認証基盤から見た
情報システムの信頼と
トラストフレームワークの抽象化

セコム(株)IS研究所
島岡政基

本講演専用の資料となりますので、
第三者への開示、転用はお控えください。

情報システムにおける信頼の重要性

信頼される安心を、社会へ。SECOM

- ビジネス・サービスの多様化・複雑化
  - 属人的→システム的
  - ステークホルダーの多様化、情報の非対称化
  - プライバシーなど法・社会・倫理的問題(ELSI)
- ICT技術の発展・普及・社会基盤化
  - ICT基盤のクラウド化
  - サイバー空間と実社会の融合
  - 急速な普及 vs. 社会受容性

ビジネスやサービスを単純化して
理解することが難しくなっている。

↓

現代社会で生活するには、専門能力を持つ
ヒトや組織などを「信頼」せざるを得ない

本発表の概要

- 「信頼」の研究トピック
  - 信頼とはそもそも何なのか
  - 何が信頼を構成するのか
  - 信頼は管理し得るのか(割愛)
- 認証基盤から学ぶ信頼
  - Web PKI
  - 認証連携と
    トラストフレームワーク
- 情報システムへの適用
  - トラストフレーワークの抽象化
  - トラストコントロール
  - ユースケース(割愛)
    - 匿名加工情報の提供
    - 暗号アルゴリズムの信頼性評価
- 議論

「信頼」の研究トピック

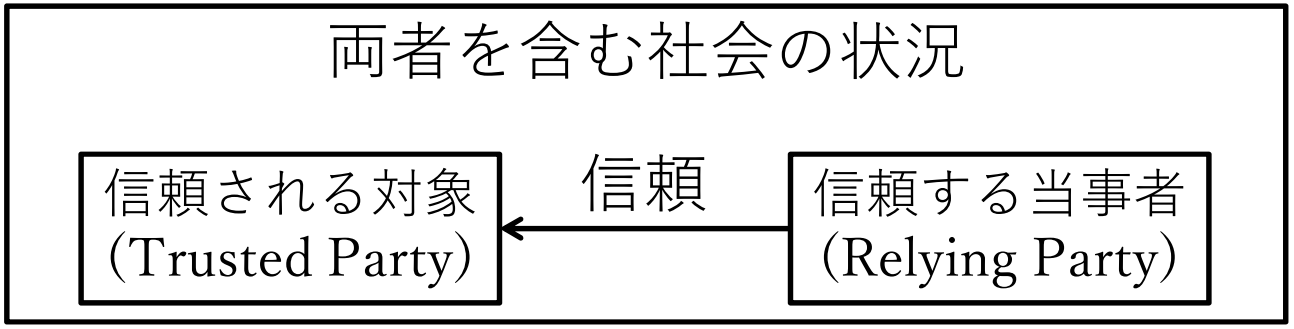
- 信頼とはそもそも何なのか
- 何が信頼を構成するのか
- (信頼は管理し得るのか)

本発表が扱う信頼のスコープ

trust: degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

— ISO/IEC 18014-2:2009

意訳：ユーザまたはその他のステークホルダーが、その製品又は
システムが期待した通りに振る舞うと信ずる度合い



[2]をもとに筆者が作成

[2] 千葉隆之「信頼の社会学的解明に向けて」年報社会学論集9号212頁(1996年)

信頼とはそもそも何なのか

完全に知っている者は信頼する必要はないし、完全にまったく知らない者は、当然のことであるが、信頼することなどできない

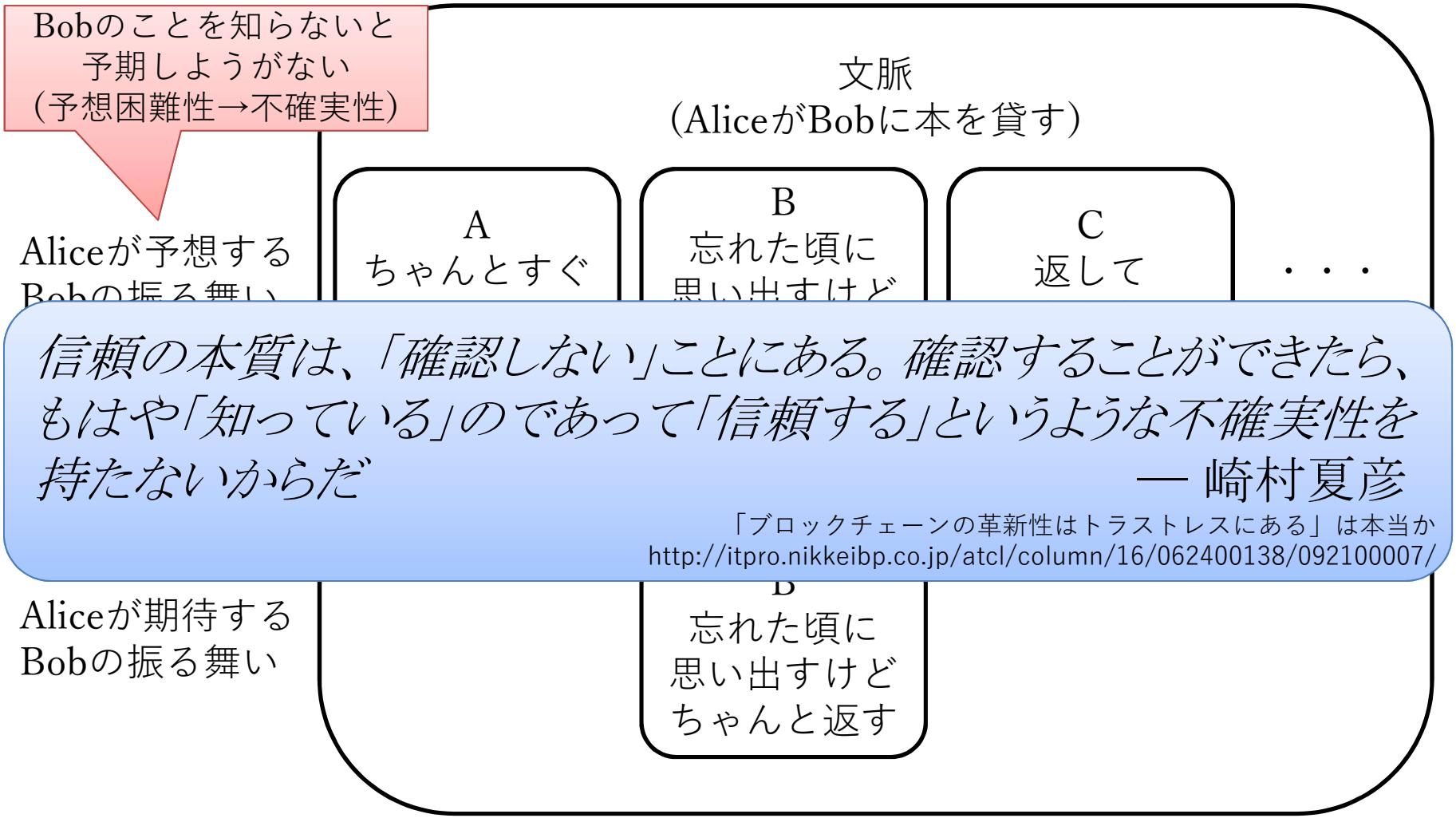
— G. Simmel [3]

