(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-221242
(P2006-221242A)
(43)公開日　平成18年8月24日(2006.8.24)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/20	(2006.01)	G06F 15/00	330A	5B285

審査請求 未請求　請求項の数 5　ＯＬ　（全 17 頁）

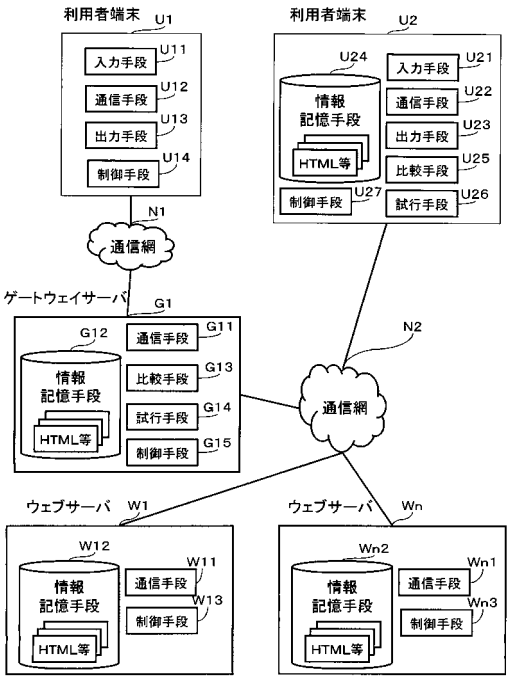
(21)出願番号　特願2005-31633(P2005-31633)
(22)出願日　平成17年2月8日(2005.2.8)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100108187
弁理士　横山　淳一
(72)発明者　捧　泰士
神奈川県横浜市神奈川区新子安一丁目２番４号　株式会社富士通アドバンストソリューションズ内
(72)発明者　林　省吾
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5B285 AA04　BA08　CA31　CB41　CB63
CB74　CB84　DA05

(54)【発明の名称】認証情報詐取防止システム、プログラム及び方法

(57)【要約】　（修正有）
【課題】接続時点で正規ウェブサイトへの接続か否かを判定し、認証情報の詐取を未然に防ぐことを可能とする認証情報詐取防止システム、プログラム及び方法を提供すること。
【解決手段】認証情報詐取防止システムが、ウェブページデータを処理する処理ステップと、前記処理ステップで処理したウェブページデータと、ＵＲＬと対応付けてウェブページデータを記憶するウェブページ記憶手段に記憶したウェブページデータとを比較する第１の比較ステップと、前記第１の比較ステップで比較した結果、類似するウェブページデータがあった場合に、該類似するウェブページデータ同士のＵＲＬが同一であるか比較する第２の比較ステップと、前記第２の比較ステップで比較した結果、ＵＲＬが異なる場合にアドレス注意メッセージを前記処理ステップで処理したウェブページデータに付加するアドレス注意メッセージ付加ステップを実行する。
【選択図】図１



【特許請求の範囲】
【請求項１】
認証情報詐取防止システムが、
　ウェブページデータを取得する取得ステップと、
　ウェブページ外見情報及び認証情報を対応付けて記憶する情報記憶手段に記憶したウェブページ外見情報と、前記取得手段で取得したウェブページデータの外見情報を比較する外見比較ステップと、
　前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する試行ステップと、
を実行することを特徴とする認証情報詐取防止方法。
【請求項２】
認証情報詐取防止システムが、
　利用者からのウェブページ取得要求に基づき、利用者の認証情報を関連付けて記憶する認証情報記憶手段を参照して、該ウェブページ取得要求に認証情報が含まれるか比較する認証比較ステップと、
　前記認証比較ステップで比較した結果、前記利用者からのウェブページ取得要求に認証情報が含まれる場合に、該利用者からのウェブページ取得要求に含まれる認証情報とは異なる試行情報を該利用者からのウェブページ取得要求に設定して出力する試行ステップと
を実行することを特徴とする認証情報詐取防止方法。
【請求項３】
認証情報詐取防止システムが、
　前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、前記取得ステップで取得したウェブページデータのアドレスと、前記情報記憶手段に該ウェブページ外見情報に対応付けて更に記憶されたアドレスとを比較するアドレス比較ステップを更に実行し、
　前記試行ステップは、前記前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合であって、且つ、前記アドレス比較ステップで比較した結果、アドレスが異なる場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する
　ことを特徴とする請求項１記載の認証情報詐取防止方法。
【請求項４】
認証情報詐取防止システムに、
　ウェブページデータを取得する取得ステップと、
　ウェブページ外見情報及び認証情報を対応付けて記憶する情報記憶手段に記憶したウェブページ外見情報と、前記取得手段で取得したウェブページデータの外見情報を比較する外見比較ステップと、
　前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する試行ステップと、
を実行させることを特徴とする認証情報詐取防止プログラム。
【請求項５】
認証情報詐取防止システムに、
　利用者からのウェブページ取得要求に基づき、利用者の認証情報を関連付けて記憶する認証情報記憶手段を参照して、該ウェブページ取得要求に認証情報が含まれるか比較する認証比較ステップと、
　前記認証比較ステップで比較した結果、前記利用者からのウェブページ取得要求に認証

情報が含まれる場合に、該利用者からのウェブページ取得要求に含まれる認証情報とは異なる試行情報を該利用者からのウェブページ取得要求に設定して出力する試行ステップとを実行させることを特徴とする認証情報詐取防止プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、フィッシングとして知られる金融機関等からの正規のメールやウェブサイトを装い、暗証番号やクレジットカード番号等の情報を盗み取る詐欺にかからないためのフィッシング防止方法及びプログラムに関する。
【背景技術】
【０００２】
近年、インターネットを経由したオンラインによる商取引が広く一般的に行われるようになってきたが、それに伴い、フィッシングと呼ばれる詐欺による被害も拡大してきている。
【０００３】
この、フィッシング詐欺とは、実在の銀行・クレジットカード会社やショッピングサイトなどを装ったメールを送付し、そこにリンクを貼り付けて、その銀行・ショッピングサイトにそっくりな「罠のサイト」に呼び込み、クレジットカード番号やパスワードなどを入力させてそれを入手してしまうという詐欺で、ジャバスクリプトを使ってＵＲＬを詐称したり、ポップアップウィンドウのアドレスバーを非表示にしたりする等の悪質な手口を利用しているため、正規サイトと錯誤して認証情報を「釣られる」被害者が後を絶たず、大きな問題となっている。
【０００４】
この問題に対し、特許文献１には、第三者機関で、各種検索サイト経由で収集したウェブページの内、ＵＲＬ登録機関や電話帳情報で登録内容の属性や存在確認情報が照会できたものを「白」として記憶しておき、チェック依頼者等からの依頼に基づき指定されたウェブページの白黒を判定したり、ジャバアプレットに、存在しているウェブページのＩＰアドレスを別途記載・記憶しておいたＩＰアドレスと比較させて異なる場合に正規のサーバで運用されていないとして利用者及び正規のウェブページの所有者に通知させたりすることが記載されている。
【特許文献１】特開２００２－２２２２８６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
この特許文献１に記載された技術では、第三者機関やページ上のアプレットによって、正規のウェブサイトであることをチェックするものであるが、ウェブページに記載したウェブサイトのＩＰアドレスや、ジャバアプレット自身が改竄されてしまっていた場合には、第三者機関に調査を依頼して回答を得るという処理を経なければ、正当なウェブページなのか否かを判断することはできない。
【０００６】
しかし、フィッシングは正規ウェブサイトへの接続であると誤認識させることによって認証情報を詐取するものであり、接続時点で正規ウェブサイトへの接続か否かを判定することができなければ、その被害を防ぐことはできず、問題であった。
【０００７】
本発明は上記の問題点に鑑みてなされたものであり、接続時点で正規ウェブサイトへの接続か否かを判定し、認証情報の詐取を未然に防ぐことを可能とする認証情報詐取防止方法及びプログラムを提供することを課題とする。

