2006－CSEC－35（11）
2006／12／8

電子署名複写を用いた紙文書へのトレーサビリティの実現

重里豪太　宇田隆哉

東京工科大学　コンピュータサイエンス学部　〒192-0982　東京都八王子市片倉町1404-1

2001年1月以降、「全ての国民が情報通信技術を活用し、そのメリットを最大限に享受できる社会の実現」を目標に発表された「e-Japan」戦略を始めとし、さまざまなIT利活用のための方策が進められている。そして、その一つである「e-Japan戦略Ⅱ加速化パッケージ」の中で、民間企業に紙での保存が義務付けられている財務や税務関連の書類・帳票を、電子データとして保存することを認める法律である「e-文書法【電子文書法】」が重点分野の一つとして2005年4月1日から施行され、電子データの流通が盛んになっている。しかし、未だに紙による文書の保存は各組織において行われており、紙文書へのセキュリティ技術は非常に重要であると考えられる。デジタルデバイド解消のために、本研究ではユーザーにソフトウェアを使用させることなく、電子署名を紙面に埋め込むことで紙文書に対するトレーサビリティの実現を目指している。

Approach to traceability of paper document copied with e-signature

Gota Jury　Ryuya Uda

Graduate School of Computer, Tokyo University of Technology
1404-1 Katakuracho,Hachioji,Tokyo,192-0982 Japan

Since January, 2001, various programs for applying information technology have been worked on. One of the aims is "Realization of the society where the whole nation enjoys benefit by using information technology". It is called "E-Japan Strategy". On April 1, 2005, the law of "E-Document Method" was enforced. Financial and tax documents have been allowed to be preserved in electronic data as well as in paper. As a result, the circulation of electronic data became popular. However, many documents are still preserved in paper. Therefore, security in the management of the paper documents is still important. The objective of this study is realization of traceability of paper documents by embedding electronic signature in the surface of the paper as a dot pattern. Moreover, operation of the system is free from using pc so that the problem of the digital divide will be resolved.

1. はじめに

2001年1月以降、「全ての国民が情報通信技術を活用し、そのメリットを最大限に享受できる社会の実現」を目標に発表された「e-Japan」戦略を始めとし、さまざまなIT利活用のための方策が進められている。そして、その一つである「e-Japan戦略Ⅱ加速化パッケージ」の中で、民間企業に紙での保存が義務付けられている財務や税務関連の書類・帳票を、電子データとして保存することを認める法律である「e-文書法【電子文書法】」が重点分野の一つとして、2005年4月1日から施行された[1]。これにより、セキュリティ面でどうしても難のある紙の文書を、セキュリティ技術の充実した電子文書で保存することが可能となり、安全性・信頼性が大幅に向上することに繋がった。しかしながら、未だにセキュリティが充分とは言えない印鑑による認証や、紙による文書の保存を行っているのが現状である。

そこで本稿では、紙文書に対する既存のセキュリティ技術を解説し、その問題点を指摘するとともに、より安全性および利便性の高い紙文書管理を実現する新規手法を示す。

2. 従来技術

2.1 紙文書に対するセキュリティ技術

情報技術が向上するにつれて、あらゆるものの電子化が推進されている。しかしそのような流れの中でも、未だ様々な組織で紙文書に対するセキュリティ技術の研究は行われている。紙文書で保存をするメリット、電子文書として保存をするデメリットが共に存在する以上完全な文書電子化が困難である。そのため紙文書の需要は未だ非常に高く、紙文書に対するセキュリティ技術の考察[2]として研究報告が存在するほどである。以上より、紙文書へのセキュリティは現在非常に重要視されている項目の一つである事は間違いない。現在までに研究されてきたセキュリティ技術の例を以下に挙げる。

文書背景に直接文字を浮かび上がらせる手法としては、社外秘などの文字を直接背景に印字する「背景文字」や文書が複写された際に複写物の背景に無効などの文字を浮かばせる「複写牽制文字」[3]などの技術がある。これらの技術は埋め込まれた情報を目視することができるため、埋め込む情報によって注意喚起の効果などを得ることができる。さらにプリンタドライバソフトに基本機能として搭載されているため、汎用性も高い。

