(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4716648号
(P4716648)
(45)発行日　平成23年7月6日(2011.7.6)　(24)登録日　平成23年4月8日(2011.4.8)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330C
H04L 9/32 (2006.01)　　H04L 9/00 673B

請求項の数 4　(全 26 頁)

(21)出願番号　特願2003-125926(P2003-125926)
(22)出願日　平成15年4月30日(2003.4.30)
(65)公開番号　特開2004-30610(P2004-30610A)
(43)公開日　平成16年1月29日(2004.1.29)
審査請求日　平成18年2月27日(2006.2.27)
(31)優先権主張番号　10/134,780
(32)優先日　平成14年4月29日(2002.4.29)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ロヒット　グプタ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ノースイースト　９０　ストリート　１７７８１　アパートメント　ジェイ－１５１

最終頁に続く

(54)【発明の名称】ピアツーピアネットワークにおいてサービス妨害攻撃を抑制する方法

(57)【特許請求の範囲】
【請求項１】
ピアツーピアネットワークにおいて、検索ベースのサービス妨害攻撃を抑制する方法であって、
第１のノードにおいて、第２のノードからＲＥＳＰＯＮＳＥメッセージを受信するステップと、
前記第１のノードにおいて、前記ＲＥＳＰＯＮＳＥメッセージ内のフィールドをハッシュしてビット位置を計算するステップと、
前記第１のノードにおいて、状態情報として維持されているビットベクトルを検査し、前記ビット位置に対応するビットがビットベクトル内にセットされているかどうかを判定して、前記ＲＥＳＰＯＮＳＥメッセージが以前のＲＥＳＯＬＶＥメッセージに対する応答であるかどうかを判定するステップと、
前記ビット位置がセットされておらず、前記ＲＥＳＰＯＮＳＥメッセージが前記以前のＲＥＳＯＬＶＥメッセージに対する応答でないとき、前記第１のノードにおいて、前記ＲＥＳＰＯＮＳＥメッセージを拒絶するステップとを備え、
前記ＲＥＳＰＯＮＳＥメッセージおよび前記ＲＥＳＯＬＶＥメッセージは、前記ＲＥＳＯＬＶＥメッセージのターゲットＩＤと前記ＲＥＳＯＬＶＥメッセージのアドレスリストの少なくとも１つのフィールドを有する状態情報を含み、
前記判定するステップは、解決を妨害する試みにおいて前記ＲＥＳＰＯＮＳＥメッセージの前記フィールドが変更されているかどうかを判定することを含み、

前記拒絶するステップは、解決を妨害する試みにおいて前記ＲＥＳＰＯＮＳＥメッセージの前記フィールドが変更されているとき、前記ＲＥＳＰＯＮＳＥメッセージを拒絶することを特徴とする方法。

【請求項２】

前記ビット位置がセットされていないとき、前記第１のノードにおいて、ビットベクトルの情報を維持するステップであって、該情報は、応答がまだ受信されていない、以前のＲＥＳＯＬＶＥメッセージを識別する情報である、ステップをさらに備えたことを特徴とする請求項１に記載の方法。

【請求項３】

前記解決を妨害する試みにおいて前記ＲＥＳＰＯＮＳＥメッセージの前記フィールドが変更されているかどうかを判定することは、

前記ＲＥＳＰＯＮＳＥメッセージ内の前記アドレスリストのハッシュとしてビット位置を計算するステップと、

ビットベクトルを検査し、前記ビット位置に対応するビットがビットベクトル内にセットされているかどうかを判定するステップと

を備えたことを特徴とする請求項１に記載の方法。

【請求項４】

請求項１に記載の方法を実行するコンピュータ実行可能命令を有することを特徴とするコンピュータ読取り可能記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、一般的にはピアツーピアプロトコルに関し、より詳細には、ピアツーピアプロトコルのためのセキュリティ・フレームワーク・インフラストラクチャに関する。

【０００２】

【従来の技術】

ピアツーピア通信、実際にはすべての種類の通信は、選択されたエンティティ間の有効な接続を確立する可能性に依存する。しかし、エンティティがネットワーク内で移動し、トポロジが変化し、またはアドレス・リース（address lease）を更新することができないために、エンティティは、変動する可能性のある１または複数のアドレスを有することができる。したがって、このアドレス指定問題に対する古典的なアーキテクチャ上の解決策は、各エンティティに安定な名前を割り当て、接続が必要なときにこの名前を現在アドレスに「解決（resolve）」することである。名前からアドレスへの変換は、非常に堅固でなければならず、容易かつ高速な更新も可能でなければならない。

【０００３】

エンティティへの接続を捜すことによって、エンティティのアドレスを見つける可能性を増加させるために、多くのピアツーピアプロトコルは、エンティティが様々な機構を介してエンティティのアドレスを発行することを可能にする。一部のプロトコルは、クライアントが、ネットワーク中の他のエンティティからの要求を処理することによって、他のエンティティのアドレスの知識を獲得することを可能にする。実際、このアドレス知識の獲得により、これらピアツーピアネットワークを首尾よく運用することが可能となる。すなわち、ネットワーク中の他のピアについての情報が良好であるほど、特定のリソースの検索が収束する可能性が高くなる。

【０００４】

しかし、ピアツーピアプロトコルの基礎となる堅固なセキュリティ・インフラストラクチャがなければ、悪意のあるエンティティは、このようなピアツーピアシステムの収束する能力を容易に破壊することができる。このような破壊は、例えば識別情報の盗用に関わるエンティティによって引き起こされる可能性がある。ピアツーピアネットワーク上のこのような識別情報の盗用攻撃において、悪意のあるノードは、許可された関係にない、すなわちその所有者でもグループのメンバなどでもないＩＤについてのアドレス情報を発行す

る。悪意のあるエンティティは、良好なノード応答の前に、最初に傍受および／または応答することができ、したがって良好なノードのように見える。

【０００５】

悪意のあるエンティティは、ネットワークに不良な情報をあふれさせることによってＰＮＲＰ解決を妨害することができ、ネットワーク中の他のエンティティが、存在しないノードに要求を転送する傾向を有し（このことは検索の収束に悪影響を与える）、または攻撃者によって制御されるノードに要求を転送する傾向を有する。このことは、リソースを見つけるために使用するＲＥＳＯＬＶＥパケットを転送する前に変更することによって、またはＲＥＳＯＬＶＥパケットを生成した要求者側に無効なＲＥＳＰＯＮＳＥを返送することによって達成される。悪意のあるエンティティは、例えば、ＩＤが近く検索の収束を助ける、悪意のあるエンティティのキャッシュ内のノードに検索を転送する代わりに、要求されたＩＤから非常に離れたノードに検索を転送することによって、ピアツーピアネットワークのオペレーションを妨害しようと試みることもできる。あるいは、悪意のあるエンティティは、単に検索要求に全く応答しないこともできる。ＰＮＲＰ解決は、有効なＩＤの代わりに無効なＢＹＥメッセージを送信する悪意のあるノードによってさらに妨害される可能性がある。その結果、クラウド（cloud）内の他のノードは、そのノードのキャッシュからこの有効なＩＤを除去し、それらに格納された有効なノードの数が減少する。

【０００６】

アドレス証明書の検証は、識別情報の盗用問題を防止することができるが、ＰＮＲＰ解決を妨害する第２の種類の攻撃に対しては効果がない。攻撃者は、検証可能なアドレス証明書を生成し続け（またはそれを事前に生成し）、対応するＩＤをピアツーピアクラウド内にあふれさせることができる。ノードのいずれかがＩＤの所有権を検証しようと試みる場合、攻撃者は、実際そのノードが、あふれたＩＤの所有者であるので、そのことを検証することができる。しかし、攻撃者が十分なＩＤを生成するならば、攻撃者は、ピアツーピア検索の大部分を、攻撃者により制御されるノードのうちの１つに導くことができる。この点、攻撃者は、ネットワークのオペレーションをかなり制御し、管理することができる。

【０００７】

【発明が解決しようとする課題】

上述した識別情報の盗用問題を防止するために、すべての新しいアドレス情報を最初に検証することをピアツーピアプロトコルが要求する場合に、第３の種類の攻撃を悪意のあるエンティティが利用できるようになる。これら種類のピアツーピアネットワークが影響を受けやすい攻撃は、サービス妨害（ＤｏＳ）攻撃の形式である。新しいレコードについて理解するすべてのノードがＩＤ所有権のチェックを実施しようとする場合に、開示されたＩＤ所有者に対してネットワークアクティビティが殺到する。この弱点を利用して、攻撃者は、非常に一般化されたターゲットに対してＩＰ　ＤｏＳ攻撃を仕掛けることができる。例えば、悪意のあるエンティティが、MicrosoftのウェブＩＰアドレスをＩＤのＩＰとして公示した場合、開示されたＩＰを受信するピアツーピアネットワーク中のすべてのノードは、そのＩＰ（MicrosoftのウェブサーバのＩＰ）に接続してレコードの真性を検証しようとする。もちろん、攻撃者がこの情報を生成したので、MicrosoftのサーバがＩＤの所有権を検証することはできない。しかし、損害は既に生じている。すなわち、攻撃者は、ピアツーピアコミュニティの良好な部分にMicrosoftを攻撃させている。

【０００８】

１または複数のリソースを消耗させることによって、ノードまたはクラウドを圧倒する別の種類のＤｏＳ攻撃は、例えば、ＦＬＯＯＤ／ＲＥＳＯＬＶＥ／ＳＯＬＩＣＩＴパケットを使用することにより、大量の無効／有効ＰＡＣを単一のノードに送信する悪意のあるノードによって仕掛けられる。これらのＰＡＣを受信するノードは、ＰＡＣのすべてを検証しようとして、ノードのすべてのＣＰＵを消費することになる。同様に、無効ＦＬＯＯＤ／ＲＥＳＯＬＶＥパケットを送信することによって、悪意のあるノードは、クラウド内でパケットの増殖を達成する。すなわち、悪意のあるノードは、少数のそのようなパケット

を使用して、ＰＮＲＰクラウド用のネットワーク帯域幅を消費することができる。このパケットの送信先のノードは、追加のパケットを送信することによって応答するからである。ネットワーク帯域幅の増殖は、悪意のあるノードが偽のＲＥＱＵＥＳＴメッセージを送信し、そのＲＥＱＵＥＳＴメッセージに対して、良好なノードがＲＥＱＵＥＳＴよりも大きいサイズのＰＡＣをＦＬＯＯＤすることによって応答することによっても達成される。

【０００９】

悪意のあるノードは、初期ノードのシンクアップ（synch up）を妨害することによってＰＮＲＰクラウドに攻撃を仕掛けることもできる。すなわち、ＰＮＲＰクラウドに加わるために、ノードは、ＰＮＲＰクラウド内の既に存在しているノードのうちの１つに接続しようと試みる。ノードが悪意のあるにノードに接続しようと試みる場合に、ノードは、悪意のあるノードによって完全に制御されてしまう。さらに、悪意のあるノードは、２つの良好なノードが同期プロセスに関係しているとき、無効なＲＥＱＵＥＳＴパケットを送信することができる。無効なＲＥＱＵＥＳＴパケットにより、それに応答してＦＬＯＯＤメッセージの生成が開始されるので、これはシンクアップを妨害する一種のＤｏＳ攻撃である。

【００１０】

したがって、このような攻撃の効果を防止または軽減することによって、Ｐ２Ｐクラウドの保全性を保証するセキュリティ機構が当技術分野で求められている。

【００１１】

【課題を解決するための手段】

本願で開示される発明の概念は、悪意のあるノードがピアツーピアネットワークの通常のオペレーションを妨害することを抑制する、新規で改良された方法を含む。具体的には、本発明は、識別情報の盗用攻撃、サービス妨害攻撃、単にピアツーピアネットワーク中のアドレス解決を妨害しようと試みる攻撃、およびピアツーピアネットワークに加わり、参加する新しいノードの能力を妨害しようと試みる攻撃を含む、悪意のあるノードによって仕掛けられる可能性のある様々な種類の攻撃に対処する方法を提示する。

【００１２】

提示されたセキュリティ・インフラストラクチャおよび方法は、ノードを自己検証型にすることにより、ノードがセキュア識別とインセキュア識別の両方を使用することを可能にする。必要なとき、または適当なときに、既存のメッセージに対する検証を便乗させることにより、または必要であれば小さい紹介メッセージを送信することにより、ＩＤ所有権が検証される。接続先のノードをランダムに選択することにより、悪意のあるノードに最初に接続する確率が減少する。さらに、将来の応答を必要とする以前の通信についての情報を維持することにより、悪意のあるノードからの情報が識別され、それを廃棄することができる。ノードのリソース使用率が所定の限界を超えたときに、ノードが要求を廃棄することを可能にすることにより、サービス妨害攻撃が抑制される。除去されるノードが取消し証明書を署名することを要求することにより、悪意のあるノードが有効ノードを除去する能力は低下する。

【００１３】

本発明の一実施形態によれば、自己検証可能なインセキュアピアアドレス証明書（ＰＡＣ）を生成する方法が提示される。これは、悪意のあるノードが、ピアツーピアネットワーク内のインセキュアＰＡＣにおいて別のノードのセキュア識別を発行することを防止する、この方法は、ピアツーピアネットワーク内で見つけることができるリソースに対するインセキュアＰＡＣを生成するステップを含む。このリソースは、ピアツーピア識別子（ＩＤ）を有する。この方法は、ピアツーピアＩＤが導出されるインセキュアＰＡＣ内に、ユニフォームリソース識別子（ＵＲＩ）を含めるステップをさらに含む。ＵＲＩは、好ましくは、「p2p://URI」のフォーマットである。ピアツーピアＩＤは、インセキュアでもよい。

