(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
2020年1月2日(02.01.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/003479 A1

(51) 国際特許分類:
G06F 21/46 (2013.01) *G06F 21/55* (2013.01)

(21) 国際出願番号： PCT/JP2018/024760

(22) 国際出願日： 2018年6月29日(29.06.2018)

(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: 株式会社オプティム (**OPTIM CORPORATION**) [JP/JP]; 〒8408502 佐賀県佐賀市本庄町１ 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).

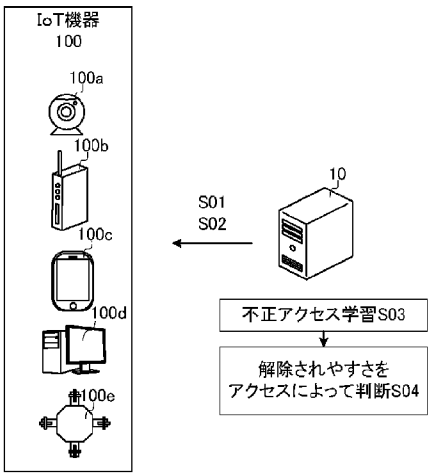
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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 2020/003479 A1

(54) **Title:** COMPUTER SYSTEM, IoT DEVICE MONITORING METHOD, AND PROGRAM

(54) 発明の名称： コンピュータシステム、ＩｏＴ機器監視方法及びプログラム

[図1]



100 IoT device
S03 Fraudulent access learning
S04 Determine ease of cancellation depending on access

(57) **Abstract:** [Problem] The purpose of the present invention is to provide a computer system, an IoT device monitoring method, and a program for which security has been improved. [Solution] A computer system for monitoring a connected IoT device 100, the computer system: monitoring the login state of the IoT device 100; detecting fraudulent access on the basis of the monitoring results; learning an ID and/or a password of the detected fraudulent access; determining whether the ID and/or the password previously possessed by the IoT device 100 is easily cancelled; and performing control such

［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))

that the IoT devices 100 to be accessed for making the determination are accessed in a prescribed priority order.

(57) 要約:【課題】セキュリティを向上させたコンピュータシステム、ＩｏＴ機器監視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】接続されたＩｏＴ機器１００を監視するコンピュータシステムは、前記ＩｏＴ機器１００のログイン状態を監視し、前記監視の結果に基づいて、不正アクセスを検出し、前記検出した不正アクセスのＩＤ又はパスワードの双方又はいずれかを学習し、前記ＩｏＴ機器１００が事前に保有しているＩＤ又はパスワードの双方又はいずれかが解除されやすいかどうかを判断し、判断するためにアクセスするＩｏＴ機器１００は、所定の優先順位でアクセスするように制御する。

明　細　書

発明の名称 ：

コンピュータシステム、ＩｏＴ機器監視方法及びプログラム

技術分野

[0001] 本発明は、接続されたＩｏＴ機器を監視するコンピュータシステム、ＩｏＴ機器監視方法及びプログラムに関する。

背景技術

[0002] 近年、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）に接続されるＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）機器の数そのものが増加している。ユーザは、所定の端末に、ＩＤ又はパスワードを入力することにより、ＩｏＴ機器にログインし、ＩｏＴ機器の様々な機能を使用することが可能となる。

[0003] このようなＩｏＴ機器へのログインに際し、他のユーザが不正アクセスを行うことにより、ユーザが意図していないＩｏＴ機器を利用される問題が発生している。

[0004] このような不正アクセスを防止するシステムとして、例えば、行動計画情報を予め作成し、監視対象の機器の位置情報が、この行動計画情報と一致しなかった場合、機器をロック状態にすることにより、パスワードが漏洩した後であっても、不正利用者が対象の機器を利用不可能とする構成が開示されている。

先行技術文献

特許文献

[0005] 特許文献1：特開２０１０－２２００１７

発明の概要

発明が解決しようとする課題

[0006] しかしながら、特許文献１の構成では、ＩｏＴ機器のパスワードが漏洩した後の対処であって、そもそもこのようなパスワードが破られやすい状態で

あるかどうかを判断することができなかった。加えて、近年では一のユーザが所有するＩｏＴ機器が増加していることから、全てのＩｏＴ機器に対して順番に不正利用を判断するのは時間がかかりすぎるという問題があった。

[0007] 本発明の目的は、危険性が高いＩｏＴ機器を優先的に確認することにより、セキュリティを向上させたコンピュータシステム、ＩｏＴ機器監視方法及びプログラムを提供することを目的とする。

課題を解決するための手段

[0008] 本発明では、以下のような解決手段を提供する。

[0009] 本発明は、接続されたＩｏＴ機器を監視するコンピュータシステムであって、

前記ＩｏＴ機器のログイン状態を監視する監視手段と、

前記監視の結果に基づいて、不正アクセスを検出する検出手段と、

前記検出された不正アクセスのＩＤ又はパスワードの双方又はいずれかを学習する学習手段と、

前記ＩｏＴ機器が事前に保有しているＩＤ又はパスワードの双方又はいずれかが解除されやすいかどうかを当該ＩｏＴ機器に対するアクセスによって判断する判断手段と、

判断するためにアクセスするＩｏＴ機器は、所定の優先順位でアクセスするように制御する優先アクセス手段と、

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。

[0010] 本発明によれば、接続されたＩｏＴ機器を監視するコンピュータシステムは、前記ＩｏＴ機器のログイン状態を監視し、前記監視の結果に基づいて、不正アクセスを検出し、前記検出された不正アクセスのＩＤ又はパスワードの双方又はいずれかを学習し、前記ＩｏＴ機器が事前に保有しているＩＤ又はパスワードの双方又はいずれかが解除されやすいかどうかを当該ＩｏＴ機器に対するアクセスによって判断し、判断するためにアクセスするＩｏＴ機器は、所定の優先順位でアクセスするように制御する。

[0011] 本発明は、コンピュータシステムのカテゴリであるが、ＩｏＴ機器監視方

法及びプログラム等の他のカテゴリにおいても、そのカテゴリに応じた同様の作用・効果を発揮する。

発明の効果

[0012] 本発明によれば、セキュリティを向上させたコンピュータシステム、ＩｏＴ機器監視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

[0013] [図1]図１は、ＩｏＴ機器監視システム１の概要を示す図である。

[図2]図２は、ＩｏＴ機器監視システム１の全体構成図である。

[図3]図３は、コンピュータ１０、ＩｏＴ機器１００の機能ブロック図である。

[図4]図４は、コンピュータ１０、ＩｏＴ機器１００が実行するＩｏＴ機器監視処理を示すフローチャートである。

[図5]図５は、ＩｏＴ機器１００が実行するＩｏＴ機器ログイン処理を示すフローチャートである。

[図6]図６は、追加通知画面の一例を示す図である。

[図7]図７は、第１の入力画面の一例を示す図である。

[図8]図８は、第２の入力画面の一例を示す図である。

発明を実施するための形態

[0014] 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。

[0015] ［ＩｏＴ機器監視システム１の概要］

本発明の好適な実施形態の概要について、図１に基づいて説明する。図１は、本発明の好適な実施形態であるＩｏＴ機器監視システム１の概要を説明するための図である。ＩｏＴ機器監視システム１は、コンピュータ１０、ＩｏＴ機器（ネットワークカメラ１００ａ、センサ装置１００ｂ、携帯端末１００ｃ、コンピュータ装置１００ｄ、ドローン１００ｅ）１００から構成され、コンピュータ１０に接続されたＩｏＴ機器１００を監視するコンピュー

