FATF

FATF 報告書

ランサムウェアによる不正資金調達への対策

2023 年 3 月

金融活動作業部会（FATF）は、マネー・ローンダリングやテロ資金供与、大量破壊兵器の拡散への資金供与からグローバル金融システムを保護する政策を策定し、推進する独立の政府間組織である。FATF の勧告はマネー・ローンダリング対策（AML）とテロ資金供与対策（CFT）のグローバル基準とみなされる。

FATFについての詳細は、ウェブサイトを参照：**www.fatf-gafi.org.**

本書及び/又は本書に含まれる地図は、特定の地域の地位又は主権、国境や境界の画定、並びに地域、都市、領域の名称を害するものではない。

引用：

FATF(2023)、*ランサムウェアによる不正資金調達への対策*、FATF、パリ
http://www.fatf-gafi.org/publications/Methodsandtrends/countering-ransomware-financing.html

目次

以下参照：

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

潜在的リスク指標のこのリストはFATFの報告書 *Countering Ransomware Financing* を補完し、ランサムウェアに関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ちうる。

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

頭字語

AEC	匿名性を高めた暗号通貨
AML/CFT	マネー・ローンダリング /テロ資金供与対策
CERT	コンピューター緊急対応チーム
DeFi	分散型金融
DNFBP	特定非金融業者及び職業専門家
FIU	資金情報機関
IP	インターネットプロトコル
LEA	法執行機関
ML	マネー・ローンダリング
OTC	店頭取引
PPP	官民パートナーシップ
RaaS	サービスとしてのランサムウェア
STR	疑わしい取引の届出
VACG	暗号資産コンタクト・グループ
VASP	暗号資産交換業者
VPN	仮想専用通信網

要約

ランサムウェア攻撃に関連する資金移転は、近年世界規模で急激に拡大している。攻撃による 2020 年と 2021 年の身代金支払額は 2019 年と比較して最大 4 倍増になると業界では推計している。技術の進化により、攻撃の収益性と成功率が高まっており、大規模かつ重要な組織を標的にしたケースのほか、ランサムウェア攻撃者がユーザーフレンドリーなソフトウェアキットをアフィリエイト（提携者）に販売する、サービスとしてのランサムウェア（RaaS）も存在する。ランサムウェア攻撃がもたらす影響は非常に深刻で、重要なインフラやサービスに損害や混乱をもたらし、国家安全保障上の脅威となる可能性がある。

FATF による本調査は、ランサムウェア攻撃に関連する資金移転に対する理解を世界に広め、この脅威に対処するためのグッドプラクティスの特定を目的として実施された。本報告書には、関係当局や民間企業が、こうした資金移転を検知するための潜在リスクの指標リストも掲載している。本報告書の調査結果は、FATF グローバルネットワークの 40 以上の代表組織から得た情報やケーススタディを始めとする官民双方の経験と専門知識に基づくものである。

ランサムウェア攻撃は、恐喝の一種であり、FATF 基準では、マネー・ローンダリング（ML）の前提犯罪としての犯罪化を求めている。本報告書では、ランサムウェア攻撃による身代金支払いやそれに続く ML のほとんどがもっぱら暗号資産を通じて行われていることを指摘している。ランサムウェア攻撃者は、暗号資産の国際的な性質を利用して、大規模かつほぼ瞬時に国境を越えた取引を行い、時には、ML 及びテロ資金供与対策（AML/CFT）プログラムを採用している従来の金融機関を介さずに取引することもある。攻撃者は、匿名性の高い暗号通貨やミキサーなど、匿名性を強化する技術や手法、トークンを ML に使用することによって、取引をさらに複雑化させている。

ランサムウェア関連の ML のほとんどに暗号資産が使用されていることから、FATF 勧告 15 の迅速な実施の重要性がさらに高まっている。この勧告では、暗号資産に関連するリスクを低減するための措置の適用と、暗号資産交換業者（VASP）の規制をそれぞれの国・地域に求めている。これは、攻撃者が犯罪収益を洗浄するために、AML/CFT が弱い、あるいは存在しない国や地域の VASP に簡単にアクセスすることを防止するために重要である。

本調査の結果、民間企業による検知の難しさ、被害者の事業への悪影響、攻撃を報告した場合の攻撃者からの報復への恐れなどの理由で、ランサムウェア攻撃が過少報告されていることが明らかになった。こうした理由もあり、ランサムウェア関連の ML の捜査は、これまで十分に行われてこなかった。各国・地域には、検知・報告件数を増やし、強化するための取組みが求められており、関係当局は、重要な情報を迅速に収集し、暗号資産を効果的に追跡・回収するためのツールやスキルを備えておく必要がある。

ランサムウェアは、幅広い分野にまたがり、その捜査においては、サイバーセキュリティやデータ保護機関など従来の AML/CFT 当局以外の機関が関与することもあるため、ランサムウェア及びランサムウェア関連の ML に効果的に対処するためには、複合領域的アプローチが必要である。暗号資産には、分散性・越境性という本質的な性質があるため、既存の国際協力の枠組みを整備・活用することが、ランサムウェア関連の ML 対策に不可欠となる。

ランサムウェア及び関連する ML に対するグローバルな対策を強化するため、FATF は各国・地域に以下の行動を推奨している。

推奨される行動

本調査で収集した情報に基づいて、ランサムウェア関連の不正な資金移転を阻止するために、各国が取り得る行動の実例を挙げる。本セクションでは、これらのグッドプラクティスを紹介し、各国・地域がより効果的にランサムウェア関連の ML を阻止する方法を提案する。

VASP に関する項目を含めた FATF 基準の実施及び検知の強化

- 各国・地域は、勧告 15（トラベルルール[1]を含む）を可及的速やかに履行し、VASP に関連する FATF 基準の遵守を促進することによって、VASP が重要な金融情報を取得し、疑わしい取引を報告する AML/CFT 義務を確実に遵守するようにするべきである。
- 各国・地域は、FATF 勧告 3 に沿って、ランサムウェア攻撃を ML の前提犯罪（例えば、恐喝の一種）として犯罪化するべきである。
- 各国・地域に対して、以下の方法でランサムウェアの検知を強化するべきである。
    - 傾向、検知ガイド、レッドフラッグ指標（例えば、*Countering Ransomware Financing : Potential Risk Indicators*[2]に含まれている指標）を関連報告事業者と共有するなどして、規制対象事業者がランサムウェアや関連する ML を検知し、疑わしい取引を報告できるよう支援する。
    - 利用可能な支援やリソースについての啓発、安心して報告できる手段の確保などを通じて、被害者が自発的にインシデントを報告することを奨励する。
- 各国・地域は、検知源を増やすために、AML/CFT 義務の対象外となる可能性のある従来と異なる形態の組織（サイバー保険会社やインシデント対応会社など）とのコミュニケーション経路の確立を検討するべきである。

資金捜査及び財産回復の取組みの推進

- 権限ある当局は、必要に応じて従来の法執行技術と暗号資産に特化した技術を活用して、ランサムウェア関連の ML 捜査を実施するべきである。権限ある当局には、ランサムウェア関連の資金捜査に必

[1] 「トラベルルール」は、重要な AML/CFT の 1 つで、VASP が暗号資産移転の発信者と受益者に関する情報を取得、保持、共有することを義務付けるものである。これによって、金融機関や VASP は、制裁審査を実施し、疑わしい取引の検知が可能となる。

[2] 以下を参照のこと。https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

要となる専門的な技能や知識が求められており、ブロックチェーン分析や監視ツールに関する開発、アクセス、トレーニングの実施をするべきである。

- 各国・地域は、法執行機関が特に暗号資産に関して、迅速かつ効果的に資産を差押え・没収するために必要な能力と権限を有し、これを維持するようにするべきである。各国・地域は、差し押さえた暗号資産を適切に管理する特別なメカニズムを整備するべきである。

ランサムウェア対策のための複合領域的アプローチ

- 各国・地域は、国のリスク評価において、ランサムウェアがもたらす ML リスクの特定・評価をするべきである。暗号資産やランサムウェア犯罪集団の分散性を考慮すると、暗号資産業界が存在するものの現在国内ではランサムウェアが脅威となっていない国や地域も、リスクの評価・特定の対象となる。このようなリスク評価で特定された情報は、ランサムウェアのリスクを国レベルで総体的に把握することによって、国家サイバー戦略の支援にさらに役立つと考えられる。
- 各国・地域は、法執行機関、AML/CFT 当局、サイバー犯罪当局から、サイバーセキュリティ機関やデータ保護機関などの従来と異なるパートナーに至るまで、関係当局間の連携メカニズムを構築して、情報やインテリジェンスの共有を促進し、さまざまな技術的専門知識の相互共有に有用なプラットフォームを提供するべきである。

民間セクターとの連携の支援

- 各国・地域は、官民の連携を支える体制を特定・確立し、このような連携メカニズムに、VASP 及び他の従来と異なるパートナーを含めることを検討するべきである。これは、意識の向上、専門知識や知見の共有、法執行の目的を支援するために有用なプラットフォームを形成するものである。

国際協力の強化

- 各国・地域は、迅速な国際協力と情報共有を促進するために、連絡事務所や 24 時間 365 日対応の窓口の設置など、二国間、地域間、多国間のメカニズムを確立し、積極的に参加するべきである。これによって、国境を越えた迅速な資金追跡と効果的な財産回復を効率的に支援し、各当局による、ランサムウェアや関連する ML に加担する国際的ネットワークの解体に寄与する。

はじめに

焦点と対象範囲

1. ランサムウェアとは、攻撃者が開発・使用する悪意のあるソフトウェアの一種で、データ、システム、ネットワークへアクセスできないようにし、解除の対価として身代金を要求するマルウェアである。一般的な攻撃手法としては、データの暗号化や漏洩、被害者の業務妨害などがあり、攻撃には複数の手法が使われることが多く、被害者のデータを公開するといった脅迫が含まれるケースもある[3]。

2. 近年、ランサムウェアのインシデントは、件数・規模ともに著しく拡大している[4]。ランサムウェアは主に利益を追求するものであり、攻撃の件数・規模の拡大は、ランサムウェア関連の収益と ML の増加につながっている。業界では、2020 年と 2021 年のランサムウェア攻撃による身代金支払額は 2019 年と比較して少なくとも 4 倍増になると推計している[5]。最新の業界データでは、2022 年には減少傾向に転じた（被害者の支払い拒否による可能性がある）ものの、ランサムウェア攻撃者が受け取る暗号資産の価値は 2019 年以前と比較して大幅に高いままである[6]。ランサムウェア攻撃は報告されないことが多いため、実際の攻撃総数や関連する被害ははるかに多いと考えられる。

3. ランサムウェア攻撃は、政府、公共機関、企業、国民に大きな混乱と損害を与え、場合によっては、重要なインフラやサービスの停止や、機密情報の漏洩など、医療に影響を与え、国家安全保障を脅かすこともある[7]。ランサムウェア攻撃者は、攻撃の収益性と成功率を高めるための技術を開発しており、ランサムウェアに関連する不正な資金移転の脅威は今後も拡大する可能性が高いと考えられる。

4. 攻撃者のほとんどは、もっぱら暗号資産による身代金支払いを要求する。被害者、又は被害者に代わって行動する第三者は、身代金支払いに暗号資産交換業者（VASP）[8]を利用することが多い。ランサムウェア攻撃者も、VASP を利用して、不正な資金を洗浄し、収益を法定通貨に交換する。暗号資産と比較して法定通貨は、財やサービスとの交換が容易で、安定的な価値貯蔵機能に優れてい

---

[3] FBI「Scams and Safety: Ransomware」（2022 年 9 月）www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; オーストラリア・Cyber Security Centre「Ransomware」（2022 年 9 月）www.cyber.gov.au/ransomware

[4] ENISA Threat Landscape 2022（2022 年 10 月）www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[5] Chainalysis「Chainalysis Crypto Crime Report 2022」（2022 年 2 月）https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

[6] Chainalysis「Ransomware Revenue Down As More Victims Refuse to Pay」（2023 年 1 月）https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

[7] 例えば、病院に対する攻撃は患者を対象とする医療を危険にさらし、警察に対する攻撃は治安に影響を及ぼす。

[8] 暗号資産交換業者とは、FATF 勧告の他の項目でカバーされていない自然人又は法人で、他の自然人又は法人のため、又はその代理として、事業として次のいずれかを行う者を指す。暗号資産と法定通貨との交換／1 つ又は複数の形態の暗号資産間の交換／暗号資産の移転／暗号資産又は暗号資産のコントロールを可能にする金融商品の保護預かりや管理／暗号資産の発行や販売に関する金融サービスへの参加や提供。

る。

5. 2018 年に、FATF 勧告が改訂され、暗号資産と VASP が対象に加わって以来、FATF は、各国・地域と民間セクターが、ML やテロ資金供与（TF）のレッドフラッグ指標など、リスクを監視・低減するためのさまざまなガイダンスを提供している[9]。それらのガイダンスではこれまでもランサムウェアについて取り上げてきたが、FATF がランサムウェア攻撃関連の ML の傾向や技術に特に着目した報告は今回が初めてである。

6. シンガポール議長の下、FATF は暗号資産に関わる資金捜査の経験を活かし、ランサムウェアによる資金調達や関連する ML に対処するための課題を特定し、グッドプラクティスを共有している。本報告書では、ランサムウェア関連の身代金支払いの特定・報告方法、ランサムウェアによる資金移転の阻止・検知・捜査手法、資金の洗浄方法に焦点を当てている。本調査のために提出された情報やケーススタディにおいて、テロ資金調達目的のランサムウェア攻撃は顕著に見られなかったため、本報告書ではこの目的によるランサムウェア攻撃には焦点を当てていない。

7. ランサムウェア攻撃は、一種の恐喝であるため、FATF 勧告では、すべての国・地域にランサムウェアに関連する ML の犯罪化を求めている（R.3）。また、FATF は、ML リスクを特定・評価し、低減するための措置を講じること（R.1～2）、VASP を含めた民間セクターが疑わしい取引の届出など適切な予防措置を講じること（R.9～23）、法執行機関が犯罪収益を捜査、追跡、没収すること（R.4、29～31）、ML、前提犯罪、関連収益を追跡するために国際的に連携すること（R.36～40）などを各国・地域に求めている。

8. ランサムウェア攻撃は、サイバー犯罪の一種であるが、本報告書で紹介する情報は、ランサムウェアに焦点を当てたものであり、マルウェア、フィッシング、ビジネスメール詐欺、金融情報の漏洩と不正売買など、他の種類のサイバー犯罪に必ずしも当てはまるわけではない。

目的・構成

9. 本報告書の第 1 部では、ランサムウェア攻撃者が、違法な収益をどのように受領、洗浄、現金化するかを紹介し、世界的なランサムウェア脅威の規模、どのようにランサムウェアに対する、又はそれに関連する支払いがなされるか、ランサムウェア攻撃関連の収益がどのようにサイバー犯罪者に提供されるかについて、グローバルな認識と理解の向上を図る。

10. 第 2 部では、ランサムウェアに関連する資金移転を特定、捜査、阻止するための課題とグッドプラクティスを紹介する。

11. 本報告書は、**対策の実務を担う当局**が、質の高い金融インテリジェンスを作成し、資金捜査を実施し、違法な収益を特定、追跡、差押えするために活用することを目的として作成されている。各国の**規制当局**や**政策当局**は、本報告書の情報を利用して、脆弱性を特定し、リスクの低減を図ることができる。

