(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
2019年11月28日(28.11.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/224907 A1

(51) 国際特許分類:
G06F 13/00 (2006.01)

(21) 国際出願番号： PCT/JP2018/019656

(22) 国際出願日： 2018年5月22日(22.05.2018)

(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:三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

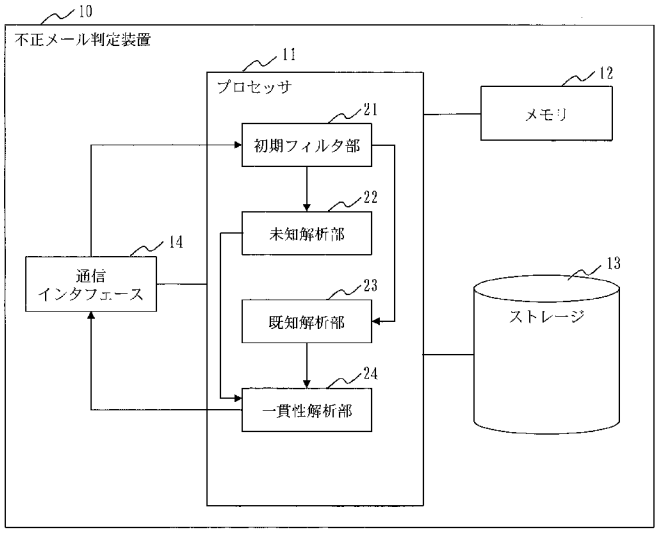
(72) 発明者: 山本 匠 (**YAMAMOTO, Takumi**); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 西川 弘毅 (**NISHIKAWA, Hiroki**); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 河内 清人 (**KAWAUCHI, Kiyoto**); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井国際特許業務法人(**MIZOI INTERNATIONAL PATENT FIRM**); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号３階 Kanagawa (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,

(54) **Title:** UNAUTHORIZED EMAIL DETERMINATION DEVICE, UNAUTHORIZED EMAIL DETERMINATION METHOD AND UNAUTHORIZED EMAIL DETERMINATION PROGRAM

(54) 発明の名称： 不正メール判定装置、不正メール判定方法及び不正メール判定プログラム



10 Unauthorized email determination device
11 Processor
12 Memory
13 Storage
14 Communication interface
21 Initial filter unit
22 Unknown analysis unit
23 Known analysis unit
24 Consistency analysis unit

(57) **Abstract:** This unauthorized email determination device (10) is provided with a consistency analysis unit (24). The consistency analysis unit (24) identifies the intention of a newly received, target email with a method involving extracting function words, which are words that show the reason that the target email was sent, from the body of the target email. The consistency analysis unit (24) determines whether or not the target email is an unauthorized email on the basis of the

WO 2019/224907 A1

[続葉有]

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)）

relation between the identified intention of the target email, and other emails received in the past from the same sender as the target email.

(57) 要約：不正メール判定装置（１０）は、一貫性解析部（２４）を備える。一貫性解析部（２４）は、新たに受信した受信メールを対象メールとして、対象メールの本文から、対象メールを送信した理由を示す単語である機能語を抽出するといった方法により、対象メールの意図を特定する。一貫性解析部（２４）は、対象メールと同一の差出人から過去に受信した他の受信メールと、特定された対象メールの意図との関係から、対象メールが不正なメールであるか否かを判定する。

明　細　書

発明の名称 ：

不正メール判定装置、不正メール判定方法及び不正メール判定プログラム

技術分野

[0001] この発明は、標的型攻撃メールを検知する技術に関する。

背景技術

[0002] Ａｄｖａｎｃｅｄ　Ｐｅｒｓｉｓｔｅｎｔ　Ｔｈｒｅａｔといった標的型攻撃の多くは、攻撃の侵入手口として不正なメールを利用した標的型攻撃メールである。

標的型攻撃メールでは、組織及び人物といった攻撃対象に関係のある情報を用い、巧みに作りこみをした文章が利用される。標的型攻撃メールでは、メールに添付された悪性なファイルを開かせようとしたり、本文に記載されたＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）が示す悪性なＷｅｂサイトに訪れさせようとしたりする。

[0003] 添付ファイル及びＵＲＬに関しては、コンテンツの悪性度合いを静的又は動的に解析する既存の技術が知られている。例えば、検査対象の添付ファイルが既知のマルウェアのパターンにマッチするかを確認することでマルウェアを検知する技術がある。また、ファイルの実行時のふるまいの特徴を利用してマルウェアを検知する技術もある。また、悪性なＷｅｂサイトを示すＵＲＬのブラックリストを用意し、ユーザが危険なＷｅｂサイトを訪れることを未然に防止する技術もある。そして、これらの技術を搭載したマルウェア検知ソフトウェアがある。

しかし、高度な攻撃者になればなるほど、添付ファイル及びＵＲＬがマルウェア検知ソフトウェアに検知されるかどうかを事前に確認した上で、攻撃を実行する。そのため、未知のマルウェア及び新しい悪性なＵＲＬについては、適切に検知することは難しい。

[0004] また、メールのヘッダ情報の不自然さから攻撃を検知する技術が存在する

。この技術では、差出人の送信ドメイン認証結果と、送信経路と、使用メールソフトと、経由国といった情報に基づき、不正なメールであるか否かを判定する。しかし、この技術では、正規ユーザのアカウントを悪用したなりすましメールに関しては検知することはできない。

[0005] 非特許文献１には、なりすましメールを検知する技術が記載されている。

非特許文献１に記載された技術では、メールの差出人本人が出すメールが、語彙レベルと、構文レベルと、構造レベルとで分析され、個人性を表すプロファイルが作成される。語彙レベルとは、単語数と、単語単位の文字数と、テキスト全体の文字数と、行単位の文字数と、行数と、文章数と、テキスト中の個々の文字の頻度と、文の終端用の文字の頻度と等である。構文レベルとは、形容詞の数と、副詞の数と、等位接続詞の数と、過去分詞の数と等である。構造レベルとは、署名と住所と電話番号といった著者を特定する情報と、挨拶文の形式と、文の始め方と、文の終わり方と等である。文の始め方は、大文字の数と小文字の数といったことである。文の終わり方は、文章を区切りにスペースを利用している文章の数と文章区切りにドットを利用している文章の数と文章区切りにドット以外の句読点を利用している文章の数と文章が終わった後にスペースを利用している文章の数といったことである。

非特許文献１に記載された技術では、差出人から過去に受信したメールから、差出人のプロファイルが作成され、新たに受信したメールがプロファイルにマッチしない場合にはなりすましメールと判定される。

先行技術文献

非特許文献

[0006] 非特許文献1：Ｓｅｖｔａｐ Ｄｕｍａｎ, Ｋｕｂｒａ Ｋａｌｋａｎ Ｃａｋｍａｋｃｉｙ, Ｍａｎｕｅｌ Ｅｇｅｌｅｚ, Ｗｉｌｌｉａｍ Ｒｏｂｅｒｔｓｏｎ ａｎｄ Ｅｎｇｉｎ Ｋｉｒｄａ：“ＥｍａｉｌＰｒｏｆｉｌｅｒ：Ｓｐｅａｒｐｈｉｓｈｉｎｇ Ｆｉｌｔｅｒｉｎｇ ｗｉｔｈ Ｈｅａｄｅｒ ａｎｄ Ｓｔｙｌｏｍｅｔｒｉｃ Ｆｅａｔｕｒｅｓ

of Emails”, Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual

発明の概要

発明が解決しようとする課題

[0007] しかし、攻撃者がなりすまし対象の人物の文章の癖を正確に真似た場合と、過去のメールがそのまま流用された場合とには、非特許文献１に記載された技術を利用しても検知することができない。

この発明は、標的型攻撃メールを適切に検知可能にすることを目的とする。

課題を解決するための手段

[0008] この発明に係る不正メール判定装置は、

新たに受信した受信メールを対象メールとして、前記対象メールの本文から前記対象メールの意図を特定する意図特定部と、

前記対象メールと同一の差出人から受信した他の受信メールと、前記意図特定部によって特定された前記対象メールの意図との関係から、前記対象メールが不正なメールであるか否かを判定するメール判定部と

を備える。

発明の効果

[0009] この発明では、対象メールと同一の差出人から受信した他の受信メールと、対象メールの意図との関係から、対象メールが不正なメールであるか否かを判定する。これにより、標的型攻撃メールを適切に検知可能になる。

図面の簡単な説明

[0010] [図1]実施の形態１に係る不正メール判定装置１０の構成図。

[図2]実施の形態１に係る初期フィルタ部２１の構成図。

[図3]実施の形態１に係る未知解析部２２の構成図。

[図4]実施の形態１に係る既知解析部２３の構成図。

[図5]実施の形態１に係る一貫性解析部２４の構成図。

[図6]実施の形態１に係る不正メール判定装置１０の全体的な処理のフローチャート。

[図7]実施の形態１に係る初期フィルタ部２１の処理のフローチャート。

[図8]実施の形態１に係る未知解析部２２の処理のフローチャート。

[図9]実施の形態１に係る既知解析部２３の処理のフローチャート。

[図10]実施の形態１に係るプロファイル生成部２３３の処理のフローチャート。

[図11]実施の形態１に係る一致判定部２３４の処理のフローチャート。

[図12]実施の形態１に係る一貫性解析部２４の処理のフローチャート。

[図13]実施の形態１に係る意図特定部２４１の処理のフローチャート。

[図14]実施の形態１に係るルール適用部２４２及びメール判定部２４３の処理のフローチャート。

[図15]実施の形態１に係る一貫性判定ルール２４４に登録されるルールを示す図。

[図16]実施の形態１に係る機能語及びメール種類毎に適用されるルールを示す図。

[図17]変形例１に係る不正メール判定装置１０の構成図。

[図18]実施の形態２に係る一貫性解析部２４の構成図。

[図19]実施の形態２に係る意図学習部２４５の処理のフローチャート。

[図20]実施の形態２に係る意図推定部２４６の処理のフローチャート。

発明を実施するための形態

[0011] 実施の形態１.

＊＊＊構成の説明＊＊＊

図１を参照して、実施の形態１に係る不正メール判定装置１０の構成を説明する。

不正メール判定装置１０は、コンピュータである。

不正メール判定装置１０は、プロセッサ１１と、メモリ１２と、ストレー

ジ１３と、通信インタフェース１４とのハードウェアを備える。プロセッサ１１は、信号線を介して他のハードウェアと接続され、これら他のハードウェアを制御する。

[0012] プロセッサ１１は、プロセッシングを行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）である。プロセッサ１１は、具体例としては、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ）、ＧＰＵ（Ｇｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。

[0013] メモリ１２は、データを一時的に記憶する記憶装置である。メモリ１２は、具体例としては、ＳＲＡＭ（Ｓｔａｔｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＤＲＡＭ（Ｄｙｎａｍｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）である。

[0014] ストレージ１３は、データを保管する記憶装置である。ストレージ１３は、具体例としては、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）である。また、ストレージ１３は、ＳＤ（登録商標，Ｓｅｃｕｒｅ Ｄｉｇｉｔａｌ）メモリカード、ＣＦ（ＣｏｍｐａｃｔＦｌａｓｈ，登録商標）、ＮＡＮＤフラッシュ、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）といった可搬記録媒体であってもよい。

[0015] 通信インタフェース１４は、外部の装置と通信するためのインタフェースである。通信インタフェース１４は、具体例としては、Ｅｔｈｅｒｎｅｔ（登録商標）、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）、ＨＤＭＩ（登録商標，Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ Ｍｕｌｔｉｍｅｄｉａ Ｉｎｔｅｒｆａｃｅ）のポートである。

[0016] 不正メール判定装置１０は、機能構成要素として、初期フィルタ部２１と、未知解析部２２と、既知解析部２３と、一貫性解析部２４とを備える。不正メール判定装置１０の各機能構成要素の機能はソフトウェアにより実現される。

ストレージ１３には、不正メール判定装置１０の各機能構成要素の機能を実現するプログラムが格納されている。このプログラムは、プロセッサ１１によりメモリ１２に読み込まれ、プロセッサ１１によって実行される。これにより、不正メール判定装置１０の各機能構成要素の機能が実現される。

[0017] 図２を参照して、実施の形態１に係る初期フィルタ部２１の構成を説明する。

初期フィルタ部２１は、機能構成要素として、送信元抽出部２１１と、ブラックリスト判定部２１２と、コンテンツ判定部２１３と、差異判定部２１４とを備える。初期フィルタ部２１は、ストレージ１３に記憶されたブラックリスト２１６を使用する。

[0018] 図３を参照して、実施の形態１に係る未知解析部２２の構成を説明する。

未知解析部２２は、機能構成要素として、宛名判定部２２１と、身元判定部２２２と、名刺判定部２２３と、公開情報判定部２２４とを備える。未知解析部２２は、ストレージ１３に記憶された人名辞書データ２２５と、定型文データ２２６と、受信者プロファイル２２７とを使用する。また、未知解析部２２は、通信インタフェース１４を介して接続された名刺管理システム３０を使用する。

[0019] 図４を参照して、実施の形態１に係る既知解析部２３の構成を説明する。

既知解析部２３は、機能構成要素として、本人性判定部２３１と、トピック判定部２３２とを備える。トピック判定部２３２は、プロファイル生成部２３３と、一致判定部２３４とを備える。既知解析部２３は、ストレージ１３に記憶された差出人プロファイル２３５を使用する。

[0020] 図５を参照して、実施の形態１に係る一貫性解析部２４の構成を説明する。

一貫性解析部２４は、機能構成要素として、意図特定部２４１と、ルール適用部２４２と、メール判定部２４３とを備える。一貫性解析部２４は、ストレージ１３に記憶された一貫性判定ルール２４４を使用する。

[0021] 図１では、プロセッサ１１は、１つだけ示されていた。しかし、プロセッ

サ１１は、複数であってもよく、複数のプロセッサ１１が、各機能を実現するプログラムを連携して実行してもよい。

[0022] ＊＊＊動作の説明＊＊＊

図６から図１６を参照して、実施の形態１に係る不正メール判定装置１０の動作を説明する。

実施の形態１に係る不正メール判定装置１０の動作は、実施の形態１に係る不正メール判定方法に相当する。また、実施の形態１に係る不正メール判定装置１０の動作は、実施の形態１に係る不正メール判定プログラムの処理に相当する。

[0023] 図１及び図６を参照して、実施の形態１に係る不正メール判定装置１０の全体的な処理を説明する。

（ステップＳ１：初期フィルタ処理）

初期フィルタ部２１は、新たに受信した受信メールを分析対象の対象メールとして、対象メールに明らかに不正な特徴が含まれているかを確認する。初期フィルタ部２１は、明らかに不正な特徴を有している場合には、対象メールを不正なメールとしてステップＳ２以降の処理から除外する。

