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

特許第5556180号
(P5556180)

(45)発行日　平成26年7月23日(2014.7.23)　(24)登録日　平成26年6月13日(2014.6.13)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675D
G09C 1/00	(2006.01)	G09C	1/00	640E
G06F 21/14	(2013.01)	G09C	1/00	640D
G06F 21/62	(2013.01)	G06F	21/22	114C
		G06F	21/24	166A

請求項の数 5　(全 20 頁)

(21)出願番号　特願2009-550489 (P2009-550489)
(86)(22)出願日　平成21年1月8日(2009.1.8)
(86)国際出願番号　PCT/JP2009/050127
(87)国際公開番号　WO2009/093485
(87)国際公開日　平成21年7月30日(2009.7.30)
審査請求日　平成23年7月5日(2011.7.5)
(31)優先権主張番号　特願2008-13728 (P2008-13728)
(32)優先日　平成20年1月24日(2008.1.24)
(33)優先権主張国　日本国(JP)

前置審査

(73)特許権者　000001270
コニカミノルタ株式会社
東京都千代田区丸の内二丁目７番２号
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　吉田　宏樹
東京都日野市さくら町１番地　コニカミノルタテクノロジーセンター株式会社内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】電子証明書を用いた認証に係るネットワークシステム、認証サーバ装置および認証方法

(57)【特許請求の範囲】

【請求項１】

互いにデータ通信可能に構成された複数の認証サーバ装置（ＣＡ１，ＣＡ２）と、

少なくとも１つのクライアント（ＰＣ１）とを備え、

前記複数の認証サーバ装置の各々は、予め定められた独自の鍵ペア（２０６ｃ）の一方を用いて、前記クライアントからの証明書発行要求に応じて電子証明書を発行するための証明書発行部（２０６ａ）を含み、

前記複数の認証サーバ装置のうち第１の認証サーバ装置（ＣＡ１）は、

自身が発行した電子証明書に対して、自身の鍵ペアの他方を用いて認証を行なうための認証検証部（２０６ｂ）と、

第２の認証サーバ装置（ＣＡ２）が発行した電子証明書に対して、前記第２の認証サーバ装置の鍵ペアの他方を用いて認証が行なわれた結果内容を、格納するための認証リスト記憶部（２１２）とを含み、

前記認証検証部は、前記第２の認証サーバ装置が発行した電子証明書に対して、前記結果内容を参照して認証を行ない、

前記認証検証部は、前記クライアントから受信した前記電子証明書についての発行元を判断し、自身が発行元ではない場合に、発行元の認証サーバ装置へ前記電子証明書を転送し、

前記複数の認証サーバ装置のうち前記電子証明書の発行元の認証サーバ装置は、前記第１の認証サーバ装置から前記電子証明書を受信した場合に、自身の鍵ペアの他方を用いて

認証を行ない、その結果内容を応答する応答部（２０８）を含む、ネットワークシステム。

【請求項２】

前記認証検証部は、前記発行元の認証サーバ装置が予め定められた連携先である場合に限って、前記電子証明書を前記発行元の認証サーバ装置へ転送する、請求項１に記載のネットワークシステム。

【請求項３】

前記認証リスト記憶部は、クライアントの識別情報に対応付けて、前記クライアントに発行されている前記電子証明書の内容、前記電子証明書の有効期限、前記電子証明書の許可範囲のうち少なくとも１つを格納する、請求項１に記載のネットワークシステム。

【請求項４】

他の認証サーバ装置（ＣＡ２）およびクライアント（ＰＣ１－ＰＣ４）との間でデータ通信可能に構成された認証サーバ装置（ＣＡ１）であって、

予め定められた鍵ペアの一方を用いて、前記クライアントからの証明書発行要求に応じて電子証明書を発行するための証明書発行部（２０６ａ）と、

自身が発行した電子証明書に対して、前記鍵ペアの他方を用いて認証を行なうための認証検証部（２０６ｂ）と、

他の認証サーバ装置が発行した電子証明書に対して、前記他の認証サーバ装置の鍵ペアを用いて認証が行なわれた結果内容を、格納するための認証リスト記憶部（２１２）とを含み、

前記認証検証部は、前記他の認証サーバ装置が発行した電子証明書に対して、前記結果内容を参照して認証を行ない、

前記認証検証部は、前記クライアントから受信した前記電子証明書についての発行元を判断し、自身が発行元ではない場合に、発行元の認証サーバ装置へ前記電子証明書を転送し、

前記発行元の認証サーバ装置は、前記認証検証部から前記電子証明書を受信した場合に、自身の鍵ペアの他方を用いて認証を行ない、その結果内容を応答する、認証サーバ装置。

【請求項５】

互いにデータ通信可能に構成された複数の認証サーバ装置（ＣＡ１，ＣＡ２）と、少なくとも１つのクライアント（ＰＣ１）とを含むネットワークシステムにおける認証方法であって、前記複数の認証サーバ装置の各々は、予め定められた独自の鍵ペアの一方を用いて、前記クライアントからの証明書発行要求に応じて電子証明書を発行することが可能であり、

前記複数の認証サーバ装置のうち第１の認証サーバ装置において、第２の認証サーバ装置（ＣＡ２）が発行した電子証明書に対して前記第２の認証サーバ装置の鍵ペアの他方を用いて認証が行なわれた結果内容を取得するステップ（Ｓ５８）と、

前記第１の認証サーバ装置（ＣＡ１）において、前記クライアントから前記電子証明書を受信した場合に、前記電子証明書の発行元を判断するステップ（Ｓ５２）と、

前記第１の認証サーバ装置において、受信した電子証明書の発行元が自身である場合に、自身の鍵ペアの他方を用いて認証を行なうステップ（Ｓ６０）と、

前記第１の認証サーバ装置において、受信した電子証明書の発行元が前記第２の認証サーバ装置である場合に、前記結果内容を参照して認証を行なうステップ（Ｓ６０）と、

前記第１の認証サーバ装置において、前記クライアントから受信した前記電子証明書についての発行元を判断し、自身が発行元ではない場合に、発行元の認証サーバ装置へ前記電子証明書を転送するステップと、

前記複数の認証サーバ装置のうち前記電子証明書の発行元の認証サーバ装置において、前記第１の認証サーバ装置から前記電子証明書を受信した場合に、自身の鍵ペアの他方を用いて認証を行ない、その結果内容を応答するステップとを含む、認証方法。

【発明の詳細な説明】

【技術分野】
【０００１】
この発明は、電子証明書を用いた認証に係るネットワークシステム、認証サーバ装置および認証方法に関し、特に同一のクライアントを異なる認証サーバ装置で認証可能にする構成に関する。
【背景技術】
【０００２】
セキュリティ上の観点から、ネットワークを介して接続された複数のデバイス（代表的に、パーソナルコンピュータ、あるいは当該パーソナルコンピュータ上で実行されるアプリケーション）が互いにデータ通信を行なう場合には、特定の認証サーバ装置による認証が実行される。具体的には、各デバイスには、各デバイスの公開鍵などの情報および共通の認証サーバ装置によるデジタル署名（以下、単に「署名」とも記す。）を含む電子証明書が予め発行されており、アクセス先のデバイスは、アクセス元のデバイスが保有する電子証明書を共通の認証サーバ装置の公開鍵を用いて検証を行なう。この検証が成功した場合には、当該アクセス元のデバイスが共通の認証サーバ装置によって認証済みであると判断し、データ通信を許可する。
【０００３】
ところで、このような認証処理を採用した場合には、互いに異なる認証サーバ装置が発行した電子証明書を保有するデバイス同士での認証は成功しない。これは、認証サーバ装置が異なれば、検証に用いる公開鍵が異なるためである。そのため、特定のアプリケーションを販売する会社が、地域毎（代表的には、国ごと）に認証サーバ装置を設置している場合を想定すると、たとえば、日本に設置されている認証サーバ装置で発行される電子証明書を保有するデバイスと、アメリカに設置されている認証サーバ装置で発行される電子証明書を保有するデバイスとの間では、電子証明書の検証が成功しない。そのため、アメリカの認証サーバ装置が発行した電子証明書を格納するデバイスを日本で使用することができない事態が発生する。特に、当該アプリケーションの製造会社とは別の地域毎の販売会社が認証サーバ装置を設置するような場合には、各販売会社がデバイスのセキュリティなどをコントロールしたいというニーズがあり、上述のような形態が採用される。
【０００４】
しかしながら、ユーザ側からみると、同一のアプリケーションであるのに、使用地域を変更する毎に電子証明書を再度取得する必要がある。そのため、たとえば出張先でパーソナルコンピュータを使用する必要があるユーザなどにとってみれば、利便性が悪いという課題があった。
【０００５】
このような課題に対する一つのアプローチとして、特開２００７－１１０３７７号公報（特許文献１）には、認証サーバ間を連携させることによって、該クライアントの認証データを保有しない移動先認証サーバにおいても、クライアントの認証が可能なネットワークシステムが開示されている。このネットワークシステムでは、認証サーバが、自サーバに認証用データを持つクライアントに有効期限付きの認証チケットを発行し、信頼関係が構築されている他の認証サーバによって発行された認証チケットの有効性を検証し、認証チケットの有効性が確認されると、認証成功とする。
【特許文献１】特開２００７－１１０３７７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、上述の特開２００７－１１０３７７号公報（特許文献１）に開示されるネットワークシステムでは、多数のデバイスが別の認証サーバ装置で認証を受けようとすると、各デバイスに対して有効期限付きの認証チケットを発行する必要があり、管理者による設定作業が煩雑になり、設定操作に係る負担が増大するという問題があった。
【０００７】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、より簡素化した手続きによって、同一のクライアントを複数の認証装置で認証可能なネットワークシステム、認証サーバ装置および認証方法を提供することである。