タシステムである。

[0016] なお、図１において、コンピュータ１０、ＩｏＴ機器１００の数は、適宜変更可能である。また、ＩｏＴ機器１００の種類は、適宜変更可能である。また、コンピュータ１０、ＩｏＴ機器１００は、実在する装置に限らず、仮想的な装置であってもよい。また、後述する各処理は、コンピュータ１０、ＩｏＴ機器１００のいずれか又は複数の組み合わせにより実現されてもよい。

[0017] コンピュータ１０は、ＩｏＴ機器１００とデータ通信可能に接続されたコンピュータ装置である。なお、コンピュータ１０は、ＩｏＴ機器１００とＬＡＮ接続するルータ等のネットワーク装置でもよい。

[0018] ＩｏＴ機器１００は、コンピュータ１０とデータ通信可能に接続された端末装置である。ＩｏＴ機器１００は、例えば、動画や静止画等の画像を撮像するネットワークカメラ１００ａや、日照、温度、風力等の空間データや時間データ等の環境データを取得するセンサ装置１００ｂや、携帯電話、携帯情報端末、タブレット端末、パーソナルコンピュータに加え、ネットブック端末、スレート端末、電子書籍端末、携帯型音楽プレーや等の電化製品である携帯端末１００ｃ及びコンピュータ装置１００ｄや、無人航空機や無人移動体等のドローン１００ｅや、その他の物品である。

[0019] はじめに、コンピュータ１０は、ＩｏＴ機器１００のログイン状態を監視する（ステップＳ０１）。ログイン状態とは、ＩＤ又はパスワードの双方又はいずれかが解除されている状態である。

[0020] コンピュータ１０は、監視の結果に基づいて、不正アクセスを検出する（ステップＳ０２）。不正アクセスとは、過去のＩＤ又はパスワードの入力ミスが所定の回数（例えば、３回）以内であったにも関わらず、それを上回る回数ＩＤ又はパスワードが入力され、ＩＤ又はパスワードの双方又はいずれかが解除されている状態であることである。

[0021] コンピュータ１０は、検出した不正アクセスのＩＤ又はパスワードの双方又はいずれかを学習する（ステップＳ０３）。コンピュータ１０は、例えば

、不正アクセスに利用される頻度の高いＩＤ又はパスワードの組み合わせを教師データとして学習するとともに、今回不正アクセスが行われたＩＤ又はパスワードの組み合わせを学習する。

[0022] コンピュータ１０は、今回不正アクセスが行われたＩｏＴ機器１００とは異なるＩｏＴ機器１００が事前に保有しているＩＤ又はパスワードの双方又はいずれかが解除されやすいかどうかをこのＩｏＴ機器１００に対するアクセスによって判断する（ステップＳ０４）。例えば、コンピュータ１０は、上述した教師データと一致又は類似したＩＤ又はパスワードに基づいて、このＩｏＴ機器１００へのアクセスを試み、ログイン状態にできた場合、解除されやすいと判断し、ログイン状態にできない場合、解除されにくいと判断する。

[0023] このとき、コンピュータ１０は、この判断を行うためにアクセスするＩｏＴ機器１００に対して、所定の優先順位でアクセスするような制御を実行する。所定の優先順位とは、例えば、外部からのアクセス数が多いものに対して優先順位を上げておき、そうでないものは優先順位を下げておき、アクセスするような制御を実行する。また、コンピュータ１０は、記憶していないＩＰアドレスからのアクセスを検出したＩｏＴ機器１００に対して優先順位を上げて、アクセスするような制御を実行する。

[0024] 以上が、ＩｏＴ機器監視システム１の概要である。

[0025] ［ＩｏＴ機器監視システム１のシステム構成］

図２に基づいて、本発明の好適な実施形態であるＩｏＴ機器監視システム１のシステム構成について説明する。図２は、本発明の公的な実施形態であるＩｏＴ機器監視システム１のシステム構成を示す図である。ＩｏＴ機器監視システム１は、コンピュータ１０、ＩｏＴ機器（ネットワークカメラ１００ａ、センサ装置１００ｂ、携帯端末１００ｃ、コンピュータ装置１００ｄ、ドローン１００ｅ）１００、公衆回線網（インターネット網や、第３、第４世代通信網等）５から構成され、コンピュータ１０に接続されたＩｏＴ機器１００を監視するコンピュータシステムである。

[0026] なお、ＩｏＴ機器監視システム１を構成する各装置類の数及びその種類は、適宜変更可能である。また、ＩｏＴ機器監視システム１は、実在する装置に限らず、仮想的な装置類により実現されてもよい。また、後述する各処理は、ＩｏＴ機器監視システム１を構成する各装置類のいずれか又は複数の組み合わせにより実現されてもよい。また、コンピュータ１０は、ＩｏＴ機器１００とＬＡＮ接続するルータ等のネットワーク装置でもよい。

[0027] コンピュータ１０は、後述の機能を備えた上述したコンピュータ装置である。

[0028] ＩｏＴ機器１００は、後述の機能を備えた上述した端末装置である。

[0029] ［各機能の説明］

図３に基づいて、本発明の好適な実施形態であるＩｏＴ機器監視システム１の機能について説明する。図３は、コンピュータ１０、ＩｏＴ機器１００の機能ブロック図を示す図である。

[0030] コンピュータ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、他の機器と通信可能にするためのデバイス、例えば、ＩＥＥＥ８０２．１１に準拠したＷｉＦｉ（Ｗｉｒｅｌｅｓｓ Ｆｉｄｅｌｉｔｙ）対応デバイス等を備える。また、コンピュータ１０は、記憶部１３として、ハードディスクや半導体メモリ、記録媒体、メモリカード等によるデータのストレージ部を備える。

[0031] コンピュータ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により、通信部１２と協働して、機器検出モジュール２０、監視モジュール２１、学習モジュール２２、設定モジュール２３、通知送信モジュール２４、優先アクセスモジュール２５を実現する。また、コンピュータ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により、記憶部１３と協働して、判断モジュール３０、記憶モジュール３１を実現する。

[0032] ＩｏＴ機器１００は、コンピュータ１０と同様に、制御部１１０として、

ＣＰＵ、ＲＡＭ、ＲＯＭ等を備え、通信部１２０として、他の機器と通信可能にするためのデバイスを備える。また、ＩｏＴ機器１００は、入出力部１４０として、制御部１１０で制御したデータや画像を出力表示する表示部や、ユーザからの入力を受け付けるタッチパネルやキーボード、マウス等の入力部等や、動画や静止画等の画像を撮像する撮像部、環境データの取得や各種処理を実行するための各種デバイス等を備える。

[0033] ＩｏＴ機器１００において、制御部１１０が所定のプログラムを読み込むことにより、通信部１２０と協働して、通知受信モジュール１５０、データ送受信モジュール１５１、判断モジュール１５２、ログインモジュール１５３を実現する。また、ＩｏＴ機器１００において、制御部１１０が所定のプログラムを読み込むことにより、入出力部１４０と協働して、表示モジュール１６０を実現する。

[0034] ［ＩｏＴ機器監視処理］

図４に基づいて、ＩｏＴ機器監視システム１が実行するＩｏＴ機器監視処理について説明する。図４は、コンピュータ１０、ＩｏＴ機器１００が実行するＩｏＴ機器監視処理のフローチャートを示す図である。上述した各装置のモジュールが実行する処理について、本処理に併せて説明する。

[0035] 機器検出モジュール２０は、自身に接続されたＩｏＴ機器１００を検出する（ステップＳ１０）。ステップＳ１０において、機器検出モジュール２０は、自身にＬＡＮ接続又はＷＡＮ接続されたＩｏＴ機器１００を検出する。本実施形態において、機器検出モジュール２０は、ＩｏＴ機器１００として、ネットワークカメラ１００ａ、センサ装置１００ｂ、携帯端末１００ｂ、コンピュータ装置１００ｄ、ドローン１００ｅを検出する。