【課題を解決するための手段】
【０００８】
上述した課題を解決するために、本発明の請求項１にかかる認証情報詐取防止方法は、認証情報詐取防止システムが、ウェブページデータを取得する取得ステップと、前記取得手段で取得したウェブページデータと、ウェブページのアドレス情報、ウェブページ外見情報、認証情報を対応付けて記憶する情報記憶手段に記憶したウェブページ外見情報とを比較する比較ステップと、前記比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けられた認証情報を該認証情報とは異なる試行情報に変えて前記取得ステップで取得したウェブページデータに設定したウェブページ処理要求を出力する試行ステップと、を実行することを特徴とする。なお本願では、以降、ｈｔｔｐ，ｈｔｔｐｓなどで通信されるネットワーク上のデータ授受要求をウェブページ処理要求と表現する。
【発明の効果】
【０００９】
本発明によれば、予めウェブページ記憶手段に正しい接続先の認証に関するウェブページに関する情報を記憶しておき、ウェブページ取得時、取得したウェブページとウェブページ記憶手段に記憶したウェブページの見た目を比較し、相似するウェブページについて、認証情報を試行情報に置換してウェブページ処理要求を出力するので、利用者は接続時点で正規ウェブサイトに良く似た別のウェブページへの接続であることが判り、認証情報が詐取されるのを未然に防ぐことが可能となる。
【発明を実施するための最良の形態】
【００１０】
以下、本発明にかかる認証情報詐取防止システムの実施形態を図面に基づいて説明する。まず、図１に基づいて、実施形態の認証情報詐取防止システムの概要を説明する。図１は本発明にかかる認証情報詐取防止システムの概要構成を示すブロック図である。
【００１１】
図１で、利用者端末Ｕ１は、利用者が操作して情報を入力するキーボードやマウス等の入力手段Ｕ１１、イントラネット等の通信網Ｎ１を介して接続されるゲートウェイサーバＧ１及びインターネット等の通信網Ｎ２を介して接続される利用者端末Ｕ２やウェブサーバＷ１～Ｗｎとの間で情報の送受信を行う通信手段Ｕ１２、入力手段Ｕ１１で入力した情報や通信手段Ｕ１２で受信した情報を出力するディスプレイ等の出力手段Ｕ１３、及びこれら各手段を制御して利用者端末機能の提供を行う制御手段Ｕ１４の各手段を備えるコンピュータ、携帯電話、ＰＤＡ等の情報処理装置である。
【００１２】
ゲートウェイサーバＧ１は、通信網Ｎ１を介して接続される利用者端末Ｕ１及び通信網Ｎ２を介して接続される利用者端末Ｕ２やウェブサーバＷ１～Ｗｎとの間で情報の送受信を行う通信手段Ｇ１１、通信手段Ｕ１２で受信した情報等を記憶する情報記憶手段Ｇ１２、通信手段Ｇ１１で受信した情報と情報記憶手段Ｇ１２に記憶した情報とを比較する比較手段Ｇ１３、通信手段Ｇ１１で受信した情報が所定の条件に合致する場合に異なる送信情報を生成する試行手段Ｇ１４、及びこれら各手段を制御してゲートウェイサービスの提供を行う制御手段Ｇ１５の各手段を備えるコンピュータ等の情報処理装置である。情報記憶手段Ｇ１２に記憶する情報については後述する。
【００１３】
利用者端末Ｕ２は、上述した利用者端末Ｕ１及びゲートウェイサーバＧ１の各手段を備えたものであって、利用者が操作して情報を入力するキーボードやマウス等の入力手段Ｕ２１、通信網Ｎ２を介して接続されるゲートウェイサーバＧ１及びウェブサーバＷ１～Ｗｎとの間で情報の送受信を行う通信手段Ｕ２２、入力手段Ｕ２１で入力した情報や通信手段Ｕ２２で受信した情報を出力するディスプレイ等の出力手段Ｕ２３、利用者が入力手段Ｕ２１で入力した情報や通信手段Ｕ２２で受信した情報等を記憶する情報記憶手段Ｕ２４、入力手段Ｕ２１で入力した入力情報や通信手段Ｕ２２で受信した情報と情報記憶手段Ｕ

２４に記憶した情報とを比較する比較手段Ｕ２５、入力手段Ｕ２１で入力した情報が所定の条件に合致する場合に異なる情報を生成する試行手段Ｕ２６、及びこれら各手段を制御して利用者端末機能の提供を行う制御手段Ｕ２７の各手段の各手段を備えるコンピュータ、携帯電話、ＰＤＡ等の情報処理装置である。情報記憶手段Ｕ２４に記憶する情報については後述する。

【００１４】

ウェブサーバＷ１～Ｗｎは、それぞれ、通信網Ｎ２を介して接続される利用者端末Ｕ２、ゲートウェイサーバＧ１及び更に通信網Ｎ１を介して接続される利用者端末Ｕ１と情報の送受信を行う通信手段Ｗ１１～Ｗｎ１、通信手段Ｗ１１～Ｗｎ１で受信した情報を記憶する情報記憶手段Ｗ１２～Ｗｎ２、及びこれら手段を制御してウェブサービスの提供を行う制御手段Ｗ１３～Ｗｎ３の各手段を備えるコンピュータ等の情報処理装置である。

【００１５】

通信網Ｎ１は、利用者端末Ｕ１とゲートウェイサーバＧ１との間におけるデータ送受信を仲介するイントラネット等の通信網であって、有線及び無線による接続形態を取ることができる。

【００１６】

通信網Ｎ２は、利用者端末Ｕ２、ゲートウェイサーバＧ１及びウェブサーバＷ１～Ｗｎの間におけるデータ送受信を仲介するインターネット等の通信網であって、有線及び無線による接続形態を取ることができる。

【００１７】

図２は、ゲートウェイサーバＧ１の情報記憶手段Ｇ１２（または利用者端末Ｕ２の情報記憶手段Ｕ２４）に記憶する認証情報テーブルＧ１２１（Ｕ２４１）の例を示す。この認証情報テーブルＧ１２１（Ｕ２４１）は、利用者端末Ｕ１（またはＵ２）からの入力・登録指示に基づき、利用者単位に入力対象となる正規ウェブページのアドレスに対応付けて認証情報を記憶するものであって、本実施例ではアドレスＧ１２１１（Ｕ２４１１）と１以上のパラメタＧ１212（Ｕ２４１２）とを含む認証情報レコードＧ１２１ｒからなる。尚、このアドレスとして本願ではＵＲＬを例としてあげているが、ウェブページの所在が識別可能な、ウェブサーバのＩＰアドレスやＭＡＣアドレスなどのその他のアドレス、及びこれらの組み合わせを利用することも可能である。また、このパラメタＧ１２１２（Ｕ２４１２）は該当ウェブページの認証情報入力欄の数に応じて複数設けることが可能であり、口座番号またはログインＩＤとこれに対応するパスワードとが含まれることが一般的である。

