

署名Webサービスの提案

～暗号便PKIを用いたユビキタス署名の実現～

梅野健^{1) 2)}、寺井秀明¹⁾、高明慧¹⁾

Web:<http://www.angobin.jp>

1)株式会社カオスウェア

2)独立行政法人情報通信研究機構

2008年11月14日

INFOPRO2008

現状のメール、ファイル転送の課題

- **迷惑メールの問題(本当に信頼できる送信者か?)**
 - **フィッシング詐欺の問題(本当に信頼できるダウンロードサイトか?)**
 - **中身の改竄が行われていないかチェックできない。**
 - **伝送日時の証明が郵便の様にできない。**
-

この問題を解決する 電子署名の基本要件

■ 要件

- 電子署名の作成は本人しかできないこと
 - 電子署名のチェックは署名者の公開鍵を用いることで万人ができること
 - 署名する文書を一文字でも変えれば改ざんされていることがわかること
-

だが、“電子署名”の抱えている課題もある。

- **メールの電子署名機能を用いる場合、相手も、同じメーカー電子署名機能が必要(普遍的に誰もが用いることはできない。)**
 - **物理的に利用が制約される(電子署名機能ソフトがインストールされているPCのみ等)。どこでも、いつでも、という訳にはいかない。**
-

これらの問題を全て解決する “署名Webサービス”(今回提案)の概要

- まず、Webサービス提供者自身の真正性を証明。
 - Web上で署名し、Web上で電子署名Check
 - Webサービスログインアカウントと電子署名用の鍵(公開鍵、秘密鍵のペア)を紐付ける。
 - 送信ファイルの暗号化に必要な公開鍵とは、別の電子署名用公開鍵を用いて署名Checkする。
 - 電子署名は、QRコード表示でも提供し、携帯電話でも、いつでもどこでも電子署名のチェック可能(ユビキタス署名)。
 - Web上で、誰もが、電子署名Checkできる様(電子署名基本要件の一つ)にする(電子署名用の公開鍵データベースにアクセスする)。
 - WebApplicationなので、プラットフォーム非依存(Windows, Mac, 携帯電話)。
-

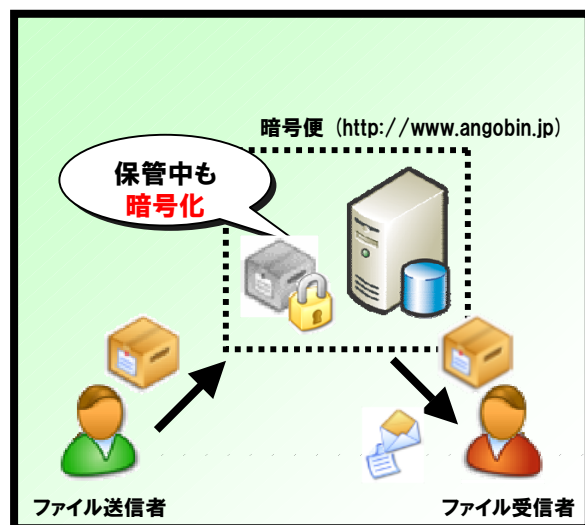
署名Webシステム

- **実は、先月(2008年10月10日)から稼動しています。**

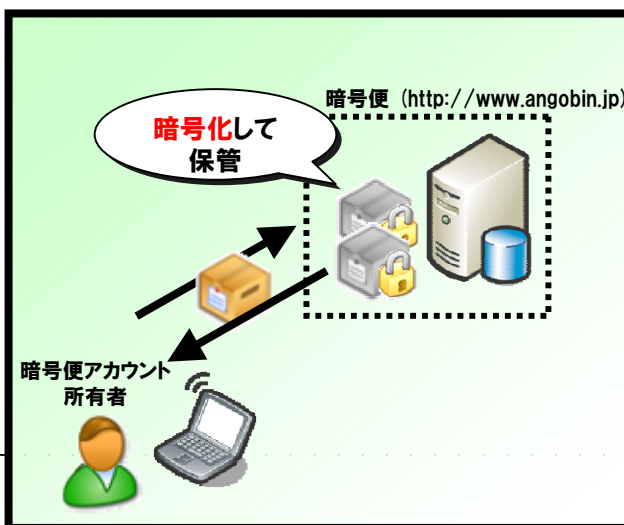
暗号便(angobin.jp)について

- 2006年12月から提供のユビキタス公開鍵インフラシステム
- 大きく以下の3つの機能を持つ
 - メールに添付できない重たいファイルを**公開鍵で暗号化**し送信する機能
 - ファイルを暗号化保管することができる**ストレージ**機能
 - **暗号便インフラを通して送信されるファイル・コンテンツに対して電子署名を行う署名Web**(2008.10.10からサービス開始)

