

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4892008号
(P4892008)

(45) 発行日 平成24年3月7日(2012.3.7)

(24) 登録日 平成23年12月22日(2011.12.22)

(51) Int.Cl.		F I		
H04L	9/32	(2006.01)	H04L	9/00 675Z
G06F	21/20	(2006.01)	H04L	9/00 673B
			G06F	21/20 144C

請求項の数 20 (全 30 頁)

(21) 出願番号	特願2008-557157 (P2008-557157)	(73) 特許権者	000004226
(86) (22) 出願日	平成20年2月7日(2008.2.7)		日本電信電話株式会社
(86) 国際出願番号	PCT/JP2008/052054		東京都千代田区大手町二丁目3番1号
(87) 国際公開番号	W02008/096825	(74) 代理人	100121706
(87) 国際公開日	平成20年8月14日(2008.8.14)		弁理士 中尾 直樹
審査請求日	平成21年3月18日(2009.3.18)	(74) 代理人	100128705
(31) 優先権主張番号	特願2007-27985 (P2007-27985)		弁理士 中村 幸雄
(32) 優先日	平成19年2月7日(2007.2.7)	(74) 代理人	100147773
(33) 優先権主張国	日本国(JP)		弁理士 義村 宗洋
		(74) 代理人	100066153
			弁理士 草野 卓
		(72) 発明者	唐澤 圭
			東京都千代田区大手町二丁目3番1号 日 本電信電話株式会社内

最終頁に続く

(54) 【発明の名称】 証明書認証方法、証明書発行装置及び認証装置

(57) 【特許請求の範囲】

【請求項1】

第1のネットワークにおいて通信IDを使用して接続可能な端末装置に対し、第2のネットワークにおいて接続を可能にする認証を与える証明書認証方法であって、

(a) 端末装置が、第1のネットワークを介して前記端末装置の通信IDとサブIDを含む証明書発行要求を証明書発行装置に送信するステップと、

(b) 前記証明書発行装置が、前記端末装置から前記第1のネットワークを介して前記証明書発行要求を受信すると、該証明書発行要求に含まれる前記端末装置の通信IDが使用中か否かの確認を通信ID確認装置に要求し、更に前記通信IDと前記サブIDの対応関係が正しいか否かの確認を前記第1のネットワーク上の通信IDーサブID確認装置に要求し、少なくとも前記通信ID確認装置からの確認結果と前記通信IDーサブID確認装置からの確認結果がOKであれば、当該証明書発行装置のID、前記端末装置の通信IDとサブID及び有効期間を少なくとも含む証明書を作成し、前記端末装置へ送信するステップと、

(c) 前記端末装置が、第2のネットワークにおいて前記サブIDを含む認証要求と前記証明書を認証装置に送信するステップと、

(d) 前記認証装置が、前記認証要求に対し認証を与え前記第2のネットワークにおいて前記サブIDを使ってサービスプロバイダに接続可能にするステップ、
とを含む。

【請求項2】

10

20

請求項1記載の証明書認証方法において、

前記ステップ(c)は、

(c-1) 前記認証要求を前記第2のネットワークを介して認証装置へ送信し、

(c-2) 前記認証装置から前記第2のネットワークを介してチャレンジを受信すると、該チャレンジに当該端末装置の秘密鍵を用いてレスポンスを生成するステップと、

(c-3) 前記レスポンスと、前記端末装置の公開鍵と、前記証明書とを前記第2のネットワークを介して前記認証装置へ送信するステップ、

とを含み、

前記ステップ(d)は、

(d-1) 前記認証要求を受信すると、チャレンジを生成して記憶するとともに前記第2ネットワークを介して前記端末装置へ送信するステップと、 10

(d-2) 前記端末装置から前記第2のネットワークを介して前記チャレンジに対するレスポンスと当該端末装置の公開鍵とともに前記証明書を受信するステップと、

(d-3) 該受信したレスポンスを前記端末装置の公開鍵及び前記記憶したチャレンジにより検証し、検証に失敗したときはNGの認証結果を、また、検証に成功し且つ有効期間内であればOKの認証結果を前記第2のネットワークを介して端末装置へ送信するステップ、

とを含む。

【請求項3】

請求項1記載の証明書認証方法において、前記証明書発行装置による前記ステップ(b)は、 20

前記証明書発行要求に含まれている前記通信ID又は前記サブIDに対応する確認結果が前記証明書発行装置内に保存されているか検索するステップと、

保存されていなければ、前記確認要求を前記通信ID確認装置又は前記通信IDーサブID確認装置の一方又は両方に送信して確認結果を求め、得られた確認結果を保存すると共にそれに基づいて前記証明書を生成し、前記証明書発行装置内に保存されている場合は、その保存されている確認結果に基づいて前記証明書を生成するステップ、

とを含む。

【請求項4】

請求項1乃至3のいずれか記載の証明書認証方法において、前記ステップ(b)において、前記証明書発行要求に含まれる前記通信IDが使用中か否かの確認または前記証明書発行要求に含まれる前記通信IDと前記サブIDとが対応関係にあるか否かの確認のいずれか一方もしくは両方をそれぞれ、前記端末装置を介して前記通信ID確認装置または前記通信IDーサブID確認装置のいずれか一方もしくは両方に要求する。 30

【請求項5】

請求項1乃至3のいずれか記載の証明書認証方法において、

前記端末装置による前記ステップ(a)は、第3のネットワークにおける第2通信IDを前記証明書発行要求に含めて前記証明書発行装置に送信するステップであり、

前記証明書発行装置による前記ステップ(b)は、前記第2の通信IDを使って前記証明書を前記第3のネットワークを介して前記端末装置へ送信するステップである。 40

【請求項6】

請求項1記載の証明書認証方法において、前記認証装置による前記ステップ(d-3)は、前記レスポンスの検証に成功し且つ前記有効期間内であれば、さらに前記通信ID確認装置または前記通信IDーサブID確認装置のいずれか一方もしくは両方に前記通信IDまたは前記通信IDと前記サブIDとの関係の確認を要求し、確認結果がOKであれば、OKの認証結果を前記第2のネットワークを介して前記端末装置へ送信するステップである。

【請求項7】

請求項1または6記載の証明書認証方法において、端末装置の証明書失効要求に応じて前記証明書発行装置が生成した端末装置の通信ID又はサブIDに対応して証明書の失効 50

情報を保存する失効情報記憶装置が設けられており、前記方法は更に、

(e) 前記証明書発行装置が、前記端末装置から前記第1のネットワークを介して前記通信IDを少なくとも含む証明書失効要求を受信すると、前記証明書失効要求に含まれる前記通信IDが使用中であるか否かの確認を前記通信ID確認装置に要求し、前記通信ID確認装置からの確認結果がOKであれば、前記通信IDを少なくとも含む証明書の失効情報を生成し、前記失効情報記憶装置に保存するステップを含む。

【請求項8】

請求項7記載の証明書認証方法において、前記認証装置による前記ステップ(d-3)は、前記証明書に含まれる前記通信ID及びサブIDの一方に対応する証明書の失効情報が前記失効情報記憶装置に保存されているか否かを確認するステップを含み、保存されていない
10

【請求項9】

請求項1乃至3いずれか記載の証明書認証方法において、

前記端末装置は発行された複数の証明書を所有しており、前記ステップ(c)は、発行された複数の証明書から、それらの利用履歴や用途に応じて証明書を選択して前記認証装置へ送信するステップを含む。

【請求項10】

請求項1乃至3いずれか記載の証明書認証方法において、前記ステップ(b)は、前記通信IDーサブID確認装置により、所定のサブIDと前記第1のネットワークにおける所定の通信IDとが対応関係にあるか否かを、前記端末装置と前記第1のネットワークとの間に設置された通信IDーサブID変換装置と連携して確認するステップを含む。
20

【請求項11】

請求項1乃至3いずれか記載の証明書認証方法において、通信IDへの料金の請求確認に応じて端末装置に対する課金確認を行い、所定の通信IDへの料金の請求に応じて与信確認を行う通信ID課金装置が設けられており、

前記証明書発行装置による前記ステップ(b)は、前記証明書発行要求に含まれる通信IDが使用中か否かの確認及び通信IDとサブIDとが対応関係にあるか否かの確認後、前記証明書発行要求に含まれる通信IDへの証明書の発行に伴う料金の請求確認及び請求を前記通信ID課金装置に要求し、前記通信ID課金装置からの応答が共にOKであれば前記証明書を生成する。
30

【請求項12】

請求項10記載の証明書認証方法において、証明書の認証に伴う料金の請求確認及び請求を、当該証明書に含まれる通信IDに関わる前記第1のネットワークの前記通信ID課金装置へ転送し、その応答を受信するローミング課金装置が設けられており、

前記認証装置による前記ステップ(d)は、

前記端末装置の前記証明書及び有効期間を確認した後、前記証明書に含まれる前記通信IDへの証明書の認証に伴う料金の請求確認及び請求を前記ローミング課金装置に要求するステップを含み、前記ローミング課金装置からの応答が共にOKであることを、OKの認証結果を前記端末装置へ送信することを必要条件とする。

【請求項13】

第1のネットワークにおいて通信IDを使用して接続可能な端末装置に対し、第2のネットワークにおいて接続を可能にするための証明書を発行する証明書発行装置であって、

前記端末装置から前記第1のネットワークを介して前記端末装置の通信IDとサブIDを含む証明書発行要求を受信すると、該証明書発行要求に含まれる前記端末装置の通信IDが使用中か否かの確認を上記第1のネットワーク上の通信ID確認装置に要求する通信ID確認要求手段と、

前記通信IDと前記サブIDの対応関係が正しいか否かの確認を前記第1のネットワーク上の通信IDーサブID確認装置に要求する通信IDーサブID確認要求手段と、

少なくとも前記通信ID確認装置からの確認結果と前記通信IDーサブID確認装置からの確認結果がOKであれば、当該証明書発行装置のID、前記端末装置の通信IDとサ
50

ブ I D 及び有効期間を少なくとも含む証明書を生成して前記端末装置へ送信し、前記端末装置が前記第 2 のネットワークにおいて前記サブ I D を使ってサービスプロバイダに接続を可能にする証明書生成手段、
とを含む。

【請求項 1 4】

請求項 1 3 記載の証明書発行装置は、さらに通信 I D 又はサブ I D に対応する確認結果を保存する記憶手段を更に含み、前記証明書生成手段は、前記証明書発行要求に含まれる前記通信 I D 又はサブ I D に対応する確認結果が前記記憶手段に保存されているか検索し、保存されていない場合は、前記確認要求を前記通信 I D 確認装置又は前記通信 I D－サブ I D 確認装置の一方又は両方に送信して確認結果を求め、得られた確認結果を保存すると共にそれに基づいて前記証明書を生成し、前記証明書発行装置内に保存されている場合は、その保存されている確認結果に基づいて前記証明書を生成するように構成されている。

10

【請求項 1 5】

請求項 1 3 または 1 4 記載の証明書発行装置において、更に、前記端末装置から前記第 1 のネットワークを介して前記通信 I D を少なくとも含む証明書失効要求を受信すると、前記通信 I D 確認要求手段は前記証明書失効要求に含まれる前記通信 I D が使用中であるか否かの確認を前記通信 I D 確認装置に要求し、前記通信 I D 確認装置からの確認結果が OK であれば、前記通信 I D を少なくとも含む証明書の失効情報を生成し、予め決めた第 3 のネットワーク上の失効情報記憶装置に送信保存する証明書失効情報生成手段を含む。

【請求項 1 6】

20

請求項 1 3 乃至 1 5 いずれか記載の証明書発行装置において、

前記証明書生成手段は、前記証明書発行要求に含まれる通信 I D が使用中か否かの確認及び通信 I D とサブ I D とが対応関係にあるか否かの確認後、前記証明書発行要求に含まれる通信 I D への証明書の発行に伴う料金の請求確認及び請求を予め決めた第 4 のネットワーク上の通信 I D 課金装置に要求し、前記通信 I D 課金装置からの応答が共に OK であれば前記証明書を生成するように構成されている。