信頼は、社会的な複雑性を縮減するメカニズムである

— N. Luhmann [4]

[3] Simmel, G.: *Philosophie des geldes*, Berlin: Duncker&Humblot. (1900). 居安正訳: 貨幣の哲学, 白水社(1999).
[4] Luhmann, N.: Vertrauen: ein Mechanismus der reduktion sozialer Komplaxitat, Ferdinand Enke Verlag(1968).
大庭健, 正村俊之訳: 信頼—社会的な複雑性の縮減メカニズム, 勁草書房(1990).

信頼とは(島岡版解釈)



信頼の本質は、「確認しない」ことにある。確認することができたら、もはや「知っている」のであって「信頼する」というような不確実性を持たないからだ

— 崎村夏彦

「ブロックチェーンの革新性はトラストレスにある」は本当か
http://itpro.nikkeibp.co.jp/atcl/column/16/062400138/092100007/

何が信頼を構成するのか

信頼される安心を、社会へ。SECOM

■ 伝統的信頼モデル

- 戦後の説得コミュニケーション研究からの成果
- 情報源の信憑性に関する2つの規定因
  - 能力：知識や能力に対する期待
  - 動機づけ：誠実さや公正性、説明責任への期待など

■ SVS (Salient Value Similarity)モデル[9]

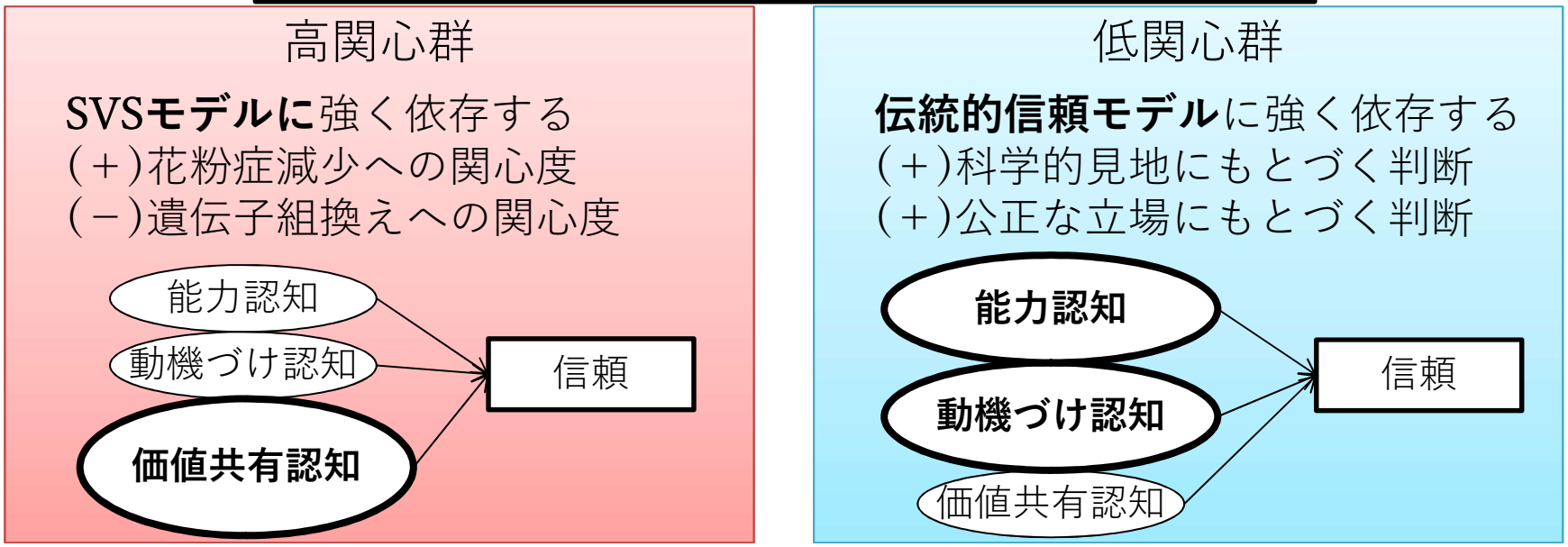
- 古典的信頼モデルで説明できない事象
  - たとえ正しい知識と倫理観を備えていても、主義主張が相いれない専門家は信頼してもらえない
- 能力、動機付けに加えて「価値共有」への期待
  - 共有したい価値はRPによって異なる

[9] Earle, T. C. and Cvetkovich, G.: Social trust: Toward a cosmopolitan society, Greenwood Publishing Group (1995).

