

研究記録管理・公開・検証システム arXivにおける確認者署名機能の実現

島根大学

加藤 康
島貫 稚華
藤坂 達也
○小林 聡

はじめに

- ◆ 研究成果、論文の捏造、剽窃
 - ◆ 本年東京大学において、学位論文に他人の著作物の一部を盗用した箇所が全体の約4割にわたって存在するなどの理由により、一旦授与した博士号の取り消しがなされた
- ◆ 技術的な対策は困難
- ◆ 研究記録が適切に管理・運用されていれば
 - ◆ 研究の経緯
 - ◆ 研究の実態
 - ◆ これらの検証の助けになる

はじめに

- ◆ 研究記録の正真性と非改竄性, および存在証明の保証をいかに行なうかが課題
 - ◆ 電子署名を用いた研究記録管理・公開・検証システムarXivesを構築
- ◆ 研究記録の証拠能力を高めるためには…
 - ◆ 確認者(証人)による確認および署名が必要
 - ◆ ただし、誰でも良いわけではない
 - ◆ 当然、信用できる人物でなければならない
 - ◆ 加えて…

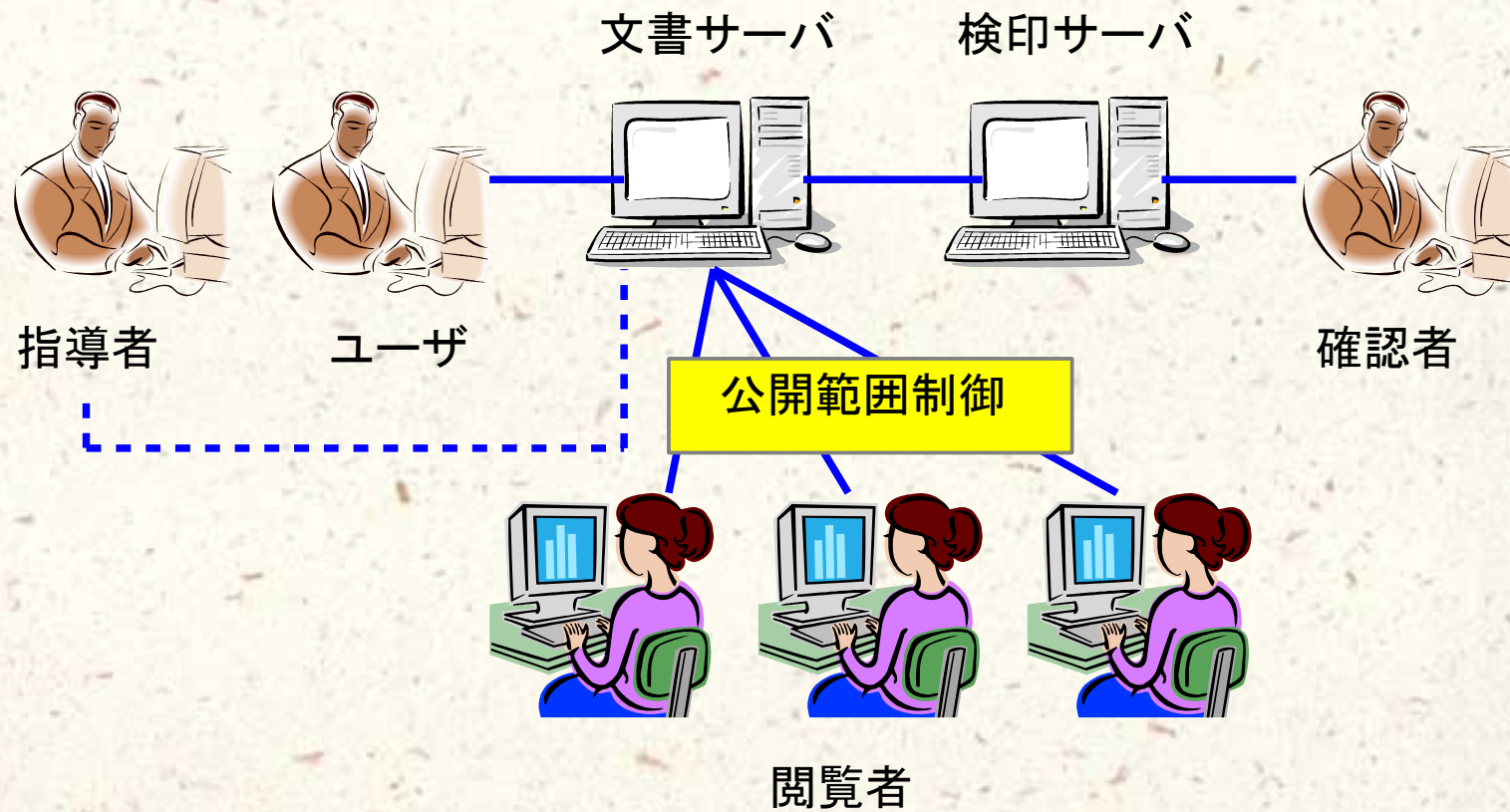
はじめに

- ◆ 確認者の要件(岡崎ら, 2007)
 - ◆ 必須要件:
 - ◆ 発明が理解できる者
 - ◆ 共同研究者でない者
 - ◆ 好ましい要件:
 - ◆ 将来にわたり, 発明について証言可能な者
 - ◆ 避けるべき要件:
 - ◆ 共同発明者の疑念を持たれる共同研究者や上司

