

(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
2015 年 12 月 30 日(30.12.2015)



(10) 国際公開番号

WO 2015/198451 A1

- (51) 国際特許分類:
G06F 21/31 (2013.01)
- (21) 国際出願番号: PCT/JP2014/066993
- (22) 国際出願日: 2014 年 6 月 26 日(26.06.2014)
- (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: 楽天株式会社(RAKUTEN, INC.) [JP/JP]; 〒1400002 東京都品川区東品川四丁目 1 2 番 3 号 Tokyo (JP).
- (72) 発明者: 山原 久範(YAMAHARA Hisanori); 〒1400002 東京都品川区東品川四丁目 1 2 番 3 号 楽天株式会社内 Tokyo (JP).
- (74) 代理人: 特許業務法人 インテクト国際特許事務所, 外(INTECT INTERNATIONAL PATENT OFFICE et al.); 〒1020083 東京都千代田区麹町四丁目 7 番 2 号 Daiwa 麹町 4 丁目ビル 4 階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA,

BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーロパ (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).

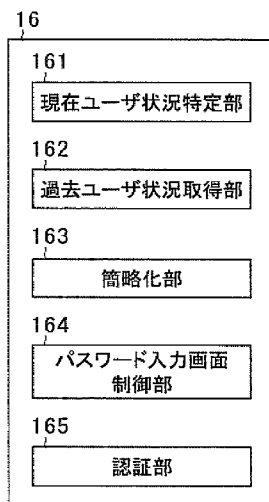
添付公開書類:

— 国際調査報告 (条約第 21 条(3))

(54) Title: INFORMATION-PROCESSING DEVICE, INFORMATION-PROCESSING METHOD, AND INFORMATION-PROCESSING PROGRAM

(54) 発明の名称: 情報処理装置、情報処理方法及び情報処理プログラム

[図2B]



- 161 Unit for specifying current conditions of user
162 Unit for acquiring past conditions of user
163 Simplification unit
164 Password input screen control unit
165 Authentication unit

(57) Abstract: The purpose of the present invention is to make it possible to simplify the authentication information to be inputted by a user while securing safety. An information-processing device specifies the current conditions in which the user is situated. The information-processing device acquires the conditions in which the user was situated at the time of past authentication. When the user is currently in an authenticated state, the information-processing device simplifies the authentication information to be inputted by the user in accordance with the current and the past conditions. The information-processing device outputs information for prompting the input of simplified authentication information.

(57) 要約: 安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することを可能とすることを目的とする。情報処理装置は、ユーザが置かれている現在の状況を特定する。情報処理装置は、過去の認証時にユーザが置かれていた状況を取得する。情報処理装置は、ユーザが現在認証されている状態である場合、現在の状況及び過去の状況に応じて、ユーザが入力すべき認証情報を簡略化する。情報処理装置は、簡略化された認証情報の入力を促す情報を出力する。

明 細 書

発明の名称：

情報処理装置、情報処理方法及び情報処理プログラム

技術分野

[0001] 本発明は、認証に用いられる認証情報のユーザによる入力を受け付ける技術分野に関する。

背景技術

[0002] 従来、サービスや機能等を利用するために、ユーザに対する認証が行われる場合がある。この認証のため、ユーザは認証情報を入力する。認証情報として、例えばパスワード（例えば、非特許文献1）や生体情報等がある。こうした認証情報の入力は、例えばユーザがサービスを初めて利用するときに要求される。その後、例えば一定期間は認証情報の入力が要求されなかったり、例えば利用中のサービス内の特定のサービスをユーザが利用するときに認証情報の入力が再度要求されたりすることがある。

先行技術文献

非特許文献

[0003] 非特許文献1：Yahoo! Inc.、 “Sign in to Yahoo”、 [online]、 [平成26年5月28日検索]、 インターネット<URL: <https://login.yahoo.com/config/login?.src=fpctx&.intl=us&.done=https%3A%2F%2Fwww.yahoo.com%2F>>

発明の概要

発明が解決しようとする課題

[0004] しかしながら、特定のサービスや機能を利用するたびに認証情報の全てを再入力することはユーザにとって煩雑であった。そこで、認証情報の入力を省略することも考えられるものの、そうした対応は安全性の観点からは好ましくない。

[0005] 本発明は、以上の点に鑑みてなされたものであり、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することを可能とする情報処理装置、

情報処理方法及び情報処理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

- [0006] 上記課題を解決するために、請求項 1 に記載の発明は、ユーザが置かれている現在の状況を特定する特定手段と、過去の認証時に前記ユーザが置かれていた状況を取得する取得手段と、前記ユーザが現在認証されている状態である場合、前記特定手段により特定された前記現在の状況及び前記取得手段により取得された前記過去の状況に応じて、前記ユーザが入力すべき認証情報を簡略化する簡略化手段と、前記簡略化手段により簡略化された前記認証情報の入力を促す情報を出力する出力手段と、を備えることを特徴とする。
- [0007] この発明によれば、情報処理装置は、ユーザが認証されている状態において、ユーザの現在の状況と過去の認証時のユーザの状況に応じて認証情報を簡略化する。そのため、ユーザは簡略化された認証情報を入力すればよい。従って、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することができる。
- [0008] 請求項 2 に記載の発明は、請求項 1 に記載の情報処理装置において、前記ユーザが認証されている状態で再度の認証を要する利用対象を前記ユーザが利用しようとするごとに、前記取得手段、前記特定手段、前記簡略化手段及び前記出力手段は動作し、前記簡略化手段は、前記特定手段により特定された状況と前記取得手段により取得された状況とが一致することに応じて簡略化された認証情報を用いる認証が連続する場合、前回の簡略化の度合いよりも小さい度合いで簡略化された認証情報を生成することを特徴とする。
- [0009] この発明によれば、現在と過去の状況が一致する場合であっても、状況が一致することに応じた認証が連続すると、情報処理装置は認証情報の簡略化の度合いを小さくする。そのため、前回の認証時よりもパスワードの入力負担が重くなる。従って、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することができる。
- [0010] 請求項 3 に記載の発明は、請求項 1 又は 2 に記載の情報処理装置において、前記簡略化手段は、前記現在の状況と前記過去の状況とが異なる場合、状

況の差が大きいほど小さい度合いで簡略化された認証情報を生成することを特徴とする。

[0011] この発明によれば、現在と過去の状況の差が大きいほど、情報処理装置は認証情報の簡略化の度合いを小さくする。従って、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することができる。

[0012] 請求項 4 に記載の発明は、請求項 3 に記載の情報処理装置において、前記ユーザが認証されている状態で再度の認証を要する利用対象を前記ユーザが利用しようとするごとに、前記取得手段、前記特定手段、前記簡略化手段及び前記出力手段は動作し、前記簡略化手段は、前記特定手段により特定された状況と前記取得手段により取得された状況とが異なることに応じて簡略化された認証情報を用いる認証が連続するごとに、前回の簡略化の度合いと同じ度合いで認証情報を簡略化することが可能な状況の差を前回よりも小さくすることを特徴とする。

[0013] この発明によれば、現在と過去の状況が異なることに応じた認証が連続する場合、前回の認証時の簡略化の度合いと同じ度合いで情報処理装置が認証情報を簡略化するための状況の差が、前回よりも小さくなる。従って、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することができる。

[0014] 請求項 5 に記載の発明は、請求項 1 乃至 4 の何れか 1 項に記載の情報処理装置において、前記簡略化手段は、前記現在の状況が、安全性に関連する所定条件に合致しない場合、前記認証情報を簡略化しないことを特徴とする。

[0015] この発明によれば、ユーザが現在置かれている状況が安全性に関連する条件に合致しない場合、ユーザは本来入力すべき認証情報を全部入力する必要がある。そのため、安全性を確保することができる。

[0016] 請求項 6 に記載の発明は、請求項 1 乃至 5 の何れか 1 項に記載の情報処理装置において、前記簡略化手段は、前記現在の状況と前記過去の状況とに応じて、前記ユーザが本来入力すべき認証情報のうち簡略化によって前記ユーザに入力させる部分を異ならせることを特徴とする。

[0017] この発明によれば、情報処理装置がユーザに入力させる部分を異ならせる

ことで、簡略化の度合いを変えることができる。

[0018] 請求項 7 に記載の発明は、請求項 6 に記載の情報処理装置において、前記簡略化手段は、前記認証情報が複数のコードを含む場合、前記現在の状況と前記過去の状況との差に応じて、前記ユーザが本来入力すべき認証情報のうち簡略化によって前記ユーザに入力させるコードの種類を異ならせることを特徴とする。

[0019] この発明によれば、情報処理装置がユーザに入力させるコードの種類を異ならせることで、簡略化の度合いを変えることができる。

[0020] 請求項 8 に記載の発明は、請求項 6 又は 7 に記載の情報処理装置において、前記簡略化手段は、前記認証情報が複数のコードを含む場合、前記現在の状況と前記過去の状況との差に応じて、前記ユーザが本来入力すべき認証情報のうち簡略化によって前記ユーザに入力させるコードの種類を異ならせることを特徴とする。

[0021] この発明によれば、情報処理装置がユーザに入力させるコードの種類を異ならせることで、簡略化の度合いを変えることができる。

[0022] 請求項 9 に記載の発明は、請求項 6 乃至 8 の何れか 1 項に記載の情報処理装置において、前記簡略化手段は、前記認証情報が複数のコードを含む場合、前記現在の状況と前記過去の状況との差に応じて、前記認証情報に含まれる複数のコードのうち前記ユーザが入力すべきコードの数を異ならせることを特徴とする。

[0023] この発明によれば、情報処理装置がユーザに入力させるコードの数を異ならせることで、簡略化の度合いを変えることができる。

[0024] 請求項 10 に記載の発明は、請求項 1 乃至 9 の何れか 1 項に記載の情報処理装置において、記憶手段に記憶された、前記ユーザが本来入力すべき認証情報から、前記簡略化手段により簡略化された認証情報に含まれない部分を取得する部分取得手段と、前記部分取得手段により取得された部分で、前記出力手段により出力された前記情報に応じて入力された認証情報を補完することにより生成された認証情報を取得する認証情報取得手段と、前記認証情

報取得手段により取得された前記認証情報と、前記記憶手段に記憶された前記認証情報とを比較して前記ユーザの認証の成否を判定する判定手段と、を更に備えることを特徴とする。

[0025] この発明によれば、記憶手段に記憶された認証情報と補完によって生成された認証情報とが一致するか否かに基づいて、情報処理装置は認証の成否を判定することができる。

[0026] 請求項 1 1 に記載の発明は、請求項 1 乃至 9 の何れか 1 項に記載の情報処理装置において、記憶手段に記憶された、前記ユーザが本来入力すべき認証情報のうち、前記簡略化手段により簡略化された認証情報の位置を特定する位置特定手段と、前記出力手段により出力された前記情報に応じて入力された認証情報と、前記記憶手段に記憶された前記認証情報のうち前記位置特定手段により特定された位置にある部分とを比較して前記ユーザの認証の成否を判定する判定手段と、を更に備えることを特徴とする。

[0027] この発明によれば、情報処理装置は、ユーザにより入力された認証情報に情報を補完しなくても、認証の成否を判定することができる。

[0028] 請求項 1 2 に記載の発明は、請求項 1 乃至 1 1 の何れか 1 項に記載の情報処理装置において、前記出力手段は、前記ユーザが本来入力すべき認証情報のうち前記簡略化手段により簡略化された前記認証情報に含まれない部分について所定記号を出力することを特徴とする。

[0029] この発明によれば、ユーザは所定記号を見ることにより、本来入力すべき認証情報のうちユーザが入力する必要がない部分を認識することができる。

[0030] 請求項 1 3 に記載の発明は、請求項 1 乃至 1 2 の何れか 1 項に記載の情報処理装置において、前記出力手段により出力された前記情報に応じて入力された認証情報を用いた認証が失敗した場合、前記出力手段は、前記ユーザが本来入力すべき認証情報全部の入力を促す第 2 情報を出力することを特徴とする。

[0031] この発明によれば、簡略化された認証情報を用いた認証の失敗により、認証情報を入力した者が認証されているユーザであることが疑わしい場合であ

っても、安全性を確保することができる。

[0032] 請求項 1 4 に記載の発明は、請求項 1 乃至 1 3 の何れか 1 項に記載の情報処理装置において、前記簡略化手段は、前記ユーザが入力すべき該ユーザの識別情報を簡略化し、前記出力手段は、前記簡略化手段により簡略化された前記識別情報の入力を促す前記情報を出力することを特徴とする。

[0033] この発明によれば、情報処理装置がユーザの現在と過去の認証時のユーザの状況に応じてパスワードを簡略化する。従って、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することができる。

[0034] 請求項 1 5 に記載の発明は、コンピュータにより実行される情報処理方法であって、ユーザが置かれている現在の状況を特定する特定ステップと、過去の認証時に前記ユーザが置かれていた状況を取得する取得ステップと、前記ユーザが現在認証されている状態である場合、前記特定ステップにより特定された前記現在の状況及び前記取得ステップにより取得された前記過去の状況に応じて、前記ユーザが入力すべき認証情報を簡略化する簡略化ステップと、前記簡略化ステップにより簡略化された前記認証情報の入力を促す情報を出力する出力ステップと、を含むことを特徴とする。

[0035] 請求項 1 6 に記載の発明は、コンピュータを、ユーザが置かれている現在の状況を特定する特定手段、過去の認証時に前記ユーザが置かれていた状況を取得する取得手段、前記ユーザが現在認証されている状態である場合、前記特定手段により特定された前記現在の状況及び前記取得手段により取得された前記過去の状況に応じて、前記ユーザが入力すべき認証情報を簡略化する簡略化手段、及び、前記簡略化手段により簡略化された前記認証情報の入力を促す情報を出力する出力手段、として機能させることを特徴とする。

発明の効果

[0036] 本発明によれば、情報処理装置は、ユーザが認証されている状態において、ユーザの現在の状況と過去の認証時のユーザの状況に応じて認証情報を簡略化する。そのため、ユーザは簡略化された認証情報を入力すればよい。従って、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化すること

ができる。

図面の簡単な説明

[0037] [図1A]認証装置 1 をサーバ装置に適用した場合の情報処理システム S 1 の概要構成の一例を示す図である。

[図1B]認証装置 1 を端末装置に適用した場合の情報処理システム S 2 の概要構成の一例を示す図である。

[図2A]一実施形態に係る認証装置 1 の概要構成の一例を示すブロック図である。

[図2B]一実施形態に係る認証装置 1 のシステム制御部 1 6 の機能ブロックの一例を示す図である。

[図3A]簡略度の決定方法の一例を示す図である。

[図3B]ユーザに入力させる文字種のバリエーション数の決定方法の一例を示す図である。

[図3C]パスワードの簡略化の例を示す図である。

[図3D]ユーザに入力させる文字種の数決定方法の一例を示す図である。

[図3E]パスワードの簡略化の例を示す図である。

[図3F]ユーザに入力させる文字数の決定方法の一例を示す図である。

[図3G]パスワードの簡略化の例を示す図である。

[図4A]パスワード入力画面の表示例を示す図である。

[図4B]パスワード入力画面の表示例を示す図である。

[図4C]パスワード入力画面の表示例を示す図である。

[図4D]パスワード入力画面の表示例を示す図である。

[図5]一実施形態に係る認証装置 1 のシステム制御部 1 6 のログイン認証処理の一例を示すフローチャートである。

[図6]一実施形態に係る認証装置 1 のシステム制御部 1 6 のパスワード入力画面出力処理の一例を示すフローチャートである。

[図7]一実施形態に係る認証装置 1 のシステム制御部 1 6 の簡略化処理の一例を示すフローチャートである。

[図8A]入力文字決定処理の例を示すフローチャートである。

[図8B]入力文字決定処理の例を示すフローチャートである。

[図8C]入力文字決定処理の例を示すフローチャートである。

[図9]一実施形態に係る認証装置 1 のシステム制御部 1 6 のパスワード入力画面生成処理の一例を示すフローチャートである。

[図10A]一実施形態に係るユーザ端末 2 のパスワード送信処理の一例を示すフローチャートである。

[図10B]一実施形態に係る認証装置 1 のシステム制御部 1 6 の簡略化パスワード認証処理の一例を示すフローチャートである。

[図11]簡略度の決定方法の一例を示す図である。

[図12]一実施形態に係る認証装置 1 のシステム制御部 1 6 のログイン認証処理の一例を示すフローチャートである。

[図13]一実施形態に係る認証装置 1 のシステム制御部 1 6 の簡略化処理の一例を示すフローチャートである。

[図14]簡略度の決定方法の一例を示す図である。

[図15]一実施形態に係る認証装置 1 のシステム制御部 1 6 の簡略化処理の一例を示すフローチャートである。

[図16A]簡略度の決定方法の一例を示す図である。

[図16B]簡略度の決定方法の一例を示す図である。

[図16C]簡略度の決定方法の一例を示す図である。

[図17]一実施形態に係る認証装置 1 のシステム制御部 1 6 のログイン認証処理の一例を示すフローチャートである。

[図18]一実施形態に係る認証装置 1 のシステム制御部 1 6 の簡略化処理の一例を示すフローチャートである。

[図19]、一実施形態に係る認証装置 1 のシステム制御部 1 6 のパスワード入力画面出力処理の一例を示すフローチャートである。

[図20]一実施形態に係るユーザ端末 2 のパスワード送信処理の一例を示すフローチャートである。

[図21]一実施形態に係る認証装置1のシステム制御部16の簡略化パスワード認証処理の一例を示すフローチャートである。

[図22]一実施形態に係る認証装置1のシステム制御部16の簡略化パスワード認証処理の一例を示すフローチャートである。

[図23]パスワード入力画面の表示例を示す図である。

[図24]一実施形態に係る認証装置1のシステム制御部16の簡略化処理の一例を示すフローチャートである。

[図25]一実施形態に係る認証装置1のシステム制御部16のパスワード入力画面生成処理の一例を示すフローチャートである。

[図26]一実施形態に係るユーザ端末2のパスワード送信処理の一例を示すフローチャートである。

[図27]一実施形態に係る認証装置1のシステム制御部16の簡略化パスワード認証処理の一例を示すフローチャートである。

発明を実施するための形態

[0038] 以下、図面を参照して本発明の実施形態について詳細に説明する。なお、以下に説明する実施の形態は、複数の文字コードを含むパスワードを用いた認証を行う認証装置に対して本発明を適用した場合の実施形態である。データとしてのパスワードは、実際には文字を示す文字コードを含む。ただし、実施形態においては、説明の便宜上、文字コードのことも単に文字と称する。また、実施形態においては、記号も文字に含まれるものとする。

[0039] [1. 第1実施形態]

認証装置は、ユーザにより入力されたパスワードを用いたユーザ認証を行うコンピュータである。また、認証装置は、ユーザの現在の状況及び過去に置かれていた状況に基づいて、ユーザが入力すべきパスワードを簡略化する。認証装置は、例えばサーバ装置であってもよいし、端末装置であってもよい。まずは認証装置がサーバ装置に適用された場合について説明し、最後に認証装置が端末装置に適用された場合について説明する。

[0040] [1-1. 情報処理システムの概要]

先ず、本実施形態に係る情報処理システム S 1 の概要について、図 1 A を用いて説明する。図 1 A は、認証装置 1 をサーバ装置に適用した場合の情報処理システム S 1 の概要構成の一例を示す図である。

[0041] 図 1 A に示すように、情報処理システム S 1 は、サーバ装置としての認証装置 1 と複数のユーザ端末 2 とを含んで構成されている。そして、認証装置 1 と各ユーザ端末 2 とは、ネットワーク NW を介して、例えば、通信プロトコルに TCP / IP 等を用いて相互にデータの送受信が可能になっている。なお、ネットワーク NW は、例えば、インターネット、専用通信回線（例えば、CATV (Community Antenna Television) 回線）、移動体通信網（基地局等を含む）、及びゲートウェイ等により構築されている。

[0042] 認証装置 1 は、例えば、情報処理システム S 1 を利用するユーザへ所定のサービスを提供するための処理を行うサーバ装置であってもよい。或いは、認証装置 1 は、例えば情報処理システム S 1 で提供されるサービスをユーザが受けるためのユーザ認証を行う認証サーバであってもよい。認証装置 1 は、ユーザ情報 DB 3 にアクセス可能に構成されている。ユーザ情報 DB 3 は、情報処理システム S 1 に会員登録されたユーザに関する情報を登録するデータベースである。例えば、ユーザ情報 DB 3 には、ユーザごとにユーザ ID、パスワード等が対応付けて登録されている。ユーザ ID は、ユーザの識別情報である。パスワードは、本発明における認証情報の一例である。情報処理システム S 1 自身がユーザ情報 DB 3 を備えてもよいし、情報処理システム S 1 とユーザ情報 DB 3 がネットワークを介して接続されてもよい。ユーザ情報 DB 3 には、例えば所定の登録要件を満たすパスワードのみが登録されてもよい。登録要件は、例えばパスワードの文字数が所定数以上であることであってもよい。また登録要件は、例えばパスワードの文字数が第 1 所定数以上であり且つ第 2 所定数以下であることであってもよい。また登録要件は、例えばパスワードに含まれる文字の種類が所定数以上であることであってもよい。また登録要件は、例えばパスワードに含まれる文字が所定の種類の文字を必ず含むことであってもよい。また登録要件は、例えば複数の条

件の組み合わせであってもよい。管理者はパスワードに用いることが可能な文字種を自由に決めることができる。文字種として、例えば、英小文字、英大文字、数字、記号、マルチバイト文字等がある。マルチバイト文字として、例えば、漢字、ひらがら、片仮名などがある。ユーザを認証するとき、認証装置 1 は、ユーザ端末 2 からユーザ ID 及びパスワードを受信する。認証装置 1 は、例えば受信したユーザ ID に対応するパスワードをユーザ情報 DB 3 から取得し、取得したパスワードと受信したパスワードとが一致するかどうかを判定する。認証装置 1 は、パスワードが一致する場合には、認証が成功したと判定し、パスワードが一致しない場合には、認証が失敗したと判定する。認証が成功することにより、ユーザは情報処理システム S 1 にログインする。

[0043] ユーザ端末 2 は、情報処理システム S 1 を利用しようとするユーザが用いる端末装置である。端末装置の例として、スマートフォン、タブレット型コンピュータ、携帯電話機、パーソナルコンピュータ、PDA (Personal Digital Assistant)、STB (Set Top Box) 等がある。ユーザ端末 2 は、例えば CPU、ROM、RAM、フラッシュメモリ、ハードディスクドライブ等を備えてもよい。また、ユーザ端末 2 には、例えばブラウザ、電子メールクライアント等のソフトウェアがインストールされている。

[0044] ユーザが情報処理システム S 1 にログインすると、例えばユーザがログアウトの操作を行うまでそのユーザは認証装置 1 によって認証されている状態である。すなわち、ログイン中であるユーザは認証されている状態にある。また例えば、ログインから所定期間が経過したとき、認証装置 1 は自動的にログインを解除してもよい。ユーザがログイン中であるとき、ユーザは、例えば情報処理システム S 1 から会員に提供される基本的なサービスや機能を利用可能である。その一方で、ユーザがログイン中であっても、ユーザが特定のサービス又は機能の利用を認証装置 1 へ要求したとき、認証装置 1 は、ユーザ認証を再度行う。サービス及び機能は、本発明における利用対象の例である。このようなサービス又は機能としては、例えば情報処理システム S

