論文の内容の要旨

論文題目　攻撃モデルに基づいた暗号モジュールの評価に関する研究

氏名　山岸　篤弘

さまざまな社会基盤に情報通信システムが組み込まれ、さらに、異種の社会基盤ともネットワーク化されるようになっている。この様な情報通信システムで扱うデータや情報に対する侵害は、社会システムの存続さえ左右しかねない。そのため、ネットワーク化された情報システムの安全性の確保は、重要な課題になっている。情報システムの安全性を実現する上で、暗号技術は重要な中核技術であり、情報システムの安全性を確保するためには、暗号技術の安全性を確保する必要がある。暗号アルゴリズムの数学的な安全性評価は、近年の米国のAES 選定プロジェクト、我が国のCRYPTREC プロジェクト、欧州のNESSIEプロジェクト等を通じて長足の進歩を遂げている。しかし、情報システムで実際に使用されるのは暗号アルゴリズムを、ハードウェア、ソフトウェア、ファームウェア、あるいはそれらの組み合わせである「暗号モジュール」である。　従って、情報システムの安全性を確保するためには「暗号モジュール」の安全性の評価が重要となる。暗号モジュールの工学的な安全性評価に関しては、適合性評価として知られている枠組みで行われ、米国とカナダが共同運用している暗号モジュール評価制度CMVP(Cryptographic Module Validation Program)が最もよく知られている。このCMVP制度では、1980年代に米国国防総省が定めた技術基準を基に２度の改訂を経て現在に至っている。この要求基準は、暗号モジュールに必要とされる最低限のセキュリティ機能を定めているので、ユーザーとベンダー双方にとり理解しやすい内容となっている。しかし、制定されてから20年以上経過し、新しい実装技術や攻撃技術への対処が困難となってきている。　そこで、本研究では暗号モジュールに対して加えられる攻撃法を前提として、暗号モジュールに対するセキュリティ要求基準を再構成することを提案している。また、評価された暗号モジュールを用いた情報セキュリティシステムの設計法を提案する。