(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2006-236251
(P2006-236251A)
(43)公開日　平成18年9月7日(2006.9.7)

(51)Int.Cl.			F I			テーマコード（参考）
G06F	1/14	(2006.01)	G06F	1/04	351A	2F002
G04G	5/00	(2006.01)	G04G	5/00	J	

審査請求 未請求　請求項の数 10　ＯＬ　（全 26 頁）

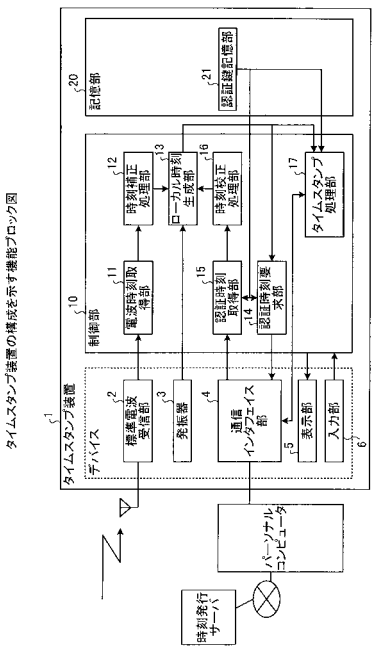
(21)出願番号　特願2005-53592(P2005-53592)
(22)出願日　平成17年2月28日(2005.2.28)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(71)出願人　000001960
シチズン時計株式会社
東京都西東京市田無町六丁目１番１２号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　川島　健信
東京都西東京市田無町六丁目１番１２号
シチズン時計株式会社内

Ｆターム(参考)　2F002 AA12　FA16

(54)【発明の名称】タイムスタンプ装置、時刻校正方法および時刻校正プログラム

(57)【要約】
【課題】タイムスタンプ装置が提供する時刻の信頼性を保証すること。
【解決手段】ローカル時刻生成部が生成したローカル時刻を、電波時刻取得部が取得した電波時刻を用いて補正するとともに、認証時刻取得部が時刻発行装置から取得した認証時刻を用いて校正することとし、認証時刻要求部は、ローカル時刻と電波時刻とのずれが所定値より小さい場合の回数と、所定値以上である場合の回数とが所定値を上回ったことをトリガーとして認証時刻を取得し、時刻校正処理部は、取得した認証時刻の遅延時間を考慮したうえでローカル時刻の校正をおこなう。
【選択図】　図４



【特許請求の範囲】
【請求項１】
内部時計が出力するローカル時刻に基づいて該ローカル時刻を含んだ電子署名をおこなうタイムスタンプ装置であって、
標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得手段と、
前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得手段と、
前記電波時刻取得手段により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正手段と、
前記認証時刻取得手段により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正手段と
を備えたことを特徴とするタイムスタンプ装置。
【請求項２】
前記認証時刻取得手段は、
前記時刻補正手段が算出した前記差分の絶対値が前記第一の閾値よりも小さい回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正手段は、
該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする請求項１に記載のタイムスタンプ装置。
【請求項３】
前記認証時刻取得手段は、
前記時刻補正手段が算出した前記差分の絶対値が前記第一の閾値以上である回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正手段は、
該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする請求項１または２に記載のタイムスタンプ装置。
【請求項４】
前記認証時刻取得手段は、
定期的に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正手段は、
該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする請求項１に記載のタイムスタンプ装置。
【請求項５】
前記認証時刻取得手段は、
所定の操作がおこなわれた場合に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正手段は、
該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする請求項１に記載のタイムスタンプ装置。
【請求項６】
前記時刻校正手段は、
前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値よりも小さい場合に、該認証時刻を該ローカル時刻として設定することを特徴とする請求項１～５のいずれか一つに記載のタイムスタンプ装置。
【請求項７】
前記時刻校正手段は、
前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値以上である場合に、該ローカル時刻の校正をおこなわないことを特徴とする

請求項１～６のいずれか一つに記載のタイムスタンプ装置。
【請求項８】
前記時刻校正手段は、
前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値以上である回数が所定数連続した場合に、前記電子署名への前記ローカル時刻の付加を中止し、警報を出力することを特徴とする請求項１～７のいずれか一つに記載のタイムスタンプ装置。
【請求項９】
内部時計が出力するローカル時刻と標準時刻とのずれを校正する時刻校正方法であって、
前記標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得工程と、
前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得工程と、
前記電波時刻取得工程により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正工程と、
前記認証時刻取得工程により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正工程と
を含んだことを特徴とする時刻校正方法。
【請求項１０】
内部時計が出力するローカル時刻と標準時刻とのずれを校正する時刻校正プログラムであって、
前記標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得手順と、
前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得手順と、
前記電波時刻取得手順により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正手順と、
前記認証時刻取得手順により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正手順と
をコンピュータに実行させることを特徴とする時刻校正プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、内部時計が出力するローカル時刻に基づいて該ローカル時刻を含んだ電子署名をおこなうタイムスタンプ装置、時刻校正方法および時刻校正プログラムに関し、特に、悪意の利用者による時刻改ざんを防止することにより電子署名に用いられる時刻の信頼性を高めるとともに、ネットワークに常時接続しない場合であっても時刻の信頼性を保証することができるタイムスタンプ装置、時刻校正方法および時刻校正プログラムに関するものである。
【背景技術】
【０００２】
近年、電子認証技術の進展にともない、電子文書の作成者や発行者を証明する電子署名が用いられるようになってきている。この電子署名には暗号鍵などの技術が用いられており電子署名の信頼性を担保している。また、かかる電子署名に国家標準時刻（以下、「標準時刻」と呼ぶ。）を含めることにより、電子文書の作成時刻や送信時刻を証明しようと

いう試みもおこなわれている。
【０００３】
時刻を含んだ電子署名をおこなう装置は、一般的にタイムスタンプ装置と呼ばれる。このタイムスタンプ装置は内部時計を有しており、内部時計によりローカル時刻を計時するとともに、標準時刻を含んだ電波を受信するなどしてローカル時刻を補正することで電子署名に用いる時刻の精度を向上させている。
【０００４】
このように、時刻を含んだ電子署名をおこなう場合には、タイムスタンプ装置のローカル時刻と標準時刻とのずれを所定値以下に抑える必要がある。すなわち、電子署名に含まれる時刻と標準時刻とのずれが所定値以下であることを保証できれば、ローカル時刻を含んだ電子署名により、署名対象となる電子文書に関する時刻を証明できることになる。
【０００５】
なお、かかるローカル時刻と標準時刻とのずれを所定値以下に抑える方法としては、上記した、いわゆる電波時計と同様の方法の他に、ネットワーク接続された標準時刻管理サーバに接続してこのサーバから標準時刻を得る方法もある。たとえば、特許文献１には、標準時刻を管理するサーバが、常時このサーバと通信できるクライアント装置に対して標準時刻を送信するとともに、送信した標準時刻に保証期間を設けることで、クライアント装置の内部時計の狂いや改ざんを検出する方法が開示されている。
【０００６】
【特許文献１】特開２００２－２２９８６９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、上記した従来のタイムスタンプ装置では、悪意の利用者によるローカル時刻の改ざんを防止することができない。たとえば、真の標準時刻を含んだ電波のかわりに偽の標準時刻を含んだ電波を用いることで、タイムスタンプ装置のローカル時刻を真の標準時刻から大きくずらすことが可能となる。このようなローカル時刻の改ざんがおこなわれると、電子文書に関する時刻を証明できないことになってしまう。
【０００８】
たとえ、タイムスタンプ装置のローカル時刻と、電波に含まれる標準時刻とのずれを監視し、このずれが所定値を超えた場合に改ざんがおこなわれたと判定する仕組みを設けたとしても、タイムスタンプ装置を加熱または冷却する温度攻撃と、偽の電波による電波攻撃とが併用された場合には、かかる仕組みは機能せずローカル時刻の改ざんを許す結果となる。
【０００９】
また、各種デバイスの小型化によりタイムスタンプ装置自体も小型化することが可能となってきており、ＬＡＮなどのネットワークに常時接続しておくのではなく、腕時計や携帯電話のように利用者が手軽に持ち運んで必要なときに使用される形態が想定され、このような使用形態を望むユーザニーズが予想される。
【００１０】
なお、特許文献１に開示されている技術は、標準時刻管理サーバと常に通信できるように、ＬＡＮなどのネットワークに常時接続されているクライアント装置に関するものであり、上記したような使用形態のタイムスタンプ装置には適用することができない。
【００１１】
これらのことから、悪意の利用者による時刻改ざんを防止することにより電子署名に用いられる時刻の信頼性を高めるとともに、ネットワークに常時接続しておく必要のないタイムスタンプ装置をいかにして実現するかが大きな課題となっている。
【００１２】
この発明は、上述した従来技術による問題点を解消するためになされたものであり、悪意の利用者による時刻改ざんを防止することにより電子署名に用いられる時刻の信頼性を

高めるとともに、ネットワークに常時接続しない場合であっても時刻の信頼性を保証することができるタイムスタンプ装置、時刻校正方法および時刻校正プログラム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】

【００１３】

上述した課題を解決し、目的を達成するため本発明は、内部時計が出力するローカル時刻に基づいて該ローカル時刻を含んだ電子署名をおこなうタイムスタンプ装置であって、標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得手段と、前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得手段と、前記電波時刻取得手段により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正手段と、前記認証時刻取得手段により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正手段とを備えたことを特徴とする。

【００１４】

また、本発明は、前記認証時刻取得手段は、前記時刻補正手段が算出した前記差分の絶対値が前記第一の閾値よりも小さい回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、前記時刻校正手段は、該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする。

【００１５】

また、本発明は、前記認証時刻取得手段は、前記時刻補正手段が算出した前記差分の絶対値が前記第一の閾値以上である回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、前記時刻校正手段は、該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする。

【００１６】

また、本発明は、前記認証時刻取得手段は、定期的に、前記時刻発行装置から前記認証時刻を取得し、前記時刻校正手段は、該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする。

【００１７】

また、本発明は、前記認証時刻取得手段は、所定の操作がおこなわれた場合に、前記時刻発行装置から前記認証時刻を取得し、前記時刻校正手段は、該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする。

