(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 11 月 26 日(26.11.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/178002 A1

(51) 国際特許分類:
G06F 21/55 (2013.01) *G06F 13/00* (2006.01)

(21) 国際出願番号: PCT/JP2015/002476

(22) 国際出願日: 2015 年 5 月 18 日(18.05.2015)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2014-106226 2014 年 5 月 22 日(22.05.2014) JP

(71) 出願人: 日本電気株式会社(NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 池田 聡(IKEDA, Satoshi); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

(74) 代理人: 下坂 直樹(SHIMOSAKA, Naoki); 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

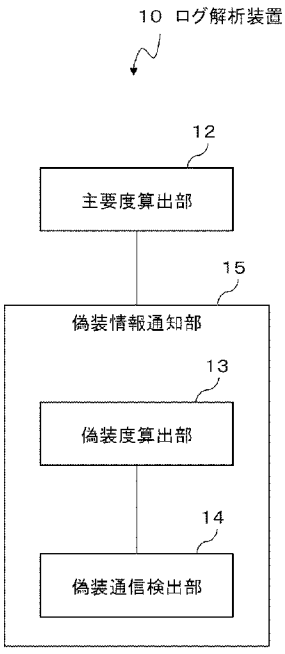
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING SYSTEM, AND COMMUNICATION HISTORY ANALYSIS METHOD

(54) 発明の名称 : 情報処理装置、情報処理システム及び通信履歴解析方法

[図1]



10 Log analysis device
12 Importance level calculation unit
13 Disguise level calculation part
14 Disguised communication detection part
15 Disguise information notification unit

(57) **Abstract**: The present invention provides an information processing device for obtaining information pertaining to communication by malware disguised as a user agent regardless of use environment. Said information processing device includes: a means for calculating an importance level with regard to each communication control means on the basis of history of communication between a client and a server, said importance level indicating the level of certainty that the communication control means is a real user agent that is permitted to operate as a part of the client; and a means for outputting, on the basis of the importance level, disguise information pertaining to communication by a disguised user agent disguised as a real user agent.

(57) 要約: 本発明は、利用環境に係わらず、ユーザエージェントに偽装するマルウェアによる通信に関する情報を得る情報処理装置を提供する。その情報処理装置は、クライアントとサーバとの間の通信履歴に基づいて、通信制御手段のそれぞれについて、そのクライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出する手段と、その主要度に基づいて、実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する偽装情報を出力する手段と、を含む。

WO 2015/178002 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

情報処理装置、情報処理システム及び通信履歴解析方法

技術分野

[0001] 本発明は、ネットワークにおける通信の履歴を解析する技術に関する。

背景技術

[0002] 企業ネットワークでは、ファイアウォールやＩＤＳ（Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）などにより、通信の遮断や監視が行われている。その目的は、企業ネットワークからの情報漏えいや企業ネットワーク内の機器に対する外部からの攻撃などを防ぐことである。

[0003] 一方で、電子メールの送受信やワールドワイドウェブの閲覧などは、業務上不可欠であることが多く、そのような通信は一定の制限のもとで許可されていることが多い。例えば、クライアントからの外部のウェブサーバへのアクセスに関しては、プロキシサーバを経由するアクセスのみが許可される構成がある。そのような構成は、企業ネットワーク内のクライアントが外部ネットワークに直接晒されることを防止し、不正アクセスや侵入行為を困難にする。

[0004] しかし、標的型攻撃が一般的になったことで、外部からの不正アクセスや侵入行為を防ぐことを目的とした入口対策だけでは、セキュリティの確保が難しい状況が発生する。ここで、標的型攻撃は、メールやウェブなどの外部ネットワークとの接点を巧妙に利用し、企業内ネットワーク内の端末にＲＡＴ（Ｒｅｍｏｔｅ　Ａｃｃｅｓｓ　Ｔｏｏｌ；リモート管理ツール）などのマルウェアを侵入させる攻撃である。

[0005] 標的型攻撃は、特定の企業や団体を対象とすることから、通常のウィルスやアドウェアと比較して、検体の入手が困難である。そのため、セキュリティベンダーがマルウェアの定義ファイルを更新するまでに、既に攻撃が進行している可能性が高く、入口対策だけでは防ぐことが困難である。例えば、

企業を対象とする標的型攻撃は、機密情報の盗取が目的であることが多い。この場合、機密情報の外部への漏えいを防ぐための出口対策が重要である。

[0006] このような課題を解決する技術が特許文献１に記載されている。

[0007] 一般的に、ＲＡＴなどのマルウェアに感染した端末は、自律的に実行できる処理が限られている。そのため、その感染した端末は、Ｃ＆Ｃ（Ｃｏｍｍａｎｄ ａｎｄ Ｃｏｎｔｒｏｌ）サーバと呼ばれる制御サーバと通信を行い、そのＣ＆Ｃサーバからの指示を受けて情報収集やデータの送受信を行う。そのため、その感染した端末とそのＣ＆Ｃサーバ間での通信を不正な通信として検出することができれば、それはインシデントの発見、情報漏えいの防止につながる。

[0008] 特許文献１に記載のマルウェア通信検出システムは、以下の構成を含む。第1に、プロキシサーバが、クライアントのブラウザから外部サーバへ対するリクエストに応じて、認証用プログラムを生成し、その認証用プログラムをクライアントへ送信する。第２に、そのクライアントのブラウザは、受信したその認証用プログラムを実行し、実行結果をそのプロキシサーバへ送信する。第３に、そのプロキシサーバは、受信したその実行結果に基づいて、そのリクエストがマルウェアからのリクエストであるか否か、即ちそのリクエストによるアクセスの可否を判断する。

[0009] 上述の構成を含む特許文献１のマルウェア通信検出システムは、マルウェアがブラウザを偽装して通信を行った場合にも、そのマルウェアによる通信であることの検出が可能である。

先行技術文献

特許文献

[0010] 特許文献1：特開２０１３－１９２０１９号公報

発明の概要

発明が解決しようとする課題

[0011] しかしながら、上述した先行技術文献に記載された技術においては、通信

履歴を解析する技術を適用可能な環境（システムが利用される業務環境や、サービス環境など）が限定的であるという問題点がある。

[0012] その理由は、特許文献１に記載のマルウェア通信検出システムのブラウザが、認証用プログラムを実行可能な、特殊なブラウザでなければならないからである。

[0013] 換言すると、特許文献１に記載のマルウェア通信検出システムのプロキシサーバは、その認証用プログラムに対応ブラウザ以外のプログラムが実行する、外部ネットワークへのいずれかの通信を、遮断する可能性がある。しかしながら、環境によっては、そのような不便を招く防御策が取れない場合がある。

[0014] そのような環境においても、ブラウザに偽装するマルウェアによる通信の検出を可能にすることが求められる。

[0015] 本発明の目的は、通信履歴を解析する技術を適用可能な環境が限定的であるという問題点を解決できる情報処理装置、情報処理システム、通信履歴解析方法、及びそのためのプログラム或いはそのプログラムを記録したコンピュータ読み取り可能な非一時的記録媒体を提供することにある。

課題を解決するための手段

[0016] 本発明の一様態における情報処理装置は、クライアントとサーバとの間の、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出するための主要度算出手段と、前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する情報である、偽装情報を出力するための偽装情報通知手段と、を含む。

[0017] 本発明の一様態における情報処理システムは、ネットワークに接続され、クライアントからのサーバに対するリクエストを中継するプロキシサーバと

、前記プロキシサーバと接続され、前記ネットワークに接続された前記サーバを、前記プロキシサーバを介してアクセスする前記クライアントと、前記プロキシサーバが生成する、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴を記憶するログ記憶手段と、前記通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出するための主要度算出手段と、前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する情報である、偽装情報を出力するための偽装情報通知手段と、を含む。

[0018] 本発明の一様態における通信履歴解析方法は、クライアントとサーバとの間の、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出し、前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する情報である、偽装情報を出力する。

[0019] 本発明の一様態におけるコンピュータ読み取り可能な非一時的記録媒体は、クライアントとサーバとの間の、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出し、前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関

する情報である、偽装情報を出力する処理をコンピュータに実行させるプログラムを記録する。

発明の効果

[0020] 本発明は、利用環境に係わらず、ユーザエージェントに偽装するマルウェアによる通信に関する情報を得ることが可能になるという効果がある。

図面の簡単な説明

[0021] [図1]本発明の第１の実施形態に係るログ解析装置の構成を示すブロック図である。

[図2]第１の実施形態に係るログ解析装置を含むログ解析システムの構成を示すブロック図である。

[図3]第１の実施形態におけるアクセスログの構造の一例を示す図である。

[図4]第１の実施形態に係るログ解析装置を実現するコンピュータのハードウェア構成を示すブロック図である。

[図5]第１の実施形態におけるログ解析装置の動作を示すフローチャートである。

[図6]第１の実施形態における主要度の一例を示す図である。

[図7]第１の実施形態における偽装度の一例を示す図である。

[図8]本発明の第２の実施形態に係るログ解析装置の構成を示すブロック図である。

[図9]第２の実施形態に係るログ解析装置を含むログ解析システムの構成を示すブロック図である。

[図10]第２の実施形態におけるアクセスログの構造の一例を示す図である。

[図11]第２の実施形態におけるログ解析システムの動作を示すフローチャートである。

発明を実施するための形態

[0022] 本発明を実施するための形態について図面を参照して詳細に説明する。尚、各図面及び明細書記載の各実施形態において、同様の構成要素には同様の符号を付与し、適宜説明を省略する。

[0023] ＜＜＜第１の実施形態＞＞＞

図１は、本発明の第１の実施形態に係るログ解析装置（情報処理装置とも呼ばれる）１０の構成を示すブロック図である。図１に示すように本実施形態に係るログ解析装置１０は、主要度算出部１２及び偽装情報通知部１５を含む。

