(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4901272号
(P4901272)
(45)発行日　平成24年3月21日(2012.3.21)　(24)登録日　平成24年1月13日(2012.1.13)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
H04L 9/00 675Z

請求項の数 7　(全 19 頁)

(21)出願番号　特願2006-103568(P2006-103568)
(22)出願日　平成18年4月4日(2006.4.4)
(65)公開番号　特開2007-281713(P2007-281713A)
(43)公開日　平成19年10月25日(2007.10.25)
審査請求日　平成21年2月4日(2009.2.4)

(73)特許権者　390017891
シヤチハタ株式会社
愛知県名古屋市西区天塚町４丁目６９番地
(74)代理人　100083839
弁理士　石川　泰男
(72)発明者　宍倉　勝仁
愛知県名古屋市西区天塚町４丁目６９番地
シヤチハタ株式会社内
(72)発明者　村松　賢治
愛知県名古屋市西区天塚町４丁目６９番地
シヤチハタ株式会社内

審査官　新田　亮

最終頁に続く

(54)【発明の名称】情報生成処理プログラム、情報生成装置及び情報生成方法

(57)【特許請求の範囲】
【請求項１】
コンテンツデータの真正性を確保する複数の真正確保情報を、当該複数の真正確保情報により真正性が夫々確保される属性を示す複数の属性情報とともに付加したコンテンツデータを生成するコンピュータを、
前記複数の属性情報が設定される属性情報設定領域と、互いに異なる前記真正確保情報が設定される複数の真正確保情報設定領域と、を含む１の設定領域を前記コンテンツデータに追加する設定領域追加手段、
前記属性情報として少なくとも、前記コンテンツデータの承認者を示す承認者情報を前記属性情報設定領域に設定する属性情報設定手段、
前記複数の真正確保情報の夫々を互いに異なる前記真正確保情報設定領域に順次設定する真正確保情報設定手段、として機能させ、
前記真正確保情報設定手段は、
前記真正確保情報を設定するとき、前記設定領域が追加されたコンテンツデータのうち、前記属性情報設定領域内において、今回設定する前記真正確保情報が生成されるよりも後に設定が行われる前記属性情報が設定される部分と、前記真正確保情報が設定されていない前記真正確保情報設定領域と、を除く部分を対象として前記真正確保情報を所定の生成手段により生成させて、当該生成された真正確保情報を前記真正確保情報設定領域に設定し、
前記承認者情報の真正性を確保する前記真正確保情報を除く前記真正確保情報を設定す

る際には、前記真正確保情報により真正性が確保される前記属性情報を含んで前記生成手段により生成された当該真正確保情報から前記属性情報を取得して、当該取得された属性情報を前記属性情報設定領域に設定することを特徴とする情報生成処理プログラム。

【請求項２】

請求項１に記載の情報生成処理プログラムにおいて、

前記属性情報は、前記コンテンツデータを承認した日時を示す承認日時情報を含み、

前記真正確保情報設定手段は、前記コンテンツデータの承認日時の真正性を確保する前記真正確保情報を設定する際に、前記真正確保情報により真正性が確保される現在日時を示す日時情報を含んで前記生成手段により生成された当該真正確保情報から前記日時情報を取得して、当該取得された日時情報を前記承認日時情報として前記属性情報設定領域に設定することを特徴とする情報生成処理プログラム。

【請求項３】

請求項１または請求項２に記載の情報生成処理プログラムにおいて、

前記コンテンツデータは所定のフォーマットで生成されたデータであり、

前記設定領域追加手段は、前記フォーマットの仕様上、１の領域として前記設定領域を追加することを特徴とする情報生成処理プログラム。

【請求項４】

請求項１乃至３のいずれか１項に記載の情報生成処理プログラムにおいて、

前記コンテンツデータは、文字情報を少なくとも含む電子文書であり、

前記承認者情報は、前記コンピュータが所定のアプリケーションプログラムを実行することにより前記電子文書が表示されたときに当該電子文書とともに表示される画像情報であって前記承認者を示す印影を表す画像情報を含むことを特徴とする情報生成処理プログラム。

【請求項５】

請求項１乃至４のいずれか１項に記載の情報生成処理プログラムにおいて、

前記設定領域追加手段は、前記設定領域に設定された前記複数の真正確保情報を夫々特定するための特定情報が設定される特定情報設定領域を含んで前記設定領域を追加し、

各前記真正確保情報について、その種類を示す情報と、前記真正確保情報設定領域の範囲を示す情報と、を前記特定情報として前記特定情報設定領域に設定する特定情報設定手段として更に前記コンピュータを機能させることを特徴とする情報生成処理プログラム。

【請求項６】

コンテンツデータの真正性を確保する複数の真正確保情報を、当該複数の真正確保情報により真正性が夫々確保される属性を示す複数の属性情報とともに付加したコンテンツデータを生成する情報生成装置において、

前記複数の属性情報が設定される属性情報設定領域と、互いに異なる前記真正確保情報が設定される複数の真正確保情報設定領域と、を含む１の設定領域を前記コンテンツデータに追加する設定領域追加手段と、

前記属性情報として少なくとも、前記コンテンツデータの承認者を示す承認者情報を前記属性情報設定領域に設定する属性情報設定手段と、

前記複数の真正確保情報の夫々を互いに異なる前記真正確保情報設定領域に順次設定する真正確保情報設定手段、とを備え、

前記真正確保情報設定手段は、

前記真正確保情報を設定するとき、前記設定領域が追加されたコンテンツデータのうち、前記属性情報設定領域内において、今回設定する前記真正確保情報が生成されるよりも後に設定が行われる前記属性情報が設定される部分と、前記真正確保情報が設定されていない前記真正確保情報設定領域と、を除く部分を対象として前記真正確保情報を所定の生成手段により生成させて、当該生成された真正確保情報を前記真正確保情報設定領域に設定し、

前記承認者情報の真正性を確保する前記真正確保情報を除く前記真正確保情報を設定する際には、前記真正確保情報により真正性が確保される前記属性情報を含んで前記生成手

段により生成された当該真正確保情報から前記属性情報を取得して、当該取得された属性情報を前記属性情報設定領域に設定することを特徴とする情報生成装置。

【請求項７】

コンテンツデータの真正性を確保する複数の真正確保情報を、当該複数の真正確保情報により真正性が夫々確保される属性を示す複数の属性情報とともに付加したコンテンツデータを生成する情報生成装置により実行される情報生成方法において、

前記情報生成装置が備える設定領域追加手段が、前記複数の属性情報が設定される属性情報設定領域と、互いに異なる前記真正確保情報が設定される複数の真正確保情報設定領域と、を含む１の設定領域を前記コンテンツデータに追加する設定領域追加工程と、

前記情報生成装置が備える属性情報設定手段が、前記属性情報として少なくとも、前記コンテンツデータの承認者を示す承認者情報を前記属性情報設定領域に設定する属性情報設定工程と、

前記情報生成装置が備える真正確保情報設定手段が、前記複数の真正確保情報の夫々を互いに異なる前記真正確保情報設定領域に順次設定する真正確保情報設定工程と、を含み、

前記真正確保情報設定工程において、

前記真正確保情報を設定するとき、前記真正確保情報設定手段が、前記設定領域が追加されたコンテンツデータのうち、前記属性情報設定領域内において、今回設定する前記真正確保情報が生成されるよりも後に設定が行われる前記属性情報が設定される部分と、前記真正確保情報が設定されていない前記真正確保情報設定領域と、を除く部分を対象として前記真正確保情報を所定の生成手段により生成させて、当該生成された真正確保情報を前記真正確保情報設定領域に設定し、