[9] 以下を参照のこと。FATF（2022 年 6 月）*Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers*、（2020 年 9 月）*Virtual Assets Red Flag Indicators*、（2019 年 8 月） Confidential FATF Guidance on Financial Investigations Involving Virtual Assets

また、本報告書の情報は、**金融機関**、**VASP**、**特定非金融業者及び職業専門家（DNFBP）**が、ランサムウェア関連収益の不正な移転を検知、報告、阻止するための対策を設計・実施するにあたっての一助となる。

方法

12. 本プロジェクトは、イスラエルと米国の専門家による共同リードのもと実施され、以下の国・地域や組織がプロジェクトチームのメンバーとして参加した。

オーストラリア、カナダ、欧州委員会（EC）、フランス、ドイツ、日本、ルクセンブルク、メキシコ、フィリピン、シンガポール、南アフリカ、スペイン、スイス、トルコ、英国、アジア太平洋マネー・ローンダリング対策グループ、資金情報機関(FIU：Financial Intelligence Unit)で構成されるエグモント・グループ。

13. 本報告書の所見は、以下に基づくものである。

- 本テーマに関する既存の文献及びオープンソースの資料レビュー。
- 200 以上の国・地域からなる FATF のグローバルネットワークに対して、各国・地域のリスク認識、国内法と権限、課題とグッドプラクティス、ランサムウェアに関連するケーススタディの情報提供を要請して得られた 40 以上の国・地域からの情報。
- FATF の暗号資産コンタクト・グループ（VACG）における議論[10]。
- VACG を通じての的を絞った民間セクターとの連携。

[10] 2019 年 6 月、政策活動作業部会は、FATF の要求事項を民間セクターに伝え、これを業界が実現できるように適切な技術ソリューションを迅速に開発するために、暗号資産コンタクト・グループ（VACG）を設置することに合意した。

第 1 部 ランサムウェアに関連する資金移転

資金移転の規模

14. ランサムウェア攻撃と関連する資金移転の規模は、世界各国で急激に拡大している。近年、多くの国や地域で、ランサムウェア攻撃の頻度が増加している。その増加率は 10%から数百%まで、国や地域によって異なる。これに伴い、被害者からの報告も増加しており、さまざまな国や地域でランサムウェア関連の疑わしい取引の届出（STR）が増加している。ある地域では、2021 年上半期に届出された STR から 5 億 9000 万米ドル（5 億 5200 万ユーロ）相当のランサムウェア関連の取引が確認された。総額 4 億 1600 万米ドル（3 億 8900 万ユーロ）に達した 2020 年と比較して 42%増加している[11]。法執行機関による最近の年次報告書によると、ランサムウェア攻撃は大幅に増加しており[12]、業界の推計によると攻撃数とアクティブなランサムウェアの数も同様に増加している。2021 年のランサムウェアの推定攻撃数は約 6 億 2330 万件で、2020 年の 3 億 460 万件の 2 倍以上となっている[13]。同様に、アクティブなランサムウェアの推定数は、2019 年から倍増していると報告されている[14]。

15. 一部の国・地域からの報告ではランサムウェア攻撃の水準は低い。しかし、本調査で収集した情報によると、一部の国・地域では STR 数や被害者による報告件数が増加しているにもかかわらず、依然としてランサムウェア攻撃の件数は実際よりも過少報告されていることが明らかになった。そのため、インシデントの総件数や身代金の支払額を正確に推計することは困難であるが、本報告書のために提出されたケーススタディで、ランサムウェアは先進国、途上国など、地域にかかわらずリスクとなる可能性があることが示されている。

16. 複数の地域で、ランサムウェア攻撃と関連する資金移転の増加は、ランサムウェア攻撃者が攻撃の有効性とその結果としての収益性を最大化するための、**大物狩り、サービスとしてのランサムウェア（RaaS）、二重・三重・多重脅迫型**の攻撃の技術開発と関連性があることが明らかになっている（Box 1 を参照）。

---

[11] FinCEN 「Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021」（2021 年 6 月） www.fincen.gov/sites/default/files/2021-10/Financial_Trend_Analysis_Ransomware_508FINAL.pdf

[12] FBI「Internet Crime Report 2021」（2022 年 12 月 1 日アクセス）www.ic3.gov/Home/AnnualReports; EUROPOL「Internet Organised Crime Threat Assessment (IOCTA) 2021」（2022 年 12 月 1 日アクセス）www.europol.europa.eu/publications-events/main-reports/iocta-report

[13] SonicWall「2022 SonicWall Cyber Threat Report」（2022）www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

[14] Chainalysis「Chainalysis Crypto Crime Report 2022」（2022 年 2 月） https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

Box 1. ランサムウェア技術の発展

ランサムウェア攻撃者は、世間の注目を避けたり、事業活動を再開したりするために身代金を支払う可能性が高いと思われる、価値の高い大企業や知名度の高い組織をターゲットに**大物狩り**を行う。また、ランサムウェア攻撃者は、発生した動作不能の時間に応じたコストが高くなりがちなジャストインタイムの商品・サービス提供を行うサプライチェーンで事業展開する組織や、重要なインフラ、機密情報や貴重な情報を保有する組織も選択的な標的としている。攻撃者は、このような組織が他の組織と比較して身代金を支払う可能性が高いと判断する可能性がある。

RaaS とは、ランサムウェア攻撃者によるダークウェブ上でのランサムウェアのソフトウェアキットの提供や、マルウェアの配布、被害者のネットワークへの初期侵入、データの漏洩、アフィリエイトに代わって身代金の交渉を行うなどランサムウェア攻撃要素を外部委託し、手数料や身代金の一定割合を対価として支払う犯罪ビジネスモデルを指す。また、犯罪者は、ランサムウェアを拡散するために被害者のシステムにアクセスして不正利用する目的で、窃取された認証情報を購入できる。また、特定の国・地域における特定の業界に関する情報を入手し、標的を定め、攻撃の効果を最大化できる。RaaS モデルによって、ランサムウェア攻撃を実施するためのコストと、必要となる技術的専門知識が軽減される。これにより参入障壁が下がり、高度なスキルを持たない犯罪者でもランサムウェア攻撃を仕掛けられる。

二重脅迫型とは、ランサムウェア攻撃者が、データを搾取したうえで被害者のデータを暗号化し、身代金の要求に応じない場合は、搾取したデータを公開すると脅迫する行為を指す。システム攻撃に関する脅迫に加えて、データを公開すると脅迫するこの手法は、被害者がシステムを復旧できたとしても、身代金を支払わせるためのさらなる圧力となり得る。

三重脅迫型とは、ランサムウェア攻撃者が、最初に標的となった被害者だけでなく、保護された医療情報、個人情報、アカウント情報、知的財産など、その被害者が所有する情報を開示することによって影響を受ける可能性のある第三者からも身代金を要求する行為を指す。

多重脅迫型とは、三重以上の脅迫を伴う行為を指す。暗号化と流出を利用した二重脅迫型を基本としながら、分散型サービス妨害攻撃（DDoS）、被害者の顧客への連絡、被害者の株式の空売り、インフラシステムの障害など、さらに圧力をかける戦術が含まれている。

17. 報告されたランサムウェア攻撃の被害者の半数以上は、政府・公共機関、医療、工業製品・サービス分野であることが、公開情報から明らかになった[15, 16]。多額の支払いが要求される大物狩りの影響もあり、ランサムウェアによる支払い額は全体的に増加していると考えられる。近年、ランサムウェア攻撃者は、エネルギー、金融、通信、教育機関も標的にするようになっている。大物狩りを狙うランサムウェア攻撃者は、大規模な組織を標的とする場合もあるが、中・小規模の組織や産業もまた、大いにランサムウェア攻撃の標的とされている。実際、今なおランサムウェア攻撃の標的の主流は、中小企業であることが明らかになっている。このような小規模な標的は、注目を集める大規模な標的に対する攻撃と比較して、リスクとリターンの比率がより安定している可能性がある。2020 年第 2 四半期の総攻撃数の約 55%が従業員 100 名未満の企業に対するもので、約 75%が売上高 5000 万米ドル（4700 万ユーロ）未満の企業に対する攻撃であった[17]。

18. 身代金の金額は、個人を標的とした小規模な攻撃では数百米ドル・ユーロ相当の暗号資産から、大企業、特に重要なインフラ、機密情報や貴重な情報を保有する組織を標的とした攻撃では、数百万米ドル・ユーロ相当の暗号資産までさまざまである。各国・地域の報告から、攻撃者が要求する身代金額も近年増加していることが明らかになっている。2021 年、身代金の平均支払額は約 80 万米ドル（74 万 8000 ユーロ）相当の暗号資産で、2020 年の約 5 倍となった[15]。この増加は、前述の大物狩りの手法の活用と関連していると考えられる。身代金の要求額が数千万米ドル・ユーロ相当の暗号資産に達するケースもあり、例えば、2021 年に米国の保険会社が Phoenix CryptoLocker（2021 年の収益で、Conti、DarkSide に次ぐ第 3 位の RaaS であったと報じられている）[18]の攻撃を受け、ネットワークの制御を取り戻すために 4000 万米ドル（3700 万ユーロ）を支払ったと報じられている[19]。

---

[15] Sophos「The State of Ransomware in State and Local Government」（2022 年 9 月）https://assets.sophos.com/X24WTUEQ/at/rbjqpp5wwm6v5h3wj9v3733/sophos-state-of-ransomware-government-2022-wp.pdf.

[16] Digital Shadows「Ransomware: Analyzing The Data From 2020」（2021 年 1 月）www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from-2020/.

[17] Coveware「Q2 Quarterly Report」（2020 年 8 月）www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

[18] Chainalysis「Chainalysis Crypto Crime Report 2022」（2022 年 2 月）https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

[19] Mehrotra, Kartikay and Turton, William 「CNA Financial Paid $40 Million in Ransom After March Cyberattack」 Bloomberg、2021 年 5 月 20 日（2022 年 12 月 1 日アクセス）www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

特徴と地域別の傾向

19. ランサムウェアはサイバー犯罪と暗号資産の両方の要素を含んだ、一般的に国際的に発生している事象である。FATF グローバルネットワークからの情報、ケーススタディ、業界データから、ランサムウェア攻撃における特徴や地理的傾向が指摘されている。多くのランサムウェアネットワークが、ML リスクの高い国や地域とつながっており（Box 2 を参照）、ランサムウェア攻撃者は、このような国・地域で、収益を預金または現金化する。また、このような国・地域からランサムウェア攻撃が仕掛けられたり、潜在的に支援があったりするケースも見られる[20]。

Box 2. より高いマネー・ローンダリングリスクのある国・地域

ある地域の ML/TF 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 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

20. ランサムウェア攻撃の規模は、地域によって異なる。2022 年の業界レポートによると、ランサムウェア攻撃の標的となったのは、中東・アフリカ地域が最も少なく（4%）、次いで中南米（6%）、アジア太平洋（10%）、欧州（28%）、北米（52%）となっている[21]。国・地域が受けた攻撃の規模の差によって、それらの国・地域がランサムウェアによるリスクをどのように認識しているかは異なる。FATF グローバルネットワークの情報によると、大物狩りの増加やそれに伴う高額な身代金要求を経験している国・地域では、ランサムウェア関連の ML のリスクが高いと評価する傾向が強い。

[20] 米国 Cybersecurity & Infrastructure Security Agency からの警告 （AA22-187A）（2022 年 7 月）を参照のこと。www.cisa.gov/uscert/ncas/alerts/aa22-187a.

[21] Group-IB「Ransomware Uncovered Report. Group-IB」（2022 年 5 月）https://spiresolutions.com/wp-content/uploads/2021/07/ransomware_uncovered_2020.pdf.

21. 多くの大規模なランサムウェアグループは、アフィリエイトモデルと呼ばれるRaaS の一種を運営しており、ランサムウェア攻撃の要素を外部委託し、一定の料金や身代金の一部を対価として支払う。このような攻撃者は、地理的に分散していることが多く、ランサムウェア攻撃の関係者と所在地の特定が困難な場合がある。例えば、Box 3 の EMOTET のケーススタディのように、ランサムウェア攻撃者たちは、異なる国・地域で活動しながら、協力して攻撃を行ったり、共有のインフラを利用したりできる。また、さまざまな国・地域にまたがる多様な攻撃者が関与しているため、鍵となるランサムウェア攻撃者に関連する資金移転の追跡が複雑化する可能性がある。

Box 3. EMOTET のケーススタディ [1]

近年で最大級の規模のマルウェアキャンペーン EMOTET は、2014 年にバンキング型トロイの木馬 [2] として初めて検知され、他のマルウェアやランサムウェアの重要なツールとなった。2021 年 1 月のネットワーク解体までに、EMOTET は RYUK や DopperlPaymer を含む世界のマルウェアの最大 70%を有効化しており、英国企業に大きな経済的影響を及ぼしている。EMOTET の解体には、カナダ、フランス、ドイツ、リトアニア、オランダ、ウクライナ、英国、米国の法執行機関による緊密な連携と、Europol と Eurojust による国際的な活動が貢献した。この協力体制により、各国の法執行機関は、EMOTET を利用した犯罪者の支払いや登録の詳細と関連するデータをピンポイントで分析できるようになった。この事例は、サイバー犯罪の規模と特徴を例証し、脅威に対処するために国際協力がいかに重要かを裏付けるものである。

出典：英国

注釈：

1. EMOTET に関する Europol のプレスリリースを参照のこと。
www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

2. バンキング型トロイの木馬とは、金融機関の顧客から認証情報を不正入手したり、金融情報にアクセスしようとしたりするマルウェアの一種を指す。

22. ほとんどのランサムウェア攻撃による身代金支払いに使用される暗号資産の越境性から、ランサムウェア攻撃に対して支払われた身代金の ML は国境をまたいで行われている。暗号資産のユーザーは、地理的な国境に関係なく、AML/CFT の義務を負う事業者の関与なしに、秘密鍵とインターネット接続のみを使用して、P2P（peer-to-peer）で互いに直接取引できる。ランサムウェア攻撃者などの犯罪者は、暗号資産のこうした特性を利用して、AML/CFT プログラムを実施している従来の金融機関を介さずに、インターネットによって、国境を越えた大規模な取引をほぼ瞬時に完了できる。また、ランサムウェア攻撃者は、AML/CFT が脆弱または存在しない国や地域の VASP にアクセスし、不正な収益を法定通貨に交換するために利用している。

Box 4. 暗号資産とは何か？

暗号資産とは、デジタル処理によって取引や移転ができる、デジタルによる価値表現で、支払や投資の目的で使用できる資産である。暗号資産には、FATF 勧告の他の箇所ですでに取り上げられている法定通貨、証券などの金融資産のデジタル表象は含まれない。

最も一般的に使用されている暗号資産は、ブロックチェーンのような暗号に依存した分散型台帳技術によって生成・所有記録がサポートされる交換媒介物である。後述するように、一般的な暗号資産の多くは、偽名の取引情報が視認可能なパブリックブロックチェーン上で運用されている。

出典：FATF

一般的な手法・傾向

23. ランサムウェア攻撃に関する資金捜査を成功させるには、ML に使われる手法や技術を正しく理解する必要がある。ランサムウェア攻撃は、一般的に過少報告されているため、本報告書では、身代金がどのように支払われ、洗浄され、受け取られ、場合によっては法定通貨に換金されるかについて理解を深めるために、さまざまなオープンソースからの情報と各国・地域の事例を収集した。