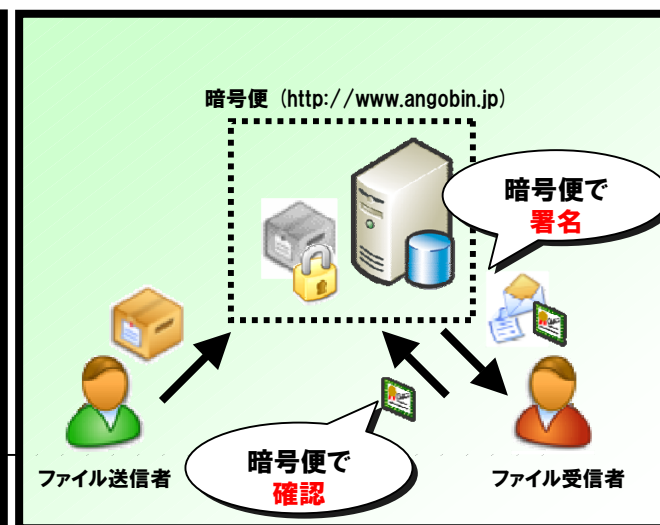
ファイル転送機能



ファイルストレージ機能

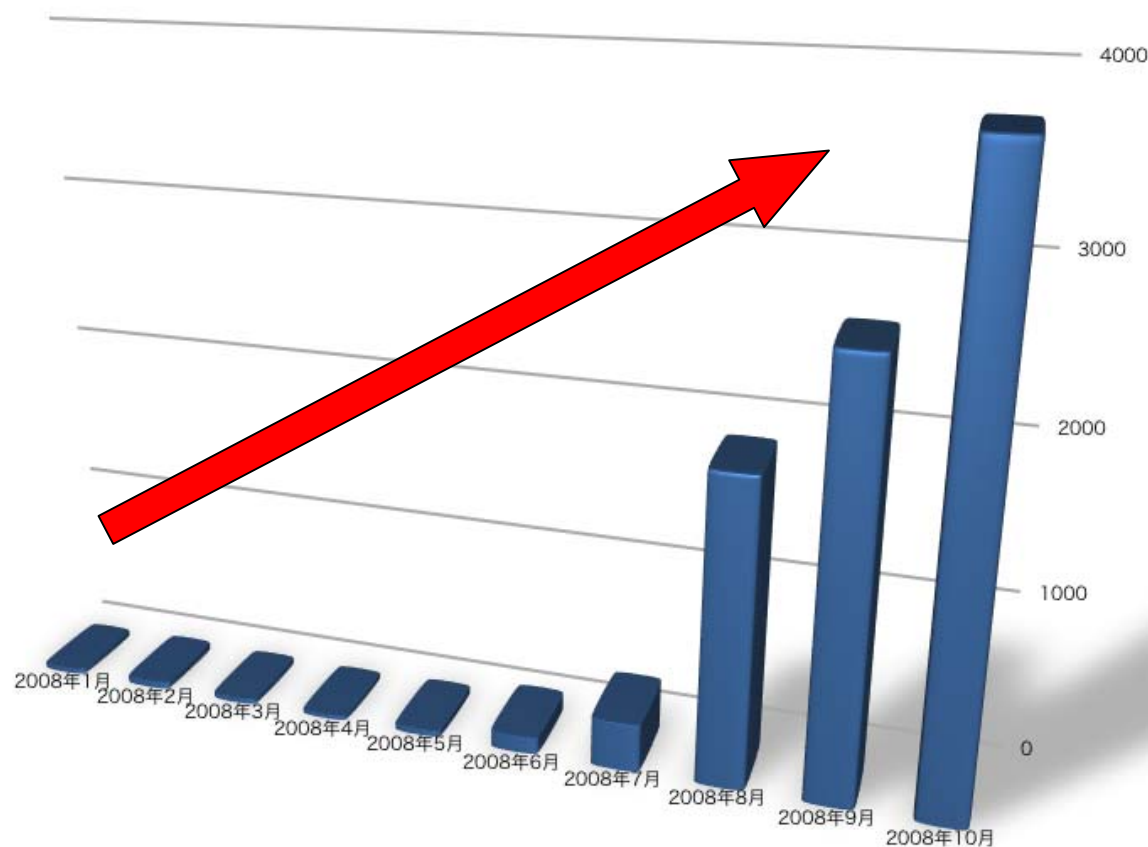


署名Web



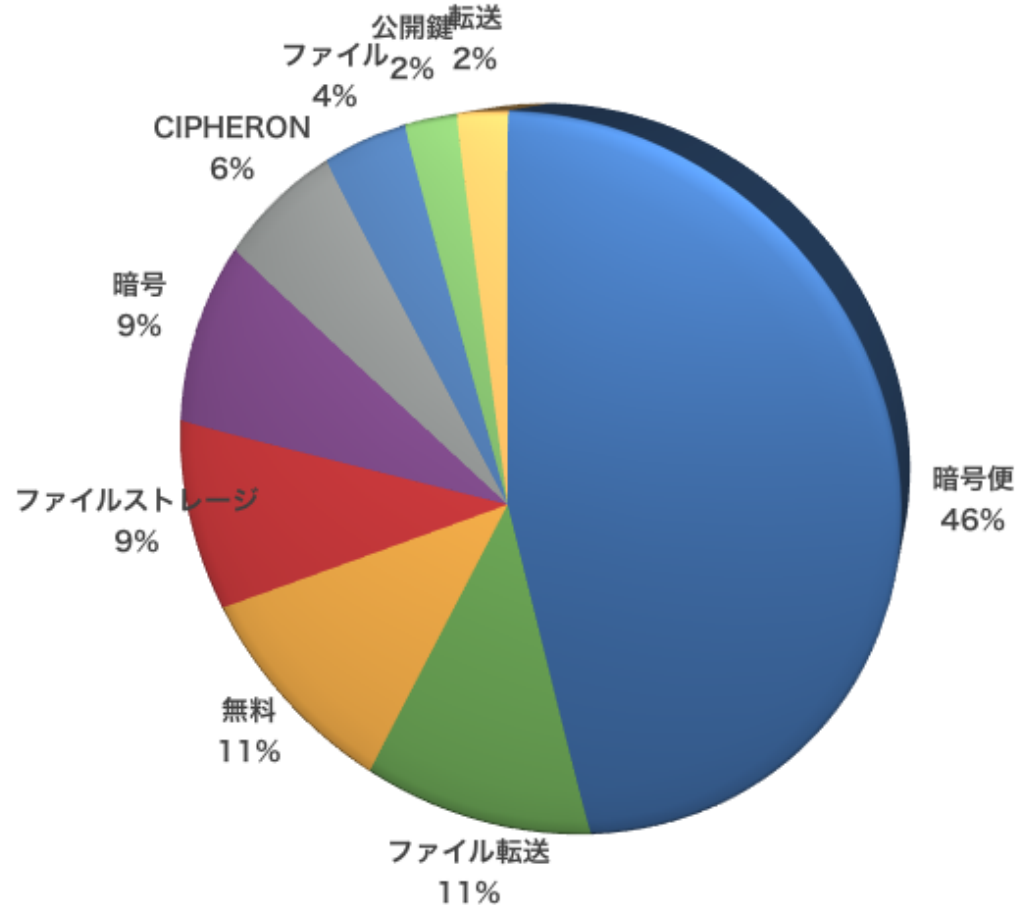
angobin.jp トラフィック遷移について

- 2008年8月よりトラフィックが急増中
