

電子文書墨塗り問題

宮崎 邦彦^{†1,6} 洲崎 誠一^{†1,3} 岩村 充^{†2} 松本 勉^{†3} 佐々木 良一^{†4} 吉浦 裕^{†5}

†1 株式会社日立製作所システム開発研究所 〒244-0817 横浜市戸塚区吉田町 292

†2 早稲田大学大学院アジア太平洋研究科 〒169-0051 東京都新宿区西早稲田 1-21-1

†3 横浜国立大学大学院環境情報研究院 〒240-8501 横浜市保土ヶ谷区常盤台 79-7

†4 東京電機大学工学部 〒101-8457 東京都千代田区神田錦町 2-2

†5 電気通信大学 電気通信学部 〒182-8585 調布市調布ヶ丘 1-5-1

†6 東京大学大学院情報理工学系研究科 〒153-8505 東京都目黒区駒場 4-6-1

E-mail: †1{kunihiko, susaki}@sdl.hitachi.co.jp, †2 iwamuram@waseda.jp, †3 tsutomu@mlab.jks.ynu.ac.jp,

†4 sasaki@im.dendai.ac.jp, †5 yoshiura@hc.uec.ac.jp

あらまし 署名つき電子文書は、必ずしも署名したときそのまま利用されるとは限らない。たとえば、行政文書が情報公開制度に基づき開示されるときには、そこに記述された個人情報や国家安全情報は、通常「墨塗り」された上で開示される。この一連の手続きを従来の電子署名技術を使って実現しようとした場合、保管時に付与した署名が、文書の一部が墨塗りされたことにより、検証できなくなる可能性がある。本稿では、ある文書に対して施された署名が、その文書の一部を秘匿することによって検証できなくなる問題を「電子文書墨塗り問題」とよび、これに対応可能な電子文書の真正性保証技術を提案する。

キーワード 電子署名、情報公開、プライバシー保護

Digital Document Sanitizing Problem

Kunihiko MIYAZAKI^{†1,6} Seiichi SUSAKI^{†1,3} Mitsuru IWAMURA^{†2} Tsutomu Matsumoto^{†3}

Ryoichi SASAKI^{†4} and Hiroshi YOSHIURA^{†5}

†1 Systems Development Laboratory, Hitachi Ltd. 292 Yoshida-cho, Totsuka-ku, Yokohama-shi, 244-0817 Japan

†2 Graduate School of Asia-Pacific Studies, Waseda University 1-21-1 Nishi-Waseda, Shinjuku-ku, Tokyo, 169-0051 Japan

†3 Graduate School of Environment and Information Sciences, Yokohama National University 79-7 Tokiwadai, Hodogaya-ku, Yokohama-shi, 240-8501 Japan

†4 Faculty of Engineering, Tokyo Denki University 2-2 Kandanishikicho, Chiyoda-ku, Tokyo, 101-8457 Japan

†5 Graduate School of Information Science and Technology, The University of Tokyo 4-6-1 Komaba, Meguro-ku, Tokyo, 153-8505 Japan

E-mail: †1{kunihiko, susaki}@sdl.hitachi.co.jp †2 iwamuram@waseda.jp, †3 tsutomu@mlab.jks.ynu.ac.jp,

†4 sasaki@im.dendai.ac.jp, †5 yoshiura@hc.uec.ac.jp

Abstract Digital signature does not allow any alteration of the document. However, “appropriate” alteration should be allowed for some signed document because of other security requirements etc. Disclosure of official information is a typical example of this. Sensitive information such as private information should be sanitized from the original digitally signed document when it is disclosed. “Digital document sanitizing problem” is the problem that signed document cannot be verified if some part of the signed document is concealed. In this paper, we propose new digital signature techniques which can solve digital document sanitizing problem.