【００１４】

別の実施形態では、ピアツーピアネットワーク内の第１ノードでピアアドレス証明書を適

当なときに検証する方法が提示される。この第１ノードは、ピアアドレス証明書を格納するために複数レベルのキャッシュを使用し、この方法は、第２ノードから意図的にピアアドレス証明書（ＰＡＣ）を受信するステップと、複数レベルのキャッシュのどのレベルにＰＡＣを格納すべきかを決定するステップとを含む。２つの最低のキャッシュレベルの一方にＰＡＣを格納すべきとき、この方法は、ＰＡＣを保留リストに配置し、検証すべきＰＡＣのＩＤを含むＩＮＱＵＩＲＥメッセージを生成し、ＩＮＱＵＩＲＥメッセージを第２ノードに送信する。２つの最低のキャッシュレベル以外の上位のキャッシュレベルにＰＡＣを格納すべきとき、この方法は、「未検証」としてマークされる上位のキャッシュレベルにＰＡＣを格納する。この場合、ＰＡＣは、それが使用される最初に検証される。この方法は、ＰＡＣを求める証明書チェーンを要求することもできる。

【００１５】

好ましい実施形態では、ＩＮＱＵＩＲＥメッセージの生成は、ＩＮＱＵＩＲＥメッセージに含めるべきトランザクションＩＤを生成するステップを含む。ＩＮＱＵＩＲＥメッセージに応答して第２ノードからＡＵＴＨＯＲＩＴＹメッセージが受信されたとき、ＰＡＣは、保留リストから除去され、２つの最低のキャッシュレベルの一方に格納される。証明書チェーンが要求された場合、ＡＵＴＨＯＲＩＴＹメッセージが検査され、証明書チェーンが存在し、かつ有効であるかどうかが判定される。そうである場合に、ＰＡＣは、２つの最低のキャッシュレベルの一方に格納され、そうでない場合に、ＰＡＣは削除される。本発明の実施形態では、ＡＵＴＨＯＲＩＴＹメッセージが以前の通信に対する応答であることを保証するためにトランザクションＩＤを使用することもできる。

【００１６】

本発明の別の実施形態では、悪意のあるノードに接続する確率が減少するようにピアツーピアネットワーク内のノードを見つける方法が提示される。この方法は、ピアツーピアネットワーク内で、ローカルに登録されたＩＤを含めずに発見メッセージを同報通信するステップと、ピアツーピアネットワーク内のノードから応答を受信するステップと、ノードとピアリング関係を確立するステップとを含む。一実施形態では、ノードから応答を受信するステップは、ピアツーピアネットワーク内の少なくとも２つのノードから応答を受信するステップを含む。この状況では、ノードとピアリング関係を確立するステップは、少なくとも２つのノードの一方をランダムに選択するステップと、少なくとも２つのノードのうちランダムに選択された一方とピアリング関係を確立するステップとを含む。

【００１７】

本発明のさらに別の実施形態では、ピアツーピアネットワーク内の同期プロセスに基づくサービス妨害攻撃を抑制する方法が提示される。この方法は、キャッシュ同期を要求する、ピアアドレス証明書（ＰＡＣ）を含むＳＯＬＩＣＩＴメッセージ要求を第１ノードから受信するステップと、ＰＡＣを検査して、ＰＡＣの有効性を判定するステップと、ＰＡＣを検査するステップが、ＰＡＣが有効でないと判定したとき、ＳＯＬＩＣＩＴパケットを除去するステップとを含む。好ましくは、ＰＡＣを検査するステップが、ＰＡＣが有効であると判定したとき、この方法は、ナンス（nonce）を生成するステップと、ナンスを第１ノードの公開鍵で暗号化するステップと、暗号化ナンスを含むＡＤＶＥＲＴＩＳＥメッセージを生成するステップと、ＡＤＶＥＲＴＩＳＥメッセージを第１ノードに送信するステップとをさらに含む。ＲＥＱＵＥＳＴメッセージが第１ノードから受信されたとき、この方法は、ＲＥＱＵＥＳＴメッセージを検査して、第１ノードが暗号化ナンスを暗号化解除することができたかどうかを判定し、第１ノードが暗号化ナンスを暗号化解除することができたとき、ＲＥＱＵＥＳＴメッセージを処理する。

【００１８】

好ましくは、この方法は、第１ノードとの通信を具体的に識別する接続情報を維持するステップと、ＲＥＱＵＥＳＴメッセージを検査し、ＲＥＱＵＥＳＴメッセージが具体的にＡＤＶＥＲＴＩＳＥメッセージと関係することを保証するステップと、ＲＥＱＵＥＳＴメッセージが具体的にＡＤＶＥＲＴＩＳＥメッセージと関係しないとき、ＲＥＱＵＥＳＴメッセージを拒絶するステップとをさらに含む。一実施形態では、第１ノードとの通信を具体

的に識別する接続情報を維持するステップは、ナンスおよび第１ノードの識別のハッシュとして第１ビット位置を計算するステップと、ビットベクトル中の第１ビット位置でビットをセットするステップとを含む。これを行ったとき、ＲＥＱＵＥＳＴメッセージを検査するステップは、ＲＥＱＵＥＳＴメッセージからナンスおよび第１ノードの識別を抽出するステップと、ナンスおよび第１ノードの識別のハッシュとして第２ビット位置を計算するステップと、ビットベクトルを検査し、ビットベクトルが第２ビット位置に対応するビットセットを有するかどうかを判定するステップと、ビットベクトルを検査するステップで第２ビット位置に対応するビットセットが見つからないとき、ＲＥＱＵＥＳＴがＡＤＶＥＲＴＩＳＥメッセージに具体的に関係しないことを示すステップとを含む。あるいは、ナンスをビット位置として直接的に使用することもできる。この場合、ＲＥＱＵＥＳＴが受信されたとき、同封のナンスに対応するビット位置がチェックされる。このビット位置がセットされている場合、これは有効なＲＥＱＵＥＳＴであり、ビット位置がクリアされる。そうでない場合、これは無効なＲＥＱＵＥＳＴまたは応答攻撃であり、このＲＥＱＵＥＳＴは廃棄される。

【００１９】

本発明のさらに別の実施形態では、ピアツーピアネットワーク内の同期プロセスに基づくサービス妨害攻撃を抑制する方法は、第１ノードから意図的に要求メッセージを受信するステップと、ＲＥＱＵＥＳＴメッセージが第１ノードとの以前の通信に対する応答であるかどうかを判定するステップと、ＲＥＱＵＥＳＴメッセージが第１ノードとの以前の通信に対する応答でないとき、ＲＥＱＵＥＳＴメッセージを拒絶するステップとを含む。好ましくは、ＲＥＱＵＥＳＴメッセージが以前の通信に対する応答であるかどうかを判定するステップは、ＲＥＱＵＥＳＴメッセージから、第１ノードのナンスおよび識別を意図的に抽出するステップと、ナンスおよび識別のハッシュとしてビット位置を計算するステップと、ビットベクトルを検査し、ビットベクトルがビット位置に対応するビットセットを有するかどうかを判定するステップと、ビット位置に対応するビットセットが存在しないとき、ＲＥＱＵＥＳＴが第１ノードとの以前の通信の応答ではないことを示すステップとを含む。

【００２０】

ピアツーピアネットワーク内のノードリソースの消費に基づくサービス妨害攻撃を抑制する方法も提示される。この方法は、ピアツーピアネットワーク内のノードからメッセージを受信するステップと、現在のリソース使用率を検査するステップと、現在のリソース使用率が所定のレベルを超えているとき、メッセージの処理を拒絶するステップとを含む。ＲＥＳＯＬＶＥメッセージが受信されたとき、メッセージの処理を拒絶するステップは、ＡＵＴＨＯＲＩＴＹメッセージを第１ノードに送信するステップを含む。このＡＵＴＨＯＲＩＴＹメッセージは、現在のリソース使用率が高過ぎるためにＲＥＳＯＬＶＥメッセージが処理されないことの表示を含む。ピアアドレス証明書（ＰＡＣ）を含むＦＬＯＯＤメッセージが受信され、かつＰＡＣを２つの最低のキャッシュレベルの一方に格納すべきであることをこの方法が決定したとき、メッセージの処理を拒絶するステップは、後の処理のために保留リスト内にＰＡＣを配置するステップを含む。２つの最低のキャッシュレベルよりも高いキャッシュレベルにＰＡＣを格納すべきであることをこの方法が決定した場合には、メッセージの処理を拒絶するステップは、ＦＬＯＯＤメッセージを拒絶するステップを含む。

【００２１】

本発明の別の実施形態では、ピアツーピアネットワーク内のノード帯域幅消費に基づくサービス妨害攻撃を抑制する方法が提示される。この方法は、ピアツーピアネットワーク内のノードからキャッシュ同期を求める要求を受信するステップと、過去に実施されたキャッシュ同期の数を示すメトリック（metric）を検査するステップと、過去に実施されたキャッシュ同期の数が所定の最大値を超えているとき、キャッシュ同期を求める要求の処理を拒絶するステップとを含む。別の実施形態では、この方法はメトリックを検査し、所定の先行期間に実施されたキャッシュ同期の数を判定する。この実施形態では、要求の処理

を拒絶するステップは、所定の先行期間に実施されたキャッシュ同期の数が所定の最大値を超えているとき、キャッシュ同期を求める要求の処理を拒絶するステップを含む。

【００２２】

本発明の別の実施形態では、ピアツーピアネットワーク内の検索ベースのサービス妨害攻撃を抑制する方法は、既知のピアアドレス証明書のキャッシュエントリを検査し、解決要求を送信する適切なノードを決定するステップと、適切なノードのうち１つをランダムに選択するステップと、ランダムに選択したノードに解決要求を送信するステップとを含む。一実施形態では、適切なノードのうち１つをランダムに選択するステップは、ターゲットＩＤからのＰＮＲＰ　ＩＤの距離に基づいて、適切なノードごとに、重み付けした確率を計算するステップを含む。特定の次のホップを選ぶ確率は、そのノードとターゲットノードの間のＩＤ距離に対する反比例として決定される。

【００２３】

本発明の別の実施形態では、ピアツーピアネットワーク内の検索ベースのサービス妨害攻撃を抑制する方法は、ＲＥＳＰＯＮＳＥメッセージを受信するステップと、ＲＥＳＰＯＮＳＥメッセージが以前のＲＥＳＯＬＶＥメッセージに対する応答であるかどうかを判定するステップと、ＲＥＳＰＯＮＳＥメッセージが以前のＲＥＳＯＬＶＥメッセージに対する応答でないとき、ＲＥＱＵＥＳＴメッセージを拒絶するステップとを含む。好ましくは、ＲＥＳＰＯＮＳＥメッセージが以前のＲＥＳＯＬＶＥメッセージに対する応答であるかどうかを判定するステップは、ＲＥＳＰＯＮＳＥメッセージ内の情報のハッシュとしてビット位置を計算するステップと、ビットベクトルを検査し、ビット位置に対応するビットがビットベクトル内にセットされているかどうかを判定するステップとを含む。

【００２４】

一実施形態では、ＲＥＳＰＯＮＳＥメッセージはアドレスリストを含み、この方法は、解決を妨害する試みにおいてＲＥＳＰＯＮＳＥメッセージが変更されているかどうかを判定するステップと、解決を妨害する試みにおいてＲＥＳＰＯＮＳＥメッセージが変更されているとき、ＲＥＳＰＯＮＳＥメッセージを拒絶するステップとをさらに含む。好ましくは、解決を妨害する試みにおいてＲＥＳＰＯＮＳＥメッセージが変更されているかどうかを判定するステップは、ＲＥＳＰＯＮＳＥメッセージ内のアドレスリストのハッシュとしてビット位置を計算するステップと、ビットベクトルを検査し、ビット位置に対応するビットがビットベクトル内にセットされているかどうかを判定するステップとを含む。

【００２５】

本発明の別の実施形態では、悪意のあるノードがピアツーピアネットワークから有効ノードを除去することを抑制する方法は、キャッシュ内に格納されたピアアドレス証明書（ＰＡＣ）を有する有効ノードから、取消し証明書を意図的に受信するステップと、取消し証明書が有効ノードによって署名されていることを検証するステップとを含む。

【００２６】

本明細書に含まれ、本明細書の一部を形成する添付の図面は、本発明のいくつかの態様と、本発明の原理を説明するのに用いるための開示とを示す。

【００２７】

【発明の実施の形態】

ある好ましい実施形態に関連して本発明を説明するが、本発明をその実施形態に限定することを意図するものではない。むしろ、すべての代替方法、修正形態、および均等物が、頭記の特許請求の範囲で定義される本発明の精神および範囲内に含まれるものとする。

【００２８】

図面を参照すると、同様の参照符号は同様の要素を指しており、本発明が、適切なコンピューティング環境に実装されているものとして示されている。必須ではないが、パーソナルコンピュータによって実行中の、プログラムモジュールなどのコンピュータ実行可能命令の一般的文脈で本発明を説明する。一般に、プログラムモジュールは、特定のタスクを実行し、または特定の抽象データ種類を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。さらに、ハンドヘルド装置、マルチプロセッサ

システム、マイクロプロセッサベースの消費者向け電子機器またはプログラマブル消費者向け電子機器、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータなどを含む他のコンピュータシステム構成を用いて本発明を実施できることを当業者は理解されよう。本発明はまた、通信ネットワークを介してリンクされるリモート処理装置によってタスクが実行される分散コンピューティング環境でも実施することができる。分散コンピューティング環境では、プログラムモジュールは、ローカルメモリ記憶装置とリモートメモリ記憶装置のどちらにも位置することができる。

