2Z-9

単一の鍵で多重帰属できるグループファイル共有システムの実装

佐々木　啓[†]　長澤　悠貴[†]　毛利　公美[††]　福田　洋治[‡]　白石　善明[†]　野口　亮司[†††]

名古屋工業大学[†]　岐阜大学[††]　愛知教育大学[‡]　(株)豊通シスコム[†††]

1. はじめに

近年，クラウドから提供されるサービスの利用場面が拡大している．クラウドサービスの一つにグループウェアがある．グループウェアとはグループ内でのコミュニケーションツールであり，電子メール／スケジュール／会議室予約／掲示板／ファイル共有などの機能がある．報告[1]によると，53.7%の企業がクラウド型のグループウェアを「現在利用している」「利用すべく評価中」「利用することを検討している」となっている．

ここで，グループウェアの中のグループファイル共有を考えると，ファイルはサービス提供側のサーバで保管するため，クラウド提供者の不正が懸念される．我々は既に，利用者側での暗号化によりサービス提供者にファイルの内容を知られず，かつ利用者が複数のグループに多重帰属する場合でも鍵管理の負担を軽減できるプロトコルを提案している[2]．そこで，本稿では，提案プロトコルを組み込んだグループファイル共有システムの実装について述べる．今回実装するグループファイル共有システムはローカルクライアントアプリを各メンバの端末にインストールし，ユーザがログインして使うものを考えている．実装する上では，鍵管理のための DB の設計についてと，グループファイル共有に求められる UI についての検討が必要である．そこで，サーバ側／クライアント側での DB 設計と Flex を使った UI の設計について検討する．

2. 単一の鍵で多重帰属できるグループファイル共有プロトコル

2.1 クラウド型グループファイル共有の課題とプロトコルの概要

クラウド上でのファイル共有を実現する際の課題として，サーバ管理者による閲覧を不可能にすることが挙げられる．そのためには，クライアント側で暗号化を行う必要があるが，クライアントが複数グループに多重帰属する場合，グループ毎に秘密鍵が必要であり，鍵管理が難しい．そこで，我々は以下の方法を提案している[2]．グループ秘密鍵を（2,2）閾値秘密分散で二つに分け，一方をサーバが保持するサーバ部分復号鍵とし，もう一方をメンバの保持するメンバ部分復号鍵とする．同じようにメンバ部分復号鍵に対して秘密分散を繰り返し適用し，生成された二分木構造（図 1）を用いて鍵を管理する．ファイルは共通鍵であるファイル復号鍵で暗号化し，ファイル復号鍵はグループ公開鍵で暗号化される．暗号化されたファイル復号鍵はサーバ部分復号鍵によって部分復号され，メンバ部分復号鍵によって完全復号される．

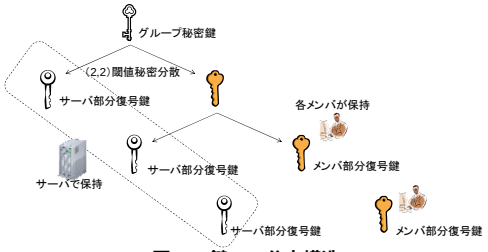

図 1　鍵の二分木構造

Implementation of Group File Sharing System Based on a Certain Secret Sharing Scheme

†Kei Sasaki, Yuuki Nagasawa, and Yoshiaki Shiraishi・Nagoya Institute of Technology

‡Youji Fukuta・Aichi University of Education

††Masami Mohri・Gifu University

†††Ryoji Noguchi・Toyotsu Syscom Corporation

2.2 5 つのプロトコル

［ファイル共有プロトコル］ファイル暗号化とファイル復号を行う．ファイル暗号化では，ファイル復号鍵を生成し，ファイルを暗号化する．ファイル復号鍵をグループ公開鍵を用いて暗号化し，ファイルと共にサーバに保管する．ファイル復号では，暗号化されたファイル復号鍵をサーバ部分復号鍵を用いて“**部分復号**”し，メンバ部分復号鍵を用いて“**完全復号**”する．復号されたファイル復号鍵でファイルを復号する．

［グループ構築プロトコル］分散構造を成す全ての鍵の生成，及び生成した鍵の保管サーバとメンバへの配布を行う．

［メンバ追加プロトコル］最後に追加されたメンバの部分復号鍵を更に（2,2）閾値秘密分散し，新たなメンバ及びサーバ部分復号鍵を生成し，配布する．

［メンバ離脱プロトコル］離脱メンバの親メンバの部分復号鍵を（2,2）閾値分散し，離脱メンバの子メンバに再分散する．

［鍵更新プロトコル］ルートノードメンバとサーバはプロアクティブ秘密分散[3]により部分復号鍵を更新し，その他メンバの部分復号鍵を更新する．

3. 実装上の課題とその解決

3.1 課題 1：鍵管理

本プロトコルでは機密保持すべき鍵の構造が一般的な鍵構造と異なるため，鍵管理方法の検討が必要である．まず，保持する必要のある鍵は表 1 のとおりである．なお，メンバ部分復号鍵はメンバのパスワードのハッシュ値で暗号化したものをサーバが保持する．