【請求項 1 7】

第 1 のネットワークにおいて通信 I D を使用して接続可能な端末装置に対し、第 2 のネットワークにおいて接続を可能にするための認証を与える認証装置であって、
記憶手段と、

30

端末装置からサブ I D を含む認証要求と第 1 のネットワークにおいて証明書発行装置が前記端末に対し発行した証明書を受信すると、チャレンジを生成し、前記記憶手段に保存すると共に前記端末装置に前記第 2 のネットワークを介して送信するチャレンジ生成手段と、

前記端末装置から前記第 2 のネットワークを介して前記チャレンジに対するレスポンスと当該端末装置の公開鍵と有効期間付きの証明書とを受信し、該レスポンスを前記端末装置の公開鍵及び前記記憶手段に保存したチャレンジを使って検証するレスポンス検証手段と、

前記証明書の有効期間内であるか判定する有効期間判定手段、
とを含み、前記検証に成功し、かつ有効期間内と判定された場合に OK の認証結果を前記第 2 のネットワークを介して前記端末装置へ送信し、前記端末装置が前記第 2 のネットワークにおいて前記サブ I D を使ってサービスプロバイダに接続を可能にするように構成されている。

40

【請求項 1 8】

請求項 1 7 記載の認証装置において、前記レスポンスの検証に成功し且つ前記有効期間内であれば、さらに予め決めた第 3 のネットワーク上の通信 I D 確認装置または通信 I D－サブ I D 確認装置のいずれか一方もしくは両方に前記通信 I D または前記通信 I D と前記サブ I D との関係の確認を要求し、確認結果が OK であれば、OK の認証結果を前記第 2 のネットワークを介して前記端末装置へ送信するように構成されている。

【請求項 1 9】

50

請求項 17 記載の認証装置において、更に、前記証明書に含まれる前記通信 ID 及びサブ ID の一方に対応する証明書の失効情報が予め決めた第 4 のネットワーク上の失効情報記憶装置に保存されているか否かを確認する失効情報確認手段を含み、保存されていないれば、OK の認証結果を前記端末装置へ送信することを必要条件とする。

【請求項 20】

請求項 17 記載の認証装置において、前記証明書に含まれる前記通信 ID への証明書の認証に伴う料金の請求確認及び請求を予め決めた第 5 のネットワーク上のローミング課金装置に要求し、前記ローミング課金装置からの応答が共に OK であることを、OK の認証結果を前記端末装置へ送信する更に 1 つの必要条件とする。

【発明の詳細な説明】

10

【技術分野】

【0001】

本発明は、異なるネットワークでサービスを受けるために発行された証明書を認証する証明書認証方法、証明書発行装置及び認証装置に関する。

【背景技術】

【0002】

通信サービスを簡単かつ安全に提供するために、端末の通信 ID を利用して認証を行う通信サービスが普及している。端末は、加入している通信サービスの宛先と、サービスを利用するためのユーザ ID・パスワードなどの認証情報を保持しており、安全に複数の通信サービスを利用することを可能にしている。しかし、端末の移動先で通信サービスを利用するなど、異なるアクセス NW を介して接続する場合には、元々利用していた通信 ID が利用できず、サービスを受けられなくなるという問題がある。また、元の通信 ID とは異なるサブ ID を利用して通信を行う場合も同様に、サービスを受けられなくなるという問題がある。

20

【0003】

〔従来技術〕

この課題を解決するため、信頼できるアクセス NW における端末の認証結果を利用して、端末が別の NW サービスを利用する際に、以前の認証結果を利用する技術が存在している。シングルサインオン技術は、アサーションを用いて認証結果を転送し、一度の認証だけで、複数の通信サービスを利用可能にしている。しかし、アサーションはオンラインでのみ使用できるため、元々利用していた通信 ID が利用できない場合や、元の通信 ID とは異なるサブ ID を利用して通信を行う場合には、サービスを受けられなくなるという問題が残る。

30

【0004】

また、証明書発行を行うことにより、通信サービスからの認証結果を証明書に保存する方法も提案されている。特許文献 1 は、IP v 6 ネットワークにおける NW サービス認証装置である IP v 6 ルータが端末を認証し、NW サービス認証装置に接続された認証局が認証結果を証明するデジタル証明書を NW アクセス端末に発行することによって、新たに IP v 4 ネットワークのサービス認証を受ける際に、NW アクセス端末がデジタル証明書を利用して自動的に認証を受けられるようにするものである。但し、この提案では、NW サービス認証装置とデジタル証明書発行装置が直接接続されている必要があり、別の NW サービス認証装置もデジタル証明書発行装置と安全な通信路で直接通信できる必要がある。しかし、NW サービス認証装置、デジタル証明書発行装置、別の NW サービス認証装置は別々に管理されることがあり、その場合、直接接続することや直接通信することは難しい。

40

【特許文献 1】特開 2006-25010 号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

この発明の目的は、通信 ID を使って第 1 のネットワークで通信サービスへ接続可能で

50

ある端末装置が第2のネットワークにおいても接続可能とできる証明書認証方法、証明書発行装置及び認証装置を提供することである。

【課題を解決するための手段】

【0006】

この発明の第1の観点によれば、第1のネットワークにおいて通信IDを使用して接続可能な端末装置に対し、第2のネットワークにおいて接続を可能にする認証を与える証明書認証方法は、

(a) 端末装置が、第1のネットワークを介して前記端末装置の通信IDとサブIDを含む証明書発行要求を証明書発行装置に送信するステップと、

(b) 前記証明書発行装置が、前記端末装置から前記第1のネットワークを介して前記証明書発行要求を受信すると、該証明書発行要求に含まれる前記端末装置の通信IDが使用中か否かの確認を通信ID確認装置に要求し、更に前記通信IDと前記サブIDの対応関係が正しいか否かの確認を前記第1のネットワーク上の通信ID－サブID確認装置に要求し、少なくとも前記通信ID確認装置からの確認結果と前記通信ID－サブID確認装置からの確認結果がOKであれば、当該証明書発行装置のID、前記端末装置の通信IDとサブID及び有効期間を少なくとも含む証明書を生成し、前記端末装置へ送信するステップと、

(c) 前記端末装置が、第2のネットワークにおいて前記サブIDを含む認証要求と前記証明書を認証装置に送信するステップと、

(d) 前記認証装置が、前記認証要求に対し認証を与え前記第2のネットワークにおいて前記サブIDを使ってサービスプロバイダに接続可能にするステップ、
とを含む。

【0007】

この発明の第2の観点によれば、第1のネットワークにおいて通信IDを使用して接続可能な端末装置に対し、第2のネットワークにおいて接続を可能にするための証明書を発行する証明書発行装置は、

前記端末装置から前記第1のネットワークを介して前記端末装置の通信IDとサブIDを含む証明書発行要求を受信すると、該証明書発行要求に含まれる前記端末装置の通信IDが使用中か否かの確認を上記第1のネットワーク上の通信ID確認装置に要求する通信ID確認要求手段と、

前記通信IDと前記サブIDの対応関係が正しいか否かの確認を前記第1のネットワーク上の通信ID－サブID確認装置に要求する通信ID－サブID確認要求手段と、

少なくとも前記通信ID確認装置からの確認結果と前記通信ID－サブID確認装置からの確認結果がOKであれば、当該証明書発行装置のID、前記端末装置の通信IDとサブID及び有効期間を少なくとも含む証明書を生成して前記端末装置へ送信し、前記端末装置が前記第2のネットワークにおいて前記サブIDを使ってサービスプロバイダに接続を可能にする証明書生成手段、
とを含むように構成される。

【0008】

この発明の第3の観点によれば、第1のネットワークにおいて通信IDを使用して接続可能な端末装置に対し、第2のネットワークにおいて接続を可能にするための認証を与える認証装置は、

記憶手段と、

端末装置からサブIDを含む認証要求と第1のネットワークにおいて証明書発行装置が前記端末装置に対し発行した証明書を受信すると、チャレンジを生成し、前記記憶手段に保存すると共に前記端末装置に前記第2のネットワークを介して送信するチャレンジ生成手段と、

前記端末装置から前記第2のネットワークを介して前記チャレンジに対するレスポンスと当該端末装置の公開鍵と有効期間付きの証明書とを受信し、該レスポンスを前記端末装置の公開鍵及び前記記憶手段に保存したチャレンジを使って検証するレスポンス検証手段

10

20

30

40

50

と、

前記証明書の有効期間内であるか判定する有効期間判定手段、
とを含み、前記検証に成功し、かつ有効期間内と判定された場合にOKの認証結果を前記第2のネットワークを介して前記端末装置へ送信し、前記端末装置が前記第2のネットワークにおいて前記サブIDを使ってサービスプロバイダに接続を可能にするように構成されている。

【0009】

この発明によれば、有効期間を指定された証明書を発行／利用する技術により、証明書の有効性確認を不要にできるため、通信サービスへ接続できない場合でも、認証手段が利用できるようになる。使い捨てられる証明書を発行する技術とは、a. 証明書のオンライン発行によって実現される短い有効期間を持つ証明書の発行技術と、b. 証明書の短い有効期間だけシステム側で利用履歴を保存することにより、認証回数を制限できる証明書利用技術の組合せで実現されるものである。

電話番号のように広いサービス提供者の管理する通信IDに加えて、子番号のように一つの組織が独自に管理するサブIDを連携させる際に、通信ID管理手段とサブID管理手段を連携させて認証する技術である。具体例として、電話番号を管理する通信網側機能と子番号を管理する構内側機能とが連携する場合は、構内機能と通信網機能の間で連携IDを使って状態を交換することによって、連携が実現される。また、グローバルIPアドレスを管理するISP側機能とプライベートIPアドレスを管理する宅内機能とが連携する場合は、グローバルIPアドレスとプライベートIPアドレスの変換を行うNAT機能とDHCP機能の状態を得ることによって、連携が実現される。

【発明の効果】

【0010】

本発明によれば、NWサービス中継装置が持つ情報をNWアクセス端末が使えない場合でも、NWサービス中継装置が持つ情報が利用できることをデジタル証明書として第三者機関が発行することによって、NWアクセス端末が別のNWサービスの認証を受けられるようにできる。

また、NWサービス認証装置、デジタル証明書発行装置、別のNWサービス認証装置は別々に管理されている場合でも、NWアクセス端末が通信を仲介することにより、デジタル証明書を取得でき、NWアクセス端末が別のNWサービスの認証を受けられるようにできる。

