(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-253860
(P2009-253860A)
(43)公開日　平成21年10月29日(2009.10.29)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675Z	5J104
H04L	9/08	(2006.01)	H04L	9/00	601F	

審査請求 未請求　請求項の数 14　ＯＬ　（全 16 頁）

(21)出願番号　特願2008-101901 (P2008-101901)
(22)出願日　平成20年4月9日 (2008.4.9)

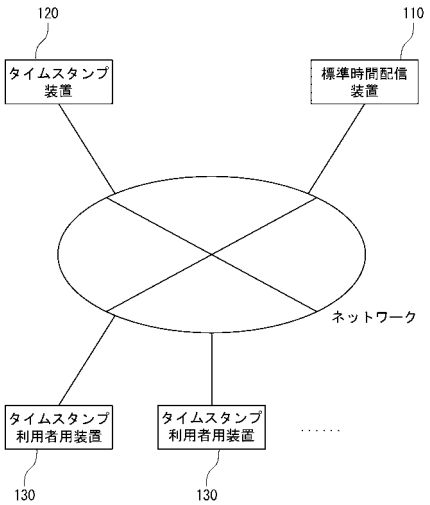
特許法第３０条第１項適用申請有り　研究集会名：第４回情報プロフェッショナルシンポジウム　主催者名：社団法人　情報科学技術協会　開催日：平成１９年１０月３１日～１１月１日　刊行物名：第４回情報プロフェッショナルシンポジウム予稿集　発行日：平成１９年１０月１０日

(71)出願人　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

Ｆターム(参考)　5J104 AA09 AA11 AA12 AA16 EA01 EA04 EA05 EA08 EA17 EA19 GA03 JA21 LA06 MA01 MA05 NA02 NA12 NA37 NA38

(54)【発明の名称】標準時刻配信システム、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)【要約】
【課題】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。
【解決手段】本発明の時刻認証システムは、標準時刻配信システム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。標準時刻配信システム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。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。そして、標準時刻配信システム１１０から配信される標準時刻情報にこの標準時刻情報と対をなす乱数情報を付加して所定の処理を実行することで、電子データ作成時刻の改ざんまたは故意の遅延を防止する。
【選択図】図１



【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任意のコンピューターに配信する標準時刻配信システムであって、
常に正確な標準時刻情報を生成する標準時刻情報生成手段と、
当該標準時刻情報と一対となる乱数情報を発生する乱数情報発生手段と、
当該標準時刻情報および乱数情報を特定のコンピューターに配信する情報配信手段と、
を備えていることを特徴とする標準時刻配信システム。
【請求項２】
前記標準時刻情報と対となる乱数情報の組合せ情報の一部を記憶することができる記憶手段を有することを特徴とする請求項１に記載の標準時刻配信システム。
【請求項３】
前記記憶手段によって記憶される標準時刻情報と対となる乱数情報の組合せ情報が、外部からの通信アクセスによって閲覧可能であることを特徴とする請求項２に記載の標準時刻配信システム。
【請求項４】
前記標準時刻情報と対となる乱数情報の組合せ情報の一部が、少なくとも時刻認証局によるタイムスタンプ時刻とその対になる乱数情報、又は任意に定めた時刻とその対になる乱数情報を含むことを特徴とする請求項２又は３に記載の標準時刻配信システム。
【請求項５】
ネットワークへの接続が可能であり、標準時刻配信システムから送信された時刻情報および乱数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用装置から送信されたファイルデータを取得するファイルデータ取得手段と、
前記ファイルデータ、前記標準時刻配信システムから送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報を用い、時刻認証局の秘密鍵で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情報生成手段と、
前記タイムスタンプ情報を前記タイムスタンプ利用者用装置へ送信するタイムスタンプ情報送信手段と、
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６】
ネットワークへの接続が可能であり、標準時刻配信システムから送信された時刻情報および乱数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、
前記ハッシュ値取得手段が取得したハッシュ値、前記標準時刻配信システムから送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報を用い、時刻認証局の秘密鍵で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情報生成手段と、
前記タイムスタンプ情報を前記タイムスタンプ利用者用装置へ送信するタイムスタンプ情報送信手段と、
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７】
ネットワークへの接続が可能であり、標準時刻配信システムから送信された時刻情報および乱数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用装置から送信された入力データを復号する復号手段と、
前記復号手段により復号された前記入力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、前記標準時刻配信システムから送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報を用い、時刻認証局の秘密鍵で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情報生成手段と、
前記タイムスタンプ情報を前記タイムスタンプ利用者用装置へ送信するタイムスタンプ情報送信手段と、
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８】
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５または６に記載のタイムスタンプ装置。
【請求項９】
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標準時刻配信システムから送信された時刻情報および乱数情報に基づいて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・電子データを入力する入力手段と、
前記入力手段から入力された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、
前記ハッシュ値を前記タイムスタンプ装置へ送信するためのハッシュ値送信手段と、
時刻認証局の公開鍵を用いて、前記タイムスタンプ装置から送信されたタイムスタンプ情報を復号する復号手段と、
前記復号手段により復号されたタイムスタンプ情報に含まれる時刻情報および当該時刻情報と対をなす乱数情報と、外部記憶装置に記憶された標準時刻情報および当該標準時刻情報と対をなす乱数情報とを比較し、前記タイムスタンプ情報に含まれる時刻情報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、
を備えていることを特徴とするタイムスタンプ利用者用装置。
【請求項１０】
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標準時刻配信システムから送信された時刻情報および乱数情報に基づいて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・電子データを入力する入力手段と、
前記入力手段から入力されたデータをタイムスタンプ利用者の秘密鍵で暗号化する暗号化手段と、
前記暗号化手段で暗号化された入力データを前記タイムスタンプ装置へ送信するための入力データ送信手段と、
時刻認証局の公開鍵を用いて、前記タイムスタンプ装置から送信されたタイムスタンプ情報を復号する復号手段と、
前記復号手段により復号されたタイムスタンプ情報に含まれる時刻情報および当該時刻情報と対をなす乱数情報と、外部記憶装置に記憶された標準時刻情報および当該標準時刻情報と対をなす乱数情報とを比較し、前記タイムスタンプ情報に含まれる時刻情報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、
を備えていることを特徴とするタイムスタンプ利用者用装置。
【請求項１１】
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９に記載のタイムスタンプ利用者用装置。
【請求項１２】
請求項１～４に記載のいずれかの標準時刻配信システムと、
請求項５～７に記載のいずれかのタイムスタンプ装置と、
請求項８～１０に記載のいずれかのタイムスタンプ利用者用装置と、
を備えていることを特徴とする時刻認証システム。
【請求項１３】

