

(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
2021年12月9日(09.12.2021)



(10) 国際公開番号

WO 2021/245786 A1

(51) 国際特許分類:
G06F 21/46 (2013.01)

(21) 国際出願番号: PCT/JP2020/021763

(22) 国際出願日: 2020年6月2日(02.06.2020)

(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: 藤田 真浩 (FUJITA, Masahiro); 〒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).

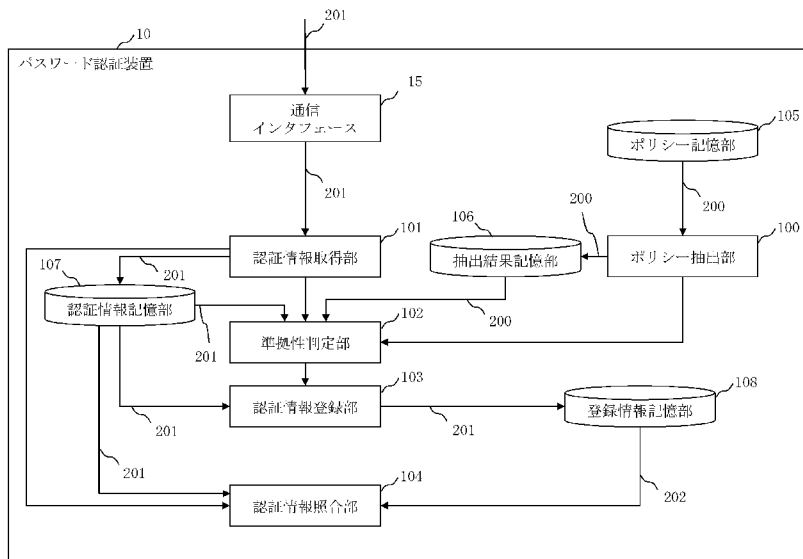
(74) 代理人: 溝井 国際特許業務法人(MIZOI INTERNATIONAL PATENT FIRM); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (JP).

(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, 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,

(54) Title: PASSWORD AUTHENTICATION DEVICE, PASSWORD AUTHENTICATION METHOD, AND PASSWORD AUTHENTICATION PROGRAM

(54) 発明の名称: パスワード認証装置、パスワード認証方法、及びパスワード認証プログラム

図3



10 Password authentication device
15 Communication interface
100 Policy extraction unit
101 Authentication information acquisition unit
102 Conformance determination unit
103 Authentication information registration unit
104 Authentication information collation unit
105 Policy storage unit
106 Extraction results storage unit
107 Authentication information storage unit
108 Registration information storage unit

(57) Abstract: In the present invention, a policy storage unit (105) stores a plurality of password policies which describe requirements for certifying a password to be used in authentication of a user, and with which a password can be certified as a correct password if the password conforms to at least one password policy among the plurality of password policies. A policy extraction unit (100) extracts one or more password policies from the plurality of password policies. An authentication information acquisition unit (101) acquires authentication information including a password. A conformance determination unit (102) determines whether or not the password included in the authentication information conforms to at least one password policy among the one or more password policies. An authentication information registration unit (103) registers the authentication information as registration information if the conformance determination unit (102) has

MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

- 一 国際調査報告（条約第21条(3)）

determined that the password conforms to at least one password policy.

(57) 要約：ポリシー記憶部（105）は、ユーザの認証に用いるパスワードの認定要件を記述した複数のパスワードポリシーであり、パスワードが複数のパスワードポリシーのうち少なくともいずれか1つのパスワードポリシーに準拠していればパスワードを正当なパスワードとして認定可能な複数のパスワードポリシーを記憶する。ポリシー抽出部（100）は、複数のパスワードポリシーから1つ以上のパスワードポリシーを抽出する。認証情報取得部（101）は、パスワードを含む認証情報を取得する。準拠性判定部（102）は、認証情報に含まれるパスワードが、1つ以上のパスワードポリシーのうち、少なくともいずれか1つのパスワードポリシーに準拠しているか否かを判定する。認証情報登録部（103）は、準拠性判定部（102）が少なくともいずれか1つのパスワードポリシーに準拠していると判定したときに、認証情報を登録情報として登録する。

明 細 書

発明の名称：

パスワード認証装置、パスワード認証方法、及びパスワード認証プログラム

技術分野

[0001] 本開示は、パスワード認証装置、パスワード認証方法、及びパスワード認証プログラムに関する。

背景技術

[0002] パスワードを用いたパスワード認証システムでは、ユーザに強固で安全なパスワードを使用してもらうために、パスワード認証システム側が単一のパスワード生成ルール（以下、パスワードポリシーという）を指定する。そして、そのパスワードポリシーに従って、ユーザがパスワードを生成し、登録する方法が用いられている場合がある。しかし、このような方法では、ユーザのパスワードの生成方針とパスワードポリシーとが矛盾していても、ユーザのパスワードの生成方針とかけ離れたパスワードポリシーに従って、ユーザはパスワードを生成し、登録しなければならないという課題があった。

この課題を解決するために、特許文献1ではユーザ等が入力した文字列からパスワードポリシーに準拠したパスワードを生成するパスワード生成装置が開示されている。より具体的には、特許文献1で開示のパスワード生成装置は、パスワードを構成する文字種別を示すパスワードポリシーを受け付け、受け付けたパスワードポリシーに基づいて、複数の変換パターンのうち使用する変換パターンを決定する。そして、パスワード生成装置は、第1の文字列の入力を受け付け、入力された第1の文字列を解析し、変換に用いられる複数の文字群を抽出する。そして、パスワード生成装置は、決定した変換パターンに基づいて、抽出した複数の文字群を第2の文字列に変換し、変換した第2の文字列を合成してパスワードを生成する。

このパスワード生成装置によって、ユーザが入力した文字列から、パスワ

ードポリシーに準拠し、且つユーザ自身のパスワードの生成方針に沿った、強固で安全なパスワードを生成することが可能となる。

先行技術文献

特許文献

[0003] 特許文献1：特開2014-178978号公報

発明の概要

発明が解決しようとする課題

[0004] 特許文献1に記載の手法では、パスワードの安全性を保障するために、パスワード生成装置はユーザが入力した文字列を変換する変換パターンは秘密情報として非公開で管理しなければならないという課題があった。

変換パターンが公開されれば、攻撃者が、ユーザにより入力された文字列を推定し、推定した文字列を公開された変換パターンを用いて変換し、パスワードを推測するというパスワード推測攻撃が可能となる。

さらに、ユーザにより入力された文字列がパスワードポリシーに準拠せず十分に安全な文字列でなければ、このパスワード推測攻撃は効率的に行われ、パスワードの安全性が保障されない可能性があるからである。

[0005] 本開示は、パスワードポリシーに準拠し、且つユーザ自身のパスワードの生成方針に沿った安全なパスワード生成を可能とすることを主な目的とする。

課題を解決するための手段

[0006] 本開示に係るパスワード認証装置は、

ユーザの認証に用いるパスワードの認定要件を記述した複数のパスワードポリシーであり、パスワードが前記複数のパスワードポリシーのうち少なくともいずれか1つのパスワードポリシーに準拠していれば前記パスワードを正当なパスワードとして認定可能な複数のパスワードポリシーを記憶するポリシー記憶部と、

前記ポリシー記憶部が記憶する前記複数のパスワードポリシーから1つ以

上のパスワードポリシーを抽出するポリシー抽出部と、

パスワードを含む認証情報を取得する認証情報取得部と、

前記認証情報取得部が取得した前記認証情報に含まれるパスワードが、前記ポリシー抽出部が抽出した前記1つ以上のパスワードポリシーのうち、少なくともいずれか1つのパスワードポリシーに準拠しているか否かを判定する準拠性判定部と、

前記準拠性判定部が前記少なくともいずれか1つのパスワードポリシーに準拠していると判定したときに、前記認証情報を登録情報として登録する認証情報登録部と

を備える。

発明の効果

[0007] 本開示によれば、パスワードポリシーに準拠し、且つユーザ自身のパスワードの生成方針に沿った安全なパスワード生成を可能とすることができる。

図面の簡単な説明

[0008] [図1]実施の形態1に係るパスワード認証システムの構成例を示す図。

[図2]実施の形態1に係るパスワード認証装置のハードウェア構成例を示す図。

[図3]実施の形態1に係るパスワード認証装置の機能構成例を示す図。

[図4]実施の形態1に係る認証情報登録の処理を示すフローチャート。

[図5]実施の形態1に係るポリシー記憶部に記憶される複数のパスワードポリシーの例を示す図。

[図6]実施の形態1に係る登録フォームへのパスワード入力例を示す図。

[図7]実施の形態1に係る認証の処理を示すフローチャート。

[図8]実施の形態1に係る認証フォームへのパスワード入力例を示す図。

[図9]実施の形態1に係る認証情報登録時に抽出ポリシーを表示したパスワード入力例を示す図。

[図10]実施の形態2に係るパスワード認証装置の機能構成例を示す図。

[図11]実施の形態2に係るパスワード認証装置の認証情報登録の処理例を示す図。

すフローチャート。

[図12]実施の形態2に係るポリシー記憶部に記憶される複数のパスワードポリシーの例を示す図。

[図13]実施の形態2に係る抽出結果記憶部に記憶される抽出ポリシーの例を示す図。

[図14]実施の形態3に係るパスワード認証装置の機能構成例を示す図。

[図15]実施の形態3に係る認証情報登録の処理例を示すフローチャート。

[図16]実施の形態3に係る認証情報登録時のユーザポリシーの選択例を示す図。

[図17]実施の形態3に係る認証の処理例を示すフローチャート。

[図18]実施の形態3に係る認証時のパスワード入力例を示す図。

[図19]実施の形態4に係るパスワード認証システムの構成例を示す図。

[図20]実施の形態4に係るパスワード認証装置の機能構成例を示す図。

[図21]実施の形態4に係るポリシー取得部の動作例を示すフローチャート。

[図22]実施の形態4に係る認証情報登録の処理例を示すフローチャート。

[図23]実施の形態4に係る変換パスワードの生成例を示すフローチャート。

[図24]実施の形態4に係る認証の処理例を示すフローチャート。

発明を実施するための形態

[0009] 以下、本開示の実施の形態について、図を用いて説明する。以下の実施の形態の説明及び図面において、同一の符号を付したものは、同一の部分又は相当する部分を示す。

[0010] 実施の形態1.

本実施の形態について、図1から図9を用いて説明する。

構成の説明

図1を用いて、本実施の形態に係るパスワード認証システム1の構成例について説明する。

図1は、本実施の形態に係るパスワード認証システム1の構成例を示す。

パスワード認証システム1は、パスワード認証装置10、端末装置20、

及びネットワーク 30 を備える。

パスワード認証装置 10 は、端末装置 20 を用いて入力されたパスワードを含む認証情報の登録を行う。また、パスワード認証装置 10 は、端末装置 20 を用いて入力されたパスワードを含む認証情報を用いて認証を行う。

なお、パスワード認証装置 10 の動作手順は、パスワード認証方法に相当する。また、パスワード認証装置 10 の動作を実現するプログラムは、パスワード認証プログラムに相当する。

端末装置 20 は、ユーザによる認証情報の入力に用いられる。端末装置 20 の具体例は、パーソナルコンピュータである。

ネットワーク 30 は、データを送受信するための有線又は無線の通信路である。ネットワーク 30 は、具体例としては、Ethernet（登録商標）やWi-Fi（登録商標）といった通信規格に準拠した通信路、又は機器専用の通信路である。

パスワード認証装置 10 と端末装置 20 とは、ネットワーク 30 を介して接続される。

[0011] 本実施の形態に係るパスワード認証システム 1 では、大きく分けて認証情報登録と認証という 2 つのフェーズが存在する。

認証情報登録では、ユーザが端末装置 20 を用いて認証情報をパスワード認証装置 10 に入力する。そして、パスワード認証装置 10 は、ユーザが入力した認証情報を登録情報として登録する。

認証では、ユーザが端末装置 20 を用いて認証情報をパスワード認証装置 10 に入力する。そして、パスワード認証装置 10 は、ユーザが入力した認証情報が、ユーザの登録情報と一致した場合に、ユーザの認証を「成功」と判定する。また、パスワード認証装置 10 は、ユーザが入力した認証情報が、ユーザの登録情報と一致しなかった場合に、ユーザの認証を「失敗」と判定する。

[0012] 図 2 を用いて、本実施の形態に係るパスワード認証装置 10 のハードウェア構成例について説明する。

図2は、本実施の形態に係るパスワード認証装置10のハードウェア構成例を示す。

パスワード認証装置10は、プロセッサ11、メモリ12、補助記憶装置13、入出力インタフェース14、及び通信インタフェース15を備える。

補助記憶装置13には、後述する、ポリシー抽出部100、認証情報取得部101、準拠性判定部102、認証情報登録部103、及び認証情報照合部104の機能を実現するプログラムが記憶されている。

補助記憶装置13に記憶されたポリシー抽出部100、認証情報取得部101、準拠性判定部102、認証情報登録部103、及び認証情報照合部104の機能を実現するプログラムは、メモリ12によりロードされる。また当該プログラムはプロセッサ11に読み出され、実行される。

また、後述する、ポリシー記憶部105、抽出結果記憶部106、認証情報記憶部107、及び登録情報記憶部108は、メモリ12及び補助記憶装置13により実現される。

[0013] 図3を用いて、本実施の形態に係るパスワード認証装置10の機能構成例について説明する。

図3は、本実施の形態に係るパスワード認証装置10の機能構成例を示す。

パスワード認証装置10は、ポリシー抽出部100、認証情報取得部101、準拠性判定部102、認証情報登録部103、及び認証情報照合部104を備える。また、パスワード認証装置10は、ポリシー記憶部105、抽出結果記憶部106、認証情報記憶部107、及び登録情報記憶部108を備える。

[0014] ポリシー記憶部105は、ユーザの認証に用いるパスワードの認定要件を記述した複数のパスワードポリシーを記憶する。

パスワードポリシーは、パスワードが複数のパスワードポリシーのうち少なくともいずれか1つのパスワードポリシーに準拠していればパスワードを正当なパスワードとして認定可能なものである。

より具体的には、1つのパスワードポリシーには、パスワードに使用可能な文字の使用要件が記述される。

ここで「文字」とは、以下を1種類以上含むものとする。

1. 半角英字
2. 半角数字
3. 半角記号

以下では、「文字」が英字、数字、及び記号の3種のみを含む場合について説明する。

しかし、「文字」は、全角英字、全角数字、又は、全角記号を含んでもよい。

また、「文字」は、漢字、かな、又は、カナを含んでもよい。

さらに、「文字」は、アラビア文字、ギリシア文字、又は、その他の外国の文字を含んでもよい。

1つのパスワードポリシーには、英字、数字、及び記号の3種のうち、少なくとも1種の使用要件が記述されていればよい。安全性を向上させるためには、1つのパスワードポリシーには、英字、数字、及び記号の3種のうち、少なくとも2種以上の使用要件が記述されていることが好ましく、さらに、3種すべての使用要件が記述されていることがより好ましい。

パスワードポリシーの具体例は、「8文字以上半角英数字」又は「16文字以上半角英字」である。複数のパスワードポリシーは、これら1つのパスワードポリシーの集合である。ポリシー記憶部105に記憶される複数のパスワードポリシーは、ハードコーディングされ、ポリシー記憶部105に記憶されてもよい。また、入出力インタフェース14を介して取得され、ポリシー記憶部105に記憶されてもよい。また、複数のパスワードポリシーは、通信インタフェース15を介して外部のシステム又はデータベース等から取得され、ポリシー記憶部105に記憶されてもよい。

[0015] ポリシー抽出部100は、ポリシー記憶部105が記憶する複数のパスワードポリシーから1つ以上のパスワードポリシーを抽出し、抽出結果記憶部

１０６に記憶する。以下では、ポリシー抽出部１００が抽出した、１つ以上のパスワードポリシーを抽出ポリシー２００と記す。

認証情報取得部１０１は、通信インタフェース１５を介して、端末装置２０を用いて入力された認証情報を取得し、認証情報記憶部１０７に記憶する。認証情報は、ユーザの認証に用いられる情報であり、少なくともパスワードが含まれる。認証情報の具体例は、「パスワード」又は「ＩＤとパスワードとの組み合わせ」である。

準拠性判定部１０２は、認証情報取得部１０１が取得した認証情報に含まれるパスワードが、ポリシー抽出部１００が抽出した抽出ポリシー２００のうち、少なくともいずれか１つのパスワードポリシーに準拠しているか否かを判定する。

認証情報登録部１０３は、準拠性判定部１０２が少なくともいずれか１つのパスワードポリシーに準拠していると判定したときに、認証情報を登録情報として登録情報記憶部１０８に記憶する。

認証情報照合部１０４は、端末装置２０を用いて入力されたパスワードを含む認証情報を用いてパスワード認証装置１０に登録された登録情報を照会し、認証情報がユーザの認証を行う。

