(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5252539号
(P5252539)
(45)発行日　平成25年7月31日(2013.7.31)　(24)登録日　平成25年4月26日(2013.4.26)

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

請求項の数 14 (全 26 頁)

(21)出願番号　特願2007-292097(P2007-292097)
(22)出願日　平成19年11月9日(2007.11.9)
(65)公開番号　特開2009-118402(P2009-118402A)
(43)公開日　平成21年5月28日(2009.5.28)
審査請求日　平成22年10月27日(2010.10.27)

(73)特許権者　301022471
独立行政法人情報通信研究機構
東京都小金井市貫井北町４－２－１
(74)代理人　100130111
弁理士　新保　斉
(72)発明者　梅野　健
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置、時刻認証システム、時刻認証方法、および時刻認証プログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークへの接続が可能であり、タイムスタンプを生成するための時刻情報をタイムスタンプ装置に配信する標準時刻配信装置であって、
公開鍵暗号方式に基づくタイムスタンプ利用者の秘密鍵で公開鍵暗号化された、タイムスタンプ利用者がタイムスタンプ押印を要求する際のタイムスタンプ押印要求時刻情報が含まれている発行時刻要求データを前記タイムスタンプ利用者の公開鍵を用いて復号する復号手段と、
常に正確な時刻を保持しており、前記タイムスタンプ装置からの時刻情報の要求を受け付けると、時刻情報を生成する標準時刻生成手段と、
前記標準時刻生成手段により生成された時刻情報とともに、前記タイムスタンプの利用者が押印を要求する際発行される押印要求時刻情報を、標準時刻配信事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化する暗号化手段と、
前記標準時刻生成手段で生成された時刻情報とともに、前記暗号化手段で暗号化された、前記時刻情報と前記タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報とを前記時刻認証局の公開鍵を用いて公開鍵暗号化してタイムスタンプ装置用の二重暗号化時刻データを生成する二重暗号化手段と、
前記二重暗号化時刻データを前記タイムスタンプ装置へ配信する通信手段と、
を備えていることを特徴とする標準時刻配信装置。
【請求項２】

標準時刻配信事業者の公開鍵証明書データを発行する公開鍵証明書データ発行手段を備えていることを特徴とする請求項１に記載の標準時刻配信装置。
【請求項３】
ネットワークへの接続が可能であり、標準時刻配信装置から送信された時刻情報に基づいてタイムスタンプを生成してタイムスタンプ利用者用装置へ提供するタイムスタンプ装置であって、
前記タイムスタンプ利用者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化されたハッシュ値をタイムスタンプ利用者の公開鍵を用いて復号すると共に、前記標準時刻配信装置から送信された前記タイムスタンプ装置用の二重暗号化時刻データを時刻認証局の秘密鍵で復号化する復号手段と、
前記タイムスタンプ利用者用装置から送信され、前記復号手段で復号されたハッシュ値を取得するハッシュ値取得手段と、
前記復号手段により復号化されたハッシュ値、前記標準時刻配信装置から送信された標準時刻情報、
前記復号手段により二重暗号化時刻データが復号化された暗号化時刻データ、前記二重暗号化時刻データに含まれる標準時刻配信事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化され、前記復号化手段により復号化されたタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を、前記時刻認証局の公開鍵暗号に基づく秘密鍵で公開鍵暗号化することによりタイムスタンプデータを生成するタイムスタンプ生成手段と、
前記タイムスタンプ利用者用装置へタイムスタンプ情報に送信するためのタイムスタンプ送信手段と、
を備えていることを特徴とするタイムスタンプ装置。
【請求項４】
時刻認証局の公開鍵証明書データを発行する公開鍵証明書データ発行手段を備えていることを特徴とする請求項３に記載のタイムスタンプ装置。
【請求項５】
ネットワークへの接続が可能であり、タイムスタンプ装置が生成したタイムスタンプの配信を受けるタイムスタンプ利用者用装置であって、
文書・電子データを作成する文書・電子データ作成手段と、
前記文書・電子データ作成手段で作成された文書・電子データからハッシュ値を生成するハッシュ値生成手段と、
タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を含む発行時刻要求データを生成する発行時刻要求データ生成手段と、
前記タイムスタンプ装置から送信された前記タイムスタンプデータを時刻認証局の公開鍵を用いて復号して、標準時刻配信事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化された時刻情報およびタイムスタンプ利用者が押印を要求する際のタイムスタンプの押印要求時刻情報と、ハッシュ値を得る復号手段と、
前記タイムスタンプが示す時刻情報と前記タイムスタンプ利用者が押印を要求するタイムスタンプの押印要求時刻情報とを比較し、前記タイムスタンプが示す時刻が改ざんまたは遅延されているか否かを判定する判定手段と
を備えたことを特徴とするタイムスタンプ利用者用装置。
【請求項６】
タイムスタンプ利用者の公開鍵証明書データを発行する公開鍵証明書データ発行手段を備えていることを特徴とする請求項５に記載のタイムスタンプ利用者用装置。
【請求項７】
ネットワークへの接続が可能であり、タイムスタンプ装置が生成したタイムスタンプの配信を受けるタイムスタンプ利用者用装置であって、
ハッシュ値を公開鍵暗号方式におけるタイムスタンプ利用者の秘密鍵で公開鍵暗号化する暗号化手段と、
当該ハッシュ値を時刻認証局のサーバーに送信する送信手段と、

タイムスタンプ利用者が押印を要求するタイムスタンプの押印要求時刻情報を含む発行時刻要求データを生成する発行時刻要求データ生成手段と、
前記発行時刻要求データを公開鍵暗号方式における標準時刻配信事業者の公開鍵で暗号化する暗号化手段と、
当該暗号化された発行時刻要求データを標準時刻配信事業者のサーバーに送信する送信手段と、
前記タイムスタンプ装置から送信された前記タイムスタンプデータを時刻認証局の公開鍵を用いて復号して、標準時刻配信事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化された時刻情報およびタイムスタンプ利用者が押印を要求する際のタイムスタンプの押印要求時刻情報とハッシュ値を得る復号手段と、
前記タイムスタンプが示す時刻情報と前記タイムスタンプ利用者が押印を要求するタイムスタンプの押印要求時刻情報とを比較し、前記タイムスタンプが示す時刻が改ざんまたは遅延されているか否かを判定する判定手段と
を備えたことを特徴とするタイムスタンプ利用者用装置。
【請求項８】
文書・電子データからハッシュ値を生成するハッシュ値生成手段と、
前記ハッシュ値生成手段が生成したハッシュ値を格納する格納手段を備え、
前記判定手段は、前記復号手段で復号されたハッシュ値と、前記格納手段に格納されているハッシュ値とを比較し、同値であるか否かを判定することを特徴とする請求項７に記載のタイムスタンプ利用者用装置。
【請求項９】
タイムスタンプ利用者用装置以外の格納手段に格納したハッシュ値を取得するハッシュ値取得手段を備え、
前記判定手段は、前記復号手段で復号されたハッシュ値と、取得したハッシュ値とを比較し、同値であるか否かを判定することを特徴とする請求項７に記載のタイムスタンプ利用者用装置。
【請求項１０】
請求項１又は２に記載の標準時刻配信装置と、請求項３又は４に記載のタイムスタンプ装置と、請求項５～９のいずれかに記載のタイムスタンプ利用者用装置と、を備えたことを特徴とする時刻認証システム。
【請求項１１】
タイムスタンプを発行するタイムスタンプ装置と、前記タイムスタンプを生成するための時刻を前記タイムスタンプ装置に配信する標準時刻配信装置と、前記タイムスタンプ装置から前記タイムスタンプの提供を受けるタイムスタンプ利用者用装置とを備えた時刻認証システムにおいて実行される時刻認証方法であって、
前記タイムスタンプ利用者用装置において、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報が含まれている発行時刻要求データを、タイムスタンプ利用者の公開鍵暗号方式における秘密鍵を用いて暗号化して標準時刻配信事業者の標準時刻配信装置へ送信する工程と、
前記タイムスタンプ利用者用装置において、ハッシュ値を生成し当該ハッシュ値をタイムスタンプ利用者の秘密鍵で公開鍵暗号化して前記タイムスタンプ装置へ送る工程と、
前記標準時刻配信装置において、前記秘密鍵を用いて暗号化された発行時刻要求データを前記タイムスタンプ利用者の公開鍵を用いて復号して取得した押印要求時刻情報と、前記標準時刻配信装置で生成した時刻情報とを標準時刻配信事業者の秘密鍵で公開鍵暗号化して生成したデータを、さらに時刻認証局の公開鍵で暗号化して生成したタイムスタンプ装置用の二重暗号化時刻データを前記タイムスタンプ装置へ送信する工程と、
前記タイムスタンプ装置において、前記公開鍵暗号化されたハッシュ値を前記タイムスタンプ利用者の公開鍵を用いて復号して前記ハッシュ値を取得し、当該ハッシュ値に対して前記標準時刻配信装置から送信された前記タイムスタンプ装置用の二重暗号化時刻データを、時刻認証局の公開鍵暗号に基づく秘密鍵で復号して取得した前記時刻情報に基づい

てタイムスタンプを生成し、前記タイムスタンプ利用者用装置へ送信する工程と、
前記タイムスタンプ利用者用装置において、前記タイムスタンプデータを前記時刻認証局の公開鍵で復号して前記タイムスタンプを取得し、標準時刻配信事業者の秘密鍵で公開鍵暗号化して生成したデータを標準時刻配信事業者の公開鍵で復号して生成された時刻情報および前記押印要求時刻情報を取得し、前記タイムスタンプと押印要求時刻情報とを比較する工程と、
を備えたことを特徴とする時刻認証方法。
【請求項１２】
前記タイムスタンプ利用者用装置において、ハッシュ値を生成し当該ハッシュ値を公開鍵暗号方式におけるタイムスタンプ利用者の秘密鍵で公開鍵暗号化して前記タイムスタンプ装置へ送る工程が、当該ハッシュ値を暗号化せずに前記タイムスタンプ装置へ送る工程とすることを特徴とする請求項１１に記載の時刻認証方法。
【請求項１３】
前記タイムスタンプ利用者用装置において、前記タイムスタンプデータを前記時刻認証局の公開鍵で復号して前記タイムスタンプデータに含まれる前記ハッシュ値を取得し、当該ハッシュ値とあらかじめ前記タイムスタンプ利用者用装置で生成したハッシュ値とを比較する工程を備えたことを特徴とする請求項１１又は１２に記載の時刻認証方法。
【請求項１４】
請求項１１～１３のいずれか一つに記載の時刻認証方法をコンピュータに実行させることを特徴とする時刻認証プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、時刻認証局における時刻の改ざんを防止する標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置、時刻認証システム、時刻認証方法、および時刻認証プログラムに関する。
【背景技術】
【０００２】
近年、情報通信技術の発達にともない、電子データによって種々の情報がやり取りされるようになってきている。このような状況下にあっては、電子データの真正性はもとより、電子データが「いつ」作成されたのか、電子データの作成時刻を証明することが重要である。
【０００３】
電子データの作成時刻を証明する方法としては、時刻認証局によるタイムスタンプを刻印する方法があるが、第三者により時刻の改ざんなどの問題がある。このため、時刻の改ざんを防止するために種々の提案がなされている（たとえば、特許文献１を参照。）。
【０００４】
【特許文献１】特開２００４－２３５８２６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１に記載の技術をはじめとして従来技術では、時刻認証局以外による時刻の改ざんを防止することは可能であるが、時刻認証局自体が時刻の改ざんを行おうとした場合、又は故意若しくは故障等によるタイムスタンプ時刻の遅延などに、有効な防止対策を講ずることができないという問題がある。
【０００６】
本発明は、上述した従来技術による問題点を解消するため、第三者による電子データ作成時刻の改ざんはもとより、時刻認証局における時刻の改ざんまたは遅延を防止する標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置、時刻認証システム、時刻認証方法、および時刻認証プログラムを提供することを目的とする。さらに、時刻認

