明治大学総合数理学部

2016 年度

卒　業　研　究

PDF ファイル 1000 個を用いた Acrobat pro のユーザビリティ調査

学位請求者　先端メディアサイエンス学科

清水雄太

目次

１はじめに

１．１研究背景

インターネットワークで広く普及している情報媒体の一つにPDF(Portable Document Format)がある。アドビシステムズによって開発されたソフトウェア、ハードウェア、オペレーティングシステムに関係なく文書を確実に表示および交換するために使用されるファイル形式である。国際標準化機構で管理されているオープンスタンダードの一つになっており、様々な場面で利用されている[1]。Acrobat proには、PDFには文書の改ざんや作者のなりすましを防止するための電子署名がある。

１．２研究目的

PDFの電子署名、検証をすることにより現在のAcrobat proのユーザビリティを評価することを研究の目的とする。

２電子署名について

２．１電子署名とは

電子署名とは電子文書に対して行われる電磁的記録である。また「電子文書の作成者を示すために行われたものであること。」と「作成された電子文書に対する改ざんが行われていないことを確認できるものであること。」の二つの要件を満たしていることが必要となる。電子文書の長所は編集が容易であり、扱いが容易である点である。その反面、作成者が曖昧で改ざんの有無が明確でないという短所も仰せ持つ。電子署名とはこの短所を補うものであり、作成者を証明し、改ざんの有無を確認できるものである。

２．２公開鍵暗号の仕組み

電子署名では公開鍵暗号を利用している。公開鍵暗号は「秘密鍵A」と「公開鍵B」を作成し、「秘密鍵A」で平文を署名、「公開鍵B」で暗号文を検証する[2]。秘密鍵Aで署名した平文は、ペアとなっている公開鍵Bでしか検証できない仕組みとなっている。これは、署名を公開鍵Bで検証できた場合、秘密鍵Aで署名されたことを証明している。この秘密鍵Aが署名者の所有で署名者以外知らない情報という前提の下、署名者によって署名されたことが証明される（図１）。

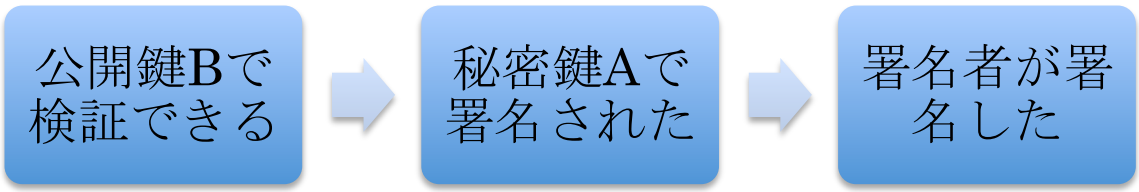

図１　公開鍵暗号の仕組み

この「秘密鍵 A がある署名者の所有で、署名者以外知らない情報」という前提を制度にしたものが公開鍵基盤（PKI）である。信頼できる第三者の認証局が署名者の本人確認を行い、署名者が提出した公開鍵 B に、ディジタル署名して、公開鍵証明書を発行する。公開鍵 B は電子証明書の中に含まれており、検証者は受け取った公開鍵 B を使用してファイルの証明書の有効性を確認する（図２）。

