

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4451253号
(P4451253)

(45) 発行日 平成22年4月14日(2010.4.14)

(24) 登録日 平成22年2月5日(2010.2.5)

(51) Int.Cl.

F I

H04L 9/32 (2006.01)

H04L 9/00 675Z

H04L 9/00 675D

請求項の数 49 (全 121 頁)

(21) 出願番号 特願2004-256035 (P2004-256035)
 (22) 出願日 平成16年9月2日(2004.9.2)
 (65) 公開番号 特開2005-110225 (P2005-110225A)
 (43) 公開日 平成17年4月21日(2005.4.21)
 審査請求日 平成18年8月4日(2006.8.4)
 (31) 優先権主張番号 特願2003-315701 (P2003-315701)
 (32) 優先日 平成15年9月8日(2003.9.8)
 (33) 優先権主張国 日本国(JP)

(73) 特許権者 000004226
 日本電信電話株式会社
 東京都千代田区大手町二丁目3番1号
 (74) 代理人 100083806
 弁理士 三好 秀和
 (72) 発明者 堀田 英一
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内
 (72) 発明者 小野 諭
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内
 (72) 発明者 田倉 昭
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

最終頁に続く

(54) 【発明の名称】時刻証明方法、時刻証明監査方法、時刻証明装置、監査装置、時刻証明プログラム、時刻証明監査プログラム、時刻証明検証プログラム、およびプログラム記録媒体

(57) 【特許請求の範囲】

【請求項1】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリー

10

20

フに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめステップと、

前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、

10

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信ステップと、

20

前記第2のルート値を前記公表機関に公表する公表ステップと、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信ステップと、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

30

【請求項2】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

40

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

50

複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめステップと、

前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成ステップと、

10

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

20

前記第2のルート値を前記公表機関に公表する公表ステップと、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信ステップと、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

30

【請求項3】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

40

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

50

複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめステップと、

前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第 1 の補完情報送信ステップと、

前記第 2 のルート値を前記公表機関に公表する公表ステップと、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第 2 の補完情報送信ステップと、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第 2 のルート値と前記公表機関に公表された前記第 2 のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを特徴とする時刻証明方法。

【請求項 4】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に

10

20

30

40

50

従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめステップと、

10

前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得ステップと、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成ステップと、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

20

前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

前記第2のルート値を前記公表機関に公表する公表ステップと、

30

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信ステップと、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

40

【請求項5】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、

50

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、

前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、

前記要求が割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得ステップと、

10

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成ステップと、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、

前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、

20

を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする時刻証明方法。

【請求項6】

前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを特徴とする請求項3乃至5のいずれか1項に記載の時刻証明方法。

【請求項7】

30

前記第1の時刻証明要求まとめステップは、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成ステップは、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項1乃至6のいずれか1項に記載の時刻証明方法。

40

【請求項8】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割

50

り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査ステップと、

前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第2の監査ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査ステップと、

前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、

を有することを特徴とする時刻証明監査方法。

【請求項9】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

10

前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、

20

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査ステップと、

前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第1のルート値に一致するか否かにより、前記受理証明書を検証する第2の監査ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査ステップと、

前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、

30

を有することを特徴とする時刻証明監査方法。

【請求項10】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記

40

50

要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

10

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

20

を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することの特徴とする時刻証明監査方法。

【請求項11】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

30

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介

40

50

して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項12】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前

10

20

30

40

50

記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することの特徴とする時刻証明監査方法。

【請求項13】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻

及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする時刻証明監査方法。

10

【請求項14】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

20

30

40

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査ステップと、

50

前記第 1 の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと

、
前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、

前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第 2 の監査ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第 3 の監査ステップと、

10

前記第 1 の監査ステップ、前記第 2 の監査ステップ、及び前記第 3 の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、

を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項 15】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

20

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前記補完情報を 1 次補完情報として取得する 1 次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記 1 次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第 2 の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

30

40

50

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査ステップと、

前記第1の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと、

前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、

前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否かを検証する第2の監査ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査ステップと、

前記第1の監査ステップ、前記第2の監査ステップ、及び前記第3の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、

を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項16】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、

を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする時刻証明監査方法。

【請求項17】

前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを特徴とする請求項12乃至16のいずれか1項に記載の時刻証明監査方法。

【請求項18】

前記第1の時刻証明要求まとめ手段は、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成手段は、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項8乃至17のいずれか1項に記載の時刻証明監査方法。

【請求項19】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、

前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリー

フより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信手段と、

10

前記第2のルート値を前記公表機関に公表する公表手段と、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信手段と、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。

20

【請求項20】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

30

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、

40

前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

50

前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第 2 の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

前記第 2 のルート値を前記公表機関に公表する公表手段と、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第 2 の補完情報送信手段と、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第 2 のルート値と前記公表機関に公表された前記第 2 のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第 2 の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第 1 のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。

【請求項 2 1】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、それぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、

前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリー

10

20

30

40

50

フより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、

前記第2のルート値を前記公表機関に公表する公表手段と、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信手段と、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを特徴とする時刻証明装置。

【請求項22】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、

前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位

10

20

30

40

50

置情報、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

前記要求から計算された前記第１のルート値が割り当てられた前記第２の二分木のリーフより右側のリーフである監視点から前記第２の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第２の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

10

前記第２のルート値を前記公表機関に公表する公表手段と、

前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第２の補完情報送信手段と、

を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第２のルート値と前記公表機関に公表された前記第２のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第２の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第１のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。

20

【請求項２３】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、

前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、

30

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、

予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第１の二分木において、同一の親を有する２つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第１の二分木のリーフに割り当てて、前記単位時間終了後、前記第１の二分木のルートに割り当てる第１のルート値を計算する第１の時刻証明要求まとめ手段と、

前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

前記要求が割り当てられた前記第１の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第１の二分木における前記補完情報を１次補完情報として取得する１次補完情報取得手段と、

40

前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第１のルート値、および前記１次補完情報を含む受理証明書を作成する受理証明書作成手段と、

前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、

前記要求から計算された前記第１のルート値が割り当てられた単位時間における前記第１の二分木のルート値、割り当てられた前記時刻情報、及び前記第１の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、

50

前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、

を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする時刻証明装置。

【請求項24】

前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを特徴とする請求項21乃至23のいずれか1項に記載の時刻証明装置。

10

【請求項25】

前記第1の時刻証明要求まとめ手段は、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成手段は、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項19乃至24のいずれか1項に記載の時刻証明装置。

20

【請求項26】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

30

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点

40

50

の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査手段と、

前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第2の監査手段と、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、

前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、

を有することを特徴とする監査装置。

【請求項27】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネット

ワークを介して受信する検証要求受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査手段と、

前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第1のルート値に一致するか否かにより、前記受理証明書を検証する第2の監査手段と、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、

前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、

を有することを特徴とする監査装置。

【請求項28】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュ

10

20

30

40

50

ータネットワークを介して閲覧可能な状態にする公開手段と、
を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することの特徴とする監査装置。

【請求項 29】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、

前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、
を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することの特徴とする監査装置。

【請求項 30】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成す

るとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、

前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することの特徴とする監査装置。

【請求項31】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の

10

20

30

40

50

乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、それぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、

前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを特徴とする監査装置。

【請求項32】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、それぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられた

それぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

10

20

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査手段と、

前記第1の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、

30

前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、

前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第2の監査手段と、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、

前記第1の監査手段、前記第2の監査手段、及び前記第3の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、

40

を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする監査装置。

【請求項33】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタン

50

プ・システムにおける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

10

20

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査手段と、

30

前記第1の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、

前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、

前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否かを検証する第2の監査手段と、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、

前記第1の監査手段、前記第2の監査手段、及び前記第3の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、

40

を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを特徴とする監査装置。

【請求項34】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムに

50

おける前記監査装置であって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、

10

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、

20

前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と

、
を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証することを特徴とする監査装置。

【請求項35】

前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを特徴とする請求項30乃至34のいずれか1項に記載の監査装置。

30

【請求項36】

前記第1の時刻証明要求まとめ手段は、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成手段は、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項26乃至35のいずれか1項に記載の監査装置。

40

【請求項37】

請求項1乃至7に記載の時刻証明方法の各ステップを前記時刻証明装置に実行させることを特徴とする時刻証明プログラム。

【請求項38】

請求項8乃至18に記載の時刻証明監査方法の各ステップを前記監査装置に実行させる

50

ことを特徴とする時刻証明監査プログラム。

【請求項 39】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、

前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第 1 の補完情報受信ステップと、

前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する検証結果受信ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第 2 の補完情報受信ステップと、

前記公表機関から公表されている前記第 2 のルート値を取得する公表機関利用ステップと、

10

20

30

40

50

前記公表機関から取得した前記第2のルート値と、前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項40】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

10

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

20

30

前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれる前記第2次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する監査結果受信ステップと、

40

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、

前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第2のルート値と、前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項41】

50

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、

前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第1の補完情報受信ステップと、

前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第1の検証ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第2の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、

前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第2のルート値と、前記時刻証明装置に前記受理証明書

10

20

30

40

50

および後付の補完情報から計算した前記第 2 のルート値が一致するか否かを検証する第 3 の検証ステップと、
を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項 4 2】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

10

予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前記補完情報を 1 次補完情報として取得する 1 次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記 1 次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第 2 の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

20

30

前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれる前記第 2 次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第 1 のルート値に一致するか否かを検証する第 1 の検証ステップと、

前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第 2 の検証ステップと、

40

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第 2 の補完情報受信ステップと、

前記公表機関から公表されている前記第 2 のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第 2 のルート値と、前記受理証明書および後付の補完情報から計算した前記第 2 のルート値が一致するか否かを検証する第 3 の検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項 4 3】

50

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおいてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、

前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第1の補完情報受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第1の検証ステップと、

前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第2の検証ステップと、

10

20

30

40

50

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、

前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第2のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する第3の検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項44】

10

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

20

30

40

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれる前記第2次二分木のいずれかのリーフの値が、前記受理証明書

50

に含まれる前記第 1 のルート値に一致するか否かを検証する第 1 の検証ステップと、

前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第 2 の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第 2 の補完情報受信ステップと、

前記公表機関から公表されている前記第 2 のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第 2 のルート値と、前記受理証明書および後付の補完情報から計算した前記第 2 のルート値が一致するか否かを検証する第 3 の検証ステップと、を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項 45】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、

前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情

10

20

30

40

50

報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第1の補完情報受信ステップと、

前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、

10

前記保証書に含まれる前記デジタル署名の署名検証を行う第1の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、

前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第2のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する第2の検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

20

【請求項46】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフ

30

40

50

に割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受信ステップと、

前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、

前記監査装置が、前記監査情報に含まれる前記第2次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、

前記保証書に含まれる前記デジタル署名の署名検証を行う第1の検証ステップと、

前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、

前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、

前記公表機関から取得した前記第2のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する第2の検証ステップと、

を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項47】

所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、

前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、

前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応す

る時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、

前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証する検証ステップと、
を前記利用者装置に実行させることを特徴とする時刻証明検証プログラム。

【請求項48】

前記第1の時刻証明要求まとめ手段は、

前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、

前記受理証明書作成手段は、

前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを特徴とする請求項39乃至47のいずれか1項に記載の時刻証明検証プログラム。

【請求項49】

請求項37乃至48のいずれか1項に記載されたプログラムを記録していることを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、所定のデジタル情報に時刻情報を付与するタイムスタンプ・システムに関し、より詳しくは、該タイムスタンプ・システムにおける時刻証明方法、時刻証明監査方法、時刻証明装置、監査装置、時刻証明プログラム、時刻証明監査プログラム、時刻証明検証プログラム、およびプログラム記録媒体に関する。

【背景技術】

【0002】

タイムスタンプ技術は、デジタルデータがある特定時刻に存在していることを証明するとともに、その時刻以降データが変更されていないことを証明する技術である。近年、インターネット上での電子商取引の活発化や、デジタル文書管理の利用拡大に伴い、「誰が、いつ、どんなデータを生成し、送信したか」を第三者が証明する電子公証の仕組みが必要とされている。電子公証は、送受信者の特定、到達確認、時刻情報の付与、改ざんの検知、電子文書保管等の機能を具備するものであるが、タイムスタンプ技術は、このうち、時刻情報の付与及び改ざんの検知の機能を実現するものである。

【0003】

図35は、このようなタイムスタンプ技術を用いたタイムスタンプ・システムを説明する図である。同図に示すタイムスタンプ・システム900は、利用者（要求者、検証者）30がタイムスタンプの対象データをTSA（Time Stamping Authority；タイムスタンプ生成機関）10に送信すると、TSA10がTA（Time Authority；時刻源である時刻情報提供機関）20から時刻情報を入手して、利用者30から要求された対象データに対してタイムスタンプを付した受理証明書を生成し、該受理証明書を利用者に返信するようになっている。そして、TSA10で発行された受理証明書は、PKI（Public Key Infrastructure；公開鍵基盤）のもとでデジタル署名を主要な偽造防止／証明手段として採用する場合には、一般に、利用者30から送られた対象データに時刻情報を付したデジタル署名を含んだ受理証明書となっている。

【0004】

この受理証明書の真正性の主要な根拠としてデジタル署名を用いるタイムスタンプ・システムに関しては、T S A 10の不正、受理証明書の有効期間、およびシステム運用の面などにおいて問題点が指摘されている。そのため、受理証明書の真正性の主要な根拠としてデジタル署名を用いないタイムスタンプの方法も提案されている。例えば、線形リンキング (Linear Linking Protocol) による方法 (例えば、特許文献1および特許文献2参照。)

) は、T S A 10が仮に信頼できないとしてもシステム全体として高い安全性を確保することが可能となっている方法である。図36は、P K I に依存しない線形リンキングによるタイムスタンプ・システムを説明する図である。同図に示すタイムスタンプ・システム910は、複数の利用者30のタイムスタンプ対象データ (ハッシュ値) を相互に関連付けるリンク情報 L n を生成し、リンク情報 L n に時刻を付したタイムスタンプを返信するようになっており、各タイムスタンプが、それまでに生成されたすべてのタイムスタンプに依存するようになっている。そして、このリンク情報の一部 (L M、L N) が定期的にメディア等 (例えば新聞) に公表されるので、これにより、T S A 10の不正を防止し、結果としてシステム全体の信頼を高めることができるようになっている。

10

【特許文献1】特許第3278721号明細書

【特許文献2】特許第3281881号明細書

【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、上述した線形リンキングによるタイムスタンプの方法に関しては、利用者30が利用する利用者装置で受理証明書の検証を行うには、膨大な計算処理が必要となり、検証が容易でないという課題がある。例えば、時刻証明を毎秒間隔で行い、1週間に1回メディア等 (例えば新聞) に公表するタイムスタンプ・システムの場合、利用者30は、最大約60万個 ($60 \times 60 \times 24 \times 7$) のリンク情報をT S A 10からもらって計算しなければならないこととなる。

20

【0006】

また、リンク情報を1回メディア等 (例えば新聞) に公表してから、次の公表までの間においては、利用者30はT S A 10で発行された受理証明書を検証することができないという課題がある。即ち、T S A 10が一旦1回メディア等 (例えば新聞) にリンク情報を公表した後は、受理証明書を偽造することは不可能であるが、リンク情報の公表と次の公表までの間においては、受理証明書を偽造することは原理的に可能であるため、この期間にT S A 10が不正をしていないという検証が必要となっても、検証をすることができない。

30

【0007】

さらに、上述したデジタル署名を受理証明書の真正性証明の主要手段とする方法、および線形リンキングによるタイムスタンプにおいては、受理証明書に付された時刻の真正性についてT S A 10の誤動作や不正を検出する手段が与えられていないため、該時刻の真正性については全面的にT S A 10を信頼する他に方法がないという課題がある。

【0008】

本発明は、上記の課題を解決するためになされたものであり、デジタル署名を用いない、又はデジタル署名を主要な手段とはしないタイムスタンプ・システムにおいて、利用者装置で簡単に受理証明書の検証ができるとともに、定期的にメディア等へ公表する公表情報を用いなくとも受理証明書の検証を行うことができ、かつ、受理証明書に付された時刻の真正性を検証することができる時刻証明方法、時刻証明監査方法、時刻証明装置、監査装置、時刻証明プログラム、時刻証明監査プログラム、時刻証明検証プログラム、およびプログラム記録媒体を提供することを目的とする。

40

【課題を解決するための手段】

【0009】

上記目的を達成するため、請求項1記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔をおい

50

てメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめステップと、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信ステップと、前記第2のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【 0 0 1 0 】

請求項2記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる

10

20

30

40

50

第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめステップと、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記第2のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【0011】

請求項3記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木におい

10

20

30

40

50

て、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめステップと、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第 1 の補完情報送信ステップと、前記第 2 のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第 2 の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第 2 のルート値と前記公表機関に公表された前記第 2 のルート値とが一致するかどうかにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するかどうか、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを要旨とする。

【 0 0 1 2 】

請求項 4 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り

当てる第2のルート値を計算する第2の時刻証明要求まとめステップと、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信ステップと、前記第2のルート値を前記公表機関に公表する公表ステップと、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信ステップと、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【0013】

請求項5記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置の時刻証明方法であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信ステップと、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得ステップと、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめステップと、前記時刻情報を前記単位時間に割り当てる時刻情報提供ステップと、前記要求が割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得ステップと、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成ステップと、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信ステップと、前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得ステップと、前記監査情報を前記コンピュータネットワークを介して

前記監査装置に送信する監査情報送信ステップと、を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【0014】

請求項6記載の本発明は、請求項3乃至5のいずれか1項に記載の発明において、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを要旨とする。

【0015】

請求項7記載の本発明は、請求項1乃至6のいずれか1項に記載の発明において、前記第1の時刻証明要求まとめステップは、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成ステップは、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【0016】

請求項8記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前

10

20

30

40

50

記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査ステップと、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第2の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査ステップと、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有することを要旨とする。

【0017】

請求項9記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査ステップと、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第1のルート値に一致するか否かにより、前記受理証明書を検証する第2の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付される

10

20

30

40

50

べき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査ステップと、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有することを要旨とする。

【0018】

請求項10記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した連接値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【0019】

請求項11記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機

10

20

30

40

50

関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【0020】

請求項12記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、

前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第 1 の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【 0 0 2 1 】

請求項 1 3 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当

10

20

30

40

50

てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【0022】

請求項14記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即

10

20

30

40

50

時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査ステップと、前記第1の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第2の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査ステップと、前記第1の監査ステップ、前記第2の監査ステップ、及び前記第3の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【0023】

請求項15記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てら

れた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査ステップと、前記第1の監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成ステップと、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信ステップと、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否かを検証する第2の監査ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査ステップと、前記第1の監査ステップ、前記第2の監査ステップ、及び前記第3の監査ステップのそれぞれにおいて検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信ステップと、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【0024】

請求項16記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置の時刻証明監査方法であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信す

る監査情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査ステップと、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開ステップと、を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【0025】

請求項17記載の本発明は、請求項12乃至16のいずれか1項に記載の発明において、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを要旨とする。

10

【0026】

請求項18記載の本発明は、請求項8乃至17のいずれか1項に記載の発明において、前記第1の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

20

【0027】

請求項19記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当て

30

40

50

られた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

10

【0028】

請求項20記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完

20

30

40

50

情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算される前記第2のルート値と前記公表機関に公表された前記第2のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【0029】

請求項21記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第2の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第2のルート値と前記公表機関に公表された前記第2のルート

10

20

30

40

50

値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれるいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部から計算されるノードの値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて、前記受理証明書を検証することを要旨とする。

【 0 0 3 0 】

請求項 2 2 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前記補完情報を 1 次補完情報として取得する 1 次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記 1 次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第 2 の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として取得して該後付の補完情報を前記コンピュータネットワークを介して前記利用者装置に送信する第 2 の補完情報送信手段と、を有し、前記利用者装置は、受信した前記受理証明書および前記後付の補完情報から計算された前記第 2 のルート値と前記公表機関に公表された前記第 2 のルート値とが一致するか否かにより前記受理証明書を検証し、前記監査装置又は前記利用者装置は、前記監査情報に含まれる前記第 2 の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第 1 のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証することを要旨とする。

【 0 0 3 1 】

請求項 2 3 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記時刻証明装置であって、前記利用者装置から前記要求を前記コンピュータネットワークを介して受信する受信手段と、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前記補完情報を 1 次補完情報として取得する 1 次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、および前記 1 次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第 1 のルート値が割り当てられた単位時間における前記第 1 の二分木のルート値、割り当てられた前記時刻情報、及び前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、を有し、前記監査装置は、前記監査情報に付された前記時刻情報と前記時刻タグの正確さに基づいて前記監査情報を公表し、前記利用者装置は、公表された前記監査情報に含まれる前記第 1 のルート値が、前記受理証明書に含まれる前記第 1 のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【 0 0 3 2 】

請求項 2 4 記載の本発明は、請求項 2 1 乃至 2 3 のいずれか 1 項に記載の発明において、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを要旨とする。

【 0 0 3 3 】

請求項 2 5 記載の本発明は、請求項 1 9 乃至 2 4 のいずれか 1 項に記載の発明において、前記第 1 の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第 1 のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第 1 の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第 1 の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第 2 の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第 1 の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【 0 0 3 4 】

請求項 2 6 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイ

ムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して前記利用者装置に送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査手段と、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第2の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有することを要旨とする。

【0035】

請求項27記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値

を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てた第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する第1の監査手段と、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記利用者装置から受信した前記受理証明書に含まれる前記第1のルート値に一致するか否かにより、前記受理証明書を検証する第2の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、前記検証の結果を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有することを要旨とする。

【0036】

請求項28記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てた第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てた値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てた第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てた時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てた第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置

に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、前記監査ステップで前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【0037】

請求項29記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内か否かを検証する監査手段と、前記監査ステップで前記監査情報に

含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻とが所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【0038】

請求項30記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれるいずれかのノードの値が、受信した前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノード

10

20

30

40

50

の値に一致するか否か、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【 0 0 3 9 】

請求項 3 1 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前記補完情報を 1 次補完情報として取得する 1 次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記 1 次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第 2 の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、前記監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公開されている前記監査情報に含まれる前記第 2 の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第 1 のルート値に一致するか否か、及び前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証することにより、前記受理証明書を検証することを要旨とする。

【 0 0 4 0 】

請求項 3 2 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機

10

20

30

40

50

関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記受理証明書を前記利用者装置に送信後、前記一定の時間間隔内に前記利用者装置から前記補完情報の要求があった場合には、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として送信する第1の補完情報送信手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査手段と、前記第1の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、前記利用者装置から前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれるいずれかのノードの値が、前記時刻証明検証要求から計算されるノードの値に一致するか否かを検証する第2の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、前記第1の監査手段、前記第2の監査手段、及び前記第3の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【0041】

請求項33記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報

10

20

30

40

50

を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する第1の監査手段と、前記第1の監査手段においてそれぞれの時刻差が前記所定の時刻差以内である場合には、デジタル署名を含む前記監査情報に対する保証書を作成する保証書作成手段と、前記利用者装置から前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して受信する検証要求受信手段と、前記監査情報に含まれる前記第2の二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否かを検証する第2の監査手段と、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第3の監査手段と、前記第1の監査手段、前記第2の監査手段、及び前記第3の監査手段においてそれぞれの検証に成功した場合には、前記保証書を前記利用者装置に前記コンピュータネットワークを介して送信する送信手段と、を有し、前記利用者装置は、前記監査装置から受信した前記保証書の有無及び前記デジタル署名の署名検証に基づいて前記受理証明書を検証することを要旨とする。

【0042】

請求項34記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを

10

20

30

40

50

行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記監査装置であって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記受理証明書を前記コンピュータネットワークを介して前記利用者装置に送信する送信手段と、前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、を有する前記時刻証明装置から前記監査情報を前記コンピュータネットワークを介して受信する監査情報受信手段と、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻とがそれぞれ所定の時刻差以内か否かを検証する監査手段と、前記監査ステップにおけるそれぞれの時刻差が前記所定の時刻差以内である場合には、前記監査情報を前記コンピュータネットワークを介して閲覧可能な状態にする公開手段と、を有し、前記利用者装置は、公表された前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証することを要旨とする。

【0043】

請求項35記載の本発明は、請求項30乃至34のいずれか1項に記載の発明において、前記監査装置は複数であり、前記時刻証明装置は、前記時刻タグの値に基づいて前記監査装置を選択することを要旨とする。

【0044】

請求項36記載の本発明は、請求項26乃至35のいずれか1項に記載の発明において、前記第1の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

【0045】

請求項37記載の本発明は、請求項1乃至7に記載の時刻証明方法の各ステップを前記時刻証明装置に実行させる時刻証明プログラムであることを要旨とする。

【0046】

請求項38記載の本発明は、請求項8乃至18に記載の時刻証明監査方法の各ステップを前記監査装置に実行させる時刻証明監査プログラムであることを要旨とする。

【0047】

請求項 39 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第 1 の補完情報受信ステップと、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する検証結果受信ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第 2 の補完情報受信ステップと、前記公表機関から公表されている前記第 2 のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第 2 のルート値と、前記受理証明書および後付の補完情報から計算した前記第 2 のルート値が一致するか否かを検証する検証ステップと、を前記利用者装置に実行させることを要旨とする。

【 0 0 4 8 】

請求項 40 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報

10

20

30

40

50

を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれる前記第2次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否か、並びに、前記監査情報に付された前記時刻情報及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書を検証した結果を、前記監査装置から前記コンピュータネットワークを介して受信する監査結果受信ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第2のルート値と、前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0049】