[0024] （ステップＳ２：既知判定処理）

初期フィルタ部２１は、対象メールの差出人が過去にやりとりしたことのない未知差出人であるか、過去にやりとりしたことのある既知差出人であるかを判定する。

初期フィルタ部２１は、対象メールの差出人が未知差出人である場合には、処理をステップＳ３に進める。一方、初期フィルタ部２１は、対象メールの差出人が既知差出人である場合には、処理をステップＳ４に進める。

[0025] （ステップＳ３：未知解析処理）

未知解析部２２は、対象メールが初めてメールのやりとりをする相手からのメールとして不適切な特徴を持つメールであるか否かを判定する。未知解析部２２は、不適切な特徴を持つメールである場合には、対象メールを不正なメールとしてステップＳ５の処理から除外する。

[0026] （ステップＳ４：既知解析処理）

既知解析部２３は、対象メールのトピックが過去に対象メールの差出人とやりとりされたトピックか否かを判定する。

[0027] （ステップＳ５：一貫性解析処理）

一貫性解析部２４は、対象メールと、対象メールの差出人からの過去の受信メールとの関係から、やりとりの一貫性を解析する。一貫性解析部２４は、やりとりに矛盾がある場合には、対象メールを不正なメールと判定する。

[0028] 図２及び図７を参照して、実施の形態１に係る初期フィルタ部２１の処理を説明する。

初期フィルタ部２１の処理は、図６のステップＳ１及びステップＳ２の処理に対応する。具体的には、ステップＳ１１からステップＳ１４の処理が図６のステップＳ１の処理に対応する。また、ステップＳ１５の処理が図６のステップＳ２の処理に対応する。

[0029] （ステップＳ１１：送信元抽出処理）

送信元抽出部２１１は、対象メールの差出人の情報を抽出する。具体的には、送信元抽出部２１１は、対象メールのヘッダ情報からＦｒｏｍフィールドの情報及びＲｅｃｅｉｖｅｄフィールドの情報を、差出人の情報及び経由したサーバ情報として抽出する。

[0030] （ステップＳ１２：ブラックリスト判定処理）

ブラックリスト判定部２１２は、ステップＳ１１で抽出された差出人と経由したサーバとの少なくともいずれかが、ブラックリスト２１６に含まれているか否かを判定する。ブラックリスト２１６は、事前に作成される。ブラックリスト２１６は、不正なメールを送信する差出人が発見される度に追加されてもよい。

ブラックリスト判定部２１２は、差出人と経由したサーバとの少なくともいずれかがブラックリスト２１６に含まれている場合には、対象メールを不正なメールであると判定し、処理を終了する。一方、ブラックリスト判定部２１２は、差出人及び経由したサーバがブラックリスト２１６に含まれてな

い場合には、処理をステップＳ１３に進める。

[0031] （ステップＳ１３：コンテンツ判定処理）

コンテンツ判定部２１３は、対象メールに添付ファイルとＵＲＬとの少なくともいずれかが含まれているか否かを判定する。

コンテンツ判定部２１３は、添付ファイルとＵＲＬとのどちらも含まれていない場合には、対象メールを不正なメールでないと判定し、処理を終了する。一方、コンテンツ判定部２１３は、添付ファイルとＵＲＬといずれか一方でも含まれている場合には、処理をステップＳ１４に進める。

[0032] （ステップＳ１４：差異判定処理）

差異判定部２１４は、添付ファイルとＵＲＬとのうちステップＳ１３で含まれると判定されたものを対象として、対象のコンテンツが本文の内容と一致しているか否かを判定する。具体的には、差異判定部２１４は、添付ファイルを対象とする場合には、添付ファイルのコンテンツが本文の内容と一致しているか否かを判定する。一方、差異判定部２１４は、ＵＲＬを対象とする場合には、ＵＲＬが示すＷｅｂサイトのコンテンツが本文の内容と一致しているか否かを判定する。なお、コンテンツが本文の内容に一致しているか否かの判定には、例えば、文献（西川　弘毅、山本　匠、河内　清人、メールとそのコンテキスト情報を基にした不審メール検知手法の提案、コンピュータセキュリティシンポジウム２０１７、１Ｂ３－３）に記載された技術を利用することが可能である。

差異判定部２１４は、一致していない場合には、対象メールを不正なメールであると判定し、処理を終了する。一方、差異判定部２１４は、一致している場合には、処理をステップＳ１５に進める。

[0033] （ステップＳ１５：既知判定処理）

既知判定部２１５は、対象メールの差出人が過去の受信メールの差出人に含まれるか否かを判定することにより、対象メールの差出人が未知差出人であるか既知差出人であるかを判定する。

具体的には、既知判定部２１５は、ストレージ１３に記憶された過去の全

ての受信メールのＦｒｏｍフィールドの差出人メールアドレスまたは差出人名から、対象メールの差出人を検索する。過去の受信メールは、ストレージ１３に記憶されていてもよいし、通信インタフェース１４を介して接続された外部の記憶装置に記憶されていてもよい。既知判定部２１５は、検索されない場合には、対象メールの差出人は未知差出人と判定して、処理を図６のステップＳ３に進める。一方、既知判定部２１５は、検索された場合には、対象メールの差出人は既知差出人であると判定して、処理を図６のステップＳ４に進める。

[0034] 図３及び図８を参照して、実施の形態１に係る未知解析部２２の処理を説明する。

未知解析部２２の処理は、図６のステップＳ３の処理に対応する。

[0035] （ステップＳ２１：宛名判定処理）

宛名判定部２２１は、対象メールの本文の宛名として対象メールの受信者の名前があるか否かを判定する。具体的には、宛名判定部２２１は、英文メールの場合であれば、本文の先頭の“Ｄｅａｒ　Ｍｒ．Ｓｕｚｕｋｉ”といった宛名の記載に受信者の名前が含まれているか否かを判定する。宛名判定部２２１は、宛名等の定型的な記載形式を示す定型文データ２２６を参照して、宛名の記載を特定する。また、受信者の名前は、事前にメモリ１２等に記憶されているものとする。

宛名判定部２２１は、受信者の名前が含まれていない場合には、対象メールを不正なメールであると判定し、処理を終了する。一方、宛名判定部２２１は、受信者の名前が含まれている場合には、処理をステップＳ２２に進める。なおメーリングリスト宛などの宛先が複数あるケースもあるため、「ｄｅａｒ　ａｌｌ」「ｄｅａｒ　ｆｏｌｋｓ」「ｄｅａｒ　ｐｅｒｓｏｎ　ｗｈｏ　ｍａｙ　ｃｏｎｃｅｒｎ」などの定型文も登録しておき、このような場合は、受信者の名前が含まれていなくても不正なメールと判断しない。

[0036] （ステップＳ２２：身元判定処理）

身元判定部２２２は、対象メールの差出人が、本文中で名乗っているか否

かを判定する。具体的には、身元判定部２２２は、本文から受信者以外の人名を検索する。この際、身元判定部２２２は、人名辞書データ２２５を参照して、本文から受信者以外の人名を検索する。また、身元判定部２２２は、定型文データ２２６を参照して、「Ｍｙ　ｎａｍｅ　ｉｓ　ＸＸ」と「Ｉ’ｍ　ＸＸ」と署名（Ｓｉｇｎａｔｕｒｅ）といった差出人を名乗る際の定型的な記載形式を本文中から検索して、人名辞書データ２２５にはない人名を検索してもよい。

身元判定部２２２は、差出人が本文中で名乗っていない場合には、対象メールを不正なメールであると判定し、処理を終了する。一方、身元判定部２２２は、差出人が本文中で名乗っている場合には、処理をステップＳ２３に進める。

[0037] （ステップＳ２３：名刺判定処理）

名刺判定部２２３は、受信者が対象メールの差出人と名刺交換しているか否かを判定する。具体的には、名刺判定部２２３は、通信インタフェース１４を介して接続された名刺管理システム３０に、対象メールの差出人の名前が登録されていれば、受信者が差出人と名刺交換していると判定する。名刺管理システム３０は、名刺を管理する外部システムである。なお、受信者ではなく、受信者の所属する組織の誰かが差出人と名刺交換しているか否かを判定してもよい。

名刺判定部２２３は、名刺交換している場合には、対象メールを名刺存在メールであると判定して、処理を図６のステップＳ５に進める。一方、名刺判定部２２３は、名刺交換していない場合には、処理をステップＳ２４に進める。

[0038] （ステップＳ２４：公開情報判定処理）

公開情報判定部２２４は、対象メールの差出人に関する公開情報が、受信者に関連する内容であるか否かを判定する。

具体的には、公開情報判定部２２４は、ＯＳＩＮＴ（Ｏｐｅｎ　Ｓｏｕｒｃｅ　Ｉｎｔｅｌｌｉｇｅｎｃｅ）ツールを利用して、対象メールの差出人

に関する公開情報を収集する。公開情報判定部２２４は、収集された公開情報に、受信者プロファイル２２７に登録された情報が含まれているか否かにより、公開情報が受信者に関連する内容であるか否かを判定する。受信者プロファイル２２７には、受信者の業務とプロジェクトと趣味といった事柄に関する単語がリストとして事前に登録されている。

具体例としては、公開情報判定部２２４は、ＯＳＩＮＴで収集されたＷｅｂページについてはＴＦ－ＩＤＦ（Ｔｅｒｍ　Ｆｒｅｑｕｅｎｃｙ－Ｉｎｖｅｒｓｅ　Ｄｏｃｕｍｅｎｔ　Ｆｒｅｑｕｅｎｃｙ）といったキーワード抽出技術を用いてページのキーワードを抽出する。そして、公開情報判定部２２４は、Ｗｏｒｄ２Ｖｅｃ等の単語の類似度を計算する技術を用いて、プロファイルの単語とキーワードとの類似度を計算する。公開情報判定部２２４は、計算された類似度が第１閾値以上のペアが第１基準数以上含まれている場合には、収集された公開情報に受信者プロファイル２２７に登録された情報が含まれていると判定し、公開情報が受信者に関連する内容である判定する。一方、公開情報判定部２２４は、計算された類似度が第１閾値以上のペアが第１基準数以上含まれていない場合には、収集された公開情報に受信者プロファイル２２７に登録された情報が含まれていないと判定し、公開情報が受信者に関連しない内容である判定する。

公開情報判定部２２４は、公開情報が受信者に関連する内容である場合には、対象メールを関連分野メールであると判定し、処理を図６のステップＳ５に進める。一方、公開情報判定部２２４は、公開情報が受信者に関連する内容でない場合には、対象メールを不正なメールであると判定し、処理を終了する。

[0039] 図４及び図９を参照して、実施の形態１に係る既知解析部２３の処理を説明する。

既知解析部２３の処理は、図６のステップＳ４の処理に対応する。

[0040] （ステップＳ３１：本人性判定処理）

本人性判定部２３１は、対象メールの本文の文体から、本文が差出人本人

の文章であるか否かを判定する。具体的には、本人性判定部２３１は、非特許文献１に記載された技術等を用いて、本文が差出人本人の文章であるか否かを判定する。

本人性判定部２３１は、本文が差出人本人の文章でない場合には、対象メールを不正なメールであると判定し、処理を終了する。一方、本人性判定部２３１は、本文が差出人本人の文章である場合には、処理をステップＳ３２に進める。

[0041] （ステップＳ３２：トピック判定処理）

トピック判定部２３２は、対象メールのトピックが、対象メールと同一の差出人から受信した他の受信メールに含まれるか否か判定する。つまり、トピック判定部２３２は、対象メールのトピックが、受信者と差出人との間で過去にやりとりされたトピックであるか否かを判定する。

トピック判定部２３２は、対象メールのトピックが他の受信メールに含まれる場合には、対象メールをトピック一致メールであると判定し、処理を図６のステップＳ５に進める。一方、トピック判定部２３２は、対象メールのトピックが他の受信メールに含まれない場合には、対象メールをトピック不一致メールであると判定し、処理を図６のステップＳ５に進める。

[0042] 図４と図１０と図１１とを参照して、実施の形態１に係るトピック判定処理（図９のステップＳ３２）を詳細に説明する。トピック判定処理は、プロファイル生成部２３３の処理と一致判定部２３４の処理とを含む。

[0043] まず、図４及び図１０を参照して、実施の形態１に係るプロファイル生成部２３３の処理を説明する。

（ステップＳ４１：第１本文抽出処理）

プロファイル生成部２３３は、過去の全ての受信メールから本文を抽出する。

[0044] （ステップＳ４２：第１特徴抽出処理）

プロファイル生成部２３３は、ステップＳ４１で抽出された各受信メールの本文から特徴を抽出する。特徴としては、ＬＤＡ（Ｌａｔｅｎｔ　Ｄｉｒ

ｉｃｈｌｅｔ　Ａｌｌｏｃａｔｉｏｎ）を用いたトピックの選択確率と、ＴＦ－ＩＤＦによるキーワードとなどが考えられる。

[0045] （ステップＳ４３：クラスタリング処理）

プロファイル生成部２３３は、ステップＳ４２で抽出された特徴に基づき、過去の受信メールを複数のクラスタにクラスタリングする。プロファイル生成部２３３は、クラスタリングのアルゴリズムとして、ＤＢＳＣＡＮ（Ｄｅｎｓｉｔｙ－ｂａｓｅｄ　ｓｐａｔｉａｌ　ｃｌｕｓｔｅｒｉｎｇ　ｏｆ　ａｐｐｌｉｃａｔｉｏｎｓ　ｗｉｔｈ　ｎｏｉｓｅ）と、ＫＭＥＡＮＳといった既存の技術を用いればよい。

[0046] （ステップＳ４４：ラベル付け処理）

プロファイル生成部２３３は、ステップＳ４３で複数のクラスタにクラスタリングされた受信メールを学習用データとし、受信メールが所属するクラスタの識別子をその受信メールのラベルとして割り当てる。

[0047] （ステップＳ４５：学習処理）

プロファイル生成部２３３は、ステップＳ４４でラベル付けされた学習用データに基づき、教師有学習を行う。教師有学習のアルゴリズムとしては、ＳＶＭ及びランダムフォレストといった既存の手法を用いればよい。これにより、受信メールがどのクラスタに分類されるかを識別する識別器が生成される。

