(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2016-532381
(P2016-532381A)
(43)公表日　平成28年10月13日(2016.10.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5K030
G06F 21/55	(2013.01)	G06F	21/55		

審査請求 未請求　予備審査請求 未請求　（全 33 頁）

(21)出願番号　特願2016-534574 (P2016-534574)
(86)(22)出願日　平成26年3月19日 (2014.3.19)
(85)翻訳文提出日　平成28年4月11日 (2016.4.11)
(86)国際出願番号　PCT/US2014/031244
(87)国際公開番号　WO2015/023316
(87)国際公開日　平成27年2月19日 (2015.2.19)
(31)優先権主張番号　13/967,155
(32)優先日　平成25年8月14日 (2013.8.14)
(33)優先権主張国　米国 (US)

(71)出願人　516045643
チエン　ダニエル
アメリカ合衆国　ワシントン州　９８１０８　シアトル　サウス　ブランドン　コート　２５３４
(74)代理人　100116872
弁理士　藤田　和子
(72)発明者　チエン　ダニエル
アメリカ合衆国　ワシントン州　９８１０８　シアトル　サウス　ブランドン　コート　２５３４

Ｆターム(参考)　5K030 GA15 HA08 HC01 HD03 HD06 HD10 KA05 LD20 MB08

最終頁に続く

(54)【発明の名称】疑わしいネットワーク通信の評価

(57)【要約】
ネットワーク通信から疑わしいネットワークアドレスを識別する。実施形態では、ネットワーク装置は、着信又は発信接続要求、ウェブページ、電子メール又は他のネットワーク通信を受信する。評価モジュールは、対応するネットワークアドレスについてのネットワーク通信を評価し、これは、ネットワーク通信のソース又は宛先についてであってもよい。ネットワークアドレスは、一般的に、ＩＰアドレスを含む。評価モジュールは、時刻、コンテントタイプ、方向性等のようなネットワーク通信の１以上のプロパティを判定する。評価モジュールは、プロパティが、ＩＰアドレスに関連付けられるホワイトリストにおいて特定されるプロパティに基づいて一致する又は許容されるかを判定する。
【選択図】図１

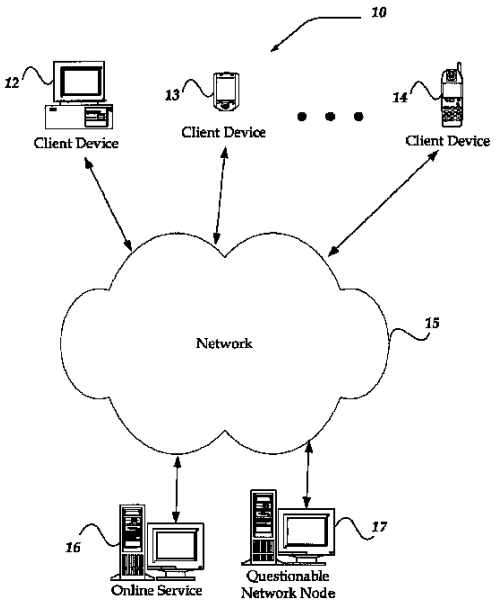


Fig. 1

【特許請求の範囲】
【請求項１】
通信を制御するためのコンピュータシステムにおける方法であって、
認証されないネットワークノードのアドレスを含まず、かつ、信頼できるネットワークアドレスの各々に対して、許容通信プロパティの１以上の指標を含む、信頼できるネットワークアドレスの予め定義されたホワイトリストを受信するステップであって、前記許容通信プロパティは、許容地理的位置の指標の指標、許容プログラムの指標、許容アクセス時間の指標、許容ユーザの指標、許容データタイプの指標及び許容アクセスコントロールの指標のうちの複数を含む、ステップと、
ネットワーク通信に対応する第１のインターネットプロトコル（ＩＰ）アドレスを決定するステップと、
前記ネットワーク通信と関連付けられる第１の通信プロパティを決定するステップと、
前記第１のＩＰアドレスに対応する前記ホワイトリストにおけるエントリにより特定される許容通信プロパティである第２の通信プロパティを決定するステップと、
前記第１の通信プロパティが前記第２の通信プロパティで包含されるかどうかを判定することにより、前記ホワイトリストに対して前記ネットワーク通信を評価するステップと、
前記第１の通信プロパティが前記第２の通信プロパティで包含されないと判定したことに応じて、前記ネットワーク通信が許容されないことの指標を設定するステップと、
前記第１の通信プロパティが前記第２の通信プロパティで包含されると判定したことに応じて、前記ネットワーク通信が許容されることの指標を設定するステップと、
により、前記コンピュータシステムにおいて、前記ネットワーク通信を評価することを含む、方法。
【請求項２】
前記ホワイトリストにおける前記許容通信プロパティは、前記ホワイトリストにおけるそれぞれのネットワークアドレスについて、許容地理的位置の指標を含み、
ゲオロケーション情報プロバイダに問い合わせることにより、前記第１のＩＰアドレスに関連付けられる地理的位置を決定するステップと、
前記第１のＩＰアドレスに関連付けられる地理的位置が、前記ホワイトリストのおけるエントリにより許容可能と示される前記地理的位置に一致する又は包含されるかを判定するステップと、
を更に備える請求項１に記載の方法。
【請求項３】
前記ホワイトリストにおける前記許容通信プロパティは、前記ホワイトリストにおけるそれぞれのネットワークアドレスについて、前記ネットワークアドレスを介して通信可能であるプログラムの指標を含み、前記プログラムの指標は、プログラム名称及び／又はプログラムコードのハッシュを含み、
前記コンピュータシステムで実行しており、かつ前記ネットワーク通信に関与している通信プログラムを判定するステップと、
前記通信プログラムが前記ホワイトリストのおけるエントリにより許容可能と示されるプログラムと一致するか判定するステップと、
を更に備える請求項１に記載の方法。
【請求項４】
前記ホワイトリストにおける前記許容通信プロパティは、前記ホワイトリストにおけるそれぞれのネットワークアドレスについて、許容アクセス時間の指標を含み、
前記ネットワーク通信が生じている時間を求めるステップと、
前記求められた時間が前記ホワイトリストのおけるエントリにより許容可能と示されるアクセス時間と一致する又は包含されるかを判定するステップと、
を更に備える請求項１に記載の方法。
【請求項５】

前記ホワイトリストにおける前記許容通信プロパティは、前記ホワイトリストにおけるそれぞれのネットワークアドレスについて、許容ユーザの指標を含み、
前記ネットワーク通信と関連付けられるユーザを決定するステップと、
前記決定されたユーザが前記ホワイトリストのおけるエントリにより許容可能と示されるユーザと一致する又は包含されるかを判定するステップと、
を更に備える請求項１に記載の方法。
【請求項６】
前記ホワイトリストにおける前記許容通信プロパティは、前記ホワイトリストにおけるそれぞれのネットワークアドレスについて、実行可能なコード、スクリプト、マクロ、オーディオ、ビデオ、画像及びテキストのうちの１つである許容データタイプの指標を含み、
ネットワーク接続を介して転送されるデータに対応するデータタイプを決定するステップと、
前記決定されたデータタイプが前記ホワイトリストのおけるエントリにより許容可能と示されるデータタイプと一致する又は包含されるかを判定するステップと、
を更に備える請求項１に記載の方法。
【請求項７】
前記ホワイトリストにおける前記許容通信プロパティは、前記ホワイトリストにおけるそれぞれのネットワークアドレスについて、非インタラクティブなプログラムが前記ネットワークアドレスを介して通信可能であるかどうかの指標を含み、
前記コンピュータシステムで実行しており、かつ前記ネットワーク通信に関与している通信プログラムを決定するステップと、
前記通信プログラムがインタラクティブ又は非インタラクティブモードで動作しているかを判定するステップと、
を更に備える請求項１に記載の方法。
【請求項８】
ＲＥＣＥＩＶＥＤヘッダフィールドに基づいて前記第１のＩＰアドレスを決定するステップと、
ソース電子メールアドレスに基づいてドメインネームルックアップを実行することにより第２のＩＰアドレスを決定するステップと、
前記第１及び第２のＩＰアドレスが一致するするかどうかを判定し、一致しない場合には、電子メールメッセージが偽のソースアドレスを有することの指標を設定するステップと、
により、受信ＳＭＴＰサーバにより挿入されるＲＥＣＥＩＶＥＤヘッダフィールド、及び送信者側のシステムにおいて挿入されるソース電子メールアドレスを特定するＦＲＯＭヘッダフィールドを有する電子メールメッセージの真正性を評価するステップを更に備える請求項１に記載の方法。
【請求項９】
前記ネットワーク通信は、内部ネットワーク内で生じ、前記第１のＩＰアドレスは、前記内部ネットワークのＩＰアドレスである請求項１に記載の方法。
【請求項１０】
前記ネットワーク通信は、着信ＴＣＰ／ＩＰ接続要求を介して開始される請求項１に記載の方法。
【請求項１１】
前記ネットワーク通信は、発信ＴＣＰ／ＩＰ接続要求を介して開始される請求項１に記載の方法。
【請求項１２】
前記ホワイトリストにおける前記許容通信プロパティは、前記ホワイトリストにおけるそれぞれのネットワークアドレスについて、許容ユーザ及びアクセスコントロールの指標を含み、

前記ネットワーク通信と関連付けられるユーザを決定するステップと、
前記ネットワーク通信と関連付けられるユーザアクセスコントロール権限を決定するステップと、
ユーザＩＰアドレス及び／又はポート番号を決定するステップと、
前記決定されたユーザ、ユーザアクセスコントロール権限及びユーザＩＰアドレス及び／又はポート番号が前記ホワイトリストのおけるエントリと一致する又は包含されるかを判定するステップと、
を更に備える請求項１に記載の方法。
【請求項１３】
前記第１のＩＰアドレスは、顧客コンピュータ装置と関連付けられるＩＰアドレスであり、
前記ネットワーク通信を評価するステップは、
前記第１のＩＰアドレスが、顧客に対応する識別子を有する前記ホワイトリストにより関連付けられるか判定するステップと、
前記第１のＩＰアドレスと関連付けられる地理的位置が、前記第１のＩＰアドレスを有する前記ホワイトリストにより関連付けられる地理的位置に包含されるかを判定するステップと、
を更に備える請求項１に記載の方法。
【請求項１４】
請求項１から１３のいずれか一項に記載の方法をコンピュータ装置に実行させる実行可能な命令を含む非一時的なコンピュータ可読媒体。
【請求項１５】
通信を制御するシステムであって、
ＴＣＰ／ＩＰスタックを含み、ネットワークリソースとの通信のための通信インターフェースと、
命令を記憶するメモリと、
前記通信インターフェース及び前記メモリと通信するプロセッサと、を備え、
前記プロセッサは、請求項１から１３のいずれか一項に記載の方法を実行することにより、ネットワーク通信を評価するように構成される、システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書で開示される発明は、ネットワークセキュリティに関し、より具体的には、ハッカー、侵入者、フィシングソース、ウイルス、電子メール送信者及び／又は他の虚偽又は疑わしいソースから受信される疑わしいネットワーク通信を識別及び妨げることに関する。
【背景技術】
【０００２】
今日、インターネットのようなネットワークを通じて、侵入者、ハッカー、認証されないユーザ、他のコンピュータ、サーバ、ファイアウォール、ルーター、ＰＤＡ、携帯電話機、ゲームコンソール、及びネットワークに接続される他の電子デバイスに侵入しようとするプログラムされたデバイスが存在する。例えば、ウェブサイトサーバ、他のデバイス及びユーザは、ウイルス、ワーム、アドウェア、スパイウェア又は他のファイルをネットワーク上の別の電子デバイスへ送信する。ファイルは、他のデバイスに、ウイルスを拡散する、別のウイルスを得る、機密情報を他者へ送信する、及び／又は他の望まれないアクションを行うために、ウェブサーバのような他の装置へのネットワーク接続を開始する一部のマルウェア（例えば、バックドア、ワーム、トロイの木馬等）を実行させる。事件になる前にこれらのアクションを検出及び防ぐことが望まれている。
【発明の概要】
【０００３】

ファイルは、ウェブベース電子メールシステムのような電子メールによって届けられることが多い。電子メールメッセージは、通常は、“Ｆｒｏｍ”フィールドに送信者の識別子を含むが、送信者の識別子が正当であることを確実にすることは困難である。例えば、フィシング電子メールのＦｒｏｍフィールドは、正規の金融機関のメールサーバを示すように見える送信者のドメインネームを有する電子メールアドレスを含む場合がある。ユーザは、送信者の識別子が真正であるかを判定することは困難である。別のケースでは、ネットワークデバイスは、ウェブページ、ポップアップ広告又は他のデータを届けるために、クライアントデバイスへのアクセスを要求する。要求ネットワークデバイスのドメインネームは、正規の金融機関のサーバを示す。一部のセキュリティソフトウェアは、アドレス情報を有するメッセージをユーザへ提供する。ユーザは、要求を受け入れるかどうかを選択する。しかし、多くのユーザは、送信者のアドレス情報が真正であるかを判定することは困難である。

【０００４】

別の望ましくない行動は、フィシングと呼ばれる。用語「フィシング」は、一般的に、非合法又は不正目的に個人及び／又は機密情報を得ようとすることに関連付けられる。典型的には、虚偽の人物又は団体は、ユーザが個人及び／又は機密情報を入力することができるフィシングウェブサイトへのハイパーリンクを含む１以上の電子メールを送信する。インターネットフィシングウェブサイトは、それらが、企業又は他の団体の実際のオフィシャルウェブサイトに入力していると人々に信じさせる。これらのフィシングウェブサイトは、典型的には、オフィシャルウェブサイトのように見えるそれらのウェブサイトを作ることによりこれを遂行する。一般的なユーザは、そして、彼らがフィシングウェブサイトに情報を送信したことを理解せずに個人／機密情報を与えてしまい、そのオペレーターは、非合法又は不正目的の情報を用いる。フィシングウェブサイトは、通常、実際のオフィシャルウェブサイトに非常に類似するドメインネームを有するｕｎｉｆｏｒｍ ｒｅｓｏｕｒｃｅ ｌｏｃａｔｏｒ（ＵＲＬ）を用いる。ドメインネームは、また、ドメインネームアドレス（ｄｏｍａｉｎ ｎａｍｅ ａｄｄｒｅｓｓ（ＤＮＡ））とも呼ばれる。例えば、フィシングウェブサイトは、人々がこれをＰａｙｐａｌ，Ｉｎｃ．のオフィシャルウェブサイトであると考えるように、ｗｗｗ．ｐａｙｐａｌ．ｂｉｌｌｉｎｇ．ｃｏｍのようなＤＮＡを用いる。オフィシャルに見えるドメインネームの内在するインターネットプロトコル（ＩＰ）アドレスは、一般的に、ユーザを、正規の企業のオフィシャルウェブサイトではないフィシングウェブサイトへ転送する。又は、フィシングウェブサイトは、ハイパーリンクについてのオフィシャル企業のドメインネームを用いるが、ハイパーリンクのフィシングウェブサイトＩＰアドレスを用いる。ユーザが電子メール又はウェブサイトのハイパーリンクをクリックすると、ユーザは、オフィシャルウェブサイトではないフィシングウェブサイトへ向けられる。

