07

Verification of cryptographic protocols using formal methods

ネットワークの安全性を厳密に評価します

～フォーマルメソッドを用いた暗号プロトコルの安全性検証～

どんな研究

秘匿性やなりすまし防止などのセキュリティが重要となる通信では、暗号技術を組みあわせた**暗号プロトコル**と呼ばれる仕組みを用いますが、その欠陥により思わぬ攻撃が可能になることがあります。本研究はこれを防ぐため、暗号プロトコルの**安全性**を厳密に**評価（検証）**します。

どこが凄い

プロトコルの仕様から、実際にプロトコルを実行することなく膨大な攻撃の可能性を網羅的に調べ、安全性を評価します。膨大な数の攻撃から成功確率が無視できるほど小さいものをあらかじめ除外し、残りの攻撃のみを調べることで**高速化**を可能にしました。

目指す未来

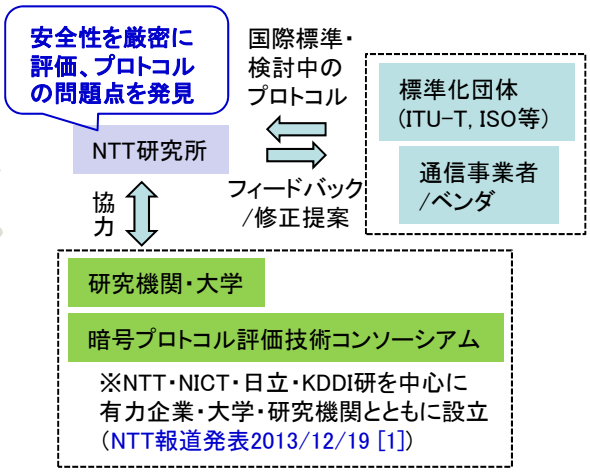
現在の暗号プロトコルは安全性の厳密な保証がないまま使われ、しばしば欠陥が発見されユーザーが危険にさらされたりその修正と再配布に多大な費用がかかるなどします。本技術によりプロトコルの問題点を網羅的に発見でき、広く使用される前に修正できます。

暗号プロトコルの安全性の課題

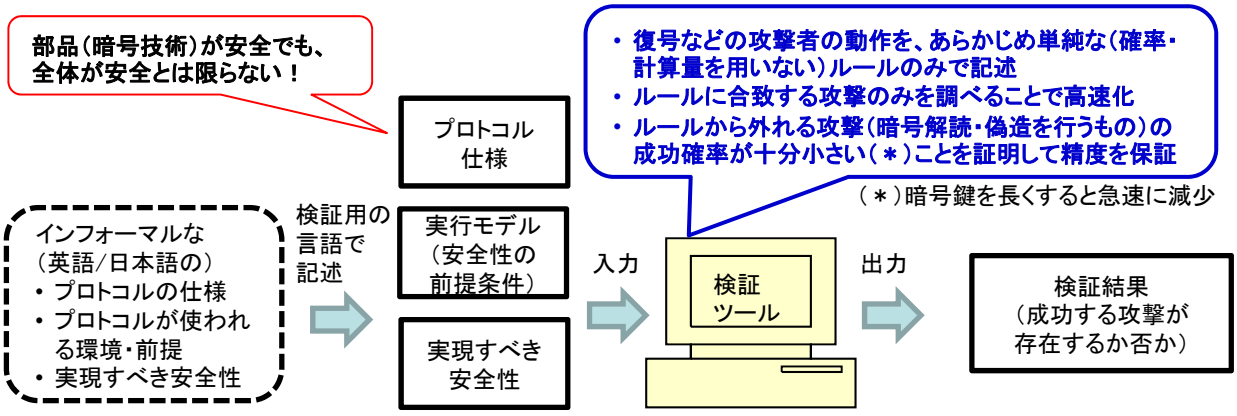
インターネットショッピングなどの通信は暗号技術を応用した暗号プロトコルを利用して保護されるが、

- その安全性（欠陥がないこと）の評価は十分行われていない
- 高精度な評価方法も確立されていない

安全性評価のためアライアンス



高速かつ高精度な安全性評価（検証）を可能に



関連文献

[1] NICT, 日立, KDDI研究所, NTT, “「暗号プロトコル評価技術コンソーシアム」の設立について,” NTT報道発表, 2013

[2] H. Sakurada, “Computational soundness of symbolic blind signatures under active attacker,” in *Proc. The Sixth International Symposium on Foundations & Practice of Security (FPS'2013)*, 2013.

連絡先

櫻田 英樹 (Hideki Sakurada)　協創情報研究部 情報基礎理論グループ

E-mail: sakurada.hideki{at}lab.ntt.co.jp ({at}の部分を@に置き換えてください)