(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-116281
(P2007-116281A)
(43)公開日　平成19年5月10日(2007.5.10)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	200A	5K033
		H04L	12/28	200M	

審査請求 未請求　請求項の数 13　ＯＬ　（全 13 頁）

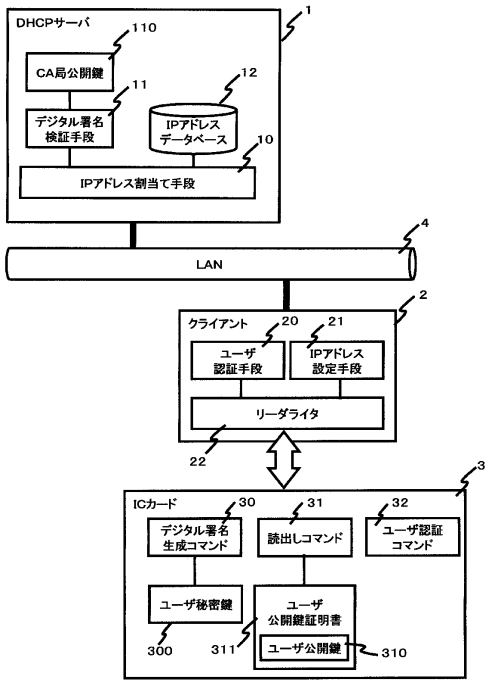
(21)出願番号　特願2005-303496 (P2005-303496)
(22)出願日　平成17年10月18日 (2005.10.18)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100111659
弁理士　金山　聡
(72)発明者　半田　富己男
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　矢野　義博
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

Ｆターム(参考)　5K033 AA08　CB09　CC01　EC03

(54)【発明の名称】ＤＨＣＰ運用システム、ＤＨＣＰ運用方法およびＤＨＣＰサーバ

(57)【要約】
【課題】正当なユーザが使用しているクライアントに対してのみ、動的にネットワークパラメータを割当てることができるＤＨＣＰ運用システムを提供する。
【解決手段】ＤＨＣＰサーバ１にクライアント２から送信されるＤＨＣＰのプロトコルメッセージには、ＩＣカード３に記憶されたユーザ秘密鍵３００によって生成されたデジタル署名が付加され、ＤＨＣＰサーバ１がプロトコルメッセージに付加されたデジタル署名を、クライアント２から取得したユーザ公開鍵３１０を用いて検証することで、クライアント２は、正当なユーザが使用しているクライアントであることを確認する。そして、ＤＨＣＰサーバ１は、正当なユーザが使用しているクライアントに対してのみ、動的にネットワークパラメータを割当てる。
【選択図】図２



【特許請求の範囲】
【請求項１】
クライアントを操作するユーザが所持する認証デバイスを利用して、ネットワークへの接続を管理するＤＨＣＰ運用システムであって、ネットワークに接続するクライアントは、前記認証デバイスとデータ通信する手段を備え、前記認証デバイスから、デジタル署名が付加された署名付きメッセージを取得し、前記ＤＨＣＰサーバは、前記クライアントが送信した前記署名付きメッセージのデジタル署名の正当性を検証し、デジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とするＤＨＣＰ運用システム。
【請求項２】
請求項１のＤＨＣＰ運用システムにおいて、前記認証デバイスは前記ユーザの正当性を認証する認証コマンドを備え、前記認証コマンドを用いた前記ユーザの認証に成功した場合のみ、前記クライアントは、前記認証デバイスから、デジタル署名が付加された署名付きメッセージを取得することを特徴とするＤＨＣＰ運用システム。
【請求項３】
請求項１または請求項２に記載のＤＨＣＰ運用システムにおいて、ユーザが所持する前記認証デバイスにはユーザの公開鍵であるユーザ公開鍵が前記公開鍵証明書の形式で記憶され、前記クライアントが前記認証デバイスから取得する前記署名付きメッセージは前記公開鍵証明書であって、前記ＤＨＣＰサーバは、前記公開鍵証明書を発行した発行者の公開鍵で、前記公開鍵証明書のデジタル署名の正当性を検証し、前記公開鍵証明書のデジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とするＤＨＣＰ運用システム。
【請求項４】
請求項３に記載のＤＨＣＰ運用システムにおいて、ユーザが所持する前記認証デバイスには、前記公開鍵証明書に加え、ユーザ公開鍵と対になるユーザの秘密鍵であるユーザ秘密鍵が記憶され、更に、前記認証デバイスは、ユーザ秘密鍵を用いて、前記クライアントから送信されるメッセージのデジタル署名を生成する手段を備え、前記クライアントは、ＤＨＣＰの一連の手順で前記ＤＨＣＰサーバと前記クライアント間で交換されるプロトコルメッセージを前記認証デバイスに送信し、前記認証デバイスから、前記ユーザ秘密鍵で生成されたプロトコルメッセージのデジタル署名を取得することで、前記署名付きメッセージとしてデジタル署名が付加された前記プロトコルメッセージを生成し、前記ＤＨＣＰサーバは、前記クライアントが送信した前記プロトコルメッセージのデジタル署名の正当性を、前記公開鍵証明書に記述された前記ユーザ公開鍵で検証し、前記プロトコルメッセージのデジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とするＤＨＣＰ運用システム。
【請求項５】
請求項１から請求項４のいずれかに記載のＤＨＣＰ運用システムにおいて、前記ユーザが所持する前記認証デバイスはＩＣカードであって、前記クライアントに備えられた前記認証デバイスとデータ通信する手段はリーダライタであることを特徴とするＤＨＣＰ運用システム。
【請求項６】
請求項１から請求項４のいずれかに記載のＤＨＣＰ運用システムにおいて、前記ユーザが所持する前記認証デバイスは、ＵＳＢトークンとすることを特徴とするＤＨＣＰ運用システム。
【請求項７】
クライアントを操作するユーザが所持する認証デバイスを利用して、ネットワークへの接続を管理するＤＨＣＰサーバであって、前記ＤＨＣＰサーバは、ネットワークに接続する前記クライアントから送信され、デジタル署名が付加されたメッセージである署名付きメッセージのデジタル署名の正当性を検証するデジタル署名認証手段を備え、デジタル署

