(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5254656号
(P5254656)
(45)発行日　平成25年8月7日(2013.8.7)　(24)登録日　平成25年4月26日(2013.4.26)

(51)Int.Cl.　F I
H04L 12/70 (2013.01)　H04L 12/56 400Z
G06F 21/55 (2013.01)　G06F 21/00 155A

請求項の数 20　(全 27 頁)

(21)出願番号　特願2008-122127 (P2008-122127)
(22)出願日　平成20年5月8日 (2008.5.8)
(65)公開番号　特開2008-283686 (P2008-283686A)
(43)公開日　平成20年11月20日 (2008.11.20)
審査請求日　平成23年4月27日 (2011.4.27)
(31)優先権主張番号　11/746,188
(32)優先日　平成19年5月9日 (2007.5.9)
(33)優先権主張国　米国 (US)

(73)特許権者　501113353
シマンテック　コーポレーション
Ｓｙｍａｎｔｅｃ　Ｃｏｒｐｏｒａｔｉｏｎ
アメリカ合衆国，カリフォルニア州　９４０４３，マウンテン　ビュー，エリス　ストリート　３５０
(74)代理人　100147485
弁理士　杉村　憲司
(72)発明者　ショーン・クーリー
アメリカ合衆国カリフォルニア州９０２４５・エルセグンド・ウエストマリポーサ６２４

最終頁に続く

(54)【発明の名称】ドライブバイ・ファーミングに対するリファラーチェックを介したクライアント側の保護

(57)【特許請求の範囲】
【請求項１】
コンピュータで実行される方法であって、
ＨＴＴＰヘッダーを含むＨＴＴＰリクエストをルータにリリースする前に、クライアント・コンピュータシステムで、前記ＨＴＴＰリクエストをプロキシするステップと、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別するか否かを判定するステップと、
前記ＨＴＴＰヘッダーを判定する前記ステップにおいて、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別すると判定したとき、
前記ＨＴＴＰリクエストをブロックするステップと、
アラート通知を発生するステップとを含むことを特徴とするコンピュータで実行される方法。
【請求項２】
前記ＨＴＴＰリクエストをブロックする前記ステップの前に、
前記ＨＴＴＰリクエストのブロックを解除するか否かを判定するステップと、
前記ＨＴＴＰリクエストのブロックの解除を判定する前記ステップにおいて、
前記ＨＴＴＰリクエストのブロックを解除すると判定したとき、前記ＨＴＴＰリクエス

トをリリースするステップと、
前記ＨＴＴＰリクエストのブロックを解除しないと判定したとき、前記ＨＴＴＰリクエストをブロックするステップとをさらに含むことを特徴とする請求項１に記載のコンピュータで実行される方法。
【請求項３】
前記ＨＴＴＰリクエストをブロックする前記ステップの前に、
ユーザに、前記ＨＴＴＰリクエストのブロックを承認するか又は拒否するかを入力させるステップと、
前記ＨＴＴＰリクエストのブロックの拒否を受信したとき、前記ＨＴＴＰリクエストをリリースするステップと、
前記ＨＴＴＰリクエストのブロックの承認を受信したとき、前記ＨＴＴＰリクエストをブロックするステップとをさらに含むことを特徴とする請求項１に記載のコンピュータで実行される方法。
【請求項４】
前記ＨＴＴＰヘッダーを判定する前記ステップにおいて、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別しないと判定したとき、
前記ＨＴＴＰリクエストをリリースするステップをさらに含み、
前記ＨＴＴＰリクエストをリリースする前記ステップにおいて、
前記ＨＴＴＰリクエストを、リリースされたＨＴＴＰリクエストとして、前記ターゲットＵＲＬへ送信されるようにすることを特徴とする請求項１に記載のコンピュータで実行される方法。
【請求項５】
前記リリースされたＨＴＴＰリクエストに応じて受信されたＨＴＴＰレスポンスをプロキシするステップと、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別するか否かを判定するステップと、
前記ＨＴＴＰレスポンスを判定する前記ステップにおいて、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別しないと判定したとき、
前記ＨＴＴＰレスポンスを送信するステップと、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別すると判定したとき、
悪意のある行動を防止するために前記コンテンツを修正するステップと、
前記ＨＴＴＰレスポンスをリリースするステップとをさらに含むことを特徴とする請求項４に記載のコンピュータで実行される方法。
【請求項６】
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツを識別すると判定したとき、悪意のある行動を防止するために前記コンテンツを修正する前記ステップが、
前記コンテンツに存在する各ＨＴＭＬ参照ＵＲＬを識別するため、前記コンテンツを解析するステップと、
前記各ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応するか否かを判定するステップと、
前記各ＨＴＭＬ参照ＵＲＬを判定する前記ステップにおいて、
ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応しているとき、
前記ＨＴＭＬ参照ＵＲＬを安全なＵＲＬに置き換えるステップと、
前記ＨＴＴＰリクエストをリリースするステップとをさらに含むことを特徴とする請求

項５に記載のコンピュータで実行される方法。
【請求項７】
前記ＨＴＴＰレスポンスが、コンテンツタイプがスクリプトのコンテンツを識別すると判定したとき、悪意のある行動を防止するために前記コンテンツを修正する前記ステップが、
前記コンテンツの先頭に、かつ任意のスクリプトの前に、安全なＸＭＬＨＴＴＰリクエストＡＰＩ及びアクティブＸ置換オブジェクトを定義するジャバスクリプト・オーバライドを挿入するステップと、
前記ジャバスクリプト・オーバライド以外の各スクリプトを識別するため、前記コンテンツを解析するステップと、
前記各スクリプトにＸＭＬＨＴＴＰリクエストＡＰＩがある場合、前記安全なＸＭＬＨＴＴＰリクエストＡＰＩに置き換えるステップと、
前記各スクリプトにオブジェクトタグがある場合、前記アクティブＸ置換オブジェクトに置き換えるステップと、
前記ＨＴＴＰリクエストをリリースするステップとをさらに含むことを特徴とする前記請求項５に記載のコンピュータで実行される方法。
【請求項８】
コンピュータプログラムコードを含むコンピュータで読み出し可能な有形のメディアを含むコンピュータプログラムであって、
ＨＴＴＰヘッダーを含むＨＴＴＰリクエストをルータに送信する前に、クライアントコンピュータで、前記ＨＴＴＰリクエストをプロキシするためのクライアント・アンチファーミング・アプリケーションを含み、
前記クライアント・アンチファーミング・アプリケーションが、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別するか否かを判定するステップと、
前記ＨＴＴＰヘッダーを判定する前記ステップにおいて、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別すると判定したとき、
前記ＨＴＴＰリクエストをブロックするステップと、
アラート通知を発生するステップとをさらに含むことを特徴とするコンピュータプログラム。
【請求項９】
前記クライアント・アンチファーミング・アプリケーションが、
前記ＨＴＴＰリクエストをブロックする前記ステップの前に、前記ＨＴＴＰリクエストのブロックを解除するか否かを判定するステップと、
前記ＨＴＴＰリクエストのブロックの解除を判定する前記ステップにおいて、
前記ＨＴＴＰリクエストのブロックを解除すると判定したとき、前記ＨＴＴＰリクエストをリリースするステップと、
前記ＨＴＴＰリクエストのブロックを解除しないと判定したとき、前記ＨＴＴＰリクエストをブロックするステップとをさらに含むことを特徴とする請求項８に記載のコンピュータプログラム。
【請求項１０】
前記クライアント・アンチファーミング・アプリケーションが、
前記ＨＴＴＰリクエストをブロックする前記ステップの前に、ユーザに、前記ＨＴＴＰリクエストのブロックを承認するか又は拒否するかを入力させるステップと、
前記ＨＴＴＰリクエストのブロックの拒否を受信したとき、前記ＨＴＴＰリクエストをリリースするステップと、
前記ＨＴＴＰリクエストのブロックの承認を受信したとき、前記ＨＴＴＰリクエストを

ブロックするステップとをさらに含むことを特徴とする請求項８に記載のコンピュータプログラム。
【請求項１１】
前記ＨＴＴＰヘッダーを判定する前記ステップにおいて、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別しないと判定したとき、
前記クライアント・アンチファーミング・アプリケーションが、
前記ＨＴＴＰリクエストをリリースするステップをさらに含み、
前記ＨＴＴＰリクエストをリリースする前記ステップにおいて、
前記ＨＴＴＰリクエストを、リリースされたＨＴＴＰリクエストとして、前記ターゲットＵＲＬへ送信されるようにすることを特徴とする請求項８に記載のコンピュータプログラム。
【請求項１２】
前記クライアント・アンチファーミング・アプリケーションが、
リリースされたＨＴＴＰリクエストに応じて受信されたＨＴＴＰレスポンスをプロキシするステップと、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別するか否かを判定するステップと、
前記ＨＴＴＰレスポンスを判定する前記ステップにおいて、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別しないと判定したとき、
前記ＨＴＴＰレスポンスをリリースするステップと、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別すると判定したとき、
悪意のある行動を防止するために前記コンテンツを修正するステップと、
前記ＨＴＴＰレスポンスをリリースするステップとをさらに含むことを特徴とする請求項８に記載のコンピュータプログラム。
【請求項１３】
前記ＨＴＴＰレスポンスを判定する前記ステップにおいて、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツを識別すると判定したとき、
前記クライアント・アンチファーミング・アプリケーションが、
前記コンテンツに存在する各ＨＴＭＬ参照ＵＲＬを識別するため、前記コンテンツを解析するステップと、
前記各ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応するか否かを判定するステップと、
前記各ＨＴＭＬ参照ＵＲＬを判定する前記ステップにおいて、
ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応するとき、
前記ＨＴＭＬ参照ＵＲＬを安全なＵＲＬに置き換えるステップとをさらに含むことを特徴とする請求項１２に記載のコンピュータプログラム。
【請求項１４】
前記ＨＴＴＰレスポンスを判定する前記ステップにおいて、
前記ＨＴＴＰレスポンスが、コンテンツタイプがスクリプトのコンテンツを識別すると判定したとき、
前記クライアント・アンチファーミング・アプリケーションが、
安全なＸＭＬＨＴＴＰリクエストＡＰＩ及びアクティブＸ置換オブジェクトを含むジャバスクリプト・オーバライドを、前記コンテンツの先頭に、かつ任意のスクリプトの前に挿入するステップと、

前記ジャバスクリプト・オーバライド以外の各スクリプトを識別するため、前記コンテンツを解析するステップと、
前記各スクリプトにＸＭＬＨＴＴＰリクエストＡＰＩがある場合、前記安全なＸＭＬＨＴＴＰリクエストＡＰＩに置き換えるステップと、
前記各スクリプトにオブジェクトタグがある場合、前記アクティブＸ置換オブジェクトに置き換えるステップとをさらに含むことを特徴とする請求項１２に記載のコンピュータプログラム。
【請求項１５】
コンピュータシステムであって、
クライアント・アンチファーミング・アプリケーションを記憶させたメモリと、
前記メモリに接続したプロセッサとを含み、
前記クライアント・アンチファーミング・アプリケーションを実行すると、
ＨＴＴＰヘッダーを含むＨＴＴＰリクエストをルータに送信する前に、クライアント・コンピュータシステムで、前記ＨＴＴＰリクエストをプロキシするステップと、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別するか否かを判定するステップと、
前記ＨＴＴＰヘッダーを判定する前記ステップにおいて、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別すると判定したとき、
前記ＨＴＴＰリクエストをブロックするステップと、
アラート通知を発生するステップとを含む方法が実行されることを特徴とするコンピュータシステム。
【請求項１６】
前記ＨＴＴＰリクエストをブロックする前記ステップの前に、ユーザに、前記ＨＴＴＰリクエストのブロックを承認するか又は拒否するかを入力させるステップと、
前記ＨＴＴＰリクエストのブロックの拒否を受信したとき、前記ＨＴＴＰリクエストを送信するステップと、
前記ＨＴＴＰリクエストのブロックの承認を受信したとき、前記ＨＴＴＰリクエストをブロックするステップとをさらに含むことを特徴とする請求項１５に記載のコンピュータシステム。
【請求項１７】
前記ＨＴＴＰヘッダーを判定する前記ステップにおいて、
前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別しないと判定したとき、
前記ＨＴＴＰリクエストをリリースするステップをさらに含み、
前記ＨＴＴＰリクエストをリリースする前記ステップにおいて、
前記ＨＴＴＰリクエストを、リリースされたＨＴＴＰリクエストとして、前記ターゲットＵＲＬへ送信されるにようすることを特徴とする請求項１５に記載のコンピュータシステム。
【請求項１８】
前記リリースされたＨＴＴＰリクエストに応じて受信されたＨＴＴＰレスポンスをプロキシするステップと、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別するか否かを判定するステップと、
前記ＨＴＴＰレスポンスを判定する前記ステップにおいて、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別しないと判定したとき、