 - 2008年1月と比較して2008年10月の月間トラフィックは、**約35倍**のトラフィック。



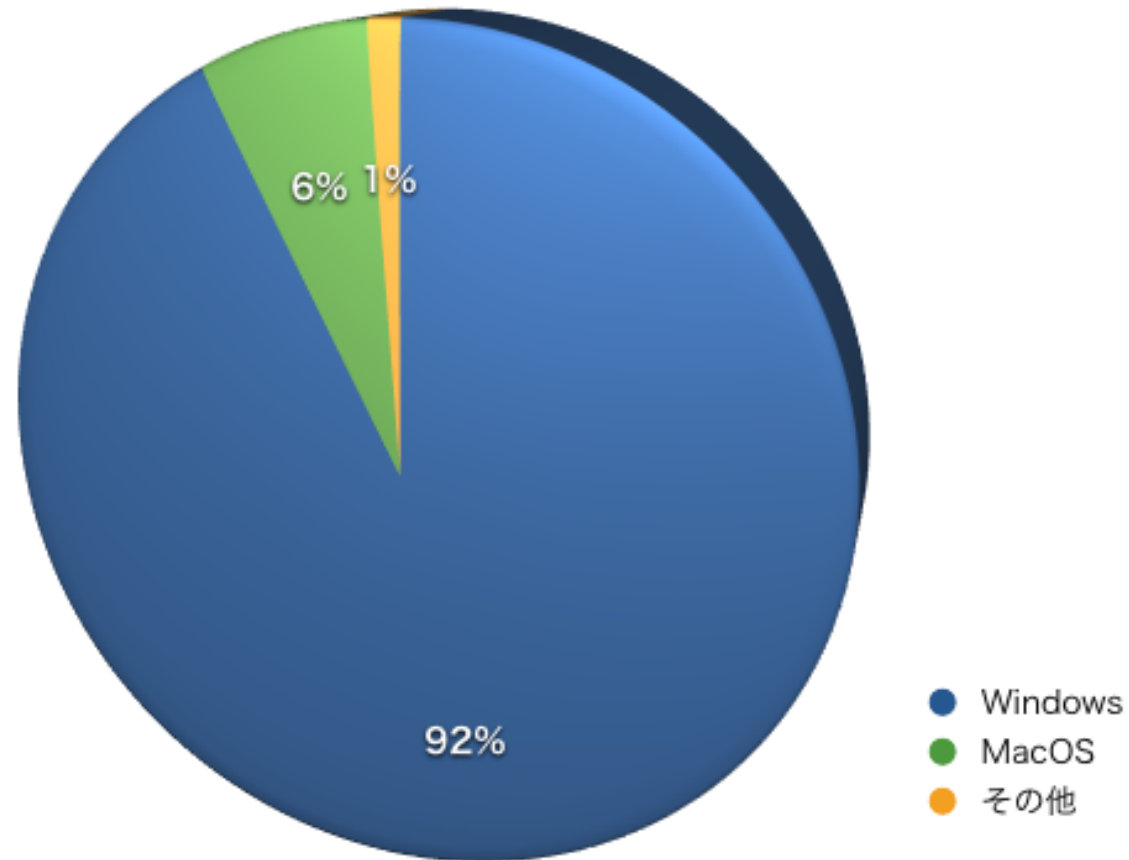
参照：検索エンジンでの検索ワード割合

- google, Yahoo!等の検索エンジンの検索結果から angobin.jp が開かれた際の検索キーワード統計

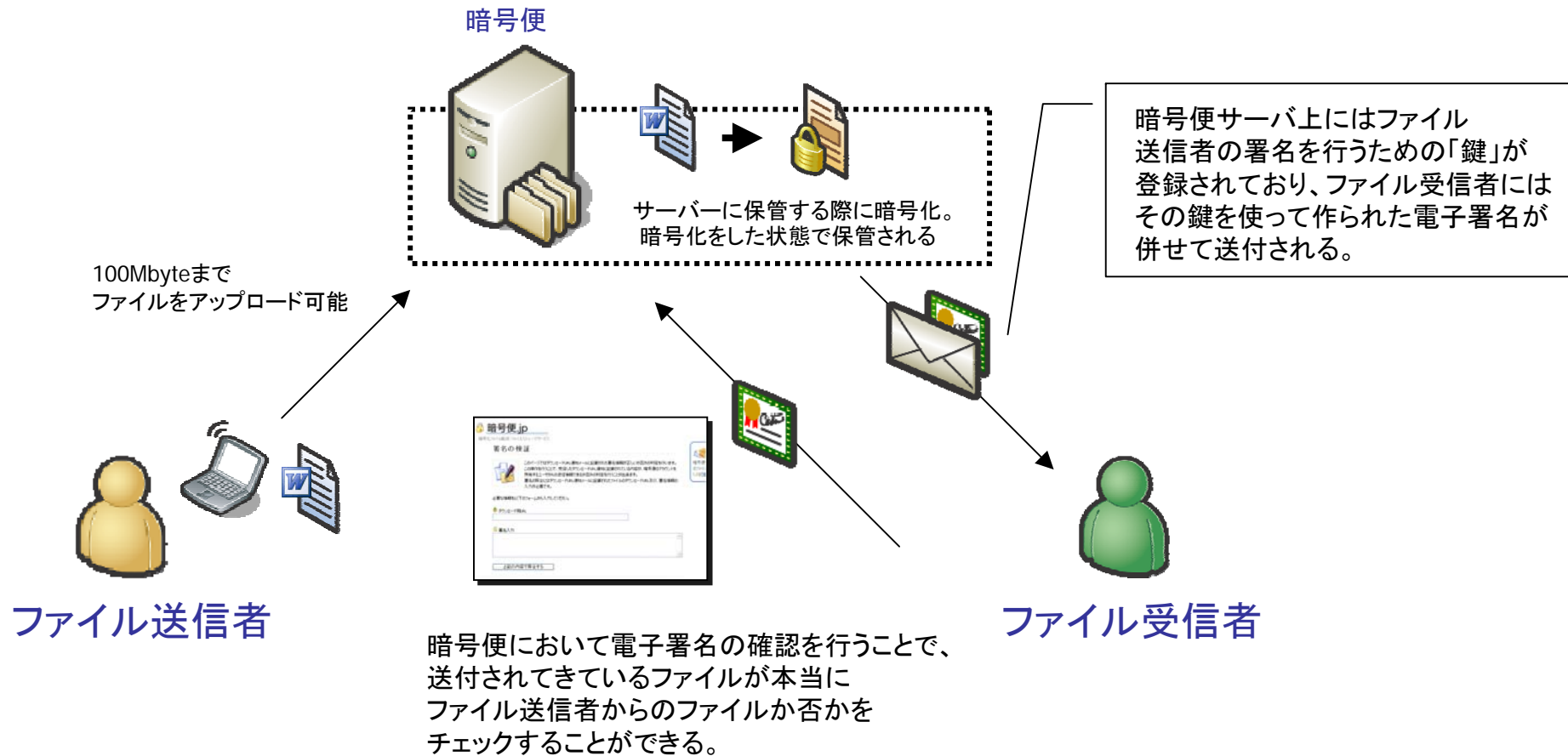


参照：利用OS種別

angobin.jp 利用OS統計

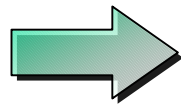


署名Webによる電子署名の確認によって行えること



署名Webを利用するまでの手順

- 電子署名入りのファイルを送信するユーザ
 - Step.1
 - 暗号便上で**電子署名用の鍵ペア(公開鍵、秘密鍵)**を**あらかじめ**作成しておく。
 - Step.2
 - 暗号便からファイルを作成した電子署名と**併せて**送付する。

