第3章 TLSや5G/Bluetooth認証の安全性証明にも使われている「ProVerif」で試す

形式検証ツールを使って暗号の安全性を証明してみる

米山 一樹

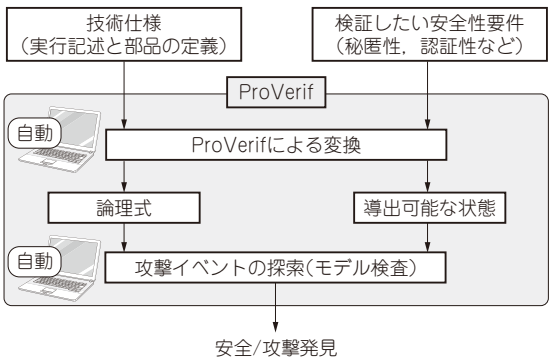

図1　ProVerifの検証手順
ProVerifはフランス国立情報学自動制御研究所のBruno Blanchetが中心になって開発した形式検証のツール

前章で紹介した帰着のような数学的な安全性証明は人間の手で行うため，見落としや間違いによる証明の誤りが起こりえます．実際に，安全性証明が与えられた暗号技術に対して，後になってから証明の誤りが見つかり，安全と考えられていた環境において攻撃が見つかることがあります[注1]．

本稿では，計算機の力を借りることで厳密かつ自動的に安全性を検証するアプローチである形式検証について説明します．主要なツールの1つである検証ツールProVerif（**図1**）を取り上げ，無線LANの端末認証（EAP-SIM）を例として，検証コードの作成と検証結果の読み取り方について説明します．

暗号技術における形式検証とは

● ソフトウェア工学分野における形式手法を応用

見落としのない厳密な安全性を検査する技法として，形式手法を応用した形式検証があります．

形式手法とはソフトウェア工学分野において発展してきた技術です．オートマトン理論や形式言語理論などに基づいて，ソフトウェア設計や実装が仕様通りに正しく動作することを検査したり，矛盾のない整合した仕様を記述したりするためのものです．形式手法は社会においてさまざまなサービスやシステムの開発に実用されています．例えば，パリの地下鉄の制御システムの設計や実装(2)，マイクロカーネルのオープンソース・リアルタイムOSであるseL4の実装の正しさの証明(3)などが挙げられます．

● 計算機を使うことで厳密に検証できる

暗号分野での形式検証とは，形式手法を暗号技術の安全性検証に応用したものです．暗号技術に要求される安全性を仕様，暗号技術のアルゴリズムや実行記述（技術仕様）を設計とみなすことにより，その暗号技術が安全性を満たしているかどうかを検証します．形式検証では計算機を用いることで厳密かつ自動的に安全性を検証することができます．

● 暗号技術をブラック・ボックスとして扱う

形式検証では，部品となる暗号技術を完全に安全なブラック・ボックスとして考えたり，値のビット長などを考慮せず記号として単純化したりするなど，抽象化を行うことによって検証します．従って，人手による安全性証明と異なり，ビットの部分情報や部品の暗号技術の脆弱性を利用した攻撃に対する安全性は捉えられないことに注意が必要です．

形式手法には，大きく分けてモデル検査[注2]と定理証明器の2つの手法がありますが，本稿では主にモデル検査に基づく応用について取り上げます．

形式検証の利点

● 検証範囲は限定的だが厳密な結果が得られる

人手による安全性証明に対して，モデル検査に基づく形式検証の利点の1つとして，抽象化した検証の範

注1：具体例として，ISO/IECで国際標準化され安全と認識されていた共通鍵暗号方式であるOCB2に安全性証明の誤りに起因する脆弱性があることが発見され，標準規格から除外されたという事例(1)がある．

注2：システムの振舞いを一連の状態遷移により表し，システムの満たすべき性質を状態空間の探索により検証する技術．

◆参考文献◆
(1) A. Inoue, T. Iwata, K. Minematsu, B. Poettering：Cryptanalysis of OCB2：Attacks on Authenticity and Confidentiality, J. Cryptol. 33 (4)：1871-1913, 2020.