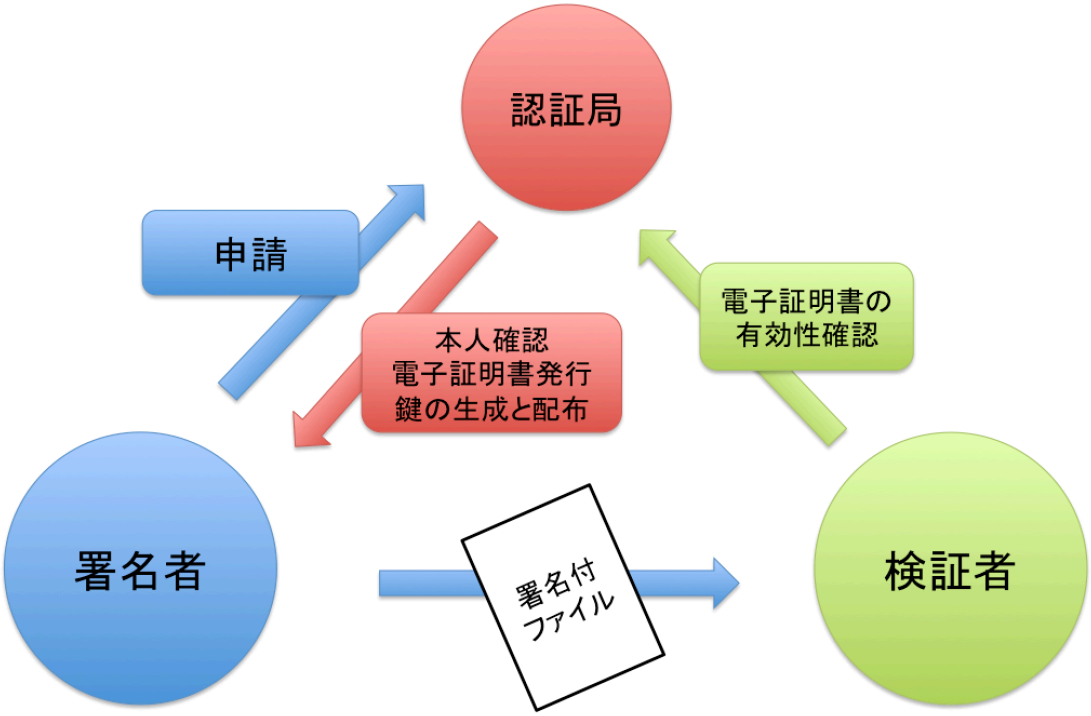

図２　電子証明の仕組み

２．３ハッシュ関数の利用

ハッシュ関数とは、あるデータが与えられた場合、データを固定長の数値に変換する関数である。代表的なハッシュ関数として、SHA-1、SHA-256 がある[3]。それぞれ 160 ビット、256 ビットの固定長の数値（英数字）に変換する。これによりあらゆる電子ファイルを小さな固定長の数値に変換することができる。また同じハッシュ値を持つ電子ファイルを意図的に作成することは難しく成りすまし、改ざんを防いでいる。

３Adobe Acrobat pro の操作方法

３．１署名

３．１．１署名の手順

電子署名の手順を説明する。PDF ファイルを Adobe Acrobat Pro で開き、右上の「入力と署名」を選択する（図３）。署名をする場所、範囲をドラッグで指定する。電子署名タグの中の「証明書を使用して署名」を選択する（図４）。「署名に使用する ID」一覧の中から「新規 ID」を選択し、「今すぐデジタル ID を新規作成」を選択する。デジタル ID 情報（名前、部署、会社名、メールアドレス）を入力する（図５）。デジタル ID ファイルの保存場所とパスワードを入力する（図６）。設定したパスワードを入力し、署名を完了させる。