証事業者が、特定の時刻認証局へのサービスを提供して、課金でき得るシステムを提供することも目的とする。

【課題を解決するための手段】

【０００７】

上述した課題を解決し、目的を達成するため、本発明にかかる標準時刻配信装置は、ネットワークへの接続が可能であり、タイムスタンプを生成するための時刻情報をタイムスタンプ装置に配信する標準時刻配信装置であって、常に正確な時刻を保持しており、タイムスタンプ装置からの時刻情報の要求を受け付けると、時刻情報を生成する標準時刻生成手段と、標準時刻生成手段により生成された時刻情報を公開鍵暗号方式に基づく標準時刻配信事業者の秘密鍵で公開鍵暗号化する暗号化手段と、標準時刻生成手段で生成された時刻情報とともに、暗号化手段で暗号化された時刻情報をタイムスタンプ装置へ配信する通信手段とを備えていることを特徴とする。ここで、時刻認証局とは、時刻認証事業を行っている団体、民間企業、公的機関や政府から時刻認証局として認証・承認を受けた団体・民間企業、公的機関が挙げられる。また、ここで、標準時刻配信事業者とは、日本標準時を配信している、独立行政法人情報通信研究機構などの公的機関が挙げられるが、日本標準時を配信しているその他の公的機関、準公的機関、公的機関から認証・承認を受けた団体が挙げられる。また、外国においても、同様に当該国・政府の公的機関などが挙げられる。

【０００８】

また、本発明にかかる標準時刻配信装置は、上記の標準時刻配信装置において、標準時刻生成手段で生成された時刻情報とともに、暗号化手段で暗号化された時刻情報を時刻認証局の公開鍵で暗号化してタイムスタンプ装置用暗号化時刻データを生成する二重暗号化手段を備え、通信手段は、タイムスタンプ装置用の暗号化時刻データをタイムスタンプ装置へ配信することを特徴とする。

【０００９】

また、本発明にかかる標準時刻配信装置は、上記発明において、公開鍵暗号方式に基づくタイムスタンプ利用者の秘密鍵で公開鍵暗号化された、タイムスタンプ利用者がタイムスタンプ押印を要求する際のタイムスタンプ押印要求時刻情報が含まれている発行時刻要求データをタイムスタンプ利用者の公開鍵を用いて復号する復号手段を備え、暗号化手段は、標準時刻生成手段により生成された時刻情報とともに、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を標準時刻配信事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化し、二重暗号化手段は、標準時刻生成手段で生成された時刻情報とともに、暗号化手段で暗号化された、時刻情報とタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報とを時刻認証局の公開鍵を用いて公開鍵暗号化してタイムスタンプ装置用の二重暗号化時刻データを生成し、通信手段は、二重暗号化時刻データをタイムスタンプ装置へ配信することを特徴とする。

【００１０】

また、請求項２の発明にかかる標準時刻配信装置は、請求項１に記載の発明において、標準時刻配信事業者の公開鍵証明書データを発行する公開鍵証明書データ発行手段を備えていることを特徴とする。

【００１１】

本発明において、タイムスタンプの押印要求時刻情報とは、タイムスタンプ利用者が押印を要求するタイミングを示すものである。また、本発明は、公開鍵暗号化されたタイムスタンプ押印要求時刻情報が含まれている発行時刻要求データについて、標準時刻配信装置において復号化するものであるが、別の態様として、標準時刻配信装置やタイムスタンプ装置で復号化することなく、タイムスタンプ利用者の要求情報自体を秘匿させてもよい。その他に、標準時刻配信装置では復号化でき、タイムスタンプ装置では復号化できないようにするために、この要求情報を標準時刻配信装置の公開鍵で暗号化することが挙げられる。

【００１２】

また、請求項３の発明にかかるタイムスタンプ装置は、ネットワークへの接続が可能であり、標準時刻配信装置から送信された時刻情報に基づいてタイムスタンプを生成してタイムスタンプ利用者用装置へ提供するタイムスタンプ装置であって、タイムスタンプ利用者用装置から送信されたハッシュ値を取得するハッシュ値取得手段と、ハッシュ値取得手段が取得したハッシュ値、標準時刻配信装置から送信された標準時刻情報、標準時刻配信装置から送信された標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を、時刻認証局の秘密鍵で公開鍵暗号化することによりタイムスタンプ情報を生成するタイムスタンプ生成手段と、タイムスタンプ利用者用装置へタイムスタンプ情報に送信するためのタイムスタンプ送信手段とを備えていることを特徴とする。

【００１３】

また、本発明にかかるタイムスタンプ装置は、上記のタイムスタンプ装置において、標準時刻配信装置から送信されたタイムスタンプ装置用の暗号化時刻データを時刻認証局の秘密鍵で復号する復号手段を備え、ハッシュ値取得手段が取得したハッシュ値、標準時刻配信装置から送信された標準時刻情報、復号手段により復号された暗号化時刻データを、時刻認証局の秘密鍵で公開鍵暗号化することによりタイムスタンプ情報を生成するタイムスタンプ生成手段と、タイムスタンプ利用者用装置へタイムスタンプ情報に送信するためのタイムスタンプ送信手段とを備えていることを特徴とする。

【００１４】

また、本発明にかかるタイムスタンプ装置は、上記のタイムスタンプ装置において、タイムスタンプ利用者の秘密鍵で公開鍵暗号化されたハッシュ値をタイムスタンプ利用者の公開鍵を用いて復号する復号手段を備え、ハッシュ値取得手段は、復号手段で復号されたハッシュ値を取得し、復号手段は、標準時刻配信装置から送信されたタイムスタンプ装置用の二重暗号化時刻データを時刻認証局の秘密鍵で復号し、復号手段により復号化されたハッシュ値、標準時刻配信装置から送信された標準時刻情報、二重暗号化時刻データが復号化された暗号化時刻データ、二重暗号化時刻データに含まれる標準時刻配信事業者の秘密鍵で公開鍵暗号化され、復号化手段により復号化されたタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を、時刻認証局の秘密鍵で公開鍵暗号化することによりタイムスタンプデータを生成するタイムスタンプ生成手段とを備えていることを特徴とする。

【００１５】

また、請求項４の発明にかかるタイムスタンプ装置は、請求項３に記載の発明において、時刻認証局の公開鍵証明書データを発行する公開鍵証明書データ発行手段を備えていることを特徴とする。

【００１６】

また、請求項５の発明にかかるタイムスタンプ利用者用装置は、ネットワークへの接続が可能であり、タイムスタンプ装置が生成したタイムスタンプの配信を受けるタイムスタンプ利用者用装置であって、文書・電子データを作成する文書・電子データ作成手段と、

文書・電子データ作成手段で作成された文書・電子データからハッシュ値を生成するハッシュ値生成手段と、標準時刻配信事業者の公開鍵を用いて、タイムスタンプ装置から送信されたタイムスタンプ利用者用の暗号化時刻データに含まれる標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を復号する復号手段とを備えていることを特徴とする。

【００１７】

また、本発明にかかるタイムスタンプ利用者用装置は、上記のタイムスタンプ利用者用装置において、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を含む発行時刻要求データを生成する発行時刻要求データ生成手段と、タイムスタンプ装置から送信されたタイムスタンプデータを時刻認証局の公開鍵を用いて復号して、標準時刻配信事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化された時刻情報およびタイムスタンプ利用者が押印を要求する際のタイムスタンプの押印要求時刻情報と、ハッシュ値を得る復号手段とを備え、復号手段は、標準時刻配信事業者の公開鍵を用いて、標準時刻配信

事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化された時刻情報およびタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を復号し、判定手段は、タイムスタンプが示す時刻情報とタイムスタンプ利用者が押印を要求するタイムスタンプの押印要求時刻情報とを比較し、タイムスタンプが示す時刻が改ざんまたは遅延されているか否かを判定することを特徴とする。

【００１８】

また、請求項５の発明にかかるタイムスタンプ利用者用装置は、請求項９に記載の発明において、タイムスタンプ利用者の公開鍵証明書データを発行する公開鍵証明書データ発行手段を備えていることを特徴とする。

【００１９】

また、請求項７の発明にかかるタイムスタンプ利用者用装置は、ネットワークへの接続が可能であり、タイムスタンプ装置が生成したタイムスタンプの配信を受けるタイムスタンプ利用者用装置であってハッシュ値を公開鍵暗号方式におけるタイムスタンプ利用者の秘密鍵で公開鍵暗号化する暗号化手段と、当該ハッシュ値を時刻認証局のサーバーに送信する送信手段と、タイムスタンプ利用者が押印を要求するタイムスタンプの押印要求時刻情報を含む発行時刻要求データを生成する発行時刻要求データ生成手段と、発行時刻要求データを公開鍵暗号方式における標準時刻配信事業者の公開鍵で暗号化する暗号化手段と、当該暗号化された発行時刻要求データを標準時刻配信事業者のサーバーに送信する送信手段と、タイムスタンプ装置から送信されたタイムスタンプデータを時刻認証局の公開鍵を用いて復号して、標準時刻配信事業者の公開鍵暗号に基づく秘密鍵で公開鍵暗号化された時刻情報およびタイムスタンプ利用者が押印を要求する際のタイムスタンプの押印要求時刻情報とハッシュ値を得る復号手段と、タイムスタンプが示す時刻情報とタイムスタンプ利用者が押印を要求するタイムスタンプの押印要求時刻情報とを比較し、タイムスタンプが示す時刻が改ざんまたは遅延されているか否かを判定する判定手段とを備えたことを特徴とする。

【００２０】

また、請求項８の発明にかかるタイムスタンプ利用者用装置は、文書・電子データからハッシュ値を生成するハッシュ値生成手段と、ハッシュ値生成手段が生成したハッシュ値を格納する格納手段を備え、判定手段は、復号手段で復号されたハッシュ値と、格納手段に格納されているハッシュ値とを比較し、同値であるか否かを判定することを特徴とする。

【００２１】

また、請求項９の発明にかかる時刻認証システムは、タイムスタンプ利用者用装置以外に格納したハッシュ値を取得するハッシュ値取得手段を備え、判定手段は、復号手段で復号されたハッシュ値と、格納手段に格納されているハッシュ値とを比較し、同値であるか否かを判定することを特徴とする。

【００２２】

また、請求項１０の発明にかかる時刻認証システムは、請求項1又は２に記載の標準時刻配信装置と、請求項3又は４に記載のタイムスタンプ装置と、請求項５～９のいずれかに記載のタイムスタンプ利用者用装置とを備えたことを特徴とする。

【００２３】

また、請求項１１の発明にかかる時刻認証方法は、タイムスタンプを発行するタイムスタンプ装置と、タイムスタンプを生成するための時刻をタイムスタンプ装置に配信する標準時刻配信装置と、タイムスタンプ装置からタイムスタンプの提供を受けるタイムスタンプ利用者用装置とを備えた時刻認証システムにおいて実行される時刻認証方法であって、タイムスタンプ利用者用装置において、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報が含まれている発行時刻要求データを、タイムスタンプ利用者の公開鍵暗号方式における秘密鍵を用いて暗号化して標準時刻配信事業者の標準時刻配信装置へ送信する工程と、タイムスタンプ利用者用装置において、ハッシュ値を生成し当該ハッシュ値をタイムスタンプ利用者の秘密鍵で公開鍵暗号化してタイムスタンプ装置へ送る工

