資料２

暗号資産がセキュリティの観点から
国民から広く信頼されるために必要な取り組み

September 29, 2025

Shin’ichiro Matsuo
Georgetown University CyberSMART Research Center

GEORGETOWN UNIVERSITY

過去の重大インシデントの振り返りと傾向

当初は、取引所など単体のエンティティに対する攻撃が主であったが、現在では、複雑化するサプライチェーンに対して、多様な攻撃がなされいてる。（The Weakest Linkが認識されないまま多数放置されいている状態）

事件名	発生時期	被害額	概要
マウントゴックス	2014年	480億円	ホットウォレットへのサイバー攻撃。
Coincheck	2018年	580億円	ホットウォレットへのサイバー攻撃。
Zaif	2018年	67億円	ホットウォレットへのサイバー攻撃。
BITPoint	2019年	35億円	ホットウォレットへのサイバー攻撃。
Poly Network	2021年	915億円	クロスチェーンブリッジの脆弱性を突いたハッキング。
Wormhole	2022年	480億円	ブロックチェーンブリッジの脆弱性を突いた不正送金。
BNBチェーン	2022年	855億円	クロスチェーンブリッジからの不正送金。
Grand Base	2024年4月	3億円	DeFiプロトコルの秘密鍵が盗まれ、不正にミントされた。
DMM Bitcoin	2024年5月	482億円	サプライチェーンに対するソーシャルエンジニアリング。
WazirX	2024年7月	345億円	マルチシグウォレットの脆弱性を突いた不正取引。
Bybit	2025年2月	2200億円	サプライチェーンに対するソーシャルエンジニアリング（DMM事案に類似）
Bitopro	2025年5月	16億円	古いホットウォレットへのサイバー攻撃。
Nobitex	2025年6月	135億円	プロトコルの脆弱性を突いた不正送金。
CrediX	2025年8月	6.7億円	DeFiレンディングプロトコルへのハッキング。
SwissBorg	2025年9月	61億円	ステーキングのサードパーティに対するサプライチェーン攻撃。

暗号資産エコシステムに係るセキュリティの観点と標準との対応

運用	鍵管理、監査、バックアップ、ガバナンス	ISO/IEC 27000
実装	プログラム、セキュアハードウエア	ISO/IEC 15408
ビジネスロジック	金融トランザクション, 契約	Secure coding guides
応用プロトコル	プライバシ保護, セキュアトランザクション	ISO/IEC 29128
基本プロトコル	P2P, コンセンサス, マークル木	ISO/IEC 29128
暗号アルゴリズム	ECDSA, SHA-2, RIPEMD160	NIST,ISO

これに加え、現状の複雑な暗号資産関連サービスではこれ以上に、
多様で無数の管理されていないステークホルダーが存在している

従来の情報システムにおけるセキュリティの取り組み

ガバナンス	金融庁：金融検査マニュアル、サイバーセキュリティモジュール 国家サイバー統括室（NCO）：サイバーセキュリティ戦略、CSIRT連携
基準・ガイドライン	金融庁：金融分野におけるサイバーセキュリティ関するガイドライン FISC安全対策基準 ISO/IEC 27001, NIST Cyber Security Framework 金融ISAC：ガイドライン、ベストプラクティス
実務支援	IPA：脆弱性対策情報（JVN iPedia）、SECURITY ACTION、サイバーセキュリティ経営ガイドライン（経産省と共同） JPCERT/CC：インシデント対応支援、脆弱性情報ハンドリング（JVN）、注意喚起・アラート 金融ISAC：脅威情報共有プラットフォーム（TLP分類での共有）、机上演習（Tabletop Exercise）、演習Cyber Range

暗号資産エコシステムの特殊性と課題(1)

