(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3880957号
(P3880957)
(45)発行日　平成19年2月14日(2007.2.14)　(24)登録日　平成18年11月17日(2006.11.17)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
H04L	9/08	(2006.01)	H04L	9/00	601F
			H04L	9/00	675Z

請求項の数 9　(全 25 頁)

(21)出願番号　特願2003-359862(P2003-359862)
(22)出願日　平成15年10月20日(2003.10.20)
(65)公開番号　特開2005-124097(P2005-124097A)
(43)公開日　平成17年5月12日(2005.5.12)
審査請求日　平成15年10月20日(2003.10.20)

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

最終頁に続く

(54)【発明の名称】ルート証明書配布システム、ルート証明書配布方法、コンピュータ実行可能なルート証明書配布プログラム、サーバ装置及びクライアント装置

(57)【特許請求の範囲】

【請求項１】

クライアント装置と、クライアント装置にネットワークを介して接続され、クライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書に基づいて証明される第１のサーバ証明書によって公開鍵を証明する第１のサーバ装置と、クライアント装置および第１のサーバ装置にネットワークを介して接続され、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵を証明する第２のサーバ装置と、を備えたルート証明書配布システムであって、

前記第１のサーバ装置は、

前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書、前記第２のルート証明書、前記第１の公開鍵を証明し前記第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書、および前記第１のサーバ証明書を含み前記第２の相互認証証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、

前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段と、を有し、

前記クライアント装置は、

前記第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段と、

前記証明書チェーン送信手段によって送信された証明書チェーンに含まれる各証明書を

前記ルート証明書記憶手段に記憶されたルート証明書に基づいて順次検証する証明書検証手段と、

前記証明書検証手段によって前記証明書チェーンに含まれる各証明書が正当なものであると検証された場合には、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段と、

前記第２のサーバ装置を表すサーバ情報を前記第１のサーバ装置に送信するサーバ情報送信手段と、を有し

前記第１のサーバ装置は、前記クライアント装置のサーバ情報送信手段によって送信されたサーバ情報に表される第２のサーバ装置の公開鍵を連鎖的に証明するルート証明書を要求するルート証明書要求情報を、前記第２のサーバ装置に送信するルート証明書要求情報送信手段を、さらに有し、

前記第２のサーバ装置は、前記ルート証明書要求情報送信手段によって送信されたルート証明書要求情報に応じて前記第２のルート証明書を前記第１のサーバ装置に送信するルート証明書送信手段を有し、

前記第１のサーバ装置の証明書チェーン生成手段は、前記第２のサーバ装置のルート証明書送信手段によって送信された第２のルート証明書に基づいて、前記証明書チェーンの生成を行う

ことを特徴とするルート証明書配布システム。

【請求項２】

利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置、およびこのクライアント装置にネットワークを介して接続され、前記クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置を備えたルート証明書配布システムであって、

前記サーバ装置は、

前記クライアント装置との公開鍵認証時において、前記クライアント装置から前記第１のルート証明書を受け付けて、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書、前記第２のルート証明書、および前記サーバ証明書を含み前記第２のルート証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、

前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段とを有し、

前記クライアント装置は、

前記サーバ装置との公開鍵認証時において、前記第１のルート証明書を前記サーバ装置に送信するルート証明書送信手段と、

前記証明書チェーン送信手段によって送信された証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶された第１のルート証明書に基づいて順次検証する証明書検証手段と、

前記証明書チェーン送信手段によって送信された前記証明書チェーンに含まれる各証明書が正当なものであると前記証明書検証手段によって検証された場合に、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段と、を有し、

前記サーバ装置の証明書チェーン生成手段は、前記クライアント装置から公開鍵認証時に受け付けた第１のルート証明書に基づいて前記相互認証証明書を記憶手段から取得すること

ことを特徴とするルート証明書配布システム。

【請求項３】

クライアント装置と、クライアント装置にネットワークを介して接続され、クライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１

のルート証明書に基づいて証明される第１のサーバ証明書によって公開鍵を証明する第１のサーバ装置、および前記クライアント装置および第１のサーバ装置にネットワークを介して接続され、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵を証明する第２のサーバ装置を備えたシステムにおけるルート証明書配布方法であって、

前記第１のサーバ装置においては、

前記クライアント装置から送信されたサーバ情報に表される第２のサーバ装置の公開鍵を連鎖的に証明する前記第２のルート証明書を要求するルート証明書要求情報を前記第２のサーバ装置に送信し、

前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書、前記第２のルート証明書、前記第１の公開鍵を証明し前記第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書、および前記第１のサーバ証明書を含み前記第２の相互認証証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成し、

この生成された証明書チェーンを前記クライアント装置に送信し、

前記クライアント装置においては、

前記第１のルート証明書を含むルート証明書をルート証明書記憶手段に記憶し、

前記第２のサーバ装置を表すサーバ情報を前記第１のサーバ装置に送信し、

前記第１のサーバ装置から送信された証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶されたルート証明書に基づいて順次検証し、

この順次検証によって前記証明書チェーンに含まれる各証明書が正当なものであると検証された場合には、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させ、

前記第２のサーバ装置においては、前記第1のサーバ装置から送信されたルート証明書要求情報に応じて前記第２のルート証明書を前記第１のサーバ装置に送信し、

前記第１のサーバ装置における証明書チェーンの作成は、前記第２のサーバ装置から送信された第２のルート証明書に基づいて行われる

ことを特徴とするルート証明書配布方法。

【請求項４】

利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置、およびこのクライアント装置にネットワークを介して接続され、前記クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置を備えたシステムにおけるルート証明書配布方法であって、

前記サーバ装置においては、

前記クライアント装置との公開鍵認証時において、前記クライアント装置から前記第１のルート証明書を受け付けて、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書、前記第２のルート証明書、および前記サーバ証明書を含み前記第２のルート証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成し、

この生成された証明書チェーンを前記クライアント装置に送信し、

前記クライアント装置においては、

前記サーバ装置との公開鍵認証時において、前記第１のルート証明書を前記サーバ装置に送信し、

前記サーバ装置から送信された証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶された第１のルート証明書に基づいて順次検証し、

前記サーバ装置から送信された前記証明書チェーンに含まれる各証明書が正当なものであると検証した場合に、前記証明書チェーンに含まれる前記第２のルート証明書を前記ル

ート証明書記憶手段に記憶させ、
前記サーバ装置は、前記証明書チェーンの生成において、前記クライアント装置から公開鍵認証時に受け付けた第１のルート証明書に基づいて前記相互認証証明書を記憶手段から取得する
ことを特徴とするルート証明書配布方法。
【請求項５】
請求項３または請求項４記載のルート証明書配布方法をコンピュータに実行させることを特徴とするコンピュータ実行可能なルート証明書配布プログラム。
【請求項６】
ネットワークを介して接続されるクライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書に基づいて証明される第１のサーバ証明書によって公開鍵を証明するサーバ装置であって、
クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書、第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書、前記第１の公開鍵を証明し前記第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書、および前記第１のサーバ証明書を含み前記第２の相互認証証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、
前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段と、
クライアント装置から送信されたサーバ情報に表される別のサーバ装置であって、かつ、前記第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵の証明される別のサーバ装置における公開鍵を連鎖的に証明するルート証明書を要求するルート証明書要求情報を当該別のサーバに送信するルート証明書要求情報送信手段と、を有し、
前記証明書チェーン生成手段は、前記別のサーバ装置から前記ルート証明書要求情報に応じて返信されてくる第２のルート証明書を受信し、当該第２のルート証明書に基づいて、前記証明書チェーンの生成を行う
ことを特徴とするサーバ装置。
【請求項７】
利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置であって、
前記クライアントとの公開鍵認証時において、前記クライアント装置から前記第１のルート証明書を受け付けて、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書、前記第２のルート証明書、および前記サーバ証明書を含み前記第２のルート証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、
前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段と、を有し、
前記サーバ装置の証明書チェーン生成手段は、前記クライアント装置から公開鍵認証時に受け付けた第１のルート証明書に基づいて前記相互認証証明書を記憶手段から取得すること
を特徴とするサーバ装置。
【請求項８】
ネットワークに接続されたクライアント装置であって、
前記クライアント装置は、当該クライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書に基づいて証明される第１の

サーバ証明書によって公開鍵を証明する第１のサーバ装置、および当該クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵を証明する第２のサーバ装置と、ネットワークを介して接続され、

前記第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段と、

前記第２のサーバ装置を表すサーバ情報を、前記第１のサーバ装置にネットワークを介して送信するサーバ情報送信手段と、

前記第１のサーバ装置からネットワークを介して送信されてくる、前記サーバ情報に基づいて生成された証明書チェーンに含まれる各証明書を、前記ルート証明書記憶手段に記憶されたルート証明書に基づいて順次検証する証明書検証手段と、

前記証明書検証手段によって前記証明書チェーンに含まれる各証明書が正当なものであると検証された場合に、前記証明書チェーンに含まれる第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段と

を有することを特徴とするクライアント装置。

【請求項９】

ネットワークに接続され、利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置であって、

前記クライアント装置は、当該クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置とネットワークを介して接続され、