程と、標準時刻配信装置において、秘密鍵を用いて暗号化された発行時刻要求データをタイムスタンプ利用者の公開鍵を用いて復号して取得した押印要求時刻情報と、標準時刻配信装置で生成した時刻情報とを標準時刻配信事業者の秘密鍵で公開鍵暗号化して生成したデータを、さらに時刻認証局の公開鍵で暗号化して生成したタイムスタンプ装置用の二重暗号化時刻データをタイムスタンプ装置へ送信する工程と、タイムスタンプ装置において、公開鍵暗号化されたハッシュ値をタイムスタンプ利用者の公開鍵を用いて復号してハッシュ値を取得し、当該ハッシュ値に対して標準時刻配信装置から送信されたタイムスタンプ装置用の二重暗号化時刻データを、時刻認証局の公開鍵暗号に基づく秘密鍵で復号して取得した時刻情報に基づいてタイムスタンプを生成し、タイムスタンプ利用者用装置へ送信する工程と、タイムスタンプ利用者用装置において、タイムスタンプデータを時刻認証局の公開鍵で復号してタイムスタンプを取得し、標準時刻配信事業者の秘密鍵で公開鍵暗号化して生成したデータを標準時刻配信事業者の公開鍵で復号して生成された時刻情報および押印要求時刻情報を取得し、タイムスタンプと押印要求時刻情報とを比較する工程と、を備えたことを特徴とする。

【００２４】

また、請求項１２の発明にかかる方法は、上記のタイムスタンプ利用者用装置において、ハッシュ値を生成し当該ハッシュ値を公開鍵暗号方式におけるタイムスタンプ利用者の秘密鍵で公開鍵暗号化してタイムスタンプ装置へ送る工程が、当該ハッシュ値を暗号化せずにタイムスタンプ装置へ送る工程とすることを特徴とする。

【００２５】

また、請求項１３にかかる時刻認証方法は、タイムスタンプ利用者用装置において、タイムスタンプデータを時刻認証局の公開鍵で復号してタイムスタンプデータに含まれるハッシュ値を取得し、当該ハッシュ値とあらかじめタイムスタンプ利用者用装置で生成したハッシュ値とを比較する工程を備えたことを特徴とする。

【００２６】

また、請求項１４の発明にかかる時刻認証プログラムは、請求項１１～１３のいずれか一つに記載の時刻認証方法をコンピュータに実行させることを特徴とする。

【００２７】

なお、本発明の変形として、タイムスタンプ利用者用装置において、ハッシュ値を時刻認証局への送信は、暗号化せずに特定の者が送信したことが分かる方法で送信してもよい。また、タイムスタンプ利用者用装置において、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を標準時刻配信事業者の公開鍵で暗号化することなく、特定の者が送信したことが分かる方法で送信してもよい。

【発明の効果】

【００２８】

本発明によれば、第三者による電子データ作成時刻の改ざんはもとより、時刻認証局による電子データ作成時刻の改ざんまたは遅延を防止することができるという効果を奏する。また、標準時刻配信事業者が特定の時刻認証局のみに、標準時刻を配信することができ、同事業者の管理や課金などの制御を可能とする。

【発明を実施するための最良の形態】

【００２９】

以下、添付図面を参照して、本発明にかかる標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置、時刻認証システム、時刻認証方法、および時刻認証プログラムの好適な実施の形態を詳細に説明する。

【００３０】

（実施の形態１）

まず、本発明の実施の形態１にかかる時刻認証システム、標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置について説明する。

【００３１】

（時刻認証システムの全体構成）

図１は、本発明の実施の形態１にかかる時刻認証システムの全体構成を示す図である。実施の形態１にかかる時刻認証システムは、標準時刻配信装置１１０と、タイムスタンプ装置１２０と、複数のタイムスタンプ利用者用装置１３０と、がそれぞれネットワークを介して相互通信可能に接続されている。標準時刻配信装置１１０は、正確な時刻を保持しており、タイムスタンプ装置１２０に対して時刻の配信を行う。この標準時刻配信装置１１０は、標準時刻配信事業者が所持している。また、タイムスタンプ装置１２０は、タイムスタンプ利用者用装置１３０に対して時刻証明のためのタイムスタンプサービスを提供する。このタイムスタンプ装置１２０は、時刻認証局が所持している。

【００３２】

（標準時刻配信装置の機能的構成）

図２は、実施の形態１にかかる標準時刻配信装置の機能的構成を示すブロック図である。この標準時刻配信装置１１０は、通信制御部２０１と、時刻情報要求受付部２０２と、標準時刻生成部２０３と、第１暗号化部２０４と、公開鍵証明書データ発行部２０５と、を備えている。なお、図示していないが、本装置に付随して原子時計等の標準時刻を示す時計がある。

【００３３】

通信制御部２０１は、ネットワークとの通信を制御する。時刻情報要求受付部２０２は、通信制御部２０１を介して、タイムスタンプ装置１２０からの時刻情報配信要求を受け付ける。標準時刻生成部２０３は、常に正確な時刻を保持しており、時刻情報要求受付部２０２が時刻情報配信要求を受け付けると、通信制御部２０１を介して時刻情報をタイムスタンプ装置１２０へ配信するとともに、同様の時刻情報を第１暗号化部２０４へも配信する。第１暗号化部２０４は、標準時刻生成部２０３から配信された時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化する。ここで暗号化された時刻情報は、通信制御部２０１を介してタイムスタンプ装置１２０へ配信される。公開鍵証明書データ発行部２０５は、タイムスタンプ利用者用装置１３０からの要求に基づき標準時刻配信事業者の公開鍵証明書データを発行する。ここで、タイムスタンプ装置１２０へ配信される時刻情報は、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報とともに、暗号化されていない時刻情報を含むものとする。

【００３４】

（タイムスタンプ装置の機能的構成）

図３は、実施の形態１にかかるタイムスタンプ装置の機能的構成を示すブロック図である。このタイムスタンプ装置１２０は、通信制御部３０１と、ハッシュ値取得部３０２と、時刻情報配信要求発行部３０３と、時刻情報受信部３０４と、タイムスタンプ生成部３０５と、タイムスタンプ利用者用の暗号化時刻データ生成部３０６と、を備えている。

【００３５】

通信制御部３０１は、ネットワークとの通信を制御する。ハッシュ値取得部３０２は、通信制御部３０１を介してタイムスタンプ利用者用装置１３０から送信されたハッシュ値を取得する（詳細は後述する）。時刻情報配信要求発行部３０３は、ハッシュ値取得部３０２がタイムスタンプ利用者用装置１３０から送信されたハッシュ値を取得すると、通信制御部３０１を介して、標準時刻配信装置１１０へ時刻情報の配信要求を発行する。時刻情報受信部３０４は、通信制御部３０１を介して標準時刻配信装置１１０から送信された時刻情報を受信する。タイムスタンプ生成部３０５は、ハッシュ値取得部３０２が取得したハッシュ値に対して、時刻情報受信部３０４が受信した時刻情報からタイムスタンプを生成する。タイムスタンプ利用者用の暗号化時刻データ生成部３０６は、標準時刻配信装置１１０から送信された標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報にタイムスタンプ生成部３０５で生成されたタイムスタンプを付加し、タイムスタンプ利用者用装置１３０へ送信するためのタイムスタンプ利用者用の暗号化時刻データを生成する。ここで、タイムスタンプを生成するとは、標準時刻配信装置１１０から送信された時刻情報（当該処理では非暗号化時刻情報）について、利用者が視覚的に把握され易い特定の形式にすることをいう。また、送信するためのタイムスタンプ利用者用の暗号化時刻データ

を生成するとは、送信可能となるデータ形式とすることをいう。
【００３６】
（タイムスタンプ利用者用装置の機能的構成）
図４は、実施の形態１にかかるタイムスタンプ利用者用装置の機能的構成を示すブロック図である。このタイムスタンプ利用者用装置１３０は、通信制御部４０１と、文書・電子データ作成部４０２と、ハッシュ値生成部４０３と、格納部４０４と、タイムスタンプ利用者用データ受信部４０５と、第１復号部４０６と、判定部４０７と、を備えている。
【００３７】
通信制御部４０１は、ネットワークとの通信を制御する。文書・電子データ作成部４０２は、ユーザの操作により文書・電子データを作成する。ハッシュ値生成部４０３は、文書・電子データ作成部４０２で作成された文書・電子データからハッシュ値を生成する。ここで生成されたハッシュ値は、文書・電子データ作成部４０２で作成された文書・電子データとともに格納部４０４に格納される。また、通信制御部４０１を介して、タイムスタンプ装置１２０へ送信される。タイムスタンプ利用者用データ受信部４０５は、通信制御部４０１を介してタイムスタンプ装置１２０から送信されたタイムスタンプ利用者用の暗号化時刻データを受信する。第１復号部４０６は、タイムスタンプ利用者用データ受信部４０５がタイムスタンプ利用者用の暗号化時刻データを受信すると、標準時刻配信装置１１０にアクセスして標準時刻配信事業者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した標準時刻配信事業者の公開鍵を用いて前記タイムスタンプ利用者用の暗号化時刻データに含まれる標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を復号する。判定部４０７は、前記タイムスタンプ利用者用の暗号化時刻データに含まれているタイムスタンプが示す時刻情報と第１復号部４０６で復号された時刻情報とを比較し、タイムスタンプが示す時刻が改ざんされているか否かを判定する。前記タイムスタンプが示す時刻が第１復号部４０６で復号された時刻情報と同じであれば、時刻認証局における時刻の改ざんがないと判断できる。
【００３８】
（時刻認証システムの処理）
次に、実施の形態１にかかる時刻認証システムの処理の内容について説明する。図５は、実施の形態１にかかる時刻認証システムの処理手順を示すフローチャートである。
【００３９】
図５のフローチャートにおいて、まず、文書・電子データを生成する（ステップＳ５０１）。この処理は、ユーザの操作によりタイムスタンプ利用者用装置１３０の文書・電子データ作成部４０２が実行する。
【００４０】
次に、ハッシュ値を生成する（ステップＳ５０２）。この処理は、ハッシュ値生成部４０３が、ステップＳ５０１で作成された文書・電子データからハッシュ値を生成する。このハッシュ値は、前記文書・電子データとともに格納部４０４に格納される。また、タイムスタンプ装置１２０へ送信される。
【００４１】
次に、ハッシュ値を取得する（ステップＳ５０３）。具体的には、タイムスタンプ装置１２０のハッシュ値取得部３０２が、タイムスタンプ利用者用装置１３０から送信されたハッシュ値を取得する。
【００４２】
次に、時刻情報の配信要求を発行する（ステップＳ５０４）。具体的には、タイムスタンプ装置１２０の時刻情報配信要求発行部３０３が、標準時刻配信装置１１０へ時刻情報の配信要求を発行する。
【００４３】
次に、時刻情報を配信する（ステップＳ５０５）。標準時刻配信装置１１０の標準時刻生成部２０３は、常に正確な時刻を保持しており、時刻情報要求受付部２０２が時刻情報配信要求を受け付けると、時刻情報をタイムスタンプ装置１２０へ配信する。

