(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4月4日(04.04.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/064458 A1

(51) 国際特許分類:
G06F 21/57 (2013.01)

(21) 国際出願番号： PCT/JP2017/035309

(22) 国際出願日： 2017年9月28日(28.09.2017)

(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: 株式会社オプティム (**OPTIM CORPORATION**) [JP/JP]; 〒8400047 佐賀県佐賀市与賀町４番１８号 Saga (JP).

(72) 発明者: 菅谷 俊二(**SUGAYA Shunji**); 〒1050022 東京都港区海岸１丁目２番２０号 汐留ビルディング ２１階 株式会社オプティム内 Tokyo (JP).

(74) 代理人: 小木 智彦(**KOGI Tomohiko**); 〒8800804 宮崎県宮崎市宮田町１１－２４ 黒木ビル１Ｆ Miyazaki (JP).

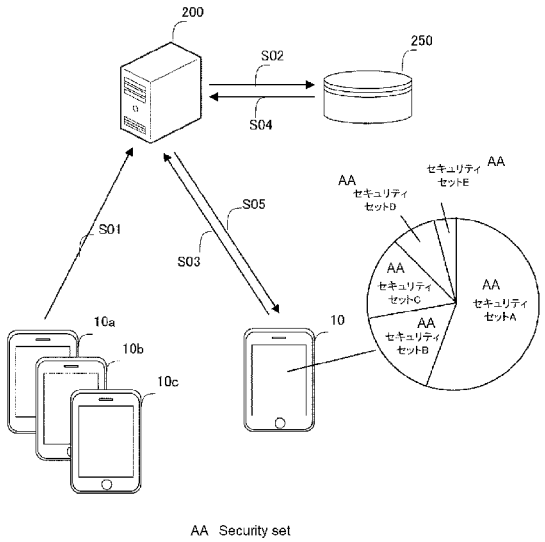
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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,

WO 2019/064458 A1

(54) **Title:** COMPUTER SYSTEM, SECURITY SETTING SUGGESTION METHOD, AND PROGRAM

(54) 発明の名称： コンピュータシステム、セキュリティ設定提案方法及びプログラム

[図1]



(57) **Abstract:** [Problem] To provide: a computer system which suggests an appropriate security set to a user, on the basis of user information and statistical information related to collected statistical security parameters; a security setting suggestion method; and a program. [Solution] This computer system, which is connected to at least one user terminal 10 so as to be capable of communicating therewith, and which is provided with a security statistics database 250, acquires, from the user terminal 10, a suggestion request for a security set, and user information including at least attributes, uses

[続葉有]

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))

the suggestion request and the acquired user information to extract, from the security set statistics database 250, a security set associated with user information which is identical to the aforementioned user information, or similar to said user information to a prescribed extent, and presents, to the user terminal 10, at least one extracted security set as a suggested security set.

(57) 要約:【課題】ユーザ情報とともに収集した統計的なセキュリティパラメータの統計情報から、あるユーザに対して適切なセキュリティセットを提案するコンピュータシステム、セキュリティ設定提案方法及びプログラムを提供することを目的とする。【解決手段】一以上のユーザ端末１０と通信可能に接続され、セキュリティ統計データベース２５０を備えたコンピュータシステムは、ユーザ端末１０から、少なくとも属性を含むユーザ情報とともに、セキュリティセットの提案要求を取得し、この提案要求とともに取得したユーザ情報を用いて、セキュリティセット統計データベース２５０から、ユーザ情報と同一、又は所定の範囲でユーザ情報と類似するユーザ情報に関連付けられているセキュリティセットを抽出し、抽出した一以上のセキュリティセットを提案セキュリティセットとして、ユーザ端末１０に提供する。

明　細　書

発明の名称 ：

コンピュータシステム、セキュリティ設定提案方法及びプログラム

技術分野

[0001] 本発明は、ユーザ情報に対して適切なセキュリティセットを提案するコンピュータシステム、セキュリティ設定提案方法及びプログラムに関する。

背景技術

[0002] 近年、公衆回線網に接続された携帯端末をＷｅｂサーバ等と接続することで、ユーザに様々なサービスが提供されている。特に、スマートフォン（高機能携帯電話）の登場により、従来、パソコンに対して行われていた高度なサービスを、携帯電話で行うことが可能になってきた。

[0003] しかしながら、ユーザ端末の普及に伴い、インターネットに精通していなかったりするユーザが、個人の端末により、業務に関する情報を扱う事例が増えてきている。そうしたユーザによるインターネットへの無制限なアクセスを許可した結果、有害なコンテンツが提供されてしまったり、情報の漏洩が発生してしまったりすることがあった。

[0004] したがって、こうしたユーザ端末には、利用するユーザに応じて適切なセキュリティを設定することで、利便性を可能な限り損なわずに、危険を回避する必要がある。

[0005] このような課題に対して、協調フィルタリングを用いて、有害情報を自動的にフィルタリングする手法が開示されている。

先行技術文献

特許文献

[0006] 特許文献1：特開２００２－２２２１９３号公報

発明の概要

発明が解決しようとする課題

[0007] 特許文献１において開示される手法では、ブラウザに取り込もうとするイ

ンターネット情報から文字情報を抽出し、入力文ベクトルＱを作成する。そしてあらかじめ登録してある学習情報ベクトル群３０中の学習情報ベクトル各々との類似度又は相関係数を算出し、類似度又は相関係数が高い学習情報ベクトル群を抽出する。そして抽出された学習情報ベクトル群中に含まれる単語のスコアを利用して拡張対象単語を選択し、元の入力文ベクトルに対する拡張入力文ベクトルＱｎｅｗを作成する。そしてこの拡張入力文ベクトルを用いて、取得しようとしているインターネット情報が不適切情報であるか否かを判断し、不適切情報であればその取込みを阻止する。