【０００５】

インターネット又は他のネットワーク上のリソースは、それらに一意なＩＰアドレスを有する。企業、民間組織、政府機関等を含む団体は、それら独自の一意なＩＰアドレス又はＩＰアドレスの範囲を割り当てられる。フィシングウェブサイトにも同じことが言える。フィシングウェブサイト又は他のネットワークノードは、インターネットＩＰネットワークルーティングメカニズムによる他の誰かのオフィシャルＩＰアドレスであるそのＩＰアドレスを偽装することはできない。フィシングウェブサイトも、フィシングウェブサイトに人々を連れてくるために、その独自のＩＰアドレスを有する必要がある。本発明は、これら及び他の問題に対して関連するものである。

【図面の簡単な説明】

【０００６】

本発明の非限定的かつ非包括的な実施形態は、以下の図面を参照しながら説明される。図面では、同様の参照番号は、特に言及しないかぎり、各種の図面を通じて同様の部位を示す。

【０００７】

本発明をより良く理解するために、添付の図面と共に以下の発明の詳細な説明が参照される。

【０００８】

【図１】図１は、本発明を実施するための環境の一実施形態を示す機能ブロック図を示す。

【図２】図２は、本発明を実装するシステムに含まれるクライアント及び／又はサーバ装置の一実施形態を示す。

【図３】図３は、本発明の一実施形態のアーキテクチャ及び通信シーケンスを示す。

【図４】図４は、本発明の一実施形態のスクリーンショットを示す。

【図５】図５は、本発明の別の実施形態のアーキテクチャ及び通信シーケンスを示す。

【図６】図６は、ネットワーク通信エレベータ処理を示すフローチャートである。

【発明を実施するための形態】

【０００９】

ここで、本発明の実施形態は、本明細書の一部を形成し、図示によって、本発明が実施される特定の実施形態を示す添付の図面を参照することで以下により完全に説明される。しかし、本発明は、多くのことなる形態で具現化されてもよく、本明細書に示される実施形態に限定されるものと解釈されるべきではなく、これらの実施形態は、本開示が十分及び完全になるように提供され、本発明の範囲を当業者に十分に伝えるであろう。特に、本発明は、方法又は装置として具現化されてもよい。したがって、本発明は、全体的にハードウェアの実施形態、全体的にソフトウェアの実施形態又はソフトウェアとハードウェアとを組み合わせた態様の実施形態の形式を取ってもよい。したがって、以下の発明の詳細な説明は、限定的な意味として取られない。

【００１０】

発明の詳細な説明及び特許請求の範囲を通して、以下の用語は、特に明確に記されない限り、本明細書に明示的に関連付けられた意味を取る。本明細書で用いられるような用語“一実施形態”又は“一例の実施形態”は、そう思われるかもしれないが、必ずしも同一の実施形態を指さない。更に、本明細書で用いられるような用語“別の実施形態”は、そう思われるかもしれないが、異なる実施形態を指さない。よって、いかに説明されるように、本発明の各種実施形態は、本発明の範囲又は趣旨から逸脱せずに、明示的に組み合わせられてもよい。

【００１１】

また、本明細書で用いられるような、用語“又は（ｏｒ）”は、特に明確に記されない限り、両立的な“ｏｒ”演算子であり、用語“及び／又は”と等しい。用語“基づいて（ｂａｓｅｄ　ｏｎ）”は、特に明確に記されない限り、排他的ではなく、記載されない追加要素に基づくことを可能にする。また、発明の詳細な説明を通して、“ａ”、“ａｎ”及び“ｔｈｅ”の意味は、複数の参照を含む。“ｉｎ”の意味は、“ｉｎ”及び“ｏｎ”を含む。

【００１２】

本明細書では、用語“クライアント”は、コンピュータモジュールのデータ又はサービスのエンドプロセッサとしての一般的役割を指し、用語“サーバ”は、１以上のクライアントへのデータ又はサービスのプロバイダとしてのコンピュータモジュールの役割を指す。通常、コンピュータモジュールは、あるトランザクションのデータ又はサービスを要求し、クライアントとして機能することが可能であり、別のトランザクションのデータ又はサービスを提供するサーバとして機能することが可能であり、よって、その役割をクライアントからサーバへ又はその逆に変化する。

【００１３】

用語“ウェブ”は、一般的に、デバイス、データ及び／又は他のリソースの集合を指す。１以上のプロトコル、フォーマット、シンタックス、及び／又は、パーソナルコンピュータ、ラップトップコンピュータ、ワークステーション、サーバ、ミニコンピュータ、メインフレーム、携帯電話機、パーソナルデジタルアシスタント（ＰＤＡ）等のようなコン

ピュータデバイスでの使用を意図される他のコンベンションに基づいてネットワークにアクセス可能である。ウェブプロトコルは、ｈｙｐｅｒｔｅｘｔ ｔｒａｎｓｆｅｒ ｐｒｏｔｏｃｏｌ（ＨＴＴＰ）を含むが、これに限定されない。このようなコンベンションは、ｈｙｐｅｒｔｅｘｔ ｍａｒｋｕｐ ｌａｎｇｕａｇｅ（ＨＴＭＬ）及びｅｘｔｅｎｓｉｂｌｅ ｍａｒｋｕｐ ｌａｎｇｕａｇｅ（ＸＭＬ）を含むが、これに限定されない。用語“ウェブページ”及び“ウェブデータ”は、一般的に、ドキュメント、ファイル、アプリケーション、サービス及び／又はウェブコンベンションを確認し、一般的に、汎用ブラウザのようなアプリケーションを実行するコンピュータデバイスでアクセス可能である他のデータを指す。例示的な汎用ブラウザは、Ｍｉｃｒｏｓｏｆｔ ＣｏｒｐｏｒａｔｉｏｎのＩｎｔｅｒｎｅｔ Ｅｘｐｌｏｒｅｒ（登録商標）、Ｎｅｔｓｃａｐｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ ＣｏｒｐのＮｅｔｓｃａｐｅ（登録商標）、及びＭｏｚｉｌｌａ ＦｏｕｎｄａｔｉｏｎのＦｉｒｅｆｏｘ（登録商標）を含む。ウェブページは、一般的に、ウェブページにアクセス可能であるサーチエンジンによってインデックス化される。例示的なサーチエンジンは、Ｇｏｏｇｌｅ， Ｉｎｃ．によるＧｏｏｇｌｅ（登録商標）である。

【００１４】

用語“ＵＲＬ”は、一般的に、ｕｎｉｆｏｒｍ ｒｅｓｏｕｒｃｅ ｌｏｃａｔｏｒを指すが、ｕｎｉｆｏｒｍ ｒｅｓｏｕｒｃｅ ｉｄｅｎｔｉｆｉｅｒ及び／又は他のアドレス情報を含んでもよい。ＵＲＬは、一般的に、ｈｙｐｅｒｔｅｘｔ ｔｒａｎｓｆｅｒ ｐｒｏｔｏｃｏｌ（例えば、“ｈｔｔｐ：／／”）のようなプロトコル、ホストネーム（例えば、“ｎｅｗｓ．ｇｏｏｇｌｅ．ｃｏｍ”）又はドメインネーム（例えば、“ｇｏｏｇｌｅ．ｃｏｍ”）、パス（例えば、“／ｉｎｔｌ／ｅｎ／ｏｐｔｉｏｎｓ”）、及び特定のファイル（例えば、“ｐａｃｋ＿ｉｎｓｔａｌｌｅｒ．ｈｔｍｌ”）又はクエリ文字列（例えば、“？ｈｌ＝ｅｎ”）を識別する。用語“ＵＲＬ”は、名称又はウェブリソースを識別するために用いられる文字列を指す。ＵＲＬとの組み合わせ、これは、ネットワークにおけるウェブリソースを表す。

【００１５】

つまり、本発明の実施形態は、通信の正当性を立証するための既知の信頼できるアドレスのリストに対するネットワークアドレスを評価する。複数の段階のセキュリティが提供される。一実施形態では、最上位の段階は、ＩＰアドレスであり、第２の段階は、ポート番号であり、第３の段階は、通信ペイロードのプロパティである。他の段階は、通信の他の態様と関連付けられてもよい。１以上の段階は、選択的に実装されうる。各段階は、通信を承認するために必要なユーザ関与のレベルと関連付けられてもよい。

【００１６】

動作環境の実例

図１は、本発明が動作する環境の一実施形態を示す。しかし、これらの構成要素の全てが本発明を実施するために必要ではなく、配置及び構成要素の種類は、本発明の趣旨又は範囲から逸脱しない範囲で変更される。

【００１７】

図に示されるように、システム１０は、クライアントデバイス１２－１４と、ネットワーク１５と、オンラインサービス１６と、オンラインサービスと直接的には関連付けられない疑わしいネットワークノード１７と、を含む。ネットワーク１５は、クライアントデバイス１２－１４、オンラインサービス１６及び疑わしいネットワークノード１７のそれぞれと接続され、通信可能である。オンラインサービス１６は、正当なウェブサイト、電子メールサービス、ファイルストレージサービス、ドメインネームアサイメントサービス、ネットワークアドレスアイデンティフィケーションサービス等のための１以上のサーバを備えてもよい。疑わしいネットワークノード１７は、不正ユーザのクライアントデバイス、コンピュータウィルスのソース、別のサイトとして装ったウェブサイト用の１以上のサーバ、ハッカーによって不正アクセスされている有効なネットワークノード、又は不正若しくは虚偽目的のために用いられる別のネットワークノードを備えてもよい。各ネット

ワークノードは、各ネットワークノードに一意なＩＰアドレスのようなネットワークアドレスを有する。ネットワークアドレスは、また、一般的に、特定の通信セッション、ネットワークノード内の特定のリソース、又はノード間で適切に通信を可能にするためのネットワークアドレスに対する他の改善を識別するためのポート番号を含む。真正なネットワークアドレスは、ネットワークノードへ又はネットワークノードからの通信のために必要とされる。アドレスマスキング、ドメインネームトランスレーション及び他のスキームは、通信経路に沿った各種ポイントでのネットワークアドレスを偽装する。しかし、真正なネットワークアドレスは、いくつかのポイントから生成される、又は通信は、意図したノード間で発生しない。

【００１８】

クライアントデバイス１２－１４は、ネットワーク１５のようなネットワークにおいて、互いに、メッセージをオンラインサービス１６のようなコンピュータデバイスへ又はコンピュータデバイスから送受信すること等を可能にするコンピュータデバイスを事実上含んでもよい。このようなデバイスのセットは、通常、一般的なデバイスとみなされ、かつ典型的にはパーソナルコンピュータ、マルチプロセッサシステム、マルチプロセッサベース又はプログラマブルコンシューマエレクトロニクス、ネットワークＰＣ等のような有線通信媒体を用いて接続するデバイスを含んでもよい。このようなデバイスのセットは、また、通常、特化したデバイスとみなされ、かつ携帯電話機、スマートフォン、ページャー、ウォーキートーキー、無線（ＲＦ）デバイス、赤外線デバイス、ＣＢ、前述のデバイスの１以上を組み合わせた集積デバイス、又はバーチャルなモバイルデバイス等のような無線通信媒体を用いて接続するデバイスを含んでもよい。同様に、クライアントデバイス１２－１４は、パーソナルデジタルアシスタント（ＰＤＡ）、ＰＯＣＫＥＴ　ＰＣ、ウェアラブルコンピュータ及び有線及び／又は無線通信媒体に亘って通信するために装備される任意の他のデバイスのような有線又は無線通信媒体を用いて接続可能な任意のデバイスであってもよい。

【００１９】

クライアントデバイス１２－１４内の各クライアントデバイスは、ユーザが設定を制御可能であり、処理を実行するためにクライアントデバイスに指示可能であるユーザインタフェースを含む。各クライアントデバイスは、また、ウェブページ、ウェブベースメッセージ等を送受信するように構成されるブラウザアプリケーションを含んでもよい。ブラウザアプリケーションは、これらに限定されないが、Ｓｔａｎｄａｒｄ　Ｇｅｎｅｒａｌｉｚｅｄ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ（ＳＧＭＬ）、ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ（ＨＴＭＬ）、Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ（ＸＭＬ）、ｗｉｒｅｌｅｓｓ　ａｐｐｌｉｃａｔｉｏｎ　ｐｒｏｔｏｃｏｌ（ＷＡＰ）、Ｈａｎｄｈｅｌｄ　Ｄｅｖｉｃｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ（ＨＤＭＬ）、例えば、Ｗｉｒｅｌｅｓｓ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ（ＷＭＬ）、ＷＭＬＳｃｒｉｐｔ、ＪａｖａＳｃｒｉｐｔ（登録商標）等を含む、事実上ウェブベースの言語を用いて、グラフィック、テキスト、マルチメディア等を受信及び表示するように構成されてもよい。クライアントデバイス１２－１４は、更に、これらに限定されないが、インスタントメッセージング（ＩＭ）、ショートメッセージサービス（ＳＭＳ）メッセージング、マルチメディアメッセージサービス（ＭＭＳ）メッセージング、インターネットリレーチャット（ＩＲＣ）、Ｍａｒｄａｍ－Ｂｅｙ’ｓインターネットリレーチャット（ｍＩＲＣ）、Ｊａｂｂｅｒ等を含む、同一又は異なる通信ノードを用いて、クライアントデバイスが他のコンピュータデバイスからメッセージを送受信することを可能にする通信インターフェースで構成されてもよい。

【００２０】

ネットワーク１５は、通信可能にするために１つのコンピュータデバイスを別のコンピュータデバイスと結合するように構成される。ネットワーク１５は、１つの電子デバイスから別の電子デバイスへ情報を伝えるための任意の形式のメディアを用いることを可能にする。また、ネットワーク１５は、インターネットインターフェースのような有線インタ