【００１８】

また、本発明は、前記時刻校正手段は、前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値よりも小さい場合に、該認証時刻を該ローカル時刻として設定することを特徴とする。

【００１９】

また、本発明は、前記時刻校正手段は、前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値以上である場合に、該ローカル時刻の校正をおこなわないことを特徴とする。

【００２０】

また、本発明は、前記時刻校正手段は、前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値以上である回数が所定数連続した場合に、前記電子署名への前記ローカル時刻の付加を中止し、警報を出力することを特徴とする。

【００２１】

また、本発明は、内部時計が出力するローカル時刻と標準時刻とのずれを校正する時刻校正方法であって、前記標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得工程と、前記標準時刻と同期した認証時刻を発行する時刻

発行装置から該認証時刻を取得する認証時刻取得工程と、前記電波時刻取得工程により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正工程と、前記認証時刻取得工程により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正工程とを含んだことを特徴とする。

【００２２】

また、本発明は、内部時計が出力するローカル時刻と標準時刻とのずれを校正する時刻校正プログラムであって、前記標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得手順と、前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得手順と、前記電波時刻取得手順により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正手順と、前記認証時刻取得手順により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正手順とをコンピュータに実行させることを特徴とする。

【発明の効果】

【００２３】

本発明によれば、標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得し、標準時刻と同期した認証時刻を発行する時刻発行装置から認証時刻を取得し、取得された電波時刻とローカル時刻との差分の絶対値を算出し、差分の絶対値が第一の閾値よりも小さい場合に電波時刻をローカル時刻として設定する補正をおこない、差分の絶対値が第一の閾値以上である場合にローカル時刻の補正をおこなわないこととし、取得された認証時刻に基づいてローカル時刻の校正をおこなうよう構成したので、電波時刻および認証時刻を用いてローカル時刻の調整をおこなうことにより、悪意の利用者による時刻改ざんを防止して電子署名に用いられる時刻の信頼性を高めるとともに、ネットワークに常時接続しない場合であっても時刻の信頼性を保証することができるという効果を奏する。

【００２４】

また、本発明によれば、認証時刻取得手段は、時刻補正手段が算出した差分の絶対値が第一の閾値よりも小さい回数が所定数連続した場合に、時刻発行装置から認証時刻を取得し、時刻校正手段は、認証時刻取得手段が取得した認証時刻をローカル時刻として設定するよう構成したので、ネットワークに常時接続しない場合であっても時刻の信頼性を保証することができるという効果を奏する。

【００２５】

また、本発明によれば、認証時刻取得手段は、時刻補正手段が算出した差分の絶対値が第一の閾値以上である回数が所定数連続した場合に、時刻発行装置から認証時刻を取得し、時刻校正手段は、認証時刻取得手段が取得した認証時刻をローカル時刻として設定するよう構成したので、悪意の利用者による時刻改ざんを防止して電子署名に用いられる時刻の信頼性を高めることができるという効果を奏する。

【００２６】

また、本発明によれば、認証時刻取得手段は、定期的に、時刻発行装置から認証時刻を取得し、時刻校正手段は、認証時刻取得手段が取得した認証時刻をローカル時刻として設定するよう構成したので、悪意の利用者による時刻改ざんを防止して電子署名に用いられる時刻の信頼性を高めるとともに、ネットワークに常時接続しない場合であっても時刻の信頼性を保証することができるという効果を奏する。

【００２７】

また、本発明によれば、認証時刻取得手段は、所定の操作がおこなわれた場合に、時刻発行装置から前記認証時刻を取得し、時刻校正手段は、認証時刻取得手段が取得した認証

時刻をローカル時刻として設定するよう構成したので、悪意の利用者による時刻改ざんを防止して電子署名に用いられる時刻の信頼性を高めるとともに、ネットワークに常時接続しない場合であっても時刻の信頼性を保証することができるという効果を奏する。

【００２８】

また、本発明によれば、時刻校正手段は、認証時刻取得手段が取得した認証時刻と、ローカル時刻との差分の絶対値が第二の閾値よりも小さい場合に、該認証時刻をローカル時刻として設定するよう構成したので、ネットワークを遅延させる不正行為を効果的に検出することができるという効果を奏する。

【００２９】

また、本発明によれば、時刻校正手段は、認証時刻取得手段が取得した認証時刻と、ローカル時刻との差分の絶対値が第二の閾値以上である場合に、ローカル時刻の校正をおこなわないよう構成したので、ネットワークを遅延させる不正行為の影響を含んだ認証時刻を取り込むことを防止することができるという効果を奏する。

【００３０】

また、本発明によれば、時刻校正手段は、認証時刻取得手段が取得した認証時刻と、ローカル時刻との差分の絶対値が第二の閾値以上である回数が所定数連続した場合に、電子署名へのローカル時刻の付加を中止し、警報を出力するよう構成したので、ネットワークを遅延させる不正行為の影響を排除してローカル時刻の信頼性を保証することができるという効果を奏する。

【発明を実施するための最良の形態】

【００３１】

以下に添付図面を参照して、この発明に係るタイムスタンプ装置、時刻校正方法および時刻校正プログラムの好適な実施例を詳細に説明する。なお、以下の実施例においては、本発明に係る時刻校正処理をタイムスタンプ装置に適用した場合について説明する。また、本実施例によりこの発明が限定されるものではない。

【実施例】

【００３２】

まず、本実施例の特徴部分である時刻校正処理を適用するタイムスタンプ装置について図１～図３－３および図１２～図１４を用いて説明する。なお、図１～図３－３が本実施例に係るタイムスタンプ装置に関する図であり、図１２～図１４が従来のタイムスタンプ装置に関する図である。

【００３３】

最初に、従来のタイムスタンプ装置の概要について図１２を用いて説明する。図１２は、従来のタイムスタンプ装置の概要を示す図である。ここで、タイムスタンプ装置とは、電子文書などの電子データに対して時刻を含んだ電子署名をおこなう装置のことである。近年、ネットワークを介して電子データをやりとりすることは一般的におこなわれており、かかる電子データの作成時刻や送信時刻などを証明するビジネス（いわゆる「タイムビジネス」）も本格化しつつある。

【００３４】

たとえば、カルテや死亡診断書などの医療関係の電子書類、売上伝票や領収書などの経理・税金関係の電子書類といった文書データのほか、画像データや映像データなどにタイムスタンプ装置を用いた電子署名が付加されていれば、これらの電子データが作成された日時や送信された日時を証明することが可能となる。また、デジタルカメラやデジタルビデオカメラなどの装置にタイムスタンプ装置を内蔵させることにより、日付や時刻の記録が必要な分野にもタイムビジネスの適用範囲を広げることができる。

【００３５】

このようなタイムビジネスを構築するにあたっては、電子署名に含まれる時刻の管理が非常に重要である。すなわち、単に時刻の正確性のみを追求するのではなく、悪意をもった利用者などによる時刻の改変を許さない仕組みづくりが必要となる。たとえば、医療事故を隠蔽するためにカルテに付加された時刻を改変したり、特許の発明日を改変したりす

る悪意の利用者が想定されるので、これらの利用者による時刻の改変を防止する必要がある。

【００３６】

ところで、かかるタイムビジネスの一形態として、信頼のおける時刻を発行する施設や装置と、これらの施設や装置が発行する時刻を受信する多数のタイムスタンプ装置との間で時刻を同期させることがおこなわれる。なお、信頼のおける時刻を発行する施設や装置としては、標準時刻を含んだ電波を発信する標準電波送信所や衛星、インタネットなどに接続され認証鍵の提示により標準時刻を提供する時刻発行サーバなどがある。

【００３７】

タイムビジネスを展開するためにタイムスタンプ装置を製造・販売する企業は、販売したタイムスタンプ装置がおこなう時刻付き電子署名の「時刻」と、標準時刻とのずれが所定値以下であることを保証しなければならない。このような時刻保証をおこなうことで、タイムビジネスが成立することになる。

【００３８】

しかし、タイムスタンプ装置の流通過程に介在する人や購入する人のなかには、タイムスタンプ装置の時刻を改変し、偽の時刻を含んだ電子署名をおこなう悪意の利用者が存在することが予想される。このような時刻の改変を許してしまうと、時刻保証をおこなうことができないので、タイムビジネスそのものが成立しなくなってしまう。

【００３９】

図１２に示した従来のタイムスタンプ装置は、装置内部に内部時計を有しており、この内部時計が刻む時刻を、標準電波送信所から送信される標準電波に含まれた電波時刻（T_W）により補正するものである。そして、補正した内部時計を用いて時刻を含んだ署名処理をおこなう。このタイムスタンプ装置は、いわゆる「電波時計」の機能をタイムスタンプ装置にもたせたものであり、善意の利用者が使用するかぎりは時刻の正確性が担保される。

【００４０】

しかし、上記した従来のタイムスタンプ装置は、いったん悪意の利用者の手に渡ってしまうと時刻の改変を許してしまうことになる。ここで、かかる時刻の改変について図１３を用いて説明する。図１３は、従来のタイムスタンプ装置の内部時刻の改変を示す図である。

【００４１】

図１３に示すように、悪意の利用者は、タイムスタンプ装置を地下室のような標準電波が届かない場所に持ってゆき、標準電波と同形式の電波（偽電波）を用いて標準時刻からずれた時刻を発信する。この偽電波を受信したタイムスタンプ装置は、この偽電波に基づいて内部時計が刻むローカル時刻を補正するので、ローカル時刻は真の時刻からずれていくことになる。

【００４２】

電波時刻を用いた補正をおこなうタイムスタンプ装置では、このような不正行為を防止するために、ローカル時刻と電波時刻との差分が所定値（ε）を上回った場合には、電波時刻を用いた補正を中止してローカル時刻をそのまま用いる防止策を講じている場合も多い。しかし、このような偽電波と連動する温度操作をおこなわれると、かかる防止策は機能しないこととなってしまう。

【００４３】

一般的に、内部時計を有する装置には、水晶発振器（crystal Oscillator）や、水晶発振器に温度補償回路を付加して温度変化に対する安定化を図ったＴＣＸＯ(Temperature Compensated Xtal Oscillator)が用いられる。特に、流通段階や使用場所などが多岐にわたるタイムスタンプ装置にはＴＣＸＯが適している。これらの発振器は、縦軸に誤差（上方向が正）を横軸に温度変化をとった場合に、概ね上に凸の二次曲線の形状となる温度特性を有している。