[0024] 図２は、ログ解析装置１０を含むログ解析システム（情報処理システムとも呼ばれる）１０１の構成を示すブロック図である。図２に示すように、ログ解析システム１０１は、ログ解析装置１０、プロキシサーバ２０及びクライアント３０を含む。また、プロキシサーバ２０は、ネットワーク４０を介してサーバ５０と接続する。

[0025] 尚、図２に示す例に係わらず、プロキシサーバ２０及びクライアント３０は任意の台数であってよい。ネットワーク４０は、インターネットであってよいし、特定の限定されたネットワークであってもよい。サーバ５０は、例えば、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）サーバなどである。

[0026] ＝＝＝ログ解析装置１０＝＝＝

ログ解析装置１０は、プロキシサーバ２０が生成するアクセスログ（通信履歴とも呼ばれる）８１０を解析し、実用ユーザエージェントに偽装した偽装ユーザエージェントによる通信を検出する。実用ユーザエージェント及び偽装ユーザエージェントは、総称して、通信制御手段とも呼ばれる。

[0027] ここで、「実用ユーザエージェント」は、クライアント３０の一部として動作することを許容された、ユーザエージェントを示す。その実用ユーザエージェントは、例えば、クライアント３０上で動作することを許容されたウェブブラウザの、ＨＴＴＰユーザエージェントである。また、その実用ユーザエージェントは、クライアント３０上で動作することを許容された、通信時にユーザエージェント文字列を送信する、その他のユーザエージェントであってよい。

[0028] 「偽装ユーザエージェント」は、実用ユーザエージェントに偽装して、通

信を実行する不正なソフトウェアを示す。例えば、その偽装ユーザエージェントは、マルウェア等の一部である。

[0029] アクセスログ８１０は、プロキシサーバ２０が中継する、クライアント３０とサーバ５０との間の、通信の履歴である。換言すると、アクセスログ８１０は、クライアント３０がプロキシサーバ２０を介して実行する、サーバ５０へのアクセスのアクセスログである。具体的には、アクセスログ８１０は、クライアント３０上で動作する実用ユーザエージェント及び偽装ユーザエージェントのそれぞれが、プロキシサーバ２０を介して、ネットワーク４０に接続されたサーバ５０にアクセスする通信の履歴である。

[0030] 図３は、アクセスログ８１０の構造の一例を示す図である。図３に示すように、アクセスログ８１０は、少なくともクライアント識別子８１１、サーバ識別子８１２、ユーザエージェント文字列８１３を含む。

[0031] クライアント識別子８１１は、例えば、アクセス元のクライアント３０のＩＰ（ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスである。尚、クライアント識別子８１１は、ＩＰアドレスに限らず、クライアント３０を識別可能な任意の情報であってよい。

[0032] サーバ識別子８１２は、例えば、ドメイン名である。尚、サーバ識別子８１２は、ドメイン名に限らず、サーバ５０を識別可能な任意の情報であってよい。

[0033] ユーザエージェント文字列８１３は、アクセス元のクライアント３０が送出するリクエストに含まれる、実用ユーザエージェントを識別するための文字列である。

[0034] ログ解析装置１０は、例えば、ログ解析装置１０内の図示しない記憶手段にアクセスログ８１０を記憶する。また、ログ解析装置１０は、図示しない外部の記憶手段から、必要に応じてアクセスログ８１０を読み出してもよい。

[0035] ＝＝＝プロキシサーバ２０＝＝＝

プロキシサーバ２０は、クライアント３０からのリクエストを受け付け、

そのリクエストで指定されたサーバ５０にそのリクエストを中継する機能を、少なくとも備える。そのリクエストは、例えば、クライアント３０とサーバ５０との間の通信（例えば、ＨＴＴＰ通信）のリクエストである。尚、そのリクエストは、ＨＴＴＰ通信に限らず、任意のリクエストであってよい。

[0036] プロキシサーバ２０は、そのリクエストに関する情報である、アクセスログ８１０を、例えば、ログ解析装置１０に出力する。また、プロキシサーバ２０は、アクセスログ８１０を、図示しない記憶手段に出力してよい。プロキシサーバ２０は、そのアクセスログ８１０を、ＨＴＴＰ通信を中継する度に出力する。また、プロキシサーバ２０は、所定の時刻や、ログ解析装置１０から要求されたタイミングなどに、そのアクセスログ８１０を纏めてログ解析装置１０に出力してもよい。

[0037] ＝＝＝クライアント３０＝＝＝

クライアント３０は、プロキシサーバ２０を経由して、ネットワーク４０に接続されたサーバ５０と通信を行う。換言すると、クライアント３０は、プロキシサーバ２０を介して、ネットワーク４０に接続されたサーバ５０にアクセスする。

[0038] 次に、第一の実施形態におけるログ解析装置１０が備える各構成要素について説明する。尚、図１に示す各構成要素は、ハードウェア単位の回路でも、コンピュータ装置の機能単位に分割された構成要素でもよい。ここでは、図１に示す構成要素は、コンピュータ装置の機能単位に分割された構成要素として説明する。

[0039] ＝＝＝主要度算出部１２＝＝＝

主要度算出部１２は、アクセスログ８１０に基づいて、ユーザエージェント文字列８１３に対応する通信制御手段のそれぞれについて、主要度を算出する。その主要度は、その通信制御手段がクライアント３０の一部として動作することを許容された実用ユーザエージェントであることの、確度を示す。換言すると、その主要度は、例えばウェブサーバであるサーバ５０にアクセスする通信を実行したその通信制御手段が、クライアント３０上で動作す

ることを許容されたウェブブラウザの実用ユーザエージェントである可能性を示す指標である。

[0040] 具体的には、主要度算出部１２は、アクセスログ８１０を解析し、ユーザエージェント文字列８１３のそれぞれに対応する主要度を算出する。ここで、ユーザエージェント文字列８１３に対応する主要度は、即ち、実用ユーザエージェント及び偽装ユーザエージェント（即ち、通信制御手段）のいずれかに対応する主要度である。

[0041] 例えば、主要度算出部１２は、クライアント３０毎に、ユーザエージェント文字列８１３のそれぞれに対応する主要度を算出する。この場合、その主要度は、クライアント３０とユーザエージェント文字列８１３との組、即ちクライアント３０と通信制御手段との組、に対して算出される値である。尚、主要度算出部１２は、任意の基準に基づいてグループ分けされたクライアント３０のグループ毎に、ユーザエージェント文字列８１３のそれぞれに対応する主要度を算出してよい。また、主要度算出部１２は、全てのクライアント３０を纏めて、ユーザエージェント文字列８１３のそれぞれに対応する主要度を算出してもよい。

[0042] 主要度の算出の詳細な説明は後述する。

[0043] ＝＝＝偽装情報通知部１５＝＝＝

偽装情報通知部１５は、主要度算出部１２が算出した主要度に基づいて、偽装情報を出力する。その偽装情報は、実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信（サーバ５０へのアクセス）に関する情報である。

[0044] 図１に示すように、偽装情報通知部１５は、例えば、偽装度算出部１３及び偽装通信検出部１４を含む。

[0045] 偽装度算出部１３は、主要度算出部１２が算出した主要度に基づいて、サーバ５０のそれぞれに対応する、偽装度を算出する。その偽装度は、通信が偽装ユーザエージェントにより実行された通信である確度を示す。換言すると、その偽装度は、あるサーバ５０へアクセスしているクライアント３０上

の通信制御手段が、実用ユーザエージェントを偽装している偽装ユーザエージェントであるか否かを示す指標である。尚、偽装度の算出方法の詳細な説明は後述する。

[0046] 偽装通信検出部１４は、例えば、偽装度算出部１３が算出した偽装度が閾値以上であるサーバ５０を検出し、検出したそのサーバ５０のサーバ識別子８１２を含む、偽装情報を出力する。その閾値は、例えば、経験的に或いは理論的に予め算出され、ログ解析装置１０に与えられる。

[0047] また、偽装通信検出部１４は、その閾値以上の偽装度に関連する、クライアント識別子８１１やユーザエージェント文字列８１３、アクセスログ８１０など、任意の情報を含む偽装情報を出力してよい。

[0048] 以上が、ログ解析装置１０の機能単位の各構成要素についての説明である。

[0049] 次に、ログ解析装置１０のハードウェア単位の構成要素について説明する。

[0050] 図４は、本実施形態におけるログ解析装置１０を実現するコンピュータ７００のハードウェア構成を示す図である。

[0051] 図４に示すように、コンピュータ７００は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）７０１、記憶部７０２、記憶装置７０３、入力部７０４、出力部７０５及び通信部７０６を含む。更に、コンピュータ７００は、外部から供給される記録媒体（または記憶媒体）７０７を含む。例えば、記録媒体７０７は、情報を非一時的に記憶する不揮発性記録媒体（非一時的記録媒体）である。また、記録媒体７０７は、情報を信号として保持する、一時的記録媒体であってもよい。

[0052] ＣＰＵ７０１は、オペレーティングシステム（不図示）を動作させて、コンピュータ７００の全体の動作を制御する。例えば、ＣＰＵ７０１は、記憶装置７０３に装着された記録媒体７０７から、そのプログラムやデータを読み込み、読み込んだそのプログラムやそのデータを記憶部７０２に書き込む。ここで、そのプログラムは、例えば、後述の図５に示すフローチャートの

動作をコンピュータ７００に実行させるためのプログラムである。

[0053] そして、ＣＰＵ７０１は、その読み込んだプログラムに従って、またその読み込んだデータに基づいて、図１に示す主要度算出部１２及び偽装情報通知部１５として各種の処理を実行する。

