

(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
2022年10月20日(20.10.2022)



(10) 国際公開番号

WO 2022/219683 A1

(51) 国際特許分類:
H04L 12/70 (2013.01)

(21) 国際出願番号: PCT/JP2021/015195

(22) 国際出願日: 2021年4月12日(12.04.2021)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

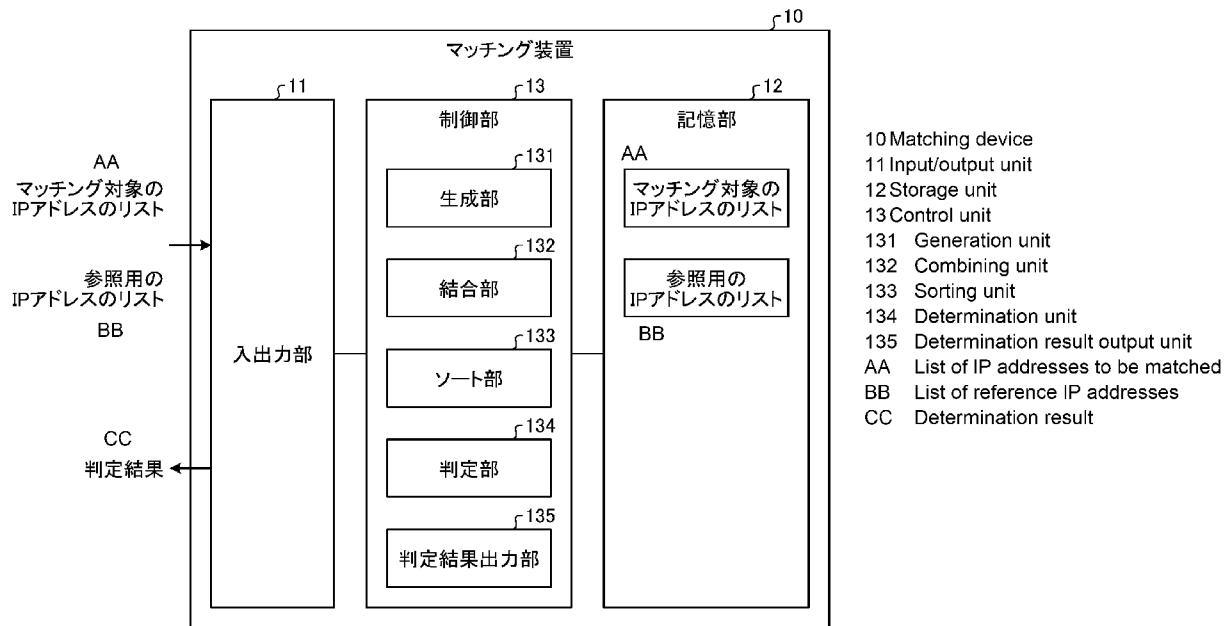
(72) 発明者: 渡邊 卓弥 (WATANABE, Takuya); 〒1808585 東京都武蔵野市緑町3丁目9-1 NTT 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号 虎の門三井ビルディング 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH,

(54) Title: MATCHING DEVICE, MATCHING METHOD, AND MATCHING PROGRAM

(54) 発明の名称: マッチング装置、マッチング方法、および、マッチングプログラム



(57) Abstract: A matching device (10), for each range of reference IP addresses, generates a record for a starting IP address and a record for an ending IP address for the relevant IP address range, and joins the records with a record indicating an IP address to be matched. Next, the matching device (10) performs sorting by: using, as a primary key, the IP addresses of the group of combined records; and using, as a secondary key, information indicating a record for the IP address to be matched, the record indicating the starting IP address, or the record indicating the ending IP address. After sorting, if there is a record for an IP address to be matched between a record indicating the starting IP address and a recording indicating the ending IP address for one of the IP address ranges, the matching device (10) determines that the IP address

KN, KP, KR, KW, 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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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).

添付公開書類：

一 国際調査報告(条約第21条(3))

to be matched matches said IP address range.

(57) 要約：マッチング装置（10）は、参照用のIPアドレスの範囲ごとに、IPアドレスの範囲の開始IPアドレスのレコードおよび終了IPアドレスのレコードを生成し、マッチング対象のIPアドレスを示すレコードと結合する。次に、マッチング装置（10）は、結合されたレコード群のIPアドレスを主キーとし、マッチング対象のIPアドレスのレコードか、開始IPアドレスを示すレコードか、終了IPアドレスのレコードかを示す情報を副キーとしてソートする。そして、マッチング装置（10）は、ソート後、いずれかのIPアドレスの範囲における開始IPアドレスを示すレコードと終了IPアドレスを示すレコードとの間に、マッチング対象のIPアドレスのレコードがある場合、当該マッチング対象のIPアドレスは、当該IPアドレスの範囲にマッチすると判定する。

明 細 書

発明の名称：

マッチング装置、マッチング方法、および、マッチングプログラム

技術分野

[0001] 本発明は、IPアドレスのマッチング装置、マッチング方法、および、マッチングプログラムに関する。

背景技術

[0002] サーバ等への疑わしいアクセスを検知するため、サーバへのアクセスログに示されるアクセスのうち、Proxyサーバや悪性IPアドレスからのアクセスはどれか、また、Proxyサーバからのアクセスがある場合、どのような種別のProxyサーバからのアクセスかを特定することが行われる。

[0003] ここでサーバが多数のアクセスを受け付けるサーバである場合、大量のアクセス元のIPアドレス（単体）のリストと、ProxyサーバのIPアドレスや悪性IPアドレスのリスト等の大量のIPアドレス（IPアドレスのレンジを含む）のリストとのマッチングを行う必要がある。

先行技術文献

非特許文献

[0004] 非特許文献1：N.Yazdani, et al., Fast and Scalable schemes for the IP address Lookup Problem, High Performance Switching and Routing, 2000. ATM 2000.

非特許文献2：Changhoon Yim, et al., Efficient Binary Search for IP Address Lookup, IEEE Communications Letters (Volume: 9, Issue: 7, July 2005)

非特許文献3：Ju Hyoung Mun, et al., New Approach for Efficient IPAddress Lookup Using a Bloom Filter in Trie Based Algorithms, IEEE Transactions on Computers (Volume: 65, Issue: 5, May 1 2016)

発明の概要

発明が解決しようとする課題

- [0005] ここで、アクセス元のIPアドレスの数や、ProxyサーバのIPアドレスおよび悪性IPアドレスのリスト（参照用のIPアドレスのリスト）のIPアドレスのレンジの数が膨大である場合、マッチングに要する時間が膨大になる。
- [0006] 例えば、アクセス元のIPアドレスの数がMであり、参照用のIPアドレスのリストにおけるIPアドレスのレンジの数がNである場合、IPアドレスのマッチングに要する時間計算量は $O(MN)$ となる。
- [0007] また、参照用のIPアドレスのリストにおけるIPアドレスのレンジを展開して得られたIPアドレス群と、アクセス元のIPアドレスそれぞれとをハッシュ等でマッチングすることも考えられる。このような方法によれば、マッチングに要する時間計算量は $O(M)$ となるが、参照用のIPアドレスのリストの示されるIPアドレスのレンジの大きさによっては、メモリ使用量（空間計算量）が膨大になる可能性がある。
- [0008] なお、IPアドレスlookupにおける高速マッチング方法（非特許文献1，2，3参照）もあるが、この方法は、アクセス元のIPアドレスが、複数のIPアドレスのレンジにマッチする場合については考慮されていない。
- [0009] そこで、本発明は、前記した問題を解決し、大量のIPアドレスのリストのマッチングを行う際の計算量を低減することを課題とする。