直接印字に対して、情報を電子的に埋め込むことで、部外者への情報漏えいを防ぐ手法がある。これらは大きく 2 種類に分けることができる。1 つは埋め込み事実が目視できるが、埋め込み内容は理解し難い方式。もう 1 つは埋め込み事実自体を視認し難くする方式である。目視できる電子透かしの代表として、文書の背景部分に微小ドットパターンを描くことで、その配置によって情報を抽出する技術[4][5]が挙げられる。見えない電子透かしの例としては、文書に含まれる文字のフォントや図形の位置、形などの情報をわずかに変化させることにより、電子情報を埋め込む技術[6][7]がある。その他特殊なものとして、文書の白紙領域に二次元バーコードと呼ばれる、デジタル情報を格納した画像を埋め込むことにより、紙文書に情報を付加する技術[8]などがある。これらの技術は埋め込まれた情報を容易に抽出することができないため、紙文書におけるセキュリティ技術の基盤となっている。

2.2 問題点

各研究に対する問題点、今後の課題の詳細については上述の紙文書に対するセキュリティ技術の考察[1]に示されている。そこで本研究では上記研究報告で指摘されていなかった点を新たな問題点として提起し、その問題点において特化したセキュリティシステムを提案する。

従来研究されてきたほぼ全ての技術は各々の指定した印刷用アプリケーションを中継した利用方法が主である。企業には PC の利用が得意ではない者も少なからず存在し、特にこのような文書の印刷・コピーを行う業務は大抵が PC などの知識を必要としない、事務担当やアルバイトの人間である。そのような利用者にこれらのソフトウェアの利活用を求めるのは困難である。

さらに従来技術の場合、既に印刷されてしまっている文書や手書きの文書などに署名を付加するためには、一度スキャナなどを利用して PC 内に取り込む作業を必要とするため、作業効率の低下が懸念される。

2.3 解決案

本稿では、上述の問題点解決案として、従来の透かし技術のアルゴリズムを参考とし、使いやすさ・効率の良さという点を重視した紙文書へのトレーサビリティ実現手法を提案する。本システムでは、署名に微小ドットパターンを用いることにより、外部の人間に文書が渡っても、その署名内容が認知できず、さらに流出元の特定を可能とすることで、二次被害を防ぐための業務システムの一部としても活用できるものを目指す。さらに実際に文書に署名を付加する作業ではソフトウェアを一切必要とせず、PC 作業を不得意とするユーザーでも容易に利用できるインタフェースを作成する。

3. 電子署名付き紙面複写システム

3.1 想定環境

本システムは主として、内部での利用を目的とする文書の保存を紙文書にて行っている組織において、文書の印刷・複製の作業担当として PC 関係の知識に乏しい者が割り当てられている環境を想定している。しかし、それら以外の環境においても、既存文書の電子化作業などを省くことが可能となるため、作業効率化の一環としても取り入れることができると考えている。

3.2 システム概要

本システムでは、マスターとなる電子署名シートの発行・管理と、電子署名シート複写による文書への署名付加の作業を完全に分別している。これにより、署名付加を施すユーザーが高度なソフトウェアの利用知識を必要とせず、負担の軽減へとつなぐことができる。本システムの概要を図 1 に示す。

まず電子署名シートの発行責任者が、OHP フィルムなどの透明印刷媒体に署名画像を印刷する。作成した署名画像には検証に必要なデータが格納されており、これらは専門部署で一元的に管理される。ここまでが署名シートの発行・管理までの流れである。

次に署名付加作業者側の流れである。印刷利用者は管理元より署名フィルムを借り出し、署名を添付する文書と重ねてコピーすることで印刷文書に署名画像を埋め込む。直前に通常印刷された文書・既存文書共に、システムの利用方法は同じである。