前記ＨＴＴＰレスポンスをリリースするステップと、
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツ又はコンテンツタイプがスクリプトのコンテンツを識別すると判定したとき、
悪意のある行動を防止するために前記コンテンツを修正するステップと、
前記ＨＴＴＰレスポンスをリリースするステップとをさらに含むことを特徴とする請求項１７に記載のコンピュータシステム。
【請求項１９】
前記ＨＴＴＰレスポンスが、コンテンツタイプがtext/htmlのコンテンツを識別すると判定したとき、悪意のある行動を防止するために前記コンテンツを修正する前記ステップが、
前記コンテンツに存在する各ＨＴＭＬ参照ＵＲＬを識別するため、前記コンテンツを解析するステップと、
前記各ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応するか否かを判定するステップと、
前記各ＨＴＭＬ参照ＵＲＬを判定するステップにおいて、
ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応するとき、
前記ＨＴＭＬ参照ＵＲＬを安全なＵＲＬに置き換えるステップと、
前記ＨＴＴＰリクエストをリリースするステップとをさらに含むことを特徴とする請求項１８に記載のコンピュータシステム。
【請求項２０】
前記ＨＴＴＰレスポンスが、前記コンテンツタイプがスクリプトの前記コンテンツを識別すると判定したとき、悪意のある行動を防止するために前記コンテンツを修正する前記ステップが、
安全なＸＭＬＨＴＴＰリクエストＡＰＩ及びアクティブＸ置換オブジェクトを定義するジャバスクリプト・オーバライドを、前記コンテンツの先頭に、かつ任意のスクリプトの前に挿入するステップと、
前記ジャバスクリプト・オーバライド以外の各スクリプトを識別するため、前記コンテンツを解析するステップと、
前記各スクリプトにＸＭＬＨＴＴＰリクエストＡＰＩがある場合、前記安全なＸＭＬＨＴＴＰリクエストＡＰＩに置き換えるステップと、
前記各スクリプトにオブジェクトタグがある場合、前記アクティブＸ置換オブジェクトに置き換えるステップと、
前記ＨＴＴＰリクエストをリリースするステップとをさらに含むことを特徴とする請求項１８に記載のコンピュータシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータシステムに関するものである。より詳しくは、本発明は、コンピュータのセキュリティに関するものである。
【背景技術】
【０００２】
低価格のブロードバンドルータは、コンピュータユーザが、ホームネットワークや、ワイヤレスホームネットワークを作る際によく使用されている。残念なことに、ユーザが悪意のあるウェブページを訪れることによって、そのユーザのルータは知らぬ間に悪質な攻撃を受ける。クライアント側のルータに組み込まれ得るあるタイプの悪質な攻撃は、ドライブバイ・ファーミング（drive-by pharming）攻撃と呼ばれるものであり、サービスの拒否、悪意のあるコードによる感染、又は個人情報の盗難のほか、その他の迷惑な結果をもたらす。
【発明の開示】

【課題を解決するための手段】
【０００３】
本発明のある実施形態によれば、ドライブバイ・ファーミング攻撃からクライアント・コンピュータシステムを保護するための方法であって、ＨＴＴＰヘッダーを含むＨＴＴＰリクエストをルータにリリースする前に、クライアント・コンピュータシステムで、前記ＨＴＴＰリクエストをプロキシするステップと、前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別するか否かを判定するステップとを含み、前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別すると判定したとき、前記ＨＴＴＰリクエストをブロックするステップと、アラート通知を発生するステップとをさらに含む方法を提供する。前記ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬ及びルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬを識別しないと判定したとき、前記ＨＴＴＰリクエストはリリースされる。
【０００４】
本発明の別の実施形態によれば、前記方法はさらに、リリースされたＨＴＴＰリクエストをウェブブラウザに送信する前に、前記リリースされたＨＴＴＰリクエストに対するＨＴＴＰレスポンスをプロキシするステップと、前記ＨＴＴＰレスポンスのコンテンツタイプを判定するステップと、前記コンテンツタイプがtext/htmlタイプ又はスクリプトタイプか否かを判定するステップとを含み、前記コンテンツタイプがtext/htmlタイプ又はスクリプトタイプであると判定されたとき、悪意のある行動を防止するために前記コンテンツを修正するステップと、前記ＨＴＴＰレスポンスをリリースするステップとをさらに含む。前記コンテンツタイプがtext/htmlタイプ又はスクリプトタイプではないと判定されたとき、ＨＴＴＰレスポンスはリリースされる。
【０００５】
前記コンテンツタイプがtext/htmlタイプのとき、悪意のある行動を防止するために前記コンテンツを修正する前記ステップが、各ＨＴＭＬ参照ＵＲＬについてＨＴＭＬコンテンツを解析するステップと、各ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応するか否かを判定するステップとを含み、ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応すると判定されたとき、前記ＨＴＭＬ参照ＵＲＬを安全なＵＲＬに置き換えるステップと、前記ＨＴＴＰレスポンスをリリースするステップとをさらに含む。ある実施形態では、ユーザへ警告が通知される。ＨＴＭＬ参照ＵＲＬが、ルーティング不可能なプライベートＩＰアドレスに対応しないと判定されたとき、ＨＴＴＰレスポンスがリリースされる。
【０００６】
前記コンテンツタイプがスクリプトタイプのとき、悪意のある行動を防止するために前記コンテンツを修正するステップが、安全なＸＭＬＨＴＴＰリクエスト及び安全なアクティブＸ置換オブジェクトを定義するジャバスクリプト・オーバライドを、前記コンテンツの先頭、かつ任意のスクリプトの前に挿入するステップと、前記ジャバスクリプト・オーバライド以外のスクリプトについて前記コンテンツを解析するステップと、各スクリプトの各ＸＭＬＨＴＴＰリクエストを安全な各ＸＭＬＨＴＴＰリクエストに置き換えるステップと、各スクリプトの各オブジェクトタグをアクティブＸ置換オブジェクトに置き換えるステップと、前記ＨＴＴＰレスポンスをリリースするステップとをさらに含む。
【０００７】
本明細書で説明される実施形態は、以下の詳細な説明を添付の図面と共に参照することによって、最も良く理解されるであろう。
【発明を実施するための最良の形態】
【０００８】
ルータを利用した代表的なホームネットワークにおいては、ユーザが、ウェブページの

ＵＲＬなどのリソースに対するリクエスト（要求）をホームネットワークのクライアント・コンピュータシステム上でウェブブラウザに入力する。ウェブブラウザは、ホームネットワーク上のコンピュータシステムについてのＤＮＳ設定を管理するルータに送信されるウェブページに対するＨＴＴＰリクエストを生成する。一般的に、ルータは、ＤＮＳルックアップを実行してリクエストされたウェブページのＵＲＬに対応するＩＰアドレスを割り出し、それが終わると、前記ＨＴＴＰリクエストは、ウェブページをホストする対応するサーバに送信される。

【０００９】

ドライブバイ・ファーミング攻撃においては、ドライブバイ・ファーミング・コードなどの悪意のあるコードを含むウェブページが、前記ＨＴＴＰリクエストに対するＨＴＴＰレスポンスとして返信される。ユーザのウェブブラウザにおいて前記ウェブページを起動すると、悪意のあるコードが、ルータのＩＰアドレスを突き止めようとしてウェブブラウザからルータへＨＴＴＰリクエストを送信する。そして、ルータのＩＰアドレスを入手すると、悪意のあるコードは、ルータのウェブインタフェースに接続して、ＤＮＳレゾリューションが偽のウェブサイトにリダイレクト（出力先変更）するようにＤＮＳ設定を変更する。

【００１０】

多くの場合、偽のウェブサイトの見た目は、ユーザがリダイレクトを警戒しないように、本物のウェブサイトそっくりに似せている。このことにより、ユーザが偽のウェブサイトに入力した情報、例えば個人情報及びパスワードが、攻撃者に詐取されてしまう。そして、攻撃者が、ユーザの情報を利用したデータへの不正アクセスやユーザの銀行口座から金を盗むなどの悪質な行為を行うことが可能となる。ドライブバイ・ファーミングに関する更なる情報は、シド・スタム（Sid Stamm）、ズルフィカル・ラムザン（Zulfikar Ramzan）及びマーカス・ヤコブソン（Markus Jakobsson）による論文「ドライブバイ・ファーミング（Drive-By Pharming）」（２００６年１２月１３日）に記載されている（http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf.参照）。

【００１１】

ＨＴＴＰリクエストにおいては、リクエストされたリソースは通常、ＵＲＬ（Uniform Resource Locator）によって識別される。ＵＲＬは、ＨＴＴＰを介してアクセス可能なリソースの位置を指定する一連のテキストである。例えば、ＨＴＴＰを用いて、ＵＲＬは、「http://abigbank.com」のように記述することができる。

【００１２】

ＵＲＬは、一般的に、例えばウェブブラウザによってドメインネームサーバ（ＤＮＳ）クエリを介して特定のインターネットプロトコル（ＩＰ）アドレスに分解される。通常、ＩＰアドレスは３２ビットの数である。したがって、例えば、「http://abigbank.com」というＵＲＬを「25.234.56.71」というＩＰアドレスに分解する。

【００１３】

ＩＰアドレスは、プライベートＩＰアドレス又はパブリックＩＰアドレスのいずれかである。ＵＲＬは特定のＩＰアドレスに対応するので、本明細書中では、プライベートＩＰアドレスに対応するＵＲＬをプライベートＵＲＬと称し、パブリックＩＰアドレスに対応するＵＲＬをパブリックＵＲＬと称する。

【００１４】

本明細書中では、プライベートＩＰアドレスは、ルーティング不可能なＩＰアドレスである。すなわち、プライベートＩＰアドレスは、インターネットへの直接接続に使用することができない。一般的に、ホームルータによってサービスを提供されるホームネットワーク上のクライアント・コンピュータシステムに割り当てられるＩＰアドレスは、ルーティング不可能なプライベートＩＰアドレスである。例えば、通常、ドット形式１０進表記法に対応するＩＰアドレス、10.x.x.x、172.16.x.x、192.168.x.xは、プライベートＩＰアドレスであり、ルーティング不可能である。

【００１５】

本明細書中では、パブリックＩＰアドレスは、ルーティング可能であるＩＰアドレスである。すなわち、パブリックＩＰアドレスは、インターネットへの直接接続に使用することができる。一般的に、インターネット上でウェブページをホストするウェブサーバに割り当てられるＩＰアドレスは、ルーティング可能なパブリックＩＰアドレスである。例えば、通常、ドット形式１０進表記法に対応しないＩＰアドレス、10.x.x.x、172.16.x.x、192.168.x.xは、パブリックＩＰアドレスであり、ルーティング可能である。

【００１６】

ウェブページなどのリソースに対するＨＴＴＰリクエストのフォーマットは、ＨＴＴＰリクエストについての情報を提供するＨＴＴＰヘッダーを必要とするＨＴＴＰプロトコルによって指定される。ＨＴＴＰプロトコルは、ＨＴＴＰヘッダー中に利用可能な多数のフィールドを定義する。具体的には、ＨＴＴＰクライアントからのＨＴＴＰリクエストは、一般的に、ターゲットＵＲＬフィールドと、リファラーＵＲＬフィールドとを含む。ターゲットＵＲＬフィールドは、リクエストされたＵＲＬ（本明細書中では「ターゲットＵＲＬ」と称する）を識別するデータを含む。リファラーＵＲＬフィールドは、ＨＴＴＰリクエストが開始されたときにユーザが現在のページへ移動するのに辿ったリンクを含むページのＵＲＬ（本明細書中では「リファラーＵＲＬ」と称する）を識別するデータを含む。

