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

2006－CSEC－34 (52)
2006／7／21

告発文書から告発者の発覚を防ぐ公益通報者保護技術の提案

多田 真崇† 高塚 光幸‡ 増渕 孝延‡ 佐々木 良一‡

†,‡東京電機大学工学研究科情報メディア学専攻 〒101-8457 東京都千代田区神田錦町 2－2

E-mail: † tada@isl.im.dendai.ac.jp, ‡ {takatsuka, masubuchi}@isl.im.dendai.ac.jp, ‡ sasaki@im.dendai.ac.jp

あらまし

自分の所属している企業，または取引先の企業が不正を行っている事実を知り，匿名で公益通報を行いたいと考える場合は多い．しかし，不正行為の証拠である不正者の署名付き電子文書の内容から通報者が発覚してしまっては匿名で告発する効果がまったく発揮されない．そこで，電子文書から自分に関連する情報を秘匿するために墨塗りを施したいと考えたとしても，墨塗りを施した電子文書に告発される側が再度署名を施すとは考えにくいため，証拠性が確保できない．本研究では，この問題を解決するため，自分に関連する情報を墨塗りで秘匿しつつ，証拠性を確保するために不正者の署名を検証可能な状態を保つ電子文書墨塗りシステムの提案を行う．

キーワード 電子文書墨塗り，グループ署名，内部告発，公益通報，プライバシ保護

Proposal on Whistle-blower Protection Technology to Prevent the Exposure of Accuser from an Indictment Document

Masataka TADA† Mitsuyuki TAKATSUKA‡ Takanobu MASUBUCHI‡ and Ryoichi SASAKI‡

†,‡ Engineering graduate course information media studies specialty, Tokyo Denki University 2-2 Nishiki-cho, Chiyoda-ku, Tokyo, 101-8457 Japan

E-mail: † tada@isl.im.dendai.ac.jp, ‡ {takatsuka, masubuchi}@isl.im.dendai.ac.jp, ‡ sasaki@im.dendai.ac.jp

Abstract

When the person who knows the fact that the enterprise to which he/she belongs or his/her customer's enterprise do wrong, he /she sometimes would like to whistle-blow it with anonymity. However, if the content of an electronic document with the signature of the illegal person that is the evidence of misbehavior is used to guess who the whistle – blower is, it is difficult to keep the anonymity of the whistle blower. The evidence of an electronic document disappears when he/she sanitizes on an electronic document to prevent the whistle-blower being identified. However, it is not easy to think that the defendant signs again. In this study, we propose the electronic document sanitizing system that keeps in the state that the illegal person's signature can be verified to secure evidence hiding whistle-blower's information secretly by the sanitizing to solve this problem.

Keyword Sanitizing, Group Signature Scheme, Whistle-blowing, Privacy Issues

1. はじめに

企業の不正を報告する方法の一つに公益通報がある．近年，いくつかの企業が起こした不祥事がこの公益通報によって明らかにされ，不祥事の対応を迫られる事例が多数報告されている[6]．また，2006 年には公益通報者保護法という公益通報者を保護する内容を含んだ法律も施行された．これらのことから，社会の公益通報に対する関心がおのずと高まってきていると判断できる．しかし，公益通報はいくつかの大きな問題を孕んでいることもまた事実である．

以下に告発を行った場合に問題が発生した二つの事例を挙げる．

(1) 永田メール事件

民主党の永田元議員がジャーナリストから堀江氏が作成したとされる電子メールを入手し，それを証拠として国会の場において自民党幹事長の身内の不正を暴こうとした．しかし，電子メールには正当性を証明する電子署名などは存在せず，後にこの電子メールは偽造されたものであることが判明した．

(2) トナミ運輸における冷遇問題

トナミ運輸が他社と違法カルテルを結んでいたことを知った従業員が，この不正行為を実名で公益通報した．その後，従業員は企業からの非情な冷遇を受けた．

以上の二つの問題から判明した課題として，告発を行おう

とした場合には不正行為の証拠の正当性を確保しなければならないということと，公益通報時における公益通報者のプライバシが保護されなければならないといったことが重要な課題であることが浮かび上がってくる．そして現在，これらの課題を解決し，公益通報者を支援するためのシステムや技術の開発が必須であることは言うまでも無い．

