(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4596554号
(P4596554)
(45)発行日　平成22年12月8日(2010.12.8)　(24)登録日　平成22年10月1日(2010.10.1)

(51)Int.Cl.　F I
H04L 9/36 (2006.01)　H04L 9/00 685

請求項の数 15 (全 10 頁)

(21)出願番号	特願2007-557463 (P2007-557463)	(73)特許権者	390009531
(86)(22)出願日	平成18年2月20日 (2006.2.20)		インターナショナル・ビジネス・マシーンズ・コーポレーション
(65)公表番号	特表2008-532398 (P2008-532398A)		INTERNATIONAL BUSINESS MASCHINES CORPORATION
(43)公表日	平成20年8月14日 (2008.8.14)		アメリカ合衆国10504 ニューヨーク州 アーモンク ニュー オーチャード ロード
(86)国際出願番号	PCT/EP2006/060107	(74)代理人	100108501
(87)国際公開番号	WO2006/089879		弁理士 上野 剛史
(87)国際公開日	平成18年8月31日 (2006.8.31)	(74)代理人	100112690
審査請求日	平成21年1月23日 (2009.1.23)		弁理士 太佐 種一
(31)優先権主張番号	11/067,990	(74)代理人	100091568
(32)優先日	平成17年2月28日 (2005.2.28)		弁理士 市位 嘉宏
(33)優先権主張国	米国(US)		

早期審査対象出願

最終頁に続く

(54)【発明の名称】暗号化されたＨＴＴＰＳネットワーク・パケットを、セキュアなウェブ・サーバ外部での復号なしに特定のＵＲＬ名および他のデータにマッピングするための、方法およびシステム（マッピン

(57)【特許請求の範囲】
【請求項１】
ネットワークを介してクライアントと通信可能なサーバが実行する方法であって、
（ａ）セキュアなウェブ・サーバ上にプラグイン・モジュールを作成し、取り込まれた暗号化されたネットワーク要求パケットから少なくとも１つのネットワーク・アドレスおよびポート番号を保存するステップと、
（ｂ）前記プラグイン・モジュールによって、前記セキュアなウェブ・サーバの復号モジュールから前記ネットワーク要求パケットの復号されたコピーが取得され、
（ｃ）前記コピーを取得した前記プラグイン・モジュールから、前記復号されたネットワーク・パケット、ネットワーク・アドレス、およびポート番号を取得するステップと、
（ｄ）前記保存するステップにおいて保存されたネットワーク・アドレスおよびポート番号と、前記取得するステップにおいて取得されたネットワーク・アドレスおよびポート番号との合致により、暗号化されたネットワーク要求パケットをその復号されたコピーに関連付けるステップと、
を有する、方法。
【請求項２】
前記ステップ（ｃ）が、前記ネットワーク・アドレスおよびポート番号によってインデックス付けされたデータ構造内に、前記ネットワーク・アドレスおよびポート番号と、前記復号されたネットワーク・パケットとを保存するステップをさらに有する、請求項１に記載の方法。