【００４４】

したがって、これらの発振器を含んだタイムスタンプ装置を、加熱しても冷却しても内部時計は遅れていくことになる。ＴＣＸＯの場合には、温度補償回路が動作する温度範囲内においては誤差が０付近となるような制御がおこなわれるが、かかる温度範囲を超えると急激に時刻の遅れをもたらす誤差を生じるようになる。

【００４５】

このような温度攻撃を偽電波による攻撃と連動させると、ローカル時刻と電波時刻（偽電波による電波時刻）との差分を所定値（ε）以内に抑えることが可能となるため、ローカル時刻を、標準時刻から大きくずらしていくこと（以下、「不正行為によるドリフト」と呼ぶ。）を許してしまう結果となる。ここで、この不正行為によるドリフトについて図１４を用いて説明しておく。図１４は、従来のタイムスタンプ装置における不正行為によるドリフトを示す図である。

【００４６】

図１４に示すように、不正行為がおこなわれていない場合には、ローカル時刻と標準時刻（真の時刻）との誤差は、上述したように、所定値（ε）を閾値とした防止策により、－ε～＋εの範囲に抑えられる。一方、温度攻撃と偽電波による攻撃とを連動させた場合には、ローカル時刻と偽電波に含まれる時刻との誤差は－ε～＋εの範囲に抑えられたまま、ローカル時刻は真の時刻から大きくずれていくことになる。

【００４７】

このように、従来のタイムスタンプ装置では、悪意の利用者による時刻改ざんに対する防止策が十分ではなく、タイムスタンプ装置の目的である時刻証明あるいは時刻保証を担保することができなかった。そこで、本発明に係る時刻校正処理を備えたタイムスタンプ装置では、このような時刻改ざんを防止するための仕組みを提供することとした。

【００４８】

次に、本実施例に係るタイムスタンプ装置の概要について図１を用いて説明する。図１は、本実施例に係るタイムスタンプ装置の概要を示す図である。同図に示すように、本実施例に係るタイムスタンプ装置では、上記した電波時刻の取得に加え、時刻発行サーバからネットワークを介して認証時刻（T_N）を取得することとし、この認証時刻を用いて内部時計が刻むローカル時刻の校正をおこなうこととした。

【００４９】

ここで、時刻発行サーバとは、認証鍵が提示された場合にかかるサーバが管理している標準時刻を提供する装置であり、インタネットなどのネットワークに接続されネットワークを介して信頼性の高い標準時刻を提供するものである。なお、本実施例では、タイムスタンプ装置がかかる時刻発行サーバから標準時刻（T_N）を取得する場合について説明するが、標準時刻発行機能を備えないサーバに、標準時刻を発行する時刻発行装置を接続することとし、かかるサーバを介して標準時刻（T_N）を取得することとしてもよく、ネットワークに直接接続された時刻発行装置から標準時刻（T_N）を取得することとしてもよい。

【００５０】

次に、かかる認証時刻を用いた時刻校正について図２を用いてさらに詳細に説明する。図２は、時刻校正の概要を示す図である。なお、図２は、従来のタイムスタンプ装置に関する図１４に対応する図である。また、同図におけるT_N'は、タイムスタンプ装置のローカル時刻をあらわしている。

【００５１】

図２に示すように、本実施例に係るタイムスタンプ装置では、時刻保証のための閾値(σ)を設定し、ローカル時刻と真の時刻とのずれが、かかる閾値（σ）の範囲内になるような制御をおこなう。そして、所定の条件を満たした場合に、時刻発行サーバから取得した認証時刻（T_N）をローカル時刻（T_N'）に設定する校正をおこなうことで、ローカル時刻と標準時刻とのずれを閾値（σ）の範囲内に抑える制御をおこなう。なお、かかる制御の詳細については、後述することとする。

【００５２】

上述した時刻校正をおこなうことにより、従来のタイムスタンプ装置では対処できなかった温度と偽電波とによる連動攻撃がおこなわれた場合であっても、ローカル時刻のずれを所定値（σ）以内に抑えることができるので、タイムスタンプにおける時刻を保証することが可能となる。

【００５３】

このように、本実施例に係るタイムスタンプ装置では、善意の利用者に対しては電波時計と同程度の精度でタイムスタンプを提供することができ、たとえ悪意の利用者の手に渡った場合であっても時刻誤差が所定値（σ）以下の時刻精度を保証することができる。また、本実施例に係るタイムスタンプ装置は、基本的には標準電波に従った計時処理をおこない、不正行為による誤差が蓄積した段階で認証時刻（T_N）を取得して校正をおこなうので、ネットワークに常時接続しておく必要はない。

【００５４】

次に、本実施例に係るタイムスタンプ装置の構成例について図３－１～図３－３を用いて説明する。なお、これらの構成例においては、タイムスタンプ装置は携帯可能なものを想定しているが据え置き型とすることもできる。

【００５５】

図３－１は、タイムスタンプ装置の構成例１を示す図である。図３－１に示す構成では、タイムスタンプ装置は、インタネットに接続されたパーソナルコンピュータのＵＳＢ（Universal Serial Bus）ポートなどに接続して用いられる。そして、署名対象となる電子文書をパーソナルコンピュータから受け取り、タイムスタンプ装置のローカル時刻（T_N'）および認証鍵を用いて時刻を含んだ電子署名を付加したうえで、署名済の電子文書をパーソナルコンピュータに渡す。

【００５６】

また、このタイムスタンプ装置が時刻校正をおこなう際には、パーソナルコンピュータおよびインタネットを介して時刻発行サーバに接続し、認証時刻（T_N）を取得する。なお、かかるタイムスタンプ装置については、腕時計や携帯電話のように利用者が手軽に持ち運んで必要なときに用いられる利用形態を想定している。

【００５７】

図３－２は、タイムスタンプ装置の構成例２を示す図である。図３－２に示す構成例では、図３－１と同様にインタネットに接続されたパーソナルコンピュータのＵＳＢポートなどに接続して用いられる。図３－１の場合と異なるのは、電子署名の機能はパーソナルコンピュータに搭載されるプログラムが有している点にある。

【００５８】

この構成例においては、電子署名が必要な場合には、パーソナルコンピュータはＵＳＢポートなどを介してタイムスタンプ装置に認証要求メッセージを送信する。このメッセージを受け取ったタイムスタンプ装置は、ローカル時刻と認証鍵とをパーソナルコンピュータに返信する。そして、パーソナルコンピュータは自身が有する署名機能により認証対象文書に電子署名を付加する。

【００５９】

なお、このタイムスタンプ装置が時刻校正をおこなう際には、パーソナルコンピュータおよびインタネットを介して時刻発行サーバに接続し、認証時刻（T_N）を取得する点、および、腕時計や携帯電話のように利用者が手軽に持ち運んで必要なときに用いられる利用形態を想定している点については図３－１の場合と同様である。

【００６０】

図３－３は、タイムスタンプ装置の構成例３を示す図である。図３－３に示す構成例では、タイムスタンプ装置は直接インタネットなどのネットワークに接続される。そして、署名対象となる電子文書を受け取ると、ローカル時刻（T_N'）および認証鍵を用いて電子署名を付加したうえで署名済の電子文書を出力する。なお、同図においては、タイムスタンプ装置が外部から署名対象文書を受け取る場合について図示しているが、タイムスタンプ装置が署名対象文書を内部のメモリなどに保持しておく構成としてもよい。

【００６１】
また、このタイムスタンプ装置が時刻校正をおこなう際には、パーソナルコンピュータおよびインタネットを介して時刻発行サーバに接続し、認証時刻（T_N）を取得する。なお、かかるタイムスタンプ装置については、腕時計や携帯電話のように利用者が手軽に持ち運んで必要なときに用いられる利用形態を想定している点は、図３－１や図３－２と同様である。
【００６２】
なお、図３－１～図３－３に示したタイムスタンプ装置の構成例では、電子署名の対象データを文書データとした場合について示したが、文書データに限らず、画像データや映像データといった電子データを、署名対象データとすることができる。また、デジタルカメラなどの装置にタイムスタンプ装置を内蔵させ、撮像するたびに時刻を含んだ電子署名をおこなうこととしてもよい。
【００６３】
次に、本実施例の特徴部分である時刻校正処理を含んだタイムスタンプ装置１の構成について図４を用いて説明する。図４は、タイムスタンプ装置１の構成を示す機能ブロック図である。なお、図４に示した構成は、タイムスタンプ装置１が図３－１の構成をとった場合について示している。
【００６４】
同図に示すように、タイムスタンプ装置１は、各種デバイスとして標準電波受信部２と、発振器３と、通信インタフェイス部４と、表示部５と、入力部６とを備えており、さらに、制御部１０と、記憶部２０とを備えている。
【００６５】
また、制御部１０は、電波時刻取得部１１と、時刻補正処理部１２と、ローカル時刻生成部１３と、認証時刻要求部１４と、認証時刻取得部１５と、時刻校正処理部１６と、タイムスタンプ処理部１７とをさらに備えており、記憶部２０は、認証鍵記憶部２１をさらに備えている。
【００６６】
標準電波受信部２は、標準電波送信所や衛星から標準電波を受信し、国家標準時刻と同期した電波時刻（T_W）を制御部１０に渡す処理をおこなうデバイスである。たとえば、標準電波送信所から送信される標準電波には、時、分、秒、年初からの通算日、年（西暦下２桁）、曜日などの時刻情報が含まれている。なお、この標準電波受信部２が標準電波を受信するタイミングは任意に指定することが可能であり、７：００と１９：００に受信するなどの指定をおこなうことができるほか、利用者の操作により強制的に受信処理をおこなうこともできる。
【００６７】
発振器３は、水晶発振器などのローカル時刻を計時するためのデバイスであり、発振したパルスを制御部１０に提供する処理をおこなう。タイムスタンプ装置１は、さまざまな温度環境で用いられるうえ、さらに温度攻撃も予想されることから、この発振器３にはＴＣＸＯ（温度補償水晶発振器）のように広い温度範囲で計時精度が安定している発振器を用いることが望ましい。
【００６８】
通信インタフェイス部４は、ＵＳＢポートやＬＡＮボードといった双方向の通信が可能なデバイスであり、タイムスタンプ装置１とパーソナルコンピュータ間でデータの送受信をおこない、これらのデータを制御部１０との間で受け渡しする処理をおこなう。なお、時刻発行サーバとのデータ送受信も、この通信インタフェイス部４を介しておこなわれる。
【００６９】
表示部５は、液晶ディスプレイなどの表示用デバイスであり、制御部１０や各デバイスからの警告情報やエラー情報を表示したり、ローカル時刻を表示したりするために用いられる。また、入力部６は、電源ボタンなどのデバイスであり、タイムスタンプ装置１の電

