Vol.2010-DPS-142 No.20
Vol.2010-CSEC-48 No.20
2010/3/4

プライバシー保護のための墨塗り機能を持つ電子証明書システムの提案と評価

佐久間貴士[†]　　佐々木良一[†]

公開鍵暗号技術と電子署名を使い，インターネットで安全な処理を実現するシステムとして PKI（Public Key Infrastructure：公開鍵暗号基盤）がある．これは信頼できる認証機関を設け，電子証明書を発行することによる，通信相手や署名者の正当性を証明する仕組みである．ここで使用する電子証明書には氏名や住所など個人を特定できる情報が含まれており，すべてを開示するのはプライバシー問題になるという指摘もある．本稿では，墨塗り署名技術を改良したものを導入することにより，プライバシー問題を解決し，墨塗り部分以外の不正な改ざんを防止できる電子証明書システムの提案を行う．また，システムの一部を実装し，その機能，性能面での評価を行う．

Proposal and evaluation of the digital certificate system with SUMI coating for privacy protection

Takashi Sakuma[†]　and Ryoichi Sasaki[†]

PKI (Public Key Infrastructure) is a system to achieve secure procedure on the Internet by using the public key cryptosystem and the digital signature. In this system, a trusted certification authority enables the authentication of communicators and/or signers using digital certificate published from the certificate authority. The digital certificate contains information such as names or addresses etc which can be used to identify the individual. There is an opinion that it can be a cause of the privacy problem to disclose such all information. In this paper, therefore, we proposal the digital certificate system using revised SUMI coating signature in order to solve the privacy as well as security problem. We also report the evaluated results on the function and the performance using partially implemented system.

1. はじめに

近年，コンピュータ社会の進展に伴い，行政や企業での文書の電子化が進んでいる．平成 17 年には電子文書法が施行され，それまで紙での保存が義務付けられていた書類・帳票を，電子データとして保存することが可能となり，法律面でも文書の電子化を後押ししている．

これらの電子文書のセキュリティを確保し，安全に使うためには，従来のハンコと同じように①確かに本人が承知したことを証明する「本人性」や，②承知した後、改ざんされていないことを証明できる「非改ざん性」(「安全性」ともいう）の機能が必要となる．このような機能を電子の世界で実現するのが公開鍵暗号とハッシュ関数を用いる電子署名である[1]．そして，この電子署名を運用する上で必要となるのが後述する PKI（Public Key Infrastructure：公開鍵暗号基盤）である．PKI は，署名における本人証明の基盤となる公開鍵が確かに本人のものであることを証明するためのものである．現実世界の①印鑑登録，②印鑑証明，③印鑑の無効化の機能を持ち，認証局（現実世界の市役所などの相当）というところからその電子署名をつけた公開鍵証明書というものを発行することによって実現する．

なお，公開鍵証明書と似たものに属性証明書があり，両方を合わせて電子証明書ともいう．属性証明書は 20 歳以上であるかどうか，ある組織に属しているかどうかなどの属性を証明するものである．

ところで，この公開鍵証明書には①氏名，②生年月日，③性別，④住所など個人を特定する情報が含まれており，これら（特に住所）を他人に知られることがプライバシー問題になると指摘する人もいる．すなわち，セキュリティ対策がプライバシー問題を引き起こすことになる．このような対立するリスクの問題を解決するために考案したのが「プライバシー保護のための墨塗り機能を持つ電子証明書システム」である．

証明上，住所などがどうしても必要な場合がある一方，なくてもよいような場合もあり，目的に応じて公開鍵証明書を発行してもらうという方法も考えられるが，この発行を受けるには公開鍵の提出，本人であることの証明など多くの時間と手間がかかることから，できるだけ 1 回で済ませたい．ここでは，①氏名，②生年月日，③性別，④住所以外にいろいろな属性（メールアドレス，所属学会など）をつけたものに一度に証明書を発行してもらい電子文書への署名者と検証者との間で必要であると認めたもの以外（例えば住所やメールアドレスなど）は，電子文書に署名した人が，電子文書と一緒に送る公開鍵証明書に電子的に墨を塗り，墨塗り部分は検証者などに知られないようにしようというものである．ここでは，すべての情報を消すのではなく，住所における町名や丁目，番地，生年月日における生年だけを消すことも考えられる．

