arχves: 公開鍵暗号を用いた研究記録管理・公開・検証システム構築の試み

加藤未来
島根大学 総合理工学部

〇小林 聡
島根大学 総合情報処理センター

はじめに

- 研究成果の捏造が社会問題となったことは記憶に新しい
  - このような問題の発生を技術的に食い止めることは困難
  - しかし、研究記録の検証の補助は可能
- 課題
  - 研究記録の真正性と非改竄性の保証
- タイムスタンプサービス
  - DVCS (Data Validation & Certification Server Protocol)
  - TAP (Trusted Archival Protocol)

はじめに

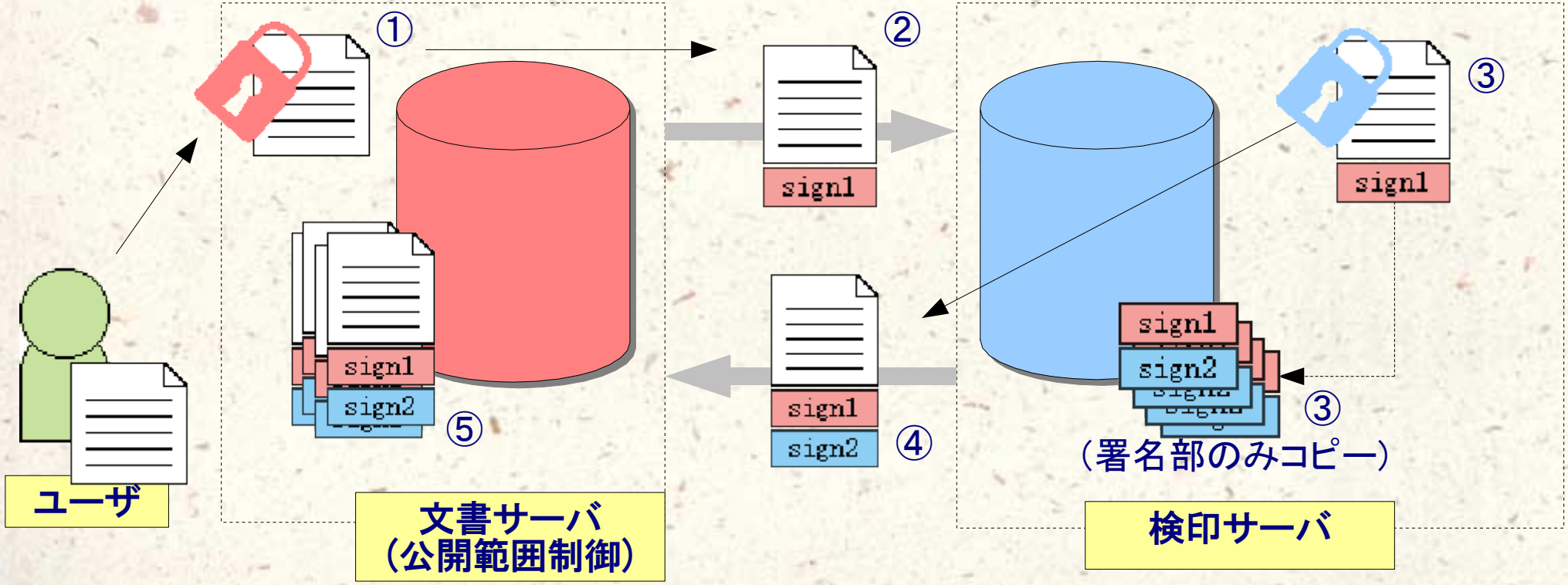
- WWWに代表されるインターネット環境は重要なコミュニケーションツール
- 研究者間での、論文の公刊前/後の意見交換、資料/試料公開に活用可能
- ただし、論文の公刊前であれば、公開範囲の柔軟な制御が必要
  - 一般のSNSでは3段階/種類程度の制御のみ

はじめに

- 研究記録などの管理・公開・検証を行なうシステム、arχvesの構築を試みた
  - 研究記録などの管理を主目的
  - 検印モデルにより、記録などの真正性および非改竄性を可能な限り保証
  - 情報の公開範囲の柔軟な制御
  - 機能的には二重署名と柔軟な公開範囲制御があるSNS/blog

（二重署名: 原田ら, “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, 2003.）

モデル



- 本システムの運用組織(研究室～学科程度を想定)が相互に検印を行なうモデルを想定

機能

表1: 利用ツール等

開発言語:	Ruby ver. 1.8.6
フレームワーク:	Ruby on Rails ver. 1.2.6
公開鍵暗号ソフト:	GnuPG ver. 1.4.9
ウェブサーバ:	Apache ver. 2.0.6
SSLライブラリ:	OpenSSL ver. 0.9.8
DBMS:	MySQL ver. 5.0.27

機能

- 記事の閲覧

公開鍵暗号を用いた研究記録管理

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

- -----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。
この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。

ClientTimeStamp: 2008-07-16 15:02:05
- -----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAkh9jt0ACgkQFfuywYqu77h vwCg4TbT0j6VmA81itgNc918BVcj
57wAoNdd4g3dX7Wi/pKZpEcFoiZdGI/P
=m2iZ
- -----END PGP SIGNATURE-----

Server TimeStamp. 2008-07-16 15:02:05
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAkh9jt0ACgkQNkcjG4aWrL3U1ACeITAQY/cnnvgo1/oVYuhRN7h9
4moAoIErpmkVJm9DRuTybs9EbndH217D
=oqwK
-----END PGP SIGNATURE-----

