

# 形式化手法を利用した 暗号プロトコル評価の適用拡大に向けて

2013.3.15

日本応用数学会2013年春の研究部会連合発表会FAISセッション

松尾真一郎(NICT)、  
大塚玲(産業技術総合研究所)、手塚悟( 東京工科大学)

# 本発表の概要

- ISO/IEC 29128 (Verification of Cryptographic Protocols) のおさらい
- 適用拡大に向けた論点 (現状認識と課題)
- 課題の解決に向けて

# 暗号プロトコル評価の標準化の背景

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、SCYTHERR、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, Coq, CertiCrypt, EasyCrypt)

## 暗号プロトコル評価の標準化の背景（続き）

### 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	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

- “Verification of Cryptographic Protocols”
- 日本からの提案により、ISO/IEC JTC1 SC27/WG3において標準化を開始
- 2011年に標準化を完了

# ISO/IEC 29128の概要


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、自己評価資料)を規定し、さらに検証の度合いに応じて、以下の4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  
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  
プロトコル仕様、攻撃者モデル、セキュリティ要件は数学的に厳密な形で記述されなければならない。検証には、安全性証明の正しさを専門家が確認できることが求められる。
- プロトコル保証レベル3  
プロトコル仕様、攻撃者モデル、セキュリティ要件は機械的に処理可能な形で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4  
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

客観的な信頼性の高さ



プロトコル保証レベル	PAL1	PAL2	PAL3	PAL4
プロトコル仕様	<b>PPS_SEMIFORMAL</b> プロトコル仕様を準形式的に記述	<b>PPS_FORMAL</b> プロトコル仕様を形式的に記述	<b>PPS_MECHANIZED</b> プロトコル仕様を形式的に記述。その記述はツールに対応した言語で記述され、その言語の文法は数学的に定義されている。	
攻撃者モデル	<b>PAM_INFORMAL</b> 攻撃者モデルを非形式的に記述	<b>PAM_FORMAL</b> 攻撃者モデルを形式的に記述	<b>PAM_MECHANIZED</b> 攻撃者モデルを形式的に記述。その記述はツールに対応した言語で記述され、その言語の文法は数学的に定義されている。	
セキュリティ要件	<b>PSP_INFORMAL</b> セキュリティ要件を非形式的に記述	<b>PSP_FORMAL</b> セキュリティ要件を形式的に記述	<b>PSP_MECHANIZED</b> 攻撃者モデルを形式的に記述。その記述はツールに対応した言語で記述され、その言語の文法は数学的に定義されている。	
自己評価エビデンス	<b>PEV_ARGUMENT</b> 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事を非形式的に評価	<b>PEV_HANDPROVEN</b> 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事を数学的形式が整った人間による証明で評価	<b>PEV_BOUNDED</b> 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事をツールを利用した有限チェックで評価	<b>PEV_UNBOUNDED</b> 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事をツールを利用した無限チェックで評価

# 適用拡大に向けた論点

## - ターゲットとなる暗号プロトコルの範囲 -

- ターゲットとなるプロトコルの候補
  - 既存の国際標準暗号プロトコル
    - IETF、ISO/IEC、ITU-T、民間団体などで標準化されている暗号プロトコルの脆弱性の発見と修正
  - 標準に新しく提案する暗号プロトコル
    - 一定のPALを獲得していることを、標準化のアドバンテージとして利用
  - Proprietaryな暗号プロトコル
    - 標準化はしないが、個々の企業などが開発し製品に搭載する暗号プロトコルで、一定のPALを獲得していることを、製品の安心感として利用

# 適用拡大に向けた論点

## - 評価結果のとらえ方 -

- **暗号プロトコル作成者や検証者でない第三者(暗号プロトコルの利用者)などは、検証結果をどう認識するか**
- **脆弱性が発見された後の対応をどうするか？**  
→脆弱性情報の管理と公開のプロセス(早期警戒パートナーシップ制度あるいはその類似プロセス)
- **「PAL○」をどのように認識してもらうか？**  
→厳しい安全性条件を満たすPAL2と、弱い安全性を満たすPAL4  
→PAL4は必ずしも「高い安全性」を保証しない  
→セキュリティ要件、攻撃者モデルの内容・共通化が重要

# 適用拡大に向けた論点

## - 暗号プロトコルの標準化との関係 -

- 暗号プロトコルを標準化している標準化団体でISO/IEC 29128に準じた評価を実施できるか？
- ISO/IEC、ITU-T: 一国一票の標準化プロセス。標準化過程が厳格に決まっており、その標準化プロセスに組み込む必要がある。
- IETF: 公開議論ベースの緩やかなプロセスによる標準化。形式化手法を用いた標準化結果のインパクトが重要

# 適用拡大に向けた論点

## - ツール利用の平易化と認知度向上 -

- 暗号プロトコルを作成する人が容易に形式化手法のツールを使えるか？
  - ツールのUser Interfaceを含めた平易化が必要
  - 暗号プロトコル作成者以外の追試も容易に行える
- 暗号プロトコル評価結果の積極的な公表による認知度向上
  - 既存の脆弱性情報の流通のためのしくみとの互換性

# 課題の解決に向けて

- 対象となるプロトコルの明確化
  - 暗号プロトコル評価の効果が見えやすい分野から順次実行し、その有効性に関する認知を広げていく  
→標準的なプロトコルに関する網羅的な評価の実施
- 評価結果に対する知見の蓄積
  - 暗号プロトコルの評価結果について、NISTやIPAの脆弱性DBに近いしくみで蓄積し、いつでも参照できるようにする。  
→評価結果へのアクセスと、新たな評価実施への知見の再利用

# 課題の解決に向けて(続き)

- 標準化組織への評価結果の積極的な提出と貢献
  - 標準プロトコルの脆弱性解消
  - 認知度向上
- インターフェースや形式化部分の、できる限りの共通化
  - 暗号プロトコル設計者、および評価者に必要な訓練を少なくする
  - より高度なツールの登場に際する互換性確保

# まとめ

- ISO/IEC 29128 “Verification of Cryptographic Protocols”のおさらい
- ISO/IEC 29128を通じて、形式化手法による検証結果を適用していく際の論点と解決の方向性