(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2009-59358
(P2009-59358A)
(43)公開日　平成21年3月19日(2009.3.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B089
G06F 13/00	(2006.01)	G06F	13/00	351Z	5B285

審査請求 未請求　請求項の数 20　ＯＬ　（全 16 頁）

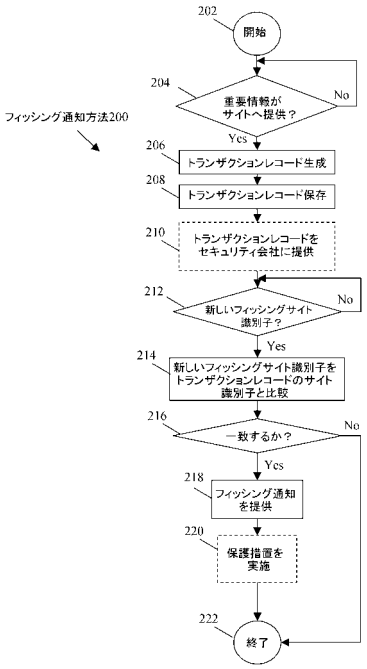
(21)出願番号　特願2008-212540 (P2008-212540)
(22)出願日　平成20年8月21日 (2008.8.21)
(31)優先権主張番号　11/849,093
(32)優先日　平成19年8月31日 (2007.8.31)
(33)優先権主張国　米国 (US)

(71)出願人　501113353
シマンテック　コーポレイション
Ｓｙｍａｎｔｅｃ　Ｃｏｒｐｏｒａｔｉｏｎ
アメリカ合衆国　カリフォルニア州　９５０１４　クーパーティノ、スティーブンス　クリーク　ブルバード、２０３３０
２０３３０ Ｓｔｅｖｅｎｓ Ｃｒｅｅｋ Ｂｏｕｌｅｖａｒｄ, Ｃｕｐｅｒｔｉｎｏ, Ｃａｌｉｆｏｒｎｉａ ９５０１４, ＵＳＡ
(74)代理人　100089266
弁理士　大島　陽一

最終頁に続く

(54)【発明の名称】フィッシング通知サービス

(57)【要約】
【課題】フィッシング攻撃からの保護を提供する方法を提供する。
【解決手段】本発明の方法は、新しいフィッシングサイト識別子（例えば、これらに限定されるものではないが、ＵＲＬ及び／又はＩＰアドレス）が生成されたか否かを判定し（２１２）、新しいフィッシングサイト識別子が生成されたと判定された場合は、前記新しいフィッシングサイト識別子を、過去に重要情報（critical values）（例えば、ユーザの個人／秘密情報）を提供したことがあるサイトのサイト識別子と比較する（２１４）。前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくとも１つと一致すると判定された場合は、ユーザが過去にフィッシングされたというフィッシング通知が提供される（２１８）。
【選択図】図２



【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、
新しいフィッシングサイト識別子が生成されたか否かを判定するステップと、
前記新しいフィッシングサイト識別子が生成されたと判定された場合に、前記新しいフィッシングサイト識別子を、以前に重要情報を提供したことがあるサイトのサイト識別子と比較するステップと、
前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくとも１つと一致すると判定された場合に、フィッシング通知を提供するステップとを含むことを特徴とする方法。
【請求項２】
請求項１に記載の方法であって、
前記新しいフィッシングサイト識別子が、新しく発見されたフィッシングサイトのサイト識別子であることを特徴とする方法。
【請求項３】
請求項２に記載の方法であって、
前記新しいフィッシングサイト識別子が、前記新しく発見されたフィッシングサイトのユニフォーム・リソース・ロケータ（ＵＲＬ）を含むことを特徴とする方法。
【請求項４】
請求項２に記載の方法であって、
前記新しいフィッシングサイト識別子が、前記新しく発見されたフィッシングサイトのインターネットプロトコル（ＩＰ）アドレスを含むことを特徴とする方法。
【請求項５】
請求項１に記載の方法であって、
前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくとも１つと一致しないと判定された場合、
フィッシングサイトであることが判明したサイトへ重要情報を提供したことがないと判断することを特徴とする方法。
【請求項６】
請求項１に記載の方法であって、
前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくとも１つと一致すると判定された場合、
フィッシングサイトであることが判明したサイトへ重要情報を提供したことがあると判断することを特徴とする方法。
【請求項７】
請求項６に記載の方法であって、
前記フィッシング通知が、前記フィッシングサイトへ前記重要情報を提供したことがあるという通知を含むことを特徴とする方法。
【請求項８】
請求項６に記載の方法であって、
前記フィッシング通知が、
（１）前記重要情報が前記フィッシングサイトへ提供された日付及び／又は時間、
（２）前記フィッシングサイトへ提供された前記重要情報、
（３）前記フィッシングサイトの前記サイト識別子、
（４）前記フィッシングサイトの名前、
（５）前記フィッシングサイトによって偽装された本物の商業者、
から成る群より選択される通知を含むことを特徴とする方法。
【請求項９】
請求項６に記載の方法であって、
前記フィッシングサイトから保護するための保護措置を実施するステップをさらに含む