公開範囲

::全体公開
::GROUP2
::GROUP2:GROUP11
::GROUP4:GROUP13
::GROUP2:GROUP11:GROUP15
::GROUP4:GROUP13:GROUP17

2008-07-16 15:02:05 | 管理者 | 簡易検証 | 通常検証 | コメント(0) | category3

コメントを書く

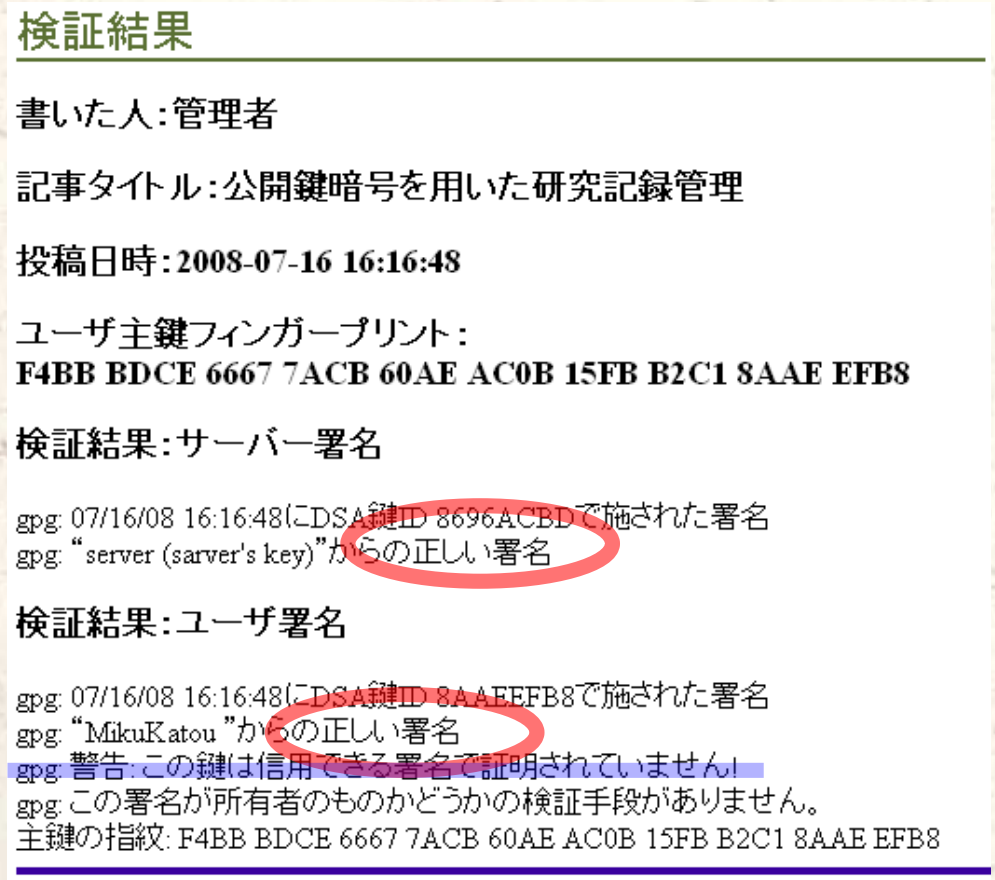
(データ添付も可能)

機能

- 記事の検証
  - 簡易検証
    - 文書サーバのみで、ユーザの公開鍵と検印サーバの公開鍵を用いて検証
  - 通常検証
    - 簡易検証に加えて、検印サーバに保管されている署名データとも照合
  - 人力検証
    - 記事等をDL(Copy&Paste)、ユーザと検印サーバの公開鍵をDL、GnuPGを各自で用いて検証

機能

- 検証例(簡易検証)


検証結果

書いた人:管理者

記事タイトル:公開鍵暗号を用いた研究記録管理

投稿日時:2008-07-16 16:16:48

ユーザ主鍵フィンガープリント:
F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8

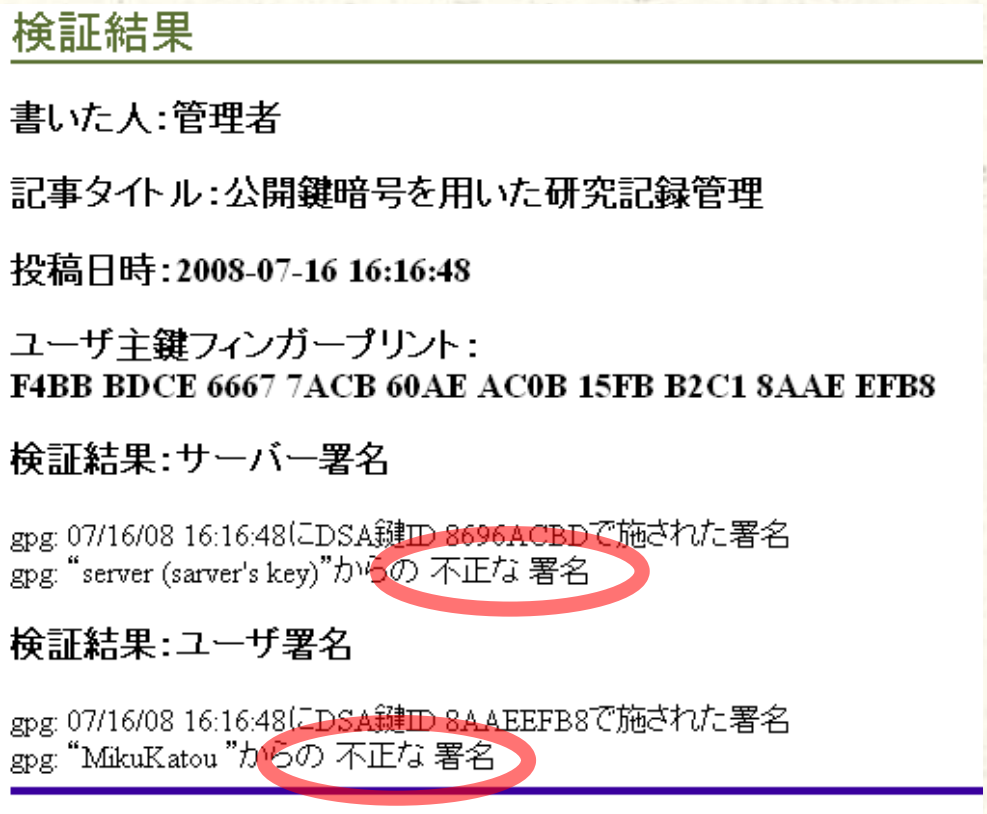
検証結果:サーバー署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8696ACBDで施された署名
gpg: "server (sarver's key)"からの正しい署名