1で提供されるサービス又は機能の中で特に安全性が要求されるサービス又は機能が挙げられる。このようなサービス、機能の例として、商品の購入、サービスの予約、購入履歴の閲覧、会員情報の変更等が挙げられる。この場合、ユーザはパスワードを再度入力する必要がある。パスワードの再入力の際、認証装置1は例えばユーザIDの入力を省略可能にしてもよい。そうではあっても、特定のサービス又は機能を利用するたびに、ユーザ情報DB3に登録されているパスワードをユーザが全部入力することは、ユーザにとって負担である。このような理由から、パスワードの入力も省略することも考えられる。しかしながら、パスワードの入力の省略は、安全性の観点から好ましくない。

[0045] そこで、ユーザがログイン中である場合に再度の認証を要するとき、認証装置1は、ユーザが現在置かれている状況、及び過去の認証時にそのユーザが置かれていた状況に応じて、ユーザが入力すべきパスワードを簡略化する。そして、認証装置1は、簡略化されたパスワードの入力をユーザに促す情報を出力する。簡略化されたパスワードに対して、ユーザ情報DB3に登録されているパスワードを登録パスワードと称する。登録パスワードは、本来入力すべきパスワードである。パスワードの簡略化は、例えば登録パスワードの中の一部の文字の入力を省略することである。従って、簡略化されたパスワードは登録パスワードよりも短くなっている。従って、登録パスワードの全部を入力するよりも、簡略化されたパスワードを入力する方がユーザにとって簡単である。認証装置1は、ユーザの現在及び過去の状況に基づき、例えば現在の状況の安全性を判定してもよい。この場合の安全性とは、例えばパスワードを入力する者がユーザ本人であることの蓋然性であってもよい。すなわち、パスワードを入力する者がユーザ本人であるという蓋然性が高いほど、簡単に入力することが可能なパスワードを入力させる。これによって、安全性を確保しつつ、ユーザが入力すべき認証情報を簡略化することができる。

[0046] [1-2. 認証装置の構成]

次に、認証装置 1 の構成について、図 2 A を用いて説明する。図 2 A は、本実施形態に係る認証装置 1 の概要構成の一例を示すブロック図である。図 2 A に示すように、認証装置 1 は、通信部 1 1 と、記憶部 1 2 と、操作部 1 3 と、表示部 1 4 と、入出力インターフェース 1 5 と、システム制御部 1 6 と、を備えている。そして、システム制御部 1 6 と入出力インターフェース 1 5 とは、システムバス 1 7 を介して接続されている。

[0047] 通信部 1 1 は、ネットワーク NW に接続して、ユーザ端末 2 等との通信状態を制御する。記憶部 1 2 は、データやプログラムを記憶する。記憶部 1 2 の例として、ハードディスクドライブ、フラッシュメモリ等が挙げられる。記憶部 1 2 には、例えばユーザ情報 DB 3 が記憶されていてもよい。記憶部 1 2 には、更にオペレーティングシステム、認証処理プログラム等のプログラムが記憶されている。認証処理プログラムは、ユーザの認証に関する処理を行うためのプログラムである。認証処理プログラムは、本発明における情報処理プログラムの一例である。なお、各種のプログラムは、例えば、他のサーバ装置等からネットワーク NW を介して取得されるようにしてもよいし、光ディスク等の記録媒体に記録されてドライブ装置を介して読み込まれるようにしてもよい。操作部 1 3 は、操作者による操作を受け付け、操作内容に対応する信号をシステム制御部 1 6 に出力する。操作部 1 3 の例として、キー、ボタン、スイッチ、キーボード、マウス、タッチパネル、リモコン等が挙げられる。なお、認証装置 1 は操作部 1 3 を備えていなくてもよい。例えば認証装置 1 は、操作部 1 3 と有線又は無線により接続されていてもよい。表示部 1 4 は、システム制御部 1 6 の制御により、画像、文字等の情報を表示する。表示部 1 4 の例として、液晶ディスプレイ、CRT ディスプレイ、LED 等が挙げられる。なお、認証装置 1 は表示部 1 4 を備えていなくてもよい。例えば認証装置 1 は、表示部 1 4 と有線又は無線により接続されていてもよい。入出力インターフェース 1 5 は、通信部 1 1 及び記憶部 1 2 とシステム制御部 1 6 との間のインターフェース処理を行う。システム制御部 1 6 は、CPU (Central Processing Unit) 1 6 a、ROM (Read Only Me

mory) 16b、RAM (Random Access Memory) 16c等により構成されている。CPU 16aは、プロセッサの一例である。なお、本発明は、CPUと異なる様々なプロセッサに対しても適用可能である。記憶部12、ROM 16b及びRAM 16cは、それぞれメモリの一例である。なお、本発明は、ハードディスク、ROM及びRAMと異なる様々なメモリに対しても適用可能である。

[0048] [1-3. システム制御部の機能概要]

次に、図2B乃至図4Dを用いて、システム制御部16の機能概要について説明する。図2Bは、本実施形態に係る認証装置1のシステム制御部16の機能ブロックの一例を示す図である。システム制御部16は、CPU 16aが、認証処理プログラム等のプログラムを読み出し実行することにより、図2Bに示すように、現在ユーザ状況特定部161、過去ユーザ状況取得部162、簡略化部163、パスワード入力画面出力部164、認証部165等として機能する。現在ユーザ状況特定部161は、本発明における特定手段の一例である。過去ユーザ状況取得部162は、本発明における取得手段の一例である。簡略化部163は、本発明における簡略化手段の一例である。パスワード入力画面出力部164は、本発明における出力手段の一例である。認証部165は、本発明における判定手段の一例である。

[0049] 現在ユーザ状況特定部161は、ユーザの認証時、そのユーザが現在置かれている状況を特定する。例えば、現在ユーザ状況特定部161は、ユーザの状況を示すユーザ状況情報を取得する。ユーザの状況の例として、ユーザの位置、ユーザが利用するユーザ端末2の位置、時刻等が挙げられる。ユーザやユーザ端末2の位置の例として、絶対的な位置や相対的な位置が挙げられる。絶対的な位置を示すユーザ状況情報の例として、ユーザ又はユーザ端末2の地理的位置や、ユーザ端末2に割り当てられたIPアドレス等が挙げられる。相対的な位置を示すユーザ状況情報の例として、特定の装置からの距離、ユーザとは異なる誰かからの距離等が挙げられる。現在ユーザ状況特定部161は、1つの状況のみを特定してもよいし、複数の状況を特定して

もよい。

- [0050] 例えば、ユーザ端末2がGPS (Global Positioning System) を備える場合、ユーザ端末2はユーザ端末2が位置する場所の経緯度等を示す位置情報を取得することができる。また例えば、ユーザ端末2が、スマートフォンや携帯電話機等の移動体通信端末である場合、基地局の位置情報に基づいて、ユーザ端末2の位置情報を取得することができる。このような場合、現在ユーザ状況特定部161は、ユーザ端末2から位置情報をユーザ状況情報として取得してもよい。また、現在ユーザ状況特定部161は、ユーザ端末2から認証装置1へ送信されるパケットのヘッダからユーザ端末2のIPアドレスをユーザ状況情報として取得することができる。IPアドレスにより、例えばユーザ端末2が位置する地域を特定することができる場合がある。また例えば、ユーザ端末2が無線LANを介してネットワークNWに接続する場合、ユーザ端末2は、アクセスポイントと通信することにより無線LANに接続する。このとき、ユーザ端末2は、アクセスポイントから送信されてくる信号の強度を検出してもよい。アクセスポイントからの信号の強度により、アクセスポイントからのユーザ端末2までの距離を大まかに推定することができる。この距離は相対的な位置の例である。このような場合、現在ユーザ状況特定部161は、ユーザ端末2から、例えばアクセスポイントを識別する情報とアクセスポイントからの距離を示す情報とをユーザ状況情報として取得してもよい。アクセスポイントを識別する情報の例として、アクセスポイントのIPアドレス、SSID (Service Set Identifier) 等が挙げられる。距離を示す情報の例として、アクセスポイントからの信号の強度、信号強度に基づいてユーザ端末2が推定した距離等が挙げられる。また、システム制御部16は計時機能を有する。従って、現在ユーザ状況特定部161は、計時機能から現在時刻をユーザ状況情報として取得することができる。
- [0051] 過去ユーザ状況取得部162は、ユーザがログイン中に再度の認証を要するとき、過去の認証時にユーザが置かれていた状況を取得する。例えば、情報処理システムS1へログインするためのユーザの認証が成功したとき、認

証部 165 によりログインセッション情報が記憶部 12 に記憶される。ログインセッション情報は、ログイン中のユーザを識別するための情報である。ログインセッション情報は、例えばユーザ ID、セッション ID 等を含む。ユーザ ID は、ログイン中のユーザを示す。セッション ID は、セッションの識別情報である。例えば、ユーザの認証が成功したとき、認証部 165 は、そのときに現在ユーザ状況特定部 161 により取得されたユーザ状況情報をログインセッション情報内に登録してもよい。この場合、過去ユーザ状況取得部 162 は、再度の認証時に、ログインセッション情報からユーザ状況情報を取得してもよい。過去ユーザ状況取得部 162 は、例えばログイン時におけるユーザの状況を取得してもよいし、ログイン中に再度の認証が成功したときのユーザの状況を取得してもよい。すなわち、過去ユーザ状況取得部 162 は、ユーザが登録パスワードの全部を入力することにより認証が成功したときの状況を取得してもよいし、ユーザが簡略化されたパスワードを入力することにより認証が成功したときの状況を取得してもよい。

[0052] 簡略化部 163 は、現在ユーザ状況特定部 161 により特定されたユーザの現在の状況、及び過去ユーザ状況取得部 162 により取得されたユーザの過去の状況に応じて、ユーザが入力すべきパスワードを簡略化する。例えば、簡略化部 163 は、ユーザの現在の状況と過去の状況が一致しているか否かに応じて、又はユーザの現在の状況と過去の状況との差に応じて、パスワードの簡略度を決定してもよい。そして、簡略化部 163 は、決定した簡略度に応じてパスワードを簡略化してもよい。簡略度は、パスワードの簡略化の度合いを示す。例えば、認証装置 1 は、安全性が相対的に低い場合は簡略度を小さくし、安全性が相対的に高い場合は簡略度を大きくする。例えば、簡略化部 163 は、現在と過去の状況に基づいて特定される現在の状況の安全性が高いほど簡略度を大きくしてもよい。従って、簡略度は現在の状況の安全性をも示す。なお、簡略化部 163 は、簡略度を決定しなくてもよい。この場合、簡略化部 163 は、ユーザの現在と過去の状況に応じた度合いでパスワードを簡略化すればよい。

[0053] 本実施形態においては、簡略化部 163 は、現在の状況と過去の状況が一致しているか否かに応じて簡略度を決定するものとする。図 3A は、簡略度の決定方法の一例を示す図である。例えば、ユーザの現在の状況が、過去に認証が成功したときの状況と一致している場合、状況が一致しない場合よりも現在の状況が安全であると考えることができる。具体的に、過去にユーザの認証が成功したときから状況が変わっていない場合、状況が変わっている場合よりも、今回パスワードを入力する者が認証されたユーザ本人である蓋然性が高い。そこで、図 3A に示すように、簡略部 163 は、状況が一致している場合は状況が一致しない場合よりも大きい簡略度を決定してもよい。簡略化部 163 は、現在ユーザ状況特定部 161 により取得されたユーザ状況情報と過去ユーザ状況取得部 162 により取得されたユーザ状況情報とを比較することにより、現在の状況と過去の状況とが一致するか否かを判定する。すなわち、簡略化部 163 は、例えば現在のユーザ又はユーザ端末 2 の位置と過去の認証時のユーザ又はユーザ端末 2 の位置とを比較したり、現在時刻と過去の認証時の時刻とを比較したりする。このとき、過去ユーザ状況取得部 162 は、ユーザ状況情報が一致する場合には状況が一致すると判定する。また過去ユーザ状況取得部 162 は、ユーザ状況情報一致しない場合であっても、例えばユーザ状況情報の差が所定値以下であれば、状況が一致すると判定してもよい。そして、過去ユーザ状況取得部 162 は、ユーザ状況情報の差が所定値を超える場合には、状況が一致しないと判定してもよい。

[0054] 簡略化部 163 は、ユーザの現在と過去の状況に応じて、例えば登録パスワードのうち簡略化によってユーザに入力させる部分を異ならせる。例えば、簡略化部 163 は、現在と過去の状況に基づいて特定される現在の状況の安全性が高いほど、入力が簡単な部分、記憶しやすい部分又は思い出しやすい部分にパスワードを簡略化してもよい。

[0055] 簡略化によってユーザに入力させる部分を異ならせる方法としては様々な方法が挙げられる。例えば、簡略化部 163 は、現在と過去の状況に応じて

、登録パスワードのうち入力させる文字の種類を異ならせてもよい。図3Bは、ユーザに入力させる文字種のバリエーション数の決定方法の一例を示す図である。一般的に、パスワードは複数の文字種の文字を含む。文字種によってその文字種に属する文字の数が異なる。例えば、数字に属する文字の数は10であり、英小文字に属する文字の数は26である。或る文字種に属する文字の数をバリエーション数と称する。一般的に、バリエーション数が少ない文字種ほど、その文字種の文字の推測が簡単である。そこで、図3Bに示すように、簡略化部163は、安全性が低いほど、すなわち簡略度が低いほど、入力させる文字の種類を、バリエーション数が多い文字種に決定してもよい。図3Cは、パスワードの簡略化の例を示す図である。例えば、登録パスワードが「q3nifa83e」とする。安全な状況である場合、簡略化部163は、例えばパスワードを「383」に簡略化し、安全な状況ではない場合、簡略化部163は、例えばパスワードを「qni」に簡略化してもよい。登録パスワードが3種類以上の文字を含む場合、簡略化部163は、簡略化によってユーザに入力させる文字の種類を2種類以上決定してもよい。

- [0056] また例えば、簡略化部163は、現在と過去の状況に応じて、登録パスワードのうち入力させる文字の種類を異ならせてもよい。図3Dは、ユーザに入力させる文字種の数の決定方法の一例を示す図である。パスワードを入力するとき、一般的に入力する文字の種類が少ないほどパスワードの入力が簡単である。そこで、図3Dに示すように、簡略化部163は、安全性が低いほど、すなわち簡略度が低いほど、入力させる文字の種類を多くしてもよい。図3Eは、パスワードの簡略化の例を示す図である。例えば、登録パスワードが「q3nifa83e」とする。安全な状況である場合、簡略化部163は、例えばパスワードを「nifa」に簡略化し、安全な状況ではない場合、簡略化部163は、例えばパスワードを「a83e」に簡略化してもよい。なお、簡略化によってユーザに入力させる文字は登録パスワードにおいて連続していてもよいし連続していなくてもよい。

[0057] また例えば、簡略化部 163 は、現在と過去の状況に応じて、登録パスワードのうち入力させる文字数を異ならせてもよい。図 3 F は、ユーザに入力させる文字数の決定方法の一例を示す図である。パスワードを入力するとき、入力する文字数が少ないほどパスワードの入力が簡単である。そこで、図 3 F に示すように、簡略化部 163 は、例えば安全性が低いほど、すなわち簡略度が低いほど、入力させる文字数を多くしてもよい。図 3 G は、パスワードの簡略化の例を示す図である。例えば、登録パスワードが「q 3 n i f a 8 3 e」であるとする。安全な状況である場合、簡略化部 163 は、例えばパスワードを「q 3 n」に簡略化し、安全な状況ではない場合、簡略化部 163 は、例えばパスワードを「q 3 n i」に簡略化してもよい。簡略化部 163 は、ユーザに入力させる文字を決定するとき、例えば登録パスワードの先頭の文字から決定してもよいし、登録パスワードの末尾の文字から決定してもよいし、登録パスワードの途中の文字から決定してもよい。

[0058] また例えば、簡略化部 163 は、現在と過去の状況に応じて、登録パスワードのうち入力させる文字の位置を異ならせてもよい。一般的に、登録パスワードの先頭の文字の方が末尾の文字よりもユーザにとって入力が簡単である。具体的に、安全な状況である場合、簡略化部 163 は、例えばパスワードを先頭の所定数の文字に簡略化し、安全な状況ではない場合、簡略化部 163 は、例えばパスワードを末尾の所定数の文字に簡略化してもよい。また例えば、簡略化部 163 は、現在と過去の状況に応じて、登録パスワードのうち入力させる文字の位置を連続させるか否かを異ならせてもよい。一般的に、登録パスワードの中で連続している文字を入力する方が、不連続な文字を入力するよりもユーザにとって入力が簡単である。例えば、安全な状況である場合、簡略化部 163 は、登録パスワードの 1～3 番目の文字に簡略化し、安全な状況ではない場合、簡略化部 163 は、例えばパスワードを 1、3 及び 5 番目の文字に簡略化してもよい。また例えば、簡略化部 163 は、登録パスワードのうち簡略化によってユーザに入力させる部分を、複数の方法を組み合わせて決定してもよい。また例えば、簡略化部 163 は、登録パ

スワードの内容に応じて、簡略化の方法を決定してもよい。

[0059] パスワード入力画面出力部 164 は、簡略化されたパスワードの入力を促す情報を出力する。具体的に、パスワード入力画面出力部 164 は、パスワード入力画面のウェブページをユーザ端末 2 に出力する。

[0060] 図 4 A は、パスワード入力画面の表示例を示す図である。パスワード入力画面には、メッセージ 110、ユーザ ID 入力領域 120、パスワード入力領域 130、送信ボタン 140 が表示される。メッセージ 110 は、簡略化されたパスワードの入力を促すメッセージである。ユーザ ID 入力領域 120 は、ユーザ ID を入力するための領域である。ただし、ユーザ ID 入力領域 120 には、ログイン時にユーザが入力したユーザ ID が予め入力されている。従って、ユーザがユーザ ID 入力領域 120 のユーザ ID を変更する必要はない。なお、ユーザ ID 入力領域 120 にはユーザ ID が予め入力されていなくてもよい。この場合、ユーザは再度ユーザ ID を入力することになる。また例えば、ユーザ ID 入力領域 120 は表示されなくてもよい。この場合、ユーザはパスワードのみ入力すればよい。パスワード入力領域 130 は、パスワードを入力するための領域である。パスワード入力領域 130 には、1 つ以上のアスタリスク 131 が表示される。具体的に、登録パスワードのうち簡略化されたパスワードに含まれない文字の位置に対応して、アスタリスク 131 が表示される。図 4 A は、7 文字の登録パスワードを、末尾の 3 文字に簡略化した場合の例を示す。従って、パスワード入力領域 130 には、先頭の 4 文字分のアスタリスク 131 が表示されている。アスタリスク 131 により、登録パスワードの中で入力する必要がない文字をユーザが認識することができる。また、登録パスワードに含まれる文字が表示されないため、安全性を確保することができる。このような記号はアスタリスクと異なる記号であってもよい。パスワード入力領域 130 には、更にカーソル 132 が表示される。カーソル 132 は、簡略化されたパスワードにおける文字の入力位置を示す。例えば、登録パスワードのうちユーザが入力すべき部分の先頭の文字の位置にカーソル 132 が表示される。ユーザがパス

ワード入力領域 130 に文字を入力する都度、入力位置にアスタリスクが表示され、カーソル 132 が右に移動する。送信ボタン 140 は、パスワードを送信するためのボタンである。

[0061] 図 4 B は、7 文字の登録パスワードを、1、3 及び 5 番目の文字に簡略化した場合のパスワード入力画面の表示例を示す図である。図 4 B と同様に、パスワード入力領域 130 には、2、4、6 及び 7 番目の文字に対応してアスタリスク 131 が表示される。また、1、3 及び 5 番目の文字に対応して文字入力欄 133 が表示される。最も左に位置する文字入力欄 133 には、カーソル 132 が表示されている。ユーザが文字を入力した場合、カーソル 132 は、文字が入力された文字入力欄 133 の右にある文字入力欄 133 に移動してもよい。例えば、ユーザが 1 番目の文字を入力した場合、カーソル 132 は 3 番目の文字の位置に移動する。なお、アスタリスク 131 が表示されている位置に対応する文字、すなわち登録パスワードのうち簡略化されたパスワードに含まれない部分をユーザによって上書き可能なようにパスワード入力領域 130 が構成されてもよい。この場合、ユーザが 1 番目の文字を入力すると、例えばカーソル 132 は 2 番目の文字の位置に対応するアスタリスク 131 に移動してもよい。このとき、ユーザは、アスタリスク 131 に対応する文字を上書きすることも可能であるし、上書きをせずにカーソル 132 を移動させることも可能である。アスタリスク 131 が表示されている位置に対応する文字は、ユーザが入力する必要がない部分である。そのため、このような文字が上書きされたとしても、システム制御部 16 は文字入力欄 133 に入力された文字のみを用いてユーザ認証を行ってもよい。この場合、アスタリスク 131 が表示されている位置に対応する文字の上書きの有無、及び上書きされた文字の正誤は認証結果に影響しない。また例えば、システム制御部 16 は上書きされた文字も用いてユーザ認証を行ってもよい。この場合、アスタリスク 131 が表示されている位置に対応する文字が誤った文字で上書きされると、認証は失敗する。

[0062] 図 4 C は、図 4 A 及び図 4 B とは異なるパスワード入力画面の表示例を示

す図である。図4Cに示すように、パスワード入力画面には、メッセージ110、ユーザID入力領域120、文字入力位置表示領域150、簡略化パスワード入力領域160、送信ボタン140が表示されてもよい。文字入力位置表示領域150は、登録パスワードのうちユーザが入力すべき文字の位置を示す。文字入力位置表示領域150には、登録パスワードのうち簡略化されたパスワードに含まれる文字の位置に対応して空欄151が表示され、簡略化されたパスワードに含まれない文字の位置に対応してアスタリスク152が表示される。簡略化パスワード入力領域160には、1以上の文字入力欄161が表示される。各文字入力欄161は、簡略化されたパスワードの中の1文字を入力するための入力フィールドである。各文字入力欄161の位置は、文字入力位置表示領域150内の空欄151の位置と対応している。これにより、ユーザはどの位置の文字を入力すればよいかを認識することができる。最も左にある文字入力欄161には、入力位置を示すカーソル162が表示される。ユーザが何れかの文字入力欄161に文字を入力すると、例えばその位置にアスタリスクが表示され、文字入力された文字入力欄161の右にある文字入力欄161にカーソル162が移動してもよい。

[0063] パスワード入力画面で入力されたパスワードを用いた認証が失敗した場合、パスワード入力画面出力部164は、パスワード入力画面をユーザ端末2により表示させて、ユーザにパスワードを再度入力させる。このとき、パスワード入力画面出力部164は、簡略化されたパスワードを入力するためのパスワード入力画面を表示させてもよいし、登録パスワードの全部を入力するためのパスワード入力画面を表示させてもよい。認証が失敗した場合に登録パスワードをユーザに入力させることにより、安全性を確保することができる。図4Dは、登録パスワードの全部を入力するためのパスワード入力画面の表示例を示す図である。図4Dに示すように、パスワード入力画面には、メッセージ170、ユーザID入力領域120、パスワード入力領域180、送信ボタン140が表示される。メッセージ170は、登録パスワードの全部の入力を促すメッセージである。パスワード入力領域180は、登録

