(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2021-111925
(P2021-111925A)
(43)公開日　令和3年8月2日(2021.8.2)

(51)Int.Cl.			F I		テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B
H04L	9/10	(2006.01)	H04L	9/00	621A
G09C	1/00	(2006.01)	G09C	1/00	640E
G06F	21/64	(2013.01)	G06F	21/64	
G06F	21/33	(2013.01)	G06F	21/33	

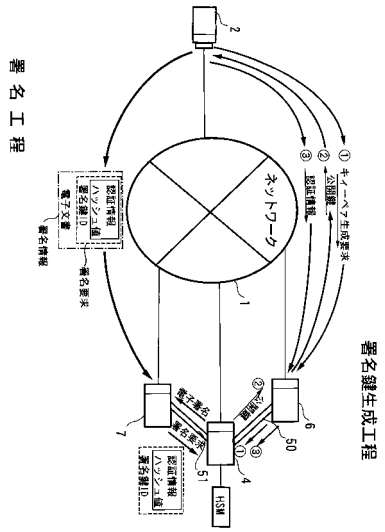
審査請求 未請求　請求項の数 8　ＯＬ　（全 15 頁）

(21)出願番号　特願2020-4147(P2020-4147)
(22)出願日　令和2年1月15日(2020.1.15)

(71)出願人　519430778
木戸　啓介
神奈川県横浜市青葉区みすずが丘１２－１１
(74)代理人　100124280
弁理士　大山　健次郎
(72)発明者　木戸　啓介
神奈川県横浜市青葉区みすずが丘１２－１１

(54)【発明の名称】電子署名システム

(57)【要約】
【課題】システム管理者による署名鍵の悪用が防止され、セキュリティレベルの高い電子署名システムを実現する。
【解決手段】利用者は、端末装置（２）を介して耐タンパ装置（５）に保存されている自己の署名鍵について利用者自身が想到した認証情報を設定する。電子文書に電子署名を行う場合、利用者は、端末装置（２）を介して自身の認証情報及び署名対象データ（ハッシュ値）を暗号化し、暗号化された認証情報及び署名対象データを耐タンパ装置（５）に送信して署名鍵の使用許可を求める。耐タンパ装置（５）は、入力された認証情報について検証を行い、正しい認証情報が入力された場合だけ署名を許可し、電子署名を行う。この結果、署名鍵について正当な使用権限を有する者しか電子署名できない署名システムが構築される。
【選択図】図８



【特許請求の範囲】
【請求項１】
署名鍵を生成及び管理する機能を有する１つ又は１つ以上の耐タンパ装置、及び、耐タンパ装置を制御する機能を有する鍵管理サーバを有する署名システムと、利用者が利用する端末装置とを具えるリモート署名方式の電子署名システムにおいて、
前記耐タンパ装置は、署名鍵となる秘密鍵と公開鍵とのキーペアを生成する機能、生成された署名鍵を当該署名鍵についての使用権限を示す認証情報と関連付けて保存する機能、認証情報を含む暗号化情報を復号する機能、復号された認証情報を検証する機能、及び検証結果に基づいて前記署名鍵を用いて署名対象データにデジタル署名する機能を有し、
前記端末装置は、電子文書から署名対象データを生成する手段、認証情報を入力する手段、入力された認証情報及び生成された署名対象データを暗号化する暗号化手段を有し、
耐タンパ装置は、利用者からのキーペア生成要求又は署名鍵生成要求に応じて、署名鍵となる秘密鍵と公開鍵とのキーペァを生成し、生成されたキーペアは、利用者によって想到され端末装置から送られた認証情報と関連付けて耐タンパ装置内に保存され、
電子署名に際し、利用者は自身の認証情報を端末装置に入力し、端末装置は署名対象の電子文書から署名対象データを生成し、さらに、端末装置は、入力された認証情報及び生成された署名対象データを暗号化し、暗号化された認証情報及び署名対象データ並びに署名鍵識別情報を含む署名要求を耐タンパ装置に送信し、
耐タンパ装置は、受信した署名要求に含まれる認証情報及び署名対象データを復号し、復号された認証情報と署名鍵識別情報により特定される署名鍵と関連付けて保管されている認証情報との一致性を検証し、これらの認証情報が一致する場合当該署名鍵を用いて前記復号された署名対象データにデジタル署名することを特徴とする電子署名システム。
【請求項２】
請求項１に記載の電子署名システムにおいて、前記耐タンパ装置は、キーペア生成後、生成したキーペアの公開鍵を端末装置に送信し、端末装置の暗号化手段は、キーペアの公開鍵を暗号鍵として用いて認証情報及び署名対象データを暗号化し、前記耐タンパ装置は、前記キーペアの秘密鍵を解読鍵として用いて受信した認証情報及び署名対象データを復号することを特徴とする電子署名システム。
【請求項３】
請求項１又は２に記載の電子署名システムにおいて、前記キーペアの公開鍵は、生成された署名鍵の識別情報として用いられ、端末装置から耐タンパ装置に送信される署名要求は前記公開鍵を含むことを特徴とする電子署名システム。
【請求項４】
請求項１に記載の電子署名システムにおいて、前記耐タンパ装置は公開鍵暗号通信を行うために設定された秘密鍵と公開鍵のキーペアを有し、前記端末装置の暗号化手段は、前記キーペアの公開鍵を暗号鍵として用いて認証情報及び署名対象データを暗号化し、前記耐タンパ装置は、前記キーペアの秘密鍵を解読鍵として用いて入力した認証情報及び署名対象データを復号することを特徴とする電子署名システム。
【請求項５】
請求項１、２、３又は４に記載の電子署名システムにおいて、当該電子署名システムは、さらに、電子証明書を生成する証明書発行サーバ及び電子文書を編集する機能を有する編集サーバを有し、
鍵管理サーバと証明書発行サーバは第１のＶＰＮ接続により相互接続され、鍵管理サーバと編集サーバは第２のＶＰＮ接続により相互接続されていることを特徴とする電子署名システム。
【請求項６】
請求項５に記載の電子署名システムにおいて、署名鍵の生成に際し、端末装置はキーペア生成要求を鍵管理サーバに送信し、耐タンパ装置は、キーペア生成要求に応じてキーペアを生成し、生成されたキーペアの公開鍵は鍵管理サーバから第１のＶＰＮ接続及び証明書発行サーバを介して端末装置に送信され、端末装置は、受信した公開鍵を用いて認証情

