論文の内容の要旨

論文題目　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

氏名　宮崎　邦彦

インターネット等の情報ネットワークの発展に伴い，ネットワーク上での電子商取引，電子申請等，従来は紙文書によって処理されていたさまざまな手続き，サービスが電子化されるようになった．これらの電子化されたデータの真正性を保証する技術として，電子署名技術が注目されている．

電子署名は，秘密鍵と呼ばれる特別な情報を知るものだけが生成することができ，また，その正当性は，公開鍵と呼ばれる誰もが入手可能な情報によって確認できるという特徴を持つ．これらの特徴から，認証，否認防止，改ざん検知，などの機能を実現する技術になると期待されている．しかしこれまでのところ，実際の利用については，主に認証や電子申請など，比較的短い時間で完結する処理での利用に限られていた．

ところが，近年，電子署名を，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利用されるようになってきた．たとえば，平成 17 年 4 月 1 日には「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，長期間の保管が義務付けられた文書を，紙ではなく，電子的に保管できるようになったが，重要な文書については，その証拠性を保つために，電子署名を付与することが，省令等で定められている．また，企業や組織に対して内部統制が重視されるようになり，業務遂行のログを残すことが求められつつある．このログの証拠性を保つ目的でも，電子署名の利用が期待されている．

本論文では，上述のような，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電子署名を利用した場合における課題を挙げ，それらに対する解決策を提案する．

従来の認証目的での利用における電子署名に対する要件と，長期間にわたる証拠性を支える技術としての電子署名に対する要件の違いとしては，次の 2 点が挙げられる．

1. 長期にわたる証拠性目的で利用する場合は，認証等を目的とした短時間の利用の場合と比較し，秘密鍵漏洩の危険性が高く，また影響が大きい
2. 長期にわたる証拠性確保目的で署名を付与されたデータは，保存期間中に編集される可能性がある

1 に挙げた秘密鍵漏洩は，認証等を目的とした場合においても課題となる．しかし，短時間で処理が完結する場合には，仮に秘密鍵が漏洩したとしても，直ちに，その秘密鍵が不正に利用されることを止められれば，影響の範囲は限定される．実際に現在の PKI においては，鍵を無効化する仕組みが整備されている．一方，証拠を保つ目的での電子署名の利用においては，秘密鍵の漏洩は，より深刻な問題となる．なぜなら，鍵

を無効化するだけでは，新たな不正は防止できても，過去に築かれたデータの証拠性が失われることは防止できないからである．特に，これらのデータが，たとえば契約書類のような，実質的に金銭的な価値を持つデータであった場合には，大きな問題になる．

2 に挙げた，署名付与後のデータに対する編集の問題は，電子署名を長期間にわたる証拠性を支える技術として利用した場合に固有の課題である．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．

本研究では，秘密鍵漏洩問題に対する対策技術として 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する．また，署名者自らが秘密鍵を漏洩する行為について，それが署名者にとって不正な利益をもたらす可能性について議論し，対策技術を提案する．署名付与後のデータに対する編集，特に墨塗りに対しては，署名付きデータを墨塗りした後であっても検証可能な新しい電子署名技術の提案を行う．