前記サーバ装置との公開鍵認証時において、前記第１のルート証明書を、当該サーバ装置に送信するルート証明書送信手段と、

ネットワークを介して前記サーバ装置から送信されてくる証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶された第１のルート証明書に基づいて順次検証する証明書検証手段と、

前記証明書チェーンに含まれる各証明書が正当なものであると前記証明書検証手段によって検証された場合に、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段と

を有することを特徴とするクライアント装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ルート証明書配布システムに関し、詳しくは、クライアント装置からサーバ装置に送信されるデータをサーバ装置の公開鍵を以って暗号化する非対称鍵暗号通信またはクライアント装置がサーバ装置の認証を行うサーバ認証において、サーバ装置の公開鍵を証明するためのルート証明書を配布するルート証明書配布システム、方法およびプログラムとサーバ装置およびクライアント装置に関する。

【背景技術】

【０００２】

従来、クライアント装置からサーバ装置に送信されるデータをサーバ装置の公開鍵を以って暗号化する非対称鍵暗号通信またはクライアント装置がサーバ装置の認証を行うサーバ認証において、サーバ装置の公開鍵を証明するものとして、国際電気通信連合の電気通信標準化部門（International Telecommunications Union-Telecommunications Standardization Sector、ＩＴＵ－Ｔとも称する）Ｘ．５０９によって規格化されたＸ．５０９証明書を用いたものが知られている。

【０００３】

Ｘ．５０９証明書は、公開鍵とその所有者との対応を証明するものであり、証明する公開鍵を含み、他者の秘密鍵によって署名されている。Ｘ．５０９証明書によって公開鍵の所有者を他者が証明し、他者の公開鍵を更に別の者が証明するといった連鎖的な公開鍵の

証明を行うことができる。Ｘ．５０９証明書のように連鎖的に公開鍵を証明するものを本明細書においては、単に「証明書」という。

【０００４】

ここで、クライアント装置の利用者にとって確かな公開鍵が存在すれば、この公開鍵に基づいて連鎖的に他の公開鍵を証明することができる。このクライアント装置の利用者にとって確かな公開鍵を提供する機関は、ルート認証機関と呼ばれ、ルート認証機関の公開鍵は、ルート認証機関の秘密鍵によって自己署名されたルート証明書によって証明される。クライアント装置は、ルート証明書を記憶することによって、他の装置の公開鍵をルート証明書から連鎖的に検証することができる。

【０００５】

ルート認証機関は、他のルート認証機関の公開鍵を証明する相互認証証明書および他のルート認証機関によって公開鍵が証明される相互認証証明書によって、他のルート認証機関と信頼関係を結ぶことができ、この相互認証証明書によって一方のルート認証機関を信頼するクライアント装置に対して、他方のルート認証機関を信頼させることができる。

【０００６】

例えば、検証者側認証局が相互認証用鍵で他階層の認証局の相互認証用公開鍵を認証する相互認証証明書を生成し、認証局は自分の相互認証用秘密鍵で自分の階層認証用公開鍵に署名をつけた認証連鎖変換証明書を生成し、検証者は認証局の階層認証用公開鍵証明書と相互認証証明書間を、認証連鎖変換証明書を介在させて相互認証パスを構築し、異なる階層の階層認証と相互認証で使用する鍵が異なる認証局を含む認証局間の相互認証パス構築において第３者が認証局に成りすますことができないようにするものがある（例えば、特許文献１参照）。

【特許文献１】特開２００２－２１７９０１号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、前述したような従来の技術では、クライアント装置が相互認証証明書を検証前に取得しておかないと認証が失敗してしまうため、クライアント装置側で相互認証証明書を取得する手間が生じるといった課題が残されていた。

【０００８】

本発明は、上記に鑑みてなされたもので、その目的とするところは、クライアント装置側で相互認証証明書を取得する手間を生じさせることなく、クライアント装置に信頼されていない他のルート認証機関を信頼させることができるルート証明書配布システムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

請求項１記載の本発明のルート証明書配布システムは、クライアント装置と、クライアント装置にネットワークを介して接続され、クライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書に基づいて証明される第１のサーバ証明書によって公開鍵を証明する第１のサーバ装置と、クライアント装置および第１のサーバ装置にネットワークを介して接続され、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵を証明する第２のサーバ装置と、を備えたルート証明書配布システムであって、前記第１のサーバ装置が、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書、前記第２のルート証明書、前記第１の公開鍵を証明し前記第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書、および前記第１のサーバ証明書を含み前記第２の相互認証証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段と、

を有し、前記クライアント装置が、前記第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段と、前記証明書チェーン送信手段によって送信された証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶されたルート証明書に基づいて順次検証する証明書検証手段と、前記証明書検証手段によって前記証明書チェーンに含まれる各証明書が正当なものであると検証された場合には、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段と、前記第２のサーバ装置を表すサーバ情報を前記第１のサーバ装置に送信するサーバ情報送信手段と、を有し、前記第１のサーバ装置は、前記クライアント装置のサーバ情報送信手段によって送信されたサーバ情報に表される第２のサーバ装置の公開鍵を連鎖的に証明するルート証明書を要求するルート証明書要求情報を、前記第２のサーバ装置に送信するルート証明書要求情報送信手段を、さらに有し、前記第２のサーバ装置は、前記ルート証明書要求情報送信手段によって送信されたルート証明書要求情報に応じて前記第２のルート証明書を前記第１のサーバ装置に送信するルート証明書送信手段を有し、前記第１のサーバ装置の証明書チェーン生成手段は、前記第２のサーバ装置のルート証明書送信手段によって送信された第２のルート証明書に基づいて、前記証明書チェーンの生成を行うことを要旨とする。

【００１１】

請求項２記載の本発明のルート証明書配布システムは、利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置、およびこのクライアント装置にネットワークを介して接続され、前記クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置を備えたルート証明書配布システムであって、前記サーバ装置が、前記クライアント装置との公開鍵認証時において、前記クライアント装置から前記第１のルート証明書を受け付けて、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書、前記第２のルート証明書、および前記サーバ証明書を含み前記第２のルート証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段とを有し、前記クライアント装置が、前記サーバ装置との公開鍵認証時において、前記第１のルート証明書を前記サーバ装置に送信するルート証明書送信手段と、前記証明書チェーン送信手段によって送信された証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶された第１のルート証明書に基づいて順次検証する証明書検証手段と、前記証明書チェーン送信手段によって送信された前記証明書チェーンに含まれる各証明書が正当なものであると前記証明書検証手段によって検証された場合に、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段と、を有し、前記サーバ装置の証明書チェーン生成手段は、前記クライアント装置から公開鍵認証時に受け付けた第１のルート証明書に基づいて前記相互認証証明書を記憶手段から取得することを要旨とする。

【００１３】

請求項３記載の本発明のルート証明書配布方法は、クライアント装置と、クライアント装置にネットワークを介して接続され、クライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書に基づいて証明される第１のサーバ証明書によって公開鍵を証明する第１のサーバ装置、および前記クライアント装置および第１のサーバ装置にネットワークを介して接続され、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵を証明する第２のサーバ装置を備えたシステムにおけるルート証明書配布方法であって、前記第１のサーバ装置においては、前記クライアント装置から送信されたサーバ情報に表される第２のサーバ装置の公開鍵を連鎖的に証明する前記第２のルート証明書を要求するルート証明書要求情

報を前記第２のサーバ装置に送信し、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書、前記第２のルート証明書、前記第１の公開鍵を証明し前記第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書、および前記第１のサーバ証明書を含み前記第２の相互認証証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成し、この生成された証明書チェーンを前記クライアント装置に送信し、前記クライアント装置においては、前記第１のルート証明書を含むルート証明書をルート証明書記憶手段に記憶し、前記第２のサーバ装置を表すサーバ情報を前記第１のサーバ装置に送信し、前記第１のサーバ装置から送信された証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶されたルート証明書に基づいて順次検証し、この順次検証によって前記証明書チェーンに含まれる各証明書が正当なものであると検証された場合には、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させ、前記第２のサーバ装置においては、前記第1のサーバ装置から送信されたルート証明書要求情報に応じて前記第２のルート証明書を前記第１のサーバ装置に送信し、前記第１のサーバ装置における証明書チェーンの作成は、前記第２のサーバ装置から送信された第２のルート証明書に基づいて行われることを要旨とする。

【００１５】

請求項４記載の本発明のルート証明書配布方法は、利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置、およびこのクライアント装置にネットワークを介して接続され、前記クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置を備えたシステムにおけるルート証明書配布方法であって、前記サーバ装置においては、前記クライアント装置との公開鍵認証時において、前記クライアント装置から前記第１のルート証明書を受け付けて、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書、前記第２のルート証明書、および前記サーバ証明書を含み前記第２のルート証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成し、この生成された証明書チェーンを前記クライアント装置に送信し、前記クライアント装置においては、前記サーバ装置との公開鍵認証時において、前記第１のルート証明書を前記サーバ装置に送信し、前記サーバ装置から送信された証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶された第１のルート証明書に基づいて順次検証し、前記サーバ装置から送信された前記証明書チェーンに含まれる各証明書が正当なものであると検証した場合に、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させ、前記サーバ装置は、前記証明書チェーンの生成において、前記クライアント装置から公開鍵認証時に受け付けた第１のルート証明書に基づいて前記相互認証証明書を記憶手段から取得することを要旨とする。