本研究では，既存の電子文書墨塗り技術を改良し，システムに組み込むことによって，公益通報を支援するシステムの実現を目指す．

2. 公益通報における匿名性確保の必要性

ここでは公益通報を行う際に，公益通報者の匿名性を確保しなければならない理由と匿名性を定義する際に必要となってくる要素(要件)について説明する．

2.1. 匿名性の必要性

1.の部分でも触れたが，実名での公益通報には非常に大きなリスクが伴う．リスクには，あからさまな冷遇などの会社からの報復措置が考えられる．このような報復措置に恐れ，公益通報を思い止まってしまうという状況を生み出さないためにも，公益通報者の匿名性を確保することが重要であることは明らかである．

2.2. 匿名性確保に必要な要件

A) 発信元秘匿

公益通報を行う際，発信元から公益通報者が特定されないよう秘匿する．この要件を満たす技術としては，匿名通信路，秘密通信路などに関するいくつかの提案がなされているがまだ課題も多い．

B) 署名者秘匿

告発時における証拠データの証拠性を高めるために証拠データに署名を施すことは有効な手段である．しかし，実名での告発は高いリスクが伴うので，グループ署名やリング署名などの特殊な署名を用いることによって，署名者(公益通報者)が企業に所属していることを匿名で証明することにより，署名者の情報を秘匿しながらも証拠性の向上を実現することが出来る．

C) 証拠文書内の公益通報者関連情報の秘匿

不祥事の証拠データ(電子文書など)から公益通報者に関連する情報を秘匿することによって，公益通報者の発覚を防ぐ必要がある．たとえば，公益通報者に向けた会社幹部などからの指示を記述した電子文書であれば，指示対象者である自分の名前に墨を塗るなどして，公益通報者が誰であるかわからなくする必要がある．

しかし，これによって文書の証拠性が失われてはならないという問題も同時に存在する．たとえばメールの文書に会社幹部の署名がなされている場合に限り，その文書は証拠性を持つ．しかし，何も対策をしないで墨を塗ってしまうと，墨を塗った部分以外を改ざんしてもわからなくなり，証拠性が失われてしまう．ゆえに，墨を塗っても証拠性が確保される方式を提案する必要がある．

3. 従来の公益通報システム

ここでは既存の公益通報システムの一つとして，エシックスポイント(Ethicspoint)社が行っているウェブ・ベースの公益通報システム[7]について解説する．

3. 1. エシックスポイント社の公益通報システム

1. 告発者が同社の行っているウェブ・サイトに接続し，専用フォーマットを使い告発内容を記入し，送信する．
2. 送信されてきたデータを同社が検証し，ウェブ・サイトを経由して告発者と質疑応答を繰り返し，情報の信憑性と事実関係の詳細な確認作業を繰り返す．
3. 告発者は通常，送付から 48 時間後に特殊なパスワードを使って特定のサイトにログインし，同社からの質問を閲覧，これに回答し，対策の進捗状況を確認できる．
4. 一定の検証作業を経て，提言を盛り込んだ情報が予め指定された取締役，社外監査員などに渡った時点でサービスが終了する．

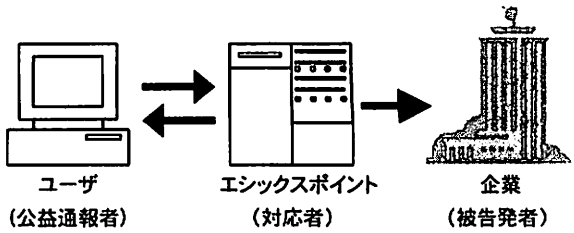

図1　既存の公益通報システム

3.2. 従来システムの問題点

エシックスポイント(Ethicspoint)社の行っている公益通報支援システムでは，公益通報者のプライバシを確保するため，一貫して完全な匿名によりシステムを実現している．つまり，要件 A) 発信元の第三者への秘匿や，要件 B) 署名者の秘匿といった要件は満たしている．しかし，証拠内容を提出し，その内容から告発者を特定できないとは言い切れない．つまり，要件 C) 証拠文書内の公益通報者関連情報の秘匿という要件を満たしていない．

