(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
2018年9月7日(07.09.2018)

WIPO | PCT

(10) 国際公開番号
WO 2018/159361 A1

(51) 国際特許分類:
G06F 21/56 (2013.01)

(21) 国際出願番号： PCT/JP2018/005772

(22) 国際出願日： 2018年2月19日(19.02.2018)

(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 2017-041122 2017年3月3日(03.03.2017) JP

(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).

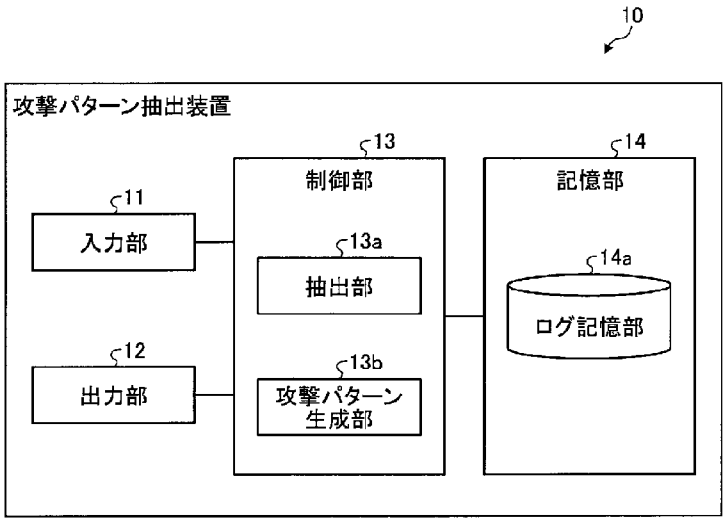
(72) 発明者: 折原 慎吾 (**ORIHARA, Shingo**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 佐藤 徹(**SATO, Tohru**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 嶋田 陽介(**SHIMADA, Yohsuke**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 岩城 悠太(**IWAKI, Yuta**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 鐘 揚(**ZHONG, Yang**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ 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

WO 2018/159361 A1

(54) **Title:** ATTACK PATTERN EXTRACTION APPARATUS, ATTACK PATTERN EXTRACTION METHOD, AND ATTACK PATTERN EXTRACTION PROGRAM

(54) 発明の名称： 攻撃パターン抽出装置、攻撃パターン抽出方法および攻撃パターン抽出プログラム



10 Attack pattern extraction apparatus
11 Input unit
12 Output unit
13 Control unit
13a Extraction unit
13b Attack pattern generation unit
14 Storage unit
14a Log storage unit

(57) **Abstract:** An attack pattern extraction apparatus (10) has: an extraction unit (13a); and an attack pattern generation unit (13b). The extraction unit (13a) extracts character strings common among parameters in a communication access log determined as being an attack. The attack pattern generation unit (13b) generates an attack pattern on the basis of a character string, the length of which is equal to or longer than a prescribed character string length, among the extracted continuous character strings.

［続葉有］

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, JO, JP, KE, KG, KH, 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, 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).

添付公開書類：

一　国際調査報告（条約第21条(3)）

(57) 要約：攻撃パターン抽出装置（１０）は、抽出部（１３ａ）および攻撃パターン生成部（１３ｂ）を有する。抽出部（１３ａ）は、攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する。そして、攻撃パターン生成部（１３ｂ）は、抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する。

明　細　書

発明の名称 ：

攻撃パターン抽出装置、攻撃パターン抽出方法および攻撃パターン抽出プログラム

技術分野

[0001] 本発明は、攻撃パターン抽出装置、攻撃パターン抽出方法および攻撃パターン抽出プログラムに関する。

背景技術

[0002] 近年、インターネットの普及に伴い、Ｗｅｂサーバに対する攻撃が急増している。このような攻撃の対策としてＩＤＳ(Intrusion Detection System)、ＩＰＳ(Intrusion Prevention System)、ＷＡＦ(Web Application Firewall)等によるネットワークへの不正侵入検知・防御システムが知られている。これらは主に、攻撃パターンをシグネチャとして覚えておき、シグネチャとマッチした通信を検知するものである。従って、新たな攻撃に対応するには、攻撃パターンに合わせてシグネチャを作成する必要がある。

[0003] 従来、シグネチャ等の攻撃パターンの生成においては、攻撃コードに共通した特徴を元にパラメータの形態素解析を行い、その結果の最長共通部分列（ＬＣＳ：Longest Common Subsequence）を算出して生成する手法が知られている。

先行技術文献

非特許文献

[0004] 非特許文献1：越智　勇貴、安部　剛、“Exploitに対するWAFシグネチャ自動生成の研究”、Computer Security Symposium 2016、pp.958-963.

発明の概要

発明が解決しようとする課題

[0005] しかしながら、上記した従来の技術では、適切な攻撃パターンを生成する

ことができない場合があるという課題があった。つまり、従来の技術では、既知の攻撃コードの特徴を元にしているため、未知の攻撃には形態素解析が適切に行われず、適切な攻撃パターンを生成できない場合があった。また、ＬＣＳ算出の際に、共通部分の文字列長を考慮していないため、偶然一致した短い文字列を有意な攻撃パターンとして生成してしまう可能性があるという課題があった。

課題を解決するための手段

[0006] 上述した課題を解決し、目的を達成するために、本発明の攻撃パターン抽出装置は、攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する抽出部と、前記抽出部によって抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する攻撃パターン生成部とを備えたことを特徴とする。

[0007] また、本発明の攻撃パターン抽出方法は、攻撃パターン抽出装置で実行される攻撃パターン抽出方法であって、攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する抽出工程と、前記抽出工程によって抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する攻撃パターン生成工程とを含んだことを特徴とする。

[0008] また、本発明の攻撃パターン抽出プログラムは、攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する抽出ステップと、前記抽出ステップによって抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する攻撃パターン生成ステップとをコンピュータに実行させることを特徴とする。

発明の効果

[0009] 本発明によれば、適切な攻撃パターンを生成することができるという効果を奏する。

図面の簡単な説明

[0010] [図1]図１は、第一の実施の形態に係る攻撃パターン抽出装置の概要を示す構

成図である。

[図2]図２は、テーブル初期化処理について説明する図である。

[図3]図３は、テーブル更新処理について説明する図である。

[図4]図４は、結果文字列更新処理について説明する図である。

[図5]図５は、通常のＬＣＳを用いた場合について説明する図である。

[図6]図６は、区切り文字入りＬＣＳを用いた場合について説明する図である。

[図7]図７は、第一の実施の形態に係る攻撃パターン抽出装置におけるクラスタリング処理の流れを示すフローチャートである。

[図8]図８は、第一の実施の形態に係る攻撃パターン抽出装置におけるＬＣＳ算出処理の流れを示すフローチャートである。

[図9]図９は、攻撃パターン抽出プログラムを実行するコンピュータを示す図である。

発明を実施するための形態

[0011] 以下に、本願に係る攻撃パターン抽出装置、攻撃パターン抽出方法および攻撃パターン抽出プログラムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態により本願に係る攻撃パターン抽出装置、攻撃パターン抽出方法および攻撃パターン抽出プログラムが限定されるものではない。

[0012] ［第一の実施の形態］

以下の実施の形態では、第一の実施の形態に係る攻撃パターン抽出装置１０の構成、攻撃パターン抽出装置１０の処理の流れを順に説明し、最後に第一の実施の形態による効果を説明する。

[0013] ［攻撃パターン抽出装置の構成］

まず、図１を用いて、攻撃パターン抽出装置１０の構成を説明する。図１は、第一の実施の形態に係る攻撃パターン抽出装置の概要を示す構成図である。図１に示すように、この攻撃パターン抽出装置１０は、入力部１１、出力部１２、制御部１３および記憶部１４を有する。

[0014] 入力部１１は、各種情報の入力操作を受け付けるデバイスであり、例えば、攻撃と判定されたＷｅｂサーバへのアクセスログの入力を受け付ける。出力部１２は、各種情報を出力するデバイスであり、例えば、攻撃パターンを出力する。