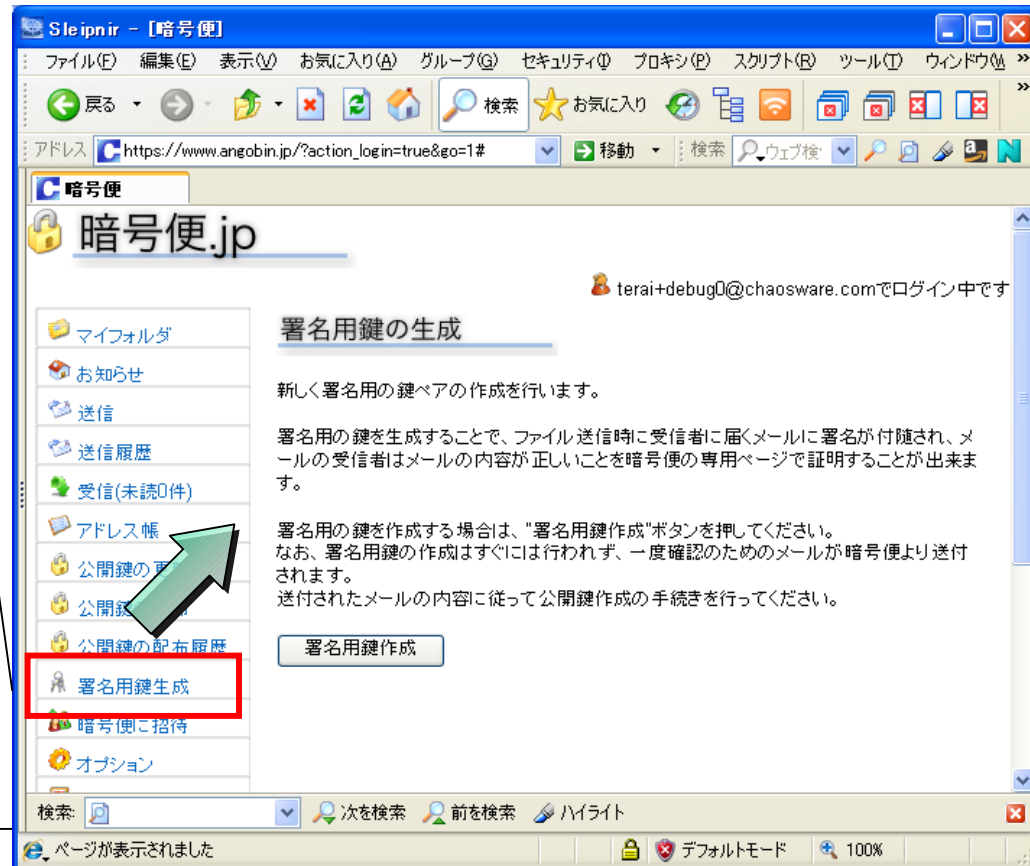


暗号便にアカウントを作成することで電子署名を付与したファイル送信が可能に。

署名Webの利用（ファイル送信までの手順）

- Step.1
 - 「暗号便上で電子署名を行うための鍵を作成する」(最初に一回必要)