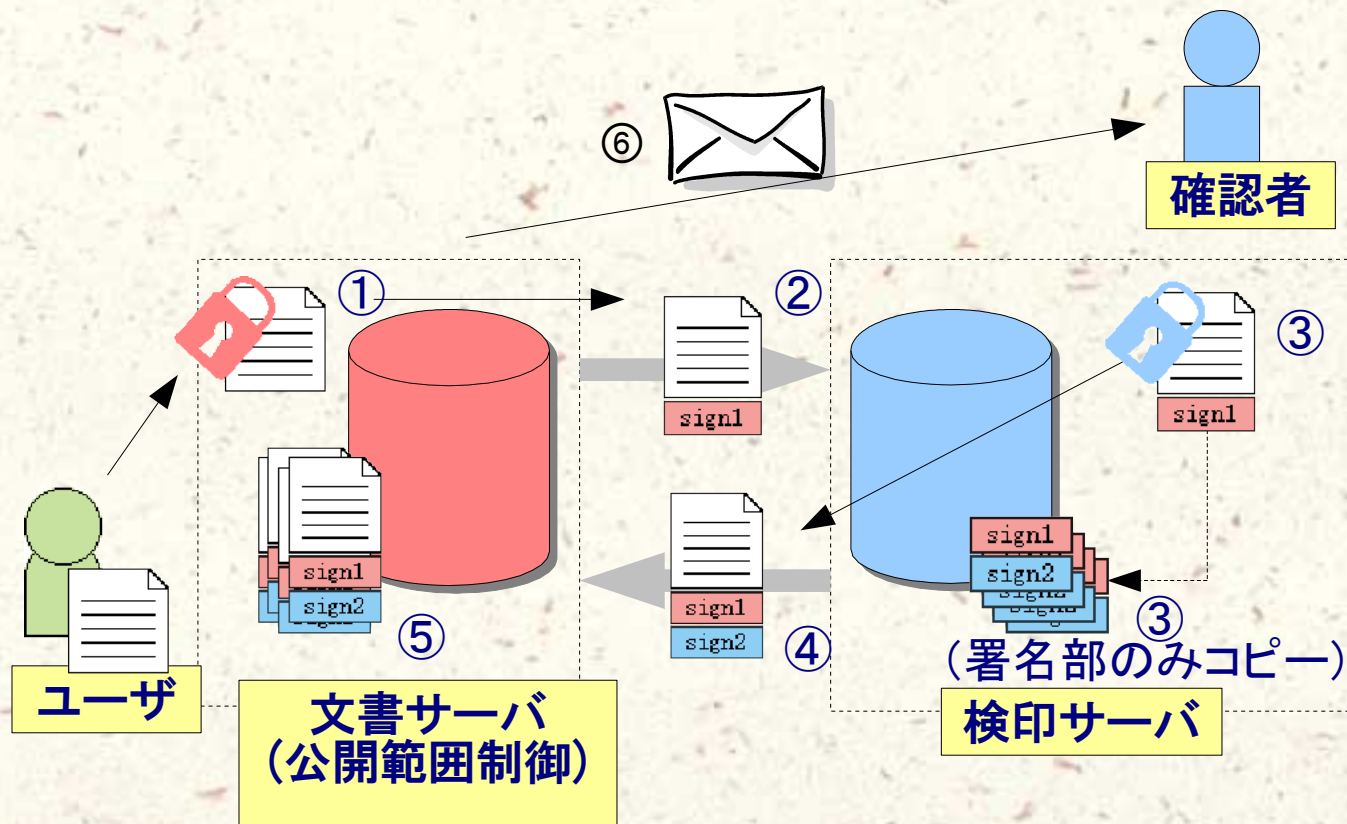
はじめに

- ◆ このような要件を満たす確認者を身近に見つけることは必ずしも用意ではない
- ◆ ネットワークを用いれば、地理的に離れた場所にいる人物に確認を依頼することも可能
- ◆ そこで、ar χ vesに確認者署名機能を実現