【図面の簡単な説明】

【0011】

【図1】本発明の第1の実施例に係る証明書発行システムの構成を示すブロック図。

【図2】図2Aは証明書発行装置の機能構成例を示すブロック図であり、図2Bは証明書の例を説明するための図であり、図2Cは認証装置の機能構成を示すブロック図。

【図3】本発明の第1の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すシーケンス図。

【図4】本発明の第1の実施例に係る証明書発行システムにおける証明書認証処理の主要な流れを示すシーケンス図。

【図5】本発明の第2の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すシーケンス図。

【図6】本発明の第3の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すシーケンス図。

【図7】本発明の第4の実施例に係る証明書発行システムの構成を示すブロック図。

【図8】本発明の第4の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すシーケンス図。

【図9】本発明の第5の実施例に係る証明書発行システムの構成を示すブロック図。

【図10】本発明の第5の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すシーケンス図。

【図 1 1】本発明の第 6 の実施例に係る証明書発行システムの構成を示すブロック図。

【図 1 2】本発明の第 6 の実施例に係る証明書発行システムにおける証明書認証処理の主要な流れを示すシーケンス図。

【図 1 3】本発明の第 7 の実施例に係る証明書発行システムの構成を示すブロック図。

【図 1 4】本発明の第 7 の実施例に係る証明書発行システムにおける証明書失効処理の主要な流れを示すシーケンス図。

【図 1 5】本発明の第 7 の実施例に係る証明書発行システムにおける証明書認証処理の主要な流れを示すシーケンス図。

【図 1 6】本発明の第 8 の実施例に係る証明書発行システムの構成を示すブロック図。

【図 1 7】本発明の第 9 の実施例に係る証明書発行システムの構成を示すブロック図。

10

【図 1 8】本発明の第 10 の実施例に係る証明書発行システムの構成を示すブロック図。

【図 1 9】本発明の第 10 の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すシーケンス図。

【図 2 0】本発明の第 10 の実施例に係る証明書発行システムにおける他の証明書発行処理の主要な流れを示すシーケンス図。

【図 2 1】本発明の第 10 の実施例に係る証明書発行システムにおける更に他の証明書発行処理の主要な流れを示すシーケンス図。

【図 2 2】本発明の第 11 の実施例に係る証明書発行システムの構成を示すブロック図。

【図 2 3】本発明の第 11 の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すシーケンス図。

20

【図 2 4】本発明の第 12 の実施例に係る証明書発行システムの構成を示すブロック図。

【図 2 5】本発明の第 12 の実施例に係る証明書発行システムにおける証明書発行認証の主要な流れを示すシーケンス図。

【発明を実施する為の最良の形態】

【0012】

以下、本発明の実施例について、図面を参照して説明する。

<第 1 の実施例>

図 1 は本発明の第 1 の実施例に係る証明書発行システムの構成を示すもので、図中、NW 1, NW 2 はそれぞれ通信ネットワーク、4 は端末装置、5 は通信 ID 確認装置、6 は通信 ID サブ ID 確認装置、7 は証明書発行装置、8 は認証装置である。図 1 の例では通信 ID 確認装置 5 と通信 ID サブ ID 確認装置 6 はそれぞれ直接証明書発行装置 7 に接続されている場合を示しているが、いずれか一方、又は両方ともネットワーク NW 1 を介して接続可能とする構成でもよい。

30

【0013】

ネットワーク NW 1, NW 2 (以下単に NW 1 あるいは NW 2 と記す) は、公衆電話網やインターネット等の広域通信網であり、NW 1 及び NW 2 は同一の通信 ID を使用できない異なる通信ネットワークであるとする。ここで、証明書発行装置 7 は NW 1 に接続され、認証装置 8 は NW 2 に接続されるが、端末装置 4 は NW 1, NW 2 のいずれにも接続して使用可能であるとする。

端末装置 4 は、特定のネットワーク、ここでは NW 1 に接続された装置と該 NW 1 における通信 ID とは異なるサブ ID を用いて通信可能とされている。具体的には、端末装置 4 は図示しない PBX や HGW 等を介して NW 1 に接続された電話機やパーソナルコンピュータであり、通信 ID 記憶部 4 1 と、証明書記憶部 4 2 と、証明書発行要求部 4 3 と、認証要求部 4 4 とを備えている。

40

【0014】

通信 ID 記憶部 4 1 は、NW 1 における通信 ID (例えば、グローバル IP アドレス) を記憶する。証明書記憶部 4 2 は、証明書発行装置 7 が発行する証明書や当該端末装置 4 における公開鍵と秘密鍵の鍵ペアを保存する。

証明書発行要求部 4 3 は、通信 ID 記憶部 4 1 から通信 ID を読み出し、該通信 ID とともに (別途記憶された) サブ ID (例えば、プライベート IP アドレス) を少なくとも

50

含む証明書発行要求をNW 1を介して証明書発行装置7へ送信し、証明書発行装置7からNW 1を介して送信されてきた証明書を受信し、当該証明書を証明書記憶部42に保存する。

【0015】

認証要求部44は、サブIDを少なくとも含む認証要求をNW 2を介して認証装置8へ送信し、認証装置8からNW 2を介してチャレンジを受信すると、前記認証要求が初めて（1回目）であるかを判定する。初めてであれば、該チャレンジに当該端末装置4の秘密鍵を用いてレスポンスを生成するとともに証明書記憶部42から証明書を読み出し、当該証明書と、当該端末装置4の公開鍵と、前記レスポンスとをNW 2を介して認証装置8へ送信する。また、前記認証要求が2回目以降であれば、前記チャレンジに当該端末装置4の秘密鍵を用いてレスポンスを生成し、これを当該端末装置4の公開鍵とともにNW 2を介して認証装置8へ送信し、認証装置8からNW 2を介して送信されてきた認証結果を受信する。

10

【0016】

通信ID確認装置5は、NW 1における所定の通信IDが使用中か否かを確認、具体的にはNW 1上の図示していない交換局やISP (Internet Service Provider)と連携して確認する。この確認は外部からの要求、例えば証明書発行装置7からの要求に応じて実行され、通信IDが使用中であればOK、そうでなければNGの確認結果を返す。

通信ID－サブID確認装置6は、所定のサブIDとNW 1における所定の通信IDとが対応関係にあるか否かを確認する。この確認は外部からの要求、例えば証明書発行装置7からの要求に応じて実行され、対応関係にあればOK、そうでなければNGの確認結果を返す。

20

【0017】

図2Aに示すように、証明書発行装置7は、通信ID確認要求部7Aと、通信ID－サブID確認要求部7Bと、証明書生成部7Cと、記憶部7Dと、制御部7Eとから構成されている。端末装置4からNW 1を介してサブID及び通信IDを少なくとも含む証明書発行要求を受信すると、通信ID確認要求部7Aは該証明書発行要求に含まれる通信IDが使用中か否かを確認を通信ID確認装置5に要求する。また、通信ID－サブID確認要求部7Bは前記証明書発行要求に含まれる通信IDとサブIDとが対応関係にあるか否かを確認を通信ID－サブID確認装置6に要求する。

30

【0018】

通信ID確認装置5及び通信ID－サブID確認装置6からの確認結果が共にOKであれば、証明書生成部7Cは端末装置4の通信ID、サブID、当該証明書発行装置のID、及び有効期間（通常、例えば1～2日程度と短く設定）を少なくとも含む図2Bに示すような証明書CTFを生成し、NW 1を介して端末装置4へ送信する。いずれかがNGであればNW 1を介して端末装置4へ発行拒否を通知する。

記憶部7Dには端末装置との通信に必要な情報、証明書生成に必要な情報などを予め保存し、あるいは証明書発行処理に使われる情報を必要に応じて保存する。制御部7Eは証明書発行装置7と他の装置（端末装置4、通信ID確認装置5、通信ID－サブID確認装置6）との間の通信を制御実行し、また、通信ID確認要求部7A、通信ID－サブID確認要求部7B、証明書生成部7C、記憶部7Dによる処理を制御する。

40

【0019】

認証装置8は、図2Cに示すようにチャレンジ生成部8Aと、記憶部8Bと、レスポンス検証部8Cと、有効期間判定部8Dと、制御部8Eとから構成されている。端末装置4から他のネットワーク、ここではNW 2を介して例えばサブIDを少なくとも含む認証要求を受信すると、チャレンジ生成部8Aは例えば認証手順に用いられる周知のチャレンジ&レスポンス方式に基づくチャレンジを生成して記憶部8Bに記憶するとともに、NW 2を介して端末装置4へ送信する。

認証装置8は端末装置4からNW 2を介して前記チャレンジに対するレスポンス及び当該端末装置4の公開鍵と共に証明書CTFを受信し、これらを記憶部8Bに記憶する。さ

50

らに、該受信したレスポンスをレスポンス検証部 8 C により、端末装置 4 の公開鍵及び前記記憶したチャレンジを使って検証する。検証に成功した場合は、有効期間判定部 8 D により受信日時が前記記憶した証明書 C T F 中の有効期間内であるか判定する。期間内であれば証明書 C T F に対する認証結果として O K を NW 2 を介して端末装置 4 へ送信する。レスポンスの検証に失敗したときは N G の認証結果を端末装置 4 へ送信する。

【0020】

認証装置 8 が O K の認証結果を端末装置 4 に送信した場合、このシステムにおいて端末装置 4 はサブ I D を使って認証装置を経由して NW 2 上の図示してない所望のサービス提供サーバに接続することができる。端末装置 4 が NW 2 上の所望のサービス提供サーバに直接接続する場合は、例えば認証装置 8 が端末装置 4 に認証結果 O K と共に認証装置 8 のデジタル署名を送信し、端末装置 4 はサブ I D を使って所望のサービス提供サーバに接続するときにそのデジタル署名を提示するようにしても良い。このようにして端末装置 4 は NW 2 上でサブ I D を使って所望のサービス提供サーバに接続することが可能となる。

10

【0021】

制御部 8 E は、他の装置（ここでは端末装置 4）との通信を制御実行し、また、チャレンジ生成部 8 A、記憶部 8 B、レスポンス検証部 8 C、有効期間判定部 8 D の処理を制御する。

なお、本実施例においては、NW 1 には 1 つの端末装置 4 が接続されているが、本発明の証明書発行システムに接続できる端末装置の数を限定するものではない。

20

以上のように構成された本発明の第 1 の実施例に係る証明書発行システムの動作について、図面を参照して説明する。

【0022】

図 3 は本発明の第 1 の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

まず、端末装置 4 はその証明書発行要求部 4 3 により、通信 I D 記憶部 4 1 から通信 I D を読み出し、該通信 I D とともにサブ I D を少なくとも含む証明書発行要求を NW 1 を介して証明書発行装置 7 へ送信する（ステップ S 1）。

証明書発行装置 7 は、端末装置 4 から NW 1 を介して証明書発行要求を受信すると、該証明書発行要求に含まれる通信 I D が使用中か否かの確認を通信 I D 確認装置 5 に要求する（ステップ S 2）。

30

【0023】

通信 I D 確認装置 5 は、証明書発行装置 7 からの確認要求に応じて、前記証明書発行要求に含まれる通信 I D が NW 1 で使用中であるか否かを NW 1 と連携して確認し、使用中であれば O K の確認結果を、使用中でなければ N G の確認結果を証明書発行装置 7 に応答する（ステップ S 3）。NW 1 と連帯して通信 I D の確認を行なうには、例えば NW 1 上にある図示してない交換局や I S P のような通信管理装置が通信網機能の 1 つとして通信 I D を管理し、通信 I D 確認装置 5 はこの通信管理装置から通信 I D が使用中であるか否かの情報を取得する。

40

【0024】

次に、証明書発行装置 7 は、通信 I D 確認装置 5 からの確認結果を受信し、前記証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かの確認を通信 I D ーサブ I D 確認装置 6 に要求する（ステップ S 4）。

通信 I D ーサブ I D 確認装置 6 は、証明書発行装置 7 からの確認要求に応じて、前記証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かを確認し、対応関係にあれば O K の確認結果を、対応関係になれば N G の確認結果を証明書発行装置 7 に応答する（ステップ S 5）。

【0025】

証明書発行装置 7 は、通信 I D ーサブ I D 確認装置 6 からの確認結果を受信し、前記通信 I D 確認装置 5 からの確認結果と共に O K であれば、当該証明書発行装置 7 の I D、前

50

記端末装置４の通信ＩＤ及びサブＩＤ、有効期間を少なくとも含む証明書ＣＴＦを生成し、NW１を介して端末装置４へ送信する。また、確認結果のいずれか一方がNGであれば、NW１を介して端末装置４へ発行拒否を通知する（ステップＳ６）。

端末装置４はその証明書発行要求部４３により、証明書発行装置７からNW１を介して送信されてきた証明書ＣＴＦを受信し（ステップＳ７）、該受信した証明書ＣＴＦを証明書記憶部４２に保存する。また、発行拒否が通知された場合は処理を終了する（ステップＳ８）。

【００２６】

図４は本発明の第１の実施例に係る証明書発行システムにおける証明書認証処理の主要な流れを示すもので、以下、動作を詳細に説明する。

まず、端末装置４はその認証要求部４４により、サブＩＤを少なくとも含む認証要求をNW２を介して認証装置８へ送信する（ステップＳ１１）。

次に、認証装置８は、端末装置４からNW２を介して認証要求を受信すると、チャレンジを生成して記憶部８Ｂに記憶するとともにNW２を介して端末装置４へ送信する（ステップＳ１２）。

【００２７】

端末装置４はその認証要求部４４により、認証装置８からNW２を介してチャレンジを受信すると、該チャレンジに当該端末装置４の秘密鍵を用いてレスポンスを生成し（ステップＳ１３）、前記認証要求が初めて（１回目）であるか判定し（ステップＳ１４）、初めてであれば証明書記憶部４２から証明書ＣＴＦを読み出し（ステップＳ１５）、当該証明書ＣＴＦと、当該端末装置４の公開鍵と、前記レスポンスとをNW２を介して認証装置８へ送信し（ステップＳ１６）、前記認証要求が２回目以降であれば、前記チャレンジに対するレスポンスを当該端末装置４の公開鍵とともにNW２を介して認証装置８へ送信する（ステップＳ１６）。即ち、２回目以降の認証要求の場合は、証明書の送信を省略する。

【００２８】

認証装置８は、端末装置４からNW２を介して前記チャレンジに対するレスポンス及び当該端末装置４の公開鍵、もしくはこれらとともに証明書を受信する。受信情報に証明書ＣＴＦが含まれている場合は、これを記憶部８Ｂに記憶し、レスポンス検証部８Ｃにより該受信したレスポンスを端末装置４の公開鍵及び記憶部８Ｂから読み出したチャレンジを使って検証する（ステップＳ１７）。検証に成功したか判定し、検証に失敗したときはNGの認証結果をNW２を介して端末装置４に送信する（ステップＳ１８）。また、検証に成功した場合は前記記憶した証明書ＣＴＦ中の有効期間が満了しているか判定し、満了していなければOKの認証結果を、満了していればNGの認証結果をNW２を介して端末装置４へ送信する（ステップＳ１９）。

【００２９】

端末装置４からの受信情報に証明書が含まれていない場合は、同じ端末装置４による２回目以降の認証要求であることを示しており、従って、ステップＳ１９において記憶部８Ｂに記憶されている１回目の認証時の証明書ＣＴＦをサブＩＤ（又は通信ＩＤ）により検索し、読み出した証明書ＣＴＦの有効期間をチェックする。

端末装置はその認証要求部４４により、認証装置８からNW２を介して認証結果を受信する。

この実施例によれば、NW１を介した端末装置４の証明書発行装置７へのアクセスの確認及び通信ＩＤとサブＩＤとの対応関係の確認のみを根拠とし、本人の確認を必要としない、有効期間の短い証明書を発行する。これにより、証明書発行装置７が接続されたNW１とは異なるNW２に接続された認証装置８でも認証可能とすることで、端末装置４を移動して用いるような、元の通信ＩＤが利用できないような場合であっても、様々なサービスを利用可能とすることができる。

【００３０】

<第２の実施例>

本発明の第2の実施例は、前述した第1の実施例において、証明書発行装置7が、通信ID確認装置5からの確認結果または通信ID－サブID確認装置6からの確認結果のいずれか一方もしくは両方を受信した際に記憶部7Dに保存しておき、2回目以降の証明書発行要求に対して、その通信IDもしくはその通信IDとサブIDを用いて前記保存した確認結果を検索し、その通信IDが使用中か否かの確認結果、もしくはその通信IDとサブIDとが対応関係にあるか否かの確認結果があればこれらを参照して証明書CTFを生成し、端末装置4へ送信する。

【0031】

なお、本実施例に係る証明書発行システムの構成は、前述した証明書発行装置7における処理手順が異なる点を除いて第1の実施例の場合と同様である。

10

図5は本発明の第2の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

証明書発行装置7は、端末装置4からNW1を介して証明書発行要求を受信すると（ステップS1）、該証明書発行要求に含まれる通信IDもしくはその通信IDとサブIDを用いて前記保存した確認結果を検索して確認結果が保存されているか判定する（ステップS2A）。確認結果が保存されていれば、読み出してステップS4Aに移る。確認結果が保存されていなければ確認要求を通信ID確認装置5に送信する（ステップS2B）。通信ID確認装置5から通信IDが使用中か否かの確認結果を受信すると（ステップS3A）、それを記憶部7Dに保存する（ステップS3B）。

【0032】

20

次に通信IDとサブIDとが対応関係にあるか否かの確認結果が保存されているか検索し（ステップS4A）、保存されていれば読み出してステップS6に移る。対応関係が保存されていなければ通信IDとサブIDが対応関係にあるか否かの確認要求を通信ID－サブID確認装置6に要求し（ステップS4B）、その確認結果を受信して（ステップS5A）記憶部7Dに保存する（ステップS5B）。通信IDが使用中であり、かつ通信IDとサブIDの対応関係が正しければ、証明書CTFを生成して端末装置4へ送信する（ステップS6、S7）。

【0033】

なお、証明書認証処理の動作は第1の実施例の場合と同様である。

この実施例によれば、同一の端末装置4からの2回目以降の証明書発行要求に対し、通信ID確認装置5または通信ID－サブID確認装置6のいずれか一方もしくは両方への確認処理が不要となり、より高速に証明書を発行可能となる。

30

【0034】

<第3の実施例>

図1に示したシステムにおいて、例えば通信ID確認装置5および通信ID－サブID確認装置6が端末装置4と同じHGWの内側において互いに接続されている場合、HGWの外のNW1上の証明書発行装置7から直接通信ID確認装置5及び通信ID－サブID確認装置6にアクセスすることはできない。このような場合、本発明の第3の実施例では、前述した第1の実施例において、証明書発行装置7が、証明書発行要求に含まれる通信IDが使用中か否かの確認または証明書発行要求に含まれる通信IDとサブIDとが対応関係にあるか否かの確認のいずれか一方もしくは両方をそれぞれ、端末装置4を介して通信ID確認装置5または通信ID－サブID確認装置6のいずれか一方もしくは両方に要求する。

40

【0035】

なお、本実施例に係る証明書発行システムの構成は、前述した証明書発行装置7における処理手順が異なる点を除いて第1の実施例の場合と同様である。

図6は本発明の第3の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

証明書発行装置7は、端末装置4からNW1を介して証明書発行要求を受信すると（ステップS1）、該証明書発行要求に含まれる通信IDが使用中か否かの確認要求をNW1

50

を介して端末装置 4 へ送信する（ステップ S 2 a）。

【0036】

端末装置 4 は、証明書発行装置 7 から NW 1 を介して送信されてきた証明書発行要求に含まれる通信 I D が使用中か否かの確認要求を受信すると、そのまま通信 I D 確認装置 5 へ送信する（ステップ S 2 b）。

通信 I D 確認装置 5 は、端末装置 4 を介して送信された証明書発行装置 7 からの要求に応じて、前記証明書発行要求に含まれる通信 I D が NW 1 で使用中であるか否かを NW 1 と連携して確認し、使用中であれば OK の確認結果を、使用中でなければ NG の確認結果を証明書発行装置 7 へ送信する（ステップ S 3）。

【0037】

証明書発行装置 7 は、通信 I D 確認装置 5 からの確認結果を受信し、前記証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かの確認要求を NW 1 を介して端末装置 4 へ送信する（ステップ S 4 a）。

また、端末装置 4 は、証明書発行装置 7 から NW 1 を介して送信されてきた証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かの確認要求を受信すると、そのまま通信 I D－サブ I D 確認装置 6 へ送信する（ステップ S 4 b）。

通信 I D－サブ I D 確認装置 6 は、端末装置 4 を介して送信された証明書発行装置 7 からの要求に応じて、前記証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かを確認し、対応関係にあれば OK の確認結果を、対応関係になれば NG の確認結果を証明書発行装置 7 へ送信する（ステップ S 5）。

【0038】

証明書発行装置 7 は、通信 I D 確認装置 5 からの通信 I D が使用中である確認結果及び通信 I D－サブ I D 確認装置 6 からの通信 I D とサブ I D が正しく対応している確認結果に基づいて証明書 C T F を生成し（ステップ S 6）、端末装置 4 へ送信する（ステップ S 7）。

なお、ステップ S 3 及び S 5 はそれぞれ通信 I D 確認装置 5 及び通信 I D－サブ I D 確認装置 6 が証明書発行装置 7 へ直接応答する場合を示したが、破線のステップ S 3' 及び S 5' で示すように端末装置 4 を経由するリダイレクトで応答してもよい。証明書認証処理の動作は第 1 の実施例の場合と同様である。

【0039】

この実施例によれば、証明書発行装置 7 は、通信 I D 確認装置 5 または通信 I D－サブ I D 確認装置 6 のいずれか一方もしくは両方が端末装置 4 と同じ H G W 内にある場合でも証明書発行装置 7 は端末装置 4 を介して確認要求を通信 I D 確認装置 5 及び／又は通信 I D－サブ I D 確認装置 6 に送信することができる。なお、この実施例は第 2 の実施例にも適用可能であることはいうまでもない。

【0040】

<第 4 の実施例>

本発明の第 4 の実施例は、前述した第 1 の実施例において、端末装置 4 からの証明書発行要求に NW 1 側で当該端末装置 4 の通信 I D を付与する。

【0041】

図 7 は本発明の第 4 の実施例に係る証明書発行システムの構成を示すもので、第 1 の実施例のシステムにおいて、端末装置 4 からの証明書発行要求に当該端末装置 4 の通信 I D を付与する通信 I D 付与装置 9 を備えた点が異なる。この通信 I D 付与装置 9 は、通常、この端末装置 4 が収容される図示してない P B X や H G W に設けられる。

また、端末装置 4 は、図 1 に示されている通信 I D 記憶部 4 1 を備えず、通信 I D 記憶装置 9 A が通信 I D 付与装置 9 に接続されている。証明書発行要求部 4 3 は通信 I D を含まず、サブ I D を少なくとも含む証明書発行要求を通信 I D 付与装置 9 を介して証明書発行装置 7 へ送信する。このとき、通信 I D 付与装置 9 は通信 I D 記憶装置 9 A から読み出した通信 I D を証明書発行要求に含めて証明書発行装置 7 へ送信する。端末装置 4 の証明書発行要求部 4 3 は証明書発行装置 7 から NW 1 を介して送信されてきた証明書 C T F を

10

20

30

40

50

受信し、当該証明書 C T F を証明書記憶部 4 2 に保存する。

【0042】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第 1 の実施例の場合と同様である。

図 8 は本発明の第 4 の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

まず、端末装置 4 はその証明書発行要求部 4 3 により、サブ I D を少なくとも含む証明書発行要求を NW 1 を介して証明書発行装置 7 へ送信する。この際、通信 I D 付与装置 9 は、証明書発行要求を受信し、これに通信 I D 記憶装置 9 A から読み出した当該端末装置 4 の通信 I D を付与して証明書発行装置 7 へ送信する。なお、以降の動作、並びに証明書
10 認証処理の動作は第 1 の実施例の場合と同様であり、説明を省略する。

【0043】

この実施例によれば、端末装置 4 は通信 I D を記憶する通信 I D 記憶部 4 1 が不要になる。なお、この実施例は第 2、3 の実施例にも適用可能であることはいうまでもない。

【0044】

<第 5 の実施例>

本発明の第 5 の実施例は、前述した第 1 の実施例において、証明書を NW 1 以外の第 3 の通信ネットワークを利用して端末装置へ送信する。

図 9 は本発明の第 5 の実施例に係る証明書発行システムの構成を示すもので、第 1 の実施例のシステムにおいて、第 3 の通信ネットワーク NW 3、例えば電子メール網を備えて
20 いる。また、端末装置 4 は、通信 I D 記憶部 4 1、証明書記憶部 4 2、認証要求部 4 4 とともに、NW 3 における当該端末装置 4 の通信 I D (通信 I D 3) (例えば、メールアドレス) を記憶する第 2 の通信 I D 記憶部 (通信 I D 3 記憶部) 4 5 を備えている。通信 I D 記憶部 4 1 から通信 I D を読み出すとともに通信 I D 3 記憶部 4 5 から通信 I D 3 を読み出し、該通信 I D 及び通信 I D 3 とともにサブ I D を少なくとも含む証明書発行要求を NW 1 を介して証明書発行装置 7 へ送信する。証明書発行装置 7 から NW 3 を介して送信されてきた証明書 C T F を受信し、当該証明書 C T F を証明書記憶部 4 2 に保存する証明書発行要求部 4 3 を備えている。

【0045】

また、証明書発行装置 7 は、端末装置 4 から NW 1 を介して通信 I D、通信 I D 3 及び
30 サブ I D を少なくとも含む証明書発行要求を受信すると、該証明書発行要求に含まれる通信 I D が使用中か否かの確認を通信 I D 確認装置 5 に要求する。さらに、前記証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かの確認を通信 I D - サブ I D 確認装置 6 に要求する。通信 I D 確認装置 5 及び通信 I D - サブ I D 確認装置 6 からの確認結果が OK であれば、当該証明書発行装置 7 の I D、端末装置 4 のサブ I D 及び有効期間を少なくとも含む証明書を生成し、NW 3 を介して端末装置 4 へ送信する。

【0046】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第 1 の実施例の場合と同様である。

図 10 は本発明の第 5 の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。
40

まず、端末装置 4 はその証明書発行要求部 4 3 により、通信 I D 記憶部 4 1 から通信 I D を読み出し、さらに通信 I D 3 記憶部 4 5 から通信 I D 3 を読み出し、該通信 I D、通信 I D 3 及びサブ I D を少なくとも含む証明書発行要求を NW 1 を介して証明書発行装置 7 へ送信する (ステップ S 1)。

【0047】

証明書発行装置 7 は、端末装置 4 から NW 1 を介して証明書発行要求を受信すると (ステップ S 1)、第 1 の実施例の場合と同様にして該証明書発行要求に含まれる通信 I D が使用中か否かの確認及び通信 I D とサブ I D とが対応関係にあるか否かの確認を行う (ステップ S 2 ~ S 5)。これらの確認結果が共に OK であれば、当該証明書発行装置 7 の I
50

D、前記端末装置4の通信ID及びサブID、有効期間を少なくとも含む証明書CTFを生成し（ステップS6）、NW3を介して端末装置4へ通信ID3を宛先として送信する（ステップS7）。また、確認結果のいずれか一方がNGであれば、NW3を介して端末装置4へ発行拒否を通知する。

【0048】

端末装置4はその証明書発行要求部43により、証明書発行装置7からNW3を介して送信されてきた証明書CTFを受信し、該受信した証明書を証明書記憶部42に保存する。また、発行拒否が通知された場合は処理を終了する（ステップS8）。

なお、証明書認証処理の動作は第1の実施例の場合と同様である。

この実施例によれば、通信ID、通信ID3及びサブIDの3つのIDにより端末装置4を特定できることになり、より証明力の高い証明書を発行できる。なお、この実施例は第2乃至4の実施例にも適用可能であることはいうまでもない。

【0049】

<第6の実施例>

本発明の第6の実施例は、前述した第1の実施例において、証明書認証の際、通信ID確認装置5または通信ID－サブID確認装置6のいずれか一方もしくは両方も利用する。

図11は本発明の第6の実施例に係る証明書発行システムの構成を示すもので、第1の実施例のシステムにおいて、認証装置8は通信ID確認装置5と通信ID－サブID確認装置6の一方又は両方と例えば専用回線で接続されている。図11では認証装置8が通信ID－サブID確認装置6に接続されている例を示している。認証装置8は、端末装置4からNW2を介してサブIDを少なくとも含む認証要求を受信すると、チャレンジを生成して記憶するとともにNW2を介して端末装置4へ送信する。

【0050】

認証装置8は端末装置4からNW2を介して前記チャレンジに対するレスポンス及び当該端末装置の公開鍵とともに証明書を受信し、これらを記憶する。該受信したレスポンスを端末装置4の公開鍵及び前記記憶したチャレンジを使って検証し、検証に失敗したときはNGの認証結果をNW2を介して端末装置4に送信する。また、検証に成功し且つ前記記憶した証明書中の有効期間内であれば、さらに通信ID確認装置5または通信ID－サブID確認装置6のいずれか一方もしくは両方に通信IDまたは通信IDとサブIDとの関係の確認を要求する。図11の例では通信ID－サブID確認装置6に通信IDとサブIDとが対応関係にあるか否かの確認を要求する例を示している。確認結果がOKであれば、OKの認証結果をNW2を介して端末装置4へ送信する。

【0051】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第1の実施例の場合と同様であり、また、証明書発行処理の動作は第1の実施例の場合と同様である。

図12は図11に示した第6の実施例に係る証明書発行システムにおける証明書認証処理の主要な流れを示すもので、以下、動作を詳細に説明する。

端末装置4が認証要求を認証装置8へ送信し、認証装置8がレスポンスを検証するまでは、第1の実施例の場合と同様である。

認証装置8は、ステップS18で検証に成功し且つステップS19で有効期間内と判定された場合は、さらにステップS20Aで証明書CTFに含まれる通信IDとサブIDとが対応関係にあるか否かの確認を通信ID－サブID確認装置6に要求する。

【0052】

ステップS20Bで通信ID－サブID確認装置6は、認証装置8からの要求に応じて、前記証明書CTFに含まれる通信IDとサブIDとが対応関係にあるか否かを確認し、対応関係にあればOKの確認結果を、対応関係になればNGの確認結果を認証装置8に応答する。

認証装置8は、通信ID－サブID確認装置6からの確認結果を受信し、OKであればOKの認証結果を、また、NGであればNGの認証結果をNW2を介して端末装置4へ送

信する。端末装置 4 はその認証要求部 4 4 により、認証装置 8 から NW 2 を介して認証結果を受信する。

【0053】

この実施例によれば、端末装置 4 から認証が要求された時点での通信 ID とサブ ID の対応関係、即ち証明書 C T F の有効性、を確認できる。なお、この実施例は第 2 乃至 5 の実施例にも適用可能であることはいうまでもない。

【0054】

＜第 7 の実施例＞

本発明の第 7 の実施例は、前述した第 1 の実施例において、端末装置 4 が証明書 C T F の失効を登録する機能が追加され、また、認証装置 8 は証明書 C T F に対する認証の際、
証明書の失効情報が登録されていないか確認する機能が追加されている。

10

【0055】

図 1 3 は本発明の第 7 の実施例に係る証明書発行システムの構成を示すもので、第 1 の実施例のシステムにおいて、証明書 C T F の失効情報を登録した失効情報記憶装置 1 0 を備えている。証明書発行装置 7 及び認証装置 8 は失効情報記憶装置 1 0 に接続されている。

また、端末装置 4 は、通信 ID 記憶部 4 1、証明書記憶部 4 2、証明書発行要求部 4 3 (図示せず)、認証要求部 4 4 とともに、通信 ID 記憶部 4 1 から通信 ID を読み出し、該通信 ID とともにサブ ID を少なくとも含む証明書失効要求を NW 1 を介して証明書発行装置 7 へ送信する証明書失効要求部 4 6 を備えている。

20

【0056】

また、証明書発行装置 7 は、図 2 A に破線で示すように証明書失効情報生成部 7 F が更に追加された構成である。第 1 の実施例の場合の機能に加え、端末装置 4 から NW 1 を介して通信 ID 及びサブ ID を少なくとも含む証明書失効要求を受信すると、通信 ID 確認要求部 7 A は該証明書失効要求に含まれる通信 ID が使用中か否かの確認を通信 ID 確認装置 5 に要求し、通信 ID - サブ ID 確認要求部 7 B は前記証明書失効要求に含まれる通信 ID とサブ ID とが対応関係にあるか否かの確認を通信 ID - サブ ID 確認装置 6 に要求する。証明書失効情報生成部 7 F は、通信 ID 確認装置 5 及び通信 ID - サブ ID 確認装置 6 からの確認結果が OK であれば、当該通信 ID 及びサブ ID を含む証明書の失効情報を生成し、当該失効情報を失効情報記憶装置 1 0 に登録する。

30

【0057】

認証装置 8 は、図 2 C に破線で示すように、失効情報確認部 8 F が更に追加された構成となっている。端末装置 4 から NW 2 を介してサブ ID を少なくとも含む認証要求を受信すると、チャレンジ生成部 8 A はチャレンジを生成して記憶部 8 B に記憶するとともに NW 2 を介して端末装置 4 へ送信する。認証装置 8 は端末装置 4 から NW 2 を介して前記チャレンジに対するレスポンス及び当該端末装置の公開鍵とともに証明書 C T F を受信して記憶する。該受信したレスポンスをレスポンス検証部 8 C により端末装置 4 の公開鍵及び前記記憶したチャレンジを使って検証し、検証に失敗したときは NG の認証結果を NW 2 を介して端末装置 4 に送信する。また、検証に成功し且つ前記記憶した証明書中の有効期間内であれば、さらに証明書 C T F に含まれる通信 ID 及びサブ ID を少なくとも含む証明書の失効情報が失効情報記憶装置 1 0 中にあるか否かを失効情報確認部 8 F により確認し、なければ OK の認証結果を、また、リスト中にあれば NG の認証結果を NW 2 を介して端末装置 4 へ送信する。

40

【0058】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第 1 の実施例の場合と同様である。

図 1 4 は本発明の第 7 の実施例に係る証明書発行システムにおける証明書失効処理の主要な流れを示すもので、以下、動作を詳細に説明する。

まず、端末装置 4 はその証明書失効要求部 4 6 により、通信 ID 記憶部 4 1 から通信 ID を読み出し、該通信 ID とともにサブ ID を少なくとも含むサブ ID 証明書失効要求を

50

NW1を介して証明書発行装置7へ送信する(ステップS31)。

【0059】

証明書発行装置7は、端末装置4からNW1を介して証明書失効要求を受信すると、該証明書失効要求に含まれる通信IDが使用中か否かの確認を通信ID確認装置5に要求する(ステップS32)。

通信ID確認装置5は、証明書発行装置7からの要求に応じて、前記証明書失効要求に含まれる通信IDがNW1で使用中であるか否かをNW1と連携して確認し、使用中であればOKの確認結果を、使用中でなければNGの確認結果を証明書発行装置7に応答する(ステップS33)。

【0060】

証明書発行装置7は、通信ID確認装置5からの確認結果を受信し、前記証明書失効要求に含まれる通信IDとサブIDとが対応関係にあるか否かの確認を通信ID-サブID確認装置6に要求する(ステップS34)。

通信ID-サブID確認装置6は、証明書発行装置7からの要求に応じて、前記証明書失効要求に含まれる通信IDとサブIDとが対応関係にあるか否かを確認し、対応関係にあればOKの確認結果を、対応関係になければNGの確認結果を証明書発行装置7に応答する(ステップS35)。

【0061】

証明書発行装置7は、通信ID-サブID確認装置6からの確認結果を受信し、前記通信ID確認装置5からの確認結果と共にOKであれば、前記端末装置4の通信ID及びサブIDを少なくとも含む証明書の失効情報を生成し、失効情報記憶装置10に登録する。また、確認結果のいずれか一方がNGであれば、処理を終了する(ステップS36)。

図15は本発明の第7の実施例に係る証明書発行システムにおける証明書認証処理の主要な流れを示すもので、以下、動作を詳細に説明する。

端末装置4が認証要求を認証装置8へ送信し、認証装置8がレスポンスを検証するまでは、図12の場合と同様である。

【0062】

認証装置8は、検証に成功し(ステップS17, S18)且つ有効期間内であれば(ステップS19)、さらに証明書に含まれる通信ID及びサブIDを少なくとも含む証明書の失効情報があるか否かの確認を失効情報記憶装置10に要求する(ステップS20C)