- **攻撃者と防御側の能力の非対称性**
  - 相手にしているのは国家レベルの攻撃能力を持つ組織であることを想定する必要がある。
  - 一方で、暗号資産エコシステムの担い手はリソースが不足しているスタートアップであることが多い。扱っている金額を考慮すると、能力の非対称性が他の産業よりも際立っているといえる。
  - 特にスキルのあるセキュリティ人材の不足
    - スキルのあるセキュリティ人材が不足しており、課題を解消するためのマンパワーが圧倒的に不足している。
    - 特に暗号資産は国境を越えて移転するため、国際的な観点からの標準化を推進し、また国内で適用するためのスキルを持つ人員を確保することが喫緊の課題である。
- **動的構成を前提とした監査/評価手法の不足**
    - システム構成の自由度が高く、技術も攻撃手法も変化のスピードが速いため、「年に1回の監査」では更新や変化に十分に追随できない。
    - リスクが継続的に変化するため、静的監査では対応できないのではないか。
      →固定的な基準を設定するよりも、ガイドライン等で柔軟に対応できるような評価基準や評価手法を記載した方が良い。
- **ブリッジやスマートコントラクトの評価手法**
    - 特有のリスクモデルが確立されていない。
    - アクセス権やアップグレードに対する透明性が乏しい。
      →標準的な（安全な）運用が確立されていないため、評価を行うことも難しい。

暗号資産エコシステムの特殊性と課題(2)

- **鍵やウォレットの運用手法**
  - PKIなどでは、鍵のライフサイクルマネジメントを含めて、鍵管理の標準やベストプラクティスが一定程度確立されているが、ブロックチェーン技術ではPKIと大きく異なる鍵のライフサイクルモデルとなっており、従来のノウハウが適用できない部分が少なくない。
  - 運用が標準化されていないこともあり、各社が手探りで構築しているため、運用設計に不備があっても検知が難しい。
  - 操作ログの確保、紛失時や災害時運用の検討が進んでいない。
  - →運用手法・運用体制についても、ベストプラクティスを含めて共有できる仕組みが必要と考えられる。
- **サプライチェーン監査の継続性と可視化（SBOM/RBOM 等）**
  - SBOMの国際標準への対応が遅れている
  - 過去の事例に基づく教訓からの学習に遅れがある
    →ベストプラクティス（収集手法・活用方法）を業界内で共有することが必要と考えられる。
- **中立的第三者による評価と情報共有の制度的位置づけ**
  - 流出事案を受けても、事後規制による各社の（自己）点検に留まる。
    →事前情報を共有できる仕組みを早期に確立する必要がある。
  - 協会による監査件数を確認したところ、2022年に4会員、2023年に2会員にシステムリスク観点での監査を行った記録は確認できるが、全会員に対する監査は行われていない。

既存のセキュリティの考え方が適用できる点と新たに考えないといけない点

- P4に挙げた既存の取り組みのほとんどは、暗号資産エコシステムにおいても適用可能である。ただし、暗号資産エコシステム向けに修正が必要なものはある。
- 一方で、以下の点は、既存のセキュリティ対策では対応できない範囲であり、新たなセキュリティ対策の考え方と標準が必要である。
  - **PKIにはない署名鍵等の暗号鍵のライフサイクルマネジメント**
    NIST SP800-57で記述されているような伝統的な鍵管理の考え方とは異なるため、新たな鍵のライフサイクルマネジメントの標準モデルを確立する必要がある。
  - **インシデントハンドリング／インシデントレスポンス**
    ブロックチェーンのソフトウエアに脆弱性が発生したときに、オープンソースコミュニティに修正する義務を課すことができない。また、パーミッションレスブロックチェーンにおいて、世界的に広がるノードに対して安全性を保ったまま円滑に移行することは困難である。
  - **動的なシステム構成によるサプライチェーンリスク**
    暗号資産を用いたサービスは、複数のシステムやコンポーネントを自由に組み合わせて動的に構成を変更できるため、ISMSによるリスク分析やサプライチェーンリスクの分析をその都度行なう必要があるが、実際には煩雑かつコストがかかるため、分析が実行されずにリスクが管理できない。