課題を解決するための手段

- [0010] 前記した課題を解決するため、本発明は、参照用のIPアドレスの範囲を示すリストにおける前記IPアドレスの範囲ごとに、前記IPアドレスの範囲の開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードを生成する生成部と、前記参照用のIPアドレスの範囲それぞれの開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードと、マッチング対象のIPアドレスを示すレコードとを結合する結合部と、前記結合されたレコード群を、前記レコードのIPアドレスを主キーとし、前記レコードが、前記マッチング対象のIPアドレスのレコードか、前記開始IPアドレスを示すレコードか、

前記終了IPアドレスのレコードかを示す情報を副キーとしてソートするソート部と、前記ソートされたレコード群において、いずれかの前記IPアドレスの範囲の開始IPアドレスを示すレコードと終了IPアドレスを示すレコードとの間に、前記マッチング対象のIPアドレスのレコードがある場合、前記マッチング対象のIPアドレスは、当該IPアドレスの範囲にマッチすると判定する判定部と、前記判定の結果を出力する判定結果出力部とを備えることを特徴とする。

発明の効果

[0011] 本発明によれば、大量のIPアドレスのリストのマッチングを行う際の計算量を低減することができる。

図面の簡単な説明

[0012] [図1]図1は、マッチング装置の概要を説明する図である。

[図2]図2は、マッチング装置の動作概要を説明する図である。

[図3]図3は、マッチング装置の動作概要を説明する図である。

[図4]図4は、マッチング装置の構成例を示す図である。

[図5]図5は、マッチング装置の処理手順の例を示すフローチャートである。

[図6]図6は、マッチング装置により判定の例を示す図である。

[図7]図7は、マッチング装置によるIPアドレスのマッチングの適用例を示す図である。

[図8]図8は、マッチングプログラムを実行するコンピュータの例を示す図である。

発明を実施するための形態

[0013] 以下、図面を参照しながら、本発明を実施するための形態（実施形態）について説明する。本発明は、以下に説明する実施形態に限定されない。

[0014] なお、以下の説明において、マッチング装置は、マッチング対象のIPアドレスのリストと、参照用のIPアドレスのリストとのマッチングを行う。参照用のIPアドレスのリストは、例えば、悪性である可能性のあるIPアドレスのリストであり、ProxyサーバのIPアドレスのリスト、悪性IPアドレスのリスト

等である。

[0015] また、マッチング対象のIPアドレスのリストにおけるIPアドレス群は、それぞれ単体のIPアドレスである場合を例に説明する。また、参照用のIPアドレスのリストにおけるIPアドレス群は、それぞれ単体のIPアドレスまたはIPアドレスの範囲（レンジ）である場合を例に説明する。また、各リストは、例えば、総量が1 M以上の大規模なリストであるものとする。

[0016] [概要]

まず、図1を用いて、本実施形態のマッチング装置の概要を説明する。マッチング装置は、マッチング対象のIPアドレスのリスト（例えば、アクセスログから取得したアクセス元のIPアドレス等）と、参照用のIPアドレスのリストとをマッチングする。

[0017] 例えば、マッチング装置は、アクセス元のIPアドレスのリストと、参照用のIPアドレスのリストとをマッチングすることにより、各アクセスがProxyサーバ経由であるか否か等を判定する。例えば、マッチング装置は、アクセス元のIPアドレスが、参照用のIPアドレスのリストのProxyサーバのIPアドレス（IPアドレスのレンジ）に該当する場合、当該アクセスはProxyサーバ経由であると判定する。これにより、マッチング装置は、当該アクセス元のIPアドレスからのアクセスが、悪性のアクセスである可能性があるか否かを判定することができる。

[0018] 図2、図3を用いて、マッチング装置の動作概要を説明する。まず、マッチング装置は、参照用のIPアドレスのリストにおけるIPアドレスのレンジごとにインデックスを割り当てる（図2の（1）参照用のIPアドレスのリストにインデックスを割り当てる）。

[0019] 次に、マッチング装置は、参照用のIPアドレスのリストにおける各IPアドレスのレンジを、レンジの開始IPアドレスのレコードとレンジの終了IPアドレスのレコードとに分割する（（2）参照用のIPアドレスのリストのレンジを開始IPアドレスと終了IPアドレスに分割する）。

[0020] このときマッチング装置は、開始IPアドレスのレコードには、開始IPアド

レスのレコードであることを示す情報（例えば、BEGIN）を付与し、終了IPアドレスのレコードには、終了IPアドレスのレコードであることを示す情報（例えば、END）を付与する。

[0021] 次に、マッチング装置は、（２）の処理を行ったリストと、マッチング対象のIPアドレスのリストとを結合する（（３）マッチング対象のIPアドレスのリストと結合する）。このときマッチング装置は、マッチング対象のIPアドレスのレコードに、マッチング対象のIPアドレスのレコードであることを示す情報（例えば、TARGET）を付与する。

[0022] 図３の説明に移る。マッチング装置は、図２の（３）の処理を行ったリストの各レコードに対し、下記のルールで昇順のソートを行う（（４）下記のルールで昇順のソートを行う）。

[0023] 主キー：IPアドレス（IPアドレスを整数値としてソート）

副キー：BEGIN<TARGET<ENDの順にソート

[0024] 上記のルールにより各レコードは、例えば、図３の符号３０１に示すようにソートされる。

[0025] その後、マッチング装置は、（４）でソートされた各レコードについて、上から順に、同じインデックスを持つ開始IPアドレスのレコードと終了IPアドレスのレコードとの間に、マッチング対象のIPアドレスのレコードがあるか否かを判定する（（５）上から順に処理）。

[0026] 例えば、マッチング装置は、図３の符号３０２に示すリストの破線で囲んだ部分について、インデックス０（１．１．１．１～１．１．１．１０）の開始IPアドレス（BEGIN）と終了IPアドレス（END）との間に、マッチング対象のIPアドレス（TARGET）１．１．１．２があると判定する。よって、マッチング装置は、マッチング対象のIPアドレス１．１．１．２が、参照用のIPアドレスのインデックス０（１．１．１．１～１．１．１．１０）のIPアドレスのレンジに含まれる（マッチする）と判定する。

[0027] マッチング装置が、上記のようにして各IPアドレスのリストのマッチングを行うことにより、各リストそれぞれが大規模なものであっても、マッチングに要する計算量を低減することができる。

[0028] 例えば、マッチング対象のIPアドレスのリストのIPアドレス数がMであり、参照用のIPアドレスのリストのIPアドレスのレンジの数がNである場合、各リストのIPアドレスのマッチングに要する空間計算量を $O(M+N)$ にすることができる。また、例えば、マッチングに用いるソートアルゴリズムがTimsortである場合、各リストのIPアドレスのマッチングに要する時間計算量を、 $O((M+N) \log(M+N))$ にすることができる。

[0029] [構成例]

次に、図4を用いてマッチング装置の構成例を説明する。図4に示すようにマッチング装置10は、入出力部11と、記憶部12と、制御部13とを備える。

[0030] 入出力部11は、各種データの入出力を司るインターフェースである。例えば、入出力部11は、マッチング対象のIPアドレスのリスト、参照用のIPアドレスのリスト等の入力を受け付ける。なお、各リストのIPアドレスは、IPv4のIPアドレスでもよいし、IPv6のIPアドレスでもよい。

