(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3573718号
(P3573718)
(45)発行日　平成16年10月6日(2004.10.6)　(24)登録日　平成16年7月9日(2004.7.9)

(51)Int.Cl.[7]　F I
G06F 12/14　G06F 12/14　560C
G06F 15/00　G06F 15/00　330Z
G06F 17/60　G06F 17/60　142
G06F 17/60　150
G06F 17/60　504

請求項の数 2　(全 13 頁)　最終頁に続く

(21)出願番号　特願2001-17563(P2001-17563)
(22)出願日　平成13年1月25日(2001.1.25)
(65)公開番号　特開2002-222286(P2002-222286A)
(43)公開日　平成14年8月9日(2002.8.9)
審査請求日　平成13年1月25日(2001.1.25)

(73)特許権者　501032951
株式会社クローバー・ネットワーク・コム
東京都新宿区市谷田町２－３１－３　ユービー市ヶ谷ビル３階
(74)代理人　100107777
弁理士　高橋　和夫
(72)発明者　長嶋　克佳
神奈川県相模原市新磯野３－４－７

審査官　高橋　克

最終頁に続く

(54)【発明の名称】不正使用防止機能付きホームページサーバ装置及びプログラム

(57)【特許請求の範囲】
【請求項１】
ホームページ情報に埋め込まれる不正使用防止機能プログラムであって、
前記不正使用防止機能プログラムは、第１及び第２の協調プログラムからなり、
前記第２の協調プログラムは、
端末を、
前記ホームページ情報を前記端末で編集する際に、前記ホームページ情報から前記第１の協調プログラムが削除されたことを検知し、ホームページの不正使用と判定する判定手段と、
インターネットに接続された段階で前記不正使用の判定結果をホームページ関連情報と共に配信する報知手段、
として機能させるものであること、
を特徴とする不正使用防止機能プログラム。
【請求項２】
前記第２の協調プログラムは、
前記端末を、
前記不正使用の判定に基づいて、閲覧者側の画面上に警告情報を報知させる報知手段として機能させるものであること、
を特徴とする請求項１に記載の不正使用防止機能プログラム。
【発明の詳細な説明】

【０００１】
【発明の属する技術分野】
本発明は、インターネットを介して得られる商取引情報や製品情報の不正使用を防止するホームページサーバ装置に関するものである。より詳しくは、インターネット商取引や製品情報の提供中に使用される企業名並びに商品名を勝手に第三者がなりすまして使用する不正使用を防止するものである。さらに、インターネットを介して受信した情報に基づいて、電話帳データ、地図データ、登記簿情報、ＮＴＴ登録情報、インターネットのＵＲＬ、商標などの現在登記や登録された信用のある確認情報と比較し、当該受信した情報の真偽を判定するホームページサーバ装置に係るものである。
【０００２】
さらにまた、本発明は、インターネットを利用した商取引若しくは収集した情報の提供者又は提供物のなりすましを事前に検証し、その真偽の白黒を判定する装置に関し、その検証結果を所定のサーバ装置内に記憶させると共に、記憶した登記簿情報や登録商標などの公認データを一般利用者若しくは所轄機関に提供する装置に係るものである。また、本発明は、収集した情報や商取引におけるなりすまし行為を検証した上でその真偽を白黒判定してから、その白黒判定結果を不正使用された被害者、言い換えれば真のホームページ所有者宛てに自動的に配信することにより、インターネットを利用した情報収集の精度を高め、さらにはインターネット社会における電子商取引の安全性を担保する技術に係るものである。
【０００３】
【従来の技術】
一般に、新規の商取引を開始する場合、相手側の信用情報を得る方法には信用調査会社に依頼して調査報告をさせて、自らその信用状態を判断する方法がある。この場合、商取引を開始する者が調査期間と費用を負担しなければならなかった。近年のインターネットを利用した電子商取引においては、企業の信用調査の重要性が一般の商取引に比してさらに高まり、取引の迅速性が求められている状態にある。また、信用情報の信憑性についても即座に判断しなければならない。さらに、インターネットの電子商取引の普及を拡大させるためには、「なりすまし」ウェブサイトのようなホームページの不正使用を未然に排除する必要がある。
【０００４】
図１は、従来の違反ホームページ摘発システムの構成図である。図１は、西暦２００１年１月６日の朝日新聞・朝刊に掲載された内容である。記事には、違法業者摘発にメールを活用することが記述され、政府側の公正取引委員会は来年度から消費者からの協力を得て、独占禁止法や景品表示法の違反事件を効率よく摘発するため、インターネットを活用した調査体制の強化に乗り出す。これまで「申告」と呼ばれる被害企業や消費者の通報などの情報提供が調査の発端となる場合が多かったが、情報を電子メールで入手するインフラを整備、消費者から「調査員」を募り、ネット上の悪質な虚偽広告なども摘発する考えで、公取委は「情報技術（ＩＴ）を駆使して複雑化する違反事件に対処したい」と話している、と紹介されている。
【０００５】
【発明が解決しようとする課題】
しかしながら、前述の如く、調査会社や電子メールを活用する対処方法では、所詮人手による作業が不可欠であり、調査時間を多く費やし且つ費用も膨大である。
【０００６】
本発明は、斯かる実情に鑑み、ウェッブサイトのホームページ情報の真偽を検証するための基礎資料を所轄機関並びに情報の管理運営している企業から入手してから、所定のデータを単一のサーバ装置に集約して蓄積することにより、蓄積データや資料に基づきインターネット上の電子商取引に係る提供者と提供物若しくは提供役務の真偽を正確且つ迅速に行えるシステムを提供しようとするものである。
【０００７】

