【FinTech実証実験ハブ⑬】暗号資産分野のマネロン等対策の高度化・共同化に関する実証実験

○ 本実証実験では、暗号資産交換業者等の間で、詐欺等に関連していることが疑われるブロックチェーンアドレス等の情報連携を行い、共同で情報収集・分析を行うことで、マネー・ローンダリング及びテロ資金供与対策（マネロン等対策）の高度化・共同化の実現可能性を検証。

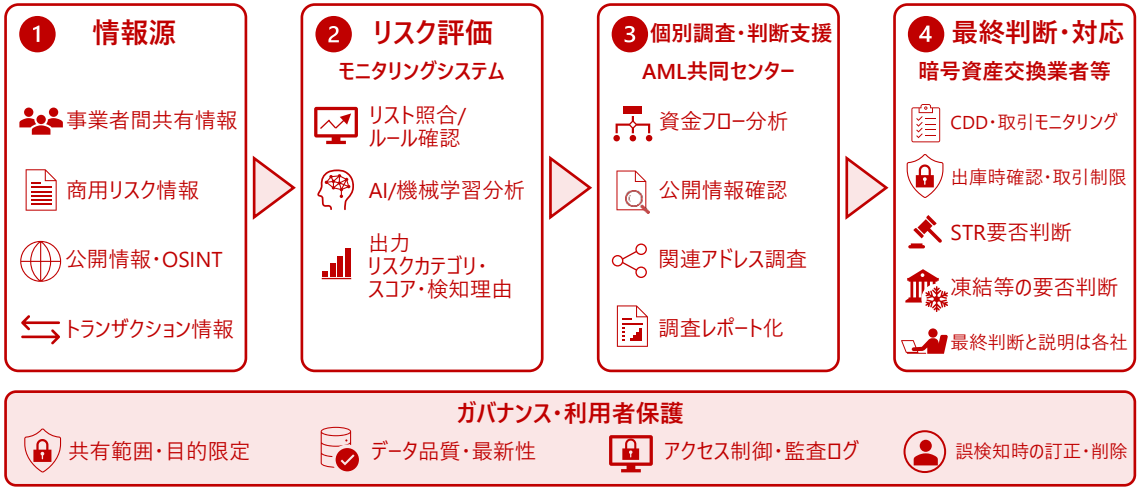
○ 事業者間での共有情報、商業的に入手可能な情報、公開情報をもとに、リスト照合と機械学習（AI）処理を併用し、アドレスのリスク評価を実施。当該リスク評価を暗号資産交換業者等による継続的顧客管理（CDD）や取引モニタリング、暗号資産交換業者ウォレットからの移転（出庫）時のリアルタイムでのリスク検知、ステーブルコイン発行者による対応（資産の凍結等）の判断材料に活用。

○ 参加企業は、株式会社日立製作所ほか17社。

実験概要

- 暗号資産交換業者等の間で、疑わしいアドレス、トランザクション情報、リスクカテゴリ、リスクスコア、検知理由等からなる情報を共有。
- モニタリングシステム提供者において、当該共有された情報、商業的に入手可能な情報、公開情報をもとに、リスク評価を実施。評価は複数項目からなり、既知の疑わしいアドレスのリストとの照合と機械学習処理を併用。
- 暗号資産交換業者等は、定期的に又は任意のタイミングで、特定のアドレス又は特定のトークンを保有するアドレスについて、モニタリングシステムを通じて、リスク評価を実施。継続的顧客管理（CDD）、取引モニタリング、ステーブルコイン発行者による犯罪利用疑いのあるステーブルコインの凍結等の判断材料として活用。

＜本実証実験における情報共有・リスク評価の流れ＞



✓ リスク評価はシステムで行うが、アラートだけで最終判断しない

✓ 個社単独では把握しにくいリスク情報を、業界横断で補完

実験結果等

○ 個社単位では把握しにくい情報の活用可能性、機械学習処理の併用による既知ではない疑わしいアドレスの捕捉可能性、取引モニタリング等への実務的な運用可能性を確認。一方、モニタリングシステムが発するアラートだけでは、疑わしい取引の届出（STR）等の判断材料としては不十分な場合があり、個別の調査の必要性も確認。

○ 当庁からは、①疑わしい取引の届出（STR）等は暗号資産交換業者等の責任で行う必要があり、アラートにのみ依存するのではなく、根拠の説明可能性が必要であること、②誤検知による権利侵害防止のため、データ品質確保や顧客による権利行使等の手続整備等を検討する必要があること、③疑わしいアドレスの提供・共有については、個人情報保護法上のいわゆる財産保護例外を適用しうること等を助言。

○ 今後、暗号資産分野でも、「共助」によるマネロン等対策の高度化・効率化に期待。