暗号プロトコル制度の視点から数理的技法研究に期待すること

大塚玲（産業技術総合研究所）
松尾真一郎（情報通信研究機構）
宮崎邦彦（日立製作所）

JSIAM 年会
2009年9月28日

これまでの経緯

- **2003年　CRYPTREC**
  - **フォーマルメソッドによる暗号プロトコルの評価手法に関する調査**
- **2004-2006年 JST科振費プロジェクト**
  （政策目標2：国際競争力の確保・強化による経済の活性化）
  ④ 情報セキュリティに資する研究開発
  「セキュリティ情報の分析と共有システムの開発」徳田英幸（慶応）
  大阪大学、京都大学、（独）情報通信研究機構、奈良先端科学技術大学院大学、（独）産業技術総合研究所、（株）三菱総合研究所、
  東京大学、横浜国立大学、筑波大学、東京電機大学、日本電気（株）、情報セキュリティ大学院大学、（独）情報処理推進機構、慶應義塾大学
  2. 情報通信機器における情報セキュリティ事故の早期警戒、事故発生時の被害局所化技術
  (11) コンポーザビリティ概念に基づくセキュアプロトコルの評価に関する研究

- **2007年－現在　ISO/IEC 29128「Verification of Cryptographic Protocols」**
  - 2007年4月 WG3でプロジェクト開始
  - 2007年10月 日本のProject Editor（宮崎、大塚、松尾）提案が承認され就任
  - 2008年4月 1st WD提出、2009年10月（現在） CD投票中
  - 2011年10月頃IS化予定（楽観的？）

- **2009年－現在　CRYPTREC**
  - Authentication Protocolの電子政府暗号リスト化（2009年度公募、NICT松尾）
  - 基本的な仕組みはISO/IEC 29128での検討結果を活用
  - CRYPTRECでの実践経験をISO/IEC 29128に反映したい！

話の構成

1. **ISO/IEC 29128「Verification of Cryptographic Protocols」**
   Speaker: 宮崎（日立製作所）
   暗号プロトコルの国際標準／制度設計

2. **CRYPTREC「エンティティ認証プロトコルの公募指針」**
   Speaker: 松尾（NICT:情報通信研究機構）

3. **暗号プロトコル制度の視点から数理的技法研究に期待すること（まとめ）**
   Speaker: 大塚（AIST:産業技術総合研究所）

暗号プロトコル評価技術

- 多数の技術・ツールが研究開発されている
  - (1)様相論理を用いるもの
    - 限定された認証性質についてしか推論できないため、現在ではあまり利用されていない（例：BANロジック）
  - (2)モデルチェッキング手法を用いるもの
    - 自動検証可能。安全性評価に大きな効果を上げている（例：NRL、FDR、AVISPA、ProVerif、SCYTHER、CryptoVerifなど多数）
  - (3)定理証明を用いるもの
    - 通常、人手による証明戦略の指示などが必要であるため、完全な自動証明は困難だが、セッション数の制限などはないため、より強い検証結果を得られる（例：Isabelle）

暗号プロトコル評価技術の分類

- 抽象化レベルもさまざま
  - Dolev-Yaoモデル：暗号プリミティブを完全なものと仮定するモデル
  - 計算量理論的なモデル：暗号プリミティブを確率的な振る舞いをする、より現実的なものと仮定するモデル
- 検証範囲もさまざま
  - Unbounded：セッション数に制限を設けず検証
  - Bounded：セッション数に制限を設けた範囲のみの探索により検証

主な暗号プロトコル検証ツール

	Model checking		Theorem proving
Symbolic	NRL FDR AVISPA	SCYTHER ProVerif AVISPA (TA4SP)	Isabelle/HOL
Cryptographic		CryptoVerif	BPW(on Isabelle/HOL) Game-based Security Proof（on Coq)

