(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2009-200980
(P2009-200980A)
(43)公開日　平成21年9月3日(2009.9.3)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/46	(2006.01)	H04L	12/46	A	5J104
H04L 9/32	(2006.01)	H04L	9/00	675D	5K033

審査請求 未請求　請求項の数 10　ＯＬ　（全 11 頁）

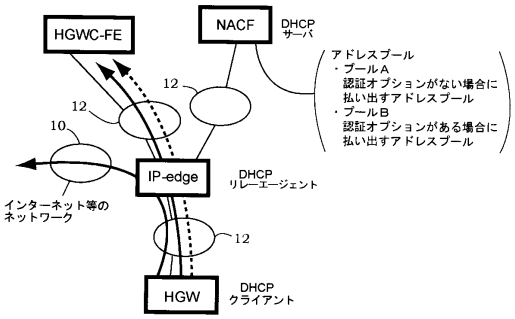
(21)出願番号　特願2008-42280(P2008-42280)
(22)出願日　平成20年2月23日(2008.2.23)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100082197
弁理士　森崎　俊明
(72)発明者　林　孝起
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5J104 AA07 AA16 BA01 EA04 EA16 KA02 MA01 MA05 NA02 NA06 NA37 NA38 PA07
5K033 AA08 CB08 CB11 CC01 DA05 DB13 DB18 EC03

(54)【発明の名称】ＤＨＣＰクライアントへ最新認証キーを配布するネットワークシステム及び方法

(57)【要約】
【課題】ＤＨＣＰサーバとＤＨＣＰクライアントの両方に同一の認証キーを予め設定し、ＤＨＣＰクライアントが正しい認証キーを持っていない場合にはインターネット等への接続サービスを阻止する手法において、ＤＨＣＰサーバにおいて認証キーが更新された場合にはＤＨＣＰクライアントに最新の認証キーを簡便に配布できるようにする。
【解決手段】ＴＣＰ／ＩＰプロトコルを使用するネットワークシステムにおいて、ＤＨＣＰサーバは、ＤＨＣＰ信号の認証をする際に、ＤＨＣＰクライアントから送出されるＤＨＣＰ信号の内容に応じてＤＨＣＰクライアントに払い出すアドレスを払い出し分けすることにより、ＤＨＣＰクライアントに認証キーを更新させる。
【選択図】図１



【特許請求の範囲】
【請求項１】
ＴＣＰ／ＩＰプロトコルを使用するネットワークシステムにおいて、ＤＨＣＰサーバは、ＤＨＣＰ信号の認証をする際に、ＤＨＣＰクライアントから送出されるＤＨＣＰ信号の内容に応じてＤＨＣＰクライアントに払い出すアドレスを払い出し分けすることにより、ＤＨＣＰクライアントに認証キーを更新させることを特徴とするネットワークシステム。
【請求項２】
ＤＨＣＰサーバは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を要求してこない場合、或いは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を要求してきたが正しい認証キーを持っていない場合には、認証キーを配布するサーバのみに接続できるアドレスを前記ＤＨＣＰクライアントに払い出すことを特徴とする請求項１記載のネットワークシステム。
【請求項３】
ＤＨＣＰサーバは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を正しいと判断した場合には、インターネットなどのネットワークに接続できるアドレスを前記ＤＨＣＰクライアントに払い出すことを特徴とする請求項１記載のネットワークシステム。
【請求項４】
ＤＨＣＰ信号の認証は、認証オプションを用いることを特徴とする請求項１から３の何れかに記載のネットワークシステム。
【請求項５】
ＤＨＣＰ信号の認証は、ベンダ拡張可能なオプションを用いたベンダ独自のものであることを特徴とする請求項１から３の何れかに記載のネットワークシステム。
【請求項６】
ＴＣＰ／ＩＰプロトコルを使用するネットワークシステムにおいて、ＤＨＣＰサーバは、ＤＨＣＰ信号の認証をする際に、ＤＨＣＰクライアントから送出されるＤＨＣＰ信号の内容を検討し、該検討の結果に応じてＤＨＣＰクライアントに払い出すアドレスを払い出し分けすることにより、ＤＨＣＰクライアントに認証キーを更新させることを特徴とする認証キー更新方法。
【請求項７】
ＤＨＣＰサーバは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を要求してこない場合、或いは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を要求してきたが正しい認証キーを持っていない場合には、認証キーを配布するサーバのみに接続できるアドレスを前記ＤＨＣＰクライアントに払い出すことを特徴とする請求項６記載の認証キー更新方法。
【請求項８】
ＤＨＣＰサーバは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を正しいと判断した場合には、インターネットなどのネットワークに接続できるアドレスを前記ＤＨＣＰクライアントに払い出すことを特徴とする請求項６記載の認証キー更新方法。
【請求項９】
ＤＨＣＰ信号の認証は、認証オプションを用いることを特徴とする請求項６から８の何れかに記載の認証キー更新方法。
【請求項１０】
ＤＨＣＰ信号の認証は、ベンダ拡張可能なオプションを用いたベンダ独自のものであることを特徴とする請求項６から８の何れかに記載の認証キー更新方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＴＣＰ／ＩＰプロトコルを用いるネットワークシステムにおいて、ＤＨＣＰ(Dynamic Host Configuration Protocol)信号の認証を行う際に、ＤＨＣＰサーバは、ＤＨＣＰクライアントから受けるＤＨＣＰ信号の内容により、ＤＨＣＰクライアントに払い出すアドレスを払い出し分けることにより、ＤＨＣＰクライアントに最新の認証キーを配布するシステム及び方法に関する。なお、ＤＨＣＰ信号の認証とは、ＤＨＣＰ信号を受信