SVSモデルと伝統的信頼モデルの統合

- 遺伝子組換えによる花粉症緩和米が開発されたとした際に、その安全性を判断する公的機関に対する信頼をアンケート調査
  - 公的機関は、その安全性や有用性、また生態系への悪影響の有無などを評価した上で、公的機関が商用認可の判断を下すものとする。

花粉症への関心(価値共有)と信頼の相関を分析



[10] 中谷内一也、G. Cvetkovich、「リスク管理機関への信頼：SVSモデルと伝統的信頼モデルの統合」, 社会心理学研究, vol.23, no.3, pp.259-268, 2008

信頼は管理し得るのか

信頼される安心を、社会へ。
SECOM

■ 分散環境におけるトラストの研究動向

- アプリケーションポリシにもとづくアクセス制御[12]
  - 認証はアプリケーションに依存しないが、
    認可はアプリケーションの文脈に依存する
  - 如何にして信頼できるアクセス制御を実現するか
- トラストの定式化[13]
  - 分散AI、マルチエージェントシステムにおける「信頼」の実装
  - エージェント間の信頼構築、信頼の伝搬など

[12] Blaze, M., Feigenbaum, J. and Lacy, J.: Decentralized trust management, *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, IEEE, pp. 164-173 (1996).
[13] Marsh, S. P.: Formalising trust as a computational concept (1994).

認証基盤から学ぶ信頼

- Web PKI
- 認証連携とトラストフレームワーク

PKIの3コーナーモデル

Subscriber(SC)

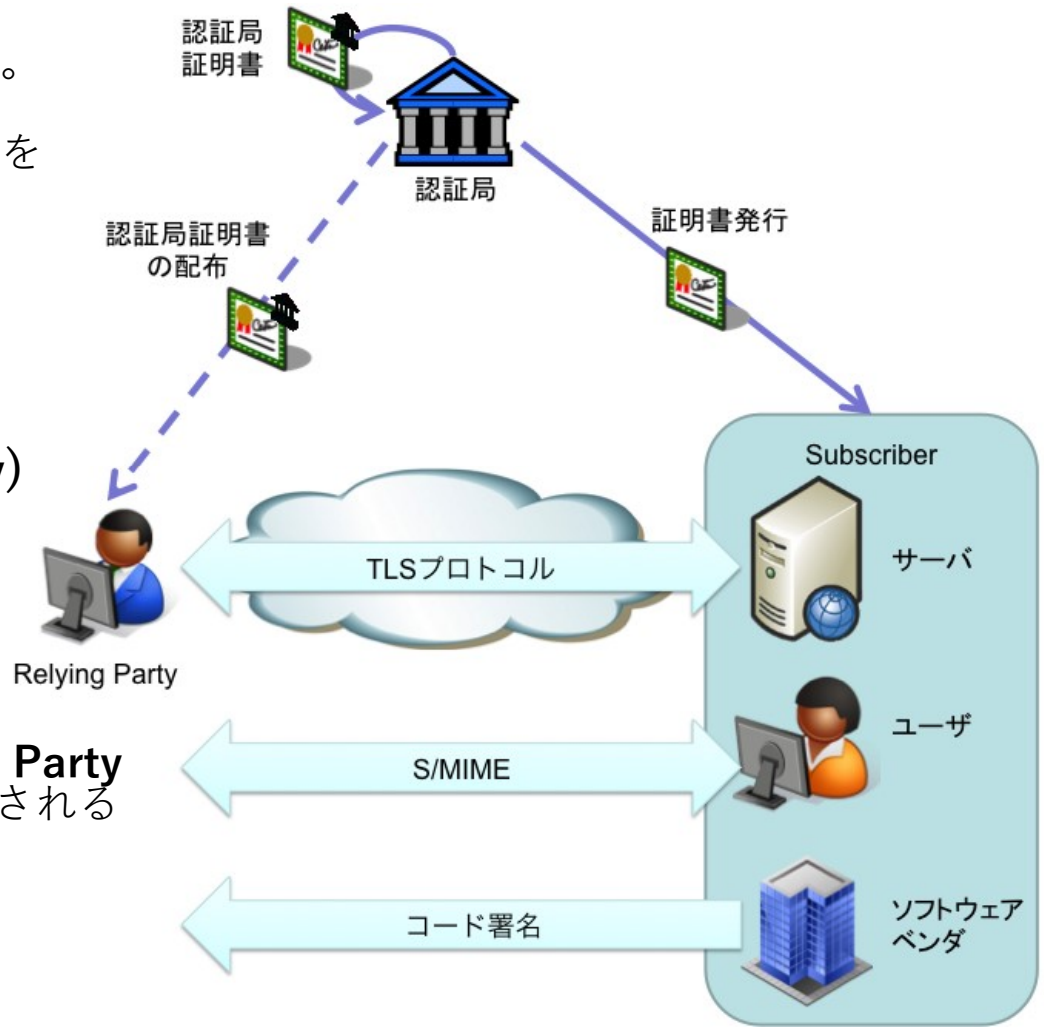
- 鍵ペアオーナー即ち私有鍵を持つ。これまでのTrusted Partyに相当。
- 公開鍵に対して認証局から証明書を発行してもらう

Relying Party(RP)

