墨塗り者を特定可能な電子文書の墨塗り署名方式

伊豆哲也[†] 金谷延幸[†]
武仲正彦[†] 吉岡孝司[†]

2005 年に施行された個人情報保護法は，公文書の公開における個人情報の墨塗りを義務づけている．しかし公文書が電子文書として保管・運用され，さらに電子署名が付されている場合，署名生成後に墨塗りを施した文書は検証に失敗する．これは，通常の署名技術が文書に対する正当な変更（墨塗り）と不正な変更（改竄）を区別できないためである．このような問題を解決する手段として，いくつかの墨塗り署名方式が提案されている．しかし従来の墨塗り署名方式では，誰が墨塗りを施したかを特定することが困難であった．本稿は，墨塗り者の特定を可能とする新しい墨塗り署名方式（PIAT 署名）を提案する．またいくつかの墨塗り署名方式の比較検討を行う．

A Sanitizable Signature Scheme with Sanitizer Identification

Tetsuya Izu,[†] Nobuyuki Kanaya,[†] Masahiko Takenaka[†]
and Takashi Yoshioka[†]

When a document is disclosed with hiding privacy information, masking (sanitization) is widely used as a standard technology for paper documents. However, no corresponding technology has not been established for electronic documents. In addition, when digital signature schemes are combined in order to assure the integrity of disclosed information, the verification will be failed because standard digital signature schemes are not able to distinguish appropriate alternations (sanitizations) from inappropriate alternations (forgeries) in the sanitized document. The *sanitizable signature scheme* is a possible solution in which sanitizings of partial information are possible, after a signature is signed on the original (unsanitized) document. However, in previously proposed schemes, sanitizations by plural sanitizers were impossible, or even if it is possible, it was hard to identify who sanitized which subdocuments. This paper proposes a new sanitizable signature scheme "PIATS" in which plural sanitizations are possible and verifiers can identify sanitizers. Also some sanitizable signature schemes are compared and analyzed in this paper.

1. はじめに

官公庁や自治体は，情報公開法（1999 年 5 月施行）[20] の要請により，自らが保持する文書を開示することが原則となっている．しかし公開文書においては，プライバシや国防上の理由から個人情報や国家機密の秘匿も義務づけられている．従来の紙文書では情報秘匿の手段としてマスキング（墨塗り）技術が標準的に用いられていたが，電子文書については対応する標準的な技術が確立されておらず，不十分な墨塗りに基づいた情報漏洩が国内外で後を絶たない状況である[1),7),21),24),25)]．他方，電子文書に対するディジタル署名技術は，オリジナル文書に対する改竄を検知可能であることから，文書の完全性を保証するための標準的な技術となっている．しかし現在の署名技術はオリジナル文書の正当な変更（墨塗り）と不正な変更（改竄）を区別できないため，前述のような墨塗りを改竄として見なしてしまう．したがって，署名者が署名した後でも墨塗りが可能であり，墨塗り箇所については墨塗り前の内容の秘匿性が，開示された箇所（墨塗りされてない箇所）についてはその完全性が保証できるような電子文書の処理方式の確立が望まれている．

墨塗り署名方式（Sanitizable Signature Scheme）は上記の問題に対する 1 つの解決方法であり，署名が生成された後でも部分情報に対する墨塗りが可能であって，墨塗り箇所の秘匿性と開示箇所の完全性を保証することが可能である[2),14),15),18)]．これら墨塗り署名方式では，正当な変更（墨塗り）と不正な変更（改竄）は区別され，墨塗りは許容，改竄は排除される．

† 株式会社富士通研究所
FUJITSU LABORATORIES LTD.

しかし既存の墨塗り署名方式では，誰が墨塗りをしたかを検証することができないため，墨塗り文書の偽造が可能になることがあった[14]．

本稿は新しい墨塗り署名方式（PIAT 署名）の提案を目的とする．PIAT 署名は RSA-PSS[17] といった任意の安全な（つまり適応的選択文書攻撃に対して存在的偽造不可能な）署名方式を併用することで，開示部分の完全性と非開示部分の秘匿性を両立させる電子文書への墨塗り方式を実現する．特に PIAT 署名は，複数の墨塗り者による墨塗りを可能とする一方で，検証者はどの墨塗り者がどこの墨塗り部分を墨塗りしたかを特定することができることを特徴とし，前記のような墨塗り文書の偽造を防ぐことが可能となる．アメリカでは不正会計問題（エンロン事件やワールドコム事件など）に対処する目的で 2002 年に SOX 法が導入され，日本でも同様の法律（JSOX 法）が 2008 年にも施行される予定となっている．これら法律の理念は企業などが保持する文書の統制であり，墨塗りを含む文書のあらゆる変更の監査証跡の保管が求められることが予想されている．提案墨塗り署名方式は，墨塗りに対する監査証跡の保管を可能としており，実社会での広い応用性を持っていると考える．

本稿の構成は以下のとおりである：2 章でこれまでに提案された墨塗り署名方式を簡単に紹介し，3 章で我々の提案する墨塗り署名方式（PIAT 署名）の詳細を説明する．そして 4 章においてこれら墨塗り署名方式を比較する．

2. 既存の墨塗り署名方式

本章では，従来までに提案されてきた墨塗り署名方式を概観し，特に提案墨塗り署名方式との関連性が高い CES[18]，SUMI[14),15)] の処理手順を簡単に紹介する．

