# 金融システムにおける暗号技術利用の変容と
# セキュリティ上の対応


**January 31, 2025**
**Shin’ichiro Matsuo, Georgetown University**

GEORGETOWN UNIVERSITY
*CyberSMART*

# 自己紹介: 松尾真一郎

@shanematsuo

- 主な研究領域：暗号、暗号プロトコル、プライバシ、情報セキュリティ
  - 例：電子現金、電子投票、暗号学的タイムスタンプ、RFID認証、ブロックチェーン
- ジョージタウン大学 Department of Computer Science 研究教授
  - CyberSMART研究センターダイレクター（Blockchain Technology and Ecosystem Design Research Lead）
- バージニア工科大学 研究教授
- Blockchain Governance Initiative Network（BGIN）暫定共同チェア
- ISO/IECにおける技術標準の6つのプロジェクトのリーダー（TC307, JTC1 SC27）、元日本HoD（SC27/WG2）
- OCED  Blockchain Expert Policy Advisory Board (BEPAB)メンバー
- ISO TC68 X.9 (米国国内委員会）メンバー （CBDC標準化）
- Scaling Bitcoin 2018 Tokyo, IEEE ICBC 2022プログラム委員長（その他、ブロックチェーンの国際会議のプログラム委員メンバー（Financial Crypgoraphy, ACMCCS等）
- 内閣官房Trusted Web推進協議会構成員、金融庁 デジタル・分散型金融への対応のあり方等に関する研究会メンバー、デジタル庁 Web3.0研究会 構成員
- 過去に暗号技術検討会構成員等

**ビットコインや暗号資産は持っていません。**
**暗号資産と既存通貨との交換レートについては関心はありません。**

# インターネットの登場による金融システムのセキュリティ環境の変化

- インターネット以前から銀行システム、銀行間システムなどは、ネットネットワーク接続されていた。店舗間などでは、専用線であるものの暗号化や認証が行われていた。
  →セキュリティ上のリスクや攻撃界面は非常に限定的
- インターネットにより、Webサービスなどのユーザとの接点で、オープンなネットワークを利用
  →ユーザとの接点に攻撃界面が生じるため、ユーザの認証、通信路の暗号化の導入（PKI, SSL/TLS, ワンタイムパスワード等）
- 異なるサービスをインターネット上で連携して利用するようになる（API連携など）
  →ID、認証の連携（認証・認可、OpenIDなど）
- しかし、依然金融システムの基幹部分は、インターネット上の脅威・リスクとは分離されていた

# 新しいデジタル金融のルールは誰が作り手になるか？

# Bitcoinの発明に繋がる学術会議：Financial Cryptography Conference


通常はカリブ海の島で開催

第一回は (1997) Anguillaで開催

暗号の輸出規制から逃れるため

タックスヘイヴンである

サイファーパンクによって始められた

# パーミッションレスイノベーション

- すべての人に新しいイノベーションとエコシステムを作る権利を与える
- イノベーションを起こす人の数を増やす
- イノベーションのジレンマの解決

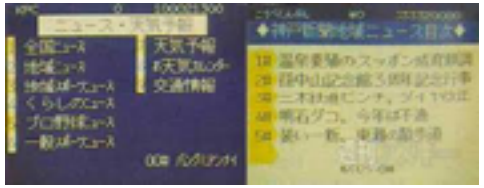
# インターネットの開発・普及が変えたイノベーションのあり方

## パーミッションレスイノベーション

- 通信チャネルと多方向の通信の権利をアンバンドル**（新たなルール作りがやりやすいアーキテクチャ）**
  - 非中央のアーキテクチャ: Routing, BGP
  - テクノロジのレイヤ化

    TCP/IP, i.e. “stupid network”
- アンバンドル化が、新しいサービス、ビジネス、経済の発生を草の根から促進
- ただし、Step-by-stepであり、インターネットらしい多方向のサービス（例：SNS）の登場は、インターネット商用化の約8年後

Minitel (France)



CAPTAIN (Japan)