。

失効情報記憶装置10は、認証装置8からの要求に応じて、前記通信ID及びサブIDを少なくとも含む証明書の失効情報があるか否かを確認し、該当する失効情報があれば該当情報有り、また、なければ該当情報無しの確認結果を認証装置8に応答する(ステップS20D)。

【0063】

認証装置8は、失効情報記憶装置10からの確認結果を受信し、該当情報がなければOKの認証結果を、また、該当情報があればNGの認証結果をNW2を介して端末装置4へ送信する。端末装置4はその認証要求部44により、認証装置8からNW2を介して認証結果を受信する。

この実施例によれば、端末装置4、即ちユーザは証明書の失効を求めることができ、認証装置8は証明書の認証要求に対し失効情報を登録した失効情報記憶装置10を利用して証明書CTFの有効性を確認できる。なお、この実施例は第2乃至6の実施例にも適用可能であることはいうまでもない。

【0064】

<第8の実施例>

本発明の第8の実施例は、前述した第1の実施例において、複数の証明書のうち、最適の証明書を利用可能とする。

図16は本発明の第8の実施例に係る証明書発行システムの構成を示すもので、第1の実施例のシステムにおいて、端末装置4は、図1の場合と同様に通信ID記憶部41、証

10

20

30

40

50

明書記憶部 4 2、証明書発行要求部 4 3、認証要求部 4 4 を有している。この実施例において端末装置 4 は更に、証明書記憶部 4 2 に保存されている各証明書の利用者、利用先、利用場所、利用時間、利用目的などの利用履歴を管理し、証明書記憶部 4 2 から証明書を読み出して認証要求装置 8 へ送る際、その利用履歴や当該証明書自体に記載された用途などに応じて、最適の証明書を読み出す証明書管理部 4 7 を備えている。

【0065】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第 1 の実施例の場合と同様である。

この実施例によれば、証明書記憶部 4 2 に複数の証明書が保存されている場合、半自動的に最適なものを選択することができる。なお、この実施例は第 2 乃至 7 の実施例にも適用可能であることはいうまでもない。

【0066】

<第 9 の実施例>

本発明の第 9 の実施例は、前述した第 1 の実施例において、端末装置 4 において証明書をより安全に保存可能とする。

【0067】

図 1 7 は本発明の第 9 の実施例に係る証明書発行システムの構成を示すもので、端末装置 4 は第 1 の実施例のシステムにおける端末装置 4 と同様に、通信 ID 記憶部 4 1、証明書記憶部 4 2、証明書発行要求部 4 3、認証要求部 4 4 を有している。図 1 7 の実施例においては端末装置 4 は更に、耐タンパ部 4 8 を内蔵し、証明書記憶部 4 2 を該耐タンパ部 4 8 内に設けた構成となっている。耐タンパ部 4 8 は、例えば TPM (Trusted Platform Module) や SIM (Subscriber Identification Module) のようなデバイスや IC カードにより構成される。

【0068】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第 1 の実施例の場合と同様である。

この実施例によれば、証明書や当該端末装置 4 における公開鍵と秘密鍵の鍵ペアが耐タンパ部 4 8 内に保存されるため、第三者による外部からの攻撃はもとより、本人であってもその内容を改ざんすることはできず、証明書の証明力をより高めることができる。なお、この実施例は第 2 乃至 8 の実施例にも適用可能であることはいうまでもない。

【0069】

<第 10 の実施例>

本発明の第 10 の実施例は、前述した第 1 の実施例において、通信 ID サブ ID 確認装置 6 におけるサブ ID と通信 ID との対応関係の具体的な確認方法の例を示す。

【0070】

図 1 8 は本発明の第 10 の実施例に係る証明書発行システムの構成を示すもので、第 1 の実施例のシステムにおいて、端末装置 4 は通信 ID サブ ID 変換装置 1 1 を介して NW 1 に接続されている。通信 ID サブ ID 確認装置 6 は、所定のサブ ID と NW 1 における所定の通信 ID とが対応関係にあるか否かを、端末装置 4 と NW 1 との間に設置される通信 ID サブ ID 変換装置 1 1 と連携して確認する。ここで、通信 ID サブ ID 変換装置 1 1 とは、子番号と親番号との変換、プライベート IP アドレスとグローバル IP アドレスとの変換などを行う PBX や HGWなどを指す。

【0071】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第 1 の実施例の場合と同様である。

図 1 9 は本発明の第 10 の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

証明書発行装置 7 は、端末装置 4 から証明書発行要求を受信し (ステップ S 1)、通信 ID 確認装置 5 に対して通信 ID が使用中か否かを確認した後 (ステップ S 2, S 3)、証明書発行要求に含まれる通信 ID とサブ ID とが対応関係にあるか否かの確認を通信 I

10

20

30

40

50

Dーサブ I D 確認装置 6 に要求する (ステップ S 4)。

【0072】

通信 I Dーサブ I D 確認装置 6 は、証明書発行装置 7 からの要求に応じて、前記証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かの確認要求を NW 1 を介して通信 I Dーサブ I D 変換装置 11 へ送信する (ステップ S 5 a)。

通信 I Dーサブ I D 変換装置 11 は、通信 I Dーサブ I D 確認装置 6 からの要求を受信し、前記証明書発行要求に含まれるサブ I D の端末装置 4 に対して前述したようなチャレンジ及びレスポンスによる確認を行い (ステップ S 5 b, S 5 c)、確認できれば OK の確認結果を、確認できなければ NG の確認結果を NW 1 を介して通信 I Dーサブ I D 確認装置 6 へ送信する (ステップ S 5 d)。

10

【0073】

通信 I Dーサブ I D 確認装置 6 は、前記通信 I Dーサブ I D 変換装置 11 から受信した確認結果を証明書発行装置 7 に応答する (ステップ S 5 e)。

なお、以降の動作は第 1 の実施例の場合と同様である。

図 20 は本発明の第 10 の実施例に係る証明書発行システムにおける他の証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

証明書発行装置 7 は、端末装置 4 から証明書発行要求を受信し (ステップ S 1)、通信 I D 確認装置 5 に対して通信 I D が使用中か否かを確認した後 (ステップ S 2, S 3)、証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かの確認を通信 I Dーサブ I D 確認装置 6 に要求する (ステップ S 4)。

20

【0074】

通信 I Dーサブ I D 確認装置 6 は、証明書発行装置 7 からの要求に応じて、チャレンジを含み、前記証明書発行要求に含まれる通信 I D を宛先とする端末装置 4 の確認要求を NW 1 を介して通信 I Dーサブ I D 変換装置 11 へ送信する (ステップ S 5 a)。

通信 I Dーサブ I D 変換装置 11 は、前記確認要求の宛先を通信 I D からサブ I D に自動変換して端末装置 4 へ送信する (ステップ S 5 b)。

端末装置 4 は、前記確認要求を受信すると、前記チャレンジに対するレスポンスを計算し、当該レスポンスとその公開鍵を少なくとも含む応答を通信 I Dーサブ I D 変換装置 11 へ送信する (ステップ S 5 c)。

【0075】

30

通信 I Dーサブ I D 変換装置 11 は、前記応答の送信元のサブ I D を通信 I D に自動変換して NW 1 を介して通信 I Dーサブ I D 確認装置 6 へ送信する (ステップ S 5 d)。

通信 I Dーサブ I D 確認装置 6 は、前記通信 I Dーサブ I D 変換装置 11 から端末装置 4 の確認要求に対する応答を受信すると、チャレンジに対するレスポンスを検証し、正しければ OK の確認結果を証明書発行装置 7 に応答する (ステップ S 5 e)。

なお、以降の動作は第 1 の実施例の場合と同様である。

更にまた、図 21 は本発明の第 10 の実施例に係る証明書発行システムにおける更に他の証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

【0076】

証明書発行装置 7 は、端末装置 4 から証明書発行要求を受信し (ステップ S 1)、通信 I D 確認装置 5 に対して通信 I D が使用中か否かを確認した後 (ステップ S 2, S 3)、証明書発行要求に含まれる通信 I D とサブ I D とが対応関係にあるか否かの確認を通信 I Dーサブ I D 確認装置 6 に要求する (ステップ S 4)。

40

通信 I Dーサブ I D 確認装置 6 は、証明書発行装置 7 からの要求に応じて、チャレンジを含み、前記証明書発行要求に含まれる通信 I D を宛先とする端末装置 4 の確認要求を NW 1 を介して通信 I Dーサブ I D 変換装置 11 へ送信する (ステップ S 5 a)。

【0077】

通信 I Dーサブ I D 変換装置 11 は、前記確認要求の宛先を通信 I D からサブ I D に自動変換して端末装置 4 へ送信する (ステップ S 5 b)。

通信端末 4 は、前記確認要求を受信すると、通信 I Dーサブ I D 変換装置 11 へ転送 (

50

リダイレクト)する。

通信 I Dーサブ I D変換装置 11は、前記確認要求を受信すると、前記チャレンジに対するレスポンスを計算し、当該レスポンスとその公開鍵を少なくとも含む応答を端末装置 4へ送信する(ステップ S5c)。

【0078】

端末装置 4は、前記応答を受信すると、通信 I Dーサブ I D変換装置 11へ転送(リダイレクト)する。通信 I Dーサブ I D変換装置 11は、前記応答の送信元をサブ I Dから通信 I Dに自動変換して NW1を介して通信 I Dーサブ I D確認装置 6へ送信する(ステップ S5d)。

通信 I Dーサブ I D確認装置 6は、前記通信 I Dーサブ I D変換装置 11から端末装置 4の確認要求に対する応答を受信すると、OKの確認結果を証明書発行装置 7に応答する(ステップ S5e)。

【0079】

なお、以降の動作は第1の実施例の場合と同様である。また、証明書認証処理の動作は第1の実施例の場合と同様である。

この実施例によれば、端末装置 4と NW1との間に設置される通信 I Dーサブ I D変換装置 11を利用して、所定のサブ I Dと特定のネットワークにおける所定の通信 I Dとが対応関係にあるか否かを確認することができる。なお、この実施例は第2乃至9の実施例にも適用可能であることはいうまでもない。

【0080】

<第11の実施例>

本発明の第11の実施例は、前述した第1の実施例において、証明書の発行を有料とするような形態である。

【0081】

図22は本発明の第11の実施例に係る証明書発行システムの構成を示すもので、第1の実施例のシステムにおいて、所定の通信 I Dへの料金の請求確認に応じて通信端末に対する課金確認を行い、所定の通信 I Dへの料金の請求に応じて与信確認を行う通信 I D課金装置 12が予め決めたネットワーク上に設けられている。

また、証明書発行装置 7は、図2Aに破線で示すように通信 I D課金確認部 7Gを更に含んでおり、端末装置 4から NW1を介して証明書発行要求を受信すると、第1の実施例の場合と同様にして該証明書発行要求に含まれる通信 I Dが使用中か否かの確認及び通信 I Dとサブ I Dとが対応関係にあるか否かの確認を行う。これらの確認結果が共に OKであれば、さらに前記証明書発行要求に含まれる通信 I Dへの証明書の発行に伴う料金の請求確認及び請求を通信 I D課金装置 12に要求し、通信 I D課金装置 12からの応答が共に OKであれば、当該証明書発行装置 7の I D、端末装置 4の通信 I D、サブ I D及び有効期間を少なくとも含む証明書 CTFを生成し、NW1を介して端末装置 4へ送信する。

【0082】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第1の実施例の場合と同様である。

図23は本発明の第11の実施例に係る証明書発行システムにおける証明書発行処理の主要な流れを示すもので、以下、動作を詳細に説明する。

端末装置 4が証明書発行要求を証明書発行装置 7に送信すると(ステップ S1)、証明書発行装置 7は、通信 I D確認装置 5及び通信 I Dーサブ I D確認装置 6からの確認結果を受信し(ステップ S2～S5)、これらが共に OKであれば、証明書発行要求に含まれる通信 I Dへの証明書の発行に伴う料金の請求確認及び請求を通信 I D課金装置 12に要求する(ステップ S9a)。