ことを特徴とする方法。
【請求項１０】
請求項９に記載の方法であって、
前記保護措置を実施するステップが、前記フィッシングサイトに関連するあらゆるフィッシング電子メールを無効にすることを含むことを特徴とする方法。
【請求項１１】
請求項１に記載の方法であって、
前記重要情報を或るサイトへ提供したことがあるか否かを判定するステップをさらに含むことを特徴とする方法。
【請求項１２】
請求項１１に記載の方法であって、
前記重要情報を或るサイトへ提供したことがあると判定された場合に、
前記サイトのサイト識別子を含むトランザクションレコードを生成するステップをさらに含むことを特徴とする方法。
【請求項１３】
請求項１２に記載の方法であって、
前記トランザクションレコードを保存するステップをさらに含むことを特徴とする方法。
【請求項１４】
請求項１３に記載の方法であって、
前記トランザクションレコードが、複数のトランザクションレコードを含むトランザクションレコードストアに保存されることを特徴とする方法。
【請求項１５】
請求項１４に記載の方法であって、
前記新しいフィッシングサイト識別子を、重要情報を提供したことがあるサイトのサイト識別子と比較する前記ステップが、
前記新しいフィッシングサイト識別子のいずれかが、前記トランザクションレコードに含まれている前記サイト識別子のいずれかと一致するか否かを判定するステップを含むことを特徴とする方法。
【請求項１６】
請求項１３に記載の方法であって、
前記トランザクションレコードをセキュリティ会社に提供するステップをさらに含むことを特徴とする方法。
【請求項１７】
請求項１に記載の方法であって、
前記サイト識別子が、ウェブブラウザのキャッシュ内に含まれていることを特徴とする方法。
【請求項１８】
請求項１に記載の方法であって、
前記サイト識別子が、電子メール内に含まれていることを特徴とする方法。
【請求項１９】
コンピュータプログラムコードが記憶された有形のコンピュータで読取り可能な媒体を備えたコンピュータプログラム製品であって、
新しいフィッシングサイト識別子が生成されたか否かを判定するフィッシング通知サービス・アプリケーションを含み、
前記フィッシング通知サービス・アプリケーションが、
前記新しいフィッシングサイト識別子が生成されたと判定された場合に、
前記新しいフィッシングサイト識別子を、重要情報を提供したことがあるサイトのサイト識別子と比較し、
前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくと

も１つと一致すると判定された場合に、フィッシング通知を生成するように構成されたことを特徴とするコンピュータプログラム製品。
【請求項２０】
コンピュータシステムであって、
フィッシング通知サービス・アプリケーションを記憶させたメモリと、
前記メモリに接続されたプロセッサとを備え、
前記フィッシング通知サービス・アプリケーションを実行することにより、
新しいフィッシングサイト識別子が生成されたか否かを判定するステップと、
新しいフィッシングサイト識別子が生成されたと判定された場合に、前記新しいフィッシングサイト識別子を、重要情報を提供したことがあるサイトのサイト識別子と比較するステップと、
前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくとも１つと一致すると判定された場合に、フィッシング通知を生成するステップとを含む方法が実施されることを特徴とする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のユーザの保護に関する。より詳細には、本発明は、フィッシング攻撃からの保護を提供するための方法及び装置に関するものである。
【背景技術】
【０００２】
フィッシングという用語は、ユーザ個人情報の窃盗（未遂を含む）を意味する。例えば、成りすまし窃盗に使用されるユーザ個人情報を騙し取ろうとして、実在の商業者を偽称した電子メールがユーザに送られてくる。典型的には、その電子メールに張られたリンクによってユーザをウエブサイトへ誘導し、本物の商業者が既に持っているユーザ個人情報（パスワード、クレジットカード番号、社会保障番号、銀行口座番号など）の更新手続をユーザに求める。前記ウエブサイトは、実在する本物のサイトの偽物であり、ユーザの情報を窃盗するために本物のサイトとそっくりに作られている。
【０００３】
なお、上述したフィッシング攻撃は一例であり、フィッシング攻撃はその他にも様々な種類がある。
【０００４】
ユーザをフィッシング攻撃から保護するために、アンチフィッシング・アプリケーションなどのセキュリティアプリケーションが開発されてきた。かかるセキュリティアプリケーションは、判明したフィッシングサイト（例えばウエブサイト）へユーザがアクセスしようとした場合に、保護措置を実施する。例えば、前記セキュリティアプリケーションは、フィッシングサイトへのアクセスを遮断する。或いは、少なくとも、ユーザが判明したフィッシングサイトに接続していることを通知する。
【０００５】
セキュリティアプリケーションは、セキュリティ会社の更新サイトからの更新に依存している。かかる更新は、前記セキュリティアプリケーションの重要な要素である。例えば、新しいフィッシングサイトが発見されると、前記セキュリティアプリケーションが新しく発見されたフィッシングサイトからユーザを保護するために、新しいフィッシングサイトのユニフォーム・リソース・ロケータ（ＵＲＬ）が更新として配布される。
【０００６】
しかしながら、フィッシングサイトがセキュリティ会社によって発見されるまでの間に、多くの場合はユーザがフィッシング攻撃されたことに気付くことなく、ユーザの個人情報が既に盗まれている可能性もある。ほとんどの場合、ユーザは、成りすまし窃盗の被害に遭うまではフィッシング攻撃されたことに気付かない。
【発明の開示】

【課題を解決するための手段】
【０００７】
本発明の一実施形態の方法は、新しいフィッシングサイト識別子（例えば、これらに限定されるものではないが、ＵＲＬ及び／又はＩＰアドレス）が生成されたか否かを判定する。新しいフィッシングサイト識別子が生成されたと判定された場合は、前記新しいフィッシングサイト識別子を、過去に重要情報（critical values）（例えば、ユーザの個人／秘密情報）を提供したことがあるサイトのサイト識別子と比較する。
【０００８】
前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくとも１つと一致すると判定された場合は、ユーザが過去にフィッシングされたというフィッシング通知が提供される。
【０００９】
このようにして、ユーザは、現在においてフィッシングサイトから保護されるだけでなく、過去にフィッシング攻撃の被害に遭ったことがある場合はフィッシング通知を受け取ることができる。さらに、前記フィッシング通知は、フィッシング攻撃に関連する成りすまし窃盗を防止する又は最小限に抑えるべく、フィッシング攻撃の影響（例えば、ユーザのクレジットビューローへの接触）を減少させるために、ユーザが保護措置を実施するのに十分な情報を含んでいる。
【００１０】
本発明の実施形態は、添付図面を参照して行う以下の詳細な説明によって、最もよ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】
【００１１】
図２を参照して、フィッシング通知方法２００は、新しいフィッシングサイト識別子（例えば、これらに限定されるものではないが、ＵＲＬ及び／又はＩＰアドレス）が生成されたか否かを判定するオペレーションを含む（オペレーション２１２）。前記新しいフィッシングサイト識別子が生成されたと判定された場合は、前記新しいフィッシングサイト識別子を、過去に重要情報（critical values）（例えば、ユーザの個人／秘密情報）を提供したことがあるサイトのサイト識別子と比較する（オペレーション２１４）。前記新しいフィッシングサイト識別子の少なくとも１つが前記サイト識別子の少なくとも１つと一致すると判定された場合（オペレーション２１６でＹｅｓと判定された場合）は、ユーザが過去にフィッシングされたというフィッシング通知が提供される（オペレーション２１８）。
【００１２】
このようにして、ユーザは、現在においてフィッシングサイトから保護されるだけでなく、過去にフィッシング攻撃の被害に遭ったことがある場合はフィッシング通知を受け取ることができる。さらに、前記フィッシング通知は、フィッシング攻撃に関連する成りすまし窃盗を防止する又は最小限に抑えるべく、フィッシング攻撃の影響（例えば、ユーザのクレジットビューローへの接触）を減少させるために、ユーザが保護措置を実施するのに十分な情報を含んでいる。
【００１３】
より詳しく説明すると、図１は、本発明の一実施形態による、ホス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）で実行されるフィッシング通知サービス（Phishing notification Service：ＰＮＳ）アプリケーション１０６を含むクライアントサーバシステム１００を示す図である。
【００１４】
ホストコンピュータシステム１０２（クライアント又はユーザデバイスとも称する）は一般に、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１１４を備える。
【００１５】