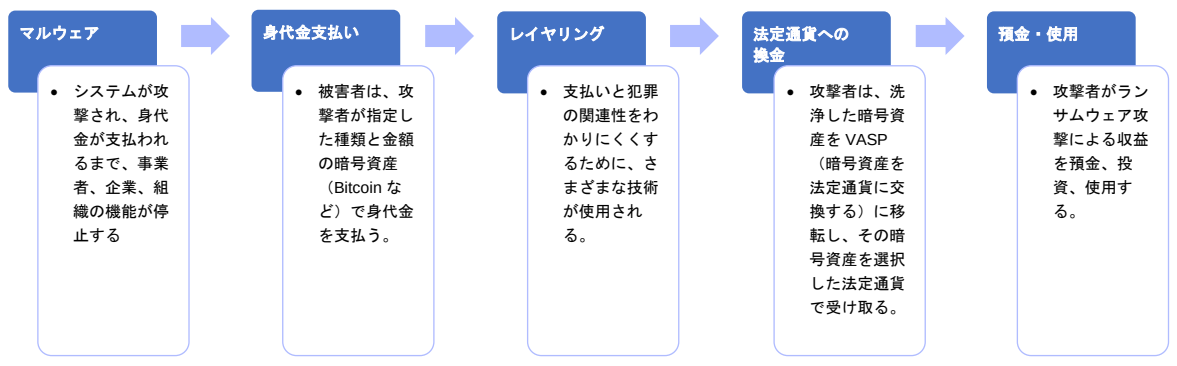
24. ランサムウェア関連の資金移転には、複数の従来型金融機関や VASP が関与していることが多い。また、被害者の身代金支払いプロセスを含むランサムウェア攻撃への対応には、サイバー保険会社、インシデント対応会社、サイバーセキュリティ会社などの第三者が関与している場合もある。

25. 身代金の支払い手段は、主に暗号資産であるが、ランサムウェアに関連する資金移転全般には、複数の従来型金融機関や VASP などの第三者も関わっている。

表 1. ランサムウェア関連の資金移転に関与する可能性のある業態

金融機関	ランサムウェアの被害者（又は被害者に代わって行動する第三者）が、暗号資産を購入するために VASP に資金を送金する際の仲介役として機能する。
VASP	ランサムウェアの被害者（又は被害者に代わって行動する第三者）は、VASP を利用して、ランサムウェア攻撃者が指定した種類と額の暗号資産を購入し移転する。
保険会社	サイバー保険の適用範囲の一部として、身代金を補償し、時には支払うこともある。
インシデント対応会社	ランサムウェアの被害者と契約を締結しているインシデント対応会社の多くは、身代金の支払いについて攻撃者と交渉する役割を果たす。サービスの一環として、被害者に代わって、身代金支払いのための暗号資産を VASP から購入し、攻撃者に移転することもある。
サイバーセキュリティ会社	顧客のデータ、システム、ネットワーク、接続機器を不正・違法なアクセスから保護する。

Box 5. ランサムウェアの支払いに関連する典型的な資金移転



身代金の要求を被害者が受け取った後、被害者又は被害者に代わって行動する第三者は、通常、電信送金、自動クリアリングハウス、又はクレジットカード払いで資金を VASP に送金し、ランサムウェア攻撃者が指定した種類と金額の暗号資産を購入する。被害者に代わって行動する第三者としては、インシデント対応会社やサイバー保険会社などが挙げられる。

次に、被害者又は第三者が、多くの場合、VASP がホストするウォレットから、攻撃者の暗号資産アドレスに身代金を送金する。これは、ランサムウェア攻撃者やマネーミュールが管理する非ホスト型ウォレット（アンホステッドウォレット、VASP などの第三者の外部で暗号資産を保有、保管、移転できるソフトウェアやハードウェア。非保護型ウォレット・ノンカストディアルウォレットとも呼ばれる）や、攻撃が発生した地域外に位置し、法執行機関や資金情報機関と通常は連携していない VASP がホストするウォレットである。

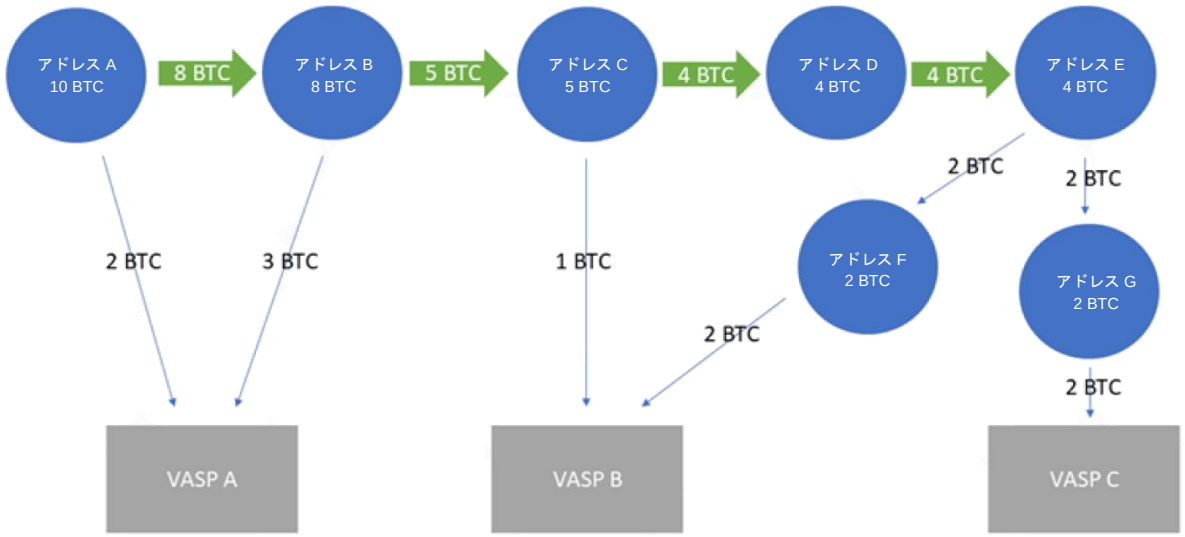
多くの場合、ランサムウェア攻撃者は、レイヤリングのためにさまざまな技術を使用する（詳細については後述を参考のこと）。ランサムウェア攻撃者は、暗号資産を法定通貨に交換するために、自分たちの拠点外の国・地域にある VASP を利用することが多いが、資金を非ホスト型ウォレットに長期間放置したり、攻撃に関わった第三者への支払いに暗号資産を使用したりすることもある。

26. ランサムウェア攻撃者は、ML のプロセスにおいて、以下のような匿名性を強化する技術、手法、トークンを使用するケースが多い。ランサムウェア攻撃者は、収益を洗浄する際に、毎回同じ要素を利用したり、同じ手順を踏んだりするとは限らない。

- 攻撃者は、被害者からの暗号資産による支払いを、自分が管理するウォレットアドレスに送金するよう要求することが多く、不正な収益を受け取るために攻撃ごとに**異なるウォレットアドレス**を使用することがよくある。
- 攻撃者は、身代金を受け取った後、複数の中間アドレスを使用して、暗号資産を少しずつ複数の新しいアドレスに連続して移転することによって、1 つのウォレットアドレスから暗号資産を移転する。資金は、複数の VASP がホ

ストするウォレットアドレスに送金されることが多い。このような取引パターンは、**ピールチェーン**と呼ばれ、暗号資産の移転を不明瞭化するだけでなく[22]、攻撃者がこのような行動を追跡されにくくするため、少額の取引を繰り返して、多額の暗号資産を洗浄するケースもある。特に、迅速かつ頻繁な取引によって、暗号資産の痕跡を不明瞭化できる。

図 1. ピールチェーンのイメージ図



- ランサムウェア攻撃者は、**ミキサーやタンブラー**（Wasabi など）を通じて暗号資産を洗浄することが多く、これらは、ピールチェーンによる暗号資産の移転に代わるものとして、又はそれに加えて、暗号資産を送信するアドレスと受け取るアドレスとの間のつながりを隠すためにさまざまな手法を用いる。サイバー攻撃者は、複数の資金の送信者と受信者の支払いをまとめて 1 つの集約的な取引を行うコインジョイン取引を利用するケースもある。この場合、JoinMarket のような専用サービスが必要となることが多く、関心を持つユーザーをマッチングして取引をサポートする。
- Bitcoin による支払いを要求するランサムウェア攻撃者が多いが、**匿名性を高めた暗号通貨（AEC、プライバシーコインとも呼ばれる）**も使用される場合がある。各国・地域や業界からの報告によると、AEC は、送受信ウォレットを不明瞭化できるため、ランサムウェア攻撃者への支払いに利用されている。例えば、AEC は、ミキサー、リング署名、ステルスアドレス、リング・コンフィデンシャル・トランザクションなど、送受信ウォレットを不明瞭化し、プライバシー保護を強化する技術を組み合わせて使用できる。Monero のみで支払いを要求するランサムウェア攻撃者も増えているが、身代金支払いに最

[22] ピールチェーンはよく見られる手法であるが、暗号資産ウォレットの設計上、自然に発生する可能性がある。

も多く使われている暗号資産は Bitcoin（99%）[23]である。一部の国・地域では、攻撃者が Bitcoin と Monero の両方で支払いを受け入れた事例が確認されている。ただし、Bitcoin による支払いは追跡が比較的容易なため、攻撃者は身代金の 10～20%の手数料を追加で請求しようとしていた。こうして、サイバー犯罪者は追加料金を支払い、ミキシングサービスなど匿名性を強化する技術を利用して、関係当局による取引の追跡や属性特定を困難にする。

- 複数の国・地域では、攻撃者が VASP や DeFi プロトコル[24]を介して、身代金の支払いを Bitcoin から他の暗号資産に交換するケースが多いことも指摘されている[25]。ある暗号資産から別のブロックチェーンに移動させる手法は、**チェーンホッピング**と呼ばれており、多くの場合、その動きを追跡されないように、連続して行われる。また、ある国では、ランサムウェア攻撃者が、資金を法定通貨に交換する前に、いわゆるステーブルコイン[26]と呼ばれる暗号資産にチェーンホッピングするために、DeFi プロトコルを使用するケースが増えていることが報告されている。ビジネスモデルの状況によっては AML/CFT 義務の対象となる可能性があるにもかかわらず、AML/CFT を実施していない DeFi が多いため、攻撃者にとって DeFi は魅力的なプラットフォームである。ある国では、ランサムウェア攻撃者が、DeFi プロトコルやミキサーを一貫して使用し、時には ML のプロセスで複数回連続使用している事例も報告されている。
- 攻撃者は多くの場合、ML のプロセスで、店頭取引（OTC）トレーダーなどの集中型 VASP を利用して、収益を現金化している。また、リスクの高い地域の VASP や、AML/CFT が脆弱又は存在しない地域の VASP に暗号資産を送り、法定通貨に交換する攻撃者も多い。このような目的のために、リスクの高い地域を拠点とする攻撃者は、米国指定の VASP、Suex[27]、Chatex[28]、Garantex[29]、Bitzlato Limited（Box 6 を参照のこ

---

[23] Coveware「Q3 Ransomware Marketplace Report」（2019 年 11 月）www.coveware.com/blog/q3-ransomware-marketplace-report.

[24] DeFi（分散型金融）とは、スマートコントラクトで提供されるブロックチェーンによる分散型アプリが、VASP が提供するような金融サービスを提供することを指す。FATF 基準は、基礎となるソフトウェアや技術には適用されないため、DeFi アプリ（ソフトウェアプログラム）は FATF 基準では VASP に該当しない。ただし、DeFi を管理、又はその運用に十分な影響力を持つクリエイター、オーナー、オペレーターなどは、VASP のサービスを提供、又は積極的に促進している場合、FATF が定めた VASP の定義に該当する可能性がある。

[25] ランサムウェアの ML に使われるだけでなく、DeFi プロトコル自体、特にクロスチェーンブリッジが、セキュリティギャップを悪用して、暗号資産を窃取しようとするサイバー犯罪者の標的となるケースも増えている。

[26] 用語に関する注意：FATF では、ステーブルコインという用語は、法的にも技術的にも明確なカテゴリーではなく、そのような通貨の推進者が使用するマーケティング用語と見なしている。そのため、本報告書では、推進者の主張を無意識に支持することを避けるために「いわゆるステーブルコイン」と記述している。

[27] 米国 Treasury のプレスリリースを参照のこと。 https://home.treasury.gov/news/press-releases/jy0364

[28] 米国 Treasury のプレスリリースを参照のこと。 https://home.treasury.gov/news/press-releases/jy0471

[29] 米国 Treasury のプレスリリースを参照のこと。 https://home.treasury.gov/news/press-releases/jy0701

と）[30]のように、現地の集中型 VASP を利用できる場合がある。複数の国・地域では、現金化の施設が都市中心部に集中していると報告されている。さまざまなグループのランサムウェア攻撃者が、同じ VASP を利用して、暗号資産の受け取りや洗浄を行っていたケースもある。

- 複数の関係者が関与している場合、攻撃者は通常は犯罪パートナーやインフラの運営者に対価を支払う必要がある。暗号資産による支払いに応じる犯罪インフラの運営者が増えており、ランサムウェア攻撃者は攻撃で得た収益を使用してこれらを支払うことが多い。ブロックチェーン分析会社は、多くのケースで身代金支払いが、悪意のある犯罪者の「サービスとしてのインフラ」運営者に紐付く暗号資産アドレスに直接転用されていることを指摘している。

Box 6. Bitzlato Limited[1]

2023 年 1 月、国際的作戦ではロシアで大規模な事業を展開する暗号資産取引所 Bitzlato Limited が換金型暗号資産（CVC：Convertible Virtual Currency）の洗浄に重要な役割を果たしたと判断した。この作戦は、Europol から支援を受け、ベルギー、キプロス、ポルトガル、スペイン、オランダの当局も関与し、フランスと米国の当局の主導で実施された。Bitzlato は、ロシア関連の RaaS グループ Conti を含むランサムウェア攻撃者の様々な不正取引を促進していると疑われていた。また、米国 Department of Justice は、Bitzlato がランサムウェアの収益として、1500 万ドルを超える資金を受け取ったと主張している。平行して、米国 FIU（Financial Enforcement Network）は、Bitzlato を「マネー・ローンダリングの主要な懸念事項」として認定する命令を発出した。

これらの捜査により、フランスにおけるデジタルインフラと暗号ウォレットの 1800 万ユーロの犯罪資産の差押えを含む取引交換所の解体、及び様々な国・地域の主要な人物の逮捕につながった。

Bitzlato は、ユーザーに最小限の ID しか求めないことを売りにしており、こうした顧客の身元確認（KYC：know-your-customer）の手続きの不備により、犯罪収益や、犯罪活動に利用することを目的とした資金の避難所となったと考えられている。

出典：フランス及び米国

1. フランス National Gendarmerie のプレスリリース www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2023/demantelement-d-une-plateforme-de-cryptomonnaies-servant-au-blanchiment、及び、Europol のプレスリリースを参照のこと。www.europol.europa.eu/media-press/newsroom/news/bitzlato-senior-management-arrested

