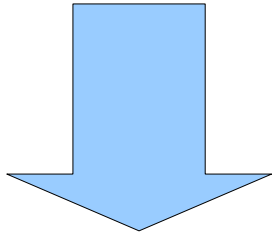
研究記録管理・公開・検証システム arχvesの数式およびグラフへの対応

小林聡研究室

S043052　島貫稚華

目的

- arχves：研究記録などの管理を主目的としたシステム



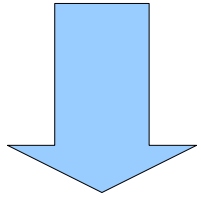
研究記録への対応を中心に改良

・数式

・グラフ

arχvesとは

- 研究データの捏造対策として、記事の真正性と非改竄性を保証し、検証機能を持つシステム
- 研究記録を共有できる範囲を柔軟に指定可能にするシステム



研究記録管理システムarχves

特徴

- SNSおよびBlogをベースにしている
- 記事ごとに公開範囲を設定可能
- 公開鍵暗号を用いてデータの二重署名処理を行う

概要①

- 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

グループ例）::島根大学

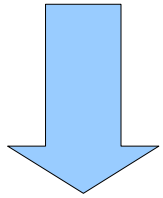
::島根大学:総合理工学部

概要②

- 二重署名（検印モデル）とは

業務記録の真正性および非改竄性を保証する方法

→部下が書いた記録に、上司が検印を捺す



文書作成者自身の署名＋第三者による署名

→真正性と非改竄性を保証

概要③

- データの二重署名処理

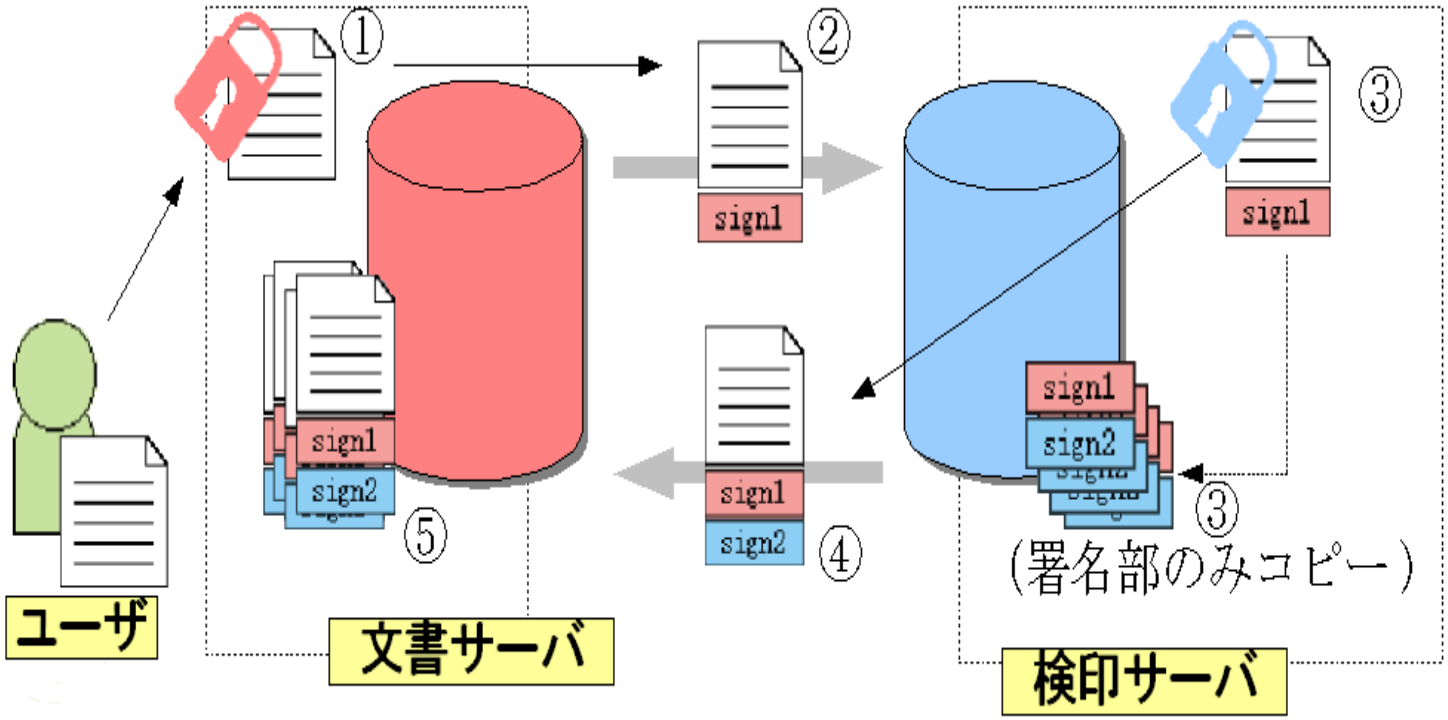


図1「検印モデル」を基にしたシステムの流れ

概要④

- 記事や投稿ファイルの検証機能
  - ・投稿された記事から1クリックで検証可能
  - ・検証は「簡易検証」と「通常検証」の2種