【請求項３】
前記ネットワークがインターネットであり、暗号化がセキュアなハイパーテキスト転送プロトコル（ＨＴＴＰＳ）に従って実行され、前記暗号化されたネットワーク要求がハイパーテキスト・マークアップ言語（ＨＴＭＬ）に準拠する、請求項１又は２に記載の方法。
【請求項４】
前記暗号化されたデータが、アプリケーション固有のコンテンツ、または、テキスト、オーディオ、ビデオ、グラフィック、アニメーション、静止画、プログラム・ファイル、ＨＴＭＬページ、およびＪＡＶＡ(登録商標)アプレットを含むグループから選択されたリモート・ターゲット・リソースへのハイパーテキスト・リンクを有する、請求項１乃至３のいずれかに記載の方法。
【請求項５】
前記復号が、ウェブ・サーバの従来の復号ソフトウェアによって、前記ウェブ・サーバの通常の処理の一部として実行され、前記プラグイン・モジュールがＷｅｂＦｉｌｔｅｒおよびＮＳＡＰＩを含むグループから選択され、前記取り込まれた暗号化されたネットワーク要求パケットからの前記ネットワーク・アドレスおよびポート番号が暗号化されずに転送される、請求項１乃至４のいずれかに記載の方法。
【請求項６】
前記（ｂ）において、前記復号されたネットワーク要求パケットに関連付けられた、オリジナルの暗号化された要求のネットワーク・アドレスおよびポート番号を取得するために、セキュアなウェブ・サーバで、前記プラグイン・モジュールがアプリケーション・プログラム・インターフェース（ＡＰＩ）をさらに呼び出す、請求項１乃至５のいずれかに記載の方法。
【請求項７】
前記ステップ（ｃ）が、前記プラグイン・モジュールがネットワーク・ソケットを作成し、前記復号されたＨＴＴＰＳネットワーク・パケット、前記ネットワーク・アドレス、およびポート番号を、パイプを介して転送するステップをさらに有する、請求項１乃至６のいずれかに記載の方法。
【請求項８】
ネットワークを介してクライアントと通信可能なシステムであり、
（ａ）セキュアなウェブ・サーバ上にプラグイン・モジュールを作成し、取り込まれた暗号化されたネットワーク要求パケットから少なくとも１つのネットワーク・アドレスおよびポート番号を保存するための手段と、
（ｂ）前記セキュアなウェブ・サーバの復号モジュールから前記ネットワーク要求パケットの復号されたコピーを取得するための前記プラグイン・モジュールと、
（ｃ）前記コピーを取得した前記プラグイン・モジュールから、前記復号されたネットワーク・パケット、ネットワーク・アドレス、およびポート番号を取得するための手段と、
（ｄ）前記保存するための手段において保存されたネットワーク・アドレスおよびポート番号と、前記取得するための手段において取得されたネットワーク・アドレスおよびポート番号との合致により、暗号化されたネットワーク要求パケットをその復号されたコピーに関連付ける手段と、
を有する、システム。
【請求項９】
前記（ｃ）のための手段が、前記ネットワーク・アドレスおよびポート番号によってインデックス付けされたデータ構造内に、前記ネットワーク・アドレスおよびポート番号と、前記復号されたネットワーク・パケットとを保存するための手段をさらに有する、請求項８に記載のシステム。
【請求項１０】
前記ネットワークがインターネットであり、暗号化がセキュアなハイパーテキスト転送プロトコル（ＨＴＴＰＳ）に従って実行され、前記暗号化されたネットワーク要求がハイ

パーテキスト・マークアップ言語（ＨＴＭＬ）に準拠する、請求項８又は９に記載のシステム。
【請求項１１】
前記暗号化されたデータが、アプリケーション固有のコンテンツ、または、テキスト、オーディオ、ビデオ、グラフィック、アニメーション、静止画、プログラム・ファイル、ＨＴＭＬページ、およびＪＡＶＡ(登録商標)アプレットを含むグループから選択されたリモート・ターゲット・リソースへのハイパーテキスト・リンクを有する、請求項８乃至１０のいずれかに記載のシステム。
【請求項１２】
前記復号が、ウェブ・サーバの従来の復号ソフトウェアによって、前記ウェブ・サーバの通常の処理の一部として実行され、前記プラグイン・モジュールがＷｅｂＦｉｌｔｅｒおよびＮＳＡＰＩを含むグループから選択され、前記取り込まれた暗号化されたネットワーク要求パケットからの前記ネットワーク・アドレスおよびポート番号が暗号化されずに転送される、請求項８乃至１１のいずれかに記載のシステム。
【請求項１３】
前記（ｂ）のための前記プラグイン・モジュールが、前記復号されたネットワーク要求パケットに関連付けられた、オリジナルの暗号化された要求のネットワーク・アドレスおよびポート番号を取得するために、セキュアなウェブ・サーバで、アプリケーション・プログラム・インターフェース（ＡＰＩ）を呼び出す手段をさらに有する、請求項８乃至１２のいずれかに記載のシステム。
【請求項１４】
前記（ｃ）のための手段が、前記プラグイン・モジュールがネットワーク・ソケットを作成し、前記復号されたＨＴＴＰＳネットワーク・パケット、前記ネットワーク・アドレス、およびポート番号を、パイプを介して転送する手段をさらに有する、請求項８乃至１３のいずれかに記載のシステム。
【請求項１５】
請求項１乃至７のいずれかに記載の方法をコンピュータに実行させるコンピュータ・プログラム。
【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・ネットワークの分野に関し、特に、暗号化されたＨＴＴＰＳネットワーク・パケットを、セキュアなウェブ・サーバ外部で復号を実行することなく、特定のＵＲＬ名および他の暗号化されたデータにかなり効率的にマッピングするための、方法およびシステムに関する。
【背景技術】
【０００２】
インターネットは、グローバルな情報交換を可能にするためにすべてが互いに通信し合う、異機種のコンピュータおよびサブネットワークの膨大なネットワークである。ワールド・ワイド・ウェブ（ＷＷＷ）は、テキスト、オーディオ、ビデオ、グラフィック、アニメーション、静止画などの形のマルチメディア情報にアクセスするために、ウェブ・ブラウザ・ソフトウェアを使用して、リモート・コンピュータまたはコンテンツ・サーバ上に配置されたドキュメントおよびファイルへのハイパーテキスト・リンクを復号する、インターネット上でのさらに人気の高い情報サービスの１つである。ユーザにとっては、公衆ネットワークおよび専用ネットワークにリモートにアクセスすることがますます必要となってきており、一般にセキュアでないインターネットなどの公衆ネットワークを介した、セキュアなサーバおよびネットワーク上で使用可能なリソースへのセキュアなアクセスを可能にする方法に関する問題が生じている。
【０００３】
ネットワーク性能モニタなどの、多くのハードウェアおよびソフトウェアのユーティリ