[†] 東京電機大学工学部　〒101-8457　東京都千代田区神田錦町 2-2
School of Engineering Tokyo Denki University　2-2 Kandanishikicho, Chiyoda-ku, Tokyo, 101-8457 Japan

Vol.2010-DPS-142 No.20
Vol.2010-CSEC-48 No.20
2010/3/4

しかし，公開鍵証明書に対し通常の署名をしたうえで墨塗りをすると改ざんとみなされ，墨塗り部以外を改ざんしてもわからないという問題が生じてしまう．そこで，本システムでは宮崎らが提案した墨塗り署名に注目し，これを改良し，墨塗り禁止部分の指定を可能とした方式を使うこととした．墨塗り署名の電子証明書への適用は本提案システムが初めてとなる．

本稿では，電子署名，PKI，墨塗り署名などの概要を説明した上で，プライバシー保護を目的とした墨塗り機能を持つ電子証明書システムの提案と評価を行う．

2. 電子署名と PKI

2.1 PKI に基づく方式

PKI（Public Key Infrastructure：公開鍵暗号基盤）とは，公開鍵暗号を利用した認証基盤である．基盤技術であるため，PKI という一つの仕組みをユーザ認証や正当性確認など，様々な認証のために利用することができる[2][3]．PKI では通信相手が本物であるかどうかの確認（認証）に公開鍵証明書を利用する．この公開鍵証明書は，発行者の名前などの情報が記述されており，身分証明書の役割を果たす．この身分証明書を信頼できる第三者機関（認証局と呼ぶ）に発行してもらうことで，その身分証明書を信頼できるようにする．図 1 は PKI の特徴を表す．

公開鍵証明書を利用して相手を認証する際には，公開鍵証明書が偽造されていないか，その発行元は信頼がおけるのか，といった確認が行われる．これらが有効であれば，その公開鍵証明書の提示を行ったのが正しい相手であることがわかる．

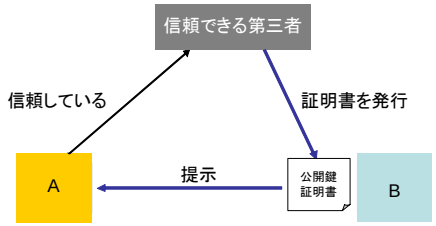

図 1　PKI の特徴

また，PKI で用いられる公開鍵証明書は，認証局（CA：Certificate Authority）によって発行され，これが信頼できる第三者機関にあたる．ユーザは自分が信頼している CA が発行した公開鍵証明書であれば信じられることになる．この公開鍵証明書は身元を証明する内容だけでなく，公開鍵暗号方式で使用される暗号鍵（公開鍵）や CA のデジタル署名なども含まれ，図 2 のようになっている．公開鍵証明書の詳しい概要については次項で述べる．

図 2　公開鍵証明書

2.2 公開鍵証明書の概要と問題点

電子証明書は ITU-T が X.509 規格で標準化されており，ディレクトリに関する一連の規格である X.500 シリーズの一つに該当する．

X.509 公開鍵証明書は複数のバージョンがある．1988 年に公開されたバージョン 1 は基本的な必須項目が定義され，1993 年に公開されたバージョン 2 ではエンティティの一意性を表すためのオプショナルな固有識別子が追加された．更に 1996 年にはさまざまな情報を埋め込めることのできる追加領域を定義したバージョン 3 が発行されている．現在はこの X.509v3 公開鍵証明書が利用されている．

主に以下の情報が格納されている．

1. 証明書の基本情報
   証明書のバージョン（X.509v3），証明書番号，署名に使われるアルゴリズム
2. 証明書の証明者情報
3. 証明書の有効期限
4. 証明書が証明する対象の情報
5. 証明書に含まれる公開鍵情報
6. 証明書発行局の署名
7. 証明書の拡張部分