請求項41記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木の

ルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第1の補完情報受信ステップと、前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第1の検証ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第2の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第2のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する第3の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0050】

請求項42記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、予め定めた単位時間内に受信した複数の要求を二分木のリーフに所定の手順に従って割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計

10

20

30

40

50

算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第1の二分木における前記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点の受理証明書が作成される時点において取得可能な前記第2の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報を含む監査情報として取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記監査装置により公開されている前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれる前記第2次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第1のルート値に一致するか否かを検証する第1の検証ステップと、前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第2の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第2のルート値と、前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する第3の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0051】

請求項43記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第1のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第2の二分木において、前記計算方法により、前記要求から計算された前記第1のルート値を前記第2の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノード

10

20

30

40

50

の値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第 1 の補完情報受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれているいずれかのノードの値が、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求から計算されるノードの値と一致するか否かを検証する第 1 の検証ステップと、前記監査情報及び前記時刻証明検証要求に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第 2 の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第 2 の補完情報受信ステップと、前記公表機関から公表されている前記第 2 のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第 2 のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第 2 のルート値が一致するか否かを検証する第 3 の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【 0 0 5 2 】

請求項 4 4 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計

算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前記補完情報を 1 次補完情報として取得する 1 次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記 1 次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第 2 の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれる前記第 2 次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第 1 のルート値に一致するか否かを検証する第 1 の検証ステップと、前記監査情報及び前記受理証明書に基づいて計算される受理証明書に付されるべき時刻と、前記受理証明書に付された時刻とが所定の時刻差以内か否かを検証する第 2 の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第 2 の補完情報受信ステップと、前記公表機関から公表されている前記第 2 のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第 2 のルート値と、前記受理証明書および後付の補完情報から計算した前記第 2 のルート値が一致するか否かを検証する第 3 の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【 0 0 5 3 】

請求項 4 5 記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフ

に割り当てて、前記一定の時間間隔終了後、前記第2の二分木のルートに割り当てる第2のルート値を計算する第2の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第1の二分木のリーフから前記第2の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記要求の受信時点において取得可能な補完情報を即時の補完情報として取得する即時の補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、該第1のルート値の前記第2の二分木における位置情報、および前記即時の補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた前記第2の二分木のリーフより右側のリーフである監視点から前記第2の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能なノードの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第2のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記受理証明書を受信後、前記一定の時間間隔内に前記補完情報の要求を前記コンピュータネットワークを介して前記時刻証明装置に送信する送信ステップと、前記時刻証明装置から、前記補完情報の要求時点において新たに取得可能な前記補完情報を後付の補完情報の一部として前記コンピュータネットワークを介して受信する第1の補完情報受信ステップと、前記受理証明書および前記後付の補完情報の一部を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれるいずれかのノードの値と、前記時刻証明検証要求から計算されるノードの値と、が一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、前記保証書に含まれる前記デジタル署名の署名検証を行う第1の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第2の補完情報受信ステップと、前記公表機関から公表されている前記第2のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第2のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第2のルート値が一致するか否かを検証する第2の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【0054】

請求項46記載の本発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成するとともに、一定の時間間隔においてメディアを含む公表機関に前記受理証明書に関連する情報を公表する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第1の二分木において、同一の親を有する2つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第1の二分木のリーフに割り当てて、前記単位時間終了後、前記第1の二分木のルートに割り当てる第1のルート値を計算する第1の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、

複数の、前記単位時間ごとに計算される前記第 1 のルート値を時刻順に二分木のリーフに左から順次割り当てて、前記一定の時間間隔で生成される第 2 の二分木において、前記計算方法により、前記要求から計算された前記第 1 のルート値を前記第 2 の二分木のリーフに割り当てて、前記一定の時間間隔終了後、前記第 2 の二分木のルートに割り当てる第 2 のルート値を計算する第 2 の時刻証明要求まとめ手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから前記第 2 の二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前記補完情報を 1 次補完情報として取得する 1 次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第 1 のルート値、該第 1 のルート値の前記第 2 の二分木における位置情報、および前記 1 次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第 1 のルート値が割り当てられた前記第 2 の二分木のリーフより右側のリーフである監視点から前記第 2 の二分木のルート値を計算するのに必要なノードの値のうち、前記監視点の受理証明書が作成される時点において取得可能な前記第 2 の二分木のリーフの値及び位置情報、並びに前記監視点に割り当てられた前記時刻情報及び前記監視点の前記第 1 の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、前記第 2 のルート値を前記公表機関に公表する公表手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受信ステップと、前記受理証明書を含む時刻証明検証要求を前記コンピュータネットワークを介して前記監査装置に送信する検証要求送信ステップと、前記監査装置が、前記監査情報に含まれる前記第 2 次二分木のいずれかのリーフの値が、前記受理証明書に含まれる前記第 1 のルート値に一致するか否か、並びに前記監査情報に付された前記時刻情報と前記時刻タグ、及び前記受理証明書に付された前記時刻情報の正確さに基づいて前記受理証明書の検証に成功した場合には、前記監査装置から前記コンピュータネットワークを介して、デジタル署名を含む前記監査情報に対する保証書を受信する検証結果受信ステップと、前記保証書に含まれる前記デジタル署名の署名検証を行う第 1 の検証ステップと、前記時刻証明装置から、前記一定の時間間隔終了後、前記受理証明書に含まれていなかった補完情報を後付の補完情報として前記コンピュータネットワークを介して受信する第 2 の補完情報受信ステップと、前記公表機関から公表されている前記第 2 のルート値を取得する公表機関利用ステップと、前記公表機関から取得した前記第 2 のルート値と、前記時刻証明装置に前記受理証明書および後付の補完情報から計算した前記第 2 のルート値が一致するか否かを検証する第 2 の検証ステップと、を前記利用者装置に実行させることを要旨とする。

【 0 0 5 5 】

請求項 4 7 記載の発明は、所定のデジタル情報に時刻情報の付与を要求する利用者装置と、前記利用者装置からの前記要求を受け付けて、前記所定のデジタル情報に時刻情報を付した受理証明書を作成する時刻証明装置と、前記受理証明書の真偽を監査する監査装置と、所定の乱数である時刻タグを提供するとともに前記時刻タグと時刻との対応付けを行う時刻タグシステムと、がそれぞれコンピュータネットワークを介して接続されているタイムスタンプ・システムにおける前記利用者装置の時刻証明検証プログラムであって、前記時刻タグシステムから前記時刻タグを取得する時刻タグ取得手段と、予め定めた単位時間内に受信した複数の要求又は取得した前記時刻タグを所定の手順に従って二分木のリーフに割り当てる第 1 の二分木において、同一の親を有する 2 つの子に割り当てられたそれぞれの値を接続した接続値のダイジェストを前記親に割り当てる値とする計算方法により、前記要求の値を前記第 1 の二分木のリーフに割り当てて、前記単位時間終了後、前記第 1 の二分木のルートに割り当てる第 1 のルート値を計算する第 1 の時刻証明要求まとめ手段と、前記時刻情報を前記単位時間に割り当てる時刻情報提供手段と、前記要求が割り当てられた前記第 1 の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記要求の補完情報と定義すると、前記第 1 の二分木における前

記補完情報を1次補完情報として取得する1次補完情報取得手段と、前記要求、前記要求が割り当てられた前記単位時間に付与された前記時刻情報、前記要求から計算された前記第1のルート値、および前記1次補完情報を含む受理証明書を作成する受理証明書作成手段と、前記要求から計算された前記第1のルート値が割り当てられた単位時間における前記第1の二分木のルート値、割り当てられた前記時刻情報、及び前記第1の二分木のリーフに割り当てられた前記時刻タグを含む監査情報を取得する監査情報取得手段と、前記監査情報を前記コンピュータネットワークを介して前記監査装置に送信する監査情報送信手段と、を有する前記時刻証明装置から、前記受理証明書を前記コンピュータネットワークを介して受信する受理証明書受信ステップと、前記監査情報に含まれる前記時刻情報と、前記監査装置が前記監査情報を受信した時刻及び前記時刻タグシステムから取得した、前記監査情報に含まれる前記時刻タグに対応する時刻との時刻差がそれぞれ所定の時刻差以内である場合には、前記監査装置により公開される前記監査情報を前記コンピュータネットワークを介して取得する監査情報取得ステップと、前記監査情報に含まれる前記第1のルート値が、前記受理証明書に含まれる前記第1のルート値と一致するか否かに基づいて前記受理証明書を検証する検証ステップと、を前記利用者装置に実行させることを要旨とする。

10

【0056】

請求項48記載の発明は、請求項39乃至47のいずれか1項に記載の発明において、前記第1の時刻証明要求まとめ手段は、前記要求が割り当てられた前記単位時間の直前の単位時間における前記第1のルートを直前ルート値と定義すると、前記要求が割り付けられた前記単位時間に構成される前記第1の二分木の所定のリーフに前記直前ルート値を割り当て、前記受理証明書作成手段は、前記要求が割り当てられた前記単位時間に付与された前記時刻情報に代えて、前記要求が割り当てられた前記単位時間の終了時に取得された第1の時刻、及び前記要求が割り当てられた前記単位時間の直前の単位時間の終了時に取得された第2の時刻を受理証明書に含めるとともに、前記直前ルート値を割り当てられた前記第1の二分木のリーフから該二分木のルート値を計算するのに必要な他のノードの値及び位置情報を前記直前ルート値の補完情報として受理証明書に含めることを要旨とする。

20

【0057】

請求項49記載の本発明は、請求項33乃至48のいずれか1項に記載されたプログラムを記録しているプログラム記録媒体であることを要旨とする。

30

【発明の効果】

【0058】

本発明によれば、デジタル署名を用いない、又はデジタル署名を主要な手段とはしないタイムスタンプ・システムにおいて、利用者装置で簡単に受理証明書の検証ができるとともに、定期的にメディア等へ公表する公表情報を用いなくても受理証明書の検証を行うことができ、かつ、受理証明書に付された時刻の真正性を検証することができる。

【0059】

これにより、利用者は、大量のデータから膨大な計算処理を行わずに、受理証明書の検証をすることができる。また、時刻証明に関する情報がメディア等に公表されてから、次の公表までの間においても、受理証明書の検証を行うことができる。さらに、受理証明書に付された時刻についても検証をすることができる。

40

【発明を実施するための最良の形態】

【0060】

以下、本発明の実施の形態を図面を用いて説明する。

【0061】

<第1の実施の形態>

図1は、本発明の第1の実施の形態に係るタイムスタンプ・システム100のシステム構成図である。同図に示すタイムスタンプ・システム100は、T S A 10に設けられた時刻証明装置1、T A 20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情

50

報提供装置2、利用者30が利用する複数のクライアント装置3*i* (*i*は自然数)、監視/監査機関に設けられ、時刻証明装置1が発行した受理証明書の監査を行う監査装置5、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置1がクライアント装置3*i*からのタイムスタンプ要求(時刻証明要求)に応じて、タイムスタンプつき受理証明書をクライアント装置3*i*に返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置3*i*は、時刻証明装置1がメディア等40に公表した情報、又は、監査装置5による監査結果によって受理証明書を検証することができるようになっているコンピュータシステムである。

【0062】

10

尚、上記コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

【0063】

時刻証明装置1は、コンピュータネットワーク4を介して時刻情報提供装置2、クライアント装置3*i*、および監査装置5とデータを送受信する送受信部11、複数のクライアント装置3*i*からの時刻証明要求として送信されたメッセージ・ダイジェスト(デジタル・データから作成されるハッシュ値)を二分木を用いてまとめる時刻証明要求まとめ部12、受理証明書を作成する際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部12でまとめられたメッセージ・ダイジェストに対して時刻情報取得部13で取得した時刻情報を付して受理証明書を作成する時刻証明作成部14、定期的にメディア等40に受理証明書に関する情報を公表する時刻証明公表部15、時刻証明作成部14で作成された受理証明書を記憶する受理証明書記憶部16、および監査装置5に送信する監査情報を作成する監査情報作成部17を具備している。

20

【0064】

以下、時刻証明装置1の時刻証明要求まとめ部12、時刻証明作成部14、時刻証明公表部15、および監査情報作成部17の機能について、より詳しく説明する。

【0065】

上述したように時刻証明要求まとめ部12は、二分木を用いて時刻証明要求をまとめるが、この二分木について図2および図3を用いて説明する。ここで、図2は、単位時間(例えば1秒、受理証明書を発行する時間間隔であり、この時間間隔をラウンドという。)に受け付けた時刻証明要求を二分木のリーフに割り当てる値とする第1次二分木の一具体例を示す図であり、図3は、一定期間(例えば1週間、時刻証明装置1がメディア等40に受理証明書に関する情報を公表する公表サイクル)において第1次二分木のルート値をリーフに割り当てる値とする第2次二分木の一具体例を示す図である。

30

【0066】

図2に示す第1次二分木は、予め定められた単位時間(上述したように例えば、1秒など)に1つ用意されるものであり、第1次二分木のリーフ(レベル0)には、ラウンド内に複数のクライアント装置3*i*から受け付けたメッセージ・ダイジェストを所定の手順に従って割り当てるようになっている。尚、第1次二分木の構成(高さ(レベルで表現する)、幅(番号で表現する))は、クライアント装置3*i*からの時刻証明要求の数に応じて変化するものであるため、本実施の形態における第1次二分木は動的に構成されるものであるが、以下においては、図2に示すように、16のリーフを有する第1次二分木の場合について説明し、動的な第1次二分木の構成に関しては、すべての実施の形態に共通の機能であるため、後述することとする。

40

【0067】

第1次二分木の各ノード(リーフを除く)に割り当てられる値は以下のように計算する。第1次二分木の親の割当値は、左側の子の割当値 H' と右側の子の割当値 H'' を接続(ビット列とビット列の結合)して、ハッシュ値を計算することにより求められるものであり、これを $h(H' \parallel H'')$ と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル(ルート)の割当値(ルート値) H を求め

50

ると、該ルート値Hは、時刻証明作成部14において作成される受理証明書の一部である。

【0068】

以後、第1次二分木のレベルj、番号iのノードを $h(j, i)$ と表し、ルート値Hの算出方法を、図2を具体例に説明する。

【0069】

あるクライアント装置3iから送信されたメッセージ・ダイジェストが $h(0, 5)$ であるとき、このリーフに割り当てられるハッシュ値 $h(0, 5)$ からルート値 $H (= h(4, 0))$ を求めるには、 $h(0, 5)$ に $h(0, 4)$ を左から接続して、ハッシュ値 h_1 を計算し、該ハッシュ値 h_1 に $h(1, 3)$ を右側から接続してハッシュ値 h_2 を計算し、該ハッシュ値 h_2 に $h(2, 0)$ を左側から接続してハッシュ値 h_3 を計算し、さらに該ハッシュ値 h_3 に $h(3, 1)$ を右側から接続してハッシュ値 $h_4 (= H)$ を計算すればよい。即ち、 $H = h(h(h(h(2, 0) \text{ } h(h(h(0, 4) \text{ } h(0, 5))) \text{ } h(1, 3))) \text{ } h(3, 1))$ である。ここで、例えば、 $h(0, 4)$ を左(右)側から接続する場合を $(L(R), h(0, 4))$ のように表し、 $h(0, 5)$ の値から二分木のルート値Hを計算するのに、必要なデータの集合を接続する方向、および接続する順序も含めて表すと、 $((L, h(0, 4)), (R, h(1, 3)), (L, h(2, 0)), (R, h(3, 1)))$ となるが、以後、このデータの集合を、第1次二分木における $h(0, 5)$ の1次補完情報とよぶ。ここで、補完情報とは、二分木のルート値を計算するのに必要な自己の値以外のノード値の集合(ノードの位置情報も含む)をいい、第1次二分木における補完情報を1次補完情報、第2次二分木における補完情報を2次補完情報という。

【0070】

このようにして、第1次二分木が構成され、ルート値Hが計算されると、次に各ラウンドで計算されたルート値Hをもとに第2次二分木が構成される。図3に示す第2次二分木は、予め定められた一定期間(上述したように例えば、1週間など)に1つ用意されるものであり、第2次二分木のリーフ(レベル0)には、第1次二分木のルート値Hを経時的に順次左側から割り当ててようになっている。尚、第1次二分木とは異なり、第2次二分木は固定的な構成となっているが(例えば、1ラウンドが1秒、公表サイクルが1週間の場合には、約60万個($60 \times 60 \times 24 \times 7$)のリーフを有する第2次二分木が構成される)、以下においては、図3に示すように、16のリーフを有する第2次二分木の場合について説明する。

【0071】

第2次二分木の各ノード(リーフを除く)に割り当てられる値は、第1次二分木の計算方法と同じである。ここで、第2次二分木のレベルj、番号iのノードを $M(j, i)$ と表して、図3に示す具体例を説明する。

【0072】

今、第2次二分木のリーフに割り当てるハッシュ値が $M(0, 5)$ であるとき、このハッシュ値 $M(0, 5)$ からルート値 $RH (= M(4, 0))$ を求めるには、 $M(0, 5)$ に $M(0, 4)$ を左から接続して、ハッシュ値 h_1' を計算し、該ハッシュ値 h_1' に $M(1, 3)$ を右側から接続してハッシュ値 h_2' を計算し、該ハッシュ値 h_2' に $M(2, 0)$ を左側から接続してハッシュ値 h_3' を計算し、さらに該ハッシュ値 h_3' に $M(3, 1)$ を右側から接続してハッシュ値 $h_4' (= RH)$ を計算すればよい。そして、このルート値RHが、時刻証明公表部15を介してメディア等40に公表される公表情報である。また、第2次二分木における $M(0, 5)$ の補完情報(以下、2次補完情報という)は、 $((L, M(0, 4)), (R, M(1, 3)), (L, M(2, 0)), (R, M(3, 1)))$ となる。

【0073】

時刻証明作成部14は、このようにして作成された第1次二分木のルート値H、第1次二分木のルート値Hの識別番号(第2次二分木のリーフを一意に特定できる番号)、それぞれのラウンドに付与される時刻(例えば、1秒間隔で付される) t 、1次補完情報HK1、および2次補完情報HK2を含む受理証明書 $TSC(H, t)$ を作成し、クライアント装置3iに送信するようになっている。尚、2次補完情報HK2に関しては、即時に取得できる2次補完情報(以後、即時2次補完情報という)と対象となる一定期間が終了後に取得できる2次補完情報(以後、後付2次補完情報という)の双方があるが、受理証明書 $TSC(H, t)$

が作成される段階においては、即時 2 次補完情報だけが送信されるものであり、後付 2 次補完情報は、対象となる一定期間が終了後に送信されるものである。例えば、図3の具体例においては、 $M(0,5)$ にとって、 $M(2,0)$ 、 $M(0,4)$ は即時 2 次補完情報であるが、 $M(1,3)$ 、 $M(3,1)$ は後付 2 次補完情報である。

【 0 0 7 4 】

図4に受理証明書 $TSC(H,t)$ の構成を示す。尚、図4に示す受理証明書 $TSC(H,t)$ は、上述したようにクライアント装置3iから送付されたメッセージ・ダイジェストそのものを第 1 次二分木のリーフに割り付ける場合のものであるが、メッセージ・ダイジェストにキー付ハッシュ関数を適用した結果を第 1 次二分木のリーフに割り付けてもよく、この場合には、図5に示すように受理証明書 $TSC(H,t)$ は、キー付ハッシュ関数を適用する際のハッシュ・キー k も含む必要がある。より詳しくは、メッセージ・ダイジェスト y を含む時刻証明要求に対して、予め定められた手順に従ってハッシュ・キー k を決定し、 k をキーとして、 y に対して、所定のキー付ハッシュ関数 h' を作用させ、ハッシュ値 $h'(k,y)$ を計算し、該ハッシュ値 $h'(k,y)$ を第 1 次二分木のリーフに割り当てるもので、これにより、あるクライアント装置3iの送付したメッセージ・ダイジェストを他のクライアント装置3iに知られないようにすることが可能となる。

【 0 0 7 5 】

また、時刻証明作成部14は、クライアント装置3iから後付けの 2 次補完情報の要求があったときは、ある一定期間の途中であっても、その時点において取得できるとともに、まだ送信していない 2 次補完情報（以後、後付 2 次補完情報の一部という）を、オンライン補完証明書としてクライアント装置3iに送信するようになっている。

【 0 0 7 6 】

尚、時刻証明装置1から受理証明書 $TSC(H,t)$ をクライアント装置3iへの送信する際には、受理証明書 $TSC(H,t)$ の完全性の保証を高める補助手段として、時刻証明装置1が準備しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵を用いてデジタル署名をつけても送信するようにしてもよい。この場合、当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いてクライアント装置3iからアクセス可能になっているものとする。

【 0 0 7 7 】

ここで、上記においては、受理証明書に付する時刻として、現在のラウンドに付与される時刻を用いたが、本発明はこれに限定されるものではなく、例えば、受理証明書に対して、以下に示す 2 つの時刻 t_1 及び t_2 を付し、当該の時刻証明要求が受け付けられた時刻が、時刻 t_1 より前であつ時刻 t_2 より後であることを証明するような区間証明書にしてもよい。

【 0 0 7 8 】

図 4 6 に、この場合の受理証明書の構成を示す。ここで、時刻 t_1 は、現在のラウンドの終結時刻とし、時刻 t_2 は、直前のラウンドの終結時刻である。そして、直前のラウンドの第 1 次二分木のルート値 H' を現在の第 1 次二分木のリーフ a_0 への割当値とし、この直前のラウンドの第 1 次二分木のルート値 H' と、リーフ a_0 の 1 次補完情報、即ち、リーフ a_0 の現在の第 1 次二分木における補完情報 H_{K1}' を受理証明書に含めるものである。

【 0 0 7 9 】

リーフ a_0 を現在の第 1 次二分木のどこに置くかについては、次の 2 つの方法がある。

【 0 0 8 0 】

第 1 の方法は、図 4 7 に示すように、リーフ a_0 を現在のラウンドのルートの子ノードとして、現在の第 1 次二分木に含める方法である（リーフ a_0 のレベルとクライアント装置3iからの要求が割り当てられるリーフのレベルは異なる）。

【 0 0 8 1 】

第 2 の方法は、図 4 8 に示すように、リーフ a_0 を現在の第 1 次集約木のレベル 0 の一番左のリーフとする方法である（リーフ a_0 のレベルとクライアント装置3iからの要求が割り当てられるリーフのレベルは同じである）。

【 0 0 8 2 】

尚、第1の方法は、第2の方法より、補完情報 $HK1'$ のデータ量が少なく済むという効果がある（図46に示す例においては、補完情報 $HK1'$ は、 $h(3, 0)$ のみ）。一方、第2の方法は、第1の方法より、実装上、第1次二分木を簡単に構成することができるという効果がある。

【 0 0 8 3 】

時刻証明公表部15は、時刻証明要求まとめ部12で作成された第2次二分木のルート値 H を定期的（上述した一定期間ごと）にメディア等40に公表するものである。

【 0 0 8 4 】

監査情報作成部17は、監査情報を第2次二分木から取得して監査装置5に送信するものであり、より詳しくは、監査情報とは、第2次二分木のリーフに設けられた監視点に基づいて、監視点の1次情報（第1次二分木のあるリーフに割り当てられた情報およびその1次補完情報の組み合わせをいう）、監視点に割り当てられた第1次二分木のルート値 H 、該第1次二分木のルート値 H の識別番号、即時2次補完情報、および監視点に付与された時刻情報を意味する。図3に示す具体例によれば、 $M(0, 10)$ が監視点となっているので、監査装置5に送信するデータは、 $M(0, 10)$ の一次情報、 $M(3, 0)$ 、 $M(1, 4)$ 、および $M(0, 10)$ に付与された時刻となる。

【 0 0 8 5 】

尚、図3の具体例においては、監視点は1つしか設けられていないが、所定のアルゴリズムに従って複数設けてよいのは勿論であり、また、監視点は時刻証明要求から作成されたルート値 H が割り当てられたリーフ（図3の具体例においては、 $M(r; 5)$ ）より、右側のリーフ（時間的に後）に割り当てられていればどこに設けていてもよいものである。従って、時刻証明要求が割り当てられる第2次二分木のリーフの位置に依存せずに、監視点を有効に機能させるためには、第2次二分木の各リーフそれぞれを監視点とするのが好適である。

【 0 0 8 6 】

クライアント装置3iは、コンピュータネットワーク4を介して時刻証明装置1および監査装置5とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置1からの時刻証明要求に対する受理証明書 $TSC(H, t)$ を記憶する受理証明書記憶部34、および受理証明書 $TSC(H, t)$ を検証する時刻証明検証部35を具備している。尚、時刻証明検証部35は、定期的にメディア等40に公表される公表情報を利用して検証を行う受理証明書に対する第1の検証機能と、メディア等公表前に監査装置5を利用して検証を行う受理証明書に対する第2の検証機能とを備えるものである。また、受理証明書が上述した区間証明書である場合には、時刻証明検証部35は、第1及び第2の検証に加えて、直前のラウンドの第1次二分木のルート値の検証を行う。これは、受理証明書に含まれる直前のラウンドの第1次二分木のルート値 H' と該ルート値 H' が割り当てられたリーフの1次補完情報 $HK1'$ から、現在のラウンドの第1次二分木のルート値を計算し、計算された該ルート値と受理証明書に含まれる第1次二分木のルート値が一致するか否かを検証するものである。