[0036] 監視モジュール２１は、検出したＩｏＴ機器１００のログイン状態を監視する（ステップＳ１１）。ステップＳ１１において、ログイン状態とは、ＩｏＴ機器１００のＩＤ又はパスワードの双方又はいずれかが解除されている状態を意味する。監視モジュール２１は、ＩｏＴ機器１００がログイン状態であるか否かを監視する。

[0037] 監視モジュール２１は、このＩｏＴ機器１００への外部からのアクセス数を計測する（ステップＳ１２）。ステップＳ１２において、監視モジュール２１は、単純に外部のＩＰアドレスからこのＩｏＴ機器１００へアクセスが行われた回数を、アクセス数として計測する。

[0038] 監視モジュール２１は、ＩｏＴ機器１００へアクセスしたＩＰアドレスを記憶モジュール３１に記憶させる（ステップＳ１３）。

[0039] 監視モジュール２１は、監視の結果に基づいて、不正アクセスを検出したか否かを判断する（ステップＳ１４）。ステップＳ１４において、監視モジュール２１は、不正アクセスを、過去に受け付けたＩＤ又はパスワードの入力ミスの回数を上回る回数の入力を受け付け、ＩＤ又はパスワードの双方又はいずれかかが解除されたことにより検出する。例えば、監視モジュール２１は、過去に受け付けたＩＤ又はパスワードの入力ミスの回数が３回以内であったにも関わらず、今回それを上回る回数である５回ＩＤ又はパスワードの入力を受け付け、その結果、ＩＤ又はパスワードのいずれか又は双方が解除された場合、不正アクセスとして検出する。

[0040] なお、監視モジュール２１は、その他の方法により、不正アクセスを検出してもよい。例えば、通常ログインする位置情報とは異なる位置情報からログインした場合、通常ログインする時間帯とは異なる時間帯にログインした場合、通常ログインする端末とは異なる端末からログインした場合等、通常におけるログインとは異なるログインを受け付けた場合に、不正アクセスを検出してもよい。

[0041] ステップＳ１４において、監視モジュール２１は、不正アクセスを検出していない場合（ステップＳ１４　ＮＯ）、本処理を終了する。

[0042] 一方、ステップＳ１４において、監視モジュール２１は、不正アクセスを検出した場合（ステップＳ１４　ＹＥＳ）、学習モジュール２２は、検出した不正アクセスが行われたＩＤ又はパスワードの双方又はいずれかを学習する（ステップＳ１５）。ステップＳ１５において、学習モジュール２２は、不正アクセスに利用される頻度の高いＩＤ又はパスワード及び今回不正アク

セスが行われたＩＤ又はパスワードを教師データとして、学習する。不正アクセスに利用される頻度の高いＩＤ又はパスワードとしては、初期設定のもの（ＩＤがａｄｍｉｎ、パスワードがａｄｍｉｎや、ＩＤがｕｓｅｒ、パスワードがｕｓｅｒ等）、複数のＩｏＴ機器等で同一又はいずれかが同じもの、同一の文字列のもの（００００、１１１１、ＡＡＡＡ等）、連続した英数字のもの（１２３４、５６７８、ＡＢＣＤ、ａｂｃ１２３等）、大文字や小文字や英数字や記号が組み合わされていないもの、キーボードを順番に押したもの（ｑｗｅｒｔｙ、ｐｏｉｕｙ等）、単純な名前のみのもの（ｙａｍａｄａ、ｓａｔｏｕ等）、辞書に登録される単純な単語のもの（ａｐｐｌｅ、ｓａｍｐｌｅ等）である。

[0043] 優先アクセスモジュール２５は、ＩｏＴ機器１００へのアクセスの優先順位を制御する（ステップＳ１６）。ステップＳ１６において、優先アクセスモジュール２５は、ＩＤ又はパスワードが解除されやすいかどうかを判断するためにアクセスするＩｏＴ機器２００に対して、所定の優先順位に基づいてアクセスするように制御する。

[0044] このとき、優先アクセスモジュール２５は、上述したステップＳ１２の処理により計測したアクセス数に基づいて、優先順位を決定する。例えば、優先アクセスモジュール２５は、アクセス数が多い順番にＩｏＴ機器１００の優先順位を決定する。その結果、優先アクセスモジュール２５は、アクセス数が多いＩｏＴ機器２００に対して優先順位を上げてアクセスするように制御することになる。判断モジュール３０は、この制御結果に基づいて、対象とするＩｏＴ機器１００へのアクセスを順次実行していく。

[0045] また、優先アクセスモジュール２５は、上述したステップＳ１３の処理により記憶したＩＰアドレスとは異なる新しいＩＰアドレスに基づいて、優先順位を決定する。例えば、優先アクセスモジュール２５は、新しいＩＰアドレスであった場合、このＩｏＴ機器１００の優先順位を上げてアクセスするように制御する。このとき、このような新しいＩＰアドレスが多い順番に優先順位を決定してもよいし、新しいＩＰアドレスを検知する毎に、優先順位

をそれ以前の状態よりも一段階挙げたもので決定してもよい。

[0046] なお、優先アクセスモジュール２５は、上述した二つの方法を組み合わせて優先順位を決定してもよい。例えば、アクセス数が多く新しいＩＰアドレスを検知したＩｏＴ機器１００の優先順位を上げていき、アクセス数が低いものの新しいＩＰアドレスを検知したＩｏＴ機器１００を先ほどのＩｏＴ機器１００の次の優先順位に決定するといったものである。また、優先アクセスモジュール２５は、組み合わせてに基づいて適宜優先順位を決定することも可能である。

[0047] 判断モジュール３０は、今回不正アクセスを検出したＩｏＴ機器１００とは異なるＩｏＴ機器１００が事前に記憶モジュール３１に保有しているＩＤ又はパスワードの双方又はいずれかが解除されやすいかどうかをＩｏＴ機器１００に対するアクセスによって判断する（ステップＳ１７）。ステップＳ１７において、判断モジュール３０は、学習した教師データに基づいて、このＩｏＴ機器１００へのアクセスを試みる。判断モジュール３０は、試みた結果、このＩｏＴ機器１００がログイン状態になった場合、解除されやすいと判断し、ログイン状態にならない場合、解除されにくいと判断する。判断モジュール３０は、このアクセスを複数回繰り返すことにより、この判断を実行する。このとき、判断モジュール３０は、上述したステップＳ１６の処理により決定した優先順位に基づいて、ＩｏＴ機器１００のアクセス順を決定し、このアクセス順に基づいて、アクセスを試みていく。

[0048] ステップＳ１７において、判断モジュール３０は、解除されにくいと判断した場合（ステップＳ１７　ＮＯ）、本処理を終了する。なお、判断モジュール３０は、解除されにくいと判断した場合、その旨の通知をユーザが所持する端末や、携帯端末１００ｃやコンピュータ装置１００ｄに送信してもよい。端末や携帯端末１００ｃやコンピュータ装置１００ｄは、この通知を表示してもよい。