27. ランサムウェア攻撃者が、VASP にアカウントを持つ**マネーミュール**を利用して、暗号資産を法定通貨に交換できるサービス・プラットフォームであるオフランプ（キャッシュアウトとも呼ばれる）で収益を法定通貨に交換しているケースもある。

[30] 米国 Department of Justice のプレスリリースを参照のこと。www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchange-charged-processing-over-700-million

このようなアカウントは、不正入手された ID や偽の ID を使用して作成される場合や、アカウント使用に加担する関係者が保有する正規のアカウントである場合がある。マネーミュールは、通常、攻撃自体と関連のない第三者であり、ML のプロセスの最終段階に関与し、資金移転全体の中で部分的な役割を担っているが、犯罪組織から切り離され、価値の移転が小規模なため、特定が困難な場合がある。

Box 7 マネーミュール採用の例

ランサムウェア攻撃者はマネーミュール（不正資金の運び屋）を募集・採用し、モバイルデバイスを提供する。マネーミュールの多くは、インターネット上の存在感がなく、インターネットリテラシーも低い。拠点とする国・地域外の匿名メールサービスプロバイダーでメールアカウントを作成し、そのアカウントの利用者が特定されないようにしている。マネーミュールは、犯罪者「ハンドラー」が提供したモバイルデバイスを、オンボーディングプロセス（新規手続き）と金融機関や VASP のアカウント作成に利用する。オンボーディングに成功した後、マネーミュールは、犯罪者「ハンドラー」にデバイスを返却し、犯罪者「ハンドラー」は、マネーミュールに代わって、そのデバイスを使用し、オンライン取引を行う。使用するデバイスの IP（インターネットプロトコル）アドレスを匿名化する VPN（仮想専用通信網）サービスを利用するケースもあり、取引を行う犯罪者の実際の地理的位置は隠されたままとなる。

出典：南アフリカ

第 2 部 ランサムウェアに関連する ML 対策の課題とグッドプラクティス

法的枠組み

28. 強固な法的枠組みは、権限ある当局が効果的なランサムウェアのリスク低減策を策定するための基礎となる。本セクションでは、（i）ランサムウェア関連の ML の犯罪化、（ii）関連する規制対象セクターへの予防措置の適用、に対する FATF 基準の関連性を分析する。

ＭＬの前提犯罪としてのランサムウェア

29. 多くの国・地域では、ランサムウェアに特化した刑事法制は存在しないが、ランサムウェア攻撃を前提犯罪として刑事的に追及できないわけではない[31]。

30. 本プロジェクトによる調査では、各国・地域は、恐喝罪、あるいは、データ損害、侵入、コンピュータープログラムやシステムの損害などのコンピューター関連犯罪として、ランサムウェアの前提犯罪を追及する傾向にある。FATF 勧告 3 では、恐喝関連の犯罪に関わる ML の犯罪化を各国・地域に求めている。恐喝罪は、通常、技術的に中立であるという利点があり、方法や形態にかかわらず、ランサムウェア攻撃を摘発できる。恐喝罪を適用している国・地域は、権限ある当局が不正な暗号資産のフローについて効果的に捜査・財産回復できるように、その法制が適切であることを常に確認するべきである（セクション 6 参照）。

31. 恐喝とは異なり、コンピューター犯罪は、FATF が定める前提犯罪のミニマムリストには含まれていない[32]。しかし、このことが、実際にランサムウェア攻撃関連の ML を追及する上で妨げになるとは考えられない。報告によると、コンピューター犯罪を通じてランサムウェア攻撃者を追及している国・地域は、これらの犯罪を（前提犯罪指定リストに定める方法又は「全犯罪アプローチ（all-crimes approach）」に基づいて）前提犯罪と見なしている。本調査では、ランサムウェアに関連する ML を追及することについて問題を報告する国・地域はなかったが、ランサムウェアに関連する ML の追及の妨げにならないように、前提犯罪を指定するべきである。

関係する者への予防措置の適用

32. FATF 基準は、金融機関、DNFBP、VASP を通じたものも含めて ML を予防するための措置の適用を国・地域に求めている。これらの措置は、FATF 勧告 9～23 に沿って、上記の事業者が ML リスクを理解・低減し、顧客の身元確認を含めて適切な管理策を講じ、疑わしい取引の届出を行うためのものである。

---

[31] ほとんどの国・地域では、被害者がランサムウェア攻撃者に身代金を支払うことを犯罪としていないが、支払わないように強く勧告している国や地域もある。

[32] FATF 勧告用語集に定義されている犯罪の指定カテゴリーを参照のこと。

33. ランサムウェアと暗号資産の関係を考慮すると、2018 年の FATF 基準の改訂によって、FATF 基準が求める措置を VASP に適用したことは、ランサムウェアがもたらすリスクに対する世界の AML/CFT 強化における重要な一歩となった。しかし、2023 年 1 月現在[33]、改訂された基準（勧告 15）に基づき審査を行った 86 の国と地域のうち、63 カ国（73%）は基準が求める義務に対して一部履行又は不履行であると評価され[34]、完全に遵守していると評価されたのは 86 か国・地域のうち 1 カ国だけであった。

34. 改訂勧告 15 に基づき審査を行った国・地域の評価の幅を考慮すると、これらの評価の幅は FATF グローバルネットワーク全体の状況をほぼ反映していると思われる。この審査結果は、2022 年 3 月の FATF 調査で、2022 年時点で暗号資産や VASP に対するライセンス付与や登録制度を設けている国や地域が半数に満たなかったことからも裏付けられる。そのため、ほとんどの国・地域では、顧客の身元確認や疑わしい取引の届出など、VASP に対する AML/CFT 義務の適用に隔たりがある可能性が高い。暗号資産の越境性を考慮すると、グローバルネットワークの各国・地域が勧告 15（トラベルルールを含む）の遵守を迅速に進めることが重要である。

推奨される行動

- 各国・地域は、勧告 15（トラベルルールを含む）を可及的速やかに履行し、VASP に関連する FATF 基準の実施を迅速に進めることによって、VASP が重要な資金情報を取得し、疑わしい取引の届出に関する AML/CFT 義務を確実に遵守するべきである。
- 各国・地域は、FATF 勧告 3 に沿って、ランサムウェア攻撃を ML の前提犯罪（例えば、恐喝の一種）として犯罪化するべきである。

[33] 審査結果のレーティングの統合表を参照のこと。www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html. すべての国・地域が、改訂勧告 15 に基づいて審査が行われているわけではないことに留意すること。

[34] この分析は、改訂勧告 15 に基づいて審査を受けた国・地域の相互審査及びフォローアップ報告に基づくものである。

検知と報告

35. ランサムウェア攻撃者の地理的分散性、ML 手法の利用、現在のランサムウェア攻撃の特徴（本報告書第 1 部を参照）などにより、ランサムウェア攻撃関連の資金移転の規模の推計は困難である。また、ほとんどの国・地域において、ランサムウェア攻撃は過少報告されているため、ランサムウェア関連の金銭的利益や資金移転の全体像を把握することも難しい。

36. 確実な検知と報告は、資金捜査を成功させる基盤となる（セクション 6 参照）。各国・地域のケーススタディなどによると、STR と被害者からの報告が、ランサムウェア関連の資金移転を検知するための主な情報源となっている。本セクションでは、STR 届出の義務、疑わしい取引の特定、被害者からの報告の慫慂などに関連する課題とグッドプラクティスを検証する。

疑わしい取引の届出義務の対象範囲

37. 権限ある当局は、ランサムウェア攻撃の検知や捜査の情報源として、STR を利用することが多い。これまで、ランサムウェア支払いに関連する STR のほとんどは、VASP と銀行から提出されている。

38. 不正なランサムウェア関連の収益を検知するための潜在的な情報源として、通常は AML/CFT の対象外となるセクターを追加的に特定している国・地域も少数ながら存在する。このように AML/CFT 対象外の従来と異なるセクターに対する STR の届出慫慂や要請は、これらのセクターが被害者に代わってランサムウェア攻撃の解決に直接関与している場合には、特に有効であると考えられる。

39. 例えば、より広範囲な保険関連セクター、特にランサムウェアやサイバー保険関連の機関は、サイバー保険に加入している顧客が保険金の支払いを請求するランサムウェア攻撃に関する、直接的な情報を持っている可能性がある。このような組織は、FATF の「金融機関」（生命保険などの投資関連保険の引受・斡旋を行う組織）の定義には当てはまらないが、届出を慫慂・要請することによって、いくつかの国・地域ではランサムウェア関連の報告に関して、前向きな好影響が認められた。

Box 8. ランサムウェア攻撃に関する STR 届出の啓発活動を保険会社に対して実施

損害保険セクターが AML/CFT 義務の対象となっているフランスでは、2021 年に、官民の代表者を集めた専門ワーキンググループによる、同セクターへの啓発活動が実施された。これらのワーキンググループの目的は、サイバーリスクに対する保険引受能力を検証し、サイバー攻撃に対する企業のレジリエンスを強化することにあった。主な成果として、特にランサムウェア関連の ML リスクの動向、AML/CFT 義務と身代金支払いと返還に関連するグッドプラクティスなどを網羅した報告書を公表した。

Prudential Supervision and Resolution Authority（ACPR）が、保険会社に対して、立ち入り検査を含めてさらに個別の監督上の精査を実施した。ACPR は、その後、そのようなサービスを提供する際の AML/CFT 義務について、関連する資金情報（特に支払いの追跡情報）を監視・収集する必要性を含めて、規制対象事業者に注意を促した。

また、保険会社が届け出たランサムウェア攻撃による支払いに関連する STR の数が 2019 年 19 件、2020 年 28 件、2021 年 66 件と増加していることが TRACFIN によって確認された。2021 年の増加の一部は、保険会社 1 社によるものであり、結論や成果を導くにはまだ十分な件数とは言えない。

出典：フランス

1. 詳細はこちらを参照のこと（フランス語）。 www.banque-france.fr/sites/default/files/rapport_45_f.pdf

40. インシデント対応会社も、ランサムウェア攻撃や支払いに関連する情報へのアクセスが可能である。デジタルフォレンジック会社やインシデント対応会社、法律事務所などの組織は、ランサムウェア攻撃の被害者を支援し、身代金額を交渉し、被害者の法定通貨を暗号資産に交換し、攻撃者が管理するアカウントに送金することによって、ランサムウェア攻撃に関連する支払いプロセスを円滑化することもある。このようなセクターからの報告を慫慂又は要請することで、ランサムウェア攻撃の迅速な検知と報告につながる。特に、被害者は、まずインシデント対応会社に（場合によっては法執行機関よりも先に）攻撃について報告する可能性が高いためである。このような会社は、ビジネスモデルや提供しているサービスによって、他の自然人又は法人のために、又はその代理として、暗号資産を他の暗号資産や法定通貨と交換したり、暗号資産を移転したり、暗号資産を保管・管理したりしている場合、VASP の定義に該当し、結果として AML/CFT 及び STR 届出義務の対象となる可能性がある。

Box 9. デジタルフォレンジック&インシデント対応（DFIR）企業の規制

DFIR 企業やサイバー保険会社（CIC）は、サービスを提供する過程で、身代金支払いプロセスを円滑化することによって、被害者を支援することがあるが、状況によっては、これが送金行為に該当する可能性があることが、2020 年と 2021 年の FinCEN（米国の資金情報機関）が発出しているランサムウェアに関するアドバイザリー[1] で明らかにされている。資金送金を営む事業者は、資金サービス事業者として登録する必要があり、AML/CFT 義務の対象となる。同勧告は、DFIR と CIC が疑わしい活動の特定と SAR の届出を支援するためのレッドフラッグ指標、ランサムウェアに関連する支払いについても触れている。

2021 年上半期中に、米国を拠点とする DFIR 企業が提出した届出は、ランサムウェア関連の SAR 届出の約 63%を占めている [2]。2021 年に FinCEN が受理したランサムウェア関連の届出全体も 188%増加した。これらの届出により、FinCEN はパターンやトレンド情報を分析・解明することができ、ランサムウェア攻撃の予防と対策に向けた政府全体の取組みを支援した。例えば、FinCEN の分析によると、2021 年全体で、ランサムウェアは、米国の重要インフラセクター、企業、一般市民に対して深刻な脅威を与え続けていることが明らかになっている。また、同分析から、ロシア関連のランサムウェアの亜種が、報告されたランサムウェア攻撃の大半を占めており、2021 年下半期のランサムウェアによる被害額の 69%、ランサムウェア関連インシデントの 75%を占めていることが明らかになった [3]。

出典：米国

1. 詳細はこちらを参照のこと（フランス語）。 www.banque-france.fr/sites/default/files/rapport_45_f.pdf

2. FinCEN の「Financial Trend Analysis」を参照のこと。www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

3. FinCEN の「Financial Trend Analysis」：www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

41. 上述の事例は、リスクや状況に応じて、これまで対象外だった幅広い事業者に対する届出の慫慂・要請による有用性を示すものである。これにより、異なるセクターの立場から疑わしい金融取引活動が届出・認識され、各情報を関係当局がつなぎ合わせることで、見逃していたはずのインシデントを発見・検知する能力が向上できる。

疑わしい取引の検知を強化するための対策

42. 各国・地域は、業種を問わず、概してランサムウェア関連の STR が過少に届出されている可能性が高いことを認識している。ランサムウェア攻撃グループの地理的分散性、関与する犯罪者の多様性、多様な ML 手法によって、検知が困難になる可能性がある。また、どのセクターも全体像を把握できない可能性がある。

43. 各国・地域は、規制対象事業者による届出の頻度と質を向上し、疑わしい取引をより広範に検知するために、民間セクターの関与、レッドフラッグ指標や検知ガイドの作成・共有など、さまざまな対策を実施している（セクション 8.3 も参照のこと）。

Box 10. Israel Money Laundering and Terror Financing Prohibition Authority（IMPA）によるランサムウェアガイダンス文書

イスラエルの FIU である IMPA は、ランサムウェア関連の支払いの特徴を特定するために、正常ではない資金活動に係る届出を戦略的に分析した。同届出には、攻撃の頻度、標的となった事業者の種類、支払額、使用された暗号資産の種類、第三者の関与に関する情報などが掲載されており、分析結果に基づいて、レッドフラッグやケーススタディを含む、ランサムウェアに焦点を当てたガイダンス文書が発出された。同文書は、IMPA のウェブサイト[1]で公開されており、関連するすべての届出主体に送付され、公式のプレスリリースも公表された。

また、分析結果は、公開フォーラムや専門家会議などさまざまな場で発表された。同文書の発行は、イスラエルのインシデント対応セクターとの連携を促進し、このような関係を拡大し、今後の協力と情報共有の機会を模索する道を切り拓くものとなった。

出典：イスラエル

1. IMPA の公式ウェブサイト（ヘブライ語のみ）
www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typology-ransomware-impa-140222/he/professional-docs_red_flags_typology_ransomware_impa_140222.pdf

44. VASP によって届出されるランサムウェア関連の STR は、身代金要求のために暗号資産が購入された疑いに基づくケースが多い。VASP が依拠する有用な指標には、VASP に対する被害者自身の証言、知名度の高いインシデント対応会社による購入、ブロックチェーン分析を通じて特定される可能性の高いランサムウェアにさらされることに伴う、暗号資産アドレスに直接的又は間接的に紐づけられた支払いなどがある。多くの身代金支払いにおいて、直接的な仲介役としての役割を担う VASP は、ランサムウェア関連の不正な資金移転に関する STR の重要な情報源となる。VASP が依拠する可能性のある関連リスク指標の概要については、”*Countering Ransomware Financing : Potential Risk Indicators*”を参照のこと。