この公開鍵証明書の所有者情報には，①氏名，②生年月日，③性別，④住所など個人を特定する情報が含まれており，これら（特に住所）を他人に知られることがプライバシー問題になると指摘する人もいる．すなわち，セキュリティ対策がプライバシー問題を引き起こすことになる．この X.509v3 公開鍵証明書のフォーマットを図 3 に示す．

Vol.2010-DPS-142 No.20
Vol.2010-CSEC-48 No.20
2010/3/4

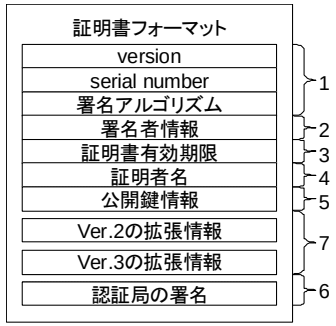

図 3　X.509v3 フォーマット

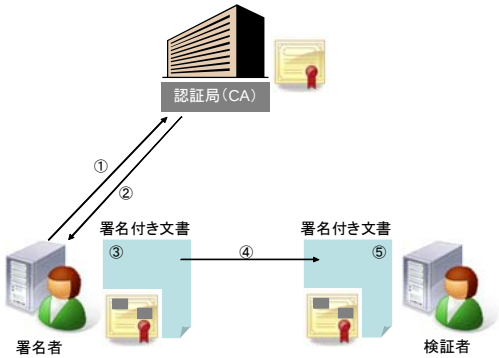

図 4　提案システムの利用モデル

3. 提案システム

3.1 提案システムの狙い

このような対立するリスクの問題を解決するために考案したのが「プライバシー保護のための墨塗り機能を持つ電子証明書システム」である．

証明上，住所などがどうしても必要な場合がある一方，なくてもよいような場合もあり，目的に応じて電子証明書を発行してもらうという方法も考えられるが，この発行を受けるには公開鍵の提出，本人であることの証明など多くの時間と手間がかかることからできるだけ 1 回で済ませたい．ここでは，①氏名，②生年月日，③性別，④住所以外にいろいろな属性（メールアドレス，所属学会など）をつけたものに一度に証明書を発行してもらい電子文書への署名者と検証者の間で必要であると認められたもの以外（例えば住所やメールアドレスなど）は，電子文書に署名した人が，電子文書と一緒に送る電子証明書に電子的に墨を塗り，墨塗り部分は検証者などに知られないようにしようというものである．なお，墨塗りは住所全体ではなく，丁目や番地だけに塗ることも可能である．

3.2 提案システムの概要

本研究では，PKI 技術を中心として公開鍵証明書を利用した墨塗り技術を持つ電子証明書システムを提案する．利用モデルは図 4 の通りである．

① 属性を追加した公開鍵証明書の申請
② 認証局は証明書を発行
③ 署名者は証明書のうち検証者などに知られたくない部分（住所など）に墨塗り
④ 検証者へ署名付き文書を送信
⑤ 検証者は証明書と文書の検証

まず認証局（CA ともいう）への属性追加型の証明書の発行を申請する．そして発行された証明書を検証し，その後③において検証者に公開したくない部分（氏名，生年月日，性別，住所，その他属性情報など）に墨を塗り，署名する．その際，検証者との間で決めた必要情報以外が墨塗り対象となる．図 3 の X.509v3 フォーマットにおいて，7 の拡張領域にこれらの情報を記載し，処理を行う．検証者は証明書に記載されている情報をもとに CA の署名を確認し，証明書内の公開鍵を入手する．仮に第三者が署名者になりすまして公開鍵を配布しても，CA から発行された証明書がないため，その証明書は信頼されたものではなくなる．そのため簡単に見破られてしまう．

通常，CA はどの公開鍵がどのユーザのものであるかという各人の ID との対応付けを行っている．この ID と公開鍵の対応付けに属性部分を用いて行えば，公開する情報を減らすことが可能である．例えば，国民 ID や住所，IP アドレス，メールアドレスなど考えることができる．そこで公開する情報をこのような情報のどれかに限定することができれば，情報量も軽減することができ，利便性は高まる．これらの処理は先に述べたとおり，図 3 の X.509v3 フォーマットの 7（拡張領域）で処理を行うことができる．また，フォーマット内の他領域（署名者情報，公開鍵情報，署名など）においては必要事項となるため，墨塗り処理を施すと改ざん処理と見なされる．