【００２９】

図１に、本発明を実装することができる適切なコンピューティング環境１００の例を示す。例示的コンピューティング環境１００は、適切なコンピューティング環境の一例に過ぎず、本発明の使用および機能の範囲に関して何らかの制限を示唆するものではない。例示的動作環境１００に図示する構成要素のうちのいずれか１つ、あるいはそれらの組合せに関係する何らかの依存関係または要件をコンピューティング環境１００が有するものと解釈すべきでもない。

【００３０】

本発明は、他の多数の汎用コンピューティングシステム環境または構成、あるいは他の多数の特殊目的コンピューティングシステム環境または構成で動作可能である。本発明と共に使用するのに適した周知のコンピューティングシステム、環境、および／または構成の例には、限定はしないが、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルド装置またはラップトップ装置、マルチプロセッサシステム、マイクロプロセッサベースのシステム、セットトップボックス、プログラマブル消費者向け電子機器、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、ならびに上記のシステムまたは装置のいずれかを含む分散コンピューティング環境などが含まれる。

【００３１】

本発明は、コンピュータによって実行中の、プログラムモジュールなどのコンピュータ実行可能命令の一般的文脈で説明することができる。一般に、プログラムモジュールは、特定のタスクを実施し、または特定の抽象データ種類を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。本発明はまた、通信ネットワークを介してリンクされるリモート処理装置によってタスクが実行される分散コンピューティング環境でも実施することができる。分散コンピューティング環境では、プログラムモジュールは、メモリ記憶装置を含む、ローカルコンピュータ記憶媒体とリモートコンピュータ記憶媒体のどちらにも位置することができる。

【００３２】

図１を参照すると、本発明を実装するための例示的システムは、コンピュータ１１０の形式の汎用コンピューティング装置を含む。コンピュータ１１０の構成要素は、限定はしないが、処理装置１２０と、システムメモリ１３０と、システムメモリを含む様々なシステム構成要素を処理装置１２０に結合するシステムバス１２１とを含むことができる。システムバス１２１は、様々なバスアーキテクチャのうちのいずれかを用いる、メモリバスまたはメモリコントローラと、周辺バスと、ローカルバスとを含むいくつかの種類のバス構造のうちのいずれでもよい。例えば、限定はしないが、このようなアーキテクチャには、ＩＳＡ（Industry Standard Architecture）バス、ＭＣＡ（Micro Channel Architecture）バス、ＥＩＳＡ（Enhanced ISA）バス、ＶＥＳＡ（Video Electronics Standards Association）ローカルバス、およびメザニンバスとも呼ばれるＰＣＩ（Peripheral Component Interconnect）バスが含まれる。

【００３３】

コンピュータ１１０は、一般に様々なコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータ１１０がアクセス可能である入手可能などんな媒体でもよく、それには揮発性媒体と不揮発性媒体の両方、取外し可能媒体と取外し不能媒体の両方が含まれる。例えば、限定はしないが、コンピュータ可読媒体はコンピュータ記憶媒体および通信媒体を含むことができる。コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、

プログラムモジュール、または他のデータなどの情報を格納するための何らかの方法または技術で実装される、揮発性媒体と不揮発性媒体、取外し可能媒体と取外し不能媒体のどちらも含む。コンピュータ記憶媒体には、限定はしないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、または他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤ（digital versatile disk）、または他の光記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置、または他の磁気記憶装置、あるいは、所望の情報を格納するのに使用することができ、コンピュータ１１０でアクセスすることができる他のどんな媒体も含まれる。通信媒体は一般に、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータを、搬送波または他の移送機構などの被変調データ信号で実施し、その通信媒体にはどんな情報送達媒体も含まれる。「被変調データ信号」という用語は、その特徴のうちの１または複数を有する信号、または情報を符号化するように変化する信号を意味する。例えば、限定はしないが、通信媒体には、ワイヤードネットワークまたはダイレクトワイヤード接続などのワイヤード媒体、ならびに音響媒体、ＲＦ媒体、赤外線媒体、および他のワイヤレス媒体などのワイヤレス媒体が含まれる。上記のいずれかの組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。

【００３４】

システムメモリ１３０は、読取り専用メモリ（ＲＯＭ）１３１およびランダムアクセスメモリ（ＲＡＭ）１３２などの揮発性メモリおよび／または不揮発性メモリの形態のコンピュータ記憶媒体を含む。始動中などにコンピュータ１１０内の要素間で情報を転送する助けになる基本ルーチンを含む基本入出力システム（ＢＩＯＳ）１３３が、一般にＲＯＭ１３１内に記憶される。ＲＡＭ１３２は、一般に、処理装置１２０に即座にアクセス可能であり、かつ／または処理装置１２０が現在操作しているデータおよび／またはプログラムモジュールを含む。例えば、限定はしないが、図１に、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７を示す。

【００３５】

コンピュータ１１０は、他の取外し可能／取外し不能な、揮発性／不揮発性コンピュータ記憶媒体も含むことができる。単なる一例であるが、図１に、取外し不能不揮発性磁気媒体を読み書きするハードディスクドライブ１４１と、取外し可能不揮発性磁気ディスク１５２を読み書きする磁気ディスクドライブ１５１と、ＣＤ－ＲＯＭまたは他の光媒体などの取外し可能不揮発性光ディスク１５６を読み書きする光ディスクドライブ１５５とを示す。例示的動作環境で使用することのできる他の取外し可能／取外し不能な揮発性／不揮発性コンピュータ記憶媒体には、限定はしないが、磁気テープカセット、フラッシュメモリカード、デジタルバーサタイルディスク、デジタルビデオテープ、固体ＲＡＭ、および固体ＲＯＭが含まれる。ハードディスクドライブ１４１は一般に、インタフェース１４０などの取外し不能メモリインタフェースを介してシステムバス１２１に接続され、磁気ディスクドライブ１５１および光ディスクドライブ１５５は、インタフェース１５０などの取外し可能メモリインタフェースによってシステムバス１２１に接続される。

【００３６】

上述した、図１に図示するドライブとその関連するコンピュータ記憶媒体は、コンピュータ１１０に対してコンピュータ可読命令データ構造、データ構造、プログラムモジュール、および他のデータの記憶を実現する。例えば図１では、ハードディスクドライブ１４１がオペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７を格納するものとして図示している。これらの構成要素は、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７と同じにすることも、異なるものにすることもできることに留意されたい。オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７には、少なくともこれらが相異なるコピーであることを示すために異なる符号を付けてある。ユーザは、キーボード１６２や、マウス、トラックボール、

またはタッチパッドと一般に呼ばれるポインティングデバイス１６１などの入力装置を介して、コマンドおよび情報をコンピュータ１１０に入力することができる。他の入力装置（図示せず）には、マイクロフォン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナなどを含めることができる。これらの入力装置や他の入力装置はしばしば、システムバスに結合されるユーザ入力インタフェース１６０を介して処理装置１２０に接続されるが、パラレルポート、ゲームポート、またはユニバーサルシリアルバス（ＵＳＢ）などの他のインタフェースおよびバス構造によって接続することもできる。モニタ１９１または他の種類のディスプレイ装置もまた、ビデオインタフェース１９０などのインタフェースを介してシステムバス１２１に接続される。モニタに加えて、コンピュータはまた、スピーカ１９７およびプリンタ１９６などの他の周辺出力装置も含むことができ、その周辺出力装置は、出力周辺インタフェース１９５を介して接続することができる。

【００３７】

コンピュータ１１０は、リモートコンピュータ１８０などの１または複数のリモートコンピュータへの論理接続を使用して、ネットワーク環境で動作することができる。リモートコンピュータ１８０は、別のパーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピア装置、または他の共通ネットワークノードでよく、一般にコンピュータ１１０に関して上記で述べた要素のうちの多くまたはすべてを含むが、図１にはメモリ記憶装置１８１だけを示してある。図１に示す論理接続は、ローカルエリアネットワーク（ＬＡＮ）１７１および広域ネットワーク（ＷＡＮ）１７３を含むが、他のネットワークも含めることができる。このようなネットワーキング環境は、オフィス、企業全体のコンピュータネットワーク、イントラネット、およびインターネットで一般的なものである。

【００３８】

ＬＡＮネットワーキング環境で使用する際、パーソナルコンピュータ１１０は、ネットワークインタフェースまたはアダプタ１７０を介してＬＡＮ１７１に接続される。ＷＡＮネットワーキング環境で使用する際、コンピュータ１１０は一般に、インターネットなどのＷＡＮ１７３を介して通信を確立するためのモデム１７２または他の手段を含む。モデム１７２は内蔵でも外付けでもよく、ユーザ入力インタフェース１６０、または他の適切な機構を介してシステムバス１２１に接続することができる。ネットワーク環境では、コンピュータ１００に関して示したプログラムモジュールまたはその一部を、リモートメモリ記憶装置内に格納することができる。例えば、限定はしないが、図１に、リモートアプリケーションプログラム１８５をメモリ装置１８１上に常駐するものとして示す。図示するネットワーク接続は例示的なものであって、コンピュータ間の通信リンクを確立する他の手段も使用できることを理解されたい。

【００３９】

以下の説明では、別段の表示がない限り、１または複数のコンピュータによって実行される動作と、オペレーションの象徴的表現とを参照しながら本発明を説明する。したがって、このような動作およびオペレーションは、コンピュータで実行される動作およびオペレーションと呼ばれることもあり、構造化形式のデータを表す電気信号の、コンピュータの処理装置による操作を含むことを理解されよう。この操作は、データを変換し、またはデータをコンピュータのメモリシステム内の位置に維持し、このデータは、当業者の理解する方式でコンピュータのオペレーションを再構成し、あるいは変更する。データを維持するデータ構造は、データのフォーマットによって定義される特定の特性を有するメモリの物理位置である。しかし、上記の状況で本発明を説明するものの、当業者は理解するであろうが、以下で説明する様々な動作およびオペレーションをハードウェアでも実装できることを制限することを意味するわけではない。

【００４０】

上述したように、ピアツーピア（Ｐ２Ｐ）プロトコルの成功は、選択されたエンティティ間の有効な接続を確立するプロトコルの能力に依存する。特定のユーザは、異なるアドレスを有する様々な位置で、様々な方式でネットワークに接続することができるので、好ましい手法は、ユーザに対して固有の識別を割り当て、次にプロトコルを介してその識別を

特定のアドレスに変換することである。Peer-To-Peer Name Resolution Protocol (PNRP) And Multilevel Cache For Use Therewithという名称の２００１年８月２９日出願の同時係属出願第０９／９４２１６４号には、本発明のセキュリティ・インフラストラクチャの特定の適用範囲が見出されるＰＮＲＰが記載されている。この同時係属出願の教示および開示全体を参照により組み込む。しかし、本発明のセキュリティ・インフラストラクチャおよび方法が、この同時係属出願の特定のピアツーピアプロトコルに限定されず、他のプロトコルにも等しい効力で適用できることを、以下の教示から当業者は理解されよう。

【００４１】

上記で組み込んだ同時係属出願で論じられているように、ＰＮＲＰは、ピアベースの名前－アドレス解決プロトコルである。名前は、ＰＮＲＰ　ＩＤと呼ばれる２５６ビットの数である。アドレスは、ＩＰｖ４アドレスまたはＩＰｖ６アドレス、ポート、ならびにプロトコル番号からなる。ＰＮＲＰ　ＩＤがアドレスに変換されるとき、ピアアドレス証明書（ＰＡＣ）が返される。この証明書は、ターゲットのＰＮＲＰ　ＩＤ、現ＩＰアドレス、公開鍵、およびその他の多くのフィールドを含む。ＰＮＲＰプロトコルのインスタンスは、ノードと呼ばれる。ノードは、ローカルに登録された１または複数のＰＮＲＰ　ＩＤを有することができる。ノードは、登録を介してＰＮＲＰで見つけることができるＩＤ－アドレスマッピングを作成する。各登録は、ローカルに構築されたピア証明書を含み、ＰＮＲＰキャッシュの適切なビューを必要とする。ＰＮＲＰノードではないホストは、ＰＮＲＰ　ＤＮＳゲートウェイを介してＰＮＲＰ　ＩＤをＩＰアドレスに変換することができる。ＰＮＲＰ　ＤＮＳゲートウェイは、ＤＮＳ「Ａ」および「ＡＡＡＡ」照会を受諾し、指定のホスト名のサブセットを求めるＰＮＲＰ検索を実行し、結果をＤＮＳ照会回答として返す。

【００４２】

上述したように、ＰＮＲＰは、Ｐ２ＰおよびＰＮＲＰ　ＩＤをピアアドレス証明書（ＰＡＣ）と関連付けるピアベースの機構を提供する。Ｐ２Ｐ　ＩＤは、永続的な１２８ビット識別子である。Ｐ２Ｐ　ＩＤは、正しくフォーマットされたＰ２Ｐ名をハッシングすることによって作成される。Ｐ２Ｐ　ＩＤには、セキュアとインセキュアの２つの種類がある。セキュアＰ２Ｐ　ＩＤは、公開鍵と検証可能な関係を有するＩＤである。インセキュアＰ２Ｐ　ＩＤは、セキュアでない任意のＩＤである。所与のＰ２Ｐ　ＩＤは、多くの異なるノードによって発行することができる。ＰＮＲＰは、発行される各インスタンスが固有のＰＮＲＰ　ＩＤを有することを保証するために、「サービス位置」サフィックスを使用する。「サービス位置」は、固有ネットワークサービスエンドポイントに対応する１２８ビットの数である。サービス位置は、いくつかの認識可能な要素を有するが、ＰＮＲＰクライアントからは不透明とみなされるべきである。サービス位置は、２つの重要な特性を有する。どの時点でも、クラウド内の１つのソケットだけが所与のサービス位置に対応する。２つのサービス位置を比較したとき、各サービス位置についての共通プレフィックスの長さは、ネットワークの近さの妥当な指標である。同一の４ビットで始まる２つのサービス位置は、同一の３ビットで始まる２つのサービス位置よりも遠くに離れていない。