国内における暗号資産セキュリティのノウハウ化の取り組み

CGTFによる「暗号資産カストディアンのセキュリティ対策についての考え方」

■ **背景／目的**

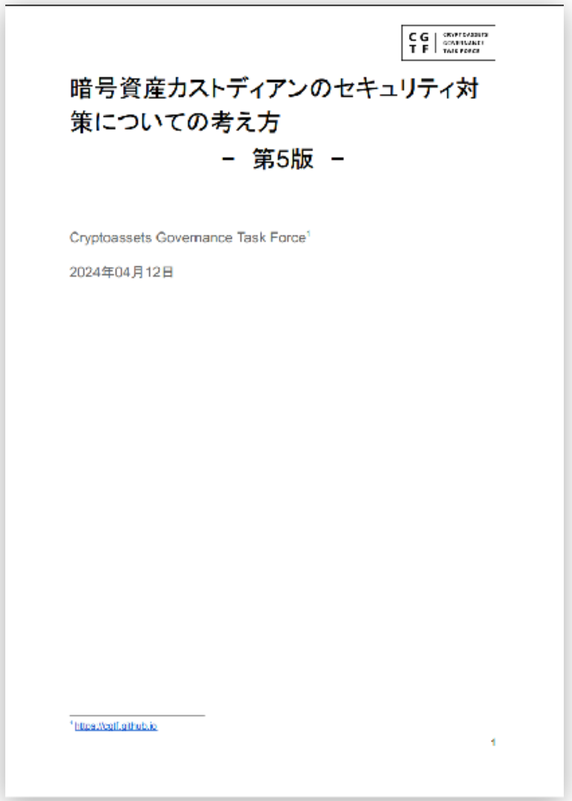
- カストディアン事業者が顧客の暗号資産を安全に管理するための基本的な考え方と推奨セキュリティ対策を整理
- 署名鍵（トランザクション署名鍵）に関する固有のリスクに重点を置く

■ **主要テーマ**

1. 鍵管理のガバナンス・技術的留意点
2. カストディ業務におけるリスク分析
3. セキュリティ管理策と運用注意点
4. 外部リスク・システム停止・法的リスク対応

■ **ハイライト**

- 鍵のライフサイクル管理に関するガイドライン
- 権限分離・承認操作・証跡管理
- 鍵情報の外部保存回避、アドレスポイズニング対策
- 事業継続性・障害対応を含む設計と運用


暗号資産カストディアンのセキュリティ対策についての考え方
－ 第5版 －
Cryptoassets Governance Task Force[1]
2024年04月12日

ISO TR23576として出版済み

https://cgtf.github.io/publications/20240412/custodiandocument_ver5.pdf

国内における暗号資産セキュリティのノウハウ化の取り組み

JPCrypto-ISACによる委託先管理ガイドライン（案）による仕組みの構築

1.ガイドラインの目的

- 近年増加しているサイバーリスクや外部委託の高度化を背景に、利用者保護・システム安定性・法令遵守を確保するための基盤とするため、暗号資産交換業者などが委託先管理を適切に行うための指針を示すことを目的としている。

2.委託先管理の基本原則

- リスクベース・アプローチの考え方を採用し、契約前の評価（デューデリジェンス）から、契約締結、実施状況のモニタリング、終了・更新までのライフサイクル管理を明確化。

3.契約・リスク管理

- 委託契約には、秘密保持・再委託制限・情報セキュリティ要求・監査受入れ義務などを盛り込む必要があるが、サイバー攻撃、個人情報流出、システム障害等のリスクに対応できるよう、リスク評価と対応計画を事前に作成。

4.モニタリングと監査

- 定期的なモニタリング（報告書・面談・点検など）と、監査（書面監査・実地監査）を組み合わせて実施。また、監査結果に基づく改善要求とフォローアップが不可欠。特に重要業務を担う委託先には、年次計画に基づき重点的に監査を行うことを推奨。