Box 11 危機管理会社の関与

IMPA は、イスラエルの VASP 経由で、危機管理（インシデント対応）会社が、身代金の支払いに使用することを目的とした暗号資産（当時の評価額で数万ドル）を未公表の攻撃被害者に代わって購入したという STR を受理した。
STR によると、追加の暗号通貨も、攻撃の標的と思われる代表者が、同じイスラエルの VASP から独自に購入していた。

IMPA の資金捜査により、資金の大半を受け取ったウォレットアドレスが、他のランサムウェア攻撃に紐づいており、他のアドレスから資金を受け取っていることが判明した。蓄積された資金は、その後、リスクの高い地域を拠点とする VASP に移管された。また、同社が独自に購入した資金は、複数のアドレスを経由し、最終的には大部分がミキサーを通じて送金された。さらに捜査を進めるためのインテリジェンスレポートが、関連法執行機関に共有された。

出典：イスラエル

45. VASP とは異なり、銀行などの金融・決済機関は、被害者が、身代金支払いに関して被害者の代理となる VASP や第三者に法定通貨を送金することを確認した場合、STR を作成・届出できる。しかし、法定通貨ではなく暗号資産が使用されることが多いため、ランサムウェア関連の支払いや ML を直接特定できない可能性もある。そのため、これらの金融・決済機関が把握できる暗号資産のアドレスや資金源に関する情報は非常に限られており、ブロックチェーン分析が困難な場合もある。こうした課題に対処するために、身代金支払いの可能性を特定する代理指標を必要としている事業者が多い。ケーススタディによると、一般的な指標としては、VASP への異常な送金（特に送金元企業が通常仮想資金を扱っていない場合）、サイバーセキュリティ、保険、インシデント対応会社による暗号資産の購入、銀行送金による身代金支払いが要求されているという顧客自身の声明、攻撃を裏付ける公開情報（ニュース発表、インシデント報告など）などが挙げられる。関連するリスク指標については、*"Countering Ransomware Financing : Potential Risk Indicators"*の詳細一覧を参照のこと。

被害者による報告

46. 多くの国・地域では、身代金支払いに関する疑わしい取引の届出率が低いため、STR は検知源として、あるいはランサムウェア攻撃及び関連する ML の全体像を把握して捜査を支援するには、依然として不十分である。よって、被害者による報告も、ランサムウェアに関連する資金移転を検知・捜査するための重要な情報源となっている。法執行機関（LEA）が迅速に対応して資金移転を追跡し、法執行の成果を上げるためには、被害者によるタイムリーな報告が重要である。

47. インシデント報告の義務は国・地域によって異なり、各国・地域の法的枠組みに左右される。多くの場合、インシデントの報告は自発的なものである。被害者が報告を行う場合は、警察かサイバーセキュリティ機関、サイバーインシデント専門の報告部門、又は地域のコンピューター緊急対応チーム（CERT：Computer Emergency Response Teams）に届け出るのが一般的である。

48. しかし、攻撃の報告件数が少ないのと同様に、被害者による報告も限定されている。被害者による自発的なランサムウェア攻撃の報告を阻害する要因は、事業に及ぼし得る潜在的な障害についての認識によってさまざまである。これにはイメージ悪化への懸念や、業務を迅速に復旧したいという願望、ランサムウェア攻撃者からの報復に対する恐れなどが含まれる。ランサムウェアは通常、顧客の個人情報や機密情報への不正なアクセスに関連するものである。LEA や公衆に対してセキュリティ又はデータの喪失を認めるのは、事業に悪影響を及ぼすと考えられ、民事訴訟につながる可能性もある。また、被害者は、LEA に通知すればデータを公開すると攻撃者に脅迫されることもある。

49. さらに、身代金の支払い後には、自発的にインシデントを報告する動機が失われるかもしれない。被害者がサイバー保険に加入している場合、支払った費用は保険会社によって補償されるため、被害者にとっては攻撃を報告する金銭的動機がない可能性がある。一部の国・地域では、国の規制に違反する（認定事業者への支払いなど）、あるいは犯罪グループに加担したと見なされる恐れから、身代金支払い後には報告しない可能性もある。

50. 各国・地域は、被害者が攻撃を報告することを慫慂するため、さまざまな方法を採用している。例えば、一部の国・地域では、ランサムウェア攻撃に対する認識を高めて報告を慫慂するために政策を実施したり、パブリックキャンペーンなどの活動を実施したりしている。こうした政策や活動は民間企業にも関係することが多く、関係当局がランサムウェア攻撃の影響を軽減するためにどのように支援できるのかを浮き彫りにする役割を果たす。これには被害者の財産回復や、入手できる場合はデータを回復するための復号キーの共有が含まれる。

Box 12. No More Ransom[1]

「No More Ransom」ウェブサイトは、オランダ警察の National High Tech Crime Unit、Europol の European Cybercrime Centre、パートナー企業 2 社による取組みで、ランサムウェアの被害者が犯罪者に身代金を支払うことなく暗号データを取り戻す際の支援を目的としている。同ウェブサイトには、さまざまなランサムウェアによってロックされたデータを復号できる鍵やアプリケーションの集積がある。これによって、被害者は身代金を支払うことなく、暗号ファイルやロックされたシステムへのアクセスを回復することができる。

この取組みには、さまざまな国・地域の法執行機関や IT セキュリティ企業など、多数の公共機関や民間企業のパートナーが協力している。目的は、ランサムウェアの仕組みや、効果的な感染防止策についてユーザーを啓発することである。さらに、同ウェブサイトは被害者に身代金を支払わないよう勧告しており、インシデントを報告するための国の報告用ウェブサイトのリンクを掲載している。

出典：No More Ransom

1. 詳細は www.nomoreransom.org/en/index.html を参照のこと。

51. 報告することに伴う評判上のリスクに関する懸念に対処するため、一部の国・地域では、定期的な関与やビジネス会議への参加などを通じて、ランサムウェア攻撃の被害者である企業が評判に傷を付ける恐れなく報告できる安全な環境の創出に努めている。もう 1 つのグッドプラクティスは、専門家のアドバイスと復旧活動のリソースハブとして機能するとともに、被害者がインシデントを報告する単一のソースとなる「ワンストップ」ウェブサイトの作成である。こうした取組みはランサムウェア攻撃そのものの検知に重点を置いていることが多いとはいえ、関連する資金移転や ML の追跡など、資金捜査には被害者による報告から得られる情報が不可欠である。

Box 13. Canadian Centre for Cyber Security

Canadian Centre for Cyber Security（以下「Cyber Centre」）は、カナダの National Cyber Security Strategy の主要イニシアチブとして、2018 年に開設された。Cyber Centre は、政府及び重要インフラの所有者と運営者、民間企業、カナダ国民に向けたサイバーセキュリティに関する専門家のアドバイス、ガイダンス、サービス、サポートを 1 カ所にまとめたソースである。ランサムウェアインシデントの予防・復旧方法に関するガイダンスや、ランサムウェアの脅威動向に関するレポートなどのリソースを個人や企業に提供している。Cyber Centre は、国内外の政府及び民間のステークホルダーから、サイバーインシデントの報告を収集している。報告はオンライン、電子メール、電話によって行われる。Cyber Centre は、サイバーインシデントが生命を脅す差し迫った脅威である場合や犯罪性がある場合には、警察に報告することを慫慂している。

出典：カナダ

52. 一部の国や地域では、重要インフラ（エネルギー、通信、医療など）への攻撃やデータ漏洩など、被害者による報告が必須の産業や事例を特定する取組みを行っている。多くの国・地域では、AML/CFT の義務が適用される金融セクター（銀行など）もこのような産業に含まれる。規制対象事業者は、規制の枠組みの一環として、監督機関などの権限ある当局に重大なインシデントを報告する必要がある。データ保護の枠組みでは、個人情報に関わるデータ漏洩の報告も奨励又は要求される場合があり、これによってタイムリーな検知が可能となる。不正な資金移転の検知を推進するには、このような報告時に、関連する金融情報（ウォレットアドレス、暗号資産の種類など）を収集するのがグッドプラクティスである。

その他の検知源

53. 上述のとおり、金融機関や DNFBP、VASP セクター以外のステークホルダー（インターネットサービスプロバイダーやサイバーセキュリティセクターなど）との情報交換や連携は、有益な情報源となり得る。ただし、これらのセクターには、STR 届出などの AML/CFT 規制の義務が適用されない場合がある。潜在的な利益相反（サイバーセキュリティ企業が被害者の代理となる場合など）により、積極的な届出が阻止される可能性もある。そのような状況では、これらの事業者との官民パートナーシップなどの非公式な手段や、直接の関与によって情報を入手できる場合がある。

Box 14. サイバーセキュリティ企業との連携

ある被害を受けた企業は、ランサムウェアグループの攻撃を受けた後にサイバーセキュリティ企業と契約を結んだ。身代金は Bitcoin か Monero のいずれかで支払うことを要求された。被害者は結局、サイバーセキュリティ企業を通じて犯罪グループに身代金を支払った。

サイバーセキュリティ企業はその後、法執行機関にこのインシデントについて通知し、それによって関係当局は不正な資金移転を追跡することができた。法執行機関は頻繁にサイバーセキュリティ企業と連携している。こうした連携は、サイバーセキュリティ企業が最小限の介入でクライアントの回復作業を実行できることを目的としているが、これによって IP や暗号アドレスなどの重要な要素が犯罪捜査に提供される。

この例では、法執行機関はミキサーなどの匿名化の手法や、大量の非ホスト型ウォレットアドレスの使用を確認した。捜査時に資産のかなりの部分が非ホスト型のウォレットに保管され、それ以上追跡できなくなった。資金のかなりの部分が国外の VASP 2 社を通じて流出したと報告されている。

出典：スイス

54. 権限ある当局は、ランサムウェアに関連しているとみられるウォレットに対するブロックチェーン分析を用いた独自の資金捜査によっても、ランサムウェアの攻撃と支払いを検知する。これにはブロックチェーン分析企業によって共有された既知の攻撃、ブログ、オープンソース分析の監視と、分析後の潜在的被害者との事前接触も含まれる。

55. こうした取組みにより、過去のランサムウェア攻撃の新たな手がかりが判明する可能性がある。また、ランサムウェア犯罪に起因する攻撃の規模や、犯罪者が不正収益を洗浄・受領・使用するために利用する傾向や類型、インフラに関する知見が明らかになる場合もある。

Box 15. オープンソース分析による RaaS 犯罪者の検知

トルコの FIU は、VASP により「Name 1」として登録されている人物にリンクされた暗号資産のウォレットアドレスに関して、VASP から STR を受けた。この名前をオンライン検索したところ、同名のウェブサイトが見つかった。さらなる捜査により、このウェブサイトはダークネットに関連する活動を行っており、ランサムウェアソフトウェア、その他の悪意のあるソフトウェアの販売の仲介となっていることが判明した。

オープンソースを介したさらなる分析の結果、以下が判明した。

- この人物は別のニックネーム（「Name 2」）を使用して、STR で言及されている取引に関わっていた。これによってこの人物の本名が特定された（「人物 X」）。この人物は以前に、Police Department's Anti-Cyber Crime Branch が捜査対象としていた容疑者であった。
- 容疑者（人物 X）は、不正アクセス、秘密情報へのアクセス、偽の ID 認証情報、ソーシャルメディアアカウントのハッキング、ハッキングリンクやフィッシングページの販売などのサービスや製品を提供していた。
- こうした違法な製品やサービスへの支払いは、Bitcoin やその他の暗号資産によって行われていた。

トルコの FIU はその後、STR に記載されているこの人物に関連するさらなる情報、特に暗号資産のウォレットアドレス、（暗号資産と法定通貨の）金融取引、その他の個人情報の提供を VASP に要請した。STR に記載されている人物はランサムウェアやその他の悪意のあるソフトウェアの販売を仲介している疑いがあるとして、分析レポートが作成され、トルコ警察の Cyber Crime Departments に提出された。捜査は現在も継続中である。

出典：トルコ

56. 各国・地域は、他の国・地域によって共有される情報を通じて、ランサムウェアの攻撃と支払いへの注意を喚起されることもある。国際協力や司法共助、他国・地域との非公式な情報交換により、他国・地域の攻撃や被害者に関連した資金に関する情報で、国内当局間の情報交換を通じて重層化された情報が得られる場合がある。

推奨される行動

- 各国・地域は、傾向や検知ガイド、レッドフラッグ指標（*"Countering Ransomware Financing : Potential Risk Indicators"*に含まれているような情報）を関連する報告主体の事業者と共有するなどして、規制対象事業者がランサムウェアや関連する ML を検知し、疑わしい取引を届出できるよう支援するべきである。
- 各国・地域は、利用可能な支援やリソースについての啓発や、安全な報告経路の構築などにより、被害者による自発的なインシデントの報告を慫慂するべきである。
- 各国・地域は、検知源を増やすために、AML/CFT 義務が適用されない可能性のある従来と異なる組織（サイバー保険会社やインシデント対応会社など）とのコミュケーション経路の構築を検討するべきである。

資金捜査のための戦略

57. 大抵のランサムウェア攻撃は、収益を獲得することを目的としている。多くの国・地域は、ランサムウェアの捜査に大きな金融的要素があることを認識している。ケーススタディによって、暗号資産の追跡がランサムウェア捜査の柱であることが分かっている。ランサムウェア攻撃の捜査を公表している国・地域では、身代金支払いを追跡する資金捜査が並行して実施されている場合が多い。

58. ランサムウェアに関連する ML の捜査においては、世界的に経験不足が見られる。ランサムウェアの事例において、ML が告発された国・地域はほとんどない。これは、一つにはセクション 5 で見たような検知と報告の課題が影響している。

59. 本セクションでは、(i) 被害者との連携による情報の入手、(ii) 捜査技術と方法、(iii) 財産回復など、ランサムウェア及び関連する ML の資金捜査を成功させるための具体的な課題とグッドプラクティスを検討する。

迅速な対応と被害者との連携による情報の入手

60. ランサムウェアのようなサイバー犯罪の性質を考えると、法執行の成果は、迅速に対応し、ランサムウェアの攻撃と支払いに関する重要情報を収集できるかどうかにかかっている。この情報には、暗号資産アドレス、身代金総額と使用された暗号資産の種類、取引日、関連するサービスの種類、被害者の身元、被害者とランサムウェア犯罪者間の通信、身代金支払いに関わった第三者が含まれる。

61. 多くの場合、このような情報の収集には被害者、あるいはインシデント対応や身代金支払いプロセスに関わった第三者の協力が必要となる。しかし、前述したように、被害者は法執行機関へのインシデントの報告に消極的な場合がある（セクション 5.3 参照）。また、法執行機関との利益相反のために協力を渋る場合や、一刻も早く業務を再開したいために身代金の支払いを選択する場合もある。法執行機関と関わることによって攻撃者から報復を受けるのを恐れている場合もある。一方、法執行機関はフォレンジックな証拠を確保し、統制された

