(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4250618号
(P4250618)
(45)発行日　平成21年4月8日(2009.4.8)　(24)登録日　平成21年1月23日(2009.1.23)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 660J
G06F 21/24 (2006.01)　　G06F 12/14 560C

請求項の数 1　(全 16 頁)

(21)出願番号　特願2005-182783(P2005-182783)
(22)出願日　平成17年6月23日(2005.6.23)
(65)公開番号　特開2007-4415(P2007-4415A)
(43)公開日　平成19年1月11日(2007.1.11)
審査請求日　平成20年4月2日(2008.4.2)

早期審査対象出願

(73)特許権者　596155786
長嶋　克佳
東京都町田市原町田２－２０－１６
(74)代理人　100144048
弁理士　坂本　智弘
(72)発明者　長嶋　克佳
神奈川県相模原市新磯野３丁目４番７号

審査官　小林　秀和

最終頁に続く

(54)【発明の名称】ファーミング詐欺防止方法

(57)【特許請求の範囲】
【請求項１】
コンピュータの要求に応えてドメイン名をＩＰアドレスに変換し、その結果をネットワークを介して前記コンピュータに返すDNSサーバに接続され、前記コンピュータのシステムを始動させたとき、ｈｔｔｐアクセスリクエストの有無を前記コンピュータがチェックするｈｔｔｐアクセスリクエスト有無チェック工程と、
前記ｈｔｔｐアクセスリクエストが前記コンピュータにより検知された場合に、リクエストされたドメインが前記コンピュータに登録されたhostsファイルに存在するか否かを前記コンピュータが判定するドメインhostsファイル内存在チェック工程と、
前記ドメインがhostsファイル内に存在する場合、前記コンピュータがhostsファイルを使う設定になっているか否かを判定し、hostsファイルを使う場合、hostsファイルのドメイン名若しくはIPアドレスが本人確認を行った登録企業のドメイン名とIPアドレスを対で前記コンピュータに登録された登録ドメイン情報にあるか否かを判定し、この登録ドメイン情報に存在しない場合、前記コンピュータが警告を表示すると共に、前記hostsファイルを使うか否か、hostsファイル使用要否のユーザ判断を実行するhostsファイル使用要否ユーザ判断チェック工程と、
ユーザがhostsファイルを使用すると判断する場合に、前記コンピュータのhostsファイル設定で前記コンピュータを前記ネットワークへアクセスさせるhostsファイル設定アクセス実施工程と、
を含むファーミング詐欺防止方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、フィッシング詐欺防止のため、特にファーミング詐欺の防止システムに関するものである。
【背景技術】
【０００２】
フィッシング詐欺と共に最近新たにファーミング詐欺が登場した。 このファーミング詐欺は、大勢のユーザをまとめて刈り取ろうとしているネット詐欺の手口である。 ファーミング詐欺の手口の概要は、可能な限り多くのユーザを、本来訪れようとしている真正のウェブサイトから、悪意あるウェブサイトへ自動的に導くというものである。このファーミング詐欺においては、ユーザが知らぬ間に偽サイトに誘導され、この誘導される偽サイトは、見た目は、一見本物のサイトと変わらない。だが、これに気づかないで、ユーザが自分の口座番号や暗証番号を入力すると、その情報はサイバー詐欺師たちにいつの間にか盗まれてしまう。このネット詐欺の手口 最近になり、米国から日本へ普及しだした新たなサイバー犯罪の手口である。しかし、現在のところ、これに対して、画期的対応手段が提供されていない。
【０００３】
ファーミング詐欺の手口は、例えば、正しいＤＮＳ情報が「４１．１．２７．２２０ｗｗｗ．ａｃｏｍ．ｃｏ．ｊｐ」であるのに、偽装されたｈｏｓｔｓファイルが、「２０２．２．３５．２１１ｗｗｗ．ａｃｏｍ．ｃｏ．ｊｐ」として変えられ、ユーザのマシンのｈｏｓｔｓファイル若しくは参照するＤＮＳサーバに、偽のドメイン情報を登録するもので、これにより、正しいサイトにアクセスしようとしても、偽サイトにアクセスさせるフィッシングの新しい手口である。
【０００４】
ここで、hostsファイルとは、一般に、TCP/IPを使ったネットワーク（インターネットなど）で、あるノード（IPアドレスが付いている端末のこと）のIPアドレスと、そのノードをあらわす文字列（別名）の対応を記録したファイルです。 その効果は、hostsファイルにIPアドレスと名前の対応を書いておくと、DNSサーバを参照することなくＩＰアドレスが解決できる。
例えば、LANにおいていくつかのパソコンを連結し、そのうちの一つをWebサーバとするとき、hostsファイルに該ＷｅｂサーバのＩＰアドレスと名前の対応を書いておくと、ＤＮＳサーバを参照することなく名前の解決が出来る。Webアクセスに限らずドメイン名を使ったサーバへのアクセスはhostsファイルが優先される。
従って、通常のWeb検索において、hostsファイルには一般的にはＩＰアドレスが記載されていない。
ファーミング詐欺においては、該hostsファイルに誘導先IPアドレスを書き込むことで目的のサイトに誘導し端末側ユーザ情報（住所、氏名、口座番号、暗証番号、クレジット等のカード番号、生年月日等）を不正に取得しようとする。
hostsファイルは、通常は、Windows（登録商標）2000/XPの場合、「C:\WINNT（またはWindows（登録商標））\system32\drivers\etc」、Windows（登録商標）98の場合は「C:\Windows（登録商標）」にある。Linux（登録商標）の場合は、一般に「/etc/hosts」にあることが、技術マニュアルなどで公開されている。
【０００５】
しかし、ユーザのマシンも、ＤＮＳサーバも、その書き換えはウィルスソフトによるものが殆どであったが、最近ではＤＮＳサーバをなりすまして設定する悪質行為も発生している（２００５年５月３０日、日経産業新聞、朝刊）。これらの書き換えを防ぐ対策はウィルスバスターなどにより採られ、アクセスに関しての対策としては、何ら対策がなく、ウィルスバスターなどによるウィルス駆逐のみでは全く対処できないのが現状であった。
上記したように、例えば、正しいＤＮＳ情報が「４１．１．２７．２２０ｗｗｗ．ａｃ

ｏｍ．ｃｏ．ｊｐ」であるのに、偽装されたｈｏｓｔｓファイルが、「２０２．２．３５．２１１ｗｗｗ．ａｃｏｍ．ｃｏ．ｊｐ」として変えられているときには、Ｗｅｂページにアクセスする場合に、通常は使用しているＤＮＳサーバに登録されている情報を基にＩＰアドレスを変換してアクセスするが、ｈｏｓｔｓファイルは、ＤＮＳサーバよりも先に判断されるので、ｈｏｓｔｓファイルに偽の情報が書かれていると、偽の情報が先に判断され、これに気づかないという問題を残すものであった。