鍵作成のメニューがWeb上に用意。そこから選択することで署名Web利用のための鍵ペアを作成することができる。



署名Webの利用（ファイル送信までの手順）

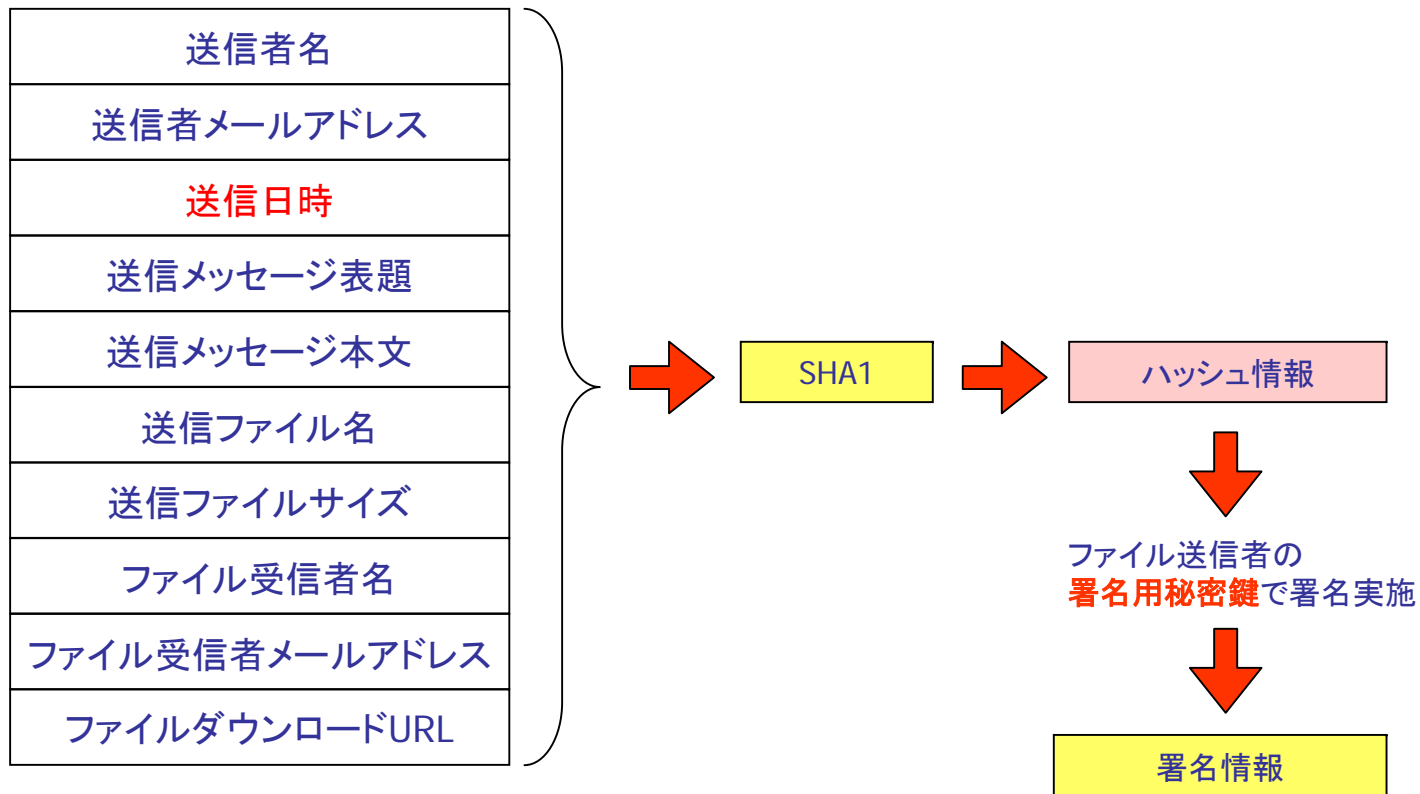
- Step.2
 - 「暗号便からファイルを電子署名入りで送付する」

The screenshot shows the 'Angbin' web interface in a browser window. The page title is '暗号便.jp'. The main content area is titled '暗号化方法の設定とメッセージの設定'. It includes sections for '暗号化を行う方法を設定してください。' (Set the encryption method), 'パスワードの設定' (Set the password), 'メッセージ' (Message), 'タイトル' (Title), and '本文' (Body). A red box highlights the '署名の設定' (Signature setting) section, which contains a checked checkbox '送信するファイルに署名を設定する' (Set signature for files to be sent) and a text input field. Below the input field are '戻る' (Back) and '次へ' (Next) buttons.

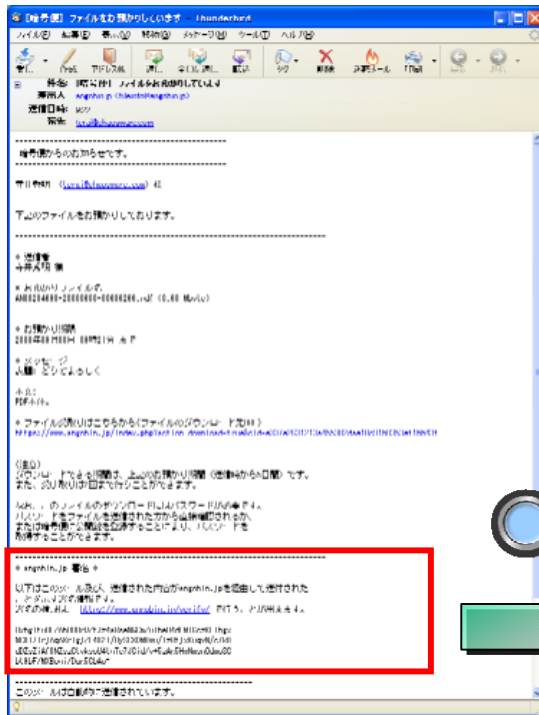
「送信するファイルに署名を設定する」に
チェックを入れた後、暗号便のログイン用の
パスワードを入力

