

(11) 特許出願公開番号

特開2011-211677

(P2011-211677A)

(43) 公開日 平成23年10月20日(2011.10.20)

(51) Int.Cl.

F I

テーマコード (参考)

H04L 9/32 (2006.01)

HO 4 L 9/00

6 7 5 B

5 B 2 8 5

G09C 1/00 (2006.01)

G09C 1/00

640D

5 J 104

G06Q 50/00 (2006.01)

G O 6 F 17/60

124

G06F 21/20 (2006.01)

G O 6 F 17/60

140

G O 6 F 15/00

330A

審査請求 有 請求項の数 22 O L (全 21 頁)

(21) 出願番号 特願2010-111575 (P2010-111575)

(22) 出願日 平成22年5月13日 (2010. 5. 13)

(31) 優先權主張番号 10-2010-0027398

(32) 優先日 平成22年3月26日 (2010. 3. 26)

(33) 優先権主張国 韓国 (KR)

(31) 優先權主張番号 10-2010-0036935

(32) 優先日 平成22年4月21日 (2010. 4. 21)

(33) 優先權主張国 韓国 (KR)

(71) 出願人 510132956

ザ インダストリ アンド アカデミック
コーポレーション イン チュンナム
ナショナル ユニバーシティ (アイエーシ
ー)

大韓民国 デジョン 305-764, ユ
ソン-グ, ダン-ドン, 220, チュンナ
ムユニバーシティ

(74) 代理人 100082072

弁理士 清原 義博

(72) 発明者 クワングウー リー

大韓民国 ギョンギード 440-746
，スウォン-シ，ソンギョクアンユニバー
シティ，#27303

[最終頁に続く](#)

(54) 【発明の名称】 認証書基盤のインターネット電子遺言状の管理システム及び方法

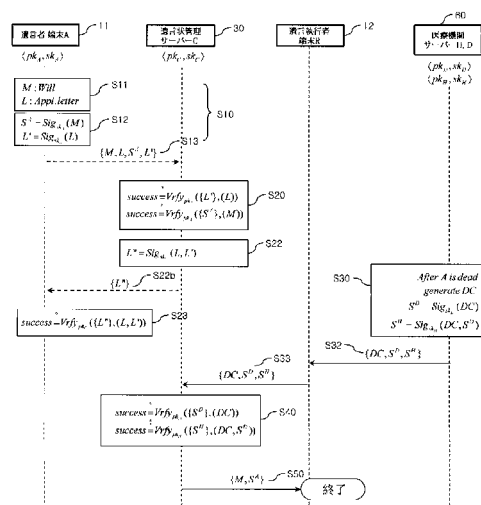
(57) 【要約】

【課題】 認証機関から発給する認証書を利用して申込書及び遺言状に電子署名して否認防止機能を提供するインターネット電子遺言状の管理システム及び方法 を提供する。

【解決手段】 本発明によるインターネット電子遺言状の管理システム及び方法は、(a) 遺言者端末は遺言者の認証書で申込書及び遺言状を電子署名して管理サーバーに伝送するステップと、(b) 遺言状管理サーバーは電子署名された申込書及び遺言状を受信して申込書及び遺言状の電子署名を検証して保存するステップと、(c)

死亡確認機関サーバーは、死亡確認書を電子署名して遺言状管理サーバーに伝送するステップと、(d) 遺言状管理サーバーは、電子署名された死亡確認書を受信して死亡確認書の電子署名を検証するステップと、(e) 死亡確認書を受信した後、遺言執行者端末から遺言状閲覧申込みを受信すれば、遺言状管理サーバーは電子署名された遺言状を伝送するステップと、を含んで構成されることを特徴とする。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

遺言者端末及び遺言執行者端末とネットワークで連結された遺言状管理サーバーにより、認証機関から発給する認証書で電子署名を行って遺言状を管理するインターネット電子遺言状の管理方法であって、

(a) 前記遺言者端末は、遺言者の認証書で申込書及び遺言状を電子署名して前記遺言状管理サーバーに伝送するステップと、

(b) 前記遺言状管理サーバーは、電子署名された申込書及び遺言状を受信して申込書及び遺言状の電子署名を検証して保存するステップと、

(c) 前記遺言状管理サーバーは、遺言者の死亡を確認するステップと、

(d) 遺言者の死亡を確認した後、前記遺言状管理サーバーは、前記遺言執行者端末に電子署名された遺言状を伝送するステップと、を含むこと

を特徴とするインターネット電子遺言状の管理方法。

【請求項 2】

遺言者端末及び遺言執行者端末とネットワークで連結された遺言状管理サーバーにより、認証機関から発給する認証書で電子署名を行って遺言状を管理するインターネット電子遺言状の管理方法であって、

(a) 前記遺言者端末は、遺言者の認証書で申込書及び遺言状を電子署名して秘密鍵とともに前記遺言状管理サーバーに伝送するが、前記遺言状は前記秘密鍵で暗号化するステップと、

(b) 前記遺言状管理サーバーは、電子署名された申込書及び遺言状と、秘密鍵を受信して申込書及び遺言状の電子署名を検証して保存するステップと、

(c) 前記遺言状管理サーバーは、遺言者の死亡を確認するステップと、

(d) 遺言者の死亡を確認した後、前記管理サーバーは、前記遺言執行者端末に電子署名された遺言状及び秘密鍵を伝送するステップと、を含むこと

を特徴とするインターネット電子遺言状の管理方法。

【請求項 3】

前記(a)ステップで、前記遺言者端末は前記遺言状管理サーバーの公開鍵で秘密鍵を暗号化し、

前記(d)ステップで、前記遺言状管理サーバーは暗号化された秘密鍵を自分の個人鍵で復号化して伝送すること

を特徴とする請求項 2 に記載のインターネット電子遺言状の管理方法。

【請求項 4】

前記方法は、前記(b)ステップの以後、

(b 2) 前記遺言状管理サーバーは、前記申込書に前記申込書の電子署名を含ませて自分の認証書で 2 次電子署名を施し、その 2 次電子署名を前記遺言者端末に伝送するステップと、

(b 3) 前記遺言者端末は、前記 2 次電子署名を検証するステップと、をさらに含むこと

を特徴とする請求項 1 又は 2 に記載のインターネット電子遺言状の管理方法。

【請求項 5】

前記(c)ステップで、前記遺言状管理サーバーは、死亡確認機関サーバーから電子署名された死亡確認書を受信して、前記死亡確認書の電子署名を検証することにより遺言者の死亡を確認すること

を特徴とする請求項 1 又は 2 に記載のインターネット電子遺言状の管理方法。

【請求項 6】

前記(c)ステップで、前記電子署名された死亡確認書は遺言執行者端末を経て伝送されること

を特徴とする請求項 5 に記載のインターネット電子遺言状の管理方法。

【請求項 7】

前記死亡確認機関サーバーが医療機関サーバーである場合、前記電子署名された死亡確

10

20

30

40

50

認書は医師及び病院の認証書により電子署名された遺言者の死亡診断書であること
を特徴とする請求項 5 に記載のインターネット電子遺言状の管理方法。

【請求項 8】

前記電子署名された遺言者の死亡診断書は、遺言者の死亡診断書を医師の認証書により
1 次電子署名して前記死亡診断書に 1 次電子署名が含まれて医療機関の認証書により 2 次
電子署名を施して生成されること
を特徴とする請求項 7 に記載のインターネット電子遺言状の管理方法。

【請求項 9】

前記方法は、前記 (b) ステップの以後、
(b 1) 前記遺言状管理サーバーは、少なくとも 2 名の証人端末に電子署名された申込書
及び遺言状を伝送するステップと、
(b 2) 前記証人端末は、証人の認証書で申込書及び遺言状に 2 次電子署名を行って前記
遺言状管理サーバーに送信するステップと、
(b 3) 前記遺言状管理サーバーは、前記証人端末から証人の認証書による 2 次電子署名
を受信して検証するステップと、をさらに含むこと
を特徴とする請求項 1 又は 2 に記載のインターネット電子遺言状の管理方法。

10

【請求項 10】

前記方法は、前記 (b 3) ステップの以後、
(b 4) 前記遺言状管理サーバーは、申込書及び遺言状に 1 次電子署名及び 2 次電子署名
を含ませて自分の認証書で 3 次電子署名を施し、2 次電子署名及び 3 次電子署名を前記遺
言者端末に伝送するステップと、
(b 5) 前記遺言者端末は、前記 3 次電子署名を検証するステップと、をさらに含むこと
を特徴とする請求項 9 に記載のインターネット電子遺言状の管理方法。

