(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5467591号
(P5467591)

(45)発行日　平成26年4月9日(2014.4.9)　(24)登録日　平成26年2月7日(2014.2.7)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
G06F 21/64	(2013.01)	H04L	9/00	675D
		H04L	9/00	675Z
		G06F	21/24	167A

請求項の数 5　(全 28 頁)

(21)出願番号　特願2009-259524 (P2009-259524)
(22)出願日　平成21年11月13日 (2009.11.13)
(65)公開番号　特開2011-109203 (P2011-109203A)
(43)公開日　平成23年6月2日 (2011.6.2)
審査請求日　平成24年9月5日 (2012.9.5)

(73)特許権者　000002325
セイコーインスツル株式会社
千葉県千葉市美浜区中瀬１丁目８番地
(74)代理人　100142837
弁理士　内野　則彰
(74)代理人　100123685
弁理士　木村　信行
(74)代理人　100166305
弁理士　谷川　徹
(74)代理人　100096655
弁理士　川井　隆
(74)代理人　100091225
弁理士　仲野　均

最終頁に続く

(54)【発明の名称】電子署名用サーバ

(57)【特許請求の範囲】
【請求項１】
携帯端末と通信する通信手段と、
前記通信している携帯端末から、当該携帯端末で撮影した被写体の画像データを特定する画像特定情報と、前記撮影の際の撮影位置を特定する撮影位置特定情報と、前記撮影の撮影日時刻を特定する撮影日時刻特定情報と、を含む画像時刻位置情報を受信する画像時刻位置情報受信手段と、
前記携帯端末の現在位置を検出する現在位置検出手段と、
現在日時刻を取得する現在日時刻取得手段と、
前記受信した画像時刻位置情報の撮影位置が前記検出した現在位置と所定の範囲で一致し、かつ、前記受信した画像時刻位置情報の撮影日時刻が前記取得した現在日時刻と所定の範囲で一致するか否かを判断する判断手段と、
前記判断手段が一致すると判断した場合に、前記受信した画像時刻位置情報に対して電子署名を行う署名手段と、
を具備したことを特徴とする電子署名用サーバ。
【請求項２】
前記判断手段で一致すると判断した場合に、長期署名データを作成する所定のサーバに前記画像時刻位置情報を送信する画像時刻位置情報送信手段と、
前記送信した画像時刻位置情報を用いて作成した長期署名データ用の署名対象データを受信する署名対象データ受信手段と、

を具備し、
前記署名手段は、前記受信した署名対象データに電子署名することにより前記画像時刻位置情報に対して電子署名を行うことを特徴とする請求項１に記載の電子署名用サーバ。
【請求項３】
前記署名手段で電子署名をする前に、当該電子署名に用いる秘密鍵に対応する公開鍵の公開鍵証明書を前記所定のサーバに送信する公開鍵証明書送信手段と、
前記署名手段で電子署名した電子署名値を前記所定のサーバに送信する電子署名値送信手段と、
を具備したことを特徴とする請求項２に記載の電子署名用サーバ。
【請求項４】
前記画像特定情報は、前記画像データを所定の関数で計算した関数値であることを特徴とする請求項１、請求項２、又は請求項３に記載の電子署名用サーバ。
【請求項５】
前記現在位置検出手段は、前記携帯端末が存在する領域を検出し、前記判断手段は、前記受信した画像時刻位置情報の撮影位置が前記検出した領域の内部にある場合に、前記撮影位置と前記現在位置が所定の範囲で一致すると判断することを特徴とする請求項１から請求項４までのうちの何れか１の請求項に記載の電子署名用サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子署名用サーバに関し、例えば、電子データに対して署名を行うものに関する。
【背景技術】
【０００２】
ある日時、ある場所で撮影したある被写体の画像データが、確かにその日時、その場所で撮影され、しかも画像データが改竄されていないことを証明したい場合がある。
これにより、例えば、人を被写体として、当該人がある日時にある場所にいたことを証明したり、あるいは、事故現場を撮影して保険業務に適用したりすることができる。
【０００３】
人がある時刻にある場所に存在したことを証明する技術として、次の特許文献１の「位置証明方法、位置証明サービスシステム及びネットワークシステム」がある。
この技術は、ユーザの指紋を携帯電話で読み取ってサーバに送信し、サーバは、当該指紋によってユーザを認証し、その時刻と携帯電話の位置（携帯電話が通信した基地局より特定）を電子署名する。
【０００４】
しかし、このシステムでは、携帯電話に指紋センサを実装する必要があるという問題があった。
また、画像を撮影して非改竄性を証明したい場合には使用することができなかった。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００３－２８４１１３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明は、携帯端末で撮影した画像データの非改竄性、撮影した日時刻、及び撮影場所を検証できるようにすることを目的とする。
【課題を解決するための手段】
【０００７】
本発明は、前記目的を達成するために、請求項１に記載の発明では、携帯端末と通信す

る通信手段と、前記通信している携帯端末から、当該携帯端末で撮影した被写体の画像データを特定する画像特定情報と、前記撮影の際の撮影位置を特定する撮影位置特定情報と、前記撮影の撮影日時刻を特定する撮影日時刻特定情報と、を含む画像時刻位置情報を受信する画像時刻位置情報受信手段と、前記携帯端末の現在位置を検出する現在位置検出手段と、現在日時刻を取得する現在日時刻取得手段と、前記受信した画像時刻位置情報の撮影位置が前記検出した現在位置と所定の範囲で一致し、かつ、前記受信した画像時刻位置情報の撮影日時刻が前記取得した現在日時刻と所定の範囲で一致するか否かを判断する判断手段と、前記判断手段が一致すると判断した場合に、前記受信した画像時刻位置情報に対して電子署名を行う署名手段と、を具備したことを特徴とする電子署名用サーバを提供する。

請求項２に記載の発明では、前記判断手段で一致すると判断した場合に、長期署名データを作成する所定のサーバに前記画像時刻位置情報を送信する画像時刻位置情報送信手段と、前記送信した画像時刻位置情報を用いて作成した長期署名データ用の署名対象データを受信する署名対象データ受信手段と、を具備し、前記署名手段は、前記受信した署名対象データに電子署名することにより前記画像時刻位置情報に対して電子署名を行うことを特徴とする請求項１に記載の電子署名用サーバを提供する。

請求項３に記載の発明では、前記署名手段で電子署名をする前に、当該電子署名に用いる秘密鍵に対応する公開鍵の公開鍵証明書を前記所定のサーバに送信する公開鍵証明書送信手段と、前記署名手段で電子署名した電子署名値を前記所定のサーバに送信する電子署名値送信手段と、を具備したことを特徴とする請求項２に記載の電子署名用サーバを提供する。

請求項４に記載の発明では、前記画像特定情報は、前記画像データを所定の関数で計算した関数値であることを特徴とする請求項１、請求項２、又は請求項３に記載の電子署名用サーバを提供する。

請求項５に記載の発明では、前記現在位置検出手段は、前記携帯端末が存在する領域を検出し、前記判断手段は、前記受信した画像時刻位置情報の撮影位置が前記検出した領域の内部にある場合に、前記撮影位置と前記現在位置が所定の範囲で一致すると判断することを特徴とする請求項１から請求項４までのうちの何れか１の請求項に記載の電子署名用サーバを提供する。

【発明の効果】

【０００８】

本発明は、被写体を撮影した日時刻、場所を確認してから画像データに対して電子署名することにより、携帯端末で撮影した画像データの非改竄性、撮影した日時刻、及び撮影場所を検証することができる。

【図面の簡単な説明】

【０００９】

【図１】本実施の形態の概要を説明するための図である。
【図２】長期署名システムのネットワーク構成を説明するための図である。
【図３】長期署名データのフォーマットを説明するための図である。
【図４】携帯端末のハードウェア的な構成の一例を示した図である。
【図５】長期署名サーバなどのハードウェア的な構成を説明するための図である。
【図６】長期署名データを作成する手順を説明するためのフローチャートである。
【図７】画像ＧＰＳ情報処理を説明するためのフローチャートである。
【図８】ＥＳ作成処理を説明するためのフローチャートである。
【図９】ＥＳ－Ｔ作成処理を説明するためのフローチャートである。
【図１０】ＥＳ－ＸＬ作成処理を説明するためのフローチャートである。
【図１１】ＥＳ－Ａ（１ｓｔ）作成処理を説明するためのフローチャートである。
【図１２】ＥＳ－Ａ（２ｎｄ）を作成する手順を説明するためのフローチャートである。
【図１３】長期署名データの検証方法を説明するためのフローチャートである。

【発明を実施するための形態】

【００１０】
（１）実施形態の概要
図１は、本実施の形態の概要を説明するための図である。
長期署名データ（ＥＳ－Ａ）は、ＸＭＬによって構成されており、図に示したように、ＥＳ、ＳＴＳ、ＥＳ－Ｔ、検証情報、ＥＳ－ＸＬ、ＡＴＳなどの各要素を用いて構成されている。
ＡＴＳには、第１世代のＡＴＳ（１ｓｔ）、第２世代のＡＴＳ（２ｎｄ）、・・・など各世代のものがあり、これらによって、ＥＳ－Ａは、第１世代のＥＳ－Ａ（１ｓｔ）、第２世代のＥＳ－Ａ（２ｎｄ）などと構成される。
【００１１】
ＡＴＳ（ｎ）（ｎは、１ｓｔ、２ｎｄ、３ｒｄ、・・・）は、ＥＳ－Ａ（ｎ）の内容を検証するアーカイブタイムスタンプである。
長期署名データの作成時はＥＳ－Ａ（１ｓｔ）が作成され、ＡＴＳ（１ｓｔ）の有効期限が切れる前にＡＴＳ（２ｎｄ）を作成してＥＳ－Ａ（２ｎｄ）に更新する、といったように、ＥＳ－Ａ（ｎ）の有効期限が切れる前にＥＳ－Ａ（ｎ＋１）に更新することにより長期署名データの有効期限を永続的に延長していくことができる。
【００１２】
長期署名データは、次のようにして作成される。
携帯端末６で被写体を撮影すると、携帯端末６は、当該被写体の画像データを生成して記憶すると共に、当該画像データのハッシュ値（以下、画像ハッシュ値）を計算する。
また、携帯端末６は、ＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍｓ）機能を備えており、撮影時の現在日時刻と現在位置を検出し、これらを撮影日時刻、及び撮影位置とする。
そして、携帯端末６は、被写体を撮影すると速やかに画像データ、撮影日時刻、及び撮影位置を特定する画像時刻位置情報（以下、画像ＧＰＳ情報）を基地局サーバ５に送信する。なお、これら画像データ、撮影日時、撮影位置を特定する情報は、個別に送信してもよい。
【００１３】
基地局サーバ５は、画像ＧＰＳ情報を受信すると、画像ＧＰＳ情報のうちの撮影日時刻、及び撮影位置が正しいか否かを確認する。
撮影日時刻の確認は、現在日時刻と撮影日時刻を比較することにより行われる。
一方、撮影位置の確認は、携帯端末６の電波を受信した基地局サーバ５によって携帯端末６の存在するエリアを特定し、画像ＧＰＳ情報による撮影位置が当該エリア内にあることを確認することにより行われる。
基地局サーバ５は、撮影日時刻と撮影時刻が正しいことを確認すると、画像ＧＰＳ情報と電子署名に用いる秘密鍵の公開鍵証明書を長期署名サーバ３に送信する。
【００１４】
長期署名サーバ３は、画像ＧＰＳ情報と公開鍵証明書を受信すると、これを用いてＥＳを生成するための署名前ＸＡｄＥＳデータを生成して基地局サーバ５に送信し、基地局サーバ５は、これに秘密鍵で電子署名して電子署名値を長期署名サーバ３に送信する。
長期署名サーバ３は、電子署名値を受信すると、これを用いてＥＳを生成し、引き続きＳＴＳ、ＥＳ－Ｔ、検証情報、ＥＳ－ＸＬを生成する。
そして、長期署名サーバ３は、ＡＴＳ（１ｓｔ）を作成するためのハッシュ値対象データ作成用データを生成してこれを携帯端末６に送信する。
【００１５】
携帯端末６は、ハッシュ値対象データ作成用データを受信すると、これに画像データ、撮影日時刻、撮影位置を付加してハッシュ値を計算して長期署名サーバ３に送信する。
長期署名サーバ３は、このハッシュ値を用いてＡＴＳ（１ｓｔ）を生成し、ＥＳ－Ａ（１ｓｔ）を完成させて携帯端末６に送信する。
その後、ＥＳ－Ａ（１ｓｔ）の有効期限が切れる前に、携帯端末６は、ＥＳ－Ａ（１ｓ

ｔ）を長期署名サーバ３に送信し、長期署名サーバ３は、これをＥＳ－Ａ（２ｎｄ）に更新する。

【００１６】

なお、画像ＧＰＳ情報には、第１の画像ＧＰＳ情報（画像データ、撮影日時刻、撮影位置）、第２の画像ＧＰＳ情報（画像ハッシュ値、撮影日時刻、撮影位置）、第３の画像ＧＰＳ情報（画像ハッシュ値、撮影日時刻ハッシュ値、撮影位置ハッシュ値）などの形態（バリエーション）がある。

第１の画像ＧＰＳ情報は、携帯端末６で被写体が撮影された際に生成される画像ＧＰＳ情報であり、第２の画像ＧＰＳ情報は、携帯端末６が基地局サーバ５に送信する画像ＧＰＳ情報であり、第３の画像ＧＰＳ情報は、長期署名サーバ３が長期署名データを作成する際に使用する画像ＧＰＳ情報である。

画像データと画像ハッシュ値は、何れも画像データを特定する画像特定情報として機能しており、撮影位置と撮影位置ハッシュ値は、何れも撮影位置を特定する撮影位置特定情報として機能しており、撮影日時刻と撮影日時刻ハッシュ値は、何れも撮影日時刻を特定する撮影日時刻特定情報として機能している。