抽出結果記憶部１０６は、ポリシー抽出部１００により記憶された抽出ポリシー２００を記憶する。

認証情報記憶部１０７は、認証情報取得部１０１により記憶された認証情報を記憶する。

登録情報記憶部１０８は、認証情報登録部１０３により記憶された登録情報を記憶する。

[0016] ***動作の説明***

図４を用いて、本実施の形態に係る認証情報登録の処理例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図４は、本実施の形態に係る認証情報登録の処理例を示す。

図４の、ステップＳ１００はポリシー抽出部１００、ステップＳ１１０は

認証情報取得部101、ステップS120からステップS170は準拠性判定部102、ステップS180は認証情報登録部103の処理に対応する。

[0017] ステップS100では、ポリシー抽出部100は、ポリシー記憶部105に記憶された複数のパスワードポリシーのうち、全てのパスワードポリシーを抽出し、抽出結果記憶部106に記憶する。以下では、抽出されたパスワードポリシーを抽出ポリシー200という。

そして、ポリシー抽出部100は、処理が完了したことを準拠性判定部102に通知する。

[0018] 図5は、本実施の形態に係るポリシー記憶部105に記憶される複数のパスワードポリシーの例を示す。

図5では、ポリシー記憶部105に、複数のパスワードポリシーとして、3つのパスワードポリシーが記憶されている。より具体的には、ポリシー記憶部105に記憶されている3つのパスワードポリシーは、以下の3つである。

1. 「8文字以上半角英数字」
2. 「16文字以上半角英字」
3. 「6文字以上半角英字記号」

[0019] 次に、ステップS110では、認証情報取得部101は、端末装置20を用いて入力されたパスワード（以下、入力パスワード201という）を取得し、認証情報記憶部107に記憶する。

そして、認証情報取得部101は、処理が完了したことを準拠性判定部102に通知する。

[0020] 図6は、端末装置20を用いた認証情報登録時の認証情報の入力例である。図6では、端末装置20のGUI（Graphic User Interface）画面に表示された登録フォームで、パスワードの入力が求められている。また、図6では、ユーザが「System!p@ssowrD」を入力した状態を示している。この状態で「OK」を押すと、ネットワーク30を通じてパスワード認証装置10に「System!p@ssowrD」が入力パスワード201として入

力される。以下では、入力パスワード201が「System!p@ssowrD」であるとして説明を続ける。

[0021] 次に、ステップS120では、準拠性判定部102は、ポリシー抽出部100及び認証情報取得部101から処理の完了通知を待つ。

そして、ポリシー抽出部100及び認証情報取得部101から通知を受ければ、準拠性判定部102は、抽出結果記憶部106から抽出ポリシー200を、認証情報記憶部107から入力パスワード201「System!p@ssowrD」を読み込む。

そして、準拠性判定部102は、読み込んだ全ての抽出ポリシー200のステータスを「未選択」とする。

[0022] 次に、ステップS130では、準拠性判定部102は、全ての抽出ポリシー200のうち、「未選択」のステータスである抽出ポリシー200が存在するか否かを確認する。

[0023] 次に、ステップS140では、準拠性判定部102が「未選択」のステータスである抽出ポリシー200が存在することを確認すれば、処理はステップS150へ進む。

一方、準拠性判定部102が「未選択」のステータスである抽出ポリシー200が存在しないことを確認すれば、入力パスワード201「System!p@ssowrD」は全ての抽出ポリシー200のいずれにも準拠していない判定する。そして、処理がステップS110に戻る。

[0024] 次に、ステップS150では、準拠性判定部102は、「未選択」のステータスである抽出ポリシー200のうち、1つの抽出ポリシー200を選択する。以下では、選択した抽出ポリシー200を選択ポリシーという。

そして、準拠性判定部102は、選択ポリシーのステータスを「選択」とする。

[0025] 次に、ステップS160では、準拠性判定部102は、入力パスワード201「System!p@ssowrD」が選択ポリシーに準拠しているか否かを確認する。

より具体的には、準拠性判定部102は、選択ポリシーに記述されたパス

ワードの認定要件を確認する。そして、準拠性判定部 102 は、入力パスワード 201 が選択ポリシーに記述されたパスワードの認定要件を満たしているか否かを確認する。

[0026] 次に、ステップ S 170 では、準拠性判定部 102 は、入力パスワード 201 「System!p@ssowrD」が、抽出ポリシー 200 のうち、いずれか一つのパスワードポリシーである選択ポリシーに準拠しているか否かを判定する。

より具体的には、準拠性判定部 102 が、入力パスワード 201 「System!p@ssowrD」が選択ポリシーに記述されたパスワードの認定要件を満たしていることを確認すれば、選択ポリシーに「準拠している」と判定する。そして、入力パスワード 201 「System!p@ssowrD」は正当なパスワードと認定される。

また、準拠性判定部 102 が、入力パスワード 201 「System!p@ssowrD」が選択ポリシーに記述されたパスワードの認定要件を満たしていないことを確認すれば、「準拠していない」と判定する。そして、入力パスワード 201 「System!p@ssowrD」は正当なパスワードと認定されない。

そして、準拠性判定部 102 は、処理が完了したことを認証情報登録部 103 に通知する。

[0027] 以下に具体例を用いて、準拠性判定部 102 による入力パスワード 201 「System!p@ssowrD」が選択ポリシーに準拠しているか否かの判定を説明する。

入力パスワード 201 が「System!p@ssowrD」で、且つ選択ポリシーが「6 文字以上半角英字記号」である場合、「System!p@ssowrD」は「6 文字以上半角英字記号」であるため、パスワードの認定要件を満たしている。したがって、準拠性判定部 102 は「準拠している」と判定する。

また、別の例として、入力パスワード 201 が「hell0hell0」で、且つ選択ポリシーのパスワードが「8 文字以上半角英数字」である場合、「hell0hell0」は「8 文字以上半角英数字」であるため、パスワードの認定要件を満たしている。したがって、準拠性判定部 102 は「準拠している」と判定する。

。

また、別の例として、入力したパスワードが「hell0」で、且つ選択ポリシーが「8文字以上半角英数字」である場合、「hell0」は「8文字以上半角英数字」でないため、パスワードの認定要件を満たさない。したがって、準拠性判定部102は「準拠していない」と判定する。

準拠性判定部102が「準拠している」と判定した場合、準拠性判定部102は認証情報登録部103に処理の完了を通知する。そして処理はステップS180へ進む。

一方、準拠性判定部102が「準拠していない」と判定した場合、処理はステップS130に戻る。

[0028] 次に、ステップS180では、認証情報登録部103は、準拠性判定部102から処理完了の通知を待つ。

認証情報登録部103が準拠性判定部102から処理完了の通知を受けた場合、認証情報登録部103は、認証情報記憶部107に記憶された認証情報である入力パスワード201「System!p@ssowrD」を読み込む。そして、認証情報登録部103は、登録情報記憶部108に登録情報として記憶する。そして、認証情報登録の処理が完了する。

[0029] 図7を用いて、本実施の形態に係る認証の処理例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図7は、本実施の形態に係る認証情報登録の処理例を示す。

図7の、ステップS200は認証情報取得部101、ステップS210からステップS230は認証情報照合部104の処理に対応する。

[0030] ステップS200では、認証情報取得部101は、端末装置20を用いて入力された入力パスワード201を取得し、認証情報記憶部107に記憶する。

そして、認証情報取得部101は、処理が完了したことを認証情報照合部104に通知する。

図8は、端末装置20を用いた認証時の認証情報の入力例である。図8で

は、端末装置 20 の GUI 画面に表示された認証フォームで、パスワード入力が求められている。また、図 8 では、ユーザが「System!p@ssowrD」を入力した状態を示している。この状態で「OK」を押すと、ネットワーク 30 を通じてパスワード認証装置 10 に「System!p@ssowrD」が入力パスワード 201 として入力される。以下では、入力パスワード 201 が「System!p@ssowrD」であるとして説明を続ける。

[0031] 次に、ステップ S 210 では、認証情報照合部 104 は、認証情報取得部 101 から処理完了の通知を待つ。

そして、認証情報照合部 104 が認証情報取得部 101 から処理完了の通知を受けた場合、登録情報記憶部 108 から登録情報であるパスワード（以下、登録パスワード 202 という）を読み込む。以下では、登録パスワード 202 が「System!p@ssowrD」であるとして説明を続ける。

認証情報照合部 104 は、読み込んだ登録パスワード 202 と入力パスワード 201 とを確認する。

[0032] 次に、ステップ S 220 では、認証情報照合部 104 は、読み込んだ登録パスワード 202 と入力パスワード 201 とが一致するか否かを判定する。

そして、認証情報照合部 104 が登録パスワード 202 と入力パスワード 201 とが一致すると判定した場合、処理がステップ S 230 へ進む。

そして、認証情報照合部 104 が登録パスワード 202 と入力パスワード 201 とが一致しないと判定した場合、処理がステップ S 200 に戻る。

本例では、登録パスワード 202 「System!p@ssowrD」と入力パスワード 201 「System!p@ssowrD」とが一致するため、処理がステップ S 230 へ進む。

[0033] 次に、ステップ S 230 では、認証情報照合部 104 は認証を成功とする。そして、認証の処理が完了する。

[0034] ***実施の形態の効果の説明***

以上のように、本実施の形態に係るパスワード認証装置は、複数のパスワードポリシーを記憶する。そして、ユーザ自身のパスワードの生成方針に沿

って入力された入力パスワード201が、複数のパスワードポリシーから抽出された抽出ポリシー200のいずれかに準拠すれば、正当なパスワードとして認定され、登録情報として登録される。つまり、秘密情報である変換パターンを用いない。したがって、パスワードポリシーに準拠し、且つユーザー自身のパスワードの生成方針に沿った安全なパスワード生成を可能とすることができる。

[0035] <変形例1>

実施の形態1では、パスワード認証システムは、パスワード認証装置10、端末装置20、及びネットワーク30を備えると説明した。また、パスワード認証装置10は、端末装置20を用いて入力された認証情報を用いて認証情報登録及び認証を行うと説明した。

しかし、それに限らず、パスワード認証装置10は、入出力インタフェース14を介して入力された認証情報を用いて認証情報登録及び認証を行ってもよい。

より具体的には、図4のステップS110では、認証情報取得部101は、出力装置のGUI画面に表示された登録フォームに、入力装置を用いて入力されたパスワードを取得し、認証情報記憶部107に記憶してもよい。

また、図7のステップS200では、認証情報取得部101は、出力装置のGUI画面に表示された認証フォームに、入力装置を用いて入力されたパスワードを取得し、認証情報記憶部107に記憶してもよい。

したがって、パスワード認証システムは、端末装置20及びネットワーク30を備えなくてもよい。

[0036] <変形例2>

実施の形態1では、図6を用いて、端末装置20のGUI画面に表示された登録フォームで、パスワードの入力が求められる例を説明した。

しかし、パスワード入力の要求は、それに限らず、認証情報取得部101が端末装置20に、端末装置20のGUI画面に抽出ポリシー200を表示させてパスワードの入力を求めてもよい。

より具体的には、図4のステップS110では、認証情報取得部101は、抽出結果記憶部106から抽出ポリシー200を読み込み、通信インタフェース15を介して、抽出ポリシー200を端末装置20に送信する。そして、認証情報取得部101は、端末装置20に、端末装置20のGUI画面に抽出ポリシー200を表示させ、ユーザにパスワードの入力を求めてもよい。

図9は、認証情報登録時に抽出ポリシー200を表示した認証情報の入力例である。図9では、端末装置20のGUI画面に抽出ポリシー200が表示された登録フォームで、パスワードの入力が求められている。また、図9では、ユーザが「ポリシー3：6文字以上半角英字記号」に準拠した「System!p@ssowrD」を入力した状態を示している。この状態で「OK」を押すと、ネットワーク30を通じてパスワード認証装置10に「System!p@ssowrD」が入力パスワード201として入力される。

[0037] 実施の形態2.

実施の形態1では、ポリシー抽出部100が、ポリシー記憶部105に記憶された複数のパスワードポリシーのうち、全てのパスワードポリシーを抽出ポリシー200として抽出した。しかし、ポリシー記憶部105に大量の複数のパスワードポリシーを記憶させた上で、ポリシー抽出部100にパスワードポリシーの強度を計算させ、要求強度を満たすパスワードポリシーのみを抽出させるという運用も可能である。

本実施の形態では、ポリシー記憶部105に記憶された大量の複数のパスワードポリシーから、ポリシー抽出部100がパスワードポリシーの強度を計算し、要求強度を満たすパスワードポリシーのみを抽出する例を説明する。

[0038] なお、パスワードポリシーの強度とは、パスワードポリシーにより定まるパスワードの安全性を評価する尺度である。パスワードポリシーの強度の具体例は、パスワードポリシーにより定まるパスワードの文字（英字、数字、及び記号）の組み合わせの総数を示すパスワード総数（パスワード空間とも

いう)である。

より具体的には、 m 種類の文字(英字、数字、及び記号)から、 n 文字のパスワードが作られるとき、パスワード空間は m^n で計算される。ここで「 $^$ 」はべき乗を示す。

「8文字以上半角小文字英字及び半角数字」というパスワードポリシーの具体例を用いてパスワード空間を説明する。

半角小文字英字($a\sim z$)と半角数字($0\sim 9$)とは合わせて計36種類の文字がある。そして、最低の文字数は、8文字である。したがって、「8文字以上半角小文字英字及び半角数字」というパスワードポリシーの場合、 36^8 が最低のパスワード空間であり、パスワードポリシーの強度である。

[0039] また、要求強度とは、複数のパスワードポリシーから、抽出ポリシー200を抽出するために用いられる基準である。要求強度の具体例は、「パスワード空間が 36^8 以上」である。また、別の具体例として、「“半角小文字英字と半角数字とから構成される8文字以上”というパスワードポリシーのパスワード空間以上」のように、特定のパスワードポリシーを利用してもよい。

[0040] 本実施の形態について、図10から図13を用いて説明する。

本実施の形態では、主に実施の形態1との差異を説明する。

なお、以下で説明していない事項は、実施の形態1と同様である。

[0041] ***構成の説明***

本実施の形態に係るパスワード認証システムの構成及びパスワード認証装置10のハードウェア構成は、実施の形態1と同一の構成であるため、説明を省略する。

図10を用いて、本実施の形態に係るパスワード認証装置10の機能構成例について説明する。

図10は、本実施の形態に係るパスワード認証装置10の機能構成例を示す。

なお、実施の形態1と同一構成部分には同一番号を付してその説明を省略

する。

[0042] 本実施の形態に係るパスワード認証装置 10 は、新たに抽出要件記憶部 109 を備える。

抽出要件記憶部 109 は、複数のパスワードポリシーからパスワードポリシーを抽出するために用いられる抽出要件を記憶する。抽出要件の具体例は、要求強度である。以下では、抽出要件記憶部 109 が記憶する要求強度を、要求強度 203 と記す。

抽出要件記憶部 109 に記憶される要求強度 203 は、ハードコーディングされ、抽出要件記憶部 109 に記憶されてもよい。また、要求強度 203 は、入出力インタフェース 14 を介して取得され、抽出要件記憶部 109 に記憶されてもよい。また、要求強度 203 は、通信インタフェース 15 を介して外部のシステム又はデータベース等から取得され、抽出要件記憶部 109 に記憶されてもよい。

抽出要件記憶部 109 は、メモリ 12 及び補助記憶装置 13 により実現される。

[0043] また、本実施の形態に係るポリシー抽出部 100 は、ポリシー記憶部 105 に記憶された複数のパスワードポリシーの各々のパスワードポリシーのパスワード空間を計算する。また、ポリシー抽出部 100 は、抽出要件記憶部 109 に記憶された要求強度 203 を読み込む。そして、ポリシー抽出部 100 は、各々のパスワードポリシーのパスワード空間と要求強度 203 とを用いて複数のパスワードポリシーから抽出ポリシー 200 を抽出し、抽出結果記憶部 106 に記憶する。

[0044] ***動作の説明***

図 11 を用いて、本実施の形態に係る認証情報登録の処理例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図 11 は、本実施の形態に係る認証情報登録の処理例を示す。

なお、実施の形態 1 と同一の動作には同一番号を付してその説明を省略する。

図 1 1 の、ステップ S 1 0 0 からステップ S 3 7 0 はポリシー抽出部 1 0 0 の処理に対応する。

[0045] ステップ S 1 0 0 は、実施の形態 1 と同一の動作であるため、説明を省略する。

図 1 2 は、本実施の形態に係るポリシー記憶部 1 0 5 に記憶される複数のパスワードポリシーの例を示す。

図 1 2 では、ポリシー記憶部 1 0 5 に、複数のパスワードポリシーとして、4 つのパスワードポリシーが記憶されていることが示されている。より具体的には、ポリシー記憶部 1 0 5 に記憶されている 4 つのパスワードポリシーは、以下の 4 つである。

1. 「8 文字以上半角英数字」
2. 「1 6 文字以上半角英字」
3. 「6 文字以上半角英字記号」
4. 「4 桁半角数字」

[0046] ステップ S 1 0 0 の後、ステップ S 3 0 0 では、ポリシー抽出部 1 0 0 は、抽出要件記憶部 1 0 9 に記憶された要求強度 2 0 3 を読み込む。

