研究記録管理・公開・検証システム ar χ ves への確認者署名機能の付加

小林 聡 研究室
S043028 加藤 康

はじめに

研究記録管理公開検証システム ar χ ves とは

- 記事に対し、暗号技術を用いた署名を行い、記事の改竄を検出可能にするシステム
- 研究記録を共有できる範囲を柔軟に指定可能なシステム
- 記事に対し、確認者による署名を行い、研究記録としての価値を高めることのできるシステム

arχves の特徴

- SNS/ ブログベース
- 記事ごとの柔軟な公開範囲設定が可能
- 公開鍵暗号を用いたデータへの四重署名処理
- 確認者による記事への署名機能
- 数式表現に対応
- Ruby 及び Ruby on Rails による実装

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.

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.

柔軟なグループ設定

- 記事ごとの公開範囲の指定
  - 「自分のみ」、「グループ指定」、「全体公開」の三段階で指定可能
  - 「グループ指定」時は複数のグループを指定可能
  - グループ作成に階層構造を活用

arχves の公開グループ選択画面

記事公開グループ

- ☐ ::
- ☐ ::鳥根大学
- ☐ ::岡取大学
- ☐ ::広山大学
- ☐ ::山島大学
- ☐ ::島口大学
- ☐ ::鳥根大学:総合理工学部
- ☐ ::岡取大学:理学部
- ☐ ::広山大学:工学部
- ☐ ::山島大学:医学部
- ☐ ::島口大学:薬学部
- ☐ ::鳥根大学:総合理工学部:数理情報システム学科
- ☐ ::鳥根大学:総合理工学部:電子工学科
- ☐ ::岡取大学:理学部:数学科
- ☐ ::広山大学:工学部:情報工学科
- ☐ ::山島大学:医学部:医学科
- ☐ ::島口大学:薬学部:薬学科