[0054] 尚、ＣＰＵ７０１は、通信網（不図示）に接続される外部コンピュータ（不図示）から、記憶部７０２にそのプログラムやそのデータをダウンロードしてもよい。

[0055] 記憶部７０２は、そのプログラムやそのデータを記憶する。記憶部７０２は、アクセスログ８１０や、後述のアクセスログ８８０、図６に示す情報、図７に示す情報などを記憶してよい。

[0056] 記憶装置７０３は、例えば、光ディスクや、フレキシブルディスク、磁気光ディスク、外付けハードディスク半導体メモリなどであって、記録媒体７０７を含む。記憶装置７０３（記録媒体７０７）は、そのプログラムをコンピュータ読み取り可能に記憶する。また、記憶装置７０３は、そのデータを記憶してもよい。記憶装置７０３は、アクセスログ８１０や、後述のアクセスログ８８０、図６に示す情報、図７に示す情報などを記憶してよい。

[0057] 入力部７０４は、オペレータによる操作の入力や外部からの情報の入力を受け付ける。入力操作に用いられるデバイスは、例えば、マウスや、キーボード、内蔵のキーボタン及びタッチパネルなどである。

[0058] 出力部７０５は、例えばディスプレイで実現される。出力部７０５は、例えばＧＵＩ（Ｇｒａｐｈｉｃａｌ Ｕｓｅｒ Ｉｎｔｅｒｆａｃｅ）によるオペレータへの入力要求や、オペレータに対する出力提示などのために用いられる。

[0059] 通信部７０６は、プロキシサーバ２０とのインタフェースを実現する。通信部７０６は、例えば、主要度算出部１２の一部として含まれる。

[0060] 以上説明したように、図１に示すログ解析装置１０の機能単位のブロックは、図４に示すハードウェア構成のコンピュータ７００によって実現される。但し、コンピュータ７００が備える各部の実現手段は、上記に限定されな

い。すなわち、コンピュータ７００は、物理的に結合した１つの装置により実現されてもよいし、物理的に分離した２つ以上の装置を有線または無線で接続し、これら複数の装置により実現されてもよい。

[0061] 尚、上述のプログラムのコードを記録した記録媒体７０７が、コンピュータ７００に供給される場合、ＣＰＵ７０１は、記録媒体７０７に格納されたそのプログラムのコードを読み出して実行してもよい。或いは、ＣＰＵ７０１は、記録媒体７０７に格納されたそのプログラムのコードを、記憶部７０２、記憶装置７０３またはその両方に格納してもよい。すなわち、本実施形態は、コンピュータ７００（ＣＰＵ７０１）が実行するそのプログラム（ソフトウェア）を、一時的にまたは非一時的に、記憶する記録媒体７０７の実施形態を含む。尚、情報を非一時的に記憶する記憶媒体は、不揮発性記憶媒体とも呼ばれる。

[0062] 以上が、本実施形態におけるログ解析装置１０を実現するコンピュータ７００の、ハードウェア単位の各構成要素についての説明である。

[0063] 次に本実施形態の動作について、図面を参照して詳細に説明する。

[0064] 図５は、本実施形態におけるログ解析装置１０の動作を示すフローチャートである。尚、このフローチャートによる処理は、前述したＣＰＵ７０１によるプログラム制御に基づいて、実行されてよい。また、処理のステップ名については、Ｓ１１のように、記号で記載する。

[0065] ログ解析装置１０は、アクセスログ８１０（通信履歴）の解析処理を、ある期間（例えば１日分）のアクセスログ８１０を対象に、バッチ的に実行する。ここでは、主要度算出部１２の一部である記憶部７０２に、１日分のアクセスログ８１０が蓄積されているものとして説明する。

[0066] ログ解析装置１０は、例えば所定の時刻（例えば、午前０時）毎に、図５に示すフローチャートの処理を実行する。また、ログ解析装置１０は、例えば入力部７０４を介してオペレータからの指示を受け取った場合に、図５に示すフローチャートの処理を実行してもよい。

[0067] 主要度算出部１２は、主要度を算出する（ステップＳ１１）。

[0068] 図６は、算出される主要度８２５の一例を示す図である。主要度算出部１２は、例えば以下の手順で主要度８２５を算出する。

[0069] 第１に、主要度算出部１２は、アクセスログ８１０に基づいて、クライアント識別子８１１とユーザエージェント文字列８１３との組毎に、アクセス先のドメイン数８２４を集計する。ここで、クライアント識別子８１１とユーザエージェント文字列８１３との組は、即ち、クライアント３０と通信制御手段（実用ユーザエージェントまたは偽装ユーザエージェント）との組を示す。また、ドメイン数８２４は、そのアクセス先のサーバ識別子８１２の数である。

[0070] 第２に、主要度算出部１２は、ドメイン数８２４に基づいて、クライアント識別子８１１とユーザエージェント文字列８１３との組に対応する、主要度８２５を求める。

[0071] 例えば、主要度算出部１２は、主要度８２５を、ドメイン数８２４が閾値（例えば、「１０」）を超えている場合に「１」と、ドメイン数８２４がその閾値以下の場合に「０」と、算出する。その閾値は、経験的或いは理論的に、予め定められた閾値である。

[0072] また、主要度算出部１２は、独立変数の値が大きいほど従属変数の値が「１」に近づき、その独立変数の値が小さいほどその従属変数の値が「０」に近づくような関数を利用し、ドメイン数８２４を独立変数として従属変数にあたる主要度８２５を算出してもよい。そのような関数としては、例えばシグモイド関数やゴンペルツ関数などがある。

[0073] 尚、主要度算出部１２は、素性が明らかな、即ち検出対象の偽装エージェントではないことが確実な、実用ユーザエージェントに対応するユーザエージェント文字列８１３を含むアクセスログ８１０を処理の対象（解析対象）から除外してもよい。更に、主要度算出部１２は、素性が明らかな、ユーザエージェント文字列８１３とサーバ識別子８１２との、組を含むアクセスログ８１０を処理の対象（解析対象）から除外してもよい。

[0074] 例えば、ウェブブラウザのユーザエージェント文字列８１３は、「Ｍｏｚ

ｉｌｌａ／」で始まる文字列であることがほとんどである。そのため、ウェブブラウザの実用ユーザエージェントを偽装した偽装ユーザエージェントの検出という観点では、上述のようなユーザエージェント文字列８１３を含むものだけを解析対象とすることが効率的である。

[0075] 一方、全てのアクセスログ８１０を解析対象とすることで、ユーザのブラウザ操作に関連しない、様々なアクセスにおける、偽装ユーザエージェントを検出することが、可能である。

[0076] 図５に戻って、次に、偽装情報通知部１５の偽装度算出部１３は、主要度８２５に基づいて偽装度を算出する（ステップＳ１２）。偽装度算出部１３は、例えば、サーバ５０毎に偽装度を算出する。

[0077] 図７は、算出される偽装度８３７の一例を示す図である。図７は、「ｍａｌｉｃｉｏｕｓ．ｅｘａｍｐｌｅ．ｃｏｍ」というサーバ識別子８１２に対して、４つの＜クライアント、通信制御手段＞８３６の組からアクセスがあったことを示し、それらの組のそれぞれに対応する主要度８２５を示す。尚、＜クライアント、通信制御手段＞８３６において、「クライアント」はクライアント識別子８１１であり、「通信制御手段」は、ユーザエージェント文字列８１３である。

[0078] そして、図７は、サーバ識別子８１２に対応する、偽装度８３７を示す。換言すると、図７は、サーバ識別子８１２で特定されるサーバ５０と、＜クライアント、通信制御手段＞８３６で特定されるクライアント３０上で動作する通信制御手段との通信に対応する、偽装度８３７を示す。

[0079] 偽装度算出部１３は、図７の例では、「１」から主要度８２５の平均値「０．２５」を引いた値「０．７５」を、偽装度８３７として算出する。尚、偽装度算出部１３は、上述の例に係わらず、任意の適切な手法で、偽装度８３７を算出してよい。

[0080] 図５に戻って、次に、偽装情報通知部１５の偽装通信検出部１４は、偽装度８３７に基づいて、偽装ユーザエージェントによる通信を検出する（ステップＳ１３）。

[0081] 例えば、偽装通信検出部１４は、偽装度算出部１３が算出した偽装度８３７が、予め定められた閾値を超えている場合に、そのサーバ識別子８１２のドメインへの通信を偽装ユーザエージェントによる通信であると判断する。

[0082] 次に、偽装通信検出部１４は、偽装ユーザエージェントによる通信に関する偽装情報を出力する（ステップＳ１４）。その偽装情報は、例えば、サーバ識別子８１２を含む。

[0083] 例えば、偽装通信検出部１４は、その偽装情報を、図４に示す出力部７０５を介して、ログ解析システム１０１の管理を行っているオペレータに通知する。また、偽装通信検出部１４は、その偽装情報を、プロキシサーバ２０に通知してもよい。この場合、プロキシサーバ２０は、通知されたその偽装情報に含まれるサーバ識別子８１２を、ブラックリストに登録し、そのサーバ識別子８１２に対応するサーバ５０に対する以降の通信を、遮断してもよい。上述の構成により、オペレータの最終的な判断が得られるまでの、一時的な対応を可能にすることができる。