Keyword digital signature, information disclosure, privacy issues

1. はじめに

電子文書の安全性を支える重要な技術である現在の電子署名技術は、電子文書に対するいかなる改変も

検知できるように設計されている。この性質は、不正者による改ざんから電子文書を守るという意味では、非常に有用であるが、電子文書の有効活用という観点

からは、一切の加工が許されなくなるため、逆に障害となりうる。

この問題を端的に示す利用場面としては、行政機関等における情報公開が挙げられる。たとえば、次のような電子署名の利用形態が想定される。

「行政機関において、職員が職務上作成した文書（行政文書）を、作成者を明らかにし、また、改ざんを防止するために、電子署名を付された上で保管する。この文書が情報公開法に基づき開示されるときに、そこに記述された個人情報や国家安全情報が削除された上で開示される。」

従来の電子署名技術では、上記の一連の手続きに従って開示された文書の真正性、すなわち、文書作成者が誰であるか、また開示された文書はもともと作成された文書と同一であるか、を確認することができない。なぜなら、情報公開の過程で、文書の一部が削除されているからである。悪意による改ざんであらうと、プライバシー情報の保護のための個人情報削除であらうと、署名対象文書に対し、なんらかの改変が加えられた、という点では変わらない。結果として、従来の電子署名技術の利用では、「公開された文書の真正性保証」と、「プライバシー情報の保護」という2つの重要なセキュリティ要件を両立できず、どちらかをあきらめざるをえない。

この問題に対するシステムの解決策としては、個人情報等が削除された後の開示用の文書に対し別の電子署名を付してから公開する、という方法も考えられる。

しかしこの場合、公開された文書に付された署名から技術的に確認できることは、あくまでも、開示用に加工された文書が誰によって作成されたのか、またそれが作成されてから変更されていないか、という点であることに注意を要する。開示用に加工された文書と元々の行政文書との関係（同一性）については、保証し得ない。情報公開制度が、行政機関のアカウンタビリティ（説明責任）を果たすための制度であるということを考えて、個人情報等が削除された後の開示用の文書からでも、元々の行政文書との同一性を検証できることが望ましい。

本稿では、電子文書の一部を秘匿することにより、その真正性が確認できなくなる問題を「電子文書墨塗り問題（Digital Documents Sanitizing Problem）」と呼び、この問題に対する対策技術として、一部を秘匿した後であっても、元々の文書との（秘匿部分以外の）同一性を保証可能な電子署名方式を提案する。

以下、第2節において、上述の情報公開制度を例に挙げ、墨塗り問題に対応可能な電子文書の真正性保証技術（墨塗り技術）に求められる性質を明らかにする。

また第3節において、墨塗り技術の具体的な方式を提案し、その安全性について考察する。次に第4節において、関連技術との関係について述べた後に、第5節において、まとめを述べる。

2. 電子文書墨塗り問題

本節では、「行政機関の保有する情報の公開に関する法律」[2]（以下、情報公開法と呼ぶ）に基づく行政機関における情報公開制度の場合を例に挙げ、電子文書墨塗り問題の概要について述べる。また、墨塗り問題に対応可能な電子文書の真正性保証技術に求められる要件を整理する。

2.1. 情報公開制度における電子文書墨塗り問題

情報公開法に基づく情報公開の基本的な流れは、以下の通りである（図1）。

1. 行政機関の職員は当該行政機関の意思決定の際などに随時文書（行政文書）を作成し、適切に管理する
2. 開示請求者は、行政機関の長（または行政機関の長から委任された職員、以下、開示者と呼ぶ）に対し、開示請求を行う
3. 開示者は、開示請求者からの請求を受けて、開示請求に係る行政文書を開示する。ただし、個人に関する情報等、情報公開法第5条の各号に掲げられた情報（以下、「不開示情報」という）が含まれる場合には、不開示または当該部分を除いた（i.e.墨塗りされた）部分開示とする

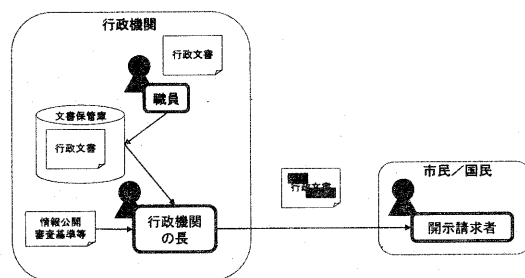


図1 情報公開の流れ

さて、情報公開制度が行政機関のアカウンタビリティ（説明責任）を果たすための制度であるということを考えて、上記の一連の流れに従って開示された文書を受け取った開示請求者が、以下の2点を確認できることが望ましい。