フィッシング通知サービス（ＰＮＳ）アプリケーション１０６は、随意的に、ハイパーテキスト転送プロトコル（ＨＴＴＰ）プロキシと、トランザクションレコードストア（transaction record store）１４２とを備える。ＨＴＴＰプロキシは、当業者には周知である。一般に、ＨＴＴＰプロキシ１４０は、ホストコンピュータシステム１０２のユーザプリケーション（例えば、ホストコンピュータシステム１０２のウェブブラウザ）と、ネットワーク１２４との間に位置する。ホストコンピュータシステム１０２のユーザプリケーションのＨＴＴＰトラフィックは、ＨＴＴＰプロキシ１４０を通過する。

【００１６】

ホス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及びディスプレイデバイス１２２などの標準的なデバイス、並びに、１つ以上の標準的な入出力（Ｉ／Ｏ）デバイス１２３をさらに備え得る。入出力（Ｉ／Ｏ）デバイス１２３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、又はホストコンピュータ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、フィッシング通知サービス（ＰＮＳ）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が記憶されているＣＤ、ＤＶＤ又はフレキシブルディスクなどから、入出力装置１２４を介してホストコンピュータシステム１０２にロードされる。

【００１７】

ホストコンピュータシステム１０２は、ネットワーク１２４によって、クライアントサーバシステム１００のサーバコンピュータシステム１３０に接続される。サーバコンピュータシステム１３０は一般に、ディスプレイデバイス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。

【００１８】

さらに、ホストコンピュータシステム１０２はまた、ネットワーク１２４によって、商業者サーバ１５２、フィッシングサーバ１５４、及びセキュリティ会社サーバ１５６に接続される。ある実施形態では、商業者サーバ１５２、フィッシングサーバ１５４、及びセキュリティ会社サーバ１５６は、ホストコンピュータシステム１０２及び／又はサーバ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、及びメモリを備える。

【００１９】

商業者サーバ１５２、フィッシングサーバ１５４、及びセキュリティ会社サーバ１５６は、キーボード、マウス、プリンタ、ディスプレイデバイス、及びＩ／Ｏデバイスなどの標準的なデバイスをさらに備え得る。商業者サーバ１５２、フィッシングサーバ１５４、及びセキュリティ会社サーバ１５６の種々のハードウェアコンポーネントは、本発明の本質から逸れることを避けるために示されていない。

【００２０】

ネットワーク１２４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、デジタルモデム又はネットワークインタフェースカードなどがある。

【００２１】

フィッシング通知サービス（ＰＮＳ）アプリケーション１０６は、ホストコンピュータシステム１０２のメモリ１１４に保存され、ホストコンピュータシステム１０２上で実行される。ホストコンピュータシステム１０２、商業者サーバ１５２、フィッシングサーバ１５４、セキュリティ会社サーバ１５６、及びサーバコンピュータシステム１３０の特定の種類及び構成は、本実施形態に必須ではない。

【００２２】

図２は、本発明の一実施形態によるフィッシング通知方法２００を説明するためのフロー図である。図１及び図２を共に参照して、プロセッサ１０８でフィッシング通知サービ

ス（ＰＮＳ）アプリケーション１０６を実行すると、フィッシング通知方法２００が以下のように実施される。

【００２３】

方法２００は開始オペレーション２０２で開始され、フローは、重要情報の或るサイトへの提供をチェックするオペレーション２０４へ進む。重要情報の或るサイトへの提供をチェックするオペレーション２０４では、重要情報（例えば、少なくとも１つの重要情報）を或るサイト（例えばウエブサイト）へ提供したことがあるか否かの判定が行われる。

【００２４】

重要情報を或るサイトへ提供したことがない場合、フローは、重要情報の或るサイトへの提供をチェックするオペレーション２０４に留まる。

【００２５】

反対に、重要情報をサイトへ提供したことがある場合、フローは、トランザクションレコード生成オペレーション２０６へ進む。

【００２６】

ある実施形態では、 重要情報（パラメータとも称す）は、フィッシング攻撃を成功させるために極めて重要なユーザの個人／秘密情報などのデータである。重要情報のいくつかの例としては、ユーザの氏名、アカウント番号、パスワード、クレジットカード番号、社会保障番号、及び銀行口座番号などがある。例として、どの情報が重要情報であるかは、例えば、ホストコンピュータシステム１０２のユーザ若しくはシステム管理者によって、又はセキュリティ会社によって設定可能である。

