研究所が信ずるに足ると判断した情報に基づき作成していますが、その正確性、完全性に対する責任は負いません。見通しは予告なく変更されることがあります。また、記載された内容は、第一生命保険ないしはその関連会社の投資方針と常に整合的であるとは限りません。