電子署名の内容

- angobin.jpは以下の情報から署名を生成する



メールに付与される電子署名の例



～署名情報の例～

* angobin.jp 署名 *

以下はこのメール及び、送信された内容がangobin.jpを経由して送付されたことを示す署名情報です。

署名の検証は、<https://www.angobin.jp/verify/> で行うことができます。

joA55mZJzoJNI+eQTVIXQf5/xN+UJ3hQVj7p783sfedU8c+btN
+tg1v4ixXJGqoMSiS3MmADCJC51p5JNVWuXsrUdkFJSYs3MmE5
KmB1dNrLzoicU54KOldAOncIlgjGtK83FjqvxDlawuLtahQ51b
TYvTFGDOJPqxCqlc/Vf54=

送信完了時にQRコードでも署名情報表示

電子署名を加えたファイルの送信が完了した際に表示される画面

暗号便.jp

送信ファイルの選択

ファイルの送信が完了しました。

また、送信したファイルと併せて、以下の署名情報がファイル受信者へ送付されました。
ファイルの受信者は、署名情報を検証することで送信者の確認を行うことができます。

署名情報
e/uvsmsog4cgymbP1n4BVVvhQ4s6TwrIH5C+Lf4BPSXQg4t7oo lm7beLLjTxGqDleEa2wkSzRczulDfhJQRIPNPRTdobBxzVhIQI D3goNx5a0FbR0mc+mjSZvdQ4+Uq2Z17S+00Z1+84+8huh91kDZ AI6ld48g0GdPh6b6fCiXY=

署名情報QRコード

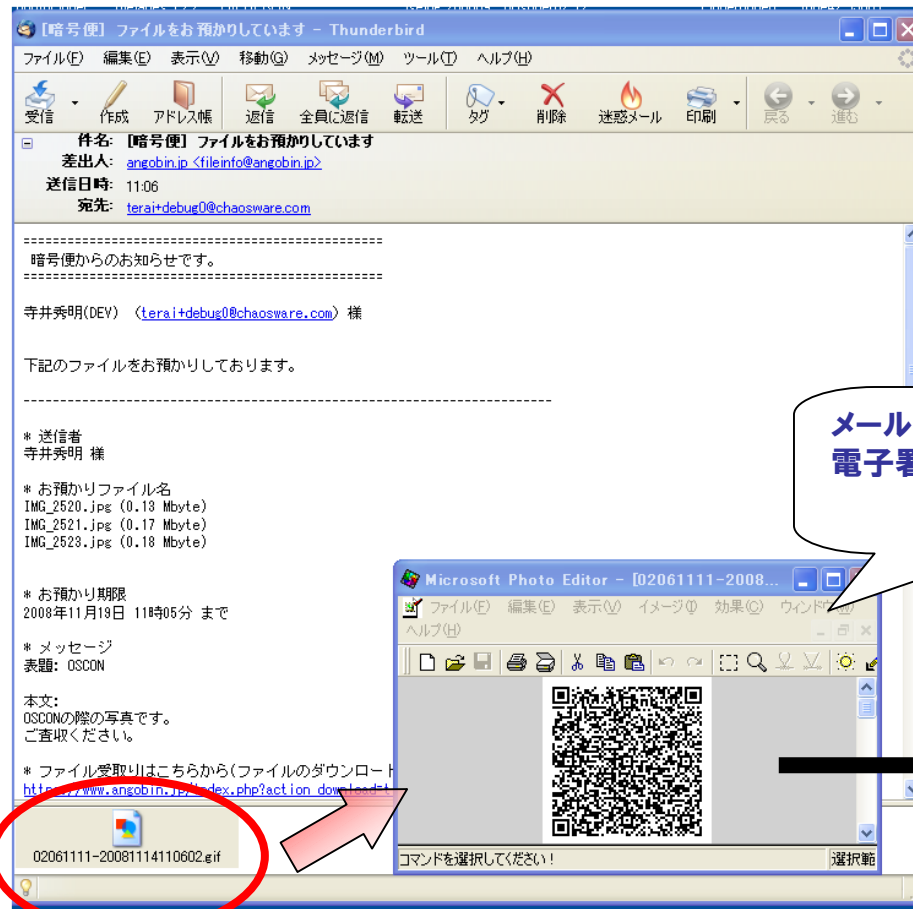

3個の鍵が受領待ちです。

文字列で表された
電子署名情報

QRコード化された
電子署名情報

QRコード化された電子署名はメールにも添付

電子署名入りのファイルが送付された際の通知メール



メールにQRコード化された
電子署名の情報も添付される



携帯電話で
読み取ることで
電子署名の検証も可能

署名検証用ページ

- <https://www.angobin.jp/verify/> で電子署名検証が可能

暗号便.jp

暗号化ファイル転送・ファイルストレージサービス


[トップページ](#) - [ログイン](#)