ーフェース、及び／又はセルラーネットワークのような無線インターフェース、加えて、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、ユニバーサルシリアルバス（ＵＳＢ）ポート、他の形式のコンピュータ可読媒体を通じたダイレクトコネクションへのインターフェース、又はそれらの組み合わせ等を含んでもよい。異なるアーキテクチャ及びプロトコルに基づくものを含むインターコネクトされたＬＡＮのセットで、ルーターは、メッセージが一方から他方へ送信されることを可能にするＬＡＮ間のリンクとして機能する。また、ＬＡＮ内の通信リンクは、典型的には、ツイストペア線又は同軸ケーブルを含むが、ネットワーク間の通信リンクは、無線での携帯電話信号、アナログ電話線、Ｔ１、Ｔ２、Ｔ３及びＴ４を含む全て又は一部の専用デジタル線、Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ ｌｅｖｅｌ ３（ＤＳ３）、Ｏｐｔｉｃａｌ Ｃａｒｒｉｅｒ ３（ＯＣ３）、ＯＣ１２、ＯＣ４８、Ａｓｙｎｃｈｒｏｎｏｕｓ Ｔｒａｎｓｆｅｒ Ｍｏｄｅ（ＡＴＭ）、Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅｓ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋｓ（ＩＳＤＮｓ）、Ｄｉｇｉｔａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｌｉｎｅｓ（ＤＳＬｓ）、衛生リンクを含む無線リンク、又は当業者にとって同等及び／又は当業者に知られている他の通信リンクを用いてもよい。更に、リモートコンピュータ及び他の関連する電子デバイスは、モデム及び一時的な電話リンクを介してＬＡＮ又はＷＡＮとリモート接続されうる。本質的には、ネットワーク１５は、クライアントデバイス１２－１４、オンラインサービス１６及び／又は疑わしいネットワークノード１７間を伝わる情報による任意の通信方法を含む。ネットワーク１５は、ｔｒａｎｓｍｉｓｓｉｏｎ ｃｏｎｔｒｏｌ ｐｒｏｔｏｃｏｌ／ｉｎｔｅｒｎｅｔ ｐｒｏｔｏｃｏｌ（ＴＣＰ／ＩＰ）、ｕｓｅｒ ｄａｔａｇｒａｍ ｐｒｏｔｏｃｏｌ（ＵＤＰ）、ＷＡＰ、ｃｏｄｅ ｄｉｖｉｓｉｏｎ ｍｕｌｔｉｐｌｅ ａｃｃｅｓｓ（ＣＤＭＡ）、ｇｌｏｂａｌ ｓｙｓｔｅｍ ｆｏｒ ｍｏｂｉｌｅ ｃｏｍｍｕｎｉｃａｔｉｏｎｓ（ＧＳＭ（登録商標））等を含む各種の通信プロトコルでの使用のために構築される。

【００２１】

上述したような通信リンクにおける情報を送信するために用いられるメディアは、一般的に、コンピュータデバイスによってアクセスされうる任意のメディアを含む。コンピュータ可読メディアは、コンピュータストレージメディア、有線及び無線通信メディア、又はそれらの組み合わせを含んでもよい。また、コンピュータ可読メディアは、典型的には、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又はプロセッサに提供されうる他のデータを記憶及び／又は搬送する。コンピュータ可読メディアは、搬送波のような変調されたデータ信号、データ信号を送信するための送信メディア又は他の搬送機構及び情報伝達メディアを含んでもよい。用語“変調されたデータ信号（ｍｏｄｕｌａｔｅｄ ｄａｔａ ｓｉｇｎａｌ）”及び“搬送波信号（ｃａｒｒｉｅｒ－ｗａｖｅ ｓｉｇｎａｌ）”は、その特徴セットの１以上を有する又は情報、命令、データ等を信号にエンコードするための方法で変更された信号を含む。実施例により、通信メディアは、音響、ＲＦ、赤外線及び他の無線メディアのような無線メディア、及びツイストペア線、同軸ケーブル、ファイバーオプティクス、ウェーブガイド及び他の有線メディアのような有線メディアを含む。

【００２２】

電子デバイスの一実施形態は、図２と共に以下に詳細に説明される。説明の目的のために、汎用クライアントコンピュータデバイスが一例として説明される。しかし、サーバデバイス、特化した用途のデバイス（例えば、携帯電話機）、及び／又は他の電子デバイスが本発明の実施形態に用いられてもよい。この例では、クライアントデバイス２０は、ユーザが、クライアントデバイス、ポータルサーバ１６及び／又は疑わしいネットワークノード１７のような他のネットワークリソースと通信することを可能にするために、ネットワーク１５との接続を可能にするコンピュータデバイスを含んでもよい。クライアントデバイス２０は、図示されるものよりも多数の構成要素を含んでもよい。しかし、図示される構成要素は、本発明を実施するための例示的な実施形態を開示するのに充分である。クライアントデバイス２０の構成要素の多くは、また、オンラインサービス１６のサーバ、

疑わしいネットワークノード１７のサーバ、及び／又は他の電子デバイスで重複してもよい。

【００２３】

図に示されるように、クライアントデバイス２０は、バス２３を介して大容量メモリ２４と通信されるプロセッシングユニット２２を含む。大容量メモリ２４は、一般的に、ＲＡＭ２６、ＲＯＭ２８及び他のストレージ手段を含む。大容量メモリ２４は、コンピュータ可読メディアの一種、つまり、コンピュータストレージメディアを示す。コンピュータストレージメディア（“コンピュータ可読媒体”とも呼ばれる）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又は他のデータのような情報の蓄積のための方法又は技術で実行される揮発性及び不揮発性、リムーバブル及びノンリムーバブルメディアを含んでもよい。コンピュータストレージメディアの他の例は、ＥＥＰＲＯＭ、フラッシュメモリ又は他の半導体メモリ技術、ＣＤ－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ）又は他の光学ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ又は所望の情報を記憶するために用いられ、コンピュータデバイスによりアクセスされうる他の磁気ストレージデバイス、又は他の媒体を含む。コンピュータストレージメディアは、一時的又は非一時的データ及び／又は信号を記憶してもよい。

【００２４】

大容量メモリ２４は、クライアントデバイス２０の低レベル処理を制御する基本入／出力システム（“ＢＩＯＳ”）３０を記憶する。大容量メモリ２４は、また、クライアントデバイス２０の処理を制御するオペレーティングシステム３１を記憶する。この構成要素は、Ｗｉｎｄｏｗｓ（登録商標）、ＵＮＩＸ（登録商標）、ＬＩＮＵＸ（登録商標）のバージョン等のような汎用オペレーティングシステムを含んでもよいことが理解されるであろう。オペレーティングシステムは、また、ハードウェアコンポーネント及び／又はアプリケーションプログラムを介したオペレーティングシステム処理の制御を可能にするバーチャルマシンモジュールを含む又はバーチャルマシンモジュールとインターフェース接続してもよい。

【００２５】

大容量メモリ２４は、とりわけ、プログラム３４及び／又は他のデータを記憶するためにクライアントデバイス２０によって用いられうる１以上のデータストレージユニット３２を更に含む。プログラム３４は、ＨＴＴＰ通信を送信、受信及び処理するためのＨＴＴＰハンドラーアプリケーションを実装するためにクライアントデバイス２０によって実行されうるコンピュータ実行可能な命令を含んでもよい。同様に、プログラム３４は、安全な手法で外部アプリケーションとの通信を開始するようなセキュアな接続を扱うＨＴＴＰＳハンドラーアプリケーションを含みうる。アプリケーションプログラムの他の例は、スケジューラー、カレンダー、ウェブサービス、トランスコーダー、データベースプログラム、ワードプロセッシングプログラム、スプレッドシートプログラム等を含む。したがって、プログラム３４は、ウェブページ、オーディオ、ビデオを処理し、他の電子デバイスの他のユーザとの通信を可能にする。

【００２６】

また、大容量メモリ２４は、メッセージングのための１以上のプログラム及び／又は他のアプリケーションを記憶する。メッセージングクライアントモジュール３６は、電子メール、インスタントメッセージング、ＳＭＳ及び／又は他のメッセージングサービスを可能にするために、オペレーティングシステム３１の制御下で実行されるコンピュータ実行可能な命令を含んでもよい。同様に、クライアントデバイス２０に酷似して構成されるサーバデバイス（及び／又はクライアントデバイス２０自体）は、ルーティング、アクセスコントロール及び／又は他のサーバ側のメッセージングサービスを提供するメッセージングサーバモジュール３７を含んでもよい。クライアントデバイス２０は、一般的に、有効な送信者、要求及び／又は他のデータのための通信を評価する評価モジュール３８を更に含んでもよい。一実施形態では、評価モジュール３８は、クライアントデバイス２０が、フィッシングウェブサイトのネットワークアドレスを識別することを可能にするために、

フィッシングウェブサイトと相互作用し、ネットワークアドレスが非合法なウェブサイトと関連付けられるかどうかを判定するアンチフィッシングモジュールを含んでもよい。別の例の実施形態は、認証モジュールを含み、これは、電子メールメッセージ、ファイルダウンロード、リディレクション及び／又は他の通信をチェックしてもよい。評価モジュール３８は、他のアプリケーションとは別に実装されてもよく、別のアプリケーション（例えば、ブラウザ）へのプラグインとして実装されてもよく、別のアプリケーション（例えば、電子メールアプリケーション）内に直接的に実装されてもよく、サーバアプリケーションとして、及び／又は他の形態で実装されてもよい。

【００２７】

クライアントデバイス２０は、また、図２に示されないキーボード、マウス、ホイール、ジョイスティック、ロッカースイッチ、キーパッド、プリンター、スキャナー及び／又は他の入力デバイスのような入／出力デバイスと通信するための入／出力インターフェースを含む。クライアントデバイス２０のユーザは、オペレーティングシステム３１及び／又はプログラム３４－３８とは別々の又は集積されるユーザインターフェースと相互作用するために入／出力デバイスを使用することができる。ユーザインターフェースとの相互作用は、ディスプレイ及びビデオディスプレイアダプタ４２を介したビジュアルインタラクションを含む。

【００２８】

パーソナルコンピュータのような一部のクライアントデバイスについて、クライアントデバイス２０は、コンピュータ可読ストレージメディアのためのリムーバブルメディアドライブ４４及び／又はパーマネントメディアドライブ４６を含んでもよい。リムーバブルメディアドライブ４４は、光学ディスクドライブ、フロッピーディスクドライブ及び／又はテープドライブの１以上を備えてもよい。パーマネント又はリムーバブルストレージメディアは、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又は他のデータのような情報の蓄積のための方法又は技術で実装される揮発性、不揮発性、リムーバブル及びノンリムーバブルメディアを含んでもよい。コンピュータストレージメディアの例は、ＣＤ－ＲＯＭ４５、デジタルバーサタイルディスク（ＤＶＤ）又は他の光学ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ又は他の磁気ストレージデバイス、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ，フラッシュメモリ又は所望の情報を記憶するために用いられ、コンピュータデバイスによってアクセスされうる他のメモリ技術又は任意の他の媒体を含んでもよい。

【００２９】

ネットワーク通信インターフェースユニット４８を介して、クライアントデバイス２０は、インターネット、ローカルエリアネットワーク、有線電話ネットワーク、携帯電話ネットワーク又は図１のネットワーク１５のような一部の他の通信ネットワークと通信しうる。ネットワーク通信インターフェースユニット４８は、時折、トランシーバ、トランシービングデバイス、ネットワークインターフェースカード（ＮＩＣ）等としても知られている。

【００３０】

例示的な実装

ネットワークアドレスをユーザが覚えやすくするために、ｗｗｗ．ｃｎｎ．ｃｏｍのようなドメインネームは、数字ＩＰアドレスと関連付けられる。ドメインネームは、また、ドメインネームアドレス（ｄｏｍａｉｎ　ｎａｍｅ　ａｄｄｒｅｓｓ（ＤＮＡ））とも呼ばれる。追加情報は、マークアップドキュメント、画像、又は他のデータのようなリソースのネットワーク位置を特定する数字のｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ（ＵＲＬ）と関連付けられるｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｉｄｅｎｔｉｆｉｅｒ（ＵＲＩ）を特定するために、パスのようなドメインネームへ追加されてもよい。セントラルデータベースは、典型的には、ＩＰアドレスと対応するドメインネームとの関連性を維持するために用いられる。一般的に、ドメインネームサーバ（ＤＮＳ）、インターネットサービスプロバイダ（ＩＳＰ）又は他のデータベースは、この関連性を維持する。

インターネットを含む実施形態の例では、Ｉｎｔｅｒｎｅｔ Ｃｏｒｐｏｒａｔｉｏｎ ｆｏｒ Ａｓｓｉｇｎｅｄ Ｎａｍｅｓ ａｎｄ Ｎｕｍｂｅｒｓ（ＩＣＡＮＮ）、Ｉｎｔｅｒｎｅｔ Ａｓｓｉｇｎｅｄ Ｎｕｍｂｅｒｓ Ａｕｔｈｏｒｉｔｙ（ＩＡＮＡ）又は他のアサイン団体のような団体は、ドメインネームとＩＰアドレスとの関連性を維持する。所有者名、国及び／又は他の情報も各ＩＰアドレスと関連付けられる。

【００３１】

複数の実施形態は、疑わしいネットワークノードを識別することが可能である。例えば、本発明の実施形態は、フィッシングウェブサイトを識別することができる。以下に限定されないが、２つの例が以下に説明される。

【００３２】

１．フィッシングウェブサイトＩＰアドレス－フィッシングウェブサイトがそのＩＰアドレスをクライアントに直接提供する場合、ＩＰアドレスは、ローカルデータベース又はアサイン権限でチェックされる。ローカルアサイメントデータベース又はＩＣＡＮＮ、ＩＡＮＡ又は他のアサイン団体のデータベースに対してウェブサイトのＩＰアドレスを問い合わせることにより、ウェブサイトの所有者は、識別される。

【００３３】

２．フィッシングウェブサイトドメインネーム－一般的に、ＩＰアドレスは、通常、直接的には提供されない。その代わり、ｗｗｗ．ｃｎｎ．ｃｏｍのようなドメインネームは、通常、提供される。ＤＮＳに対してドメインネームを問い合わせることにより、対応するＩＰアドレスを探すことができる。ローカルアサイメントデータベース又はＩＣＡＮＮ、ＩＡＮＡ又は他のアサイン団体のデータベースに対してＩＰアドレスを問い合わせることにより、ウェブサイトの所有者は、識別される。当業者は、２つのステップが単一のサービスによってなされてもよいことを理解するであろう。

【００３４】

複数の実施形態は、また、異なるアプリケーションも可能にする。以下に限定されないが、３つの例が以下に説明される。

【００３５】

Ａ）組み込み機能－アプリケーションプログラムは、ドキュメントにおけるリンクを評価する組み込み機能を含む。例えば、電子メールプログラム、ＩＭプログラム又はワードプロセッシングプログラムは、メッセージ又はドキュメントにおけるリンクを評価するための組み込み機能をアクティベートするためにメニューオプション又はボタンを含む。ユーザは、機能をアクティベートする、又は機能は、ドキュメント内にリンクを検出すると自動的に実行してもよい。機能は、ＩＰアドレス及びポート番号に戻るリンクと関連付けられるアドレスにアクセスする。機能は、所有者の名称及び国名を得るために、ローカル又はリモートアサイメントデータベースを問い合わせる。機能は、ユーザが、リンクに及び／又は予め設定された画面位置マウスポインタを配置したとき等に、所有者の名称及び国名を表示してもよい。機能は、追加又は代替的に、所有者の名称及びアドレスを、ドメインネームと関連付けられる既知の所有者のデータベースと比較してもよい。マウスオーバー又は予め設定された画面位置で警告が表示される。

【００３６】

Ｂ）ブラウザ表示－ブラウザは、１以上の新たなフィールドを提供するために、直接又はプラグインで変更され、ブラウザで表される現在のＵＲＬ又はウェブページと関連付けられるＩＰアドレス及び所有者の名称及び国名を示す。また、ブラウザは、現在のドメインネームの所有者が、ドメインについての既知の所有者及び国名と一致しない場合には、視覚、音響又は他の警告を発してもよい。