20

【請求項 11】

前記方法は、
(f) 前記遺言状管理サーバーは、前記遺言者の認証書満了日の以前の更新期間が渡来す
れば、タイムスタンプング機関 T S A サーバーから前記申込書及び遺言状に対するタイム
スタンプトークンを獲得して、前記申込書及び認証書に追加するステップをさらに含み、
前記 (f) ステップは、追加されたタイムスタンプトークンの満了日以前の更新期間が渡来
すれば、タイムスタンプトークンを再獲得すること
を特徴とする請求項 1 又は 2 に記載のインターネット電子遺言状の管理方法。

30

【請求項 12】

前記遺言状は、マルチメディアデータを含むこと
を特徴とする請求項 1 又は 2 に記載のインターネット電子遺言状の管理方法。

【請求項 13】

前記マルチメディアデータは、音声データ、動画データ、イメージデータの中で少なくと
も一つを含むこと
を特徴とする請求項 12 に記載のインターネット電子遺言状の管理方法。

【請求項 14】

遺言者端末及び遺言執行者端末とネットワークで連結され、認証機関から発給する認証
書で電子署名を行って遺言状を管理するインターネット電子遺言状の管理システムであっ
て、
前記遺言者端末から遺言者の認証書で電子署名された申込書及び遺言状を受信して前記申
込書及び遺言状の電子署名を検証して保存する遺言状受信部と、
遺言者の死亡を確認する死亡確認受信部と、
遺言者の死亡を確認した後、前記遺言執行者端末に電子署名された遺言状を伝送する遺言
状伝送部と、を含むこと
を特徴とするインターネット電子遺言状の管理システム。

40

【請求項 15】

遺言者端末及び遺言執行者端末とネットワークで連結され、認証機関から発給する認証

50

書で電子署名を行って遺言状を管理するインターネット電子遺言状の管理システムであって、

前記遺言者端末から遺言者の認証書で電子署名された申込書及び遺言状、秘密鍵を受信して、前記申込書及び遺言状の電子署名を検証して保存するが、前記遺言状は前記秘密鍵で暗号化される遺言状受信部と、

遺言者の死亡を確認する死亡確認受信部と、

遺言者の死亡を確認した後、前記遺言執行者端末で遺言状及び秘密鍵を伝送する遺言状伝送部と、を含むこと

を特徴とするインターネット電子遺言状の管理システム。

【請求項 16】

前記遺言状受信部は、システム自分の公開鍵で暗号化された秘密鍵を受信し、

前記遺言状伝送部は、暗号化された秘密鍵をシステム自分の個人鍵で復号化して伝送すること

を特徴とする請求項 15 に記載のインターネット電子遺言状の管理システム。

【請求項 17】

前記遺言状受信部は、電子署名が検証されると、申込書に申込書の電子署名を含ませてシステムの認証書で 2 次電子署名を施し、2 次電子署名を前記遺言者端末に伝送するが、前記 2 次電子署名は前記遺言者端末により検証を受けること

を特徴とする請求項 14 又 15 に記載のインターネット電子遺言状の管理システム。

【請求項 18】

前記死亡確認受信部は、死亡確認機関サーバーから電子署名された死亡確認書を受信して、前記死亡確認書の電子署名を検証することにより遺言者の死亡を確認すること

を特徴とする請求項 14 又 15 に記載のインターネット電子遺言状の管理システム。

【請求項 19】

前記死亡確認機関サーバーが医療機関サーバーである場合、前記電子署名された死亡確認書は医師及び病院の認証書により電子署名された遺言者の死亡診断書であること

を特徴とする請求項 18 に記載のインターネット電子遺言状の管理システム。

【請求項 20】

前記システムは、少なくとも 2 名の証人端末に電子署名された申込書及び遺言状を伝送し、前記証人端末から証人の認証書による申込書及び遺言状の 2 次電子署名を受信し、2 次電子署名を検証する証人署名部をさらに含むこと

を特徴とする請求項 14 又 15 に記載のインターネット電子遺言状の管理システム。

【請求項 21】

前記システムは、前記遺言者の認証書満了日の以前の更新期間が渡来すれば、タイムスタンプ機関 T S A サーバーから前記申込書及び遺言状に対するタイムスタンプトークンを獲得して、前記申込書及び認証書に追加する長期検証部をさらに含み、

前記長期検証部は、追加されたタイムスタンプトークンの満了日以前の更新期間が渡来すれば、タイムスタンプトークンを再獲得すること

を特徴とする請求項 14 又 15 に記載のインターネット電子遺言状の管理システム。

【請求項 22】

前記遺言状は、マルチメディアデータを含むこと

を特徴とする請求項 14 又 15 に記載のインターネット電子遺言状の管理システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、認証機関から発給する認証書を利用して申込書及び遺言状に電子署名を施して否認防止機能を提供するインターネット電子遺言状の管理システム及び方法に関する。

【0002】

また、本発明は、電子署名された遺言状に使われた認証書の満了日の以前に電子署名された遺言状に対するタイムスタンプを獲得して長期保管するインターネット電子遺言状の管

10

20

30

40

50

理システム及び方法に関する。

【0003】

また、本発明は、自筆、音声または動画などのマルチメディア形式で作成された遺言状を認証機関から発給する認証書で電子署名して否認防止機能を提供するインターネット電子遺言状の管理システム及び方法に関する。

【背景技術】

【0004】

最近、自分の死後に備えて遺言状をあらかじめ作成することが重要になっている。遺言状は遺言者が死んだ後に遺言者の周辺人にメッセージを伝達する唯一の方法である。もし、ある人が遺言状を作成しないで死亡した場合、財産の分配問題などに関連して紛争が発生することがある。

10

【0005】

したがって、死後に家族、親類、周辺人に残す財産があったら、遺言者がその財産をどのように分配するかを遺言状に書いておく必要がある。遺言者の意思が死後にもまともに反映されるためには可能な効果的な方法で文書化することが重要である。

【0006】

一般的に、遺言状は遺言者や代理人により紙文書形態で作成されるが、このような方式は代理人の手数料やその他の付帯費用によりコストが上昇し、不便な短所がある。

【0007】

このような問題点を解決するために多様なインターネット基盤の遺言状関連サービスが登場した(非特許文献1乃至6参照)。しかし、このようなサービスは遺言状作成と関連して非常に制限された機能のみを提供しており、法的でも認められにくい。

20

【0008】

また、インターネット通信網を利用して遺言状を作成して管理する技術が提案されており、その一例が“インターネット通信網を利用した遺言状作成システム及びその方法”(特許文献1参照)に提示されている。前記特許文献1は、インターネット通信網を介して接続したユーザーが遺言状作成に必要な情報の提供を受けて遺言状を作成し、作成された遺言状に対して認証機関サーバーから認証手続きを実行し、作成された遺言状及び認証された遺言状を保存管理し、インターネット通信網を通じて閲覧または伝送するようにし、遺言者の有故時にはそれに対する情報を公共機関サーバーから提供を受ける技術を提案している。

30

【0009】

しかし、前記特許文献1は、紙形態の認証書を利用しており、遺言状に対する署名も自筆などを使用するので、従来のオフライン上の遺言状作成及び管理方式を単純に電算化したことに過ぎない。また、特許文献1は、公証機関(認証機関サーバー)を利用するので公証費用が追加されるなどの問題点を有している。

【0010】

最近、チアン(Chien)はインターネットへの遺言状作成システムとして自筆電子遺言状(holographic e-will system)、封印電子遺言状(sealed e-will system)などの二つの種類の遺言書作成方式を提案している。チアンは彼の提案した方式が安全で、中華民国の市民法を満足させると言ったが、多少の問題点がある。

40

【0011】

図1の(a)に示したように、チアンの自筆電子遺言状方式は、システム設定ステップ、鍵登録ステップ、遺言状生成ステップ、死亡診断書発給及び提出ステップ、及び遺言状公開ステップで構成される。

【0012】

システム設定ステップで、信頼機関(TAまたは裁判所)はシステムパラメータ $\{E, q, G_1, G_2, e, H_1, H_2, P, P_{TA}\}$ を設定する。 G_1 が楕円曲線E上での群である時、 G_1 と G_2 は素数 q を位数で持つ二つの群であり、 P を G_1 の生成者とする時、関数