- A) 開示された文書が確かに職員によって作成された文書と同一であるか？（たとえば、情報公開時に開示者によって新たに捏造されたものでないか）
- B) さらに部分開示の場合は、開示された文書に対して適切な墨塗りがされているか？

後者については、さらに次の2つに細分化できる。

B-1) 墨塗り箇所は適切か？(たとえば情報公開法第5条の各号に掲げられた以外の情報を墨塗りしていないか)

B-2) 墨塗り方法は適切か？(たとえば墨塗り時に他の箇所の情報を書き換えていないか)

行政文書が電子文書である場合には、電子署名技術が上記Aを実現する上で有用な技術となる。すなわち、行政文書作成者である職員が、文書に電子署名を付した上で管理するようにしておけば、開示請求者はその署名を検証することで開示された文書と職員が作成した文書との同一性を確認可能である。

ただし、この方法は、部分開示の場合にはうまくいかないことに注意を要する。

なぜなら、部分開示の場合には、職員が署名を生成した後で、開示者によって文書の一部が削除されるため、署名対象であった元の行政文書に対する改変が生じていることになる。したがって、たとえ元の行政文書や開示文書に対する不正な改ざんがなかったとしても、開示請求者による署名検証処理は失敗してしまう。すなわち、上記Aを確認できない。またこれは、上記B-2に挙げた「墨塗り時に他の箇所の情報を書き換える」という不正行為を許してしまうことも意味する。

本稿では、この部分開示の場合に見られるような、ある文書に対して施された署名が、署名後にその文書の一部を秘匿することによって検証できなくなる問題を、**電子文書墨塗り問題**(Digital Document Sanitizing Problem)と呼ぶ。また、電子文書墨塗り問題への対応技術に求められる要件を整理し、具体的な方式を提案する。

なお、以降の議論では、上記B-1に関わる問題、たとえば、情報公開請求を受けたときに「公開すべき行政文書はどれか」「その文書のうちのどの部分を秘匿すべきか」を判断する方法など、については、特に述べない¹。本稿においては、これらは情報公開請求を受け付けた時点で、自動的に決定されるものとする。

2.2. 墨塗り技術

前節で述べた電子文書墨塗り問題への対応技術を、以下、墨塗り技術と呼ぶ。墨塗り技術は、次のような三者モデルの下で整理できる(図2)。

墨塗り技術とは、それぞれ以下に述べる振舞いに従う署名者、墨塗り者、検証者からなる三者モデルにおいて、最終的に検証者が受け入れる開示文書を作成可能な署名生成、墨塗り、署名検証技術のことである。

(署名者の振舞い) 署名者は、オリジナルの文書の

内容を保証するために署名を生成する。それ以外の目的では署名しない。また、署名対象文書のうちのどの部分が、将来的に墨塗りされるか分からない状態で署名しなければならない。

(墨塗り者の振舞い) 墨塗り者は、署名者がオリジナル文書に署名を付与した後のある時点において、開示範囲を決定し、検証者に開示する。署名者がオリジナル文書に署名を付与する以前には、開示範囲は決定できない。また、オリジナルの文書の内容を知っていてもよいが、あらたにオリジナルの文書を作り出すことはできない。

(検証者の振舞い) 検証者は、開示された文書が署名者によって保証されていることを確認できない限り、開示文書を受け入れない。

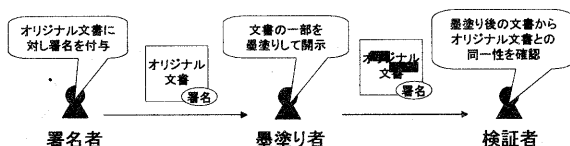


図2 墨塗り技術における各エンティティ

上記の三者モデルの各エンティティを前節で述べた行政機関における情報公開の場合と対応付けると、

署名者・・・行政機関の職員

墨塗り者・・・開示者(行政機関の長など)