[0031] 記憶部12は、制御部13が各種処理を実行する際に参照する各種データを記憶する。例えば、記憶部12は、入出力部11経由で入力されたマッチング対象のIPアドレスのリストや、参照用のIPアドレスのリストを記憶する。また、記憶部12は、制御部13がマッチングを行う過程で作成するデータを一時的に記憶する。

[0032] 制御部13は、マッチング装置10全体の制御を司る。制御部13は、例えば、生成部131と、結合部132と、ソート部133と、判定部134と、判定結果出力部135とを備える。

[0033] 生成部131は、参照用のIPアドレスのリストにおけるIPアドレスのレンジごとに、当該IPアドレスのレンジの開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードを生成する。

[0034] 例えば、生成部131は、まず、参照用のIPアドレスのリストにおけるIPアドレスのレンジごとに、インデックスを付与する（図2の（1）参照）。そして、生成部131は、IPアドレスのレンジそれぞれについて、当該IPア

ドレスのレンジの開始IPアドレスのレコードおよび終了IPアドレスのレコードを生成する。

[0035] そして、生成部131は、IPアドレスのレンジの開始IPアドレスのレコードには、当該レコードが開始IPアドレスのレコードであることを示す情報（例えば、BEGIN）を付与する。また、生成部131は、IPアドレスのレンジの終了IPアドレスのレコードには、当該レコードが終了IPアドレスのレコードであることを示す情報（例えば、END）を付与する（図2の（2）参照）。

[0036] 結合部132は、生成部131により生成されたレコードと、マッチング対象のIPアドレスのリストのIPアドレスのレコードとを結合する。また、このとき、結合部132は、マッチング対象のIPアドレスのレコードに、当該レコードがマッチング対象のIPアドレスのレコードである旨の情報（例えば、TARGET）を付与する（図2の（3）参照）。

[0037] ソート部133は、結合部132により結合されたレコード群を、各レコードのIPアドレスを主キーとし、各レコードがマッチング対象のIPアドレスのレコードか、開始IPアドレスのレコードか、終了IPアドレスのレコードかを示す情報（例えば、TARGET、BEGIN、END）を副キーとしてソートする（図3の（4）参照）。例えば、ソート部133は、各レコードをBEGIN<TARGET<ENDの昇順でソートする。

[0038] これによりソート部133は、例えば、TARGETが付されたレコードのIPアドレスと、BEGINまたはENDが付されたレコードのIPアドレスとが一致する場合でも、BEGINが付されたレコードとENDが付されたレコードとの間に、TARGETが付されたレコードが配置されるようにソートすることができる。

[0039] なお、ソート部133が用いるソートアルゴリズムは、例えば、Timsort等である。

[0040] 判定部134は、ソート部133によりソートされたレコードにおいて、参照用のIPアドレスのリストにおけるいずれかのIPアドレスのレンジの開始IPアドレスのレコードと終了IPアドレスのレコードとの間に、マッチング対象のIPアドレスのレコードがある場合（図3の（5）参照）、当該マッチング

対象のIPアドレスは、当該IPアドレスのレンジに該当すると判定する。

[0041] なお、ソート部133によりソートされたレコードにおいて、参照用のIPアドレスのリストにおけるいずれのIPアドレスのレンジの開始IPアドレスを示すレコードと終了IPアドレスを示すレコードとの間にも、マッチング対象のIPアドレスのレコードがない場合、判定部134は、マッチング対象のIPアドレスのリストの各IPアドレスは、参照用のIPアドレスのリストにおけるいずれのIPアドレスのレンジにも該当しないと判定する。

[0042] 判定結果出力部135は、判定部134による判定の結果を出力する。例えば、判定部134により、マッチング対象のIPアドレスが、悪性IPリストのIPアドレスのレンジに該当すると判定された場合、判定結果出力部135は、マッチング対象のIPアドレスからのアクセスは、悪性のアクセスである可能性がある旨の判定結果を出力する。

[0043] また、判定結果出力部135は、マッチング対象のIPアドレスがマッチするIPアドレスのレンジの属性情報を判定結果として出力してもよい。例えば、判定部134により、マッチング対象のIPアドレスが、Web ProxyのIPアドレスのレンジおよびResidential ProxyのIPアドレスのレンジに含まれると判定された場合、判定結果出力部135は、マッチング対象のIPアドレスは、Web ProxyおよびResidential Proxyからのアクセスである旨の判定結果を出力してもよい。

[0044] [処理手順の例]

次に、図5を用いて、マッチング装置10の処理手順の例を説明する。なお、マッチング装置10は、参照用のIPアドレスのリストおよびマッチング対象のIPアドレスのリストを取得済みであるものとする。

[0045] まず、マッチング装置10の生成部131は、参照用のIPアドレスのリストにおける各IPアドレスのレンジのレコードにインデックスを割り当てる（S1）。次に、生成部131は、参照用のIPアドレスのリストの各IPアドレスのレンジのレコードを、開始IPアドレスのレコードと終了IPアドレスのレコードとに分割する（S2）。そして、結合部132は、S2で分割された

参照用のIPアドレスのリストを、マッチング対象のIPアドレスのリストのレコードと結合する（S3）。

[0046] S3の後、ソート部133は、S3で結合されたリストの各レコードを昇順にソートする（S4）。このときの主キーは、IPアドレスであり、副キーは、各レコードが、マッチング対象のIPアドレスのレコードか、開始IPアドレスのレコードか、終了IPアドレスのレコードかを示す情報（例えば、TARGET、BEGIN、END）である。

[0047] 例えば、ソート部133は、S3で結合されたリストの各レコードについて、主キーであるIPアドレスを整数値に変換した値が昇順になり、副キーであるTARGET、BEGIN、ENDが $BEGIN < TARGET < END$ であるとして昇順になるようソートする。

[0048] S4の後、判定部134は、ソート後の各レコードのうち、未処理のレコードについて上から順に、同じインデックスが付された開始IPアドレスのレコードと終了IPアドレスとの間に、マッチング対象のIPアドレスがあるか否かを判定する（S5）。

[0049] ここで判定部134が、同じインデックスが付された開始IPアドレスのレコードと終了IPアドレスとの間に、マッチング対象のIPアドレスがあると判定した場合（S5でYes）、当該マッチング対象のIPアドレスは、当該インデックスのIPアドレスのレンジに含まれる（マッチする）と判定する（S6）。そして、判定部134が、ソート後のすべてのレコードを処理済みと判定した場合（S7でYes）、S8へ進む。一方、判定部134が、未処理のレコードがあると判定した場合（S7でNo）、S5へ戻る。

[0050] S7で、判定部134が、ソート後のすべてのレコードを処理済みと判定した場合（S7でYes）、判定部134は、判定の結果を判定結果出力部135に出力する。そして、判定結果出力部135は、判定部134による判定の結果を入出力部11経由で出力する（S8）。例えば、判定結果出力部135は、マッチング対象のIPアドレスが該当する（マッチする）IPアドレスのレンジの属性情報（例えば、Web Proxy、Residential Proxy等）と

、マッチング対象のIPアドレスとを出力する。

[0051] マッチング装置 10 が上記の処理を行うことで、IPアドレスのリストがそれぞれ大規模なものであっても、マッチングに要する計算量を低減することができる。その結果、マッチング装置 10 は、大規模なIPアドレスのリスト同士でも、高速かつ高効率でマッチングすることができる。