[0008] しかしながら、この手法は自動的で有効なフィルタリング機能を提供可能ではあるものの、学習情報ベクトル群が同一である限りフィルタリング結果が同一となるため、ユーザの属性に応じてフィルタリングの基準を変更することができない。また、本発明は文字情報に基づくフィルタリングに過ぎないため、ユーザ端末１０が備える電話やＧＰＳ機能、決済機能といった他の機能に有効なセキュリティを設定することもできないという課題がある。

[0009] 本発明は、これらの課題に鑑み、ユーザ情報とともに収集した統計的なセキュリティパラメータの統計情報から、あるユーザに対して適切なセキュリティセットを提案するコンピュータシステム、セキュリティ設定提案方法及びプログラムを提供する事を目的とする。

課題を解決するための手段

[0010] 本発明では、以下のような解決手段を提供する。

[0011] 第１の特徴に係る発明は、一以上のユーザ端末と通信可能に接続され、セキュリティ統計データベースを備えたコンピュータシステムであって、

前記ユーザ端末から、少なくとも属性を含むユーザ情報とともに、セキュリティセットの提案要求を取得する提案要求取得手段と、

前記提案要求とともに取得したユーザ情報を用いて、前記セキュリティセット統計データベースから、当該ユーザ情報と同一、又は所定の範囲で当該ユーザ情報と類似するユーザ情報に関連付けられているセキュリティセットを抽出するセキュリティセット抽出手段と、

前記抽出した一以上のセキュリティセットを提案セキュリティセットとして、前記ユーザ端末に提供する提案セキュリティセット提供手段と、

を備えることを特徴とするコンピュータシステムを提供する。

[0012] 第１の特徴に係る発明によれば、一以上のユーザ端末と通信可能に接続され、セキュリティ統計データベースを備えたコンピュータシステムは、前記ユーザ端末から、少なくとも属性を含むユーザ情報とともに、セキュリティセットの提案要求を取得し、前記提案要求とともに取得したユーザ情報を用いて、前記セキュリティセット統計データベースから、当該ユーザ情報と同一、又は所定の範囲で当該ユーザ情報と類似するユーザ情報に関連付けられているセキュリティセットを抽出し、前記抽出した一以上のセキュリティセットを提案セキュリティセットとして、前記ユーザ端末に提供する。

[0013] 第１の特徴に係る発明は、コンピュータシステムのカテゴリであるが、方法及びプログラムであってもカテゴリに応じた同様の作用、効果を奏する。

発明の効果

[0014] 本発明によれば、ユーザ情報とともに収集した統計的なセキュリティパラメータの統計情報から、あるユーザに対して適切なセキュリティセットを提案するコンピュータシステム、セキュリティ設定提案方法及びプログラムを提供することが可能となる。

図面の簡単な説明

[0015] [図1]図１は、本発明の好適な実施形態であるセキュリティ設定提案システム１の概要図である。

[図2]図２は、セキュリティ設定提案システム１の全体構成図である。

[図3]図３は、ユーザ端末１０、セキュリティ設定提案サーバ２００の機能ブロックと各機能の関係を示す図である。

[図4]図４は、ユーザ端末１０、セキュリティ設定提案サーバ２００が実行するセキュリティ設定提案処理のフローチャート図である。

[図5]図５は、セキュリティ設定の提案を受けたユーザ端末１０の画面の一例である。

[図6]図６は、セキュリティセット統計データベース２５０内のセキュリティセットテーブルの一例である。

[図7]図７は、セキュリティセット統計データベース２５０内のセキュリティセット統計テーブルの一例である。

発明を実施するための形態

[0016] 以下、本発明を実施するための最良の形態について図を参照しながら説明する。なお、これはあくまでも一例であって、本発明の技術的範囲はこれに限られるものではない。

[0017] ［セキュリティ設定提案システム１の概要］

図１は、本発明の好適な実施形態であるセキュリティ設定提案システム１の概要を説明するための図である。この図１に基づいて、セキュリティ設定提案システム１の概要を説明する。

[0018] セキュリティ設定提案システム１において、セキュリティ設定提案サーバ２００は、複数のユーザ端末１０と通信可能となっている。ここでは、今セキュリティ設定の提案を受ける端末をユーザ端末１０、それ以外のユーザ端末１０をユーザ端末１０ａ、ユーザ端末１０ｂ、ユーザ端末１０ｃとして区別する。

[0019] 初めに、ユーザ端末１０ａ、ユーザ端末１０ｂ、ユーザ端末１０ｃは、利用中のセキュリティセットを、ユーザ情報とともにセキュリティ設定提案サーバ２００へ送信する（ステップＳ０１）。ここでセキュリティセットとは、セキュリティ設定として利用されるパラメータの一連の組み合わせであって、例えば、ユーザ端末１０の使用場所制限、インターネット制限、電話制限、利用時間制限といった設定のパラメータの組み合わせである。これらのパラメータは、オン、オフの二値を取るフラグであってもよいし、具体的な値であってもよい。具体的な値とは、例えば、使用を許可する位置情報の範囲や、閲覧を許可しないウェブサイトのドメインや、検索結果を表示させない検索単語や、利用時間制限に係る連続利用時間の数値が挙げられる。

[0020] 次に、セキュリティ設定提案サーバ２００は、受信したセキュリティセッ

トとユーザ情報とを関連付けて、記憶部に備えるセキュリティセット統計データベース２５０に記憶させる（ステップＳ０２）。セキュリティセット統計データベース２５０は、ユーザ情報ごとに利用中のセキュリティセットを統計データとして記憶させるデータベースである。セキュリティ設定提案システム１は、ユーザ端末１０からセキュリティセットとユーザ情報とを受信することにより、セキュリティセットとユーザ情報とを取得する。