[0084] 本実施形態のログ解析装置１０は、主要ブラウザのユーザエージェント文字列８１３の偽装が困難であるほど、より好適に、偽装ユーザエージェントによる通信を検出する。例えば、利用シェアの高いＩｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ（登録商標）では、インストールされているプラグインやツールバーなどの情報が、ユーザエージェント文字列に付与される。このため、Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒのそのユーザエージェント文字列と完全に一致するように、偽装ユーザエージェントがそのユーザエージェント文字列を生成することは難しい。但し、マルウェアである偽装ユーザエージェントが、クライアント３０の通信の盗聴やレジストリ情報の特定エントリの参照などを行い、それによって得た情報を利用して完全な偽装をすることは、不可能ではない。しかし、マルウェア（偽装ユーザエージェント）のこのような振る舞いは、ウィルス対策ソフトに実装される振る舞い型の検知手法によってマルウェア活動として検知される。本実施形態のログ解析装置１０は、そのようなウィルス対策ソフトの手法に対して、補完的な役割を果たす

ものである、とも言える。

[0085] 上述した本実施形態における第１の効果は、利用環境に係わらず、実用ユーザエージェントに偽装するマルウェアによる通信に関する情報を得ることが可能になる点である。

[0086] その理由は、主要度算出部１２が主要度８２５を算出し、偽装情報通知部１５が主要度８２５に基づいて偽装情報を出力するようにしたからである。

[0087] 具体的には、ログ解析装置１０は、あるサーバ５０に対する通信の偽装度８３７の算出を、プロキシサーバ２０を経由してそのサーバ５０との通信を行う複数のクライアント３０上の、主要度８２５に基づいて行う。そして、ログ解析装置１０は、この偽装度８３７に基づいて、主要な実用ユーザエージェント以外によるアクセスを検出することができる。その主要な実用ユーザエージェントは、例えばクライアント３０で主に利用されているウェブブラウザの実用ユーザエージェントである。その結果、ログ解析装置１０は、ウェブブラウザの実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信を検出できる。

[0088] 上述した本実施形態における第２の効果は、実用ユーザエージェントに偽装するマルウェアによる通信の検出において、誤検出を防止することが可能になる点である。

[0089] その理由は、偽装情報通知部１５が、サーバ識別子８１２に対応する偽装度８３７を、複数のクライアント３０のそれぞれに対応する主要度８２５を、集計して算出するからである。

[0090] 例えば、ログ解析装置１０は、多くのクライアント３０が主要なブラウザを利用してアクセスするサーバ５０を、偽装ユーザエージェントによる通信の対象であるサーバ５０として誤検出することを、抑制することができる。なぜならば、その主要なブラウザの実用ユーザエージェントは、比較的多数のクライアント３０において、比較的高い主要度が算出されるからである。

[0091] ＜＜＜第１の実施形態の変形例＞＞＞

主要度算出部１２は、ユーザエージェント文字列８１３と、「Ａｃｃｅｐ

ｔ」ヘッダや「Ａｃｃｅｐｔ－Ｌａｎｇｕａｇｅ」ヘッダなど他のヘッダ情報とを組み合わせて、主要度８２５の算出を行う。

[0092] こうすることで、ログ解析装置１０は、偽装ユーザエージェントによって偽装されたユーザエージェント文字列８１３が、実用ユーザエージェントのユーザエージェント文字列８１３と一致する場合でも、偽装ユーザエージェントによる通信を検出する。

[0093] ＜＜＜第２の実施形態＞＞＞

次に、本発明の第２の実施形態について図面を参照して詳細に説明する。以下、本実施形態の説明が不明確にならない範囲で、前述の説明と重複する内容については説明を省略する。

[0094] 図８は、本発明の第２の実施形態に係るログ解析装置８０の構成を示すブロック図である。図８に示すように、本実施形態におけるログ解析装置８０は、第１の実施形態のログ解析装置１０と比べて、主要度算出部１２に替えて主要度算出部８２を含む点が異なる。

[0095] 図９は、ログ解析装置８０を含むログ解析システム１０８の構成を示すブロック図である。図９に示すように、ログ解析システム１０８は、ログ解析装置８０、プロキシサーバ６０及びクライアント７０を含む。また、プロキシサーバ６０は、ネットワーク４０を介してサーバ５０と接続する。

[0096] 尚、図９に示す例に係わらず、プロキシサーバ６０及びクライアント７０は任意の台数であってよい。

[0097] ＝＝＝クライアント７０＝＝＝

クライアント７０は、プロキシサーバ６０へのリクエストを送信する場合に、そのリクエストに含まれるリクエストヘッダに、実用ユーザエージェントからのアクセスであることを示すためのエージェントタグを付加する。

[0098] ここで、そのエージェントタグは偽装が困難な文字列であることが、好ましい。具体的には、そのエージェントタグは、クライアント７０毎に異なり、ネットワーク４０側からの推測が困難であることが、好ましい。

[0099] クライアント７０は、例えばそのリクエストヘッダに含まれるユーザエー

ジェント文字列に、そのエージェントタグを埋め込む。尚、クライアント７０は、そのユーザエージェント文字列以外のそのリクエストヘッダの情報に、そのエージェントタグを埋め込んでもよい。

[0100] ＝＝＝プロキシサーバ６０＝＝＝

プロキシサーバ６０は、そのリクエストに関する情報である、アクセスログを、例えば、ログ解析装置８０に出力する。また、プロキシサーバ６０は、そのアクセスログを、図示しない記憶手段に出力してよい。

[0101] そのアクセスログは、そのエージェントタグがそのユーザエージェント文字列に埋め込まれる場合は、図３に示す構造のアクセスログ８１０である。

[0102] 図１０は、そのエージェントタグがそのユーザエージェント文字列以外のそのリクエストヘッダの情報に埋め込まれる場合の、アクセスログ８８０の構造の一例を示す図である。図１０に示すように、アクセスログ８８０は、少なくともクライアント識別子８１１、サーバ識別子８１２、ユーザエージェント文字列８１３及びエージェントタグ８８８を含む。

[0103] また、プロキシサーバ６０は、クライアント７０からリクエストを受信し、そのリクエストをサーバ５０に中継する際に、そのリクエストに含まれるエージェントタグを削除してよい。

[0104] ＝＝＝主要度算出部８２＝＝＝

主要度算出部８２は、アクセスログ８１０に基づいて、ユーザエージェント文字列８１３に対応する通信制御手段のそれぞれについて、主要度８２５を算出する。主要度８２５は、上述したように、クライアント７０の一部として動作することを許容された実用ユーザエージェントであることの確度を示す。この場合、主要度算出部８２は、そのエージェントタグを含むユーザエージェント文字列８１３に対応する通信制御手段のそれぞれについて、その主要度８２５を算出する。

[0105] また、主要度算出部８２は、アクセスログ８８０に基づいて、ユーザエージェント文字列８１３に対応する通信制御手段のそれぞれについて、主要度８２５を算出する。この場合、主要度算出部８２は、そのエージェントタグ

を含まないユーザエージェント文字列８１３とエージェントタグ８８８との組に対応する通信制御手段のそれぞれについて、その主要度８２５を算出する。

[0106] 本実施形態のログ解析装置８０は、図４に示すコンピュータ７００で構成されてよい。この場合、ＣＰＵ７０１は、その読み込んだプログラムに従って、またその読み込んだデータに基づいて、図８に示す主要度算出部８２及び偽装情報通知部１５として各種の処理を実行する。

[0107] 次に、本実施形態の動作について図面を参照して、詳細に説明する。

[0108] 図１１は、本実施形態における、アクセスログ８１０及びアクセスログ８８０を生成する際の、ログ解析システム１０８の動作を示すシーケンス図である。

[0109] クライアント７０は、サーバ５０へのリクエストにエージェントタグを付加する（ステップＳ２１）。

[0110] 次に、クライアント７０は、プロキシサーバ６０にそのリクエストを送信する（ステップＳ２２）。

[0111] 次に、クライアント７０からのリクエストを受信したプロキシサーバ６０は、そのエージェントタグを削除する（ステップＳ２３）。この時、プロキシサーバ６０は、そのエージェントタグを削除していないそのリクエストを、例えば、図４に示す記憶部７０２に記録する。

[0112] 次に、プロキシサーバ６０は、そのエージェントタグを削除されたそのリクエストをサーバ５０に中継する（ステップＳ２４）。

[0113] 次に、プロキシサーバ６０は、サーバ５０から送信されたレスポンスを受信する（ステップＳ２５）。

[0114] 次に、プロキシサーバ６０は、そのレスポンスをクライアント７０へ中継する（ステップＳ２６）。

[0115] 次に、プロキシサーバ６０は、そのエージェントタグを削除される前のリクエスト情報に基づいて、アクセスログ８１０或いはアクセスログ８８０を出力する（ステップＳ２７）。

[0116] 尚、ログ解析装置８０の動作は、図５に示すフローチャートの動作と同等である。

[0117] 上述した本実施形態における第１の効果は、第１の実施形態の効果に加えて、ブラウザに偽装するマルウェアによる通信の検出精度を向上させることが可能になる点である。

[0118] その理由は、クライアント７０がリクエストヘッダにエージェントタグを付加し、ログ解析装置８０が、そのエージェントタグに更に基づいて、主要度８２５を算出するからである。

[0119] 例えば、ウェブブラウザの中には、プラグインなどの情報がユーザエージェント文字列に反映されないウェブブラウザがある。そのため、そのようなウェブブラウザでは、マルウェアがそのような固定的なユーザエージェントヘッダを利用した場合でも、ユーザエージェント文字列が一致してしまい、偽装が見逃される可能性がある。本実施形態のログ解析システム１０８は、エージェントタグを付加することで、固定的なユーザエージェント文字列との一致を防ぐ効果がある。

[0120] 上述した本実施形態における第２の効果は、エージェントタグがネットワーク４０に送出されることを防ぎ、ネットワーク４０側でのそのエージェントタグの推測をより困難することが可能になる点である。