ティおよびアプリケーションは、それらの中心技術として、それらの入力としてのネットワーク・データに依存する、測定方法を有する。インターネットを介した電子商取引が展開されるほど、セキュアなネットワーク移送の使用が増加する。ウェブ・ブラウザによる暗号化は、セキュアなハイパーテキスト転送プロトコル（ＨＴＴＰＳ）を通じてインターネットを介してセキュアなデータを送信する、単一の最も多く使用されるソースである。ＨＴＴＰＳプロトコルの場合、ウェブ・ブラウザは、対応するセキュアなウェブ・サーバのみが復号できるようにネットワーク・データを強固に暗号化する、公開／秘密鍵技術を使用する。これらの暗号化されたネットワーク・フローへのアクセス権を有するハードウェアまたはソフトウェア・モニタの場合、それらのコンテンツに関するすべては言うまでもなく、それらのフォーマットに関するすべてを理解することは、事実上不可能である。このＨＴＴＰＳ環境での監視ツールに関する制限により、このネットワークのハードウェアおよびソフトウェア・モニタに対するデータの価値は、ＨＴＴＰＳの非セキュア・バージョンであるＨＴＴＰを使用する環境に対してのみ実現可能である。

【０００４】

さらに、セキュアなウェブ・サーバの外部で復号が実行される場合、政府によって規制された特別な復号ソフトウェアが必要であるため、マーケティングおよび流通にとっての魅力を低下させる。またこれは、顧客には許可されないウェブ・サーバ・セキュリティ証明書へのアクセス権を必要とするため、顧客にとっても魅力的でない。したがって、政府の規制、市場、および顧客に対してより許容可能な他の技法を使用することが重要である。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

したがって、ハードウェアおよびソフトウェア・ネットワーク・モニタが、動作に必要な情報を取得し、セキュア・ネットワーク・サーバ外部で特殊な復号ソフトウェアを使用せずに、あたかもＨＴＴＰ非セキュア環境で動作しているかのように同じデータを戻すことができるようにネットワーク・データの一部を復号するためにセキュアなネットワーク・サーバを使用する、単純な最適化された総称的な方法およびシステムが求められている。