今までは，要件 A), B) に関する研究は比較的盛んに行われてきた[1]．しかし，要件 C) に関する研究はいまだ行われていないという現状がある．

そこで我々は，既存の電子文書墨塗り技術[2]を改良し，この要件を満たす新しい電子文書墨塗り技術を用いた公益通報システムを提案する．

提案技術は，電子文書墨塗りという観点からは，「署名者と墨塗り者が協力関係にない場合の墨塗り問題」に対する改良技術として位置づけることができる．

4. 提案方式

本節では，公益通報者の匿名性を確保するために不正行為の証拠となる電子文書から公益通報者の関連情報を墨塗りした場合においても，電子文書に対する不正者の電子署名を検証可能な状態を保つことを可能にする技術を提案する．

4.1. 前提条件

前提条件として，以下の三つの条件を設定する．

1. 文書に対する署名は常に行われるようになっている．
2. メールの発信元は秘匿できる仕組みが用意されている．
3. IC カード内に保存された秘密鍵 S は取り出せないものとする．

4.2. 従来の墨塗り技術

(1) 署名付き文書に単純に墨を塗った場合の問題

署名付きの電子文書に墨塗りを行ってしまうと，文書の改ざんとみなされ，署名検証に失敗してしまうという問題が発生する．これを電子文書墨塗り問題[2]と呼ぶ．この問題を解決するために提案された技術として電子文書墨塗り技術がある．いくつか提案されている墨塗り方式のうち以下の (2) において SUMI-4 を説明する．

(2) 電子文書墨塗り技術(SUMI-4 方式[3])

SUMI-4 方式では，署名者，墨塗り者，検証者に対して以下のような条件を設けている．

- 署名者は，ある文書の内容を署名することで保証する者と定義する．署名を行う際は，対象文書のうちどの部分が墨塗りされるかわかってはならない．
- 墨塗り者は，署名者が署名した文書の非開示部分に対して墨塗り処理を行い，検証者に開示する．墨塗り処理の条件は，署名時に開示範囲を決定できないこと，新たな文書を作成することは出来ないことである．
- 検証者は，開示された文書が署名者によって署名されたものかを検証する．検証条件は非開示部分以外の開示部分が署名者により内容の正当性が保証されているかである．

以下に墨塗りの手順を示す．

1. オリジナル文書を N 個のブロックに分割する．
2. N 個のブロックに対して，それぞれ乱数を生成した乱数を結合したデータ（以下，乱数付きブロックと呼ぶ）を生成する．
3. 各乱数付きブロックのハッシュ値を算出し，生成されたN個のハッシュ値を結合したデータ（HMRとする）に対して，署名者の秘密鍵Skで署名を生成する（1個の署名を生成）．
4. 生成された署名（1個）と，N個の乱数付きブロックからなるデータを署名付きオリジナル文書とする．

署名付きオリジナル文書を図2に示す．

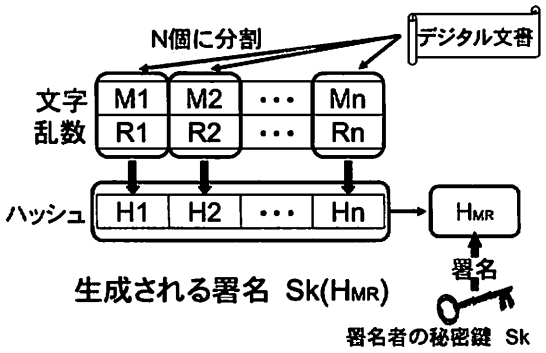

図 2　SUMI-4 署名生成手順

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，不開示情報つきブロックを選択する
2. 選択されたかく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．