2.1 記　　号

署名の対象となるオリジナル文書は n 個の（必ずしも等しくないビット長の）部分文書から構成される列 $(M_1, \ldots, M_n)$ として与えられているとする．たとえば，部分文書として XML 構文における最小構文単位[3] や JPEG 画像ファイルにおける最小符号化ユニット[23] が考えられる．乱数は適当な（疑似）乱数生成機によって生成され，また関数 $H(\cdot)$ は SHA-256 のような安全な任意のハッシュ関数とする．関数 $\mathsf{Sign}_{\mathsf{sk}}(\cdot)$ は RSA-PSS[17] のように安全な（つまり適応的選択文書攻撃に対して存在的偽造不可能な）任意の署名方式の署名生成関数を表すとする．

2.2 墨塗り署名方式のモデルと安全性

墨塗り署名方式は鍵生成者，署名者☆，墨塗り者，検証者から構成される[14),15),18)]．鍵生成者は秘密鍵・公開鍵ペアを生成する確率的アルゴリズムである．署名者は自分の秘密鍵を用いて受け取った文書に対する署名を生成する．墨塗り者はオリジナルの（または墨塗りされた）文書と署名を受け取り，新たな墨塗り文書と署名を出力する．最後に検証者は墨塗り文書と署名を受け取り，検証作業を通じて墨塗り文書の開示部分に改竄がないことを確認する．

墨塗り署名方式は安全性として秘匿性（Secrecy）と偽造不能性（Unforgeability）を満たす必要がある[14),18)]．詳細な安全性の定義は方式によって異なるが，秘匿性とは墨塗りされた部分からもとの文書内容が漏れないこと，偽造不能性とは正当な墨塗り文書・署名ペアは墨塗り者以外には作成できないことを意味する．

2.3 CES

CES（Content Extraction Signature）は Steinfeld らによって提案された墨塗り署名方式で[18]，CES-CV，CES-HT，CES-RSAP，CES-MERP の 4 つのアルゴリズムから構成されている．このうち CES-CV が中心アルゴリズムで，残りはその変形である．CES-CV と CES-HT は任意の署名方式と組合せ可能なのに対し，CES-RSAP と CES-MERP は RSA 型の署名方式としか組み合わせられない．

CES-CV では，署名者は n 個の（乱数を添付した）部分文書に対応する個々のハッシュ値を求め，これらハッシュ値の連結に対して署名を生成する☆☆．墨塗り者は墨塗り（非開示）する部分文書をハッシュ値で置き換え，墨塗り文書と非開示部分文書の添字集合を出力する．検証者は，添字集合を用いて開示部分と非開示部分を識別し，墨塗り文書の開示部分については部分文書内容のハッシュ値を，非開示部分については部分文書内容をそのまま用い，署名対象となっているハッシュ値の連結を復元・検証する．CES-CV では，署名者はさらに CEAS（Content Extraction Access Structure）と呼ばれる開示可能な部分文書の組合せを指定することとなっており，CEAS で定められた組合せ以外の部分文書は開示できないようになっている．CES-HT は，CES-CV における CEAS のデータ量をハッシュ木を用いて削減した方式である．

☆ CES 方式では，署名者は所有者と呼ばれている[18]．

☆☆ オリジナルの CES-CV はハッシュ関数ではなくメッセージコミットメントを用いているが[18]，簡単のため本稿ではハッシュ関数を用いることとする．

CES は複数の墨塗り者による墨塗りが可能であるうえに，署名を 1 個しか必要としないことから，その効率はきわめて優れている．安全性については，秘匿性と偽造不能性が示されている．ただし CES が偽造として想定している墨塗り文書では，CEAS が指定していない墨塗り文書と，すでに署名が生成された文書の墨塗り文書・その墨塗り文書は除外されている[18]．

2.4 SUMI

SUMI は Miyazaki らによって提案された墨塗り署名方式で[14),15)]，SUMI-1，SUMI-2，SUMI-3，SUMI-4，SUMI-5 の 5 つのアルゴリズムから構成されている．いずれのアルゴリズムも任意の署名方式との組合せが可能である．

2.4.1 SUMI-1，SUMI-2

n 個の部分文書から構成されている文書に対し，SUMI-1 は考えられるすべて（2^n 通り）の部分文書の部分集合とそれに対する（2^n 通りの）署名を生成する．墨塗り者は開示する部分文書を定め，対応する部分集合と署名を検証者に送る．したがって SUMI-1 の墨塗りは 1 回に限定され，効率も良いとはいえない．

SUMI-2 では，署名者は n 個の部分文書に対応する n 個の署名を生成する．墨塗り者は開示する部分文書と署名の集合を出力し，検証者は受け取った部分文書・署名ペアを個々に検証する．同様の手順を繰り返すことで，SUMI-2 は複数の墨塗りに対応するが，n 個の署名を必要とするため効率は悪い．

2.4.2 SUMI-3，SUMI-4

CES-CV では開示可能な部分文書の添字集合 CEAS の署名者による特定が必須であった．しかし，たとえば法律によってオリジナル文書とその署名の長期間にわたる保管が義務づけられる場合，署名時に定めた開示・非開示ポリシが，法律の改正などによって墨塗り時にはそぐわなくなる可能性が考えられる．このような観点から，SUMI-3，SUMI-4 における署名者は署名生成しか行わず，開示する部分文書の開示・非開示ポリシの決定はすべて墨塗り者に委ねられるようになっている．

