

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5508042号
(P5508042)

(45) 発行日 平成26年5月28日 (2014.5.28)

(24) 登録日 平成26年3月28日 (2014.3.28)

(51) Int. Cl. F I
G06Q 50/10 (2012.01) G O 6 Q 50/10
G06Q 30/02 (2012.01) G O 6 Q 30/02 1 3 0

請求項の数 8 (全 13 頁)

<p>(21) 出願番号 特願2010-10535 (P2010-10535) (22) 出願日 平成22年1月20日 (2010.1.20) (65) 公開番号 特開2011-150494 (P2011-150494A) (43) 公開日 平成23年8月4日 (2011.8.4) 審査請求日 平成24年10月19日 (2012.10.19)</p> <p>早期審査対象出願</p> <p>前置審査</p>	<p>(73) 特許権者 596155786 長嶋 克佳 東京都町田市原町田2-20-16</p> <p>(74) 代理人 100144048 弁理士 坂本 智弘</p> <p>(72) 発明者 長嶋 克佳 東京都渋谷区初台一丁目34番地14 株 式会社クローバー・ネットワーク・コム 内</p> <p>審査官 山本 雅士</p>
--	---

最終頁に続く

(54) 【発明の名称】 IPアクセスログ解析装置およびその方法

(57) 【特許請求の範囲】

【請求項1】

IPアドレス、このIPアドレスに対応する都道府県および市町村の住所情報を記憶する記憶装置と、

ユーザ端末からインターネット網を介して、同一の登録番号情報が所定期間内に複数のIPアドレスおよび住所から使用されているかに関連する条件指定情報、照会IPアドレス情報がアクセスされたアクセス日付情報、申込者の登録番号情報、照会住所情報、および前記ユーザ端末の照会IPアドレス情報を受信し、

前記照会IPアドレス情報のIPアドレスを検索キーとして前記記憶装置から前記住所情報を検索し前記照会IPアドレス情報の住所情報を判定するIP住所判定手段と、

前記IP住所判定手段による住所情報の判定結果と前記照会住所情報との一致または不一致に基づいて、前記照会IPアドレス情報の住所情報および/または前記照会住所情報を識別表示し前記登録番号情報を使用する申込者の信頼性の有無を報知する報知情報のほか、

前記照会住所情報、前記アクセス日付情報、前記登録番号情報、前記照会IPアドレス情報、およびマーケティングまたは偽装アクセス防止のセキュリティに関連する情報のうち、少なくとも1つの情報を、含むリスト情報を生成し、

前記条件指定情報に対応させて、前記リスト情報を前記インターネット網を介して前記ユーザ端末へ送信する判定データ送信手段と、

を備えるコンピュータを用いたIPアクセスログ解析装置。

10

20

【請求項 2】

前記登録番号情報は、クレジットカード番号または銀行口座番号であることを特徴とする請求項 1 に記載の IP アクセスログ解析装置。

【請求項 3】

IP アドレス、この IP アドレスに対応する都道府県および市町村の住所情報を記憶する記憶装置と、

申込者端末からインターネット網を介し、申込者の登録番号情報、照会住所情報、および前記申込者端末の照会 IP アドレス情報を受信し、

この照会 IP アドレス情報を検索キーとして前記記憶装置から前記住所情報を検索し、前記照会 IP アドレス情報の住所情報を判定する IP 住所判定手段と、を備えた IP アクセスログ解析装置において、

前記照会住所情報または前記申込者の登録番号情報に対応する住所情報と、照会された前記照会 IP アドレス情報の都道府県および市町村の住所情報とを突合せ、リアルタイムに、前記照会住所情報または前記登録番号情報に対応する住所情報と、前記照会 IP アドレス情報の住所情報との同一性を判定し、

前記 IP 住所判定手段による住所情報の判定結果と、前記照会住所情報または前記登録番号情報に対応する住所情報との同一性に基づいて、前記登録番号情報を使用する申込者の信頼性をディスプレイの表示画面に識別表示し、前記登録番号情報および前記照会住所情報が不正に使用されていないことが直ちに判断される、

ことを特徴とするコンピュータを用いた IP アクセスログ解析装置。

【請求項 4】

前記登録番号情報は、クレジットカード番号または銀行口座番号であることを特徴とする請求項 3 に記載の IP アクセスログ解析装置。

【請求項 5】

IP アドレス、この IP アドレスに対応する都道府県および市町村の住所情報を記憶する記憶ステップと、

ユーザ端末からインターネット網を介して、同一の登録番号情報が所定期間内に複数の IP アドレスおよび住所から使用されているかに関連する条件指定情報、照会 IP アドレス情報がアクセスされたアクセス日付情報、申込者の登録番号情報、照会住所情報、および前記ユーザ端末の照会 IP アドレス情報を受信し、

前記照会 IP アドレス情報の IP アドレスを検索キーとして前記記憶ステップから前記住所情報を検索し前記照会 IP アドレス情報の住所情報を判定するステップと、

前記照会 IP アドレス情報の住所情報を判定するステップによる住所情報の判定結果と前記照会住所情報との一致または不一致に基づいて、前記照会 IP アドレス情報の住所情報および / または前記照会住所情報を識別表示し前記登録番号情報を使用する申込者の信頼性の有無を報知する報知情報のほか、