[0015] また、記憶部１４は、制御部１３による各種処理に必要なデータおよびプログラムを格納するが、特に本発明に密接に関連するものとしては、ログ記憶部１４ａを有する。例えば、記憶部１４は、ＲＡＭ（Random Access Memory）、フラッシュメモリ（Flash Memory）等の半導体メモリ素子、又は、ハードディスク、光ディスク等の記憶装置などである。

[0016] ログ記憶部１４ａは、攻撃と判定されたＷｅｂサーバへのアクセスログを記憶する。アクセスログは、例えば、データ項目として、「発ＩＰ」、「日時」、「リクエスト」を含むものとする。あるいはアクセスログから、リクエストに含まれるパラメータのみを抽出してデータ項目としても良い。

[0017] 制御部１３は、各種の処理手順などを規定したプログラムおよび所要データを格納するための内部メモリを有し、これらによって種々の処理を実行するが、特に本発明に密接に関連するものとしては、抽出部１３ａおよび攻撃パターン生成部１３ｂを有する。ここで、制御部１３は、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路やＡＳＩＣ（Application Specific Integrated Circuit）やＦＰＧＡ（Field Programmable Gate Array）などの集積回路である。

[0018] 抽出部１３ａは、攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する。抽出部１３ａは、パラメータ同士で共通する文字列であって、且つ、連続しない文字列間を区切る区切り文字を入れたまま最長共通部分列を算出し、該最長共通部分列を用いて、共通した文字列を抽出する。

[0019] 抽出部１３ａは、攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出するために、以下のクラスタリング処理を行う。以下に、クラスタリング処理について詳しく説明するが、以降の説明で

は、文字列Ｘの長さを「ｌｅｎ（Ｘ）」と表記し、文字列Ｘのｉ番目の文字（１から数える）を「Ｘ［ｉ］」と表記する。また、複数のパラメータをp_1，p_2，・・・，p_nと表記する。最初に、抽出部１３ａは、複数のパラメータp_1，p_2，・・・，p_nをクラスタリングする。

[0020] まず、抽出部１３ａは、クラスタ集合Ｃを初期化する。クラスタ集合Ｃ（Ｃ＝｛C_1，C_2，．．．，C_n｝）に含まれるクラスタC_i（１≦ｉ≦ｎ）を、｛ｌｃｓ:パラメータp_i自身、ｓｔｒｉｎｇｓ：p_iのみからなる配列｝からなる連想配列（C_i＝｛ｌｃｓ：p_i，ｓｔｒｉｎｇｓ：［p_i］｝（１≦ｉ≦ｎ））とする。また、抽出部１３ａは、結果リストＲも空の配列で初期化する。

[0021] 続いて、抽出部１３ａは、処理対象クラスタ抽出処理を行う。具体的には、抽出部１３ａは、クラスタ集合Ｃから処理対象クラスタ（例えば最後の要素）を１つ抽出し、C_tとする。クラスタ集合ＣをＣ＼｛C_t｝で更新する。ここで“＼”は差集合を表す。すなわち、クラスタ集合Ｃから要素C_tを取り除いたものでＣを更新する。

[0022] そして、抽出部１３ａは、処理対象クラスタと他クラスタのＬＣＳ算出を行う。具体的には、抽出部１３ａは、クラスタ集合Ｃの各要素C_i（１≦ｉ≦｜Ｃ｜）のｌｃｓ要素と、C_tのｌｃｓ要素とのＬＣＳ（最長共通部分列）を順次算出する。ＬＣＳの算出は、後述の手順で行い、連続しない部分は区切り文字（例：“|”）で区切られた結果が得られる。具体的を挙げて説明すると、抽出部１３ａは、要素C_iのｌｃｓ要素“ａｂＣＤｅＦＧｈ”とC_tのｌｃｓ要素“ｘｙＣｚＤＦＧ”とのＬＣＳの算出結果として、“Ｃ｜Ｄ｜ＦＧ”が得られる。

[0023] そして、抽出部１３ａは、処理対象クラスタとクラスタ集合Ｃの各クラスタとのＬＣＳ算出を行うと、ＬＣＳを区切り文字で分割した文字列の長さのうち、最長のものをC_iとC_tのスコアｓ（C_i，C_t）とする。

[0024] つまり、スコアｓ（C_i，C_t）は、クラスタC_i，C_tのｌｃｓ要素同士の区切り文字入りＬＣＳを算出し、それを区切り文字で分割した文字列の長さの

うち、最長のものである。例えば、クラスタC_i「C_i＝｛ｌｃｓ：“ＡＢ｜ＣＤ”，ｓｔｒｉｎｇｓ：［“ＡＢ１２ＣＤ”，“ＡＢＣＤ”］｝」とクラスタC_t「C_t＝｛ｌｃｓ：“ＡＢ｜Ｃ｜Ｅ”，ｓｔｒｉｎｇｓ：［“ＡＢｘＣＥ”，“ＡＢｙＣｄＥ”］｝」とでは、“ＡＢ｜ＣＤ”と“ＡＢ｜Ｃ｜Ｅ”の区切り文字入りＬＣＳとして、“ＡＢ｜Ｃ”が得られる。そして、“ＡＢ｜Ｃ”を区切り文字で分割し、“ＡＢ”，“Ｃ”の文字列長（２、１）のうち最長の“２”がスコアｓ（C_i，C_t）となる。スコアｓ（C_i，C_t）が最大となるC_i（$1 \leqq i \leqq |C|$）をC_kとする。なお、スコアｓ（C_i，C_t）が最大となるC_iが複数ある場合には、スコアｓ（C_i，C_t）が最大となる複数のC_iのうち任意の一つをC_kとする。

[0025] 続いて、抽出部１３ａは、最大スコア確認処理を行う。具体的には、抽出部１３ａは、C_kとC_tのスコアｓ（C_k，C_t）（最大スコア）が最小文字列長閾値以上かを確認する。抽出部１３ａは、確認の結果、閾値未満の場合には、処理対象クラスタC_tを結果リストＲに追加し、処理対象クラスタ抽出処理に戻って、新しい処理対象クラスタを抽出して上記の処理を繰り返す。一方、抽出部１３ａは、確認の結果、閾値以上の場合には、C_kとC_tを以下の通りマージしてC_Nを作成する。C_Nのｌｃｓ：C_kのｌｃｓとC_tのｌｃｓの区切り文字入りＬＣＳ、C_Nのｓｔｒｉｎｇｓ：C_kのｓｔｒｉｎｇｓとC_tのｓｔｒｉｎｇｓを配列として連結する。その後、抽出部１３ａは、Ｃを（Ｃ＼｛C_k｝）∪｛C_N｝で更新し、処理対象クラスタ抽出処理に戻って、新しい処理クラスタを抽出して上記の処理を繰り返す。

[0026] そして、抽出部１３ａは、クラスタ集合Ｃのサイズが１になるまで、前述した処理対象クラスタ抽出処理、ＬＣＳ算出処理および最大スコア確認処理を繰り返す。その後、抽出部１３ａは、クラスタ集合のサイズが１になった場合には、最後のクラスタを結果リストＲに追加する。そして、抽出部１３ａは、結果リストＲを攻撃パターン生成部１３ｂに通知する。

[0027] ここで、上述したＬＣＳ算出処理について詳しく説明する。抽出部１３ａは、ＬＣＳ算出処理において、２つの文字列ｘ，ｙが与えられた時、これら

の最長共通部分列（ＬＣＳ）を算出する。抽出部１３ａは、算出の際、連続しない部分は区切り文字（例えば、“|”）で区切る。なお、区切り文字はｘ，ｙに現れない文字であれば何でもよい。以降の説明では、ｘ＝“ａＢＣｄ”，ｙ＝“ＢｅＣ”を例として説明する。