【課題を解決するための手段】

【０００６】

本発明の前述および他の目的、特徴、および利点は、いくつかの図面を参照する好ましい諸実施形態の以下の詳細な説明から明らかとなろう。

【０００７】

本発明の好ましい一実施形態は、暗号化されたネットワーク要求パケットを、セキュアなコンピュータ・ネットワーク・ウェブ・サーバ内のその復号されたコピーにマッピングする方法である。この方法では、セキュアなウェブ・サーバ上にプラグイン・モジュールを作成し、取り込まれた暗号化されたネットワーク要求パケットから少なくとも１つのネットワーク・アドレスおよびポート番号を保存する。プラグイン・モジュールは、セキュアなウェブ・サーバ復号モジュールからネットワーク要求パケットの復号されたコピーを取得し、これをネットワーク・アドレスおよびポート番号と共に戻す。

【０００８】

本発明の他の好ましい実施形態は、本発明の前述の方法の諸実施形態を実施するシステムである。

【０００９】

本発明の他の好ましい実施形態は、本発明の前述の方法の諸実施形態の方法ステップを実行するための、コンピュータによって実行可能な命令のプログラムを有形に具体化する、コンピュータ使用可能メディアを含む。

【００１０】

次に図面を参照すると、全体を通じて同じ参照番号が対応する部分を表す。

【発明を実施するための最良の形態】
【００１１】
好ましい諸実施形態の以下の説明では、その一部を形成し、たとえば本発明が実施可能な特定の諸実施形態が示された、添付の図面を参照する。本発明の範囲を逸脱することなく、他の諸実施形態が利用可能であり、構造上および機能上の変更が可能であることを理解されよう。
【００１２】
本発明の主な目的は、ハードウェアおよびソフトウェア・ネットワーク・ユーティリティおよびアプリケーションがセキュア環境で動作できるようにすること、および、あたかもハイパーテキスト転送プロトコル（ＨＴＴＰ）の非セキュア環境で動作しているように、同じデータへのアクセス権を有すること、ならびにネットワーク・データの復号をウェブ・サーバの通常動作の一部としてセキュア・ウェブ・サーバによって実行させることである。
【００１３】
本発明は、暗号化されたネットワーク要求パケットを、セキュアなコンピュータ・ネットワーク・サーバ内のその復号されたコピーにマッピングする方法を実行するための、システム、方法、およびコンピュータによって実行可能な命令のプログラムを具体化するコンピュータ使用可能メディアを開示する。本発明のモニタ・モジュールは、ネットワーク要求パケットの復号されたコピーを、セキュアなウェブ・サーバ復号モジュールから取得する。
【００１４】
暗号化されたネットワーク要求は、好ましくは、暗号化されたハイパーテキスト・マークアップ言語（ＨＴＭＬ）要求であり、ウェブ・サイトにアクセスするためには、Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）名などのその暗号化されたデータが必要である。特殊な復号技術を実施する必要なしに、ＨＴＴＰＳネットワーク要求パケットから暗号化された情報を取得するために、本発明は、ウェブ・サーバの機能を使用して、復号されたＨＴＴＰＳネットワーク・パケットをウェブ・サーバ・プラグインの一部として送達させる。したがって本発明は、セキュアなウェブ・サーバの外部で復号を実施する必要がない。さらに、特殊な復号ソフトウェアも必要とせず、その通常の動作時にセキュアなウェブ・サーバの従来の復号ソフトウェアから取得したデータを利用する。このように、復号は、すでに政府によって承認され、すでにマーケティングおよび流通の世界で受け入れられ、すでに顧客によってデプロイされた、従来のウェブ・サーバ・ソフトウェアによって実行される。
【００１５】
本発明の主な態様では、ハードウェアまたはソフトウェアの監視ソフトウェアから見て完全に暗号化されたＨＴＭＬ要求を、セキュアなウェブ・サーバから見て完全に復号されたＨＴＭＬ要求にマッピングする。これは、すべての商用のセキュアなウェブ・サーバが、暗号化されたＨＴＭＬ要求パケットのコピーを取得するため、および復号後に、非セキュアなＨＴＴＰ環境から獲得されたデータに見えるようにデータを正規化する本発明のモニタに、復号された要求パケットのコピーを引き渡すために、公表された技法を提供するという事実によって、実施することができる。ＨＴＭＬ要求パケットの復号されたコピーを取得するために必要な公表された技法のタイプは、顧客によって使用されるベンダのセキュアなウェブ・サーバ・タイプに依存する。
【００１６】
図１は、本発明の好ましい諸実施形態に従った、効率的なマッピングを実行可能にするハードウェアおよびソフトウェア・ネットワーク環境を示す。このシステムは、図２の流れ図に示されるマッピングのためのアルゴリズムを使用する。図１のブロック図では、クライアント・サイト１００側の顧客が、ネットワーク３００を介して、好ましくはセキュアなサーバ・サイト２００と対話する。ネットワーク３００は、通常、インターネットを介したパケット交換プロトコルである、伝送制御プロトコル／インターネット・プロトコ