【課題を解決するための手段】
本発明の一態様は、ホームページ情報に埋め込まれる不正使用防止機能プログラムであって、不正使用防止機能プログラムは、第１及び第２の協調プログラムからなり、第２の協調プログラムは、端末を、ホームページ情報を端末で編集する際に、ホームページ情報から第１の協調プログラムが削除されたことを検知し、ホームページの不正使用と判定する判定手段と、インターネットに接続された段階で不正使用の判定結果をホームページ関連情報と共に配信する報知手段、として機能させるものであること要旨とするものである。
【００１８】
【発明の実施の形態】
図２から図１５は本発明を実施する形態の一例であって、図中、図２と同一の符号を付した部分は同一物を表わしており、本図示例の特徴とするところは、図３に示す如く、ジャバアプレット（ＪａｖａＡｐｐｌｅｔ）を「なりすまし」ウエッブサイト（ＷｅｂＳｉｔｅ）に接続している端末で起動した際に自動的に真のウエッブサイト所有者のメールサーバに対してなりすまし発生を電子メールで通報するようにした点にある。
【００１９】
次に、上記図示例の作動を説明する。
【００２０】
図２は、本発明を例示したなりすましホームページチェックシステムのブロック図である。ユーザー端末１は、中央処理センター２との間でファックス又はインターネット網９を介して接続されている。また中央処理センター２も複数の情報提供サーバ７とインターネット網９を介して接続されている。この場合ユーザー端末はダイアルアップ接続でも良く、Ｔ２程度の回線速度でルータを介してインターネット網９に接続しても良く、複数のユーザー端末を代表して図示しているものである。これによって、ユーザ端末１、中央処理センター２及び情報提供サーバ７との間では相互にデジタル情報が送受信することができる。この場合、ユーザ端末１は情報提供サーバ７からの情報を送受信し必要な情報の検索及び紹介をすることができる。本発明の一実施態様ではＴＣＰ／ＩＰプロトコルを使用したインターネット技術を使用したが、これに拘わらずインターネット接続できるプロトコルであれば他の仕様を妨げるものではない。
【００２１】
図２の中央処理センター２のサーバ５は、サーバ内に記録したホームページをインターネット９へ送信するホームページサーバ装置を内在するものである。またホームページサーバ装置の他に収集した登記済白黒ファイル５ａ、５ｂ、ＪＰＮＩＣのようなＵＲＬ登録機関６、電話帳データ▲１▼等の存在確認情報５ｆおよび危険用語辞典５ｃ、金融用語辞典５ｂをも備えると共にこれらを記録し管理制御する中央処理装置４をも備えている。ここで中央処理装置４は、収集ホームページ合成処理手段４ａ、既存登録白・黒ファイルチェック処理手段４ｂ、依頼者ドメイン名チェック処理手段４ｃ、ＪＰＮＩＣ等機関情報チェック処理手段４ｄおよびチェック済情報報告処理手段４ｅを備えており、このシステムによって種々の「なりすまし」チェック方法を次の手順で実行することができる。
【００２２】
本発明の方法を例示すると、図２に示すインターネット９に接続するユーザ端末１において、先ず複数のウエッブサイトのホームページ情報を検索し収集する収集手段となる検索エンジン、例えばマイクロソフト社製のインターネットエクスプロラやネットスケープ社のネットスケープブラウザなどの一般にブラウザと称するソフトウエアを使用することができる。この収集手段からインターネット上のＹＡＨＯＯ、ＭＳＮ、ｉｎｆｏｓｅｅｋ，ｇｏｏ、Ｅｘｃｉｔｅなどで取引先相手の企業名若しくは商品名を画面上のキーワードボックスに入力することができる。次にサーバ５が検索結果を受信すると、中央処理装置４に接続された収集ＨＰ合成処理手段４ａは、検索したホームページをサーバ５内に収集することができる。また該当する企業名若しくは商品名で検索したホームページを各ドメイン名を使用して並べ換えるソート処理を実行することができる。さらにソート処理したホームページ情報の中で内容が重複するファイルを排除し単独にするよう整理合成した合成

ファイルを作成する処理を実行することができる。

【００２３】

本発明の実施態様では、初期状態のなりすましＨＰチェックシステムは、白黒データを蓄積していないので、依頼者のドメイン名と検索し収集したホームページ情報とを比較し両者が一致するか否かを判断する処理を実行する。この場合、上述した合成ファイルのデータのチェックは、省略されるが「なりすまし」ウエッブサイトを発見するという効果に何ら影響するものではない。つまり、２回目以降の処理では少なくとも初回に作成した「白黒判定ファイル」を利用することができるので、これまで蓄積した「登録済の白黒判定ファイル」のデータのドメイン名と一致するか否かを判定することができる。この合成ファイル内の情報は、依頼者ドメイン名チェック処理手段４ｃによって合成したホームページの各ドメイン名と依頼者ドメイン名とを比較し両者が一致するか否かを判断させるために使用することができる。この場合、依頼者ドメイン名と一致する合成ファイル内のホームページ情報は「白」と判定され正規の使用状態に在るウエッブサイトである。そしてこのホームページ情報は白ファイル５ａに登録し記憶することができる。白ファイル５ａは磁気ディスク装置でも光ディスク装置でもデジタル情報が記録再生できる手段であれば他の同等の装置を使用することができるのは言うまでもない。また依頼者ドメイン名に一致しない合成ファイル内のホームページ情報は、次の処理に分岐することができるが、ここでは白黒がはっきりしない未決の情報としてセンターサーバ６内のホームページサーバの記憶領域にデジタル情報として記憶することができる。なお、図示した白ファイル５ａと黒ファイル５ｂ並びに図示しない未決ファイルは物理的に独立したディスク装置に記憶しても共用するディスク装置にパーテションを区切って記憶しても良く、また共用するディスク装置内部で各フォルダ名を使用して区別して記憶しても良いことは言うまでもない。