[0028] まず、抽出部１３ａは、ＬＣＳ算出対象の２つの文字列ｘ，ｙを入力として受け取る。そして、抽出部１３ａは、テーブル初期化処理を行う。例えば、抽出部１３ａは、図２に例示するように、（ｌｅｎ（ｙ）＋１）×（ｌｅｎ（ｘ）＋１）の配列ｔを用意し、０行目、０列目の全ての要素を０で初期化する。図２は、テーブル初期化処理について説明する図である。

[0029] そして、抽出部１３ａは、テーブル更新処理を行う。具体的には、抽出部１３ａは、ｉ＝１，２，・・・，ｌｅｎ（ｙ）、ｊ＝１，２，・・・，ｌｅｎ（ｘ）とし、以下の（１）、（２）の規則に従って、テーブルを更新する。（１）ｘ［ｊ］＝ｙ［ｉ］の場合には、ｔ［ｉ］［ｊ］＝ｔ［ｉ－１］［ｊ－１］＋１と更新し、（２）ｘ［ｊ］＝ｙ［ｉ］以外の場合には、ｔ［ｉ］［ｊ］＝ｍａｘ（ｔ［ｉ－１］［ｊ］，ｔ［ｉ］［ｊ－１］）と更新する。

[0030] ここで、図３の例を用いて、テーブル更新処理を説明する。図３は、テーブル更新処理について説明する図である。図３の例を挙げて説明すると、例えば、抽出部１３ａは、３列目（ｘ［３］）の文字「Ｃ」と、３行目（ｙ［３］）の文字「Ｃ」とが同じである場合には、２行２列目の要素「ｔ［２，２］＝１」に１を加算した値「２」を、３行目３列目の要素ｔ［３，３］として更新する。また、抽出部１３ａは、４列目（ｘ［４］）の文字「ｄ」と、３行目（ｙ［３］）の文字「Ｃ」とが異なる場合には、３行３列目の要素「ｔ［３，３］＝２」と、２行４列目の要素「ｔ［２，４］＝１」とのうち、最大の「２」を、３行４列目の要素ｔ［３，４］として更新する。

[0031] そして、抽出部１３ａは、結果文字列を空文字列“”で初期化する。続いて、抽出部１３ａは、ｉ＞０かつｊ＞０の間、以下の（１）、（２）を繰り返し、結果文字列を更新する。（１）ｘ［ｊ］＝ｙ［ｉ］の場合には、結果

文字列にｘ［ｊ］を追記し、ｉ，ｊをともに１減ずる。（２）ｘ［ｊ］＝ｙ［ｉ］以外の場合には、ｔ［ｉ－１］［ｊ］＞ｔ［ｉ］［ｊ－１］ならばｉを１減じ、そうでないならばｊを１減ずる。結果文字列の末尾が区切り文字でなければ区切り文字を追記、末尾が区切り文字ならば何もしない。

[0032] ここで、図４の例を用いて、結果文字列更新処理について説明する。図４は、結果文字列更新処理について説明する図である。図４の例を挙げて説明すると、例えば、抽出部１３ａは、４列目（ｘ［４］）の文字「ｄ」と、３行目（ｙ［３］）の文字「Ｃ」とが異なる場合には、２行４列目の要素「ｔ［２，４］＝１」と３行３列目の要素「ｔ［３，３］＝２」とを比較し、３行３列目の要素「ｔ［３，３］＝２」が大きい場合には、ｊを１減ずる。なお、結果文字列の末尾が区切り文字ではないので、結果文字列を“”から“｜”に更新する。

[0033] 続いて、抽出部１３ａは、３列目（ｘ［３］）の文字「Ｃ」と、３行目（ｙ［３］）の文字「Ｃ」とが同じである場合には、結果文字列を“｜”から“｜Ｃ”に更新し、ｉ，ｊをともに１減ずる。そして、抽出部１３ａは、２列目（ｘ［２］）の文字「Ｂ」と、２行目（ｙ［２］）の文字「ｅ」とが異なる場合には、１行２列目の要素「ｔ［１，２］＝１」と２行１列目の要素「ｔ［２，１］＝０」とを比較し、１行２列目の要素「ｔ［１，２］＝１」が大きい場合には、ｉを１減ずる。また、結果文字列の末尾が区切り文字ではないので、結果文字列を“｜Ｃ”から“｜Ｃ｜”に更新する。

[0034] そして、抽出部１３ａは、２列目（ｘ［２］）の文字「Ｂ」と、１行目（ｙ［１］）の文字「Ｂ」とが同じである場合には、結果文字列を“｜Ｃ｜”から“｜Ｃ｜Ｂ”に更新し、ｉ，ｊをともに１減ずる。

[0035] その後、抽出部１３ａは、結果文字列を反転する。例えば、抽出部１３ａは、結果文字列が“｜Ｃ｜Ｂ”である場合には、結果文字列を“Ｂ｜Ｃ｜”に反転させる。

[0036] 図１の説明に戻って、攻撃パターン生成部１３ｂは、抽出部１３ａによって抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字

列を基に攻撃パターンを生成する。また、攻撃パターン生成部１３ｂは、文字列長が所定の文字列長以上の文字列が複数ある場合には、複数の文字列と各文字列の出現順序とを基に攻撃パターンを生成する。また、攻撃パターン生成部１３ｂは、抽出部１３ａによって抽出された連続する文字列が既に生成された攻撃パターンに含まれる場合には、何もしない。

[0037] 具体的には、攻撃パターン生成部１３ｂは、結果リストＲ＝［Ｃ’$_1$，Ｃ’$_2$，・・・，Ｃ’$_m$］の各要素について、ｓｔｒｉｎｇｓ要素の個数が最小クラスタサイズ閾値以上であるものを抽出する。抽出した要素のＩｃｓ要素が、抽出したい共通部分である。攻撃パターン生成部１３ｂは、共通部分を区切り文字で分割し、最小文字列長閾値以上の長さの文字列を“＊”で連結した正規表現が、最終的に求める攻撃パターンとなる。なお、閾値として最小文字列長閾値とは別の新しい閾値を採用してもよい。

[0038] 具体例を挙げて説明すると、攻撃パターン生成部１３ｂは、例えば、Ｉｃｓ：“ａ｜ＢＣＤ｜ｅｆ｜ｇ｜ＨＩＪＫ”を区切り文字で分割して、“ａ”，“ＢＣＤ”，“ｅｆ”，“ｇ”，“ＨＩＪＫ”とし、閾値（例えば、「３」）以上の長さの文字列を出現順に“＊”で連結して攻撃パターンとして“ＢＣＤ＊ＨＩＪＫ”を生成する。また、“ＢＣＤ＊ＨＩＪＫ”が攻撃パターンとして既に生成されている場合には、何もしない。

[0039] このように、攻撃パターン抽出装置１０は、ＬＣＳを算出する際、文字が連続しない箇所に区切り文字を入れながら算出し、閾値以上の長さのものを抽出するため、極端に短い共通部分を攻撃パターンとして抽出することがない。

[0040] また、攻撃パターン抽出装置１０は、クラスタをマージする際、区切り文字を入れたままでＬＣＳを算出するため、「共通部が連続している」という情報を失うことなく、３つ以上のパラメータから共通部を効率よく抽出することができる。

[0041] ここで、図５および図６の例を用いて、区切り文字列のない通常のＬＣＳを用いた場合と比較することで、区切り文字列入りＬＣＳを用いた場合の効

果について説明する。図５は、通常のＬＣＳを用いた場合について説明する図である。図６は、区切り文字入りＬＣＳを用いた場合について説明する図である。図５および図６では、ＡＢ１２ＣＤ，ＡＢＣＤ，ＡＢｘＣＥ，ＡＢｙＣｄＥから、連続する最長の共通部分列を抽出する場合を例示している。

[0042] 図５に示すように、区切り文字列のない通常のＬＣＳを用いた場合には、４つの文字列のＬＣＳを算出後、元の文字列全てと比較し直さないと、連続する最長の共通部分列“ＡＢ”が分からない。これに対して、図６に示すように、区切り文字入りＬＣＳを用いた場合には、４つの文字列のＬＣＳを算出した時点で、もとの文字列でどこが連続していたかが分かるため、すぐに連続する最長の共通部分列“ＡＢ”が得られる。このため、区切り文字入りＬＣＳを用いた場合には、共通部分列を効率よく抽出することができる。