報を暗号化して耐タンパ装置に送信することを特徴とする電子署名システム。
【請求項７】
請求項５又は６に記載の電子署名システムにおいて、電子署名に際し、端末装置は署名の対象である電子文書から署名対象データを生成し、生成された署名対象データ及び認証情報を暗号化し、暗号化された署名対象データ及び認証情報と署名鍵識別情報とを含む署名鍵要求を生成し、署名鍵要求と前記電子文書を含む署名情報を編集サーバに送信し、
編集サーバは、署名情報から署名要求を取り出して耐タンパ装置に送信することを特徴とする電子署名システム。
【請求項８】
請求項７に記載の電子署名システムにおいて、前記耐タンパ装置により生成された電子署名は鍵管理サーバ及び第２のＶＰＮ接続を介して編集サーバに送信され、編集サーバは受け取った電子署名を電子文書に埋め込み、署名済み電子文書を生成することを特徴とする電子署名システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、リモート署名方式の電子署名システムに関するものである。
【背景技術】
【０００２】
利用者の署名鍵を事業者のサーバに設置し、利用者がサーバに遠隔でログインし、事業者のサーバ上で自身の署名鍵を用いて電子署名するリモート署名システムが提案されている。リモート署名システムは電子署名を遠隔で行うことができると共にユーザが署名鍵を管理する必要がないため、ユーザにとって利便性の高い署名システムとして期待されている。
【０００３】
リモート署名方式の電子署名システムとして、署名鍵を管理する鍵管理システムと、証明書を発行する証明書発行システムと、利用者が利用する端末装置とを含む電子署名システムが提案されている（例えば、特許文献１参照）。この既知の電子署名システムでは、鍵管理システムに設定されたユーザのアカウントに基づき、ユーザIDとパスワードの組合せによりユーザ認証が行われている。
【０００４】
別のリモート署名システムとして、非特許文献１には以下のシステム構成例が開示されている。署名者は、署名アプリケーションに対して自身の署名者IDと署名対象データを送信して認証要求を行う。署名アプリケーションによって署名者が正しく認証されると、署名アプリケーションから署名デバイスに署名者IDと関連する署名鍵IDと署名対象データが送られる。署名装置では、署名鍵IDにより指定された署名鍵を用いて署名が行われ、署名付きの署名対象データが出力される。
【０００５】
さらに、上記非特許文献１には、リモート署名システムにおいて、２要素認証を行うことも記載されている。２要素認証として、署名鍵を活性化するための情報が端末装置から署名デバイスに送信されている。
【特許文献１】特許第６４６５４２６号公報
【非特許文献１】「リモート署名の検討状況」（Network Security Forum 2017 ）
【発明の概要】
【発明が解決しようとする課題】
【０００６】
現在実用化されている電子署名システムでは、ユーザIDとパスワードによるユーザ認証

だけしか行われていないのが実情である。しかしながら、ユーザIDとパスワードによるユーザ認証だけでは、成り済ましの危険性が高く、セキュリティレベルを一層高くすることが要請されている。

【０００７】

リモート署名システムでは、本人しか署名できないことが重要であり、且つそれを論理的に立証できるシステムであることが望ましい。しかし、署名鍵は事業者のサーバに保管され、電子署名は事業者のサーバ上で行われるため、悪意のあるシステム管理者により署名鍵が悪用される危険性がある。すなわち、電子署名をHSMのような耐タンパ装置で行っても、種々の情報は耐タンパ装置を管理する鍵管理サーバを経由して耐タンパ装置に送られる。よって、鍵管理サーバを管理するシステム管理者は、鍵管理サーバにおいて各種情報を盗み又は抜き取ることが可能である。現状、前記文献に記載されているシステムでは、システム管理者は情報を保護する人に位置づけられ、保護対象は第三者の攻撃に向けられている。従って、システム管理者による署名鍵や署名鍵を制御する情報の盗用と悪用の危険性は否めず、結果として、論理的に本人しか署名できないことを立証できるシステムに至っていない。

【０００８】

本発明の目的は、署名鍵について正当な使用権限を有する者しか電子署名できない電子署名システムを提供する。

本発明の目的は、システム管理者による署名鍵の悪用が防止され、一層高いセキュリティレベルの電子署名システムを実現することにある。

【課題を解決するための手段】

【０００９】

本発明による電子署名システムは、署名鍵を生成及び管理する機能を有する１つ又は１つ以上の耐タンパ装置、及び、耐タンパ装置を制御する機能を有する鍵管理サーバを有する署名システムと、利用者が利用する端末装置とを具えるリモート署名方式の電子署名システムにおいて、

前記耐タンパ装置は、署名鍵となる秘密鍵と公開鍵とのキーペアを生成する機能、生成された署名鍵を当該署名鍵についての使用権限を示す認証情報と関連付けて保存する機能、入力した暗号化された認証情報を復号する機能、復号された認証情報を検証する機能、及び検証結果に基づいて前記署名鍵を用いて署名対象データにデジタル署名する機能を有し、

前記端末装置は、電子文書から署名対象データを生成する手段、認証情報を入力する手段、入力された認証情報及び生成された署名対象データを暗号化する暗号化手段を有し、

耐タンパ装置は、利用者からのキーペア生成要求又は署名鍵生成要求に応じて、署名鍵となる秘密鍵と公開鍵とのキーペァを生成し、生成されたキーペアは、利用者によって想到され端末装置から送られた認証情報と関連付けて耐タンパ装置内に保存され、

電子署名に際し、利用者は自身の認証情報を端末装置に入力し、端末装置は署名対象の電子文書から署名対象データを生成し、さらに、端末装置は、入力された認証情報及び生成された署名対象データを暗号化し、暗号化された認証情報及び署名対象データ並びに署名鍵識別情報を含む署名要求を耐タンパ装置に送信し、

耐タンパ装置は、受信した署名要求に含まれる認証情報及び署名対象データを復号し、復号された認証情報と署名鍵識別情報により特定される署名鍵と関連付けて保管されている認証情報との一致性を検証し、これらの認証情報が一致する場合当該署名鍵を用いて前記復号された署名対象データにデジタル署名することを特徴とする。

【００１０】

本発明では、耐タンパ装置は利用者からのキーペア生成要求又は署名鍵生成要求に応じて署名鍵を生成する。利用者は、署名鍵についての使用権限を示す認証情報を想到し、自身により記憶すると共に端末装置を介して耐タンパ装置に送信する。耐タンパ装置は、各利用者の署名鍵を当該利用者の認証情報と関係付けて保存する。一方、電子署名に当たり、利用者は自身の認証情報を耐タンパ装置に送信して署名鍵の使用許可を求める。耐タン

パ装置は、入力された認証情報について検証を行い、正しい認証情報が入力された場合だけ署名を許可し、電子署名が行われる。この結果、署名鍵について正当な使用権限を有する者しか電子署名できない署名システムが構築される。よって、従来実施されている電子署名システムよりも一層高いセキュリティレベルの電子署名システムが実現される。

【００１１】

上述した電子署名システムでは、認証情報を知っているユーザしか電子署名が許可されない高度な利点が達成される。しかしながら、この方式の電子署名システムでは、利用者により設定された認証情報が他人により盗まれた場合、署名鍵が悪用される危険性がある。例えば、署名鍵IDと認証情報が盗まれ、ハッシュ値が改ざんされた署名要求が行われた場合、耐タンパ装置は、入力された認証情報は有効であると判断するため、当該署名要求は有効であると判定され、改ざんされたハッシュ値に電子署名が行われる。従って、この電子署名システムを有効活用するには、正当な使用権限を示す認証情報の盗用に対して有効に対処する必要がある。特に、端末装置から耐タンパ装置に送られる認証情報は、耐タンパ装置を管理する鍵管理サーバないし署名サーバを経由して耐タンパ装置に送られるため、これらのサーバで署名要求が抜き取られ、悪用される危険性がある。

【００１２】

この課題を解決するため、本発明では、電子署名に際し、認証情報を入力すると共に、端末装置において電子文書から署名対象データを生成する。そして、端末装置に設けられた暗号化手段を用いて、認証情報及び署名対象データの両方を一緒に暗号化し、暗号化された認証情報及びハッシュ値を含む署名要求を耐タンパ装置に送信する。このように、認証情報及びハッシュ値の両方を暗号化して耐タンパ装置に送信すれば、たとえ鍵管理サーバにおいて署名要求が抜き取られても、認証情報だけでなく署名対象であるハッシュ値についても改ざんできないため、改ざんされたハッシュ値を含む署名要求について電子署名を行う不具合を有効に防止することができる。この結果として、署名鍵について正当な使用権限を有する者しか電子署名できないと共にシステム管理者による署名鍵の悪用が有効に防止された電子署名システムが構築される。このように、本発明の要旨は、端末装置において、署名鍵の使用権限を示す認証情報及び電子文書から生成した署名対象データの両方を一緒に暗号化して耐タンパ装置に送信することにある。

【００１３】

本発明による電子署名システムの好適実施例は、耐タンパ装置は、キーペア生成後、生成したキーペアの公開鍵を端末装置に送信し、端末装置の暗号化手段は、キーペアの公開鍵を暗号鍵として用いて認証情報及び署名対象データを暗号化し、前記耐タンパ装置は、前記キーペアの秘密鍵を解読鍵として用いて受信した認証情報及び署名対象データを復号することを特徴とする。本発明では、署名鍵を生成するために作成されたキーペアの秘密鍵と公開鍵を公開鍵暗号通信に利用する。すなわち、署名鍵を作成するために生成されたキーペアの公開鍵を暗号鍵として用い秘密鍵を解読鍵として用いて公開鍵暗号通信を行う。キーペアの公開鍵で暗号化された認証情報は、対応する秘密鍵でしか復号されず、解読鍵である秘密鍵は耐タンパ装置内に安全に保存されている。よって、たとえ暗号化された認証情報や署名対象データがシステム管理者によって盗まれても復号されることはない。しかも、キーペアの公開鍵は、耐タンパ装置で生成された後端末装置に送信されるので、端末装置における耐タンパ装置のアドレス設定の煩雑性が解消される利点も達成される。

【００１４】

本発明による電子署名システムの好適実施例は、前記キーペアの公開鍵は、署名鍵の識別情報として用いられ、端末装置から耐タンパ装置に送信される署名要求は前記公開鍵を含むことを特徴とする。本例では、署名鍵を形成するために生成されたキーペアの公開鍵は、暗号鍵として用いると共に署名鍵を特定する署名鍵識別情報として用いる。公開鍵は秘密鍵に対応して生成されるので、キーペアの生成に応じて署名鍵を特定する識別情報が生成されるので、署名鍵識別情報を別途作成する必要性が解消される。

【００１５】

本発明による電子署名システムの別の好適実施例は、耐タンパ装置は公開鍵暗号通信を

行うために設定された秘密鍵と公開鍵のキーペアを有し、前記端末装置の暗号化手段は、前記キーペアの公開鍵を暗号鍵として用いて認証情報及び署名対象データを暗号化し、前記耐タンパ装置は、前記キーペアの秘密鍵を解読鍵として用いて入力した認証情報及び署名対象データを復号することを特徴とする。耐タンパ装置に設定された公開鍵暗号通信用のキーペアの秘密鍵は、耐タンパ装置内に安全に保存され、外部に流出することはない。従って、耐タンパ装置に設定された公開鍵暗号通信のためのキーペアの秘密鍵及び公開鍵を解読鍵及び暗号鍵としてそれぞれ用いれば、認証情報が端末装置から鍵管理サーバを中継して耐タンパ装置に送信される際の問題点が解消される。

【発明の効果】

【００１６】

本発明では、端末装置において、電子文書から署名対象データを生成し、署名鍵の使用権限を示す認証情報及び署名対象データの両方について暗号化し、暗号化された認証情報及び署名対象データを含む署名要求を耐タンパ装置に送信しているので、たとえシステム管理者によって認証情報が盗まれても、改ざんされた署名対象データに電子署名を行うことが防止される。

さらに、本発明では、端末装置から耐タンパ装置へ認証情報及び署名対象データを送信する際、公開鍵暗号方式を利用する。そして、秘密鍵が耐タンパ装置内に常時保存されているキーペアを用い、キーペアの秘密鍵を解読鍵として用い公開鍵を暗号鍵として用いる。この場合、公開鍵により暗号化された情報は、耐タンパ装置内に保存されている秘密鍵でしか解読されないため、署名要求が鍵管理サーバを中継して耐タンパ装置に送信されても、端末装置と耐タンパ装置は直接相互接続されているものと等価な通信状態に維持される。この結果、耐タンパ装置の有用性を利用しながら、鍵管理サーバを中継する課題が解消され、システム管理者による署名鍵の悪用が防止され、一層高いセキュリティが達成される。

署名鍵を作成するために生成されたキーペアの公開鍵は認証情報を暗号化するための暗号鍵として用いることができると共に署名鍵の識別情報として用いることができる。この場合、キーペアの公開鍵は２つの役割を果たすので、端末装置における作業性が増大する。

【図面の簡単な説明】

【００１７】

【図１】本発明による電子署名システムの全体構成を示す図である。

【図２】本発明による電子署名システムの署名鍵生成工程のアルゴリズムを示す図である。

【図３】本発明による電子署名システムの署名工程のアルゴリズムを示す図である。

【図４】署名鍵生成工程の変形例を示す図である。

【図５】端末装置の一例を示すブロック図である。

【図６】鍵管理サーバの一例を示す図である。

【図７】耐タンパ装置の一例を示す図である。

【図８】本発明による電子署名システムの変形例を示す図である。

【発明を実施するための形態】

【００１８】

本発明では、ユーザ認証に加えて、署名鍵の使用権限についても検証する。署名鍵の正当な使用権限を示す認証情報としてアクティベーションコード信号（「Activation Code信号」、 以下「ＡＣ信号」と称する）を用い、 個々の署名鍵について署名者しか知らないＡＣ信号を設定する。すなわち、署名鍵の生成に当たって、利用者はＡＣ信号を想到して端末装置に入力する。このＡＣ信号は利用者しか知らないコード情報である。端末装置は、入力されたＡＣ信号を暗号化して署名システムに設けた耐タンパ装置に送信する。また、電子署名を求める場合、ＡＣ信号及び署名対象データの両方を暗号化して耐タンパ装置に送信する。