[0048] ステップＳ４６からステップＳ４９の処理は、受信メールの各差出人を対象として実行される。

[0049] （ステップＳ４６：第２本文抽出処理）

プロファイル生成部２３３は、過去の全ての受信メールのうち、対象の差出人から送信された受信メールから、本文を抽出する。

[0050] （ステップＳ４７：第２特徴抽出処理）

プロファイル生成部２３３は、ステップＳ４２と同じ方法により、ステップＳ４６で抽出された各受信メールの本文から特徴を抽出する。

[0051] （ステップＳ４８：第１識別処理）

プロファイル生成部２３３は、ステップＳ４６で抽出された各受信メールを対象として、ステップＳ４５で生成された識別器と、ステップＳ４７で対象の受信メールから抽出された特徴とに基づき、対象の受信メールを分類する。そして、プロファイル生成部２３３は、対象の受信メールに、分類されたクラスタの識別子をラベルとして割り当てる。

[0052] （ステップＳ４９：プロファイル生成処理）

プロファイル生成部２３３は、ステップＳ４６で抽出された各受信メールに対して割り当てられたラベルのリストを、対象の差出人についてのプロファイルとして差出人プロファイル２３５に書き込む。

[0053] 次に、図４及び図１１を参照して、実施の形態１に係る一致判定部２３４の処理を説明する。

（ステップＳ５１：送信元抽出処理）

一致判定部２３４は、対象メールの差出人の情報を抽出する。差出人の情報の抽出方法は、図７のステップＳ１１と同じである。ここでは、対象メールをＭ０とする。また、抽出された差出人の情報が示す差出人をＰとする。つまり、対象メールＭ０の差出人をＰとする。

[0054] （ステップＳ５２：送信元特定処理）

一致判定部２３４は、差出人プロファイル２３５から、差出人Ｐについてのプロファイルを読み出す。

[0055] （ステップＳ５３：第３本文抽出処理）

一致判定部２３４は、過去の全ての受信メールのうち、差出人Ｐについての受信メールを特定する。一致判定部２３４は、特定された差出人Ｐについての受信メールのうち、受信日時が新しいものから順にＸ通の受信メールを抽出する。Ｘは、１以上の整数である。ここでは、抽出されたＸ通の受信メールを、受信日時が新しいものから順にＭ１，．．．，ＭＸとする。

一致判定部２３４は、対象メールＭ０と、抽出されたＸ通の受信メールＭ１，．．．，ＭＸから本文を抽出する。

[0056] （ステップＳ５４：第３特徴抽出処理）

一致判定部２３４は、図１０のステップＳ４２と同じ方法により、受信メールＭ０，．．．，ＭＸの本文から特徴を抽出する。

[0057] （ステップＳ５５：第２識別処理）

一致判定部２３４は、図１０のステップＳ４８と同様に、対象メールＭ０と、受信メールＭ１，．．．，ＭＸとを分類して、識別子をラベルとして割り当てる。ここでは、対象メールＭ０に割り当てられたラベルをＣ０とし、受信メールＭ１，．．．，ＭＸに割り当てられたラベルをＣ１，．．．，ＣＸとする。

[0058] （ステップＳ５６：第１トピック判定処理）

一致判定部２３４は、ステップＳ５５で対象メールＭ０に割り当てられたラベルＣ０が、ステップＳ５２で読み出された差出人Ｐについてのプロファイルに含まれるか否かを判定する。

一致判定部２３４は、ラベルＣ０がプロファイルに含まれない場合には、対象メールをトピック不一致メールであると判定し、処理を図６のステップＳ５に進める。一方、一致判定部２３４は、ラベルＣ０がプロファイルに含まれる場合には、処理をステップＳ５７に進める。

[0059] （ステップＳ５７：第２トピック判定処理）

一致判定部２３４は、ステップＳ５５で対象メールＭ０に割り当てられたラベルＣ０が、ステップＳ５５で受信メールＭ１，．．．，ＭＸに割り当てられたラベルＣ１，．．．，ＣＸに含まれるか否かを判定する。

一致判定部２３４は、ラベルＣ０がラベルＣ１，．．．，ＣＸに含まれない場合には、対象メールをトピック不一致メールであると判定し、処理を図６のステップＳ５に進める。一方、一致判定部２３４は、ラベルＣ０がラベルＣ１，．．．，ＣＸに含まれる場合には、対象メールをトピック一致メールであると判定し、処理を図６のステップＳ５に進める。

[0060] 図５及び図１２を参照して、実施の形態１に係る一貫性解析部２４の処理を説明する。

ここで、初期フィルタ部２１と未知解析部２２と既知解析部２３との処理

が実行された結果、対象メールは、不正なメールと、不正でないメールと、名刺存在メールと、関連分野メールと、トピック一致メールと、トピック不一致メールとに分類されている。一貫性解析部２４は、名刺存在メールと関連分野メールとトピック一致メールとトピック不一致メールとのメール種類に対象メールが分類された場合に、対象メールが不正であるか否かを判定する。

[0061] （ステップＳ６１：意図特定処理）

意図特定部２４１は、対象メールの本文から対象メールの意図を特定する。ここで、対象メールの意図とは、転送と再送と添付忘れと更新と依頼対応といった対象メールを送信した理由である。実施の形態１では、意図特定部２４１は、対象メールの本文から、事前に登録された機能語に類似する単語を抽出し、抽出された単語に類似する機能語が示す意図を対象メールの意図として特定する。

[0062] （ステップＳ６２：ルール適用処理）

ルール適用部２４２は、ステップＳ６１で特定された意図と、対象メールのメール種類とに対応するルールを、一貫性判定ルール２４４から読み出す。一貫性判定ルール２４４には、事前にルールが登録されている。一貫性判定ルール２４４には、ルールがプラグイン等として適宜追加可能である。ルールは、不正なメールであると判定するための条件を示す。上述した通り、メール種類は、名刺存在メールと関連分野メールとトピック一致メールとトピック不一致メールとのどれかである。

[0063] （ステップＳ６３：メール判定処理）

メール判定部２４３は、対象メールと同一の差出人から受信した他の受信メールと、ステップＳ６１で特定された対象メールの意図との関係から、対象メールが不正なメールであるか否かを判定する。

具体的には、メール判定部２４３は、ステップＳ６２で読み出されたルールが示す条件と、対象メールと同一の差出人から受信した他の受信メールとにより、対象メールが不正なメールであるか否かを判定する。

[0064] 図５及び図１３を参照して、実施の形態１に係る意図特定部２４１の処理を詳細に説明する。

意図特定部２４１の処理は、図１２のステップＳ６１に対応する。

[0065] （ステップＳ７１：第４本文抽出処理）

意図特定部２４１は、対象メールから本文を抽出する。

[0066] （ステップＳ７２：単語抽出処理）

意図特定部２４１は、ステップＳ７１で抽出された本文から単語を抽出する。例えば、意図特定部２４１は、本文に対して形態素解析を行い、名詞及び動詞といった一部の品詞を単語として抽出する。

[0067] （ステップＳ７３：類似度計算処理）

意図特定部２４１は、ステップＳ７２で抽出された各単語を対象として、対象の単語について各機能語との類似度を計算する。類似度の計算には、Ｗｏｒｄ２Ｖｅｃ等の単語の類似度を計算する技術が用いられる。機能語は、転送と再送と添付忘れと間違いと更新と回答といった対象メールを送信した理由を示す単語であり、事前に登録されている。機能語とルール機能語は、プラグイン等として適宜追加可能である。

[0068] （ステップＳ７４：類似度判定処理）

意図特定部２４１は、ステップＳ７３で計算された類似度が第２閾値以上の単語が第２基準数以上含まれているか否かを判定する。

意図特定部２４１は、第２閾値以上の単語が第２基準数以上含まれていない場合には、対象メールを不正なメールでないと判定し、処理を終了する。一方、意図特定部２４１は、第２閾値以上の単語が第２基準数以上含まれている場合には、単語との類似度が第２閾値以上である判定された機能語をリスト化して、処理を図１２のステップＳ６２に進める。

[0069] 図５及び図１４を参照して、実施の形態１に係るルール適用部２４２及びメール判定部２４３の処理を詳細に説明する。

ルール適用部２４２及びメール判定部２４３の処理は、図１２のステップＳ６２及びステップＳ６３の処理に対応する。

[0070] （ステップＳ８１：リスト判定処理）

ルール適用部２４２は、ステップＳ７４で生成されたリストの全ての機能語が選択されたか否かを判定する。

ルール適用部２４２は、全ての機能語が選択された場合には、対象メールを不正なメールでないと判定し、処理を終了する。一方、ルール適用部２４２は、選択されていない機能語がある場合には、処理をステップＳ８２に進める。

[0071] （ステップＳ８２：機能語選択処理）

ルール適用部２４２は、リストから未だ選択されていない機能語を１つ選択する。

[0072] （ステップＳ８３：ルール読出処理）

ルール適用部２４２は、ステップＳ８２で選択された機能語と、対象メールのメール種類とに応じたルールを、一貫性判定ルール２４４から読み出す。

[0073] （ステップＳ８４：ルール判定処理）

メール判定部２４３は、ステップＳ８３で読み出されたルールが示す条件と、対象メールと同一の差出人から受信した他の受信メールとにより、対象メールが不正なメールであるか否かを判定する。ここでは、メール判定部２４３は、ルールが示す条件を対象メールもしくは他の受信メールが満たす場合には、対象メールを不正なメールであると判定する。一方、メール判定部２４３は、ルールが示す条件を対象メールもしくは他の受信メールが満たさない場合には、対象メールを不正なメールでないと判定する。

[0074] 図１５及び図１６を参照して、一貫性判定ルール２４４に登録されるルールの例を説明する。

図１５には、ルール１からルール７の７個のルールが示されている。図１６には、機能語及びメール種類毎に適用されるルールが示されている。図１６では、メール種類が名刺存在メールと関連分野メールとについてルールが示されているが、メール種類がトピック一致メールとトピック不一致メール

とについても同様にルールが設定される。

[0075] 例えば、名刺存在メールに「再送」の機能語に関係する単語が含まれていた場合、ルール１が適用される。

ルール１は、対象メールの本文に機能語が含まれている場合には、不正なメールであると判定されるルールである。対象メールの本文に機能語が含まれている場合のみ図１４のステップＳ８４の処理が実行される。そのため、ルール１が適用されると、必ず不正なメールと判定される。普段やりとりの無い人物から突然メールを「再送」されることは不自然なためである。

[0076] 例えば、名刺存在メールに「転送」の機能語に関係する単語が含まれていた場合、ルール２が適用される。

ルール２では、メール判定部２４３は、対象メールの本文と添付ファイルのコンテンツとＵＲＬのコンテンツとからトピック及びキーワードを抽出し、差出人と過去にやりとりしたメールのトピックと一致するか否かを判定する。トピックが一致するか否かの判定方法は、一致判定部２３４の処理と同じである。トピックが一致しなければ、不正なメールと判定される。普段やりとりの無い人物から関係の無いトピックの情報が送られることは不自然なためである。

[0077] 例えば、関連分野メールに「再送」の機能語に関係する単語が含まれていた場合、ルール３又はルール４が適用される。

ルール３では、メール判定部２４３は、同じ差出人から直前に同じ内容のメールが送られているか否かを判定する。送られていなければ不正なメールと判定される。再送したことを通知するメールの前に、同じ内容のメールが過去に送られていなければ不自然なためである。同じ内容のメールか否かは、Ｄｏｃ２Ｖｅｃといった既存技術を利用し、閾値以上の類似度であれば同じ内容の文章であると判定することにより判定可能である。

ルール４では、メール判定部２４３は、同じ差出人から直前に送られた同じメールに同じ添付ファイルがついているか否かを判定する。違う添付ファイルが添付されていれば不正なメールと判定される。再送であるにも関わら

ず、異なる添付ファイルが送られていれば不自然なためである。

[0078] 例えば、関連分野メールに「添付し忘れ」の機能語に関係する単語が含まれていた場合、ルール３又はルール５が適用される。

ルール５では、メール判定部２４３は、同じ差出人から直前に送られたメールに添付ファイルが添付されているか否かを判定する。添付されていれば不正なメールと判定される。添付し忘れているはずなのに添付されているのは不自然なためである。

[0079] ＊＊＊実施の形態１の効果＊＊＊

以上のように、実施の形態１に係る不正メール判定装置１０は、対象メールと同一の差出人から受信した他の受信メールと、対象メールの意図との関係から、対象メールが不正なメールであるか否かを判定する。これにより、標的型攻撃メールを適切に検知可能になる。

特に、なりすまし対象の人物の文章の癖を正確に真似た場合、及び、過去のメールをそのまま流用された場合においても、受信メールのトピックの不一致とやりとりの矛盾といった条件から、不正なメールを検知することができる。そのため、巧妙な攻撃者による、メール経由でのマルウェア感染を防ぐことが可能となる。

[0080] 特に、実施の形態１に係る不正メール判定装置１０は、対象メールの意図を示す機能語及びメール種類に応じた条件に基づき、対象メールが不正なメールであるか否かを判定する。これにより、標的型攻撃メールをより適切に検知可能になる。

[0081] ＊＊＊他の構成＊＊＊

＜変形例１＞

実施の形態１では、各機能構成要素がソフトウェアで実現された。しかし、変形例１として、各機能構成要素はハードウェアで実現されてもよい。この変形例１について、実施の形態１と異なる点を説明する。

[0082] 図１７を参照して、変形例１に係る不正メール判定装置１０の構成を説明する。

各機能構成要素がハードウェアで実現される場合には、不正メール判定装置１０は、プロセッサ１１とメモリ１２とストレージ１３とに代えて、電子回路１５を備える。電子回路１５は、各機能構成要素と、メモリ１２と、ストレージ１３との機能とを実現する専用の回路である。

[0083] 電子回路１５としては、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ロジックＩＣ、ＧＡ（Ｇａｔｅ Ａｒｒａｙ）、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）が想定される。

各機能構成要素を１つの電子回路１５で実現してもよいし、各機能構成要素を複数の電子回路１５に分散させて実現してもよい。

[0084] ＜変形例２＞

変形例２として、一部の各機能構成要素がハードウェアで実現され、他の各機能構成要素がソフトウェアで実現されてもよい。

[0085] プロセッサ１１とメモリ１２とストレージ１３と電子回路１５とを処理回路という。つまり、各機能構成要素の機能は、処理回路により実現される。

[0086] 実施の形態２．

実施の形態２は、対象メールの本文全体から意図を特定する点が実施の形態１と異なる。実施の形態２では、この異なる点を説明し、同一の点については説明を省略する。

[0087] ＊＊＊構成の説明＊＊＊

図１８を参照して、実施の形態２に係る一貫性解析部２４の構成を説明する。

一貫性解析部２４は、意図特定部２４１が、意図学習部２４５と、意図推定部２４６と、学習用メール２４７とを備える点が図５に示す構成と異なる。

[0088] ＊＊＊動作の説明＊＊＊

図１９及び図２０を参照して、実施の形態２に係る不正メール判定装置１

０の動作を説明する。

実施の形態２に係る不正メール判定装置１０の動作は、実施の形態２に係る不正メール判定方法に相当する。また、実施の形態２に係る不正メール判定装置１０の動作は、実施の形態２に係る不正メール判定プログラムの処理に相当する。