前記照会住所情報、前記アクセス日付情報、前記登録番号情報、前記照会 IP アドレス情報、およびマーケティングまたは偽装アクセス防止のセキュリティに関連する情報のうち、少なくとも 1 つの情報を、含むリスト情報を生成し、

前記条件指定情報に対応させて、前記リスト情報を前記インターネット網を介して前記ユーザ端末へ送信するステップと、

を備えるコンピュータを用いた IP アクセスログ解析方法。

【請求項 6】

前記登録番号情報は、クレジットカード番号または銀行口座番号であることを特徴とする請求項 5 に記載の IP アクセスログ解析方法。

【請求項 7】

IP アドレス、この IP アドレスに対応する都道府県および市町村の住所情報を記憶する記憶ステップと、

申込者端末からインターネット網を介し、申込者の登録番号情報、照会住所情報、および前記申込者端末の照会 IP アドレス情報を受信し、

この照会 I P アドレス情報を検索キーとして前記記憶ステップから前記住所情報を検索し、前記照会 I P アドレス情報の住所情報を判定するステップと、を備えた I P アクセスログ解析方法において、

前記照会住所情報または前記申込者の登録番号情報に対応する住所情報と、照会された前記照会 I P アドレス情報の都道府県および市町村の住所情報とを突合せ、リアルタイムに、前記照会住所情報または前記登録番号情報に対応する住所情報と、前記照会 I P アドレス情報の住所情報との同一性を判定し、

前記照会 I P アドレス情報の住所情報を判定するステップによる住所情報の判定結果と、前記照会住所情報または前記登録番号情報に対応する住所情報との同一性に基づいて、前記登録番号情報を使用する申込者の信頼性をディスプレイの表示画面に識別表示し、前記登録番号情報および前記照会住所情報が不正に使用されていないことが直ちに判断される、

10

ことを特徴とするコンピュータを用いた I P アクセスログ解析方法。

【請求項 8】

前記登録番号情報は、クレジットカード番号または銀行口座番号であることを特徴とする請求項 7 に記載の I P アクセスログ解析方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、I P アクセスログ解析装置およびその方法に関する。特に、ウェブサイトが受信するユーザ端末のインターネットプロトコルの I P アクセスログ情報を検索キー情報として、I P アドレスデータベースに記憶している I P アドレスおよびエリア情報を抽出し、ユーザ端末のアクセス地域を特定する検証結果ファイルを生成するコンピュータを用いた I P アクセスログ解析装置およびその方法に関する。

20

【背景技術】

【0002】

従来の I P アクセスログ解析装置は、企業の名称、住所、電話番号、URL の企業固有情報を、その企業の I P アドレスあるいはドメイン名と対応づけて登録している企業情報データベースを利用して、インターネット網を介してアクセスしているコンピュータ端末から受信したインターネットプロトコルの I P アクセスログ情報を使用し、ウェブサイトへのアクセスログを様々な条件下で解析し、その結果をウェブサイトの運営者であるユーザに提供して、ユーザが見込み客の判断を的確に行える I P アクセスログ解析装置が知られている（特許文献 1）。

30

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2008 - 97259 号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、従来の I P アクセスログ解析装置では、企業の I P アドレスあるいはドメイン名と対応づけて登録している企業情報データベースを利用しているため、個人ユーザがユーザ端末からインターネットを介してウェブサイトへアクセスしても、ユーザ端末の I P アドレスと企業情報データベースに記憶している I P アドレスとの突合せ処理が困難であり、I P アクセスログを企業が提供するウェブサイトへ収集しても、その情報価値が著しく低下する。

40

【0005】

そして、企業が提供するウェブサイトは、電子商取引を実行する場合には、ユーザに対して発行する I D 情報およびパスワード情報をユーザ端末からインターネット網を介して受信し、I D およびパスワード情報がウェブサイト側の認証情報と一致することを条件に

50

電子商取引を許可する。つまり、ユーザ端末がどの地域からアクセスしているのが不明であるにもかかわらず電子商取引を実行するため、悪意の第三者が他人のクレジットカード番号、銀行口座番号を使用して詐欺行為を働いても、直ちに電子商取引を停止することが困難であり、新たなセキュリティ技術の提供が望まれていた。したがって、IPアクセスログ情報を解析して新たなセキュリティ技術を提供することが本発明の技術的な課題である。

【0006】

本発明は、上記課題に対応してなされたものであり、IPアクセスログ情報からユーザ端末のIPアドレスの地域情報を抽出し、所定期間内に同一の登録番号（例えば、クレジットカード番号または銀行口座番号）が複数のIPアドレスから使用されているのか、単一のIPアドレスから使用されているのか、登録番号の使用状況を表示するリストを出力し記憶装置に記憶するコンピュータを用いたIPアクセスログ解析装置を提供することを目的とする。

10

【0007】

そして、IPアクセスログ情報からユーザ端末のIPアドレスの地域情報を抽出し、所定期間内に同一のIPアドレスから複数の登録番号が使用されているのか、登録番号の使用状況を表示するリストを出力し記憶装置に記憶するコンピュータを用いたIPアクセスログ解析装置を提供することを目的とする。

