ブロックチェーンと信頼関係のもたらす防御者革命

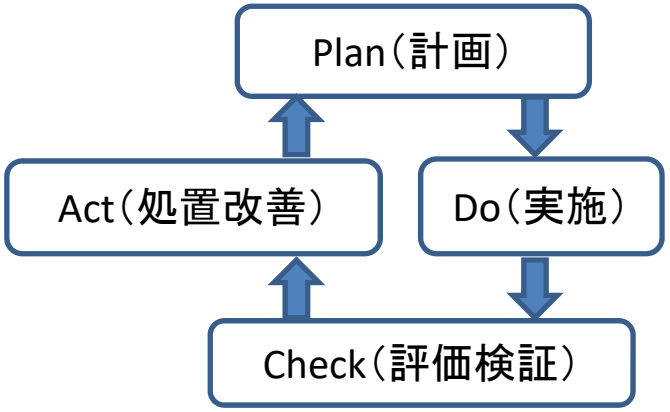
松浦幹太
（東京大学 生産技術研究所
ソシオグローバル情報工学研究センター）

2017年7月24日　ワークショップ「ブロックチェーンの未来」

情報セキュリティ

■ 情報セキュリティの確保とは？

- 守るべき基本要素(Confidentiality, Integrity, Availability)に関する品質管理の徹底



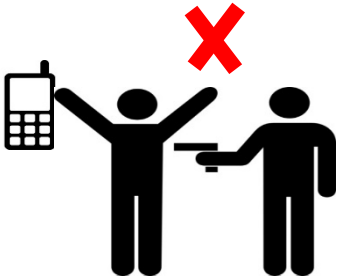
■ 分野と焦点

- 暗号（情報内容に関する安全性を確保）
  - 焦点：　独立したデータ
- ネットワークセキュリティ（通信に関する安全性を確保）
  - 焦点：　通信や通信路を介したリモートの情報資源
- コンピュータセキュリティ（端末に関する安全性を確保）
  - 焦点：　端末における情報資源

アプリケーションセキュリティ

■ サービスや業務に関する安全性を確保

- 焦点：　アプリケーション固有の信頼関係
- 例１：　電子投票（「本人確認（認証）」や「プライバシー保護」だけでなく「投票者本人の意思による投票であること」なども必要）
- 例２：　電子的な「お金」（分類により差があるがポイントは「二重使用の防止」）



■ ブロックチェーンは、トラスト基盤を低コストで実現する技術として期待されている。

■ 精査を経ない技術も、持論の押しつけに過ぎない運用も、真の守りにはならない。

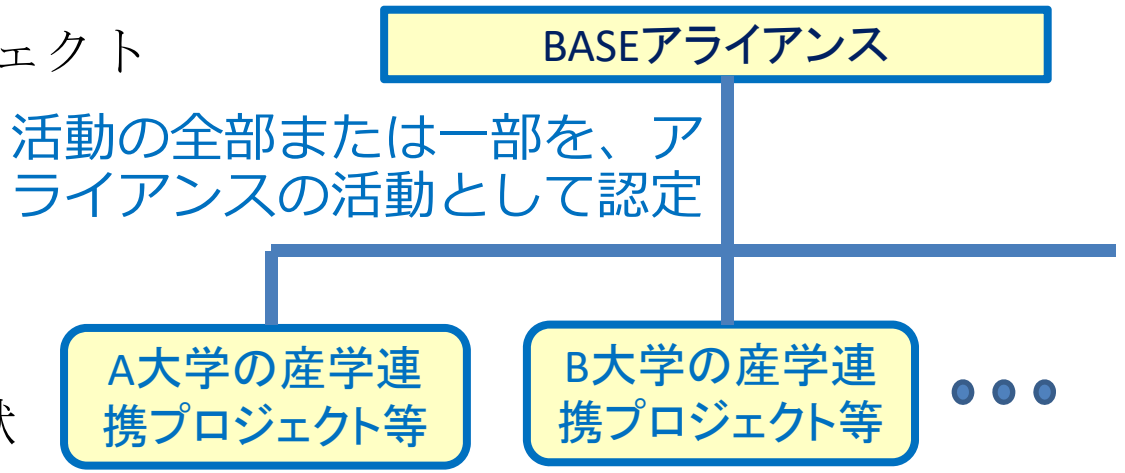
BASEアライアンス

■ Blockchain Academic Synergized Environment: ブロックチェーンの学術研究環境における産学連携のシナジーを意図。オープンな議論を旨とする。

