(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-539643
(P2008-539643A)
(43)公表日　平成20年11月13日(2008.11.13)

(51)Int.Cl.			F I			テーマコード（参考）
H04Q	7/38	(2006.01)	H04Q	7/00	184	5J104
H04L	9/08	(2006.01)	H04L	9/00	601B	5K067
H04L	9/14	(2006.01)	H04L	9/00	641	
H04Q	7/20	(2006.01)	H04Q	7/00	629	
			H04Q	7/00	636	

審査請求 有　予備審査請求 未請求　（全 32 頁）　最終頁に続く

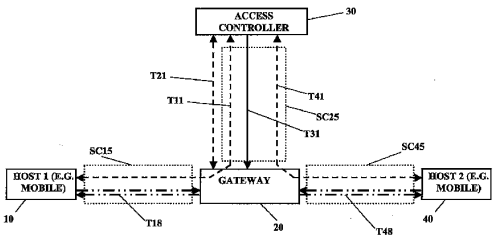
(21)出願番号　特願2008-508402 (P2008-508402)
(86)(22)出願日　平成18年4月28日 (2006.4.28)
(85)翻訳文提出日　平成19年11月21日 (2007.11.21)
(86)国際出願番号　PCT/IB2006/051336
(87)国際公開番号　WO2006/117738
(87)国際公開日　平成18年11月9日 (2006.11.9)
(31)優先権主張番号　60/675,858
(32)優先日　平成17年4月29日 (2005.4.29)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/159,146
(32)優先日　平成17年6月23日 (2005.6.23)
(33)優先権主張国　米国 (US)

(71)出願人　398012616
ノキア　コーポレイション
フィンランド　エフイーエンー０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100127188
弁理士　川守田　光紀
(72)発明者　コードリ　ライーヴ
アメリカ合衆国　９４０８６　カリフォルニア州，サニーベール，Ｗ．マッキンリー　アヴェニュー　８７０
(72)発明者　フォルスバーグ　ダン
フィンランド共和国　Ｆ１－００２１０
ヘルシンキ，メルコカツ　７　Ａ　３３

最終頁に続く

(54)【発明の名称】セキュアな通信の確立

(57)【要約】
【課題】通信ネットワーク内のネットワーク要素間のセキュアな通信を確立するための機構を提案する。
【解決手段】ネットワークノードは、認証ネットワーク要素と共に認証プロシージャを実行する。認証ネットワークは、ネットワーク要素のうちの１つをゲートウェイ要素とすることも可能である。次いで、認証されたネットワーク要素に対するそれぞれのデータキーが生成され、認証ネットワーク要素とゲートウェイ要素との間のセキュアチャネルを使用することによって、ゲートウェイ要素に配布される。データキーは、ゲートウェイ要素に格納される。セキュアな通信を設定するときには、セキュアな通信に参加しようとしているネットワーク要素にそれぞれのセッションキーが生成される。セッションキーは、ゲートウェイ要素とネットワーク要素との間のセキュアチャネルを介して、セキュアな通信に参加しようとしているネットワーク要素間で交換される。
【選択図】図１



【特許請求の範囲】
【請求項１】
通信ネットワーク内の複数のネットワーク要素間のセキュアな通信を確立するための方法であって、
・　認証ネットワーク要素と共に前記複数のネットワーク要素のための認証プロシージャを実行するステップと、
・　前記複数のネットワーク要素のうちの１つをゲートウェイ要素として設定するステップと、
・　前記認証ネットワーク要素において、認証された前記複数のネットワーク要素に対するそれぞれのデータキーを生成するステップと、
・　前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用して、前記複数のネットワーク要素のための前記それぞれのデータキーを前記ゲートウェイ要素に配布し、前記それぞれのデータキーを前記ゲートウェイ要素に格納するステップと、
・　前記セキュアな通信に参加しようとしている前記複数のネットワーク要素に対するそれぞれのセッションキーを生成するステップと、
・　前記ゲートウェイ要素と前記複数のネットワーク要素との間のセキュアチャネルを介して、前記セキュアな通信に参加しようとしている前記ネットワーク要素間で前記それぞれのセッションキーを交換するステップと、を含む方法。
【請求項２】
前記複数のネットワーク要素のための認証プロシージャを実行するステップは、前記複数のネットワーク要素うちのそれぞれ１つと前記認証ネットワーク要素との間の認証およびキー同意プロシージャを実行するステップを含む、請求項１に記載の方法。
【請求項３】
前記複数のネットワーク要素のための認証プロシージャを実行するステップは、前記複数のネットワーク要素のうちの１つによって、前記ゲートウェイ要素となる意思表示を伝送するステップを含み、前記複数のネットワーク要素のうちの１つを前記ゲートウェイ要素として設定するステップは、前記意思表示を処理することによって実行される、請求項１に記載の方法。
【請求項４】
前記認証ネットワーク要素において、少なくとも１つのそれぞれのデータキーを生成するステップは、ネットワークデバイスの前記少なくとも１つのそれぞれのデータキーを計算するために、前記それぞれのネットワーク要素の前記認証プロシージャにおいて生成した前記それぞれのセッションキーのうちの少なくとも１つと、前記ネットワーク要素の識別データと、前記ゲートウェイ要素に関連付けられた識別要素とを使用するステップを含む、請求項１に記載の方法。
【請求項５】
前記セキュアな通信に参加しようとしている前記複数のネットワーク要素間でそれぞれのセッションキーを交換するステップは、
・　或るネットワーク要素によって生成されたセッションキー及び宛先ネットワーク要素を識別するデータを含む第一のパケットを、前記パケットを暗号化すべく前記或るネットワーク要素のデータキーを使用して、ゲートウェイノードへ伝送するステップと、
・　前記ゲートウェイ要素に格納された前記或るネットワーク要素の前記データキーを使用して前記第一のパケットを解読するステップと、
・　宛先ネットワーク要素を決定するために前記第一のパケットのコンテンツを処理するステップと、
・　前記宛先ネットワーク要素のために格納した前記データキーを用いて前記ゲートウェイ要素によって暗号化された第二のパケットを使用して、前記第一のパケットに含まれる情報を前記宛先ネットワーク要素に転送するステップと、を含む、請求項１に記載の方法。

【請求項６】
前記複数のネットワーク要素のための前記それぞれのデータキーを前記ゲートウェイ要素に配布するステップは、前記それぞれのデータキーに関連する情報を暗号化および解読するために、前記認証ネットワーク要素での前記ゲートウェイ要素の前記認証プロシージャにおいて生成された前記それぞれのセッションキーを使用するステップを含む、請求項１に記載の方法。
【請求項７】
前記複数のネットワーク要素は、前記通信ネットワークのモバイルホストを備えるホストである、請求項１に記載の方法。
【請求項８】
前記ゲートウェイ要素は、インターネットを構成する外部ネットワーク、およびイントラネットを構成する内部ネットワークへのアクセスを提供するように構成される前記ネットワーク要素のためのルーターである、請求項１に記載の方法。
【請求項９】
前記認証ネットワーク要素は、プロバイダーネットワークのアクセスネットワークコントローラである、請求項１に記載の方法。
【請求項１０】
前記セキュアな通信は、ピアツーピア仮想プライベートネットワーク環境を備える近接ネットワーク環境内に確立される、請求項１に記載の方法。
【請求項１１】
前記セキュアな通信に参加しようとしている前記複数のネットワーク要素間でそれぞれのセッションキーを交換するステップの後に、双方向性のセキュアな通信セッションが確立され、前記ゲートウェイ要素が通信経路の一部ではない、請求項１に記載の方法。
【請求項１２】
通信ネットワーク内の複数のネットワーク要素間のセキュアな通信を確立するためのシステムであって、ゲートウェイ要素と、前記ゲートウェイ要素に接続可能な認証ネットワーク要素と、を備え、
前記複数のネットワーク要素は、前記認証ネットワーク要素に接続されて、該認証ネットワーク要素と共に認証プロシージャを実行しうるように構成され、
前記認証ネットワーク要素は、前記複数のネットワーク要素のうちの１つを前記ゲートウェイ要素として設定し； 認証された前記複数のネットワーク要素に対するそれぞれのデータキーを生成し； 前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用することによって、前記複数のネットワーク要素のための前記それぞれのデータキーを前記ゲートウェイ要素に配布する；ように構成され、
前記ゲートウェイ要素は、前記それぞれのデータキーを格納するように構成され、
前記複数のネットワーク要素は、セキュアな通信に参加しようとするときに、それぞれセッションキーを生成するようにさらに構成され、
前記ゲートウェイ要素は、前記ゲートウェイ要素と前記複数のネットワーク要素との間のセキュアチャネルを使用して、前記セキュアな通信に参加しようとしている前記複数のネットワーク要素間での前記それぞれのセッションキーの交換をサポートするようにさらに構成される、システム。
【請求項１３】
前記複数のネットワーク要素は、前記複数のネットワーク要素のうちのそれぞれの１つと前記認証ネットワーク要素との間の認証およびキー同意プロシージャを使用して、前記認証プロシージャを実行しうるように接続・構成される、請求項１２に記載のシステム。
【請求項１４】
前記複数のネットワーク要素のうちの少なくとも１つは、前記認証プロシージャの実行中に、前記ゲートウェイ要素となる意思表示を伝送しうるように接続・構成され、前記認証ネットワーク要素は、前記意思表示を処理することによって、前記複数のネットワーク要素のうちの１つを前記ゲートウェイ要素として設定するように構成される、請求項１２

に記載のシステム。
【請求項１５】
前記少なくとも１つのそれぞれのデータキーの生成において、前記認証ネットワーク要素は、ネットワークデバイスの前記少なくとも１つのそれぞれのデータキーを計算するために、前記それぞれのネットワーク要素の前記認証プロシージャにおいて生成した前記それぞれのセッションキーの少なくとも１つと、前記ネットワーク要素の識別データと、前記ゲートウェイ要素に関連付けられた識別要素とを使用するように構成される、請求項１２に記載のシステム。
【請求項１６】
前記セキュアな通信に参加しようとしている前記複数のネットワーク要素間の前記それぞれのセッションキーの交換のために、
前記複数のネットワーク要素は、或るネットワーク要素によって生成されたセッションキーおよび宛先ネットワーク要素を識別するデータを含む第一のパケットを、前記パケットを暗号化するためにネットワーク要素のデータキーを使用して前記ゲートウェイノードに伝送するように構成され、
前記ゲートウェイ要素は、該ゲートウェイ要素に格納された前記或るネットワーク要素の前記データキーを使用することによって、前記第一のパケットを解読し；前記宛先ネットワーク要素を決定するために前記第一のパケットのコンテンツを処理し；前記宛先ネットワーク要素のために格納した前記データキーを用いて前記ゲートウェイ要素によって暗号化された第二のパケットを使用して、前記第一のパケットに含まれる情報を前記宛先ネットワーク要素に転送するように構成される、
請求項１２に記載のシステム。
【請求項１７】
前記認証ネットワーク要素は、前記それぞれのデータキーに関連する情報を暗号化および解読するために、前記ゲートウェイ要素の前記認証プロシージャにおいて生成された前記それぞれのセッションキーを使用することによって、前記複数のネットワーク要素のための前記それぞれのデータキーを前記ゲートウェイ要素に配布するように構成される、請求項１２に記載のシステム。
【請求項１８】
前記複数のネットワーク要素は、前記通信ネットワークのモバイルホストを備えるホストである、請求項１２に記載のシステム。
【請求項１９】
前記ゲートウェイ要素は、インターネットを構成する外部ネットワーク、およびイントラネットを構成する内部ネットワークへのアクセスを提供するように構成される前記ネットワーク要素のためのルーターである、請求項１２に記載のシステム。
【請求項２０】
前記認証ネットワーク要素は、プロバイダーネットワークのアクセスネットワークコントローラである、請求項１２に記載のシステム。
【請求項２１】
前記システムは、ピアツーピア仮想プライベートネットワーク環境を備える近接ネットワーク環境内に確立されたセキュアな通信に適用可能である、請求項１２に記載のシステム。
【請求項２２】
前記セキュアな通信に参加しようとしている前記ネットワーク要素間での前記それぞれのセッションキーの交換が完了した後に、前記複数のネットワーク要素は、双方向性のセキュアな通信セッションが確立されるように接続・構成され、前記ゲートウェイ要素が通信経路の一部ではない、請求項１２に記載のシステム。
【請求項２３】
通信ネットワーク内のネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素であって、

・　認証ネットワーク要素と共に認証プロシージャを実行するように構成される認証手段と、
・　前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用することによって、前記認証ネットワーク要素で認証された前記ネットワーク要素のデータキーを、前記認証ネットワーク要素から受信するための受信手段と、
・　前記ネットワーク要素の前記データキーを格納するための格納手段と、を備え、
前記ゲートウェイ要素は、前記ゲートウェイ要素と前記ネットワーク要素との間のセキュアチャネルを使用して、前記セキュアな通信に参加しようとしている前記ネットワーク要素間でのそれぞれのセッションキーの交換をサポートするようにさらに構成される、ゲートウェイ要素。