する装置（システム構成要素）が、受信したＤＨＣＰ信号を検証し、その信号が正当な送信相手から送信されたことを確認することである。

【背景技術】

【０００２】

ＤＨＣＰは、クライアントがサーバにアクセスしてＩＰアドレスの取得を要求する際、サーバがクライアントにＩＰアドレスを動的に割り当て、クライアントのＩＰ接続終了時に「割り当てたＩＰアドレス」を回収するプロトコルである。ＩＰアドレスを配布する手続過程でのセキュリティを確保するため、ＲＦＣ(Request for comments)はＤＨＣＰサーバとＤＨＣＰクライアンとの間でやり取りされるＤＨＣＰ信号の認証について規定している。ＲＦＣは、サーバとクライアントとの間の認証について、ＤＨＣＰ認証オプション(Authentication Option)を利用する方法、ベンダ拡張可能なオプションを用いたベンダ独自の方法などを規定している。

【０００３】

ＤＨＣＰ認証オプションは、ＤＨＣＰｖ４ではOption 90, RFC3118で規定され、ＤＨＣＰｖ６ではOption 11, RFC3315で規定されている。一方、ベンダ拡張可能なオプションについてもＲＦＣに規定されている。

【０００４】

図９を参照してＤＨＣＰ認証オプションを使用した従来方式（方法）を簡単に説明する。

【０００５】

ＤＨＣＰ認証オプションを利用するためには、先ず、ＤＨＣＰクライアントであるＨＧＷ(Home Gate Way)と、ＤＨＣＰサーバであるＮＡＣＦ(Network Attachment Control Functions)の両方に、認証オプションに使用するキーのセット（複数のキーとキーを特定するキーＩＤ）を予め設定しておく。なお、ＨＧＷ及びＮＡＣＦはITU-TY.2012に規定されている。

【０００６】

ＤＨＣＰクライアントは、起動時に、ＤＨＣＰサーバに対してＩＰアドレスの要求を開始する(DHCPDISCOVER/Solicit)。なお、DHCPDISCOVER（スラッシュの前）はＤＨＣＰｖ４での表示であり、Solicit（スラッシュの後）はＤＨＣＰｖ６での表示である（以下同様）。

【０００７】

ＤＨＣＰサーバ（ＮＡＣＦ）は、ＤＨＣＰクライアント（ＨＧＷ）からＩＰアドレス要求開始信号(DHCPDISCOVER/Solicit)を受けると、予め設定してある複数のキーの中から或るキー（例えばキーＩＤ＝１で特定されるキー）を選択し、ＤＨＣＰクライアントに「選択したキーＩＤ＝１」と「認証情報」を返信する(DHCPOFFER/Advertise)。認証情報とは、ＤＨＣＰメッセージと選択されたキーとから計算するハッシュ値である。

【０００８】

ＤＨＣＰクライアントは、受け取ったキーＩＤ＝１で特定されるキーを使用して認証情報が正しいかどうかを判断し、チェックが正しければキーＩＤ＝１と認証情報とをＤＨＣＰサーバに送ってＩＰアドレス配布の要求を行う(DHCPREQUEST/Request)。

【０００９】

ＤＨＣＰサーバは、ＤＨＣＰクライアントから送られてきた認証情報をチェックして正しいと判断すれば、プールしておいた複数のＩＰアドレスの中から１つを選んでＤＨＣＰクライアントに送信する(DHCPACK/Reply)。このようにして、ＤＨＣＰサーバは認証オプションの使用によりセキュリティを確保しつつＤＨＣＰクライアントにＩＰアドレスを与える。ＲＦＣではキーの配布方法については定められてなく、高いセキュリティを確保するためには定期的にキーを変更する必要がある。

【００１０】

図１０を参照して他の従来技術を説明する。この従来技術は、図９で説明したように認証オプションを利用するのではなく、ベンダ拡張を利用した認証に係わるものである。な

お、ベンダ拡張とは、Vendor classオプション、Vendor-Specific InformationオプションなどのＤＨＣＰのベンダ拡張用オプションを使用した場合が該当する。

【００１１】

図１０に示した従来技術は、ベンダ拡張用オプションを使用した点で図９の場合と異なるだけであり、動作シーケンス自体は略同じである。

【００１２】

図１０において、ＤＨＣＰベンダ拡張用オプションを使用した認証を行うためには、先ず、ＤＨＣＰクライアント（ＨＧＷ）とＤＨＣＰサーバ（ＮＡＣＦ）の両方に、認証に使用するための複数のキーを予め設定しておく。ＤＨＣＰクライアントは、起動時に、ＤＨＣＰサーバに対して認証要求開始を示す信号を送出する(DHCPDISCOVER/Solicit)。ＤＨＣＰサーバは、ＤＨＣＰクライアントからこの認証要求開始信号を受けると、予め設定してある複数のキーの中から或るキーを選択し（選択したキーを○○○と仮定する）、選択したキーの情報を含む認証情報である認証適用信号をＤＨＣＰクライアントに送る(DHCPOFFER/Advertise)。認証情報とは、図９の場合と同様に、ＤＨＣＰメッセージと選択されたキーとから計算するハッシュ値である。

【００１３】

ＤＨＣＰクライアントは、受け取ったキーを使用して認証情報が正しいかどうかを判断し、正しければキー情報を含んだ認証情報である認証適用信号をＤＨＣＰサーバに送る(DHCPREQUEST/Request)。ＤＨＣＰサーバは、ＤＨＣＰクライアントから送られてきた認証適用信号を、先に選択したキー○○○を使用してチェックし、正しいと判断すれば認証適用信号にＩＰアドレスを含ませてＤＨＣＰクライアントに送る。ＤＨＣＰクライアントは、受け取った認証情報を先に選択されたキー○○○を使ってチェックし、チェックが正しければ受け取ったＩＰアドレスを正式のアドレスと認定し、ベンダ独自の認証が終了する。

