審査の結果の要旨

論文提出者氏名　山岸　篤弘

本論文は，「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」と題し，情報セキュリティシステムに組み込まれ暗号処理機能を提供する暗号モジュールの適合性評価に関し，新たな提案を行ったものである．まず，暗号モジュールの適合性評価の基準となる「セキュリティ要求」を，暗号モジュールに対する脅威，すなわち，暗号モジュールに対する攻撃に基づいて作成することを提案している．また，適合性認証を受けた暗号モジュールを利用した情報セキュリティシステムの設計手法と日本における暗号モジュールに対する適合性認証制度の在り方に関して提案している．これにより，暗号モジュールに対するセキュリティ要件を暗号モジュールに対する脅威に対応して構成することが可能となり，情報セキュリティシステムの設計過程から当該システムが必要とする暗号モジュールのセキュリティ要件を決定することが容易になることを示している．論文の構成は「序論」を含めて６章からなる．

第１章は「序論」で，暗号技術を取り巻く環境と本研究の背景と位置付けについて整理している．ここでは，暗号技術を取り巻く環境として，暗号技術の用途が大幅に広がりつつあり，暗号アルゴリズムだけでなく暗号アルゴリズムを実装した「暗号モジュール」の安全性評価の重要性が高くなっていることを強調している．

第２章は，暗号技術の簡単な解説と安全性評価に関する動向を整理した上で，情報セキュリティシステムで暗号技術を利用する場合に用いられる「暗号モジュール」とその評価についての動向を紹介し，その中で，暗号システムの安全性・信頼性を向上させていくために必要な研究の方向を提示している．特に，暗号モジュールの評価の動向に関しては，暗号システムの用途の拡大や実装技術の多様化に伴い，評価対象となる暗号モジュールが直面する新たな攻撃技術の動向に関しても整理し，次章の提案に関する根拠を明らかにしている．

第３章は「攻撃者モデルに基づく暗号モジュール評価」と題し，暗号モジュールの評価の現状を適合性評価の立場から概括し，現在の暗号モジュールに対するセキュリティ要件は，限定された使用環境を想定したものであるために汎用性に乏しく，しかも暗号モジュールに対する攻撃技術の進歩に追従しにくいことを指摘している．この問題点を解決するために，暗号モジュールに対して加えられる攻撃と暗号モジュールの構成の分析に基づいてセキュリティ要件や暗号モジュールの構成要素毎に攻撃要素を定義し，さらに暗号モジュールのセキュリティレベル毎のセキュリティ要件を攻撃要素に基づいて構成する手法を提案し，その有効性を論じている．

第４章は「暗号モジュール評価制度」を題し，情報セキュリティシステム評価制度（Common Criteria）や米国やカナダの暗号モジュール評価制度（CMVP）を参考にして，日本における暗号モジュール評価制度の提案を行っている．ここでは，先行する情報セキュリティ評価基準との整合性・補完性を考慮する必要があることを指摘し，その前提の下で，我が国が目指すべき暗号モジュール評価制度としては，国際的な相互承認制度を目指すことを最終的な目標とすべきであるが，要員の教育や制度維持のためのコストを勘案した移行措置が重要であること述べ，その具体的方策を提示している．

第５章は「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」と題し，既存の情報セキュリティシステムの設計手法に基づき，暗号モジュールが曝される脅威・攻撃から，当該システムで用いるべき暗号モジュールに求められるセキュリティ要件の抽出法とセキュリティレベルの決定方法について提案を行っている．特に，先行する米国・カナダにおける暗号モジュール評価制度では，情報セキュリティシステムの設計結果から，使用すべき暗号モジュールのセキュリティレベルを具体的には決定しにくいという問題点が存在するが，本研究の提案を用いることで，暗号モジュールの満たすべきセキュリティレベルを具体的に決定できることを示している．

最後に第６章は「結論」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文は暗号モジュールに対する攻撃モデルに基づくセキュリティ要件，それに基づく暗号モジュールの適合性評価制度およびその導入法，情報セキュリティシステム設計手法に基づいた暗号モジュールに対するセキュリティレベルの選択方法を提案したものであり，特に暗号モジュールの適合性評価制度に関しては，本論文での提案を基盤に我が国の制度が構築されつつあり，電子情報学，特に情報セキュリティ分野上貢献するところが少なくない．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる．