(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-134312
(P2006-134312A)
(43)公開日　平成18年5月25日(2006.5.25)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B285
H04L 9/32	(2006.01)	H04L	9/00	675Z	5J104
		H04L	9/00	675B	

審査請求 未請求　請求項の数 20　ＯＬ　外国語出願　（全 17 頁）

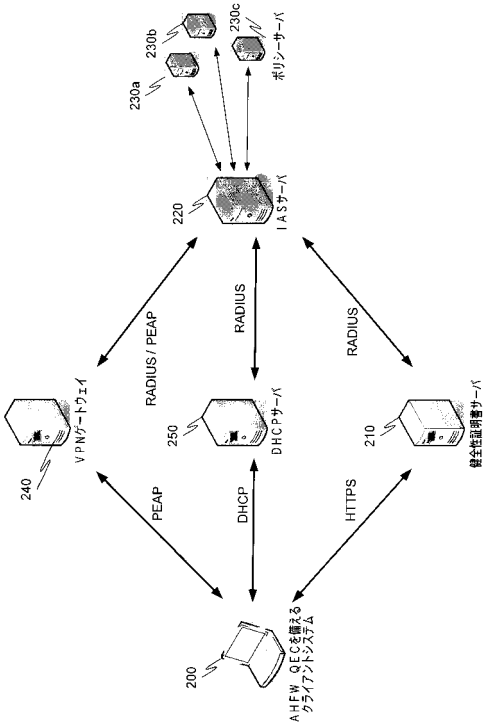
(21)出願番号　特願2005-299941 (P2005-299941)
(22)出願日　平成17年10月14日 (2005.10.14)
(31)優先権主張番号　60/618,139
(32)優先日　平成16年10月14日 (2004.10.14)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/056,276
(32)優先日　平成17年2月14日 (2005.2.14)
(33)優先権主張国　米国 (US)

(71)出願人　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　ブライアン　ディー．スワンダー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】ＩＰｓｅｃを使ってネットワーク検疫を提供するシステムおよび方法

(57)【要約】
【課題】ＩＰｓｅｃを使ってネットワーク検疫を提供するシステムおよび方法を提供すること。
【解決手段】無効な、または破損した状態を有するマシンがホストリソースにアクセスするのを制限されるようにするシステムおよび方法が提供される。クライアントマシン上に位置する検疫エージェント（ＱＡ）は、複数の検疫ポリシークライアントから健全性ステートメントを獲得する。ＱＡは、それらのステートメントをパッケージ化し、そのパッケージを検疫実施クライアント（ＱＥＣ）に提供する。ＱＥＣは、健全性証明書を求める要求と共にそのパッケージを検疫健全性証明書サーバ（ＨＣＳ）に送る。クライアントが有効な健全性ステートメントを提供した場合、ＨＣＳは、ＩＰｓｅｃセッション折衝で使用され得るクライアント健全性証明書を与える。
【選択図】図２



【特許請求の範囲】
【請求項１】
ホストが、ＩＰセキュリティプロトコル（ＩＰｓｅｃ）を使用するネットワークにおいて選択的ネットワーク隔離を提供する方法であって、
クライアントからクライアント健全性証明書を含むインターネットキー交換（ＩＫＥ）パケットを受け取ること、
前記クライアント健全性証明書を検証すること、
前記クライアント健全性証明書が有効である場合、前記クライアントにホスト健全性証明書を送ること、および
前記クライアント健全性証明書が無効である場合、前記ホストへの前記クライアントのアクセスを拒否すること
を備えることを特徴とする方法。
【請求項２】
健全性証明書は、前記証明書の所有者が前記ネットワークのセキュリティポリシーに適合していることを示すことを特徴とする請求項１に記載の方法。
【請求項３】
前記クライアント健全性証明書が有効である場合、ＩＰｓｅｃ通信を介して前記クライアントと通信を行うことをさらに備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記健全性証明書はＸ５０９証明書であることを特徴とする請求項１に記載の方法。
【請求項５】
前記健全性証明書はＫｅｒｂｅｒｏｓチケットであることを特徴とする請求項１に記載の方法。
【請求項６】
前記健全性証明書はＷＳ－Ｓｅｃｕｒｉｔｙトークンであることを特徴とする請求項１に記載の方法。
【請求項７】
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が格納されていることを特徴とするコンピュータ可読媒体。
【請求項８】
ホストが健全性証明書を獲得する方法であって、
少なくとも１つの健全性ステートメントを健全性証明書サーバに送ること、
健全性証明書サーバから少なくとも１つの健全性ステートメント応答を受け取ること、および
前記少なくとも１つの健全性ステートメントが前記健全性証明書サーバによって有効と確認される場合、健全性証明書を受け取り、前記ホストへのクライアントのアクセスを許可する前に前記クライアントからのクライアント健全性証明書を必要とするＩＰｓｅｃポリシーを実施するように前記ホストを構成すること
を備えることを特徴とする方法。
【請求項９】
前記少なくとも１つの健全性ステートメントが有効と確認されない場合、前記少なくとも１つの健全性ステートメント応答は、前記ホストがネットワークセキュリティポリシーに適合していないことを示すことを特徴とする請求項８に記載の方法。
【請求項１０】
前記健全性証明書はＸ５０９証明書であることを特徴とする請求項８に記載の方法。
【請求項１１】
前記健全性証明書はＫｅｒｂｅｒｏｓチケットであることを特徴とする請求項８に記載の方法。
【請求項１２】
前記健全性証明書はＷＳ－Ｓｅｃｕｒｉｔｙトークンであることを特徴とする請求項８