なお、ここで、ＤＮＳとは、ドメイン名をＩＰアドレスに変換するための通信サービスの一つであり、コンピュータネットワークによる通信の際には人間が覚えやすいドメイン名を使用するのに対し、コンピュータは数値で表わせるＩＰアドレスを使用して通信を実行しなければならないので、ドメイン名とＩＰアドレスの対応づけが必要であり、この対応付けのため、ドメイン名とＩＰアドレスの対応づけのデータベースを登録管理し、ドメイン名のＩＰアドレスへの変換を行う通信サービスのことである。また、ＤＮＳサーバとは、ＤＮＳのプログラムとデータベースを備え、各コンピュータの要求に応えてドメイン名をＩＰアドレスに変換し、結果をコンピュータに返すサーバをいう。

【０００６】

また、具体的手口は、ファーミング詐欺プログラム（不正プログラム）がサーバに進入し、hostsファイルを書き換えたり、一時的に外部から不正侵入しhostsファイルを書き換えたりする場合がある。

【０００７】

例えば、サーバドメインに対応するＩＰアドレスの書き換えは、各種サーバドメインに対応するＩＰアドレス（ｈｔｔｐ、ｆｔｐ、ＳＭＴＰ）のhostsファイル書き換えである。　具体的には次ぎの例が挙げられる。

（１）ドメイン名によるｈｔｔｐアクセス時にhostsファイルが書き換えられていた場合、より具体的には、「ｈｔｔｐ：／／ｗｗｗ．ｈｏｇｅ．ｈｏｇｅ．ｊｐ」にアクセスしようとしたときに、「ｗｗｗ．ｈｏｇｅ．ｈｏｇｅ．ｊｐ」がhostsファイルで偽装定義されている場合であり、この場合には、偽のWebサイトにアクセスされることになり、クレジットカード番号や各種のＩＤが盗まれ。　したがって、何らかの対策をしなければ気がつきにくいという問題がある。

【０００８】

また、（２）ドメイン名によるｆｔｐアクセス時にhostsファイルが書き換えられていた場合、より具体的には、「ｆｔｐ：／／ｆｔｐ．ｈｏｇｅ．ｈｏｇｅ．ｊｐ」にアクセスしようとしたときに、「ｆｔｐ．ｈｏｇｅ．ｈｏｇｅ．ｊｐ」がhostsファイルで偽装定義されている場合であり、この場合には、偽のｆｔｐサーバにアクセスされることになり、アップロードの場合、転送したファイルが盗まれる。この場合には、ダウンロードの際に、必要なファイルがないことに気づく可能性はあるが、気づくまでは時間がかかる。また、アップロードの際に、真正のサーバにファイルがないことに気づく可能性があるが、気づくまでに時間がかかるという問題がある。

【０００９】

さらに、（３）ドメイン名によるメール送信時にhostsファイルが書き換えられていた場合、より具体的には、メール送信しようとした場合に、指定しているＳＭＴＰサーバ、「ｓｍｔｐ．ｈｏｇｅ．ｈｏｇｅ．ｊｐ」が、hostsファイルで偽装定義されている場合であり、この場合には、送信メールが全て盗まれてしまう。この場合、メールは相手に届くと共にメールの送受信とも行なわれるので、非常に気がつきにくいという問題がある。

【００１０】

新聞情報（日経産業新聞２００５年５月３０日付朝刊）によれば、ブログを使い、架空請求詐欺を狙った動きが急増し、「トラックバック」機能を使い特定ブログとリンクを張る手口が現れた。さらに、ドメイン名管理するＤＮＳサーバになりすまして住所を書換え、偽サイトに導く手法も出現し、セキュリテー業界からも恐れられている。これらの現状から、早急な対応が求められている。

以上の状況から、hostsファイルを監視し書き換えられたことをいち早く検知し、該不

正プログラムの存在を発見削除し、ファーミング詐欺プログラムによる詐欺を防止する手段が待たれている。

【特許文献１】特願２００５－１０７５４０

【非特許文献１】Wired News－正しいＵＲＬを偽サイトにつなげる「ファーミング詐欺」（上）

【発明の開示】

【発明が解決しようとする課題】

【００１１】

従って、本願発明は、hostsファイルを監視すると共にＤＮＳサーバが書換えやなりすましにあっていないか等監視し、書き換えられたことをいち早く迅速に検知し、該不正プログラムの存在を発見して、これを削除し、ファーミング詐欺を防止するシステムとその装置を提供するものである。

また、「hostsファイル」書換えプログラムの解析と駆除を実行する際に、ファーミングプログラムの発見に基づいて、「hostsファイル」を書換えたプログラム名と書き換え内容を認証局に自動通報し、この自動通報により、ウィルス情報、ファーミングプログラム等の情報提供により、ファーミング詐欺防止の迅速対処と確実化を図り、そのためのシステム装置を提供することである。

【課題を解決するための手段】

【００１２】

上記課題を解決するため、本願発明のファーミング詐欺防止方法は、（イ）「hostsファイル」のバックアップ（コピー）を作成する第１の処理工程（Ｓ１１）と、（ロ）作成したバックアップ「hostsファイル」について、「hostsファイル」書換え有無チェック、プログラムウィルス汚染チェックの下に、「hostsファイル」を書換えたプログラムの解析と駆除を行う第2の処理工程（Ｓ１２、Ｓ１３、Ｓ１４）と、（ハ）第2の処理工程に続いて、バックアップ（コピー）から元の「hostsファイル」を復元し、インターネットへのアクセスを有効とする第３の処理工程（Ｓ１５，Ｓ１６）と、を含む。

【００１３】

より具体的には、（イ）「hostsファイル」のバックアップ（コピー）を作成するバックアップ用「hostsファイル」複製工程Ｓ１１と、(ロ)複製「hostsファイル」について、タイムスタンプの変更の有無により、「hostsファイル」書換え発生の有無をチェックする「hostsファイル」書換え有無チェック工程Ｓ１２と、（ハ）書換え発生を検知したときに、＜プログラムがウィルスか＞否か、プログラムウィルス汚染をチェックするプログラムウィルス汚染チェック工程Ｓ１３と、（ニ）前記プログラムウィルス汚染チェック工程で、ウィルスがないことを検知したとき、インターネットへのアクセスを一時的に無効にする処理（Ｓ１４１）を実行し、その間に、「hostsファイル」を書換えたプログラムの解析と駆除の処理（Ｓ１４２）を実行すると共に、その際、解析によって「hostsファイル」の書き換えが得られたときには該ファーミングプログラムの強制削除処理（Ｓ１４３）を実行する「解析発見書換えプログラムの名称・内容通報及び強制削除」工程Ｓ１４と、(ホ）この「解析発見書換えプログラムの名称・内容通報及び強制削除」工程に続いて、バックアップ（コピー）から元の「hostsファイル」を復元する「hostsファイル」を復元工程Ｓ１５と、（ヘ）「hostsファイル」を復元工程に続いて、インターネットへのアクセスを有効にするインターネットへのアクセス許容工程Ｓ１６と、ファーミング詐欺防止システムの始動点にフィッドバックを掛け、繰り返しチェック処理するチェック工程と、を含む。