データの四重署名

- arχves における四重署名とは

文書作成者自身の署名 (ユーザ署名),TimeStamp

＋

第三者による署名 (サーバ署名),TimeStamp

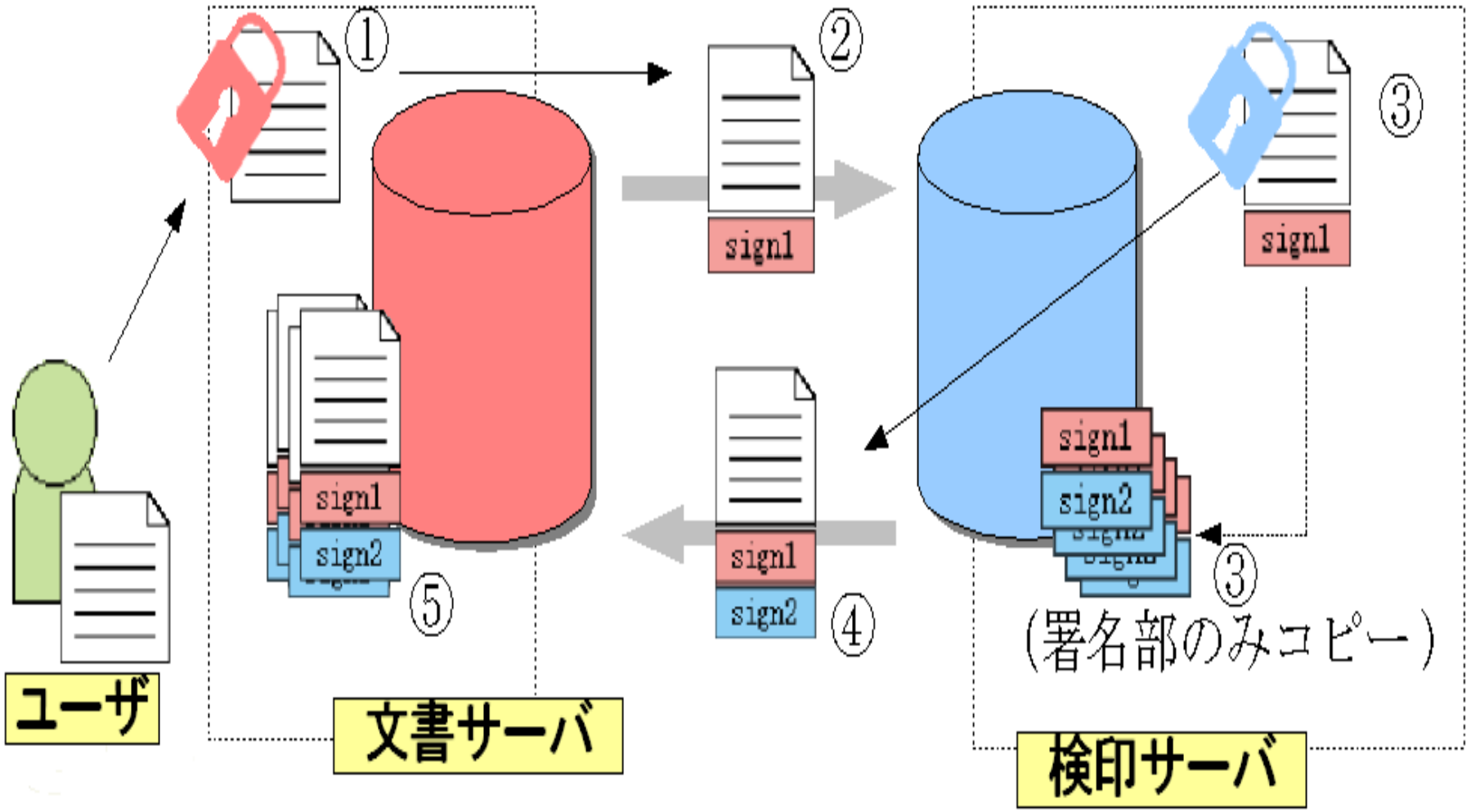
＋

確認者による署名 (確認者署名),TimeStamp

＋

第三者による署名 (サーバ署名),TimeStamp

データの２重署名処理


①
②
③
sign1
sign1
sign1
sign2
sign1
sign2
sign1
sign2
④
⑤
③
(署名部のみコピー)
ユーザ
文書サーバ
検印サーバ

arχves の署名処理の流れ

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

文書サーバ：二重署名された文書を保管するサーバ
検印サーバ：第三者による署名を行うサーバ

arχvesの記事投稿画面

arχves記事投稿例

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

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

実際のarχvesの記事の投稿例

チェックボックスによる柔軟なグループ指定
公開鍵暗号によるデータの2重署名

数式に対応
$\forall\ x \in \mathbb{C}\left(\sin^2 x + \cos^2 x = 1\right) + 1$

ClientTimeStamp: 2009-09-07T15:14:49+09:00
- -----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAkqkpNkACgkQFfuywYqu77gtgACgnsKLsVLXJE0slWFR63aBtbNt
W4MAoIFcVgCcMFMBJ7fuKXYYE8W6AKAm
=nYec
- -----END PGP SIGNATURE-----

Server TimeStamp. 2009-09-07T15:14:51+09:00
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAkqkpNsACgkQNkcjG4aWrL3ErACfTfuY0JyFIjWZwZ6UrheL2wFV
edQAn2t0Pp46ldk5SXiuWF+zSST1v4QF
=ssRz
-----END PGP SIGNATURE-----

公開範囲

::全体公開

研究記録としての価値

- ここまでの二重署名処理で正真性と非改竄性を保証

- さらに研究記録としての価値を高める為には・・・

⇒　**”確認者による署名”**が必要

確認者による署名

- 研究ノート (紙媒体の場合) :