ル（ＴＣＰ／ＩＰ）を使用するインターネットである。クライアント・サイト１００は、ハイパーテキスト転送プロトコル（ＨＴＴＰ）の下で、またはセキュア・ハイパーテキスト転送プロトコル（ＨＴＴＰＳ）の下で、ウェブ・サイトに関する要求などのその要求を、図示されていないインターネット・サービス・プロバイダ（ＩＳＰ）に送信する、デスクトップまたはラップトップ型コンピュータ、携帯情報端末（ＰＤＡ）、車両搭載コンピュータ、携帯電話などとすることができる。ＩＳＰは、インターネットへのリンクを確立し、次にこれが、図示されていないコンテンツ・サーバに要求を渡し、これがその要求を、通常はＵｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（ＵＲＬ）名によってアドレス指定されたコンテンツ・プロバイダに転送する。

【００１７】

コンテンツ・サーバからの応答は、クライアント・サイト１００へと戻され、通常は、ＷＷＷ上でドキュメントを作成するための標準言語であるハイパーテキスト・マークアップ言語（ＨＴＭＬ）に準拠する。ＨＴＭＬは、ドキュメントの一部または全体をどのようにフォーマットするべきであるかを指定するためにドキュメントに挿入された様々なタグ・コマンドを使用して、ウェブ・ドキュメントの構造およびレイアウトを定義する。要求は、第３者の改ざんから保護するためにメッセージを暗号化および復号する、いずれかの主要なセキュリティ・プロトコルをサポートするコンテンツ・サーバである、セキュアなサーバに送信することができる。典型的なこうしたプロトコルが、公開および秘密鍵ならびにパスワードを利用した暗号化を使用する、Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ（ＳＳＬ）プロトコルであり、他の方法では暗号化されたデジタル証明書を使用する。ＳＳＬのソケットは、通常、ソフトウェア・オブジェクトである。

【００１８】

本発明の一意性は、ネットワーク監視ハードウェアまたはソフトウェアによって取り込まれたランダムな暗号化されたＨＴＭＬ要求を、ＵＲＬ名および監視ソフトウェアに価値を与える他の暗号化されたデータにマッピングすることにある。各ＨＴＴＰＳ要求は、要求の一部としてネットワーク上を流れ、要求の直前に収められた、短い暗号化されていないヘッダを有する。これは、ルータおよびスイッチなどのネットワーク・デバイスが、要求を宛先ネットワーク・アドレスにルーティングするために必要である。ネットワーク・デバイスは暗号化されたデータを読み取ることができないため、このヘッダは暗号化されないままでなければならない。このヘッダは、この発明に有利となるように使用される。ランダムな暗号化されたＨＴＭＬ要求がネットワーク監視ソフトウェアによって取り込まれた場合、後でこの暗号化された要求にアクセスするために、その起点および宛先ネットワーク・アドレスおよびポートがメモリ内データ構造に保存される。