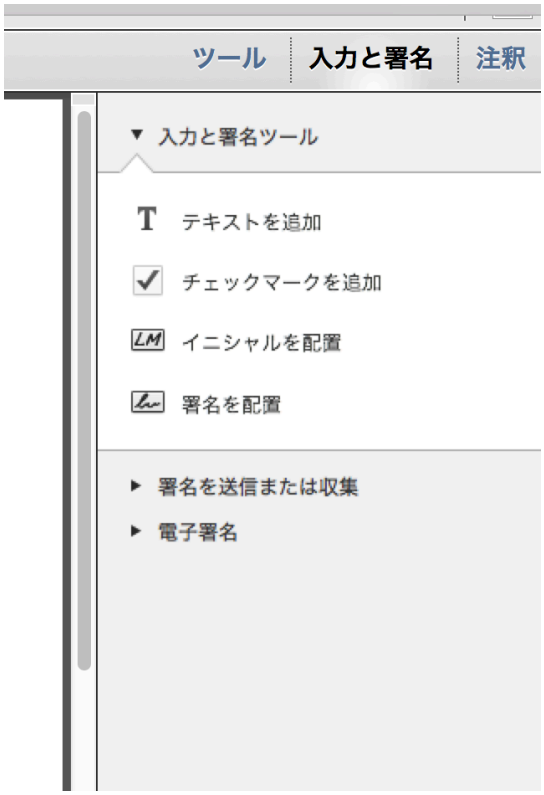

図 3 Acrobat の「入力と署名」ツール実行例

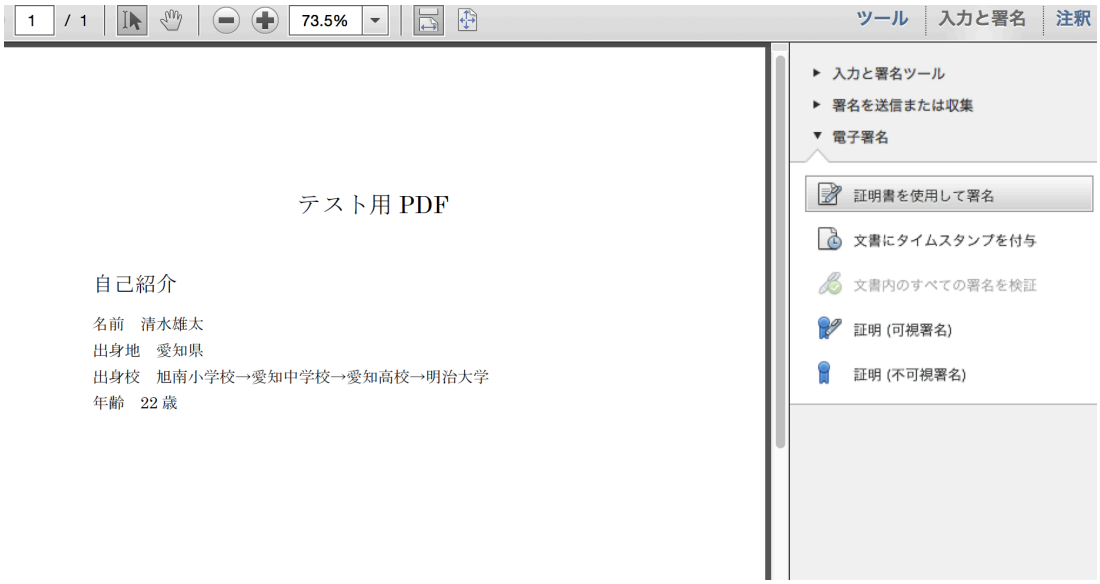

図 4 Acrobat の「入力と署名」ツール電子署名選択実行例

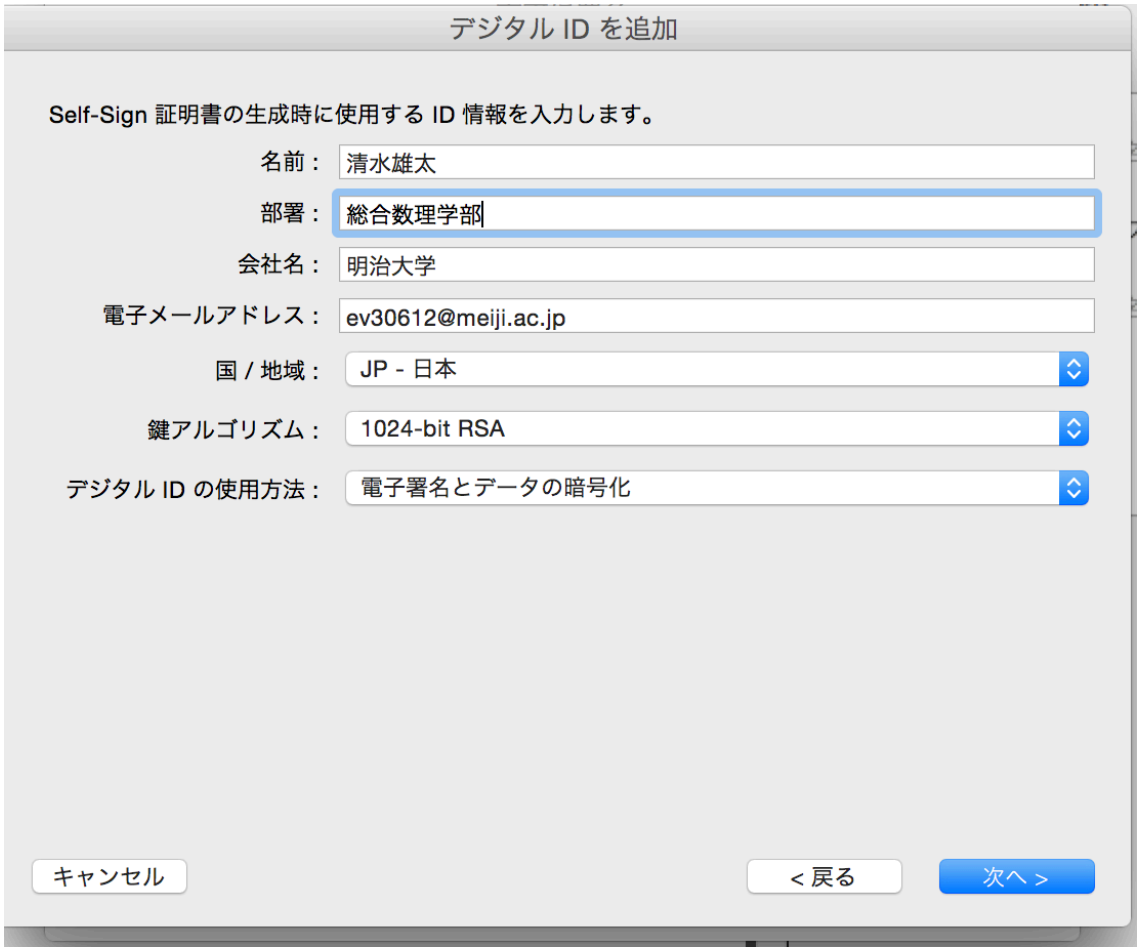