[0021] 次に、今回セキュリティセットの提案を受けるユーザ端末１０は、ユーザ情報とともにセキュリティ設定提案サーバ２００に提案要求を送信する（ステップＳ０５）。ここで、ユーザ情報は少なくともユーザの属性を含み、ユーザに適したセキュリティセットを提供する際に有意な統計を取れる変数として扱われる値であればよい。すなわち、個人名や電話番号といったユーザを特定可能な識別子ではなく、職務に関する情報（役職、肩書、利用時間帯、勤続年数）といったデモグラフィー情報を指す。

[0022] そのほか、ユーザ端末１０は、セキュリティセットにおいインターネット制限を有効化するかといったアンケート項目や、利用者のインターネットに関する理解度を計る設問といった所定の質問を行い、その結果を前記ユーザ情報に含めることで、ユーザの要望や理解度に応じたより適切なセキュリティセットの統計を取ることが可能となる。

[0023] セキュリティ設定提案サーバ２００は、提案要求を受信すると、同時に受信したユーザ情報を用いて、統計情報を抽出する（ステップＳ０４）。セキュリティ設定提案システム１は、ユーザ端末１０から提案要求を受信することにより、提案要求を取得する。そしてその結果から提案セキュリティセットを生成し、提案要求を送信したユーザ端末１０に送信する（ステップＳ０５）。セキュリティ設定提案システム１は、セキュリティ設定提案サーバ２００から提案セキュリティセットをユーザ端末１０に送信することにより、提案セキュリティセットを提供する。

[0024] 提案セキュリティセットとして最も単純なのは、図１に示すように複数のセキュリティセットの利用割合の統計情報を、円グラフとしてそのまま送信

することである。ユーザは、グラフとセキュリティセットの詳細を見ながら、適切なセキュリティセットを選ぶことが可能となる。そのほか、初めに最も多いセキュリティセット一件のみを送り、ユーザ端末１０に設定させた後で、ユーザが個別にカスタマイズを行ったり、前記質問項目に対して回答した要望を反映させたりしてもよい。以上が、セキュリティ設定提案システム１の概要である。

[0025] ［セキュリティ設定提案システムのシステム構成］

図２は、セキュリティ設定提案システム１の全体構成図である。セキュリティ設定提案システム１において、複数のユーザ端末１０、セキュリティ設定提案サーバ２００によって構成される。ユーザ端末１０とセキュリティ設定提案サーバ２００は、それぞれ公衆回線網３を介して通信可能に接続されている。ユーザ端末１０同士は、相互に通信可能である必要はない。

[0026] ユーザ端末１０は、ユーザが利用する一般的な情報端末であってよく、後述する機能を備える情報機器や電化製品である。ユーザ端末１０は、例えば、携帯電話、スマートフォン、複合型プリンタ、テレビ、ルータ又はゲートウェイ等のネットワーク機器、コンピュータに加えて、冷蔵庫、洗濯機等の白物家電であってもよいし、電話機、ネットブック端末、スレート端末、電子書籍端末、電子辞書端末、携帯型音楽プレーヤ、携帯型コンテンツ再生・録画プレーヤ等の一般的な情報家電であってよい。

[0027] セキュリティ設定提案サーバ２００は、セキュリティセットの提案を行うサーバであって、記憶部にセキュリティセット統計データベース２５０を備え、後述する機能を備える情報機器や電化製品である。

[0028] ［各機能の説明］

図３は、ユーザ端末１０、セキュリティ設定提案サーバ２００の機能ブロックと各機能の関係を示す図である。

[0029] ユーザ端末１０は、制御部１１として、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ），ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ），ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）等を備え、通信

部１２として、例えば、ＩＥＥＥ８０２．１１に準拠したＷｉＦｉ（Ｗｉｒｅｌｅｓｓ　Ｆｉｄｅｌｉｔｙ対応デバイス又は、第３世代移動通信システム等のＩＭＴ－２０００規格に準拠した無線デバイス等を備える（有線によるＬＡＮ接続であってもよい）。

[0030] さらに、ユーザ端末１０は、入出力部１３として、制御部で制御したデータや画像、音声を出力表示する出力部を備え、かつ、ユーザからの入力を受付けるタッチパネルやキーボード、マウス等の入力部を備える。

[0031] ユーザ端末１０において、制御部１１が所定のプログラムを読み込むことで、通信部１２と協働して、ユーザ情報送信モジュール１４、提案要求送信モジュール１５、提案セキュリティセット受信モジュール１６、提案セキュリティセット設定モジュール１７を実現する。また、ユーザ端末１０において、制御部１１が所定のプログラムを読み込むことで、入出力部１３と協働して、質問実施モジュール１８を実現する。

[0032] セキュリティ設定提案サーバ２００は、同様に、制御部２０１として、ＣＰＵ，ＲＡＭ，ＲＯＭ等を備え、通信部２０２として、例えば、ＩＥＥＥ８０２．１１に準拠したＷｉＦｉ対応デバイスを備える（有線であってもよい）。加えて、セキュリティ設定提案サーバ２００は、記憶部２０３として、ハードディスクや半導体メモリによる、データのストレージ部を備える。記憶部２０３は、セキュリティセット統計データベース２５０を、記憶部に備える。

[0033] セキュリティ設定提案サーバ２００の制御部２０１が所定のプログラムを読み込むことで、通信部２０２と協働して、セキュリティセット受信モジュール２０４、ユーザ情報受信モジュール２０５、提案要求受信モジュール２０６、提案セキュリティセット送信モジュール２０７を実現する。また、セキュリティ設定提案サーバ２００の制御部２０１が所定のプログラムを読み込むことで、記憶部２０３と協働して、セキュリティセット記憶モジュール２０８、セキュリティセット抽出モジュール２０９を実現する。

[0034] ［セキュリティ設定提案処理］

図４は、ユーザ端末１０、セキュリティ設定提案サーバ２００が実行するセキュリティ設定提案処理のフローチャートである。上述した各装置のモジュールが行う処理について、本処理にて併せて説明する。