【0008】

ここで、IPアクセスログ情報とは、特定のウェブサイトにはアクセスしている総カウント数（COUNT）、ユーザ端末のアクセス時間（TIME）、ユーザ端末のIPアドレス（ADDR = [203.141.xxx.x x x]）、ユーザ端末のホストネーム（HOST = [ppp123.xkcom.ne.jp]）、ユーザ端末のブラウザ（AGENT = [Mozilla/3.01 [ja] (Win95; l)]）、リンク元情報（REFER = [http://www.xxxxxx.co.jp/link/]）を含み、このユーザ端末情報がウェブサイト側の記憶装置に記録される。

20

【0009】

IPアドレスとは、インターネットやイントラネットのようなIPネットワーク網に接続されたコンピュータや通信機器に割り当てられた識別番号である。この識別番号は唯一無二のものであり世界中のインターネット網からコンピュータや通信機器を識別できる電話番号に相当する。インターネット網では識別番号の数値に重複が生じないように、IPアドレスの割り当て管理業務を各国のネットワークインフォメーションセンタNICが実行している。ウェブサイトの管理者は、ウェブサイトにはアクセスしているユーザ端末のIPアドレスを分析することにより、ユーザ端末の設置場所、インターネット網の接続環境および接続方法をウェブサイトの運営者が認識することができる。

30

【課題を解決するための手段】

【0010】

上記目的を達成するために、本発明のコンピュータを用いたIPアクセスログ解析装置は、例えば、図1に示すように、IPアドレス、このIPアドレスに対応する都道府県および市町村の住所情報を記憶する記憶装置16と、ユーザ端末からインターネット網12を介して、同一の登録番号情報が所定期間内に複数のIPアドレスおよび住所から使用されているかに関連する条件指定情報、照会IPアドレス情報がアクセスされたアクセス日付情報、申込者の登録番号情報、照会住所情報、および前記ユーザ端末の照会IPアドレス情報を受信し、前記照会IPアドレス情報のIPアドレスを検索キーとして前記記憶装置から前記住所情報を検索し前記照会IPアドレス情報の住所情報を判定するIP住所判定手段18（CPU22で実行するソフトウェアプログラム）と、前記IP住所判定手段による住所情報の判定結果と前記照会住所情報との一致または不一致に基づいて、前記照会IPアドレス情報の住所情報および/または前記照会住所情報を識別表示し前記登録番号情報を使用する申込者の信頼性の有無を報知する報知情報のほか、前記照会住所情報、前記アクセス日付情報、前記登録番号情報、前記照会IPアドレス情報、およびマーケティングまたは偽装アクセス防止のセキュリティに関連する情報のうち、少なくとも1つ

40

50

の情報を、含むリスト情報を生成し、前記条件指定情報に対応させて、前記リスト情報を前記インターネット網を介して前記ユーザ端末へ送信する判定データ送信手段（CPU 22で実行するソフトウェアプログラム）と、を備える。

【0011】

そして、IPアクセスログ解析装置14は、アクセス日付情報、登録番号情報、照会IPアドレス情報に対応させた住所情報付きリスト情報をユーザ端末へ送信する。ユーザ端末10の使用者は、住所情報付きリスト情報を参照してマーケティング情報または偽装アクセス防止のセキュリティ情報として活用でき、警告情報（照会住所又はIPアドレスの住所を強調表示タグ）を含むリスト情報を参照して電子商取引申込者の信頼性を確認することができる。

10

【0012】

また、コンピュータを用いたIPアクセスログ解析装置14は、IPアドレス、このIPアドレスに対応する都道府県および市町村の住所情報を記憶する記憶装置16と、申込者端末30a、30bからインターネット網を介し、申込者の登録番号情報、照会住所情報、および前記申込者端末の照会IPアドレス情報を受信し、この照会IPアドレス情報を検索キーとして前記記憶装置から前記住所情報を検索し、前記照会IPアドレス情報の住所情報を判定するIP住所判定手段18と、を備えたIPアクセスログ解析装置において、前記照会住所情報または前記申込者の登録番号情報に対応する住所情報と、照会された前記照会IPアドレス情報の都道府県および市町村の住所情報とを突合せ、リアルタイムに、前記照会住所情報または前記登録番号情報に対応する住所情報と、前記照会IPアドレス情報の住所情報との同一性を判定し、前記IP住所判定手段による住所情報の判定結果と、前記照会住所情報または前記登録番号情報に対応する住所情報との同一性に基づいて、前記登録番号情報を使用する申込者の信頼性をディスプレイの表示画面32a、32bに識別表示し、前記登録番号情報および前記照会住所情報が不正に使用されていないことが直ちに判断される。

20

【0013】

これにより、IPアクセスログ解析装置14の使用者は、表示画面32a、32bに表示されるIP住所判定手段18の判定結果と照会住所情報との同一性を確認することができ、登録番号情報を使用する申込者の信頼性の有無を表現する判定結果に基づいて、受信した登録番号情報、照会住所情報が不正に使用されていないか直ちに判断することができる。