源ＯＮ／ＯＦＦなどの各種操作に用いられ、操作結果は制御部１０に通知される。

【００７０】

制御部１０は、ローカル時刻を生成するとともに、標準電波を用いた時刻補正および認証時刻を用いた時刻校正を適宜おこなうことにより、ローカル時刻と真の時刻とのずれを所定値以下に抑え、このローカル時刻を用いて電子署名処理をおこなう処理部である。

【００７１】

電波時刻取得部１１は、標準電波受信部２から電波時刻（T_W）を受け取り、時刻補正処理部１２に渡す処理をおこなう処理部である。また、時刻補正処理部１２は、電波時刻取得部１１から受け取った電波時刻（T_W）を用いてローカル時刻生成部１３が生成するローカル時刻（T_N'）を補正する処理をおこなう処理部である。

【００７２】

具体的には、この時刻補正処理部１２は、電波時刻（T_W）とローカル時刻（T_N'）との差分の絶対値（$|T_W-T_N'|$）を算出し、この絶対値と所定の閾値（ε）とを対比する。そして、絶対値が閾値（ε）よりも小さい場合には（$|T_W-T_N'|<\varepsilon$）、ローカル時刻（T_N'）を電波時刻（T_W）に置き換える補正をおこなう。なお、かかる状態（$|T_W-T_N'|<\varepsilon$）が連続した回数は、認証時刻要求部１４が時刻発行サーバに対して認証時刻の要求をおこなう際のトリガーとして用いられる。

【００７３】

また、時刻補正処理部１２は、かかる絶対値（$|T_W-T_N'|$）が閾値（ε）以上である場合には（$|T_W-T_N'|\geqq\varepsilon$）、ローカル時刻（$T_N'$）の補正をおこなわない。なお、かかる状態（$|T_W-T_N'|\geqq\varepsilon$）が連続した回数は、認証時刻要求部１４が時刻発行サーバに対して認証時刻の要求をおこなう際のトリガーとして用いられる。

【００７４】

ローカル時刻生成部１３は、発振器３から出力されたパルスを受け取り、このパルスに基づいてローカル時刻（T_N'）を生成する処理部である。このローカル時刻（T_N'）は、時刻補正処理部１２により電波時刻（T_W）を用いた時刻補正処理の対象となるとともに、時刻校正処理部１３により認証時刻（T_N）を用いた時刻校正処理の対象となる。なお、このローカル時刻生成部１３は、生成したローカル時刻（T_N'）を認証時刻要求部１４およびタイムスタンプ処理部１５に通知する処理をおこなう。

【００７５】

認証時刻要求部１４は、所定のタイミングで、ローカル時刻生成部１３が生成したローカル時刻（T_N'）および認証鍵記憶部２１に記憶された認証鍵を用い、ネットワーク上の時刻発行サーバに認証時刻の発行要求をおこなう処理部である。また、認証時刻の発行要求をおこなう際には、ローカル時刻（T_N'）を含んだ要求メッセージを認証鍵により暗号化したうえで通信インタフェイス部４に渡す。

【００７６】

この認証時刻要求部１４は、利用者の操作により強制的に認証時刻の発行要求をおこなうほか、時刻補正処理部１２が計数した「$|T_W-T_N'|<\varepsilon$が連続した回数」および「$|T_W-T_N'|\geqq\varepsilon$が連続した回数」をトリガーとして認証時刻の発行要求をおこなう。

【００７７】

たとえば、「$|T_W-T_N'|<\varepsilon$が連続した回数」が９０日に相当する場合に、時刻発行サーバに対して認証時刻の発行要求をおこなう。εを０．５秒とし、電波時刻（T_W）による時刻補正を一日一回おこなったと仮定すると、ローカル時刻（T_N'）は、真の時刻から最大４５秒（９０×０．５）の誤差範囲で認証時刻（T_N）による校正処理を受けることが可能となる。このようにすることで、偽電波と温度操作による連携攻撃がおこなわれた場合であってもローカル時刻（T_N'）の誤差を所定値内に抑えることができる。

【００７８】

また、強制的な認証時刻発行要求の例としては以下のものがある。たとえば、「強制的な認証時刻取得」をあらわす操作（該当するボタンを押下など）を、利用者が任意のタイミングで入力部６を介しておこなった場合に、認証時刻要求部１４はネットワーク上の時

刻発行サーバに認証時刻の発行要求をおこなう。この場合、時刻補正処理部１２が計数した「｜$T_W - T_N'$｜＜εが連続した回数または期間」あるいは「｜$T_W - T_N'$｜≧εが連続した回数または期間」などの情報を表示部５に表示して利用者の操作を促すこととしてもよい。

【００７９】

なお、かかる認証時刻要求部１４は、利用者の操作をトリガーとすることなく、ローカル時刻生成部１３が生成したローカル時刻（T_N'）に基づき定期的に時刻発行サーバに認証時刻の発行要求をおこなうこととしてもよい。たとえば、標準時刻とローカル時刻とのずれを４５秒以内に抑えたい場合、１日あたりの時刻のずれが最大０．５秒であるとすれば、９０日に１回の間隔で時刻発行サーバに認証時刻の発行要求をおこなうこととすればよい。

【００８０】

認証時刻取得部１５は、認証時刻要求部１４からの要求に応えて時刻発行サーバから送信された認証時刻（T_N）を、通信インタフェイス部４を介して受け取り、受け取った認証時刻（T_N）を時刻校正処理部１６に渡す処理をおこなう処理部である。なお、この認証時刻取得部１５は、暗号化された状態の認証時刻（T_N）を、認証鍵記憶部２１に記憶された認証鍵を用いて復号する処理をおこなう。

【００８１】

時刻校正処理部１６は、認証時刻取得部１５から受け取った認証時刻（T_N）を用いてローカル時刻生成部１３が生成するローカル時刻（T_N'）を校正する処理をおこなう処理部である。なお、電波時刻に基づいた時刻調整を「補正」と呼び、認証時刻に基づいた時刻調整を「校正」と呼ぶ理由は以下のとおりである。

【００８２】

すなわち、電波時刻は、本来、標準時刻を指しており電波による遅延もほとんどないため、ローカル時刻の基準とする時刻としては適したものである。しかし、図２などを用いて説明したように、偽電波による不正行為を受ける可能性もあるため、電波時刻に絶対的な信頼をおくことは適当ではない。

【００８３】

一方、認証時刻を取得するには、認証鍵が必要であることから認証時刻には電波時刻よりも高い信頼性がある。そこで、これらの時刻調整を区別するために、電波時刻に基づいた時刻調整を「補正」と呼び、より信頼性の高い認証時刻に基づいた時刻調整を「校正」と呼ぶこととした。

【００８４】

かかる時刻校正処理部１６は、認証時刻（T_N）とローカル時刻（T_N'）との差分の絶対値（｜$T_N - T_N'$｜）を算出し、この絶対値と所定の閾値（σ）とを対比する。そして、絶対値が閾値(σ)よりも小さい場合には（｜$T_N - T_N'$｜＜σ）、ローカル時刻（T_N'）を認証時刻（T_N）に置き換える校正をおこなう。

【００８５】

また、時刻校正処理部１６は、かかる絶対値が閾値（σ）以上である場合には（｜$T_N - T_N'$｜≧σ）、ローカル時刻（T_N'）の校正をおこなわず、認証時刻要求部１４に認証時刻の取得をおこなうよう指示する。

【００８６】

タイムスタンプ処理部１７は、ローカル時刻生成部１３が生成して時刻補正処理部１２および時刻校正処理部１６による時刻補正および時刻校正を受けたローカル時刻と、認証鍵記憶部２１に記憶されている認証鍵とを用いて電子文書に時刻を含んだ電子署名をおこなう処理部である。具体的には、このタイムスタンプ処理部１７は、通信インタフェイス部４を介して認証対象となる電子文書を受け取り、受け取った電子文書に電子署名をおこなったうえで、署名済の電子文書を、通信インタフェイス部４を介して出力する。

【００８７】

記憶部２０は、揮発性のＲＡＭ（Random Access Memory）で構成された記憶デバイスで

あり、製造時などにあらかじめ割り当てられた認証鍵を記憶する認証鍵記憶部２１をさらに備えている。認証鍵が記憶された後は、記憶部２０には常に通電がおこなわれている。このような構成とするのは、悪意の利用者により認証鍵が取り出されることを防止するためである。すなわち、悪意の利用者が認証鍵を取り出そうとしてタイムスタンプ装置を分解しようとすると、この記憶部２０への通電が停止され、記憶されていた認証鍵も失われる。

【００８８】

次に、タイムスタンプ装置１の初期処理について図５および図６を用いて説明する。図５は、時刻校正をおこなわない初期処理の処理手順を示すフローチャートであり、図６は、時刻校正をおこなう初期処理の処理手順を示すフローチャートである。

【００８９】

図５に示すように、認証時刻を用いた時刻校正をおこなわない場合には、電波時刻取得部１１は、標準電波受信部２を介して電波時刻（T_W）を強制受信し、時刻補正処理部１２は、ローカル時刻生成部１３が生成したローカル時刻（T_N'）を、受信した電波時刻（T_W）に置き換える補正をおこなうことにより、電波時刻（T_W）をローカル時刻（T_N'）の初期値とし（ステップＳ１０１）、初期処理を終了する。

【００９０】

一方、認証時刻を用いた時刻校正をおこなう場合には、図６に示すように、まず、電波時刻取得部１１は、標準電波受信部２を介して電波時刻（T_W）を強制受信し、時刻補正処理部１２は、ローカル時刻生成部１３が生成したローカル時刻（T_N'）を、受信した電波時刻（T_W）に置き換える補正をおこなうことにより、電波時刻（T_W）をローカル時刻（T_N'）の初期値とする（ステップＳ２０１）。