前記承認者情報の真正性を確保する前記真正確保情報を除く前記真正確保情報を設定する際には、前記真正確保情報設定手段が、前記真正確保情報により真正性が確保される前記属性情報を含んで前記生成手段により生成された当該真正確保情報から前記属性情報を取得して、当該取得された属性情報を前記属性情報設定領域に設定することを特徴とする情報生成方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンテンツデータの真正性を確保する電子署名等の真正確保情報をコンテンツデータに付加したコンテンツデータを生成する情報生成処理プログラム、情報生成装置及び情報生成方法の技術分野に関する。

【背景技術】

【０００２】

近年、インターネットやイントラネット等のネットワーク上において、電子文書等といったコンテンツデータの公開や送受信等が盛んになるにつれて、真正性を確保することが重要なコンテンツデータに対して電子署名（デジタル署名とも称されている）の手法を用いて、コンテンツデータが改竄されていないことを保証する電子署名情報を生成し、当該電子署名情報を当該コンテンツデータに付加することが行われるようになってきている。

【０００３】

かかる電子署名の一般的なものとしては、コンテンツデータが改竄されていないことを保証するとともに当該コンテンツデータを承認した者等を証明（本人性を確保）するために用いられている。

【０００４】

この場合は、例えば、承認者の情報処理装置は、コンテンツデータに署名者（承認者）の名称、署名日時、署名理由等の属性情報を付加し、これらの情報を強力な一方向性ハッシュ関数により固定長のダイジェストに変換した後、当該ダイジェストを秘密鍵で暗号化することにより電子署名情報を生成し、当該電子署名情報をコンテンツデータに付加してネットワークを介して送信する。

【０００５】
一方、コンテンツデータの受信者の情報処理装置は、当該コンテンツデータに付加された電子署名情報を署名者の公開鍵により復号し、コンテンツデータ及びこれに付加された署名者の名称、署名日時、署名理由等の属性情報を前記ハッシュ関数と同一のハッシュ関数によりダイジェストに変換し、当該ダイジェストと復号された情報とを比較することにより、当該コンテンツデータが前記の作成者により作成されたものか否か、改竄されているか否かを検証する。
【０００６】
しかし、上記電子署名においては、署名者の真正性を確保することはできても署名時刻の真正性を確保することはできない。なぜなら、電子署名の属性情報として付加される署名時刻は、一般的には署名者自身の情報処理装置のタイマ回路等から取得される信頼性の低い情報だからである。
【０００７】
そこで、コンテンツデータがある日時に存在していたことを証明（存在性を確保）するためには、ＣＡ（Certificate Authority）等の信頼性のある第三者機関が提供するタイムスタンプサービス（タイムスタンピングサービスとも称されている）が利用されている。
【０００８】
かかるサービスにおいては、例えば、承認者の情報処理装置は、コンテンツデータのダイジェストを生成し、当該ダイジェストを、ネットワークを介して第三者機関のサーバに送信すると、第三者機関のサーバは、受信したダイジェスト及び原子時計等により正確に得られた日時情報を第三者機関自身の秘密鍵で暗号化することにより電子署名情報を生成し、当該電子署名情報と日時情報とを含むタイムスタンプトークンを署名者の情報処理装置に送信する。そして、署名者の情報処理装置は、受信したタイムスタンプトークンをコンテンツデータに付加してネットワークを介して送信する。
【０００９】
一方、コンテンツデータの受信者の情報処理装置は、当該コンテンツデータに付加されたタイムスタンプトークンの電子署名情報部分を第三者機関の公開鍵により復号することにより、当該コンテンツデータが日時情報に示される日時に存在していたか否かを検証する。
【００１０】
ところで、一つのコンテンツデータについて、その本人性と存在性（誰が何時承認したか）等、複数の属性についてその真正性を証明したい場合には、従来、例えば、特許文献１及び２に記載されているように、証明したい属性夫々について電子署名を実施することにより、複数の電子署名情報を生成し、当該コンテンツデータに付加することが一般的であった。
【００１１】
【特許文献１】特開２００５－２２９４５０号公報
【特許文献２】特開２００５－３０３９５１号公報
【発明の開示】
【発明が解決しようとする課題】
【００１２】
しかしながら、上述したような従来の方法では、電子署名情報毎に個々の属性の真正性を確保することはできても、個々の属性を関連付けて真正性を確保することは困難である。例えば、電子署名情報により本人性が確保され、タイムスタンプトークンにより存在性が確保されるとしても、電子署名情報に示される承認者が、タイムスタンプトークンに示される日時にコンテンツデータを真に承認したものとはいいきれない。
【００１３】
本発明は、以上の点に鑑みてなされたものであり、複数の真正確保情報によりコンテンツデータの真正性が確保される夫々の属性同士の関連性を強めて、その真正性を確実にす

ることを可能とする情報生成処理プログラム、情報生成装置及び情報生成方法を提供することを目的とする。

【課題を解決するための手段】

【００１４】

上記課題を解決するために、請求項１に記載の発明は、コンテンツデータの真正性を確保する複数の真正確保情報を、当該複数の真正確保情報により真正性が夫々確保される属性を示す複数の属性情報とともに付加したコンテンツデータを生成するコンピュータを、前記複数の属性情報が設定される属性情報設定領域と、互いに異なる前記真正確保情報が設定される複数の真正確保情報設定領域と、を含む１の設定領域を前記コンテンツデータに追加する設定領域追加手段、前記属性情報として少なくとも、前記コンテンツデータの承認者を示す承認者情報を前記属性情報設定領域に設定する属性情報設定手段、前記複数の真正確保情報の夫々を互いに異なる前記真正確保情報設定領域に順次設定する真正確保情報設定手段、として機能させ、前記真正確保情報設定手段は、前記真正確保情報を設定するとき、前記設定領域が追加されたコンテンツデータのうち、前記属性情報設定領域内において、今回設定する前記真正確保情報が生成されるよりも後に設定が行われる前記属性情報が設定される部分と、前記真正確保情報が設定されていない前記真正確保情報設定領域と、を除く部分を対象として前記真正確保情報を所定の生成手段により生成させて、当該生成された真正確保情報を前記真正確保情報設定領域に設定し、前記承認者情報の真正性を確保する前記真正確保情報を除く前記真正確保情報を設定する際には、前記真正確保情報により真正性が確保される前記属性情報を含んで前記生成手段により生成された当該真正確保情報から前記属性情報を取得して、当該取得された属性情報を前記属性情報設定領域に設定することを特徴とする。

【００１５】

請求項２に記載の発明は、請求項１に記載の情報生成処理プログラムにおいて、前記属性情報は、前記コンテンツデータを承認した日時を示す承認日時情報を含み、前記真正確保情報設定手段は、前記コンテンツデータの承認日時の真正性を確保する前記真正確保情報を設定する際に、前記真正確保情報により真正性が確保される現在日時を示す日時情報を含んで前記生成手段により生成された当該真正確保情報から前記日時情報を取得して、当該取得された日時情報を前記承認日時情報として前記属性情報設定領域に設定することを特徴とする。

【００１６】

請求項３に記載の発明は、請求項１または請求項２に記載の情報生成処理プログラムにおいて、前記コンテンツデータは所定のフォーマットで生成されたデータであり、前記設定領域追加手段は、前記フォーマットの仕様上、１の領域として前記設定領域を追加することを特徴とする。

【００１７】

請求項４に記載の発明は、請求項１乃至３のいずれか１項に記載の情報生成処理プログラムにおいて、前記コンテンツデータは、文字情報を少なくとも含む電子文書であり、前記承認者情報は、前記コンピュータが所定のアプリケーションプログラムを実行することにより前記電子文書が表示されたときに当該電子文書とともに表示される画像情報であって前記承認者を示す印影を表す画像情報を含むことを特徴とする。

【００１８】

請求項５に記載の発明は、請求項１乃至４のいずれか１項に記載の情報生成処理プログラムにおいて、前記設定領域追加手段は、前記設定領域に設定された前記複数の真正確保情報を夫々特定するための特定情報が設定される特定情報設定領域を含んで前記設定領域を追加し、各前記真正確保情報について、その種類を示す情報と、前記真正確保情報設定領域の範囲を示す情報と、を前記特定情報として前記特定情報設定領域に設定する特定情報設定手段として更に前記コンピュータを機能させることを特徴とする。