Unbounded

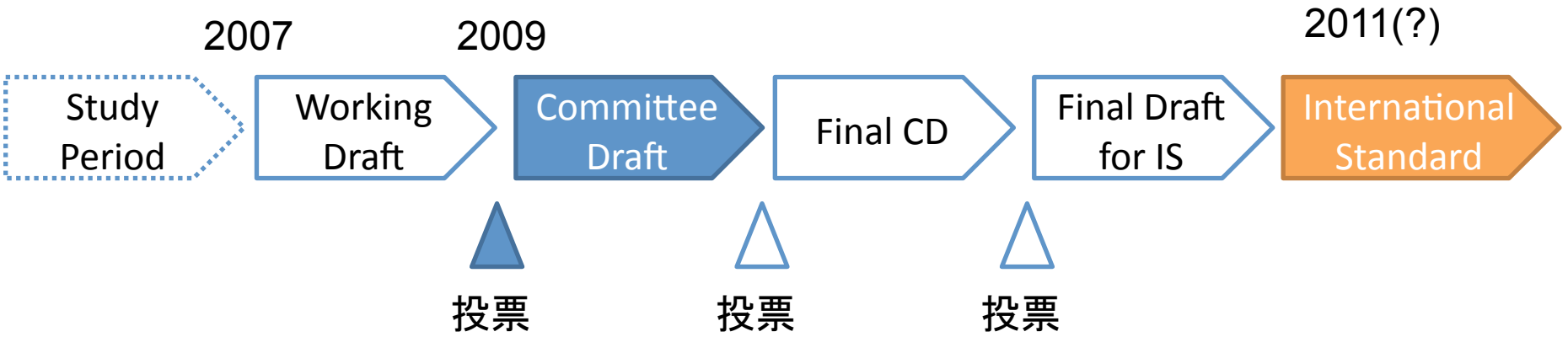
実用上の課題

- 各ツールが扱えるプロトコル／セキュリティ要件はそれぞれ異なり、また、検証結果の保証の程度も異なる
- 異なる手法間の関係性も必ずしも明らかではない
- その結果、暗号プロトコルを、実務的に、開発あるいは利用する立場からは、プロトコルをどのツールを使って評価すればよいのか、またどういう結果が得られれば安心できるのか、が分からない状況にある

- ➔暗号プロトコル評価に一定の基準を与えたい！

ISO/IEC 29128

- ISO/IEC 29128 “Verification of Cryptographic Protocols”
- 日本からの提案に基づきISO/IEC JTC/1 SC/27 WG/3にて2007年にプロジェクト開始
- 標準化スケジュール



（注）本発表の内容は現在のドラフトに基づくものであり今後の改定により変更される可能性があります

ISO/IEC 29128概要

- プロトコル評価を行う上で、共通的に必要となると考えられる記述事項（プロトコル仕様、攻撃者モデル、セキュリティ要件）を規定し、さらに検証の度合いに応じて、以下の3つのプロトコル保証レベルを定義
  - プロトコル保証レベル1では、プロトコル仕様は準形式的に記述され、攻撃者モデル、セキュリティ要件は非形式的に記述されていてよい。また検証は、非形式的な議論によるものでよい。
  - プロトコル保証レベル2では、プロトコル仕様、攻撃者モデル、セキュリティ要件は形式的に記述されなければならない。また検証は、ツールを用いた形式的な証明でなければならない。ただし検証に当たっては、並行動作するセッション数には上限を設けてよい。
  - プロトコル保証レベル3では、プロトコル保証レベル2に加えて、さらにセッション数に関する制限なしに検証されなければならない。

プロトコル保証レベル(PAL)

Protocol Assurance Level	**PAL1**	**PAL2**	**PAL3**
Protocol Specification	**PPS_SEMIFORMAL** Semiformal description of protocol specification.	**PPS_FORMAL** Formal description of protocol specification in a tool-specific specification language, whose semantics is mathematically defined.	
Adversarial Model	**PAM_INFORMAL** Informal description of adversarial model.	**PAM_FORMAL** Formal description of adversarial model in a language.	
Security Property	**PSP_INFORMAL** Informal description of security property	**PSP_FORMAL** Formal description of security property.	
Self-assessment Evidence	**PEV_HANDPROVEN** Informal argument or mathematically formal proof only by hand that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties.	**PEV_BOUNDED** Bounded verification by verification tool that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties.	**PEV_UNBOUNDED** Unbounded verification by verification tool that the specification of the cryptographic protocol in its adversarial model achieves and satisfies its objectives and properties.