# ブロックチェーンに関わる大まかなステークホルダーとその関係

出典：2019 G20財務大臣・中央銀行総裁会議 ハイレベルセミナー
「デジタル時代の未来」セッション2：分散型金融システムのガバナンス

規制当局

十分なコミュニケーション
チャネルがない
共通言語がない
技術自体への規制の可否

スピードの違い

なるべく規制による制約を避けたい

技術の成熟度への誤解

透明性の欠如

分散型技術の作り手（含む研究者）
オープンソースエンジニア

ビジネス

消費者・投資家

# 暗号を使ってセキュアなはずが...


Mt. Gox


The DAO Attack

Coincheck

Selfish Mining


Monacoin

Zaif

Zaif

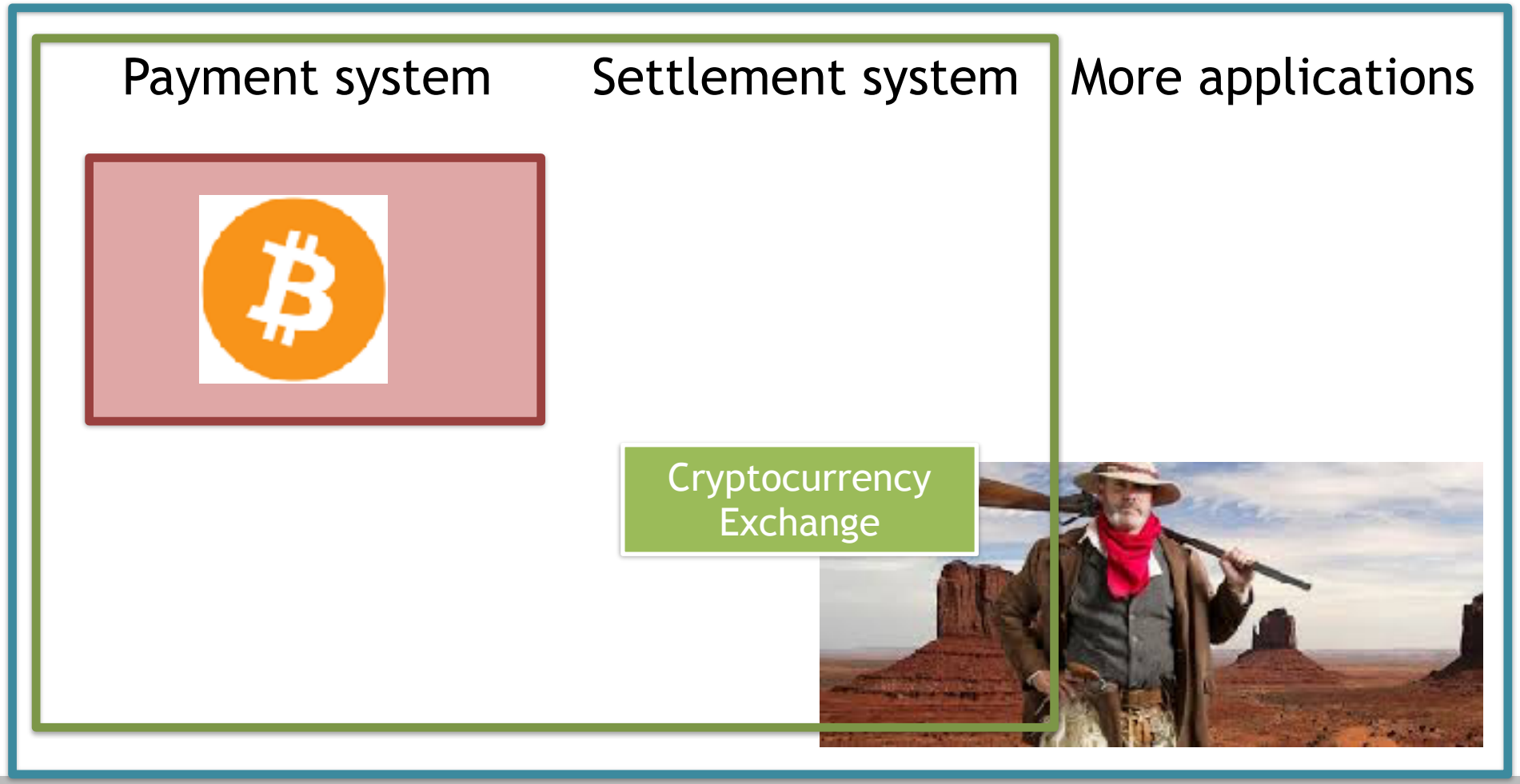
DMM Bitcoin

DMM Bitcoin

# Satoshi Nakamotoの境界線

信頼できる第三者機関がなくても二重支払いが防げる

信頼できる第三者機関の助けが必要



# ブロックチェーンの応用をセキュアに作るために

| | | |
|---|---|---|
| 運用 | 鍵管理、監査、バックアップ | 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 |