【００１９】

請求項６に記載の発明は、コンテンツデータの真正性を確保する複数の真正確保情報を

、当該複数の真正確保情報により真正性が夫々確保される属性を示す複数の属性情報とともに付加したコンテンツデータを生成する情報生成装置において、前記複数の属性情報が設定される属性情報設定領域と、互いに異なる前記真正確保情報が設定される複数の真正確保情報設定領域と、を含む１の設定領域を前記コンテンツデータに追加する設定領域追加手段と、前記属性情報として少なくとも、前記コンテンツデータの承認者を示す承認者情報を前記属性情報設定領域に設定する属性情報設定手段と、前記複数の真正確保情報の夫々を互いに異なる前記真正確保情報設定領域に順次設定する真正確保情報設定手段、とを備え、前記真正確保情報設定手段は、前記真正確保情報を設定するとき、前記設定領域が追加されたコンテンツデータのうち、前記属性情報設定領域内において、今回設定する前記真正確保情報が生成されるよりも後に設定が行われる前記属性情報が設定される部分と、前記真正確保情報が設定されていない前記真正確保情報設定領域と、を除く部分を対象として前記真正確保情報を所定の生成手段により生成させて、当該生成された真正確保情報を前記真正確保情報設定領域に設定し、前記承認者情報の真正性を確保する前記真正確保情報を除く前記真正確保情報を設定する際には、前記真正確保情報により真正性が確保される前記属性情報を含んで前記生成手段により生成された当該真正確保情報から前記属性情報を取得して、当該取得された属性情報を前記属性情報設定領域に設定することを特徴とする。

【００２０】

請求項７に記載の発明は、コンテンツデータの真正性を確保する複数の真正確保情報を、当該複数の真正確保情報により真正性が夫々確保される属性を示す複数の属性情報とともに付加したコンテンツデータを生成する情報生成装置により実行される情報生成方法において、前記情報生成装置が備える設定領域追加手段が、前記複数の属性情報が設定される属性情報設定領域と、互いに異なる前記真正確保情報が設定される複数の真正確保情報設定領域と、を含む１の設定領域を前記コンテンツデータに追加する設定領域追加工程と、前記情報生成装置が備える属性情報設定手段が、前記属性情報として少なくとも、前記コンテンツデータの承認者を示す承認者情報を前記属性情報設定領域に設定する属性情報設定工程と、前記情報生成装置が備える真正確保情報設定手段が、前記複数の真正確保情報の夫々を互いに異なる前記真正確保情報設定領域に順次設定する真正確保情報設定工程と、を含み、前記真正確保情報設定工程において、前記真正確保情報を設定するとき、前記真正確保情報設定手段が、前記設定領域が追加されたコンテンツデータのうち、前記属性情報設定領域内において、今回設定する前記真正確保情報が生成されるよりも後に設定が行われる前記属性情報が設定される部分と、前記真正確保情報が設定されていない前記真正確保情報設定領域と、を除く部分を対象として前記真正確保情報を所定の生成手段により生成させて、当該生成された真正確保情報を前記真正確保情報設定領域に設定し、前記承認者情報の真正性を確保する前記真正確保情報を除く前記真正確保情報を設定する際には、前記真正確保情報設定手段が、前記真正確保情報により真正性が確保される前記属性情報を含んで前記生成手段により生成された当該真正確保情報から前記属性情報を取得して、当該取得された属性情報を前記属性情報設定領域に設定することを特徴とする。

【発明の効果】

【００２１】

請求項１に記載の発明によれば、各真正確保情報により真正性が確保された情報が属性情報として属性設定領域に設定さることにより、当該設定された属性情報により、複数の真正確保情報が関連付けられるので、より正確な属性情報をユーザに認識させることができ、また、その属性情報の真正性を検証することもできる。

【００２２】

請求項２に記載の発明によれば、何時誰がコンテンツデータの内容を承認したかということについて、その真正性をより確実にすることができる。

【００２３】

請求項３に記載の発明によれば、各真正確保情報の関連性が強まるため、真正性が確保される夫々の属性情報同士の関連性を強めて、その真正性をより確実にすることができる

。
【００２４】
請求項４に記載の発明によれば、複数の真正確保情報が１つの設定領域に設定されて電子文書に付加されていること、及び当該電子文書の内容を承認した者を容易に認識することがきる。
【００２５】
請求項５に記載の発明によれば、各真正確保情報を確実に特定することができるので、設定する真正確保情報の種類や数等を容易に変更することができる。
【発明を実施するための最良の形態】
【００２６】
以下、図面を参照して本発明の最良の実施形態について詳細に説明する。なお、以下に説明する実施の形態は、電子文書に対して真正確保情報の一例としての電子署名情報及びタイムスタンプトークンを含む複合署名情報を作成し、当該複合署名情報を電子文書に付加することにより複合電子署名を実施する署名付電子文書作成装置に対して本発明を適用した場合の実施形態である。
【００２７】
［１．複合署名情報が付加された電子文書の構造］
始めに、本実施形態に係る複合署名情報が付加された電子文書（以下、複合署名付電子文書と称する）の構造等について、図１を用いて説明する。なお、以下の説明において、単に電子文書というときは、複合署名情報が付加されていない電子文書及び複合署名付電子文書の双方を意味するものとする。
【００２８】
図１は、本実施形態に係る複合署名付電子文書１００の構造の一例を示す図である。
【００２９】
図１に示すように、複合署名付電子文書１００は、署名対象である元の電子文書１０１と、設定領域の一例としての複合署名領域１０２と、により構成される。
【００３０】
ここで、本実施形態に係る電子文書は、署名付電子文書作成装置が所定のアプリケーションプログラム（以下、所定アプリケーションと称する）を実行することにより、処理（例えば、表示、印刷、編集等）することが可能な所定フォーマットの電子文書ファイルである。当該フォーマットは、複数のデータを１ファイルとして取り扱うことが可能であり、この場合、１ファイル中に複数の領域が設けられて、当該領域夫々にデータが格納される。また、当該フォーマットは、元の電子文書ファイルに新たにデータを追加することが可能となっており、この場合は、元のファイルに新たな領域が追加されて、当該領域に新たなデータが格納される。このようなフォーマットの一例としては、Adobe Systems社が提唱するＰＤＦ（Portable Document Format）が挙げられるが、後から複合署名情報等のデータを追加することが可能であれば、これ以外のフォーマットを用いても良い。なお、所定アプリケーションの一例としては、Adobe Systems社のAdobe Acrobat（商標）が挙げられるが、これに限られるものではない。
【００３１】
本実施形態においては所定フォーマットの仕様に従い、電子文書１０１が格納される領域とは別に新たな領域として複合署名領域１０２を設けて、当該領域に複合署名情報を格納するようになっている。ここで、上記フォーマット仕様に従った場合、複合署名付電子文書１００には、例えば、ヘッダ領域や各領域を管理するための領域等が存在するが、図示は省略する。なお、元の電子文書１０１には、複数のデータが含まれても良く、この場合、先に付加された複合署名情報等の電子署名情報が含まれていても良い。
【００３２】
複合署名領域１０２内には、属性情報設定領域の一例としての属性領域２００と、特定情報設定領域の一例としての分割管理領域３００と、署名格納領域４００と、が設けられている。