5.インシデント対応

- 委託先で発生したインシデント（例：システム障害・情報漏洩）について、速やかな報告・連携体制を整備することを求める。また、委託元と委託先の責任分担や対応手順を事前に合意しておく必要がある。

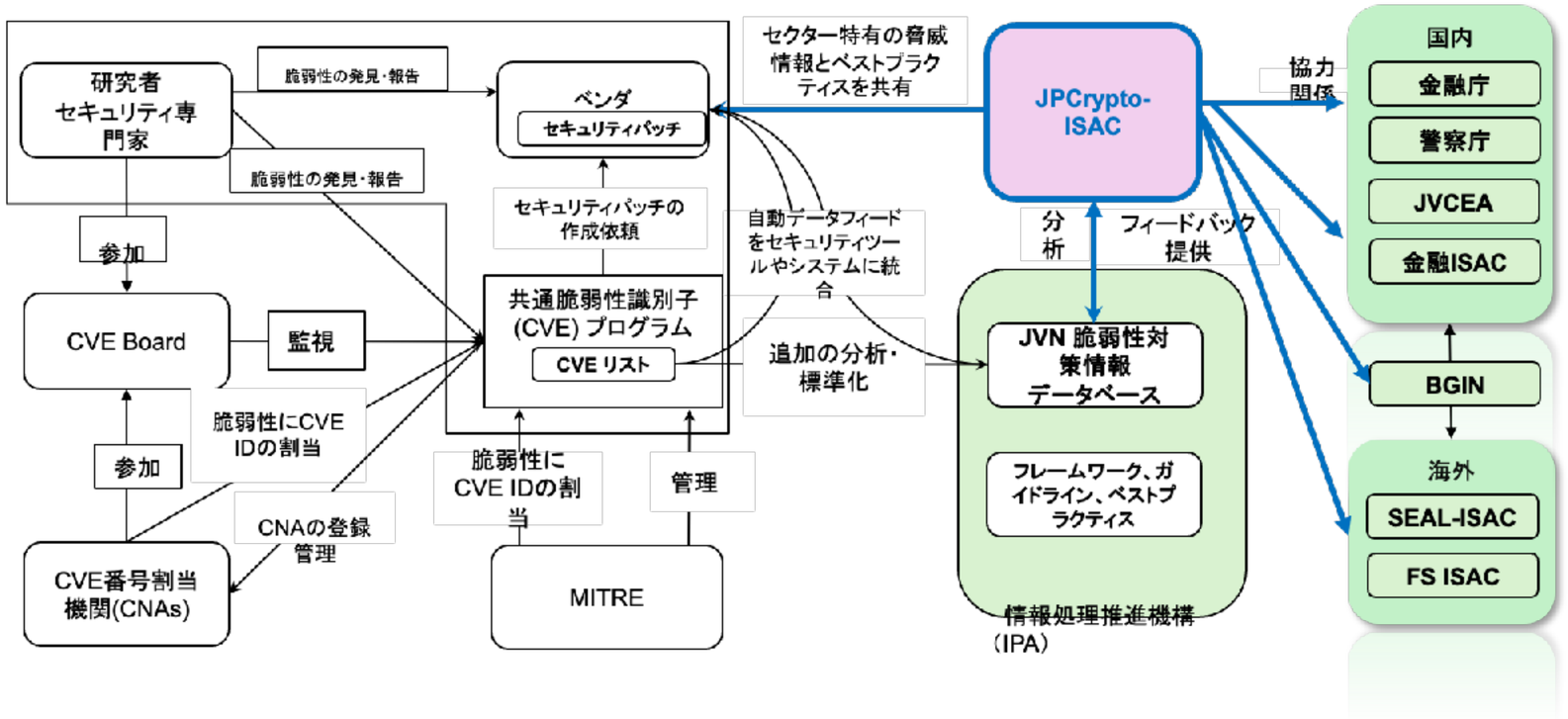
6.内部統制・ガバナンス

- 委託先管理の方針・手順を社内規程として整備し、経営層が関与することを明確化。また、内部監査部門による検証を定期的に行い、管理態勢の有効性を確認する仕組みを持つ。