[0035] 初めに、セキュリティ設定の提案を受けるに先駆けて、ユーザ端末１０の質問実施モジュール１８は、所定の質問項目に基づいて、ユーザに質問を実施する（ステップＳ１１）。この質問は、適切なセキュリティ設定の提案を受けるためのもので、ユーザのデモグラフィー情報を取得したり、セキュリティ設定に関する要望を諮ったり、インターネットや端末に関するユーザの習熟度を計ったりするために行う。具体的な質問として、インターネット制限の有無の希望や、インターネットの利用歴を問う事が考えられる。

[0036] 次に、ユーザ端末１０のユーザ情報送信モジュール１４は、質問に対する回答と、ユーザ自身の情報をあわせてユーザ情報として、セキュリティ設定提案サーバ２００へ送信し（ステップＳ１２）、セキュリティ設定提案サーバ２００のユーザ情報受信モジュール２０５がこれを受信する（ステップＳ１３）。ここで、質問項目以外のユーザ情報としては、主としてデモグラフィー情報、すなわち人口統計学的情報である。具体的には、ユーザの属性を示す情報として、このユーザの職務（役職、肩書、利用時間帯、勤続年数等）に関する情報等が挙げられ、ユーザ端末１０の登録情報から読み込んでもよいし、前記の様な質問によって情報を取得しても良い。

[0037] 次に、ユーザ端末１０の提案要求送信モジュール１５は、セキュリティ設定の提案要求を送信し（ステップＳ１４）、セキュリティ設定提案サーバ２００の提案要求受信モジュール２０６はこれを受信する（ステップＳ１５）。

[0038] そして、セキュリティ設定提案サーバ２００のセキュリティセット抽出モジュール２０９は、提案要求とともに受信したユーザ情報を用いて、セキュリティセット統計データベース２５０からセキュリティセットを抽出する（ステップＳ１６）。セキュリティセット統計データベース２５０には、セキュリティセットとユーザ情報とが関連付けて記憶されているため、ユーザ情

報が同一又は類似なセキュリティセットを抽出し、それぞれ数を数える事で、セキュリティセットの統計データを作成可能である。

[0039] 図６は、セキュリティセット統計データベース２５０内のセキュリティセットテーブルの一例である。セキュリティセットテーブルでは、セキュリティ設定を構成するパラメータの組み合わせが一つのセキュリティセットとして、セキュリティセット名とともに記憶されている。例えば図６によれば、「セキュリティセットＡ」は、利用時間制限、インターネット制限、メール制限、及びＧＰＳ追跡が有効になっており、電話制限は無効になっている。これらのセキュリティセットテーブルは、セキュリティ設定を行う種々のセキュリティソフトごとに必ずしも別れている必要はなく、上位概念化できる要素として記憶され、共有されていてよい。

[0040] また、図７は、セキュリティセット統計データベース２５０内のセキュリティセット統計テーブルの一例である。セキュリティセット統計テーブルでは、セキュリティセットと利用中のユーザ情報とが関連付けられて記憶されている。この図に示される範囲において、ユーザの属性が「１」～「３」であるユーザのセキュリティセットを抽出した場合、「セキュリティセットＡ」が抽出される。また、ユーザの属性が「４」～「５」であるユーザのセキュリティセットを抽出した場合、「セキュリティ設定Ｂ」が抽出される。また、ユーザの属性が「１０」～「１２」であるユーザのセキュリティセットを抽出した場合、「セキュリティ設定Ｃ」が抽出される。属性とは、上述した役職、肩書、利用時間帯、勤続年数等を便宜的に評価して数値化したものである。例えば、役職や肩書が高位なユーザに対しては、高い数値とする（例えば、新人の場合には「１」、中間管理職である場合には「５」、執行役員である場合には「１０」）。また、肩書も役職と同様に評価し数値化する。また、ユーザ端末１０を使用する時間帯が深夜や早朝等の通常よりも長時間の使用が想定されるユーザに対しては、高く数値化する。また、ユーザの勤続年数の長短に基づいて数値化する。実際にユーザ情報として記憶される「属性」は、これらの各数値の平均、最大値又は最小値の何れかの数値が用

いられる。セキュリティ設定は、属性の数値が高くなるほど、その制限を緩和したものになる。なお、各ユーザの職務内容に基づいて、各数値の重み付けを行い、最も重み付けが大きく設定された内容の数値を「属性」の数値として用いてもよい。また、その他の条件に基づいて、数値を評価し、評価結果を「属性」の数値として用いてもよい。また、属性の数値の大小ではなく、数値毎にセキュリティ設定における制限の詳細を決定していてもよい。

[0041] また、抽出の条件はユーザ情報に含まれる質問項目の内容でも指定可能であるし、値に幅を持たせ、類似の情報を増やしてもよい。例えば、受信したユーザの属性からプラスマイナス三の範囲を類似として抽出したり、ある属性においては大きな影響を与えない質問項目Ａを無視して抽出したり、ある属性のユーザの属性は類似を抽出せずに、所定の範囲内の属性のユーザの属性は類似を抽出したりといったことも可能である。

[0042] その後、提案セキュリティセット送信モジュール２０７が、抽出したセキュリティセットをユーザ端末１０に提案セキュリティセットとして送信する（ステップＳ１７）。提案セキュリティセットは、抽出したセキュリティセット全てであってもよいし、抽出したセキュリティセットから、加工や選別がなされていてもよい。例えば、インターネット制限を希望するのに無効になっているといった、質問項目の回答結果に明らかに矛盾するセキュリティセットを除外することが可能である。また、提案セキュリティセットは複数のセキュリティセットを含み、ユーザにその中から選択をさせる形式であってよい。