署名の検証



このページではダウンロードURL通知メールに記載された署名情報が正しいか否かの判定を行います。この操作を行うことで、受信したダウンロードURL通知に記載されている内容が、暗号便のアカウントを所有するユーザからの送信情報であるか否かの判定を行うことができます。署名の照合にはダウンロードURL通知メールに記載されたファイルのダウンロードURL及び、署名情報の入力が必要です。

必要な情報を以下のフォームから入力してください。

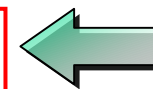
 ダウンロード用URL

 署名入力

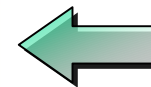


暗号便を利用してみませんか？

暗号便を利用するとメールで添付できない様な巨大サイズのファイルを暗号化して安全に送信できる様になります。詳しくは「[暗号便について](#)」をご覧ください。



ファイルダウンロードページのURLを入力

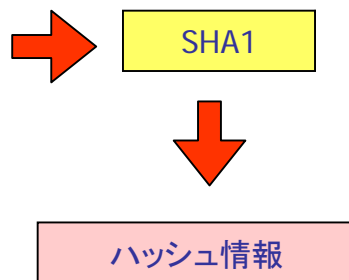


メールに記載の署名情報を入力

署名確認処理の内容

ダウンロードURLを検索の鍵として、
angobin.jp内のDBから抽出

送信者名
送信者メールアドレス
送信日時
送信メッセージ表題
送信メッセージ本文
送信ファイル名
送信ファイルサイズ
ファイル受信者名
ファイル受信者メールアドレス
ファイルダウンロードURL

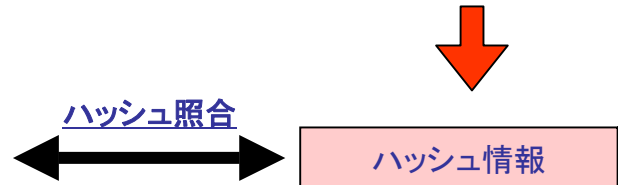


署名情報として渡された文字列

* 署名情報

```
ABUABQAAAPOACgAAAAMAFQAGAAAA/QAKAA  
AABAAVAACAAAD9AAoAAAAFABUACAAAAP0A  
CgABAAAAFOABAAAAvQAKAAEAQAWAAAwq  
0AWAACksEAWAADss0AWAAD4tkAWAAAEuk
```

ファイル送信者の
署名用公開鍵で署名チェック



ハッシュを照合し、一致すれば署名は正当。
異なれば、不当。

署名確認結果表示画面(検証成功の場合)

 **暗号便.jp** [トップページ](#) - [ログイン](#)

暗号化ファイル転送・ファイルストレージサービス

署名検証結果

署名確認成功

署名の検証に成功しました。
この署名が付与されたダウンロードURL通知メールは、暗号便によって以下の内容が証明されています。

項目	内容
送信日時	2008年9月3日 09時21分
ファイル送信者	寺井秀明 (terai@chaosware.com)
ファイル受信者	terai@chaosware.com
メッセージ表題	どうぞよろしく
メッセージ本文	PDF本体。
送信ファイル	AN00234698-20000600-00686266.pdf (640.2kb)

 [別の署名情報のチェックを行う](#)
 [暗号便トップページに戻る](#)

[会社概要](#) - [お問い合わせ](#) - [プレスリリース](#) - [関連資料](#) - [パートナー](#)
© Copyright 2007-2008 Chaosware Inc. All Rights Reserved.

 **暗号便を利用してみませんか？**
暗号便を利用するとメールで添付できない様な巨大サイズのファイルを暗号化して安全に送信できる様になります。詳しくは「[暗号便について](#)」をご覧ください。

署名によって確認された情報の一覧が表示される

署名確認結果表示画面(検証失敗の場合)



暗号便.jp
暗号化ファイル転送・ファイルストレージサービス

[トップページ](#) - [ログイン](#)

署名検証結果

署名確認失敗

署名の検証に失敗しました。
この署名が付与されたダウンロードURL通知メールの内容を暗号便が証明することはできませんでした。

[別の署名情報のチェックを行う](#)
[暗号便トップページに戻る](#)



暗号便を利用してみませんか？
暗号便を利用するとメールで添付できない様な巨大サイズのファイルを暗号化して安全に送信できるようになります。詳しくは「[暗号便について](#)」をご覧ください。

[会社概要](#) - [お問い合わせ](#) - [プレスリリース](#) - [関連資料](#) - [パートナー](#)
© Copyright 2007-2008 [Chaosware Inc.](#) All Rights Reserved.

まとめ

■ 署名Webシステムの応用

- 電子郵便局(証明付き、電子ファイル送信)。
 - 電子署名SNS(SNSのなりすましを防ぐ)
 - タイムスタンプ(参照:2007年InfoPro発表内容。
日本標準時との連動可能。)
 - 電子文書(アーカイブ)の真正性証明サービス
 - 時間制限付き有料コンテンツ配信(一定時刻が経過すると、**厳密にコンテンツを完全消去**)
-