【００１７】

請求項５記載の本発明のルート証明書配布プログラムは、請求項３または請求項４記載のルート証明書配布方法をコンピュータに実行させるコンピュータ実行可能なルート証明書配布プログラムであることを要旨とする。

【００１８】

請求項６記載の本発明のサーバ装置は、ネットワークを介して接続されるクライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書に基づいて証明される第１のサーバ証明書によって公開鍵を証明するサーバ装置であって、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書、第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書、前記第１の公開鍵を証明し前記第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書、および前記第１のサーバ証明書を含み前記第２の相互認証証明書によっ

て連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段と、クライアント装置から送信されたサーバ情報に表される別のサーバ装置であって、かつ、前記第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵の証明される別のサーバ装置における公開鍵を連鎖的に証明するルート証明書を要求するルート証明書要求情報を当該別のサーバに送信するルート証明書要求情報送信手段と、を有し、前記証明書チェーン生成手段は、前記別のサーバ装置から前記ルート証明書要求情報に応じて返信されてくる第２のルート証明書を受信し、当該第２のルート証明書に基づいて、前記証明書チェーンの生成を行うことを要旨とする。

【００２０】

請求項７記載の本発明のサーバ装置は、利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置であって、前記クライアントとの公開鍵認証時において、前記クライアント装置から前記第１のルート証明書を受け付けて、前記第２の公開鍵を証明し前記第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書、前記第２のルート証明書、および前記サーバ証明書を含み前記第２のルート証明書によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段と、

前記証明書チェーン生成手段によって生成された証明書チェーンを前記クライアント装置に送信する証明書チェーン送信手段と、を有し、前記サーバ装置の証明書チェーン生成手段は、前記クライアント装置から公開鍵認証時に受け付けた第１のルート証明書に基づいて前記相互認証証明書を記憶手段から取得することを要旨とする。

【００２１】

請求項８記載の本発明のクライアント装置は、ネットワークに接続されたクライアント装置であって、前記クライアント装置は、当該クライアント装置の利用者によって信頼される第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書に基づいて証明される第１のサーバ証明書によって公開鍵を証明する第１のサーバ装置、および当該クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明される第２のサーバ証明書によって公開鍵を証明する第２のサーバ装置と、ネットワークを介して接続され、前記第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段と、前記第２のサーバ装置を表すサーバ情報を、前記第１のサーバ装置にネットワークを介して送信するサーバ情報送信手段と、前記第１のサーバ装置からネットワークを介して送信されてくる、前記サーバ情報に基づいて生成された証明書チェーンに含まれる各証明書を、前記ルート証明書記憶手段に記憶されたルート証明書に基づいて順次検証する証明書検証手段と、前記証明書検証手段によって前記証明書チェーンに含まれる各証明書が正当なものであると検証された場合に、前記証明書チェーンに含まれる第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段と、を有することを要旨とする。

【００２３】

請求項９記載の本発明のクライアント装置は、ネットワークに接続され、利用者が信頼する第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書を含むルート証明書を記憶するルート証明書記憶手段を有するクライアント装置であって、前記クライアント装置は、当該クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書に基づいて証明されるサーバ証明書によって公開鍵を証明するサーバ装置とネットワークを介して接続され、前記サーバ装置との公開鍵認証時において、前記第１のルート証明書を、当該サーバ装置に送信するルート証明書送信手段と、ネットワークを介して前記サーバ装置から送信されてくる証明書チェーンに含まれる各証明書を前記ルート証明書記憶手段に記憶された第１のルート証明書に

基づいて順次検証する証明書検証手段と、前記証明書チェーンに含まれる各証明書が正当なものであると前記証明書検証手段によって検証された場合に、前記証明書チェーンに含まれる前記第２のルート証明書を前記ルート証明書記憶手段に記憶させるルート証明書登録手段とを有することを要旨とする。

【発明の効果】

【００２５】

本発明によれば、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明しクライアント装置の利用者によって信頼されている第１のルート認証機関の第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２のルート証明書、クライアント装置の利用者によって信頼されている第１のルート認証機関の第１の公開鍵を証明しクライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書を含む証明書チェーンで第１のサーバ装置の公開鍵を認証させるので、クライアント装置側で相互認証証明書を取得する手間を生じさせることなく、クライアント装置に信頼されていない第２のルート認証機関を信頼させることができる。

【００２６】

本発明によれば、クライアント装置によって送信されたサーバ情報に基づいて証明書チェーンを生成するので、クライアント装置が公開鍵認証したいサーバ装置の公開鍵を連鎖的に証明するルート認証機関をクライアント装置に信頼させることができる。

【００２７】

本発明によれば、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明しクライアント装置の利用者が信頼する第１のルート認証機関の第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書、クライアント装置の利用者によって信頼されていない第２のルート認証機関の第２のルート証明書を含む証明書チェーンでサーバ装置の公開鍵を認証させるので、クライアント装置側で相互認証証明書を取得する手間を生じさせることなく、サーバ装置の公開鍵を認証させることができ、クライアント装置に信頼されていない第２のルート認証機関を信頼させることができる。

【００２８】

本発明によれば、サーバ装置の公開鍵の認証時に送信される証明書チェーンに含まれる各証明書が正当なものであると検証された場合に、証明書チェーンに含まれるルート証明書がクライアント装置に登録されるので、クライアント装置においてサーバ装置の公開鍵の認証時にクライアント装置の利用者によって信頼されていないルート認証機関の公開鍵を証明するルート証明書を登録することができる。

【００２９】

本発明によれば、ルート証明書配布方法をルート証明書配布プログラムとして例えば記録媒体などに記録してコンピュータに実行させるので、該記録媒体を用いて、その流通性を高めることができる。

【発明を実施するための最良の形態】

【００３０】

以下、図面を用いて、本発明を実施するための最良の形態（以下、実施形態と称する）を説明する。

【００３１】

（第１の実施形態）

図１は、本発明の第１の実施形態に係るルート証明書配布システム１００の構成を示すブロック図である。同図に示す実施形態のルート証明書配布システム１００は、ネットワーク１０に接続されたクライアント装置１１０と、クライアント装置１１０の利用者によって信頼されている第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書Ｃａ１に基づいて証明される第１のサーバ証明書Ｓ１によって公開鍵を証明する第１のサ

ーバ装置１２０と、クライアント装置１１０の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書Ｃａ２に基づいて証明される第２のサーバ証明書Ｓ２によって公開鍵を証明する第２のサーバ装置１３０とを備えている。

【００３２】

なお、本発明のルート証明書配布システム１００は、複数のクライアント装置１１０、複数の第１のサーバ装置１２０、および複数の第２のサーバ装置１３０によって構成することができるが、説明を簡単にするために１つのクライアント装置１１０、１つの第１のサーバ装置１２０、および１つの第２のサーバ装置１３０によって構成されるものとして以下説明する。

【００３３】

図２は、第１のサーバ装置１２０の構成を示すブロック図である。この第１のサーバ装置１２０は、中央処理装置（Central Processing Unit、以下単に「ＣＰＵ」と称する）を有するコンピュータ装置によって構成されており、証明書を記憶する証明書記憶手段１２１を備えている。

【００３４】

証明書記憶手段１２１は、コンピュータ装置を構成するハードディスク装置やフラッシュメモリ等の不揮発性の記憶媒体によって構成され、この証明書記憶手段１２１には、第１のサーバ証明書Ｓ１を含み第１のルート証明書Ｃａ１によって連鎖的に証明される一連の証明書が第１のサーバ装置１２０の管理者によって予め記憶されている。ここで、第１のサーバ証明書Ｓ１を含み第１のルート証明書Ｃａ１によって連鎖的に証明される一連の証明書には、説明を簡単にするために第１のサーバ証明書Ｓ１のみが含まれるものとする。

【００３５】

また、第１のルート認証機関と第２のルート認証機関とが相互に信頼関係を結んだ場合には、第２のルート証明書Ｃａ２、第２の公開鍵を証明し第１の公開鍵と対を成す秘密鍵を以って署名された第１の相互認証証明書Ｍ１、および第１の公開鍵を証明し第２の公開鍵と対を成す秘密鍵を以って署名された第２の相互認証証明書Ｍ２が第１のサーバ装置１２０の管理者によって証明書記憶手段１２１に記憶される。

【００３６】

ここで、第１のルート証明書Ｃａ１は、第１のルート認証機関の第１の公開鍵が含まれ、第１のルート認証機関の秘密鍵で署名されており、クライアント装置１１０に既に記憶されている。なお、署名は、証明書または証明書のハッシュ値を秘密鍵で暗号化したものであり、暗号化した秘密鍵と対を成す公開鍵で署名を復号することによって証明書が改竄されていないことが検証できる。

【００３７】

第２のルート証明書Ｃａ２は、第２のルート認証機関の第２の公開鍵が含まれ、第２のルート認証機関の秘密鍵で署名されている。第１の相互認証証明書Ｍ１は、第２のルート認証機関の第２の公開鍵が含まれ、第１のルート認証機関の秘密鍵で署名されている。第２の相互認証証明書Ｍ２は、第１のルート認証機関の第１の公開鍵が含まれ、第２のルート認証機関の秘密鍵で署名されている。第１のサーバ証明書Ｓ１は、第１のサーバ装置１２０の公開鍵が含まれ、第１のルート認証機関の秘密鍵によって署名されている。