そのため、画像ＧＰＳ情報（第１～第３の画像ＧＰＳ情報）は、画像特定情報、撮影位置特定情報、撮影日時刻特定情報を含む画像時刻位置情報として機能している。

【００１７】

（２）実施形態の詳細

図２は、本実施の形態に係る長期署名システム１のネットワーク構成を説明するための図である。

長期署名システム１は、タイムスタンプサーバ２、長期署名サーバ３、ネットワーク４、基地局サーバ５、携帯端末６、ＣＡのリポジトリサーバ１０、ＣＡ－ＴＳＡのリポジトリサーバ１１などを用いて構成されている。

【００１８】

携帯端末６は、カメラ機能とＧＰＳ機能を有する携帯端末であり、本実施の形態では一例として携帯電話で構成されている。

なお、携帯端末６は、例えば、デジタル式カメラ、携帯型ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ）、携帯型ゲーム機など、カメラ機能とＧＰＳ機能を有する携帯端末であればよい。

【００１９】

携帯端末６は、カメラ機能によって被写体を撮影して画像データを生成する。

また、携帯端末６は、ＧＰＳ機能によって撮影した際の現在日時刻と現在位置を計測することにより、これを撮影日時刻、及び撮影位置として取得する。

携帯端末６は、このようにして撮影と同時に現在日時刻と現在位置を計測して、第１の画像ＧＰＳ情報（画像データ、撮影日時刻、撮影場所）を生成する。

【００２０】

そして、携帯端末６は、画像データのハッシュ値を計算して第２の画像ＧＰＳ情報（画像ハッシュ値、撮影日時刻、及び撮影位置）を生成し、これを基地局サーバ５に送信する。

更に、長期署名データの作成にあたって長期署名サーバ３は、後ほどハッシュ値対象データ作成用データを携帯端末６に送信するが、携帯端末６は、これを処理する機能も有している。

【００２１】

基地局サーバ５は、基地局に設置されたサーバであって、携帯端末６と無線通信し、携帯端末６をネットワーク４に接続する。

基地局サーバ５は、所定の通信エリアをカバーしており、図示しないが、このような基地局サーバ５を複数設置することにより全体の通信エリアをカバーしている。

そして、基地局サーバ５は、携帯端末６が発する電波を受信することにより、携帯端末６が自己の通信エリアに存在することを検出することができる。

即ち、携帯端末６からの電波を受信した基地局サーバ５によって携帯端末６の存在する範囲（以下、存在エリア）を特定することができる。

なお、携帯端末６からの電波を受信する基地局サーバ５が複数ある場合、それらの存在エリアの重なる領域に携帯端末６が存在するため、携帯端末６の存在エリアをより限定することができる。

【００２２】

そして、基地局サーバ５は、第２の画像ＧＰＳ情報を受信すると、第２の画像ＧＰＳ情報の撮影日時刻と現在日時刻を比較し、撮影日時刻が現在日時刻より過去の所定時間以内である場合（例えば、５分前以内）、当該撮影日時刻が正しいと判断する。

また、基地局サーバ５は、第２の画像ＧＰＳ情報の撮影位置と携帯端末６の存在エリアを比較し、撮影位置が存在エリア内にある場合、撮影位置が正しいと判断する。

このように、第２の画像ＧＰＳ情報には、撮影日時刻と撮影場所が含まれているため、基地局サーバ５は、撮影日時刻と撮影場所を検証することができる。

【００２３】

基地局サーバ５は、撮影日時刻と撮影位置が正しいと判断した場合、第２の画像ＧＰＳ情報の撮影日時刻のハッシュ値と撮影場所のハッシュ値（以下、撮影日時刻ハッシュ値、撮影場所ハッシュ値）を計算して、第３の画像ＧＰＳ情報（画像ハッシュ値、撮影日時刻ハッシュ値、撮影場所ハッシュ値）を生成し、これを長期署名サーバ３に送信する。

これは、長期署名データのＥＳ（後述）に撮影日時刻と撮影場所をそのままの形では含めることができないためである。

また、基地局サーバ５は、電子署名用の秘密鍵と、当該秘密鍵に対応する公開鍵の公開鍵証明書を記憶しており、当該公開鍵証明書も長期署名サーバ３に送信する。

【００２４】

すると、長期署名サーバ３は、第３の画像ＧＰＳ情報と公開鍵証明書を用いて署名前ＸＡｄＥＳデータ（図３）を生成して基地局サーバ５に送信してくるが、基地局サーバ５は、これを秘密鍵で電子署名して、当該電子署名による電子署名値を長期署名サーバ３に送信する。

このように、基地局サーバ５は、携帯端末６の第２の画像ＧＰＳ情報を確認する機能と、署名前ＸＡｄＥＳデータに電子署名する機能を有している。

【００２５】

長期署名サーバ３は、証明センタが運営するサーバであって、ネットワーク４を介して基地局サーバ５、携帯端末６、タイムスタンプサーバ２、リポジトリサーバ１０、リポジトリサーバ１１と通信することができる。

長期署名サーバ３は、署名前ＸＡｄＥＳデータを生成して基地局サーバ５に電子署名してもらい、また、ＡＴＳを携帯端末６と協働して作成し、長期署名データを生成する。

【００２６】

その際に、長期署名サーバ３は、タイムスタンプサーバ２でＥＳやＥＳ－ＸＬやＡＴＳにタイムスタンプを発行してもらったり、電子署名に用いた秘密鍵の公開鍵証明書の失効情報、及びタイムスタンプに用いた秘密鍵の公開鍵証明書の失効情報をリポジトリサーバ１０、リポジトリサーバ１１から収集する。

なお、ＡＴＳの作成には第１の画像ＧＰＳ情報を要するが、ＡＴＳの作成に関しては、第１の画像ＧＰＳ情報を携帯端末６からユーザ端末（例えば、ユーザのＰＣ）に移動しておき、長期署名サーバ３とユーザ端末との間で行ってもよい。

【００２７】

タイムスタンプサーバ２は、ＴＳＡ（Ｔｉｍｅ　Ｓｔａｍｐ　Ａｕｔｈｏｒｉｔｙ：タイムスタンプ局）が運営しているサーバであって、電子文書などの電子データにタイムスタンプを発行して時刻証明などを行うサーバであり、本実施の形態では、長期署名サーバ３が長期署名データを作成するに際してＥＳやＥＳ－ＸＬやＡＴＳにタイムスタンプを発行する。

タイムスタンプの発行は、ネットワーク４経由で送信されてきたタイムスタンプ発行対

象の電子データに時刻を付与して秘密鍵で電子署名することにより行われる。
この電子署名の確認は、タイムスタンプに用いた秘密鍵に対応する公開鍵を用いて電子署名が復号化できたことを以て行うことができ、当該電子署名がタイムスタンプサーバ２によってなされたものであることを確認することができる。
【００２８】
リポジトリサーバ１０は、ＣＡ（Ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ：認証局）が運営しているサーバであって、基地局サーバ５が行った電子署名の検証に用いる公開鍵証明書（電子署名に用いた秘密鍵に対応する公開鍵の公開鍵証明書）の失効情報を提供している。
第三者が基地局サーバ５の秘密鍵の公開鍵証明書を用いて基地局サーバ５の電子署名を検証する場合に、当該公開鍵証明書が失効情報に記載されていないことを確認することにより、当該公開鍵証明書が有効な状態で電子署名がなされたことを確認することができる。
失効情報は、例えば、２４時間ごとなど、定期・不定期に最新のものに更新される。
【００２９】
リポジトリサーバ１１は、ＴＳＡ－ＣＡ（Ｔｉｍｅ Ｓｔａｍｐ Ａｕｔｈｏｒｉｔｙ Ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ：タイムスタンプ認証局）が運営するサーバであって、タイムスタンプの検証に用いる公開鍵証明書（タイムスタンプに用いた秘密鍵に対応する公開鍵の公開鍵証明書）の失効情報を提供する。
第三者がタイムスタンプの公開鍵証明書を用いてタイムスタンプサーバ２の電子署名を検証する場合に、当該公開鍵証明書が失効情報に記載されていないことを確認することにより、当該公開鍵証明書が有効な状態でタイムスタンプが発行されたことを確認することができる。
失効情報は、例えば、２４時間ごとなど、定期・不定期に最新のものに更新される。
【００３０】
ネットワーク４は、例えば、インターネットや携帯電話網などの通信ネットワークによって構成されており、携帯端末６と長期署名サーバ３の間の通信、及び長期署名サーバ３とタイムスタンプサーバ２、リポジトリサーバ１０、リポジトリサーバ１１の間の通信を仲介する。
【００３１】
図３は、本実施の形態で使用する長期署名データのフォーマット（長期署名フォーマット）を説明するための図である。
本実施の形態の長期署名データは、ＸＡｄＥＳ（ＸＭＬ Ａｄｖａｎｃｅｄ Ｅｌｅｃｔｒｏｎｉｃ Ｓｉｇｎａｔｕｒｅｓ）の規定に従い、ＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）言語を用いて記述されている。
なお、このフォーマットは一例であって、長期署名データのフォーマットをＸＭＬに限定するものではない。
【００３２】
署名前ＸＡｄＥＳデータは、長期署名サーバ３が電子署名を行う対象となる署名対象データを格納したＸＭＬ要素であって、ＫｅｙＩｎｆｏ、署名対象プロパティ、ＳｉｇｎｅｄＩｎｆｏの各要素から構成されている。署名前ＸＡｄＥＳデータを長期署名サーバ３が電子署名することによりＥＳが生成される。
【００３３】
ＫｅｙＩｎｆｏには、基地局サーバ５が電子署名に用いた秘密鍵に対応する公開鍵の公開鍵証明書が設定されている。公開鍵証明書には、例えば、公開鍵、公開鍵の所有者、認証局、認証局の署名などが含まれている。
署名対象プロパティには、公開鍵証明書のハッシュ値が設定されている。
ＳｉｇｎｅｄＩｎｆｏには、第３の画像ＧＰＳ情報、及び署名対象プロパティのハッシュ値（以下、署名対象プロパティハッシュ値）が設定されている。
【００３４】

ＥＳは、上記の署名前ＸＡｄＥＳデータとＳｉｇｎａｔｕｒｅＶａｌｕｅを要素として構成されている。

ＳｉｇｎａｔｕｒｅＶａｌｕｅには、ＳｉｇｎｅｄＩｎｆｏを基地局サーバ５が秘密鍵で署名した署名値が設定されている。

署名値によってＳｉｇｎｅｄＩｎｆｏが検証されると、これによって署名対象プロパティが検証され、更に署名対象プロパティによってＫｅｙＩｎｆｏが検証されるため、このように、長期署名サーバ３がＳｉｇｎａｔｕｒｅＶａｌｕｅに対して電子署名することにより、署名前ＸＡｄＥＳデータに対する署名が行われる。

【００３５】

ＥＳ－Ｔは、上記のＥＳと署名タイムスタンプを要素として構成されている。

署名タイムスタンプには、ＥＳに対して発行されたＳＴＳ（署名タイムスタンプ）が設定されている。ＳＴＳは、タイムスタンプサーバ２において、ＳｉｇｎａｔｕｒｅＶａｌｕｅのハッシュ値に現在日時刻を付与して、これをタイムスタンプサーバ２の秘密鍵で電子署名したものである。

【００３６】

ＥＳ－ＸＬ（ＥＳ－ＸＬｏｎｇ）は、上記のＥＳ－Ｔと検証情報を要素として構成されている。

検証情報は、証明書群と失効情報群を用いて構成されている。

証明書群は、長期署名サーバ３が署名に用いた秘密鍵の公開鍵証明書と、タイムスタンプサーバ２がタイムスタンプに用いた秘密鍵の公開鍵証明書の認証パス上の公開鍵証明書である。

この認証パスは、ルート認証局は自己署名証明書を発行し、そのルート認証局は子認証局に証明書を発行し、その子認証局は孫認証局に証明書を発行し、・・・、末端の認証局は、個人、証明書所有者に証明書を発行するという証明書信頼チェーンにおいて、公開鍵証明書の検証をルート認証局まで遡って確認するものである。

失効情報群は、証明書群に含まれる各公開鍵証明書の失効情報である。

【００３７】

ＥＳ－Ａ（１ｓｔ）は、上記のＥＳ－ＸＬとＡＴＳ（１ｓｔ）を要素として構成されている。

ＡＴＳ（Ａｒｃｈｉｖｅ　Ｔｉｍｅ　Ｓｔａｍｐ：アーカイブタイムスタンプ）（１ｓｔ）は、第１世代のＡＴＳであって、ＥＳ－Ｔを検証する情報、第３の画像ＧＰＳ情報、長期署名サーバ３による電子署名、タイムスタンプサーバ２によるタイムスタンプなどが含まれており、ＡＴＳ（１ｓｔ）によってＥＳ－ＸＬの正当性を検証することができる。

より詳細には、ＡＴＳ（１ｓｔ）は、ハッシュ値対象データ（第１の画像ＧＰＳ情報、第３の画像ＧＰＳ情報、署名対象プロパティ、ＳｉｇｎｅｄＩｎｆｏ、ＳｉｇｎａｔｕｒｅＶａｌｕｅ、ＫｅｙＩｎｆｏ、ＳＴＳ（署名タイムスタンプ）、証明書群、失効情報群などを連結したデータ）のハッシュ値にタイムスタンプを発行したものを用いて構成されている。

【００３８】

ＥＳ－Ａ（２ｎｄ）は、ＥＳ－Ａ（１ｓｔ）とＡＴＳ（２ｎｄ）を要素として構成されている。

ＡＴＳ（２ｎｄ）は、第２世代のＡＴＳであって、ＥＳ－Ａ（１ｓｔ）を検証する情報、第３の画像ＧＰＳ情報、タイムスタンプサーバ２による電子署名、タイムスタンプサーバ２によるタイムスタンプなどが含まれており、ＡＴＳ（２ｎｄ）によってＡＴＳ（１ｓｔ）の正当性を検証することができる。

図示しないが、更に、ＥＳ－Ａ（２ｎｄ）とＡＴＳ（３ｒｄ）を要素とするＥＳ－Ａ（３ｒｄ）、ＥＳ－Ａ（３ｒｄ）とＡＴＳ（４ｔｈ）を要素とするＥＳ－Ａ（４ｔｈ）、・・・と更に世代を続けることができる。

【００３９】

以上のように構成された長期署名データの各世代は、次のようにして作成される。

まず、ＥＳ－ＸＬまで作成し、署名タイムスタンプと検証情報が有効なうちにＡＴＳ（１ｓｔ）を取得し、ＥＳ－Ａ（１ｓｔ）を構築する。
そして、ＡＴＳ（１ｓｔ）が有効性を失う前（タイムスタンプトークンの公開鍵証明書の有効期限切れや失効前、あるいは、関連する暗号アルゴリズムの危殆化前）に、ＡＴＳ（２ｎｄ）を取得して、ＥＳ－Ａ（１ｓｔ）をＥＳ－Ａ（２ｎｄ）に更新する。
以下、同様にして現在のＡＴＳが有効性を失う前に次世代のＡＴＳを取得する処理を繰り返すことにより、ＥＳ－Ａを更新していく。
このようにして、ＥＳ－ＸＬに対してＡＴＳが時系列的に付与され、最新の世代のＡＴＳが有効期限内である長期署名データが得られる。
このようにして作成された長期署名データの検証については、後ほど詳細に説明する。

【００４０】
図４は、携帯端末６のハードウェア的な構成の一例を示した図である。
携帯端末６は、一例としてカメラ機能とＧＰＳ機能を有する携帯電話であり、以下の構成を有する。
ＣＰＵ２２は、ＥＥＰＲＯＭ３３などに記憶されたプログラムに従って、各種の情報処理や携帯端末６の各部の制御を行う。
例えば、ＣＰＵ２２は、被写体の撮影、被写体を撮影した画像データの保存、画像データのハッシュ値の計算、ＧＰＳによる現在位置と現在日時刻の検出、第１の画像ＧＰＳ情報の生成、第２の画像ＧＰＳ情報の生成と基地局サーバ５への送信などの各処理を行う。

【００４１】
スピーカ２３は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）２２からの制御を受けて、通話相手の音声など、各種音声を出力する。
ディスプレイ２４は、ＣＰＵ２２からの制御を受けて、カメラ３０が写している被写体の画像、被写体を撮影した場合は撮影した画像データによる画像、ネットワーク４に接続するためのブラウザ画面、基地局サーバ５からの通知などの各種の画面を表示する。

【００４２】
キー２５は、例えば、コマンドや文字・記号・数字などを入力するデバイスであって、携帯端末６を操作して被写体を撮影したり、撮影した画像データに対する長期署名データを取得するための操作画面を操作したりするのに用いられる。
マイク２６は、ユーザの通話音声などを電気変換し、これによる音声信号はデジタル化された後ＣＰＵ２２に入力される。
バッテリ２７は、充電可能な二次電池であって、携帯端末６の各部に電力を供給する。

【００４３】
ＲＦ回路２８は、アンテナを備えており、基地局サーバ５とＣＰＵ２２を無線通信により接続する。
これにより、ＣＰＵ２２は、第２の画像ＧＰＳ情報を基地局サーバ５に送信することができる。

【００４４】
ＧＰＳ２９は、携帯端末６の現在位置と現在時刻を検出する。ＧＰＳ２９は、ＧＰＳ衛星からの電波を受信すると共に所定のサーバと通信し、これらの情報を解析して現在位置の緯度経度と現在日時刻を取得する。
カメラ３０は、レンズを用いた光学系で被写体の像をＣＣＤ（Ｃｈａｒｇｅ－Ｃｏｕｐｌｅｄ　Ｄｅｖｉｃｅ）上に投影し、その像を画像データに変換する。
カメラ３０は、シャッターボタンを備えており、ユーザがシャッターボタンを押下すると、ＣＰＵ２２の処理によって、シャッターボタン押下時の画像データがＥＥＰＲＯＭ３３に記憶されて保存される。

【００４５】
ＲＯＭ３１は、読み取り専用のメモリであり、ＣＰＵ２２が携帯端末６で必要とされる機能を発揮するためのプログラムやパラメータなどが記憶されている。
ＲＡＭ３２は、読み書きが可能なメモリであって、ＣＰＵ２２が、画像データのハッシ

ュ値の計算や、ＧＰＳによる現在位置と現在日時刻の解析、その他各種の情報処理を行う際のワーキングメモリを提供する。

【００４６】

ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）３３は、読み書きが可能なメモリであって、バッテリ２７による電力供給がなくても記憶内容を保持することができる。

ＥＥＰＲＯＭ３３には、ＣＰＵ２２に実行させるプログラムを記憶したプログラム部３４、及びカメラ３０で撮影した画像データ、撮影日時刻、撮影位置、その他のデータを記憶するデータ部３５が形成されている。

なお、ＥＥＰＲＯＭ３３は、フラッシュメモリなどの不揮発性メモリでも実現可能である。

【００４７】

図５（ａ）は、長期署名サーバ３のハードウェア的な構成を説明するための図である。

長期署名サーバ３は、ＣＰＵ４１、ＲＯＭ４２、ＲＡＭ４３、通信部４４、記憶部４５などから構成されている。

【００４８】

ＣＰＵ４１は、所定のプログラムに従って各種情報処理や長期署名サーバ３の各部の制御を行い、例えば、基地局サーバ５、携帯端末６、タイムスタンプサーバ２、リポジトリサーバ１０、リポジトリサーバ１１と通信しながら長期署名データを作成する。

【００４９】

ＲＯＭ４２は、読み出し専用メモリであって、長期署名サーバ３が動作するための基本的なプログラムやパラメータなどを記憶している。

ＲＡＭ４３は、読み書きが可能なメモリであって、ＣＰＵ４１がプログラムをロードしたり、各種情報処理を行う際のワーキングメモリを提供する。

通信部４４は、長期署名サーバ３をネットワーク４に接続する。長期署名サーバ３は、通信部４４を介して基地局サーバ５、携帯端末６、タイムスタンプサーバ２、リポジトリサーバ１０、リポジトリサーバ１１などと通信することができる。

【００５０】

記憶部４５は、例えば、ハードディスクなどの大容量の記憶装置を用いて構成されている。

記憶部４５には、プログラム格納部４６とデータ格納部４７が形成されている。

プログラム格納部４６には、ＣＰＵ４１に上記の機能を発揮させるプログラムなどが記憶されている。

データ格納部４７には、公開鍵証明書を発行したＣＡの証明書、ＣＡのルート証明書、ＴＳＡの証明書、ＴＳＡのルート証明書など、長期署名データを作成するために必要な情報が記憶されている。

【００５１】

図５（ｂ）は、基地局サーバ５のハードウェア的な構成を説明するための図である。

基地局サーバ５は、ＣＰＵ５１、ＲＯＭ５２、ＲＡＭ５３、通信部５５、記憶部５６などから構成されている。

ＣＰＵ５１は、所定のプログラムに従って各種情報処理や基地局サーバ５の各部の制御を行う。具体的には、例えば、携帯端末６のネットワーク４への接続を仲介する他、携帯端末６から第２の画像ＧＰＳ情報を受信して、当該第２の画像ＧＰＳ情報の撮影日時刻と撮影位置が正しいか確認したり、長期署名サーバ３から送信されてきた署名前ＸＡｄＥＳデータに電子署名したりする。

【００５２】

ＲＯＭ５２は、読み出し専用メモリであって、基地局サーバ５が動作するための基本的なプログラムやパラメータなどを記憶している。

ＲＡＭ５３は、読み書きが可能なメモリであって、ＣＰＵ５１がプログラムをロードしたり、各種情報処理を行う際のワーキングメモリを提供する。

通信部５５は、携帯端末６と通信したり、ネットワーク４を介して各種サーバと通信する。

記憶部５６は、例えば、ハードディスクなどの大容量の記憶装置を用いて構成されており、プログラム格納部５７には、ＣＰＵ５１に上記の機能を発揮させるプログラムなどが記憶されており、データ格納部５８には、電子署名を行うための秘密鍵や、当該秘密鍵に対応する公開鍵の公開鍵証明書などが記憶されている。

【００５３】

図示しないが、タイムスタンプサーバ２は、基地局サーバ５などと同様にＣＰＵ、ＲＯＭ、ＲＡＭ、記憶部、通信部、入出力部などを備える他、原子時計を有しており、正確な日時刻を計測している。

タイムスタンプサーバ２は、タイムスタンプ用の秘密鍵を記憶しており、例えば、電子データに原子時計で計測した日時刻を付加してこれを秘密鍵で暗号化して電子署名を行うことによりタイムスタンプを発行する。

この電子署名は、当該秘密鍵に対応する公開鍵で復号化することにより、電子データの内容とタイムスタンプサーバ２が付与した日時刻の正当性を確認できるため、タイムスタンプとして機能する。

この他、リポジトリサーバ１０、リポジトリサーバ１１は、基地局サーバ５などと同様にＣＰＵ、ＲＯＭ、ＲＡＭ、記憶部、通信部、入出力部などを備えている。

【００５４】

図６は、携帯端末６、基地局サーバ５、及び長期署名サーバ３が長期署名データを作成する手順を説明するためのフローチャートである。

なお、以下の処理は、携帯端末６のＣＰＵ２１、基地局サーバ５のＣＰＵ５１、及び長期署名サーバ３のＣＰＵ４１が所定のプログラムに従って行うものである。

まず、携帯端末６と基地局サーバ５は、協働して画像ＧＰＳ情報処理を行う（ステップ５０）。

次に、基地局サーバ５と長期署名サーバ３は、協働してＥＳ作成処理を行う（ステップ１００）。

【００５５】

次に、長期署名サーバ３が、ＥＳ－Ｔ作成処理（ステップ２００）と、ＥＳ－ＸＬ作成処理を行う（ステップ３００）。

そして、携帯端末６と長期署名サーバ３が協働してＥＳ－Ａ（１ｓｔ）作成処理を行う（ステップ４００）。

このようにして長期署名データ（ＥＳ－Ａ）が作成される。

そして、図示しないが、作成されたＥＳ－Ａ（１ｓｔ）は、有効なうちに、ＡＴＳ（２ｎｄ）を付与してＥＳ－Ａ（２ｎｄ）に更新され、以下、長期署名データの有効性が失われないように世代を重ねていく。

【００５６】

長期署名データの作成手順は、大きく分けて、以上のようなフェーズから構成されているが、以下に、これら各フェーズの詳細な手順を説明する。

図７は、ステップ５０の画像ＧＰＳ情報処理を説明するためのフローチャートである。

ユーザが携帯端末６の撮影用のシャッターボタンを操作すると、携帯端末６は、ＧＰＳ２９により現在日時刻と現在位置を検出すると共に（ステップ５５）、カメラ３０によって被写体を撮影して当該被写体の画像データを生成する。

次に、携帯端末６は、カメラ３０が被写体を撮影した際にＧＰＳ２９で取得した現在日時刻と現在位置をそれぞれ撮影日時刻、及び撮影位置とする。

そして、携帯端末６は、画像データ、撮影日時刻、及び撮影位置を含む（例えば、所定のフォーマットに従って連結する）第１の画像ＧＰＳ情報を生成する（ステップ６０）。

【００５７】

次に、携帯端末６は、第１の画像ＧＰＳ情報の画像データからハッシュ関数を用いて画像ハッシュ値を計算する（ステップ６５）。

次に、携帯端末６は、画像ハッシュ値、撮影日時刻、及び撮影位置を含む（例えば、所定のフォーマットに従って連結する）第２の画像ＧＰＳ情報を生成して基地局サーバ５に送信する（ステップ７０）。

なお、これら画像ハッシュ値、撮影日時刻、撮影位置は、個別に基地局サーバ５に送信し、基地局サーバ５で第２の画像ＧＰＳ情報を生成するように構成することもできる。

【００５８】

基地局サーバ５は、携帯端末６から第２の画像ＧＰＳ情報を受信し（ステップ７５）、第２の画像ＧＰＳ情報に含まれる撮影日時刻と撮影位置を取得する。

次に、基地局サーバ５は、以下のようにしてＧＰＳ情報が正しいか否かを判断する。

まず、基地局サーバ５は、自身の有する時計などにより現在日時刻を取得し、当該現在日時刻と撮影日時刻が所定の範囲（例えば、撮影日時刻が現在日時刻以前の５分以内）内で一致するか否かを確認する（ステップ８０）。

これは、携帯端末６の時計の精度、携帯端末６が第２の画像ＧＰＳ情報を生成して基地局サーバ５に送信する時間などを考慮し、一致の判断においてある程度の範囲をもたせたものである。

【００５９】

更に、基地局サーバ５は、撮影位置が現在の携帯端末６の存在エリア内に存在するか否かを確認する。

なお、複数の基地局サーバ５で携帯端末６の電波を受信し、携帯端末６の存在エリアを更に絞り込むことができる場合は、絞り込まれた存在エリアに携帯端末６が存在するか否かを確認するように構成することもできる。

そして、基地局サーバ５は、現在日時刻と撮影日時刻が所定範囲で一致し、かつ、撮影位置が存在エリア内にある場合、第２の画像ＧＰＳ情報が正しいと判断し、少なくとも一方の条件が満たされない場合は、第２の画像ＧＰＳ情報が正しくないと判断する。

【００６０】

第２の画像ＧＰＳ情報が正しい場合（ステップ８０；Ｙ）、基地局サーバ５は、ステップ１００のＥＳ作成処理に移行し、第２の画像ＧＰＳ情報が正しくない場合（ステップ８０；Ｎ）、基地局サーバ５は、携帯端末６にエラー通知を送信して処理を終了する（ステップ８５）。

携帯端末６は、基地局サーバ５からエラー通知を受信すると、これをディスプレイ２４に表示して、ユーザにエラー通知を提示する。

【００６１】

なお、変形例として、第２の画像ＧＰＳ情報（画像ハッシュ値、撮影日時刻、撮影日時刻ハッシュ値、撮影位置、撮影位置ハッシュ値）とすることも可能である。

即ち、第２の画像ＧＰＳ情報に、基地局サーバ５で確認する撮影日時刻及び撮影位置と、長期署名サーバ３で長期署名データの作成に必要な撮影日時刻ハッシュ値と撮影位置ハッシュ値を含めておくのである。このように構成すると、基地局サーバ５が撮影日時刻ハッシュ値と撮影位置ハッシュ値を計算する必要がなくなる。