に記載の方法。
【請求項１３】
請求項８に記載の方法を実行するコンピュータ実行可能命令が格納されていることを特徴とするコンピュータ可読媒体。
【請求項１４】
ネットワーク隔離モデルを実施するコンピュータネットワークであって、
各コンピュータが健全性証明書を所有し、やはり有効な健全性証明書を所有するコンピュータとだけ通信を行う第１のコンピュータグループと、
各コンピュータが健全性証明書を所有し、前記ネットワーク中の他のすべてのコンピュータと通信を行う第２のコンピュータグループと、
各コンピュータが健全性証明書を所有せず、前記ネットワーク中の他のすべてのコンピュータと通信を行う第３のコンピュータグループと
を備えることを特徴とするコンピュータネットワーク。
【請求項１５】
前記第１のグループ中のコンピュータ間、および前記第１のグループのコンピュータと前記第２のグループのコンピュータの間の通信がＩＰｓｅｃを使って達成されることを特徴とする請求項１４に記載のネットワーク。
【請求項１６】
前記健全性証明書はＸ５０９証明書であることを特徴とする請求項１４に記載のネットワーク。
【請求項１７】
前記健全性証明書はＫｅｒｂｅｒｏｓチケットであることを特徴とする請求項１４に記載のネットワーク。
【請求項１８】
前記健全性証明書はＷＳ－Ｓｅｃｕｒｉｔｙトークンであることを特徴とする請求項１４に記載のネットワーク。
【請求項１９】
前記健全性証明書は、前記証明書の所有者が前記ネットワークの既定のセキュリティポリシーに適合していることを示すことを特徴とする請求項１４に記載のネットワーク。
【請求項２０】
前記第１のグループ中のコンピュータは、前記第３のグループ中のコンピュータと通信を開始することができるが、前記第３のグループ中のコンピュータは前記第１のグループ中のコンピュータと通信を開始することができないことを特徴とする請求項１４に記載のネットワーク。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、コンピュータアクセス管理に関し、より詳細には、クライアントのホストリソースへのアクセスを許可する前にクライアントのセキュリティ状態をチェックすることに関する。
【背景技術】
【０００２】
コンピュータネットワークにおいて、クライアント、サーバ、およびピアは、一般に、信頼モデルおよび機構を使って、許可されていないユーザがネットワーク上のホストコンピュータにアクセスできないようにする。これらの信頼モデルおよび機構は、悪意のないユーザを識別するのに使用される。しかしながら、ユーザのマシンが、そのユーザの知らないうちに他のコンピュータに危険をもたらすこともあり得る。例えば、マシンは、ウイルスを含むこともあり、ユーザが気付いていないセキュリティホールを有することもある。ゆえに、ユーザにどんなに悪意がなくとも、ユーザのマシンの保護されていない状態は、そのセキュリティ欠陥が修復されるまでネットワークから隔離される結果となるべきで

ある。
【０００３】
ＩＰｓｅｃは、データ暗号化およびデータ保全を含む、通信を保護する複数の機能を定義する。ＩＰｓｅｃは、認証ヘッダ（ＡＨ）を使って暗号化なしで発信元認証および保全性を提供し、カプセル化セキュリティペイロード（ＥＳＰ）を使って暗号化と共に認証および保全性を提供する。ＩＰｓｅｃを用いる場合、送信者と受信者だけがセキュリティ鍵を知っている。認証データが有効である場合、受信者は、その通信がその送信者からもたらされたこと、およびその通信が送信中に変更されなかったことがわかる。
【０００４】
ＩＰｓｅｃは、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）スタック内の１つの層としてイメージされ得る。この層は、各コンピュータ上のセキュリティポリシーおよび送信者と受信者の間のネゴシエートされたセキュリティアソシエーションによって制御される。このポリシーは、１組のフィルタおよび関連付けられたセキュリティ挙動からなる。あるパケットのＩＰアドレス、プロトコル、およびポート番号がフィルタにマッチする場合、そのパケットは、それに関連付けられたセキュリティ挙動に従う。第１のそのようなパケットは、送信者と受信者の間のセキュリティアソシエーションのネゴシエーションをトリガする。インターネットキー交換（ＩＫＥ）はこのネゴシエーションの標準プロトコルである。ＩＫＥネゴシエーションの間、２つのコンピュータは、認証およびデータセキュリティ方法に同意し、相互認証を行い、次いで、その後のデータ暗号化のための共有鍵を生成する。
【０００５】
セキュリティアソシエーションが確立された後、データ伝送が各コンピュータごとに進行し、リモートの受信者に送信するパケットにデータセキュリティ処理を適用する。この処理は、単に送信されるデータの保全性を保証することもでき、送信されるデータを暗号化することもできる。ＩＰペイロードのデータ保全性およびデータ認証は、ＩＰヘッダとトランスポートヘッダの間に位置する認証ヘッダによって提供され得る。認証ヘッダは認証データおよびシーケンス番号を含み、それらは共に、送信者を検証し、メッセージが送信中に変更されていないことを保証し、反射攻撃を防ぐのに使用される。
【０００６】
ＥＳＰは、このアーキテクチャにおける鍵形式であり、保護されるデータを暗号化し、暗号化されたデータをＩＰ　ＥＳＰのデータ部分に入れることによって機密性および保全性を提供する。ユーザのセキュリティ要件に応じて、この機構は、トランスポート層セグメント（例えば、ＴＣＰ、ＵＤＰ、ＩＣＭＰ、ＩＧＭＰ）を暗号化するのにも、ＩＰデータグラム全体を暗号化するのにも使用され得る。元のデータグラム全体の機密性を提供するためには、保護されたデータをカプセル化することが必要である。ＥＳＰヘッダは、ＩＰヘッダの後、上位層プロトコルヘッダ（トランスポートモード）の前またはカプセル化ＩＰヘッダ（トンネルモード）の前に挿入される。
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、従来の認証手順は、保護されていない、または悪質ですらあるマシンがホストのアクセスするのを妨げない。コンピュータは有効な認証を提示し得るが、マシン自体が、そのマシンが別のコンピュータのネットワークリソースへのアクセスを許可される前に修正されるべきウイルスに感染し、またはセキュリティホールを含んでいることがある。したがって、当分野では、クライアントが、セキュリティチェックに合格するまでホストにアクセスすることを許可されないようにするシステムおよび方法が求められている。
【課題を解決するための手段】
【０００８】
以上を考慮して、本発明は、ホストが、クライアントからのクライアント健全性ステー

トメントを含むインターネットキー交換（ＩＫＥ）パケットを受け取り、クライアント健全性ステートメントを検証し、クライアント健全性ステートメントが有効である場合には、クライアントにホスト健全性ステートメントを送り、クライアント健全性ステートメントが無効である場合には、ホストへのクライアントのアクセスを拒否することによって、ＩＰセキュリティプロトコル（ＩＰｓｅｃ）を使用するネットワークにおいて選択的ネットワーク隔離（ｉｓｏｌａｔｉｏｎ）を提供する方法を提供する。健全性ステートメントは、クライアントの、ネットワークのセキュリティポリシーへの適合性（ｃｏｎｆｏｒｍａｎｃｅ）を記述する。この方法は、クライアント健全性証明書（ｃｌｉｅｎｔ　ｈｅａｌｔｈ　ｃｅｒｔｉｆｉｃａｔｅ）が受け入れられる場合には、任意選択で暗号化された通信を介してクライアントと通信を行うことをさらに含む。健全性証明書は、本発明の様々な実施形態では、Ｘ５０９証明書、Ｋｅｒｂｅｒｏｓチケット、またはＷＳ－Ｓｅｃｕｒｉｔｙトークンとすることができる。