【００１８】

図３は、ゲートウェイサーバＧ１の情報記憶手段Ｇ１２（または利用者端末Ｕ２の情報記憶手段Ｕ２４）に記憶するウェブページ情報テーブルＧ１２２（Ｕ２４２）の例を示す。このウェブページ情報テーブルＧ１２２（Ｕ２４２）は、利用者端末Ｕ１（またはＵ２）からの入力・登録指示に基づき、正規ウェブページのアドレスに対応付けて画面の外見情報に関する情報を記憶するものであって、本実施例ではアドレスＧ１２２１（Ｕ２４２１）と、ウェブページを１つの外見情報にした外見情報データの格納位置へのリンク情報Ｇ１２２２（Ｕ２４２２）とからなる。

【００１９】

図４は、ゲートウェイサーバＧ１の情報記憶手段Ｇ１２（または利用者端末Ｕ２の情報記憶手段Ｕ２４）に記憶する正規ウェブページの外見情報Ｇ１２３（Ｕ２４３）の例を示す。尚、本実施例ではウェブページ情報をビットマップにフォーマット変換した外見情報の例をあげているが、これはブラウザで表示された結果、つまり人が正規ウェブページであると誤認する外見を比較可能とするために表示結果の外見情報のフォーマットを統一することを意味する一例として挙げたものに過ぎず、ｊｐｅｇやＰＤＦなど、ウェブページの表示結果の外見を統一フォーマットで表現できる他の各種の公知技術を適用することが出来る。これにより、ウェブページを構成するＨＴＭＬ等の構成は相似していないが、表示結果の見た目が相似するウェブページの存在を検出することが可能となる。なお、ウェ

ブページ情報をビットマップ等のフォーマットに変換する方法については、公知技術によるものであり、本願の要旨ではないため説明は省略する。また、フォーマット変換することなく、単純にＨＴＭＬを比較することによってもある程度のウェブページの外見の類似度を比較することが可能であるため、ＨＴＭＬを単純に比較するという構成をとることも可能である。

【００２０】

図５は、ゲートウェイサーバＧ１の情報記憶手段Ｇ１２（または利用者端末Ｕ２の情報記憶手段Ｕ２４）に記憶する、試行結果であることを示す試行注意メッセージＧ１２４２（Ｕ２４４２）の例、図６は、アドレスの正当性が確認できないことを示すアドレス注意メッセージＧ１２４１（Ｕ２４４１）の例をそれぞれ示す。尚、本実施例では、ポップアップメッセージの外形を取った例を挙げているが、利用者端末Ｕ１またはＵ２において出力可能であれば良く、本実施例以外にも例えばフレーム分割やブラウザのツールバーの利用、ＨＴＭＬの追加等、各種の方法を取ることが可能である。また、単に注意であることを示す音、光（高輝度化、明滅）等であっても良い。

【００２１】

次に、本願の認証情報詐取防止方法の第１の実施例を図７に基づいて説明する。図７は、本願の認証情報詐取防止方法の第１の実施例の処理フローチャートを示す。

【００２２】

利用者端末Ｕ１は、利用者のキーボードからＵＲＬを入力したりマウスでメールなどに記載されたリンクをクリックしたりするなどの操作に基づき入力手段Ｕ１１が情報を入力する（Ｓ１０１）と、制御手段Ｕ１４が情報の送信指示であるか判定する（Ｓ１０２）。情報の送信指示であると判定すると（Ｓ１０２でＹ）、Ｓ１０１で入力された情報に基づき通信手段Ｕ１２から通信網Ｎ１に情報を送出する（Ｓ１０３）。上記の例では、入力されたＵＲＬのドメインで表されるウェブサーバを宛先とするウェブページ処理要求を送出することになる。なお、Ｓ１０２で送信指示として判定される入力としては、上記例の他、ウェブページのアップロード指示やメール送信指示などもあるが、本願要旨とは直接関係しないため詳述しない。

【００２３】

Ｓ１０１の入力が送信指示で無い場合（Ｓ１０２でＮ）、終了指示であるか判定して（Ｓ１０４）、終了指示であった場合には終了する。

【００２４】

また、通信手段Ｕ１２で通信網Ｎ１から情報を受信すると（Ｓ１０６）、制御手段Ｕ１４がウェブページであるか判定して（Ｓ１０７）、ウェブページであると判定した場合には（Ｓ１０７でＹ）、出力手段Ｕ１３にウェブページを出力し（Ｓ１０８）、Ｓ１０１に戻る。

【００２５】

制御手段Ｕ１４がＳ１０４で終了指示ではないと判定した場合（Ｓ１０４でＮ）、及びＳ１０７でウェブページではないと判定した場合（Ｓ１０７でＮ）には、それぞれの情報に応じた別の処理を行い（Ｓ１０５）、Ｓ１０１に戻るが、Ｓ１０５で行う具体的な処理の内容については、本願要旨とは直接関係しないため説明は省略する。

【００２６】

ゲートウェイサーバＧ１は、通信手段Ｇ１１が通信網Ｎ１から情報を受信すると（Ｓ３０１）、制御手段Ｇ１５がウェブページの処理要求であるか判定して（Ｓ３０２）、処理要求でない場合（Ｓ３０２でＮ）、例えばウェブページのアップロード要求やメール送信などの場合にはこの情報を送信情報としてＳ３０６に進む。

【００２７】

ウェブページの処理要求である場合（Ｓ３０２でＹ）には、比較手段Ｇ１３が情報記憶手段Ｇ１２に予め記憶した図２に示す認証情報テーブルＧ１２１を参照してパラメタＧ１２１２と同じ値が含まれるか更に判定する（Ｓ３０３）。一般に、認証については殆どのウェブページでＳＳＬ等を採用した暗号化通信を行っているが、フィッシングを目的とし

た偽のウェブページではそうしたセキュリティを採用しておらず、認証情報が暗号化されずに送られてくることが考えられ、既存の文字列検索技術を用いることにより認証情報が含まれるかの判定は容易である。

【００２８】

パラメタＧ１２１２と同じ値が含まれない場合（Ｓ３０３でＮ）、受信した情報をそのまま送信情報としてＳ３０６に進む。パラメタＧ１２１２と同じ値が含まれる場合（Ｓ３０３でＹ）には、試行手段Ｇ１４がこれを別の試行情報に置換した情報を送信情報として生成する（Ｓ３０５）。この試行情報については、情報記憶手段Ｇ１２に記憶した認証情報テーブルＧ１２１に認証情報であるパラメタＧ１２１２の各値と対応付けて試行情報を登録しておきこれを試行情報とする、認証情報の順番を入れ替えて試行情報とする、乱数を発生させて試行情報とする等の他、認証情報とは別の情報を生成可能な各種の任意の方法を採用して生成可能であり、また、それらの方法を任意に組み合わせることも好ましい。これらの処理が終わると、送信情報を通信網Ｎ２へ送出する（Ｓ３０６）。

【００２９】

また、通信手段Ｇ１１が通信網Ｎ２から情報を受信すると（Ｓ３０７）、制御手段Ｇ１５がウェブページを受信したか判定し（Ｓ３０８）、ウェブページの受信ではないと判定すると（Ｓ３０８でＮ）、受信した情報をそのまま送信情報としてＳ３１５に進む。