【００１４】

上述の従来技術では、ＤＨＣＰサーバとＤＨＣＰクライアントの両方に同一のキーを予め設定し、ＤＨＣＰクライアントが正しい認証キーを持っていない場合にはインターネット等への接続サービスを阻止するようにしている。認証キーを用いた接続手法のセキュリティを維持するためには、ＤＨＣＰサーバで定期的或いは不定期に認証キーを更新することが必要である。ＤＨＣＰサーバで認証キーを更新した際には、ＤＨＣＰクライアントのキーも更新する必要がある。しかし、従来、ＤＨＣＰクライアントの認証キーの更新ついてはなんらの提案もない。

【００１５】

なお、ＤＨＣＰサーバを用いたＴＣＰ／ＩＰネットワークでのセキュリティ向上については、例えば、特許文献１に記載がある。

【特許文献１】特開２００１－３６５６１

【発明の開示】

【発明が解決しようとする課題】

【００１６】

ＤＨＣＰサーバとＤＨＣＰクライアントの両方に同一の認証キーを予め設定し、ＤＨＣＰクライアントが正しい認証キーを持っていない場合にはインターネット等への接続サービスを阻止する手法において、ＤＨＣＰサーバにおいて認証キーが更新された場合にはＤＨＣＰクライアントに最新の認証キーを簡便に配布できるようにすることである。

【課題を解決するための手段】

【００１７】

本発明によれば、ＴＣＰ／ＩＰプロトコルを使用するネットワークシステムにおいて、ＤＨＣＰサーバは、ＤＨＣＰ信号の認証をする際に、ＤＨＣＰクライアントから送出されるＤＨＣＰ信号の内容に応じてＤＨＣＰクライアントに払い出すアドレスを払い出し分けすることにより、ＤＨＣＰクライアントに認証キーを更新させるようにしている。

【００１８】
更に、前記のＤＨＣＰサーバは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を要求してこない場合、或いは、ＤＨＣＰクライアントがＤＨＣＰ信号の認証を要求してきたが正しい認証キーを持っていない場合には、認証キーを配布するサーバのみに接続できるアドレスを前記ＤＨＣＰクライアントに払い出すようにしている。
【発明の効果】
【００１９】
ＤＨＣＰサーバは、ＤＨＣＰクライアントからのＤＨＣＰ信号に応じてクライアントに払い出すアドレスを払い出し分けすることにより、ＤＨＣＰクライアントに最新のＤＨＣＰ認証キーを配布することができる。更に、ＤＨＣＰ認証キーを更新する場合、サーバとクライアントの双方に新たなキーを個別に設置するという煩雑な作業を避けることができる。
【発明を実施するための最良の形態】
【００２０】
以下、図１～図４を参照して第1の実施の形態について説明する。第１の実施の形態は認証オプションを使用する場合である。
【００２１】
図１は第1の実施の形態の動作の概略を説明する図である。ＤＨＣＰサーバ（ＮＡＣＦ）は２種類のアドレスプールＡ及びＢを備え、ＤＨＣＰクライアント（ＨＧＷ）が認証オプションを使用しないでアドレス要求をしてきた場合、或いは、認証オプションを使用してきたが正しいキーを用いないでアドレス要求をしてきた場合にはアドレスプールＡからアドレスをクライアントに払い出す。一方、ＤＨＣＰクライアントが正しいキーを用いて認証オプションを使用してきた場合にはアドレスをアドレスプールＢからクライアントに払い出す。
【００２２】
ＤＨＣＰクライアントは、アドレスプールＡからのアドレスでは、ＨＧＷＣ－ＦＥ(Home GateWay Configuration Functional Entity (ITU-T Y.2012))にアクセスできるがインターネット等の他のネットワーク（参照番号１０で示す）にはアクセスできない。一方、ＤＨＣＰクライアントがアドレスプールＢからのアドレスを使用する場合には、ＨＧＷＣ－ＦＥの他にインターネット等のネットワーク（参照番号１２で示す）にもアクセスできる。
【００２３】
プールＡ及びＢのアドレスは、ＤＨＣＰｖ４ではＩＰｖ４アドレスを意味し、ＤＨＣＰｖ６ではＩＰｖ６アドレスとＩＰｖ６プレフィックスを意味する。
【００２４】
ＤＨＣＰサーバとＤＨＣＰクライアントの間に設けたＩＰ-Edge（ＤＨＣＰリレーエージェント）は、クライアントからのアドレスの種類に応じてＤＨＣＰクライアントの接続先を決めるフィルタリング設定を行う。即ち、ＩＰ-Edgeは、ＤＨＣＰクライアントからのアドレスがプールＡから払い出されたものであれば、ＤＨＣＰクライアントをＨＧＷＣ－ＦＥのみへの接続を許容する設定し、ＤＨＣＰクライアントからのアドレスがプールＢから払い出されたものであれば、ＤＨＣＰクライアントをＨＧＷＣ－ＦＥへの接続或いはインターネット等のネットワークへの接続を許容する設定を行う。
【００２５】
次に、図２～図４を参照して第1の実施の形態を更に説明する。なお、図１で示したようにＤＨＣＰクライアント（ＨＧＷ）とＤＨＣＰサーバ（ＮＡＣＰ）の間にはＩＰ-Edgeが存在するが、ＩＰ-Edgeの前後で信号の内容に影響を及ぼす方式的な変更がないため、図２～図４ではＩＰ-Edgeの図示は省略している。
【００２６】
図２では、ＤＨＣＰクライアントは、認証オプションを利用する際に必要なキーを持っていない。即ち、ＤＨＣＰクライアントがインターネット等のネットワーク１２（図１）

にアクセスするには、ＤＨＣＰサーバからキーを貰わなければならない。ＤＨＣＰクライアントは、先ず、認証オプションを利用しないでＩＰアドレス割当要求を開始する(Solicit)。ＤＨＣＰサーバは、ＤＨＣＰクライアントが認証オプションを利用してこないのでプールＡからアドレスを選択してＤＨＣＰクライアントに応答する(Advertise)。なお、この応答信号(Advertise)には選択されたアドレスは含まれていない。