【００１４】

また、本願発明のファーミング詐欺防止方法は、「hostsファイル」書換え有無チェック工程Ｓ１２で、書換え発生を検知しなかったとき、監視するためフィードバックしてチェックを掛け直す常駐監視回路を構成する常駐監視工程Ｓ１２１を備えたり、

前記「hostsファイル」書換え有無チェック工程Ｓ１２で、書換え発生を検知しなかったとき、同時に、「hostsファイル」復元工程Ｓ１５へと進める工程Ｓ１２２を備え（請求

項４）たり、前記プログラムウィルス汚染チェック工程Ｓ１３で、ウィルス検知のとき、ウィルスを駆除するソフトにより駆除し、「解析発見書換えプログラムの名称・内容通報及び強制削除」工程Ｓ１４へと接続されるウィルス駆除回路になるウィルス駆除工程Ｓ１３１を備え、「hostsファイル」書換えプログラムの解析と駆除を実行する際に、ファーミングプログラムの発見に基づいて、「hostsファイル」を書換えたプログラム名と書き換え内容を認証局に自動的に通報する自動通報工程Ｓ１４４と、情報提供によるウィルス情報、ファーミングプログラム等のデータベース化（DB化）のための通報により、認証局がこれらの情報を受信し、ウィルス情報DBに登録し、ファーミングプログラムをウィルス情報DBに蓄積する認証局ウィルス情報DB化工程Ｓ１４５を含む。

【００１５】

上記課題を解決するため、本願発明のファーミング詐欺防止方法は、（イ）システム（F2）を始動させたとき、＜「ｈｔｔｐアクセス」のリクエストがあったか＞「ｈｔｔｐアクセス」リクエストの有無をチェックする「ｈｔｔｐアクセス」リクエスト有無チェック工程Ｓ２１と、（ロ）「ｈｔｔｐアクセス」リクエスト有無チェック工程２１において「YES」の場合に続く、＜リクエストされたドメインは「hostsファイル」に存在するか＞を判定するドメイン「hostsファイル」内存在チェック工程Ｓ２２と、（ハ）ドメイン「hostsファイル」内存在チェック工程Ｓ２２において「YES」の場合に続く、＜「hostsファイル」を使う設定になっているか＞を判定し、「hostsファイル」仕様条件チェック工程Ｓ２３と、（ニ）「hostsファイル」仕様条件チェック工程２３において「YES」の場合に続く、＜「hostsファイル」のドメイン名（IPアドレス）が登録ドメイン情報にあるか＞を判定するドメイン名符合チェック工程Ｓ２４と、（ホ）ドメイン名符合チェック工程Ｓ２４において「ＮＯ」の場合に、警告を表示するＳ２４１と共に、これに続いて、＜hostsファイルを使うか＞hostsファイル使用要否のユーザ判断を実行するhostsファイル使用要否ユーザ判断チェック工程Ｓ２５と、（ヘ）hostsファイル使用要否ユーザ判断チェック工程Ｓ２５において「YES」の場合にhostsファイル設定でアクセスするhostsファイル設定アクセス実施工程Ｓ２６とを含む。

【００１６】

さらに、本願発明のファーミング詐欺防止方法は、「ｈｔｔｐアクセス」リクエスト有無チェック工程Ｓ２１のチェック結果「ＮＯ」の場合に、リクエスト待機可能に、「ｈｔｔｐアクセス」リクエスト有無チェックの前段へとフィードバックするリクエスト待機回路を形成するリクエスト待機回路形成工程を備え（請求項８）たり、

ドメイン「hostsファイル」内存在チェック工程Ｓ２２のチェック結果「ＮＯ」の場合に、ドメイン名及びＩＰアドレス含むＤＮＳ情報をゲットするＤＮＳ情報取得工程Ｓ２２１と、これに続き＜ゲットしたＩＰアドレスとドメイン名の対が、ドメイン情報にあるか＞を判定する、ドメイン情報内ＩＰアドレス・ドメイン名両項目有無チェック工程Ｓ２２２と、ドメイン情報内ＩＰアドレス・ドメイン名両項目有無チェック工程Ｓ２２２のチェック結果「ＮＯ」の場合に、警告メッセージの表示（Ｓ２２３１）、書き換えられたＩＰアドレスに基づくホーム頁をブラックリストの登録（Ｓ２２３２）、真正登録企業にファーミング詐欺発生とブラックリストの通知（Ｓ２２３３）の少なくとも一つの処理及び強制終了（Ｓ２２３４）の処理を含む不正プログラム警告・登録・強制終了工程（Ｓ２２３）を備え（請求項９）たり、

ドメイン情報内ＩＰアドレス・ドメイン名両項目有無チェック工程Ｓ２２２のチェック結果「ＹＥＳ」の場合に、通常のアクセスへと進める工程Ｓ２２４を備え（請求項１０）たり、 hostsファイル使用要否ユーザ判断チェック工程Ｓ２５のチェック結果「ＮＯ」の場合に、書き換えられたＩＰアドレスに基づくホーム頁をブラックリストの登録（Ｓ２５１１）、真正登録企業にファーミング詐欺発生とブラックリストの通知（Ｓ２５１２）する処理を含み、

「hostsファイル」仕様条件チェック工程２３のチェック結果「ＮＯ」の場合に、ドメイン「hostsファイル」内存在チェック工程Ｓ２２のチェック結果「ＮＯ」の場合に、ドメイン名及びＩＰアドレス含むＤＮＳ情報をゲットするＤＮＳ情報取得工程Ｓ２２１と、こ

れに続き＜ゲットしたＩＰアドレスとドメイン名の対が、ドメイン情報にあるか＞を判定する、ドメイン情報内ＩＰアドレス・ドメイン名両項目有無チェック工程Ｓ２２２と、ドメイン情報内ＩＰアドレス・ドメイン名両項目有無チェック工程Ｓ２２２のチェック結果「ＮＯ」の場合に、警告メッセージの表示（Ｓ２２３１）、書き換えられたＩＰアドレスに基づくホーム頁をブラックリストの登録（Ｓ２２３２）、真正登録企業にファーミング詐欺発生とブラックリストの通知（Ｓ２２３３）の少なくとも一つの処理及び強制終了（Ｓ２２３４）の処理を含む不正プログラム警告・登録・強制終了工程（Ｓ２２３）を備え（請求項１２）たり、
ドメイン名符合チェック工程Ｓ２４のチェック結果「ＮＯ」の場合に、hostsファイル設定でアクセスするhostsファイル設定アクセス実施工程Ｓ２６を含む。

