審査の結果の要旨

論文提出者氏名　　宮崎　邦彦

本論文は，「デジタル社会の証拠性を支える電子署名技術に関する研究」と題し，デジタル社会の証拠性を支える技術としての電子署名技術における課題を挙げ，それらに対する解決策を提案している．電子データの真正性を保証する技術である電子署名技術は、従来、認証や電子申請等の比較的短い時間で完結する処理での利用が中心であった．しかしながら，近年，「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（電子文書法）」が施行され，関係省令等で，長期間の保管が義務付けられた文書を，紙ではなく，電子的に保管する際に，電子署名を付与することが求められるなど，電子データの長期間にわたる証拠性を支える技術としての，電子署名技術の利用へのニーズが高まっている．証拠性を支える技術としての電子署名技術は、従来の電子署名技術とは異なり，秘密鍵漏洩の危険性及び影響が大きいこと，署名を付与された後のデータに対する適切な変更要求がありうること，への配慮が求められる．本論文は，これらの課題に対する有効な解決策を示したものである．論文の構成は「序論」を含めて５章からなる．

第１章は「序論」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第２章は「秘密鍵漏洩問題への対策技術」と題し，証拠性維持目的での署名技術に求められる要件のひとつである秘密鍵漏洩問題を取り上げ，この問題に対する対策技術を分析し，鍵漏洩防止型対策と，被害防止型対策とに分類している．さらに，前者に分類される対策技術として，今後情報処理装置として中心的な役割を担うことが期待される IC カード等の小型端末でも実装可能な，効率的なしきい値署名方式を提案している．また，後者に分類される技術について，従来から知られている長期利用文書向けのさまざまな技術を，各々の技術が明示的あるいは暗黙のうちに仮定している，第三者機関への依存度の観点から評価し，これらの技術をデジタル社会の証拠性を支える基盤技術として活用するために，基盤として整備すべき第三者機関の役割を明らかにしている．

第３章は「署名者による秘密鍵自己漏洩攻撃とその対策技術」と題し，秘密鍵漏洩問題に対し，署名者自身による攻撃の可能性について論じている．従来，署名者が自身の秘密鍵を安全に管理することは，署名者自身にとっての利益であり，したがって，これに反す

る行為を行う動機はないと考えられることが普通であった．しかし，本論文では，ゲーム理論を用いて，署名者の状況によっては，自ら秘密鍵を公にさらすことが，署名者自身にとってもメリットとなるケースがあり，攻撃として成立しうることを示している．また，この分析結果をもとに，どのような方針で対策を講じることが効果的であるかを示し，具体的な対策技術を提案している．

第４章は「電子文書墨塗り問題とその対策技術」と題し，証拠性維持目的での署名技術に求められるもうひとつの要件である，署名を付与されたデータに対する適切な変更への対応技術について述べている．電子署名技術は，もともと 1 ビットでもデータを変更すると検知できるように設計された技術である．ところが，証拠を保つ目的で署名を付与され，保管されたデータは，そのままで利用されるとは限らない．たとえば，行政機関における活動記録として保管された行政文書は，市民・国民からの請求に応じて公開されることがあるが，そこに含まれる個人情報や国家機密情報は，墨塗りされた上で公開されることが定められている．この場合の墨塗りは，個人情報保護の観点からは，適切な処置であるが，一方で，署名の検証を妨げるため，データの真正性保証と情報漏洩防止を両立できない結果となる．本論文では，この問題を解決するための電子署名技術に求められる基本的な要件を整理し，それらを満たす対策技術を提案している．また，多くの電子データにおいては，基本的な要件に加え，さらに，開示条件の制御が可能であること，墨塗り箇所の長さを秘匿可能であること，ビット単位での墨塗り箇所の指定が可能であること，などの追加的な要件が望まれることを指摘し，これらを満たす改良方式について提案している．

最後に第５章は「まとめと今後の展望」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，デジタル社会の証拠性を支える技術として，電子署名技術が備えるべき要件に関する基礎検討を行うとともに，それらの要件を満たす電子署名技術を具体的に明示するものであり，電子情報学，特に情報セキュリティ工学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．