FATF 報告書

ランサムウェアによる不正資金調達への対策

潜在的リスク指標

2023 年 3 月

ランサムウェアによる不正資金調達への対策：潜在的リスク指標

以下の潜在的リスク指標は、グローバルネットワークの国・地域から収集した経験・データから得られたものである。これらの指標は、ランサムウェアに関連する疑わしい取引の検知を強化させることを目的としている。本リストは、身代金支払プロセスの様々な観点にさらに区分される。

リスク指標を使用する前に、読者には以下の取扱注意事項及びランサムウェアによる不正資金調達への対策に関する 2023 年 FATF 報告書を読むことを推奨する。

ランサムウェアによる不正資金調達への対策

本報告書は、犯罪者がランサムウェア攻撃を実行するための手法と身代金の洗浄方法について分析している。

本報告書では、ランサムウェアの身代金支払いの洗浄に効果的に対処するためには、当局が既存の国際協力の仕組みを構築し活用する必要があることを強調している。また、重要な情報を迅速に収集し、ほぼ瞬時に行われる仮想取引を追跡し、暗号資産が散逸する前に回復するために必要なスキルやツールを開発する必要がある。

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

顧客又は取引と関連するそれぞれの指標は、ランサムウェア攻撃の疑いがあることを保証するものではなく、また必ずしもこのような活動を明示するものでもない。ただし、必要に応じて、さらなる監視や調査を促すものである。

指標リストは、FATF の暗号資産レッドフラッグ指標[1]に記載の指標を補完するものであり、公共機関と民間企業の両者に関係する。後者では、指標は VASP（Virtual Asset Service Provider）、銀行、その他の金融機関・送金機関に関係する場合がある。

[1] FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorism Financing（2020 年 9 月）を参照のこと。 www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

銀行及びその他の金融機関・送金機関による、ランサムウェア被害者の支払いの特定

- ランサムウェア復旧を扱うサイバーセキュリティコンサルティング企業又はインシデント対応企業への仕向電信送金
- ランサムウェア復旧を扱う保険会社からの通常と異なる被仕向電信送金
- 顧客によるランサムウェア攻撃又は支払いに関する自己報告
- 顧客へのランサムウェア攻撃に関するオープンソース情報
- 同一の銀行口座から VASP の複数の口座への大量の取引
- 支払明細に「身代金」などの語句やランサムウェアグループの名前が含まれる
- リスクの高い国・地域にある VASP に対する支払い（Box を参照）

VASP によるランサムウェア被害者の支払いの特定

- インシデント対応企業又は保険会社による、第三者の代理での暗号資産購入の依頼
- 顧客が身代金支払いのために暗号資産を購入していると VASP に申告する
- 暗号資産取引の履歴のないユーザーによる標準的なビジネス慣行以外の送金
- 顧客が口座の限度額を引き上げて第三者に送金する
- 顧客が支払いにかかる時間について不安や焦りを感じているようである
- 匿名性を強化した暗号通貨の購入あるいは関連する取引
- リスクの高い国・地域にある VASP に対する支払い
- 新規顧客が暗号資産を購入し、口座の残高全額を単一のアドレスに送金する

VASP による身代金の支払い受領・ランサムウェア犯罪口座の特定

- 最初の大規模な暗号資産移転後に、顧客がデジタル通貨の取引をほとんど、あるいはまったく行っていない
- ウォレットアドレスのブロックチェーン分析によりランサムウェアとのつながりが判明する
- 暗号資産への資金の変換後、即時の引き出し
- ランサムウェアに関係のあるウォレットへの暗号資産の送金
- リスクの高い国・地域での VASP の利用
- ミキシングサービスへの暗号資産の送金
- 暗号化されたネットワークの使用
- 確認情報がコンピューター画面上のデータの写真である、あるいはファイル名に「WhatsApp image」などの文言が含まれる
- 顧客の構文（Syntax）が顧客のデモグラフィックと一致しない
- 顧客情報により、顧客が Proton Mail や Tutanota などのプライバシーの高い電子メールアカウントを所有していることが示される
- 認証情報の不整合、又は偽の身元情報での口座作成の試み
- 複数の口座が同一の連絡先とつながっている、アドレスが異なる名前で共有されている
- 顧客が VPN を使用しているように思われる
- 匿名性を強化した暗号通貨に関連する取引

Box: マネー・ローンダリングリスクのより高い国・地域

ある地域の ML/TF（マネー・ローンダリング/テロ資金供与）のリスクの高さを判断するための統一された定義や方法論はないが、他のリスク要因とともに国別のリスクを考慮することによって、潜在的な ML/TF のリスクを特定するための有益な情報が得られる。高リスクを示す指標は、(a) テロ活動への資金提供や支援をしていること、又は指定されたテロ組織が活動していることが、信頼できる情報源から特定されている国や地域、(b) 違法薬物、人身売買、密輸、違法賭博の供給国や中継国であることを含む、組織犯罪、汚職などの犯罪活動が著しいと、信頼できる情報源から特定されている国、(c) 国連などの国際機関による制裁、貿易禁止、又は類似の措置の対象となっている国、(d) ガバナンス、法執行、規制体制が脆弱であると、信頼できる情報源から特定されている国。FATF 声明の中で、特に VASP のための AML/CFT（マネー・ローンダリング/テロ資金供与対策）が脆弱であるため、VASP やその他の義務付けられている事業体がビジネス関係や取引に特別な注意を払うべきと特定されている国も含まれる。

出典: FATF（2021 年）「Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs」パラグラフ 154

www.fatf-gafi.org

2023 年 3 月

ランサムウェアによる不正資金調達への対策：潜在的リスク指標

これら潜在的リスク指標は、ランサムウェアに関係する疑わしい活動を公共機関や民間企業が特定するのに役立つだろう。これらの指標は、ランサムウェア攻撃を実行するために犯罪者が使用する手段及び支払いの方法、ローンダリングの方法を分析している FATF の報告書 *Countering ransomware financing* を補完する。