【００６２】

図８は、ステップ１００のＥＳ作成処理を説明するためのフローチャートである。

まず、基地局サーバ５は、後に電子署名を行う秘密鍵の公開鍵証明書を長期署名サーバ３に送信する（ステップ１１０）。

次に、長期署名サーバ３は、基地局サーバ５から公開鍵証明書を受信し（ステップ１１５）、署名前ＸＡｄＥＳデータのフォーマットをＸＭＬによって作成する（ステップ１２０）。

【００６３】

次に、基地局サーバ５は、携帯端末６から受信した第２の画像ＧＰＳ情報の撮影日時刻と撮影位置からハッシュ関数によって撮影日時刻ハッシュ値と撮影位置ハッシュ値を計算し、画像ハッシュ値、撮影日時刻ハッシュ値、及び撮影位置ハッシュ値を含む（例えば、所定のフォーマットに従って連結する）第３の画像ＧＰＳ情報を生成する。

そして、基地局サーバ５は、第３の画像ＧＰＳ情報を長期署名サーバ３に送信し（ステップ１２５）、長期署名サーバ３は、当該第３の画像ＧＰＳ情報を受信する（ステップ１３０）。

なお、基地局サーバ５は、長期署名サーバ３に第２の画像ＧＰＳ情報を送信し、長期署名サーバ３は、第２の画像ＧＰＳ情報から第３の画像ＧＰＳ情報を生成するように構成することもできる。

【００６４】

長期署名サーバ３は、基地局サーバ５から第３の画像ＧＰＳ情報を受信すると（ステップ１３０）、署名前ＸＡｄＥＳデータにＫｅｙＩｎｆｏのエリアを作成し、これに基地局サーバ５から受信した公開鍵証明書を設定する（ステップ１３５）。

次に、長期署名サーバ３は、公開鍵証明書のハッシュ値を計算すると共に（以下、公開鍵証明書ハッシュ値）、署名前ＸＡｄＥＳデータに署名対象プロパティのエリアを作成し、ここに公開鍵証明書ハッシュ値を設定する（ステップ１４０）。

【００６５】

次に、長期署名サーバ３は、署名対象プロパティハッシュ値を計算し（ステップ１４５）、署名前ＸＡｄＥＳデータにＳｉｇｎｅｄＩｎｆｏのエリアを作成して、ここに基地局サーバ５から受信した第３の画像ＧＰＳ情報と署名対象プロパティハッシュ値を設定する。

長期署名サーバ３は、このようにしてＳｉｇｎｅｄＩｎｆｏを作成すると、署名前ＸＡｄＥＳデータからＳｉｇｎｅｄＩｎｆｏエリアを抽出して基地局サーバ５に送信する（ステップ１５０）。

【００６６】

基地局サーバ５は、長期署名サーバ３からＳｉｇｎｅｄＩｎｆｏを受信すると、これに秘密鍵で電子署名して電子署名値を生成し、当該生成した電子署名値を長期署名サーバ３に送信する（ステップ１５５）。

長期署名サーバ３は、基地局サーバ５から電子署名値を受信すると、ＳｉｇｎａｔｕｒｅＶａｌｕｅエリアを作成して、これに電子署名値を設定し、ＥＳを作成する（ステップ１６０）。

【００６７】

図９は、ステップ２００のＥＳ－Ｔ作成処理を説明するためのフローチャートである。

まず、長期署名サーバ３は、ステップ１００で作成したＥＳを処理対象として入力する（ステップ２０５）。この際に、ＥＳを検証するように構成することもできる。

次に、長期署名サーバ３は、ＥＳからＳｉｇｎａｔｕｒｅＶａｌｕｅエリアを抽出し（ステップ２１０）、ＳｉｇｎａｔｕｒｅＶａｌｕｅのハッシュ値を計算する（ステップ２１５）。

【００６８】

次いで、長期署名サーバ３は、ＳｉｇｎａｔｕｒｅＶａｌｕｅのハッシュ値に対するタイムスタンプを要求するためのＴＳＱ（Ｔｉｍｅ－ｓｔａｍｐ　Ｒｅｑｕｅｓｔ）を生成し、タイムスタンプサーバ２に送信する（ステップ２２０）。

タイムスタンプサーバ２は、ＴＳＱを受信すると、現在日時刻の付与後、秘密鍵で署名してＴＳＴ（Ｔｉｍｅ　Ｓｔａｍｐ　Ｔｏｋｅｎ）を生成する。

そして、タイムスタンプサーバ２は、発行したＴＳＴを用いてＴＳＲ（Ｔｉｍｅ－ｓｔａｍｐ　Ｒｅｓｐｏｎｓｅ）を生成し、長期署名サーバ３に送信する（ステップ２２５）。

より詳細に説明すると、ＴＳＲの中にはＴＳＴが存在し、ＴＳＲから取り出したＴＳＴが、ＳＴＳ（署名タイムスタンプ）やＡＴＳ（アーカイブタイムスタンプ）などと呼ばれる。

【００６９】

長期署名サーバ３は、タイムスタンプサーバ２からＴＳＲを受信し、ＴＳＲからＴＳＴを抽出する（ステップ２３０）。

そして、長期署名サーバ３は、ＥＳ－Ｔに署名タイムスタンプエリアを作成してＴＳＴをＳＴＳ（署名タイムスタンプ）として設定し、ＥＳ－Ｔの作成をする（ステップ２３５）。

【００７０】

図１０は、ステップ３００のＥＳ－ＸＬ作成処理を説明するためのフローチャートである。

まず、長期署名サーバ３は、ステップ２００で作成したＥＳ－Ｔを処理対象として入力する（ステップ３０５）。

【００７１】

次に、長期署名サーバ３は、ＥＳ－Ｔから必要な証明書情報を割り出して、次のように収集する。

まず、長期署名サーバ３は、基地局サーバ５の公開鍵証明書を検証するための認証局による署名証明書を取得し（ステップ３１０）、更に、当該署名証明書のルート証明書を取得する（ステップ３１５）。

次いで、長期署名サーバ３は、署名タイムスタンプを証明するためのＴＳＡ証明書を取得し（ステップ３２０）、次いで、当該ＴＳＡ証明書のルート証明書を取得する（ステップ３２５）。これら取得対象の証明書群は長期署名サーバ３に記憶されている。

【００７２】

次に、長期署名サーバ３は、証明書群の各証明書から、基地局サーバ５の公開鍵証明書やＳＴＳの公開鍵証明書、これらを検証するための認証局の証明書などが失効リストにリストアップされていないことを確認するために必要な失効情報を割り出し、これらを次のように収集する。

【００７３】

なお、署名証明書は、例えば、正当な署名鍵所有者が鍵を紛失したなどの理由で、認証局に対して失効申請が行われているのにもかかわらず、失効手続きの事務処理や失効情報公開タイミングの関係で、失効情報にその失効状態が登録されていない可能性がある。

このような場合、失効してから失効情報に登録されるまで時間を要するので、長期署名サーバ３は、証明書群を作成した後、一定期間経過後（署名証明書を発行した認証局の運用ポリシーに基づく、例えば、２４時間、あるいは数日）に失効情報を収集する。

【００７４】

まず、長期署名サーバ３は、ＣＡのリポジトリサーバ１０にアクセスし、収集した署名証明書のＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を要求する（ステップ３３０）。

これに対し、リポジトリサーバ１０は、長期署名サーバ３に署名証明書のＣＲＬを送信する（ステップ３３５）。

ここで、ＣＲＬは、失効した証明書を一覧したリストであって、証明書とＣＲＬを照合することにより証明書が有効であるか否かを判断するためのものである。

【００７５】

次に、長期署名サーバ３は、リポジトリサーバ１０に署名証明書のルート証明書のＡＲＬ（Ａｕｔｈｏｒｉｔｙ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を要求する（ステップ３４０）。

これに対し、リポジトリサーバ１０は、長期署名サーバ３に署名証明書のルート証明書のＡＲＬを送信する（ステップ３４５）。

ここで、ＡＲＬは、失効した自己署名証明書などのリストである。ルートのＣＡは、証明書信頼チェーンにおいて最上位に位置するため、ルートのＣＡは、自己を自己署名証明書にて証明する。そして、ルート証明書とＡＲＬを照合することによりルート証明書が有効であるか否かを判断することができる。

【００７６】

署名証明書のＣＲＬによって署名証明書の有効性が検証でき、署名証明書のルート証明書のＡＲＬによって署名証明書のルート証明書の有効性が検証でき、署名証明書、及び署

名証明書のルート証明書の検証により基地局サーバ５による署名の正当性を検証することができる。

【００７７】

次に、長期署名サーバ３は、ＴＳＡ－ＣＡのリポジトリサーバ１１にアクセスし、ＴＳＡ証明書のＣＲＬを要求する（ステップ３５０）。

これに対し、リポジトリサーバ１１は、長期署名サーバ３にＴＳＡ証明書のＣＲＬを送信する（ステップ３５５）。

次に、長期署名サーバ３は、リポジトリサーバ１１にＴＳＡ証明書のルート証明書のＡＲＬを要求する（ステップ３６０）。

これに対し、リポジトリサーバ１１は、長期署名サーバ３にＴＳＡ証明書のルート証明書のＡＲＬを送信する（ステップ３６５）。

【００７８】

ＴＳＡ証明書のＣＲＬによってＴＳＡ証明書の有効性が検証でき、ＴＳＡ証明書のルート証明書のＡＲＬによってＴＳＡ証明書のルート証明書の有効性が検証でき、ＴＳＡ証明書、及びＴＳＡ証明書のルート証明書の検証によりＳＴＳの正当性を検証することができる。

【００７９】

長期署名サーバ３は、以上のようにして、証明書群と失効情報群を収集すると、これらを用いて証明書信頼チェーンの階層による認証パスを構築し、これをＥＳ－Ｔに追加して、ＥＳ－ＸＬを作成する（ステップ３７０）。

【００８０】

図１１は、ステップ４００のＥＳ－Ａ（１ｓｔ）作成処理を説明するためのフローチャートである。

なお、以下の処理は、携帯端末６が行うが、第１の画像ＧＰＳ情報（画像データ、撮影日時刻、撮影位置を記憶していて、第１の画像ＧＰＳ情報を生成してもよい）を記憶するユーザ端末で行ってもよい。

まず、長期署名サーバ３は、ステップ３００で作成したＥＳ－ＸＬを処理対象として入力する（ステップ４０５）。この際に、長期署名サーバ３が、ＥＳ－ＸＬを検証するように構成することもできる。

次に、長期署名サーバ３は、長期署名データにＡＴＳエリアを作成する（ステップ４１０）。

【００８１】

長期署名サーバ３は、ＡＴＳエリアを作成し、ＥＳ－Ａ（１ｓｔ）を作成する準備が整うと、準備完了通知を携帯端末６に送信する（ステップ４１５）。

携帯端末６は、当該通知を受信すると、記憶しておいた第１の画像ＧＰＳ情報を読み込んで取得する（ステップ４２０）。

長期署名サーバ３は、携帯端末６に準備完了通知を送信すると、ＥＳ－Ａ（１ｓｔ）用のハッシュ値対象データ作成用データを作成する。

【００８２】

具体的には、長期署名サーバ３は、ＥＳ－ＸＬから、署名対象プロパティ、ＳｉｇｎｅｄＩｎｆｏ、ＳｉｇｎａｔｕｒｅＶａｌｕｅ、ＫｅｙＩｎｆｏ、ＳＴＳ、証明書群、失効情報群を抽出して、これらを所定のフォームに従って設定することにより結合し、ハッシュ値対象データ作成用データを生成する。

なお、このハッシュ値対象データ作成用データは、ハッシュ値対象データから第１の画像ＧＰＳ情報を除いたものである。

長期署名サーバ３は、署名値対象データ作成用データを作成すると、これを携帯端末６に送信する（ステップ４２５）。

【００８３】

携帯端末６は、長期署名サーバ３からハッシュ値対象データ作成用データを受信すると、これにステップ４２０で読み込んだ第１の画像ＧＰＳ情報を追加し（ステップ４３０）

、ハッシュ値対象データを作成する。
次に、携帯端末６は、ハッシュ値対象データのハッシュ値を計算し、長期署名サーバ３に送信する（ステップ４３５）。
長期署名サーバ３は、携帯端末６から当該ハッシュ値を受信すると、これにタイムスタンプを要求するためのＴＳＱを生成してタイムスタンプサーバ２に送信する（ステップ４４０）。
タイムスタンプサーバ２は、ＴＳＱを受信すると、ＴＳＱからハッシュ値対象データのハッシュ値を取り出し、これに現在日時刻を付与して秘密鍵で署名することによりＴＳＴを生成する。
そして、タイムスタンプサーバ２は、ＴＳＴを用いてＴＳＲを生成し、長期署名サーバ３に送信する（ステップ４４５）。
【００８４】
長期署名サーバ３は、タイムスタンプサーバ２からＴＳＲを受信すると（ステップ４５０）、これからＴＳＴを抽出する（ステップ４６０）。
そして、長期署名サーバ３は、抽出したＴＳＴをＡＴＳ（１ｓｔ）としてＥＳ－ＸＬに追加し、ＥＳ－Ａ（１ｓｔ）を生成して携帯端末６に送信する（ステップ４６５）。
【００８５】
そして、携帯端末６は、長期署名サーバ３からＥＳ－Ａ（１ｓｔ）を受信して記憶する（ステップ４７０）。
以上のようにして、画像データを携帯端末６の内部に保持したまま、当該画像データに対する長期署名データ（ＥＳ－Ａ（１ｓｔ））を作成することができる。
【００８６】
以上のようにして作成されたＥＳ－Ａ（１ｓｔ）は、クライアント側で保存されるが、ＡＴＳ（１ｓｔ）の有効性が失われる前に、ＥＳ－Ａ（１ｓｔ）にＡＴＳ（２ｎｄ）を付与してＥＳ－Ａ（２ｎｄ）に更新する必要がある。そこで、次にＥＳ－Ａ（２ｎｄ）に更新する手順について説明する。
【００８７】
図１２は、ＥＳ－Ａ（２ｎｄ）を作成する手順を説明するためのフローチャートである。
なお、以下の処理は、携帯端末６が行うが、第１の画像ＧＰＳ情報を記憶するユーザ端末で行ってもよい。
まず、携帯端末６は、ＥＳ－Ａ（１ｓｔ）を長期署名サーバ３に送信する（ステップ５０５）。携帯端末６でＥＳ－Ａ（１ｓｔ）が入力された際に、これを検証するように構成することもできる。
長期署名サーバ３は、携帯端末６からＥＳ－Ａ（１ｓｔ）を受信する（ステップ５１０）。
そして、長期署名サーバ３は、ＥＳ－Ａ（１ｓｔ）からＡＴＳ（１ｓｔ）に必要な証明書情報を割り出して、これらを以下のように収集する。
【００８８】
まず、長期署名サーバ３は、ＡＴＳ（１ｓｔ）のＴＳＡ証明書を取得し（ステップ５１５）、更に、ＴＳＡ証明書のルート証明書を取得する（ステップ５２０）。これらの証明書は、長期署名サーバ３に記憶されている。
次に、長期署名サーバ３は、ＴＳＡ－ＣＡのリポジトリサーバ１１にアクセスし、ＡＴＳ（１ｓｔ）のＴＳＡ証明書のＣＲＬを要求し（ステップ５２５）、リポジトリサーバ１１は、長期署名サーバ３にＣＲＬを送信する（ステップ５３０）。
そして、長期署名サーバ３は、ＣＲＬを受信する。
【００８９】
次に、長期署名サーバ３は、リポジトリサーバ１１にＡＴＳ（１ｓｔ）のＴＳＡ証明書のルート証明書のＡＲＬを要求し（ステップ５３５）、リポジトリサーバ１１は、長期署名サーバ３に当該ルート証明書のＡＲＬを送信する（ステップ５４０）。