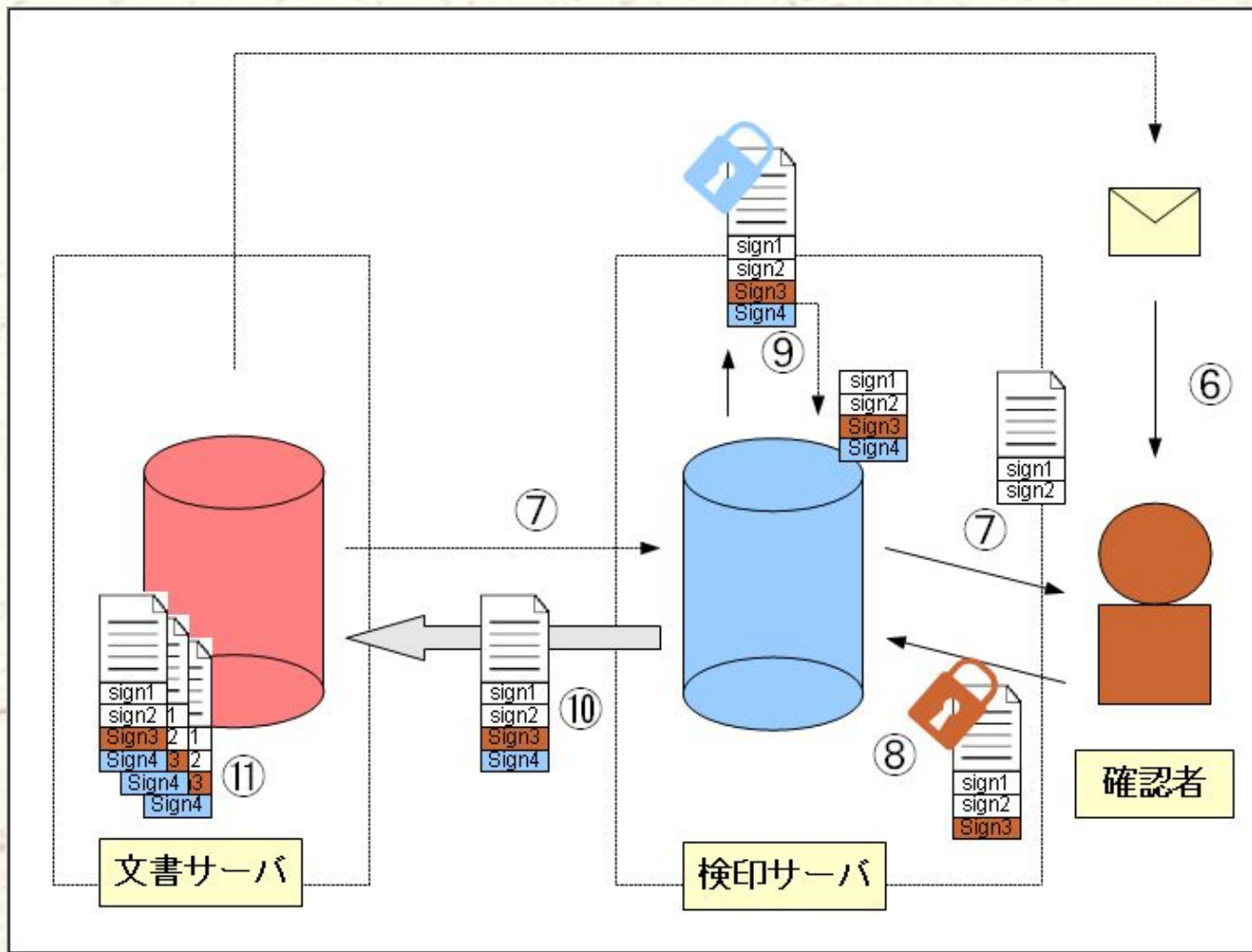
システム概要



システム概要 (Phase 1)



システム概要 (Phase 2)



環境・ツールなど

- ◆ 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
Mongrel ver. 1.1.5
- ◆ SSL ライブラリ: OpenSSL ver.0.9.8
- ◆ DBMS: MySQL ver. 5.0.27

Phase 2: ログイン

検印サーバへの ログイン

TOP | 未確認記事リスト

ログイン

ユーザー名:

パスワード:

Powered by [Ruby on Rails 1.2](#)

リンク

- [aerX ves](#)

文書サーバへの ログイン (via 検印サーバ)

確認者さんのアカウント | [ログアウト](#)

TOP | 未確認記事リスト

文書サーバログイン

ユーザー名:

パスワード:

ログインに失敗しました

Powered by [Ruby on Rails 1.2](#)

リンク

- [aerX ves](#)

面倒・欠点は承知の上

Phase 2: 検印サーバ経由での 文書サーバへのアクセス

[確認者さんのアカウント](#) | [ログアウト](#)

TOP | [未確認記事リスト](#)

新規記事作成

文書サーバ

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

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

新規に記事を作成します

ClientTimeStamp: 2010-02-05T15:29:42+09:00

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAktrutcACgkQFFuywYqu77JYjwCfbCcOub3zcDS3J/PktkrFAPnc
evgAn0nq07NtEAaZaR0ZoAulG0tEnu5I
=puBe

-----END PGP SIGNATURE-----

ServerTimeStamp: 2010-02-05T15:29:44+09:00