【0083】

通信 I D課金装置 12は、証明書発行装置 7からの要求に応じて、端末装置 4に対して証明書の発行に伴う料金の課金の確認を要求し(ステップ S9b)、端末装置 4から OKの応答があれば(ステップ S9c)、さらに当該通信 I Dの与信を確認、即ち当該通信 I

10

20

30

40

50

Dに関わる金融機関の口座の残高などの確認を行い（ステップS9d）、その確認結果を証明書発行装置7に応答する（ステップS9e）。

証明書発行装置7は、前記請求確認及び請求に対する通信ID課金装置12からの応答が共にOKであれば、当該証明書発行装置7のID、通信ID、サブID及び有効期間を少なくとも含む証明書CTFを生成し（ステップS6）、NW1を介して端末装置4へ送信する（ステップS7）。

【0084】

なお、証明書認証処理の動作は第1の実施例の場合と同様である。

この実施例によれば、証明書の発行に際し、当該証明書に含まれる通信IDに対して料金を課金することができ、証明書を有料チケットとして販売するサービスを行うことができる。なお、この実施例は第2乃至10の実施例にも適用可能であることはいうまでもない。

【0085】

<第12の実施例>

本発明の第12の実施例は、前述した第11の実施例において、証明書の認証に伴う料金を証明書発行元のネットワークへ請求可能とする。

【0086】

図24は本発明の第12の実施例に係る証明書発行システムの構成を示すもので、第11の実施例のシステムにおいて、証明書の認証に伴う料金の請求確認及び請求を、当該証明書に含まれる通信IDに関わるネットワークNW1へ転送し、その応答を受信するローミング課金装置13が予め決めたネットワーク上に設けられている。

また、認証装置8は、図2Cに破線で示すように更にローミング課金確認部8Gを含んでおり、端末装置4からNW2を介して認証要求を受信すると、第1の実施例の場合と同様にして端末装置、証明書及び有効期間を確認した後、さらに証明書の認証に伴う料金の請求確認及び請求をローミング課金装置13に要求し、ローミング課金装置13からの応答が共にOKであれば、OKの認証結果をNW2を介して端末装置4へ送信する。

【0087】

なお、本実施例に係る証明書発行システムの構成は、前述した点を除いて第11の実施例の場合と同様である。

図25は本発明の第12の実施例に係る証明書発行システムにおける証明書認証処理の主要な流れを示すもので、以下、動作を詳細に説明する。

端末装置4が認証要求を認証装置8へ送信し、認証装置8がレスポンスを検証するまで（ステップS11～S18）は、図12の場合と同様である。

認証装置8は、ステップS18で検証に成功し且つステップS19で有効期間内と判定されると、通信IDを含む証明書CTFの認証に伴う料金の請求確認及び請求をローミング課金装置13に要求する（ステップS20E）。

【0088】

ローミング課金装置13は、前記請求確認及び請求を、当該証明書に含まれる通信IDに関わるネットワークNW1上の通信ID課金装置12へ転送する（ステップS20F）。

通信ID課金装置12は、ローミング課金装置13からの要求に応じて、端末装置4に対して証明書の認証に伴う料金の課金の確認を要求し（ステップS20G）、端末装置4からOKの応答があれば（ステップS20H）、さらに当該通信IDの与信を確認、即ち当該通信IDに関わる金融機関の口座の残高などの確認を行い（ステップS20I）、その確認結果をローミング課金装置13に応答する（ステップS20J）。

【0089】

ローミング課金装置13は、前記請求確認及び請求に対する確認結果を、認証装置8へ転送する（ステップS20K）。

認証装置8は、前記請求確認及び請求に対するローミング課金装置13からの応答が共にOKであれば、OKの認証結果を、そうでなければNGの認証結果をNW2を介して端

10

20

30

40

50

末装置 4 へ送信する（ステップ S 2 0 L）。

この実施例によれば、NW 1 で発行される証明書を用いて NW 2 にアクセスするローミング・サービスの際の料金を NW 1 側に課金することができる。

【0090】

＜その他の実施例＞

これまでの実施例では、端末装置 4 は少なくともそのサブ I D を含む証明書発行要求及び証明書失効要求を送信し、最終的に証明書発行装置 7 に到達する証明書発行要求及び証明書失効要求には通信 I D 及びサブ I D の両方が含まれるものとしたが、最終的に証明書発行装置 7 に到達する証明書発行要求及び証明書失効要求として通信 I D のみを含むものを用いるようにしても良い。

10

この場合、証明書発行要求及び証明書失効要求に含まれる通信 I D は、端末装置 4 の証明書発行要求部 4 3 により通信 I D 記憶部 4 1 から読み出されて付与される場合と、第 4 の実施例で説明したように、NW 1 側の通信 I D 付与装置 9 により付与される場合とがある。

【0091】

また、証明書発行装置 7 は、端末装置 4 から NW 1 を介して通信 I D のみを含む証明書発行要求を受信すると、該証明書発行要求に含まれる通信 I D が使用中か否かの確認を通信 I D 確認装置 5 に要求し、通信 I D 確認装置 5 からの確認結果が OK であれば、当該証明書発行装置 7 の I D、端末装置 4 の通信 I D 及び有効期間を少なくとも含む証明書 C T F を生成し、NW 1 を介して端末装置 4 へ送信する。また、端末装置 4 から NW 1 を介して通信 I D のみを含む証明書失効要求を受信すると、該証明書失効要求に含まれる通信 I D が使用中か否かの確認を通信 I D 確認装置 5 に要求する。通信 I D 確認装置 5 からの確認結果が OK であれば、当該通信 I D を含む証明書 C T F の失効情報を生成し、当該失効情報を失効情報記憶装置 1 0 に追加登録する。

20

【0092】

なお、証明書発行処理及び証明書認証処理の動作は、通信 I D－サブ I D 確認装置 6 へのアクセスがない点を除いて基本的に第 1 の実施例の場合と同様であり、また、証明書失効処理及びその際の証明書認証処理の動作も通信 I D－サブ I D 確認装置 6 へのアクセスがない点を除いて基本的に第 7 の実施例の場合と同様である。

この実施例によれば、端末装置単位ではなく、端末装置 4 が所属するサブネットワークを単位とする、本人の確認を必要としない、有効期間の短い証明書を発行することにより、証明書発行装置 7 が接続された NW 1 とは異なる NW 2 に接続された認証装置 8 でも認証可能とする。それにより、端末装置 4 を移動して用いるような、元の通信 I D が利用できないような場合であっても、様々なサービスを利用可能とすることができる。

30

【図 1】

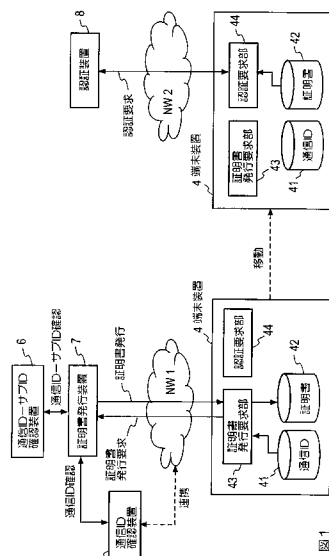


図 1

【図 2】

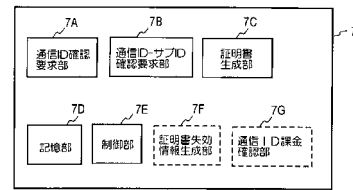


図 2A

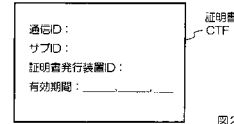


図 2B

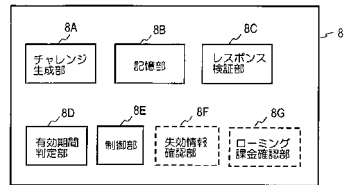


図 2C

【図 3】

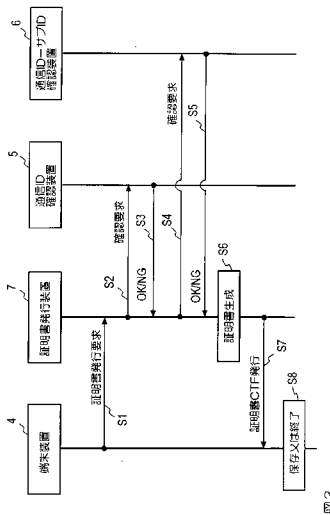


図 3

【図 4】

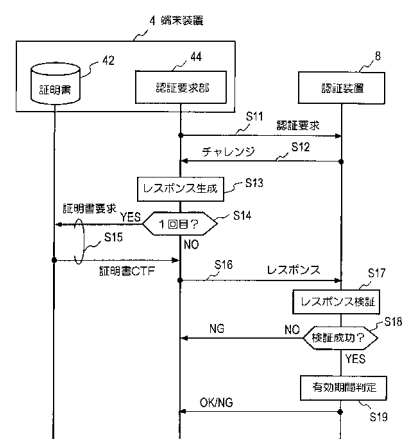


図 4

【図 5】

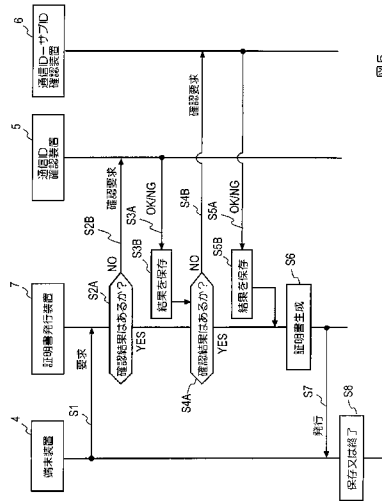


図5

【図 6】

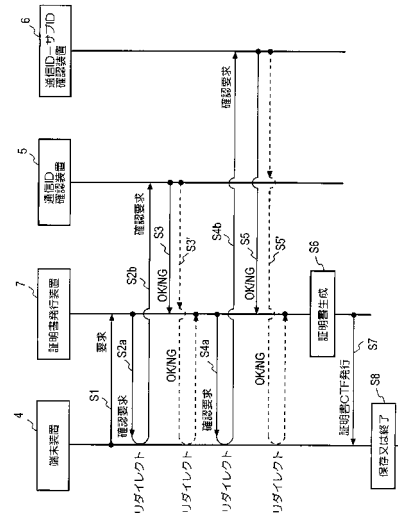


図6

【図 7】

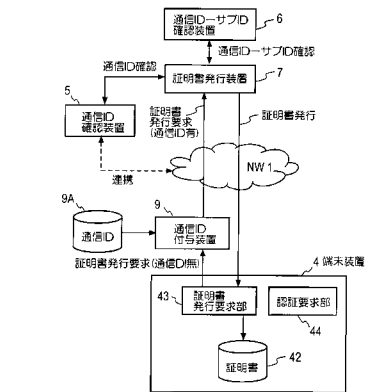


図7

【図 8】

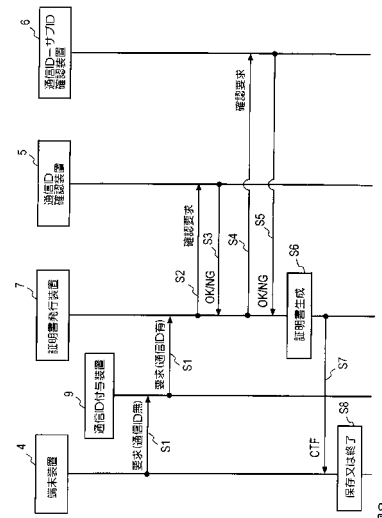
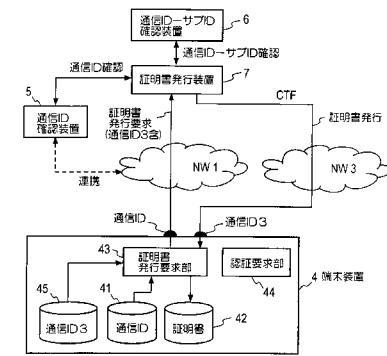