[0052] 例えば、マッチング装置 10 が100万件のIPアドレスのリストと、100万件の参照用のIPアドレスのリストとをマッチングする場合、各リストのIPアドレスを1つ1つマッチングする場合と比べ、IPアドレス同士の比較回数を1/10000以下にすることができる。その結果、IPアドレスのリストのマッチングに要する時間を大幅に低減できる。

[0053] なお、前記した図5のS5の処理は、例えば、以下のようにして行ってもよい。例えば、判定部 134 は、未処理のレコードについて上から順に見ていき、BEGINが付与されたレコードを見つけると、当該レコードに付与されたインデックスのフラグを立てる。また、判定部 134 は、TARGETが付与されたレコードを見つけると、フラグが立っているインデックスに対応するIPアドレスのレンジに、当該TARGETが付与されたレコードのIPアドレスが含まれると判定する。また、判定部 134 は、ENDが付与されたレコードを見つけると、当該レコードに付与されたインデックスのフラグを降ろす。

[0054] 判定部 134 は、上記の処理を上から順に最後のレコードまで実行する。そして、判定部 134 は、フラグの立っているインデックスに対応するIPアドレスのレンジを、マッチング対象のIPアドレスがマッチするIPアドレスのレンジとする。このようにすることで、判定部 134 は、例えば、マッチング対象のIPアドレスが複数のIPアドレスのレンジに含まれる場合でも、漏れなく検出することができる。

[0055] 例えば、図6に示すようにマッチング対象のIPアドレスが該当する複数のIPアドレスのレンジ同士が、入れ子状になっている場合（符号601参照）や、部分的に重複している場合（符号602参照）でも、漏れなく検出することができる。

[0056] 例えば、符号 601 に示す例の場合、判定部 134 は、マッチング対象の IP アドレス「1.1.1.2」が、インデックス 0 (1.1.1.1-1.1.1.10) およびインデックス 1 (1.1.1.1-1.1.1.5) に含まれることを検出することができる。

[0057] また、符号 602 に示す例の場合、判定部 134 は、マッチング対象の IP アドレス「1.1.1.3」が、インデックス 0 (1.1.1.1-1.1.1.10) およびインデックス 2 (1.1.1.2-1.1.1.15) に含まれることを検出することができる。

[0058] [適用例]

図 7 を用いて、マッチング装置 10 による IP アドレスのリストのマッチングの適用例を説明する。例えば、マッチング装置 10 による IP アドレスのマッチングを、図 7 の (1) に示すような、あるショッピングサイトにおけるクレジットカード決済の IP (IP アドレス) ログと、あらかじめ用意した Proxy List とのマッチングに適用してもよい。ここで、IP ログに記載された IP アドレスが、あらかじめ用意した Proxy List のいずれかの IP アドレスのレンジに該当すれば、当該 IP ログに対応するアクセスは Proxy 経由の疑わしいアクセスと判断することができる。

[0059] また、マッチング装置 10 による IP アドレスのマッチングを、図 7 の (2) に示すような、あるウェブサイトにおけるサーバへのアクセスログと、あらかじめ用意した悪性 IP (IP アドレス) リストとのマッチングに適用してもよい。ここで、アクセスログに記載された IP アドレスが、あらかじめ用意した悪性 IP リストのいずれかの IP アドレスのレンジに該当すれば、当該 IP ログに対応するアクセスは乗っ取られた端末によるアクセス等と判断することができる。

[0060] [システム構成等]

また、図示した各部の各構成要素は機能概念的なものであり、必ずしも物理的に図示のように構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部又は一部を、各種の負荷や使用状況等に応じて、任意の単位で機能的又は物理的に分散・統合して構成することができる。さらに、各装置にて行われる各処理機能は、そ

の全部又は任意の一部が、CPU及び当該CPUにて実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0061] また、前記した実施形態において説明した処理のうち、自動的に行われるものとして説明した処理の全部又は一部を手動的に行うこともでき、あるいは、手動的に行われるものとして説明した処理の全部又は一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

[0062] [プログラム]

前記したマッチング装置10は、パッケージソフトウェアやオンラインソフトウェアとしてプログラムを所望のコンピュータにインストールさせることによって実装できる。例えば、上記のプログラムを情報処理装置に実行させることにより、情報処理装置をマッチング装置10として機能させることができる。ここで言う情報処理装置には、デスクトップ型又はノート型のパーソナルコンピュータが含まれる。また、その他にも、情報処理装置にはスマートフォン、携帯電話機やPHS (Personal Handyphone System) 等の移動体通信端末、さらには、PDA (Personal Digital Assistant) 等の端末等がその範疇に含まれる。

[0063] また、マッチング装置10は、ユーザが使用する端末装置をクライアントとし、当該クライアントに上記の処理に関するサービスを提供するサーバ装置として実装することもできる。この場合、サーバ装置は、Webサーバとして実装することとしてもよいし、アウトソーシングによって上記の処理に関するサービスを提供するクラウドとして実装することとしてもかまわない。

[0064] 図8は、マッチングプログラムを実行するコンピュータの一例を示す図である。コンピュータ1000は、例えば、メモリ1010、CPU1020を有する。また、コンピュータ1000は、ハードディスクドライブインタフェース1030、ディスクドライブインタフェース1040、シリアルポ

ートインタフェース 1050、ビデオアダプタ 1060、ネットワークインタフェース 1070を有する。これらの各部は、バス 1080によって接続される。

[0065] メモリ 1010は、ROM (Read Only Memory) 1011及びRAM (Random Access Memory) 1012を含む。ROM 1011は、例えば、BIOS (Basic Input Output System) 等のブートプログラムを記憶する。ハードディスクドライブインタフェース 1030は、ハードディスクドライブ 1090に接続される。ディスクドライブインタフェース 1040は、ディスクドライブ 1100に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブ 1100に挿入される。シリアルポートインタフェース 1050は、例えばマウス 1110、キーボード 1120に接続される。ビデオアダプタ 1060は、例えばディスプレイ 1130に接続される。

[0066] ハードディスクドライブ 1090は、例えば、OS 1091、アプリケーションプログラム 1092、プログラムモジュール 1093、プログラムデータ 1094を記憶する。すなわち、上記のマッチング装置 10が実行する各処理を規定するプログラムは、コンピュータにより実行可能なコードが記述されたプログラムモジュール 1093として実装される。プログラムモジュール 1093は、例えばハードディスクドライブ 1090に記憶される。例えば、マッチング装置 10における機能構成と同様の処理を実行するためのプログラムモジュール 1093が、ハードディスクドライブ 1090に記憶される。なお、ハードディスクドライブ 1090は、SSD (Solid State Drive) により代替されてもよい。

[0067] また、上述した実施形態の処理で用いられるデータは、プログラムデータ 1094として、例えばメモリ 1010やハードディスクドライブ 1090に記憶される。そして、CPU 1020が、メモリ 1010やハードディスクドライブ 1090に記憶されたプログラムモジュール 1093やプログラムデータ 1094を必要に応じてRAM 1012に読み出して実行する。

[0068] なお、プログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０９０に記憶される場合に限らず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ１１００等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、プログラムモジュール１０９３及びプログラムデータ１０９４は、ネットワーク（LAN（Local Area Network）、WAN（Wide Area Network）等）を介して接続される他のコンピュータに記憶されてもよい。そして、プログラムモジュール１０９３及びプログラムデータ１０９４は、他のコンピュータから、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