[0043] ユーザ端末１０の提案セキュリティセット受信モジュール１６が提案セキュリティセットを受信すると（ステップＳ１８）、提案セキュリティセット設定モジュール１７が、その提案セキュリティセットをユーザ端末１０のセキュリティ設定として設定する（ステップＳ１９）。

[0044] 図５は、提案セキュリティセットを受信したユーザ端末１０の画面の一例である。デモグラフィー情報５１のように、統計情報の抽出条件が示され、その下に統計情報５２が示される。設定ボタン５３を押す事で、対応するセ

キュリティセットをユーザ端末１０に設定することが可能である。また、円グラフの各項目をタッチすることで、各項目の詳細が示されてよいし、そこからセキュリティセットに任意の変更を加えたうえで設定可能であってよい。

[0045] 次に、ユーザ端末１０は設定したセキュリティセットの内容をセキュリティ設定提案サーバに送信する（ステップＳ２０）。セキュリティ設定提案サーバ２００のセキュリティセット受信モジュール２０４は、これを受信する（ステップＳ２１）。

[0046] 最後に、セキュリティ設定提案サーバ２００のセキュリティセット記憶モジュール２０８は、受信したセキュリティセットを、ステップＳ１３で受信したユーザ情報と関連付けて、セキュリティセット統計データベース２５０に記憶する（ステップＳ２１）。こうすることで、次回の提案要求の際に利用可能な統計情報が増加する。

[0047] 上述した手段、機能は、コンピュータ（ＣＰＵ，情報処理装置，各種端末を含む）が、所定のプログラムを読み込んで、実行することによって実現される。プログラムは、例えば、コンピュータからネットワーク経由で提供される（ＳａａＳ：ソフトウェア・アズ・ア・サービス）形態で提供される。プログラムは、例えば、フレキシブルディスク、ＣＤ（ＣＤ－ＲＯＭなど）、ＤＶＤ（ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭなど）等のコンピュータ読取可能な記録媒体に記録された形態で提供される。この場合、コンピュータはその記録媒体からプログラムを読み取って内部記憶装置または外部記憶装置に転送し記憶して実行する。また、そのプログラムを、例えば、磁気ディスク、光ディスク、光磁気ディスク等の記憶装置（記録媒体）に予め記録しておき、その記憶装置から通信回線を介してコンピュータに提供するようにしてもよい。

[0048] 以上、本発明の実施形態について説明したが、本発明は上述したこれらの実施形態に限るものではない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果

は、本発明の実施形態に記載されたものに限定されるものではない。

符号の説明

[0049] １　セキュリティ設定提案システム、３　公衆回線網、１０　ユーザ端末、２００　セキュリティ設定提案サーバ、２５０　セキュリティセット統計データベース

請求の範囲

[請求項1] 一以上のユーザ端末と通信可能に接続され、セキュリティ統計データベースを備えたコンピュータシステムであって、

前記ユーザ端末から、少なくとも属性を含むユーザ情報とともに、セキュリティセットの提案要求を取得する提案要求取得手段と、

前記提案要求とともに取得したユーザ情報を用いて、前記セキュリティセット統計データベースから、当該ユーザ情報と同一、又は所定の範囲で当該ユーザ情報と類似するユーザ情報に関連付けられているセキュリティセットを抽出するセキュリティセット抽出手段と、

前記抽出した一以上のセキュリティセットを提案セキュリティセットとして、前記ユーザ端末に提供する提案セキュリティセット提供手段と、

を備えることを特徴とするコンピュータシステム。

[請求項2] 前記ユーザ端末から、利用中の一連のセキュリティ設定に関するパラメータの組み合わせであるセキュリティセットを取得するセキュリティセット取得手段と、

前記ユーザ端末から、前記取得したセキュリティセットを利用中であるユーザの、少なくとも属性を含むユーザ情報を取得するユーザ情報取得手段と、

前記取得したセキュリティセットと、前記取得したユーザ情報とを、関連付けて前記セキュリティセット統計データベースに記憶させるセキュリティセット記憶手段と、

を備えることを特徴とする請求項１に記載のコンピュータシステム。

[請求項3] 前記ユーザ端末から取得する前記ユーザ情報に、当該ユーザ端末のユーザに対して実施された、所定の質問項目に対する回答を含めることを特徴とした、請求項１に記載のコンピュータシステム。

[請求項4] 前記属性とは、前記ユーザ端末のユーザの職務に関する情報である

、

ことを特徴とする請求項１に記載のコンピュータシステム。

[請求項5] 一以上のユーザ端末と通信可能に接続され、セキュリティ統計データベースを備えたコンピュータシステムが実行するセキュリティ設定提案方法であって、

前記ユーザ端末から、少なくとも属性を含むユーザ情報とともに、セキュリティセットの提案要求を取得するステップと、

前記提案要求とともに取得したユーザ情報を用いて、前記セキュリティセット統計データベースから、当該ユーザ情報と同一、又は所定の範囲で当該ユーザ情報と類似するユーザ情報に関連付けられているセキュリティセットを抽出するステップと、