【００１７】

また、ＨＴＴＰリクエストに対するＨＴＴＰレスポンスのフォーマットも、ＨＴＴＰレスポンスについての情報を提供するＨＴＴＰヘッダーを必要とするＨＴＴＰプロトコルによって指定される。ＨＴＴＰレスポンスは、一般的に、ＨＴＴＰメッセージ・フィールド（コンテンツ・フィールドと呼ばれることもある）を含む。ＨＴＴＰメッセージ・フィールドは、例えば、ＨＴＭＬウェブページ、スクリプト、ファイル又はプログラムコードなどの、リクエストされたデータまたはコンテンツを含む。ＨＴＴＰレスポンスには、一般的に、ＨＴＴＰレスポンスにおいて返信されるコンテンツのメディアタイプ及び適用できる場合はサブタイプ（本明細書中では「コンテンツタイプ」と呼ぶ）を識別するデータを含むコンテンツタイプ・フィールドが含まれる。例えば、コンテンツタイプ・フィールドは、コンテンツのメディア型をtext/htmlあるいはスクリプトと識別するデータを含み得る。

【００１８】

図２を参照して、ある実施形態では、クライアント・コンピュータシステムにおいて例えばウェブブラウザによって作成されたＨＴＴＰリクエストは、クライアント・コンピュータシステムからルータ（例えば、クライアント側ホームルータ）へリリースする前にプロキシされる（オペレーション２０４）。ＨＴＴＰリクエストに含まれるＨＴＴＰヘッダーは、ターゲットＵＲＬ（オペレーション２０６）及びリファラーＵＲＬ（オペレーション２０８）を判定するために解析される。

【００１９】

ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬと、ルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬとの両方を識別するか否かが判定される（オペレーション２１０）。ＨＴＴＰヘッダーが、パブリックＩＰアドレスに対応するリファラーＵＲＬと、プライベートＩＰアドレスに対応するターゲットＵＲＬとの両方を識別する場合は、ＨＴＴＰリクエストはドライブバイ・ファーミング攻撃の徴候であると判定される。選択的に排除されない場合は（オペレーション２１２）、ＨＴＴＰリクエストのルータへの送信はブロックされ（オペレーション２１４）、ユーザへの警告が作成される（オペレーション２１６）。

【００２０】

反対に、ＨＴＴＰヘッダーが、ルーティング可能なパブリックＩＰアドレスに対応するリファラーＵＲＬと、ルーティング不可能なプライベートＩＰアドレスに対応するターゲットＵＲＬとの両方を識別しない場合は、ＨＴＴＰリクエストはドライブバイ・ファーミング攻撃の徴候ではないと判定され、ＨＴＴＰリクエストはルータへ送信するためにリリースされる（オペレーション２１８）。

【００２１】
他の実施形態では、図２の方法を拡張して、埋め込まれたＨＴＭＬオブジェクトタグ、スクリプトで作成されたＨＴＭＬオブジェクトタグ、及びＡＪＡＸスタイルＸＭＬのＨＴＴＰリクエストコールを利用したドライブバイ・ファーミング攻撃からクライアント・コンピュータシステムを保護するために、リリースされたＨＴＴＰリクエストに対するＨＴＴＰレスポンスを前述したようにプロキシし修正する。従って、図４Ａ～４Ｄに概略的に示すように、ある実施形態では、リリースされたＨＴＴＰリクエストに対するＨＴＴＰレスポンスは、ウェブブラウザに受信される前にプロキシされ（オペレーション４０６）、ＨＴＴＰレスポンスのコンテンツタイプが判定される（オペレーション４０８）。そして、コンテンツタイプが、text／html又はスクリプトとして識別されるか否かが判定される（オペレーション４１０）。

【００２２】
コンテンツタイプがtext／html又はスクリプトであると判定されない場合（「ＮＯ」）は、ＨＴＴＰレスポンスが、ウェブブラウザへ送信するためにリリースされる（オペレーション４１２）。反対に、コンテンツタイプがtext／html又はスクリプトであると判定された場合は、図４Ｃに概略的に示すように、前記コンテンツは、例えばＨＴＭＬ参照ＵＲＬについて解析される（オペレーション４１６）。各ＨＴＭＬ参照ＵＲＬは、前記ＵＲＬがルーティング不可能なプライベートＩＰアドレスを示すか否か判定するために解析される（オペレーション４２０、４２２）。ＨＴＭＬ参照ＵＲＬがルーティング不可能なプライベートＩＰアドレスを示す場合は、元のＨＴＭＬ参照ＵＲＬを、例えば、空白文字列や安全な代替ＵＲＬなどの安全なＵＲＬに置き換える（オペレーション４２６）。選択的に、ユーザへの警告が作成される（オペレーション４２４）。前記ＨＴＴＰレスポンスは、その後、ウェブブラウザへ送信するためにリリースされる（オペレーション４１２）。

【００２３】
反対に、コンテンツタイプがスクリプトであると判定された場合は、図４Ｄに概略的に示すように、任意のスクリプトの前に、ジャバスクリプト・オーバライドがコンテンツの先頭に挿入される（オペレーション４３２）。ある実施形態では、ジャバスクリプト・オーバライドは、安全なＸＭＬＨＴＴＰリクエスト及びアクティブＸ置換オブジェクトを定義する。前記コンテンツは、ジャバスクリプト・オーバライド以外は、スクリプトについて解析される（オペレーション４３４）。各スクリプトにおけるＸＭＬＨＴＴＰリクエストの直接的使用の各例は、安全なＸＭＬＨＴＴＰリクエストと置き換えられ（オペレーション４４０）、各オブジェクトタグはアクティブＸ置換オブジェクトと置き換えられる（オペレーション４４２）。前記ＨＴＴＰレスポンスは、その後、ウェブブラウザへ送信するためにリリースされる（オペレーション４１２）。

【００２４】
図１は、本発明の一実施形態に係るコンピュータシステム１００を示す図である。コンピュータシステム１００は、クライアント・アンチファーミング・アプリケーション１０６で実行されるクライアント・コンピュータシステム１０２（例えば第１のコンピュータシステム）を含む。クライアント・コンピュータシステム１０２（以降、ユーザデバイスとも称する）は、一般的に、中央演算処理装置（ＣＰＵ）１０８（以降、プロセッサ１０８とも称する）、入出力（Ｉ／Ｏ）インターフェース１１０、及びメモリ１１２を備える。メモリ１１２は、オペレーティングシステム１０４を含む。

【００２５】
ある実施形態では、メモリ１１２は、クライアント・アンチファーミング・アプリケーション１０６と、ウェブブラウザ・アプリケーション１１４を含む。ある実施形態では、ウェブブラウザ・アプリケーション１１４は、ウェブページコンテンツを表示する。ウェブブラウザ・アプリケーション１１４は、従来のウェブブラウザ・アプリケーションのうちのいずれか１つであり、特定のウェブブラウザ・アプリケーションは本実施形態に必須ではない。従来のウェブブラウザは当業者には周知であるので、本発明の本質についての説明から逸れることを避けるためにここではこれ以上の詳しい説明は省略する。

【００２６】
クライアント・コンピュータシステム１０２は、キーボード１１６、マウス１１８、プリンタ１２０及びディスプレイ装置１２２などの標準的な装置、並びに、１つ以上の標準的な入出力（Ｉ／Ｏ）装置１２４をさらに含み得る。入出力（Ｉ／Ｏ）装置１２４としては、例えば、コンパクトディスク（ＣＤ）若しくはＤＶＤドライブ、フレキシブルディスクドライブ、又は、クライアント・コンピュータシステム１０２との間でデータの入出力を行うための他のデジタル信号若しくは波形信号用のポートなどがある。ある実施形態では、クライアント・アンチファーミング・アプリケーション１０６は、クライアント・アンチファーミング・アプリケーション１０６を記憶しているＣＤ、ＤＶＤ又はフレキシブルディスクなどから、入出力装置１２４を介してクライアント・コンピュータシステム１０２にロードされる。
【００２７】
クライアント・コンピュータシステム１０２は、家庭用ブロードバンドルータなどのルータ１４０に接続される。ルータ１４０は、ウェブブラウザ１１４で作成され、クライアント・コンピュータシステム１０２から送信されたアウトバウンドＨＴＴＰリクエストを受信する。ルータ１４０は、ＨＴＴＰリクエストを、コンピュータシステム１２８などの指定されたコンピュータシステムへ送信する。
【００２８】
また、ルータ１４０は、ＨＴＴＰリクエストに対して返信されたインバウンドＨＴＴＰレスポンスなどのインバウンド通信を受信する。ルータ１４０は、ＨＴＴＰレスポンスを、クライアント・コンピュータシステム１０２などの指定されたコンピュータシステムへ送信する。より詳細には、ルータ１４０は、ＨＴＴＰレスポンスを、クライアント・コンピュータシステム１０２のウェブブラウザ１１４へ送信する。ルータ１４０は、家庭用ブロードバンドルータなどの従来のルータのうちのいずれか１つであり、特定のルータは本実施形態に必須ではない。
【００２９】
本実施形態では、クライアント・アンチファーミング・アプリケーション１０６は、ウェブブラウザ１１４で作成されたＨＴＴＰリクエストを、クライアント・コンピュータシステム１０２からルータ１４０へリリースする前にプロキシする。ＨＴＴＰリクエストは、例えばドライブバイ・ファーミング攻撃などの悪意のあるコードの活動の徴候について解析される。ＨＴＴＰリクエストにドライブバイ・ファーミング攻撃の徴候があると判定された場合は、クライアント・コンピュータシステム１０２からルータ１４０へのＨＴＴＰリクエストのリリースがブロックされる、又は、ＨＴＴＰリクエストがルータ１４０へリリースされる前に他の保護アクションが実行される。
【００３０】
ある実施形態では、クライアント・アンチファーミング・アプリケーション１０６は、ＨＴＴＰレスポンス（例えば、ウェブブラウザ１１４からのＨＴＴＰリクエストに応えてコンピュータシステム１２８から送信されたＨＴＴＰレスポンス）を、ウェブブラウザ１１４に受信される前にプロキシする。ＨＴＴＰレスポンスは、ドライブバイ・ファーミング攻撃などの悪意のある活動を防止するために解析され修正される。
【００３１】
ルータ１４０は、ネットワーク１２６を介して外部コンピュータシステム１３０に接続される。例えば、ルータ１４０は、ネットワーク１２６（例えば、インターネット）を介して、サーバー・コンピュータシステム１３０及びコンピュータシステム１２８に接続される。サーバー・コンピュータシステム１３０は、一般的に、ディスプレイ装置１３２、プロセッサ１３４、メモリ１３６、及びネットワークインタフェース１３８を備える。
【００３２】
ある実施形態では、コンピュータシステム１２８は、コンピュータシステムにダウンロードしたときにドライブバイ・ファーミング攻撃を引き起こす悪意のあるコードを有するウェブページをホスティングするウェブコンテンツサーバーであり得る。本明細書では、

ある実施形態では、悪意のあるコードは、認定ユーザの承認及び／又は許可を得ずにコンピュータシステム環境に侵入するコンピュータプログラム、モジュール、一組のモジュール、又はコードと定義される。ドライブバイ・ファーミング攻撃を引き起こすコードは、悪意のあるコードの一例である。そして、本明細書では、悪意のある活動は、悪意のあるコードの実行により引き起こされる任意の活動と定義される。