【請求項２４】
前記ゲートウェイ要素は、認証およびキー同意プロシージャを使用して、前記認証ネットワーク要素と共に前記認証プロシージャを実行する、請求項２３に記載のゲートウェイ要素。

【請求項２５】
前記ゲートウェイ要素は、
・　前記認証プロシージャの実行中に、前記ゲートウェイ要素となる意思表示を伝送し、
・　前記認証ネットワーク要素から前記ゲートウェイ要素として設定する指示を受信するように構成される、請求項２３に記載のゲートウェイ要素。

【請求項２６】
前記認証ネットワーク要素から受信して前記ゲートウェイ要素に格納された前記データキーは、ネットワーク要素の前記認証プロシージャにおいて生成された前記それぞれのセッションキーのうちの少なくとも１つと、前記ネットワーク要素の識別データと、前記ゲートウェイ要素に関連付けられた認証要素とに基づくものである、請求項２３に記載のゲートウェイ要素。

【請求項２７】
前記セキュアな通信に参加しようとしている前記ネットワーク要素間での前記それぞれのセッションキーの交換時に、前記ゲートウェイ要素は、
・　或るネットワーク要素によって生成されたセッションキー及び宛先ネットワーク要素を識別するデータを含む第一のパケットを受信し、ここで前記第一のパケットは、前記或るネットワーク要素のデータキーを使用することによって暗号化されると共に、前記ゲートウェイ要素に格納された前記データキーによって解読され、
・　前記宛先ネットワーク要素のための前記第一のパケットのコンテンツを処理し、
・　前記宛先ネットワーク要素のために格納された前記データキーによって暗号化された第二のパケットを使用して、前記第一のパケットに含まれる情報を前記宛先ネットワーク要素に転送するように構成される、請求項２３に記載のゲートウェイ要素。

【請求項２８】
前記ゲートウェイ要素は、前記それぞれのデータキーに関連する情報の暗号化および解読のために、前記ゲートウェイ要素の前記認証プロシージャに生成された前記それぞれのセッションキーを使用することによって伝送された前記ネットワーク要素の前記それぞれのデータキーを、前記認証ネットワーク要素から受信するように構成される、請求項２３に記載のゲートウェイ要素。

【請求項２９】
前記ネットワーク要素は、前記通信ネットワークのモバイルホストを備えるホストである、請求項２３に記載のゲートウェイ要素。

【請求項３０】
前記ゲートウェイ要素は、インターネットを構成する外部ネットワーク、およびイントラネットを構成する内部ネットワークへのアクセスを提供するように構成される前記ネットワーク要素のためのルーターである、請求項２３に記載のゲートウェイ要素。

【請求項３１】

前記認証ネットワーク要素は、プロバイダーネットワークのアクセスネットワークコントローラである、請求項２３に記載のゲートウェイ要素。
【請求項３２】
前記ゲートウェイ要素は、ピアツーピア仮想プライベートネットワーク環境を備える近接ネットワーク環境内に確立されたセキュアな通信に適用可能である、請求項２３に記載のゲートウェイ要素。
【請求項３３】
前記ゲートウェイ要素は、前記セキュアな通信に参加しようとしている前記ネットワーク要素間での前記それぞれのセッションキーの交換完了後に、ネットワーク要素間の双方向性のセキュアな通信セッションの一部ではない、請求項２３に記載のゲートウェイ要素。
【請求項３４】
通信ネットワーク内のネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素を備える装置であって、前記ゲートウェイ要素が、
・　認証ネットワーク要素と共に認証プロシージャを実行し、
・　前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用することによって、前記認証ネットワーク要素において認証されたネットワーク要素のデータキーを前記認証ネットワーク要素から受信し、
・　前記ネットワーク要素のデータキーを格納する、
ように構成され、さらに前記ゲートウェイ要素が、前記ゲートウェイ要素と前記ネットワーク要素との間のセキュアチャネルを使用して、前記セキュアな通信に参加しようとしている前記ネットワーク要素間での前記それぞれのセッションキーの交換をサポートするようにさらに構成される、装置。
【請求項３５】
通信ネットワーク内のネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素を備える装置であって、前記ゲートウェイ要素が、
・　セキュアな通信への参加のリクエストを示す送信ネットワーク要素から、宛先ネットワーク要素を識別するデータを含む第一のメッセージを受信し、
・　前記ゲートウェイ要素が前記宛先ネットワーク要素へのルートに対するエントリを有することを検証し、
・　ルートに対するエントリが見つからなかったときは、前記宛先ネットワーク要素を識別する前記データを対応するアドレスデータに関連付けて、前記アドレスデータを使用して前記宛先ネットワーク要素への前記ルートを確立し、
・　ルートに対するエントリが見つかったときは、第二のメッセージを前記宛先ネットワーク要素に直接ユニキャストするように構成される、
装置。
【請求項３６】
通信ネットワーク内の複数のネットワーク要素間のセキュアな通信の確立に使用可能な認証ネットワーク要素を含む装置であって、前記認証ネットワーク要素が、
・　ネットワーク要素によって認証プロシージャを実行し、
・　前記ネットワーク要素のうちの１つをゲートウェイ要素として設定し、
・　認証された前記ネットワーク要素に対する個別のデータキーを生成し、
・　前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用することによって、前記ネットワーク要素の前記個別のデータキーを前記ゲートウェイ要素に配布するように構成される、
装置。
【請求項３７】
・　通信ネットワークにセキュアな通信を確立するように構成される端末ノードを備える装置であって、前記端末ノードは、
・　認証ネットワーク要素と共に認証を実行し、

・　セキュアな通信に参加しようとするときにそれぞれのセッションキーを生成し、
・　前記個別のセッションキーをゲートウェイ要素に伝送し、
・　前記ゲートウェイ要素へのセキュアなチャネルを使用して前記セキュアな通信に参加しようとする少なくとも１つの他の端末要素とセッションキーを交換するように構成される、装置。
【請求項３８】
・　認証ネットワーク要素と共に、複数のネットワーク要素に対する認証プロシージャを実行することと、
・　前記認証ネットワーク要素において、認証された前記複数のネットワーク要素に対するそれぞれのデータキーを生成することと、
・　前記認証プロシージャの結果に基づいてセッションキーを導出することと、
・　前記セッションキーを、キーディストリビュータから、ゲートウェイ要素と前記ネットワーク要素との間のセキュアなチャネルを介して、セキュアな通信に参加しようとしている前記ネットワーク要素に配布することと、
・　前記ネットワーク要素間のセキュアな通信を確立することと、
を含む方法。
【請求項３９】
前記セッションキーは、全てのネットワーク要素に提供される共有セッションキーである、請求項３８に記載の方法。
【請求項４０】
前記ネットワーク要素のうちの１つを前記ゲートウェイ要素として設定することをさらに含む、請求項３８に記載の方法。
【請求項４１】
前記ゲートウェイのアイデンティティと、ネットワーク要素としてのホストにおける前記認証プロシージャの結果に基づいて、セッションキーを導出することをさらに含む、請求項３８に記載の方法。
【請求項４２】
前記ゲートウェイ要素の前記キーディストリビュータを提供することをさらに含む、請求項３８に記載の方法。
【請求項４３】
ネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素として機能するように構成されるネットワーク要素を備えるデバイスであって、前記ネットワーク要素が、
・　認証ネットワーク要素と共に、それ自体およびネットワーク要素に対する認証プロシージャを実行するように構成され、
・　前記認証プロシージャの結果に基づいて導出されたセッションキーを、前記ネットワーク要素間のセキュアなチャネルを介して、セキュアな通信に参加しようとしている前記ネットワーク要素に配布する、
デバイス。
【請求項４４】
前記ネットワーク要素は、キーディストリビュータ要素を備える、請求項４３に記載のデバイス。
【請求項４５】
・　認証ネットワーク要素と共に、複数のネットワーク要素に対する認証プロシージャを実行することと、
・　前記認証ネットワーク要素において、認証された前記ネットワーク要素に対するデータキーをそれぞれ生成することと、
・　前記データキーに基づいて前記ネットワーク要素のセッションキーを導出することと、
・　前記認証ネットワーク要素と前記ネットワーク要素との間のセキュアなチャネルを使

用することによって、前記それぞれのセッションキーを、前記認証ネットワーク要素を介して前記ネットワーク要素に配布することと、
・　ネットワーク要素間のセキュアな通信を確立することと、
を含む方法。
【請求項４６】
前記複数のネットワーク要素のうちの１つをゲートウェイ要素として設定することをさらに含む、請求項４５に記載の方法。
【請求項４７】
複数のネットワーク要素間のセキュアな通信の確立に使用可能な認証ネットワーク要素として機能するように構成されるネットワーク要素を備えるデバイスであって、該ネットワーク要素が、
・　認証ネットワーク要素と共に、複数のネットワーク要素に対する認証プロシージャを実行し、
・　認証された複数の前記ネットワーク要素に対するそれぞれのデータキーを生成し、
・　前記認証ネットワーク要素と前記ネットワーク要素との間のセキュアチャネルを使用して、前記データキーに基づいて前記ネットワーク要素において導出されたそれぞれのセッションキーを、前記ネットワーク要素に配布するように構成される、
デバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
〔関連出願の記載〕
本出願は、米国暫定特許出願第60/675,858号（2005年4月29日出願）、および米国特許出願第11/159146号に優先権を主張するものである。先に提出された本出願書の内容は、参照することにより組み込まれる。
【０００２】
〔技術分野〕
本発明は、通信ネットワーク内のネットワーク要素間のセキュアな通信を確立するための機構に関する。特に、本発明は、方法、システム、および信頼できるユーザーのネットワークの構築に使用可能な、ゲートウェイ要素と呼ばれるネットワーク要素、例えば、企業ネットワークなどを介した伝送を必要とせずに、動的に形成されたネットワークを使用することによって、ユーザーがセキュアに通信することができるピアツーピア仮想プライベートネットワークに関する。
【０００３】
本願明細書において本発明を説明するために、以下に留意されたい。
【０００４】
通信デバイスとして機能するネットワーク要素は、例えば、ユーザーが通信ネットワークにアクセスすることが可能なあらゆるデバイスとすることが可能である。これは、モバイルおよび非モバイルデバイスならびにネットワークを包含し、これらをベースとする技術プラットホームに依存しない。一例として、第三世代パートナーシッププロジェクト（3rd Generation Partnership Project：3GPP）および、例えば既知のUMTS（Universal Mobile Telecommunications System：汎用モバイル通信システム）要素によって標準化された原理に基づいて作動するネットワーク要素は、本発明に関連した使用に特に好適である。
【０００５】
ネットワーク要素は、本発明の観点では、クライアントエンティティとして、またはサーバーエンティティとして機能することができるか、あるいはこれら両方の機能を統合したものとすることも可能である。
【０００６】
通信のコンテンツは、オーディオデータ、ビデオデータ、画像データ、テキストデータ

、およびオーディオ、ビデオ、画像、および/またはテキストデータの属性を記述するメタデータ、これらのデータを組み合わせたもの、代替的または追加的に、更なる例として、アクセスおよびダウンロードされるアプリケーションプログラムのプログラムコードのような他のデータのうちの少なくとも１つを含むことが可能である。

【０００７】

ソフトウェアコード部分として実行される可能性があり、サーバー/クライアントのうちの１つにおいてプロセッサを使用して実行される方法ステップは、ソフトウェアコードに依存せず、あらゆる既知の、または将来開発されるプログラミング言語を使用して規定することができる。

【０００８】

サーバー/クライアントのうちの１つにおいてハードウェアコンポーネントとして実装される可能性のある方法ステップおよび/またはデバイスは、ハードウェアに依存せず、あらゆる既知の、または将来開発されるハードウェア技術、または、例えば、ASIC（Application Specific Integrated Circuit：特定用途向け集積回路）コンポーネントまたはDSP（Digital Signal Processing：デジタル信号処理）コンポーネントを使用して、MOS（Metal-Oxide Semiconductor：金属酸化膜半導体）、CMOS（Complementary Metal-Oxide Semiconductor：相補型MOS）、BiCMOS（Bipolar Complementary Metal-Oxide Semiconductor：バイポーラ相補型MOS）、ECL（Emitter Coupled Logic：エミッタ結合型論理回路）、TTL（Transistor- Transistor Logic：トランジスタ-トランジスタ論理回路）などのような、これらの技術をハイブリッド化したものを使用して実装することができる。

【０００９】

概して、あらゆる方法ステップは、本発明の概念を変更せずに、ソフトウェアとしての、またはハードウェアによる実装に好適である。

【００１０】

デバイスまたはネットワーク要素は、個々のデバイスとして実装することができるが、デバイスの機能が保持されるのであれば、それらがシステムを通じて配布される形態で実装されることを除外しない。