30

【発明の効果】

【0014】

本発明のコンピュータを用いたIPアクセスログ解析装置によれば、照会IPアドレスの住所情報に対応するアクセス日付情報、登録番号情報をリスト情報として提供することができるので、同一登録番号が同日に複数のIPアドレスおよび住所から使用されているか、同一照会IPアドレスおよび住所から複数の登録番号が使用されているか、所定期間内に複数の照会IPアドレスおよび住所から同一登録番号が使用されているか、何れか1つのリスト情報を条件指定情報により指定しているため、ユーザ端末の住所情報やアクセス日付けや照会住所情報との不一致を識別表示する警告情報を参照し、直ちに正規または不正アクセスの状態を把握することができる。

40

【図面の簡単な説明】

【0015】

【図1】本発明のIPアクセスログ解析装置のブロック図。

【図2】本発明のIPアクセスログ解析装置の動作シーケンスを示す図。

【図3】本発明のIPアクセスログ解析装置を金融システムに利用するブロック図。

【発明を実施するための形態】

【0016】

本発明の実施形態を図1を参照しながら説明する。本実施形態のIPアクセスログ解析装置14は、概略的には、コンピュータ24にIP住所判定手段18および判定データ送

50

信手段 20 を設け、IP アドレスに対応する住所情報を記憶する記憶装置 16 を接続し、コンピュータ 24 に設けられた CPU 22 により記憶装置 16、IP 住所判定手段 18 および判定データ送信手段 20 を制御する。IP アクセスログ解析装置 14 とユーザ端末 10 とはインターネット網 12 を介して情報を相互に伝送することにより、ユーザ端末 10 から受信するリクエスト情報に含まれる IP アクセスログを解析し、この解析結果をユーザ端末 10 へ返信することができる。

【0017】

図 1 に示す本実施形態の IP アクセスログ解析装置 14 は、IP アドレスに対応する住所情報を蓄積する IP アドレスデータベース DB を記憶する記憶装置 16 (例えば、ハードディスク) に接続され、内部に CPU 22 および不図示のメモリ、I/O、コンピュータソフトウェアプログラムを記憶する記憶部を備え、CPU 22 がコンピュータソフトウェアプログラムを実行し IP 住所判定手段と判定データ送信手段を機能させる。

10

【0018】

記憶装置 16 は、IP アドレスに対応する住所(位置)情報として、国、地方、都道府県、市町村、市外局番、経緯緯度を特定する情報、および IP アドレスに対応する接続環境情報として、ドメイン、回線種別、プロキシ利用有無を特定する情報を IP アドレスデータベース DB として記憶する。

【0019】

例えば、インターネットサービスプロバイダ(以下、「ISP」と略記する)の IP アドレス「202.234.1.10」に対応する住所情報は北海道、接続環境情報は ISDN 回線を特定することができる。同様に、ISP の IP アドレス「202.234.2.100」に対応する住所情報は東京、接続環境情報は FTTN 回線を特定ことができ、IP アドレス「202.234.3.200」に対応する住所情報は大阪、接続環境情報は ADSL 回線を特定することができる。

20

【0020】

ただし、本発明は、記憶装置 16 に記憶する IP アドレスデータベース DB に限定するものではなく、例えば、IP アクセスログ解析装置 14 は、インターネット網 12 を介して不図示のウェブサーバの IP アドレスデータベース DB から住所情報および接続環境情報をリアルタイムに受信して利用することもできる。

【0021】

図 1 および図 2 を参照し、IP アクセスログ解析装置 14 の動作について説明する。

30

【0022】

IP アクセスログ解析装置 14 は、ユーザ端末 10 からインターネット網 12 を介してリクエスト情報を受信し IP アクセスログ解析装置 14 のメモリ領域に入力する。このリクエスト情報を XML 仕様で例示する。ステップ S1 ではユーザ端末 10 から、XML のバージョン、認証情報「ID = xxx、PASS = xxx」、照会 IP アドレス「163.135.172.4」、都道府県情報「神奈川県」、市町村情報「川崎市」、接続環境情報「FTTN」、都道府県コード「90」、市町村コード「95」、接続環境コード「85」を記述するリクエスト情報をインターネット網 12 を介して IP アクセスログ解析装置 14 が受信しメモリ領域に入力する。次に、CPU 22 は認証情報と記憶装置 16 の中に記憶したアカウント情報と突合せ一致することを条件として CPU 22 が IP ログ情報入力処理を実行する。例示したリクエスト情報は照会 IP アドレスの一部を示すものでユーザ端末から後続の照会 IP アドレスを複数受信する。

40

【0023】

IP アクセスログ解析装置 14 は、XML 仕様の他に CSV 仕様のリクエスト情報をユーザ端末 10 からインターネット網 12 を介して受信しメモリ領域に入力することもできる。この場合、IP アクセスログ解析装置 14 とユーザ端末 10 との間でインターネット網 12 を介して認証処理を完了する。IP アクセスログ解析装置 14 はユーザ端末 10 から条件指定情報、IP アクセスログの収集日付情報、支店名情報(省略可能)、登録番号情報、照会 IP アドレス情報、顧客登録の都道府県名情報、顧客登録の市町村名情報を