[0089] 図１９を参照して、実施の形態２に係る意図学習部２４５の処理を説明する。

（ステップＳ９１：第１パラグラフ抽出処理）

意図学習部２４５は、学習用メール２４７に含まれるメールデータから全てのパラグラフを抽出する。学習用メール２４７は、各パラグラフに機能語を示すラベルが付された複数のメールの本文のデータが登録されている。

[0090] （ステップＳ９２：第４特徴抽出処理）

意図学習部２４５は、図１０のステップＳ４２と同じ方法により、ステップＳ９１で抽出された各パラグラフから特徴を抽出する。

[0091] （ステップＳ９３：学習処理）

意図学習部２４５は、図１０のステップＳ４５と同様に、ステップＳ９２で各パラグラフから抽出された特徴と、各パラグラフに付されたラベルとに基づき、教師有学習を行う。これにより、特徴がどのラベルに対応するかを識別する識別器が生成される。つまり、特徴がどの機能語に対応するかを識別する識別器が生成される。

[0092] 図２０を参照して、実施の形態２に係る意図推定部２４６の処理を説明する。

（ステップＳ１０１：第５本文抽出処理）

意図推定部２４６は、対象メールから本文を抽出する。

[0093] （ステップＳ１０２：第２パラグラフ抽出処理）

意図推定部２４６は、ステップＳ１０１で抽出された本文からパラグラフを抽出する。

[0094] （ステップＳ１０３：第５特徴抽出処理）

意図推定部２４６は、図１０のステップＳ４２と同じ方法により、ステップＳ１０２で抽出された各パラグラフから特徴を抽出する。

[0095] （ステップＳ１０４：第３識別処理）

意図推定部２４６は、各パラグラフを対象として、ステップＳ９３で生成された識別器と、ステップＳ１０３で対象のパラグラフから抽出された特徴とに基づき、対象のパラグラフが各機能語に対応する識別スコアを計算する。

[0096] （ステップＳ１０５：識別スコア判定処理）

意図推定部２４６は、ステップＳ１０４で計算された識別スコアが第３閾値以上の機能語が含まれているか否かを判定する。

識別スコアが第３閾値以上の機能語が含まれている場合には、識別スコアが第３閾値以上の機能語をリストとして生成する。一方、識別スコアが第３閾値以上の機能語が含まれていない場合には、対象メールを不正なメールでないと判定し、処理を終了する。

ここで、単に各パラグラフが対応すると識別された機能語をリスト化するのではなく、識別スコアが第３閾値以上の機能語をリスト化する。これにより、パラグラフが対応する可能性が一定レベル以上ある機能語だけがリスト化される。

[0097] ＊＊＊実施の形態２の効果＊＊＊

実施の形態１では、意図特定部２４１は、事前に登録された機能語に類似する単語を抽出することにより、対象メールの意図を特定した。この場合、機能語に類似する単語が本文で意図せずに使用されていると、意図が誤検出されてしまう。

これに対して、実施の形態２に係る不正メール判定装置１０は、メールの本文全体から意図を特定する。そのため、機能語に類似する単語が本文で意図せずに使用されていても、適切に意図を特定することが可能である。

符号の説明

[0098] １０　不正メール判定装置、１１　プロセッサ、１２　メモリ、１３　ス

トレージ、１４　通信インタフェース、１５　電子回路、２１　初期フィルタ部、２１１　送信元抽出部、２１２　ブラックリスト判定部、２１３　コンテンツ判定部、２１４　差異判定部、２１５　既知判定部、２１６　ブラックリスト、２２　未知解析部、２２１　宛名判定部、２２２　身元判定部、２２３　名刺判定部、２２４　公開情報判定部、２２５　人名辞書データ、２２６　定型文データ、２２７　受信者プロファイル、２３　既知解析部、２３１　本人性判定部、２３２　トピック判定部、２３３　プロファイル生成部、２３４　一致判定部、２３５　差出人プロファイル、２４　一貫性解析部、２４１　意図特定部、２４２　ルール適用部、２４３　メール判定部、２４４　一貫性判定ルール、２４５　意図学習部、２４６　意図推定部、２４７　学習用メール、３０　名刺管理システム。

請求の範囲

[請求項1] 新たに受信した受信メールを対象メールとして、前記対象メールの本文から前記対象メールの意図を特定する意図特定部と、

前記対象メールと、前記対象メールと同一の差出人から受信した他の受信メールと、前記意図特定部によって特定された前記対象メールの意図との関係から、前記対象メールが不正なメールであるか否かを判定するメール判定部と

を備える不正メール判定装置。

[請求項2] 前記意図特定部は、前記対象メールの本文から、事前に登録された意図を表す機能語に類似する単語を抽出し、抽出された単語に類似する機能語が示す意図を前記対象メールの意図として特定する

請求項１に記載の不正メール判定装置。

[請求項3] 前記意図特定部は、過去の受信メールから機械学習により得られた識別器に基づき、前記対象メールの本文が各機能語に対応する評価値を計算し、計算された前記評価値が閾値以上の機能語を抽出し、抽出された前記機能語が示す意図を前記対象メールの意図として特定する

請求項１に記載の不正メール判定装置。

[請求項4] 前記メール判定部は、前記意図特定部によって特定された意図に応じた条件と、前記対象メールと、前記他の受信メールとにより、前記対象メールが不正なメールであるか否かを判定する

請求項１から３までのいずれか１項に記載の不正メール判定装置。

[請求項5] 前記不正メール判定装置は、さらに、

前記対象メールのトピックが前記他の受信メールに含まれるか否か判定するトピック判定部

を備え、

前記メール判定部は、前記対象メールのトピックが前記他の受信メールに含まれると前記トピック判定部によって判定されたトピック一致メールであるかと前記対象メールのトピックが前記他の受信メール

に含まれないと前記トピック判定部によって判定されたトピック不一致メールとであるかとを示すメール種類と、前記意図特定部によって特定された意図とに応じた条件により、前記対象メールが不正なメールであるか否かを判定する

請求項４に記載の不正メール判定装置。

[請求項6] 前記メール種類は、前記対象メールと同一の差出人から受信した他の受信メールがあるか否かを示し、前記対象メールと同一の差出人から受信した他の受信メールがある場合に、前記トピック一致メールであるかと前記トピック不一致メールであるかとを示す

請求項５に記載の不正メール判定装置。

[請求項7] 前記メール種類は、前記対象メールと同一の差出人から受信した他の受信メールがない場合には、名刺を管理する名刺管理システムに前記対象メールの差出人が登録されている名刺存在メールであるかと、前記対象メールの差出人のメールアドレスから特定された情報が前記対象メールの受信者に関連する関連分野メールであるかとを示す

請求項６に記載の不正メール判定装置。

[請求項8] 前記不正メール判定装置は、さらに、

前記対象メールの本文の宛名として前記対象メールの受信者の名前がない場合に、前記対象メールが不正なメールであると判定する宛名判定部

を備える請求項１から７までのいずれか１項に記載の不正メール判定装置。

[請求項9] 前記不正メール判定装置は、さらに、

対象メールの差出人が、本文中で名乗っていない場合に、前記対象メールが不正なメールであると判定する宛名判定部

を備える請求項１から８までのいずれか１項に記載の不正メール判定装置。

[請求項10] 意図特定部が、新たに受信した受信メールを対象メールとして、前

記対象メールの本文から前記対象メールの意図を特定し、

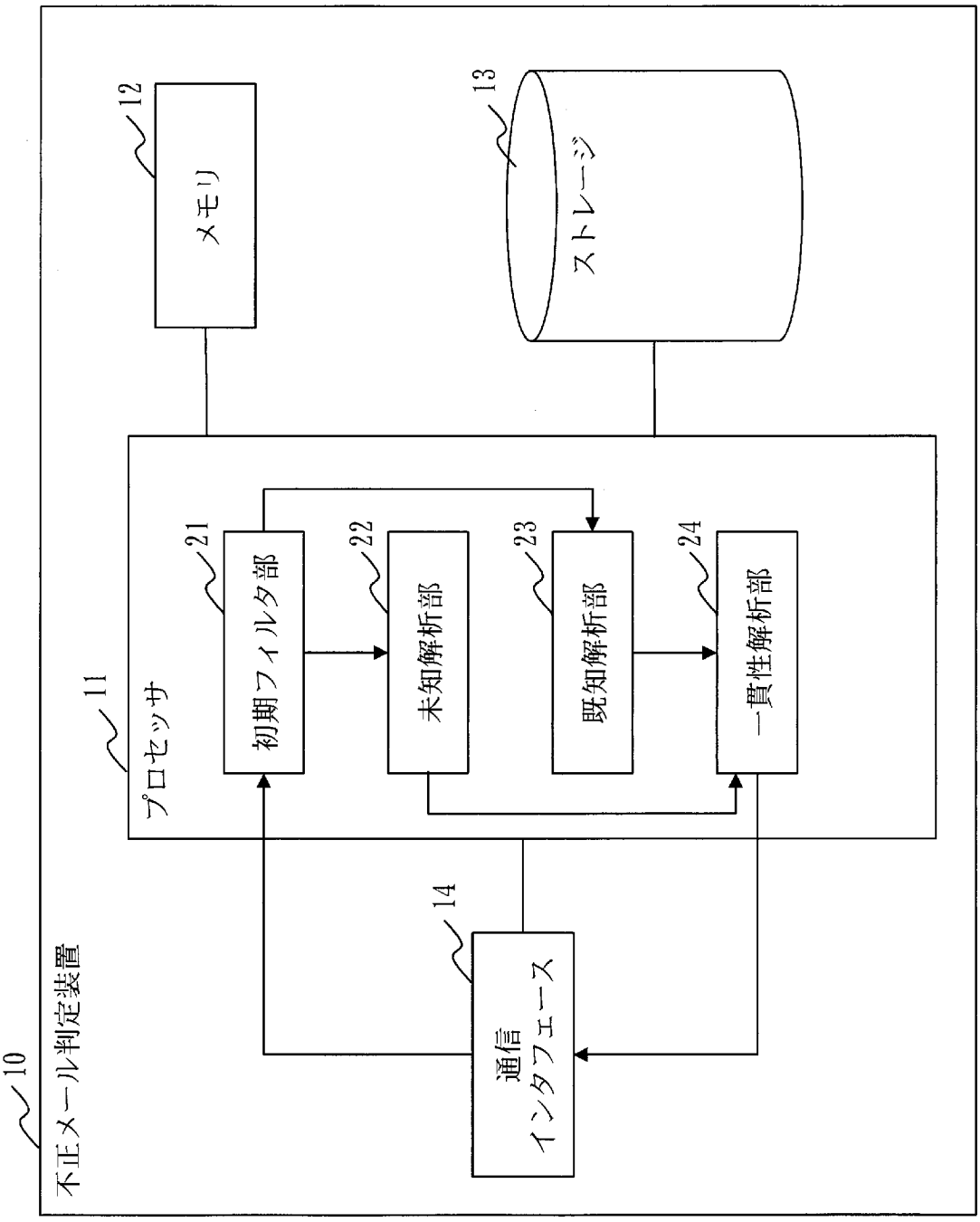
メール判定部が、前記対象メールと、前記対象メールと同一の差出人から受信した他の受信メールと、前記意図特定部によって特定された前記対象メールの意図との関係から、前記対象メールが不正なメールであるか否かを判定する不正メール判定方法。

[請求項11] 新たに受信した受信メールを対象メールとして、前記対象メールの本文から前記対象メールの意図を特定する意図特定処理と、

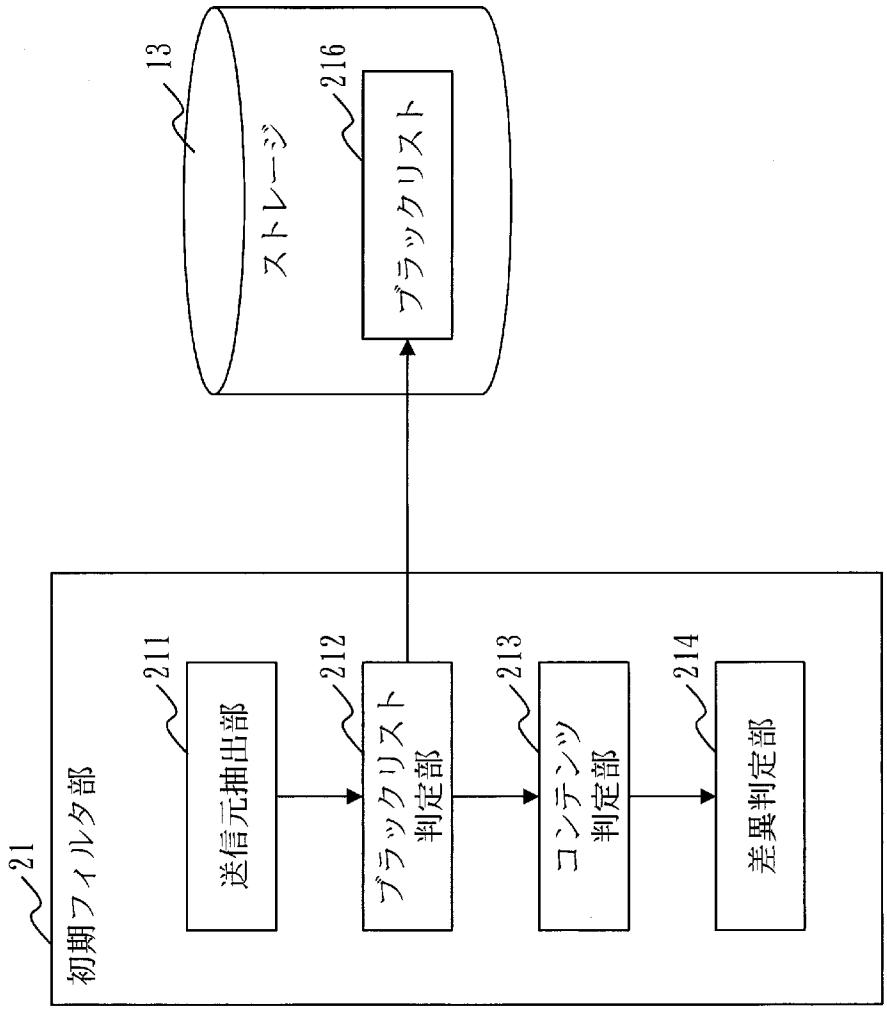
前記対象メールと、前記対象メールと同一の差出人から受信した他の受信メールと、前記意図特定処理によって特定された前記対象メールの意図との関係から、前記対象メールが不正なメールであるか否かを判定するメール判定処理と