【００４４】
続いて、時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化し、配信する（ステップＳ５０６）。具体的には、標準時刻配信装置１１０の第１暗号化部２０４が、標準時刻生成部２０３から配信された時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化し、これをタイムスタンプ装置１２０へ配信する。
【００４５】
次に、タイムスタンプを生成する（ステップＳ５０７）。ここでは、タイムスタンプ装置１２０のタイムスタンプ生成部３０５が、ハッシュ値取得部３０２が取得したハッシュ値に対して、時刻情報受信部３０４が受信した時刻情報からタイムスタンプを生成する。
【００４６】
続いて、タイムスタンプ利用者用の暗号化時刻データを生成する（ステップＳ５０８）。ここでは、タイムスタンプ装置１２０のタイムスタンプ利用者用の暗号化時刻データ生成部３０６が、標準時刻配信装置１１０から送信された標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報にステップＳ５０７で生成されたタイムスタンプを付加し、タイムスタンプ利用者用装置１３０へ送信するためのタイムスタンプ利用者用の暗号化時刻データを生成する。
【００４７】
次に、タイムスタンプ利用者用の暗号化時刻データを受信する（ステップＳ５０９）。ここでは、タイムスタンプ利用者用装置１３０のタイムスタンプ利用者用データ受信部４０５が、ステップＳ５０８で生成されたタイムスタンプ利用者用の暗号化時刻データを受信する。
【００４８】
続いて、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を復号する（ステップＳ５１０）。具体的には、タイムスタンプ利用者用装置１３０の第１復号部４０６が、標準時刻配信装置１１０にアクセスして標準時刻配信事業者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した標準時刻配信事業者の公開鍵を用いて前記タイムスタンプ利用者用の暗号化時刻データに含まれる標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を復号する。
【００４９】
そして、タイムスタンプの真偽を判定する（ステップＳ５１１）。ここでは、タイムスタンプ利用者用装置１３０の判定部４０７が、ステップＳ５０９で取得したタイムスタンプ利用者用の暗号化時刻データに含まれているタイムスタンプが示す時刻情報とステップＳ５１０で復号された時刻情報とを比較し、タイムスタンプの示す時刻が改ざんされているか否かを判定する。この処理により、タイムスタンプの示す時刻が、標準時刻配信装置１１０が発行した正確な時刻どおりであるか否かが判明する。
【００５０】
以上のような処理を実行することで、実施の形態１にかかる時刻認証システムでは、時刻認証局のタイムスタンプ装置１２０が受付時刻を改ざんしているか否かを判別することができる。すなわち、実施の形態１にかかる時刻認証システムでは、標準時刻配信装置１１０が、タイムスタンプ装置１２０においてタイムスタンプを生成するための時刻情報とともに、標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１３０でのみ復号できる時刻情報を供給している。したがって、タイムスタンプ装置１２０の不具合もしくは時刻認証局の故意によりタイムスタンプが示す時刻が改ざんされた場合であっても、タイムスタンプ利用者用装置１３０側で、タイムスタンプが示す時刻と標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１３０でのみ復号できる時刻情報とを比較することにより、時刻認証局における時刻改ざんの有無が判別できる。前記タイムスタンプが示す時刻が標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１３０でのみ復号できる時刻情報と同じであれば、時刻認証局における時刻改ざんはないと判断できる。
【００５１】

（実施の形態２）
次に、本発明の実施の形態２にかかる時刻認証システム、標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置について説明する。
【００５２】
（時刻認証システムの全体構成）
実施の形態２にかかる時刻認証システムは、標準時刻配信装置１４０と、タイムスタンプ装置１５０と、複数のタイムスタンプ利用者用装置１３０と、がそれぞれネットワークを介して相互通信可能に接続されている。この構成は、図１に示した実施の形態１のものと同様であるため、図は省略する。
【００５３】
（標準時刻配信装置の機能的構成）
図６は、実施の形態２にかかる標準時刻配信装置の機能的構成を示すブロック図である。この標準時刻配信装置１４０は、通信制御部２０１と、時刻情報要求受付部２０２と、標準時刻生成部２０３と、第１暗号化部２０４と、公開鍵証明書データ発行部２０５と、第２暗号化部２０６（二重暗号化手段）と、を備えている。
【００５４】
通信制御部２０１は、ネットワークとの通信を制御する。時刻情報要求受付部２０２は、通信制御部２０１を介して、タイムスタンプ装置１５０からの時刻情報配信要求を受け付ける。標準時刻生成部２０３は、常に正確な時刻を保持しており、時刻情報要求受付部２０２が時刻情報配信要求を受け付けると、時刻情報を第１暗号化部２０４および第２暗号化部２０６へ配信する。第１暗号化部２０４は、標準時刻生成部２０３から配信された時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化する。ここで暗号化された時刻情報は、第２暗号化部２０６へ配信される。公開鍵証明書データ発行部２０５は、タイムスタンプ利用者用装置１３０からの要求に基づき標準時刻配信事業者の公開鍵証明書データを発行する。第２暗号化部２０６は、第１暗号化部２０４で暗号化された時刻情報および標準時刻生成部２０３から配信された時刻情報を受け付けると、タイムスタンプ装置１５０にアクセスして時刻認証局の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した時刻認証局の公開鍵を用いて第１暗号化部２０４で暗号化された時刻情報および標準時刻生成部２０３から配信された時刻情報を暗号化する（以後、タイムスタンプ装置用暗号化時刻データという）。このタイムスタンプ装置用暗号化時刻データは、通信制御部２０１を介してタイムスタンプ装置１５０へ配信される。この変形例として、タイムスタンプ装置１５０にアクセスして時刻認証局の公開鍵証明書データの発行を受ける工程を省略して、標準時刻配信装置１４０に、特定の時刻認証局の公開鍵を予め保有させていてもよい。また、標準時刻生成部２０３から生成された時刻情報のコピーは、標準時刻配信事業者の秘密鍵で公開鍵暗号化しないものを含んでもよい。
【００５５】
（タイムスタンプ装置の機能的構成）
図７は、実施の形態２にかかるタイムスタンプ装置の機能的構成を示すブロック図である。このタイムスタンプ装置１５０は、通信制御部３０１と、ハッシュ値取得部３０２と、時刻情報配信要求発行部３０３と、時刻情報受信部３０４と、タイムスタンプ生成部３０５と、タイムスタンプ利用者用の暗号化時刻データ生成部３０６と、第１復号部３０７と、公開鍵証明書データ発行部３０８と、を備えている。
【００５６】
通信制御部３０１は、ネットワークとの通信を制御する。ハッシュ値取得部３０２は、通信制御部３０１を介してタイムスタンプ利用者用装置１３０から送信されたハッシュ値を取得する（詳細は後述する）。時刻情報配信要求発行部３０３は、ハッシュ値取得部３０２がタイムスタンプ利用者用装置１３０から送信されたハッシュ値を取得すると、通信制御部３０１を介して、標準時刻配信装置１４０へ時刻情報の配信要求を発行する。時刻情報受信部３０４は、通信制御部３０１を介して標準時刻配信装置１４０から送信されたタイムスタンプ装置用暗号化時刻データを受信する。第１復号部３０７は、前記タイムス

タンプ装置用の暗号化時刻データを時刻認証局の秘密鍵で復号する。ここで復号されたデータは、時刻情報と標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を含んでいる。第１復号部３０７において前記タイムスタンプ装置用の暗号化時刻データが時刻認証局の秘密鍵で復号できることにより、前記タイムスタンプ装置用の暗号化時刻データが確かに標準時刻配信装置１４０から特定の時刻認証局へ送信されたものであることが判明する。タイムスタンプ生成部３０５は、ハッシュ値取得部３０２が取得したハッシュ値に対して、第１復号部３０７で復号された時刻情報からタイムスタンプを生成する。タイムスタンプ利用者用の暗号化時刻データ生成部３０６は、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報にタイムスタンプ生成部３０５で生成されたタイムスタンプを当該ハッシュ値に付加し、タイムスタンプ利用者用装置１３０へ送信するためのタイムスタンプ利用者用の暗号化時刻データを生成する。公開鍵証明書データ発行部３０８は、標準時刻配信装置１４０からの要求に基づき時刻認証局の公開鍵証明書データを発行する。

【００５７】

（タイムスタンプ利用者用装置の機能的構成）

この実施の形態２にかかるタイムスタンプ利用者用装置の機能的構成は、図４に示した実施の形態１のものと同様であるため、説明は省略する。

【００５８】

（時刻認証システムの処理）

次に、実施の形態２にかかる時刻認証システムの処理の内容について説明する。図８は、実施の形態２にかかる時刻認証システムの処理手順を示すフローチャートである。

【００５９】

図８のフローチャートにおいて、まず、文書・電子データを生成する（ステップＳ８０１）。この処理は、ユーザの操作によりタイムスタンプ利用者用装置１３０の文書・電子データ作成部４０２が実行する。

【００６０】

次に、ハッシュ値を生成する（ステップＳ８０２）。この処理は、ハッシュ値生成部４０３が、ステップＳ８０１で作成された文書・電子データからハッシュ値を生成する。このハッシュ値は、前記文書・電子データとともに格納部４０４に格納される。また、タイムスタンプ装置１５０へ送信される。

【００６１】

続いて、ハッシュ値を取得する（ステップＳ８０３）。具体的には、タイムスタンプ装置１５０のハッシュ値取得部３０２が、タイムスタンプ利用者用装置１３０から送信されたハッシュ値を取得する。

【００６２】

次に、時刻情報の配信要求を発行する（ステップＳ８０４）。具体的には、タイムスタンプ装置１５０の時刻情報配信要求発行部３０３が、標準時刻配信装置１４０へ時刻情報の配信要求を発行する。

【００６３】

次に、時刻情報を配信する（ステップＳ８０５）。標準時刻配信装置１４０の標準時刻生成部２０３は、常に正確な時刻を保持しており、時刻情報要求受付部２０２が時刻情報配信要求を受け付けると、時刻情報を第１暗号化部２０４および第２暗号化部２０６へ配信する。

【００６４】

続いて、第１の暗号化を行う（ステップＳ８０６）。ここでは、第１暗号化部２０４が、標準時刻生成部２０３から配信された時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化する。

【００６５】

続いて、第２の暗号化を行う（ステップＳ８０７）。具体的には、第２暗号化部２０６が、ステップＳ８０６において標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報をステップＳ８０５で配信された時刻情報とともに、時刻認証局の公開鍵を用いて暗号

化を行い、タイムスタンプ装置用暗号化時刻データを生成する。

【００６６】

タイムスタンプ装置用暗号化時刻データを配信する（ステップＳ８０８）。すなわち、ステップＳ８０７で生成されたタイムスタンプ装置用暗号化時刻データを、通信制御部２０１を介してタイムスタンプ装置１５０へ配信する。

【００６７】

次に、タイムスタンプ装置用暗号化時刻データを時刻認証局の秘密鍵で復号する（ステップＳ８０９）。ここでは、第１復号部３０７が、前記タイムスタンプ装置用の暗号化時刻データを時刻認証局の秘密鍵で復号する。ここで復号されたデータは、非暗号化の時刻情報と標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を含んでいる。第１復号部３０７において前記タイムスタンプ装置用の暗号化時刻データが自らの秘密鍵で復号できることにより、前記タイムスタンプ装置用の暗号化時刻データが確かに標準時刻配信装置１４０から送信されたものであることが判明する。

【００６８】

次に、タイムスタンプを生成する（ステップＳ８１０）。ここでは、タイムスタンプ装置１５０のタイムスタンプ生成部３０５が、ハッシュ値取得部３０２が取得したハッシュ値に対して、ステップＳ８０９において復号された時刻情報に基づいてタイムスタンプを生成する。

【００６９】

続いて、タイムスタンプ利用者用の暗号化時刻データを生成する（ステップＳ８１１）。ここでは、タイムスタンプ装置１５０のタイムスタンプ利用者用の暗号化時刻データ生成部３０６が、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報にステップＳ８１０で生成されたタイムスタンプを付加し、タイムスタンプ利用者用装置１３０へ送信するためのタイムスタンプ利用者用の暗号化時刻データを生成する。

【００７０】

次に、タイムスタンプ利用者用の暗号化時刻データを受信する（ステップＳ８１２）。ここでは、タイムスタンプ利用者用装置１３０のタイムスタンプ利用者用データ受信部４０５が、ステップＳ８１１で生成されたタイムスタンプ利用者用の暗号化時刻データを受信する。