SUMI-4 のアルゴリズムは，CES-CV から CEAS の利用を除いたアルゴリズムと見なすことができる．安全性については秘匿性と偽造不能性を満たすことが示されている．ただし SUMI-4 が想定している墨塗り文書では，すでに署名が生成された文書の墨塗り文書・その墨塗り文書は除外されている[15)]．また SUMI-3 は SUMI-4 のアルゴリズムから確率的な振舞いを取り除いたアルゴリズムであり，Secrecy を満たさないことが指摘されている[15)]．

2.4.3 SUMI-5

SUMI-5 は Miyazaki らが提案した墨塗り署名方式であり，各部分文書に強制非開示（Closed），強制開示（DASP，Disclosed and Additional Sanitizing is Prohibited），開示（DASA，Disclosed and Additional Sanitizing is Allowed）の 3 つのいずれかのステータスを付与することを特徴としている[14)]（これに対し CES-CV，SUMI-4 におけるステータスは開示または強制非開示の 2 つである）．

SUMI-5 の署名時では，すべての部分文書のステータスは開示となっており，墨塗り者はステータスが開示である部分文書のステータスを強制開示または強制非開示に変更することが可能である．このように SUMI-5 では各文書の開示・非開示があらかじめ定められているため，追加墨塗り攻撃に対する耐性を持つ[14)]．しかし検証者はどの墨塗り者がどこの墨塗り部分を墨塗りしたか特定できない．

2.5 その他の方式

2005 年に Miyazaki らは双線形写像を利用した墨塗り署名方式を提案した[12)]．この方式は，墨塗りされた部分文書が検証者には検知できないという顕著な特徴（invisibility）を持っており，他の墨塗り署名方式の提案に大きな影響を与えた[5),6),9),19),22)]．

また近年は，墨塗り署名の機能を向上させる研究も見られるようになっている．2005 年に Ateniese らが提案した SSCH と呼ばれる墨塗り署名方式[2)] は，カメレオンハッシュ関数という特殊なハッシュ関数を用いることで，署名者による墨塗り者の指定が可能という特徴を持っている．また 2006 年に宮崎らは，部分文書への分割を必要としない墨塗り署名方式を提案している[13)]．さらに 2007 年には，ID ベース型の墨塗り署名が永村らによって提案されている[16)]．

なお 2002 年に Johnson らは Redactable Signature を提案してるが，これは CES や SUMI-4 のデータ格納方法を改良した墨塗り署名方式と見なすことができる[8)]．

3. 提案墨塗り署名方式：PIAT 署名

本章では新しい墨塗り署名方式 “PIAT 署名”（Partial Information Assuring Technology for Signature）を提案する．

3.1 既存墨塗り署名方式に対する考察

CES-CV，SUMI-4，SUMI-5 の偽造不能性の定義では，署名された文書に対する墨塗り文書は偽造文書から除外されており，墨塗り文書の作成は偽造には該当していなかった．またこれら墨塗り署名方式におけ

る検証者は，墨塗りされた部分が正しい処理で墨塗りされたこと（つまりオリジナル内容のハッシュ値に置き換えられていること）は検証できるが，誰が墨塗りしたかを識別することはできなかった．したがって，攻撃者がある墨塗り文書・署名ペアを受け取り，墨塗り箇所を不正に追加して新たな墨塗り文書・署名ペアを作成した場合，これら墨塗り署名方式の安全性の定義では偽造にはあたらないことになる．

誰が墨塗りしたかを識別できない原因として，墨塗り時に個人情報を用いずに墨塗りしている点があげられる．そこで我々は墨塗り者も秘密鍵・公開鍵ペアを有していることを仮定し，墨塗りに秘密鍵が必要となるような墨塗り署名方式を次節で提案する．

3.2 提案墨塗り署名方式

本節では，新しい墨塗り署名方式（PIAT 署名）を提案する．PIAT 署名の処理概要を**図 1** に示す（**図 2** も参照されたい．ここで各部分文書の左上の文字列は部分文書の識別子となる乱数 r_i を表す．墨塗り者は 5 番目の部分文書 “identified.” を，そのハッシュ値によって墨塗りしている）．ここで墨塗り者は m 人いるとし，署名者の秘密鍵・公開鍵ペアを $(\mathsf{sk}_0, \mathsf{pk}_0)$，$j$ 番目の墨塗り者の秘密鍵・公開鍵ペアを $(\mathsf{sk}_j, \mathsf{pk}_j)$ $(j = 1, \ldots, m)$ と記す．これらの秘密鍵・公開鍵ペアはあらかじめ与えられているとする．

PIAT 署名における署名者は，乱数を添付した各部分文書のハッシュ値 h_i の連結 $h = h_1 || \ldots || h_n$ に対する署名 σ を生成し，ハッシュ値集合・署名ペア (h, σ) を出力する．ここで乱数を添付する目的は 2 つあり，1 つはハッシュ関数の一方向性を確保する（つまり部分文書のビット長が短くても総当たり攻撃を無効にする）ため，もう 1 つは部分文書間の識別不能性を確保する（つまり同じ内容の部分文書であっても対応するハッシュ値が異なるようにする）ためである．したがって，たとえば出力 256 ビットのハッシュ関数を用いる場合，128 ビットの乱数を用いれば十分である．

（墨塗り）文書とハッシュ値・署名のペアを受け取った墨塗り者は，開示する部分文書については内容をそのままに保持し，新たに墨塗りする部分文書については，（乱数つき）部分文書をそのハッシュ値で置き換え，さらにそのハッシュ値を求める．このようにして新しいハッシュ値集合 $h' = h'_1 || \ldots || h'_n$ を求めて墨塗り者による署名 σ' を生成し，変更後の（墨塗り）文書とハッシュ値集合・署名ペア (h, σ)，(h', σ') を出力する．CES-CV や SUMI-4 とは異なり，墨塗り者はハッシュ値集合を比較することによってどの部分文書が墨塗りされているかを識別できるため，添字集合を出力する必要はない．