【００３７】

Ｃ）オンラインサービス－ユーザは、ウェブページフィールドを通じてオンラインクエリサービスへＵＲＬ又はドメインネームを送信し、ドメインネームの実際の名称及び国名を受信することができる。オンラインサービスは、ＩＰアドレスを取得するためにＵＲＬにアクセスするリスクを取る。オンラインサービスは、更なる評価のために送信ユーザの

クライアントへＩＰアドレスをリターンしてもよい。それに代えて、オンラインサービスは、所有者の名称及び国名を判定し、この情報を、送信されたドメインネームに対応する既知の所有者及び国名のデータベースと比較してもよい。オンラインサービスは、その後、所有者の名称及び国名を送信ユーザのクライアントへ送信する。オンラインサービス又はクライアントウェブページは、ドメインネームが、ドメインネームの所有者の実際の名称及び国名と関連付けられていない場合には、ユーザに警告を発する。

【００３８】

ここで、所有者及び国名を判定するための更なる詳細が提供される。ＩＰアドレス（例えば、ＩＰ　Ｖ４又はＶ６について）は、一般的に、委託されて割り当てられる。ユーザは、ＩＳＰによりＩＰアドレスを割り当てられる。ＩＳＰは、一般的に、ローカルインターネットレジストリ（ＬＩＲ）から、ナショナルインターネットレジストリ（ＮＩＲ）、又は１以上の適切なリージョナルインターネットレジストリ（ＲＩＲ）からのＩＰアドレスのアロケーションを取得する。

【００３９】

ＡｆｒｉＮＩＣ（Ａｆｒｉｃａｎ　Ｎｅｔｗｏｒｋ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｃｅｎｔｒｅ）－－アフリカ地域（ｈｔｔｐ　：／／ｗｗｗ．ａｆｒｉｎｉｃ．ｎｅｔ／）

ＡＰＮＩＣ（Ａｓｉａ　Ｐａｃｉｆｉｃ　Ｎｅｔｗｏｒｋ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｃｅｎｔｒｅ）－－アジア／太平洋地域（ｈｔｔｐ：／／ｗｗｗ．ａｐｎｉｃ．ｎｅｔ／）

ＡＲＩＮ（Ａｍｅｒｉｃａｎ　Ｒｅｇｉｓｔｒｙ　ｆｏｒ　Ｉｎｔｅｒｎｅｔ　Ｎｕｍｂｅｒｓ）－－北アメリカ地域（ｈｔｔｐ　：／／ｗｗｗ．ａｒｉｎ．ｎｅｔ／）

ＬＡＣＮＩＣ（Ｒｅｇｉｏｎａｌ　Ｌａｔｉｎ－　Ａｍｅｒｉｃａｎ　ａｎｄ　Ｃａｒｉｂｂｅａｎ　ＩＰ　Ａｄｄｒｅｓｓ　Ｒｅｇｉｓｔｒｙ）－－ラテンアメリカ及び一部のカリブ海諸島（ｈｔｔｐ：／／ｌａｃｎｉｃ．ｎｅｔ／ｅｎ／ｉｎｄｅｘ．ｈｔｍｌ）

ＲＩＰＥ　ＮＣＣ（Ｒｅｓｅａｕｘ　ＩＰ　Ｅｕｒｏｐｅｅｎｓ）－－欧州、中東及び中央アジア（ｈｔｔｐ：／／ｗｗｗ．ｒｉｐｅ．ｎｅｔ／）。

【００４０】

レジストリ団体は、典型的には、ドメインネームとＩＰアドレスとの関連性を維持するサーバを動作する。このようなサーバは、“ｗｈｏｉｓ”サーバとも呼ばれることがある。上記のウェブサイトサーバの１以上に問い合わせることにより、ＩＰアドレスの所有者の名称及び国名が見つけられうる。問い合わせは、ＨＴＴＰ要求を適切なサーバに送信し、応答を得るブラウザを有することにより行われうる。それに代えて、クライアントブラウザデータベースのような１つのローカルデータベース又は他のローカル又はキャッシュデータベースは、より容易かつ速く問い合わせをするために、“ｗｈｏｉｓ”サーバの１つ又は全てのデータベースを含みうる。所有者及び／又は国名が識別されると、ユーザ又は自動化された処理は、ウェブサイトが真正であるか又はフィッシングウェブサイトであるかを判定しうる。

【００４１】

同様のＤＮＳデータベース、パブリックｗｈｏｉｓデータベースは、全面的に信頼性できない場合がある。フィッシングウェブサイトの所有者は、所有者自身のレジストリを利用して、ｗｈｏｉｓレジストリに登録する場合がある。この潜在的な問題に対抗するために、ローカルデータベースは、“ｗｈｏｉｓ”サーバからの情報を補う又は置き換えるために用いられてもよく、所有者の名称の解明を促進する。例えば、正規の国名は、“ｗｈｏｉｓ”サーバから明示的に認識されない場合がある。補助データベースは、ＩＰアドレスに沿ったこの国名についてのユニークコードのようなより正確な情報を提供することができる。その別の例では、正規の金融機関、企業又は政府機関は、この補助データベースに追加される前に、別々に照合及び認証されうる。

【００４２】

一部の状況では、ＩＰアドレスは、プロキシサーバ、ネットワークアドレストランスレーション（ＮＡＴ）サーバ、ファイアウォール及び／又は他のネットワーク中継を識別す

る。可能性のあるフィッシングウェブサイト（又は他の正規のリソース）の真正なＩＰアドレスを見つけるために、ネットワーク中継デバイス、その所有者又は他の認証されたエントリは、１以上の中継マッピングテーブル、ログファイル及び／又は他のマッピングデータをチェックする。この中継マッピングデータから、認証されたエントリは、タイムスタンプ及び／又はＴＣＰポート番号を内部ＩＰアドレス情報へマッピングする。内部ＩＰアドレスは、名称、位置及び／又は他の内部情報を決定するために内部的に割り当てられた名称に対してチェックされうる。このような内部情報を取得することは、一般的に、インターネットサービスプロバイダから、ネットワーク中継の所有者から、及び／又は他のソースからの協調を含む。この追加内部情報は、ウェブサイトが有効であるか又はフィッシングウェブサイトであるかを判定するために、クライアント又は信頼できる評価サービスへ提供されうる。

【００４３】

一実施形態では、ログファイル又はマッピングデータは、逆引きのための以下の情報を有してもよい。１．タイムスタンプ２．可能性のあるフィッシングウェブサイト、可能性のあるハッカーのアカウント、内部ファイル、及び／又は別の内部リソースへの内部ＩＰアドレスのような内部／ローカルデータ３．インターネットソース及び／又は宛先ＩＰアドレス、ソース及び／又はＴＣＰ／ＵＤＰポート番号、及び／又は可能性のあるフィッシングウェブサイト、可能性のあるハッカーのアカウント及び／又は別のソースへのマッピング情報を識別する他のデータのような外部ネットワークデータ例えば、中継ゲートウェイログファイルは、スパム送信者が、フィッシングウェブサイトへのリンクを有する電子メールを送信したソースＩＰアドレス及びソースＴＣＰポート番号を含んでもよい。ログファイルは、また、電子メールメッセージが送信された宛先ＩＰアドレス及び宛先ポート番号を含んでもよい。同様に、ログファイルは、中継ゲートウェイログファイルを含んでもよく、中継ゲートウェイログファイルは、ハッカーが宛先ＩＰアドレス及び宛先ポート番号にアクセスしようとしたソースＩＰアドレス及びソースＴＣＰポート番号を含んでもよい。頻繁に、ポート番号８０又は４４３が用いられる。これらのポート番号がリターンされない場合、リンクは、フィッシングウェブサイトと関連付けられている可能性がある。逆に、有効なウェブサイトが、８０又は４４３以外のポート番号を用いており、リターンされるポート番号が８０又は４４３である場合、対応するリンクは、フィッシングウェブサイトと関連付けられている可能性がある。

【００４４】

図３は、本発明の一実施形態についてのアーキテクチャ、通信シーケンス及び方法を示す。図示されたモジュールの全てが本発明を実施するために要求されなくてもよい、又は追加のモジュールが別の実施形態に含まれてもよい。各種実施形態では、一部のモジュールは、組み合わせられる一方で、他のモジュールは、複数のモジュールに分割されてもよい。

【００４５】

この例の実施形態では、アーキテクチャは、パブリックインターネット１５ａを通じて、フィッシングウェブサイトに対応するＩＰアドレスウェブサーバへ伝えるクライアント２０ａを含む。クライアント２０ａは、インターネット１５ａ及びＴＣＰ／ＩＰスタック３３と接続するオペレーティングシステム３１を含む。ＴＣＰ／ＩＰスタック３３は、アンチフィッシングモジュール３８ａと接続されるウェブブラウザ３４ａと接続される。アンチフィッシングモジュールは、ネットワークアドレス５０と接続され、クライアント２０ａのローカルデータベースである、又はローカルネットワーク又はインターネット１５ａを通じて利用可能なネットワークアドレスレジストリデータベースのようなリモートネットワークデータベースであってもよい。ネットワークアドレスデータベース５０は、一般的に、ＩＰアドレス及びドメインネームとそれらの所有者との関連性を記憶する。

【００４６】

クライアント２０ａのユーザは、リンクを含む電子メールを受信する、又はブラウザ３４ａにより表されるウェブページのリンクを閲覧してもよい。リンクは、有効に見えるが

、ユーザは、リンクの有効性を確信していなくてもよい。ユーザは、リンクにマウスポインタを配置する又はリンクを選択してもよい。一実施形態では、ユーザは、リンクのマウスポインタを配置し、マウスの右ボタンを押して、メニューオプションを選択し、リンクをチェックするためにアンチフィッシングモジュール３８ａを呼び出す。別の実施形態では、ユーザは、単に、リンクを選択してもよい。以下の説明は、ユーザがウェブブラウザ３４ａを通じてリンクを選択する実施形態を説明する。しかし、当業者は、電子メール及び／又は他のアプリケーションのようなメッセージングサービスが用いられてもよいことを理解するであろう。同様に、当業者は、リンクの受動的なチェックが、右マウスボタンが押されたときに、利用可能なメニューオプションを通じて行われてもよいことを理解するであろう。

【００４７】

この実施形態の例では、ブラウザ３４ａは、リンクのユーザ選択を検出し、通信ステップ１０１における対応するウェブページに対する要求を送信する。要求は、先ず、ＩＰアドレスへのリンクＵＲＬを解決するためにＴＣＰ／ＩＰスタック３３へ送信される。ＵＲＬを解決することは、ネットワークアドレスレジストリデータベース、インターネットサービスプロバイダ（ＩＳＰ）又はその対応するＩＰアドレスとＵＲＬを関連付ける他のソースへのアクセスを要求してもよい。しかし、このようなソースからのＩＰアドレスは、マスクされる又は欺かれる場合がある。また、ポート番号は、ＵＲＬを解決するために取得される必要はない。真正なＩＰアドレス及びポート番号が取得されることを確実にするために、ＴＣＰ／ＩＰスタック３３は、通信ステップ１０２において、オペレーティングシステム３１ａを通じた要求を送信し、オペレーティングシステムは、通信ステップ１０３において、インターネットを通じて、疑わしいネットワークノード１７ａへのＴＣＰ接続をする。

【００４８】

疑わしいネットワークノード１７ａ（例えば、その対応するサーバ）は、通信ステップ１０４において、要求されたウェブページをリターンする。また、リターンされるのは、フィッシングウェブサイトの正確なＩＰアドレス及びポート番号である。クライアントオペレーティングシステム３１ａは、通信ステップ１０５において、ウェブページ、アドレス及びポート番号を受信し、この情報をＴＣＰ／ＩＰスタック３３にパスする。ＴＣＰ／ＩＰスタックは、通信ステップ１０６において、ウェブページをブラウザ３４ａにパスする。通信ステップ１０７において、ブラウザは、ＴＣＰ／ＩＰスタックからのＩＰアドレス及びポート番号を要求する。例えば、ブラウザは、ＧｅｔＩＰＡｄｄｒｅｓｓＢｙＮａｍｅオブジェクト又はＧｅｔＨｏｓｔＢｙＮａｍｅオブジェクトを呼び出す。ＴＣＰ／ＩＰスタックは、通信ステップ１０８において、ＩＰアドレス及びポート番号をブラウザへリターンする。

【００４９】

ブラウザ３４ａは、通信ステップ１０９において、その後、ＩＰアドレス、ポート番号及びＵＲＬ（又はドメインネーム又はホストネーム）をアンチフィッシングモジュール３８ａへパスする。アンチフィッシングモジュールは、通信ステップ１１０において、データベース５０から所有者名称、国名及び／又は他の識別データを要求するために、この情報を用いる。データベース５０は、通信ステップ１１１において、要求された情報をアンチフィッシングモジュール３８ａにリターンする。アンチフィッシングモジュール３８ａは、表示のために、情報をブラウザ３４ａに直接的にパスする。しかし、一実施形態では、アンチフィッシングモジュール３８ａは、所有者名称及び国名が、ＵＲＬのドメインネームについての既知の情報と一致するかを判定する。一致しない場合には、通信ステップ１１２において、アンチフィッシングモジュールは、警告を表示するために、ブラウザ３４ａに対して命令を送信する。

【００５０】

図４は、本発明の一実施形態についてのウェブページ２００のスクリーンショットを示す。この例では、フィッシングウェブサイトは、Ｐａｙｐａｌ，　Ｉｎｃ．のような企業

のオフィシャルウェブサイトを装っている。ｕｎｉｆｏｒｍ ｒｅｓｏｕｒｃｅ ｌｏｃａｔｏｒ（ＵＲＬ）２０２は、ブラウザアドレスフィールドに示される。当該ＵＲＬは、勝手に送りつけられた電子メールからのハイパーリンクを介してアクセスされた。ＵＲＬのドメインネームと関連付けられたＩＰアドレスは、６８．１４２．２３４．５９である。関連付けられたＩＰアドレスの所有者名称２０４及び国名２０６は、ブラウザアドレスフィールドに示されるドメインネームアドレスの近傍に表示される。ユーザ、アンチフィッシングプラグイン及び／又は他の決定モジュールは、真正性を判定するために、所有者の名称及び国名をドメインネームと比較してもよい。一部の比較は、相対的に容易である。例えば、ＩＰ所有者名称が不明な団体又は個人名称であり、ドメインネームがよく知られた企業を示す場合ドメインネームの真正な所有者であるＩＰ所有者に対する重み付けされた決定である。同様に、ＩＰ所有者が、偽装活動の履歴を有するものである、又は既知の企業の本国から程遠い場合、ドメインネームの真正な所有者であるＩＰ所有者に対する更なる重み付けが存在する。ＩＰアドレスは、また、既知のＩＰアドレス又は既知の企業のアドレスの範囲と単に比較されてもよい。重み付けされた情報は、ＩＰアドレスが真正なウェブサイトではなく、フィッシングウェブサイトであるということの決定に導く。