以下では、要求強度 2 0 3 の具体例として、「パスワード空間が 1 0 0, 0 0 0 以上」がポリシー抽出部 1 0 0 に読み込まれる例を説明する。

[0047] 次に、ステップ S 3 1 0 では、ポリシー抽出部 1 0 0 は、全ての抽出ポリシー 2 0 0 のステータスを「未選択」とする。

[0048] 次に、ステップ S 3 2 0 では、ポリシー抽出部 1 0 0 は、全ての抽出ポリシー 2 0 0 のうち、「未選択」のステータスである抽出ポリシー 2 0 0 が存在するか否かを確認する。

[0049] 次に、ステップ S 3 3 0 では、ポリシー抽出部 1 0 0 が、全ての抽出ポリシー 2 0 0 のうち、「未選択」のステータスである抽出ポリシー 2 0 0 が存在することを確認すれば、処理はステップ S 3 4 0 へ進む。

一方、ポリシー抽出部 1 0 0 が、全ての複数のパスワードポリシーのうち、「未選択」のステータスであるパスワードポリシーが存在しないことを確

認すれば、ポリシー抽出部 100 は、後述の強度確認ポリシーを用いて、抽出結果記憶部 106 に記憶された抽出ポリシー 200 を更新する。そして、ポリシー抽出部 100 は、処理が完了したことを準拠性判定部 102 に通知する。そして、処理は図 4 のステップ S 110 へ進む。なお、図 4 のステップ S 110 へ進んだ以降の動作は、実施の形態 1 の動作と同一の動作であるため、説明を省略する。

[0050] 次に、ステップ S 340 では、ポリシー抽出部 100 は、「未選択」のステータスである抽出ポリシー 200 のうち、1 つの抽出ポリシー 200 を選択する。以下ではポリシー抽出部 100 が選択した抽出ポリシー 200 を強度確認ポリシーという。

そして、ポリシー抽出部 100 は、強度確認ポリシーのステータスを「選択」とする。

[0051] 次に、ステップ S 350 では、ポリシー抽出部 100 は、強度確認ポリシーのパスワードポリシーの強度を計算する。より具体的には、ポリシー抽出部 100 は、強度確認ポリシーに記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件により定まるパスワードの文字（英字、数字、及び記号）の組み合わせの総数を示すパスワード空間を計算する。

そして、ポリシー抽出部 100 は、要求強度 203 のパスワード空間を確認する。

本例では、要求強度 203 は、「パスワード空間が 100, 000 以上」であるため、要求強度 203 のパスワード空間は 100, 000 以上である。

また、別の例として、要求強度 203 が「“8 文字以上半角小文字英字及び半角数字” というパスワードポリシーのパスワード空間以上」のように特定のパスワードポリシーを利用したものであれば、ポリシー抽出部 100 は、要求強度 203 のパスワード空間を計算し、確認する。

[0052] 次に、ステップ S 360 では、ポリシー抽出部 100 は、強度確認ポリシーのパスワードポリシーの強度が要求強度 203 を満たしているか否かを判

定する。

ポリシー抽出部100が強度確認ポリシーのパスワードポリシーの強度は要求強度203を満たしていると判定した場合、処理はステップS370へ進む。

一方、ポリシー抽出部100が強度確認ポリシーのパスワードポリシーの強度は要求強度203を満たしていないと判定した場合、処理はステップS320に戻る。

半角英字は、大文字英字A～Z、及び小文字英字a～zの52種類の文字である。また、半角数字は、0～9の10種類の数字である。また、記号は、便宜上、32種類の記号とする。

つまり、図12に示す4つの複数のパスワードポリシーの各々のパスワード空間は、以下の通り計算される。

1. 「8文字以上半角英数字」の場合、 62^8 （なお、 $62^8 > 100,000$ ）。
2. 「16文字以上半角英字」の場合、 52^{16} （なお、 $52^{16} > 100,000$ ）。
3. 「6文字以上半角英字記号」の場合、 84^6 （なお、 $84^6 > 100,000$ ）。
4. 「4桁半角数字」の場合、 10^4 （なお、 $10^4 < 100,000$ ）。

したがって、上記4つの複数のパスワードポリシーのうち、（1）、（2）、（3）は要求強度203を満たす。また、上記4つの複数のパスワードポリシーのうち、（4）は要求強度203を満たさない。

[0053] 次に、ステップS370では、ポリシー抽出部100は、抽出ポリシー200の更新に用いるため、強度確認ポリシーを記憶する。

図13は、本実施の形態に係る抽出結果記憶部106に記憶される抽出ポリシー200の例を示す。

図13では、図12の複数のパスワードポリシーのうち、抽出結果記憶部

106に、抽出ポリシー200として、3つのパスワードポリシーが記憶されていることが示されている。より具体的には、抽出結果記憶部106に記憶されている3つのパスワードポリシーは、以下の3つである。

1. 「8文字以上半角英数字」
2. 「16文字以上半角英字」
3. 「6文字以上半角英字記号」

[0054] ***実施の形態の効果の説明***

以上のように、本実施の形態によれば、パスワード認証装置は、大量に用意された複数のパスワードポリシーから、要求強度を満たすパスワードポリシーのみを抽出する。そして、パスワード認証装置は、認証情報登録時に抽出したパスワードポリシーを用いてパスワードを認定し、登録情報として登録する。つまり、パスワード認証装置は、秘密情報である変換パターンを用いない。したがって、パスワードポリシーに準拠し、且つユーザ自身のパスワードの生成方針に沿った安全なパスワード生成を可能とすることができる。

さらに、パスワード認証装置の管理者は、予め大量に複数のパスワードポリシーを用意しておけば、抽出要件を変更するだけで認証情報登録時に登録が認められるパスワードの安全性の基準を調整することができる。つまり、パスワード認証装置の管理者が、認証情報登録時に登録が認められるパスワードの安全性の基準を調整する都度、複数のパスワードポリシーを用意する必要がなくなる。したがって、パスワード認証装置の管理者が認証情報登録時に登録が認められるパスワードの安全性の基準を調整するために複数のパスワードポリシーを用意しなければいけない手間を削減することが可能である。

[0055] 実施の形態3.

実施の形態1では、入力パスワード201が、抽出結果記憶部106に記憶された抽出ポリシー200のうち、どの抽出ポリシー200に準拠するかを一つ一つ確認するという方法がとられていた。しかし、図9のように抽出

ポリシー２００をユーザに提示した際に、提示した抽出ポリシー２００のうち、ユーザに抽出ポリシー２００を選択させることも可能である。

本実施の形態では、認証情報取得部１０１が、端末装置２０に、端末装置２０のＧＵＩ画面に抽出ポリシー２００を表示させ、パスワードの入力と共に利用する抽出ポリシー２００の選択を求める例を説明する。

本実施の形態について、図１４から図１８を用いて説明する。

本実施の形態では、主に実施の形態１との差異を説明する。

なお、以下で説明していない事項は、実施の形態１と同様である。

[0056] ***構成の説明***

本実施の形態に係るパスワード認証システムの構成及びパスワード認証装置１０のハードウェア構成は、実施の形態１及び実施の形態２と同一の構成であるため、説明を省略する。

次に、図１４を用いて、本実施の形態に係るパスワード認証装置１０の機能構成例について説明する。

図１４は、本実施の形態に係るパスワード認証装置１０の機能構成例を示す。

なお、実施の形態１と同一構成部分には同一番号を付してその説明を省略する。

[0057] 本実施の形態に係るパスワード認証装置１０の機能構成は、実施の形態１と同一の構成である。ただし、認証情報取得部１０１、準拠性判定部１０２、及び準拠性判定部１０２の動作が異なる。

本実施の形態に係る認証情報取得部１０１は、認証情報登録時に、ポリシー抽出部１００が抽出した１つ以上のパスワードポリシーである抽出ポリシー２００を認証情報の入力画面に表示する。より具体的には、認証情報取得部１０１は、端末装置２０に、端末装置２０のＧＵＩ画面に抽出ポリシー２００を表示させることで、抽出ポリシー２００を認証情報の入力画面に表示する。そして、認証情報取得部１０１は、表示された抽出ポリシー２００のうち、ユーザにより選択されたパスワードポリシーを、ユーザポリシー２０

4として取得する。

また、認証情報取得部101は、認証情報登録時に、登録情報記憶部108に記憶されたユーザポリシー204を認証情報の入力画面に表示する。より具体的には、認証情報取得部101は、端末装置20に、端末装置20のGUI画面にユーザポリシー204を表示させることで、ユーザポリシー204を認証情報の入力画面に表示する。

本実施の形態に係る準拠性判定部102は、認証情報取得部101が取得した認証情報に含まれる入力パスワード201が、ユーザポリシー204に準拠しているか否かを判定する。

本実施の形態に係る認証情報登録部103は、準拠性判定部102が認証情報に含まれる入力パスワード201はユーザポリシー204に準拠していると判定したときに、認証情報及びユーザポリシー204を登録情報として登録する。

[0058] ***動作の説明***

図15を用いて、本実施の形態に係る認証情報登録の処理例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図15は、本実施の形態に係る認証情報登録の処理例を示す。

なお、実施の形態1と同一の動作には同一番号を付してその説明を省略する。

図15の、ステップS100がポリシー抽出部100、ステップS400が認証情報取得部101、ステップS410及びステップS420が準拠性判定部102、ステップS180及びステップS430が認証情報登録部103の処理に対応する。

[0059] ステップS100は、実施の形態1と同一の動作であるため、説明を省略する。

[0060] ステップS100の後、ステップS400では、認証情報取得部101は、抽出結果記憶部106から抽出ポリシー200を読み込む。そして、認証情報取得部101は、通信インタフェース15を介して、端末装置20に抽

出ポリシー２００を送信する。そして、認証情報取得部１０１は、端末装置２０に、端末装置２０のＧＵＩ画面に抽出ポリシー２００を表示させる。そして、認証情報取得部１０１は、端末装置２０を用いて入力された入力パスワード２０１及び選択されたユーザポリシー２０４を取得し、認証情報記憶部１０７に記憶する。

そして、認証情報取得部１０１は、処理が完了したことを準拠性判定部１０２に通知する。

[0061] 図１６は、端末装置２０を用いた認証情報登録時のユーザポリシー２０４の選択例である。図１６では、端末装置２０のＧＵＩ画面に抽出ポリシー２００が表示された登録フォームで、ユーザポリシー２０４の選択が求められている。また、図１６では、ユーザが「ポリシー３：６文字以上半角英字記号」を選択した状態を示している。この状態で「ＯＫ」を押すと、ネットワーク３０を通じてパスワード認証装置１０に「６文字以上半角英字記号」がユーザポリシー２０４として入力される。

[0062] 次に、ステップＳ４１０では、準拠性判定部１０２は、認証情報取得部１０１からの通知を待つ。

そして、ポリシー抽出部１００及び認証情報取得部１０１から通知を受ければ、準拠性判定部１０２は、認証情報記憶部１０７から入力パスワード２０１及びユーザポリシー２０４を読み込む。

そして、準拠性判定部１０２は、入力パスワード２０１がユーザポリシー２０４に準拠しているか否かを確認する。

より具体的には、準拠性判定部１０２は、ユーザポリシー２０４に記述されたパスワードの認定要件を確認する。そして、準拠性判定部１０２は、入力パスワード２０１がユーザポリシー２０４に記述されたパスワードの認定要件を満たしているか否かを確認する。

[0063] 次に、ステップＳ４２０では、準拠性判定部１０２は、入力パスワード２０１がユーザポリシー２０４に準拠しているか否かを判定する。

より具体的には、準拠性判定部１０２が、入力パスワード２０１がユーザ

ポリシー 204 に記述されたパスワードの認定要件を満たしていることを確認すれば、「準拠している」と判定する。そして、入力パスワード 201 は正当なパスワードと認定される。

また、準拠性判定部 102 が、入力パスワード 201 がユーザポリシー 204 に記述されたパスワードの認定要件を満たしていないことを確認すれば、「準拠していない」と判定する。そして、入力パスワード 201 は正当なパスワードと認定されない。

準拠性判定部 102 が「準拠している」と判定した場合、準拠性判定部 102 は認証情報登録部 103 に処理の完了を通知する。そして処理はステップ S180 へ進む。

一方、準拠性判定部 102 が「準拠していない」と判定した場合、処理はステップ S400 に戻る。

[0064] ステップ S180 は、実施の形態 1 と同一の動作であるため、説明を省略する。

[0065] 次に、ステップ S430 では、認証情報登録部 103 は、認証情報記憶部 107 に記憶されたユーザポリシー 204 を読み込み、登録情報記憶部 108 に登録情報として記憶する。そして、認証情報登録の処理が完了する。

[0066] 図 17 を用いて、本実施の形態に係る認証の処理例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図 17 は、本実施の形態に係る認証情報登録の処理例を示す。

なお、実施の形態 1 と同一の動作には同一番号を付してその説明を省略する。

図 17 の、ステップ S500 及びステップ S510 は認証情報取得部 101、ステップ S210 からステップ S230 は認証情報照合部 104 の処理に対応する。

[0067] ステップ S500 では、認証情報取得部 101 は、登録情報記憶部 108 からユーザポリシー 204 を読み込む。

以下では、認証情報取得部 101 が、ユーザポリシー 204 として「6 文

字以上半角英字記号」を読み込んだものとして説明を行う。

[0068] 次に、ステップS 5 1 0では、認証情報取得部1 0 1は、端末装置2 0に、端末装置2 0のG U I画面にユーザポリシー2 0 4表示させることで、ユーザポリシー2 0 4に準拠した入力パスワード2 0 1を取得する。

より具体的には、認証情報取得部1 0 1は、通信インタフェース1 5を介して、端末装置2 0にユーザポリシー2 0 4を送信する。そして、認証情報取得部1 0 1は、端末装置2 0に、端末装置2 0のG U I画面にユーザポリシー2 0 4を表示させる。そして、認証情報取得部1 0 1は、端末装置2 0を用いて入力された入力パスワード2 0 1を取得し、認証情報記憶部1 0 7に記憶する。

そして、認証情報取得部1 0 1は、処理が完了したことを準拠性判定部1 0 2に通知する。

[0069] 図1 8は、本実施の形態に係る、端末装置2 0を用いた認証時の認証情報の入力例である。図1 8では、端末装置2 0のG U I画面に表示された認証フォームで、パスワード入力が求められている。また、端末装置2 0のG U I画面に表示された認証フォームで、ユーザポリシー2 0 4である「6文字以上半角英字記号」が表示されている。また、図1 8では、ユーザが「System!p@ssowrD」を入力した状態を示している。この状態で「OK」を押すと、ネットワーク3 0を通じてパスワード認証装置1 0に「System!p@ssowrD」が入力パスワード2 0 1として入力される。

[0070] 次に、ステップS 5 2 0では、認証情報照合部1 0 4は、認証情報取得部1 0 1から処理完了の通知を待つ。

そして、認証情報照合部1 0 4が認証情報取得部1 0 1から処理完了の通知を受けた場合、登録情報記憶部1 0 8から登録情報である登録パスワード2 0 2を読み込む。

認証情報照合部1 0 4は、読み込んだ登録パスワード2 0 2と入力パスワード2 0 1とを確認する。

[0071] ステップS 2 1 0からステップS 2 3 0は、実施の形態1と同一の動作で

あるため、説明を省略する。そして、認証情報登録の処理が完了する。

[0072] ***実施の形態の効果の説明***

以上のように、本実施の形態によれば、パスワード認証装置は、認証情報登録時に、複数のパスワードポリシーの中から、ユーザに使用したいパスワードポリシーを選択させる。そして、パスワード認証装置は、パスワードを含む認証情報と共にユーザが選択したパスワードポリシーを取得し、登録情報として登録する。つまり、パスワード認証装置は、秘密情報である変換パターンを用いない。したがって、パスワードポリシーに準拠し、且つユーザ自身のパスワードの生成方針に沿った安全なパスワード生成を可能とすることができる。

さらに、ユーザは、認証時において、端末装置のGUIに表示された、認証情報登録時に自身が選択したパスワードポリシーを確認しながらパスワードを入力することができる。したがって、ユーザの利便性が高めることができる。

[0073] 実施の形態4.