標準化過程での議論（1）

- 特定手法・ツールに対する中立性
  - 特定のツールを「標準ツール」として標準化するのではなく、各保証レベルにおいてツールに求められる性質を標準化すべき
  - Model CheckingかTheorem Proverかではなく、BoundedかUnboundedか、で保証レベルを分ける
  - 新たな（より高性能、高機能な）プロトコル評価ツールの活用を妨げない

標準化過程での議論（2）

- 計算量モデル（暗号学的健全性）
  - 多くのツールはDolev-Yaoモデルを前提としている
    - 攻撃者はネットワークを自由にコントロールできる
    - 暗号プリミティブは完全である
  - 一方、暗号プリミティブを完全なものと仮定しない、より現実的なモデル（計算量モデル）に基づく、プロトコル検証技術も存在する。これらをより保証レベルの高い評価とみなすべきではないか？
  - ➔現時点では、標準規格の中で独立した保証レベルを定義するには未成熟と判断。今後の技術の進展に期待

標準化過程での議論（３）

- 手証明の扱い
  - 「紙と鉛筆による証明」も「非形式的な議論」もともにPAL1とみなしているのは妥当なのか？
  - 理論的には両者は区別されるべき。しかし、手証明は誤りが混入しやすく、認定を与える機関等が証明の正しさを確認するのが困難
  - 本規格では、将来的に認定制度などとして運用された場合も考慮にいれ、手証明はPAL1とみなす
  - ➔優れた最新の理論的成果がツールとして利用可能なレベルにまで成熟することを期待

制度化に向けた課題

- 手法・ツール改良
  - 多くのツールが開発されているが、個々のツールにはそれぞれ制限事項もある(例：代数的な性質は扱えるツールと扱えないツールが存在する）
  - 有用な暗号プロトコルとそれを評価可能なツールとのギャップを埋めることが継続的に望まれる
- 熟練技術者
  - 制度として確立するためにはツールが存在するだけでは不十分であり、それらを活用して評価する能力をもった熟練技術者を十分に有した体制が必要
  - ツールの改良により熟練技術者の教育に必要なコストの削減を図ることも重要かつ有用と考えられる

CRYPTREC とは

- CRYPTography Research and Evaluation Committees の略
- 電子政府で利用する暗号技術について、その安全性を担保することを目的として、総務省・経済産業省の両省によって運営されている
- 電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクト
- 3 つの委員会で構成
  - 暗号方式委員会
  - 暗号実装委員会
  - 暗号運用委員会
- “電子政府推奨暗号リスト” を公開、維持管理をするとともに、リスト掲載暗号暗号技術に関連する報告書や、リスト掲載暗号の利用方法を示す “リストガイド” を発行

電子政府推奨暗号リスト

- （2003 年時点で）10 年程度安全性が担保される暗号技術をリスト形式でまとめたもの
- 1 つの技術を選抜する事が目的ではなく、基準を満たしているものをスクリーニングすることが目的
- 国内外から暗号技術を公募し、国内外の専門家のレビューと公開の議論を経て、選考を実施
- NISC[1]の政府機関統一基準において参照され、電子政府システムにおける強化遵守事項となっている
- FISC[2]のガイドラインで参照され、金融機関の情報システムにおいてリスト掲載暗号以外の技術を利用している場合、金融庁検査の際にその正当性を別途示す必要がある

