解説

文書画像の正当性保証法

小西一也, 梅村晃広*

[著者抄録] デジタルネットワークの発展の中で、今まで紙メディアで扱われてきた文書の電子化が進められている。重要文書を電子化する場合の最大の課題は、改ざん、なりすまし等の不正行為をどのように防ぐかという正当性保証の問題である。特にインターネットのようなオープンネットワークを流通させる場合には、正当性保証の技術的困難さは高くなる。本稿では、電子文書の正当性保証の問題を解説し、この問題に対する一つの検討事例として、文書画像の形式で扱われる文書に対する正当性保証法を紹介する。

[著者付与キーワード] 電子文書, 正当性保証, 電子署名, 暗号, メッセージダイジェスト, 電子透かし

Commentary article

Authentication method for document images

KONISHI Kazuya, UMEMURA Akihiro

[Author Abstract] With rapid growth of digital network, a large amount of paper documents are being migrated to digital ones. One large problem to treat important digital documents is to provide with secure authentication mechanism to prevent tampering or pretending. On open networks such as the Internet, the authentication problem is more difficult than that on closed systems. In this paper, we explain authentication issues of digital documents, and illustrate an authentication method for document images.

[Keywords by Author] digital document, authentication, digital signature, cryptography, message digest, digital watermarking

* (株) NTT データ情報科学研究所 (〒210-0913 川崎市幸区堀川町66-2)
Tel. 044(548)4605 E-mail: koni@lit.rd.nttdata.co.jp
Laboratory for Information Technology, NTT Data Corporation
(66-2, Horikawa-cho, Saiwai-ku, Kawasaki-shi, 210-0913)

1. はじめに

ここ数年、WWW (World Wide Web) の普及により、誰もがデジタルネットワーク上で電子文書を書き、読み、さらにそれを活用する社会が訪れようとしている。このデジタルネットワークの発展と普及の中で、公共機関の申請書類や、高額のコストが関係する商取引文書などの重要な文書についても、電子的な取り扱いが開始されている。

こういった重要文書を扱う場合には、文書の正当性をどのように保証するかを考慮しなければならない。例えば、他人が誰かになりすまして記述した文書、一度書かれた後に改ざんされた文書、決裁権のない人が決裁処理をした文書などは正当なものとはいえない。文書の正当性を保証するには、このような不正処理が行われていないことを証明することである。

紙の文書の場合に広く使われる正当性保証の方法は、印鑑や署名である。しかし、電子文書に対しては、メディアとしての性質の違いから、印鑑や署名のような伝統的な方法をそのまま適用することはできない。そこで、電子文書に対応した新しい正当性保証のしくみが必要となる。

本稿では、このような背景のもとに開発が進められている、文書画像の形式で扱われる電子文書に対する正当性保証の一つの方法を紹介する。2章で正当性保証の必要性を述べ、3章で正当性を守るしくみとして電子署名技術を説明する。4章で文書画像に対する正当性保証法の解説を行い、5章でそのプロトタイプシステムを紹介する。

2. 情報の正当性保証の必要性

重要な情報を電子化する例として、省庁への申請手続きの電子化を見てみる。総務庁によるまとめでは、各省庁における申請手続きの総数は7,375種類であり、そのうち74%が平成10年度末までに電子化される運びであるという。例えば、特許出願や、いくつかの関税手続きなどがすでに電子化

されている。残された26%の申請が電子化されていない理由の一つは、原本性の保証が問題になるためである。原本性の保証とは、紙メディアの場合の概念である原本・謄本・正本・抄本を、電子メディアの場合にどのように対応させていくかという問題である。この問題に対して技術的に求められていることは、高いレベルの正当性保証技術を確立することである。そのことによって、さらに多くの申請手続きを電子化することが可能となる。このように、電子文書の正当性保証に対する必要性は高い。