【０００９】

本発明の別の実施形態は、１つまたは複数の健全性ステートメントを健全性証明書サーバに送ること、健全性証明書サーバから健全性ステートメント応答を受け取ること、および健全性ステートメントが健全性証明書サーバによって有効と確認される場合には、健全性証明書を受け取り、ホストを、ホストへのクライアントのアクセスを許可する前にクライアントからのクライアント健全性証明書を必要とするＩＰｓｅｃポリシーを実施するように構成することを含む、ホストが健全性証明書を獲得する方法を提供する。健全性ステートメントが有効と確認されない場合には、健全性ステートメント応答は、そのホストがネットワークセキュリティポリシーに適合していないことを示す。

【００１０】

本発明のさらに別の実施形態は、ネットワーク隔離モデルを実施するコンピュータネットワークを対象とする。このネットワークは、各コンピュータが健全性証明書を所有し、やはり有効な健全性証明書を所有するコンピュータとだけ通信を行う第１のコンピュータグループと、各コンピュータが健全性証明書を所有し、ネットワーク中の他のすべてのコンピュータと通信を行う第２のコンピュータグループと、各コンピュータが健全性証明書を所有せず、ネットワーク中の他のコンピュータの全部または一部と通信を行う第３のコンピュータグループとを含む。第１のグループ中のコンピュータ間、および第１のグループのコンピュータと第２のグループのコンピュータの間の通信は、ＩＰｓｅｃを使って達成される。

【００１１】

本発明のさらなる特徴および利点は、添付の図を参照して進められる、以下の例示的実施形態の詳細な説明を読めば明らかになる。

【００１２】

本明細書に組み込まれ、その一部を形成する添付の図面には、本発明のいくつかの態様が示されており、それらは、その記述と共に、本発明の原理を説明する役割を果たす。

【００１３】

本発明をいくつかの好ましい実施形態との関連で説明するが、本発明をそれらの実施形態に限定する意図はない。その反対に、すべての代替形態、変更形態および均等物を、添付の特許請求の範囲によって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して包含することが意図されている。

【発明を実施するための最良の形態】

【００１４】

図面に戻ると、そこでは類似の参照番号は類似の要素を参照しており、本発明が、適切なコンピューティング環境で実施されるものとして示されている。以下の説明は、本発明の実施形態に基づくものであり、本明細書で明示的に説明されない代替の実施形態に関して本発明を限定するものとみなすべきではない。

【００１５】

次に、本発明が使用され得る、ネットワーク化された環境の一例を、図１Ａを参照して

説明する。この例示的ネットワークは、雲形によって表されるネットワーク１１１を介して相互に通信を行ういくつかのコンピュータ１１０を含む。ネットワーク１１１は、ルータ、ゲートウェイ、スイッチなど、多くの周知の構成要素を含むことができ、コンピュータ１１０が有線および／または無線媒体を介して通信することを可能にする。ネットワーク１１１を介して相互に対話するとき、コンピュータの１つまたは複数は、他のコンピュータに対してクライアント、ネットワークサーバ、検疫サーバ、またはピアとして機能することができる。したがって、本発明の様々な実施形態は、たとえ本明細書に含まれる具体例がこれらの種類のコンピュータすべてに言及しないとしても、クライアント、ネットワークサーバ、検疫サーバ、ピア、またはこれらの組合せにおいて実施され得る。

【００１６】

図１Ｂに、本発明が実施され得る適切なコンピューティングシステム環境１００の一例を示す。コンピューティングシステム環境１００は、適切なコンピューティング環境の一例にすぎず、本発明の用途または機能の範囲に関するどんな限定を示唆することを意図したものではない。また、コンピューティング環境１００は、例示的コンピューティング環境１００に示す構成要素のいずれか１つまたはそれらの組合せに関連するいずれの依存関係または要件を有するものであるとも解釈すべきではない。

【００１７】

本発明は、他の多数の汎用または専用コンピューティングシステム環境または構成と共に動作する。本発明と共に使用するのに適し得る周知のコンピューティングシステム、環境、および構成の例には、それだけに限らないが、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルドまたはラップトップ機器、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、プログラム可能な家庭用電化製品、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、上記のシステムまたは機器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。

【００１８】

本発明は、コンピュータにより実行される、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なコンテキストで説明することができる。一般に、プログラムモジュールには、特定のタスクを実行し、または特定の抽象データ型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、データ構造体などが含まれる。また、本発明は、タスクが、通信ネットワークを介してリンクされたリモート処理装置により実行される分散コンピューティング環境でも実施され得る。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とリモート両方のコンピュータ記憶媒体に置くことができる。

【００１９】

図１Ｂを参照すると、本発明を実施する例示的システムは、本発明のコンテキスト内でクライアント、ネットワークサーバ、検疫サーバ、またはピアとして働くことのできるコンピュータ１１０の形態の汎用コンピューティングデバイスを含む。コンピュータ１１０の構成要素には、それだけに限らないが、処理装置１２０、システムメモリ１３０、およびシステムメモリ１３０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が含まれ得る。システムバス１２１は、様々なバスアーキテクチャのいずれかを使用したメモリバスまたはメモリコントローラ、周辺バス、およびローカルバスを含む数種類のバス構造のいずれでもよい。例をあげると、それだけに限らないが、そのようなアーキテクチャには、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡバス（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎａｎｃｅｄ ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｅ）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。