【００１９】

例示的なマッピング手順に関するアルゴリズムが、図２の流れ図によって示される。本発明の好ましい諸態様では、クライアント・サイト１００のユーザは、ＨＴＴＰＳプロトコルを使用してそのネットワーク・パケットを暗号化する。これによって、ネットワーク・パケット・スニファ（Sniffer）などの、ネットワーク３００を横切るパケットを監視する技術でこれらを読み取ることができなくなり、対応するＨＴＴＰＳプロトコルを備えたウェブ・サーバのみが、受け取ったネットワーク・パケットを暗号化することができる。ユーザは、ネットワーク・パケットを暗号化し、ＨＴＴＰＳ要求をネットワーク３００上に置く、クライアント・サイト１００に配置されたウェブ・ブラウザ１１０を介して、サーバ・サイト２００と対話する。要求はネットワーク３００を横切り、本発明のモニタ２１０と命名された監視ソフトウェアが実行中のサーバ２００に到達する。モニタ２１０は、常時実行中のネットワーク・パケット・スニファ２２０と連絡する。したがって、モニタ２１０には、ネットワーク・パケットの暗号化されたコンテンツが見えるが、深く理解することはできない。しかしながら、たとえ暗号化されたネットワーク・パケットであっても、ヘッダ内には、復号の機能を持たないハードウェア・ルータによって使用されるために暗号化しないでおく必要のある、ネットワーク・アドレスおよびポート番号などの暗号化されていない部分を有する。したがってモニタ２１０は、他はともかくとして、暗

号化されたネットワーク・パケットのネットワーク・アドレスおよびポート番号だけは首尾よく読み取ることができる。しかしながらユーザは、ＵＲＬ名などの、暗号化されたネットワーク・パケットに埋め込まれた何らかのデータを読み取ることができる必要がある。したがって、図２のステップ４００で、モニタ２１０はプラグイン・モジュール２３０を作成し、ウェブ・サーバ２０５が開始された時点でウェブ・サーバ２０５に登録する。

【００２０】

ＵＲＬ名と他の暗号化されたデータとの間、およびクライアントのネットワーク・アドレスとポート番号との間でマッピングを実行するために、ステップ４１０で、モニタ２１０は、クライアント・サイト１００から発信され、ネットワーク・パケット・スニファ２２０から受け取った、暗号化されたネットワーク要求パケットからのネットワーク・アドレスおよびポート番号を保存する。次にモニタ２１０は、暗号化されたネットワーク・パケットのコピーを取り、その暗号化されたパケットをメモリ２５０内のデータ構造２４０に配置する。データ構造は、特定のルートＵＲＬに関するツリー、あるいはクライアント・サイトのネットワーク・アドレスおよびポート番号によってインデックス付けされたテーブルまたはキューとすることができる。

【００２１】

ウェブ・サーバ２０５では、ウェブ・サーバの通常の処理の一部として、ウェブ・サーバ２０５内部に配置されたウェブ・サーバの従来の復号ソフトウェア２２５によって、ネットワーク・パケットが復号される。プラグイン・モジュール２３０は、通常、Ｍｉｃｒｏｓｏｆｔ　ＩＩＳウェブ・サーバの場合、Ｗｅｂ　Ｆｉｌｔｅｒと呼ばれ、ＡｐａｃｈｅおよびＮｅｔｓｃａｐｅのウェブ・サーバの場合、ＮＳＡＰＩと呼ばれる。ステップ４２０で、プラグイン・モジュール２３０は、復号されたＨＴＭＬ要求からＨＴＴＰＳネットワーク・パケットのコピーを取得する。

【００２２】

プラグイン・モジュール２３０が、ウェブ・サーバの従来の復号ソフトウェア２２５からＨＴＴＰＳネットワーク・パケットの復号されたコピーを取得すると、ＵＲＬ名、ＵＲＬ参照者（referrer）、およびアプリケーション固有のコンテンツなどの重要なデータを、この要求のコピーから抽出することができる。しかしながら、Ｗｅｂ　ＦｉｌｔｅｒまたはＮＳＡＰＩが取得したのはＨＴＭＬ要求のコピーのみであるため、ネットワーク固有の情報は使用不可能であり、その情報こそが、オリジナルの暗号化された要求に合致する関係を築くために必要なものである。したがってセキュアなウェブ・サーバでは、この要求のコピーに関連付けられたネットワーク・アドレスおよびポート番号を得るために、いくつかのアプリケーション・プログラム・インターフェース（ＡＰＩ）を起動しなければならない。これらのＡＰＩは、それぞれのセキュアなウェブ・サーバ・ベンダによって異なる。したがってプラグイン・モジュール２３０は、ウェブ・サーバ２０５に対してＡＰＩ呼び出しを行い、ネットワーク・パケットに関連付けられたネットワーク・アドレスおよびポート番号を取得する。