また、先に述べた申請の電子化の運びは、FDを使った申請や、専用の端末からの申請を可能にするものが主であって、必ずしもインターネットで申請できるということではない。これらを今後インターネットに対応させていくためには、オープンネットワーク上の電子文書通信に対する正当性保証の方法を確立することが重要な課題となる。

一般に価値の高い情報は、電子的形態をとっているか否かにかかわらず不正利用の脅威にさらされているといえる。特にデジタル化された情報の場合、アクセスの容易さという長所がそのまま不正利用の容易さという欠点となりやすい。このことが顕著に現れるのが、情報がインターネット上を流通する場合である。インターネットの特徴の一つはそのオープン性である。インターネットには全体を管理する人は存在せず、誰でもどこからでもアクセスできる。通信途中の情報は誰に見られるかわからない状況にある。

電子情報を不正利用から守るために行われる措置のうち最も確実なものは、関連する計算機、通信路などを物理的に隔離し、厳重に管理することである。しかしこれでは、インターネットには対応できない。オープンネットワーク上を流通させる情報を保護するためには、流通される情報自体に、自分の正当性を守るしくみを持たせる必要がある。そのうち代表的なものをここで二つ挙げる。

(1) 通信情報の暗号化

通信情報を勝手に傍受され、利用される危険に対する手段として通常利用されるのが、情報の暗

号化である。オープンネットワークの場合には、情報を傍受することについての技術的な障壁は少ない。暗号化することによって、傍受することができても、解読されない限り、その情報の内容は守られることになる。

(2) 電子署名

情報に対して勝手に手を加え、あたかも元の情報の発信者のものであるかのように再発信する（情報の改ざん）という脅威も考えられる。あるいは、もともと別人の名前（あるいは電子メールアドレス等）を騙って情報を発信すること（なりすまし）もありうる。この脅威に対抗する手段として考案されたものが、第3章で説明する電子署名である。

本稿の4章以降では、この電子署名技術と電子透かし技術を組み合わせた、文書画像の正当性保証システムを紹介する。通常の電子署名の場合は、署名されている対象の情報と署名とを容易に分離できるが、本稿で紹介した方法では両者が一体化していて、分離が困難になる。このことは、各種の権利問題や法的な手続きなどが関係して署名自体の正当性が問われる場合により有利になると考えられる。

3. 電子署名

電子署名とは、電子情報に対する署名者を特定し、情報が改ざんあるいは偽造されていないことを証明する方法である²⁾。「署名」は以下の機能を備えていなければならない³⁾。

- (1) 署名が対象情報に対するものであることを証明できること（メッセージ認証機能）
- (2) 署名が本人のものであることを証明できること（ユーザ認証機能）

紙の文書に対する上記機能の実現に対しては、情報をインクで記述し、押印や署名を施す方法が採用されている。これは、記述された情報の改ざんが困難であるという性質と、印鑑や筆跡が個人に固有であり、他者が容易に複製することはできないという性質に基づいている。しかし、電子情

報の内容の証明は非常に困難である。証明の対象となる電子情報は誰でも容易に改ざんすることができる。また、個人に固有であり、他者による複製が困難であるような電子情報を作成することは不可能である。そこで、この問題に対する解決策として、メッセージダイジェストと公開鍵暗号システムを利用した電子署名方法が考案された。

メッセージダイジェストとは、ある電子情報に固有な特徴を表す情報であり、公開鍵暗号システムとは、その情報を暗号化した者を特定することのできる暗号システムである。メッセージダイジェストを利用することでメッセージ認証機能を、公開鍵暗号システムを利用することでユーザ認証機能を実現することができる。

以下では、メッセージダイジェストおよび公開鍵暗号システムと、それらを利用して実現する電子署名方法について説明する。

3.1 メッセージダイジェスト

メッセージダイジェストとは、電子情報の指紋とでも呼ぶべき特徴パターンである⁴⁾。通常、電子情報からメッセージダイジェストを抽出するときは、図1に示すように、以下の特徴を有する一方方向ハッシュ関数が利用される。