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標準時刻情報を前記タイムスタンプ装置に配信する標準時刻配信システムと、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、
前記標準時刻配信システムにおいて、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、標準時刻情報を生成する標準時刻生成工程と、
前記標準時刻配信システムにおいて、前記標準時刻生成工程で生成された標準時刻情報と対をなす乱数情報を発生する乱数情報発生工程と、
前記標準時刻配信システムにおいて、前記標準時刻情報および該標準時刻情報と対をなす乱数情報を前記タイムスタンプ装置および前記タイムスタンプ利用者用装置へ配信する時刻情報配信工程と、
前記タイムスタンプ装置において、前記標準時刻配信システムから送信された標準時刻情報および該標準時刻情報と対をなす乱数情報を用い、時刻認証局の秘密鍵で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情報生成工程と、
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情報を時刻認証局の公開鍵で復号して時刻情報および該時刻情報と対をなす乱数情報を取得する時刻情報取得工程と、
前記タイムスタンプ利用者用装置において、前記時刻情報取得工程で取得した時刻情報および該時刻情報と対をなす乱数情報と、前記標準時刻配信システムから送信された標準時刻情報および該標準時刻情報と対をなす乱数情報とを比較し、前記時刻情報取得工程で取得した時刻情報の真偽を判定する判定工程と、
を備えたことを特徴とする時刻認証方法。
【請求項１４】
請求項１０に記載の時刻認証方法をコンピューター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、電子取引などの際に、時刻の改ざんを防止する標準時刻配信システム、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２００６－３３３４３５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システム、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、請求項１の発明にかかる標準時刻配信システムは、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任意のコンピューターに配信する標準時刻配信システムであって、常に正確な標準時刻情報を生成する標準時刻情報生成手段と、当該標準時刻情報と一対となる乱数情報を発生する乱数情報発生手段と、当該標準時刻情報および乱数情報を特定のコンピューターに配信する情報配信手段とを備えていることを特徴とする。
【０００８】
また、請求項２の発明にかかる標準時刻配信システムは、請求項１に記載の発明において、前記標準時刻情報と対となる乱数情報の組合せ情報の一部を記憶することができる記憶手段を有することを特徴とする。
【０００９】
また、前記記憶手段によって記憶される標準時刻情報と対となる乱数情報の組合せ情報が、外部からの通信アクセスによって閲覧可能であることを特徴とする。標準時刻情報とそれに対となる乱数情報が開示されることで、広く公衆が確認することができ、たとえば、標準時刻情報と対となる乱数情報が、後に書き換えなど改竄することを抑止する効果を有する。
【００１０】
さらに、前記標準時刻情報と対となる乱数情報の組合せ情報の一部が、少なくとも時刻認証局によるタイムスタンプ時刻とその対になる乱数情報、又は任意に定めた時刻とその対になる乱数情報を含むことを特徴とする。秒単位ですべての時刻情報とそれに対となる乱数情報が記憶する場合には大規模なストレージなど記憶装置を必要とするが、タイムスタンプの時刻情報とそれに対となる乱数情報のみを記憶させることや、これに加えて任意に定めた時刻、たとえば、１３時、１４時など１時間毎の基準時刻をも記憶させることで必要十分な記憶情報とさせてもよい。ここで、標準時刻配信システムとは、タイムスタンプ装置などを含む広いものであってもよく、標準時刻と乱数情報を記憶する記憶手段も、外部に設ける記憶装置であってもよい。
【００１１】
また、請求項５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、標準時刻配信システムから送信された時刻情報および乱数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、前記ハッシュ値取得手段が取得したハッシュ値、前記標準時刻配信システムから送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報を用い、時刻認証局の秘密鍵で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情報生成手段と、前記タイムスタンプ情報を前記タイムスタンプ利用者用装置へ送信するタイムスタンプ情報送信手段とを備えていることを特徴とする。
【００１２】
また、請求項４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、標準時刻配信システムから送信された時刻情報および乱数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用装置から送信された入力データを復号する復号手段と、前記

復号手段により復号された前記入力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、前記標準時刻配信システムから送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報を用い、時刻認証局の秘密鍵で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情報生成手段と、前記タイムスタンプ情報を前記タイムスタンプ利用者用装置へ送信するタイムスタンプ情報送信手段と、を備えていることを特徴とする。