[1]内閣官房情報セキュリティセンター
[2]金融情報システムセンター

現在の電子政府推奨暗号リスト（2003 年度版）

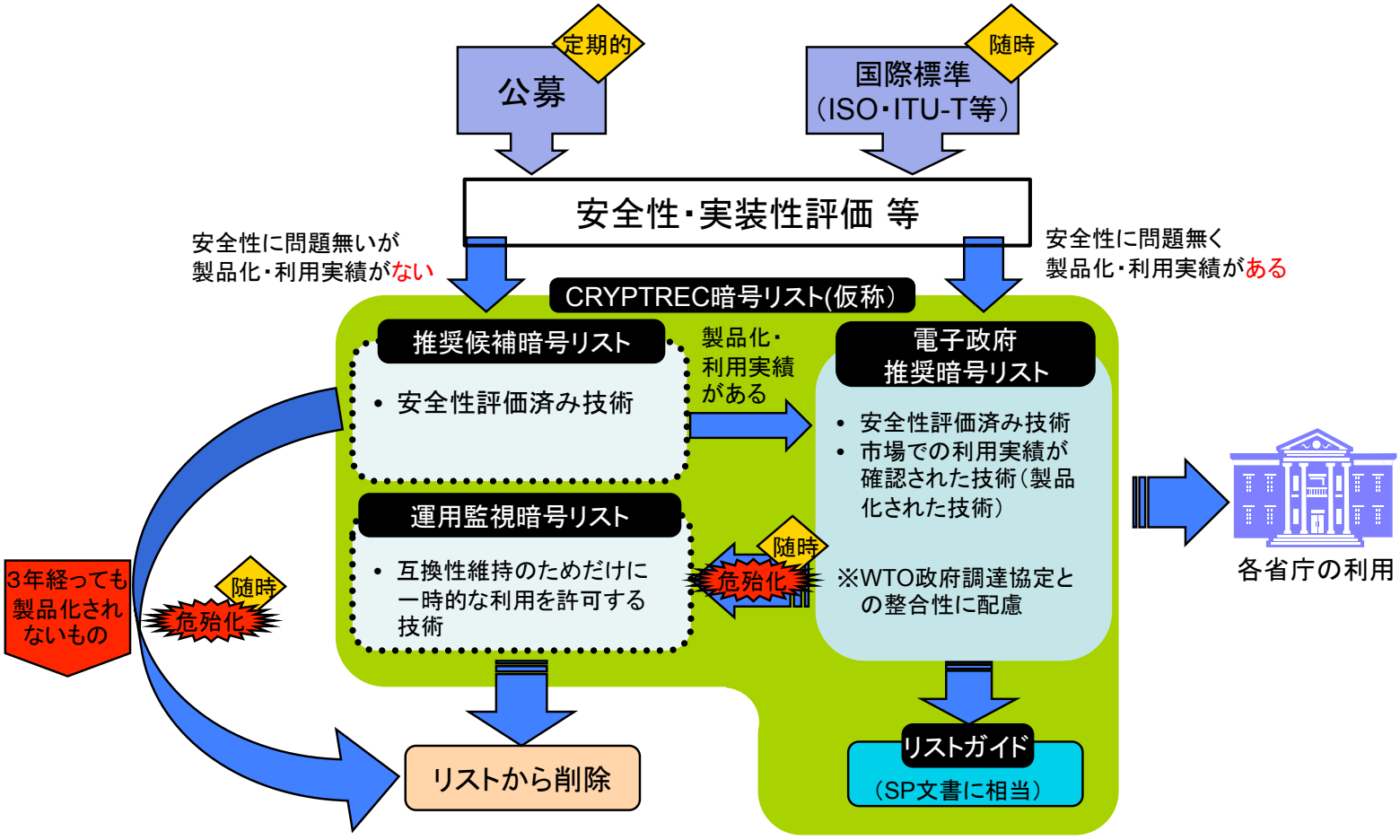
技術分類	小分類	技術名
公開鍵暗号	署名	DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS
	守秘	RSA-OAEP, RSAES-PKCS1-v1_5
	鍵共有	DH, ECDH, PSEC-KEM
共通鍵暗号	64 ビット ブロック暗号	CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3-key Triple DES
	128 ビット ブロック暗号	AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000
ストリーム暗号		MUGI, MULTI-S01, 128-bit RC4
その他	ハッシュ関数	RIPEMD-160, SHA-1, SHA-256/384/512
	疑似乱数生成	3 アルゴリズムを例示