【００２０】

コンピュータ１１０は、通常、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によってアクセスされ得る任意の使用可能な媒体とすることができ、それには揮発性と不揮発性両方の媒体、取り外し可能と取り外し不能両方の媒体が含まれる。例をあげると、それだけに限らないが、コンピュータ可読媒体には、コンピュータ記憶媒体および通信媒体が含まれ得る。コンピュータ記憶媒体には、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その他のデータなどの情報を記憶するための任意の方法または技術で実施された、揮発性と不揮発性両方、取り外し可能と取り外し不能両方の媒体が含まれる。コンピュータ記憶媒体には、それだけに限らないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリや他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスクや他の光ディスク記憶、磁気カセット、磁気テープ、磁気ディスク記憶や他の磁気記憶装置、あるいは所望の情報を格納するのに使用でき、コンピュータ１１０によってアクセスすることができる他の任意の媒体が含まれる。通信媒体は、通常、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その他のデータを、搬送波や他の搬送機構などの変調されたデータ信号中に具現化されるものであり、任意の情報配信媒体を含む。「変調されたデータ信号」という用語は、その特性の１つまたは複数が、その信号に情報を符号化するような方式で設定または変更されている信号を意味する。例をあげると、それだけに限らないが、通信媒体には、有線ネットワークや直接配線接続などの有線媒体、および音響、ＲＦ、赤外線、その他の無線媒体などの無線媒体が含まれる。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めるべきである。

【００２１】

システムメモリ１３０は、読出し専用メモリ（ＲＯＭ）１３１やランダムアクセスメモリ（ＲＡＭ）１３２などの揮発性および不揮発性メモリの形でコンピュータ記憶媒体を含む。基本入出力システム（ＢＩＯＳ）１３３は、始動時などに、コンピュータ１１０内の諸要素間での情報転送を支援する基本ルーチンを含み、通常、ＲＯＭ１３１に格納される。ＲＡＭ１３２は、通常、処理装置１２０から直ちにアクセス可能であり、または処理装置１２０によって現在操作されているデータおよびプログラムモジュールを含む。例として、それだけに限らないが、図１Ｂ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、その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。

【００２２】

また、コンピュータ１１０は、他の取り外し可能／取り外し不能、揮発性／不揮発性コンピュータ記憶媒体も含み得る。例にすぎないが、図１Ｂに、取り外し不能、不揮発性磁気媒体との間で読取りまたは書込みを行うハードディスクドライブ１４１、取り外し可能、不揮発性磁気ディスク１５２との間で読取りまたは書込みを行う磁気ディスクドライブ１５１、およびＣＤ－ＲＯＭや他の光媒体などの取り外し可能、不揮発性光ディスク１５６との間で読取りまたは書込みを行う光ディスクドライブ１５５を示す。例示的コンピューティング環境１００で使用され得るその他の取り外し可能／取り外し不能、揮発性／不揮発性のコンピュータ記憶媒体には、それだけに限らないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭなどが含まれる。ハードディスクドライブ１４１は、通常、インターフェース１４０などの取り外し不能メモリインター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、通常、インターフェース１５０などの取り外し可能メモリインターフェースによってシステムバス１２１に接続される。

【００２３】

前述の、図１Ｂに示す各ドライブおよびそれらに関連するコンピュータ記憶媒体は、コンピュータ１１０のための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およびその他のデータの記憶を提供する。図１Ｂでは、例えば、ハードディスクドライブ１４１は、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、その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示されている。これらのコンポーネントは、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、その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と同じでも、異なっていてもよい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、その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、少なくともそれらが異なるコピーであることを示すために、異なる番号を付与してある。

【００２４】

ユーザは、キーボード１６２や、一般に、マウス、トラックボール、タッチパッドと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ンピュータ１１０にコマンドおよび情報を入力することができる。他の入力装置（図示せず）には、マイクロホン、ジョイスティック、ゲームパッド、衛星パラボラアンテナ、スキャナなどが含まれ得る。上記およびその他の入力装置は、しばしば、システムバス１２１に結合されたユーザ入力インターフェース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、ユニバーサルシリアルバスなどの他のインターフェースおよびバス構造によっても接続することができる。また、モニタ１９１または他の種類の表示装置も、ビデオインターフェース１９０などのインターフェースを介してシステムバス１２１に接続される。また、モニタ１９１に加えて、コンピュータ１１０は、出力周辺装置インターフェース１９５を介して接続され得る、スピーカ１９７やプリンタ１９６など他の周辺出力装置を含むこともできる。

【００２５】

コンピュータ１１０は、リモートコンピュータ１８０など、１つ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た、ネットワーク化された環境で動作し得る。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、ピアデバイスまたはその他一般のネットワークノードとすることができ、図１Ｂにはメモリ記憶装置１８１だけしか示されていないが、通常は、パーソナルコンピュータ１１０に関連して前述した要素の多くまたはすべてを含む。図１Ｂに示す論理接続には、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が含まれるが、他のネットワークも含まれ得る。そのようなネットワーク環境は、オフィス、企業規模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は一般的なものである。

【００２６】

ＬＡＮネットワーク環境で使用されるとき、パーソナルコンピュータ１１０はネットワークインターフェースまたはアダプタ１７０を介してＬＡＮ１７１に接続される。ＷＡＮネットワーク環境で使用されるとき、コンピュータ１１０は、通常、モデム１７２、またはインターネットなどのＷＡＮ１７３を介して通信を確立する他の手段を含む。モデム１７２は、内蔵されても外付けされてもよく、ユーザ入力インターフェース１６０または他の適切な機構を介してシステムバス１２１に接続され得る。ネットワーク化された環境では、パーソナルコンピュータ１１０に関連して示すプログラムモジュール、またはその一部は、リモートのメモリ記憶装置１８１に格納され得る。例として、それだけに限らないが、図１Ｂ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上にあるものとして示す。図示のネットワーク接続は例であり、コンピュータ間での通信リンクを確立する他の手段も使用され得ることが理解されよう。

【００２７】

以下の説明では、特に指示しない限り、本発明を、１つまたは複数のコンピュータによって実行される動作および操作の記号表現を参照して説明する。そのようなものとして、そのような動作および操作は、時々コンピュータで実行されるともいわれ、構造化された形で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が理解されよう。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中の場所に維持し、当業者によってよく理解されている手法でコンピュータの操作を再構成し、または別のやり方で変更する。データが維持されるデータ構造体は、データの形式によって定義される特定の属性を持つメモリの物理的場所である。しかしながら、本発明は、

前述のコンテキストで説明されてはいるが、以下で説明される様々な動作および操作がハードウェアでも実施され得ることを当業者が理解するように、限定することを意図していない。