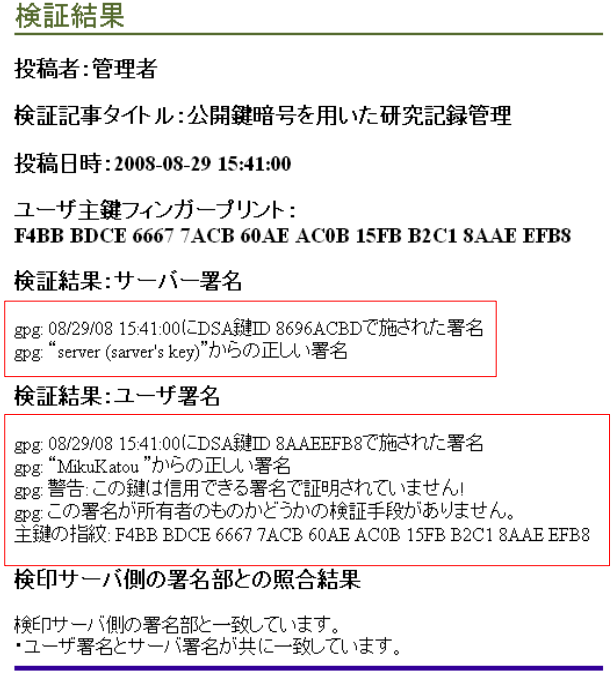
簡易検証：文書サーバのみで、ユーザの公開鍵と検印サーバの公開鍵を用いて検証を行う

通常検証：簡易検証に加えて検印サーバに記録されている署名との照合も含めて検証を行う

  - ・手作業での検証も可能

概要⑤

- # 記事の検証画面


検証結果

投稿者：管理者

検証記事タイトル：公開鍵暗号を用いた研究記録管理

投稿日時：2008-08-29 15:41:00

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: 08/29/08 15:41:00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

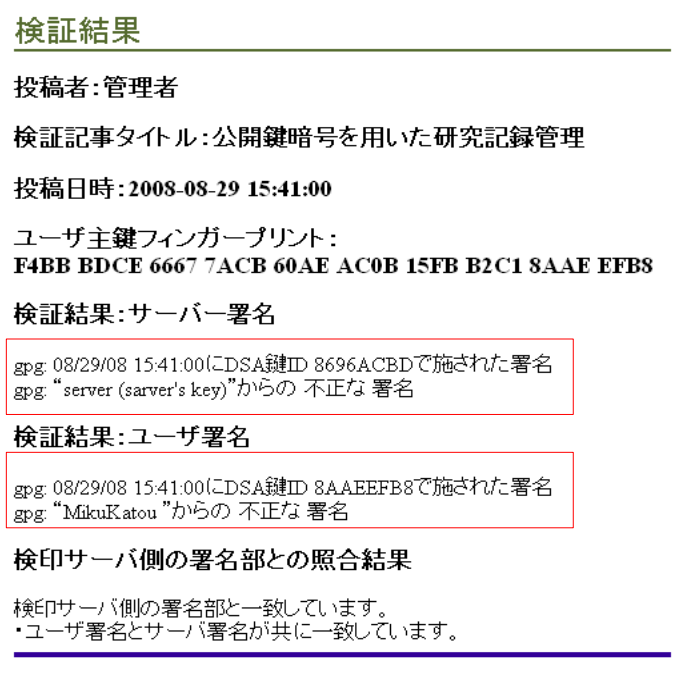
検証結果：ユーザ署名

gpg: 08/29/08 15:41:00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。

図2　通常の記事の検証


検証結果

投稿者：管理者

検証記事タイトル：公開鍵暗号を用いた研究記録管理

投稿日時：2008-08-29 15:41:00

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: 08/29/08 15:41:00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: 08/29/08 15:41:00にDSA鍵ID 8AAEEFB8で施された署名
gpg: “MikuKatou ”からの 不正な 署名