【００１９】

利用者から署名要求がされた場合、利用者に対してＡＣ信号を入力させ、正しいＡＣ信号が入力されたか否かを耐タンパ装置で検証する。そして、正しいＡＣ信号が入力された場合のみ当該署名鍵を用いてデジタル署名を行うことを許可する。この署名システムでは、ＡＣ信号を知る者しか署名できないため、署名鍵の真の所有者しか署名できない電子署名システムが構築される。よって、署名鍵が盗まれても、悪用されることはない。

【００２０】

しかしながら、ＡＣ信号により署名鍵を制御する署名システムの場合、たとえ署名鍵が堅牢に保護されていても、ＡＣ信号がシステム管理者に渡った場合、システム管理者は入手したＡＣ信号を鍵管理サーバに入力することにより署名鍵を作動させることが可能である。すなわち、盗まれたＡＣ信号を含む署名要求が耐タンパ装置に送信された場合、ＡＣ信号自体は正常であるため、耐タンパ装置は正当な使用権限を有する者からの署名要求と判断し、デジタル署名が行われてしまう。従って、ＡＣ信号を盗用から厳格に保護することが重要な課題である。この課題を解決するため、ＡＣ信号を端末装置から耐タンパ装置に伝送する伝送工程及び署名及び検証等の信号処理を行う処理工程について検討する。

【００２１】

初めに、処理工程について検討する。本発明では、耐タンパ装置を用いてデジタル署名等の各種処理を実行する。耐タンパ装置は、署名鍵の生成、署名、復号及び検証を含む信号処理を耐タンパ装置の内部で行うことができる。また、耐タンパ装置は、署名鍵及び入力された情報が外部に流出しないように構成されている。しかも、耐タンパ装置は、外部から攻撃されても、保存されている情報を防護することができる。従って、耐タンパ装置を用いることにより、署名鍵及びＡＣ信号は安全に保存され、耐タンパ装置の外部に流出してシステム管理者に渡る危険性は無い。

【００２２】

次に、伝送工程について検討する。端末装置から耐タンパ装置に送信されたＡＣ信号は、耐タンパ装置を管理する鍵管理サーバを経由して耐タンパ装置に入力する。すなわち、耐タンパ装置はハードウェアであり、ネットワークを介する通信機能を有しない。よって、鍵管理サーバを介して信号の送受信が行われる。すなわち、端末装置から送信されたＡＣ信号は、鍵管理サーバを必ず経由するため、ＡＣ信号を含む署名要求は、鍵管理サーバにおいて悪意のシステム管理者によって盗まれ或いは抜き取られる危険性がある。すなわち、HSMのような耐タンパ装置を用いて署名鍵を堅牢に管理しても、ＡＣ信号を端末装置から耐タンパ装置に送信される間に抜き取られる危険性がある。このように、耐タンパ装置は、優れた有用性を有するものの、鍵管理サーバを通して送受信することに起因する課題がある。

【００２３】

そこで、本発明では、利用者によって入力されたＡＣ信号及び電子文書から生成された署名対象データを適切に暗号化して耐タンパ装置に送信する。本発明では、伝送方法として公開鍵暗号通信を用いる。暗号鍵及び解読鍵として作用する公開鍵と秘密鍵のキーペアとして、秘密鍵が常時耐タンパ装置内に保存されているキーペアを用いる。この場合、耐タンパ装置に格納されている秘密鍵でしか暗号化情報は復号されないため、たとえ署名要求が鍵管理サーバで抜き取られても、ＡＣ信号及び署名対象データが復号されることはない。よって、ＡＣ信号及び署名対象データを署名鍵とほぼ同等のセキュリティレベルに維持することができる。

【００２４】

耐タンパ装置との間で公開鍵暗号通信を行うために用いることができる公開鍵として、耐タンパ装置自身に設定されたキーペアの公開鍵、及び署名鍵を生成する際に作成されるキーペアの公開鍵がある。本発明では、これら両方の公開鍵を用いることができる。しかしながら、耐タンパ装置の公開鍵で暗号化する場合、事前に耐タンパ装置の公開鍵を入手して、端末装置のプログラムに読み込ます必要があり、設定作業が煩雑になる問題がある。すなわち、複数の耐タンパ装置を用いるシステムの場合、複数の公開鍵の中から利用可能な公開鍵を事前に入手し、入手した公開鍵をプログラムに読み込ませる必要がある。し

かしながら、この作業は煩雑であり、利用者に対して大きな負担となる欠点がある。
【００２５】
これに対して、署名鍵生成要求の際に生成されたキーペアの公開鍵は、署名鍵生成後に署名鍵生成通知と共に耐タンパ装置から端末装置に送ることができる。この場合、端末装置における煩雑な設定作業が不要になる。従って、署名鍵生成の際に生成されるキーペアの公開鍵を用いて暗号化することは極めて有益な手法である。
【００２６】
このように、本発明は、耐タンパ装置の利点を有効に活用しながら、適切な暗号化方法を採用することにより端末装置と耐タンパ装置とを直接相互接続したものと等価な通信状態に維持する。この結果、耐タンパ装置の利点を有効利用しながら耐タンパ装置の欠点が解消され、一層高いセキュリティレベルの電子署名システムが実現される。
【００２７】
図１は本発明による電子署名システムの全体構成を示す図である。ネットワーク１には端末装置２－１～２－ｎが接続される。これら端末装置は、利用者が電子署名を行うために利用する装置であり、例えばパーソナルコンピュータやスマートフォーンが用いられる。
【００２８】
ネットワーク１には、署名システム３を接続する。署名システム３は、鍵管理サーバ４及び鍵管理サーバに接続した１つ又は複数の耐タンパ装置５を有する。鍵管理サーバ４はネットワークに接続され、耐タンパ装置５を管理ないし制御する機能を有する。
【００２９】
耐タンパ装置５は署名鍵を外部に流出することなく安全に生成及び管理する機能を有し、例えばHardware Security Module（HSM）とすることができる。耐タンパ装置は、鍵を管理するプログラムである鍵管理モジュールを有し、秘密鍵（署名鍵）と公開鍵のキーペアの生成、署名鍵によるデジタル署名、署名鍵の保管、暗号化されたＡＣ信号又は暗号化されたＡＣ信号を含む情報信号の復号、復号されたＡＣ信号の検証する機能を実行する。また、耐タンパ装置５は、端末装置との間で公開鍵暗号通信を行うための秘密鍵と公開鍵のキーペアを有する。
【００３０】
さらに、ネットワーク１には、認証局に設けた証明書発行サーバ６を接続する。証明書発行サーバ６は、端末装置から送られる証明書発行要求に応じて証明書発行要求（CSR）を生成して電子証明書を生成する。
【００３１】
さらに、ネットワーク１には編集サーバ７も接続する。編集サーバ７は、端末装置から送られてくる署名対象である電子文書を編集し、署名システムで生成された電子署名を電子文書に埋め込み、署名済み電子文書を生成する。生成した署名済み電子文書は編集サーバ７に保管する。
【００３２】
次に、署名済み電子文書の生成アルゴリズムについて説明する。図２は署名鍵生成工程を示すフローチャートであり、図３は署名工程を示すフローチャートである。本例では、端末装置から耐タンパ装置にＡＣ信号を安全に送信するため、署名鍵を形成するためのキーペアの公開鍵及び秘密鍵を暗号鍵及び解読鍵として用いる公開鍵暗号通信を利用する。
【００３３】
図２を参照するに、利用者は端末装置２を介して署名システム３の鍵管理サーバ４に対して認証要求を行う。認証要求は、ユーザIDとパスワードによるユーザ認証とする。尚、利用者のアカウントが未作成の場合、鍵管理サーバ４は当該利用者のためのアカウントを新規に作成する。また、ユーザ認証方法として、ユーザIDとパスワードの組合せを認証する方式だけでなく、ＩＣカードに格納されたトークンを鍵管理サーバに送信することにより認証することもできる。ユーザ認証の後に、鍵管理サーバ４から端末装置２に認証応答が送信される。

