社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（43）
2005－CSEC－28（43）
2005／3／23

電磁的記録の時刻認証に適した電子文書墨塗り応用方式

佐藤　亮太　　藤村　明子　　千田　浩司　　塩野入　理　　金井　敦

日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
〒 239-0847 神奈川県横須賀市光の丘 1-1

{ryota,akiko,chida}@isl.ntt.co.jp, {shionoiri.osamu,atsushi.kanai}@lab.ntt.co.jp

あらまし　現在、e-文書法の制定に向けて電磁的記録の作成・保存・利用に関する様々な技術的、運用的な対策が求められている。その技術的な対策の一つとして、電子文書墨塗り技術の応用が考えられる。この電子文書墨塗り技術は、電磁的記録の一部を秘匿しても、残りの部分の完全性を検証可能な技術である。本論文では、電磁的記録の作成・保存・利用の要件についてまとめ、その要件の中の電磁的記録の完全性の確保と柔軟性の確保を行うための電子文書墨塗り技術の応用方式について提案する。

An Application of Digital Document Sanitizing Scheme Suitting to Timestamps for Digital documents.

Ryota SATO　　Akiko FUJIMURA　　Koji CHIDA　　Osamu SHIONOIRI
Atsushi KANAI

NTT Information Sharing Platform Laboratories, NTT Corporation
1-1, Hikarino-oka, Yokosuka, 239-0847, Japan

{ryota,akiko,chida}@isl.ntt.co.jp, {shionoiri.osamu,atsushi.kanai}@lab.ntt.co.jp

Abstract　The present technical and operational measures concerning making, preservation and use of digital documents are required to prepare for the legal of digital documents. We propose that an application of digital sanitizing scheme as one of the technical measures. The digital sanitizing scheme enables us to verify the integrity of partially sanitized document. In this paper, we adjust the requirements for making, preservation and use of digital documents and propose an application of digital sanitizing scheme to meet the requirements for integrity and flexibility demand.

1　はじめに

1.1　背景

2004 年 2 月に IT 戦略本部によって「e-Japan 戦略　加速化パッケージ」が策定され [1]、その中の、IT 規制改革の推進（Deregulation）において「e-文書イニシアティブ」が提言されている。ここでは、民間に保存が義務付けられている財務関係書類、税務関係書類等の文書等のうち、電子的な保存が認められていないものについて、文書等の内容、性格に応じた真実性・可視性等を確保しつつ、原則としてこれらの文書等の電子保存が可能となるよう統一的な法律の制定等により行うとされており、その統一的な法律として「民間事業者等が書面の保存等における情報通信の技術の利用に関する法律」（以下、e-文書法）が 2004 年 11 月に成立した [2]。

経団連の試算によれば、経済界における税務書類の紙による保存コストは年間約 3,000 億円にも及ぶことが示されており [3]、法令により義務付けられている紙での保存が、民間の経営活動や業務運営の効率化の阻害要因となっていることが指摘されている。そのため、これらの電子保存を容認することにより、文書保存コストを軽減することや、新たなビジネスプロセスの創出による利便性の向上、企業の競争力の向上、そして電子商取引の発展に資することが e-文書イニシアティブのねらいとされている。

また、e-文書法においては文書の電子的保存だけでなく、書面の作成や、縦覧、交付等の利用についても書面に代えて、電磁的記録により電子的に行うことを容認している。紙文書から電磁的記録への移行を行う場合には、電磁的記録の作成・保存・利用上の問題点を整理し、それを解決することが e-文書法を実行性のあるものにするために重要となろう。

そこで本論文においては、「紙文書と比較した場合の電磁的記録の作成・保存・利用上の問題点が解決された状態にすること」を「電磁的記録の優位性を確保すること」と定義する。この電磁的記録の優位性確保の観点から、その際の問題点、要件とその対策について次節で述べることにする。