検証結果:ユーザ署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8AAEEFB8で施された署名
gpg: "MikuKatou"からの正しい署名
gpg: 警告: この鍵は信用できる署名で証明されていません!
gpg: この署名が所有者のものかどうかの検証手段がありません。
主鍵の指紋: F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8

図8: 記事の簡易検証


検証結果

書いた人:管理者

記事タイトル:公開鍵暗号を用いた研究記録管理

投稿日時:2008-07-16 16:16:48

ユーザ主鍵フィンガープリント:
F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8

検証結果:サーバー署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8696ACBDで施された署名
gpg: "server (sarver's key)"からの 不正な 署名

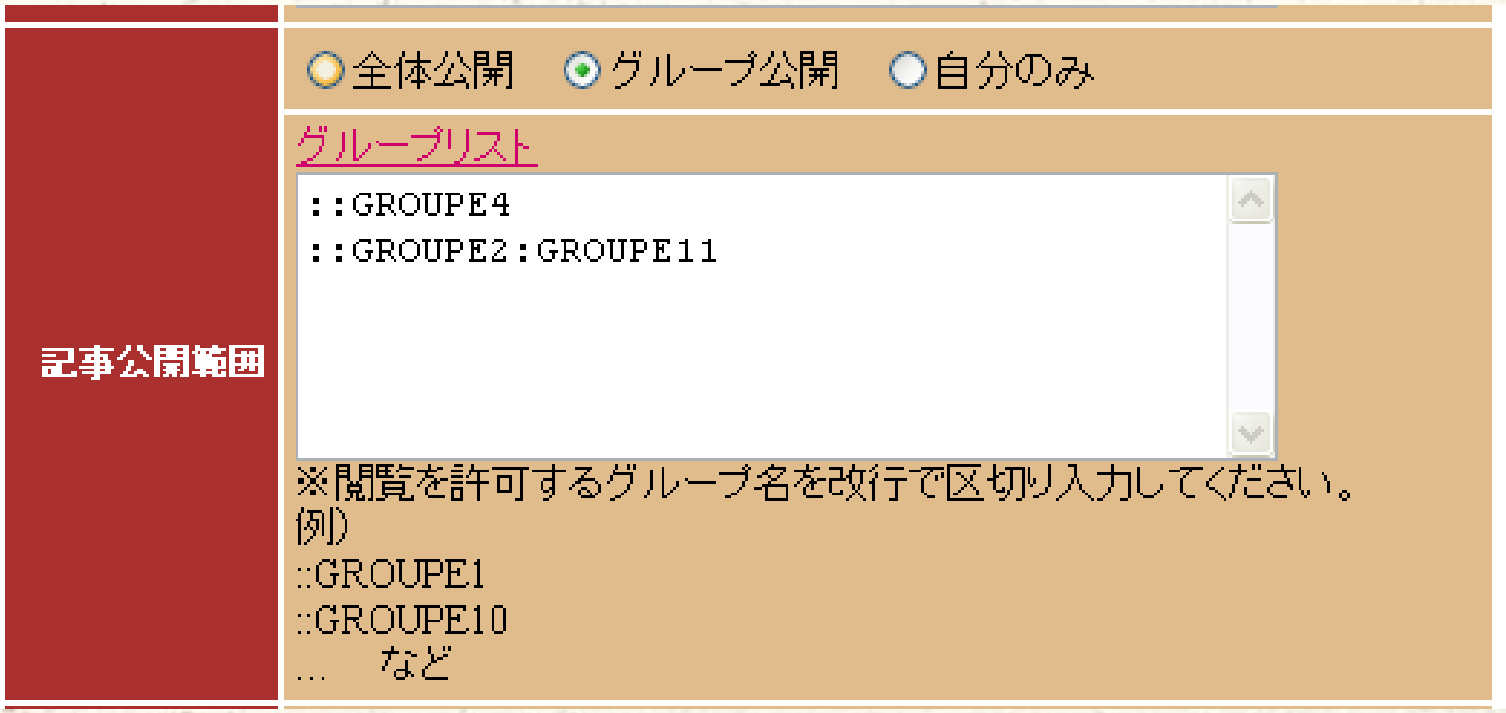
検証結果:ユーザ署名

gpg: 07/16/08 16:16:48にDSA鍵ID 8AAEEFB8で施された署名
gpg: "MikuKatou"からの 不正な 署名

図9: 改竄された記事の検証

機能

- 公開範囲制御



(記事投稿画面より抜粋)

機能

- 閲覧範囲制御
  - 利用者(ゲスト、ユーザ)は、それぞれ1つ以上のグループに属する
  - 記事ごとに、利用者(ゲスト、ユーザ)が属するグループに対して閲覧許可を発行
  - グループ
    - ::島根大学:総合理工学部:数理・情報システム学科:小林聡研究室
    - 上記グループに属するゲスト/ユーザは、上位のグループに対して閲覧許可が発行されている記事も閲覧可
    - 仮想的なグループも可能
      - ::豊橋技術科学大学:情報工学系:中川研究室:OB:教員

比較

- 真正性および非改竄正の保証
  - 本システムではシステム運用組織(研究室～学科程度を想定)による相互検印
  - 商用サービスは、第三者の認証を受けたサービス
    - 強度については商用サービスに劣る?
  - ラボノートの運用、証拠能力から、十分な能力有
- コスト
  - 本システムでは、ほぼ導入時のコストのみ
  - 商用サービスでは、利用に応じて課金/プリペイドで購入
- 住み分けが可能

比較

- 公開範囲制御

表4: 公開範囲の指定方法と変更

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5: 公開範囲の設定方法

Enzin:	自分のみ	メンバ	グループ	インターネット全体
ACS:	自分のみ	グループ	一般公開	パブリックリリース
本システム:	自分のみ	グループ	全体公開	グループの階層化が可能

(永田ら, “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, 2007.
高井ら, “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グシステム”, 情報処理学会論文誌, vol. 48, no. 7, 2007.)