【００１３】

また、請求項５の発明にかかるタイムスタンプ装置は、請求項３または４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。

【００１４】

また、請求項６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標準時刻配信システムから送信された時刻情報および乱数情報に基づいて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・電子データを入力する入力手段と、前記入力手段から入力された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、前記ハッシュ値を前記タイムスタンプ装置へ送信するためのハッシュ値送信手段と、時刻認証局の公開鍵を用いて、前記タイムスタンプ装置から送信されたタイムスタンプ情報を復号する復号手段と、前記復号手段により復号されたタイムスタンプ情報に含まれる時刻情報および当該時刻情報と対をなす乱数情報と、前記標準時刻配信システムから送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報とを比較し、前記タイムスタンプ情報に含まれる時刻情報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、を備えていることを特徴とする。

【００１５】

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標準時刻配信システムから送信された時刻情報および乱数情報に基づいて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・電子データを入力する入力手段と、前記入力手段から入力されたデータをタイムスタンプ利用者の秘密鍵で暗号化する暗号化手段と、前記暗号化手段で暗号化された入力データを前記タイムスタンプ装置へ送信するための入力データ送信手段と、時刻認証局の公開鍵を用いて、前記タイムスタンプ装置から送信されたタイムスタンプ情報を復号する復号手段と、前記復号手段により復号されたタイムスタンプ情報に含まれる時刻情報および当該時刻情報と対をなす乱数情報と、前記標準時刻配信システムから送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報とを比較し、前記タイムスタンプ情報に含まれる時刻情報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、を備えていることを特徴とする。

【００１６】

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、請求項７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。

【００１７】

また、請求項９の発明にかかる時刻認証システムは、請求項１または２に記載のいずれかの標準時刻配信システムと、請求項３～５に記載のいずれかのタイムスタンプ装置と、請求項６～８に記載のいずれかのタイムスタンプ利用者用装置と、を備えていることを特徴とする。

【００１８】

また、請求項１０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標準時刻情報を前記タイムスタンプ装置に配信する標準時刻配信システムと、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、前記標準時刻配信システムにおいて、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、標準時刻情報を生成する標準時刻生成工程と、前記標準時刻配信システムにおいて、前記標準時刻生成工程で生成された標準時刻情報と対をなす乱数情報を発生する乱数情報発生工程と、前記標準時刻配信システムにおいて、前記標準時刻情報および該標準時刻情報と対をなす乱数情報を前記タイムスタンプ装置および前記タイムスタンプ利用者用装置へ配信する時刻情報配信工程と、前記タイムスタンプ装置において、前記標準時刻配信システムから送信された標準時刻情報および該標準時刻情報と対をなす乱数情報を用い、時刻認証局の秘密鍵で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情報生成工程と、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情報を時刻認証局の公開鍵で復号して時刻情報および該時刻情報と対をなす乱数情報を取得する時刻情報取得工程と、前記タイムスタンプ利用者用装置において、前記時刻情報取得工程で取得した時刻情報および該時刻情報と対をなす乱数情報と、前記標準時刻配信システムから送信された標準時刻情報および該標準時刻情報と対をなす乱数情報とを比較し、前記時刻情報取得工程で取得した時刻情報の真偽を判定する判定工程と、を備えたことを特徴とする。

【００１９】

また、請求項１１の発明にかかる時刻認証プログラムは、請求項１０に記載の時刻認証方法をコンピューターに実行させることを特徴とする。

【発明の効果】

【００２０】

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】

【００２１】

以下、添付図面を参照して、本発明にかかる標準時刻配信システム、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。

【００２２】

（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、標準時刻配信システム、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。

【００２３】

（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、標準時刻配信システム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。標準時刻配信システム１１０は、正確な時刻を保持しており、タイムスタンプ装置１２０に対して時刻情報の配信を行う。この標準時刻配信システム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に対して電子取引などにおける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。

【００２４】

（標準時刻配信システムの機能的構成）

図２は、実施の形態１にかかる標準時刻配信システムの機能的構成を示すブロック図である。この標準時刻配信システム１１０は、通信制御部２０１と、時刻情報要求受付部２０２と、標準時刻情報生成部２０３と、乱数情報発生部２０４と、情報配信部２０５と、記憶部２０６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。

