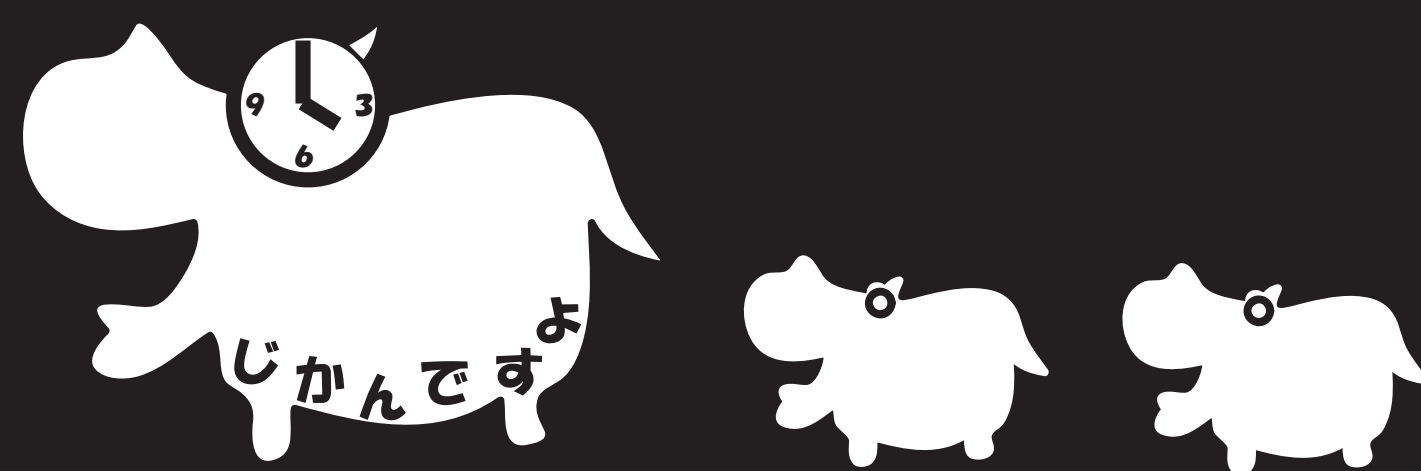


タイムカプセル署名

Time Capsule Signature



氏名	藤田 真可	野田坂 祥史	中西 真起子	伊藤 拓也
Name	Hujita Manaka	Nodasaka Shoji	Nakanishi Makiko	Ito Takuya

概要

- ・タイムカプセル署名とは、署名を受け取った人が指定された時刻にならないと検証できない署名方式こと。

デジタル署名

特徴

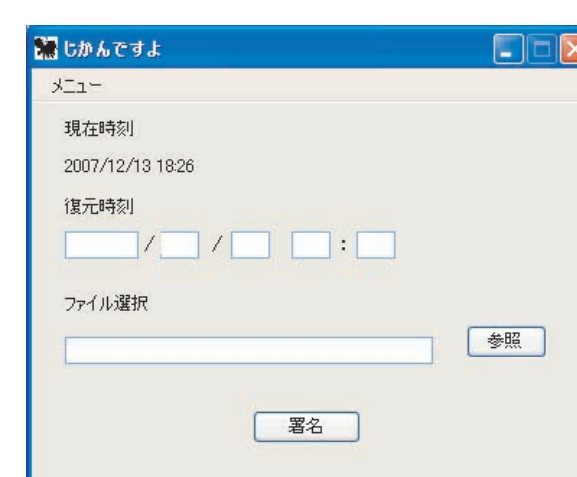
- ・署名する人は暗号化鍵を管理する必要がない。
- ・不特定多数への配信が従来のものより容易にすることが出来る。
- ・特定の時刻にならないと、誰も検証出来ない。

- ・デジタル文書が正しいかどうかを保障するために付けられる署名情報のこと。送信者はメッセージにデジタル署名を添付して送信する。受信者は、メッセージ本体から割り出した値と照合することで署名の検証を行う。

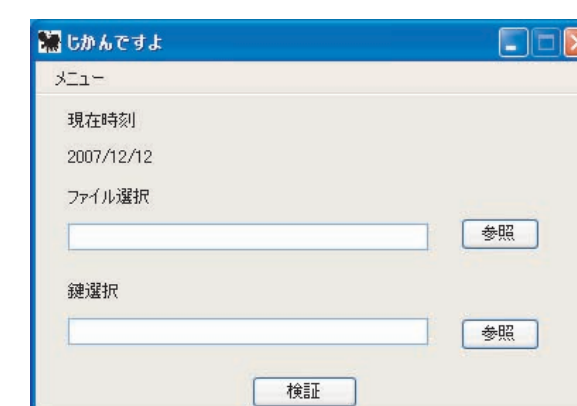
※デジタル署名は電子署名を実現するための方式の一つ。電子署名とは紙に署名する行為を電子的に代替したもののことを広く指す。

アプリケーションじかんですよ

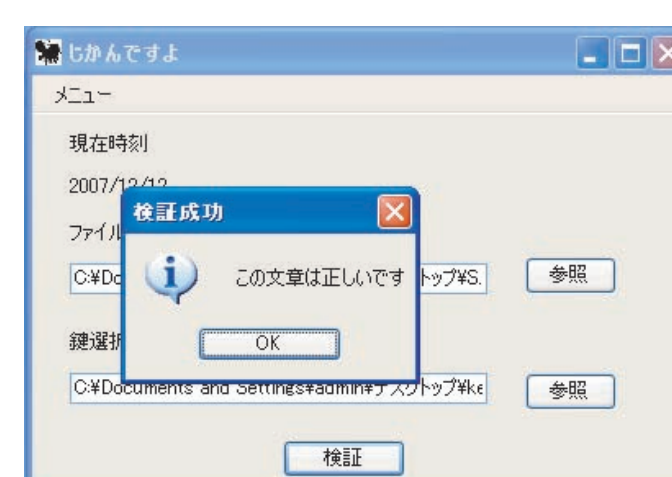
- ・検証可能時刻を指定し、署名と公開鍵を作成できる。
- ・署名と公開鍵を選択し、署名の検証を行える。その時、現在時刻と検証可能時刻との比較を行い、時刻が一致していれば検証することが出来る。



署名画面



検証画面



署名を行った時刻が、指定時刻であれば、署名を検証することが出来る。

応用例

- ・時刻情報にPC内蔵時計を使用しているので時報局に変更する。そうすることにより更なる安全性と公益性を確保できる。
- ・映画配信、銀行取引などへの利用。