実務を行えるよう整え、また、他の捜査手順を踏むために時間を要することにより、業務の再開が遅れる可能性がある。

62. 報告が遅かったり、不十分だったりする場合や、被害者の協力が得られない場合には、捜査を円滑に進めるために利用できる情報の質が損なわれる。被害者が攻撃を受けた後や支払いを行った後の明確な行動計画がなければ、データが保存されず、十分な証拠が入手できなくなる可能性がある。セクション 5.3 で言及したパブリックキャンペーンや、その他の被害者の関与を慫慂する取組みなどのグッドプラクティスは、こうした課題を軽減する上で重要である。

63. 一部の国・地域では、サイバー（前提犯罪）捜査官と ML 捜査官の間で情報を共有することがますます重要になっている。ランサムウェア前提犯罪捜査のフォレンジックな証拠を収集する中で、法執行機関は必然的に ML 捜査に関連する情報を収集することになる。このような情報により、法執行機関はさまざまなグループとランサムウェア攻撃提携者との関係を把握し、より広範な資金捜査を支援する追跡の手がかりを得ることができる。どうすれば国内の様々な権限ある当局が効果的に協力できるのかについての詳細は、セクション 8.2 を参照のこと。

Box 16. 前提犯罪捜査時に得られた資金捜査の関連証拠源

フォレンジックな証拠：フォレンジックな証拠には、攻撃ベクトル（攻撃者が不正アクセスを実現した方法）、ランサムウェア、IP アドレス、使用された名前又はニックネーム、攻撃者の使用デバイスなどがある。このような情報は、被害者、インターネットサービスプロバイダー、サイバーセキュリティ及びインシデント対応企業から直接収集することや、フォレンジックテクノロジーの利用によって収集することができる。

民間セクターからの直接的証拠：関連する民間企業として、ランサムウェア攻撃に悪用された技術やインフラを所有する企業がある。捜査官は、攻撃者が被害者との通信用にアカウントを所有している電子メール又はソーシャルメディア企業から、登録者の情報を入手できる場合がある。

オープンソースの情報：ソーシャルメディア、オンラインフォーラム、ダークネット市場、ランサムウェア攻撃者による通信などのオープンソースの情報の調査は、潜在的攻撃者を特定するのに役立つ。

捜査技術・メカニズム

従来の捜査技術の関連性

64. ランサムウェア攻撃者は、居場所や身元、資金移転を隠すために技術を使用して捜査を妨げる場合がある。特に注目すべき課題として、VPN、「The Onion Router」[35]、暗号化された電子メールなどの使用によるプライバシーとセキュリティの強化、トラフィックがネットワークを通過する際のアクティビティの匿名化などがある。こうした課題は、技術進化のスピードによってさらに複雑化する可能性がある。

65. FATF 勧告 31 は、効果的な資金捜査に必要な権限を LEA に提供するための基盤となるものである。こうした従来の捜査技術は、上記の課題を克服して、ランサムウェアの資金移転に関する重要情報を収集・分析できるようにする上で、依然として有用である。監視、通信の傍受、おとり捜査などがこうした技術に含まれる。ただし、これら従来の技術は、暗号資産に関わる資金捜査の状況に合わせる必要がある。捜査を成功させるための実施例として、以下のようなものがある。

- *監視*：容疑者が使用している電子デバイスの種類を特定して、使用されているウォレットや電子通信の方法を突き止めること。
- *通信傍受とおとり捜査*：対象の行動や犯罪組織の活動実態を明らかにし、対象に関係する人物及び関連する金融情報と資産を特定し、犯罪者のコミュニティ（ダークネットフォーラムなど）に潜入して最終的な犯人及び受益者の身元を暴くこと。
- *提出命令：*VASP や、身代金支払いに関与したその他の金融機関から情報を入手すること。

66. 資金捜査において上記の手段を利用する場合は、STR 又は被害者による報告によって、さらに詳しい情報が得られる（セクション 5 参照）。法執行機関は、STR やブロックチェーン分析（セクション 6.2.2 参照）を通じて関連する金融機関や VASP を特定し、提出命令により必要な証拠を入手できる場合がある。ランサムウェアに関連する資金捜査を支援する有用な ID 情報が VASP から提供され、基本情報、実質的支配者及び取引に関する情報（ユーザーID 及び関連情報、IP アドレス、クレジットカードまたは銀行口座など）が得られる場合がある。

67. しかし、セクション 3 で見たように、一部のランサムウェアネットワークは、VASP の AML/CFT 義務が脆弱又は存在しない、あるいは義務を遵守できていない VASP が多い、リスクの高い国・地域ともつながっている。資金がこのような VASP 経由で移転されるか、VASP に保管されれば、捜査が複雑になる恐れがある。このような場合、VASP は関連する情報をまったく収集しないか、法執行機関の要求に反応しない可能性がある。

68. 攻撃者が非ホスト型ウォレットを使用している場合も、捜査官は同様の課題に直面する。これは、VASP が関与することなくユーザーが暗号資産を管理する

[35] 別名 TOR。ユーザーが匿名でネットサーフィンできるようにするオープンソースソフトウェア。

ことができるもので、ML 活動の検知・防止が困難になる。第三者機関（及び FATF 基準に基づき登録・認可された機関）とのつながりがなければ、情報を要請する外部関係者が存在せず、関係当局がウォレットの所有者を特定することが難しくなる可能性がある。

69. VASP による FATF「トラベルルール」の実施が限定的な場合も、サイバー犯罪者が検知を避けて捜査を妨害する機会となる。トラベルルールは、VASP や暗号資産取引に関わるその他の金融機関に、送金の送り手（発信者）と受け手（受益者）の情報提供を要求するものである。これによって取引の透明性を高めて犯罪者による悪用を防止し、法執行機関が情報を入手して取引の関係者を特定できるようにする。しかし、2022 年の FATF レポートによると、VASP に対するトラベルルールの義務を求める法整備を行った国・地域はわずか 3 分の 1 のみであり、これらの義務を実際に施行しているのはさらに少数である[36]。一貫した規制がないことで、トラベルルールが義務化されていない国・地域において法執行機関が VASP から入手できる情報量が減少する。また、FATF 勧告の不遵守国・地域の VASP と取引を行っている遵守国・地域の VASP は情報を入手できる可能性が低いため、トラベルルールが施行されている国・地域であっても、捜査官が入手できる情報が限定される。

[36] FATF（2022 年 6 月）*Targeted Update on Implementation of the FATF Standards on Virtual Assets And Virtual Asset Service Providers*。実施対象の改訂は、2021 年 6 月から 2022 年 5 月までに MER/FUR が発行された国のみを対象としている。

Box 17. ランサムウェアグループに対する従来型の資金捜査技術

イタリアのある被害を受けた企業は、Bitcoin での身代金支払い後に警察に通報し、ランサムウェアに感染したデータの解除に成功した。支払いは、身代金要求で言及された VASP を通じて行われた。

警察の捜査により、この VASP のウェブサイトはイタリアで正式登録されていることが判明した。その後、イタリア人の容疑者が特定され、身代金の支払いに関連する Bitcoin の移転を支援していたことが明らかになった。警察はこの人物の住居を捜索して、支払い用カードや携帯電話、さらにハードディスクや USB ドライブ、タブレットなどのハードウェアを押収した。電話の盗聴と、携帯電話でやり取りされたメッセージの分析により、ランサムウェアに関連する Bitcoin の移転を支援する上で同様の役割を果たしたイタリア人容疑者のグループ（以下「同グループ」）が割り出された。資金捜査により、ランサムウェア被害者が送金した法定通貨建て資金は、同グループによって、リスクの高い国・地域を含む外国の VASP が保有する外国の銀行口座に移転されたことが判明した。

関係当局は、資金捜査及び電話やハードウェアのフォレンジック分析に基づき、同グループがランサムウェアを被害者に拡散し、攻撃ごとに数百ユーロの身代金を要求したとの判断を下した。同グループはランサムウェアに関連する恐喝とその後の資金洗浄の罪で起訴された。複数の被害者の身代金総額は約 30 万ユーロに達するとみられる。捜査は現在も継続中である。

出典：イタリア

暗号資産特有の技術

70. 法執行機関は、従来の技術に加え、暗号資産特有の技術を利用して、ランサムウェアに関連する資金捜査を実施するべきである。暗号資産の大半はパブリックブロックチェーンで運用される。これは、オープンソース又はサブスクリプション型のブロックチェーン分析ツールを使用して暗号資産取引に関連する匿名の情報を追跡できる、閲覧可能なデータベースとなる（セクション 7 参照）。ブロックチェーン分析と従来の捜査技術を組み合わせることで、捜査官はオンラインのランサムウェア攻撃者とその提携者を特定し、不正な資金の動きを追跡するのに必要な情報を得ることができる。

71. ブロックチェーン分析を用いて資金を追跡するには、最初のウォレットアドレスを特定する必要がある。これは、身代金支払情報の検知と収集の重要な第一歩となる。最初のウォレットアドレスが入手できれば、捜査官は当該ウォレットアドレスで入出金される支払いを特定することなどが可能となる。ただし、入手可能な情報は利用しているサービスによって異なる。パブリックブロックチェーンには資金捜査に役立つ情報が含まれるが、暗号資産の取引にはオフチェーンで発生するものもある。さらに一部のブロックチェーン分析では、クラスタ化アルゴリズムやその他の技術を利用して、ウォレットアドレスや、ランサムウェアなどの犯罪に関連する取引を分類する。

72. 従来の捜査技術を使用する場合は、ブロックチェーン分析からさらに詳しい情報を得ることができる。例えば、ブロックチェーン分析によって、ランサムウェア攻撃者を受け手・送り手とする支払い取引が実施されたウォレットアドレスをホストする VASP を特定できる。これによって LEA は、強制的な手段を使い、当該 VASP にウォレットアドレスに関する情報を要求することができる。

Box 18. 既知のランサムウェアウォレットの捜査による、さらなる被害者の判明

2017 年 5 月 12 日から 2021 年 5 月 27 日までに約 20 Bitcoin を受領した Bitcoin アドレスに関連する、ブロックチェーン脅威のオンライン分析が継続されてきた。当該 Bitcoin アドレスは、南アフリカの複数の事業者や政府機関が感染したランサムウェアと直接関係している可能性があることが判明した。分析により、2018 年 2 月に南アフリカのある VASP が所有する個別のローカル Bitcoin アドレスから、前述した捜査中のアドレスに 0.06 Bitcoin が提供されたことが明らかになった。

VASP から登録者の情報を入手した後、被害者が特定され、被害者は金銭的な損失を受けたことを認めた。被害者は、顧客データの保護が不十分だったことが公になるのを恐れて、地域の捜査当局にインシデントを報告することを望まなかった。この事例は、南アフリカの FIU によって地域の捜査当局に委ねられた。被害者が刑事告訴を望まなかったため、本事例は不起訴となり、地域の法執行機関によって終了となった。

出典：南アフリカ

73. ランサムウェア攻撃者が使用する匿名性を強化したローンダリング方法（セクション 3 参照）は、一部のブロックチェーン分析企業がそうした匿名性を軽減する技術を開発しているとはいえ、法執行機関がブロックチェーン分析を用いて取引を追跡・特定するのを困難にするものである。アフィリエイトモデルや RaaS プロバイダー、マネーミュールの関与などにより、ランサムウェアに関連する資金捜査がより困難になる。常に被害者まで支払いを追跡できるとは限らないため、ブロックチェーン分析の手がかりとなることの多い、暗号資産の最初の支払いに使用されたアドレスを特定するのが難しくなる。

74. 捜査官は、ブロックチェーン分析をランサムウェア攻撃からローンダリングまでの支払いの追跡に利用するだけでなく、ランサムウェアグループに関連する事前取引の追跡にも利用する必要がある。この追加の手順により、法執行機関は潜在的傾向や類型、新たな犯罪を特定することができる。

75. グッドプラクティスとして、一部の国・地域の法執行機関は、ランサムウェア事例に関連するミュールやウォレットアドレスに関する重要情報のデータベースを構築している。

このようなデータベースには一般に、インシデント、ミュールの身元情報、被害額、ランサムウェア攻撃者に関するデータ（口座番号、ウォレットアドレス、ユーザー名など）が含まれる。このデータベースは、事前の捜査で得られた手がかり（支払い情報など）と既存及び将来のインシデントを照合する集積データを提供して、身代金支払いとそれに関連する ML の特定・追跡を支援する。これにより、法執行機関はさまざまな規制対象事業者やセクターにおよぶ広範なローンダリングネットワークを把握することができる。

財産回復

76. 法執行機関は、検知及び資金捜査の能力を強化することに加えて、暗号資産を差押え・没収するための立法権限及び能力を有していなければならない。暗号資産の取引は、ほぼ瞬間的なものである。つまり、権限ある当局は、ランサムウェアの攻撃と身代金支払いを認識し次第、速やかに身代金支払いを追跡し、理想的には数時間以内に凍結の権限を利用して、散逸を防止できなければならない。FATF 勧告 4 に従い、このような権限は、形はさまざまであっても、多くの国・地域にすでに存在しているはずである。

77. いくつかの国・地域では、STR で特定された疑わしい犯罪資産に対処する上で、FIU による停止・延期の権限など、不正な資産を阻止する手段の有用性が浮き彫りになっている。暗号資産の進化に遅れずについていくため、既存の資産の没収に関する法規制やポリシー、手続きの最新化を検討することも必要であろう。

Box 19. Colonial Pipeline

2021 年 6 月、米国 Department of Justice は約 230 万ドル相当の 63.7 Bitcoin を押収したと発表した。これらの資金は、2021 年 5 月 8 日に DarkSide と呼ばれるグループのメンバーに支払われた身代金だとされている。これは、Colonial Pipeline を標的とした攻撃で、重要インフラが操業停止に追い込まれた。押収令状は、同日のそれまでの時間に、カリフォルニアの判事によって承認されたものである。

2021 年 5 月 7 日頃、Colonial Pipeline はランサムウェア攻撃の被害を受け、同社インフラの一部が操業を停止した。この事件は大きく報道された。Colonial Pipeline が Federal Bureau of Investigation に報告したところでは、同社のコンピューターネットワークに DarkSide と名乗る組織によるアクセスがあり、約 75 Bitcoin の身代金を要求されて、同社はこれを支払った。裏付けとなる宣誓供述書によると、法執行機関は、Bitcoin の公開台帳を確認して複数の Bitcoin 取引を追跡し、被害者が支払った身代金の収益である約 63.7 Bitcoin が特定のアドレスに移転されていたことを突き止めた。この Bitcoin は、コンピューター侵害による収益及び ML に関連する資産に相当するもので、刑事・民事没収法に従って押収される可能性がある。

出典：米国

推奨される行動

- 権限ある当局は必要に応じて、従来の法執行技術と暗号資産特有の技術を使用して、ランサムウェアに関連する ML の捜査を実施するべきである。
- 各国・地域は、法執行機関が特に暗号資産に関して、迅速かつ効果的に資産を差押え・没収するために必要な能力と権限を有し、これを維持するようにするべきである。

スキル・専門知識

78. セクション 6.2 で述べたとおり、ランサムウェアに関連する ML の捜査には従来の法執行技術も依然として重要であるが、暗号資産に関連する ML の捜査と起訴を成功させて財産回復を図るには、技術的な専門知識も必要である。これには暗号資産エコシステムの技術的・法的知識が含まれる。