[0049] 一方、ステップＳ１７において、判断モジュール３０は、解除されやすいと判断した場合（ステップＳ１７　ＹＥＳ）、設定モジュール２３は、記憶

モジュール３１が保有するＩｏＴ機器１００のＩＤ又はパスワードとは別に、このＩｏＴ機器１００に対して新たなＩＤ又はパスワードを設定する（ステップＳ１８）。ステップＳ１８において、設定モジュール２３は、保有したＩＤ又はパスワードに加えて、さらに新たなＩＤ又はパスワードを設定する。すなわち、このＩｏＴ機器１００は、２つのＩＤ又はパスワードが設定される。このとき、設定モジュール２３は、上述した不正アクセスに利用される頻度の高いＩＤ又はパスワードに合致しにくいＩＤ又はパスワードを設定する。また、設定モジュール２３は、ユーザの利便性を考慮したＩＤ又はパスワードを設定する。例えば、設定モジュール２３は、元々のＩＤ又はパスワードの一部に英数字を挿入することや、ＩＤ又はパスワードの始まり又は終わりのいずれか又は双方に英数字を挿入することや、これらを組み合わせることにより、不正アクセスに利用される頻度の高いＩＤ又はパスワードに合致しにくいＩＤ又はパスワードを設定する。例えば、設定モジュール２３は、元々のＩＤが「ｙａｍａｄａ」である場合、「０１ｙａｍａ０２ｄａ」と設定する。同様に、設定モジュール２３は、元々のパスワードが「ｔａｒｏｕ」である場合、「ｔａ０５ｒ１２ｏｕ」と設定する。

[0050] なお、設定モジュール２３が設定するＩＤ又はパスワードは、上述した例に限らず、適宜変更可能である。

[0051] 通知送信モジュール２４は、新たなＩＤ又はパスワードが設定されたことを示す通知を、ＩｏＴ機器１００に送信する（ステップＳ１９）。ステップＳ１９において、ＩｏＴ機器１００として、表示部や入出力部等を有する携帯端末１００ｃ又はコンピュータ装置１００ｄに、この通知を送信する。なお、通知送信モジュール２４は、その他のユーザが保有する端末装置等にこの通知を送信してもよい。

[0052] 通知受信モジュール１５０は、通知を受信する。表示モジュール１６０は、この通知に基づいて、追加通知画面を表示する（ステップＳ２０）。

[0053] 図６に基づいて、表示モジュール１６０が表示する追加通知画面について説明する。図６は、追加通知画面の一例を示す図である。表示モジュール１

６０は、追加通知画面３００として、追加内容表示領域３１０、完了アイコン３２０を表示する。追加内容表示領域３１０は、ＩＤ又はパスワードの追加理由と、追加前のＩＤ又はパスワードと、追加後のＩＤ又はパスワードとを表示する領域である。表示モジュール１６０は、追加理由として、「ＩＤ又はパスワードが単純だったため、新たにＩＤ又はパスワードを追加しました。」と表示する。表示モジュール１６０は、追加理由として、上述した不正アクセスに利用される頻度の高い内容に基づいたものを表示する。表示モジュール１６０は、追加前のＩＤとして、「旧ＩＤ：ｙａｍａｄａ」を表示し、追加前のパスワードとして「旧パスワード：ｔａｒｏｕ」を表示する。表示モジュール１６０は、追加後のＩＤとして「０１ｙａｍａｄａ０２」を表示し、追加後のパスワードとして「ｔａ０５ｒ１２ｏｕ」を表示する。完了アイコン３２０は、ユーザからの入力を受け付けることにより、本画面を終了する。

[0054] 表示モジュール１６０は、追加通知画面の表示を終了する入力を受け付けたか否かを判断する（ステップＳ２１）。ステップＳ２１において、表示モジュール１６０は、入力を受け付けていないと判断した場合（ステップＳ２１　ＮＯ）、すなわち、完了アイコン３２０の入力を受け付けていないと判断した場合、本処理を繰り返す。

[0055] 一方、ステップＳ２１において、表示モジュール１６０は、入力を受け付けたと判断した場合（ステップＳ２１　ＹＥＳ）、すなわち、完了アイコン３２０の入力を受け付けた場合、本処理を終了する。

[0056] 以上が、ＩｏＴ機器監視処理である。

[0057] ［ＩｏＴ機器ログイン処理］

図５に基づいて、ＩｏＴ機器監視システム１が実行するＩｏＴ機器ログイン処理について説明する。図５は、ＩｏＴ機器１００が実行するＩｏＴ機器ログイン処理のフローチャートを示す図である。上述した各モジュールが実行する処理について、本処理に併せて説明する。

[0058] 表示モジュール１６０は、ＩｏＴ機器１００に対するログインの入力を受

け付けたか否かを判断する（ステップＳ３０）。ステップＳ３０において、表示モジュール１６０は、専用のアプリケーションやウェブブラウザ等を起動することにより、ＩｏＴ機器１００へのログインの入力を受け付ける。

[0059] ステップＳ３０において、表示モジュール１６０は、入力を受け付けていないと判断した場合（ステップＳ３０　ＮＯ）、本処理を終了する。

[0060] 一方、ステップＳ３０において、表示モジュール１６０は、入力を受け付けたと判断した場合（ステップＳ３０　ＹＥＳ）、表示モジュール１６０は、第１の入力画面を表示する（ステップＳ３１）。

[0061] 図７に基づいて、表示モジュール１６０が表示する第１の入力画面について説明する。図７は、第１の入力画面の一例を示す図である。表示モジュール１６０は、第１の入力画面４００として、ＩＤ入力領域４１０、パスワード入力領域４２０、ログインアイコン４３０を表示する。ＩＤ入力領域４１０は、ユーザからの入力を受け付け、ＩＤの入力を受け付ける領域である。パスワード入力領域４２０は、ユーザからの入力を受け付け、パスワードの入力を受け付ける領域である。ＩＤ入力領域４１０及びパスワード入力領域４２０は、ユーザからの入力を受け付けることを契機として、仮想キーボードを表示し、この仮想キーボードへの入力を受け付けることによりユーザからの入力を受け付けてもよいし、音声入力等によりユーザからの入力を受け付けてもよい。ログインアイコン４３０は、ユーザからの入力を受け付け、データ送受信モジュール１５１は、入力を受け付けたＩＤ又はパスワードをログインデータとして対象となるＩｏＴ機器１００に送信する。

[0062] 表示モジュール１６０は、ＩＤ又はパスワードの入力を受け付ける（ステップＳ３２）。ステップＳ３２において、表示モジュール１６０は、元々のＩＤ又はパスワードの入力を受け付ける。すなわち、本実施形態では、ＩＤとして「ｙａｍａｄａ」、パスワードとして「ｔａｒｏｕ」の入力を受け付ける。

[0063] 表示モジュール１６０は、入力が完了したか否かを判断する（ステップＳ３３）。ステップＳ３３において、表示モジュール１６０は、ログインアイ

コン４３０の入力を受け付けたか否かに基づいて判断する。

[0064] ステップＳ３３において、表示モジュール１６０は、完了していないと判断した場合（ステップＳ３３　ＮＯ）、すなわち、ログインアイコン４３０の入力を受け付けていないと判断した場合、本処理を繰り返す。

[0065] 一方、ステップＳ３３において、表示モジュール１６０は、完了したと判断した場合（ステップＳ３３　ＹＥＳ）、すなわち、ログインアイコン４３０の入力を受け付けたと判断した場合、データ送受信モジュール１５１は、受け付けたＩＤ又はパスワードを、ログインデータとして、対象とするＩｏＴ機器１００に送信する（ステップＳ３４）。

[0066] データ送受信モジュール１５１は、ログインデータを受信する。判断モジュール１５２は、受信したログインデータが、正しいログインデータであるか否かを判断する（ステップＳ３５）。ステップＳ３５において、判断モジュール１５２は、ログインデータに含まれるＩＤとパスワードとが正しいものであるか否かを判断する。判断モジュール１５２は、正しいログインデータではないと判断した場合（ステップＳ３５　ＮＯ）、判断モジュール１５２は、入力ミスをカウントするとともに、再度ＩＤ又はパスワードの入力を促す通知をＩｏＴ機器１００に送信し、表示モジュール１６０は、この通知を表示し（ステップＳ３６）、上述したステップＳ３１以降の処理を繰り返す。さらに、判断モジュール１５２は、所定の回数以上、入力ミスをカウントした場合、ＩｏＴ機器監視システム１は、上述したＩｏＴ機器監視処理を実行する。