【００９１】

つづいて、認証時刻要求部１４は、認証時刻（T_N）の取得要求をおこなうため、時刻発行サーバに接続する（ステップＳ２０２）。そして、認証時刻取得部１５は、時刻発行サーバから受け取った認証時刻（T_N）を一時的に記憶し（ステップＳ２０３）、時刻校正処理部１６は、一時的に記憶された認証時刻（T_N）と、ローカル時刻生成部１３が生成したローカル時刻（T_N'）とを比較する（ステップＳ２０４）。つづいて、両者の誤差（$|T_N - T_N'|$）が校正閾値（σ）より小さいか否かを判定する（ステップＳ２０５）。

【００９２】

そして、両者の誤差（$|T_N - T_N'|$）が校正閾値（σ）より小さい場合には（ステップＳ２０５，Ｙｅｓ）、校正をおこなうことなくローカル時刻（T_N'）をそのまま用いて計時をおこなう（ステップＳ２０７）。一方、両者の誤差（$|T_N - T_N'|$）が校正閾値（σ）以上である場合には（ステップＳ２０５，Ｎｏ）、校正閾値（σ）以上である回数がM回以上であるか否かを判定する（ステップＳ２０６）。

【００９３】

そして、かかる回数がM回以上である場合には（ステップＳ２０６，Ｙｅｓ）、タイムスタンプ装置１の運用を停止する。一方、かかる回数がM回よりも小さい場合には（ステップＳ２０６，Ｎｏ）、ステップＳ２０１以降の処理を繰り返す。なお、図５および図６に示した各初期処理のうちどちらの初期処理を選択するかは、タイムスタンプ１の運用形態に基づいて最適なものを選ぶこととしてもよいし、あらかじめ指定することとしてもよい。

【００９４】

次に、タイムスタンプ装置１の運用中における処理手順について図７を用いて説明する。図７は、時刻補正処理および時刻校正処理の処理手順を示すフローチャートである。同図に示すように、タイムスタンプ装置１が運用を開始すると、まず、後の処理において用いられる連続回数を計数するためのカウンタを初期化する（ステップＳ３０１）。そして、電波時刻取得部１１は、標準電波受信部２を介して電波時刻（T_W）を取得する（ステップＳ３０２）。

【００９５】
つづいて、時刻補正処理部１２は、電波時刻（T_W）とローカル時刻（T_N'）との差分を算出し、誤差｜T_W-T_N'｜が補正閾値（ε）よりも小さいか否かを判定する(ステップＳ３０３)。そして、誤差｜T_W-T_N'｜が補正閾値（ε）よりも小さい場合には（ステップＳ３０３，Ｙｅｓ）、かかる電波時刻（T_W）をローカル時刻（T_N'）として採用する補正をおこなう（ステップＳ３０４）。
【００９６】
つづいて、誤差｜T_W-T_N'｜が補正閾値（ε）よりも小さい回数が所定値（α回）以上となったか否かを判定し（ステップＳ３０５）、α回以上である場合には（ステップＳ３０５，Ｙｅｓ）ステップＳ３０８以降の処理をおこなう。一方、α回よりも小さい場合には（ステップＳ３０５，Ｎｏ）、ステップＳ３０２以降の処理を繰り返す。
【００９７】
また、誤差｜T_W-T_N'｜が補正閾値（ε）以上である場合には（ステップＳ３０３，Ｎｏ）、ローカル時刻（T_N'）をそのまま採用する（ステップＳ３０６）。つづいて、誤差｜T_W-T_N'｜が補正閾値（ε）以上である回数が所定値（β回）以上となったか否かを判定し（ステップＳ３０７）、β回以上である場合には（ステップＳ３０７，Ｙｅｓ）ステップＳ３０８以降の処理をおこなう。一方、β回よりも小さい場合には（ステップＳ３０７，Ｎｏ）、ステップＳ３０２以降の処理を繰り返す。
【００９８】
つづいて、ステップＳ３０５またはステップＳ３０７が「Ｙｅｓ」である場合には、認証時刻要求部１４は、認証時刻（T_N）の取得要求をおこなうため、時刻発行サーバに接続する（ステップＳ３０８）。そして、校正処理部１６は、認証時刻取得部１５を介して認証時刻（T_N）を受け取ると、受け取った認証時刻（T_N）とローカル時刻（T_N'）との差分を算出し、誤差（｜T_N-T_N'｜）が校正閾値（σ）より小さいか否かを判定する（ステップＳ３０９）。
【００９９】
そして、誤差（｜T_N-T_N'｜）が校正閾値（σ）より小さい場合には（ステップＳ３０９，Ｙｅｓ）、認証時刻（T_N）をローカル時刻（T_N'）として採用し（ステップＳ３１０）、ステップＳ３０１以降の処理を繰り返す。一方、誤差（｜T_N-T_N'｜）が校正閾値（σ）以上である場合には（ステップＳ３０９，Ｎｏ）、誤差（｜T_N-T_N'｜）が校正閾値（σ）以上である回数が所定値（γ回）以上となったか否かを判定し（ステップＳ３１１）、γ回以上である場合には（ステップＳ３１１，Ｙｅｓ）運用を停止する。一方、γ回よりも小さい場合には（ステップＳ３１１，Ｎｏ）、ステップＳ３０８以降の処理を繰り返す。
【０１００】
次に、時刻発行サーバから認証時刻（T_N）を取得する際の遅延補正処理について図８～図１０を用いて説明する。図８は、認証時刻に対する遅延補正処理の概要を示す図である。同図に示すように、タイムスタンプ装置１が時刻発行サーバ１０１に認証時刻（T_N）の要求をおこなってから、認証時刻（T_N）を受け取るまでには、往復分のネットワーク遅延が含まれる。
【０１０１】
具体的には、タイムスタンプ装置１が送信した要求が時刻発行サーバ１０１に届くまでには、τ_1の時間がかかり、時刻発行サーバ１０１が送信した認証時刻（T_N）がタイムスタンプ装置１に届くまでには、τ_2の時間がかかる。すなわち、タイムスタンプ装置１は、時刻発行サーバ１０１が送信した認証時刻（T_N）をτ_2遅れで受信することになる。通常は、これらの遅延時間（τ_1およびτ_2）は１００ｍｓｅｃ程度の小さいものであるため問題とはならないが、ネットワークを遅延させるような不正行為がおこなわれると、せっかく取得した認証時刻（T_N）の正確性が保証されないこととなってしまう。
【０１０２】
そこで、タイムスタンプ装置１は、上記した$\tau_1+\tau_2$の値を求め、この値に基づいてτ

$_2$の値を推定することとしている。具体的には、認証時刻要求部１４が認証時刻の要求をおこなう時点のローカル時刻（T_N'）を含めた要求メッセージ５１を送信する。この要求メッセージ５１を受信した時刻発行サーバ１０１は、認証時刻（T_N）と、受け取ったローカル時刻（T_N'）を含んだ応答メッセージ５２を返信する。なお、図８における５２ａは、この応答メッセージに含まれるローカル時刻（T_N'）を示しており、５２ｂは、同じく認証時刻（T_N）を示している。

【０１０３】

タイムスタンプ装置１は、この応答メッセージ５２を受信した時刻（$T_N'+(\tau_1+\tau_2)$）から、この応答メッセージに含まれる５２ａ（T_N'）を差し引くことにより、をタイムスタンプ装置１は、往復の遅延時間をあらわす（$\tau_1+\tau_2$）を算出する。そして、この（$\tau_1+\tau_2$）を２で除することによりτ_2を推定し、受け取った認証時刻（T_N）からτ_2を差し引いた値を、認証時刻として取り込む。

【０１０４】

なお、本実施例においては、１回の要求から得られた遅延時間（$\tau_1+\tau_2$）を２で除することによりτ_2を推定したが、かかる要求を数回おこなって得られた遅延時間（$\tau_1+\tau_2$）の平均をとることとしてもよいし、複数の時刻発行サーバ１０１に要求をおこなって得られた遅延時間（$\tau_1+\tau_2$）の平均をとることとしてもよい。

【０１０５】

次に、時刻発行サーバ１０１の遅延補正の処理手順について図９を用いて説明する。図９は、時刻発行サーバにおける遅延補正の処理手順を示すフローチャートである。同図に示すように、時刻発行サーバ１０１は、タイムスタンプ装置１からローカル時刻（T_N'）を受信すると（ステップＳ４０１）、自らが管理する認証時刻（T_N）と受信したローカル時刻（T_N'）との差分の絶対値が所定値（σ′）よりも小さいか否かを判定する（ステップＳ４０２）。

【０１０６】

そして、認証時刻（T_N）と受信したローカル時刻（T_N'）との差分の絶対値が所定値（σ′）よりも小さい場合には（ステップＳ４０２，Ｙｅｓ）、受信したローカル時刻（T_N'）および認証時刻（T_N）をタイムスタンプ装置１に送信して（ステップＳ４０３）処理を終了する。一方、かかる絶対値が所定値（σ′）以上である場合には（ステップＳ４０２，Ｎｏ）、タイムスタンプ装置１への認証時刻（T_N）送信を禁止するとともに（ステップＳ４０４）、タイムスタン装置１へ警報コマンドを送信して（ステップＳ４０５）処理を終了する。

【０１０７】

このようにすることで、時刻発行サーバ１０１は、認証時刻（T_N）から大きくずれたローカル時刻（T_N'）をもつタイムスタンプ装置１への認証時刻（T_N）の提供を中止することができる。したがって、不正行為がおこなわれている可能性が高いタイムスタンプ装置１が運用されることを効果的に防止することが可能となる。

【０１０８】

次に、タイムスタンプ装置１の遅延補正の処理手順について図１０を用いて説明する。図１０は、タイムスタンプ装置における遅延補正の処理手順を示すフローチャートである。同図に示すように、まず、タイムスタンプ装置１は時刻発行サーバ１０１へローカル時刻（T_N'）を送信する（ステップＳ５０１）。そして、時刻発行サーバ１０１からの応答を待ち、警報コマンドを受信した場合には（ステップＳ５０２，Ｙｅｓ）、表示部５などに警報を出力して（ステップＳ５１０）時刻発行サーバへの接続を停止する。