【００２３】

次にプラグイン・モジュール２３０は、プラグイン・モジュール２３０とモニタ２１０との間にネットワーク通信ソケット２６０をオープンし、ステップ４３０で、復号されたＨＴＴＰＳネットワーク・パケット、ネットワーク・アドレス、およびポート番号を、パイプを介してモニタ２１０に渡す。次にモニタ２１０は、組み合わせ（merging）および正規化を実行する。モニタ２１０は、ネットワーク・アドレスおよびポート番号に基づいて、第１にメモリ内データ構造２４０の検索を実行し、そのネットワーク・アドレスおよびポート番号に基づいて、渡された復号されたＨＴＴＰＳネットワーク・パケットのエントリ合致を見つけるように試行する。

【００２４】

こうしたエントリが見つかった場合、格納済みのネットワーク・パケットの暗号化されたコンテンツは、プラグイン・モジュール２３０から受け取った復号されたコンテンツに置き換えられる。合致が見つからなかった場合、モニタ２１０はプラグイン・モジュール

２３０から受け取ったデータを破棄して続行する。合致エントリが存在する場合、通常はＵＲＬ名に関連付けることができない取り込まれた暗号化されたネットワークＨＴＴＰＳ要求と、ＵＲＬ名および他の以前に暗号化されたデータとのペアが作成され、ＨＴＴＰＳプロトコルによって隠されたネットワーク・モニタにデータを戻す。したがってモニタ２１０は、通常はプロトコルが、イメージ、プログラム・ファイル、ＨＴＭＬページ、ＪＡＶＡ（登録商標）アプレットなどとすることができるターゲット・リソースのＵＲＬ名などの、非セキュアなＨＴＴＰであった場合に有したであろう、すべての情報を、メモリ内データ構造２４０内に有する。

【００２５】

したがって、この時点でモニタ２１０は、ＵＲＬ名および他のデータを格納済みの復号されたネットワーク・パケットから抽出することが可能であり、それを、データ・マイニング、パターン認識、データ分析、ＨＴＭＬから無線アプリケーション・プロトコル（ＷＡＰ）へのトランスコーディング、データ変換、インターネットＨＴＴＰサーバ・アプリケーションの監視パフォーマンス、およびクライアントとサーバ・サイトとの間での通信ネットワークを介したデータ転送を含む、バンキングおよび他のソフトウェア・サービス、アプリケーションおよびデータ処理プログラムのためのネットワーク・トランザクションにおいて、様々なデータ管理ソリューションに使用することができる。

【００２６】

本発明は、ハードウェア、ファームウェアまたはソフトウェア、ハードウェア、ファームウェア、およびソフトウェアの任意の組み合わせ、あるいは、開示された機能を提供することが可能な任意の他のプロセスで、実現可能である。本発明の方法およびシステムの実施は、１つのサーバ・コンピュータ・システムにおける集中型で、または異なる要素がいくつかの相互接続されたコンピュータ・システムにわたって拡散している分散型で、実現可能である。本明細書に記載された方法を実施するように適合された任意のタイプのコンピュータ・システムまたは装置は、本明細書に記載された機能を実行するのに適している。図１は、ロードおよび実行された場合に、本発明の方法の諸態様を実施するような方法でコンピュータ・システムを制御する、コンピュータ・プログラムのグループを備えた汎用コンピュータ・システムを示す。コンピュータ・プログラムは、本明細書に記載された方法の実施を可能にし、コンピュータ・システム内にロードされた場合にこれらの方法を実施することができる、すべての機能を備えたコンピュータ使用可能メディア内に埋め込むことができる。図１の例示的な環境では、サーバ・サイト２００のコンピュータ・システムは、ディスク・ドライブなどの図示されていない１つまたは複数の電子ストレージ・デバイスに接続可能な、図示されていない１つまたは複数のプロセッサからなる。

【００２７】

本発明の好ましい諸実施形態の前述の説明は、例示および説明の目的で提示したものである。これは、本発明を網羅するか、または開示された精密な形に限定することを意図するものではない。前述の教示に鑑みて、多くの修正形態および変形形態が可能である。本発明の範囲は、詳細な説明によってではなく、添付の特許請求の範囲によって限定されるものであることが意図される。