【００２７】

次に、ＤＨＣＰクライアントがＤＨＣＰサーバにＩＰアドレス割当要求を行うと(Request)、ＤＨＣＰサーバは、プールＡから選択したアドレスを払い出してＤＨＣＰクライアントに応答する(Reply)。即ち、ＤＨＣＰサーバはＤＨＣＰクライアントにプールＡから選択されたアドレスを渡す。このアドレスでは、ＤＨＣＰクライアントは、ＨＧＷＣ－ＦＥにアクセスできるだけであり、インターネット等のネットワークにアクセスできない。

【００２８】

このため、ＤＨＣＰクライアントは、ＨＧＷＣ－ＦＥにアクセスして認証オプションに使用するキーを獲得し、続いて、ＤＨＣＰサーバにアクセスしてプールＢから選択されたアドレスを貰う必要がある。

【００２９】

ＤＨＣＰクライアントはプールＡから選択されたアドレスを用い、ＨＴＴＰＳ(hypertext transfer protocol over transport layer security/secure sockets layer)等の暗号化された通信でＨＧＷＣ－ＦＥに接続する。ＨＧＷＣ－ＦＥは、これに応答し、ＤＨＣＰサーバにキー取得要求をする（このとき、ＨＧＷＣ－ＦＥはＤＨＣＰサーバにＤＨＣＰクライアントのＩＰアドレスを付与する）。ＤＨＣＰサーバは、ＨＧＷＣ－ＦＥからのキー取得要求に含まれているＩＰアドレスからＤＨＣＰクライアントを特定し、そのＤＨＣＰクライアント用のキーＩＤとキーのセットを選択し、ＨＧＷＣ－ＦＥに対してキー取得要求の応答を行う（ＨＧＷのキーＩＤとキーを送信する）。次に、ＨＧＷＣ－ＦＥは、この受け取ったキーＩＤとキーをＤＨＣＰクライアントに配布する。したがって、ＤＨＣＰクライアントは認証オプションに使用できるキー及びキーＩＤを有することになる。

【００３０】

図３は、図２で説明したキーＩＤとキーを用いて認証オプションを利用するシーケンスを図示したものである。ＤＨＣＰクライアントは、自分が有する複数のキーの内から１個を選択し、認証オプションを利用してＤＨＣＰサーバにアクセスする(Solicit)。ＤＨＣＰサーバは、送られてきたキーと自己所有のキーとの一致を確認したら、認証オプションありと認識してプールＢからアドレスを選択し、認証オプションを使用してＤＨＣＰクライアントに応答する(Advertise)。なお、この応答信号(Advertise)には選択されたアドレスは含まれていない。これに対し、ＤＨＣＰクライアントは認証オプションを使用してＤＨＣＰサーバに返答する(Request)と、ＤＨＣＰサーバは、プールＢから払いだしたアドレスを払い出してＤＨＣＰクライアントに与える(Reply)。従って、ＤＨＣＰクライアントはこのアドレスを使用してインターネット等の他のネットワークにアクセスすることができる。ＤＨＣＰクライアントがインターネット等にアクセスするシーケンスは従来と同じなので説明を省略する。

【００３１】

図４は、認証オプションに使用するキーの更新について説明する図である。ＤＨＣＰクライアントが図２及び図３で説明したキー(キーＩＤ１及び２)を有するときに、ＤＨＣＰサーバがキー(キーＩＤが１及び２)を新たなキー(キーＩＤが３及び４)に更新したとする。このような状態で、ＤＨＣＰクライアントは、ＤＨＣＰサーバに対して認証オプションを使用してＩＰアドレス取得動作を開始する(Solicit)。ＤＨＣＰサーバは、この場合、認証オプションが使用されているのでプールＢからアドレスを選択し、更新した認証キーＩＤの内の３或いは４をＤＨＣＰクライアントに送る。ＤＨＣＰクライアントはＤＨＣＰサーバから送られてきた更新されたキーＩＤ（及びキー）を持っていないので、所持しているキーＩＤとキーとを削除する。この結果、ＤＨＣＰクライアントはキーなしとなる。

したがって、ＤＨＣＰクライアントは、図２で説明した新規キー配布シーケンスにより更新されたキーをＨＧＷＣ－ＦＥから配布してもらう。

【００３２】

以上説明したように、ＤＨＣＰサーバは、ＤＨＣＰクライアントからのＤＨＣＰ信号に応じてクライアントに払い出すアドレスを払い出し分けすることにより、ＤＨＣＰクライアントに最新のＤＨＣＰ認証キーを配布することができる。更に、本発明によれば、ＤＨＣＰ認証キーを更新する場合、サーバとクライアントの双方に新たなキーを個別に設置するという煩雑な作業を避けることができる。

【００３３】

図５～図８は本発明の第２の実施の形態を説明する図である。この実施の形態は、上述した第１の実施の形態のように認証オプションを利用するのではなく、ベンダ拡張を利用した認証に係わるものである。ベンダ拡張とは、Vendor classオプション、Vendor-Specific
InformationオプションなどのＤＨＣＰのベンダ拡張用オプションを使用した場合が該当する。

【００３４】

図５は図１と同一であるが説明の便宜上再掲する。図５に示すＤＨＣＰサーバ（ＮＡＣＦ）は、図１で説明したように、２種類のアドレスプールＡ及びＢを備え、ＤＨＣＰクライアント（ＨＧＷ）が認証オプションを使用しないでアドレス要求をしてきた場合、或いは、認証オプションを使用してきたが正しいキーを用いないでアドレス要求をしてきた場合にはアドレスプールＡからアドレスをクライアントに払い出す。一方、ＤＨＣＰクライアントが正しいキーを用いて認証オプションを使用してきた場合にはアドレスをアドレスプールＢからクライアントに払い出す。図５についてのその他の説明は図１と同一なので明細書の説明を簡略にするため省略する。