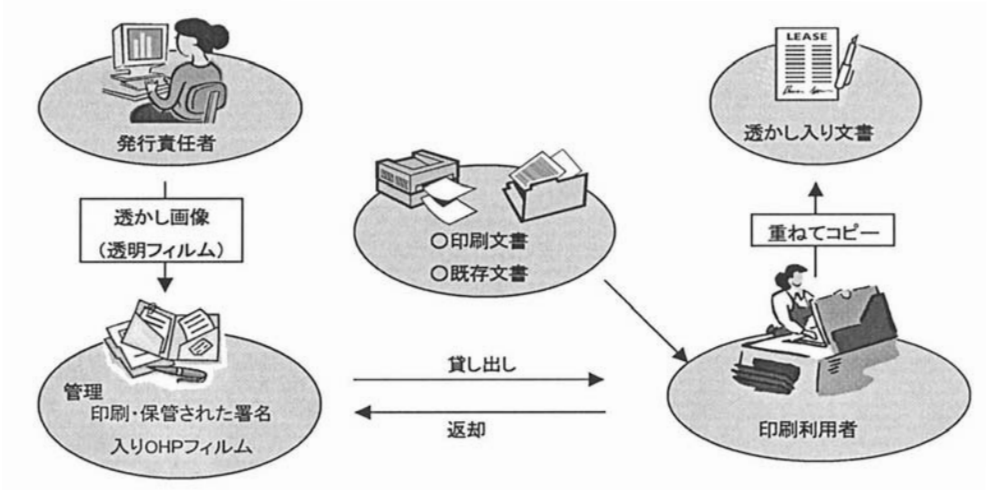

図 1　システムの概要図

3.3　2値ドットパターンの構成

n×n画素の2値ドットパターン1つを1ブロックとし、ブロックの集合を1つの署名として構成する。各ブロックには 1bitの情報（0or1）を持ち、埋め込む情報により並べて配置される。各ブロックは情報毎に異なるドット数で出力し、ランダムな濃淡を持たせることで変化させる。これにより情報判別の際は各ブロックあたりの疎密度を用いる。0 出力時に打ち込まれるドット数をN_1、1 出力時に打ち込まれるドット数をN_2、比較変数をCとしたときの比較変数の決定方法を式（1）に示す。ただし画像をAD変換する際の誤差を考え、$N_2 - N_1 \geqq 20$ とする

$$C = \frac{(N_2 + N_1)}{2} \tag{1}$$

これにより得られた C の値を画像読み取り時の01判別の際に比較変数として用いる。本稿では画像読み取り時の各ブロックのドット数をSとしたとき、判別式を式（2）とする。

$$\begin{cases} S > C : 1 \\ S < C : 0 \end{cases} \tag{2}$$

以上より抽出した情報を順に並べることにより、2進数で表記された署名データを得られる。現在は10×10画素で検証を行っている。この場合各ブロックに100pixelの要素が格納されているため、ブロック毎において冗長性を持たせることが可能となっており、検証率は非常に高い。利用環境に合わせて、画素数を変化させることで冗長性を変動させることができる、冗長性可変性能を有している。以下の図2,3にドットパターンの例を示す。これらのドットパターンには共に「01234567890123456789」の同じ数字列が格納されており、4bit の 2 進数に変換されたのちそれぞれのポイント数でドットを打ち込んでいる。そのため濃部分と淡部分の割合が近似しているのが分かる。ドットパターン作成時のポイント座標は完全ランダムであるため、全く同じ画像が出来上がる可能性は極めて低い。