[0043] ［攻撃パターン抽出装置の処理の一例］

次に、図７および図８を用いて、攻撃パターン抽出装置１０における処理の流れを説明する。図７は、第一の実施の形態に係る攻撃パターン抽出装置におけるクラスタリング処理の流れを示すフローチャートである。図８は、第一の実施の形態に係る攻撃パターン抽出装置におけるＬＣＳ算出処理の流れを示すフローチャートである。

[0044] まず、図７を用いて、攻撃パターン抽出装置１０におけるクラスタリング処理の流れを説明する。図７に示すように、攻撃パターン抽出装置１０の抽出部１３ａは、クラスタ集合Ｃを初期化する（ステップＳ１０１）。そして、抽出部１３ａは、クラスタ集合Ｃのサイズが２以上であるか否かを判定する（ステップＳ１０２）。

[0045] この結果、抽出部１３ａは、クラスタ集合のサイズが２以上であると判定した場合には（ステップＳ１０２肯定）、処理対象クラスタ抽出処理を行う（ステップＳ１０３）。具体的には、抽出部１３ａは、クラスタ集合Ｃから処理対象クラスタ（例えば最後の要素）を１つ抽出し、C_tとする。クラスタ集合Ｃを$C \setminus \{C_t\}$で更新する。ここで“＼”は差集合を表す。すなわち、クラスタ集合Ｃから要素C_tを取り除いたものでＣを更新する。

[0046] そして、抽出部１３ａは、処理対象クラスタと他クラスタのＬＣＳ算出を行う（ステップＳ１０４）。具体的には、抽出部１３ａは、クラスタ集合Ｃの各要素C_i（$1 \leqq i \leqq |C|$）のｌｃｓ要素と、C_tのｌｃｓ要素とのＬＣＳ（最長共通部分列）を順次算出する。C_tとのＬＣＳの一致部分文字列長が最長となるC_iをC_kとする。

[0047] そして、抽出部１３ａは、最長一致部分文字列長が最小文字列長閾値以上かを判定する（ステップＳ１０５）。この結果、抽出部１３ａは、最長一致部分文字列長が最小文字列長閾値以上であると判定した場合には（ステップＳ１０５肯定）、クラスタのマージを行って（ステップＳ１０６）、ステップＳ１０２の処理に戻る。具体的には、抽出部１３ａは、C_kとC_tを以下の通りマージしてC_Nを作成する。C_Nのｌｃｓ：C_kのｌｃｓとC_tのｌｃｓの区切り文字入りＬＣＳ、C_Nのｓｔｒｉｎｇｓ：C_kのｓｔｒｉｎｇｓとC_tのｓｔｒｉｎｇｓを配列として連結する。

[0048] また、抽出部１３ａは、最長一致部分文字列長が最小文字列長閾値未満であると判定した場合には（ステップＳ１０５否定）、処理対象クラスタC_tを結果リストＲに追加し（ステップＳ１０７）、ステップＳ１０２の処理に戻る。

[0049] また、ステップＳ１０２において、抽出部１３ａは、クラスタ集合のサイズが１であると判定した場合には（ステップＳ１０２否定）、最後のクラスタを結果リストに追加する（ステップＳ１０８）。そして、攻撃パターン生成部１３ｂは、クラスタサイズが閾値以上のものを抽出する（ステップＳ１０９）。具体的には、攻撃パターン生成部１３ｂは、結果リストＲ＝［C'_1，C'_2，・・・，C'_m］の各要素について、ｓｔｒｉｎｇｓ要素の個数が最小クラスタサイズ閾値以上であるものを抽出する。抽出した要素のｌｃｓ要素が、抽出したい共通部分である。攻撃パターン生成部１３ｂは、共通部分を区切り文字で分割し、最小文字列長閾値以上の長さの文字列を“＊”で連結した正規表現が、最終的に求める攻撃パターンとなる。

[0050] 次に、図８を用いて、攻撃パターン抽出装置１０におけるＬＣＳ算出処理

の流れを説明する。図８に例示するように、抽出部１３ａは、ＬＣＳ算出対象の２つの文字列ｘ，ｙを入力として受け取る（ステップＳ２０１）。そして、抽出部１３ａは、テーブル初期化処理を行う（ステップＳ２０２）。例えば、抽出部１３ａは、（ｌｅｎ（ｙ）＋１）×（ｌｅｎ（ｘ）＋１）のテーブル（配列）ｔを用意し、０行目、０列目の全ての要素を０で初期化する。

[0051] そして、抽出部１３ａは、ｉ＝１，２，・・・，ｌｅｎ（ｙ）、ｊ＝１，２，・・・，ｌｅｎ（ｘ）として、ステップＳ２０３～ステップＳ２０９のテーブルを更新する処理を繰り返す。ステップＳ２０５において、抽出部１３ａは、ｘ［ｊ］＝ｙ［ｉ］であるか判定し（ステップＳ２０５）、ｘ［ｊ］＝ｙ［ｉ］の場合には（ステップＳ２０５肯定）、ｔ［ｉ］［ｊ］＝ｔ［ｉ－１］［ｊ－１］＋１と更新し（ステップＳ２０７）、ｘ［ｊ］＝ｙ［ｉ］以外の場合には（ステップＳ２０５否定）、ｔ［ｉ］［ｊ］＝ｍａｘ（ｔ［ｉ－１］［ｊ］，ｔ［ｉ］［ｊ－１］）と更新する（ステップＳ２０６）。

[0052] 続いて、抽出部１３ａは、結果文字列を空文字列“”で初期化する（ステップＳ２１０）。そして、抽出部１３ａは、ｉ＞０かつｊ＞０の間、ステップＳ２１１～Ｓ２１９の処理を繰り返す。ステップＳ２１２において、抽出部１３ａは、ｘ［ｊ］＝ｙ［ｉ］であるか否かを判定する（ステップＳ２１２）。この結果、抽出部１３ａは、ｘ［ｊ］＝ｙ［ｉ］の場合には（ステップＳ２１２肯定）、結果文字列にｘ［ｊ］を追記し（ステップＳ２１７）、ｉ，ｊをともに１減ずる（ステップＳ２１８）。

[0053] また、抽出部１３ａは、ｘ［ｊ］＝ｙ［ｉ］以外の場合には（ステップＳ２１２否定）、ｔ［ｉ－１］［ｊ］＞ｔ［ｉ］［ｊ－１］であるか判定する（ステップＳ２１３）。この結果、抽出部１３ａは、ｔ［ｉ－１］［ｊ］＞ｔ［ｉ］［ｊ－１］である場合には（ステップＳ２１３肯定）、ｉを１減じ（ステップＳ２１４）ｔ［ｉ－１］［ｊ］＞ｔ［ｉ］［ｊ－１］でない場合には（ステップＳ２１３否定）、ｊを１減ずる（ステップＳ２１５）。そして、抽出部１３ａは、結果文字列の末尾が区切り文字でなければ区切り文字

を追記する（ステップＳ２１６）。

[0054] その後、抽出部１３ａは、結果文字列を反転する（ステップＳ２２０）。例えば、抽出部１３ａは、結果文字列が“｜Ｃ｜Ｂ”である場合には、結果文字列を“Ｂ｜Ｃ｜”に反転させる。

[0055] ［第一の実施の形態の効果］

このように、第一の実施の形態に係る攻撃パターン抽出装置１０は、攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する。そして、攻撃パターン抽出装置１０は、抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する。このため、第一の実施の形態に係る攻撃パターン抽出装置１０は、適切な攻撃パターンを生成することが可能である。

[0056] また、攻撃パターン抽出装置１０は、ＬＣＳを算出する際、文字が連続しない箇所に区切り文字を入れながら算出し、閾値以上の長さのものを抽出するため、極端に短い共通部分を攻撃パターンとして抽出せずに、適切な攻撃パターンを生成することが可能である。