考察

- 真正性の保証
  - ユーザの秘密鍵をICカードやUSBメモリに保管し、必要時のみ参照
- 非改竄性の強度
  - リンキング、ヒステリシス署名、履歴交差などの導入
- 秘密鍵の危殆化
  - 検討課題

考察

- 検印時の通信時の秘密保持
  - 現在はSSLで対処
  - ハッシュ値のみの通信も検討
- 公開鍵の正当性の確保
  - 信頼の輪(Web of Trust)も含めたPKIの利用を検討
- 認証のdelegate機能
- ユーザインタフェースの高機能化
- 数式、表、グラフ、図への対応

まとめ

- arχvesの構築を試みた
  - 研究記録などの管理を主目的
  - 公開範囲を柔軟に制御可能
  - 記録などの真正性および非改竄正の保証
- DVCSでもTAPでもない電子署名付き電子文書管理のあり方を実現/提案
- 今後
  - 本システムの機能の追加・改良
  - 本システム上に蓄積される記録の知的処理

ご清聴ありがとうございました

はじめに

- Masui et al., “Instant Group Communication with QuickML”, Proc. ACM Conference on Supporting Group Work, pp.268-273, 2003.
- 江渡ら, “quikWeb: メーリングリストとWikiを統合したコミュニケーションシステム”, 情報処理学会研究報告, 2004-HI-111, pp.5-11, 2004.
- 永田ら, “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.
- 高井ら, “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グシステム”, 情報処理学会論文誌, vol. 48, no. 7, pp. 2328-2339, 2007.
- 高田ら, “多様なアクセス制限に対応した自然科学データベースシステムの開発”, 学術情報処理研究, no. 11, pp. 50-59, 2007.

モデル

- 検印モデル
  - 部下が書いた記録(日報など)に、上司が検印を捺す
  - ラボノートに、直接的な利害関係者でない者が検印を捺す
  - 原田らは、公開鍵暗号を用い、二重書名を行なうモデルを提案
    - 文書サーバが検印を行なう
    - 原田ら, “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.
  - 本システムでは、検印サーバと文書サーバが異なることを仮定

機能

- 利用者範疇
  - ゲスト: 要認証
    - blog記事等の閲覧、コメントが可能
  - ユーザ: 要認証
    - システム内に自身のblogを持つ
  - 管理者: 要認証
    - システムの管理者、管理者メニューにアクセスできる
  - 一般: 認証不要
    - 一般公開された記事のみ閲覧可

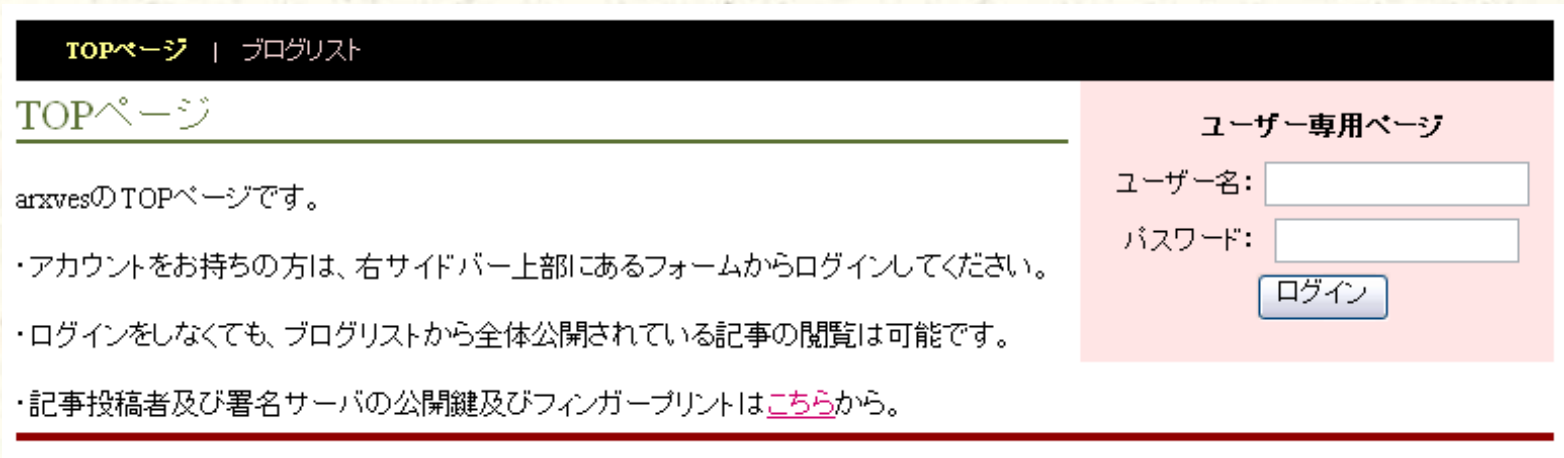
機能

- アクセス権限一覧

	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	○			

機能

- ログイン画面


TOPページ | ブログリスト
TOPページ
arxvesのTOPページです。
・アカウントをお持ちの方は、右サイドバー上部にあるフォームからログインしてください。
・ログインをしなくても、ブログリストから全体公開されている記事の閲覧は可能です。
・記事投稿者及び署名サーバの公開鍵及びフィンガープリントはこちらから。
ユーザー専用ページ
ユーザー名:
パスワード:
ログイン