【００３５】

図６～図８は、夫々、図２～図４に対応し、動作シーケンスもほぼ同一である。

【００３６】

図６では、図２の場合と同様に、ＤＨＣＰクライアントは、ベンダ拡張を利用した認証を利用する際に必要なキーを持っていない。即ち、ＤＨＣＰクライアントがインターネット等のネットワーク１２（図５）にアクセスするには、ＤＨＣＰサーバからキーを貰わなければならない。ＤＨＣＰクライアントは、先ず、認証要求をしないでＩＰアドレス割当要求を開始する(Solicit)。ＤＨＣＰサーバは、ＤＨＣＰクライアントが認証要求をしてこないのでプールＡからアドレスを選択してＤＨＣＰクライアントに応答する(Advertise)。なお、この応答信号(Advertise)には選択されたアドレスは含まれていない。

【００３７】

次に、ＤＨＣＰクライアントがＤＨＣＰサーバにＩＰアドレス割当要求を行うと(Request)、ＤＨＣＰサーバは、プールＡから選択したアドレスを払い出してＤＨＣＰクライアントに応答する(Reply)。即ち、ＤＨＣＰサーバはＤＨＣＰクライアントにプールＡから選択されたアドレスを渡す。このアドレスでは、ＤＨＣＰクライアントは、ＨＧＷＣ－ＦＥにアクセスできるだけであり、インターネット等のネットワークにアクセスできない。

【００３８】

このため、ＤＨＣＰクライアントは、ＨＧＷＣ－ＦＥにアクセスして認証要求に使用するキーを獲得し、続いて、ＤＨＣＰサーバにアクセスしてプールＢから選択されたアドレスを貰う必要がある。

【００３９】

ＤＨＣＰクライアントはプールＡから選択されたアドレスを用い、ＨＴＴＰＳ等の暗号化された通信でＨＧＷＣ－ＦＥに接続する。ＨＧＷＣ－ＦＥは、これに応答し、ＤＨＣＰサーバにキー取得要求をする（このとき、ＨＧＷＣ－ＦＥはＤＨＣＰサーバにＤＨＣＰクライアントのＩＰアドレスを付与する）。ＤＨＣＰサーバは、ＨＧＷＣ－ＦＥからのキー取得要求に含まれているＩＰアドレスからＤＨＣＰクライアントを特定し、そのＤＨＣＰ

クライアント用のキーＩＤとキーのセットを選択し、ＨＧＷＣ－ＦＥに対してキー取得要求の応答を行う（ＨＧＷのキーＩＤとキーを送信する）。次に、ＨＧＷＣ－ＦＥは、この受け取ったキーＩＤとキーをＤＨＣＰクライアントに配布する。したがって、ＤＨＣＰクライアントは認証オプションに使用できるキー及びキーＩＤを有することになる。

【００４０】

図７は、ＤＨＣＰサーバとＤＨＣＰクライアントが同一のキーを用いてベンダ拡張を利用した認証を行なうシーケンスを図示したものである。ＤＨＣＰクライアントは、自分が有する複数のキーの内から１個を選択し、認証要求信号をＤＨＣＰサーバに送信する(Solicit)。ＤＨＣＰサーバは、送られてきたキーと自己所有のキーとの一致を確認したら、認証要求ありと認識してプールＢからアドレスを選択し、認証適用信号をＤＨＣＰクライアントに送出する(Advertise)。なお、この認証適用信号(Advertise)には選択されたアドレスは含まれていない。これに対し、ＤＨＣＰクライアントは認証適用信号をＤＨＣＰサーバに送る(Request)と、ＤＨＣＰサーバは、プールＢから払いだしたアドレスを払い出してＤＨＣＰクライアントに与える(Reply)。従って、ＤＨＣＰクライアントはこのアドレスを使用してインターネット等の他のネットワークにアクセスすることができる。ＤＨＣＰクライアントがインターネット等にアクセスするシーケンスは従来と同じなので説明を省略する。

【００４１】

図８は、認証オプションに使用するキーの更新について説明する図である。ＤＨＣＰクライアントが図６及び図７で説明したキーを有するときに、ＤＨＣＰサーバがキーを新たなキーに更新したとする。このような状態で、ＤＨＣＰクライアントは、ＤＨＣＰサーバに対して認証要求信号を出す(Solicit)。ＤＨＣＰサーバは、この場合、認証要求ありと判断してプールＢからアドレスを選択し、更新した認証キーを付加して認証適用信号をＤＨＣＰクライアントに送る。しかし、ＤＨＣＰクライアントはＤＨＣＰサーバから送られてきた更新されたキーを持っていないので、所持しているキーを削除する。この結果、ＤＨＣＰクライアントはキーなしとなる。したがって、ＤＨＣＰクライアントは、図６で説明した新規キー配布シーケンスにより更新されたキーをＨＧＷＣ－ＦＥから配布してもらう。

【００４２】

以上説明したように、ＤＨＣＰサーバは、ＤＨＣＰクライアントからのＤＨＣＰ信号に応じてクライアントに払い出すアドレスを払い出し分けすることにより、ＤＨＣＰクライアントに最新のＤＨＣＰ認証キーを配布することができる。更に、ＤＨＣＰ認証キーを更新する場合、サーバとクライアントの双方に新たなキーを個別に設置するという煩雑な作業を避けることができる。

