要 旨

SAS を用いた安全な
ファイル共有方法の提案

多田菜南

近年，クラウドストレージサービスを利用してファイルの保存や共有をする場面が増えている．これらのサービスは低コストで容易に利用を開始することができるためユーザの利便性が高い一方，ユーザがアップロードしたファイルは常にオンライン上に晒されるため情報漏洩の危険がある．そのため，ユーザはクラウドストレージサービスを利用してファイルの保存・共有を行う場合，ユーザ自身がファイルを暗号化することで第三者への情報漏洩を防ぐことができる．しかし，ファイルを暗号化したとしてもファイルを復号できる権限をサービス提供者が持っている場合，サービス提供者の不正による情報漏洩を防ぐことができない．既存システムではサービス提供者がファイルを復号できる権限を持つことになり，サービス提供者の不正によって起きる情報漏洩の危険が残る．

本論文では，暗号化されたファイルと暗号鍵の管理者を分け，ワンタイムパスワード認証方式 SAS を用いた第三者に鍵管理を委託した場合でも安全にファイル共有することのできるファイル共有システムを提案する．また，提供システムの実装を行い，提案システムは実用上問題ない時間で動作することを確認した．

キーワード　ファイル共有, ワンタイムパスワード, SAS, SAS-2

Abstract

Proposal of a secure sharing method for confidentiality files using SAS

Nana TADA

In recent years, scenes of storing and sharing files using cloud storage services are increasing. Since the cloud storage services are easy to use at low cost, the services's users can use it convenience. However the users uploaded files are constantly exposed in online, and then there are risks of information leakage. When the users store and share files by the cloud storage service, the users encrypt sharing files to protect information leakage to third parties. However even if the files are encrypted, the service provider has the authority to restore the file. Therefore it will not be possible to prevent information leakage to fraud by the service provider.

In this paper, I propose a secure sharing system by using SAS, which the one-time password authentication method. the system divided the administrator of the encrypted file and the encryption key, and share files safely. Therefore if encryption keys management server is entrusted to a third party, there is no risks. Also, I implemented the system. I confiremed that this result is within the the allowable range time.

key words File Sharing, One-Time Password, SAS, SAS-2