【００３３】
属性領域２００には、複合電子署名の属性情報が設定される領域であり、署名識別部２０１、承認者情報の一例としての署名イメージ２０２及び署名者２０３、承認日時情報の一例としての署名時刻２０４、署名理由２０５及び署名場所２０６が設定される。
【００３４】
署名識別部２０１は、複合署名領域１０２が電子署名情報を格納した領域であることを示す識別情報であり、上記フォーマット仕様により設定すべき識別情報が定められている。
【００３５】
署名イメージ２０２は、電子文書１０２の内容等を承認した者（電子文書１０２を作成した者等を含む）の名称等が刻印された印鑑の印影を表した印影画像データであり、署名付電子文書作成装置が所定アプリケーションを実行したときに、当該印影が電子文書に重畳して表示される。なお、署名イメージ２０２には、その印影が表示される際における表示位置を示す情報（例えば、電子文書上における表示ページ及び表示座標等）が含まれている。
【００３６】
署名者２０３は、電子文書１０２の内容等を承認した者の名称を示すテキストである。
【００３７】
また、署名時刻２０４は、電子文書１０２の内容等を承認した日時をＵＴＣ（Coordinated Universal Time）で表した日時情報であり、後述するように正確な日時情報が設定される。
【００３８】
署名理由２０５は、電子文書１０２の内容等を承認する理由を示すテキストであり、署名場所２０６は、承認した場所を示すテキストであるが、本実施形態においては、夫々署名者により入力された任意の情報等が設定される。
【００３９】
次に、分割管理領域３００は、電子署名情報とタイムスタンプトークンとを特定するための管理領域であり、領域分割数３０１、目次情報３０２及び３０３が設定される。
【００４０】
領域分割数３０１は、署名格納領域４００内に設けられた署名領域の数を示す情報であり、本実施形態においては２である。
【００４１】
目次情報３０２及び３０３には、夫々電子署名領域４０１（領域＃１）及びタイムスタンプ領域４０２（領域＃２）の種類と、範囲を示す情報の一例としての開始位置（例えば、複合署名領域１０２先頭からのオフセット位置）及びサイズとが設定される。
【００４２】
次に、署名格納領域４００には、真正確保情報設定領域の一例として、電子署名情報が設定される電子署名領域４０１及びタイムスタンプトークンが設定されるタイムスタンプ領域４０２が設けられている。
【００４３】
当該各領域は本実施形態における独自の領域であるり、上記フォーマット上は、まとまった一つの複合署名領域１０２として認識されるものである。
【００４４】
属性領域２００、分割管理領域３００及び署名格納領域４００（電子署名領域４０１及びタイムスタンプ領域４０２）は、複合署名領域１０２を独自に内部分割したものである。このように、所定フォーマットの仕様に従い一つの領域を複合署名領域１０２として追加し、その内部を独自に分割して電子署名情報とタイムスタンプトークンとを設定可能とする構造とすることにより、署名付電子文書作成装置が所定アプリケーションを実行した際には、一つの電子署名情報として認識されるようになっている。
【００４５】

［２．署名付電子文書作成装置の構成及び機能等］

次に、本実施形態に係る署名付電子文書作成装置１の構成及び機能等について、図２を用いて説明する。

【００４６】

図２は、本実施形態に係る署名付電子文書作成装置１の概要構成の一例を示す図である。

【００４７】

図２に示すように、署名付電子文書作成装置１は、ネットワークＮＷに接続されるようになっている。このネットワークＮＷは、例えば、ローカルエリアネットワーク、公衆回線網、移動体通信回線網、インターネット等を含んで構成されている。

【００４８】

ネットワークＮＷには、署名付電子文書作成装置１以外にも当該署名付電子文書作成装置１と同様の構成を有する署名付電子文書作成装置１ａ及び１ｂが接続されている。署名付電子文書作成装置１、１ａ及び１ｂは、夫々複合署名情報付の電子文書を作成可能であり、当該電子文書等のデータを、ネットワークＮＷを介して相互に送受信することが可能である。また、これらの署名付電子文書作成装置は、複合署名情報付の電子文書の検証が夫々可能である。これらの署名付電子文書作成装置は、例えば、同一企業に属する各社員等により夫々使用される。なお、以下においては、署名付電子文書作成装置１、１ａ及び１ｂを代表して署名付電子文書作成装置１について主に説明する。

【００４９】

ネットワークＮＷには、更に、タイムスタンプトークンを生成する生成手段の一例としてのタイムスタンプサーバ２が接続されている。タイムスタンプサーバ２と署名付電子文書作成装置１とは、ネットワークＮＷを介して相互にデータを送受信することが可能である。このタイムスタンプサーバ２は、例えば、図示せぬ原子時計等から正確な日時情報をタイムスタンプ時刻として取得するようになっている。そして、タイムスタンプサーバ２は、署名付電子文書作成装置１等から電子文書のダイジェストを受信し、当該ダイジェストとタイムスタンプ時刻等を暗号化し、これらの情報からなるタイムスタンプトークンを署名付電子文書作成装置１に送信するようになっている。なお、タイムスタンプサーバ２の構成及び機能は公知であるため、詳細な説明は省略する。

【００５０】

署名付電子文書作成装置１は、図２に示すように、ネットワークＮＷに接続して署名付電子文書作成装置１ａ、１ｂやタイムスタンプサーバ２との通信を制御する信部１１と、文字や画像等の情報を表示する表示部１２（例えば、液晶ディスプレイ等）と、ユーザからの操作指示を受け付け、その指示内容を指示信号としてシステム制御部１６に出力する操作部１３（例えば、ボタン、キーボード、マウス等）と、現在の日時を示す日時情報をシステム制御部１６に出力する計時部１４と、各種プログラム及びデータ等を記憶する記憶部１５（例えば、ハードディスクドライブ、フラッシュメモリ等）と、ＣＰＵ（Central Processing Unit）、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等を備える設定領域追加手段、属性情報設定手段、特定情報設定手段、真正確保情報設定手段及び生成手段の一例としてのシステム制御部１６と、を備え、システム制御部１６と各部とはシステムバス１７を介して相互に接続されている。

【００５１】

署名付電子文書作成装置１としては、例えば、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）等を適用することができるが、これらに限られるものではない。

【００５２】

記憶部１５には、所定のオペレーティングシステム、各種アプリケーションプログラム、情報生成処理プログラムの一例としての複合電子署名プログラム等が記憶されている。なお、複合電子署名プログラム等は、例えば、ネットワークＮＷを介して所定のサーバ等からダウンロードされるようにしても良いし、ＣＤ－ＲＯＭ等の記録媒体に記録されて、

光ディスクドライブ等を介して読み込まれるようにしても良い。

【００５３】

また、記憶部１５には、複数の電子文書が所定のフォーマットの電子文書ファイルとして記憶されている。

【００５４】

更に、記憶部１５には、印鑑管理情報、電子署名作成用の秘密鍵、電子証明書、タイムスタンプ検証用の公開鍵等が記憶されている。

【００５５】

印鑑管理情報は、署名付電子文書作成装置１のユーザの所有する印鑑に関する情報であり、具体的には、その印影を表した印影画像データ及び所有者名（すなわちユーザの名称）が含まれている。印影画像データは、例えば、実際にユーザが所有する印鑑の印影がイメージスキャナ等により取り込まれ、所定フォーマットの画像データとして記憶される。

【００５６】

電子署名作成用の秘密鍵は、電子文書の署名者が署名付電子文書作成装置１のユーザであることを保証するための電子署名情報を作成する際に用いられる鍵である。当該秘密鍵を用いて電子署名情報を作成するためには、当該ユーザ自身の電子証明書が必要である。

【００５７】

電子証明書は、署名付電子文書作成装置１のユーザ自身の電子証明書と、他の署名付電子文書作成装置１ａ、１ｂのユーザの電子証明書が存在する。この電子証明書は、ユーザに対してＣＡ等から発行された情報であり、秘密鍵を用いて作成された電子署名情報を検証するための公開鍵を含んでいる。

【００５８】

タイムスタンプ検証用の公開鍵は、タイムスタンプサーバ２により作成されたタイムスタンプトークンを検証するための鍵である。

【００５９】

システム制御部１６は、ＲＯＭや記憶部１５に記憶された各種プログラムを読み出し実行することにより署名付電子文書作成装置１全体を制御するとともに、設定領域追加手段、属性情報設定手段、特定情報設定手段、真正確保情報設定手段及び電子署名情報を作成する生成手段として機能するようになっている。