符号の説明

- [0069] １０ マッチング装置
- １１ 入出力部
- １２ 記憶部
- １３ 制御部
- １３１ 生成部
- １３２ 結合部
- １３３ ソート部
- １３４ 判定部
- １３５ 判定結果出力部

請求の範囲

[請求項1] 参照用のIPアドレスの範囲を示すリストにおける前記IPアドレスの範囲ごとに、前記IPアドレスの範囲の開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードを生成する生成部と、

前記参照用のIPアドレスの範囲それぞれの開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードと、マッチング対象のIPアドレスを示すレコードとを結合する結合部と、

前記結合されたレコード群を、前記レコードのIPアドレスを主キーとし、前記レコードが、前記マッチング対象のIPアドレスのレコードか、前記開始IPアドレスを示すレコードか、前記終了IPアドレスのレコードかを示す情報を副キーとしてソートするソート部と、

前記ソートされたレコード群において、いずれかの前記IPアドレスの範囲の開始IPアドレスを示すレコードと終了IPアドレスを示すレコードとの間に、前記マッチング対象のIPアドレスのレコードがある場合、前記マッチング対象のIPアドレスは、当該IPアドレスの範囲にマッチすると判定する判定部と、

前記判定の結果を出力する判定結果出力部と
を備えることを特徴とするマッチング装置。

[請求項2] 前記ソート部は、

前記結合されたレコード群を、各レコードのIPアドレスを主キーとし昇順でソートし、前記副キーについて、前記開始IPアドレスを示すレコード、前記マッチング対象のIPアドレスを示すレコード、前記終了IPアドレスを示すレコードの順になるようソートする

ことを特徴とする請求項1に記載のマッチング装置。

[請求項3] 前記判定部が、

前記マッチング対象のIPアドレスが、いずれかの前記IPアドレスの範囲にマッチすると判定した場合、

前記判定結果出力部は、

前記マッチング対象のIPアドレスからのアクセスは、悪性のアクセスである可能性がある旨の判定結果を出力する

ことを特徴とする請求項1に記載のマッチング装置。

[請求項4]

前記判定部が、

前記マッチング対象のIPアドレスが、いずれかの前記IPアドレスの範囲にマッチすると判定した場合、

前記判定結果出力部は、

前記マッチング対象のIPアドレスがマッチする前記IPアドレスの範囲それぞれの属性情報を出力する

ことを特徴とする請求項1に記載のマッチング装置。

[請求項5]

マッチング装置により実行されるマッチング方法であって、

参照用のIPアドレスの範囲を示すリストにおける前記IPアドレスの範囲ごとに、前記IPアドレスの範囲の開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードを生成する工程と、

前記参照用のIPアドレスの範囲それぞれの開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードと、マッチング対象のIPアドレスを示すレコードとを結合する工程と、

前記結合されたレコード群を、前記レコードのIPアドレスを主キーとし、前記レコードが、前記マッチング対象のIPアドレスのレコードか、前記開始IPアドレスを示すレコードか、前記終了IPアドレスのレコードかを示す情報を副キーとしてソートする工程と、

前記ソートされたレコード群において、いずれかの前記IPアドレスの範囲における開始IPアドレスを示すレコードと終了IPアドレスを示すレコードとの間に、前記マッチング対象のIPアドレスのレコードがある場合、前記マッチング対象のIPアドレスは、当該IPアドレスの範囲にマッチすると判定する工程と、

前記判定の結果を出力する工程と

を含むことを特徴とするマッチング方法。

[請求項6] 参照用のIPアドレスの範囲を示すリストにおける前記IPアドレスの範囲ごとに、前記IPアドレスの範囲の開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードを生成する工程と、

 前記参照用のIPアドレスの範囲それぞれの開始IPアドレスを示すレコードおよび終了IPアドレスを示すレコードと、マッチング対象のIPアドレスを示すレコードとを結合する工程と、

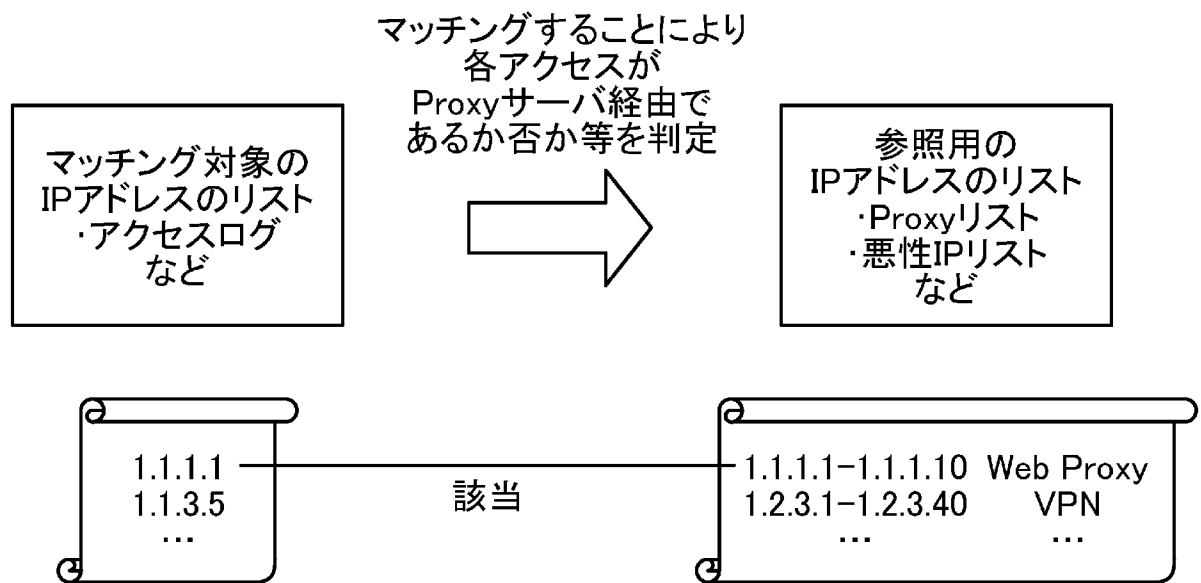
 前記結合されたレコード群を、前記レコードのIPアドレスを主キーとし、前記レコードが、前記マッチング対象のIPアドレスのレコードか、前記開始IPアドレスを示すレコードか、前記終了IPアドレスのレコードかを示す情報を副キーとしてソートするソート部と、

 前記ソートされたレコード群において、いずれかの前記IPアドレスの範囲における開始IPアドレスを示すレコードと終了IPアドレスを示すレコードとの間に、前記マッチング対象のIPアドレスのレコードがある場合、前記マッチング対象のIPアドレスは、当該IPアドレスの範囲にマッチすると判定する工程と、