# ブロックチェーンの課題と日本における推進のために必要な技術投資の骨格

**ブロックチェーンの課題**

- セキュリティ・トラスト
  - 鍵管理
  - 危殆化対策
  - ブロックチェーンのトリレンマ、スケーラビリティとセキュリティ
  - スマートコントラクトセキュリティ
  - オラクル問題（よく指摘されているNFTの問題もここに帰着する）
  - ブリッジ問題
  - 安全性証明がない
  - インシデントハンドリング・レスポンス
- 運用上の課題
  - 永続性（暗号の危殆化、経済的インセンティブ）
  - 電力消費問題（本来の思想やセキュリティとのトレードオフ）
- 規制上の課題
  - 証券該当性
  - ガバナンス問題

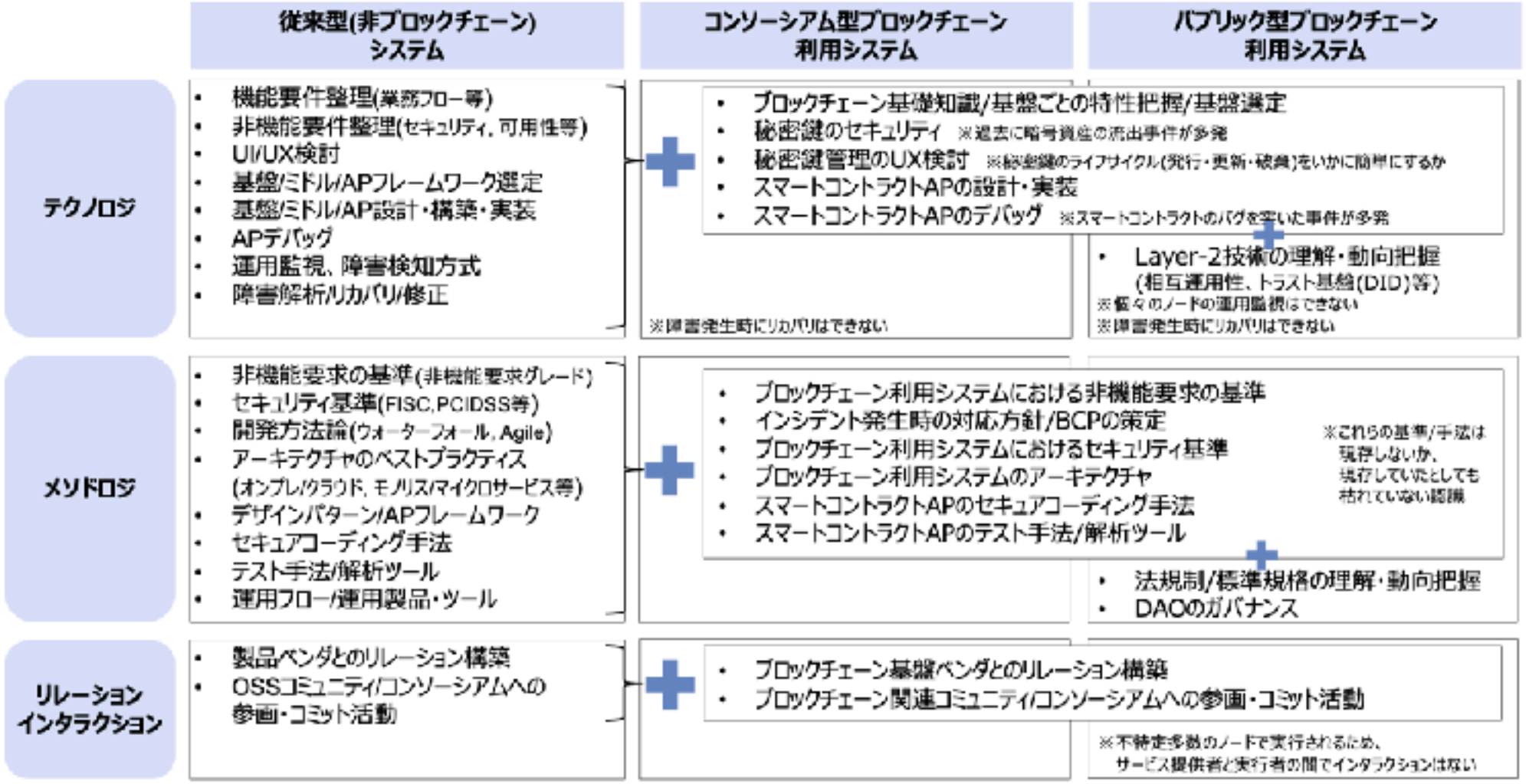
セキュリティとスケーラビリティを両立させる理論と技術

システムセキュリティの技術と運用

