エンティティ認証、
暗号プロトコルの評価について

独立行政法人産業技術総合研究所
情報セキュリティ研究センター
セキュリティ基盤技術研究チーム長
大塚　玲

エンティティ認証プロトコルの概要

（1）安全性評価項目

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評価を行います。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。

（2）実装性評価項目

エンティティ認証プロトコルの実装性能評価として、ソフトウェアによる実装性評価を行います。標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。通信時間は考慮しません。

付録）電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009年度）（案）17ページ

エンティティ認証プロトコルの概要

- エンティティ認証：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）
- セキュリティ機能：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）
•検査関数を用いた方式（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）

その他
•Kerberos（IETF）
•SASL（IETF）
•One-time Password
など

暗号プロトコルの安全性解析例

フォーマルメソッドの利用により、技術標準となっている暗号プロトコルにおいて、多くの脆弱性が発見されている。

AVISPAプロジェクトの例

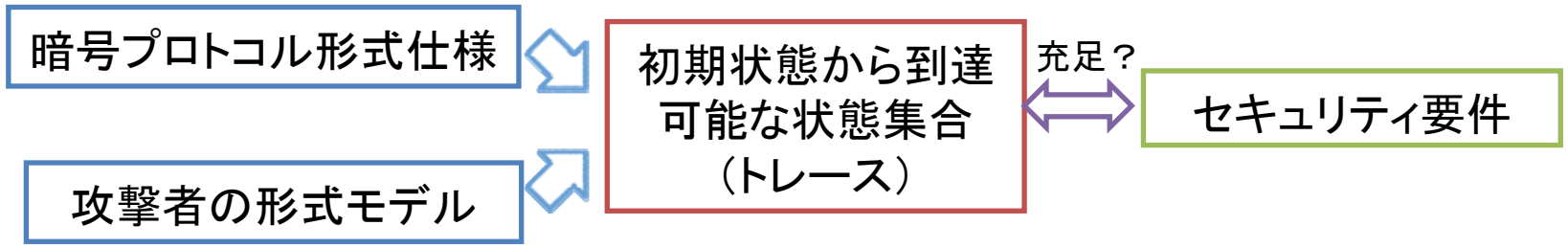
Protocol	Properties	Attacks	Time
UMTS_AKA	3	0	0,01
AAAMobileIP	7	0	0,20
ISO-PK1	1	1	0,00
ISO-PK2	1	0	0,00
ISO-PK3	2	2	0,01
ISO-PK4	2	0	0,03
LPD-MSR	2	2	0,02
LPD-IMSR	2	0	0,01
CHAPv2	3	0	0,01
EKE	3	2	0,04
TLS	3	0	0,32
DHCP-delayed	2	0	0,00
Kerb-Cross-Realm	8	0	4,14
Kerb-Ticket-Cache	6	0	0,38
Kerb-V	8	0	0,42
Kerb-Forwardable	6	0	10,89
Kerb-PKINIT	7	0	0,64
Kerb-preauth	7	0	0,62

Protocol	Properties	Attacks	Time
CRAM-MD5	2	0	0,40
PKB	1	1	0,01
PKB-fix	2	0	0,88
SRP_siemens	3	0	2,86
EKE2	3	0	0,16
SPEKE	3	0	3,11
IKEv2-CHILD	3	0	1,19
IKEv2-DS	3	1	5,22
IKEv2-DSx	3	0	42,56
IKEv2-MAC	3	0	8,03
IKEv2-MACx	3	0	40,54
h.530	3	1	0,64
h.530-fix	3	0	4.277,54
lipkey-spkm-known	2	0	0,23
lipkey-spkm-unknown	2	0	7,33

62nd IETF MEETING資料から引用

暗号プロトコルの安全性評価の概要

暗号プロトコルに求められるセキュリティ要件を満たすかどうかを評価



	フォーマルメソッド	暗号学的メソッド
メリット	安全性証明の信頼性が高い （Realityを捨象する場合もある）	豊富な理論を活用してRealityに近い 安全性証明が可能
デメリット	扱える暗号プリミティブやセキュリティ要件に制限（モデルチェッカ） 関連理論のライブラリ開発が必要	証明の誤り・バグの発見が困難

プリミティブが理想化できない場合に暗号学的メソッドとの融合が必要

CRYPTRECにおける評価に向けて

- フォーマルメソッドに基づく安全性解析の実績が揃ってきている
- フォーマルメソッドと暗号理論の境界領域の研究が進展してきている
- 検証ツール／理論ライブラリ（Scyther、ProVerif、CryptoVerif、Coqなど）の充実
- 暗号プロトコル評価スキームの標準化の開始（ISO/IEC 29128）

- フォーマルメソッドによる安全性評価の実施（暗号プロトコル公募として世界初?）
  - 信頼性の高い安全性証明
  - フォーマルメソッドツール／ライブラリの信頼性評価が重要（Evidence）
  - 将来のCRYPTRECにおける安全性評価の範囲の拡大
    - ✓ 実システムで用いられる個別プロトコルの安全性評価への展開
- エンティティ認証技術について
  - エンティティ認証は電子政府システムの重要な構成要素（認証の要）
  - 安全が客観的に確認されたエンティティ認証プロトコルに基づいて電子政府システムを構築すべき