研究記録管理・公開・検証システム arχves への確認者署名機能の付加

情報工学コース　加藤　康(S043028)
指導教員:小林　聡　准教授

1.　はじめに

本研究では、研究記録管理・公開・検証システム arχves[1,2](以下 arχves)に対して、確認者による署名の機能を付加し、記事の研究記録としての価値を高めることを目的とした改良を試みた。

2.　システム概要

2.1　arχves の特徴

arχves は以下のような特徴を持つ。

・SNS/Blog をベースとしている
・記事ごとに柔軟な公開範囲を設定可能
・データへの二重署名による、正真性と非改竄性の保証
・ASCIIMathML を用いた数式表記が可能

2.2　データの二重署名

arχves は、投稿された記事に対して、以下のような処理を行うことで記事に署名を行っている。研究記録データの投稿者を「ユーザ」、ユーザ署名を行い、二重署名された文書を保管するサーバを「文書サーバ」、第三者による署名を行うものを「検印サーバ」とし、①～⑤の順に処理を行う。(図1)

①作成文書に文書サーバでユーザ署名を行う
②文書サーバから検印サーバへ文書を転送する
③検印サーバで文書に署名をし、署名部を保存する
④文書サーバに二重に署名済みのデータを送る
⑤文書サーバにデータを保存する

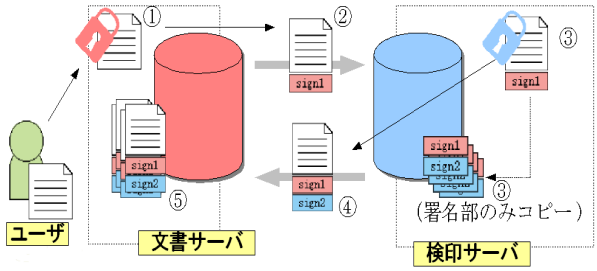

図 1 二重署名処理の流れ

3.　確認者署名機能

3.1　確認者署名の意味

arχves では二重署名によって、研究記録の正真性と非改竄性を保証している[1,2]が、研究記録としての価値を高めるためには確認者による署名が必須である。紙媒体の研究ノートの場合、確認者による署名により、研究記録の証拠としての効力を持つ。確認者とは、研究記録に対して不正がないことを証明する第三者である。確認者には以下のような条件が挙げられる。

・共同研究者でないこと
・記録の内容を理解できる者

身近でこれらの条件を満たす人物を探し出すことは、必ずしも容易ではない[3]。本研究では、ネットワークを通じて遠方の確認者との通信も容易に行うことが可能である。

3.2　データへの確認者署名

本研究では arχves に確認者による記事への確認署名機能を新たに構築した。投稿された二重署名済みのデータに対して、以下の処理を行い、確認者による署名を行う。(図 2)

⑥記事が投稿されたことを確認者にメールで知らせる
⑦確認者は検印サーバで、記事を閲覧する
⑧二重署名済み文書に対し、確認者署名を行う
⑨検印サーバでサーバ署名を行い、署名部を保存する
⑩文書サーバに四重署名済みデータを送る
⑪文書サーバにデータを保存する

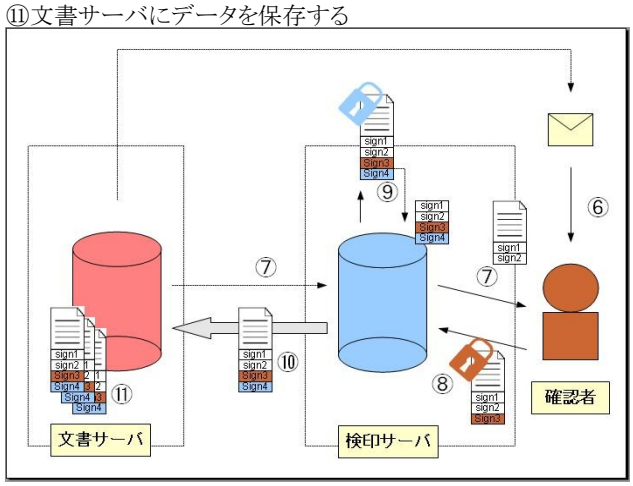

図2　記事確認処理の流れ

3.3　検印サーバを介した記事の表示

⑦での記事閲覧は、検印サーバ上で文書サーバにログインし、文書サーバのページを検印サーバを介して表示している。

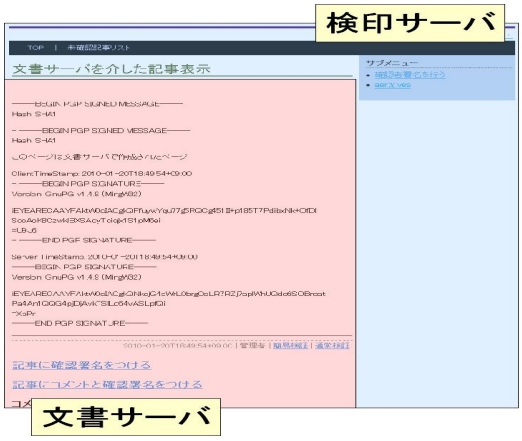

図3　検印サーバを介した記事表示

4.　その他改良点

4.1　複数の文書サーバへの対応

これまで文書サーバと検印サーバは一対一の通信を行っているが、一つの検印サーバに対し、複数の文書サーバに対応することを想定し、文書サーバ毎に ID とパスワードを用いた認証を行う機能を実装した。これにより、他サーバからのなりすましも回避することが可能である。

4.2　複数の添付ファイルに対応

これまで一つの記事に対し、一つのファイルしか添付できなかったが、5 つまでのファイルを添付可能に改良を行った。

5.　今後の課題

ユーザインタフェースの問題として、記事中での表、画像表示への対応、セキュリティの問題として、PGP のハッシュ関数の変更(2010 年問題)などが挙げられる。

6.　参考文献

[1]加藤　未来,「GnuPG を用いた研究記録管理・公開・検証システムの構築」,島根大学卒業論文,2008
[2]島貫　稚華,「研究記録管理・公開・検証システム arχves の数式およびグラフへの対応」,島根大学卒業論文,2009
[3]編集　岡崎康司,隅蔵康一,「ラボノートの書き方」,株式会社羊土社,2007