[0067] 一方、ステップＳ３５において、判断モジュール１５２は、正しいログインデータであると判断した場合（ステップＳ３５　ＹＥＳ）、判断モジュール１５２は、第２の入力画面を、ＩｏＴ機器１００に送信し、表示モジュール１６０は、この第２の入力画面を表示する（ステップＳ３７）。

[0068] 図８に基づいて、表示モジュール１６０が表示する第２の入力画面について説明する。図８は、第２の入力画面の一例を示す図である。表示モジュール１６０は、第２の入力画面５００として、追加ＩＤ入力領域５１０、追加

パスワード入力領域５２０、ログインアイコン５３０を表示する。追加ＩＤ入力領域５１０は、ユーザからの入力を受け付け、上述したステップＳ１５の処理において設定されたＩＤを入力する領域である。また、追加パスワード入力領域５２０は、ユーザからの入力を受け付け、上述したステップＳ１５の処理において設定されたパスワードを入力する領域である。追加ＩＤ入力領域５１０及び追加パスワード入力領域５２０は、ユーザからの入力を受け付けることを契機として、仮想キーボードを表示し、この仮想キーボードへの入力を受け付けることによりユーザからの入力を受け付けてもよいし、音声入力等によりユーザからの入力を受け付けてもよい。ログインアイコン５３０は、ユーザからの入力を受け付け、データ送受信モジュール１５１は、入力を受け付けた追加ＩＤ又は追加パスワードをログインデータとして対象となるＩｏＴ機器１００に送信する。

[0069] 表示モジュール１６０は、追加ＩＤ又は追加パスワードの入力を受け付ける（ステップＳ３８）。ステップＳ２８において、表示モジュール１６０は、新たに設定されたＩＤ又はパスワードの入力を受け付ける。すなわち、本実施形態では、追加ＩＤとして、「０１ｙａｍａｄａ０２」、追加パスワードとして「ｔａ０５ｒ１２ｏｕ」の入力を受け付ける。

[0070] 表示モジュール１６０は、入力が完了したか否かを判断する（ステップＳ３９）。ステップＳ２９において、表示モジュール１６０は、ログインアイコン５３０の入力を受け付けたか否かに基づいて判断する。

[0071] ステップＳ３９において、表示モジュール１６０は、完了していないと判断した場合（ステップＳ３９　ＮＯ）、すなわち、ログインアイコン５３０の入力を受け付けていないと判断した場合、本処理を繰り返す。

[0072] 一方、ステップＳ３９において、表示モジュール１６０は、完了したと判断した場合（ステップＳ３９　ＹＥＳ）、すなわち、ログインアイコン５３０の入力を受け付けたと判断した場合、データ送受信モジュール１５１は、受け付けた追加ＩＤ又は追加パスワードを、ログインデータとして、対象とするＩｏＴ機器１００に送信する（ステップＳ４０）。

[0073] データ送受信モジュール１５１は、ログインデータを受信する。判断モジュール１５２は、受信したログインデータが、正しいログインデータであるか否かを判断する（ステップＳ４１）。ステップＳ４１の処理は、上述したステップＳ３５の処理と同様である。ステップＳ４１において、判断モジュール１５２は、正しいログインデータではないと判断した場合（ステップＳ４１　ＮＯ）、判断モジュール１５２は、入力ミスをカウントするとともに、再度ＩＤ又はパスワードの入力を促す通知をＩｏＴ機器１００に送信し、表示モジュール１６０は、この通知を表示し（ステップＳ４２）、上述したステップＳ３７以降の処理を繰り返す。さらに、判断モジュール１５２は、所定の回数以上、入力ミスをカウントした場合、ＩｏＴ機器監視システム１は、上述したＩｏＴ機器監視処理を実行する。

[0074] 一方、ステップＳ４１において、判断モジュール１５２は、正しいログインデータであると判断した場合（ステップＳ４１　ＹＥＳ）、ログインモジュール１５３は、ＩｏＴ機器１００にログインする（ステップＳ４３）。

[0075] なお、上述した実施形態において、第１の入力画面において、元々のＩＤ又はパスワードを入力し、第２の入力画面において新たに設定されたＩＤ又はパスワードを入力しているが、第１の入力画面において、新たに設定されたＩＤ又はパスワードを入力し、第２の入力画面において、元々のＩＤ又はパスワードを入力してもよい。すなわち、ＩｏＴ機器１００のログイン画面の前後のいずれかに、新たなＩＤ又はパスワードを入力させるための入力を受け付ける構成であってもよい。

[0076] 以上が、ＩｏＴ機器ログイン処理である。

[0077] 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。また、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又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。

[0078] 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

[0079] １　ＩｏＴ機器監視システム、１０　コンピュータ、１００　ＩｏＴ機器

請求の範囲

[請求項1] 接続されたＩｏＴ機器を監視するコンピュータシステムであって、

前記ＩｏＴ機器のログイン状態を監視する監視手段と、

前記監視の結果に基づいて、不正アクセスを検出する検出手段と、

前記検出された不正アクセスのＩＤ又はパスワードの双方又はいずれかを学習する学習手段と、

前記ＩｏＴ機器が事前に保有しているＩＤ又はパスワードの双方又はいずれかが解除されやすいかどうかを当該ＩｏＴ機器に対するアクセスによって判断する判断手段と、

判断するためにアクセスするＩｏＴ機器は、所定の優先順位でアクセスするように制御する優先アクセス手段と、

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] 前記監視手段は、前記ＩｏＴ機器への外部からのアクセス数を計測し、

前記優先アクセス手段は、前記アクセス数が多いＩｏＴ機器に対して優先順位を上げてアクセスするように制御する、

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] 前記監視手段は、前記ＩｏＴ機器にアクセスしたＩＰアドレスを記憶し、

前記優先アクセス手段は、前記ＩｏＴ機器へのアクセスが、記憶されたＩＰアドレスに存在しない新しいＩＰアドレスによる場合に、当該ＩＰアドレスでアクセスされたＩｏＴ機器に対して優先順位を上げてアクセスするように制御する、

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4] 解除されやすいと判断した場合に、前記ＩｏＴ機器が事前に保有しているパスワードとは別に、当該ＩｏＴ機器に対して新たなパスワードを設定する設定手段と、