また，電子証明書に対し通常の署名をしたうえで墨塗りをすると改ざんとみなされ，墨塗り部以外を改ざんしてもわからないという問題が生じてしまう．そこで，本シス

Vol.2010-DPS-142 No.20
Vol.2010-CSEC-48 No.20
2010/3/4

テムは宮崎らが提案した墨塗り署名[4]を改良して使うことにした．

3.3 従来の墨塗り署名と提案方式

宮崎らが提案した墨塗り署名では，オリジナル文書を N 個のブロックに分割し，そのブロックに対して乱数を生成し，ハッシュ値を計算する．N 個のハッシュ値を結合したデータに対し，署名者の秘密鍵 Sk で署名を生成する．この署名生成手順を記す．

① オリジナル文書を N 個のブロックに分割する．
② N 個のブロックをそれぞれに対し，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，図 5 のように算出された N 個のハッシュ値を結合したデータ（HMR とする）に対し，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．

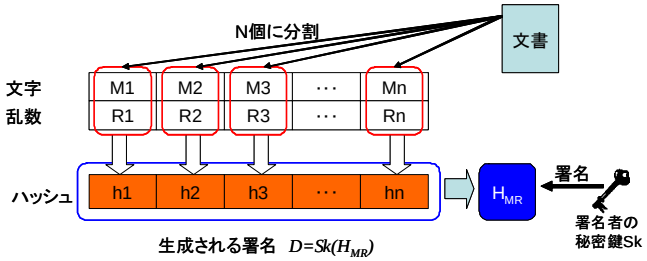

図 5　宮崎方式の署名生成処理

次に墨塗りを行う必要が生じたときに行う手順を記す．

① 開示対象である署名付きオリジナル文書の中から，不開示情報を含む各ブロックを選択し，墨塗り処理を施す．
② ①で選択された各乱数付きブロックのハッシュ値と，それ以外の各乱数付きブロックと署名からなるデータを開示文書とする．

このようにすることにより，自由に墨塗りができ，かつ，墨塗りする部分以外を改ざんすれば容易に検知することが可能となる．

報告者らが提案した方法を示す図 4 の⑤において墨塗り署名を行う．ここで，宮崎らの墨塗り署名を行おうとすると，次のような問題が生じる．

（a）乱数付きで文書を保管するため文書のデータ量が増加してしまう．
（b）墨塗り者が開示文書を墨塗りせずに公開することが可能である．

2.3 で説明したとおり電子証明書はいくつもの情報で構成されている．その中でも証明書の基本情報や公開鍵情報，あるいは署名部分などに墨塗りが施されることが考えられる．証明書情報に対し，墨塗り可能な部分と不可能な部分のコントロールを適切に行う必要があることから，（b）はそれが確保されていない．

このような問題を解決するために採用することにしたが，佐々木研究室で開発した次のような方式[5] [6]を参考に以下のような方式を採用することとした．乱数は乱数生成用 Seed で管理することで，データ量の増加を防ぐ．また署名者が墨塗り必須，禁止といったフラグを付加することで墨塗り部分のコントロールを可能にしている．