【発明の効果】
【００１７】
本発明のシステム及び装置によれば、hostsファイルを監視し書き換えられたことをいち早く検知し、該不正プログラムの存在を発見することができ、これに基づいて発見した不正プログラムを削除し、hostsファイルを復元するプログラムにより詐欺を防止することができる。
さらに、ファーミング詐欺であるhostsファイルの書き換えに対して、また、hostsファイルの書き換え以外に、DNSサーバに存在するドメイン名とIPアドレス対応テーブルのIPアドレスを書き換えに対しても、これらの場合にファーミング詐欺防止機能を果すことができる。
【発明を実施するための最良の形態】
【００１８】
本願発明のファーミング詐欺防止システムによれば、
（イ）システムの始動によって、「hostsファイル」のバックアップ（コピー）を作成するバックアップ用「ｈｏｓｔｓファイル」複製処理と、コピーされたバックアップ用「ｈｏｓｔｓファイル」について、「hostsファイル」書換え発生有無をチェックする「ｈｏｓｔｓファイル」書換えチェック処理と、「ｈｏｓｔｓファイル」書換えチェックの結果、書換え不発生で「ＮＯ」のとき、フィードバックして「ｈｏｓｔｓファイル」書換えチェックを掛け直す常駐監視によって、回路タイムスタンプの変更の有無を監視する第一チェック工程と、
（ロ）「ｈｏｓｔｓファイル」書換え発生し「ＹＥＳ」のときに、＜プログラムがウィルスか＞否か、プログラムウィルス汚染をチェックし、このプログラムウィルス汚染チェックするプログラムウィルス汚染チェック処理を実行し、プログラムウィルス汚染チェック処理の結果、「ＹＥＳ」でウィルスであったとき、ソフトによる駆除でウィルスを駆除し、「解析発見書換えプログラムの名称・内容通報及び強制削除」工程Ｓ１４へと接続されるウィルス駆除回路を備える第二チェック工程と、
（ハ）前記第二チェック工程のプログラムウィルス汚染チェック処理の結果、「ＮＯ」で、ウィルスでないと判断されたときでも、インターネットへのアクセスを一時的に無効にし、その間、「hostsファイル」を書換えたプログラムの解析と駆除を実行処理し、その際、ファーミングプログラムの発見時当該プログラムを強制削除すると共に、その「hostsファイル」を書換えたプログラム名と書き換え内容を認証局に自動通報処理する、発見ファーミングプログラム強制削除・通報処理工程と、
（ホ）発見ファーミングプログラム強制削除・通報処理に続いて、バックアップ（コピー）から元の「hostsファイル」を復元し、これによって、インターネットへのアクセスを有効にする処理し、以上、バックアップ用「ｈｏｓｔｓファイル」チェック処理後、「hostsファイル」復元によりインターネットへのアクセスを有効に実行するため、システムの始動点へとフィードバックする処理工程を備え、
（ヘ）認証局では、前記発見ファーミングプログラム強制削除・通報処理工程における自動通報により、ウィルス情報、ファーミングプログラム等の情報提供を受信し、ファーミ

ングプログラムを蓄積したウィルス情報DBに登録処理する工程を包含している。

【００１９】

本願発明の、他のファーミング詐欺防止システムによれば、

（イ）システム（F2）を始動させると、最初に、＜「hostsアクセス」のリクエストがあったか＞「hostsアクセス」リクエストの有無をチェックすると共に、その結果、「NO」の場合にはリクエスト待機可能に、「hostsアクセス」リクエスト有無チェックの前段へとフィードバックするリクエスト待機回路を包含する第一チェック工程と、（ロ）第一チェック工程において「YES」の場合に、＜リクエストされたドメインは「hostsファイル」に存在するか＞を判定する「hostsファイル」内ドメイン存在チェックの第二チェック工程と、（ハ）「hostsファイル」内ドメイン存在チェックにおいて、「NO」の場合に、ドメイン名又はＩＰアドレスからＤＮＳ情報をゲットし、＜ゲットしたＩＰアドレスとドメイン名の対が、ドメイン情報にあるか＞を判定する、ドメイン情報内ＩＰアドレス・ドメイン名両項目有無チェックの第三チェック工程と、（ニ）ドメイン情報内ＩＰアドレス・ドメイン名両項目有無チェックの結果、「ＹＥＳ」の場合には、通常のアクセスを行ない、一方「ＮＯ」の場合には、警告メッセージ、「ＤＮＳサーバが何者かに書き換えられています。」「ファーミング詐欺が発生しています。」「アクセスを中断してください。」の表示を行い、併せて、書き換えられたＩＰアドレスに基づくホーム頁をブラックリストに登録し、且つ真正登録企業にファーミング詐欺発生とブラックリストを通告し、最終的に強制終了する「通常アクセス／通報・登録・強制終了選択工程と、（ホ）上記第二チェック工程において「YES」の場合に、さらに＜「hostsファイル」を使う設定になっているか＞を判定し、所定の設定条件成立チェックを実行する第四チェック工程と、（ヘ）第四チェック工程の結果、「Ｎｏ」の場合に、第三チェック工程を経て「通常アクセス／通報・登録・強制終了選択工程へ進められるが、「ＹＥＳ」の場合に、＜「hostsファイル」のドメイン名（IPアドレス）が登録ドメイン情報にあるか＞が判定されるドメイン名符合チェックの第５チェック工程と、（ト）第５チェックの結果、「YES」である場合には、hostsファイルの設定でアクセスする工程に進められるが、「ＮＯ」の場合には、警告表示が実施され、次いで、＜hostsファイルを使うか＞hostsファイル使用要否のユーザ判断が実行される第６チェック工程と、（チ）第６チェック工程の結果、「YES」の場合には、hostsファイル設定でアクセスし、「NO」の場合には、書き換えられたＩＰアドレスに基づくホーム頁をブラックリストに登録すると共に真正登録企業にファーミング詐欺発生とブラックリストを通知し、さらに、前記した第三チェック工程を経て「通常アクセス／通報・登録・強制終了選択工程へ進められる選択工程とを包含している。

これによって、hostsファイルの監視により、hostsファイルの書き換えを迅速に検知して、該不正プログラムの存在を発見し、発見した不正プログラムを削除すると共に、hostsファイルを復元するプログラムにより一層確実に詐欺の防止が可能である。

【実施例１】

【００２０】

図１は、別途具体的なプログラムの構成の一つとして、ファーミング詐欺防止システムの第１の実施例を示す。この第１のファーミング詐欺防止システムＦ１による情報処理フローは次のとおり実施される。

第１のファーミング詐欺防止システムＦ１を始動Ｓ１０させる。

すると、最初に、「hostsファイル」複製工程Ｓ１１で、「hostsファイル」のバックアップ（コピー）を作成する。「hostsファイル」複製工程Ｓ１１に「hostsファイル」書換え有無チェック工程Ｓ１２が続き、この「hostsファイル」書換え有無チェック工程Ｓ１２で、＜プログラムによる「hostsファイル」の書換えが発生したか＞タイムススタンプの変更の有無による「hostsファイル」書換え有無チェック（ＱＦ１１）を実施する。