【００２４】

中央処理装置４は未決ファイルを次の処理で追加の白黒判定を実行することができる。即ち、ＪＰＮＩＣやＩＣＡＮＮなどのＵＲＬ登録機関６の登録内容の属性に一致するか否かをＪＰＮＩＣなどの機関情報チェック手段４ｄによって処理することができる。ＪＰＮＩＣなど登録内容一致性チェックの結果、ＪＰＮＩＣ等のＵＲＬ登録機関６の登録内容に属性が一致すると判定された未決ファイル内のホームページ情報は「白」と判定し、上述した白ファイル５ａに登録し記憶することができる。一方、当該登録機関の登録内容に属性が一致しない未決ファイル内のホームページ情報は、さらに電話帳データ▲１▼等の存在確認情報５ｆに従い自動判定処理手段４ｅによって比較検討され、「企業名が一致するか否か」、「ＵＲＬが分岐ＵＲＬか否か」、「企業属性のどこが存在確認情報と相違するか否か」という複数の検証を自動的に実行することができる。この処理結果のデータには、企業名と一致・相違判定情報に加えて、電話帳データ等による比較結果の存在確認ステータス、例えば企業名、電話番号、住所、代表者、その他の情報が追加記憶される。また、この自動処理は一般にノンクライアントプロシジャに属しオペレータの指示なしに実行することができるが、本発明の実施態様を例示すれば自動処理の他に「企業名が一致するか否か」、「ＵＲＬが分岐ＵＲＬか否か」、「企業属性のどこが存在確認情報と相違するか否か」という３つの検証をセンターサーバ５と対話形式でオペレータに指示させることもできる。そして、存在確認情報５ｆを例示すると、電話帳法人データ、▲２▼地図情報、▲３▼土地、建物、会社法人等の登記簿、▲４▼東西ＮＴＴデータベース、▲５▼企業情報、▲６▼特許庁データベースＩＰＬ内の商標やホームページ上の商標、▲７▼ＧＩＦファイル、▲８▼ＤｒＢｅｌｌファイル等が存在し、検証するチェック対象物３から目的とする企業名、商品名に係るより精度の高い情報を得るための基盤となる情報を単一のセンターサーバ５に集約して構築することができる。さらにまた、本発明の一実施態様では、ホームページ上に掲載された▲６▼商標について検索できる商標検索システムを具備しているので、ユーザは、各自ユーザ端末１からインターネットを介して検索結果の提供を享受することができる。

【００２５】

上述した自動判定処理は、依頼者ドメイン名一致性チェック及びＪＰＮＩＣ等登録内容一

致性チェックを処理してから登録された白ファイル５ａに対しても実行することができる。存在確認情報チェックによる自動判定処理の結果、自動判定が既済である場合に、中央処理センター１は、「判定；黒」で処理し、一連の「判定ステータス」、「判定期日」、「時間」、及び、「存在ステータス」が黒ファイル５ｂに登録され記憶することができる。また、ホームページチェック依頼者１０若しくは公正取引委員会や仲裁機関などの関係機関８のメールサーバに対して電子メールでこれら黒ファイルデータを自動的に送信することができる。

【００２６】

一方、自動判定で未済であったホームページ情報は、追加的にマニュアルによる目視検証で判定することもできる。目視検証で白判定されたウェッブサイトのホームページ情報は白ファイル５ａに登録し記憶することができる。一方、マニュアルで黒と判定されたウェッブサイトのホームページ情報は自動判定済の情報と同様に、黒ファイル５ｂに登録され記憶することができる。この場合黒判定の情報についても、チェック依頼者１若しくは関係機関８のメールサーバに対して自動的に電子メールを送信することができる。但し、本発明の実施態様の一部として電子メールを使用したが、チェック依頼者１や関係機関８が電子的なメールを嫌う場合、例えば、特許庁が行う電子送達システムより書留郵便やファクシミリで送達された方がプリントをする手間が省けるなどの理由で電子メールを使用しない依頼者も存在する。この場合、電子メールに代えてファクシミリ自動送信や郵政省のＥ－ＭＡＩＬ受付で郵便物を発送する手段に適宜変更しても本発明の効果に何ら影響しないことは言うまでもない。

【００２７】

本発明の実施態様で得られた白ファイル及び黒ファイルは、以後の処理において白黒ファイル、ドメイン名一致性チェックの基礎データとなる。

【００２８】

上記実施態様では、検索エンジンを使用して発見したウェッブサイトのドメイン名の整合性や商標の機能侵害の有無を基礎に、信用力の高い企業になりすましてホームページを開設している不正使用者を特定しているが、信用のただ乗り、商標のダイリュージョンを引き起こす不正使用者がなりすましを開始してから、本発明を実施するまでの間はなりすましホームページは野放し状態になり、電子商取引の安全を害する事となる。そこで発明者は第２の実施態様をここに開示する。つまり著名企業のホームページやポータルサイトのホームページのサーバ装置内に蓄積されたホームページ情報の中にこれら「なりすまし」などの不正使用を防止するプログラムを内在させることで、なりすましホームページが稼動した時点、つまりインタネットに接続された状態に達したときに、なりすまされた被害者に電子メールを用いて通報することができる。以下、本発明の実施の態様を詳述する。