【 0 0 8 7 】

監査装置5は、コンピュータネットワーク4を介して時刻証明装置1およびクライアント装置3iとデータを送受信する送受信部51、時刻証明装置1から送信される監査情報を記憶する監査情報記憶部52、およびクライアント装置3iから受理証明書 $TSC(H, t)$ の検証要求を受けた際には、クライアント装置3iから送信された検証要求情報および監査情報記憶部52に記憶されている監査情報を用いて受理証明書 $TSC(H, t)$ の検証を行い、その結果をクライアント装置3iに返信する時刻証明検証部53を具備している。

【 0 0 8 8 】

ここで、時刻証明検証部53の機能について、図3の具体例を用いて説明する。図3の具体例においては、 $M(0, 10)$ が監視点となっているので、この時点において監査装置5が受け取

10

20

30

40

50

っている監査情報は、上述した通り、 $M(0,10)$ の1次情報、 $M(3,0)$ および $M(1,4)$ である。一方、クライアント装置3iは、検証要求情報として、 $M(0,5)$ の1次情報、2次補完情報として $M(0,4)$ 、 $M(1,3)$ 、および $M(2,0)$ を送信するものである。これは、クライアント装置3iが検証を求める時点（即ち、受理証明書 $TSC(H,t)$ が発行された $M(0,5)$ の時点より後刻である $M(0,10)$ の時点）においては、即時2次補完情報に含まれていなかった $M(1,3)$ も時刻証明装置1から取得することが可能であるので、 $M(1,3)$ をオンライン補完証明書として時刻証明検証要求者が時刻証明装置1から取得し、検証要求情報に含めたものである。

【0089】

そして、時刻証明検証部53は、自己が有している監査情報 $M(3,0)$ が、クライアント装置3iから送信された検証要求情報から計算された $M(3,0)$ と一致するか否かを検証するものである。ここで、比較検証の対象となる第2次二分木のノード（図3の具体例においては、 $M(3,0)$ ）を以後、認証点とよぶ。尚、一般に、クライアント装置3iから送信された時刻証明要求から作成されたルート値Hが割り当てられた第2次二分木のリーフ（対象点とよぶ）の番号が監視点であるリーフの番号より小さい場合、認証点のラベルは監査情報に含まれており、また、監視点における時刻証明処理が終了した時点において、クライアント装置3iが受信できる1次情報および2次補完情報から作成されるラベルには、認証点のラベルが含まれるので、上記検証は常に実施可能なものであるが、この理由に関しては後述する。

【0090】

また、時刻証明検証部53は、受信した監査情報に付された時刻および受理証明書 $TSC(H,t)$ に付された時刻の真正性を検証する機能を有している。ここで、前者は、監査情報を受信した時刻（自己の参照する時計から取得）と監査情報に付された時刻の差が一定の限度内か否かを検証するものである。これに対して、後者は、前者の監査情報に付されている時刻が正しいときには、監査点に付与された時刻がわかるので、この監査点から受理証明書 $TSC(H,t)$ に付されるべき時刻を所定の単位時間間隔過去に遡ることにより算出し（例えば、図3に示す具体例においては、 $M(0,5)$ を含む受理証明書の検証要求を受けたとき、 $M(0,5)$ を含む受理証明書 $TSC(H,t)$ に付される時刻T1は、監査点に付与された時刻Tより、5単位時間間隔、過去にあるはずである）、該算出した時刻と受理証明書 $TSC(H,t)$ に実際に付された時刻の差が一定の限度内か否かを検証するものである。

【0091】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、時刻証明装置1の時刻証明要求まとめ部12、時刻情報取得部13、時刻証明作成部14、時刻証明公表部15および監査情報作成部17、クライアント装置3iの時刻証明要求部33および時刻証明検証部35、並びに監査装置5の時刻証明検証部53の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、時刻証明装置1の受理証明書記憶部16、クライアント装置3iのメッセージ記憶部32および受理証明書記憶部34、並びに監査装置5の監査情報記憶部52は、上記主記憶装置の機能を備えたものである。

【0092】

次に、以上の構成を有するタイムスタンプ・システム100における時刻証明方法、および時刻証明検証方法を図6乃至図9を用いて説明する。ここで、図6は、一公表サイクルにおいて時刻証明装置1が受理証明書 $TSC(H,t)$ を作成する動作を説明するシーケンス図であり、図7は、監査装置5が監査情報の検証を行う動作を説明するフローチャートであり、図8および図9は、クライアント装置3iが受理証明書 $TSC(H,t)$ の検証を行う動作を説明するフローチャートおよびシーケンス図である。

【0093】

但し、ここで検証を行うクライアント装置3iを使用する利用者30は、検証の対象となる受理証明書 $TSC(H,t)$ を要求し取得した時刻証明要求者、及びこの時刻証明要求者から受理

10

20

30

40

50

証明書TSC(H, t)を渡された時刻証明検証者の双方が考えられる。

【0094】

まず、時刻証明方法について説明する。クライアント装置3i が時刻証明装置1にメッセージ・ダイジェストyを含む時刻証明要求を送信すると、時刻証明装置1は送受信部11を介して、メッセージ・ダイジェストyを含む時刻証明要求を受信し、時刻証明要求まとめ部12が、このメッセージ・ダイジェストyを第1次二分木のリーフに割り当てる(ステップS11, S12, S13)。そして、同一ラウンド内においては、複数のクライアント装置3iから受信した複数の時刻証明要求に対して、第1次二分木への割り当てが所定の手順に従って行われ、単位時間経過後ラウンドが終了すると、時刻証明要求まとめ部12がそれぞれのリーフに割り当てられたメッセージ・ダイジェストから第1次二分木のルート値Hを計算する(ステップS14, S15)。

10

【0095】

次に、時刻証明要求まとめ部12が、第1次二分木のルート・ハッシュ値Hを第2次二分木のリーフに割り当てて、インクリメンタルに第2次二分木を構成していくとともに、時刻証明作成部14は、クライアント装置3iから送付されたメッセージ・ダイジェストy、第1次二分木のルート・ハッシュ値H、該ルート・ハッシュ値Hの識別番号n、時刻t、1次補完情報HK1、および2次補完情報HK2を含む受理証明書TSC(H, t)を作成し、送受信部11を介してクライアント装置3iに受理証明書TSC(H, t)を送信する(ステップS16, S17, S18)。

【0096】

20

これにより、クライアント装置3iは、受理証明書TSC(H, t)を取得することができる(ステップS19)。尚、受理証明書TSC(H, t)に含まれる2次補完情報には、この時点において取得できる即時2次補完情報は含まれているが、後付2次補完情報は含まれていない。

【0097】

次に、第1次二分木のルート値Hが割り当てられた第2次二分木のリーフが、監視点である場合には、監査情報作成部17が監査情報を作成し、この監査情報を送受信部11を介して監査装置5に送信する(ステップS20, S21, S22)。これにより、監査装置5は、監査情報を取得することができる(ステップS23)。ここで、監査装置5は、図7に示すように、監査情報に付与された時刻値のチェックを行う。これは、監査装置5が当該監査情報を受信した時刻t1を自己が参照する時計から取得し、該時刻t1と、監査情報に付与された時刻時刻t'とを比較し、時刻差が、予め定められた限界値(例えば1秒)以内であれば、当該監査情報は時刻について正しいとみなすものである(ステップS301, S302, S303, S304)。尚、監査装置5が参照する時計は標準時にトレーサブルであることが望ましい。

30

【0098】

そして、一定期間内においては、上述した時刻証明装置1の動作は繰り返され、一定期間が終了すると、時刻証明作成部14は、送受信部11を介して、クライアント装置3iに後付2次補完情報を含む補完証明書を送信する(ステップS24, S25)。これにより、クライアント装置3iは、受理証明書TSC(H, t)とそのすべての2次補完情報を取得したことになる(ステップS26)。また、時刻証明公表部15は、第2次二分木のルート値RHを計算し、このルート値RHをメディア等40に公表する(ステップS27, S28)。

40

【0099】

次に、メディア等40に公表された公表情報を用いた時刻証明検証方法について説明する。これは、クライアント装置3iの第1の検証機能に相当するものである。

【0100】

まず、クライアント装置3iは、自己が時刻証明装置1に時刻証明要求として送信したメッセージ・ダイジェスト、並びに受信した受理証明書TSC(H, t)及び補完証明書に含まれている1次補完情報および2次補完情報(この時点においては、すべての2次補完情報を具備している)、から第2次二分木のルート値RHcalを計算する(ステップS31)。

【0101】

50

次に、メディア等40に公表されている同一公表サイクルのルート値RHを取得し、このルート値RHが、計算したルート値RHcal に一致するか否か検証する（ステップS32, S33）。

【0102】

以上の検証において、検証に成功すれば、受理証明書 TSC(H,t) が改ざんされていないことを確認することができる（ステップS34）。一方、検証に失敗すれば、受理証明書 TSC(H,t) が改ざんされていることを確認することができる（ステップS35）。これにより、メディア等公表後においては、公表された情報を利用して、時刻証明装置1が発行した受理証明書 TSC(H,t) を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

10

【0103】

次に、監査装置5を用いた時刻証明検証方法について説明する。これは、クライアント装置3iの第2の検証機能に相当するものである。

【0104】

まず、クライアント装置3iが、検証する時点における後付2次補完情報を含むオンライン補完証明書を時刻証明装置1に要求する（ステップS41）。この要求を時刻証明装置1が送受信部11を介して受信すると、時刻証明作成部14は、後付2次補完情報の一部（この時点において取得できる後付2次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置3iに送信する（ステップS42, S43, S44）。これにより、クライアント装置3iは、オンライン補完証明書を取得するので、時刻証明検証部35は、これに既に受け取っている受理証明書TSC(H,t)（1次情報および即時2次補完情報、並びに受理証明書TSC(H,t)に付された時刻）を加えた検証要求情報を監査装置5に送信する（ステップS46）。

20

【0105】

次に、監査装置5が検証要求情報を送受信部51を介して受信すると、時刻証明検証部53は、この検証要求情報から認証点のラベル値Acalを計算する（ステップS47, S48）。一方、時刻証明検証部53は、監査情報として既に受け取っているこの認証点のラベル値Aを監査情報記憶部52から取得して、この認証点のラベル値Aが、計算により求めた認証点のラベル値Acalに一致するか否かを検証する（ステップS49）。そして、この検証に成功した場合には、受理証明書TSC(H,t)に付された時刻の真正性についても検証する（ステップS50, S51）。これは監査情報に付された時刻から受理証明書TSC(H,t)に付されるべき時刻を算出し、該算出した時刻と受理証明書に付された時刻との差が一定時間内か否かを検証するものである。尚、受理証明書TSC(H,t)に付された時刻の真正性についての検証は、監査情報の時刻が正しいと検証された場合（ステップS303）を前提に行われるものである。

30

【0106】

以上の検証それぞれにおいて、検証に成功すれば、受理証明書TSC(H,t)が改ざんされていないことに加えて、当該の受理証明書TSC(H,t)に付された時刻の真正性についても確認することができる（ステップS52）。一方、いずれかの検証に失敗すれば、受理証明書 TSC(H,t) が改ざんされていること、もしくは受理証明書TSC(H,t)に付された時刻が不正であることを確認することができる（ステップS53）。そして、時刻証明検証部53は、この検証結果を送受信部51を介してクライアント装置3iに送信する（ステップS54, S55）。これにより、メディア等公表前においても、時刻証明装置1が発行した受理証明書 TSC(H,t) を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

40

【0107】

以上、第1の実施の形態のタイムスタンプ・システム100によれば、クライアント装置3iから時刻証明要求を受け付けた時刻証明装置1が、第1次二分木を用いて時刻証明要求をまとめ、このまとめた値に対して時刻情報を付した受理証明書TSC(H,t)を発行し、第2次二分木のルート値をメディア等40に公表するので、デジタル署名を用いない、又はデジタル署名を主要な手段としないタイムスタンプ・システムであっても、クライアント装置

50

3i は公表情報および補完情報から簡単に受理証明書TSC(H, t)の検証をすることができる。また、第2次二分木のルート値をメディア等40に公表する前であっても、監査装置5が第2次二分木の監視点に関する監査情報を有しているので、監査装置5はクライアント装置3iからの検証要求を受けて、受理証明書TSC(H, t)の検証をすることができる。

【0108】

尚、第1の実施の形態のタイムスタンプ・システム100は、上述した形態に限定されるものではなく、受理証明書に含まれる補完情報のパターン、監査情報に含まれる補完情報のパターン、監視点の決定方法、監査機関の選択方法、補完証明書の種類などについて種々のバリエーションを施すことが可能である。以下、このことについて説明する。

【0109】

まず、受理証明書に含まれる補完情報のパターンについて説明する。

【0110】

本実施の形態の受理証明書は、1次補完情報および即時2次補完情報を含める方式であったが、受理証明書に含める補完情報（以下、受理証明書内補完情報という。）については、以下に述べるような3つの方式の中から、状況に応じて利点のある方式を採用することができるものである。

【0111】

タイプ0の受理証明書内補完情報は、第1次二分木のルート値と、第1次二分木における補完情報（1次補完情報）のみを含むものとする。

【0112】

タイプ1の受理証明書内補完情報は、上記タイプ0の情報と、第2次二分木のルート値を計算するための補完情報（2次補完情報）を含むものとする（これは、上述した本実施の形態で採用された方式である）。

【0113】

タイプ2の受理証明書内補完情報は、公表間隔の中の、指定された時刻あるいは第1次二分木のルート値の識別番号以降に取得できる全ての第1次二分木のルート値（第2次二分木のリーフ値）を含むものとする。

【0114】

通常の場合においては、クライアント装置3iで第2の検証を行うためには、タイプ1の情報があれば十分である。また、タイプ0の受理証明書内補完情報を採用した場合においては、時刻証明装置1が、タイプ1の情報に含まれタイプ0の情報には含まれない補完情報をクライアント装置3iの要求に応じて提供することにより、クライアント装置3iで第2の検証を行うことが可能である。

【0115】

上記のようにクライアント装置3iで第2の検証を行うためにはタイプ0の受理証明書内補完情報を採用することも可能であるが、タイプ1の受理証明書内補完情報を採用することにより、該公表期間内に、当該の受理証明書より前に発行された他の受理証明書とリンクする情報を取得できるという利点がある。この利点を生かす例としては、クライアント装置3iが、タイプ1の受理証明書内補完情報を取得することにより、必要ならば、図9における監査装置5の役割を実行することが可能となることが挙げられる。具体的には、あるクライアント装置3aが時刻証明を要求したのがある時刻 t より前であることを、他のクライアント装置3bが時刻証明装置1や監査装置5に頼ることなく検証することが以下のように可能となる。まず、クライアント装置3bは、時刻 t において時刻証明装置1に対して時刻証明要求を送付し、それに対する受理証明書 TSC(H, t) を受信するものとする。但し、受理証明書 TSC(H, t) にはタイプ1の受理証明書内補完情報がふくまれているものとする。その後、クライアント装置3bは、他のクライアント装置3aに対して、クライアント装置3aが受信した受理証明書TSC(H, t)とオンライン補完証明書を含む検証に必要なデータを自己に送付させ、さらにクライアント装置3bは、図9における監査装置5の役割を実行するものである。そして、ステップS49の判定で YES と判断されれば、時刻 t 以前にクライアント装置3aが時刻証明要求をしたことが、他のクライアント装置3

10

20

30

40

50

bにより確認されるものである。

【0116】

これに対して、タイプ2の受理証明書内補完情報は、ある公表期間の途中で事故等によりTSA10のサービスが中止した場合でも、該公表期間内に、当該の受理証明書より前に発行された他の受理証明書とリンクする情報を取得できるという利点があるものである。

【0117】

第2次二分木を示す図3を参照して、タイプ2の受理証明書内補完情報について説明する。ここで、クライアント装置3iが受け取る第1次二分木のルート・ハッシュ値を $M(0,5)$ とする。このとき、タイプ2の受理証明書内補完情報は、指定された識別番号が2のとき、 $[M(0,2), M(0,3), M(0,4)]$ となる。そして、クライアント装置3iは上記の受理証明書内補完情報を受信していれば、たとえTSA10が受理証明書受信後に破綻したとしても、受理証明書が正しいことを検証することができる（例えば、他のクライアント装置3iが受け取った第1次二分木のルート・ハッシュ値 $M(0,2)$ と、受理証明書に含まれた $M(0,2)$ が一致すれば、自己の受理証明書が正しいことを検証できる）。

【0118】

ところで、クライアント装置3iにおいては、どのタイプの受理証明書内補完情報を受理証明書と同時に受信するかを、利用者30とTSA10との契約により指定することができる。尚、受理証明書内補完情報と補完証明書に含まれる補完情報は相関があるものであり、例えば、タイプ1又は2の受理証明書内補完情報を受信する契約をしている場合には、補完証明書として後付の2次補完情報を受信することになり、また、タイプ0の受理証明書内補完情報を受信する契約をしている場合には、補完証明書として2次補完情報すべてを受信することになる。また、契約とは別に、時刻証明要求時のオプションにより、受理証明書内補完情報を指定できるようにしてもよいものである。また、クライアント装置3iは、第2の検証を行うために、オンライン補完証明書を要求することができるものであるが、その際、タイプ1の受理証明書内補完情報を取得していた場合には、受理証明書発行以後に確定した2次補完情報を受信すればよいが、タイプ0の受理証明書内補完情報を取得していた場合には、その時点で確定している2次補完情報の全てを受信する必要がある。

【0119】

さらに、クライアント装置3iは、クライアント装置3iからの要求時にのみ補完証明書を受信するという契約（補完証明書を公表間隔終了時に受信しない）をしてもよいものであり、この場合には、2次補完情報は、直前に終了した公表間隔の間に発行された受理証明書の補完証明書のみではなく、さらに遡って過去に発行された受理証明書に対応する補完証明書を要求することも可能となるものである。

【0120】

ここで、一般にTSA10の提供する時刻証明サービスの契約者は、個人の場合もあるし組織/法人の場合もあるが、いずれにせよ、契約者が時刻証明サービスを使用する契約をする際には、アカウントが発行され、契約者はこのアカウントを用いて、時刻証明サービスを受けることになる。その際、パスワード等の認証用の情報が発行されるのが普通である。従って、各契約者は契約時に、その契約者のアカウントを用いて為された時刻証明要求に対する補完証明書の送付先を指定することができるが、これは、例えば、電子メールのアドレスなどの電子的手段の他、郵送の宛先など電子的でない手段もありえるものである。

【0121】

次に、上記補完証明書の種類について説明する。

【0122】

公表間隔の間に、ある契約者に対して発行される受理証明書は一般に複数あると考えられる。このような場合、契約者に対して送信されるデータ量の合計を考慮すると、複数の受理証明書に対する補完証明書のデータ構成は次の2つの種類が考えられる。以下において、Nは公表間隔の間に計算する、第1次二分木のルート値の個数である。

【0123】

第1は、本実施の形態において説明した簡約型の補完証明書であり、公表用データである第2次二分木のルート値を再構成するのに必要な、最小限の補完情報を含めるものである（2次補完情報の個数は、各受理証明書に対して $\log_2(N)$ ）。例えば、図3において、時刻証明要求の第1次二分木ルート値が $M(0,5)$ の場合には、 $M(0,4)$ 、 $M(1,3)$ 、 $M(2,0)$ 、 $M(3,1)$ ）。第2は、列挙型の補完証明書であり、公表間隔の間に発行した受理証明書の第1次二分木のルート値を全て含めるものである（2次補完情報の個数は N 。図3の場合においては、 $M(0,0)$ 、 $M(0,1)$ 、...、 $M(0,15)$ ）。

そして、契約者は契約時に、上記2つの種類の補完証明書のうち、どちらかを選択して指定できるようになっている。ここで、契約に際しては、1つの公開期間の間に、時刻証明サービスのある契約者が受領する受理証明書の数が、一定の限度より少ないときには簡約型の補完証明書の方がデータ量が小さいが、その限度を超えると列挙型の補完証明書の方がデータ量が小さくなるので、契約者は受領する受理証明書の数に応じて最適な方式を選択すればよい。

【0124】

尚、クライアント装置3iが、列挙型の補完証明書を用いて第1の検証を行う場合には、図8のステップS31において列挙型の補完証明書に記載されている第1次二分木のルート値の識別番号、及び第1次二分木のルート値から、第2次二分木のルート値を計算する。

【0125】

次に、監査情報に含まれる補完情報のパターンについて説明する。

【0126】

本実施の形態の監査情報は、1次補完情報および即時2次補完情報を含める方式であったが、監査情報に含める補完情報（以下、監査情報内補完情報という。）については、以下に述べるような3つの方式の中から、状況に応じて利点のある方式を採用することができるものである。

【0127】

タイプ0の監査情報内補完情報は、監視点の1次情報（第1次二分木のあるリーフに割り当てられた情報およびその1次補完情報の組み合わせをいう）からなる。

【0128】

タイプ1の監査情報内補完情報は、上記タイプ0の情報と、第2次二分木のルート値を計算するための補完情報（2次補完情報）を含むものとする（これは、上述した本実施の形態で採用された方式である）。

【0129】

タイプ2の受理証明書内補完情報は、公表間隔の中の、指定された時刻あるいは第1次二分木のルート値の識別番号以降に取得できる全ての第1次二分木のルート値（第2次二分木のリーフ値）を含むものとする。

【0130】

タイプ0の監査情報内補完情報を採用する場合、ある監査装置5は、自己の担当する監視点に属する受理証明書に対してのみ、クライアント装置3iからの時刻証明検証要求に応じることができる。これは、第2次二分木において監視点と時刻証明要求点が一致するのであれば、クライアント装置3iが受け取る受理証明書に含まれる受理証明書内補完情報と、監査装置5が受け取る監査情報内補完情報との一致を検証することにより、受理証明書の検証ができるからである。従って、任意の時刻証明検証要求にどれかの監視/監査機関が確実に応じるためには、全ての単位時間（すべての第2次二分木のリーフ）がなんらかの監視/監査機関の監視点となっている必要がある。

【0131】

通常の場合においては、公表期間の終了前にあるクライアント装置3iが受信した受理証明書の内容を監査装置5が受信した監査情報とリンクし、時刻証明検証を行うためには、タイプ1の情報があれば十分である。

【0132】

タイプ2の受理証明書内補完情報は、上述した受理証明書内補完情報の場合と同様に、

10

20

30

40

50

通常の状況において時刻証明検証を行うためには必要ないが、ある公表期間の途中で事故等によりTSA10のサービスが中止した場合でも、該公表期間内に、当該の受理証明書より前に発行された受理証明書に対して時刻証明検証を行うことができるという利点があるものである。

【 0 1 3 3 】

第2次二分木を示す図3を参照して、タイプ2の監査情報内補完情報について説明する。ここで、監査装置5が受け取る第1次二分木のルート・ハッシュ値を $M(0,5)$ とする。このとき、タイプ2の監査情報内補完情報は、指定された識別番号が2 のとき、 $[M(0,2)$ 、 $M(0,3)$ 、 $M(0,4)]$ となる。そして、監査装置5は上記の監査情報内補完情報を受信していれば、たとえTSA10が監査情報受信後に破綻したとしても、受理証明書が正しいことを検証

10

【 0 1 3 4 】

また、本実施の形態の監査情報は、時刻証明装置1から監査装置5に自動的に送信される方式であったが、これとは異なり、監査装置5の方から監査情報の送信を時刻証明装置1に要求し、監査情報を受信することができるようにしてもよい。そして、いずれの方式においても、監査装置5にどのタイプの監査情報内補完情報を送信するかは、当該の監視／監査機関とTSA10の事前の契約により定められるものである。また、監査装置5の方から監査情報の送信を時刻証明装置1に要求し、監査情報を受信する方式においては、契約

20

【 0 1 3 5 】

尚、上記で説明した受理証明書に含まれる補完情報のパターン、及び監査情報に含まれる補完情報のパターンは、それぞれ組み合わせが可能であるが、例えば、受理証明書に含まれる補完情報のタイプ0、監査情報に含まれる補完情報のタイプ2の組み合わせの場合には、第2の検証を行うに際して、オンライン補完証明書は不要となるものである。これは、監査装置5がタイプ2の監査情報（監視点以前の第2次二分木のリーフ値すべて、即ち、第1次二分木のルート値すべて）を備えているので、この中にクライアント装置3iが受信した受理証明書に含まれる第1次二分木のルート値と同一のものがあるか否か検証

30

【 0 1 3 6 】

次に、監視点の決定方法について説明する。

【 0 1 3 7 】

第2次二分木のどのリーフ（どの単位時間間隔）を監視点とするかは、例えば、以下の3つの方式が考えられるもので、どの方式も本実施の形態に適用可能なものである。

【 0 1 3 8 】

方式1： 全ての単位時間間隔を監視点とする。

【 0 1 3 9 】

方式2： M と m を予め定められた整数とし、 $0 < m < M$ を満たすものとし、当該の単位時間間隔を表す時刻値を所定の方法で整数に変換し、その結果を x とする。

40

【 0 1 4 0 】

$x \bmod M = m$ の時、当該の単位時間間隔を監視点とする。

【 0 1 4 1 】

ここで、 M が大きくなれば、監視される単位時間間隔の割合が減少し、それに応じて安全度も減少し、また監視のためのコストも減少する。 M の決め方は、求められる安全度と監視のためのコストを勘案して決める必要がある。

【 0 1 4 2 】

方式3：上記と同様に M と m を定める。この単位時間間隔に構成される第1次二分木のルートのラベル値を v とすると、所定の方法で v を整数 w に変換する。