【００２５】
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。標準時刻情報生成部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、当該要求受付時の標準時刻情報を生成する。乱数情報発生部２０４は、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、乱数情報を発生する。このとき発生される乱数情報は、第三者が認識不能なビット長を有している。このビット長は、標準時刻配信システム１１０の所有者である標準時刻配信事業者が任意に設定することができるようになっている。情報配信部２０５は、前記時刻情報配信要求受信の際に生成された標準時刻情報と乱数情報を対としてタイムスタンプ装置１２０やタイムスタンプ利用者用装置１３０へ配信する。記憶部２０６は、前記標準時刻情報および当該標準時刻情報と対となる乱数情報を記憶する。
【００２６】
（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、タイムスタンプ情報生成部３０５と、公開鍵証明書データ発行部３０６と、を備えている。
【００２７】
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、標準時刻配信システム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システム１１０から送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報を受信する。タイムスタンプ情報生成部３０５は、ハッシュ値取得部３０２が取得したハッシュ値と、時刻情報受信部３０４が受信した標準時刻情報および当該標準時刻情報と対をなす乱数情報とを用い、時刻認証局の秘密鍵で暗号化することによりタイムスタンプ情報を生成する。このタイムスタンプ情報は、通信制御部３０１を介してタイムスタンプ利用者用装置１３０へ送信される。なお、タイムスタンプとは、標準時刻配信システム１１０から送信された標準時刻情報を、利用者が視覚的に把握され易い特定の形式で表現することをいう。公開鍵証明書データ発行部３０６は、タイムスタンプ利用者用装置１３０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。
【００２８】
（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、入力部４０２と、ハッシュ値生成部４０３と、記憶部４０４と、タイムスタンプ情報受信部４０５と、標準時刻情報受信部４０６と、復号部４０７と、判定部４０８と、を備えている。
【００２９】
通信制御部４０１は、ネットワークとの通信を制御する。入力部４０２は、ユーザが作成しようとする文書データなどのデータを入力する。ハッシュ値生成部４０３は、入力部４０２から入力された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、前記入力データとともに記憶部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。タイムスタンプ情報受信部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情報を受信する。標準時刻情報受信部４０６は、標準時刻配信システム１１０から配信された標準時刻情報と当該標準時刻情報と対をなす乱数情報を受信する。復号部４０７は、タイムスタンプ情報受信部４０５が前記タイムスタンプ情報を受信すると、タイムスタンプ装置１２

０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情報を復号する。判定部４０８は、復号されたタイムスタンプ情報に含まれるタイムスタンプが示す時刻情報および当該時刻情報と対をなす乱数情報と、標準時刻情報受信部４０６が受信した標準時刻情報および当該標準時刻情報と対をなす乱数情報とを比較し、タイムスタンプが示す時刻が改ざんまたは故意による遅延がな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および乱数情報が、標準時刻情報受信部４０６が受信した標準時刻情報および乱数情報といずれもが一致すれば、時刻認証局における時刻の改ざんまたは故意による遅延がないと判断できる。このようにして、検証対象であるタイムスタンプが示す時刻情報の正当性が検証される。

【００３０】

（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。

【００３１】

図５のフローチャートにおいて、まず、データ入力を行う（ステップＳ５０１）。ここでは、ユーザがタイムスタンプ利用者用装置１３０の入力部４０２から作成しようとする文書データなどの入力を行う。

【００３２】

次に、ハッシュ値を生成する（ステップＳ５０２）。この処理は、タイムスタンプ利用者用装置１３０のハッシュ値生成部４０３が、ステップＳ５０１で入力されたデータからハッシュ値を生成する。このハッシュ値は、前記データとともに記憶部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。

【００３３】

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。

【００３４】

次に、標準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、標準時刻配信システム１１０へ時刻情報の配信要求を発行する。

【００３５】

次に、標準時刻情報を生成する（ステップＳ５０５）。標準時刻配信システム１１０の標準時刻情報生成部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、標準時刻情報を生成する。

【００３６】

同時に、乱数情報を発生する（ステップＳ５０６）。具体的には、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、標準時刻配信システム１１０の乱数情報発生部２０４が乱数情報を発生する。

【００３７】

次に、標準時刻情報を配信する（ステップＳ５０７）。ここでは、標準時刻配信システム１１０の情報配信部２０５が、ステップＳ５０５で生成された標準時刻情報とステップＳ５０６で発生された乱数情報とを対としてタイムスタンプ装置１２０およびタイムスタンプ利用者用装置１３０へ配信する。

【００３８】

次に、タイムスタンプ情報を生成する（ステップＳ５０８）。ここでは、タイムスタンプ装置１２０のタイムスタンプ情報生成部３０５が、ハッシュ値取得部３０２が取得したハッシュ値と、時刻情報受信部３０４が受信した標準時刻情報および当該標準時刻情報と対をなす乱数情報とを用い、時刻認証局の秘密鍵で暗号化することによりタイムスタンプ情報を生成する。

