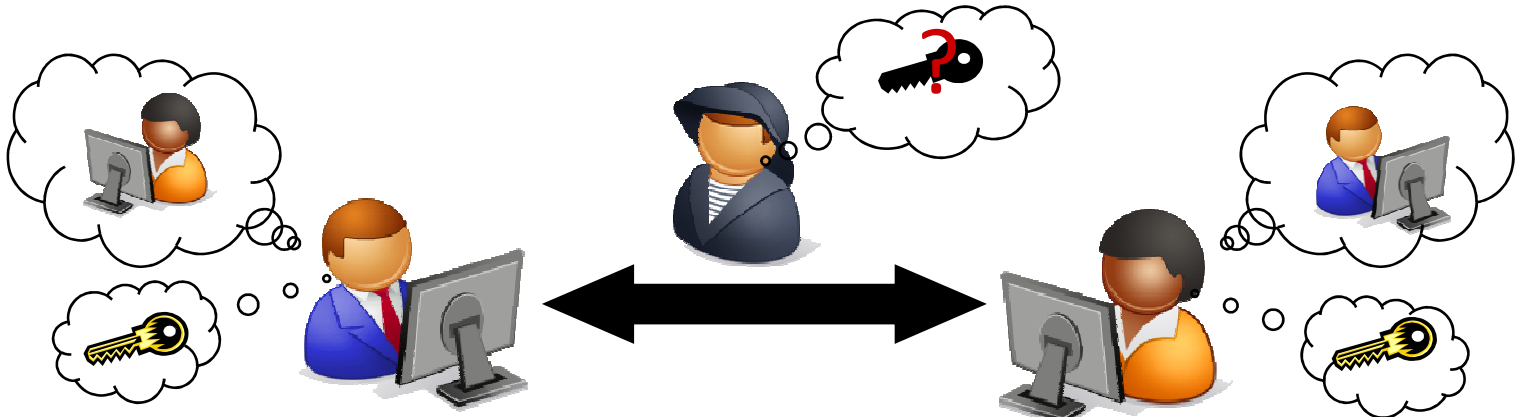
汎用的結合可能な鍵交換の安全性検証法

鈴木 斎輝，吉田 真紀，藤原 融
大阪大学 大学院情報科学研究科

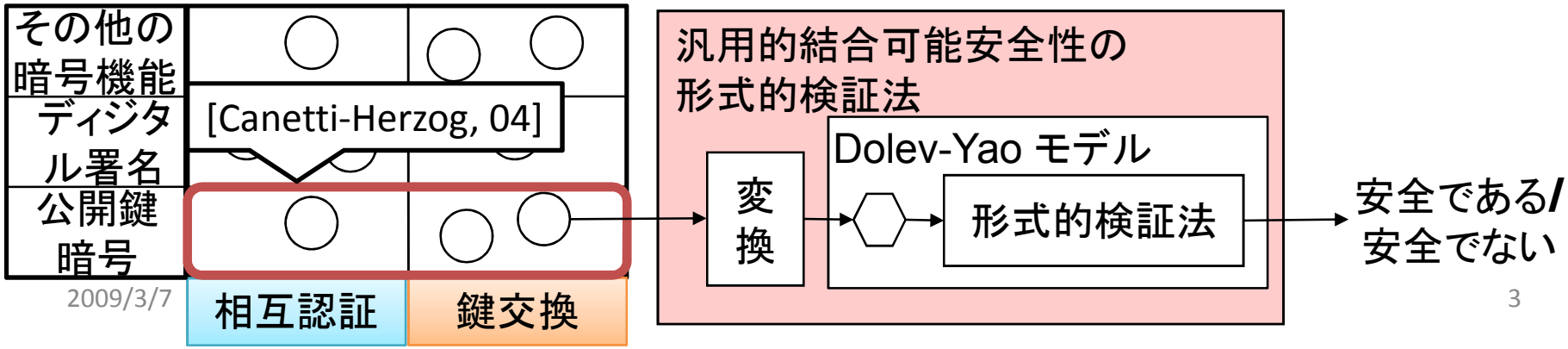
研究の背景

- さまざまな暗号機能を実現するプロトコルの利用
  - –例：相互認証、鍵交換
- 複数のプロトコルが組み合わされて実行
- そのような状況を想定した安全性の証明が必須
  - –単体では安全でも、組み合わせによって安全でなくなる可能性



結合可能性を保証する安全性

- 組み合わせて実行しても損なわれない安全性
- [Canetti, 01] 汎用的結合可能性の枠組みの提案
  - 広く利用されている
- [Canetti-Herzog, 04] 自動証明のための最初の形式的検証法の提案
  - 公開鍵暗号を利用した相互認証・鍵交換プロトコルを対象
  - 既存の記号的モデル [Dolev-Yao, 83] に基づく
  - 健全性証明
    - 検証結果が安全であれば、検証対象プロトコルは安全

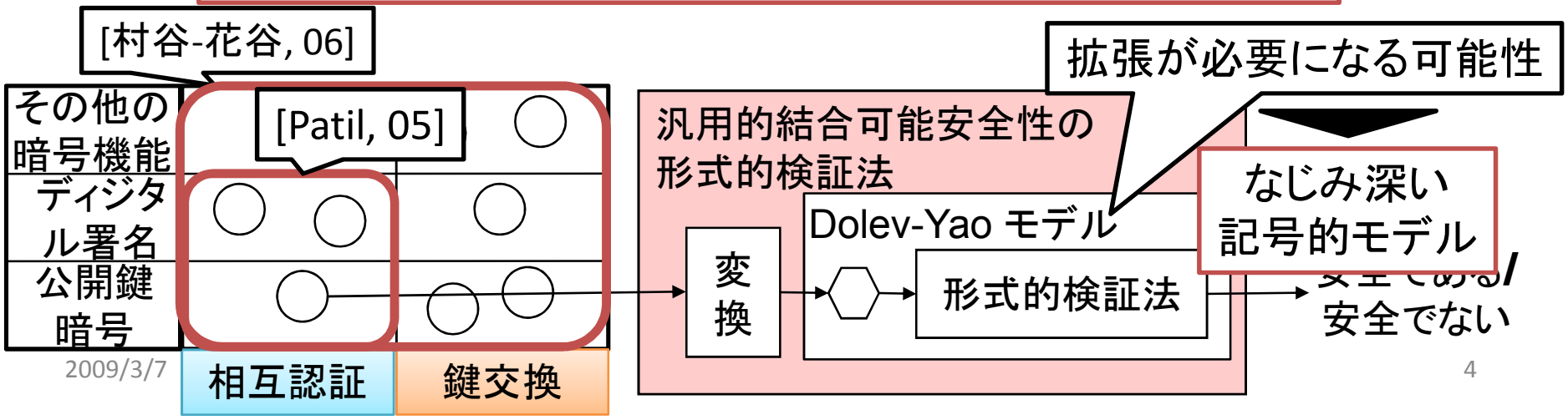


従来研究

- [Patil, 05] 公開鍵暗号とディジタル署名を利用した相互認証プロトコル
- [村谷-花谷, 06] 任意の暗号機能を利用した相互認証・鍵交換プロトコル