まず署名生成手順を記す．

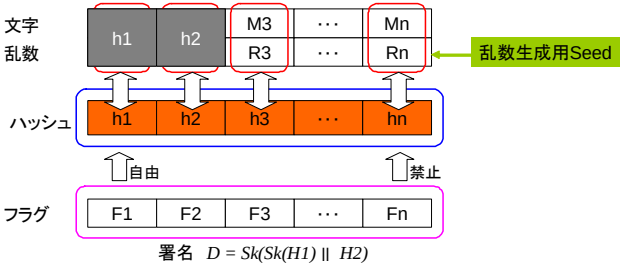

図 6　増渕らによる提案方式（墨塗り）

① 文書に N 個のブロック（以下，文字ブロックとする）に分割する．
② 文字ブロックに対して墨塗り自由，墨塗り禁止を示すフラグをそれぞれ指定する．
③ Seed を設定後，乱数を生成し，署名者がセキュアデバイスに保管する．
④ Seed を分散し，分散情報を適切に墨塗り者へ分配する．
⑤ 各文字ブロックに③で生成された乱数を付加する．（以下このように乱数を付加した文字ブロックを「墨塗り自由ブロック」「墨塗り禁止ブロック」とする）
⑥ ⑤で乱数を付加した文字ブロックのハッシュ値を算出する．
⑦ ⑥で算出したハッシュ値を結合し，一つのハッシュ値（HMR とする）を生成する．
⑧ ⑦で算出したハッシュ値に署名者の秘密鍵 Sk で署名を生成する．
⑨ 各フラグを結合したハッシュ値（HF とする）を算出する．
⑩ ⑧で生成した署名と⑨で算出したハッシュ値（HF）に対し署名者の秘密鍵 Sk で署名を生成する．
⑪ オリジナル文書，⑩で生成された署名，フラグの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．

Vol.2010-DPS-142 No.20
Vol.2010-CSEC-48 No.20
2010/3/4

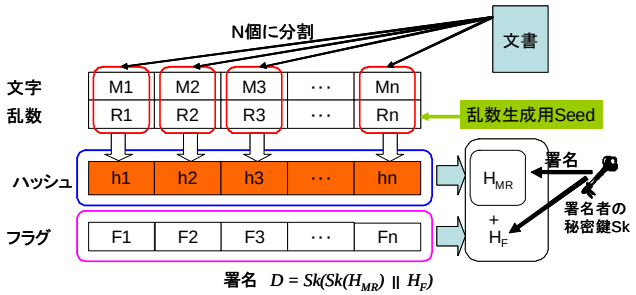

図 7　増渕らによる提案方式

次に墨塗り手順を記す．

① 署名付きオリジナル文書中から，オリジナル文書を取り出し，署名生成手順と同様に文書を N 個のブロックに分割する．
② ここで，墨塗り者が Seed の分散情報を持ち寄り，Seed を復元する．
③ 復元した Seed を指定して，各文字ブロックに乱数を付加する．
④ 墨塗り自由ブロックの中からブロックを選択し，墨塗り処理をする．
⑤ 墨塗り処理をしたブロックのハッシュ値（以下「墨塗り部分」とする）と，それ以外の各墨塗り自由ブロックおよび残りの墨塗り禁止部分のブロック，署名，フラグのブロックからなるデータを開示文書とする．

これにより，証明書への墨塗り制御を行う．この証明書は X.509 規格に準拠し，所有者情報，公開鍵，認証局の署名が含まれる．これには証明書発行者が情報を追加することができる拡張領域が存在する．この領域を利用し，所有者の属性情報への墨塗りを可能にし，プライバシーを保護することができる．

4. 提案システムの部分実装と評価

4.1 部分実装

提案システムを部分的に実装した．具体的には，証明書の生成，証明書への墨塗り処理，証明書の検証の部分である．この実装環境は以下のとおりである．

（1）ハードウェア
CPU：Pentium M 1.1GHz
RAM：760MB
（2）ソフトウェア
OS：WindowsXP ProfessionalEdition SP3
開発言語：C++　約 1000 ステップ

図 8 は部分実装を行ったプログラムの全体的なインタフェースを示す．プログラム開発した墨塗り部分を指定する入力部分は図 9 に示すとおりである．インタフェースにはチェックボックスを採用することにより，墨塗り箇所の指定方法を容易にし，墨塗り者自身の適切な情報のコントロールを可能にした．