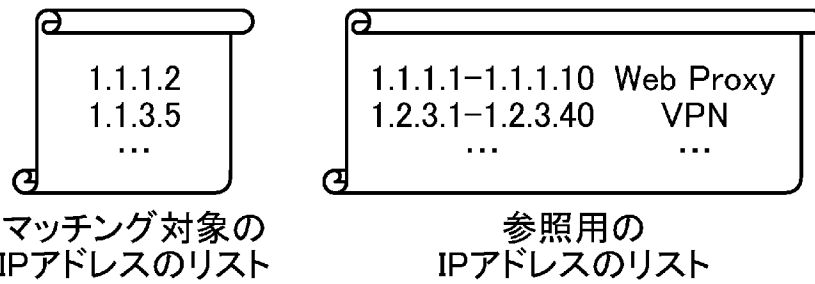
 前記判定の結果を出力する工程と

 をコンピュータに実行させることを特徴とするマッチングプログラム。

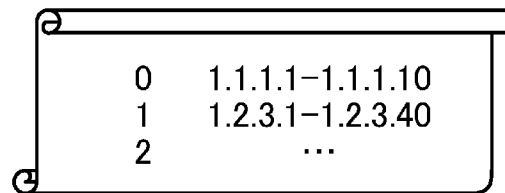
[図1]



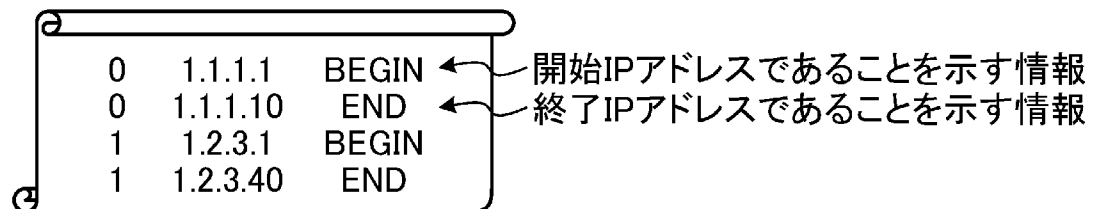
[図2]



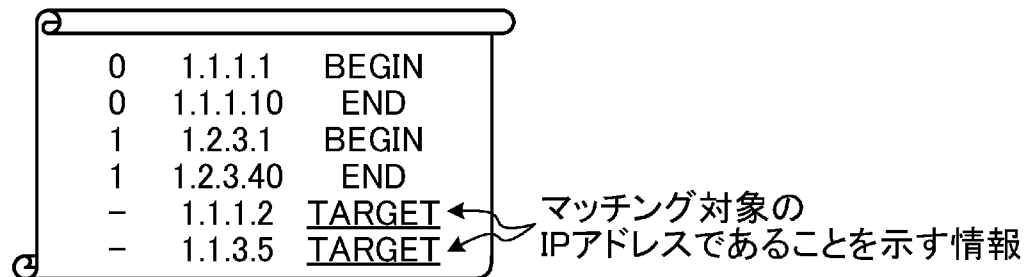
(1) 参照用のIPアドレスのリストにインデックスを割り当てる



(2) 参照用のIPアドレスのリストのレンジを開始IPアドレスと終了IPアドレスに分割する



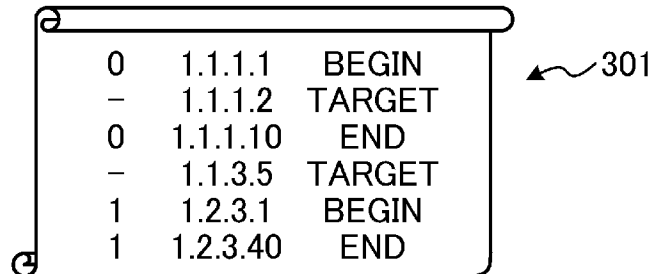
(3) マatching対象のIPアドレスのリストと結合する



[図3]