【００３８】

第１のサーバ装置１２０には、第２のサーバ装置１３０を表すサーバ情報がクライアント装置１１０によってネットワーク１０を介して送信されるようになっており、第１のサーバ装置１２０は、送信されたサーバ情報に表される第２のサーバ装置１３０の公開鍵を連鎖的に証明するルート証明書を要求するルート証明書要求情報を第２のサーバ装置１３０にネットワーク１０を介して送信するルート証明書要求情報送信手段１２２を更に備えている。ここで、サーバ情報には、第２のサーバ装置１３０のアドレス情報、および第２のサーバ装置１３０の公開鍵または第２のサーバ証明書Ｓ２等の第２のサーバ装置１３０

を識別するための情報が含まれる。

【００３９】

また、第１のサーバ装置１２０は、クライアント装置１１０を含む特定のクライアント装置に関する情報を記憶するクライアント記憶手段１２３を更にに備えている。クライアント記憶手段１２３は、証明書記憶手段１２１を構成する記憶媒体によって構成され、ルート証明書要求情報送信手段１２２によって送信されたルート証明書要求情報に応じて第２のサーバ装置１３０より返信された第２のルート証明書Ｃａ２をクライアント装置１１０に対応させて記憶するようになっている。

【００４０】

また、第１のサーバ装置１２０は、第１の相互認証証明書Ｍ１、第２のルート証明書Ｃａ２、第２の相互認証証明書Ｍ２、および第１のサーバ証明書Ｓ１よりなる証明書チェーンを生成する証明書チェーン生成手段１２４を更に備えている。

【００４１】

証明書チェーン生成手段１２４は、クライアント記憶手段１２３に記憶されたクライアント装置１１０に対応した第２のルート証明書Ｃａ２に基づいて第１の相互認証証明書Ｍ１および第２の相互認証証明書Ｍ２を証明書記憶手段１２１より取得し、証明書チェーンを生成するようになっている。

【００４２】

図３は、証明書チェーン生成手段１２４によって生成される証明書チェーンに関する検証の説明図である。

【００４３】

この証明書チェーンにおいて、第１の相互認証証明書Ｍ１に含まれる第２の公開鍵は、クライアント装置１１０に既に記憶されている第１のルート証明書Ｃａ１に含まれる第１の公開鍵によって検証することができ、第２のルート証明書Ｃａ２に含まれる第２の公開鍵は、第１の相互認証証明書Ｍ１に含まれる第２の公開鍵によって検証することができる。

【００４４】

また、第２の相互認証証明書Ｍ２に含まれる第１の公開鍵は、第２のルート証明書Ｃａ２に含まれる第２の公開鍵によって検証することができ、第１のサーバ証明書Ｓ１に含まれる第１のサーバ装置１２０の公開鍵は、第２の相互認証証明書Ｍ２に含まれる第１の公開鍵によって検証することができる。

【００４５】

なお、証明書チェーン生成手段１２４は、証明書チェーンを予め生成し、証明書記憶手段１２１を構成する記憶媒体に予め記憶しておくようにしてもよい。また、証明書チェーン生成手段１２４は、第１のルート証明書Ｃａ１を含むように証明書チェーンを生成するようにしてもよい。

【００４６】

証明書チェーン生成手段１２４は、クライアント装置１１０に対応したルート証明書がクライアント記憶手段１２３に記憶されていなかった場合には、第１のサーバ証明書Ｓ１よりなる証明書チェーン、すなわち第１のサーバ装置１２０の公開鍵を証明するためのみの証明書チェーンを生成するようになっている。

【００４７】

また、証明書チェーン生成手段１２４は、クライアント装置１１０に対応したルート証明書に対応する第１の相互認証証明書Ｍ１および第２の相互認証証明書Ｍ２が証明書記憶手段１２１に予め記憶されていない場合にも、第１のサーバ証明書Ｓ１よりなる証明書チェーンを生成するようになっている。

【００４８】

図２に戻り、第１のサーバ装置１２０は、証明書チェーン生成手段１２４によって生成された証明書チェーンをクライアント装置１１０にネットワーク１０を介して送信する証明書チェーン送信手段１２５を更に備えている。

【００４９】
なお、上述したように、クライアント装置１１０に対応したルート証明書に対応する第１の相互認証証明書Ｍ１および第２の相互認証証明書Ｍ２が証明書記憶手段１２１に予め記憶されていない場合には、証明書チェーン送信手段１２５は、証明書チェーンと共に第２のルート証明書Ｃａ２を配布できない旨のエラー情報をクライアント装置１１０にネットワーク１０を介して送信するようにしてもよい。
【００５０】
図４は、クライアント装置１１０の構成を示すブロック図である。
【００５１】
クライアント装置１１０は、ＣＰＵを有するコンピュータ装置によって構成されており、第１のルート証明書Ｃａ１を含むルート証明書を記憶するルート証明書記憶手段１１１と、サーバ情報を第１のサーバ装置１２０に送信するサーバ情報送信手段１１２と、証明書チェーン送信手段１２５によって送信された証明書チェーンに含まれる各証明書をルート証明書記憶手段１１１に記憶されたルート証明書に基づいて順次検証する証明書検証手段１１３と、証明書検証手段１１３によって証明書チェーンに含まれる各証明書が正当なものであると検証された場合に証明書チェーンに含まれる第２のルート証明書Ｃａ２をルート証明書記憶手段１１１に記憶させるルート証明書登録手段１１４とを備えている。なお、ルート証明書記憶手段１１１は、コンピュータ装置を構成するハードディスク装置やフラッシュメモリ等の不揮発性の記録媒体によって構成されている。
【００５２】
クライアント装置１１０が第２のサーバ装置１３０の第２のサーバ証明書Ｓ２を検証する際に、第２のルート認証機関がクライアント装置１１０の利用者に信頼されていない、すなわち第２のルート証明書Ｃａ２がルート証明書記憶手段１１１に記憶されていない場合には、サーバ情報送信手段１１２は、サーバ情報を第１のサーバ装置１２０にネットワーク１０を介して送信するようになっている。
【００５３】
証明書検証手段１１３は、証明書チェーンに基づいてルート証明書記憶手段１１１に記憶された第１のルート証明書Ｃａ１に含まれる第１の公開鍵で第１の相互認証証明書Ｍ１を検証し、第１の相互認証証明書Ｍ１に含まれる第２の公開鍵で第２のルート証明書Ｃａ２を検証し、第２のルート証明書Ｃａ２に含まれる第２の公開鍵で第２の相互認証証明書Ｍ２に含まれる第１の公開鍵を検証し、第２の相互認証証明書Ｍ２に含まれる第１の公開鍵で第１のサーバ証明書Ｓ１に含まれる公開鍵を検証することができる。
【００５４】
すなわち、証明書検証手段１１３は、第１のサーバ証明書Ｓ１に含まれる公開鍵を検証すると共に、第２のルート証明書Ｃａ２を検証することができる。なお、証明書検証手段１１３は、上述したように署名によって各証明書を検証するほかに、各証明書の有効期間が満了しているか否か、およびＸ．５０９によって規格化された証明書廃棄リスト（Certificate Revocation List、ＣＲＬとも称する）に各証明書が含まれているか否かにも基づいて各証明書を検証するようになっている。
【００５５】
なお、証明書検証手段１１３によって第２のルート証明書Ｃａ２が正当なものであると検証され、ルート証明書登録手段１１４によって第２のルート証明書Ｃａ２がルート証明書記憶手段１１１に記憶される際に、クライアント装置１１０を構成するコンピュータ装置を構成する出力装置を介して第２のルート証明書Ｃａ２を登録する旨を出力し、第２のルート証明書Ｃａ２をルート証明書記憶手段１１１に記憶させることの可否をクライアント装置１１０の利用者に問い合わせるようにしてもよい。
【００５６】
また、第２のルート証明書Ｃａ２がルート証明書記憶手段１１１に登録された際には、サーバ情報送信手段１１２は、第１のサーバ装置１２０のクライアント記憶手段１２３にクライアント装置１１０と対応して記憶された第２のルート証明書Ｃａ２の抹消を要求す

る旨のサーバ情報を送信するようになっており、以降のクライアント装置１１０からの公開鍵認証時には、第１のサーバ装置１２０の公開鍵を証明するのみの証明書チェーンを第１のサーバ装置１２０に送信させるようになっている。

【００５７】

図５は、第２のサーバ装置１３０の構成を示すブロック図である。

【００５８】

第２のサーバ装置１３０は、ＣＰＵを有するコンピュータ装置によって構成されており、証明書を記憶する証明書記憶手段１３１を備えている。

【００５９】

証明書記憶手段１３１は、コンピュータ装置を構成するハードディスク装置やフラッシュメモリ等の不揮発性の記憶媒体によって構成され、証明書記憶手段１３１には、第２のルート証明書、および第２のサーバ証明書Ｓ２を含み第２のルート証明書Ｃａ２によって連鎖的に証明される一連の証明書が第２のサーバ装置１３０の管理者によって予め記憶されている。