【図面の簡単な説明】

【００４３】

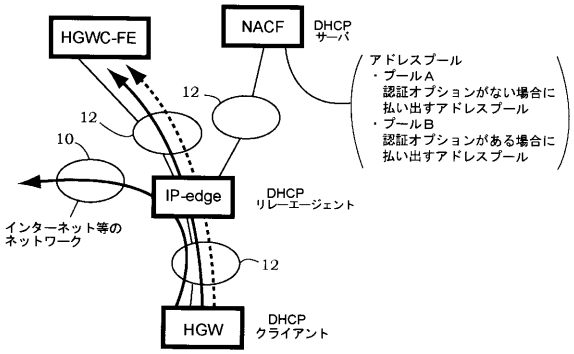
【図１】第１の実施の形態を説明する図
【図２】第１の実施の形態を説明する図
【図３】第１の実施の形態を説明する図
【図４】第１の実施の形態を説明する図
【図５】第２の実施の形態を説明する図
【図６】第２の実施の形態を説明する図
【図７】第２の実施の形態を説明する図
【図８】第２の実施の形態を説明する図
【図９】第１の従来の技術を説明する図
【図１０】第２の従来の技術を説明する図

【符号の説明】

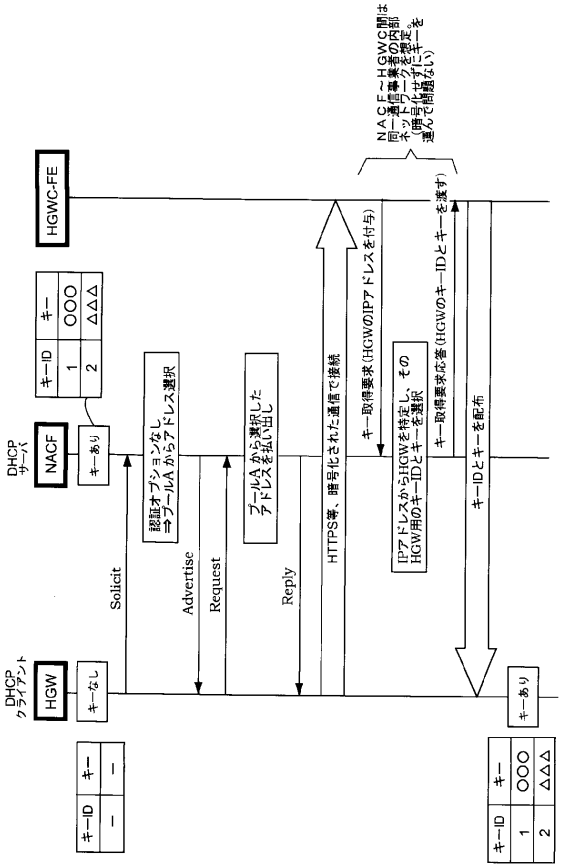
【００４４】

１０　インターネット等のネットワーク
１２　ネットワーク

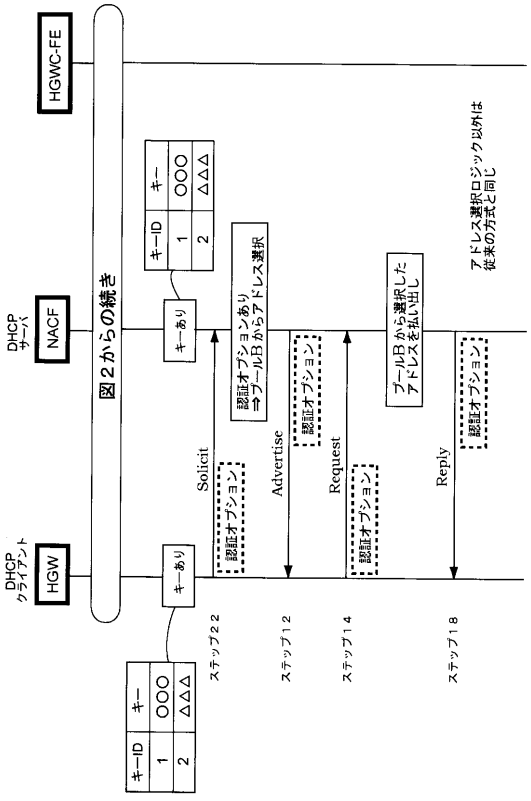
【図１】


HGWC-FE
NACF
DHCP
サーバ
アドレスプール
・プールA
認証オプションがない場合に
払い出すアドレスプール
・プールB
認証オプションがある場合に
払い出すアドレスプール
12
12
10
IP-edge
DHCP
リレーエージェント
インターネット等の
ネットワーク
12
HGW
DHCP
クライアント

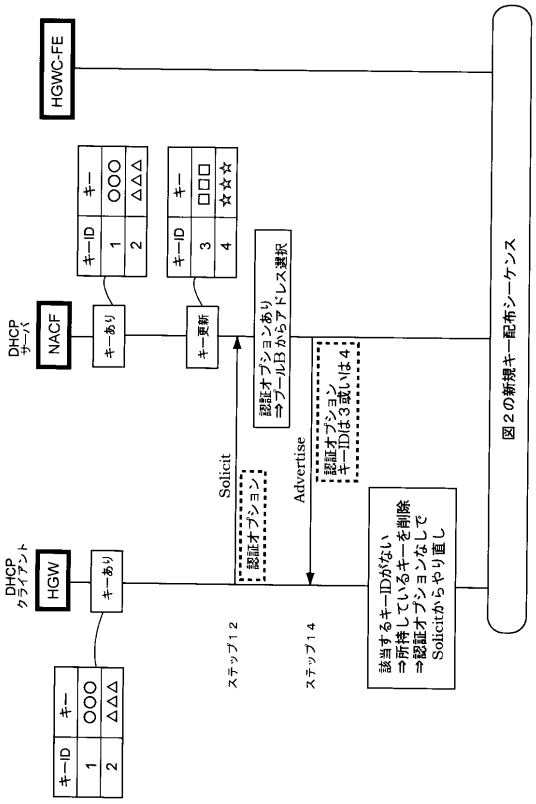
【図２】


NACF～HGWC間は
同一通信内部
(暗号化せずに平文
通信で問題ない)
HGWC-FE
DHCP
サーバ
NACF
DHCP
クライアント
HGW
キーID
キー
1
OOO
2
△△△
キーあり
キーなし
Solicit
Advertise
Request
Reply
認証オプションなし
⇒プールAからアドレス選択
プールAから選択した
アドレスを払い出し
HTTPS等、暗号化された通信で接続
キー取得要求(HGWのIPアドレスを付与)
IPアドレスからHGWを特定し、その
HGW用のキーIDとキーを選択
キー取得要求応答(HGWのキーIDとキーを渡す)
キーIDとキーを配布