【背景技術】

【００１１】

近年、統合サービスディジタル通信網（Integrated Services Digital Network：ISDN）のようなワイヤーベースの通信ネットワーク、CDMA2000（Code Division Multiple Access：符号分割多重アクセス）システム、汎用モバイル通信システム（Universal Mobile Telecommunications System：UMTS）のような携帯電話の第三世代通信ネットワーク、汎用パケット無線システム（General Packet Radio System：GPRS）のような無線通信ネットワーク、または無線ローカルエリアネットワーク（Wireless Local Area Network：WLAN）のような他の無線通信システムが、世界中で急速に拡大している。第三世代パートナーシッププロジェクト（3rd Generation Partnership Project：3GPP）、国際電気通信連合（International Telecommunication Union：ITU）、第三世代パートナーシッププロジェクト2（3rd Generation Partnership Project 2：3GPP2）、インターネット技術特別調査委員会（Internet Engineering Task Force：IETF）などのような様々な組織が、通信ネットワークおよび多重アクセス環境に取り組んでいる。

【００１２】

一般的に、通信ネットワークのシステム構造は、移動局、携帯電話、固定電話、パーソナルコンピュータ（PC）、ラップトップ、携帯情報端末（Personal Digital Assistant：PDA）などのような、あるパーティ（例、加入者のユーザー機器）が、トランシーバおよびエアインターフェース、有線インターフェースなどのようなインターフェースを介して、アクセスネットワークサブシステムに接続されるといったものである。アクセスネットワークサブシステムは、ユーザー機器との通信接続を制御し、インターフェースを介して、対応するコアまたはバックボーンネットワークサブシステムに接続される。コア（またはバックボーン）ネットワークサブシステムは、伝送したデータを、別のユーザー機器、

サービスプロバイダ（サーバー/プロキシ）、または別の通信ネットワークのような宛先パーティへ通信接続を介して切り替える。なお、コアネットワークサブシステムは、複数のアクセスネットワークサブシステムに接続することが可能であることに留意されたい。当業者に既知のように、また、例えばUMTS、GSMなどのようなそれぞれの使用で定義されるように、実際のネットワーク構造は、使用される通信ネットワークによって様々である。

【００１３】

概して、ユーザー機器と別のユーザー端末、データベース、サーバーなどとの間のような、ネットワーク要素間の通信接続を適切に確立して処理するためには、制御ネットワーク要素、サポートノード、またはサービスノードのような１つ以上の中間ネットワーク要素が必要である。

【００１４】

特別なタイプの通信ネットワークには、いわゆる近接ネットワーク（Proximity Network）がある。近接ネットワークは、比較的小規模で、かなり距離の短い、しばしばアドホックであり、一般的に無線伝送に基づいたネットワークである。近接ネットワークの一例には、例えば、企業ネットワークまたは企業ソリューションがあり、文書の共有、インスタントメッセージング、カレンダリング、会議などのタスクが、一般的に近接ネットワークによって行われる。

【００１５】

通信接続における１つの重要な側面は、特に機密データが伝送されうる企業ネットワークにおける通信のセキュリティである。通信パーティだけが、通信セッションにおいて伝送された情報を取り込むことができ、他のパーティが機密データを収集しないようにすることが望ましく、場合によってはそのようにする必要がある。通信のセキュリティは、例えば、パーティ間で伝送されるデータおよびメッセージに対して、セキュアチャネルおよび、暗号化および暗号解読技術を使用することによって達成することができる。セキュアな通信の確立には、他のパーティが信頼できるユーザー/ホストであることを検証すること、すなわち、受信パーティがセキュアな通信の一部となることを許可されていることを確認することも必要である。

【００１６】

本願の出願人によって出願されたEP1458151（またはUS 2004/179502）では、モバイル"アドホック"ネットワークに対するセキュリティサービスの提供が開示されている。セキュリティサービスを提供するために、一組のユーザー識別子が、第一のアドホックノードから、アドホックネットワーク外部の第二のネットワークに伝送される。この一組のユーザー識別子は、少なくとも１つのアドホックノードに関連するユーザー識別子を含む。第一組の認証パラメータは、外部ネットワークにおいて生成される。第一組の認証パラメータは、一組のユーザー識別子に含まれる各ユーザー識別子に対する認証ベクトルを含み、各認証ベクトルは、第二組の認証パラメータを含む。第二組の認証パラメータのうちのいくつかは、第一のアドホックノードに転送され、それによって、第三組の認証パラメータを第一のアドホックノードで受信する。第三組の認証パラメータは、アドホックネットワークにおいてセキュリティサービスを提供するために、第一のアドホックのノードで使用される。

【特許文献１】EP1458151

【発明の開示】

【００１７】

本発明の目的は、例えば近接ネットワーク環境において、信頼できるユーザーのネットワークを動的に確立するための改善された機構を提供することである。

【００１８】

本発明の目的は、特に、データのセキュアな伝送が可能なピアツーピア仮想プライベートネットワークに使用可能な方法および対応するシステム、および少なくとも２つのホスト間でのセキュアな通信の確立をサポートする特定のネットワーク要素またはゲートウェ

イ要素を提供することである。

【００１９】

前記目的は、添付の請求の範囲に定義された方法によって達成される。

【００２０】

特に、解決案の一側面によれば、例えば、通信ネットワーク内のネットワーク要素間のセキュアな通信を確立するための方法であって、認証ネットワーク要素と共に複数のネットワーク要素のための認証プロシージャを実行するステップと、前記複数のネットワーク要素のうちの１つをゲートウェイ要素として設定するステップと、前記認証ネットワーク要素において、認証された前記複数のネットワーク要素に対するそれぞれのデータキーを生成するステップと、前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用して、前記複数のネットワーク要素のための前記それぞれのデータキーを前記ゲートウェイ要素に配布し、前記それぞれのデータキーを前記ゲートウェイ要素に格納するステップと、前記セキュアな通信に参加しようとしているネットワーク要素内のそれぞれのセッションキーを生成するステップと、前記ゲートウェイ要素と前記ネットワーク要素との間のセキュアチャネルを介して、前記セキュアな通信に参加しようとしている前記ネットワーク要素間で前記それぞれのセッションキーを交換するステップと、を含む方法が提供される。

【００２１】

さらに、解決案の一側面によれば、例えば、通信ネットワーク内の複数のネットワーク要素間のセキュアな通信を確立するためのシステムであって、複数のネットワーク要素と、ゲートウェイ要素と、前記ゲートウェイ要素に接続可能な認証ネットワーク要素と、を備え、前記ネットワーク要素は、されて、前記認証ネットワーク要素に接続され、該認証ネットワーク要素と共に認証プロシージャを実行しうるように構成され、前記認証ネットワーク要素は、前記複数のネットワーク要素のうちの１つを前記ゲートウェイ要素として設定し、認証された前記複数のネットワーク要素に対するそれぞれのデータキーを生成し、前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用することによって、前記複数のネットワーク要素のための前記それぞれのデータキーを前記ゲートウェイ要素に配布するように構成され、前記ゲートウェイ要素は、前記データキーを格納するようにさらに構成され、前記複数のネットワーク要素は、セキュアな通信に参加しようとするときに、それぞれセッションキーを生成するようにさらに構成され、前記ゲートウェイ要素は、前記ゲートウェイ要素と前記ネットワーク要素との間のセキュアチャネルを使用して、前記セキュアな通信に参加しようとしている前記ネットワーク要素間での前記それぞれのセッションキーの交換をサポートするようにさらに構成される、システムが提供される。

【００２２】

さらに、解決案の一側面によれば、例えば、通信ネットワーク内のネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素であって、認証ネットワーク要素と共に認証プロシージャを実行するように構成される認証手段と、前記認証ネットワークと前記ゲートウェイ要素との間のセキュアチャネルを使用することによって、前記認証ネットワーク要素で認証されたネットワーク要素のデータキーを、前記認証ネットワーク要素から受信するための受信手段と、前記ネットワーク要素の前記データキーを格納するための格納手段と、を備え、前記ゲートウェイ要素は、前記ゲートウェイ要素と前記ネットワーク要素との間のセキュアチャネルによって、前記セキュアな通信に参加しようとしているネットワーク要素間でのそれぞれのセッションキーの交換をサポートするようにさらに構成される、ゲートウェイ要素が提供される。

【００２３】

加えて、解決案の一側面によれば、例えば、通信ネットワーク内のネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素を備える装置であって、前記ゲートウェイ要素は、認証ネットワーク要素と共に認証プロシージャを実行し、前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用することによって

、前記認証ネットワーク要素において認証されたネットワーク要素のデータキーを前記認証ネットワーク要素から受信し、前記ネットワーク要素のデータキーを格納するように構成され、前記ゲートウェイ要素は、前記ゲートウェイ要素と前記ネットワーク要素との間のセキュアチャネルを使用して、前記セキュアな通信に参加しようとしているネットワーク要素間での前記それぞれのセッションキーの交換をサポートするようにさらに構成される、装置が提供される。

【００２４】

さらに、解決案の一側面によれば、例えば、通信ネットワーク内のネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素を備える装置であって、前記ゲートウェイ要素は、セキュアな通信への参加のリクエストを示す送信ネットワークから第一のメッセージを受信し、前記第一のメッセージは、宛先ネットワーク要素を識別するデータを含み、前記ゲートウェイ要素が前記宛先ネットワークへのルートに対するエントリを有することを検証し、ルートに対するエントリが見つからなかったときは、前記宛先ネットワーク要素を識別する前記データを対応するアドレスデータに関連付けて、前記アドレスデータを使用して前記宛先ネットワーク要素への前記ルートを確立し、ルートに対するエントリが見つかったときは、第二のメッセージを前記宛先ネットワーク要素に直接ユニキャストするように構成される、装置が提供される。

【００２５】

さらに、解決案の一側面によれば、例えば、通信ネットワーク内の複数のネットワーク間のセキュアな通信の確立に使用可能な認証ネットワーク要素を含む装置であって、前記認証ネットワーク要素は、ネットワーク要素によって認証プロシージャを実行し、ネットワーク要素のうちの１つをゲートウェイ要素として設定し、認証された前記ネットワーク要素に対する個別のデータキーを生成し、前記認証ネットワーク要素と前記ゲートウェイ要素との間のセキュアチャネルを使用することによって、前記ネットワーク要素の前記個別のデータキーを前記ゲートウェイ要素に配布するように構成される、装置が提供される。

【００２６】

加えて、解決案の一側面によれば、例えば、通信ネットワークにセキュアな通信を確立するように構成される端末ノードを備える装置であって、前記端末ノードは、認証ネットワーク要素と共に認証を実行し、セキュアな通信に参加しようとするときに個別のセッションキーを生成し、前記セッションキーをゲートウェイ要素に伝送し、前記ゲートウェイ要素へのセキュアなチャネルによって前記セキュアな通信に参加しようとする少なくとも１つの他の端末要素とセッションキーを交換するように構成される、装置が提供される。

【００２７】

更なる改良によれば、本解決案は、下記の機能のうちの１つ以上を備えることが可能である。

【００２８】

前記複数のネットワーク要素のための認証プロシージャを実行するステップは、前記複数のネットワーク要素うちのそれぞれ１つと前記認証ネットワーク要素との間の認証およびキー同意プロシージャを実行するステップを含むことが可能である。

【００２９】

前記複数のネットワーク要素のための認証プロシージャを実行するステップは、前記複数のネットワーク要素のうちの１つによって、前記ゲートウェイ要素となる意思表示を伝送するステップをさらに含むことが可能であり、前記認証ネットワーク要素は、前記意思表示の処理に基づいて、前記複数のネットワーク要素のうちの１つを前記ゲートウェイ要素として設定することが可能である。

【００３０】

前記認証ネットワーク要素において、少なくとも１つのそれぞれのデータキーを生成するステップは、ネットワークデバイスの前記少なくとも１つのそれぞれのデータキーを計算するために、前記それぞれのネットワーク要素の前記認証プロシージャにおいて生成し

た前記それぞれのセッションキーのうちの少なくとも１つと、前記ネットワーク要素の識別データと、前記ゲートウェイ要素に関連付けられた識別要素とを使用するステップを含むことが可能である。

【００３１】

前記セキュアな通信に参加しようとしている前記複数のネットワーク要素間でそれぞれのセッションキーを交換するステップは、或るネットワーク要素（すなわち送信ネットワーク要素）によって生成されたセッションキーおよび宛先ネットワーク要素を識別するデータを含む第一のパケットを、前記パケットを暗号化するために前記或るネットワーク要素のデータキーを使用して、前記ゲートウェイノードに伝送するステップと、前記ゲートウェイ要素に格納された前記１つのネットワーク要素の前記データキーを使用して前記第一のパケットを解読するステップと、前記宛先ネットワーク要素のために格納した前記データキーを用いて前記ゲートウェイ要素によって暗号化された第二のパケットを使用して、前記第一のパケットに含まれる情報を前記宛先ネットワーク要素に転送するステップとを含むことが可能である。

