

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6170982号
(P6170982)

(45) 発行日 平成29年7月26日 (2017. 7. 26)

(24) 登録日 平成29年7月7日 (2017. 7. 7)

(51) Int. Cl. F I
G06F 21/31 (2013.01) G O 6 F 21/31 3 6 0
G06F 21/50 (2013.01) G O 6 F 21/50

請求項の数 13 (全 34 頁)

<p>(21) 出願番号 特願2015-206280 (P2015-206280)</p> <p>(22) 出願日 平成27年10月20日 (2015. 10. 20)</p> <p>(65) 公開番号 特開2017-78944 (P2017-78944)</p> <p>(43) 公開日 平成29年4月27日 (2017. 4. 27)</p> <p>審査請求日 平成28年11月1日 (2016. 11. 1)</p> <p>早期審査対象出願</p>	<p>(73) 特許権者 500257300 ヤフー株式会社 東京都千代田区紀尾井町1番3号</p> <p>(74) 代理人 110002147 特許業務法人酒井国際特許事務所</p> <p>(72) 発明者 五味 秀仁 東京都港区赤坂九丁目7番1号 ヤフー株式会社内</p> <p>(72) 発明者 寺岡 照彦 東京都港区赤坂九丁目7番1号 ヤフー株式会社内</p> <p>審査官 脇岡 剛</p>
---	--

最終頁に続く

(54) 【発明の名称】 判定装置、判定方法及び判定プログラム

(57) 【特許請求の範囲】

【請求項1】

端末装置を利用するユーザの本人性の認証の要求を受信する受信部と、
 前記端末装置のコンテキストを示す情報であるコンテキスト情報を定期的を取得する取得部と、

前記取得部によって取得されたコンテキスト情報に基づいて、前記端末装置から要求された認証に関する判定を行う判定部と、

を備え、

前記判定部は、

過去に前記端末装置から要求された認証に関する判定を行った時点におけるコンテキスト情報と、新たに前記受信部によって認証の要求が受信された時点において取得されたコンテキスト情報とに変化がない場合には、認証の要求の時点間において定期的取得されたコンテキスト情報の中に、過去に取得されたいずれかのコンテキスト情報に一致又は類似するコンテキスト情報が含まれるか否かに基づいて、新たに認証を行うか否かを判定する、

ことを特徴とする判定装置。

【請求項2】

前記判定部は、

前記受信部によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化に基づいて、前記受

信部によって受信された認証の要求に対する認証手続きを行うことを要するか否かを判定する、

ことを特徴とする請求項 1 に記載の判定装置。

【請求項 3】

前記判定部は、

前記受信部によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化率に基づいて、前記受信部によって受信された認証の要求に対する認証手続きを行うことを要するか否かを判定する、

ことを特徴とする請求項 1 又は 2 に記載の判定装置。

10

【請求項 4】

前記判定部は、

前記受信部によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化量に基づいて、前記受信部によって受信された認証の要求に対する認証手続きを行うことを要するか否かを判定する、

ことを特徴とする請求項 1 ~ 3 のいずれか一つに記載の判定装置。

【請求項 5】

前記判定部は、

前記受信部によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化のパターンに基づいて、前記受信部によって受信された認証の要求に対する認証手続きを行うことを要するか否かを判定する、

ことを特徴とする請求項 1 ~ 4 のいずれか一つに記載の判定装置。

20

【請求項 6】

前記端末装置が認証される際の当該端末装置のコンテキストについて登録を受け付ける登録部、

をさらに備え、

前記判定部は、

前記認証の要求が受信された場合に取得されたコンテキスト情報が、前記登録部によって登録済みのコンテキストを示すものである場合には、当該認証の要求に対する認証手続きを行うことを要しないと判定する、

ことを特徴とする請求項 1 ~ 5 のいずれか一つに記載の判定装置。

30

【請求項 7】

前記取得部によって取得されたコンテキスト情報に基づいて、前記端末装置が認証される際の当該端末装置のコンテキストを推定する推定部、

をさらに備え、

前記判定部は、

前記認証の要求が受信された場合に取得されたコンテキスト情報が、前記推定部によって推定されたコンテキストを示すものである場合には、当該認証の要求に対する認証手続きを行うことを要しないと判定する、