社会工学・経済学とコンピューターサイエンスとの協業

規制対応のための技術（Regtech/Suptech）

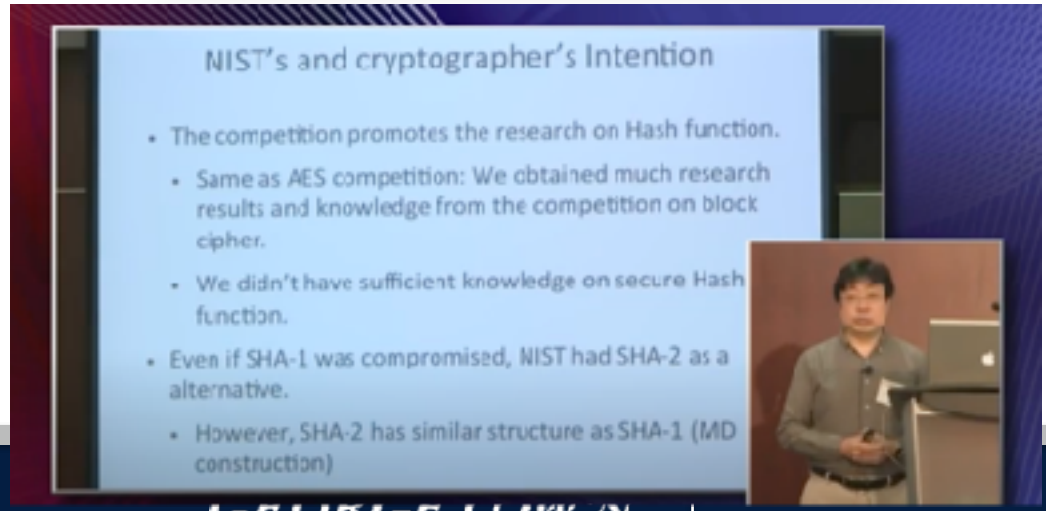
# ブロックチェーンエコシステムに必要な人材




第1回デジタル資産ラウンドテーブル平栗勇人 様（NTTデータ）資料「分散台帳技術を用いたシステム開発・運用に必要なスキルマップ」より

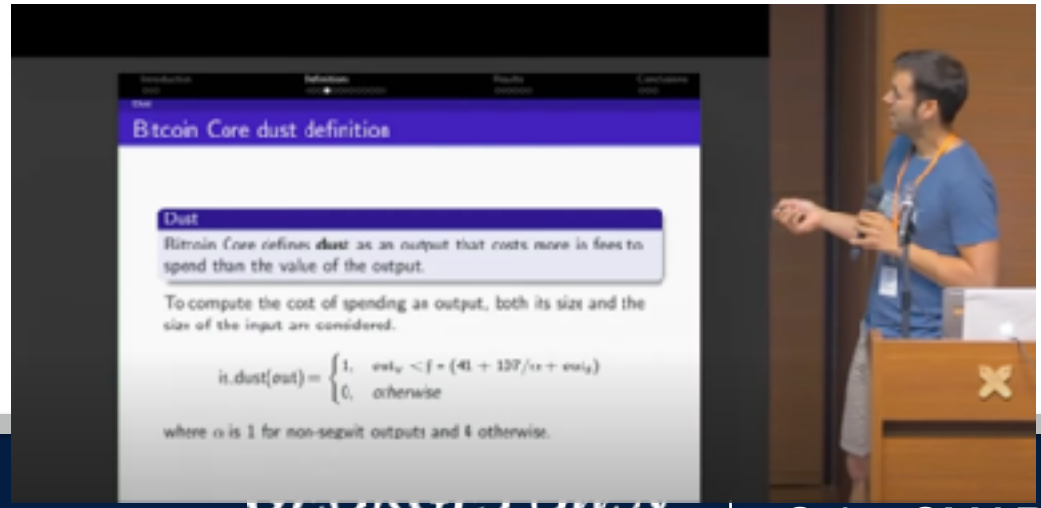
# グローバルな技術な暗号技術の作り手はどうなっているか

- Scaling Bitcoin 1
- Bitcoin Coreエンジニアが、スケーラビリティ問題の解決方法をアカデミアの流儀で議論するための会議
  - NISTのSHA-3コンペティションのモデルを参考
- 一方で、Bitcoin Coreのメンバーの多くが暗号技術の安全性に関する基本的な知識を持たずに開発していることも判明。