【００３０】

制御手段Ｇ１５がウェブページの受信であると判断すると（Ｓ３０８でＹ）、比較手段Ｇ１３がこのウェブページを情報記憶手段Ｇ１２に記憶したウェブページ外見情報Ｇ１２３と同一のフォーマットにフォーマット変換し（Ｓ３０９）、情報記憶手段Ｇ１２に記憶したウェブページ外見情報Ｇ１２３と比較して、外見の類似度の高いものがあるか判定する（Ｓ３１０）。比較手段Ｇ１３による比較の結果、類似度が高いものがなかった場合（Ｓ３１０でＮ）、Ｓ３０７で受信した情報をそのまま送信情報としてＳ３１５に進む。

【００３１】

比較手段Ｇ１３による比較の結果、類似度が高いものがあった場合（Ｓ３１０でＹ）、制御手段Ｇ１５がＳ３０５で情報置換を行った送信情報に対する応答であるかを判定し（Ｓ３１１）、Ｓ３０５で情報置換を行った送信情報に対する応答であると判定すると（Ｓ３１１でＹ）、Ｓ３０７で受信した情報に、図５に示すような試行注意メッセージを付加する（Ｓ３１２）。

【００３２】

例えば、正規ウェブページであれば、実際に認証を行って認証可否を判定し結果を通知するという処理になるため、Ｓ３０５で認証情報とは別の試行情報を生成して送信すると、認証がエラーとなって、同じ入力項目と認証エラーを知らせる旨の情報からなるウェブページ、または、エラーであるため再度最初から入力するよう戻るボタンをクリックする旨の指示等の情報からなるウェブページが返信されてくることになる。これに対し、フィッシングを目的とした偽のウェブページでは実際の認証が行われないため、正しくログインした旨の情報が送信されてくることが考えられる。このウェブページに図５に示す試行注意メッセージ１２４２を付加することになる。そしてこの情報を送信情報としてＳ３１５に進む。図８に図５に示す試行注意メッセージ１２４２を付加したウェブページの出力例を示す。

【００３３】

一方、制御手段Ｇ１５がＳ３０５で情報置換を行った送信情報に対する応答ではないと判定すると（Ｓ３１１でＮ）、比較手段Ｇ１３が図３に示す情報記憶手段Ｇ１２に予め記憶したウェブページ情報テーブルＧ１２２を参照して、Ｓ３１０で類似度が高いと判定したウェブページ外見情報Ｇ１２３のファイル名Ｇ１２２２に対応するアドレスＧ１２２１を取得し、受信したウェブページのアドレスと比較して、アドレスが同一であるか判定し（Ｓ３１３）、アドレスが同一であれば（Ｓ３１３でＹ）正規ウェブページであるため、Ｓ３１５に進む。一方、フィッシングサイトのウェブページは、正規ウェブページの画面と酷似していても、アドレスが異なるため、アドレスが異なれば（Ｓ３１３でＮ）、認証

情報テーブルＧ１２１を参照し、アドレスＧ１２２１と同じ値を持つアドレスＧ１２１１に対応するパラメタＧ１２１２を取得し（Ｓ３１４）、Ｓ３０５で試行手段Ｇ１４がこれを別の試行情報に置換してＳ３０７で取得したウェブページに設定する。Ｓ３１５では送信情報を通信網Ｎ１に送出する。

【００３４】

ウェブサーバＷ１～Ｗｎはいずれも処理は同じで、通信手段Ｗ１１～Ｗｎ１が通信網Ｎ２から情報を受信する（Ｓ５０１）と、制御手段Ｗ１３～Ｗｎ３がウェブページ処理要求であるか判定し（Ｓ５０２）、ウェブページのアップロードなど、ウェブページ処理要求でなければ（Ｓ５０２でＮ）、情報記憶手段Ｗ１２～Ｗｎ２に記憶するなどの別の対応処理を行い（Ｓ５０３）、Ｓ５０９に進む。なおこのＳ５０３の処理の詳細については、本願要旨に直接関係しないため詳述しない。

【００３５】

Ｓ５０２で制御手段Ｇ１５がウェブページ処理要求であると判定した場合（Ｓ５０２でＹ）、更に認証が必要か判定し（Ｓ５０４）、認証が必要な場合には（Ｓ５０４でＹ）、図示しない認証サーバに通信手段Ｗ１１～Ｗｎ１から認証依頼を送信（Ｓ５０５）して認証結果を受信し（Ｓ５０６）、認証結果が認証成功か判定する（Ｓ５０７）。Ｓ５０１で受信した情報がウェブページ処理要求であった場合（Ｓ５０２でＹ）で、認証要求を含まない場合（Ｓ５０４でＮ）、及びＳ５０６で受信した認証結果が認証成功であった場合（Ｓ５０６でＹ）、情報記憶手段Ｗ１２～Ｗｎ２を検索して（Ｓ５０８）、該当する情報があればその情報を、無ければ無い旨を、また、Ｓ５０５で受信した認証結果が認証失敗であった場合には認証失敗の旨を、ウェブページ処理要求に対する結果として通信手段Ｗ１１～Ｗｎ１から情報要求元に返信する（Ｓ５０９）。

【００３６】

また、上記処理に加えて、複数のウェブページ処理要求からなる一連の処理（セション）を管理するために利用者を一意に識別するためのクッキーの発行・管理なども行っているが、本願要旨に直接関係しないため詳述しない。

【００３７】

以上説明した本実施形態では、変形も可能である。次に本願の認証情報詐取防止方法の第２の実施例を図９に基づいて説明する。図９は、本願の認証情報詐取防止システムの第２の実施例の処理フローチャートを示す。この図９では、図７に示す本願の認証情報詐取防方法の第１の実施例を示すフローチャートと比較して、Ｓ３０４が追加され、Ｓ３１４の処理が異なるだけであるため、この部分についてだけ以下に説明する。

【００３８】

Ｓ３０４では、比較手段Ｇ１３が情報記憶手段Ｇ１２に予め記憶した図２に示す認証情報テーブルＧ１２１を参照してパラメタＧ１２１２と同じ値が含まれると判定した場合（Ｓ３０３でＹ）に、制御手段Ｇ１５が後述するＳ３１４で図６に示すアドレス注意メッセージＧ１２４１を付加したウェブページへの入力であるか判定し（Ｓ３０４）、図６に示すアドレス注意メッセージＧ１２４１を付加したウェブページではないと判定した場合（Ｓ３０４でＮ）には、受信した情報をそのまま送信情報としてＳ３０６に進み、一方、図６に示すアドレス注意メッセージＧ１２４１を付加したウェブページであると判定した場合（Ｓ３０４でＹ）だけＳ３０５の情報置換を行う。

【００３９】

Ｓ３１４では、比較手段G１３が情報記憶手段Ｇ１２に予め記憶した図３に示すウェブページ情報テーブルＧ１２２から処理した、Ｓ３１０で類似度が高いと判定したウェブページ外見情報Ｇ１２３のファイル名Ｇ１２２２に対応するアドレスＧ１２２１と、受信したウェブページのアドレスとを比較して、アドレスが異なる場合に（Ｓ３１３でＮ）、図６に示すアドレス注意メッセージ１２４１をＳ３０７で受信した情報に付加し、これらの情報を送信情報としてＳ３１５に進む。図１０にアドレス注意メッセージ１２４１を付加したウェブページの例を示す。