- 慶應義塾大学 SFC研究所 および 東京大学 生産技術研究所 ソシオグローバル情報工学研究センター が設立
- 2017年度は運営方法などを検討し、2018年度から本格的に活動

信頼関係が基礎

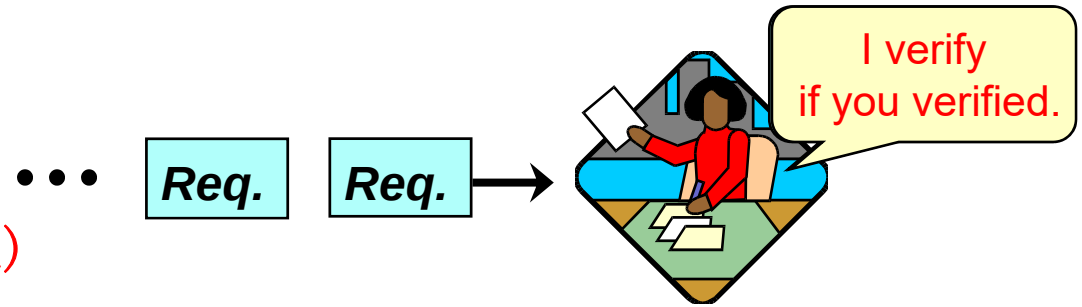
- WG:個別研究プロジェクト
- 研究会
- 公開イベント
- 報告書
- 国際標準化への貢献
- BSafe.networkへの貢献



ブロックチェーンの研究

■ 要素技術や基本的な考え方の多くは、新しくない。

- 電子署名
- ハッシュ関数
- POW (Proof-of-Work)



  - C. Dwork, M. Naor: Pricing via processing or combatting junk mail. CRYPTO 1992.
  - K. Matsuura, H. Imai: Modified aggressive modes of Internet Key Exchange resistant against Denial-of-Service attacks. IEICE Trans. Info. Sys., Vol.E83-D (5), pp.972-979, 2000.
- 追記型記録や証拠の保管と分散した鎖の連携
  - B. Schneier, J. Kelsey: Cryptographic support for secure logs on untrusted machines. 7th USENIX Security Symposium, 1998.

では、一体、何がとくに面白いのか？

エキサイティングなトリプルS

■ 社会(Society)を含むシステム

- 組織、制度、人も（モデル内で）扱う。
- 技術的なアプローチだけでは研究できない。
- 情報セキュリティ経済学（信頼関係を左右する人や組織の行動原理を科学的に研究する有力なツール）が育ってきた。

■ プロトコル一式(Protocol Suite)を含むシステム

- 仕様全てを網羅的かつ詳細に、科学的な厳密さを保って記した資料はまだ無い。
- 伝統的なセキュリティ評価手法だけでは限界がある。

■ シナジー(Synergy)を考えて効果を評価

- コスト削減だけが利点とは限らない。

エキサイティングなトリプルS

■ 社会(Society)を含むシステム

- 組織、制度、人も（モデル内で）扱う。
- 技術的なアプローチだけでは研究できな
- 情報セキュリティ経済学（信頼関 や組織の行動原理を科学的に研究する有 ってきた。

■ プロトコル一式( )を含むシステム

- 仕様全て 細に、科学的な厳密さを保って記した資料

キュリティ評価手法だけでは限界がある。

ンジー(Synergy)を考えて効果を評価

- コスト削減だけが利点とは限らない。

（「分散台帳とその応用技術特別研究会」代表幹事　談）
もちろん応用も面白いですよ！

情報セキュリティ経済学

- **会議(WEIS: Workshop on the Economics of Information Security)を中心とする国際的な研究コミュニティに15年少々の歴史があり、定着してきた。**