名の正当性が確認された前記署名付きメッセージを送信した前記クライアントに対してのみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とするＤＨＣＰサーバ。

【請求項８】

請求項７に記載のＤＨＣＰサーバにおいて、前記ＤＨＣＰサーバが前記クライアントから受信する前記署名付きメッセージの一つは、前記クライアントを操作するユーザの公開鍵であるユーザ公開鍵の公開鍵証明書であって、前記ＤＨＣＰサーバに備えられた前記デジタル署名認証手段は、前記公開鍵証明書のデジタル署名の正当性を、前記公開鍵証明書を発行した発行機関の公開鍵で検証することを特徴とするＤＨＣＰサーバ。

【請求項９】

請求項８に記載のＤＨＣＰサーバにおいて、前記ＤＨＣＰサーバが前記クライアントから受信する前記署名付きメッセージの一つは、前記ユーザ公開鍵と対になる秘密鍵であるユーザ秘密鍵で生成されたデジタル署名が付加され、ＤＨＣＰの一連の手順で前記ＤＨＣＰサーバと前記クライアント間で交換されるプロトコルメッセージであって、前記ＤＨＣＰサーバは、前記クライアントが送信した前記プロトコルメッセージのデジタル署名の正当性を、前記公開鍵証明書に記述された前記ユーザ公開鍵で検証することを特徴とするＤＨＣＰサーバ。

【請求項１０】

ユーザが所持する認証デバイスを利用したＤＨＣＰ運用方法であって、前記ＤＨＣＰ運用方法は、

（ａ）ＤＨＣＰを用いてネットワークに接続するクライアントが、前記認証デバイスから、デジタル署名が付加された署名付きメッセージを取得するステップ、（ｂ）前記ＤＨＣＰサーバが、前記クライアントが送信した前記署名付きメッセージのデジタル署名の正当性を検証するステップ、

（ｃ）デジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てるステップ、

とを含むことを特徴とするＤＨＣＰ運用方法。

【請求項１１】

請求項１０に記載のＤＨＣＰ運用方法において、前記認証デバイスは前記ユーザの正当性を認証する認証コマンドを備え、前記認証コマンドを用いた前記ユーザの認証に成功した場合のみ、前記ステップ（ａ）を実行することを特徴とするＤＨＣＰ運用方法。

【請求項１２】

請求項１０または請求項１１に記載のＤＨＣＰ運用方法において、ユーザが所持する前記認証デバイスにはユーザの公開鍵であるユーザ公開鍵が前記公開鍵証明書の形式で記憶され、

前記ステップ（ａ）は、（ａ１）前記クライアントが前記認証デバイスから前記署名付きメッセージとして前記公開鍵証明書を取得するステップを含み、

前記ステップ（ｂ）は、（ｂ１）前記ＤＨＣＰサーバは、前記公開鍵証明書を発行した発行者の公開鍵で、前記公開鍵証明書のデジタル署名の正当性を検証するステップを含むことを特徴とするＤＨＣＰ運用方法。

【請求項１３】

請求項１２に記載のＤＨＣＰ運用方法において、ユーザが所持する前記認証デバイスには、前記公開鍵証明に加え、ユーザ公開鍵と対になるユーザの秘密鍵であるユーザ秘密鍵が記憶され、更に、前記認証デバイスは、ユーザ秘密鍵を用いて、前記クライアントから送信されるメッセージのデジタル署名を生成する手段を備え、

前記ステップ（ａ）は、（ａ２）前記クライアントは、ＤＨＣＰの一連の手順で前記ＤＨＣＰサーバと前記クライアント間で交換されるプロトコルメッセージを前記認証デバイスに送信し、前記認証デバイスから前記プロトコルメッセージのデジタル署名を取得して、前記署名付きメッセージとしてデジタル署名が付加された前記プロトコルメッセージを生成するステップを含み、

ステップ（ｂ）は、（ｂ２）前記ＤＨＣＰサーバは、前記クライアントが送信した前記プロトコルメッセージのデジタル署名の正当性を、前記公開鍵証明書に記述された前記ユーザ公開鍵で検証するステップを含むことを特徴とするＤＨＣＰ運用方法。