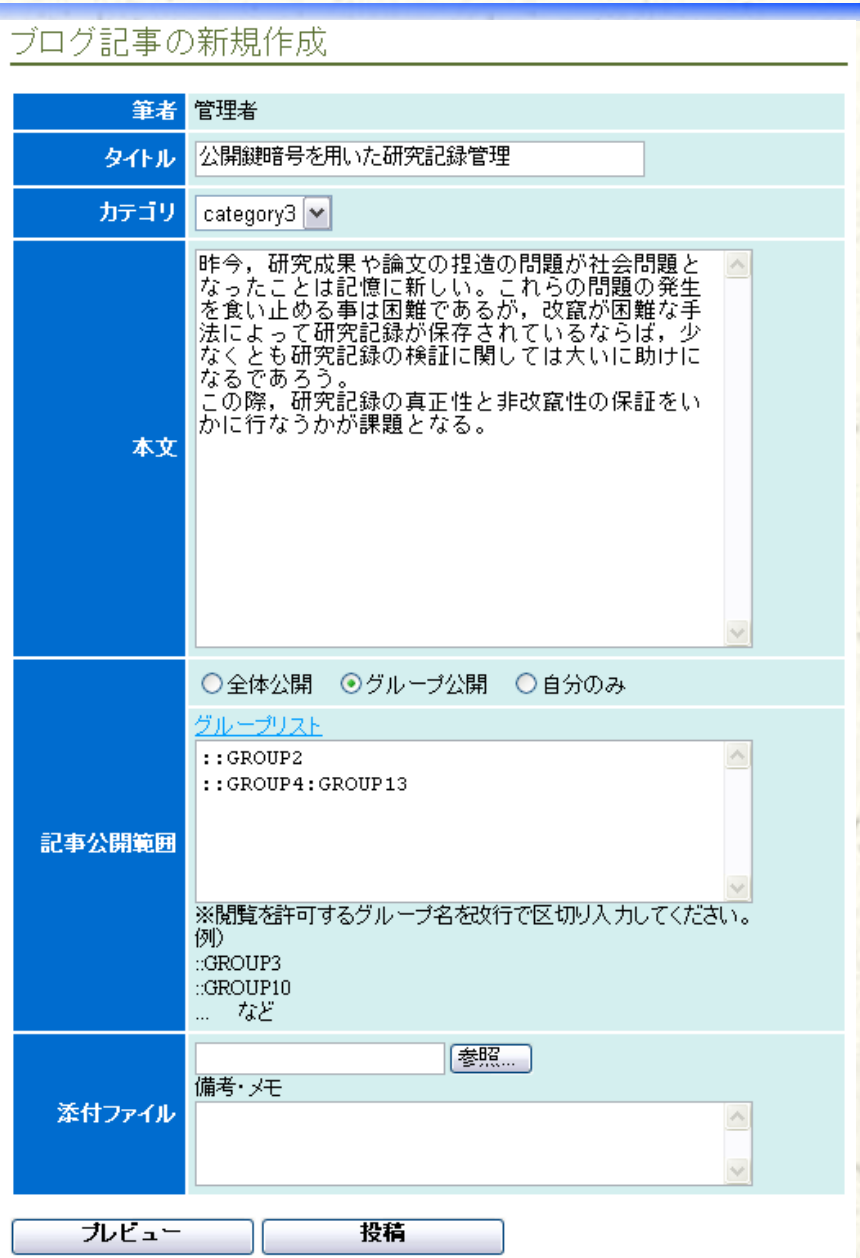
機能

- 記事の閲覧


ブログ
管理者さんのブログ
公開鍵暗号を用いた研究記録管理
昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。
ClientTimeStamp: 2008-08-01 10:00:34
Server TimeStamp. 2008-08-01 10:00:35
2008-08-01 10:00:34 | 管理者 | 全文(署名付き) | コメント(0) | category3
公開鍵暗号を用いた研究記録管理
昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。
ClientTimeStamp: 2008-08-01 09:59:54
Server TimeStamp. 2008-08-01 09:59:55
2008-08-01 09:59:54 | 管理者 | 全文(署名付き) | コメント(0) | category3
記事表示メニュー
管理者さんのブログ (47)
ユーザーさんのブログ (10)
田中さんのブログ (10)
作成者一覧
最新の3件
タイトルリスト表示
管理者さんのブログカテゴリ
category3 (42)
category6 (4)
category9 (1)
ユーザメニュー
自分のブログ記事を作成
記事検索
検索

機能

- 記事の投稿
  - 以下を指定/入力
    - タイトル
    - 本文
    - カテゴリ
    - 公開範囲
    - 添付ファイル
  - 「投稿」ボタンにより投稿