【００３９】
標準時刻情報を受信する（ステップＳ５０９）。ここでは、タイムスタンプ利用者用装置１３０の標準時刻情報受信部４０６が、ステップＳ５０７で配信された標準時刻情報と当該標準時刻情報と対をなす乱数情報を受信する。
【００４０】
次に、タイムスタンプ情報を受信する（ステップＳ５１０）。ここでは、タイムスタンプ利用者用装置１３０のタイムスタンプ情報受信部４０５が、ステップＳ５０８で生成されたタイムスタンプ情報を受信する。
【００４１】
続いて、タイムスタンプ情報を復号する（ステップＳ５１１）。具体的には、タイムスタンプ利用者用装置１３０の復号部４０７が、タイムスタンプ装置１２０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ステップＳ５１０で受信したタイムスタンプ情報を復号する。
【００４２】
そして、タイムスタンプの真偽を判定する（ステップＳ５１２）。ここでは、タイムスタンプ利用者用装置１３０の判定部４０８が、ステップＳ５０９で取得した標準時刻配信システム１１０から配信された標準時刻情報と当該標準時刻情報と対をなす乱数情報と、ステップＳ５１１で復号されたタイムスタンプ情報に含まれるタイムスタンプが示す時刻情報および当該時刻情報と対をなす乱数情報とを比較し、タイムスタンプの示す時刻が改ざんまたは故意に遅延されているか否かを判定する。この処理では、時刻情報の他、当該時刻情報と対をなしている乱数情報をも比較することで、タイムスタンプの示す時刻が、標準時刻配信システム１１０が発行した真の時刻情報どおりであるか否かが判明する。
【００４３】
以上のように、実施の形態１にかかる時刻認証システムでは、時刻認証局が配信するタイムスタンプ情報を生成する基準となる標準時刻配信事業者が生成した標準時刻情報および当該標準時刻情報と対をなす乱数情報をタイムスタンプ利用者側が直接取得する。そして、時刻認証局が配信したタイムスタンプ情報に含まれる時刻情報および乱数情報と、前記標準時刻配信事業者から直接配信された標準時刻情報および当該標準時刻情報と対をなす乱数情報とを、タイムスタンプ利用者側で比較検証することにより、時刻認証局における時刻改ざんまたは故意による遅延の有無が判別できる。すなわち、前記タイムスタンプ情報に含まれる時刻情報および当該時刻情報と対をなす乱数情報と、前記標準時刻配信事業者から直接配信された標準時刻情報および当該標準時刻情報と対をなす乱数情報とがいずれも一致していれば、時刻認証局における時刻改ざんや故意による遅延はないと判断できる。このように、検証の対象を、時刻情報のみではなく、時刻情報と対をなしている乱数情報にまで拡大していることで、より精度の高い検証が可能になる。なお、標準時刻配信システム１１０において生成される標準時刻情報および当該標準時刻情報と対をなす乱数情報を暗号化して配信するようにしてもよい。
【００４４】
（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、標準時刻配信システム、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。
【００４５】
（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、標準時刻配信システム１１０と、タイムスタンプ装置１４０と、複数のタイムスタンプ利用者用装置１５０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。
【００４６】
（標準時刻配信システムの機能的構成）
この実施の形態２にかかる標準時刻配信システムの機能的構成は、図２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。

【００４７】

（タイムスタンプ装置の機能的構成）

図６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１４０は、通信制御部３０１と、データ取得部６０１と、復号部６０２と、ハッシュ値生成部６０３と、時刻情報配信要求発行部３０３と、時刻情報受信部３０４と、タイムスタンプ情報生成部３０５と、公開鍵証明書データ発行部３０６と、を備えている。

【００４８】

通信制御部３０１は、ネットワークとの通信を制御する。データ取得部６０１は、タイムスタンプ利用者用装置１５０から送信された、タイムスタンプ利用者の秘密鍵で暗号化された入力データ（詳細は後述）を取得する。復号部６０２は、データ取得部６０１が前記入力データを取得すると、タイムスタンプ利用者用装置１５０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入力データを復号する。ハッシュ値生成部６０３は、復号された前記入力データからハッシュ値を生成する。時刻情報配信要求発行部３０３は、データ取得部６０１がタイムスタンプ利用者用装置１５０から送信された入力データを取得すると、通信制御部３０１を介して、標準時刻配信システム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システム１１０から送信された標準時刻情報および当該標準時刻情報と対をなす乱数情報を受信する。タイムスタンプ情報生成部３０５は、ハッシュ値生成部６０３が生成したハッシュ値と、時刻情報受信部３０４が受信した標準時刻情報および当該標準時刻情報と対をなす乱数情報とを用い、時刻認証局の秘密鍵で暗号化することによりタイムスタンプ情報を生成する。このタイムスタンプ情報は、通信制御部３０１を介してタイムスタンプ利用者用装置１５０へ送信される。なお、タイムスタンプとは、標準時刻配信システム１１０から送信された標準時刻情報を、利用者が視覚的に把握され易い特定の形式で表現することをいう。公開鍵証明書データ発行部３０６は、タイムスタンプ利用者用装置１５０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。

【００４９】

（タイムスタンプ利用者用装置の機能的構成）

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１５０は、通信制御部４０１と、入力部４０２と、暗号化部７０１と、記憶部４０４と、タイムスタンプ情報受信部４０５と、標準時刻情報受信部４０６と、復号部４０７と、判定部４０８と、公開鍵証明書データ発行部７０２と、を備えている。

【００５０】

通信制御部４０１は、ネットワークとの通信を制御する。入力部４０２は、ユーザが作成しようとする文書データなどのデータを入力する。ここで入力されたデータは、記憶部４０４に格納される。暗号化部７０１は、入力部４０２から入力されたデータをタイムスタンプ利用者の秘密鍵で暗号化する。暗号化された入力データは、通信制御部４０１を介して、タイムスタンプ装置１４０へ送信される。タイムスタンプ情報受信部４０５は、通信制御部４０１を介してタイムスタンプ装置１４０から送信されたタイムスタンプ情報を受信する。標準時刻情報受信部４０６は、標準時刻配信システム１１０から配信された標準時刻情報と当該標準時刻情報と対をなす乱数情報を受信する。復号部４０７は、タイムスタンプ情報受信部４０５が前記タイムスタンプ情報を受信すると、タイムスタンプ装置１４０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情報を復号する。判定部４０８は、復号されたタイムスタンプ情報に含まれるタイムスタンプが示す時刻情報および当該時刻情報と対をなす乱数情報と、標準時刻情報受信部４０６が受信した標準時刻情報および当該標準時刻情報と対をなす乱数情報とを比較し、タイムスタンプが示す時

刻情報が改ざんまたは故意に遅延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情報および乱数情報が、標準時刻情報受信部４０６が受信した標準時刻情報および乱数情報といずれも一致すれば、時刻認証局における時刻の改ざんまたは故意による遅延がないと判断できる。このようにして、検証対象であるタイムスタンプが示す時刻情報の正当性が検証される。また、公開鍵証明書データ発行部７０２は、タイムスタンプ装置１４０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。