50

【0143】

$w \bmod M = m$ の時、当該の単位時間間隔を監視点とする。

【0144】

次に、監査装置5の選定方法について説明する。

【0145】

本実施の形態においては、受理証明書に対応する監査情報を送信した監査装置5に対して、クライアント装置3iは監査要求を行うことを前提として説明し、監査装置5の選定については特に記載しなかった。以下においては、監視／監査機関が複数ある場合に特定の監査機関を選定するアルゴリズムについて説明するが、該アルゴリズムは、ある監視点において監査情報が送信される監査装置5を前もって予想することが困難であるようなものが望ましく、例えば、以下の方式が考えられる。

10

【0146】

方式1：

(1) 監査機関の全体の個数を N とし、各監査機関には 0 から $N-1$ までの番号を割り当てる。

【0147】

(2) 第1次二分木のルート値を所定の方法で整数に変換し、その値を x とし、 $x \bmod N$ を計算して i とおき、 i を番号とするような監査機関を選ぶ。

【0148】

そして、このようにして選ばれた監査機関の監査装置5に監査情報を送信する。

20

【0149】

また、1つの監視点において監査情報が送信される監査装置5は複数であってもよいとすると、例えば以下の方式が考えられる。

【0150】

方式2：

(1) 上記と同じく、監査機関の全体の個数を N とし、各監査機関には 0 から $N-1$ までの番号を割り当てる。

【0151】

(2) $1 \leq N' < N$ となるような N' を選ぶ。

【0152】

(3) 第1次二分木のルート値を所定の方法で整数に変換し、その値を x とし、 $x \bmod N'$ を計算して i とおき、 $n \bmod N' = i$ となるような番号 n を割り当てられた複数の監査機関を選ぶ。

30

【0153】

そして、このようにして選ばれた監査機関の監査装置5に監査情報を送信する。

【0154】

尚、上述の監査機関選定のアルゴリズムは、クライアント装置3iにも組み込まれているもので、これにより、クライアント装置3iは、時刻証明装置1と同様に第1次二分木のルート値から、監査を依頼すべき監査装置5を特定できるようになっている。

【0155】

尚、第1の実施の形態においては、TSA10が、公開期間を定め、各公開期間における第2次二分木を構成し、そのルートに割り付けられた値を、公開メディア等に公開することを前提としていたが、この方法以外に、監査機関が、既に終了した公開期間に発行された受理証明書に対応することも含めて、長期に渡って受理証明書の保証書の発行を続けることにより、第2次二分木のルートの値を公開メディア等などに公表することを前提としない方式としてもよい。

40

【0156】

< 第2の実施の形態 >

図10は、本発明の第2の実施の形態に係るタイムスタンプ・システム200のシステム構成図である。同図に示すタイムスタンプ・システム200は、TSA10に設けられた時刻証

50

明装置1、T A 20に設けられ、タイムスタンプ生成に使用される時刻情報を提供する時刻情報提供装置2、利用者30が利用する複数のクライアント装置203 i (i は自然数)、監視 / 監査機関に設けられ、時刻証明装置1が発行した受理証明書に関する監査情報を公表する監査装置6、及び以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置1がクライアント装置203 i からのタイムスタンプ要求 (時刻証明要求) に応えて、タイムスタンプつき受理証明書をクライアント装置203 i に返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置203 i は、時刻証明装置1がメディア等40に公表した情報、又は、監査装置5から公表された監査情報によって受理証明書を検証できるようになっているコンピュータシステムである。

10

【 0 1 5 7 】

尚、上記コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

【 0 1 5 8 】

即ち、タイムスタンプ・システム100においては、監査装置5はクライアント装置3 i の検証要求を受け付けて自ら検証を行っていたが、タイムスタンプ・システム200においては、監査装置6は監査情報を公開するだけであり、クライアント装置203 i が自ら検証を行うようになっており、この点が両タイムスタンプ・システムの相違点となっている。尚、本実施の形態においては、第 1 の実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

20

【 0 1 5 9 】

監査装置6は、コンピュータネットワーク4を介して時刻証明装置1およびクライアント装置203 i とデータを送受信する送受信部51、時刻証明装置1から送信された監査情報を記憶する監査情報記憶部52、およびこの監査情報をWeb上に公開する監査情報公開部63を具備している。

【 0 1 6 0 】

クライアント装置203 i は、コンピュータネットワーク4を介して時刻証明装置1および監査装置6とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置1からの時刻証明要求に対する受理証明書TSC(H, t) を記憶する受理証明書記憶部34、および受理証明書TSC(H, t) を検証する時刻証明検証部36を具備している。尚、時刻証明検証部36は、定期的にメディア等40に公表される公表情報を利用して検証を行う第 1 の検証機能と、メディア等公表前に監査装置6を利用して検証を行う第 2 の検証機能とを備えるものである。

30

【 0 1 6 1 】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置 (C P U : Central Processing Unit)、プログラムやデータを収納する機能を有する R A M (Random Access Memory) 等からなる主記憶装置 (メモリ) を有する電子的な装置から構成されている。このうち、監査装置6の監査情報公開部63、およびクライアント装置203 i の時刻証明検証部36の処理は、上記 C P U による演算制御機能を具体的に示したものに他ならない。

40

【 0 1 6 2 】

次に、以上の構成を有するタイムスタンプ・システム200における時刻証明検証方法を図11を用いて説明する。ここで、図11は、時刻証明装置1が第 2 次二分木のルート値RHをメディア等40に公表する前に、クライアント装置203 i が受理証明書TSC(H, t) の検証を行う動作 (クライアント装置203 i の第 2 の検証機能に相当する) を説明するシーケンス図である。尚、タイムスタンプ・システム200における時刻証明方法、監査装置5が監査情報の検証を行う動作、およびメディア等公表後にクライアント装置203 i が受理証明書TSC(H, t) の検証を行う動作 (クライアント装置203 i の第 1 の検証機能に相当する) は、第 1 の実施の形態と同様であるため、説明を省略する。

50

【 0 1 6 3 】

但し、ここで検証を行うクライアント装置203iを使用する利用者30は、検証の対象となる受理証明書TSC(H, t)を要求し取得した時刻証明要求者、及びこの時刻証明要求者から受理証明書TSC(H, t)を渡された時刻証明検証者の双方が考えられる。

【 0 1 6 4 】

まず、クライアント装置203 i が、検証する時点における後付 2 次補完情報を含むオンライン補完証明書を時刻証明装置1に要求する（ステップ S 61）。この要求を時刻証明装置1が送受信部11を介して受信すると、時刻証明作成部14は、後付 2 次補完情報の一部（この時点において取得できる後付 2 次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置203 i に送信する（ステップ S 62, S 63, S 64）。

10

【 0 1 6 5 】

これにより、クライアント装置203 i は、オンライン補完証明書を取得するので、時刻証明検証部36は、これに既に受け取っている 1 次情報および即時 2 次補完情報を加えて、当該の受理証明書に対応する第 2 次二分木のリーフから該第 2 次二分木のルートに向かうパスに属するノードのラベル値のうち計算可能なものを計算する（ステップ S 65, S 66, S 67）。

【 0 1 6 6 】

次に、時刻証明検証部36は、監査装置6から公開されている監査情報の中から自己の受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第 1 次二分木のルート値の識別番号と等しいか、あるいは大きい第 1 次二分木のルート値の識別番号を含むような）監査情報が存在するか否かを確認する（ステップ S 68, S 69）。尚、監査情報は、図 7 に示す監査情報の時刻検証において監査情報に付された時刻が正しい場合（ステップ S 303）に、公開されるものである。

20

【 0 1 6 7 】

このような監査情報 $AI(H', t')$ が Web上に存在する場合には、該監査情報（該監査情報による、当該の受理証明書に対する認証点のラベル値、及び監査情報に付された時刻値を含むもの）を取得し、そこに含まれる認証点のラベル値 A と、上記計算（ステップ S 65, S 66, S 67）により求めた認証点のラベル値 A_{cal} とが一致するか否かを検証し、この検証に成功した場合には、受理証明書TSC(H, t)に付された時刻の真正性についても検証する（ステップ S 70, S 71, S 72, S 73）。これは監査情報 $AI(H', t')$ に付された時刻から受理証明書TSC(H, t)に付されるべき時刻を算出し、該算出した時刻と受理証明書TSC(H, t)に付された時刻との差が一定時間内か否かを検証するものである。

30

【 0 1 6 8 】

以上より、監査装置6に受理証明書TSC(H, t) の検証に利用可能な（即ち、該受理証明書に含まれる第 1 次二分木のルート値の識別番号と等しいか、あるいは大きい第 1 次二分木のルート値の識別番号を含むような）監査情報 $AI(H', t')$ が存在し、かつそれぞれの検証において、検証に成功すれば、受理証明書 TSC(H, t) が改ざんされていないことに加えて、当該の受理証明書TSC(H, t)に付された時刻の真正性についても確認することができる（ステップ S 74）。一方、いずれかの検証に失敗、もしくは監査装置 6 に受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第 1 次二分木のルート値の識別番号と等しいか、あるいは大きい第 1 次二分木のルート値の識別番号を含むような）監査用情報が存在しない場合には、受理証明書 TSC(H, t) が改ざんされていること、もしくは受理証明書TSC(H, t)に付された時刻が不正であることを確認することができる（ステップ S 75）。これにより、メディア等公表前においても、時刻証明装置1が発行した受理証明書TSC(H, t)を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

40

【 0 1 6 9 】

以上、第 2 の実施の形態のタイムスタンプ・システム200によれば、第 1 の実施の形態のタイムスタンプ・システム100と同様の効果を得ることができる。加えて、本実施の形態においては、メディア等40に公表する前であっても、クライアント装置203 i 自らで受

50

理証明書TSC(H, t)の検証をすることができる。

【0170】

尚、第2の実施の形態のタイムスタンプ・システム200は、上述した形態に限定されるものではなく、第1の実施の形態のタイムスタンプ・システム100に施すことが可能であった種々のバリエーションをタイムスタンプ・システム200に適用することが可能なものである。

【0171】

<第3の実施の形態>

図12は、本発明の第3の実施の形態に係るタイムスタンプ・システム300のシステム構成図である。同図に示すタイムスタンプ・システム300は、T S A 10に設けられた時刻証明装置7、利用者30が利用する複数のクライアント装置303 i (i は自然数)、監視 / 監査機関に設けられ、時刻証明装置7が発行した受理証明書に関する監査情報を公表する監査装置8、時刻タグを供給する時刻タグシステム800、および以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置7がクライアント装置303 i からのタイムスタンプ要求 (時刻証明要求) に応えて、タイムスタンプつき受理証明書をクライアント装置303 i に返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置303 i は、時刻証明装置7がメディア等40に公表した情報、又は、監査装置8から公表された監査情報によって受理証明書を検証できるようになっているコンピュータシステムである。

【0172】

また、タイムスタンプ・システム300は、時刻のトレーサビリティを確保する役割を時刻タグシステム800に集約しているので、T S A 10は時刻のトレーサビリティを確保する必要がなく、さらに、時刻証明装置7が付与する時刻が本来の時刻より、過去の時刻になることを確実に防止することができるコンピュータシステムとなっている。尚、時刻タグ τ とは、所定の方法と手段により生成される乱数 (但し、時刻タグ供給サービスの継続期間の間に、乱数の衝突を起こす確率が無視できる程度のビット長を有する) であり、時刻タグシステム800を介して、各時刻タグに対応する時刻値を取得することができるものである。また、本実施の形態においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【0173】

時刻タグシステム800は、時刻タグ作成業者801が作成した時刻タグ τ をデジタル放送業者に802に提供すると、デジタル放送業者802は、この時刻タグ τ を時刻タグ認証業者803および時刻証明装置7に供給するようになっている。また、時刻タグ認証業者803は、受け取った時刻タグ τ と時刻源である時刻情報提供装置2から提供される時刻値を対応付けて管理しているので、監査装置8から時刻タグ τ と時刻値との対応に関する問い合わせがあった場合には、監査装置8に時刻タグ τ に対応する時刻値を回答できるようになっている。

【0174】

時刻証明装置7は、コンピュータネットワーク4を介して監査装置8、クライアント装置303 i、および時刻タグシステム800とデータを送受信する送受信部11、受理証明書に使用する時刻タグ τ を時刻タグシステム800から取得する時刻タグ情報取得部73、複数のクライアント装置303 i からの時刻証明要求として送信されたメッセージ・ダイジェスト (デジタル・データから作成されるハッシュ値) および時刻タグ情報取得部73で取得した時刻タグ τ を二分木を用いてまとめる時刻証明要求まとめ部72、受理証明書を作成する際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部72でまとめられたメッセージ・ダイジェストに対して時刻情報取得部13で取得した時刻情報を付して受理証明書を作成する時刻証明作成部14、定期的にメディア等40にデータを公表する時刻証明公表部15、時刻証明作成部14で作成された受理証明書を記憶する受理証明書記憶部16、および監査装置8に送信する監査情報 (監査用受理証明書) を作成する監査情報作成部77を具備している。

【 0 1 7 5 】

尚、ここで、時刻証明要求まとめ部72は、クライアント装置303iから送信されたメッセージ・ダイジェストに加えて時刻タグシステム800から取得した時刻タグ τ を第1次二分木のリーフに割り当てる点が時刻証明要求まとめ部12と異なっている。即ち、時刻タグ τ は、第1次二分木の所定のリーフ（予め定められた方法に従って、少なくとも1箇所以上）に、メッセージ・ダイジェストの代わりに割り付けられ、メッセージダイジェストと同様に扱われるものである。これにより、第1次二分木のリーフは、メッセージダイジェスト又は時刻タグが割り当てられる。

【 0 1 7 6 】

また、監査情報作成部77は、作成する監査情報（監査用受理証明書）の構成において、監査情報作成部17と異なっているものである。より詳しくは、本実施の形態における受理証明書 $TSC(H, t)$ は、第1次二分木のルート値 H 、該ルート値 H の識別番号、それぞれのラウンドに付与される時刻 t 、1次補完情報HK1、および2次補完情報HK2を含む構成となっており、また、監査用受理証明書 $TSC'(H', t')$ は、第1次二分木のルート値 H 、該ルート値 H の識別番号、1つの時刻タグ τ （監査点において複数の時刻タグが割り当てられる場合には、任意の1つ）、それぞれのラウンドに付与される時刻 t 、1次補完情報HK1、および2次補完情報HK2を含む構成となっている。

【 0 1 7 7 】

図4に受理証明書 $TSC(H, t)$ の構成を示す。尚、図4に示す受理証明書 $TSC(H, t)$ は、上述したようにクライアント装置303iから送信されたメッセージ・ダイジェストそのものを第1次二分木のリーフに割り付ける場合のものであるが、メッセージ・ダイジェストにキー付ハッシュ関数を適用した結果を第1次二分木のリーフに割り付けてもよく、この場合には、図5に示すように受理証明書 $TSC(H, t)$ は、キー付ハッシュ関数を適用する際のハッシュ・キー k も含む必要がある。より詳しくは、メッセージ・ダイジェスト y を含む時刻証明要求に対して、予め定められた手順に従ってハッシュ・キー k を決定し、 k をキーとして、 y に対して、所定のキー付ハッシュ関数 h' を作用させ、ハッシュ値 $h'(k, y)$ を計算し、該ハッシュ値 $h'(k, y)$ を第1次二分木のリーフに割り当てるものでこれにより、あるクライアント装置303iの送信したメッセージ・ダイジェストを他のクライアント装置303iに知られないようにすることが可能となる。

【 0 1 7 8 】

図13に監査用受理証明書 $TSC'(H', t')$ の構成を示す。図13に示すように監査用受理証明書 $TSC'(H', t')$ は、受理証明書 $TSC(H, t)$ と同様に構成されるが、受理証明書においては当該のクライアント装置303iから送信されたメッセージ・ダイジェストを置くフィールドに、時刻タグ τ を置く点が受理証明書とは異なる点である。尚、図13は第1次二分木のリーフに割り付ける値として、クライアント装置303iから送られたメッセージ・ダイジェストあるいは取得した時刻タグをそのまま用いた場合の監査用受理証明書 $TSC'(H', t')$ の構成を示すものであるが、受理証明書 $TSC(H, t)$ の場合と同様に、第1次二分木のリーフに、クライアント装置303iから送られたメッセージ・ダイジェストあるいは時刻タグのキー付ハッシュ値を割り付けることも可能であり、この場合の監査用受理証明書 $TSC'(H', t')$ の構成は、図14に示す通りである。

【 0 1 7 9 】

尚、時刻証明装置7から受理証明書 $TSC(H, t)$ をクライアント装置303iへ送信する際には、受理証明書 $TSC(H, t)$ の完全性の保証を高める補助手段として、時刻証明装置7が準備しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵を用いてデジタル署名をつけて送信するようにしてもよい。この場合、当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いてクライアント装置303iからアクセス可能になっているものとする。

【 0 1 8 0 】

監査装置8は、コンピュータネットワーク4を介して時刻証明装置7、クライアント装置303i、および時刻タグシステム800とデータを送受信する送受信部81、時刻証明装置7から

10

20

30

40

50

送信された監査情報（監査用受理証明書 $TSC'(H', t')$ ）を記憶する監査情報記憶部82、および監査情報（監査用受理証明書 $TSC'(H', t')$ ）の検証を行い、その結果をWeb上に公表する時刻証明公表部83を具備している。

【0181】

クライアント装置303iは、コンピュータネットワーク4を介して時刻証明装置7、監査装置8および時刻タグシステム800とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置7からの時刻証明要求に対する受理証明書 $TSC(H, t)$ を記憶する受理証明書記憶部34、および受理証明書 $TSC(H, t)$ を検証する時刻証明検証部37を具備している。尚、時刻証明検証部37は、定期的にメ
10
ディア等40に公表される公表情報を利用して検証を行う第1の検証機能と、メディア等公表前に監査装置8を利用して検証を行う第2の検証機能とを備えるものである。

【0182】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、時刻証明装置7の時刻証明要求まとめ部72、時刻タグ情報取得部73、および監査情報作成部77、監査装置8の時刻証明公表部83、並びにクライアント装置303iの時刻証明検証部37の処理は、上記CPUによる演算制御機能を具体的に示したものに他な
20
る。また、監査装置8の監査情報記憶部82は、上記主記憶装置の機能を備えたものである。

【0183】

次に、以上の構成を有するタイムスタンプ・システム300における時刻証明方法、および時刻証明検証方法を図15乃至図18を用いて説明する。ここで、図15は、一公表サイクルにおいて時刻証明装置7が受理証明書 $TSC(H, t)$ を作成する動作を説明するシーケンス図であり、図16は、監査装置8が監査用受理証明書 $TSC'(H', t')$ の時刻付与に不正がないことを検証する動作を説明するフローチャートであり、図17及び図18は、時刻証明装置7が第2次二分木のルート値RHをメディア等40に公表する前に、クライアント装置303iが受理証明書 $TSC(H, t)$ の検証を行う動作（クライアント装置303iの第2の検証機能に相当する）を説明するシーケンス図である。尚、メディア等公表後にクライアント装置303iが受理証
30
明書 $TSC(H, t)$ の検証を行う動作（クライアント装置303iの第1の検証機能に相当する）は、第1および第2の実施の形態と同様であるため、説明を省略する。

【0184】

まず、時刻証明方法について説明する。クライアント装置303iが時刻証明装置7にメッセージ・ダイジェストyを含む時刻証明要求を送信すると、時刻証明装置7は送受信部11を介して、メッセージ・ダイジェストyを含む時刻証明要求を受信し、時刻証明要求まとめ部72が、このメッセージ・ダイジェストyを第1次二分木のリーフに割り当てる（ステップS201, S202, S203）。また、時刻証明要求まとめ部72aは、処理中の単位時間において時刻タグ放送業者から受信した時刻タグのうちから、前もって定められた選別手順に従って全部または一部を選び出し、当該の単位時間に対応する第1次二分木のリーフのなか
40
から前もって定められた手順に従って選ばれた一部のリーフに割り当てる（ステップS203）。そして、同一ラウンド内においては、複数のクライアント装置303iから受信した複数の時刻証明要求に対して、第1次二分木への割り当てが所定の手順に従って行われ、単位時間経過後ラウンドが終了すると、時刻証明要求まとめ部72がそれぞれのリーフに割り当てられたメッセージ・ダイジェストから第1次二分木のルート値Hを計算する（ステップS204, S205）。

【0185】

次に、時刻証明要求まとめ部72が、第1次二分木のルート値Hを第2次二分木のリーフに割り当てて、インクリメンタルに第2次二分木を構成していくとともに、時刻証明作成部14は、クライアント装置303iから送信されたメッセージ・ダイジェストy、第1次二分
50

木のルート値H、該ルート値Hの識別番号 n、時刻 t、1次補完情報HK1、および2次補完情報HK2を含む受理証明書 TSC(H,t)を作成し、送受信部11を介してクライアント装置303 i に受理証明書 TSC(H,t)を送信する(ステップS 206, S 207, S 208)。

【0186】

これにより、クライアント装置303 i は、受理証明書 TSC(H,t)を取得することができる(ステップS 209)。尚、受理証明書 TSC(H,t)に含まれる2次補完情報には、この時点において取得できる即時2次補完情報は含まれているが、後付2次補完情報は含まれていない。

【0187】

次に、第1次二分木のルート値Hが割り当てられた第2次二分木のリーフが、監視点である場合には、監査情報作成部77が、監査情報(監査用受理証明書 TSC'(H', t'))を作成し、該監査情報(監査用受理証明書 TSC'(H', t'))を送受信部11を介して監査装置8に送信する(ステップS 210, S 211, S 212)。これにより、監査装置8は、監査情報(監査用受理証明書 TSC'(H', t'))を取得することができる(ステップS 213)。

10

【0188】

そして、一定期間内においては、上述した時刻証明装置7の動作は繰り返され、一定期間が終了すると、時刻証明作成部74は、送受信部11を介して、クライアント装置303 i に後付2次補完情報を含む補完証明書を送信する(ステップS 214, S 215)。これにより、クライアント装置303 i は、受理証明書 TSC(H,t)とその全ての2次補完情報を取得したことになる(ステップS 216)。また、時刻証明公表部15は、第2次二分木のルート値RHを計算し、このルート値RHをメディア等40に公表する(ステップS 217, S 218)。

20

【0189】

次に、監査装置8の検証動作について説明する。監査装置8が、送受信部81を介して監査用受理証明書TSC'(H', t')を受信すると、時刻証明公表部83は、この監査用受理証明書TSC'(H', t')を受信したときの時刻 t1を取得する(ステップS 81, S 82)。尚、この時刻 t1は、監査装置8が参照する時計から取得するものであるが、この時計はある一定程度の正確性が保たれているものである。

【0190】

次に、時刻証明公表部83は、監査用受理証明書 TSC'(H', t') から時刻 t' を抽出し、この時刻 t' と時刻 t1 の時間差が一定時間 d 1 (例えば、1秒)以内であるか否かを検証する(ステップS 83, S 84)。

30

【0191】

上記検証において時刻 t' と時刻 t1 の時間差が一定時間以内の場合には、続いて、時刻証明公表部83は、受信した監査用受理証明書 TSC'(H', t')に含まれる時刻タグτに対応する時刻 t''を時刻タグ認証業者803から取得し(ステップS 85)、この時刻 t''と時刻 t'の時間差が一定時間 d 2 (例えば、1秒)以内であるか否かを検証する(ステップS 85, S 86)。

【0192】

以上の検証それぞれにおいて、時間差が一定時間以内であれば、受信した監査用受理証明書 TSC'(H', t')の時刻は正しいということが証明される(ステップS 87)。一方、いずれかの検証において時間差が一定時間以内でなければ、監査用受理証明書 TSC'(H', t')の時刻は不正であることが証明される(ステップS 88)。これにより、本来、直近に受信した時刻タグτを用いて監査用受理証明書 TSC'(H', t')を発行する時刻証明装置7が、何らかの不正動作により、古い時刻タグτを用いて監査用受理証明書 TSC'(H', t')を発行するということを確実に排除することができる。そして、時刻証明公表部83は、検証の結果、監査用受理証明書 TSC'(H', t')の時刻が正しいと判断した場合には、Web上に監査用受理証明書 TSC'(H', t')を公開する(ステップS 89)。

40

【0193】

次に、監査装置8を用いた時刻証明検証方法について説明する。まず、クライアント装置303 i の時刻証明検証部37は、時刻証明装置7に送信した時刻証明要求に含まれるメッセ

50

ージ・ダイジェスト、受信した受理証明書 $TSC(H, t)$ に含まれる第1次補完情報から第1次二分木のルート値 H_{cal} を計算する（ステップ S 311）。次に、時刻証明検証部37は、計算したルート値 H_{cal} と受理証明書 $TSC(H, t)$ に含まれる第1次二分木のルート値 H とが一致するか否かを検証する（ステップ S 312）。

【0194】

そして、ステップ S 312において、第1次二分木のルート値が一致した場合には、検証する時点における後付2次補完情報を含むオンライン補完証明書を時刻証明装置1に要求する（ステップ S 313）。この要求を時刻証明装置7が送受信部11を介して受信すると、時刻証明作成部14は、後付2次補完情報の一部（この時点において取得できる後付2次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置303 i に送信する（ステップ S 314, S 315, S 316）。

10

【0195】

これにより、クライアント装置303 i は、オンライン補完証明書を取得するので、時刻証明検証部37は、これに既に受け取っている受理証明書 $TSC(H, t)$ （1次情報および即時2次補完情報、並びに受理証明書 $TSC(H, t)$ に付された時刻）を加えて、当該の受理証明書に対応する第2次二分木のリーフから該第2次二分木のルートに向かうパスに属するノードのラベル値のうち計算可能なものを計算する（ステップ S 317, S 318, S 319）。