機能

- 公開範囲設定

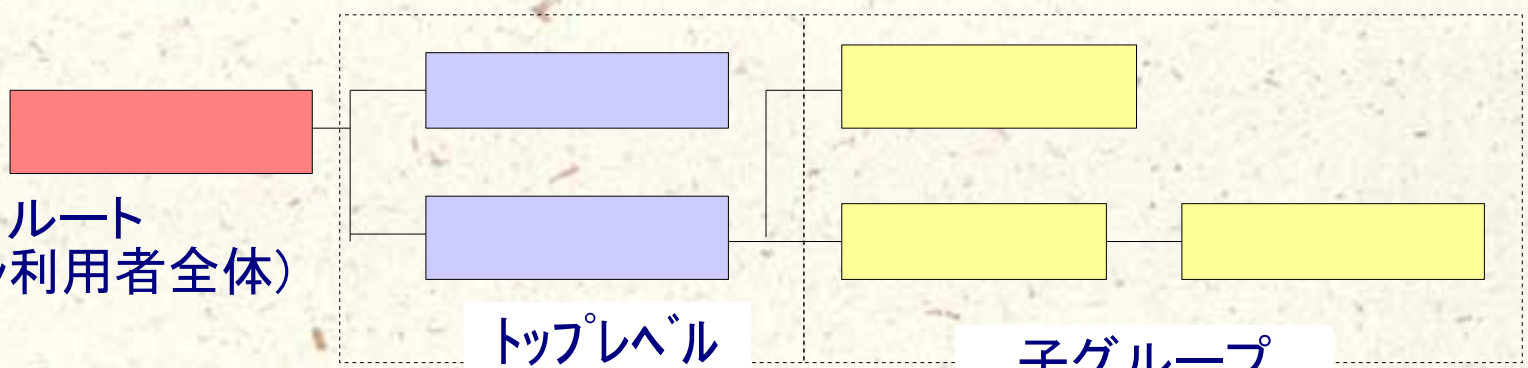
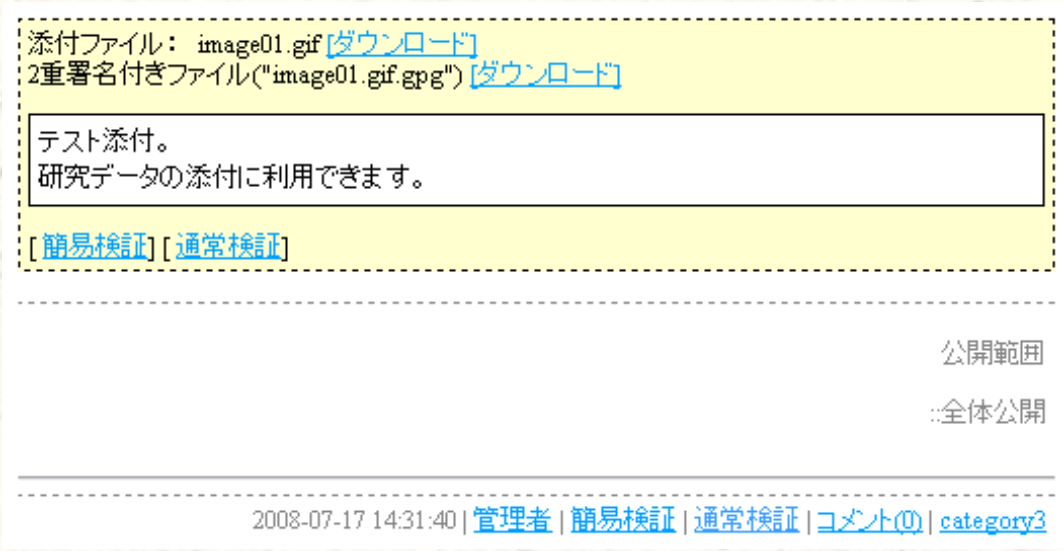


図　グループの構成

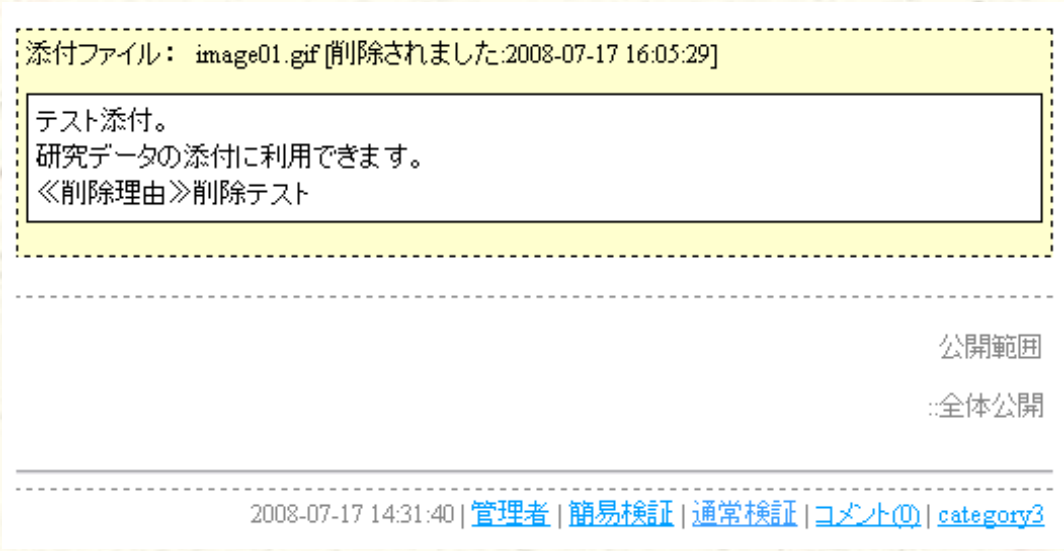
機能

- ファイル添付


添付ファイル： image01.gif [ダウンロード]
2重署名付きファイル("image01.gif.gpg") [ダウンロード]
テスト添付。
研究データの添付に利用できます。
[簡易検証] [通常検証]
公開範囲
::全体公開
2008-07-17 14:31:40 | 管理者 | 簡易検証 | 通常検証 | コメント(0) | category3

機能

- ファイル削除


添付ファイル： image01.gif [削除されました:2008-07-17 16:05:29]
テスト添付。
研究データの添付に利用できます。
≪削除理由≫削除テスト
公開範囲
::全体公開
2008-07-17 14:31:40 | 管理者 | 簡易検証 | 通常検証 | コメント(0) | category3