【００２９】

図３は、本発明を例示した不正使用ウェッブサイトの通報システムの構成図である。図３には、業務上の信用を盗用されそうなＡ社のウェッブサイト２０と、なりすましホームページを企図する者が使用するパーソナルコンピュータ２２と、パーソナルコンピュータ２２にダウンロードしたＡ社のホームページ情報を保存してそのまま、若しくは改竄をしてパーソナルコンピュータ２２からＡ社のホームページ情報のアップロードを受ける「なりすまし」のＡ’社のウェッブサイトのホームページサーバ２４と、なりすまし被害の通報を受けるＡ社のウエッブサイトの管理者２６が示されている。

本発明のホームページサーバ装置を使用した場合、Ａ社のウェッブサイトを訪問したネットサーファは、ウエッブサイト２０のホームページ内に記憶したジャバアプレット（ＪａｖａＡｐｐｌｅｔ）によりネットサーファが使用するパーソナルコンピュータの画面上に「このサイトは正規のサイト」である旨の表示を見る事ができる。このため電子商取引の場面で偽者サイトと区別が容易につくため、ネットサーファは安心して希望の商品を取得することができる。

ＩＰアドレスはインターネット技術においてはホームページサーバ固有の識別符合として使用され、現時点では３２ビットのコードで全世界のサーバを識別することができる。

したがって、インターネットに接続するホームページサーバであるＡ社のウエッブサイト２０にも個別の識別番号が割り当てられている。サーバ内の中央処理装置４はこのホームページサーバ固有の識別符号、例えばＩＰアドレス若しくはサブネットマスクの一方若しくは両方をＡ社のウェッブサイト２０のサーバ内から読み出して、ホームページ情報記憶領域であるジャバアプレットを記憶するプログラム領域やホームページ情報を記憶するＨＴＭＬ言語を記述した領域に予め記憶したＩＰアドレス若しくはサブネットマスクの所定情報とを比較することができる。

そして、比較をするための中処理装置４が一致情報を出力したときはホームページの正規使用と判定することができる。一方、パーソナルコンピュータ２２で悪意ある改竄をしたＡ社のホームページ情報がＡ’社のウェッブサイト２４のホームページにアップロードされた場合は、端末としてのパーソナルコンピュータ２２上でジャバアプレットを起動してウエッブサイト２４のサーバ内からＩＰアドレス若しくはサブネットマスクのコードを読み出して、ホームページ情報記憶領域であるジャバアプレットを記憶するプログラム領域やホームページ情報を記憶するＨＴＭＬ言語を記述した領域に予め記憶したＩＰアドレス若しくはサブネットマスクの所定情報とを比較することができる。

パーソナルコンピュータ２２は、ジャバアプレットを起動して正規のＩＰアドレス若しくはサブネットマスクと異なる場所のウェッブサイトで処理を実行している事実をこの比較結果が不一致情報を出力していることで認識することができる。

このようにパーソナルコンピュータ２２は、ジャバアプレットを用いてホームページの不正使用と判定したときは、Ａ’社のウェッブサイト２４のホームページサーバがインターネットへ接続された段階で不正使用の判定結果を不正使用されたホームページ関連情報、例えばＩＰアドレスやサブネットマスクやドメイン名等と共に正規のホームページ所有者であるＡ社のウェッブサイトの管理者２６へ電子メールを使用して自動的に配信することができる。

この自動報知手段は、一般に使用されるハイパーリンク技術を使用しても、独自のメーリングシステムをも使用することができる。また、本実施の形態では電子メールを使用したがＡ社のウェッブサイトの管理者に不正使用の事実を通報する手段であれば上述したファクシミリ転送や電子メールオーダによる郵便システムを使用することができるのは言うまでもない。

さらに、ジャバアプレットは不正使用と判定したときはＡ’社のウェッブサイトのホームページ上に「このサイトは不正使用です」などの警報を表示させることもできる。したがって、ネットサーファが検索エンジンを利用してアクセスした「なりすまし」サイトであるＡ’社のウェッブサイト２４が偽物であるということが一見して判断するとができ、電子商取引の安全を担保することができる。但し、悪意ある改竄者は改竄した情報がＡ’社のウェッブサイト２４で意図しているように表示されているか確認するために、ウェッブサイト２４にアクセスしてホームページの表示状態を確認するであろうから、本発明で例示した「このサイトは不正使用です」などの警報を表示させずに上述した電子メール等を利用した自動報知手段のみを使用することもできる。

通報を受けたＡ社のウェッブサイトの管理者２６は直ちにＡ’社のウェッブサイト２４のホームページにアクセスして「なりすまし」の状態を確認することができる。この場合、一般になりすましホームページには悪意ある改竄者にコンタクトする電子メールアドレスが表示され若しくはハイパーリンクしているので、そのアドレスに警告状を送信することもできる。

本実施態様では、自動報知手段が管理者２６へ通報したが、電子商取引の他に絵画や美術品や文章などの著作物を表現しているホームページの場合には、著作権者に直接自動報知手段から電子メールを送信することができる。さらにまた、公正取引委員会などの公的機関のメールサーバに対しても自動通報できることも言うまでもない。