検証者・・・開示請求者

となる。

次節において、この墨塗り技術に求められるセキュリティ要件を明らかにする。

2.3. 墨塗り技術に求められるセキュリティ要件

本節では、前節で定義した墨塗り技術に求められるセキュリティ要件を明らかにする。

プライバシー情報等の機密情報の墨塗りが可能であり、かつ、検証者によって墨塗り後の開示文書が受け入れられるためには、以下の要件を満たす必要がある。

墨塗り技術に求められるセキュリティ要件

(条件1) 開示文書に墨塗り部分が含まれていても検証が可能であり墨塗り以外の改変がなければ検証に成功すること

(条件2) 開示文書にオリジナル文書に対する墨塗り以外の改変があったときには検証が失敗すること

(条件3) 墨塗り部分に対応するオリジナル文書の情報が漏洩しないこと

(条件4) 墨塗り部分の情報を推定しようとする攻撃者が、開示文書自体を、推定結果の正当性を保証する手段として利用できないこと

¹ これらの点を適切に判断すること自体は、情報公開システムを設計する上では重要な課題であるが、本稿では独立して解決すべき課題とする。

(条件 1)は、従来の署名技術にはなかった墨塗り技術特有の特徴である。なお、この性質は、現代暗号理論に基づく通常の署名の定義(たとえば[1])によれば、ある種の改ざんを許す(したがって安全ではない)ことを意味することになる。しかし、本稿では、任意の改変(改ざん)を許すことと、「適切な」改変のみを許すことを、同一視すべきではない、という立場をとる。その上で、許される改変と、許されない改変を区別するための条件として挙げたのが、上記の(条件 2)である。これら 2 条件は併せて、開示文書がオリジナル文書の部分情報であるときかつそのときに限り検証が成功する、ことを意味する。

上記の(条件 3)は、墨塗りしたはずの情報が漏洩しないことを意味する。なお、具体的な方式設計によって、情報量的な意味で漏洩しない場合や、計算量的な意味で漏洩しない場合などがありうる。

これに対し、上記の(条件 4)は、墨塗り部分を前後の文脈等から推定した攻撃者にとって、その推定結果が正しいことを証明する材料として使われないようにすること、言い換えると、たとえ墨塗り部分が推定されたとしてもそれを否認できるようにすること、を意味する。

たとえば、署名つきオリジナルの文書の内容が「容疑者宮崎邦彦は犯行を否認した」であり、開示文書が「容疑者****は犯行を否認した」であったとする。すなわち、情報公開にあたり、オリジナルの文書から個人情報である「宮崎邦彦」が墨塗りされたとする。さらに、この開示文書を見た攻撃者が、前後の文脈等から「****」は「宮崎邦彦」ではないかと推定²したとする。このとき、攻撃者が「****」部分に、仮に「宮崎邦彦」を当てはめて検証を試みた場合に、検証に成功してしまったとすると、開示文書自体が、「****」部分は実は「宮崎邦彦」であった、ということを保証することになる。したがって、そのような方式は、墨塗り問題対応技術としては望ましくない。

次節において、上記(条件 1)～(条件 4)を満たす墨塗り技術を提案する。

3. 実現方式の提案

本節では、前節で定義したセキュリティ要件を満たす墨塗り技術を 4 方式提案し、それらを安全性・効率性の観点から比較する。

3.1. 方式 1

署名生成手順

1. オリジナル文書を構成要素(以降、ブロックと

²必ずしも墨塗り部分の直接解読によって推定されるとは限らない。前後の文脈や、オリジナル文書が作られたとされるときの社会情勢、ニュース等から、攻撃者が墨塗り部分を推定する場合も含まれる。

呼ぶ)に分割する。構成要素をどのように定めるかについては、たとえばオリジナル文書の先頭から 1 バイトごとにひとつの構成要素として定めてもよいし、あるいは、XML(eXtensible Markup Language)を使って記述された文書のようにならかじめ構造化された文書であれば、その最小構成要素を利用してもよい。以下、オリジナル文書を N ブロックの列とみなす。

2. オリジナル文書である N ブロックの列の、すべての部分列に対し、それぞれオリジナル文書作成者の秘密鍵を用いて署名を生成する (2^N 個の署名が生成されることになる)。

墨塗り手順

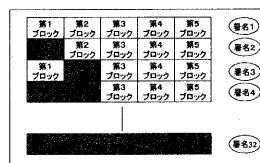
1. 開示対象である署名付きオリジナル文書の中から、不開示情報を含むブロックを選択する
2. 選択されたブロック以外のブロックからなるオリジナル文書の部分列を生成
3. 生成された部分列と、その部分列に対応する署名とからなるデータを、開示文書とする