- (1) 異なる二つの入力値から同じ一つの出力値を得ることは困難
- (2) 出力値から入力値を復元することは困難

一方方向ハッシュ関数は元の電子情報と改ざんされた電子情報からは異なる値を出力するため、両

図1 メッセージダイジェストの特徴

者は区別される。また、元の電子情報から得られる出力値と同一の出力値が得られる別の電子情報を偽造することは困難になる。したがって、電子情報に固有な特徴を表すメッセージダイジェストとして、一方向ハッシュ関数の出力値を利用することが可能となる。元の電子情報そのものをメッセージダイジェストとして利用することも可能であるが、情報量および公開鍵暗号システムの処理速度を考慮すると、ハッシュ値を利用の方が望ましい。

電子署名では、対象電子情報にそのメッセージダイジェストを添付し、署名とする。もし、電子情報が改ざんされた場合、改ざんされた電子情報からは、添付されたものとは異なるメッセージダイジェストが抽出される。したがって、電子情報から抽出されたメッセージダイジェストと添付されたメッセージダイジェストを比較照合することにより、メッセージ認証機能を実現することができる。

3. 2 公開鍵暗号システム

電子情報に対し、単純にメッセージダイジェストを添付するだけでは電子署名システムは実現されない。メッセージダイジェストは誰でも抽出できるため、電子文書を改ざんあるいは偽造し、そこから新たに抽出したメッセージダイジェストを添付することも可能である。メッセージダイジェストを利用しても、このような不正行為は発見できず、ユーザ認証機能は実現されない。

そこで、公開鍵暗号システムを利用し、暗号化

されたメッセージダイジェストを署名情報として対象電子情報に添付する。公開鍵暗号システムとは、公開鍵と秘密鍵という二つの鍵を組で使用するもので、公開鍵で暗号化された情報は、その組の秘密鍵でのみ復号化が可能であり、秘密鍵で暗号化された情報は、その組の公開鍵でのみ復号化が可能である暗号システムである³⁾。公開鍵は認証局に登録して誰でも参照できるようにし、秘密鍵は自身で保管する。公開鍵暗号システムは、暗号化と復号化を同一の鍵で実現する秘密鍵暗号システムに比べて処理速度が遅いという欠点がある一方、鍵の取り扱いは非常に安全になる。秘密鍵暗号システムと公開鍵暗号システムの概念を、図2に示す。

公開鍵暗号システムを利用し、AがBに対して情報を送信する場合、AはBの公開鍵を使用して暗号化した情報を送信する。この暗号化情報を復号化できるのは、Bの公開鍵と組を成す秘密鍵を所有するBのみである。

また、Aが自分の所有する秘密鍵を使用して暗号化した情報を送信することも可能である。この場合、この情報を復号化できるのはAの公開鍵のみであることから、情報の送信者がAであることが証明される。したがって、Aが署名対象となる電子情報のメッセージダイジェストを自分の秘密鍵で暗号化して添付することにより、その電子情報の作成者はAであることが証明され、ユーザ認証機能が実現される。また、第三者が改ざんあるいは偽造した電子情報から新たにメッセージダイジェストを抽出しても、Aの秘密鍵を知らない限り、有効な署名としてそれを添付することはできない。

図2 秘密鍵暗号システムと公開鍵暗号システム

3. 3 メッセージダイジェストと公開鍵暗号システムを利用した電子署名

メッセージダイジェストと公開鍵暗号システムを利用した電子署名を、図3に示す。電子署名では、対象電子情報から抽出されたメッセージダイジェストを、署名者の所有する秘密鍵で暗号化し、署名情報として対象電子情報に添付する。電子情