【００３４】
ユーザ認証に成功すると、利用者は端末装置から鍵管理サーバ４に対してキーペア生成要求を送信する。鍵管理サーバ４は耐タンパ装置５にキーペア生成要求を送る。耐タンパ装置は、キーペア生成要求の受信に応じて、秘密鍵と公開鍵のキーペアを生成する。生成された秘密鍵は署名鍵となり電子署名に用いられる。また、公開鍵は、認証情報を暗号化する暗号鍵として機能すると共に署名鍵識別情報として利用する。耐タンパ装置は、生成した公開鍵を含むキーペア生成通知を鍵管理サーバに送り、鍵管理サーバは受信したキーペア生成通知を端末装置に送信する。端末装置は、受信した公開鍵を保管する。
【００３５】
利用者は、キーペア生成通知の受信に応じて、ＡＣ信号を想到し、想到したＡＣ信号をキーボードのような入力装置を介して端末装置に入力する。ＡＣ信号として、例えば８桁のコード情報とすることができる。或いは、利用者は記憶し易い簡単なコード信号の認証情報を設定し、端末装置においてメールアドレスと端末固有の定数との組合せ演算を行い、多数桁の複雑なコード信号に変換し、変換された多数桁のコード信号をＡＣ信号とすることも可能である。例えばＳＨＡ２５６ハッシュ演算を行う場合、利用者は、簡単なコード情報を記憶するだけであるから、認証情報を失念するケースが低減されると共に、３２バイト（２５６ビット）のランダムコードとなり、ＡＣコードのセキュリティは格段に向上する。
【００３６】
端末装置は、利用者によって入力されたＡＣ信号をキーペアの公開鍵を暗号鍵として用いて暗号化し、公開鍵を含む署名鍵生成要求を生成する。端末装置は、生成した署名鍵生成要求を鍵管理サーバを経由して耐タンパ装置に送信する。
【００３７】
耐タンパ装置は、受信した暗号化されたＡＣ信号をキーペアの秘密鍵を解読鍵として用いて復号する。耐タンパ装置は、署名鍵識別情報（キーペアの公開鍵）を用いて対応する署名鍵を検索し、復号されたＡＣ信号を対応する署名鍵と関連付けて保管する。続いて、ＡＣ信号保管完了通知を鍵管理サーバを経由して端末装置に送信する。尚、保管すべきキーペアが大量になり、オーバーフローするような場合、一部のキーペアを暗号化して耐タンパ装置の外部のデータベースに保管することもできる。
【００３８】
続いて、利用者は、電子証明書を取得するため、端末装置を介して証明書発行サーバ６に認証要求を送信する。このユーザ認証もユーザIDとパスワードの組合せとする。証明書発行サーバから端末装置に認証応答が送信される。
【００３９】
ユーザ認証に成功すると、端末装置は、ユーザID及びキーペアの公開鍵を含む電子証明書発行要求を証明書発行サーバに送信する。証明書発行サーバは、受信した公開鍵及び必要な情報を用いて証明書発行要求（CSR）を作成し、生成した証明書発行要求にデジタル署名を行って電子証明書を生成する。生成された電子証明書は端末装置に送信される。端末装置は、受信した電子証明書を格納する。
【００４０】
図３は、生成された署名鍵を用いて電子署名を行う署名工程を示す。利用者は、端末装置２を介して鍵管理サーバに対してユーザ認証を要求する。ユーザ認証が正常に行われると、鍵管理サーバは端末装置に認証応答を送信する。続いて、利用者は自身のＡＣ信号を入力する。また、端末装置は署名対象である電子文書から署名対象データであるハッシュ値を生成する。続いて、端末装置は、入力されたＡＣ信号及び生成されたハッシュ値を暗号化手段により暗号化する。本例では、暗号化手段は、署名鍵を生成するためのキーペアの公開鍵を暗号鍵として用いる。さらに、端末装置は、署名に用いられる署名鍵を特定する署名鍵識別情報である公開鍵、暗号化されたＡＣ信号及びハッシュ値を含む署名要求を生成する。生成された署名要求は、鍵管理サーバを介して耐タンパ装置に送信する。
【００４１】

耐タンパ装置は、受信した署名要求からＡＣ信号及びハッシュ値を取り出し、これらを復号する。復号は、署名鍵を生成するためのキーペアの秘密鍵を解読鍵として用いる。また、署名鍵識別情報（公開鍵）を用いて署名鍵を検索する。続いて、復号されたＡＣ信号と検索された署名鍵と関連付けて保管されているＡＣ信号との比較検証を行う。検証結果として、復号されたＡＣ信号が保管されているＡＣ信号と一致した場合、復号されたハッシュ値についてデジタル署名を行い電子署名が生成される。電子署名及び公開鍵を含む署名結果は鍵管理サーバを経由して編集サーバに送信する。尚、ＡＣ信号が不一致の場合、エラーとして処理する。