【００６０】

また、第２のサーバ装置１３０は、第２のサーバ証明書Ｓ２を含み第２のルート証明書Ｃａ２によって連鎖的に証明される一連の証明書よりなる証明書チェーンを生成する証明書チェーン生成手段１３２と、証明書チェーン生成手段１３２によって生成された証明書チェーンをクライアント装置１１０に送信する証明書チェーン送信手段１３３を更に備え、第２のサーバ装置１３０の公開鍵を他の装置に認証させるようになっている。

【００６１】

また、第２のサーバ装置１３０は、第１のサーバ装置１２０のルート証明書要求情報送信手段１２２によって送信されたルート証明書要求情報に応じて第２のルート証明書Ｃａ２を第１のサーバ装置１２０に送信するルート証明書送信手段１３４を更に備えている。

【００６２】

次に、ルート証明書配布システム１００の動作について図６～図８に示すフローチャートを参照して説明する。

【００６３】

まず、図６に示すフローチャートを参照して、第１のサーバ装置１２０のサーバ情報受信動作について説明する。クライアント装置１１０のサーバ情報送信手段１１２によってネットワーク１０を介して送信されたサーバ情報は、第１のサーバ装置１２０のルート証明書要求情報送信手段１２２によって受信される（ステップＳ１１０）。

【００６４】

次に、ルート証明書要求情報送信手段１２２によって受信されたサーバ情報に第２のサーバ装置１３０を識別するための情報が含まれているか否かがルート証明書要求情報送信手段１２２によって判断され（ステップＳ１２０）、第２のサーバ装置１３０を識別するための情報が含まれていない、すなわちクライアント装置１１０と対応した第２のルート証明書Ｃａ２の抹消と判断された場合には、クライアント記憶手段１２３にクライアント装置１１０と対応して記憶された第２のルート証明書Ｃａ２がルート証明書要求情報送信手段１２２によって抹消される（ステップＳ１３０）。

【００６５】

一方、ルート証明書要求情報送信手段１２２によって受信されたサーバ情報に第２のサーバ装置１３０を識別するための情報が含まれている、すなわちクライアント装置１１０と対応した第２のルート証明書Ｃａ２の登録と判断された場合には、サーバ情報に表される第２のサーバ装置１３０の公開鍵を連鎖的に証明するルート証明書を要求するルート証明書要求情報が、第２のサーバ装置１３０にネットワーク１０を介してルート証明書要求情報送信手段１２２によって送信される（ステップＳ１４０）。

【００６６】

ルート証明書要求情報送信手段１２２によって送信されたルート証明書要求情報に応じて第２のサーバ装置１３０のルート証明書送信手段１３４によって送信された第２のルー

ト証明書Ｃａ２は、ネットワーク１０を介してクライアント記憶手段１２３によって受信され（ステップＳ１５０）、受信された第２のルート証明書Ｃａ２がクライアント装置１１０に対応させてクライアント記憶手段１２３に記憶される（ステップＳ１６０）。

【００６７】

次に、図７に示すフローチャートを参照して、第１のサーバ装置１２０の証明書チェーン送信動作について説明する。

【００６８】

まず、クライアント装置１１０との公開鍵認証時において、クライアント装置１１０と対応するルート証明書がクライアント記憶手段１２３に記憶されているか否かが証明書チェーン生成手段１２４によって判断される（ステップＳ２１０）。

【００６９】

クライアント装置１１０と対応するルート証明書がクライアント記憶手段１２３に記憶されていると判断された場合には、クライアント記憶手段１２３に記憶されたクライアント装置１１０に対応した第２のルート証明書Ｃａ２に基づいて第１の相互認証証明書Ｍ１および第２の相互認証証明書Ｍ２が証明書記憶手段１２１に記憶されているか否かが証明書チェーン生成手段１２４によって判断される（ステップＳ２２０）。

【００７０】

第１の相互認証証明書Ｍ１および第２の相互認証証明書Ｍ２が証明書記憶手段１２１に記憶されていると判断された場合には、クライアント記憶手段１２３に記憶されたクライアント装置１１０に対応した第２のルート証明書Ｃａ２に基づいて第１の相互認証証明書Ｍ１、第２のルート証明書Ｃａ２、第２の相互認証証明書Ｍ２、および第１のサーバ証明書Ｓ１よりなる証明書チェーンが証明書チェーン生成手段１２４によって生成される（ステップＳ２３０）。

【００７１】

一方、クライアント装置１１０と対応するルート証明書がクライアント記憶手段１２３に記憶されていない、または第１の相互認証証明書Ｍ１および第２の相互認証証明書Ｍ２が証明書記憶手段１２１に記憶されていないと判断された場合には、第１のサーバ証明書Ｓ１よりなる証明書チェーンが証明書チェーン生成手段１２４によって生成される（ステップＳ２４０）。

【００７２】

証明書チェーン生成手段１２４によって生成された証明書チェーンは、クライアント装置１１０にネットワーク１０を介して証明書チェーン送信手段１２６によって送信される（ステップＳ２５０）。

【００７３】

次に、図８に示すフローチャートを参照して、クライアント装置１１０の公開鍵認証動作について説明する。

【００７４】

まず、第１のサーバ装置１２０の証明書チェーン送信手段１２５によって送信された証明書チェーンに含まれる各証明書、すなわち第１の相互認証証明書Ｍ１、第２のルート証明書Ｃａ２、第２の相互認証証明書Ｍ２、および第１のサーバ証明書Ｓ１よりなる証明書チェーンの各証明書は、ルート証明書記憶手段１１１に記憶された第１のルート証明書Ｃａ１に含まれる公開鍵に基づいて証明書検証手段１１３によって順次検証される（ステップＳ３１０～Ｓ３４０）。

【００７５】

すなわち、証明書チェーンに含まれる第１の相互認証証明書Ｍ１をルート証明書記憶手段１１１に記憶された第１のルート証明書Ｃａ１に含まれる第１の公開鍵で検証し、第１の相互認証証明書Ｍ１に含まれる第２の公開鍵で第２のルート証明書Ｃａ２を検証し、第２のルート証明書Ｃａ２に含まれる第２の公開鍵で第２の相互認証証明書Ｍ２に含まれる第１の公開鍵を検証し、第２の相互認証証明書Ｍ２に含まれる第１の公開鍵で第１のサーバ証明書Ｓ１に含まれる公開鍵を検証するというように順次検証を行う（ステップＳ３１

０）。
【００７６】
この順次検証において、証明書検証手段１１３によって第１のサーバ証明書Ｓ１が正当なものであると検証された場合（ステップＳ３２０）には、第１のサーバ証明書Ｓ１に含まれる公開鍵が第１のサーバ装置１２０のものであることが証明されたこととなる（ステップＳ３３０）。
【００７７】
一方、証明書チェーン送信手段１２５によって送信された証明書チェーンに含まれる各証明書を順次検証した結果、第１のサーバ証明書Ｓ１が正当なものであると検証されなかった場合には、第１のサーバ証明書Ｓ１に含まれる公開鍵が第１のサーバ装置１２０のものであることが証明されなかったこととなる（ステップＳ３４０）。
【００７８】
また、ステップＳ３２０における判定において、第１のサーバ証明書Ｓ１が正当なものであると検証されなかった場合において、前記順次検証の途中までの検証において第２のルート証明書Ｃａ２が正当なものであると検証された場合（ステップＳ３５０）には、第２のルート証明書Ｃａ２がルート証明書登録手段１１４によってルート証明書記憶手段１１１に記憶される（ステップＳ３６０）。
【００７９】
また、ステップＳ３５０における判定において、第２のルート証明書Ｃａ２が正当なものであると検証されなかった場合には、第１のサーバ証明書Ｓ１に含まれる公開鍵が第１のサーバ装置１２０のものであることが証明されなかったこととなる（ステップＳ３４０）。
【００８０】
上述したルート証明書配布システム１００を構成するクライアント装置１１０、第１のサーバ装置１２０、および第２のサーバ装置１３０の各構成要素は、上記で説明した各動作を記述したプログラムを各ＣＰＵに実行させるようにしてもよい。すなわち、クライアント装置１１０を構成するサーバ情報送信手段１１２、証明書検証手段１１３、およびルート証明書登録手段１１４は、上記プログラムを実行するＣＰＵによって構成するようにしてもよい。また、第１のサーバ装置１２０を構成するルート証明書要求情報送信手段１２２、証明書チェーン生成手段１２４、および証明書チェーン送信手段１２５は、上記プログラムを実行するＣＰＵによって構成するようにしてもよい。また、第２のサーバ装置１３０を構成する証明書チェーン生成手段１３２、証明書チェーン送信手段１３３、およびルート証明書送信手段１３４は、上記プログラムを実行するＣＰＵによって構成するようにしてもよい。
【００８１】
以上説明したように、本実施形態によれば、クライアント装置１１０の利用者によって信頼されていない第２のルート認証機関の第２のルート証明書Ｃａ２を含めた証明書チェーンで第１のサーバ装置１２０の公開鍵を認証させるため、クライアント装置１１０側で相互認証証明書を取得する手間を生じさせることなく、クライアント装置１１０に信頼されていない第２のルート認証機関を信頼させることができる。
【００８２】
（第２の実施形態）
図９は、本発明の第２の実施形態に係るルート証明書配布システム２００の構成を示すブロック図である。
【００８３】
ルート証明書配布システム２００は、ネットワーク１０に接続され、第１のルート認証機関の第１の公開鍵を証明する第１のルート証明書Ｃａ１に基づいて利用者が第１のルート認証機関を信頼するクライアント装置２１０と、クライアント装置１１０の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明する第２のルート証明書Ｃａ２に基づいて証明されるサーバ証明書Ｓによって公開鍵を証明するサーバ装置２３