を備えることを特徴とする請求項１に記載にコンピュータシステム

。

[請求項5] 前記設定手段は、新たなパスワードを設定するとともに、前記ＩｏＴ機器が事前に保有しているＩＤとは別に、当該ＩｏＴ機器に対して新たなＩＤを設定する、

ことを特徴とする請求項４に記載のコンピュータシステム。

[請求項6] 前記新たなパスワードを設定した際に、前記ＩｏＴ機器のログイン画面の前後に、新たなパスワードを入力させるための入力を受け付ける受付手段と、

を備えることを特徴とする請求項４に記載のコンピュータシステム。

[請求項7] 接続されたＩｏＴ機器を監視するコンピュータシステムが実行するＩｏＴ機器監視方法であって、

前記ＩｏＴ機器のログイン状態を監視するステップと、

前記監視の結果に基づいて、不正アクセスを検出するステップと、

前記検出された不正アクセスのＩＤ又はパスワードの双方又はいずれかを学習するステップと、

前記ＩｏＴ機器が事前に保有しているＩＤ又はパスワードの双方又はいずれかが解除されやすいかどうかを当該ＩｏＴ機器に対するアクセスによって判断するステップと、

判断するためにアクセスするＩｏＴ機器は、所定の優先順位でアクセスするように制御するステップと、

を備えることを特徴とするＩｏＴ機器監視方法。

[請求項8] 接続されたＩｏＴ機器を監視するコンピュータシステムに、

前記ＩｏＴ機器のログイン状態を監視するステップ、

前記監視の結果に基づいて、不正アクセスを検出するステップ、

前記検出された不正アクセスのＩＤ又はパスワードの双方又はいずれかを学習するステップ、

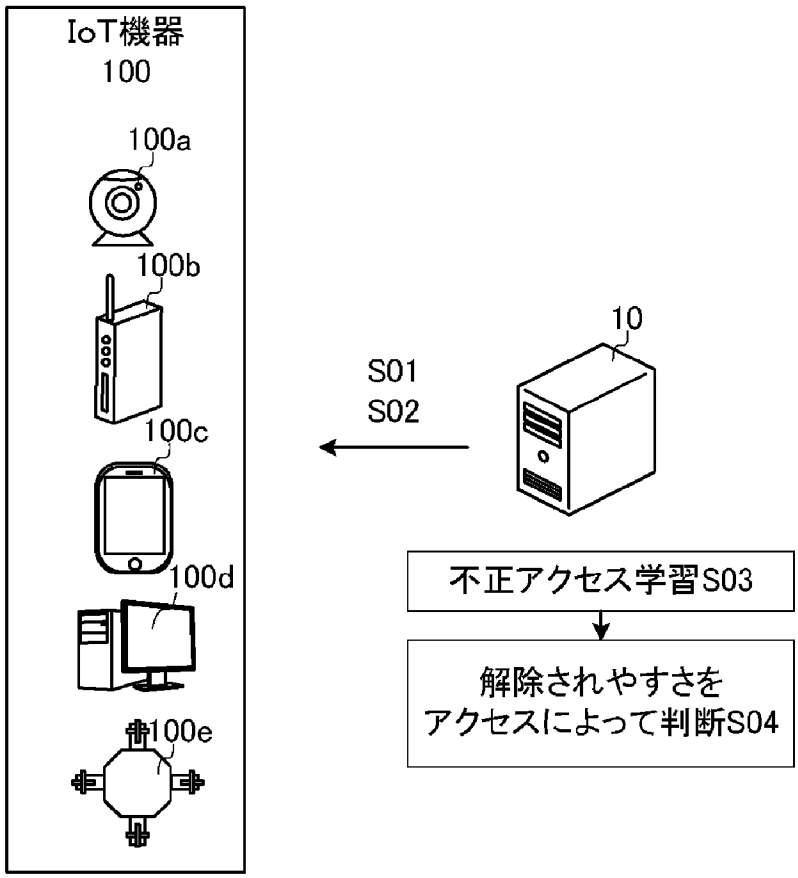
前記ＩｏＴ機器が事前に保有しているＩＤ又はパスワードの双方又

はいずれかが解除されやすいかどうかを当該ＩｏＴ機器に対するアクセスによって判断するステップ、

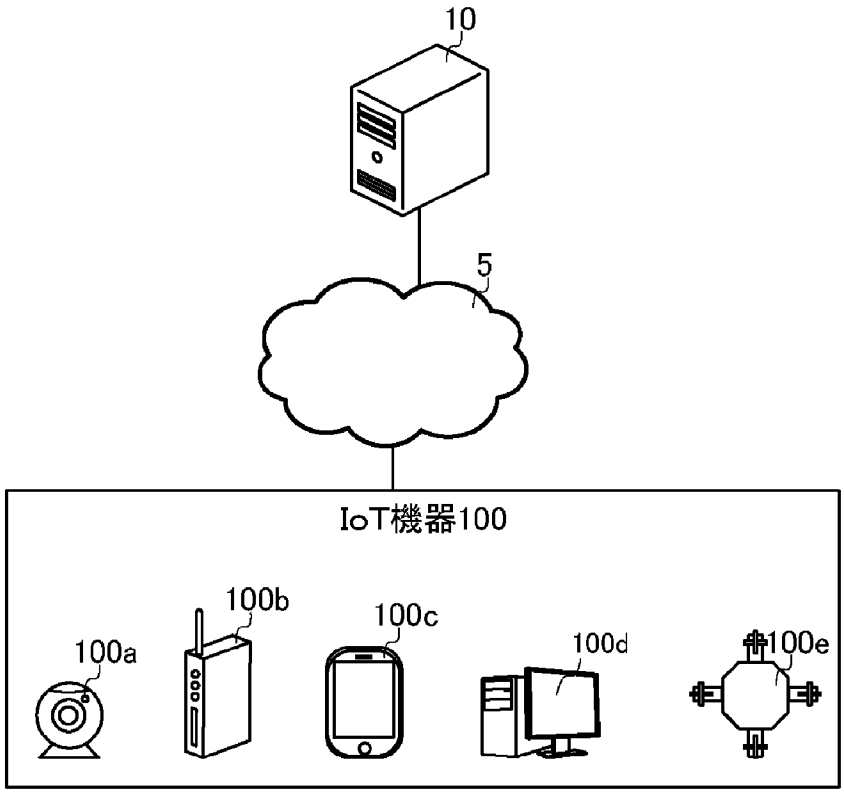
判断するためにアクセスするＩｏＴ機器は、所定の優先順位でアクセスするように制御するステップ、

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。

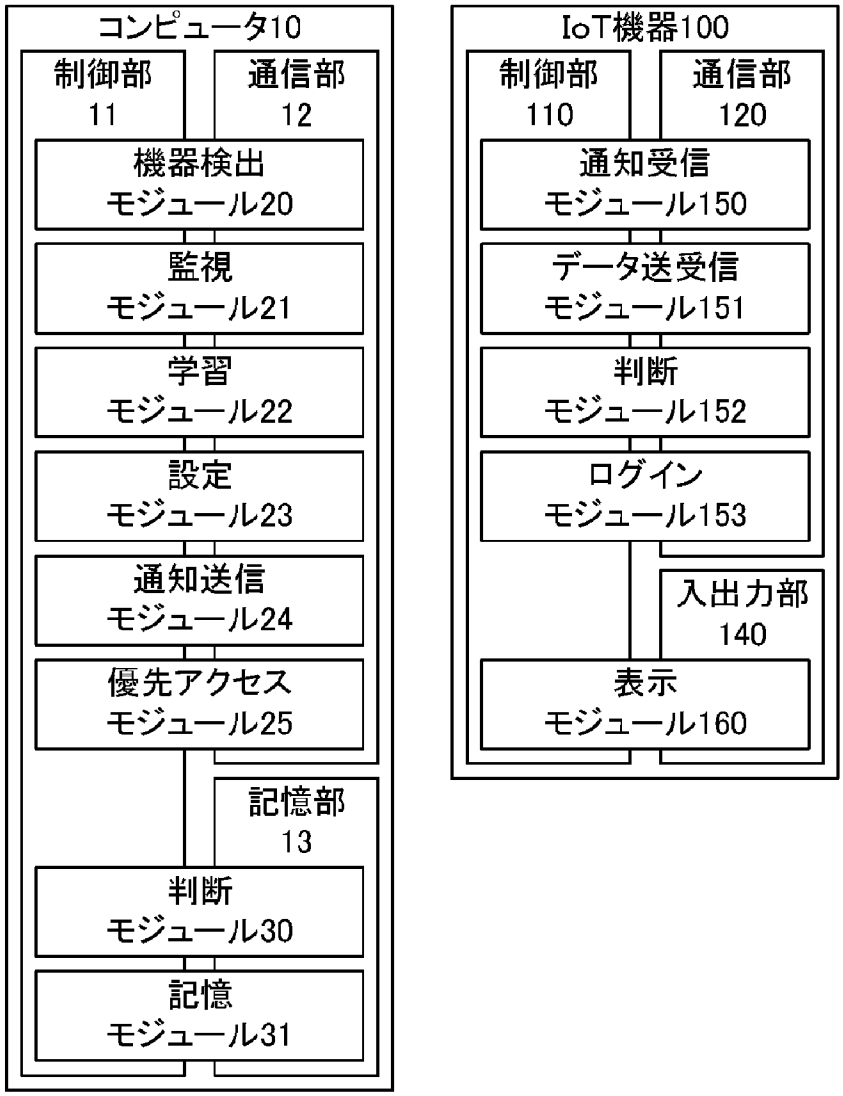
[図1]