図3 電子署名

報の内容を確認するときは、対象電子情報からメッセージダイジェストを抽出し、添付された署名情報を署名者の公開鍵で復号化する。抽出したメッセージダイジェストと復号化した情報が一致すれば、電子情報は改ざんされていないことが証明され、署名者も確認される。第三者が改ざんあるいは偽造した電子情報のメッセージダイジェストを用いて署名情報を作成しようとしても、署名者の秘密鍵がない限り、署名者の公開鍵で復号化が可能な署名情報となるように暗号化することはできない。これにより、メッセージ認証機能およびユーザ認証機能を実現することができる。

4. 文書画像の正当性保証

我々は、電子署名と電子透かし技術を利用して、

図4 電子透かし

文書画像の正当性を保証する研究を実施している。電子透かし技術とは、図4に示すように、画像や音声等の電子情報に対して、全く別の情報を人間には知覚できないように埋め込む技術である⁵⁾。電子透かしには、埋め込まれた情報の第三者による発見や改ざん、破壊は、非常に困難であるという特徴がある。電子署名において、通常は対象の電子情報に添付して扱われる署名情報を、電子透かし技術を利用して電子情報自体に埋め込むことで、電子情報と署名情報の対応づけが容易になる。また、署名情報のみを消去することが困難になるため、紙面への押印と同様に、署名した事実が保証されるという効果も得られる。電子情報の正当性の確認は、実際に電子情報から得られるメッセージダイジェストと、電子透かし技術で電子情報に埋め込まれた署名情報を復号化して得られるメッセージダイジェストとを照合することで実現することができる。

以下では、電子署名と電子透かし技術を利用した文書画像の正当性保証方法について、具体的に説明する。

4.1 メッセージダイジェスト抽出技術

電子署名を実現する際に必要なメッセージダイジェスト抽出技術としては、MD5⁴⁾やRIPEMD⁶⁾などが考案されている。これらは署名対象の電子情報の大きさにかかわらず、128ビットのメッセージダイジェストを抽出する。抽出方法を図5に示す。まず、128ビットの初期ベクトルを設定し、対

図5 メッセージダイジェストの抽出

象電子情報から抜き出した固定長（通常512ビット）のブロック情報と初期ベクトルから新たなベクトルを作り出す。そして、署名対象情報の次のブロック情報と新たに作り出されたベクトルから、さらに新しいベクトルを作り出すという処理を繰り返し実行し、メッセージダイジェストを生成する。しかし、このメッセージダイジェスト抽出方法を利用しても、異なる電子情報から同一のメッセージダイジェストが容易に抽出され得ることが、最近になって指摘された⁶⁾。この問題を解決するために、より安全なメッセージダイジェスト抽出技術として RIPEMD-160が考案された。これは RIPEMD と同様の処理を行うが、より大きな160ビットのメッセージダイジェストを抽出する。

文書画像からメッセージダイジェストを抽出するときは、画像データをビット列として捉え、それに上記メッセージダイジェスト抽出技術を適用する。

4. 2 電子透かし技術

情報埋め込みの対象となる電子情報を主情報、埋め込む情報を副情報と呼ぶ⁷⁾。一般に電子透かし技術は、主情報に含まれる成分のうち、人間の知覚に対して影響の少ない成分を、副情報を表すように変換することで実現する。

グレースケール濃淡画像を主情報とした、最も簡単な電子透かし技術の一例を、図6を用いて説明する。濃淡画像における各画素値は、画像の指

定された位置における濃度を示している。ところで、各画素は偶数または奇数のいずれかであり、これが濃度とは別の1ビットの情報を表しているとも考えることもできる。また、階調数が多くなるほど、人間の視覚ではわずかな濃度の差を認識することはできなくなる。そこで、各画素値を視覚上では知覚できない程度にわずかに変化させ、偶数、奇数のいずれであるかを示す1ビットの情報が目的の副情報を表すように処理を施すことで、画像に対する副情報の埋め込みを実現することができる。副情報の読み出しは、各画素値が偶数、奇数のいずれであるかを判定すればよい。図6では、画素値が偶数である場合は副情報を0とし、奇数の場合は1としている。原画像の左上の4画素はすべて偶数であるため、副情報を読み出すと0000となる。ここに0101という副情報を埋め込む場合は、2番目および4番目の画素値をわずかに変更し、それぞれ奇数にする。これにより、視覚上は原画像との違いを認識することが困難な、かつ0101という副情報の埋め込まれた画像が生成される。

