学位論文 博士（工学）

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

2014年2月

慶應義塾大学大学院理工学研究科

手塚 伸

主　論　文　要　旨

報告番号	甲　乙　第　　号	氏　名	手塚　伸

主論文題目：

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

（内容の要旨）

近年，e-文書法の施行により，保存義務期間が定められた電子カルテや国税関連の書類など，プライバシーや機密情報を多分に含む書類が電子的に扱われている．他方，クラウドコンピューティングが注目を集めており，電子文書をクラウド上で管理する試みがなされている．しかし，クラウドにはセキュリティに関連する問題も多いのが現状である．

そこで本研究では，クラウドストレージにおける「削除保証」と「完全性の保証」という問題に着目した．削除保証とは，保存されたデータが完全に削除され，それ以後は何人であってもデータを復元できないことを保証することである．しかし，高いレベルで抽象化されたクラウドストレージでは，物理デバイスをユーザが直接操作できないため，これを実現する手法が必要とされている．また，e-文書法ではファイルの変更記録とアクセスログについても完全性が保証される形で保全することが求められている．

既存研究にも，削除保証を目的としたものがある．しかし，追記型のファイルに対して保存義務期間を超過した版のみの削除ができない点や，共有ファイルに対して柔軟な削除条件の指定ができないなどの課題があった．また，それらはファイルの完全性や変更記録の順序性については留意していない．

そこで，本研究では２つの手法を提案した． 第一の手法は，ハッシュ関数による連鎖鍵と(k, n)閾値秘密分散法により，削除条件を制御する暗号鍵を生成する手法である．これにより，アクセスログなどの追記型ファイルに対して，保存義務期間を超過した版の削除保証を可能にする．また，AND/OR 演算を含む複数ポリシに基づいた削除保証が可能となり，複数のユーザやグループにファイルが共有されるような場合でも，適切な削除条件の設定が実現される．

第二に，本研究ではヒステリシス署名を応用した手法を提案した．これは，各ファイルの変更記録に対するヒステリシス署名を Merkle Hash Tree で集約し，組織内のクライアントへ分散保存するものである．これにより，署名履歴のロールバックアタックを防止し，ファイルに対する変更記録の完全性と順序性が保証される．

実装面では，クラウドストレージをバックエンドとする仮想ファイルシステムを開発し，上記の２つの手法を具現化させた． また，この仮想ファイルシステムでは，通常のファイルシステムと透過的なインターフェースが提供される．そのため，組織は既存のアプリケーション資産を活かしながら，クラウドへの移行を実施できる．また，評価実験の結果より，提案手法がパフォーマンスに与えるオーバーヘッドは小さく，有用であることを検証した．

SUMMARY OF Ph.D. DISSERTATION

School School of Science for Open and Environmental Systems	Student Identification Number	SURNAME, First name TEZUKA Shin

Title

A Study on Deletion and Integrity Assurance of Electronic Documents for Cloud Storage

Abstract

Recent years, because of the enforcement of the e-Document Law, documents that include sensitive and private information, such as medical records, and documents that are related to the national tax are now handled electronically. At the same time, "the cloud" is considered to be a viable location to store such documents; however, cloud computing has several security concerns.

Therefore, this study focused on the assured deletion and the integrity of files on cloud storage. Assured deletion means that files are securely deleted so that no one can retrieve them after the deletion. Because cloud storage is highly abstracted, users cannot control the storage device directly; therefore, they cannot verify the complete deletion of the file. Furthermore, the e-Document Law requires organizations to preserve the integrity of the file's version history as well as the access logs.

Some studies have attempted to achieve assured deletion. However, they cannot delete only the file's versions whose retention period has elapsed according to the law. They also do not enable users to delete files according to flexible deletion conditions. Moreover, none of these studies considered the integrity of a file and the order of its versions.

To overcome these problems, we propose two methods. The first method is based on a hash chained encryption key and a (k, n) threshold secret sharing scheme to control the deletion conditions of a file. This allows users to delete part of the file's version, such as a recordable access log file. Further, the method allows the assignment of flexible deletion conditions to a file based on multiple policies, including AND/OR operations. Even if the file is shared with users or groups, it can be assigned accurate deletion conditions.

The second method is the hysteresis signature scheme with the Merkle Hash Tree. The method aggregates the hysteresis signatures of the file versions using Merkle Hash Tree and distributes it to client PCs in the organization. This strategy can prevent a roll-back attack on signature histories and can guarantee the integrity of a file and the order of its versions.

These two methods are implemented as a virtual file system that uses storage in the cloud as the backend storage. This virtual file system provides a transparent interface to generic file systems, and the organization can utilize existing applications. Furthermore, the evaluation results show that the proposed methods require minimal performance overhead.