【発明の詳細な説明】
【技術分野】
【０００１】
発明は、ＤＨＣＰサーバを利用し、ネットワークに接続するクライアントに対して、動的かつ自動的にネットワークパラメータを割当てる技術に関し、更に詳しくは、認証されたクライアントに対してのみ、動的かつ自動的にネットワークパラメータを割当てる技術に関する。
【背景技術】
【０００２】
ＤＨＣＰ（Dynamic Host Configuration Protocol）とは、サーバがクライアントに、ＩＰアドレスなどのネットワーク接続に必要なネットワークパラメータを、動的に割当てるプロトコルである。ＤＨＣＰは、ネットワークに接続されたクライアントに対してのみ、ＩＰアドレスなどのネットワークパラメータを割当てるので、限られたＩＰアドレスを有効に活用したいネットワークシステム（例えば、大学のネットワークシステム）に適している。
【０００３】
非特許文献１で定義されているように、ＤＨＣＰでクライアントに動的にネットワークパラメータを割当てるときは、まず、ＤＨＣＰを利用してネットワークへの接続を希望するクライアントが、ＤＨＣＰの機能を備えたサーバ（以下、ＤＨＣＰサーバ）を発見するため、ネットワークに接続されたサーバ・コンピュータ対してＤＨＣＰＤＩＳＣＯＶＥＲメッセージをブロードキャストする。そして、ＤＨＣＰサーバーは、そのＤＨＣＰＤＩＳＣＯＶＥＲメッセージに対して、クライアントが利用可能なネットワークパラメータを通知し、クライアントは、通知されたネットワークパラメータの中から、クライアントが利用したいネットワークパラメータを打診し、ＤＨＣＰサーバが、クライアントにそのネットワークパラメータの利用を許可することで、クライアントに動的にネットワークパラメータが割当てられる。
【０００４】
このように、ＤＨＣＰサーバは、ネットワークに接続要求のあったクライアントを識別・認証しないので、ネットワークにアクセス権を持たない者が使用するクライアントから要求があった場合でも、ネットワークへの接続を許可してしまう可能性があるため、ネットワーク上のコンピュータに格納されている機密情報が第三者のクライアントからアクセスされてしまう危険性がある。
【０００５】
許可されたクライアントに対してのみ、ネットワークパラメータを割当てる技術としては、特許文献１で、ネットワークへの接続が許可されているクライアントのＭＡＣアドレスをＤＨＣＰサーバに登録し、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージを送信したクライアントのＭＡＣアドレスがＤＨＣＰサーバに登録されていた場合のみ、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージを送信したクライアントに対してＩＰアドレスを動的に割当てるＤＨＣＰサーバが開示されている。
【非特許文献１】（社）日本ネットワークインフォメーションセンターの
ＨＰで公開されている技術資料　ＵＲＬ：http://rfc-jp.nic.ad.jp/rfc/rfc2131.txt
【特許文献１】特開２００１－２１１１８０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、特許文献１で開示されているように、クライアントごとに固有の情報であるＭＡＣアドレスを利用して、ネットワークに接続するクライアントを認証する技術では、悪意のある者がパケットのＭＡＣアドレスを書き換えて正当なクライアントを使用しているかのようになりすますことで、不正にネットワークにアクセスできてしまう可能性がある。加えて、予めＭＡＣアドレスがＤＨＣＰサーバに登録されていないクライアントでしかネットワークに接続できないと、ユーザが利用できるクライアントが限定されるため、ユーザの利便性が悪くなってしまう問題がある。
【０００７】
そこで、上述した問題を鑑みて、本発明は、上述のなりすまし行為も含め、悪意のある者がネットワークへ不正にアクセスすることをセキュリティ高く防止でき、かつ、ユーザが利用できるクライアントを限定することがなくユーザの利便性を高めることのできる、ＤＨＣＰ運用システム、ＤＨＣＰ運用方法、およびＤＨＣＰサーバ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】
【０００８】
上述した課題を解決する第１の発明の態様１は、クライアントを操作するユーザが所持する認証デバイスを利用して、ネットワークへの接続を管理するＤＨＣＰ運用システムであって、ネットワークに接続するクライアントは、前記認証デバイスとデータ通信する手段を備え、前記認証デバイスから、デジタル署名が付加された署名付きメッセージを取得し、前記ＤＨＣＰサーバは、前記クライアントが送信した前記署名付きメッセージのデジタル署名の正当性を検証し、デジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とする。
【０００９】
ここで前記認証デバイスとは、ユーザが携帯可能で、ユーザの公開鍵証明書や公開鍵の暗号鍵対などの情報を機密に格納でき、好ましくは、公開鍵暗号を用いたデジタル署名生成機能や暗号演算機能を備えたデバイスを意味する。
【００１０】
第１の発明の態様１によれば、前記ＤＨＣＰサーバが、前記クライアントから前記署名付きメッセージを受信し、前記署名付きメッセージのデジタル署名を検証することで、前記ＤＨＣＰサーバは、前記クライアントが正当なユーザが使用していることを確認できる。
【００１１】
加えて、前記ＤＨＣＰサーバが、前記署名付きメッセージのデジタル署名を検証することで、前記ＤＨＣＰサーバは、前記署名付きメッセージのメッセージが改ざんされていないことを確認でき、悪意のある者が正当なクライアントを使用しているかのようになりすまして、不正にネットワークに接続することを防止できる。
【００１２】
第１の発明の態様２は、ＤＨＣＰ運用システムの態様１において、前記認証デバイスは前記ユーザの正当性を認証する認証コマンドを備え、前記認証コマンドを用いた前記ユーザの認証に成功した場合のみ、前記クライアントは、前記認証デバイスから、デジタル署名が付加された署名付きメッセージを取得又することを特徴とする。
【００１３】
第１の発明の態様２によれば、前記認証デバイスが前記認証コマンドを備えることで、前記認証デバイスの盗難時などに、正当なユーザ以外の者が前記認証デバイスを不正に使用することを防止できる。
【００１４】
第１の発明の態様３は、ＤＨＣＰ運用システムの態様１または態様２において、ユーザが所持する前記認証デバイスにはユーザの公開鍵であるユーザ公開鍵が前記公開鍵証明書

の形式で記憶され、前記クライアントが前記認証デバイスから取得する前記署名付きメッセージは前記公開鍵証明書であって、前記ＤＨＣＰサーバは、前記公開鍵証明書を発行した発行者の公開鍵で、前記公開鍵証明書のデジタル署名の正当性を検証し、前記公開鍵証明書のデジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とする。

【００１５】

第１の発明の態様３によれば、前記ＤＨＣＰサーバが前記クライアントから前記公開鍵証明書を取得することで、前記クライアントを操作しているユーザの正当性は、前記公開鍵証明書を発行した発行機関によって保証される。