  客観的な証拠（研究記録としての証拠）として機能するためには、本人の署名だけでは不十分

  ⇒ 内容を確認できる第三者の署名 (witness) により、研究記録としての証拠として力をもつ

これは、電子ノートでも言える

確認者に求められる条件

- 共同開発者でないこと
- 記録の内容を理解することができる

⇒

  - 近隣の研究室のリーダー
  - 同じ研究室の異なる研究チームのリーダー

実際にこのような第三者を見つけ出すことは必ずしも容易ではない

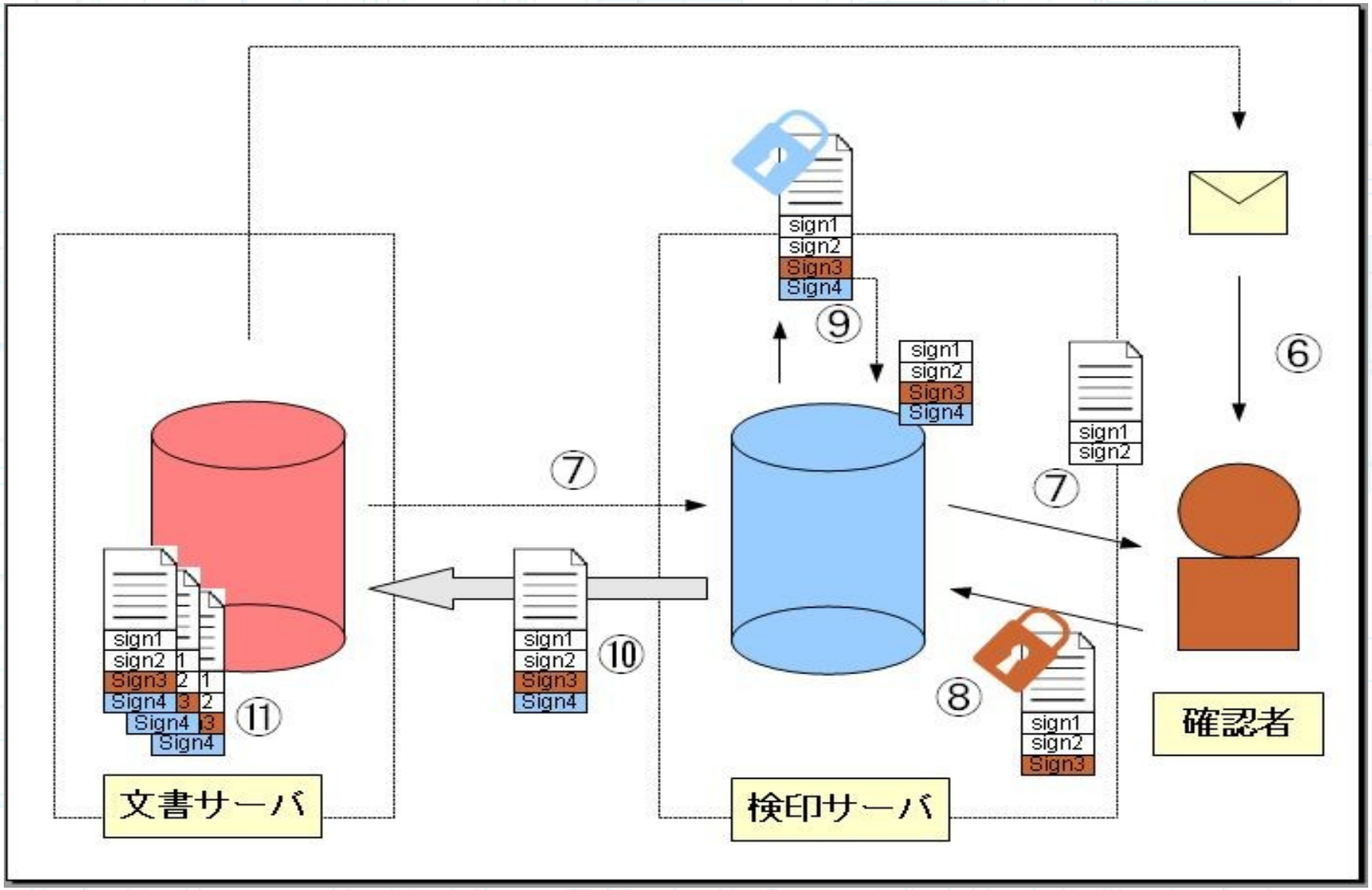
岡崎康司 , 隅蔵康一　編集 ,「理系なら知っておきたいラボノートの書き方」, 株式会社羊土社 ,2007