０とを備えている。
【００８４】
なお、本実施形態のルート証明書配布システム２００は、複数のクライアント装置２１０および複数のサーバ装置２３０によって構成することができるが、説明を簡単にするために１つのクライアント装置２１０、１つのサーバ装置２３０によって構成されるものとして以下説明する。
【００８５】
図１０は、サーバ装置２３０の構成を示すブロック図である。
【００８６】
サーバ装置２３０は、ＣＰＵを有するコンピュータ装置によって構成されており、証明書を記憶する証明書記憶手段２３１を備えている。証明書記憶手段２３１は、コンピュータ装置を構成するハードディスク装置やフラッシュメモリ等の不揮発性の記憶媒体によって構成され、証明書記憶手段２３１には、サーバ証明書Ｓを含み第２のルート証明書Ｃａ２によって連鎖的に証明される一連の証明書がサーバ装置２３０の管理者によって予め記憶されている。ここで、サーバ証明書Ｓを含み第２のルート証明書Ｃａ２によって連鎖的に証明される一連の証明書には、説明を簡単にするためにサーバ証明書Ｓのみが含まれるものとする。
【００８７】
また、第１のルート認証機関と第２のルート認証機関とが相互に信頼関係を結んだ場合には、第１のルート証明書Ｃａ１、および第２の公開鍵を証明し第１の公開鍵と対を成す秘密鍵を以って署名された相互認証証明書Ｍがサーバ装置２３０の管理者によって証明書記憶手段２３１に記憶される。
【００８８】
ここで、第１のルート証明書Ｃａ１は、第１のルート認証機関の第１の公開鍵が含まれ、第１のルート認証機関の秘密鍵で署名されており、クライアント装置１１０に既に記憶されている。第２のルート証明書Ｃａ２は、第２のルート認証機関の第２の公開鍵が含まれ、第２のルート認証機関の秘密鍵で署名されている。相互認証証明書Ｍは、第２のルート認証機関の第２の公開鍵が含まれ、第１のルート認証機関の秘密鍵で署名されている。サーバ証明書Ｓは、サーバ装置２３０の公開鍵が含まれ、第２のルート認証機関の秘密鍵によって署名されている。
【００８９】
サーバ装置２３０の公開鍵認証時には、第１のルート証明書Ｃａ１がクライアント装置１１０によってネットワーク１０を介して送信されるようになっており、サーバ装置２３０は、相互認証証明書Ｍ、第２のルート証明書Ｃａ２、およびサーバ証明書Ｓよりなる証明書チェーンを生成する証明書チェーン生成手段２３２を更に備えている。
【００９０】
証明書チェーン生成手段２３２は、クライアント装置２１０によって送信された第１のルート証明書Ｃａ１に基づいて相互認証証明書Ｍを証明書記憶手段２３１より取得し、証明書チェーンを生成するようになっている。
【００９１】
図１１は、証明書チェーン生成手段２３２によって生成される証明書チェーンに関する検証の説明図である。
【００９２】
この証明書チェーンにおいて、相互認証証明書Ｍに含まれる第２の公開鍵は、クライアント装置２１０に既に記憶されている第１のルート証明書Ｃａ１に含まれる第１の公開鍵によって検証することができ、第２のルート証明書Ｃａ２に含まれる第２の公開鍵は、相互認証証明書Ｍに含まれる第２の公開鍵によって検証することができ、サーバ証明書Ｓに含まれるサーバ装置２３０の公開鍵は、第２のルート証明書Ｃａ２に含まれる第２の公開鍵によって検証することができる。
【００９３】

なお、証明書チェーン生成手段２３２は、証明書チェーンを予め生成し、証明書記憶手段２３１を構成する記憶媒体に予め記憶しておくようにしてもよい。また、証明書チェーン生成手段２３２は、第１のルート証明書Ｃａ１を含むように証明書チェーンを生成するようにしてもよい。

【００９４】

証明書チェーン生成手段２３２は、サーバ装置２３０の公開鍵認証時にクライアント装置２１０から第１のルート証明書Ｃａ１が送信されなかった場合には、サーバ証明書Ｓよりなる証明書チェーン、すなわちサーバ装置２３０の公開鍵を証明するためのみの証明書チェーンを生成するようになっている。

【００９５】

また、証明書チェーン生成手段２３２は、相互認証証明書Ｍが証明書記憶手段２３１に記憶されていない場合にも、サーバ証明書Ｓよりなる証明書チェーンを生成するようになっている。

【００９６】

なお、サーバ装置２３０の公開鍵認証時に、クライアント装置２１０が複数のルート証明書を送信するようにしてもよい。この場合には、証明書チェーン生成手段２３２は、対応する相互認証証明書が証明書記憶手段２３１に記憶されたルート証明書を選択し、選択したルート証明書に基づいて証明書チェーンを生成するように構成する。

【００９７】

図１０に戻り、サーバ装置２３０は、証明書チェーン生成手段２３２によって生成された証明書チェーンをクライアント装置２１０にネットワーク１０を介して送信する証明書チェーン送信手段２３３を更に備えている。

【００９８】

図１２は、クライアント装置２１０の構成を示すブロック図である。

【００９９】

クライアント装置２１０は、ＣＰＵを有するコンピュータ装置によって構成されており、第１のルート証明書Ｃａ１を含むルート証明書を記憶するルート証明書記憶手段２１１と、第１のルート証明書Ｃａ１をサーバ装置２３０に送信するルート証明書送信手段２１２と、証明書チェーン送信手段２３３によって送信された証明書チェーンに含まれる各証明書をルート証明書記憶手段２１１に記憶されたルート証明書に基づいて順次検証する証明書記憶手段２１３と、証明書記憶手段２１３によって証明書チェーンに含まれる各証明書が正当なものであると検証された場合に証明書チェーンに含まれる第２のルート証明書Ｃａ２をルート証明書記憶手段２１１に記憶させるルート証明書登録手段２１４とを備えている。

【０１００】

ルート証明書記憶手段２１１は、コンピュータ装置を構成するハードディスク装置やフラッシュメモリ等の不揮発性の記憶媒体によって構成されている。ルート証明書送信手段２１２は、サーバ装置２３０の公開鍵認証時にルート証明書記憶手段２１１に記憶された第１のルート証明書Ｃａ１をサーバ装置２３０にネットワーク１０を介して送信するようになっている。なお、ルート証明書送信手段２１２は、ルート証明書記憶手段２１１に複数のルート証明書が記憶されている場合には、複数のルート証明書を送信するようにしてもよい。

【０１０１】

また、ルート証明書送信手段２１２は、第２のルート証明書Ｃａ２がルート証明書記憶手段２１１に登録されている場合には、第１のルート証明書Ｃａ１の送信を行わないようにしてもよい。

【０１０２】

証明書検証手段２１３は、証明書チェーンに基づいてルート証明書記憶手段２１１に記憶された第１のルート証明書Ｃａ１に含まれる第１の公開鍵で相互認証証明書Ｍを検証し、相互認証証明書Ｍに含まれる第２の公開鍵で第２のルート証明書Ｃａ２を検証し、第２

のルート証明書Ｃａ２に含まれる第２の公開鍵でサーバ証明書Ｓに含まれる公開鍵を検証することができる。

【０１０３】

すなわち、証明書検証手段２１３は、サーバ証明書Ｓに含まれる公開鍵を検証すると共に、第２のルート証明書Ｃａ２を検証することができる。なお、証明書検証手段２１３は、上述したように署名によって各証明書を検証するほかに、各証明書の有効期間が満了しているか否か、およびＸ．５０９によって規格化された証明書廃棄リストに各証明書が含まれているか否かにも基づいて各証明書を検証するようになっている。

【０１０４】

なお、証明書検証手段２１３によって第２のルート証明書Ｃａ２が正当なものであると検証され、ルート証明書登録手段２１４によって第２のルート証明書Ｃａ２がルート証明書記憶手段２１１に記憶される際に、クライアント装置２１０を構成するコンピュータ装置を構成する出力装置を介して第２のルート証明書Ｃａ２を登録する旨を出力し、第２のルート証明書Ｃａ２をルート証明書記憶手段２１１に記憶させることの可否をクライアント装置２１０の利用者に問い合わせるようにしてもよい。

【０１０５】

次に、ルート証明書配布システム２００の動作について図１３～図１４に示すフローチャートを参照して説明する。

【０１０６】

まず、図１３に示すフローチャートを参照して、サーバ装置２３０の証明書チェーン送信動作について説明する。クライアント装置２１０との公開鍵認証時において、クライアント装置２１０のルート証明書送信手段２１２によって送信された第１のルート証明書Ｃａ１が受信されたか否かが証明書チェーン生成手段２３２によって判断される（ステップＳ４１０）。