【００４２】

続いて、利用者は、端末装置を介して編集サーバ７に認証要求を送信する。編集サーバから端末装置に認証応答が送信される。ユーザ認証に成功すると、端末装置は、ユーザID、キーペアの公開鍵、電子文書、電子署名、及び電子証明書を編集サーバに送信する。編集サーバは、電子文書を編集し、編集された電子文書に電子署名を埋め込み、署名済み電子文書（署名文書）を作成する。署名済み電子文書は、編集サーバに保管すると共に、必要に応じて端末装置に送信される。

【００４３】

この実施例では、生成された署名鍵を特定するため署名鍵識別情報として署名鍵を形成するためのキーペアの公開鍵を用いるので、公開鍵はキーペア生成後に耐タンパ装置から端末装置に送信される。よって、端末装置は暗号化手段の暗号鍵を容易に取得することができる。この結果、公開鍵暗号通信の暗号化キーを設定する煩雑な作業が不要になり、作業性が大幅に改善される。

【００４４】

次に、認証情報を暗号化するために用いる暗号鍵及び暗号化された認証情報を復号するための解読鍵として、耐タンパ装置に設定された公開鍵暗号通信のための公開鍵及び秘密鍵を用いる実施例について説明する。図４は、この実施例のアルゴリズムを示す。利用者は、事前に耐タンパ装置の公開鍵を入手して、端末装置のプログラムに読み込ませる。この事前の作業により、暗号化手段は、耐タンパ装置に設定されたキーペアの公開鍵を暗号鍵として用いて暗号化することができる。

【００４５】

利用者は端末装置を介して鍵管理サーバに対して認証要求を行う。認証要求は、ユーザIDとパスワードによるユーザ認証とする。ユーザ認証に成功すると、利用者は端末装置から鍵管理サーバに対して署名鍵生成要求を送信する。鍵管理サーバは、返信として端末装置にＡＣ信号入力要求を送信する。

【００４６】

利用者は、ＡＣ信号を想到し、入力装置介して想到したＡＣ信号を入力する。　端末装置は、入力されたＡＣ信号を耐タンパ装置に設定されたキーペアの公開鍵を暗号鍵として用いて暗号化する。端末装置は、ユーザIDと共に暗号化されたＡＣ信号を含む署名鍵生成要求を生成し、鍵管理サーバを経由して耐タンパ装置に送信する。

【００４７】

耐タンパ装置は、署名鍵生成要求の受信に応じて、秘密鍵と公開鍵のキーペアを生成する。生成された秘密鍵は署名鍵となり電子署名に用いられる。さらに、耐タンパ装置は、受信した暗号化ＡＣ信号を自身の秘密鍵を解読鍵として用いて復号する。続いて、生成されたキーペアと復号されたＡＣ信号を対として保管する。

【００４８】

続いて、耐タンパ装置は、生成した公開鍵を含む署名鍵生成完了通知を対応する端末装置に送信する。

【００４９】

署名鍵生成完了通知を受信すると、端末装置は、受信した公開鍵を保存する。

【００５０】

続いて、利用者は、端末装置を介して証明書発行サーバにアクセスし、前述した処理に

基づいて電子証明書を取得する。取得した電子証明書は端末装置に保管する。

【００５１】

署名工程は図３に示すアルゴリズムに基づいて電子署名が形成され、署名済み電子文書が作成される。尚、署名工程において、端末装置から耐タンパ装置に送信される暗号化ＡＣ信号は、耐タンパ装置に設定された公開鍵暗号通信用の公開鍵を用いて暗号化する。また、耐タンパ装置は、受信したＡＣ信号を自身の秘密鍵を解読鍵として用いて復号する。

【００５２】

図５は端末装置の機能構成を示すブロック図である。尚、図５は、図２及び図３に示す実施例の電子署名に係る部分だけを示す。端末装置は、通信手段１０、制御部１１、入力装置１２及び記憶部１３を有する。通信手段１０はネットワークに接続され、鍵管理サーバ等との間でデータの送受信を行う。制御部１１は、認証要求部１４を有し、ユーザIDとパスワードによる認証要求を署名システムの鍵管理サーバ等に送信する。続いて、署名システムにログインし、キーペア生成要求部１５からキーペア生成要求を耐タンパ装置に送信する。耐タンパ装置で生成されたキーペアの公開鍵は通信手段を介して記憶部の公開鍵記憶部１６に格納する。

【００５３】

利用者は、キーボードのような入力装置１２を介してＡＣ信号を端末装置に入力する。入力されたＡＣ信号は制御部の暗号化部１７に供給される。暗号化部１７は、公開鍵記憶部に保存されている公開鍵を暗号鍵として用いてＡＣ信号を暗号化する。暗号化されたＡＣ信号は署名鍵生成要求作成部１８に送られる。署名鍵生成要求作成部１８は、暗号化されたＡＣ信号及び署名鍵識別情報として機能するキーペアの公開鍵を含む署名鍵生成要求を作成し、通信手段を介して耐タンパ装置に送信する。

【００５４】

電子証明書発行要求部１９は、耐タンパ装置から受信した公開鍵を含む電子証明書発行要求を生成し、証明書発行サーバに送信する。作成された電子証明書は、通信手段を介して受信し、電子証明書記憶部２０に格納する。

【００５５】

電子署名の対象である電子文書は、利用者によって入力され、入力された電子文書は電子文書記憶部２１に格納する。

【００５６】

電子署名に際し、利用者は入力装置を介して認証情報を入力する。入力された認証情報は暗号化部２２に送られる。また、署名対象である電子文書は、ハッシュ値生成部２３に供給され、電子文書から署名対象データであるハッシュ値が形成される。生成されたハッシュ値は暗号化部２２に送られる。入力された認証情報及び生成されたハッシュ値は暗号化部２２により暗号化され、署名要求生成部２４に送られる。署名要求は、暗号化された認証情報及びハッシュ値と、署名鍵を特定する署名鍵識別情報とを含む。生成された署名要求は通信手段１０を介して耐タンパ装置に送信される。

【００５７】

耐タンパ装置で作成された電子署名は、電子署名記憶部２５に格納する。端末装置は、電子署名の格納が終わると、電子文書アップロード部２６から電子文書、電子署名、及び電子証明書を編集サーバに送信する。編集サーバは、電子文書を編集し、編集された電子文書に電子署名を埋め込み、署名済み電子文書を作成する。署名済み電子文書は編集サーバの署名済み電子文書記憶部に格納する。

【００５８】

図６は鍵管理サーバの機能構成を示す。鍵管理サーバは、通信手段３０、制御部３１及びユーザ情報データベース３２を有する。制御部は、ユーザ認証処理部３３を有し、端末装置の認証画面に表示された認証情報（ユーザIDとパスワード）を認証し、認証応答を端末装置に送信する。