[0121] その理由は、プロキシサーバ６０が、リクエストからエージェントタグを削除し、そのエージェントタグが削除されたリクエストを転送するからである。

[0122] 以上の各実施形態で説明した各構成要素は、必ずしも個々に独立した存在である必要はない。例えば、複数個の任意のその構成要素が１個のモジュールとして実現されてよい。また、その構成要素の内の任意のひとつが複数のモジュールで実現されてもよい。また、その構成要素の内の任意のひとつがその構成要素の内の任意の他のひとつであってよい。また、その構成要素の内の任意のひとつの一部と、その構成要素の内の任意の他のひとつの一部とが重複してもよい。

[0123] 以上説明した各実施形態における各構成要素及び各構成要素を実現するモジュールは、必要に応じ、可能であれば、ハードウェア的に実現されてよい。また、各構成要素及び各構成要素を実現するモジュールは、コンピュータ及びプログラムで実現されてよい。また、各構成要素及び各構成要素を実現するモジュールは、ハードウェア的なモジュールとコンピュータ及びプログラムとの混在により実現されてもよい。

[0124] そのプログラムは、例えば、磁気ディスクや半導体メモリなど、コンピュータが読み取り可能な非一時的記録媒体に記録され、コンピュータに提供される。そして、そのプログラムは、コンピュータの立ち上げ時などに、非一時的記録媒体からコンピュータに読み取られる。この読み取られたプログラムは、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施形態における構成要素として機能させる。

[0125] 更に、以上説明した各実施形態では、複数の動作は個々に相違するタイミングで実行されることに限定されない。例えば、ある動作の実行中に他の動作が発生してよい。また、ある動作と他の動作との実行タイミングが部分的に乃至全部において重複してもよい。

[0126] 以上、各実施形態を参照して本発明を説明したが、本発明は上記実施形態に限定されるものではない。本発明の構成や詳細には、本発明のスコープ内で当業者が理解しえる様々な変更をすることができる。

この出願は、２０１４年５月２２日に出願された日本出願特願２０１４－１０６２２６を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0127] １０ ログ解析装置
１２ 主要度算出部
１３ 偽装度算出部
１４ 偽装通信検出部
１５ 偽装情報通知部

２０　プロキシサーバ

３０　クライアント

４０　ネットワーク

５０　サーバ

６０　プロキシサーバ

７０　クライアント

８０　ログ解析装置

８２　主要度算出部

１０１　ログ解析システム

１０８　ログ解析システム

７００　コンピュータ

７０１　ＣＰＵ

７０２　記憶部

７０３　記憶装置

７０４　入力部

７０５　出力部

７０６　通信部

７０７　記録媒体

８１０　アクセスログ

８１１　クライアント識別子

８１２　サーバ識別子

８１３　ユーザエージェント文字列

８２４　ドメイン数

８２５　主要度

８３６　＜クライアント、通信制御手段＞

８３７　偽装度

８８０　アクセスログ

８８８　エージェントタグ

請求の範囲

[請求項1] クライアントとサーバとの間の、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出するための主要度算出手段と、

前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する情報である、偽装情報を出力するための偽装情報通知手段と、を含む

情報処理装置。

[請求項2] 前記偽装情報通知手段は、

前記主要度に基づいて、前記サーバのそれぞれに対応する、前記通信が前記偽装ユーザエージェントにより実行された前記通信である確度を示す、偽装度を算出する偽装度算出手段と、

前記偽装度が閾値以上の前記サーバを検出し、検出した前記サーバの識別子を含む前記偽装情報を出力する偽装通信検出手段と、を含む

ことを特徴とする請求項１記載の情報処理装置。

[請求項3] 前記偽装度算出手段は、前記サーバ毎に、前記サーバに対応する前記主要度が小さいほど、相対的に大きい前記偽装度を算出する

ことを特徴とする請求項２記載の情報処理装置。

[請求項4] 前記主要度算出手段は、前記ユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とに基づいて、前記クライアントと前記通信制御手段との組のそれぞれに対応する前記主要度を算出する

ことを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。

[請求項5] 前記通信履歴は、前記クライアントが付加する、前記実用ユーザエージェントからのアクセスであることを示す、エージェントタグを更に含み、

前記主要度算出手段は、前記エージェントタグに更に基づいて、前記主要度を算出する

ことを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。

[請求項6] ネットワークに接続され、クライアントからのサーバに対するリクエストを中継するプロキシサーバと、

前記プロキシサーバと接続され、前記ネットワークに接続された前記サーバを、前記プロキシサーバを介してアクセスする前記クライアントと、

前記プロキシサーバが生成する、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴を記憶するログ記憶手段と、

前記通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出するための主要度算出手段と、

前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する情報である、偽装情報を出力するための偽装情報通知手段と、を含む

情報処理システム。

[請求項7] 前記クライアントは、前記プロキシサーバへのリクエスト送信時に、前記ユーザエージェントからのアクセスであることを示す、エージェントタグを前記リクエストヘッダに付加し、

前記通信履歴は、前記エージェントタグを更に含み、

前記主要度算出手段は、前記ユーザエージェント文字列及び前記エージェントタグに基づいて、前記クライアントと前記ユーザエージェントとの組のそれぞれに対応する前記主要度を算出する

ことを特徴とする請求項６記載の情報処理システム。

[請求項8] 前記プロキシサーバは、前記リクエストを中継する際に、前記リクエストから前記エージェントタグを削除する

ことを特徴とする請求項７記載の情報処理システム。

[請求項9] クライアントとサーバとの間の、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出し、

前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する情報である、偽装情報を出力する

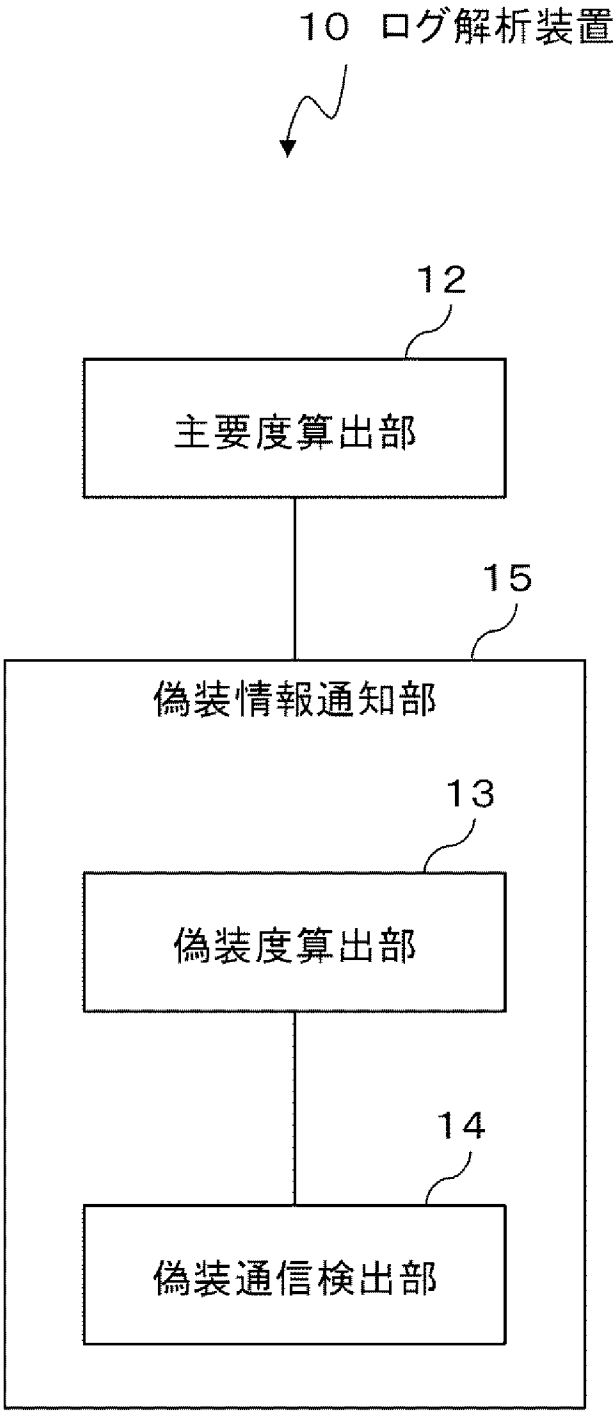
通信履歴解析方法。

[請求項10] クライアントとサーバとの間の、前記クライアントから送信されるリクエストヘッダに含まれるユーザエージェント文字列と前記クライアントの識別子と前記サーバの識別子とを少なくとも含む、通信履歴に基づいて、前記ユーザエージェント文字列に対応する通信制御手段のそれぞれについて、前記クライアントの一部として動作することを許容された実用ユーザエージェントであることの確度を示す、主要度を算出し、