機能

- 公開鍵のダウンロード

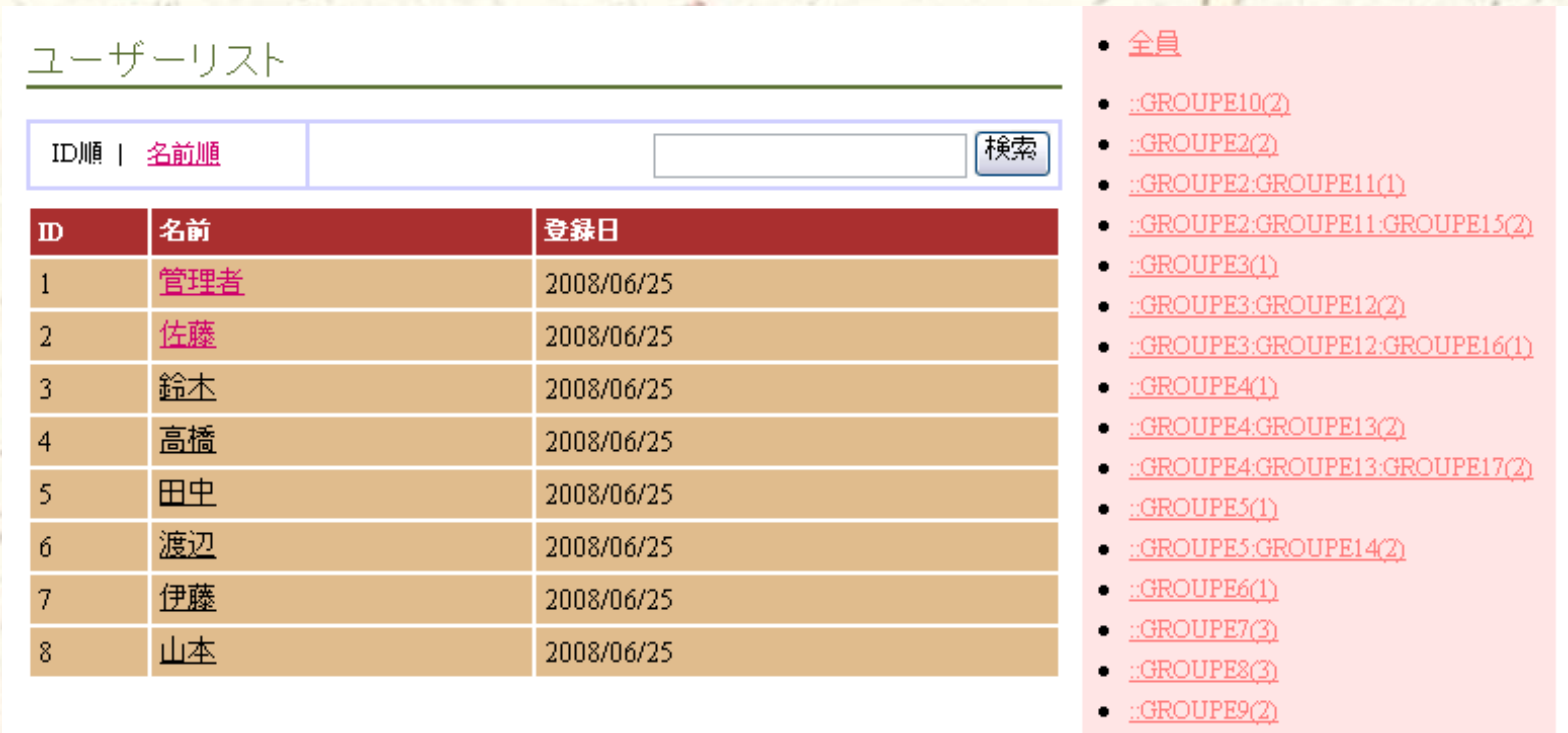
公開鍵のダウンロード

ブログ名	書いている人	公開鍵ファイルの保存	フィンガープリント
管理者さんのブログ	管理者	ダウンロード	F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8
ユーザーさんのブログ	ユーザ	ダウンロード	F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8
田中さんのブログ	田中	ダウンロード	F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8

署名サーバの公開鍵		
フィンガープリント	C55 3B84 FE90 709C DD47 C5FC DC00 4831 1294 5AC8	ダウンロード

機能

- ユーザー覧


ユーザーリスト
ID順 | 名前順
検索
ID
名前
登録日
1 管理者 2008/06/25
2 佐藤 2008/06/25
3 鈴木 2008/06/25
4 高橋 2008/06/25
5 田中 2008/06/25
6 渡辺 2008/06/25
7 伊藤 2008/06/25
8 山本 2008/06/25
全員
::GROUPE10(2)
::GROUPE2(2)
::GROUPE2:GROUPE11(1)
::GROUPE2:GROUPE11:GROUPE15(2)
::GROUPE3(1)
::GROUPE3:GROUPE12(2)
::GROUPE3:GROUPE12:GROUPE16(1)
::GROUPE4(1)
::GROUPE4:GROUPE13(2)
::GROUPE4:GROUPE13:GROUPE17(2)
::GROUPE5(1)
::GROUPE5:GROUPE14(2)
::GROUPE6(1)
::GROUPE7(3)
::GROUPE8(3)
::GROUPE9(2)