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。

図3　改竄された記事の検証

研究記録に関する改良①

- 数式への対応
  MathMLを人手で書くのは手間
  →ASCIIMathMLを用いて実現
- グラフへの対応
  →現在、ASCIIsvgに対応中

MathMLとASCIIMathMLの比較

例）数式a+b−3を書く場合

・MathMLでの書き方

```
<math xmlns=
"http://www.w3.org/1998/Math/MathML">
  <mi>a</mi>
  <mo>+</mo>
  <mi>b</mi>
  <mo>−</mo>
  <mn>3</mn>
</math>
```

・ASCIIMathMLでの書き方

```
amath a+b−3 endmath
```

研究記録に関する改良②

- 数式表示画面

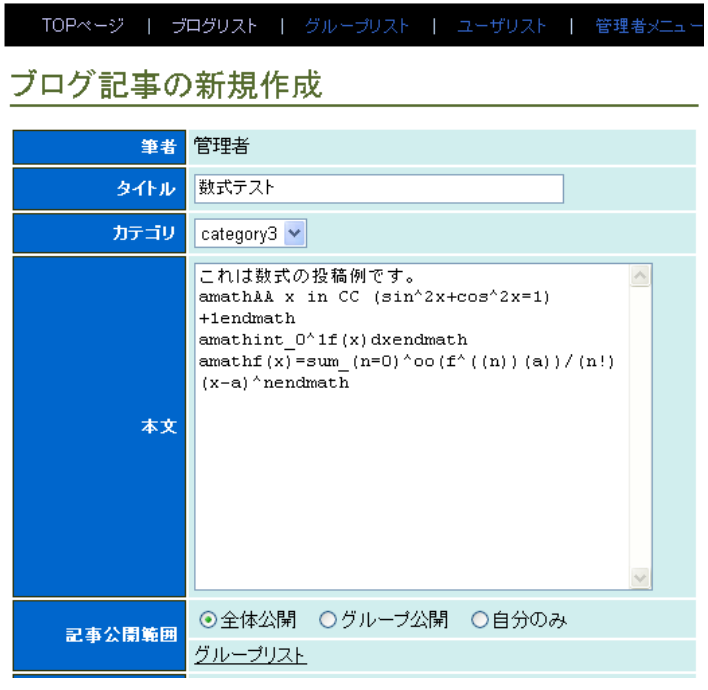


図4　記事の作成画面

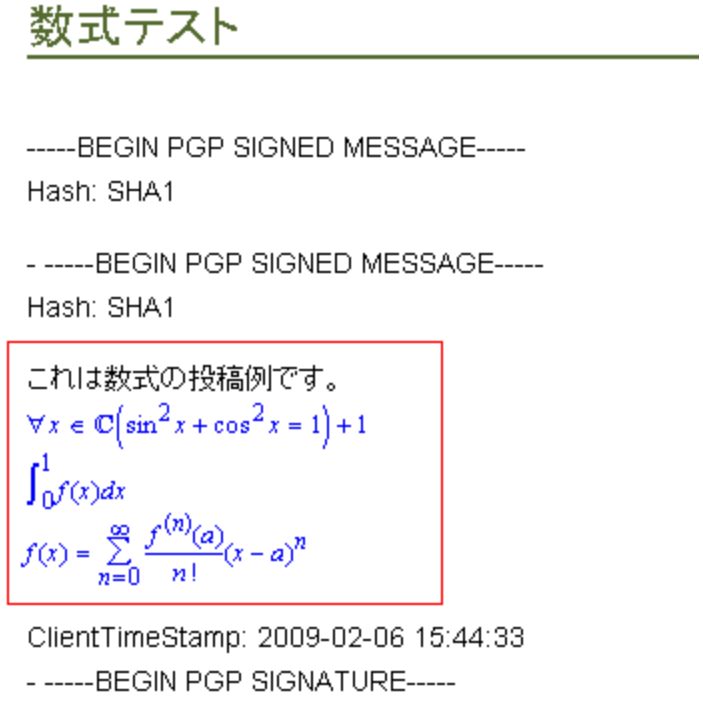


図5　図4の記事投稿画面

研究記録に関する改良③

- グラフ表示

```
<embed width="117" height="117" src="d.svg"
script='initPicture(-2,2)
axes()
stroke = "blue"
p = []
for (x = -2; x < 2; x += 0.1)