をコンピュータに実行させる不正メール判定プログラム。

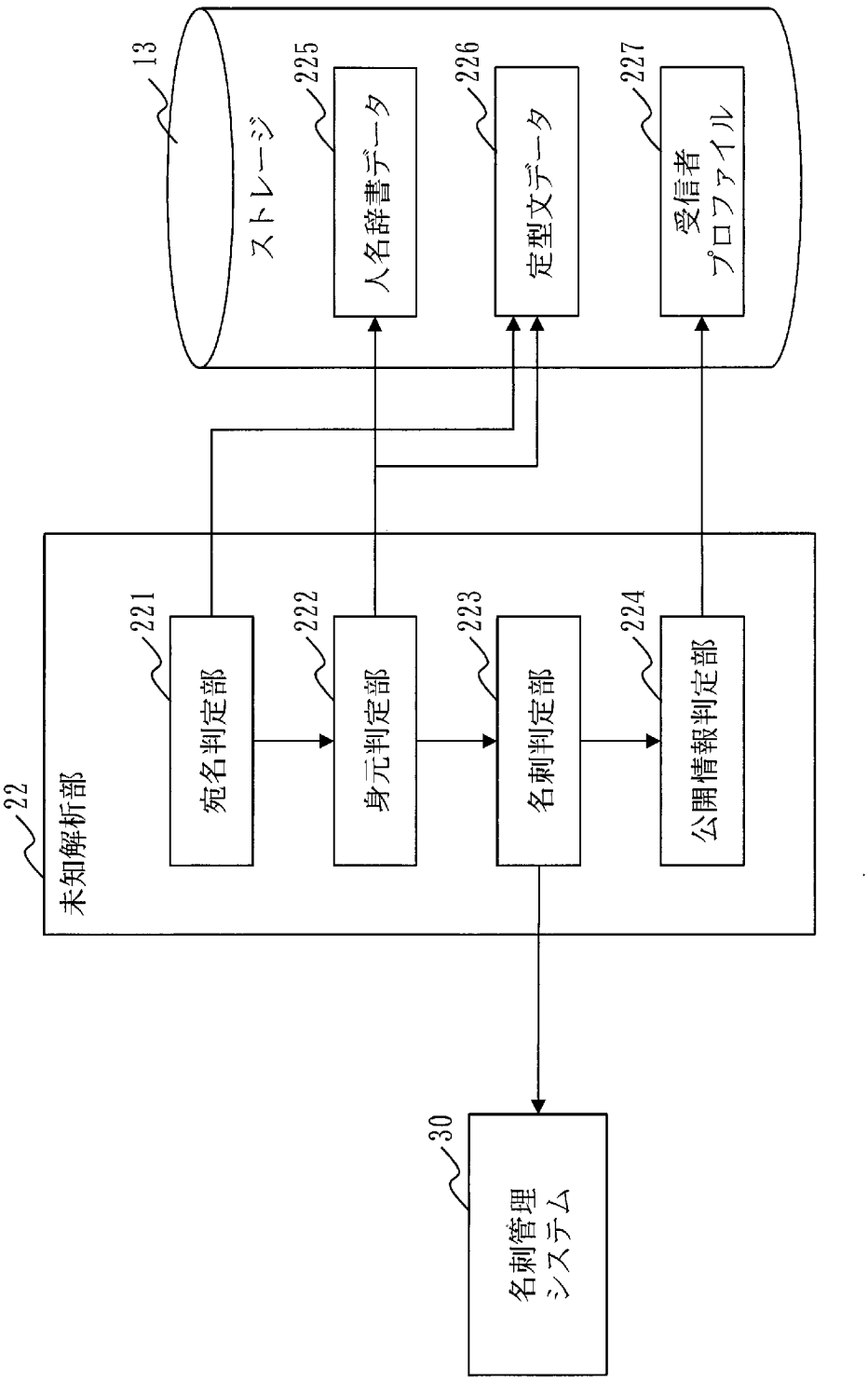
[図1]


10
不正メール判定装置
11
プロセッサ
12
メモリ
13
ストレージ
14
通信
インタフェース
21
初期フィルタ部
22
未知解析部
23
既知解析部
24
一貫性解析部

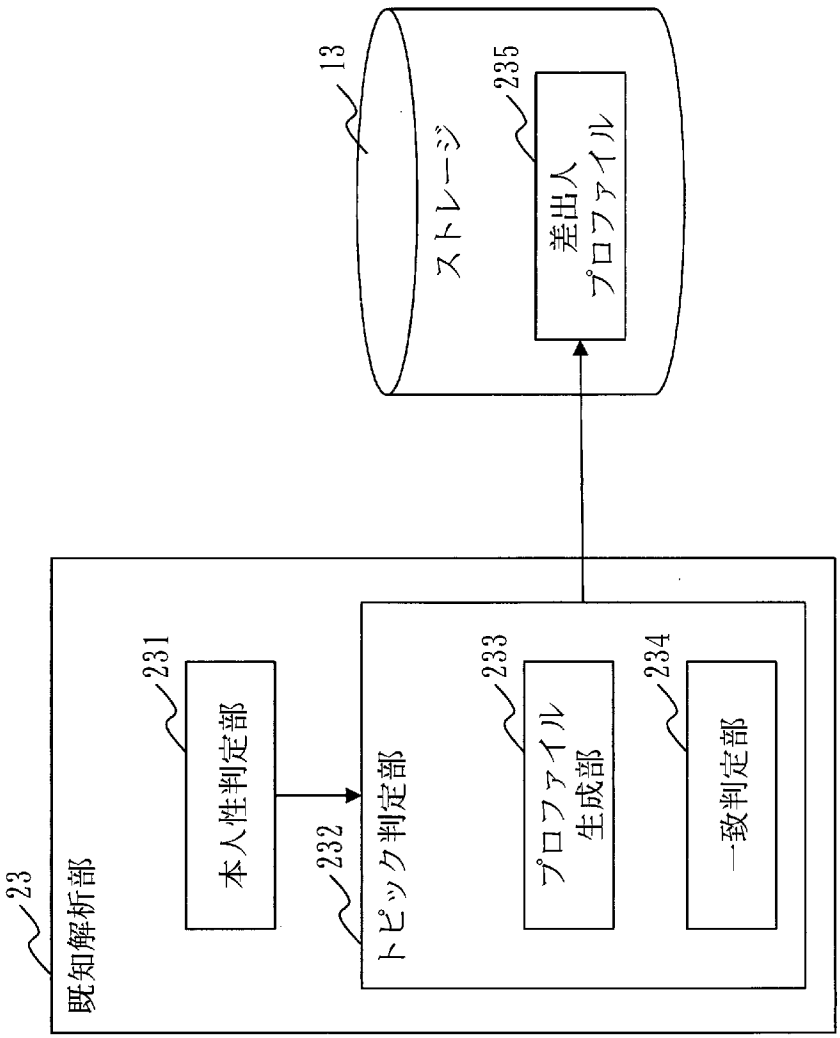
[図2]


13
ストレージ
216
ブラックリスト
21
初期フィルタ部
211
送信元抽出部
212
ブラックリスト判定部
213
コンテンツ判定部
214
差異判定部

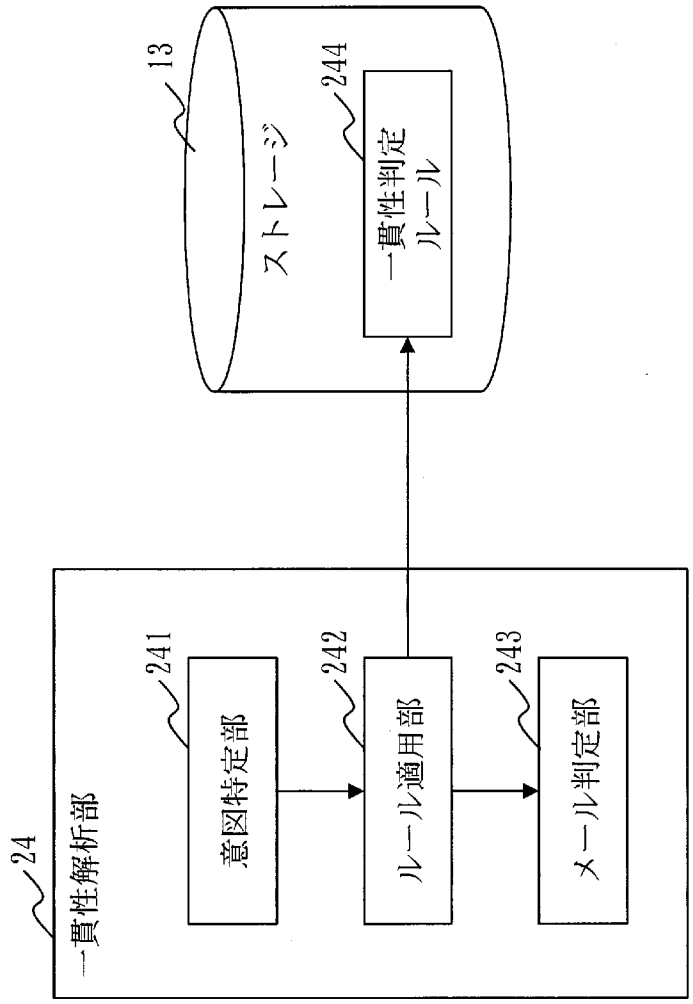
[図3]


13
ストレージ
225
人名辞書データ
226
定型文データ
227
受信者
プロファイル
22
未知解析部
221
宛名判定部
222
身元判定部
223
名刺判定部
224
公開情報判定部
30
名刺管理
システム

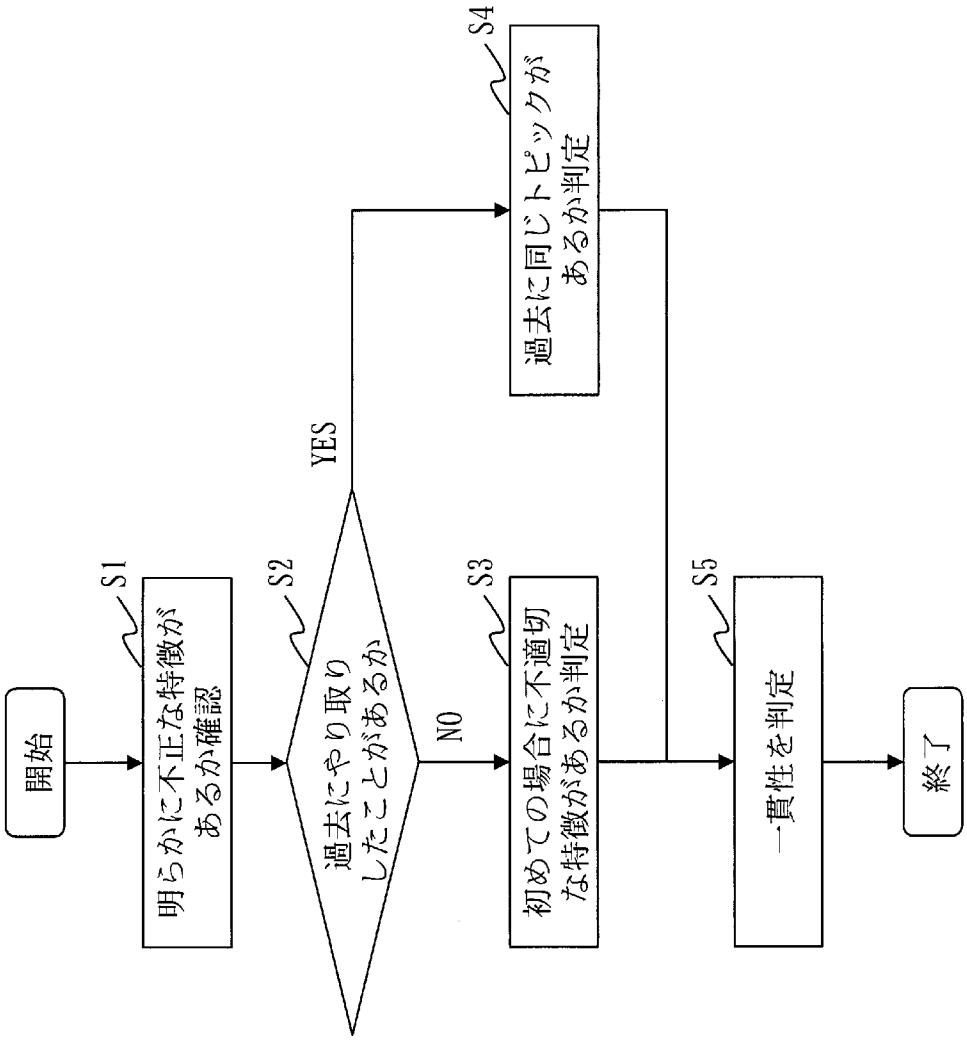
[図4]