同様の手順を繰り返すことで，複数の墨塗り者による墨塗りも可能である．m 人の墨塗り者がいると仮定し，j 番目（$j = 1, \ldots, m$）の墨塗り者を考える．こ

署名者

入力 文書 $(M_1, \ldots, M_n)$

1. 各部分文書 M_i（$i = 1, \ldots, n$）に対する識別子 r_i をランダムに生成し，$\bar{M}_i^{(0)} \leftarrow r_i || M_i$ とする．さらにハッシュ値 $h_i^{(0)} \leftarrow H(\bar{M}_i^{(0)})$ を求める．

2. 署名 $\sigma^{(0)} \leftarrow \mathsf{Sign}_{\mathsf{sk}_0}(h^{(0)})$ を生成する（sk_0 は署名者の秘密鍵）．ただし $h^{(0)} = h_1^{(0)} || \ldots || h_n^{(0)}$ とする．

出力 文書 $\bar{M}^{(0)} = (\bar{M}_1^{(0)}, \ldots, \bar{M}_n^{(0)})$，ハッシュ値集合・署名のペア $(h^{(0)}, \sigma^{(0)})$

j 番目の墨塗り者（$j = 1, \ldots, m$）

入力 墨塗り文書 $\bar{M}^{(j-1)} = (\bar{M}_1^{(j-1)}, \ldots, \bar{M}_n^{(j-1)})$，$j$ 組のハッシュ値集合・署名のペア $(h^{(0)}, \sigma^{(0)}), \ldots, (h^{(j-1)}, \sigma^{(j-1)})$

1. 2 組のハッシュ値集合 $h^{(0)}$，$h^{(j-1)}$ を比較し，墨塗りされている部分文書の添字集合 $S = \{i | h_i^{(0)} \neq h_i^{(j-1)}\}$ を求める

2. 墨塗り（非開示）する部分文書の添字集合 $S' \supseteq S$ を定める．

3. 各部分文書 $\bar{M}_i^{(j-1)}$（$i = 1, \ldots, n$）から新しい部分文書

$$\bar{M}_i^{(j)} \leftarrow \begin{cases} H(\bar{M}_i^{(j-1)}) & \text{if } i \in S' \backslash S \\ \bar{M}_i^{(j-1)} & \text{otherwise} \end{cases}$$

を生成し，さらにハッシュ値 $h_i^{(j)} \leftarrow H(\bar{M}_i^{(j)})$ を求める．

4. 署名 $\sigma^{(j)} \leftarrow \mathsf{Sign}_{\mathsf{sk}_j}(h^{(j)})$ を生成する（sk_j は j 番目の墨塗り者の秘密鍵）．ただし $h^{(j)} = h_1^{(j)} || \ldots || h_n^{(j)}$ とする．

出力 墨塗り文書 $\bar{M}^{(j)} = (\bar{M}_1^{(j)}, \ldots, \bar{M}_n^{(j)})$，$j+1$ 組のハッシュ値集合・署名のペア $(h^{(0)}, \sigma^{(0)}), \ldots, (h^{(j)}, \sigma^{(j)})$

検証者

入力 墨塗り文書 $\bar{M}^{(m)} = (\bar{M}_1^{(m)}, \ldots, \bar{M}_n^{(m)})$，$m+1$ 組のハッシュ値集合・署名のペア $(h^{(0)}, \sigma^{(0)}), \ldots, (h^{(m)}, \sigma^{(m)})$，署名者および墨塗り者の公開鍵 pk_j（$j = 0, \ldots, m$）

1.（墨塗り文書確認） 各部分文書 $\bar{M}_i^{(m)}$（$i = 1, \ldots, n$）のハッシュ値 h_i を求め，$h_1 || \ldots || h_n$ が $h^{(m)}$ に等しくない場合には invalid を出力して終了する．

2.（署名検証） 各 j（$j = 0, \ldots, m$）に対し，公開鍵 pk_j とハッシュ値 $h^{(j)}$ を用いて署名 $\sigma^{(j)}$ を検証する．検証に失敗した場合には invalid を出力して終了する．

3.（墨塗り箇所の特定） 2 組のハッシュ値集合 $h^{(0)}$，$h^{(m)}$ を比較し，墨塗り部分文書の添字集合 $S = \{i | h_i^{(0)} \neq h_i^{(m)}\}$ を求める．

4.（墨塗り者の検証） $m+1$ 組のハッシュ値集合 $h^{(0)}, \ldots, h^{(m)}$ を用いて，墨塗りされた i 番目（$i \in S$）の部分文書の墨塗り者を特定する．ここで $h_i^{(0)} = \cdots = h_i^{(j-1)} \neq h_i^{(j)} = \cdots = h_i^{(m)}$ となるとき，j 番目の墨塗り者がこの部分文書を墨塗りしたと判定する．すべての $i \in S$ に対して墨塗り者が特定できた場合には valid を，そうでなければ invalid を出力して終了する．

図 1 提案墨塗り署名方式 PIAT 署名の処理概要

Fig. 1 A description of the proposed sanitizable signature scheme “PIATS.”