【００４３】

Ｐ２Ｐ　ＩＤは、サービス位置との連鎖によって一意的に識別される。得られる２５６ビット（３２バイト）識別子は、ＰＮＲＰ　ＩＤと呼ばれる。ＰＮＲＰノードは、Ｐ２Ｐ名、権限、およびその他のいくつかのパラメータを用いてＰＮＲＰサービスを起動することによってＰＮＲＰ　ＩＤを登録する。ＰＮＲＰサービスは、提供されたデータを含むピアアドレス証明書（ＰＡＣ）を作成し、維持する。ＰＡＣは少なくとも、ＰＮＲＰ　ＩＤ、証明書有効期間、サービスアドレスおよびＰＮＲＰアドレス、公開鍵、ならびに選択ＰＡＣ内容を介して生成された暗号署名を含む。

【００４４】

ＰＮＲＰ　ＩＤの作成および登録は、ＰＮＲＰサービスの一部に過ぎない。ＰＮＲＰサービス実行は、４つの段階に分割することができる。第１段階は、ＰＮＲＰクラウドディスカバリである。この段階の間に、新しいノードは、加わりたいと望むクラウド内の既存の

ノードを見つけなければならない。クラウドは、グローバルＰＮＲＰクラウド、サイトローカル（企業）クラウド、リンクローカルクラウドとすることができる。見つかった後、ＰＮＲＰクラウドに加わるについての第２段階に入る。新しいノードが既存のノードを見つけた後、新しいノードはＳＹＮＣＨＲＯＮＩＺＥ手順を実施し、既存のノードトップキャッシュレベルのコピーを得る。単一のキャッシュレベルにより、新しいノードがクラウドに参加することを開始するための十分の基礎が与えられる。ＳＹＮＣＨＲＯＮＩＺＡＴＩＯＮを達成した後、次の段階であるクラウドへのアクティブな参加を開始することができる。初期化を完了した後、ノードは、ＰＮＲＰ　ＩＤ登録およびＰＮＲＰ　ＩＤ解決に参加することができる。この段階の間、ピアは定期的なキャッシュの保守を実施する。ノードが終了したとき、ノードは第４段階に入り、クラウドを離れる。ノードは、ローカルに登録した任意のＰＮＲＰ　ＩＤを登録解除し、次いで終了する。

【００４５】

ＰＮＲＰプロトコルは、９個の異なる種類のパケットからなる。その一部は上述した。しかし、本願では、パケットの名前は、単にパケットの機能を理解しやすくするために使用しているのであって、パケットの名前を、パケットの形式またはフォーマット、あるいはメッセージ自体を制限するものとみなすべきでないことに留意されたい。ＲＥＳＯＬＶＥパケットは、ターゲットＰＮＲＰ　ＩＤをＰＡＣに変換することを要求する。ＲＥＳＯＰＮＳＥパケットは、完了したＲＥＳＯＬＶＥ要求の結果である。ＦＬＯＯＤパケットは、受信側のＰＮＲＰキャッシュのためのＰＡＣを含む。ＳＯＬＩＣＩＴパケットは、ＰＮＲＰノードのトップレベルキャッシュをＡＤＶＥＲＴＩＳＥするようＰＮＲＰノードに依頼するために使用される。要求されるＡＤＶＥＲＴＩＳＥパケットは、ノードのトップレベルキャッシュ内のＰＡＣに関するＰＮＲＰ　ＩＤのリストを含む。ＲＥＱＵＥＳＴパケットは、ＡＤＶＥＲＴＩＳＥされたＰＡＣのサブセットをフラッディングするようにノードに依頼するために使用される。ＩＮＱＵＩＲＥパケットは、特定のＰＮＲＰ　ＩＤがそのノードに登録されたかどうかをインセキュアにノードに問い合わせるのに使用される。ＰＮＲＰ　ＩＤのローカル登録を確認するために、ＡＵＴＨＯＲＩＴＹパケットが使用される。このパケットは、任意選択で、そのＩＤに関するＰＡＣを検証する助けとなるように証明書チェーンを提供する。ＡＣＫパケットは、あるメッセージの受信、および／または処理の成功を確認する。最後に、ＲＥＰＡＩＲパケットは、分割されている可能性のあるクラウドをマージするよう試みるために使用される。

【００４６】

ノードが完全に開始された後、ノードは、５つの種類のアクティビティを実施することによってＰＮＲＰクラウドに参加することができる。第１に、ノードは、ＰＮＲＰ　ＩＤを登録および登録解除することができる。ＰＮＲＰ　ＩＤを登録するとき、ＰＮＲＰサービスは、ＰＮＲＰ　ＩＤ、サービスアドレスポートおよびプロトコル、ＰＮＲＰアドレスポートおよびプロトコル、ならびに公開鍵を関連付けるピアアドレス証明書（ＰＡＣ）を作成する。このＰＡＣは、ローカルキャッシュに入り、ＲＥＳＯＬＶＥを、新しいＰＡＣをソースとして使用し、かつ［ＰＮＲＰ　ＩＤ＋１］をターゲットとして使用して開始する。このＲＥＳＯＬＶＥは、登録されるＩＤと非常に類似したＰＮＲＰ　ＩＤを有するいくつかのノードによって処理される。ＲＥＳＯＬＶＥの各受信側は、新しいノードのＰＡＣをそれぞれのキャッシュに追加し、それによってクラウド内で新しいＰＮＲＰＩＤを公示する。ＰＮＲＰ　ＩＤを登録解除するとき、更新後のＰＡＣは、「取消し」フラグセットを用いて作成される。更新後のＰＡＣは、ローカルキャッシュの最低レベルにおけるすべてのエントリにフラッディングされる。ＦＬＯＯＤの各受信側は、ＰＡＣのバージョンが古いかについて、それぞれのキャッシュをチェックする。そのようなキャッシュが見つかった場合、受信側は、受信側のキャッシュからＰＡＣを除去する。ＰＡＣが最低のキャッシュレベルから除去される場合、受信側は、受信側の最低のキャッシュレベルにおけるその他のすべてのＰＡＣによって提示されるＰＮＲＰノードに対して取消しをＦＬＯＯＤする。

【００４７】

ＰＮＲＰノードは、ＰＮＲＰ　ＩＤ解決に参加することもできる。上記で組み込んだ出願に論じられているように、ＰＮＲＰ　ＩＤは、ターゲットＰＮＲＰ　ＩＤに近づくように、次々にＲＥＳＯＬＶＥメッセージを経路指定することによってＰＡＣに変換される。ノードがＲＥＳＯＬＶＥを受信したとき、ノードは、ＲＥＳＯＬＶＥを拒否して以前のホップに戻し、以前のホップにＲＥＳＰＯＮＳＥで応答し、またはＰＮＲＰ　ＩＤがノード自体よりもターゲットＩＤに近いノードにＲＥＳＯＬＶＥを転送することができる。ノードは、ＲＥＳＰＯＮＳＥパケットを解決の一部として受信し、転送する。ＰＮＲＰノードは、ローカルクライアントの代わりにＲＥＳＯＬＶＥＳを開始することができる。ＰＮＲＰサービスは、非同期の解決要求が可能となるようにＡＰＩを提供する。ローカルノードは、ＲＥＳＯＬＶＥパケットを生成し、対応するＲＥＳＰＯＮＳＥを最終的に受信する。

【００４８】

ＰＮＲＰノードは、キャッシュ同期要求を受ける。ＳＯＬＩＣＩＴパケットを受信する際、ノードは、ＰＮＲＰ　ＩＤを最高キャッシュレベル中にリストするＡＤＶＥＲＴＩＳＥパケットで応答する。次に、ソリシターノード（solicitor node）は、ＡＤＶＥＲＴＩＳＥされた望みのＰＡＣに関するＰＮＲＰ　ＩＤをリストする要求を送信する。ＲＥＱＵＥＳＴされた各キャッシュエントリは、ＲＥＱＵＥＳＴ側にＦＬＯＯＤされる。最後に、以下により十分に論じるように、ＰＮＲＰは、識別の検証も実施する。識別の検証は、ＰＡＣを検証するのに使用する脅威を軽減する装置である。識別の検証は、基本的に２つの目的を有する。第１に、識別の検証は、ＰＡＣで指定されるＰＮＲＰノードが、ローカルに登録されたそのＰＡＣからのＰＮＲＰ　ＩＤを有することを保証する。第２に、セキュアＰＮＲＰ　ＩＤの場合（以下で論じる）、識別の検証は、ＰＮＲＰ　ＩＤにおける権限に対して暗号的に実証可能な関係を有する鍵を使用して、ＰＡＣが署名されたことを保証する。

【００４９】

ここまで、本発明のセキュリティ・インフラストラクチャの実施形態と特定の関連性が見出されるＰＮＲＰシステムの実際に役立つ知識を与えたので、ここで、本発明のセキュリティ・インフラストラクチャによって提供されるセキュリティ機構に注意を向ける。これらの機構は、上述したようなＰ２Ｐクラウドにおいて悪意のあるノードによってもたらされる可能性のある様々な攻撃の効果をなくし、または少なくとも緩和するために、本発明のシステムによって提供される。ＰＮＲＰプロトコルは、これらの攻撃を防止する機構を有さず、これら脅威のすべてに対処する単一の解決策があるわけでもない。しかし、本発明のセキュリティ・インフラストラクチャは、悪意のあるノードによって引き起こされる可能性のある破壊を最小にし、かつ、ＰＮＲＰプロトコロルに組み込むことができる。

【００５０】

成功している多くのＰ２Ｐプロトコルの場合と同じく、容易に見つけることができるようにエンティティを発行することができる。しかし、Ｐ２Ｐプロトコルに対してセキュリティおよび保全性を実現するために、各識別は、添付の識別証明書を含むことが好ましい。しかし、堅固なセキュリティアーキテクチャは、セキュアエンティティとインセキュアエンティティのどちらも扱うことができる。本発明の実施形態によれば、この堅固性は、自己検証型ＰＡＣを使用することによって実現される。

【００５１】

セキュアＰＡＣは、ＩＤと公開鍵との間のマッピングを提供することによって自己検証型にされる。これにより、セキュアＰＡＣに署名するための秘密鍵を有することなく誰かがそのＰＡＣを発行することが防止され、したがって、多くの識別の盗用攻撃が防止される。ＩＤ秘密鍵の保持者は、証明書を使用して、ＩＰアドレス、フレンドリネームなどの追加の情報をＩＤに添付する。好ましくは、各ノードは、ノード自体の秘密鍵－公開鍵対を生成し、信頼されるサプライヤが提供することもできる。公開鍵は、ノード識別子の一部として含められる。その１対の鍵を作成したノードだけが、ノード識別の作成者であることを証明することができる秘密鍵を有する。このようにして、識別の盗用を見つけることができ、したがってそれを防止することができる。

【００５２】
このような証明書に関する汎用フォーマットは、[Version, ID, <ID Related Info>, Validity, Algorithms, P_{Issuer}]K_{Issuer}と表すことができる。実際、セキュアＩＤであるか、それともインセキュアＩＤであるかに関わらず、Ｐ２Ｐ名／ＵＲＬは、基本的な証明書フォーマットの一部である。この証明書の表現で使用しているように、Versionは、証明書のバージョンであり、ＩＤは、発行すべき識別子であり、<ID Related Info>は、ＩＤと関連付けるべき情報を表し、Validityは、世界日時（別名ＧＭＴ）として表される１対のFrom-To dateで表される有効期間を表し、Algorithmsは、鍵の対を生成し、署名するのに使用するアルゴリズムを指し、P_{Issuer}は、証明書発行者の公開鍵である。証明書発行者がＩＤ所有者と同じである場合、これは、ＩＤ所有者の公開鍵P_{ID}である。項K_{Issuer}は、P_{Issuer}に対応する秘密鍵である。証明書発行者がＩＤ所有者である場合、これは、ＩＤ所有者の秘密鍵K_{ID}である。

【００５３】
好ましい実施形態では、<ID related info>は、このＩＤを見つけることができるアドレスタプルと、発行者のＰＮＲＰサービスに関するアドレスタプルを含む。この実施形態では、アドレス証明書は、[Version, ID, $<Address>_{ID}$, $<Address>_{PNRP}$, Validity, Revoke Flag, Algorithms, P_{Issuer}]K_{Issuer}となる。この拡張された表現では、ＩＤは発行すべき識別子であり、Group IDまたはPeer IDでよい。<Address>は、ＩＰｖ６アドレス、ポート、およびプロトコルのタプルである。$<Address>_{ID}$は、IDに関連付けるべきアドレスタプルである。$<Address>_{PNRP}$は、発行者のマシンにおけるＰＮＲＰサービス（または他のＰ２Ｐサービス）のアドレスタプルである。これは、発行者のＰＮＲＰアドレスのアドレスであることが好ましい。これは、証明書の有効性を検証するために、他のＰＮＲＰノードによって使用される。Validityは、１対のFrom-To dateで表される有効期間を表す。取消しフラグは、セットされたとき取消し証明書をマークする。P_{Issuer}は、証明書発行者の公開鍵であり、K_{Issuer}は、P_{Issuer}に対応する秘密鍵である。証明書発行者がＩＤ所有者である場合、これは、ＩＤの秘密鍵K_{ID}である。