そして、長期署名サーバ３は、ＡＲＬを受信する。

【００９０】

次に、長期署名サーバ３は、これら証明書群（ＴＳＡ証明書、ＴＳＡ証明書のルート証明書）と失効情報群（ＣＲＬ、ＡＲＬ）から認証パスを構築する（ステップ５４５）。

次に、長期署名サーバ３は、収集した証明書群と失効情報群を、それぞれＡＴＳ（１ｓｔ）のｃｅｒｔｉｆｉｃａｔｅｓエリア及びｃｒｌｓエリアに追加してＡＴＳ（１ｓｔ）を更新する（ステップ５５０）。

次に、長期署名サーバ３は、ＡＴＳ（１ｓｔ）を更新したＥＳ－Ａ（１ｓｔ）にＡＴＳ（２ｎｄ）用のエリアを作成し、ＥＳ－Ａ（２ｎｄ）を作成する準備が整った旨の準備完了通知を携帯端末６に送信する（ステップ５５５）。

【００９１】

それ以降の処理は、図１１のステップ４２０以下と同じであり、画像データを携帯端末６の内部に保持したまま長期署名サーバ３でＥＳ－Ａ（２ｎｄ）を作成することができる。

即ち、長期署名サーバ３は、ハッシュ値対象データ作成用データを作成して携帯端末６に送信する。

【００９２】

そして、携帯端末６は、ハッシュ値対象データ作成用データに第１の画像ＧＰＳ情報を加えてハッシュ値を計算し、当該ハッシュ値に電子署名して署名値を長期署名サーバ３に送信する。

長期署名サーバ３は、当該署名値をタイムスタンプサーバ２に送信してタイムスタンプを発行してもらい、これをＥＳ－Ａ（１ｓｔ）に追加してＥＳ－Ａ（２ｎｄ）を作成する。

ＥＳ－Ａ（３ｒｄ）、ＥＳ－Ａ（４ｔｈ）など後の世代も同様にして作成される。

【００９３】

以上に説明した実施の形態により、次のような効果を得ることができる。

（１）携帯端末６で被写体を撮影した際に、ＧＰＳ２９により撮影日時刻と撮影場所も記録することができる。

（２）被写体を撮影した画像データのハッシュ値と、当該撮影を行った撮影日時刻、及び撮影場所を同時に基地局サーバ５に送信することができる。

（３）被写体を撮影した画像データのハッシュ値と、当該撮影を行った撮影日時刻、及び撮影場所に対して長期署名を行うことができる。

（４）画像データを基地局サーバ５や長期署名サーバ３に送らずに長期署名データを作成することができるため、プライバシーを守りつつ、被写体の存在証明を行うことができる。

（５）画像データを基地局サーバ５や長期署名サーバ３に送らずに済むため、通信費用を抑えることができる。

（６）携帯端末６からユーザ端末に画像データや第１の画像ＧＰＳ情報を移動して、その後の処理をユーザ端末で行うことができる。

（７）第１の画像ＧＰＳ情報を用いる処理だけ携帯端末６（又はユーザ端末）で行い、ＸＭＬの解析、電子署名、タイムスタンプ、検証情報の取得など、コンピュータの負荷が高い処理は長期署名サーバ３で行うため、携帯端末６（ユーザ端末）の負荷を小さくすることができる。

（８）画像データをユーザ側に保持したまま、長期署名データの作成をアウトソースすることができ、ユーザ環境に長期署名システムを構築する必要がないため、ユーザが運用管理（ログ監視、失敗監視、リカバリ処理等）を行う必要がない。

（９）ユーザ環境に長期署名システムを構築しないため、ユーザ環境からタイムスタンプ及び失効情報を取得するためのネットワーク設定（ＩＰ、ポートを開く等）が必要ない。

（１０）認証パスの取得のための署名証明書のルート証明書及びＴＳＡ証明書のルート証明書などは、長期署名サーバ３が有しているため、これらの情報をユーザ環境で保持する

必要がない。そのため、例えば、ＴＳＡが認証局を変更する場合であっても、ユーザ環境で新しい認証局証明書（ルート証明書や中間証明書）を登録しなおす必要がない。
（１１）タイムスタンプは、長期署名サーバ３が取得するため、携帯端末６やユーザ端末などのユーザ側は、ＴＳＡと契約する必要がない。
（１２）長期署名フォーマットのバージョンアップや暗号アルゴリズムの危殆化発生時には、長期署名サーバ３が対応し、ユーザ側が対応する必要がない。なお、ハッシュ関数が危殆化した場合は、ユーザ側装置のハッシュ関数を変更する必要がある。この場合、予め想定される最新の複数のハッシュ関数をユーザ側に埋め込んでおき、スイッチで切り替えられるとか、毎回、複数のハッシュ関数で計算したハッシュ値群をサーバに送るように構成してもよい（大したサイズではない）。
（１３）長期署名データの生成を長期署名サーバ３にアウトソースすることにより、例えば、保険会社などで第１の画像ＧＰＳ情報を長期署名する長期署名システムを構築したいが処理する第１の画像ＧＰＳ情報数が見積もれないため初期コストをかけられない、長期署名システムを運用するための要員を確保できないため自社内にサーバシステムを持てない、画像データは社内から持ち出したくない、といった顧客の要望を満たすソリューションを提供することができる。
（１４）長期署名フォーマットを利用することにより、電子署名の有効性を延長したり、暗号アルゴリズムの危殆化に対応することが可能となる。
（１５）第２、第３の画像ＧＰＳ情報を用いることにより第１の画像ＧＰＳ情報に対して、署名鍵で署名を行い、署名タイムスタンプを付与してＥＳ－Ｔを作成し、ＥＳ－Ｔに対して必要な検証情報(認証パス及び失効情報)を収集・付与し、アーカイブタイムスタンプを付与してＥＳ－Ａを作成する処理を機密を確保してクラウドで行うシステムを提供することができる。
（１６）画像データを長期署名サーバ３に送信してもよい場合は、画像データを長期署名サーバ３に送信することも可能であるが、データサイズが大きいことや、即時性が求められることもあり、データサイズの小さいハッシュ値を先に送り、署名及び署名タイムスタンプを証明センタ（長期署名サーバ３）に依頼することができる。
（１７）携帯端末６とユーザ端末の接続を長期署名サーバ３とし、タイムスタンプサーバ２、リポジトリサーバ１０、リポジトリサーバ１１と接続しないため、携帯端末６とユーザ端末の接続先を可能な限り少なくすることができ、接続先が多いことによるセキュリティホールの増大を防ぐことができる。
（１８）次のような、ＡＳＰにて証拠担保するシステムを構築することができる。
携帯端末６のユーザがカメラ機能を利用して画像を作成して画像のハッシュ値と同時に取得されているＧＰＳ情報を基地局サーバ５（基地局）に送付する。基地局サーバ５は、ＧＰＳ情報が正しいと判断した場合に、ＧＰＳ情報と画像のハッシュ値を長期署名サーバ３（証明センタ）に送る。長期署名サーバ３は、受け取ったデータをもとに署名対象データを作成し、基地局サーバ５へ送る。基地局サーバ５は、「位置の確認者」としての署名を行い、署名値を長期署名サーバ３へ送付する（時刻の証明は署名タイムスタンプが役割を果たす）。長期署名サーバ３は、署名値をもとに署名タイムスタンプを作成し、引き続き、アーカイブタイムスタンプ処理へ進む。一定期間経過後、証明センターは、要求のあった携帯端末６に対して通信を行い、残りの処理を行ってＥＳ－Ａを完成させる。

【００９４】

以上説明した本実施の形態により、次の構成を得ることができる。
長期署名システム１において、携帯端末６は、携帯端末として機能しており、基地局サーバ５は、電子署名用サーバとして機能しており、長期署名サーバ３は、長期署名用サーバとして機能している。
また、画像データ、及び画像ハッシュ値は、携帯端末６で撮影した被写体の画像データを特定する画像特定情報として機能しており、撮影日時刻、撮影日時刻ハッシュ値、撮影位置、撮影位置ハッシュ値は、それぞれ撮影日時刻特定情報と撮影位置特定情報として機能している。

そのため、画像ＧＰＳ情報（第１の画像ＧＰＳ情報、第２の画像ＧＰＳ情報、第３の画像ＧＰＳ情報）は、画像データ、撮影日時刻、撮影位置を特定する画像時刻位置情報として機能している。

【００９５】

基地局サーバ５は、携帯端末６と無線通信を介して通信するため、携帯端末と通信する通信手段を備えている。

そして、基地局サーバ５は、携帯端末６から第２の画像ＧＰＳ情報を受信するため、前記通信している携帯端末から、当該携帯端末で撮影した被写体の画像データを特定する画像特定情報（画像ハッシュ値）と、前記撮影の際の撮影位置を特定する撮影日時刻特定情報と、前記撮影の撮影日時刻を特定する撮影位置特定情報と、を含む画像時刻位置情報を受信する画像時刻位置情報受信手段を備えている。

また、基地局サーバ５は、携帯端末６の発する電波を受信することにより携帯端末６が当該基地局サーバ５の通信エリアに存在することを検出することができるため、前記携帯端末の現在位置を検出する現在位置検出手段を備えている。

更に、基地局サーバ５は、自己の有する時計などによって現在日時刻を取得することができるため、現在日時刻を取得する現在日時刻取得手段を備えている。

そして、基地局サーバ５は、第２の画像ＧＰＳ情報に含まれる撮影位置が携帯端末６の現在位置と所定の範囲（存在エリア）で一致し、また、撮影日時刻が現在日時刻と所定範囲で一致するか判断し、両者が一致する場合に、第２の画像ＧＰＳ情報に対して署名前ＸＡｄＥＳデータ（第２の画像ＧＰＳ情報は、署名前ＸＡｄＥＳデータには第３の画像ＧＰＳ情報として含まれている）に電子署名することにより電子署名するため、前記受信した画像時刻位置情報の撮影位置が前記検出した現在位置と所定の範囲で一致し、かつ、前記受信した画像時刻位置情報の撮影日時刻が前記取得した現在日時刻と所定の範囲で一致するか否かを判断する判断手段と、前記判断手段が一致すると判断した場合に、前記受信した画像時刻位置情報に対して電子署名を行う署名手段を備えている。

【００９６】

また、基地局サーバ５は、第２の画像ＧＰＳ情報の撮影日時刻と撮影位置が所定の範囲で現在日時刻と携帯端末６の現在位置と一致した場合に、第３の画像ＧＰＳ情報を長期署名サーバ３に送信し（第２の画像ＧＰＳ情報を長期署名サーバ３に送信して長期署名サーバ３で第３の画像ＧＰＳ情報を生成してもよい）、これに対して長期署名サーバ３から送信されてきた署名前ＸＡｄＥＳデータ（第２の画像ＧＰＳ情報を第３の画像ＧＰＳ情報として含む）に電子署名するため、前記判断手段で一致すると判断した場合に、長期署名データを作成する所定のサーバ（長期署名サーバ３）に前記画像時刻位置情報（第３の画像ＧＰＳ情報）を送信する画像時刻位置情報送信手段と、前記送信した画像時刻位置情報を用いて作成した長期署名データ用の署名対象データ（署名前ＸＡｄＥＳデータ）を受信する署名対象データ受信手段と、を具備し、前記署名手段は、前記受信した署名対象データに電子署名することにより前記画像時刻位置情報に対して電子署名を行っている。

【００９７】

また、基地局サーバ５は、長期署名サーバ３が署名前ＸＡｄＥＳデータを作成するように、第３の画像ＧＰＳ情報を送信する前に電子署名に用いる秘密鍵に対応する公開鍵の公開鍵証明書を長期署名サーバ３に送信し、これに対して送信されてきた署名前ＸＡｄＥＳデータに電子署名して電子署名値を基地局サーバ５に送信するため、前記署名手段で電子署名をする前に、当該電子署名に用いる秘密鍵に対応する公開鍵の公開鍵証明書を前記所定のサーバに送信する公開鍵証明書送信手段と、前記署名手段で電子署名した電子署名値を前記所定のサーバに送信する電子署名値送信手段を備えている。