確認者の署名機能

ar χ ves の確認者の署名機能によって

- 距離的に離れた相手でも記録の確認ができる
- 記録の知的財産としての価値を高める

確認者によるデータへの署名



確認者署名の流れ

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

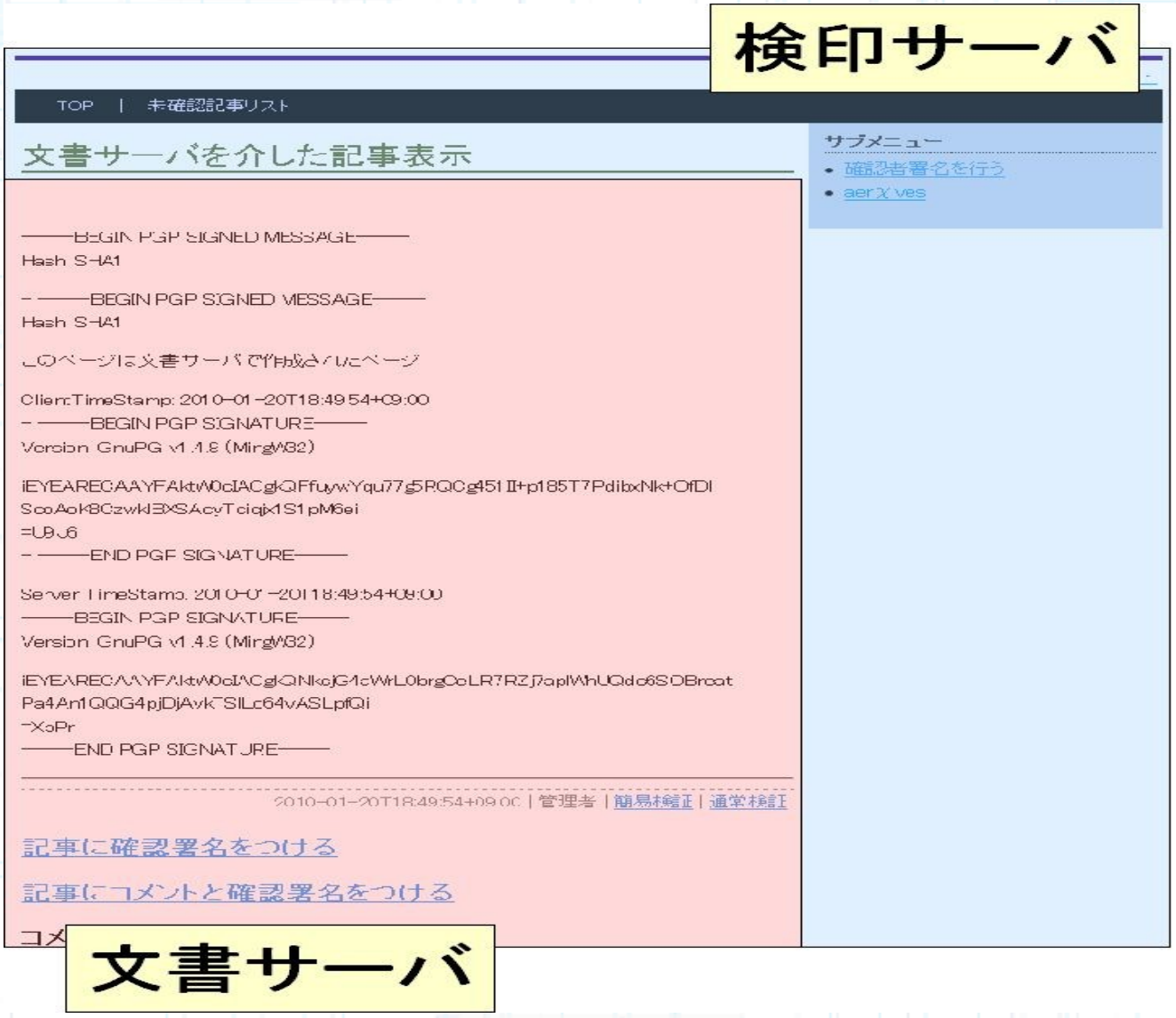
⑨ 検印サーバでサーバ署名を行い、署名部を保存する

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

以上の処理によって、データへの四重署名を行う

検印サーバを介した記事表示



確認署名済み記事表示画面

署名検証例

検証結果

投稿者：管理者

検証記事タイトル：記事の検証テスト

投稿日時：2010-01-27 14:11:50

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：確認者サーバー署名

gpg: 01/27/10 14:16:22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：確認者署名

gpg: 01/27/10 14:16:22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

検証結果：サーバー署名

gpg: 01/27/10 14:11:51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: 01/27/10 14:11:50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

検印サーバ側の署名部との照合結果

検印サーバ側の署名部と一致しています。
・ユーザ署名とサーバ署名が共に一致しています。

その他改良点

- 複数の文書サーバへの対応
- 複数の添付ファイルに対応

今後の課題

- ユーザインタフェース
  - 記事中の表、画像表示
  - 記事の表示方式
- セキュリティ
  - ハッシュ関数 sha-1 の問題 (2010 年問題)

参考文献

- 小林聡 , 加藤未来 ,「 arχves: 公開鍵暗号を用いた研究記録管理・検証・公開システム構築の試み」, 学術情報処理研究 ,No12,pp.43-51,2008.
- 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.
- 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.
- 岡崎康司 , 隅蔵康一　編集 ,「理系なら知っておきたいラボノートの書き方」, 株式会社羊土社 ,2007