79. さらに、ランサムウェアに関連する ML 事例や財産回復に従事する捜査チームには、サイバーセキュリティ、コンピューターフォレンジック、オンラインインテリジェンス、オープンソースプラットフォームの技術スキルを持つメンバーが含まれているべきである。これには、ブロックチェーン分析によって特定される情報や、ウェブサイト、ソーシャルメディア、オンラインフォーラム、ダークネット、ダークマーケットのスキャン、及びオンライン不正レポートにより特定される情報など、パブリックドメイン内の暗号資産取引に関する金融情報を収集するためのオンライン調査の取組みが含まれるべきである。

80. 特に暗号資産が関連する場合には、権限ある当局は情報を入手して解釈する新たなスキルと専門知識が必要となる。具体的には、関係当局は、パブリックブロックチェーンを表示するフリーソフトウェアなどのブロックチェーン分析ツールや、資金を追跡するための分析の利用など、ブロックチェーン分析及び監視機能を熟知していなければならない。さらに、各種ツールがさまざまな無料の機能（各種の暗号資産の分析、チェーンホッピングの分析機能、オープンソースインテリジェンスなど）を提供している。

81. 捜査時にこうしたさまざまなツールを開発して使用するには、専門的なトレーニングと専門知識が必要であり、一部の国・地域では関連する捜査に専門家を組み込む手だてを見つけている（セクション 8.2 参照）。必要なリソースの入手には費用がかかり、国・地域によってはこうしたスキルの開発支援に必要なリソースが不足しているため、関係当局がランサムウェアに関連する ML を追跡する能力が制限される可能性がある。

82. 組織内に専門家が存在しない、あるいは不足している場合には、国・地域は民間企業が作成したツールの使用を検討してもよい。サードパーティツールは、重大なものから些細なものまで、あらゆる暗号資産ブロックチェーンでの暗号資産取引を関係当局が特定・追跡・属性識別することを助ける。現在、こうしたツールは何百ものトークンをサポートしており、クラスタリングアルゴリズム、Web スクレイピング、詐欺データベースの監視などの方法により、捜査官が広範囲の取引を実在の人物や組織と結び付けて属性を識別することを可能にしている。これらのツールは、取引のグラフを生成してネットワーク分析を可

能にする。これによって関係機関は複雑なつながりを理解し、その後の起訴及び財産回復対応において陪審員・裁判官に提示することができる。これらのツールは、不正な資金を洗浄又は法定通貨に換金するのに使用され、捜査をサポートする関連情報を所有している可能性のある VASP を関係当局が特定するのに役立つ場合もある。

83. 財産回復については、暗号資産の差押えと管理には、さらなる技術的・法的知識が必要である。関係当局は、適切な手続きを実施し差押えと保管が正しく行われるように、体制を整えなければならない。暗号資産の差押え・没収・処分の専用メカニズムを構築することがグッドプラクティスである。これには適切な差押えに関する計画、シードフレーズ[37]の管理、差押えられた暗号資産の凍結（オフラインの非ホスト型ウォレットに保管）、証拠保全の一貫性などの課題が含まれる。

推奨される行動

- 権限ある当局には、ランサムウェア関連の資金捜査に必要となる専門的な技能や知識が求められており、ブロックチェーン分析や監視ツールに関する開発、アクセス、トレーニングの実施をするべきである。
- 各国・地域は、差押えした暗号資産を適切に管理する特別なメカニズムを整備するべきである。

国の政策と協調

国のリスク評価と戦略

84. FATF 勧告 1 は、各国・地域がそれぞれの ML リスクを特定・評価し、リスクベース・アプローチを適用してそれらのリスクを低減することを求めている。このアプローチは、国・地域が AML/CFT 制度にリソースを十分に割り当てるための基盤にもなる。

85. ランサムウェアは、セイバーセキュリティ脅威の評価の観点から対処される場合も多い。例えば、一部の国では、セイバーセキュリティ又はサイバー犯罪に関する国家戦略を策定し、国内の協調を支援して政治的関与を強め、ランサムウェア及び関連する不正な資金移転を積極的に追跡している。国家戦略には一般にさまざまな政府機関[38]が関与している。法務省、財務省、内務省などの関連 AML/CFT 当局及び民間セクターがこれに含まれる。ただし、これらの戦略の目的は多くは、必ずしも不正資金のリスクを重視していないことに留意が必要である。不正資金のリスクはリスク評価を通じて詳細に検討するべきである。

[37] ウォレットアプリケーションによって無作為に作成され、特定の順序でリスト化される単語の組み合わせ。別の保護（パスワードなど）をバイパスしてプライベートキーへのアクセスを回復または取得するために使用される。

[38] ランサムウェアによる国家安全の脅威を考慮し、これらの機関には、法執行、防衛、セキュリティ、情報通信に特化した機関が含まれる。

Box 20. National Cybersecurity Strategy of Spain

National Cybersecurity Strategy of Spain（2019 年更新）は、サイバー脅威と闘うためのスキルの強化を目的としている。ネットワーク及び情報システムの高度なセキュリティを実現・維持するための優先事項、目標、適切な対策が定められている。同戦略の主な行動方針は、サイバー脅威と闘うスキルを強化して、サイバー犯罪を捜査・起訴する能力を向上させることを目指すものである。

同戦略により、管轄組織に十分なリソースを割り当てて、専門スキルのトレーニングを実施し、法と警察の連携を強化する必要性が明らかになった。これがサイバーセキュリティの制度的枠組みの構築にもつながり、National Cybersecurity Council が設立された。同会議はスペイン首相が主導するもので、サイバーセキュリティに関する国家のセキュリティポリシーをまとめ、行政機関[1]と民間セクター[2]との協調、連携、協力を促進して、それぞれが適切な役割を果たし、複合領域的なアプローチを実現することを目的としている。

出典：スペイン

1. Ministries of Foreign Affairs, Justice, Defense, Home Affairs, Treasury, Presidency; National Intelligence Centre, National Security Department など。

2. 民間の専門家には、職能団体や企業、学術研究機関の専門家が含まれる。

86. 国・地域は、FATF 勧告 1 に従った国の ML リスク評価の一環として、ランサムウェアによる脅威も検討するべきである。この評価は、本レポートに記載の推奨される行動の実施など、国・地域がリスク低減策を作成するための基盤を提供するものである。ランサムウェアに関連する ML リスクを把握することにより、国・地域はリスクベース・アプローチに従って、関連する AML/CFT 当局向けの暗号資産の専門スキルや専門知識の育成や、ブロックチェーン分析ツールの取得などにリソースを割り当てることができる。

87. 今のところランサムウェア及び関連する ML が国内の重大な脅威となっていない国・地域も、ランサムウェア、特にランサムウェアと暗号資産の独特の関係による不正資金リスクについて検討するべきである。各国・地域は国内の被害者へのランサムウェア攻撃の脅威だけでなく、ランサムウェア犯罪者が自国・地域を拠点とする可能性や、自国・地域の VASP がランサムウェア収益の洗浄や現金化に利用される可能性も考慮するべきである。例えば、多くの VASP は、ある国・地域で登録して従業員を別の国・地域に配置し、異なる国・地域に技術インフラや秘密鍵を所有するなど、複数の国・地域にまたがる分散的な構造をとっている。つまり、このような国・地域は、特に VASP セクターを通じて、ランサムウェアに関連する不正な資金移転に巻き込まれる可能性がある。

Box 21 国の ML リスク評価におけるランサムウェアの評価

2022 年 3 月、米国は National Money Laundering Risk Assessment（NMLRA）第 3 版を発行した。この評価書では、サイバー犯罪、及び暗号資産に関連する脆弱性を含む、最も重大な不正資金の脅威が取り上げられている。NMLRA は、サイバー犯罪が 2018 年以降大幅に増加しており、ランサムウェアは特に重大な不正資金の脅威となっていると指摘している。例えば、新型コロナウイルス感染症のパンデミックを通じて、ランサムウェア攻撃の重大性と巧妙さが増したとされている。NMLRA は、RaaS モデルや二重脅迫型のランサムウェアの利用など、ランサムウェア攻撃の傾向に関して意義ある情報を提供している。また、ランサムウェア関連の預金に AML/CFT の管理が脆弱又は存在しない外国の VASP が利用されていることなど、多くの ML の類型も取り上げている。NMLRA の調査結果は、不正資金リスクに対処するための推奨事項を提供する、United States 2022 National Strategy for Combatting Terrorist and Other Illicit Finance 及び the Action Plan to Address Illicit Financing Risks of Digital Assets で参照されている。

出典：米国

国内の協力・協調

88. FATF 勧告 2 は、国・地域が政策立案者、FIU、LEA、その他の権限ある当局が協力・協調し、情報を交換するための国内メカニズムを構築することを求めている。ランサムウェアは広範な地域にまたがり、サイバーセキュリティ機関やデータ保護機関など、従来の AML/CFT 当局以外の関係者が関与する場合がある。関連情報、及び民間セクターも含めた広範な専門家を集めて包括的な対応を実施し、ランサムウェア及び関連する ML による脅威を低減するには、効果的な国内の協調メカニズムが不可欠である。これによって、フォレンジックな前提犯罪捜査と、並行する資金捜査を実施する執行機関の間で、重要な情報を交換することが可能となる。

89. グッドプラクティスは、サイバー犯罪専門（あるいはランサムウェア専門）の法執行チーム、又は分野横断組織を構築することである。これらの組織は、広範な専門知識（FIU 又は LEA 専門家、検事、テクニカルエンジニア、ネゴシエーターなど）を必要とするランサムウェア及び関連する ML の捜査を、協力して実施することができる。このアプローチには、一般に暗号資産追跡の専門知識を持つ法執行機関の当局者が含まれ、特にリソースや能力が限られている場合には、技術的な専門知識を一元化するのに有効な手段となり得る。

Box 22 インテリジェンスと捜査の専門知識を一元化する協調メカニズム

進化するサイバー問題に対応するため、米国政府は 2008 年に National Cyber Investigative Joint Task Force（NCIJTF）を設立した。NCIJTF は、法執行機関、情報機関、Department of Defence の 30 を超える連携機関で構成されており、代表者は政府全体の観点から、同じ場所で任務遂行に向けて協働している。

比類のない複数機関からなるサイバーセンターである NCIJTF の第一の責務は、情報を整理・統合して共有することによりサイバー脅威の捜査を支援し、機関の政策決定者向けに情報分析の提供・支援を行い、国家に対するサイバー脅威と闘う上での他の継続的取組みに価値を提供することである。

2014 年末、NCIJTF はサイバー犯罪に関連する暗号通貨取引の追跡に注力する Virtual Currency Team（VCT）を立ち上げた。同チームは、NCIJTF のすべてのメンバーに対して暗号通貨の追跡を提供している。Federal Bureau of Investigation（FBI）や米国 Secret Service（USSS）などの NCIJTF メンバーは、さまざまな犯罪において暗号資産の使用が増加しているのに伴い、捜査活動の一環として、暗号資産を追跡するチームをそれぞれ設立した。

2022 年初頭、FBI は暗号通貨プログラムの中枢となる Virtual Assets Unit（VAU）を設置し、他部門に情報、技術、運用サポートを提供している。VAU では、暗号資産の専門家及び部門をまたがるリソースがタスクフォースに従事し、FBI 全体で情報とオペレーションをシームレスに統合している。

出典：米国

民間セクターとの連携とガイダンス

90. セクション 5.2 で述べたように、本レポートに記載されている一部の課題を低減するには、民間セクターとの連携が有効である。例えば、規制対象事業者は、ランサムウェアに関連する疑わしい取引を検知・特定するのが難しい場合がある。一部の国・地域は、報告事業者と関与し、レッドフラッグ指標（*Countering Ransomware Financing : Potential Risk Indicators, FATF, 2023* 参照）や検知ガイドなどのガイダンスを提供することによって、ランサムウェアに関連する STR 届出の頻度と質を向上させることに成功している。

Box 23. オーストラリアの金融犯罪ガイド

オーストラリアの Fintel Alliance[1] は、企業が疑わしい金融活動の把握・検知・届出を支援し、犯罪活動を検知・防止できるように、金融犯罪ガイドなど広範なリソースを発行している。

金融犯罪ガイドは、さまざまな犯罪の金融に関する詳細な情報を提供している。このガイドには、金融サービスセクターが疑わしい取引を特定・検知するのをサポートするケーススタディや指標が記載されている。

ランサムウェアとの闘いを支援するため、AUSTRAC は 2022 年 4 月に、デジタル通貨の不正使用と、ランサムウェアの検知・阻止に焦点を当てた金融犯罪ガイドを発行した。これら 2 つのガイドには、身代金支払いの標的にされそうな場合や、身代金支払いから利益を得ようとする試みを検知・対応するのに役立つ実用的な情報と重要リスク指標が記載されている。これらの金融犯罪ガイドは、以下の AUSTRAC ウェブサイトで入手できる。

- Detecting and stopping ransomware payments （身代金支払いの検知と阻止）| AUSTRAC
- Preventing the criminal abuse of digital currencies （デジタル通貨の不正使用防止）| AUSTRAC

出典：オーストラリア

1. Fintel Alliance は、マネー・ローンダリング、テロ資金供与、その他の重大犯罪との闘いに従事する広範な組織の専門家が集まったオーストラリアの官民パートナーシップである。Fintel Alliance のパートナーには大手銀行、送金サービスプロバイダー、賭博場運営者、オーストラリア及び海外の法執行機関や治安当局が含まれる。

91. ランサムウェアと闘うための民間セクターとの連携の形態とレベルは、国・地域によって異なる。官民パートナーシップ（PPP）は有用かつ一般に理解されているモデルだが、多くの国・地域では、DNFBP の関与が増加しているにもかかわらず、依然として従来のステークホルダー（特に銀行や他の金融機関）が重視されている。具体的な構成は PPP の目的・目標によって異なるが、従来とは異なるステークホルダーが含まれる場合がある。ランサムウェアを効果的に阻止・検知するには、PPP を利用して、法執行機関、地域の CERT、FIU、VASP に加えて、サイバーセキュリティ企業、通信プロバイダー、ブロックチェーン分析企業を集結させるべきである（例えば、既存の PPP のサブグループ又は実務部門とするなど）。

92. こうした PPP の共通の目的となるのは、ランサムウェアと関連する ML についての参加者の認識を高め、最新の傾向に関する情報を共有し、新規及び既存の脅威を調査することなどである。このようなメカニズムによって民間セクターとの関係を強化し、報告を促すこともできる。

93. 国・企業は法執行上の目的を果たすためにも PPP を活用してきた。PPP は、戦略の手がかりを共有して情報を生成し、情報共有によって幅広い規制対象セクターでのミュールやローンダリングネットワークの検知を向上させ、高度な捜査を進めるために有用なプラットフォームを提供する。

94. VASP は法執行を成功させるために必要な情報（ウォレット所有者や法定通貨の引き出しなど）を所有しているため、関係当局はこのセクターとの協力関係を構築することにより、暗号資産の追跡や、効率的な資産の差押え・没収に必要な情報を迅速に入手することができる。

Box 24. INTERPOL の Project GATEWAY と Operation Cyclone

Project GATEWAY は、サイバー犯罪に関する情報交換を目的として 2016 年に立ち上げられた民間企業とのデータ共有の枠組みである。本プロジェクトは、法執行機関と民間企業のパートナーシップを強化して、さまざまなソースからの脅威データを生成し、警察当局が攻撃を阻止できるようにするものである。サイバー犯罪エコシステムの関係者が Project GATEWAY を構成している。サイバーセキュリティ企業、脅威インテリジェンス企業、VASP、銀行などがこれに含まれる。