【００４０】

次に本願の認証情報詐取防止方法の第３の実施例を図１１に基づいて説明する。図１１は、本願の認証情報詐取防止システムの第３の実施例の処理フローチャートを示す。この実施例は、上述した図７に対応し、図７の利用者端末Ｕ１及びゲートウェイサーバＧ１の各処理を利用者端末Ｕ２で行う場合の処理フローである。

【００４１】

利用者端末Ｕ２は、利用者がキーボードから入力したり、マウスでクリックしたりするなど、入力手段Ｕ２１から入力がある（Ｓ７０１）と、制御手段Ｕ２７が情報の送信指示であるか判定する（Ｓ７０２）。このＳ７０２で送信指示として判定される入力としては、ウェブページ処理要求の他、ウェブページのアップロード指示やメール送信指示などがあるが、ウェブページ処理要求以外については本願要旨とは直接関係しないため詳述しない。

【００４２】

Ｓ７０２で送信指示であると判定すると、比較手段Ｕ２５が図２に示すような情報記憶手段U２４に予め記憶した認証情報テーブルU２４１を参照してＳ７０１で入力した送信指示の対象となる情報にパラメタＵ２４１２と同じ値がまれているか判定する（Ｓ７０３）。パラメタＵ２４１２と同じ値が含まれない場合（Ｓ７０３でＮ）、Ｓ７０１で入力した送信指示の対象となる情報をそのまま送信情報としてＳ７０６に進む。パラメタＵ２４１２と同じ値が含まれる場合（Ｓ７０３でＹ）には、試行手段Ｕ２６がこれを別の試行情報に置換する（Ｓ７０５）。この試行情報の生成については、上述した図７のＳ３０５の説明にある各種の生成方法を採用可能である。

Ｓ７０６では送信指示対象の情報を通信手段Ｕ２２から通信網Ｎ２に情報を送出する（Ｓ７０６）。Ｓ７０１の入力が送信指示で無い場合（Ｓ７０２でＮ）、制御手段Ｕ２７が終了指示であるか判定して（Ｓ７０７）、終了指示であった場合には終了する。

【００４３】

Ｓ７０７で制御手段Ｕ２７が終了指示ではないと判定した場合（Ｓ７０７でＮ）、及び後述するＳ７１０でウェブページではないと判定した場合（Ｓ７１０でＮ）には、それぞれの情報に応じた別の処理を行い（Ｓ７０８）、Ｓ７０１に戻るが、Ｓ７０８で行う具体的な処理の内容については、本願要旨とは直接関係しないため詳述しない。

【００４４】

また、利用者端末Ｕ２の通信手段Ｕ２２が通信網Ｎ２から情報を受信すると（Ｓ７０９）、制御手段Ｕ２７がウェブページを受信したか判定して（Ｓ７１０）、ウェブページの受信ではないと判定すると（Ｓ７１０でＮ）、上述したＳ７０８に進む。

【００４５】

Ｓ７１０で制御手段Ｕ２７がウェブページであると判定した場合には（Ｓ７１０でＹ）、比較手段Ｕ２５がこのウェブページを情報記憶手段Ｕ２４に記憶したウェブページ外見情報Ｕ２４３と同一のフォーマットにフォーマット変換し（Ｓ７１１）、情報記憶手段Ｕ２４に記憶したウェブページ外見情報Ｕ２４３と比較して、外見の類似度の高いものがあるか判定する（Ｓ７１２）。類似度が高いものがなかった場合（Ｓ７１２でＮ）、Ｓ７１７に進み、この情報をそのまま出力手段Ｕ２３が出力する（Ｓ７１７）。

【００４６】

Ｓ７１２で比較手段Ｕ２５が比較した結果、類似度が高いものがあった場合（Ｓ７１２でＹ）、制御手段Ｕ２７がＳ７０５で情報置換を行いＳ７０６で送信した情報に対する応答であるかを判定し（Ｓ７１３）、応答であると判定すると（Ｓ７１３でＹ）、Ｓ７０９で受信した情報に図５に示すような試行注意メッセージ２４４２を付加して（Ｓ７１４）、Ｓ７１７に進み、出力手段Ｕ２３が出力する。図６に示す試行注意メッセージＵ２４４２を付加したウェブページの出力例は図８のようになる。

【００４７】

一方、Ｓ７１３で制御手段Ｕ２７が応答ではないと判定すると（Ｓ７１３でＮ）、比較手段Ｕ２５がウェブページ情報テーブルＵ２４２を参照して、Ｓ７１２で類似度が高いと判定したウェブページ外見情報Ｇ１２３のファイル名Ｕ２４２２に対応するアドレスＵ２

４２１を取得し、Ｓ７０９で受信した受信したウェブページのアドレスと比較して、アドレスが同一であるか判定し（Ｓ７１５）、アドレスが同一であれば正規ウェブページであるため、Ｓ７１７に進み、この情報をそのまま出力手段Ｕ２３で出力する。一方、フィッシングサイトのウェブページは、正規ウェブページの画面と酷似していても、アドレスが異なるため、アドレスが異なれば（Ｓ７１５でＮ）、認証情報テーブルＵ２４１を参照し、Ｓ７１５で取得したアドレスＵ２４２１と同じ値を持つアドレスＵ２４１１に対応するパラメタＵ２４１２を取得し（Ｓ７１６）、Ｓ７０６では試行手段Ｇ１４がこれを別の試行情報に置換して、Ｓ７０９で取得したウェブページに設定する。
なお、図１１におけるウェブサーバＷ１～Ｗｎの動作はいずれも図７、図９と同じであるため説明は省略する。

【００４８】
次に本願の認証情報詐取防止方法の第４の実施例を図１２に基づいて説明する。図１２は、本願の認証情報詐取防止システムの第４の実施例の処理フローチャートを示す。この図１２は、上述した図９に対応し、図９の利用者端末Ｕ１及びゲートウェイサーバＧ１の各処理を利用者端末Ｕ２で行う場合の処理フローである。また、図１０に示す本願の認証情報詐取防方法の第３の実施例を示すフローチャートと比較して、Ｓ７０４が追加され、Ｓ７１６の処理が異なるだけであるため、この部分についてだけ以下に説明する。　Ｓ７０４では、比較手段Ｕ２５が情報記憶手段Ｕ２４に予め記憶した図２に示す認証情報テーブルＵ２４１を参照してパラメタＵ２４１２と同じ値が含まれると判定した場合（Ｓ７０３でＹ）に、制御手段Ｕ２７が後述するＳ７１６で図６に示すようなアドレス注意メッセージＵ２４４１を付加したウェブページへの入力であるか判定し（Ｓ７０４）、図６に示すようなアドレス注意メッセージＵ２４４１を付加したウェブページへの入力ではないと判定した場合（Ｓ７０４でＮ）には、Ｓ７０１の送信指示の対象となる情報をそのまま送信情報としてＳ７０６に進み、一方、図６に示すようなアドレス注意メッセージＧ１２４１を付加したウェブページへの入力であると判定した場合（Ｓ７０４でＹ）だけＳ７０５の情報置換を行う。

【００４９】
Ｓ７１６では、比較手段Ｕ２５が図３に示す情報記憶手段Ｕ２４に予め記憶したウェブページ情報テーブルＵ２４２から取得した、Ｓ７１２で類似度が高いと判定したウェブページ外見情報Ｕ２４３のファイル名Ｕ２４２２に対応するアドレスＵ２４２１と、受信したウェブページのアドレスとを比較して、アドレスが異なる場合に（Ｓ７１５でＮ）、図６に示すようなアドレス注意メッセージＵ２４４１をＳ７０９で受信した情報に付加し、これらの情報をＳ７１７で出力手段が出力する（Ｓ７１７）。図１０にアドレス注意メッセージ１２４１を付加したウェブページの出力例を示す。