【００３０】

図４は、本発明を例示したソフトウエアの動作説明ブロック図である。図４上部には、Ａ社が作成中のホームページ３０と既に使用中の完成しているホームページ３２を例示して

いる。図４下部には、この例示したホームページ３０，３２をＷＷＷサーバ３４のホームページサーバに格納した状態を示している。このホームページ３６には４個のエージェント、即ちジャバアプレットが埋め込むように記憶することができ、ホームページは全世界にネットで公開３８される。本発明を例示する第１の協調プログラムをＡ、第２の協調プログラムをＢで説明する。これら協調プログラムは上述した比較手段の比較結果を正規の信号から不正使用の信号に変化させることができる。また、少なくとも２個のエージェントを埋め込むことにより、悪意ある改竄者が不正使用防止機能プログラムを発見してＡのエージェントを削除した場合に有効である。即ち、Ｂのエージェントがそのまま Ａ‘社のウェッブサイトのホームページ３６に発見されずに残っているため、ホームページサーバにアップロードした段階で第２の協調プログラムであるＢのエージェントがＡのエージェントを探索し始め、その結果Ａのエージェントが削除されたと判断した場合は、上述した判定手段の判定結果を正規から不正使用に変更することができる。このエージェント達はホームページ３６をダウンロードしたパーソナルコンピュータ２２に制限なくダウンロードされ該パーソナルコンピュータ２２に保存することができ、且つ当該パーソナルコンピュータ２２からホームページサーバへアップロードすることができるソフトウエアである。また、パーソナルコンピュータ２２は厳密な意味でホームページサーバとは若干相違するが、Ａ’社のウェッブサイト２４から見た場合ホームページ情報を配信するため技術的にはホームページサーバの機能を有する。この意味から、パーソナルコンピュータ２２がゲートウエイやプロキシサーバ等のイントラネット管理システムによってアクセスが制限されない限り、パーソナルコンピュータ２２は改竄した「なりすまし」ホームページ情報をインターネットに接続した段階でエージェントが機能して不正使用の事実を報知手段を通じてＡ社ウェッブ管理者２６へ通報することができる。なお、本実施の態様を第１の協調プログラムをＡのエージェント、第２の協調プログラムをＢのエージェントとして説明したが、この逆の構成としても本発明の効果には影響が無いことは言うまでも無い。

【００３１】

図５は、本発明を例示したソフトウエアの動作説明ブロック図である。ｗｗｗサーバ３４のホームページに記憶されたエージェントＡ，Ｂ，Ｃ，Ｘの関係は、相互にメッセージを交換しながらホームページのなりすましを探知することができる。悪意ある改竄者はなりすまし防止機能プログラムを発見し削除する可能性があるので、各エージェントは他のエージェントが削除さたか否かを定期的に判定するように動作している。図示したエージェントＸは他のエージェントＡ，Ｂ，Ｃが削除されていないことを確認した後に、ホームページ上にひまわり情報社の社名若しくは図形商標４０を表示するように条件付のジャバアプレット又はＧＩＦのエンコーダとして機能することができる。図６は、本発明を例示したソフトウエアの動作説明ブロック図である。悪意ある改竄者がエージェントＣを発見し削除した際の残存するエージェントの構成を示している。エージェントＸはＡのエージェントとＢのエージェントとメッセージを交換してはいるが探索の結果Ｃのエージェントとはメッセージの交換が不能である。エージェントＸはこれをＣのエージェントが削除されたと判定して上述したひまわり情報社の社名及びひまわり情報社の図形商標をホームページ上に表示することを禁止するこができる。図７は、本発明を例示したソフトウエアのブロック図である。エージェントＡ、Ｂ、Ｃ、及びＸが全てホームページ情報の中に記憶されていることがエージェント相互のメッセージ交換により確認されるため、全エージェントはキャリーに命令を送信しないのである。本実施の態様ではキャリーとはホームページを管理するオペレーティングシステムのスーパバイザなどが該当する。また、命令とは不正使用された事実を通報するコードである。このコードは、上述したジャバアプレットやＧＩＦのエンコードを禁止する情報である。図８は、本発明を例示したソフトウエアのブロック図である。Ｃのエージェントが悪意ある改竄者によって発見され削除されたためエージェントＡ、Ｂ、ＸはＣのエージェントとメッセージを交換することができない。したがって、残存するエージェントＡ、Ｂ、Ｘの３個のエージェント全てがキャリーに対してジャバアプレット若しくはＧＩＦのエンコードを規制する命令を送信することができる。図９は、本発明を例示したソフトウエアのブロック図である。エージェントＡ、Ｂ、Ｃ、

Ｘは現在保存されているホームページサーバのＩＰアドレス、例えばＩＰ１を定期的に参照し、初期にプログラムされた参照コードと一致するか否かを判断することができる。図示したＩＰ１は初期の参照コードと一致しているため、エージェントＡ、Ｂ、Ｃ及びＸはキャリーに禁止命令を送信しないので上述した社名や図形商標がホームページ上に表示することができる。一方、ホームページがコピーされて他のホームページサーバにアップロードされた場合の構成を図１０に示す。図１０は、本発明を例示したソフトウエアのブロック図である。この態様は不正使用中のなりすましサイト内の各エージェントの動作である。即ち、エージェントＡ、Ｂ、Ｃ、及び、Ｘは、なりすましサイトのホームページサーバのＩＰアドレスを参照してＩＰ２を取得することができる、初期にプログラムされた参照コードのＩＰアドレスはＩＰ１であるから、現在取得中のＩＰ２とは明らかに相違する。したがって、各エージェントＡ、Ｂ、Ｃ、及びＸはキャリーに対して規制命令を送信し、真性なる社名や図形商標の表示処理を規制することができる。図１１は、本発明を例示したソフトウエアのブロック図である。キャリー４２はエージェントから命令を受信すると現在の「年月日時分秒」、なりすましサイトの「ＩＰアドレス」、「ドメイン名」、エージェントの欠落かＩＰアドレスの変化か何れかの「事象内容」をＡ社のウェッブサイトの管理者２６へ電子メールを通じて自動的に通報することができる。本実施の態様ではＩＰアドレスはフルパスのＩＰアドレスでもグローバルアドレスでもサブネットマスクを含めても実施することができる。