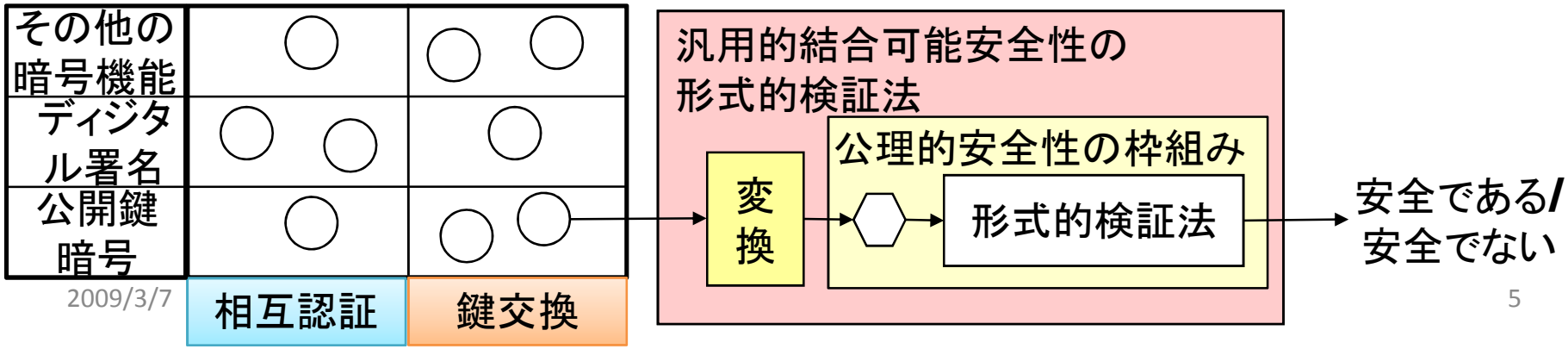
プロトコルが利用可能な暗号機能は豊富

今後の課題は相互認証・鍵交換プロトコル以外も検証可能にすること



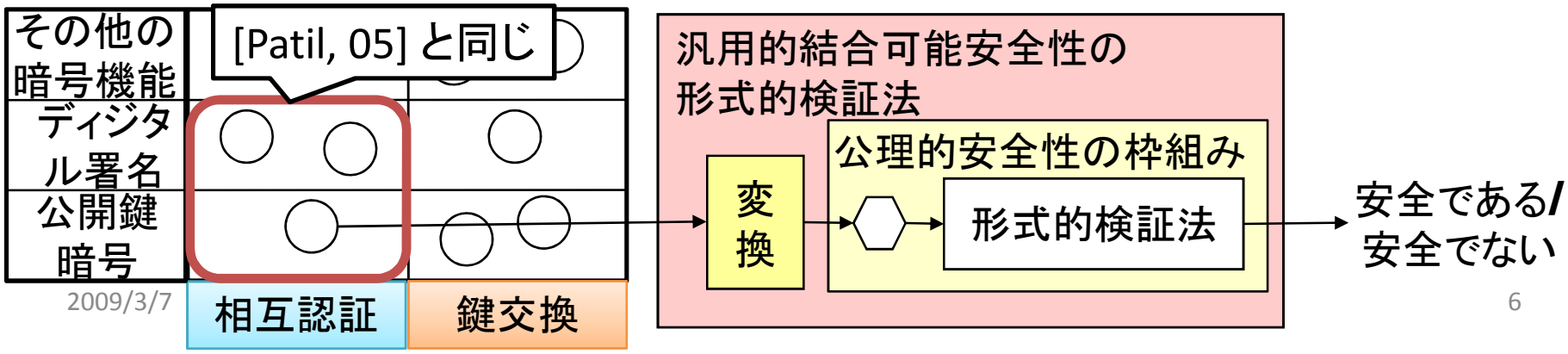
本研究で利用する記号的モデル

- 公理的安全性の枠組み
  [藤原-谷口-嵩, 86] [吉田-藤原, 98]
  - 著者らのグループが提案
  - 多様な暗号機能を直観的に記述することが目的
  - 既存の記号的モデル [Dolev-Yao, 83] の拡張



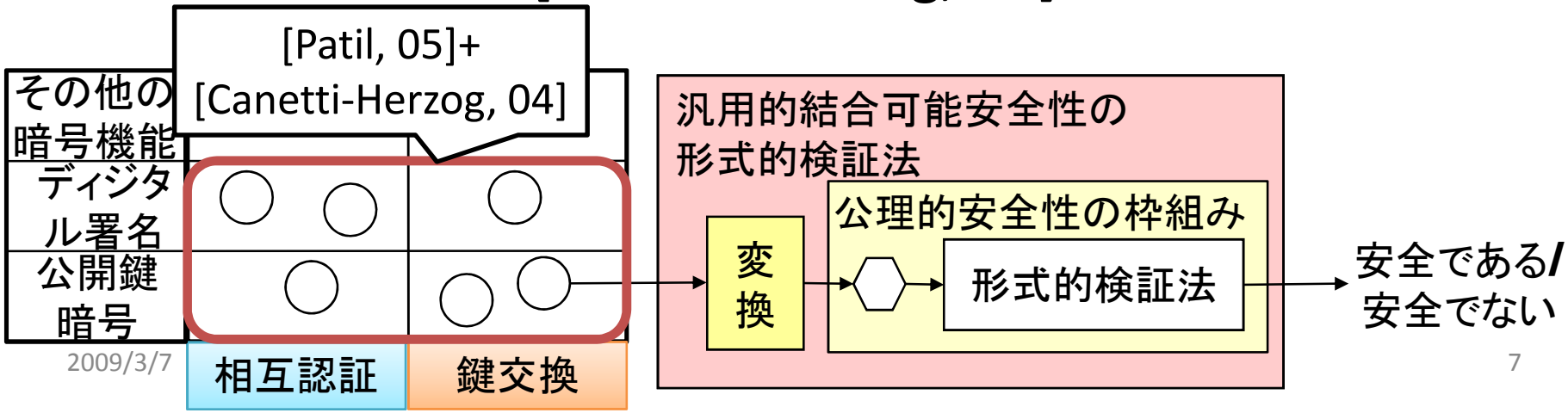
SCIS 09 の結果

- 公理的安全性の枠組みが汎用的結合可能安全性の形式的検証に利用可能であることを確認
  - [Patil, 05]と同様、公開鍵暗号とディジタル署名を利用した相互認証プロトコルを対象
  - 公理的安全性に基づく相互認証の安全性を定義
  - プロトコル記述の変換を提案
  - 健全性証明（ [Patil, 05]と同様の方針）