50

H_1 はユーザーの ID を群 G_1 の一点で対応させる。暗号学的ハッシュ関数 H_2 を $H_2 : G_2 \rightarrow \{0, 1\}^m$ に定義して、 e は双線形写像 (Bilinear pairing) とするとき、信頼機関 TA は任意の定数 s_{TA} を信頼機関 TA の秘密鍵で選択してシステムの公開鍵 $P_{TA} = s_{TA} \cdot P$ を計算する。

【0013】

登録ステップで、システムに含まれた各構成要素は個人鍵の獲得のために信頼機関 TA に登録しなければならない。遺言者 A の公開鍵は Q_A である。そして、信頼機関 TA 、医師 D 、病院 H は全て個人鍵の獲得のために信頼機関 TA に登録しなければならない。

【0014】

遺言状生成ステップで、遺言者 A は申込書を作成し、作成された申込書を信頼機関 TA に提出する。遺言状が作成されて日付を明示した後、遺言者 A は遺言状と申込書に署名する。最終的に、遺言者 A は遺言状と申込書を TA に提出し、 TA は署名された遺言状と申込書を検証する。もし、署名に対する検証が成功すると、 TA は申込書に署名し、公文書 L を遺言者に確認用で提供する。

【0015】

親戚に死亡診断書 DC を発給及び提出するステップで、遺言者が死亡した後、医師は死亡原因を診断し、電子死亡診断書 DC を親戚 R に発給する。死亡診断書には医師の電子サイン S^D と病院の電子署名 S^H が含まれる。病院は死亡診断書 DC と S^D 、 S^H を遺言者 A の親戚に伝送する。親戚は病院から受けた電子死亡診断書と医師及び病院の署名 $\{DC, S^D, S^H\}$ を裁判所に提出し、遺言状の公開を要請する。

【0016】

遺言状公開ステップで、信頼機関 TA は電子死亡診断書 DC と医師及び病院の署名 $\{DC, S^D, S^H\}$ を検証する。検証方法は次のようである。: $IBSV_{Q_D}((S^D), (DC))$ と $IBSV_{Q_H}(\{S^H\}, (DC, S^D))$ を検証する。 $IBSV_{Q_D}((S^D), (DC))$ は電子死亡診断書 DC の電子署名を検証することで成功または失敗の結果値を返還する。

【0017】

もし、電子死亡診断書 DC とそれに対する電子署名の正当性が検証されると、信頼機関 TA は遺言状 M を遺言者の親戚に伝送する。

【0018】

また、図 1 の (b) に示したように、チアンの封印電子遺言状方式は、自筆電子遺言状方式に比べて、信頼機関 TA の秘密鍵を利用して遺言状を暗号化する。以下では、チアンの自筆電子遺言状方式と異なる部分だけを説明する。

【0019】

すなわち、システム設定ステップで、信頼機関 TA はシステムパラメータを設定し、任意の定数 s_{TA} を TA の秘密鍵で選択し、システムの公開鍵 $P_{TA} = s_{TA} \cdot P$ を計算する。

【0020】

遺言状生成ステップで、遺言者 A は、申込書を作成して遺言者の内容を暗号化するために対称鍵 (Symmetric key) k を使用して暗号化された遺言状 C を得る。対称鍵 k は公開鍵暗号化アルゴリズムを利用して公開鍵 ($Q_{A_Dea_th}$) で暗号化される。次に、遺言者 A は申込書 L と暗号化された遺言状 C に電子署名を施す。そして、遺言者は暗号化された遺言状 C と暗号化された対称鍵 ($Enc_{Q_{A_Dea_th}}(k)$) と申込書 L を信頼機関 TA に伝送する。

【0021】

また、裁判所は遺言者の電子署名が正しく含まれているかを検証した後、遺言者を除いた遺言者が指名した 2 名以上の証人 (X, Y) に暗号化された遺言状 C と申込書 L を伝送して電子署名を受けて適切に署名されたかを検証する。

【0022】

最後に、遺言状を公開するステップで、信頼機関 TA は個人鍵 $S_{A_Dea_th} = s_{TA} \cdot Q_{A_Dea_th}$ を生成し、生成された個人鍵を暗号化された対称鍵 ($= Enc_{Q_{A_Dea_th}}$)

10

20

30

40

50

$t_h(k)$ の計算に使用する。IBDまたはIBEは身元(ID-based)に基盤して復号化または暗号化する関数を意味する。そして、対称鍵 k は封印された遺言状 C を開くために使用され、平文遺言状と署名 $M=(m||S^A)$ は遺言者の親戚に伝達される。

【0023】

しかし、前記チアンの提案は否認防止特性と遺言状の長期署名検証方法の不在という問題点を有している。

【0024】

すなわち、チアンなどが提案した方式は否認防止属性を満足しない。遺言状の有効な電子署名は遺言状が実際に遺言者により生成されたことを証明し、伝送中に遺言が変更されなかったことを証明する。チアンなどが提案した方式で信頼機関TAは裁判所などにより実行されると仮定し、第3の信頼当事者TTA(Trust Third Party)として見なされる。したがって、信頼機関TAはユーザーの個人鍵を知っている。このような理由で、チアンなどが提案した方式で裁判所などの信頼機関TAは遺言者の署名を生成することができるようになる。

【0025】

さらに、チアンが利用するID基盤の電子署名はどの国家でも法的効力を持たない。結果的にチアンなどが提案した方式は電子署名法を基盤して法的効力を持っていない。

【0026】

また、チアンなどが提案した方式は、電子署名に対する長期署名検証方法を提供しない。これは、遺言者が死亡した後に署名に使われた鍵の有効期間が超過すれば、遺言者の遺言状の有効性検証が困難になることを意味する。

【0027】

一般的に電子文書の無欠性は電子署名により保障される。しかし、認証書が有効期間を超過したか、認証書が廃棄された場合には電子署名の検証は不可能になる。

【0028】

【特許文献1】大韓民国公開特許2007-0108996号公報

【非特許文献1】Electronic Time-Stamping、<http://www.e-timestamping.com/chi/about/app1/html>

【非特許文献2】Prepare Life Service、<http://www.geocities.com/preparelife/>.

【非特許文献3】RC Internet Law Center、<http://www.rcclaw.com.tw/>.

【非特許文献4】Your E Will、<http://www.yourewill.com/added.html>

【非特許文献5】Hong Kong e-law service、<http://www.hkelaw.com/>.

【非特許文献6】Taiwan Creative E-integrated services、<http://egov.iii.org.tw/>

【発明の概要】

【発明が解決しようとする課題】

【0029】

したがって、本発明は上述したような従来技術の問題点を解決するためになされたもので、その目的は、認証機関から発給する認証書で申込書及び遺言状に電子署名を施すことにより否認防止機能を提供するインターネット電子遺言状の管理システム及び方法を提供することにある。

【0030】

本発明の他の目的は、電子署名された遺言状に使用された認証書の満了日の以前に電子署名された遺言状に対するタイムスタンプを獲得して長期保管するインターネット電子遺言状の管理システム及び方法を提供することにある。

【課題を解決するための手段】

10

20

30

40

50

【0031】

前記目的を達成するために本発明は、遺言者端末及び遺言執行者端末とネットワークで連結された遺言状管理サーバーにより、認証機関から発給する認証書で電子署名を行って遺言状を管理するインターネット電子遺言状の管理方法であって、(a)前記遺言者端末は遺言者の認証書で申込書及び遺言状に電子署名して前記遺言状管理サーバーに伝送するステップと、(b)前記遺言状管理サーバーは電子署名された申込書及び遺言状を受信して申込書及び遺言状の電子署名を検証して保存するステップと、(c)前記遺言状管理サーバーは遺言者の死亡を確認するステップと、(d)遺言者の死亡を確認した後、前記遺言状管理サーバーは前記遺言執行者端末に電子署名された遺言状を伝送するステップと、を含むことを特徴とする。

10

【0032】

また、本発明は、遺言者端末及び遺言執行者端末とネットワークで連結された遺言状管理サーバーにより、認証機関から発給する認証書で電子署名を行って遺言状を管理するインターネット電子遺言状管理方法であって、(a)前記遺言者端末は遺言者の認証書で申込書及び遺言状を電子署名して秘密鍵とともに前記遺言状管理サーバーに伝送し、前記遺言状は前記秘密鍵で暗号化されるステップと、(b)前記遺言状管理サーバーは電子署名された申込書及び遺言状と秘密鍵を受信して申込書及び遺言状の電子署名を検証して保存するステップと、(c)前記遺言状管理サーバーは遺言者の死亡を確認するステップと、(d)遺言者の死亡を確認した後、前記遺言状管理サーバーは前記遺言執行者端末に電子署名された遺言状及び秘密鍵を伝送するステップと、を含むことを特徴とする。