「hostsファイル」書換え有無チェック工程Ｓ１２における「hostsファイル」書換え有無チェック（ＱＦ１１）の結果、「NO」の場合にはフィードバックを掛けてタイムスタンプの変更を監視する常駐監視を繰り返す。

また、書換え発生を検知しなかった「NO」の場合には、「hostsファイル」復元工程Ｓ１５へと進める工程Ｓ１２２を備えることもできる。
上記「hostsファイル」書換え有無チェック（ＱＦ１１）の結果、書換え発生を検知し「YES」の場合には、次段のプログラムウィルス汚染チェック工程Ｓ１３で、＜プログラムがウィルスか＞否か、プログラムウィルス汚染チェック（ＱＦ１２）を実施する。このプログラムウィルス汚染チェック（ＱＦ１２）の結果、「YES」の場合には、「解析発見書換えプログラムの名称・内容通報及び強制削除」工程Ｓ１４へと接続されてウィルス駆除回路を形成するウィルス駆除工程Ｓ１３１において、ウィルス駆除ソフトによる駆除が実施される。なお、その際、認証局受信し登録したファーミングプログラムを備えたウィルス情報ＤＢ２２を利用して、プログラムウィルス汚染チェック（ＱＦ１２）を実施する。

【００２１】

上記プログラムウィルス汚染チェック（ＱＦ１２）の結果、ウィルスでないと判断され「NO」の場合であっても、前段で「hostsファイル」書換えが発生したものであるから、インターネットへのアクセスを一時的に無効Ｓ１４１にする。この状態で、「hostsファイル」を書換えたプログラムの解析と駆除Ｓ１４２を実行する。その際、解析によって得られた「hostsファイル」を書換えたプログラム名と書き換え内容を認証局に自動通報Ｓ１４４し、ファーミングプログラムの発見を通報すると共に該プログラムの強制削除Ｓ１４３を実行する。

なお、自動通報Ｓ１４４に当っては、ウィルス情報、ファーミングプログラム等の情報提供によりこれをデータベース化（DB化）される。認証局がこれらの情報を受信すると、認証局はファーミングプログラムを蓄積したウィルス情報DB２２を備えているので、このウィルス情報DB２２に登録Ｓ１４５される。

前述の「hostsファイル」を書換えたプログラムの解析と駆除Ｓ１４３に続いて、バックアップ（コピー）から元の「hostsファイル」を復元Ｓ１５する。これによって、インターネットへのアクセスを有効Ｓ１６にする。以上のチェック処理、情報処理を繰り返すため、前述の常駐監視工程Ｓ１２１と同様の常駐監視工程Ｓ１６１を介して、＜「hostsファイル」のバックアップ（コピー）を作成する＞作業の後段の２次的始動点Ｐ０へとフィードバック可能に接続される。

したがって、上記本発明のシステムによれば、hostsファイルを監視し書き換えられたことをいち早く検知し、該不正プログラムの存在を発見することができ、これに基づいて発見した不正プログラムを強制的に削除した上で、hostsファイルを復元するプログラムにより処理するので、ファーミングプログラムによる詐欺を確実に防止することができる。

【００２２】

第１のファーミング詐欺防止システムＦ１によれば、バックアップ「hostsファイル」について、「hostsファイル」書換え有無チェック、プログラムウィルス汚染チェックの下に、「hostsファイル」を書換えたプログラムの解析と駆除を行い、ウィルスはソフトにより除去し、「ｈｏｓｔｓファイル」を書換えたプログラムは解析を認証局に自動通報し認証局で登録すると共に強制駆除、その上で、バックアップ（コピー）から元の「hostsファイル」を復元し、インターネットへのアクセスを有効とするシステムであるからファーミング詐欺を効果的に防止することができる。

前記「ｈｏｓｔｓファイル」書換え有無チェック工程Ｓ１２で、書換え発生を検知しなかったとき、常駐監視するフィードバック回路を形成する常駐監視工程Ｓ１２１を備えているので、「ｈｏｓｔｓファイル」書換え発生有無のチェック漏れを皆無とすることができ、ファーミング詐欺を効果的に防止することができる。
また、前記プログラムウィルス汚染チェック工程Ｓ１３で、ウィルス検知の「ＹＥＳ」のとき、「解析発見書換えプログラムの名称・内容通報及び強制削除」工程Ｓ１４へと接続されるウィルス駆除回路のウィルス駆除工程Ｓ１３１においてウィルス駆除ソフトにより駆除することができるので、ウィルス汚染の観点からその有無のチェックを漏れなく実施することができ、ファーミング詐欺を効果的に防止することができる。

前記プログラムウィルス汚染チェック工程Ｓ１３で、書換え発生を検知しなかった「ＮＯ」ときにも、「ｈｏｓｔｓファイル」復元工程Ｓ１５へと進める工程Ｓ１２２へと処理を進め、念のためバックアップ（コピー）から元の「hostsファイル」を復元し、インターネットへのアクセスを有効として次へ進めることも可能であり、これは、プログラムウィルス汚染チェックの結果「ＹＥＳ」の場合にウィルス駆除し、始動点に戻り作成し直したバックアップ「hostsファイル」について、「hostsファイル」書換え有無チェックし、書換え発生を検知しなかった「ＮＯ」ときに、「ｈｏｓｔｓファイル」復元工程Ｓ１５へと進める工程Ｓ１２２へと処理を進める場合と同様である。

【実施例２】

【００２３】

図２は、ファーミング詐欺防止システムの第２の実施例を示す。

この第２のファーミング詐欺防止システムＦ２による情報処理フローは次のとおり実施される。

第二のファーミング詐欺防止システムＦ２を始動Ｓ２０させると、最初に、＜「hostsアクセス」のリクエストがあったか＞「hostsアクセス」リクエストの有無がチェック（ＱＦ２１）される（「ｈｔｔｐアクセス」リクエスト有無チェック工程Ｓ２１）。その結果、「NO」の場合にはリクエスト待機可能に、「hostsアクセス」リクエスト有無チェックの前段へとフィードバックされる（リクエスト待機回路形成工程Ｓ２１１）。

「hostsアクセス」リクエストの有無チェック（ＱＦ２１）の結果、「YES」の場合は、次の＜リクエストされたドメインは「hostsファイル」に存在するか＞を判定する「hostsファイル」中ドメイン存在チェック（ＱＦ２２）が実施される（「hostsファイル」内ドメイン存在チェック工程Ｓ２２）。一方「NO」の場合には、図２における、図面符号丸１以下の符号Ｓ２２１に示すように、ＤＮＳ情報チェックが実施される。斯かるＤＮＳ情報チェックの詳細については後述する。