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEUEARECAAYFAktrutcACgkQNIkcjG4aWrlL0qwQC9mQw7e7Q5HDRJ6a9OGMmyeF
awCcCWlhbHX1FIGg7Xn6euOc8IFz1PJo=
=rguj

-----END PGP SIGNATURE-----

2010-02-05T15:29:43+09:00 | [管理者](#) | [簡易検証](#) | [通常検証](#)

[記事に確認署名をつける](#)

[記事にコメントと確認署名をつける](#)

コメント

文書サーバ

Powered by [Ruby on Rails 1.2](#)

Phase 2: 確認署名

管理者さんのアカウント | ログアウト

TOPページ | ブログリスト | グループリスト | ユーザリスト | 管理者メニュー

新規記事作成

記事表示メニュー

- 管理者さんのブログ (16)
- 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5件
- タイトルリスト表示

ユーザメニュー

- 自分のブログ記事を作成
- 記事と添付ファイルの検証方法
- 数式の投稿方法

検索

検索

新規に記事を作成します

ClientTimeStamp: 2010-02-06T15:29:42+09:00

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.9 (MingW32)

iEYEAQAAAYFAktrutoACgkQGFfuywYqu77YimCfbOoUub3zdDS3J/PktrFAFho
evgAnQnq07NtEAsZaRQZoauiG0tEnJl
=puBe

-----END PGP SIGNATURE-----

ServerTimeStamp: 2010-02-06T15:29:44+09:00

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.9 (MingW32)

iELEARECAAYFAktrutoACgkQKqG4aWLDQwQCY9mQw7e7Q5HQRJ6a9QGMmyeF
awOoQWbHhX1FIgE7Xn6euOoc8IFz1PJo=