【００１６】

第１の発明の態様４は、ＤＨＣＰ運用システムの態様３において、ユーザが所持する前記認証デバイスには、前記公開鍵証明に加え、ユーザ公開鍵と対になるユーザの秘密鍵であるユーザ秘密鍵が記憶され、更に、前記認証デバイスは、ユーザ秘密鍵を用いて、前記クライアントから送信されるメッセージのデジタル署名を生成する手段を備え、前記クライアントは、ＤＨＣＰの一連の手順で前記ＤＨＣＰサーバと前記クライアント間で交換されるプロトコルメッセージを前記認証デバイスに送信し、前記認証デバイスから、前記ユーザ秘密鍵で生成されたプロトコルメッセージのデジタル署名を取得することで、前記署名付きメッセージとしてデジタル署名が付加された前記プロトコルメッセージを生成し、前記ＤＨＣＰサーバは、前記クライアントが送信した前記プロトコルメッセージのデジタル署名の正当性を、前記公開鍵証明書に記述された前記ユーザ公開鍵で検証し、前記プロトコルメッセージのデジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とする。

【００１７】

第１の発明の態様４によれば、前記ＤＨＣＰサーバが、デジタル署名が付加された前記プロトコルメッセージを前記クライアントから受信し、このデジタル署名を検証することで、前記プロトコルメッセージを送信した発信したユーザを確認できるとともに、前記プロトコルメッセージが改ざんされていないことを確認できる。

【００１８】

第１の発明の態様５は、ＤＨＣＰ運用システムの態様１から態様４のいずれかにおいて、前記ユーザが所持する前記認証デバイスはＩＣカードであって、前記クライアントに備えられた前記認証デバイスとデータ通信する手段はリーダライタであることを特徴とする。

【００１９】

ここで、ＩＣカードとは、接触ＩＣカード、非接触ＩＣカードまたはデュアルインターフェースＩＣカードのいずれかのＩＣカードであってもよく、更には、ＩＣカードは、ＳＩＭ（Subscriber Identity Module）やＵＩＭ（User Identity Module）やＭＯＰＡＳＳカード(Mobile Passport, HYPERLINK "http://www.mopass.info/" http://www.mopass.info/ 参照)をも意味している。

【００２０】

第１の発明の態様６は、ＤＨＣＰ運用システムの態様１から態様４のいずれかにおいて、前記ユーザが所持する前記認証デバイスは、ＵＳＢトークンとすることを特徴とする。

【００２１】

第１の発明の態様５によれば、前記ユーザが所持する前記認証デバイスはＩＣカードとすることで、前記認証デバイスの携帯性が高まるばかりか、前記認証デバイスに他の機能（例えば、学生書の機能）を付加することも容易になる。また、第１の発明の態様６によれば、前記認証デバイスをＵＳＢトークンとすることで、前記クライアントには、前記認証デバイスとデータ通信するリーダライタは不要になる。

【００２２】

更に、上述した問題を解決する第２の発明の態様１は、クライアントを操作するユーザが所持する認証デバイスを利用して、ネットワークへの接続を管理するＤＨＣＰサーバで

あって、前記ＤＨＣＰサーバは、ネットワークに接続する前記クライアントから送信され、デジタル署名が付加されたメッセージである署名付きメッセージのデジタル署名の正当性を検証するデジタル署名認証手段を備え、デジタル署名の正当性が確認された前記署名付きメッセージを送信した前記クライアントに対してのみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てることを特徴とする。

【００２３】

第２の発明の態様２は、ＤＨＣＰサーバの態様１において、前記ＤＨＣＰサーバが前記クライアントから受信する前記署名付きメッセージの一つは、前記クライアントを操作するユーザの公開鍵であるユーザ公開鍵の公開鍵証明書であって、前記ＤＨＣＰサーバに備えられた前記デジタル署名認証手段は、前記公開鍵証明書のデジタル署名の正当性を、前記公開鍵証明書を発行した発行機関の公開鍵で検証することを特徴とする。

【００２４】

第２の発明の態様３は、ＤＨＣＰサーバの態様２において、前記ＤＨＣＰサーバが前記クライアントから受信する前記署名付きメッセージの一つは、前記ユーザ公開鍵と対になる秘密鍵であるユーザ秘密鍵で生成されたデジタル署名が付加され、ＤＨＣＰの一連の手順で前記ＤＨＣＰサーバと前記クライアント間で交換されるプロトコルメッセージであって、前記ＤＨＣＰサーバは、前記クライアントが送信した前記プロトコルメッセージのデジタル署名の正当性を、前記公開鍵証明書に記述された前記ユーザ公開鍵で検証することを特徴とする。

【００２５】

更に、上述した問題を解決する第３の発明の態様１は、ユーザが所持する認証デバイスを利用したＤＨＣＰ運用方法であって、前記ＤＨＣＰ運用方法は、（ａ）ＤＨＣＰを用いてネットワークに接続するクライアントが、前記認証デバイスから、デジタル署名が付加された署名付きメッセージを取得するステップ、（ｂ）前記ＤＨＣＰサーバが、前記クライアントが送信した前記署名付きメッセージのデジタル署名の正当性を検証するステップ、（ｃ）デジタル署名の正当性が確認された場合のみ、ＤＨＣＰに従い、前記クライアントに対してネットワークパラメータを動的に割当てるステップ、とを含むことを特徴とする。

【００２６】

第３の発明の態様２は、ＤＨＣＰ運用方法の態様１において、前記認証デバイスは前記ユーザの正当性を認証する認証コマンドを備え、前記認証コマンドを用いた前記ユーザの認証に成功した場合のみ、前記ステップ（ａ）を実行することを特徴とする。