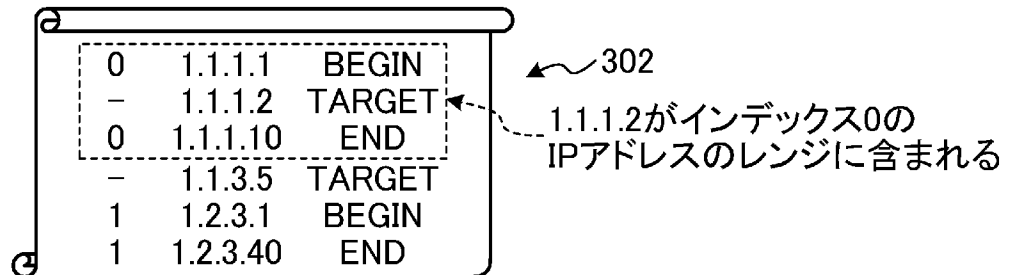
(4)下記のルールで昇順のソートを行う

- ・主キー IPアドレス(整数値としてソート)
- ・副キー BEGIN<TARGET<ENDの順でソート



0	1.1.1.1	BEGIN
-	1.1.1.2	TARGET
0	1.1.1.10	END
-	1.1.3.5	TARGET
1	1.2.3.1	BEGIN
1	1.2.3.40	END

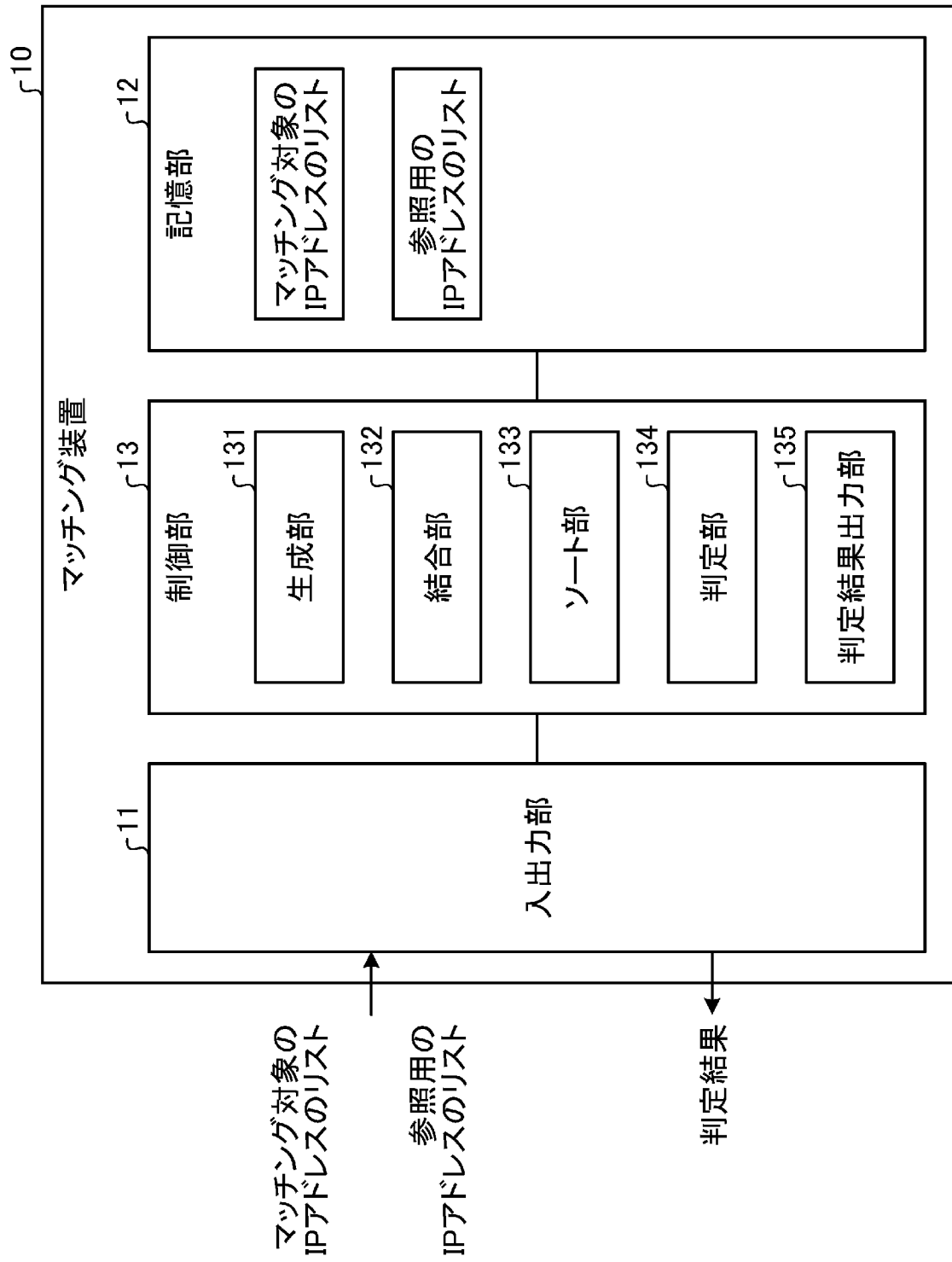
(5)上から順に処理



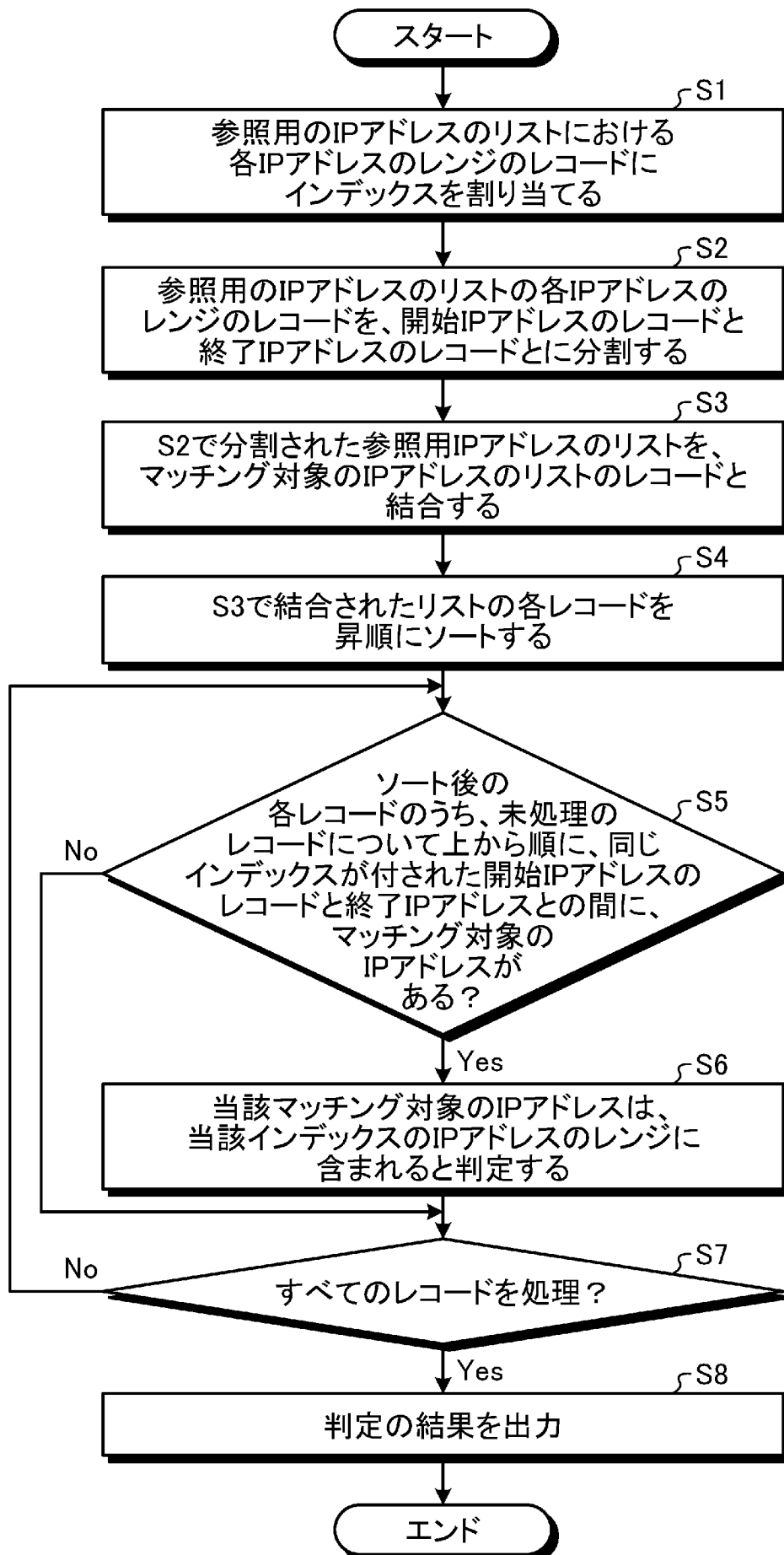
0	1.1.1.1	BEGIN
-	1.1.1.2	TARGET
0	1.1.1.10	END
-	1.1.3.5	TARGET
1	1.2.3.1	BEGIN
1	1.2.3.40	END

1.1.1.2がインデックス0のIPアドレスのレンジに含まれる

[図4]



[図5]



[図6]

インデックス

0	1.1.1.1	BEGIN	
1	1.1.1.1	BEGIN	
-	1.1.1.2	TARGET	
1	1.1.1.5	END	
0	1.1.1.10	END	

601 →

1.1.1.2がインデックス0
および1に含まれる

インデックス

0	1.1.1.1	BEGIN	
2	1.1.1.2	BEGIN	
-	1.1.1.3	TARGET	
0	1.1.1.10	END	
2	1.1.1.15	END	

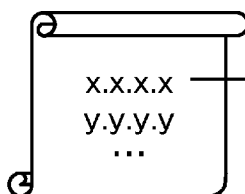
602 →

1.1.1.3がインデックス0
および2に含まれる

[図7]

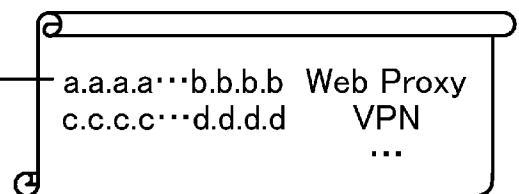
(1)

あるショッピングサイトにおける
クレジットカード決済のIPログ



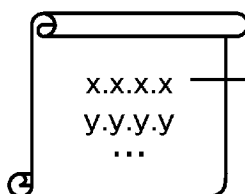
該当
(Proxy経由の疑わしい
アクセスと判断)

あらかじめ用意したProxy List



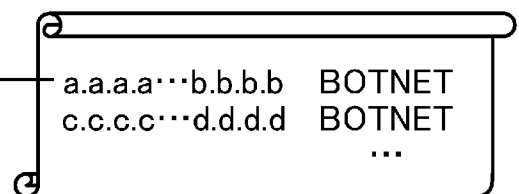
(2)