20

【0033】

また、本発明は、インターネット電子遺言状の管理方法において、前記(a)ステップで、前記遺言者端末は前記遺言状管理サーバーの公開鍵で秘密鍵を暗号化し、前記(d)ステップで、前記遺言状管理サーバーは暗号化された秘密鍵を自分の個人鍵に復号化して伝送することを特徴とする。

【0034】

また、本発明は、インターネット電子遺言状の管理方法において、前記方法は、前記(b)ステップの以後、(b2)前記遺言状管理サーバーは前記申込書に前記申込書の電子署名を含ませて自分の認証書で2次電子署名を施し、2次電子署名を前記遺言者端末に伝送するステップと、(b3)前記遺言者端末は前記2次電子署名を検証するステップと、をさらに含むことを特徴とする。

30

【0035】

また、本発明は、インターネット電子遺言状の管理方法において、前記(c)ステップで、前記遺言状管理サーバーは死亡確認機関サーバーから電子署名された死亡確認書を受信し、前記死亡確認書の電子署名を検証することにより遺言者の死亡を確認することを特徴とする。

【0036】

また、本発明は、インターネット電子遺言状の管理方法において、前記(c)ステップで、前記電子署名された死亡確認書は、遺言執行者端末を経て伝送されることを特徴とする。

【0037】

また、本発明は、インターネット電子遺言状の管理方法において、前記死亡確認機関サーバーが医療機関サーバーである場合、前記電子署名された死亡確認書は医師及び病院の認証書により電子署名された遺言者の死亡診断書であることを特徴とする。

40

【0038】

また、本発明は、インターネット電子遺言状の管理方法において、前記電子署名された遺言者の死亡診断書は、遺言者の死亡診断書を医師の認証書により1次電子署名し、1次電子署名が含まれた死亡診断書に医療機関の認証書により2次電子署名を行って生成されることを特徴とする。

【0039】

また、本発明は、インターネット電子遺言状の管理方法において、前記方法は、前記(b)

50

ステップの以後、(b 1)前記遺言状管理サーバーは少なくとも2名の証人端末に電子署名された申込書及び遺言状を伝送するステップと、(b 2)前記証人端末は証人の認証書で申込書及び遺言状に2次電子署名を行って前記遺言状管理サーバーに送信するステップと、(b 3)前記遺言状管理サーバーは前記証人端末から証人の認証書による2次電子署名を受信して検証するステップと、をさらに含むことを特徴とする。

【0040】

また、本発明は、インターネット電子遺言状の管理方法において、前記方法は、前記(b 3)ステップの以後、(b 4)前記遺言状管理サーバーは申込書及び遺言状に1次電子署名及び2次電子署名を含ませて自分の認証書で3次電子署名を施し、2次電子署名及び3次電子署名を前記遺言者端末に伝送するステップと、(b 5)前記遺言者端末は前記3次電子署名を検証するステップと、さらに含むことを特徴とする。

10

【0041】

また、本発明は、インターネット電子遺言状の管理方法において、前記方法は、(f)前記遺言状管理サーバーは、前記遺言者の認証書満了日の以前の更新期間が渡来すれば、タイムシステムピング機関T S Aサーバーから前記申込書及び遺言状に対するタイムスタンプトークンを獲得して前記申込書及び認証書に追加するステップをさらに含み、前記(f)ステップは、追加されたタイムスタンプトークンの満了日以前の更新期間が渡来すれば、タイムスタンプトークンを再獲得することの特徴とする。

【0042】

また、本発明は、遺言者端末及び遺言執行者端末とネットワークで転結され、認証機関から発給する認証書で電子署名を行って遺言状を管理するインターネット電子遺言状の管理システムにあって、前記遺言者端末から遺言者の認証書に電子署名された申込書及び遺言状を受信して前記申込書及び遺言状の電子署名を検証して保存する遺言状受信部と、遺言者の死亡を確認する死亡確認受信部と、遺言者の死亡を確認した後、前記遺言執行者端末に電子署名された遺言状を伝送する遺言状伝送部と、を含むことを特徴とする。

20

【0043】

また、本発明は、遺言者端末及び遺言執行者端末とネットワークで連結され、認証機関から発給する認証書で電子署名を行って遺言状を管理するインターネット電子遺言状の管理システムにあって、前記遺言者端末から遺言者の認証書に電子署名された申込書及び遺言状、秘密鍵を受信して、前記申込書及び遺言状の電子署名を検証して保存するが、前記遺言状は前記秘密鍵で暗号化される遺言状受信部と、遺言者の死亡を確認する死亡確認受信部と、遺言者の死亡を確認した後、前記遺言執行者端末に遺言状及び秘密鍵を伝送する遺言状伝送部と、を含むことを特徴とする。

30

【0044】

また、本発明は、インターネット電子遺言状の管理システムにおいて、前記遺言状受信部はシステム自分の公開鍵で暗号化された秘密鍵を受信し、前記遺言状伝送部は暗号化された秘密鍵をシステム自分の個人鍵で復号化して伝送することの特徴とする。

【0045】

また、本発明は、インターネット電子遺言状の管理システムにおいて、前記遺言状受信部は、電子署名が検証されると、申込書に申込書の電子署名を含ませてシステムの認証書で2次電子署名を施し、2次電子署名を前記遺言者端末に伝送するが、前記2次電子署名は前記遺言者端末により検証されることを特徴とする。

40

【0046】

また、本発明は、インターネット電子遺言状の管理システムにおいて、前記死亡確認受信部は死亡確認機関サーバーから電子署名された死亡確認書を受信し、前記死亡確認書の電子署名を検証することにより遺言者の死亡を確認することの特徴とする。

【0047】

また、本発明は、インターネット電子遺言状の管理システムにおいて、前記死亡確認機関サーバーが医療機関サーバーである場合、前記電子署名された死亡確認書は医師及び病院の認証書により電子署名された遺言者の死亡診断書であることを特徴とする。

50

【0048】

また、本発明は、インターネット電子遺言状の管理システムにおいて、前記システムは、少なくとも2名の証人端末に電子署名された申込書及び遺言状を伝送し、前記証人端末から証人の認証書による申込書及び遺言状の2次電子署名を受信し、2次電子署名を検証する証人署名部をさらに含むことを特徴とする。

【0049】

また、本発明は、インターネット電子遺言状の管理システムにおいて、前記システムは、前記遺言者の認証書満了日の以前の更新期間が渡来すれば、タイムスタンプトークンを獲得して前記申込書及び認証書に追加する長期検証部をさらに含み、前記長期検証部は追加されたタイムスタンプトークンの満了日以前の更新期間が渡来すれば、タイムスタンプトークンを再獲得することを特徴とする。

10

【発明の効果】

【0050】

本発明によるインターネット電子遺言状の管理システム及び方法によれば、遺言状は遺言者認証書の個人鍵により電子署名されて遺言者自分だけが有効な署名を行うことができるので、遺言状の内容を否認することができなくなる効果がある。

【0051】

また、本発明によるインターネット電子遺言状の管理システム及び方法によれば、遺言状管理機関が遺言状の暗号化のための秘密鍵を保有して認証機関CAが遺言状の電子署名のための認証書を保有することにより、秘密鍵と認証書(個人鍵)の保管が分離されて遺言状の内容が遺言者の死亡時まで公開されない効果がある。

20

【0052】

また、本発明によるインターネット電子遺言状の管理システム及び方法によれば、自筆、音声または動画などのマルチメディア形式で作成された遺言状を電子署名して管理することにより、遺言者が遺言内容を自分が希望するどのような形態でも作成できる効果がある。

【0053】

また、本発明によるインターネット電子遺言状の管理システム及び方法によれば、電子署名された遺言状に対してタイムスタンプを獲得して長期保管することにより、遺言者が死亡した後に電子署名を長期間検証できる効果がある。