検証手順

1. 通常の署名と同様に検証すればよい

方式 1 の場合

署名付きオリジナル文書



開示文書

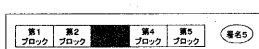


図 3 署名つきオリジナル文書と開示文書(方式 1)

セキュリティ評価

方式 1 では、開示文書は、オリジナル文書の部分列と、その部分列に対するオリジナル文書作成者の従来の電子署名とから構成される。したがって、従来の電子署名の検証技術を適用することによって、開示文書の真正性を確認可能であり、(条件 1)(条件 2)を満たす。また、開示文書には、不開示情報を含むブロックは含まれない。したがって、情報理論的な意味で(条件 3)を満たす。さらに開示文書に付された署名情報は、不開示情報を含むブロックとは無関係である、すなわち、開示文書に付された署名を生成するときに、不開示情報を含むブロックは入力情報として利用されていないため(条件 4)も満たす。

効率

- 2^N 回の署名生成処理を必要とする

3.2. 方式 2

署名生成手順

1. 方式1と同様に、オリジナル文書をブロックに分割する
2. 各ブロックのデータと当該ブロックがオリジナル文書中のどこに位置するかを示す位置情報とを結合したデータ（これを位置情報つきブロックと呼ぶ）に対し、署名を生成（i.e. N 個の署名を生成する）
3. 各位置情報つきブロックのデータ（ N 個）と、各ブロックに対する署名（ N 個）とからなるデータを、署名付きオリジナル文書とする

墨塗り手順

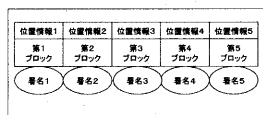
1. 方式1と同様に、開示対象である署名付きオリジナル文書の中から、不開示情報を含む位置情報つきブロックを選択する
2. 選択されたブロック以外の位置情報つきブロックと、各位置情報つきブロックに対応する署名（個数は開示ブロックの数に一致）とからなるデータを開示文書とする。

検証手順

1. 開示文書（ N 個以下の位置情報つきブロックと各ブロックに対応する署名とからなる）を、ブロックごとに通常の署名検証方法に従い検証し、すべてのブロックの検証に成功したときに「検証成功」、それ以外のときに「検証失敗」とする。

方式2の場合

署名付きオリジナル文書



開示文書

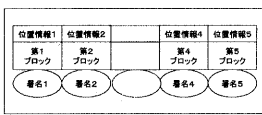


図4 署名つきオリジナル文書と開示文書（方式2）

セキュリティ評価

方式2では、開示文書は、オリジナル文書の部分列と、その部分列を構成する各ブロックに対するオリジナル文書作成者の署名とから構成される。したがって、従来の電子署名の検証技術をブロックの数だけ繰り返して適用することで、開示文書の真正性を確認可能であり（条件1）（条件2）を満たす。また、開示文書には、墨塗りブロックは含まれない。したがって、情報理論的な意味で（条件3）を満たす。さらに開示文書に付された署名情報は、不開示情報を含むブロックとは無関係である、すなわち、開示文書に付された署名を生成するときに、不開示情報を含むブロックは入力情報として利用されていないため（条件4）も満たす。

効率

N 回の署名生成処理を必要とする

3.3. 方式3

（注）後述するように、本方式は（条件4）を満たさない。

署名生成手順

1. 方式1と同様に、オリジナル文書をブロックに分割する
2. 各ブロックのデータのハッシュ値を算出し、算出された N 個のハッシュ値を結合したデータに対し、署名を生成（1 個の署名を生成）
3. 生成された署名（1 個）と、オリジナル文書とからなるデータを署名付きオリジナル文書とする

墨塗り手順

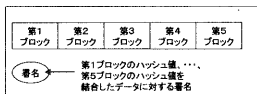
1. 方式1と同様に、開示対象である署名付きオリジナル文書の中から、不開示情報を含む位置情報つきブロックを選択する
2. 選択された各ブロックのハッシュ値と、それ以外の各ブロックと、署名とからなるデータを開示文書とする（i.e. 検索された各ブロック（墨塗りブロックに相当）についてはブロック自体ではなくハッシュ値を利用し、それ以外の各ブロック（開示ブロックに相当）についてはブロック自体を利用する）