図 5 Acrobat の「デジタル ID」情報入力実行例

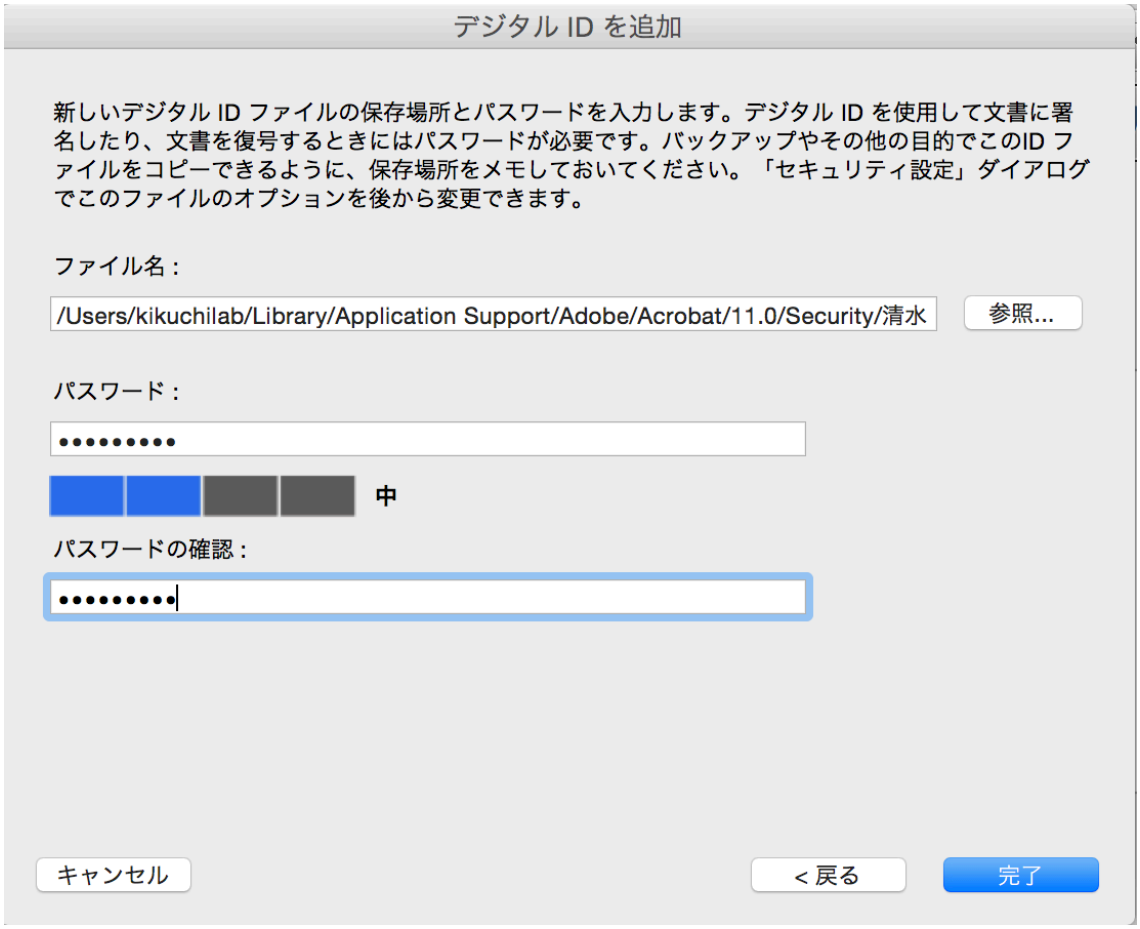

図 6 Acrobat の「デジタル ID を追加」パスワード設定実行例

３．１．２ユーザビリティ評価

特に不可解な点がなく、使用感がよく、署名初心者も手軽に扱えると感じた。署名の大きさと位置をポインタのドラッグで指定できる点が非常に便利であった。

３．２署名検証

３．２．１署名の手順

署名検証の手順を説明する。「署名パネル」から「署名のプロパティを表示…」を選択する（図７）。また、同時に、署名の正当性が確認できる（図８）。電子署名が施されていない場合、「署名パネル」が表示されない。「署名者の証明を表示…」を選択することで、発行者、証明書の有効期間の開始/終了を表示できる。