【００５１】

（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。

【００５２】

図８のフローチャートにおいて、まず、データ入力を行う（ステップＳ８０１）。ここでは、ユーザがタイムスタンプ利用者用装置１５０の入力部４０２から作成しようとする文書データなどの入力を行う。

【００５３】

次に、入力データの暗号化を行う（ステップＳ８０２）。ここでは、ステップＳ８０１で入力されたデータをタイムスタンプ利用者用装置１５０の暗号化部７０１がタイムスタンプ利用者の秘密鍵で暗号化する。この暗号化された入力データは、通信制御部４０１を介して、タイムスタンプ装置１４０へ送信される。

【００５４】

次に、入力データを取得する（ステップＳ８０３）。具体的には、タイムスタンプ装置１４０のデータ取得部６０１が、ステップＳ８０２で暗号化された入力データを取得する。

【００５５】

そして、入力データを復号する（ステップＳ８０４）。ここでは、タイムスタンプ装置１４０の復号部６０２が、ステップＳ８０３で入力データを取得すると、タイムスタンプ利用者用装置１５０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入力データを復号する。

【００５６】

次に、ハッシュ値を生成する（ステップＳ８０５）。この処理は、ステップＳ８０４で復号されたデータからタイムスタンプ装置１４０のハッシュ値生成部６０３がハッシュ値を生成する。

【００５７】

標準時刻情報の配信要求を発行する（ステップＳ８０６）。具体的には、タイムスタンプ装置１４０の時刻情報配信要求発行部３０３が、標準時刻配信システム１１０へ時刻情報の配信要求を発行する。

【００５８】

次に、標準時刻情報を生成する（ステップＳ８０７）。標準時刻配信システム１１０の標準時刻情報生成部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、標準時刻情報を生成する。

【００５９】

同時に、乱数情報を発生する（ステップＳ８０８）。具体的には、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、標準時刻配信システム１１０の乱数情報発生部２０４が乱数情報を発生する。

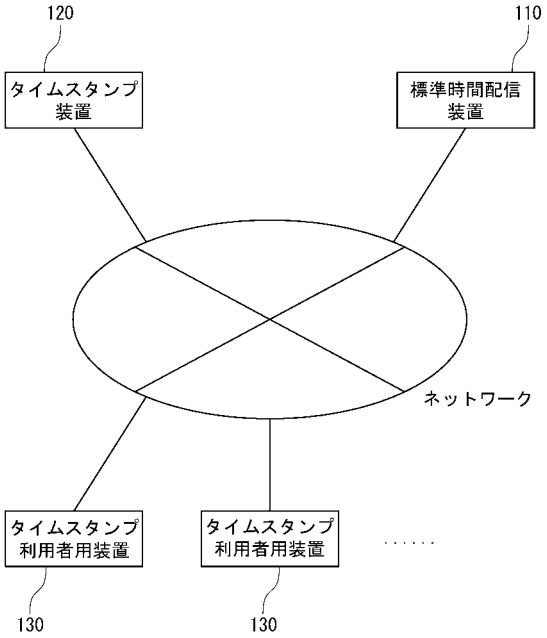
【００６０】

次に、標準時刻情報を配信する（ステップＳ８０９）。ここでは、標準時刻配信システム１１０の情報配信部２０５が、ステップＳ８０７で生成された標準時刻情報とステップＳ８０８で発生された乱数情報とを対としてタイムスタンプ装置１４０およびタイムスタンプ利用者用装置１５０へ配信する。

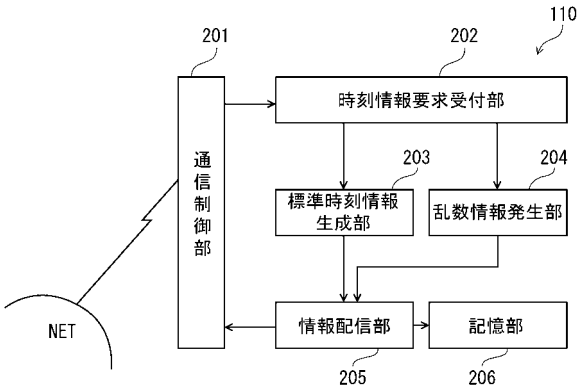
【００６１】
次に、タイムスタンプ情報を生成する（ステップＳ８１０）。ここでは、タイムスタンプ装置１４０のタイムスタンプ情報生成部３０５が、ハッシュ値生成部６０３が生成したハッシュ値と、時刻情報受信部３０４が受信した標準時刻情報および当該標準時刻情報と対をなす乱数情報とを用い、時刻認証局の秘密鍵で暗号化することによりタイムスタンプ情報を生成する。
【００６２】
標準時刻情報を受信する（ステップＳ８１１）。ここでは、タイムスタンプ利用者用装置１５０の標準時刻情報受信部４０６が、ステップＳ８０９で配信された標準時刻情報と当該標準時刻情報と対をなす乱数情報を受信する。
【００６３】
次に、タイムスタンプ情報を受信する（ステップＳ８１２）。ここでは、タイムスタンプ利用者用装置１５０のタイムスタンプ情報受信部４０５が、ステップＳ８１０で生成されたタイムスタンプ情報を受信する。
【００６４】
続いて、タイムスタンプ情報を復号する（ステップＳ８１３）。具体的には、タイムスタンプ利用者用装置１５０の復号部４０７が、タイムスタンプ装置１４０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ステップＳ８１２で受信したタイムスタンプ情報を復号する。
【００６５】
そして、タイムスタンプの真偽を判定する（ステップＳ８１４）。ここでは、タイムスタンプ利用者用装置１５０の判定部４０８が、ステップＳ８１１で取得した標準時刻配信システム１１０から配信された標準時刻情報と当該標準時刻情報と対をなす乱数情報と、ステップＳ８１３で復号されたタイムスタンプ情報に含まれるタイムスタンプが示す時刻情報および当該時刻情報と対をなす乱数情報とを比較し、タイムスタンプの示す時刻が改ざんまたは故意による遅延がなされているか否かを判定する。この処理では、時刻情報の他、当該時刻情報と対をなしている乱数情報をも比較することで、タイムスタンプの示す時刻が、標準時刻配信システム１１０が発行した真の時刻情報どおりであるか否かが判明する。
【００６６】
以上のように、実施の形態２にかかる時刻認証システムにおいても、検証の対象を、時刻情報のみではなく、時刻情報と対をなしている乱数情報にまで拡大していることで、より精度の高い検証が可能になる点ついては、実施の形態１と同様である。ただ、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１５０における処理の負荷を軽減することができる。
【００６７】
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容易に防止することができる。
【００６８】
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ー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ーで読み取り可能な記録媒体に記録され、コンピューター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】
【００６９】
以上のように、本発明にかかる標準時刻配信システム、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。