前記抽出した一以上のセキュリティセットを提案セキュリティセットとして、前記ユーザ端末に提供するステップと、

を備えることを特徴とするセキュリティ設定提案方法。

[請求項6] 一以上のユーザ端末と通信可能に接続され、セキュリティ統計データベースを備えたコンピュータシステムに、

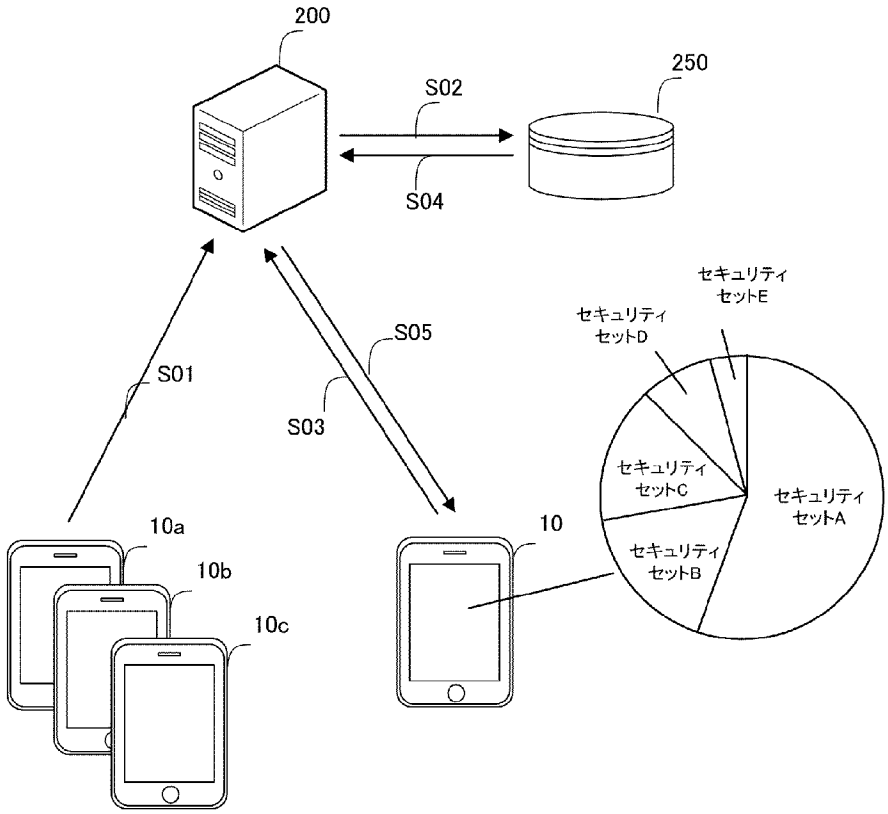
前記ユーザ端末から、少なくとも属性を含むユーザ情報とともに、セキュリティセットの提案要求を取得するステップ、

前記提案要求とともに取得したユーザ情報を用いて、前記セキュリティセット統計データベースから、当該ユーザ情報と同一、又は所定の範囲で当該ユーザ情報と類似するユーザ情報に関連付けられているセキュリティセットを抽出するステップ、

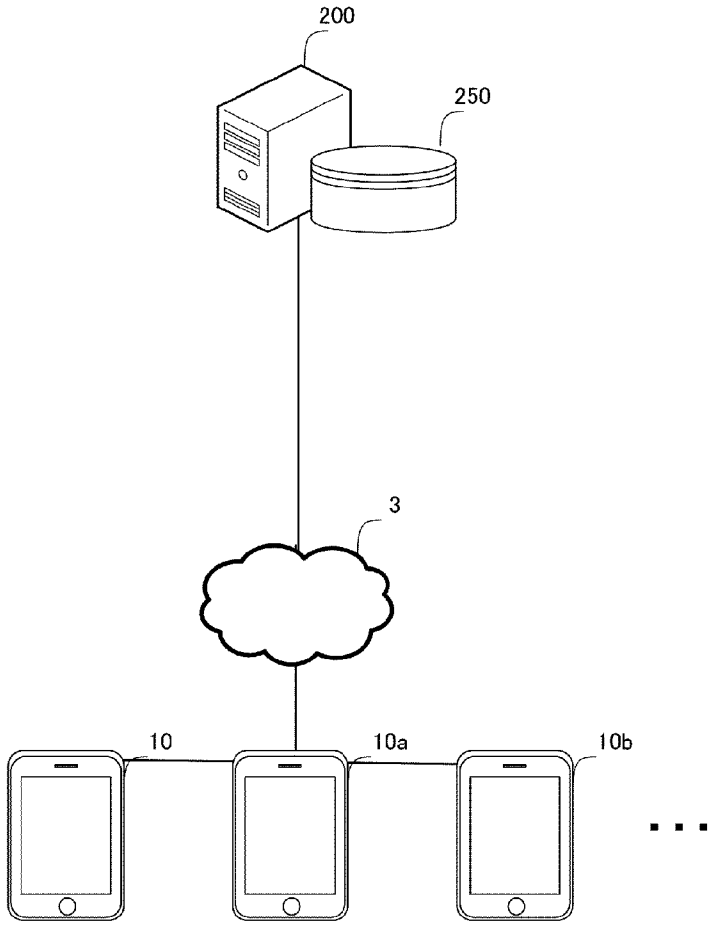
前記抽出した一以上のセキュリティセットを提案セキュリティセットとして、前記ユーザ端末に提供するステップ、