2　e-文書法からの要件整理

2.1　要件整理

電磁的記録の優位性を確保するための問題点としては表 1 に示されている a)〜 f) に分類することができる。そして、これらの問題点は見読性、検索性、機密性、完全性の 4 つの要件としてまとめられよう [4]。上述の問題点、要件に関しては様々な技術的、運用的な対策が考えられ、そのいくつかの例を以下にまとめることにする。

まず、見読性に関しては、e-文書法においては元が紙文書であるものを一定の技術基準の下にスキャナー等でイメージデータ化した電子化文書と呼ばれるものによる保存を認めることが検討されている。この見読性の要件は主に電子化文書に関して、一定以上の精度のスキャン技術や電子機器等での表示技術が必要になるであろう。

また、検索性は紙文書に比べた時の電磁的記録の優れた点の一つとして挙げられ、膨大な電磁的記録の中からある特定のキーワードを含むものを検索する等の作業の効率化を図ることができる。しかし、検索が容易になるため、閲覧権限をもたないものまで検索されてしまう可能性が危惧される。

さらに、機密性の確保の点においても電磁的記録は遠隔からでもその文書にアクセスすることが可能であると同時に、そのアクセス制限が十分でない場合は、アクセス権限のない者にも縦覧されてしまう可能性がある。これらの検索性、機密性の確保のためには、ID やパスワードによる認証からバイオメトリクス認証まで様々な認証を用いて、電磁的記録に対する正当な権限を持つ者のアクセス制限と、さらにアクセスした者がどの電磁的記録まで閲覧可能かをアクセス制限するなどの対策が必要である。

完全性の課題については、問題点 d) では、電磁的記録が長期保存により記憶されていたメディアから情報の消失や互換性の喪失によって情報が消えてしまうという物理的な問題から、長期保存の際に電子署名等の秘密鍵の漏洩や推定等の問題まであり、後者の技術的対策の一つとしてはヒステリシス署名 [5] などが挙げられる。

問題点 e)、f) に対しては、誰が、いつ、何を文書として残したかという真正性の確保が重要であり、その技術的対策としては電子署名による本人証明とタイムスタンプによる時刻証明がある [6]。

2.2　新しい要件と技術的対策

前節では要件、問題点に対する技術的な対策の例をいくつか述べたが、これらの要件の充足を求めた結果、更に「電磁的記録の優位性確保」のために必要になる要件も考えられる。その例として、電子署名やタイムスタンプによって電磁的記録の完全性を確保した場合を考える。このとき、技術的な対策を施したことによって、その文書に対して正当な権限を持った者による文書の追記、削除といった、本来の紙文書にお

表 1: 電磁的記録の優位性を確保する際の問題点と要件

要件	問題点
見読性	a). 文書に記録された事項について電子計算機等を用いて見読する必要がある.
検索性	b). 文書に対する検索が容易であるため、 必要以上の文書に記録された事項について検索される可能性がある.
機密性	c). 文書に対する遠隔からのアクセスが可能であるため、 アクセス権限を持たない者が文書にアクセスする可能性がある.
完全性	d). 長期保存の際に情報の消失や互換性の喪失が起こる可能性がある. e). 文書の改竄に当たり痕跡が残りにくい. f). 紙文書は紙やインク等の経年劣化等の情報によりある程度作成時期が推定できるが、 電磁的記録は情報の作成時期の改変が容易である.
柔軟性	g). 完全性を確保する対策を行うことにより、以降は電磁的記録に対する修正ができなくなる.