この開示文書を図3に示す．

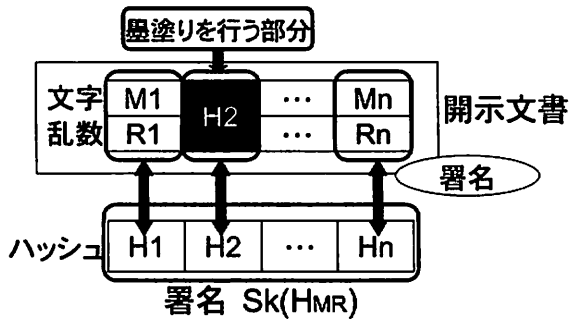

図 3　SUMI-4 墨塗り手順

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復号し，検証する

この検証手順を図4に示す.

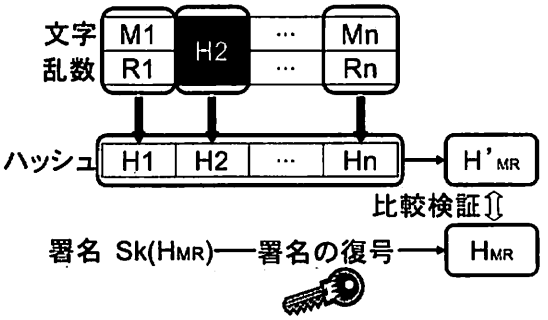

図4　SUMI-4 署名検証手順

(3) SUMI-4 を本方式に適用する場合の問題点

SUMI-4 では，署名者と墨塗り者が協力者関係にあった．しかし，本研究で提案するシステムでは署名者と墨塗り者は被告発者と告発者という非協力者関係にあり，署名者が電子文書をブロック分割し，乱数との排他論理和のハッシュ値を生成するようなことは考えられない．よって本方式に SUMI-4 を適用することができない．そこで我々は，被告発者のデジタル署名付き電子文書の墨塗りを施しても，署名検証を可能にする方式を考案した．

4.3. 提案方式

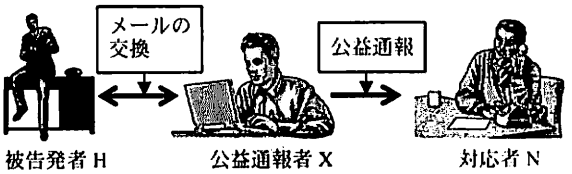

図5　システム構成図

まず，状況設定として図5に示すように，不正者である被告発者 H，不正行為を発見し公益通報を行おうと考えている公益通報者 X，X からの公益通報を受け，その対応を行う対応者 N の三者を考える．

X は H とのやり取りにおいて不正行為の証拠である文書 M を得る．X は M の中から自分に関する情報を提案方式の電子文書墨塗り技術を使い秘匿する．そうして作成された M'と後述の 4.6.グループ署名生成方式の一例内における署名生成部分で記述した方法で作成されたグループ署名 σ_G，N の公開鍵 P_Nで乱数 R を暗号化した P_N(R)と h(M)という五つのデータを N に送信する．N は IC カード内に保存された秘密鍵 S_Nにより IC カード内において R_1，R_2を取り出し，それらのデータをもとに M を復元し，h'(M)を生成する．署名検証済みの h(M)と得られた結果 h'(M)を比較検証することにより，署名の正当性を検証する．こうすることにより，証拠の正当性が向上する．

4.4. フロー

4.4.1. 事前準備

公益通報者 X は，以下の作業を実行し，必要なデータを揃えておく．

(1) 企業のグループに登録し，グループ署名を生成する準備(4.6.2.参照)をする．

(2) 対応者 N の公開鍵 P_Nを準備する．

(3) 被告発者 H の不正行為の証拠である M，H の電子署名 S_H(h(M))の入手・保管を実施．

4.4.2. 告発

公益通報者は，電子文書 M から自分に関する情報を秘匿するために提案方式の電子文書墨塗り技術を用いる．まず，M を M1~Mn にブロック分割し，秘匿したいと考える部分と乱数の排他論理和をとる．公開部分と非公開部分（排他論理和）の集合を M'とする．こうして得られた M'と乱数 R を対応者 N の公開鍵 P_Nで暗号化した P_N (R_i)，M から生成したハッシュ値 h(M)，被告発者 X の M に対する電子署名 S_H(h(M))，ならびに h(M)に対するグループ署名 σ_G (4.6.3.参照) というデータを対応者 N に送信する．