IoT機器
100
100a
100b
100c
100d
100e
10
S01
S02
不正アクセス学習S03
解除されやすさを
アクセスによって判断S04

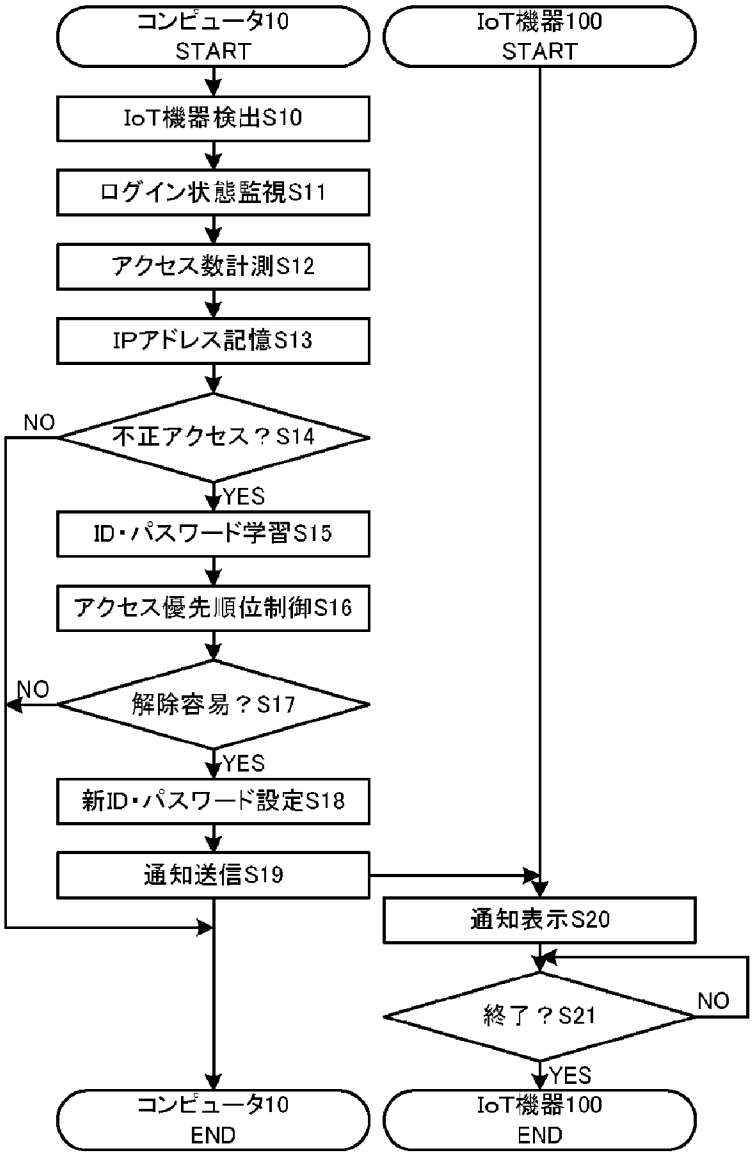
[図2]



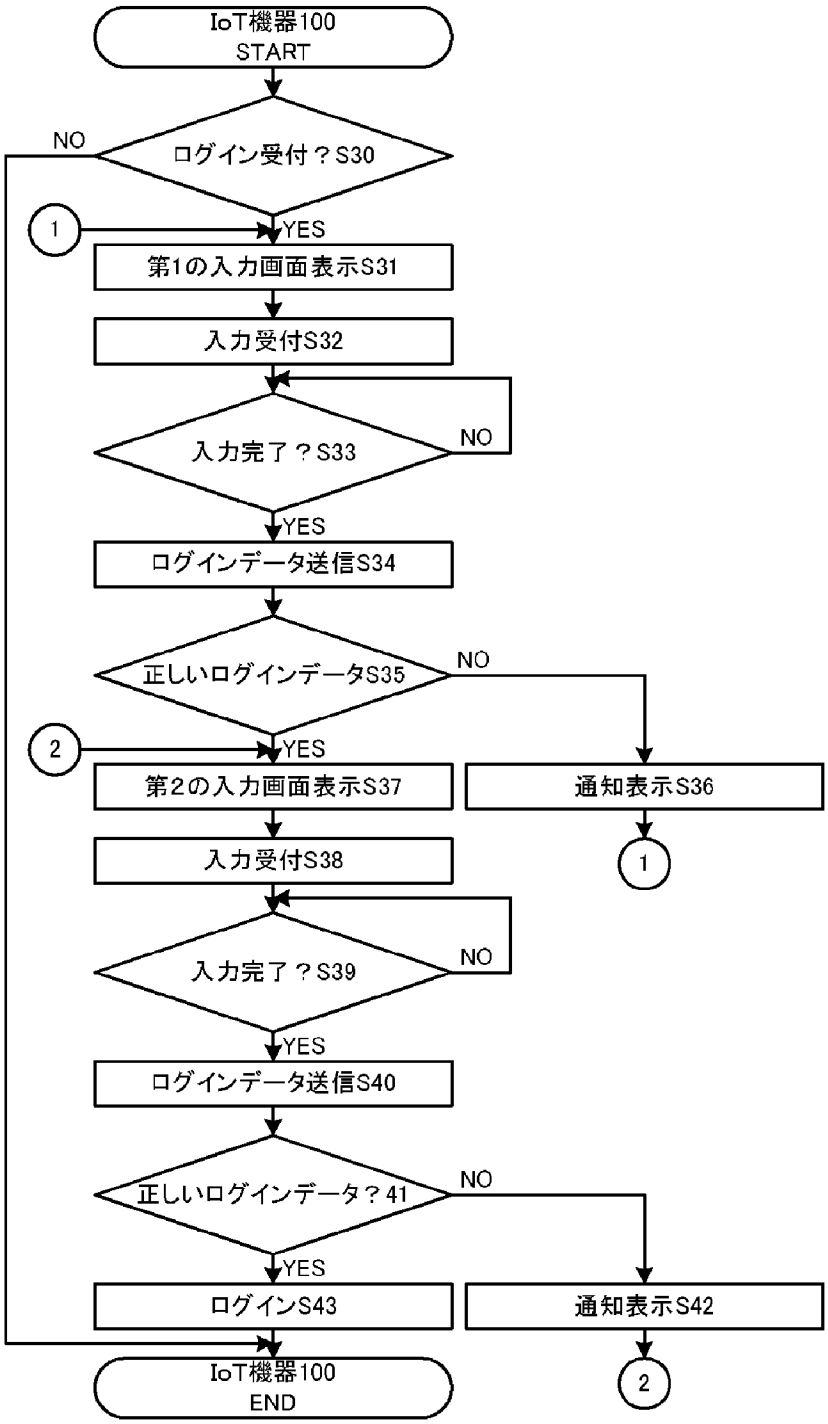
[図3]