【0196】

次に、時刻証明検証部37は、監査装置8にアクセスし、Web上に公開している情報の中に自己の受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第1次二分木のルート値の識別番号と等しいか、あるいは大きい第1次二分木のルート値の識別番号を含むような）監査用受理証明書 $TSC'(H', t')$ が存在するか否かを確認する（ステップ S 320, S 321）。このような監査用受理証明書 $TSC'(H', t')$ がWeb上に存在する場合には、該監査用受理証明書（該監査用受理証明書による、当該の受理証明書に対する認証点のラベル値、及び監査用受理証明書に付された時刻値を含むもの）を取得して、そこに含まれる認証点のラベル値 A と、上記計算（ステップ S 317, S 318, S 319）により求めた認証点のラベル値 A_{cal} とが一致するか否かを検証し、この検証に成功した場合には、さらに、受理証明書 $TSC(H, t)$ に付された時刻の真正性についても検証する（ステップ S 322, S 323, S 324, S 325）。これは監査用受理証明書 $TSC'(H', t')$ に付された時刻から受理証明書 $TSC(H, t)$ に付されるべき時刻を算出し、該算出した時刻と受理証明書 $TSC(H, t)$ に付された時刻との差が一定時間内か否かを検証するものである。

20

30

【0197】

以上より、監査装置8に受理証明書 $TSC(H, t)$ の検証に利用可能な（即ち、該受理証明書に含まれる第1次二分木のルート値の識別番号と等しいか、あるいは大きい第1次二分木のルート値の識別番号を含むような）監査用受理証明書 $TSC'(H', t')$ が存在し、かつ、それぞれの検証において、検証に成功すれば、受理証明書 $TSC(H, t)$ が改ざんされていないことに加えて、当該の受理証明書 $TSC(H, t)$ に付された時刻の真正性についても確認することができる（ステップ S 326）。一方、いずれかの検証に失敗、もしくは監査装置8に受理証明書の検証に利用可能な（即ち、該受理証明書に含まれる第1次二分木のルート値の識別番号と等しいか、あるいは大きい第1次二分木のルート値の識別番号を含むような）監査用受理証明書が存在しない場合には、受理証明書 $TSC(H, t)$ が改ざんされていること、もしくは受理証明書 $TSC(H, t)$ に付された時刻が不正であることを確認することができる（ステップ S 327）。これにより、メディア等公表前においても、時刻証明装置7が発行した受理証明書 $TSC(H, t)$ を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

40

【0198】

以上、第3の実施の形態のタイムスタンプ・システム300によれば、第1の実施の形態のタイムスタンプ・システム100と同様の効果を得ることができる。加えて、本実施の形態のタイムスタンプ・システム300においては、時刻タグシステム800を備えることにより、時刻証明装置7が付与する時刻値が本来の時刻より過去になることを確実に防止する効

50

果を備えている。

【0199】

尚、第3の実施の形態のタイムスタンプ・システム300は、上述した形態に限定されるものではなく、時刻タグの取得方法、受理証明書に含まれる補完情報のパターン、監査情報に含まれる補完情報のパターン、監視点の決定方法、監査機関の選択方法、補完証明書の種類などについて種々のバリエーションを施すことが可能である。以下、このことについて説明する（受理証明書に含まれる補完情報のパターン、監査情報に含まれる補完情報のパターン、監視点の決定方法、及び補完証明書の種類については、第1の実施の形態のタイムスタンプ・システム100で説明した内容と同一であるため、省略する）。

【0200】

まず、時刻タグの取得方法について説明する。

【0201】

本実施の形態においては、時刻証明装置7が、時刻タグシステム800から時刻タグ τ を取得して、第1次二分木の一部のリーフに時刻タグ τ 割り当てる方式について説明したが、これとは異なり、監査装置8が時刻タグシステム800から時刻タグ τ を取得して、該時刻タグ τ を時刻証明装置7に送信し、時刻証明装置7が第1次二分木の一部のリーフに受信した時刻タグ τ を割り当てる方式にしてもよい。

【0202】

この方式の場合に監査装置8が受信する監査用受理証明書の構成は、上述した図13及び図14と同じでもよいが、図19及び図20に示すような構成を採用してもよい。この場合においては、監査装置8が時刻タグシステム800から受信した時刻タグ τ のキー付ハッシュ値を時刻証明装置7に送信し、時刻タグ τ のキー付ハッシュ値を第1次二分木のリーフに割り当てる値とする。尚、図19は、クライアント装置303iから送信された時刻証明要求に含まれるメッセージ・ダイジェストを第1次二分木のリーフに割り当てる場合、図20は、クライアント装置303iから送信された時刻証明要求に含まれるメッセージ・ダイジェストのキー付ハッシュ値を第1次二分木のリーフに割り当てる場合を示している。

【0203】

次に、監査装置8の選定方法について説明する。

【0204】

本実施の形態においては、受理証明書に対応する監査情報を送信した監査装置8に対して、クライアント装置303iは監査要求を行うことを前提として説明し、監査装置8の選定については特に記載しなかった。以下においては、監視/監査機関が複数ある場合に特定の監査機関を選定するアルゴリズムについて説明するが、該アルゴリズムは、ある監視点において監査情報が送信される監査装置8を前もって予想することが困難であるようなものが望ましく、例えば、以下の方式が考えられる。

【0205】

方式1：

(1) 監査機関の全体の個数を N とし、各監査機関には 0 から $N-1$ までの番号を割り当てる。

【0206】

(2) 本実施の形態の時刻証明方法においては、その第1次二分木のリーフには一般に複数の時刻タグ $\tau(1)$, ..., $\tau(k)$ が割り当てられている。

【0207】

そして、各々の時刻タグ $\tau(i)$ ($i = 1, \dots, k$) に応じて、異なる監査用受理証明書TSC(1), ..., TSC(k)が生成される。

【0208】

(3) 各 $i = 1, \dots, k$ に対して、以下の手順を実行する。

【0209】

(3-1) 時刻タグ $\tau(i)$ を所定の方法で整数に変換し、その値を $x(i)$ とし、 $x(i) \bmod N$ を計算して $j(i)$ と置く。

【0210】

(3-2) $j(i)$ を番号とするような監査機関を $TSC(i)$ の送付先として選択する。

【0211】

そして、このようにして選ばれた監査機関の監査装置8に監査情報を送信する。

【0212】

また、1つの監視点において監査情報が送信される監査装置8は複数であってもよいとすると、例えば以下の方式が考えられる。

【0213】

方式2：

(1) 上記と同じく、監査機関の全体の個数を N とし、各監査機関には 0 から $N-1$ までの番号を割り当てる。

10

【0214】

(2) $1 \leq N' < N$ となるような N' を選ぶ。

【0215】

(3) 本実施の形態の時刻証明方法においては、その第1次二分木のリーフには一般に複数の時刻タグ $\tau(1), \dots, \tau(k)$ が割り当てられている。

【0216】

そして、各々の時刻タグ $\tau(i)$ ($i = 1, \dots, k$) に応じて、異なる監査用受理証明書 $TSC(1), \dots, TSC(k)$ が生成される。各 $i = 1, \dots, k$ に対して、以下の手順を実行する。

【0217】

20

(3-1) 時刻タグ $\tau(i)$ を所定の方法で整数に変換し、その値を $x(i)$ とし、 $x(i) \bmod N'$ を計算して $j(i)$ と置く。

【0218】

(3-2) $n \bmod N' = j(i)$ となるような番号 n を割り当てられ監査機関を $TSC(i)$ の送付先として選択する。

【0219】

そして、このようにして選ばれた監査機関の監査装置8に監査情報を送信する。

【0220】

尚、本実施の形態においては、時刻証明装置7は、クライアント装置303iからの時刻証明要求を第1次二分木に集約し、該第1次二分木に対して時刻を割り付けていた。しかし、このような第1次二分木を用いての集約を行わず、各時刻証明要求に対して時刻を割り付け、受理証明書を発行し、同時に上述した方法に従って、該受理証明書の監査を行う監査機関を決定し、 $TSA10$ と複数の監査機関が連動する時刻証明システムを構成するようにしてもよい。これにより、 $TSA10$ を完全には信頼しなくても、システム全体の信頼性を確保することができる。さらに、第1次二分木を用いての集約は行いが、第2次二分木を用いての集約は行わない方法も考えられるが、これに関しては第3の実施の形態の変形例として後述する。

30

【0221】

また、本実施の形態においては、公開期間を定め、各公開期間で第2次二分木を構成し、そのルートに割り付けられた値を、公開メディア等に公開することを前提としていた。この方法以外に、監査機関が、既に終了した公開期間に発行された受理証明書に対応することも含めて、長期に渡ってWeb等への掲載を続けることにより、第2次二分木のルートの値を公開メディア等などに公表することを前提としない方式としてもよい。

40

【0222】

さらに、本実施の形態においては、受理証明書 $TSC(H, t)$ に時刻タグ τ を含めていなかったが、受理証明書 $TSC(H, t)$ に時刻タグ τ を付加するようにしてもよい。これにより、上述の監査機関選定のアルゴリズムをクライアント装置303iに組み込めば、クライアント装置303iは、監査を依頼すべき監査装置8をクライアント装置303i自身で選定することができるというメリットがある。尚、受理証明書に時刻タグ τ を含めた場合の受理証明書の構成を、図21及び図22に示す。

50

【 0 2 2 3 】

< 第 3 の実施の形態の変形例 >

図37は、本発明の第 3 の実施の形態の変形例であるタイムスタンプ・システム310のシステム構成図である。同図に示すタイムスタンプ・システム310は、T S A 10に設けられた時刻証明装置7a、利用者30が利用する複数のクライアント装置303a i (i は自然数) , 監視 / 監査機関に設けられ、時刻証明装置7aが発行した受理証明書に関する監査情報を公表する監査装置8a、時刻タグを供給する時刻タグシステム800、および以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク4を備えており、時刻証明装置7aがクライアント装置303a i からのタイムスタンプ要求 (時刻証明要求) に応えて、タイムスタンプつき受理証明書をクライアント装置303a i に返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置303a i は、監査装置8aから公表された監査情報によって受理証明書を検証できるようになっているコンピュータシステムである。

10

【 0 2 2 4 】

また、タイムスタンプ・システム310は、時刻のトレーサビリティを確保する役割を時刻タグシステム800に集約しているので、T S A 10は時刻のトレーサビリティを確保する必要がなく、さらに、時刻証明装置7aが付与する時刻が本来の時刻より、過去の時刻になることを確実に防止することができるコンピュータシステムとなっている。尚、時刻タグ τ とは、所定の方法と手段により生成される乱数 (但し、時刻タグ供給サービスの継続期間の間に、乱数の衝突を起こす確率が無視できる程度のビット長を有する) であり、時刻タグシステム800を介して、各時刻タグに対応する時刻値を取得することができるものである。また、本変形例においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

20

【 0 2 2 5 】

時刻証明装置7aは、コンピュータネットワーク4を介して監査装置8a、クライアント装置303a i 、および時刻タグシステム800とデータを送受信する送受信部11、受理証明書に使用する時刻タグ τ を時刻タグシステム800から取得する時刻タグ情報取得部73、複数のクライアント装置303a i からの時刻証明要求として送信されたメッセージ・ダイジェスト (デジタル・データから作成されるハッシュ値) および時刻タグ情報取得部73で取得した時刻タグ τ を二分木を用いてまとめる時刻証明要求まとめ部72 a 、受理証明書を作成する際に時刻情報提供装置2から時刻情報を取得する時刻情報取得部13、時刻証明要求まとめ部72 a でまとめられたメッセージ・ダイジェストに対して時刻情報取得部13で取得した時刻情報を付して受理証明書 TSC(H, t) を作成する時刻証明作成部14 a 、時刻証明作成部14 a で作成された受理証明書TSC(H, t)を記憶する受理証明書記憶部16、および監査装置8aに送信する監査情報 (監査用受理証明書TSC'(H, t)) を作成する監査情報作成部77 a を具備している。

30

【 0 2 2 6 】

尚、ここで、時刻証明要求まとめ部72 a は、クライアント装置303aiから送信されたメッセージ・ダイジェストに加えて時刻タグシステム800から取得した時刻タグ τ を第 1 次二分木のリーフに割り当てる点、及び第 2 次二分木を作成しない点 (但し、第 1 次二分木のルート値に対する識別番号の取得は行う) が、時刻証明要求まとめ部12と異なっている。即ち、時刻タグ τ は、第 1 次二分木の所定のリーフ (予め定められた方法に従って、少なくとも 1 箇所以上) に、メッセージ・ダイジェストの代わりに割り付けられ、メッセージダイジェストと同様に扱われるものである。これにより、第 1 次二分木のリーフは、メッセージダイジェスト又は時刻タグが割り当てられる。

40

【 0 2 2 7 】

また、時刻証明作成部14a、及び監査情報作成部77aは、それぞれ作成する受理証明書、及び監査情報 (監査用受理証明書) の構成において、時刻証明作成部14、及び監査情報作成部17と異なっているものである。より詳しくは、本実施の形態における受理証明書 TSC(H, t) は、第 1 次二分木のルート値H、該ルート値Hの識別番号、それぞれのラウンドに付

50

与される時刻 t 、および 1 次補完情報 HK1 を含む構成となっており、また、監査用受理証明書 $TSC'(H', t')$ は、第 1 次二分木のルート値 H 、該ルート値 H の識別番号、1 つの時刻タグ τ (監査点において複数の時刻タグが割り当てられる場合には、任意の 1 つ)、それぞれのラウンドに付与される時刻 t 、および 1 次補完情報 HK1 を含む構成となっている。

【0228】

図38に受理証明書 $TSC(H, t)$ の構成を示す。尚、図38に示す受理証明書 $TSC(H, t)$ は、上述したようにクライアント装置303aiから送信されたメッセージ・ダイジェストそのものを第1次二分木のリーフに割り付ける場合のものであるが、メッセージ・ダイジェストにキー付ハッシュ関数を適用した結果を第1次二分木のリーフに割り付けてもよく、この場合には、図39に示すように受理証明書 $TSC(H, t)$ は、キー付ハッシュ関数を適用する際のハッシュ・キー k も含む必要がある。より詳しくは、メッセージ・ダイジェスト y を含む時刻証明要求に対して、予め定められた手順に従ってハッシュ・キー k を決定し、 k をキーとして、 y に対して、所定のキー付ハッシュ関数 h' を作用させ、ハッシュ値 $h'(k, y)$ を計算し、該ハッシュ値 $h'(k, y)$ を第1次二分木のリーフに割り当てるものでこれにより、あるクライアント装置303aiの送信したメッセージ・ダイジェストを他のクライアント装置303aiに知られないようにすることが可能となる。

【0229】

図40に監査用受理証明書 $TSC'(H, t)$ の構成を示す。図40に示すように監査用受理証明書 $TSC'(H', t')$ は、受理証明書 $TSC(H, t)$ と同様に構成されるが、受理証明書においては当該のクライアント装置303aiから送信されたメッセージ・ダイジェストを置くフィールドに、時刻タグ τ を置く点が受理証明書とは異なる点である。尚、図40は第1次二分木のリーフに割り付ける値として、クライアント装置303aiから送られたメッセージ・ダイジェストあるいは取得した時刻タグをそのまま用いた場合の監査用受理証明書 $TSC'(H, t)$ の構成を示すものであるが、受理証明書 $TSC(H, t)$ の場合と同様に、第1次二分木のリーフに、クライアント装置303aiから送られたメッセージ・ダイジェストあるいは時刻タグのキー付ハッシュ値を割り付けることも可能であり、この場合の監査用受理証明書 $TSC'(H, t)$ の構成は、図41に示す通りである。

【0230】

尚、時刻証明装置7aから受理証明書 $TSC(H, t)$ をクライアント装置303aiへ送信する際には、受理証明書 $TSC(H, t)$ の完全性の保証を高める補助手段として、時刻証明装置7aが準備しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵を用いてデジタル署名をつけて送信するようにしてもよい。この場合、当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いてクライアント装置303aiからアクセス可能になっているものとする。

【0231】

監査装置8aは、コンピュータネットワーク4を介して時刻証明装置7a、クライアント装置303ai、および時刻タグシステム800とデータを送受信する送受信部81、時刻証明装置7aから送信された監査情報(監査用受理証明書 $TSC'(H, t)$)を記憶する監査情報記憶部82、および監査情報(監査用受理証明書 $TSC'(H, t)$)の検証を行い、その結果をWeb上に公表する時刻証明公表部83aを具備している。

【0232】

クライアント装置303aiは、コンピュータネットワーク4を介して時刻証明装置7a、監査装置8aおよび時刻タグシステム800とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置7aからの時刻証明要求に対する受理証明書 $TSC(H, t)$ を記憶する受理証明書記憶部34、および受理証明書 $TSC(H, t)$ を検証する時刻証明検証部37aを具備している。尚、時刻証明検証部37aは、監査装置8を利用して検証を行う検証機能を備えるものである。

【0233】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU

10

20

30

40

50

：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、時刻証明装置7aの時刻証明要求まとめ部72a、時刻証明作成部14a、および監査情報作成部77a、監査装置8aの時刻証明公表部83a、並びにクライアント装置303aiの時刻証明検証部37aの処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。

【0234】

次に、以上の構成を有するタイムスタンプ・システム310における時刻証明方法、および時刻証明検証方法を図42乃至 図45を用いて説明する。ここで、図42は、時刻証明装置7aが受理証明書TSC(H,t)を作成する動作を説明するシーケンス図であり、図43は、クライ

10

アント装置303aiが受理証明書 TSC(H,t)の検証を行う動作を説明するシーケンス図である。尚、監査装置8aが監査用受理証明書 TSC'(H,t)の時刻付与に不正がないことを検証する動作については、第3の実施の形態と同様であるため、説明を省略する。

【0235】

まず、時刻証明方法について説明する。クライアント装置303aiが時刻証明装置7aにメッセージ・ダイジェストyを含む時刻証明要求を送信すると、時刻証明装置7aは送受信部11を介して、メッセージ・ダイジェストyを含む時刻証明要求を受信し、時刻証明要求まとめ部72aが、このメッセージ・ダイジェストyを第1次二分木のリーフに割り当てる（ステップS401, S402, S403）。また時刻証明要求まとめ部72aは、処理中の単位時間において時刻タグ放送業者から受信した時刻タグのうちから、前以って定められた選別手順に従って全部または一部を選び出し、当該の単位時間に対応する1次二分木のリーフのなかから前以って定められた手順に従って選ばれた一部のリーフに割り当てる。そして、同一ラウンド内においては、複数のクライアント装置303aiから受信した複数の時刻証明要求に対して、第1次二分木への割り当てが所定の手順に従って行われ、単位時間経過後ラウンドが終了すると、時刻証明要求まとめ部72aがそれぞれのリーフに割り当てられたメッセージ・ダイジェストから第1次二分木のルート値Hを計算する（ステップS404, S405）。

20

【0236】

時刻証明作成部14aは、第1次二分木のルート値Hの識別番号を割り当て、クライアント装置303iから送信されたメッセージ・ダイジェストy、第1次二分木のルート値H、該ルート値Hの識別番号 n、時刻 t、1次補完情報HK1を含む受理証明書 TSC(H,t) を作成し、送受信部11を介してクライアント装置303aiに受理証明書 TSC(H,t) を送信する（ステップS406, S407, S408）。これにより、クライアント装置303aiは、受理証明書 TSC(H,t) を取得することができる（ステップS409）。

30

【0237】

次に、監査情報作成部77aが、監査情報（監査用受理証明書 TSC'(H,t)）を作成し、該監査情報（監査用受理証明書 TSC'(H,t)）を送受信部11を介して監査装置8aに送信する（ステップS410, S411）。これにより、監査装置8aは、監査情報（監査用受理証明書 TSC'(H,t)）を取得することができる（ステップS412）。

【0238】

次に、監査装置8aを用いた時刻証明検証方法について説明する。まず、クライアント装置303aiの時刻証明検証部37aは、時刻証明装置7aに送信した時刻証明要求に含まれるメッセージ・ダイジェスト、受信した受理証明書 TSC(H,t) に含まれる1次補完情報から第1次二分木のルート値 Hcal を計算する（ステップS431）。次に、時刻証明検証部37aは、計算したルート値Hcal と受理証明書 TSC(H,t) に含まれる第1次二分木のルート値Hとが一致するか否かを検証する（ステップS432）。

40

【0239】

そして、ステップS432において、第1次二分木のルート値が一致した場合には、時刻証明検証部37は、監査装置8aにアクセスし、Web上に公開している情報の中に自己の受理証明書に対応する監査用受理証明書TSC'(H,t)が存在するか否かを確認する（ステップS433, S434）。監査用受理証明書TSC'(H,t)がWeb上に存在する場合には、受理証明書TSC

50

(H, t) に含まれる第 1 次二分木のルート値と監査用受理証明書 TSC'(H, t) に含まれるの第 1 次二分木のルート値が一致するか否か検証する (ステップ S 435, S 436)。

【 0 2 4 0 】

以上より、監査装置 8a に受理証明書 TSC(H, t) に対応する監査用受理証明書 TSC'(H, t) が存在し、かつ、検証に成功すれば、受理証明書 TSC(H, t) が改ざんされていないことに加えて、当該の受理証明書 TSC(H, t) に付された時刻の真正性についても確認することができる (ステップ S 437)。一方、検証に失敗、もしくは監査装置 8a に受理証明書 TSC(H, t) に対応する監査用受理証明書 TSC'(H, t) が存在しない場合には、受理証明書 TSC(H, t) が改ざんされていること、もしくは受理証明書 TSC(H, t) に付された時刻が不正であることを確認することができる (ステップ S 438)。これにより、時刻証明装置 7a が発行した受理証明書 TSC(H, t) を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

10

【 0 2 4 1 】

以上、第 3 の実施の形態の変形であるタイムスタンプ・システム 310 によれば、第 1 の実施の形態のタイムスタンプ・システム 100 と同様に TSA を完全に信頼しなくとも監査機関を用いることにより、受理証明書の真正性検証することができる。加えて、タイムスタンプ・システム 310 においては、時刻タグシステム 800 を備えることにより、時刻証明装置 7 が付与する時刻値が本来の時刻より過去になることを確実に防止する効果を備えている。

【 0 2 4 2 】

20

尚、タイムスタンプ・システム 310 においては、受理証明書 TSC(H, t) に時刻タグ τ を含めていなかったが、受理証明書 TSC(H, t) に時刻タグ τ を付加するようにしてもよい。これにより、上述の監査機関選定のアルゴリズムをクライアント装置 303ai に組み込めば、クライアント装置 303ai は、監査を依頼すべき監査装置 8a をクライアント装置 303i 自身で選定することができるというメリットがある。尚、受理証明書に時刻タグ τ を含めた場合の受理証明書の構成を、図 44 及び図 45 に示す。

【 0 2 4 3 】

< 第 4 の実施の形態 >

図 23 は、本発明の第 4 の実施の形態に係るタイムスタンプ・システム 400 のシステム構成図である。同図に示すタイムスタンプ・システム 400 は、T S A 10 に設けられた時刻証明装置 7、利用者 30 が利用する複数のクライアント装置 403 i (i は自然数)、監視 / 監査機関に設けられ、時刻証明装置 7 が発行した受理証明書の保証書を作成する監査装置 9、時刻タグを供給する時刻タグシステム 800、および以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成される、コンピュータネットワーク 4 を備えており、時刻証明装置 7 がクライアント装置 403 i からのタイムスタンプ要求 (時刻証明要求) に応えて、タイムスタンプつき受理証明書をクライアント装置 403 i に返信するとともに、受理証明書に疑義が生じた場合には、クライアント装置 403 i は、時刻証明装置 7 がメディア等 40 に公表した情報、又は、監査装置 9 から送信された受理証明書の保証書によって受理証明書を検証できるようになっているコンピュータシステムである。

30

【 0 2 4 4 】

40

尚、上記コンピュータネットワーク 4 は、郵便など他の通信手段に置き換えることも可能である。

【 0 2 4 5 】

また、第 3 の実施の形態と同様に、タイムスタンプ・システム 400 は、時刻のトレーサビリティを確保する役割を時刻タグシステム 800 に集約しているので、T S A 10 は時刻のトレーサビリティを確保する必要がなく、さらに、時刻証明装置 7 が付与する時刻値が本来の時刻より、過去の時刻になることを確実に防止することができるコンピュータシステムとなっている。尚、時刻タグ τ とは、所定の方法と手段により生成される乱数 (但し、時刻タグ供給サービスの継続期間の間に、乱数の衝突を起こす確率が無視できる程度のビット長を有する) であり、時刻タグシステム 800 を介して、各時刻タグに対応する時刻値

50

を取得することが出来るものである。また、本実施の形態においても、上記実施の形態と異なる構成及び機能のみ説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【0246】

監査装置9は、コンピュータネットワーク4を介して時刻証明装置7、クライアント装置403i、および時刻タグシステム800とデータを送受信する送受信部81、時刻証明装置7から送信された監査情報（監査用受理証明書 $TSC'(H', t')$ ）の検証を行い、その結果として監査用受理証明書 $TSC'(H', t')$ の保証書を作成するとともに、クライアント装置403からの時刻証明要求を監査用受理証明書 $TSC'(H', t')$ の保証書を用いて検証する時刻証明検証部93、および監査用受理証明書 $TSC(H, t)$ 、及び監査用受理証明書 $TSC'(H', t')$ の保証書を記憶する監査情報記憶部92、を具備している。