いては行うことが可能であった柔軟な利用は全て改竄とみなされてしまうという問題点がある。

そこで本論文では、この完全性を充足する技術を施した後も文書の追記、削除等の修正が行えるようにすることを「柔軟性」という新たな要件として定義する。そして、この柔軟性確保のうち、完全性確保と文書の削除との両立を可能にするための技術的な対策として電子文書墨塗り技術の応用が考えられる [7][8][9]。

3 電子文書墨塗り技術

3.1 従来方式

「行政機関の保有する情報の公開に関する法律」（以下、情報公開法）において [10]、情報公開を求められた文書中にプライバシ情報等の非開示情報が含まれている場合は、その部分を墨塗り等の秘匿を行った上で開示しなくてはならない事が明示されている。しかしながら、これを従来の電子署名を施した電子文書に対して行うと、墨塗り部分が改竄として検知されてしまい、プライバシ保護と電子文書の作成者証明、改竄検知・防止の両立が困難になる。これが電子文書墨塗り問題と呼ばれており、この問題を解決する技術が幾つか提案されている [7][8][9]。

これまでの情報公開法の例に沿った電子文書墨塗り技術は、プライバシ保護と電子文書の作成者証明、改竄検知・防止の両立が問題となっていた。これを e-文書法における完全性の確保のためのタイムスタンプなどの認証と、それによって失った、文書作成者の修正の機会を両立させ、柔軟性を確保するための技術であると考える。このとき、柔軟性を確保するためには、情報の部分的な秘匿と文書の作成者証明、改竄検知・防止の両立をするだけでなく、その文書に対する修正に関する記録が電磁的記録に残るようにすることによって、例えば e-文書法において利用が想定される税務関係書類等に対しても適用可能となるような高い証拠力をもたせることが重要である。そこで本論文では、電磁的記録の修正履歴を保存し、柔軟性を確保するためにタイムスタンプ認証を用いた場合の電子墨塗り応用方式を提案する。

3.2 提案手法

従来の電子文書墨塗り方式は、電子文書の作成者が自らの電子署名を付し、情報公開にあたっては、それを電子文書の作成者とは異なる墨塗りを行う者（以下、墨塗り者）が電子文書の適当な箇所に墨塗りを施し、開示請求を行った者（以下、検証者）に渡すものであった。しかし、公的に電磁的記録の完全性を確保するためには、その電磁的記録を他の信頼できる第三者が署名することで、その完全性を第三者が担保する必要がでてくるであろう。そこで今回は、電磁的記録がいつ修正されたかについての履歴を残すために、電磁的記録の作成者は信頼できる署名者であるタイムスタンプ・オーソリティ（以下、ＴＳＡ）にタイムスタンプを依頼することを考える。

提案方式では、元の電磁的記録を n 分割した

情報の結合 M を生成し（以下、改めて電磁的記録 M)、作成者は以下の処理を行う。

作成者

$$
\begin{aligned}
M &= \{m_1 \parallel m_2 \parallel \cdots \parallel m_n\} \\
h_i &= \mathbf{Hash}(r_i, m_i) \qquad (r_i : \text{乱数}) \\
\mathcal{H} &= \{h_1 \parallel h_2 \parallel \cdots \parallel h_n\} \\
H &= \mathbf{Hash}(\mathcal{H}) \\
S &= \mathbf{Sign}_{\text{writer}}(H)
\end{aligned}
$$

ここで、$\mathbf{Sign}_{\text{writer}}()$ は作成者による電子署名を表しており、また $i = 1, 2, \cdots, n$ である。このハッシュ値の結合 $\mathcal{H}$ をさらにハッシュしたもの H をＴＳＡに送信し、このハッシュ値 H に対してのタイムスタンプを押してもらう。

ＴＳＡ

$$T = \mathbf{Sign}_{\text{TSA}}(H, t) .$$

ここで、t はそのときの時刻情報を表している。このように、ＴＳＡに対してハッシュ値 H のみを提出することによって、ＴＳＡは電子墨塗り技術特有の処理をすることなく、従来のタイムスタンプの処理と同様の手続きを行えばよい。特に、IETF/PKIX で策定されているタイムスタンプ・プロトコルの標準の RFC3161(Internet X.509 Public Key Infrastructure Time-Stamp Protocol) において、ＴＳＡの要件としてハッシュ値に対して署名を行うことが決められている [6]。ＴＳＡからタイムスタンプ T を受け取った作成者は、それを元に署名情報 s を生成する。