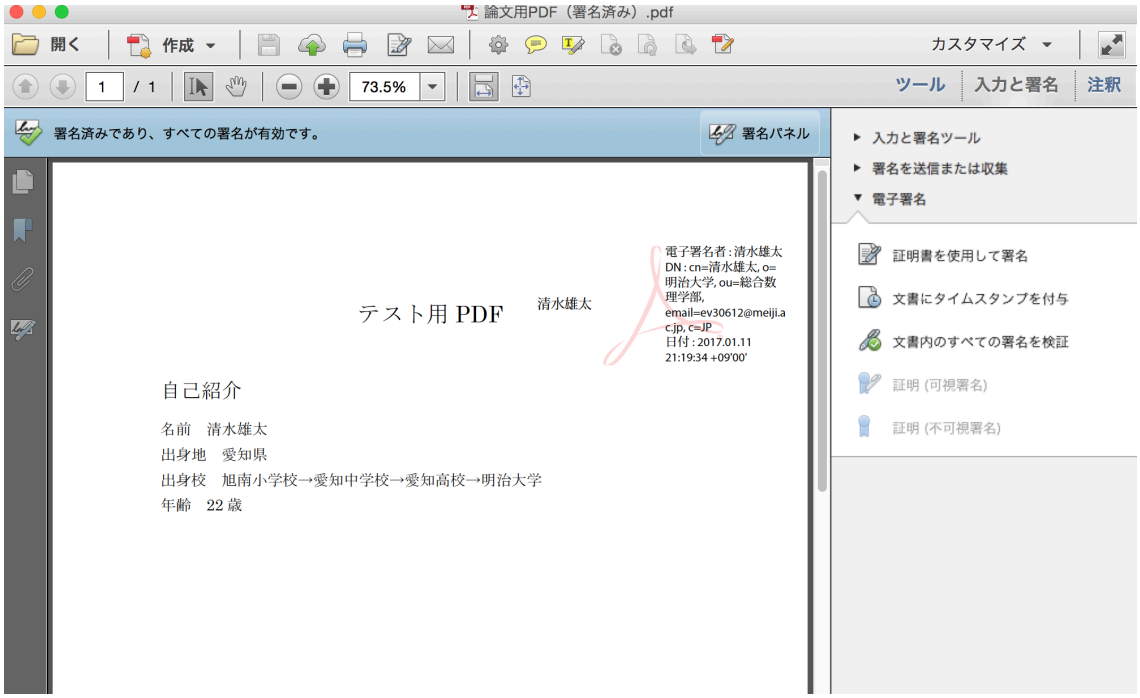
論文用PDF（署名済み）.pdf
開く
作成
カスタマイズ
1 / 1
73.5%
ツール
入力と署名
注釈
署名済みであり、すべての署名が有効です。
署名パネル
入力と署名ツール
署名を送信または収集
電子署名
証明書を使用して署名
文書にタイムスタンプを付与
文書内のすべての署名を検証
証明 (可視署名)
証明 (不可視署名)
テスト用 PDF
清水雄太
電子署名者：清水雄太
DN：cn=清水雄太, o=明治大学, ou=総合数理学部, email=ev30612@meiji.ac.jp, c=JP
日付：2017.01.11 21:19:34 +09'00'
自己紹介
名前　清水雄太
出身地　愛知県
出身校　旭南小学校→愛知中学校→愛知高校→明治大学
年齢　22 歳