【０１０９】

一方、受け取ったメッセージが警報コマンドではない場合には（ステップＳ５０２，Ｎｏ）、かかるメッセージから認証時刻（T_N）および先に送信したローカル時刻（T_N'）を取得する（ステップＳ５０３）。そして、メッセージの受信時刻と、メッセージに含まれたローカル時刻（T_N'）との差（$\tau_1+\tau_2$）を算出する。なお、この差（$\tau_1+\tau_2$）は、往復のネットワーク遅延をあらわしている。

【０１１０】
つづいて、この遅延時間（$\tau_1+\tau_2$）を２で除した値が所定値（ε′）よりも小さいか否かを判定する（ステップＳ５０５）。そして、（$\tau_1+\tau_2$）／２が所定値（ε′）よりも小さい場合には（ステップＳ５０５，Ｙｅｓ）、あらたなローカル時刻（T_N'）として受信した認証時刻（T_N）を採用して（ステップＳ５０６）処理を終了する。
【０１１１】
一方、遅延時間（$\tau_1+\tau_2$）を２で除した値が所定値（ε′）以上である場合には（ステップＳ５０５，Ｎｏ）、所定値（ε′）以上となる回数が所定回数連続しているか否かを判定し（ステップＳ５０７）、所定回数以上連続している場合には（ステップＳ５０７，Ｙｅｓ）、警報を出力したうえで（ステップＳ５０８）時刻発行サーバへの接続を停止する。また、連続回数が所定回数よりも小さい場合には、表示部５などに警報を出力したうえで（ステップＳ５０９）、ステップＳ５０１以降の処理を繰り返す。
【０１１２】
上述してきたように、本実施例では、ローカル時刻生成部が生成したローカル時刻を、電波時刻取得部が取得した電波時刻を用いて補正するとともに、認証時刻取得部が時刻発行サーバから取得した認証時刻を用いて校正することとし、認証時刻要求部は、ローカル時刻と電波時刻とのずれが所定値より小さい場合の回数と、所定値以上である場合の回数とが所定値を上回ったことをトリガーとして認証時刻を取得し、時刻校正処理部は、取得した認証時刻の遅延時間を考慮したうえでローカル時刻の校正をおこなうよう構成したので、悪意の利用者による時刻改ざんを防止することにより電子署名に用いられる時刻の信頼性を高めるとともに、ネットワークに常時接続しない場合であっても時刻の信頼性を保証することができる。
【０１１３】
ところで、上記の実施例で説明した各種の処理は、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って実現することができる。そこで、以下では、図１１を用いて、上記の実施例と同様の機能を有する時刻校正プログラムを実行するコンピュータの一例を説明する。図１１は、時刻校正プログラムを実行するコンピュータを示す図である。
【０１１４】
ここで、この「コンピュータ」には、パーソナルコンピュータのみならず、デジタルカメラやデジタルビデオカメラといった装置に内蔵されるいわゆる「組み込みコンピュータ」が含まれるものとする。かかる時刻校正プログラムをこれらのコンピュータ上で動作させることにより、文書データ、画像データ、映像データといった電子データの日付や時間を保証することが可能となる。
【０１１５】
同図に示すようにタイムスタンプ装置としてのコンピュータ３０は、標準電波受信部３１、発振器３２、通信インタフェイス部３３、表示部３４、入力部３５、揮発性ＲＡＭ３６、ＲＯＭ（Read Only Memory）３７およびＣＰＵ（Central Processing Unit）３８をバス３９で接続して構成される。ここで、標準電波受信部３１、発振器３２、通信インタフェイス部３３、表示部３４および入力部３５は、図４に示した、標準電波受信部２、発振器３、通信インタフェイス部４、表示部５および入力部６にそれぞれ対応する。そして、通信インタフェイス部３３を介して、このコンピュータ３０は他のコンピュータやネットワークに接続される。
【０１１６】
ＲＯＭ３７には、時刻校正プログラム３７ａがあらかじめ記憶されており、ＣＰＵ３８が、ＲＯＭ３７の時刻校正プログラム３７ａを読み出して実行することで、図１１に示すように、時刻校正プログラム３７ａは時刻校正プロセス３８ａとして機能するようになる。また、揮発性ＲＡＭ３６には認証鍵３６ａが記憶されており、この認証鍵３６ａは時刻校正プログラム３７ａが時刻校正処理をおこなう際に使用される。
【０１１７】

ところで、上記した時刻校正プログラム３７ａについては、必ずしもあらかじめＲＯＭ３７に記憶させておく必要はなく、たとえば、コンピュータ３０が読み出し可能なフレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、光磁気ディスクなどの「可搬用の物理媒体」、または、公衆回線、インタネット、ＬＡＮ、ＷＡＮなどを介してコンピュータ３０に接続される「他のコンピュータ（またはサーバ）」などにプログラムを記憶させておき、コンピュータ３０がこれらからプログラムを読み出して実行するようにしてもよい。

【０１１８】

（付記１）内部時計が出力するローカル時刻に基づいて該ローカル時刻を含んだ電子署名をおこなうタイムスタンプ装置であって、

標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得手段と、

前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得手段と、

前記電波時刻取得手段により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正手段と、

前記認証時刻取得手段により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正手段と

を備えたことを特徴とするタイムスタンプ装置。

【０１１９】

（付記２）前記認証時刻取得手段は、

前記時刻補正手段が算出した前記差分の絶対値が前記第一の閾値よりも小さい回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、

前記時刻校正手段は、

該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１に記載のタイムスタンプ装置。

【０１２０】

（付記３）前記認証時刻取得手段は、

前記時刻補正手段が算出した前記差分の絶対値が前記第一の閾値以上である回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、

前記時刻校正手段は、

該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１または２に記載のタイムスタンプ装置。

【０１２１】

（付記４）前記認証時刻取得手段は、

定期的に、前記時刻発行装置から前記認証時刻を取得し、

前記時刻校正手段は、

該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１に記載のタイムスタンプ装置。

【０１２２】

（付記５）前記認証時刻取得手段は、

所定の操作がおこなわれた場合に、前記時刻発行装置から前記認証時刻を取得し、

前記時刻校正手段は、

該認証時刻取得手段が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１に記載のタイムスタンプ装置。

【０１２３】

（付記６）前記時刻校正手段は、

前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値よりも小さい場合に、該認証時刻を該ローカル時刻として設定することを特

徴とする付記１～５のいずれか一つに記載のタイムスタンプ装置。
【０１２４】
（付記７）前記時刻校正手段は、
前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値以上である場合に、該ローカル時刻の校正をおこなわないことを特徴とする付記１～６のいずれか一つに記載のタイムスタンプ装置。
【０１２５】
（付記８）前記時刻校正手段は、
前記認証時刻取得手段が取得した前記認証時刻と、前記ローカル時刻との差分の絶対値が第二の閾値以上である回数が所定数連続した場合に、前記電子署名への前記ローカル時刻の付加を中止し、警報を出力することを特徴とする付記１～７のいずれか一つに記載のタイムスタンプ装置。
【０１２６】
（付記９）前記認証時刻取得手段は、
前記時刻発行装置に対して前記認証時刻の発行依頼をおこなってから該認証時刻を受け取るまでの遅延時間を算出し、該遅延時間を２で除した値が第三の閾値より小さい場合に、該認証時刻を取得することを特徴とする付記１～８のいずれか一つに記載のタイムスタンプ装置。
【０１２７】
（付記１０）前記認証時刻取得手段は、
前記遅延時間を２で除した値が第三の閾値以上である場合に、前記時刻発行装置に再度前記認証時刻の発行依頼をおこなうことを特徴とする付記９に記載のタイムスタンプ装置。
【０１２８】
（付記１１）前記認証時刻取得手段は、
前記時刻発行装置に対して前記認証時刻の発行依頼を複数回おこない、算出した複数の前記遅延時間を代表する遅延時間を求めることを特徴とする付記９または１０に記載のタイムスタンプ装置。
【０１２９】
（付記１２）前記認証時刻取得手段は、
複数の前記時刻発行装置に対して前記認証時刻の発行依頼をおこない、算出した複数の前記遅延時間を代表する遅延時間を求めることを特徴とする付記９または１０に記載のタイムスタンプ装置。
【０１３０】
（付記１３）前記認証時刻取得手段は、
前記時刻発行装置に対して署名付のローカル時刻を送信することにより前記認証時刻の発行依頼をおこない、該時刻発行装置から前記署名付のローカル時刻および該認証時刻を受信したならば、受信した時刻をあらわすローカル時刻から該署名付のローカル時刻を差し引くことにより前記遅延時間を算出することを特徴とする付記９～１２のいずれか一つに記載のタイムスタンプ装置。
【０１３１】
（付記１４）署名付のローカル時刻を受信した時点の標準時刻と、該署名付のローカル時刻との差分の絶対値が第四の閾値より小さい場合に、該標準時刻に署名をつけた認証時刻と、該署名付のローカル時刻とを返信することを特徴とする時刻発行装置。
【０１３２】
（付記１５）署名付のローカル時刻を受信した時点の標準時刻と、該署名付のローカル時刻との差分の絶対値が第四の閾値以上である場合に、依頼元への認証時刻の返信を停止するとともに該依頼元に対して署名付の警報情報を返信することを特徴とする時刻発行装置。
【０１３３】

（付記１６）内部時計が出力するローカル時刻と標準時刻とのずれを校正する時刻校正方法であって、
前記標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得工程と、
前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得工程と、
前記電波時刻取得工程により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正工程と、
前記認証時刻取得工程により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正工程と
を含んだことを特徴とする時刻校正方法。

【０１３４】

（付記１７）前記認証時刻取得工程は、
前記時刻補正工程が算出した前記差分の絶対値が前記第一の閾値よりも小さい回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正工程は、
該認証時刻取得工程が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１６に記載の時刻校正方法。

【０１３５】

（付記１８）前記認証時刻取得工程は、
前記時刻補正工程が算出した前記差分の絶対値が前記第一の閾値以上である回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正工程は、
該認証時刻取得工程が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１６または１７に記載の時刻校正方法。