http://www.cryptrec.go.jp/images/cryptrec_01.pdf で公開中

電子政府推奨暗号リスト改訂の背景

- 2013 年に現在のリスト発行から 10 年経過するために、（当初の予定通り）見直しを行う
- “暗号技術の危殆化” がクローズアップされるようになったため、危殆化が発生することを前提としたリストの体系と運用を整備する必要性がでてきた
- 暗号技術の進展により、現在のリストに掲載された技術よりも優れた暗号技術が登場しており、これらの技術の評価を行った上で、電子政府にとって有用な技術をリストに取り込む必要がある（同一分類内での技術の改訂）
- 暗号技術が多様化し、現在のリストの技術分類にない技術が広く使われるようになっており、これらの技術をリストにおいて推奨を示す必要があるため（新たな技術分類の追加）

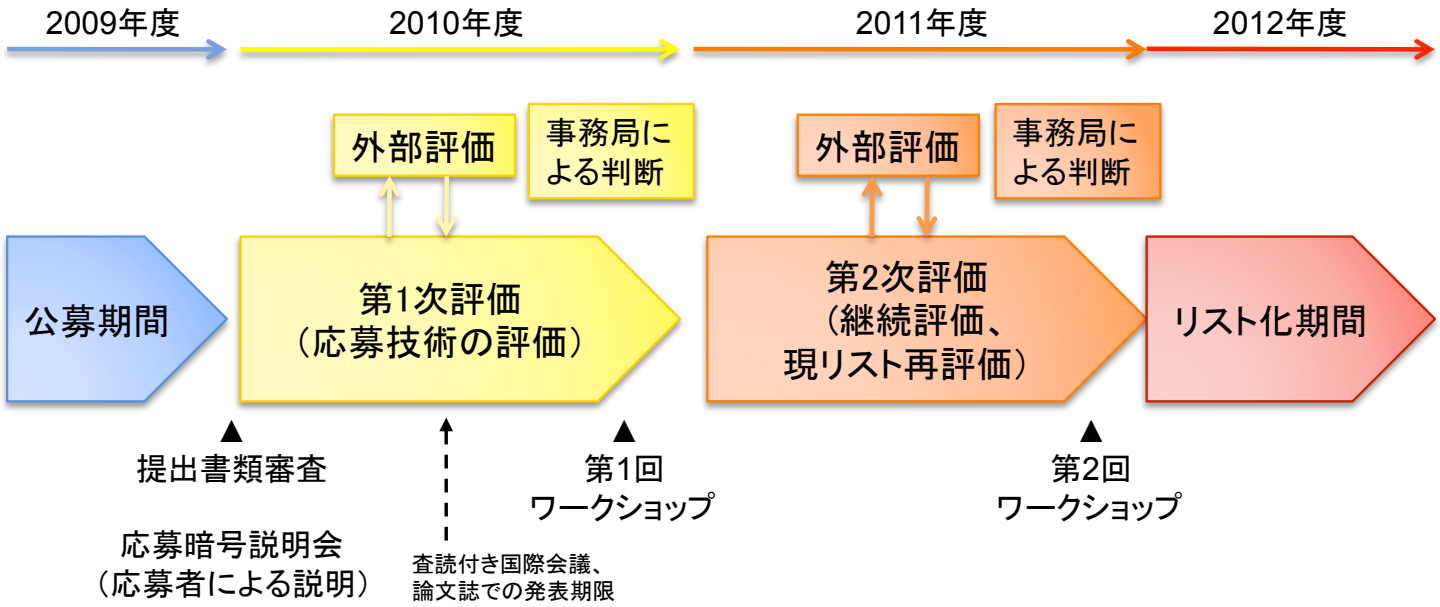
2013 年以降の電子政府推奨暗号リストの体系



2013 年の電子政府推奨暗号リスト改訂の概要

- 新たな暗号技術の公募
  - 既存の技術分類に対する新技術の公募
    - 128 ビットブロック暗号
    - ストリーム暗号
  - 新たな技術分類に対する公募
    - メッセージ認証コード
    - 秘匿のための暗号利用モード
    - エンティティ認証プロトコル
- リストガイドの拡充
  - アプリケーションを意識した、リスト掲載暗号の推奨される利用方法の提示
    - 認証付き鍵交換、PKI 向け電子署名、ワンタイムパスワード
    - 通信路の暗号化、蓄積データの暗号化、ID ベース暗号
    - 鍵管理　など
  - 相互運用性が不要な暗号関連技術（疑似乱数生成など）について、推奨を提示する

電子政府推奨暗号リスト改訂のスケジュール



エンティティ認証における公募対象技術

公募の対象

電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証を公募します。エンティティ認証を構成する要素技術は、現リストに掲載されている暗号技術を用いることを原則とします。要素技術として、現リストに掲載されていない共通鍵暗号、メッセージ認証コードを用いる場合は、これらの要素技術を同時に応募する必要があります。また、上記以外の要素技術を用いたエンティティ認証技術の応募も可能です。