【課題を解決するための手段】

【０００８】

この発明のある局面に従うネットワークシステムは、互いにデータ通信可能に構成された複数の認証サーバ装置と、少なくとも１つのクライアントとを含む。複数の認証サーバ装置の各々は、予め定められた独自の鍵ペアの一方を用いて、クライアントからの証明書発行要求に応じて電子証明書を発行するための証明書発行部を含む。複数の認証サーバ装置のうち第１の認証サーバ装置は、自身が発行した電子証明書に対して、自身の鍵ペアの他方を用いて認証を行なうための認証検証部と、第２の認証サーバ装置が発行した電子証明書に対して、第２の認証サーバ装置の鍵ペアの他方を用いて認証が行なわれた結果内容を、格納するための認証リスト記憶部とを含む。

【０００９】

また、認証検証部は、第２の認証サーバ装置が発行した電子証明書に対して、結果内容を参照して認証を行なう。認証検証部は、クライアントから受信した電子証明書についての発行元を判断し、自身が発行元ではない場合に、発行元の認証サーバ装置へ電子証明書を転送する。複数の認証サーバ装置のうち電子証明書の発行元の認証サーバ装置は、第１の認証サーバ装置から電子証明書を受信した場合に、自身の鍵ペアの他方を用いて認証を行ない、その結果内容を応答する応答部を含む。

【００１０】

好ましくは、認証検証部は、クライアントから受信した電子証明書についての発行元を判断し、自身が発行元ではない場合に、発行元の認証サーバ装置へ電子証明書を転送する。複数の認証サーバ装置のうち電子証明書の発行元の認証サーバ装置は、第１の認証サーバ装置から電子証明書を受信した場合に、自身の鍵ペアの他方を用いて認証を行ない、その結果内容を応答する応答部を含む。

【００１１】

さらに好ましくは、認証検証部は、発行元の認証サーバ装置が予め定められた連携先である場合に限って、電子証明書を発行元の認証サーバ装置へ転送する。

【００１２】

好ましくは、認証リスト記憶部は、クライアントの識別情報に対応付けて、クライアントに発行されている電子証明書の内容、電子証明書の有効期限、電子証明書の許可範囲のうち少なくとも１つを格納する。

【００１３】

この発明の別の局面に従えば、他の認証サーバ装置およびクライアントとの間でデータ通信可能に構成された認証サーバ装置を提供する。認証サーバ装置は、予め定められた鍵ペアの一方を用いて、クライアントからの証明書発行要求に応じて電子証明書を発行するための証明書発行部と、自身が発行した電子証明書に対して、鍵ペアの他方を用いて認証を行なうための認証検証部と、他の認証サーバ装置が発行した電子証明書に対して、他の認証サーバ装置の鍵ペアを用いて認証が行なわれた結果内容を、格納するための認証リスト記憶部とを含む。また、認証検証部は、他の認証サーバ装置が発行した電子証明書に対して、結果内容を参照して認証を行なう。認証検証部は、クライアントから受信した電子証明書についての発行元を判断し、自身が発行元ではない場合に、発行元の認証サーバ装置へ電子証明書を転送する。発行元の認証サーバ装置は、認証検証部から電子証明書を受信した場合に、自身の鍵ペアの他方を用いて認証を行ない、その結果内容を応答する。

【００１４】

この発明のさらに別の局面に従えば、互いにデータ通信可能に構成された複数の認証サーバ装置と、少なくとも１つのクライアントとを含むネットワークシステムにおける認証方法を提供する。複数の認証サーバ装置の各々は、予め定められた各自の鍵ペアの一方を用いて、クライアントからの証明書発行要求に応じて電子証明書を発行することが可能で

ある。認証方法は、複数の認証サーバ装置のうち第１の認証サーバ装置において、他の認証サーバ装置が発行した電子証明書に対して第２の認証サーバ装置の鍵ペアの他方を用いて認証が行われた結果内容を取得するステップと、第１の認証サーバ装置において、クライアントから電子証明書を受信した場合に、電子証明書の発行元を判断するステップと、第１の認証サーバ装置において、受信した電子証明書の発行元が自身である場合に、自身の鍵ペアの他方を用いて認証を行なうステップと、第１の認証サーバ装置において、受信した電子証明書の発行元が他の認証サーバ装置である場合に、結果内容を参照して認証を行なうステップと、第１の認証サーバ装置において、クライアントから受信した電子証明書についての発行元を判断し、自身が発行元ではない場合に、発行元の認証サーバ装置へ電子証明書を転送するステップと、複数の認証サーバ装置のうち電子証明書の発行元の認証サーバ装置において、第１の認証サーバ装置から電子証明書を受信した場合に、自身の鍵ペアの他方を用いて認証を行ない、その結果内容を応答するステップとを含む。

【発明の効果】

【００１５】

この発明によれば、より簡素化した手続きによって、同一のクライアントを複数の認証装置で認証できる。

【図面の簡単な説明】

【００１６】

【図１】この発明の実施の形態に従うネットワークシステムＳＹＳの概略構成図である。

【図２】この発明の実施の形態に従う認証サーバ装置およびクライアントの概略のハードウェア構成を示す模式図である。

【図３】この発明の実施の形態に従う認証サーバ装置ＣＡにおける概略の制御構造を示す図である。

【図４】この発明の実施の形態に従うクライアントの代表例であるクライアントＰＣにおける概略の制御構造を示す図である。

【図５】この発明の実施の形態に従うクライアント間の接続処理に係る手順を説明するための図である。

【図６】この発明の実施の形態に従うクライアント間の接続処理に係る手順を説明するための図である。

【図７】この発明の実施の形態に従うクライアント間の接続処理に係る手順を説明するための図である。

【図８】認証サーバ装置ＣＡ２に格納されるエリア外ＷｈｉｔｅＬｉｓｔの一例を示す図である。

【図９】この発明の実施の形態に従うクライアント間の接続に係る処理手順を示すシーケンス図である。

【図１０】この発明の実施の形態に従う認証サーバ装置に対するクライアントの認証に係る処理手順を示すシーケンス図である。

【図１１】この発明の実施の形態の変形例に従う接続処理に係る手順を説明するための図である。

【図１２】この発明の実施の形態の変形例に従う接続処理に係る手順を説明するための図である。

【符号の説明】

【００１７】

１０２　内部バス、１０４　ディスプレイ部、１０６　インターフェイス（Ｉ／Ｆ）部部、１０８　入力部、１１０　ハードディスク部（ＨＤＤ）、１１２　メモリ部、１１４　ＣＤ－ＲＯＭドライブ、１１４ａ　ＣＤ－ＲＯＭ、１１６　ＦＤドライブ、１１６ａ　フレキシブルディスク、２０２　データ受信部、２０４　データ解析部、２０６　認証部、２０６ａ　証明書発行機能、２０６ｂ　認証検証機能、２０８　連携処理部、２０８ａ　連携情報管理機能、２０８ｂ　管理機能、２０８ｃ　認証要求機能、２０８ｄ　認証検証機能、２１０　その他処理部、２１０ａ　提供機能、２１０ｂ　更新機能、２１０ｃ

問い合せ機能機能、２１０ｄ　管理機能、２１２　データ格納部、２１２ａ　連携情報、２１４　データ作成部、２１６　データ送信部、３０２　データ受信部、３０４　データ解析部、３０６　認証部、３０６ａ　認証要求機能、３０６ｂ　認証検証機能、３０８　接続処理部、３０８ａ　認証機能、３０８ｂ　管理機能、３１０　その他処理部、３１０ａ　提供機能、３１０ｂ　更新機能、３１０ｃ　問い合せ機能、３１０ｄ　管理機能、３１２　データ格納部、３１２ａ　証明書、３１４　データ作成部、３１６　データ送信部、ＣＡ，ＣＡ１，ＣＡ２　認証サーバ装置、ＮＷ１，ＮＷ２，ＮＷ３　ネットワーク、ＰＣ，ＰＣ１-ＰＣ３　クライアント、ＲＴ　ルータ、ＳＹＳ　ネットワークシステム。

【発明を実施するための最良の形態】

【００１８】

この発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中の同一または相当部分については、同一符号を付してその説明は繰返さない。