【００３２】

前記複数のネットワーク要素のための前記それぞれのデータキーを前記ゲートウェイ要素に配布するステップは、前記それぞれのデータキーに関連する情報を暗号化および解読するために、前記認証ネットワーク要素での前記ゲートウェイ要素の前記認証プロシージャにおいて生成された前記それぞれのセッションキーを使用するステップを含むことが可能である。

【００３３】

前記ネットワーク要素は、前記通信ネットワークのホスト、特にモバイルホストとすることが可能である。

【００３４】

前記ゲートウェイ要素は、インターネットのような外部ネットワーク、およびイントラネットのような内部ネットワークへのアクセスを提供するように構成される前記ネットワーク要素のためのルーターとすることが可能である。

【００３５】

前記認証ネットワーク要素は、アクセスネットワークコントローラ、特にプロバイダーネットワークのアクセスコントローラとすることが可能である。

【００３６】

前記セキュアな通信は、近接ネットワーク環境内、特にピアツーピア仮想プライベートネットワーク環境内に確立することが可能である。

【００３７】

前記セキュアな通信に参加しようとしている前記ネットワーク要素間でのそれぞれのセッションキーの交換後に、双方向性のセキュアな通信セッションを確立することが可能であり、前記ゲートウェイ要素は通信経路の一部ではない。

【００３８】

加えて、解決案の一側面によれば、例えば、認証ネットワーク要素と共に、複数のネットワーク要素に対する認証プロシージャを実行することと、前記認証ネットワーク要素において、認証された前記複数のネットワーク要素に対するそれぞれのデータキーを生成することと、前記認証プロシージャの結果に基づいてセッションキーを導出することと、前記セッションキーを、キーディストリビュータから、ゲートウェイ要素と前記ネットワーク要素との間のセキュアなチャネルを介して、セキュアな通信に参加しようとしている前記ネットワーク要素に配布することと、前記ネットワーク要素間のセキュアな通信を確立することと、を含む方法が提供される。

【００３９】

加えて、解決案の一側面によれば、例えば、ネットワーク要素間のセキュアな通信の確立に使用可能なゲートウェイ要素として機能するように構成されるネットワーク要素を備えるデバイスであって、前記ネットワーク要素は、認証ネットワーク要素と共にそれ自体

およびネットワーク要素に対する認証プロシージャを実行するように構成され、前記認証プロシージャの結果に基づいて導出されたセッションキーを、前記ネットワーク要素間のセキュアなチャネルを介してセキュアな通信に参加しようとしている前記ネットワーク要素に配布する、デバイスが提供される。

【００４０】

加えて、解決案の別の側面によれば、例えば、認証ネットワーク要素と共に、複数のネットワーク要素に対する認証プロシージャを実行することと、前記認証ネットワーク要素において、認証された前記ネットワーク要素に対するそれぞれのデータキーを生成することと、前記データキーに基づいて前記ネットワーク要素のセッションキーを導出することと、前記認証ネットワーク要素と前記ネットワーク要素との間のセキュアなチャネルを使用することによって、前記認証ネットワーク要素を介して前記それぞれのセッションキーを前記ネットワーク要素に配布することと、ネットワーク要素間のセキュアな通信を確立することと、を含む方法が提供される。

【００４１】

さらに、解決案の一側面によれば、例えば、ネットワーク要素間のセキュアな通信の確立に使用可能な認証ネットワーク要素として機能するように構成されるネットワーク要素を備えるデバイスであって、前記ネットワーク要素は、認証ネットワーク要素と共にネットワーク要素に対する認証プロシージャを実行し、認証されたネットワーク要素に対するそれぞれのデータキーを生成し、前記データキーに基づいて前記ネットワーク要素において導出されたそれぞれのセッションキーを、前記認証ネットワーク要素と前記ネットワーク要素との間のセキュアチャネルを使用して、前記ネットワーク要素に配布するように構成される、デバイスが提供される。

【００４２】

前記解決案によって、以下の利点を達成することができる。

【００４３】

前記提案された機構は、ユーザーが、企業ネットワークを介した（トラフィック）伝送を必要とせずに、動的に形成されたネットワークを使用して通信することができる、ピアツーピア仮想プライベートネットワーク（peer-to-peer virtual private network：PVPN）の構築に適用可能である。すなわち、ユーザーが信頼できる近接ネットワークをオンデマンドに形成することが可能である。これは、特に、加入者端末が、Bluetooth、赤外線、WLAN（Wireless Local Area Network：無線ローカルエリアネットワーク）機能などのような、異なる通信用インターフェースを備える場合に有用である。

【００４４】

一方で、PVPNによって前記セキュアな通信に参加しようとしているネットワーク要素は、プロバイダのネットワークインフラストラクチャを使用した既知の認証機構を使用することによって認証することが可能である。したがって、既存のインフラストラクチャを容易に使用することができるので、本発明は、実装が容易でコストが抑えられる。

【００４５】

セキュアな通信が確立されたとき、すなわちセッションキーが交換されたとき、インターネットへのルーターとしても機能することが可能なゲートウェイ要素は、前記ホスト間のセキュアな通信経路に関わる必要が無い。これは、Bluetoothなどのような代替的な通信インターフェースの使用を容易にし、また、確立してすぐに通信に関わる必要が無いので、ゲートウェイネットワーク要素への負担も軽減する。それでも、セキュアな通信が構築される。

【００４６】

セキュアな通信を確立するための機構によって、携帯電話のセキュリティを活用すること、また、特定のネットワーク要素、すなわちゲートウェイ要素における近接ネットワークのセキュリティ管理機能を定義することが可能である。これは、特に、セキュアな通信のためのパーティとして端末またはホストを有する3GPPまたは3GPP2ベースのネットワークのような携帯電話通信ネットワークにおいて有用であり、また対応する近接ネットワー

クにおいても有用である。したがって、オペレータは、例えば、アドホックネットワークなどのセキュリティおよび有用性を改善するために追加機能を提供することによって、ある程度の制御を行うことが可能である。

【００４７】

本発明によれば、受信側が、例えば信頼できるノードであることを確実に知ることなく、IMSI（International Mobile Subscriber Identity：国際移動電話加入者識別番号）のような、ホストに関する機密情報が、通信確立の初期段階において伝送されないようにすることができる。

【００４８】

本発明の上述の目的および更なる目的、機能、および利点は、以下の説明および添付図面を参照することにより、より明らかとなろう。

【図面の簡単な説明】

【００４９】

本発明の更なる実施形態、詳細、利点、および変更は、添付図面に関連してなされる以下の好適な実施形態の詳細な説明から明らかになろう。

【００５０】

【図１】本発明の一実施形態による、２つのホスト間のセキュアな通信を確立するためのシステムのブロック回路図である。

【００５１】

【図２】本発明の一実施形態による、２つのホスト間のセキュアな通信を確立する方法の全般的なフローチャートを示す図である。

【００５２】

【図３】本発明の実施形態による、図2に示される方法のサブルーチンのフローチャートを示す図である。

【００５３】

【図４】本発明の実施形態による、図2に示される方法の別のサブルーチンのフローチャートを示す図である。

【００５４】

【図５】本発明の実施形態による、図2に示される方法の別のサブルーチンのフローチャートを示す図である。

【図６】本発明の実施形態による、図2に示される方法の別のサブルーチンのフローチャートを示す図である。

【００５５】

【図７】本発明の更なる一実施形態による、２つのホスト間のセキュアな通信を確立するためのシステムのブロック回路図である。

【００５６】

【図８】本発明の別の実施形態による、２つのホスト間のセキュアな通信を確立するためのシステムのブロック回路図である。

【好適な実施形態の詳細な説明】

【００５７】

以下、本発明の実施形態を図面を参照して説明する。

【００５８】

本実施形態に基づいて、いわゆるピアツーピア仮想プライベートネットワーク、すなわちPVPN（すなわち近接の範囲）を構築することによって、２つのネットワーク要素間または端末ノード（ホストまたはピアとも称する）間のセキュアな通信を確立するための機構を説明する。すなわち、２つのピアは、通信のためのセキュアチャネルの確立において支援され、セキュアな通信に参加する全てのノードまたはネットワーク要素に対して認証を実行するために、ゲートウェイ要素（ゲートウェイとも称する）と認証ネットワーク要素（アクセスコントローラとも称する）との間の単一のセキュアチャネルを使用する。

【００５９】

上述のように、本は実施形態によるPVPNの構築に重要な１つのネットワーク要素はノードであり、ゲートウェイと呼ばれる。ゲートウェイによって、そのネットワーク内の２つのホストは、互いにセキュアに通信することができる。このために、認証を実行するゲートウェイとネットワーク要素との間のセキュアチャネル（すなわち、上述のアクセスコントローラ）を必要とする。

【００６０】

一般的に、モバイルノードなどである場合があり、PVPNのメンバーとなることを望む各ホストは、アクセスネットワーク認証を実行しなければならない。加えて、PVPNにおいてゲートウェイ要素として機能することを望むホスト（例、モバイルノード）は、その認証プロシージャ中にその旨を示さなければならない。ゲートウェイは、ピアが、今後の通信を保護するために互いのセキュリティパラメータを交換できるように、セキュアチャネルを通信に提供する。ゲートウェイとして機能するネットワーク要素は、その近接ネットワーク内のホストのための、インターネットおよびイントラネットのような内部または外部ネットワークへの接続性も提供することが好ましいことに留意されたい。

【００６１】

認証を実行するネットワーク要素（すなわち、以下に説明する図1に示されるようなアクセスコントローラ）は、セッションキータプル（後述する）、名前（後述する）、およびホストに対応するIPアドレスを、PVPNにセキュアに配布し、PVPNゲートウェイ自体の認証プロシージャ中に確立されたパラメータが使用される（すなわち、セキュアチャネルを経た伝送のために）。

【００６２】

任意の２つのホスト間のPVPN内の初期の通信は、ゲートウェイを介して行われる。これは、意図するピアとセキュアにキータプルを交換するまで、各ホストは、近接ネットワーク内のゲートウェイとしかセキュアに通信することができないからである。ゲートウェイは、アクセスコントローラからバインディングを受信しているので、名前およびIPアドレスバインディングが信頼できるという保証を提供する。ピアが互いのセッションキーを持つと、ゲートウェイはピア間の通信経路に残存する必要が無くなる。

【００６３】

アクセスネットワーク認証プロシージャは、UMTS AKA（Authentication and key agreement：認証およびキー同意、例、3GPP仕様 TS30.102（2004年12月）に記述）、またはケルベロス（Kerberos、RFC1510に記述）のような既知の方法を使用することによって達成されることに留意されたい。アクセスネットワークプロバイダの役割は、ユーザー（すなわちホスト）が、同じ"エンティティ"（同じ企業または企業体など）に属することを確認することである。加えて、ユーザーは、企業ネットワークにアクセスするためにプロバイダのネットワークが必要である。なお、PVPN内の通信は、WLAN、Bluetoothなどのような近接ネットワークを使用して行うことができる。

【００６４】

図1を参照する。図1は、本実施形態による、セキュアな通信を確立するための簡略化したシステム構造およびシグナリング経路を示す図である。なお、図1によるシステムは、本発明が実装される当該のシステムの簡略化した構造を示すに過ぎないことに留意されたい。さらに、本願明細書に記述されるネットワーク要素および/またはそれらの機能は、ソフトウェアまたはハードウェアによって実装することが可能である。いずれにせよ、それぞれの機能を実行するために、それに応じて使用されるデバイスまたはネットワーク要素が、制御、処理、および通信機能に必要な複数の手段（図1には示さず）を備える。当該の手段は、例えば、命令の実行およびデータ処理のためのプロセッサユニットと、プロセッサなどのワークエリアとしての機能を果たすために、命令およびデータを格納するためのメモリ手段（例、ROM、RAM、EEPROMなど）と、ソフトウェアによってデータおよび命令を入力するための入力手段（例、フレキシブルディスク、CD-ROM、EEPROMなど）と、監視および操作の可能性をユーザーに提供するためのユーザーインターフェース手段（例、スクリーン、キーボードなど）と、プロセッサユニットの制御下で通信接続を確立するた

めのインターフェース手段（例、有線および無線インターフェース手段、アンテナなど）と、を備えることが可能である。

【００６５】

図1では、PVPNの確立のためのプロシージャ全体を、PVPN構造を簡略化して示す。参照符号10および40は、PVPNを介してセキュアな通信を確立すべきネットワーク要素またはホスト（例、モバイルホスト）を示す。以下、ホスト1（10）は呼び出しホストであり、ホスト2（40）は着呼ホストである。参照符号20は、ゲートウェイとして機能するネットワーク要素を示す。上述のように、ゲートウェイは、（モバイル）ホストとすることも可能であり、また、インターネットなどへの接続性を提供するために、近接ネットワークにおいてルーターとして機能することが可能である。参照符号30は、ゲートウェイ20に接続可能であり、PVPN通信に参加するホストの認証に使用される認証ネットワーク要素またはアクセスコントローラを示す。