実施の形態1から実施の形態3では、パスワード認証システム1で、パスワード認証装置10が、認証情報登録及び認証を行う例を説明した。

しかし、パスワード認証システム1に別のパスワード認証システムが存在し、認証情報登録及び認証を行う場合もある。そして、別のパスワード認証システムが認証情報登録及び認証に使用するパスワードポリシーを指定し、パスワードポリシーの変更又は追加等が出来ない場合もある。そして、そのような場合、実施の形態1から実施の形態3のように、ユーザ自身のパスワードの生成方針に沿ったパスワード生成を実現することが出来ない可能性がある。

そこで、本実施の形態では、パスワード認証装置10が、別のパスワード認証システムの認証情報登録及び認証時に、ユーザが入力する認証情報の仲介を行う例を説明する。

本実施の形態について、図19から図24を用いて説明する。

本実施の形態では、主に実施の形態 2 との差異を説明する。

なお、以下で説明していない事項は、実施の形態 2 と同様である。

[0074] ***構成の説明***

本実施の形態に係るパスワード認証装置 10 のハードウェア構成は、実施の形態 1 と同一の構成であるため、説明を省略する。

図 19 を用いて、本実施の形態に係るパスワード認証システム 1 の構成例について説明する。

図 19 は、本実施の形態に係るパスワード認証システム 1 の構成例を示す。

パスワード認証システム 1 は、パスワード認証装置 10、端末装置 20、及びネットワーク 30 に加え、新たに外部認証システム 40 を備える。

[0075] 本実施の形態に係るパスワード認証装置 10 は、端末装置 20 を用いて入力された認証情報に含まれるパスワードを変換し、変換パスワード 207 を生成する。そして、パスワード認証装置 10 は、認証情報登録時及び認証時に、変換パスワード 207 を含む認証情報を外部認証システム 40 に入力する。

外部認証システム 40 は、パスワード認証装置 10 の外部で、ユーザの認証を行う。より具体的には、外部認証システム 40 は、パスワード認証装置 10 の外部で、パスワード認証装置 10 が生成した変換パスワード 207 を含む認証情報の登録を行う。また、外部認証システム 40 は、パスワード認証装置 10 の外部で、パスワード認証装置 10 が生成した変換パスワード 207 を含む認証情報を用いて認証を行う。

パスワード認証装置 10 と端末装置 20 とは、ネットワーク 30 を介して接続される。また、パスワード認証装置 10 と外部認証システム 40 とは、ネットワーク 30 を介して接続される。

[0076] 図 20 を用いて、本実施の形態に係るパスワード認証装置 10 の機能構成例について説明する。

図 20 は、本実施の形態に係るパスワード認証装置 10 の機能構成例を示

す。

なお、実施の形態 2 及び実施の形態 3 と同一構成部分には同一番号を付してその説明を省略する。

本実施の形態に係るパスワード認証装置 10 は、新たにポリシー取得部 110 及び取得ポリシー記憶部 112 を備える。また、パスワード認証装置 10 は、認証情報照合部 104 に代わり、認証情報仲介部 111 を備える。

[0077] ポリシー取得部 110 は、パスワード認証装置 10 の外部で認証を行う外部認証システム 40 がユーザの認証に用いるパスワードポリシーを取得ポリシー 205 として取得し、取得ポリシー記憶部 112 に記憶する。そして、ポリシー取得部 110 は、取得ポリシー 205 により定まるパスワードの文字（英字、数字、及び記号）の組み合わせの総数を示す取得ポリシー 205 のパスワード総数を計算し、計算結果を要求強度 203 として抽出要件記憶部 109 に記憶する。以下では、取得ポリシー 205 により定まるパスワードの文字（英字、数字、及び記号）の組み合わせの総数を示す取得ポリシー 205 のパスワード総数を組み合わせ総数 206 と記す。

認証情報仲介部 111 は、認証情報登録時に、登録情報記憶部 108 から登録情報を読み込み、登録情報に含まれる登録パスワード 202 を取得ポリシー 205 に準拠する変換パスワード 207 へと変換する。そして、認証情報仲介部 111 は、登録情報及び変換パスワード 207 を用いて、外部認証システム 40 に、外部認証システム 40 の認証に用いられる認証情報を入力する。

また、認証情報仲介部 111 は、認証時に、認証情報記憶部 107 から認証情報を読み込み、認証情報に含まれる入力パスワード 201 を取得ポリシー 205 に準拠する変換パスワード 207 へと変換する。そして、認証情報仲介部 111 は、認証情報及び変換パスワード 207 を用いて、外部認証システム 40 に、外部認証システム 40 の認証に用いられる認証情報を入力する。

また、本実施の形態に係る認証情報取得部 101、準拠性判定部 102、

及び準拠性判定部 102 は、実施の形態 3 と同一の動作を行う。また、図 20 の認証情報取得部 101、準拠性判定部 102、及び準拠性判定部 102 以外の構成部分は、実施の形態 2 と同一の動作を行う。

取得ポリシー記憶部 112 は、ポリシー取得部 110 が取得した取得ポリシー 205 を記憶する。

ポリシー取得部 110 及び認証情報仲介部 111 を実現するプログラムは補助記憶装置 13 に記憶されている。

補助記憶装置 13 に記憶されたポリシー取得部 110 及び認証情報仲介部 111 を実現するプログラムは、メモリ 12 によりロードされる。また当該プログラムはプロセッサ 11 に読み出され、実行される。

取得ポリシー記憶部 112 は、メモリ 12 及び補助記憶装置 13 により実現される。

[0078] ***動作の説明***

図 21 を用いて、本実施の形態に係るポリシー取得部 110 の動作例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図 21 は、本実施の形態に係るポリシー取得部 110 の動作例を示す。

本実施の形態に係るポリシー取得部 110 の動作は、認証情報登録の処理の前に行われる。

[0079] ステップ S600 では、ポリシー取得部 110 は、通信インタフェース 15 を介して、外部認証システム 40 からユーザの認証に用いるパスワードポリシーを取得ポリシー 205 として取得する。そして、ポリシー取得部 110 は、取得ポリシー 205 を取得ポリシー記憶部 112 に記憶する。

[0080] 次に、ステップ S610 では、ポリシー取得部 110 は、取得ポリシー 205 のパスワードポリシーの強度を計算し、計算結果を要求強度 203 として抽出要件記憶部 109 に記憶する。

具体的には、ポリシー取得部 110 は、取得ポリシー 205 に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件により定

まるパスワードの文字（英字、数字、及び記号）の組み合わせの総数を示す組み合わせ総数206を計算する。

そして、ポリシー取得部110は、組み合わせ総数206を要求強度203として抽出要件記憶部109に記憶する。そして、ポリシー取得部110の処理が完了する。

[0081] 図22を用いて、本実施の形態に係る認証情報登録の処理例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図22は、本実施の形態に係る認証情報登録の処理例を示す。

なお、実施の形態2及び実施の形態3と同一の動作には同一番号を付してその説明を省略する。

図22の、ステップS100からステップS370及びステップS700がポリシー抽出部100、ステップS400が認証情報取得部101、ステップS410及びステップS420が準拠性判定部102の処理に対応する。また、ステップS180及びステップS430が認証情報登録部103、ステップS710及びステップS720が認証情報仲介部111の処理に対応する。

[0082] ステップS100からステップS320は、実施の形態2と同一の動作であるため、説明を省略する。

[0083] ステップS320の後、ステップS700では、ポリシー抽出部100が、全ての抽出ポリシー200のうち、「未選択」のステータスである抽出ポリシー200が存在することを確認すれば、処理はステップS340へ進む。

一方、ポリシー抽出部100が、全ての複数のパスワードポリシーのうち、「未選択」のステータスであるパスワードポリシーが存在しないことを確認すれば、ポリシー抽出部100は、強度確認ポリシーを用いて、抽出結果記憶部106に記憶された抽出ポリシー200を更新する。そして、ポリシー抽出部100は、処理が完了したことを準拠性判定部102に通知する。そして、処理はステップS400へ進む。

[0084] ステップS 3 4 0からステップS 3 7 0は、実施の形態2と同一の動作であるため、説明を省略する。また、ステップS 4 0 0からステップS 4 3 0は、実施の形態3と同一の動作であるため、説明を省略する。

[0085] ステップS 4 3 0の後、ステップS 7 1 0では、認証情報仲介部1 1 1は、登録情報記憶部1 0 8より、登録情報である登録パスワード2 0 2を読み込む。また、認証情報仲介部1 1 1は、取得ポリシー記憶部1 1 2より、取得ポリシー2 0 5を読み込む。

そして、認証情報仲介部1 1 1は、登録パスワード2 0 2を取得ポリシー2 0 5に準拠するように変換し、変換パスワード2 0 7を生成する。

変換は、後述の、登録パスワード2 0 2を取得ポリシー2 0 5に準拠するように変換する変換アルゴリズム（変換パターンともいう）を用いて行われる。変換アルゴリズムは、変換の際に、パスワードの安全性を低下させないように構築されたものである。変換アルゴリズムは、公開情報であってもよい。

[0086] 次に、ステップS 7 2 0では、認証情報仲介部1 1 1は、通信インタフェース1 5を介して、変換パスワード2 0 7を用いて外部認証システム4 0に、外部認証システム4 0の認証に用いられる認証情報を入力する。そして、外部認証システム4 0で、認証情報登録が行われる。そして、認証情報登録の処理が完了する。

[0087] 図2 3を用いて、本実施の形態に係る変換パスワード2 0 7の生成例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図2 3は、本実施の形態に係る変換パスワード2 0 7の生成例を示す。

以下では、具体例として、登録パスワード2 0 2が「p@ssword」であり、取得ポリシー2 0 5が「5文字以上半角小文字英字」である場合の、変換パスワード2 0 7の生成の動作を詳細に説明する。なお、本例の登録パスワード2 0 2及び取得ポリシー2 0 5は、変換パスワード2 0 7の生成の説明を明瞭に行うための単純な例であり、安全性が低いため、実際の運用では用い

ない方が好ましい。

[0088] ステップS 8 0 0では、認証情報仲介部 1 1 1は、変数Sを定義し、登録パスワード2 0 2「p@ssword」を格納する。

[0089] 次に、ステップS 8 1 0では、認証情報仲介部 1 1 1は、取得ポリシー2 0 5に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件に基づき、使用可能な文字の種類の総数 x を算出する。

本例では、取得ポリシー2 0 5が「5文字以上半角小文字英字」であるため、総数 x は $x = 26$ である。

[0090] 次に、ステップS 8 2 0では、認証情報仲介部 1 1 1は、取得ポリシー2 0 5に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件に基づく使用可能な文字の各々に対してインデックス（0, 1, 2, ..., $x - 1$ ）を割り当てる。

本例では、取得ポリシー2 0 5が「5文字以上半角小文字英字」であり、使用可能な文字は、a~zである。そのため、認証情報仲介部 1 1 1は、インデックスを、 $a = 0$ 、 $b = 1$ 、...、 $g = 6$ 、 $h = 7$ 、...、 $z = 25$ と割り当てる。

[0091] 次に、ステップS 8 3 0では、認証情報仲介部 1 1 1は、変数Sをハッシュ化する。

以下では、ハッシュ化した変数SをTと記す。

ハッシュ化は、暗号学的に安全であれば、任意のハッシュ関数を利用してよい。

ハッシュ化の具体例としてSHA 256を利用した場合、認証情報仲介部 1 1 1は、変数S（=p@ssword）をハッシュ化し、T（=0 f d 2 0 5 9 6 5 c e 1 6 9 b 5 c 0 2 3 2 8 2 b b 5 f a 2 e 2 3 9 b 6 7 1 6 7 2 6 d b 5 d e f a a 8 c e f f 2 2 5 b e 8 0 5 d c）へ変換する。

[0092] 次に、ステップS 8 4 0では、認証情報仲介部 1 1 1は、ステップS 8 3 0でTを x 進数表現に変換する。

本例では、 x は $x = 26$ であるため、認証情報仲介部 1 1 1は、Tを26進数表現に変換する。

以下では、26進数表現に変換されたTをVと記す。

ただし、認証情報仲介部111は、Tを一旦y進数（yはx以下の数）表現に変換し、その後さらにy進数表現に変換したTをx進数に変換してもよい。具体例としては、認証情報仲介部111は、Tを一旦16進数表現に変換し、その後さらに26進数表現に変換してもよい。

本例のTは、一旦16進数表現へ変換され、その後更に26進数表現に変換される。

そして、本例のVはV＝「7、6、21、6、16、6、25、7、5、13、10、4、15、18、2、8、12、19、24、11、20、18、10、21、19、5、25、14、21、8、20、11、3、21、5、19、23、7、23、23、8、5、19、22、5、8、10、1、7、18、6、25、21、6」である。なお、Vの数字と数字との間のカンマ「、」は、各桁の区切りを示す。具体例としては、Vの先頭から1桁目の値は「7」であり、先頭から2桁目の値は「6」であることを示す。

[0093] 次に、ステップS850では、認証情報仲介部111は、Vの各桁の値をインデックスとした文字へ変換し、Vを文字列Wへ変換する。

本例のVの先頭から1桁目の値は「7」である。そして、インデックス「7」が割り当てられた文字は「h」である。したがって、Vの先頭から1桁目は「h」に変換される。

また、本例のVの先頭から2桁目の値は「6」である。そして、インデックス「6」が割り当てられた文字は「g」である。したがって、Vの先頭から2桁目は「g」に変換される。

このように、認証情報仲介部111は、Vの全ての桁の値を文字へ変換することで、Vを文字列Wへ変換する。

そして、本例のWは、W＝「hgvqgqzhfnkepscimtyluskvtfzoviuldvftxhxxifftwfikbhsgzvg」である。

[0094] 次に、ステップS860では、認証情報仲介部111は、Wが取得ポリシー205に記述されたパスワードに使用可能な文字（英字、数字、及び記号

)の使用要件を満たしているか否かを確認する。

[0095] 次に、ステップS 8 7 0では、認証情報仲介部1 1 1が、Wは取得ポリシー2 0 5に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件を満たしていることを確認すれば、処理はステップS 8 8 0へ進む。

一方、認証情報仲介部1 1 1が、Wは取得ポリシー2 0 5に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件を満たしていないことを確認すれば、処理はステップS 8 3 0に戻る。そして、認証情報仲介部1 1 1は、Wとなった変数Sを用いて、再度ステップS 8 3 0からステップS 8 6 0の処理を行う。

本例のWは、W=「hgvqgqzhfnkepscimtyluskvtfzoviuldvftxhxxiftwifikbhsgzvq」であり、これは取得ポリシー2 0 5の「5文字以上半角小文字英字」を満たすため、処理はステップS 8 8 0へ進む。

[0096] 別の具体例を用いて、処理がステップS 8 3 0に戻る例を詳細に説明する。

取得ポリシー2 0 5が「8文字以上半角小文字英字及び半角数字（半角小文字英字と半角数字を少なくとも1文字以上含める）」であったとする。このような取得ポリシー2 0 5に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件を満たすためには、少なくとも、1字の「半角小文字英字」と1字の「半角数字」とがWに含まれていることが必須である。しかし、ステップS 8 5 0で変換されたWに、「半角小文字英字」又は「半角数字」のどちらかが1字も含まれていない場合が考えられる。このような場合には、ステップS 8 6 0で、Wは取得ポリシー2 0 5に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件を満たしていないことが確認される。そして、ステップS 8 7 0で、処理がステップS 8 3 0に戻る。そして、認証情報仲介部1 1 1は、Wとなった変数Sに2度目のハッシュ化を行う。そして、ステップS 8 4 0及びステップS 8 5 0を経て、Sは新たなWへと変換される。そして、Wが取得ポリシー2 0 5

に記述されたパスワードに使用可能な文字（英字、数字、及び記号）の使用要件を満たすまで、S 8 3 0 から S 8 6 0 の処理が繰り返される。

[0097] 次に、ステップ S 8 8 0 では、認証情報仲介部 1 1 1 は、W を変換パスワード 2 0 7 として記憶する。そして、変換パスワード 2 0 7 の生成の処理は完了する。

[0098] 図 2 4 を用いて、本実施の形態に係るパスワード認証装置 1 0 の認証の処理例について説明する。以下では、認証情報はパスワードのみであるとして詳細に説明する。

図 2 4 は、本実施の形態に係るパスワード認証装置 1 0 の認証の処理例を示す。

なお、実施の形態 3 と同一の動作には同一番号を付してその説明を省略する。

図 2 4 の、ステップ S 9 0 0 がポリシー取得部 1 1 0、ステップ S 5 1 0 及びステップ S 5 2 0 が認証情報取得部 1 0 1、ステップ S 9 1 0 及びステップ S 9 2 0 が認証情報仲介部 1 1 1 の処理に対応する。

[0099] ステップ S 5 0 0 及びステップ S 5 1 0 は、実施の形態 3 と同一の動作であるため、説明を省略する。

[0100] ステップ S 5 2 0 の後、ステップ S 9 1 0 では、認証情報仲介部 1 1 1 は、認証情報記憶部 1 0 7 より、認証情報である入力パスワード 2 0 1 を読み込む。また、認証情報仲介部 1 1 1 は、取得ポリシー記憶部 1 1 2 より、取得ポリシー 2 0 5 を読み込む。

そして、認証情報仲介部 1 1 1 は、入力パスワード 2 0 1 を取得ポリシー 2 0 5 に準拠するように変換し、変換パスワード 2 0 7 を生成する。

変換は、図 2 3 の変換パスワード 2 0 7 の生成で、登録パスワード 2 0 2 を入力パスワード 2 0 1 に置き換えた動作であるため、説明は省略する。