【００２７】

例えば、ホストコンピュータシステム１０２のユーザは、実在の商業者を偽称する電子メールを受け取る。前記電子メールには、前記商業者に関連するウエブサイトへユーザを騙して誘導する（例えば、商業者サーバ１５２に接続させる）ためのリンクが張られている。前記電子メールのリンクをクリックすると、ユーザは、知らないうちに、本物の商業者サーバ１５２によりホストされるウエブサイトに似せて作られた（そっくりにコピーした）、フィッシング・ウエブサイトをホストするフィッシングサーバ１５４に接続させられる。そして、ユーザは、商業者サーバ１５２へ提供しているものだと信じて、フィッシングサーバ１５４によりホストされる前記フィッシング・ウエブサイトへ個人情報（例えば、重要情報）を提供してしまう。

【００２８】

ある実施形態では、フィッシングサーバ１５４によりホストされるフィッシング・ウエブサイトは、判明したフィッシングサイトではなく、例えば、セキュリティ会社によってフィッシングサイトとして認定されていない。したがって、アンチフィッシング・アプリケーションを含むセキュリティアプリケーションをホストコンピュータシステム１０２上で実行したとしても、フィッシングサーバ１５４によりホストされるフィッシング・ウエブサイトは前記アンチフィッシング・アプリケーションによって判明したフィッシングサイトと認識されないので、ユーザはフィッシングサーバ１５４によりホストされるフィッシング・ウエブサイトに重要情報を提供してしまう。

【００２９】

この例では、ユーザは、成りすまし窃盗に使用される個人情報を騙し取られてしまう。さらに、ユーザは、自分がそうしたと気付かずに、個人情報を渡してしまう。

【００３０】

ある実施形態では、重要情報を或るサイトへ提供する行為は、トランザクション（transaction）と呼ばれる。トランザクションは、金銭的な取引（例えば、お金の振替又は製品の購入）に限定されるものではなく、重要情報のあらゆる送信を含む。トランザクションは、ＨＴＴＰプロキシ１４０を使用してモニタすることができる。

【００３１】

上述したフィッシング攻撃は一例であり、フィッシング攻撃にはその他にも様々な種類があり、特定のフィッシング攻撃はこの実施形態に必須ではない。

【００３２】
したがって、重要情報が或るサイトへ提供されると、フローはトランザクションレコード生成オペレーション２０６へ進む。トランザクションレコード生成オペレーション２０６では、前記トランザクションに関してのトランザクションレコードが生成される。トランザクションレコードは、例えば、重要情報が提供されたサイトの完全なＵＲＬ、サブＵＲＬ、及び／又はインターネットプロトコル（ＩＰ）アドレスなどのサイト識別子を含む。本明細書中では、本発明の開示の観点から、サイト識別子の例としてＵＲＬ及び／又はＩＰアドレスを挙げているが、サイトの識別に様々なサイト識別子を使用できることは当業者に明らかであろう。したがって、サイト識別子としては、これらに限定されるものではないが、ＵＲＬとＩＰアドレスがある。

【００３３】
ＩＰアドレスは、ＴＣＰ／ＩＰ（伝送制御プロトコル／インターネットプロトコル）ネットワーク上のコンピュータ又はデバイスのための識別子である。ＴＣＰ／ＩＰプロトコルルートを使用したネットワークは、目的地のＩＰアドレスに基づいてメッセージをルートする。ＩＰＶ４におけるＩＰアドレスのフォーマットは一般的に、ドットで区切られた４組の数字で記された３２ビット数のアドレスである。例えば、ＩＰアドレスは、１２７．０．０．１で表わされる。

【００３４】
しかし、ＩＰアドレスは、人間にとって覚えづらい。そのため、人間の便宜のために、ＩＰアドレスの代わりに、ホスト（マシン）名とドメイン名が一般的に使用される。

【００３５】
ホスト／ドメイン名は、１つ以上のＩＰアドレスを識別する名前である。インターネットトラフィックはＩＰアドレスを使用してルートされるので、全てのウエブサーバは、ホスト／ドメイン名をＩＰアドレスへ変換するためのＤＮＳ（ドメインネームシステム）サーバを必要とする。

【００３６】
より詳しく説明すると、ホストコンピュータは、ＤＮＳサーバがホスト／ドメイン名をＩＰアドレスへ変換するためのＤＮＳクエリを生成する。ＤＮＳクエリに応答して変換が成功すると、ホスト／ドメイン名は、前記ホスト／ドメイン名に関連する前記ホストサイトのＩＰアドレスに戻される。

【００３７】
このようにして、サイト（例えば、ウエブサイト）は、ＵＲＬ（サブＵＲＬを含む）及び／又はＩＰアドレスによって識別することができる。したがって、ＵＲＬ及び／又はＩＰアドレスは、サイトを識別するためのサイト識別子である。本明細書中ではサイト識別子としてＵＲＬ及び／又はＩＰアドレスを挙げているが、ＵＲＬ及び／又はＩＰアドレスは前記サイトをホストするコンピュータシステムのためのものであることに留意されたい。上述したように、サイト識別子は、これらに限定されるものではないが、ＵＲＬ及び／又はＩＰアドレスを含む。

【００３８】
ある実施形態では、前記トランザクションレコードは、次の（１）～（４）の１つ以上を含む。
（１）提供された重要情報。例えば、銀行口座番号などの実際の数字。
（２）提供された重要情報の種類。例えば、実際の銀行口座番号を特定することなく、銀行口座番号が提供された。
（３）重要情報が提供された日付。
（４）要情報が提供された時間。

【００３９】
トランザクションレコード生成オペレーション２０６からは、フローは、トランザクションレコード保存オペレーション２０８へ進む。トランザクションレコード保存オペレーション２０８では、トランザクションレコード生成オペレーション２０６で生成されたト

ランザクションレコードが保存される。具体的には、トランザクションレコードは、トランザクションレコードストア１４２に保存される。ある実施形態では、トランザクションレコードストア１４２は、複数のトランザクションレコードを含む。

【００４０】

他の実施形態では、前記トランザクションレコードは、トランザクションレコードをセキュリティ会社に提供するオペレーション２１０において後述するのと同様な方法でセキュリティ会社に提供される。この実施形態では、前記トランザクションレコードは、セキュリティ会社（例えば、セキュリティ会社サーバ１５６）に保存される。