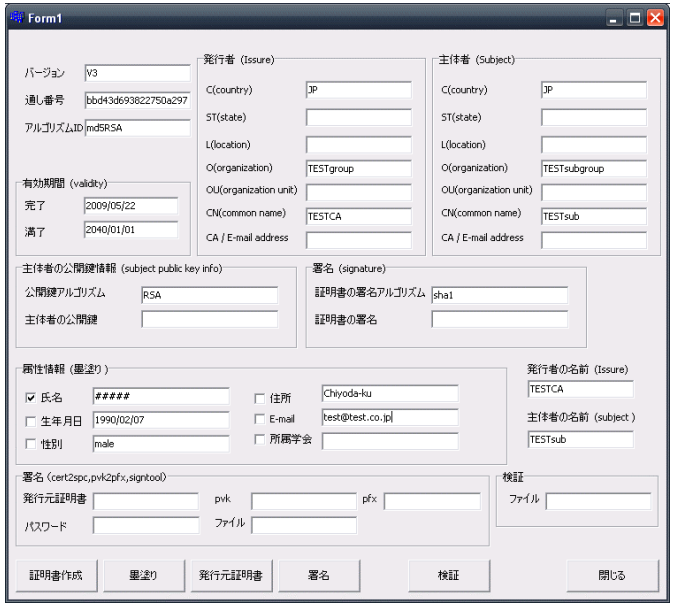

図 8　部分実装のインタフェース

図 9　墨塗り部分の指定

Vol.2010-DPS-142 No.20
Vol.2010-CSEC-48 No.20
2010/3/4

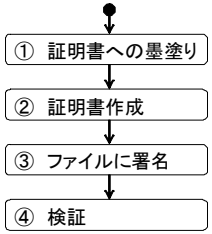

図 10　部分実装実験の流れ

部分実装の実験を行った手順は図 10 のとおりである．CA の証明書は PC にインストール済みである．まず証明書への墨塗りを施し，証明書を生成する．その時，秘密キー生成を行う．そして生成された証明書で署名を行う．証明書の生成，署名にはマイクロソフト社が提供している証明書作成ツール（makecert）と署名ツール（signtool）を使用した．この実験では，メモ帳（notepad）に署名を行った．そして最後に署名の検証を行った．この検証の際も署名ツール（signtool）に含まれる機能を利用した．その検証結果を図 12 に示す. 署名された証明書にチェーン先とするルート証明書とつながっていることを表している．また，図 12 の出力結果と CA の証明書に記載されている情報を比べても正しい結果であることがわかる．

図 11　秘密キーパスワード入力画面

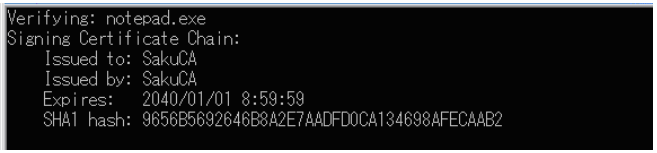

図 12　署名証明書に記載されているルート証明書情報

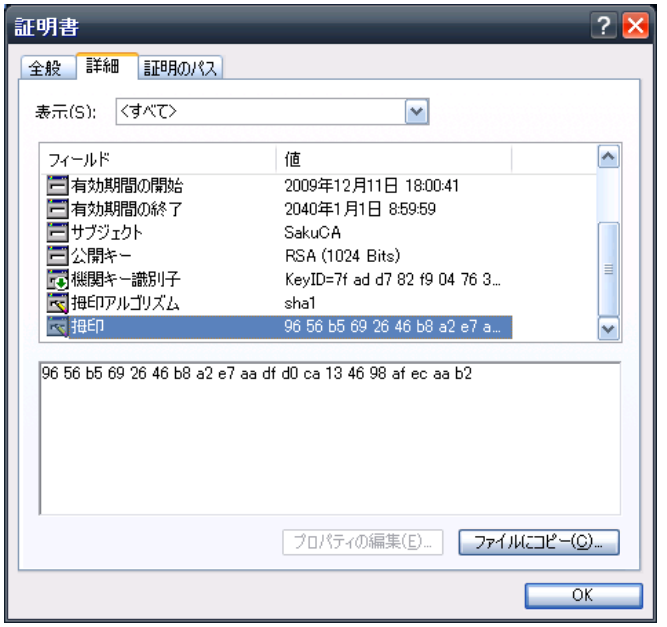

図 13　CA 証明書内容

図 14　検証ツールにおける出力結果

4.2 評価

4.2.1 機能の評価

以下に証明書の持つ機能の比較を示す．従来における証明書はプライバシー保護機能，および情報開示のコントロール機能は持ち得ないのに対し，本研究の提案方式では両立の機能を持つ．そして，改ざん防止機能は従来の証明書も CA による署名などにより保有している．提案方式でも同様のことがいえる．