30

【図面の簡単な説明】

【0054】

【図1a】従来技術によるインターネット電子遺言状の管理方法を説明するフローチャートである。

【図1b】従来技術によるインターネット電子遺言状の管理方法を説明するフローチャートである。

【図2a】本発明を実施するための全体システムの構成を示した図である。

【図2b】本発明を実施するための全体システムの構成を示した図である。

【図3】本発明の第1の実施形態によるインターネット電子遺言状の管理方法を説明するフローチャートである。

40

【図4】本発明の第2の実施形態によるインターネット電子遺言状の管理方法を説明するフローチャートである。

【図5】図3または図4の表記に対して説明した表である。

【図6】本発明の一実施形態によるインターネット電子遺言状の管理システムの構成に対するブロック図である。

【図7】本発明によるインターネット電子遺言状の管理システム及び方法と従来技術との効果を比べた対比表である。

【発明を実施するための形態】

【0055】

50

以下、添付図面を参照して本発明の望ましい実施の形態について詳細に説明する。

【0056】

また、本発明の説明において同一部分には同一符号を付けて、その繰り返し説明は省略する。

【0057】

先に、本発明を実施するための全体システムの構成の一例に対して図2を参照して説明する。

【0058】

図2の(a)~(b)は、本発明を実施するための全体システムの構成を示した図である。図2に示したように、本発明を実施するための全体システムは、遺言者端末11と、遺言執行者端末12と、死亡確認機関サーバー60と、遺言状管理サーバー30と、認証機関サーバー51と、で構成される。また、証人端末13と、タイムシステムピング機関サーバー52と、をさらに含んで構成することができる。前記サーバーまたは端末は全てネットワーク20に接続される。

10

【0059】

遺言者端末11、遺言執行者端末12、または証人端末13は遺言者、遺言執行者、または証人が利用するPC、ノートブック、ネットブック、PDA、モバイルなどの通常のコンピュータ端末機である。遺言者、遺言執行者、または証人は前記端末を利用して遺言状を作成するか、受信するか、証言するなどの遺言状関連作業を実行する。以下では、遺言者、遺言執行者、または証人の図面符号を前記端末の図面符号と同一に使用する。すなわち、遺言者11がある作業を実行することは遺言者端末11を通じて処理することを意味する。

20

【0060】

一方、遺言執行者12は、遺言者の相続人、親戚、代理人など遺言を執行することができる人々を含む。

【0061】

証人13は遺言状が遺言者11により作成されたことに対する証拠を提供するために遺言者11により任命される。幼児(*Infants*)、禁治産者(*incompetent persons*)、相続人(*heirs*)、相続人の連れ合い(*the heirs' spouses*)、相続人の直系親戚(*heirs' lineal relatives by blood*)などは証人になれない。

30

【0062】

死亡確認機関サーバー60、遺言状管理サーバー30、認証機関サーバー51、またはタイムシステムピング機関サーバー52は通常のサーバーとしてネットワーク20に連結され、ネットワーク20を通じて接続する端末に対してサービスを提供するアプリケーションサーバーである。前記サーバーにはウェブ上でサービスを提供するウェブサーバーまたはウェブアプリケーションサーバーも該当する。

【0063】

前記サーバーは各々死亡確認機関、遺言状管理機関、認証機関、タイムシステムピング機関などにより運営されて前記機関のサービスを提供する。以下では前記機関の図面符号を前記サーバーの図面符号と同一に使用し、前記機関が提供するサービスに関する記載は前記サーバーを通じて提供されることを意味する。

40

【0064】

死亡確認機関60は遺言者の死亡を確認する医療機関、官公署などの機関である。一般的に、人が死亡すれば、医療機関が死亡者に対する死亡診断書を発給して死亡者の死亡を確認する。しかし、失踪による死亡宣告や災難などにより死体を探すことができない場合には関係機関が死亡を確認する。

【0065】

死亡確認機関60が医療機関である場合、医療機関は死亡者に対する(電子)死亡証明書を家族または親戚に発給する責任がある。電子死亡証明書は名前、性別、生年月日、血液型

50

、死亡日、死亡原因、死亡者に対するその他の情報を含む証明書である。この電子文書には医者Dと病院Hにより署名が行われる。

【0066】

認証機関51は公開鍵証明書または認証書を発給する通常の認証機関(Certificate Authority)である。この証明書は該当公開鍵が特定個人や団体、サーバーに属していることを証明する。認証機関の義務は証明書に対する情報をユーザーに確認させることである。

【0067】

認証機関51による証明書はPKI(Public Key Infrastructure)基盤により実行される。すなわち、該当証明書を発給した認証機関51からOCSP(Online Certificate Status Protocol:オンライン証明書状態プロトコル)、CRL(Certificate Revocation List:証明書廃止リスト)またはARL(Authority Revocation List:認証機関の証明書廃止リスト)などの証明書状態確認情報の伝送を受けてその有効性を検証する。

【0068】

タイムスタンプ機関(TSA:Time Stamping Authority)52は電子文書に対するタイムスタンプトークンを生成する。このタイムスタンプトークンは該当電子文書のハッシュ値と時間ソースを含み、TSAの証明書署名が添付される。結局、電子文書の有効性検証可能期間はTSAの証明書有効期間ほど増加される。この有効期間はTSAの証明書満了前に新しいタイムスタンプトークンを追加生成することにより更新することができる。IETF(Internet Engineering Task Force)RFC3126はこのように電子文書の有効性検証可能期間を適切に延長させる方法を提示している。

【0069】

遺言状管理サーバー30は裁判所など遺言状を管理する機関のサーバーとして、作成された遺言状を保管するか閲覧可能とするなどの遺言状管理サービスを提供する。

【0070】

次に、本発明の第1の実施形態によるインターネット電子遺言状の管理方法を図3を参照して説明する。図3は、本発明の第1の実施形態によるインターネット電子遺言状の管理方法を説明するフローチャートであり、図3に示した表記法は図5のようである。

【0071】

図3に示したように、本発明の第1の実施形態によるインターネット電子遺言状の管理方法は、登録ステップ、遺言状生成ステップ、死亡診断書発給及び提出ステップ、及び遺言状公開ステップで構成される。

【0072】

登録ステップ(Registration phase)

向上された電子遺言状システムは電子署名を使用する。各システムの構成要素A、C、H、Dは公開鍵(public key) pk_i と個人鍵(private key) sk_i を生成して証明書の発給を受ける。例えば、遺言者はCAに登録して証明書 $Cert_A$ の発給を受ける。この時、証明書には公開鍵が含まれている。

【0073】

遺言状管理サーバーC、医師D、病院Hは、認証機関CAに証明書を要請し、証明書に公開鍵を含んで受ける。したがって、各々のプロトコル参加者は証明書を持つようになる。個人鍵の場合にはPIN(Personal Identification Number)により保護されると仮定する。

【0074】

2 遺言状生成ステップ(Creating a living will)

遺言者端末は遺言者の証明書で申込書及び遺言状を電子署名して前記遺言状管理サーバーに伝送する(ステップS10)。

10

20

30

40

50

【0075】

すなわち、遺言者A(または遺言者端末11)は、遺言状Mと申込書Lを作成する(ステップS11)。遺言状が作成されて日付を明示した後、遺言者Aは遺言状Mと申込書Lに電子署名を行う(ステップS12)。最後に、遺言者Aは遺言状と申込書を遺言状管理サーバーCに伝送する(ステップS13)。

【0076】

遺言状Mは電子文書で作成されるかまたはマルチメディアデータで作成される。マルチメディアデータ自体が遺言状Mになることもできる。または、遺言状Mは電子文書で作成して前記電子文書にマルチメディアデータを添付することができる。マルチメディアデータは音声データ、動画データ、イメージデータなどを含む。

10

【0077】

音声データは遺言者が自分の遺言内容を音声で録音したデータである。音声データはマイクなどの音声録音装置を通じて録音されてファイル形態で保存される。動画データは遺言者が自分の遺言内容を音声で言うか行動を取ることを映像で録画したデータである。動画データはカムコーダー、カメラまたはウェブカメラなどの映像録画装置を通じて録画されてファイル形態で保存される。イメージデータは遺言者が自分の遺言内容を自筆で筆記用紙に書いたもの、または自分の遺言内容に遺言者の自筆署名や拇印、印鑑などを捺印したものなどをイメージに変換したデータである。イメージデータはカメラ、スキャナなどのイメージ装置を通じてイメージファイルに保存される。

【0078】

前記マルチメディアは音声データ、動画データ、イメージデータの中でいずれの一つで作成するか2個以上で作成することができる。したがって、遺言状Mは電子文書、音声データ、動画データ、イメージデータの中でいずれの一つで作成するか2個以上で作成することができる。

20

【0079】

遺言状Mは前記電子文書またはデータで構成された全体データを一つのデジタルデータまたはデジタル文書で見なす。遺言状Mは一つの電子文書として電子署名されて管理される。以下で、遺言状Mを一つの文書または電子文書で記載しても、遺言状のデータ形式が電子文書に限定されることではない。