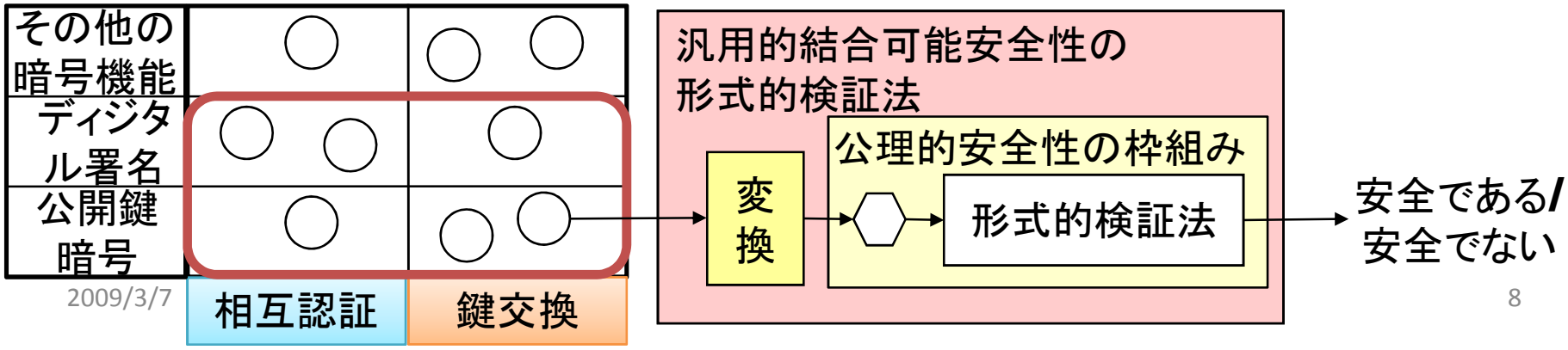
本発表の目的と内容

- 目的
  - 検証対象プロトコルの拡張
    - 今後の検証対象プロトコルの拡張のための知見を得る
- 内容
  - 公開鍵暗号とディジタル署名を利用した鍵交換プロトコルを対象（[Patil, 05] + [Canetti-Herzog, 04]）
  - 鍵交換に対応する公理的安全性を定義
  - プロトコル記述の変換を提案
  - 健全性証明（ [Canetti-Herzog, 04]と同様の方針）



