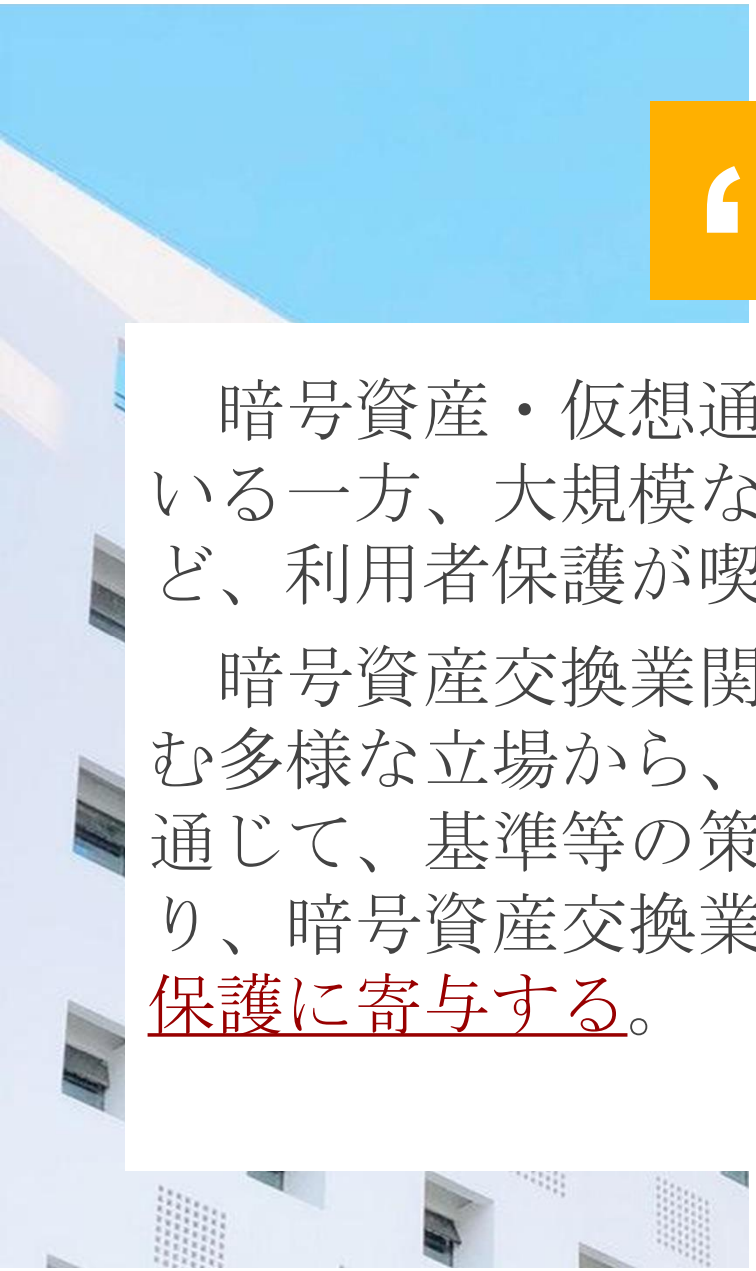
資料４

CGTFのご紹介



暗号資産・仮想通貨(Cryptoassets)の認知が急速に拡大している一方、大規模なセキュリティインシデントが発生するなど、利用者保護が喫緊の課題とされている。

暗号資産交換業関係者に留まらずセキュリティ専門家を含む多様な立場から、情報セキュリティのための知見の集約を通じて、基準等の策定に資する技術情報を提供することにより、暗号資産交換業のセキュリティの底上げを図り、利用者保護に寄与する。

General Policy

Neutrality
中立性

暗号資産交換業者にとどまらず、学術・セキュリティ専門家など、多面的な視点から本問題について取り組んでまいります。

Transparency
透明性

本TFで策定する文書、議事録などを広く一般に提供することにより、透明性が担保されたTF運営を目指します。

Effectivity
実効性

本TFの成果について、標準化機関等での国内外の専門家による知見の反映を通じ、実務に資するドキュメントの作成を目指します。

主要メンバーの専門性とミーティングポリシー

- メンバーの専門性
  - 行政
  - 法規制
  - 情報セキュリティ
  - 暗号資産
  - ブロックチェーン
  - ハードウェアセキュリティ
  - （暗号資産の）脆弱性
  - （既存）金融
  - 暗号学、公開鍵暗号