【００５０】
上述した第１及び第３の実施例は、ウェブページ処理要求にパラメタＧ１２１２と同じ値、つまり認証情報が含まれる場合には、正常に認証を行うかを試すために試行情報に置換して応答を得るものである。また、正規ウェブページと外見が酷似するにもかかわらずアドレスが違うウェブページについては、フィッシングを目的としたウェブページである可能性が高いことから、利用者に問い合せるまでもなく試行情報に置換して応答を得るものである。これらの結果、利用者端末にはこの試行情報に基づく認証結果応答であるウェブページと試行注意メッセージとが出力されることになるため、利用者はこの出力結果を元にフィッシングを目的としたページか否かを確認でき、認証情報の詐取を未然に防ぐことが出来る。

【００５１】
また、上述した第２及び第４の実施例は、ウェブページ処理要求にパラメタＧ１２１２と同じ値、つまり認証情報が含まれ、且つ、この認証情報が正規ウェブページと外見が酷似するにもかかわらずアドレスが違うウェブページとしてアドレス注意メッセージを付加したウェブページ、つまりフィッシングを目的としている可能性が高いウェブページへの入力値として含まれる場合だけ認証情報を試行情報に置換し、正規ウェブページに対する

認証の試行は行わない。この結果、利用者端末には、フィッシングが疑わしい正規ウェブページに外見の似たウェブページについて、試行情報に基づく認証結果応答であるウェブページと試行注意メッセージとが出力されることになるため、利用者はこの出力結果を元にフィッシングを目的としたページか否かを確認でき、認証情報の詐取を未然に防ぐことが出来る。

【００５２】

上記実施例では、情報記憶手段、比較手段、試行手段をそれぞれゲートウェイサーバＧ１または利用者端末Ｕ２のいずれかに全て備えた実施例を記載したが、これは一例であって、本願の要旨を逸脱しない範囲でこれら実施例として上げた組み合わせ以外にも情報処理装置と手段の組み合わせが可能である。

（付記１）

認証情報詐取防止システムが、

ウェブページデータを取得する取得ステップと、

ウェブページ外見情報及び認証情報を対応付けて記憶する情報記憶手段に記憶したウェブページ外見情報と、前記取得手段で取得したウェブページデータの外見情報を比較する外見比較ステップと、

前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する試行ステップと、

を実行することを特徴とする認証情報詐取防止方法。（１）

（付記２）　認証情報詐取防止システムが、

利用者からのウェブページ取得要求に基づき、利用者の認証情報を関連付けて記憶する認証情報記憶手段を参照して、該ウェブページ取得要求に認証情報が含まれるか比較する認証比較ステップと、

前記認証比較ステップで比較した結果、前記利用者からのウェブページ取得要求に認証情報が含まれる場合に、該利用者からのウェブページ取得要求に含まれる認証情報とは異なる試行情報を該利用者からのウェブページ取得要求に設定して出力する試行ステップとを実行することを特徴とする認証情報詐取防止方法。（２）

（付記３）　認証情報詐取防止システムが、

前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、前記取得ステップで取得したウェブページデータのアドレスと、前記情報記憶手段に該ウェブページ外見情報に対応付けて更に記憶されたアドレスとを比較するアドレス比較ステップを更に実行し、

前記試行ステップは、外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合であって、且つ、前記アドレス比較ステップで比較した結果、アドレスが異なる場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する

ことを特徴とする付記１記載の認証情報詐取防止方法。（３）

（付記４）前記外見比較ステップは、前記取得手段で取得したウェブページデータを、前記情報記憶手段に記憶したウェブページ外見情報と同一のフォーマットに変換した後、情報記憶手段に記憶したウェブページ外見情報と比較する

ことを特徴とする付記１記載の認証情報詐取防止方法。

（付記５）

情報処理装置が、

ウェブページデータを取得する取得ステップと、

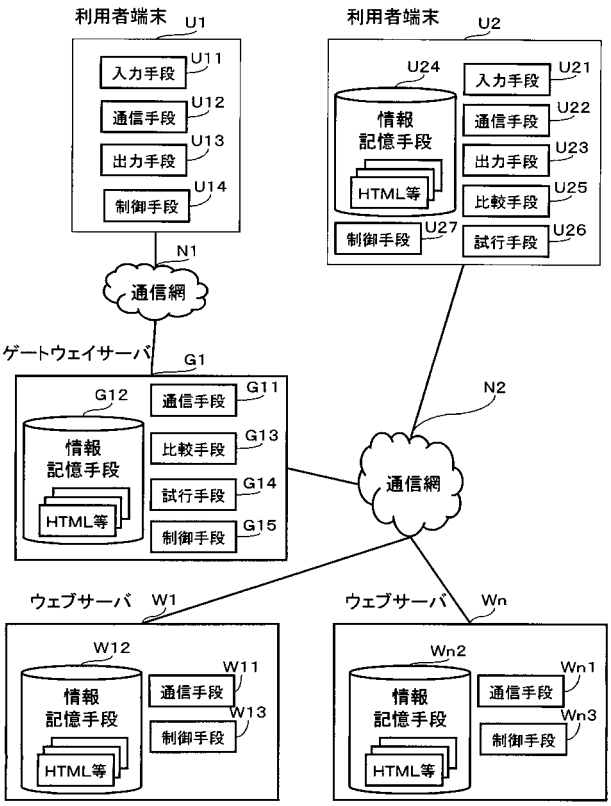
ウェブページ外見情報及び認証情報を対応付けて記憶する情報記憶手段に記憶したウェブページ外見情報と、前記取得手段で取得したウェブページデータの外見情報を比較する外見比較ステップと、

前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する試行ステップと、
を実行することを特徴とする認証情報詐取防止方法。（１）
（付記６）　情報処理装置が、
利用者からのウェブページ取得要求に基づき、利用者の認証情報を関連付けて記憶する認証情報記憶手段を参照して、該ウェブページ取得要求に認証情報が含まれるか比較する認証比較ステップと、
前記認証比較ステップで比較した結果、前記利用者からのウェブページ取得要求に認証情報が含まれる場合に、該利用者からのウェブページ取得要求に含まれる認証情報とは異なる試行情報を該利用者からのウェブページ取得要求に設定して出力する試行ステップと
を実行することを特徴とする認証情報詐取防止方法。
（付記７）　情報処理装置が、
前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、前記取得ステップで取得したウェブページデータのアドレスと、前記情報記憶手段に該ウェブページ外見情報に対応付けて更に記憶されたアドレスとを比較するアドレス比較ステップを更に実行し、
前記試行ステップは、外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合であって、且つ、前記アドレス比較ステップで比較した結果、アドレスが異なる場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する
ことを特徴とする付記５記載の認証情報詐取防止方法。
（付記８）前記外見比較ステップは、前記取得手段で取得したウェブページデータを、前記情報記憶手段に記憶したウェブページ外見情報と同一のフォーマットに変換した後、情報記憶手段に記憶したウェブページ外見情報と比較する
ことを特徴とする付記５記載の認証情報詐取防止方法。
（付記９）　認証情報詐取防止システムに、
ウェブページデータを取得する取得ステップと、
ウェブページ外見情報及び認証情報を対応付けて記憶する情報記憶手段に記憶したウェブページ外見情報と、前記取得手段で取得したウェブページデータの外見情報を比較する外見比較ステップと、
前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する試行ステップと、
を実行させることを特徴とする認証情報詐取防止プログラム。（４）
（付記１０）　認証情報詐取防止システムに、
利用者からのウェブページ取得要求に基づき、利用者の認証情報を関連付けて記憶する認証情報記憶手段を参照して、該ウェブページ取得要求に認証情報が含まれるか比較する認証比較ステップと、
前記認証比較ステップで比較した結果、前記利用者からのウェブページ取得要求に認証情報が含まれる場合に、該利用者からのウェブページ取得要求に含まれる認証情報とは異なる試行情報を該利用者からのウェブページ取得要求に設定して出力する試行ステップと
を実行させることを特徴とする認証情報詐取防止プログラム。（５）
（付記１１）　認証情報詐取防止システムに、
前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、前記取得ステップで取得したウェブページデータのアドレスと、前記情報記憶手段に該ウェブページ外見情報に対応付けて更に記憶されたアドレスとを比較

