金融審議会 第4回 暗号資産制度に関するワーキング・グループ

資料2

事務局説明資料（サイバーセキュリティに関する取組み）

2025年10月22日

金融庁
Financial Services Agency, the Japanese Government

サイバーセキュリティに関する金融庁の取組み

ガイダンスの提供 

- ✓ 金融行政方針
- ✓ 監督指針、金融分野におけるサイバーセキュリティに関するガイドライン
- ✓ 脆弱性に関する注意喚起
- ✓ 要請（体制整備、脆弱性診断、演習・訓練、監視・分析の強化、フィッシング対策など）
- ✓ G7サイバーエキスパートグループ
- ✓ 業界との意見交換会、各種講演
- ✓ 耐量子計算機暗号への対応に関する検討会

モニタリング 

- ✓ 実態把握、オン・オフの検査・モニタリング、障害対応

公助の取組み 

- ✓ 演習（Delta Wall）
- ✓ サイバーセキュリティセルフアセスメント（CSSA）
- ✓ TLPT（※）事例還元　（※Threat-led penetration testingの略。脅威ベースのペネトレーションテスト）
- ✓ 地域金融機関向けTLPT実証事業
- ✓ 金融分野におけるITレジリエンスに関する分析レポート

2025事務年度の金融行政方針（抄）

- **地政学的な緊張も背景として近年高まっているサイバーリスク**に関しては、金融業界全体の底上げを図る観点から、引き続き**業界横断的なサイバーセキュリティ演習（Delta Wall）の実施等に官民が連携して取り組む**。
- 金融機関の業務委託先等のサードパーティへのサイバー攻撃の発生状況を踏まえ、**金融機関における業務委託先等のサードパーティのリスク管理等の強化**について検討を進める。

金融分野におけるサイバーセキュリティに関するガイドライン

- これまでの検査・モニタリングの結果及び金融セクター内外の状況の変化を踏まえ、**2024年10月、監督指針等とは別に、更に詳細な「金融分野におけるサイバーセキュリティに関するガイドライン」を策定**。
- **暗号資産交換業者も本ガイドラインの適用対象**。

（金融庁ウェブサイト）https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html

1．基本的考え方

1.1. サイバーセキュリティに係る基本的考え方
1.2. 金融機関等に求められる取組み
1.3. 業界団体や中央機関等の役割
1.4. 本ガイドラインの適用対象等

2．サイバーセキュリティ管理態勢

2.1. サイバーセキュリティ管理態勢の構築
2.2. サイバーセキュリティリスクの特定
2.3. サイバー攻撃の防御
2.4. サイバー攻撃の検知
2.5. サイバーインシデント対応及び復旧
2.6. サードパーティリスク管理

3．金融庁と関係機関の連携強化

3.1. 情報共有・情報分析の強化
3.2. 捜査当局等との連携
3.3. 国際連携の深化
3.4. 官民連携

近年の脅威動向及び国内外の情勢や、これまでの実態把握、建設的対話、検査・モニタリングの結果、金融機関が直面するリスクが増加し、リスク管理態勢の強化が必須

脅威動向及びリスク環境、並びに、検査・モニタリングの目線を盛り込み、明確化

- サイバーリスクは企業経営に重大な影響を与えるトップリスクのひとつ。サイバーセキュリティについて経営上プライオリティを置いて考慮しないことは金融機関にとって大きなリスクに
- 外部（内部）の脅威に対抗するため、官民連携が重要
- 極力これまでに明らかになったリスクや検査・モニタリング上の教訓を盛り込み明確化
- 金融機関によってリスクプロファイルが異なるため、詳細で一律のチェックリスト方式は馴染まない。リスクベースアプローチ、自助・共助・公助（及び官民連携）を組み合わせて駆使する必要

サイバーセキュリティ管理態勢

基本的な対応事項

- いわゆるサイバーハイジーンと呼ばれる事項その他の金融機関等が一般的に実施する必要のある基礎的な事項

対応が望ましい事項

- 金融機関等の規模・特性等を踏まえると、インシデント発生時に、地域社会・経済等に大きな影響を及ぼしうる先において実践することが望ましいと考えられる取組み
- 他国の当局又は金融機関等との対話等によって把握した先進的な取組み等の大手金融機関及び主要な清算・振替機関等が参照すべき優良事例