【００２７】

第３の発明の態様３は、ＤＨＣＰ運用方法の態様１または態様２において、ユーザが所持する前記認証デバイスにはユーザの公開鍵であるユーザ公開鍵が前記公開鍵証明書の形式で記憶され、前記ステップ（ａ）は、（ａ１）前記クライアントが前記認証デバイスから前記署名付きメッセージとして前記公開鍵証明書を取得するステップを含み、前記ステップ（ｂ）は、（ｂ１）前記ＤＨＣＰサーバは、前記公開鍵証明書を発行した発行者の公開鍵で、前記公開鍵証明書のデジタル署名の正当性を検証するステップを含むことを特徴とする。

【００２８】

第３の発明の態様４は、ＤＨＣＰ運用方法の態様３において、ユーザが所持する前記認証デバイスには、前記公開鍵証明書に加え、ユーザ公開鍵と対になるユーザの秘密鍵であるユーザ秘密鍵が記憶され、更に、前記認証デバイスは、ユーザ秘密鍵を用いて、前記クライアントから送信されるメッセージのデジタル署名を生成する手段を備え、前記ステップ（ａ）は、（ａ２）前記クライアントは、ＤＨＣＰの一連の手順で前記ＤＨＣＰサーバと前記クライアント間で交換されるプロトコルメッセージを前記認証デバイスに送信し、前記認証デバイスから前記プロトコルメッセージのデジタル署名を取得して、前記署名付きメッセージとしてデジタル署名が付加された前記プロトコルメッセージを生成するステップを含み、ステップ（ｂ）は、（ｂ２）前記ＤＨＣＰサーバは、前記クライアントが送

信した前記プロトコルメッセージのデジタル署名の正当性を、前記公開鍵証明書に記述された前記ユーザ公開鍵で検証するステップを含むことを特徴とする。

【発明の効果】

【００２９】

上述した本発明によれば、本発明は、なりすまし行為も含め、悪意を持ったユーザがネットワークへ不正にアクセスすることをセキュリティ高く防止でき、かつ、ユーザが利用できるクライアントを限定することなくユーザの利便性を高めることのできる、ＤＨＣＰ運用システム、ＤＨＣＰ運用方法、およびＤＨＣＰサーバを提供できる。

【発明を実施するための最良の形態】

【００３０】

ここから本発明に係り、クライアントにＩＰアドレスを動的に割当てるＤＨＣＰ運用システムについて、図を参照しながら詳細に説明する。図１は、本発明に係るＤＨＣＰ運用システムのネットワークトポロジーである。図１に示したように、本発明に係るＤＨＣＰ運用システムは、ユーザが所持する認証デバイスであるＩＣカード３とデータ通信するためのリーダライタ２２を備え、ＤＨＣＰを利用しＬＡＮ４（Local Area Network）に接続するクライアント２と、クライアント２に対し、動的にＩＰアドレスを振り分けるＤＨＣＰサーバ１とが、ＬＡＮ４に接続されている。

【００３１】

図１のＤＨＣＰ運用システムでは、「公開鍵基盤」（PKI: Public Key Infrastructure）の機能を備えたＩＣカード３をユーザは所持し、ＤＨＣＰサーバ１は、ユーザが所持するＩＣカード３を利用して、ＬＡＮ４に接続するクライアント２を操作しているユーザの正当性を確認し、正当なユーザが操作しているクライアント２に対してのみＩＰアドレスを割当てる。

【００３２】

なお、実際は、ＬＡＮ４には、ＤＨＣＰサーバ１およびクライアント２以外の複数のコンピュータが接続されているが、本発明を分かり易く説明するために、図１では、ＤＨＣＰサーバ１およびクライアント２以外のコンピュータは図示していない。

【００３３】

図２は、図１のＤＨＣＰ運用システムのブロック図である。図２に示したように、ＤＨＣＰサーバ１には、ＤＨＣＰに従い、ＬＡＮ４に接続するクライアント２に対し動的にＩＰアドレスを割当てる手段であるＩＰアドレス割当て手段１０と、クライアント２に割当てるＩＰアドレスを管理するデータベースであるＩＰアドレスデータベース１２と、ある特定のアルゴリズムにてデジタル署名を検証するデジタル署名検証手段１１を備え、予めＤＨＣＰサーバ１は公開鍵として、第三者機関であるＣＡ局（CA: Certificate Authority）の公開鍵であるＣＡ局公開１１０鍵を有している。

【００３４】

ＤＨＣＰサーバ１に備えられたＩＰアドレス割当て手段１１は、ＤＨＣＰに準拠して、ＬＡＮ４に接続するクライアント２に対し、動的にＩＰアドレスを割当てる手段である。ＤＨＣＰサーバ１は、ＩＰアドレス以外のネットワークパラメータ（例えば、サブネットマスクや、ゲートウェイサーバなど）を割当てることもができるが、本実施の形態では、ＤＨＣＰサーバ１はＩＰアドレスのみを割当てるものとしている。

【００３５】

ＤＨＣＰサーバ１がクライアント２に割当てることのできるいくつかのＩＰアドレスは、予めＩＰアドレスデータベース１２に登録されている。ＤＨＣＰサーバ１は、クライアント２に割当てたＩＰアドレスに関連付けて、ＭＡＣアドレスなどのクライアント２ごとに固有な情報をＩＰアドレスデータベース１２に記憶することで、ＩＰアドレスの管理を行う。