するアドレス比較ステップを更に実行させ、
前記試行ステップは、外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合であって、且つ、前記アドレス比較ステップで比較した結果、アドレスが異なる場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する
ことを特徴とする付記９記載の認証情報詐取防止プログラム。
（付記１２）前記外見比較ステップは、前記取得手段で取得したウェブページデータを、前記情報記憶手段に記憶したウェブページ外見情報と同一のフォーマットに変換した後、情報記憶手段に記憶したウェブページ外見情報と比較する
ことを特徴とする付記９記載の認証情報詐取防止プログラム。
（付記１３）
情報処理装置に、
ウェブページデータを取得する取得ステップと、
ウェブページ外見情報及び認証情報を対応付けて記憶する情報記憶手段に記憶したウェブページ外見情報と、前記取得手段で取得したウェブページデータの外見情報を比較する外見比較ステップと、
前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する試行ステップと、
を実行させることを特徴とする認証情報詐取防止プログラム。
（付記１４）　情報処理装置に、
利用者からのウェブページ取得要求に基づき、利用者の認証情報を関連付けて記憶する認証情報記憶手段を参照して、該ウェブページ取得要求に認証情報が含まれるか比較する認証比較ステップと、
前記認証比較ステップで比較した結果、前記利用者からのウェブページ取得要求に認証情報が含まれる場合に、該利用者からのウェブページ取得要求に含まれる認証情報とは異なる試行情報を該利用者からのウェブページ取得要求に設定して出力する試行ステップとを実行させることを特徴とする認証情報詐取防止プログラム。
（付記１５）　情報処理装置に、
前記外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、前記取得ステップで取得したウェブページデータのアドレスと、前記情報記憶手段に該ウェブページ外見情報に対応付けて更に記憶されたアドレスとを比較するアドレス比較ステップを更に実行させ、
前記試行ステップは、外見比較ステップで比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合であって、且つ、前記アドレス比較ステップで比較した結果、アドレスが異なる場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得ステップで取得したウェブページデータに設定したウェブページ取得要求を出力する
ことを特徴とする付記１３記載の認証情報詐取防止プログラム。
（付記１６）前記外見比較ステップは、前記取得手段で取得したウェブページデータを、前記情報記憶手段に記憶したウェブページ外見情報と同一のフォーマットに変換した後、情報記憶手段に記憶したウェブページ外見情報と比較する
ことを特徴とする付記１３記載の認証情報詐取防止プログラム。
（付記１７）
ウェブページデータを取得する取得手段と、
ウェブページ外見情報及び認証情報を対応付けて記憶する情報記憶手段と、
前記情報記憶手段に記憶したウェブページ外見情報と、前記取得手段で取得したウェブページデータの外見情報を比較する外見比較手段と、

前記外見比較手段で比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得手段で取得したウェブページデータに設定したウェブページ取得要求を出力する試行手段と、
を備えることを特徴とする認証情報詐取防止システム。
（付記１８）
利用者の認証情報を関連付けて記憶する認証情報記憶手段と、
利用者からのウェブページ取得要求に基づき、前記認証情報記憶手段を参照して、該ウェブページ取得要求に認証情報が含まれるか比較する認証比較手段と、
前記認証比較手段で比較した結果、前記利用者からのウェブページ取得要求に認証情報が含まれる場合に、該利用者からのウェブページ取得要求に含まれる認証情報とは異なる試行情報を該利用者からのウェブページ取得要求に設定して出力する試行手段と
を備えることを特徴とする認証情報詐取防止システム。
（付記１９）
前記情報記憶手段はウェブページ外見情報に対応付けてアドレスを更に記憶し、
前記外見比較手段で比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合に、前記取得手段で取得したウェブページデータのアドレスと、前記情報記憶手段に該ウェブページ外見情報に対応付けて更に記憶されたアドレスとを比較するアドレス比較手段を更に備え、
前記試行手段は、前記外見比較手段で比較した結果、前記情報記憶手段に類似するウェブページ外見情報があった場合であって、且つ、前記アドレス比較手段で比較した結果、アドレスが異なる場合に、該外見情報に関連付けて該情報記憶手段に記憶された認証情報とは異なる試行情報を前記取得手段で取得したウェブページデータに設定したウェブページ取得要求を出力する
ことを特徴とする付記１７記載の認証情報詐取防止システム。
（付記２０）前記外見比較手段は、前記取得手段で取得したウェブページデータを、前記情報記憶手段に記憶したウェブページ外見情報と同一のフォーマットに変換した後、情報記憶手段に記憶したウェブページ外見情報と比較する
ことを特徴とする付記１７記載の認証情報詐取防止システム。
【図面の簡単な説明】
【００５３】
【図１】認証情報詐取防止システムの概要構成を示すブロック図
【図２】認証情報テーブル例
【図３】ウェブページ情報テーブル例
【図４】ウェブページ外見情報例
【図６】アドレス注意メッセージ例
【図５】試行注意メッセージ例
【図７】本願の認証情報詐取防止方法の第１の実施例の処理フローチャート
【図８】試行注意メッセージを付加したウェブページ出力例
【図９】本願の認証情報詐取防止方法の第２の実施例の処理フローチャート
【図１０】アドレス注意メッセージを付加したウェブページ出力例
【図１１】本願の認証情報詐取防止方法の第３の実施例の処理フローチャート
【図１２】本願の認証情報詐取防止方法の第３の実施例の処理フローチャート
【符号の説明】
【００５４】
Ｕ１、Ｕ２　利用者端末
Ｇ１　　ゲートウェイサーバ
Ｗ１、Ｗｎ　ウェブサーバ
Ｎ１、Ｎ２　通信網

【図１】



【図２】

認証情報テーブルG121(U241)

G1211(U2411) G1212(U2412) G121r(U241r)

アドレス	第一パラメータ	第二パラメータ	第三パラメータ	
http://www.abcdbank.co.jp	014	7162534	4132	…
http://xyzcredit.co.jp	4152637	1192	–	…
http://onetwoclub.login.jsp			–	…
:	:	:	:	:

【図３】

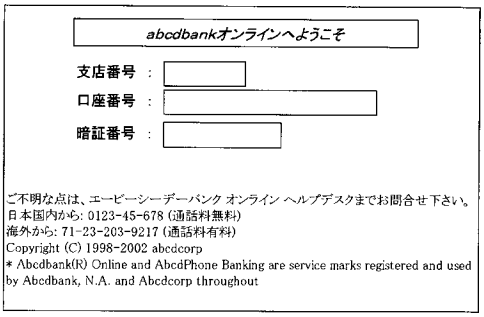
ウェブページ情報テーブルＧ１２２（Ｕ２４２）

G1221(U2421) G1222(U2422) G122r(U242r)