【００５４】
本発明の好ましい実施形態では、証明書が有効であるためには以下の条件を満たさなければならない。証明書署名が有効でなければならず、証明書は満了することができない。すなわち、ＵＤＴとして表される現在の日付は、Validityフィールドで指定される範囲内になければならない。公開鍵のハッシュもまた、ＩＤと一致しなければならない。発行者がＩＤ所有者と同じである場合、発行者の公開鍵の、ＩＤへのハッシングを検証しなければならない。P_{Issuer}がP_{ID}と異なる場合、K_{ID}で署名された証明書に導く証明書のチェーンが存在しなければならない。このようなチェーンにより、発行者とＩＤ所有者との間の関係が検証される。加えて、証明取消しリスト（ＣＲＬ）が、ＩＤのそのクラスに関して発行され、ＣＲＬがアクセス可能である場合、オーセンティケータは、チェーン中の証明書がＣＲＬ内に出現しないことを検証することができる。

【００５５】
本発明のセキュリティ・インフラストラクチャはまた、インセキュアＰＡＣも扱う。本発明によれば、インセキュアＰＡＣは、ＩＤの導出元のユニフォームリソース識別子（ＵＲＩ）を含めることによって自己検証型となる。実際、セキュアＩＤとインセキュアＩＤはどちらも、ＰＡＣ内にＵＲＩを含む。ＵＲＩは、「p2p://URI」というフォーマットである。これにより、悪意のあるノードが、インセキュアＰＡＣで別のノードのセキュアＩＤを発行することが防止される。

【００５６】
本発明のセキュリティ・インフラストラクチャは、インセキュアＩＤの使用も可能にする。このようなインセキュアＩＤに伴う問題は、偽造が非常に容易であることである。悪意のあるノードは、他の任意のノードのインセキュアＩＤを発行することができる。インセキュアＩＤは、良好なノードの発見を困難にすることが可能となるセキュリティホールも開く。しかし、本発明に従ってＵＲＩを含めることにより、インセキュアＩＤは、決して

セキュアＩＤに影響を及ぼすことがない。さらに、本発明のインフラストラクチャにより、インセキュアＩＤを含むＰＡＣが、セキュアＰＡＣと同じフォーマットとなることが必要となる。すなわち、これらは公開鍵と秘密鍵を含む。セキュアＰＡＣに対する構造と同じ構造をインセキュアＰＡＣに対して実施することにより、ＰＡＣを生成するためのバー（bar）は低下しない。さらに、ＰＡＣ内にＵＲＩを含めることにより、特定のセキュアＩＤにマッピングするＵＲＩを生成することは、計算上実現不可能となる。

【００５７】

ここで生じる１つの問題は、Ｐ２Ｐクラウドセキュリティの向上とオーバヘッドの増加との兼ね合いを認識した上で、ＰＡＣをいつ検証するかということである。しかし、上述した様々なパケットに含まれるＰＡＣは、ある時点で検証しなければならない。このＰＡＣ検証は、ＩＤの署名が有効かどうかをチェックすること、およびＩＤがセキュアＩＤについての公開鍵に対応するかどうかをチェックすることを含む。オーバヘッドとセキュリティの問題の平衡をとるため、本発明の一実施形態では、そのパケットのどんな処理を行うよりも前にＰＡＣを検証する。これにより、無効データは決して処理されないことが保証される。しかし、ＰＡＣ検証がパケットの処理を低下させる可能性があり、そのことは、あるクラスのパケット、例えばＲＥＳＯＬＶＥパケットには適さないことを認識して、本発明の代替実施形態ではこのパケット中のＰＡＣを検証しない。

【００５８】

ＰＡＣの検証に加えて、本発明のセキュリティ・インフラストラクチャはまた、ＩＤ所有権のチェックを実施してＰＡＣを検証する。上述したように、個人情報の盗用は、ＰＮＲＰまたは他のＰ２Ｐプロトコルでアドレスを使用する前に、そのアドレス証明書の単純な検証によって見つけることができる。この検証は、ＩＤが、証明書に含まれる公開鍵のハッシュであることを単に検証することを伴うことがある。所有権の検証は、そのＰＡＣ中のアドレスにＩＮＱＵＩＲＥパケットを発行することも伴う。ＩＮＱＵＩＲＥパケットは、検証すべきＩＤと、トランザクションＩＤを含む。ＩＤがそのアドレスに存在する場合、ノードはそのＩＮＱＵＩＲＥを確認すべきである。ＩＤがそのアドレスに存在しない場合、ノードはそのＩＮＱＵＩＲＥを確認すべきではない。識別を検証するのに証明書チェーンが必要である場合、ノードは、完全な証明書チェーンを返す。供給される証明書チェーンにおける承認のチェーンを検証するのと同様に、署名およびＩＤ－＞ＵＲＬの検証は、依然として複雑であり、本発明のシステムは、ＰＡＣの検証に追加の複雑さを加えることになるあらゆるチャレンジ／応答プロトコルを回避する。さらに、トランザクションＩＤを含めることにより、悪意のあるノードがＩＮＱＵＩＲＥＳに対する応答を事前生成することを防止する。加えて、この機構は、ＰＡＣが完全な証明書チェーンを搬送するという要件が不要となる。

【００５９】

標準ＲＥＳＯＬＶＥパケットを変更することにより、本発明のシステムにおいて、ＩＤ所有権チェックを容易にし、標準ＲＥＳＯＬＶＥパケットがＩＤ所有権チェックも実施することができるようにする。変更されたＲＥＳＯＬＶＥパケットは、ＲＥＳＯＬＶＥの転送先アドレスのＩＤを含む。ＩＤがそのアドレスにある場合はＡＣＫを送信し、そうでない場合はＮＡＣＫを送信する。ＩＤがＲＥＳＯＬＶＥを処理しない場合、またはＮＡＣＫが受信される場合、ＩＤはキャッシュから除去される。このようにして、ある種のチャレンジ／応答プロトコルに頼ることなしに、特別などんなＩＮＱＵＩＲＥパケットも送信することなく、本質的には、ＩＮＱＵＩＲＥメッセージをＲＥＳＯＬＶＥに便乗させることによってＰＡＣを検証する。この便乗プロセスを、図２に参照して以下で再度論じる。この手順により、無効なＰＡＣ、または古いＰＡＣを見つけることが容易になる。

【００６０】

この識別検証チェックは、２つの相異なる時刻に行われる。最初は、ノードが、ノードの最低の２つのキャッシュレベルの一方にＰＡＣを加えようとしているときである。最低の２つのキャッシュレベルにおけるＰＡＣ有効性は、ＰＮＲＰＩＤを変換するＰＮＲＰの能力にとって重要である。これらの２つのレベルの一方にＰＡＣを加える前に、識別検証を

実施することにより、いくつかの攻撃が軽減される。ＰＡＣをより高位のレベルのキャッシュに加えるべき場合、これらの高位レベルでは入替りがあるために、ＩＤ所有権は実施されない。キャッシュの高位レベルのすべてのＰＡＣエントリのほぼ８５％は、それが使用される前に置換され、または有効期限が切れることが確認されている。したがって、これらの高位レベルに無効ＰＡＣを有することによる何らかの効果を確認する確率は、無効ＰＡＣが入ったときにＩＤ検証を実施することが正当化されないほどに十分低い。

【００６１】

エントリが最低の２つのキャッシュレベルの一方に属すると判定されるとき、ＰＡＣは、その識別を検証することができるまで、保留リスト内に配置される。この第１種の識別検証は、ＩＮＱＵＩＲＥメッセージを使用する。このような識別検証は、ＰＡＣがその発信側ノードで依然として有効である（登録されている）ことを確認し、発信側ノードの検証権限がそのＰＡＣを発行する助けになる情報を要求する。ＩＮＱＵＩＲＥメッセージ中の１つのフラグは、ＡＵＴＨＯＲＩＴＹ応答内の証明書チェーン（それが存在する場合）を送信するように受信側に要求する「フラグ」フィールド、すなわちＲＦ＿ＳＥＮＤ＿ＣＨＡＩＮに対して定義される。ＩＮＱＵＩＲＥの受信側がＰＡＣを発行する権限を有さない場合、またはＰＡＣがもはやローカルに登録されていない場合、受信側は単にＩＮＱＵＩＲＥメッセージを除去する。ローカルノードがＡＵＴＨＯＲＩＴＹメッセージを介して適切な応答を受信しないので、不良なＰＡＣは、そのキャッシュ内に決して入らず、したがって、Ｐ２Ｐクラウドにおけるオペレーションに対して悪意のある効果を有さないようにすることができる。

【００６２】

ＩＮＱＵＩＲＥの受信側がＰＡＣを発行する権限を有し、および依然としてローカルに登録されている場合、そのノードは、図２に示すように、ＡＵＴＨＯＲＩＴＹメッセージでＩＮＱＵＩＲＥメッセージに応答する（２００）。図２には示していないが、本発明の実施形態での受信側ノードは、ＡＵＴＨＯＲＩＴＹを送信したノードでＩＤが依然として登録されているとＡＵＴＨＯＲＩＴＹメッセージが示すか否かを確認するためにチェックする。ローカルノードが、このＡＵＴＨＯＲＩＴＹメッセージがＩＮＱＵＩＲＥに対する応答であると判定した後（２０２）、ローカルノードは、保留リストからＰＡＣを除去する（２０４）。証明書チェーンが要求された場合（２０６）、証明書チェーンが存在し、有効であるかどうかを確認するためにＡＵＴＨＯＲＩＴＹメッセージをチェックする（２０８）。証明書チェーンが存在し、有効である場合、ＰＡＣがキャッシュに追加され、有効なものとしてマークされる（２１０）。そうでない場合、ＰＡＣは削除される（２１２）。証明書チェーンが要求されなかった場合（２０６）、単にＰＡＣがキャッシュに追加され、有効なものとしてマークされる（２１０）。

【００６３】

今や明らかであろうが、このＡＵＴＨＯＲＩＴＹメッセージは、ＰＮＲＰ　ＩＤが依然としてローカルノードに登録されていることを確認または否定するのに使用され、任意選択で、このＡＵＴＨＯＲＩＴＹメッセージは、ＡＵＴＨＯＲＩＴＹ受信側がノードの権利を検証してターゲットＩＤに対応するＰＡＣを発行することを可能にする証明書チェーンを提供する。ＩＮＱＵＩＲＥメッセージに加えて、ＡＵＴＨＯＲＩＴＹメッセージは、以下に論じるようにＲＥＳＯＬＶＥメッセージに対する適切な応答でよい。ＡＵＴＨＯＲＩＴＹメッセージは、否定的応答を示すために受信側ノードがセットすることができる様々なフラグを含む。このような１つのフラグは、ＲＥＳＯＬＶＥに対する応答においてのみ有効であるＡＦ＿ＲＥＪＥＣＴ＿ＴＯＯ＿ＢＵＳＹフラグである。このフラグは、ホストが非常にビジーであるためにＲＥＳＯＬＶＥを受諾することができないことを示し、送信側に、処理のためにＲＥＳＯＬＶＥを別のところに転送すべきであることを伝える。識別検証では助けとはならないが、以下でより完全に論じるように、このフラグは、ＤｏＳ攻撃を防止するための本発明の別のセキュリティ機構である。フラグＡＦ＿ＩＮＶＡＬＩＤ＿ＳＯＵＲＣＥは、ＲＥＳＯＬＶＥに対する応答においてのみ有効であり、ＲＥＳＯＬＶＥ内のＳｏｕｒｃｅ　ＰＡＣが無効であることを示す。ＡＦ＿ＩＮＶＡＬＩＤ＿ＢＥＳＴ＿

ＭＡＴＣＨフラグは、ＲＥＳＯＬＶＥに対する応答においてのみ有効であり、ＲＥＳＯＬＶＥ内の「最良マッチ」ＰＡＣが無効であることを示す。ＡＦ＿ＵＮＫＮＯＷＮ＿ＩＤフラグは、指定された「検証」ＰＮＲＰ　ＩＤがこのホストで登録されていないことを示す。ＡＵＴＨＯＲＩＴＹメッセージ内の他のフラグは、要求された情報が含まれていることを受信側ノードに示す。ＡＦ＿ＣＥＲＴ＿ＣＨＡＩＮフラグは、「検証」ＰＮＲＰ　ＩＤと、そのＰＡＣに署名するのに使用する公開鍵との関係を検証することを可能にする証明書チェーンが含まれていることを示す。ＡＵＴＨＯＲＩＴＹメッセージは、ＩＮＱＵＩＲＥメッセージまたはＲＥＳＯＬＶＥメッセージのどちらかに対する確認／応答としてのみ送信される。ＡＵＴＨＯＲＩＴＹがこの状況外で受信される場合、ＡＵＴＨＯＲＩＴＹは廃棄される。

【００６４】

識別検証が実施される第２のときは、ＲＥＳＯＬＶＥプロセスの間の適当なときに実施される。上述したように、ＰＮＲＰキャッシュは、高速に入れ替わる。したがって、キャッシュ内の大部分のキャッシュエントリは、それが使用される前に上書きされる。したがって、本発明のセキュリティ・インフラストラクチャは、これらのＰＡＣが実際に使用されるまで、かつ実際に使用されない限り、これらのＰＡＣを検証しない。ＰＡＣを使用してＲＥＳＯＬＶＥ経路を経路指定するとき、本発明のシステムは、上述したＲＥＳＯＬＶＥパケットに加えて識別検証を便乗させる。ＲＥＳＯＬＶＥは、ＩＮＱＵＩＲＥパケット中の「ターゲットＩＤ」と同様に扱われる「次のホップ」ＩＤを含む。次に、ＲＥＳＯＬＶＥは、上述したＩＮＱＵＩＲＥに対して予想されるのと同様に、ＡＵＴＨＯＲＩＴＹパケットを用いて確認される。適当なときの識別検証が失敗した場合、ＲＥＳＯＬＶＥの受信側は、送信側が受信側であると信じるものではない。したがって、ＲＥＳＯＬＶＥは別のところに経路指定され、無効ＰＡＣがキャッシュから除去される。

