研究記録管理・公開・検証システム arχves の web 認証基盤への対応

情報工学コース　藤坂達也（S063078）
指導教員　小林聡　准教授

1.　arχves とは

1.1　システムの特徴

・電子署名を用いた研究記録への四重署名

・研究記録の公開範囲の細かな設定が可能

・確認者による研究記録への確認機能

・数式表現に対応

・Ruby on Rails による実装

1.2　データの四重署名の流れ

arχves では投稿された研究記録に対して、次のような手順で署名を行っている

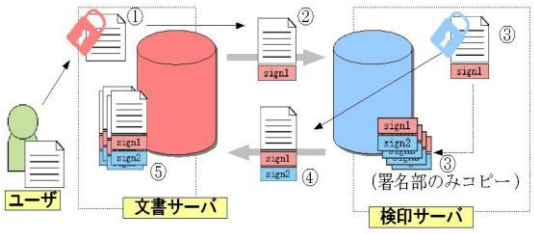
①文書サーバにログインし、研究記録を文書サーバに送信する

②作成者の秘密鍵で研究記録に署名し、研究記録＋署名部分を検印サーバに送信する

③検印サーバの秘密鍵で研究記録＋署名 1 に署名し、署名部を検印サーバのデータベースに保存する。

④研究記録＋署名部を文書サーバに送信する

⑤研究記録＋署名部を文書サーバのデータベースに保存



⑥確認者は依頼メールを受信後、まず検印サーバにログインする。

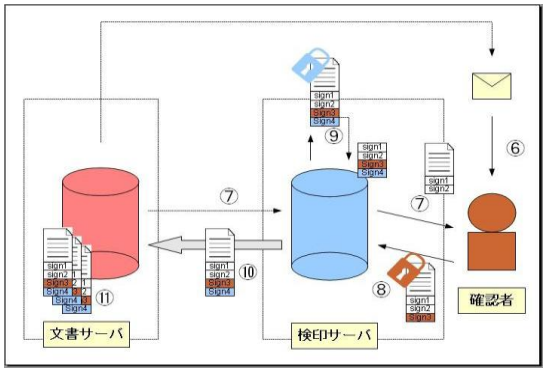
⑦検印サーバを介して、文書サーバから研究記録を取り寄せる。

⑧研究記録の内容を確認し、確認者の秘密鍵で署名する。

⑨検印サーバの秘密鍵で署名し、署名部を検印サーバのデータベースに保存する。

⑩研究記録＋署名部を文書サーバに送信する。

⑪研究記録＋署名部を文書サーバのデータベースに保存



1.3　データの四重署名の意味

arχves では署名 1 と署名 2 によって、研究記録の正真性と非改竄性を保証している。研究記録を証拠として機能させるためには本人の確認に加え、内容を確認できる第三者の署名が必要である。そのため、arχves では署名 3 と署名 4 によって、研究記録に証拠能力を持たせている。これらの四重署名により投稿された研究記録の知的財産としての価値を高めている。

2.　Rails2 への移行

今後、より柔軟な機能の作成や蓄積されるデータの柔軟な活用を行っていくことを考慮し, HTML だけではなく XML や JSON などの複数のフォーマットでの出力も可能な Ruby on Rails2 への移行を行った。

3.　web 認証基盤への対応

本システムでは、研究記録の投稿と確認の際に、文書サーバまたは検印サーバに再度ログインしなおす必要がある。この点を改善するため、シングルサインオンを導入した。シングルサインオンとは、1 つの ID とパスワードを複数のウェブサイトで利用できるようにする認証システムのことである。異なるウェブサイトで 1 つの ID とパスワードを利用するため、ユーザが覚える必要のあるパスワードの総数が減少する。その結果として、複雑なパスワードを設定しやすくなるため、セキュリティの強化につながる。認証サービスを行うサイトをユーザが選べ、ログインなどの認証の際に、認証の結果と必要最小限の情報のみをサービス側に通知する。

4.　今後の課題

研究記録を対象として、自然言語処理・知的処理を行う。

5.　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]加藤康「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」島根大学卒業論文 2010