[0057] また、攻撃パターン抽出装置１０は、クラスタをマージする際、区切り文字を入れたままでＬＣＳを算出するため、「共通部が連続している」という情報を失うことなく、３つ以上のパラメータから共通部を効率よく抽出することが可能である。

[0058] ［第二の実施の形態］

上述した第一の実施の形態では、C_kとC_tのスコアｓ（C_k, C_t）（最大スコア）が最小文字列長閾値以上である場合に、クラスタをマージすることを説明したが、クラスタをマージする際、共通部の長さが極端に短くなる（スコアが大きく下がる）場合は、マージを抑制することで、攻撃パターンとして残すべき文字列長の長い共通部分が失われることを防ぐようにしてもよい。

[0059] そこで、以下の第二の実施の形態では、クラスタをマージする際、共通部の長さが極端に短くなる（スコアが大きく下がる）場合は、マージを抑制す

る場合について説明する。なお、第一の実施の形態と同様の構成や処理については説明を省略する。

[0060] 第二の実施の形態に係る攻撃パターン抽出装置の抽出部１３ａは、共通した文字列の長さが、所定の比率以下に低下する場合は、当該文字列からの共通した文字列の抽出を抑制する。具体的には、抽出部１３ａは、最大スコア確認処理において、C_kとC_tのスコアｓ（C_k,C_t）（最大スコア）が最小文字列長閾値以上の場合、マージする前に、C_tのｓｔｒｉｎｇｓの要素数が最小クラスタサイズ閾値以上であり、かつマージ後のスコア低下率がスコア低下率閾値以上となる場合、マージは行わず、C_tを結果リストＲに追加し、処理対象クラスタ抽出処理に戻る。ここで、スコア低下率はC_tのｌｃｓ要素を区切り文字で分割した文字列の最長文字列長Ｌとスコアｓ（C_k,C_t）を比較して算出する。例えば、１－ｓ（C_k,C_t）／Ｌをスコア低下率とする。

[0061] このため、第二の実施の形態では、既に十分な量のパラメータから十分に長い共通部が得られている場合に、さらにマージを行うことで得られる共通部が短くなってしまうことを防ぐことができる。

[0062] 例えば、第一の実施の形態では、｛ｌｃｓ：“ＰＡＴＴＥＲＮ”，ｓｔｒｉｎｇｓ：［“ＰＡＴＴＥＲＮ１”，“ＰＡＴＴＥＲＮ２”，“ＰＡＴＴＥＲＮ３”］｝というクラスタが得られている場合に、“ＴＥＲＮ”というパラメータからなるクラスタもマージされて、｛ｌｃｓ：“ＴＥＲＮ”，ｓｔｒｉｎｇｓ：［“ＰＡＴＴＥＲＮ１”，“ＰＡＴＴＥＲＮ２”，“ＰＡＴＴＥＲＮ３”，“ＴＥＲＮ”］｝というクラスタが生成されてしまう。ここで、最小文字列長閾値は「４」とする。

[0063] 攻撃パターンとしては、できるだけ長い共通部分を抽出したいので、この場合はマージせずに“ＰＡＴＴＥＲＮ”という共通部が得られた時点で、マージを終了してクラスタを確定させたほうが良い。これに対して、第二の実施の形態では、“ＰＡＴＴＥＲＮ”が“ＴＥＲＮ”になるとスコアが大きく低下するので、マージを抑制して、所望の共通部を得ることができる。

[0064] ［第二の実施の形態の効果］

このように、第二の実施の形態では、クラスタをマージする際、共通部の長さが極端に短くなる場合は、マージを抑制することで、攻撃パターンとして残すべき文字列長の長い共通部分が失われることを防ぐことが可能である。

[0065] ［システム構成等］

また、図示した各装置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如く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、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析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。例えば、抽出部１３ａと攻撃パターン生成部１３ｂとを統合してもよい。

[0066] また、本実施の形態において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。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。

[0067] ［プログラム］

また、上記実施形態において説明した攻撃パターン抽出装置が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。例えば、実施形態に係る攻撃パターン抽出装置１０が実行する処理をコンピュータが実行可能な言語で記述した攻撃パターン抽出プログラムを作成することもできる。この場合、コンピュータが攻撃パターン抽出プログラムを実行することにより、上記実施形態と同様の効果を得ることができる

。さらに、かかる攻撃パターン抽出プログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録された攻撃パターン抽出プログラムをコンピュータに読み込ませて実行することにより上記実施形態と同様の処理を実現してもよい。

[0068] 図９は、攻撃パターン抽出プログラムを実行するコンピュータ１０００を示す図である。図９に例示するように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有し、これらの各部はバス１０８０によって接続される。

[0069] メモリ１０１０は、図９に例示するように、ＲＯＭ（Read Only Memory）１０１１及びＲＡＭ１０１２を含む。ＲＯＭ１０１１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、図９に例示するように、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、図９に例示するように、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、図９に例示するように、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、図９に例示するように、例えばディスプレイ１１３０に接続される。

[0070] ここで、図９に例示するように、ハードディスクドライブ１０９０は、例えば、ＯＳ１０９１、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、上記の攻撃パターン抽出プログラムは、コンピュータ１０００によって実行される指令が記述されたプログラムモジュールとして、例えばハードディスクドライブ１０９０に記憶される。

[0071] また、上記実施形態で説明した各種データは、プログラムデータとして、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、ＣＰＵ１０２０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ＲＡＭ１０１２に読み出し、各種処理手順を実行する。

[0072] なお、攻撃パターン抽出プログラムに係る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れず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、攻撃パターン抽出プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ネットワーク（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された他のコンピュータに記憶され、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

[0073] １０ 攻撃パターン抽出装置

１１ 入力部

１２ 出力部

１３ 制御部

１３ａ 抽出部

１３ｂ 攻撃パターン生成部

１４ 記憶部

１４ａ ログ記憶部

請求の範囲

[請求項1] 攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する抽出部と、

前記抽出部によって抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する攻撃パターン生成部と

を備えたことを特徴とする攻撃パターン抽出装置。

[請求項2] 前記攻撃パターン生成部は、文字列長が所定の文字列長以上の文字列が複数ある場合には、複数の文字列と各文字列の出現順序とを基に攻撃パターンを生成することを特徴とする請求項１に記載の攻撃パターン抽出装置。

[請求項3] 前記抽出部は、パラメータ同士で共通する文字列であって、且つ、連続しない文字列間を区切る区切り文字を入れたまま最長共通部分列を算出し、該最長共通部分列を用いて、共通した文字列を抽出することを特徴とする請求項１に記載の攻撃パターン抽出装置。

[請求項4] 前記攻撃パターン生成部は、前記抽出部によって抽出された連続する文字列が既に生成された攻撃パターンに含まれる場合には、抽出された連続する文字列を攻撃パターンから削除することを特徴とする請求項１に記載の攻撃パターン抽出装置。

[請求項5] 前記抽出部は、共通した文字列の長さが、所定の比率以下に低下する場合は、当該文字列からの共通した文字列の抽出を抑制することを特徴とする請求項１に記載の攻撃パターン抽出装置。