10

【0247】

クライアント装置403iは、コンピュータネットワーク4を介して時刻証明装置7、監査装置9および時刻タグシステム800とデータを送受信する送受信部31、デジタル文書などのメッセージを記憶しているメッセージ記憶部32、メッセージ記憶部32に記憶されているメッセージの時刻証明要求を行う時刻証明要求部33、時刻証明装置7からの時刻証明要求に対する受理証明書 $TSC(H, t)$ を記憶する受理証明書記憶部34、および受理証明書 $TSC(H, t)$ を検証する時刻証明検証部38を具備している。尚、時刻証明検証部38は、定期的にメディア等40に公表された公表情報を利用して検証を行う第1の検証機能と、メディア等公表前に監査装置9を利用して検証を行う第2の検証機能とを備えるものである。

20

【0248】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）を有する電子的な装置から構成されている。このうち、監査装置9の時刻証明検証部93、およびクライアント装置403iの時刻証明検証部38の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、監査装置9の監査情報記憶部92は、上記主記憶装置の機能を備えたものである。

【0249】

次に、以上の構成を有するタイムスタンプ・システム400における時刻証明検証方法を図24乃至図26を用いて説明する。ここで、図24は、監査装置9が監査用受理証明書 $TSC'(H', t')$ の時刻付与に不正がないことを検証する動作を説明するフローチャートであり、図25及び図26は、時刻証明装置7が2次二分木のルート値RHをメディア等40に公表する前に、クライアント装置403iが受理証明書 $TSC(H, t)$ の検証を行う動作（クライアント装置403iの第2の検証機能に相当する）を説明するシーケンス図である。尚、タイムスタンプ・システム400における時刻証明方法、およびメディア等公表後にクライアント装置303iが受理証明書 $TSC(H, t)$ の検証を行う動作（クライアント装置403iの第1の検証機能に相当する）は、第3の実施の形態と同様であるため、説明を省略する。

30

【0250】

まず、監査装置9の検証動作について説明する。監査装置9が、送受信部81を介して監査用受理証明書 $TSC'(H', t')$ を受信すると、時刻証明検証部93は、この監査用受理証明書 $TSC'(H', t')$ を受信したときの時刻 t_1 を取得する（ステップS101、S102）。尚、この時刻 t_1 は、監査装置9が参照する時計から取得するものであるが、この時計はある一定程度の正確性が保たれているものである。

40

【0251】

次に、時刻証明検証部93は、監査用受理証明書 $TSC'(H', t')$ から時刻 t' を抽出し、この時刻 t' と時刻 t_1 の時間差が一定時間 d_1 （例えば、1秒）以内であるか否かを検証する（ステップS103、S104）。

【0252】

上記検証において時刻 t' と時刻 t_1 の時間差が一定時間以内の場合には、続いて、時

50

時刻証明検証部93は、受信した監査用受理証明書 $TSC'(H', t')$ に含まれる時刻タグ τ に対応する時刻 t'' を時刻タグ認証業者803から取得し（ステップ S 105）、この時刻 t'' と時刻 t' の時間差が一定時間 d_2 （例えば、1秒）以内であるか否かを検証する（ステップ S 105, S 106）。

【 0 2 5 3 】

以上の検証それぞれにおいて、時間差が一定時間以内であれば、受信した監査用受理証明書 $TSC'(H', t')$ の時刻は正しいということが証明される（ステップ S 107）。一方、いずれかの検証において時間差が一定時間以内でなければ、監査用受理証明書 $TSC'(H', t')$ の時刻は不正であることが証明される（ステップ S 108）。これにより、本来、直近に受信した時刻タグ τ を用いて監査用受理証明書 $TSC'(H', t')$ を発行する時刻証明装置7が、何らかの不正動作により、古い時刻タグ τ を用いて監査用受理証明書 $TSC'(H', t')$ を発行するということを確実に排除することができる。そして、時刻証明検証部93は、検証の結果、監査用受理証明書 $TSC'(H', t')$ の時刻が正しいと判断した場合には、デジタル署名を付した監査用受理証明書 $TSC'(H', t')$ の保証書を作成し、監査情報記憶部92に記憶させる（ステップ S 109）。尚、このデジタル署名は、「この監査用受理証明書の時刻タグ付けは正しい」ということを意味するメッセージ RM のハッシュ値に対して署名鍵 SK を用いてデジタル署名をしたものであり、監査用受理証明書の保証書は、該デジタル署名 $sig(SK, h(RM))$ 、メッセージ RM 、および監査用受理証明書 $TSC'(H', t')$ を含む構成となっている。

【 0 2 5 4 】

次に、監査装置9を用いた時刻証明検証方法について説明する。まず、クライアント装置403 i の時刻証明検証部38は、時刻証明装置7に送信した時刻証明要求であるメッセージ・ダイジェスト、受信した受理証明書 $TSC(H, t)$ に含まれる1次補完情報から第1次二分木のルート値 H_{cal} を計算する（ステップ S 111）。次に、時刻証明検証部38は、計算したルート値 H_{cal} と受理証明書 $TSC(H, t)$ に含まれる第1次二分木のルート値 H とが一致するか否かを検証する（ステップ S 112）。

【 0 2 5 5 】

そして、ステップ S 112において、第1次二分木のルート値が一致した場合には、検証する時点における後付2次補完情報を含むオンライン補完証明書を時刻証明装置7に要求する（ステップ S 113）。この要求を時刻証明装置7が送受信部11を介して受信すると、時刻証明作成部14は、後付2次補完情報の一部（この時点において取得できる後付2次補完情報のすべて）を取得し、これを含むオンライン補完証明書を送受信部11を介してクライアント装置403 i に送信する（ステップ S 114, S 115, S 116）。

【 0 2 5 6 】

これにより、クライアント装置403 i は、オンライン補完証明書を取得するので、時刻証明検証部38は、これに既に受け取っている受理証明書 $TSC(H, t)$ （1次情報および即時2次補完情報、並びに受理証明書 $TSC(H, t)$ に付された時刻）を加えた検証要求情報を監査装置9に送信する（ステップ S 117, S 118）。

【 0 2 5 7 】

次に、監査装置9が検証要求情報を送受信部81を介して受信すると、時刻証明検証部93は、受理証明書に対応する監査用受理証明書の保証書が監査情報記憶部92に存在するか否かを確認して、保証書が存在する場合には、監査用受理証明書の保証書を取得する（ステップ S 119, S 120, S 121）。

【 0 2 5 8 】

そして、保証書が存在する場合には、受信した検証要求情報から認証点のラベル値 A_{cal} を計算し、監査情報として既に受け取っているこの認証点のラベル値 A を監査情報記憶部92から取得して、この認証点のラベル値 A が、計算により求めた認証点のラベル値 A_{cal} に一致するか否かを検証する（ステップ S 122, S 123）。そして、この検証に成功した場合には、受理証明書 $TSC(H, t)$ に付された時刻の真正性についても検証する（ステップ S 124, S 125）。これは監査情報に付された時刻から受理証明書 $TSC(H, t)$ に付されるべき時刻

を算出し、該算出した時刻と受理証明書に付された時刻との差が一定時間内か否かを検証するものである。

【 0 2 5 9 】

以上より、監査装置9に受理証明書に対応する監査用受理証明書の保証書が存在し、かつ、それぞれの検証において、検証に成功すれば、受理証明書TSC(H,t)が改ざんされていないことに加えて、当該の受理証明書TSC(H,t)に付された時刻の真正性についても確認することができる(ステップS126)。一方、いずれかの検証に失敗、もしくは監査装置9に受理証明書に対応する監査用受理証明書の保証書が存在しない場合には、受理証明書 TSC(H,t) が改ざんされていること、もしくは受理証明書TSC(H,t)に付された時刻が不正であることを確認することができる(ステップS127)。

10

【 0 2 6 0 】

監査装置9は、上記の検証結果を踏まえて、受理証明書が正しいと判断した場合には、監査用受理証明書の保証書、正しくないと判断した場合には、検証結果をクライアント装置403iに送受信部81を介して送信する(ステップ128)。

【 0 2 6 1 】

クライアント装置403iは、送受信部31を介して監査用受理証明書の保証書を受信すると、時刻証明検証部38が署名鍵SKに対応する公開鍵PKを取り出し、受理証明書の保証書に含まれているデジタル署名 $\text{sig}(\text{SK}, h(\text{RM}))$ が、監査用受理証明書の保証書に含まれているメッセージRMを含むデジタル・データに対してなされたことを公開鍵PKを用い検証する(ステップS129, S130, S131)。

20

【 0 2 6 2 】

以上、クライアント装置403iにおける検証において、検証に成功した場合には、受理証明書TSC(H,t)が正しいことを確認することができる(ステップS132)。一方、ステップS112、またはステップS131の検証に失敗した場合には、受理証明書TSC(H,t)が不正であることを確認することができる(ステップS133)。これにより、メディア等公表前においても、時刻証明装置7が発行した受理証明書TSC(H,t)を的確に検証でき、時刻情報やデータの真正性を明確にすることができる。

【 0 2 6 3 】

以上、第4の実施の形態のタイムスタンプ・システム400によれば、第3の実施の形態のタイムスタンプ・システムと同様の効果を得ることができる。加えて、本実施の形態のタイムスタンプ・システム400においては、デジタル署名を用いた受理証明書の保証書を用いて受理証明書 TSC(H,t) の検証を行うので、データの守秘性をさらに高めることができる。

30

【 0 2 6 4 】

尚、第4の実施の形態のタイムスタンプ・システム400は、上述した形態に限定されるものではなく、第3の実施の形態のタイムスタンプ・システム300に施すことが可能であった種々のバリエーションをタイムスタンプ・システム400に適用することが可能なものである(もちろん、第3の実施の形態の変形例であるタイムスタンプ・システム310に対応するタイムスタンプ・システム410を構築することも可能である)。

【 0 2 6 5 】

以上、本発明の実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対してさらに種々の変形や変更を施すことができる。例えば、上記実施の形態においては、時刻証明装置がメディア等40を利用して第2次二分木のルート値RHを定期的にメディア等40に公表してきたが、メディア等40を利用する代わりに、コンピュータネットワーク4で接続されている公表装置(オンラインサーバ)が、第2次二分木のルート値RHを保持し、クライアント装置にFTPやHTTPなどのプロトコルを用いて提供するようにしてもよい。ここで、公表装置に関しては、メディア等40に公表する目的、即ち、多数の第三者に保証の拠り所となる値を公開し記録させることによって、その値の改竄を不可能にするという目的、と同一の目的を達成するためには、一定数以上の複数の公表装置が独立に運営されている必要がある。尚、前提として、公表装置は、

40

50

時刻証明装置から第2次二分木のルート値RHが送信されるようになっている、もしくは、第2次二分木のリーフに割り当てる値から第2次二分木を構成するようになっているものである。また、クライアント装置における受理証明書の検証は、上記実施の形態と同様であるが、複数の公表装置を利用したそれぞれの検証結果が異なる場合には、一定数以上の公表装置をもとに同一検証結果が得られているかどうかにより、最終的な判定を下すものである。

【0266】

図27(a)は、上述した第2次二分木のルート値RHと一定期間との対応付けを掲載しているログファイル41の内容を示しているものである。このログファイル41は、一定期間毎に第2次二分木のルート値RHが順次追加されるとともに、公表装置を介して、クライアント装置に提供されるようになっている。

10

【0267】

尚、公表装置は、図27(b)に示すように、ログファイル41のハッシュ値を計算し、該ハッシュ値を保持するとともに、該ハッシュ値を掲載しているファイル42をクライアント装置に提供するようにしてもよい。尚、この場合においては、クライアント装置からの要求に応じてログファイル41を別途を提供する必要がある、クライアント装置においては、ログファイル41から計算されるハッシュ値とファイル42に掲載されているハッシュ値が一致するか否かを検証することになる。そして、この場合においても、複数の公表装置を利用したそれぞれの検証結果が異なる場合には、一定数以上の公表装置をもとに同一検証結果が得られているかどうかにより、最終的な判定を下すことになる。

20

【0268】

従って、コンピュータネットワーク4に接続された公表装置を別途設ける方法によれば、時刻証明装置が保持すべき公表情報のコピーを公表装置がもつことになるので、当該データが事故などにより消失することを確実に防止することができる。さらに、ファイル42を公表情報とする方法においては、掲載情報は少なく済むので、例えば、Webページの広告等に掲載することも可能であるとともに、公表装置に必要とされるストレージの量を大幅に減らすことができるという効果がある。

【0269】

尚、公表装置の機能を、監査装置に組み込んで、監査装置が定期的に受理証明書に関する情報を公表するようにしてもよい。この場合においては、監査装置を利用すれば、いかなるときにおいても、利用者装置は受理証明書の検証をすることが可能となる。

30

【0270】

また、以上の上記実施の形態における各装置の動作は、各装置に格納されたプログラムを実行することにより実現される。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、コンピュータネットワークを介して配信することも可能である。

【0271】

<第1次二分木の構成，および認証点の性質>

上記実施の形態において用いられた第1次二分木の動的な構成方法、および認証点の性質について説明するが、その前提としてまず、二分木の構成に必要な基本関数について説明する。

40

【0272】

高さ k の二分木は、レベル0からレベル k までのノードで構成されるが、レベル j ($j = 0, 1, \dots, k$) のノードの数は、 $2^{(k-j)}$ であるので、レベル j 、番号 i のノードを (j, i) と表すことにすると、 $i = 0, 1, \dots, 2^{(k-j)} - 1$ となる。

【0273】

以下、実数 x に対して、 $\text{ceiling}(x)$ を x 以上の最小の整数、 $\text{floor}(x)$ を x 以下の最大の整数として、説明する。

【0274】

50

ノード (j, i) (但し, $j < k$) の親は、 $(j+1, \text{floor}(i/2))$ であるので、
 $\text{parent}(j, i) = (j+1, \text{floor}(i/2))$ と定義する。

【0275】

また、ノード (j, i) (但し, $0 < j$) の左側の子供は $(j-1, 2i)$ 、右側の子供は $(j-1, 2i+1)$ であるので、

$\text{leftChild}(j, i) = (j-1, 2i)$

$\text{rightChild}(j, i) = (j-1, 2i+1)$ と定義する。

【0276】

このとき、高さ k の二分木のノード (j, i) ($0 \leq i < 2^{(k-j)}$) のルートパス $\text{rtPath}(k, j, i)$ (ノード (j, i) からルートに至るノード (j, i) の列をいう) は、 $\text{rtPath}(k, j, i) = ((j, r(j)), \dots, (k, r(k)))$ と表せる。

10

【0277】

但し、 $r(j') = i$ ($j' = j, \dots, k$)、 $r(j'+1) = \text{floor}(r(j')/2)$ ($j' < k$ とし、 $r(j')$ は既に定まっているものとする) であるとする。尚、 $(k, r(k))$ は、二分木のルートを表し、常に $r(k) = 0$ となる。

【0278】

また、高さ k の二分木のノード (j, i) ($0 \leq i < 2^{(k-j)}$) の認証パス authPath (ノード (j, i) からルート値を計算するのに必要なノード (j, i) の集合。但し、該ノードを接続する方向 (左又は右) の情報も含んでいる) は、 $\text{rtPath}(k, j, i)$ を用いて次のように表せる。

【0279】

20

$\text{authPath}(k, j, i) = ((j, a(j), \text{LR}(j)), \dots, ((k-1, a(k-1), \text{LR}(k-1)))$

ここで、 $r(j')$ が偶数の場合、 $a(j') = r(j') + 1$ 、 $r(j')$ が奇数の場合、 $r(j') - 1$ であり、また、 $r(j')$ が偶数の場合、 $\text{LR}(j') = R$ 、 $r(j')$ が奇数の場合、 $\text{LR}(j') = L$ である (但し、 $j' = j, \dots, k-1$)。

【0280】

そして、 $\text{authPath}(k, j, i)$ の要素 $((j, a(j), \text{LR}(j)))$ について、 $\text{LR}(j)$ の部分を (LR) タグという。さらに、 $\text{rtPath}(k, j, i)$ の要素 $(j, r(j))$ について、 $r(j)$ が偶数のとき、 $((j, r(j)+1), R)$ を $(j, r(j))$ の右補完点という。 $r(j)$ が奇数のとき、 $((j, r(j)-1), L)$ を $(j, r(j))$ の左補完点という。

【0281】

30

このとき、 $\text{authPath}(k, j, i)$ は、 $\text{rtPath}(k, j, i)$ のルート以外の点の右補完点あるいは左補完点からなる。

【0282】

上述した基本関数の定義のもと、第1の動的な第1次二分木の構成方法について説明する。この第1次二分木の構成方法は、深さの違いを1以内に押さえ、ダミーノードを作成しない方法である。

【0283】

単位時間 (1ラウンドの時間であり、例えば、1秒) に受け付けた時刻証明要求の数を n とすると、高さ k は、 $k = \text{ceiling}(\log_2(n))$ である。高さ k の二分木のリーフ数は最大で 2^k であるので、 $d = 2^k - n$ として、レベル0のノードのうち、 $2d$ 個を消去すれば、時刻証明要求の数 n をダミーノードなしでリーフに割り当てることが可能となる。これは、レベル0のリーフが $2d$ 個減ると、レベル1のリーフが新たに d 個できるので、合計で d 個減り、リーフの数は結局、 $2^k - d = n$ となるからである。

40

【0284】

以下、 $L1W = 2^{(k-1)}$ (レベル1のノードの個数)、 $L1L = 2^{(k-1)} - d$ (子を有するレベル1のノードの個数) の、 $L0L = 2(2^{(k-1)} - d)$ (レベル0のノードの個数) とおくと、 n 個の時刻証明要求のうち、初めの $L0L$ 個をレベル0に配置し、残りをレベル1に配置するとき、 i 番目の時刻証明要求の配置先を表す関数 $\text{place}(i)$ は次式で表すことができる。

【0285】

$\text{place}(i) = (0, i)$ ($0 \leq i < L0L$)

50

$place(i) = (1, L1L + i - L0L) \quad (L0L < i \leq n)$

ここで、 $place(i) = (\text{レベル}, \text{番号})$ で構成されているものである。

【0286】

図28は、第1の動的な第1次二分木の構成方法の $n = 10$ の場合の具体例を示すものである。この場合においては、図28に示す通り、 $k = \text{ceiling}(\log_2(10)) = 4$ となり、高さは4である。そして、 $d = 2^4 - 10 = 6$ であるので、 $6 \times 2 = 12$ 個のレベル0のリーフを消去する。この結果、 $L1W = 2^3 = 8$ 、 $L1L = 8 - 6 = 2$ 、 $L0L = 2 \times 2 = 4$ となる。従って、レベル0のリーフが4個、レベル1のリーフが6個で、リーフの合計数は $n = 10$ となる。この結果、図28に示すような第1次二分木を動的に作成することができる。

【0287】

次に、第2の動的な第1次二分木の構成方法について説明する。この二分木の構成方法は、深さを単一にして、ダミーノードを作成する方法である。

【0288】

単位時間（1ラウンドの時間であり、例えば、1秒）に受け付けた時刻証明要求の数を n とすると、高さ k は、 $k = \text{ceiling}(\log_2(n))$ である。高さ k の二分木のリーフ数は最大で 2^k であるので、0から $n - 1$ までの n 個の時刻証明要求をレベル0のノード $(0, 0)$ からノード $(0, n-1)$ に割り当てる。ここで、レベル0に割り当てられた、最も右のノード $(0, n-1)$ に対して、ルートパス $rtPath(k, 0, n-1)$ を計算する。次に、各レベル j ($j = 0, \dots, k-1$) においては、以下の手順を実行するものとする。

【0289】

$r(j)$ が偶数のとき、ノード $(j, r(j)+1)$ をダミーノードとする。

【0290】

$r(j)+1 < i < 2^{(k-j)}$ となる各 i に対して、ノード (j, i) は消去される。

【0291】

$r(j)$ が奇数のとき、 $r(j)+1 < i < 2^{(k-j)}$ となる各 i に対して、ノード (j, i) は消去される。また、ルートにあるレベル k については、何も行わない。

【0292】

以上のような方法に基づいて構成される二分木は、ダミーノードは各レベルの右端のみ現れる、および作成されるダミーノードの数は、 k 以下であるという性質を有する。

【0293】

図29は、第2の動的な第1次二分木の構成方法の $n = 9$ の場合の具体例を示す図である。この場合においては、図29に示す通り、 $k = \text{ceiling}(\log_2(9)) = 4$ となり、高さは4である。そして、9個の時刻証明要求をノード $(0, 0) \dots (0, n-1)$ に割り当てると、レベル0において時刻証明要求が割り当てられた最も右のノードは $(0, 8)$ である。

【0294】

ここで、ノード $(0, 8)$ のルートパス $rtPath(4, 0, 8)$ は $rtPath(4, 0, 8) = ((0, 8), (1, 4), (2, 3), (3, 1), (4, 0))$ となる。これにより、各レベルでの手順は、以下の通りになる。

【0295】

レベル0では、 $(0, 9)$ がダミーノードになり、番号10以降が消去される。レベル1では、 $(1, 5)$ がダミーノードとなり、 $5 < i < 2^3 = 8$ であれば、ノード (j, i) は削除される。レベル2では、ノード $(2, 3)$ がダミーノードになる。レベル3および4においては、ダミーノードも消去されるノードもない。この結果、図29に示すような第1次二分木を動的に作成することができる。

【0296】

次に、第3の動的な二分木の構成方法について説明する。第1および第2の動的な第1次二分木の構成方法は、ともに受け付けた時刻証明要求の数が確定した後に、二分木を構成する方法であったが、この方法は、第2の動的な二分木の構成方法をベースに、インクリメンタルに第1次二分木を構成する方法である。ここで、インクリメンタルとは、時刻証明要求を受け付ける都度、そこから計算できる二分木の部分を計算していくという意味で

10

20

30

40

50

ある。この意味で、前もって定めた時間間隔（ラウンドの時間）に受け付ける時刻証明要求の数は予想できないものとする。以下では、受け付ける時刻証明要求の数は予想できないが、その上界 N は見積もることができるとして説明する。尚、この方法においては、第2の動的な第1次二分木の構成方法と同様に、時刻証明要求はすべてレベル0に割り付けられるものとする（ダミーノードを使用する方法である）。

【0297】

図30は、第3の動的な第1次二分木の構成方法のアルゴリズムを示すものであり、該アルゴリズムに従って第1次二分木がインクリメンタルに構成されるようになっている。ここで、前提として以下の定義を行う。

【0298】

・ $K = \text{ceiling}(\log_2(N))$ とする。

【0299】

・ n は受け付けた時刻証明要求の数を示す整数変数とする。初期値は0である。

【0300】

・ k は定められた時間間隔が終了したときの二分木の高さを表す変数とする。

【0301】

($K+1$)個のカウンタの列を、 $i(0), \dots, i(K)$ とする。ここで、 $i(j)$ の初期値は0である($j=0, \dots, K$)。 $i(j)$ はレベル j において、既に生成されたノードの数を表すと同時に、次にレベル j に作成されるノードの番号を表す。

【0302】

・($K+1$)個のブール変数の列を、 $b(0), \dots, b(K)$ とする。ここで、 $b(j)$ の初期値はfalseである($j=0, \dots, K$)。 $b(j)$ は、レベル j にダミーノードがあるか否かを表す。

【0303】

・($K+1$)個の配列の列を、 $A(0), \dots, A(K)$ とする。各配列は、 $2^{(K-j)}$ の長さを持ち、レベル j のノードに割り付けられる値を保持する($j=0, \dots, K$)。ノード(j, i)に対して、 $A(j, i)$ は、 $A(j)[i]$ を表すものとする。ノード(j, i)の左側の子が(j', i')のとき、 $A(\text{left Child}(j, i))$ は $A(j')[i']$ を表す。

【0304】

・ r はダミーノードに割り当てるダミー値を保存する変数である。

【0305】

・ $R(j, i)$ は2つの引数 i, j に対してノード(j, i)に割り当てるべきダミー値を計算する関数である。

【0306】

・ X, X_0, X_1, X_2 は、ノードに割り当てる値を表す変数である。

【0307】

・ $X_1 \ X_2$ は、バイト列で表された2つの値の接続である。

【0308】

・ $h(x)$ は x のハッシュ値を計算する関数である。

【0309】

このような定義のもと、図30の処理手順1が終了すると（定められた時間が終了すると）、 n は、受け付けた時刻処理要求の数、 k は生成された二分木の高さ、 $i(j)$ は、レベル j のノードの数、 $b(j)$ は、レベル j にダミーノードがあるか否か、 $A(j)$ は、レベル j のノードに割り付けられた値、をそれぞれ有することになる。

【0310】

図31は、第3の動的な二分木の構成方法の $n=9$ の場合の具体例を示す図である。即ち、定められた時間間隔が終了したとき、 $n=9$ であったとする。このとき、 $k = \text{ceiling}(\log_2(9)) = 4$ となり、高さは4の二分木を構成することになる。尚、0から $n-1$ までの n 個の時刻処理要求は、処理手順1により、既にノード(0,0), ..., (0,n-1)に割り当てられている。また、処理手順1により、 $i(0)=9, i(1)=4, i(3)=1, i(4)=0$ となっている。

【0311】

10

20

30

40

50

このとき、処理手順2の(2.2)から、ノード(0,9)のルートパス $rtPath(4,0,9)$ は、 $rtPath(4,0,9) = ((0,9), (1,4), (2,3), (3,1), (4,0))$ となる。これから、各レベルの手順は、以下の通りになる。