【図面の簡単な説明】
【００７０】
【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システム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７】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。
【符号の説明】
【００７１】
１１０　標準時刻配信システム
１２０，１４０　タイムスタンプ装置
１３０，１５０　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　標準時刻情報生成部
２０４　乱数情報発生部
２０５　情報配信部
２０６，４０４　記憶部
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　タイムスタンプ情報生成部
３０６，７０２　公開鍵証明書データ発行部
４０２　入力部
４０３，６０３　ハッシュ値生成部
４０５　タイムスタンプ情報受信部
４０６　標準時刻情報受信部
４０７，６０２　復号部
４０８　判定部
６０１　データ取得部
７０１　暗号化部

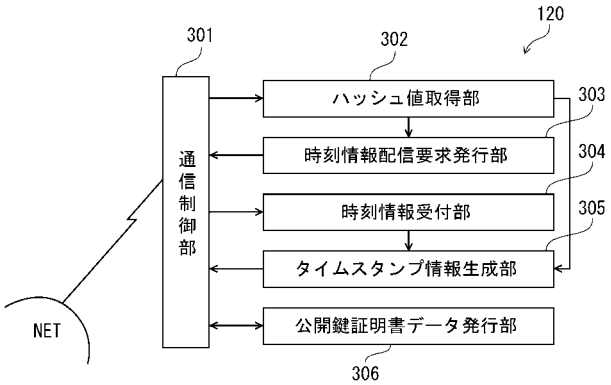
【図１】


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

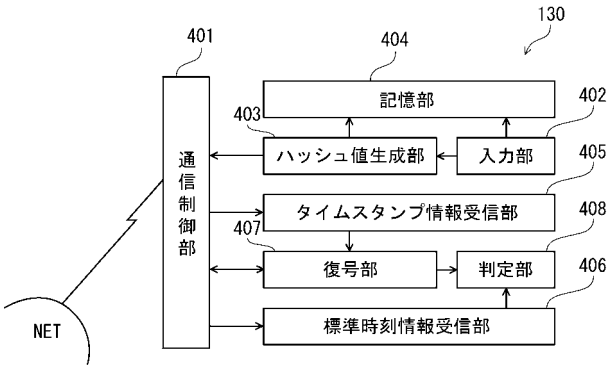
【図２】


110
201
202
通信制御部
時刻情報要求受付部
203
204
標準時刻情報生成部
乱数情報発生部
NET
情報配信部
記憶部
205
206

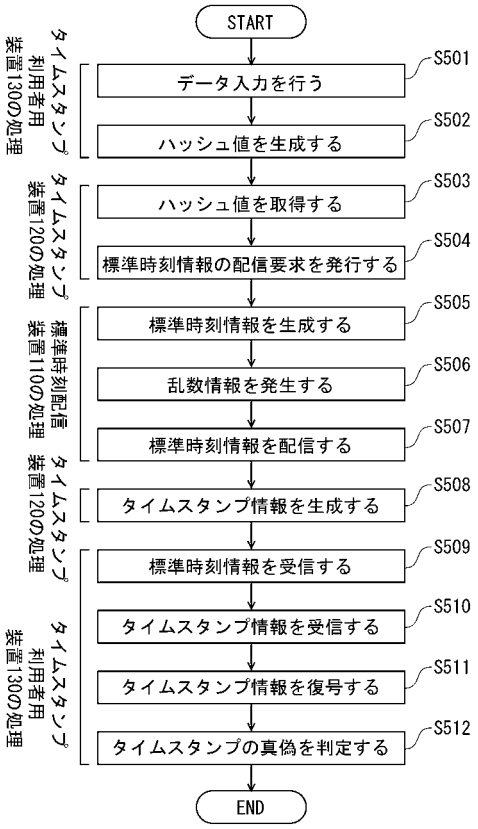
【図３】


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
304
時刻情報受付部
305
タイムスタンプ情報生成部
NET
公開鍵証明書データ発行部
306