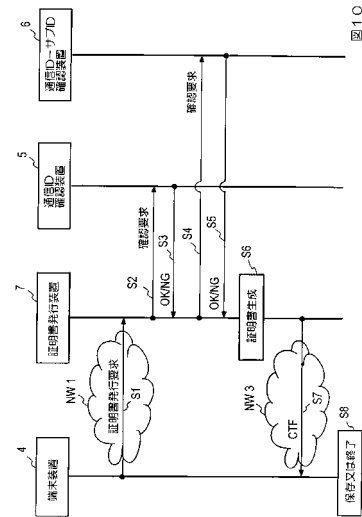
図8

【図 9】



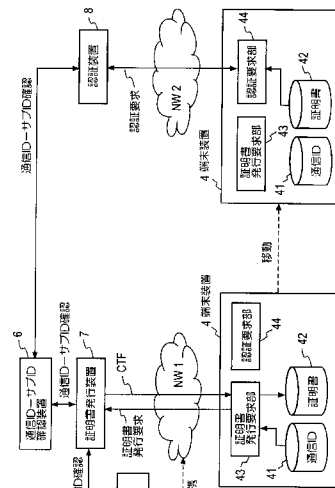
9

【図 10】



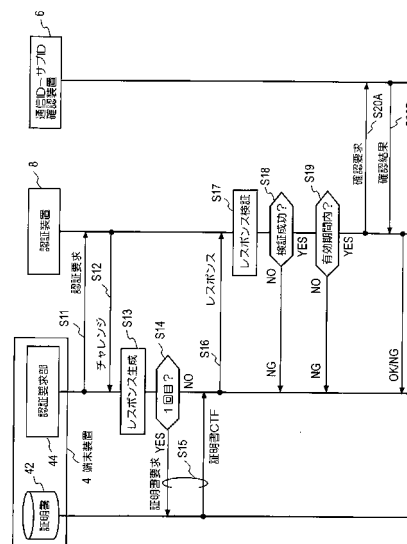
10

【図 1 1】



11

【图 1 2】



12

【図 13】

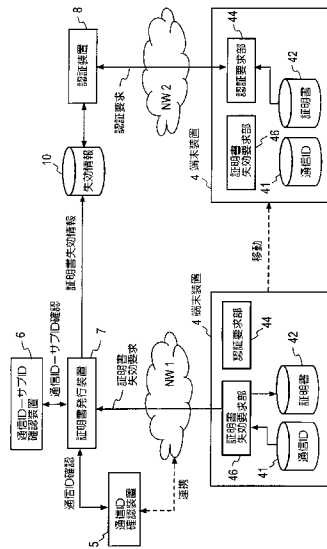


図 13

【図 14】

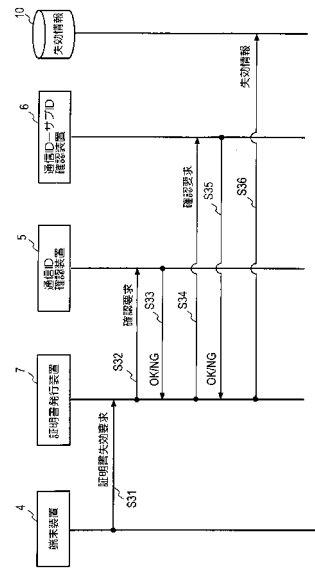


図 14

【図 15】

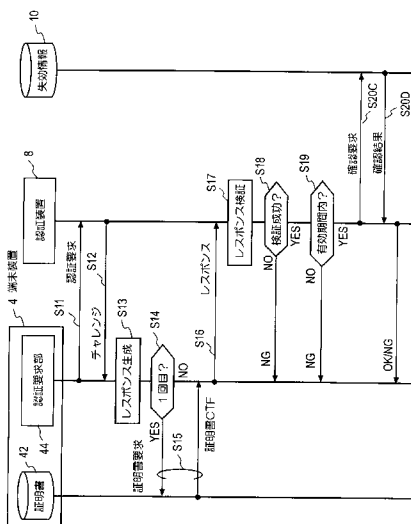


図 15

【図 16】

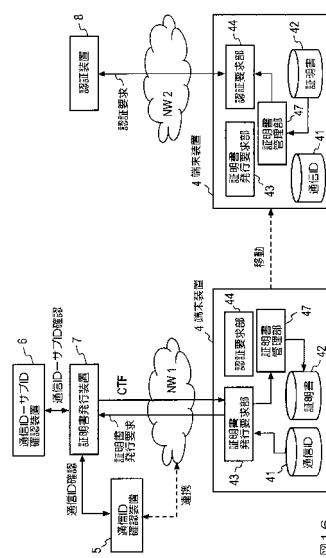
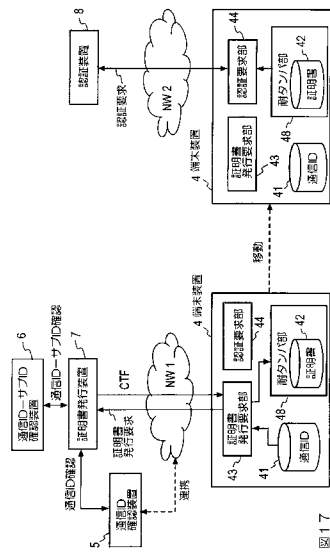
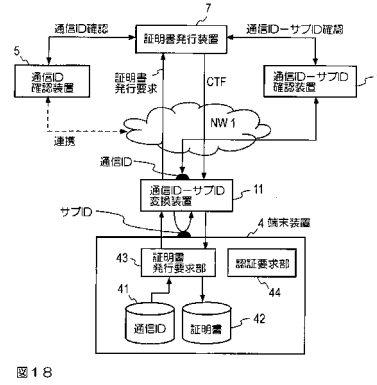


図 16

【図 17】

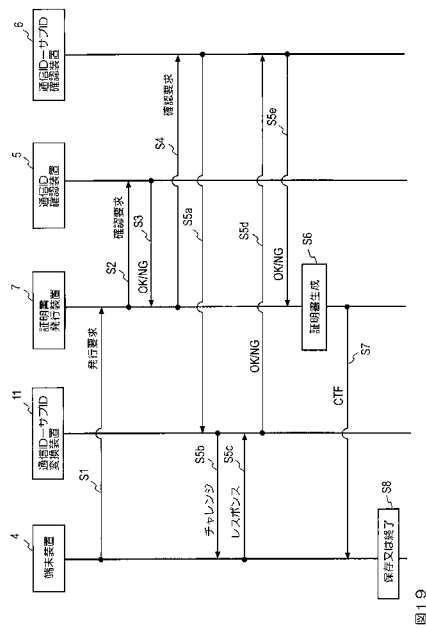


【図 18】

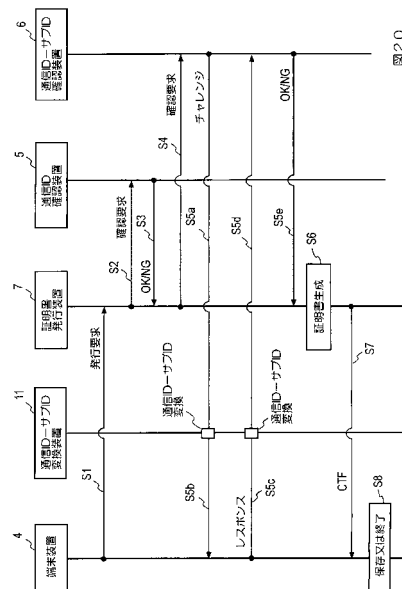


18

【図 19】

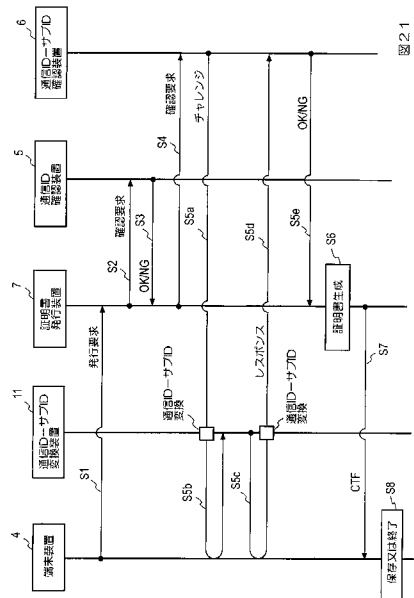


【图 20】

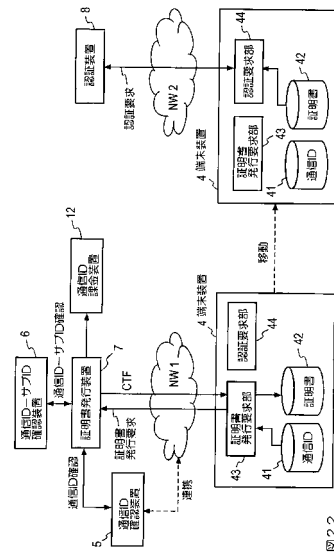


20

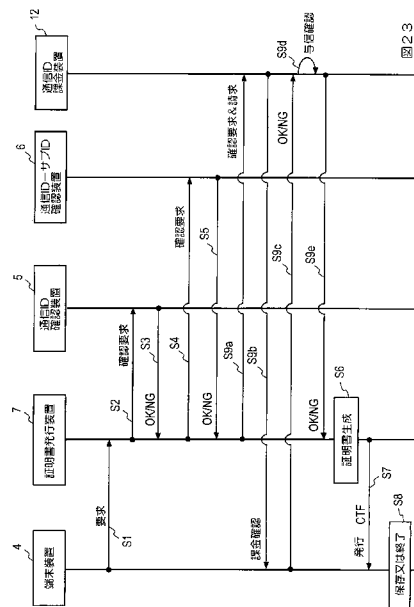
【図 2 1】



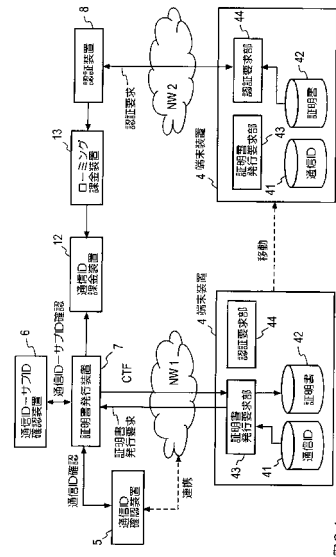
【図 2 2】



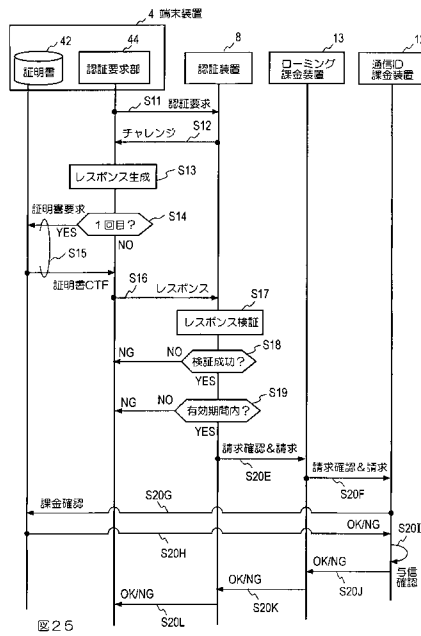
【図 2 3】



【図 2 4】



【図 25】



フロントページの続き

- (72)発明者 川島 正久
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
- (72)発明者 鶴岡 行雄
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
- (72)発明者 高橋 健司
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
- (72)発明者 折原 慎吾
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

審査官 石田 信行

- (56)参考文献 特開2006-025010 (JP, A)
特開2003-188873 (JP, A)
特開2005-339093 (JP, A)
特開2004-343442 (JP, A)
特表2008-541242 (JP, A)
特開2008-015934 (JP, A)
特開2007-323326 (JP, A)
再公表特許第2005/011192 (JP, A1)
特開2004-272380 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 9/32
G09C 1/00
G06F 21/20