暗号資産を巡るサイバー攻撃の状況

- ビットコイン誕生以降、全世界で暗号資産の流出に繋がるサイバー事案が数多く発生。
- かつてのMt. Gox事件では秘密鍵の盗難が原因となったが、直近の事案では、**ソーシャルエンジニアリングを用いるなど、手口がより巧妙化。**
- これらの事案が発生していることに加え、国内外の投資家において暗号資産が投資対象と位置付けられる状況が生じていることを踏まえて、**業界・個社のサイバーセキュリティ体制の継続的な強化に向けた官民の対応が不可避。**


一般社団法人
日本暗号資産等取引業協会
JVCEA - Japan Virtual and Crypto assets Exchange Association

English

HOME　協会概要　ニュース　会員紹介

HOME › お知らせ › 当協会会員における暗号資産の不正流出について

ニュース NEWS

2024年6月1日　お知らせ

当協会会員における暗号資産の不正流出について

第一種会員である株式会社DMM bitcoinから、同社ウォレットからのビットコイン（BTC）不正流出検知について公表がなされています。

同社の公表によれば、同社ウォレットから不正流出したビットコイン（BTC）の数量は、4,502.9BTC（約482億円相当）とのことです。
なお、同社が利用者からお預りしているビットコイン（BTC）全量については、流出相当分のBTCを、グループ会社からの支援のもと調達を行い、全額保証する旨も併せて公表されております。

また、今回の事案が発生したことを受けて、当協会から暗号資産交換業を営む全会員に対して、暗号資産管理業務に係る緊急点検の実施及び暗号資産の安全管理の徹底を要請いたします。

当協会は、引き続き利用者保護を最優先事項とし、当局とも連携しつつ、暗号資産交換業を営む会員が利用者の皆様からお預かりしている暗号資産に関し、法令や自主規制規則に基づく安全管理措置を適切に実施するよう、会員に対するその他必要な措置を講じてまいります。

出典: JVCEA「当協会会員における暗号資産の不正流出について」
2024年6月1日
https://jvcea.or.jp/news/main-info/20240601-001/


警察庁
National Police Agency

› English › 国家公安委員会 › サイトマップ

警察庁について　お知らせ　政策　法令

ホーム › 各部局から › サイバー警察局 › 注意喚起 ›
北朝鮮を背景とするサイバー攻撃グループTraderTraitorによる暗号資産関連事業者を標的としたサイバー攻撃につ

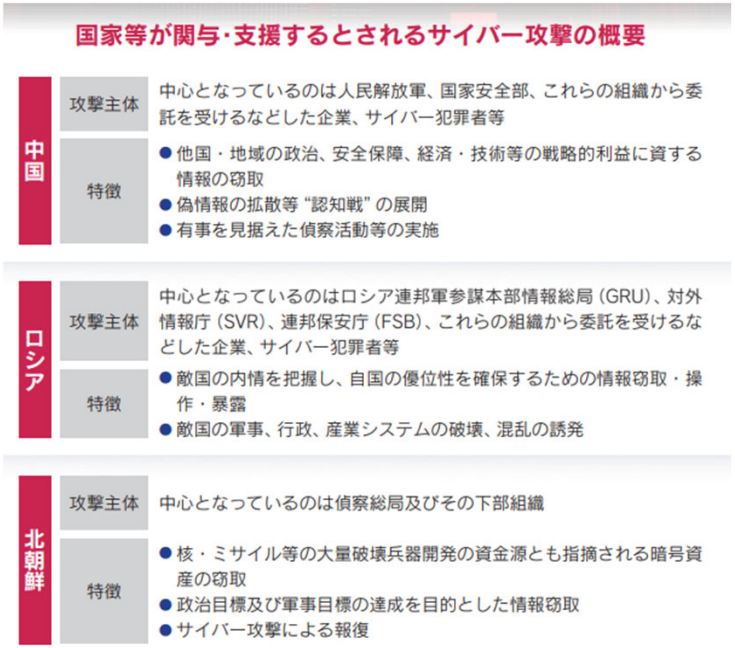
北朝鮮を背景とするサイバー攻撃グループTraderTraitorによる暗号資産関連事業者を標的としたサイバー攻撃について

警察庁は、関東管区警察局サイバー特別捜査部及び警視庁による捜査・分析の結果を総合的に評価し、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）とともに、令和６年５月に北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）が、我が国の暗号資産関連事業者「株式会社DMM Bitcoin」から約482億円相当の暗号資産を窃取したことを特定し、合同で文書を公表しました。

また、今回の公表を受け、NISC及び金融庁と連名で、同グループの手口例及び緩和策に関する文書を公表しました。

北朝鮮を背景とするサイバー攻撃グループTraderTraitorによる暗号資産関連事業者を標的としたサイバー攻撃について

出典: 警察庁「北朝鮮を背景とするサイバー攻撃グループTraderTraitorによる暗号資産関連事業者を標的としたサイバー攻撃について」
2024年12月24日
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20241224.html