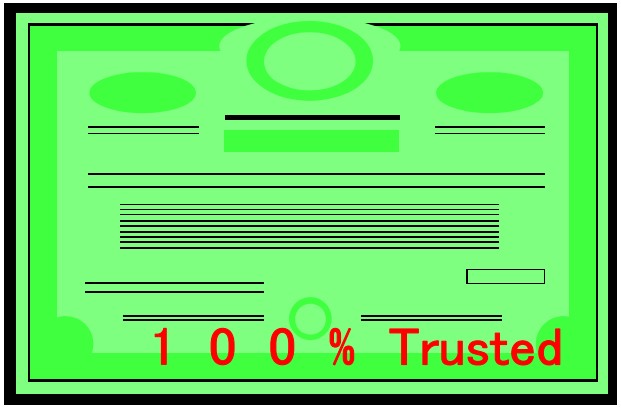
- **理論研究と実証研究が揃ってこそ威力を発揮する。**
  - 情報セキュリティに関するある問題の発生要因が「経済学的最適戦略が直感に反し、人々がそれに従わないこと」にある。この事実を科学的に説明し、直感を正させる。
  - 情報セキュリティに関するある問題の発生要因が「人々が経済学的最適戦略に従うままにしておくと問題が発生するにもかかわらず、それを抑制/回避する社会制度設計などの対策が十分にとられていないこと」にある。この事実を科学的に説明し、十分な対策を促す。

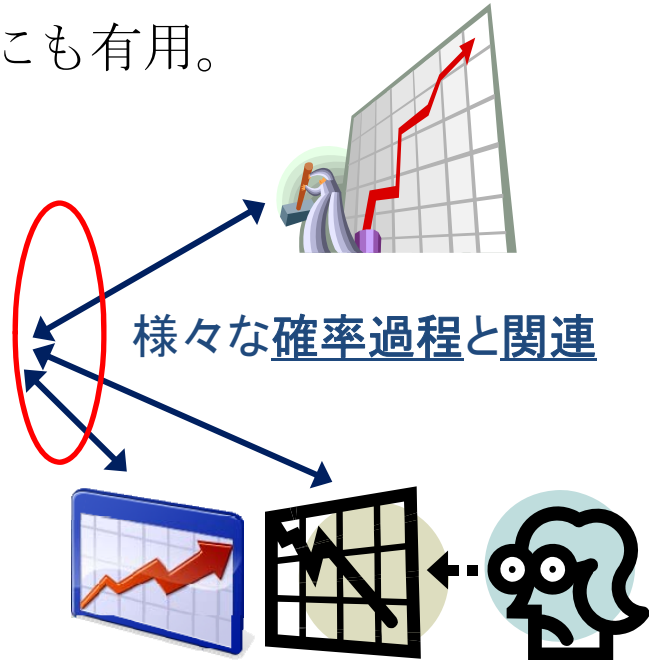
仮想通貨も従来から研究対象

■ 抽象化されたトークンとその金融派生商品の評価

- K. Matsuura: Digital security tokens and their derivatives. Netnomics, Vol.5, No.2, pp.161-179, 2003.
- 応用： 観測できるデータから、逆問題を解いて、リスク管理に必要なパラメータを推定する。制度設計にも有用。