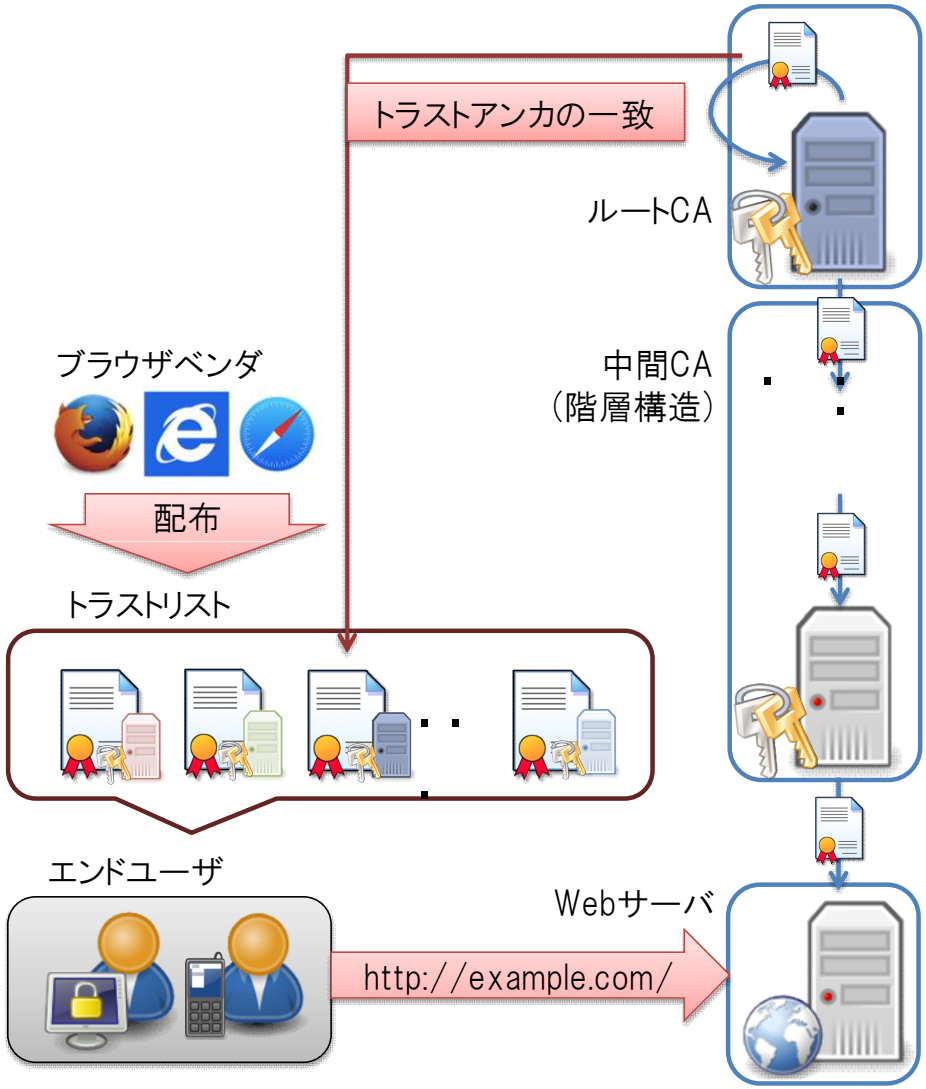
- SCの公開鍵証明書を利用する(暗号化また署名検証)
- 信頼する認証局の公開鍵を持つ

認証局(CA, Certification Authority)

- 自身の鍵ペアを持つ
- SCに証明書を発行する(SCの公開鍵に署名する)
- 証明書発行にあたりSCの**身元確認**を行う義務を負う
- RPから信頼される**Trusted Third Party (TTP)**として振る舞うことが期待される



Web PKIのトラストモデル



- 信頼の連鎖
  - 予めブラウザに登録されたルートCA
  - ルートCAから連鎖するサーバ証明書
- 信頼の根拠
  - 認証局の証明書ポリシ(CP)
  - 認証局運用規程(CPS)
  - 認証局に対する外部監査
  - 国際的な監査基準(WebTrust for CAなど)

CP: Certificate Policy
CPS: Certification Practice Statement

理想的3コーナーモデルからの変容

考察(1) 期待する文脈の明文化

- CP/CPSフレームワーク(RFC 3647)
  - CP/CPSとして記載すべき項目が体系化されている
  - ほぼすべてのルートCAがこれに準拠
- RPに対して認証局が果たすべき責任が明文化されている
  - 認証局による身元確認の厳密性
  - 証明書と紐づく鍵ペア管理の安全性