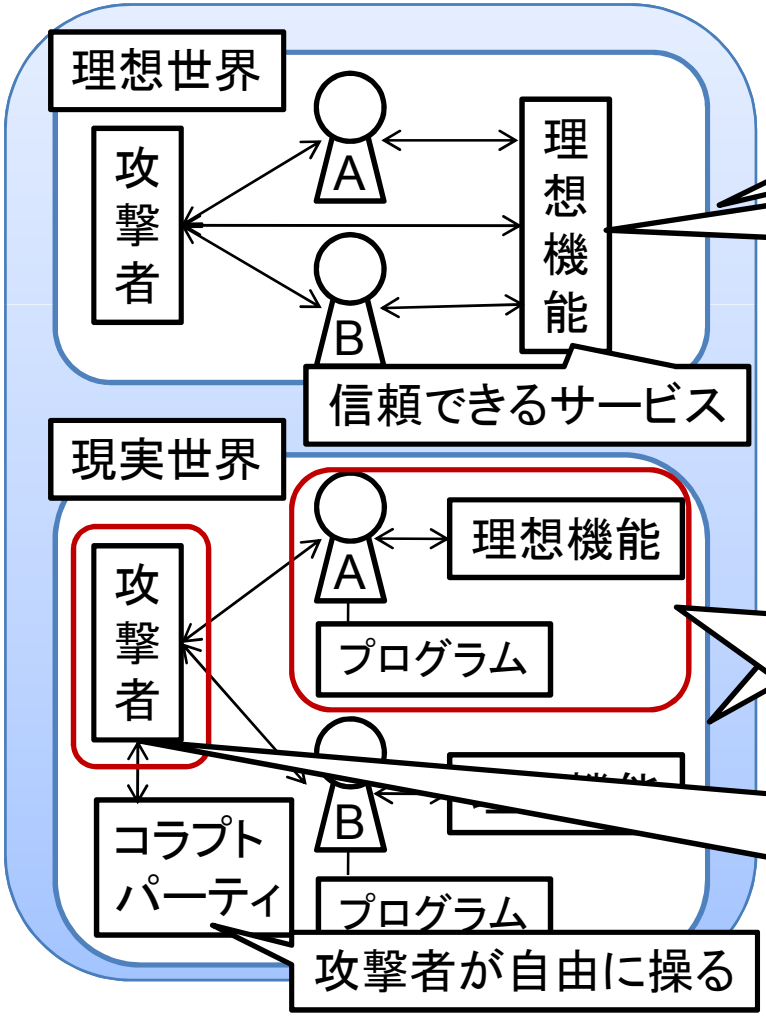
以降の発表の流れ

- 汎用的結合可能性の枠組み
- 公理的安全性の枠組み
- 提案する変換
- まとめと今後の課題



汎用的結合可能性の枠組み
モデル

- 2つの世界が定義される



目標とする暗号機能を理想的に実現した世界

鍵交換理想機能：プロトコルを実行するパーティだけにランダムに選択された共通の鍵を与える

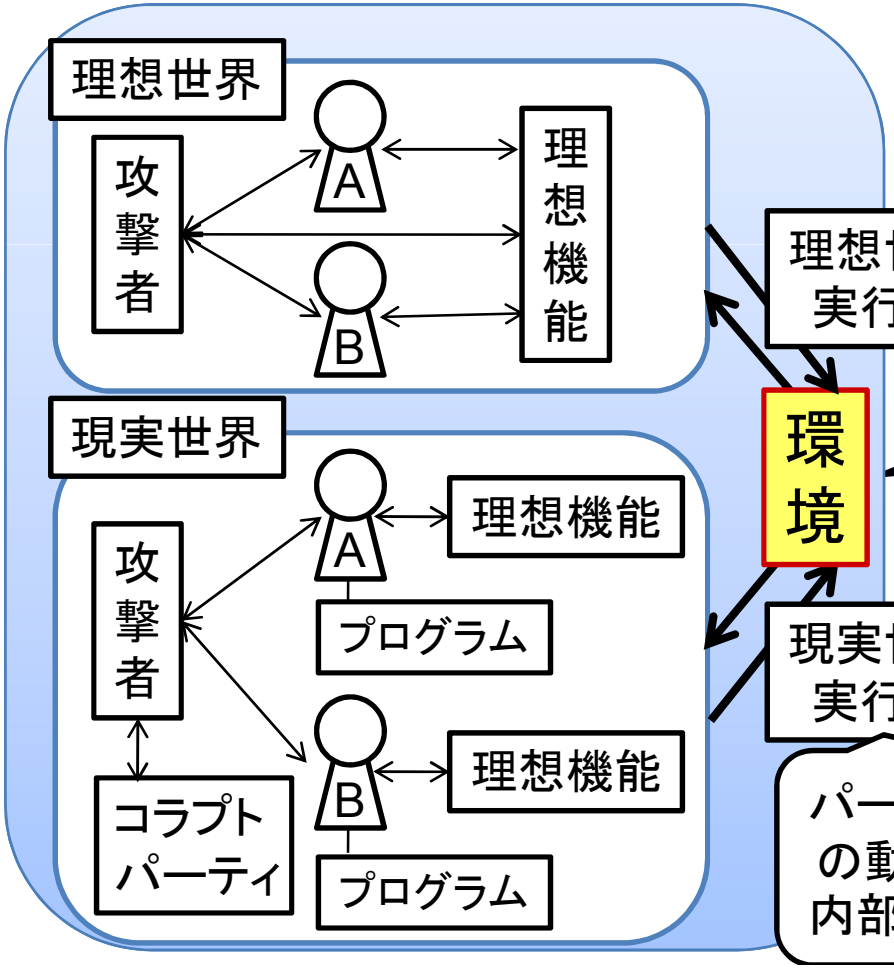
現実のプロトコルを実行する世界
目標とする暗号機能を実現しようとする

プロトコルを実行するパーティ
・パーティIDとセッション番号をもつ
・動作をプログラム（コマンド系列）で記述
・公開鍵暗号とディジタル署名の理想機能を利用

現実世界における攻撃者
・プロトコルが暗号機能を実現するのを妨害
・パーティ間のやり取りをコントロール
・コラプトパーティを操り、コマンドを利用可能

汎用的結合可能性の枠組み
安全性

- プロトコルが安全とは理想世界と現実世界を識別できないこと



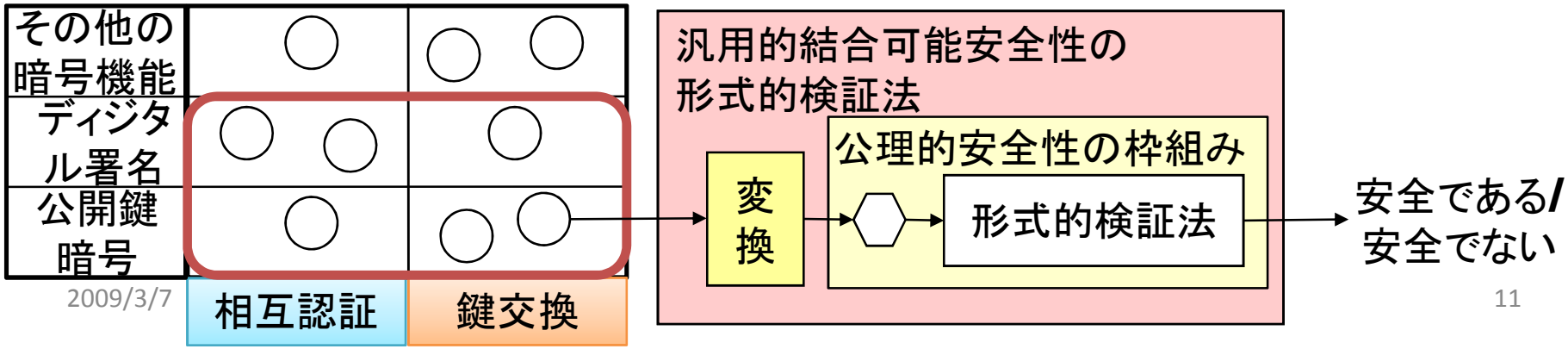
- 2つの世界の識別が目的
- 攻撃者に指示を与える
- パーティ、攻撃者の内部出力を見れる