【００６５】

このプロセスもまた図２に示す。ＰＮＲＰノードＰが、ＲＥＳＯＬＶＥをセットする（２０２）ヘッダのMessage Typeフィールドを有するＡＵＴＨＯＲＩＴＹパケットを受信するとき（２００）、上述したように、受信側ノードは、ＡＵＴＨＯＲＩＴＹフラグを検査し、このＡＵＴＨＯＲＩＴＹフラグが否であるかどうかを判定する（２１４）。ＡＵＴＨＯＲＩＴＹメッセージに、否定的な応答フラグのいずれかがセットされている場合、ＰＡＣをキャッシュから削除し、ＲＥＳＯＬＶＥを別のところに経路指定する（２１６）。ＲＥＳＯＬＶＥの送信先のアドレスをＲＥＳＯＬＶＥ経路に追加し、ＲＥＪＥＣＴＥＤとマークする。次に、ＲＥＳＯＬＶＥを新しい宛先に転送する。ＡＵＴＨＯＲＩＴＹが否でなく、かつ証明書チェーンが要求された場合（２１８）、ＡＵＴＨＯＲＩＴＹメッセージフラグＡＦ＿ＣＥＲＴ＿ＣＨＡＩＮをチェックし、証明書チェーンが存在するかどうかを確認する。証明書チェーンが存在する場合、受信側ノードは、検証で指定されたＰＮＲＰ　ＩＤに関するキャッシュされたＰＡＣに対するチェーン検証オペレーションを実施すべきである。チェーンをチェックして、チェーン内のすべての証明書が有効であり、かつチェーンのルートとリーフの間の関係が有効であることを保証すべきである。チェーンルートに関する公開鍵のハッシュは、少なくとも、ＰＡＣのＰ２Ｐ名での権限と比較して、確実にそれらがマッチするようにすべきである。チェーンリーフに関する公開鍵は、ＰＡＣを署名するのに使用する鍵と比較して、確実にそれらが一致するようにすべきである。これらのチェックのいずれかが失敗し、または要求時に証明書チェーンが存在しない場合（２２０）、キャッシュ２２２からＰＡＣを除去し、ＲＥＳＯＬＶＥを再処理すべきである。要求された証明書チェーンが含まれており、かつ検証された場合（２２０）、検証ＰＮＲＰ　ＩＤに対応するＰＡＣを、完全に検証したものとしてマークすべきである（２２４）。望むなら、ＰＮＲＰ　ＩＤ、ＰＮＲＰサービスアドレス、および検証時間を、ＰＡＣから保持することができ、ＰＡＣ自体は、メモリを節約するためにキャッシュから削除することができる。

【００６６】

この識別検証の一例として、ＰがＰＮＲＰ　ＩＤ「Ｔ」に関する識別検証を要求するノー

ドであると仮定する。Ｎが、識別検証要求を受信するノードである。このことは、ターゲットＩＤ＝ＴのＩＮＱＵＩＲＥパケット、または次のホップ＝ＴであるＲＥＳＯＬＶＥパケットのどちらかを受信するＰの結果として生じる可能性がある。Ｎは、ローカルに登録されたＰＮＲＰ　ＩＤのリストをチェックする。Ｔがそのリスト中に存在しない場合、受信したパケットの種類をチェックする。パケット種類がＩＮＱＵＩＲＥであった場合、Ｎは暗黙のうちにＩＮＱＵＩＲＥ要求を除去する。通常の再送信の試行が満了した後、Ｐは、ＰＡＣを無効なものとして廃棄し、処理は終了する。パケット種類がＲＥＳＯＬＶＥであった場合、Ｎは、ＩＤ　Ｔがローカルに登録されていないことを示すＡＵＴＨＯＲＩＴＹパケットで応答する。次に、Ｐは、ＲＥＳＯＬＶＥを別のところに送信する。ＴがＮのＰＮＲＰ　ＩＤのリスト中に存在する場合、Ｎは、ＡＵＴＨＯＲＩＴＹパケットを構築し、ターゲットＩＤをＴにセットする。Ｔがインセキュアドである場合、Ｎは、ＡＵＴＨＯＲＩＴＹパケットをＰに送信する。Ｔがセキュアドであり、かつセキュアＩＤに関する権限が、ＰＡＣに署名するのに使用する鍵である場合、ＮはＡＵＴＨＯＲＩＴＹパケットをＰに送信する。これらのどれも真ではなく、かつＲＦ＿ＳＥＮＤ＿ＣＨＡＩＮフラグがセットされている場合、Ｎは、ＰＮＲＰ　ＩＤ　Ｔに関する権限に対してＰＡＣに署名するのに使用する鍵に関する証明書チェーンを取り出す。証明書チェーンは、ＡＵＴＨＯＲＩＴＹパケットに挿入され、Ｎは、ＡＵＴＨＯＲＩＴＹパケットをＰに送信する。この点で、Ｔがインセキュアドである場合、処理は完了する。そうでない場合、Ｐは、ＰＡＣに署名する鍵と、ＰＮＲＰ　ＩＤ　Ｔを生成するのに使用する権限との関係を検証する。検証が失敗した場合、ＰＡＣを廃棄する。検証が失敗し、かつ開始メッセージがＲＥＳＯＬＶＥであった場合、Ｐは、別のところにＲＥＳＯＬＶＥを転送する。

【００６７】

ここで識別所有権検証を２回実施したことから今や理解するであろうが、ＩＮＱＵＩＲＥパケット、または修正後のＲＥＳＯＬＶＥパケットにより、ＦＬＯＯＤを使用してＰ２Ｐクラウド全体にわたって無効ＰＡＣを一般化することができず、検索は、存在しないＩＤまたは無効なＩＤに転送されない。ＦＬＯＯＤパケットが検証なしにネットワーク中を伝播することが可能である場合、ＦＬＯＯＤパケットがＤｏＳ攻撃を引き起こす可能性があるので、ＦＬＯＯＤに対してＰＡＣ検証が必要である。これらの機構により、一般ノードのＩＤが非常に少数のノードの最低の２つのキャッシュレベルのみに属することになるので、一般ノードがＩＤ所有権チェックでフラッディングを受けることはない。

【００６８】

上述した同時係属出願により完全に記載されているように、ＰＮＲＰノードＮは、４つの方式のうちの１つにより、新しいＩＤについて認識する。ＰＮＲＰノードＮは、近隣のキャッシュの初期フラッディングによって新しいＩＤを認識することができる。具体的には、Ｐ２Ｐノードが浮上するとき、Ｐ２Ｐノードは、Ｐ２Ｐクラウドの別のノードメンバと接触し、キャッシュ同期シーケンスを開始する。Ｐ２Ｐノードは、近隣がその最低のキャッシュの新しいレコードをフラッディングする結果として、新しいＩＤを認識することができる。例えば、ノードＮがノードＭの最低レベルのキャッシュ内のエントリとして出現すると仮定する。Ｍが新しいＩＤについて認識するとき、ＩＤがＭの最低レベルのキャッシュと適合する場合、Ｍは、そのキャッシュレベル内の他のエントリと、ＮにそのＩＤをそれぞれフラッディングする。ノードは、検索要求の結果として新しいＩＤを認識することができる。検索要求の発信元は、要求内に発信元のアドレス証明書を挿入し、検索要求に対する「最良マッチ」のＰＡＣもまた、そのＰＡＣを要求内に挿入する。このようにして、検索要求経路に沿うノードのすべては、検索発信元のアドレス、および最良マッチのアドレスでノードのキャッシュを更新することになる。同様に、ノードは、検索応答の結果として新しいＩＤを認識することができる。検索要求の結果は、要求経路のサブセットを逆の順序で移動する。この経路に沿うノードは、検索結果でノードのキャッシュを更新する。

【００６９】

ＰＮＲＰによれば、ノードが最初に浮上するとき、ノードは近隣を見つける。しかし、上

述したように、最初に見つかったノードが悪意のあるノードである場合、その新しいノードは、悪意のあるノードによって制御される可能性がある。このような発生の可能性を防止し、または最小にするため、本発明のセキュリティ・インフラストラクチャは、セキュアノードブートアップを保証するための２つの機構を提供する。第１の機構は、ランダム化されたディスカバリである。ノードが、そのノードがＰＮＲＰクラウドに加わることを可能にする別のノードを見つけようと試みるとき、見つけるための最後の選択肢は、マルチキャスト／同報通信を使用することである。マルチキャスト／同報通信は、最もインセキュアなＰＮＲＰの発見方法だからである。ディスカバリの性質のために、良好なノードと不良なノードとを区別することが非常に難しい。したがって、このマルチキャスト／同報通信方法が必要なとき、本発明のセキュリティ・インフラストラクチャは、同報通信ディスカバリ（ＭＡＲＣＯＰＯＬＯまたは既存のマルチキャストディスカバリプロトコル。例えばＳＳＤＰ）メッセージに応答したノードのうちの１つを、ノードにランダムに選択させる。ランダムなノードを選択することにより、本発明のシステムは、不良なノードを選択する確率を最小にする。本発明のシステムは、そのＩＤのいずれも使用せずにこのディスカバリを実施する。ディスカバリ中にＩＤを使用しないことにより、本発明のシステムは、悪意のあるノードが特定のＩＤをターゲットにすることを防止する。

【００７０】

ノードがその間にビットベクトルを維持する修正された同期段階により、第２のセキュアノードブートアップ機構が提供される。修正された同期段階機構は、図３の単純化した流れ図に示す例により、最もよく理解できる。アリス２２６が、アリス２２６のＰＡＣが含まれるＳＯＬＩＣＩＴ　２２８をボブ２３０に送信すると仮定する。アリスのＰＡＣが有効でない場合（２３２）、ボブ２３０は、単にＳＯＬＩＣＩＴ　２３４を除去する。ＰＡＣが有効である場合、ボブ２３０は、この接続の状態を格納するためにビットベクトルを維持する。このＳＯＬＩＣＩＴを受信したとき、ボブ２３０は、ナンスを生成し、それをアリスのＰＮＲＰ　ＩＤでハッシュする（２３６）。得られる数は、ボブがセットするこのビットベクトルの索引として使用される。次に、ボブ２３０は、ＡＤＶＥＲＴＩＳＥメッセージでアリス２２６に応答する（２３８）。このＡＤＶＥＲＴＩＳＥは、他の情報とは別にアリスの公開鍵で暗号化されたボブのＰＡＣおよびナンスを含み、ボブ２３０によって署名される。アリス２２６がこのＡＤＶＥＲＴＩＳＥを受信したとき、アリス２２６は、署名およびボブのＰＡＣを検証する（２４０）。それを検証することができない場合、除去される（２４１）。それを検証することができる場合、アリス２２６は、ナンスを暗号化解除する（２４２）。次に、アリス２２６は、このナンスおよびアリスのＰＮＲＰ　ＩＤを含むＲＥＱＵＥＳＴを生成する（２４４）。ボブ２３０は、ＲＥＱＵＥＳＴパケットで送信されたナンスでアリスのＰＮＲＰ　ＩＤをハッシングすることによって、このＲＥＱＵＥＳＴを処理する（２４６）。ハッシングされた結果を索引として有するビットベクトルにビットがセットされている場合（２４８）、ボブは、ビットをクリアし、ＲＥＱＵＥＳＴの処理を開始する（２５０）。そうでない場合、ＲＥＱＵＥＳＴは応答攻撃である可能性があるので、ボブは、ＲＥＱＵＥＳＴを無視する（２５２）。

【００７１】

これにより、シーケンスを再生することができないので、ノードブートアップは、セキュアプロセスになる。これにより、ＣＰＵ、ネットワークポート、およびネットワークトラフィックを含む、消費されるリソースの点で、必要なオーバヘッドが最小となる。状態情報に対して維持すべきタイマは不要であり、シンクアップを開始したＩＤだけが送信データとなる。実際、修正された同期段階は、非同期であり、それにより、ノードが複数のＳＯＬＩＣＩＴを同時に処理することが可能となる。

【００７２】

パケットを処理する速度を制御し、すなわちノードリソース消費を制限することにより、上述した脅威の多くを最小にすることができる。この背後にある考えは、ノードは、ＰＮＲＰパケットを処理しようとするノードのＣＰＵを１００％消費すべきでないということである。したがって、本発明の実施形態によれば、あるメッセージの処理が、ノードが効

果的に機能することを妨害するとノードが検出したとき、ノードは、そのようなメッセージの処理を拒絶することができる。

【００７３】

処理しないとノードが判断することができるそのような１つのメッセージは、別のノードから受信したＲＥＳＯＬＶＥメッセージである。図４に、このプロセスを単純化した形で示す。ＲＥＳＯＬＶＥメッセージを受信した後（２５４）、ノードは、所定の限界を超えるＣＰＵ能力でノードが現在動作しているかどうかをチェックする（２５６）。ノードのＣＰＵが非常にビジーであるためにＲＥＳＯＬＶＥメッセージを処理することができない場合、ノードは、ノードが非常にビジーであるために要求を処理することに失敗したことを示すＡＦ＿ＲＥＪＥＣＴ＿ＴＯＯ＿ＢＵＳＹフラグセットを有するＡＵＴＨＯＲＩＴＹメッセージを送信する（２５８）。ＣＰＵがそれほどビジーではない場合（２５６）、ノードは、ＲＥＳＯＬＶＥメッセージ内のＰＡＣのすべてが有効であるかどうかを判定し（２６０）、いずれかが無効であることが判明した場合、メッセージを拒絶する（２６２）。ＰＡＣのすべてが有効である場合（２６０）、ノードはＲＥＳＯＬＶＥを処理する（２６４）。