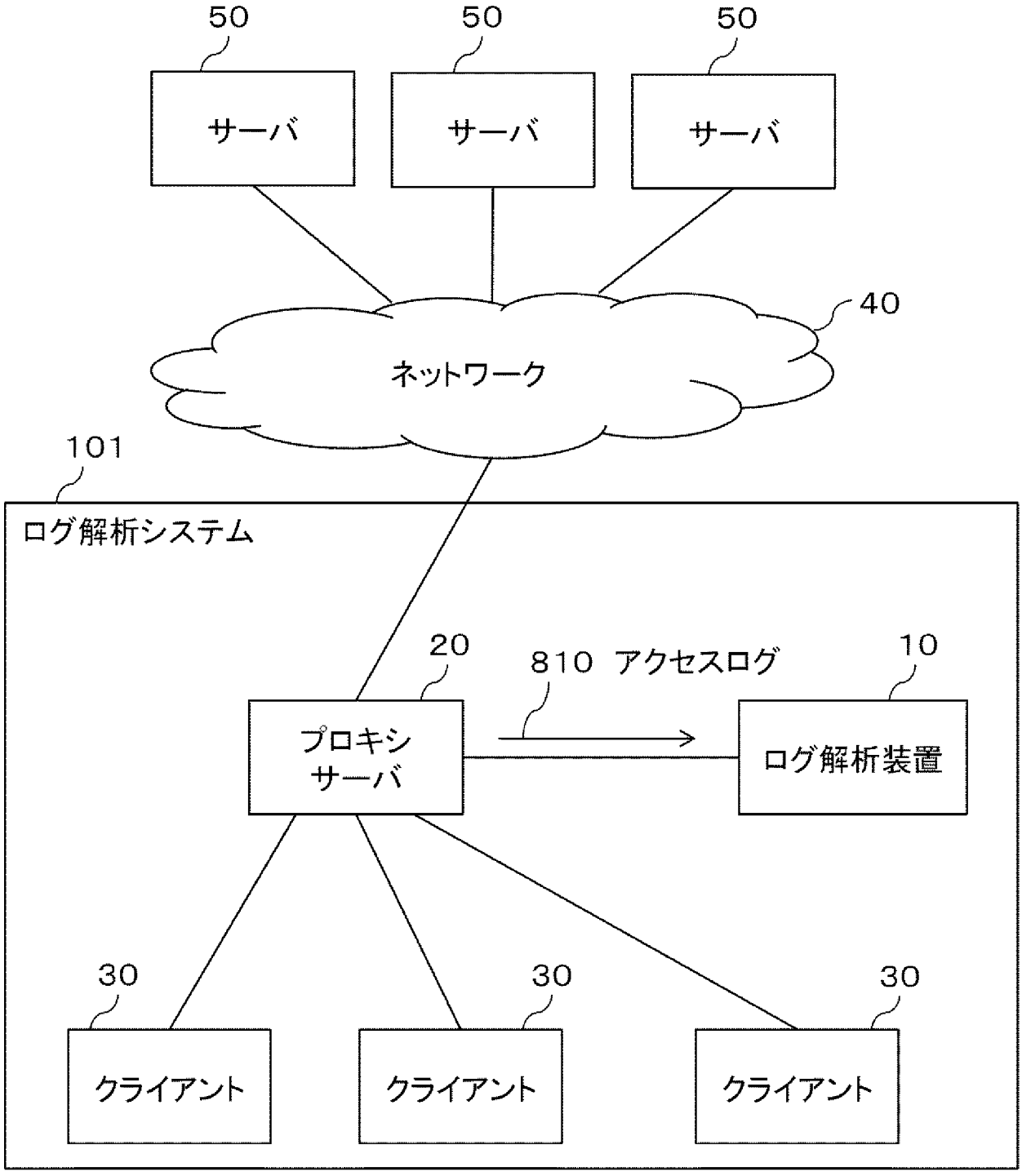
前記主要度に基づいて、前記実用ユーザエージェントを偽装した偽装ユーザエージェントによる通信に関する情報である、偽装情報を出力する処理をコンピュータに実行させる

プログラムを記録したコンピュータ読み取り可能な非一時的記録媒体。

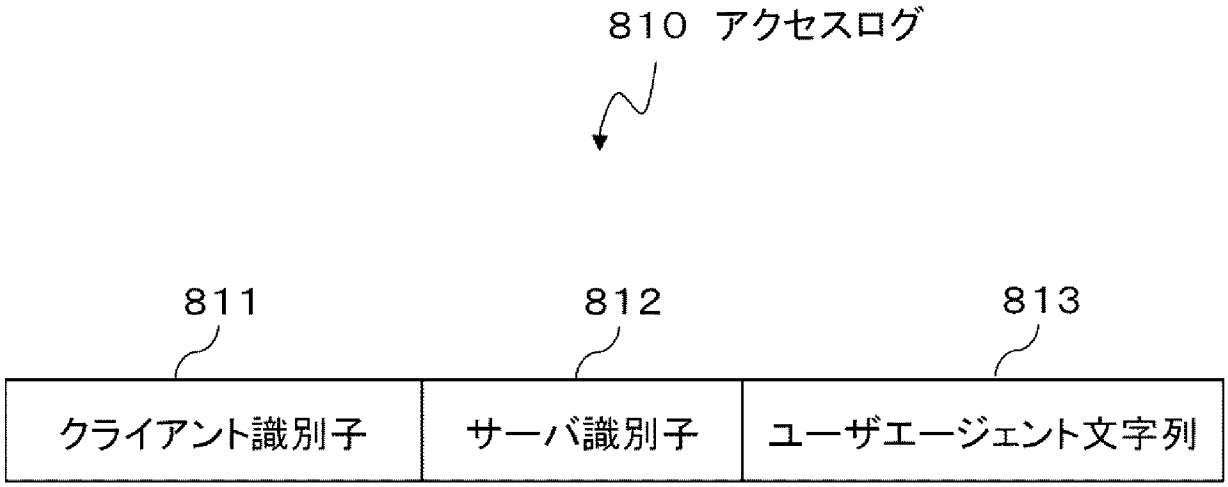
[図1]



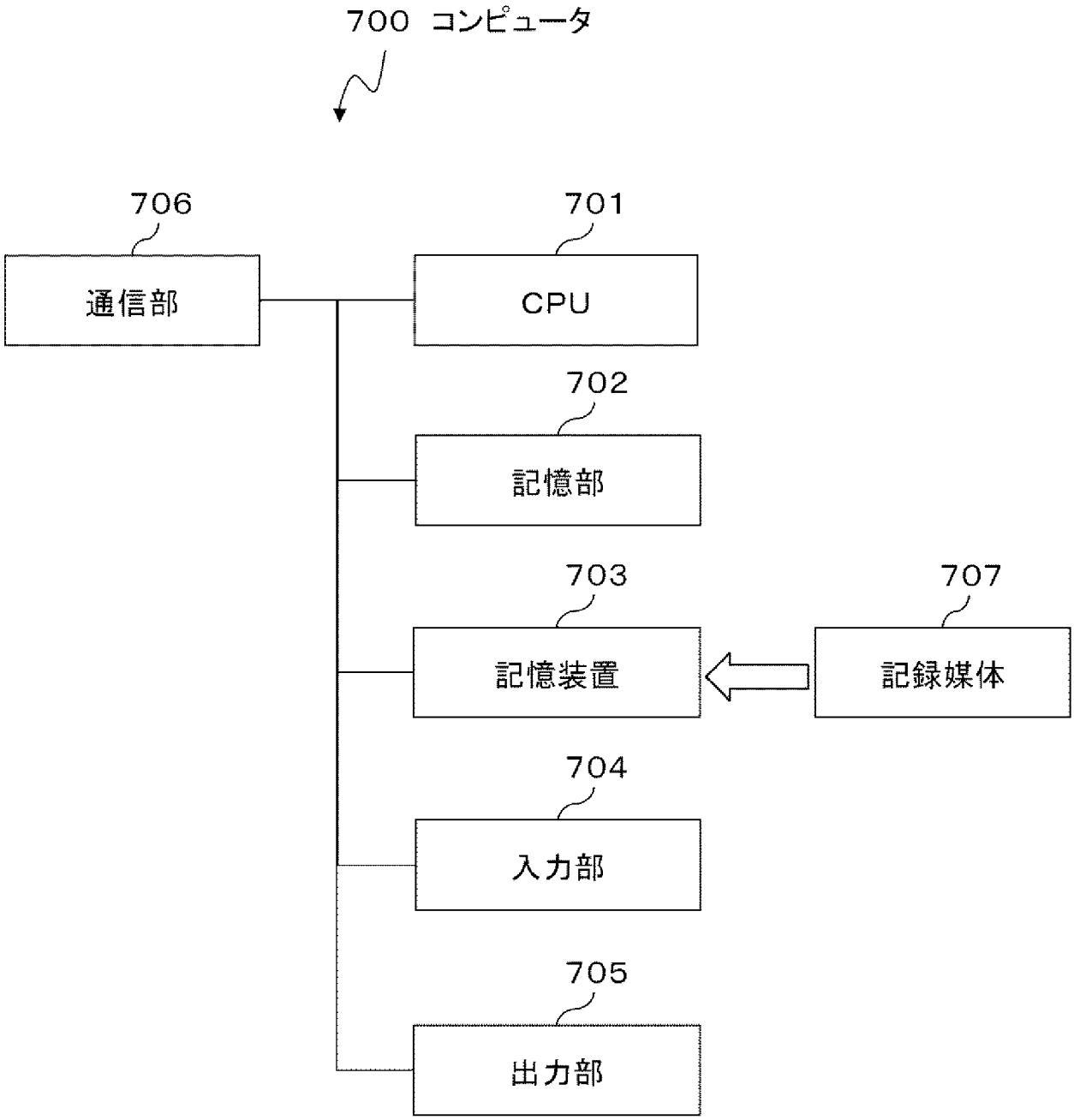
[図2]


50
50
50
サーバ
サーバ
サーバ
40
ネットワーク
101
ログ解析システム
20
810 アクセスログ
10
プロキシ
サーバ
ログ解析装置
30
30
30
クライアント
クライアント
クライアント