図 7

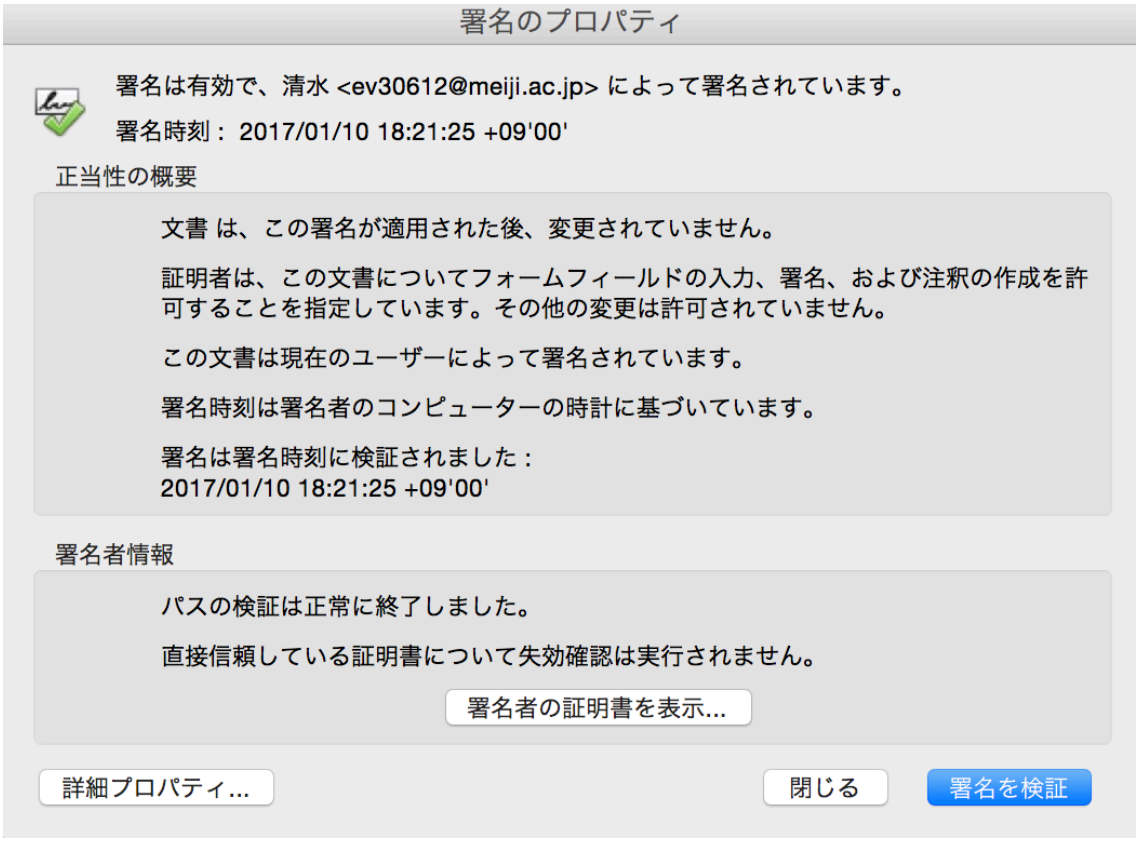

図 8 署名検証実行例

３．２．２ユーザビリティ評価

PDF50 個に 1 度くらい頻度で、アプリケーションが強制終了するという欠点が見つかった。また、電子署名が施されている PDF を開く際に、7〜9 秒ほどの処理時間がかかることが明らかになった。

４調査実験

４．１調査内容

４．１．１調査項目

インターネットから抽出した PDF1000 個に対し、電子署名の有無、PDF の詳細（表１）を調査し、その操作にかかる時間を計測した。また、電子署名が施されている PDF に関しては署名の詳細（表２）を調査した。

表１　PDF の基本情報例

調査項目	平均	値の例
ファイル名		P20140409.pdf
ページ数	26	17
ファイル長[Kbyte]	1479.526	7546.802
所要時間	16.7	12.16

表２　電子署名の詳細

調査項目	値の例	最頻値
バージョン	3	3
署名アルゴリズム	SHA1	SHA256
Cn	ApplicationCA2	ApplicationCA2
Ou	Sub GPKI	Sub GPKI
O	JapaneseGoverment	
C	JP	

４．１．２PDF1000 個の選出方法

グーグル検索でワードクエリを「官公庁」、ファイルタイプを PDF に指定したもの 1000 個を選出した。

４．２調査環境

調査環境を以下の表３に示す。

表３　調査環境

使用したPC	MacBook Pro
使用したアプリケーション	Adobe Acrobat XI pro

４．３調査結果

抽出したPDF1000個の内、電子署名が施されていたPDFは79個であった（7.9%）。また署名のバージョンは全て3であった。署名アルゴリズムの比率を表４に示す。

表４　アルゴリズムの種類と個数

	SHA256	SHA1	計
PDF（個）	65	14	79

表５　署名アルゴリズムとcn、ouの関連

署名アルゴリズム	cn	ou
SHA256	ApplicationCA2Sub	GPKI
SHA1	N/A	OfficialStatusCA

電子署名の有無についてのPDFファイルの平均ページ数、平均ファイル長を表６に示す。

表６PDFファイルの平均ページ数、平均ファイル長

	電子署名あり	電子署名なし
平均ページ数	23.8	26.5
平均ファイル長[Kbyte]	1402.633	1479.526
平均処理時間	49.8	13.9
PDFの個数	79	921

PDFファイルの署名検証調査にかかった時間の分布を図9に示す。横軸がPDFの番号、縦軸が署名検証処理時間（秒）である。赤色が署名ありのPDF、青色が署名なしのPDFのデータである。検証を重ねる度に、処理時間が短くなっている。この結果はAcrobatの利便性を顕著に表していると考察した。署名ありのPDFの場合、読み込みに時間がかかるため署名なしのPDFと比べて大きな処理時間の差が見られた。