【００６６】

また、図1に示されるように、ゲートウェイ20とホスト10および40のそれぞれとの間に、セキュアチャネルSC15およびSC45が備えられる。加えて、セキュアチャネルSC25が、アクセスコントローラ30とゲートウェイ20との間に備えられる。セキュアチャネルは、点線の四角形で示され、本願明細書において以下に詳述する。

【００６７】

さらに、ネットワーク要素間の複数のシグナリング経路を矢印によって示す。詳しくは、破線の矢印T11、T21、T41は、アクセスコントローラ30によるネットワーク要素10、20、および40のそれぞれのうちの１つの認証中のシグナリングを示す。一方で、二点鎖線の矢印T18およびT48は、ゲートウェイ20を経たホスト10と40との間のセキュアな接続（すなわち、セッションキー交換）の設定中のそれぞれのシグナリングを示す。シグナリングについては、以下に詳述する。

【００６８】

上述のように、ホスト1（10）およびホスト2（40）は、ピアツーピアのセキュアな通信に参加しようとするピアである。ゲートウェイ20は、セキュアなピアツーピア通信を容易にするノードであり、また、モバイルホストからなる（近接）ネットワークのためのルーターである。アクセスコントローラ30は、近接ネットワーク内の全てのホストによって理解される認証プロシージャを実行するノードである。ゲートウェイを含む全てのホストは、セキュアなオンデマンドのネットワーク（すなわち、PVPN）の一部になることができるようになる前に、アクセスコントローラによってそれら自体の認証を成功させる必要がある。

【００６９】

図2は、PVPNを構築し、セキュアなオンデマンドのネットワーク（すなわち、セキュアなピアツーピア接続）を確立するためのプロシージャの全般的な概要を示す図である。ステップS10でプロシージャを開始した後、最初に、ステップS20で、認証ネットワーク要素（アクセスコントローラ）30によって認証プロシージャおよびゲートウェイ20の設定を行う。次いで、ステップS30で、認証ネットワーク要素30によってPVPNに参加しようとしているホストの認証と、認証ネットワーク要素30からゲートウェイ20へのセッションキー配布を実行する。最後に、ステップS40で、ゲートウェイ20を介してホスト10および40によって、セキュアなピアツーピア通信が確立される。ステップS20、S30、およびS40に応じたサブプロシージャを図3（ステップS20）、図4（ステップS30）、図5および6（ステップS40）に示し、以下に説明する。

【００７０】

以下、本実施形態によるPVPNの確立を図1および3乃至6を参照して詳述する。

【００７１】

ホストの各ユーザーは、SIP URI（Session Initiation Protocol Universal Resource Identifier：セッション開始プロトコルユニバーサルリソース識別子）のような名前を有し、各ホストには、グローバルにルーティング可能なIPアドレスが構成されていることに

留意されたい。

【００７２】

ネットワーク要素（例、図1の呼び出しホスト1（10）など）がPVPNの一部になろうとするときには、ゲートウェイまたはホストとして機能する。ネットワーク要素がゲートウェイ要素として機能しようとするとき、図3によるプロシージャ（図2のステップS20を参照のこと）が実行され、以下に説明する。

【００７３】

上述のように、PVPNの一部となる各ネットワーク要素は、アクセスコントローラ30によってそれ自体を認証しなければならない。したがって、ステップS210で、ネットワーク要素は、（PVPNの一部となるために）認証メッセージをアクセスコントローラに送信する（図1のシグナリングT21）。この認証メッセージにおいて、ネットワーク要素は、ゲートウェイとして機能する意思表示を含む。

【００７４】

アクセスコントローラ30では、ネットワークノードがゲートウェイとして機能することを望んでいることを判断するために、認証メッセージを確認する（ステップS220）。ステップS230で、要求ホストに対する適切なゲートウェイ（すなわち、ゲートウェイとして機能する別のネットワーク要素）が存在するかどうかを判断する。この判断は、例えば、データテーブル内のゲートウェイ（図示せず）などとして機能するようなネットワーク要素に対するエントリがすでに存在するかどうかを判断することによって行われる。

【００７５】

ステップS230での判断がNOである場合、すなわち、ネットワーク要素がゲートウェイになることを望み、既知の適切なゲートウェイが存在しない場合、アクセスコントローラ30によって、ネットワーク要素は、認証プロシージャの実行が成功した後に、ゲートウェイ20として機能すること、すなわち、ネットワーク要素をゲートウェイ20として設定することができる（ステップS270およびS280）。ステップS270における認証プロシージャは、複数回のシグナリングを伴うことが可能であり、例えば、UMTS AKAのチャレンジ/レスポンス機構を含む認証方法に基づくことができる。UMTS AKAを使用することで、アクセスコントローラは、SGSN（Serving GPRS support Node：サービングＧＰＲＳサポートノード）/P-CSCF（Proxy-Call Session Control Function：プロキシ-呼セッション制御機能）と同じように機能することが可能である。この場合、PVPNジョインメッセージは、IMS（IP Multimedia Subsystem：IPマルチメディアサブシステム）に類似したサブネット要請（solicitation）およびAKA認証メッセージを含むことが可能である。

【００７６】

ステップS270およびS280の後、ゲートウェイの認証に成功した結果は、アクセスコントローラ30による通信を保護できることを示す（ステップS290）。これは、アクセスコントローラ30とゲートウェイ20との間の通信が、例えば、認証プロシージャにおいて生成されたセッションキーによって暗号化および解読することができることを意味するものであり、図1のセキュアチャネルSC25によって示される。

【００７７】

一方で、要求ホストに対する適切なゲートウェイが存在する（ステップS230でNOである）場合、アクセスコントローラは、ネットワーク要素をこのゲートウェイにリダイレクトする（ステップS240）。しかし、ステップS230で、ネットワーク要素が、アクセスコントローラによって決定されたゲートウェイに到達できない場合がある。これは、例えば、ステップS250で、ネットワーク要素が、ステップS230のNOの判断に関連して、アクセスコントローラによって示されたゲートウェイが到達可能であるかどうかを判断する場合に確認される。

【００７８】

ステップS250の判断がYESの場合、ステップS230のNOの判断に関連してアクセスコントローラによって示されたゲートウェイが、更なる通信で使用される（ステップS255）。一方で、ステップS250の判断がNOの場合、ネットワーク要素は、ゲートウェイとして機能す

る旨のリクエストをアクセスコントローラ30に再発行することが可能である（ステップS260）。次いで、ステップS270乃至S290が実行されるが、これは、例えば、ホスト認証が、少なくとも１回の通信を伴うチャレンジ/レスポンス方法を再び含むことが可能であることを意味する。

【００７９】

これは、PVPNの初期フェーズにおいて、上述のように、アクセスコントローラによって認証プロシージャを実行する最初のネットワーク要素を、デフォルトでゲートウェイとして機能するように設定する、本実施形態の好適なオプションであることに留意されたい。

【００８０】

ネットワーク要素が、ゲートウェイとなる意思表示を送信せずに、単にホストとして機能することを望む場合、図4に示されるように、（図2のステップS30に従って）ホスト認証およびセッションキー配布のためのプロシージャが実行される。

【００８１】

図4によるプロシージャでは、ステップ310乃至330は、図3によるステップS210、S220、およびS270に類似する。ステップS310では、ネットワーク要素すなわちホスト（例、図1の10および40）は、認証メッセージをアクセスコントローラ30に送信する（図1のシグナリング経路T11およびT41）。認証のためのシグナリングは、ホストのIPアドレスがゲートウェイの20のプレフィックスから導出されるので、図1に示されるように、ゲートウェイ20を介して実行される。ホストの認証にはセキュアチャネルが不要であることにあらためて留意されたい。なお、後述するように、データキーがアクセスコントローラから伝送されるときには、当該のセキュアチャネルが使用される。アクセスコントローラは、例えば、要求ホストが企業ネットワークの一部であることを判断するために、認証メッセージのコンテンツを確認するので、通常、PVPNのメンバーとなることを許可される（ステップS320）。ステップS320による確認が要求ホストの認証にいかなる障害ももたらさない場合、アクセスコントローラ30は、ステップS330で、認証プロシージャを実行および完了する。

【００８２】

アクセスコントローラ30は、ホスト10および40の認証に成功し、PVPNの一部になると、認証された全てのホストに対する認証プロシージャ中に確立された、それぞれのセッションキーも登録される。これらのセッションキーに基づいて、アクセスコントローラは、ステップS340で、各ホストがPVPNの設定時に使用すべき新しいキーを生成する。新しいキーの生成は、例えば、次のロジックに基づくことが可能である。

新しいキー = SHA1（既存のキー ｜ ホストのIPアドレス ｜ PVPNのID ｜ シリアル番号）

【００８３】

ここで、SHA1は、（例えばRFC3174による）セキュアなハッシュアルゴリズムを表し、「既存のキー」は、関連するホストと共有されるセッションキーを意味し、「ホストのIPアドレス」は、そのホストに関連し、「PVPNのID」は、認証メッセージに応じてアクセスコントローラによって割り当てられた特定のゲートウェイに関連付けられた一意の識別子であり、「シリアル番号」は、ホストによって送信された認証メッセージ内のランダムな整数である。当該ホストが、PVPNで使用するための類似したキーを生成することにも留意されたい。

【００８４】

アクセスコントローラは、完全性保護および暗号化のそれぞれに対する１つのキー、または単一のキーを生成することが可能である。いずれにせよ、アクセスコントローラ30は、続いて、ステップS350で、単一または複数のキー、すなわち、アクセスコントローラ30によって認証プロシージャを実行した全てのホストの単一または複数のキーをゲートウェイ20に転送する。加えて、セキュアな通信に必要な、当該のホストの名前およびIPアドレスのような当該のホストに関連する識別データ、および他のパラメータが、新しい単一または複数のキーによってゲートウェイ20に伝送される。特に、アクセスコントローラ30は、これらのパラメータを有する新しいIPメッセージを構成し、ゲートウェイ20と共有する

セッションキーを使用してパケットのコンテンツを暗号化し、暗号化したパケットを伝送する。これを、図1の矢印T31によって示す。ゲートウェイ20は、共有セッションキーを使用してパケットを解読し、その詳細（すなわち、上記の導出された名前、IPアドレス、および「新しいキー」）をメモリに記録する（ステップS360）。したがって、ゲートウェイには、アクセスコントローラによって認証が行われ、PVPNに参加しようとするホストのデータキーおよび識別情報が提供される。さらに、ホスト10および40は、ゲートウェイ20と通信すること、すなわち図1に参照符号SC15およびSC45で示されるそれぞれのセキュアチャネルを介して通信することが可能となる。

【００８５】

次に、PVPNを経たセキュアなピアツーピア接続の確立の一例を、図5および6を参照して説明する。図5および6の複合フローチャートは、図2のステップS40に基づいたサブルーチンに対応する。

【００８６】

以下の説明において、用語"New-key-sender"とは、同様に派生した"New-key-receiver"である受信者（すなわち、ホスト40のような別のホスト）との通信の開始を試みているネットワーク要素またはホスト（例えば、図1のホスト10）によって、上述のように生成されたキーのことである。上述のように、シグナリングT31およびステップS350の結果として、両方のキーをゲートウェイ20で利用することが可能である。

【００８７】

ネットワークノードがアクセスコントローラ30によって認証プロシージャを実行し、アクセスコントローラ30がデータキー情報をゲートウェイ20に転送するときに、セキュアな接続の確立を開始することができる。呼び出しホスト10のような送信者が、ホスト40のような別のネットワーク要素との通信を望むときには、最初に、SIP URIのようなユーザーフレンドリーな名前をIPアドレスに対応付ける必要がある。以下、当該の構成を名前と称する。送信者10は、最初にセッションキーS_{ks}を生成する。次いで、送信者は、受信者の名前を対応付けるためのリクエストを構成または作成する。このリクエストは、例えば、送信者の名前と、そのIPアドレスと、セッションキーS_{ks}と、セッションキー長さと、暗号化に使用すべきアルゴリズムと、受信者の名前とを含む。セッションキーと、キー長さと、アルゴリズムを含む構成をキータプルとも称する。

【００８８】

送信者10は、New-key-senderを使用することによって上述のように作成されたリクエストを暗号化して（ステップS410）、パケットをゲートウェイ20に伝送する（ステップS420）。送信者10は、利用可能なルーティング方法を使用して、リクエストがゲートウェイ20に到達するようにできる。これを、図1に参照符号T18の上段の二点差線で示す。