50

インターネット網 12 を介して受信する。

【0024】

IPアクセスログ解析装置 14 は、ステップ S2 において、IP住所判定手段 18 を機能させリクエスト情報の中の照会 IP アドレス「163.135.172.4」をピックアップし検索キーに使用する。この検索キーと一致する IP アドレスに対応する住所情報を記憶装置 16 から読み出す。

【0025】

IP住所判定手段 18 は、照会 IP アドレス「163.135.172.4」と完全に一致する IP アドレスが記憶装置 16 内でヒット（一致）しなくても、先頭アドレス「163」、第2アドレス「135」、および第3アドレス「172」が一致した場合は、住所情報として都道府県および市町村の情報を取得できる。

10

【0026】

IP住所判定手段 18 は、処理をステップ S3 に移行させ、ユーザ端末 10 から受信するリクエスト情報のすべての照会 IP アドレスを記憶装置 16 内の IP アドレスデータベースに問い合わせ解析が完了したか否かを判定する。

【0027】

IPログ解析完了の条件は、リクエスト情報内の「End Of File」の読み出しを検知してすべての照会 IP アドレスの IP ログ解析完了と判定してもよく、ユーザ端末 10 から受信する照会 IP アドレスの最大値に達した段階で IP ログ解析完了と判定してもよい。IP住所判定手段 18 はステップ S3 の IP ログ解析完了の判定結果「Y」が出力されるまでステップ S2 に分岐して（判定結果 = N）、住所情報抽出処理を CPU 22 がタイムアップするまで繰り返す。

20

【0028】

上述した条件指定情報は、検証ルール ID を「R00」から「R07」の種類から選択できる。例えば、検証ルール ID「R00」は、ユーザ登録住所と異なる IP アドレス住所からのアクセス検証を実行する。

【0029】

検証ルール ID「R01」は、同じ登録番号（クレジットカード番号または銀行口座番号）が同一日で複数の IP アドレスから使用されているアクセス検証を実行する。

【0030】

検証ルール ID「R02」は、同じ登録番号（クレジットカード番号または銀行口座番号）を用いて複数の県（参照 IP アドレスから判明）からのアクセス検証を実行する。

30

【0031】

検証ルール ID「R03」は、同じ照会 IP アドレス（ドメイン名を用いてもよい）から複数の登録番号（クレジットカード番号または銀行口座番号）が使用されるアクセス検証を実行する。

【0032】

検証ルール ID「R04」は、複数の場所（参照 IP アドレスから判明）から同一登録番号（クレジットカード番号または銀行口座番号）を利用する購入支払があるアクセス検証を実行する。

40

【0033】

検証ルール ID「R05」は、ユーザ端末 10 を管理する企業が管理するブラック IP リストに登録されているサイト（ドメイン名または IP アドレス）からのアクセス検証を実行する。

【0034】

検証ルール ID「R06」は、日本以外からのアクセス検証の中から何れか1つを選択することができる。ただし本発明は、7種類の検証ルールに限定されず参照 IP アドレスの検索キーを用いた他のカスタマイズされた検証ルール ID を追加することもできる。

【0035】

IP住所判定手段 18 は、IPログ解析完了の判定結果「Y」を検出すると、ステップ

50

S 4 の IP ログ解析結果表示処理を実行する。この場合、IP 住所判定手段 18 はインターネット網 12 を介してユーザ端末 10 に IP ログ解析結果をディスプレイ（図示せず）に表示することができる。ディスプレイには、IP 住所判定手段 18 の判定結果と照会住所情報との不一致を識別表示する警告情報を表示する。

【0036】

「警告情報」は、照会住所の文字列を強調表示（bold 又はアンダーライン）してもよく、住所不一致の登録番号を表示する行を上又は下の行の背景色と異なる背景色を指定して表示することにより、使用者に対して容易に識別させることができる。

【0037】

また、「警告情報」は、照会住所の文字列に代えて判定結果による IP アドレスの住所の文字列を表示してもよい。要は、照会住所と IP アドレスの住所が一致しない事象を使用者に警告できる手段を任意に設定することができる。

【0038】

さらに、IP 住所判定手段 18 をユーザ企業へ設置する形態では IP 住所判定手段 18 のディスプレイ（図示せず）に上述した形態で表示することもできる。IP ログ解析結果のリスト情報を次の表に例示する。

【0039】

【表 1】

検出ID	日付時刻	支店名	口座番号	IPアドレス	Fメイン名	都道府県名	回線種別
R01	09/08/21	XXX	002	45.244.204.5 52	yournet.ne.jp	新潟県	その他 判定不明
R01	09/08/21	XXX	002	58.0.49.8 52	infoweb.ne.jp	岐阜県	FTTH
R01	09/08/21	XXX	009	58.3.75.2 52	bbiq.jp	福岡県	FTTH
R01	09/08/20	XXX	002	45.244.204.5 52	yournet.ne.jp	新潟県	その他 判定不明
R01	09/08/20	XXX	009	58.3.75.2 52	bbiq.jp	福岡県	FTTH
R01	09/08/21	XXX	002	45.244.204.5 52	yournet.ne.jp	新潟県	その他 判定不明
R01	09/08/21	XXX	002	58.0.49.8 52	infoweb.ne.jp	岐阜県	FTTH
R01	09/08/21	XXX	009	58.0.65.7 52	infoweb.ne.jp	埼玉県	FTTH
R01	09/08/21	ZZZ	010	59.145.58.25 52	dion.ne.jp	東京都	FTTH
R01	09/08/21	ZZZ	010	202.217.44.87 52	primestage.net	東京都	FTTH