【0312】

レベル0においては、ステップ(2.3.2.1)より、ノード(0,9)がダミーノードになる。レベル1においては、ステップ(2.3.2.1.5)より、ノード(1,4)に値が割り付けられ、(1,5)がダミーノードになる。レベル2においては、ステップ(2.3.2.1.5)より、ノード(0,2)に値が割り付けられ、(0,3)がダミーノードになる。レベル3においては、ステップ(2.3.2.1)により、ノード(3,1)に値が割り付けられる。レベル4においては、ステップ(2.3.2.1)により、ノード(4,0)に値が割り付けられる。

10

【0313】

この結果、図31に示すような第1次二分木をインクリメンタルに構成することができる。

【0314】

尚、上記実施の形態におけるタイムスタンプ・システム100、200、300および400は、上述した動的な第1次二分木の構成方法のいずれをも採用できるものであり、これにより、クライアント装置3i、203i、303iおよび403iからの時刻証明要求の量的変化に柔軟に対応することができるので、スケーラビリティの高いタイムスタンプ・システムを構築することが可能となる。

【0315】

20

次に、第2次二分木における対象点の監視点に対する認証点を計算するアルゴリズムについて、説明する。前提として、第2次二分木の高さを k とし、対象点の番号を $i0$ 、監視点の番号を $i1$ とし、 $i0 < i1$ とする。このとき、ノード(0, $i0$)のルートパス $rtPath0$ を計算する。同様に、ノード(0, $i1$)のルートパス $rtPath1$ を計算する。すると、 $rtPath0$ と $rtPath1$ は、ある要素以降は一致する。このとき、最初に一致した要素を、ノード(0, $i0$)とノード(0, $i1$)の合流点(confluent point)と呼ぶ。そして、合流点のレフト・チャイルドを、ノード(0, $i0$) (対象点)のノード(0, $i1$) (監視点)に対する認証点(authentication point)とよぶ。

【0316】

一般に、 $i0 < i1$ のとき、認証点は以下の性質を有する。

30

【0317】

(1) 認証点のラベルは、監視点、即ち、ノード(0, $i1$)の受理証明書内補完情報に含まれる。

【0318】

(2) ノード(0, $i1$)の時刻証明処理が終わった時点で、認証点のラベルは、対象点、即ち、ノード(0, $i0$)が受信できる受理証明書内補完情報およびオンライン補完証明書から計算することができる。

【0319】

以下、上記性質の証明を行う。ここで、合流点を(j, i)、そのレフト・チャイルドである認証点を(j', i')とおく。まず、(1)について図32を用いつつ説明する。

40

【0320】

ノード(0, $i1$)のルートパス $rtPath(k, 0, i1)$ において、(0, $i1$)から出発して、合流点に至る直前のノードを(j'', i'')とおく。このとき、認証点は、(j'', i'')の左補完点である。従って、認証パス $authPath(k, 0, i1)$ の定義から、($(j', i'), L$)はノード(0, $i1$)の認証パスに含まれる。よって、($(j', i'), L$)は(0, $i1$)に対する受理証明書内補完情報に含まれる。

【0321】

次に(2)について図33および図34を用いつつ説明する。

【0322】

認証点(j', i')はノード(0, $i0$)のルートパス $rtPath(k, 0, i0)$ に含まれる。こ

50

こで、

$rtPath(k, 0, i0) = ((0, r(0)), \dots, (j', r(j')), (j' + 1, r(j' + 1)), \dots, (k, r(k)))$ とする。

【0323】

$j1 = 0, \dots, j'$ に対して、ノード $(j1, r(j1))$ のラベルを、ノード $(0, i1)$ の時刻証明処理が終わった時点で、ノード $(0, i0)$ が受信できるオンライン補完証明書と受理証明書内補完情報、及びノード $(0, i0)$ のラベルの情報から、以下のように $j1$ について再帰的に計算する。

【0324】

$j1 = 0$ のときは、 $r(0) = i0$ だから、 $(j1, r(j1)) = (0, i0)$ 。 $(0, i0)$ のラベルを $(j1, r(j1))$ のラベルとおく。

10

【0325】

次に、 $j2 < j1$ (j') に対して、 $(j2, r(j2))$ のラベルは計算済みとする。これから $(j1, r(j1))$ のラベルを以下のように計算する。

【0326】

$rtPath(k, 0, i0)$ の高さ $j1-1$ の要素は、高さ $j1$ の要素の、レフト・チャイルドかライト・チャイルドである。どちらであるかによって場合分けする。

【0327】

(a) レフト・チャイルドであるとき、図33に示すように、 $rtPath(k, 0, i0)$ 上の高さ $j1$ の点 $p3$ のラベルは、高さ $j1-1$ の点 $p1$ のラベルとその兄弟 $p2$ のラベルから合成される。高さ $j1-1$ の点 $p1$ のラベル $v1$ は計算済みである。一方 $p2$ のラベル $v2$ は、 $(0, i1)$ の時刻証明処理が終わった時点で、 $(0, i0)$ が受信できるオンライン補完証明書に含まれる。なぜならば、 $(0, i1)$ の時刻証明処理が終わった時点で、図33の A で表された部分木のラベルは計算可能であり、その時点でのオンライン補完証明書に含まれるからである。従って、 $(0, i0)$ の時刻証明要求者は、点 $p3$ のラベル $v3$ は、次のように計算できる。

20

【0328】

$v3 = h(v1, v2)$

(b) ライト・チャイルドであるとき、図34に示すように、 $rtPath(k, 0, i0)$ 上の高さ $j1$ の点 $p3$ のラベルは、高さ $j1-1$ の点 $p1$ のラベルとその兄弟 $p2$ のラベルから合成される。高さ $j1-1$ の点 $p1$ のラベル $v1$ は計算済みである。一方点 $p2$ のラベル $v2$ は、 $(0, i0)$ の要求者に対する受理証明書内補完情報に含まれる。従って、点 $p3$ のラベル $v3$ は、次のように計算できる。

30

【0329】

$v3 = h(v2, v1)$

以上から、再帰法により、 $j1 = 0, \dots, j'$ に対して、ノード $(j1, r(j1))$ のラベルを、 $(0, i1)$ の処理が終わった時点で、 $(0, i0)$ の時刻証明要求者が受信できるオンライン補完証明書と $(0, i0)$ の受理証明書内補完情報から計算することができる。従って、 $j1 = j'$ のラベル、即ち認証点のラベルも、 $(0, i0)$ の時刻証明要求者は計算することができる。

【図面の簡単な説明】

40

【0330】

【図1】本発明の第1の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。

【図2】本発明の第1の実施の形態における第1次二分木の構成を説明する図である。

【図3】本発明の第1の実施の形態における第2次二分木の構成を説明する図である。

【図4】本発明の第1の実施の形態における受理証明書の構成を説明する図である。

【図5】本発明の第1の実施の形態における受理証明書の構成を説明する図である。

【図6】本発明の第1の実施の形態に係るタイムスタンプ・システムの時刻証明方法を説明するシーケンス図である。

【図7】本発明の第1の実施の形態に係るタイムスタンプ・システムの監査情報検証方法

50

を説明するフローチャートである。

【図 8】本発明の第 1 の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図 9】本発明の第 1 の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図 10】本発明の第 2 の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。

【図 11】本発明の第 2 の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図 12】本発明の第 3 の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。

10

【図 13】本発明の第 3 の実施の形態における監査用受理証明書の構成を説明する図である。

【図 14】本発明の第 3 の実施の形態における監査用受理証明書の構成を説明する図である。

【図 15】本発明の第 3 の実施の形態に係るタイムスタンプ・システムの時刻証明方法を説明するシーケンス図である。

【図 16】本発明の第 3 の実施の形態に係るタイムスタンプ・システムの監査情報検証方法を説明するフローチャートである。

【図 17】本発明の第 3 の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するフローチャートである。

20

【図 18】本発明の第 3 の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するフローチャートである。

【図 19】本発明の第 3 の実施の形態における他の形式の監査用受理証明書の構成を説明する図である。

【図 20】本発明の第 3 の実施の形態における他の形式の監査用受理証明書の構成を説明する図である。

【図 21】本発明の第 3 の実施の形態における時刻タグを含む場合の受理証明書の構成を説明する図である。

【図 22】本発明の第 3 の実施の形態における時刻タグを含む場合の受理証明書の構成を説明する図である。

30

【図 23】本発明の第 4 の実施の形態に係るタイムスタンプ・システムの構成を説明する図である。

【図 24】本発明の第 4 の実施の形態に係るタイムスタンプ・システムの監査情報検証方法を説明するフローチャートである。

【図 25】本発明の第 4 の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図 26】本発明の第 4 の実施の形態に係るタイムスタンプ・システムの時刻証明検証方法を説明するシーケンス図である。

【図 27】公表装置が公表するファイルを説明する図である。

40

【図 28】深さの違いを 1 以内に押さえ、ダミーノードを作成しない動的な第 1 次二分木の構成方法を説明する図である。

【図 29】深さを単一にして、ダミーノードを作成する動的な第 1 次二分木の構成方法を説明する図である。

【図 30】インクリメンタルに第 1 次二分木を構成する方法のアルゴリズムを説明する図である。

【図 31】インクリメンタルに第 1 次二分木を構成する方法を説明する図である。

【図 32】第 2 次二分木における認証点を説明する図である。

【図 33】第 2 次二分木における認証点を説明する図である。

【図 34】第 2 次二分木における認証点を説明する図である。

50

【図 3 5】タイムスタンプ・システムの概念を説明する図である。

【図 3 6】線形リンクを用いたタイムスタンプ・システムの概念を説明する図である。

。

【図 3 7】本発明の第 3 の実施の形態の変形例のタイムスタンプ・システムの構成を説明する図である。

【図 3 8】本発明の第 3 の実施の形態の変形例における受理証明書の構成を説明する図である。

【図 3 9】本発明の第 3 の実施の形態の変形例における受理証明書の構成を説明する図である。

【図 4 0】本発明の第 3 の実施の形態の変形例における監査用受理証明書の構成を説明する図である。

10

【図 4 1】本発明の第 3 の実施の形態の変形例における監査用受理証明書の構成を説明する図である。

【図 4 2】本発明の第 3 の実施の形態の変形例のタイムスタンプ・システムの時刻証明方法を説明するシーケンス図である。

【図 4 3】本発明の第 3 の実施の形態の変形例のタイムスタンプ・システムの時刻証明検証方法を説明するフローチャートである。

【図 4 4】本発明の第 3 の実施の形態の変形例における時刻タグを含む場合の受理証明書の構成を説明する図である。

【図 4 5】本発明の第 3 の実施の形態の変形例における時刻タグを含む場合の受理証明書の構成を説明する図である。

20

【図 4 6】本発明の第 1 の実施の形態における受理証明書の他の構成を説明する図である。

。

【図 4 7】直前のラウンドの第 1 次二分木のルート値を現在の第 1 次二分木に割り当てる方法を説明する図である。

【図 4 8】直前のラウンドの第 1 次二分木のルート値を現在の第 1 次二分木に割り当てる方法を説明する図である。

【符号の説明】

【 0 3 3 1 】

1, 7, 7a 時刻証明装置

30

2 時刻情報提供装置

3, 203, 303, 303a, 403 クライアント装置

4 コンピュータネットワーク

5, 6, 8, 8a, 9 監査装置

10 T S A

11 送受信部

12, 72, 72a 時刻証明要求まとめ部

13 時刻情報取得部

14, 14a 時刻証明作成部

15 時刻証明公表部

40

16 受理証明書記憶部

17, 77, 77a 監査情報作成部

20 T A

30 利用者

31 送受信部

32 メッセージ記憶部

33 時刻証明要求部

34 受理証明書記憶部

35, 36, 37, 38 時刻証明検証部

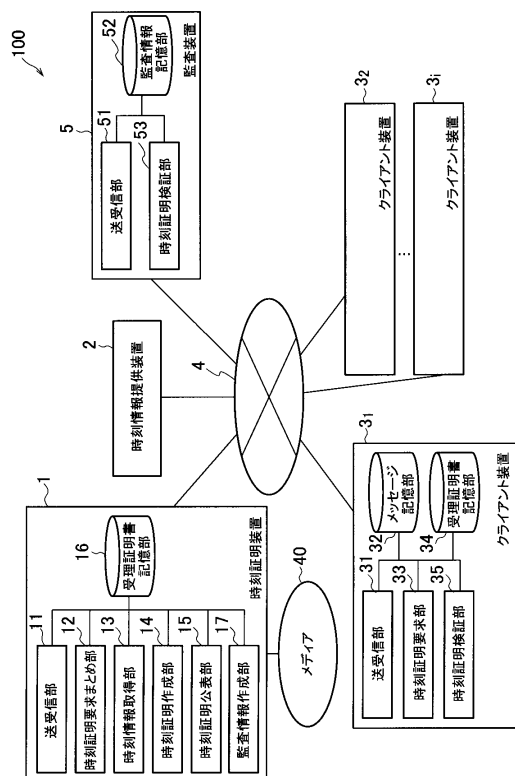
40 メディア等

50

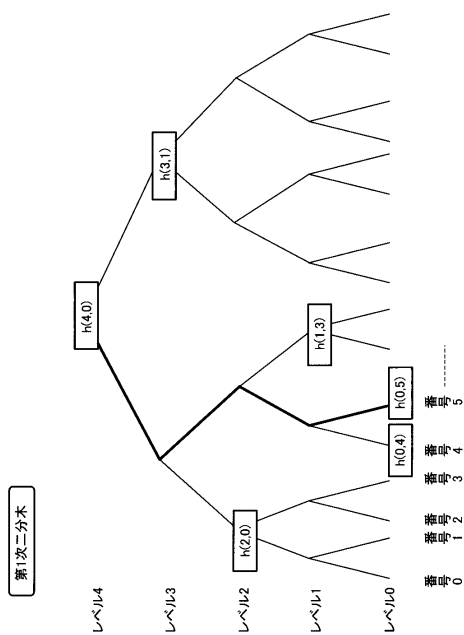
41,42 ファイル
51,81 送受信部
52,82,92 監査情報記憶部
53,93 時刻証明検証部
63 監査情報公開部
73 時刻タグ情報取得部
83,83a 時刻証明公表部
100,200,300,310,400,900,910 タイムスタンプ・システム
800 時刻タグシステム
801 時刻タグ作成業者
802 デジタル放送業者
803 時刻タグ認証業者

10

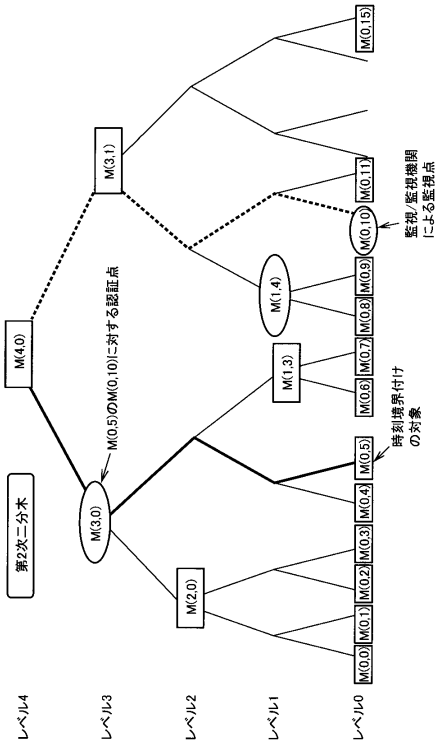
【 図 1 】



【圖 2】



【図 3】



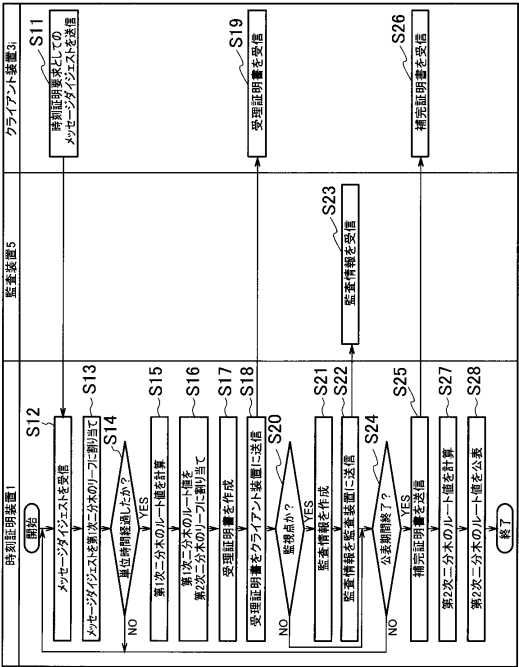
【図 4】

項目	記号	値の例
メッセージ・ダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[[L,h(0,4)), (R,h(1,3)), (L,h(2,0)), (R,h(3,1))]]
第1次二分木のルート値	H	
2次補完情報	HK2	

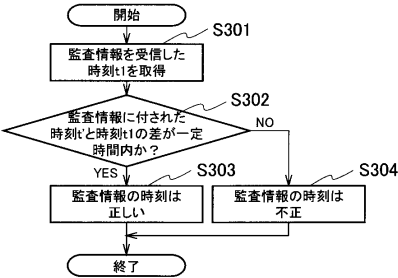
【図 5】

項目	記号	値の例
メッセージ・ダイジェスト	y	
キー付ハッシュを用いる場合のハッシュ・キー	k	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[[L,h(0,4)), (R,h(1,3)), (L,h(2,0)), (R,h(3,1))]]
第1次二分木のルート値	H	
2次補完情報	HK2	

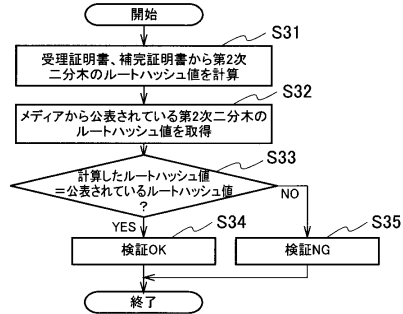
【図 6】



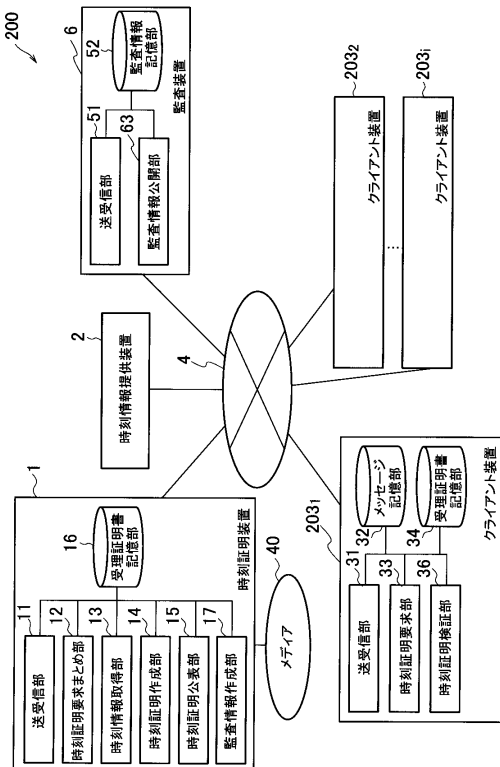
【図 7】



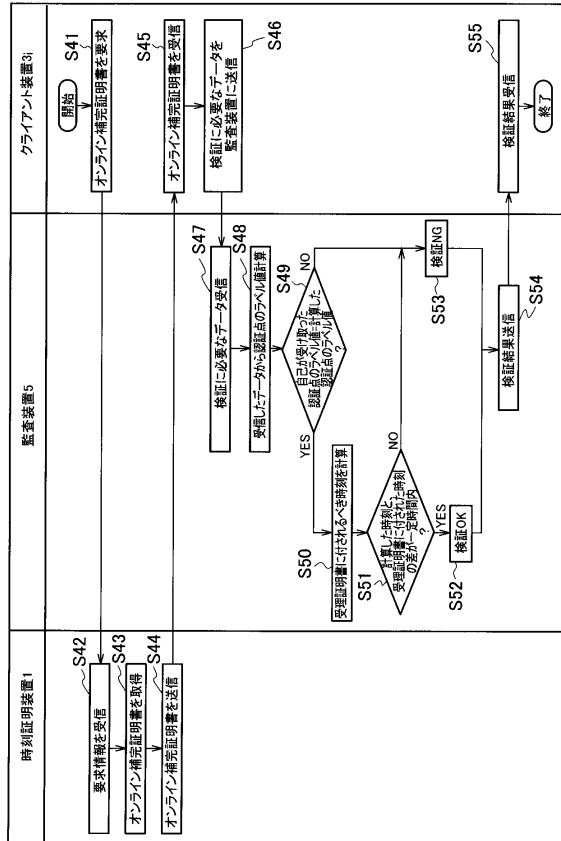
【図 8】



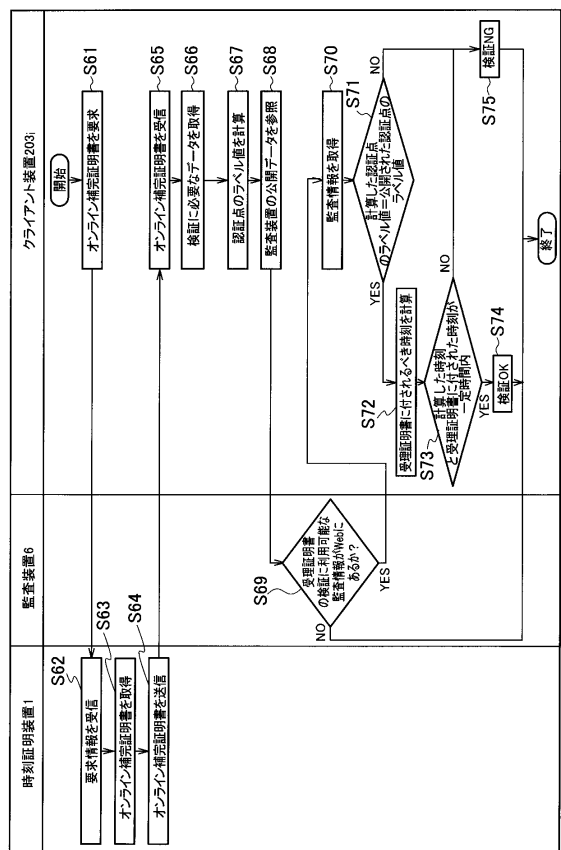
【図 10】



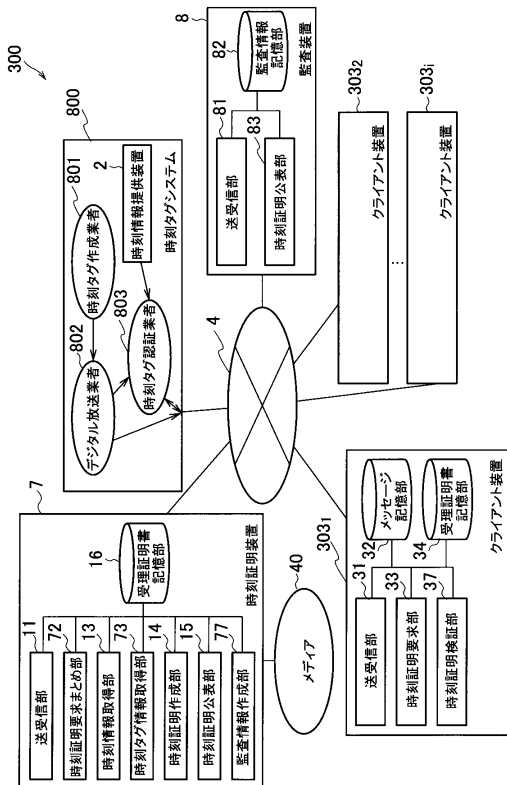
【図 9】



【図 11】



【 図 1 2 】



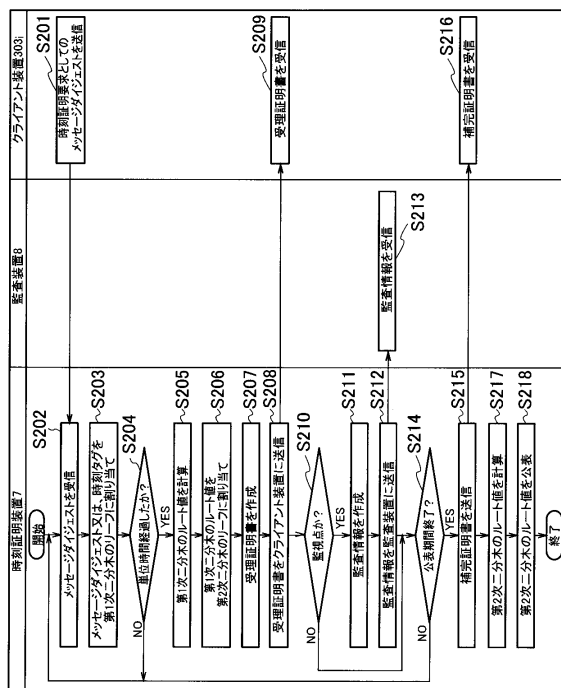
【 図 1 3 】

項目	記号	値の例
時刻タグ	τ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L_h(0,4)), (R_h(1,3)), (L_h(2,0)), (R_h(3,1))]$
第1次二分木のルート値	H	
2次補完情報	HK2	