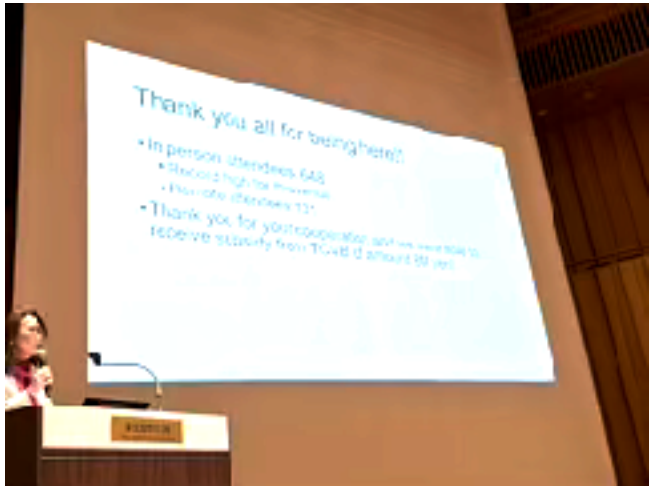
# グローバルな技術な暗号技術の作り手はどうなっているか

- Scaling Bitcoin Japan (2018)
- 2018年に日本に招致
- Program Committeeはアカデミアとエンジニア同数
- ただし、日本からのSubmissionはなかった。

# グローバルな技術な暗号技術の作り手はどうなっているか

- Real World Cryptography 2023
  - Bitcoin Coreエンジニアが、日本国外から参加
  - 一方で、日本人のブロックチェーンエンジニアは不在
- IETF Meeting 116 (Yokohama, Japan)
  - ブロックチェーンエンジニアが不在
- Financial Cryptography 2024
  - 日本からの参加者は暗号プロトコルの研究者のみ