ドメイン「hostsファイル」存在チェック（ＱＦ２２）の結果、「YES」の場合には、さらに＜「hostsファイル」を使う設定になっているか＞を判定する仕様設定適否チェック（ＱＦ２３）が実行される（「hostsファイル」仕様条件チェック工程Ｓ２３）。　その結果、「NO」のときには、前記同様、後で説明する図面符号丸１に示すＤＮＳ情報チェックが実施される。

一方、結果が「YES」の場合には、＜「hostsファイル」のドメイン名（IPアドレス）が登録ドメイン情報にあるか＞を判定するドメイン名符合チェック（ＱＦ２４）を実施する（ドメイン名符合チェック工程Ｓ２４）。本チェック（ＱＦ２４）の結果、「YES」である場合には、図２での、符号丸２以下に示すように、「hostsファイル」の設定でアクセスする（hostsファイル設定アクセス実施工程Ｓ２６）。しかし、ドメイン名符合チェック（ＱＦ２４）の結果、「NO」の場合には、警告を表示する（警告表示工程Ｓ２４１）。その際のメッセージは、図２にドメイン名符合チェック工程Ｓ２４の四角枠内に例示の「警告を表示するメッセージ例」として例示される。

【００２４】

チェック（ＱＦ２４）の結果「NO」の場合の警告表示に続いて、＜hostsファイルを使うか＞ユーザ判断によるhostsファイル使用可否チェック（ＱＦ２５）を実行する（hostsファイル使用要否ユーザ判断チェック工程Ｓ２５）。このチェック（ＱＦ２５）の結果、「YES」の場合には、hostsファイルの設定でアクセスする（hostsファイル設定アクセス実施工程Ｓ２６）。しかし、「NO」の場合には、ブラックリスト登録・通知工程Ｓ２５１へと進められ、　このブラックリスト登録・通知工程Ｓ２５１において、書き換えられたＩＰアドレスに基づくホーム頁をブラックリストに登録（Ｓ２５１１）し、且つ真正登録企業にファーミング詐欺発生とブラックリストを通知（Ｓ２５１２）し、続いて、図２、図面符号丸１以下に示すＤＮＳ情報確保工程Ｓ２２１に続きＤＮＳ情報チェックＱＦ２６が実施される（ＤＮＳ情報チェック工程Ｓ２２２）。

【００２５】

以下、この図面符号○１以下に示すＤＮＳ情報について、そのドメイン名及びＩＰアド

レスからのチェックについて説明する
先ず、ドメイン「hostsファイル」存在チェック（ＱＦ２２）時に得られたリクエストのドメイン名を基に「ＤＮＳ情報」をゲットし、アドレス情報を入手する（ＤＮＳ情報確保工程Ｓ２２１）。
そこで「ＤＮＳ情報」について＜ゲットしたＩＰアドレスとドメイン名の対が、ドメイン情報にあるか＞を判定する、ＤＮＳ情報チェック（ＱＦ２６）を実施する（ＤＮＳ情報チェック工程Ｓ２２２）。
このチェック（ＱＦ２６）の結果、「ＹＥＳ」の場合には、直接通常のアクセスを行なう（通常アクセス工程Ｓ２２４）。一方「ＮＯ」の場合には、警告・ブラックリスト登録・通知・強制終了工程Ｓ２２３へと進められ、　警告・ブラックリスト登録・通知・強制終了工程Ｓ２２３において、警告メッセージ、「ＤＮＳサーバが何者かに書き換えられています。」「ファーミング詐欺が発生しています。」「アクセスを中断してください。」が表示され（Ｓ２２３１）、次いで、書き換えられたＩＰアドレスに基づくホーム頁をブラックリストに登録する（Ｓ２２３２）と共に、真正登録企業にファーミング詐欺発生とブラックリストを通告（Ｓ２２３３）し、最終的に強制終了（Ｓ２２３４）する。
【００２６】
第２のファーミング詐欺防止システムＦ２によれば、前記「ｈｔｔｐアクセス」リクエスト有無チェック工程Ｓ２１のチェック結果「ＮＯ」の場合に、リクエスト待機可能に、「ｈｔｔｐアクセス」リクエスト有無チェックの前段へとフィードバックするリクエスト待機回路を形成するリクエスト待機回路形成工程を備えているので、次段に実施される「hostsファイル」内リクエストドメイン存在チェックの前提となる「ｈｏｓｔｓファイル」についてそのチェック漏れを皆無とすることができ、ファーミング詐欺を効果的に防止することができる。
なお、この「ｈｔｔｐアクセス」リクエスト有無チェック工程Ｓ２１のチェック結果「ＮＯ」の場合に、hostsファイルの設定でアクセスする（hostsファイル設定アクセス実施工程Ｓ２６）へと進められる（Ｓ２１２）。
また、「ｈｔｔｐアクセス」リクエストの有無がチェックＱＦ２１の結果「ＹＥＳ」と判定され、　「hostsファイル」中ドメイン存在チェックＱＦ２２、仕様設定適否チェックＱＦ２３のチェックの下に順次進めて、いずれのチェックにも「ＮＯ」と判定された場合であっても、hostsファイルの書き換え以外に、DNSサーバに存在するドメイン名とIPアドレス対応テーブルのIPアドレスを書き換えされる場合もあることから、ＤＮＳ情報チェック工程Ｓ２２２以下を追加実施し、警告・ブラックリスト登録・通知・強制終了工程Ｓ２２３を付加することによって、ブラックリストの登録・通知処理と併せて、正規の「hostsファイル」のアクセスを確実に実行し、ファーミング詐欺を効果的に防止することができる。
また、ＱＦ２５　「hostsファイル」使用可否チェックで、「ＮＯ」と判断したときでも、ブラックリスト登録・通知工程Ｓ２５１の処理を経て、ＤＮＳ情報チェック工程Ｓ２２２以下を追加実施するものであるから、警告・ブラックリスト登録・通知・強制終了工程Ｓ２２３の付加処理による、ブラックリストの登録・通知処理と併せて、正規の「hostsファイル」のアクセスを確実に実行し、ファーミング詐欺を効果的に防止することができる。
【００２７】
なお、ファーミング詐欺には、hostsファイルの書き換え以外に、DNSサーバに存在するドメイン名とIPアドレス対応テーブルのIPアドレスを書き換えされる場合もあることは上述したとおりであり、本願ファーミング詐欺防止システムに係る発明は、上記のDNSサーバ書き換え詐欺を防止するために、Webアクセス時に以下機能を追加するものであり、以下、簡単に説明する。
Webアクセスにおいて、IPアドレスを参照する順番は、hostsファイル⇒DNS情報をドメイン名から参照する。
当該発明例として、先にhostsファイル書き換えの詐欺防止手段を記載したが、DNSサー