【0080】

上述のように、遺言者は自分が便利な方式でどの形態でも選択して遺言することができる。特に、大部分の遺言者は高齢であるか体の調子が悪い場合が多いので、電子文書方式よりは音声、動画、自筆遺言をさらに好む。

30

【0081】

次に、遺言状管理サーバー30は電子署名された申込書及び遺言状を受信して申込書及び遺言状の電子署名を検証して保存する(ステップS20)。すなわち、遺言状管理サーバーCは電子署名された遺言状Mと電子署名された申込書Lを検証する。もし、署名に対する検証に成功すれば、遺言状管理サーバーCは申込書Lに電子署名を施し(ステップS22)、公文書L"を遺言者に確認用で提供する(ステップS22b)。言い換えれば、遺言状管理サーバーは申込書に前記申込書の電子署名を含ませて自分の認証書で2次電子署名を施し、その2次電子署名を前記遺言者端末に伝送する。

40

【0082】

その後、遺言者端末は前記2次電子署名を検証する(ステップS23)。

【0083】

3 親戚に死亡診断書DCを発給するステップ

死亡確認機関サーバー60は死亡確認書を電子署名して遺言状管理サーバー30に伝送する。この時、電子署名された死亡確認書は遺言執行者端末12を経て伝送される。死亡確認機関サーバーが病院などの医療機関サーバーである場合、電子署名された死亡確認書は医師及び病院の認証書により電子署名された遺言者の死亡診断書である。

【0084】

50

すなわち、遺言者が死亡した後、医師は死亡原因を診断して、電子死亡診断書 DC を親戚 R に発給する(ステップ S 3 0)。死亡診断書には医師の電子署名 S^D と病院の電子署名 S^H が含まれる。病院は死亡診断書 DC と S^D 、 S^H を遺言者 A の親戚に伝送する(ステップ S 3 2)。

【0085】

言い換えれば、電子署名された遺言者の死亡診断書は、医師の認証書により 1 次電子署名して、その 1 次電子署名が含まれた死亡診断書を医療機関(または病院)の認証書により 2 次電子署名して生成される。

【0086】

親戚(または遺言執行者)は、病院からもらった電子死亡診断書と医師及び病院の署名{DC、 S^D 、 S^H }を遺言状管理サーバーに提出する(ステップ S 3 3)。

10

【0087】

親戚は電子死亡診断書の提出とともに遺言状の公開を要請することができる。

【0088】

4 遺言状管理サーバーが電子死亡診断書 DC を認証するステップ

遺言状管理サーバー C は電子死亡診断書と医師及び病院の署名{DC、 S^D 、 S^H }を検証する(ステップ S 4 0)。検証方法は次のようである。

【0089】

$V r f y_{p k D}(\{S^D\}, DC) \text{ and } V r f y_{p k H}(\{S^H\}, (DC, S^D))$

もし、電子死亡診断書 DC とそれに対する電子署名の正当性が検証されると、次のステップを執行する。

20

【0090】

5 遺言状管理サーバーが遺言状を公開するステップ

遺言状管理サーバーは遺言状 M と遺言状に対する遺言者の電子署名 S^A を遺言者の親戚に伝送する(ステップ S 5 0)。

【0091】

次に、本発明の第 2 の実施形態によるインターネット電子遺言状の管理方法を図 4 を参照して説明する。図 4 は、本発明の第 2 の実施形態によるインターネット電子遺言状の管理方法を説明するフローチャートであり、図 4 に示した表記法は、図 5 のようである。

【0092】

30

1 登録ステップ(Registration phase)

上述した第 1 の実施形態と同一である。

【0093】

2 遺言状生成ステップ(Creating a living will)

遺言者端末 1 1 は、遺言者の認証書で申込書及び遺言状を電子署名して秘密鍵とともに前記遺言状管理サーバー 3 0 に伝送するが、前記遺言状は前記秘密鍵で暗号化される(ステップ S 1 0)。

【0094】

すなわち、遺言者 A は申込書 L を作成して遺言状の内容を暗号化するために対称鍵(symmetric key) k を使用して暗号化した後、暗号化された遺言状 C を得る。対称鍵 k は公開鍵暗号化アルゴリズムを利用して遺言状管理サーバーの公開鍵 $p k_C$ で暗号化される。

40

【0095】

遺言状 M は電子文書で作成されるかまたはマルチメディアデータで作成される。マルチメディアデータ自体が遺言状 M になることもできる。または、遺言状 M は電子文書で作成して前記電子文書にマルチメディアデータを添付することができる。マルチメディアデータは音声データ、動画データ、イメージデータなどを含む。

【0096】

音声データは遺言者が自分の遺言内容を音声で録音したデータである。音声データはマイクなどの音声録音装置を通じて録音されてファイル形態で保存される。動画データは遺言

50

者が自分の遺言内容を音声で言うか行動を取ることを映像で録画したデータである。動画データはカムコーダー、カメラまたはウェブカメラなどの映像録画装置を通じて録画されてファイル形態で保存される。イメージデータは遺言者が自分の遺言内容を自筆で筆記用紙に書いたもの、または自分の遺言内容に遺言者の自筆署名や拇印、印鑑などを捺印したものなどをイメージに変換したデータである。イメージデータはカメラ、スキャナなどのイメージ装置を通じてイメージファイルに保存される。

【0097】

前記マルチメディアは音声データ、動画データ、イメージデータの中でいずれの一つで作成するか2個以上で作成することができる。したがって、遺言状Mは電子文書、音声データ、動画データ、イメージデータの中でいずれの一つで作成するか2個以上で作成することができる。

10

【0098】

遺言状Mは前記電子文書またはデータで構成された全体データを一つのデジタルデータまたはデジタル文書で見なす。遺言状Mは一つの電子文書として電子署名されて管理される。以下で、遺言状Mを一つの文書または電子文書で記載しても、遺言状のデータ形式が電子文書に限定されることではない。

【0099】

次に、遺言者Aは申込書Lと暗号化された遺言状Cを電子署名する。遺言者は暗号化された遺言状Cと暗号化された対称鍵 $E_{nc_p k_c}(k)$ 、そして申込書Lを遺言状管理サーバーCに伝送する(ステップS15)。

20

【0100】

次に、遺言状管理サーバーは遺言者の電子署名が正しく含まれたかを検証する(ステップS21b)。

【0101】

次に、遺言者を除いた遺言者により指名された2名以上の証人X、Yに暗号化された遺言状Cと申込書Lを送って電子署名を受ける。遺言状管理サーバーは証人から暗号化された遺言状Cと申込書Lを受ければ(ステップS24b)、遺言者Aにより作成された遺言状Cと申込書Lが2名の証人X、Yから正しく署名されたかを検証する(ステップS25b)。

【0102】

すなわち、遺言状管理サーバー30は少なくとも2名の証人端末13に電子署名された申込書及び遺言状を伝送し(ステップS22b)、証人端末13は証人の認証書で申込書及び遺言状に2次電子署名を施し(ステップS23b)、前記遺言状管理サーバーに送信する(ステップS24b)。そして、遺言状管理サーバー30は証人端末13から証人の認証書による2次電子署名を受信して検証する(ステップS25b)。

30

【0103】

そして、遺言状管理サーバーは申込書及び遺言状に1次電子署名及び2次電子署名を含ませて自分の認証書で3次電子署名を行ってから、2次電子署名及び3次電子署名を前記遺言者端末に伝送する(ステップS27b)。そして、遺言者端末11は前記3次電子署名を検証する(ステップS28b)。

【0104】

3 親戚に死亡診断書DCを発給するステップ

40

遺言者が死亡した後、医師は死亡原因を診断して電子死亡診断書DCを親戚Rに発給する。死亡診断書には医師の電子署名 S^D と病院の電子署名 S^H が含まれる(ステップS30)。病院は死亡診断書DCと S^D 、 S^H を遺言者Aの親戚に伝送する(ステップS32)。

【0105】

親戚は病院から受けた電子死亡診断書と医師及び病院の署名{DC、 S^D 、 S^H }を遺言状管理サーバーに提出して(ステップS33)、遺言状の公開を要請する。

【0106】

4 遺言状管理サーバーが電子死亡診断書DCを認証するステップ

遺言状管理サーバーCは電子死亡診断書と医師及び病院の署名{DC、 S^D 、 S^H }を検証

50

する(ステップS40)。検証方法は次のようである。

【0107】

$\text{Verify}_{pk_D}(\{S^D\}, DC)$ and $\text{Verify}_{pk_H}(\{S^H\}, (DC, S^D))$