【００５９】

端末装置から送られるキーペア生成要求、署名鍵生成要求及び署名要求は耐タンパ装置

制御部３４に供給され、指定された処理に対応した指示が耐タンパ装置に送られる。耐タンパ装置で生成されたデータ等の情報は耐タンパ装置制御部を介して端末装置等に送られる。尚、鍵管理サーバと耐タンパ装置は内部バス又は外部バスを介して接続することができる。或いは、ＬＡＮを介して接続することも可能である。

【００６０】

図７は耐タンパ装置の機能構成を示す。耐タンパ装置は管理部４０、処理部４１及び記憶部４２を有する。端末装置や編集サーバから送信された情報信号は鍵管理サーバを経由して管理部４０に入力する。管理部４０は、処理部に設けた各機能部を制御し、入力した情報信号に応じて指定された機能を実行する。キーペア生成要求の受信に応じて、キーペア生成部４３が作動して署名鍵となる秘密鍵と公開鍵とのキーペアを生成する。生成されたキーペアは保管部４４に格納され、公開鍵は管理部を介して端末装置に送信する。

【００６１】

署名鍵生成要求の受信に応じて、ＡＣ信号が取り出され、復号化部４５により秘密鍵を用いて復号する。復号されたＡＣ信号は保管部４４に送られる。保管部は生成されたキーペアとＡＣ信号とを対としてキーペアデータを形成する。このキーペアデータは記憶部４２に設けたキーペアデータ記憶部４６に保存する。

【００６２】

署名要求が入力すると、復号化部４５が作動して署名要求に含まれる暗号化されたＡＣ信号及び署名対象データを復号する。また、署名鍵識別情報を用いて対応する署名鍵が検索される。復号されたＡＣ信号及び検索された署名鍵と一緒に保管されているＡＣ信号は検証部４７に送られ、比較検証が行われる。これらのＡＣ信号が互いに一致した場合署名が許可される。そして、デジタル署名部４８において、対応する署名鍵を用いて署名要求に含まれる署名対象データについてデジタル署名が行われる。

【００６３】

図８は本発明による電子署名システムの変形例を示す図である。本例では、鍵管理サーバ４と証明書発行サーバ６との間及び鍵管理サーバ４と編集サーバ７との間にＶＰＮ接続５０及び５１それぞれ設ける。ＶＰＮ接続を設けることにより、鍵管理サーバと証明書発行サーバは直接相互接続されたものと等価になり、鍵管理サーバと編集サーバも直接相互接続されたものと等価な関係なる。

【００６４】

本例では、署名鍵生成工程において、キーペア生成要求及び認証情報は、端末装置から証明書発行サーバ６及びＶＰＮ接続５０を経由して鍵管理サーバに送信され、耐タンパ装置で生成されたキーペアの公開鍵はＶＰＮ接続５０及び証明書発行サーバ６を経由して端末装置に送信される。また、署名工程において、端末装置は、電子文書からハッシュ値を形成し、生成されたハッシュ値と認証情報を暗号化する。続いて、暗号化された認証情報及びハッシュ値と署名鍵IDとを含む署名要求、並びに電子文書を含む署名情報を生成する。生成された署名情報は編集サーバ７に送信され、編集サーバは署名情報から署名要求を取り出し、署名要求をＶＰＮ接続５１を介して鍵管理サーバに送信する。生成された電子署名はＶＰＮ接続５１を介して編集サーバに送られる。編集サーバは、端末装置から送られた電子文書を編集し、編集された電子文書と鍵管理サーバから送られた電子署名とを用いて署名済み電子文書を作成する。

【００６５】

本例では、端末装置と鍵管理サーバとの間の情報伝送は、証明書発行サーバとＶＰＮ接続を経由するルート、及び編集サーバとＶＰＮ接続を経由するルートを介して行われるので、耐タンパ装置はアタッカーによる攻撃が受けにくくなり、署名鍵及び認証情報に対する防護機能が格段に向上する。

【００６６】

本発明は上述した実施例に限定されず種々の変形や変更が可能である。例えば、署名工程においてチャレンジコードを用いて署名要求の有効性を検証することもできる。すなわち、署名要求に際し、端末装置は耐タンパ装置にチャレンジコードを要求する。生成され

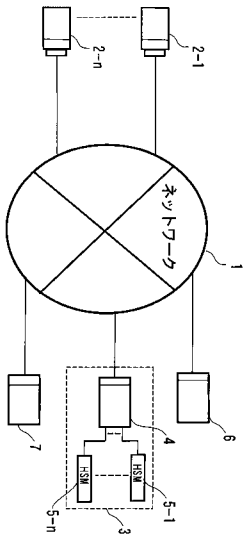
たチャレンジコードは端末装置に送られ、ＡＣ信号と共に暗号化して耐タンパ装置に送信する。耐タンパ装置は、ＡＣ信号と共にチャレンジコードを復号し、保管されているチャレンジコードと比較検証を行う。このようにチャレンジコードについても検証することにより、署名要求自体の有効性を判断することができる。

【符号の説明】

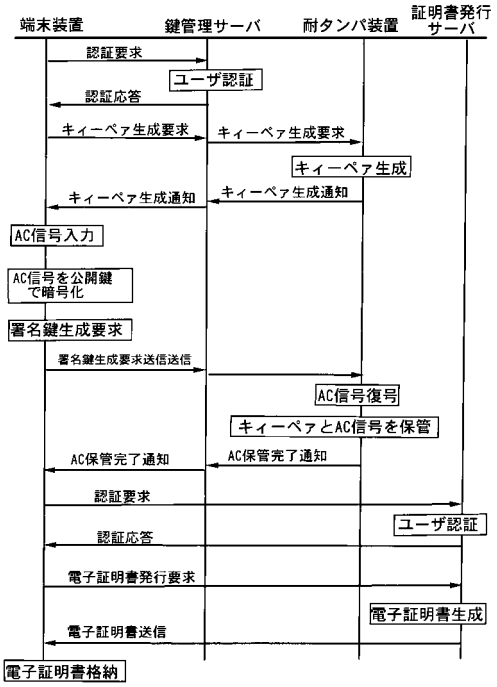
【００６７】

１　ネットワーク
２　端末装置
３　署名システム
４　鍵管理サーバ
５　耐タンパ装置
６　証明書発行サーバ
７　編集サーバ
１０，３０，通信手段
１１，３１，４１　制御部
１２　入力装置
１３，４２　記憶部
４０　管理部
５０，５１　ＶＰＮ接続