【００７１】

続いて、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を復号する（ステップＳ８１３）。具体的には、タイムスタンプ利用者用装置１３０の第１復号部４０６が、標準時刻配信装置１４０にアクセスして標準時刻配信事業者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した標準時刻配信事業者の公開鍵を用いて前記タイムスタンプ利用者用の暗号化時刻データに含まれる標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報を復号する。ここで、タイムスタンプ利用者用装置１３０に、予め、標準時刻配信事業者の公開鍵に保有させていてもよい。

【００７２】

そして、タイムスタンプの真偽を判定する（ステップＳ８１４）。具体的には、タイムスタンプ利用者用装置１３０の判定部４０７が、ステップＳ８１２で取得したタイムスタンプ利用者用の暗号化時刻データに含まれているタイムスタンプが示す時刻情報とステップＳ８１３で復号された時刻情報とを比較し、タイムスタンプの示す時刻が改ざんされているか否かを判定する。この処理により、タイムスタンプの示す時刻が、標準時刻配信装置１４０が発行した正確な時刻どおりであるか否かが判明する。

【００７３】

以上のような処理を実行することで、実施の形態２にかかる時刻認証システムでは、まず、時刻認証局のタイムスタンプ装置１２０において、時刻情報を含むタイムスタンプ装置用暗号化時刻データが確かに標準時刻配信事業者の標準時刻配信装置１４０から配信されたものか否かを判断できる。また、タイムスタンプ利用者用装置１３０において、時刻認証局のタイムスタンプ装置１２０が受付時刻を改ざんしているか否かを判別することが

できる。
【００７４】
すなわち、実施の形態２にかかる時刻認証システムでは、まず、標準時刻配信装置１４０が、時刻認証局のタイムスタンプ装置１５０を介して、標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１３０で復号できる時刻情報とともに、時刻情報を時刻認証局の公開鍵で暗号化した第１タイムスタンプ装置用データを時刻認証局のタイムスタンプ装置１５０へ供給している。このため、タイムスタンプ装置１５０において時刻認証局の秘密鍵で第１タイムスタンプ装置用データを復号することで、時刻情報が得られるとともに第１タイムスタンプ装置用データが標準時刻配信事業者の標準時刻配信装置１４０からもたらされたものであることが判断できる。また、標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１３０で復号できる時刻情報は、時刻認証局の秘密鍵で２重に暗号化され、そのままタイムスタンプ利用者用装置１３０へもたらされる。したがって、タイムスタンプ装置１２０の不具合もしくは時刻認証局の故意によりタイムスタンプが示す時刻が改ざんされた場合であっても、タイムスタンプ利用者用装置１３０側で、タイムスタンプが示す時刻と標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１３０でのみ復号できる時刻情報とを比較することにより、時刻認証局における時刻改ざんの有無が判別できる。前記タイムスタンプが示す時刻が標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１３０でのみ復号できる時刻情報と同じであれば、時刻認証局における時刻の改ざんがないと判断できる。
【００７５】
（実施の形態３）
次に、本発明の実施の形態３にかかる時刻認証システム、標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置について説明する。
【００７６】
（時刻認証システムの全体構成）
実施の形態３にかかる時刻認証システムは、標準時刻配信装置１６０と、タイムスタンプ装置１７０と、複数のタイムスタンプ利用者用装置１８０と、がそれぞれネットワークを介して相互通信可能に接続されている。この構成は、図１に示した実施の形態１のものと同様であるため、図は省略する。
【００７７】
（標準時刻配信装置の機能的構成）
図９は、実施の形態３にかかる標準時刻配信装置の機能的構成を示すブロック図である。この標準時刻配信装置１６０は、通信制御部２０１と、時刻情報要求受付部２０２と、標準時刻生成部２０３と、第１暗号化部２０４と、公開鍵証明書データ発行部２０５と、第２暗号化部２０６と、復号部２０７と、を備えている。
【００７８】
通信制御部２０１は、ネットワークとの通信を制御する。復号部２０７は、通信制御部２０１を介して、タイムスタンプ利用者用装置１８０から配信された、タイムスタンプ利用者の秘密鍵で公開鍵暗号化された発行時刻要求データ（詳細は後述する）を受信する。すると、タイムスタンプ利用者用装置１８０にアクセスしてタイムスタンプ利用者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出したタイムスタンプ利用者の公開鍵を用いて前記発行時刻要求データを復号する。この発行時刻要求データは、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報（タイムスタンプ利用者装置に内蔵されている時計に基づくもの）が含まれている。このタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報は、標準時刻生成部２０３へ送られる。時刻情報要求受付部２０２は、通信制御部２０１を介して、タイムスタンプ装置１７０からの時刻情報配信要求を受け付ける。標準時刻生成部２０３は、常に正確な時刻を保持しており、時刻情報要求受付部２０２が時刻情報配信要求を受け付けると、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報と時刻情報を第１暗号化部２０

４へ配信するとともに、時刻情報を第２暗号化部２０６へ配信する。第１暗号化部２０４は、標準時刻生成部２０３から配信された、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報と時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化する。ここで暗号化されたデータは、第２暗号化部２０６へ配信される。公開鍵証明書データ発行部２０５は、タイムスタンプ利用者用装置１８０からの要求に基づき標準時刻配信事業者の公開鍵証明書データを発行する。第２暗号化部２０６は、第１暗号化部２０４で暗号化されたデータおよび標準時刻生成部２０３から配信された時刻情報を受け付けると、タイムスタンプ装置１７０にアクセスして時刻認証局の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した時刻認証局の公開鍵を用いて第１暗号化部２０４で暗号化されたデータおよび標準時刻生成部２０３から配信された時刻情報を暗号化する（以後、タイムスタンプ装置用の二重暗号化時刻データという）。このタイムスタンプ装置用の二重暗号化時刻データは、通信制御部２０１を介してタイムスタンプ装置１７０へ配信される。ここで、タイムスタンプ利用者装置は、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を、標準時刻配信事業者に送信するとともに、同時にタイムスタンプを希望する文書データのハッシュ値を、時刻認証局へも送信する。

【００７９】

（タイムスタンプ装置の機能的構成）

図１０は、実施の形態３にかかるタイムスタンプ装置の機能的構成を示すブロック図である。このタイムスタンプ装置１７０は、通信制御部３０１と、ハッシュ値取得部３０２と、時刻情報配信要求発行部３０３と、時刻情報受信部３０４と、タイムスタンプ生成部３０５と、第１復号部３０７と、公開鍵証明書データ発行部３０８と、タイムスタンプデータ生成部３０９と、第２復号部３１０と、暗号化部３１１と、を備えている。

【００８０】

通信制御部３０１は、ネットワークとの通信を制御する。第２復号部３１０は、通信制御部３０１を介して、タイムスタンプ利用者用装置１８０から送信された、タイムスタンプ利用者の秘密鍵で公開鍵暗号化されたハッシュ値（詳細は後述する）を受信する。すると、タイムスタンプ利用者用装置１８０にアクセスしてタイムスタンプ利用者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出したタイムスタンプ利用者の公開鍵を用いて前記タイムスタンプ利用者の秘密鍵で公開鍵暗号化されたハッシュ値を復号する。ハッシュ値取得部３０２は、第２復号部３１０で復号されたハッシュ値を取得する。時刻情報配信要求発行部３０３は、ハッシュ値取得部３０２が前記ハッシュ値を取得すると、通信制御部３０１を介して、標準時刻配信装置１６０へ時刻情報の配信要求を発行する。

【００８１】

時刻情報受信部３０４は、通信制御部３０１を介して標準時刻配信装置１６０から送信されたタイムスタンプ装置用の二重暗号化時刻データを受信する。第１復号部３０７は、前記タイムスタンプ装置用の二重暗号化時刻データを時刻認証局の秘密鍵で復号する。ここで復号されたデータは、時刻情報と、標準時刻配信事業者の秘密鍵で公開鍵暗号化された、時刻情報およびタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を含んでいる。第１復号部３０７において前記タイムスタンプ装置用の二重暗号化時刻データが時刻認証局の秘密鍵で復号できることにより、前記タイムスタンプ装置用の二重暗号化時刻データが確かに標準時刻配信装置１６０から送信されたものであることが判明する。タイムスタンプ生成部３０５は、ハッシュ値取得部３０２が取得したハッシュ値に対して、第１復号部３０７で復号された時刻情報からタイムスタンプを生成する。タイムスタンプデータ生成部３０９は、標準時刻配信事業者の秘密鍵で公開鍵暗号化された、時刻情報およびタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報にタイムスタンプ生成部３０５で生成されたタイムスタンプと前記ハッシュ値を付加し、タイムスタンプ利用者用装置１８０へ送信するためのタイムスタンプデータを生成する。公開鍵証明書データ発行部３０８は、標準時刻配信装置１６０およびタイムスタンプ利用者用装置１８０からの要求に基づき時刻認証局の公開鍵証明書データを発行する。暗号化部３

１１は、前記タイムスタンプデータを時刻認証局の秘密鍵で公開鍵暗号化する。ここでのタイムスタンプデータには、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報、暗号化されていない時刻情報（標準時刻配信事業者が生成するもの）、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報、及び、当該ハッシュ値の４つのデータが含んでいる。これらのデータを全て、時刻認証局の秘密鍵で公開鍵暗号化して、タイムスタンプを生成する。

【００８２】

（タイムスタンプ利用者用装置の機能的構成）

図１１は、実施の形態３にかかるタイムスタンプ利用者用装置の機能的構成を示すブロック図である。このタイムスタンプ利用者用装置１８０は、通信制御部４０１と、文書・電子データ作成部４０２と、ハッシュ値生成部４０３と、格納部４０４と、タイムスタンプ利用者用データ受信部４０５と、第１復号部４０６と、判定部４０７と、発行時刻要求データ生成部４０８と、第１暗号化部４０９と、第２暗号化部４１０と、公開鍵証明書データ発行部４１１と、第２復号部４１２と、を備えている。

【００８３】

通信制御部４０１は、ネットワークとの通信を制御する。文書・電子データ作成部４０２は、ユーザの操作により文書・電子データを作成する。ハッシュ値生成部４０３は、文書・電子データ作成部４０２で作成された文書・電子データからハッシュ値を生成する。ここで生成されたハッシュ値は、文書・電子データ作成部４０２で作成された文書・電子データとともに格納部４０４に格納される。第１暗号化部４０９は、前記ハッシュ値をタイムスタンプ利用者の秘密鍵で公開鍵暗号化する。ここで暗号化されたハッシュ値は、通信制御部４０１を介して、タイムスタンプ装置１７０へ送信される。発行時刻要求データ生成部４０８は、発行時刻要求データ（タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報）を生成する。第２暗号化部４１０は、前記発行時刻要求データをタイムスタンプ利用者の秘密鍵で公開鍵暗号化する。ここで暗号化された前記発行時刻要求データは、通信制御部４０１を介して標準時刻配信装置１６０へ配信される。公開鍵証明書データ発行部４１１は、標準時刻配信装置１６０およびタイムスタンプ装置１７０からの要求に基づきタイムスタンプ利用者の公開鍵証明書データを発行する。