[請求項6] 攻撃パターン抽出装置で実行される攻撃パターン抽出方法であって、

攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する抽出工程と、

前記抽出工程によって抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する攻撃パ

ターン生成工程と

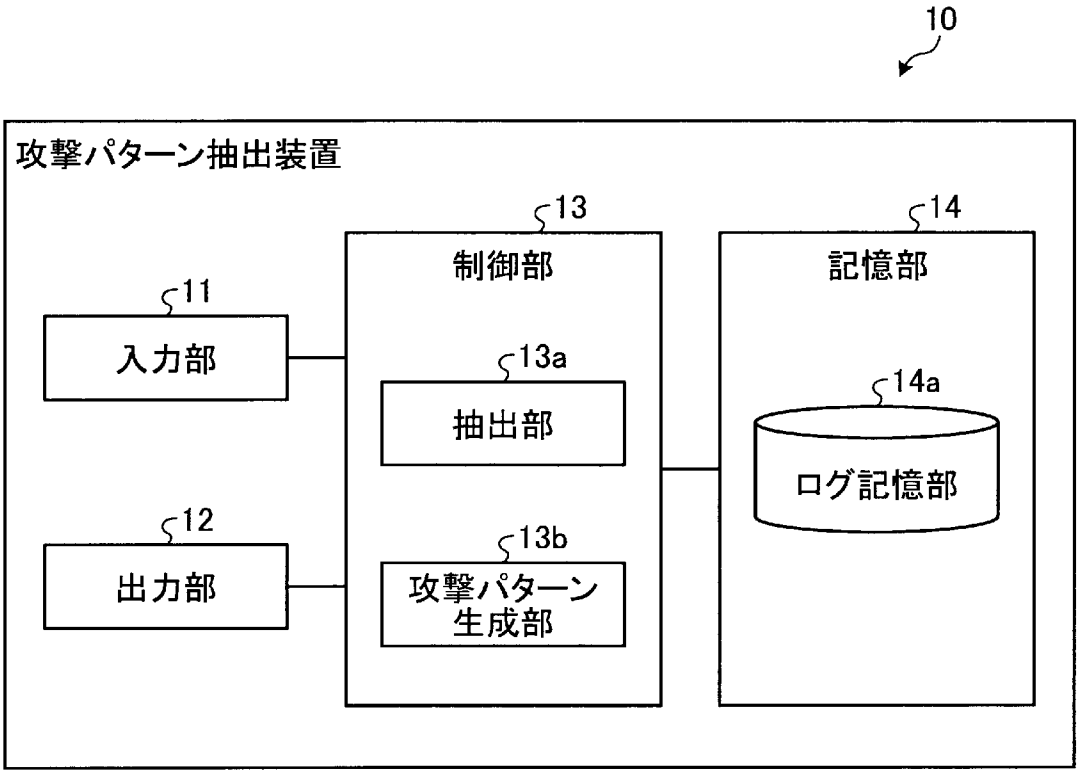
を含んだことを特徴とする攻撃パターン抽出方法。

[請求項7] 攻撃と判定された通信のアクセスログにおけるパラメータ同士の共通した文字列を抽出する抽出ステップと、

前記抽出ステップによって抽出された連続する文字列のうち、文字列長が所定の文字列長以上の文字列を基に攻撃パターンを生成する攻撃パターン生成ステップと

をコンピュータに実行させるための攻撃パターン抽出プログラム。

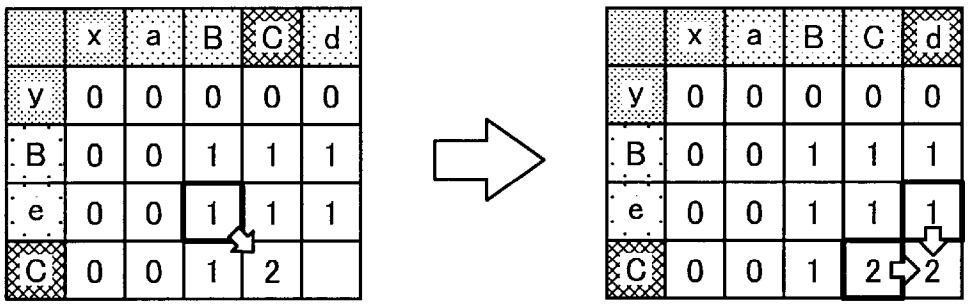
[図1]



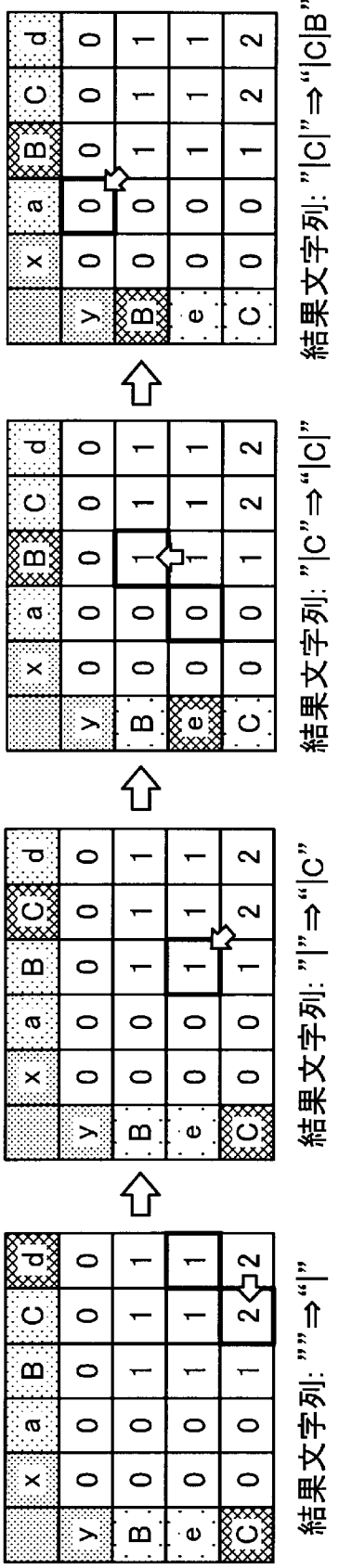
[図2]

	x	a	B	C	d
y	0	0	0	0	0
B	0				
e	0				
C	0				

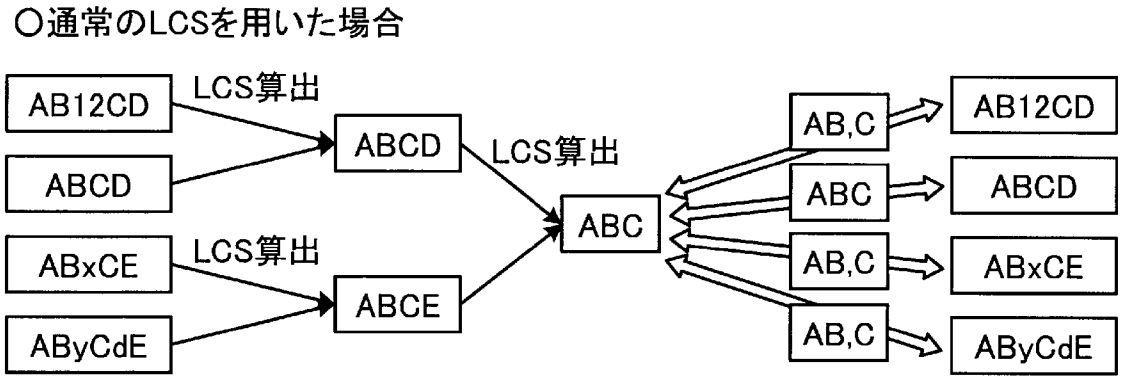
[図3]


x a B C d
y 0 0 0 0 0
B 0 0 1 1 1
e 0 0 1 1 1
C 0 0 1 2
x a B C d
y 0 0 0 0 0
B 0 0 1 1 1
e 0 0 1 1 1
C 0 0 1 2 2

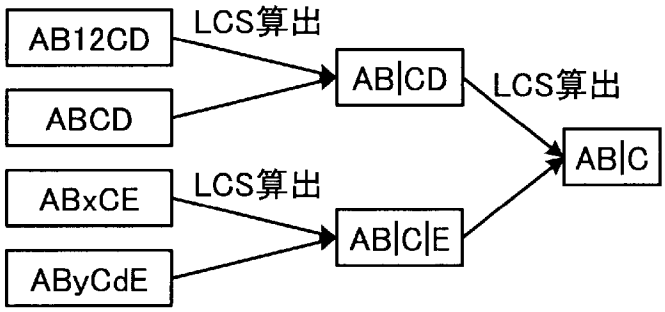
[図4]