【００９８】

また、前記画像特定情報は、前記画像データを所定の関数（ハッシュ関数）で計算した関数値（ハッシュ値）とすることができる。

【００９９】

また、基地局サーバ５は、第２の画像ＧＰＳ情報の撮影位置が携帯端末６が存在エリア

内にある場合に、撮影位置と携帯端末６の現在位置が一致すると判断するため、前記現在位置検出手段は、前記携帯端末が存在する領域（存在エリア）を検出し、前記判断手段は、前記受信した画像時刻位置情報の撮影位置が前記検出した領域の内部にある場合に、前記撮影位置と前記現在位置が所定の範囲で一致すると判断している。

【０１００】

長期署名サーバ３は、基地局サーバ５から第３の画像ＧＰＳ情報を受信するため、携帯端末（携帯端末６）と通信する電子署名用サーバ（基地局サーバ５）から、当該携帯端末で撮影した被写体の画像データを所定の関数（ハッシュ）で計算した関数値（ハッシュ値）と、前記撮影の際の撮影位置を特定する撮影位置特定情報と、前記撮影の撮影日時刻を特定する撮影日時刻特定情報と、を含む画像時刻位置情報（第３の画像ＧＰＳ情報、ただし撮影日時刻と撮影位置はハッシュ値となっている）を受信する画像時刻位置情報受信手段を備えている。

そして、長期署名サーバ３は、受信した第３の画像ＧＰＳ情報を用いて署名前ＸＡｄＥＳデータを生成して基地局サーバ５に送信し、基地局サーバ５が署名前ＸＡｄＥＳデータに対して行った電子署名の電子署名値を受信するため、前記受信した画像時刻位置情報を用いて長期署名データ用の署名対象データ（署名前ＸＡｄＥＳデータ）を生成する署名対象データ生成手段と、前記生成した署名対象データを前記電子署名用サーバに送信する署名対象データ送信手段と、前記送信した署名対象データの電子署名値を前記電子署名用サーバから受信する電子署名値受信手段を備えている。

更に、長期署名サーバ３は、当該電子署名値を用いて画像ＧＰＳ情報（第１、第２、第３の画像ＧＰＳ情報の何れでもよい）に対する長期署名データを生成するため、前記受信した電子署名値を用いて前記画像時刻位置情報の長期署名データを生成する長期署名データ生成手段を備えている。

【０１０１】

また、長期署名サーバ３は、基地局サーバ５から電子署名に用いる秘密鍵に対応する公開鍵の公開鍵証明書を受信し、当該公開鍵証明書を含めて署名前ＸＡｄＥＳデータを生成するため、前記電子署名用サーバから、前記電子署名に用いる秘密鍵に対応する公開鍵の公開鍵証明書を受信する公開鍵証明書受信手段を備え、前記署名対象データ生成手段は、前記受信した公開鍵証明書を前記署名対象データに含めている。

【０１０２】

長期署名サーバ３は、タイムスタンプサーバ２によってＳｉｇｎａｔｕｒｅＶａｌｕｅ（電子署名値が格納されている）のハッシュ値にタイムスタンプを発行してもらうため、前記受信した電子署名値に対するタイムスタンプを取得するタイムスタンプ取得手段を備えている。

また、長期署名サーバ３は、公開鍵証明書（公開鍵証明書の検証によって電子署名値が検証される）やタイムスタンプを検証するための検証情報を生成するため、前記電子署名値と前記タイムスタンプを検証する検証情報を生成する検証情報生成手段を備えている。

そして、長期署名サーバ３は、署名前ＸＡｄＥＳデータ、ＳｉｇｎａｔｕｒｅＶａｌｕｅ、署名タイムスタンプ、検証情報を用いてＥＳ－ＸＬを作成するため、前記署名対象データ（署名前ＸＡｄＥＳデータ）、前記電子署名値（ＳｉｇｎａｔｕｒｅＶａｌｕｅ）、前記タイムスタンプ（署名タイムスタンプ）、及び前記検証情報を含む基本署名データ（ＥＳ－ＸＬ）を生成する基本署名データ生成手段を備えており、また、ＥＳ－ＸＬを所定期間検証するためのＡＴＳ（１ｓｔ）を取得するため、前記生成した基本署名データを所定期間検証するための長期検証情報（ＡＴＳ（１ｓｔ））を取得する長期検証情報取得手段を備えている。

そして、前記長期署名データ生成手段は、前記取得した長期検証情報（ＡＴＳ（１ｓｔ））を前記生成した基本署名データ（ＥＳ－ＸＬ）に加えて長期署名データ（ＥＳ－Ａ（１ｓｔ））を生成している。

【０１０３】

また、長期署名サーバ３は、ＡＴＳ（１ｓｔ）を作成するためのハッシュ値対象データ

作成用データを、携帯端末６やユーザ端末に送信し、ハッシュ値対象データ作成用データに第１の画像ＧＰＳ情報を加えて計算したハッシュ値を受信するため、長期検証情報（ＡＴＳ（１ｓｔ））を作成するための長期検証情報作成用情報（ハッシュ値対象データ作成用データ）を前記画像データ、前記撮影位置、及び前記撮影日時刻を有する所定の端末（携帯端末６やユーザ端末）に送信する長期検証情報作成用情報送信手段と、前記送信した長期検証情報作成用情報に前記画像データ、前記撮影位置、及び前記撮影日時刻を加えて所定関数（ハッシュ関数）で計算した長期検証関数値（ハッシュ値）を前記所定の端末から受信する長期検証関数値受信手段を備えている。

そして、長期署名サーバ３は、タイムスタンプサーバ２によって当該ハッシュ値にタイムスタンプを付与してＡＴＳ（１ｓｔ）を取得するため、前記長期検証情報取得手段は、前記受信した長期検証関数値にタイムスタンプを付与して前記長期検証情報を取得している。

【０１０４】

また、長期署名サーバ３は、携帯端末６やユーザ端末などから長期署名データを受信して最も新しい世代のＡＴＳを抽出し、当該ＡＴＳを所定期間検証するための次世代のＡＴＳを取得するため、所定の端末（携帯端末６やユーザ端末など）から長期署名データを受信する長期署名データ受信手段と、前記受信した長期署名データから長期検証情報（最も新しいＡＴＳ）を抽出する長期検証情報抽出手段と、前記抽出した長期検証情報を所定期間検証するための再度の長期検証情報（次世代のＡＴＳ）を取得する再度の長期検証情報取得手段を備えている。

そして、長期署名サーバ３は、次世代のＡＴＳをＥＳ－Ａに加えてＥＳ－Ａを更新するため、前記長期署名データ生成手段は、前記受信した長期署名データに前記取得した再度の長期検証情報を加えて当該長期署名データを更新している。

【０１０５】

そして、長期署名サーバ３は、次世代のＡＴＳを生成するに際して、次世代のハッシュ値対象データ作成用データを生成して携帯端末６やユーザ端末などに送信し、携帯端末６やユーザ端末から、次世代のハッシュ値対象データ作成用データに第１の画像ＧＰＳ情報を加えて計算したハッシュ値を受信するため、再度の長期検証情報を作成するための再度の長期検証情報作成用情報（次世代のハッシュ値対象データ作成用データ）を前記所定の端末（携帯端末６やユーザ端末）に送信する再度の長期検証情報作成用情報送信手段と、前記送信した再度の長期検証情報作成用情報に前記画像データ、前記撮影位置、及び前記撮影日時刻を加えて所定関数（ハッシュ関数）で計算した再度の長期検証関数値（ハッシュ値）を前記所定の端末から受信する再度の長期検証関数値受信手段を備えている。

そして、長期署名サーバ３は、タイムスタンプサーバ２でこれにタイムスタンプを発行してもらって次世代のＡＴＳとすることから、前記再度の長期検証情報取得手段は、前記受信した再度の長期検証関数値にタイムスタンプを付与して前記再度の長期検証情報を取得している。

【０１０６】

次に、図１３のフローチャートを用いて長期署名データの検証方法について説明する。

以下の検証者端末は、長期署名データ、第１の画像ＧＰＳ情報取得して、長期署名データを用いて第１の画像ＧＰＳ情報を検証するユーザ端末である。

例えば、甲が作成した長期署名データ、第１の画像ＧＰＳ情報を乙が受け取り、乙が検証者端末でこれを検証する場合が想定される。

【０１０７】

検証者端末は、長期署名データ、第１の画像ＧＰＳ情報を記憶している。長期署名データによって第１の画像ＧＰＳ情報が検証されれば、第１の画像ＧＰＳ情報の撮影日時刻と撮影場所、及び画像データが検証される。

あるいは、検証者端末は、画像データ、撮影日時刻、撮影場所を取得して、これらから第１の画像ＧＰＳ情報を生成してもよい。

【０１０８】

まず、検証者端末は、長期署名データを長期署名サーバ３に送信し（ステップ６０５）、長期署名サーバ３は、これを受信する（ステップ６１０）。
次に、検証者端末は、第１の画像ＧＰＳ情報から第３の画像ＧＰＳ情報を生成して、これを長期署名サーバ３に送信し（ステップ６１５）、長期署名サーバ３は、これを受信する（ステップ６２０）。

【０１０９】

次に、長期署名サーバ３は、第３の画像ＧＰＳ情報を検証する（ステップ６２５）。
この処理は、検証者端末から送信された第３の画像ＧＰＳ情報と、長期署名データのＸＡｄＥＳ内の第３の画像ＧＰＳ情報を比較し、両者が一致することを確認することにより行われる。
次に、長期署名サーバ３は、公開鍵証明書（署名証明書）の検証を行う（ステップ６３０）。
この検証は、検証情報に含まれる証明書群、及び失効情報群を用いて、認証パスがつながること、及び認証パス上の証明書が失効していなかったことを確認することにより行われる。

【０１１０】

次に、長期署名サーバ３は、署名値を検証する（ステップ６３５）。
この検証は、ＳｉｇｎａｔｕｒｅＶａｌｕｅの署名値を公開鍵証明書から取り出した公開鍵で復号化すると共に、ＳｉｇｎｅｄＩｎｆｏのハッシュ値を計算し、当該復号化した値とハッシュ値が一致することを確認することにより行われる。
次に、長期署名サーバ３は、ＳＴＳを検証する（ステップ６４０）。
この検証は、ＳｉｇｎａｔｕｒｅＶａｌｕｅのハッシュ値を計算し、これと、ＳＴＳに記載されているハッシュ値が一致することを確認することにより行われる。

【０１１１】

次に、長期署名サーバ３は、ＳＴＳ証明書（署名タイムスタンプ証明書）を検証する（ステップ６４５）。
この検証は、ＴＳＡ証明書でＴＳＡ署名値を復号して確認する他、検証情報に含まれる証明書群、及び失効情報群を用いて、ＳＴＳ証明書の認証パスがつながること、及び認証パス上の証明書が失効していなかったことを確認することにより行われる。

【０１１２】

次に、長期署名サーバ３は、ＥＳ－ＸＬに含まれるデータからＡＴＳの対象データに第１の画像ＧＰＳ情報が結合される前のデータを作成してハッシュ値対象データ作成用データを作成し、これを検証者端末に送信する（ステップ６５０）。

【０１１３】

検証者端末は、ハッシュ値対象データ作成用データを受信すると、これに第１の画像ＧＰＳ情報を結合して追加し、ハッシュ値対象データを作成する（ステップ６５５）。
次に、検証者端末は、ハッシュ値対象データのハッシュ値を計算して長期署名サーバ３に送信する（ステップ６６０）。

【０１１４】

長期署名サーバ３は、検証者端末から当該ハッシュ値を受信すると、これとＡＴＳ（１ｓｔ）に記載されているハッシュ値が一致することを確認することによりＡＴＳ（１ｓｔ）のハッシュ値を検証する（ステップ６６５）。
次に、長期署名サーバ３は、ＡＴＳ（１ｓｔ）の証明書の認証パスを作成するための証明書（ルート証明書）を自サーバ内から取得する（ステップ６７０）。

【０１１５】

次に、長期署名サーバ３は、当該認証パス上の証明書の失効情報をリポジトリサーバ１１から取得する（ステップ６７５、６８０）。
そして、長期署名サーバ３は、認証パスがつながること、認証パス上の証明書が失効していないことを確認することによりＡＴＳ（１ｓｔ）の証明書の検証を行う（ステップ６８５）。

【０１１６】
次に、長期署名サーバ３は、その他、ＸＡｄＥＳの検証を行う（ステップ６９０）。
この検証は、各証明書、各失効情報、各タイムスタンプ間の時刻の整合性が取れることの確認、フォーマットの整合性の確認などにより行われる。
長期署名サーバ３は、以上の検証による検証結果を生成して検証者端末に送信する（ステップ６９５）。
そして、検証者端末は、長期署名サーバ３から検証結果を受信して検証者に提示する（ステップ７００）。
なお、ＡＴＳがＡＴＳ（２ｎｄ）、ＡＴＳ（３ｒｄ）と更に下の世代が存在する場合も同様にして検証する。
【０１１７】
以上のように、上の検証方法によると、検証者は画像データを検証者端末に保持したまま長期署名サーバ３で長期署名データの検証を行うことができる。
そのため、例えば、甲が第１の画像ＧＰＳ情報、及び長期署名データを乙に提供し、画像データを甲乙以外の者に渡したくない場合に、乙は画像データを長期署名サーバ３に提供せずに長期署名データによる画像データの正当性を確認することができると共に、撮影日時刻と撮影場所の正当性も確認することができる。
【０１１８】
また、例え、ＥＳ－Ｔの生成で用いたアルゴリズムが危殆化したとしてもＡＴＳ（１ｓｔ）の生成に用いたアルゴリズムが危殆化するまではＥＳ－Ａ（１ｓｔ）の証拠性は失われない。
そして、ＡＴＳ（１ｓｔ）の生成に用いたアルゴリズムが危殆化する可能性がある場合は、更に最新のアルゴリズムでＡＴＳ（２ｎｄ）を付与すれば証拠性は失われない。
以降、最新のアルゴリズムで世代を重ねていくことにより証拠性を未来に渡って維持することができる。
【０１１９】
以上に説明した検証方法により、次の構成を得ることができる。
なお、以下の構成で原本データは長期署名データで検証対象となるデータであって、本実施の形態では、画像ＧＰＳ情報（第１、第２、第３の画像ＧＰＳ情報）が相当する。
署名対象データと前記署名対象データを検証する検証情報、及び前記署名対象データと検証情報を所定期間検証する長期検証情報を含む長期検証情報を用いて構成され、原本データの正当性を検証するための長期署名データを検証者端末から受信する長期署名データ受信手段と、前記署名対象データに含まれる所定の情報を抽出して長期検証情報作成用情報を作成し、当該作成した長期検証情報作成用情報を前記検証者端末に送信する長期検証情報作成用情報送信手段と、前記検証者端末から、前記送信した長期検証情報作成用情報に前記原本データを加えて所定の関数で計算した長期検証情報作成用関数値を受信する長期検証情報作成用関数値受信手段と、前記受信した長期検証情報作成用関数値を用いて前記長期検証情報を検証する長期検証情報検証手段と、を具備したことを特徴とする長期署名検証用サーバ（第１の構成）。
前記検証情報を用いて前記署名対象データを検証する署名対象データ検証手段を具備し、前記長期検証情報検証手段は、前記署名対象データ検証手段が検証した後に前記長期検証情報を検証することを特徴とする第１の構成の長期署名検証用サーバ（第２の構成）。
【０１２０】
このように、本実施の形態は、原本データをサーバ側に渡さずにサーバ側で原本データに対する署名を検証することができる。
この場合、端末は、原本データの所定関数による関数値と、当該原本データの署名データ（原本データの関数値を秘密鍵で暗号化した署名値、当該秘密鍵に対応する公開鍵の公開鍵証明書）を送信し、サーバは、署名値を公開鍵で復号化して関数値を取り出し、当該取り出した関数値と端末が送信してきた関数値を比べることにより原本データの正当性を判断すると共に、認証パスに係る証明書を用いて公開鍵証明書の正当性を確認する。