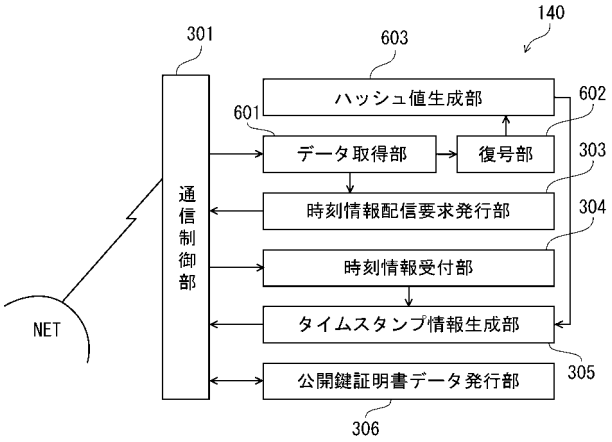
【図４】


130
401
404
通信制御部
記憶部
402
403
ハッシュ値生成部
入力部
405
タイムスタンプ情報受信部
408
407
復号部
判定部
406
NET
標準時刻情報受信部

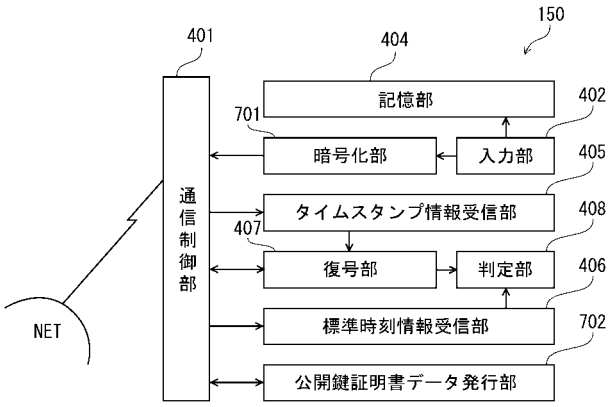
【図５】


START
タイムスタンプ利用者用装置130の処理
データ入力を行う
S501
ハッシュ値を生成する
S502
タイムスタンプ装置120の処理
ハッシュ値を取得する
S503
標準時刻情報の配信要求を発行する
S504
標準時刻配信装置110の処理
標準時刻情報を生成する
S505
乱数情報を発生する
S506
標準時刻情報を配信する
S507
タイムスタンプ装置120の処理
タイムスタンプ情報を生成する
S508
タイムスタンプ利用者用装置130の処理
標準時刻情報を受信する
S509
タイムスタンプ情報を受信する
S510
タイムスタンプ情報を復号する
S511
タイムスタンプの真偽を判定する
S512
END

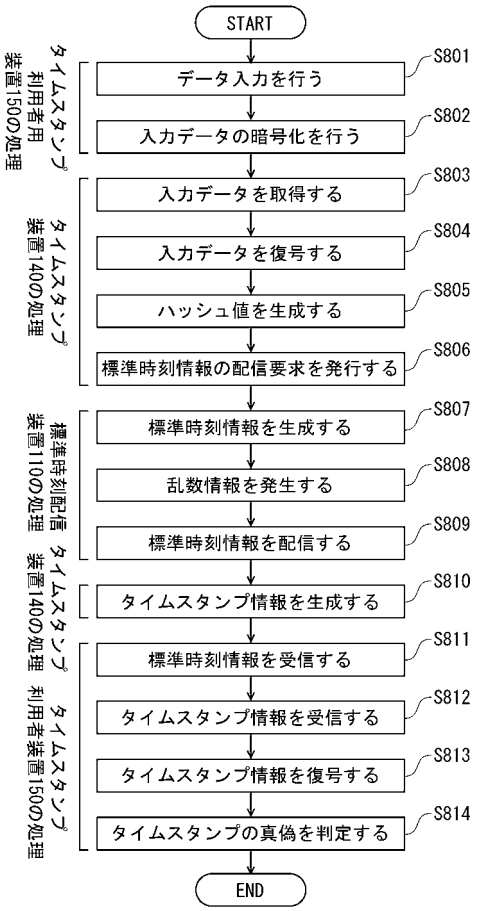
【図６】


140
301
603
ハッシュ値生成部
602
601
データ取得部
復号部
303
時刻情報配信要求発行部
304
時刻情報受付部
タイムスタンプ情報生成部
通信制御部
NET
公開鍵証明書データ発行部
305
306

【図７】


150
401
404
記憶部
402
701
暗号化部
入力部
405
タイムスタンプ情報受信部
408
407
復号部
判定部
406
通信制御部
NET
標準時刻情報受信部
702
公開鍵証明書データ発行部

【図８】


START
タイムスタンプ利用者用装置150の処理
データ入力を行う
S801
入力データの暗号化を行う
S802
タイムスタンプ装置140の処理
入力データを取得する
S803
入力データを復号する
S804
ハッシュ値を生成する
S805
標準時刻情報の配信要求を発行する
S806
標準時刻配信装置110の処理
標準時刻情報を生成する
S807
乱数情報を発生する
S808
標準時刻情報を配信する
S809
タイムスタンプ装置140の処理
タイムスタンプ情報を生成する
S810
タイムスタンプ利用者装置150の処理
標準時刻情報を受信する
S811
タイムスタンプ情報を受信する
S812
タイムスタンプ情報を復号する
S813
タイムスタンプの真偽を判定する
S814
END