【００４１】

トランザクションレコード保存オペレーション２０８からは、フローは、随意的に、トランザクションレコードをセキュリティ会社に提供するオペレーション２１０へ進む。オペレーション２１０を行わない場合は、直接、新しいフィッシングサイト識別子をチェックするオペレーション２１２へ進む。

【００４２】

トランザクションレコードをセキュリティ会社に提供するオペレーション２１０では、ホストコンピュータシステム１０２に保存されているトランザクションレコード（例えば、少なくとも１つのトランザクションレコード）がセキュリティ会社に提供される。具体的には、トランザクションレコードは、トランザクションレコードの暗号化された安全な通信を使用して、セキュリティ会社サーバ１５６に提供される。

【００４３】

ある実施形態では、各トランザクションレコードは、生成されるとすぐにセキュリティ会社に提供される。他の実施形態では、トランザクションレコードは、セキュリティ会社へ定期的（例えば、１時間毎、１日毎、１週間毎）に提供される。具体的には、トランザクションレコードがセキュリティ会社に提供される時期は、例えば、ホストコンピュータシステム１０２のユーザ若しくはシステム管理者によって、又はセキュリティ会社によって設定可能である。

【００４４】

トランザクションレコードをセキュリティ会社に提供するオペレーション２１０からは、フローは、新しいフィッシングサイト識別子をチェックするオペレーション２１２へ進む。新しいフィッシングサイト識別子をチェックするオペレーション２１２では、新しいフィッシングサイト識別子が生成されたか否かの判定が行われる。

【００４５】

新しいフィッシングサイト識別子が生成されていないと判定された場合、フローは、新しいフィッシングサイト識別子をチェックするオペレーション２１２に留まる。反対に、新しいフィッシングサイト識別子が生成されたと判定された場合、フローは、フィッシングサイト識別子をトランザクションレコードと比較するオペレーション２１４へ進む。

【００４６】

ある実施形態では、新しいフィッシングサイト識別子は、新しく発見されたフィッシングサイトのＵＲＬ及び／又はＩＰアドレス（サイト識別子とも呼ばれる）である。フィッシングサイトは、例えば成りすまし窃盗に使用するために、個人情報を不正に収集することが知られているサイト（例えば、ウエブサイトである）。フィッシングサイトの発見に使用される特定の技術はこの実施形態に必須ではなく、様々な公知技術のいずれか一つを使用することができる。一般に、以前は公知のフィッシングサイトではなかったが現在はフィッシングサイトと認識されたウエブサイトのＵＲＬ、ＩＰアドレス及び／又は他の識別子が、新しいフィッシングサイト識別子である。

【００４７】

ある実施形態では、セキュリティ会社が新しいフィッシングサイト識別子を作成する。したがって、新しいフィッシングサイト識別子が作成されるとすぐに、セキュリティ会社において、新しいフィッシングサイト識別子をチェックするオペレーション２１２で新しいフィッシングサイト識別子が存在するか否かの判定が行われる。

【００４８】
他の実施形態では、新しいフィッシングサイト識別子は、例えばセキュリティ会社サーバ１５６から、ホストコンピュータシステム１０２にダウンロードされる。具体的には、例えば、ホストコンピュータシステム１０２の総合的セキュリティアプリケーションの一部であるフィッシング通知サービス（ＰＮＳ）アプリケーション１０６が、例えば、新しいフィッシングサイト識別子を含む更新を自動的にダウンロードするシマンテック社のＬＩＶＥＵＰＤＡＴＥ（ＴＭ）システムを使用して、セキュリティ会社サーバ１５６から定期的な更新を受信する。そして、新しいフィッシングサイト識別子を受信すると、新しいフィッシングサイト識別子をチェックするオペレーション２１２で、新しいフィッシングサイト識別子が存在するか否かの判定が行われる。

【００４９】
フィッシングサイトが新しく発見された場合は、上述したように、過去にユーザはフィッシング攻撃によって未知のフィッシングサイトにアクセスして重要情報を提供した可能性がある。したがって、新しいフィッシングサイト識別子が存在すると判定された場合は、新しいフィッシングサイト識別子をトランザクションレコードのサイト識別子と比較するオペレーション２１４において、新しいフィッシングサイト識別子を、保存されたトランザクションレコードに含まれるサイト識別子と比較する。

【００５０】
新しいフィッシングサイト識別子をトランザクションレコードのサイト識別子と比較するオペレーション２１４から、フローは、一致をチェックするオペレーション２１６へ進む。一致をチェックするオペレーション２１６では、新しいフィッシングサイト識別子のいずれかが、保存されたトランザクションレコードに含まれているサイト識別子のいずれかと一致するか否かの判定が行われる。別の言い方をすれば、新しいフィッシングサイト識別子の少なくとも１つが、保存されたトランザクションレコードに含まれているサイト識別子の少なくとも１つと一致するか否かの判定が行われる。一致すると判定された場合は、フローは、フィッシング通知を提供するオペレーション２１８へ進む。反対に、一致しないと判定された場合は、フローは、終了オペレーションへ進み処理を終了する、或いは、上記のチェックオペレーション２０４に戻って、サイトへ提供されるより重要な情報を待つ。

【００５１】
より詳しくは、一致しないと判定された場合は、ホストコンピュータシステム１０２のユーザが、最近になってフィッシングサイトであることが判明したサイトに、過去に重要情報を提供したことがないと判断される。したがって、さらなる措置を取ることなく、上述したように、フローは終了オペレーション２２２へ進む。

【００５２】
しかし、一致すると判定された場合は、ホストコンピュータシステム１０２のユーザが、現在は知られたフィッシングサイトに対して、過去に重要情報を提供したことがあると判断される。すなわち、ユーザは、以前に、重要情報を提供した時点ではフィッシングサイトであると知られていないフィッシングサイトに対して、重要情報を提供したことがある。したがって、フローは、一致をチェックするオペレーション２１６からフィッシング通知を提供するオペレーション２１８へ進む。