更に、署名データが長期署名である場合には、サーバは、署名データを構成する情報を用いて長期署名を確認するための関数値を作成するための情報から原本データを除いた情報を作成して端末に送信する。

これに対し、端末は、当該情報に原本データを加えて所定関数による関数値を計算してサーバに送信し、サーバは当該関数値を用いて長期署名の正当性を検証する。

【０１２１】

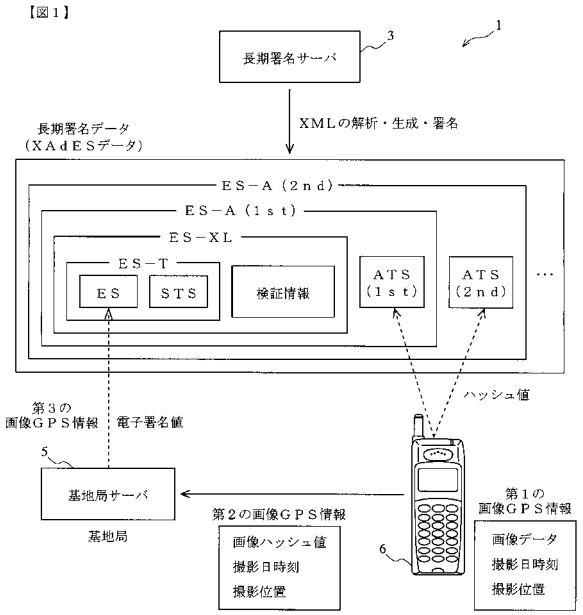
このように、本実施の形態では、署名対象となる原本データ（画像ＧＰＳ情報）を複数の原本データ（画像ハッシュ値、現在日時刻ハッシュ値、現在位置ハッシュ値）のグループとして１つのＥＳ－Ａを作成することができる。

【符号の説明】

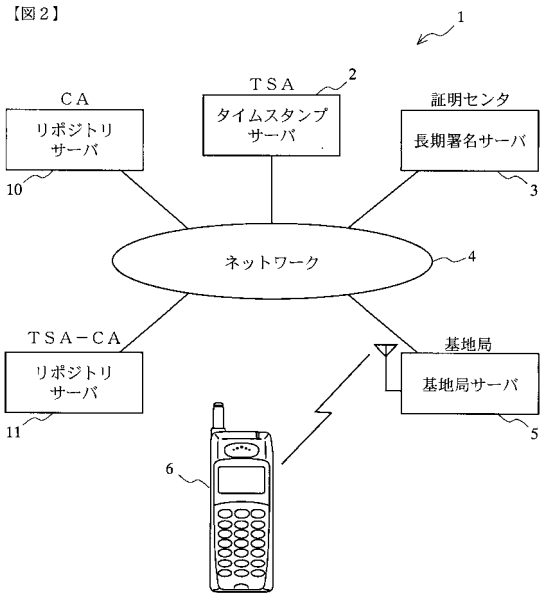
【０１２２】

１　長期署名システム
２　タイムスタンプサーバ
３　長期署名サーバ
４　ネットワーク
５　基地局サーバ
６　携帯端末
１０　リポジトリサーバ
１１　リポジトリサーバ

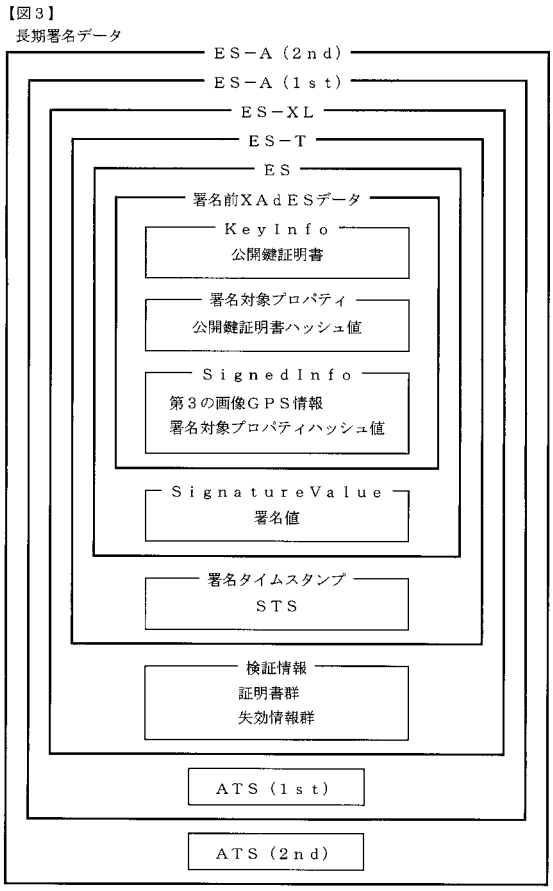
【図１】



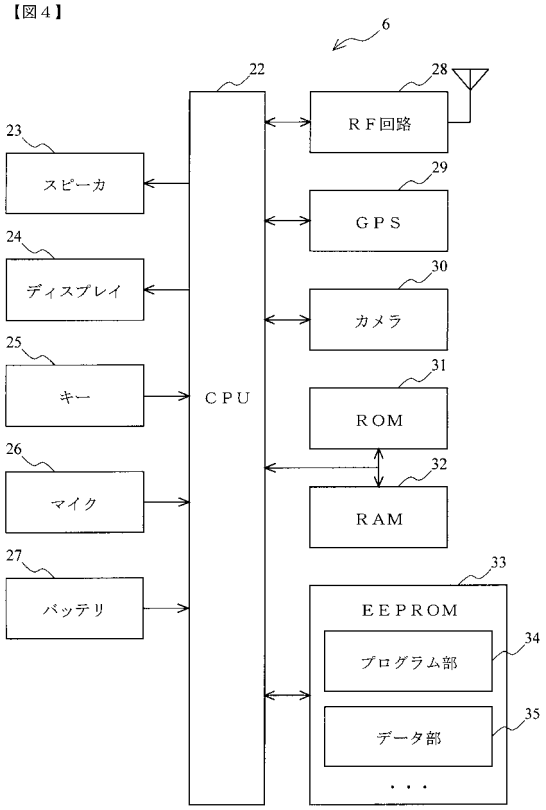
【図２】



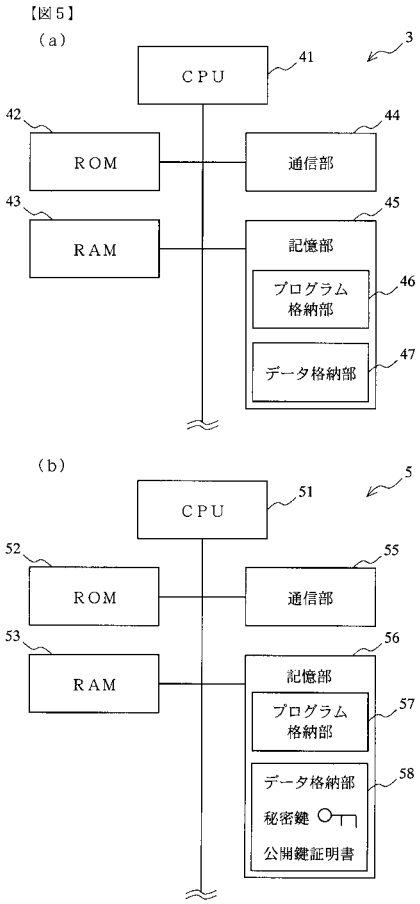
【図３】


【図３】
長期署名データ
ＥＳ－Ａ（２ｎｄ）
ＥＳ－Ａ（１ｓｔ）
ＥＳ－ＸＬ
ＥＳ－Ｔ
ＥＳ
署名前ＸＡｄＥＳデータ
ＫｅｙＩｎｆｏ
公開鍵証明書
署名対象プロパティ
公開鍵証明書ハッシュ値
ＳｉｇｎｅｄＩｎｆｏ
第３の画像ＧＰＳ情報
署名対象プロパティハッシュ値
ＳｉｇｎａｔｕｒｅＶａｌｕｅ
署名値
署名タイムスタンプ
ＳＴＳ
検証情報
証明書群
失効情報群
ＡＴＳ（１ｓｔ）
ＡＴＳ（２ｎｄ）

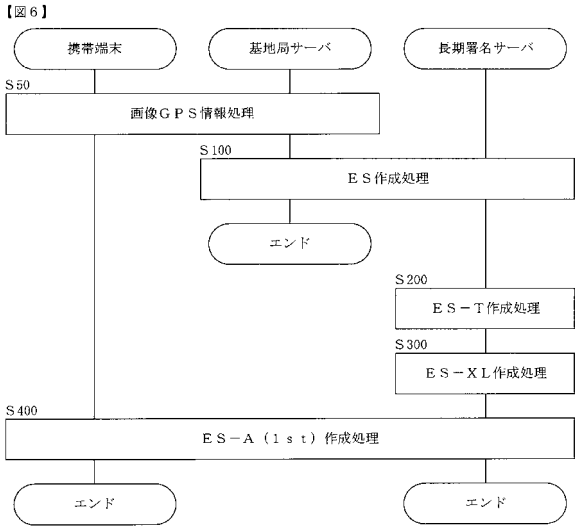
【図４】


【図４】
6
22
28
ＲＦ回路
23
スピーカ
29
ＧＰＳ
24
ディスプレイ
30
カメラ
25
キー
ＣＰＵ
31
ＲＯＭ
26
マイク
32
ＲＡＭ
27
バッテリ
33
ＥＥＰＲＯＭ
プログラム部
34
データ部
35
・・・

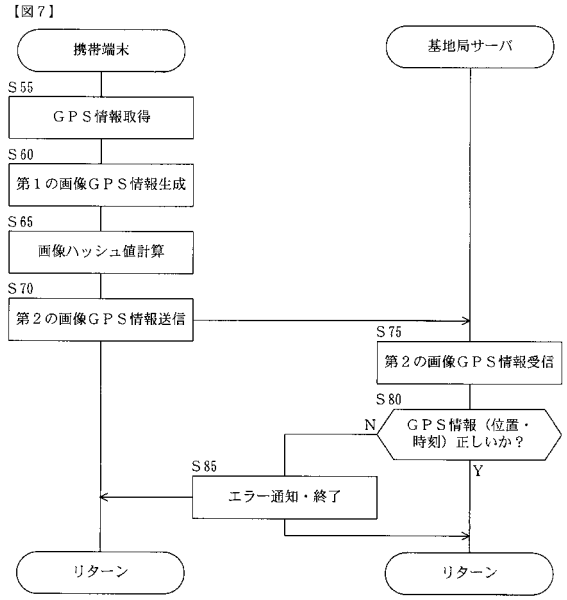
【図５】


【図５】
（ａ）
ＣＰＵ
41
3
42
ＲＯＭ
44
通信部
43
ＲＡＭ
45
記憶部
プログラム格納部
46
データ格納部
47
（ｂ）
ＣＰＵ
51
5
52
ＲＯＭ
55
通信部
53
ＲＡＭ
56
記憶部
プログラム格納部
57
データ格納部
秘密鍵
公開鍵証明書
58

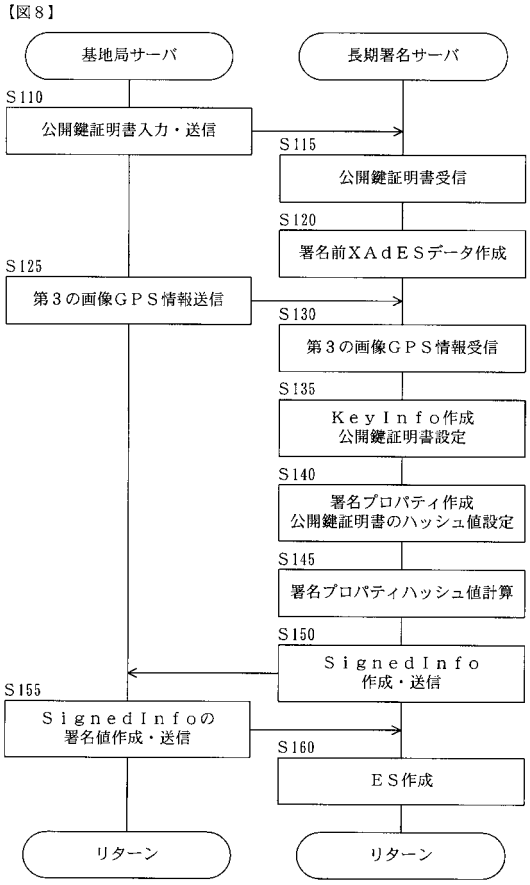
【図６】


【図６】
携帯端末
基地局サーバ
長期署名サーバ
Ｓ50
画像ＧＰＳ情報処理
Ｓ100
ＥＳ作成処理
エンド
Ｓ200
ＥＳ－Ｔ作成処理
Ｓ300
ＥＳ－ＸＬ作成処理
Ｓ400
ＥＳ－Ａ（１ｓｔ）作成処理
エンド
エンド