作成者

$$s = (\ H\ ,\ S\ ,\ T\ ) .$$

次に、検証者から電磁的記録 M の提出を求められた際に、作成者は以下の処理を行い、開示文書 M' と、それに対する電子署名 S' を生成する。

作成者

$$
\begin{aligned}
M' &= \{m'_1 \parallel m'_2 \parallel \cdots \parallel m'_n\} \\
m'_i &= \begin{cases} m'_i & (m_i : \text{非開示}) \\ m_i & (m_i : \text{開示}) \end{cases} \\
\tilde{m}'_i &= \begin{cases} (r'_i, m'_i) & (m_i : \text{非開示}) \\ (r_i, m_i) & (m_i : \text{開示}) \end{cases}
\end{aligned}
$$

$$
\begin{aligned}
h'_i &= \mathbf{Hash}(\tilde{m}'_i) \\
\mathcal{H}' &= \{h'_1 \parallel h'_2 \parallel \cdots \parallel h'_n\} \\
H' &= \mathbf{Hash}(\mathcal{H}') \\
S' &= \mathbf{Sign}_{\text{writer}}(H')
\end{aligned}
$$

この開示文書 M' に対しても時刻証明を行うために、作成者はＴＳＡに対してハッシュ値 H' を送信する。

ＴＳＡ

$$T' = \mathbf{Sign}_{\text{TSA}}(H', t') .$$

ここで、t' はそのときの時刻情報である。ＴＳＡからタイムスタンプ T' を受け取った作成者は以下の署名情報 s' を生成する。

作成者

$$s' = (\ H'\ ,\ S'\ ,\ T'\ ) .$$

作成者は検証者に対して $(M', \mathcal{H}, \mathcal{H}', s, s')$ を送信する。これを受けた検証者は $\mathcal{H}$ と $\mathcal{H}'$ とを比較し、$h_i \neq h'_i$ となる i をもって、非開示部分であることを確認する。最後に検証者は、署名情報 s, s' を以下の処理で検証する。

検証者

$$
\begin{aligned}
\mathbf{Parse}(s) &\Rightarrow (\ H\ ,\ S\ ,\ T\ ) \\
\mathbf{Parse}(s') &\Rightarrow (\ H'\ ,\ S'\ ,\ T'\ ) \\
\mathbf{Verify}_{\text{TSA}}(T, H) &\Rightarrow \mathbf{OK/NG} \\
\mathbf{Verify}_{\text{writer}}(S, H) &\Rightarrow \mathbf{OK/NG} \\
\mathbf{Verify}_{\text{TSA}}(T', H') &\Rightarrow \mathbf{OK/NG} \\
\mathbf{Verify}_{\text{sanitizer}}(S', H') &\Rightarrow \mathbf{OK/NG}
\end{aligned}
$$

ここで、$\mathbf{Verify}_{\text{TSA}}()$、$\mathbf{Verify}_{\text{writer}}()$ はそれぞれ電子署名がＴＳＡ、作成者によるものである事を確認する電子署名検証関数である。

3.3 安全性評価

提案方式の安全性を評価する。セキュリティ要件の一つとして、墨塗り部分の情報が漏洩しないことが挙げられるが、墨塗り部分に対する文書情報は、作成者がＴＳＡに対して文書のハッシュ値を渡すだけであるので、ＴＳＡに関しても、また通信路の途中で情報を傍受した悪意の

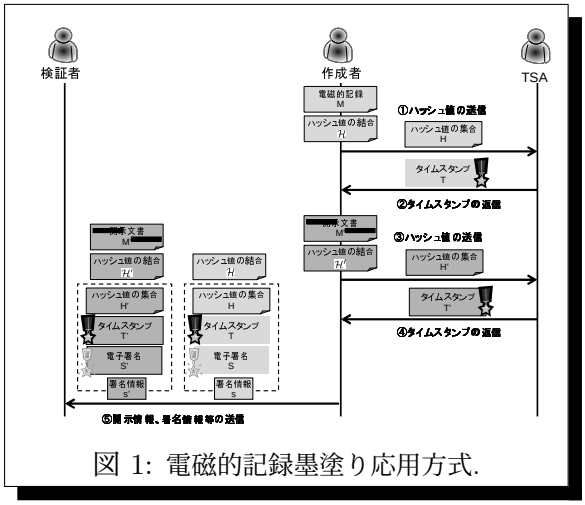

図 1: 電磁的記録墨塗り応用方式.