バ書き換え詐欺を防止するために、以下の手順でDNSサーバが書き換えられていないか、否かをチェックする。
チェック処理後において、DNSサーバからゲットされたIPアドレスが書き換えられたか、否かのチェックを行う。
先ず、ゲットされたDNS情報でのIPアドレスと該ドメイン名の一致キーにより当該発明が提供するドメイン情報を参照し、一致パターンがあるか、否か、あるいは、ドメイン名一致かつｉｐアドレス一致であるか否かによりチェックすればよい。　同一内容がドメイン情報に存在すれば書き換えられていないと判定し通常のアクセスを行う。
一致パターンがドメイン情報に存在しない場合は、ファーミング詐欺発生として警告メッセージを端末に表示し、書き換えられたIPアドレス（DNSサーバに存在する）を基にWeb検索を行い、当該ホーム頁を認証局のブラックリストに登録する。同時にファーミング詐欺の発生を真正な登録企業に通知する。ＤＮＳサーバの書換えやなりすましにおいては、ドメイン名が存在するが、ｉｐアドレスが一致しない。なぜなら、詐欺サイトへの誘導は、ｉｐアドレスを替えることで可能となるからである。したがって、この不一致を発見すれば、ファーミングは防止できる。
警告メッセージとして、画面に表示するときは、例えば「ファーミング詐欺が発生しています。直ちにアクセスを中断してください」等文字表示する。或いは、音声対応端末であれば、同様なことばを発生させても良い。表示・音声の併用も可能である。
これにより、現在米国を中心に多発しているファーミング詐欺における、現時点での手口を包含でき、詐欺を撲滅できる。
本発明の特徴は、厳正な本人確認を行った上で、真正な登録企業のドメイン名とIPアドレスを対でドメイン情報として登録していることである。　従って、昨今、一部開発提供されているhostsファイルを無視しDNS情報を優先してアクセスさせることでファーミング詐欺を防止するソフトウェアーでは不可能であった本格的なファーミング詐欺に対しても極めて有効に防止できる画期的発明を提供することができる。

【図面の簡単な説明】
【００２８】
【図１】本願発明第１実施例に係るファーミング詐欺防止システムＦ１のフロー図である。
【図２】本願発明第２実施例に係るファーミング詐欺防止システムＦ２のフロー図である。
【符号の説明】
【００２９】
Ｆ１，Ｆ２　ファーミング詐欺防止システム
ＱＦ１１　「hostsファイル」書換え有無チェック
ＱＦ１２　プログラムウィルス汚染チェック
ＱＦ２１　「ｈｔｔｐアクセス」リクエストの有無がチェック
ＱＦ２２　「hostsファイル」中ドメイン存在チェック
ＱＦ２３　使用設定適否チェック
ＱＦ２４　ドメイン名符合チェック
ＱＦ２５　「hostsファイル」使用可否チェック
ＱＦ２６　ＤＮＳ情報チェック

Ｓ１０　システムＦ１始動点
Ｓ１１　バックアップ用「hostsファイル」複製工程
Ｓ１２　「hostsファイル」書換え有無チェック工程
Ｓ１２１　常駐監視工程Ｓ１２１
Ｓ１３　プログラムウィルス汚染チェック工程
Ｓ１３１　ウィルス駆除工程

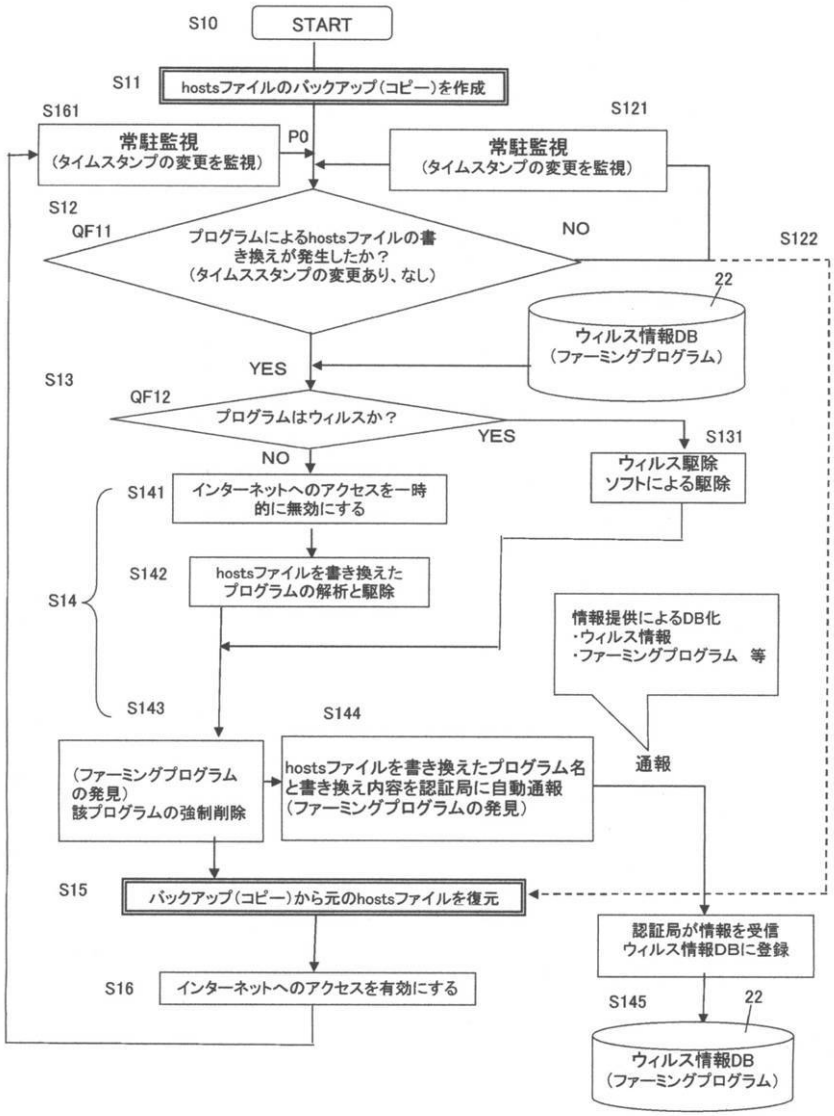
Ｓ１４　「解析発見書換えプログラムの名称・内容通報及び強制削除」工程
Ｓ１４１　インターネットへのアクセス一時的無効処理
Ｓ１４２　「hostsファイル」書換えプログラムの解析・駆除処理
Ｓ１４３　ファーミングプログラム強制削除処理
Ｓ１４４　自動通報工程
Ｓ１４５　認証局ウィルス情報DB化工程
Ｓ１５　「hostsファイル」復元工程