【００６０】

具体的に、システム制御部１６は、所定アプリケーションを実行することにより、電子文書を表示部１２の画面に表示するようになっている。

【００６１】

図３は、複合署名付電子文書の表示画面の一例を示す図である。

【００６２】

図３に示すように、電子文書の表示画面において、電子文書表示エリア５１には、電子文書が表示される。そして、当該電子文書が複合署名付電子文書である場合、電子文書表示エリア５１には、署名者を示す印影画像５２が電子文書に重畳して表示される。印影画像５２は、署名イメージ２０２に基づいて表示されるものである。この印影画像５２が電子文書とともに表示されることにより、ユーザは電子文書に複合署名情報が付加されていることを認識することができる。

【００６３】

署名リスト表示エリア５３には、電子文書表示エリア５１に表示されている電子文書に付加されている全電子署名情報の目次情報が表示される。本実施形態に係る複合署名情報は電子署名情報及びタイムスタンプトークンを含んでいるが、前述した構造により、電子文書表示エリア５１には複合署名情報の目次情報５４のみが表示される（勿論、他の電子署名情報が付加されている場合にはこの限りではない）。

【００６４】

次に、システム制御部１６は、複合電子署名プログラムを実行することにより、設定領域追加手段として、複合署名領域１０２のサイズを計算した後、所定フォーマットの仕様

に従い署名対象の電子文書に対して複合署名領域１０２を追加するようになっている。
【００６５】
また、属性情報設定手段としてのシステム制御部１６は、追加された複合署名領域１０２の属性領域２００に各属性情報を設定するようになっている。
【００６６】
更に、特定情報設定手段としてのシステム制御部１６は、追加された複合署名領域１０２の分割管理領域に領域分割数３０１、目次情報３０２及び３０３を設定するようになっている。
【００６７】
また更に、真正確保情報設定手段としてのシステム制御部１６は、追加された複合署名領域１０２の電子署名領域４０１及びタイムスタンプ領域４０２に夫々電子署名情報及びタイムスタンプトークンを設定するようになっている。
【００６８】
先ず、システム制御部１６は、電子署名情報を設定するために、複合署名領域１０２が追加された電子文書のうち、属性領域２００の署名時刻２０４が設定される部分、電子署名領域４０１及びタイムスタンプ領域４０２（署名格納領域４００全範囲）を除いた範囲についてのダイジェストを計算するようになっている。ここで、署名時刻２０４が設定される部分をダイジェスト計算の対象から除外しているのは、後で、タイムスタンプトークンに含まれるタイムスタンプ時刻が設定されるからである。そして、生成手段としてのシステム制御部１６は、当該ダイジェストを署名付電子文書作成装置１のユーザ自身の秘密鍵で暗号化したものを電子署名情報として生成するようになっている。
【００６９】
次いで、システム制御部１６は、タイムスタンプトークンを設定するために、複合署名領域１０２が追加された電子文書のうち、属性領域２００の署名時刻２０４が設定される部分及びタイムスタンプ領域４０２を除いた範囲についてのダイジェストを計算するようになっている。そして、当該ダイジェストをパラメータとしてタイムスタンプトークンの作成リクエストをタイムスタンプサーバ２に送信するとともに、当該タイムスタンプサーバ２から送信されたタイムスタンプトークンを受信し、当該タイムスタンプトークンに含まれるタイムスタンプ時刻を署名時刻２０４として属性領域２００に設定するようになっている。
【００７０】
なお、複合電子署名プログラムは、例えば、所定アプリケーションからは独立して実行されるようにしても良いし、所定アプリケーションから呼び出されることにより当該アプリケーションのアドイン等として実行されるようにしても良い。
【００７１】
［３．署名付電子文書作成装置の動作］
次に、署名付電子文書作成装置１の動作について、図４乃至図６を用いて説明するが、複合電子署名を実施する場合と、複合電子署名により複合署名付電子文書を検証する場合と、に分けて説明する。
【００７２】
図４は、本実施形態に係る署名付電子文書作成装置１のシステム制御部１６の複合電子署名を実施する場合における処理例を示す図である。
【００７３】
複合電子署名を実施する場合、先ずユーザは、マウス等の操作部１３を操作することによりシステム制御部１６に複合電子署名プログラムを起動させ、署名対象となる電子文書を表示部１２の画面に表示させる。そして、ユーザは、画面表示された電子文書に対して自身の印鑑の捺印場所（印影画像を表示させる位置）を操作部１３により指定する。
【００７４】
そうすると、システム制御部１６は、図４に示すように、複合署名領域１０２のサイズを計算する（ステップＳ１）。具体的に、属性領域２００に設定される各属性情報は固定

サイズであるため、属性領域２００のサイズは予め設定等されているサイズとする。また、分割管理領域３００のサイズは、領域分割数３０１のサイズ＋１目次情報のサイズ×目次情報の数（署名格納領域に設定される電子署名情報の数）を計算することにより求める。また、電子署名情報及びタイムスタンプトークンは、対象となるダイジェストの内容の如何にかかわらず一定のサイズで得られるため、例えば、ＲＡＭ等に設定したダミーデータを対象として得られた電子署名情報及びタイムスタンプトークンのサイズを夫々電子署名領域４０１及びタイムスタンプ領域４０２のサイズとする。なお、電子署名領域４０１及びタイムスタンプ領域４０２のサイズを夫々予め設定等されている固定サイズとして複合署名領域１０２のサイズを計算するようにしても良い。

【００７５】

その後、システム制御部１６は、所定フォーマットの仕様に従い、電子文書に対して複合署名領域１０２をステップＳ１で求められたサイズで追加し、当該領域に初期値としてゼロデータを設定する（ステップＳ２）。

【００７６】

次いで、システム制御部１６は、追加された複合署名領域１０２の属性領域２００に各属性情報を設定する（ステップＳ３）。具体的に、システム制御部１６は、所定フォーマットの仕様に従った識別情報を署名識別部２０１として設定する。また、システム制御部１６は、記憶部１５に印鑑管理情報として記憶されている印影画像データ及びユーザにより指定された印影画像の表示位置を署名イメージ２０２として設定し、印鑑の所有者名を署名者２０３として設定する。また、システム制御部１６は、計時部１４から取得した現在の日時情報を署名時刻２０４として仮に設定するが、この時点では設定しなくても良い。また、システム制御部１６は、例えば、「私はこの文書の作成者です。」等の任意のテキストを署名理由２０５として設定し、「×××株式会社」等の任意のテキストを署名場所２０６として設定する。

【００７７】

そして、システム制御部１６は、追加された複合署名領域１０２の分割管理領域３００に各管理情報を設定する（ステップＳ４）。具体的に、システム制御部１６は、領域分割数３０１として２を設定する。また、システム制御部１６は、電子署名領域４０１及びタイムスタンプ領域４０２の開始位置、サイズ及び種類を夫々目次情報３０２及び目次情報３０３として設定する。

【００７８】

次いで、システム制御部１６は、電子文書の電子署名情報を作成する（ステップＳ５）。具体的に、システム制御部１６は、複合署名領域１０２が追加された電子文書のうち、属性領域２００の署名時刻２０４が設定される部分と電子署名領域４０１とタイムスタンプ領域４０２とを除いた範囲について、そのダイジェストを所定のハッシュ関数を用いて作成する。そして、システム制御部１６は、作成されたダイジェストを記憶部１５に記憶されたユーザ自身の秘密鍵で暗号化し、電子署名情報を作成する。