【０１３６】

（付記１９）内部時計が出力するローカル時刻と標準時刻とのずれを校正する時刻校正プログラムであって、
前記標準時刻を含んだ電波を受信することにより該標準時刻を電波時刻として取得する電波時刻取得手順と、
前記標準時刻と同期した認証時刻を発行する時刻発行装置から該認証時刻を取得する認証時刻取得手順と、
前記電波時刻取得手順により取得された前記電波時刻と前記ローカル時刻との差分の絶対値を算出し、該差分の絶対値が第一の閾値よりも小さい場合に該電波時刻を該ローカル時刻として設定する補正をおこない、該差分の絶対値が該第一の閾値以上である場合に該ローカル時刻の補正をおこなわない時刻補正手順と、
前記認証時刻取得手順により取得された前記認証時刻に基づいて前記ローカル時刻の校正をおこなう時刻校正手順と
をコンピュータに実行させることを特徴とする時刻校正プログラム。

【０１３７】

（付記２０）前記認証時刻取得手順は、
前記時刻補正手順が算出した前記差分の絶対値が前記第一の閾値よりも小さい回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正手順は、
該認証時刻取得手順が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１９に記載の時刻校正プログラム。

【０１３８】

（付記２１）前記認証時刻取得手順は、

前記時刻補正手順が算出した前記差分の絶対値が前記第一の閾値以上である回数が所定数連続した場合に、前記時刻発行装置から前記認証時刻を取得し、
前記時刻校正手順は、
該認証時刻取得手順が取得した該認証時刻を前記ローカル時刻として設定することを特徴とする付記１９または２０に記載の時刻校正プログラム。

【産業上の利用可能性】

【０１３９】

以上のように、本発明に係るタイムスタンプ装置、時刻校正方法および時刻校正プログラムは、提供する時刻の信頼性を保証する必要がある場合に有用であり、特に、タイムビジネスを構成するタイムスタンプ装置に適している。

【図面の簡単な説明】

【０１４０】

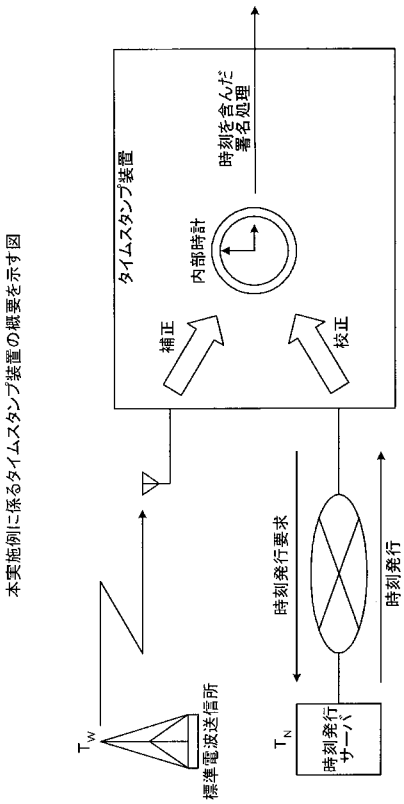
【図１】本実施例に係るタイムスタンプ装置の概要を示す図である。
【図２】時刻校正の概要を示す図である。
【図３－１】タイムスタンプ装置の構成例１を示す図である。
【図３－２】タイムスタンプ装置の構成例２を示す図である。
【図３－３】タイムスタンプ装置の構成例３を示す図である。
【図４】タイムスタンプ装置の構成を示す機能ブロック図である。
【図５】時刻校正をおこなわない初期処理の処理手順を示すフローチャートである。
【図６】時刻校正をおこなう初期処理の処理手順を示すフローチャートである。
【図７】時刻補正処理および時刻校正処理の処理手順を示すフローチャートである。
【図８】認証時刻に対する遅延補正処理の概要を示す図である。
【図９】時刻発行サーバにおける遅延補正の処理手順を示すフローチャートである。
【図１０】タイムスタンプ装置における遅延補正の処理手順を示すフローチャートである。
【図１１】時刻校正プログラムを実行するコンピュータを示す図である。
【図１２】従来のタイムスタンプ装置の概要を示す図である。
【図１３】従来のタイムスタンプ装置の内部時刻改変を示す図である。
【図１４】従来のタイムスタンプ装置における不正行為によるドリフトを示す図である。

【０１４１】

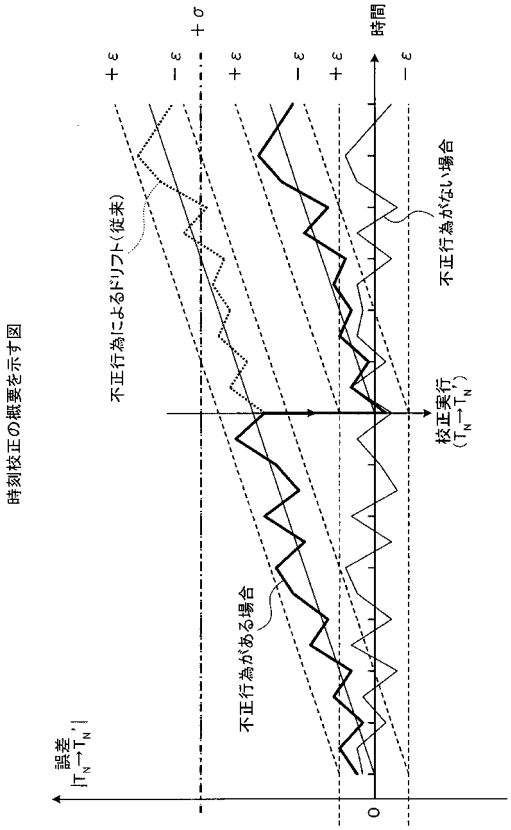
１　タイムスタンプ装置
２　標準電波受信部
３　発振器
４　通信インタフェイス部
５　表示部
６　入力部
１０　制御部
１１　電波時刻取得部
１２　時刻補正処理部
１３　ローカル時刻生成部
１４　認証時刻要求部
１５　認証時刻取得部
１６　時刻校正処理部
１７　タイムスタンプ処理部
２０　記憶部
２１　認証鍵記憶部
３０　タイムスタンプ装置（コンピュータ）
３１　標準電波受信部
３２　発振器
３３　通信インタフェイス部

３４　表示部
３５　入力部
３６　揮発性ＲＡＭ
３６ａ　認証鍵
３７　ＲＯＭ
３７ａ　時刻校正プログラム
３８　ＣＰＵ
３８ａ　時刻校正プロセス
３９　バス
５１　要求メッセージ
５２　応答メッセージ
１０１　時刻発行サーバ