ある第三者に関しても漏洩しない。これはハッシュ関数の一方向性により保証される。

もう一つのセキュリティ要件として、悪意ある第三者が、墨塗り部分以外の文書が改竄されており、且つ正しく署名検証できる署名付き開示文書を作成できないことが挙げられるが、提案方式では、作成者が元の文書 M から作成したハッシュ値の集合 $\mathcal{H}$ と、公開文書 M' から作成したハッシュ値の集合 $\mathcal{H}'$ とにおいて、ハッシュ値が変更されてないことで、墨塗り部分以外の文書の改竄がないことを保証している。これは、特定の文書に対して同じハッシュ値を持つ異なる文書の作成は困難であるというハッシュ関数の衝突困難性により保証される。

4 考察と適用事例

4.1 考察

本方式においては、電磁的記録の柔軟性を確保するために、その電磁的記録に関する改変の履歴を記すタイムスタンプをもらいながら電磁的記録に対する墨塗り処理を行う。この時、ＴＳＡに対しては電磁的記録のハッシュ値の集合のみを渡すことで、ＴＳＡは電子墨塗りをするために特化した装置を備えることなく、従来のタイムスタンプの処理を行えばよい。また、電子墨塗りされていない部分については、従来の電子文書墨塗り技術と同様に電子署名によって、元の電磁的記録との同一性を担保し、電磁的記録の信憑性を保証することができ、一方で、電子墨塗りされた部分については、ハッシュ値の一方向性により情報が漏洩しないことが保証されている。このことによって、他者に対する守秘性が高まると同時に情報の信頼性も確保されているため、情報公開制度における電子文書に限らず、様々な電磁的記録における情報の公開可能性が高まることが期待される。特に、本方式のように信頼できる第三者であるＴＳＡによるタイムスタンプのお墨付きによる改変の履歴を残すことによって、柔軟な電磁的記録の利用と、その証拠力自体を高めることが可能になる。

4.2 適用事例

電磁的記録に柔軟性や証拠力が求められる場合の例として、今後増加が予想される知的財産紛争や企業のもつ個人情報に関する紛争、企業自身の持つ機密情報に関する紛争などにおける裁判での証拠提出が挙げられよう。例えば、我が国においては知的財産重視の国家政策をとられているなかで [11]、知的財産をめぐる紛争はその証拠が非常に機微な情報を含むために、裁判の際には証拠の取り扱いが問題となっている [12]。

現在、裁判は公開の法廷で行うことが憲法の 82 条 1 項で規定されている。従って、これまでは裁判の証拠として自分に有利な情報が含まれている書類等であっても、他人に知られたくない情報が一部含まれていれば、場合によっては証拠書類（以下、書証）としての提出を断念する必要があった。また、相手から書証の提出要求をされる場合もあり、提出したくない場合は提出拒絶の理由を裁判所に提出し、裁判所が拒絶理由の正当性を判断することになる。このとき、裁判所が実際にその証拠を公開のもにせずに、裁判官のみがその書類を調査することによって提出拒絶理由が正当なものであるかどうかを判断する方法をとっており、これをインカメラ審理と呼んでいる [13]。このインカメラ審理によって拒絶理由が正しいものであれば証書の提出はする必要はなく、逆に、拒絶理由が認められない場合はそれを公開される証書として提出しなければならない。また、裁判所が証書の提出を認めた場合、その証書の中に取り調べる必要がないと認められる部分又は提出の義務