【００８４】

タイムスタンプ利用者用データ受信部４０５は、通信制御部４０１を介してタイムスタンプ装置１７０から送信された前記タイムスタンプデータを受信する。第２復号部４１２は、タイムスタンプ利用者用データ受信部４０５がタイムスタンプデータを受信すると、タイムスタンプ装置１７０にアクセスして時刻認証局の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した時刻認証局の公開鍵を用いて前記タイムスタンプデータを復号する。ここで復号されたデータには、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報および発行時刻要求データと、ハッシュ値と、タイムスタンプが示す時刻情報が含まれている。第１復号部４０６は、標準時刻配信装置１６０にアクセスして標準時刻配信事業者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した標準時刻配信事業者の公開鍵を用いて標準時刻配信事業者の秘密鍵で公開鍵暗号化された、時刻情報および発行時刻要求データ（タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報）を復号する。ここで、タイムスタンプデータの復号化の順序として、第２復号部で、時刻認証局の公開鍵で復号化した後に、標準時刻配信事業者の公開鍵で、復号化するという二重復号化の処理を行う。判定部４０７は、前記タイムスタンプが示す時刻情報と前記時刻情報と前記発行時刻要求データとを比較し、前記タイムスタンプが示す時刻が改ざんされているか否かを判定する。前記タイムスタンプが示す時刻が前記時刻情報および前記発行時刻要求データと同時刻であれば、時刻認証局における時刻の改ざんがないと判断できる。また、判定部４０７は、第２復号部で復号されたハッシュ値と、格納部４０４に格納されているハッシュ値とを比較し、同値であるか否かを判定する。ここで同値であれば文書・電子データの改ざんはないと判断できる。

【００８５】

（時刻認証システムの処理）
次に、実施の形態３にかかる時刻認証システムの処理の内容について説明する。図１２は、実施の形態３にかかる時刻認証システムの処理手順を示すフローチャートである。
【００８６】
図１２のフローチャートにおいて、まず、文書・電子データを生成する（ステップＳ１２０１）。この処理は、ユーザの操作によりタイムスタンプ利用者用装置１８０の文書・電子データ作成部４０２が実行する。
【００８７】
次に、ハッシュ値を生成する（ステップＳ１２０２）。この処理は、ハッシュ値生成部４０３が、ステップＳ１２０１で作成された文書・電子データからハッシュ値を生成する。このハッシュ値は、前記文書・電子データとともに格納部４０４に格納される。
【００８８】
次に、ハッシュ値をタイムスタンプ利用者の秘密鍵で公開鍵暗号化する（ステップＳ１２０３）。ここでは、第１暗号化部４０９が、ステップＳ１２０２で生成されたハッシュ値をタイムスタンプ利用者の秘密鍵で公開鍵暗号化する。
【００８９】
次に、タイムスタンプ利用者の秘密鍵で公開鍵暗号化されたハッシュ値を受信する（ステップＳ１２０４）。ここでは、タイムスタンプ装置１７０の第２復号部３１０が、通信制御部３０１を介して、タイムスタンプ利用者用装置１８０から送信された、タイムスタンプ利用者の秘密鍵で公開鍵暗号化されたハッシュ値を受信する。
【００９０】
そして、復号する（ステップＳ１２０５）。具体的には、第２復号部３１０が、タイムスタンプ利用者用装置１８０にアクセスしてタイムスタンプ利用者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出したタイムスタンプ利用者の公開鍵を用いて前記タイムスタンプ利用者の秘密鍵で公開鍵暗号化されたハッシュ値を復号する。
【００９１】
続いて、ハッシュ値を取得する（ステップＳ１２０６）。具体的には、タイムスタンプ装置１７０のハッシュ値取得部３０２が、ステップＳ１２０５で復号されたハッシュ値を取得する。
【００９２】
次に、時刻情報の配信要求を発行する（ステップＳ１２０７）。具体的には、タイムスタンプ装置１７０の時刻情報配信要求発行部３０３が、標準時刻配信装置１６０へ時刻情報の配信要求を発行する。
【００９３】
また、前記ステップＳ１２０１～ステップＳ１２０７の処理と平行して次のステップＳ１２０８～ステップＳ１２１１の処理が実行される。
【００９４】
まず、発行時刻要求データ（タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報）を生成する（ステップＳ１２０８）。ここでは、発行時刻要求データ生成部４０８が、発行時刻要求データを生成する。
【００９５】
次に、発行時刻要求データをタイムスタンプ利用者の秘密鍵で公開鍵暗号化する（ステップＳ１２０９）。ここでは、第２暗号化部４１０が、ステップＳ１２０８で生成された発行時刻要求データをタイムスタンプ利用者の秘密鍵で公開鍵暗号化する。
【００９６】
次に、暗号化された発行時刻要求データを受信する（ステップＳ１２１０）。ここでは、標準時刻配信装置１６０の復号部２０７が、通信制御部２０１を介して、タイムスタンプ利用者用装置１８０から配信された、タイムスタンプ利用者の秘密鍵で公開鍵暗号化された発行時刻要求データを受信する。
【００９７】

そして、復号する（ステップＳ１２１１）。具体的には、復号部２０７が、タイムスタンプ利用者用装置１８０にアクセスしてタイムスタンプ利用者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出したタイムスタンプ利用者の公開鍵を用いて前記タイムスタンプ利用者の秘密鍵で公開鍵暗号化された発行時刻要求データを復号する。この発行時刻要求データは、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報が含まれている。このタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報は、標準時刻生成部２０３へ送られる。

【００９８】

続いて、時刻情報を配信する（ステップＳ１２１２）。標準時刻生成部２０３は、常に正確な時刻を保持しており、時刻情報要求受付部２０２が時刻情報配信要求を受け付けると、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報と時刻情報を第１暗号化部２０４へ配信するとともに、時刻情報を第２暗号化部２０６へ配信する。

【００９９】

次に、第１の暗号化を行う（ステップＳ１２１３）。具体的には、標準時刻配信装置１６０の第１暗号化部２０４が、標準時刻生成部２０３から配信された、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報と時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化する。ここで暗号化されたデータは、第２暗号化部２０６へ配信される。

【０１００】

続いて、第２の暗号化を行う（ステップＳ１２１４）。具体的には、第２暗号化部２０６が、第１暗号化部２０４で暗号化されたデータおよび標準時刻生成部２０３から配信された時刻情報を受け付けると、タイムスタンプ装置１７０にアクセスして時刻認証局の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した時刻認証局の公開鍵を用いて第１暗号化部２０４で暗号化されたデータおよび標準時刻生成部２０３から配信された時刻情報を暗号化する（以後、タイムスタンプ装置用の二重暗号化時刻データという）。このタイムスタンプ装置用の二重暗号化時刻データは、通信制御部２０１を介してタイムスタンプ装置１７０へ配信される。よって、標準時刻配信装置１６０から送信される時刻情報は、二重暗号化された時刻情報と、時刻認証局の公開鍵のみで暗号化された時刻情報の２種類がある。

【０１０１】

次に、タイムスタンプ装置１７０では、タイムスタンプ装置用の二重暗号化時刻データを受信する（ステップＳ１２１５）。ここでは、タイムスタンプ装置１７０の第１復号部３０７が、通信制御部３０１を介して、前記第２のタイムスタンプ装置用データを受信する。

【０１０２】

そして、復号する（ステップＳ１２１６）。ここでは、第１復号部３０７が、前記第２のタイムスタンプ装置用データを時刻認証局の秘密鍵で復号する。ここで復号されたデータは、時刻情報と、標準時刻配信事業者の秘密鍵で公開鍵暗号化された時刻情報およびタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報を含んでいる。第１復号部３０７において前記タイムスタンプ装置用の二重暗号化時刻データが時刻認証局の秘密鍵で復号できることにより、前記タイムスタンプ装置用の二重暗号化時刻データが確かに標準時刻配信装置１６０から送信されたものであることが判明する。

【０１０３】

次に、タイムスタンプを生成する（ステップＳ１２１７）。ここでは、タイムスタンプ生成部３０５が、ハッシュ値取得部３０２が取得したハッシュ値に対して、第１復号部３０７で復号された時刻情報からタイムスタンプを生成する。

【０１０４】

続いて、タイムスタンプデータを生成する（ステップＳ１２１８）。ここでは、タイムスタンプデータ生成部３０９が、標準時刻配信事業者の秘密鍵で公開鍵暗号化された、時刻情報およびタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報に、

タイムスタンプ生成部３０５で生成されたタイムスタンプと前記ハッシュ値を付加し、タイムスタンプ利用者用装置１８０へ送信するためのタイムスタンプデータを生成する。

【０１０５】

そして、暗号化する（ステップＳ１２１９）。ここでは、暗号化部３１１が時刻認証局の秘密鍵で、前記タイムスタンプデータを暗号化する。

【０１０６】

次に、暗号化されたタイムスタンプデータを受信する（ステップＳ１２２０）。ここでは、タイムスタンプ利用者用装置１８０のタイムスタンプ利用者用データ受信部４０５が、ステップＳ１２１９で暗号化されたタイムスタンプデータを受信する。

【０１０７】

そして、復号する（ステップＳ１２２１）。具体的には、第２復号部４１２が、タイムスタンプ装置１７０にアクセスして時刻認証局の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した時刻認証局の公開鍵を用いて前記タイムスタンプデータを復号する。ここで復号されたデータには、標準時刻配信事業者の秘密鍵で公開鍵暗号化された、時刻情報および発行時刻要求データと、ハッシュ値と、タイムスタンプが示す時刻情報が含まれている。

【０１０８】

続いて、標準時刻配信事業者の秘密鍵で公開鍵暗号化された、時刻情報および発行時刻要求データを復号する（ステップＳ１２２２）。具体的には、第１復号部４０６が、標準時刻配信装置１６０にアクセスして標準時刻配信事業者の公開鍵証明書データの発行を受け、当該公開鍵証明書データから抽出した標準時刻配信事業者の公開鍵を用いて、標準時刻配信事業者の秘密鍵で公開鍵暗号化された、時刻情報および発行時刻要求データを復号する。

【０１０９】

そして、タイムスタンプなどの真偽を判定する（ステップＳ１２２３）。ここでは、判定部４０７が、前記タイムスタンプが示す時刻情報と前記時刻情報と前記発行時刻要求データ（タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報）とを比較し、前記タイムスタンプが示す時刻が改ざんされているか否かを判定する。前記タイムスタンプが示す時刻が前記時刻情報および前記発行時刻要求データと同時刻であれば、時刻認証局における時刻の改ざんや遅延がないと判断できる。また、判定部４０７は、第２復号部で復号されたハッシュ値と、格納部４０４に格納されているハッシュ値とを比較し、同値であるか否かを判定する。ここで同値であれば文書・電子データの改ざんはないと判断できる。

【０１１０】

以上のような処理を実行することで、実施の形態３にかかる時刻認証システムでは、まず、時刻認証局のタイムスタンプ装置１７０において、時刻情報を含むタイムスタンプ装置用の二重暗号化時刻データが確かに標準時刻配信事業者の標準時刻配信装置１６０から配信されたものか否かを判断できる。また、タイムスタンプ利用者用装置１８０において、時刻認証局のタイムスタンプ装置１７０が受付時刻を改ざんまたは遅延させているか否かを判別することができる。

【０１１１】

すなわち、実施の形態３にかかる時刻認証システムでは、まず、タイムスタンプ利用者用装置１８０が、タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報（文書・電子データ作成時の時刻）を標準時刻配信装置１６０へ配信する。次に、標準時刻配信装置１６０は、その時刻と時刻情報を標準時刻配信事業者の秘密鍵で公開鍵暗号化し、タイムスタンプ利用者用装置１８０で復号できるようにする。さらに、それらを時刻情報とともに時刻認証局の公開鍵で二重暗号化して生成したタイムスタンプ装置用データを時刻認証局のタイムスタンプ装置１７０へ供給している。このため、タイムスタンプ装置１７０において時刻認証局の秘密鍵で前記タイムスタンプ装置用データを復号することで、時刻情報が得られるとともに前記タイムスタンプ装置用データが標準時刻配信事業者