【００３３】

ある実施形態では、コンピュータシステム１２８は、クライアント・コンピュータシステム１０２及び／又はサーバー・コンピュータシステム１３０と同様であり、例えば、中央演算処理装置、入出力（Ｉ／Ｏ）インターフェース、及びメモリを含む。コンピュータシステム１２８は、キーボード、マウス、プリンタ、ディスプレイ装置、及びＩ／Ｏ装置などの標準的な装置をさらに含み得る。コンピュータシステム１２８の種々のハードウェアコンポーネントは、発明の本質についての説明から逸れることを避けるためにここではこれ以上の詳しい説明は省略する。

【００３４】

ネットワーク１２６は、ユーザが関心を持つあらゆるネットワークまたはネットワーク・システムであり得る。種々の実施形態において、ネットワークインタフェース１３８及びＩ／Ｏインタフェース１１０としては、アナログモデム、デジタルモデムまたはネットワークインタフェースカードなどが挙げられる。クライアント・コンピュータシステム１０２、コンピュータシステム１２８、及びサーバー・コンピュータシステム１３０の特定の種類と構成は、本発明の本実施形態に必須ではない。

【００３５】

図２は、本発明の一実施形態に係るクライアント・コンピュータシステム１０２をドライブバイ・ファーミング攻撃から保護するための方法２００を説明するためのフロー図である。この実施形態では、ウェブサイトへの第１のＨＴＴＰリクエストをウェブブラウザ１１４からコンピュータシステム１２８へ送信すると、有害なドライブバイ・ファーミング・コードを含んでいるウェブページがウェブブラウザ１１４へ返信され、ウェブブラウザ１１４で実行されると仮定する。より詳細には、ウェブブラウザ１１４で実行されるウェブページに含まれている有害なドライブバイ・ファーミング・コードは、クライアント・コンピュータシステム１０２上でドライブバイ・ファーミング攻撃をしようとして、ＨＴＴＰリクエストを開始する。

【００３６】

図１及び図２を参照すると、ある実施形態では、プロセッサ１０８でクライアント・アンチファーミング・アプリケーション１０６を実行すると、後述するような方法２００が実施される。方法２００は、開始オペレーション２０２で開始され、ＨＴＴＰリクエスト・プロキシオペレーション２０４へ進む。

【００３７】

ＨＴＴＰリクエスト・プロキシオペレーション２０４では、例えばウェブブラウザ１１４で悪意のあるコードを実行することによりクライアント・コンピュータシステム１０２で生成されたアウトバウンドＨＴＴＰリクエストは、クライアント・コンピュータシステム１０２からルータ１４０へリリースされる前にプロキシされる。ある実施形態では、前記ＨＴＴＰリクエストは、クライアント・アンチファーミング・アプリケーション１０６のＨＴＴＰプロキシコンポーネントによってプロキシされる。前記ＨＴＴＰリクエストは、当該ＨＴＴＰリクエストのルータ１４０への送信をブロックするように、例えばフッキング技術などの任意の様々なプロキシ技術を利用してプロキシされる。ＨＴＴＰリクエストのプロキシングは、当業者に周知であるので、本発明の本質についての説明から逸れることを避けるためにここではこれ以上の詳しい説明は省略する。

【００３８】

ある実施形態では、ＨＴＴＰリクエストは、少なくともリファラーＵＲＬ及びターゲットＵＲＬを有するＨＴＴＰヘッダーを含む。前述したように、リファラーＵＲＬは、ターゲットＵＲＬがリクエストされユーザがアクセスしたウェブページのＩＰアドレスに対応

する（すなわち分解する）。ターゲットＵＲＬは、リクエストされたウェブページのＩＰアドレス（以降、ターゲットＵＲＬのＩＰアドレスと称する）に対応する（すなわち、分解する）。プロセスフローは、ＨＴＴＰリクエスト・プロキシオペレーション２０４から、ターゲットＵＲＬ判定オペレーション２０６へ進む。

【００３９】

ターゲットＵＲＬ判定オペレーション２０６では、ＨＴＴＰリクエストのＨＴＴＰヘッダーからターゲットＵＲＬが判定される。ターゲットＵＲＬの判定は、例えば、ＨＴＴＰヘッダーを解析することによって、又は、ターゲットＵＲＬを判定するための他の解析技術を用いることによって行われる。プロセスフローは、ターゲットＵＲＬ判定オペレーション２０６から、リファラーＵＲＬ判定オペレーション２０８へ進む。

【００４０】

リファラーＵＲＬ判定オペレーション２０８では、オペレーション２０４でプロキシされたＨＴＴＰリクエストのＨＴＴＰヘッダーからリファラーＵＲＬが判定される。リファラーＵＲＬの判定は、例えば、ＨＴＴＰヘッダーを解析することによって、又は、リファラーＵＲＬを判定するための他の解析技術を用いることによって行われる。プロセスフローは、リファラーＵＲＬ判定オペレーション２０８から、パブリックリファラー及びプライベートターゲットのチェックオペレーション２１０へ進む。

【００４１】

パブリックリファラー及びプライベートターゲットのチェックオペレーション２１０では、オペレーション２０６で判定されたターゲットＵＲＬ及びオペレーション２０８で判定されたリファラーＵＲＬのそれぞれが分解される、あるいは、各ＩＰアドレスに対応される。例えば、ターゲットＵＲＬが分解される又はターゲットＵＲＬのＩＰアドレスに対応され、リファラーＵＲＬが分解される又はリファラーＵＲＬのＩＰアドレスに対応される。

【００４２】

リファラーＵＲＬのＩＰアドレスがルーティング可能なパブリックＩＰアドレスであるか否か、ターゲットＵＲＬのＩＰアドレスがルーティング不可能なプライベートＩＰアドレスであるか否かの判定がなされる。ある実施形態では、リファラーＵＲＬのＩＰアドレスとターゲットＵＲＬのＩＰアドレスは、既知のプライベート及び／又はパブリックＩＰアドレスのデータベースと比較される。あるいは、リファラーＵＲＬのＩＰアドレスとターゲットＵＲＬのＩＰアドレスは、各ＵＲＬのＩＰアドレスがパブリック又はプライベートＩＰアドレスであるか否かを判定するために解析される。

【００４３】

ある実施形態では、ルーティング可能なパブリックＩＰアドレスであると判定されたリファラーＵＲＬのＩＰアドレスの組み合わせは、ルーティング不可能なプライベートＩＰアドレスであると判定されたターゲットＵＲＬのＩＰアドレスと共に、ドライブバイ・ファーミング攻撃の徴候と見なされる。例えば、上記の組み合わせは、ドライブバイ・ファーミング攻撃を可能にすべくルータ１４０上で悪質な改変を実施するために、ルータ１４０のＩＰアドレスを確認するためにウェブブラウザ１１４で実行される悪意のあるコードによる攻撃の徴候と見なされる。

【００４４】

一方、パブリックＩＰアドレスであるリファラーＵＲＬのＩＰアドレスとパブリックＩＰアドレスであるターゲットＵＲＬのＩＰアドレスとの組み合わせ、又は、プライベートＩＰアドレスであるリファラーＵＲＬのＩＰアドレスとパブリック若しくはプライベートＩＰアドレスであるターゲットＵＲＬのＩＰアドレスとの組み合わせは、ドライブバイ・ファーミング攻撃の徴候と見なされない。したがって、ある実施形態では、リファラーＵＲＬのＩＰアドレスがルーティング可能なパブリックＩＰアドレスであり、ターゲットＵＲＬのＩＰアドレスがルーティング不可能なプライベートＩＰアドレスと判定されない場合（「ＮＯ」）は、ドライブバイ・ファーミング攻撃の徴候と見なされない。その場合、プロセスフローは、パブリックリファラー及びプライベートターゲットのチェックオペレ

ーション２１０から、ＨＴＴＰリクエスト・リリースオペレーション２１８へ進む。
【００４５】
ＨＴＴＰリクエスト・リリースオペレーション２１８では、オペレーション２０４でプロキシされたＨＴＴＰリクエストがリリースされ、クライアント・コンピュータシステム１０２からルータ１４０へ送信される。その後、プロセスフローは、ＨＴＴＰリクエスト・リリースオペレーション２１８から、終了オペレーション２２０へ進んで方法プロセス２００を終了する。あるいは、選択的に、次のＨＴＴＰリクエストをプロキシするときに、オペレーション２０４に戻る。
【００４６】
パブリックリファラー及びプライベートターゲットのチェックオペレーション２１０に再び戻って、リファラーＵＲＬのＩＰアドレスがルーティング可能なパブリックＩＰアドレスであり、ターゲットＵＲＬのＩＰアドレスがルーティング不可能なライベートＩＰアドレスであると判定された場合（「ＹＥＳ」）は、この組み合わせは、ドライブバイ・ファーミング攻撃の徴候と見なされる。プロセスフローは、パブリックリファラー及びプライベートターゲットのチェックオペレーション２１０からブロック解除のチェックオペレーション２１２へ選択的に進む。あるいは、チェックオペレーション２１０からＨＴＴＰリクエスト・ブロックオペレーション２１４へ直接的に進む。
【００４７】
ブロック解除のチェックオペレーション２１２では、ＨＴＴＰリクエストに対してなされているブロックを解除するか否かの判定が行われる。例えば、ある実施形態では、リファラーＵＲＬのＩＰアドレスが、ブロックが解除されたリファラーＵＲＬのＩＰアドレスのリストの項目と比較される、及び／又は、ターゲットＵＲＬのＩＰアドレスが、ブロックが解除されたターゲットＵＲＬのＩＰアドレスのリストの項目と比較される。
【００４８】
ある実施形態では、リファラーＵＲＬのＩＰアドレスとブロックが解除されたリファラーＵＲＬのＩＰアドレスのリストの項目とが一致する場合、及び／又は、ターゲットＵＲＬのＩＰアドレスがブロックが解除されたターゲットＵＲＬのＩＰアドレスのリストの項目と一致する場合は、ＨＴＴＰリクエストに対してなされているブロックが解除される。他の実施形態では、リファラーＵＲＬのＩＰアドレス及び／又はターゲットＵＲＬのＩＰアドレスを用いた排他的な解析技術が利用可能である。さらなる他の実施形態では、ＨＴＴＰリクエストのブロックを解除するか否かを判定するために、ＨＴＴＰリクエストの他のパラメータを解析する。
【００４９】
ある実施形態では、ＨＴＴＰリクエストのブロックを解除すると判定された場合（「ＹＥＳ」）は、プロセスフローは、ブロック解除のチェックオペレーション２１２から、前述したＨＴＴＰリクエスト・リリースオペレーション２１８へ進む。反対に、ＨＴＴＰリクエストのブロックを解除しないと判定された場合（「ＮＯ」）は、プロセスフローは、ブロック解除のチェックオペレーション２１２から、ＨＴＴＰリクエスト・ブロックオペレーション２１４へ進む。
【００５０】
ＨＴＴＰリクエスト・ブロックオペレーション２１４では、ＨＴＴＰリクエストがブロックされる。ある実施形態では、ＨＴＴＰリクエストのルータ１４０への送信を防止する。このようにして、悪意のあるコードがＨＴＴＰリクエストを介してルータのＩＰアドレスを取得することを防止し、ルータ１４０に対してドライブバイ・ファーミング攻撃を補助するための悪質な改変が開始されるのを防止する。プロセスフローは、ＨＴＴＰリクエスト・ブロックオペレーション２１４から、ユーザ警告オペレーション２１６へ進む。
【００５１】
ユーザ警告オペレーション２１６では、警告を作成して、ユーザへ通知する。ユーザには、様々な技術のうちの１つを使用して通知する。例えば、ディスプレイ装置１２２にポップアップ・ウィンドウを表示することにより通知する。ある実施形態では、クライアン

ト・コンピュータシステム１０２のユーザには、悪意のあるコード（例えば、ドライブバイ・ファーミング・コード）がクライアント・コンピュータシステム１０２に存在すること、及び／又は、ＨＴＴＰリクエストをブロックしたことが通知される。その後、プロセスフローは、ユーザ警告オペレーション２１６から、終了オペレーション２２０へ進んで方法プロセス２００を終了する。あるいは、クライアント・コンピュータシステム１０２で次のアウトバウンドＨＴＴＰリクエスをプロキシするときに、オペレーション２０４に戻る。