もし、電子死亡診断書DCとそれに対する電子署名の正当性が検証されると、次のステップを実行する。

【0108】

5 遺言状管理サーバーが遺言状を公開するステップ

遺言状管理サーバーは暗号化された対称鍵kを復号化する個人鍵 sk_C を使用する(ステップS51)。暗号化された遺言状Cを対称鍵kを利用して復号化した後、遺言状内容mと電子署名のために遺言状Mと遺言状内容に対する遺言者の電子署名 S^A 、そして管理サーバーの公開鍵 pk_C を遺言者の親戚に伝送する(ステップS50)。

10

【0109】

次に、本発明の一実施の形態によるインターネット電子遺言状管理システムの構成について図6を参照して説明する。

【0110】

本発明の一実施形態によるインターネット電子遺言状の管理システムは、遺言者端末11、遺言執行者端末12、及び死亡確認機関60とネットワーク20で連結された遺言状管理サーバー30を意味する。

【0111】

図6に示したように、一実施の形態によるインターネット電子遺言状の管理システムは、遺言状受信部31と、死亡確認受信部32と、遺言状伝送部33と、で構成される。また、証人署名部34、長期検証部35をさらに含んで構成できる。

20

【0112】

第1の実施形態として、遺言状受信部31は、遺言者端末11から遺言者の認証書で電子署名された申込書及び遺言状を受信して前記申込書及び遺言状の電子署名を検証して保存する。

【0113】

第2の実施形態として、遺言状受信部31は、遺言者端末11から遺言者の認証書で電子署名された申込書及び遺言状、そして秘密鍵を受信して、前記申込書及び遺言状の電子署名を検証して保存する、この時、前記遺言状は前記秘密鍵で暗号化される。特に、遺言状受信部31はシステム自分の公開鍵で暗号化された秘密鍵を受信する。

30

【0114】

一方、遺言状受信部31は、電子署名が検証されると、申込書に申込書の電子署名を含ませてシステムの認証書で2次電子署名を施し、2次電子署名を前記遺言者端末に伝送する。前記2次電子署名は前記遺言者端末11により検証を受ける。

【0115】

死亡確認受信部32は、死亡確認機関サーバー60から電子署名された死亡確認書を受信して前記死亡確認書の電子署名を検証する。

【0116】

一方、死亡確認機関サーバー60が医療機関サーバーである場合、前記電子署名された死亡確認書は医師及び病院の認証書により電子署名された遺言者の死亡診断書である。

40

【0117】

遺言状伝送部33は、死亡確認書を受信した後、遺言執行者端末12から遺言状閲覧申し込みを受信すれば、電子署名された遺言状を伝送する。

【0118】

第2の実施形態として、遺言状伝送部33は秘密鍵をさらに含んで伝送する。特に、遺言状伝送部33は暗号化された秘密鍵をシステム自分の個人鍵で復号化して伝送する。

【0119】

証人署名部34は、少なくとも2名の証人端末13に電子署名された申込書及び遺言状を伝送し、前記証人端末13から証人の認証書による申込書及び遺言状の2次電子署名を受

50

信して、その２次電子署名を検証する。

【０１２０】

長期検証部３１は、遺言者の認証書満了日の以前の更新期間が渡来すれば、タイムスタンプ機能ＴＳＡサーバー５２から前記申込書及び遺言状に対するタイムスタンプトークンを獲得して前記申込書及び認証書に追加する。また、長期検証部３１は、追加されたタイムスタンプトークンの満了日の以前の更新期間が渡来すれば、タイムスタンプトークンを再獲得する。

【０１２１】

前記インターネット電子遺言状の管理システムの中で省略された部分は、上述したインターネット電子遺言状の管理方法の説明を参照する。

10

【０１２２】

次に、本発明の一実施の形態による遺言状の電子署名に対する長期署名検証について具体的に説明する。

【０１２３】

本発明によるインターネット電子遺言状の管理システム及び方法の安全性は、電子的に作成された遺言状及び申込書に作成された電子署名の安全性を基盤とする。一般的に、電子文書の無欠性は電子署名により保障される。しかし、長期間の時間が経過すれば、電子署名の信頼性は絶対的に保障しにくい。長い時間が経過後、ハッシュアルゴリズムや公開鍵アルゴリズムは脆弱になり、認証書が有効ではないこともある。このような問題を解決するためには電子署名に対する長期署名検証方法が要求される。

20

【０１２４】

このような電子署名に対して長期署名検証が可能にするためには、電子的に署名されたデータが認証書が無効になる前に既に存在したことを証明することが必須的である。これはタイムスタンプにより証明できる。しかし、タイムスタンプも電子署名と同一な問題を有している。このような問題を解決するため、タイムスタンプは既存タイムスタンプが有効性を失う前に、新しいタイムスタンプを獲得しなければならないが、この時、既存オリジナルデータとそれに対するタイムスタンプを含んで再更新する必要がある。

【０１２５】

すなわち、遺言状管理サーバー３０は、前記遺言者の認証書満了日の以前の更新期間が渡来すれば、タイムスタンプ機能ＴＳＡサーバー５２から前記申込書及び遺言状に対するタイムスタンプトークンを獲得して、前記申込書及び認証書に追加する。そして、追加されたタイムスタンプトークンの満了日以前の更新期間が渡来すれば、タイムスタンプトークンを再獲得する。

30

【０１２６】

本発明によるインターネット電子遺言状の管理システム及び方法の効果について、図７を参照してより具体的に説明する。

【０１２７】

本発明によるインターネット電子遺言状の管理システム及び方法は、否認防止(Non-repudiation)、事前公開の防止(Prevention of Pre-reveal)、長期署名検証(Long-term validation)の側面で、次のような効果がある。

40

【０１２８】

否認防止の保安要求事項を満足するため、遺言状の内容は否認できないことである必要がある。インターネット電子遺言状の管理システム及び方法において、遺言状は実際遺言者だけが生成及び修正可能でなければならない。既存チアンなどが提案した方式の場合、ＴＡが遺言者の個人鍵を容易に計算できるか、分かりやすかった。したがって、ＴＡは遺言者と証人の電子署名を生成することが可能であった。これはＴＡが遺言状を偽造することができることを意味する。しかし、本発明は、遺言者だけの自分の個人鍵を持っているから、遺言者自分だけが有効な署名を生成することができる。また、誰も遺言者が死亡した後、遺言状の内容を修正することができないだけでなく、公開的に可能なパラメータを通じて遺言状の電子署名を検証することができる。したがって、本発明は否認防止属性を

50

満足する。

【0129】

封印電子遺言状システムでは、遺言状の事前公開防止要求事項にしたがって、遺言者が死亡してから、病院が死亡証明書を発給する前までは、遺言状の内容が他人に知られてはいけない。ID基盤の暗号システムを使用するチアンなどが提案する方式では、TAが遺言状管理サーバーの個人鍵が分かっている。したがって、TAは暗号化された遺言状を復号化することができる。結果的に、チアンなどが提案した方式は事前公開防止属性を提供しない。しかし、本発明による方式は、公開鍵構造PKIに基盤しているので、CAと管理サーバーが分離されている。言い換えれば、遺言状管理サーバーを除いた誰も暗号化された遺言状を復号化することができないので、遺言者が死亡する前までは遺言状の内容が分からないことを意味する。したがって、本発明は事前公開防止属性を満足する。

10

【0130】

長い時間が経過すると、ハッシュアルゴリズムと公開鍵アルゴリズムは脆弱になって認証書は無効になることある。したがって、電子遺言状システムは遺言者が死亡した後に電子署名を長期間検証できる方法を必要とする。本発明では遺言状に対する電子署名の長期検証方案を提示した。したがって、本発明は長期署名検証の要求事項を満足する。

【0131】

以上、本発明を具体的な実施形態を参照して詳細に説明したが、本発明の範囲は前述の実施形態によって限定されるべきではなく、特許請求の範囲の記載及びこれと均等なものの範囲内で様々な変形が可能なことは、当該技術分野における通常の知識を持つ者には明らかである。

20

【産業上の利用可能性】

【0132】

本発明は、認証機関から発給する認証書で申込書及び遺言状に電子署名して否認防止特性を提供するインターネット電子遺言状の管理システムの開発に適用が可能である。特に、本発明は、電子署名された遺言状に使われた認証書の満了日以前に電子署名された遺言状に対するタイムスタンプを獲得して長期保管するインターネット電子遺言状の管理システムの開発において有用である。