※公募要項[3]より抜粋

[3] http://www.cryptrec.go.jp/topics/cryptrec_20090527_application_guide.html

エンティティ認証の既存の標準（技術例）

エンティティ認証の基本機能

- 通信相手が意図した正しい通信相手であることを確認する
- 相手認証 (一方のみ) と相互認証 (双方)
- セキュリティ:なりすましの防止、セッションのすりかえの防止など

- ISO/IEC による規格化（ISO/IEC 9798）
  - 共通鍵暗号アルゴリズムに基づく方式 (9798-2)
  - 電子署名に基づく方式 (9798-3)
  - 検査関数に基づく方式 (9798-4)
  - ゼロ知識証明を用いた方式（9798-5）
  - 手動データ転送を用いた方式（9798-6）
- Kerberos, SASL (IETF)
- One-time Password など

エンティティ認証プロトコルの評価方針

評価項目

安全性の評価は、エンティティ認証としてのセキュリティに問題が生じないことを、形式的な手法を用いて行います。安全性を脅かす状態としては、なりすましの成功、セッションの取り換え等を想定します。　暗号プリミティブとして、電子政府推奨暗号リストに掲載されている、あるいは応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利用している場合には、暗号プリミティブを理想的に安全なものとして安全性の評価を行います。その他の暗号プリミティブを用いる場合には、暗号プリミティブを理想化せずに安全性の検証を行います。　上記のいずれの場合も、提案者はプロトコルの安全性を示す情報を提出し、本公募における安全性評価では、これらの正当性を検証します。

※公募要項[4]より抜粋

[4] http://www.cryptrec.go.jp/topics/cryptrec_20090527_application_guide.html

応募時の主な提出内容

- 暗号プロトコルの仕様書
- 自己評価書
  - 設計思想
  - 安全性評価（※）
  - ソフトウエア実装性評価
  - 第三者評価実績（※）
- テストベクトル
- 参照ソースコード