[0101] 次に、ステップ S 9 2 0 では、認証情報仲介部 1 1 1 は、通信インタフェース 1 5 を介して、変換パスワード 2 0 7 を用いて外部認証システム 4 0 に、外部認証システム 4 0 の認証に用いられる認証情報を入力する。そして、

外部認証システム 40 で、認証が行われる。そして、認証の処理が完了する。

[0102] ***実施の形態の効果の説明***

以上のように、本実施の形態によれば、パスワード認証装置は、認証情報登録時に、ユーザが入力した認証情報に含まれるパスワードを外部認証システムのパスワードポリシーに準拠するように変換する。そして、パスワード認証装置は、変換したパスワードを用いて、外部認証システムに認証情報を入力する。

また、パスワード認証装置は、認証時に、ユーザが入力した認証情報に含まれるパスワードを外部認証システムのパスワードポリシーに準拠するように変換する。そして、パスワード認証装置は、変換したパスワードを用いて、外部認証システムに認証情報を入力する。

よって、認証情報登録及び認証を行う外部認証システムが存在する場合にも、ユーザは外部認証システムのパスワードポリシーと同等以上の強度であるパスワードポリシーを選択し、ユーザ自身のパスワードの生成方針に沿ってパスワードを生成することが出来る。

また、本実施の形態のパスワード認証装置によるパスワードの変換に用いる変換パターンを公開しても、ユーザが生成するパスワードは、外部認証システムのパスワードポリシーと同等以上の強度であるパスワードポリシーに準拠する安全なパスワードである。

したがって、変換パターンを公開しても、パスワードポリシーに準拠し、且つユーザ自身のパスワードの生成方針に沿った安全なパスワード生成を可能とすることができる。

[0103] 以上、本開示の実施の形態について説明したが、これらの実施の形態のうち、2つ以上を組み合わせる実施しても構わない。

あるいは、これらの実施の形態のうち、1つを部分的に実施しても構わない。

あるいは、これらの実施の形態のうち、2つ以上を部分的に組み合わせる

実施しても構わない。

なお、本開示は、これらの実施の形態に限定されるものではなく、必要に応じて種々の変更が可能である。

ハードウェア構成の説明

最後に、パスワード認証装置10のハードウェア構成の補足説明を行う。

図2に示すプロセッサ11は、プロセッシングを行うIC(Integrated Circuit)である。プロセッサ11の具体例は、CPU(Central Processing Unit)、DSP(Digital Signal Processor)等である。

図2に示すメモリ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の具体例は、RAM(Random Access Memory)である。

図2に示す補助記憶装置13は、データを記憶する記憶装置である。補助記憶装置13の具体例は、ハードディスクである。

また、補助記憶装置13は、SSD(登録商標、Solid State Drive)、SD(登録商標、Secure Digital)メモリカード、CF(登録商標、CompactFlash)、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(登録商標、Digital Versatile Disk)といった可搬記録媒体であってもよい。

図2に示す入出力インタフェース14は、情報の入出力処理を実行する電子回路である。入出力インタフェース14の具体例は、キーボード又はマウス等の入力装置から入力された情報を受信し、モニタ等の出力装置に情報を送信する電子回路である。

図2に示す通信インタフェース15は、信号線を介して接続先との情報の通信処理を実行する電子回路である。通信インタフェース15の具体例は、Ethernet(登録商標)用の通信チップ又はNIC(Network Interface Card)である。

また、補助記憶装置 13 には、OS (Operating System) も記憶されている。そして、OS の少なくとも一部がプロセッサ 11 により実行される。

プロセッサ 11 は、OS の少なくとも一部を実行しながら、ポリシー抽出部 100、認証情報取得部 101、準拠性判定部 102、認証情報登録部 103、認証情報照合部 104、ポリシー取得部 110、及び認証情報仲介部 111 の機能を実現するプログラムを実行する。

プロセッサ 11 が OS を実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、ポリシー抽出部 100、認証情報取得部 101、準拠性判定部 102、認証情報登録部 103、認証情報照合部 104、ポリシー取得部 110、及び認証情報仲介部 111 の処理の結果を示す情報、データ、信号値及び変数値の少なくともいずれかが、プロセッサ 11、メモリ 12、補助記憶装置 13 内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、ポリシー抽出部 100、認証情報取得部 101、準拠性判定部 102、認証情報登録部 103、認証情報照合部 104、ポリシー取得部 110、及び認証情報仲介部 111 の機能を実現するプログラムは、ハードディスク、SSD (登録商標)、SD (登録商標) メモリカード、CF (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 (登録商標) といった可搬記録媒体に格納されていてもよい。

そして、ポリシー抽出部 100、認証情報取得部 101、準拠性判定部 102、認証情報登録部 103、認証情報照合部 104、ポリシー取得部 110、及び認証情報仲介部 111 の機能を実現するプログラムを流通させてもよい。

また、ポリシー抽出部 100、認証情報取得部 101、準拠性判定部 102、認証情報登録部 103、認証情報照合部 104、ポリシー取得部 110

、及び認証情報仲介部 111 の「部」を、「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。

また、パスワード認証装置 10 は、処理回路により実現されてもよい。処理回路は、例えば、ロジック IC (Integrated Circuit)、GA (Gate Array)、ASIC (Application Specific Integrated Circuit)、FPGA (Field-Programmable Gate Array) である。

なお、本明細書では、プロセッサと処理回路との上位概念を、「プロセッシングサーキットリー」という。

つまり、プロセッサと処理回路とは、それぞれ「プロセッシングサーキットリー」の具体例である。

符号の説明

- [0104] 1 パスワード認証システム、10 パスワード認証装置、11 プロセッサ、12 メモリ、13 補助記憶装置、14 入出力インタフェース、15 通信インタフェース、20 端末装置、30 ネットワーク、40 外部認証システム、100 ポリシー抽出部、101 認証情報取得部、102 準拠性判定部、103 認証情報登録部、104 認証情報照合部、105 ポリシー記憶部、106 抽出結果記憶部、107 認証情報記憶部、108 登録情報記憶部、109 抽出要件記憶部、110 ポリシー取得部、111 認証情報仲介部、112 取得ポリシー記憶部、200 抽出ポリシー、201 入力パスワード、202 登録パスワード、203 要求強度、204 ユーザポリシー、205 取得ポリシー、206 組み合わせ総数、207 変換パスワード。

請求の範囲

- [請求項1] ユーザの認証に用いるパスワードの認定要件を記述した複数のパスワードポリシーであり、パスワードが前記複数のパスワードポリシーのうち少なくともいずれか1つのパスワードポリシーに準拠していれば前記パスワードを正当なパスワードとして認定可能な複数のパスワードポリシーを記憶するポリシー記憶部と、
- 前記ポリシー記憶部が記憶する前記複数のパスワードポリシーから1つ以上のパスワードポリシーを抽出するポリシー抽出部と、
- パスワードを含む認証情報を取得する認証情報取得部と、
- 前記認証情報取得部が取得した前記認証情報に含まれるパスワードが、前記ポリシー抽出部が抽出した前記1つ以上のパスワードポリシーのうち、少なくともいずれか1つのパスワードポリシーに準拠しているか否かを判定する準拠性判定部と、
- 前記準拠性判定部が前記少なくともいずれか1つのパスワードポリシーに準拠していると判定したときに、前記認証情報を登録情報として登録する認証情報登録部とを備えるパスワード認証装置。
- [請求項2] 前記ポリシー記憶部は、パスワードに使用可能な英字、数字、及び記号の3種のうち少なくとも1種の使用要件を記述したパスワードポリシーを記憶する請求項1に記載のパスワード認証装置。
- [請求項3] 前記パスワード認証装置は、更に、
- 前記複数のパスワードポリシーからパスワードポリシーを抽出する抽出要件を記憶する抽出要件記憶部を備え、
- 前記ポリシー抽出部は、前記抽出要件記憶部が記憶する前記抽出要件に基づき、前記複数のパスワードポリシーから前記1つ以上のパスワードポリシーを抽出する請求項1又は請求項2に記載のパスワード認証装置。
- [請求項4] 前記抽出要件記憶部は、
- 前記抽出要件として、前記1つ以上のパスワードポリシーの抽出に

用いられる基準を示す要求強度を記憶し、

前記ポリシー抽出部は、前記複数のパスワードポリシーの各々のパスワードポリシーにより定まるパスワードの文字の組み合わせの総数を示すパスワード総数を計算し、前記各々のパスワードポリシーのパスワード総数と前記要求強度とを用いて、前記複数のパスワードポリシーから前記1つ以上のパスワードポリシーを抽出する請求項3に記載のパスワード認証装置。

[請求項5] 前記パスワード認証装置は、更に、

前記認証情報登録部が登録した前記登録情報を用いてユーザの認証を行う認証情報照合部を備える請求項1から請求項4のいずれか1つに記載のパスワード認証装置。

[請求項6] 前記パスワード認証装置は、更に、

ポリシー取得部と、認証情報仲介部とを備え、

前記ポリシー取得部は、前記パスワード認証装置の外部でユーザの認証を行う外部認証システムがユーザの認証に用いるパスワードポリシーを取得ポリシーとして取得し、前記取得ポリシーにより定まるパスワードの文字の組み合わせの総数を示す取得ポリシーのパスワード総数を計算し、前記取得ポリシーのパスワード総数を前記要求強度として前記抽出要件記憶部に記憶し、

前記認証情報仲介部は、前記登録情報に含まれるパスワードを前記取得ポリシーに準拠する変換パスワードへと変換する請求項4に記載のパスワード認証装置。

[請求項7] 前記認証情報仲介部は、

前記登録情報及び前記変換パスワードを用いて、前記外部認証システムに、前記外部認証システムの認証に用いられる認証情報を登録する請求項6に記載のパスワード認証装置。

[請求項8] 前記認証情報仲介部は、

前記登録情報及び前記変換パスワードを用いて、前記外部認証シス

テムの認証を行う請求項6又は請求項7に記載のパスワード認証装置。
。

[請求項9]

前記認証情報取得部は、

前記ポリシー抽出部が抽出した前記1つ以上のパスワードポリシーを認証情報の入力画面に表示し、表示された前記1つ以上のパスワードポリシーのうち、選択されたパスワードポリシーを、ユーザポリシーとして取得し、

前記準拠性判定部は、

前記認証情報取得部が取得した前記認証情報に含まれるパスワードが、前記ユーザポリシーに準拠しているか否かを判定し、

認証情報登録部は、

前記準拠性判定部が前記認証情報に含まれるパスワードは前記ユーザポリシーに準拠していると判定したときに、前記認証情報及び前記ユーザポリシーを前記登録情報として登録する請求項1から請求項8のいずれか1つに記載のパスワード認証装置。

[請求項10]

ユーザの認証に用いるパスワードの認定要件を記述した複数のパスワードポリシーであり、パスワードが前記複数のパスワードポリシーのうち少なくともいずれか1つのパスワードポリシーに準拠していれば前記パスワードを正当なパスワードとして認定可能な複数のパスワードポリシーを記憶し、

前記複数のパスワードポリシーから1つ以上のパスワードポリシーを抽出し、

パスワードを含む認証情報を取得し、

前記認証情報に含まれるパスワードが、前記1つ以上のパスワードポリシーのうち、少なくともいずれか1つのパスワードポリシーに準拠しているか否かを判定し、

前記少なくともいずれか1つのパスワードポリシーに準拠していると判定したときに、前記認証情報を登録情報として登録するパスワード

ド認証方法。

[請求項11]

ユーザの認証に用いるパスワードの認定要件を記述した複数のパスワードポリシーであり、パスワードが前記複数のパスワードポリシーのうち少なくともいずれか1つのパスワードポリシーに準拠していれば前記パスワードを正当なパスワードとして認定可能な複数のパスワードポリシーを記憶するポリシー記憶処理と、

前記ポリシー記憶処理により記憶された前記複数のパスワードポリシーから1つ以上のパスワードポリシーを抽出するポリシー抽出処理と、

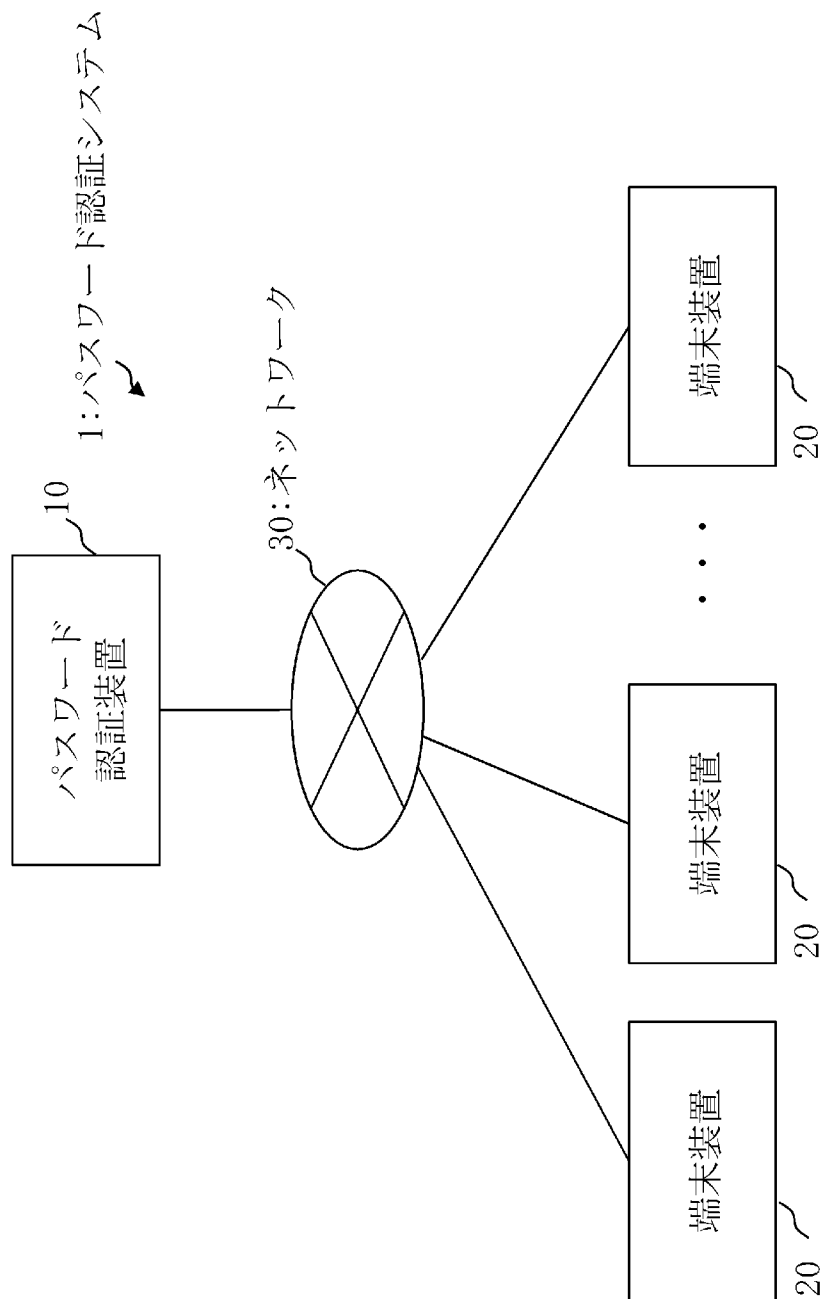
パスワードを含む認証情報を取得する認証情報取得処理と、

前記認証情報取得処理により取得された前記認証情報に含まれるパスワードが、前記ポリシー抽出処理により抽出された前記1つ以上のパスワードポリシーのうち、少なくともいずれか1つのパスワードポリシーに準拠しているか否かを判定する準拠性判定処理と、

前記準拠性判定処理により前記少なくともいずれか1つのパスワードポリシーに準拠していると判定したときに、前記認証情報を登録情報として登録する認証情報登録処理とをコンピュータに実行させるパスワード認証プログラム。

