課題179 暗号プロトコルの安全性評価手法の拡張に関する研究開発

セキュリティ対策技術の主要な部品である暗号プロトコルについて、その安全性を様々な使用環境において確認する必要がある。暗号プロトコルの安全性評価手法として、暗号プロトコルがどのような環境で使用しても安全であること（汎用的結合可能性）を形式的に検証する評価手法が、これまでに研究開発されている。しかし、ソフトウェアでは未実装であり、ITU-T, IETF, ISO/IEC, IEEEなどで国際標準化されているプロトコル（実プロトコル）の検証における実用上の課題が不明である。本委託研究では、従来手法の実用上の課題を明らかにし、その解決方針を検討することで、実用に耐えうる汎用的結合可能性の評価手法の確立につなげる。

背景と課題　実プロトコルの安全性を様々な使用環境で確認したい

- 暗号プロトコル(*)の設計に起因するセキュリティ問題が多く発見
  - 無線LANの認証と暗号化、SSL/TLSで通信内容の漏洩やなりすましなど
  - 使用している暗号そのものの問題や、実装上の問題ではない
- 広く使われる実プロトコルでは、様々な使用環境での安全性確認が必要
  - 実プロトコル：標準化団体によって規格化され（あるいは規格化されつつあり）、現在使用されている（あるいは今後使用される見込みがある）暗号プロトコル
- どのような使用環境でも安全性を保証する「汎用的結合可能性」の評価手法が提案されているが、ツールとして未実装であり、実用上の課題が不明
  - 実プロトコルに適用可能か否か、評価に必要となる計算量が爆発しないか否か

本委託研究の目的

- 様々な使用環境における安全性確認を可能とする汎用的結合可能性の評価手法について、実用上の課題を明らかにし、特に重要な課題を解決
- 実用に耐えうる評価手法の確立につなげる
- 実プロトコルの安全・安心な使用

研究開発の概要　汎用的結合可能性の評価手法の拡張とツール化

- 必須項目
  1. 汎用的結合可能性の従来評価手法のツール化
     - 評価能力は落とさず、NICTが事務局を務めるコンソーシアムCELLOSの使用に耐える
  2. 現時点で明らかな課題の解決（評価対象とできる暗号プロトコルの制約緩和）
     - ハッシュ関数を使う暗号プロトコルも評価対象とする
  3. 実プロトコルによる有効性確認、実用上の課題を明確化
- 実施することが望まれる項目
  - ツールの使いやすさ
    - 暗号設計者・研究者に分かりやすい入出力形式、インターフェース
  - 有効性確認の実用上の意義
    - 現在広く使われている、今後広く使われる見込みのある実プロトコルを数多く評価
  - 新たに発見した課題の解決、現時点で明らかな課題のさらなる解決
    - 有効性確認によって新たに明らかとなった課題を解決
    - メッセージ認証子、共通鍵暗号を使う暗号プロトコルの評価対象とする

自ら研究との関係

- 評価結果をセキュリティ知識ベース・分析エンジンREGISTAに組み込む
  →これまでセキュリティ知識ベースに蓄えられなかった安全性レベルの情報を蓄積
- 評価結果をセキュリティアーキテクチャ研究室の暗号プロトコル評価ポータルサイトに掲載
  →プロトコルはどの程度安全かという情報を、プロトコルユーザに提示（どこで使っても安全か、使用環境によるのか）

(*)暗号を用いた通信手順、通信相手の認証や通信内容の秘匿などの各種安全性の確立を可能とする

研究開発期間：平成26年度～平成28年度　（3年間）
26年度予算：　30百万円