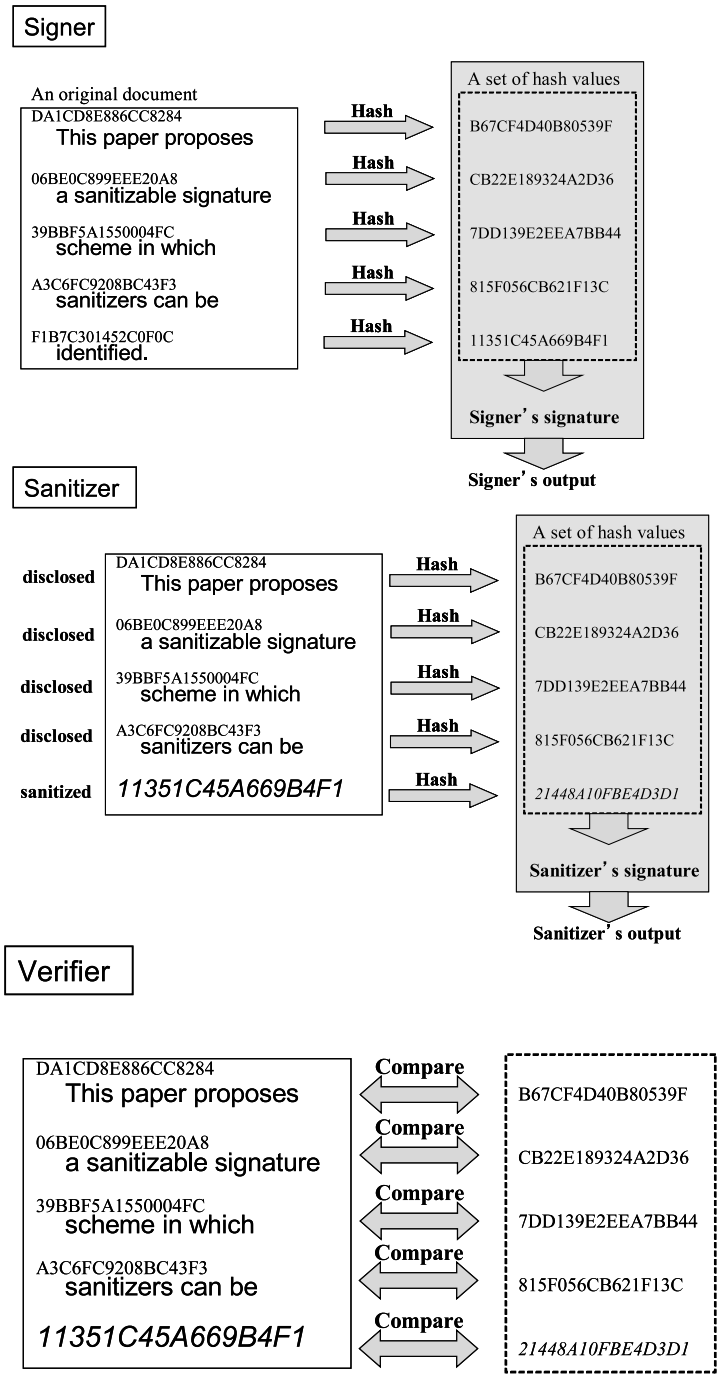


図 2 提案墨塗り署名方式 PIAT 署名
Fig. 2 An outline of the proposed sanitizable signature scheme "PIATS."

の墨塗り者は，$j-1$ 番目の墨塗り者が出力した墨塗り文書 $\bar{M}^{(j-1)}$ と，j 個のハッシュ値集合・署名ペア $(h^{(0)},\sigma^{(0)}),\ldots,(h^{(j-1)},\sigma^{(j-1)})$ を入力とする．このときハッシュ値集合 $h^{(0)}$ と $h^{(j-1)}$ を比較することで，j 番目の墨塗り者はどの部分文書が墨塗りされているか識別できる．そして新たに墨塗り文書 $\bar{M}^{(j)}$ とそれに対応するハッシュ値集合・署名 $(h^{(j)},\sigma^{(j)})$ を生成し，変更後の墨塗り文書 $\bar{M}^{(j)}$ と $j+1$ 個のハッシュ値集合・署名ペア $(h^{(0)},\sigma^{(0)}),\ldots,(h^{(j-1)},\sigma^{(j-1)}),(h^{(j)},\sigma^{(j)})$ を出力する．

検証者に開示されるのは，最後の（m 番目の）墨塗り者が出力した墨塗り文書 $\bar{M}^{(m)}$ と $m+1$ 個のハッシュ値集合・署名ペア $(h^{(0)},\sigma^{(0)}),\ldots,(h^{(m)},\sigma^{(m)})$ である．まず検証者は，各署名を署名者/墨塗り者の公開鍵を用いて検証することで，ハッシュ値集合の完全性を確認する．次にハッシュ値集合 $h^{(0)}$ と $h^{(m)}$ を比較して墨塗り部分文書を特定したうえで，墨塗りされた部分文書について $h_i^{(0)}=\cdots=h_i^{(j-1)}\neq h_i^{(j)}=\cdots=h_i^{(m)}$ となるような j を求める．このような j が求まった場合にはこの部分文書が j 番目の墨塗り者によって墨塗りされたことが特定できるし，求まらなかった場合には，不適切な墨塗り（たとえばすでに墨塗りされている部分文書をさらに墨塗りしたり，墨塗り時にハッシュ値以外の文字列に置き換えられたりした場合）がなされていたこと，さらにはそれをどの墨塗り者が行ったかを検出することができる．