図 2　10×10 , 0:40 , 1:60 でポイントしたドットパターン

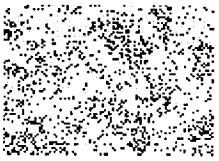

図 3　10×10 , 0:10 , 1:30 でポイントしたドットパターン

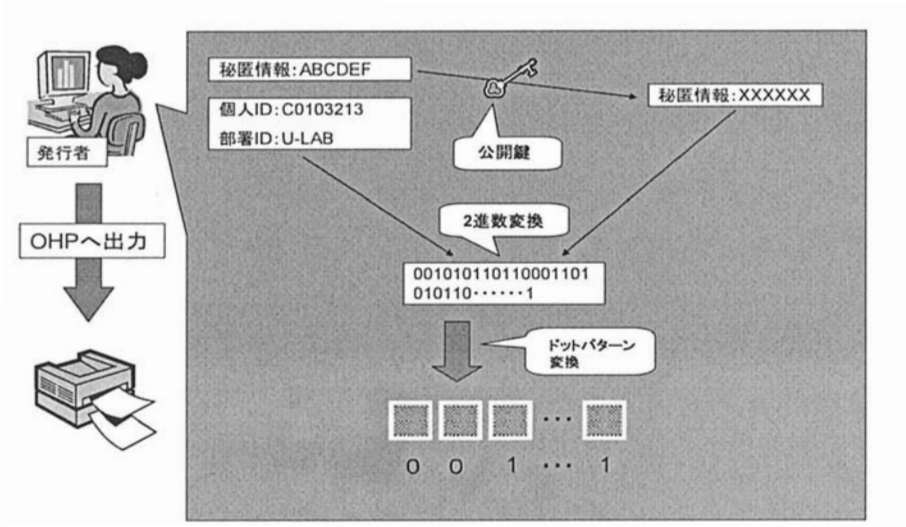

図 4　署名シートの作成

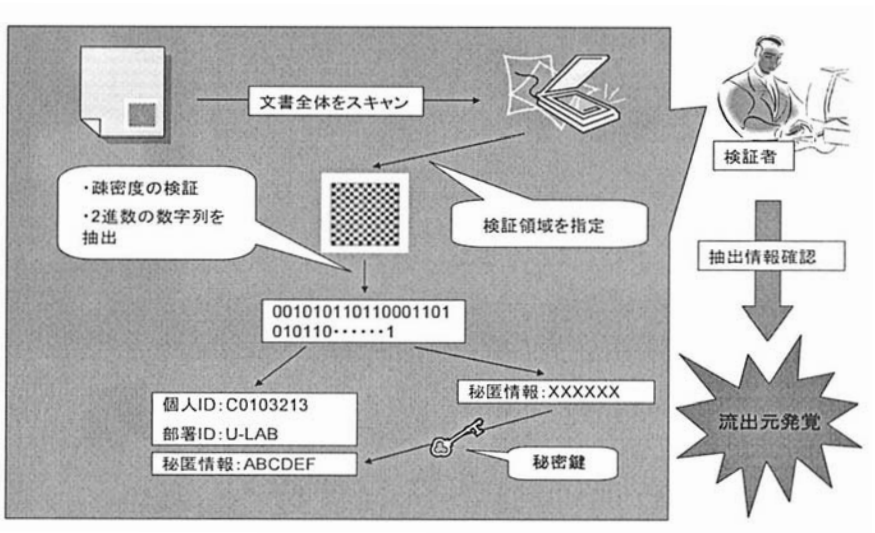

図 5　署名の検証

3.4　署名埋め込み処理

本システムでは、署名として付加する情報に、発行責任者を表す個人 ID、発行元を表す部署 ID のような公開されても良い情報に加え、関係者以外に公開されるべきではない秘匿情報を用いている。個人 ID、部署 ID は直接 2 進数変換を行うが、秘匿情報は一度公開鍵暗号方式を用いて暗号化し、その後 2 進数変換を行い、署名として付加する。実装では暗号方式に ECDSA を用いている。現在、一般的に用いられている RSA に比べ、ECDSA は短い鍵長で RSA と同等の安全性があるとされており、本システムのように埋め込むデータ量がある程度制限されているシーンでの利用に適しているため採用した。上記処理については、PC の利用に長けた専門のユーザーが行うことを想定しており、署名シートの取り扱いについても同ユーザーもしくは専門の部署が一元的に管理する。ただし、この一連の作業は自動化が容易であり、一度設定すればワンボタンで実行可能である。図 4 に署名シート作成までの流れを示す。

まず、格納するデータとして各 ID と秘匿情報を入力する。秘匿情報のみ検証者の秘密鍵と対になる公開鍵で暗号化され、各 ID と共に 2 進数の数字列に変換する。以上により生成された数字列を 1bit 毎にドットパターンへ変換し、署名画像を作製する。

3.5 署名抽出処理

署名の抽出には、上述の疎密度検証を用いる。図5に署名検証から流出元確認までの流れを示す。

まず文書全体をスキャンした後、署名画像が分布されている領域を指定し、n×n 画素のブロック毎に検証を行う。検証され生成された2進数の数字列は、署名埋め込み時の処理とは逆の変換を行い、各 ID と暗号化された秘匿情報を抽出する。秘匿情報は検証者が持つ秘密鍵により復号される。検証者以外は秘密鍵を所持していないため、秘匿情報を確認することはできない。以上の流れにより安全な情報伝達が確立される。

現在は読み取り時のずれ補正を行っていないが、ブロック読み取り時に発生する軸ずれによる検証領域のずれなども考慮し、幾何学補正用マーカーの配置や、パターン配置を偏らせるなどの手法を検討している。

3.6 優位性

本システムの最重要提案項目として挙げられるのが、この電子署名複写である。従来の紙文書への電子署名技術のほぼ全てはソフトウェアに依存しており、署名を付加する際に必ずソフトウェアを中継する流れになる。これではソフトウェアを利用するための知識が必要になってしまうことに加え、既存文書への署名付加の際、文書を電子化する作業が増え、ユーザーへの負担が大きくなってしまう。そこで本システムでは、あらかじめ作成した署名画像を OHP フィルムのような透明媒体に印刷し、管理する。その後は PC 知識の多少に関わらず、常人が経験済みであると想定されるコピー機を用いた複写作業を、用意した OHP シートと重ねて行うだけで、直前に印刷した文書や、既存の紙文書に対して容易に署名を付加することが可能となる。