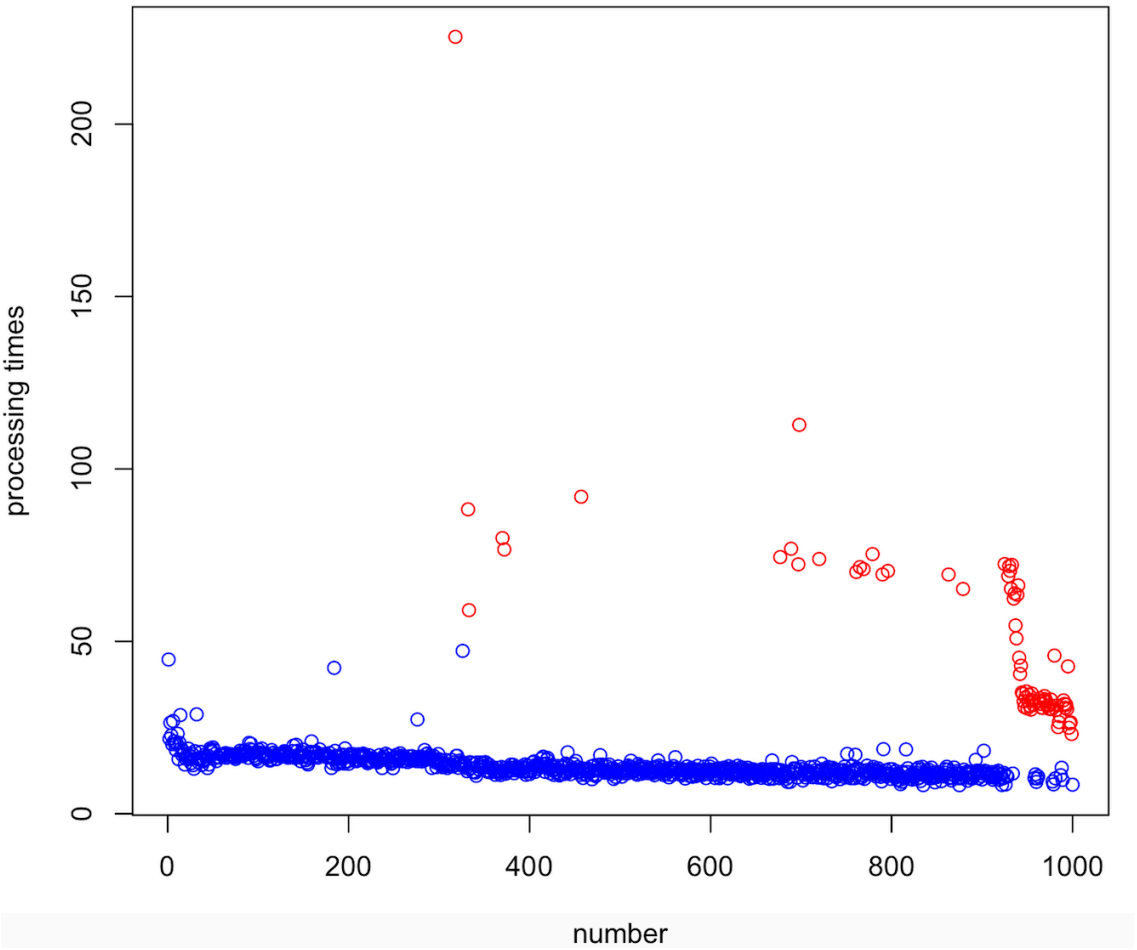

図 9 1000 個の検証時間の分布

５おわりに

調査により電子署名が施されている PDF が意外と少ないことが明らかになった。電子署名率が 7.9%と低かった原因として、政府が重要視していない原因が考えられる。電子署名を施し、信頼性を上げるべきである。

参考文献

[1]Adobe Acrobat DC(https://acrobat.adobe.com/jp/ja/why-adobe/about-adobe-pdf.html)

[2]NS Solutions その７「電子署名のしくみと機能～本人証明と非改ざん証明～」(http://www.nsxpres.com/e-contract/10hints/hint07-2.html)

[3]IT 用語辞典　e-Words(http://e-words.jp/w/SHA-256.html)