【００５２】

上述した実施形態では、ＨＴＴＰリクエストのブロック（例えば、オペレーション２１４）は、ユーザ入力を必要とせずに、自動的に実施される。他の実施形態では、図３Ａ及び３Ｂを参照しつつ後述するように、ＨＴＴＰリクエストをブロックする前に、前記ブロックの可否をユーザに確認する。

【００５３】

図３Ａ及び３Ｂは、本発明の他の実施形態に係る、クライアント・コンピュータシステム１０２をドライブバイ・ファーミング攻撃から保護するための方法３００を説明するためのフロー図である。図１、２、３Ａ及び３Ｂを参照して、ある実施形態では、プロセッサ１０８で実行されるクライアント・アンチファーミング・アプリケーション１０６は、下記のような方法３００のオペレーションとなる。

【００５４】

ＨＴＴＰリクエスト・プロキシオペレーション２０４、オペレーション２０６、２０８、チェックオペレーション２１０、及びチェックオペレーション２１２（選択された場合）が、図２を参照しつつ説明した方法２００のようにして実施される。そして、ブロック解除のチェックオペレーション２１２で「ＮＯ」が選択された場合、あるいは、チェックオペレーション２１２が実施されなくパブリックリファラー及びプライベートターゲットのチェックオペレーション２１０で「ＹＥＳ」が選択された場合は、プロセスフローは、ユーザ警告オペレーション３０６（図３参照）へ進む。

【００５５】

図３Ｂを参照して、ユーザ警告オペレーション３０６では、ユーザへの警告を作成しクライアント・コンピュータシステム１０２に表示し、ブロックの可否をユーザに尋ねる（ユーザ入力を要求する）。例えば、ある実施形態では、ポップアップ又は他の通知を作成してディスプレイ装置１２２に表示し、ＨＴＴＰリクエストのブロックの可否をユーザに尋ねる（ユーザに入力を要求する）。

【００５６】

いくつかの実施形態では、ユーザへの通知は、ＨＴＴＰリクエストが不審である及び／又はドライブバイ・ファーミング攻撃の徴候があるという文章説明によって行われる。ある実施形態では、ユーザへの通知は、クライアント・アンチファーミング・アプリケーション１０６がＨＴＴＰリクエストを受信したときに、ＨＴＴＰリクエストをブロックするかリリースするかの応答選択をユーザが入力可能なグラフィカル・ユーザ・インターフェースを使用して行われる。

【００５７】

例えば、グラフィカル・ユーザ・インターフェースは、「ドライブバイ・ファーミング攻撃の徴候があるＨＴＴＰリクエストが作成されました。このリクエストをブロックしますか？」という文章の質問と、その質問に対する「ＹＥＳ」及び「ＮＯ」の２つの選択ボタンとを含むことができる。ある実施形態では、「ＹＥＳ」のボタンを選択すると承認応答がクライアント・アンチファーミング・アプリケーション１０６へ送信され、「ＮＯ」のボタンを選択すると拒否応答がクライアント・アンチファーミング・アプリケーション１０６へ送信される。プロセスフローは、ユーザ警告オペレーション３０６から、ユーザ入力の受信オペレーション３０８へ進む。

【００５８】

ユーザ入力の受信オペレーション３０８では、クライアント・アンチファーミング・ア

プリケーション１０６は、ユーザ入力を受信する。例えば、クライアント・アンチファーミング・アプリケーション１０６は、オペレーション３０６においてグラフィカル・ユーザ・インターフェースへ入力された、ＨＴＴＰリクエストのブロックの可否についてのユーザ入力を受信する。プロセスフローは、ユーザ入力の受信オペレーション３０８から、ユーザのブロック承認のチェックオペレーション３１０へ進む。

【００５９】

ユーザのブロック承認のチェックオペレーション３１０では、オペレーション３０８で受信されたユーザ入力がＨＴＴＰリクエストのブロックを承認しているか否かが判定される。ユーザ入力が、承認応答の場合（「ＹＥＳ」）は、ＨＴＴＰリクエストのブロックが承認されたと判定する。ユーザ入力が、拒否応答の場合（「ＮＯ」）は、ＨＴＴＰリクエストのブロックが拒否されたと判定する。

【００６０】

ユーザがＨＴＴＰリクエストのブロックを拒否した場合（「ＮＯ」）は、ＨＴＴＰリクエストがリリースされる。そして、プロセスフローは、ユーザのブロック承認のチェックオペレーション３１０から、前述したＨＴＴＰリクエスト・リリースオペレーション２１８へ進む。その後、プロセスフローは、ＨＴＴＰリクエスト・リリースオペレーション２１８から、終了オペレーション３０４へ進んで方法プロセス３００を終了する。あるいは、次のアウトバウンドＨＴＴＰリクエスをプロキシするときに、オペレーション２０４に戻る。

【００６１】

ユーザのブロック承認のチェックオペレーション３１０に再び戻って、ユーザがＨＴＴＰリクエストのブロックを承認した場合（ＹＥＳ）は、ＨＴＴＰリクエストはブロックされる。プロセスフローは、ユーザのブロック承認のチェックオペレーション３１０から、前述したＨＴＴＰリクエスト・ブロックオペレーション２１４へ進む。そして、プロセスフローは、ＨＴＴＰリクエスト・ブロックオペレーション２１４から、前述したユーザ警告オペレーション２１６へ進む。その後、プロセスフローは、ユーザ警告オペレーション２１６から、終了オペレーション３０４へ進んで方法プロセス３００を終了する。あるいは、次のアウトバウンドＨＴＴＰリクエストをプロキシするときに、オペレーション２０４に戻る。

【００６２】

別の実施形態を、図４Ａ～４Ｄを参照して説明する。ドライブバイ・ファーミング攻撃から、クライアント・コンピュータシステム１０２をさらに保護するため、図示のように方法２００を拡張し、ＨＴＴＰリクエストに応じて返信されたＨＴＴＰレスポンスが解析され修正される。より詳しくは、クライアント・コンピュータシステム１０２を、ＨＴＴＰレスポンスのコンテンツに存在する悪意のあるコードから保護するため、図示のように、インバウンドＨＴＴＰレスポンスが、ウェブブラウザ１１４に受信される前にプロキシされ、プロキシされたＨＴＴＰレスポンスが解析され修正される。

【００６３】

図４Ａ～４Ｄは、本発明の別の実施形態に係るクライアント・コンピュータシステムをドライブバイ・ファーミング攻撃から保護するための方法４００を説明するためのフロー図である。図１、図２、及び図４Ａ～図４Ｄを一緒に参照して、ある実施形態では、プロセッサ１０８でクライアント・アンチファーミング・アプリケーション１０６を実行すると、後述するような方法４００が実施される。

【００６４】

ある実施形態では、方法４００は、開始オペレーション４０２で開始され、ＨＴＴＰリクエスト・プロキシオペレーション２０４へ進む。ＨＴＴＰリクエスト・プロキシオペレーション２０４が、上述の図２を参照しつつ説明した方法２００のようにして実施され（参照することによりここに組み込まれる）、オペレーション２０６、２０８、チェックオペレーション２１０、チェックオペレーション２１２、オペレーション２１４、２１６及び２１８が、ＨＴＴＰリクエスト送信オペレーション２１８の後に続くオペレーションを

除いて、上述の図２を参照しつつ説明した方法２００のようにして連続的に処理される。そして、プロセスフローは、オペレーション２１８でリリースされたＨＴＴＰリクエストに応じて返信されたＨＴＴＰレスポンスをプロキシするため、ＨＴＴＰレスポンス・プロキシオペレーション４０６（図４Ｂ）へ進む。

【００６５】

図４Ｂを参照すると、ＨＴＴＰレスポンス・プロキシオペレーション４０６では、クライアント・コンピュータシステム１０２で受信した、コンピュータシステム１２８からのインバウンドＨＴＴＰレスポンスが、ウェブブラウザ１１４へリリースされる前にプロキシされる。例えば、ある実施形態では、インバウンドＨＴＴＰレスポンスが、クライアント・アンチファーミング・アプリケーション１０６のＨＴＴＰプロキシコンポーネントによって外部に出力されないようにする。フッキング技術などの任意の様々なプロキシ技術を利用して、ＨＴＴＰレスポンスが外部に出力されないようにすることができる。ＨＴＴＰレスポンスのプロキシングは、当業者に周知であるので、本発明の本質についての説明から逸れることを避けるためにここではこれ以上の詳しい説明は省略する。

【００６６】

ある実施形態では、ＨＴＴＰレスポンスは、少なくとも１つのコンテンツタイプ・フィールドを有するＨＴＴＰヘッダーを含み、さらに悪意のあるドライブバイ・ファーミング・コードなどのコンテンツを含むこともある。プロセスフローは、ＨＴＴＰレスポンス・プロキシオペレーション４０６から、コンテンツタイプ判定オペレーション４０８へ進む。

【００６７】

コンテンツタイプ判定オペレーション４０８では、ＨＴＴＰレスポンスは、必要に応じて、ＨＴＴＰレスポンスで返信されたコンテンツのコンテンツタイプを判定するために解析される。ある実施形態では、ＨＴＴＰレスポンスのコンテンツタイプ・フィールドが、適用可能であれば、例えば、ＨＴＴＰレスポンスを解析することによって、スキャニングすることによって、又はその他の評価方法によって、コンテンツタイプ及び様々なサブタイプを判定するために解析される。プロセスフローは、コンテンツタイプ判定オペレーション４０８から、コンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０へ進む。

【００６８】

コンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０では、オペレーション４０８で判定されたコンテンツタイプが、text/html又はスクリプトのどちらかとして識別されたか否かの判定が行われる。コンテンツタイプがtext/html又はスクリプトではない場合（「ＮＯ」）は、プロセスフローは、コンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０から、ＨＴＴＰレスポンス・リリースオペレーション４１２へ進む。

【００６９】

ＨＴＴＰレスポンス・リリースオペレーション４１２では、オペレーション４０６でプロキシされたＨＴＴＰレスポンスがリリースされ、ウェブブラウザ１１４に送信される。プロセスフローは、ＨＴＴＰレスポンス・リリースオペレーション４１２から、終了オペレーション４０４へ進んで方法プロセス４００を終了する。あるいは、選択的に、次のＨＴＴＰリクエストをプロキシするときに、オペレーション２０４（図４Ａ）に戻る。

【００７０】

コンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０（図４Ｂ）に再び戻って、反対に、コンテンツタイプがtext/html又はスクリプトである場合（「ＹＥＳ」）は、コンテンツタイプがtext/htmlであれば、プロセスフローは、コンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０から、コンテンツのＨＴＭＬ参照ＵＲＬ解析オペレーション４１６（図４Ｃ）へ進み、あるいは、コンテンツタイプがスクリプトであれば、プロセスフローは、コンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０から、ジャバスクリプト・オーバライド挿入

オペレーション４３２（図４Ｄ）へ進む。

【００７１】

次に図４Ｃを参照して、コンテンツのＨＴＭＬ参照ＵＲＬ解析オペレーション４１６では、ＨＴＴＰレスポンスのコンテンツタイプがtext/htmlであると判定されたとき、ＨＴＴＰレスポンスのＨＴＭＬコンテンツは、各ＨＴＭＬ参照ＵＲＬを特定するために解析される。ある実施形態では、クライアント・アンチファーミング・アプリケーション１０６の簡易ＨＴＭＬ解析コンポーネントを、ＨＴＭＬコンテンツの解析及び各ＨＴＭＬ参照ＵＲＬの特定のために使用することができる。ある実施形態では、ＨＴＭＬ参照ＵＲＬの例として、Ａ、ＩＭＧ、スクリプト、スタイル、オブジェクト、及び埋め込みタグのほかに、インラインスタイル又はブロックスタイルから参照されるＵＲＬが含まれる。プロセスフローは、コンテンツのＨＴＭＬ参照ＵＲＬ解析オペレーション４１６から、ＨＴＭＬ参照ＵＲＬチェックオペレーション４１８へ進む。