汎用的結合可能安全性

∀現実世界の攻撃者に対し、
∃理想世界の攻撃者が存在し、
∀環境が現実世界の実行状況と理想世界の実行状況を識別できる確率が無視できる

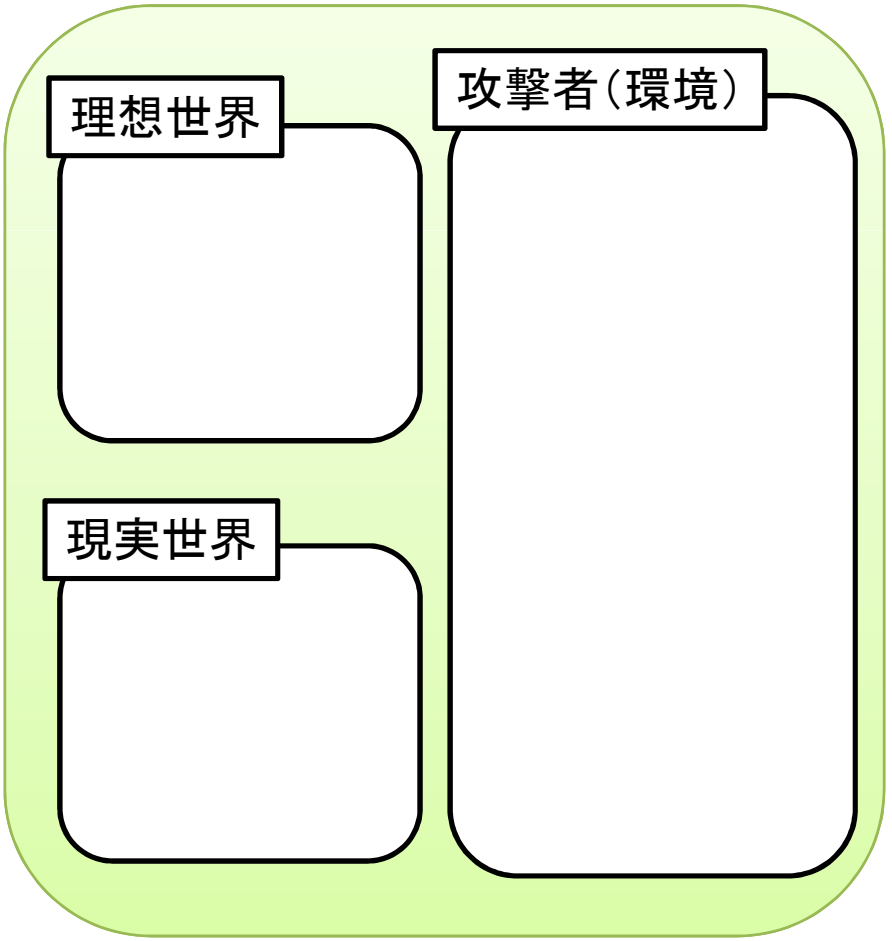
以降の発表の流れ

- 汎用的結合可能性の枠組み
- 公理的安全性の枠組み
- 提案する変換
- まとめと今後の課題



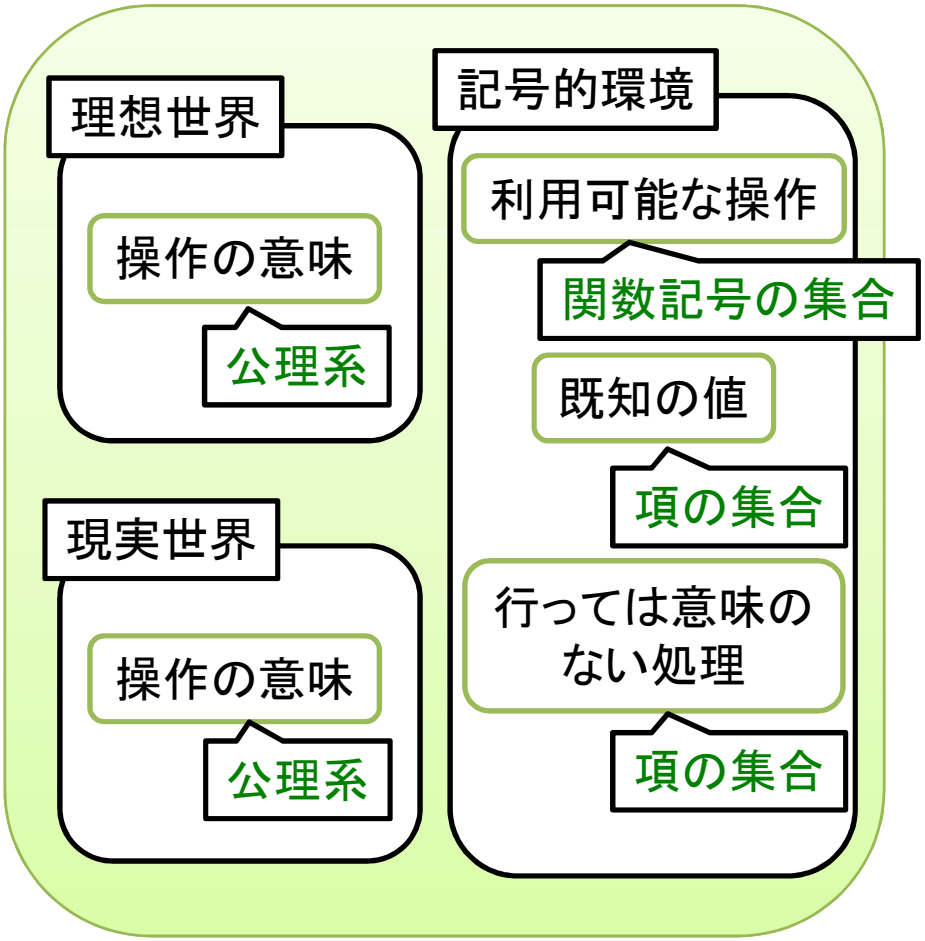
公理的安全性の枠組み

- プロトコルに対して想定する攻撃者を記述
  - 理想世界と現実世界の識別者(環境)を記述
- 操作:関数記号
  - 例:E_{pk}, D_{sk}, m
- 値:項
  - 例:$E_{pk}(m)$
- 値への操作(処理):項
- 操作の意味:
  項の間の等式(公理)
  - 例:$D_{sk}(E_{pk}(x)) = x$



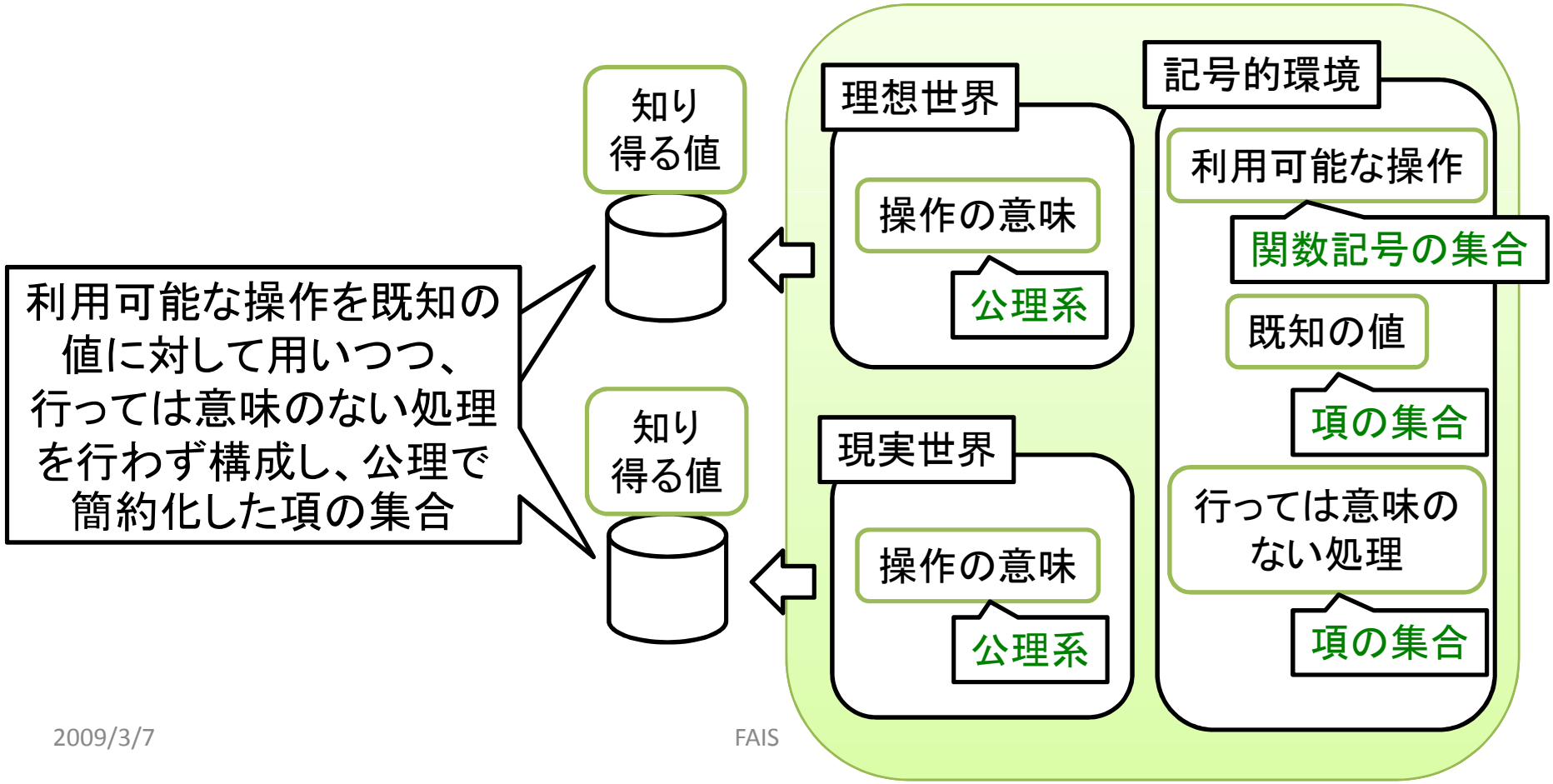
記号的環境の定義

- 記号的環境を利用可能な操作、既知の値、行っては意味のない処理で記述
  - 利用可能な操作は攻撃者に行わせる操作を記述
- 記号的環境がやり取りする理想世界、現実世界は操作の意味で記述



