7ZD-02

複数組織対応属性ベース暗号を用いたファイル共有システムの鍵生成処理の実装と評価

小松 蒼樹　鈴木 智也　石橋 拓哉　柿崎 淑郎　大東 俊博 †
東海大学 †
土田 光 ‡　金岡 晃 §　相原 玲二 ¶
日本電気株式会社 ‡　東邦大学 §　広島大学 ¶

1 はじめに

さまざまなアクセス制御が可能な公開鍵暗号方式として暗号文ポリシー属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption, CP-ABE）を用いたファイル共有方法が提案されているが，これらに用いられている CP-ABE では，鍵発行センター（Key Generation Center, KGC）はすべてのユーザーの秘密鍵を作成できる非常に強い権限があるために，利用組織内の信頼できる部署が管理することを想定している．つまり，CP-ABE を用いたファイル共有システムは単一組織での利用を想定している．そこで，石橋らが複数組織で利用可能な属性ベース暗号（Multi-Authority Attribute-Based Encryption, MA-ABE）を用いたファイル共有システムの提案と実現可能性を示しており [1]，またその実装に関する基礎検討が行われている [2]．本稿では，MA-ABE を用いたファイル共有システムの鍵生成処理についての実装と処理時間の計測を行う．

Implementation and Evaluation of Key Generation Process of a File Sharing System using MA-ABE
† Komatsu Soju, Suzuki Tomoya, Ishibashi Takuya, Kakizaki Yoshio, Ohigashi Toshihiro, Tokai University
‡ Tsuchida Hikaru, NEC
§ Kanaoka Akira, Toho University
¶ Aibara Reiji, Hiroshima University

2 鍵生成処理およびその実装

本ファイル共有システムは複数組織間での利用を想定しており，KGC は研究室単位などの小さい組織毎に存在している．KGC は学術認証フェデレーション（以下，学認）と学内認証基盤の属性情報，および各 KGC 管理者が独自に登録する属性情報を用いて，KGC で鍵発行を行う．本システムではシステム全体で利用可能なユニークな ID（GID）が必要となるため，学認の永続的な利用者識別子である eduPersonPrincipalName（以下，ePPN）を GID として用いる．また，学認の ePPN だけではユーザーの組織内での役職や所属などが取得できないので，各ユーザーが所属する学内の認証基盤から属性情報を取得して利用することとなる．東海大学では学内認証基盤として Microsoft Entra ID（以下，Entra ID）を採用しているため，本実装では学認から ePPN，Entra ID から UserPrincipalName（UPN）をそれぞれ取得し，紐付けを行う．

本研究で実装する鍵生成処理におけるユーザーの ePPN と属性情報の紐付け部分を図 1 に示す．本実装ではサーバー A およびサーバー B の 2 台を用いてシステムを構築した．サーバー A は OpenID Connect（以下，OIDC）の Relying Party として振る舞い，Apache の mod_auth_openidc を用いて，Entra ID から認証結果を取得する．サーバー B は Shibboleth が学認 SP として振る舞う．本実装における学認 SP は，テストフェデレーションとして構築

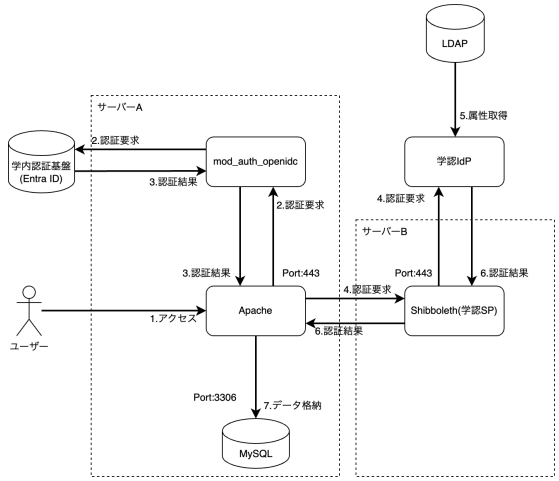

図1　システム構成図

しており，そのログインに利用できるのはテストアカウントのみに制限されている．

まず，利用者はサーバー A の Apache にアクセスする．Apache の mod_auth_openidc を用いて，学内認証基盤（Entra ID）にユーザーの認証要求を行い，認証結果を Apache に戻す．次に，Apache からサーバー B の Shibboleth（学認 SP）を通して，学認 IdP にユーザーの認証要求を行い，認証結果を学認 SP 経由で Apache に戻す．最終的に，Entra ID からは UPN，学認からは ePPN が取得できるので，これらを同一のユーザーとして紐付けて，MySQL に記録する．

ユーザーが属性鍵を取得する時には，ユーザーは学認から再度 ePPN を取得し，KGC は ePPN に対応する属性情報を MySQL から取得し，属性鍵を生成しユーザーに返す．

3　考察

構築したシステムにおける性能を評価するために，Entra ID および学認の認証にかかる時間をそれぞれ計測した．計測方法として，Chrome ブラウザのデベロッパーツールのネットワークログにて表示されるファイル毎のタイム項目を用いた．Entra ID および学認のそれぞれで，ログイン ID とパスワードを入力し，ログインボタンをクリックしてから認証結果が得られるまでの時間を取得時間，ログインボタンをクリックしてから，認証結果が Cookie に格納されてメインページにリダイレクトされるまでの時間を完了時間として計測を行った．Entra ID および学認のそれぞれに対して 5 回ずつ計測し，その平均を計測結果とした．また取得時間から完了時間を引いたものを差として表に記載した．結果を表 1 に示す．

表 1　取得時間と完了時間の計測結果 [ms]

計測対象	取得時間	完了時間	差
Entra ID	1197.0	2369.0	1172.0
学認	758.2	1969.8	1211.6

表 1 より，EntraID と学認の取得時間には 438.8ms の差がある．Entra ID は OIDC プロトコルを用いており，クライアント側が認可コードをクエリパラメータとして設定された状態で受け取り，その認可コードを認可サーバーに渡してアクセストークンを取得する処理が行われるので，学認よりも時間を要していると考えられる．また，完了時間から取得時間を差し引いた差は，Entra ID が 1172.0ms，学認が 1211.6ms である．Entra ID と学認の差は 39.6ms であり，Cookie に格納しリダイレクトする過程の処理時間にあまり差がないことがわかる．そのため，処理速度は認証処理速度に大きく依存していることがわかる．

謝辞

本研究の一部は JSPS 科研費（課題番号 22K12034）の助成，JST，CREST，PMJCR22M4 の支援を受けたものである．

参考文献

[1] 石橋拓哉，小林海，大東俊博，土田光，金岡晃，柿崎淑郎，相原玲二．複数組織対応属性ベース暗号を用いたファイル共有システムの実現可能性に関する考察，情報処理学会論文誌，Vol.64, No.3, pp.670–686, 2023.

[2] 石橋拓哉，鈴木智也，大東俊博，土田光，金岡晃，柿崎淑郎，相原玲二．複数組織対応属性ベース暗号を用いたファイル共有システムの設計，東海大学紀要 情報通信学部，出版予定，2024.