-----END PGP SIGNATURE-----

ConfirmerTimeStamp: 2010-02-06T15:33:14+09:00

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.9 (MingW32)

iEYEAQAAAYFAktrutoACgkQGFfuywYqu77glagOfatckIMm6AqYQ+KvYs9JDZ
Bb8AoOu044z/ANhFRU6Ce12QuMMoyG8
=w/et

-----END PGP SIGNATURE-----

ServerTimeStamp#2: 2010-02-06T15:33:14

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.9 (MingW32)

iEYEAQAAAYFAktrutoACgkQKqG4aWLDQwQCY9mQw7e7Q5HQRJ6a9QGMmyeF
PvQAn3Cjpe8R2NqLAdJlyDsffMmV
=KTab

-----END PGP SIGNATURE-----

公開範囲

全体公開

2010-02-06T15:29:43+09:00 | 管理者 | 簡易検証 | 通常検証 | コメント (0) | category2

コメントを書く

- by 文書サーバ(正真性)
(w/ ユーザの秘密鍵)
- by 検印サーバ(存在証明)
(w/ 検印サーバの秘密鍵)
- by 検印サーバ(正真性)
(w/ 確認者の秘密鍵)
- by 検印サーバ(存在証明)
(w/ 検印サーバの秘密鍵)

検証

[ユーザーさんのアカウント](#) | [ログアウト](#)

TOPページ | ブログリスト | グループリスト | ユーザリスト

検証結果

投稿者: ユーザ

検証記事タイトル: 数式テスト

投稿日時: 2010-06-24 19:10:57

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: 06/24/10 19:13:01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: 06/24/10 19:13:01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: 06/24/10 19:10:57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: 06/24/10 19:10:57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

検印サーバー側の署名部との照合結果

検印サーバー側の署名部と一致しています。
•全ての署名が一致しています。

サブコンテンツ

- 公開鍵のダウンロード
- ブログ著者リスト
- 確認者ログイン

Powered by [Ruby on Rails 1.2](#)

13

2010-Sep-10 第14回学術情報処理研究集会@和歌山大(和歌山ビッグ愛)

課題(1/4)

- ◆ 二重のログインが面倒
- ◆ 検印サーバ経由で文書サーバにログイン
 - ◆ 検印サーバにて両サーバのユーザID&パスワードを取得可能
 - ◆ 学術認証フェデレーションが立ち上がるので欠点はあえて無視
 - ◆ Web認証基盤の活用
 - ◆ Shibboleth? OpenID? その他?

課題(2/4)

- ◆ ユーザインタフェース
 - ◆ グループの選択
 - ◆ 添付ファイル数
 - ◆ 現状: グループ選択はチェックボックス
 - ◆ 現状: 添付ファイル数上限あり
 - ◆ DBの構造上の制限ではない
 - ◆ Javascript & DynamicHTML & Ajax?

課題(3/4)

◆ 投稿タイミング

- ◆ twitter, Google Buzzのようなつぶやきを活用?

- ◆ IRC?

- ◆ 一種の履歴交差にもなる

- ◆ Linux + Ruby 1.9.x + Rails 2 or 3への移植

- ◆ 記録の自然言語処理・知的処理

課題(4/4)

Twitter / ホーム - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

http://twitter.com/

よく見るページ HotMail の無料サー... Windows Media Windows リンクの変更 Getting Started Latest Headlines おもしろフラッシュ... Latest Release Notes Fedora Project Fedora Weekly News

ブックマーク

検索対象(S):

- rails test
- ajax test
- Methuselah1stDrft's ...
- ProjectGutenbergJP's ...
- REBOL's Wiki - FrontP...
- ProjectProgrammingT...
- HDL-GTR series - I-O ...
- 過去の講義
- System09's Wiki - Fro...
- WiredX beta
- skoba's Page
- skoba's page - skoba'...
- skoba.org
- skoba.org@livedoor
- https://hspc.flxsrj.jp/...
- http://www.skoba.org/
- https://www.skoba.org/
- http://blog.skoba.org/
- http://wiki.skoba.org/...
- https://webmail.skob...
- ホーム (skoba34)
- Google Apps
- gapps.skoba.org(Go...
- lab-wiki.gapps.skob...
- CompSec10
- mail.gapps.skoba.or...
- Google Apps
- skoba34の仕事ページ
- skoba's page
- skoba.org メール - ...
- REBOL
- Index of Japanese Do...
- ホーム (REBOLのwiki...
- REBOLについてのwiki ...
- REBOL Technologies
- REBOL - X Internet, ...
- REBOL Technologies - ...
- REBOL.org