方針を示したうえで、会員各社で方針に従って実行していることを確認する仕組みを構築中

グローバルにおける新たな取り組み

- 暗号資産エコシステムにおけるサイバーセキュリティ情報共有フレームワークをBGINにおいて標準化中
- 10/15にBGIN標準として出版予定
- 11月のISO TC307において、PASによりISO標準を策定するための提案を行う予定



https://docs.google.com/document/d/1sCJ5hnVkeqlUVe8ZLJ6FOy45eUfwtcLX/edit?usp=drive_link&ouid=111552709379139325482&rtpof=true&sd=true

BGINにおけるサイバーセキュリティWGの直近のアジェンダ

BGINでは、以下のアジェンダについて標準文書を作成している。

標準文書はISOにPASを通じて持ち込まれ、ISOの国際標準として策定される。

- Information Sharing Framework Standard
  サイバーセキュリティ情報のグローバルな共有フレームワークの定義と、
- Security Target and Protection Profile
  ウォレットや暗号資産関連のソフトウエアやハードウエアを、ISO/IEC 15408 （Common Criteria）のフレームワークでアセスメントするための評価基準
- Governance of the security supply chain
  提供先ガイドラインを含む、動的なサプライチェーンセキュリティの確保の方法
- Offline Key Management
  オフラインになっている鍵の管理方法
- PQC Migration
  耐量子計算機暗号技術への移行方法

https://bgin-global.org/events/20251015-block13

国民から広く信頼されるために必要な取り組みの全体像

- **まずは底上げ：**既存の金融業界や、他の業界で当たり前に行なわれているセキュリティの標準的なマネジメントを着実にこなせるようにする。
- **競争領域ではなくて協調領域：**暗号資産エコシステムの担い手は、他の産業にくらべて単独では十分なセキュリティ体制を組めないスタートアップであることが多い。スタートアップによるイノベーションも大事であることから、JPCrypto-ISACのような共助の組織が中心となる必要がある。
- **標準化への貢献と準拠：**技術面から運用に至るまで、継続的なリスクマネジメントサイクルの運用と、標準化されたセキュリティ対策の適用が重要。暗号資産セキュリティについては、従来のセキュリティ対策にない新しい要素が少なくない一方、技術と運用の標準がないため、標準化作業が急務。
- **適切な人材の確保：**国家レベルの攻撃にさらされることが前提。このような攻撃に耐えるセキュリティ人材は「実戦経験」を持つ人が必要であり、時間短縮をした促成はできない。既存の産業の実戦経験を持つセキュリティ人材の活用が必須。

提言

- 暗号資産エコシステムのセキュリティ対策については、システム構成も動的に変化し、攻撃環境も常に高度化するため、技術、および運用の要件などを法律の中に書き込むのではなく、法律では必要な体制の確保についての要請を書くことにとどめる一方で、ガイドラインによって柔軟に対応できるようにする。
- 協調領域であることに鑑み、JPCrypto-ISACのような共助のための組織の強化施策について、ガイドラインに記載されることが重要。特に、共助のための組織は、一方で持続性を確保することが容易ではないことに注意をする。持続性を持ち信頼された組織であるためには、独立性、中立性が不可欠であることにも注意。
- 金融庁においても、暗号資産エコシステムのサイバーセキュリティ対策について、技術的中立性の枠組みから一歩進め、暗号資産業界や産官学のセキュリティのエキスパートとの連携体制の構築、暗号資産業界のセキュリティ体制（共助）の体制構築を促すこと、および国際連携体制への協力を検討すべきである。
- こうしたサイバーに関するあらゆる取組みの姿勢を日本の業界内全体で高める必要がある根拠となるハイレベルな記載が法律上にもある必要がある。 一方で、法律で縛りすぎると柔軟性が失われるので、詳細はガイドライン等に記載することが適切である。

Thank you!

GEORGETOWN UNIVERSITY