3.3 安全性評価

墨塗り署名方式は，秘匿性（secrecy）と偽造不能性（unforgeability）を満たす必要がある[14),18)]．PIAT 署名の秘匿性と偽造不能性について，以下に簡単に考察する．ただしこれら考察は直感的なものであり，厳密な安全性の定義と証明については将来の課題としたい．

秘匿性とは，墨塗りされた部分文書からもとの部分文書のいかなる内容も漏れないことである．提案墨塗り署名方式では，墨塗り時に部分文書内容をハッシュ値で置き換えるように設計されているため，ハッシュ関数の一方向性を仮定する限り，墨塗りされた部分文書からもとの部分文書が復元されることはない．またすべての部分文書は先頭部分に部分文書識別子（乱数）が付与されるため，ある墨塗りされた部分文書から他の部分文書の内容が漏れることもない．これらの考察より，PIAT 署名は秘匿性を満たすことが分かる．

偽造不可能性とは，正当な墨塗り文書・署名ペアが作成できるのは墨塗り者だけであることを意味する．PIAT 署名では，署名者・墨塗り者は署名を生成する必要があるため，秘密鍵を持たない者は（通常の署名の偽造不可能性により）署名を生成することはできない．したがって，正当な秘密鍵を持つのは署名者・墨塗り者だけであると仮定すれば☆，PIAT 署名は偽造不可能性を満たすことが分かる．

3.4 PIAT 署名の付加的機能

PIAT 署名は，墨塗り文書における開示部分の完全性と非開示部分の秘匿性を保証するという基本機能に加え，以下のような付加的機能を持っている．

墨塗り者の特定 各墨塗り者は自分の秘密鍵に基づいた署名を出力するため，署名検証を通じて誰が墨塗り者であるかを特定できる．

不適切な墨塗りの特定 署名者/各墨塗り者は部分識別情報を出力するため，これら情報の整合性の検証を通じて不適切に墨塗りされた部分文書を特定できる．

3.5 データ量の削減

3.2 節で述べた PIAT 署名の処理アルゴリズムにおいて，検証者は n 個の部分文書，$m+1$ 個のハッシュ値集合（すなわち $(m+1)n$ 個のハッシュ値），$m+1$ 個の署名，$m+1$ 個の公開鍵を入力として必要とする．しかし i 番目の部分文書に対応する $m+1$ 個のハッシュ値 $h_i^{(0)},\ldots,h_i^{(m)}$ のほとんどの値は等しい（開示部分文書ならば $h_i^{(0)}=\cdots=h_i^{(m)}$，非開示部分文書ならば $h_i^{(0)}=\cdots=h_i^{(j-1)}\neq h_i^{(j)}=\cdots=h_i^{(m)}$ となる）ため，すべての値を保持するのは非効率的である．そこで署名者は n 個のハッシュ値 $h_1^{(0)},\ldots,h_n^{(0)}$ を従来どおり出力するが，墨塗り者はハッシュ値集合の代わりに，墨塗りした場合にのみ墨塗り情報の集合 $\{(i,j)\}$ を出力するよう変更する．ここで墨塗り情報 (i,j) は，i 番目の部分文書を j 番目の墨塗り者が墨塗りしたことを意味し，墨塗り者は自分が出力する墨塗り情報集合に対して署名を生成する．検証者は墨塗り文書の各部分文書に対応するハッシュ値が必要になるが，その部分文書が墨塗りされていなければハッシュ値は $h_i^{(0)}$ のままであり，墨塗りされていればハッシュ値は墨塗り部分文書の内容から求められる．このような変更により，検証者が必要とするハッシュ値の個数を n 個に削減することが可能となる．ただし，新たに墨塗り箇所と同じ個数の墨塗り情報を保持する必要が生じるため，ハッシュ値よりも墨塗り情報の方が情報量が小さい場合にはデータ量の削減が実現できている．オリジナル方式と改良方式のデータ量の比較を**表 1** に示す．なお本節で述べたハッシュ値の削減方法は，UNIX におけるソースコード管理ツール SCCS（Sorce Code Control System）で使用された方法を応用したものである．

4. 墨塗り署名方式の比較

本章では CES[18)]，SUMI-1，SUMI-2，SUMI-3，SUMI-4[15)]，SUMI-5[14)] および提案方式（PIAT 署名）の併用可能な署名方式，必要となる署名の個数，複数の墨塗り者による追加墨塗りの可否，および墨塗り者の特定の可否を比較する．結果を**表 2** に示す．

☆ さらには，署名者と墨塗り者は攻撃者でないことを仮定しているが，通常のディジタル署名では署名者が攻撃者でないことは暗に仮定されており，この仮定はその拡張と見なすことができる．

表 1 PIAT 署名の検証者が必要とするデータ量の比較
Table 1 A comparison of a verifier's input.

	部分文書	公開鍵	ハッシュ値	署名	墨塗り情報
オリジナル	n	n	$(m+1)n$	$m+1$	なし
改良方式	n	n	n	$m+1$	最大 n

表 2 墨塗り署名方式の比較
Table 2 A comparison of sanitizable signature schemes.