表 1　保持する必要のある鍵

ファイル復号鍵	ファイルを暗号化している共通鍵．グループ公開鍵で暗号化されている．各ファイルに対して一つある．
サーバ部分復号鍵	ファイル復号鍵の部分復号に必要な一つ目の鍵．各グループに対しグループ人数＋１個ある．
メンバ部分復号鍵	ファイル復号鍵の完全復号に必要な二つ目の鍵．各メンバに対し一つある．

これらを全ての ID やファイル本体と同様に DB に格納する．各鍵の構造からファイル復号鍵・サーバ部分復号鍵・メンバ部分復号鍵はそれぞれ，ファイル・グループ・ユーザテーブルに格納する．このとき，メンバ追加／メンバ離脱／鍵更新プロトコルではグループへのメンバ追加順が必要であるため，グループ情報管理テーブルとは別に，各グループごとに，追加された順にグループメンバ ID とサーバ部分復号鍵を格納するテーブルが必要である．これらを考え，次のように DB を設計した．

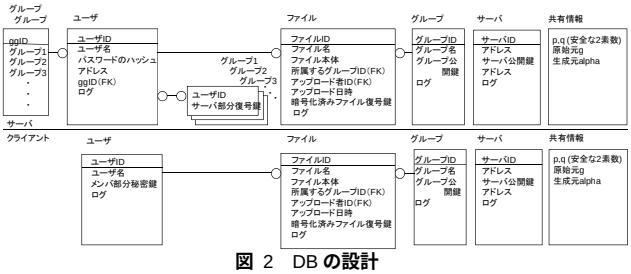

図 2　DB の設計

グループグループテーブルの内容はフラグであり，ユーザは ggID から立つフラグを調べることで所属するグループを特定する．

3.2 課題 2：インターフェース

グループウェアを利用するユーザは使い勝手に不安や不満を持っている[4]．グループウェアは毎日使われるツールであるため，UI の使い勝手は検討する必要がある．

使い勝手の良い UI を作るための技術として，リッチインターフェースが挙げられる．これは，従来のようにリンクやボタン

から画面遷移を行うことなく，シームレスに画面を更新させることでスムーズな操作性を提供する技術である．具体的にはAjax や Adobe Flex が挙げられる．これらは HTML や MXML などのマークアップ言語と JavaScript や ActionScript などのスクリプト言語を組み合わせて実装する．

スクリプト言語を GUI に使用する場合，新たな課題が発生する．スクリプト言語は表現力が高く動的な表現を行うことができるが，計算速度は速くない[5]．暗号化／復号には相応の計算が必要であるため，GUI の部分をスクリプト言語で実装し，Java や C などのコンパイラ型言語で暗号化ライブラリを実装する方法が考えられる．このとき，ユーザ端末内においてスクリプト言語とコンパイラ型言語の間でファイルやユーザのデータを受け渡す必要があるが，このようなデータ受け渡しはサポートされていない場合が多い．ここではソケット通信を用いてデータの受け渡しを実現する．具体的には，コンパイラ型言語でサーバソケットを用意し待ち受け，スクリプト言語でのインターフェース部分を立ち上げる．その後，インターフェース部分からサーバソケットへ接続を行う．

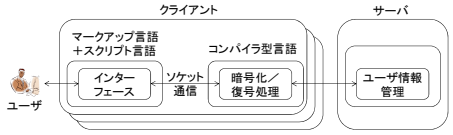

図 3　異種言語のプログラムの接続

使いやすい UI の条件として，操作性の向上が挙げられる．グループファイル共有においては各操作に必要なクリック数・画面遷移数である．操作頻度の高いグループ切り替えには，画面遷移なしで直感的にデータ集合を切り替え表示できるタブ機能を用いる．ファイルアップロード／ダウンロードにおいては OS でのファイル操作と同等の操作感とするためドラッグ＆ドロップができるようにする．

4. 実装

インターフェース部分を Adobe Flex4.0[6]，暗号化ライブラリを含むその他の部分を Java JDK6 を用いて開発した．使用した DB は，サーバ側では MySQL Server 5.1[7]を，メンバ側では SQLite 3.7.4[8]を使用した．

Adobe Flex 4.0 には Web アプリケーションとして Flash プログラムを実装する方法と，デスクトップアプリケーションとして AIR 上に実装する方法がある．今回はドラッグ＆ドロップを使うために AIR 上に実装した．

本システムの持つ機能はログイン／ログアウト，ファイルアップロード，ファイルダウンロード，グループ構築，グループへのメンバ追加，グループからのメンバ離脱，鍵更新である．

