

各取扱仮想通貨特有のリスク

仮想通貨に固有のリスクとして、本紙の「《重要事項説明》」において説明したリスク以外に下記のリスクがあります。

1. ビットコイン及びビットコインキャッシュ

記録台帳の改竄・発行プログラム改変リスク（「51%攻撃リスク」）

《重要事項説明》において説明しましたとおり「51%攻撃リスク」として、悪意ある者が取扱仮想通貨を発行済総数の51%以上有した場合、不正な取引が行われるリスクがあります。

具体的には、多数の記録者が結託し、あるいは既存の記録者が有する処理能力合計よりも強力な能力を用いることによって、記録台帳が改竄され、また発行プログラムが改変されるリスクがあります。

なりすましリスク

第三者に秘密鍵（暗号鍵）を知られた場合には、利用者になりすまして送付指示が行われるリスクがあります。

ハードフォークによる分岐リスク

《重要事項説明》において説明しましたとおり「ハードフォークによる分岐リスク」として、ハードフォークにより仮想通貨が2つ以上に分岐し、相互に互換性がなくなるリスクがあります。その場合、大幅な価値下落や取引が遡って無効になるリスクがあります。

具体的には、ハードフォークにより分岐したブロックの一方が否決された場合、否決されたブロックに収録された取引は再び認証を得なければ、次の送金が行なえなくなるリスクがあります。さらに、記録者の目に留まらず、未承認データのまま放置されるリスクがあります。

プログラムの脆弱性によるデータ改竄リスク

未検出のプログラムの脆弱性やプログラム更新などにより新たに生じた脆弱性を利用し、データが改竄され、また価値移転の記録が異常な状態に陥る可能性があります。

ハッキング被害等による盗難・価値下落リスク

Mt.Gox というビットコインを取り扱っていた取引所（交換所）がハッキング被害を受け、

ビットコインやユーザー情報・パスワードが盗難され約 1 週間取引が停止されたという事件が生じています。この影響で、連鎖的に他の取引所からもビットコインの盗難が発生し、ビットコイン価格が著しく下落したことがあります。今後も同様の事件が生じ、それによりビットコインが盗難され、又はその価格が著しく下落するリスクがあります。

2. フィスココイン・カイカコイン・ネクスコイン

ビットコインと同種のリスク

ビットコインと同様にブロックチェーンを利用しているため、フィスココイン、カイカコイン及びネクスコインには、上記のビットコインのリスクが妥当します。

フィスココインを含むカウンターパーティ（後述）上のトークンは、ビットコインの分岐の影響を受けますが、ビットコインが機能する限りはトークンの帰趨に影響を及ぼさないものと考えられています。

カウンターパーティのサービスに伴うリスク

ビットコイン上に構築されている「カウンターパーティ」と呼ばれるカラードコインサービスにおいてフィスココイン、カイカコイン及びネクスコインがそれぞれ構築されています（※）。

そのため、カウンターパーティが分散型金融プラットフォーム事業から撤退する場合又はカウンターパーティのサービスに何らかの障害が発生した場合には、フィスココイン、カイカコイン及びネクスコイン自体がその影響を受け、その結果、当該仮想通貨が存立しえなくなるリスクや、当該仮想通貨の取引ができなくなり、又はその価値が下落するリスクがあります。

（※）なお、カウンターパーティのサービスは、これが発行するビットコイン上のトークン「XCP」を支払うことで、発行者が独自トークンを発行することができるサービスです。XCP は発行の際に必要なとなりますが、その後の流通には XCP は無関係となります（流通はビットコインのブロックチェーン上で行われます。）