パスワードの全部を入力するための入力フィールドである。

[0064] 認証部 165 は、パスワード入力画面においてユーザにより入力されたパスワードを用いて認証処理を実行する。本実施形態において、認証部 165 は、登録パスワードのうち簡略化されたパスワードに含まれない部分で、ユーザにより入力されたパスワードを補完することにより生成されたパスワードを、認証用のパスワードとして取得する。そして、出力部 165 は、認証用のパスワードを登録パスワードと比較することにより、ユーザの認証の成否を判定する。例えば、7 文字の登録パスワードが末尾の 3 文字に簡略化された場合、ユーザにより入力されたパスワードの前に、登録パスワードの先頭 4 文字が追加されて、認証用のパスワードが生成される。例えば、ユーザ端末 2 により補完が行われてもよい。この場合、認証部 165 は、ユーザ端末 2 から認証用のパスワードを取得する。

[0065] [1-4. 情報処理システムの動作]

次に、情報処理システム S1 の動作について、図 5 乃至図 10B を用いて説明する。図 5 は、本実施形態に係る認証装置 1 のシステム制御部 16 のログイン認証処理の一例を示すフローチャートである。例えば、ユーザ端末 2 からのログインの要求に応じて認証装置 1 はログイン画面のウェブページをユーザ端末 2 へ出力する。ログイン画面は、ユーザ ID と登録パスワード全体とを入力するための画面である。ログイン画面においてユーザがユーザ ID 及びパスワードを入力すると、ユーザ端末 2 はユーザ ID 及びパスワードを認証装置 1 へ送信する。ユーザ端末 2 からユーザ ID 及びパスワードを受信したとき、システム制御部 16 はログイン認証処理を実行する。図 5 に示すように、認証部 165 は、受信したユーザ ID 及びパスワードと同じ組み合わせのユーザ ID 及びパスワードがユーザ情報 DB 3 に登録されているかを判定する（ステップ S1）。このとき、認証部 165 は、同じ組み合わせが登録されていないと判定した場合には（ステップ S1：NO）、ステップ S2 に進む。ステップ S2 において、認証部 165 は、ログイン画面のウェブページを再度ユーザ端末 2 へ出力して、ログイン認証処理を終了させ

る。一方、認証部 165 は、同じ組み合わせが登録されていると判定した場合には（ステップ S 1 : Y E S）、ステップ S 3 に進む。ステップ S 3 において、現在ユーザ状況特定部 161 は、現在のユーザの状況を示すユーザ状況情報を取得する。例えば、現在ユーザ状況特定部 161 は、ユーザ端末 2 から、ユーザ又はユーザ端末 2 の絶対的な位置を示す情報、ユーザ又はユーザ端末 2 の相対的な位置を示す情報を取得してもよい。また、現在ユーザ状況特定部 161 は、例えば計時部から現在時刻を取得してもよい。次いで、認証部 165 は、ログインセッション情報を生成して記憶部 12 に記憶させる（ステップ S 4）。具体的に、認証部 165 は、新たなセッション ID を生成する。そして、認証部 165 は、ユーザ端末 2 から受信したユーザ ID、セッション ID、ユーザ状況情報等を含むログインセッション情報を生成する。認証部 165 は、例えばログインの有効期限をログインセッション情報に含めてもよい。ステップ S 4 を終わると、認証部 165 は、ログイン完了後の画面のウェブページをユーザ端末 2 に出力する（ステップ S 5）。このとき、認証部 165 は、例えば生成したセッション ID を含むクッキーをユーザ端末 2 へ送信してもよい。これにより、ログインしたユーザのユーザ端末 2 から認証装置 1 へ送信される要求に、セッション ID が含まれるようになる。ステップ S 5 を終わると、認証装置 1 は、ログイン認証処理を終了させる。なお、ユーザが情報処理システム S 1 からログアウトした場合、認証装置 1 は記憶部 12 からログインセッション情報を削除する。

[0066] 図 6 は、本実施形態に係る認証装置 1 のシステム制御部 16 のパスワード入力画面出力処理の一例を示すフローチャートである。例えば、情報処理システム S 1 で提供されるサービス又は機能の中で、ユーザは再認証を要する特定のサービス又は機能を利用するための操作を行ったとする。このとき、ユーザ端末 2 は、特定利用要求を認証装置 1 へ送信する。ユーザ端末 2 から特定利用要求を受信したとき、システム制御部 16 がパスワード入力画面出力処理を実行する。図 6 に示すように、認証部 165 は、ユーザがログイン中であるか否かを判定する（ステップ S 11）。例えば、特定利用要求にセ

セッションIDが含まれていない場合、パスワード入力画面出力部164はログイン中ではないと判定する。また例えば、特定利用要求に含まれるセッションIDに対応するログインセッション情報が記憶部12に記憶されていない場合、パスワード入力画面出力部164はログイン中ではないと判定する。また例えば、ログインセッション情報に含まれる有効期限が切れている場合には、パスワード入力画面出力部164はログイン中ではないと判定する。ユーザがログイン中ではない場合（ステップS11：NO）、認証部165は、ステップS12に進む。ステップS12において、認証部165は、ログイン画面のウェブページをユーザ端末2に出力して、パスワード入力画面出力処理を終了させる。

[0067] 一方、例えば特定利用要求に含まれるセッションIDに対応するログインセッション情報の有効期限が切れていない場合、認証部165はユーザがログイン中であると判定する（ステップS11：YES）。この場合、認証部165は、ステップS13に進む。ステップS13において、現在ユーザ状況特定部161は、現在のユーザの状況を示すユーザ状況情報を取得する。ステップS13の処理は、図5に示すログイン認証処理のステップS3と同様である。次いで、簡略化部163は、特定したログインセッション情報に含まれるユーザIDに対応する登録パスワードをユーザ情報DB3から取得する（ステップS14）。次いで、簡略化部163は、簡略化処理を実行する（ステップS15）。簡略化処理は、ユーザが入力すべきパスワードを簡略化する処理である。次いで、パスワード入力画面出力部164は、パスワード入力画面生成処理を実行する（ステップS16）。パスワード入力画面生成処理は、簡略化されたパスワードを入力するためのパスワード入力画面のウェブページを生成する処理である。簡略化処理及びパスワード入力画面生成処理の詳細については後述する。次いで、パスワード入力画面出力部164は、生成されたパスワード入力画面のウェブページをユーザ端末2に出力する（ステップS17）。ステップS16を終えると、パスワード入力画面出力部164はパスワード入力画面出力処理を終了させる。

[0068] 図7は、本実施形態に係る認証装置1のシステム制御部16の簡略化処理の一例を示すフローチャートである。図7に示すように、簡略化部163は、パスワード入力画面出力処理で特定されたログインセッション情報から、過去のユーザの状況を示すユーザ状況情報を取得する（ステップS21）。次いで、簡略化部163は、パスワード入力画面出力処理で取得されたユーザ状況情報とログインセッション情報から取得したユーザ状況情報との差を算出する（ステップS22）。次いで、簡略化部163は、ユーザ状況情報の差に基づいて、ユーザの現在の状況と過去の状況とが一致するか否かを判定する（ステップS23）。このとき、簡略化部163は、状況が一致すると判定した場合には（ステップS23：YES）、ステップS24に進む。ステップS24において、簡略化部163は、簡略度を、状況が一致する場合の値に設定して、ステップS26に進む。一方、簡略化部163は、状況が一致しないと判定した場合には（ステップS23：NO）、ステップS25に進む。ステップS25において、簡略化部163は、簡略度を、状況が一致しない場合の値に設定して、ステップS26に進む。状況が一致しない場合の簡略度は、状況が一致する場合の簡略度よりも低い。ステップS26において、簡略化部163は、入力文字決定処理を実行して、簡略化処理を終了させる。

[0069] 入力文字決定処理は、登録パスワードのうちユーザに入力させる部分を決定する処理である。入力させる部分の決定方法によって、入力文字決定処理の内容が異なる。そこで、以下では、決定方法の例ごとに入力文字決定処理を説明する。図8Aは、第1の実施例に係る入力文字決定処理の一例を示すフローチャートである。第1の実施例において、簡略化部163は、ユーザの現在と過去の状況に応じて登録パスワードのうち入力させる文字の種類を異ならせる。図8Aに示すように、簡略化部163は、登録パスワードに含まれる文字の種類を特定する（ステップS31）。次いで、簡略化部163は、特定した文字種を、バリエーション数の多い順に順位を決定する（ステップS32）。次いで、簡略化部163は、文字種のバリエーション数の順

位と簡略度に基づいて、ユーザに入力させる文字種を決定する（ステップS 3 3）。例えば、簡略化部 1 6 3 は、簡略度が高いほど、順位が低い文字種を決定する。例えば、記憶部 1 2 に、登録パスワードに含まれる文字の種類の数と、簡略度と、ユーザが入力すべき文字の種類の数とを対応付けて格納するテーブルが記憶されていてもよい。そして、簡略化部 1 6 3 は、このテーブルを参照して、入力させる文字の種類を決定してもよい。次いで、簡略化部 1 6 3 は、登録パスワードの中から、決定した文字種の文字を、ユーザが入力すべき文字として例えば所定数決定する（ステップS 3 4）。次いで、簡略化部 1 6 3 は、決定した文字の位置を示す位置番号を、ログインセッション情報と関連付けて記憶部 1 2 に記憶させる（ステップS 3 5）。ステップS 3 5 を終わると、簡略化部 1 6 3 は入力文字決定処理を終了させる。

[0070] 図 8 B は、第 2 の実施例に係る入力文字決定処理の一例を示すフローチャートである。第 2 の実施例において、簡略化部 1 6 3 は、ユーザの現在と過去の状況に応じて登録パスワードのうち入力させる文字の種類数を異ならせる。図 8 B に示すように、簡略化部 1 6 3 は、登録パスワードに含まれる文字の種類を特定する（ステップS 4 1）。次いで、簡略化部 1 6 3 は、特定した文字種数を算出する（ステップS 4 2）。次いで、簡略化部 1 6 3 は、登録パスワードに含まれる文字の種類数と簡略度とに基づいて、ユーザに入力させる文字の種類数を決定する（ステップS 4 3）。例えば、簡略化部 1 6 3 は、1 から文字種数マイナス 1 までの範囲で、入力させる文字の種類数を決定してもよい。このとき、簡略化部 1 6 3 は、簡略度が高いほど、文字種数を少なくする。例えば、記憶部 1 2 に、登録パスワードに含まれる文字の種類数と、簡略度と、ユーザが入力すべき文字の種類数とを対応付けて格納するテーブルが記憶されていてもよい。そして、簡略化部 1 6 3 は、このテーブルを参照して、入力させる文字の種類数を決定してもよい。次いで、簡略化部 1 6 3 は、登録パスワードから特定された文字種の中から、決定された数分の文字種をユーザが入力すべき文字種として

決定する（ステップS 4 4）。このとき、簡略化部 1 6 3 は、例えばランダムに文字種を決定してもよいし、所定の条件に基づいて文字種を決定してもよい。次いで、簡略化部 1 6 3 は、登録パスワードの中から、決定した文字種の文字を、ユーザが入力すべき文字として例えば所定数決定する（ステップS 4 5）。このとき、簡略化部 1 6 3 は、決定した文字種ごとに、その文字種の文字を少なくとも 1 つ決定する。次いで、簡略化部 1 6 3 は、決定した文字の位置を示す位置番号を、ログインセッション情報と関連付けて記憶部 1 2 に記憶させる（ステップS 4 6）。ステップS 4 6 を終わると、簡略化部 1 6 3 は入力文字決定処理を終了させる。

[0071] 図 8 C は、第 3 の実施例に係る入力文字決定処理の一例を示すフローチャートである。第 3 の実施例において、簡略化部 1 6 3 は、ユーザの現在と過去の状況に応じて、登録パスワードのうち入力させる文字数を異ならせる。図 8 C に示すように、簡略化部 1 6 3 は、簡略度に基づいて、ユーザが入力すべき文字の数を決定する（ステップS 5 1）。このとき、簡略化部 1 6 3 は、簡略度が大きいほど、入力すべき文字の数を少なくする。例えば、記憶部 1 2 に、簡略度と、入力すべき文字の数とを対応付けて格納するテーブルが記憶されていてもよい。そして、簡略化部 1 6 3 は、このテーブルを参照して文字数を決定してもよい。また例えば、記憶部 1 2 に、登録パスワードの文字数と、簡略度と、登録パスワードのうち入力すべき文字の割合とを対応付けて格納するテーブルが記憶されていてもよい。そして、簡略化部 1 6 3 は、このテーブルを参照して文字数を決定してもよい。次いで、簡略化部 1 6 3 は、登録パスワードの中から、決定した文字数分の文字を、ユーザが入力すべき文字として決定する（ステップS 5 2）。このとき、簡略化部 1 6 3 は、例えばランダムに文字を決定してもよいし、所定の条件に基づいて文字を決定してもよい。次いで、簡略化部 1 6 3 は、決定した文字の位置を示す位置番号を、ログインセッション情報と関連付けて記憶部 1 2 に記憶させる（ステップS 5 3）。ステップS 5 3 を終わると、簡略化部 1 6 3 は入力文字決定処理を終了させる。

[0072] 図9は、本実施形態に係る認証装置1のシステム制御部16のパスワード入力画面生成処理の一例を示すフローチャートである。図9に示すように、パスワード入力画面出力部164は、登録パスワードの文字数を取得する（ステップS61）。また、パスワード入力画面出力部164は、記憶部12から、パスワード入力画面のウェブページのテンプレートとなるHTML文書を取得する。このHTML文書は、例えばユーザ端末2がパスワードの補完を行うためのスクリプトを含む。次いで、パスワード入力画面出力部164は、位置番号*i*を1に設定する（ステップS62）。次いで、パスワード入力画面出力部164は、登録パスワードの*i*番目の文字は、ユーザが入力すべき文字であるか否かを判定する（ステップS63）。例えば、ログインセッション情報に関連付けて記憶された位置番号の中に、*i*と一致する位置番号が存在する場合、パスワード入力画面出力部164は、*i*番目の文字は入力すべき文字であると判定する（ステップS63：YES）。この場合、パスワード入力画面出力部164は、例えば*i*番目の文字を入力するための文字入力欄を表示するためのデータをHTML文書に追加する（ステップS64）。次いで、パスワード入力画面出力部164は、ステップS67に進む。一方、パスワード入力画面出力部164は、*i*番目の文字は入力すべき文字ではないと判定した場合には（ステップS63：NO）、ステップS65に進む。ステップS65において、パスワード入力画面出力部164は、*i*番目の文字に対応する位置にアスタリスクを表示するためのデータをHTML文書に追加する。次いで、パスワード入力画面出力部164は、登録パスワードの*i*番目の文字を、位置番号*i*に関連付けてHTML文書に埋め込む（ステップS66）。HTML文書に埋め込まれた文字はパスワードの補完に用いられる。なお、安全性の観点から、パスワード入力画面出力部164は、文字を暗号化してHTML文書に埋め込んでもよい。次いで、パスワード入力画面出力部164は、ステップS67に進む。ステップS67において、パスワード入力画面出力部164は、位置番号*i*が登録パスワードの文字数の値未満であるか否かを判定する。このとき、パスワード入力画面出

力部 164 は、位置番号 i が登録パスワードの文字数の値未満であると判定した場合には（ステップ S67：YES）、ステップ S68 に進む。ステップ S68 において、パスワード入力画面出力部 164 は、位置番号 i に 1 を加算して、ステップ S63 に進む。一方、パスワード入力画面出力部 164 は、位置番号 i が登録パスワードの文字数の値未満ではないと判定した場合には（ステップ S67：NO）、パスワード入力画面生成処理を終了させる。

[0073] 図 10A は、本実施形態に係るユーザ端末 2 のパスワード送信処理の一例を示すフローチャートである。ユーザ端末 2 がパスワード入力画面を表示しているとき、ユーザが送信ボタン 140 を選択すると、ユーザ端末 2 はパスワード送信処理を実行する。図 10A に示すように、ユーザ端末 2 は、文字入力欄に入力された文字の位置番号と、HTML 文書に埋め込まれた文字の位置番号に従って、文字入力欄に入力された文字と HTML 文書に埋め込まれた文字を接続することにより、認証用のパスワードを生成する（ステップ S71）。具体的に、ユーザ端末 2 は、位置番号が小さい文字の順に、文字を接続する。次いで、ユーザ端末 2 は、生成したパスワードを認証装置 1 へ送信して（ステップ S72）、パスワード送信処理を終了させる。

[0074] 図 10B は、本実施形態に係る認証装置 1 のシステム制御部 16 の簡略化パスワード認証処理の一例を示すフローチャートである。パスワード入力画面においてパスワードが入力されることに基づいてユーザ端末 2 から送信されたパスワードを受信したとき、システム制御部 16 は簡略化パスワード認証処理を実行する。図 10B に示すように、認証部 165 は、ユーザ情報 DB3 から登録パスワードを取得する（ステップ S81）。具体的に、認証部 165 は、パスワードとともにユーザ端末 2 から送信されてきたセッション ID に対応するログインセッション情報を記憶部 12 から特定する。次いで、認証部 165 は、ログインセッション情報に含まれるユーザ ID に対応する登録パスワードを取得する。次いで、認証部 165 は、受信したパスワードが登録パスワードと一致するか否かを判定する（ステップ S82）。この

とき、認証部165は、パスワードが一致しないと判定した場合には（ステップS82：NO）、ステップS83に進む。ステップS83において、パスワード入力画面出力部164は、登録パスワード全部を入力させるパスワード入力画面のウェブページをユーザ端末2に出力して、簡略化パスワード認証処理を終了させる。

[0075] 一方、認証部165は、パスワードが一致すると判定した場合には（ステップS82：YES）、ステップS84に進む。ステップS84において、認証部165は、必要に応じてログインセッション情報を更新する。例えば、ログインセッション情報に含まれるユーザ状況情報を、現在のユーザの状況を示すユーザ状況情報（図6に示すステップS13で取得されている）で書き換えてもよい。この処理により、簡略化部163は、前回の認証成功時におけるユーザの状況と現在のユーザの状況とに応じて簡略化を行うことになる。一方、このような更新をしない場合、簡略化部163は、ログイン認証成功時におけるユーザの状況と現在のユーザの状況とに応じて簡略化を行うことになる。次いで、認証部165は、ユーザが要求した特定のサービス又は機能に関するウェブページをユーザ端末2に出力する（ステップS85）。ステップS85を終えると、認証部165は、簡略化パスワード認証処理を終了させる。

[0076] [1-6. 認証装置が端末装置に適用された場合]

次に、認証装置1が端末装置に適用された場合について図1Bを用いて説明する。図1Bは、認証装置1を端末装置に適用した場合の情報処理システムS2の概要構成の一例を示す図である。図2に示すように、情報処理システムS2は、端末装置として認証装置1を含む。この場合の認証装置1は例えばネットワークに接続可能であってもよい。また、2以上の認証装置1が存在してもよい。認証装置1は、例えば、スマートフォン、タブレット型コンピュータ、携帯電話機、パーソナルコンピュータ、PDA、STB等であってもよい。認証装置1はユーザにより利用される。

[0077] 記憶部12には、例えばユーザにより予め設定されたユーザID及びパス

ワードが記憶されている。このパスワードが登録パスワードである。例えば、ユーザが認証装置 1 を利用しようとするとき、ユーザはログイン操作を行う。このとき、例えばログイン画面においてユーザはユーザ ID 及びパスワードを入力する。認証装置 1 は、入力されたユーザ ID 及びパスワードと記憶部 12 に記憶されているユーザ ID 及びパスワードを比較して、ユーザ認証を行う。なお、認証装置 1 が端末装置である場合、ログイン時にユーザ ID の入力是不要なように認証装置 1 が構成されてもよい。ユーザ認証に成功したとき、認証装置 1 へのログインが成功する。ユーザが認証装置 1 にログインしている間は、認証装置 1 によってユーザが認証されている状態である。このときに、例えばユーザが認証装置 1 の特定の機能を利用しようとするとき、認証装置 1 は、ユーザ認証を再度行う。

[0078] 認証装置 1 が端末装置である場合の処理は、図 5 乃至図 10B のフローチャートで示した処理と基本的に同様である。ただし、現在ユーザ状況特定部 161 は、現在のユーザの状況として、例えば認証装置 1 の位置、認証装置 1 を利用するユーザの位置、又は時刻等を特定する。そのため、現在ユーザ状況特定部 161 は、ユーザ端末 2 の場合と同様の方法でユーザ状況情報を取得又は生成することができる。また、認証装置 1 には基本的には同時に一人のユーザのみがログイン可能であるため、ログインセッション情報の生成及び記憶をしなくてもよい。この場合、現在ユーザ状況特定部 161 は、取得したユーザ状況情報を記憶部 12 に記憶させればよい。また、ログイン画面、パスワード入力画面等の画面は表示部 14 に出力される。また、認証部 165 は、操作部 13 を用いてユーザにより入力されたパスワードを取得する。また、パスワードの補完は認証部 165 が行う。

[0079] 以上説明したように、本実施形態によれば、システム制御部 16 が、ユーザが置かれている現在の状況を特定する。また、システム制御部 16 が、過去の認証時にユーザが置かれていた状況を取得する。また、システム制御部 16 がユーザが現在認証されている状態である場合、現在の状況及び過去の状況に応じて、ユーザが入力すべきパスワードを簡略化する。そして、シス

テム制御部 16 が、簡略化されたパスワードの入力を促すパスワード入力画面のウェブページを出力する。従って、安全性を確保しつつ、ユーザが入力すべきパスワードを簡略化することができる。

[0080] また、システム制御部 16 が、現在の状況と過去の状況とに応じて、ユーザが本来入力すべきパスワードのうち簡略化によってユーザに入力させる部分を異ならせてもよい。これにより、ユーザに入力させる部分を異ならせることで、簡略化の度合いを変えることができる。例えば、システム制御部 16 は、ユーザに入力させる文字の種類を異ならせてもよい。また、システム制御部 16 は、ユーザに入力させる文字の種類数を異ならせてもよい。また、システム制御部 16 は、ユーザが入力すべき文字の数を異ならせてもよい。

[0081] また、システム制御部 16 が、ユーザ情報 DB 3 に記憶された登録パスワードから、簡略化されたパスワードに含まれない部分を取得して、パスワード入力画面の HTML 文書に埋め込む。また、システム制御部 16 が、HTML 文書に埋め込まれた部分でパスワード入力画面で入力されたパスワードを補完することにより生成された認証用パスワードをユーザ端末 2 から取得する。そして、システム制御部 16 が、認証用パスワードと登録パスワードとを比較してユーザの認証の成否を判定する。従って、認証用パスワードと登録パスワードとが一致するか否かに基づいて認証の成否を判定することができる。

[0082] また、システム制御部 16 が、パスワード入力画面において入力されたパスワードを用いた認証が失敗した場合、登録パスワード全部の入力を促すパスワード入力画面のウェブページを出力してもよい。この場合、簡略化されたパスワードを用いた認証の失敗により、パスワードを入力した者が認証されているユーザであることが疑わしい場合であっても、安全性を確保することができる。

[0083] また、システム制御部 16 が、登録パスワードのうち簡略化されたパスワードに含まれない部分についてアスタリスク等の記号を表示させてもよい。

この場合、ユーザは記号を見ることにより、登録パスワードのうちユーザが入力する必要がない部分を認識することができる。

[0084] [2. 第2実施形態]