【００５３】
フィッシング通知を提供するオペレーション２１８では、ユーザが過去にフィッシングされたという、すなわち、重要情報を判明したフィッシングサイトへ提供したことがあるという、フィッシング通知が提供される。具体的には、フィッシング通知は、次の（１）～（５）の通知の１つ以上を含む。
（１）重要情報がフィッシングサイトへ提供された日付及び／又は時間。
（２）前記フィッシングサイトへ提供された重要情報。
（３）フィッシングサイトのサイト識別子（例えば、ＵＲＬ及び／又はＩＰアドレス）。
（４）フィッシングサイトの名前。

（５）フィッシングサイトによって偽装された（コピーされた）本物の商業者。

【００５４】

ある実施形態では、フィッシング通知は、下記のようなメッセージとして表示される。あなたが＜日付＞に＜ＵＲＬ＞ロケーションを介してフィッシングされたことをお知らせします。あなたは、＜商業者サイト＞と取引しようとして、＜フッシングサイト＞に実際に接続しました。成りすまし窃盗から自身を守るために、＜商業者＞とあなたのクレジットビューローに連絡することをお薦めします。

【００５５】

上記の例を続けると、ユーザは、そうと気付くことなく個人情報をだまし取られたとする。フッシングサイトが発見されると、新しく発見されたフィッシングサイトからユーザを守るべくセキュリティアプリケーションを可能にするために、新しいフィッシングＵＲＬが配布される。詳しく説明すると、ユーザが新しいフィッシングＵＲＬと関係するフィッシングサイトとトランザクションしようとした場合に、新しいフィッシングＵＲＬを使用して保護措置が実施される。

【００５６】

さらに、この実施形態では、新しいフィッシングＵＲＬを配布する際に、新しいフィッシングサイト識別子をチェックするオペレーション２１２で、新しいフィッシングサイト識別子が存在するか否かの判定が行われる。そして、新しいフィッシングサイト識別子をトランザクションレコードのサイト識別子と比較するオペレーション２１４で、新しいフィッシングＵＲＬが、保存されたトランザクションレコードのサイト識別子と比較される。一致をチェックするオペレーション２１６で、新しいフィッシングＵＲＬと保存されたトランザクションレコードのサイト識別子との間に一致すると判定された場合は、フィッシング通知作成オペレーション２１８でフィッシング通知が作成される。

【００５７】

このようにして、ホストコンピュータシステム１０２のユーザは、現在においてフィッシングサイトから保護されるだけでなく、過去にフィッシング攻撃の被害に遭ったことがある場合はフィッシング通知を受け取ることができる。さらに、前記フィッシング通知は、フィッシング攻撃に関連する成りすまし窃盗を防止する又は最小限に抑えるべく、フィッシング攻撃（例えばユーザのクレジットビューローへの接触など）の影響を減少させるための事前措置をユーザが講じるのに十分な情報を含んでいる。

【００５８】

ある実施形態では、オペレーション２１４、２１６は、セキュリティ会社で実施される。したがって、フィッシング通知を提供するオペレーション２１８では、フィッシング通知はセキュリティ会社からホストコンピュータシステム１０２へ例えば電子メール又は他の方法によって送信される。

【００５９】

他の実施形態では、オペレーション２１４、２１６は、上述したように、例えば、新しいフィッシングサイト識別子を受信した場合に、ホストコンピュータシステム１０２で実施される。この実施形態では、フィッシング通知は、フィッシング通知サービス（ＰＮＳ）アプリケーション１０６によって、ホストコンピュータシステム１０２のユーザやシステム管理者などへ提供される。フィッシング通知は、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行われる。また、フィッシング通知は、ファイルに記録される。

【００６０】

他の例では、フィッシング通知は、関心のある第三者へ提供される。例えば、フィッシング通知は、フィッシングサイトによって偽装された商業者、クレジットビューロー、又は法執行機関へ提供される。この例では、個人ユーザ情報を含まないフィッシング通知が提供されるので、ユーザの秘密情報は保護される。この情報は、フィッシング攻撃（使用されたフィッシング攻撃の種類を含む）のマッピングに使用される。

【００６１】

フィッシング通知を提供するオペレーション２１８から、フローは、随意的に、保護処置を実施するオペレーション２２０へ進む。或いは、直接、終了オペレーション２２２へ進む。保保護処置を実施するオペレーション２２０では、新しく発見されたフィッシングサイトからの保護を提供するために、保護処置が実施される。具体的には、フィッシングサイトに関連するあらゆるフィッシング電子メールがホストコンピュータシステム１０２から削除される、隔離される、又は他の方法で使用不能にされる。

【００６２】

保護処置を実施するオペレーション２２０から、フローは、終了オペレーション２２２へ進む。或いは、上記の、重要情報の或るサイトへの提供をチェックするオペレーション２０４へ戻る。

【００６３】

図３は、本発明の他の実施形態によるフィッシング通知方法３００を説明するためのフロー図である。図１、図２及び図３を共に参照して、プロセッサ１０８でフィッシング通知サービス（ＰＮＳ）アプリケーション１０６を実行すると、フィッシング通知方法３００が以下のように実施される。

【００６４】

図３のフィッシング通知方法３００における開始オペレーション２０２、新しいフィッシングサイト識別子をチェックするオペレーション２１２、フィッシング通知を提供するオペレーション２１８、保護処置を実施するオペレーション２２０、及び終了オペレーション２２２は、図２に示したフィッシング通知方法２００における新しいフィッシングサイト識別子をチェックするオペレーション２１２、フィッシング通知を提供するオペレーション２１８、保護処置を実施するオペレーション２２０及び終了オペレーション２２２と同様又は同一であるので、ここではその詳細な説明は省略する。

【００６５】

開始オペレーション２０２から、フローは、新しいフィッシングサイト識別子をチェックするオペレーション２１２へ進む。フィッシングサイト識別子が存在すると判定された場合は、フローは新しいフィッシングサイト識別子をチェックするオペレーション２１２から、新しいフィッシングサイト識別子をローカルサイト識別子と比較するオペレーション３１４へ進む。新しいフィッシングサイト識別子をローカルサイト識別子と比較するオペレーション３１４では、新しいフィッシングサイト識別子は、ホストコンピュータシステム１０２のローカルサイト識別子と比較される。