【００１９】

（ネットワークシステムの全体構成）

図１は、この発明の実施の形態に従うネットワークシステムＳＹＳの概略構成図である。

【００２０】

図１を参照して、本実施の形態に従うネットワークシステムＳＹＳは、認証サーバ装置（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）ＣＡ１およびＣＡ２を含み、認証サーバ装置ＣＡ１とＣＡ２とは、それぞれルータＲＴおよびネットワークＮＷ３を介してデータ通信可能に構成されている。認証サーバ装置ＣＡ１は、エリアＡを管理範囲とし、ネットワークＮＷ１に接続されたクライアントに対して、電子証明書の発行や電子証明書の有効性を判断する。一方、認証サーバ装置ＣＡ２は、エリアＢを管理範囲とし、ネットワークＮＷ２に接続されたクライアントに対して、電子証明書の発行や認証の可否を判断する。なお、エリアＡおよびエリアＢは、代表的に、地域毎の設立された販売会社がその営業範囲をカバーするように物理的に定めることができるが、これに限られず、認証サーバ装置の処理能力を考慮して、ネットワークアドレスの区分やプロバイダなどに応じて論理的（すなわち、ネットワークセグメント別に）に定めてもよい。

【００２１】

より具体的には、認証サーバ装置ＣＡ１およびＣＡ２（以下、総称して「認証サーバ装置ＣＡ」とも記す。）は、クライアントからの証明書発行要求に対して署名を行って電子証明書（以下、単に「証明書」とも記す。）を発行したり、無効になった（有効期限が経過した）証明書のリスト（ＣＲＬ：Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を保有し、そのリストを参照して証明書の有効／無効を判断したりする。なお、認証サーバ装置ＣＡにおける署名とは、証明書の正真性を保証するための暗号化された電子情報である。本実施形態では、代表的な認証方法である公開鍵基盤（ＰＫＩ：ｐｕｂｌｉｃ-ｋｅｙ　ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）を用いる構成について例示する。

【００２２】

より具体的には、まず、認証サーバ装置ＣＡの各々には、独自の鍵ペア（一対の公開鍵と秘密鍵）が用意されており、かつ各クライアントにおいても独自の鍵ペア（一対の公開鍵と秘密鍵）が用意されているとする。なお、各クライアントの鍵ペアは、対応の認証サーバ装置が生成してもよい。

【００２３】

証明書の発行処理としては、各クライアントが証明書発行要求として、自身の公開鍵や自身の所有者情報などを対応の認証サーバ装置ＣＡへ送信する。すると、当該認証サーバ装置ＣＡは、クライアントからの証明書発行要求に含まれるデータを自身の秘密鍵を用いて署名（データ値）を生成し、証明書発行要求に含まれるデータに生成した署名を付加して、証明書を発行する。したがって、各クライアントが保有する証明書には、当該クライアントの公開鍵や、認証サーバ装置ＣＡの保有する秘密鍵を用いて生成した署名などが含まれる。なお、この証明書は、認証サーバ装置ＣＡによって認証されたものであるので「

ルート証明書」などとも称される。

【００２４】

以下の説明では、クライアントの代表例として、デバイスであるパーソナルコンピュータを用いる場合について例示するが、認証サーバ装置とデータ通信するための機能を有する装置であれば、特にクライアントについて限定されることはない。すなわち、パーソナルコンピュータの他にも、ネットワーク機能を搭載した画像形成装置などを用いてもよい。

【００２５】

代替的に、クライアントをハードウェア毎ではなく、各ハードウェアで実行されるアプリケーション毎あるいはファームウェア毎とすることもできる。すなわち、一般的なパーソナルコンピュータでは、複数のアプリケーションが同時に実行可能であり、アプリケーション単位で認証を行なうこともできる。したがって、認証サーバ装置ＣＡ１およびＣＡ２がパーソナルコンピュータで実行される各アプリケーションに対して証明書の発行やその有効性の判断を行なうようにしてもよい。

【００２６】

本実施の形態に従うネットワークシステムＳＹＳでは、認証サーバ装置ＣＡ１がネットワークＮＷ１に接続されたクライアントに対して証明書の発行などを行ない、認証サーバ装置ＣＡ２がネットワークＮＷ２に接続されたクライアントに対して証明書の発行などを行なう。

【００２７】

ここで、ネットワークＮＷ２に接続されているときに認証サーバ装置ＣＡ２から発行された証明書を取得したクライアントＰＣ１が、ネットワークＮＷ１に移動した場合を想定する。予めネットワークＮＷ１に接続されているクライアントＰＣ２は、認証サーバ装置ＣＡ１から発行された証明書を取得しているとする。

【００２８】

ここで、クライアントＰＣ２からクライアントＰＣ１への接続要求がなされる場合を考える。この場合、クライアントＰＣ２は、自身の証明書をクライアントＰＣ１へ送信する。これに対して、クライアントＰＣ１は、自身を認証した認証サーバ装置ＣＡ１の公開鍵を用いて、クライアントＰＣ２から受信した証明書を認証する。この認証が成功すれば、クライアントＰＣ２が認証サーバ装置ＣＡ１によって認証されたものであり、かつ当該証明書に含まれるクライアントＰＣ２の公開鍵が正真なものであると判断する。さらに、クライアントＰＣ１も自身の証明書をクライアントＰＣ２へ送信し、同様の認証処理が実行される。そして、クライアントＰＣ１およびＰＣ２は、必要に応じて、取得した互いの公開鍵を用いて暗号化通信を行なう。

【００２９】

しかしながら、クライアントＰＣ１およびＰＣ２に対して証明書を発行した認証サーバ装置が異なる以上、それぞれの公開鍵が異なったものとなっているため、証明書の認証動作は失敗することになる。そのため、クライアントＰＣ１のユーザから見れば非常に利便性が悪い。

【００３０】

そこで、本実施の形態に従うネットワークシステムＳＹＳでは、認証サーバ装置ＣＡ１とＣＡ２とが予め連携関係にあれば、一方の認証サーバ装置ＣＡから発行された証明書を保有するクライアントに対して、他方の認証サーバ装置ＣＡに対する認証要求が許可され、あるいは他方の認証サーバ装置ＣＡから発行された証明書を有するクライアントとの間の接続要求が許可される。これにより、一方の認証サーバ装置ＣＡから証明書を発行されたクライアントは、当該認証サーバ装置ＣＡと連携関係にある他の認証サーバ装置ＣＡから証明書を発行されたクライアントとの間でデータ通信が可能となる。

【００３１】

（ハードウェア構成）

図２は、この発明の実施の形態に従う認証サーバ装置およびクライアントの概略のハー

ドウェア構成を示す模式図である。

【００３２】

図２を参照して、認証サーバ装置ＣＡ１およびＣＡ２は、オペレーティングシステムを含む各種プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１００と、ＣＰＵ１００でのプログラムの実行に必要なデータを一時的に記憶するメモリ部１１２と、ＣＰＵ１００で実行されるプログラムを不揮発的に記憶するハードディスク部（ＨＤＤ）１１０とを含む。このようなプログラムは、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｋ－Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）ドライブ１１４またはフレキシブルディスク（ＦＤ：Ｆｌｅｘｉｂｌｅ Ｄｉｓｋ）ドライブ１１６によって、それぞれＣＤ－ＲＯＭ１１４ａまたはフレキシブルディスク１１６ａなどから読取られる。

【００３３】

ＣＰＵ１００は、キーボードやマウスなどからなる入力部１０８を介してユーザによる操作要求を受取るとともに、プログラムの実行によって生成される画面出力をディスプレイ部１０４へ出力する。また、ＣＰＵ１００は、ＬＡＮカードなどからなるネットワークインターフェイス（Ｉ／Ｆ）部１０６を介して、他の認証サーバ装置やクライアントとの間でデータ通信を行なう。なお、これらの部位は、内部バス１０２を介して互いに接続される。

【００３４】

クライアントＰＣ１～ＰＣ３（以下、総称して「クライアントＰＣ」とも記す。）の概略のハードウェア構成についても図２と同様であるので、詳細な説明は繰返さない。

【００３５】

（認証サーバ装置の機能構成）

図３は、この発明の実施の形態に従う認証サーバ装置ＣＡにおける概略の制御構造を示す図である。図３に示す制御構造は、代表的に、ＣＰＵ１００（図２）がハードディスク部１１０（図２）に予め格納されたプログラムをメモリ部１１２（図２）に展開して実行することで実現される。

【００３６】

図３を参照して、認証サーバ装置ＣＡは、データ受信部２０２と、データ解析部２０４と、認証部２０６と、ＣＡ連携処理部２０８と、その他処理部２１０と、データ格納部２１２と、データ作成部２１４と、データ送信部２１６とをその機能として含む。

【００３７】

データ受信部２０２は、ネットワーク上を伝送されるデータパケットを受信するとともに、分割送信されたデータパケットについては結合してデータ列に復元した上で、データ解析部２０４へ出力する。データ解析部２０４は、各データ列の内容（代表的に、ヘッダ部のアドレス情報）を解析し、当該データ列が自身宛てのものであるか否かを判断する。そして、データ解析部２０４は、自身宛てのものと判断したデータ列のみを認証部２０６、ＣＡ連携処理部２０８、その他処理部２１０のいずれかに出力する。