ただし、このような単純な手法で主情報に埋め込まれた副情報は、第三者に容易に発見、改ざん、破壊されてしまう。そこで、実用に当たっては、副情報埋め込み位置を示す鍵情報を利用して、鍵情報がない限り副情報の読み出しや改ざんが困難になるようにしたり、画像データの周波数成分に副情報埋め込み処理を施すことで、副情報を画像全体に分散させるなどの工夫が必要となる。

4. 3 メッセージダイジェスト抽出技術と電子透かし技術の結合

我々は、文書画像の正当性保証を実現するために、文書画像のメッセージダイジェストを電子透かしとして画像に埋め込むことを考えている。しかし、メッセージダイジェスト抽出技術と電子透かし技術をそのまま結合することはできない。電子情報から抽出したメッセージダイジェストを用いて署名情報を作成しても、それを電子透かし技術を適用して電子情報自体に埋め込むことで、電

図6 画素値の偶数奇数を利用した電子透かし

子情報はわずかに変化してしまう。これにより、元の電子情報と電子透かしを付加した電子情報からは、同じメッセージダイジェストを抽出することができなくなってしまう。したがって、メッセージダイジェスト抽出技術と電子透かし技術を結合するためには、主情報における両者の対象成分を明確に分けなければならない。例えば、主情報が画像データである場合、図7に示すように、水平方向の座標と垂直方向の座標が共に偶数、あるいは共に奇数である画素（図7では白色で示される画素）からメッセージダイジェストを抽出し、それ以外の画素（図7では黒色で示される画素）に電子透かし技術を適用する方法が考えられる。

文書画像作成者は、文書画像のメッセージダイジェストを自らの秘密鍵で暗号化して署名情報を作成し、電子透かし技術を利用して画像に埋め込む。文書画像の参照者は、まず、画像からメッセージダイジェストを抽出する。次に、電子透かし技術で画像に埋め込まれた署名情報を読み出し、それを文書作成者の公開鍵で復号化する。そして抽出したメッセージダイジェストと復号化した情報とを照合し、一致していればその文書画像の正当性が証明され、一致しなければ文書の一部が改ざんされたか、あるいは文書自体が偽造されたものであるということになる。

5. プロトタイプシステム

我々は、4章で説明した文書画像の正当性保証

を実現するプロトタイプシステムを構築した。以下では、プロトタイプシステムに採用した技術、プロトタイプシステムの構成、およびサービス例について説明する。

5.1 プロトタイプシステムに採用した技術

文書画像の正当性保証システムのプロトタイプでは、メッセージダイジェスト抽出技術としてRIPEMD-160を採用した。画像データをビット列として捉え、このアルゴリズムを利用して抽出した160ビットのメッセージダイジェストを暗号化し、署名情報とする。

主情報となる文書画像は、各画素値が8ビットで表される256階調グレースケール濃淡画像とした。ここで扱う濃淡画像は、画素値0の画素が黒色を、255の画素が白色を表す。電子透かし技術としては、画像全体を3×3サイズの画素ブロックに分割したとき、各画素ブロックにおいて定められたビットプレーンのパターンが副情報を表すとする手法⁹⁾を採用した。採用手法を図8に示す。ビットプレーンとは、画素ブロックにおいて各画素の同レベルのビットで構成される平面である。1画素が8ビットの値で表される画像におけるビットプレーンは8枚あり、3×3サイズの画素ブロックにおける各プレーンには9個のビット情報が含まれる。プロトタイプシステムでは、この9個のビット情報のうち、周辺の8ビットのパターンが副情報を表し、中央の1ビットは、その画素ブロックが電子透かし処理の対象であるかどうかを示す