【００６６】

ある実施形態では、ローカルサイト識別子は、ホストコンピュータシステム１０２のウェブブラウザのキャッシュ（メモリ）に含まれているＵＲＬ及び／又はＩＰアドレスを含む。他の実施形態では、ローカルサイト識別子は、ホストコンピュータシステム１０２に保存された電子メールに含まれているＵＲＬ及び／又はＩＰアドレスを含む。一般に、ホストコンピュータシステム１０２のローカルサイト識別子は、ホストコンピュータシステム１０２上のＵＲＬ及び／又はＩＰアドレス及び／又は他のサイト識別子を含む。

【００６７】

新しいフィッシングサイト識別子をローカルサイト識別子と比較するオペレーション３１４から、フローは、一致をチェックするオペレーション３１６へ進む。一致をチェックするオペレーション３１６では、新しいフィッシングサイト識別子のいずれかがローカルサイト識別子のいずれかと一致するか否かの判定が行われる。一致すると判定された場合、フローは、前述したように実施されるフィッシング通知オペレーション２１８へ進む。反対に、一致しないと判定された場合、フローは、終了オペレーション２２２へ進む。或いは、新しいフィッシングサイト識別子をチェックするオペレーション２１２に戻って、新しいフィッシングサイト識別子を待つ。

【００６８】

図１に再び戻って、フィッシング通知サービス（ＰＮＳ）アプリケーション１０６は、コンピュータメモリ１１４に格納されている。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２つの組み合わせである。

【００６９】

また、フィッシング通知サービス（ＰＮＳ）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、これは一例にすぎない。フィッシング通知サービス（ＰＮＳ）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し可能にすることもできる。ある実施形態では、アプリケーションは一般に、任意の実行可能なコードと定義される。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うとき、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、当業者には明らかであろう。

【００７０】

クライアントサーバ構成のための本発明の実施形態について説明してきたが、本発明の実施形態は、任意の適切な手段、及び／又は、パーソナルコンピュータ、ワークステーション、ポータブル機器又はコンピュータ機器のネットワークを含むハードウェア構成を使用して実施し得る。また、他の実施形態では、例えば、ピアツーピア、ウェブベース、イントラネット、インターネットネットワーク構成などの、クライアントサーバ構成以外の他のネットワーク構成が使用される。

【００７１】

ここで、コンピュータプログラム製品は、本発明の実施形態によるコンピュータが読み出し可能なコードを格納又は移植するべく構成された媒体を含む。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、コンピュータハードドライブ、ネットワーク上のサーバ、及び、ネットワークを介して伝送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ある。別の実施形態では、コンピュータプログラム製品は、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、コンピュータハードドライブ、ネットワーク上のサーバ等の、コンピュータが読み出し可能なコードを格納するように構成された有形の媒体を含む。

【００７２】

図１に示すように、この媒体は、コンピュータシステム自体に属するものであり得る。しかしながら、前記媒体は、コンピュータシステムから取り出してもよい。例えば、フィッシング通知サービス（ＰＮＳ）アプリケーション１０６は、プロセッサ１０８とは物理的に異なる場所に存在するメモリ１３６に格納され得る。プロセッサ１０８は、メモリ１３６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実現することができる。或いは、モデム及びアナログライン、又はデジタルインタフェース及び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実現することができる。

【００７３】

より具体的には、ある実施形態では、ホストコンピュータシステム１０２及び／又はサーバコンピュータシステム１３０は、ポータブルコンピュータ、ワークステーション、双方向ページャ、携帯電話、デジタル無線電話、携帯情報端末、サーバコンピュータ、インターネット機器、又は本明細書中で説明された実施形態の少なくとも１つに従ってフィッシング通知サービス機能を実行し得る構成要素を備える他の任意のデバイスである。同様に、別の実施形態では、ホストコンピュータシステム１０２及び／又はサーバ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、双方向ページャ、携帯情報端末、サーバコンピュータ、又は本明細書中で説明され方法を実行するために相互接続されたこれらのデバイスの任意の組み合わせから構成される。

【００７４】

上記開示内容に基づき、本発明の一実施形態によるフィッシング通知サービス機能を、幅広い種類の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。加えて、フィッシング通知サービスの機能を、異なるデバイスのメモリに異なるモジュールとして格納することもできる。例えば、フィッシング通知サービス（ＰＮＳ）アプリケーション１０６

を、初めにサーバコンピュータシステム１３０に格納しておき、その後、必要に応じて、フィッシング通知サービス（ＰＮＳ）アプリケーション１０６の一部をホストコンピュータシステム１０２へ転送して、ホストコンピュータシステム１０２上に実行させることもできる。その結果、フィッシング通知サービス機能の一部が、サーバーコンピュータシステム１３０のプロセッサ１３４上で実行され、前記機能の他の部分がホストコンピュータシステム１０２のプロセッサ１０８上で実行されることになる。上記開示内容に基づき、当業者であれば、ユーザが関心のあるオペレーティングシステム及びコンピュータプログラム言語を用いて、様々な種類に物理的ハードウェア構成において本発明の様々な実施形態を実施することができる。

【００７５】

更なる別の実施形態では、フィッシング通知サービス（ＰＮＳ）アプリケーション１０６は、サーバコンピュータシステム１３０のメモリ１３６に格納される。フィッシング通知サービス（ＰＮＳ）アプリケーション１０６は、ネットワーク１２４を介してホストコンピュータシステム１０２のメモリ１１２に転送される。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む。モデムが使用される場合、ネットワーク１２４は通信ネットワークを含み、フィッシング通知サービス（ＰＮＳ）アプリケーション１０６は前記通信ネットワークを介してダウンロードされる。

【００７６】

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、上記の例示的な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に基づいて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】

【００７７】

【図１】本発明の一実施形態による、ホストコンピュータシステム上で実行されるフィッシング通知サービス（ＰＮＳ）アプリケーションを含むクライアントサーバシステムを示す図である。