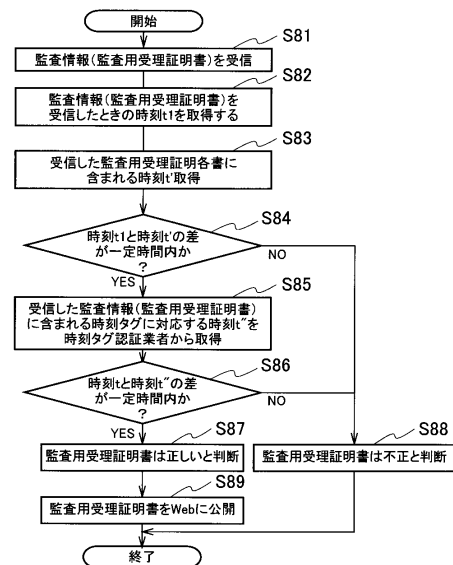
【 図 1 4 】

項目	記号	値の例
時刻タグ	τ	
時刻証明装置がキー付ハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L,h(0,4)), (R,h(1,3)), (L,h(2,0)), (R,h(3,1))]$
第1次二分木のルート値	H	
2次補完情報	HK2	

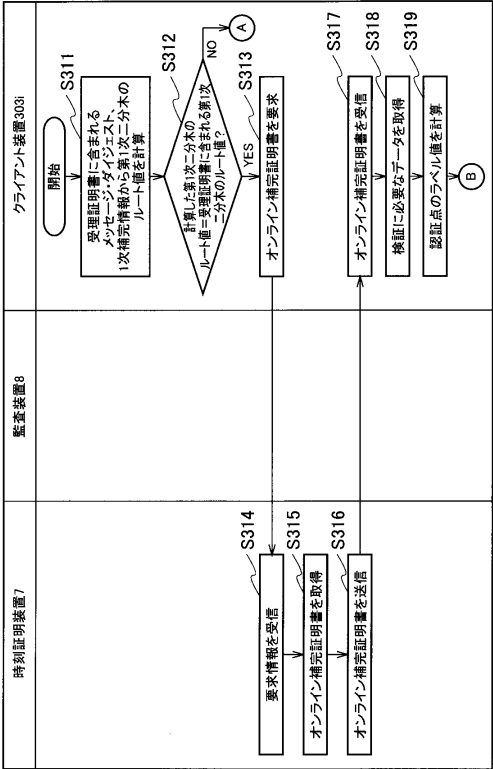
【 図 1 5 】



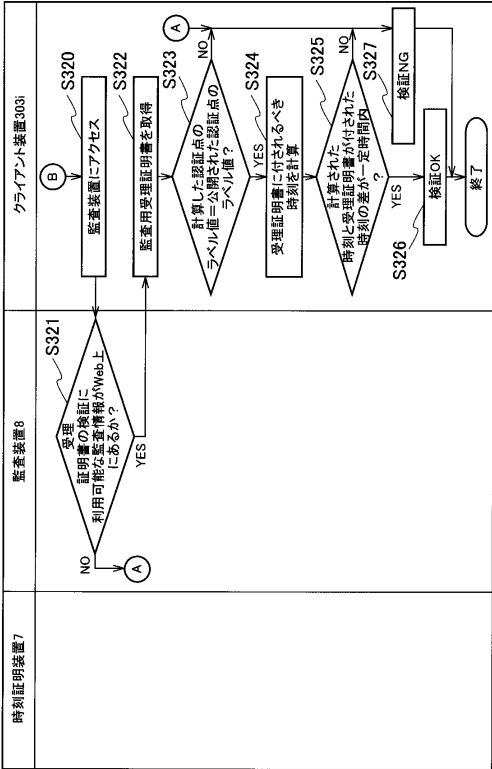
【 図 1 6 】



【図 17】



【図 18】



【図 19】

項目	記号	値の例
時刻タグのハッシュ値であるメッセージ・ダイジェスト	y	$y=h^m(k, \tau)$ で、 τ は監査機関が受信した時刻タグ、 h^m は所定のキー付ハッシュ関数、 k はハッシュ・キー
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L,h(0,4)), (R,h(1,3)), (L,h(2,0)), (R,h(3,1))]$
第1次二分木のルート値	H	
2次補完情報	HK2	

【図 21】

項目	記号	値の例
メッセージ・ダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L,h(0,4)), (R,h(1,3)), (L,h(2,0)), (R,h(3,1))]$
当該の受理証明書に対応する第1次二分木のリーフに割り付けられた時刻タグの並び	$(\tau_1, \dots, \tau_n)$	
第1次二分木のルート値	H	
2次補完情報	HK2	

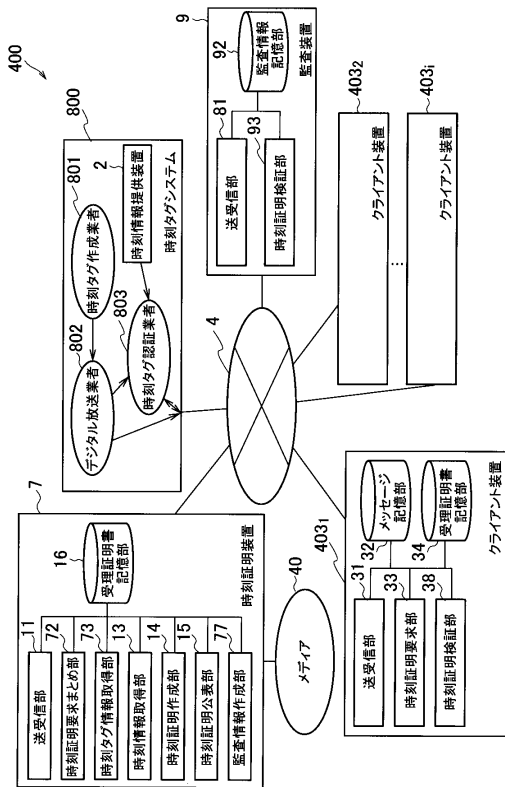
【図 20】

項目	記号	値の例
時刻タグのハッシュ値であるメッセージ・ダイジェスト	y	$y=h^m(k, \tau)$ で、 τ は監査機関が受信した時刻タグ、 h^m は所定のキー付ハッシュ関数、 k はハッシュ・キー
時刻	t	
時刻証明装置がキー付ハッシュを用いる場合のハッシュ・キー	k	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L,h(0,4)), (R,h(1,3)), (L,h(2,0)), (R,h(3,1))]$
第1次二分木のルート値	H	
2次補完情報	HK2	

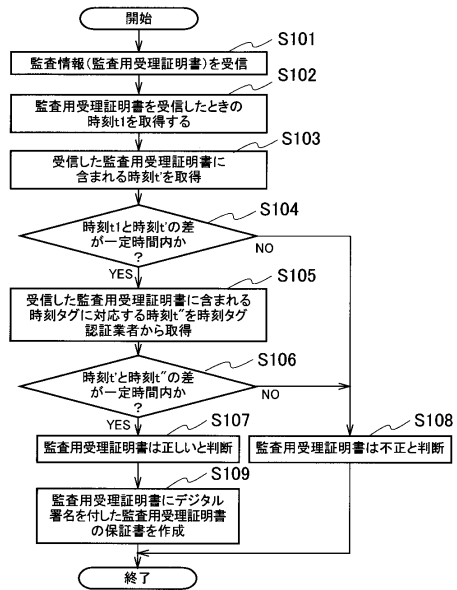
【図 22】

項目	記号	値の例
メッセージ・ダイジェスト	y	
キー付きハッシュを用いる場合のハッシュ・キー	k	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L,h(0,4)), (R,h(1,3)), (L,h(2,0)), (R,h(3,1))]$
当該の受理証明書に対応する第1次二分木のリーフに割り付けられた時刻タグの並び	$(\tau_1, \dots, \tau_n)$	
第1次二分木のルート値	H	
2次補完情報	HK2	

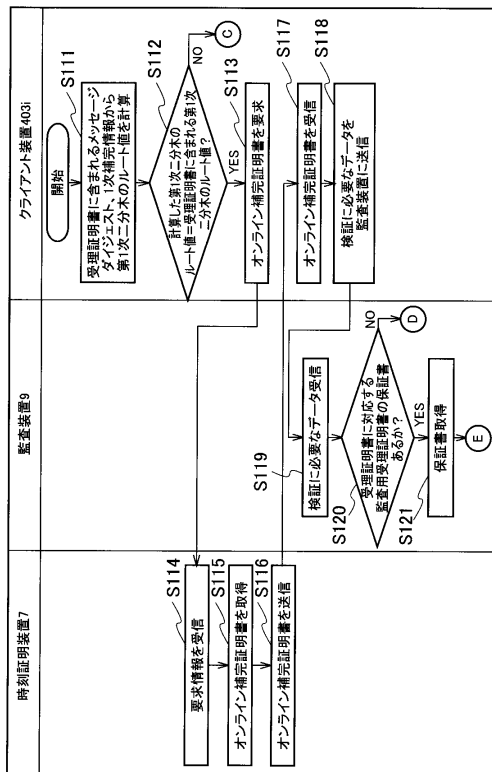
【図 2 3】



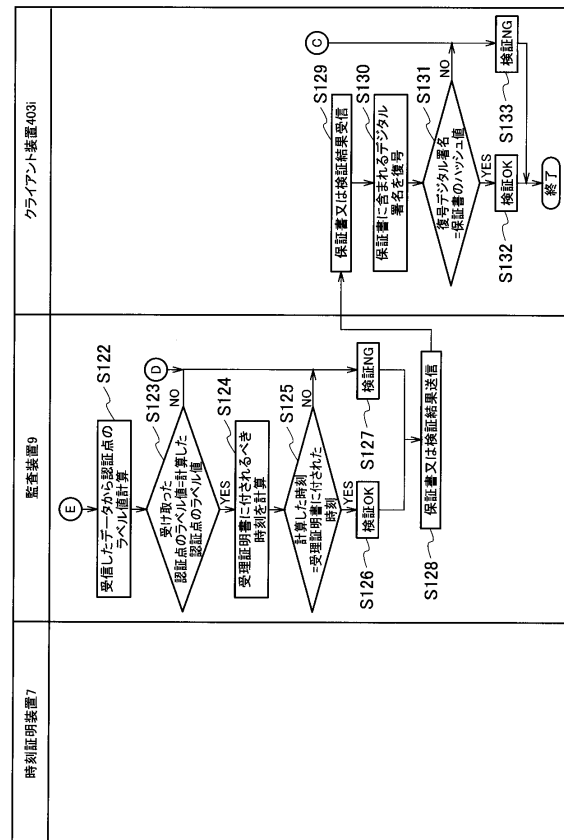
【図 2 4】



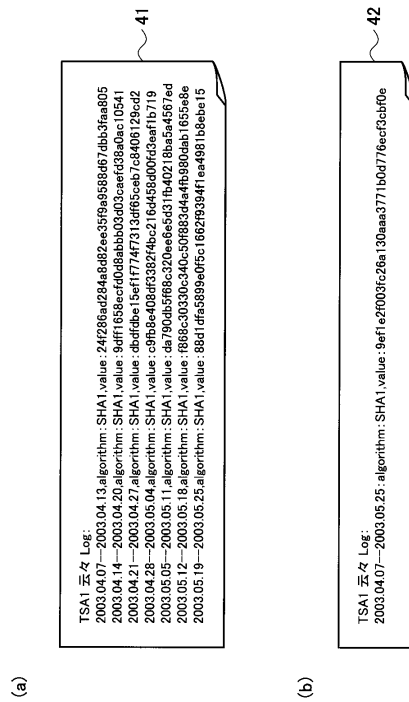
【図 2 5】



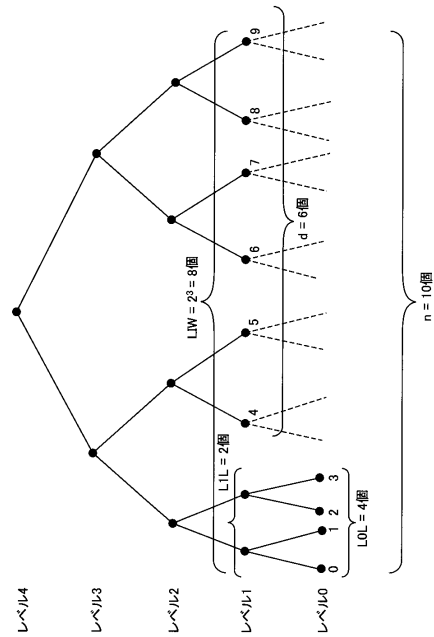
【図 2 6】



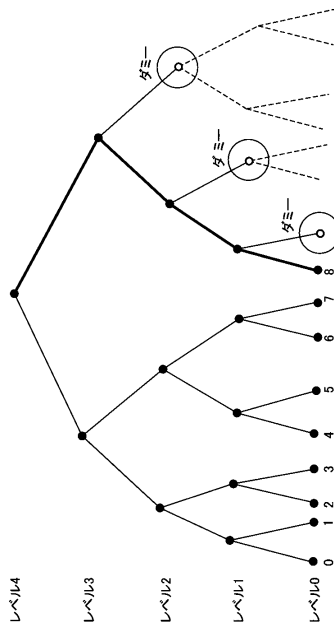
【図 27】



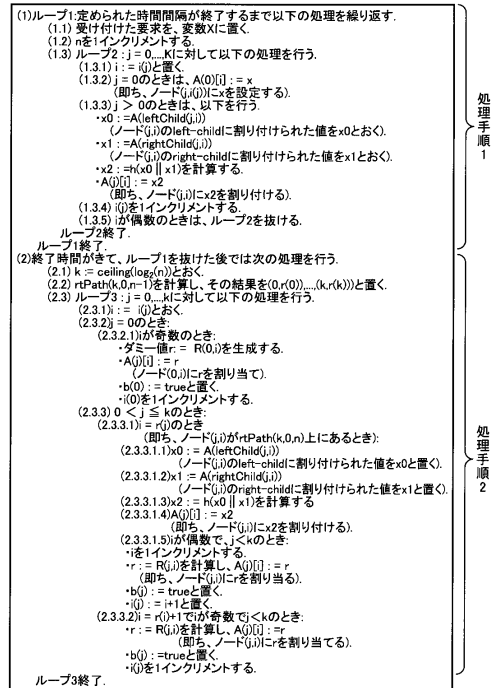
【図 28】



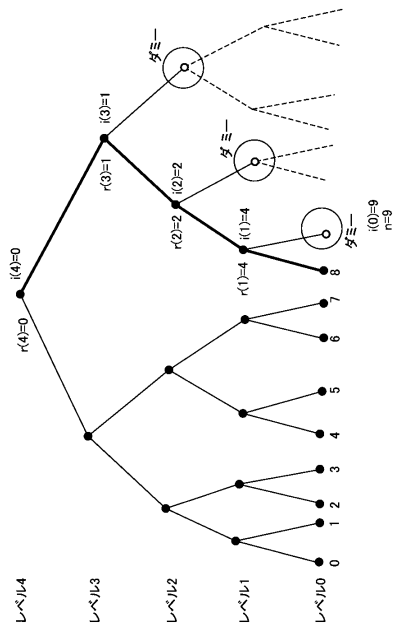
【図 29】



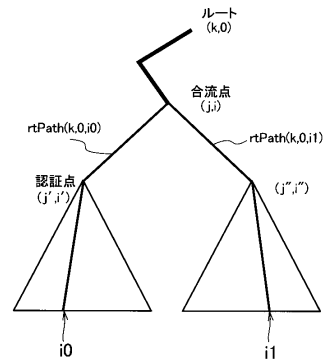
【図 30】



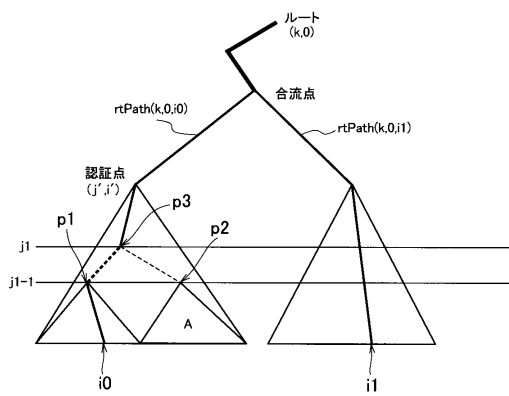
【図 3 1】



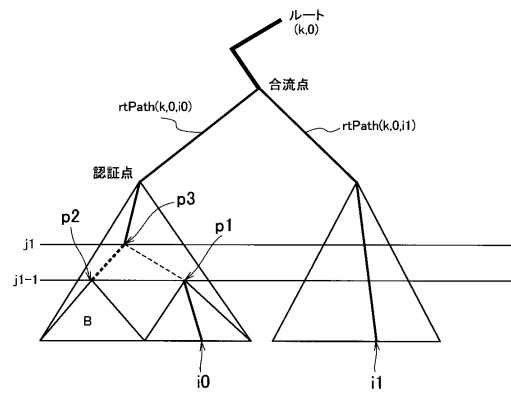
【図 3 2】



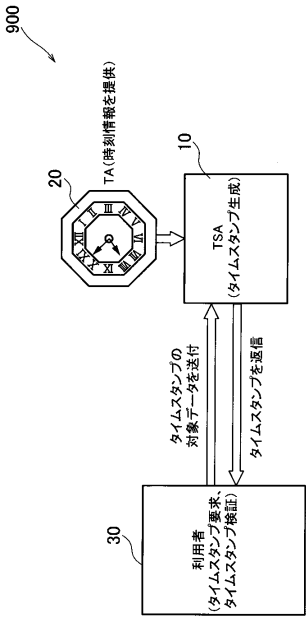
【図 3 3】



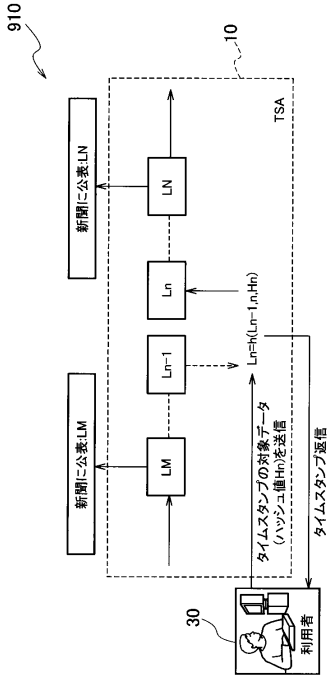
【図 3 4】



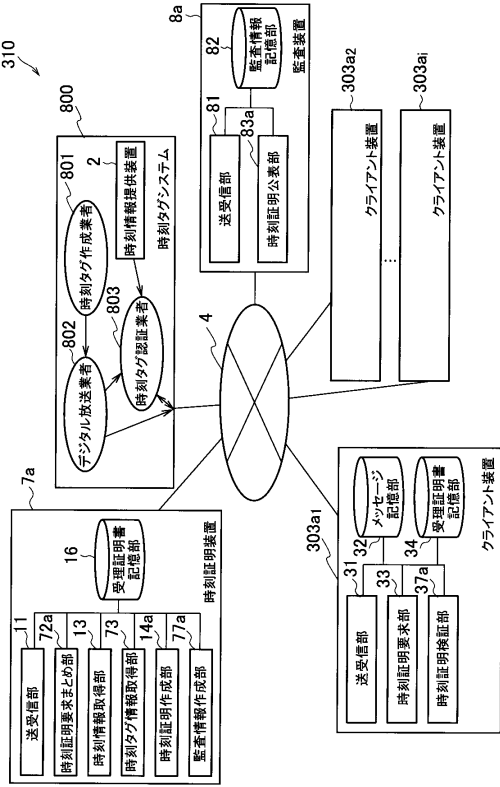
【図 3 5】



【図 3 6】



【図 3 7】



【図 3 8】

項目	記号	値の例
メッセージ・ダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
第1次二分木のルート値	H	

【図 3 9】

項目	記号	値の例
メッセージ・ダイジェスト	y	
キー付ハッシュを用いる場合のハッシュ・キー	k	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(R,h(3,1))]
第1次二分木のルート値	H	

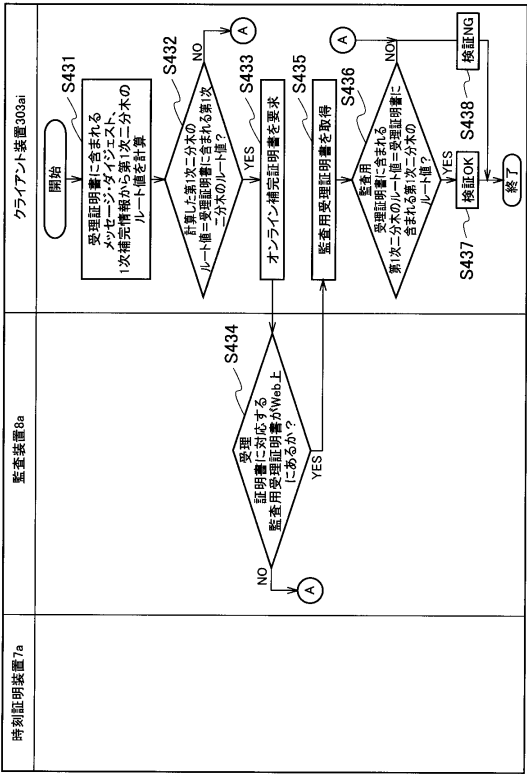
【図 4 0】

項目	記号	値の例
時刻タグ	τ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L_h(0,4)), (R_h(1,3)), (L_h(2,0)), (R_h(3,1))]$
第1次二分木のルート値	H	

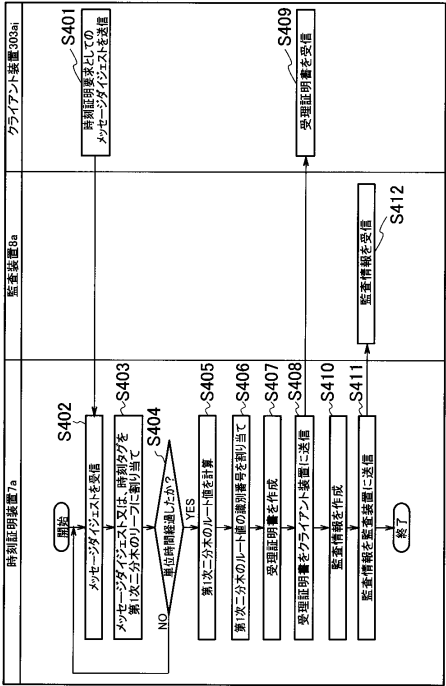
【図 4 1】

項目	記号	値の例
時刻タグ	τ	
時刻証明装置がキー付ハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L_h(0,4)), (R_h(1,3)), (L_h(2,0)), (R_h(3,1))]$
第1次二分木のルート値	H	

【図 4 3】



【図 4 2】



【図 4 4】

項目	記号	値の例
メッセージダイジェスト	y	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L_h(0,4)), (R_h(1,3)), (L_h(2,0)), (R_h(3,1))]$
当該の受理証明書に対応する第1次二分木のルート値に割り付けられた時刻タグの並び	$(\tau_1, \dots, \tau_n)$	
第1次二分木のルート値	H	

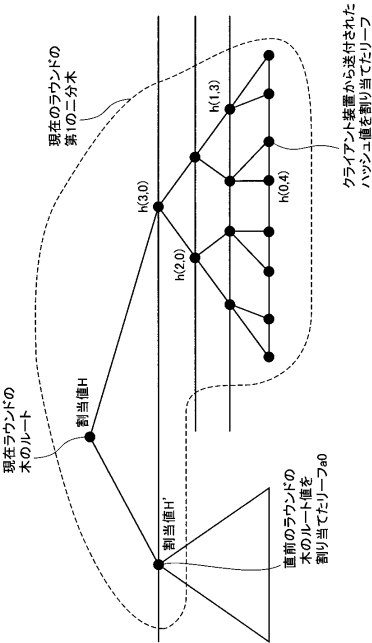
【図 4 5】

項目	記号	値の例
メッセージダイジェスト	y	
キー付きハッシュを用いる場合のハッシュ・キー	κ	
時刻	t	
第1次二分木のルート値の識別番号	n	
1次補完情報	HK1	$[(L_h(0,4)), (R_h(1,3)), (L_h(2,0)), (R_h(3,1))]$
当該の受理証明書に対応する第1次二分木のルート値に割り付けられた時刻タグの並び	$(\tau_1, \dots, \tau_n)$	
第1次二分木のルート値	H	

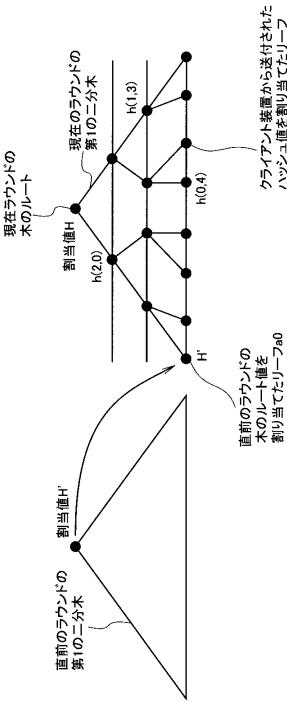
【図 4 6】

項目	記号	値の例
メッセージ・ダイジェスト	y	
現在のラウンドの終結時刻	t1	
前のラウンドの終結時刻	t2	
第1次二分木のルート値の識別番号		
1次補完情報	HK1	[(L,h(0,4)),(R,h(1,3)),(L,h(2,0)),(L,H')]
現在のラウンドの第1次二分木のルート値	H	
2次補完情報	HK2	
直前のラウンドの第1次二分木のルート値	H'	
直前のラウンドの第1次二分木のルート値が割り当てられたリーフの1次補完情報	HK1'	[(R,h(3,0))]

【図 4 7】



【図 4 8】



フロントページの続き

審査官 速水 雄太

(56)参考文献 特表平10-508121(JP,A)
特表2002-530709(JP,A)
米国特許第4309569(US,A)

(58)調査した分野(Int.Cl., DB名)
H04L 9/32