図7 メッセージダイジェスト抽出対象と電子透かし対象の分離

図8 ビットプレーンのパターンを利用した電子透かし

フラグを表すものとした。文書画像には一様に白色の領域が広く存在し、そのような領域の画素値を変換すると視覚上変化が目立ってしまう。そこで、画素ブロックに含まれるすべての画素値の平均値が、定められたしきい値を上回る場合、そのブロックを一様白色領域と判定し、電子透かしの対象から除外する。除外するブロックにおける対象ビットプレーンの中央のビットは1とする。一様白色領域ではないと判定されたブロックは電子透かしの対象とする。電子透かしの対象となるブロックについては、対象ビットプレーンの中央のビットを0とし、周辺の8ビットを目的の副情報を表すように変換する。副情報を読み出すときは、対象ビットプレーンの中央のビットが0である、すなわち電子透かしの対象である画素ブロックのみから読み出しを行う。

また、各画素の上位4ビットをメッセージダイジェスト抽出の対象とし、下位4ビットを電子透かしの対象とした。つまり、メッセージダイジェストは、画像データの上位4ビットのみから抽出

し、電子透かし処理は、各画素ブロックの下位の4ビットプレーンから選択したプレーンを対象とする。これは、視覚上特に重要な成分を利用してメッセージダイジェストを作成し、視覚に影響の少ない成分を変換して電子透かしを実現しようとしたためである。

電子署名を実現するために必要な公開鍵暗号システムとしては、RSA⁹⁾を利用した。これは、最もよく知られている、実質的標準の公開鍵暗号システムである。

5. 2 プロトタイプシステムの構成

プロトタイプシステムの構成図を図9に示す。システムは、運用上大きく三つのフェーズに分けられる。まず、公開鍵暗号システムで使用する公開鍵および秘密鍵を作成するフェーズ、次に、文書画像作成者が署名を行うフェーズ、そして、文書画像参照者が文書の正当性を確認するフェーズである。

公開鍵および秘密鍵の作成は、鍵の所有者の

図9 プロトタイプシステムの構成図

図10 プロトタイプシステムのサービス例

ユーザ ID, 乱数, および秘密鍵保管用のパスワードを用いて行う。上記三つの情報を用いて公開鍵と秘密鍵の組を作成し, パスワードは RIPEMD-160 を利用してメッセージダイジェスト化する。このメッセージダイジェストを鍵情報として, 秘密鍵暗号システムの DES₃⁹⁾ を利用し, 先に作成した秘密鍵を暗号化する。公開鍵は認証局に預けて誰でも参照できるようにし, 秘密鍵は上記のように暗号化して自分で保管する。秘密鍵の暗号化は, 万一鍵を盗まれた場合への対策である。

文書画像への署名のフェーズでは, まず, 文書作成者がパスワードを用いて自ら保管する秘密鍵を復号化する。次に, 対象となる文書画像の各画素の上位 4 ビットから RIPEMD-160 を用いてメッセージダイジェストを抽出し, それを先に復号化した秘密鍵を用いて暗号化して, 署名情報を作成する。そして, 電子透かし技術を利用して画像の各画素の下位 4 ビットに署名情報を埋め込む。これにより, 署名済み文書画像が完成する。

文書画像の正当性確認のフェーズでは, まず, 文書参照者が認証局より文書作成者の公開鍵を取り寄せる。次に, 電子透かし技術を用いて参照する文書画像の各画素の下位 4 ビットに埋め込まれた署名情報を読み出し, それを作成者の公開鍵を

用いて復号化する。そして, 各画素の上位 4 ビットから RIPEMD-160 を用いてメッセージダイジェストを抽出し, それを署名情報を復号化したものと照合する。文書画像が正当なものであれば, これらは一致する。