（※）の部分が、特に数理的技法による安全性評価が関連する項目

電子政府推奨暗号リスト掲載暗号のみを使っている場合

- 電子政府推奨暗号リストに掲載された暗号プリミティブは理想的であるとする
- よって、これらの暗号のみを利用したエンティティ認証プロトコルについては、計算量的仮定については考慮しない（Computational sound な手法は利用しなくてよい）
- 自己評価に用いるツールは、Internet などで公開されているツール、独自ツールのどちらでもよい
- Internet で公開されているツールの場合には、ツール名とバージョン番号を提示
- 独自ツールの場合は、ツールそのものも提出するとともに、ツールの正当性を証明する書類を提出する
- ツールを用いた評価結果の正当性を事務局で追試するとともに、ツール自体の正当性についての評価も行う

電子政府推奨暗号リスト掲載暗号以外の暗号プリミティブを使っている場合

- Diffie-Hellman の変形や、Fiat-Shamir などの技法を利用したエンティティ認証などを想定
- 各暗号プリミティブは理想的でないため、代数的構造や計算量的仮定を扱う事ができるツールを用いる → 代数的構造や計算量的仮定についての確認が追加で必要となる
- 自己評価に用いるツールは、Internet などで公開されているツール、独自ツールのどちらでもよい
- Internet で公開されているツールの場合には、ツール名とバージョン番号を提示
- 独自ツールの場合は、ツールそのものも提出するとともに、ツールの正当性を証明する書類を提出する
- ツールを用いた評価結果の正当性を事務局で追試するとともに、ツール自体の正当性についての評価も行う

評価実施にあたっての課題

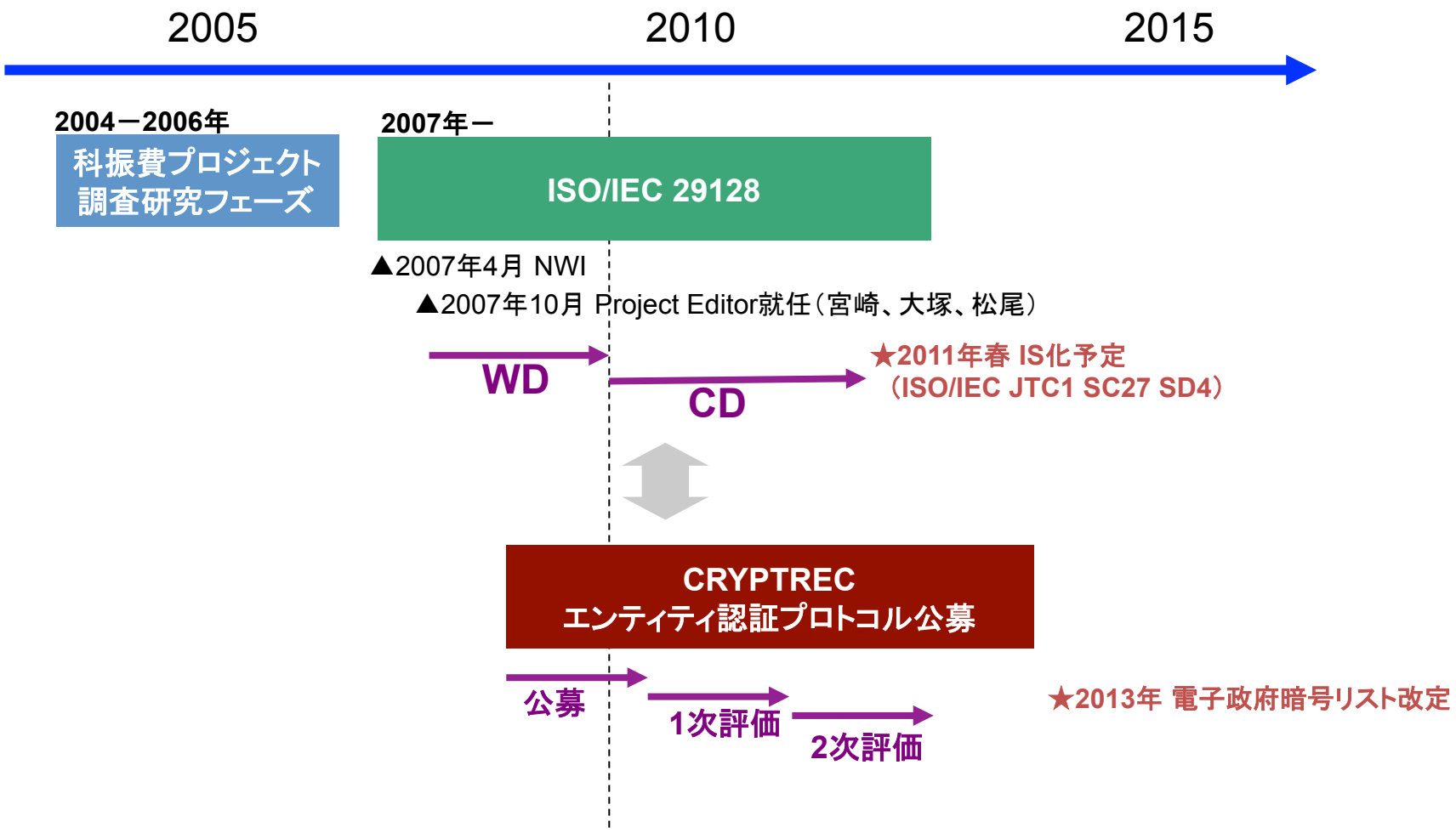
安全性の面で評価すべき項目は “暗号プロトコル自体の安全性” と “ツール自体の正当性” の 2 つ