方式名	併用可能な署名方式	署名数	追加墨塗り	墨塗り者特定
CES-CV，CES-HT	任意	1	条件付きで可能	不可能
CES-RSAP CES-MEPR	特定 （RSA 型）	1	条件付きで可能	不可能
SUMI-1	任意	2^n	不可能	不可能
SUMI-2	任意	n	可能	不可能
SUMI-3	任意	1	可能	不可能
SUMI-4	任意	1	可能	不可能
SUMI-5	任意	1	可能	不可能
PIAT 署名	**任意**	$\boldsymbol{m+1}$	**可能**	**可能**

CES-RSAP，CES-MERP は限定された署名方式（RSA 型）としか併用できないのに対し，残りの方式は任意の署名方式と併用可能である．n 個の部分文書からなる文書の墨塗りに SUMI-1，SUMI-2 はそれぞれ 2^n，n 個の署名を必要とするのに対し，残りの方式は 1 個の署名しか必要としない点で効率的であるが，PIAT 署名は $m+1$ 個の署名を必要とする（m は墨塗り者の人数）．SUMI-1 以外の方式は複数の墨塗り者による墨塗りが可能であるが，CES-CV，SUMI-2，SUMI-3，SUMI-4，SUMI-5 に対しては追加墨塗り攻撃が（部分的に）可能となっている．PIAT 署名以外では墨塗り者の識別ができないのに対し，PIAT 署名は可能となっている．2 章で述べたとおり，CES-CV，CES-HT と SUMI-4 は本質的に同じ方式であり，類似した結果となっている．

5. まとめと課題

本稿は，複数の墨塗り者による墨塗りを可能としつつ，墨塗り者の特定が可能な新しい墨塗り署名方式を提案した．本署名方式は開示部分の完全性と非開示部分の秘匿性を保証可能なため，電子的な墨塗り文書の管理に適していると考える．しかし 3.3 節で述べたとおり，その厳密な安全性証明は与えられておらず，PIAT 署名の満たすべき安全性の定義とともに将来の課題としたい．特に墨塗り者が不正を行うような場合，たとえば 2 番目の墨塗り者は，次の墨塗り者または検証者に渡すデータから，1 番目の墨塗り者の出力した情報を削除し，自分がすべての墨塗りを行ったと主張することが可能であり，そのような場合の検討は必須であると考える．また 4 章でも述べたとおり，（オリジナルの）PIAT 署名の検証者は墨塗り者の人数に比例した入力データを必要とするため，オーバヘッドとなる可能性が高い．3.5 節で 1 つの削減法を述べたが，さらなる削減法についてはこれからの課題としたい．

近年の墨塗り署名技術の関連研究として，墨塗り者は墨塗りするのではなく，署名者によってあらかじめ定められた内容のうちの 1 つを選択するような方式が提案されている[2),10),11)]．本稿で提案した PIAT 署名でも，アルゴリズムの軽微な修正によって同様の機能を実現することが可能である：PIAT 署名のアルゴリズム（図 1）において，署名者は墨塗りの際に部分文書をそのハッシュ値によって置き換えていた．これをハッシュ値ではなく，（部分文書内容とは無関係な）任意の文字列に置き換えるようにアルゴリズムを変更すると，文書内容が変更可能であり，かつその変更を検証可能であるような署名方式が得られる．しかしこれらの署名方式は，（厳密な）墨塗り署名とは異なると考えることもできるため，このような署名方式に対する考察も将来の課題となろう．

参 考 文 献

1) 朝日新聞：隠したはずの個人情報丸見え 千葉市教委のホームページ，2006 年 8 月 1 日.
2) Ateniese, G., Chou, D., Medeiros, B. and Tsudik, G.: Sanitizable Signatures, *ESORICS 2005*, LNCS 3679, pp.159–177, Springer-Verlag (2005).
3) Bull, L., Stanski, P. and McG. Squire, D.: Content Extraction Signatures using XML Digital Signatures and Custom Transforms On-Demand, *WWW 2003*, pp.170–177, ACM