5.3 文書画像正当性保証システムによるサービス例

利用者 B が市役所 A に住民票の発行を申請し, 発行された住民票を不動産屋 C に提出するという状況を考える。この状況において, 住民票を画像データとしてネットワーク上を流通させる場面を仮定し, プロトタイプシステムを適用した場合のサービス例を図 10 に示す。

利用者 B より住民票発行の申請を受けた市役所 A は, B の住民票の画像より抽出したメッセージダイジェストを, A の秘密鍵を用いて暗号化して署名情報を作成し, 電子透かし技術を利用して画像に埋め込む。A は, それを署名済みの住民票として B に発行する。B は, 署名済みの住民票を不動産屋 C に提出する。C は, A の公開鍵を利用することで, B の住民票の正当性をいつでも確認することができる。

B が C に提出する前に住民票を改ざんした場

図11 プロトタイプシステムの動作画面

合、画像から得られるメッセージダイジェストは、画像に電子透かしで埋め込まれている情報とは一致しなくなるため、その住民票が正当なものではないことが確認される。また、Bが住民票を偽造した場合、BはAの秘密鍵を知らない限り、Aの公開鍵での復号化が可能な署名情報を作成することができず、Cがメッセージダイジェストと画像に埋め込まれた情報を照合しても、それらが一致することはない。

プロトタイプシステムの実際の動作画面を図11に示す。左側が原画像である。右側は、原画像から抽出されたメッセージダイジェストを市役所の秘密鍵で暗号化して署名情報を作成し、電子透かしとして原画像に埋め込んだものである。見た目には左右の画像に違いはないように感じられ

る。同図は、市役所の公開鍵を利用することで、右側の画像の正当性を確認できた場面である。

このように、文書画像正当性保証システムを利用することで、ネットワーク上を流通する文書画像に対する正当性を、いつでも確認することができる。

6. お わ り に

我々が開発したプロトタイプシステムを中心に、電子透かしによる文書画像の正当性保証法を紹介した。

重要情報のデジタル化は今後ますます進み、オープンネットワーク上の流通量も急速に増加していくであろう。デジタルコンテンツへの脅威

に対するセキュリティ技術の確立は急務である。本稿で紹介した正当性保証技術についても、実用化に向けてさらに発展させていくことを急がなければならない。

最後に、本稿で紹介したプロトタイプシステムの開発に協力いただいた Matthew Sakai 氏に深く感謝いたします。

~~~~~ 参 考 文 献 ~~~~~

- 1) 総務庁行政管理局. 申請・届出等手続の電子化について (<http://www.somucho.go.jp/gyoukan/kanri/sinsei04.htm>)
- 2) 鈴木優一. ネットワークセキュリティ読本／電子署名 (Digital Signature) (<http://www3.tokyoweb.or.jp/isl/dokuhon/p5.htm>)
- 3) 佐々木良一. インターネットセキュリティ. Computer Today. 80 p.10-17 (1997)
- 4) 稲村雄. 最新の暗号技術によるセキュリティの実現. OPEN DESIGN. No.14 p.4-133(1996)
- 5) 井上彰. 電子透かし—マルチメディア時代の暗号システム—. 東京, 丸山学芸図書, 1997
- 6) Hans Dobbertin, Antoon Bosselaers, Bart Preneel. RIPEMD-160: A Strengthened Version of RIPEMD. Fast Software Encryption (Lecture Notes in Computer Science 1039). p.71-82 (1996)
- 7) 中村高雄, 小川宏, 高嶋洋一. 画質を考慮した電子透かし. 1997年電子情報通信学会基礎・境界ソサイエティ大会講演論文集. p.246-247 (1997)
- 8) 岡一博, 松井甲子雄. 埋め込み関数を用いた濃淡画像への署名法. 電子情報通信学会論文誌 D-II. Vol. J80-D-II No.5 p.1186-1191 (1997)
- 9) D. E. R. デニング. 暗号とデータセキュリティ. 東京, 培風館, 1988