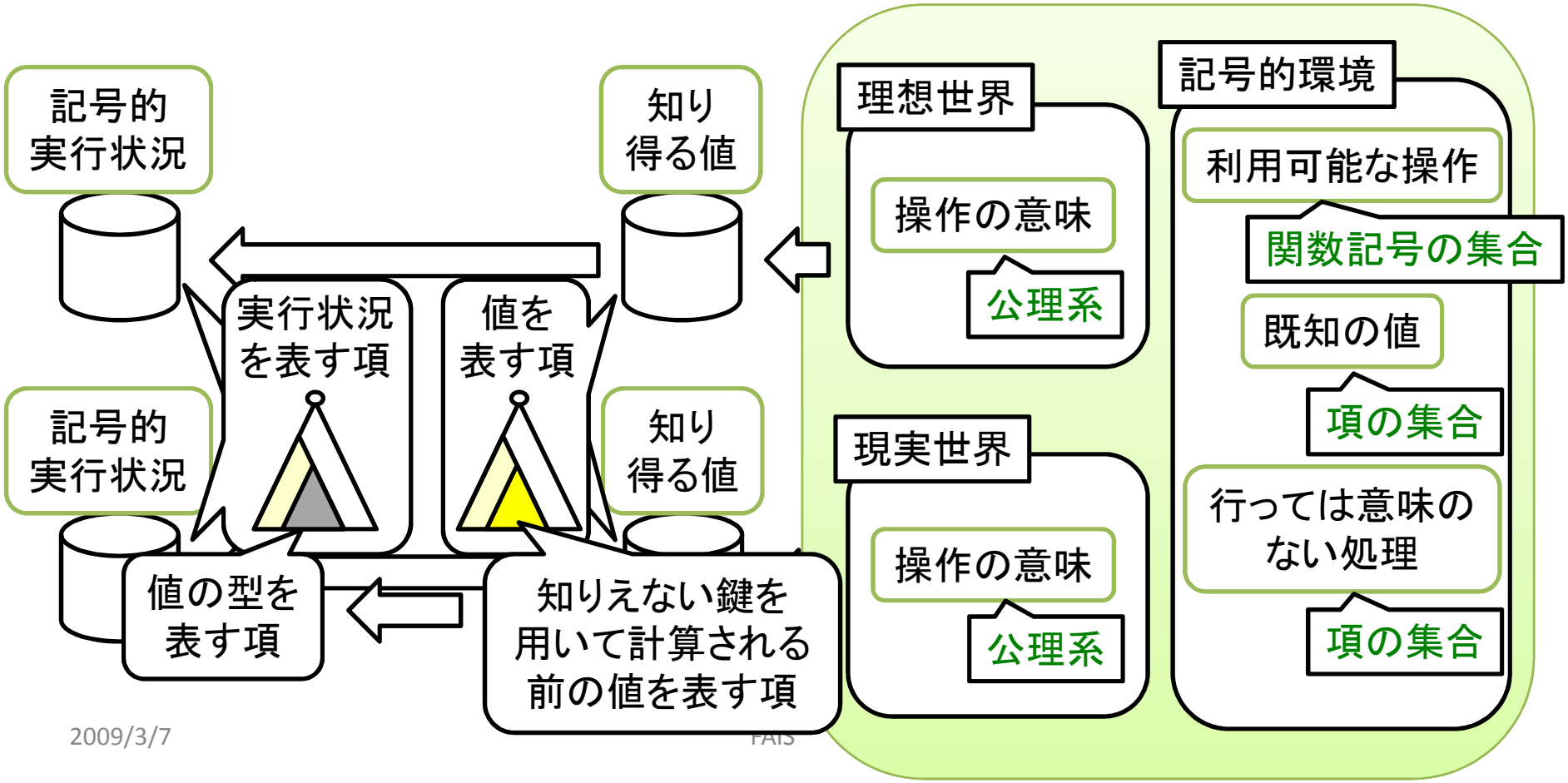
記号的実行状況の定義

- 環境が知り得る値を表す項から定義
  - 項を上から見ていくとき、環境がどこまで識別できるかを表す



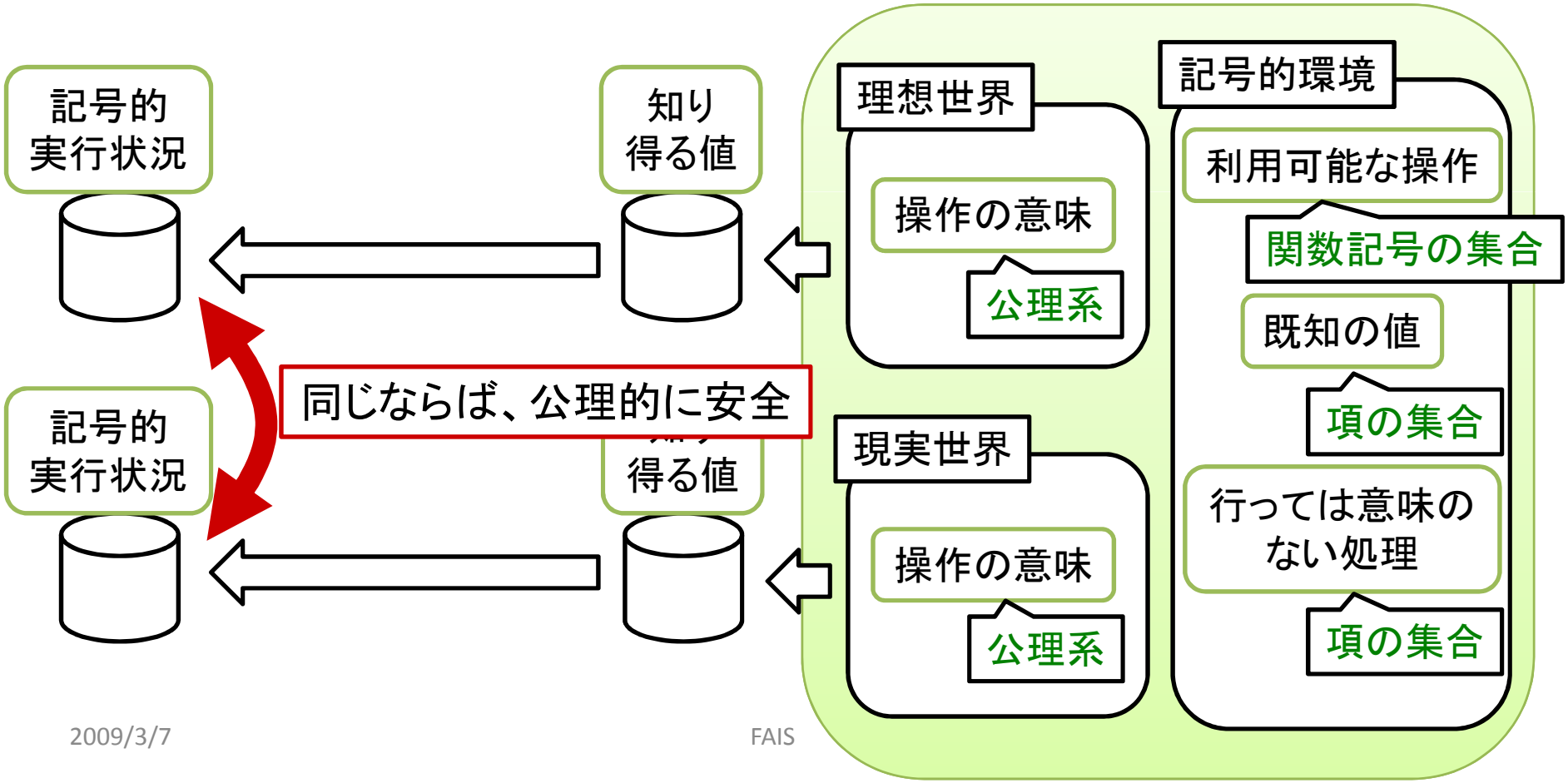
記号的実行状況の定義

- 環境が知り得る値を表す項から定義
  - 項を上から見ていくとき、環境がどこまで識別できるかを表す



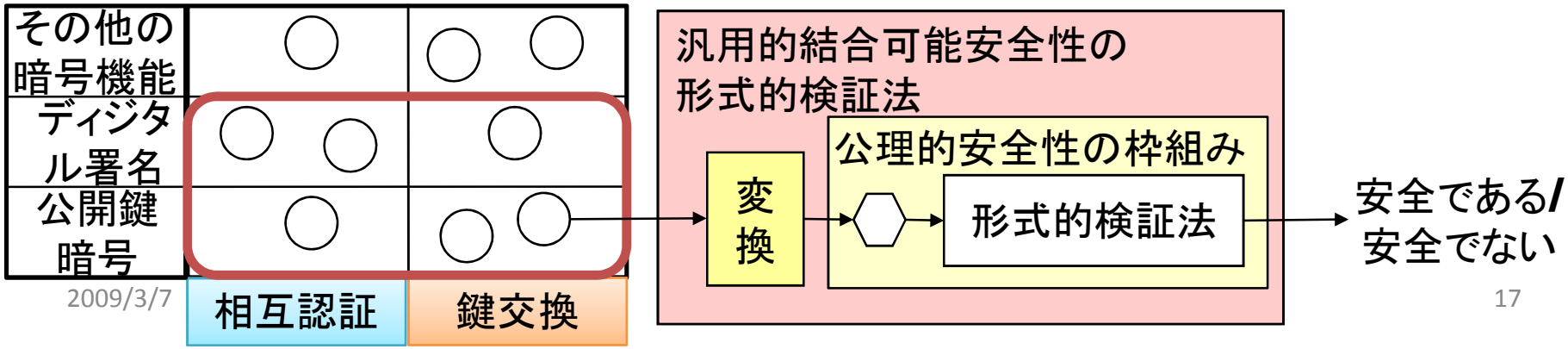
公理的安全性の定義