【００３６】

従来のＤＨＣＰサーバ１と本発明に係るＤＨＣＰサーバ１とで異なる点は、ＤＨＣＰサーバ１は、ＰＫＩを利用して、クライアント２を操作しているユーザの正当性を確認し、

正当性の確認されたユーザが操作しているクライアント２に対してのみ、動的にＩＰアドレスを割当てる点である。

【００３７】

クライアント２を操作しているユーザの正当性の確認は、クライアント２から送信されるメッセージに付加されたデジタル署名を検証することで行われる。詳しくは、クライアント２から送信されるＤＨＣＰのプロトコルメッセージに付加されるデジタル署名は、ＩＣカード３に機密に記憶されたユーザの秘密鍵であるユーザ秘密鍵３００によって生成され、ＤＨＣＰサーバ１のＩＰアドレス割当て手段１０は、ＤＨＣＰのプロトコルメッセージに付加されたデジタル署名を、クライアント２から取得したユーザの公開鍵であるユーザ公開鍵３１１を用いて、このデジタル署名を検証することで、クライアント２を操作しているユーザの正当性は確認される。

【００３８】

なお、ＤＨＣＰサーバ１は、クライアント２からＣＡ局が発行したユーザ公開鍵３１０の公開鍵証明書３１１を取得し、ユーザ公開鍵証明書３１１のデジタル署名をＣＡ局公開鍵１１０で検証することで、ユーザ公開鍵証明書３１１の信頼性モデルに基づき、ユーザ公開鍵３１０の正当性はＣＡ局によって保証される。

【００３９】

ＤＨＣＰサーバ１を利用してＬＡＮ４に接続するクライアント２には、ＤＨＣＰに準拠し、ＤＨＣＰサーバ１からＩＰアドレスを取得し設定するＩＰアドレス設定手段２１と、ＩＣカード３を用いて、クライアント２を操作するユーザを認証する手段であるユーザ認証手段２０と、ＩＣカード３とデータ通信するための手段であるリーダライタ２２とを備えている。

【００４０】

クライアント２に備えられたユーザ認証手段２０がユーザを認証する方法は、如何なる方法でもよく、例えば、銀行のＡＴＭのようにユーザのＰＩＮ（Personal Identification Number）を照合することでユーザを認証する方法でもよく、ユーザの指紋情報や静脈情報などの生体情報を照合することでユーザを認証する方法でもよい。

【００４１】

クライアント２を操作するユーザが所持するＩＣカード３は、公開鍵暗号の暗号鍵対として、ユーザの秘密鍵であるユーザ秘密鍵３００と、ユーザの公開鍵であるユーザ公開鍵３１０を公開鍵証明書の形式で有している。ユーザ公開鍵３１０の公開鍵証明書であるユーザ公開鍵証明書３１１には、ＣＡ局によって、ＤＨＣＰサーバ１のデジタル署名検証手段１１に対応したアルゴリズムに従い、ＤＨＣＰサーバ１が有するＣＡ局公開鍵１１０と対になるＣＡ局秘密鍵を用い、デジタル署名が付加されている。

【００４２】

また、ＩＣカード３には、ユーザ秘密鍵３００を用いてデジタル署名を生成するデジタル署名生成コマンド３０と、ユーザ公開鍵証明書３１１を外部装置（ここでは、リーダライタ）に送信する読出しコマンド３１と、外部装置から送信される認証情報とＩＣカード３に記憶された参照情報とを照合し、ＩＣカード３を利用するユーザを認証するユーザ認証コマンド３２を備えている。

【００４３】

ＩＣカード３に備えられたユーザ認証コマンド３０は、クライアント２に備えられたユーザ認証手段２０と同じユーザ認証の方法で、ユーザを認証するコマンドである。例えば、クライアント２に備えられたユーザ認証手段２０がユーザの指紋情報を認証する手段であるならば、ＩＣカード３に備えられたユーザ認証コマンド３０は、リーダライタ２２から送信された認証情報である指紋情報と、ＩＣカード３に記憶された参照情報とを照合するコマンドになる。

【００４４】

なお、ＩＣカード３に備えられたデジタル署名生成コマンド３０と読出しコマンド３１とは、ユーザ認証コマンド３２が外部装置（ここでは、リーダライタ２２）から送信され

る認証情報とＩＣカード３に記憶された参照情報との照合に成功した場合のみ動作できるように設計されている。

【００４５】

ここから、図１および図２で示したＤＨＣＰ運用システムの動作について、図を参照しながら詳細に説明する。なお、ＤＨＣＰ運用システムの動作の説明は、本発明に係るＤＨＣＰ運用方法の説明も兼ねている。

【００４６】

図３は、ＤＨＣＰ運用システムのシーケンスダイアグラムである。ＤＨＣＰ運用システムのシーケンスの手順１では、ユーザを認証するための情報であるユーザ認証情報をクライアント２がユーザから取得し、ユーザ認証情報の照合をＩＣカード３に要求する動作が実行される。

【００４７】

クライアント２に備えられたユーザ認証手段２０が、ＰＩＮを照合しユーザを認証する手段であるときは、クライアント２は、ユーザが入力したＰＩＮを認証情報とし、認証情報を含むユーザ認証コマンド３２のＡＰＤＵをＩＣカード３に送信することで、ＩＣカード３を所持するユーザを認証する。また、クライアント２に備えられたユーザ認証手段２０が、指紋情報を照合しユーザを認証する手段であるときは、クライアント２は、ユーザから読み取った指紋情報を認証情報とし、認証情報を含むユーザ認証コマンド３２のＡＰＤＵをＩＣカード３に送信することで、ＩＣカード３を所持するユーザを認証する。

【００４８】

次に実行される手順２では、ＩＣカード３がユーザ認証コマンド３２の実行結果をクライアント２に返信する。この手順２では、ＩＣカード３は、ユーザ認証コマンド３２のコマンドＡＰＤＵに含まれる認証情報とＩＣカード３に記憶された参照情報とを、定められたアルゴリズムに従い照合することでユーザを認証し、ユーザの認証結果を示すレスポンスＡＰＤＵを、クライアント２に返信する。