この枠組みは、INTERPOL と民間セクターとの間でサイバー犯罪情報を授受できるようにし、民間セクターが INTERPOL のサイバー犯罪分析を支援することを可能とするものである。民間セクターのパートナーはそれぞれの技術的な専門知識を利用して、未知のランサムウェア感染の種類の特定や、有力な属性識別の手がかりの分析を支援する。

Operation Cyclone[1] は、ランサムウェアグループ「Cl0p」による、韓国企業及び米国学術機関への攻撃に対する警察の国際的な捜査に従い実施されたものである。2021 年 6 月、INTERPOL と韓国、ウクライナ、米国の法執行機関が連携した国際的な作戦により、悪名高いランサムウェアグループのメンバー6 人が逮捕された。容疑者は、ランサムウェアグループのために 5 億ドル以上の資産の移転と現金化を支援したとされている。INTERPOL は、Project GATEWAY を通じて民間パートナーから提供された情報を活用して、Operation Cyclone を展開した。

出典：INTERPOL

1. 詳細は、www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring を参照のこと。

推奨される行動

- 各国・地域は、国のリスク評価においてランサムウェアによる ML のリスクを特定・評価するべきである。暗号資産及びランサムウェア攻撃グループの分散的な特性を考えると、ランサムウェアが今のところ国内の脅威ではないものの、暗号資産セクターが存在する国・地域もこの対象となる。このような知見は、ランサムウェアのリスクを国レベルで総体的に把握することによって、国家サイバー戦略の支援にさらに役立つと考えられる。
- 各国・地域は、法執行機関、AML/CFT 当局、サイバー犯罪当局から、サイバーセキュリティ機関やデータ保護機関などの従来と異なるパートナーに至るまで、権限ある当局同士の連携メカニズムを構築して、情報やインテリジェンスの共有を促進し、さまざまな技術的専門知識の相互共有に有用なプラットフォームを提供するべきである。
- 各国・地域は、官民の連携を支える体制を特定・確立し、各国・地域は、このような連携メカニズムに VASP 及び他の従来と異なるパートナーを含めることを検討するべきである。

国際協力

95. ランサムウェア及び関連する資金移転は、国境を越えた多国籍なものである場合が多い。ランサムウェア犯罪は一般に、資金（特に暗号資産）が洗浄され、最終的に現金化される複数の国・地域とは別の国・地域を拠点としている。ランサムウェアに関連する ML スキームは複雑で、課題が数多くあるため、関連情報、ツール、専門知識についての法執行機関同士の国境を越えた継続的な協力が必要である。特にランサムウェアの場合、資金捜査と財産回復を成功させるためには、国際的な協力メカニズムの構築及び既存メカニズムの活用が不可欠である。

Box 25. Lockergoga に対する国際合同捜査

2019 年 1 月、フランスの大企業に対するランサムウェア攻撃が発生した。同社の複数のファイルや内部サーバーの暗号化に使用されたランサムウェアとして、Lockergoga マルウェアが特定された。交渉後に身代金として 410 Bitcoin が要求されたが、同社はこれを支払わなかった。しかし、他の数多くの攻撃においても Lockergoga がハッカーに使用されていたことが判明した。

Eurojust・Europol と複数の欧州国合同の捜査チームが結成された。これは、European Investigative Orders（EIO）や Mutual Legal Agreement Treaty（MLAT）を通じた法的協力など、効率的な情報共有につながり、捜査の円滑化に役立った。

さらに、Europol・Eurojust は、大容量のハードウェアと資金により、技術支援を提供した。その後、ハッカーが解読したメッセージの流出とともに、犯罪の指令・管理インフラが特定され、犯罪グループは東欧を本拠地としていることが判明した。この結果、当該国における複数回の検挙が可能となった。

捜査は現在も継続中である。捜査官はブロックチェーン分析を通じて、使用されたさまざまなピールチェーンの手法を解明した。これがスイスの主要な資金洗浄犯罪者の逮捕につながった。

他の国・地域においても複数のマネーミュールが逮捕された。さらなる捜査により、支払われた身代金はハッカー単独の利益となったわけではないことが判明した。さまざまな犯罪協力者に対して不正な支払いが行われており、例えばインフラ（ソフトウェアエンジニア・開発者、セキュアサーバーの防弾ホスティング、指揮管理サーバーへの通信・接続を隠蔽する防弾 VPN サービス、ピールチェーン取引を手配する ML サービスなど）や、ミュール及び現金化する場所を見つけるために使用されていた。

出典：フランス

96. 国際的な共助要請で求められる情報は一般に、前提犯罪捜査に必要なフォレンジックな証拠と、ML 捜査に必要な金融データの両方に関連するものである。これには海外の IP アドレス、使用された名前とニックネーム、登録者の情報、実質的支配者の情報、取引の詳細、外国の VASP がホストするウォレットの関係者情報などが含まれる。

暗号資産の利用によって生じる特有の課題

97. ランサムウェアに関連するローンダリングにおける暗号資産の関与により、国境を越えた連携に新たな課題が生じる可能性がある。法制度間の暗号資産規制の実質的な扱いの違いや、一部の国・地域では、セクターにおいて政府の関与や監督が限定されている、あるいは存在しないことにより、関係当局が国際連携に関与する能力または意欲を低下させる可能性がある。

98. 例えば、VASP が登録されていない、あるいは VASP を監督していない国・地域では、情報提供を要請する先の企業を特定するのが難しい場合がある。たとえ適切な事業者が見つかっても、関係当局は強制的な捜査手法を利用して、国際的な協力要請を行わなければならないかもしれない。これによって、非公式な連携プロセスを通じて入手出来る情報が限定される。

99. ランサムウェア攻撃者とそのマネーミュールが拠点としている、あるいは収益の洗浄や現金化に利用する VASP が拠点とするか運営されている多くの国・地域は、こうした不正な活動に寛容であり、外国の法執行機関の要請に応じない可能性があるという事実が、この課題を一層複雑にしている。VASP が AML/CFT 義務のない国・地域にある場合は、法執行機関が利用できる関連記録が単純に存在しないかもしれない。この結果、継続中の資金捜査及び財産回復の試みが阻止される。

これらの課題により、FATF 勧告 15（トラベルルールを含む）の国際的な実施を加速する重要性がさらに高まっている。

Box 26. 非協力的な海外 VASP に起因する捜査上の課題

企業 X は、Caley ランサムウェアと思われるランサムウェア攻撃の被害を受けた。交渉後、被害者はランサムウェア攻撃者に 0.25 Bitcoin を支払い、復号鍵が記載されたメールを受け取った。被害者は復号後に業務を再開することができた。

関係当局は、身代金支払いの数日後に被害者が警察に届けた報告によって遅ればせながら事例を認識したが、すでに支払いの痕跡は途絶えていた。ブロックチェーン分析により、身代金支払いの痕跡は海外拠点の VASP に移り、0.0081 Bitcoin の残高が海外 VASP がホストする暗号ウォレットに移転していることが判明した。この VASP は度重なる情報提供の要請にも関わらず、口を閉ざしたままである。

犯人が取引を難読化するためにミキサーを使用していたことから、捜査はさらに困難となった。このような事例の状況から、犯人は不明のままであり、財産回復や逮捕は実現していない。

出典：シンガポール

100. （運営が複数の国・地域にまたがる）一部の VASP の分散的構造が原因となり、法執行機関が情報を要請するのに適した事業者、あるいは支援を要請するのにふさわしい国・地域を見つける上で、大きな調査上の負担がかかる可能性がある。例えば、ある国は、外国の金融機関で VASP が管理する銀行口座のものと推定される IBAN に基づいて、支援を求める関係国を特定することにおける課題を挙げている。別の国は、一部の VASP に物理的所在地がないことから、連携先として適切な国・地域を特定するのが困難となる可能性を指摘している。

速やかな協力の必要性

101. ランサムウェア攻撃は全世界に広く拡散され、暗号資産はほぼ瞬間的に移転できるため、法執行機関は迅速に行動して、ランサムウェアに関連する収益を追跡し、国境を越えた散逸を防止しなければならない。そのためには通常、公式の国際的協力メカニズム（司法共助など）により、刑事訴訟手続きにおいて、証拠を入手して差押えを確実に実施する必要がある。ただし、このような公式の協力メカニズムは常に迅速に実施されるとは限らず、捜査の大幅な遅れや失速、さらには妨げにつながる可能性がある。ランサムウェア関連の捜査は、関与する国・地域や企業が多いために複雑であり、国際協力には他の犯罪活動より多くの時間とリソースが必要となることが、こうした課題をさらに増大させている。

102. 非公式な協力の活用は、こうした課題に対処するのに有効であり、司法共助の要請を合理化・円滑化するのに役立つ場合がある。タイムリーな協力を促進するため、一部の国・地域は、外国の関係者との接触・関与のための既存の関係性や、実績のある非公式なチャネルの重要性を指摘している。これにより、情報を保護するために必要なプロセスに従いながら、刑事訴訟手続きを進めるのに必要な情報を迅速に交換することが容易になる。このような非公式の情報交換は、Egmont Secure Web を通じて FIU 間で行われる。警察同士の協力は、INTERPOL の I-24/7、及び Camden Asset Recovery Inter-Agency Network（CARIN）や地域の Asset Recovery Inter-Agency Networks（ARINs）などの他の非公式ネットワークを通じて行われる。関係当局は、国際間及び地域間の協力経路を利用するためのプロセスと連絡窓口を構築して、迅速な資金追跡と効果的な財産回復を支援するべきである。

103. 一部の国・地域は、二国間の関係を確立して、協力を成功させている。国をまたいで配置したサイバー犯罪専門の連絡官を活用することにより、連絡のホスト国とホーム国間での情報・インテリジェンスの共有が大幅に円滑化され、ランサムウェアに関連する捜査において、関係当局が外国と証拠を授受し合うことが可能になる。関係当局は協力のプロセス及び連絡窓口を公表して二国間の協力を推進し、迅速な資産の追跡と財産回復を支援するべきである。

Box 27. Project CODA

2021 年 11 月、ランサムウェアキャンペーン及びアラスカの政府機関と医療施設のサイバー攻撃に関わりのある、カナダのサイバー犯罪者が逮捕され、複数のサイバー犯罪に関連する違法行為で起訴された。国際パートナーに連絡するのに先立ち、FBI は関連する数件のサイバー侵入を捜査していた。容疑者を特定して居場所を突き止めた後、FBI は Ontario Provincial Police（OPP）の連携窓口と連絡を取った。

カナダ National Cybercrime Coordination Centre（NC3）、Europol、オランダの法執行機関のサポートを受けて、OPP と FBI により両国で捜査が並行して開始された。NC3 は、23 カ月間にわたる国際的な捜査の一環として、運営支援、データ及び行動の分析、情報の要約・報告、暗号通貨の追跡サービスと分析を提供した。これらの取組みによって容疑者の身元が特定され、逮捕につながった。この種のサイバー犯罪の捜査には、先進的な分析技術や、暗号資産追跡などの専用ツールの使用が重要となる。

出典：カナダ及び米国

多国間協調の重要性

104. 法執行活動の成功事例を取り上げたケーススタディでは、複数の国・地域の当局が関係していることが多い。これは、ランサムウェア攻撃及び関連する ML の国際的かつ分散的な特性を反映したものである。成功の主な要素は、影響を受ける国・地域間の国際的協調により、サイバー組織と提携者を同時に分断・根絶することである。これによって、犯罪組織がデジタルオペレーションを別の安全な避難場所に簡単に移転させることのできるリスク移転が低減される。

105. Europol・Eurojust や INTERPOL など、この目的に利用できる国際的な法執行の協調メカニズムがいくつか存在する。これらの組織は、データベースをホストし、ロジスティクスや専門知識を提供して、複数の国・地域のステークホルダーと協力している。このような多国間のメカニズムは、資金捜査や財産回復のために重要な情報の共有を促進する上で有用である。

Box 28. Operation GoldDust[1]

2021 年 11 月、ルーマニア当局は、Sodinokibi/REvil ランサムウェアを展開するサイバー攻撃の疑いで 2 人の人物を逮捕した。容疑者は 5,000 件の感染に関わり、総額 50 万ユーロの身代金を受け取ったとみられる。2021 年 2 月以来、法執行機関は他の Sodinokibi/REvil の提携者 3 人と、GandCrab に関係する 2 人の容疑者も逮捕した。これらの逮捕は、17 の国・地域[2]、Europol、Eurojust、INTERPOL が関わる Operation GoldDust の成果の一部である。これらの逮捕はすべて、国際的な合同法執行機関による、GandCrab の後継者とみられる Sodinokibi/REvil ランサムウェアグループによって使用されたインフラの特定、通信傍受、差押えなど、国際的な法執行機関の共同での取組みの結果である。

Operation GoldDust は、Europol 及び英国や米国など複数の国・地域の法執行機関のサポートを得て、ルーマニア主導で行われた GandCrab の捜査に関連する手がかりを元に実施された。

Europol は、情報交換を容易にし、Operation GoldDust の協調を支援するとともに、オペレーション分析支援や、暗号資産、マルウェア、フォレンジック分析を提供した。さらに、場所毎に専門家を配備し、Virtual Command Post を設置して、現場での活動の調整を行った。国際的協力により、Europol は他の EU 諸国とともに被害者減少の取組みを合理化することが可能となった。これらの活動により、民間企業は Sodinokibi/REvil ランサムウェアの被害を免れた。

Europol の Joint Cybercrime Action Taskforce（J-CAT）がこの作戦を支援した。この常設の作戦チームは、複数の国・地域のサイバー連絡官で構成され、同じオフィスで重大なサイバー犯罪の捜査に取り組んでいる。

出典：Europol

注釈

1. 詳細は、www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged を参照のこと

2. 参加国：オーストラリア、ベルギー、カナダ、フランス、ドイツ、オランダ、ルクセンブルグ、ノルウェー、フィリピン、ポーランド、ルーマニア、韓国、スウェーデン、スイス、クウェート、英国、米国。

推奨される行動

- 各国・地域は、迅速な国際協力と情報共有を促進するために、連絡事務所や 24 時間 365 日対応の窓口の設置など、二国間、地域間、多国間のメカニズムを確立し、積極的に参加するべきである。

結論

106. 近年、ランサムウェアに関連する資金移転は世界的に拡大しているが、関連する ML の捜査は十分に行われていない。本調査により、ランサムウェアは分野横断的かつ国際的な問題であることが明らかになった。この脅威に効果的に対処するには、協調的な取組みが必要である。これを実現するために、各国・地域は、公的機関間、官民、外国及び国際組織の 3 つのレベルでのパートナーシップを活用するべきである。

107. 本調査では、FATF 基準の履行を促進して、ランサムウェア、特に暗号資産と VASP セクターとの関係による不正な収益に対処するための効果的な枠組みを提供することの重要性について詳しく説明している。今後も FATF は、このセクターにおける FATF 基準の履行を推進していく。

108. 最後に、ランサムウェアにより獲得した収益の洗浄における暗号資産の役割、及びランサムウェアグループが使用する技術の進化は、さらなる課題を提示するものである。権限ある当局は、絶えず変化するデジタル犯罪の状況において、法令を常に適切なものに保つこと、敏捷性を保つためのスキルと能力を備えているべきである。

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。