次に、第2実施形態について図11乃至図13を用いて説明する。認証装置1は、ログイン中に特定のサービス又は機能をユーザが利用するごとに、簡略化されたパスワードを用いてユーザ認証を行う。第1実施形態においては、ユーザの現在と過去の状況が一致するとき、そのような状況が連続しても、簡略度は同一であった。本実施形態において、認証装置1は、状況が一致することに応じて簡略化されたパスワードを用いる認証が連続する場合、前回の簡略化の度合いよりも小さい度合いで簡略化されたパスワードを生成することにより、パスワードを簡略化する。ユーザの現在の状況が過去の状況が一致する場合であっても、簡略化されたパスワードでの認証を重ねて行くにつれて、安全性が低下していく可能性がある。すなわち、パスワードを入力する者が、認証されているユーザ本人ではない可能性が高くなる。そこで、状況に一致することにより簡略化されたパスワードを用いる認証が連続するときは、前回よりも簡略度を小さくすることにより、安全性を確保することができる。本実施形態においても、認証装置1は、例えばサーバ装置であってもよいし、端末装置であってもよい。以下に説明する点を除き、第2実施形態は第1実施形態と基本的に同様である。

[0085] 図11は、簡略度の決定方法の一例を示す図である。図11に示すように、現在と過去の状況が初めて一致する場合、例えば、簡略度が最大の値に設定されてもよい。図11の例では、簡略度は6である。そして、状況が連続して一致する回数が2、3と増えて行くにつれて、簡略度が小さくなっている。例えば、簡略度は1ずつ小さくなっていてもよい。図11の例では、状況が連続して一致する回数が5以上である場合、例えば簡略度が2に設定される。状況が連続して一致する回数を一致回数と称する。現在の状況と過去の状況が異なる場合の簡略度は、例えば状況が一致する場合の最小の簡略度よりも小さくてもよい。図11の例では、状況が異なる場合の簡略度は1

である。また例えば、現在の状況と過去の状況が異なる場合の簡略度は、状況が一致する場合の最小の簡略度と一致してもよい。記憶部12には、例えば一致回数／簡略度変換テーブルが記憶される。一致回数／簡略度変換テーブルは、状況が連続して一致する回数と簡略度とを対応付けて格納するテーブルである。簡略化部163は、このテーブルを参照して簡略度を決定してもよい。

[0086] 図12は、本実施形態に係る認証装置1のシステム制御部16のログイン認証処理の一例を示すフローチャートである。図12において図5と同様の処理については同様の符号が付されている。図12に示すように、認証部165は、ステップS1の判定に基づいてステップS2又はS3を実行する。ステップS3の後、簡略化部163は一致回数を0に設定する（ステップS91）。次いで、認証部165は、ユーザ状況情報及び一致回数を含むログインセッション情報を生成して記憶部12に記憶させる（ステップS92）。そして、認証部165は、ステップS5を実行する。

[0087] 図13は、本実施形態に係る認証装置1のシステム制御部16の簡略化処理の一例を示すフローチャートである。図13において図7と同様の処理については同様の符号が付されている。図13に示すように、システム制御部16は、ステップS21～S23を実行する。ステップS23において、簡略化部163は、ユーザの現在の状況と過去の状況とが一致すると判定した場合には（ステップS23：YES）、ステップS101に進む。ステップS101において、簡略化部163は、ログイン情報に含まれる一致回数に1を加算する。次いで、簡略化部163は、一致回数に対応する簡略度を一致回数／簡略度変換テーブルから取得する（ステップS102）。そして、簡略化部163は、入力文字決定処理を実行する（ステップS26）。一方、簡略化部163は、ユーザの現在の状況と過去の状況とが一致しないと判定した場合には（ステップS23：NO）、ステップS103に進む。ステップS103において、簡略化部163は、ログイン情報に含まれる一致回数を0に設定する。そして、簡略化部163は、ステップS25及びS26

を実行する。

[0088] 以上説明したように、本実施形態によれば、システム制御部 16 が、状況が一致することに応じて簡略化されたパスワードを用いる認証が連続する場合、前回の簡略化の度合いよりも小さい度合いで簡略化されたパスワードを生成する。従って、安全性を確保しつつ、ユーザが入力すべきパスワードを簡略化することができる。

[0089] [3. 第3実施形態]

次に、第3実施形態について図14及び図15を用いて説明する。第1実施形態においては、ユーザの現在と過去の状況とが異なるとき、如何なる場合であっても簡略度は同一であった。本実施形態において、認証装置1は、ユーザの現在と過去の状況の差が大きいほど簡略度を小さくする。現在と過去の状況の差が大きいほど、安全性が低くなると考えられる。すなわち、パスワードを入力する者が、認証されているユーザ本人ではない可能性が高くなる。そこで、現在と過去の状況の差が大きいほど簡略度を小さくすることにより、安全性を確保することができる。本実施形態においても、認証装置1は、例えばサーバ装置であってもよいし、端末装置であってもよい。以下に説明する点を除き、第2実施形態は第1実施形態又は第2実施形態と基本的に同様である。

[0090] 図14は、簡略度の決定方法の一例を示す図である。図14に示すように、状況の差に応じて簡略度が決定される。図14では、状況の差がレベル0である場合、すなわち現在の状況と過去の状況とが一致する場合、簡略度は6である。状況の差がレベル1以上である場合、現在と過去の状況が異なることを示す。状況の差が1である場合、簡略度は5である。そして、状況の差が大きくなるに従って簡略度が小さくなっている。そして、状況の差がレベル5以上である場合、簡略度は1である。なお、状況が異なる場合の最低の簡略度は0であってもよい。簡略度の0は、パスワードを簡略化しないことを示す。すなわち、ユーザは登録パスワードを全部入力する必要がある。説明の便宜上、図14の例では状況の差をレベルで表し、レベルごとに簡略

度が示されている。実際には距離の範囲や時間の範囲等ごとに簡略度が決定される。例えば、現在の位置と過去の位置との間の距離が5 m未満である場合、簡略度は6に設定され、距離が5 m以上20 m未満である場合、簡略度は5に設定され、距離が20 m以上50 m未満である場合、簡略度は4に設定されてもよい。記憶部12には、例えば状況差／簡略度変換テーブルが記憶される。状況差／簡略度変換テーブルは、状況の差と簡略度とを対応付けて格納するテーブルである。簡略化部163は、このテーブルを参照して簡略度を決定してもよい。

[0091] なお、簡略化部163は、現在と過去の状況が異なる場合には状況の差が大きいほど簡略度を小さくする一方で、現在と過去の状況が一致する場合には、第2実施形態の場合のように、連続して状況が一致するごとに、前回の簡略度よりも小さい簡略度を決定してもよい。この場合、例えば、状況が一致する場合の最大の簡略度が、状況が異なる場合の最大の簡略度よりも大きくなればよい。

[0092] 図15は、本実施形態に係る認証装置1のシステム制御部16の簡略化処理の一例を示すフローチャートである。図15において図7と同様の処理については同様の符号が付されている。図15に示すように、システム制御部16は、ステップS21～S23を実行する。ステップS23において、簡略化部163は、ユーザの現在の状況と過去の状況とが一致すると判定した場合には（ステップS23：YES）、ステップS24及びS26を実行する。一方、簡略化部163は、ユーザの現在の状況と過去の状況とが一致しないと判定した場合には（ステップS23：NO）、ステップS111に進む。ステップS111において、簡略化部163は、ステップS22で算出したユーザ状況情報の差に対応する簡略度を状況差／簡略度変換テーブルから取得する。そして、簡略化部163は、入力文字決定処理を実行する（ステップS26）。

[0093] 以上説明したように、本実施形態によれば、システム制御部16が、現在の状況と過去の状況とが異なる場合、状況の差が大きいほど小さい度合いで

簡略化されたパスワードを生成する。従って、安全性を確保しつつ、ユーザが入力すべきパスワードを簡略化することができる。

[0094] [4. 第4実施形態]

次に、第4実施形態について図16A乃至図18を用いて説明する。本実施形態において、認証装置1は、ユーザの現在と過去の状況が異なることに応じて簡略化されたパスワードを用いる認証が連続するごとに、前回の簡略度と同じ簡略度を決定することが可能な状況の差を、前回よりも小さくする。ユーザの現在の状況が過去の状況に異なる場合においても、簡略化されたパスワードでの認証を重ねて行くにつれて、安全性が低下していく可能性がある。そこで、認証装置1が過去の簡略度と同じ簡略度でパスワードを簡略化することが可能な状況の差を小さくすることで、安全性を確保することができる。例えば、認証時に、現在の状況と過去の状況とが初めて異なるとき、例えば過去と現在の時間差が1時間未満である場合には簡略度が5に決定されてもよい。現在の状況と過去の状況とが2回連続して異なるとき、例えば過去と現在の時間差が30分未満である場合には簡略度が5に決定され、時間差が30分以上1時間未満である場合には簡略度が4に決定されてもよい。本実施形態においても、認証装置1は、例えばサーバ装置であってもよいし、端末装置であってもよい。以下に説明する点を除き、第5実施形態は第4実施形態と基本的に同様である。

[0095] 図16A乃至図16Cは、簡略度の決定方法の一例を示す図である。図16Aは、現在と過去の状況が初めて異なる場合の簡略度の決定方法の決定例を示す。状況が初めて異なる場合、例えば図16Aに示すように、状況の差がレベル1以上4以下である場合、簡略度は5に設定され、状況の差がレベル5以上8以下である場合、簡略度が4に設定されている。その後も同様に、状況の差が4大きくなるごとに簡略度が小さくなっていく。図16Bは、現在と過去の状況が連続して2回異なる場合の簡略度の決定方法の決定例を示す。状況が2回連続して異なる場合、例えば図16Bに示すように、状況の差がレベル1以上2以下である場合、簡略度は5に設定され、状況の差が

レベル 3 以上 4 以下である場合、簡略度が 4 に設定されている。その後も同様に、状況の差が 2 大きくなるごとに簡略度が小さくなっていく。図 16C は、現在と過去の状況が連続して 3 回異なる場合の簡略度の決定方法の決定例を示す。状況が 3 回連続して異なる場合、例えば図 16C に示すように、状況の差がレベル 1 である場合、簡略度は 5 に設定され、状況の差がレベル 2 である場合、簡略度が 4 に設定されている。その後も同様に、状況の差が 1 大きくなるごとに簡略度が小さくなっていく。状況が連続して異なる回数を不一致回数と称する。記憶部 12 には、例えば状況差／簡略度変換テーブルが複数記憶される。各状況差／簡略度変換テーブルは、不一致回数と関連付けて記憶される。簡略化部 163 は、不一致回数に基づいて状況差／簡略度変換テーブルを決定し、決定したテーブルを参照して簡略度を決定してもよい。

[0096] 図 17 は、本実施形態に係る認証装置 1 のシステム制御部 16 のログイン認証処理の一例を示すフローチャートである。図 17 において図 5 と同様の処理については同様の符号が付されている。図 17 に示すように、認証部 165 は、ステップ S1 の判定に基づいてステップ S2 又は S3 を実行する。ステップ S3 の後、簡略化部 163 は、不一致回数を 0 に設定する（ステップ S121）。次いで、認証部 165 は、ユーザ状況情報及び不一致回数を含むログインセッション情報を生成して記憶部 12 に記憶させる（ステップ S122）。そして、認証部 165 は、ステップ S5 を実行する。

[0097] 図 18 は、本実施形態に係る認証装置 1 のシステム制御部 16 の簡略化処理の一例を示すフローチャートである。図 18 において図 7 と同様の処理については同様の符号が付されている。図 18 に示すように、システム制御部 16 は、ステップ S21～S23 を実行する。ステップ S23 において、簡略化部 163 は、ユーザの現在の状況と過去の状況とが一致すると判定した場合には（ステップ S23：YES）、ステップ S131 に進む。ステップ S131 において、簡略化部 163 は、ログイン情報に含まれる不一致回数を 0 に設定する。そして、簡略化部 163 は、ステップ S24 及び S26 を

実行する。一方、簡略化部 163 は、ユーザの現在の状況と過去の状況とが一致しないと判定した場合には（ステップ S 23 : NO）、ステップ S 132 に進む。ステップ S 132 において、簡略化部 163 は、ログイン情報に含まれる不一致回数に 1 を加算する。次いで、簡略化部 163 は、不一致回数に対応する状況差／簡略度変換テーブルを記憶部 12 から特定する（ステップ S 133）。次いで、簡略化部 163 は、簡略化部 163 は、ステップ S 22 で算出したユーザ状況情報の差に対応する簡略度を、ステップ S 133 で特定した状況差／簡略度変換テーブルから取得する（ステップ S 134）。そして、簡略化部 163 は、入力文字決定処理を実行する（ステップ S 26）。

[0098] 以上説明したように、本実施形態によれば、システム制御部 16 が、状況が異なることに応じて簡略化されたパスワードを用いる認証が連続するごとに、前回の簡略化の度合いと同じ度合いでパスワードを簡略化することが可能な状況の差を小さくする。従って、安全性を確保しつつ、ユーザが入力すべきパスワードを簡略化することができる。

[0099] [5. 第 5 実施形態]

次に、第 5 実施形態について図 19 を用いて説明する。本実施形態において、認証装置 1 は、ユーザの現在の状況が、安全性に関連する所定の条件に合致しない場合、パスワードを簡略化しない。過去の状況とは関係なく、ユーザが現在置かれている状況の安全性が低い場合がある。そのような場合に、認証装置 1 は、登録パスワードの全部をユーザに入力させることによって安全性を確保することができる。本実施形態においても、認証装置 1 は、例えばサーバ装置であってもよいし、端末装置であってもよい。以下に説明する点を除き、第 5 実施形態は、第 1 実施形態～第 4 実施形態と基本的に同様である。

[0100] 安全性に関連する条件に合致しない状況として、例えばユーザ端末 2 が、会員登録が不要、又は接続料金が無料の公衆無線 LAN にアクセスしている場合や、公衆無線 LAN を利用するときに認証が不要な公衆無線 LAN にユ

ーザ端末2がアクセスしている場合がある。このような場合、認証装置1で認証されたユーザ本人以外の者が認証装置1を利用する蓋然性が高くなる。例えばこのような場合に、簡略化部163は、パスワードを簡略化しなくてもよい。

[0101] 図19は、本実施形態に係る認証装置1のシステム制御部16のパスワード入力画面出力処理の一例を示すフローチャートである。図19において図6と同様の処理については同様の符号が付されている。図19に示すように、認証部165は、ステップS11の判定に基づいてステップS12又はS13を実行する。ステップS13において、現在ユーザ状況特定部161は、ユーザの現在の状況を示すユーザ状況情報として、ユーザ端末2からの要求からユーザ端末2に割り当てられたIPアドレスを少なくとも取得する。次いで、簡略化部163は、取得したIPアドレスに基づいて、ユーザ端末2が、安全性に関連する所定の条件を満たさない公衆無線LANからアクセスしているか否かを判定する（ステップS141）。例えば、記憶部12に、安全性に関連する条件を満たさない公衆無線LANのIPアドレスのリストが記憶されていてもよい。そして、簡略化部163は、取得したIPアドレスがリストに含まれている場合に、ユーザ端末2が、安全性に関連する条件を満たさない公衆無線LANからアクセスしていると判定してもよい（ステップS141：YES）。この場合、パスワード入力画面出力部164は、登録パスワード全部を入力させるパスワード入力画面のウェブページをユーザ端末2に出力して（ステップS142）、簡略化パスワード認証処理を終了させる。一方、簡略化部163は、安全性に関連する条件を満たさない公衆無線LANからアクセスしていないと判定した場合には（ステップS141：NO）、ステップS14に進む。そして、システム制御部16は、ステップS14～S17を実行する。

[0102] 以上説明したように、本実施形態によれば、システム制御部16が、現在の状況が、安全性に関連する所定条件に合致しない場合、パスワードを簡略化しない。従って、安全性を確保することができる。

[0103] [6. 第 6 実施形態]

次に、第 6 実施形態について図 20 及び図 21 を用いて説明する。第 1 実施形態においては、ユーザ端末 2 がパスワードの補完を行っていた。本実施形態においては、ユーザ端末 2 は、パスワード入力画面においてユーザにより入力された文字のみを認証装置 1 へ送信する。そして、認証装置 1 がパスワードの補完を行う。以下に説明する点を除き、第 6 実施形態は、第 1 実施形態～第 5 実施形態と基本的に同様である。

[0104] 図 20 は、本実施形態に係るユーザ端末 2 のパスワード送信処理の一例を示すフローチャートである。ユーザ端末 2 がパスワード入力画面を表示しているとき、ユーザが送信ボタン 140 を選択すると、ユーザ端末 2 はパスワード送信処理を実行する。図 20 に示すように、ユーザ端末 2 は、文字入力欄ごとに、文字入力欄に入力された文字とその文字入力欄に対応する位置番号との組み合わせを取得する。文字入力欄に文字が入力されていない場合、ユーザ端末 2 はその文字入力欄の位置番号と例えば空白文字とを組み合わせる。そして、ユーザ端末 2 は、取得した組み合わせを接続して、入力パスワードを生成する（ステップ S 151）。次いで、ユーザ端末 2 は、生成した入力パスワードを認証装置 1 へ送信して（ステップ S 152）、パスワード送信処理を終了させる。

[0105] 図 21 は、本実施形態に係る認証装置 1 のシステム制御部 16 の簡略化パスワード認証処理の一例を示すフローチャートである。図 21 において図 10B と同様の処理については同様の符号が付されている。図 21 に示すように、認証部 165 は、ユーザ情報 DB 3 から登録パスワードを取得する（ステップ S 81）。次いで認証部 165 は、認証用パスワードを初期化する（ステップ S 161）。次いで、認証部 165 は、位置番号 i を 1 に設定する（ステップ S 162）。次いで、認証部 165 は、ユーザ端末 2 から受信した入力パスワードが位置番号 i を含むか否かを判定する（ステップ S 163）。このとき、認証部 165 は、入力パスワードが位置番号 i を含むと判定した場合には（ステップ S 163：YES）、ステップ S 164 に進む。ス

ステップS 1 6 4において、認証部1 6 5は、入力パスワードから、位置番号 i に関連付けられた文字を取得する。そして、認証部1 6 5は、取得した文字を認証用パスワードに追加して、ステップS 1 6 6に進む。一方、認証部1 6 5は、入力パスワードが位置番号 i を含まないと判定した場合には（ステップS 1 6 3 : NO）、ステップS 1 6 5に進む。ステップS 1 6 5において、認証部1 6 5は、登録パスワードから、 i 番目の文字を取得する。そして、認証部1 6 5は、取得した文字を認証用パスワードに追加して、ステップS 1 6 6に進む。ステップS 1 6 6において、認証部1 6 5は、位置番号 i が登録パスワードの文字数の値未満であるか否かを判定する。このとき、認証部1 6 5は、位置番号 i が登録パスワードの文字数の値未満であると判定した場合には（ステップS 1 6 6 : YES）、ステップS 1 6 7に進む。ステップS 1 6 7において、認証部1 6 5は、位置番号 i に1を加算して、ステップS 1 6 3に進む。一方、認証部1 6 5は、位置番号 i が登録パスワードの文字数の値未満ではないと判定した場合には（ステップS 1 6 6 : NO）、ステップS 1 6 8に進む。

[0106] ステップS 1 6 8において、認証部1 6 5は、入力パスワードが位置番号 $i + 1$ 以上の位置番号を含むか否かを判定する。このとき、認証部1 6 5は、入力パスワードが位置番号 $i + 1$ 以上の位置番号を含むと判定した場合には（ステップS 1 6 8 : YES）、ステップS 8 3に進む。ステップS 8 3において、パスワード入力画面出力部1 6 4は、登録パスワード全部を入力させるパスワード入力画面のウェブページをユーザ端末2に出力して、簡略化パスワード認証処理を終了させる。一方、認証部1 6 5は、入力パスワードが位置番号 $i + 1$ 以上の位置番号を含まないと判定した場合には（ステップS 1 6 8 : NO）、ステップS 1 6 9に進む。ステップS 1 6 9において、認証部1 6 5は、認証用パスワードが登録パスワードと一致するか否かを判定する。このとき、認証部1 6 5は、認証用パスワードが登録パスワードと一致しないと判定した場合には（ステップS 1 6 9 : NO）、ステップS 8 3に進む。一方、認証部1 6 5は、認証用パスワードが登録パスワードと

一致すると判定した場合には（ステップS 1 6 9：Y E S）、ステップS 8 4 及びS 8 5を実行する。これにより、認証部1 6 5は、ユーザが要求した特定のサービス又は機能に関するウェブページをユーザ端末2に出力する。

[0107] 以上説明したように、本実施形態によれば、システム制御部1 6が、ユーザ情報D B 3に記憶された登録パスワードから、簡略化されたパスワードに含まれない部分を取得する。また、システム制御部1 6が、取得した部分で入力されたパスワードを補完することにより認証用パスワードを生成、取得する。そして、システム制御部1 6が認証用パスワードと登録パスワードとを比較してユーザの認証の成否を判定する。従って、認証用パスワードと登録パスワードとが一致するか否かに基づいて認証の成否を判定することができる。

[0108] [7. 第7実施形態]

次に、第7実施形態について図2 2を用いて説明する。本実施形態においては、認証装置1及びユーザ端末2の何れもパスワードの補完を行わない。認証装置1は、簡略化されたパスワードに含まれる文字の登録パスワード内における位置を特定する。そして、認証装置1は、ユーザにより入力されたパスワードに含まれる文字と、登録パスワードのうち特定された位置の文字とを比較することにより、ユーザ認証の成否を判定する。本実施形態においても、認証装置1は、例えばサーバ装置であってもよいし、端末装置であってもよい。以下に説明する点を除き、第7実施形態は、第1実施形態～第5実施形態と基本的に同様である。

[0109] パスワード入力画面においてユーザにより入力されたパスワードをユーザ端末2が認証装置1へ送信する処理は、例えば図2 0に示すパスワード送信処理と同様であってもよい。認証装置1は、入力パスワードに含まれる位置番号から、簡略化されたパスワードに含まれる文字の位置を特定することができる。

[0110] 図2 2は、本実施形態に係る認証装置1のシステム制御部1 6の簡略化パスワード認証処理の一例を示すフローチャートである。図2 2において図1

0 Bと同様の処理については同様の符号が付されている。図22に示すように、認証部165は、ユーザ情報DB3から登録パスワードを取得する（ステップS81）。次いで認証部165は、位置番号iを1に設定する（ステップS171）。次いで、認証部165は、ユーザ端末2から受信した入力パスワードが位置番号iを含むか否かを判定する（ステップS172）。このとき、認証部165は、入力パスワードが位置番号iを含まないと判定した場合には（ステップS172：NO）、ステップS175に進む。一方、認証部165は、入力パスワードが位置番号iを含むと判定した場合には（ステップS172：YES）、ステップS173に進む。ステップS173において、認証部165は、入力パスワードから、位置番号iに関連付けられた文字を取得する。次いで、認証装置1は、取得した文字が、登録パスワードのi番目の文字と一致するか否かを判定する（ステップS174）。このとき、認証装置1は、取得した文字が、登録パスワードのi番目の文字と一致しないと判定した場合には（ステップS174：NO）、ステップS83に進む。ステップS83において、パスワード入力画面出力部164は、登録パスワード全部を入力させるパスワード入力画面のウェブページをユーザ端末2に出力して、簡略化パスワード認証処理を終了させる。一方、認証装置1は、取得した文字が登録パスワードのi番目の文字と一致すると判定した場合には（ステップS174：YES）、ステップS175に進む。