(2003).
4) Izu, T., Kanaya, N., Takenaka, M. and Yoshioka, T.: PIATS: A Partially Sanitizable Signature Scheme, *ICICS 2005*, LNCS 3783, pp.72–83, Springer-Verlag (2005).
5) 伊豆哲也，國廣 昇，太田和夫，武仲正彦：双線形写像を用いた墨塗り署名方式の安全性について，情報処理学会論文誌，Vol.47, No.8, pp.2409–2416 (2006).
6) 伊豆哲也，佐野 誠，國廣 昇，太田和夫，武仲正彦：Aggregate 署名を用いた墨塗り署名方式の提案，2007 年暗号と情報セキュリティシンポジウム（*SCIS 2007*），2C4-3 (Jan. 2007).
7) J-CAST:「墨塗り」が丸見え！東京地裁赤っ恥，2007 年 2 月 18 日．Available at http://www.j-cast.com/2007/02/18005589.html
8) Johnson, R., Molnar, D., Song, D. and Wagner, D.: Homomorphic Signature Scheme, *CT-RSA 2002*, LNCS 2271, pp.244–262, Springer (2002).
9) 加賀谷雅人，清藤武暢，四方順司，松本 勉：アグリゲート署名を用いた Content Extraction Signature の構成法について，2007 年暗号と情報セキュリティシンポジウム（*SCIS 2007*），2C4-4 (Jan. 2007).
10) Klonowski, M. and Lauks, A.: Extended Sanitizable Signatures, *ICISC 2006*, LNCS 4296, pp.343–355, Springer-Verlag (2006).
11) Kuwakado, H. and Morii, M.: Restrictively Sanitizable Signature Scheme, *2006 Symposium on Cryptography and Information Security* (*SCIS 2006*), 4A1-2 (Jan. 2006).
12) Miyazaki, K., Hanaoka, G. and Imai, H.: Digitally Signed Document Sanitizing Scheme from Bilinear Maps, *2005 Symposium on Cryptography and Information Security* (*SCIS 2005*), 3E3-5, pp.1471–1476 (Jan. 2005).
13) 宮崎邦彦，花岡悟一郎，今井秀樹：ビット単位で連続領域を墨塗り可能な電子文書墨塗り技術，2006 年暗号と情報セキュリティシンポジウム（*SCIS 2006*），4A1-1 (Jan. 2006).
14) Miyazaki, K., Iwamura, M., Matsumoto, T., Sasaki, R., Yoshiura, H., Tezuka, S. and Imai, H.: Digitally Signed Document Sanitizing Scheme with Disclosure Condition Control, *The Institute of Electronics, Information and Communication Engineers* (*IEICE*) *Trans. Fundamentals*, Vol.E88-A, No.1, pp.239–246 (Jan. 2005).
15) Miyazaki, K., Susaki, S., Iwamura, M., Matsumoto, T., Sasaki, R. and Yoshiura, H., Digital Documents Sanitizing Problem, *The Institute of Electronics, Information and Communication Engineers* (*IEICE*) *technical report*, ISEC 2003-20, pp.61–67 (May 2003).
16) 永村建索，左 瑞麟，岡本 健，岡本栄司：墨塗り者の指定と匿名性を実現した ID ベース型墨塗り署名，2007 年暗号と情報セキュリティシンポジウム（*SCIS 2007*），2C4-2 (Jan. 2007).
17) RSA Laboratories: PKCS #1 v2.1: RSA Encryption standard (June 14, 2002). Available at http://www.rsasecurity.com/rsalabs/node.asp?id=2125
18) Steinfeld, R., Bull, L. and Zheng, Y.: Content Extraction Signatures, *ICISC 2001*, LNCS 2288, pp.285–304, Springer-Verlag (2001).
19) 佐野 誠，伊豆哲也，國廣 昇，太田和夫，武仲正彦：部分情報の墨塗りと削除が可能な署名方式の提案，2007 年暗号と情報セキュリティシンポジウム（*SCIS 2007*），2C4-1 (Jan. 2007).
20) 行政機関の保有する情報の公開に関する法律，総務省 (1999). Available at http://law.e-gov.go.jp/htmldata/H11/H11HO042.html
21) 小西 寛（北陸無線データ通信協議会）：意見書（2003 年 6 月 30 日提出），総務省総合通信基盤局電波部電波政策課，2003 年 7 月 3 日公開．Available at http://www.soumu.go.jp/s-news/2003/pdf/030703_2_11.pdf
22) Suzuki, M., Isshiki, T. and Tanaka, K.: Sanitizable Signature with Secret Information, *2006 Symposium on Cryptography and Information Security* (*SCIS 2006*), 4A1-2 (Jan. 2006).
23) 武仲正彦，吉岡孝司：画像ファイルに対する部分完全性保証技術の実現，電子情報通信学会技術研究報告，ISEC 2005-69, pp.183–188 (July 2005).
24) Carnivoe Review Team Exposed!, an article of Wired News Reports (2000). Available at http://www.wired.com/news/politics/0,1283,39102,00.html
25) NYT Site Exposes CIA Agents, an article of Wired News Reports (2002). Available at http://www.wired.com/news/politics/0,1283,37205,00.html

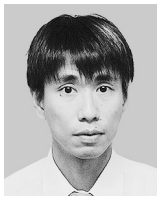
(平成 18 年 11 月 27 日受付)
(平成 19 年 6 月 5 日採録)

伊豆　哲也（正会員）

1967 年生．1992 年東京大学理学部数学科卒業．1994 年立教大学大学院理学研究科数学専攻博士前期課程修了．1997 年立教大学大学院理学研究科数学専攻博士後期課程退学．博士（工学）．1997 年より富士通株式会社および株式会社富士通研究所に勤務，現在に至る．情報セキュリティ，暗号理論の研究に従事．2001 年 Waterloo 大学（カナダ）客員研究員．1999 年暗号と情報セキュリティシンポジウム（SCIS 1999）論文賞受賞．2002 年コンピュータセキュリティシンポジウム（CSS 2002）優秀論文賞受賞．2005 年電子情報通信学会基礎・境界ソサイエティ功労賞受賞．2007 年科学技術分野の文部科学大臣表彰若手科学者賞受賞．電子情報通信学会，IACR 各会員．

金谷　延幸

1967 年生．1992 年群馬大学大学院工学研究科情報工学専攻修士課程修了．同年株式会社富士通研究所入社．現在，同社ソフトウェア&ソリューション研究所セキュアコンピューティング研究部に勤務．ソフトウェアセキュリティ，Web アプリケーションセキュリティの研究に従事．



武仲　正彦

1967 年生．1990 年大阪大学工学部電気工学科卒業．1992 年大阪大学大学院工学研究科電気工学専攻博士前期課程修了．同年より富士通株式会社および株式会社富士通研究所に勤務．主任研究員．公開鍵・共通鍵暗号の攻撃・実装技術，サイドチャネル攻撃，ネットワークセキュリティの研究に従事．2002 年コンピュータセキュリティシンポジウム（CSS 2002）優秀論文賞受賞．2005 年財団法人電気科学技術奨励会第 53 回電気科学技術奨励賞受賞．電子情報通信学会会員．

吉岡　孝司

1992 年富士通株式会社入社．株式会社富士通研究所にて並列・分散 OS の高性能化・高信頼化，および電子文書の原本性保証技術に関する研究開発に従事．1998 年東京工業大学像情報工学研究施設研究員．現在，株式会社富士通研究所ソフトウェア&ソリューション研究所セキュアコンピューティング研究部に所属し，電子署名応用技術の研究開発に従事．