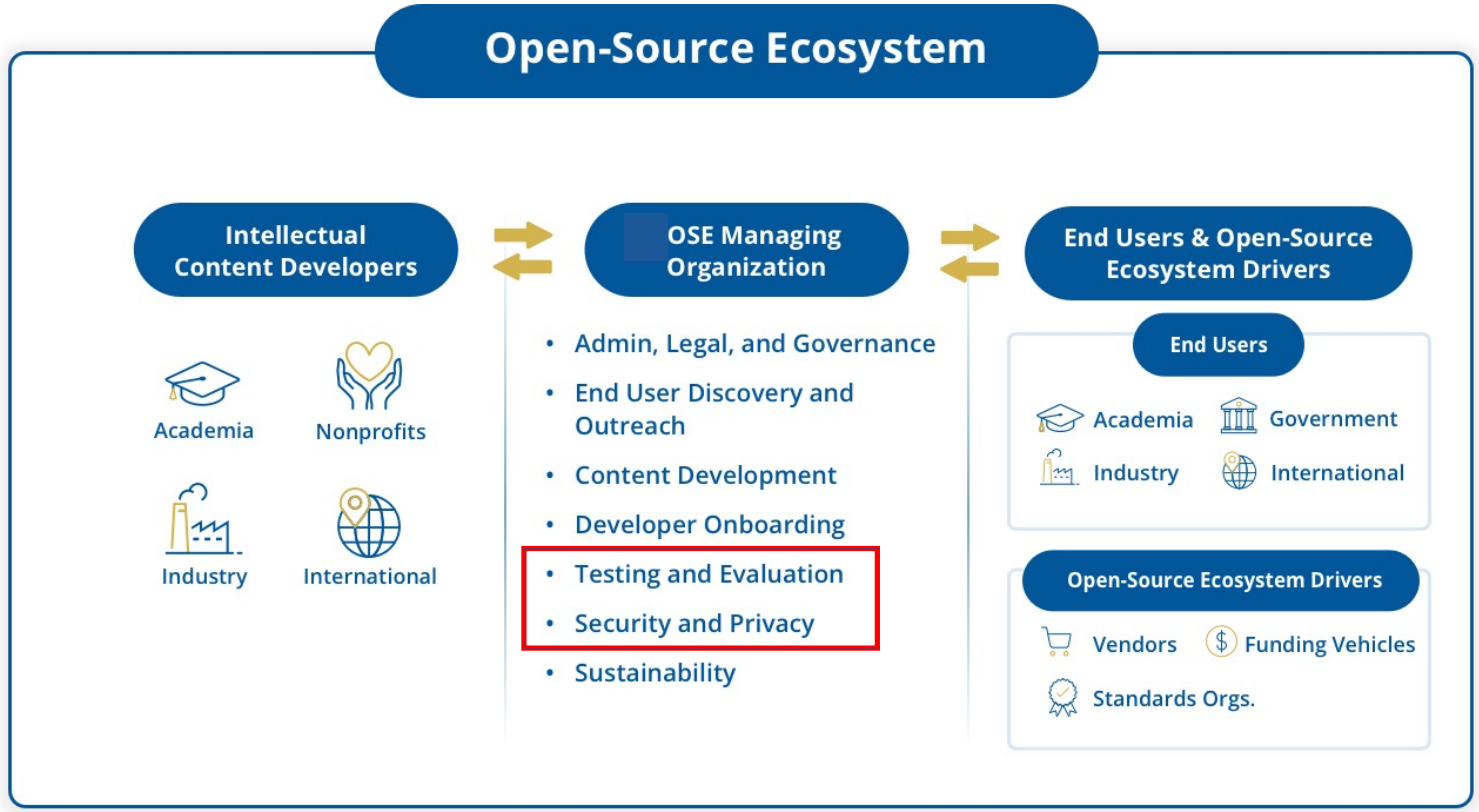



# 「最高峰の士俵」を作る米国のグローバル戦略

- 暗号・セキュリティの例では、世界中の研究者がNISTのコンペティションの動向によって動く
  - NISTのコンペティションに新しい暗号を提案すること、コンペティションにおいて攻撃論文や評価論文を発表すること、コンペティションの勝者に選ばれることが、研究者コミュニティで一番評価される。
  - 上記のような規模のコンペティションを主催できる組織が他国にないため、NISTの標準文書が、事実上ISOの標準の骨格をなす。
- 将来のコンペティションのロードマップは、ワシントンDC・東海岸のコミュニティ（NIST, NSF, DAPRA, NSA, 大学, 政府, 議会, シンクタンク）で常に議論される。
- 最高峰の土俵の魅力を増すためであれば、人材を惜しみなく獲得する、あるいはその支援をする
  - 標準化
  - 学会（IEEE, ACM）