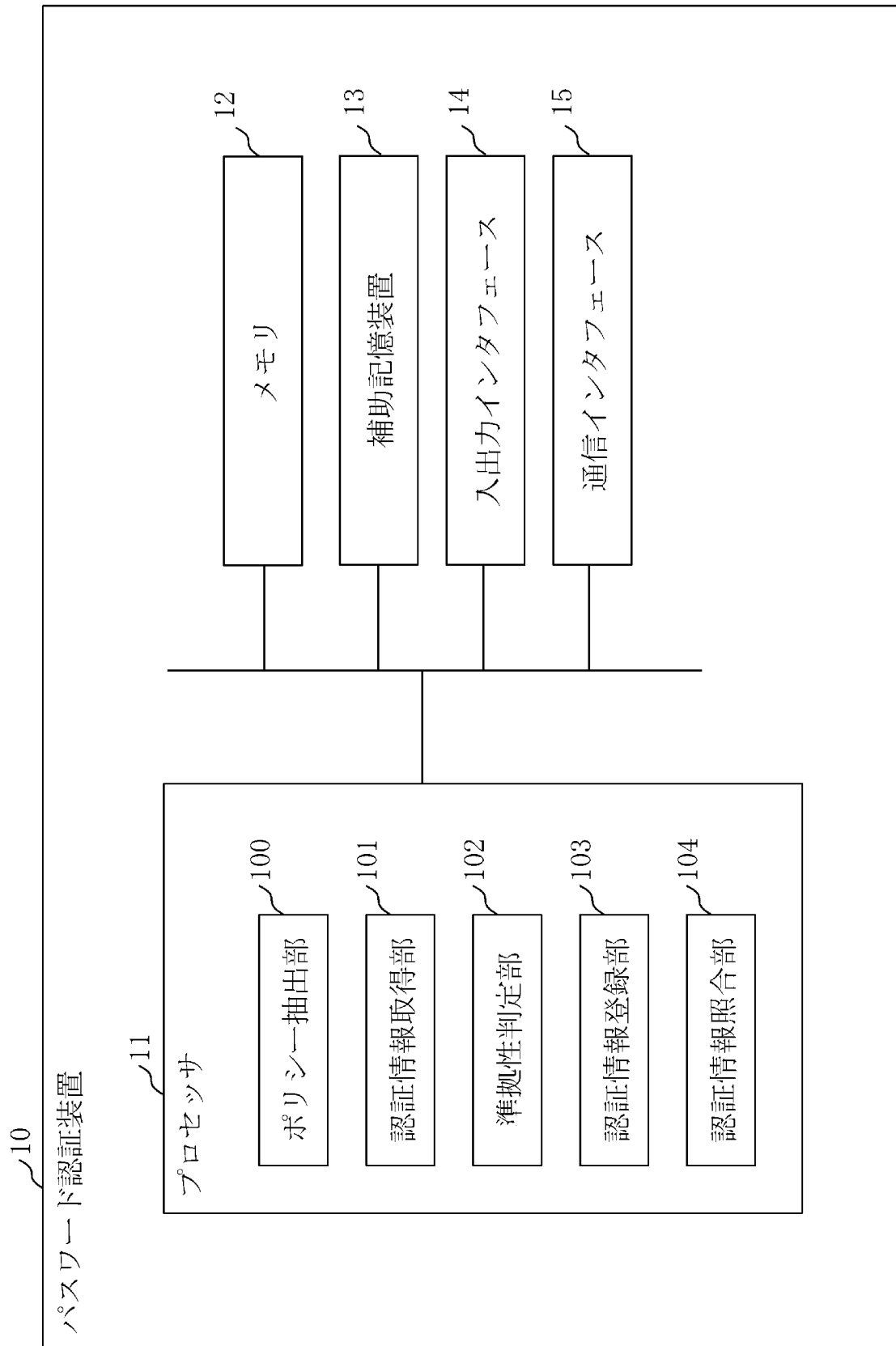
[図1]

図1



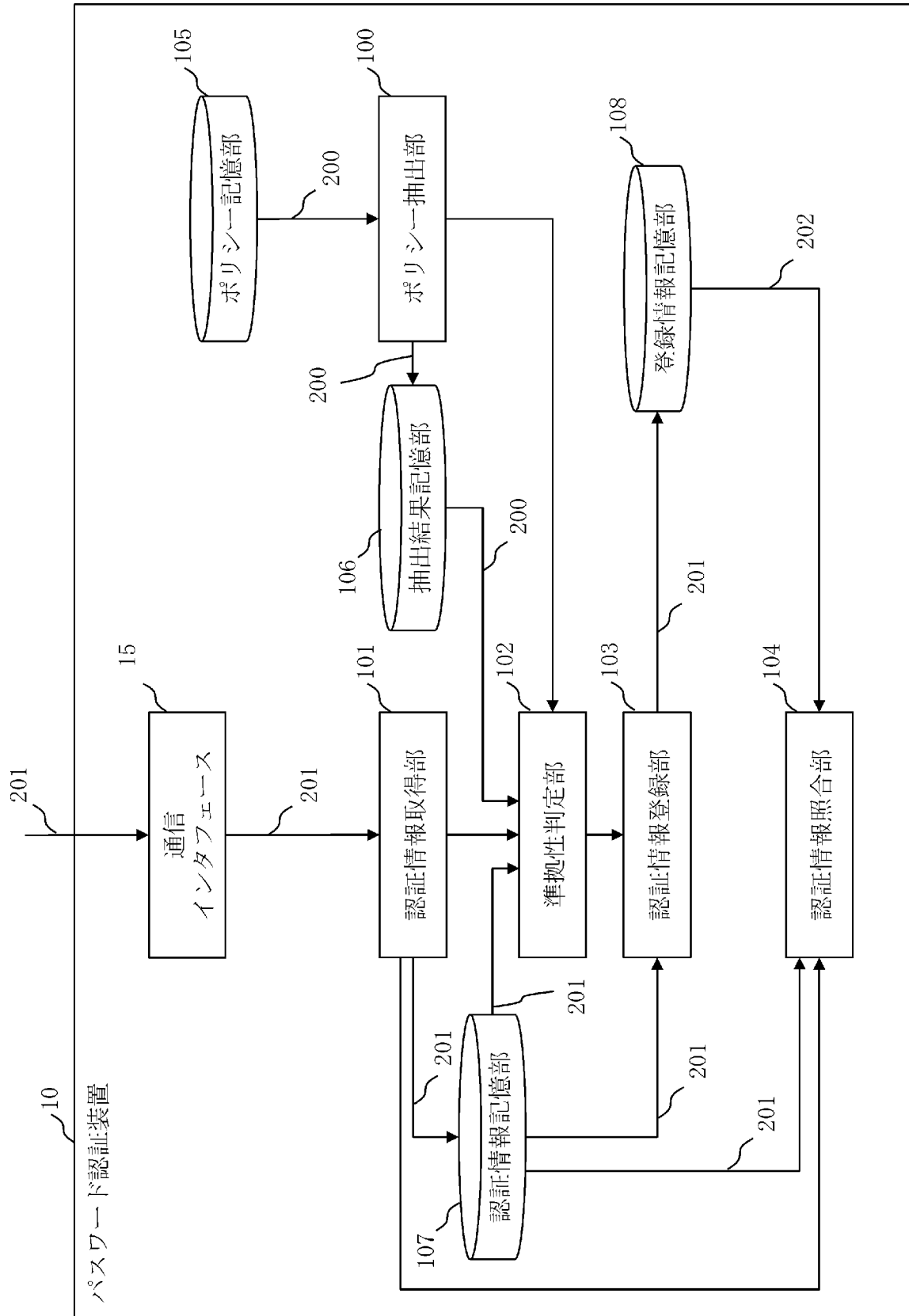
[図2]

図2



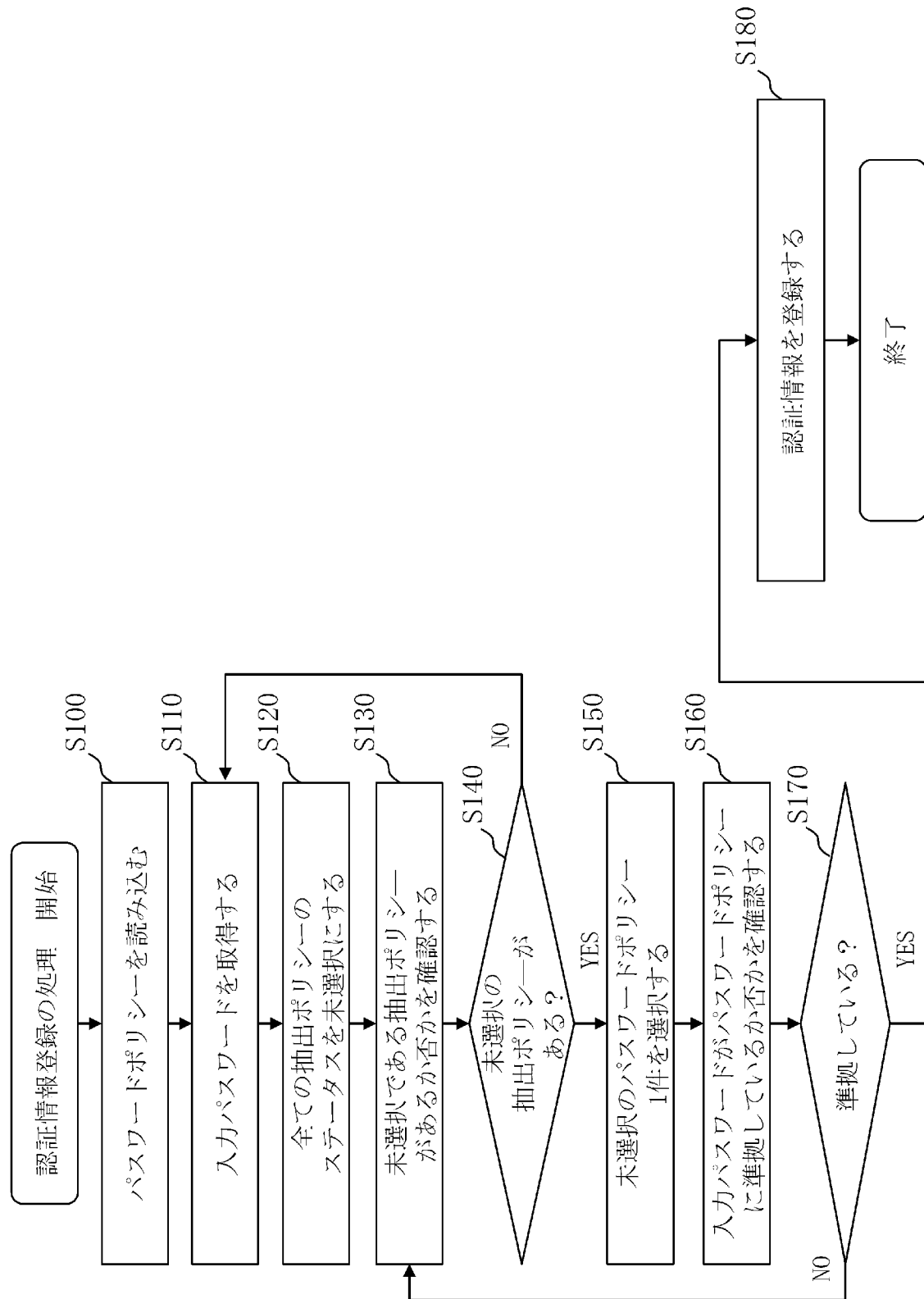
[図3]

図3



[図4]

図4



[図5]

図5

パスワードポリシー
8文字以上半角英数字
16文字以上半角英字
6文字以上半角英字記号

[図6]

図6

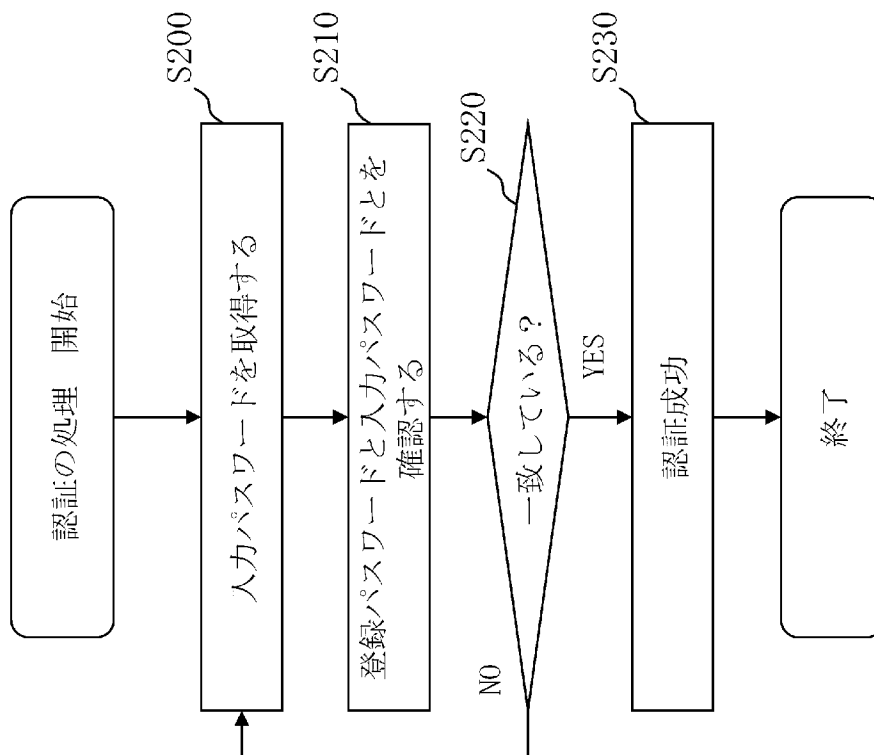
登録するパスワードを入力してください。

System!p@ssowrD

OK

[図7]

図7



[図8]

図8

登録したパスワードを入力してください。

System!p@ssowrD

OK

[図9]