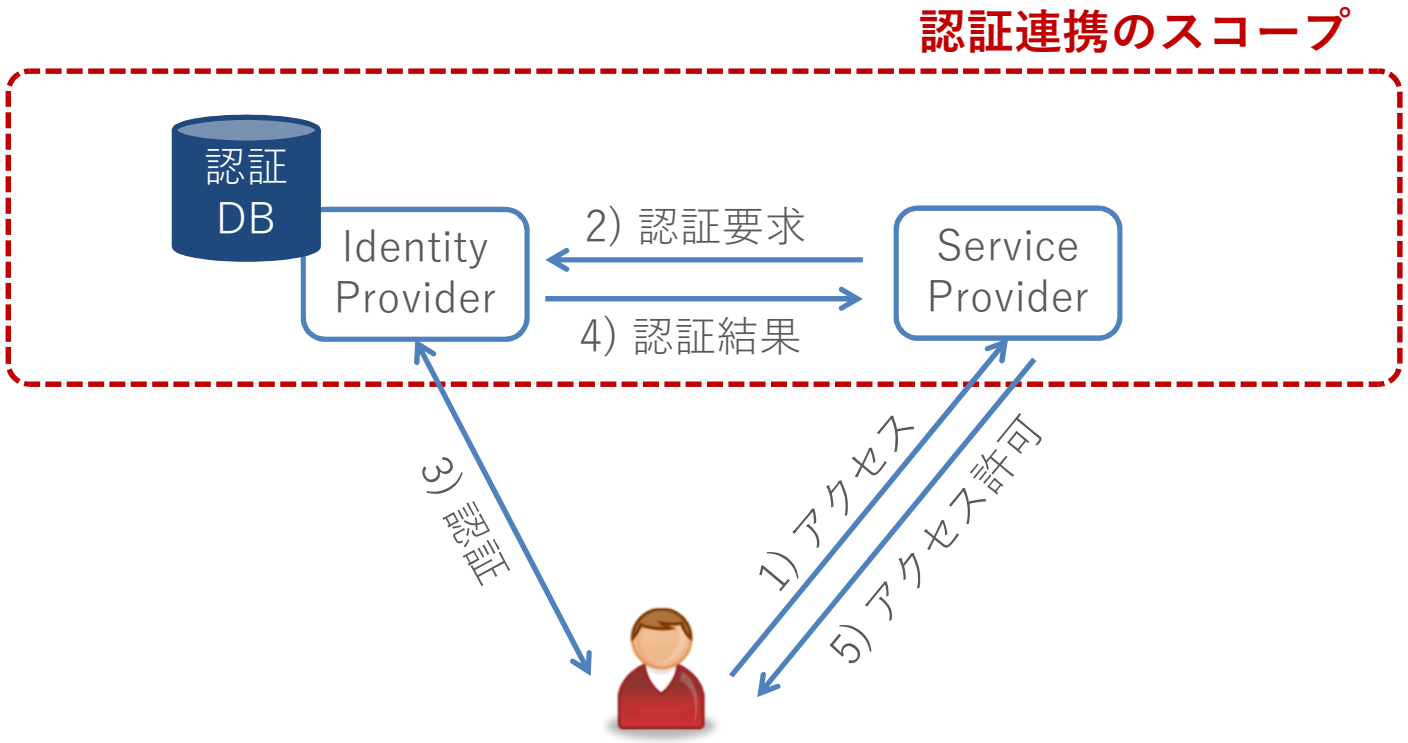
CP/CPS Framework

1. はじめに
2. 発行とリポジトリの責任
3. I&A（身元確認と認証）
4. 証明書のライフサイクル運用的要件
5. マネジメントコントロール、管理的コントールおよび運用的コントロール
6. 技術的セキュリティコントロール
7. 証明書、CRL および OCSP のプロファイル
8. 準拠性監査や他の評価
9. 他の業務事項と法的事項

- CP/CPSに準じたフレームワークの事例
  - DP/DPS (DNSSEC Policy & DNSSEC Practice Statement)
  - IP/KGPS (Identifier Policy & Key Generation Practice Statement)
    など

認証連携

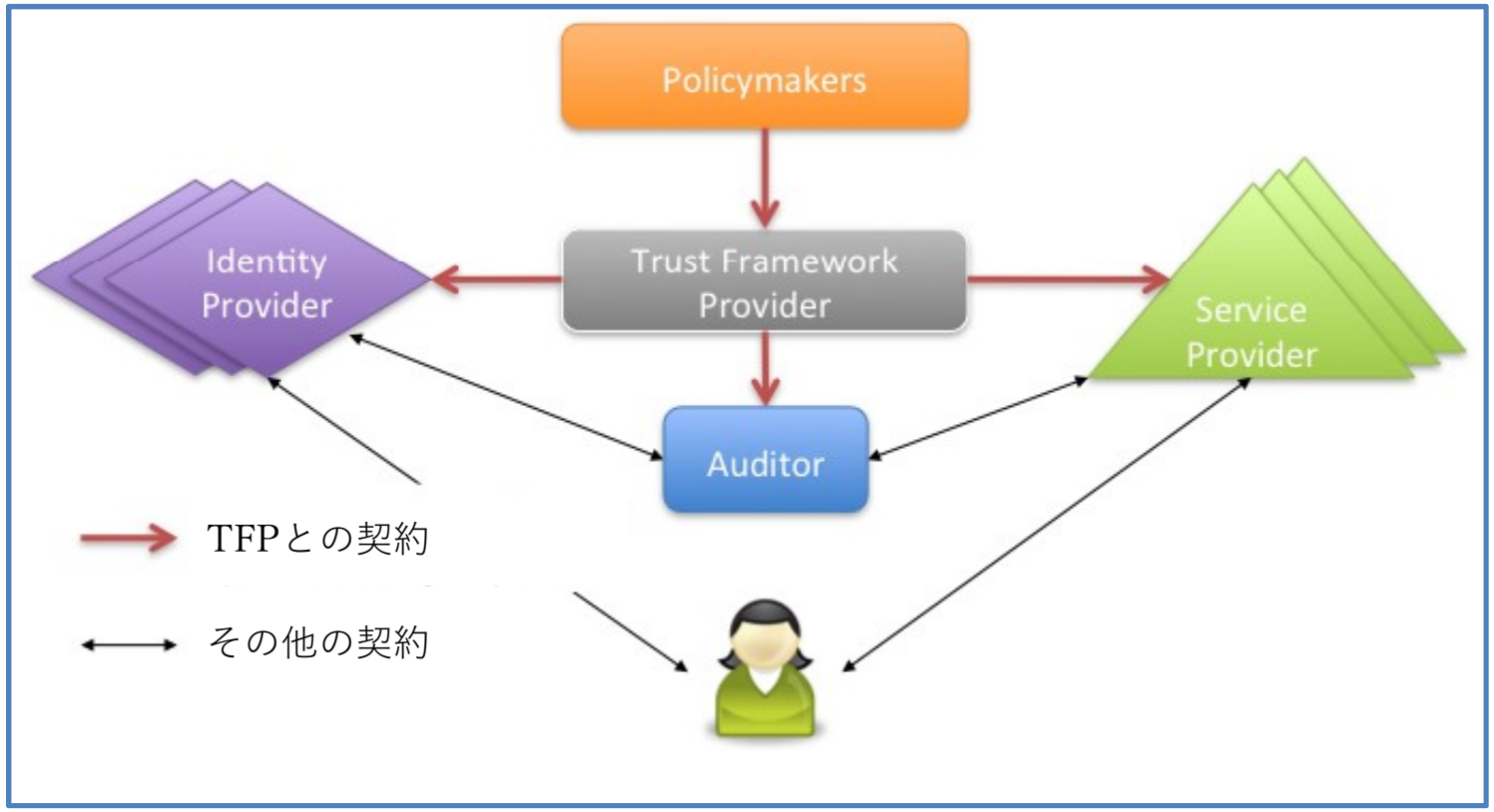
サービス提供者(SP)が、**認証機能を**
第三者である認証事業者(IdP)**に委託**するモデル