【図２】本発明の一実施形態によるフィッシング通知方法２００を説明するためのフロー図である。

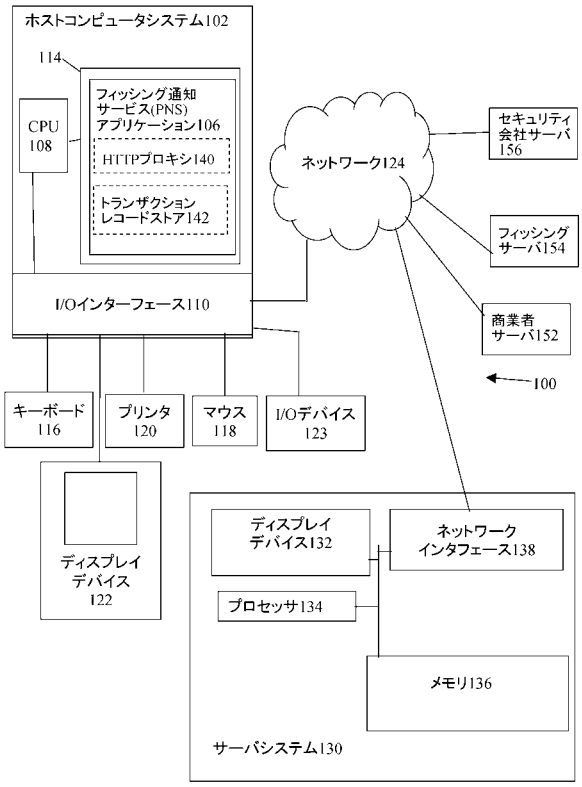
【図３】本発明の他の実施形態によるフィッシング通知方法３００を説明するためのフロー図である。

【符号の説明】

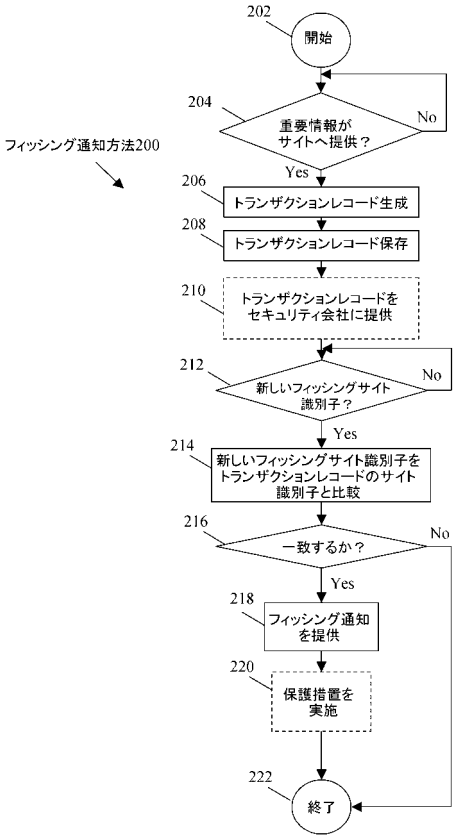
【００７８】

１００　クライアントサーバシステム
１０２　ホストコンピュータシステム
１０６　フィッシング通知サービス（ＰＮＳ）アプリケーション
１０８　ＣＰＵ
１１０　Ｉ／Ｏインタフェース
１１４　メモリ
１４０　ＨＴＴＰプロキシ
１４２　トランザクションレコードストア
１２４　ネットワーク
１３０　サーバシステム
１５２　商業者サーバ
１５４　フィッシングサーバ
１５６　セキュリティ会社サーバ

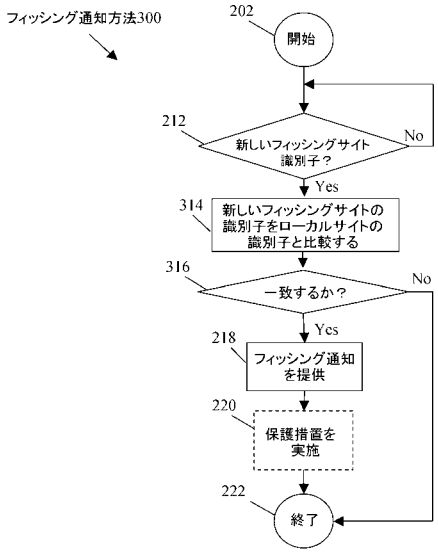
【図１】


ホストコンピュータシステム102
114
フィッシング通知
サービス(PNS)
アプリケーション106
CPU
108
HTTPプロキシ140
トランザクション
レコードストア142
I/Oインターフェース110
ネットワーク124
セキュリティ
会社サーバ
156
フィッシング
サーバ154
商業者
サーバ152
100
キーボード
116
プリンタ
120
マウス
118
I/Oデバイス
123
ディスプレイ
デバイス
122
ディスプレイ
デバイス132
ネットワーク
インタフェース138
プロセッサ134
メモリ136
サーバシステム130

【図２】


フィッシング通知方法200
202
開始
204
重要情報が
サイトへ提供？
No
Yes
206
トランザクションレコード生成
208
トランザクションレコード保存
210
トランザクションレコードを
セキュリティ会社に提供
212
新しいフィッシングサイト
識別子？
No
Yes
214
新しいフィッシングサイト識別子を
トランザクションレコードのサイト
識別子と比較
216
一致するか？
No
Yes
218
フィッシング通知
を提供
220
保護措置を
実施
222
終了

【図３】


フィッシング通知方法300
202
開始
212
新しいフィッシングサイト
識別子？
No
Yes
314
新しいフィッシングサイトの
識別子をローカルサイトの
識別子と比較する
316
一致するか？
No
Yes
218
フィッシング通知
を提供
220
保護措置を
実施
222
終了

フロントページの続き

(72)発明者　サラ・スーザン・ゴードン・フォード
アメリカ合衆国フロリダ州３２９３７・サテライトビーチ・バルセロナコート　６３０
(72)発明者　リチャード・エイ・フォード
アメリカ合衆国フロリダ州３２９３７・サテライトビーチ・バルセロナコート　６３０

Ｆターム(参考) 5B089 GB09　JA21　JA31　KA17
5B285 AA04　BA08　CA32　CB43