【符号の説明】

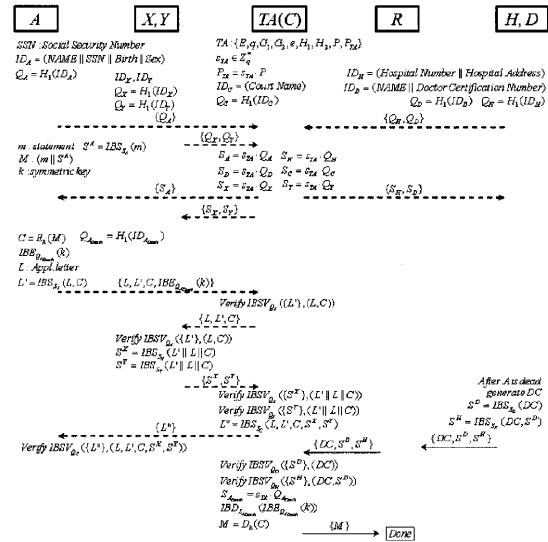
【0133】

30

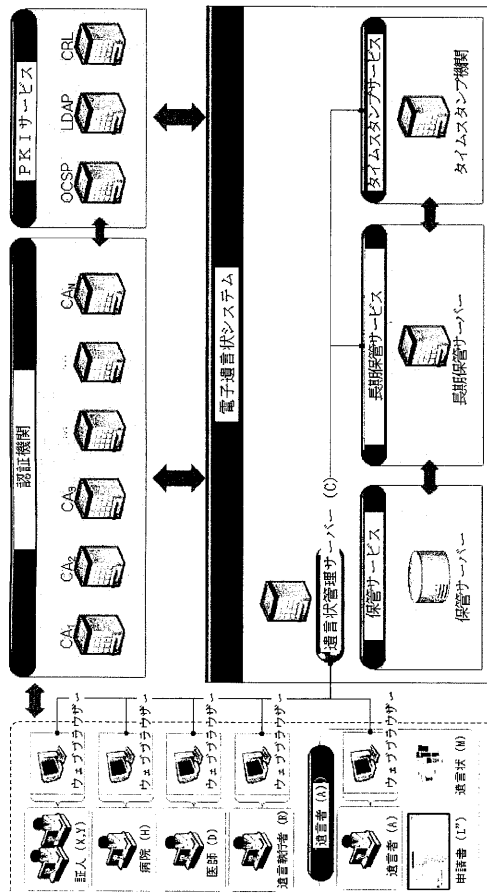
- | | |
|-----|------------------|
| 1 1 | 遺言者端末 |
| 1 2 | 遺言執行者端末 |
| 1 3 | 証人端末 |
| 2 0 | ネットワーク |
| 3 0 | 遺言状管理サーバー |
| 3 1 | 遺言状受信部 |
| 3 2 | 死亡確認受信部 |
| 3 3 | 遺言状伝送部 |
| 3 4 | 証人署名部 |
| 3 5 | 長期検証部 |
| 4 0 | データベース |
| 4 1 | 遺言状DB |
| 4 2 | 秘密鍵DB |
| 5 1 | 認証機関サーバー |
| 5 2 | タイムシステムピング機関サーバー |
| 6 0 | 死亡確認機関サーバー |

40

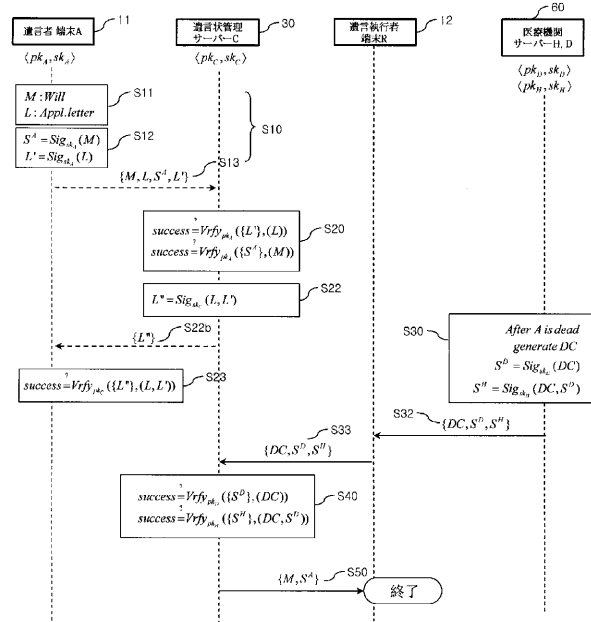
【 図 1 b 】



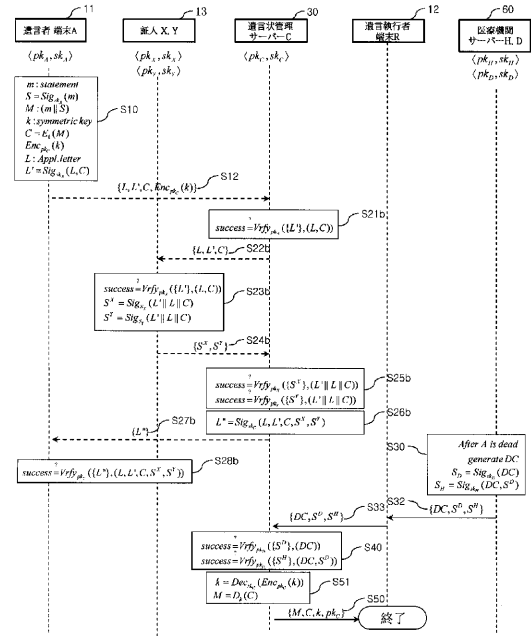
【 図 2 b 】



【図 3】



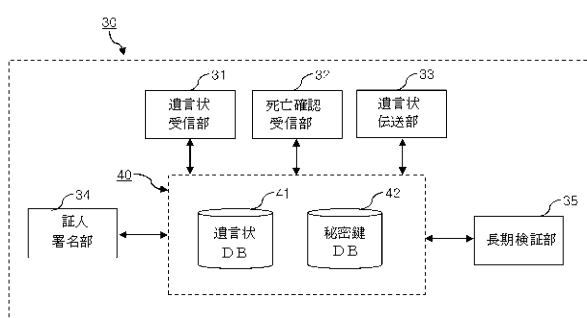
【図 4】



【図 5】

表記	説明
$Cert_x$	Xの認証書
$C \leftarrow Enc_{pk_i}(M)$	公開鍵 pk_i によるメッセージMの公開鍵暗号化
$\{M \text{ or } \perp\} \leftarrow Dec_{sk_i}(C)$	iの個人鍵を使用して暗号化されたメッセージCを公開鍵復号化
$S^i \leftarrow Sig_{sk_i}(M)$	署名者の個人鍵 sk_i でメッセージMを公開鍵署名
$Ver_{pk_i}(S^i, M)$	署名を公開鍵 pk_i で検証して成功又は失敗値を返還
$E_k(M)/D_k(C)$	対称鍵k下でメッセージM又はCを対照的に暗号化/復号化
pk_A	A主体の公開鍵
sk_A	A主体の個人鍵
L^*	遺言状と申込書の受付を遺言者に確認させるために遺言状管理サーバーが発給する公文書
$S^A/S^D/S^H$	A主体、医師、病院の電子署名
$\leftarrow$	暗号化チャンネルによるデータ伝送
$\leftarrow$	公開チャンネルによるデータ伝送

【図 6】



【図 7】

安全性要求	従来技術の一般方式	従来技術の封印方式	本発明の第1の実施形態	本発明の第2の実施形態
否認防止	X	X	○	○
事前公開の防止	N/A	X	N/A	○
長期署名検証	X	X	○	○
台湾市民法の遵守	○	○	○	○
電子署名法の遵守	X	X	○	○

※○：不満足
※X：満足

フロントページの続き

(72)発明者 ドンホ ウォン

大韓民国 ギョンギード 440-746, スウォン-シ, ソンギョクァンユニバーシティ, #
27303

(72)発明者 ソンジョ キム

大韓民国 ギョンギード 440-746, スウォン-シ, ソンギョクァンユニバーシティ, #
27303

Fターム(参考) 5B285 AA04 AA05 BA07 CA43 CA44 CA45 CB47 CB52 CB55 CB62
CB63 CB72 CB74
5J104 AA08 AA16 EA04 EA15 EA16 EA17 EA19 JA21 LA03 LA06
MA05 NA02 NA27 NA37 NA38 PA07 PA14