コンピュータ10
制御部
11
通信部
12
機器検出
モジュール20
監視
モジュール21
学習
モジュール22
設定
モジュール23
通知送信
モジュール24
優先アクセス
モジュール25
記憶部
13
判断
モジュール30
記憶
モジュール31
IoT機器100
制御部
110
通信部
120
通知受信
モジュール150
データ送受信
モジュール151
判断
モジュール152
ログイン
モジュール153
入出力部
140
表示
モジュール160

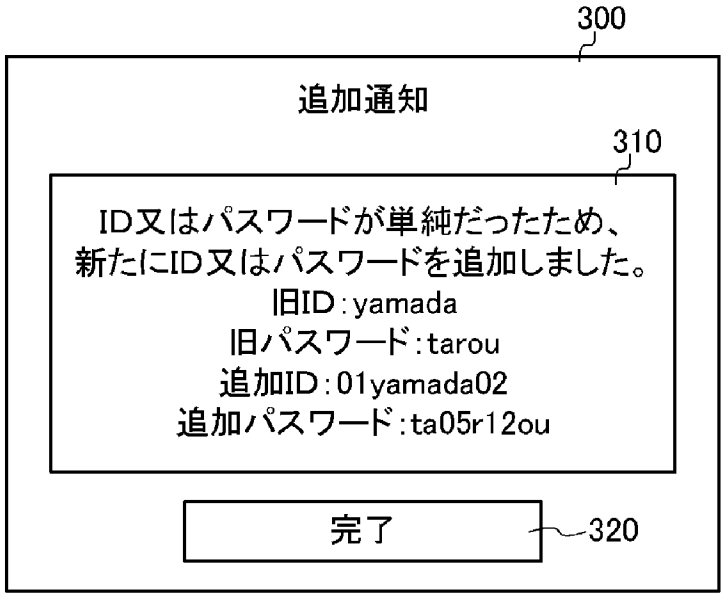
[図4]


コンピュータ10
START
IoT機器100
START
IoT機器検出S10
ログイン状態監視S11
アクセス数計測S12
IPアドレス記憶S13
不正アクセス？S14
NO
YES
ID・パスワード学習S15
アクセス優先順位制御S16
解除容易？S17
NO
YES
新ID・パスワード設定S18
通知送信S19
通知表示S20
終了？S21
NO
YES
コンピュータ10
END
IoT機器100
END

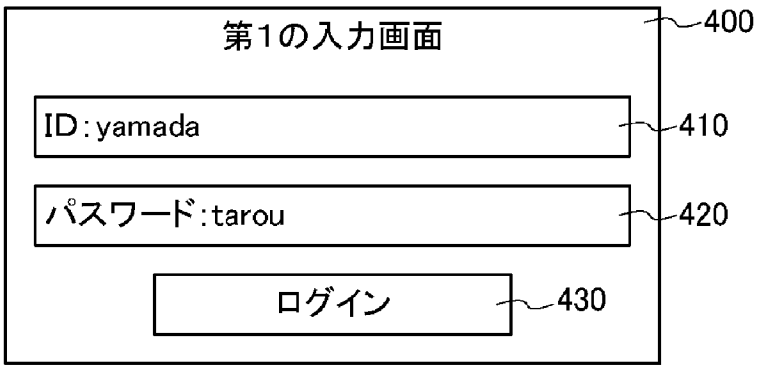
[図5]


IoT機器100
START
ログイン受付？S30
NO
YES
1
第1の入力画面表示S31
入力受付S32
入力完了？S33
NO
YES
ログインデータ送信S34
正しいログインデータS35
NO
YES
2
第2の入力画面表示S37
通知表示S36
1
入力受付S38
入力完了？S39
NO
YES
ログインデータ送信S40
正しいログインデータ？41
NO
YES
ログインS43
通知表示S42
2
IoT機器100
END

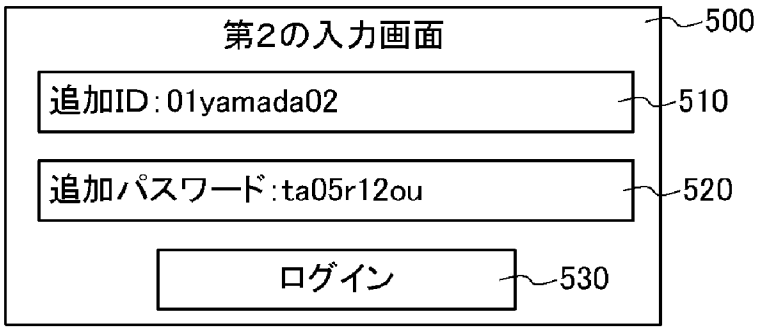
[図6]


300
追加通知
310
ID又はパスワードが単純だったため、
新たにID又はパスワードを追加しました。
旧ID：yamada
旧パスワード：tarou
追加ID：01yamada02
追加パスワード：ta05r12ou
完了
320

[図7]


第1の入力画面
400
ID：yamada
410
パスワード：tarou
420
ログイン
430

[図8]


第2の入力画面
500
追加ID：01yamada02
510
追加パスワード：ta05r12ou
520
ログイン
530

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/024760

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/46(2013.01)i, G06F21/55(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. G06F21/46, G06F21/55

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.
X A	JP 6310620 B1 (OPTIM CORPORATION) 11 April 2018, claims 1-4, paragraphs [0034]-[0044] & WO 2018/100682 A1	1, 4-8 2, 3
X A	JP 6310621 B1 (OPTIM CORPORATION) 11 April 2018, claim 1, paragraphs [0034]-[0044] & WO 2018/100667 A1	1, 4-8 2, 3

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
13.09.2018	25.09.2018

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/024760

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018/0144139 A1 (ZINGBOX, LTD.) 24 May 2018, paragraphs [0104]-[0117] (Family: None)	2, 3
A	WO 2017/208969 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 07 December 2017, paragraphs [0025], [0054] (Family: None)	2, 3
A	山口 利恵ほか, スマートフォンを事例とする多要素認証確率の提案, 2015 年 暗号と情報セキュリティシンポジウム (SCIS 2015) 概要集, 20 January 2015, pp. 1-8, (YAMAGUCHI, Rie et al.), non-official translation (A proposal of multi-factor authentication probability with smartphone as a case, Abstracts of the 32nd Symposium on Cryptography and Information Security (SCIS 2015))	2, 3

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０２４７６０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/46(2013.01)i, G06F21/55(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.　G06F21/46, G06F21/55

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
X A	JP 6310620 B1 (株式会社オプティム) 2018.04.11, 請求項 1-4, 段落 0034-0044 & WO 2018/100682 A1	1, 4-8 2, 3
X A	JP 6310621 B1 (株式会社オプティム) 2018.04.11, 請求項 1, 段落 0034-0044 & WO 2018/100667 A1	1, 4-8 2, 3

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１３．０９．２０１８	２５．０９．２０１８

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　４８７６
金木　陽一
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
A	US 2018/0144139 A1 (ZINGBOX, LTD.) 2018.05.24, paras. 0104-0117 (Family: None)	2, 3
A	WO 2017/208969 A1 (日本電信電話株式会社) 2017.12.07, 段落 0025, 0054 (Family: None)	2, 3
A	山口 利恵ほか, スマートフォンを事例とする多要素認証確率の提案, 2015 年 暗号と情報セキュリティシンポジウム (SCIS 2015) 概要集, 2015.01.20, pp. 1-8	2, 3