When I obtain ,



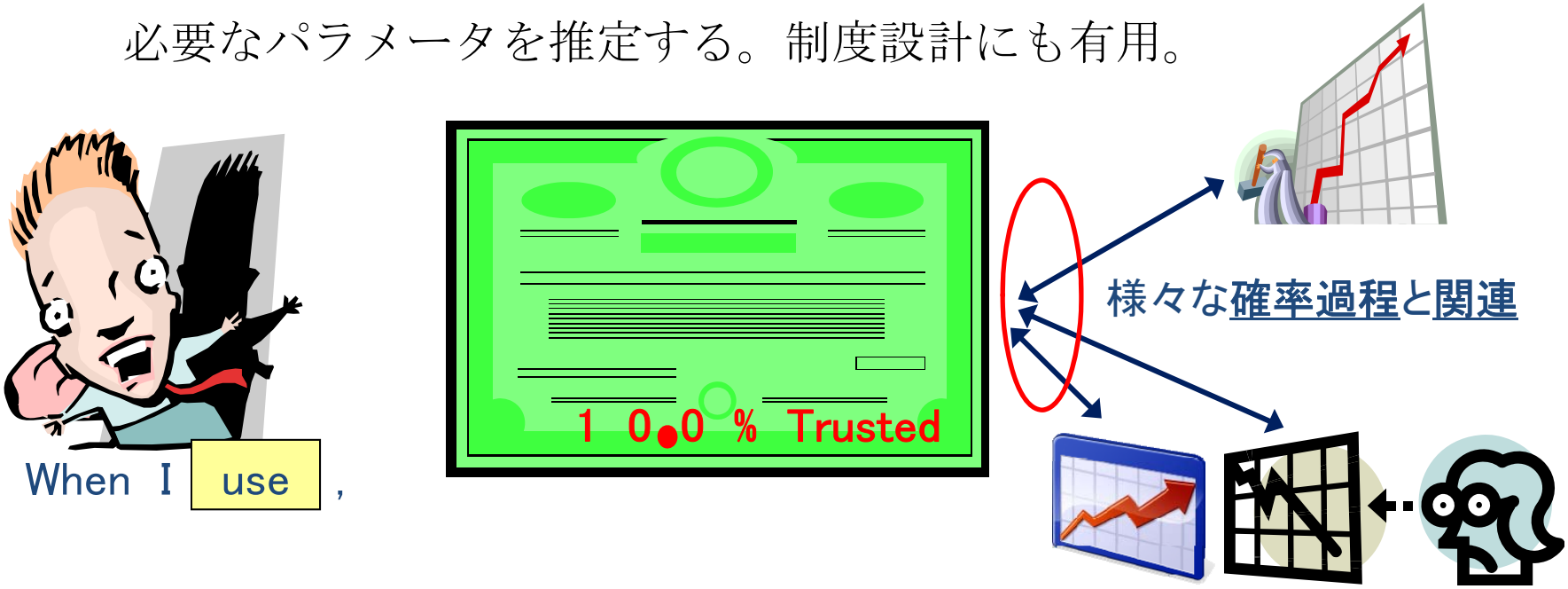


（個々の時刻での値はその時刻が来れば確定するが、事前に正確に予測することはできない。）

仮想通貨も従来から研究対象

■ 抽象化されたトークンとその金融派生商品の評価

- K. Matsuura: Digital security tokens and their derivatives. Netnomics, Vol.5, No.2, pp.161-179, 2003.
- 応用： 観測できるデータから、逆問題を解いて、リスク管理に必要なパラメータを推定する。制度設計にも有用。

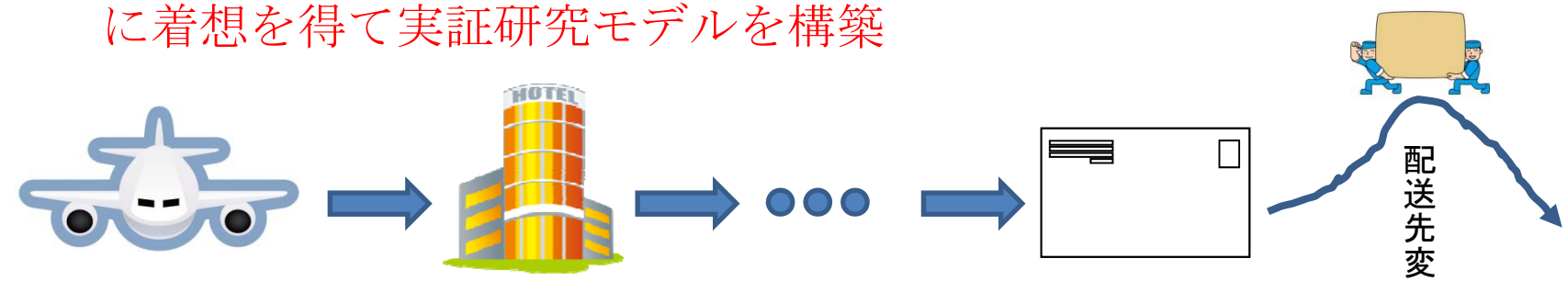


（個々の時刻での値はその時刻が来れば確定するが、事前に正確に予測することはできない。）

ブロックチェーンの応用研究と好相性

■ Loyalty Program（ポイント制度やFFP）のセキュリティ

- B. Jenjarrussakul, K. Matsuura: Analysis of Japanese loyalty programs considering liquidity, security efforts, and actual security levels. WEIS2014.
- 情報セキュリティ投資理論（「攻撃が生起する確率」として定義される「脅威」と、「攻撃が生起したという条件の下で、攻撃が成功し被害が発生する条件付き確率」として定義される「脆弱性」を分けて定式化）に着想を得て実証研究モデルを構築



■ Bitcoinに関する地道な実証分析も色々ある。

- N. Gandal et.al.: Price manipulation in the Bitcoin ecosystem. WEIS2017.