Ｓ２０　システムＦ２始動点
Ｓ２１　「ｈｔｔｐアクセス」リクエスト有無チェック工程
Ｓ２１１　リクエスト待機回路形成工程
Ｓ２２　「hostsファイル」内ドメイン存在チェック工程
Ｓ２２１　ＤＮＳ情報確保工程
Ｓ２２２　ＤＮＳ情報チェック工程
Ｓ２２３　警告・ブラックリスト登録・通知・強制終了工程
Ｓ２２３１　警告メッセージの表示
Ｓ２２３２　書き換えられたＩＰアドレスに基づくホーム頁をブラックリストの登録
Ｓ２２３３　真正登録企業にファーミング詐欺発生とブラックリストの通知
Ｓ２２３４　強制終了
Ｓ２２４　通常アクセス工程
Ｓ２３　「hostsファイル」仕様条件チェック工程
Ｓ２４　ドメイン名符合チェック工程
Ｓ２４１　警告表示工程
Ｓ２５　hostsファイル使用要否ユーザ判断チェック工程
Ｓ２５１　ブラックリスト登録・通知工程
Ｓ２５１　書き換えられたＩＰアドレスに基づくホーム頁をブラックリストの登録
Ｓ２５２　真正登録企業にファーミング詐欺発生とブラックリストの通知
Ｓ２６　hostsファイル設定アクセス実施工程
Ｓ２６１　常駐監視工程
２２　ウィルス情報ＤＢ

【図１】

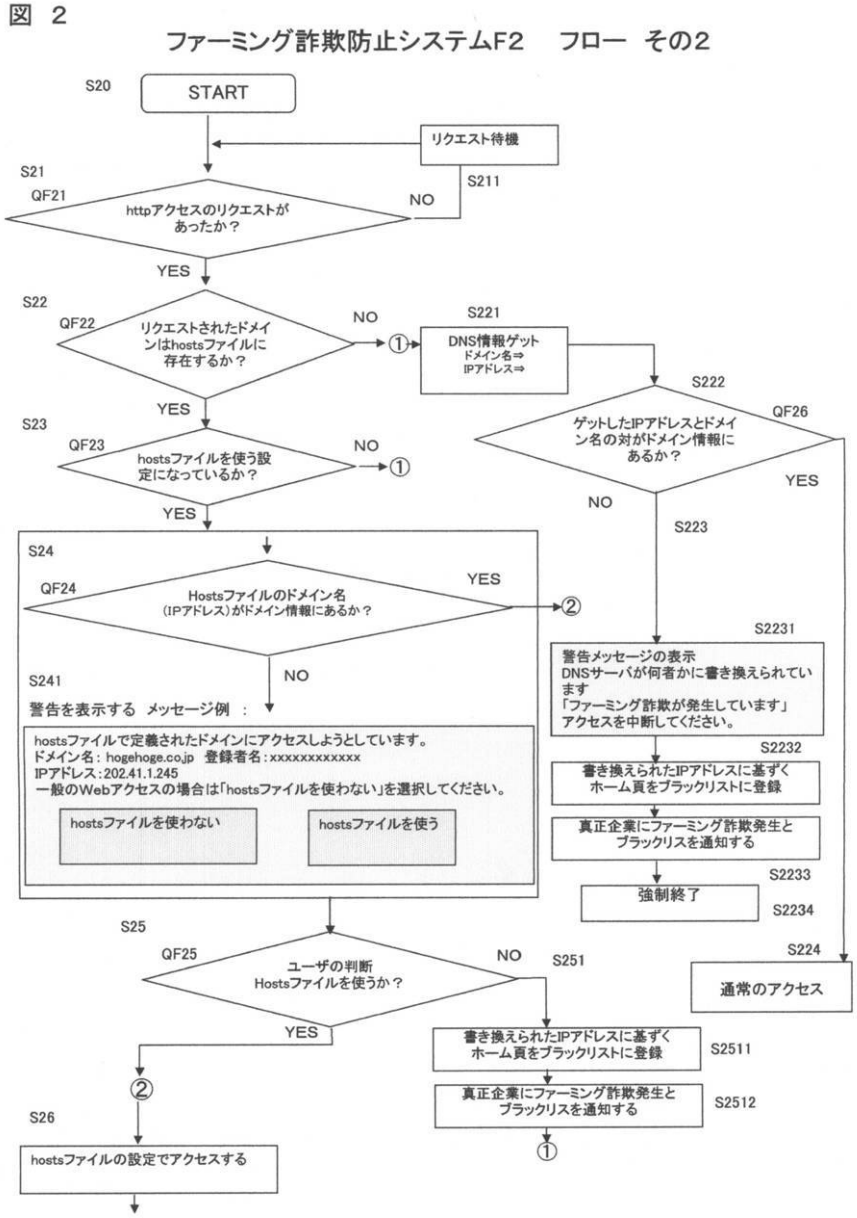
図 1

ファーミング詐欺防止システムF1　フローその1



【図２】

図 2


ファーミング詐欺防止システムF2　フロー その2
S20
START
リクエスト待機
S21
QF21
httpアクセスのリクエストがあったか？
NO
S211
YES
S22
QF22
リクエストされたドメインはhostsファイルに存在するか？
NO
①
S221
DNS情報ゲット
ドメイン名⇒
IPアドレス⇒
YES
S23
QF23
hostsファイルを使う設定になっているか？
NO
①
YES
S222
QF26
ゲットしたIPアドレスとドメイン名の対がドメイン情報にあるか？
YES
NO
S223
S24
QF24
Hostsファイルのドメイン名（IPアドレス）がドメイン情報にあるか？
YES
②
NO
S241
警告を表示する メッセージ例 ：
hostsファイルで定義されたドメインにアクセスしようとしています。
ドメイン名：hogehoge.co.jp 登録者名：xxxxxxxxxxx
IPアドレス：202.41.1.245
一般のWebアクセスの場合は「hostsファイルを使わない」を選択してください。
hostsファイルを使わない
hostsファイルを使う
S2231
警告メッセージの表示
DNSサーバが何者かに書き換えられています
「ファーミング詐欺が発生しています」
アクセスを中断してください。
S2232
書き換えられたIPアドレスに基ずくホーム頁をブラックリストに登録
真正企業にファーミング詐欺発生とブラックリスを通知する
S2233
強制終了
S2234
S25
QF25
ユーザの判断
Hostsファイルを使うか？
NO
S251
YES
S224
通常のアクセス
書き換えられたIPアドレスに基ずくホーム頁をブラックリストに登録
S2511
真正企業にファーミング詐欺発生とブラックリスを通知する
S2512
①
②
S26
hostsファイルの設定でアクセスする

フロントページの続き

(56)参考文献 特開２００２－２０７６２３（ＪＰ，Ａ）
特開２００３－２３３５０４（ＪＰ，Ａ）
特開２００３－２４８５９６（ＪＰ，Ａ）
特開２００３－０５０７３２（ＪＰ，Ａ）
渡辺 弘美，「ファーミングを中心とした悪意ある行為」，[online]，日本，社団法人コンピュータソフトウェア協会，２００５年 ６月１３日，p.1-p.21，[retrieved on 2008.06.04] Retrieved from the Internet，ＵＲＬ，http://www.csaj.jp/info/05/20050613_2_us_it_softmarket.pdf

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２２
Ｇ０６Ｆ ２１／２４