ことを特徴とする請求項 1 ~ 6 のいずれか一つに記載の判定装置。

40

【請求項 8】

前記推定部は、

前記取得部によって取得されたコンテキスト情報のログと、前記端末装置が以前に認証された際のコンテキスト情報のログとの類似度に基づいて、前記端末装置が認証される際の当該端末装置のコンテキストを推定する、

ことを特徴とする請求項 7 に記載の判定装置。

【請求項 9】

前記推定部によってコンテキストが推定される際に用いられる推定ルールに関する学習

50

を行う学習部、
 をさらに備え、
 前記推定部は、
 前記学習部によって学習された推定ルールであって、前記端末装置を利用するユーザに対応して学習された推定ルールに基づいて、当該端末装置のコンテキストを推定する、
 ことを特徴とする請求項 7 又は 8 に記載の判定装置。

【請求項 10】

前記推定部は、
 前記学習部によって学習された推定ルールであって、前記端末装置を利用するユーザ以外のユーザに対応して学習された推定ルールに基づいて、当該端末装置のコンテキストを推定する、
 ことを特徴とする請求項 9 に記載の判定装置。

10

【請求項 11】

前記判定部によって前記認証の要求に対する認証手続きを行うことを要すると判定された場合には、前記端末装置に対する認証手続きを行い、前記判定部によって前記認証の要求に対する認証手続きを行うことを要しないと判定された場合には、認証手続きを省いて当該端末装置を認証する認証部、
 をさらに備えたことを特徴とする請求項 1 ~ 10 のいずれか一つに記載の判定装置。

【請求項 12】

コンピュータが実行する判定方法であって、
 端末装置を利用するユーザの本人性の認証の要求を受信する受信工程と、
 前記端末装置のコンテキストを示す情報であるコンテキスト情報を取得する取得工程と、
 前記取得工程によって取得されたコンテキスト情報に基づいて、前記端末装置から要求された認証に関する判定を行う判定工程と、
 を含み、
 前記判定工程は、

20

過去に前記端末装置から要求された認証に関する判定を行った時点におけるコンテキスト情報と、新たに前記受信工程によって認証の要求を受信された時点において取得されたコンテキスト情報とに変化がない場合には、認証の要求の時点間において定期的に取得されたコンテキスト情報の中に、過去に取得されたいずれかのコンテキスト情報に一致又は類似するコンテキスト情報が含まれるか否かに基づいて、新たに認証を行うか否かを判定する、

30

ことを特徴とする判定方法。

【請求項 13】

端末装置を利用するユーザの本人性の認証の要求を受信する受信手順と、
 前記端末装置のコンテキストを示す情報であるコンテキスト情報を取得する取得手順と、
 前記取得手順によって取得されたコンテキスト情報に基づいて、前記端末装置から要求された認証に関する判定を行う判定手順と、
 をコンピュータに実行させ、
 前記判定手順は、

40

過去に前記端末装置から要求された認証に関する判定を行った時点におけるコンテキスト情報と、新たに前記受信手順によって認証の要求を受信された時点において取得されたコンテキスト情報とに変化がない場合には、認証の要求の時点間において定期的に取得されたコンテキスト情報の中に、過去に取得されたいずれかのコンテキスト情報に一致又は類似するコンテキスト情報が含まれるか否かに基づいて、新たに認証を行うか否かを判定する、

ことを特徴とする判定プログラム。

【発明の詳細な説明】

50

【技術分野】

【0001】

本発明は、判定装置、判定方法及び判定プログラムに関する。

【背景技術】

【0002】

近年、通信ネットワークの普及が進み、ネットワークを介したサービスが盛んに提供されている。例えば、ユーザは、通信端末装置を用いて、ネットワークを介して提供されるサービスにログインし、サービスを利用する。ユーザは、サービスのログイン等に際して、サービスを利用するユーザの本人認証が求められる。

【0003】

ネットワークにおける本人認証の技術として、端末に複数の認証方式が備えられている場合に、端末のおかれた環境に適したセンサを利用する認証方式を自動的に選択する技術が知られている（例えば、特許文献1）。

