論文審査の要旨および学識確認結果

報告番号	甲　第　　号	氏　名	手塚　伸

論文審査担当者：				
	主査	慶應義塾大学　教授	工学博士	岡田　謙一
	副査	慶應義塾大学　教授	工学博士	笹瀬　巌
		慶應義塾大学　教授	博士(工学)	重野　寛
		慶應義塾大学　准教授	博士(理学)	河野　健二

(論文審査の要旨)

学士（工学），修士（工学）手塚伸君提出の博士学位請求論文は「クラウドストレージにおける電子文書の削除と完全性の保証に関する研究」と題し，全7章より構成されている．

近年，インターネットの普及やe-文書法の施行により，多くの文書が電子的に扱われており，これらをクラウドストレージ上で管理する試みがなされている．なかでも，医療や国税関係の書類は，定められた一定の期間は機密性，完全性が担保される形で保全される必要がある．他方，その期間が経過した後は，プライバシーや機密保持の観点から確実な削除が求められる．しかし，高度に抽象化されたクラウドストレージでは，記憶デバイスを直接操作できないため，ユーザがこれを実施したり確認したりすることができないという，削除保証の問題があった．削除保証を実現するために，暗号化を用いた関連研究もあるが，削除実施の条件となるポリシーを論理演算で複数指定することや，保存義務期間を超過した版のみの削除といった複雑な操作を行うことができなかった．また，これらはファイルの変更記録の完全性を保証する点については留意していなかった．

そこで手塚君は，ファイルの削除を保証するために用いる暗号鍵の生成方法に着目し，ハッシュ関数と(n, k)閾値秘密分散法を用いた手法を提案している．これにより，保存義務期間の長さや，複数ユーザによる共有の有無といった文書の性格に応じて，完全な削除を実施する条件を論理演算で指定し，柔軟に制御することが可能となった．さらに，ファイルの変更記録に対してヒステリシス署名を適用することで，変更記録の順序性を含めて完全性が保証される．また，本研究で開発されたファイルシステムは削除と完全性の保証に関する手法の適用に加えて，他のファイルシステムと透過的なインターフェースを提供している．これにより，利便性の向上や既存のソフトウェア資産の有効活用が可能となった．

本論文の構成を以下に示す．本論文は全 7 章から構成され， 1 章では本研究の背景と位置づけ，学術的貢献について述べている．

2 章では，クラウドストレージで文書を管理する上での一般的な問題を法律，運用，セキュリティの観点から整理し，本研究が着目した削除と完全性の保証に関する関連研究の技術的な課題について詳述している．

3 章では，削除保証と完全性の保証に対して，本研究の中核となる 2 つの手法について述べている．まず，ハッシュ関数で連鎖された暗号鍵を導入することで，ファイルの一部の変更記録に対する削除保証を実現する手法について記している．そして削除を実施するための条件を AND/OR の論理演算で指定できるように，(k, n)閾値秘密分散法を導入した手法について述べている．次に，第三者機関に頼らずに，保存されたファイルの各版の完全性を保証するため，ヒステリシス署名と Merkle Hash Tree により生成された電子署名を複数のクライアントへ分散保存させる手法について述べている．

4 章では，クラウドストレージに対して定期的にファイルを増分バックアップする環境を対象に，削除保証の手法を適用したクラウド型ファイルバックアップシステムについて述べ，5 章では，削除保証に加えて，ファイルの完全性を保証するための手法を適用した仮想ファイルシステムについて述べている．

また，6 章では提案手法およびシステムの安全性や今後の課題について考察し，7 章で本研究の結論を述べている．

以上のとおり，本研究により，クラウドストレージ上の電子文書に対して，機密性，完全性が保たれた状態で，より柔軟な管理と確実な削除を実現する手法が示された．これらの研究成果は，工学上，工業上寄与するところが少なくない．よって，本論文の著者は，博士（工学）の学位を受ける資格があるものと認める．

学識確認結果	学位請求論文を中心にして関連学術について上記審査委員会委員で試問を行い，当該学術に関し広く深い学識を有することを確認した． また，語学（英語）についても十分な学力を有することを確認した．