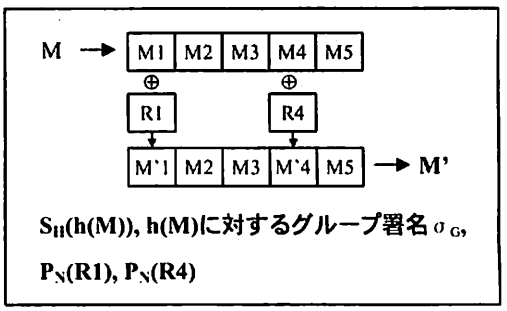

図6　関連情報墨塗り処理済データ

4.4.3. 検証

対応者 N は Trusted Third Party とみなした IC カード内において，P_N (R_i)を IC カード内に保存された N の秘密鍵 S_Nを用いて復号し，R を取り出す．取り出された R と M'の排他論理和をとり，M を復元し，h'(M)を得る．IC カードから対応者 N が参照できる結果は h'(M)のみであり，一時的に復元された M や R_iは参照できない．対応者 N は得られた結果 h'(M)と被告発者 A の電子署名 S_H (h(M))を検証した結果 h(M)を比較・検証し，墨塗りされた文書 M'が M から作成された事実を確認する．また，M に墨塗りを施し，告発を行った者が内部の人間であることを h(M)に対するグループ署名 σ_Gを検証し確認する．具体的には，図7を参照していただきたい．

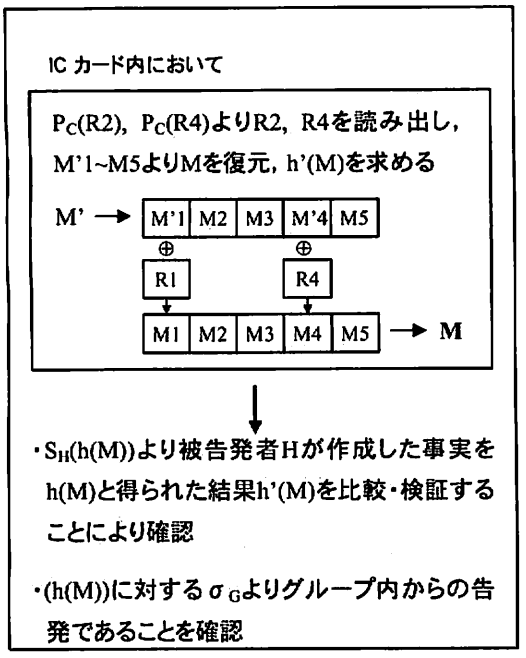

図7　対応者による検証作業

4.5. 既存方式(SUMI-4)と提案方式の相違点

1. 非開示部分の墨塗り実現方法として，既存方式がブロックと乱数の排他論理和のハッシュ値を公開するのに対し，提案方式ではブロックと乱数の排他論理和を公開する
2. 提案方式では，墨塗り部分に使用した乱数を対応者（検証者）が Trusted Third Party 内で復号可能にするために，対応者の公開鍵で乱数を暗号化する
3. 提案方式では，署名者ではなく墨塗り者が電子文書をブロック分割することが可能である
4. 署名者と墨塗り者が非協力関係にあっても，墨塗り者は墨を塗ることが可能である