【００７２】

ＨＴＭＬ参照ＵＲＬチェックオペレーション４１８では、少なくとも１つのＨＴＭＬ参照ＵＲＬが、オペレーション４１６で識別されたか否かの判定が行われる。ＨＴＭＬ参照ＵＲＬが、オペレーション４１６で１つも識別されなかった場合（「ＮＯ」）は、プロセスフローは、ＨＴＭＬ参照ＵＲＬチェックオペレーション４１８から、オペレーション４３０に進んで、上述のＨＴＴＰレスポンスのウェブブラウザ１１４への送信を含むＨＴＴＰレスポンス・リリースオペレーション４１２（図４Ｂ）へ進むようにする。

【００７３】

図４Ｃに再び戻って、反対に、少なくとも１つのＨＴＭＬ参照ＵＲＬが、オペレーション４１６で識別された場合（「ＹＥＳ」）は、プロセスフローは、ＨＴＭＬ参照ＵＲＬチェックオペレーション４１８から、ＨＴＭＬ参照ＵＲＬ選択オペレーション４２０へ進む。

【００７４】

ＨＴＭＬ参照ＵＲＬ選択オペレーション４２０では、解析するための、オペレーション４１６で識別された第１のＨＴＭＬ参照ＵＲＬが選択される。プロセスフローは、ＨＴＭＬ参照ＵＲＬ選択オペレーション４２０から、プライベートＩＰアドレスの指示チェックオペレーション４２２へ進む。

【００７５】

プライベートＩＰアドレスの指示チェックオペレーション４２２では、オペレーション４２０で選択されたＨＴＭＬ参照ＵＲＬが、プライベートＩＰアドレスに対応しているか否かの判定が行われる。ある実施形態では、ＨＴＭＬ参照ＵＲＬが分解されるとき、あるいは、ＨＴＭＬ参照ＵＲＬのＩＰアドレスに対応されるとき、本明細書中では、それをＨＴＭＬ参照ＵＲＬのＩＰアドレスと称する。

【００７６】

ある実施形態では、ＨＴＭＬ参照ＵＲＬのＩＰアドレスは、既知のプライベート及び／又はパブリックＩＰアドレスのデータベースと比較される。あるいは、ＨＴＭＬ参照ＵＲＬのＩＰアドレスは、ＨＴＭＬ参照ＵＲＬのＩＰアドレスがプライベートＩＰアドレスであるか否かを判定するために解析される。ＨＴＭＬ参照ＵＲＬのＩＰアドレスが、プライベートＩＰアドレスではないとき、即ちパブリックＩＰアドレスである場合（「ＮＯ」）は、プロセスフローは、プライベートＩＰアドレスの指示チェックオペレーション４２２から、次のＨＴＭＬ参照ＵＲＬチェックオペレーション４２８へ進む。

【００７７】

次のＨＴＭＬ参照ＵＲＬチェックオペレーション４２８では、オペレーション４１６で識別されたＨＴＭＬ参照ＵＲＬで、まだ評価されていない次のＨＴＭＬ参照ＵＲＬが残っているか否かの判定が行われる。まだ評価されていない次のＨＴＭＬ参照ＵＲＬが残っている場合（「ＹＥＳ」）は、プロセスフローは、選択された次のＨＴＭＬ参照ＵＲＬを解析するために、次のＨＴＭＬ参照ＵＲＬチェックオペレーション４２８から、オペレーション４２０に戻る。また、まだ評価されていない次のＨＴＭＬ参照ＵＲＬが残っていない

場合（「ＮＯ」）は、プロセスフローは、次のＨＴＭＬ参照ＵＲＬチェックオペレーション４２８から、オペレーション４３０へ進んで、ウェブブラウザ１１４へ送信するためにリリースされたＨＴＴＰレスポンスが、ＨＴＴＰレスポンス・リリースオペレーション４１２（図４Ｂ）へ進むようにし、終了オペレーション４０４で方法プロセス４００を終了する。あるいは、選択的に、次のＨＴＴＰリクエストをプロキシするときに、オペレーション２０４（図４Ａ）に戻る。

【００７８】

図４Ｃ及びプライベートＩＰアドレスの指示チェックオペレーション４２２に再び戻って、反対に、ＨＴＭＬ参照ＵＲＬのＩＰアドレスが、プライベートＩＰアドレスである場合（「ＹＥＳ」）は、プロセスフローは、プライベートＩＰアドレスの指示チェックオペレーション４２２から、選択的に、ユーザ警告オペレーション４２４へ進む、あるいは、ＨＴＭＬ参照ＵＲＬの安全なＵＲＬへの置き換えオペレーション４２６へ直接的に進む。

【００７９】

オプションのユーザ警告オペレーション４２４では、ユーザへの警告が作成され、ユーザへ通知される。ユーザには、様々な技術のうちの１つを使用して通知する。例えば、ディスプレイ装置１２２にポップアップ・ウィンドウを表示することにより通知する。ある実施形態では、クライアント・コンピュータシステム１０２（図１）のユーザには、悪意のあるコード（例えば、ドライブバイ・ファーミングコード）が検出されたことや、ＨＴＴＰレスポンスのＨＴＭＬ参照ＵＲＬが安全なＨＴＭＬＵＲＬに置き換えられたこと又はＨＴＴＰレスポンスのＨＴＭＬ参照ＵＲＬが削除されたことが通知される。プロセスフローは、オプションのユーザ警告オペレーション４２４から、ＨＴＭＬ参照ＵＲＬの安全なＵＲＬへの置き換えオペレーション４２６へ進む。

【００８０】

ＨＴＭＬ参照ＵＲＬの安全なＵＲＬへの置き換えオペレーション４２６では、元のＨＴＭＬ参照ＵＲＬが、安全なＵＲＬ、例えば、空白文字列、又はダミーファイルを指定するダミーＵＲＬに置き換えられる。ある実施形態では、元のＨＴＭＬ参照ＵＲＬ、例えば、「A HREF= "http://192.168.1.1"」が削除され、「A HREF=""」になる。あるいは、元のＨＴＭＬ参照ＵＲＬに特定の処理が行われ、ゼロバイトの返信が戻るようにする。プロセスフローは、ＨＴＭＬ参照ＵＲＬの安全なＵＲＬへの置き換えオペレーション４２６から、次のＨＴＭＬ参照ＵＲＬチェックオペレーション４２８へ進み、その後、上述のオペレーション４２０に戻る（「ＹＥＳ」の場合）、又は上述のＨＴＴＰレスポンス・リリースオペレーション４１２（図４Ｂ）（「ＮＯ」の場合）へ進む。ＨＴＴＰレスポンス・リリースオペレーション４１２（図４Ｂ）では、ＨＴＴＰレスポンスは、ウェブブラウザ１１４へ送信するためにリリースされる。

【００８１】

図４Ｂ及びコンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０に再び戻って、反対に、ＨＴＴＰレスポンスのコンテンツタイプが、スクリプトであると判定されたとき、プロセスフローは、コンテンツタイプ（text/html又はスクリプト）チェックオペレーション４１０から、ジャバスクリプト・オーバライド挿入オペレーション４３２（図４Ｄ）へ進む。次に図４Ｄを参照して、ジャバスクリプト・オーバライド挿入オペレーション４３２では、スクリプトに記述された攻撃を防止するべく、コンテンツ内の選択された適切な機能をオーバライドするジャバスクリプト（本明細書中では、ジャバスクリプト・オーバライドと称する）が、ＨＴＭＬリクエストのコンテンツに挿入される。ある実施形態では、ジャバスクリプト・オーバライドが、ＨＴＭＬページのコンテンツの先頭に、全ての＜スクリプト＞タグの前に挿入される。

【００８２】

ある実施形態では、ジャバスクリプト・オーバライドは、安全なアプリケーションプログラムインタフェース（ＡＰＩ）のクラス、例えば、標準的なＸＭＬＨＴＴＰリクエストＡＰＩの全機能を含む、安全なＸＭＬＨＴＴＰリクエストＡＰＩ（安全なＸＭＬＨＴＴＰリクエストと称する）を定義し、またＨＴＴＰリクエストを発信する前にリファラーＩＰ

アドレス及びターゲットＩＰアドレスを判定する。ジャバスクリプト・オーバライドは、次に、「document.write = SafeWrite」の実行を行う。

【００８３】

「document.write = SafeWrite」は、document.write()に対する全ての呼び出しが、プライベートＩＰアドレスを参照する新たなＨＴＭＬを挿入しないようにする、又は標準的なＸＭＬＨＴＴＰリクエストを使用させようとする新たなジャバスクリプトを挿入しないようにする。document.write()が、プライベートＩＰアドレスを参照するＨＴＭＬで呼び出されたとき、オペレーション４２６（図４Ｃ）を参照しつつ説明した上述の削除／置き換え（参照することによりここに組み込まれる）と、同一の削除／置き換えが行われる。

【００８４】

document.write()が、標準的なＸＭＬＨＴＴＰリクエストＡＰＩを使用させようとするジャバスクリプトで呼び出されたとき、そのジャバスクリプトは、安全なＸＭＬＨＴＴＰリクエストＡＰＩに置き換えられる、あるいは、ランダムに選択された同等の名称に置き換えられる。ある実施形態では、挿入されたジャバスクリプト・オーバライドで使用される変数及びクラス名を攻撃者が知ってしまったときに、ジャバスクリプト・オーバライドの抜け道を見つける可能性を減少させるため、ジャバスクリプト・オーバライドで使用される変数及びクラス名はランダムに選択される。

【００８５】

ある実施形態では、ジャバスクリプト・オーバライドは、アクティブＸ置換オブジェクトも定義する。アクティブＸ置換オブジェクトが呼び出されたとき、アクティブＸ置換オブジェクトは、元のアクティブＸオブジェクトに対するリクエストをプロキシする。まず、そのリクエストが、パブリックのリファラーＩＰアドレス及びプライベートのターゲットＩＰアドレスを識別するか否かを確認し、方法２００及び３００を参照しつつ説明した上述の適切なブロック／指示を実行する。これにより、ＸＭＬＨＴＴＰリクエストＡＰＩをサポートしていない、いくつかのウェブブラウザ、例えば、インターネットエクスプローラの旧バージョンを保護し、コンピュータシステムを攻撃するため、旧バージョンのアクティブＸオブジェクトを使用させようとするウェブサイトに対する防御を可能にする。

【００８６】

アクティブＸ置換オブジェクトは、オペレーション４２６（図４Ｃ）を参照しつつ説明した上述のＸＭＬＨＴＴＰリクエストＡＰＩを安全なＸＭＬＨＴＴＰリクエストＡＰＩに置き換える方法のように、真のアクティブＸオブジェクト用のレジストを引き継ぐ必要がない。アクティブＸ置換オブジェクトは、Microsoft.XMLHTTPを、例えば、Symantec.Safe XMLHTTPなどの安全なオブジェクトに置き換えるために使用することもできる。例えば、存在するジャバスクリプトを探して置き換えたり、作成されたスクリプトを検索しているdocument.write()の呼び出しを探して置き換えたりする。プロセスフローは、ジャバスクリプト・オーバライド挿入オペレーション４３２から、コンテンツのスクリプト解析オペレーション４３４へ進む。

【００８７】

コンテンツのスクリプト解析オペレーション４３４では、ＨＴＴＰレスポンスのコンテンツは、オペレーション４３２で挿入されたジャバスクリプト・オーバライド以外は、各スクリプトについて解析される。ある実施形態では、ＨＴＴＰレスポンスのコンテンツフィールドに存在するデータが、各スクリプトを識別するために解析される。プロセスフローは、コンテンツのスクリプト解析オペレーション４３４から、スクリプトチェックオペレーション４３６へ進む。

【００８８】

スクリプトチェックオペレーション４３６では、少なくとも１つのスクリプトが、オペレーション４３４で識別されたか否かの判定が行われる。オペレーション４３４で１つのスクリプトも識別されなかった場合（「ＮＯ」）は、プロセスフローは、スクリプトチェックオペレーション４３６から、オペレーション４５０へ進み、上述のウェブブラウザ１１４へＨＴＴＰレスポンスを送信することに関連するＨＴＴＰレスポンス・リリースオペ