【００２８】

本発明は、ＩＰセキュリティ（ＩＰｓｅｃ）プロトコルとホストファイアウォールを組み合わせてネットワーク隔離を提供するネットワークアクセス保護のための実施機構（ｅｎｆｏｒｃｅ　ｍｅｃｈａｎｉｓｍ）を対象とする。ＩＰｓｅｃとホストファイアウォールの組合せを認証ファイアウォール（ＡＦＷ）という。検疫実施クライアント（ＱＥＣ：Ｑｕａｒａｎｔｉｎｅ　Ｅｎｆｏｒｃｅｍｅｎｔ　Ｃｌｉｅｎｔ）は、ホスト上で、ＩＰｓｅｃおよびファイアウォールポリシーを連係させるように動作する。ＱＥＣは、さらに、他のＩＰｓｅｃポリシー対応ホストと通信を行うための健全性証明書を獲得する役割も果たす。

【００２９】

図２に、本発明が実施され得る典型的なネットワーク環境を示す。クライアント２００は、健全性証明書サーバ（ＨＣＳ）２１０に健全性ステートメント（ＳｏＨ）を送る。ＨＣＳは、ポリシーサーバ２３０ａ、２３０ｂ、２３０ｃからの更新されたポリシー要件を維持するインターネット認証サーバ（ＩＡＳ）２２０を介してＳｏＨを検証する。ＳｏＨがすべてのポリシー要件に合格した場合、ＨＣＳ２１０は、クライアント２００に健全性証明書を発行する。次いで、クライアント２００は、健全性証明書を使って、図２のＶＰＮゲートウェイ２４０やＤＨＣＰサーバ２５０など他の保護されたシステムと通信を行うことができる。

【００３０】

ＨＣＳは、健全性チェックを満足させるクライアントに証明書を発行する。一実施形態では、健全性証明書は、（構成可能であるが、数時間程度の）非常に短い存続期間を有するＸ５０９証明書である。しかしながら、健全性証明書は、Ｋｅｒｂｅｒｏｓチケットや ＷＳ－Ｓｅｃｕｒｉｔｙトークンなど、システムの健全性を示す任意の検証可能なデータ構造体とすることができる。システムは、健全性証明書を持つと、それを使って他のシステムとの認証によってその健全性を証明することができる。一実施形態では、ＨＣＳは独立型であり、ＨＣＳがすでにインストールされている場合には、ＰＫＩ階層に統合される必要がない。別の実施形態では、ＨＣＳは、管理目的のために、または特定のエンティティに結び付けられた健全性証明書を使用可能にするために、既存のＰＫＩに統合される。標準ＮＡＰブートストラップの一部として、クライアントに、そのＨＣＳからルート証明書が与えられる。クライアントは、このルートを、検疫目的専用の専用ストアにインストールすることもでき（既存のＰＫＩが活用されている場合、システムは、このルートトラスト（ｒｏｏｔ　ｔｒｕｓｔ）がすでに備わっており、ブートストラップが不要であると想定する）、このルートを、マシンまたはユーザの標準証明書ストアにインストールすることもできる。

【００３１】

ＡＦＷ隔離は、ＤＨＣＰや８０２．１ｘといった他の検疫実施機構によって提供される隔離とは異なる。ＡＦＷ隔離は、ネットワーク接続が提供されているポイントで一元的に実施されるのではなく、各個別ホストによって分散して実施される。これは、各ホストに、ＤＨＣＰや８０２．１ｘ検疫などの他の実施機構では不可能な、ネットワーク上に悪質なホストが存在する場合でさえもそれ自体を保護する能力が与えられることを意味する。ＡＦＷは、ホストごと、ポートごと、またはアプリケーションごとに提供され得る唯一の隔離オプションである。

【００３２】

ＡＦＷ検疫は、図３に示すように、物理ネットワークを３つ以上の論理リングに分割する。各コンピュータは、いかなるときにもただ１つの論理リングに存在する。これらのリングは、健全性証明書の所有および健全性証明書の通信要件に関して定義される。これらのリングは、すべてのシステムに最大限の通信機能を与え、しかも、不健全なシステムか

らの攻撃から健全なシステムを保護する。保護されたリングは、健全性証明書を持ち、それらのピアが健全性証明書を持つことを必要とし得るコンピュータの集合体（ｃｏｌｌｅｃｔｉｏｎ）であると定義される。大部分のクライアントおよびサーバは、このリングに存在するであろう。保護されたリング中のコンピュータは、管理者によって定義されるサイトポリシーに従って、保護されたリングまたは境界リング中のコンピュータの一部または全部と自由に通信を行うことができる。保護されたリング中のコンピュータは、やはりサイトポリシーに従って、その保護されたリング中のコンピュータが通信を開始するという条件で、検疫リング中のコンピュータと通信を行うことができる。例えば、保護されたリング中のクライアントは、検疫リング中のサーバにＷｅｂページを要求することができる。しかしながら、検疫リング中のクライアントは、保護されたリング中のサーバにＷｅｂページを要求するのを阻止される。管理者が（全コンピュータではなく）特定のアプリケーションを検疫しようとする場合、リング間の通信は、それらのアプリケーションについてのみ制限される。例えば、ＦＴＰ通信が検疫される場合、検疫リング中のＦＴＰクライアントは、保護されたリング中のＦＴＰサーバに接続するのを阻止される。しかしながら、その特定の場合において、同じ２つのコンピュータは、それらのリングへの帰属に関係なく、ＨＴＴＰを介して自由に通信を行うことができるであろう。

【００３３】

境界リングは、健全性証明書を持つが、それらのピアが健全性証明書を持つことを必要としないコンピュータの集合体であると定義される。そのようなコンピュータは、リングへの帰属に関係なく、他の任意のコンピュータと自由に通信を行うことができる。境界リングは、通常、そこに存在するように特に構成されたごくわずかなコンピュータを含むであろう。境界リング中のシステムは、普通、リングへの帰属に関係なく、すべてのクライアントへのトラフィックを開始する必要があるサーバである。例えば、パッチサーバ（ｐａｔｃｈ　ｓｅｒｖｅｒ）は、検疫リング中のクライアントに健全性証明書が発行されるように、それらのクライアントにパッチを提供する必要がある。また、パッチサーバは、保護されたリング中のクライアントにサービスを提供し、保護されたリング中の管理サーバから通信を受け入れる必要もある。

【００３４】

検疫リングは、健全性証明書を持たないコンピュータの集合体であると定義される。それらのコンピュータは、それらが健全性チェックを完了していないため、それらがネットワーク上のゲストであるため、またはそれらが検疫システムに関与することができないため、健全性証明書を持つことができない。検疫リング中のコンピュータは、保護されたリング中のコンピュータとの場合を除いて、自由に通信を行うことができる。ＩＰｓｅｃポリシーおよび要件を変更することにより、他の隔離モデルも実施され得ることを当業者は理解されよう。