の標準時刻配信装置１６０からもたらされたものであることが判断できる。また、標準時刻配信事業者の秘密鍵で公開鍵暗号化され、タイムスタンプ利用者用装置１８０で復号できる時刻情報やあらかじめタイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報は、タイムスタンプ装置１７０では復号せず、そのままタイムスタンプ利用者用装置１８０へもたらされる。したがって、タイムスタンプ装置１７０によりタイムスタンプが示す時刻が改ざんまたは遅延された場合であっても、タイムスタンプ利用者用装置１８０側で、タイムスタンプが示す時刻と標準時刻配信事業者の秘密鍵で公開鍵暗号化されタイムスタンプ利用者用装置１８０で復号できる時刻情報および前記タイムスタンプ利用者が押印を要求する際発行される押印要求時刻情報とを比較することにより、時刻認証局における時刻改ざんまたは遅延の有無が判別できる。

【０１１２】

さらに、タイムスタンプ利用者用装置１８０側で、タイムスタンプ利用者用装置１８０とタイムスタンプ装置１７０との間のやり取りの後、文書・電子データのハッシュ値を比較することで、文書の改ざんの有無を判別することも可能になる。

【０１１３】

以上説明したように、本発明によれば、第三者による電子データ作成時刻の改ざんはもとより、時刻認証局による電子データ作成時刻の改ざんまたは遅延を防止することができる。

【０１１４】

なお、本実施の形態で説明した時刻認証方法は、あらかじめ用意されたプログラムをコンピュータで実行することにより実現することができる。このプログラムは、ハードディスクなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。

【産業上の利用可能性】

【０１１５】

以上のように、本発明にかかる標準時刻配信装置、タイムスタンプ装置、タイムスタンプ利用者用装置、時刻認証システム、時刻認証方法、および時刻認証プログラムは、電子データ作成時刻の改ざんの防止に有用であり、特に、時刻認証局による電子データ作成時刻の改ざんまたは故意の遅延の防止に適している。また、標準時刻配信事業者は、時刻情報を特定の時刻認証局にのみ送信できるので、時刻認証局の信憑性が高まるとともに、標準時刻配信事業者が時刻認証局に対して、課金などのコントロールがし易いものとなる。

【図面の簡単な説明】

【０１１６】

【図１】本発明の実施の形態１にかかる時刻認証システムの全体構成を示す図である。

【図２】実施の形態１にかかる標準時刻配信装置の機能的構成を示すブロック図である。

【図３】実施の形態１にかかるタイムスタンプ装置の機能的構成を示すブロック図である。

【図４】実施の形態１にかかるタイムスタンプ利用者用装置の機能的構成を示すブロック図である。

【図５】実施の形態１にかかる時刻認証システムの処理手順を示すフローチャートである。

【図６】実施の形態２にかかる標準時刻配信装置の機能的構成を示すブロック図である。

【図７】実施の形態２にかかるタイムスタンプ装置の機能的構成を示すブロック図である。

【図８】実施の形態２にかかる時刻認証システムの処理手順を示すフローチャートである。

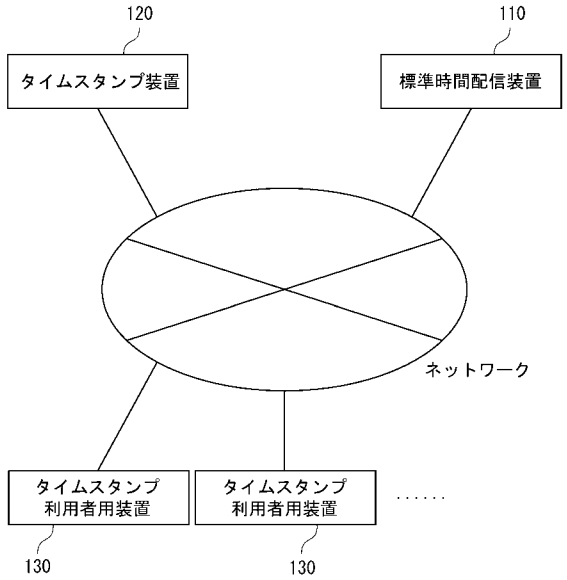
【図９】実施の形態３にかかる標準時刻配信装置の機能的構成を示すブロック図である。

【図１０】実施の形態３にかかるタイムスタンプ装置の機能的構成を示すブロック図である。

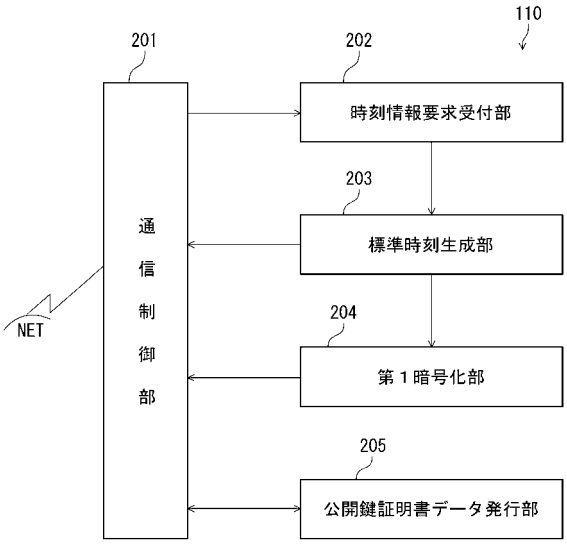
【図１１】実施の形態３にかかるタイムスタンプ利用者用装置の機能的構成を示すブロッ

ク図である。
【図１２】実施の形態３にかかる時刻認証システムの処理手順を示すフローチャートである。
【符号の説明】
【０１１７】
１１０，１４０，１６０　標準時刻配信装置
１２０，１５０，１７０　タイムスタンプ装置
１３０，１８０　タイムスタンプ利用者用装置
２０１，３０１，４０１　通信制御部
２０２　時刻情報要求受付部
２０３　標準時刻生成部
２０４，４０９　第１暗号化部
２０５，３０８，４１１　公開鍵証明書データ発行部
２０６，４１０　第２暗号化部
２０７　復号部
３０２　ハッシュ値取得部
３０３　時刻情報配信要求発行部
３０４　時刻情報受信部
３０５　タイムスタンプ生成部
３０６　タイムスタンプ利用者用の暗号化時刻データ生成部
３０７，４０６　第１復号部
３０９　タイムスタンプデータ生成部
３１０，４１２　第２復号部
３１１　暗号化部
４０２　文書・電子データ作成部
４０３　ハッシュ値生成部
４０４　格納部
４０５　タイムスタンプ利用者用データ受信部
４０７　判定部
４０８　発行時刻要求データ生成部

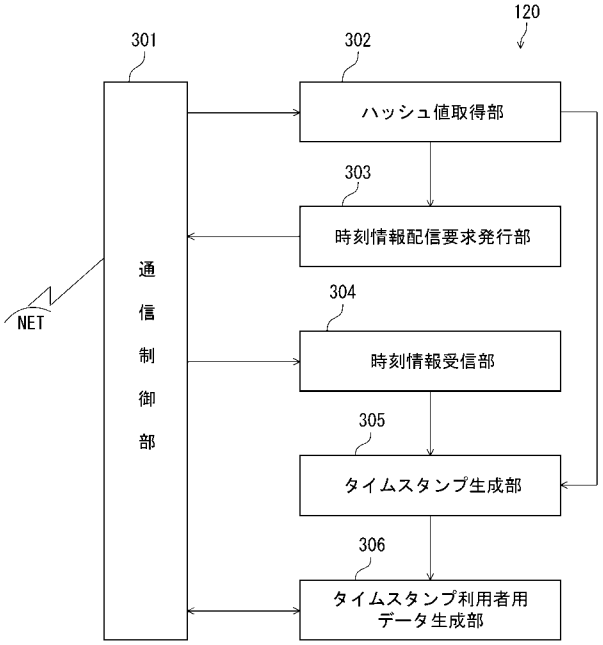
【図１】


120
110
タイムスタンプ装置
標準時間配信装置
ネットワーク
タイムスタンプ
利用者用装置
タイムスタンプ
利用者用装置
130
130

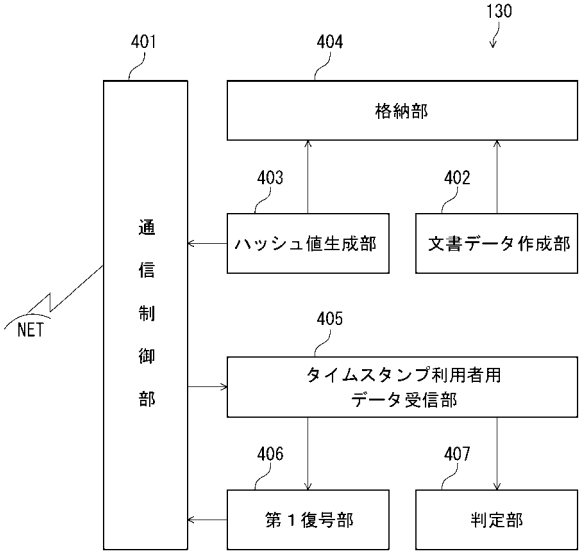
【図２】


110
201
202
通信制御部
時刻情報要求受付部
203
標準時刻生成部
NET
204
第１暗号化部
205
公開鍵証明書データ発行部

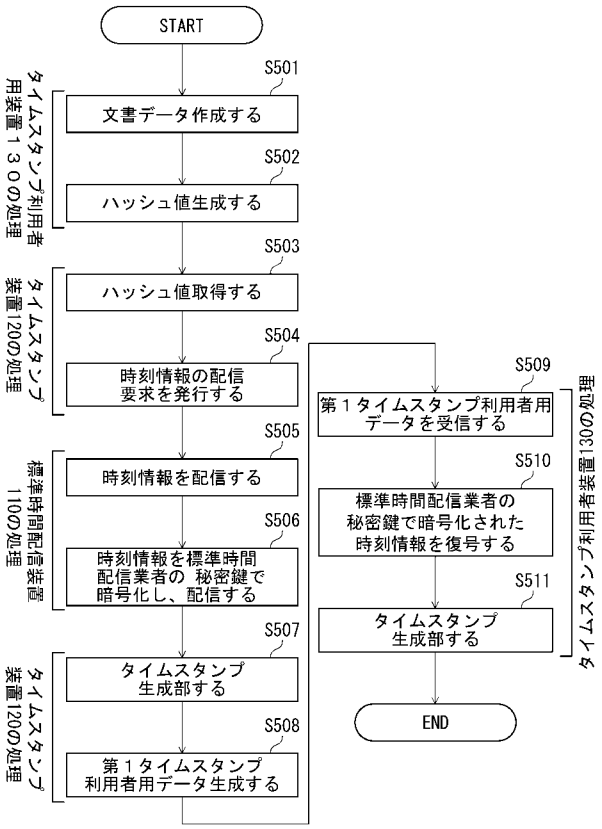
【図３】


120
301
302
通信制御部
ハッシュ値取得部
303
時刻情報配信要求発行部
NET
304
時刻情報受信部
305
タイムスタンプ生成部
306
タイムスタンプ利用者用
データ生成部

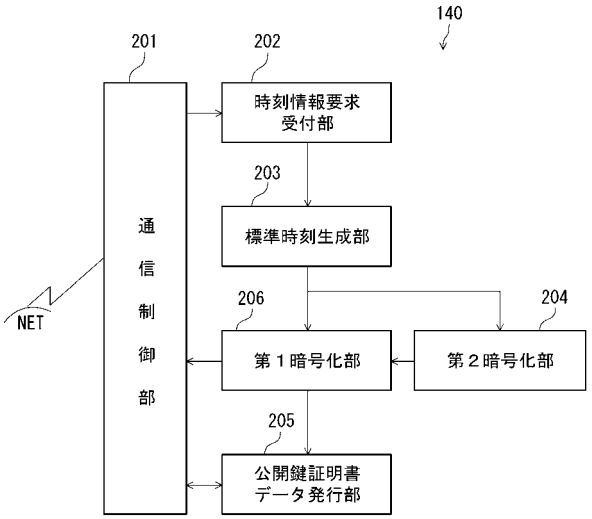
【図４】


130
401
404
通信制御部
格納部
403
402
ハッシュ値生成部
文書データ作成部
NET
405
タイムスタンプ利用者用
データ受信部
406
407
第１復号部
判定部