【００５１】

図４に示されるように、ウェブページ２００は、Ｐａｙｐａｌ，　Ｉｎｃのもののように見える。ＩＰ所有者２０２は、正当な企業であるＩｎｋｔｏｍｉ，　Ｉｎｃ．として表示される。しかし、ドメインネームｗｗｗ．ｐａｙｐａｙ．ｃｏｍと関連付けられるＩＰアドレスは、２１６．１１３．１８８．６７である。大規模団体は、多くのＩＰアドレスを有する場合があり、そのため、ＩＰアドレスが正当な団体によって所有されるかどうかが不明確である。ＵＲＬのＩＰアドレスに関連付けられる国名２０６は、Ｕｎｉｔｅｄ　Ｓｔａｔｅｓであり、正当に見える。よって、追加情報が用いられる。この例では、Ｐａｙｐａｌ，　Ｉｎｃ．は、企業Ｅｂａｙ，　Ｉｎｃ．によって所有されており、これは、Ｉｎｋｔｏｍｉ，　Ｉｎｃ．とは関連付けられていない。よって、示されているウェブサイトは、フィッシングウェブサイトである可能性がある。オプション警告２０８は、ポップアップウィンドウ又は別の手法で、別のブラウザフィールドに表示される。

【００５２】

別の実装例

インターネットのようなＩＰネットワークでは、２つのノード間の接続及びセッションは、一般的に、ＩＰアドレス及びＴＣＰ／ＵＤＰポート番号を用いてなされる。いずれかのノードは、それ自体及び他のノードのＩＰアドレス及びポート番号を知っている。ポートは、一般的に、ネットワークノードへのエンドポイントである。ポート番号は、典型的には、特定の通信セッション、特定の機能、特定のリソース、又はこのネットワークノード内の他のアイデンティティを表す。ポート番号は、一般的に、３つのレンジに分割される：ウェルノウンポート（Ｗｅｌｌ　Ｋｎｏｗｎ　Ｐｏｒｔｓ）、登録ポート（Ｒｅｇｉｓｔｅｒｅｄ　Ｐｏｒｔｓ）及びダイナミック及び／又はプライベートポート（Ｄｙｎａｍｉｃ　ａｎｄ／ｏｒ　Ｐｒｉｖａｔｅ　Ｐｏｒｔｓ）。ウェルノウンポートは、一般的に、ＩＡＮＡのようなアサイメントサービスによって割り当てられる。登録ポートは、所望の目的のために、付加的に登録されてもよい。ダイナミック又はプライベートポートは、一般的に、頻繁に通信を変更する及び／又はプライベート目的のためにネットワークノードによって用いられる。

【００５３】

他のノードへのアウトバウンド接続要求のために、クライアントは、他のノードのＩＰアドレス及びポート番号を用いる。クライアントへのようなインバウンド接続のために、リクエスタは、そのＩＰアドレス及びポート番号を識別する。中継ノードがインターネットサービスプロバイダサーバ等に用いられる場合、中継ノードは、一般的に、各ノードのＩＰアドレス及びポート番号を知る。例えば、サーバは、一般的に、要求ノード及びクライアントノードの両方のＩＰアドレス及びローカルポート番号を知り、中継サーバは、要求ノードとクライアントノードとの通信をリレーすることができる。

【００５４】
同様に、サーバ又はクライアントによって開始されるファイルのダウンロードのために、ＩＰアドレス及びポート番号が知られている。例えば、ダウンロードがウェブサイト又は他のネットワークサービスからである場合、ファイルを提供するＩＰアドレス及びポート番号は、上述したような、パブリック又はローカルアサイメントデータベースから求められうる。一部の状況では、ＩＰアドレス及びポート番号は、正当な、つまり、信頼できるネットワークノードのものであってもよい。しかし、ハッカーは、信頼できるノードにアクセスし、ウイルス又は他の望まれないファイルを配布させようとする。この場合、本発明の実施形態は、通信のペイロードを評価する。一実施形態では、評価モジュールは、許容データを示すカテゴリ識別子に対してペイロードデータを決定及びチェックするために、パケットのペイロードを評価する。別の実施形態では、評価モジュールは、ファイルがブロックされる及び／又は警告が発せられるべきであるかどうかを判定するために、全体のファイル拡張子、ファイルオーサー、生成日、及び／又は転送されるファイルの他のプロパティを評価する。例えば、信頼できるネットワークノードから新たなドキュメントをダウンロードすることを容認するが、実行可能なコードをダウンロードすることを容認しない。１以上のカテゴリコードは、ペイロードデータ、ダウンロードファイル又は許容される他のデータの種類を示すために、各信頼できるノードのＩＰアドレス及びポート番号と関連付けられうる。

【００５５】
ＩＰアドレス、ポート番号及びカテゴリコードは、正当及び／又は信頼できるネットワークノード及びファイルを識別するファイル、データベース、及び／又は他のデータソースに記憶される。このようなデータソースは、ホワイトリストとしても本明細書で示されている。ホワイトリストは、一般的に、ブロックされる又は信頼出来ないアドレス、ノード、データソース又は他の情報を具体的に識別するブラックリストとは異なる。例えば、本発明の特定の実施形態に用いられるホワイトリストは、認証されないネットワークノード又は匿名プロキシサーバについてのＩＰアドレスを含まない。

【００５６】
ホワイトリストは、ＩＡＮＡ　ＷＨＯＩＳデータベースのサブセットであってもよい。これは、正規の金融機関、信頼できるウェブサイト、信頼できるダウンロードウェブサイト、信頼できるアンチウイルス企業ウェブサイト、及び／又は他のサービスプロバイダのみのネットワークノードを識別してもよい。このようなサービスプロバイダは、ＩＳＰを含んでもよい。よって、ホワイトリストは、ＩＰアドレス及び１以上のインターネットサービスプロバイダと関連付けられる情報を含むために、インストール時又はそのほかの時に、変更されてもよい。サービスプロバイダは、クライアント設備、クライアントノードがアクセスする必用がある他のインターネットノード、又は特定の機能のために特定のデバイスにアクセスするための許可を有する一部の他のネットワークノードにアクセスするために必要であってもよい。また、ホワイトリストは、アドレス所有者の名称、ドメインネーム、カテゴリコード及び他の情報を含んでもよい。ホワイトリストは、クライアント、ファイルを提供するサーバ、通信の中継ノード、又は２つのノード間の通信のディレクトリパートではないニュートラルノードに記憶されてもよい。複数のホワイトリストは、マスクされたネットワークアドレス、プロキシサーバ等を承諾するために、単一又は複数のノードで使用されてもよい。例えば、複数のホワイトリストは、メッセージ、ウェブページ又は通信経路に沿う他の通信ムーブとして中間チェックを行うために、様々なルーター又は他のノードに分配されてもよい。

【００５７】
本発明の実施形態は、複数の段階のセキュリティを提供するために実装されうる。最上位の段階は、ＩＰアドレスである。第２の段階は、ポート番号である。第３の段階は、カテゴリである。他の段階は、通信の他の態様に関連付けられてもよい。アプリケーション要件に応じて、実施形態は、様々なレベルの評価を適用してもよい。一実施形態は、信頼できるＩＰアドレスについてのホワイトリストをチェックすることにより第１の段階のみ

を実行してもよい。更に高いセキュリティのために、実施形態は、３つ全ての段階をチェックしてもよい。アドミニストレータは、評価モジュールにおいて評価のレベルを設定してもよい。

【００５８】

ホワイトリストの他の情報は、セキュリティレーティングを含んでもよく、これは、ユーザインタラクションが必要かどうかを示すために用いられる。例えば、最も高いセキュリティレーティングのために、評価モジュールは、その評価を自動的に行い、全ての決定をなす。別のセキュリティレーティングのために、ユーザインタラクションは、通信、ファイルダウンロード又は疑わしいネットワークノードに関連付けられる他のアクションを可能にするために必要とされてもよい。最も低いレーティングのために、評価モジュールは、自動的に通信、ファイルダウンロード又は他のアクセスをブロックしてもよい。追加又は代替的に、セキュリティレーティングは、通信をチェックしている間に、確認される又は別々に決定されてもよい。例えば、ＩＰアドレス、ポート番号及びカテゴリコードが、ホワイトリストのものと一致した場合には、評価モジュールは、高いセキュリティレーティングを示してもよい。ＩＰアドレス及びポート番号が一致するが、カテゴリコードが一致しない場合には、評価モジュールは、中間のセキュリティレーティングであると決定し、どのように処理するかのユーザ指示を要求する。ＩＰアドレス及びポート番号がホワイトリストのものと一致しない場合には、評価モジュールは、最も低いセキュリティレーティングであると決定する。評価モジュール及び／又は他のアプリケーションは、セキュリティレーティングに応じて、異なるアクションを取りうる。

【００５９】

評価モジュールが高リスクネットワークノードを識別する複数の状況が存在する。以下に限定されないが、いくつかの実施例を含む。

【００６０】

１．ウェブサイト、ＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）又は他のネットワークノードを訪れるようなアウトバウンド接続要求のために、宛先ノードのＩＰアドレス及びポート番号は、チェックされる。宛先ノードのＩＰアドレス及びポート番号がホワイトリストと一致しない、又は高リスクとみなされる場合には、評価モジュールは、接続を妨げる、警告を与える、ユーザ承認を要求する、宛先ノードの追加認証を要求する又は別の予め設定されたアクションを行うことができる。ユーザが接続を承認することの場合、宛先ノードのＩＰアドレス、ポート番号及び／又は他の情報は、ホワイトリストに追加される。

【００６１】

２．インバウンド接続要求のために、要求ノードのＩＰアドレス及びローカルデバイスポート番号は、ホワイトリストに対してチェックされる。これは、受信デバイスへのアクセスを得ることから、侵入者、ハッカー又は他の認証されないユーザを止めることができる。受信デバイス（又は中間ノード）は、接続を拒否する、警告を与える、ユーザ承認を要求する、追加認証を要求する又は別の予め設定されたアクションを行うことができる。ユーザが接続を承認することの場合、宛先ノードのＩＰアドレス、ポート番号及び／又は他の情報は、ホワイトリストに追加される。

【００６２】

３．ファイル転送のために、ソースノードは、ファイルがダウンロードされる前にチェックされうる。逆に、宛先ノードは、ファイルが疑わしいノードへ送信される前にチェックされうる。上述したように、ＩＰアドレス、ポート番号及びファイルタイプは、ホワイトリストに対してチェックされうる。接続状況と同様に、評価モジュールは、ファイル転送を妨げる、ユーザ承認を要求する、要求ノードの追加認証を要求する又は別の予め設定されたアクションを行うことができる。ユーザがファイル転送を承認することの場合、疑わしいノードのＩＰアドレス、ポート番号及び／又は他の情報は、ホワイトリストに追加される。ファイル拡張子は、また、対応するＩＰアドレス、ポート番号及び／又は他の情報に沿ってカテゴリとして記憶される。

【００６３】
図５は、本発明の別の実施形態のためのアーキテクチャ、通信シーケンス及び方法を示す。図示されたモジュールの全てが本発明を実施するために要求されなくてもよい、又は追加のモジュールが別の実施形態に含まれてもよい。各種実施形態では、一部のモジュールは、組み合わせられる一方で、他のモジュールは、複数のモジュールに分割されてもよい。実施例の状況は、以下のアーキテクチャに対して説明される。
【００６４】
実施例の実施形態では、アーキテクチャは、ウェブサイト、ＦＴＰサイト又は他のインターネットサービスに対応するネットワークノード３１７のＩＰアドレスへのパブリックインターネット１５ｂを通じて通信するクライアント２０ｂを含む。クライアント２０ｂは、インターネット１５ｂと通信され、ＴＣＰ／ＩＰスタック３３３と通信されるオペレーティングシステム３１ｂを含む。ＴＣＰ／ＩＰスタック３３３は、インターネットネットワークアプリケーション３４ｂと通信され、これは、認証モジュール３８ｂと通信される。インターネットネットワークアプリケーション３４ｂは、電子メールアプリケーション、又はハッカー、ウイルス又は他の望まれないエンティティを含む通信を妨げるために用いられうる他のアプリケーションであってもよい。認証モジュールは、ローカルデータベース３５０と通信され、これは、クライアント２０ｂに含まれてもよく、クライアント２０ｂと通信されてもよい。ローカルデータベース３５０は、一般的に、ＩＰアドレス、ＴＣＰ／ＩＰポート番号、カテゴリ、セキュリティレーティング、ドメインネーム、それらの所有者及び／又は他のデータ間の関連性を記憶するホワイトリストを含む。
【００６５】
状況例１：アウトバウンド接続
この実施形態の例では、クライアント２０ｂのユーザは、ウェブサイトのようなインターネット接続を開始する。インターネットネットワークアプリケーション３４ｂは、通信ステップ３０１において、接続のためのユーザ要求を検出する。要求は、先ず、ドメインネーム又はＵＲＬをＩＰアドレスに変化するために、ＴＣＰ／ＩＰスタック３３３へ送信される。変化したドメインネームは、ＤＮＳへのアクセスを要求する。しかし、ＤＮＳからのＩＰアドレスは、マスクされる又は欺かれている場合がある。ＴＣＰ／ＩＰスタック３３３は、通信ステップ３０２において、オペレーティングシステム３１ｂを通じて要求を送信し、オペレーティングシステムは、通信ステップ３０３において、インターネットを通じて、ネットワークノード３１７へのＴＣＰ接続をする。
【００６６】
ネットワークノード３１７（例えば、ウェブサイトの対応するサーバ）は、通信ステップ３０４において、要求をリターンする。また、リターンされるのは、ネットワークエンティティの正確なＩＰアドレス及びポート番号である。クライアントオペレーティングシステム３１ｂは、ＩＰアドレス及びポート番号を受信し、通信ステップ３０５において、この情報をＴＣＰ／ＩＰスタック３３３へパスする。ＴＣＰ／ＩＰスタックは、通信ステップ３０６において、制御をアプリケーション３４ａへパスする。アプリケーションプログラムは、ネットワークノード３１７から受信される任意のファイル又は他データのカテゴリコードを決定してもよい。通信ステップ３０７において、アプリケーションは、ＴＣＰ／ＩＰスタックからのＩＰアドレス及びポート番号を要求する。例えば、ネットワークアプリケーションは、ＧｅｔＩＰＡｄｄｒｅｓｓＢｙＮａｍｅオブジェクト又はＧｅｔＨｏｓｔＢｙＮａｍｅオブジェクトを呼び出してもよい。ＴＣＰ／ＩＰスタックは、通信ステップ３０８において、ＩＰアドレス及びポート番号をアプリケーションへリターンする。
【００６７】
ネットワークアプリケーション３４ｂは、その後、通信ステップ３０９において、ＩＰアドレス、ポート番号、カテゴリコード及び他の情報を認証モジュール３８ｂへパスする。認証モジュールは、データベース３５０をチェックするために、この情報を用いる。認証モジュールは、通信ステップ３１０において、ＩＰアドレス、ポート番号、カテゴリコ