【図１】

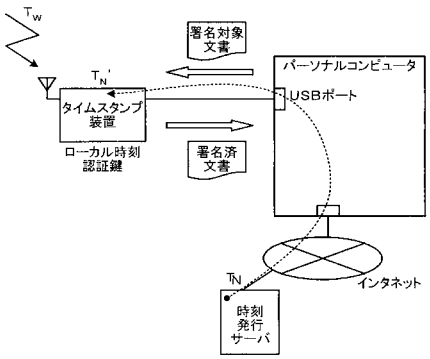


【図２】



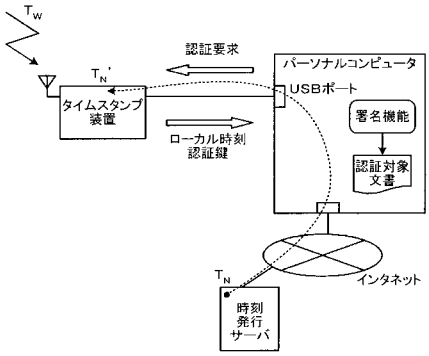
【図３－１】

タイムスタンプ装置の構成例1を示す図



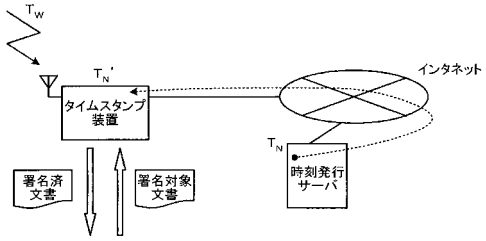
【図３－２】

タイムスタンプ装置の構成例2を示す図



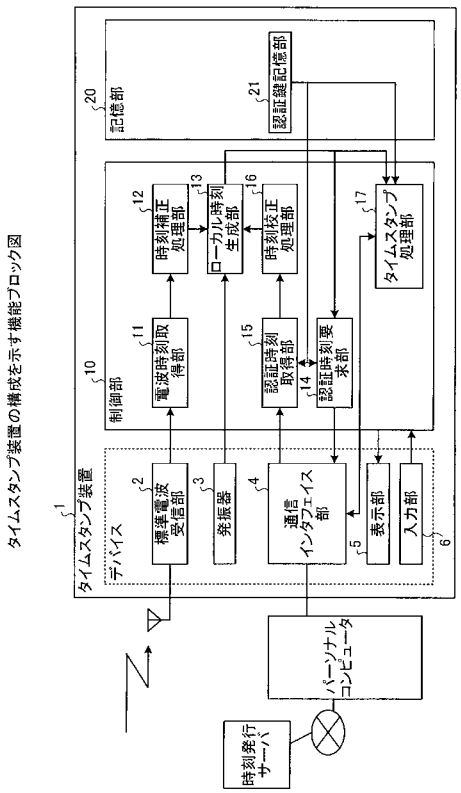
【図３－３】

タイムスタンプ装置の構成例3を示す図



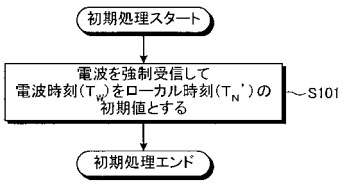
【図４】

タイムスタンプ装置の構成を示す機能ブロック図



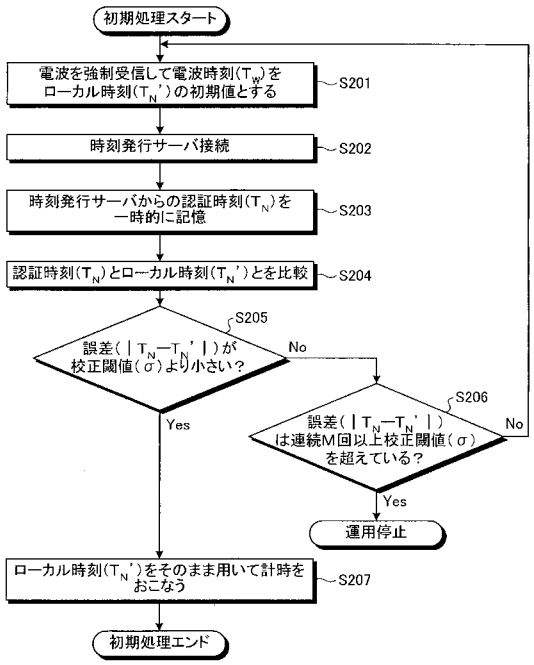
【図５】

時刻校正をおこなわない初期処理の処理手順を示すフローチャート



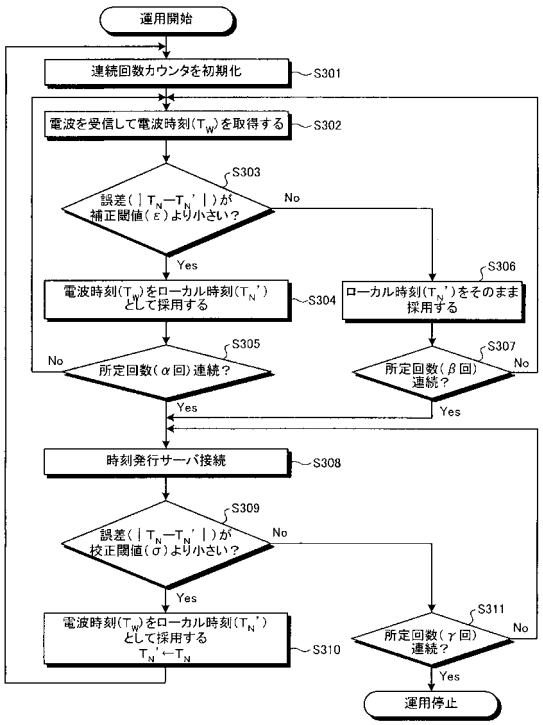
【図６】

時刻校正をおこなう初期処理の処理手順を示すフローチャート



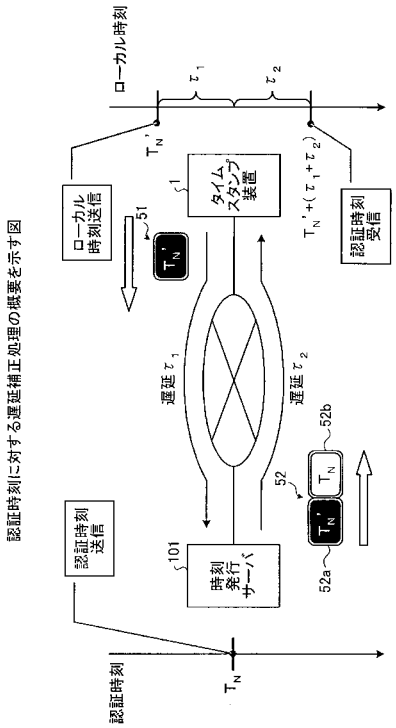
【図７】

時刻補正処理および時刻校正処理の処理手順を示すフローチャート



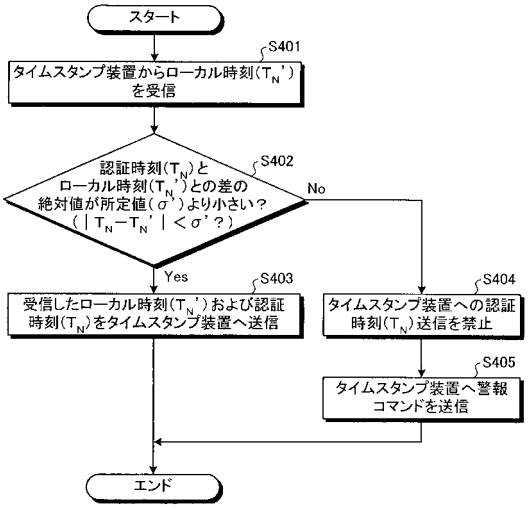
【図８】

認証時刻に対する遅延補正処理の概要を示す図

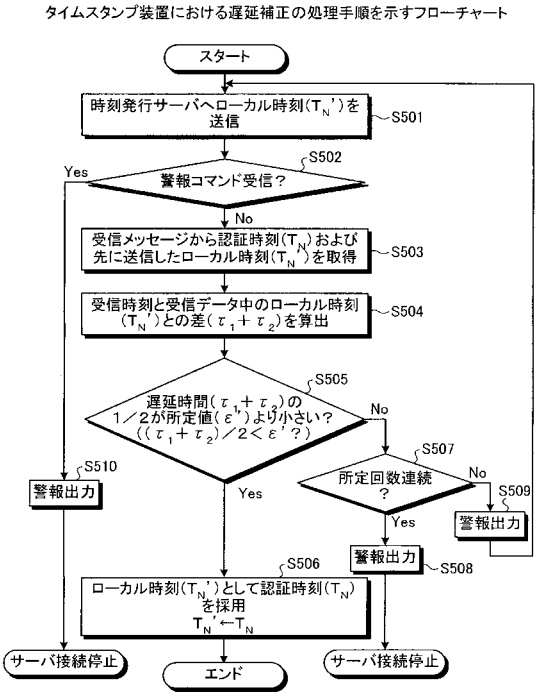


【図９】

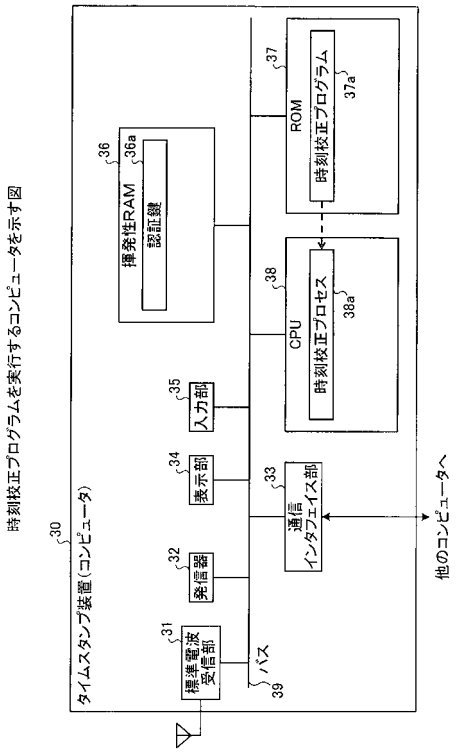
時刻発行サーバにおける遅延補正の処理手順を示すフローチャート



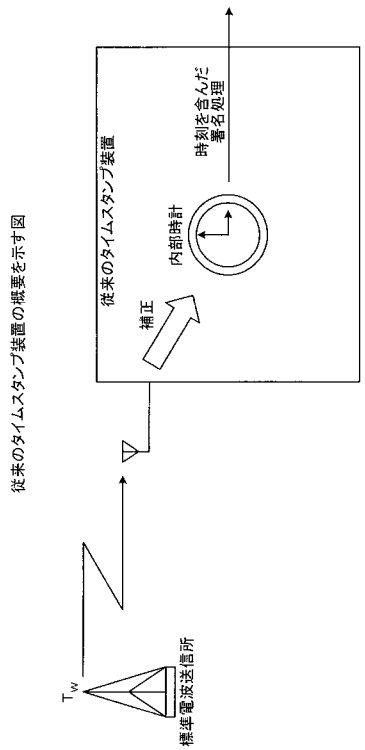
【図１０】



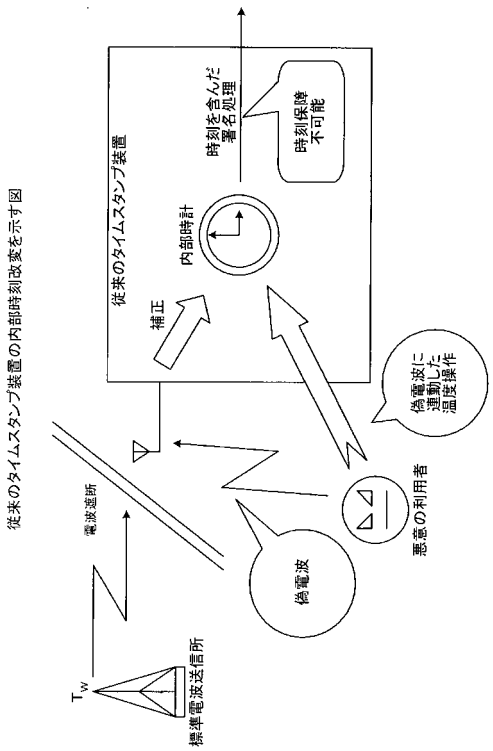
【図１１】



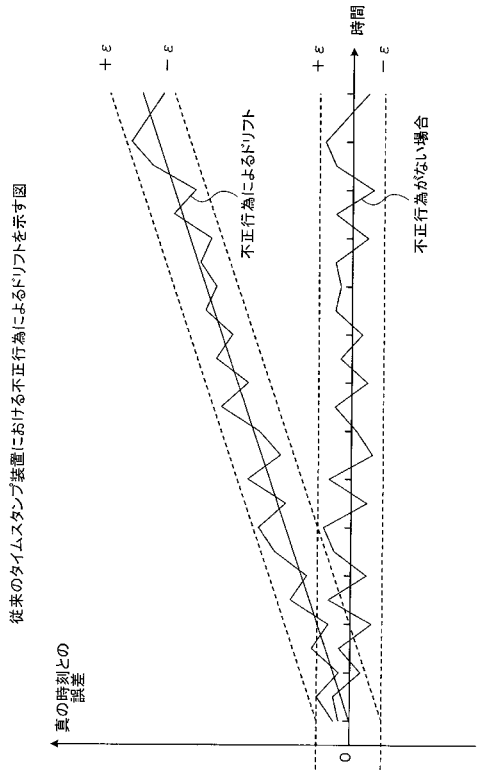
【図１２】



【図１３】



【図１４】


従来のタイムスタンプ装置における不正行為によるドリフトを示す図
真の時刻との誤差
時間
＋ε
－ε
＋ε
－ε
0
不正行為によるドリフト
不正行為がない場合