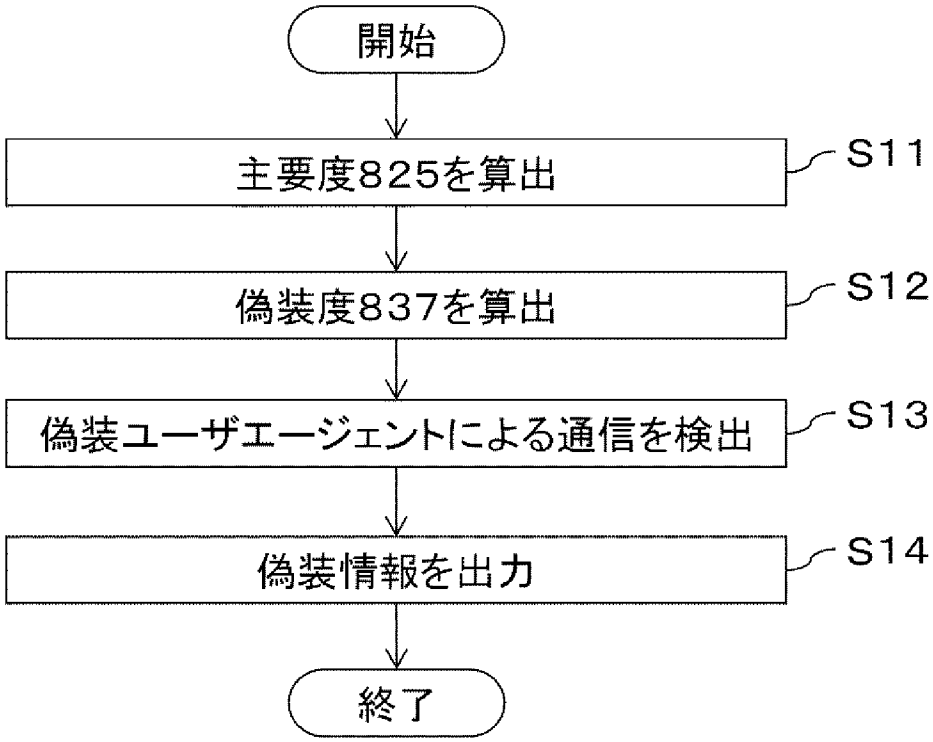
[図3]



[図4]


700 コンピュータ
706
通信部
701
CPU
702
記憶部
703
記憶装置
707
記録媒体
704
入力部
705
出力部

[図5]



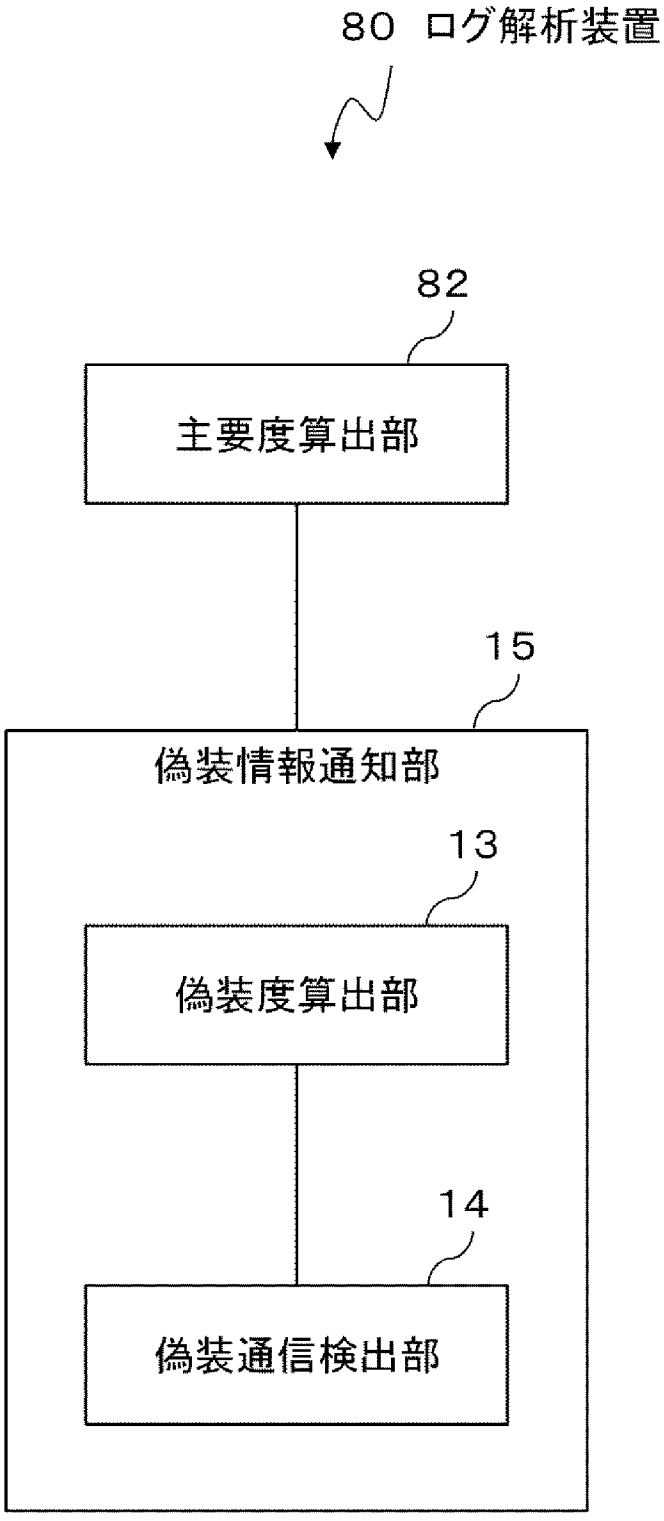
[図6]

811 クライアント識別子	813 ユーザエージェント文字列	824 ドメイン数	825 主要度
192.168.1.1	Mozilla/4.0 (XXX)	20	1.00
192.168.1.1	Mozilla/4.0 (YYY)	2	0.00
192.168.1.2	Mozilla/5.0 (ZZZ)	32	1.00
192.168.1.2	Mozilla/4.0 (XXX)	1	0.00
192.168.1.3	Mozilla/4.0 (YYY)	15	1.00

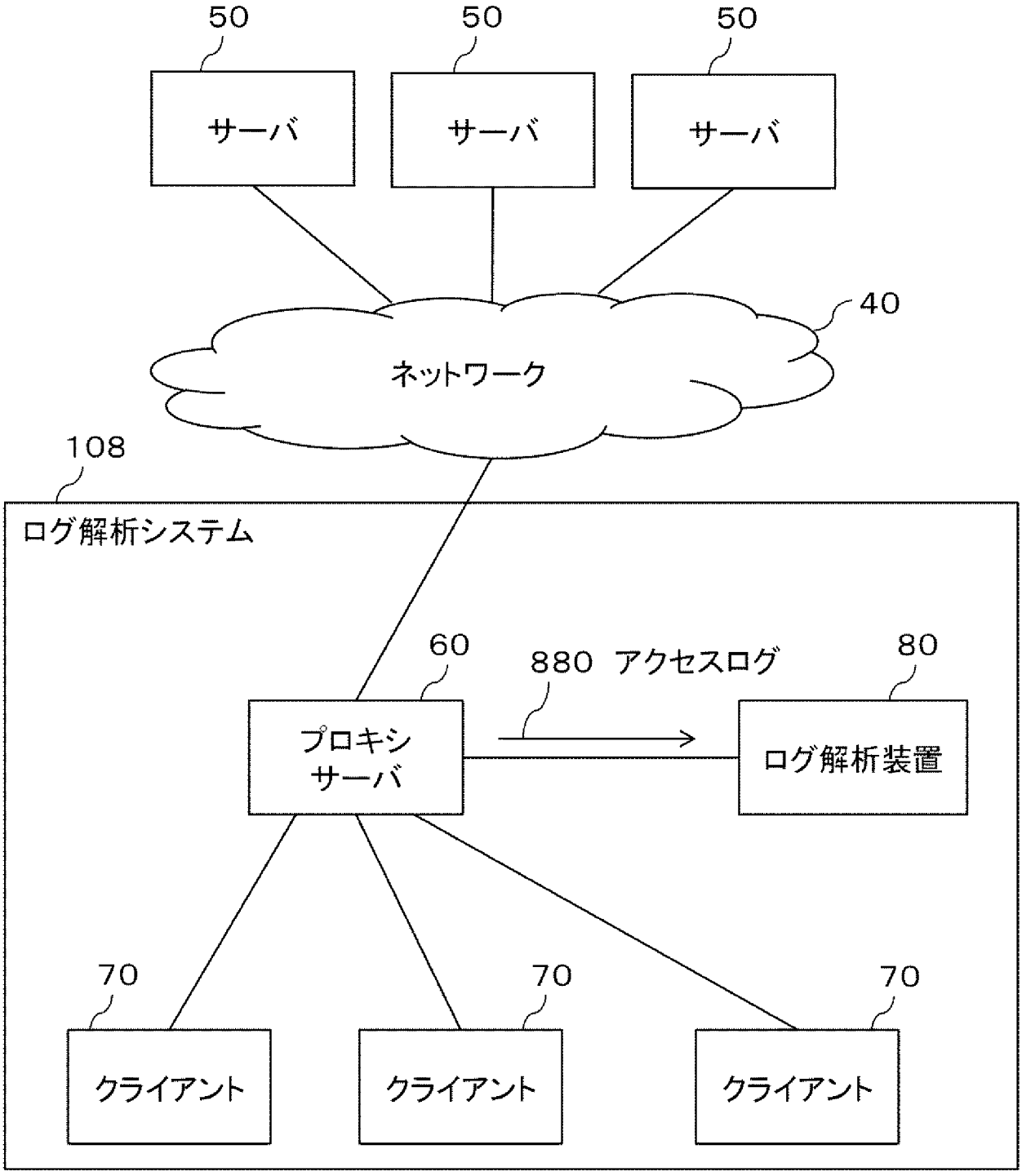
[図7]

812	836	825	837
サーバ識別子	<クライアント、通信制御手段>	主要度	偽装度
malicous.example.com	<192.168.1.1, Mozilla/4.0 (XXX)>	0.00	0.75
	<192.168.1.2, Mozilla/4.0 (XXX)>	0.00	
	<192.168.1.3, Mozilla/5.0 (YYY)>	1.00	
	<192.168.1.4, Mozilla/4.0 (XXX)>	0.00	