【0040】

表 1 は、検証ルール ID 「R 0 1」の IP ログ解析結果である。最上段のタイトル欄には、左から検証ルール ID 「検出 ID」、参照 IP アドレスがウェブサイトへアクセスした日付け「日付時刻」、金融機関の「支店名」、金融機関の「口座番号」、参照 IP アドレスの「IP アドレス」、参照 IP アドレスの「ドメイン名」、住所情報の「都道府県」、参照 IP アドレスが使用した「回線種別」が表示され、各タイトルに該当する情報がリスト情報として表示されている。表 1 では、同じ口座番号が同一日で複数の参照 IP アドレスおよび住所からのアクセスを検証している。住所が一致しない行のリスト情報は、「警告情報」付きで表示する。

【0041】

10

20

30

【表 2】

検出ID	日付時刻	支店名	口座番号	IPアドレス	ドメイン名	都道府県名	回線種別
R02	09/08/24	ZYX	001	222.230.191.129/32	kinotrope.co.jp	石川県	FTTH
R02	09/08/24	XVZ	001	222.230.191.129/32	kinotrope.co.jp	福井県	FTTH
R02	09/08/24	TSR	001	222.230.138.117/32	gol.ne.jp	神奈川県	FTTH
R02	09/08/24	QPO	001	222.230.138.117/32	gol.ne.jp	新潟県	FTTH
R02	09/08/24	LKN	001	219.97.232.97/32	kikumasamune.co.jp	奈良県	FTTH
R02	09/08/24	OPQ	001	219.97.232.97/32	kikumasamune.co.jp	和歌山県	FTTH
R02	09/08/24	RST	001	219.97.232.97/32	kikumasamune.co.jp	鳥取県	FTTH
R02	09/08/24	JK	001	219.97.232.97/32	kikumasamune.co.jp	兵庫県	FTTH
R02	09/08/24	WVU	001	222.230.138.117/32	gol.ne.jp	東京都	FTTH
R02	09/08/24	UVW	001	222.230.191.129/32	kinotrope.co.jp	東京都	FTTH

10

【0042】

表2は、検証ルールID「R02」のIPログ解析結果である。最上段のタイトル欄には、左から検証ルールID「検出ID」、参照IPアドレスがウェブサイトへアクセスした日付け「日付時刻」、金融機関の「支店名」、金融機関の「口座番号」、参照IPアドレスの「IPアドレス」、参照IPアドレスの「ドメイン名」、住所情報の「都道府県」、参照IPアドレスが使用した「回線種別」が表示され、各タイトルに該当する情報がリスト情報として表示されている。表2では、同じ口座番号が同一日で複数の参照IPアドレスおよび住所からのアクセスを検証している。また、住所が一致しない行のリスト情報は、「警告情報」付きで表示する。

20

【0043】

【表 3】

検出ID	日付時刻	支店名	口座番号	IPアドレス	ドメイン名	都道府県名	回線種別
R03	09/08/24	XXY	002	58.0.49.8/32	info.web.ne.jp	岐阜県	FTTH
R03	09/08/24	XXN	008	58.0.55.7/32	info.web.ne.jp	埼玉県	FTTH
R03	09/08/24	XXN	001	58.0.49.8/32	info.web.ne.jp	岐阜県	FTTH
R03	09/08/24	XXN	006	58.0.55.7/32	info.web.ne.jp	埼玉県	FTTH
R03	09/08/24	XXN	002	58.0.49.8/32	info.web.ne.jp	岐阜県	FTTH
R03	09/08/24	XXY	009	58.0.55.7/32	info.web.ne.jp	埼玉県	FTTH
R03	09/08/24	XXN	009	58.0.55.7/32	info.web.ne.jp	埼玉県	FTTH
R03	09/08/24	UVV	009	58.0.55.7/32	info.web.ne.jp	埼玉県	FTTH
R03	09/08/24	JK	001	219.97.232.97/32	kikumasamune.co.jp	兵庫県	FTTH
R03	09/08/24	LKN	001	219.97.232.97/32	kikumasamune.co.jp	兵庫県	FTTH
R03	09/08/24	OPQ	001	219.97.232.97/32	kikumasamune.co.jp	兵庫県	FTTH
R03	09/08/24	RST	001	219.97.232.97/32	kikumasamune.co.jp	兵庫県	FTTH
R03	09/08/24	AAA	001	222.230.138.117/32	gol.ne.jp	東京都	FTTH

30

【0044】

表3は、検証ルールID「R03」のIPログ解析結果である。最上段のタイトル欄には、左から検証ルールID「検出ID」、参照IPアドレスがウェブサイトへアクセスした日付け「日付時刻」、金融機関の「支店名」、金融機関の「口座番号」、参照IPアドレスの「IPアドレス」、参照IPアドレスの「ドメイン名」、住所情報の「都道府県」、参照IPアドレスが使用した「回線種別」が表示され、各タイトルに該当する情報がリスト情報として表示されている。表3では、同じ参照IPアドレス(ドメイン名)から複数の口座番号が使用されるアクセスを検証している。また、住所が一致しない行のリスト情報は、「警告情報」付きで表示する。