【０１０７】

サーバ装置２３０の証明書チェーン生成手順２３２によって第１のルート証明書Ｃａ１が受信されたと判断された場合には、相互認証証明書Ｍが証明書記憶手段２３１に記憶されているか否かが証明書チェーン生成手段２３２によって判断される（ステップＳ４２０）。ここで、証明書チェーン生成手段２３２によって複数のルート証明書が受信された場合には、いずれか１つのルート証明書と対応する相互認証証明書が証明書記憶手段２３１に記憶されているか否かが判断される。

【０１０８】

相互認証証明書Ｍが証明書記憶手段２３１に記憶されていると判断された場合には、相互認証証明書Ｍ、第２のルート証明書Ｃａ２、およびサーバ証明書Ｓよりなる証明書チェーンが証明書チェーン生成手段２３２によって生成される（ステップＳ４３０）。

【０１０９】

一方、サーバ装置２３０の証明書チェーン生成手段２３２によって第１のルート証明書Ｃａ１が受信されていない、または相互認証証明書Ｍが証明書記憶手段２３１に記憶されていないと判断された場合には、第１のサーバ証明書Ｓ１よりなる証明書チェーンが証明書チェーン生成手段２３２によって生成される（ステップＳ４４０）。

【０１１０】

証明書チェーン生成手段２３２によって生成された証明書チェーンは、ネットワーク１０を介して証明書チェーン送信手段２３３によってクライアント装置２１０に送信される（ステップＳ４５０）。

【０１１１】

次に、図１４に示すフローチャートを参照して、クライアント装置２１０の公開鍵認証動作について説明する。

【０１１２】

サーバ装置２３０の証明書チェーン送信手段２３３によって送信された証明書チェーンに含まれる各証明書、すなわち相互認証証明書Ｍ、第２のルート証明書Ｃａ２、およびサ

ーバ証明書Ｓよりなる証明書チェーンの各証明は、ルート証明書記憶手段２１１に記憶されたルート証明書に含まれる公開鍵に基づいて証明書検証手段２１３によって順次検証される（ステップＳ５１０～Ｓ５４０）。

【０１１３】

すなわち、証明書チェーンに含まれる第１の相互認証証明書Ｍ１をルート証明書記憶手段２１１に記憶された第１のルート証明書Ｃａ１に含まれる第１の公開鍵で検証し、相互認証証明書Ｍに含まれる第２の公開鍵で第２のルート証明書Ｃａ２を検証し、第２のルート証明書Ｃａ２に含まれる第２の公開鍵でサーバ証明書Ｓに含まれる公開鍵で検証するというように順次検証を行う（ステップＳ５１０）。

【０１１４】

この順次検証において、証明書検証手段２１３によってサーバ証明書Ｓが正当なものであると検証された場合には（ステップＳ５２０）、サーバ証明書Ｓに含まれる公開鍵がサーバ装置２３０のものであることが証明されたこととなる（ステップＳ５３０）。一方、証明書チェーン送信手段２３３によって送信された証明書チェーンに含まれる各証明書を順次検証した結果、サーバ証明書Ｓが正当なものであると検証されなかった場合には、サーバ証明書Ｓに含まれる公開鍵がサーバ装置２３０のものであることが証明されなかったこととなる（ステップＳ５４０）。

【０１１５】

また、ステップＳ５２０における判定において、サーバ証明書が正当なものであると検証されなかった場合において、前記順次検証の途中までの検証において第２のルート証明書Ｃａ２が正当なものであると検証された場合（ステップＳ５５０）には、第２のルート証明書Ｃａ２がルート証明書登録手段１１４によってルート証明書記憶手段１１１に記憶される（ステップＳ５６０）。

【０１１６】

また、ステップＳ５５０における判定において、第２のルート証明書Ｃａ２が正当なものであると検証されなかった場合には、サーバ証明書Ｓに含まれる公開鍵がサーバ装置１２０のものであることが証明されなかったこととなる（ステップＳ５４０）。

【０１１７】

また、証明書検証手段２１３によって第２のルート証明書Ｃａ２が正当なものであると検証された場合には（ステップＳ５５０）、第２のルート証明書Ｃａ２がルート証明書登録手段２１４によってルート証明書記憶手段２１１に記憶される（ステップＳ５６０）。

【０１１８】

上述したルート証明書配布システム２００を構成するクライアント装置２１０およびサーバ装置２３０の各構成要素は、上記で説明した各動作を記述したプログラムを各ＣＰＵに実行させるようにしてもよい。すなわち、クライアント装置２１０を構成するルート証明書送信手段２１２、証明書検証手段２１３、およびルート証明書登録手段２１４は、上記プログラムを実行するＣＰＵによって構成するようにしてもよい。また、サーバ装置２３０を構成する証明書チェーン生成手段２３２、および証明書チェーン送信手段２３３は、上記プログラムを実行するＣＰＵによって構成するようにしてもよい。

【０１１９】

以上説明したように、本実施形態によれば、クライアント装置２１０の利用者によって信頼されていない第２のルート認証機関の第２の公開鍵を証明しクライアント装置２１０の利用者によって信頼された第１のルート認証機関の第１の公開鍵と対をなす秘密鍵を以って署名された相互認証証明書Ｍとクライアント装置２１０の利用者によって信頼されていない第２のルート認証機関の第２のルート証明書Ｃａ２を含めた証明書チェーンでサーバ装置２３０の公開鍵を認証させるため、クライアント装置２１０側で相互認証証明書を取得する手間を生じさせることなく、サーバ装置２３０の公開鍵を認証させることができ、クライアント装置２１０に信頼されていない第２のルート認証機関を信頼させることができる。

【０１２０】

なお、上記実施形態の処理手順をプログラムとして例えばＣＤやＦＤなどの記録媒体に記録して、この記録媒体をコンピュータシステムに組み込んだり、または記録媒体に記録されたプログラムを通信回線を介してコンピュータシステムにダウンロードしたり、または記録媒体からインストールし、該プログラムでコンピュータシステムを作動させることにより、該処理手順を実施するシステムとして機能させることができることは勿論であり、このような記録媒体を用いることにより、その流通性を高めることができるものである。

【図面の簡単な説明】

【０１２１】

【図１】本発明の第１の実施形態に係るルート証明書配布システムの構成を示すブロック図である。

【図２】図１に示す第１の実施形態のルート証明書配布システムに使用されている第１のサーバ装置の構成を示すブロック図である。

【図３】第１の実施形態に係る第１のサーバ装置を構成する証明書チェーン生成手段によって生成される証明書チェーンに関する検証の説明図である。

【図４】図１に示す第１の実施形態のルート証明書配布システムに使用されているクライアント装置の構成を示すブロック図である。

【図５】図１に示す第１の実施形態のルート証明書配布システムに使用されている第２のサーバ装置の構成を示すブロック図である。

【図６】第１の実施形態に係る第１のサーバ装置のサーバ情報受信動作を示すフローチャートである。

【図７】第１の実施形態に係る第１のサーバ装置の証明書チェーン送信動作を示すフローチャートである。

【図８】第１の実施の形態に係るクライアント装置の公開鍵認証動作を示すフローチャートである。

【図９】本発明の第２の実施形態に係るルート証明書配布システムの構成を示すブロック図である。

【図１０】図９に示す第２の実施形態のルート証明書配布システムに使用されているサーバ装置の構成を示すブロック図である。

【図１１】第２の実施形態に係るサーバ装置を構成する証明書チェーン生成手段によって生成される証明書チェーンに関する検証の説明図である。

【図１２】図９に示す第２の実施形態のルート証明書配布システムに使用されているクライアント装置の構成を示すブロック図である。

【図１３】第２の実施形態に係るサーバ装置の証明書チェーン送信動作を示すフローチャートである。

【図１４】第２の実施形態に係るクライアント装置の公開鍵認証動作を示すフローチャートである。

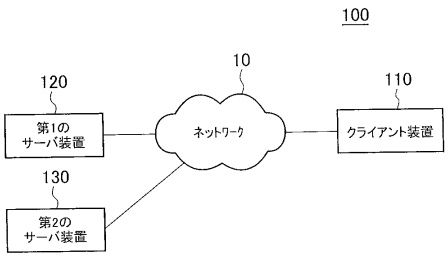
【符号の説明】

【０１２２】

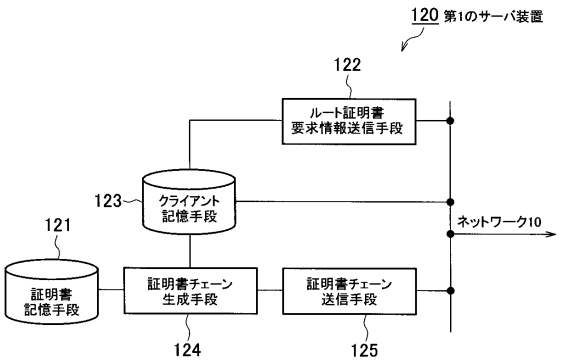
１０　　ネットワーク
１００、２００　　ルート証明書配布システム
１１０、２１０　　クライアント装置
１１１、２１１　　ルート証明書記憶手段
１１２　　サーバ情報送信手段
１１３、２１３　　証明書検証手段
１１４、２１４　　ルート証明書登録手段
１２０　　第１のサーバ装置
１２１、１３１、２３１　　証明書記憶手段
１２２　　ルート証明書要求情報送信手段
１２３　　クライアント記憶手段