IdPが提供する認証結果を、SPが信頼するモデル

(アイデンティティ)トラストフレームワーク

- IdP/SPが増えてもスケール可能なフレームワーク
- 各IdP/SPに共通の，一定のルールと技術仕様の策定
- 監査人による準拠性の確保



[15] Eve Maler, et al.「Open Identity Trust Framework Model」（2010）

考察(2) 能力の形式化

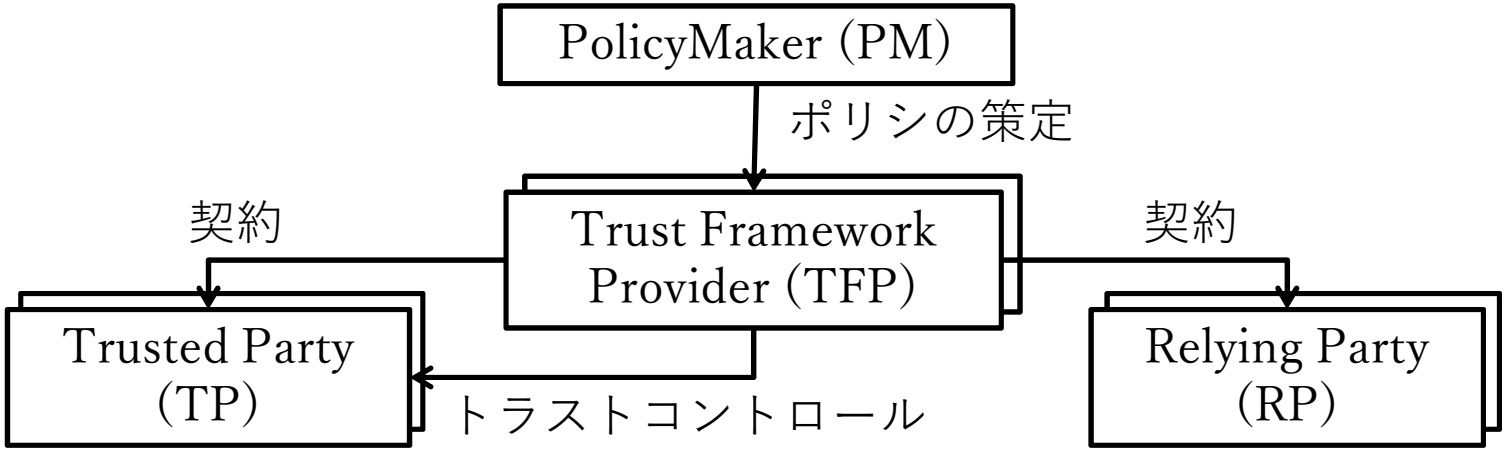
- 能力をどのように認知させるか
  - 資格や免許
  - 準拠性監査や認定制度
- CP/CPSなどをより認知しやすい形に

	Web PKI	(認証連携) トラストフレームワーク
形式化	WebTrust for CA (パブリックルート)	トラストフレームワーク
準拠性の確認	ブラウザベンダ	TFP
TPが準拠する ポリシ	CP/CPS	ポリシ

情報システムへの適用

- トラストフレームワークの抽象化
- トラストコントロール
- ユースケース
  - 匿名加工情報の提供
  - 暗号アルゴリズムの信頼性評価

トラストフレームワークの抽象化



- ポリシを策定するPM
- ポリシに準拠してTFを運営するTFP
  - ポリシに準拠するTFP規準を策定
- 任意のTFに参加するTP,RP
  - TFP規準に準拠することが要件

トラストコントロール：
継続的な準拠性を
確認(担保)する方法

TFを用いることで、TPの能力(準拠性)と動機づけ(義務)が
RPに認知されやすくなると期待できる

トラストコントロールの例

トラスト コントロール	利点/欠点
外部監査 (external audit)	○ 質の高いコントロールが可能 × スケーラビリティが弱い (監査人育成や監査コストなどの費用と期間の問題)
自己査定 (self-assessment)	○ キャッシュアウト不要 × 育成コスト、査定期間などのリソースを適切に 割り当てられないリスク
相互評価 (peer review)	○ 外部監査と自己査定のいいとこどり × 互恵的に振舞うリスク
評判システム (reputation system)	○ 低コスト(質を量でカバー)、生の声を集めやすい × 有意な数が必要、質の維持 (必ずしも本質的な評価と一致しない)