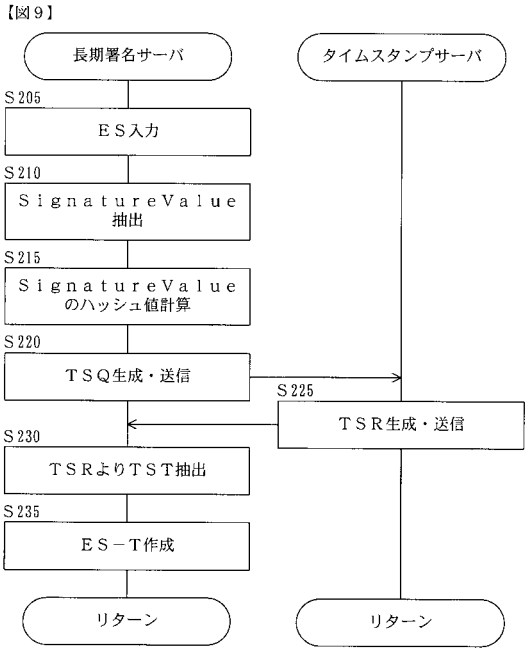
【図７】


【図７】
携帯端末
基地局サーバ
S55
ＧＰＳ情報取得
S60
第１の画像ＧＰＳ情報生成
S65
画像ハッシュ値計算
S70
第２の画像ＧＰＳ情報送信
S75
第２の画像ＧＰＳ情報受信
S80
ＧＰＳ情報（位置・時刻）正しいか？
N
Y
S85
エラー通知・終了
リターン
リターン

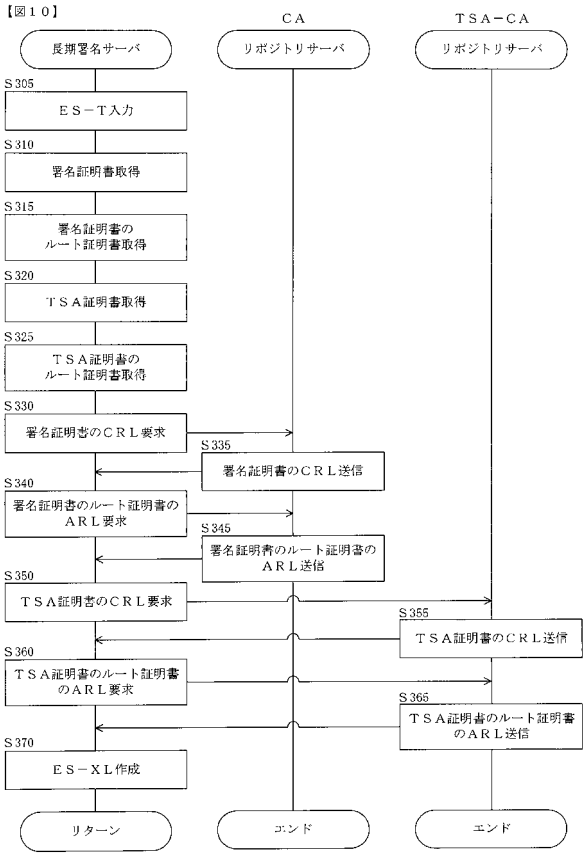
【図８】


【図８】
基地局サーバ
長期署名サーバ
S110
公開鍵証明書入力・送信
S115
公開鍵証明書受信
S120
署名前ＸＡｄＥＳデータ作成
S125
第３の画像ＧＰＳ情報送信
S130
第３の画像ＧＰＳ情報受信
S135
ＫｅｙＩｎｆｏ作成
公開鍵証明書設定
S140
署名プロパティ作成
公開鍵証明書のハッシュ値設定
S145
署名プロパティハッシュ値計算
S150
ＳｉｇｎｅｄＩｎｆｏ
作成・送信
S155
ＳｉｇｎｅｄＩｎｆｏの
署名値作成・送信
S160
ＥＳ作成
リターン
リターン

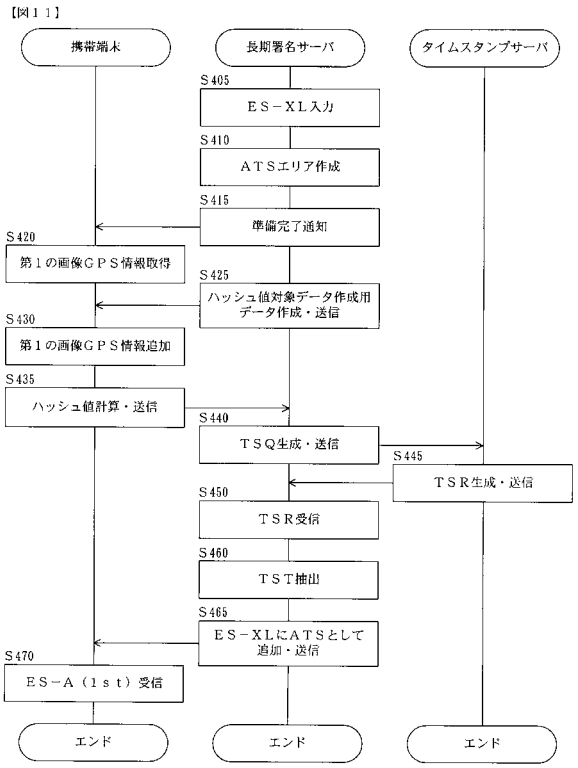
【図９】


【図９】
長期署名サーバ
タイムスタンプサーバ
S205
ＥＳ入力
S210
ＳｉｇｎａｔｕｒｅＶａｌｕｅ
抽出
S215
ＳｉｇｎａｔｕｒｅＶａｌｕｅ
のハッシュ値計算
S220
ＴＳＱ生成・送信
S225
ＴＳＲ生成・送信
S230
ＴＳＲよりＴＳＴ抽出
S235
ＥＳ－Ｔ作成
リターン
リターン

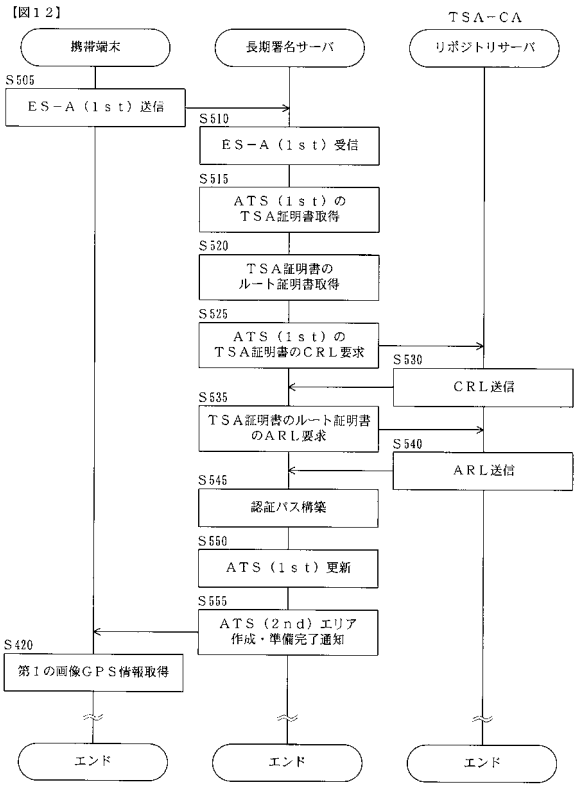
【図１０】


【図１０】
ＣＡ
ＴＳＡ－ＣＡ
長期署名サーバ
リポジトリサーバ
リポジトリサーバ
S305
ＥＳ－Ｔ入力
S310
署名証明書取得
S315
署名証明書の
ルート証明書取得
S320
ＴＳＡ証明書取得
S325
ＴＳＡ証明書の
ルート証明書取得
S330
署名証明書のＣＲＬ要求
S335
署名証明書のＣＲＬ送信
S340
署名証明書のルート証明書の
ＡＲＬ要求
S345
署名証明書のルート証明書の
ＡＲＬ送信
S350
ＴＳＡ証明書のＣＲＬ要求
S355
ＴＳＡ証明書のＣＲＬ送信
S360
ＴＳＡ証明書のルート証明書
のＡＲＬ要求
S365
ＴＳＡ証明書のルート証明書
のＡＲＬ送信
S370
ＥＳ－ＸＬ作成
リターン
エンド
エンド

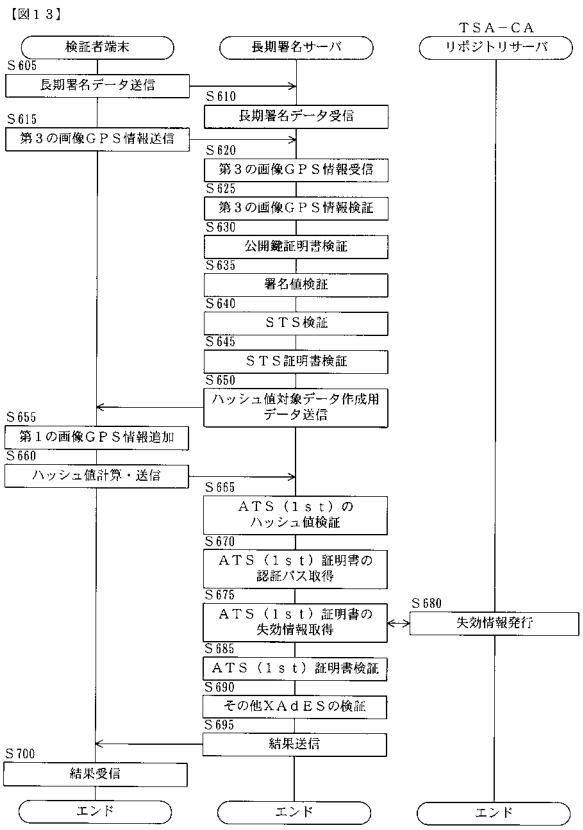
【図１１】


【図１１】
携帯端末
長期署名サーバ
タイムスタンプサーバ
S405
ＥＳ－ＸＬ入力
S410
ＡＴＳエリア作成
S415
準備完了通知
S420
第１の画像ＧＰＳ情報取得
S425
ハッシュ値対象データ作成用データ作成・送信
S430
第１の画像ＧＰＳ情報追加
S435
ハッシュ値計算・送信
S440
ＴＳＱ生成・送信
S445
ＴＳＲ生成・送信
S450
ＴＳＲ受信
S460
ＴＳＴ抽出
S465
ＥＳ－ＸＬにＡＴＳとして追加・送信
S470
ＥＳ－Ａ（１ｓｔ）受信
エンド
エンド
エンド

【図１２】


【図１２】
携帯端末
長期署名サーバ
ＴＳＡ－ＣＡ
リポジトリサーバ
S505
ＥＳ－Ａ（１ｓｔ）送信
S510
ＥＳ－Ａ（１ｓｔ）受信
S515
ＡＴＳ（１ｓｔ）のＴＳＡ証明書取得
S520
ＴＳＡ証明書のルート証明書取得
S525
ＡＴＳ（１ｓｔ）のＴＳＡ証明書のＣＲＬ要求
S530
ＣＲＬ送信
S535
ＴＳＡ証明書のルート証明書のＡＲＬ要求
S540
ＡＲＬ送信
S545
認証パス構築
S550
ＡＴＳ（１ｓｔ）更新
S555
ＡＴＳ（２ｎｄ）エリア作成・準備完了通知
S420
第１の画像ＧＰＳ情報取得
エンド
エンド
エンド

【図１３】


【図１３】
検証者端末
長期署名サーバ
ＴＳＡ－ＣＡ
リポジトリサーバ
S605
長期署名データ送信
S610
長期署名データ受信
S615
第３の画像ＧＰＳ情報送信
S620
第３の画像ＧＰＳ情報受信
S625
第３の画像ＧＰＳ情報検証
S630
公開鍵証明書検証
S635
署名値検証
S640
ＳＴＳ検証
S645
ＳＴＳ証明書検証
S650
ハッシュ値対象データ作成用データ送信
S655
第１の画像ＧＰＳ情報追加
S660
ハッシュ値計算・送信
S665
ＡＴＳ（１ｓｔ）のハッシュ値検証
S670
ＡＴＳ（１ｓｔ）証明書の認証パス取得
S675
ＡＴＳ（１ｓｔ）証明書の失効情報取得
S680
失効情報発行
S685
ＡＴＳ（１ｓｔ）証明書検証
S690
その他ＸＡｄＥＳの検証
S695
結果送信
S700
結果受信
エンド
エンド
エンド

フロントページの続き

(72)発明者　村尾　進一
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツル株式会社内
(72)発明者　上畑　正和
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツル株式会社内
(72)発明者　柴田　孝一
千葉県千葉市美浜区中瀬１丁目８番地　セイコーインスツル株式会社内

審査官　金沢　史明

(56)参考文献　特開２００７－２２１４３５（ＪＰ，Ａ）
特開２００３－２８４１１３（ＪＰ，Ａ）
特開２００７－２２１５５１（ＪＰ，Ａ）
特開２００８－０４１０１６（ＪＰ，Ａ）
特開２００７－０６０６６８（ＪＰ，Ａ）
国際公開第２００７／１２２７２６（WO，Ａ１）
特開２００８－２５２４０７（ＪＰ，Ａ）
特開２００５－０４５４８６（ＪＰ，Ａ）
特開２００５－２８６６８７（ＪＰ，Ａ）
特開２００７－１５８３９７（ＪＰ，Ａ）
国際公開第２００５／１１９５３９（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２