twitter

ホーム プロフィール 友だちを検索 設定 ヘルプ ログアウト

いまどうしてる? 140

最新ツイート: 和歌山なう。マイレーザポインタを忘れてきた... 30秒前後前

ツイート

ホーム

skoba34 和歌山なう。マイレーザポインタを忘れてきた... 30秒前後前 webから

pen_house 限定品『少数民族シリーズ マブチェ』販売開始いたしました!! http://www.pen-house.net/brand/brand0007.html#3417 #pen_house #bungu 8分前 webから

yukihiro_matz zipper?! RT @mametter: @yukihiro_matz やっぱーer ですよ 約1時間前 Chromed Birdから

pen_house 三菱鉛筆『ビューモルト オークウッドプレミアムエディション 複合筆記具 MSE4-5025』http://bit.ly/at0Paj 商品追加いたしました!! #pen_house #bungu 約1時間前 webから

yukihiro_matz そんな長い名前でもいいんですか? RT @knu: @yukihiro_matz 名前は Enumerator.zip(e1, e2, ...) では駄目かなあ。本当は [e1, e2, ...] zip かいいいりなすとかぶってる 約1時間前 Chromed Birdから

pen_house パイロット ゲルインキボールペン フリクションポイント ビズ LF-2SP4-B ブラック http://www.pen-house.net/detail/detail16987_001.html #pen_house これは便利! 消せるボールペン。ぜひお試しください☆

HottoMotto

えっ? twitter で 映画ドラえもん 豪華DVD-BOX が当たるの!? 5週連続プレゼント! 映画大集合 今すぐツイート

skoba34 54ツイート

12 フォロー 8 フォロー 1 リスト している されている

おすすめユーザー

namatshara 田原総一朗 780-する

yhara yhara 780-する

全てを見る

ホーム

@skoba34

ダイレクトメッセージ 0

お気に入り

リツイート

完了

ウ... D... T... あ般 CAPS KANA 19:40

Phase 2: ログイン

検印サーバへの
ログイン

文書サーバへの
ログイン
(via 検印サーバ)

確認者さんのアカウント | ログアウト

TOP | 未確認記事リスト

TOPページ

このページです。

未確認記事リスト

未確認の記事のリストを表示します。記事を確認するためには文書サーバへのログインが必要です。

サブメニュー

- 文書サーバにログイン
- aerX ves

Powered by [Ruby on Rails 1.2](#)

確認者さんのアカウント | ログアウト

TOP | 未確認記事リスト

文書サーバログイン

ユーザー名:

パスワード:

ログインに失敗しました

リンク

- aerX ves

Powered by [Ruby on Rails 1.2](#)

面倒・欠点は承知の上

Phase 1: 記事投稿

管理者さんのアカウント | ログアウト

TOPページ | ブログリスト | グループリスト | ユーザーリスト | 管理者メニュー

ブログ記事の新規作成

筆者	管理者
タイトル	数式テスト
カテゴリ	category3
本文	Let's try some interesting formulas: amathAA x in CC (sin²x+cos²x=1)+1endmath
記事公開範囲	☒ 全体公開 ☐ グループ公開 ☐ 自分のみ
記事公開グループ	グループリスト ☐ : ☒ :鳥根大学 ☐ :同取大学 ☐ :広山大学 ☐ :山島大学 ☐ :鳥口大学 ☐ :鳥根大学 総合理工学部 ☐ :同取大学 理学部 ☐ :広山大学 工学部 ☐ :山島大学 医学部 ☐ :鳥口大学 薬学部 ☒ :鳥根大学 総合理工学部 数情報システム学科 ☐ :鳥根大学 総合理工学部 電子工学科 ☐ :同取大学 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 ☐ :鳥口大学 薬学部 薬学科
確認者選択	☒ 管理者 ☐ conf
添付ファイル	ファイルを選択 Graph1.bmp 備考・メモ ファイルを選択 Graph2.bmp 備考・メモ ファイルを選択 Graph3.bmp 備考・メモ ファイルを選択 選択されていません 備考・メモ ファイルを選択 選択されていません 備考・メモ

