GnuPG を用いた研究記録管理・公開システム構築

計算機科学講座　加藤　未来（s023027）
指導教員：小林　聡　准教授

1.はじめに

本研究では研究データの捏造に対する対策として記事の検証を行え，また研究内容の進捗状況や内容によって公開できる範囲を柔軟に指定可能とする，研究記録公開制御システム arχves の作成を試みた。

2. システムの特徴

2.1. SNS/Blog ベース

近年広く普及してきている SNS 及び Blog をベースとすることで，手軽に研究記録の管理や作成，またグループの管理を行えるようにした。システム内のコンテンツ，また本システムのコンテンツを利用できる権限の範囲によって利用者を 4 種に分けられる。
各コンテンツと利用者の権限の対応については表1を参照。

コンテンツ＼　利用者	管理者	ユーザ	ゲスト	一般
TOPページ	○	○	○	○
ブログリスト	○	○	○	○
グループリスト	○	○	○	
ユーザリスト	○	○	○	
アカウントメニュー	○	○	△	
管理者メニュー	○			

△：アカウント情報の閲覧のみ可能

表 1　コンテンツと利用者の権限

・「グループ」について
グループとは，一人以上のユーザとゲストの集合であり，ユーザであれば誰でも作成が可能。ログイン可能な利用者全員が一つ以上のグループに属する。グループはユーザ全体で共有し，管理は作成者及びシステム・ルートが行う。
また，既存のグループを親としたグループも作成可能である。

2.2. 記事毎の公開範囲の指定

公開範囲は大きく以下の三段階で指定可能。
「自分のみ」，「グループ指定」，「全体公開（制限なし）」
記事の新規作成時，また投稿後も記事毎に公開範囲を指定する。このとき，複数のグループを指定することが可能。
また，指定されたグループの子グループは自動的に公開範囲に含まれる。

2.3. データの二重署名

作成された文書に対し，作成者自身の署名と第三者による署名を行うことによって，真正性と非改ざん性を保証するモデルが企業の書類に存在する。本研究ではこれを以下「検印モデル」と呼ぶ。これを電子データに対して電子署名で「検印モデル」を用いた研究として[1]がある。本システムはこれに基づき，データの保存時に図 3 のような処理を行うシステムの実装を行っている。

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，以下の①～⑤の順に処理を行う。

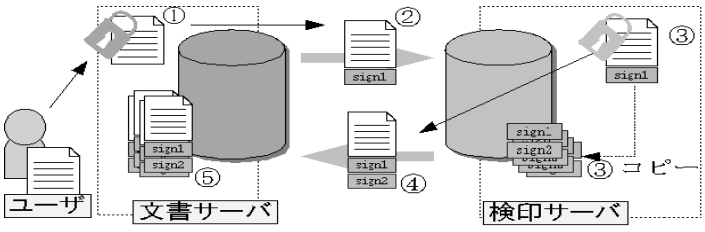

図 1 「検印モデル」を基にしたシステムの流れ

①作成文書は文書サーバでユーザ署名を行う
②検印サーバへ転送
③検印サーバで署名と署名部の保存
④文書サーバに 2 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

2.4. その他機能

2.4.1.記事に対する研究データの添付機能

各記事投稿時に，ファイルの添付が可能。この添付ファイルに対しても二重署名が行われる。

2.4.2.記事及び添付ファイルに対する検証機能

記事ページから 1 クリックで検証が可能。検証には 2 種類あり，「簡易検証」と「通常検証」がある。
「簡易検証」は二重署名されたデータに対し，それぞれの署名の検証を行う。「通常検証」は「簡易検証」に加えて，更に検印サーバに保存されている署名と一致するかどうかを調べて検証を行う。
また，署名付きのデータや，ユーザ及び検印サーバの公開鍵をダウンロードできるため，それにより本システムのスクリプトに依らない検証を行うことも可能である。

3. 比較検証

3.1.比較：記事毎の公開範囲の指定

記事ごとに公開範囲の設定が可能な類似の SNS システムとして「Enzin」[2]，「ACS」[3]がある。
設定方法のユーザインタフェースは直感的に操作できる Enzin,ACS に比べ，本システムでは若干分かりにくく手間がかかると言える。だが投稿後の変更の可・不可の差はあるが，公開時での公開範囲の機能はほぼ同等である。(表 2)

システム名	指定方法	変更
Enzin	アイコンのドラッグ&ドロップによる指定	可
ACS	チェックボックスによる指定	不可
本システム	テキストエリアへのグループ名の記入	可

表 2　公開範囲の指定方法と変更

3.2.比較：真正性と非改ざん性の保持

類似システム として「タイムスタンプサービス」がある。これは，文書作成者とは関連のない第三者である企業が，作成された文書から得られるハッシュ値に対して，非改竄性の保証を行うサービスである。項目別に比較したのが表 3 である。

	ﾀｲﾑｽﾀﾝﾌﾟｻｰﾋﾞｽ	本システム
非改竄性の保障の強度	高い	劣る
検証効率	適宜問い合わせ	記事ページより1クリック
利用コスト	一回10～2000円	導入までのコストはかかるが，導入後は手軽に利用が可能

表 3　タイムスタンプサービスと本システムの比較

以上より，非改竄性の高さをとるのであれば「タイムスタンプサービス」を，ある程度の非改竄性を保持しつつ，頻繁に利用しメモ程度の文書も残したいというのであれば「本システム」という住み分けが可能と考えられる。

4.今後の課題

『セキュリティの問題』として、非改竄性の証明の強度の向上のため各秘密鍵の管理方法、また『ユーザインタフェースの課題』として、記事中での表や数式,化学式への対応や複数システムのユーザ認証についての Delegate 機能の実装などが今後の課題としてあげられる。

5. 参考文献

[1]原田篤史，西垣正勝，曽我正和，田窪昭夫，『ﾗｲﾄﾜﾝｽ文書管理ｼｽﾃﾑ』，情報処理学会論文誌 Vol.44,no.8,pp.2093-2105,2003
[2] 永田周一，安村通晃，「Enzin:情報の公開範囲を手軽に変更できるｺﾐｭﾆｹｰｼｮﾝﾂｰﾙ」，情報処理学会論文誌 Vol.48,no.3,pp.1134-1143,2007
[3]高井一輝，河口信夫，「ACS:多様な人間関係を表現可能なｿｰｼｬﾙﾈｯﾄﾜｰｷﾝｸﾞｼｽﾃﾑ」，情報処理学会論文誌，vol. 48, no. 7, pp. 2328-2339, 2007.