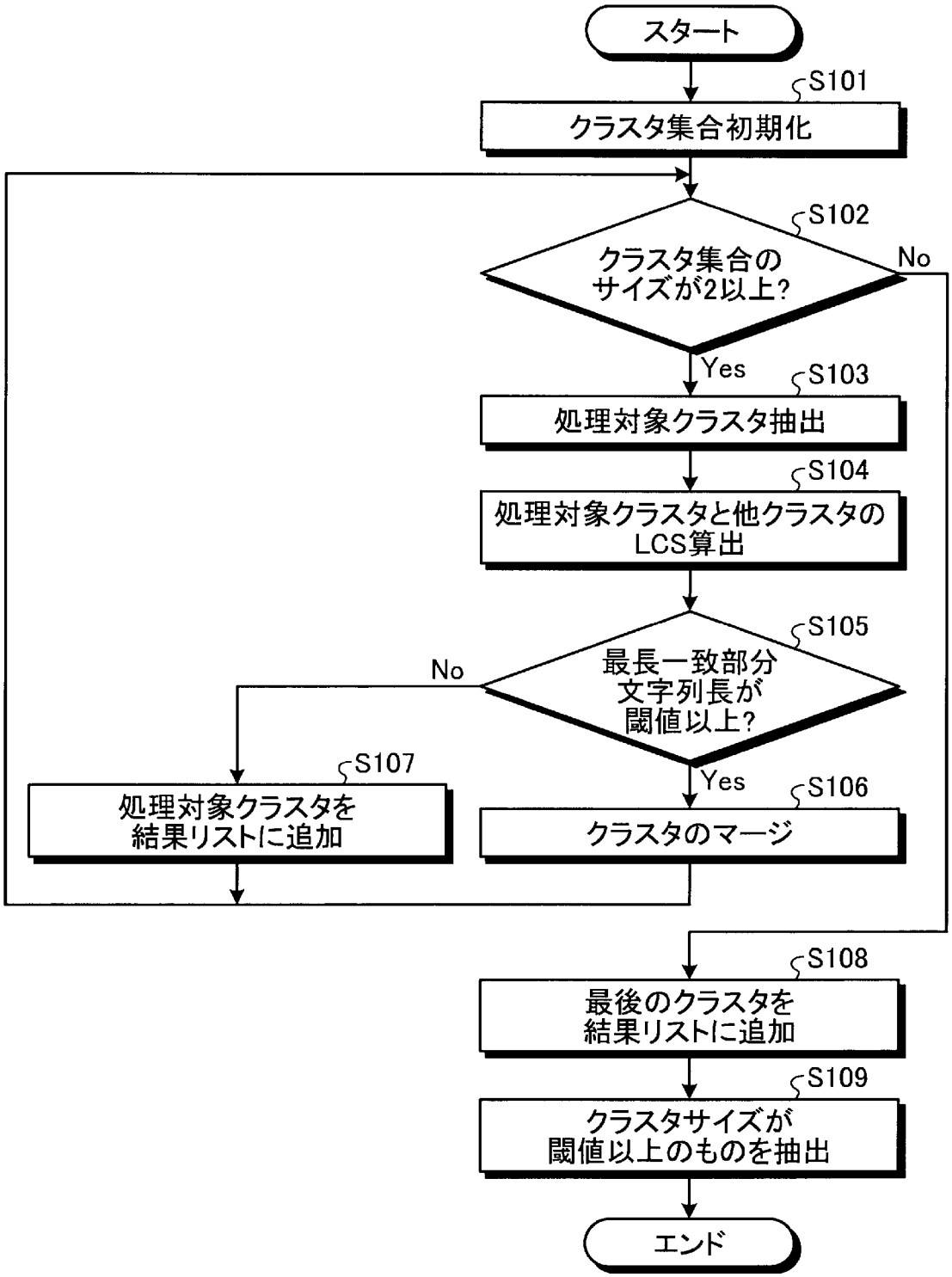
[図5]


○通常のLCSを用いた場合
AB12CD
ABCD
ABxCE
AByCdE
LCS算出
LCS算出
ABCD
ABCE
LCS算出
ABC
AB,C
ABC
AB,C
AB,C
AB12CD
ABCD
ABxCE
AByCdE

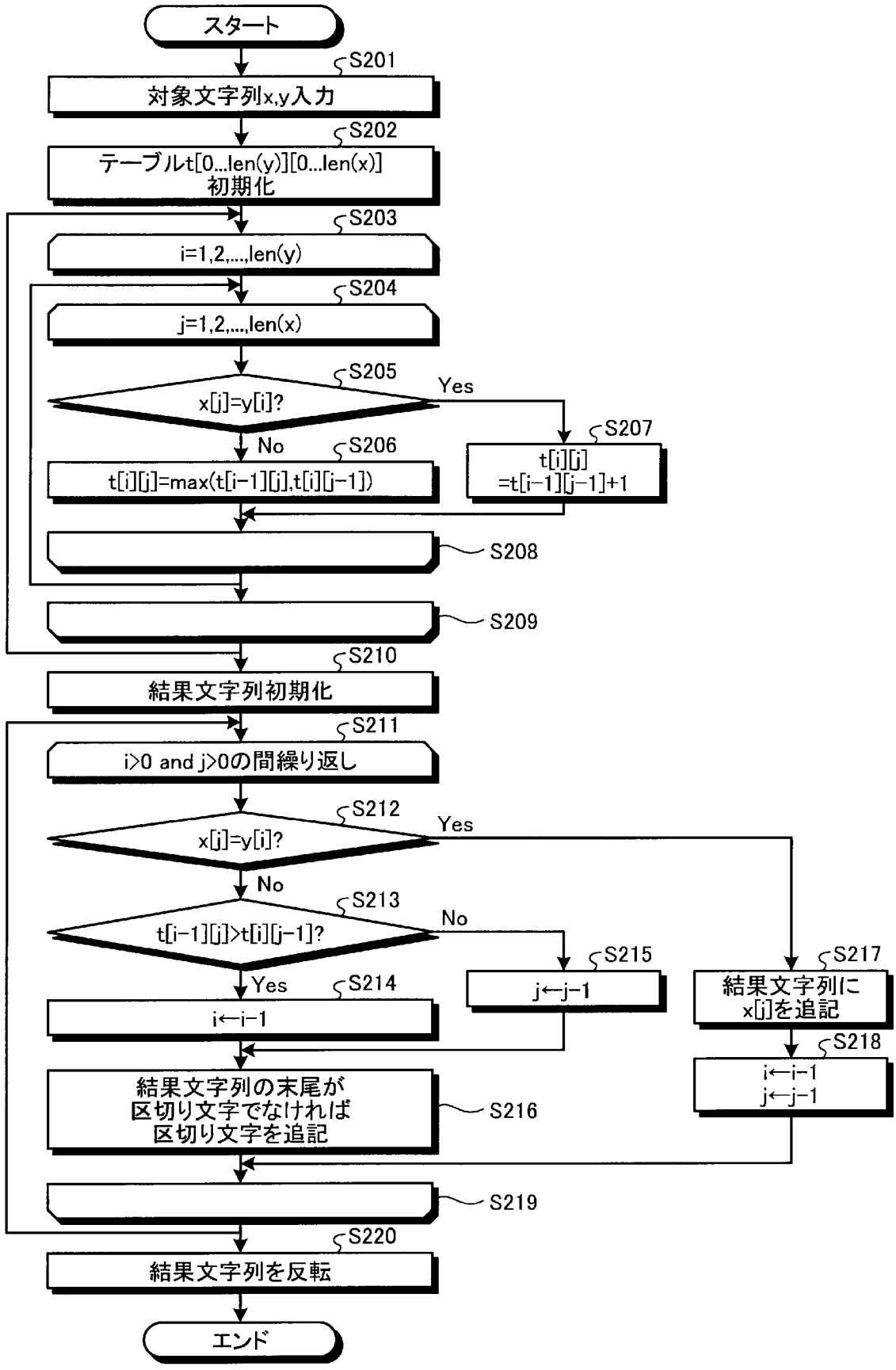
[図6]