13
ストレージ
235
差出人
プロファイル
23
既知解析部
231
本人性判定部
232
トピック判定部
233
プロファイル
生成部
234
一致判定部

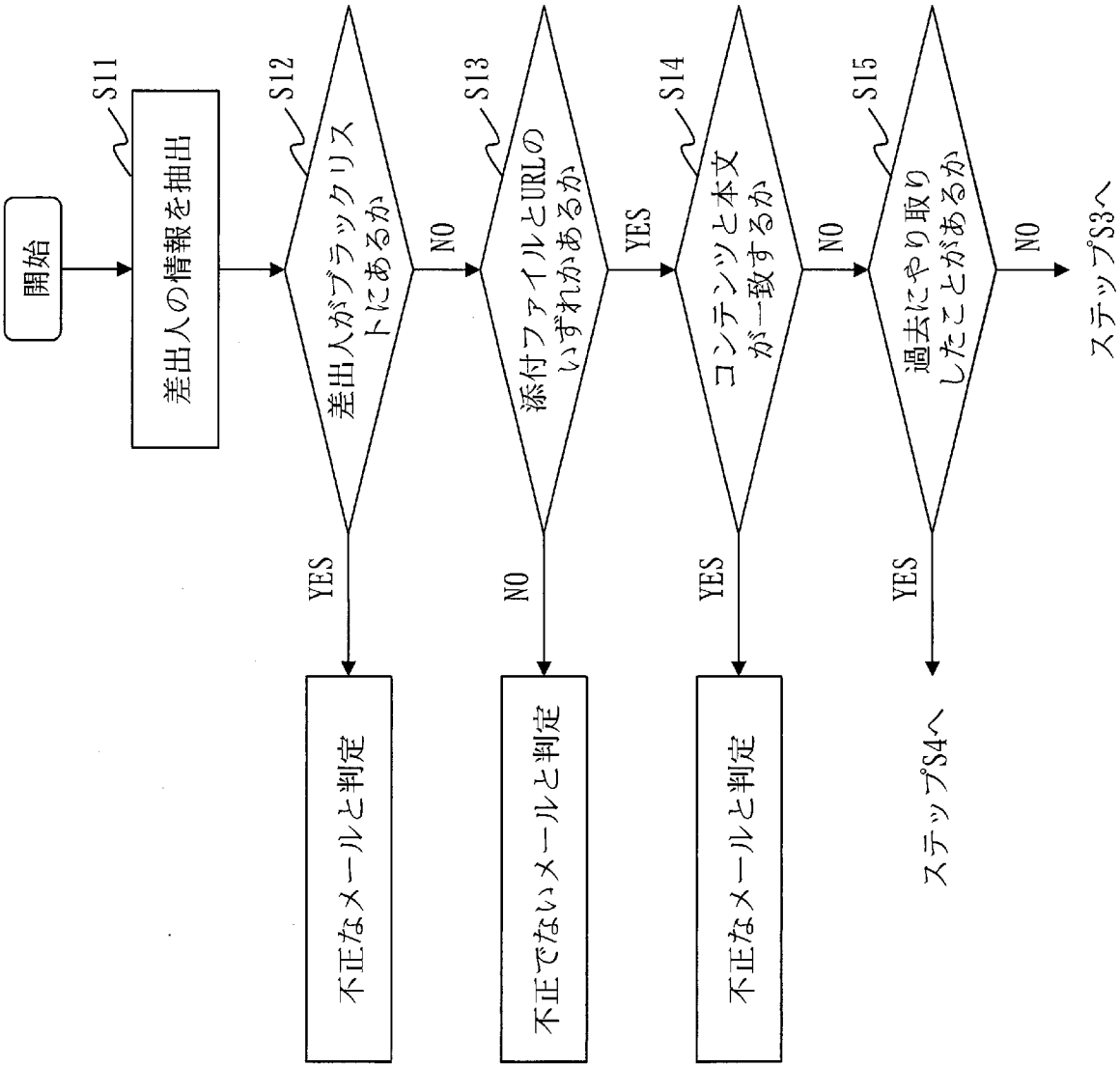
[図5]


13
ストレージ
244
一貫性判定
ルール
24
一貫性解析部
241
意図特定部
242
ルール適用部
243
メール判定部

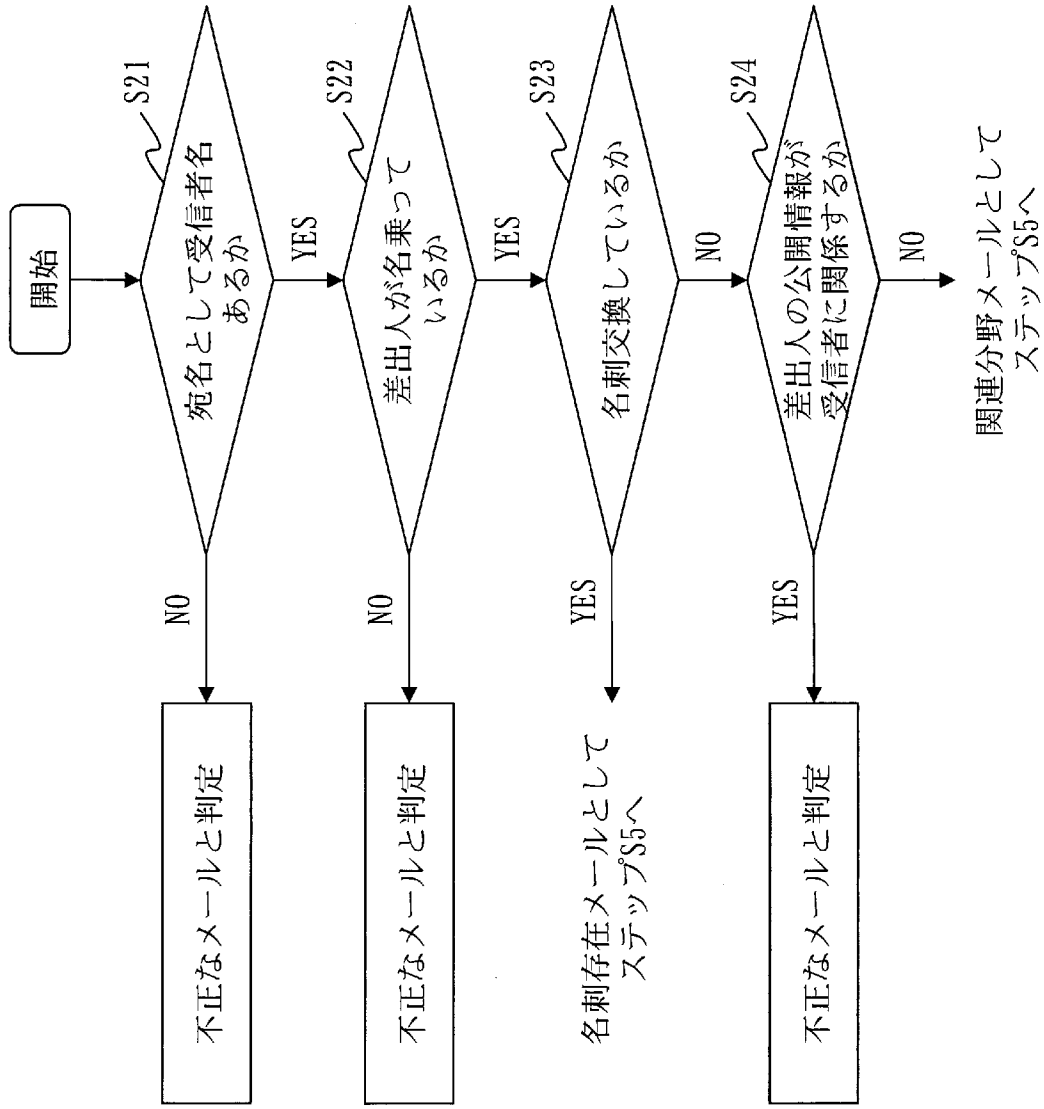
[図6]


開始
S1
明らかに不正な特徴があるか確認
S2
過去にやり取りしたことがあるか
YES
NO
S3
初めての場合に不適切な特徴があるか判定
S4
過去に同じトピックがあるか判定
S5
一貫性を判定
終了

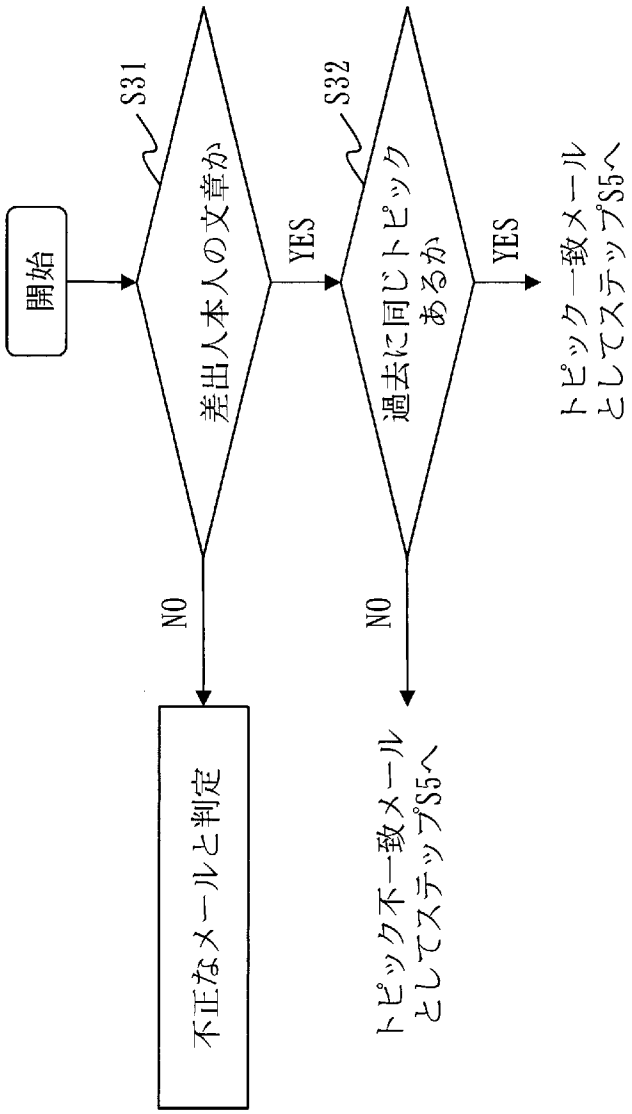
[図7]


開始
S11
差出人の情報を抽出
S12
差出人がブラックリストにあるか
YES
不正なメールと判定
NO
S13
添付ファイルとURLのいずれかあるか
NO
不正でないメールと判定
YES
S14
コンテンツと本文が一致するか
YES
不正なメールと判定
NO
S15
過去にやり取りしたことがあるか
YES
ステップS4へ
NO
ステップS3へ

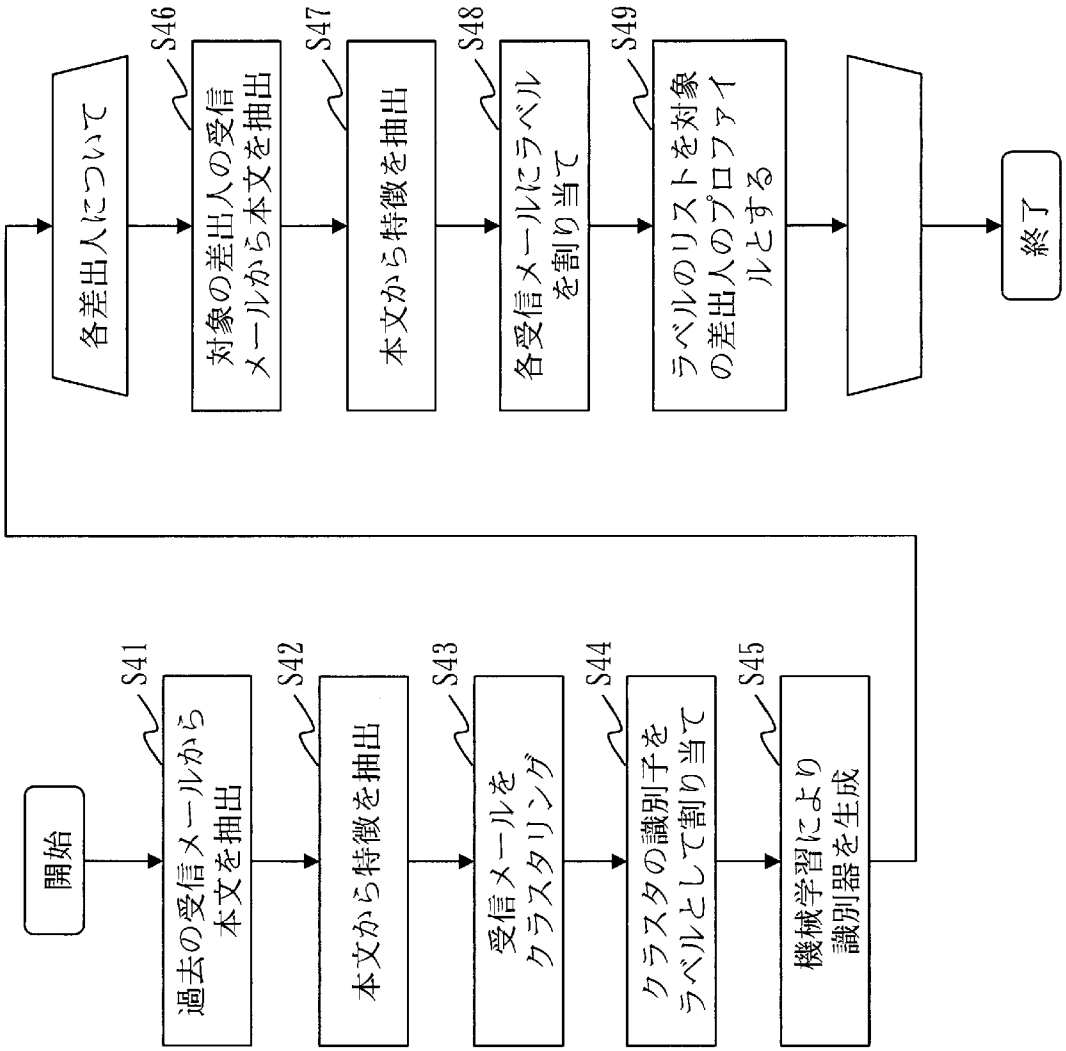
[図8]


開始
S21
宛名として受信者名あるか
YES
S22
差出人が名乗っているか
YES
S23
名刺交換しているか
NO
S24
差出人の公開情報が受信者に関係するか
NO
関連分野メールとしてステップS5へ
NO
不正なメールと判定
NO
不正なメールと判定
YES
名刺存在メールとしてステップS5へ
YES
不正なメールと判定