を実行させるためのコンピュータ読み取り可能なプログラム。

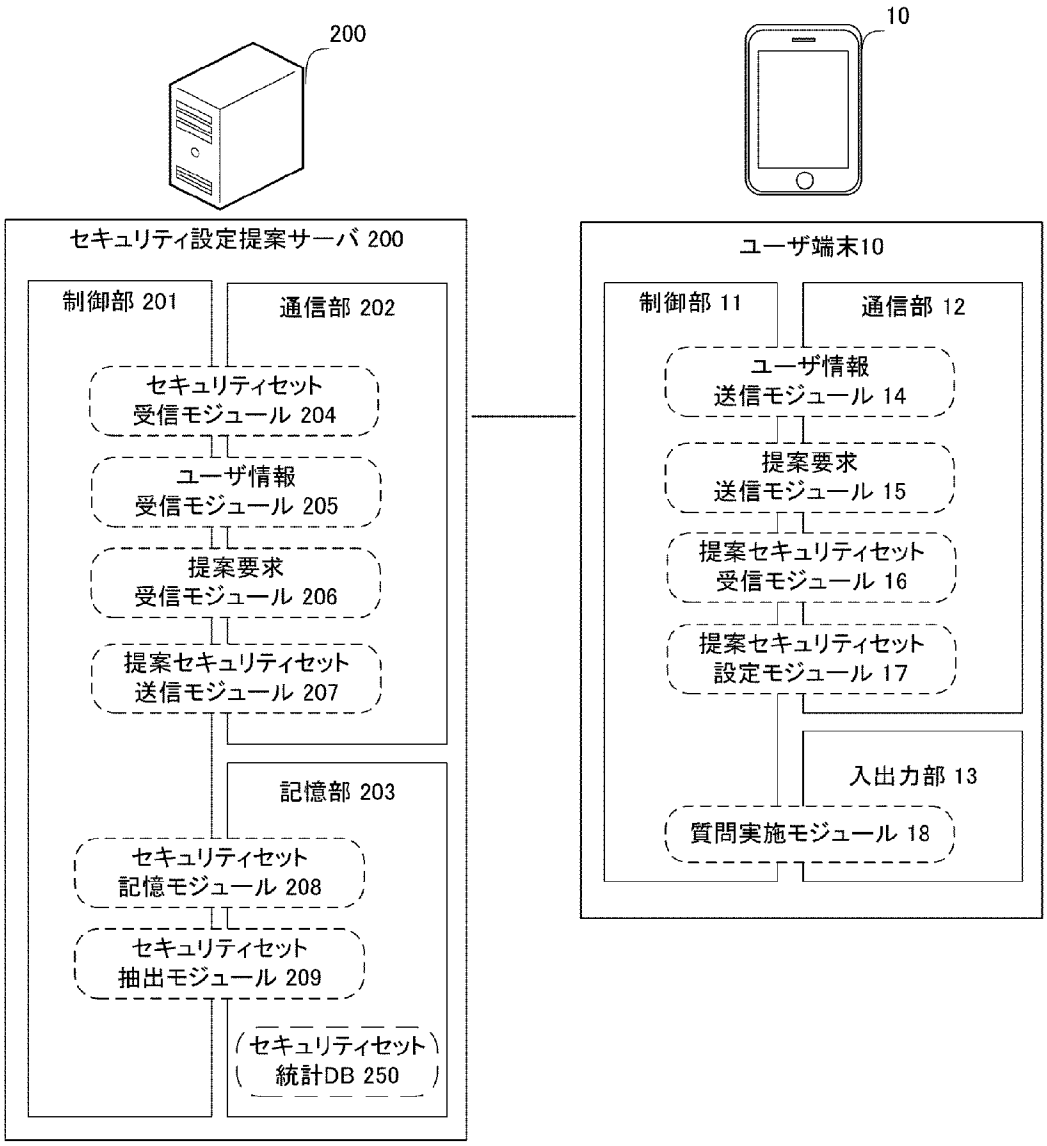
[図1]


200
250
S02
S04
S01
S03
S05
10a
10b
10c
10
セキュリティセットA
セキュリティセットB
セキュリティセットC
セキュリティセットD
セキュリティセットE

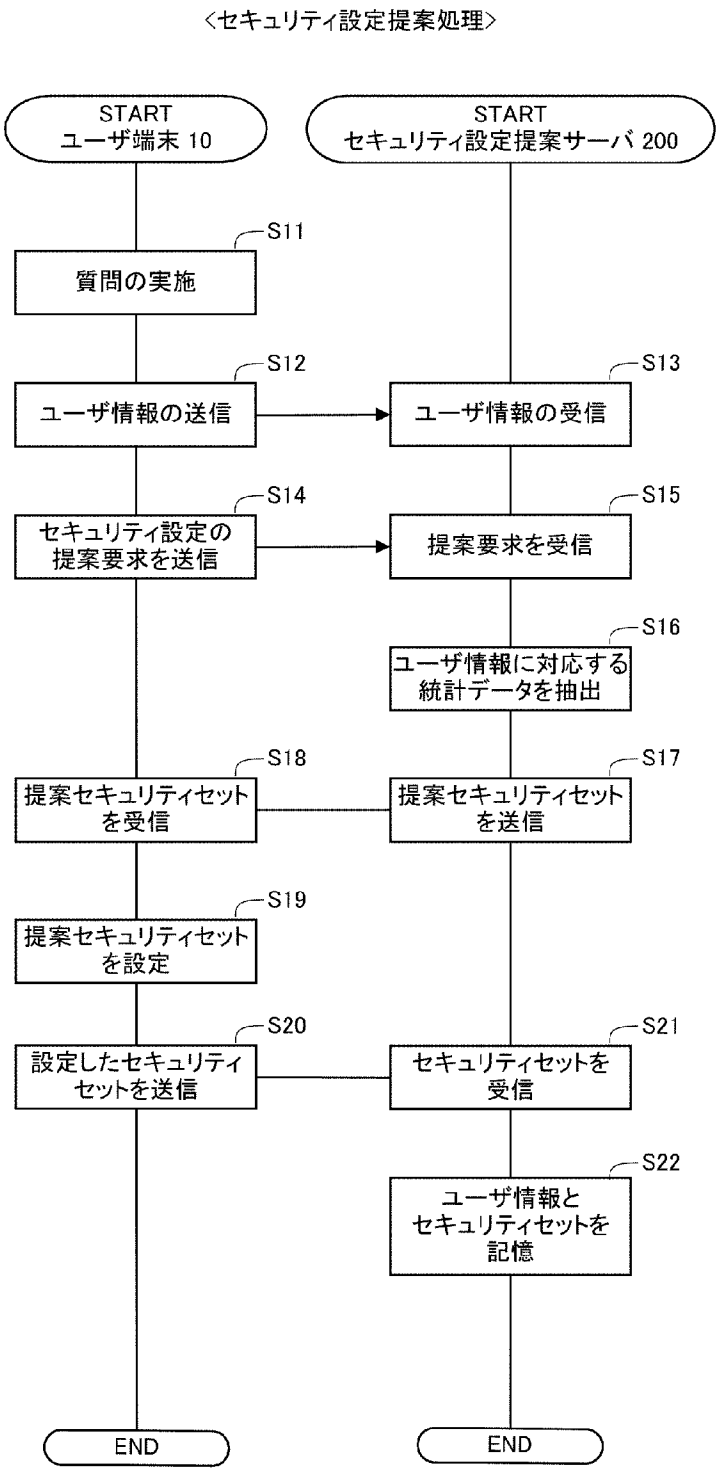
[図2]