【００４９】

手順１および手順２でＩＣカード３を所持するユーザを認証するのは、例えば、ＩＣカード３の盗難時などで、不正にＩＣカード３が利用されることを防止するためである。上述したように、ＩＣカード３に備えられたデジタル署名生成コマンド３０と読取りコマンド３１は、ユーザ認証コマンド３２が成功した場合のみ動作するので、正当なユーザでない場合は手順２以降の手順は実行されず、クライアント２はＬＡＮ４に接続できない。

【００５０】

手順２で、ＩＣカード３がユーザの認証に成功したときに実行される手順３では、クライアント２のＩＰアドレス設定手段２１は、読取りコマンド３１のコマンドＡＰＤＵをＩＣカード３に送信することで、ＩＣカード３に対してユーザ公開鍵証明書３１１の送信を要求する。

【００５１】

手順４では、ＩＣカード３は、手順２でユーザの認証に成功していた場合のみ、読取りコマンド３１を実行し、ユーザ公開鍵証明書３１１を含むレスポンスＡＰＤＵがＩＣカード３からクライアント２に返信される。

【００５２】

次の手順５では、クライアント２のＩＰアドレス設定手段２１は、ＤＨＣＰのプロトコルメッセージの一つであるＤＨＣＰＤＩＳＣＯＶＥＲメッセージを生成し、生成したＤＨＣＰＤＩＳＣＯＶＥＲメッセージのデジタル署名生成をＩＣカード３に要求する。

【００５３】

クライアント２のＩＰアドレス設定手段２１は、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージのデジタル署名を生成するために、デジタル署名生成コマンド３０のコマンドＡＰＤＵをＩＣカード３に送信する。このコマンドＡＰＤＵには、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージが含まれる。

【００５４】

次の手順６では、ＩＣカード３は、手順２でユーザの認証に成功していた場合のみ、デジタル署名生成コマンド３０は実行され、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージのデジタル署名を生成した後、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージのデジタル署名を含むレスポンスＡＰＤＵがＩＣカード３からクライアント２に返信される。

【００５５】

次の手順７では、クライアント２のＩＰアドレス設定手段２１がＤＨＣＰサーバ１を発見するために、クライアント２はＤＨＣＰＤＩＳＣＯＶＥＲメッセージをブロードキャストする。この手順７でクライアント２がブロードキャストするＤＨＣＰＤＩＳＣＯＶＥＲメッセージには、手順６でＩＣカード３から取得したデジタル署名が付加され、また、このＤＨＣＰＤＩＳＣＯＶＥＲメッセージには、手順４でクライアント２のＩＰアドレス設定手段２１が取得したユーザ公開鍵証明書３１１が含まれる。

【００５６】

次の手順８では、ＤＨＣＰサーバ１は受信したＤＨＣＰＤＩＳＣＯＶＥＲメッセージに含まれるユーザ公開鍵証明書３１１をＣＡ局公開鍵１１０で検証し、クライアント２を操作しているユーザのユーザ公開鍵３１０の正当性を確認する。そして、ユーザ公開鍵３１０の正当性が確認した後、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージのデジタル署名をユーザ公開鍵３１０で検証し、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージのデジタル署名がユーザ公開鍵３１０で検証された場合のみ、クライアント２が利用できるＩＰアドレスのリストを含むＤＨＣＰＯＦＦＥＲメッセージを、クライアント２に返信する。

【００５７】

この手順８で、ユーザ公開鍵証明書３１１をＣＡ局公開鍵１１０で検証することで、クライアント２を操作しているユーザは、正当なユーザ公開鍵３１０を所持している正当なユーザであることが確認され、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージのデジタル署名をユーザ公開鍵３１０で検証することで、ＬＡＮ４にアクセスするクライアント２は正当なユーザによって操作されているクライアント２であり、送信されたＤＨＣＰＤＩＳＣＯＶＥＲメッセージは改ざんされていないことが確認される。

【００５８】

次の手順９では、クライアント２のＩＰアドレス設定手段２１は、ＤＨＣＰサーバ１から受信したＤＨＣＰＯＦＦＥＲメッセージに含まれるＩＰアドレスのリストの中から、一つのＩＰアドレスを選択し、選択したＩＰアドレスを含むＤＨＣＰＲＥＱＵＥＳＴメッセージを生成し、ＤＨＣＰＲＥＱＵＥＳＴメッセージのデジタル署名生成をＩＣカード３に要求する。

【００５９】

次の手順１０では、手順６と同様な内容が実行され、ＩＣカード３から、クライアント２のＩＰアドレス設定手段２１はＤＨＣＰＲＥＱＵＥＳＴメッセージのデジタル署名を取得する。そして、次の手順１１では、クライアント２は、手順１０で取得したデジタル署名が付加されたＤＨＣＰＲＥＱＵＥＳＴメッセージをブロードキャストする。

【００６０】

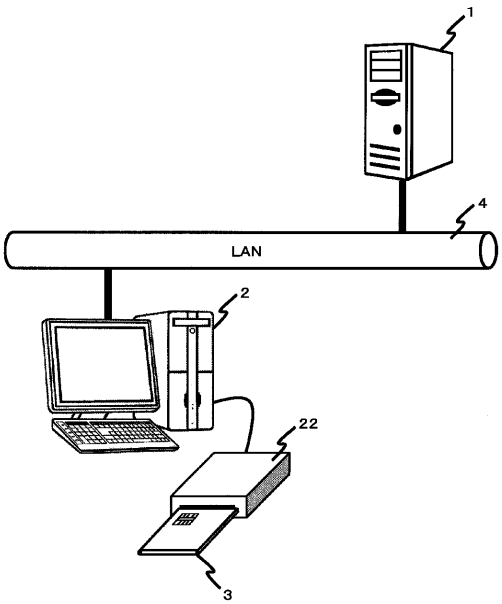
そして、次の手順１２では、ＤＨＣＰサーバ１は、手順８と同様にＤＨＣＰＲＥＱＵＥＳＴメッセージのデジタル署名を検証し、ＤＨＣＰＲＥＱＵＥＳＴメッセージのデジタル署名の検証に成功した場合は、ＤＨＣＰサーバ１は、受信したＤＨＣＰＲＥＱＵＥＳＴメッセージは正当なメッセージあると判断し、ＤＨＣＰＲＥＱＵＥＳＴメッセージに含まれるＩＰアドレスの使用を許可できる場合は、クライアント２に対して、ＤＨＣＰＡＣＫを送信し、クライアント２のＩＰアドレス設定手段２１は、クライアント２のＩＰアドレスを手順９で選択したＩＰアドレスに設定する。