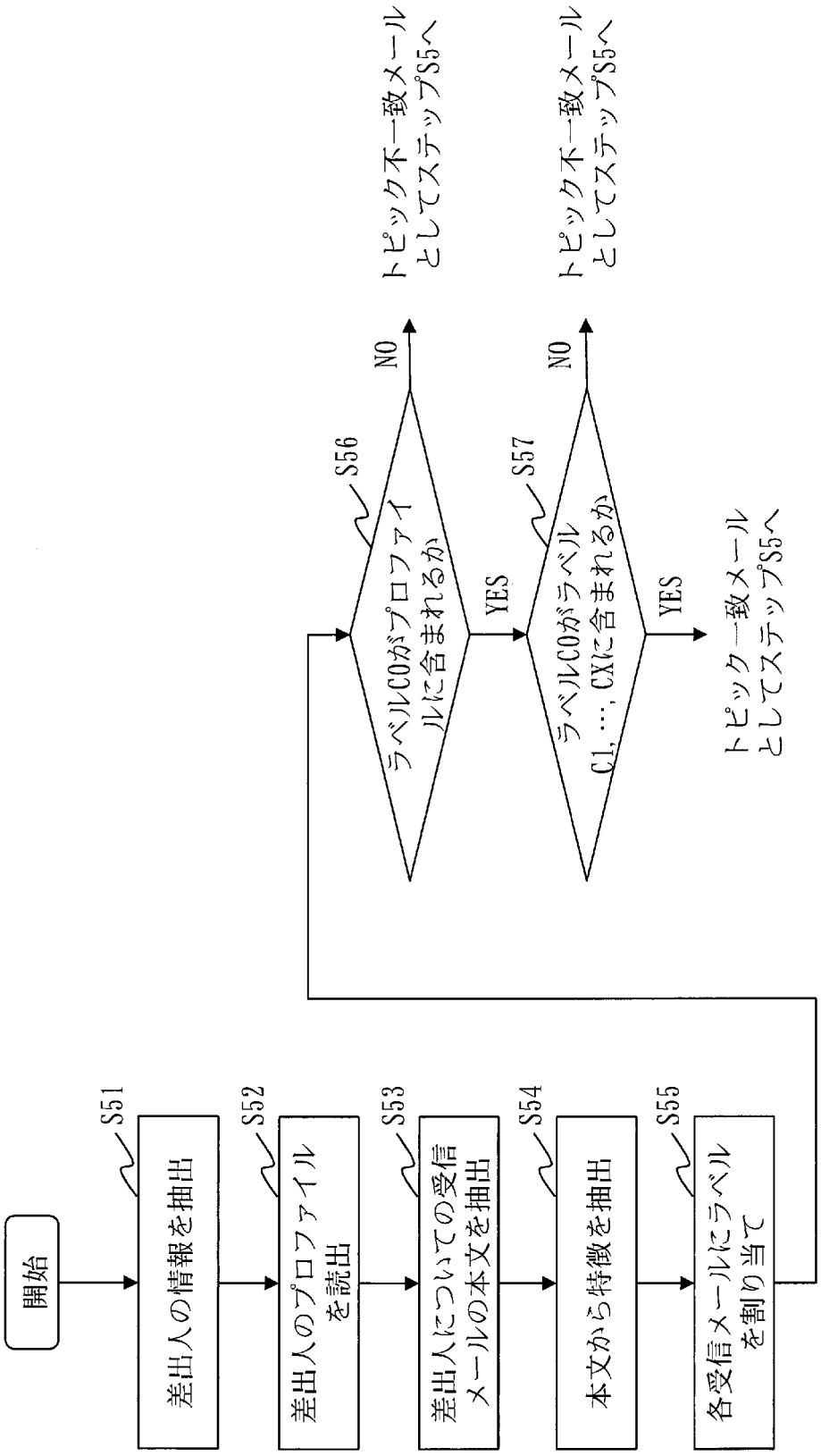
[図9]


開始
S31
差出人本人の文章か
YES
S32
過去に同じトピック
あるか
YES
トピック一致メール
としてステップS5へ
NO
不正なメールと判定
NO
トピック不一致メール
としてステップS5へ

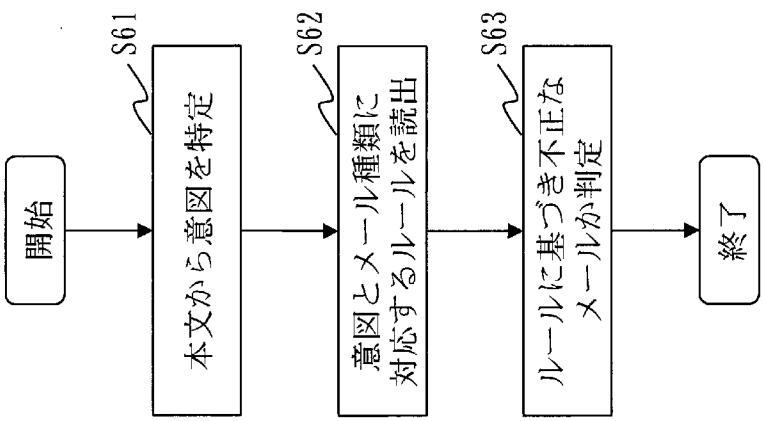
[図10]


開始
S41
過去の受信メールから本文を抽出
S42
本文から特徴を抽出
S43
受信メールをクラスタリング
S44
クラスタの識別子をラベルとして割り当て
S45
機械学習により識別器を生成
各差出人について
S46
対象の差出人の受信メールから本文を抽出
S47
本文から特徴を抽出
S48
各受信メールにラベルを割り当て
S49
ラベルのリストを対象の差出人のプロファイルとする
終了

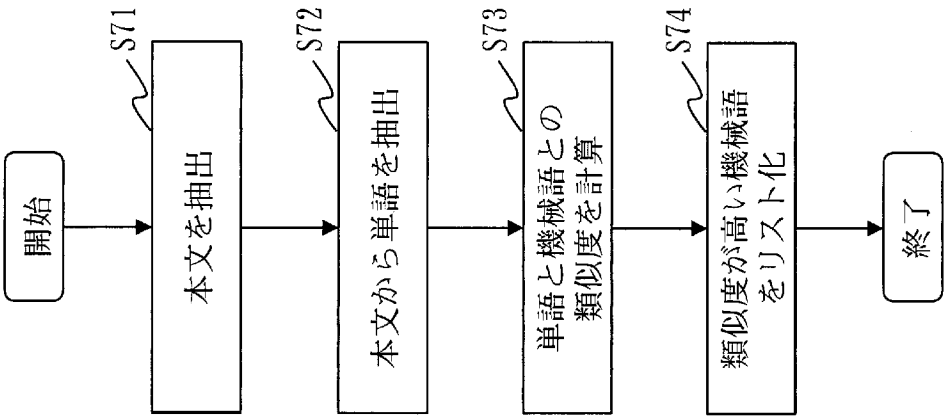
[図11]


開始
S51
差出人の情報を抽出
S52
差出人のプロファイルを読出
S53
差出人についての受信メールの本文を抽出
S54
本文から特徴を抽出
S55
各受信メールにラベルを割り当て
S56
ラベルCOがプロファイルに含まれるか
NO
トピック不一致メールとしてステップS5へ
YES
S57
ラベルCOがラベルC1, …, CXに含まれるか
NO
トピック不一致メールとしてステップS5へ
YES
トピック一致メールとしてステップS5へ

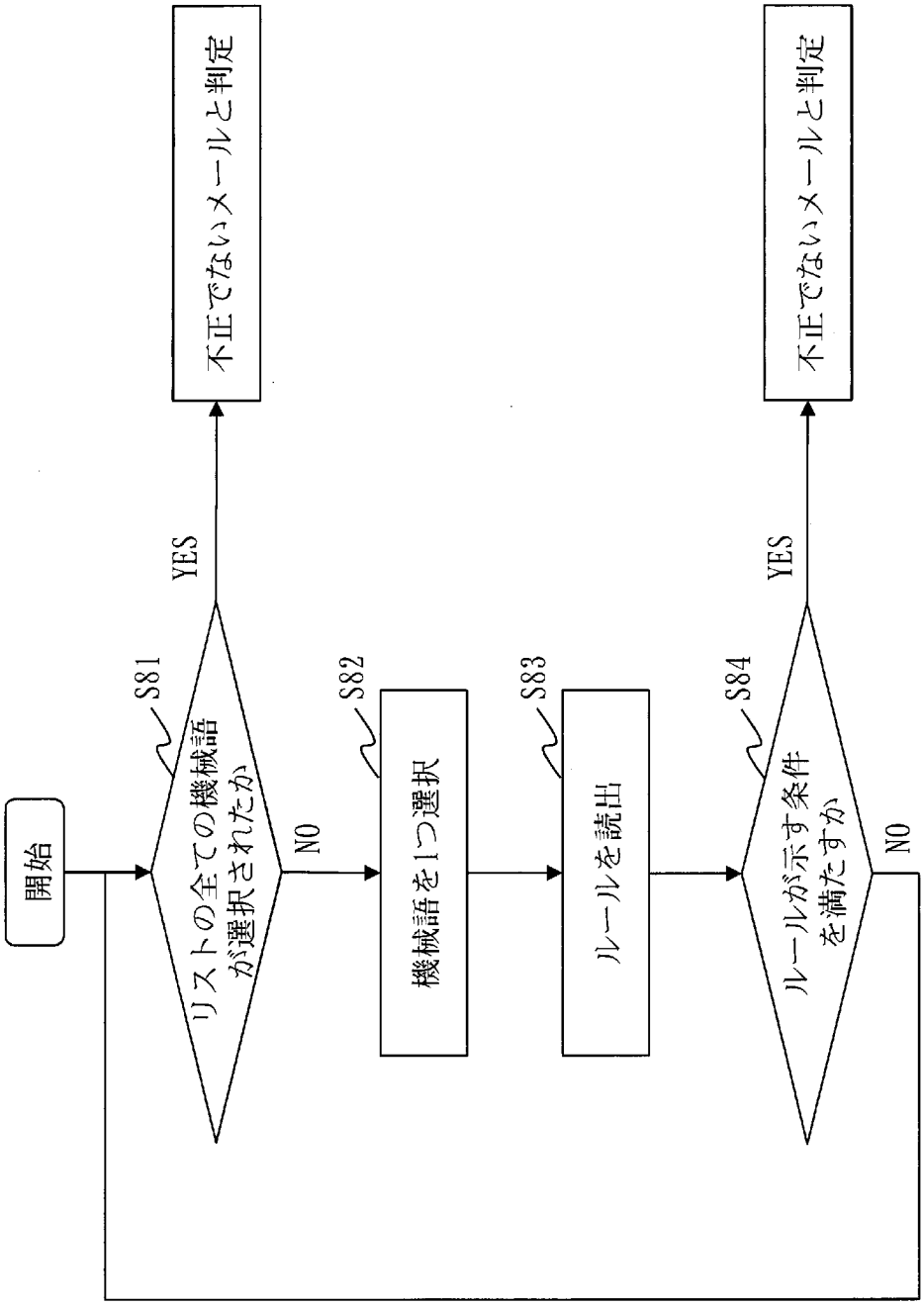
[図12]


開始
S61
本文から意図を特定
S62
意図とメール種類に対応するルールを読出
S63
ルールに基づき不正なメールか判定
終了

[図13]


開始
S71
本文を抽出
S72
本文から単語を抽出
S73
単語と機械語との類似度を計算
S74
類似度が高い機械語をリスト化
終了

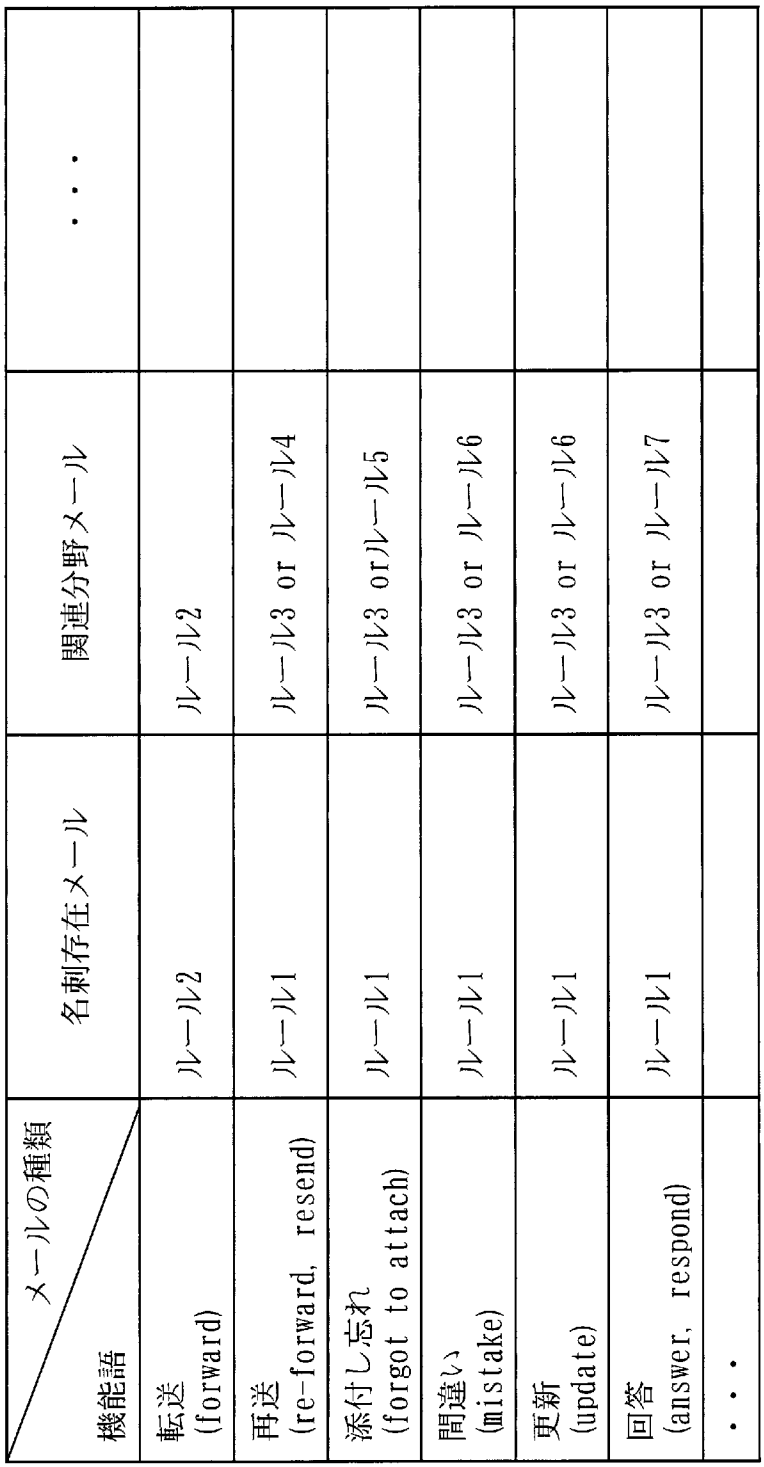
[図14]


開始
S81
リストの全ての機械語が選択されたか
YES
不正でないメールと判定
NO
S82
機械語を1つ選択
S83
ルールを読出
S84
ルールが示す条件を満たすか
YES
不正でないメールと判定
NO

[図15]