セキュリティ評価手法

- 証明可能安全性（数学的／暗号学的に困難な問題に帰着）
- 情報理論的な評価
- プロトコルの形式検証
- 実験的評価

情報セキュリティには、さらに、特有の悩みがある。

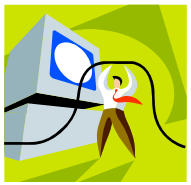
評価の前提が有効と主張できる根拠は？

「あの偉い先生の論文もこうでした」

「エッ、他に何かあるんですか？」

評価手法が有効と主張できる根拠は？

「できるだけ本格的にやりました」



実験したら、防御できました！

研究用のデータ

■ 正規データにまつわる問題

- 個人のプライバシー
- 法人等の機密
- 一般性

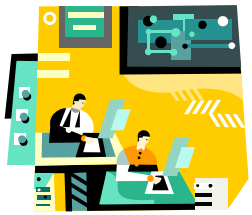
■ 不正データにまつわる問題

- 悪用の恐れ
- 悪用を懸念してデータを提供しない
- ケルクホフスの原則を満たさない
- 問題を解決しようとすると、閉じた世界になりがち（科学に必要な公開性とのトレードオフ）

防御方式を知った上で破るべく工夫してくる攻撃者に対して安全かを調べるべき。

１つの試み：MWS

- **MWS組織委員会（情報処理学会CSEC研究会内）設立趣意書（松浦, 篠田. 2011）**
  - 「インターネットの世界では毎日のようにより巧妙な仕組みを取り入れたマルウェアの亜種や新種が登場している。このような環境の中で、マルウェア対策の研究を発展させていくためには、最新のマルウェア検体を入手し、そのプログラムを解析し感染や被害に至る仕組みを解明し、それら研究成果の情報共有を行う取組が求められる。・・・」
- **制度設計の観点では、人材育成への配慮が重要**
  - 年次ワークショップの特徴：解析競技会併設



技術点と芸術点で評価

防御者の生産性を高める協働

- **第一段階：　直接的あるいは間接的な協働が研究者の間で広まっている状態**
- **第二段階：　実務家も含めて広まっている状態**
  - MWSは第二段階に近い
- **第三段階：　一般ユーザも含めて広まっている状態**
  - 攻撃者の協働は、既に第三段階にある（インターネットを取り巻く環境の進歩で、攻撃側の生産性は格段に高まっている）。
    - 優れた攻撃者はごく少数。しかし、攻撃ツールが出回れば・・・
    - 実世界では理性が勝る人の場合でも、サイバー空間で扇動されれば・・・

防御側にも革命的な生産性の向上が必要（防御者革命）

（cf. メーカー・ムーブメント）

防御者革命のコンセプト

- 情報セキュリティ分野において研究・開発・評価・実用化が織り成すサイクルの生産性を「インターネットも活用して、防御側に生産性向上の革命が起きたと言えるほどまでに」高める。
- サイバー・リアルの協働（正々堂々）
  - 攻撃者革命（？）に対するアドバンテージ
  - ソーシャルキャピタル（松浦：サイバーリスクの脅威に備える，化学同人，2015）

- リアルの組織化だけでは限界がある。
  - BASEアライアンスの今後の活動のうち、国際的なテストネットワークであるBsafe.networkへの貢献には注目すべき。

ブロックチェーンの未来

- 夢を持って未来へ向かう。
- 未来を担う人の関心を多く惹きつける。
  - トリプルS(Society, Protocol Suite, Synergy effects)に科学的に取り組むことは、エキサイティング。
- IT分野からのノーベル賞？
  - 経済学賞、医学・生理学賞、平和賞
- BASEへの期待
  - 「日本版XX」ではない。
  - 情報セキュリティとは相思相愛
  - 防御者革命の推進（正当な利用者の生産性を高め、社会の活力を増し、幸福をもたらす）