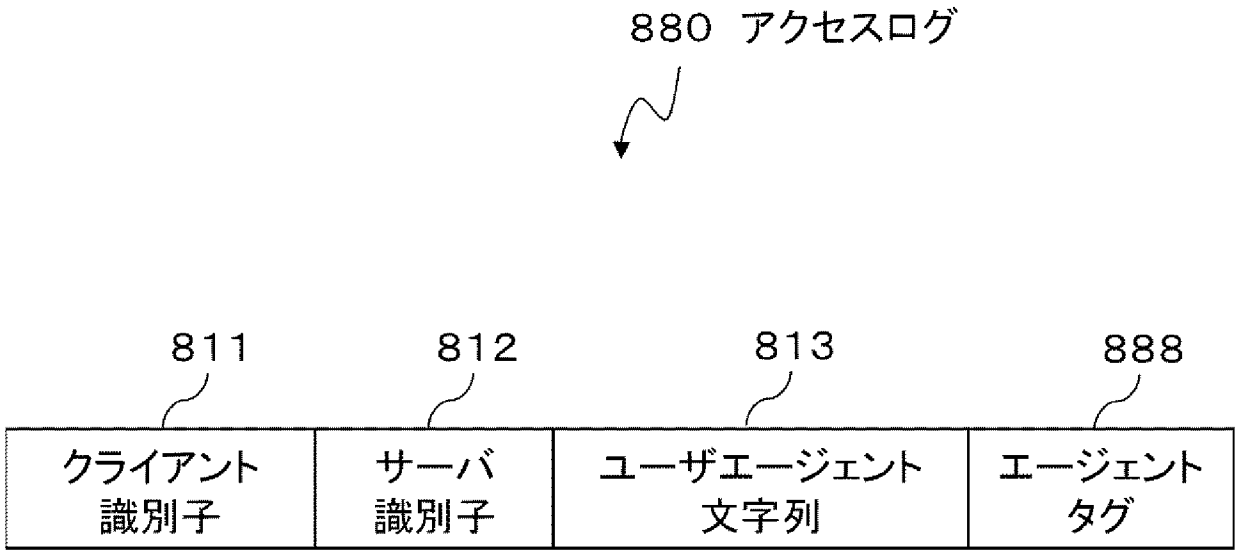
[図8]



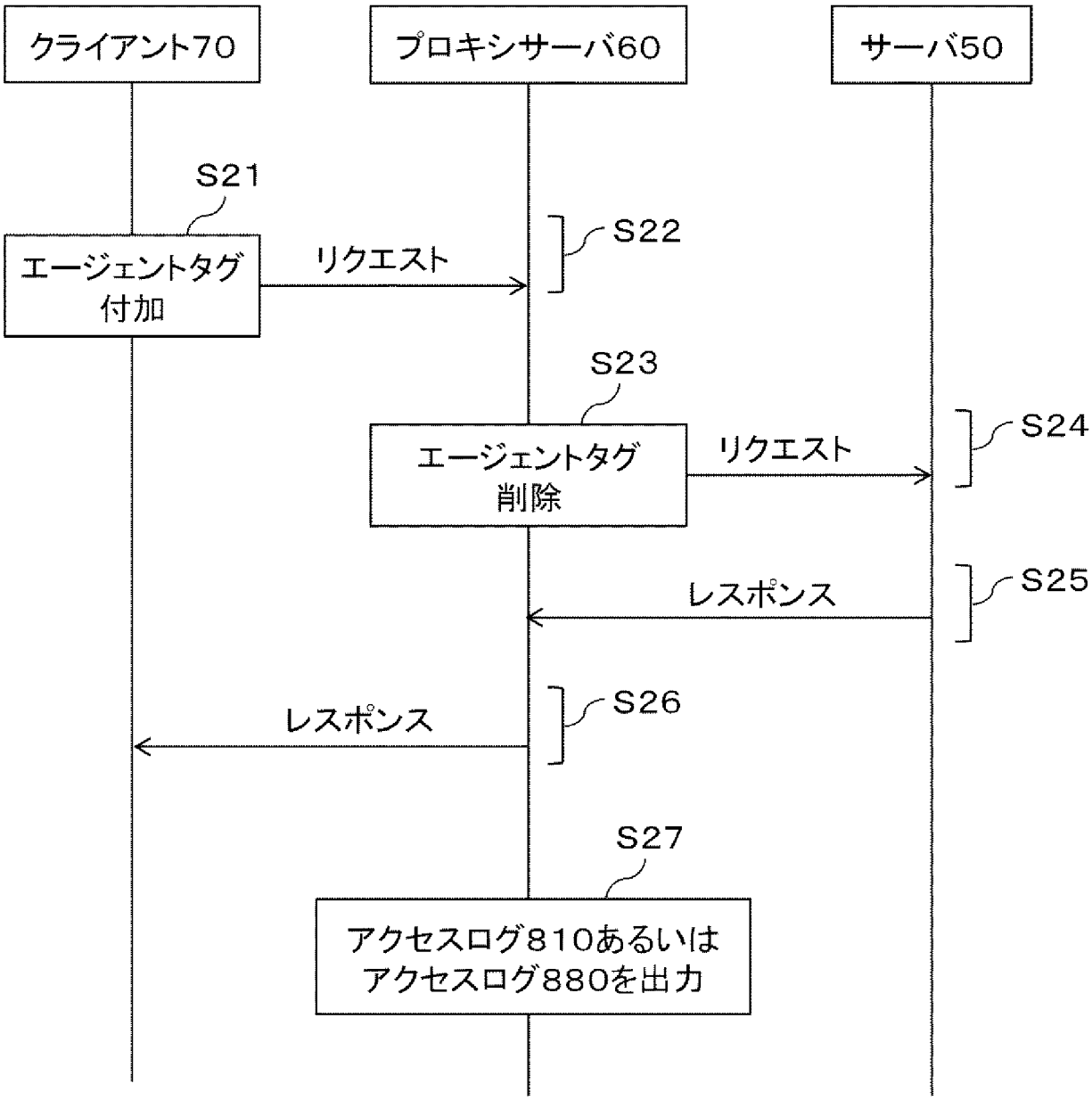
[図9]


50
50
50
サーバ
サーバ
サーバ
40
ネットワーク
108
ログ解析システム
60
880 アクセスログ
80
プロキシ
サーバ
ログ解析装置
70
70
70
クライアント
クライアント
クライアント

[図10]


880 アクセスログ
811
812
813
888
クライアント識別子
サーバ識別子
ユーザエージェント文字列
エージェントタグ

[図11]


クライアント70
プロキシサーバ60
サーバ50
S21
エージェントタグ付加
リクエスト
S22
S23
エージェントタグ削除
リクエスト
S24
レスポンス
S25
レスポンス
S26
S27
アクセスログ810あるいはアクセスログ880を出力

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/002476

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/55(2013.01)i, *G06F13/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/55, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2012/0143650 A1 (Thomass CROWLEY et al.), 07 June 2012 (07.06.2012), paragraphs [0011] to [0015], [0017] to [0020], [0022] to [0024], [0041], [0049] to [0066], [0074] to [0077], [0095]; fig. 1 to 7 (Family: none)	1,4,6,9,10 2-3,5,7-8
Y	JP 2011-233081 A (KDDI Corp.), 17 November 2011 (17.11.2011), paragraphs [0034], [0037] to [0038] (Family: none)	2-3

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 July 2015 (15.07.15)	28 July 2015 (28.07.15)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/002476

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"'Atarashii Type no Kogeki' no Taisaku ni Muketa Sekkei·Un'yo Guide", revised 2nd edition, Information-technology Promotion Agency, Japan Security Center [online], 2011.11, [retrieval date 15 July 2015 (15.07.2015)], Internet <URL:https://www.ipa.go.jp/files/000017308.pdf>	5,7-8
Y	JP 11-306067 A (Osaka Gas Co., Ltd.), 1999.11.05, paragraphs [0051], [0081]; fig. 5, 11 (Family: none)	8
A	JP 2003-280945 A (Hitachi Information Systems, Inc.), 03 October 2003 (03.10.2003), paragraphs [0002] to [0005], [0010] to [0011], [0017] to [0021]; fig. 1 to 3 (Family: none)	1-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／００２４７６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55(2013.01)i, G06F13/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55, G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X Y	US 2012/0143650 A1 (Thomass CROWLEY et al.) 2012.06.07, 段落［００１１］－［００１５］、［００１７］－［００２０］、［００２２］－［００２４］、［００４１］、［００４９］－［００６６］、［００７４］－［００７７］、［００９５］、 ＦＩＧＵＲＥ　１－ＦＩＧＵＲＥ　７（ファミリーなし）	1,4,6,9,10 2-3,5,7-8
Y	JP 2011-233081 A（ＫＤＤＩ株式会社）2011.11.17, 段落［００３４］、［００３７］－［００３８］（ファミリーなし）	2-3

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１５．０７．２０１５	２８．０７．２０１５

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　４２２９
青木　重徳
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Ｙ	“「新しいタイプの攻撃」の対策に向けた設計・運用ガイド”，改訂第２版，独立行政法人情報処理推進機構セキュリティセンター［online］，2011.11，［検索日　2015.07.15］，インターネット<ＵＲＬ：https://www.ipa.go.jp/files/000017308.pdf>	5,7-8
Ｙ	JP 11-306067 A（大阪瓦斯株式会社）1999.11.05，段落［００５１］、［００８１］、[図５]、[図１１］（ファミリーなし）	8
Ａ	JP 2003-280945 A（株式会社日立情報システムズ）2003.10.03，段落［０００２］－［０００５]、［００１０］－［００１１]、[００１７］－［００２１]、[図１］－［図３］（ファミリーなし）	1-10