【００８９】

ゲートウェイ20には、アクセスコントローラ30から対応するNew-key-senderが提供される（ステップS350）ので、リクエストを含むメッセージを解読することができる。ステップS430で、ゲートウェイ20は、送信者10からのリクエストメッセージを解読して、その送信者がPVPNへの参加を許可されたことを検証することによって処理する。ゲートウェイ20自体は、ホスト10を認証することができないが、ホストが送信したパケットを解読することができることに留意されたい。これによって、ホストは、ホストとアクセスコントローラとの間の遷移的信頼によって、ゲートウェイを信頼することができる。ゲートウェイ20は、最初に、送信者10の名前およびIPアドレスが、アクセスコントローラ30から受信した値と一致するかどうかを検証する。

【００９０】

次いで、ゲートウェイ20は、この瞬間に到達可能な受信者が存在するかどうかを確認する（ステップS440）。すなわち、ゲートウェイ20は、リクエスト内の受信者の名前に対応するIPアドレスの位置を特定するように、対応するテーブルを参照することが可能である。

【００９１】

受信者の名前に対するエントリが見つかり、受信者のIPアドレスに対する経路が存在する（ステップS440でYES）場合、ゲートウェイ20は、ステップS450で、送信者からの名前、IPアドレス、およびキータプルを含む受信者（例、ホスト40）に送信すべきパケットを作成し、受信者と共有するNew-key-receiver（ステップS350で、アクセスコントローラ30によって伝送されたもの）を使用することによってパケットを暗号化する。次いで、パケットは、受信者またはホスト40にユニキャストされる（ステップS460）。

【００９２】

一方で、受信者の名前に対するエントリが見つからないか、または受信者の名前に対応するIPアドレスに対する経路が存在しない（ステップS440でNO）場合、ゲートウェイ20は、パケットを構成して名前または経路、あるいはその両方を対応付ける。このパケットは、ディスカバリパケットとも呼ばれる。ディスカバリパケットでは、ゲートウェイ20はまた、送信者の名前と、IPアドレスと、キータプルとを含み、New-key-receiverを使用することによってそのパケットを暗号化する（ステップS470）。次いで、ディスカバリパケットは、受信者に伝送されるようにブロードキャストされる（ステップS480）。すなわち、ゲートウェイ20は、受信者の名前をそのIPアドレスに対応付けて、受信者への経路を確立する。

【００９３】

ユニキャストまたはブロードキャストされたパケットが、ステップS490で、受信者またはホスト40に到達したとき（図1にT48の上段の二点差線で示す）、受信者は、New-key-receiverを使用してそのパケットを解読することによって受信したデータを処理する（ステップS500）。加えて、受信者は、今後の通信のために、送信者のセッションキータプルをメモリ（図示せず）に記録する。次いで、ステップS510で、受信者（すなわち、ホスト40）は、それ自体の名前と、IPアドレスと、上述したものに類似したセッションキータプルとを含む、応答メッセージを作成する。作成は、再びNew-key-receiverを使用した受信者によるメッセージの暗号化も含む。応答メッセージまたはパケットが作成されると、ゲートウェイ20に伝送される。

【００９４】

ゲートウェイ20は、発見メッセージのようなゲートウェイ20のメッセージに対する応答メッセージを受信すると（図1にT48の下段の二点差線で示す）、応答メッセージを処理して、New-key-receiverを使用してそのメッセージを解読する（ステップS520）。次いで、ゲートウェイ20は、New-key-senderを使用することによって応答メッセージのコンテンツを再暗号化して、作成されたメッセージを送信者10に転送する（ステップS530）。これを、図1にT18の下段の二点差線で示す。送信者10は、ゲートウェイ20から受信したメッセージを処理して、受信者40のセッションキーを導出して格納する（ステップS540）。これで、送信者10および受信者40の両方が、互いのセッションキータプルを有することになり、セキュアな通信を行うことができる。

【００９５】

ピア10および40のどちらも、ゲートウェイ20を介した互いへの経路も確立することが可能であることに留意されたい。したがって、ステップS550で、セキュアな双方向性の通信を、ピア間で開始することができる。ピア間の通信経路では、ゲートウェイ20を含む必要は無い。

【００９６】

以下、本発明の更なる実施形態を、図7を参照して説明する。

【００９７】

図7は、２つのホスト間のセキュアな通信、およびシステム内の対応するシグナリングを確立するためのシステムのブロック回路図である。本実施形態によるシステムの基本構造は、図1に示されたものに類似する。

【００９８】

詳しくは、図7では、本実施形態によるPVPN確立のためのプロシージャ全体を、PVPN構造を簡略化して示す。参照符号100および400は、PVPNを介してセキュアな通信を確立すべ

きネットワーク要素またはホスト（例、モバイルホスト）を示す。以下、ホスト1（100）は呼び出しホストであり、ホスト2（400）は着呼ホストである。参照符号200は、ゲートウェイとして機能するネットワーク要素を示す。上述のように、ゲートウェイは、（モバイル）ホストとすることも可能であり、また、インターネットなどへの接続性を提供するために、近接ネットワークにおいてルーターとして機能することが可能である。参照符号215は、ゲートウェイに配布されるP2P（peer-to-peer：ピアツーピア）ネットワークキー配布または要素を示す。以下、P2Pネットワークキー配布機能または要素の機能を説明する。参照符号300は、ゲートウェイ200に接続可能であり、PVPN通信に参加するホストの認証に使用される認証ネットワーク要素またはアクセスコントローラを示す。

【００９９】

セキュアチャネルSC150およびSC450は、ゲートウェイ200とそれぞれのホスト100および400との間に確立される。加えて、セキュアチャネルSC250が、アクセスコントローラ300とゲートウェイ200との間に確立される。セキュアチャネルは、点線の四角形で示され、本願明細書において以下に詳述する。

【０１００】

ネットワーク要素間の複数のシグナリング経路を矢印によってさらに示す。詳しくは、破線の矢印T110、T210、T410は、アクセスコントローラ300によるネットワーク要素100、200、および400のそれぞれのうちの１つの認証中のシグナリングを示す。一方で、二点鎖線の矢印T180およびT480は、ホスト100および400と、ゲートウェイ200のP2Pネットワークキー配布要素215との間のセキュアな接続（すなわち、セッションキー配布）の設定中のそれぞれのシグナリングを示す。シグナリングについては、以下に詳述する。

【０１０１】

上述のように、ホスト1（100）およびホスト2（400）は、ピアツーピアのセキュアな通信に参加しようとするピアである。ゲートウェイ200は、セキュアなピアツーピア通信を容易にするノードであり、また、モバイルホストからなる（近接）ネットワークのためのルーターである。アクセスコントローラ300は、近接ネットワーク内の全てのホストによって理解される認証プロシージャを実行するノードである。ゲートウェイを含む全てのホストは、セキュアなオンデマンドのネットワーク（すなわち、PVPN）の一部になることができるようになる前に、アクセスコントローラによってそれら自体の認証を成功させる必要がある。

【０１０２】

本実施形態に基づいて、PVPNを構築し、セキュアなオンデマンドのネットワーク（すなわち、セキュアなピアツーピア接続）を確立するための全般的なプロシージャは、図2に示されるものと類似する。これは、プロシージャが開始された後、最初に、ゲートウェイ200および（ゲートウェイ200を経た）ホスト100および400に対して、認証ネットワーク要素（アクセスコントローラ）300によって実行されることを意味する。本実施形態の説明では、ゲートウェイ200は、ゲートウェイとして機能するように設定され、他の好適なゲートウェイが存在しないものと仮定している。なお、第二の実施形態も、第一の実施形態で説明したように、ネットワーク要素200の代わりに別のゲートウェイを使用する場合に適用することが可能である。次いで、セッションキー配布が実行されるが、これは以下に詳述する。その後、ゲートウェイ200を介して、ホスト100および400によってセキュアなピアツーピア通信が確立される。

【０１０３】

以下、本実施形態によるPVPN作成の詳細を図7を参照して説明する。

【０１０４】

上述のように、PVPNの一部となる各ネットワーク要素は、アクセスコントローラ300によってそれ自体を認証しなければならない。したがって、ネットワーク要素200は、（PVPNの一部となるために）認証メッセージをアクセスコントローラに送信する（図7のシグナリングT210）。認証メッセージでは、ネットワーク要素は、ゲートウェイとして機能する意思表示を含む。

【０１０５】
本実施形態では、アクセスコントローラ300によって、ネットワーク要素200は、認証プロシージャの実行が成功した後に、ゲートウェイとして機能することができる。すなわち、ネットワーク要素がゲートウェイ200として設定される。アクセスコントローラ300で実行される認証プロシージャは、複数回のシグナリングを伴うことが可能であり、例えば、UMTS AKAのチャレンジ/レスポンス機構を含む認証方法に基づくことができる。UMTS AKAを使用することで、アクセスコントローラは、SGSN/P-CSCFと同じように機能することが可能である。この場合、PVPNジョインメッセージは、IMS（IP Multimedia Subsystem：IPマルチメディアサブシステム）認証プロシージャに類似したサブネット要請（solicitation）およびAKA認証メッセージを含むことが可能である。

【０１０６】
ゲートウェイの認証が成功した後に、アクセスコントローラ300との通信をセキュアにすることができる。これは、アクセスコントローラ300とゲートウェイ200との間の通信を、例えば認証プロシージャにおいて生成されたセッションキーによって、暗号化および解読することができることを意味し、図7にセキュアチャネルSC250で示す。

【０１０７】
次のフェーズでは、ホスト1および2（100および400）は、ゲートウェイ200を介して、アクセスコントローラによる認証プロシージャを実行する。このプロシージャでは、ネットワーク要素、すなわちホスト100、400は、認証メッセージをアクセスコントローラ300に送信する（図７のシグナリング経路T110およびT410）。認証のためのシグナリングは、ホストのIPアドレスがゲートウェイの200のプレフィックスから導出されるので、図7に示されるように、ゲートウェイ200を介して実行される。ホストの認証にはセキュアチャネルが不要であることにあらためて留意されたい。なお、データキーがアクセスコントローラから伝送されるときには、当該のセキュアチャネルを使用することが可能である。アクセスコントローラは、例えば、要求ホストが企業ネットワークの一部であることを判断するために、認証メッセージのコンテンツを確認するので、通常、PVPNのメンバーとなることを許可される。確認が要求ホストの認証にいかなる障害ももたらさない場合、アクセスコントローラ300は、認証プロシージャを実行および完了する。

【０１０８】
アクセスコントローラ300が、ホスト100および400の認証に成功し、PVPNの一部になると、認証された全てのホストに対する認証プロシージャ中に確立された、それぞれのセッションキーも登録される。ホスト100および400は、認証プロシージャの結果として、それぞれのセッションキーも有する。

【０１０９】
さらに、アクセスコントローラ300は、セッションキーに基づいて、異なる種類のキー、例えば完全性保護および暗号化のそれぞれに対する１つのキー、または単一のキーを生成することが可能である。導出されたキーは、キー導出機能に対する入力としてのアイデンティティを作成することによって、P2Pネットワークキー配布要素のアイデンティティ（すなわち、ゲートウェイアイデンティティ）に連結される。

【０１１０】
いずれにせよ、アクセスコントローラ300は、続いて、単一または複数のキー、すなわち、アクセスコントローラ300によって認証プロシージャを実行した全てのホストの単一または複数のキーをゲートウェイ200に配布する。加えて、セキュアな通信に必要な、当該のホストの名前およびIPアドレスのような当該のホストに関連する識別データ、および他のパラメータが、新しい単一または複数のキーによってゲートウェイ200に伝送される。例えば、アクセスコントローラ300は、これらのパラメータを有する新しいIPメッセージを構成し、ゲートウェイ200と共有するセッションキーを使用してパケットのコンテンツを暗号化し、暗号化したパケットを伝送する（矢印T310）。ゲートウェイ200は、共有セッションキーを使用してパケットを解読し、その詳細（すなわち、上記の導出された名前、IPアドレス、およびNew-key）をメモリに記録する。P2Pネットワークキー配布要素21

5は、メモリおよびその中に格納されるデータにアクセスする。したがって、P2Pネットワークキー配布要素215は、アクセスコントローラによって認証が行われ、PVPNに参加しようとするホストのデータキーおよび識別情報にアクセスすることができる。

【０１１１】

次いで、ホスト1（100）およびホスト2（400）は、認証結果およびゲートウェイアイデンティティに基づいて、特定のセッションキー、すなわちゲートウェイセッションキーを導出する。これは、アクセスコントローラ300が実行するキー導出プロシージャに類似した方法で実行することが可能である。これで、セキュアチャネルSC150およびSC450が確立される。ホスト100および400、およびゲートウェイ200が互いに通信するときには、セキュアチャネルSC150およびSC450を使用する。ホスト1（100）およびホスト2（400）は、アクセスコントローラがP2Pキーディストリビュータ（例、ゲートウェイ）を認証していることを確認できるので、ホスト1（100）およびホスト2（400）がそれを認証する。ホスト100および400は、SC150およびSC450を介してゲートウェイ200と通信することができ、ゲートウェイ200（およびSC150およびSC450）を介して互いに通信することができる。