【００７９】

そして、システム制御部１６は、作成された電子署名情報を、電子署名領域４０１に設定する（ステップＳ６）。

【００８０】

次いで、システム制御部１６は、電子文書のタイムスタンプトークンを取得する（ステップＳ７）。具体的に、システム制御部１６は、複合署名領域１０２が追加された電子文書のうち、属性領域２００の署名時刻２０４が設定される部分とタイムスタンプ領域４０２とを除いた範囲について、そのダイジェストを所定のハッシュ関数を用いて作成する。そして、システム制御部１６は、作成されたダイジェストをパラメータとして、タイムスタンプトークンの作成リクエストを、ネットワークＮＷを介してタイムスタンプサーバ２に送信する。

【００８１】

リクエストを受信したタイムスタンプサーバ２は、現在の正確な日時情報をタイムスタ

ンプ時刻として取得し、当該タイムスタンプ時刻及び受信したダイジェスト等を秘密鍵で暗号化し、前記タイムスタンプ時刻及びダイジェスト等と当該暗号化されたデータとを結合してタイムスタンプトークンを作成する。そして、タイムスタンプサーバ２は、作成されたタイムスタンプトークンを署名付電子文書作成装置１に送信する。

【００８２】

システム制御部１６は、タイムスタンプトークンを受信すると、当該タイムスタンプトークンをタイムスタンプ領域４０２に設定する（ステップＳ８）。

【００８３】

次いで、システム制御部１６は、タイムスタンプトークンに含まれるタイムスタンプ時刻を取得し、当該日時情報を署名時刻２０４として属性領域２００に設定し（ステップＳ９）、処理を終了する。

【００８４】

図５（ａ）は、電子署名情報表示画面の一例を示す図であり、図５（ｂ）は、タイムスタンプ情報表示画面の一例を示す図である。

【００８５】

上述のように複合電子署名情報が付加された電子文書を、所定アプリケーションにより表示させると、前記図３に示すように表示される。そして、図３に示す表示画面において例えば、ユーザが印影画像５２または目次情報５４を選択すると、図５（ａ）に示すような電子署名情報表示画面が表示される。

【００８６】

図５（ａ）において、署名情報表示エリア６１には、属性領域２００に設定された署名者２０３、署名時刻２０４、署名理由２０５及び署名場所２０６が表示される。

【００８７】

検証結果表示エリア６２には、電子署名領域４０１に設定された電子署名情報により電子文書を検証した結果が表示される。

【００８８】

ＯＫボタン６３は電子署名情報表示画面を消去するためのボタンであり、電子証明書ボタン６４は電子文書に署名した者（署名情報表示エリア６１に表示される署名者）の電子証明書の情報を表示するためのボタンである。

【００８９】

そして、ユーザがタイムスタンプボタン６５を選択すると、図５（ｂ）に示すようなタイムスタンプ情報表示画面が表示される。

【００９０】

図５（ｂ）において、検証結果表示エリア７１には、タイムスタンプ領域４０２に設定されたタイムスタンプトークンにより電子文書を検証した結果が表示される。

【００９１】

また、タイムスタンプ時刻表示エリア７２には、タイムスタンプトークンに含まれるタイムスタンプ時刻が表示される。

【００９２】

また、ＯＫボタン７３はタイムスタンプ情報表示画面を消去するためのボタンであり、詳細ボタン７４はタイムスタンプトークンの詳細な情報を表示するためのボタンである。

【００９３】

ここで、前記ステップＳ９において、タイムスタンプトークンに含まれるタイムスタンプ時刻を署名時刻に設定したので、図５（ａ）及び（ｂ）に示すように、電子署名情報表示画面に表示された署名時刻とタイムスタンプ情報表示画面に表示されたタイムスタンプ時刻が同一になっている。このように、電子署名の署名時刻とタイムスタンプのタイムスタンプ時刻とを関連させたので、複合電子署名の属性情報として正確な署名時刻を表示させることができる。つまり、「何時誰が承認したか」ということをより正確に表示することができる。

【００９４】

図６は、本実施形態に係る署名付電子文書作成装置１のシステム制御部１６の複合電子署名により複合署名付電子文書を検証する場合における処理例を示す図である。

【００９５】

複合電子署名により複合署名付電子文書を検証する場合、図６に示すように、システム制御部１６は、追加されている複合署名領域１０２の分割管理領域３００を参照してタイムスタンプ領域４０２の位置、サイズを特定し、タイムスタンプ領域４０２からタイムスタンプトークンを読み出しＲＡＭ上にコピーする（ステップＳ２１）。

【００９６】

次いで、システム制御部１６は、タイムスタンプにより複合署名付電子文書を検証する（ステップＳ２２）。具体的にシステム制御部１６は、複合署名付電子文書のうち、タイムスタンプを実施したときと同一の範囲（属性領域２００の署名時刻２０４が設定された部分とタイムスタンプ領域４０２とを除いた範囲）について、タイムスタンプを実施したときと同一のハッシュ関数によりダイジェストを作成する。そして、作成されたダイジェストとＲＡＭ上にコピーされたタイムスタンプトークンに含まれるダイジェストとを比較する。また、システム制御部１６は、タイムスタンプトークンに含まれる暗号化データをタイムスタンプ検証用の公開鍵で復号し、当該復号されたデータと前記ダイジェストとを比較する。

【００９７】

そして、システム制御部１６は、上記検証の結果が正常であるか否かを判定し（ステップＳ２３）、作成されたダイジェストとタイムスタンプトークンに含まれるダイジェストとが一致しない場合、または、前記復号されたデータと前記ダイジェストとが一致しない場合は、異常が検出されたと判定し（ステップＳ２３：ＮＯ）、タイムスタンプによる検証において異常が検出されたことを示す情報を表示部１２の画面に表示し（ステップＳ３０）、処理を終了する。

【００９８】

一方、作成されたダイジェストとタイムスタンプトークンに含まれるダイジェストとが一致し、且つ、前記復号されたデータと前記ダイジェストとが一致する場合、システム制御部１６は、正常であると判定し（ステップＳ２３：ＹＥＳ）、属性領域２００に設定されている署名時刻とタイムスタンプトークンに含まれているタイムスタンプ時刻とを比較する（ステップＳ２４）。

【００９９】

そして、システム制御部１６は、署名時刻とタイムスタンプ時刻とが一致するか否かを判定し（ステップＳ２５）、一致しない場合は（ステップＳ２５：ＮＯ）、署名時刻が改竄されたことを示す情報を表示部１２の画面に表示し（ステップＳ３０）、処理を終了する。

【０１００】

一方、署名時刻とタイムスタンプ時刻とが一致する場合（ステップＳ２５：ＹＥＳ）、システム制御部１６は、分割管理領域３００を参照して電子署名領域４０１の位置、サイズを特定し、電子署名領域４０１から電子署名情報を読み出しＲＡＭ上にコピーする（ステップＳ２６）。

【０１０１】

次いで、システム制御部は、電子署名により複合署名付電子文書を検証する（ステップＳ２７）。具体的にシステム制御部１６は、複合署名付電子文書のうち、電子署名を実施したときと同一の範囲（属性領域２００の署名時刻２０４が設定された部分と電子署名領域４０１とタイムスタンプ領域４０２とを除いた範囲）について、電子署名を実施したときと同一のハッシュ関数によりダイジェストを作成する。そして、ＲＡＭ上にコピーされた電子署名情報を属性領域２００に設定された署名者２０３が示す署名者の公開鍵で復号し、当該復号されたデータと前記ダイジェストとを比較する。

【０１０２】

そして、システム制御部は、上記検証の結果が正常であるか否かを判定し（ステップＳ

２８）、前記復号されたデータとダイジェストとが一致しない場合は、異常が検出されたと判定し（ステップＳ２８：ＮＯ）、電子署名による検証において異常が検出されたことを示す情報を表示部１２の画面に表示し（ステップＳ３０）、処理を終了する。