プレビュー 投稿

Powered by [Ruby on Rails 1.2](#)

記事本文

公開範囲制御

添付ファイル

Phase 1: 署名

管理者さんのアカウント | ログアウト

TOPページ | ブログリスト | グループリスト | ユーザリスト | 管理者メニュー

記事を投稿しました。

新規記事作成

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

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

新規に記事を作成します

記事表示メニュー

- 管理者さんのブログ (16)
- 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5件
- タイトルリスト表示

ユーザーメニュー

- 自分のブログ記事を作成
- 記事と添付ファイルの検証方法
- 数式の投稿方法

検索

ユーザ署名

ClientTimeStamp: 2010-02-05T15:29:42+09:00
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAktrutgACgkQIFfuywYqu77JyJwCfbCc0ub3zcDS3J/PktrFAPnc
evgAn0nq07NtEAaZaR0ZoAu1G0tEnJ5I
=puBe
-----END PGP SIGNATURE-----

サーバ署名

ServerTimeStamp: 2010-02-05T15:29:44+09:00
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEUEARECAAYFAktrutgACgkQlNkcjG4aWtL0qWQC9mQw7e7Q5HDRJj6a9OGMmryeF
awC0CWlHbHX1FiGg7Xn6euOc8IFz1PJo=
=rguj
-----END PGP SIGNATURE-----

公開範囲
::全体公開

2010-02-05T15:29:43+09:00 | [管理者](#) | [簡易検証](#) | [通常検証](#) | [コメント\(0\)](#) | [category3](#)

[コメントを書く](#)

コメント

by 文書サーバ

by 検印サーバ

検印サーバにも、署名部は
保存される

Phase 1: ログイン

TOPページ ブログリスト	
TOPページ	ユーザ専用ページ
TOPページ	ユーザ名:
このページです。	パスワード:
ブログリスト	ログイン
投稿された記事が閲覧できます。	サブコンテンツ
ユーザリスト	- 公開鍵のダウンロード - ブログ著者リスト - 確認者ログイン
システムの利用者の一覧や詳細を見ることが出来ます。	
グループリスト	
グループの一覧や詳細を見ることが出来ます。	
管理者メニュー	
各種データの管理(編集・削除)を行えます(管理者のみ)。	
- アカウントを持っている方はサイドバーにあるフォームからログインしてください。 - 自分のアカウント情報や投稿した記事やグループの修正は、ログイン後画面右上の「〇〇さんのアカウント」という文字に張られたリンクから行えます。 - 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。	

Powered by [Ruby on Rails 1.2](#)

Phase 1: 二重署名

管理者さんのアカウント | ログアウト

TOPページ | ブログリスト | グループリスト | ユーザリスト | 管理者メニュー

数式表示

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

--BEGIN PGP SIGNED MESSAGE--
Hash: SHA1

Let's try some interesting formulas: $\forall x \in \mathbb{C} (\sin^2 x + \cos^2 x = 1) + 1$

ClientTimeStamp: 2010-02-01T13:08:40+09:00

--BEGIN PGP SIGNATURE--
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAktmU8gACgkQFFuywYqu77gUAQCfb3hZr4ci+7taMQrtC8B/eTVJ
SccAoNC4d9N4BBSsqMBz8DHBPeZ/vQkD
=+nvp

--END PGP SIGNATURE--

ServerTimeStamp: 2010-02-01T13:08:40+09:00

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEARECAAYFAktmU8gACgkQNKcjG4aWrl1ttgCfZ3L2vEa9SleS3u3TgQqA+WHC
REkAnRUTCJhLqXhAWHfLrsALnOVXSsx
=tXms

-----END PGP SIGNATURE-----

記事表示メニュー

- [管理者さんのブログ](#) (16)
- [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5件](#)
- [タイトルリスト表示](#)

ユーザメニュー

- [自分のブログ記事を作成](#)
- [記事と添付ファイルの検証方法](#)
- [数式の投稿方法](#)