【００６１】

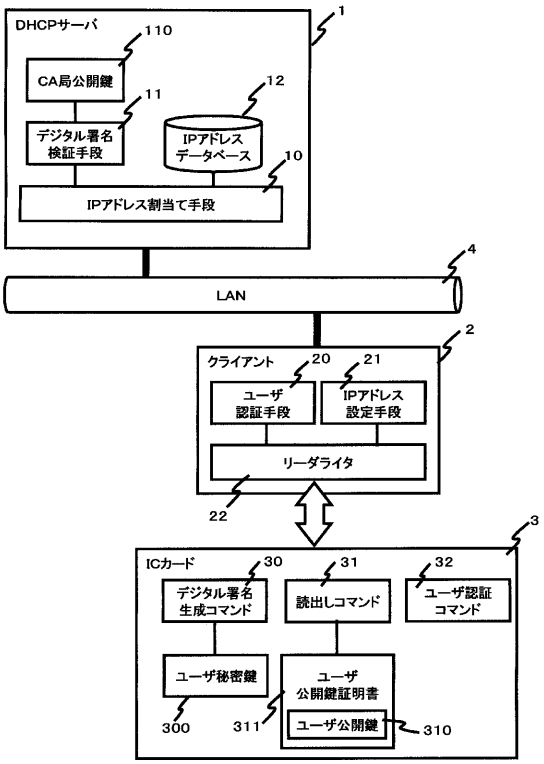
また、手順１２では、ＤＨＣＰＲＥＱＵＥＳＴメッセージのデジタル署名の検証に失敗した場合、もしくは、ＤＨＣＰＲＥＱＵＥＳＴメッセージに含まれるＩＰアドレスの使用許可をできない場合は、クライアント２に対して、ＤＨＣＰＮＡＣメッセージを送信し、クライアント２がＬＡＮ４に接続することは否認される。

【図面の簡単な説明】
【００６２】
【図１】ＤＨＣＰ運用システムのネットワークトポロジー。
【図２】ＤＨＣＰ運用システムのブロック図。
【図３】ＤＨＣＰ運用システムのシーケンスダイアグラム。
【符号の説明】
【００６３】
１　ＤＨＣＰサーバ
１１　デジタル署名検証手段
１１０　ＣＡ局公開鍵
１２　ＩＰアドレス割当て手段
２　クライアント
２０　ユーザ認証手段
２１　ＩＰアドレス取得手段
２２　リーダライタ
３　ＩＣカード
３０　デジタル署名生成コマンド
３００　ユーザ秘密鍵
３１　読出しコマンド
３１０　ユーザ公開鍵、３１１　ユーザ公開鍵証明書
３２　ユーザ認証コマンド

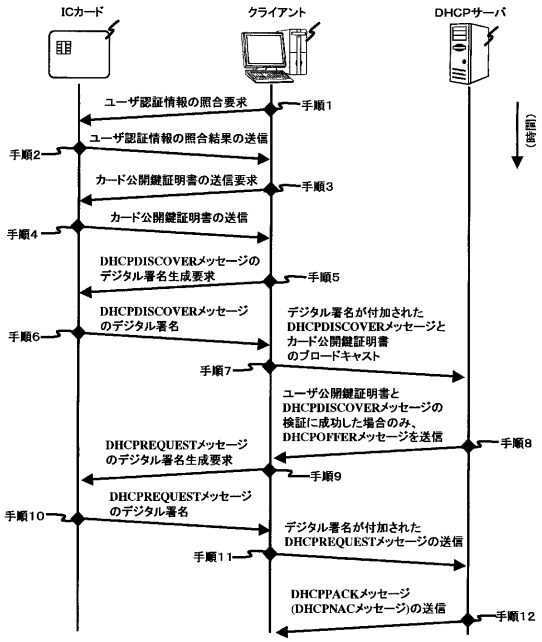
【図１】



【図２】



【図３】


ICカード
クライアント
DHCPサーバ
（時間）
ユーザ認証情報の照合要求
手順1
ユーザ認証情報の照合結果の送信
手順2
カード公開鍵証明書の送信要求
手順3
カード公開鍵証明書の送信
手順4
DHCPDISCOVERメッセージの
デジタル署名生成要求
手順5
DHCPDISCOVERメッセージ
のデジタル署名
手順6
デジタル署名が付加された
DHCPDISCOVERメッセージと
カード公開鍵証明書
のブロードキャスト
手順7
ユーザ公開鍵証明書と
DHCPDISCOVERメッセージの
検証に成功した場合のみ、
DHCPOFFERメッセージを送信
手順8
DHCPREQUESTメッセージ
のデジタル署名生成要求
手順9
DHCPREQUESTメッセージ
のデジタル署名
手順10
デジタル署名が付加された
DHCPREQUESTメッセージの送信
手順11
DHCPPACKメッセージ
(DHCPNACメッセージ)の送信
手順12