【００７４】

ノードがＲＥＳＯＬＶＥに応答することができる場合（２６６）、ノードはＲＥＳＯＬＶＥをＲＥＳＰＯＮＳＥに変換し、それをＲＥＳＯＬＶＥの送信元のノードに送信する（２６８）。しかし、ターゲットＩＤがローカルに登録されていない場合、ノードはＲＥＳＯＬＶＥ内のフィールドのハッシュとしてビット位置を計算し、対応するビット位置をビットベクトルにセットする（２７０）。上記で簡潔に論じたように、このビットベクトルは、応答が期待されるどんなメッセージもノードが送信していないときに、誤り応答メッセージの処理を防止するためのセキュリティ機構として使用される。ノードは、ノードがメッセージを処理したことを証明する適切な変更と共にＲＥＳＯＬＶＥを転送する次のホップを見つける。ＲＥＳＯＬＶＥを転送すべき転送先のノードが既に検証されている場合（２７２）、ノードは単に、ＲＥＳＯＬＶＥをその次のホップに転送する（２７６）。この選択された次のホップがまだ検証されていない場合（２７２）、ノードは、ＲＥＳＯＬＶＥにＩＤ所有権要求を便乗させ（２７４）、それをそのノードに転送する（２７６）。便乗させたＩＤ所有権要求に応答して、ノードは、上述したようにＡＵＴＨＯＲＩＴＹメッセージを受信することを期待する。そのプロセスを図２に示す。図２に示すように、ステップ２１４で検証ＡＵＴＨＯＲＩＴＹが受信されていない場合、ＲＥＳＯＬＶＥが転送されたノードのＰＡＣがキャッシュから削除され（２１６）、ＲＥＳＯＬＶＥが図４のステップ２５４から再処理される。

【００７５】

ノードのＣＰＵが非常にビジーであるためにノードが処理しないと判断することができる別のメッセージは、ＦＬＯＯＤメッセージである。図５に単純化した形で示すこのプロセスでは、ＦＬＯＯＤ中に存在する新しい情報が最低の２つのキャッシュレベルの一方に進んだ場合（２７８）、ＰＡＣをチェックして、ＰＡＣが有効であるかどうかを判定する（２８０）。ＰＡＣが有効でない場合、ＦＬＯＯＤを拒絶する（２８４）。しかし、ＰＡＣが有効である場合（２８０）、ＰＡＣを保留リストに入れる（２８２）。保留リスト中のエントリは、ランダムな間隔でとられ、ＣＰＵがそれほどビジーでないときに処理される。これらのエントリがキャッシュの最低の２つのレベルに入ろうとしているので、上述したように、ＩＤ検証と所有権検証が共に実施される。ＦＬＯＯＤ中に存在する新しい情報がより高いキャッシュレベルに進み（２７８）、かつＣＰＵが非常にビジーでそれを処理することができない場合（２８６）、それは廃棄される（２８８）。ノードが利用可能なＣＰＵ処理能力を有する場合（２８６）、ＰＡＣをチェックし、それが有効であるかどうかを判定する（２９０）。有効である場合、ＰＡＣをキャッシュに追加し（２９２）、そうでない場合ＦＬＯＯＤを拒絶する（２９４）。

【００７６】

ノードブートアップ（ＳＹＮＣＨＲＯＮＩＺＥ）は、ＣＰＵ処理能力だけでなく、ネット

ワーク帯域幅も含むかなりのリソースをノードで消費する別のプロセスである。しかし、新しいノードがＰ２Ｐクラウドに完全に参加することを可能にするためには、同期プロセスが必要である。したがって、ノードが所与の時間に利用可能なリソースを十分に有する場合、ノードは、ブートアップを求める別のノードの要求に応答する。すなわち、これまで議論した２つのメッセージと同様に、ノードのＣＰＵ稼働率が非常に高い場合、ノードは、ブートアップへの参加を拒絶することができる。しかし、このプロセスは非常に多くの能力を消費するので、悪意のあるノードが、多数のこのようなシーケンスを立ち上げることにより、依然としてこのプロセスを利用する可能性がある。したがって本発明のセキュリティ・インフラストラクチャの実施形態は、この攻撃を防止するために、所与のノードによって処理することができるノード同期の数を制限する。加えて、この制限を時間限定とすることができ、その結果、悪意のあるノードは、このような同期を将来再び実施できないようにノードを使用不能にすることができない。

【００７７】

悪意のあるノードによって立ち上げられ、または引き起こされる可能性のある多数の検索ベースの攻撃を上述した。このような検索ベースの攻撃の効果をなくし、または最小にするため、本発明のシステムは２つの機構を提供する。第１の機構はランダム化である。すなわち、ノードが、検索要求（ＲＥＳＯＬＶＥ）の転送先の適切な次のホップを検索しているとき、ノードは、いくつかの可能な候補ノードを識別し、次に、これらの候補ＩＤから、ＲＥＳＯＬＶＥの転送先となる１つのＩＤをランダムに選択する。一実施形態では、ランダムな選択のために３つの候補ノードが識別される。ＩＤは、全ランダム化の代替方法として、重み付けした確率に基づいて選択することができる。ＩＤが悪意のないノードに属することの重み付けした確率を計算する１つの方法は、ターゲットＩＤからのＰＮＲＰ　ＩＤの距離に基づく。次に、そのノードとターゲットノードとの間のＩＤ距離の反比例として確率が決定される。いずれにしても、このランダム化により、悪意のあるノードにＲＥＳＯＬＶＥ要求を送信する確率が減少する。

【００７８】

検索ベースの攻撃に対して効果的な第２のセキュリティ機構は、上述したビットベクトルを使用して状態情報を維持する。すなわち、ノードは、ノードが処理したＲＥＳＯＬＶＥメッセージであって、それに対する応答がまだ受信されていないＲＥＳＯＬＶＥメッセージのすべてを識別する情報を維持する。状態情報を維持するために使用するフィールドは、ターゲットＩＤと、ＲＥＳＯＬＶＥパケット中のアドレスリストである。この２番目のフィールドを、検索を妨害しようとする悪意のあるノードによってアドレスリストが変更されていないことを保証するために使用する。ビットベクトルの他の例に関して上述したように、ノードは、ＲＥＳＯＬＶＥからこれらのフィールドのハッシュを生成し、ビットベクトル中の対応するビット位置をセットして、そのＲＥＳＯＬＶＥの処理の履歴を維持する。

【００７９】

図６の単純化した流れ図に示すように、別のノードからＲＥＳＰＯＮＳＥメッセージを受信したとき（２９６）、このＲＥＳＰＯＮＳＥメッセージ中のフィールドをハッシュし、ビット位置を計算する（２９８）。次に、ノードは、ビットベクトルをチェックし、ビット位置がセットされているかどうかを確認する（３００）。ビットがセットされていない場合、このＲＥＳＰＯＮＳＥが以前に処理したＲＥＳＯＬＶＥとは関係がないことを意味し、パケットを廃棄する（３０２）。ビット位置がセットされている場合、このＲＥＳＰＯＮＳＥが以前に処理したＲＥＳＯＬＶＥと関係していることを示し、ビット位置をリセットする（３０４）。ビット位置をリセットすることにより、ノードは、悪意のあるノードからの再生攻撃の一部として送信された可能性のある、別の同一のＲＥＳＰＯＮＳＥメッセージを無視することになる。次に、ノードは、ＲＥＳＰＯＮＳＥを処理してそれを次のホップに転送する前に、ＲＥＳＰＯＮＳＥメッセージ中のＰＡＣのすべてが有効であるかどうかを確認するためにチェックを行う（３０６）。ＰＡＣのいずれかが無効である場合（３０６）、ノードはパケットを拒絶する（３１０）。

【００８０】
ＲＥＳＯＬＶＥプロセスは、ＲＥＳＯＬＶＥ要求をＲＥＳＰＯＮＳＥに変換することに触れる。ここで論じたこのＲＥＳＰＯＮＳＥの処理は、ＲＥＳＰＯＮＳＥが最近受信したＲＥＳＯＬＶＥに対応することを保証すること、および指定された次のホップにＲＥＳＰＯＮＳＥを転送することを含む。例えば、ノードＰが、ターゲットＰＮＲＰ　ＩＤと、ＢｅｓｔＭａｔｃｈ　ＰＡＣと、このノードの前に元のＲＥＳＯＬＶＥを処理したすべてのノードのアドレスをリストする経路とを含み、このノードがＰＮＲＰアドレスを所有することで終了するＲＥＳＰＯＮＳＥパケットＳを受信すると仮定する。ノードＰは、ＲＥＳＰＯＮＳＥの受信をＡＣＫで確認する。ノードＰは、それ自体のアドレスについてＲＥＳＰＯＮＳＥ経路をチェックする。ノードＰのアドレスは、このパケットが有効となるために、アドレスリスト中の最後のエントリでなければならない。ノードＰは、ＲＥＳＰＯＮＳＥが最近確認したＲＥＳＯＬＶＥとマッチすることを保証するために、受信したビットベクトルをチェックする。ＲＥＳＰＯＮＳＥが、受信したビットベクトル中のフィールドと一致しない場合、またはＰのアドレスが経路リスト中の最後のアドレスでない場合、ＲＥＳＰＯＮＳＥを暗黙のうちに除去し、処理は停止する。Ｐは、ＢｅｓｔＭａｔｃｈ　ＰＡＣを検証し、それをＰのローカルキャッシュに追加する。ＢｅｓｔＭａｔｃｈが無効である場合、ＲＥＳＰＯＮＳＥを暗黙のうちに除去し、処理は停止する。Ｐは、ＲＥＳＰＯＮＳＥ経路の最後からそのアドレスを除去する。Ｐは、対応するＲＥＳＯＬＶＥ要求をＡＣＣＥＰＴしたノードを示すフラグセットを有する最後のエントリまで、ＲＥＳＰＯＮＳＥ経路の最後からエントリを除去することを続行する。経路がそのときに空である場合、対応するＲＥＳＯＬＶＥがローカルに生成される。ＰＮＲＰは、ＢｅｓｔＭａｔｃｈに対する識別検証チェックを行う。識別検証チェックが成功した場合、ＢｅｓｔＭａｔｃｈが要求マネージャに渡され、そうでない場合、失敗の表示が渡される。経路が空である場合、処理は完了する。経路が空でない場合、ノードは、ＲＥＳＰＯＮＳＥパケットを経路リスト中の最後のエントリに転送する。

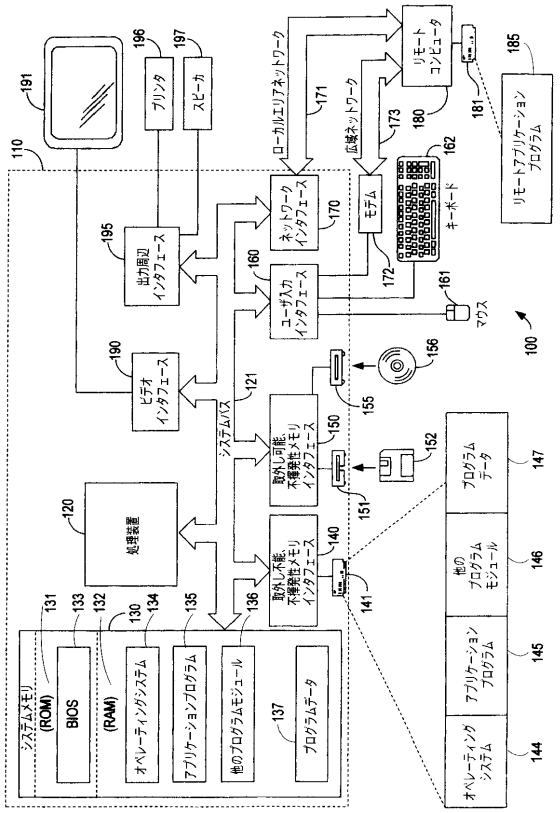
【００８１】
発行されたアドレス証明書が証明書満了日（Validity/Toフィールド）より前に無効になったときはいつでも、ＰＮＲＰアドレス証明書を取り消す必要がある。このようなイベントの例は、ノードがスムーズにＰ２Ｐネットワークから切断されるとき、またはノードがグループから離脱しつつあるときなどである。本発明の取消し機構は、取消し証明書の発行を利用する。取消し証明書は、Revoke Flagセットと、現在時刻（または証明書を取り消すべき時刻）にセットされたValidityフィールドの From dateと、以前に公示された証明書と同じ値にセットされたToフィールドとを有する。以下の条件すべてを満たす証明書すべてが取り消されるとみなされる。その証明書が同じ発行者によって署名されていること、ＩＤが取消し証明書のＩＤと一致すること、Addressフィールドが、取消し証明書のAddressフィールドと一致すること、ValidationフィールドのTo dateが、取消し証明書のValidationフィールドのTo dateと同じであること、およびValidationフィールドのFrom dateが、取消し証明書のValidationフィールドのFrom dateに先行することである。取消し証明書が署名されるので、悪意のあるノードがクラウドからどれかを切断することができないことが保証される。