【００３８】

認証部２０６は、認証サーバ装置ＣＡへ送信されたデータ列のうち、クライアントからの証明書の発行要求や認証要求に応答して処理を行なう。具体的には、認証部２０６は、証明書発行機能２０６ａと、認証検証機能２０６ｂと、鍵ペア保有部２０６ｃとを含む。証明書発行機能２０６ａとして、認証部２０６は、クライアントからの証明書の発行要求を受けると、クライアントに対する認証処理を行ない、当該認証処理が成功した場合に、自身の署名を付した証明書を発行する。

【００３９】

また、認証検証機能２０６ｂとして、認証部２０６は、クライアントから証明書が送信されると、当該証明書を自身の公開鍵を用いてその正真性を認証する。ここで、従来の認証サーバ装置は、自身の公開鍵を用いて認証を行なうのみであるので、クライアントから送信される証明書が認証サーバ装置自身の発行したものでなければ、認証は成功しない。本実施の形態に従うネットワークシステムＳＹＳでは、このような場合には、認証部２０

６が当該証明書をＣＡ連携処理部２０８へ転送し、ＣＡ連携処理部２０８によって認証処理が継続される。

【００４０】

ＣＡ連携処理部２０８は、クライアントなどから受信した証明書に対する認証を連携先の認証サーバ装置ＣＡに依頼するとともに、連携先の認証サーバ装置ＣＡによる認証結果をデータ格納部２１２内のエリア外ＷｈｉｔｅＬｉｓｔ２１２ｃに格納する。具体的には、ＣＡ連携処理部２０８は、連携情報管理機能２０８ａと、ＷｈｉｔｅＬｉｓｔ管理機能２０８ｂと、他ＣＡ認証要求機能２０８ｃと、他ＣＡ認証検証機能２０８ｄとをその機能として含む。

【００４１】

連携情報管理機能２０８ａとして、ＣＡ連携処理部２０８は、信頼関係を結んでいる他の認証サーバ装置ＣＡとの連携を管理し、定期的またはイベント発生毎に、連携先の認証サーバ装置ＣＡとの間で情報をやり取りし、データ格納部２１２内の連携情報２１２ａを作成または更新する。なお、連携先の認証サーバ装置ＣＡは、連携情報２１２ａによって特定される。

【００４２】

他ＣＡ認証要求機能２０８ｃとして、ＣＡ連携処理部２０８は、認証部２０６から転送された証明書の発行元のエントリが連携情報２１２ａに存在するか否かを判断し、当該エントリが連携情報２１２ａに存在する場合には、連携先の認証サーバ装置ＣＡに対して、当該証明書の情報とともに認証要求を送信し、そうでなければ認証要求を拒否する。

【００４３】

ＷｈｉｔｅＬｉｓｔ管理機能２０８ｂとして、ＣＡ連携処理部２０８は、連携先の認証サーバ装置ＣＡによる認証が成功した場合に取得される証明書の内容を、データ格納部２１２内のエリア外ＷｈｉｔｅＬｉｓｔ２１２ｃに追加する。また、連携先の認証サーバ装置ＣＡから、特定のクライアントに対する証明書の有効期限切（無効）などのステータスの変更が通知された場合にも、エリア外ＷｈｉｔｅＬｉｓｔ２１２ｃの内容を更新する。エリア外ＷｈｉｔｅＬｉｓｔは、連携先の認証サーバ装置ＣＡが証明書を発行したクライアントのうち、当該認証サーバ装置ＣＡでも認証可能なクライアントを特定するための情報を格納したデータ集合である。

【００４４】

他ＣＡ認証検証機能２０８ｄとして、ＣＡ連携処理部２０８は、他の認証サーバ装置ＣＡから転送された証明書を受信すると、認証部２０６の鍵ペア保有部２０６ｃに格納されている自身の公開鍵を用いて、当該証明書を認証する。そして、ＣＡ連携処理部２０８は、この認証結果を認証要求元の認証サーバ装置ＣＡへ返送する。

【００４５】

また、データ格納部２１２には、有効期限が経過するなどして無効になった証明書のリスト（以下、「ＣＲＬｉｓｔ」とも記す。）２１２ｂが格納されており、ＣＡ連携処理部２０８は、このＣＲＬｉｓｔ２１２ｂのエントリに該当する証明書に対しては、認証を拒否する。

【００４６】

その他処理部２１０は、上述した証明書の発行処理や認証処理以外の処理を実行する。具体的には、その他処理部２１０は、提供機能２１０ａと、更新機能２１０ｂと、問い合せ機能２１０ｃと、管理機能２１０ｄとをその機能として含む。

【００４７】

認証部２０６、ＣＡ連携処理部２０８およびその他処理部２１０が、他の認証サーバ装置ＣＡやクライアントにデータ送信を行なう場合には、各々が送信すべきメッセージを作成してデータ作成部２１４へ出力する。データ作成部２１４は、各部から送信されるメッセージを所定のデータパケットに整形し、データ送信部２１６へ出力する。

【００４８】

データ送信部２１６は、データ作成部２１４で順次生成されるデータパケットを、ネッ

トワークを介して指定された宛先に送信する。

【００４９】

（クライアントの機能構成）

本実施の形態に従うクライアントＰＣは、互いに認証処理が成功したクライアントとの間でのみデータ通信（必要に応じて、暗号化通信）を行なうものとする。すなわち、本実施の形態に従うクライアントＰＣは、別のクライアントＰＣから接続要求を受けると、当該接続要求とともに送信される証明書に対して認証を行ない、認証が成功した場合に限って、要求された接続を許可する。なお、接続の可否は、アプリケーション（あるいは、サービス）単位で行なうようにしてもよい。

【００５０】

図４は、この発明の実施の形態に従うクライアントの代表例であるクライアントＰＣにおける概略の制御構造を示す図である。図４に示す制御構造は、ＣＰＵ１００（図２）がハードディスク部１１０（図２）に予め格納されたプログラムをメモリ部１１２（図２）に展開して実行することで実現される。

【００５１】

図４を参照して、クライアントＰＣは、データ受信部３０２と、データ解析部３０４と、認証部３０６と、接続処理部３０８と、その他処理部３１０と、データ格納部３１２と、データ作成部３１４と、データ送信部３１６とをその機能として含む。

【００５２】

データ受信部３０２は、ネットワーク上を伝送されるデータパケットを受信するとともに、分割送信されたデータパケットについては結合してデータ列を復元した上で、データ解析部３０４へ出力する。データ解析部３０４は、各データ列の内容（代表的に、ヘッダ部のアドレス情報）を解析し、当該データ列が自身宛てのものであるか否かを判断する。そして、データ解析部３０４は、自身宛てのものと判断したデータ列のみを認証部３０６、接続処理部３０８、その他処理部３１０のいずれかに出力する。

【００５３】

認証部３０６は、ネットワークに新規参加する場合、他のクライアント（クライアントＰＣ）へ接続する場合あるいは所定周期毎に、認証サーバ装置ＣＡまたは他のクライアントへそれぞれ認証要求または接続要求を送信する。また、認証部３０６は、当該クライアントＰＣへ送信されたデータ列のうち、他のクライアントからの接続要求に応答して認証処理を行なう。具体的には、認証部３０６は、認証要求機能３０６ａと認証検証機能３０６ｂとをその機能として含む。

【００５４】

認証要求機能３０６ａとして、認証部３０６は、ユーザ操作や何らかのアプリケーションで発生するイベントに応じて、ネットワークに新規参加する必要があるか、あるいは他のクライアントへ接続する必要があるかなどを判断する。そして、認証部３０６は、ネットワークに新規参加する必要があると判断すると、認証サーバ装置ＣＡに対して証明書発行要求を送信する。認証サーバ装置ＣＡから証明書が発行されると、当該証明書は、データ格納部３１２に格納される。また、認証部３０６は、他のクライアントに接続する必要があると判断すると、当該クライアントに対して、データ格納部３１２に格納されている証明書３１２ａとともに接続要求を送信する。

【００５５】

一方、認証検証機能３０６ｂとして、認証部３０６は、他のクライアントから証明書とともに接続要求（あるいは、認証要求）を受けると、自身の所属する認証サーバ装置ＣＡの公開鍵を用いて認証する。ここで、従来のネットワークシステムであれば、他のクライアントから送信される証明書の発行元と接続先のクライアントに格納されている証明書の発行元とが一致していなければ、認証は失敗する。一方、本実施の形態に従うクライアントＰＣでは、このような場合には、認証部３０６が当該証明書を接続処理部３０８へ転送し、接続処理部３０８によって認証処理が継続される。

【００５６】

接続処理部３０８は、自身の所属する認証サーバ装置ＣＡに格納されているエリア外ＷｈｉｔｅＬｉｓｔを参照して、自身のデータ格納部３１２のエリア外ＷｈｉｔｅＬｉｓｔ３１２ｂを作成または更新する。そして、接続処理部３０８は、他のクライアントから接続要求を受けると、当該接続要求の可否の判断などを行なう。具体的には、接続処理部３０８は、ＣＡ認証機能３０８ａと、ＷｈｉｔｅＬｉｓｔ管理機能３０８ｂとして含む。