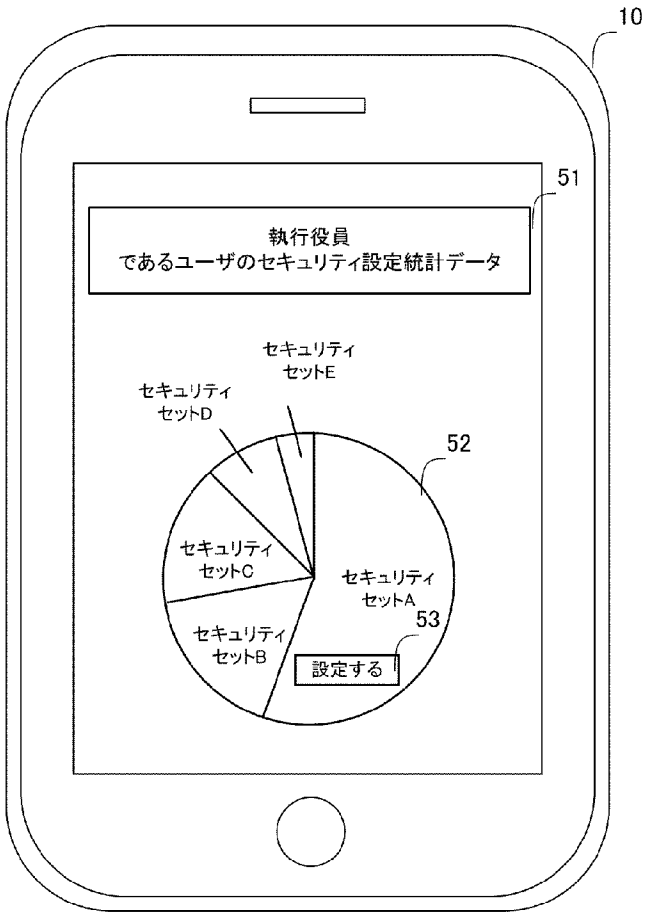
[図3]


200
10
セキュリティ設定提案サーバ 200
制御部 201
通信部 202
セキュリティセット
受信モジュール 204
ユーザ情報
受信モジュール 205
提案要求
受信モジュール 206
提案セキュリティセット
送信モジュール 207
記憶部 203
セキュリティセット
記憶モジュール 208
セキュリティセット
抽出モジュール 209
セキュリティセット
統計DB 250
ユーザ端末10
制御部 11
通信部 12
ユーザ情報
送信モジュール 14
提案要求
送信モジュール 15
提案セキュリティセット
受信モジュール 16
提案セキュリティセット
設定モジュール 17
入出力部 13
質問実施モジュール 18

[図4]


<セキュリティ設定提案処理>
START
ユーザ端末 10
START
セキュリティ設定提案サーバ 200
S11
質問の実施
S12
ユーザ情報の送信
S13
ユーザ情報の受信
S14
セキュリティ設定の
提案要求を送信
S15
提案要求を受信
S16
ユーザ情報に対応する
統計データを抽出
S18
提案セキュリティセット
を受信
S17
提案セキュリティセット
を送信
S19
提案セキュリティセット
を設定
S20
設定したセキュリティ
セットを送信
S21
セキュリティセットを
受信
S22
ユーザ情報と
セキュリティセットを
記憶
END
END

[図5]


10
51
執行役員
であるユーザのセキュリティ設定統計データ
セキュリティ
セットE
セキュリティ
セットD
52
セキュリティ
セットC
セキュリティ
セットA
53
セキュリティ
セットB
設定する

[図6]

〈セキュリティセットテーブル〉

セキュリティセット名	利用時間制限	インターネット制限	電話制限	メール制限	GPS追跡
セキュリティセットA	○	○	×	○	○
セキュリティセットB	○	○	×	×	○
セキュリティセットC	×	○	×	×	×
…	…	…	…	…	…

[図7]

〈セキュリティセット統計テーブル〉

利用中のセキュリティセット名	属性	質問項目A	質問項目B
セキュリティセットA	1	○	○
セキュリティセットA	1	×	×
セキュリティセットB	5	○	×
セキュリティセットA	3	○	○
セキュリティセットB	4	○	×
セキュリティセットC	10	○	○
セキュリティセットC	11	○	×
セキュリティセットA	2	×	○
セキュリティセットC	12	○	○
…	…	…	…

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/035309

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/57(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. G06F21/57

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	1971-2017
Registered utility model specifications of Japan	1996-2017
Published registered utility model applications of Japan	1994-2017

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2014-238675 A (OPTIM CORP.) 18 December 2014, claims 1-3, paragraph [0044], fig. 1-7 (Family: none)	1-6
A	US 2016/0344544 A1 (GARRETT VAL BIESINGER) 24 November 2016, paragraphs [0020]-[0022] (Family: none)	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	Date of mailing of the international search report
13.12.2017	26.12.2017

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１７／０３５３０９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/57(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.　G06F21/57

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	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７年

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

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X	JP 2014-238675 A (株式会社オプティム) 2014.12.18, 請求項 1-3, 段落[0044],図 1-7 (ファミリーなし)	1-6
A	US 2016/0344544 A1 (GARRETT VAL BIESINGER) 2016.11.24, 段落[0020]-[0022] (ファミリーなし)	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。

＊　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
１３．１２．２０１７	２６．１２．２０１７

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