ード及び他の情報を有するデータベース３５０へサーチ要求を送信してもよい。データベース３５０は、ＩＰアドレス及び他の情報が、信頼できる情報のホワイトリストに含まれるかどうかを判定するためにサーチを行う。データベース３５０は、また、所有者、国名、セキュリティコード及び／又はＩＰアドレスに関連付けられる他の情報を判定してもよい。データベース３５０は、通信ステップ３１１において、要求された情報を認証モジュール３８ｂへリターンする。認証モジュール３８ｂは、情報をネットワークアプリケーション３４ｂへ直接的にパスしてもよい。ＩＰアドレス及びポート番号がホワイトリストにあるかどうかに基づいて、認証モジュールは、ステップ３１２において、接続を閉じる、受信された情報を拒否する、警告メッセージを送信する、ユーザ決定を待つ、及び／又は他の予め設定されたアクションを行うために、命令を送信することができる。

【００６８】

状況例２：インバウンド接続

ネットワークノード３１７は、通信ステップ３０４において、接続をクライアント２０ｂに要求する。クライアントオペレーティングシステム３１ｂは、この要求を受信し、これは、ネットワークノード３１７のＩＰアドレス及びポート番号を含む。要求は、また、一般的に、ネットワークノードが接触することを望むリソースとして、ネットワークアプリケーション３４ｂを識別するために、ネットワークアプリケーション３４ｂのポート番号を含む。要求は、更に、ネットワークノードが望むデータにファイルネーム又は他の情報を含んでもよい。オペレーティングシステムは、通信ステップ３０５において、この情報をＴＣＰ／ＩＰスタック３３３へパスする。ＴＣＰ／ＩＰスタックは、通信ステップ３０６において、この情報をインターネットネットワークアプリケーション３４ｂにパスする。

【００６９】

ネットワークアプリケーション３４ｂは、その後、通信ステップ３０９において、ＩＰアドレス、ポート番号及び他の情報を認証モジュール３８ｂへパスする。認証モジュールは、ネットワークノード３１７によって要求される情報についてのカテゴリコードを決定してもよい。認証モジュールは、データベース３５０をチェックするために、この情報を用いる。認証モジュールは、通信ステップ３１０において、ＩＰアドレス、ポート番号、カテゴリコード及び他の情報を有するデータベースへサーチ要求を送信してもよい。データベース３５０は、ＩＰアドレス及び他の情報が、信頼できる情報のホワイトリストに含まれるかどうかを判定するためにサーチを行う。データベース３５０は、また、所有者、国名、セキュリティコード及び／又はＩＰアドレスに関連付けられる他の情報を判定してもよい。データベース３５０は、通信ステップ３１１において、要求された情報を認証モジュール３８ｂへリターンする。認証モジュール３８ｂは、情報をネットワークアプリケーション３４ｂへ直接的にパスしてもよい。ＩＰアドレス及びポート番号がホワイトリストにあるかどうかに基づいて、認証モジュールは、ステップ３１２において、接続を閉じる、受信された情報を拒否する、警告メッセージを送信する、ユーザ決定を待つ、及び／又は他の予め設定されたアクションを行うために、命令を送信することができる。

【００７０】

状況例３：メッセージング

ネットワークアプリケーション３４ｂが、Ｍｉｃｒｏｓｏｆｔ　Ｏｕｔｌｏｏｋ（登録商標）等の電子メールクライアントのようなメッセージングサービスである場合、受信される電子メールヘッダーをチェックすることができる。ヘッダーには、送信電子メールデバイスのＩＰアドレス及びポート番号を有する“Ｒｅｃｅｉｖｅｄ　Ｆｒｏｍ”フィールドが存在する。ヘッダーは、ｃｏｕｒｔｅｓｙ　ｃｏｐｙ（ＣＣ）受領者、受信された電子メールへの添付の表示、及び／又は他のデータと関連付けられたデバイスのＩＰアドレスのような他の情報を含んでもよい。ネットワークアプリケーション３４ｂは、添付フィルのカテゴリコードを決定してもよい。ネットワークアプリケーションは、その後、通信ステップ３０９において、ＩＰアドレス、ポート番号及び他の情報を認証モジュール３８ｂへパスする。認証モジュールは、電子メール送信者が信頼できるかをどうかを判定する

ためにこの情報を用いる。具体的には、認証モジュールは、通信ステップ３１０において、サーチ要求におけるＩＰアドレス及びポート番号（及び利用可能な場合にはカテゴリコード）をデータベース３５０へ送信する。データベースは、ホワイトリストにおけるＩＰアドレス及びポート番号をチェックする。データベースは、また、ドメインネーム、電子メールファンクションコード、セキュリティレーティング、及び／又は他のデータ（利用可能な場合）を検索してもよい。データベース３５０は、通信ステップ３１１において、そのサーチの結果を認証３８ａへリターンする。認証モジュール３８ｂは、情報を電子メールネットワークアプリケーション３４ｂへ直接的にパスしてもよい。ＩＰアドレス及びポート番号がホワイトリストにあるかどうかに基づいて、認証モジュールは、ステップ３１２において、電子メールを削除する、電子メールを（例えば、迷惑メールフォルダへ）リダイレクトされる、警告を送信する、ユーザ命令を待つ、及び／又は他のアクションのために命令を送信することができる。

【００７１】

より詳細には、本発明の例示的な実施形態は、ｓｉｍｐｌｅ ｍａｉｌ ｔｒａｎｓｐｏｒｔ ｐｒｏｔｏｃｏｌ（ＳＭＴＰ）を用いるインターネット電子メールシステムを含んでもよい。インターネット電子メールのために、ＳＭＴＰは、メールを届ける又は検索するために用いられる。これは、一般的には、中継メールサーバを通じて行われる。電子メールを受信するとき、メールサーバは、送信メールクライアントのＩＰアドレス及びＴＣＰ／ＵＤＰポート番号を受信する。メールサーバは、送信者のＩＰアドレスを、電子メールヘッダーの“Ｒｅｃｅｉｖｅｄ Ｆｒｏｍ”フィールドへ追加する。上述したように、ＩＰアドレスは、照合されうる。

【００７２】

このような照合の別の実施形態は、また、電子メール送信者のドメインネームを認証するために、メールサーバによるリバースＤＮＳルックアップを含んでもよい。一部の電子メールサーバは、スパム電子メールをブロックするためにドメイン情報を用いることを留意する。スパムブロッキングは、メールサーバドメイン及び／又はクライアント送信者のドメインをチェックするために、ドメイン情報を用いてもよい。しかし、上述されたように、ドメイン情報は、マスクされる場合がある。ＤＮＳルックアップあり又はなしで、本発明の実施形態は、ホワイトリストデータベースに対して電子メールの実際のＩＰアドレスをチェックすることにより電子メール送信者を照合する。それにもかかわらず、所有者及び国名のような追加情報は、電子メールヘッダー内のＩＰアドレス情報から取得されるドメイン情報からチェックされうる。追加信頼性は、受信されたＩＰアドレスが、受信された電子メールアドレスに示されるドメインと関連付けられることを確実にするために、ドメインルックアップを用いることにより取得されうる。例えば、認証モジュールは、ホワイトリスト又はドメインアサイメントサービスをサーチするために電子メールヘッダーからのＩＰアドレスを用い、ＩＰアドレスに関連付けられるドメインネームを決定してもよい。認証モジュールは、その後、電子メールメッセージの“Ｒｅｃｅｉｖｅｄ Ｆｒｏｍ”フィールドにおいて特定されたドメインネームに対して決定されたドメインネームを比較しうる。ドメインネームが一致しない場合には、メッセージは、正当ではない。メッセージからのＩＰアドレス及びポート番号が、ホワイトリストのものと一致したとしても、異なるドメインネームは、ハッカーが、信頼できるネットワークノードにアクセスし、スパムメッセージ又は他の望まれない活動のために信頼できるネットワークノードを用いていることを示す。

【００７３】

電子メールが、別のＳＭＴＰにより転送／リレーされている場合、その受信者電子メールクライアントは、また、転送／リレーメールサーバが信頼できるかをチェックする。電子メールヘッダーが不十分である場合、又は転送／リレーメールサーバが、送信者を識別するために用いることができない場合、認証モジュールは、電子メールを削除する、又は上述された他のアクションを取ることができる。

【００７４】

また、ＳＭＴＰ電子メールのために、送信者は、ｘｘｘｘ@ｍｓｎ．ｃｏｍ．のような電子メールドメインを用いる。ドメインネームだけでは、一般的に、この電子メールが一般的なＭＳＮユーザからである、又はアカウンティング又はアドミニストレーション部門のようなＭＳＮ内の重要組織のメンバーからであるかを識別するのは容易ではない。このレベルの詳細を決定することを可能にするのは、金融機関又は他の団体（オーガニゼーション）が手に入れることを望む機能である。

【００７５】

この課題を解決するために、送信電子メールサービスは、特定部門のための複数ＩＰアドレスを実現することができる。一部のＩＰアドレスは、汎用ユーザのためのものであってもよい。他のＩＰアドレスは、特別なユーザ及び／又は他の特別な目的のために用いられうる。このようにして、金融機関又は他の団体は、金融情報電子メールをそれらの顧客へ送信しうる。追加又は代替的に、ＴＣＰ／ＩＰポートは、この機能をサポートするために用いられうる。これは、制限されたＩＰアドレスがインターネットメールサービスに利用可能である場合に有益である。更に別の実施形態では、サブオーガニゼーションコードは、サブオーガニゼーション又は電子メールの他のカテゴリー化を識別するために、通信に含まれうる、及び／又はホワイトリストデータベースに追加されうる。同様に、機能コードは、通信用の目的を示すために、通信に含まれうる、及び／又はホワイトリストデータベースに追加されうる。顧客のクライアントデバイスは、送信者を認証するために本発明の実施形態を用いることができ、許容できる団体のコード及び／又は機能コードをチェックすることができ、フィッシング電子メールから正当な電子メールを区別する。

【００７６】

フィシングウェブサイトについて警告を表示すると共に、電子メールクライアントは、ディスプレイフィールドを提供しうる。電子メールクライアントは、また、正当性を制御するためにメニューオプションを提供してもよい。ユーザが電子メールを受信したとき、メニューオプション及び／又はディスプレイフィールドは、ユーザが、電子メール送信者、サブオーガニゼーション及び／又は他の機能／データを識別することを可能にする。一実施形態では、受信者電子メールクライアントは、ローカルホワイトリストデータベースに対して送信者のＩＰアドレス、ポート番号及びドメインネームを自動的に比較する。送信者のＩＰアドレス（例えば、電子メールのＦＲＯＭ又はＲＥＣＥＩＶＥＤフィールドに基づいて決定されるような）、ポート番号及び／又はドメインネームがデータベースにない、又はデータベース内のエントリのものと異なる場合、ディスプレイフィールドは、電子メールが、電子メールアドレスに示される送信者から実際には来ないことを示すために用いられる。代替的に、ユーザは、このチェックを行う、電子メール又は送信者についての情報を表示する、及び／又は他の動作を実行するために、メニューオプションをアクティベートしてもよい。

【００７７】

一部の実施形態では、ホワイトリストは、よく知られた団体のＩＰアドレスに加えて、以下の構成の１以上を有する。上述されたホワイトリストの主な利点は、２方向通信（ｔｗｏ－ｗａｙ　ｃｏｍｍｕｎｉｃａｔｉｏｎ）に用いられるＩＰアドレス（例えば、ＴＣＰ／ＩＰセッションの一部として）が偽造することが困難又は不可能であることである。攻撃者又は他の相手がパケットのソースＩＰアドレスになりすますことができるが、このようななりすましは、一般的に、ＴＣＰ／ＩＰコンテキスト（ＴＣＰ／ＩＰ　ｃｏｎｔｅｘｔ）で用いられることができず、ここで、２方向通信は、セッションを実現するために必要である。よって、ネットワークスタックから得られるＩＰアドレスを用いることにより、上述された技術は、高い信頼度で疑わしいネットワーク通信を識別することができる。

【００７８】

また、ホワイトリストは、疑わしいＩＰアドレスがブラックリストに追加されると、当該ＩＰアドレスの認証されないユーザが、それらの攻撃を、異なるＩＰアドレスで動作する異なるコンピュータシステムへ移動しうるだけであるブラックリストに利点を提供する

。犯罪組織が、感染したマシンのネットワーク全体を動作する世界では、それらの組織にとってそれらの認証されない活動（例えば、スパムの送信）をあるマシンから別のマシンへシフトすることは些細なことである。

【００７９】

上述された技術は、また、所与のコンピュータシステム内の複数の異なるレベルで機能してもよい。例えば、上述された技術は、オペレーティングシステムカーネル、ネットワークスタック及びアプリケーションから受信又は取得される情報を用いてもよい。例えば、認証モジュール３８ｂ（図５）は、アプリケーションレベル（例えば、電子メールクライアントから受信される電子メールヘッダー）、ネットワークレベル（例えば、ＴＣＰ／ＩＰスタックから受信されるＩＰアドレス）、及びオペレーティングシステム（例えば、オペレーティングシステムカーネルから受信される許可設定）から受信される情報を用いてもよい

【００８０】

また、上述された技術は、コンピュータシステムの異なるレベルのセキュリティを実装するためのインフラストラクチャ又はフレームワークを提供する。例えば、ホワイトリスト又は類似の構造は、オペレーティングシステム、ネットワークスタック及び１以上のアプリケーションにおけるセキュリティ又は許可機能を実装するために用いられる情報又はプロパティを含んでもよい。

【００８１】

ホワイトリストは、地理的情報と関連付けられるＩＰアドレスを含んでもよい。ある種の地理的情報は、特定のＩＰアドレスに割り当てられる地域インターネットレジストリ（ｒｅｇｉｏｎａｌ　Ｉｎｔｅｒｎｅｔ　ｒｅｇｉｓｔｒｙ）に基づく。上述されたように、ＩＰアドレスは、ＡＲＩＮ、ＡＰＮＩＣ、ＬＡＣＮＩＣ、ＡｆｒｉＮＩＣ、ＲＩＰＥ　ＮＣＣ等のような地域インターネットレジストリによって割り当てられる。与えられたＩＰアドレスは、ＩＰアドレスに割り当てられた地域インターネットレジストリを判定することが可能であり、それにより、ＩＰアドレスに関連付けられる地域（例えば、大陸又は国名）を判定する。地域レジストリは、更に、ＩＰアドレスに関連付けられる国名、州又は市のような国名又はより詳細な地理的情報を提供するクエリをサポートしてもよい。地理的情報の他のソースは、国名、州、市、緯度／経度、郵便番号、市外局番等を含むきめ細かい地理的情報を提供するように構成されるｗｈｏｉｓデータベース及び商業的又はパブリックゲオロケーションサービスを含む。

【００８２】

地理的情報は、特定された領域においてユーザにアクセスを制限するために用いられてもよい。例えば、政府は、当該政府の国又は管轄に位置するＩＰアドレスへのアクセスを制限してもよい。別の例として、特定の地域のためのＩＰアドレスは、それらの地域からの高レベルのコンピュータ犯罪操作に基づくような危険としてフラグ付されてもよい。別の例として、ｅ－コマースコンピュータシステム（例えば、バンキングシステム、オンラインショッピングシステム）は、顧客が住む同一の地理的地域（例えば、市、州、国）と関連付けられるＩＰアドレスからの顧客アクセスのみを可能にしてもよい。例えば、特定の顧客がシアトルに住む場合、特定のｅ－コマースシステムは、ワシントン州又はアメリカ合衆国に割り当てられるＩＰアドレスからの顧客のアカウントにのみアクセスを可能にしてもよい。また、政府又は軍のような高セキュリティな組織については、当該組織は、特定の地理的位置のみをアクセス可能にし、他の位置（例えば、中華人民共和国）をブロックしてもよい。