[0111] ステップS175において、認証部165は、位置番号iが登録パスワードの文字数の値未満であるか否かを判定する。このとき、認証部165は、位置番号iが登録パスワードの文字数の値未満であると判定した場合には（ステップS175：YES）、ステップS176に進む。ステップS176において、認証部165は、位置番号iに1を加算して、ステップS172に進む。一方、認証部165は、位置番号iが登録パスワードの文字数の値未満ではないと判定した場合には（ステップS175：NO）、ステップS177に進む。ステップS177において、認証部165は、入力パスワードが位置番号i+1以上の位置番号を含むか否かを判定する。このとき、認

証部 165 は、入力パスワードが位置番号 $i + 1$ 以上の位置番号を含むと判定した場合には（ステップ S 177 : YES）、ステップ S 83 に進む。一方、認証部 165 は、入力パスワードが位置番号 $i + 1$ 以上の位置番号を含まないと判定した場合には（ステップ S 177 : NO）、ステップ S 84 及び S 85 を実行する。これにより、認証部 165 は、ユーザが要求した特定のサービス又は機能に関するウェブページをユーザ端末 2 に出力する。

[0112] 以上説明したように、本実施形態によれば、システム制御部 16 が、ユーザ情報 DB 3 に記憶された登録パスワードのうち簡略化されたパスワードの位置を特定する。また、システム制御部 16 が、入力されたパスワードと登録パスワードのうち特定された位置にある部分とを比較してユーザの認証の成否を判定する。従って、ユーザにより入力されたパスワードに情報を補完しなくても、認証の成否を判定することができる。

[0113] [8. 第 8 実施形態]

次に、第 8 実施形態について図 23 乃至図 27 を用いて説明する。本実施形態において、認証装置 1 は、ログイン中においてユーザが特定のサービス又は機能を利用しようとするとき、ユーザにユーザ ID 及びパスワードを入力させる。そして、認証装置 1 は、入力されたユーザ ID 及びパスワードと、登録されているユーザ ID 及びパスワードとを比較することにより、ユーザ認証を行う。このとき、認証装置 1 は、ユーザが入力すべきユーザ ID を簡略化する。ユーザ ID は本発明における認証情報の一例である。認証装置 1 は、ユーザ ID 及びパスワードの両方を簡略化してもよいし、ユーザ ID のみを簡略化してもよい。例えば、ユーザ ID にユーザのメールアドレスが利用される場合、認証装置 1 は、ユーザが入力すべきユーザ ID を、メールアドレス内のアットマークより前にあるアカウント名に簡略化してもよい。また例えば、認証装置 1 は、これまでの実施形態で述べたような方法でユーザ ID を簡略化してもよい。本実施形態においても、認証装置 1 は、例えばサーバ装置であってもよいし、端末装置であってもよい。以下に説明する点を除き、第 7 実施形態は、第 1 実施形態～第 7 実施形態と基本的に同様であ

る。

[0114] 図23は、パスワード入力画面の表示例を示す図である。パスワード入力画面には、メッセージ190、ユーザID入力領域200、パスワード入力領域130、送信ボタン140が表示される。メッセージ110は、簡略化されたユーザID及びパスワードの入力を促すメッセージである。ユーザID入力領域200には、非入力文字201が表示される。非入力文字201は、ユーザIDのうちユーザが入力する必要がない文字である。なお、非入力文字201に代えて、アスタリスク等の記号が表示されてもよい。また、ユーザID入力領域200には1つ以上の文字入力欄202が表示される。各文字入力欄202は、簡略化されたユーザIDの1つの文字を入力するための入力フィールドである。図23の例では、ユーザIDの先頭3文字を入力するための文字入力欄202が表示される。

[0115] 図24は、本実施形態に係る認証装置1のシステム制御部16の簡略化処理の一例を示すフローチャートである。図24において図7と同様の処理については同様の符号が付されている。図24に示すように、簡略化部163は、ステップS21～23を実行した後、ステップS24又はS25を実行する。次いで、簡略化部163は、ユーザIDのうちユーザに入力させる部分を決定するための入力文字決定処理を実行する（ステップS181）。この場合の入力文字決定処理は、例えば、図8A～図8Cに示す処理と同様であってもよい。次いで、簡略化部163は、登録パスワードのうちユーザに入力させる部分を決定するための入力文字決定処理を実行する（ステップS182）。ステップS182を終えると、簡略化部163は、簡略化処理を終了させる。

[0116] 図25は、本実施形態に係る認証装置1のシステム制御部16のパスワード入力画面生成処理の一例を示すフローチャートである。図25において図9と同様の処理については同様の符号が付されている。図25に示すように、パスワード入力画面出力部164は、ログインセッション情報に含まれるユーザIDの文字数を取得する（ステップS191）。また、パスワード入

力画面出力部 164 は、記憶部 12 から、パスワード入力画面のウェブページのテンプレートとなる HTML 文書を取得する。この HTML 文書は、例えばユーザ端末 2 がユーザ ID 及びパスワードの補完を行うためのスクリプトを含む。次いで、パスワード入力画面出力部 164 は、位置番号 i を 1 に設定する（ステップ S 192）。次いで、パスワード入力画面出力部 164 は、ユーザ ID の i 番目の文字は、ユーザが入力すべき文字であるか否かを判定する（ステップ S 193）。このとき、パスワード入力画面出力部 164 は、 i 番目の文字は入力すべき文字であると判定した場合には、（ステップ S 193：YES）、ステップ S 194 に進む。ステップ S 194 において、パスワード入力画面出力部 164 は、例えばユーザ ID の i 番目の文字を入力するための文字入力欄を表示するためのデータを HTML 文書に追加する。次いで、パスワード入力画面出力部 164 は、ステップ S 196 に進む。一方、パスワード入力画面出力部 164 は、 i 番目の文字は入力すべき文字ではないと判定した場合には（ステップ S 193：NO）、ステップ S 195 に進む。ステップ S 195 において、パスワード入力画面出力部 164 は、 i 番目の文字を表示するため、 i 番目の文字を位置番号 i に関連付けて HTML 文書に追加する（ステップ S 196）。次いで、パスワード入力画面出力部 164 は、ステップ S 196 に進む。ステップ S 196 において、パスワード入力画面出力部 164 は、位置番号 i がユーザ ID の文字数の値未満であるか否かを判定する。このとき、パスワード入力画面出力部 164 は、位置番号 i がユーザ ID の文字数の値未満であると判定した場合には（ステップ S 196：YES）、ステップ S 197 に進む。ステップ S 197 において、パスワード入力画面出力部 164 は、位置番号 i に 1 を加算して、ステップ S 193 に進む。一方、パスワード入力画面出力部 164 は、位置番号 i がユーザ ID の文字数の値未満ではないと判定した場合には（ステップ S 196：NO）、例えば第 1 実施形態と同様に、ステップ S 61～S 68 を実行する。

[0117] 図 26 は、本実施形態に係るユーザ端末 2 のパスワード送信処理の一例を

示すフローチャートである。図 26 において図 10A と同様の処理については同様の符号が付されている。図 26 に示すように、ユーザ端末 2 は、ユーザ ID 入力領域の文字入力欄に入力された文字の位置番号と、HTML 文書に追加された文字の位置番号に従って、文字入力欄に入力された文字と HTML 文書に追加された文字を接続することにより、認証用のユーザ ID を生成する（ステップ S201）。次いで、ユーザ端末 2 は、認証用のパスワードを生成する（ステップ S202）。次いで、ユーザ端末 2 は、生成したユーザ ID 及びパスワードを認証装置 1 へ送信して（ステップ S203）、パスワード送信処理を終了させる。

[0118] 図 27 は、本実施形態に係る認証装置 1 のシステム制御部 16 の簡略化パスワード認証処理の一例を示すフローチャートである。図 27 において図 10B と同様の処理については同様の符号が付されている。図 27 に示すように、認証部 165 は、ユーザ ID、パスワードとともにユーザ端末 2 から送信されてきたセッション ID に対応するログインセッション情報からユーザ ID を取得する（ステップ S211）。次いで、認証部 165 は、受信したユーザ ID が取得したユーザ ID と一致するか否かを判定する（ステップ S212）。このとき、認証部 165 は、ユーザ ID が一致しないと判定した場合には（ステップ S212：NO）、ステップ S213 に進む。ステップ S213 において、パスワード入力画面出力部 164 は、ユーザ ID 及び登録パスワードをそれぞれ全部を入力させるパスワード入力画面のウェブページをユーザ端末 2 に出力して、簡略化パスワード認証処理を終了させる。一方、認証部 165 は、ユーザ ID が一致すると判定した場合には（ステップ S212：YES）、ステップ S81 に進む。

[0119] ステップ S81 において、認証部 165 は、ユーザ情報 DB 3 から登録パスワードを取得する。次いで、認証部 165 は、受信したパスワードが登録パスワードと一致するか否かを判定する（ステップ S82）。このとき、認証部 165 は、パスワードが一致しないと判定した場合には（ステップ S82：NO）、ステップ S213 に進む。一方、認証部 165 は、パスワード

が一致すると判定した場合には（ステップS 8 2：Y E S）、ステップS 8 4に進む。ステップS 8 4において、認証部1 6 5は、必要に応じてログインセッション情報を更新する。次いで、認証部1 6 5は、ユーザが要求した特定のサービス又は機能に関するウェブページをユーザ端末2に出力する（ステップS 8 5）。ステップS 8 5を終えると、認証部1 6 5は、簡略化パスワード認証処理を終了させる。

[0120] 以上説明したように、本実施形態によれば、システム制御部1 6が、ユーザが入力すべきユーザIDを簡略化し、簡略化されたユーザIDの入力を促すパスワード入力画面のウェブページを出力する。従って、安全性を確保しつつ、ユーザが入力すべきパスワードを簡略化することができる。

[0121] なお、上記各実施形態においては、認証情報がパスワード又はユーザIDに適用されていた。しかしながら、認証情報がこれらの情報とは異なる情報に適用されてもよい。例えば、認証情報が複数の生体情報を含んでもよい。生体情報の例として、網膜の模様、指紋、声紋等が挙げられる。例えば、本発明に係る情報処理装置は、例えばユーザが入力すべき生体情報の数を減らしたり、ユーザが入力すべき生体情報の種類を減らしたりすること等により、認証情報を簡略化してもよい。また、認証情報は、画像、アイコン、シンボル、又は符号等を示すコードを含んでもよい。

符号の説明

- [0122] 1 認証装置
- 2 ユーザ端末
 - 3 ユーザ情報DB
 - 1 1 通信部
 - 1 2 記憶部
 - 1 3 操作部
 - 1 4 表示部
 - 1 5 入出力インターフェース
 - 1 6 システム制御部

1 6 a C P U

1 6 b R O M

1 6 c R A M

1 7 システムバス

1 6 1 現在ユーザ状況特定部

1 6 2 過去ユーザ状況取得部

1 6 3 簡略化部

1 6 4 パスワード入力画面出力部

1 6 5 認証部

N W ネットワーク

S 1、S 2 情報処理システム

請求の範囲

- [請求項1] ユーザが置かれている現在の状況を特定する特定手段と、
過去の認証時に前記ユーザが置かれていた状況を取得する取得手段と、
前記ユーザが現在認証されている状態である場合、前記特定手段により特定された前記現在の状況及び前記取得手段により取得された前記過去の状況に応じて、前記ユーザが入力すべき認証情報を簡略化する簡略化手段と、
前記簡略化手段により簡略化された前記認証情報の入力を促す情報を出力する出力手段と、
を備えることを特徴とする情報処理装置。
- [請求項2] 請求項1に記載の情報処理装置において、
前記ユーザが認証されている状態で再度の認証を要する利用対象を前記ユーザが利用しようとするごとに、前記取得手段、前記特定手段、前記簡略化手段及び前記出力手段は動作し、
前記簡略化手段は、前記特定手段により特定された状況と前記取得手段により取得された状況とが一致することに応じて簡略化された認証情報を用いる認証が連続する場合、前回の簡略化の度合いよりも小さい度合いで簡略化された認証情報を生成することを特徴とする情報処理装置。
- [請求項3] 請求項1又は2に記載の情報処理装置において、
前記簡略化手段は、前記現在の状況と前記過去の状況とが異なる場合、状況の差が大きいほど小さい度合いで簡略化された認証情報を生成することを特徴とする情報処理装置。
- [請求項4] 請求項3に記載の情報処理装置において、
前記ユーザが認証されている状態で再度の認証を要する利用対象を前記ユーザが利用しようとするごとに、前記取得手段、前記特定手段、前記簡略化手段及び前記出力手段は動作し、

前記簡略化手段は、前記特定手段により特定された状況と前記取得手段により取得された状況とが異なることに応じて簡略化された認証情報を用いる認証が連続するごとに、前回の簡略化の度合いと同じ度合いで認証情報を簡略化することが可能な状況の差を前回よりも小さくすることを特徴とする情報処理装置。

[請求項5] 請求項1乃至4の何れか1項に記載の情報処理装置において、
前記簡略化手段は、前記現在の状況が、安全性に関連する所定条件に合致しない場合、前記認証情報を簡略化しないことを特徴とする情報処理装置。

[請求項6] 請求項1乃至5の何れか1項に記載の情報処理装置において、
前記簡略化手段は、前記現在の状況と前記過去の状況とに応じて、前記ユーザが本来入力すべき認証情報のうち簡略化によって前記ユーザに入力させる部分を異ならせることを特徴とする情報処理装置。

[請求項7] 請求項6に記載の情報処理装置において、
前記簡略化手段は、前記認証情報が複数のコードを含む場合、前記現在の状況と前記過去の状況との差に応じて、前記ユーザが本来入力すべき認証情報のうち簡略化によって前記ユーザに入力させるコードの種類を異ならせることを特徴とする情報処理装置。

[請求項8] 請求項6又は7に記載の情報処理装置において、
前記簡略化手段は、前記認証情報が複数のコードを含む場合、前記現在の状況と前記過去の状況との差に応じて、前記ユーザが本来入力すべき認証情報のうち簡略化によって前記ユーザに入力させるコードの種類数を異ならせることを特徴とする情報処理装置。

[請求項9] 請求項6乃至8の何れか1項に記載の情報処理装置において、
前記簡略化手段は、前記認証情報が複数のコードを含む場合、前記現在の状況と前記過去の状況との差に応じて、前記認証情報に含まれる複数のコードのうち前記ユーザが入力すべきコードの数を異ならせることを特徴とする情報処理装置。

- [請求項10] 請求項 1 乃至 9 の何れか 1 項に記載の情報処理装置において、
記憶手段に記憶された、前記ユーザが本来入力すべき認証情報から、前記簡略化手段により簡略化された認証情報に含まれない部分を取得する部分取得手段と、
前記部分取得手段により取得された部分で、前記出力手段により出力された前記情報に応じて入力された認証情報を補完することにより生成された認証情報を取得する認証情報取得手段と、
前記認証情報取得手段により取得された前記認証情報と、前記記憶手段に記憶された前記認証情報とを比較して前記ユーザの認証の成否を判定する判定手段と、
を更に備えることを特徴とする情報処理装置。
- [請求項11] 請求項 1 乃至 9 の何れか 1 項に記載の情報処理装置において、
記憶手段に記憶された、前記ユーザが本来入力すべき認証情報のうち、前記簡略化手段により簡略化された認証情報の位置を特定する位置特定手段と、
前記出力手段により出力された前記情報に応じて入力された認証情報と、前記記憶手段に記憶された前記認証情報のうち前記位置特定手段により特定された位置にある部分とを比較して前記ユーザの認証の成否を判定する判定手段と、
を更に備えることを特徴とする情報処理装置。
- [請求項12] 請求項 1 乃至 11 の何れか 1 項に記載の情報処理装置において、
前記出力手段は、前記ユーザが本来入力すべき認証情報のうち前記簡略化手段により簡略化された前記認証情報に含まれない部分について所定記号を出力することを特徴とする情報処理装置。
- [請求項13] 請求項 1 乃至 12 の何れか 1 項に記載の情報処理装置において、
前記出力手段により出力された前記情報に応じて入力された認証情報を用いた認証が失敗した場合、前記出力手段は、前記ユーザが本来入力すべき認証情報全部の入力を促す第 2 情報を出力することを特徴

とする情報処理装置。

[請求項14] 請求項1乃至13の何れか1項に記載の情報処理装置において、
前記簡略化手段は、前記ユーザが入力すべき該ユーザの識別情報を簡略化し、

前記出力手段は、前記簡略化手段により簡略化された前記識別情報の入力を促す前記情報を出力することを特徴とする情報処理装置。

[請求項15] コンピュータにより実行される情報処理方法であって、
ユーザが置かれている現在の状況を特定する特定ステップと、
過去の認証時に前記ユーザが置かれていた状況を取得する取得ステップと、

前記ユーザが現在認証されている状態である場合、前記特定ステップにより特定された前記現在の状況及び前記取得ステップにより取得された前記過去の状況に応じて、前記ユーザが入力すべき認証情報を簡略化する簡略化ステップと、

前記簡略化ステップにより簡略化された前記認証情報の入力を促す情報を出力する出力ステップと、

を含むことを特徴とする情報処理方法。

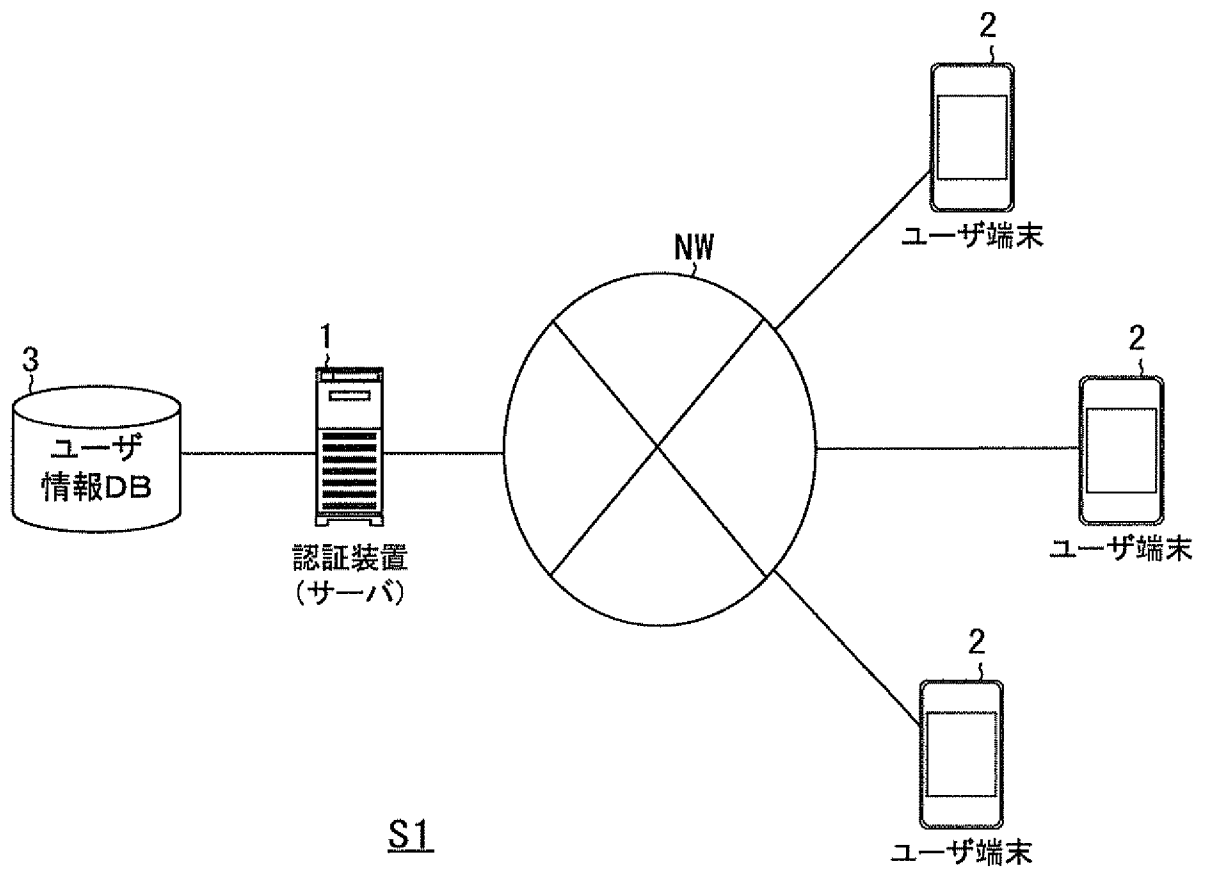
[請求項16] コンピュータを、
ユーザが置かれている現在の状況を特定する特定手段、
過去の認証時に前記ユーザが置かれていた状況を取得する取得手段、

前記ユーザが現在認証されている状態である場合、前記特定手段により特定された前記現在の状況及び前記取得手段により取得された前記過去の状況に応じて、前記ユーザが入力すべき認証情報を簡略化する簡略化手段、及び、

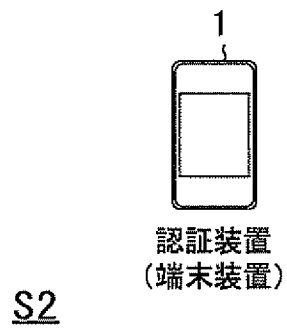
前記簡略化手段により簡略化された前記認証情報の入力を促す情報を出力する出力手段、

として機能させることを特徴とする情報処理プログラム。

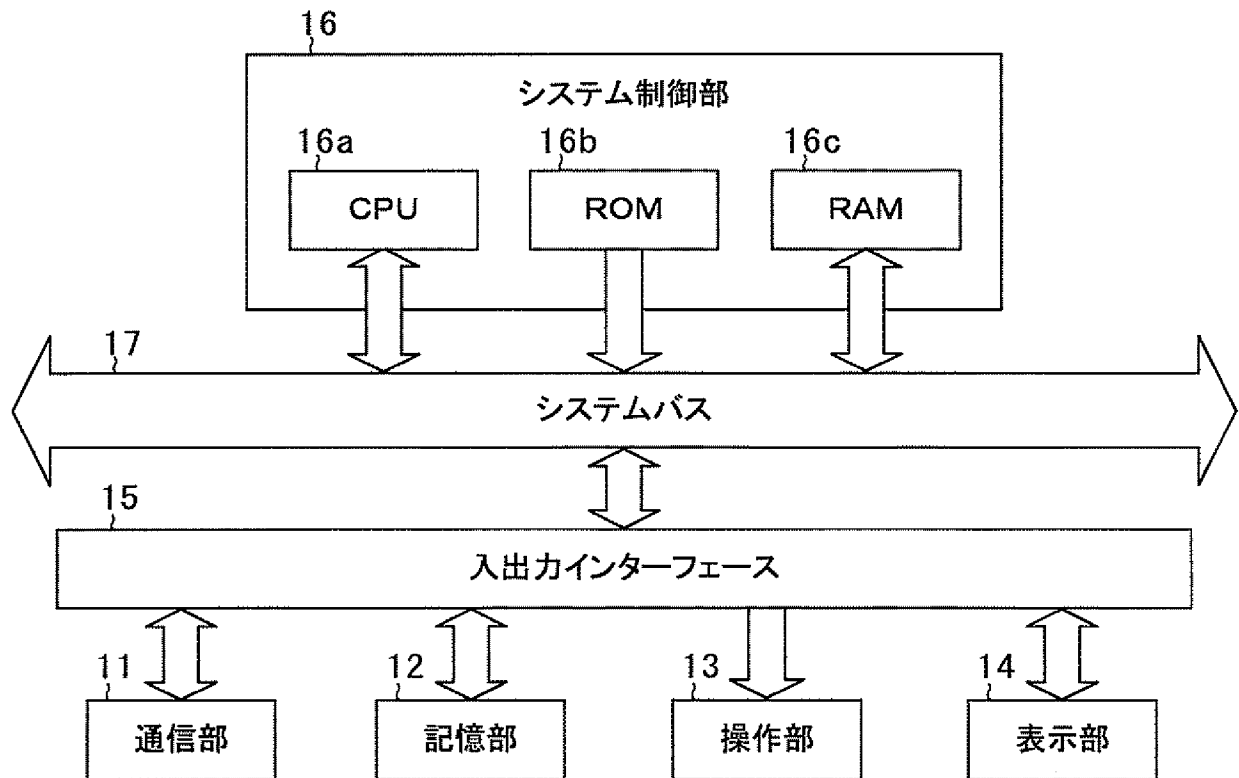
[図1A]