【００３５】

図４に戻ると、ＡＦＷ検疫実施クライアント（ＱＥＣ）４３０を備えるクライアント４００上で、検疫プラットフォームアーキテクチャが拡大されている。ＡＦＷ　ＱＥＣの目的は、健全性証明書サーバとネゴシエートして、健全性証明書を獲得し、ＩＰｓｅｃおよびファイアウォールコンポーネントをしかるべく構成することである。検疫エージェント（ＱＡ）は、システム健全性エージェント（ＳＨＡ）４１０ａ、４１０ｂ、４１０ｃと連係してＳｏＨを組み立てる。各ＳＨＡ４１０ａ、４１０ｂ、４１０ｃは、そのクライアントが、健全性証明書に必要とされるポリシーおよび要求すべてを満足させるかどうか判定する役割を果たす。ＱＡ４２０は、ＳＨＡ　ＡＰＩを介してこれらのチェックの結果を獲得し、それらの結果を、ＱＥＣ４３０に提供され得るＳｏＨに組み立てる。ＱＥＣ４３０は、新しい健全性証明書を獲得すると、まず、そのＳｏＨおよび認証資格証明（ａｕｔｈｅｎｔｉｃａｔｅ　ｃｒｅｄｅｎｔｉａｌｓ）をＨＣＳ４７０に伝達する。一実施形態では、この伝達は、保護されたハイパーテキスト転送プロトコル（ＨＴＴＰＳ）を介するものである。ＱＥＣ４３０がすべてのポリシー要件を満たす場合、ＱＥＣ４３０は、ＨＣＳ４７０からＳｏＨ応答および健全性証明書を受け取る。ＱＥＣ４３０は、ファイアウォー

ルおよびＩＰｓｅｃサブシステム４６０に対するデフォルト検疫規則を構成する。検疫システムが独立型である場合、ＱＥＣは健全性証明書を専用証明書ストア４５０に入れる。クライアントがすべての健全性チェックに合格していない場合、ＱＥＣはＨＣＳから、そのクライアントがポリシー要件の１つまたは複数に合格していないことを知らせる１つまたは複数のＳｏＨ応答を受け取る。ＳｏＨ応答は、クライアントが合格しなかった特定の要件を明示することができる。次いで、ＱＥＣは、クライアントを健全な状態に戻すのに必要なパッチおよび更新をインストールするために、修正サーバ（ｆｉｘ－ｕｐ　ｓｅｒｖｅｒ）を捜し出すことができる。

【００３６】

図５に、システムがＡＦＷ検疫システムに関与するときに従うプロセスを示す。ステップ５１０で、システムが起動する。システムは、（ＤＨＣＰベースの検疫実施が展開されていないものと仮定して）そのＤＨＣＰサーバから無制限のＩＰアドレスを獲得する。システムのファイアウォールは、他のシステムがそこに接続することができないように、「例外なしにオン」モードにある。この時点で、システムは、最新の健全性証明書を持たないため、検疫リングにある。システムは、他の検疫済みシステムと通信を行うことができ、インターネットにアクセスすることができる。保護されたリング中のコンピュータは、このシステムがそれらのコンピュータに接続することを阻止する。ステップ５２０で、ＡＦＷ　ＱＥＣが開始する。ステップ５３０で、ＱＥＣは、健全性証明書サーバ（ＨＣＳ）への接続を開始し、その証明書を信頼されるＨＣＳサーバのリストに照らして検証することによって、このＨＣＳが信頼されていることを検証する。ステップ５４０で、ＱＥＣは、クライアントの現在の健全性ステートメント（ＳｏＨ）情報をＨＣＳに送る。ステップ５５０で、ＨＣＳは、そのＳｏＨ情報をＩＡＳサーバに渡す。ステップ５６０で、ＩＡＳサーバは、ＳｏＨ情報およびその構成されたポリシーに基づいて、クライアントに健全性証明書を与えるべきかどうか決定する。ＩＡＳサーバは、健全性証明書サーバに、クライアントに健全性証明書が発行されるべきかどうか示す値と共に、健全性ステートメント応答（ＳｏＨＲ）を返す。

【００３７】

ステップ５７０で、健全性証明書サーバは、そのＳｏＨＲをＡＦＷ　ＱＥＣに返す。クライアントが健全性チェックに合格した場合、そのクライアントにはこのときに健全性証明書も発行される。ＡＦＷ　ＱＥＣは、新しいＳｏＨ情報が検疫エージェントに到着するたび、または現在の健全性証明書が失効しようとするたびに、ステップ５３０から５７０を経る。ＡＦＷ　ＱＥＣに健全性証明書が発行された場合、ステップ５８０で、ＡＦＷ　ＱＥＣはその証明書をコンピュータのマシンストアに加える。ＡＦＷ　ＱＥＣは、健全性証明書を用いて、それが認証を受けることのできる任意のピアとの認証を試みるようにＩＰｓｅｃサブシステムを構成する。ＡＦＷ　ＱＥＣは、ホストファイアウォールを、ＩＰｓｅｃを使用する健全性証明書を用いて認証を受けた任意のピアからの着信接続を許可するように構成する。この時点で、コンピュータは、今度は、保護されたリングで動作している。

【００３８】

ＡＦＷ検疫に関与することのできないシステムは、単に、検疫リングの中に起動し、そこに留まることになる。そのシステムは、インターネット、および、おそらく、境界リングまたは検疫リング中の他の任意のコンピュータにアクセスすることができる。保護されたリングのコンピュータは、これらのコンピュータに接続することができるが、その逆はできない。

【００３９】

図６に、クライアントがＩＰｓｅｃ対応のホストと通信を開始するためのプロセスを示す。ステップ６１０で、クライアントは、ホストに、クライアントの健全性証明書を含むＩＫＥパケットを送る。ステップ６２０で、ホストは、その健全性証明書を検証し、それに応答してそれ自体の健全性証明書を提供する。ステップ６３０で、クライアントは、ＥＳＰを使ってＴＣＰ／ＩＰハンドシェークを開始する。ステップ６４０で、ハンドシェー