# 米国におけるオープンソースセキュリティの取り組み例：SafeOSE

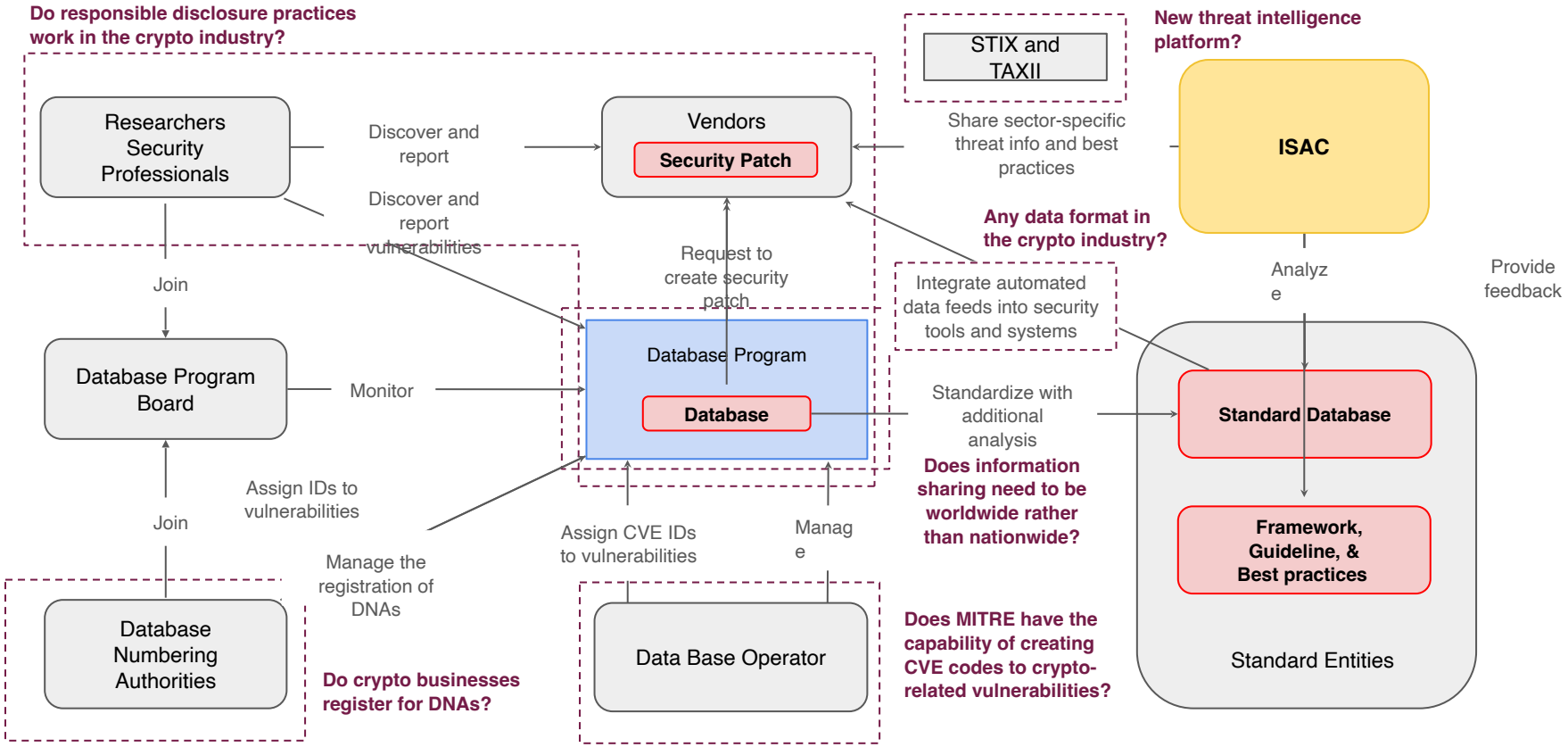
- log4jによる広範囲な脆弱性を契機に、大統領令により、オープンソースのサプライチェーンセキュリティについての取り組みが始まる。
- NSF（連邦政府の研究開発ファンディング機関）が、オープンソースのサプライチェーン背キュリティのためのコミュニティ作りへの資金助成を開始



# 安全なシステムの提供に向けて

セキュリティ面では、いまのところバラバラ。

標準の整備と、標準化プロセスを通じた人材育成が必要



# BGIN Block 12とFinancial Cryptography 2025


ブロックチェーン技術の標準化会議

2025年3月2日-3日@渋谷


トップ暗号学者による会議（12年ぶり日本で開催）

2025年4月14日-3=18日@宮古島

# Thank you


GEORGETOWN UNIVERSITY

*CyberSMART*