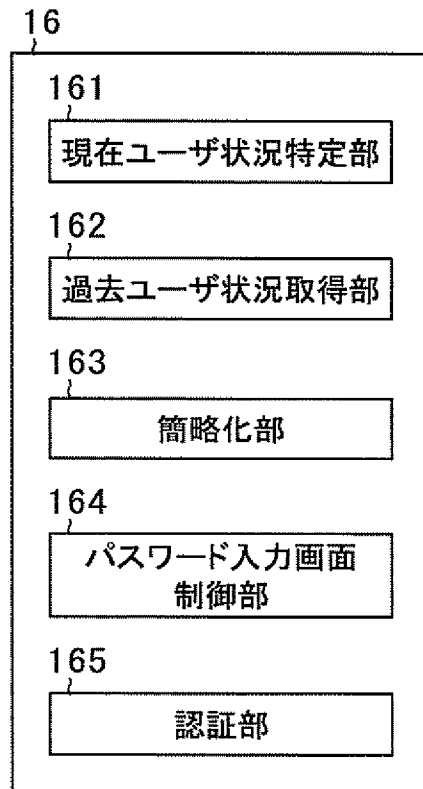
[図1B]



[図2A]



[図2B]



[図3A]

状況	一致	不一致
安全性	高	低
簡略度	2	1

[図3B]

安全性	高	低
文字種のバリエーション数	少ない	多い

[図3C]

登録パスワード	安全性	
	高	低
	簡略化されたパスワード	
q3nifa83e	383	qni

[図3D]

安全性	高	低
文字種の数	少ない	多い

[図3E]

登録パスワード	安全性	
	高	低
	簡略化されたパスワード	
q3nifa83e	nifa	a83e

[図3F]

安全性	高	↔	低
文字数	少ない	↔	多い

[図3G]

登録パスワード	安全性	
	高	低
	簡略化されたパスワード	
q3nifa83e	q3n	q3ni

[図4A]

110 ご本人確認のためパスワードの一部を入力してください。

ユーザID

120 abc@xyzsite.com

130 パスワード

131 * * * * *

132

140 ログイン

[図4B]

110 ご本人確認のためパスワードの一部を入力してください。

ユーザID

120 abc@xyzsite.com

130 パスワード

133 * * * * *

132

133

140 ログイン

[図4C]

110 ご本人確認のためパスワードの一部を入力してください。

ユーザID

120 abc@xyzsite.com

150 パスワード

151 * * * *

152

161 ↓ ↓ ↓

161 161 162 ここに入力してください 160

161

140 ログイン

[図4D]

170 ご本人確認のためパスワードを入力してください。

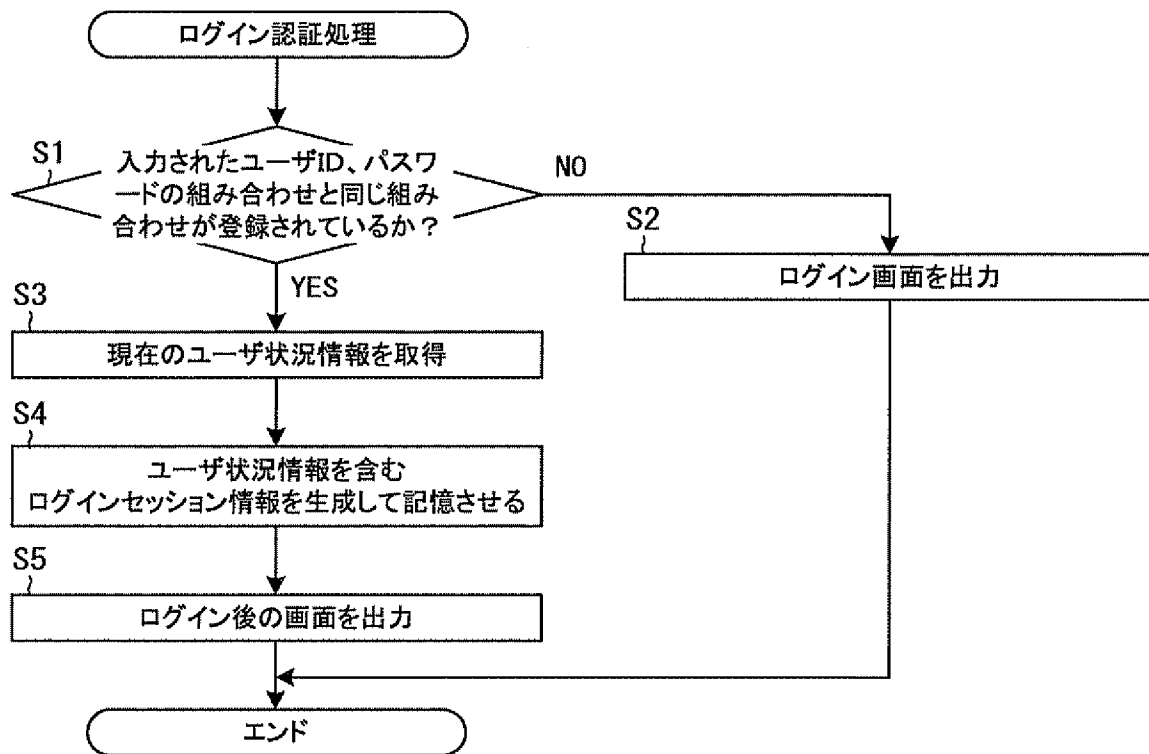
ユーザID

120 abc@xyzsite.com

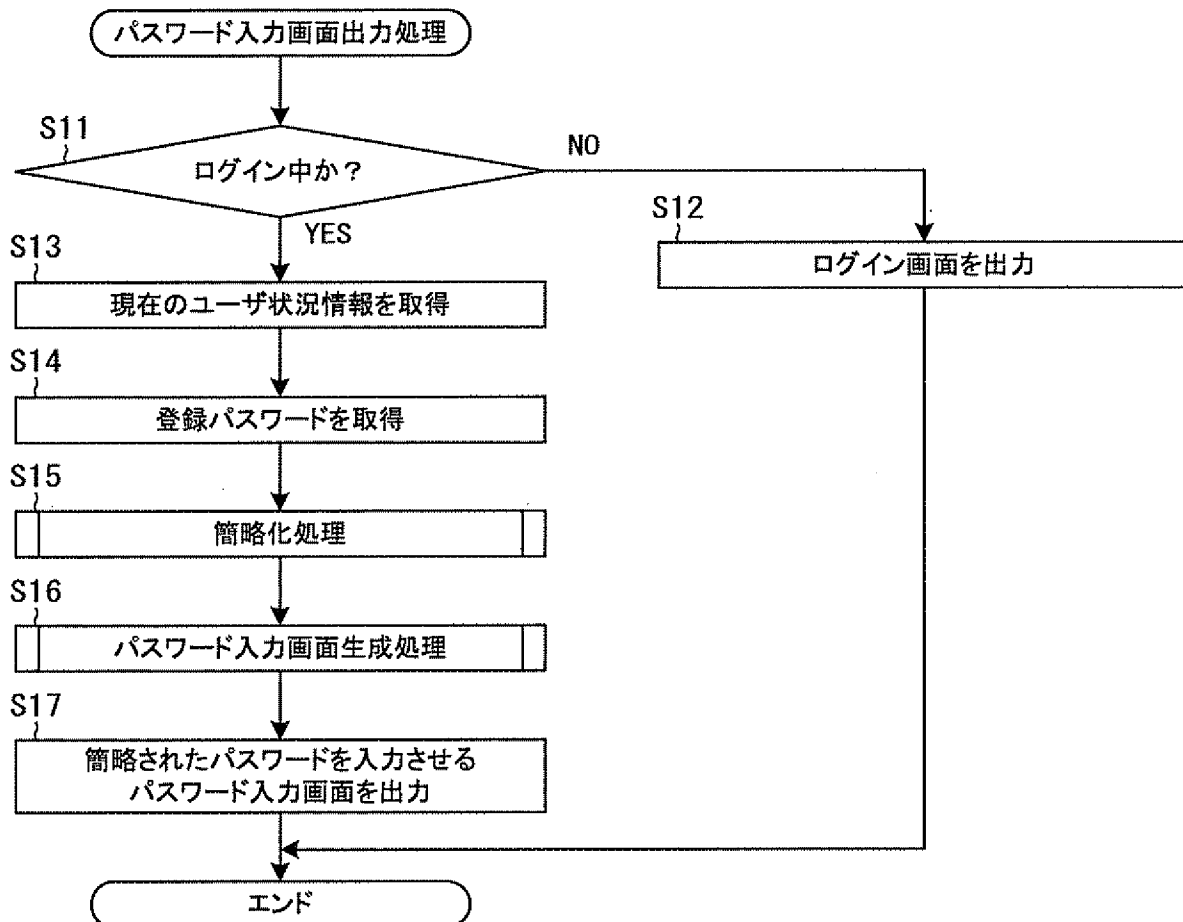
180 パスワード

140 ログイン

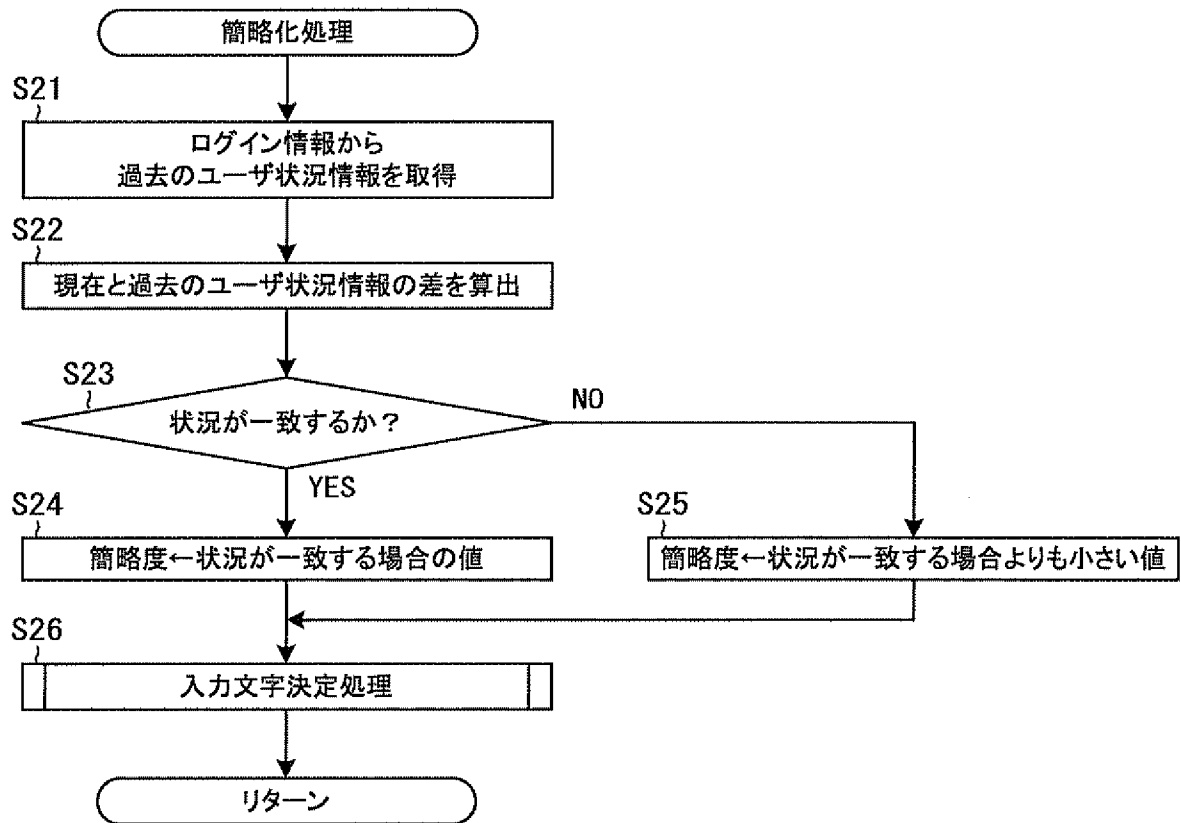
[図5]



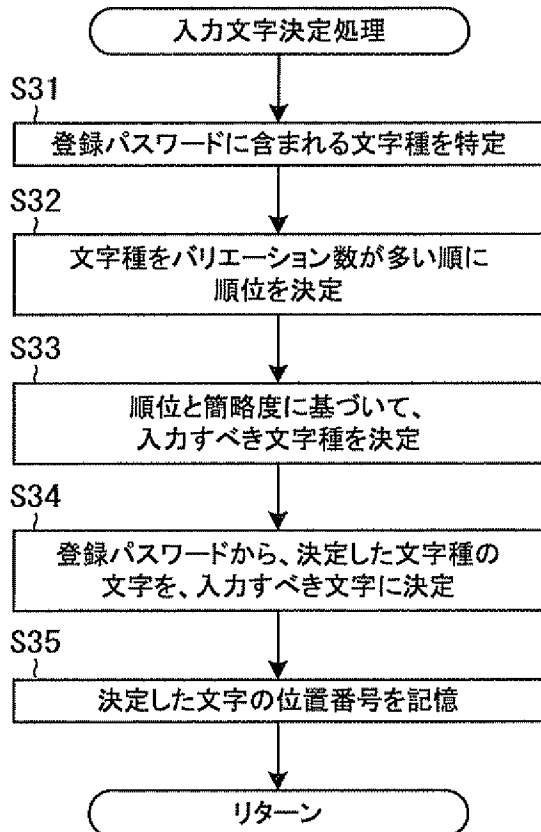
[図6]



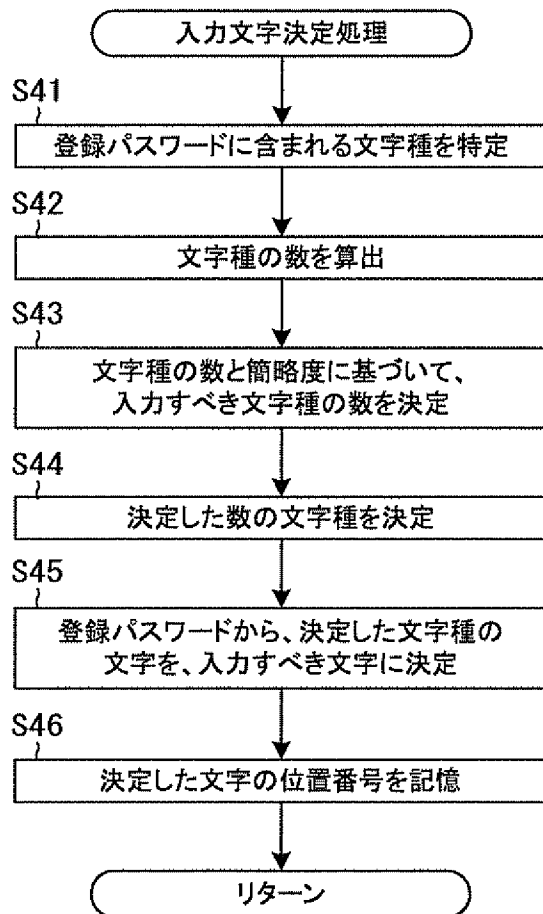
[図7]



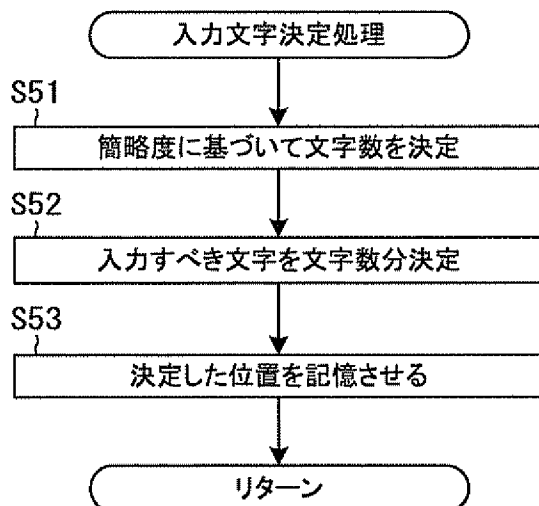
[図8A]



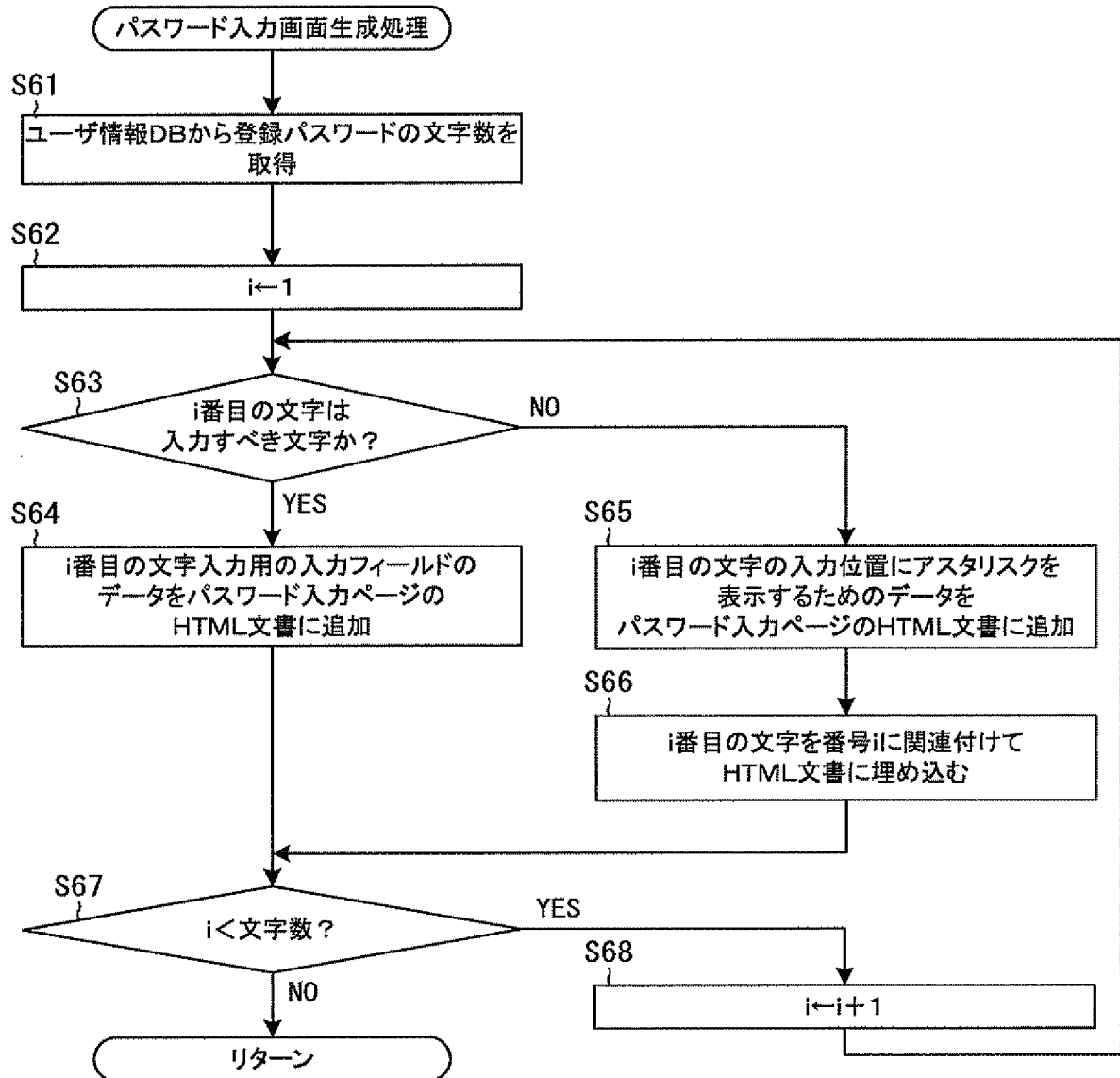
[図8B]



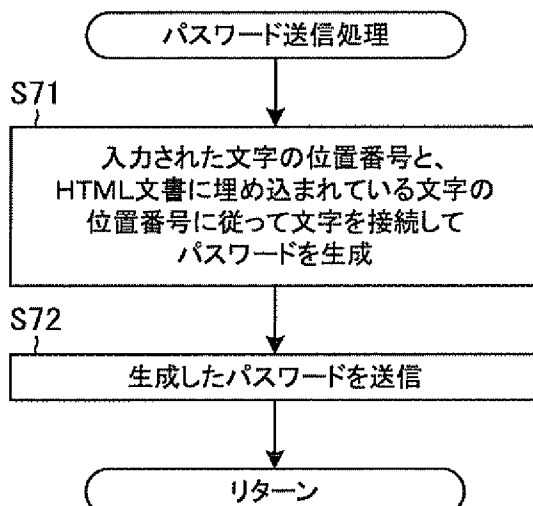
[図8C]



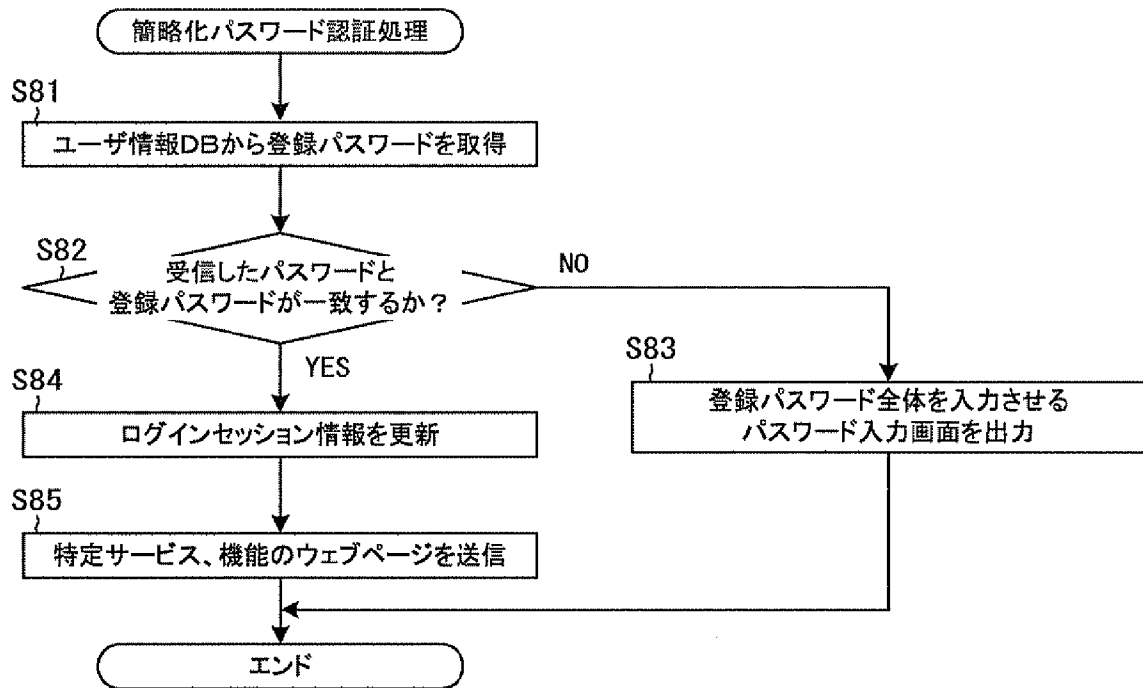
[図9]