【００８２】
本発明の様々な実施形態の上記の説明は、例示および説明のために提示した。上記の説明は、包括的なものではなく、または開示される厳密な実施形態に本発明を限定するものではない。上記の教示に照らして、多数の修正形態または変形形態が可能である。本発明の原理およびその実際的な応用例を最良に例示し、それによって当業者が、企図される特定の使用法に適するように本発明を様々な実施形態で、様々な修正を加えて利用することが可能となるように、上記で議論した実施形態を選び、説明した。このような修正形態および変形形態は、頭記の特許請求の範囲が公平に、法律的に、かつ公正に権利を有する幅に従って解釈されるとき、頭記の特許請求の範囲に記載される本発明の範囲内にある。

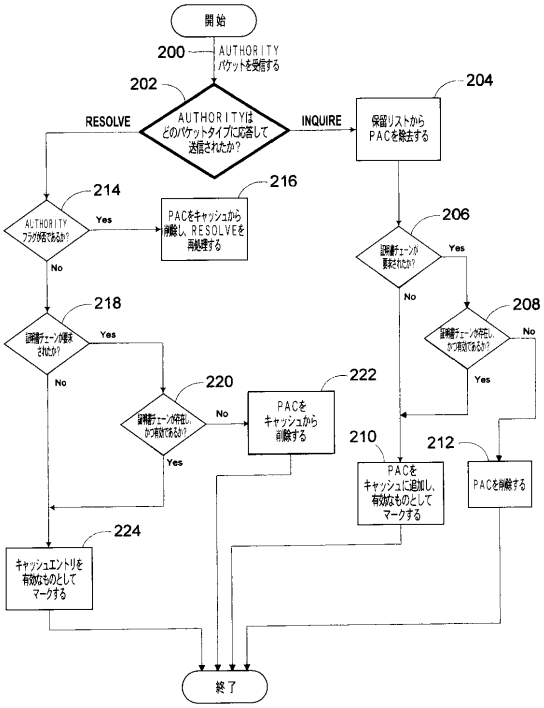
【図面の簡単な説明】

【図１】本発明が常駐する例示的コンピュータシステムを一般的に示すブロック図である。
【図２】本発明の実施形態にかかるＡＵＴＨＯＲＩＴＹパケット処理のセキュリティ面を示す、単純化した流れ図である。
【図３】本発明の実施形態にかかるＰ２Ｐディスカバリの同期段階のセキュリティ面を示す、単純化した通信処理の流れ図である。
【図４】本発明の実施形態にかかるＲＥＳＯＬＶＥパケット処理のセキュリティ面を示す、単純化した流れ図である。
【図５】本発明の実施形態によるＦＬＯＯＤパケット処理のセキュリティ面を示す、単純化した流れ図である。
【図６】本発明の実施形態によるＲＥＳＰＯＮＳＥパケット処理のセキュリティ面を示す、単純化した流れ図である。
【符号の説明】
１００　コンピューティング環境
１１０　コンピュータ
１２０　処理装置
１２１　システムバス
１３０　システムメモリ
１３１　読取り専用メモリ
１３２　ランダムアクセスメモリ
１３３　基本入出力システム
１３４、１４４　オペレーティングシステム
１３５、１４５　アプリケーションプログラム
１３６、１４６　他のプログラムモジュール
１３７、１４７　プログラムデータ
１４０、１５０　インタフェース
１６０　ユーザ入力インタフェース
１６１　ポインティングデバイス
１６２　キーボード
１７０　ネットワークインタフェースまたはアダプタ
１７１　ローカルエリアネットワーク
１７２　モデム
１７３　広域ネットワーク
１８０　リモートコンピュータ
１９０　ビデオインタフェース
１９１　モニタ
１９５　出力周辺インタフェース
１９６　プリンタ
１９７　スピーカ

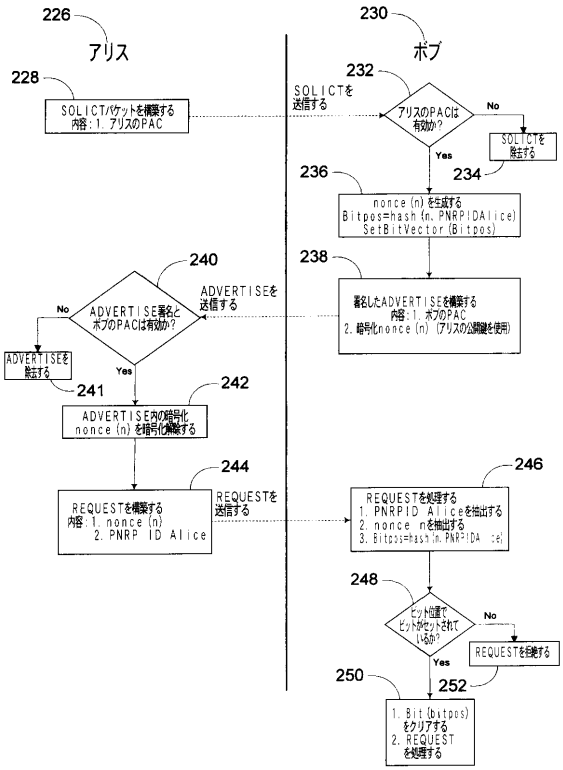
【図１】


ローカルエリアネットワーク
広域ネットワーク
リモートコンピュータ
リモートアプリケーションプログラム
プリンタ
スピーカ
ネットワークインタフェース
モデム
キーボード
出力周辺インタフェース
ユーザ入力インタフェース
マウス
ビデオインタフェース
システムバス
取外し可能、不揮発性メモリインタフェース
処理装置
システムメモリ
(ROM)
BIOS
(RAM)
オペレーティングシステム
アプリケーションプログラム
他のプログラムモジュール
プログラムデータ
プログラムデータ
他のプログラムモジュール
アプリケーションプログラム
オペレーティングシステム

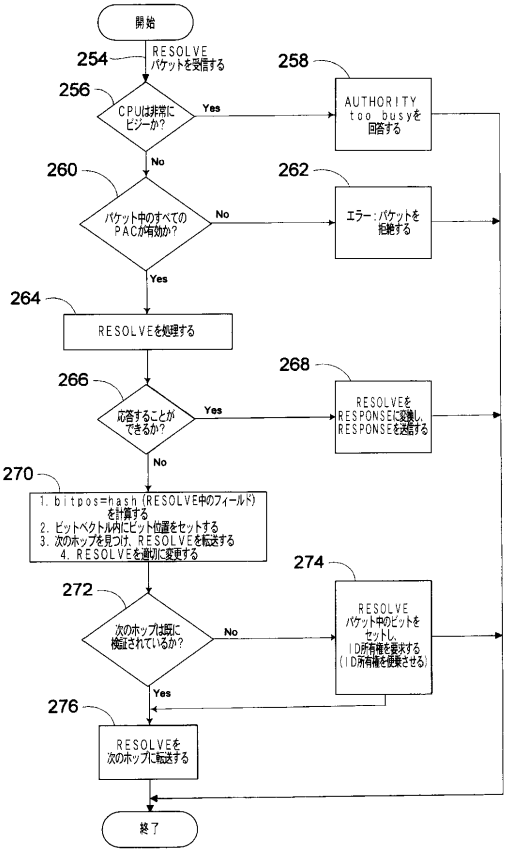
【図２】


開始
AUTHORITYパケットを受信する
AUTHORITYはどのパケットタイプに応答して送信されたか?
RESOLVE
INQUIRE
保留リストからPACを検索する
AUTHORITYフラグが立っているか?
PACをキャッシュから削除し、RESOLVEを再処理する
認証チェーンが変更されたか?
認証チェーンが変更されたか?
認証チェーンが存在し、かつ有効であるか?
PACをキャッシュから削除する
PACをキャッシュに追加し、有効なものとしてマークする
PACを削除する
キャッシュエントリを有効なものとしてマークする
終了

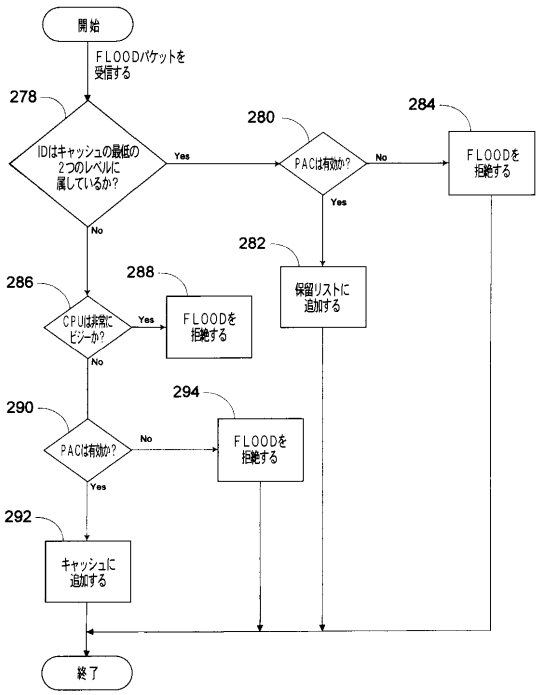
【図３】


アリス
ボブ
SOLICT/パケットを構築する
内容：1. アリスのPAC
SOLICTを送信する
アリスのPACは有効か?
SOLICTを廃棄する
nonce (n) を生成する
Bitpos=hash (n, PNRPIDAlice)
SetBitVector (Bitpos)
署名したADVERTISEを構築する
内容：1. ボブのPAC
2. 暗号化nonce (n) (アリスの公開鍵を使用)
ADVERTISEを送信する
ADVERTISE署名とボブのPACは有効か?
ADVERTISEを廃棄する
ADVERTISE内の暗号化nonce (n) を暗号化解読する
REQUESTを構築する
内容：1. nonce (n)
2. PNRP ID Alice
REQUESTを送信する
REQUESTを処理する
1. PNRPID Aliceを検出する
2. nonce nを検出する
3. Bitpos=hash (n, PNRPIDA :e)
ビット位置でビットがセットされているか?
REQUESTを廃棄する
1. Bit (bitpos) をクリアする
2. REQUEST を処理する

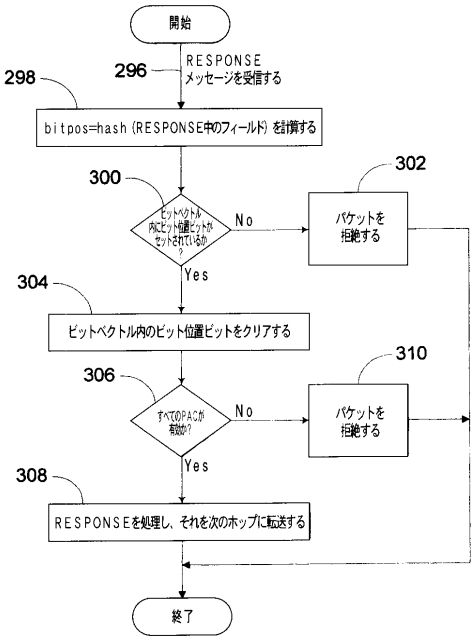
【図４】


開始
RESOLVEパケットを受信する
CPUは非常にビジーか?
AUTHORITY too busyを回答する
パケット中のすべてのPACが有効か?
エラー：パケットを拒絶する
RESOLVEを処理する
応答することができるか?
RESOLVEをRESPONSEに変換し、RESPONSEを送信する
1. bitpos=hash (RESOLVE中のフィールド) を計算する
2. ビットベクトル内にビット位置をセットする
3. 次のホップを見つけ、RESOLVEを転送する
4. RESOLVEを適切に変更する
次のホップは既に検証されているか?
RESOLVEパケット中のビットをセットし、ID所有権を要求する (ID所有権を提要させる)
RESOLVEを次のホップに転送する
終了

【図５】


開始
FLOODパケットを受信する
278
IDはキャッシュの最低の2つのレベルに属しているか?
Yes
No
280
PACは有効か?
No
Yes
284
FLOODを拒絶する
282
保留リストに追加する
286
CPUは非常にビジーか?
Yes
No
288
FLOODを拒絶する
290
PACは有効か?
No
Yes
294
FLOODを拒絶する
292
キャッシュに追加する
終了

【図６】


開始
296
RESPONSEメッセージを受信する
298
bitpos=hash(RESPONSE中のフィールド)を計算する
300
ビットベクトル内にビット位置ビットがセットされているか?
No
Yes
302
パケットを拒絶する
304
ビットベクトル内のビット位置ビットをクリアする
306
すべてのPACが有効か?
No
Yes
310
パケットを拒絶する
308
RESPONSEを処理し、それを次のホップに転送する
終了

フロントページの続き

(72)発明者　アレクサンドル　ガブリレスキュ
アメリカ合衆国　９８０５３　ワシントン州　レッドモンド　ノースイースト　７８　ウェイ　２３２０３
(72)発明者　ジョン　エル．ミラー
アメリカ合衆国　９８００７　ワシントン州　ベルビュー　１４０　プレイス　ノースイースト　１３０６
(72)発明者　グラハム　エー．ホイーラー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ノースイースト　９９　コート　１６９０５

審査官　市川　武宜

(56)参考文献　特開平０８－２４９２４９（ＪＰ，Ａ）
特開２００１－２０２０１４（ＪＰ，Ａ）
特開２００２－０５７７０１（ＪＰ，Ａ）
特開２０００－０５７１１２（ＪＰ，Ａ）
特開平１１－１２２２８３（ＪＰ，Ａ）
特開２００２－１１１７１３（ＪＰ，Ａ）
特開２００２－０６４４９５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/20
H04L　9/32