【００５７】

ＣＡ認証機能３０８ａとして、接続処理部３０８は、認証部３０６から転送された証明書のエントリがエリア外ＷｈｉｔｅＬｉｓｔ３１２ｂに存在するか否かを判断し、当該エントリがエリア外ＷｈｉｔｅＬｉｓｔ３１２ｂに存在する場合、すなわち当該証明書が所属する認証サーバ装置ＣＡと連携関係にある他の認証サーバ装置ＣＡによって発行されたものである場合には、当該接続要求を許可する。

【００５８】

ＷｈｉｔｅＬｉｓｔ管理機能３０８ｂとして、接続処理部３０８は、データ格納部３１２にエリア外ＷｈｉｔｅＬｉｓｔ３１２ｂが存在しない場合や、認証部３０６から転送された証明書の発行元が自身の所属する認証サーバ装置ＣＡではない場合には、所属する認証サーバ装置ＣＡとの間で情報をやり取りし、データ格納部３１２内のエリア外ＷｈｉｔｅＬｉｓｔ３１２ｂを更新する。

【００５９】

その他処理部３１０は、上述した証明書の発行処理や認証処理以外の処理を実行する。具体的には、その他処理部３１０は、提供機能３１０ａと、更新機能３１０ｂと、問い合せ機能３１０ｃと、管理機能３１０ｄとをその機能として含む。

【００６０】

認証部３０６、接続処理部３０８およびその他処理部３１０が、所属する認証サーバ装置ＣＡやクライアントにデータ送信を行なう場合には、各々が送信すべきメッセージを作成してデータ作成部２１４へ出力する。データ作成部２１４は、各部から送信されるメッセージを所定のデータパケットに整形し、データ送信部２１６へ出力する。

【００６１】

データ送信部２１６は、データ作成部２１４で順次生成されるデータパケットを、ネットワークを介して指定された宛先に送信する。

【００６２】

（クライアント間の接続処理）

図５～図７は、この発明の実施の形態に従うクライアント間の接続処理に係る手順を説明するための図である。

【００６３】

まず、図５を参照して、初期状態として、エリアＡでは、クライアントＰＣ２に対して、認証サーバ装置ＣＡ１から証明書（以下、「証明書Ａ」とも記す。）が発行されている。また、エリアＢでは、クライアントＰＣ１に対して、認証サーバ装置ＣＡ２から証明書（以下、「証明書Ｂ」とも記す。）が発行されているものとする。

【００６４】

以下では、この初期状態において、クライアントＰＣ１がエリアＢからエリアＡに移動する場合を考える。

【００６５】

図６を参照して、一例として、クライアントＰＣ１が何らかのイベントが発生したときに、認証サーバ装置ＣＡ１に対して、証明書Ｂを送信して認証を依頼した場合（図６の手順（ａ））を考える。認証サーバ装置ＣＡ１は、この認証依頼に対して、自身の公開鍵による認証に失敗するので、一旦は認証を拒否するが、証明書Ｂに記載されている発行者（Ｉｓｓｕｅｒ）などの値から、証明書Ｂの発行元が連携先である認証サーバ装置ＣＡ２であることを判断すると、当該証明書Ｂを認証サーバ装置ＣＡ２へ送信する（図６の手順（ｂ））。すると、認証サーバ装置ＣＡ２は、この証明書Ｂを自身の公開鍵を用いて認証し、その認証結果、および認証が成功した場合には当該証明書Ｂに記載された情報を、認証

サーバ装置ＣＡ１へ応答する（図６の手順（ｃ））。

【００６６】

認証サーバ装置ＣＡ１は、この認証サーバ装置ＣＡ２が応答した情報に基づいて、エリア外ＷｈｉｔｅＬｉｓｔを作成または更新する。

【００６７】

また、図６では、認証サーバ装置ＣＡ１がエリア外ＷｈｉｔｅＬｉｓｔを作成または更新する場合について例示するが、認証サーバ装置ＣＡ２についても同様にエリア外ＷｈｉｔｅＬｉｓｔ（図示しない）を作成または更新することもできる。

【００６８】

さらに、認証サーバ装置ＣＡ１とＣＡ２との間で送受信されるデータについても、データ送信元の認証サーバ装置が自身の署名を付加することが好ましい。このように署名が付加されることで、ＷｈｉｔｅＬｉｓｔの内容といった重要なデータの改ざんを防止することができる。

【００６９】

なお、上述のように証明書の発行元の認証サーバ装置ＣＡへ証明書自体を転送する構成に代えて、連携先の認証サーバ装置ＣＡの公開鍵を予め取得しておき、クライアントから証明書を受信した認証サーバ装置ＣＡ自身が当該公開鍵を用いて認証を行なってもよい。また、証明書の発行元を特定できない場合には、提携先の認証サーバ装置ＣＡのすべてに対して受信した証明書をブロードキャスト（マルチキャスト）してもよい。この場合には、認証が成功した認証サーバ装置ＣＡのみがその内容を応答するように構成すればよい。

【００７０】

次に、図７を参照して、エリアＡに移動後のクライアントＰＣ１は、同一のネットワークに接続されるクライアントＰＣ２とデータ通信を行なう必要がある。その場合には、クライアントＰＣ１からクライアントＰＣ２に対して、自身の保有する証明書（証明書Ｂ）とともに接続要求が送信される（図７の手順（１））。この接続要求を受けて、クライアントＰＣ２は、証明書Ｂの発行元の認証サーバ装置が自身の所属する認証サーバ装置ＣＡ１ではないと判断すると、認証サーバ装置ＣＡ１に対して、エリア外ＷｈｉｔｅＬｉｓｔ要求を送信する（図７の手順（２））。このＷｈｉｔｅＬｉｓｔ要求に応答して、認証サーバ装置ＣＡ１は、自身の格納するエリア外ＷｈｉｔｅＬｉｓｔをクライアントＰＣ２へ返答する（図７の手順（３））。さらに、クライアントＰＣ２は、認証サーバ装置ＣＡ１から受信したエリア外ＷｈｉｔｅＬｉｓｔに基づいて、証明書Ｂの認証が許可されるべきものか否かを判断する。図６に示すように、予めクライアントＰＣ１が認証サーバ装置ＣＡ１に対して認証要求を行なっていれば、認証サーバ装置ＣＡ１のエリア外ＷｈｉｔｅＬｉｓｔに証明書Ｂの内容のエントリがあるので、クライアントＰＣ２は、このエントリに一致する証明書Ｂの認証を成功と判断する。そして、クライアントＰＣ２は、クライアントＰＣ１に対して接続要求の許可通知を応答する（図７の手順（４））。

【００７１】

なお、上述の説明では、各クライアントＰＣは、他のクライアントＰＣから接続要求があった場合に、自身の所属する認証サーバ装置ＣＡに問合せを行なう構成について例示したが、認証サーバ装置ＣＡにおいてエリア外ＷｈｉｔｅＬｉｓｔの更新が実行された場合に、当該認証サーバ装置ＣＡに所属するクライアントＰＣに対して、エリア外ＷｈｉｔｅＬｉｓｔの更新を通知するようにしてもよい。

【００７２】

また、証明書を受信したクライアントは、当該受信した証明書をそのまま自身の所属する認証サーバ装置ＣＡに転送するようにしてもよい。この場合には、認証サーバ装置ＣＡでは、図６と同様の処理が行なわれる。

【００７３】

また、認証サーバ装置ＣＡ同士の連携が解消された場合には、当該解消のイベント発生に応じて、各認証サーバ装置ＣＡは、自身の格納するエリア外ＷｈｉｔｅＬｉｓｔに登録されているエントリのうち、連携が解消されたものを削除することが好ましい。