あるウェブサイトにおける
サーバーへのアクセスログ

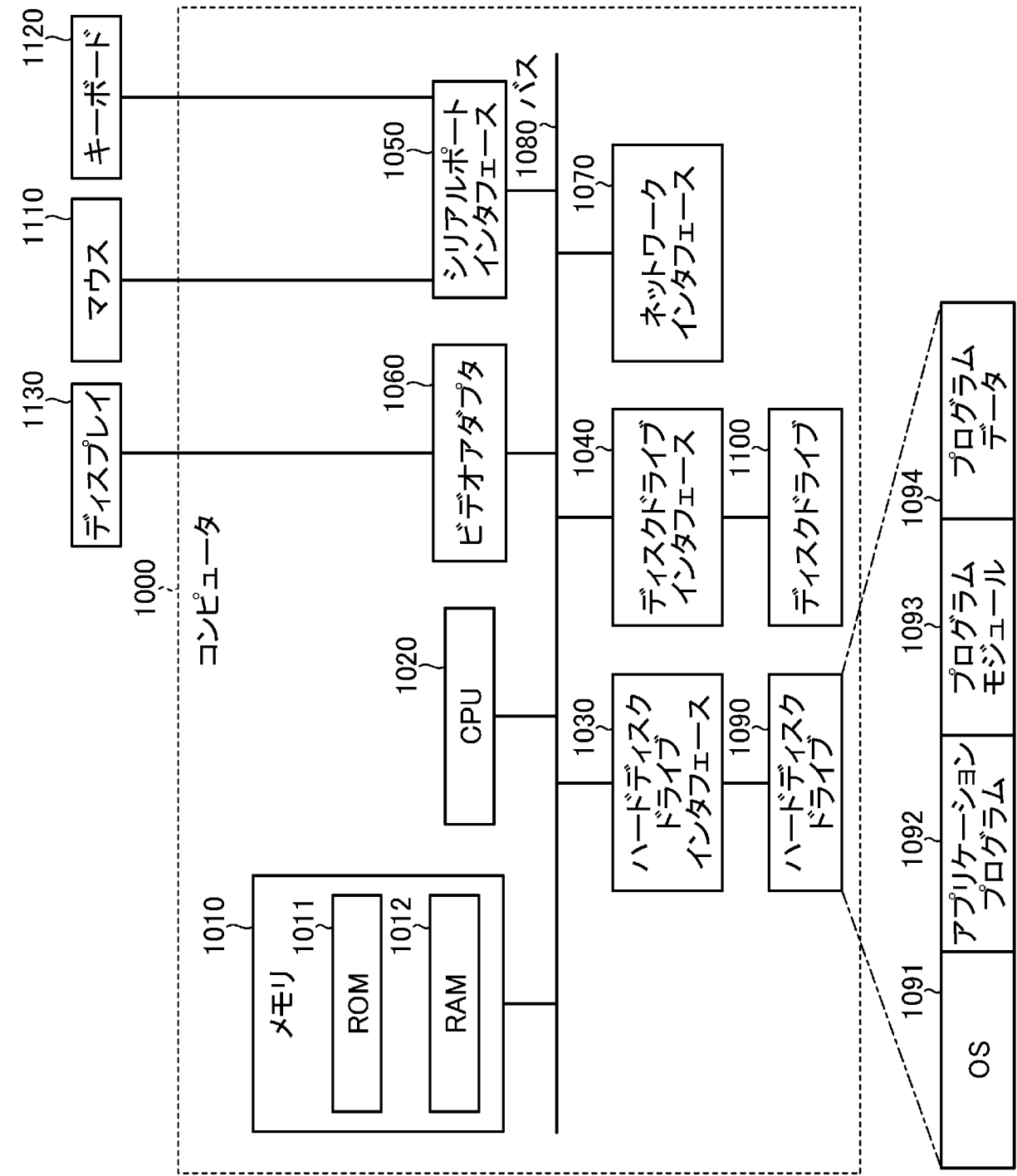


該当
(乗っ取られた端末による
アクセスと判断)

あらかじめ用意した悪性IPリスト



[図8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/015195

A. CLASSIFICATION OF SUBJECT MATTER**H04L 12/70**(2013.01)i

FI: H04L12/70 A

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)

H04L12/00-12/955

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

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2021
 Registered utility model specifications of Japan 1996-2021
 Published registered utility model applications of Japan 1994-2021

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.
A	BUTLER LAMPSON et al. IP Lookups Using Multiway and Multicolumn Search. IEEE/ACM TRANSACTIONS ON NETWORKING. June 1999, vol. 7, no. 3, pp. 324-334 IV. ADAPTING BINARY SEARCH FOR LONGEST MATCHING PREFIX SEARCH	1-6
A	US 2018/0063082 A1 (FORTRESS INFORMATION SECURITY) 01 March 2018 (2018-03-01) paragraphs [0003], [0013], [0015]-[0020], [0031]-[0038], fig. 1B, 3, etc.	1-6
A	US 6813645 B1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 02 November 2004 (2004-11-02) paragraphs [0149]-[0160], fig. 20-26, etc.	1-6
A	JP 2005-117211 A (NIPPON TELEGR & TELEPH CORP <NTT>) 28 April 2005 (2005-04-28) paragraphs [0001]-[0013], fig. 10-15, etc.	1-6
A	JP 2006-54637 A (RICOH CO LTD) 23 February 2006 (2006-02-23) paragraphs [0034]-[0039]	1-6

☐ 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

28 June 2021

Date of mailing of the international search report

06 July 2021

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
 Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/015195

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US	2018/0063082	A1	01 March 2018	US 2019/0158463 A1	
US	6813645	B1	02 November 2004	(Family: none)	
JP	2005-117211	A	28 April 2005	(Family: none)	
JP	2006-54637	A	23 February 2006	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 12/70(2013.01)i FI: H04L12/70 A														
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）） H04L12/00-12/955 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2021年</td> </tr> </table> 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）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2021年	日本国実用新案登録公報	1996 - 2021年	日本国登録実用新案公報	1994 - 2021年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2021年													
日本国実用新案登録公報	1996 - 2021年													
日本国登録実用新案公報	1994 - 2021年													
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												
A	Butler Lampson et al., IP Lookups Using Multiway and Multicolumn Search, IEEE/ACM TRANSACTIONS ON NETWORKING, 1999.06, VOL.7, NO.3, P.324-334 IV. ADAPTING BINARY SEARCH FOR LONGEST MATCHING PREFIX SEARCH	1-6												
A	US 2018/0063082 A1 (FORTRESS INFORMATION SECURITY) 01.03.2018 (2018 - 03 - 01) [0003], [0013], [0015]-[0020], [0031]-[0038], FIGs. 1B, 3等	1-6												
A	US 6813645 B1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 02.11.2004 (2004 - 11 - 02) [00149]-[0160], FIGs. 20-26等	1-6												
A	JP 2005-117211 A (日本電信電話株式会社) 28.04.2005 (2005 - 04 - 28) [0001]-[0013], 図10-15等	1-6												
A	JP 2006-54637 A (株式会社リコー) 23.02.2006 (2006 - 02 - 23) [0034]-[0039]	1-6												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 28.06.2021		国際調査報告の発送日 06.07.2021												
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 羽岡 さやか 5X 3149 電話番号 03-3581-1101 内線 3596												

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2021/015195

引用文献			公表日	パテントファミリー文献			公表日
US	2018/0063082	A1	01.03.2018	US	2019/0158463	A1	
US	6813645	B1	02.11.2004	(ファミリーなし)			
JP	2005-117211	A	28.04.2005	(ファミリーなし)			
JP	2006-54637	A	23.02.2006	(ファミリーなし)			