クが完了し、任意選択で、クライアントとホストの間で暗号化された通信が使用可能とされる。

【００４０】

以上の本発明の様々な実施形態の説明は、例示および説明のために提示したものである。網羅的であること、または本発明を開示の実施形態とまったく同一のものに限定することは意図されていない。前述の説明に照らして、多数の変更形態および変形形態が可能である。前述の実施形態は、本発明の原理およびその実際の適用の最善の例示を提供し、それによって当業者が、本発明を、様々な実施形態において、意図されている特定の用途に適した様々な変更と共に利用することができるように選択され、説明されたものである。そのようなすべての変更形態および変形形態は、添付の特許請求の範囲が、公正、合法的、かつ公平に権利を有する広さに従って解釈されるときに、添付の特許請求の範囲によって決定される本発明の範囲内に含まれる。

【図面の簡単な説明】

【００４１】

【図１Ａ】本発明がそれを介して動作する例示的ネットワーク環境を一般的に示す概略図である。

【図１Ｂ】本発明がそこに属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】本発明の一実施形態の構成要素間の対話を示す概略図である。

【図３】本発明のネットワーク隔離モデルを示す図である。

【図４】本発明の検疫実施クライアントを示す図である。

【図５】本発明による、クライアントが健全性証明書を獲得するためのプロセスを示す図である。

【図６】本発明による、クライアントがホストとの通信を開始するためのプロセスを示す図である。

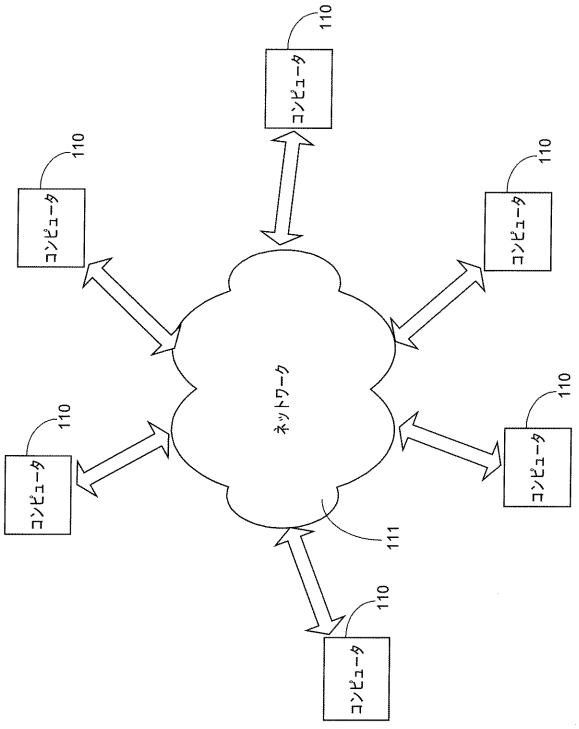
【符号の説明】

【００４２】

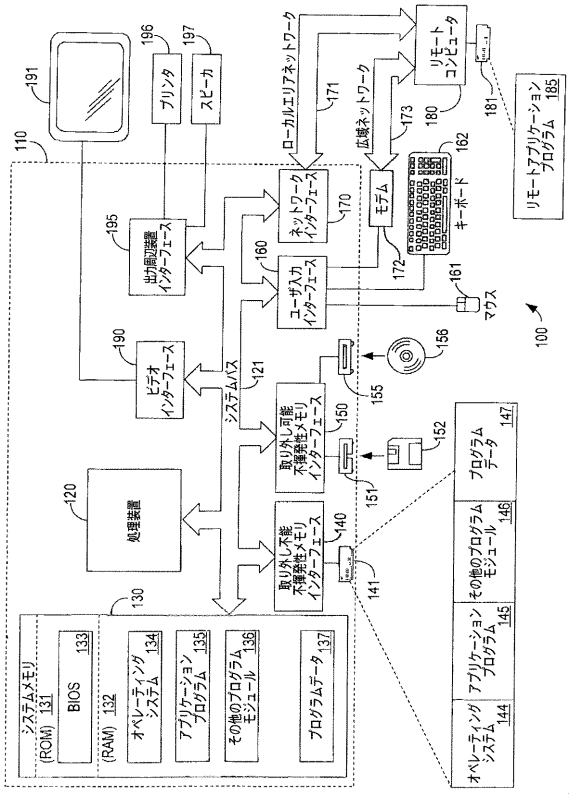
１１０　コンピュータ
１１１　ネットワーク
１２０　処理装置
１２１　システムバス
１３０　システムメモリ
１３４　オペレーティングシステム
１３５　アプリケーションプログラム
１３６　その他のプログラムモジュール
１３７　プログラムデータ
１４０　取り外し不能不揮発性メモリインターフェース
１４４　オペレーティングシステム
１４５　アプリケーションプログラム
１４６　その他のプログラムモジュール
１４７　プログラムデータ
１５０　取り外し可能不揮発性メモリインターフェース
１６０　ユーザ入力インターフェース
１６１　マウス
１６２　キーボード
１７０　ネットワークインターフェース
１７１　ロ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

１８５　リモートアプリケーションプログラム
１９０　ビデオインターフェース
１９５　出力周辺装置インターフェース
１９６　プリンタ
１９７　スピーカ
２００　ＡＨＦＷ　ＱＥＣを備えるクライアントシステム
２１０　健全性証明書サーバ
２２０　ＩＡＳサーバ
２３０ａ～ｃ　ポリシーサーバ
２４０　ＶＰＮゲートウェイ
２５０　ＤＨＣＰサーバ