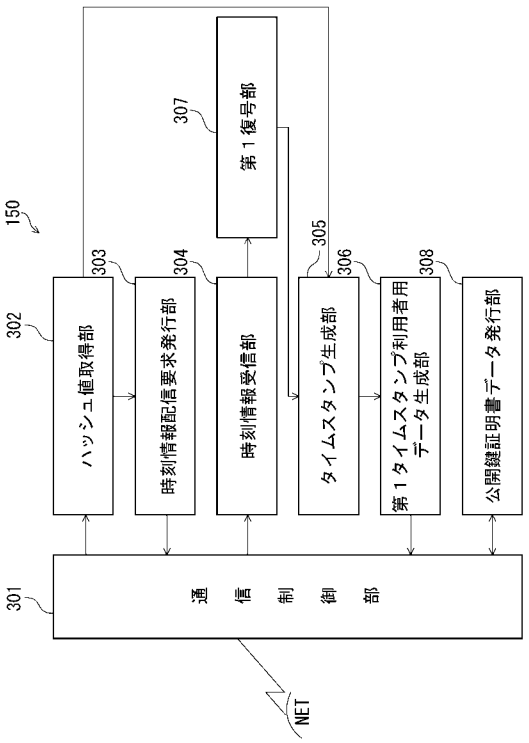
【図５】


START
S501
文書データ作成する
S502
ハッシュ値生成する
S503
ハッシュ値取得する
S504
時刻情報の配信
要求を発行する
S505
時刻情報を配信する
S506
時刻情報を標準時間
配信業者の 秘密鍵で
暗号化し、配信する
S507
タイムスタンプ
生成部する
S508
第１タイムスタンプ
利用者用データ生成する
S509
第１タイムスタンプ利用者用
データを受信する
S510
標準時間配信業者の
秘密鍵で暗号化された
時刻情報を復号する
S511
タイムスタンプ
生成部する
END
タイムスタンプ利用者装置130の処理
タイムスタンプ装置120の処理
標準時間配信業者装置110の処理
タイムスタンプ装置120の処理
タイムスタンプ利用者装置130の処理

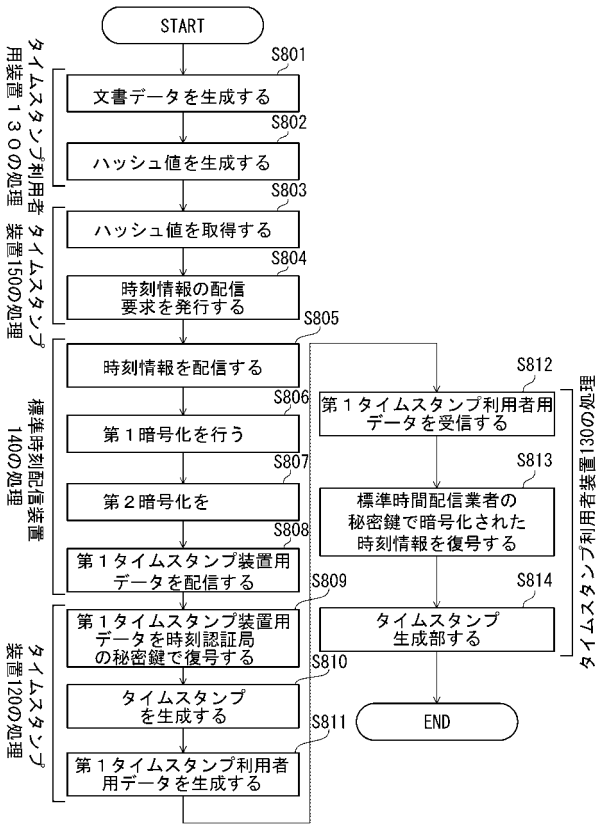
【図６】


140
201
202
時刻情報要求
受付部
203
標準時刻生成部
通信制御部
NET
206
204
第１暗号化部
第２暗号化部
205
公開鍵証明書
データ発行部

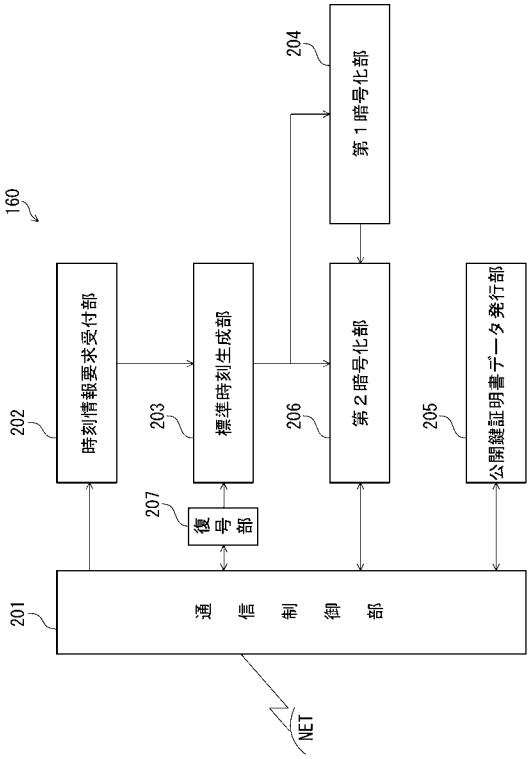
【図７】


150
307
第１復号部
303
304
305
306
308
302
ハッシュ値取得部
時刻情報配信要求発行部
時刻情報受信部
タイムスタンプ生成部
第１タイムスタンプ利用者用
データ生成部
公開鍵証明書データ発行部
301
通信制御部
NET

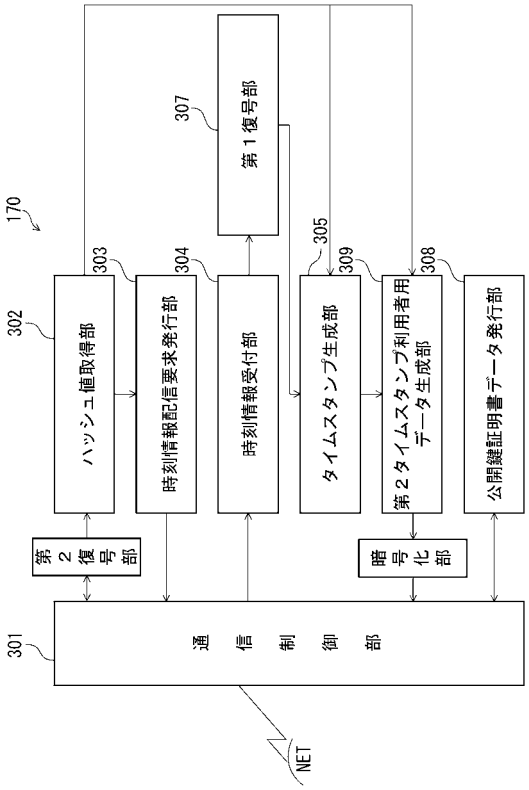
【図８】


START
S801
文書データを生成する
S802
ハッシュ値を生成する
S803
ハッシュ値を取得する
S804
時刻情報の配信
要求を発行する
S805
時刻情報を配信する
S806
第１暗号化を行う
S807
第２暗号化を
S808
第１タイムスタンプ装置用
データを配信する
S809
第１タイムスタンプ装置用
データを時刻認証局
の秘密鍵で復号する
S810
タイムスタンプ
を生成する
S811
第１タイムスタンプ利用者
用データを生成する
S812
第１タイムスタンプ利用者用
データを受信する
S813
標準時間配信業者の
秘密鍵で暗号化された
時刻情報を復号する
S814
タイムスタンプ
生成部する
END
タイムスタンプ利用者装置130の処理
タイムスタンプ装置120の処理
標準時間配信業者装置140の処理
タイムスタンプ装置120の処理
タイムスタンプ利用者装置130の処理

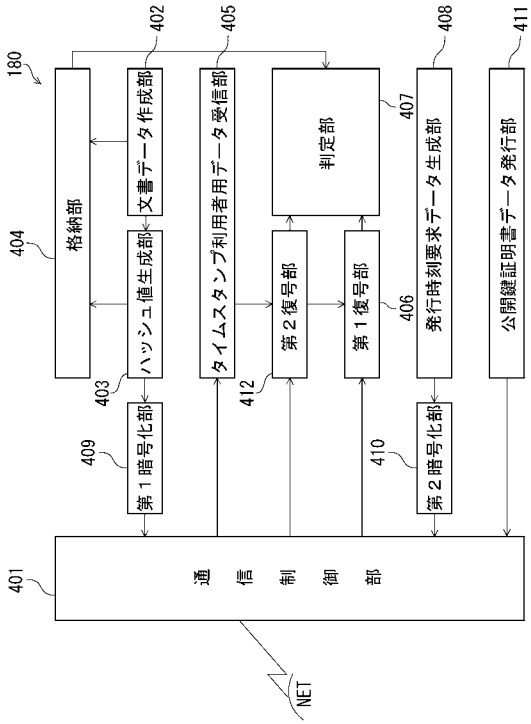
【図９】



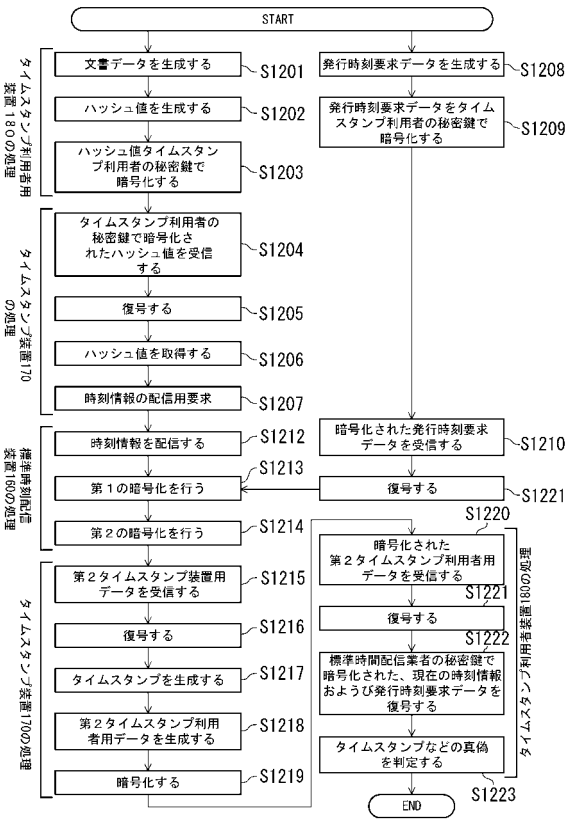
【図１０】



【図１１】



【図１２】



フロントページの続き

(56)参考文献 特開２００３－１９８５３９（ＪＰ，Ａ）
国際公開第２００６／１０９７２３（WO，Ａ１）
特開２００３－２７９６７５（ＪＰ，Ａ）
特開２００２－２１５０２９（ＪＰ，Ａ）
特開２００７－２２１５５１（ＪＰ，Ａ）
特開２００５－２４４６７８（ＪＰ，Ａ）
特表２００３－５１９４１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／６４
Ｇ０９Ｃ　　１／００