検証手順

1. 開示文書のうち、（ハッシュ値ではなく）もとのデータ自体が与えられている各ブロックのハッシュ値を算出する
2. 算出された、または、開示文書に含まれるハッシュ値（合計 N 個）を結合したデータを、オリジナル文書作成者の公開鍵を用いて検証し、検証結果を出力する

方式3の場合

署名付きオリジナル文書



開示文書

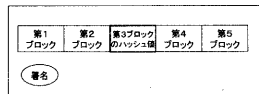


図5 署名つきオリジナル文書と開示文書（方式3）

セキュリティ評価

方式3では、上記の検証手順にしたがうことで、開示文書の真正性を確認可能である。したがって（条件1）を満たす。またハッシュ関数の衝突困難性を仮定すれば、オリジナル文書ブロックをハッシュ値ブロックに置き換える以外の変更は困難である。したがって（条件2）も満たす。開示文書に含まれる不開示情報に依存する情報は、墨塗りブロックに関するブロックのハッシュ値と、そのハッシュ値に依存して生成された署名

のみである。したがって、ハッシュ関数の一方向性を仮定すれば、(条件 3)を満たすことがわかる。

一方、前後の文脈等から墨塗りブロックを推測した攻撃者は、推測が正しかったかどうかを、推測したブロックのハッシュ値を計算し、開示されたハッシュ値と一致するか否かを調べることで確認可能である。推測が正しかった場合、推定結果の正当性を保証する情報として利用されるため、方式 3 は(条件 4)は満たさない。

効率

1 回の署名生成処理と N 回のハッシュ処理を必要とする

3.4. 方式 4

署名生成手順

1. 方式 1 と同様に、オリジナル文書をブロックに分割する
2. N 個のブロックそれぞれに対し、ブロックのデータとそのブロックに対して生成された乱数を結合したデータ（これを乱数つきブロックと呼ぶ）を生成する
3. 各乱数つきブロックのハッシュ値を算出し、算出された N 個のハッシュ値を結合したデータに対し、署名を生成（1 個の署名を生成）
4. 生成された署名（1 個）と、 N 個の乱数つきブロックとからなるデータを署名付きオリジナル文書とする

墨塗り手順

1. 方式 1 と同様に、開示対象である署名付きオリジナル文書の中から、不開示情報を含む位置情報つきブロックを選択する
2. 選択された各乱数つきブロックのハッシュ値と、それ以外の各乱数つきブロックと、署名とからなるデータを、開示文書とする（i.e. 検索された各ブロック（非開示ブロックに相当）については乱数つきブロック自体ではなくハッシュ値を利用し、それ以外の各ブロック（開示ブロックに相当）については乱数つきブロック自体を利用する）

検証手順

1. 開示文書のうち、（ハッシュ値ではなく）もとのデータ自体が与えられている各乱数つきブロックのハッシュ値を算出する
2. 算出された、または、開示文書に含まれるハッシュ値（合計 N 個）を結合したデータを、オリジナル文書作成者の公開鍵を用いて検証し、検証結果を出力する

方式 4 の場合

署名付きオリジナル文書

乱数 1	乱数 2	乱数 3	乱数 4	乱数 5
第 1 ブロック	第 2 ブロック	第 3 ブロック	第 4 ブロック	第 5 ブロック

署名

第 1 乱数つきブロックのハッシュ値、...、第 5 乱数つきブロックのハッシュ値を結合したデータに対する署名

開示文書

乱数 1	乱数 2	乱数 3	乱数 4	乱数 5
第 1 ブロック	第 2 ブロック	第 3 乱数つきブロックのハッシュ値	第 4 ブロック	第 5 ブロック

署名

図 6 署名付きオリジナル文書と開示文書（方式 4）

セキュリティ評価

方式 4 が、(条件 1)～(条件 3)を満たすことについては方式 3 と同様である。さらに、方式 4 の場合は、前後の文脈等から開示不適当なブロックを推測した攻撃者が、推測が正しかったかどうかを、ハッシュ値を比較して調べることは困難である。

なぜなら、仮に推測したブロックの情報が正しかったとしても、結合される乱数が正しくなければハッシュ値が一致しないからである。また、乱数は前後の文脈等とは無関係に生成されるため、乱数を推測することは著しく困難である。したがって方式 4 は(条件 4)も満たす。