【０１１２】

本発明の実施形態によれば、ゲートウェイ200は、P2Pネットワークキー配布機能または要素215によって、ピアツーピアキー、例えば全てのピアツーピアノード間の共有キーを配布するように構成される。別様には、ゲートウェイ200は、ホスト（例、100および400）がホストツーホストのセキュアトンネル（図7には示さず）を形成できるように、キーディストリビュータとして機能する。

【０１１３】

ゲートウェイ200からホスト100および400へのピアツーピアセッションキーの配布を、ホスト1（100）へは矢印T180で、ホスト2（400）へは矢印T480で示す。加えて、セキュアな通信に必要な、当該のホストの名前、IPアドレス（範囲/サブネット）のような当該のホストに関連する識別データ、および他のパラメータが、新しい単一または複数のキーによってホスト100および400に伝送される。例えば、ゲートウェイ200は、これらのパラメータを有する新しいIPメッセージを構成し、ホスト100および400と共有するセッションキーを使用してパケットのコンテンツを暗号化し、暗号化したパケットを伝送する（矢印T180、T480）。ホスト100および400は、共有セッションキーを使用して対応するパケットを解読し、その詳細（すなわち、ゲートウェイによって構築された名前、IPアドレス（範囲/サブネット）、および新しいピアツーピアキー）をメモリに記録する。配布されたピアツーピアセッションキーによって、例えばホスト間で直接BluetoothまたはWLAN接続を使用するときに、ホストは、互いに直接通信することができる（図7に矢印500で示す）。

【０１１４】

図8では、本発明の別の実施形態を説明する。

【０１１５】

図8は、２つのホスト間のセキュアな通信を確立するためのシステム、およびシステム内の対応するシグナリングのブロック回路図である。本実施形態によるシステムの基本構造は、図1および7に示されたものに類似する。

【０１１６】

詳しくは、図8では、本実施形態によるPVPN確立のためのプロシージャ全体を、PVPN構造を簡略化して示す。参照符号1000および4000は、PVPNを介してセキュアな通信を確立すべきネットワーク要素またはホスト（例、モバイルホスト）を示す。以下、ホスト1（1000）は呼び出しホストであり、ホスト2（4000）は着呼ホストである。参照符号2000は、ゲートウェイとして機能するネットワーク要素を示す。上述のように、ゲートウェイは、（モバイル）ホストとすることも可能であり、また、インターネットなどへの接続性を提供するために、近接ネットワークにおいてルーターとして機能することが可能である。参照符号3000は、ゲートウェイ2000に接続可能であり、PVPN通信に参加するホストの認証に使用される認証ネットワーク要素またはアクセスコントローラを示す。

【０１１７】

セキュアチャネルSC1500およびSC4500は、アクセスコントローラ3000とそれぞれのホスト1000および4000との間に確立される。アクセスコントローラ3000からホストへのトンネルは、直接ホストツーホストのセキュアな通信（すなわち、下述のSC6000）を確立するときに、発信者に対してのみ使用されることに留意されたい。加えて、セキュアチャネルSC2500が、アクセスコントローラ3000とゲートウェイ2000との間に確立される。セキュアチャネルは、点線の四角形で示され、本願明細書において以下に詳述する。

【０１１８】

さらに、ネットワーク要素間の複数のシグナリング経路を矢印によって示す。詳しくは、破線の矢印T1100、T2100、T4100は、アクセスコントローラ3000によるネットワーク要素1000、2000、および4000のそれぞれのうちの１つの認証中のシグナリングを示す。一方で、二点鎖線の矢印T1800およびT4800は、ホスト1000および4000と、アクセスコントローラ3000との間のセキュアな接続（すなわち、セッションキー配布）の設定中のそれぞれのシグナリングを示す。シグナリングについては、以下に詳述する。

【０１１９】

上述のように、ホスト1（1000）およびホスト2（4000）は、ピアツーピアのセキュアな通信に参加しようとするピアである。ゲートウェイ2000は、セキュアなピアツーピア通信を容易にするノードであり、また、モバイルホストからなる（近接）ネットワークのためのルーターである。アクセスコントローラ3000は、近接ネットワーク内の全てのホストによって理解される認証プロシージャを実行するノードである。ゲートウェイを含む全てのホストは、セキュアなオンデマンドのネットワーク（すなわち、PVPN）の一部になることができるようになる前に、アクセスコントローラによってそれら自体の認証を成功させる必要がある。

【０１２０】

本実施形態に基づいて、PVPNを構築し、セキュアなオンデマンドのネットワーク（すなわち、セキュアなピアツーピア接続）を確立するための全般的なプロシージャは、図2に示されるものと類似する。これは、プロシージャが開始された後、最初に、ゲートウェイ2000および（ゲートウェイ200を経た）ホスト1000および4000に対して、認証ネットワーク要素（アクセスコントローラ）3000によって実行されることを意味する。本実施形態の説明では、ゲートウェイ2000は、ゲートウェイとして機能するように設定され、他の好適なゲートウェイが存在しないものと仮定している。なお、本実施形態も、第一の実施形態で説明したように、ネットワーク要素2000の代わりに別のゲートウェイを使用する場合に適用することが可能である。次いで、セッションキー配布が実行されるが、これは以下に詳述する。その後、ゲートウェイ2000を介して、ホスト1000および4000によってセキュアなピアツーピア通信が確立される。

【０１２１】

以下、本実施形態によるPVPN作成の詳細を図8を参照して説明する。

【０１２２】

上述のように、PVPNの一部となる各ネットワーク要素は、アクセスコントローラ3000によってそれ自体を認証しなければならない。本実施形態では、ネットワーク要素2000およびホスト1000および4000の認証は、図1および7に示される実施形態に関連して説明したものに対応するので、ここでは、認証プロシージャ（図8に、矢印T2100、T1100、およびT4100で示す）の説明を省略する。なお、上述のように、ホスト1000および4000の認証プロシージャは、図8にT1100およびT4100で示される、セキュアトンネルの外部に位置するセキュアチャネルを使用せずに実行することができる。

【０１２３】

【０１２４】

図8に示されるように、アクセスコントローラ3000は、ホストに対するキーディストリビュータとして機能する。これは、セッションキーが、アクセスコントローラ3000によってホスト1（100）0およびホスト2（400）0に配信される（矢印T1800およびT4800を参照のこと）ので、ホスト1000および4000は、ホストツーホストのセキュアトンネル（SC6000）

を形成することができる。当該のセキュアな接続は、図8に矢印5000で示されるように、（例えば、ホスト間で直接BluetoothまたはWLAN接続を使用するときに）ホスト間に直接確立することもできる。キー配布の場合、アクセスコントローラ3000は、図7によるプロシージャにおけるゲートウェイのように、単にキーをそれぞれのホストに送信するか、またはキーをホストツーアクセスコントローラの認証結果に連結する。

【０１２５】

これは、ホスト1（1000）が、アクセスコントローラ3000によって提供された共有キーに基づいて、ホスト2（4000）に対して例えばキー１と呼ばれるセッションキーを導出し、アクセスコントローラが、ホスト2（4000）が対応するリクエストなどを送信した場合に、キーを率先的に、または反動的にホスト2（4000）に送信することを意味する。ホスト1（1000）がホスト2（4000）と交信するときには、キー１を使用する。

【０１２６】

一方で、ホスト2（4000）は、アクセスコントローラ3000によって提供された共有キーに基づいて、ホスト1（1000）に対して例えばキー２と呼ばれるセッションキーを導出する。アクセスコントローラ3000は、キー２をホスト1（1000）に送信する。ホスト2（4000）がホスト1（1000）と交信するときには、キー２を使用する。

【０１２７】

異なるキー（キー１、キー２）は、一方向のみ、または双方向で使用することができる。例えば、ホスト1からホスト2へのパケットはキー１を使用し、ホスト2からホスト1ではキー２を使用する。別様には、どのパーティ（ホスト1またはホスト2）が接続を起動したかに基づいて、１つのキーが双方向に使用される（例えば、ホスト1による起動の場合はキー１を使用し、ホスト2による起動の場合はキー２を使用する）。

【０１２８】

上述の実施形態では、PVPNシステムにおいて、ゲートウェイのアドレスおよび名前が、デバイスまたはネットワーク要素に予め構成されている場合に好都合である。その結果、そのアドレスおよび名前の認証は、上述の実施形態のプロシージャによって提供することができる。これにより、ゲートウェイと通信するピアは、そのゲートウェイが適切なゲートウェイであるかどうか分からない、ということを回避することが可能である。認証者の観点から、例えば、１つの加入者に属するネットワーク要素に対して、一方で特定のゲートウェイが適切ではない別の加入者に属するネットワーク要素に対して、ゲートウェイを、限られた組のピアに対してのみ正当化されたゲートウェイとすることが可能である。

【０１２９】

さらに、セッションキーの作成は、IPアドレスのみに明示的に結び付けてはならない。また、完全修飾ドメイン名FQDN（Fully Qualified Domain Name）またはネットワークアクセス識別子NAI（Network Access Identifier）のような他のパラメータ、またはキーの作成に使用されるデバイスタイプ、リンクレイヤータイプ、およびアルゴリズムのような付く数のパラメータの組み合わせを使用することができる。

【０１３０】

上述の実施形態では、ローカルゲートウェイがキーディストリビュータとして機能する場合の、セキュアなP2P通信を提供する可能性を説明している。さらに、アクセスコントローラ300のようなキーディストリビュータ機能を、ゲートウェイ（P2Pキーディストリビュータ）200に対して説明したように配布できることを説明している。

【０１３１】

上述のように、第一の実施形態によるP2Pネットワーク内のノードは、それらが互いに共有キーを持たないので、ユニキャストトラフィックを実行する。なお、セッションキーS_{ks}をゲートウェイに送信するための、ホストによるキーの作成の別様として、ゲートウェイが、P2Pネットワークにおけるブロードキャスト/マルチキャストトラフィックも可能であるような方法で、ピアにキーを提供することも可能である。換言すれば、ゲートウェイは、同じキーを複数のホストに提供することができる。これにより、ゲートウェイは、どのホストがキーを持ち、どれが持っていないのかを制御することもできる。対応する方

法または機構を、図7に関連する実施形態を参照して説明する。

【０１３２】

ホストが他のホストを認証することができないとき、ホストは、ゲートウェイのアクションを検証することができない。すなわち、ホストは、ゲートウェイがデータを適切なデスティネーションだけに転送していることを確認することができない。

【０１３３】

したがって、本発明の一実施形態によれば、ホストとアクセスコントローラとの間のシグナリングを実行することが可能である。アクセスコントローラプロトコルは、それに対応して、このシグナリングを可能にするために拡張される。本アクセスコントローラでは、アクセスコントローラとゲートウェイとの間のセキュアトンネル内の対応する認証方法はすでにサポートされているので、この機能は、ホストとのシグナリングにも使用することができる。対応する方法または機構を、図8に関連する実施形態を参照して説明する。

【０１３４】

上述の実施形態に関して、図1乃至6に関連する実施形態によれば、セキュアな通信接続の認証および確立のためのシグナリングがローカル化されるという点で特に好都合である。

【０１３５】

一方で、図7に関連する実施形態では、ゲートウェイがP2Pキーディストリビュータとして機能し、第一の実施形態では、キー送信者のピアがキーを提供する。したがって、図7による実施形態は、ゲートウェイが各ピアに同じキーを提供することができるような、ブロードキャスト/マルチキャスト通信に特に好都合である。換言すれば、複数のパーティによるキーの共有を容易にすることが可能である。例えば、後にパーティがPVPNに参加するときに、ゲートウェイは、同じキーをこれらのパーティにも送信することができる。

【０１３６】

図8に関連する実施形態による別の機構では、ホストツーホスト認証は、認証サーバーとしてアクセスコントローラを伴うことによって提供される。この場合、アクセスコントローラは、更なる実施形態におけるデートウェイと同じようにキーディストリビュータとして機能する。この実施形態では、アクセスコントローラを使用して、１つのホストがゲートウェイとして機能するP2P接続を形成する。