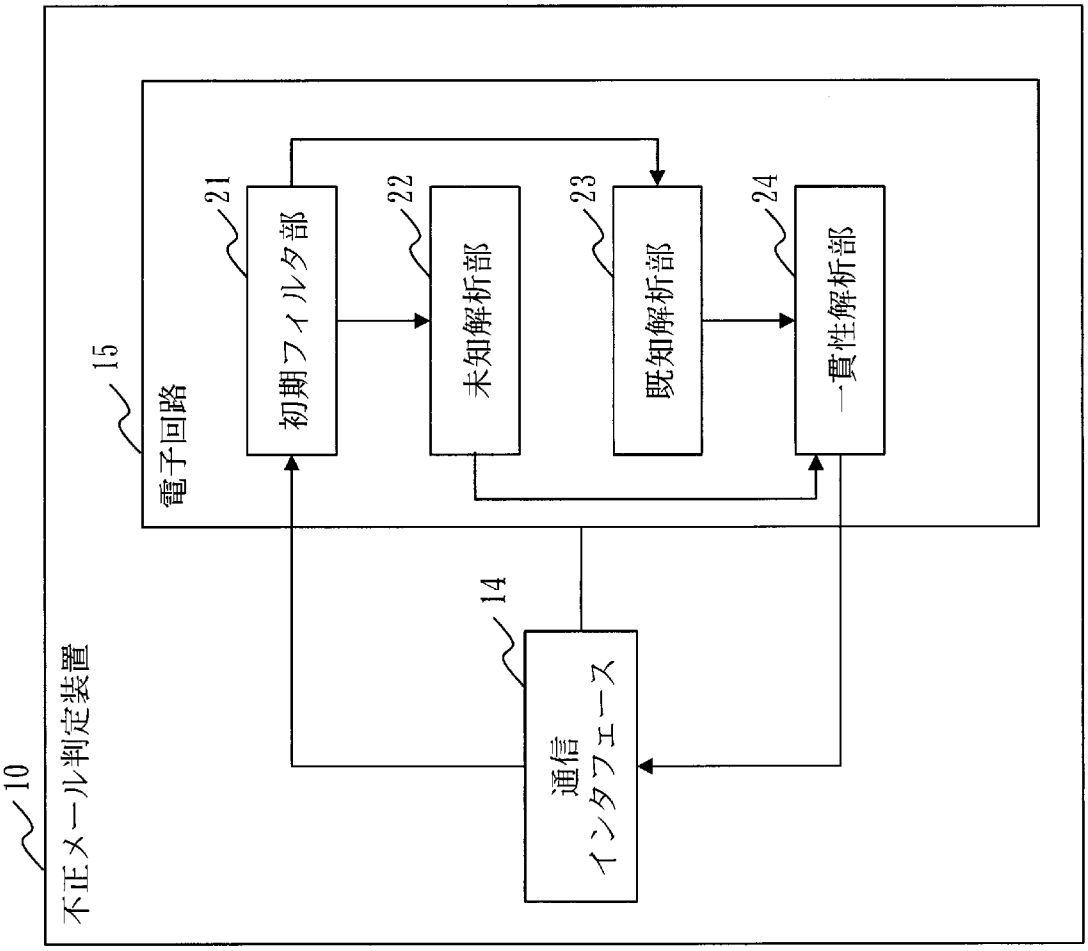
ルール	内容
ルール1	対象メールの本文に機能語が含まれている
ルール2	対象メールの添付ファイル及びURLのコンテンツがやりとりしたことのないトピック
ルール3	同じ差出人から直前に同じメールが送られていない
ルール4	同じ差出人から直前に送られた同じメールに違う添付ファイルがついている
ルール5	同じ差出人から直前に送られたメールに添付ファイルがついている
ルール6	同じ差出人から直前に送られた同じメールに同じ添付ファイルがついている
ルール7	直前に差出人に質問をしている

[図16]

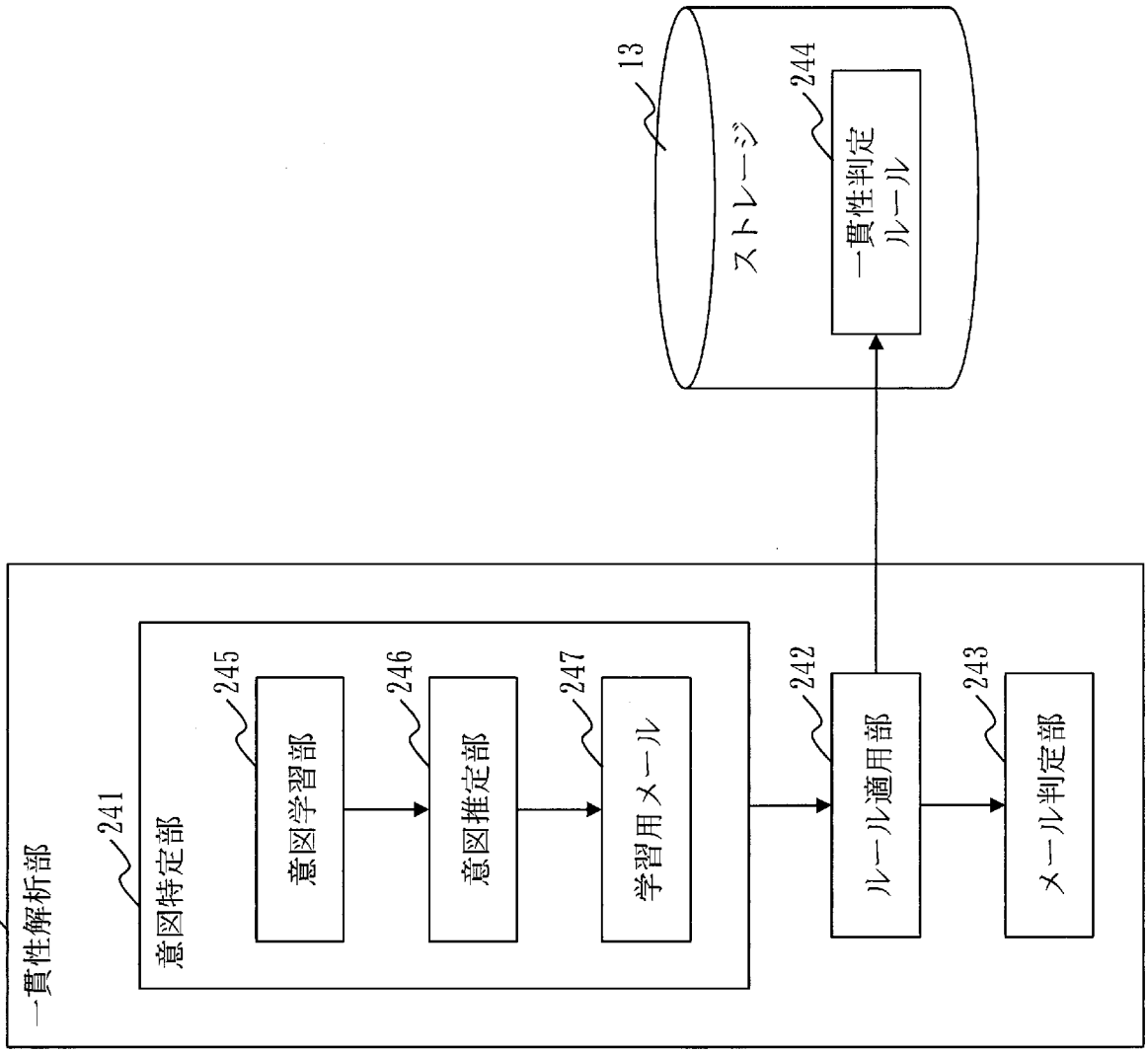


メールの種類 / 機能語	名刺存在メール	関連分野メール	・・・
転送 (forward)	ルール2	ルール2	
再送 (re-forward, resend)	ルール1	ルール3 or ルール4	
添付し忘れ (forgot to attach)	ルール1	ルール3 orルール5	
間違い (mistake)	ルール1	ルール3 or ルール6	
更新 (update)	ルール1	ルール3 or ルール6	
回答 (answer, respond)	ルール1	ルール3 or ルール7	
・・・			

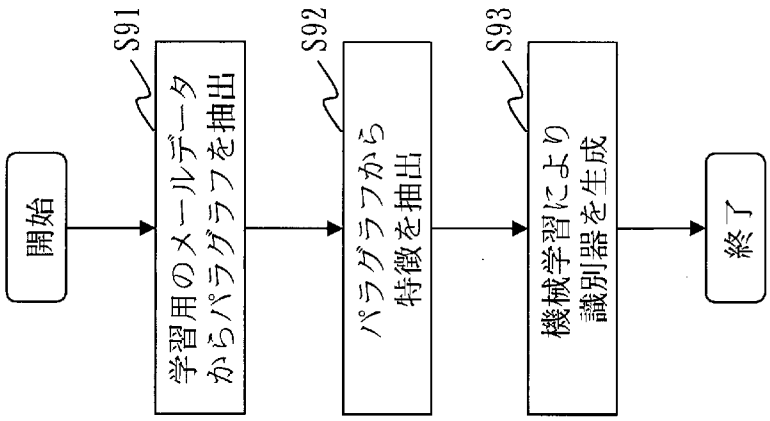
[図17]


10
不正メール判定装置
15
電子回路
21
初期フィルタ部
22
未知解析部
23
既知解析部
24
一貫性解析部
14
通信
インタフェース

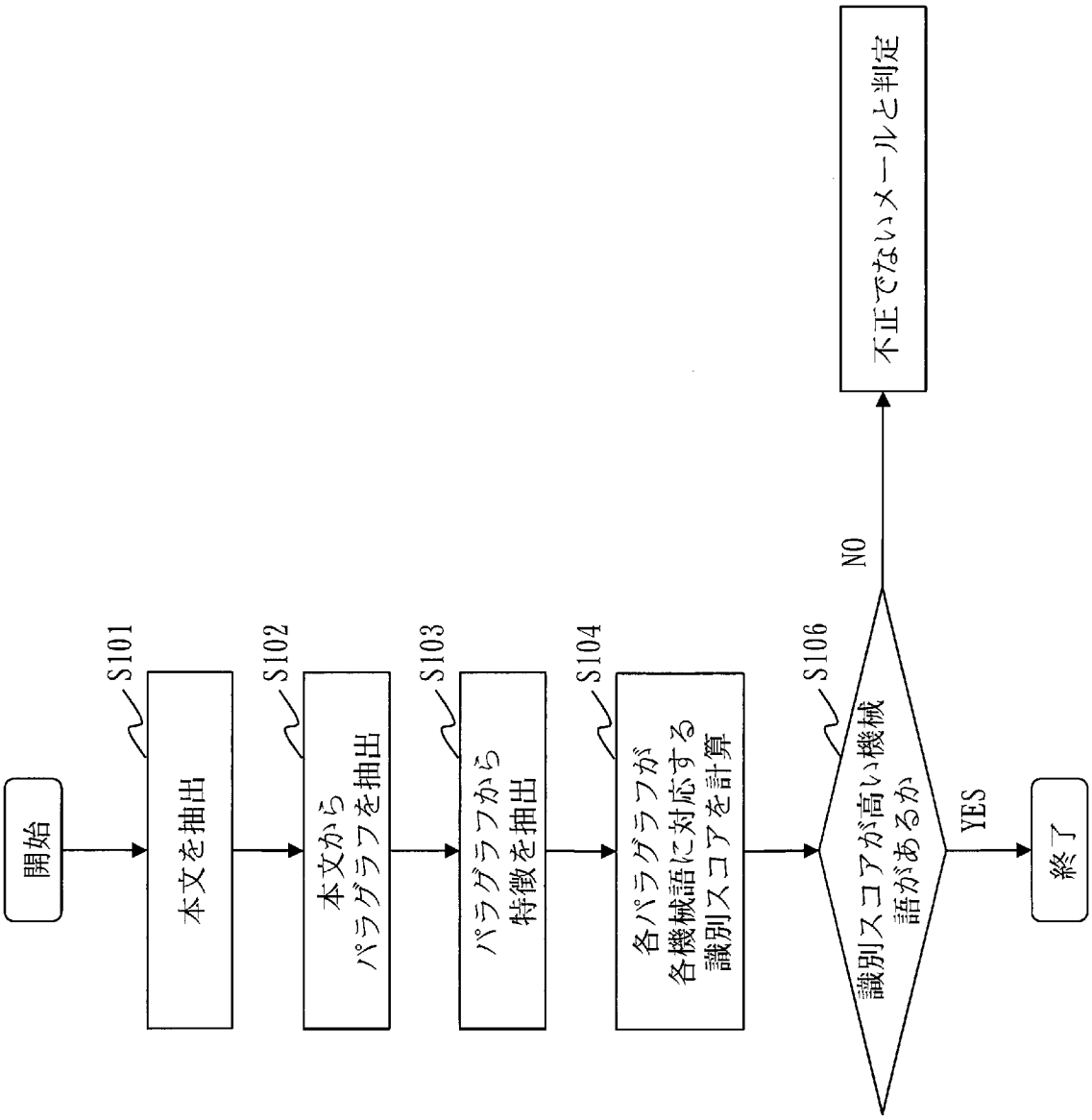
[図18]


13
ストレージ
244
一貫性判定
ルール
24
一貫性解析部
241
意図特定部
245
意図学習部
246
意図推定部
247
学習用メール
242
ルール適用部
243
メール判定部

[図19]


開始
S91
学習用のメールデータ
からパラグラフを抽出
S92
パラグラフから
特徴を抽出
S93
機械学習により
識別器を生成
終了

[図20]


開始
S101
本文を抽出
S102
本文から
パラグラフを抽出
S103
パラグラフから
特徴を抽出
S104
各パラグラフが
各機械語に対応する
識別スコアを計算
S106
識別スコアが高い機械
語があるか
NO
不正でないメールと判定
YES
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/019656

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. 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)
Int. Cl. G06F13/00

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.
A	JP 2017-126283 A (FUJITSU LTD.) 20 July 2017, paragraphs [0021]-[0034] & US 2017/0208080 A1, paragraphs [0034]-[0048]	1-11
A	JP 2013-236308 A (FUJITSU LTD.) 21 November 2013, paragraphs [0070]-[0090] (Family: none)	1-11
A	US 2013/0325991 A1 (CHAMBERS, Charles Wade) 05 December 2013, paragraphs [0009]-[0018] (Family: none)	1-11

☐ 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
29.06.2018	10.07.2018
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／ＪＰ２０１８／０１９６５６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　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.　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	１９７１－２０１８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
A	JP 2017-126283 A (富士通株式会社) 2017.07.20, 段落[0021]-[0034] & US 2017/0208080 A1, 段落[0034]-[0048]	1-11
A	JP 2013-236308 A (富士通株式会社) 2013.11.21, 段落[0070]-[0090] (ファミリーなし)	1-11
A	US 2013/0325991 A1 (CHAMBERS, Charles Wade) 2013.12.05, 段落[0009]-[0018] (ファミリーなし)	1-11

☐　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
２９．０６．２０１８	１０．０７．２０１８

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）　５Ｘ　３６５０
北川　純次
電話番号　０３－３５８１－１１０１　内線　３５９６