- 暗号プロトコル自体の安全性
  - プロトコル記述の正当性のチェック
  - 安全性定義に関する記述の正当性のチェック
  - 攻撃者の能力に関する技術の正当性チェック
  - プロトコル設計者による評価結果の吟味
- ツール自体の正当性
  - ツールの正当性をどのように検証するか？
  - 公開されたツールでもバージョンによって挙動が異なることがある
    → 信頼できるツール名とバージョンの組に関する知見の収集、合意が必要
  - ツールの正しさを検証するような方式の確立も必要
    → 暗号プリミティブにおけるテストベクトルのようなもの（テストプロトコル、テストデータなど）
  - CRYPTREC 標準ツールの構築

数理的技法による情報セキュリティに関する研究者への期待

- ツールの正当性に関する研究
  - ツールの正当性の評価方法に関する研究の進展が、制度としての運用には不可欠
  - 信頼できるツール、およびツールの利用方法に関するノウハウの蓄積も不可欠
  - “信頼できるツール” に関する（国際的な）合意を得るために必要な知見は？
- プロトコル評価の実施
  - プロトコルの評価、ツールの評価（追試）に関しては多大な労力が必要と考えられる
  - 効率的な追試の方法についての知見が不可欠
  - CRYPTREC の実際の評価において、外部評価者として研究者による評価も必要と考えられる

暗号プロトコル制度の視点から
数理的技法研究に期待すること（まとめ）



暗号プロトコル制度の視点から
数理的技法研究に期待すること（まとめ）

1. 理論／ツールの開発

理論（科学的根拠）に裏打ちされたセキュリティを実現するための制度・標準　→ 技術＝ツールが重要

- Protocol Specification　様々な暗号プロトコルの記述
- Security Property　達成すべきセキュリティ条件
- Operating Environment　攻撃者の能力記述
- Evidence　ツール／検証結果の正しさに関する証拠

※代数的な性質、理想化できない暗号学的プリミティブ等

2. 協力のお願い（Please help us!)

専門家の不足が深刻(Lack of Experts)

ISO/IEC 29128の完成には専門家の協力が不可欠

CRYPTRECの制度設計はNICT等が少人数で頑張っている

→　評価実施の詳細検討にあたり、FAISの活動との連携、CRYPTRECにおける意見集約へのご協力をお願いしたい