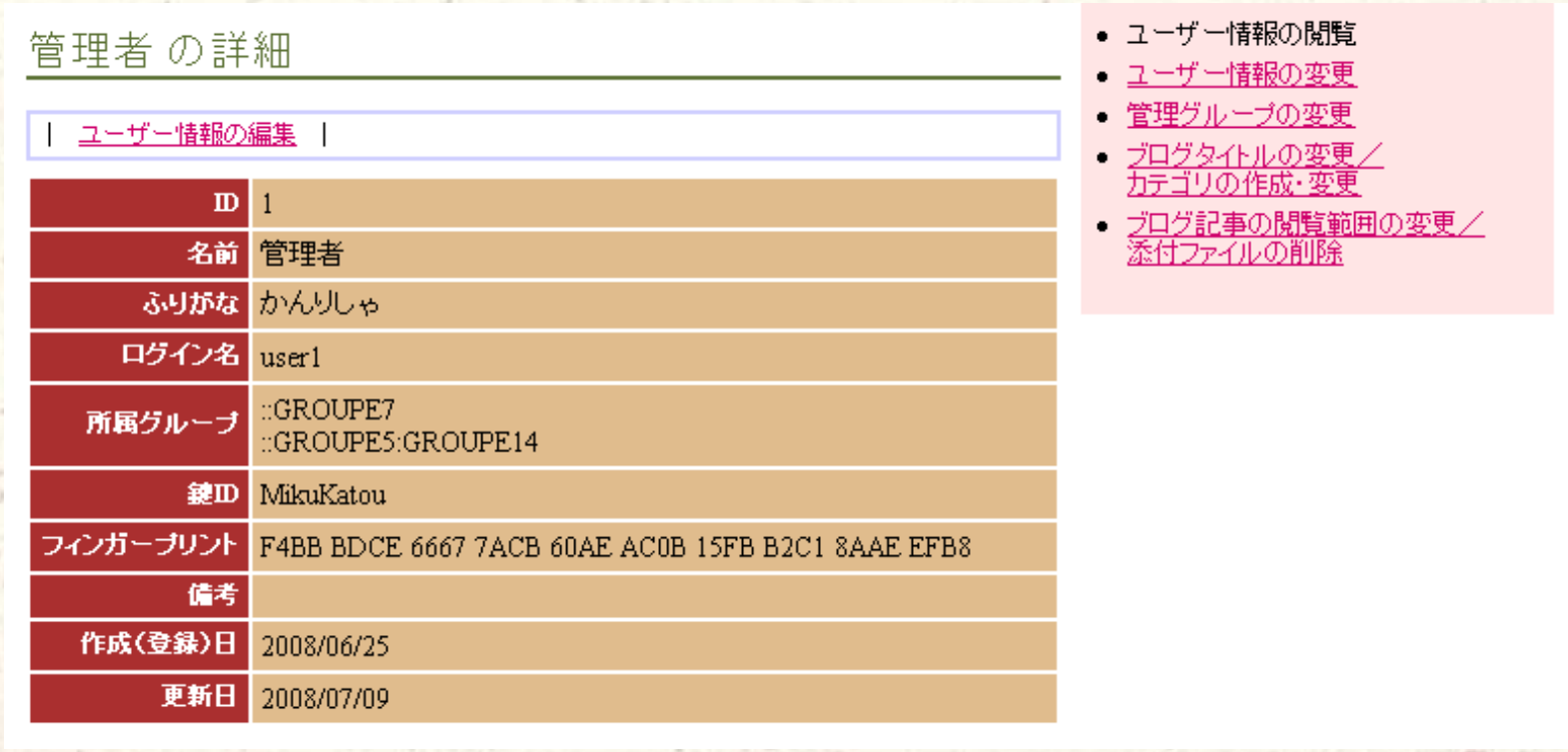
機能

- グループ一覧


グループリスト
ID順 | 階層順 | 名前順
検索
New 1 2 Old
ID グループ名 階層 登録者 登録者数 登録日
1 :: 0 管理者 15 2008/07/14
2 ::GROUP2 1 鈴木 3 2008/07/13
3 ::GROUP3 1 佐藤 4 2008/07/12
4 ::GROUP4 1 鈴木 1 2008/07/11
5 ::GROUP5 1 高橋 2 2008/07/10
6 ::GROUP6 1 管理者 1 2008/07/09
7 ::GROUP7 1 伊藤 2 2008/07/08
8 ::GROUP8 1 田中 2 2008/07/07
9 ::GROUP9 1 佐藤 1 2008/07/06
10 ::GROUP10 1 鈴木 3 2008/07/05

機能

- ユーザ情報


管理者 の詳細
| ユーザー情報の編集 |
ID 1
名前 管理者
ふりがな かんりしゃ
ログイン名 user1
所属グループ ::GROUPE7 ::GROUPE5:GROUPE14
鍵ID MikuKatou
フィンガープリント F4BB BDCE 6667 7ACB 60AE AC0B 15FB B2C1 8AAE EFB8
備考
作成(登録)日 2008/06/25
更新日 2008/07/09
ユーザー情報の閲覧
ユーザー情報の変更
管理グループの変更
ブログタイトルの変更／カテゴリの作成・変更
ブログ記事の閲覧範囲の変更／添付ファイルの削除

比較

	ﾀｲﾑｽﾀﾝﾌﾟｻｰﾋﾞｽ	本システム
非改竄性の保証の強度	高い	ﾀｲﾑｽﾀﾝﾌﾟｻｰﾋﾞｽに劣る
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	導入までにｺｽﾄはかかるが，導入後は公開範囲の制御もでき，一般のBlogであるかのように手軽な利用が可能

タイトル：公開鍵暗号を用いた研究記録管理

カテゴリ: category3

≪本文≫

昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。
この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。

≪公開範囲≫

::GROUP2:GROUP11
::GROUP2:GROUP11:GROUP15
::GROUP2
::GROUP4:GROUP13:GROUP17
::GROUP4:GROUP13

筆者	管理者
タイトル	公開鍵暗号を用いた研究記録管理
カテゴリ	category3
本文	昨今，研究成果や論文の捏造の問題が社会問題となったことは記憶に新しい。これらの問題の発生を食い止める事は困難であるが，改竄が困難な手法によって研究記録が保存されているならば，少なくとも研究記録の検証に関しては大いに助けになるであろう。 この際，研究記録の真正性と非改竄性の保証をいかに行なうかが課題となる。
記事公開範囲	○全体公開 ◉グループ公開 ○自分のみ グループリスト ::GROUP2 ::GROUP4:GROUP13