- ミーティングポリシー
  - 相互の専門性を尊重する。
  - 所属企業の立場を離れる。
  - 効果のある対策を考える。
  - 相手に伝わる表現を使う。

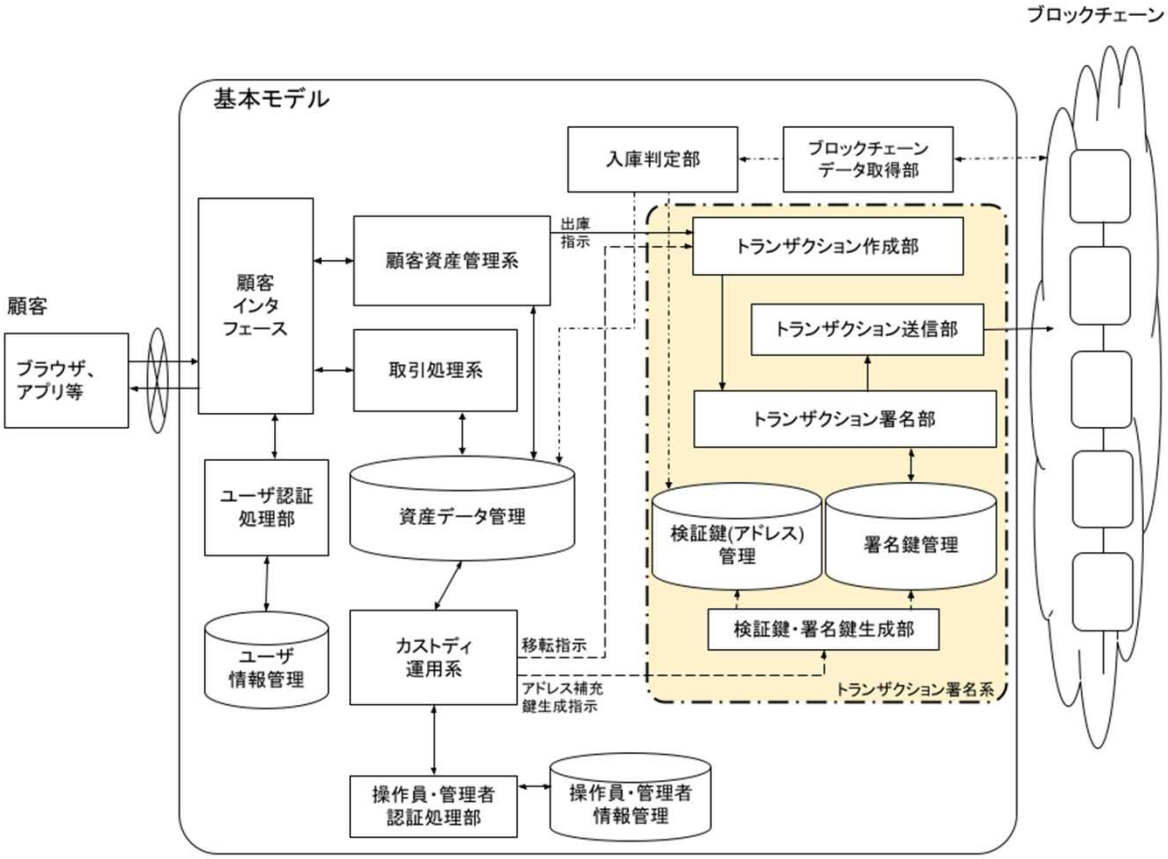
これまでの実績

2018年2月8日	第1回タスクフォースを開催
2018年10月	**日本語版ドキュメントのPublic Draftを公開。**
2019年3月14日	日本国内における仮想通貨ウォレットの実態調査（CGTFディスカッション・ペーパー#1）公開
2019年12月16日	暗号資産の署名鍵を取り扱うサービスに関する調査（CGTFディスカッション・ペーパー#2）公開
2020年7月20日	**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2版 公開**
2021年10月18日	「2021年8月に発生した暗号資産の流出に関するCGTFとしての見解」公開
2022年3月23日	**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3版 公開**
2022年11月17日	暗号資産とNFTのトラブル集　サイト公開
2023年4月10日	**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4版 公開**