レーション４１２（図４Ｂ）へ進むようにする。あるいは、少なくとも１つのスクリプトがオペレーション４３４で識別された場合（「ＹＥＳ」）は、プロセスフローは、スクリプトチェックオペレーション４３６から、スクリプト選択オペレーション４３８へ進む。

【００８９】

スクリプト選択オペレーション４３８では、解析するための、オペレーション４３４で識別されたスクリプトが選択される。プロセスフローは、スクリプト選択オペレーション４３８から、ＸＭＬＨＴＴＰリクエストＡＰＩの安全なＸＭＬＨＴＴＰリクエストＡＰＩへの置き換えオペレーション４４０へ進む。

【００９０】

ＸＭＬＨＴＴＰリクエストＡＰＩの安全なＸＭＬＨＴＴＰリクエストＡＰＩへの置き換えオペレーション４４０では、スクリプトに存在する各ＸＭＬＨＴＴＰリクエストＡＰＩは、必要に応じて、安全なＸＭＬＨＴＴＰリクエストＡＰＩ（例えば、オペレーション４３２で既に挿入及び定義済みの安全なＸＭＬＨＴＴＰリクエストＡＰＩ、又はその他の安全な同等物）に置き換えられる。プロセスフローは、ＸＭＬＨＴＴＰリクエストＡＰＩの安全なＸＭＬＨＴＴＰリクエストＡＰＩへの置き換えオペレーション４４０から、オブジェクトタグのアクティブＸ置換オブジェクトへの置き換えオペレーション４４２へ進む。

【００９１】

オブジェクトタグのアクティブＸ置換オブジェクトへの置き換えオペレーション４４２では、スクリプトに存在する各オブジェクトタグは、必要に応じて、オペレーション４３２で既に挿入及び定義済みのアクティブＸ置換オブジェクトに置き換えられる。ある実施形態では、Microsoft.XMLHTTPオブジェクトのほかに、MsXML2.XMLHTTPオブジェクト及びその他の使用済みのＸＭＬリクエスタが、アクティブＸ置換オブジェクトに置き換えられる。プロセスフローは、オブジェクトタグのアクティブＸ置換オブジェクトへの置き換えオペレーション４４２から、次のスクリプトチェックオペレーション４４８へ進む。

【００９２】

次のスクリプトチェックオペレーション４４８では、オペレーション４３４で識別されたスクリプトで、まだ評価されていない次のスクリプトが残っているか否かの判定が行われる。まだ評価されていない次のスクリプトが残っている場合（「ＹＥＳ」）は、プロセスフローは、選択された次のスクリプトを解析するため、オペレーション４３８に戻る。あるいは、まだ評価されていない次のスクリプトが残っていない場合（「ＮＯ」）は、プロセスフローは、オペレーション４５０へ進み、ウェブブラウザ１１４へ送信されるべきＨＴＴＰレスポンスがオペレーション４１２（図４Ｂ）へ進むようにし、終了オペレーション４０４（図４Ａ）で方法プロセス４００を終了する。あるいは、選択的に、次のインバウンドＨＴＴＰリクエストをプロキシするときに、オペレーション２０４（図４Ａ）に戻る。

【００９３】

別の実施形態では、方法４００は、例えば、オペレーション２１０／２１２とオペレーション２１４との間に、オペレーション３０４、３０６、及び３０８（図３Ｂ）を含むように拡張することもでき、方法３００と同様に、ユーザは、選択されたＨＴＴＰリクエストをブロックする前に、ＨＴＴＰリクエストをブロックすることの承認又は拒否を入力するように要求される。

【００９４】

さらに別の実施形態では、ＨＴＴＰレスポンスをプロキシすること及び解析することを別々に実行することもできる。したがって、別の実施形態では、オペレーション４０２～４５０は、クライアント・コンピュータシステムをドライブバイ・ファーミング攻撃などの悪意のあるコード及び／又は悪意のある行動から保護するため、クライアント・アンチファーミング・アプリケーション１０６によって別々に実行することもできる。

【００９５】

再び図１を参照して、クライアント・アンチファーミング・アプリケーション１０６が、コンピュータメモリ１１２に記憶されている。本明細書中では、コンピュータメモリは

、揮発性メモリ、不揮発性メモリ、又はそれらの組み合わせの何れかである。

【００９６】

また、クライアント・アンチファーミング・アプリケーション１０６はアプリケーションと称しているが、これは例示にすぎない。クライアント・アンチファーミング・アプリケーション１０６は、アプリケーション又はオペレーティングシステムから呼び出され得るものでなければならない。ある実施形態では、アプリケーションは、通常は任意の実行可能なコードとして定義される。さらに、アプリケーション又はオペレーションがある動作を行っている場合、その動作はプロセッサが１以上の命令を実行した結果であることは、当業者には理解されよう。

【００９７】

本発明の実施形態を、クライアント構成に基づいて説明してきたが、本発明は、パーソナルコンピュータ、ワークステーション、モバイル機器、又はコンピュータ装置のネットワークを含むハードウェア構成及び／又は任意の適切な手段を用いて実施することができる。他の実施形態では、クライアント構成以外の他のネットワーク構成（例えば、クライアント・サーバ構成、ピアツーピア構成、ウェブベースの構成、イントラネット構成、インターネット・ネットワーク構成）が用いられる。

【００９８】

ここでは、コンピュータプログラム製品は、本発明のある実施形態においてコンピュータが読み出し可能なコードを格納又は持ち運びできるように構成されたメディア（媒体）を含む。コンピュータプログラム製品の例としては、ＣＤ－ＲＯＭディスク、ＤＶＤ、ＲＯＭカード、フレキシブルディスク、磁気テープ、ＨＤＤ、ネットワーク上のサーバ、及びネットワークを介して送信されるコンピュータが読み出し可能なコードを表す信号等が挙げられる。別の実施形態では、コンピュータプログラム製品としては、ＣＤ－ＲＯＭディスク、ＤＶＤ、ＲＯＭカード、フレキシブルディスク、磁気テープ、ＨＤＤ、及びネットワーク上のサーバを含む、コンピュータが読み出し可能なコードを格納するべく構成された有形のメディアを含む。

【００９９】

図１に示すように、メディアは、コンピュータシステム自体に属するものであり得る。しかし、メディアは、コンピュータシステムから取り外すことも可能であり得る。例えば、クライアント・アンチファーミング・アプリケーション１０６は、プロセッサ１０８と異なる物理的位置に存在するメモリ１１２に記憶され得る。プロセッサ１０８は、メモリ１１２に接続されなければならない。このことは、クライアントサーバシステムによって、あるいは、モデムとアナログラインやデジタルインタフェースとデジタルキャリアラインを介した別のコンピュータとの接続によって達成され得る。

【０１００】

より詳細には、ある実施形態では、クライアント・コンピュータシステム１０２及び／又はサーバー・コンピュータシステム１３０は、モバイルコンピュータ、ワークステーション、双方向ポケベル、携帯電話、デジタル無線電話機、携帯情報端末（ＰＤＡ）、サーバー・コンピュータ、インターネット機器、又は上記した実施形態の少なくとも１つに従ってクライアント・アンチファーミング・アプリケーション１０６の機能を実行することができる構成要素を含む他の任意の装置である。同様に、別の実施形態では、クライアント・コンピュータシステム１０２及び／又はサーバー・コンピュータシステム１３０は、複数の異なるコンピュータ、無線装置、携帯電話、デジタル電話、双方向ポケベル、携帯情報端末（ＰＤＡ）、サーバー・コンピュータ、又は上記の方法を実行するために相互接続される装置の任意の組み合わせから構成される。

【０１０１】

上記の開示内容に基づき、本発明の実施形態によるクライアント・アンチファーミング・アプリケーション１０６の機能は、多種多様なコンピュータシステム構成において実施することができる。さらに、クライアント・アンチファーミング・アプリケーション１０６の機能は、異なる装置のメモリに異なるモジュールとして記憶させることができる。例

えば、最初はクライアント・アンチファーミング・アプリケーション１０６をサーバー・コンピュータシステム１３０に保存しておき、それから必要に応じて、クライアント・アンチファーミング・アプリケーション１０６の一部をクライアント・コンピュータシステム１０２へ移して、クライアント・コンピュータシステム１０２上で実行させることもできる。その結果、クライアント・アンチファーミング・アプリケーション１０６の機能の一部がサーバー・コンピュータシステム１３０のプロセッサ１３４で実行され、前記アプリケーション１０６の他の部分はクライアント・コンピュータシステム１０２のプロセッサ１０８で実行されることになる。

【０１０２】

上記の開示内容に基づき、当業者は、本発明の様々な実施形態を、多種多様な物理的ハードウェア構成において任意のオペレーティングシステム及びコンピュータ言語を用いて実施することができよう。さらなる別の実施形態では、クライアント・アンチファーミング・アプリケーション１０６は、サーバー・コンピュータシステム１３０のメモリ１３６に記憶される。クライアント・アンチファーミング・アプリケーション１０６は、ネットワーク１２６を介してクライアント・コンピュータシステム１０２のメモリ１１２に移される。この実施形態では、ネットワークインタフェース１３８及びＩ／Ｏインタフェース１１０は、アナログモデム、デジタルモデム、又はネットワークインタフェースカードを含み得る。モデムを使用する場合は、ネットワーク１２６は通信ネットワークを含み、クライアント・アンチファーミング・アプリケーション１０６は通信ネットワークを介してダウンロードされる。

【０１０３】

上記の開示内容は、本発明の例示的な実施形態を示すものである。本発明の範囲は、上記の実施形態に限定されるものではない。本明細書中に明示的に記載されている又は示唆されているか否かに関わらず、当業者であれば、本明細書の開示内容から本発明の実施形態に種々の改変を加えて実施し得るであろう。

【図面の簡単な説明】

【０１０４】

【図１】本発明の一実施形態による、クライアント・コンピュータシステム上で実行されるクライアント・アンチファーミング・アプリケーションを含むコンピュータシステムを示す図である。

【図２】本発明の一実施形態に係る、クライアント・コンピュータシステムをドライブバイ・ファーミング攻撃から保護する方法を説明するためのフロー図である。

【図３Ａ】本発明の一実施形態に係る、ユーザの指示によってクライアント・コンピュータシステムをドライブバイ・ファーミング攻撃から保護する方法を説明するためのフロー図である。