【００８３】

ホワイトリストは、異なる実施形態において異なる形態を取ってもよい。ホワイトリストは、パブリックインターネット及び／又はプライベートインターナルネットワークに存在してもよい。ホワイトリストは、パブリックインターネットで採用されるものと同様の手法でプライベートインターナルネットワークに対して生成されうる。例えば、銀行は、顧客インターネットＩＰアドレスを特定銀行アカウントと関連付けるホワイトリストを有

してもよい。顧客側では、銀行アカウント所持者は、銀行のコンピュータシステムの内部ＩＰアドレスを含むホワイトリストを有してもよい。また、複数のリストは、単一デバイスに存在してもよい。例えば、１つはインバウンドトラフィック用のホワイトリストであり、１つはアウトバウンドデータ用のホワイトリストである。また、各ネットワークインターフェースカード（ＮＩＣ）は、その独自のホワイトリストを有してもよい。また、ホワイトリストは、静的（例えば、予め設定される）又は動的に生成されうる。例えば、ウェブサイトについて、動的リストは、着信ＩＰアドレス情報に基づいて生成されてもよい。後者のアクセスは、その後、リストに基づいて比較されて、疑わしい通信は、ウェブサイトＵＲＬが、リストに記憶されるものとは異なるＩＰアドレスに変化させるとき等に示されうる。

【００８４】

ホワイトリストの実施例は、以下の表１に記載される以下のフィールド又はプロパティの１以上を含んでもよい。フィールドのそれぞれは、通信の許容方向（例えば、アップロード又はダウンロード、送信又は受信）、通信の許容期間（例えば、８ＡＭから１ＰＭ）、許容プログラム／プロセス（例えば、Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ）等のような１以上の許容通信プロパティを表す。別の実施形態では、表は、通信が許可されない期間（例えば、深夜から４ＡＭ）、許可されない通信ポート（例えば、ＨＴＴＰに共通に用いられるポート８０）等のような許容しない通信プロパティの指標を含んでもよい。

【表１－１】

フィールド／プロパティ	説明／機能
IPアドレス及びマスク	許容IPアドレス又はIPアドレス範囲を識別。内部ネットワークに対して、IPアドレスは、内部（プライベート）IPアドレスであってもよい。
ポート番号	許容ポート番号又は範囲を識別し、これにより、FTP、Telnet、HTTP等のような許容機能を意味する。
ブロック状態	対応するアドレスからのアクセスを許容する又は許容しない。
カテゴリコード／データタイプ	実行可能なコード、スクリプト、マクロ、オーディオ、ビデオ、画像、テキストファイル等のような通信からのデータの許容タイプを示す。
方向性	アップロード、ダウンロード、着信、発信等のような通信の許容方向性を定義する。非常にセキュアなデバイスは、例えば、入ってくる接続を許容しない。
セキュリティレーティング	非常にセキュアである、セキュアである、普通、セキュアでない、高リスク等のようなこのIPアドレスと関連付けられるセキュリティレベルを特定する。
サブーオーガニゼーションコード	オーガニゼーション内のIPアドレスのサブセットを特定する。例えば、オーガニゼーションについて、それらのIPアドレスを、ウェブ用の１つのグループ、Telnet用の別のグループのように分割する。
URL／URI	IPアドレスに関連付けられる組織オフィシャルURL。時折、HTTPリダイレクトは、例えば、人を欺くためのフィッシングウェブサイトをホストする非常に類似するURLにリダイレクトしてもよい。別の例としては、電子メールにおけるHTTPリンクは、正規のURLと同様に見える。通信時に現れるURLは、通信が疑わしいかどうかを判定するために、組織URLに対して比較される。更に、URIのチェックは、追加保護を提供する。
ドメインネーム	ドメインネームと一致するために用いられうる。電子メールアドレスは、チェックされうるドメインネームを有する。
地理的位置情報	国コード、市、所在地住所、zipコード等。これは、特定の地理的位置へのアクセスを制限するために用いられうる。
ネットワークインターフェース番号	これは、複数のネットワークインターフェース（NIC）デバイスのためのものである。
処理名又は署名	所定のIPアドレスにアクセス又は通信しうるプログラムを特定する。 これは、ウイルスプログラムがネットワークにアクセスして、データを送受信すること又はそれ自身を他者に拡散することを防ぐ。プログラムは、名称、位置又は署名／ハッシュ（例えば、MD5，　SHA1等）。
インタラクティブ／バッチモード	多くの悪意のあるプログラムは、バッチ又は非インタラクティブモードで動作する。これは、ウイルスプログラムが電子メールアカウントにアクセスして、データを送受信することを防ぐことができる。このモードは、アクティブコンソール、UIウィンドウ、インタラクティブ入力デバイス（例えば、マウス）等があるかどうかをチェックすること等のような各種の手法で決定されうる。

【表１－２】

アクセス時間	ネットワークアクセスが許容される時間又は期間を特定する。これは、おかしな時間（例えば、深夜）に動作する悪意のあるコードを阻止する。
接続数	どの程度の接続がネットワークになされるかを制限する。これは、サービス妨害攻撃を防ぐために用いられうる。
アクセスコントロール	どのような種類のオペレーションが、読み出し、書き込み、変更、実行等を含む対応するIPアドレスに対して行われうるかを特定する。これらのアクセス権は、オペレーションシステムの仕様又はアプリケーションの仕様であってもよい。特定のアプリケーションは、根本的なシステムのものとは異なるアクセス権を提供してもよい。例えば、メッセージングアプリケーションにおいて、発信メッセージを送信することは、着信メッセージを読み出すこととは異なるアクセス権を要求してもよい。
ユーザ／グループ識別子	対応するIPアドレスを使用することを許容するユーザ又はユーザのグループの識別子（例えば、ユーザ名、アカウント番号、ユーザ番号）。認証の目的で、ユーザ識別子、パスワード及びIPアドレス及び／又はポート番号を照合しうる。
インバウンド／アウトバウンド	インバウンドトラフィックは、アウトバウンドトラフィックのものとはセキュリティ要件を有してもよい。それぞれは、別のホワイトリストを有してもよい。

表１

【００８５】
上記のフィールドは、様々な手法で組み合わせられてもよい。例えば、図１を参照すると、クライアント１２、１３又は１４が、アウトバウンド接続を開始したとき、プロセス名称、アクセス時間ウィンドウ、バッチ／インタラクティブ処理、宛先ＩＰアドレス、適切な場合のＵＲＬ／ＵＲＩ又はドメインネーム、セキュリティレーティング、アップロード／ダウンロード、カテゴリコード又はペイロードタイプの１以上をチェックしてもよい。一部の実施形態では、これらのアイテムのいずれか１つが、ホワイトリストにおける対応するエントリ／フィールドに一致しない場合には、接続は、許可されない。別の実施形態では、疑わしい通信等を説明するポップアップウィンドウ／ダイアログを表示する、メッセージを送信する等により、ユーザに通知されてもよい。
【００８６】
別の例として、クライアント１２、１３又は１４が、インバウンド接続を受信するとき、リモートデバイスのＩＰアドレス及びポート番号、この接続（例えば、ポートでのリスニング）を供給しているプログラム、アクセス時間ウィンドウ、バッチ又はインタラクティブ処理、適切な場合のＵＲＬ／ＵＲＩ又はドメインネーム、カテゴリコード又はペイロードタイプの１以上をチェックしてもよい。
【００８７】
ホワイトリストは、また、良好なセキュリティ行為を有するよく知られた企業のような一般的なセキュリティシステム又はサービスを識別するエントリを含んでもよい。これらのシステムに対して、任意の種類のデータのアクセス、ダウンロード又はアップロードを許可しても安全である。
【００８８】
デバイスが、既に、ウイルスのような悪意のあるコードに感染している場合、上述された技術は、プログラム名称（例えば、プロセス名称）、アクセス時間ウィンドウ、ペイロ

ードタイプ、バッチ又はインタラクティブモードをチェックすることにより、重要な情報をアップロードするために、ウイルスがネットワークへアクセスすることを防ぐことができる。これは、ウイルスが他のデバイスへ広がることを防ぐ。ウイルスが、データを送出するためにオンライン電子メールアカウントにアクセスするための許可プロセスリストに既にあるウェブブラウザのような別のプログラムを開こうとしている場合、アクセス時間ウィンドウ及びバッチモードチェックは、例えば、バッチモードウェブブラウザプログラムの全てを不許可することによって、止めることができる。

【００８９】

悪意のある又は疑わしい電子メールは、一部の実施形態では、以下のような方法で検出されてもよい。先ず、電子メールクライアントと関連付けた認証モジュールは、電子メールヘッダー（例えば、ｓｏｕｒｃｅ＠ｈｏｓｔｎａｍｅ．ｎｅｔ）におけるＦＲＯＭフィールドからソース電子メールアドレスを抽出してもよい。悪意のある電子メールでは、ソース電子メールアドレスは、頻繁に偽装され、友人又は他の既知の人から来たように見せる。そして、認証モジュールは、ソース電子メールアドレスから抽出されるホストネーム（例えば、ｈｏｓｔｎａｍｅ．ｎｅｔ）でドメインネームルックアップを行うこと等により、ソース電子メールアドレスに基づいて第１のＩＰアドレスを決定する。次に、認証モジュールは、電子メールヘッダーにおけるＲＥＣＥＩＶＥＤフィールドから第２のＩＰアドレスを抽出する。ＲＥＣＥＩＶＥＤフィールドは、典型的には、受信者のＳＭＴＰサーバによって挿入され、送信者のＳＭＴＰサーバの実際のソースＩＰアドレスを含む。そして、認証モジュールは、一致のために第１及び第２のＩＰアドレスを比較する。これらが一致する場合、電子メールが真正ではなく、ソース電子メールアドレスに偽装されている可能性があり、ユーザへの通知、電子メールを開くことの拒否、画像、マックアップ言語又はコード等の描画の不許可のような適切なアクションが取られる。

【００９０】

図６は、ネットワーク通信評価処理６００を示すフローチャートである。この処理は、コンピュータシステム２０（図２）によって実行される評価モジュール３８のようなモジュールによって実行されてもよい。

【００９１】

処理は、ブロック６０２で開始し、信頼できるネットワークアドレスに対する許容通信プロパティを特定するホワイトリストにアクセスする。ホワイトリストへのアクセスは、ホワイトリストを受信、問い合わせ、サーチ又は他の処理を含んでもよい。一部の実施形態では、ホワイトリストは、上記の表１で説明されたもののような、１以上の許容通信プロパティの指標と関連付けられる信頼できるネットワークアドレスをそれぞれ含む行（ｒｏｗｓ）又はエントリを含む。

【００９２】

ブロック６０４では、処理は、ネットワーク通信に対応するＩＰアドレスを決定する。ＩＰアドレスの決定は、ＴＣＰ／ＩＰスタック又はコンピュータシステムにおける他の通信モジュールからＩＰアドレスを要求することを含んでもよい。ＩＰアドレスは、ソース又は宛先ＩＰアドレスであってもよい。典型的には、通信がインバウンド接続である場合には、ソースＩＰアドレスは、チェックされ、通信がアウトバウンドである場合には、宛先ＩＰアドレスは、チェックされる。別の状況では、ＩＰアドレスは、ネットワーク通信と関連付けられたドメインネームでＤＮＳサーバに問い合わせること等により、他の手法で決定されてもよい。ドメインネームは、例えば、ＵＲＬ、電子メールメッセージ、電子メールアドレス等を参照して決定されてもよい。

【００９３】

ブロック６０６では、処理は、ネットワーク通信と関連付けられる第１の通信プロパティを決定する。第１の通信プロパティを決定することは、例えば、表１に記載されるプロパティの１つを決定することを含む。例えば、処理は、時刻、通信の方向性、データペイロードのタイプ等のようなプロパティを決定してもよい。処理は、例えば、ゲオロケーション（ｇｅｏ－ｌｏｃａｔｉｏｎ）情報をＩＰアドレスに対して問い合わせ、ＩＰアドレ

スに関連付けられる位置（例えば、市、州、国、郵便番号）の指標に応じて受信することにより、ネットワーク通信と関連付けられる地理的位置を決定してもよい。

【００９４】

ブロック６０８では、処理は、ＩＰアドレスを有するホワイトリストによって関連付けられる許容通信プロパティである第２の通信プロパティを決定する。第２のプロパティを決定することは、ホワイトリスト内のＩＰアドレスをルックアップし、ＩＰアドレスと関連付けられ、かつ第１の通信プロパティに対応する通信プロパティを検索することを含んでもよい。例えば、第１の通信プロパティが時刻である場合、処理は、ホワイトリスト内の許容通信時間をルックアップする。第１の通信プロパティが地理的位置である場合、処理は、ホワイトリストにおける許容地理的位置をルックアップする。

【００９５】

ブロック６１０では、処理は、第１の通信プロパティが第２の通信プロパティによって包含されるかどうかを判定する。第１の通信プロパティが第２の通信プロパティによって包含されるかを判定することは、第２のプロパティが、第１のプロパティを包含する又は含むかを判定することを含む。例えば、第２のプロパティが、許容国（例えば、ワシントン州）である場合、第１のプロパティは、国に包含され、第１のプロパティ（例えば、ワシントン州、シアトル、米国郵便番号）が許容国内と同一又は許容国内に位置する。同様に、第２のプロパティが許容期間（例えば、６ＡＭから１１ＰＭ）である場合、第１のプロパティ（例えば、１０ＰＭ）が期間内にあるときに、第１のプロパティは、期間に包含される。

【００９６】

一部の実施形態では、第１のプロパティが第２のプロパティで包含されることを判定することは、２つのプロパティが一致するかどうかを判定することを含む。プロパティの一致は、２つの文字列、数字又は他のデータタイプ間の等式のような等価テストを行うことを含んでもよい。一部の場合には、一致は、厳格な等価テストであってもよく、一方で、他の場合には、ｉｎ ｃａｓｅ－ｉｎｓｅｎｓｉｔｉｖｅ ｓｔｒｉｎｇ ｍａｔｃｈｉｎｇのような近似で十分な場合もある。

【００９７】

ブロック６１２では、処理は、ネットワーク通信の許容性の指標を提供する。許容性の指標の提供は、ユーザへの通知（例えば、ダイアログボックス又は他のポップアップウィンドウを介して）、メッセージ（例えば、電子メール）の送信、ログの指標の記録、値を他の処理又はコードブロックにリターンする等を含んでもよい。