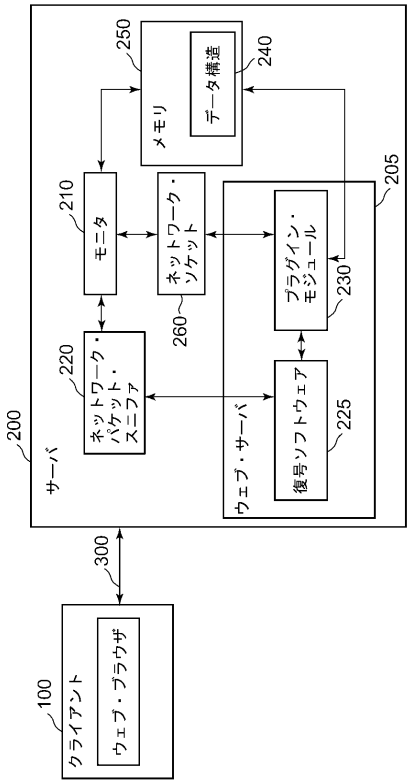
【図面の簡単な説明】

【００２８】

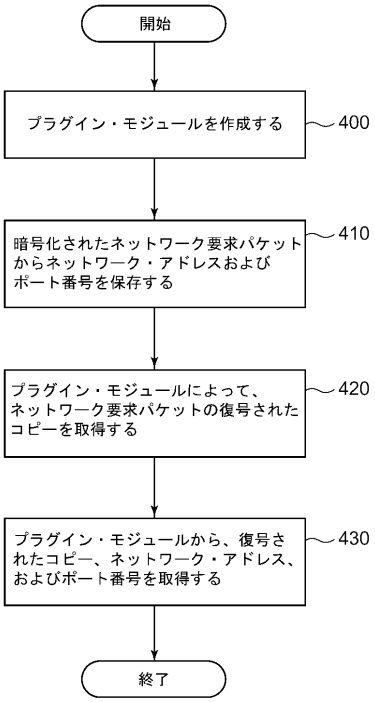
【図１】本発明の好ましい諸実施形態に従った、効率的なマッピングを実行可能にするハードウェアおよびソフトウェア・ネットワーク環境を示す図である。

【図２】本発明の好ましい諸実施形態に従った、マッピングの最上位流れ図を示す図である。

【図１】


200
サーバ
250
メモリ
240
データ構造
210
モニタ
220
ネットワーク・パケット・スニファ
260
ネットワーク・ソケット
205
ウェブ・サーバ
230
プラグイン・モジュール
225
復号ソフトウェア
300
100
クライアント
ウェブ・ブラウザ

【図２】


開始
プラグイン・モジュールを作成する
400
暗号化されたネットワーク要求パケットからネットワーク・アドレスおよびポート番号を保存する
410
プラグイン・モジュールによって、ネットワーク要求パケットの復号されたコピーを取得する
420
プラグイン・モジュールから、復号されたコピー、ネットワーク・アドレス、およびポート番号を取得する
430
終了

フロントページの続き

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 クライン、ポール、フレドリック
アメリカ合衆国９１３２０ カリフォルニア州ニューバリー・パーク フォックス・スプリングス・サークル １７１５
(72)発明者 ペレス、ジェシー、ニコラス
アメリカ合衆国３４４３６ フロリダ州フローラル・シティー マジェスティック・ポイント １３４００エス

審査官 中里 裕正

(56)参考文献 特開２００４－３５０２９６（ＪＰ，Ａ）
特開２００４－３０４７５２（ＪＰ，Ａ）
Almgren, M. et al., Application-Integrated Data Collection for Security Monitoring, Lecture Notes in Computer Science, ２００１年, Vol. 2212, p.22-36, [２０１０年４月９日検索], ＵＲＬ, http://www.ce.chalmers.se/~almgren/#publications

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/36
JSTPlus/JMEDPlus/JST7580(JDreamII)

(54)【発明の名称】暗号化されたＨＴＴＰＳネットワーク・パケットを、セキュアなウェブ・サーバ外部での復号なしに特定のＵＲＬ名および他のデータにマッピングするための、方法およびシステム（マッピングすること）