ユースケースへの適用

信頼される安心を、社会へ。
SECOM

■ 匿名加工情報の提供

- パーソナルデータを安心して利活用できる仕組み
- この仕組みが信頼を得るには何が必要か

■ 暗号アルゴリズムの~~信頼~~安全性評価

- 暗号製品を安心して利用できる仕組み
- この仕組みが信頼を得るには何が必要か

「匿名加工情報」制度

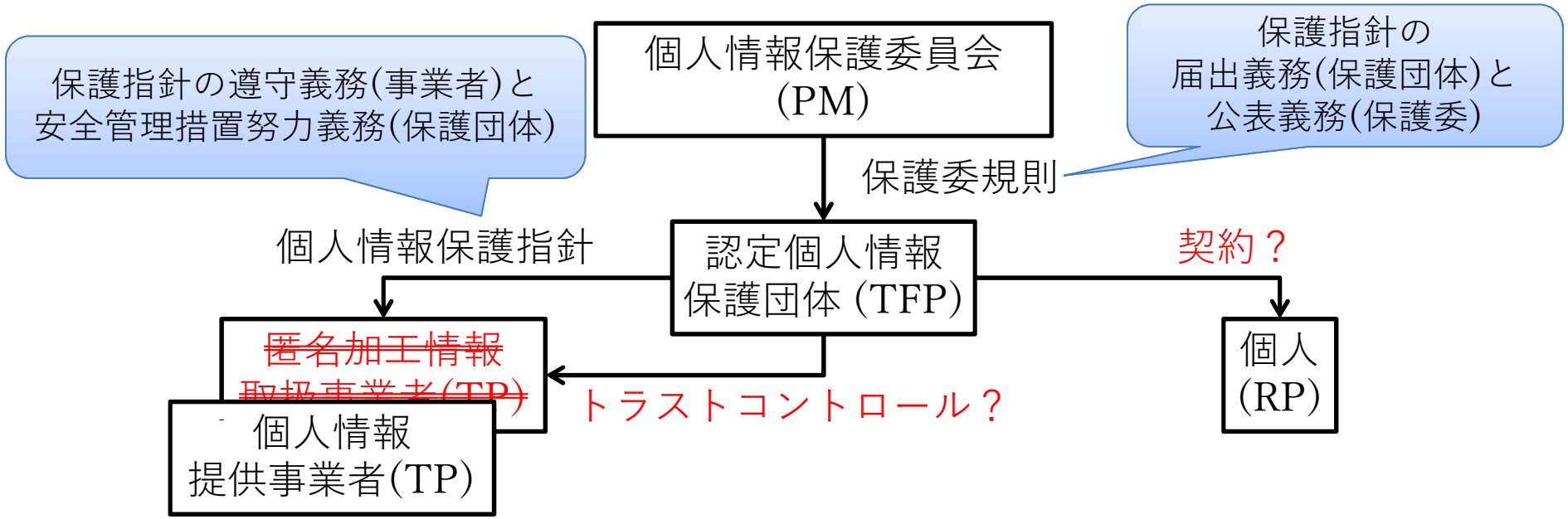
信頼される安心を、社会へ。
SECOM

■ 匿名加工情報とは

- 個人情報を匿名化することによって、本人同意に代わる一定の条件の下、第三者提供を可能とするもの
- プライバシー侵害を生じない程度の安全性が必要
- 加工の程度は事業内容や利用形態等によって異なるため、一律の規準はない

加工の程度を決める指針と、
指針を定める(業界)団体の必要性

(1) 匿名加工情報の提供



○　保護指針の届出・公表 →保護指針の明文化、認定団体の動機付け
？　認定団体の能力
？　取扱事業者へトラストコントロールの具体性
？　匿名加工情報の流通頻度
？　個人にとって信頼すべきは事業者か保護団体か