40

【0045】

【表 4】

検出ID	日付時刻	支店名	口座番号	IPアドレス	ドメイン名	都道府県名	回線種別
R04	09/08/21	NXX	002	43.244.204.5/32	youmet.ne.jp	新潟県	その他 判定不明
R04	09/08/21	NXX	002	59.0.49.8/32	mfoweb.ne.jp	岐阜県	FTTH
R04	09/08/21	NXX	009	59.3.75.2/32	bbiq.jp	福岡県	FTTH
R04	09/08/20	NXX	002	43.244.204.5/32	youmet.ne.jp	新潟県	その他 判定不明
R04	09/08/20	NXX	009	59.3.75.2/32	bbiq.jp	福岡県	FTTH
R04	09/08/24	NXX	002	43.244.204.5/32	youmet.ne.jp	新潟県	その他 判定不明
R04	09/08/24	NXX	002	59.0.49.8/32	mfoweb.ne.jp	岐阜県	FTTH
R04	09/08/24	NXX	009	59.0.65.7/32	mfoweb.ne.jp	埼玉県	FTTH
R04	09/08/24	ZZZ	010	59.145.56.25/32	dion.ne.jp	東京都	FTTH
R04	09/08/24	ZZZ	010	202.217.44.85/32	primestage.net	東京都	FTTH

10

【0046】

表4は、検証ルールID「R04」のIPログ解析結果である。最上段のタイトル欄には、左から検証ルールID「検出ID」、参照IPアドレスがウェブサイトへアクセスした日付け「日付時刻」、金融機関の「支店名」、金融機関の「口座番号」、参照IPアドレスの「IPアドレス」、参照IPアドレスの「ドメイン名」、住所情報の「都道府県」、参照IPアドレスが使用した「回線種別」が表示され、各タイトルに該当する情報がリスト情報として表示されている。表4では、複数の参照IPアドレスの場所（住所）から同一口座番号の使用による購入支払いがあるアクセスを検証している。また、住所が一致しない行のリスト情報は、「警告情報」付きで表示する。

20

【0047】

IPアクセスログ解析装置14は、ステップS4において、ユーザ端末10から指定された表1乃至表4の何れか1つの検証表示情報をインターネット網12を介してユーザ端末10へ送信してから、処理をステップS5に移行させ検証結果ファイル送信処理を実行する。

【0048】

IP電話番号調査装置10は、ユーザ端末10から指定された検証表示情報に対応させて、XML仕様またはCSV仕様の検証結果ファイルを生成し記憶装置16に記憶させるとともに、この検証結果ファイルをインターネット網12を介してユーザ端末10へ送信することで、IPアクセスログ解析処理を完了させる。

30

【0049】

本実施形態のIPアクセスログ解析装置14によれば、IPログ解析結果から、嘘の住所でのいたずら申込を検出することができ、同一参照IPアドレスからの多数の登録番号（銀行口座）開設を検出でき、不正の確率が高い地域や身元を隠しているあやしい参照IPアドレスからの登録を検出でき、海外からの申込を検出して海外からのウェブサイトのアクセスを拒絶することができるので、電子商取引の口座開設段階で与信審査により不正を検出できる。

【0050】

また、IPアクセスログ解析装置14によれば、電子商取引の段階でも同様に高リスク参照IPアドレスからの取引を検出し、不正な口座番号の利用を検出し、自宅や勤務先以外の参照IPアドレスの住所検出により成りすまし取引を防止し、中間者攻撃やセッションハイジャックを参照IPアドレスの住所判定により検出することができる。

40

【0051】

[IPアクセスログ解析装置の運用]

上述したように、IPアクセスログ解析装置14により、ユーザ端末10から要求されたIPアドレス情報を検索キーとして住所情報を判定することができる。そして、IPアクセスログ解析装置14を金融業者のコンピュータシステムに組み込むことで本発明の他の実施形態による運用を提供することもできる。

【0052】

50

図3を参照して、他の実施形態のコンピュータを用いたIPアクセスログ解析装置の運用を説明する。図示したIPアクセスログ解析装置14は、金融業者28（例えば、クレジット会社）の施設内に設置する。

【0053】

IPアクセスログ解析装置14は、IPアドレス、このIPアドレスに対応する都道府県および市町村の住所情報を記憶する記憶装置16（図1）と、申込者端末30a、30bからインターネット網12を介して登録番号情報、照会住所情報、及び照会IPアドレス情報を受信し、この照会IPアドレス情報を検索キーとして記憶装置16（図1）から住所情報を検索し照会IPアドレスの住所を判定するIP住所判定手段18（図1）と、IP住所判定手段18（図1）の判定結果と照会住所情報との同一性に基づいて、登録番号情報を使用する申込者の信頼性の有無を表現する判定結果をディスプレイの表示画面32a、32bに表示する。