[図10A]



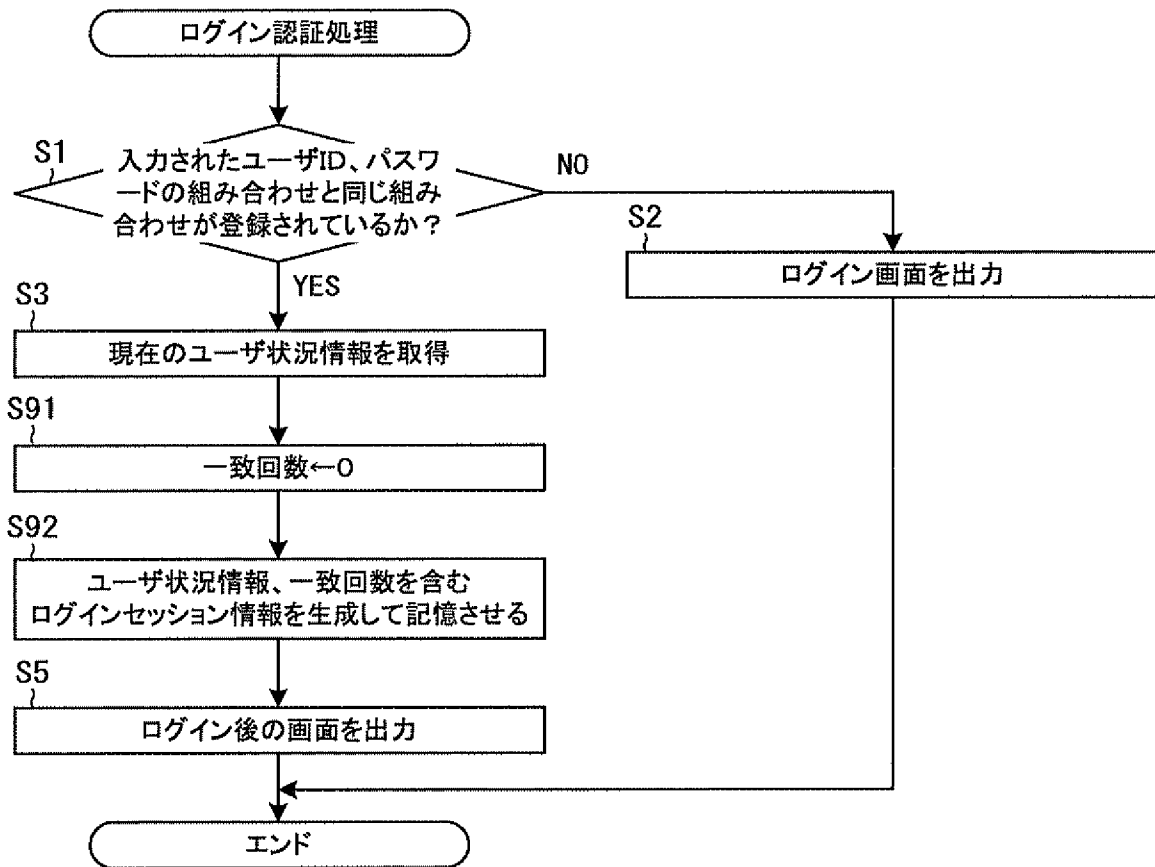
[図10B]



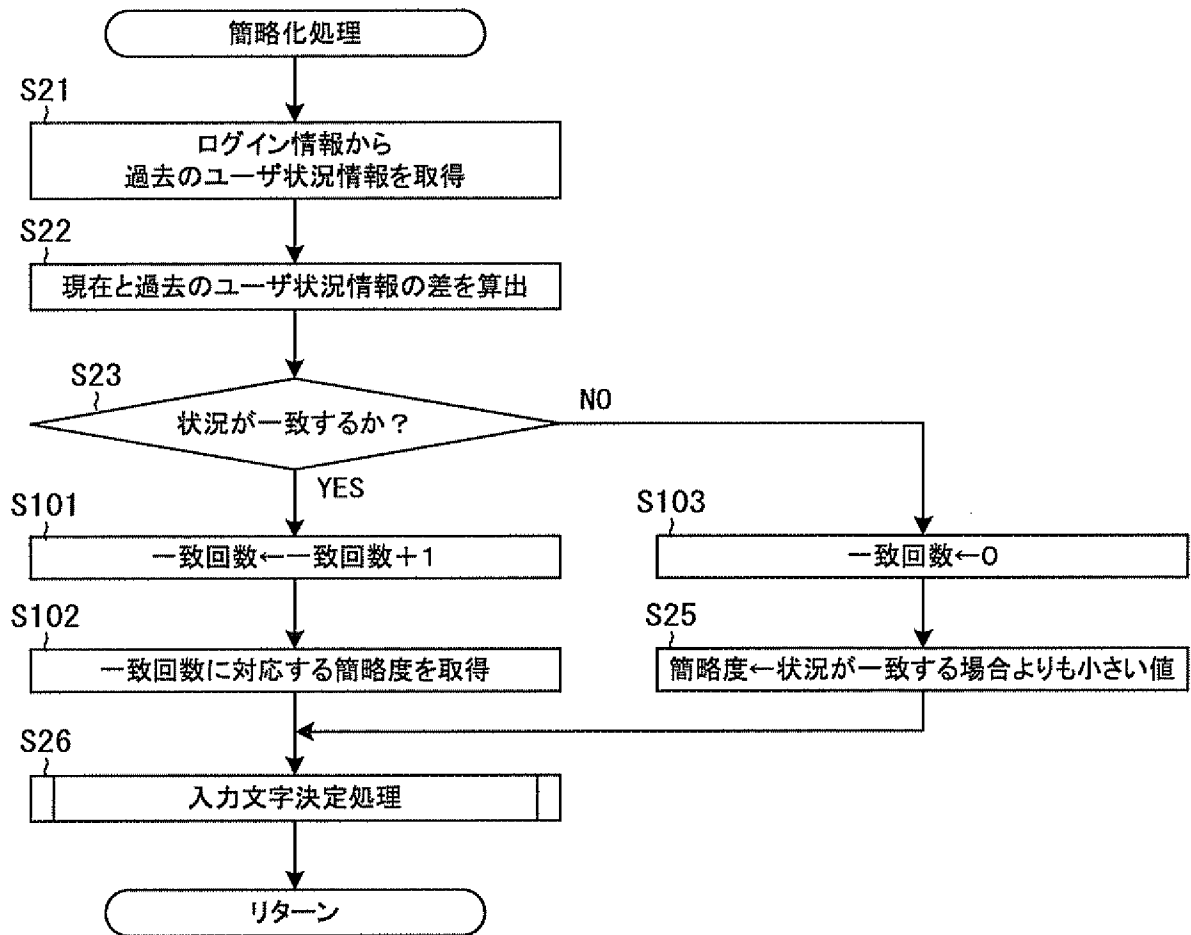
[図11]

状況	一致					不一致
状況が連続して一致する回数	1	2	3	4	5～	—
簡略度	6	5	4	3	2	1

[図12]



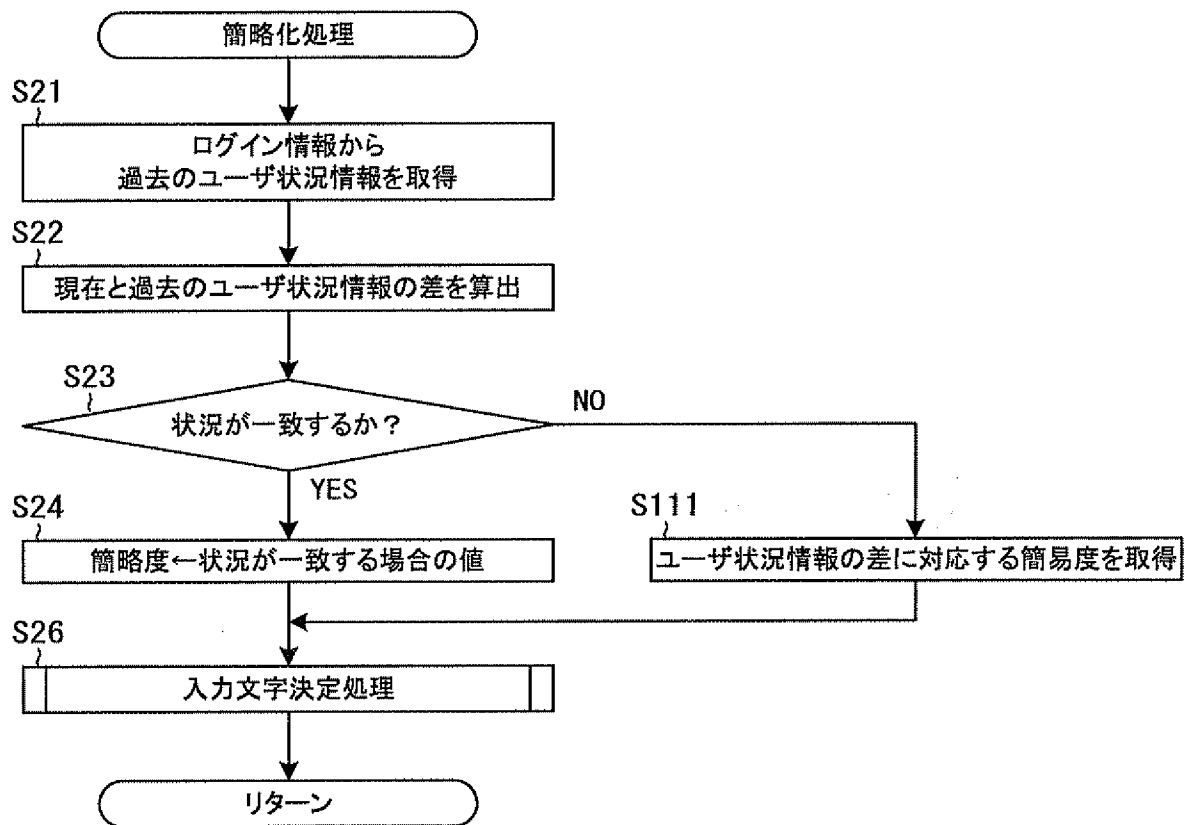
[図13]



[図14]

状況	一致	不一致				
状況の差	0	1	2	3	4	5～
簡略度	6	5	4	3	2	1

[図15]



[図16A]

状況が最初に不一致

状況の差	1~4	5~8	9~12	13~16	17~
簡略度	5	4	3	2	1

[図16B]

状況が2回連続して不一致

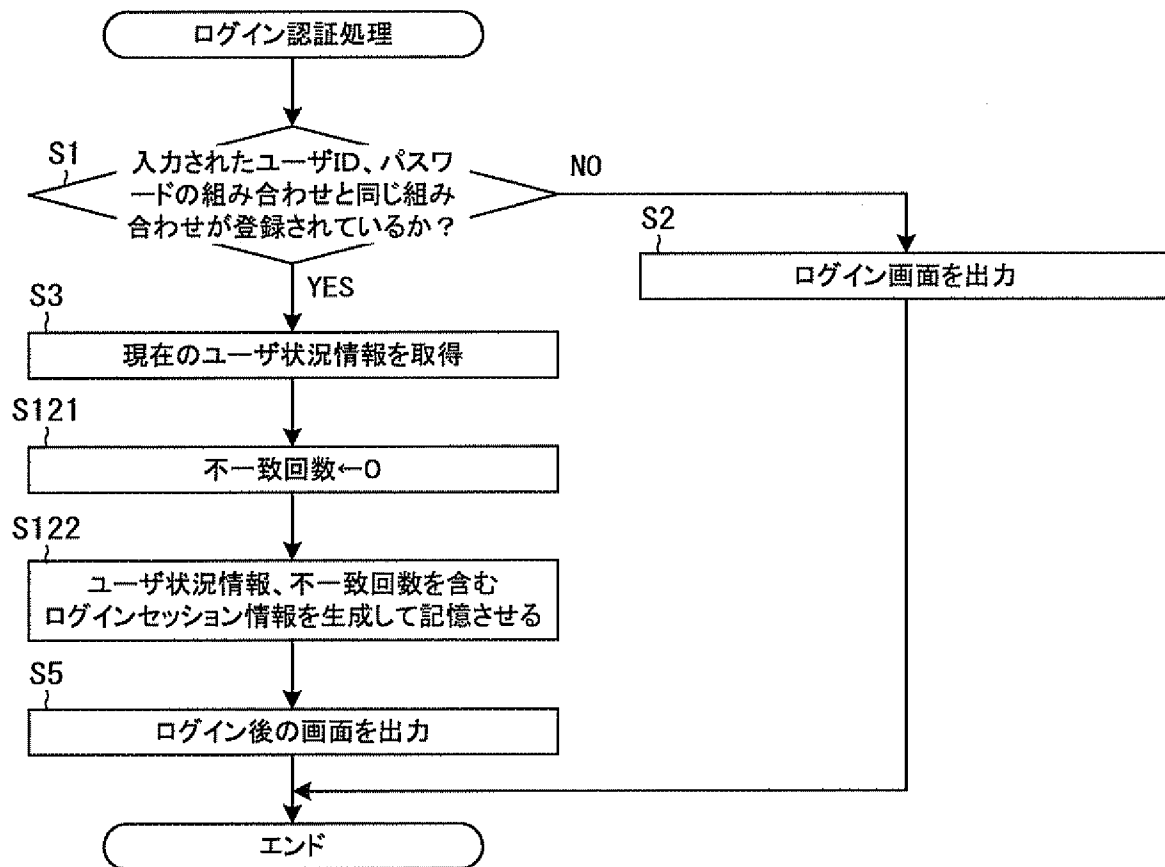
状況の差	1~2	3~4	5~6	7~8	9~
簡略度	5	4	3	2	1

[図16C]

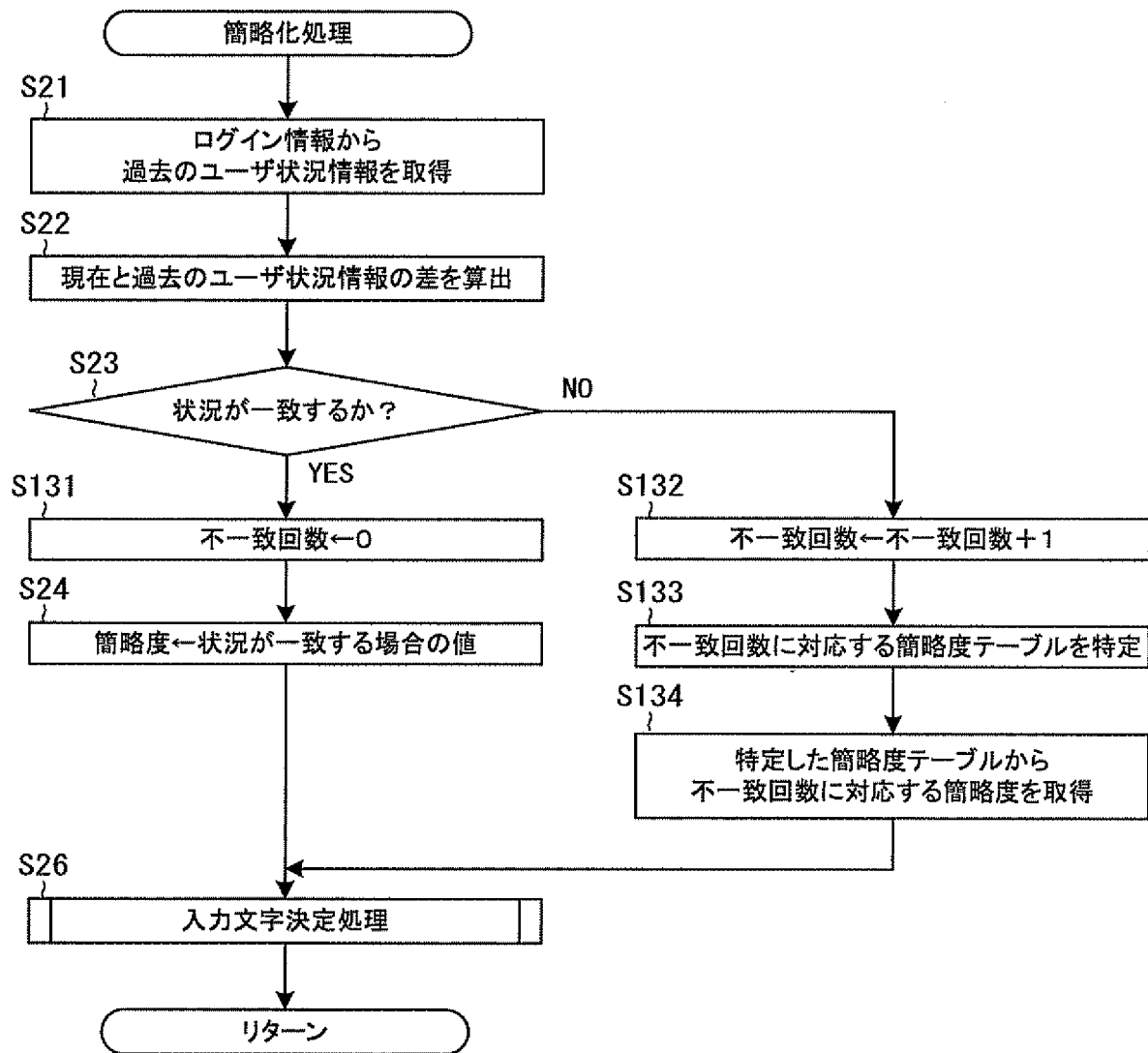
状況が3回連続して不一致

状況の差	1	2	3	4	5~
簡略度	5	4	3	2	1

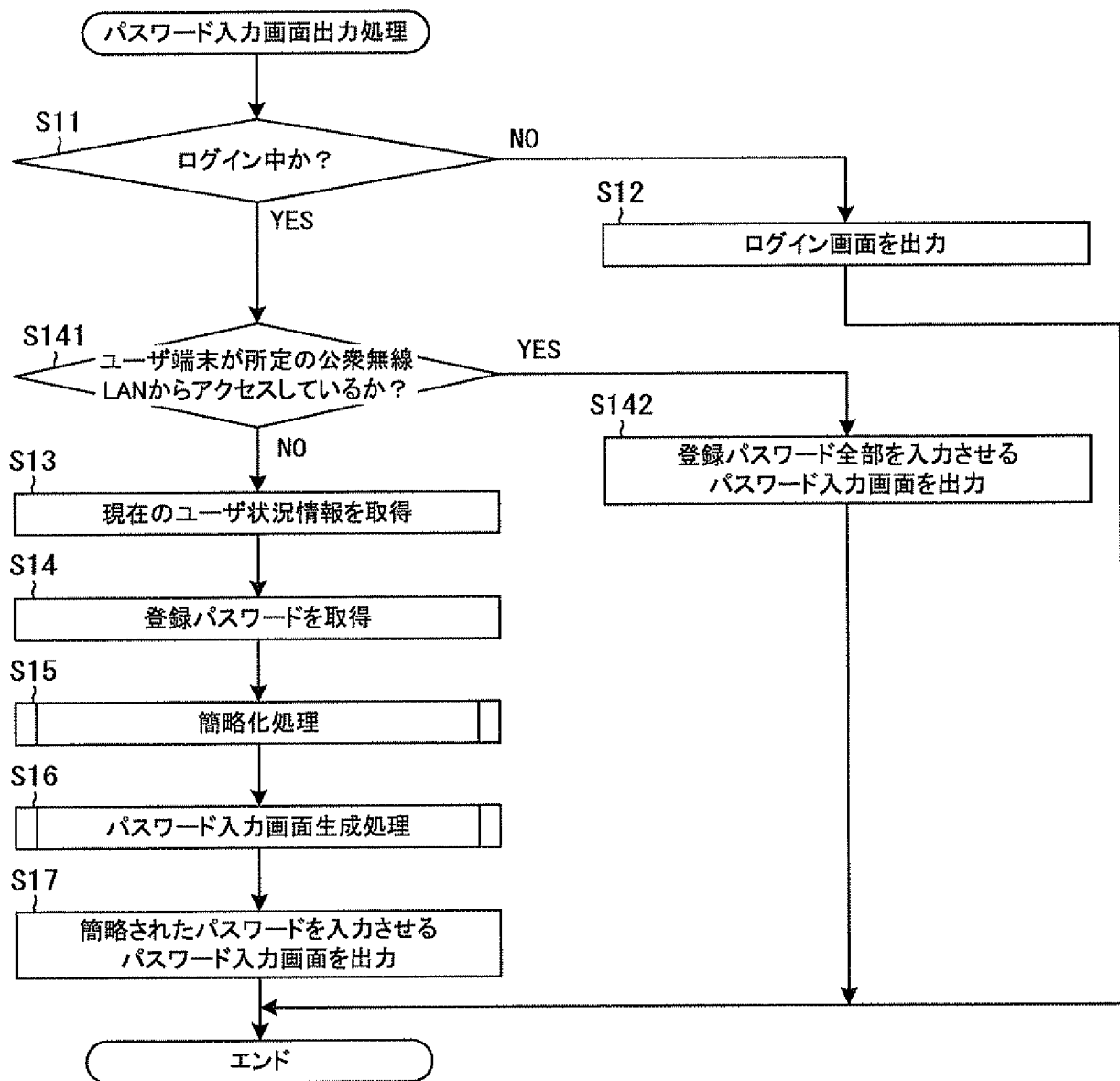
[図17]



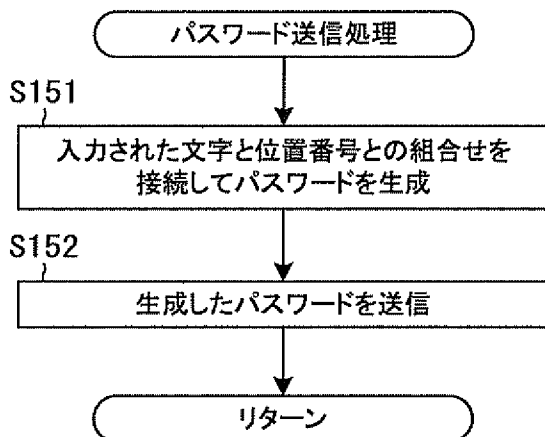
[図18]