【００７４】
さらに、各認証サーバ装置ＣＡは、必ずしもエリア外ＷｈｉｔｅＬｉｓｔを格納する必要はなく、証明書発行要求や認証要求を受信する毎に、連携先の認証サーバ装置ＣＡに問合せを行なって、当該要求の可否を判断するようにしてもよい。
【００７５】
さらに、認証サーバ装置ＣＡがエリア外ＷｈｉｔｅＬｉｓｔを格納する場合には、各クライアントＰＣが必ずしもエリア外ＷｈｉｔｅＬｉｓｔを格納する必要はなく、接続要求を受信する毎に、所属する認証サーバ装置ＣＡに問合せを行なって、当該要求の可否を判断するようにしてもよい。
【００７６】
（エリア外ＷｈｉｔｅＬｉｓｔのデータ構造）
次に、図８を参照して、エリア外ＷｈｉｔｅＬｉｓｔのデータ構造の一例について説明する。図８は、認証サーバ装置ＣＡ２に格納されるエリア外ＷｈｉｔｅＬｉｓｔの一例を示す図である。
【００７７】
図８を参照して、エリア外ＷｈｉｔｅＬｉｓｔには、各クライアント（デバイス）の識別情報（ＩＤ）に対応付けて、各クライアントに対して発行されている電子証明書、各クライアントの利用許可書、電子証明書の有効期限、電子証明書の許可範囲である許可アプリケーションといった情報が格納されている。
【００７８】
図８に示す識別情報（ＩＤ）は、各クライアントを特定するための情報であり、機器固有の識別情報（代表的に、ＭＡＣアドレス）などを含んで規定される。また、図８に示す証明書は、クライアントから送信された証明書のデータイメージであり、送信された証明書を特定するために用いられる。
【００７９】
利用許可書は、各証明書の利用可否を制御するためのデータであり、この利用許可書が与えられていなければ、認証サーバ装置ＣＡによる証明書の認証が成功した場合であっても、証明書の使用が禁止される。この利用許可書については後述する。なお、エリア外ＷｈｉｔｅＬｉｓｔのデータ構造をより簡素化するために、この利用許可書の項目を省略してもよい。
【００８０】
有効期限や許可アプリケーションは、証明書発行時に、対象のクライアントに対する権限や範囲などに応じて、認証サーバ装置や管理者の設定に従って予め設定された情報であり、各証明書に記載されている。すなわち、各証明書に対する認証が成功した場合に、当該証明書に記載の内容がエリア外ＷｈｉｔｅＬｉｓｔに格納されることになる。
【００８１】
次に、利用許可書の使用形態について説明する。認証サーバ装置ＣＡ１からクライアントＰＣ１の証明書が認証サーバ装置ＣＡ２に対して送信された場合には、認証サーバ装置ＣＡ２の管理範囲であるエリアＢからクライアントＰＣ１が移動したことを意味する。そのため、より使用管理を厳格化する観点からは、エリアＢにおけるクライアントＰＣ１の利用を禁止することが好ましい。
【００８２】
具体的には、ある認証サーバ装置自身が認証した証明書が連携先の認証サーバ装置から送信され、当該証明書の認証が成功した場合には、その証明書の内容とともに、当該証明書に対する利用許可書が当該連携先の認証サーバ装置ＣＡへ応答される。すると、図８に示すように、各証明書に格納された情報および利用許可書が、当該連携先の認証サーバ装置ＣＡのエリア外ＷｈｉｔｅＬｉｓｔに格納される。ここで、当該証明書の発行元の認証サーバ装置ＣＡは、ＣＲＬｉｓｔ２１２ｂ（図６および図７）に対応の証明書のエントリを追加する。認証サーバ装置ＣＡの管理下にあるクライアントは、認証処理毎に、このＣＲＬｉｓｔ２１２ｂを参照して各証明書の有効性を判断するので、このＣＲＬｉｓｔ２１

２ｂにエントリされることで、当該証明書は発行元の認証サーバ装置ＣＡの管理範囲では実質的に使用できなくなる。このような処理を追加的に実行することで、各クライアントに対する管理をより強化できる。

【００８３】

（認証サーバ装置同士の連携）

認証サーバ装置ＣＡ同士は、上述のようなエリア外ＷｈｉｔｅＬｉｓｔに格納される、（１）デバイスの有効／無効情報、（２）認証サーバ装置ＣＡ同士の認証／優劣情報、（３）アプリケーションの利用許可情報、などをやり取りする。

【００８４】

また、認証サーバ装置ＣＡ同士が情報をやり取りするイベントとしては、上述したものの他に、

（１）認証サーバ装置ＣＡが管轄するデバイス（クライアント）の有効／無効のステータスの変更時

（２）認証サーバ装置ＣＡが管轄するデバイス（クライアント）に対して発行されている証明書に割り当てられるアプリケーションの増加／減少の発生時

（３）認証サーバ装置ＣＡ間の連携関係の変更時

（４）いずれかの認証サーバ装置ＣＡの管理者による指示受取り時

また、認証サーバ装置ＣＡ同士のデータ通信における信頼性を確保するために、各管理者が秘密テーブルを用いて情報設定することが好ましい。そして、各認証サーバ装置ＣＡに信頼関係構築用の証明書がインストールされ、これらを利用して信頼関係の確認が行なわれる。なお、この信頼関係構築用の証明書は、各認証サーバ装置ＣＡに対して共通に証明書を発行するより上位の認証サーバ装置を用いることが好ましい。

【００８５】

（クライアント間の接続に係る処理手順）

図９は、この発明の実施の形態に従うクライアント間の接続に係る処理手順を示すシーケンス図である。なお、図９は、図７に示すようにクライアントＰＣ１からクライアントＰＣ２へ接続要求が送信される場合の処理を示す。

【００８６】

図９を参照して、まず、何らかのユーザ操作などがなされる（ステップＳ１０）と、クライアントＰＣ１は、クライアントＰＣ２に対して、自身の証明書とともに接続要求を送信する（ステップＳ１２）。この接続要求に応答して、クライアントＰＣ２は、送信された証明書が自身と同一の認証サーバ装置ＣＡで発行されたものであるか否かを判断する（ステップＳ１４）。当該証明書が自身と同一の認証サーバ装置ＣＡで発行されたものである場合（ステップＳ１４においてＹＥＳの場合）には、クライアントＰＣ２は、自身の所属する認証サーバ装置ＣＡの公開鍵を用いて、送信された証明書の認証を行なう（ステップＳ１６）。送信された証明書の認証が成功（ＯＫ）であれば（ステップＳ１６においてＹＥＳ）、クライアントＰＣ２は、クライアントＰＣ１に対して接続許可を送信する（ステップＳ１８）。これに対して、送信された証明書の認証が失敗（ＮＧ）であれば（ステップＳ１６においてＮＯ）、クライアントＰＣ２は、クライアントＰＣ１に対して接続拒否を送信する（ステップＳ２０）。

【００８７】

一方、当該証明書が自身と同一の認証サーバ装置ＣＡで発行されたものでない場合（ステップＳ１４においてＮＯの場合）には、クライアントＰＣ２は、自身の所属する認証サーバ装置ＣＡ１に対して、エリア外ＷｈｉｔｅＬｉｓｔ要求を送信し、エリア外ＷｈｉｔｅＬｉｓｔを取得する（ステップＳ２２）。そして、クライアントＰＣ２は、取得したエリア外ＷｈｉｔｅＬｉｓｔに基づいて、送信された証明書の認証を行なう（ステップＳ２４）。すなわち、エリア外ＷｈｉｔｅＬｉｓｔに受信した証明書のエントリが存在するか否かを判断する。送信された証明書の認証が成功（ＯＫ）であれば（ステップＳ２４においてＹＥＳ）、クライアントＰＣ２は、クライアントＰＣ１に対して接続許可を送信する（ステップＳ２６）。これに対して、送信された証明書の認証が失敗（ＮＧ）であれば（

ステップＳ２４においてＮＯ）、クライアントＰＣ２は、クライアントＰＣ１に対して接続拒否を送信する（ステップＳ２８）。

【００８８】

また、クライアントＰＣ１は、接続許可を受信した（ステップＳ１８またはＳ２６）後に、クライアントＰＣ２との接続を確立する（ステップＳ３０）。

【００８９】

（認証サーバ装置に対するクライアントの認証に係る処理手順）

図１０は、この発明の実施の形態に従う認証サーバ装置に対するクライアントの認証に係る処理手順を示すシーケンス図である。

【００９０】

図１０を参照して、まず、認証サーバ装置ＣＡ１は、いずれかのクライアントから認証要求を受信したか否かを判断する（ステップＳ５０）。クライアントから認証要求を受信していなければ（ステップＳ５０においてＮＯ）、ステップＳ５０が所定周期で繰返される。クライアントから認証要求を受信していれば（ステップＳ５０においてＹＥＳ）、認証サーバ装置ＣＡ１は、認証要求に付加された証明書は自身が発行したものであるか否かを判断する（ステップＳ５２）。

【００９１】

証明書は自身が発行したものでない場合（ステップＳ５２においてＮＯの場合）には、認証サーバ装置ＣＡ１は、当該証明書の発行元を判断し、当該発行元が連携先であるときには、当該証明書を連携先の認証サーバ装置ＣＡ２へ送信する（ステップＳ５４）。証明書を受信した連携先の認証サーバ装置ＣＡ２は、自身の公開鍵を用いて受信した証明書を認証する（ステップＳ５６）。そして、認証サーバ装置ＣＡ２は、その認証結果を認証サーバ装置ＣＡ１へ応答する（ステップＳ５８）。なお、認証サーバ装置ＣＡ２は、たとえば、過去に認証したことがない、あるいは認証を拒否したものである場合には、認証を拒否する。

【００９２】

続いて、認証サーバ装置ＣＡ１は、送信された証明書の認証を行なう（ステップＳ６０）。送信された証明書の認証が成功（ＯＫ）であれば（ステップＳ６０においてＹＥＳ）、認証サーバ装置ＣＡ１は、連携先の認証サーバ装置ＣＡ２により証明書が認証されたときには、当該電子証明書の内容をエリア内ＷｈｉｔｅＬｉｓｔに格納する（ステップＳ６２）。そして、クライアントＰＣ１に対して認証許可を送信する（ステップＳ６４）。これに対して、送信された証明書の認証が失敗（ＮＧ）であれば（ステップＳ６０においてＮＯ）、認証サーバ装置ＣＡ１は、クライアントＰＣ１に対して認証拒否を送信する（ステップＳ６６）。