【０１０３】

一方、前記復号されたデータとダイジェストとが一致する場合、システム制御部１６は、正常であると判定し（ステップＳ２８：ＹＥＳ）、総合的な検証結果が正常であることを示す情報及び個別の検証結果が夫々正常であることを示す情報を表示部１２の画面に表示し（ステップＳ２９）、処理を終了する。

【０１０４】

以上説明したように、本実施形態によれば、システム制御部１６が、複合電子署名の属性情報が設定される属性領域２００と、電子署名情報が設定される電子署名領域４０１と、タイムスタンプトークンが設定されるタイムスタンプ領域４０２と、を含む１の複合署名領域１０２を電子文書に追加した後、属性領域２００に各属性情報を設定し、複合署名領域１０２が追加された電子文書のうち、属性領域２００の署名時刻２０４が設定される部分と電子署名領域４０１とタイムスタンプ領域４０２とを除いた範囲について、電子署名情報を作成し、当該電子署名情報を電子署名領域４０１に設定した後、複合署名領域１０２が追加された電子文書のうち、属性領域２００の署名時刻２０４が設定される部分とタイムスタンプ領域４０２とを除いた範囲について、タイムスタンプサーバ２によりタイムスタンプトークンを作成させ、当該タイムスタンプトークンをタイムスタンプ領域４０２に設定するとともに、当該タイムスタンプトークンに含まれているタイムスタンプ時刻を署名時刻２０４として属性領域２００に設定するようになっている。

【０１０５】

従って、電子署名とタイムスタンプとが関連付けられることにより、電子文書を何時誰が承認したかということをより正確に表示することができる。また、署名時刻２０４の真正性を容易に検証することができる。

【０１０６】

また、上記の電子文書は所定フォーマットで作成されたデータであり、システム制御部１６は、複合署名領域１０２を当該フォーマットの仕様上１つの領域として電子文書に追加するので、電子イメージ２０２及び署名者２０３と署名時刻２０４との関連性がより強まり、電子文書を何時誰が承認したかということについて、その真正性をより確実にすることができる。

【０１０７】

また、属性領域２００には、署名者を示す印影を表した署名イメージ２０２が含まれており、システム制御部１６が所定アプリケーションを実行して電子文書を画面に表示させたときに、当該電子文書に重畳してその印影が表示されるので、ユーザは、電子文書に対して複合電子署名が実施されていること及びその実施者を容易に認識することがきる。

【０１０８】

また、複合署名領域１０２には、署名格納領域４００に設定された複数の電子署名情報を分割管理するための分割管理領域３００が設けられており、当該分割管理領域３００には、各電子署名情報の種類及び各電子署名領域の開始位置及びサイズが設定されるので、各電子署名情報を確実に特定することができ、また、複合電子署名に用いる電子署名の変更や拡張等に柔軟に対応することができる。

【０１０９】

なお、上記説明した実施形態においては、電子署名情報を先に作成し、タイムスタンプトークンを後に作成するようにしていたが、この順番を入れ替えても良い。この場合、タイムスタンプトークンを作成する際には、電子署名領域４０１及びタイムスタンプ領域４０２をダイジェスト作成対象から除外し、電子署名情報を作成する際には、電子署名領域４０１をダイジェスト作成対象から除外すれば良い。つまり、まだ電子署名情報が設定されていない電子署名領域をダイジェスト作成対象から除外すれば良いのである。

【０１１０】

また、用いる電子署名の種類としては、本人性を確保する電子署名とタイムスタンプのみに限られるものではなく、他の種類の電子署名を用いても良い。例えば、本人性を確保する電子署名と、ＧＰＳ（Global Positioning System）等により正確な署名場所を取得可能で且つ当該署名場所の真正性を確保することができる電子署名とを用いて、「何処で誰が承認したか」ということを確実にするための複合電子署名情報を作成するようにしても良い。この場合、各電子署名を作成する際には、属性領域２００の署名場所２０６が設定される部分をダイジェスト作成対象から除外すれば良い。

【０１１１】

また、用いる電子署名の数は３種類以上であっても良く、例えば、「何時何処で誰が承認したか」ということを確実にするための複合電子署名情報を作成するようにしても良い。このような場合は、分割管理領域３００及び署名格納領域４００のサイズを適切なサイズに設定するとともに、領域分割数３０１として適切な数を設定すればよい。

【０１１２】

また、用いる電子署名の数及び種類が固定であれば複合署名領域１０２に分割管理領域３００を設けなくても良い。

【０１１３】

また、電子署名の方式、暗号化方式、電子署名情報をどの装置で作成するか等については、上記実施形態に説明した例に限られるものではなく、適宜変更して適用することができる。

【０１１４】

また、署名者を示す画像として電子文書とともに表示される画像は印影画像だけではなく、例えば、署名者のサインや顔写真等を表した画像であっても良い。

【０１１５】

また、署名対象となるデータは電子文書に限られるものではなく、例えば、画像データや音声データ等であっても良い。

【図面の簡単な説明】

【０１１６】

【図１】本実施形態に係る複合署名付電子文書１００の構造の一例を示す図である。

【図２】本実施形態に係る署名付電子文書作成装置１の概要構成の一例を示す図である。

【図３】複合署名付電子文書の表示画面の一例を示す図である。

【図４】本実施形態に係る署名付電子文書作成装置１のシステム制御部１６の複合電子署名を実施する場合における処理例を示す図である。

【図５】（ａ）は、電子署名情報表示画面の一例を示す図であり、（ｂ）は、タイムスタンプ情報表示画面の一例を示す図である。

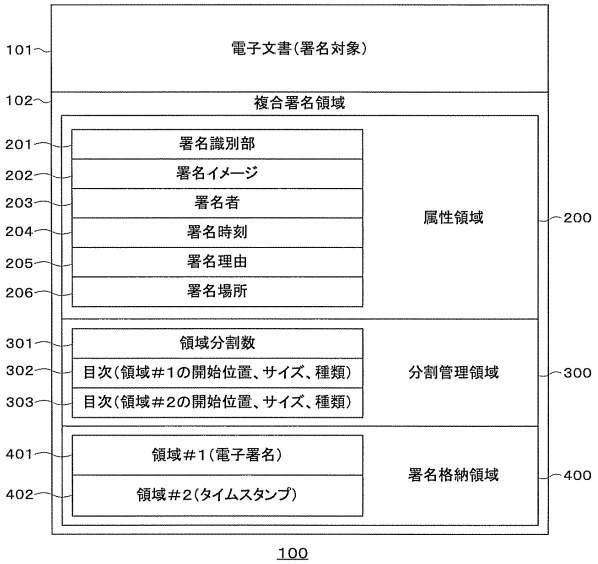
【図６】本実施形態に係る署名付電子文書作成装置１のシステム制御部１６の複合電子署名により複合署名付電子文書を検証する場合における処理例を示す図である。

【符号の説明】

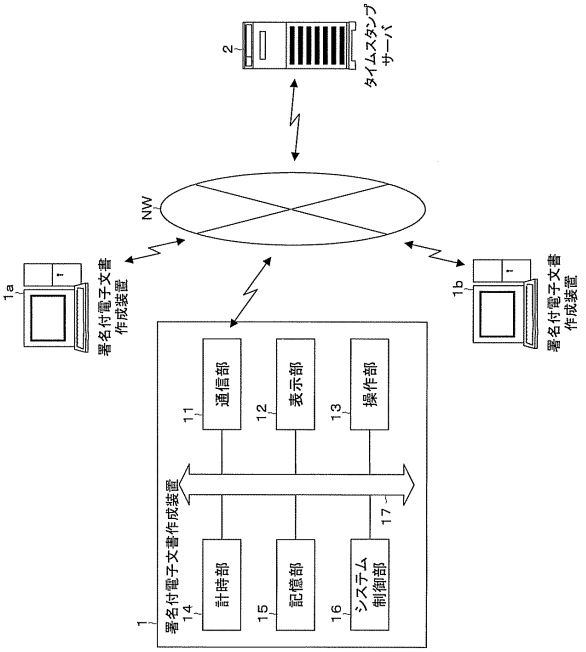
【０１１７】

１、１ａ、１ｂ　署名付電子文書作成装置
２　タイムスタンプサーバ
１１　通信部
１２　表示部
１３　操作部
１４　計時部
１５　記憶部
１６　システム制御部
１７　システムバス
ＮＷ　ネットワーク