があると認められない部分があるときは、その部分を除いて提出することを命ずることができる旨が民事訴訟法の第223条に明記されている。そこで、今回の方式を利用することにより、電磁的記録に対して部分的にマスクすることにより、これまでは電磁的記録の証拠書類は、提出する、もしくは提出しないのどちらかの選択を迫られていた場面に対して、中間解を与えることができる。さらに、タイムスタンプにより改変の履歴が残った証拠力の高い証拠書類を提出することにより、裁判官に対する心証形成に対しても効果的であると考えられる。これにより、書証に含まれる企業や個人の機密情報の保持と裁判の公開の原則の両立とが可能となり、結果として例えば、企業の知的活動の推進を促すことが可能となるであろう。

5 まとめ

本論文では、e-文書法の制定に備え、電磁的記録の作成・保存・利用に求められる要件について整理し、その中の要件である柔軟性を確保するための技術として時刻認証に適した電子文書墨塗り応用方式を提案した。提案方式より、電磁的記録の柔軟性の確保と秘密情報の秘匿の両立を可能となるだけでなく、電磁的記録に対する修正がいつ、誰によって行われたかという修正履歴を残すことにより、電磁的記録の証拠力を高めつつ文書の持つ柔軟性を確保することが可能となった。

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）(2004)“ e-Japan 戦略 加速化パッケージ ”
http://www.kantei.go.jp/jp/singi/it2/kettei/040206ejapan.pdf

[2] 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）(2004)“ e-文書法案の骨子 ”
http://www.kantei.go.jp/jp/singi/it2/dai27/27siryou7.pdf

[3] 日本経済団体連合 (2004)“ 税務書類の電子保存に関する報告書【概要】 ”
http://www.keidanren.or.jp/japanese/policy/2004/018gaiyo.pdf

[4] 文書の電磁的保存等に関する検討委員会 (2004)“ 文書の電磁的保存等に関する検討委員会中間報告書 ”
http://www.kantei.go.jp/jp/singi/it2/dai27/27siryou7.pdf

[5] 岩村充, 宮崎邦彦, 松本勉, 佐々木良一, 松木武, “ 電子署名におけるアリバイ証明問題と経時証明問題－ヒステリシス署名とデジタル古文書の概念 ”, コンピュータサイエンス誌，bit Vol.32, No.11, 共立出版，2000

[6] C. Adams, et al. ”RFC 3161-Internet X.509 Public Key Infrastructure Time-Stamp Protocol(TSP)”, IETF, 2001

[7] 宮崎邦彦, 洲崎誠一, 岩村充, 松本勉, 佐々木良一, 吉浦裕, “電子文書墨塗り問題,” 信学技報 ISEC2003-20，pp.61-67, 2003

[8] 宮崎邦彦, 岩村充, 松本勉, 佐々木良一, 吉浦裕, 手塚悟, 今井秀樹, “開示条件を制御可能な電子文書墨塗り技術,” 2004年暗号と情報セキュリティシンポジウム (SCIS2004), 2D3-2, pp.515-520, 2004

[9] 武仲正彦, 吉岡孝司, 金谷延幸, “検証者が署名者と墨塗り者を識別可能な電子文書の墨塗り方式,” コンピュータセキュリティシンポジウム 2004(CSS2004)，6C, pp.475-480, 2004

[10] 総務省行政管理局 (1999)“ 行政機関の保有する情報の公開に関する法律 ”
http://www.soumu.go.jp/gyoukan/kanri/gh003.htm

[11] 内閣官房知的財産戦略本部 (2003)
http://www.kantei.go.jp/jp/singi/titeki2/

[12] 司法制度改革推進本部事務局 (2004)“ 知的財産関係事件への総合的な対応強化 ”
http://www.kantei.go.jp/jp/singi/sihou/komon/dai15/15siryou2.pdf

[13] 第 10 回情報開示法の制度運営に関する検討会配布資料 (2005)“ いわゆるインカメラ審理に関する規定の例 ”
http://www.soumu.go.jp/gyoukan/kanri/jyohokokai/pdf/050125_sanko2.pdf