図9

登録するパスワードを入力してください。

System!p@ssowrd

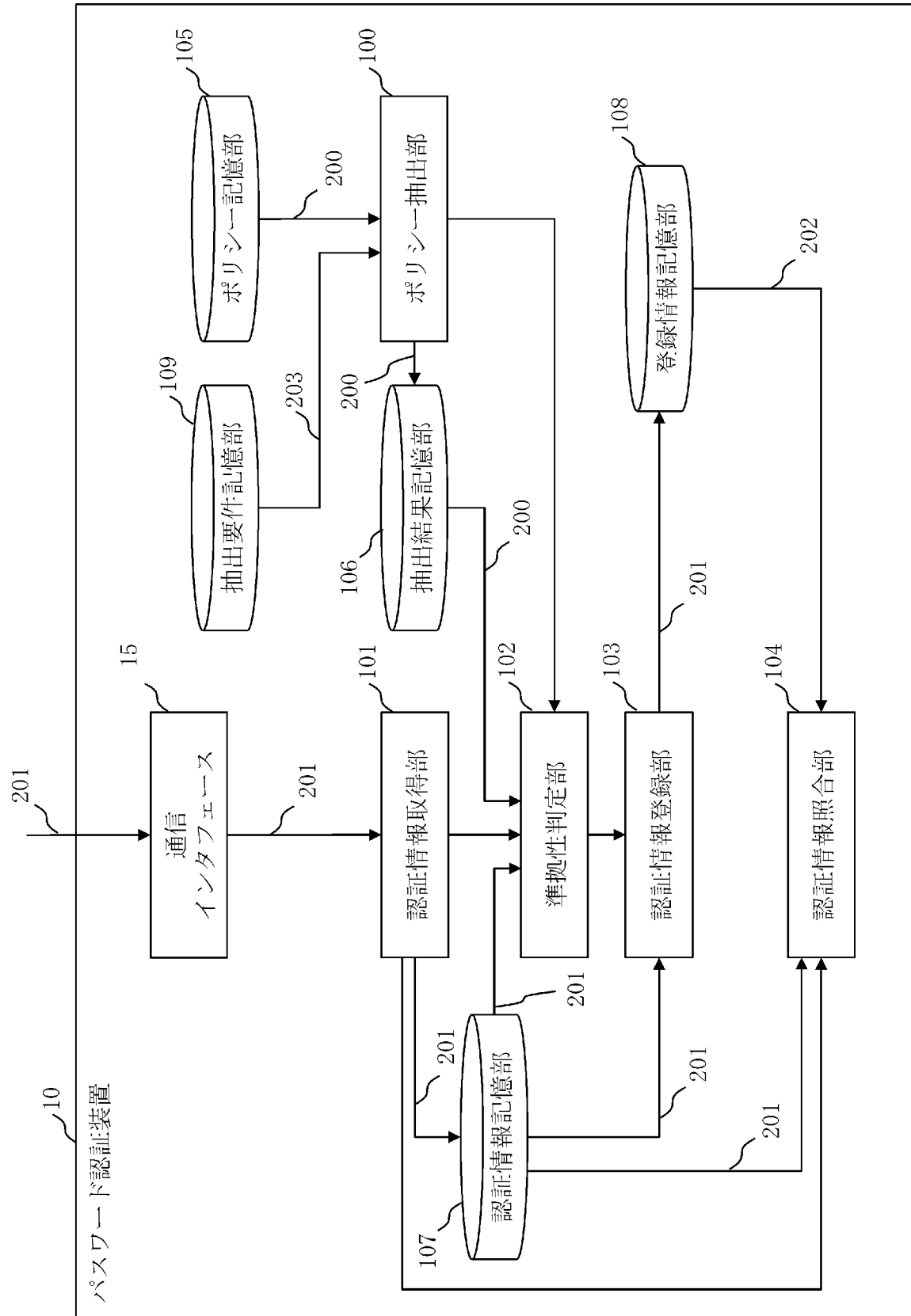
※いずれかのポリシーを満たすようにしてください。

ポリシー1: 8文字以上半角英数字
ポリシー2: 16文字以上半角英数字
ポリシー3: 6文字以上半角英数字記号

OK

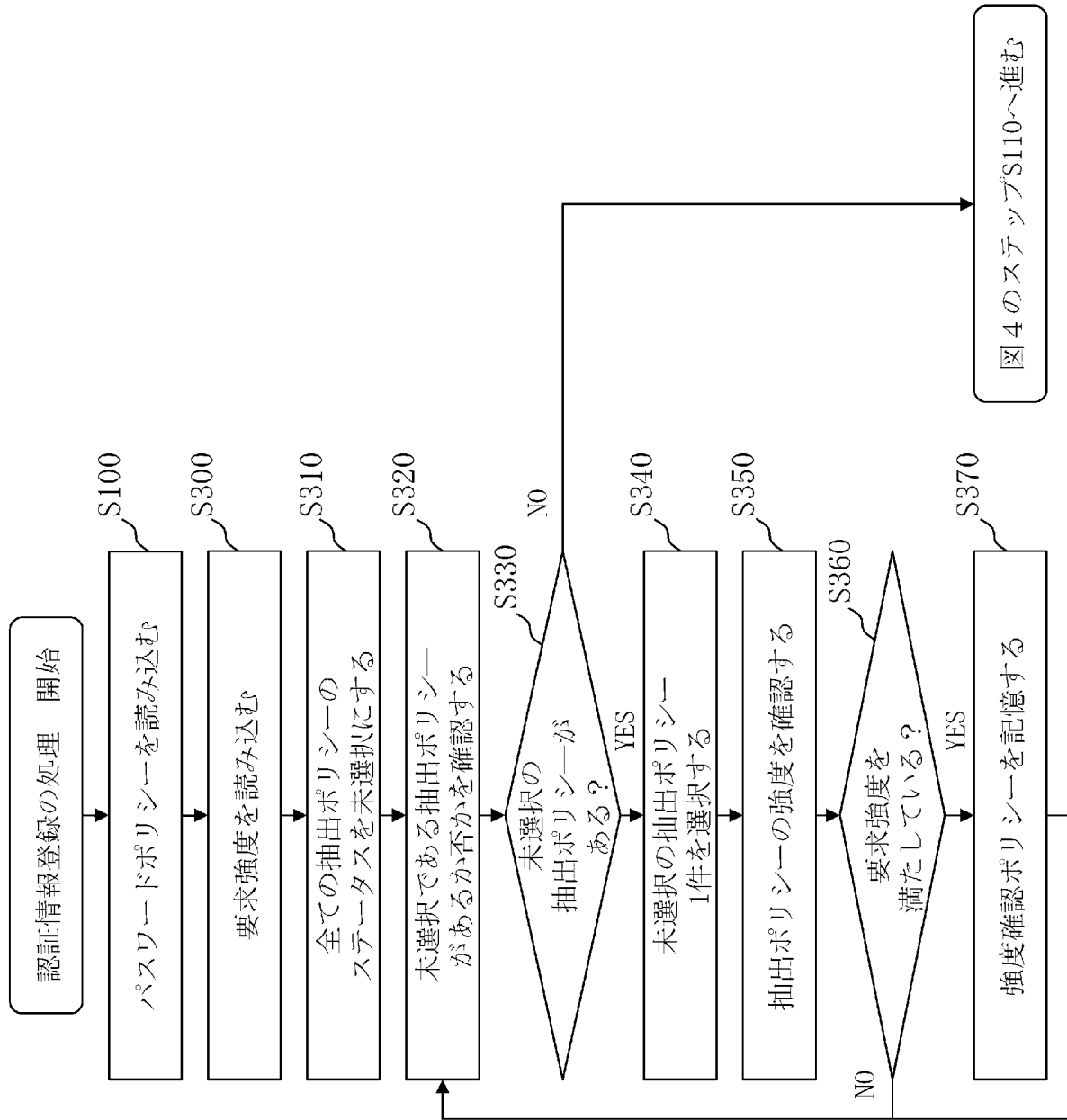
[図10]

図10



[図11]

図11



[図12]

図12

パスワードポリシー
8文字以上半角英数字
16文字以上半角英字
6文字以上半角英字記号
4桁半角数字

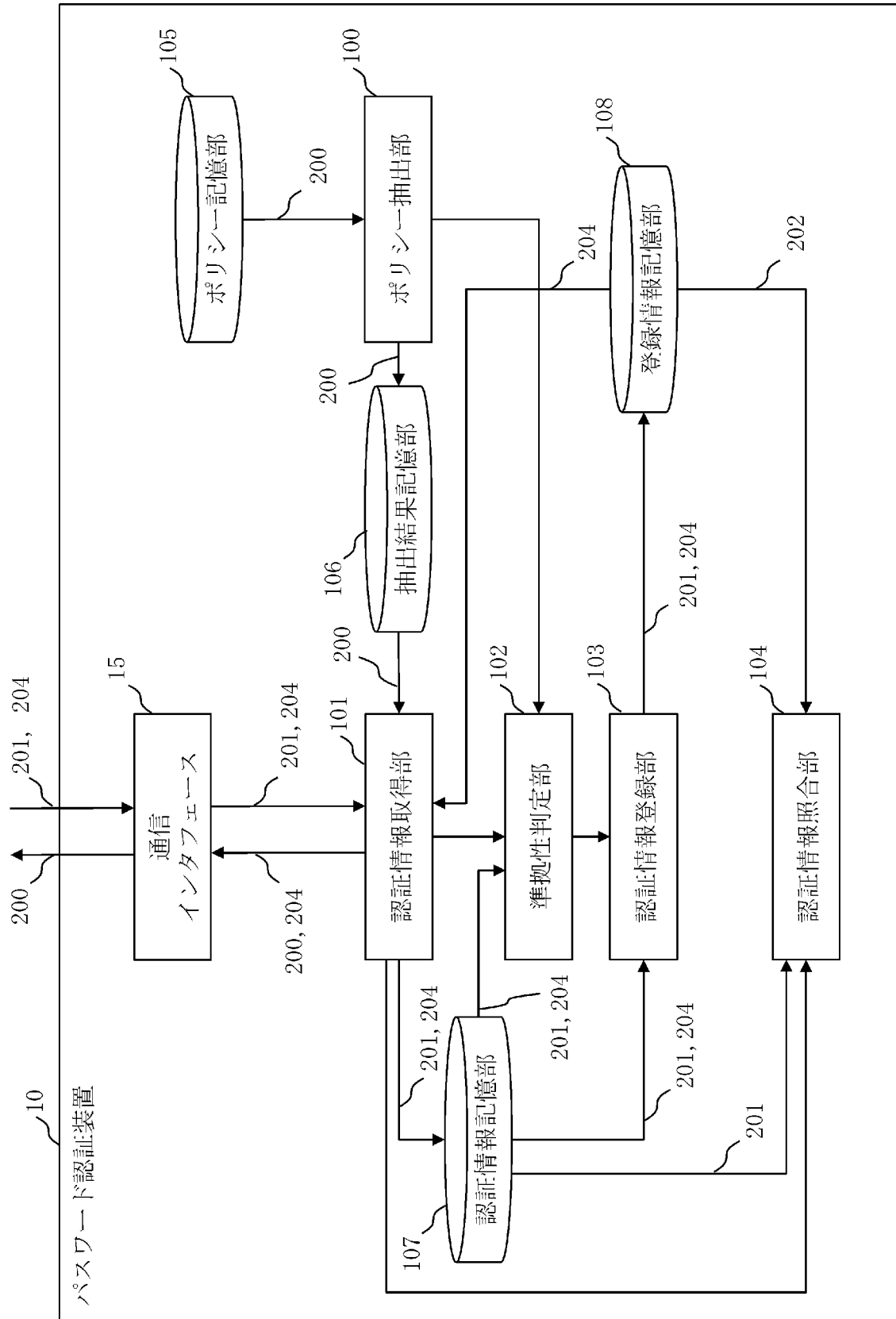
[図13]

図13

パスワードポリシー
8文字以上半角英数字
16文字以上半角英字
6文字以上半角英字記号

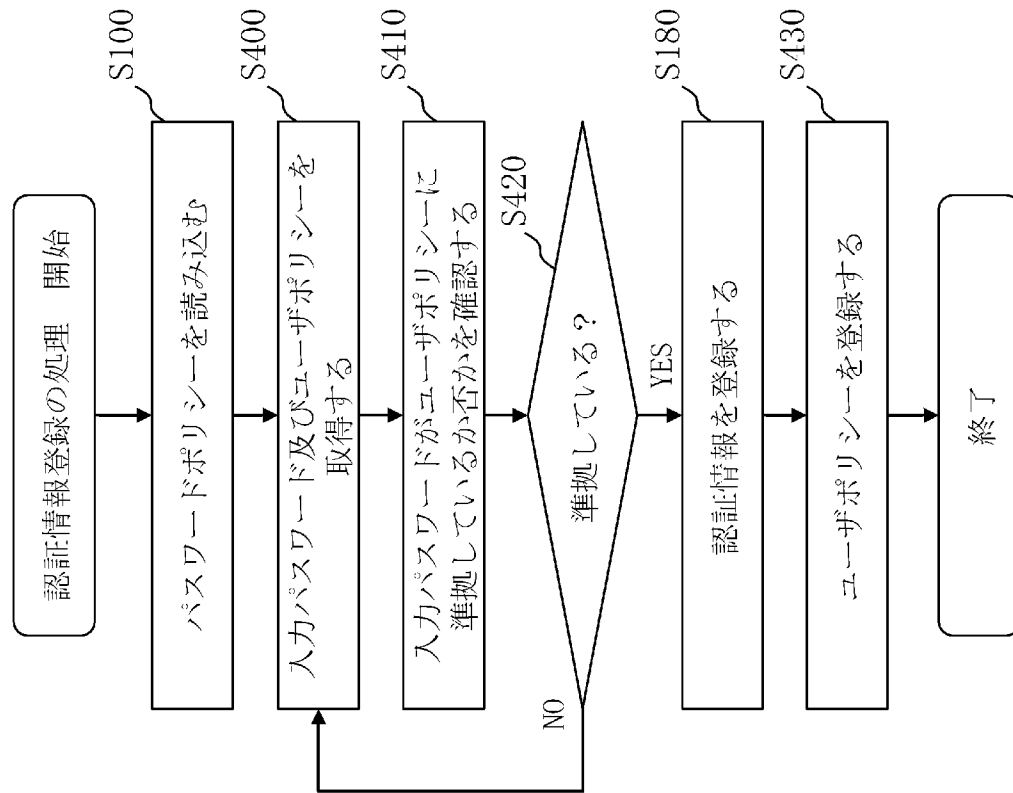
[図14]

図14



[図15]

図15



[図16]

図16

使用したいパスワードポリシーを選択してください。

☐ ポリシー1: 8文字以上半角英数字

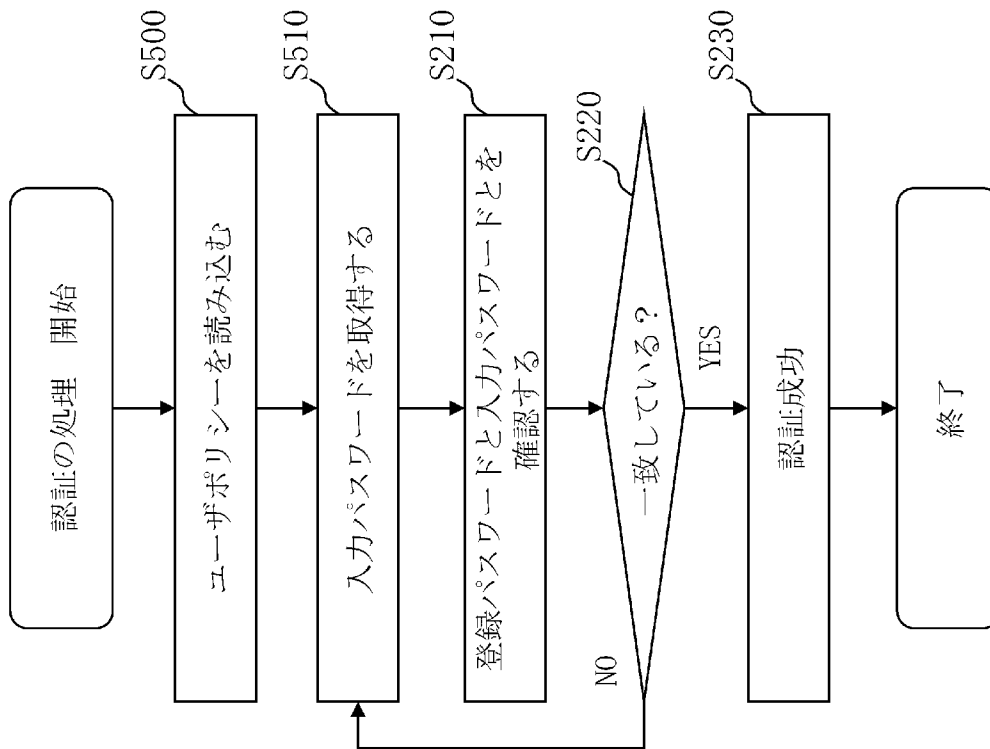
☐ ポリシー2: 16文字以上半角英数字

☒ ポリシー3: 6文字以上半角英数字記号

OK

[図17]

図17



[図18]

図18

登録したパスワードを入力してください。

System!p@ssowrd

パスワードポリシー：6文字以上半角英字記号

OK

[図19]