効率

1 回の署名生成処理と N 回のハッシュ処理と N 回の乱数生成処理を必要とする

3.5. 各方式の比較

以上、本稿では、墨塗り技術として 4 方式を提案した。表 1 にこれらの比較を示す。

表 1 墨塗り技術各方式の比較

	条件 1	条件 2	条件 3	条件 4	効率 (署名回数)
方式 1	○	○	◎	○	2^N
方式 2	○	○	◎	○	N
方式 3	○	○	○	—	1
方式 4	○	○	○	○	1

○は条件を満たすことを示す。なお条件 3 については情報量的に満たすものを◎、計算量的な仮定の上で満たすものを○で示す。効率は一文書あたりに要する署名回数を示す。

処理の効率性、安全性等を総合的に勘案すると、この中では方式 4 がもっとも実用的であると考えられる。

4. 関連技術

本稿で提案した電子文書墨塗り問題と関連する技術としては、下記のような技術が挙げられる。いずれも本稿での問題意識とは差異が見られる。

Blind Signature[3] Blind Signature は、平文を見せずに署名してもらう方法であり、暗号文に対し署名を付し、それを復号して署名つき文書を得ることができる技術である。本稿で扱う墨塗り技術のように、署名つき文書の任意の部分の後から秘匿することについては考慮

されていない。

XML Signature, XML encryption[4][5] XML signature, XML encryption は、部分データに対する署名生成や暗号化をサポートしている。また、署名した後に暗号化する、といったこれらの組み合わせも可能である。しかし、署名対象データを後から部分的に秘匿し、かつ秘匿したまま署名検証できるようにする、といった墨塗り技術が対象とするような利用方法について考慮されていない。

Dual Signature[6] Dual Signature は SET(Secure electronic transaction)の規格中で定められた署名方式で、Cardholder が Merchant に送った注文書を、そこに含まれる支払い方法に関する情報を隠したまま Merchant が検証できるようにするために利用されている。Dual Signature の場合は、署名生成時にあらかじめどの部分を隠すかが決まっているが、本稿で述べた墨塗り技術の場合は、後々どの部分が隠されるかわからない状況で署名生成できる必要がある。

5. まとめ

本稿では、情報公開における「墨塗り」を例に挙げ、署名つき電子文書の一部を秘匿することによって署名の検証が不可能となる問題「電子文書墨塗り問題」とその対策の必要性を提起した。

また、その対策技術に求められるセキュリティ要件を整理したうえで、電子文書をブロックに分割し複数の署名を付与する方式や、ハッシュ関数を用いる方式など、4つの具体的な対策方式を示した。さらにそれらの方式について、安全性・効率性の観点から比較を行った。

本稿で提起した電子文書墨塗り問題は、デジタル社会における情報公開において、開示文書の真正性確保とプライバシー保護という2つの重要なセキュリティ要件の両立を図る上では、避けられない課題である。また、その対策技術である墨塗り技術は、情報公開の場面だけではなく、署名つき文書を抜粋引用した概要資料から元の文書の真正性を確認できるようにするなどさまざまな応用が考えられる。

今後はさらに安全性についての評価を精細化し、またより効率的な方式を開発することが課題である。

謝辞 本稿の執筆にあたり、活発にご議論いただいた株式会社日立製作所の松木武、猪股宏文、手塚悟、野山英郎、青島弘和の各氏につつしんで感謝の意を表する。また、宮崎邦彦は、本稿の執筆にあたり、ご意見いただいた東京大学生産技術研究所の今井秀樹教授ならびに今井研究室の方々にあわせて感謝の意を表する。

文 献

- [1] 岡本龍明，山本博資，「現代暗号」，産業図書，(1997)。
- [2] 行政機関の保有する情報の公開に関する法律（平成十一年五月十四日法律第四十二号）
- [3] D. Chaum. Blind signatures for untraceable payments. In Advances in Cryptology: Proceedings of Crypto 82, pages 199-203. Plenum Press, New York and London, 1983, 23-25 August 1982
- [4] XML signature, <http://www.w3.org/TR/xmlsig-core/>
- [5] XML encryption, <http://www.w3.org/TR/xmlenc-core/>
- [6] SET Secure Electronic Transaction Specification Book 1: Business Description Version 1.0 May 31, 1997