10

【0054】

金融業者28は、不図示のウェブサイトを設定、このウェブサイトインターネット網12を介してアクセスする申込者端末30a又は申込者端末30bのIPアドレスを取得する。このIPアドレスは、TCP/IPの規格によりウェブサイトから申込者端末30a、30bにコンテンツを返信するために使用されるアクセス元の申込者端末を特定する情報である。

【0055】

IPアクセスログ解析装置14は、申込者端末30a又は申込者端末30bのIPアドレスを検索キーとして記憶装置16（図1）から対応する住所情報を検索し、アクセスしている申込者端末のIPアドレスの住所を判定する。

20

【0056】

金融業者28のウェブサイトは、例えば、融資を実行する条件として申込者端末30a又は申込者端末30bから登録番号情報（例えば、カードローン番号）、申込者の登録住所情報、生年月日情報を含む申込情報及び申込端末のIPアドレス情報を受信し、ウェブサイトへ接続又は組み込まれたIPアクセスログ解析装置14に申込情報及び申込端末のIPアドレス情報を転送する。

【0057】

そして、IPアクセスログ解析装置14は、申込情報の中の登録住所情報と申込端末のIPアドレス情報とを突合して両者が一致するか不一致か判定する。例えば、申込者Aが申込者端末30aからインターネット網12を介して金融業者28のウェブサイトをアクセスしている場合は、IP住所判定手段18（図1）がリアルタイムに申込者Aの申込情報に記述された登録住所又は登録番号に対応する住所（例えば、金融業者28のコンピュータに登録されている住所）がIPアドレスの住所と一致するか否かを判定する。

30

【0058】

IPアクセスログ解析装置14は、IP住所判定手段18（図1）の判定結果をIPアクセスログ解析装置14に接続するディスプレイの表示画面32aに表示する。例えば、IP住所判定手段18（図1）の判定結果が一致する場合は「OK」の許可報知を表示し、不一致のときは「NO」の否認報知を表示する。なお、申込者Bが申込者端末30bを使用して融資申込した場合は、IP住所判定手段18（図1）の判定結果をIPアクセスログ解析装置14に接続するディスプレイの表示画面32bに表示する。

40

【0059】

これにより、複数の申込者が夫々の申込者端末から金融業者28のウェブサイトへアクセスしても、リアルタイムにアクセス元の申込者端末のIPアドレス情報に基づき、このIPアドレス情報に対応する住所を都道府県又は市町村のレベルまで特定し、登録番号に対応する住所又は受信する申込情報の中の住所と突合せせることで、融資の実行条件である住所の正当性を判定することにより、不正な融資申込と正当な申込を迅速に判断することができる。

【0060】

50

他の実施形態では、金融業者 28 を例示して説明したが、本発明はこれに限定するものではなく、インターネット網 12 を介する電子商取引業や銀行業や保険業にも適用することができる。

【0061】

本実施形態をインターネット網に対応させて説明したが、本発明は上述の実施形態に限定されることはなく、通信回線網の発達に応じて適宜構成要件を変更できることは言うまでもない。

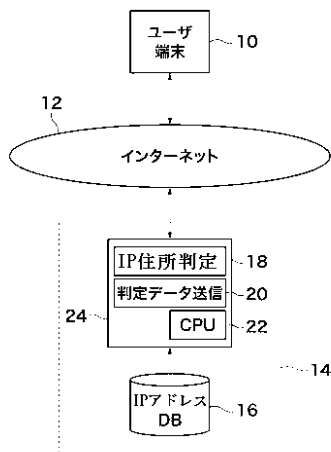
【符号の説明】

【0062】

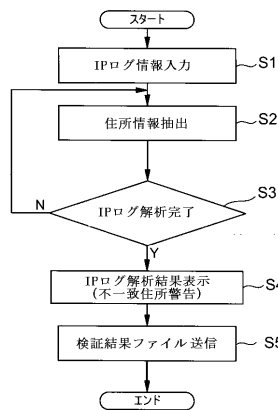
10・・・ユーザ端末、12・・・インターネット網、14・・・IPアクセスログ解析装置、16・・・記憶装置、18・・・IP住所判定手段、20・・・判定データ送信手段、22・・・中央制御装置CPU、24・・・コンピュータ、30a・・・申込者端末、30b・・・申込者端末、32a・・・判定結果画面、32b・・・判定結果画面。

10

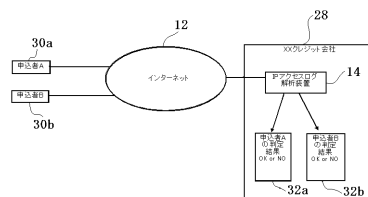
【図1】



【図2】



【図3】



フロントページの続き

(56)参考文献 特表2009-535692(JP,A)

特表2008-527761(JP,A)

特開2007-004415(JP,A)

特開2002-222286(JP,A)

津田 大介, 営業・企画・出張に役立つ資料を一撃で発見! ほしい情報が0.5秒で探せる
ビジネス検索術, 月刊ビジネスアスキー 第33巻 第8号 Monthly BUSINESS ASCII, 日本,
株式会社アスキー・メディアワークス, 2009年 8月 1日, 第33巻, p38-39

(58)調査した分野(Int.Cl., DB名)

G06Q 10/00 - 50/34