【００３２】

図１２は、本発明を例示した警報フローのフローチャートである。図１２には、Ａ社に該当するひまわり情報のホームページの表示画面の一部に表示されたＧＩＦ画面４４がダウンロードされ、悪意ある改竄者又は転用者が加工したＧＩＦ画面４６が示されている。改竄者などは不正使用するホームページ情報を加工してからＦＴＰなどのファイル転送プログラムを使用してＡ‘社のホームページサーバ４８へアップロードした後に、善意のネットサーファがホームページサーバ４８にアクセスした場合、オリジナルのひまわり情報のＧＩＦ画像４４はホームページから欠落する欠落ＧＩＦ画像５０で表示されると共に、Ａ社のウェッブ管理者、例えば今井憲一郎が所有するパーソナルコンピュータ５２にメールサーバを介して警報メールを自動的に送信することができる。即ち、不正使用をする者が意図的にＡ社の商標をなりすましサイトに表示させたいと企図しても、本発明の実施態様ではオリジナル商標の表示を規制することができる。しかも善意のネットサーファに対しても商取引の安全を確保しつつ、なりすましサイトを放置させないように商標の所有者に対してなりすましサイトの出現を警告するため、早期に法的措置を執ることもできる、という電子商取引社会の正義と公平を担保することができる技術である。本実施の形態では各エージェントがメッセージを交換するように構成したが、本発明の構成要件の一部であるメッセージ交換に代えて次のエージェント構成でも発明の効果に影響するものではない。また、本実施態様では今井憲一郎のパーソナルコンピュータ５２に電子メールを送信したが、今井憲一郎が不在で通報を見られない場合もある。この場合、本発明の他の実施態様では、今井健一郎のメールサーバが通報電子メールの着信後に所定時間内、例えば、１分乃至１０分以内に着信した電子メールを解析し通報情報に基づき不正使用中のホームページに自動的にアクセスする自動立入手段を設けることができる。この自動立入手段によって取得したなりすましサイトのホームページ情報を再編集不能なファイル、例えばＡｃｒｏｂａｔＲｅａｄｅｒで表示するような書き換え規制のできるファイルに変換し、または編集するとファイル自体が自己破壊するようなファイルに変換してから、この変換ファイルをデジタル情報で磁気ディスク若しくは書き換え不能の光ディスクなどの媒体に固定記録することができる。この媒体に固定記憶された情報は将来裁判の書証として活用することも期待できるし、少なくとも悪意のある改竄者に対して交渉材料とすることができる。なお、本実施態様では、メールサーバはなりすましサイトのホームページサーバに立ち入ることを意図しているため不正使用防止機能付きホームページサーバ装置の範疇に含む意味で使用している。

【００３３】

図１３は、本発明を例示したサーバ装置のブロック図である。ＷＷＷサーバ６０は、不正使用禁止機能プログラムであるジャバアプレット６２、６４、６６、６８を有する。このジャバアプレットはネットサーファがアクセスした際に閲覧者側のパーソナルコンピュータにダウンロードされ、相互にメッセージを交換し合う機能を有している。これらジャバアプレットはサーバ６０内に記憶したＨＴＭＬ言語で記述されたホームページ情報７０、例えば、外部からインターネットでアクセス許可された領域に記憶した“ｉｎｄｅｘ．ｈｔｍｌ”などの所定のファイルネームを持つファイル７２の内部で定義するアプレットの使用定義体によって起動が制御することができるものである。図１４は、本発明を例示したソフトウエアのフローチャートである。図１４のフローは、インターネットからアクセスされホームページが閲覧された時からプログラムの起動が開始されるステップ８０と、代表アプレットは他の定義体が欠けていないか監視するステップ８２と、他の定義体が欠落しているときはステップ８４へ分岐してホームページサーバ６０のＩＰアドレスとドメイン名を取得しつつ、このＩＰアドレス及びドメイン名を情報としてコモン・ゲートウエイ・インターフェースＣＧＩを起動させ処理を終了させるステップ８６と、他の定義体が欠落していない場合はステップ８２からステップ８８へ分岐し各アプレットが現在保存されているサーバ６６のＩＰアドレスを取得してプログラムされたコードと比較し検証するステップ８８と、このＩＰアドレスがコードと一致したときに分岐するステップ９０と各アプレットが監視処理を定期的に継続するステップ９１と、ＩＰアドレスが不一致の場合にステップ８８からステップ９２へ分岐し、図示していないがサーバ６０のＩＰアドレス及びドメイン名を取得してから、これら情報を外部に伝達するＣＧＩを起動するステップ９４と、処理を終了するステップ９６とを有している。さらに、ステップ８６、９６からターミネートした処理はＣＧＩを使用して電子メールを送信するステップ９８へ移行し、取得した不正使用者のホームページのＩＰアドレス及びドメイン名を真のオナーであるＡ社のウェッブ管理者２６のメールサーバへ着信するステップ１００をも具備しているものである。本発明の実施形態によれば真のオーナのウェッブサイト２０のホームページサーバから社名やＧＩＦ画像の商標をダウンロードするように構成したが、ネットサーファ側のパーソナルコンピュータの画面上でこれら社名と商標の表示を可能とする代わりにホームページの保存を規制するように構成しても良い。例えば、米国特許商標庁や日本国特許庁などのホームページの如く公知の構成を転用することもできる。