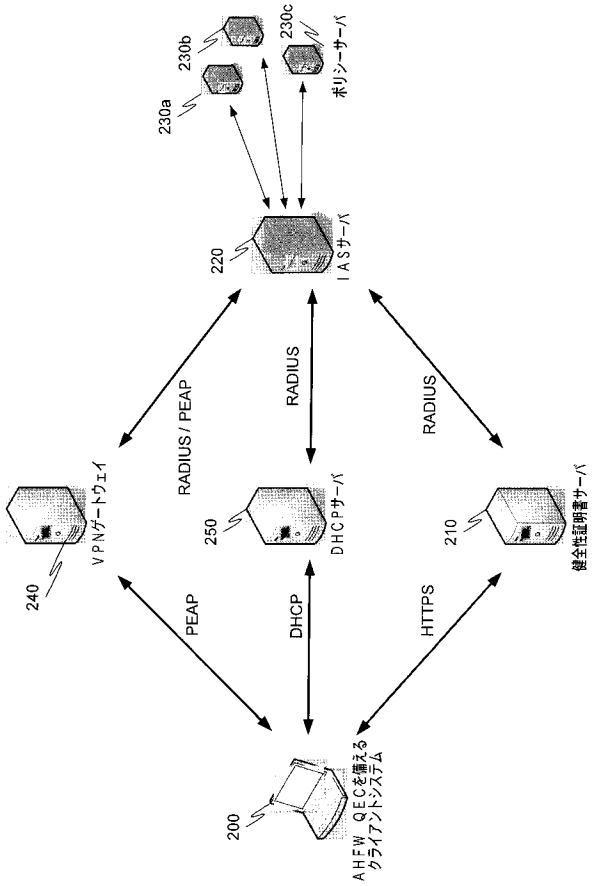
【図１Ａ】



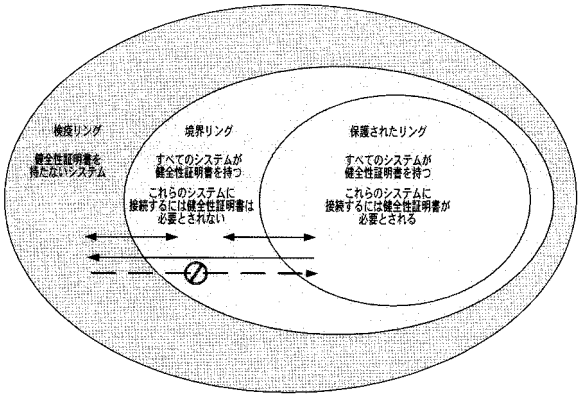
【図１Ｂ】



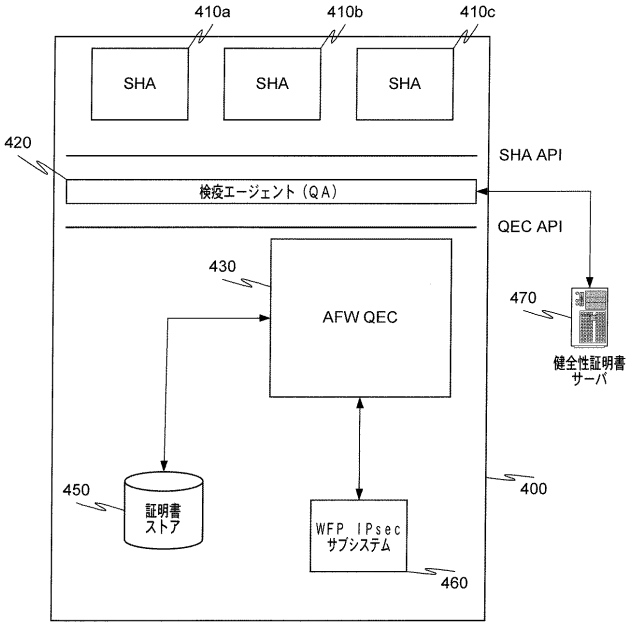
【図２】


230b
230c
ポリシーサーバ
230a
220
IASサーバ
RADIUS / PEAP
RADIUS
RADIUS
VPNゲートウェイ
240
250
DHCPサーバ
210
健全性証明書サーバ
PEAP
DHCP
HTTPS
200
AHFW QECを備えるクライアントシステム

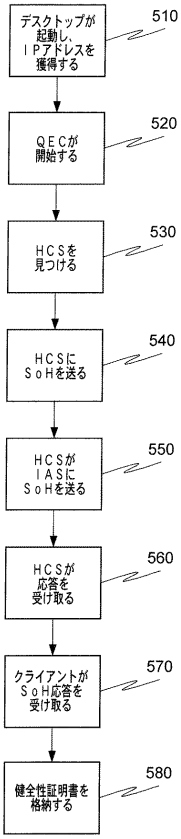
【図３】


検疫リング
健全性証明書を持たないシステム
境界リング
すべてのシステムが健全性証明書を持つ
これらのシステムに接続するには健全性証明書は必要とされない
保護されたリング
すべてのシステムが健全性証明書を持つ
これらのシステムに接続するには健全性証明書が必要とされる

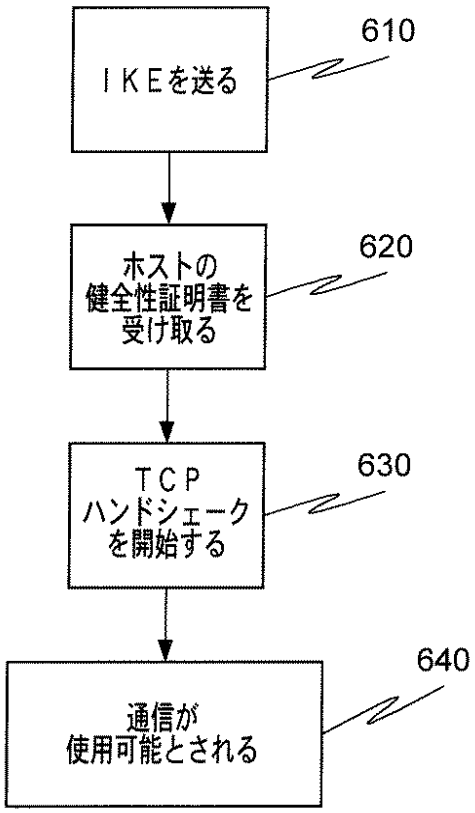
【図４】


410a
410b
410c
SHA
SHA
SHA
420
SHA API
検疫エージェント（QA）
QEC API
430
AFW QEC
470
健全性証明書サーバ
450
証明書ストア
400
WFP IPsec サブシステム
460

【図５】


デスクトップが起動し、IPアドレスを獲得する
510
QECが開始する
520
HCSを見つける
530
HCSにSoHを送る
540
HCSがIASにSoHを送る
550
HCSが応答を受け取る
560
クライアントがSoH応答を受け取る
570
健全性証明書を格納する
580

【図６】


ＩＫＥを送る
610
ホストの
健全性証明書を
受け取る
620
ＴＣＰ
ハンドシェーク
を開始する
630
通信が
使用可能とされる
640

フロントページの続き

(72)発明者　クリストファー　ジェー．ブラック
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ジェスパー　エム．ヨハンソン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　カーティク　エヌ．マーシー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ポール　ジー．メイフィールド
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

Ｆターム(参考)　5B285 AA04　CA06　CA45　CB47　DA09
5J104 EA05　KA01　KA02　KA05　MA01　PA07

【外国語明細書】
2006134312000001.pdf