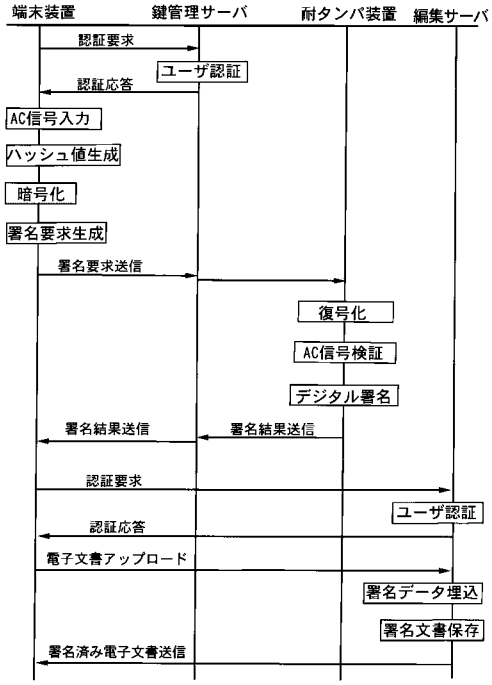
【図１】



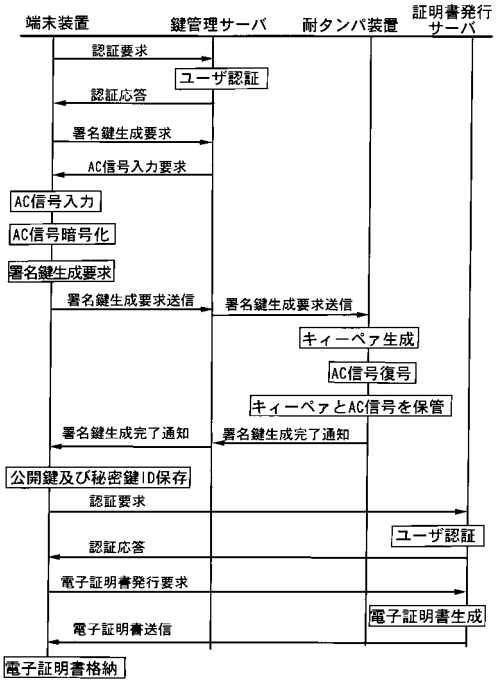
【図２】



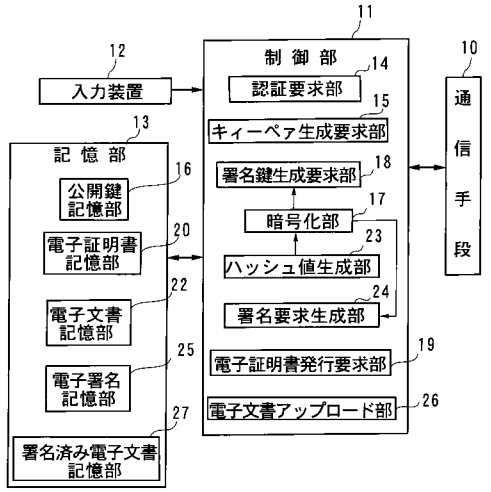
【図３】


端末装置
鍵管理サーバ
耐タンパ装置
編集サーバ
認証要求
ユーザ認証
認証応答
AC信号入力
ハッシュ値生成
暗号化
署名要求生成
署名要求送信
復号化
AC信号検証
デジタル署名
署名結果送信
署名結果送信
認証要求
ユーザ認証
認証応答
電子文書アップロード
署名データ埋込
署名文書保存
署名済み電子文書送信

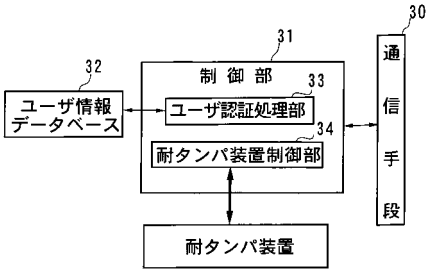
【図４】


端末装置
鍵管理サーバ
耐タンパ装置
証明書発行サーバ
認証要求
ユーザ認証
認証応答
署名鍵生成要求
AC信号入力要求
AC信号入力
AC信号暗号化
署名鍵生成要求
署名鍵生成要求送信
署名鍵生成要求送信
キィーペア生成
AC信号復号
キィーペアとAC信号を保管
署名鍵生成完了通知
署名鍵生成完了通知
公開鍵及び秘密鍵ID保存
認証要求
ユーザ認証
認証応答
電子証明書発行要求
電子証明書生成
電子証明書送信
電子証明書格納

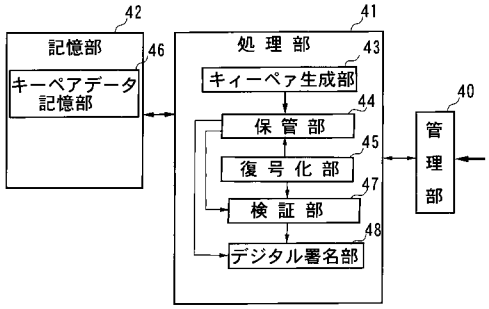
【図５】


11
制御部
12
入力装置
14
認証要求部
15
キィーペア生成要求部
10
通信手段
13
記憶部
16
公開鍵記憶部
18
署名鍵生成要求部
17
暗号化部
20
電子証明書記憶部
23
ハッシュ値生成部
22
電子文書記憶部
24
署名要求生成部
25
電子署名記憶部
19
電子証明書発行要求部
26
電子文書アップロード部
27
署名済み電子文書記憶部

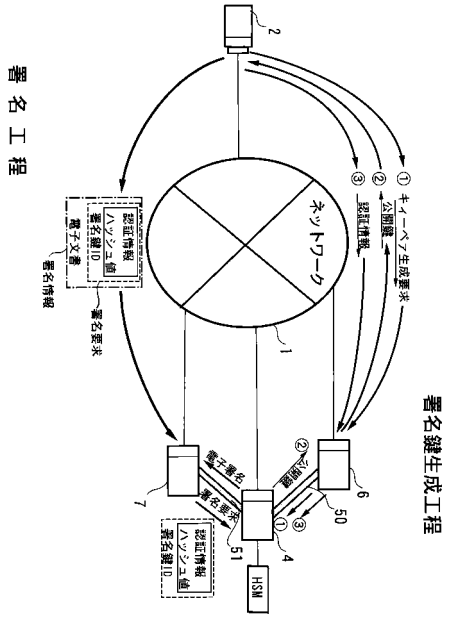
【図６】


30
31
32
制御部
ユーザ情報データベース
33
ユーザ認証処理部
34
耐タンパ装置制御部
通信手段
耐タンパ装置

【図７】


42
記憶部
46
キーペアデータ記憶部
41
処理部
43
キィーペア生成部
44
保管部
45
復号化部
47
検証部
48
デジタル署名部
40
管理部

【図８】


署名工程
署名鍵生成工程
ネットワーク
①キィーペア生成要求
②③認証情報
認証情報
ハッシュ値
署名鍵ID
電子文書
署名情報
署名要求
電子署名
署名要求
HSM
1
2
4
6
7
50
51