１２４、１３２、２３２　　証明書チェーン生成手段
１２５、１３３、２３３　　証明書チェーン送信手段
１３０　　第２のサーバ装置
１３４、２１２　　ルート証明書送信手段
２３０　　サーバ装置

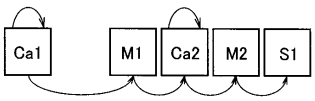
【図１】



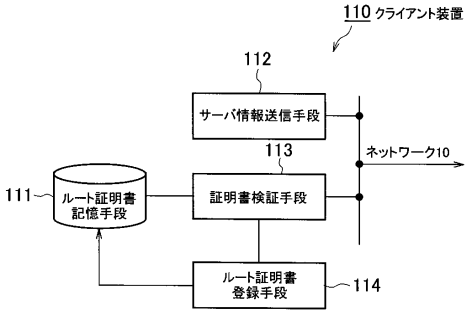
【図２】



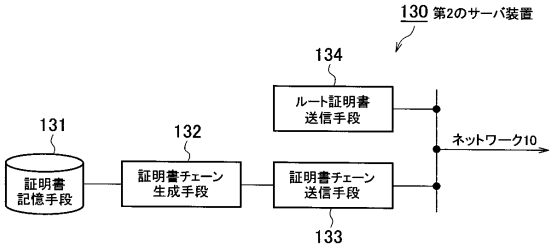
【図３】



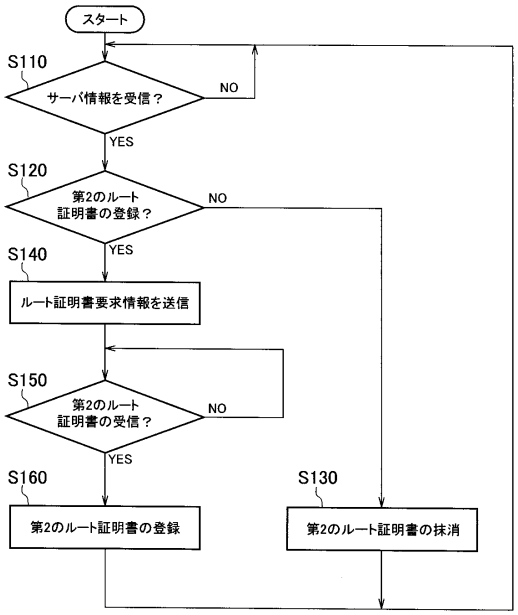
【図４】



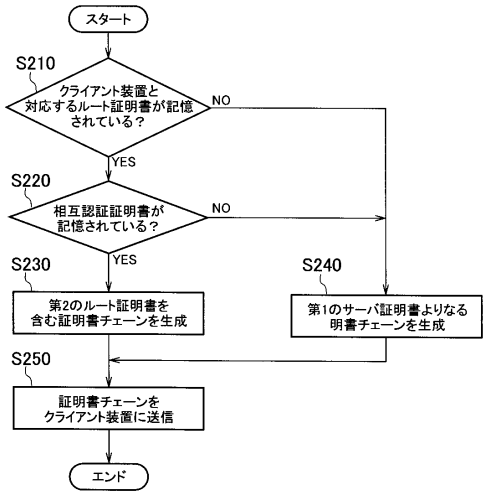
【図５】



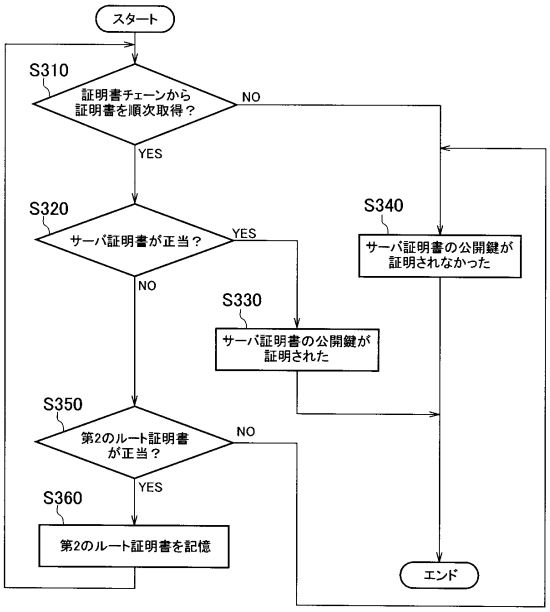
【図６】



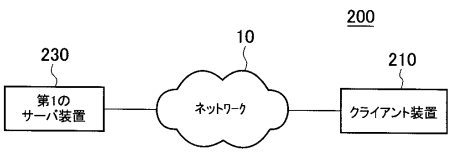
【図７】



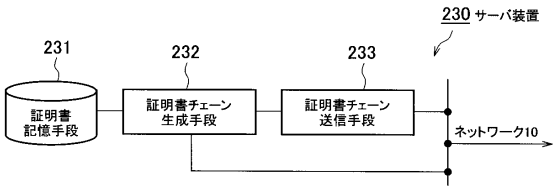
【図８】



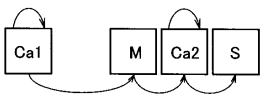
【図９】



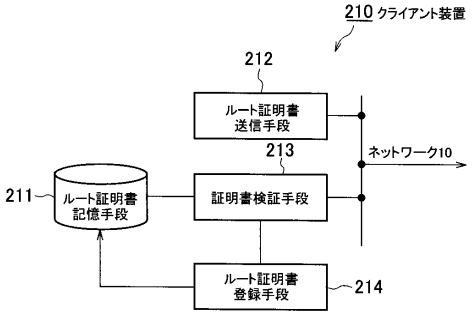
【図１０】



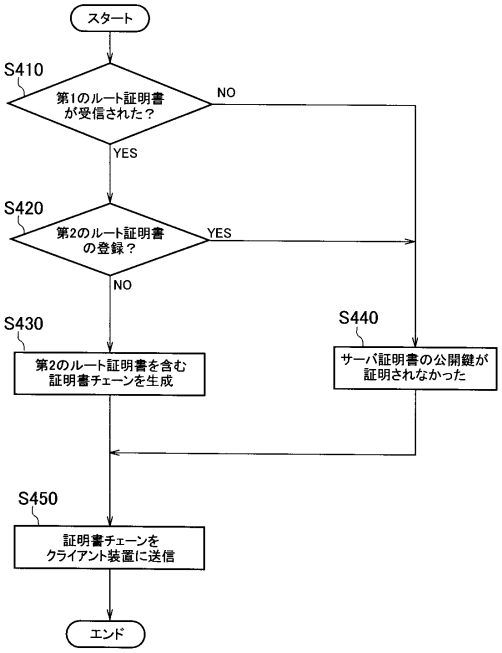
【図１１】



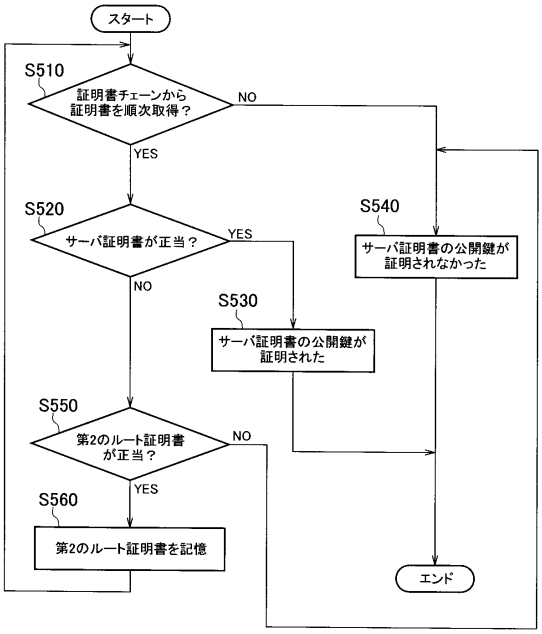
【図１２】



【図１３】


スタート
S410
第1のルート証明書が受信された？
NO
YES
S420
第2のルート証明書の登録？
YES
NO
S430
第2のルート証明書を含む証明書チェーンを生成
S440
サーバ証明書の公開鍵が証明されなかった
S450
証明書チェーンをクライアント装置に送信
エンド

【図１４】


スタート
S510
証明書チェーンから証明書を順次取得？
NO
YES
S520
サーバ証明書が正当？
YES
NO
S530
サーバ証明書の公開鍵が証明された
S540
サーバ証明書の公開鍵が証明されなかった
S550
第2のルート証明書が正当？
NO
YES
S560
第2のルート証明書を記憶
エンド

フロントページの続き

(56)参考文献 特開２００１－３１８６０１（ＪＰ，Ａ）
特開２００１－０８６１１２（ＪＰ，Ａ）
特開２００２－２１７９０１（ＪＰ，Ａ）
特開２００３－１５２７１８（ＪＰ，Ａ）
特開２０００－０１０４７７（ＪＰ，Ａ）
特表２００６－５００６５２（ＪＰ，Ａ）
特開２００５－１１７２７７（ＪＰ，Ａ）
特開２００２－０７２８７６（ＪＰ，Ａ）
特開２００１－３５０４０６（ＪＰ，Ａ）
特開平１１－３０８２１４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　９／０８
Ｇ０９Ｃ　１／００