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

- 通称：カストディアンドキュメント
- 目的は以下の通り
  - 暗号資産カストディアンの利用者保護
    - まずは署名鍵を厳重に守ること
    - これまでのセキュリティインシデントからの再発防止
    - これから発生しそうなインシデント想定からの再発防止
  - 情報セキュリティ対策体制を構築する上での考え方を示す
- 初版は2018年2月から検討。2018年10月に草案を作成、パブコメ開始。
- 最新は第4版。インシデントの発生等により、随時更新を行っている。
- 本書の特色：
  - 一般的に利用されているセキュリティ標準であるISO27002（ISMS）をベースとしており、理解しやすい形式としている。
  - （暗号資産における）インシデントを分析し、その再発防止策を取り込んでいる。

（参考）ドキュメントでの参照モデル



カストディアンドキュメントのスコープ

- スコープ
  - 顧客に対して暗号資産のカストディ業務を提供する、暗号資産カストディシステム
  - 暗号資産カストディシステムが管理する資産情報（署名鍵を含む）
  - 暗号資産カストディシステムのセキュリティ対策の不備により及ぼしうる社会的な影響

- 原則としてスコープ外
  - 暗号資産カストディアンが日常業務に利用するシステム（Webの閲覧、電子メールの送受信等）に対するセキュリティ対策
  - ブロックチェーンや分散型台帳自体に対するセキュリティ対策
  - 暗号資産カストディアン自身の経営リスク
  - 利用者と暗号資産カストディアンの資産の分離に関する具体的な要件
  - いわゆるLayer2の利用

全体の流れ

- 原則として、ISO 27002に沿って、カストディアンのセキュリティ対策として検討すべき内容を記載している。
  - 現在、27002の改訂作業が進んでいることから、日本語版の改訂後に、カストディアンドキュメントも修正する予定。

- 27002に前置する内容として、署名鍵の取扱いに関するリスクや、過去のトラブルからの再発防止などの内容を、特有のリスクとして取り上げている。
  - 署名鍵の盗難や不正利用のリスク
  - （運用）要員による署名鍵の不正利用リスク
  - ハッシュレートの急激な変動
  - いわゆるスプリット（ハードフォーク）

ドキュメント上の重要なポイント

- 鍵の形態およびライフサイクルに応じたリスク管理を行うこと
  - 鍵への厳格なアクセス制御と適切な権限分離
  - 鍵管理の形態の違いによりリスクが異なる
    - 例：KEK、マルチシグ、秘密分散、マスターシードの採用
  - いわゆる単独犯を防ぐ必要がある
- 鍵のバックアップについて十分に検討すること
  - 媒体の種類や個数、保管場所、アクセス権限、利用時の手続きや利用可能であることの検証頻度など、検討すべき点は多岐にわたる
- 決済情報の変更手続きのプロセスを確定させること
  - 例：業者間決済に使用する暗号資産アドレスの変更については、相互に合意した手続きを踏まなければ変更が行われない

現在の問題認識(1/2)

- Unhosted Wallet
  - 手元でデジタル資産を管理できる利便性がある反面、トラブルの補償は一切なく、利用者自身が安全に管理する必要がある。
  - スマホ等のウォレットアプリでは十分な暗号強度を選択できない。
  - Unhotsted Walletには、カストディアンの利用するウォレットとは別のリスク分析が必要ではないか。
  - なお、現時点ではUnhosted Walletはトラベルルールの適用対象外である。
- ハードウェアウォレット
  - 一部のハードウェアウォレットにおいて、署名鍵をエクスポート可能とする機能を搭載することについて議論があった。
    - 結果として機能が一部の国でリリースされている（日本は対象外）。
  - サプライチェーンリスクの存在
    - 中古品や、正規代理店以外からの購入以外に、当該ハードウォレットが正しく製造されているのか、という懸念がある。

現在の問題認識(2/2)

- ウォレットの分類
  - 一般的な分類として、ハードウェアとソフトウェアという分類は感覚的に理解できるが、ホットウォレット、コールドウォレット、ウォームウォレットなどには定義がない。
  - パラメータを整理することで、一定程度の分類ができるのではないか、という認識は持っているものの、なかなか検討に着手できていない。

THANKS!

You can find me at:

- cgtfjp@gmail.com
- https://cgtf.github.io/