4.6. グループ署名の概要と提案方式の位置づけ

グループ署名方式は D.Chaum[8]らが提案した特殊な署名方式であり，複数のメンバーからなるグループに所属するユーザが生成した署名を検証することにより，グループのメンバーであることは確認できるがグループの誰が作成したかを特定することが困難であるという特徴を持つ署名方式であり、いくつかの方式が提案されている．グループ署名には知識の署名と呼ばれる技術が用いられており，これはある値を保持していることを値に関する情報を明かさずに検証者に確認させる技術である．さらにグループ署名では，グループ管理者 GM と追跡管理者 EM が協力することにより，グループ署名から署名者を特定することが可能である．

以下に，D.Chaum[8]らの方式をベースにしたグループ署名の，グループへの登録から有事の際の署名者追跡までの手順の中に，4.4.で説明した方式を図8で示すように位置づけて説明する．

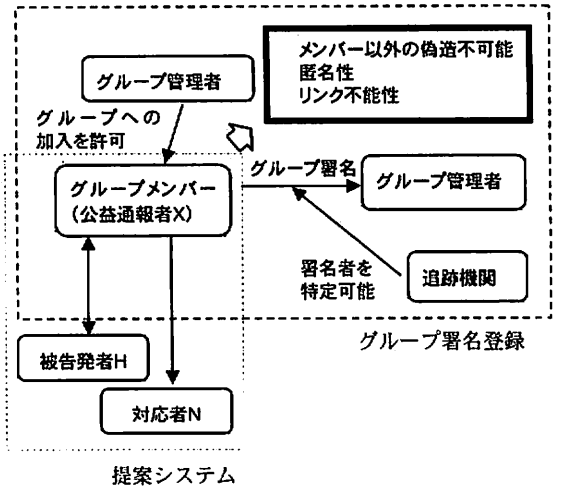

図8　グループ署名と提案方式の関係性

4.6.1. 準備

A) グループ管理者 GM は公開鍵と秘密鍵のペアを

$$P_G = h^{S_G} \bmod p$$

を計算し，作成する．S_G は GM の秘密鍵として保持し，P_G はグループ公開鍵として公開する．

B) 追跡管理者 EM は公開鍵と秘密鍵のペアを

$$P_E = g^{S_E} \bmod p$$

を計算し，作成する．S_E は EM の秘密鍵として保持し，P_E はグループ公開鍵として公開する．

4.6.2. 登録

1. ユーザ A（公益通報者 X を含む）は個人用の公開鍵と秘密鍵のペアを

$$P_A = g^{S_A} \bmod p$$

計算し，作成する．また，P_A と S_A が正しく作成されたことの知識の署名 SPK_A を生成する．また，A のデジタル署名関数を $Sign_{SA}$ として，S_A と SPK_A に対するデジタル署名 $Sign_{SA}(S_A, SPK_A)$ を作成する．A は(P_A , SPK_A , $Sign_{SA}(S_A, SPK_A)$) をグループ管理者 GM に送信する．

2. GM は SPK_A と $Sign_{SA}(S_A, SPK_A)$ の正当性を確認した後，メンバー証明書: $\sigma_A = Sign_{SG}(P_A)$ を作成し，A に送信する．
3. A は送られてきたメンバー証明書の正当性を検証する．正当性を確認できたら，S_A をメンバー秘密鍵，σ_A をメンバー証明書として所有する．
4. GM は(P_A , SPK_A , σ_A , $Sign_{SA}(S_A, SPK_A)$) をメンバーリストとして公開する．

4.6.3. 署名生成

ユーザ A（4.4 においては公益通報者 X）はメッセージ M

に対して，秘密鍵 S_A とメンバー証明書 σ_A を正しく持っていることを証明する知識の署名（メンバ証明）：$SPK_{\sigma,x}$ と σ_A を追跡管理者のグループ公開鍵 P_E で暗号化した

$$c = E_{PE}(\sigma_A)$$

を作成する．また，P_A に対応する秘密鍵 S_A を持っていることを証明する知識の署名 SPK_C を作成する．最後に A は M とともに (4.4.においては，M'，$P_N(R_i)$, h(M), S_H(h(M))とともに) $\sigma_G = (SPK_{\sigma,x}, c, SPK_C)$ をグループ署名として送信する．

4.6.4. 署名検証

検証者（4.4 においては対応者N）は知識の署名 $SPK_{\sigma,x}$ と SPK_C を検証し，グループメンバーが生成した署名であることを確認する．

4.6.5. 追跡

1. 追跡管理者 EM は，S_E を用い c からメンバー証明書である σ_A を復号し，これをグループ管理者 GM に送信する．
2. GM は σ_A を発行したメンバーを検索し，特定する．

4.6.6. 安全性

グループ署名方式 σ_Gは、次の条件を満たすとき安全であることが保障される[1][4].