【０１３７】

本発明の実施形態によれば、セキュアな通信接続に必要なキーおよび関連する情報は、例えば直接アクセスコントローラから、ホストに配布することが可能である。

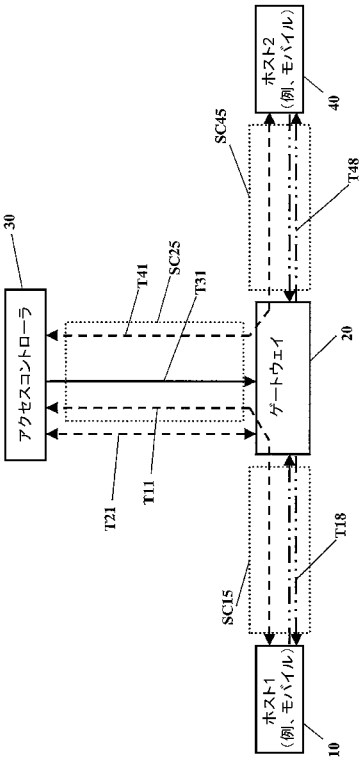
【０１３８】

上述のように、通信ネットワーク内のネットワーク要素間のセキュアな通信を確立するための機構を提案する。ネットワークノードは、認証ネットワーク要素と共に認証プロシージャを実行する。認証ネットワークは、ネットワーク要素のうちの１つをゲートウェイ要素とすることも可能である。次いで、認証されたネットワーク要素に対するそれぞれのデータキーが生成され、認証ネットワーク要素とゲートウェイ要素との間のセキュアチャネルを使用することによって、ゲートウェイ要素に配布される。データキーは、ゲートウェイ要素に格納される。セキュアな通信を設定するときには、セキュアな通信に参加しようとしているネットワーク要素にそれぞれのセッションキーが生成される。セッションキーは、ゲートウェイ要素とネットワーク要素との間のセキュアチャネルを介して、セキュアな通信に参加しようとしているネットワーク要素間で交換される。

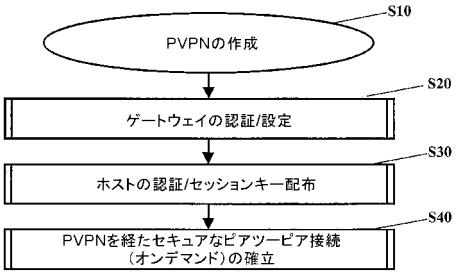
【０１３９】

上記の説明および添付図面は、単に一例として本発明を示すことを目的としたものであると理解されたい。したがって、本発明の好適な実施形態は、添付の請求項の範囲内で変更することが可能である。

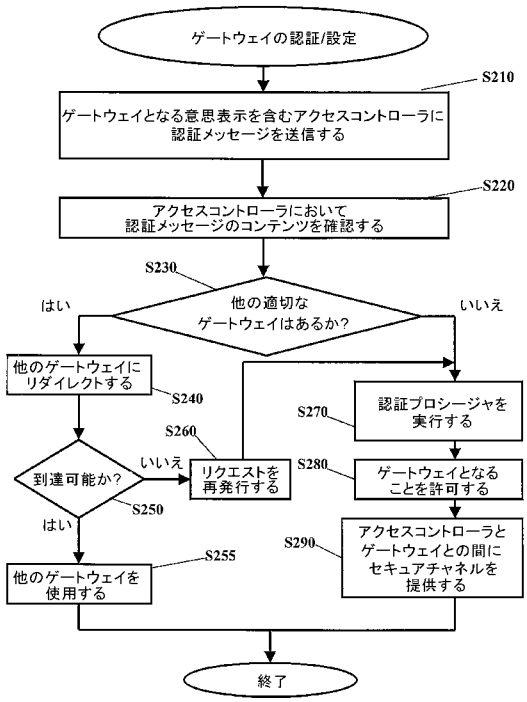
【図１】


ホスト2
（例、モバイル）
40
SC45
T48
30
T41
SC25
T31
アクセスコントローラ
ゲートウェイ
20
T21
T11
T18
SC15
ホスト1
（例、モバイル）
10

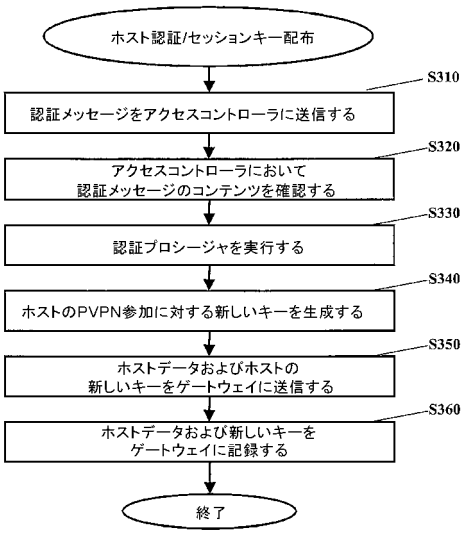
【図２】


S10
PVPNの作成
S20
ゲートウェイの認証/設定
S30
ホストの認証/セッションキー配布
S40
PVPNを経たセキュアなピアツーピア接続
（オンデマンド）の確立

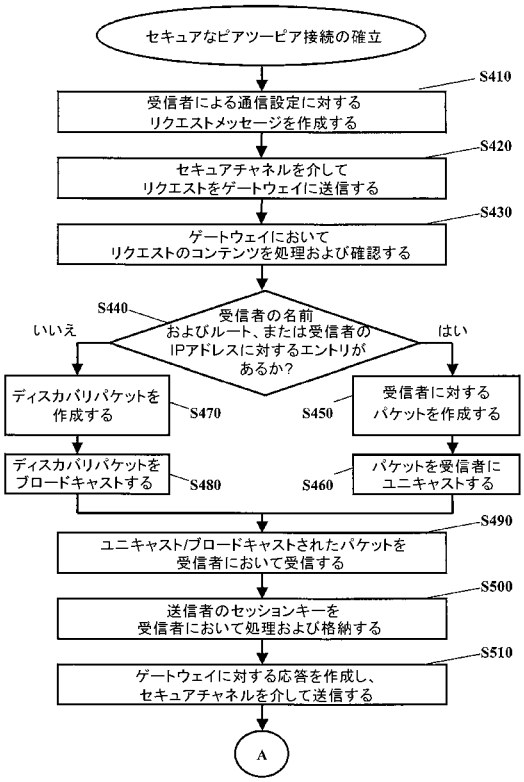
【図３】


ゲートウェイの認証/設定
S210
ゲートウェイとなる意思表示を含むアクセスコントローラに
認証メッセージを送信する
S220
アクセスコントローラにおいて
認証メッセージのコンテンツを確認する
S230
他の適切な
ゲートウェイはあるか？
はい
いいえ
他のゲートウェイに
リダイレクトする
S240
S270
認証プロシージャを
実行する
S260
到達可能か？
いいえ
リクエストを
再発行する
S280
ゲートウェイとなる
ことを許可する
S250
はい
S290
アクセスコントローラと
ゲートウェイとの間に
セキュアチャネルを
提供する
S255
他のゲートウェイを
使用する
終了

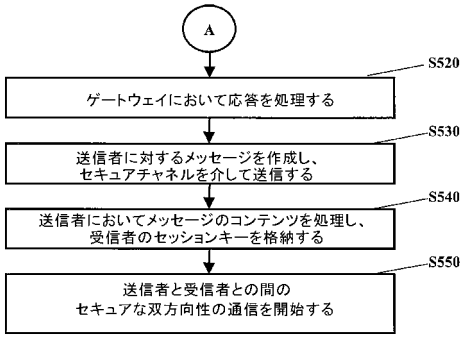
【図４】


ホスト認証/セッションキー配布
S310
認証メッセージをアクセスコントローラに送信する
S320
アクセスコントローラにおいて
認証メッセージのコンテンツを確認する
S330
認証プロシージャを実行する
S340
ホストのPVPN参加に対する新しいキーを生成する
S350
ホストデータおよびホストの
新しいキーをゲートウェイに送信する
S360
ホストデータおよび新しいキーを
ゲートウェイに記録する
終了

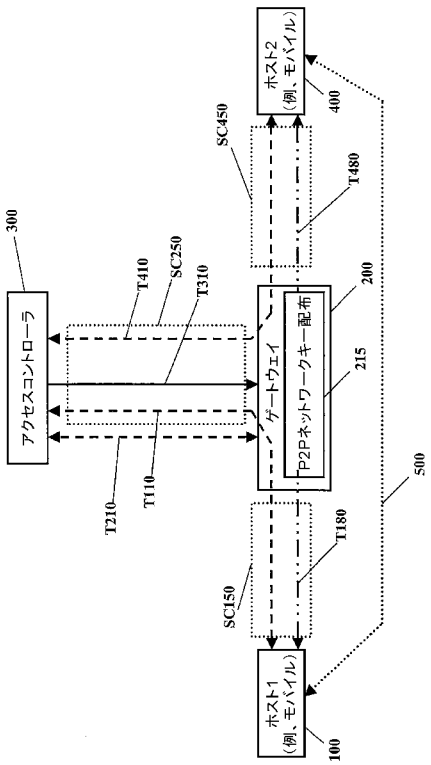
【図５】


セキュアなピアツーピア接続の確立
S410
受信者による通信設定に対する
リクエストメッセージを作成する
S420
セキュアチャネルを介して
リクエストをゲートウェイに送信する
S430
ゲートウェイにおいて
リクエストのコンテンツを処理および確認する
S440
受信者の名前
およびルート、または受信者の
IPアドレスに対するエントリが
あるか？
いいえ
はい
S470
ディスカバリパケットを
作成する
S450
受信者に対する
パケットを作成する
S480
ディスカバリパケットを
ブロードキャストする
S460
パケットを受信者に
ユニキャストする
S490
ユニキャスト/ブロードキャストされたパケットを
受信者において受信する
S500
送信者のセッションキーを
受信者において処理および格納する
S510
ゲートウェイに対する応答を作成し、
セキュアチャネルを介して送信する
A

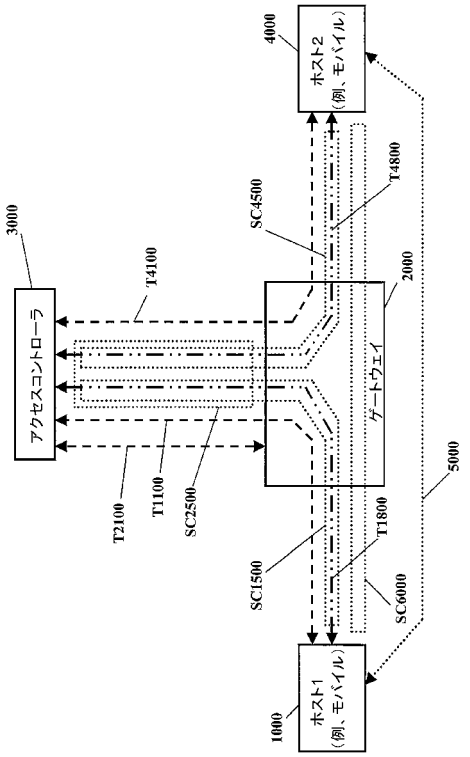
【図６】


A
S520
ゲートウェイにおいて応答を処理する
S530
送信者に対するメッセージを作成し、
セキュアチャネルを介して送信する
S540
送信者においてメッセージのコンテンツを処理し、
受信者のセッションキーを格納する
S550
送信者と受信者との間の
セキュアな双方向性の通信を開始する

【図７】


ホスト2
(例、モバイル)
400
SC450
T480
300
T410
SC250
T310
アクセスコントローラ
ゲートウェイ
200
P2Pネットワークキー配布
215
500
T210
TT110
T180
SC150
ホスト1
(例、モバイル)
100

【図８】


4000
ホスト2
(例、モバイル)
T4800
SC4500
3000
T4100
2000
アクセスコントローラ
ゲートウェイ
5000
T2100
T1100
SC2500
T1800
SC1500
SC6000
1000
ホスト1
(例、モバイル)

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/051336

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 458 151 A (NOKIA CORPORATION) 15 September 2004 (2004-09-15) cited in the application paragraph [0008] - paragraph [0012] paragraph [0023] - paragraph [0034] paragraph [0041] - paragraph [0050]	1-47
P,X	EP 1 650 915 A (ALCATEL) 26 April 2006 (2006-04-26) paragraph [0039] - paragraph [0040]; figure 6	1-47
A	US 2003/087629 A1 (JUITT DAVID ET AL) 8 May 2003 (2003-05-08) paragraph [0009] - paragraph [0016] paragraph [0048] paragraph [0056] - paragraph [0062] paragraph [0069] - paragraph [0071]	1-47

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 September 2006	02/10/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Raposo Pires, João

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2006/051336

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1458151 A	15-09-2004	US 2004179502 A1	16-09-2004
EP 1650915 A	26-04-2006	CN 1764107 A US 2006087999 A1	26-04-2006 27-04-2006
US 2003087629 A1	08-05-2003	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	Ｈ０４Ｑ　7/00　１８２	

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ

Ｆターム(参考)	5J104	AA01	AA07	AA16	BA02	DA03	EA04	EA16	EA17	EA18	KA02
		KA04	NA02	NA37	PA07						
	5K067	AA30	BB04	BB21	DD17	DD57	EE02	EE10	EE16	HH24	HH36