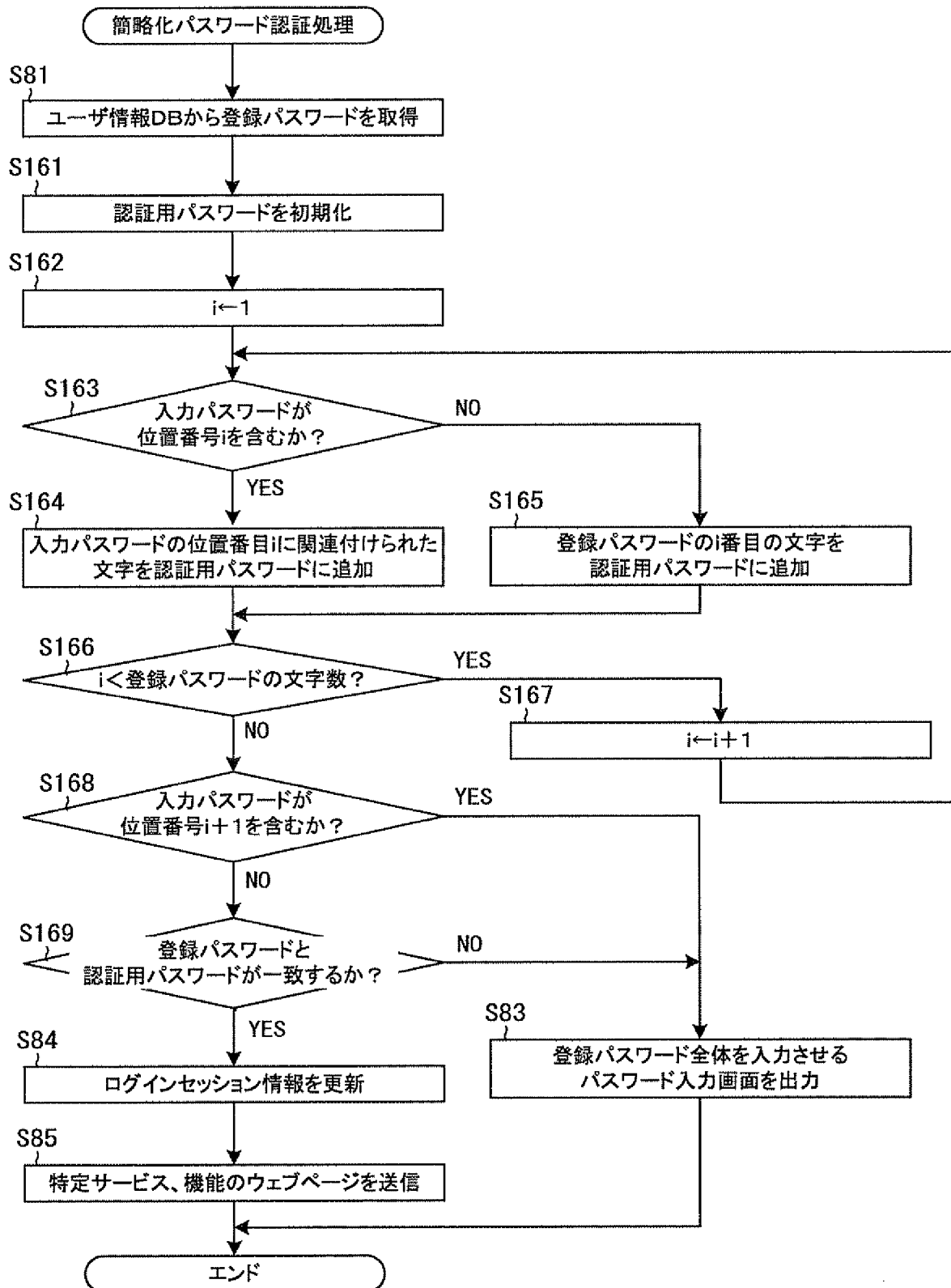
[図19]



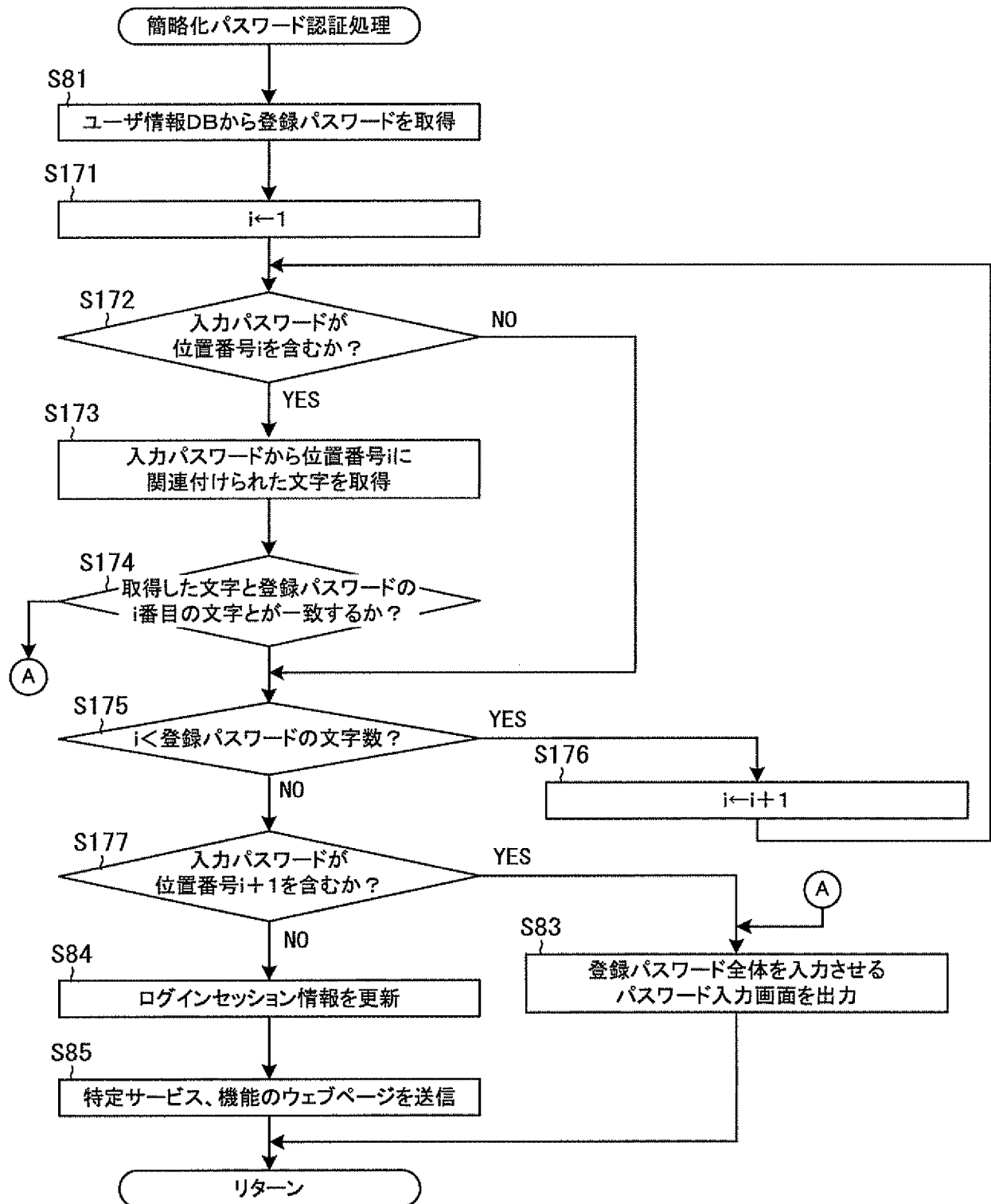
[図20]

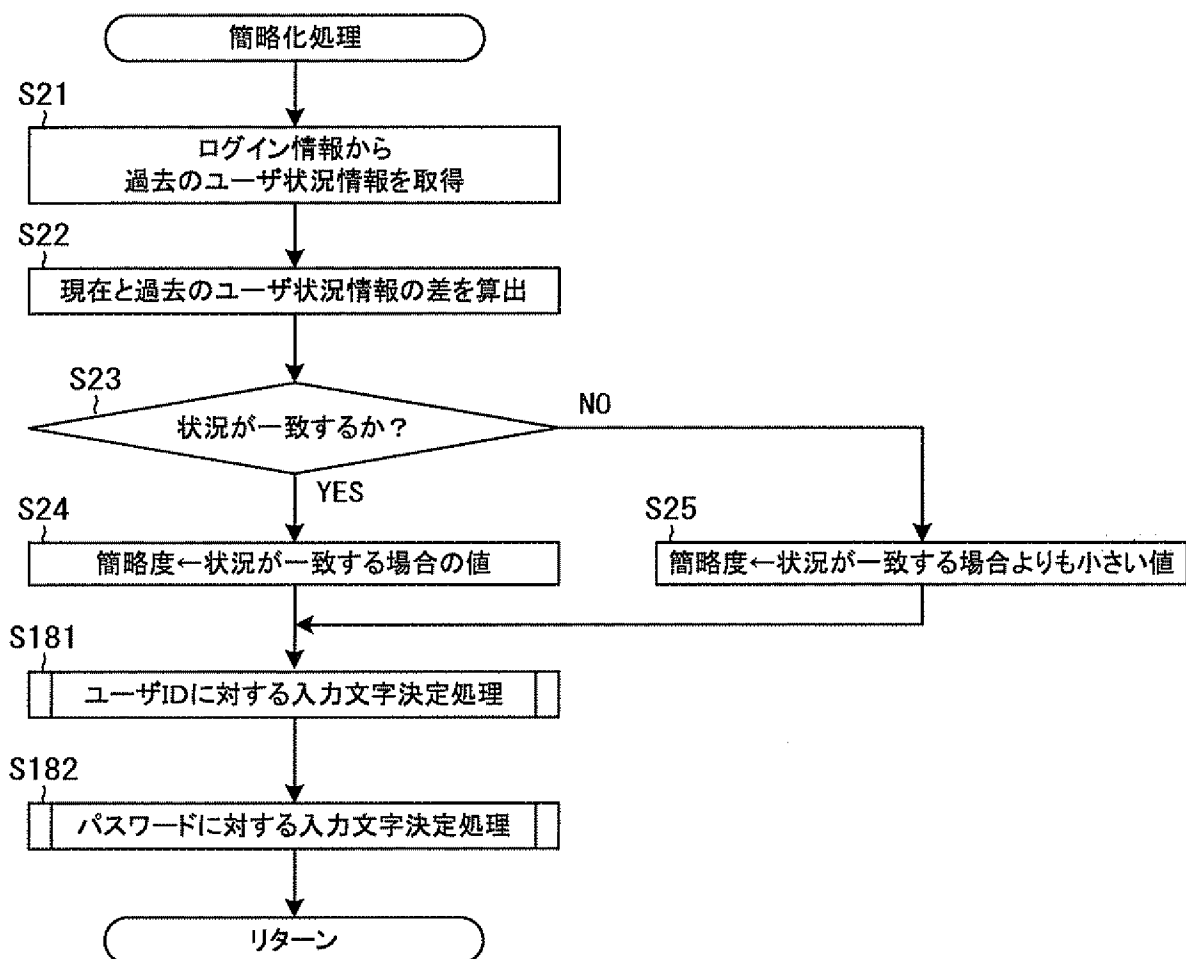
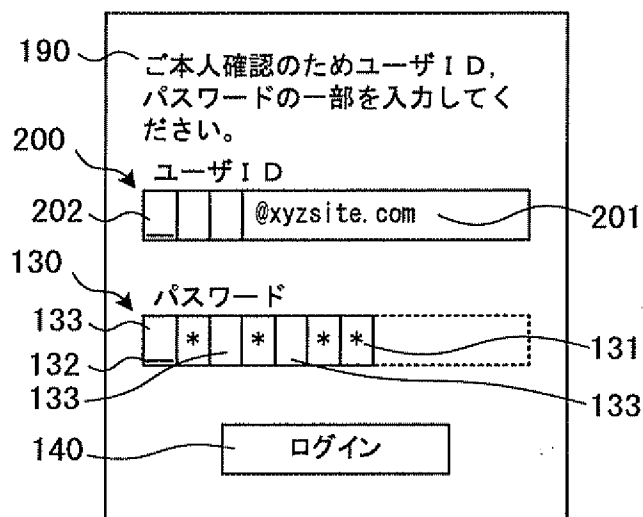


[図21]

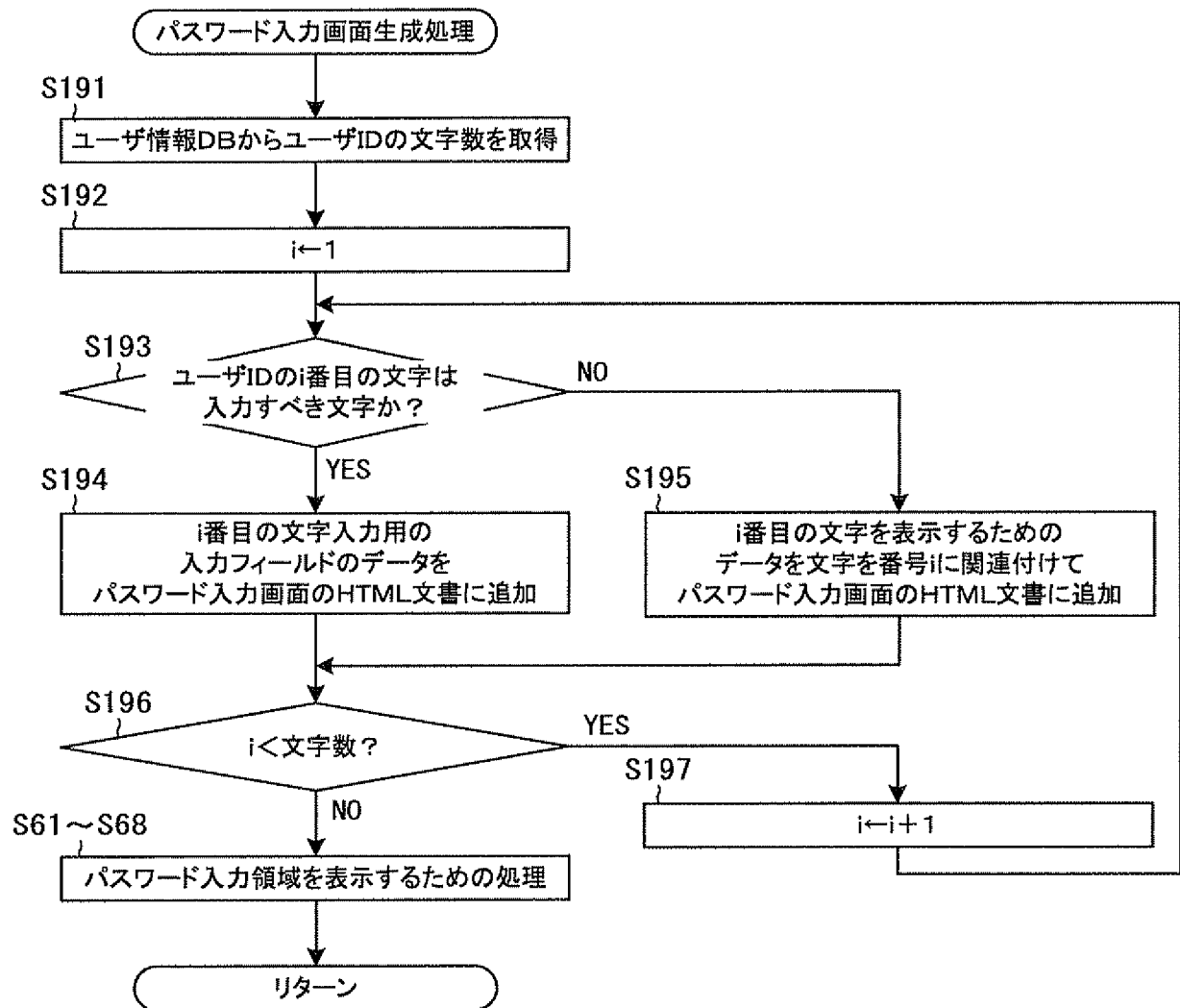


[図22]

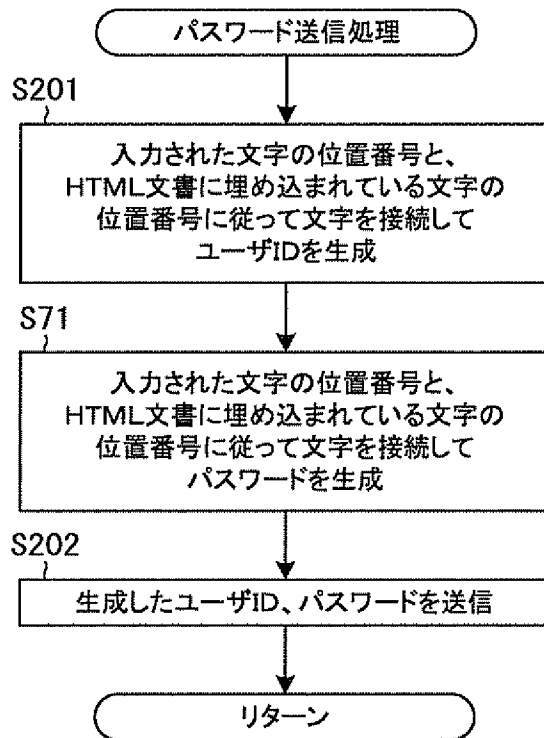




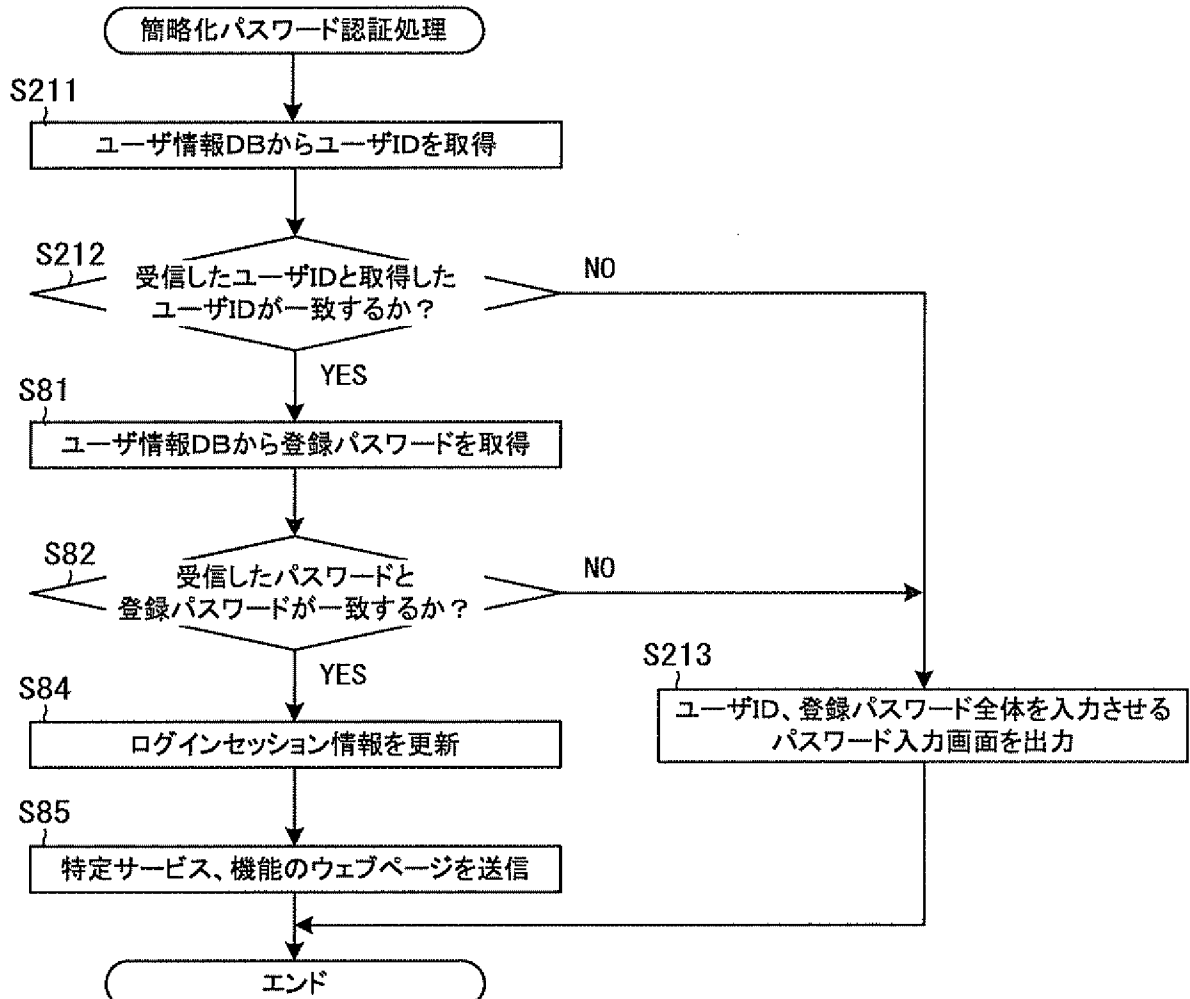
[図25]



[図26]



[図27]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/066993

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/31(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)

G06F21/31

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2004-118456 A (Japan Science and Technology Corp.), 15 April 2004 (15.04.2004), abstract; paragraphs [0013] to [0016] (Family: none)	1, 3, 5-16 2, 4
Y A	JP 2009-187183 A (NEC Corp.), 20 August 2009 (20.08.2009), paragraphs [0063] to [0069] & US 2008/0180989 A1 & US 2011/0194338 A1 & DE 102008006543 A & KR 10-2008-0071348 A & CN 101256831 A & TW 200845364 A	1, 3, 5-16 2, 4
Y	JP 2008-40984 A (NEC Corp. et al.), 21 February 2008 (21.02.2008), paragraphs [0038] to [0049]; fig. 8 (Family: none)	12-14

☒ 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
22 September, 2014 (22.09.14)

Date of mailing of the international search report
30 September, 2014 (30.09.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/066993

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/011259 A1 (TZEE, INC. D/B/A TZEE), 28 January 2010 (28.01.2010), paragraphs [25] to [32] & US 2010/0024028 A1 & US 2010/0020972 A1 & US 2010/0024020 A1 & US 2010/0162387 A1 & US 2010/0162388 A1 & WO 2010/011257 A1 & WO 2010/011258 A1	1-16
A	JP 2007-6256 A (Matsushita Electric Industrial Co., Ltd.), 11 January 2007 (11.01.2007), abstract (Family: none)	2-14
A	JP 2010-204808 A (Casio Hitachi Mobile Communications Co., Ltd.), 16 September 2010 (16.09.2010), abstract (Family: none)	2-14

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/31(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（I P C））

Int.Cl. G06F21/31

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 4 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 4 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 4 年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2004-118456 A（科学技術振興事業団） 2004.04.15, 要約, 段落 0013-0016 (No Family)	1, 3, 5-16 2, 4
Y A	JP 2009-187183 A（日本電気株式会社） 2009.08.20, 段落 0063-0069 & US 2008/0180989 A1 & US 2011/0194338 A1 & DE 102008006543 A & KR 10-2008-0071348 A & CN 101256831 A & TW 200845364 A	1, 3, 5-16 2, 4

☒ 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

2 2 . 0 9 . 2 0 1 4

国際調査報告の発送日

3 0 . 0 9 . 2 0 1 4

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

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）

金木 陽一

5 S

4 8 7 6

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2008-40984 A (日本電気株式会社ほか) 2008.02.21, 段落 0038-0049, 図 8 (No Family)	12-14
A	WO 2010/011259 A1 (TZEE, INC. D/B/A TZEE) 2010.01.28, 段落 25-32 & US 2010/0024028 A1 & US 2010/0020972 A1 & US 2010/0024020 A1 & US 2010/0162387 A1 & US 2010/0162388 A1 & WO 2010/011257 A1 & WO 2010/011258 A1	1-16
A	JP 2007-6256 A (松下電器産業株式会社) 2007.01.11, 要約 (No Family)	2-14
A	JP 2010-204808 A (株式会社カシオ日立モバイルコミュニケーショ ンズ) 2010.09.16, 要約 (No Family)	2-14