【００９８】

一部の実施形態は、追加又は代替的な機能を提供してもよい。一実施形態は、ウェブコンテキストで生じるようなユーザ認証を行う。既存の認証スキームは、ユーザ名／パスワードの組み合わせを用いる。一部の実施形態は、また、ユーザ名／パスワードの組み合わせスキームと共に上述されたような技術の１以上を用いてもよい。例えば、一実施形態は、ユーザ名及びパスワードに加えてＩＰアドレスをチェックしてもよい。ＩＰアドレスが割り当てられ、ネットワークに固有であるため、それらは、他者に容易に偽装しえない。よって、ハッカーがユーザのユーザ名及びパスワードを盗んだ場合、ハッカーは、正しいＩＰアドレスを有さないため、アカウントに侵入することができない。ポート番号及び他のプロパティ（例えば、時刻、地理的領域）は、また、認証スキームに含まれてもよい。これらのプロパティの全てが、ユーザの相互作用、介入又は関与なしで決定されるわけではないことを留意する。例えば、ＩＰアドレスは、ＴＣＰ／ＩＰスタックを直接参照して決定されてもよい。

【００９９】

また、現在のインターネットサービスプロバイダは、多くのユーザが同一のＩＰアドレスを共有するように、Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ（ＮＡＴ）又はプロキシサービスのいずれかを用いてもよい。一実施形態は、ＮＡＴ／ｐｒｏｘｙモジュールによって管理される内部ＩＰアドレスに対応する静的ＴＣＰポート番号を

割り当てるＮＡＴ／ｐｒｏｘｙサービス（例えば、ルーター又はゲートウェイによって提供される）を用いることによりＮＡＴ／ｐｒｏｘｙコンテキストにおいて機能して、各内部ＩＰは、同一のＩＰアドレスを有するが、固有かつ識別可能なポート番号を有さない。

【０１００】

一実施形態は、以下の追加動作を行うために図６の処理を拡張する：コンピュータシステムのＴＣＰ／ＩＰスタックから第１のＩＰアドレス及びポート番号を受信し、ネットワーク通信と関連付けられるｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ（ＵＲＬ）／ｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｉｄｅｎｔｉｆｉｅｒ（ＵＲＩ）を受信し、所有者名をＩＰアドレスと関連付けるアサイメントデータベースに対してＴＣＰ／ＩＰスタックから受信される第１のＩＰアドレスを問い合わせることにより、第１のＩＰアドレスと関連付けられる第１の名称を決定し、所有者名とドメインネームを関連付けるアサイメントデータベースに対してネットワークリソースと関連付けられるＵＲＬ／ＵＲＩのドメインネームを問い合わせることにより、ＵＲＬ／ＵＲＩと関連付けられる第２の名称を決定し、第１のＩＰアドレス及びポート番号が、信頼できるネットワークアドレスの予め設定されたホワイトリストに含まれているか、及び第１の名称が第２の名称と一致するかに基づいて通信動作が許容される又は許容されないことの指標を設定する。

【０１０１】

一部の実施形態は、通信を制御するシステムを提供し、通信を制御するシステムは、ＴＣＰ／ＩＰスタックを含み、ネットワークリソースと通信する通信インターフェースと、命令を記憶するメモリと、前記通信インターフェース及び前記メモリと通信されるプロセッサと、を備え、前記プロセッサは、認証されないネットワークノードのアドレスを含まず、かつ、信頼できるネットワークアドレスの各々に対して、許容通信プロパティの１以上の指標を含む、信頼できるネットワークアドレスの予め定義されたホワイトリストを受信し、前記ネットワーク通信に対応する第１のインターネットプロトコル（ＩＰ）アドレスを決定し、前記ネットワーク通信と関連付けられる第１の通信プロパティを決定し、前記第１のＩＰアドレスに対応する前記ホワイトリストにおけるエントリにより特定される許容通信プロパティである第２の通信プロパティを決定し、前記第１の通信プロパティが前記第２の通信プロパティで包含されるかどうかを判定することにより、前記ホワイトリストに対して前記ネットワーク通信を評価し、前記第１の通信プロパティが前記第２の通信プロパティで包含されないと判定したことに応じて、前記ネットワーク通信が許容されないことの指標を設定し、前記第１の通信プロパティが前記第２の通信プロパティで包含されると判定したことに応じて、前記ネットワーク通信が許容されることの指標を設定する、ことによってネットワーク通信を評価するように構成される。

【０１０２】

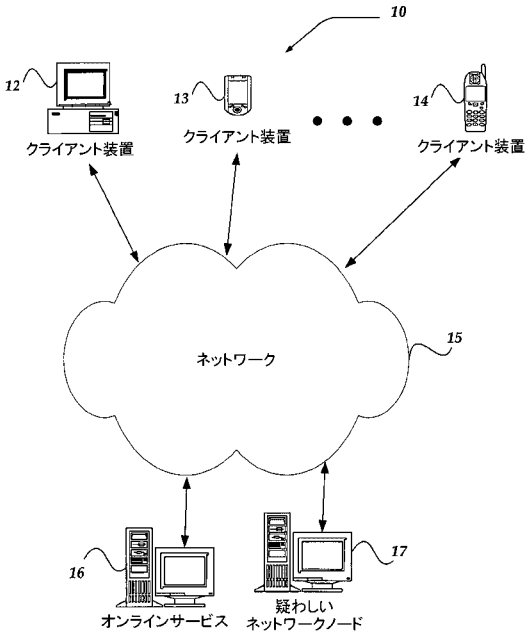
本明細書で引用される全ての参照文献は、これに限定されない、以下の関連出願を含み、その全体を参照によって援用する：２００７年２月２８日に出願された、発明の名称“Ｅｖａｌｕａｔｉｎｇ　ａ　Ｑｕｅｓｔｉｏｎａｂｌｅ　Ｎｅｔｗｏｒｋ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ”の米国特許出願第１１／７１２，６４８号、米国特許番号８，６２１，６０４、２００６年９月６日に出願された、発明の名称“Ｉｄｅｎｔｉｆｙｉｎｇ　Ａ　Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｓｏｕｒｃｅ　Ｆｏｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ”の米国特許出願第１１／４７０，５８１号、２００５年９月６日に出願された、発明の名称“Ｉｄｅｎｔｉｆｙｉｎｇ　Ａ　Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｓｏｕｒｃｅ　Ｆｏｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ”の米国特許仮出願第６０／７１４，８８９号、及び２００６年３月１７日に出願された、発明の名称“Ｉｄｅｎｔｉｆｙｉｎｇ　Ａ　Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｓｏｕｒｃｅ　Ｆｏｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ”の米国特許仮出願第６０／７８３，４４６号。

【０１０３】

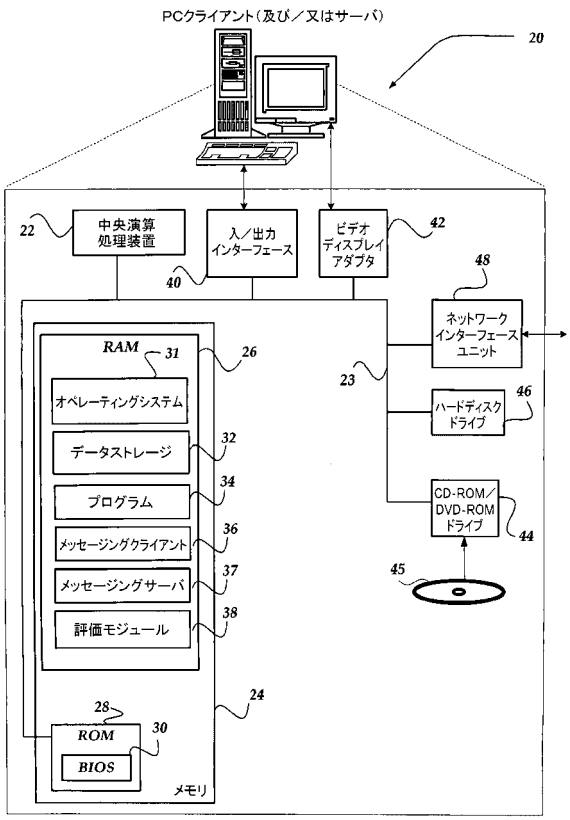
上記の発明の詳細な説明、実施例及びデータは、本発明の製造の完全な説明及び本発明の構成の使用を提供する。例えば、デジタル証明書は、認証のために用いられてもよく、暗号化は、通信のために用いられてもよく、他の構成が含まれてもよい。しかし、他の実

施形態は当業者によって明確であろう。本発明の多くの実施形態は、本発明の趣旨及び範囲から逸脱せずになされることができ、本発明は、以下に添付される特許請求の範囲に帰する。

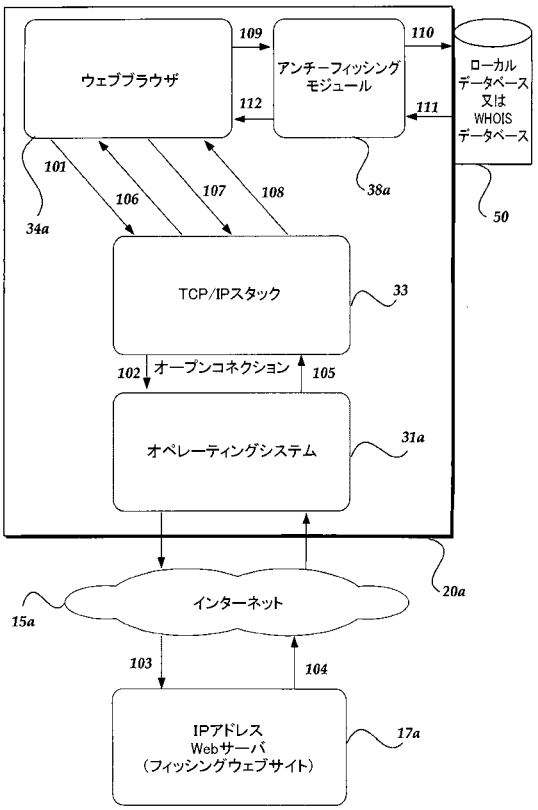
【図１】



【図２】



【図３】



【図４】

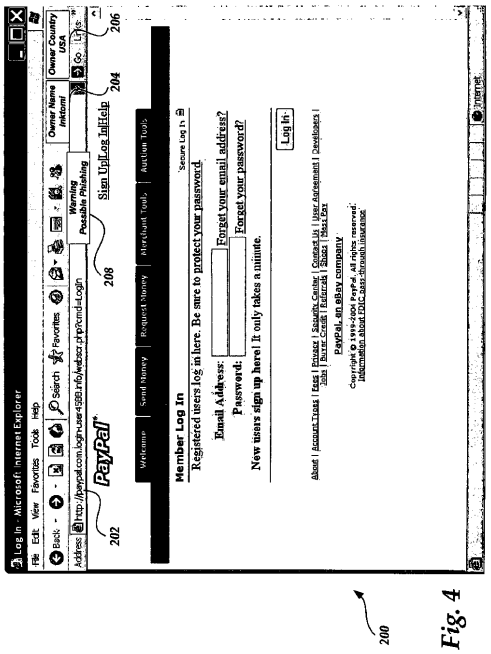
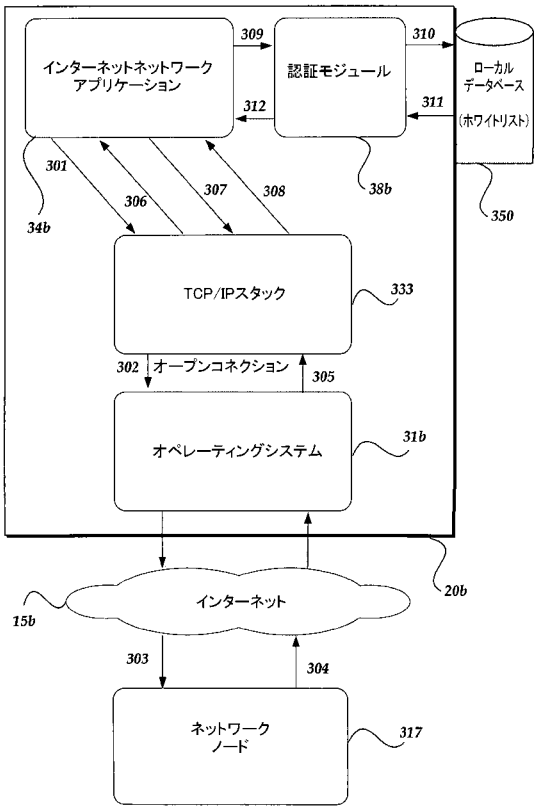
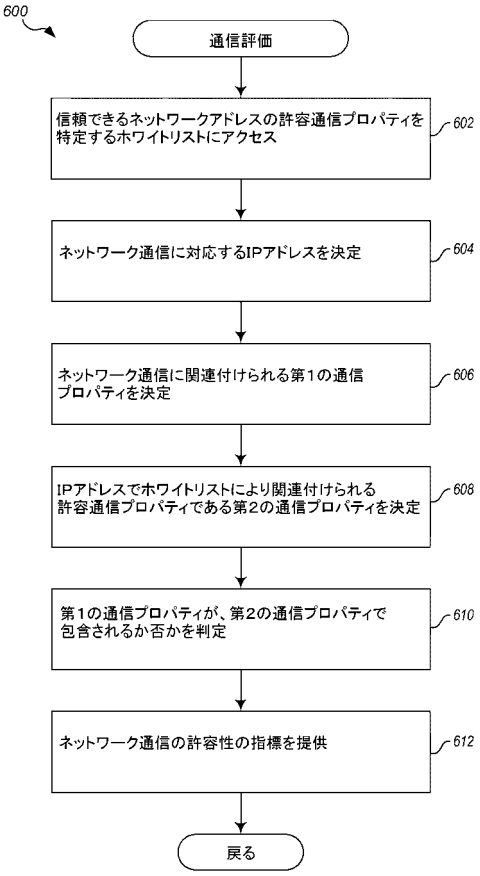


Fig. 4

【図５】



【図６】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 2014/031244

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/00 *(2006.01)*
G06F 21/51 *(2013.01)*

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)

G06F 21/00, 21/50-21/60, 15/00, 15/16, 15/163, 15/173, H04L 12/00, 12/28, 12/40, 12/54, 12/58, 29/00, 29/06, H04H 60/00, 60/61, H04W 12/00

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 practicable, search terms used)

PatSearch (RUPTO internal), USPTO, PAJ, Esp@cenet, DWPI, EAPATIS, PATENTSCOPE, Information Retrieval System of FIPS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/0043765 A1 (RHODERICK JOHN KENNEDY PUGH) 12.02.2009, abstract, par. [0063], [0064], [0068], [0071], [0074], [0095], [0108]	1-9, 12, 13
Y		10, 11, 14, 15
Y	US 2004/0162992 A1 (VIKASH KRISHNA SAMI et al.) 19.08.2004, par. [0067]	10, 11, 14, 15

☐ 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
06 August 2014 (06.08.2014)	21 August 2014 (21.08.2014)
Name and mailing address of the ISA/RU: FIPS, Russia, 123995, Moscow, G-59, GSP-5, Berezhkovskaya nab., 30-1 Facsimile No. +7 (499) 243-33-37	Authorized officer V. Aleksandrov Telephone No. 499-240-25-91

Form PCT/ISA/210 (second sheet) (July 2009)

フロントページの続き

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