アドレス	外見情報格納パス
http://www.abcdbank.co.jp	data/www.abcdbank.co.jp/001.bmp
http://xyzcredit.co.jp	data/xyzcredit.co.jp/001.bmp
http://onetwoclub.login.jsp	data/onetwoclub.login.jsp/001.bmp
・	・
・	・

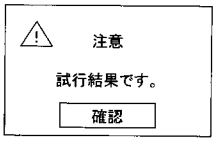
【図４】

ウェブページ外見情報Ｇ１２３（Ｕ２４３）



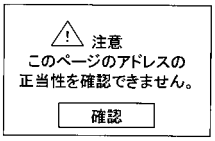
【図５】

試行注意メッセージＧ１２４２（Ｕ２４４２）

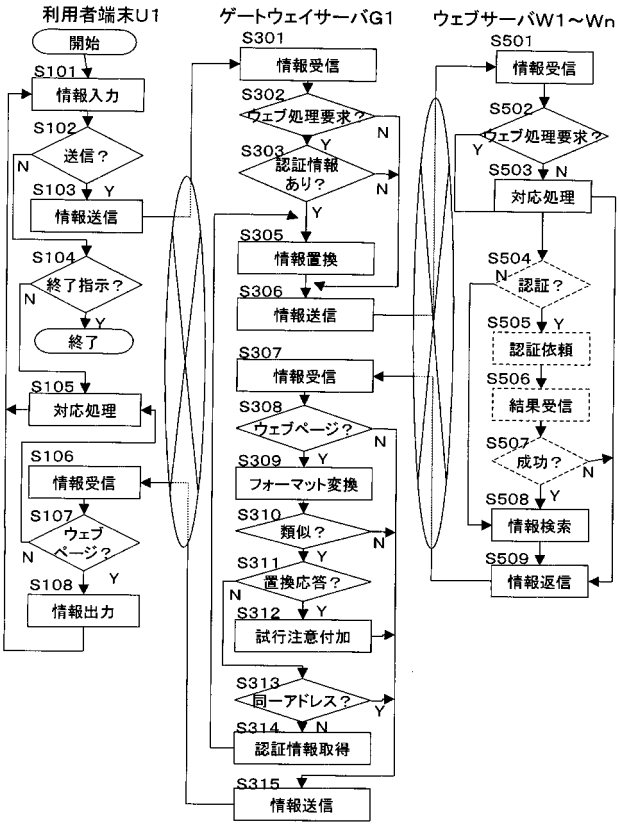


【図６】

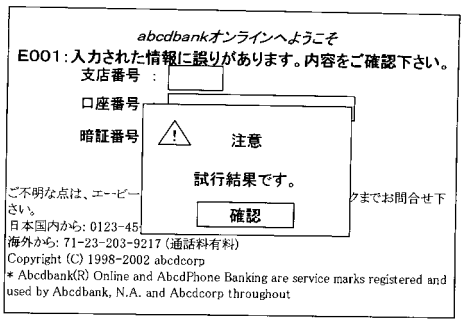
アドレス注意メッセージＧ１２４１（Ｕ２４４１）



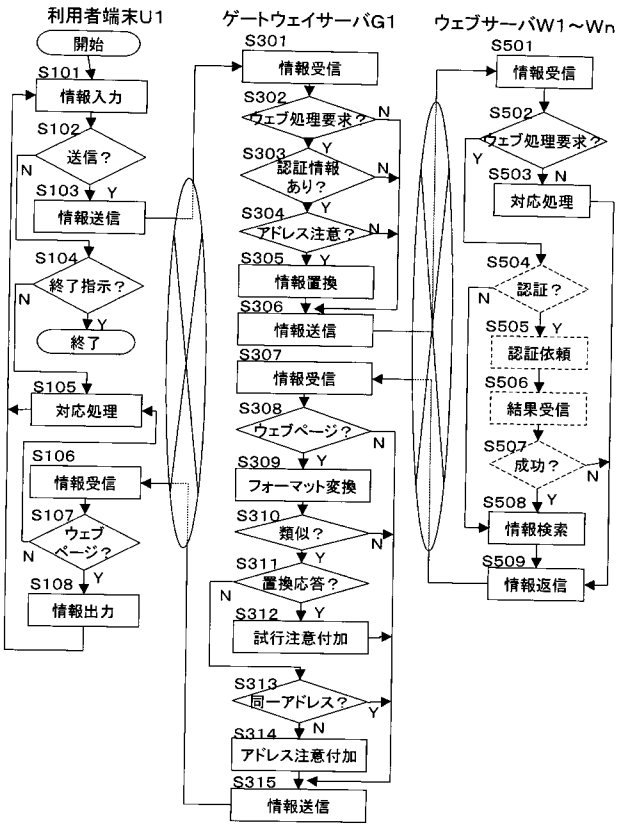
【図７】



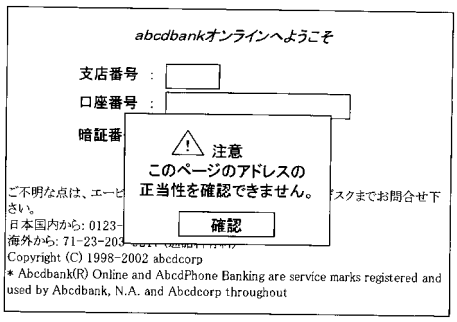
【図８】



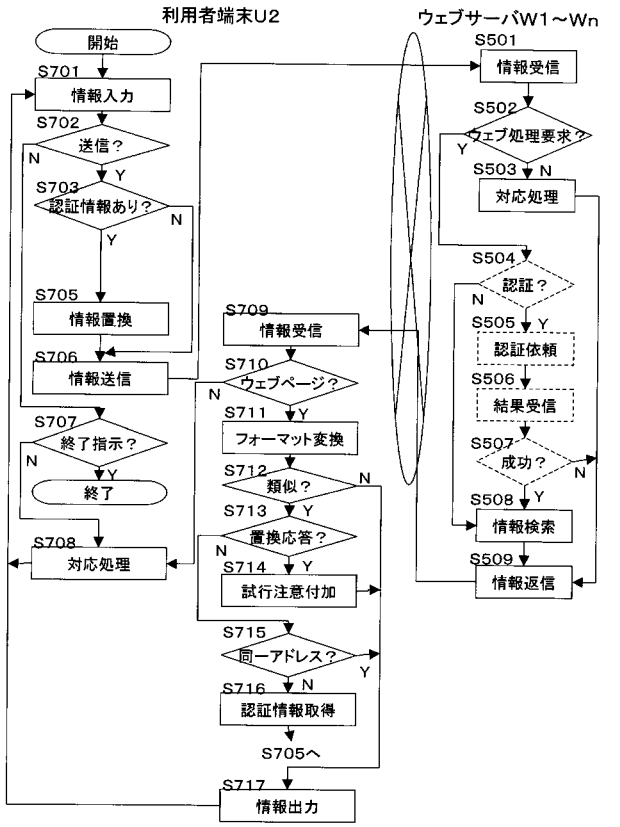
【図９】



【図１０】



【図１１】



【図１２】