埋め込むデータについても、ドットパターンの濃淡を利用するため、既存手法[5]の埋め込み方式と比較すると、埋め込みパターンと印刷内容が重なった場合の対処が可能という点で本提案方式が優位であると言える。本方式では、パターン内の連続領域を排除して濃淡の判定を行うことが可能である。

4. 性能評価

本システムでは埋め込むドットパターンを様々な条件の元で利用できる。そこで基本的な性能の評価としてドットパターン全体の濃度、濃度の割合、スキャン解像度を変化させ、その読み取り精度を比較した。図 2,3 のサンプル署名画像のドットパターンを利用し、その検証率結果を平均した値を以下の表1に示す。

表 1 検証率結果

	200dpi	300dpi	400dpi
10-30pt	92%	92%	92%
40-60pt	100%	100%	100%

本評価では主にコピーを利用する際に使われる解像度である 300dpi 前後での検証を試みている。結果として、スキャン解像度による読み取り性能はこの範囲では非常に少なく、検証結果もほぼ同じであった。大きく差が出たのはポイント数による違いである。40-60pt 時の検証率が非常に信頼性のある数字を出しているが、文字などと重ねて利用するシーンを想定すると、視認性が悪くなるという問題が発生する。そのため利用するにあたって最適と思われるのが 10-30pt であるが、空白領域が多いためか軸ずれによるブロック内ドット数の増減に大きく反応してしまい、わずか数 pixel ずれただけで検証率が下がってしまう。現在はドットをランダムに打ち込んでいるが、ブロック内のドット配置についても、隣接するブロックの濃淡を考慮し、今後見直していく必要があると考えられる。加えて本実験では、検証用画像に 24 ビット ビットマップを利用しているため、スキャンする際に滑らかさを表現する中間色が画像情報に加えられ、それらの読み取りミスによる誤差が非常に多く検出された。検証に扱うデータは二値であるため、ビット変換などを組み込むことで誤差の減少を図ることが課題である。

5. まとめ

現在はドットパターンからの情報抽出の一部のみ完成しているが、検出率が低い点や、パターン毎に検出率のバラつきがある。現在の本システムで利用している透かし技術は紙文書セキュリティとしての位置づけで表すと、二次元バーコードに近い利用形態となっている。主な欠点として、情報埋め込み位置の視認ができ、改ざんするべき箇所が明らかであるため、切り離し・塗りつぶしなどによる情報追跡

からの回避が容易なことが挙げられる。そこで今後の改善策としては、文書内の署名画像領域を広げ更なる冗長性を持たせ、文書の印刷部分の一部と故意に重ねることで、改ざんへの耐性を向上させることを検討している。主な改良点として、位置検証マーキングによる署名領域の選択支援、誤り訂正による検証率向上、重なった文字領域の抜き出し、検証効率の良いドットの配置パターンの検討が挙げられる。検出アルゴリズムに関しても部分的に見直し、随時修正していく方針である。

参考文献

[1] 高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）, http://www.kantei.go.jp/jp/singi/it2/kettei/040206honbun.html,（参照 2006-09-12）

[2] 海老澤竜,藤井康広,高橋由泰,手塚悟,"紙文書に対するセキュリティ技術の考察",情報通信学会研究報告 2006-CSEC-34 ,pp305-311,2006

[3] キヤノン ソフトウェア|imageWARE TrustStamp http://cweb.canon.jp/Product/appli/truststamp/（参照2006-9-12）

[4] 須崎昌彦,藤井明宏,保田浩之,"セキュアプリント技術を用いた印刷文書改ざん検証システムの開発",IPA次世代ソフトウェア開発事業 2003年度成果報告, http://www.ipa.go.jp/SPC/report/03fy-pro/jise/15-975d.pdf（参照2006-5-30）

[5] 前野蔵人,須藤正之," 複写・回転・クリッピング耐性を持つ印刷文書用電子透かし",電子情報通信学会 信学技報 IEICE Technical Report ISEC2005-68,pp175-182,2005-07

[6] 伊藤健介,左右田宏之,井原富士夫,木村哲也,布施マリオ,"富士ゼロックス テクニカルレポート",No.15,pp32-31,2005

[7] 藤井康広,中野和典,越前功,吉浦裕,手塚悟,"局所特徴量を用いた二値画像用電子透かしの画質維持方式",情報処理学会論文誌 ,vol.44,no.8,pp1872-1883,Aug.2003

[8] 2次元コードの基礎知識：バーコードホットライン,http://www.keyence.co.jp/barcode/2jigenbasic/,（参照2006-9-12）