  p[p.length] = [x, (x+1)*x*(x-1)]
path(p)
// there is also a plot("...") shorthand'>
```

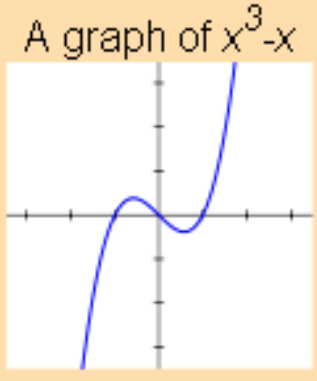


図6　ASCIIsvgのコードとグラフ

（http://www1.chapman.edu/~jipsen/asciisvg.htmlより抜粋）

ユーザインタフェースに関する改良

- グループ指定画面

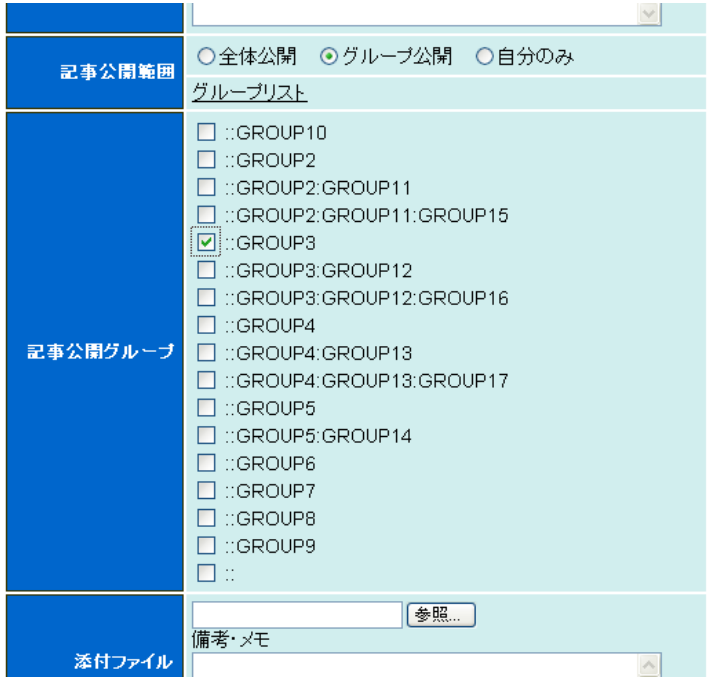


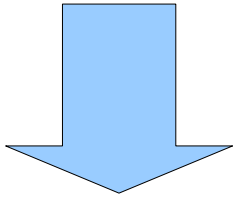
図7　記事公開範囲の指定画面

・記事投稿の際のテキストエリアでの煩雑な入力

→チェックボックスで指定可能に

セキュリティに関する改良

- 文書サーバと検印サーバ間でのIDとパスワードでの認証の実現



・他のサーバからの成りすましを回避する

・複数の文書サーバに対応

今後の課題

- **セキュリティの問題**
  - ・非改竄性の証明の強度の向上
  - ・署名時の文書サーバと検印サーバ間の通信時の情報漏洩への対策
- **ユーザインタフェースの課題**
  - ・複数システムのユーザ認証の際のDelegate機能の実装
- **研究記録への対応の課題**
  - ・記事中での表、画像や化学式などへの対応
  - ・漢字における異体字や国字に対しての対応
- **その他の課題**
  - ・記事やユーザ情報の保存・管理方法の改良
  - ・投稿された記事内容の妥当性の確認