【図３Ｂ】図３Ａのフロー図の続きである。

【図４Ａ】本発明の他の実施形態に係る、クライアント・コンピュータシステムをドライブバイ・ファーミング攻撃から保護する方法を説明するためのフロー図である。

【図４Ｂ】図４Ａのフロー図の続きである。

【図４Ｃ】図４Ｂのフロー図の続きである。

【図４Ｄ】図４Ｂのフロー図の続きである。

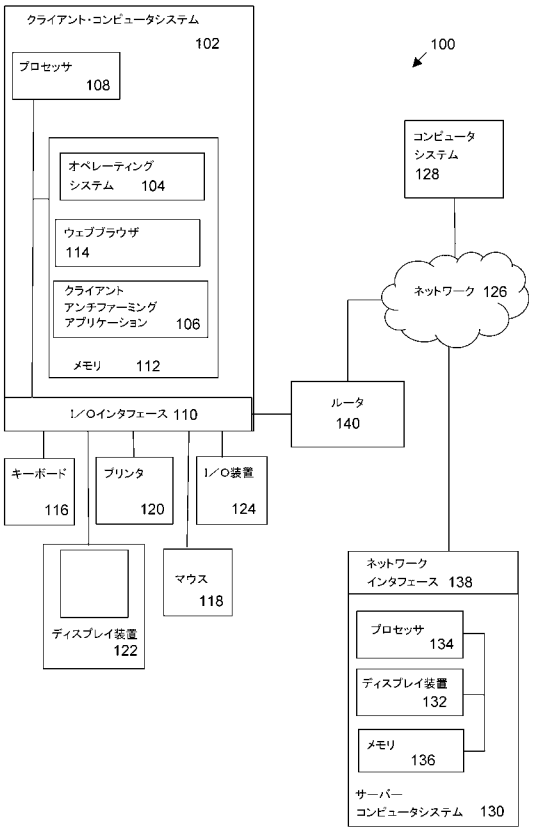
【符号の説明】

【０１０５】

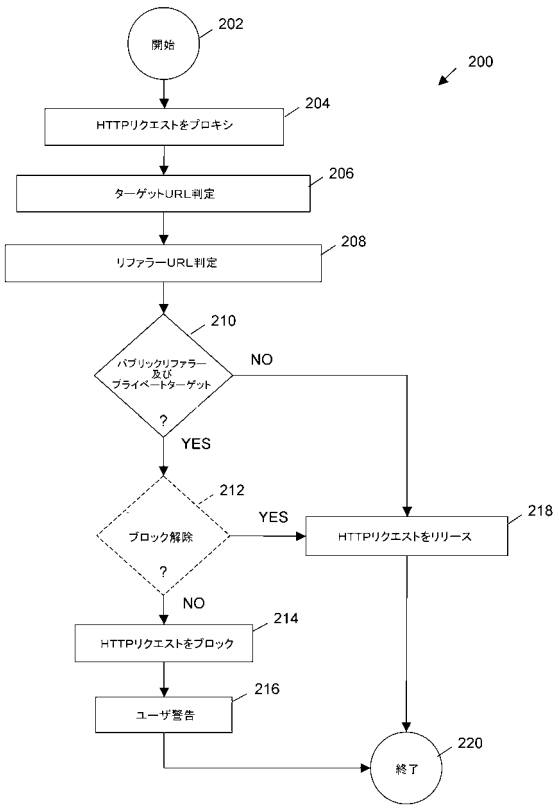
１００　コンピュータシステム
１０２　クライアント・コンピュータシステム
１０４　オペレーティングシステム
１０６　クライアント・アンチファーミング・アプリケーション
１０８　プロセッサ
１１２　メモリ
１１４　ウェブブラウザ

１１０　Ｉ／Ｏインタフェース
１１４　メモリ
１１６　キーボード
１１８　マウス
１４０　ルータ
１２６　ネットワーク
１２８　コンピュータシステム
１３０　サーバー・コンピュータシステム

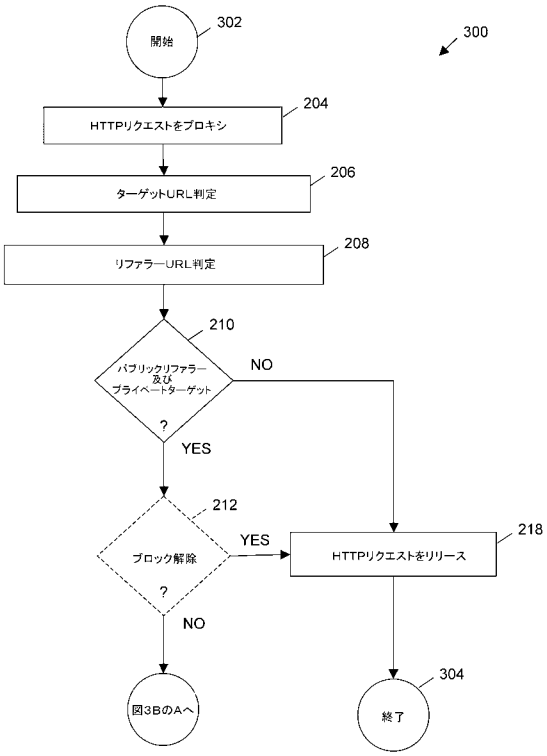
【図１】



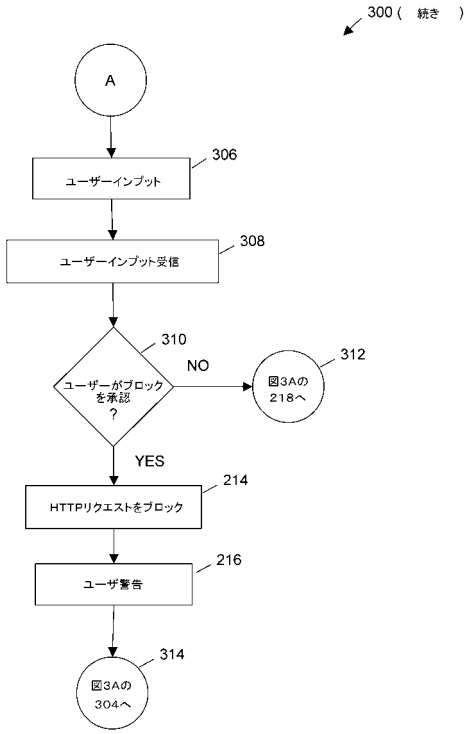
【図２】



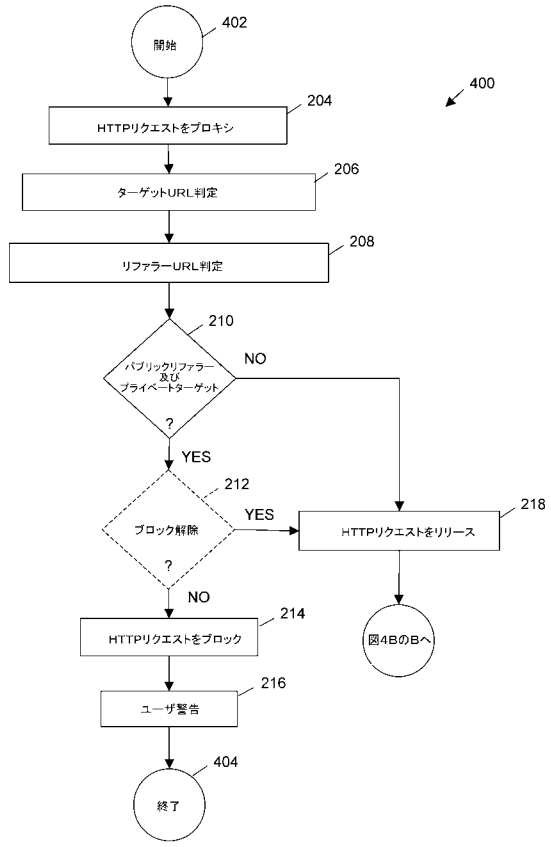
【図３Ａ】



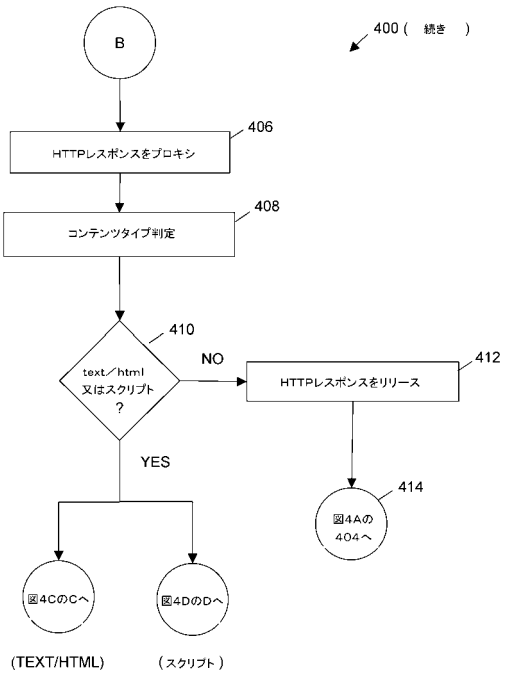
【図３Ｂ】



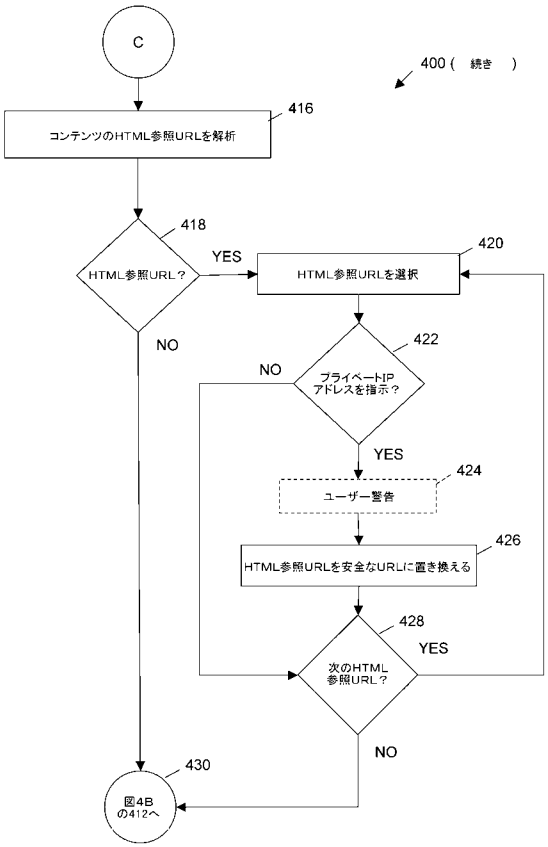
【図４Ａ】



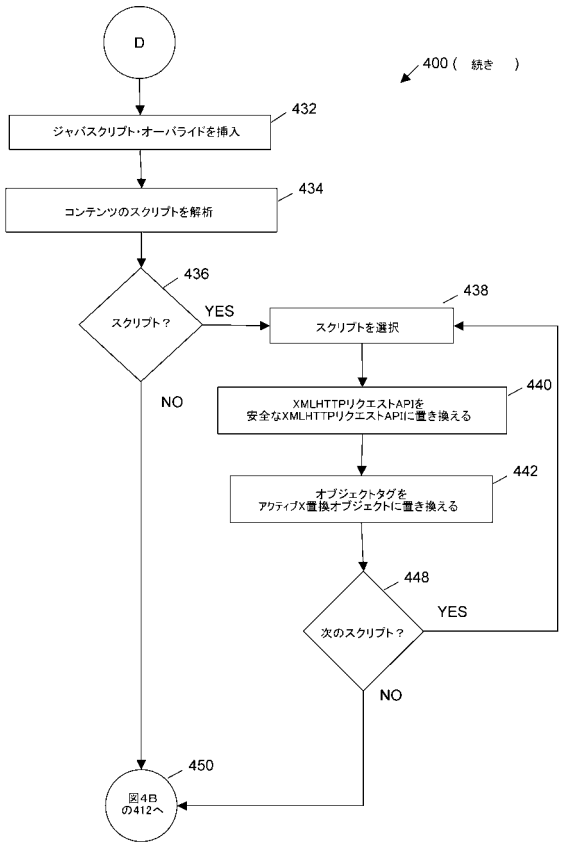
【図４Ｂ】



【図４Ｃ】


C
400（ 続き ）
コンテンツのHTML参照URLを解析
416
418
HTML参照URL？
YES
NO
420
HTML参照URLを選択
422
プライベートIP
アドレスを指示？
NO
YES
424
ユーザー警告
426
HTML参照URLを安全なURLに置き換える
428
次のHTML
参照URL？
YES
NO
430
図4B
の412へ

【図４Ｄ】


D
400（ 続き ）
ジャバスクリプト・オーバライドを挿入
432
コンテンツのスクリプトを解析
434
436
スクリプト？
YES
NO
438
スクリプトを選択
440
XMLHTTPリクエストAPIを
安全なXMLHTTPリクエストAPIに置き換える
442
オブジェクトタグを
アクティブX置換オブジェクトに置き換える
448
次のスクリプト？
YES
NO
450
図4B
の412へ

フロントページの続き

(72)発明者　ロワン・トロロープ
アメリカ合衆国カリフォルニア州９００２７・ロサンゼルス・ノースホバートブルバード　１９２９

審査官　浦口　幸宏

(56)参考文献　米国特許出願公開第２００７／００７４１６９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－２１／５７
Ｈ０４Ｌ　１２／００－１２／２６
Ｈ０４Ｌ　１２／５０－１２／９５５