【００３４】

こうして、ジャバアプレット達は不正使用を防止するためにホームページサーバのＩＰアドレスを検証したり、他のジャバアプレットの欠落を監視して改竄やなりすましを検知するように構成したが、本発明を実施するためには他の実施態様を用いることもできる。即ち、ジャバアプレットはＨＴＬＭ言語で記述したホームページ情報の文字数がオリジナルと相違するか、またはＨＴＭＬ言語で記述した行を一行毎に解析してハッシュ関数を発生させオリジナルと相違するか否かを判定することもできる。さらにＨＴＭＬ言語の記述を一行毎に解析して文字数のサムチェックを実行することもでき、このようにオリジナルとの相違点を検知し不正使用を防止できる手段であれば他の手段に置き換えても本発明の効果に影響を与えるものではない。

【００３５】

図１５は、本発明を例示したシステムのブロック図である。ホームページサーバ１１０は、外部からインターネットを介してアクセスする領域１１２と、この領域１１２内でドメイン名とＩＰアドレスを取得し、タイマー機能を使用して定期的にホームページが改竄されていないか否かを検証するように構成されている。また、ホームページ情報の中には複数の協調プログラムを含むことができる。協調プログラム１１６は一般に善玉ウイルスと称し、ＧＩＦを使用してホームページのオーナの文字商標や図形商標などをホームページ上に表示させることができる。改竄されていないホームページであると善玉ウイルス１が判断した場合は、外部不進入領域１１４からＧＩＦ画像を読み出してデータの伸張処理を実行することができる。また、善玉ウイルス１が削除されていないか否かを善玉ウイルス２が定期的に監視することもできいる。本実施の態様により真のオーナのホームペ－ジサ

ーバ１１０に悪意のハッカーがハッキングをしてホームページを改竄し、猥褻な内容や誹謗中傷や虚偽表示などホームページを不正使用した場合に、直ちに真のオーナーに電子メールを使用して自動的にハッキングの事実を通報することができる。また、ホームページサーバ１１０にアクセスしているネットサーファーが閲覧中のホームページの内容を画面に表示させた状態でインターネット回線を切断してから、表示中のホームページの内容をパーソナルコンピュータに保存し改竄してなりすましサイトにアップロードにようとした時点でインターネットに接続されるため、改竄されたホームページ情報の中に含まれる善玉ウイルス１並びに善玉ウイルス２が協調プログラムとして機能するので真のオーナであるＡ社のウェッブ管理者に電子メール通報をすることができる。

【００３６】

尚、本発明のエージェトは、上述の図示例にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【００３７】

【発明の効果】

以上、説明したように本発明の請求項１から１１記載の不正使用防止機能付きホームページサーバ装置及びソフトウエアによれば、なりすましサイトの発生を未然に防止でき、また仮になりすましサイトが出現しても真のオーナに電子通報することができ、更にはなりすましサイトに自動的に立ち入って証拠を保全できるという優れた効果を奏し得る。

【図面の簡単な説明】

【図１】従来の違反ホームページサイト摘発システムの構成図である。

【図２】本発明を例示したなりすましホームページチェックシステムのブロック図である。

【図３】本発明を例示した不正使用ウエッブサイトの通報システムの構成図である。

【図４】本発明を例示したソフトウエアの動作説明ブロック図である。

【図５】本発明を例示したソフトウエアの動作説明ブロック図である。

【図６】本発明を例示したソフトウエアの動作説明ブロック図である。

【図７】本発明を例示したソフトウエアのブロック図である。

【図８】本発明を例示したソフトウエアのブロック図である。

【図９】本発明を例示したソフトウエアのブロック図である。

【図１０】本発明を例示したソフトウエアのブロック図である。

【図１１】本発明を例示したソフトウエアのブロック図である。

【図１２】本発明を例示した警報フローのフローチャートである。

【図１３】本発明を例示したサーバ装置のブロック図である。

【図１４】本発明を例示したソフトウエアのフローチャートである。

【図１５】本発明を例示したシステムのブロック図である。

【符号の説明】

１　ユーザ端末
２　中央処理センター
３　チェック対象物
４　中央処理装置
５　センター・サーバ
６　ＵＲＬ機関
７　情報提供サーバ
８　関係機関
９　インターネット
１０ホームページチェック依頼者
２０　Ａ社のウェッブサイト
２２　悪意ある改竄者のパーソナルコンピュータ
２４　Ａ’社のウェッブサイト
２６　Ａ社のウェッブ管理者

３０　作成中のホームページ
３２　完成しているホームページ
３４　ＷＷＷサーバ
３６　ホームページ
３８　ネットで公開
４０　図形商標
４２　キャリー
４４　正規の所有者のＧＩＦ画像
４６　改竄者のＧＩＦ画像
４８　ホームページサーバ
５０　欠落したＧＩＦ画像
５２　今井憲一郎が所有するパーソナルコンピュータ
６８　ジャバアプレット
７０　ホームページ
７２　ＨＴＭＬ言語の記述リスト
８０、８２、８４、８６、８８、９０、９１、９２、９４、９６、９８、１００プログラムのステップ
１１０　開設側サーバ
１１２　インターネットでアクセス可能なホームページ
１１４　外部不進入領域
１１６　協調プログラム