【００９３】

（変形例）

上述の実施の形態に係る説明では、１つのクライアントが認証要求あるいは接続要求を送信する場合について例示した。一方、本実施の形態の変形例では、多数のクライアントが認証要求あるいは接続要求を行なう場合について説明する。

【００９４】

上述のように、各クライアントが認証要求あるいは接続要求を送信する毎に、認証サーバ装置ＣＡに問合せを行なうように構成すると、多数のクライアント装置が同時にこれらの要求を送信した場合に、連携先の認証サーバ装置ＣＡやネットワークの負荷が一時的に増加し得る。そこで、本実施の形態の変形例では、連携する認証サーバ装置ＣＡ同士が予めエリア外ＷｈｉｔｅＬｉｓｔに格納すべき情報をやり取りしておき、クライアントからの認証要求あるいは接続要求があっても、連携先の認証サーバ装置ＣＡに対する問合せを抑制する。

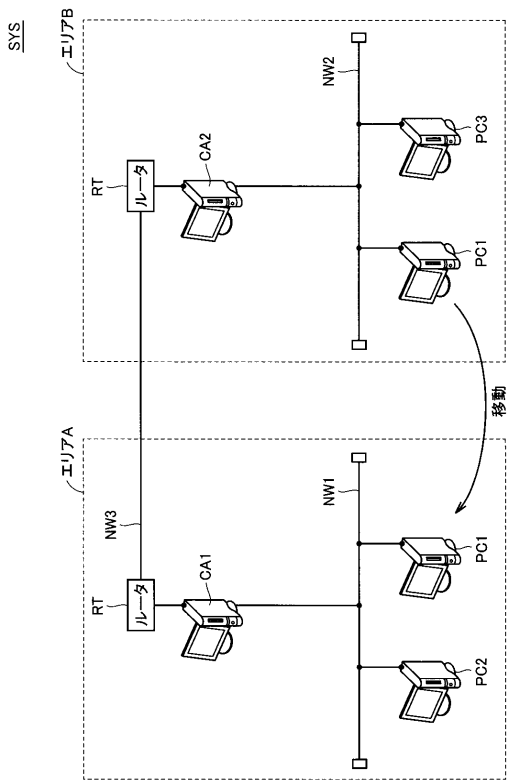
【００９５】

図１１および図１２は、この発明の実施の形態の変形例に従う接続処理に係る手順を説明するための図である。

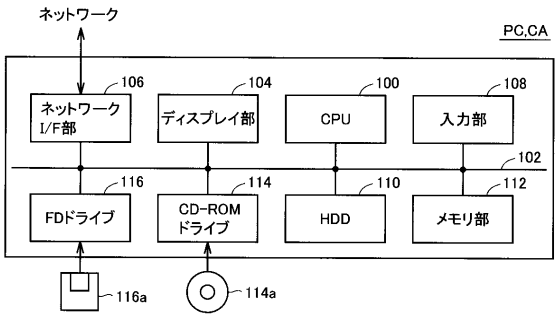
【００９６】
図１１を参照して、本実施の形態では、認証サーバ装置ＣＡ２から認証サーバ装置ＣＡ１に対して、少なくとも１つのデバイスに対して認証した証明書の内容を所定周期毎に送信される。この送信される証明書の内容に基づいて、認証サーバ装置ＣＡ１は、エリア外ＷｈｉｔｅＬｉｓｔを作成または更新する。なお、認証サーバ装置ＣＡ１から所定周期で送信される情報は、認証サーバ装置ＣＡ２の管理者などによって予め定められる。すなわち、予めエリアＢからエリアＡへの移動が予想されるクライアントを送信対象として登録しておくことができる。
【００９７】
図１２を参照して、認証サーバ装置ＣＡ２は、エリアＢから移動してきたクライアントＣＡ２－１およびＣＡ２－２からそれぞれ送信される認証要求に対して、予め作成したエリア外ＷｈｉｔｅＬｉｓｔを参照して、認証処理を行なうことができる。これにより、認証サーバ装置ＣＡ１と認証サーバ装置ＣＡ２との間でやり取りされるデータ量を低減できる。
【００９８】
（本実施の形態における効果）
この発明の実施の形態によれば、各認証サーバ装置は、他の認証サーバ装置が発行した電子証明書に基づく認証要求などに対して、連携する他の認証サーバ装置による認証結果に基づいて作成したＷｈｉｔｅＬｉｓｔを参照し、その可否を判断する。そのため、先行技術に係るような有効期限付きの認証チケットの発行といった複雑な処理を経ることなく、より簡素化した手続きによって、同一のクライアントを複数の認証装置で認証できる。すなわち、連携する認証サーバ装置を決定すればよく、認証すべきクライアントをいちいち特定する必要がなく、管理を容易化できる。
【００９９】
また、この発明の実施の形態によれば、各クライアント間の接続処理においても、その所属する認証サーバ装置からエリア外ＷｈｉｔｅＬｉｓｔを取得し、そのエリア外ＷｈｉｔｅＬｉｓｔに基づいて、認証処理を行なうことができる。そのため、各クライアントに対する設定を行なう必要がなく、より簡素化した手続きによって認証処理を実現することができる。
【０１００】
［その他の実施の形態］
本発明に係るプログラムは、コンピュータのオペレーティングシステム（ＯＳ）の一部として提供されるプログラムモジュールのうち、必要なモジュールを所定の配列で所定のタイミングで呼出して処理を実行させるものであってもよい。その場合、プログラム自体には上記モジュールが含まれずＯＳと協働して処理が実行される。このようなモジュールを含まないプログラムも、本発明にかかるプログラムに含まれ得る。
【０１０１】
また、本発明にかかるプログラムは他のプログラムの一部に組込まれて提供されるものであってもよい。その場合にも、プログラム自体には上記他のプログラムに含まれるモジュールが含まれず、他のプログラムと協働して処理が実行される。このような他のプログラムに組込まれたプログラムも、本発明にかかるプログラムに含まれ得る。
【０１０２】
提供されるプログラム製品は、ハードディスクなどのプログラム格納部にインストールされて実行される。なお、プログラム製品は、プログラム自体と、プログラムが記憶された記憶媒体とを含む。
【０１０３】
さらに、本発明に係るプログラムによって実現される機能の一部または全部を専用のハードウェアによって構成してもよい。
【０１０４】
今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えら

れるべきである。本発明の範囲は、上記した説明ではなく、請求の範囲によって示され、請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

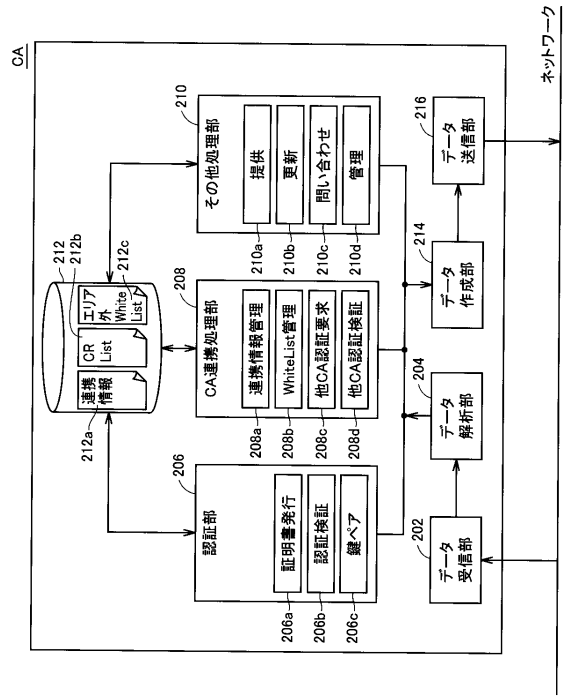
【図１】



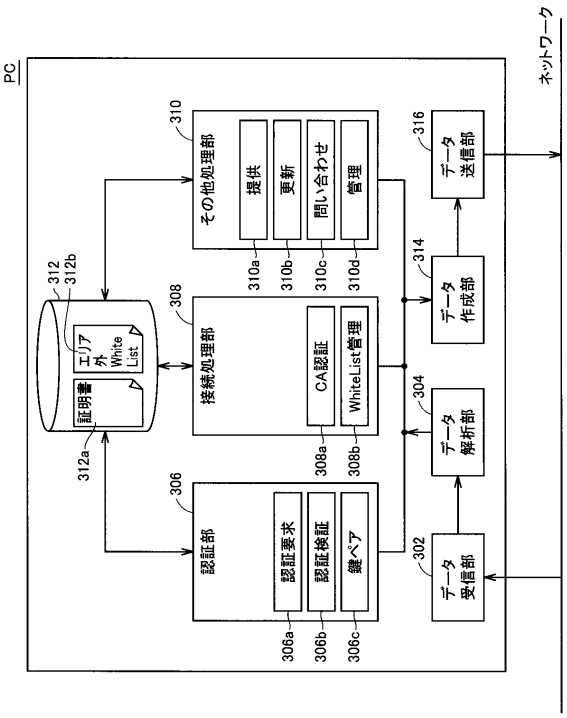
【図２】



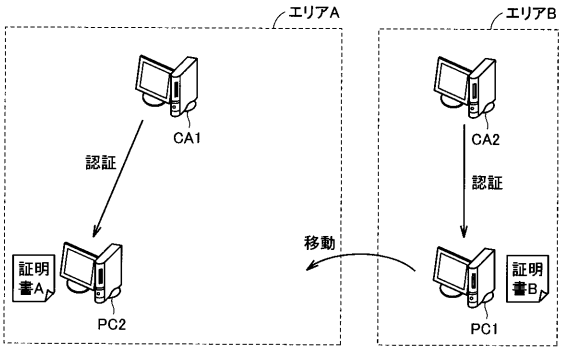
【図３】


CA
ネットワーク
その他処理部
提供
更新
問い合わせ
管理
CA連携処理部
連携情報管理
WhiteList管理
他CA認証要求
他CA認証検証
認証部
証明書発行
認証検証
鍵ペア
データ送信部
データ作成部
データ解析部
データ受信部
エリア外 White List
CR List
連携情報