図19

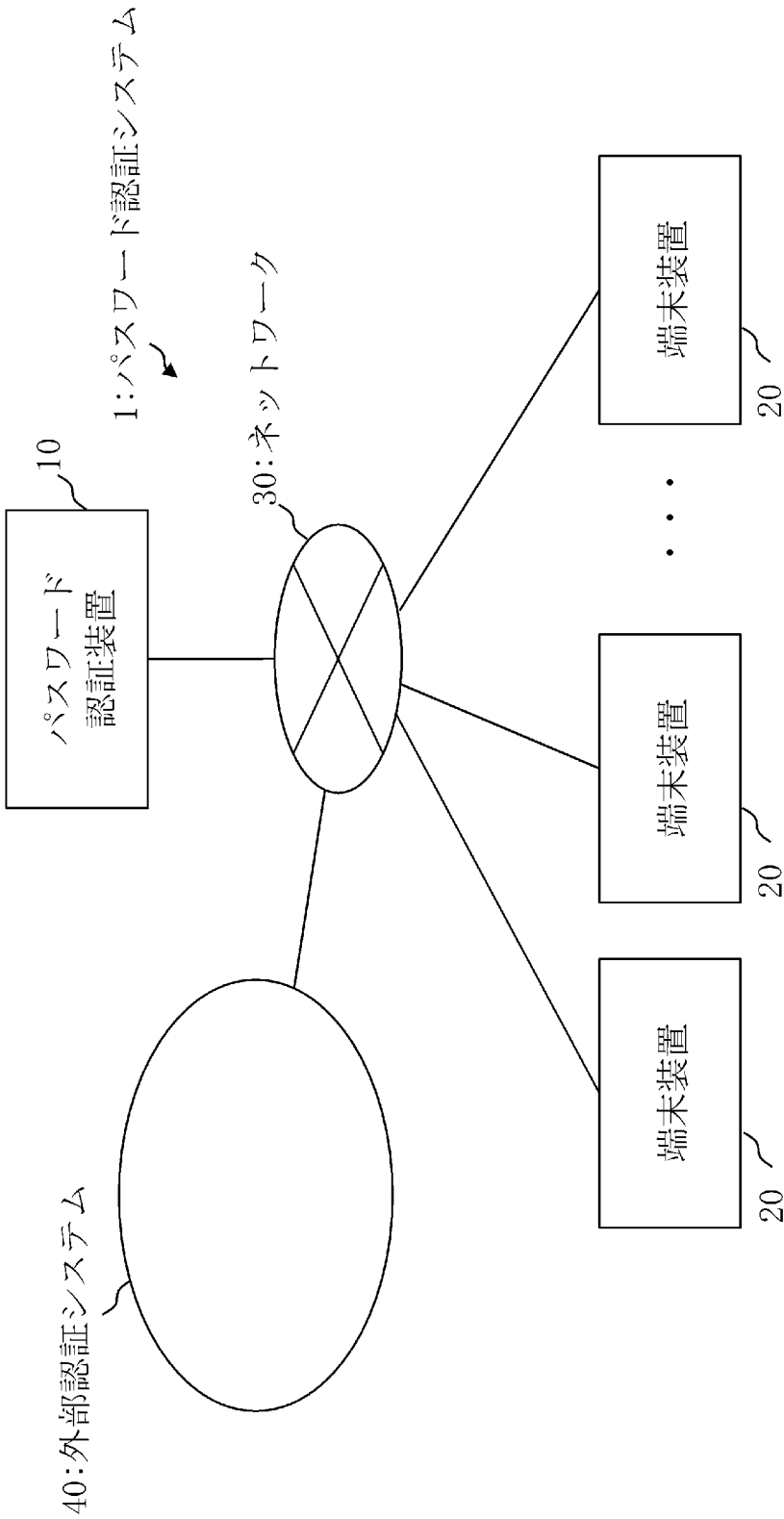
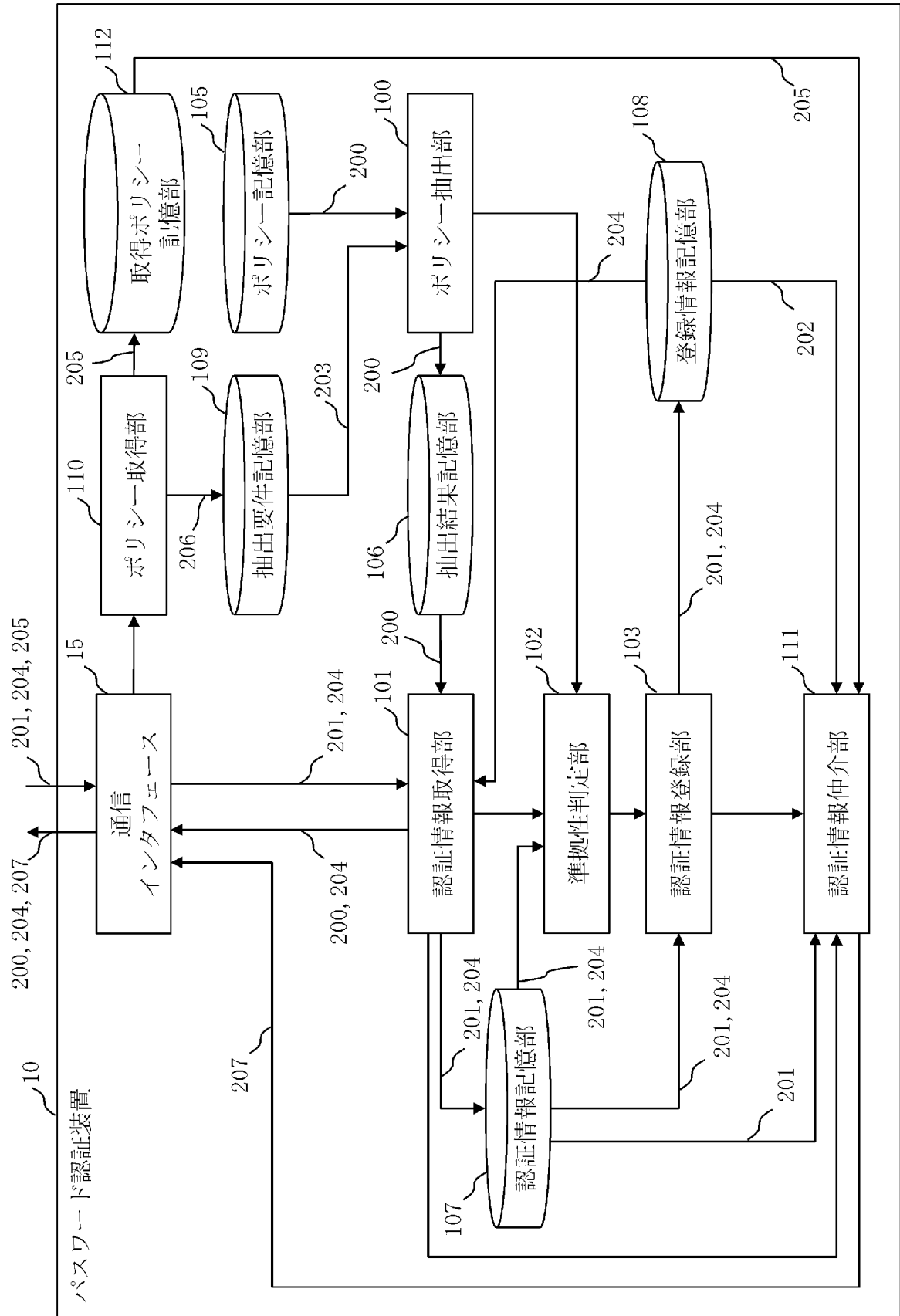
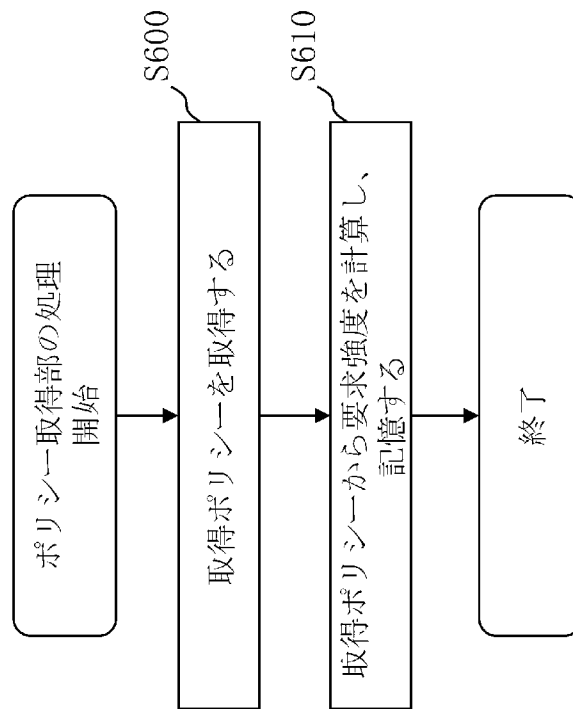


图20



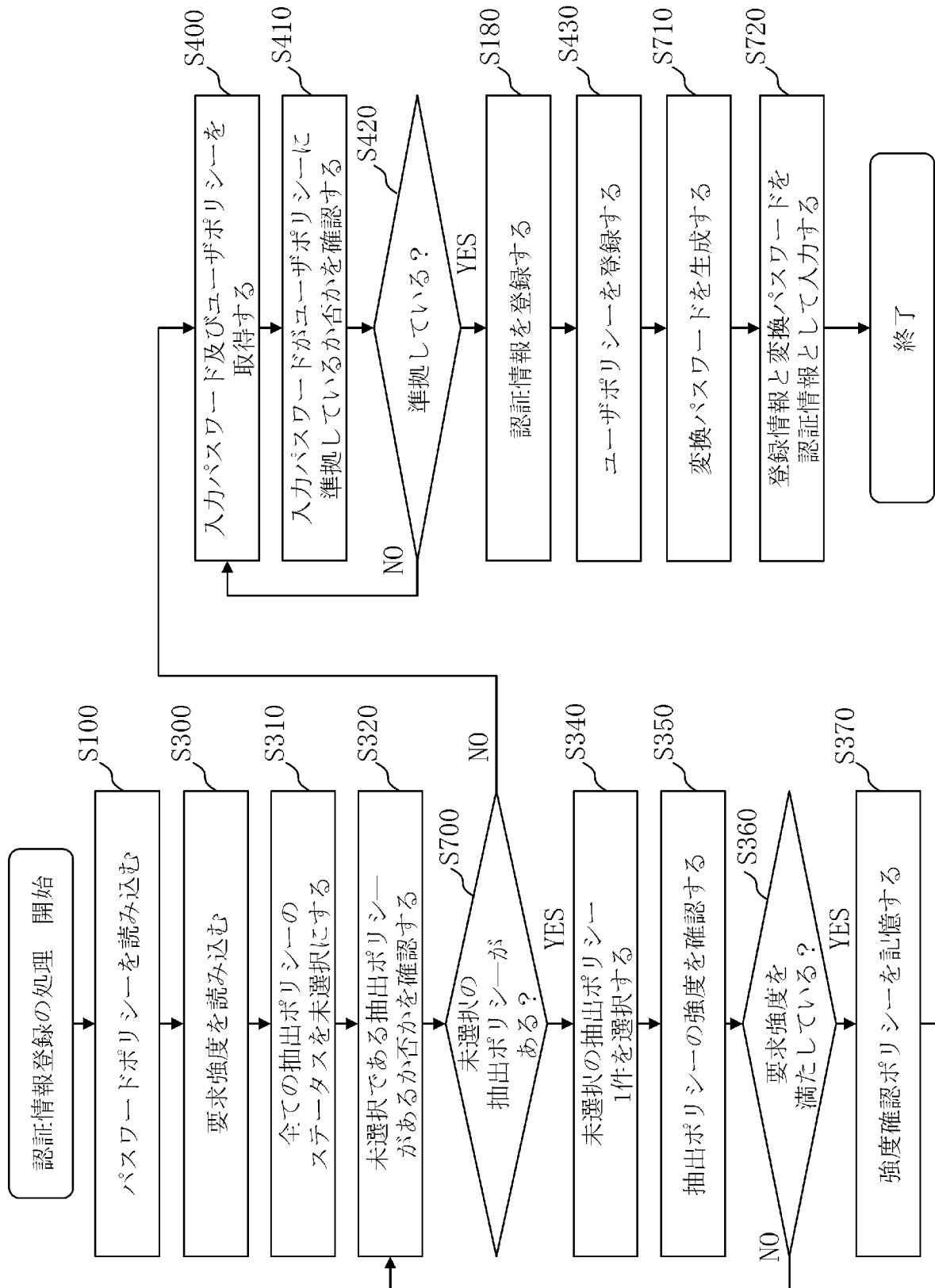
[図21]

図21



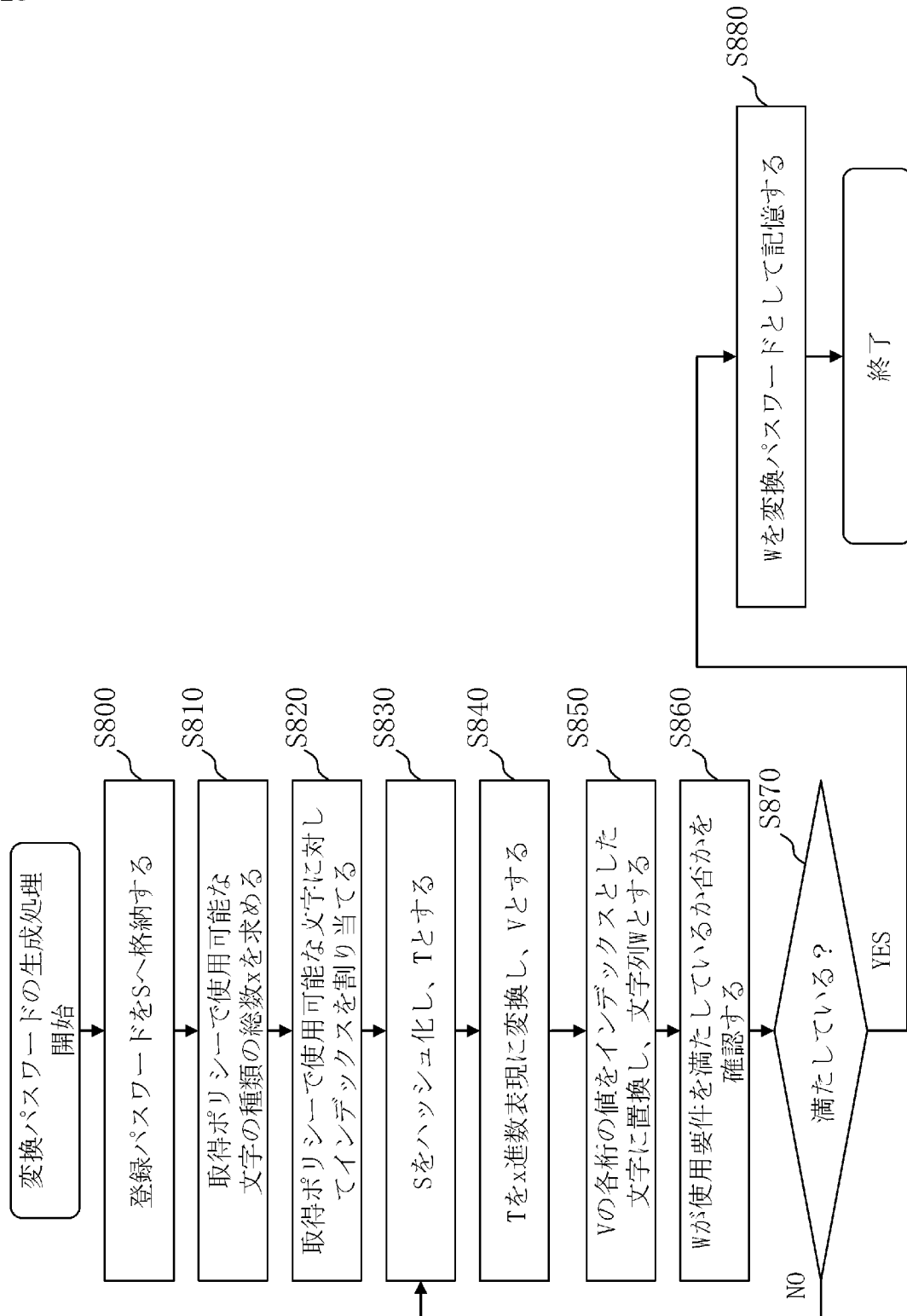
[図22]

図22



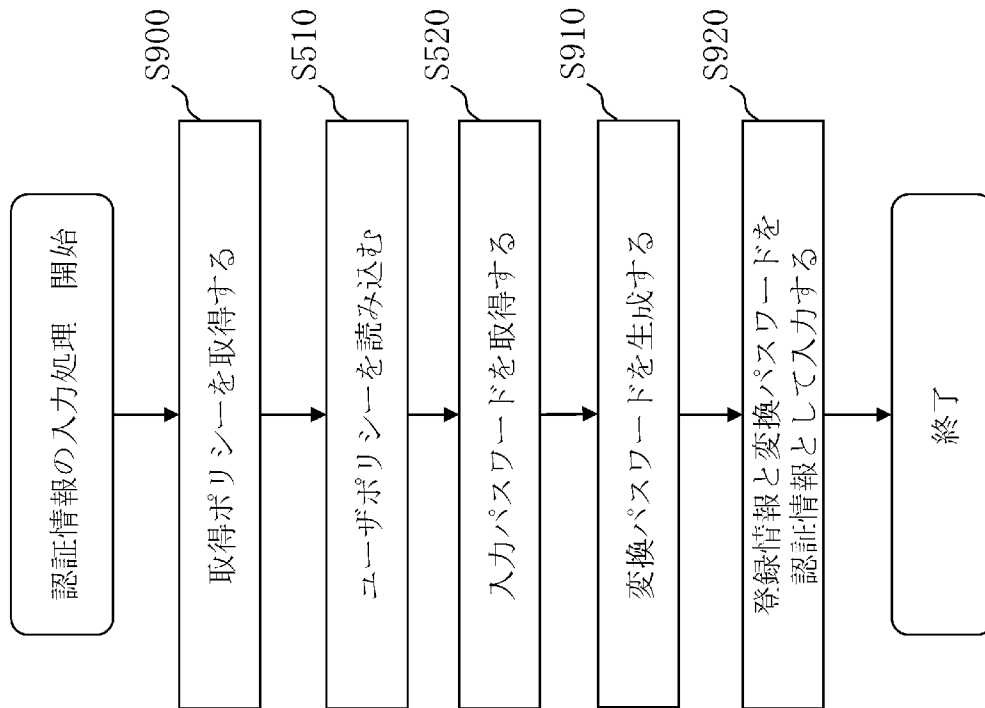
[図23]

図23



[図24]

図24



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/021763

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F21/46 (2013.01) i

FI: G06F21/46

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

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 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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 2013-41514 A (MITSUBISHI ELECTRIC CORPORATION) 28 February 2013 (2013-02-28), paragraphs [0012]-[0051]	1-3, 5, 10-11 4, 6-9
A	GB 2525413 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 28 October 2015 (2015-10-28)	9

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

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 25 August 2020	Date of mailing of the international search report 08 September 2020
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2020/021763

JP 2013-41514 A 28 February 2013 (Family: none)

GB 2525413 A 28 October 2015 US 2015/0310206 A1

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/46(2013.01)i FI: G06F21/46														
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）） G06F21/46														
最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2020年</td> </tr> </table>			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2020年	日本国実用新案登録公報	1996 - 2020年	日本国登録実用新案公報	1994 - 2020年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2020年													
日本国実用新案登録公報	1996 - 2020年													
日本国登録実用新案公報	1994 - 2020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 2013-41514 A (三菱電機株式会社) 28.02.2013 (2013 - 02 - 28)	1-3, 5, 10-11												
A	[0012]-[0051]													
	[0012]-[0071]	4, 6-9												
A	GB 2525413 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 28.10.2015 (2015 - 10 - 28)	9												
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの</td> </tr> <tr> <td>“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの</td> <td>“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの</td> </tr> <tr> <td>“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献	“O” 口頭による開示、使用、展示等に言及する文献		“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献	
* 引用文献のカテゴリー	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの													
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの	“Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの													
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）	“&” 同一パテントファミリー文献													
“O” 口頭による開示、使用、展示等に言及する文献														
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献														
国際調査を完了した日 25.08.2020	国際調査報告の発送日 08.09.2020													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 打出 義尚 5S 4440 電話番号 03-3581-1101 内線 3546													

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/021763

引用文献			公表日	パテントファミリー文献	公表日
JP	2013-41514	A	28.02.2013	(ファミリーなし)	
GB	2525413	A	28.10.2015	US 2015/0310206	A1