○区切り文字入りLCSを用いた場合
AB12CD
ABCD
ABxCE
AByCdE
LCS算出
LCS算出
AB|CD
AB|C|E
LCS算出
AB|C

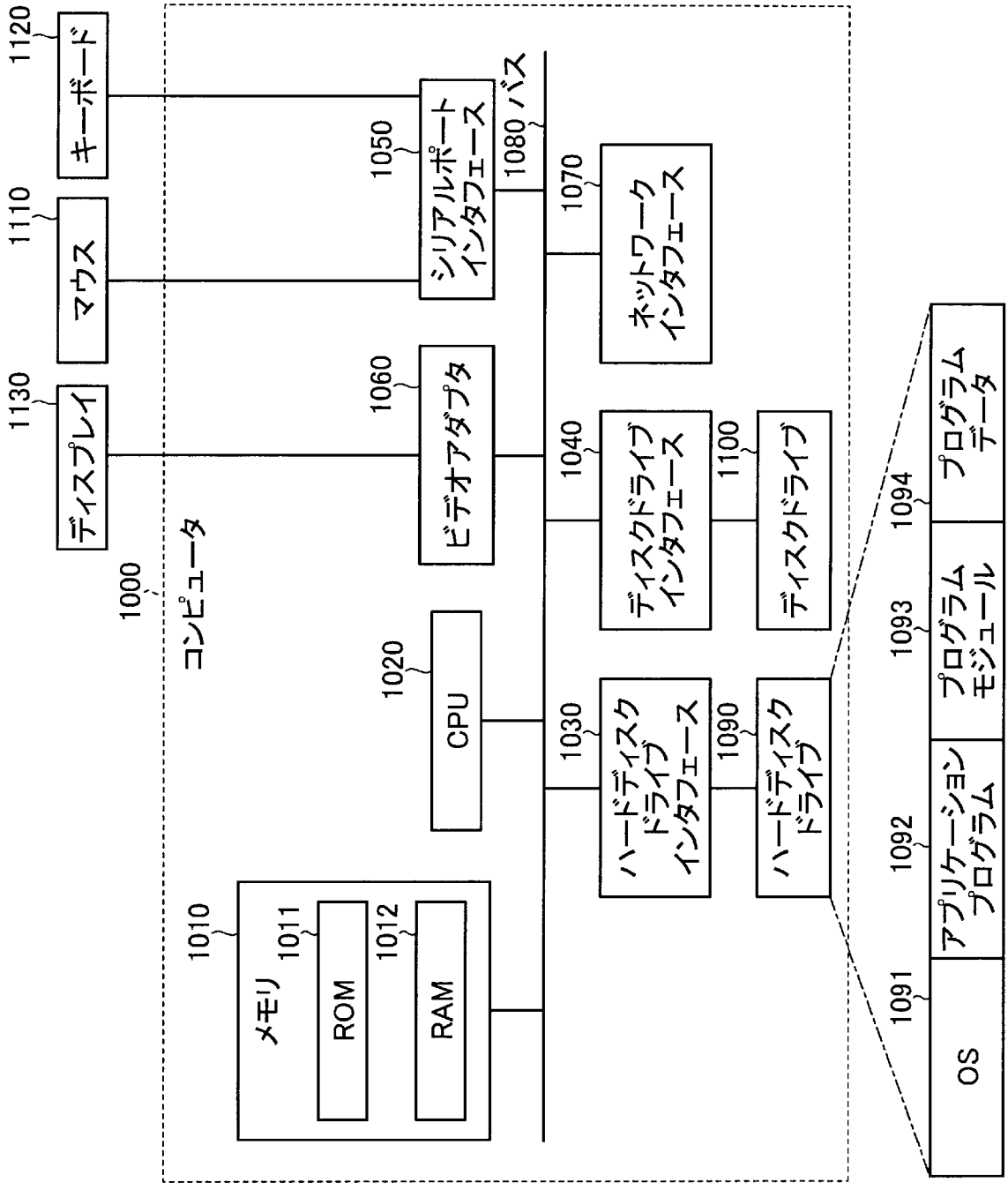
[図7]


スタート
S101
クラスタ集合初期化
S102
クラスタ集合の
サイズが2以上?
No
Yes
S103
処理対象クラスタ抽出
S104
処理対象クラスタと他クラスタの
LCS算出
S105
最長一致部分
文字列長が
閾値以上?
No
Yes
S107
処理対象クラスタを
結果リストに追加
S106
クラスタのマージ
S108
最後のクラスタを
結果リストに追加
S109
クラスタサイズが
閾値以上のものを抽出
エンド

[図8]


スタート
S201
対象文字列x,y入力
S202
テーブルt[0...len(y)][0...len(x)]
初期化
S203
i=1,2,...,len(y)
S204
j=1,2,...,len(x)
S205
x[j]=y[i]?
Yes
No
S206
t[i][j]=max(t[i-1][j],t[i][j-1])
S207
t[i][j]
=t[i-1][j-1]+1
S208
S209
S210
結果文字列初期化
S211
i>0 and j>0の間繰り返し
S212
x[j]=y[i]?
Yes
No
S213
t[i-1][j]>t[i][j-1]?
No
Yes
S214
i←i-1
S215
j←j-1
S216
結果文字列の末尾が
区切り文字でなければ
区切り文字を追記
S217
結果文字列に
x[j]を追記
S218
i←i-1
j←j-1
S219
S220
結果文字列を反転
エンド

[図9]


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1040
ディスクドライブインタフェース
1050
シリアルポートインタフェース
1060
ビデオアダプタ
1070
ネットワークインタフェース
1080
バス
1090
ハードディスクドライブ
1100
ディスクドライブ
1091
OS
1092
アプリケーションプログラム
1093
プログラムモジュール
1094
プログラムデータ
1120
キーボード
1110
マウス
1130
ディスプレイ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/005772

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/56(2013.01)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)
Int.Cl. G06F21/56

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	1971-2018
Registered utility model specifications of Japan	1996-2018
Published registered utility model applications of Japan	1994-2018

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.
Y A	JP 2007-515867 A (THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK) 14 June 2007, paragraphs [0101]-[0104] & WO 2005/047862 A2, paragraphs [0101]-[0113] & US 2005/0281291 A1	1-2, 4, 6-7 3, 5
Y A	US 2009/0235357 A1 (COMPUTER ASSOCIATES THINK, INC.) 17 September 2009, paragraphs [0001]-[0043], fig. 1-4 (Family: none)	1-2, 4, 6-7 3, 5
Y	JP 2007-242002 A (MITSUBISHI ELECTRIC CORP.) 20 September 2007, abstract, paragraph [0022] (Family: none)	4
A	JP 2005-234661 A (NEC CORP.) 02 September 2005, paragraphs [0125]-[0187], fig. 11-19 (Family: none)	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 15 March 2018 (15.03.2018)	Date of mailing of the international search report 27 March 2018 (27.03.2018)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／００５７７２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/56(2013.01)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.　G06F21/56

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	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８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
Y A	JP 2007-515867 A（ザ　トラスティーズ　オブ　コロンビア　ユニヴァーシティ　イン　ザ　シティ　オブ　ニューヨーク）2007.06.14, 段落[0101]-[0104] & WO 2005/047862 A2,段落[0101]-[0113] & US 2005/0281291 A1	1-2,4,6-7 3,5
Y A	US 2009/0235357 A1 (COMPUTER ASSOCIATES THINK, INC.) 2009.09.17, 段落[0001]-[0043],図 1-4（ファミリーなし）	1-2,4,6-7 3,5

☑　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
１５．０３．２０１８	２７．０３．２０１８

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　６２９３
上島　拓也
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	JP 2007-242002 A（三菱電機株式会社）2007.09.20, 要約,段落[0022]（ファミリーなし）	4
A	JP 2005-234661 A（日本電気株式会社）2005.09.02, 段落[0125]-[0187],図 11-19（ファミリーなし）	3