- 記号的環境に対する理想世界と現実世界の記号的実行状況が同じならば、公理的に安全



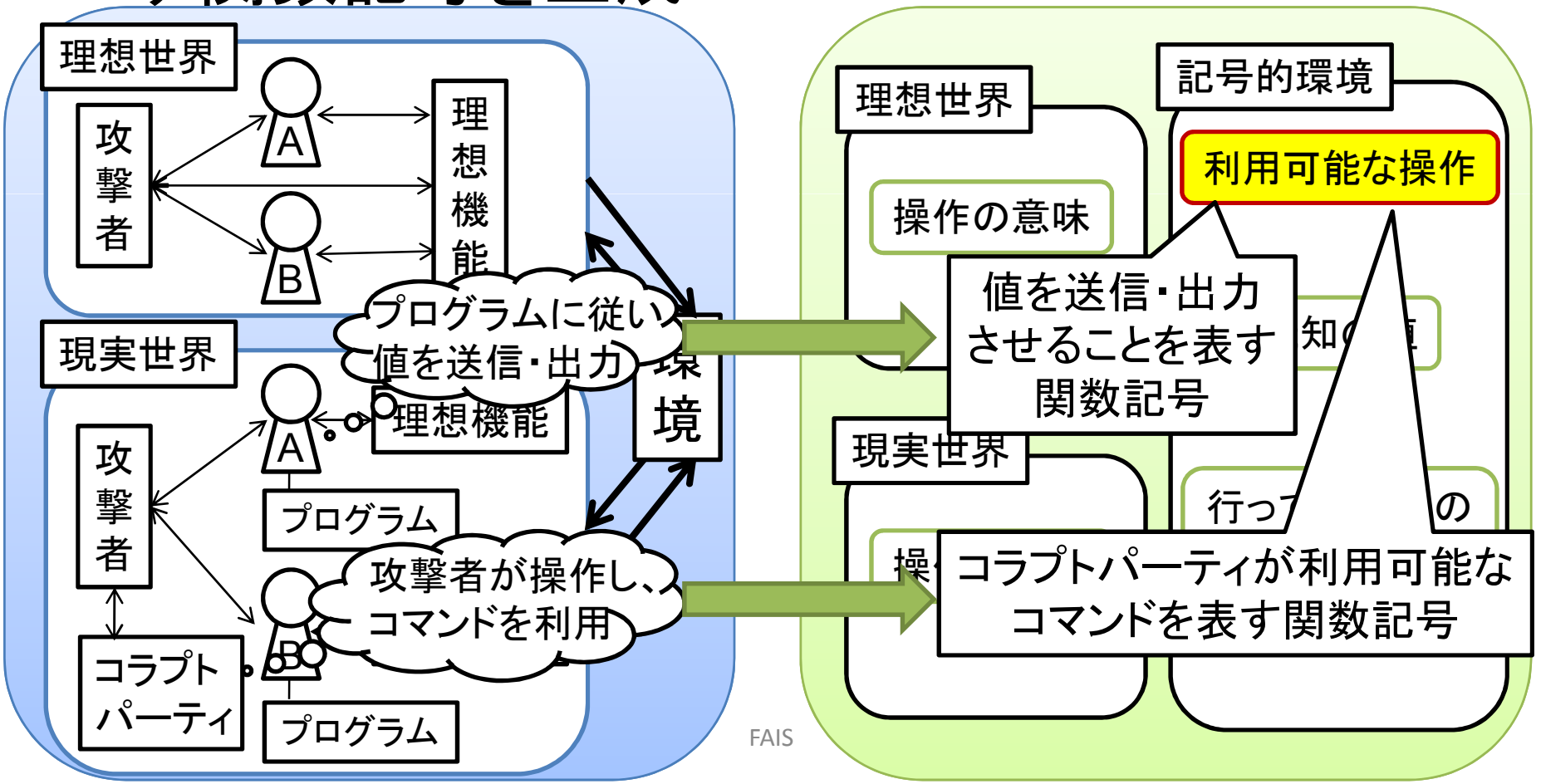
以降の発表の流れ

- 汎用的結合可能性の枠組み
- 公理的安全性の枠組み
- 提案する変換
- まとめと今後の課題



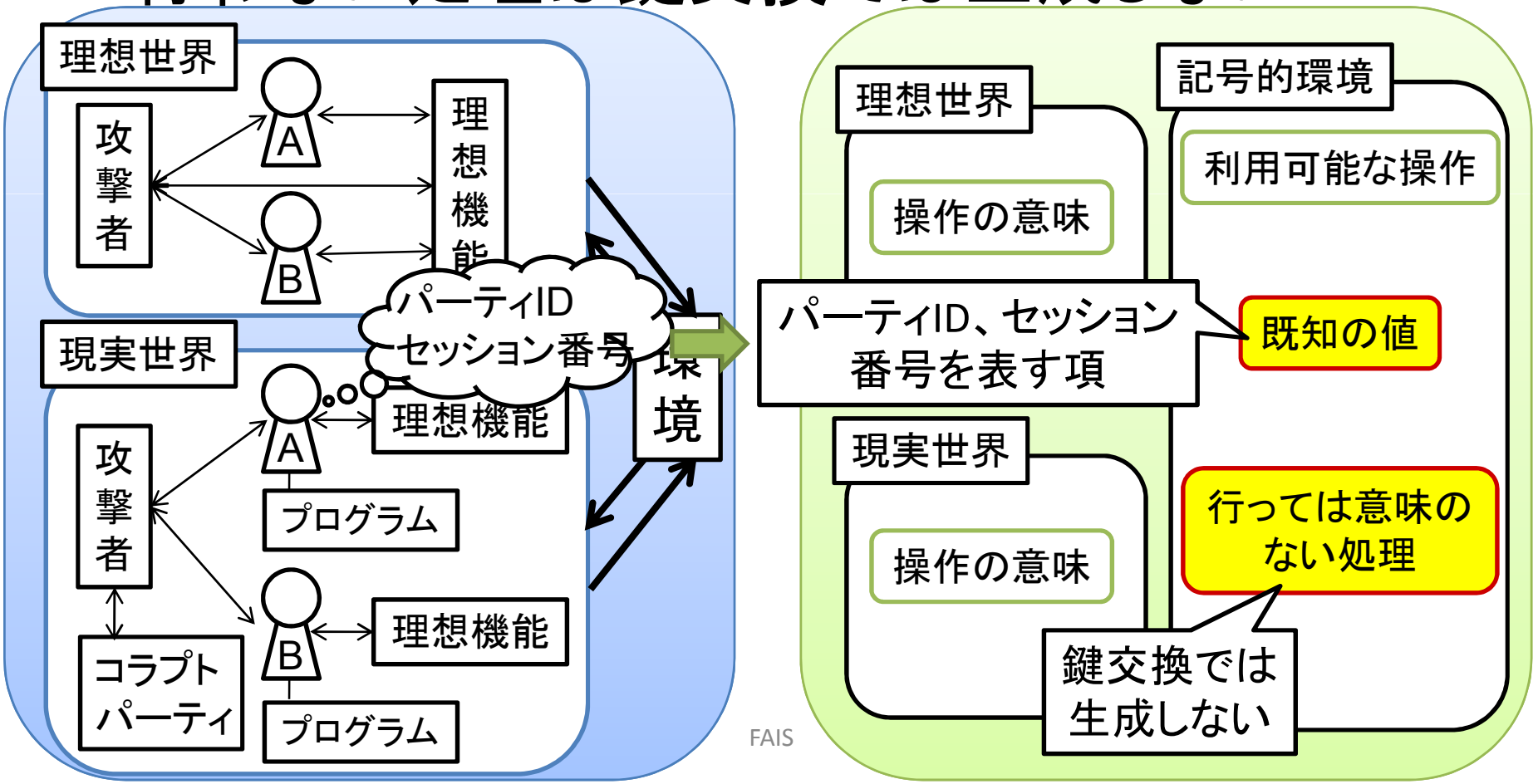
記述の変換
利用可能な操作

- 環境が攻撃者にさせることができる操作を表す関数記号を生成



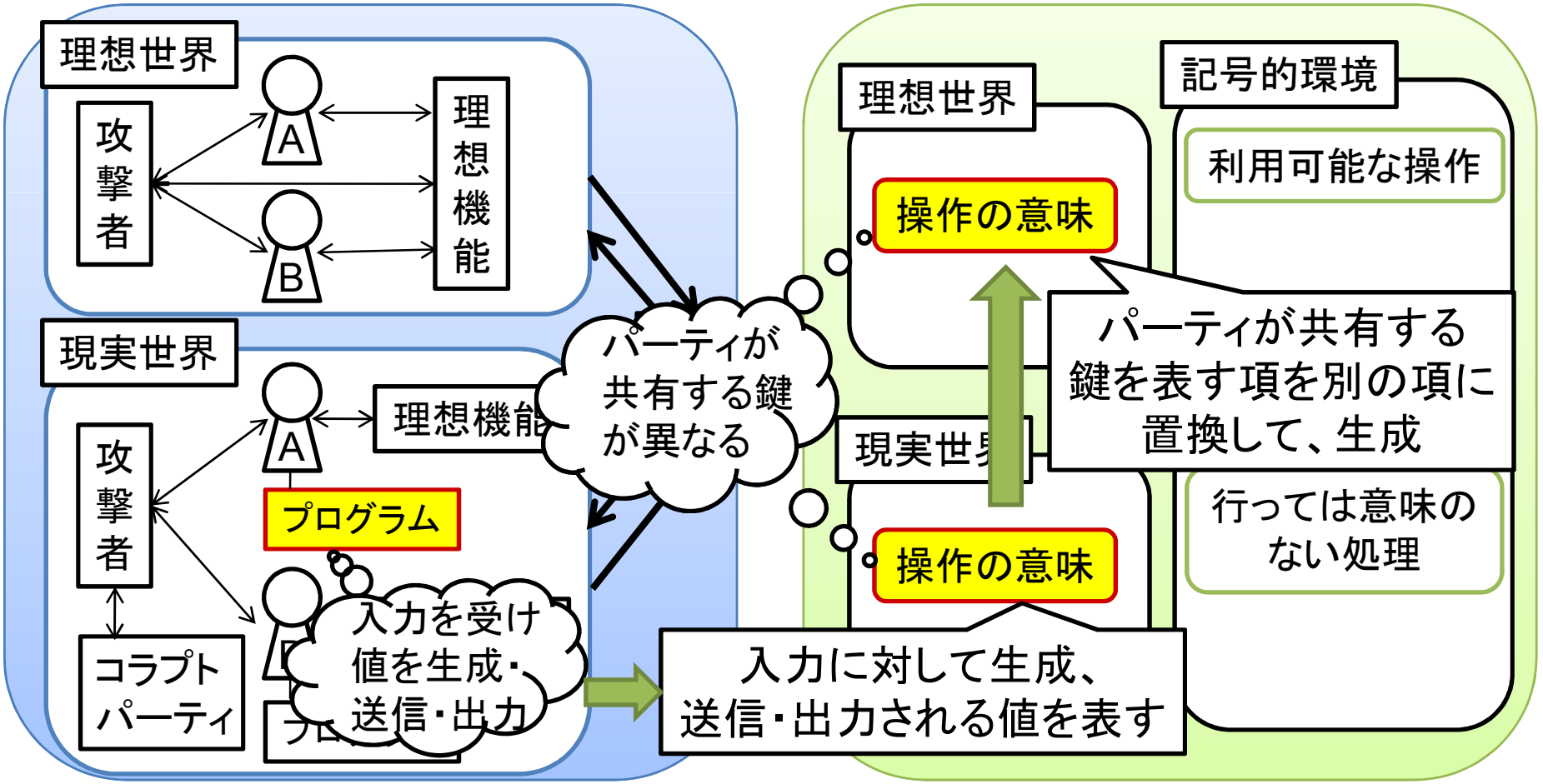
記述の変換
既知の値と行わない処理

- 既知の値を表す項を生成
- 行わない処理は鍵交換では生成しない



記述の変換
操作の意味

- 現実世界の操作の意味はプログラムから生成
- 理想世界の操作の意味は現実世界の操作の意味を表す公理から生成



まとめと今後の課題

- まとめ
  - 公理的安全性の枠組みで、汎用的結合可能安全な鍵交換プロトコルに 対する安全性を定義
    - 対象プロトコルが利用する暗号機能は公開鍵暗号とディジタル署名
- 今後の課題
  - 定義した公理的安全性の検証法の提案
    - 従来の公理的安全性検証法を拡張
  - 検証対象の拡張