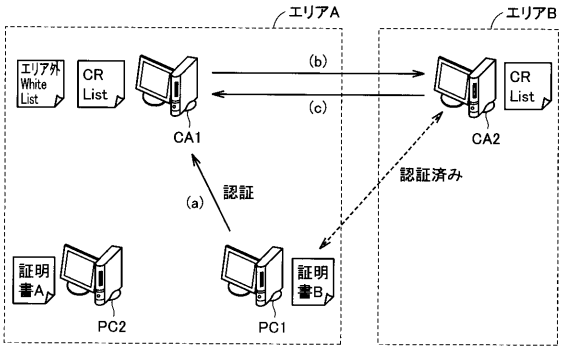
【図４】


PC
ネットワーク
その他処理部
提供
更新
問い合わせ
管理
接続処理部
CA認証
WhiteList管理
認証部
認証要求
認証検証
鍵ペア
データ送信部
データ作成部
データ解析部
データ受信部
エリア外 White List
証明書

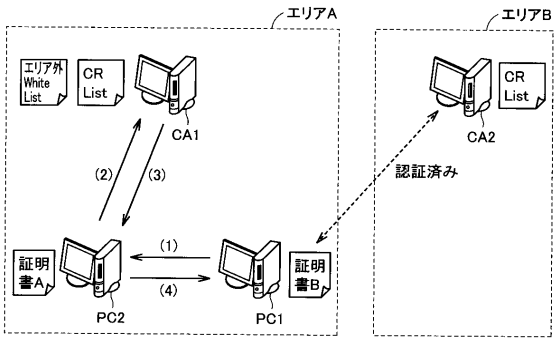
【図５】


エリアA
エリアB
CA1
CA2
認証
認証
移動
証明書A
証明書B
PC2
PC1

【図６】


エリアA
エリアB
エリア外 White List
CR List
CA1
CA2
(a)
認証
(b)
(c)
認証済み
証明書A
証明書B
PC2
PC1

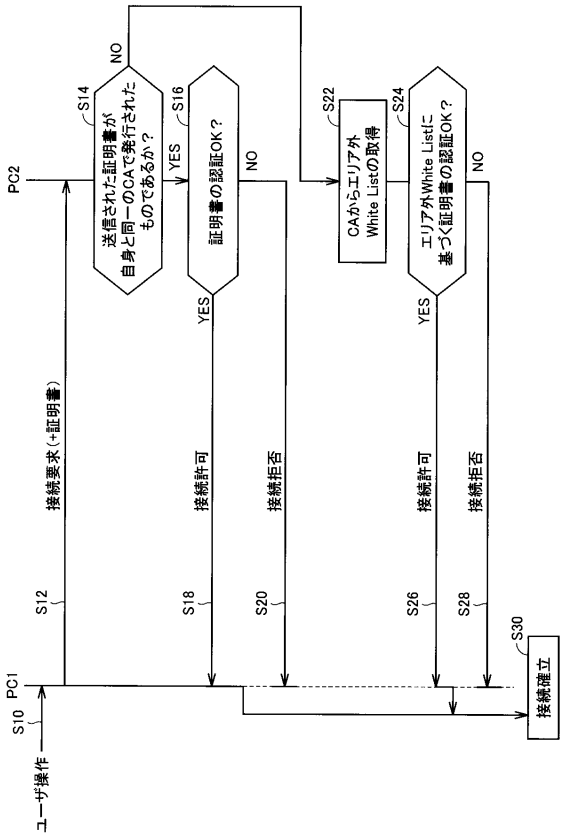
【図７】


エリアA
エリアB
エリア外 White List
CR List
CA1
CA2
(2)
(3)
(1)
(4)
認証済み
証明書A
証明書B
PC2
PC1

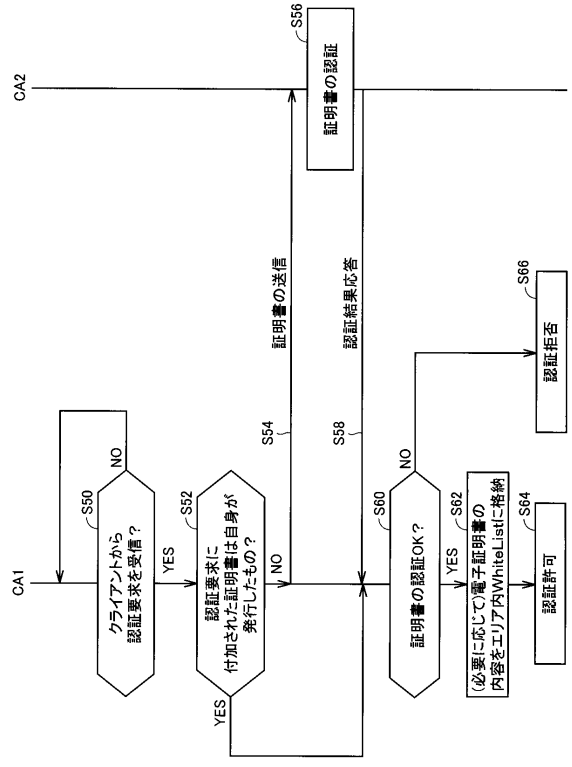
【図８】

No.1	デバイスX01のID (848ddd02-4a92-11da-a8 6b-5f4c40b81801)	デバイスX01の 証明書	デバイスX01の 利用許可証	有効期限 XXXX/YY/ZZ	許可アプリケーション ・XXXXX ・YYYYY
No.2	デバイスX02のID (848ddd02-4a92-11da-a8 6b-5f4c40b81802)	デバイスX02の 証明書	デバイスX02の 利用許可証	有効期限 XXXX/YY/UU	許可アプリケーション ・XXXXX ・ZZZZZ
No.3	デバイスX03のID (848ddd02-4a92-11da-a8 6b-5f4c40b81803)	デバイスX03の 証明書	デバイスX03の 利用許可証	有効期限 XXXX/YY/TT	許可アプリケーション ・XXXXX ・YYYYY
No.4	デバイスX04のID (969ddd02-4a92-11da-a8 6b-5f4c40b8180e)	デバイスX04の 証明書	デバイスX04の 利用許可証	有効期限 XXXX/YY/ZZ	許可アプリケーション ・XXXXX ・YYYYY
....	....	....	....	....	....

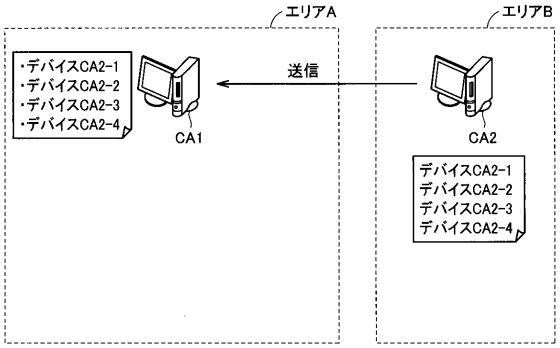
【図９】



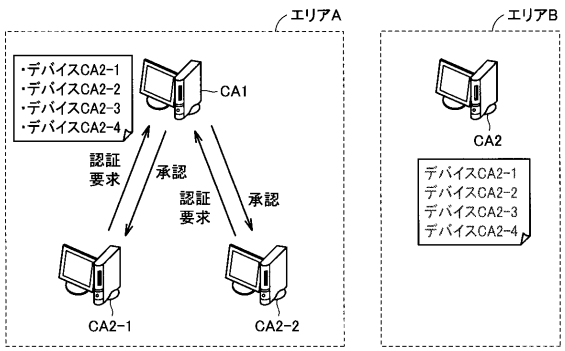
【図１０】



【図１１】



【図１２】



フロントページの続き

(56)参考文献 特開２００７－１１０３７７（ＪＰ，Ａ）
特開２００６－１６５８８１（ＪＰ，Ａ）
特開２００３－０３０３５８（ＪＰ，Ａ）
特開２００１－２９８４４８（ＪＰ，Ａ）
特開２００６－１０７３６０（ＪＰ，Ａ）
特開２００３－３１６４６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２