Unforgeability ： グループ管理者GMと正しく登録プロトコルを実行し$cert_U$およびsk_Uを取得したグループメンバーUのみが VERIFY (PK; pkM; pkT; m; s) = 1 となるグループ署名s を作成できる．

Anonymity ： あるメッセージM に対する正当なグループ署名 s を与えられたとき追跡管理者EMのほかは実際の署名者を特定することは計算量的に困難である．

Unlinkability ： 2 つの異なる正当な署名が同じメンバーU によって作成されたものかどうか判定することは計算量的に困難である．

No framing ： グループのメンバーU も，たとえグループ管理者GM，または追跡管理者EMであっても，他のグループメンバーU' が署名者として追跡されるような署名を作成できない．

Traceability ： 追跡管理者EMとグループ管理者Mが協力した場合のみ，正当な署名から実際の署名者を特定できる． どちらも単独では署名者を追跡することはできない．

Coalition-resistance ： グループのメンバー集合の任意の部分集合が結託しても，検証を通過し，結託したメンバーを追跡管理者EMが誰も追跡できない署名を作ることはできない．

以上は、グループ署名自身の安全性であるが、墨塗り問題に対する安全性については、以下に示すとおりである。

Confidentiality ： 墨塗り部分Miに対応するRiは、TTR（ICカード）内でのみ復号されるので、検証者（4.4.では対応者N）であっても知ることができない。よって墨塗り部分の安全性は保たれる。

4.7. 今後の課題

今後は，実装の検討を進めていきたいと考えている．その際に特にどのようなデバイスを用いるか対応者の設定なども考慮しつつ，実現していきたい．また公益通報システムの完成度を上げるためにほかの技術の可能性も検討していきたい．

5. まとめ

本研究では，公益通報時に用いる電子文書墨塗り技術とこれを用いた一連のシステムを提案した．既存の公益通報システムとの違いとして，コンテンツ（証拠書類など）から公益通報者が判明することを防ぐために電子文書内の公益通報者に関連する情報を提案方式の電子文書墨塗り技術を用いることにより秘匿することができる．また，本研究において提案した電子文書墨塗り方式では，本来協力関係にある署名者と墨塗り者が非協力関係にあった場合にも，文章の正当性を損なうことなく墨塗りを行うことを可能にした．

5.1. 今後の課題

今後は，実装の検討を進めていきたいと考えている．その際に特にどのようなデバイスを用いるか対応者の設定なども考慮しつつ，実現していきたい．また公益通報システムの完成度を上げるためにほかの技術の可能性も検討していきたい．

参考文献

[1] 佐古和恵，米沢祥子，古川潤，“セキュリティとプライバシを両立させる匿名認証技術について，”情報処理，vol.47, no.4, pp.410-416, April.2006.

[2] 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，” 信学技法ISEC2003- 20, pp. 61–67, 2003.

[3] 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”，css-2004, Oct.2004.

[4] 加藤岳久，岡田光司，吉田琢也，“匿名認証技術とその応用，”東芝レビュー，vol.60, no.6, pp.23-27, 2005.

[5] 黒澤馨，尾形わかは，“現代暗号の基礎数理，” コロナ社，(2004).

[6] 宮本一子，“公益通報の時代”，花伝社，(2002)

[7] こちらIT広報室，Online document, http://www.itpr.jp/us/us_report21.html May.2003.

[8] D.Chaum and E.van Heijst, “Group signatures,” Proc. EUROCRYPT '91, LNCS 547, pp.241-246, Springer, 1991.