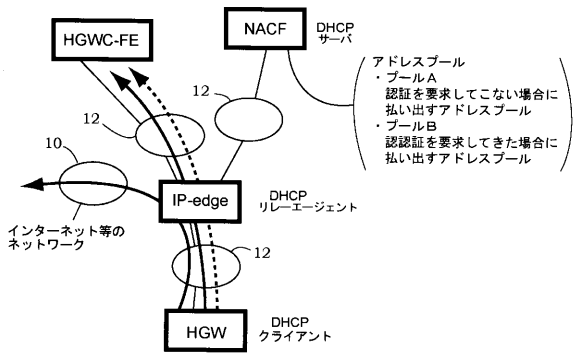
【図３】


HGWC-FE
DHCP
サーバ
NACF
DHCP
クライアント
HGW
図２からの続き
キーID
キー
1
OOO
2
△△△
キーあり
Solicit
Advertise
Request
Reply
認証オプション
認証オプションあり
⇒プールBからアドレス選択
プールBから選択した
アドレスを払い出し
アドレス選択ロジック以外は
従来の方式と同じ
ステップ22
ステップ12
ステップ14
ステップ18

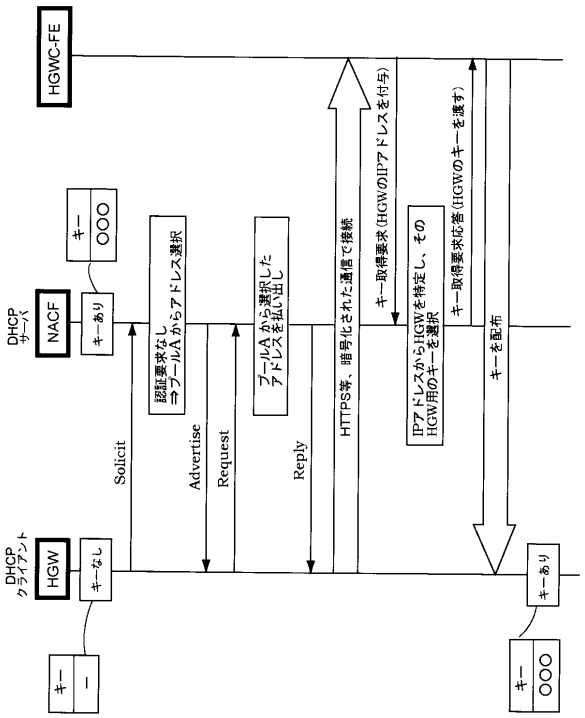
【図４】


HGWC-FE
DHCP
サーバ
NACF
DHCP
クライアント
HGW
キーID
キー
1
OOO
2
△△△
3
□□□
4
☆☆☆
キーあり
キー更新
Solicit
Advertise
認証オプション
認証オプションあり
⇒プールBからアドレス選択
認証オプション
キーIDは3或いは4
該当するキーIDがない
⇒所持しているキーを削除
⇒認証オプションなしで
Solicitからやり直し
図２の新規キー配布シーケンス
ステップ12
ステップ14

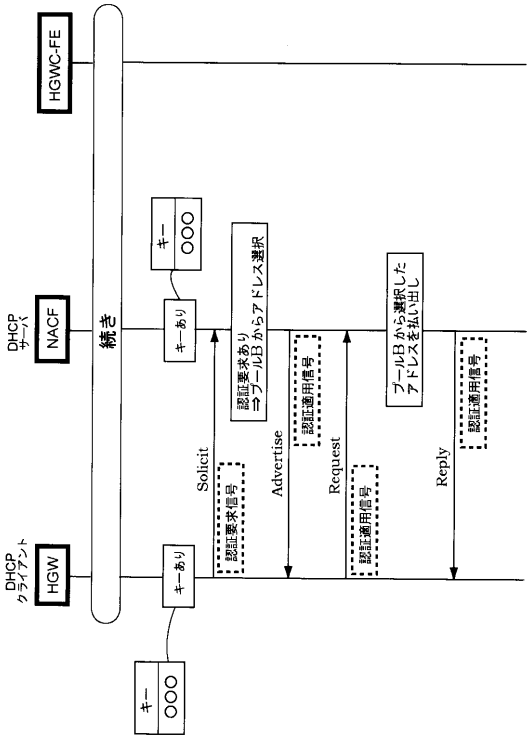
【図５】


HGWC-FE
NACF
DHCP
サーバ
アドレスプール
・プールA
認証を要求してこない場合に
払い出すアドレスプール
・プールB
認認証を要求してきた場合に
払い出すアドレスプール
12
12
10
IP-edge
DHCP
リレーエージェント
インターネット等の
ネットワーク
12
HGW
DHCP
クライアント