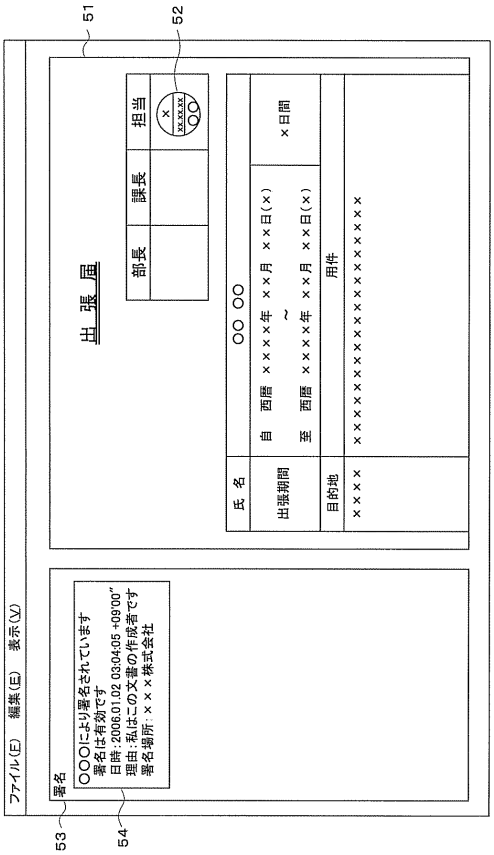
【図１】


101
電子文書(署名対象)
102
複合署名領域
201
署名識別部
202
署名イメージ
203
署名者
204
署名時刻
205
署名理由
206
署名場所
属性領域
200
301
領域分割数
302
目次(領域＃1の開始位置、サイズ、種類)
303
目次(領域＃2の開始位置、サイズ、種類)
分割管理領域
300
401
領域＃1(電子署名)
402
領域＃2(タイムスタンプ)
署名格納領域
400
100

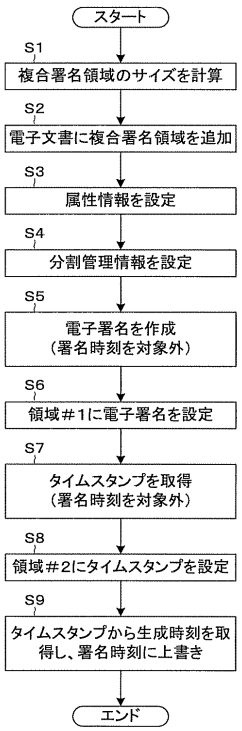
【図２】


2
タイムスタンプサーバ
NW
1a
署名付電子文書作成装置
1b
署名付電子文書作成装置
1
署名付電子文書作成装置
11
通信部
12
表示部
13
操作部
17
14
計時部
15
記憶部
16
システム制御部

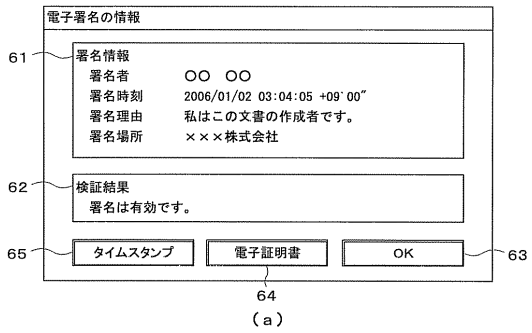
【図３】


51
52
ファイル(F) 編集(E) 表示(V)
出張届
部長
課長
担当
氏名
OO OO
出張期間
自 西暦 ××××年 ××月 ××日(×)
至 西暦 ××××年 ××月 ××日(×)
×日間
用件
××××××××××××××××
目的地
××××
署名
○○○により署名されています
署名は有効です
日時: 2006.01.02 03:04:05 +09'00'
理由: 私はこの文書の作成者です
署名場所: ×××株式会社
53
54

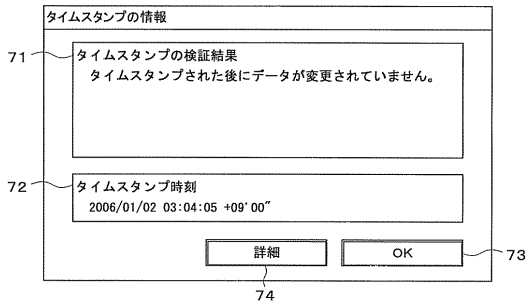
【図４】


スタート
S1
複合署名領域のサイズを計算
S2
電子文書に複合署名領域を追加
S3
属性情報を設定
S4
分割管理情報を設定
S5
電子署名を作成
(署名時刻を対象外)
S6
領域＃1に電子署名を設定
S7
タイムスタンプを取得
(署名時刻を対象外)
S8
領域＃2にタイムスタンプを設定
S9
タイムスタンプから生成時刻を取得し、署名時刻に上書き
エンド

【図５】

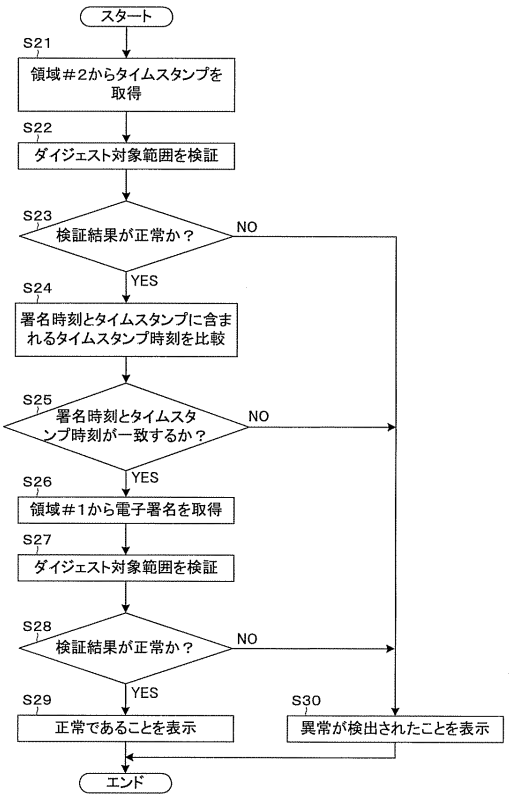

電子署名の情報
61
署名情報
署名者 ○○ ○○
署名時刻 2006/01/02 03:04:05 +09'00"
署名理由 私はこの文書の作成者です。
署名場所 ×××株式会社
62
検証結果
署名は有効です。
65
タイムスタンプ
電子証明書
OK
63
64

（ａ）


タイムスタンプの情報
71
タイムスタンプの検証結果
タイムスタンプされた後にデータが変更されていません。
72
タイムスタンプ時刻
2006/01/02 03:04:05 +09'00"
詳細
OK
73
74

（ｂ）

【図６】


スタート
S21
領域＃2からタイムスタンプを取得
S22
ダイジェスト対象範囲を検証
S23
検証結果が正常か？
NO
YES
S24
署名時刻とタイムスタンプに含まれるタイムスタンプ時刻を比較
S25
署名時刻とタイムスタンプ時刻が一致するか？
NO
YES
S26
領域＃1から電子署名を取得
S27
ダイジェスト対象範囲を検証
S28
検証結果が正常か？
NO
YES
S29
正常であることを表示
S30
異常が検出されたことを表示
エンド

フロントページの続き

(56)参考文献 特開２００５－３０３９５１（ＪＰ，Ａ）
特開２００３－２４４１３８（ＪＰ，Ａ）
特開２００５－２２９４５０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２