システムの構成は次に示す．

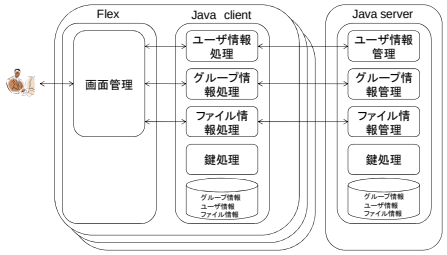

図 4　システムの構成

［画面管理部］共有しているファイルをグループ毎に表示し，ユーザの操作命令／入力を受け付ける．

［鍵処理部（クライアント／サーバ）］ファイル／ファイル復号鍵の暗号化／復号，部分復号鍵の算出を行う．

［ユーザ情報処理部］ユーザの入力したパスワードとサーバ側のパスワードのハッシュ値からユーザ認証を要求する．

［ユーザ情報管理部］ユーザを登録，またユーザの鍵やパスワードのハッシュ値，所属グループを更新する．ログイン情報を保持する．パスワードによるユーザ認証を行う．

［グループ情報処理部］グループ情報を取得する．グループ更新を要求する．

［グループ情報管理部］グループの構築・メンバ追加・メンバ離脱・鍵更新を行う．

［ファイル情報処理部］ファイルをサーバより取得．DB の差分をクライアント側 DB に反映する．ファイルの暗号化・復号を要求する．

［ファイル情報管理部］サーバ側 DB のファイルを取得・更新する．

各操作の動作手順を以下に示す．

［ログイン］画面管理部がユーザから ID，パスワードを取得する．ユーザ情報処理部が認証を行う．ファイル情報処理部がファイル情報を取得し，画面管理部がユーザへ表示する．

［ログアウト］画面管理部がユーザからログアウト命令を取得し，ログイン画面へ画面遷移する．ユーザ情報処理部はログアウトをユーザ情報管理部へ伝える．

［ファイルアップロード］画面管理部がユーザよりファイルのパスを取得する．暗号処理部（クライアント）はファイルをグループ公開鍵で暗号化し，ファイル情報管理部は暗号化済みファイルをサーバ側 DB へ保存する．

［ファイルダウンロード］画面管理部がダウンロードファイルの ID を取得する．ファイルは暗号処理部（サーバ）でサーバ部分復号鍵により部分復号され，暗号処理部（クライアント）でメンバ部分復号鍵により完全復号される．

［グループ構築］画面管理部が新たなグループ名を取得する．グループ情報管理部がグループ ID を発行・登録し，サーバ／メンバ部分秘密鍵を生成する．

［グループへのメンバ追加］画面管理部が追加する ID，グループ名を取得する．葉ノードメンバの復号鍵処理部が新メンバのサーバ／メンバ部分復号鍵を生成する．グループ情報管理部は鍵を新メンバへ送る．新メンバは受け取った鍵とメンバ部分復号鍵を単一化する．

［グループからのメンバ離脱］画面管理部が追加する ID，グループ名を取得する．離脱メンバの親ノードメンバの鍵処理部は，メンバ部分復号鍵を（2,2）閾値秘密分散により新たなサーバ／メンバ部分復号鍵を生成する．生成したメンバ部分復号鍵を子ノードの鍵処理部に渡し，元々のメンバ部分復号鍵と単一化する．

［鍵更新］画面管理部が鍵更新命令を取得する．ルートノードメンバの鍵処理部は新たなメンバ／サーバ部分復号鍵を生成し，順に子ノードの鍵処理部が鍵を更新する．

5. おわりに

本稿では単一の鍵で多重帰属できる鍵管理プロトコルを適用したグループファイル共有システムの実装を行い，動作を確認した．このプロトコルで使用する鍵を管理するための DB を設計し，Flex によりドラッグ＆ドロップが可能なインターフェースの実装した．

参考文献

[1] 株式会社 ITR：クラウド時代のコラボレーション／ツールの方向性，株式会社 ITR 入手先〈http://www.itr.co.jp/PDFPUB/ITR_WP_C10090023.pdf〉（参照 2011-01-12）

[2] 内田真理子，福田洋治，毛利公美，白石善明：多重帰属の鍵管理が容易な（2,2）閾値秘密分散を用いたグループファイル共有，信学技報, vol. 108, no. 473, ISEC2008-113, pp. 71-78, (2009)

[3] A.Herzberg,S.Jarecki,H.Krawczyk,and M.Yung: Proactive Secret Sharing or: How to Cope with Perpetual Leakage. Extended abstract, IBM T.J. Watson Research Center, November 1995.

[4] ソフトバンク ビジネス IT：【市場調査】多機能化より高速化が進むべき道？グループウェアユーザの不満はレスポンスに集中，入手先〈http://www.sbbit.jp/article/cont1/18899〉（参照 2011-01-12）

[5] Brent Fulgham: The Computer Language Benchmarks Game, available from 〈http://shootout.alioth.debian.org/〉 (accessed 2011-01-12)

[6] Adobe: Adobe Flex, available from 〈http://www.adobe.com/jp/products/flex/〉 (accessed 2011-01-12)

[7] MySQL: MySQL Enterprise Edition, available from〈http://www-jp.mysql.com/downloads/enterprise/〉(accessed 2011-01-12)

[8] SQLite : SQLite Download Page, available from 〈http://www.sqlite.org/download.html〉(accessed 2011-01-12)