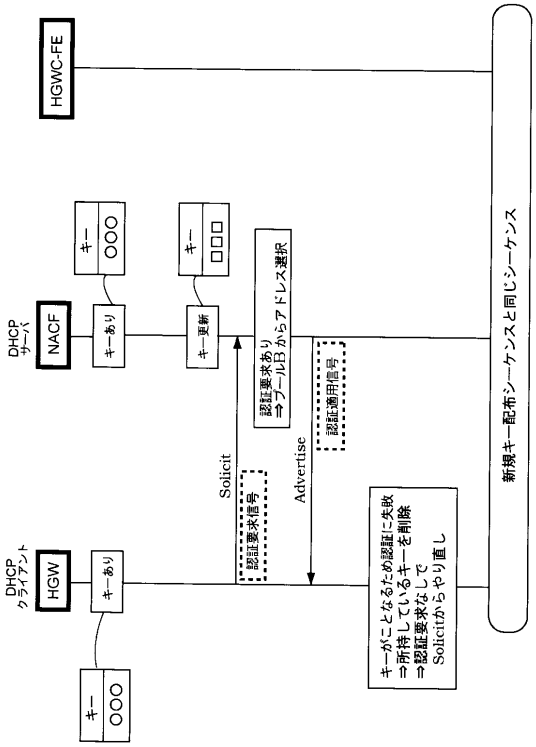
【図６】


HGWC-FE
DHCP
サーバ
NACF
キー
OOO
キーあり
認証要求なし
⇒プールAからアドレス選択
プールAから選択した
アドレスを払い出し
キー取得要求(HGWのIPアドレスを付与)
HTTPS等、暗号化された通信で接続
IPアドレスからHGWを特定し、その
HGW用のキーを選択
キー取得要求応答(HGWのキーを渡す)
キーを配布
Solicit
Advertise
Request
Reply
DHCP
クライアント
HGW
キーなし
キー
－
キーあり
キー
OOO

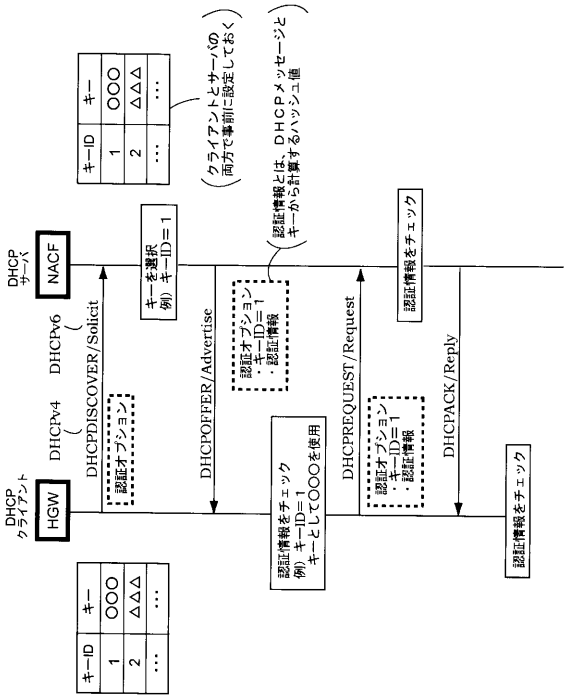
【図７】


HGWC-FE
続き
DHCP
サーバ
NACF
キー
OOO
キーあり
認証要求あり
⇒プールBからアドレス選択
プールBから選択した
アドレスを払い出し
認証適用信号
認証適用信号
認証適用信号
Solicit
Advertise
Request
Reply
DHCP
クライアント
HGW
キーあり
認証要求信号
キー
OOO

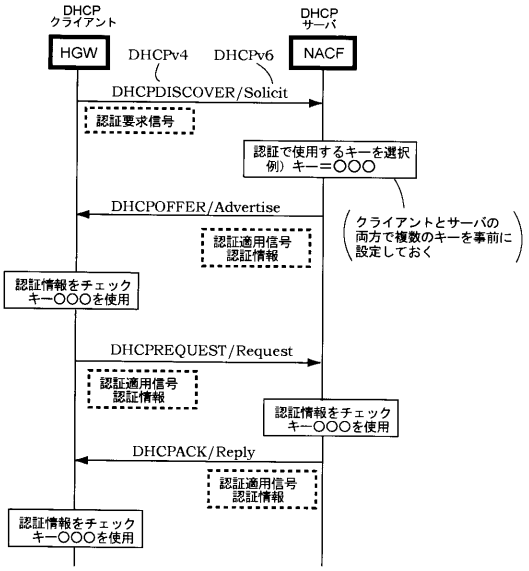
【図８】


HGWC-FE
DHCP
サーバ
NACF
キー
OOO
キーあり
キー
□□□
キー更新
認証要求あり
⇒プールBからアドレス選択
認証適用信号
新規キー配布シーケンスと同じシーケンス
Solicit
Advertise
DHCP
クライアント
HGW
キーあり
認証要求信号
キー
OOO
キーがことなるため認証に失敗
⇒所持しているキーを削除
⇒認証要求なしで
Solicitからやり直し

【図９】


DHCP サーバ
NACF
DHCP クライアント
HGW
DHCPv4 (DHCPDISCOVER/Solicit
DHCPv6 (DHCPDISCOVER/Solicit
認証オプション
キーを選択 例）キーID＝1
DHCPOFFER/Advertise
認証オプション ・キーID＝1 ・認証情報
認証情報とは、DHCPメッセージとキーから計算するハッシュ値
クライアントとサーバの両方で事前に設定しておく
キーID | キー
1 | ○○○
2 | △△△
DHCPREQUEST/Request
認証オプション ・キーID＝1 ・認証情報
認証情報をチェック 例）キーID＝1 キーとして○○○を使用
認証情報をチェック
DHCPACK/Reply
認証情報をチェック

【図１０】


DHCP クライアント
HGW
DHCPv4 (DHCPv6 (
DHCP サーバ
NACF
DHCPDISCOVER/Solicit
認証要求信号
認証で使用するキーを選択 例）キー＝○○○
DHCPOFFER/Advertise
認証適用信号 認証情報
クライアントとサーバの両方で複数のキーを事前に設定しておく
認証情報をチェック キー○○○を使用
DHCPREQUEST/Request
認証適用信号 認証情報
認証情報をチェック キー○○○を使用
DHCPACK/Reply
認証適用信号 認証情報
認証情報をチェック キー○○○を使用