検索

Phase 1: 確認者へのメール

GraceMail® Version6

受信 新規 アドレス 設定 ヘルプ ログアウト

メール検索 フォルダ整理

新着 1件

- 受信箱
- 送信済
- 下書き
- ゴミ箱
- [ゴミ箱を空にする]

1 - 49 / 49

全選択 全解除 【選択したメールをフォルダに移動します】 移動 削除

R	表題	添付	送信者	日付▼	サイズ
☐	[確認依頼]管理者さんが記事を投稿しました		arxves@matsu.shimane-u.ac.jp	2010/02/05 15:29	2 kB
☐	[確認依頼]管理者さんが記事を投稿しました		arxves@matsu.shimane-u.ac.jp	2010/02/01 11:47	2 kB
☐	[確認依頼]管理者さんが記事を投稿しました		arxves@matsu.shimane-u.ac.jp	2010/02/01 11:44	2 kB
☐	[確認依頼]管理者さんが記事を投稿しました		arxves@matsu.shimane-u.ac.jp	2010/01/27 14:11	2 kB
☐	[確認依頼]管理者さんが記事を投稿しました		arxves@matsu.shimane-u.ac.jp	2010/01/20 18:49	2 kB

[送信者に返信] [全員に返信] [転送] [再編集] [ヘッダ表示] [保存] [印刷]

subject: [確認依頼]管理者さんが記事を投稿しました
 from: arxves@matsu.shimane-u.ac.jp
 reply-to: arxves@matsu.shimane-u.ac.jp
 to: ■ ■ ■ ■ ■ ■ ■
 date: Fri, 5 Feb 2010 15:29:44 +0900

[jump to attachment file](#)

記事タイトル: 新規記事作成
 記事URL: <http://cainan.cis.shimane-u.ac.jp:3000/list/show/36>

[jump to head](#)

[送信者に返信] [全員に返信] [転送] [再編集] [ヘッダ表示] [保存] [印刷]

Phase 2: 確認(1/2)

[確認者さんのアカウント](#) | [ログアウト](#)

TOP | 未確認記事リスト

未確認記事リスト

2010-02-05T15:29:43+09:00 [管理者]	新規記事作成
2010-02-01T13:08:40+09:00 [管理者]	数式表示
2010-02-01T11:47:12+09:00 [管理者]	数式テスト
2010-02-01T11:44:07+09:00 [管理者]	神宮で野球観戦

サブメニュー

- [文書サーバにログイン](#)
- [aerX ves](#)

Powered by [Ruby on Rails 1.2](#)

Phase 2: 確認(2/2)

確認者さんのアカウント | ログアウト

TOP | 未確認記事リスト

新規記事作成

サブメニュー

- 確認者署名を行う
- aerX-yes

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

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

新規に記事を作成します

ClientTimeStamp: 2010-02-05T15:29:42+09:00
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEYEAReCAAYFAktrutcACglQFFuywYqu77YjwCfbCc0ub3zcDS3J/PktrFAPnc
evgAn0nq07NtEAaZaR0Z0AulG0tEnu5I
=puBe
-----END PGP SIGNATURE-----

ServerTimeStamp: 2010-02-05T15:29:44+09:00
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (MingW32)

iEUEARECAAYFAktrutgACglQINkcjG4aWtL0qwQC9mQw7e7Q5HDRJf6a9OGMmnyeF
awCcCWhbHX1FiGg7Xn6euOc8IFz1Pj0=
=rguj
-----END PGP SIGNATURE-----

2010-02-05T15:29:43+09:00 | 管理者 | 簡易検証 | 通常検証

記事に確認署名をつける

記事にコメントと確認署名をつける

コメント

Powered by [Ruby on Rails 1.2](#)

Phase 2: 確認(3/3)

[確認者さんのアカウント](#) | [ログアウト](#)

TOP | [未確認記事リスト](#)

検証結果

投稿者: 管理者

検証記事タイトル: 新規記事作成

投稿日時: 2010-02-05 15:29:43

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: 02/05/10 15:29:44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: 02/05/10 15:29:43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。

サブメニュー

- [文書サーバにログイン](#)
- [aerXves](#)

Powered by [Ruby on Rails 1.2](#)