国家等が関与・支援するとされるサイバー攻撃の概要

中国	攻撃主体	中心となっているのは人民解放軍、国家安全部、これらの組織から委託を受けるなどした企業、サイバー犯罪者等
	特徴	● 他国・地域の政治、安全保障、経済・技術等の戦略的利益に資する情報の窃取 ● 偽情報の拡散等“認知戦”の展開 ● 有事を見据えた偵察活動等の実施
ロシア	攻撃主体	中心となっているのはロシア連邦軍参謀本部情報総局（GRU）、対外情報庁（SVR）、連邦保安庁（FSB）、これらの組織から委託を受けるなどした企業、サイバー犯罪者等
	特徴	● 敵国の内情を把握し、自国の優位性を確保するための情報窃取・操作・暴露 ● 敵国の軍事、行政、産業システムの破壊、混乱の誘発
北朝鮮	攻撃主体	中心となっているのは偵察総局及びその下部組織
	特徴	● 核・ミサイル等の大量破壊兵器開発の資金源とも指摘される暗号資産の窃取 ● 政治目標及び軍事目標の達成を目的とした情報窃取 ● サイバー攻撃による報復

出典: 公安調査庁「サイバー空間における脅威の概況」
2024年12月
https://www.moj.go.jp/content/001396422.pdf

直近の大規模な流出事案を踏まえたサイバーセキュリティ強化の取組み

■ 2024年５月に発生した国内暗号資産交換業者における利用者財産の不正流出事案を踏まえ、同年９月、**暗号資産の流出リスクへの対応及びシステムリスク管理態勢に関して、金融庁は、以下の点について注意喚起を行った上、自主点検を行うことを要請**。

- 経営陣の認識・関与
  - 暗号資産の流出リスクは利用者保護の観点から最重要課題であると認識する必要。
  - 経営陣は社内外の情報を活用し、実効性のある管理態勢を整備する責任がある。
- 暗号資産の管理態勢
  - 事務ガイドライン・自主規制規則に沿った態勢構築が必要。
  - ３線管理の有効性を含め、問題意識を持って点検を実施する必要。

  <u>点検において特に検証すべき項目</u>

  - コールドウォレット管理：
    - 入出庫オペレーションの手続きに関する社内規則等の規定と実行
    - リスク低減に向けた措置の是非に関する検討
    - 外部ウォレット利用に伴う流出リスクの分析・特定と対応策の整備
  - 不正行為の原因究明：取引ログの保存状況と検証体制の確認

■ また、当該不正流出事案に関する具体的なソーシャルエンジニアリングの手法が判明後、同年12月、警察庁・内閣サイバーセキュリティセンター・金融庁の連名で、**参考となる手口例や緩和策を示しつつ、注意喚起を発する**とともに、**注意喚起の内容を踏まえて、改めて速やかに自主点検を行うことを要請**。

■ 以上の自主点検をフォローアップする等、当庁としても**継続的なモニタリング・監督対応**を行っていく必要。

業界全体における共助の重要性

- 「金融分野におけるサイバーセキュリティに関するガイドライン」には以下の通り記載。

  1.3. 業界団体や中央機関等の役割（抄）

  業界団体や中央機関等が、必要に応じて当局と連携しながら、金融機関等にとって参考とすべき情報や対応事例の共有、態勢構築に関する支援その他業態全体のサイバーセキュリティ強化のための活動（演習、シナリオ分析、人材育成など）等の**共助の取組みを推進**することにより、金融機関等による対応の向上に中心的・指導的な役割を果たすことが望ましい。

  金融機関等は、**共助機関である金融 ISAC等が支援している、技術的な課題への対応、ベストプラクティスの共有、最新のサイバー攻撃の動向や脆弱性情報の分析などの知見を、必要に応じ、積極的に活用**することが望ましい。

- JVCEA「暗号資産交換業者に係るシステムリスク管理に関する規則」には以下の通り記載。

  第３章 サイバーセキュリティ管理（抄）

  第９条　会員は、次の各号の事項を含め、サイバーセキュリティ管理態勢の整備に努めなければならない。

  （４）**情報共有機関等を通じた情報収集**、
  （５）**情報共有体制**

➡個社が国家レベルの攻撃に日々さらされる中で、**サイバーセキュリティ対応は、自助・共助・公助の組み合わせで対処すべき課題。特に、業界共助の取組みの発展が不可欠**であり、当局としても後押ししていく必要。