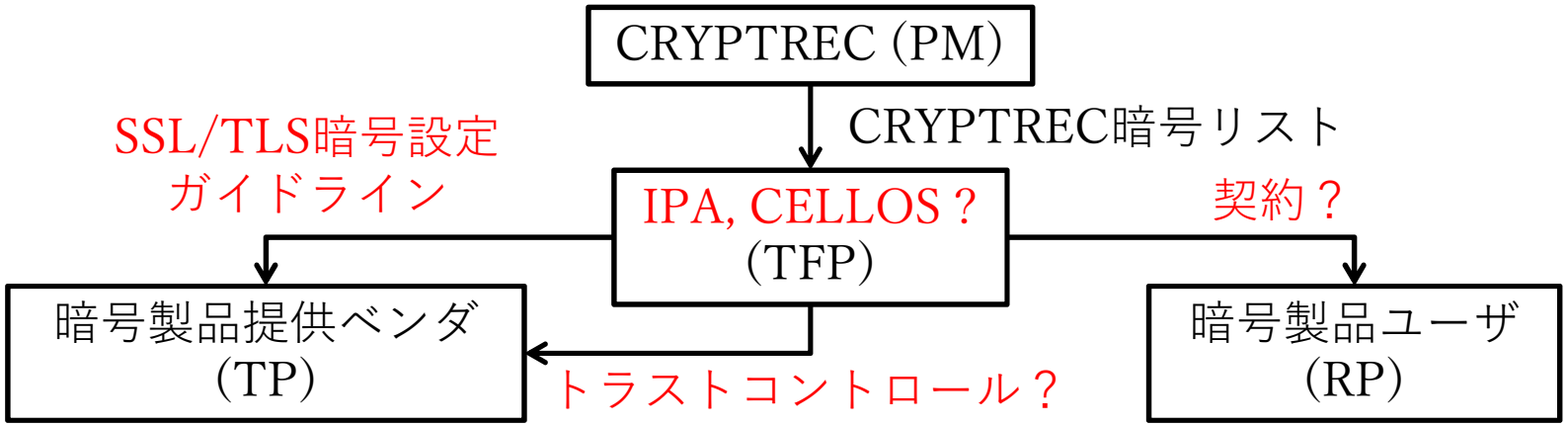
暗号製品における信頼の重要性

信頼される安心を、社会へ。 SECOM

- 暗号製品を安心して利用できる社会に向けて
  - 暗号設定の難しさ、暗号技術の脆弱性問題など
  - 暗号技術に対する安全性評価の難しさ
    - 必要な知識・技術、希少なリソース、有限の時間など
  - 安全性の高い暗号技術を、適切な設定で利用するための適切なポリシの策定とその遵守
- CRYPTREC暗号リスト
  - 電子政府に用いる安全性の高い暗号アルゴリズムのリスト
  - CRYPTREC(暗号技術検討会)が評価・公開
- SSL/TLS暗号設定ガイドライン
  - 同リストをもとに電子政府以外も対象としたガイドライン

アプリケーションレベルで一定の準拠性を期待できるフレームワーク・ポリシが未成熟

(2) 暗号アルゴリズムの安全性評価



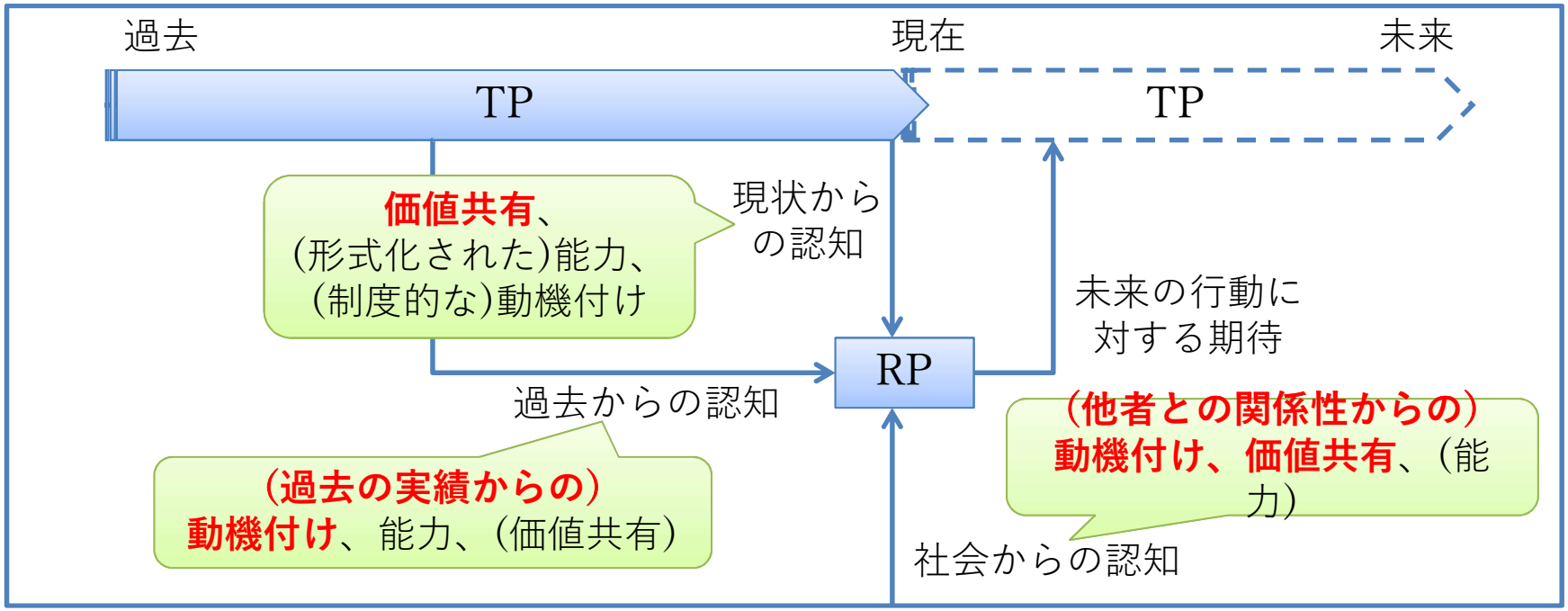
○　CRYPTRECの能力の外形化←電子政府の安全性評価

×　TFP不在(IPAやCELLOSは限定的&結果論)
　　制度設計・インセンティブ設計の不在

×　ベンダとTFPの契約(または合意)→準拠性、トラストコントロール不在

？　SSL/TLS以外はどうするのか

考察：時間軸で見た信頼とその規定因



素朴な疑問

過去のない新参TPは、果たして
どのように信頼を確立すればよいのか？

- 形式化された能力
- (制度的な動機付け)
- 価値共有

能力や動機付けは重要ではないのだろうか？

- 能力の形式化が難しい時は？
- 制度不在・(認知)未成熟な時は？

信頼の継続における価値共有の課題

信頼される安心を、社会へ。SECOM

■ 確立した信頼を継続することを考える

- 各規定因の時間安定性が重要
- 能力・動機付けは(価値観よりも)変化しにくい
  - 一朝一夕に持つことはできない
  - 動機付けは社会にも依存するが、社会変化は一般に緩やか
- TPの価値観が一概に時間安定とは言いにくい
  - 時間安定だとしたら、それはむしろ動機付けではないか
- RPの価値観もまた必ずしも時間安定とは言いにくい

信頼の継続においては能力や動機付けの方が効いてくるのではないか

まとめ

- 認証基盤の事例をもとに情報システムにおける信頼の実装を分析した
- トラストフレームワークを抽象化した汎用トラストフレームワークを提案した
- 汎用TFをユースケースに適用し、信頼確立のための分析に資することを示した
- 信頼の継続における問題提起