【図１】

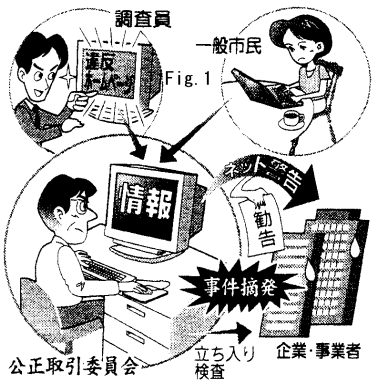

Fig. 1

【図２】

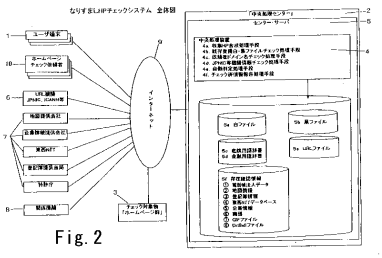
Fig. 2

【図３】

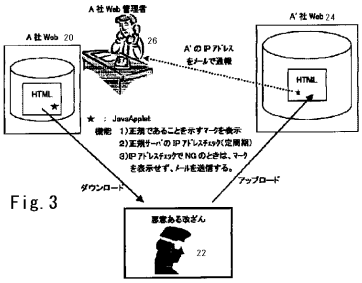

Fig. 3

【図４】

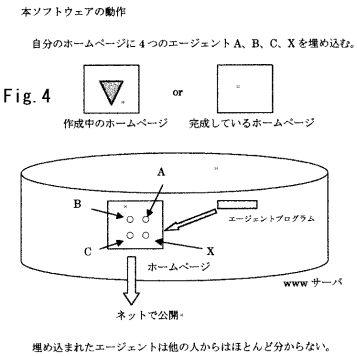

Fig. 4

【図５】

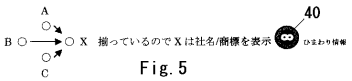

Fig. 5

【図６】

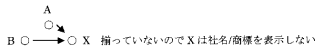


Fig. 6

【図７】

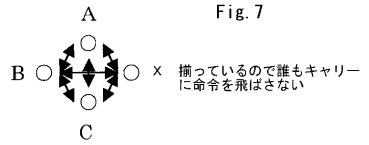


Fig. 7

【図８】

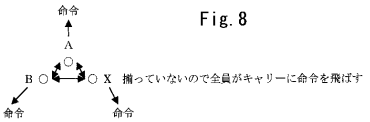


Fig. 8

【図９】

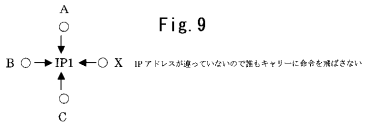


Fig. 9

【図１０】

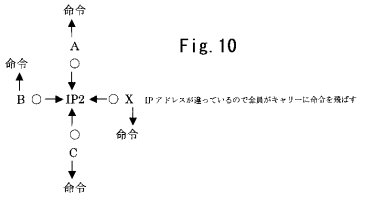


Fig. 10

【図１１】

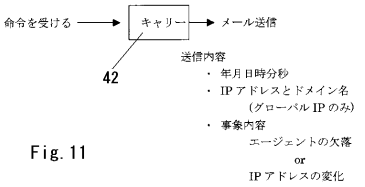


Fig. 11

【図１２】

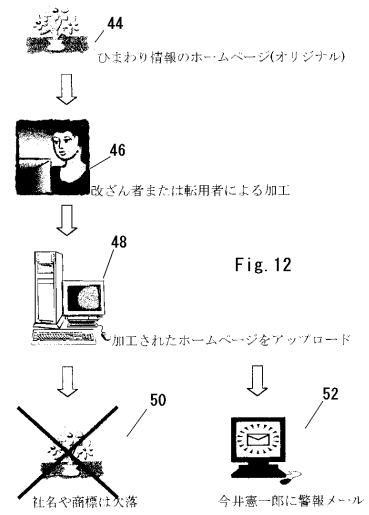


Fig. 12

【図１３】

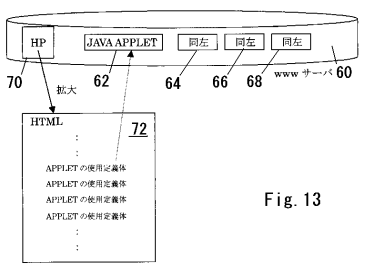


Fig. 13

【図１４】

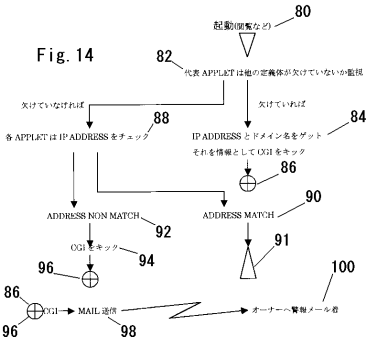


Fig. 14

【図１５】

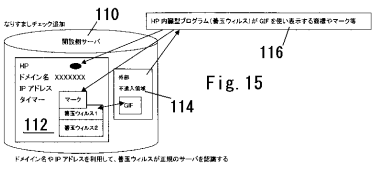


Fig. 15

フロントページの続き

(51)Int.Cl.[7]　　ＦＩ
　　Ｇ０６Ｆ　17/60　　ＺＥＣ

(56)参考文献　特開２０００－３３１０８８（ＪＰ，Ａ）
特開平１１－０３９２６３（ＪＰ，Ａ）
特開平１１－０６６００９（ＪＰ，Ａ）
特開２０００－３３０８７３（ＪＰ，Ａ）
洲崎 誠一，吉浦 裕，永井 康彦，豊島 久，佐々木 良一，手塚 悟，”Ｗｅｂサイトの真正性を確認可能とするインターネット・マークの提案”，情報処理学会論文誌，情報処理学会，２０００年　8月１５日，Vol.41，No.8，pp.2198-2207
伊原 秀明，"Tripwire for LINUX"，トリップワイヤ・ジャパン株式会社，２００１年　4月２０日，pp.1-5

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G06F 12/14
G06F 15/00　330
G06F 17/60　142
G06F 17/60　150
G06F 17/60　504
G06F 17/60　ZEC