Vol.2010-DPS-142 No.20
Vol.2010-CSEC-48 No.20
2010/3/4

表 1　機能評価比較表

	従来の証明書	提案方式
プライバシー保護	×	○
情報開示コントロール	×	○
改ざん防止	○	○

従来のそのたびごとに証明書をもらいにいく方式以外に，最初から各種証明書をすべて発行する方式が考えられる. この方式ならもらいにいくのが一回ですむ. しかし，この場合，情報量を 4 情報（住所，氏名，生年月日，性別）に限定する場合において，それぞれに対する証明書を取得した場合とすると 2 の 4 乗とおりの証明書を事前にもらっておく必要がある．いま，追加する属性証明書の数がαだとすると，事前にもらうべき証明書の数は 2 の 4+α乗となり，その数は膨大となる．さらに生年月日に生年だけ除くようなことを考えるとその数はもっと増える．これらに対し，本研究における墨塗り方式は 1 回の取得ですみ，かつ最初からもらう証明書も 1 つですむ．このようなことから，墨塗り方式は他の方式に比べ，明らかに利便性がよく，かつ効率の良い手法であるといえる.

4.2.2 性能評価

証明書の生成，証明書への墨塗りの処理時間は以下のとおりであった.

・証明書の生成：2.2（秒）
・墨塗り処理　：1.7（秒）

若干時間がかかるが，実用可能な範囲であると考えられる．今後，実装に工夫を凝らし高速化を図りたい.

4.2.3 安全評価

PKI は，証明書に記載された利用者の公開鍵を使用して，利用者が相互に相手を正当であると認めることを可能にし，安全性を確保している．本研究の提案システムにおいて，その証明書に含まれる個人を特定できる情報に墨塗り処理を施すことで，プライバシー上の問題を解決した．またその墨塗り処理には証明書内の部分制御を行うことで，公開鍵の情報や署名部分などへの改ざん，あるいは証明者の不正による墨塗り処理による偽証明書の発行などを防ぐことを実現し，安全性を確保した．属性を追加した公開鍵証明書を利用することで，属性証明書の役割も果たす．属性証明書は毎回発行する必要があるが，その必要性もない．さらに従来の証明書と比較しても発行回数も明らかに少なくて済むことから，手間が省ける．プライバシー保護，改ざん，発行における通信，といったことから安全性は確保されているといえる.

5. おわりに

プライバシー保護のための墨塗り機能を持つ電子証明書システムを研究目的として，実験を行い，その評価を行った．従来の電子証明書には氏名，生年月日，住所などが含まれており，プライバシー上問題がある．そのため提案システムにより，個人情報となる部分を先行研究の増渕らの方式により墨塗り可能とし，さらにその利用モデルを提案した．処理の高速化や使い勝手の向上などが今後の課題となる.

参考文献

1)　情報処理推進機構:セキュリティセンター:暗号技術
https://www.ipa.go.jp/security/pki/index.html
2)　ブルース･シュナイアー (著), 山形浩生 (監訳), "暗号技術大全", ソフトバンクパブリッシング株式会社(2003).
3)　電子証明書と PKI 入門:日本ベリサイン
https://www.verisign.co.jp/basic/pki/index.html
4)　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,” 電子情報通信学会技術研究報告, 情報セキュリティ(ISEC2003-20), pp.61-68, 2003.
5)　増渕孝延, 中村創, 石井真之, 小川典子, 鹿志村浩史, 佐々木良一, “内部不正者を考慮した墨塗り箇所変更可能方式の提案”, 電子情報通信学会技術研究報告, コンピュータセキュリティ(CSEC2005-30）, pp.179-186, 2005.
6)　増渕孝延, 小川典子, 鹿志村浩史,石井 真之, 佐々木良一, “より効率的な墨塗りシステムの開発と評価”, 電子情報通信学会技術研究報告, 情報セキュリティ(ISEC2004－25), pp7-13, 2004.