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2015-90589号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、上記の従来技術では、利便性に優れた本人認証を行うことは難しい。例えば、ユーザは、複数の認証方式の中から選択することのできる環境下でも、認証方式によっては、回答を入力したり、生体情報を入力したりといった煩雑な手順が要求される場合がある。また、ユーザにとっては、認証の度に情報の入力を求められることで、認証処理そのものが負担となる。

【0006】

本願は、上記に鑑みてなされたものであって、利便性に優れた本人認証を行うことができる判定装置、判定方法及び判定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】

【0007】

本願に係る判定装置は、端末装置を利用するユーザの本人性の認証の要求を受信する受信部と、前記端末装置のコンテキストを示す情報であるコンテキスト情報を取得する取得部と、前記取得部によって取得されたコンテキスト情報に基づいて、前記端末装置から要求された認証に関する判定を行う判定部と、を備えたことを特徴とする。

【発明の効果】

【0008】

実施形態の一態様によれば、利便性に優れた本人認証を行うことができるという効果を奏する。

【図面の簡単な説明】

【0009】

【図1】図1は、第1の実施形態に係る判定処理の一例を示す図である。

【図2】図2は、第1の実施形態に係る判定処理システムの構成例を示す図である。

【図3】図3は、第1の実施形態に係る判定装置の構成例を示す図である。

【図4】図4は、第1の実施形態に係る登録情報記憶部の一例を示す図である。

【図5】図5は、第1の実施形態に係る認証情報記憶部の一例を示す図である。

【図6】図6は、第1の実施形態に係る認証ログ記憶部の一例を示す図である。

【図7】図7は、第1の実施形態に係るコンテキストログ記憶部の一例を示す図である。

【図8】図8は、第1の実施形態に係るユーザ端末の構成例を示す図である。

【図9】図9は、第1の実施形態に係る判定処理手順を示すフローチャートである。

【図10】図10は、第1の実施形態に係る判定処理の変形例を示す図である。

10

20

30

40

50

【図 1 1】図 1 1 は、第 2 の実施形態に係る判定処理の一例を示す図である。

【図 1 2】図 1 2 は、第 2 の実施形態に係る判定装置の構成例を示す図である。

【図 1 3】図 1 3 は、第 3 の実施形態に係る判定装置の構成例を示す図である。

【図 1 4】図 1 4 は、判定装置の機能を実現するコンピュータの一例を示すハードウェア構成図である。

【発明を実施するための形態】

【0010】

以下に、本願に係る判定装置、判定方法及び判定プログラムを実施するための形態（以下、「実施形態」と呼ぶ）について図面を参照しつつ詳細に説明する。なお、この実施形態により本願に係る判定装置、判定方法及び判定プログラムが限定されるものではない。また、各実施形態は、処理内容を矛盾させない範囲で適宜組み合わせることが可能である。また、以下の各実施形態において同一の部位には同一の符号を付し、重複する説明は省略される。

10

【0011】

〔1. 第 1 の実施形態〕

〔1-1. 判定処理の一例〕

まず、図 1 を用いて、第 1 の実施形態に係る判定処理の一例について説明する。図 1 は、第 1 の実施形態に係る判定処理の一例を示す図である。図 1 では、本願に係る判定装置 100 によって、ユーザ端末 10 から送信される認証の要求に関する判定処理が行われる例を示す。

20

【0012】

図 1 に示す判定装置 100 は、ユーザ端末 10 の認証に関する判定を行うサーバ装置である。また、ユーザ端末 10 は、ユーザ U01 によって利用される情報処理端末である。図 1 では、ユーザ端末 10 は、例えばスマートフォン（Smartphone）である。

【0013】

判定装置 100 は、ユーザ端末 10 を利用するユーザ U01 の本人性の認証の要求を受信し、かかる要求に応答して、ユーザ端末 10 を認証する機能を有する。ユーザ端末 10 の認証とは、ユーザ端末 10 が間違いなくユーザ U01 によって操作されているという検証を通じたユーザ U01 の本人認証を示す。例えば、判定装置 100 は、ユーザ端末 10 が所定の制限が付されているサービス（アクセス制限付きのウェブサイト等）にアクセスしようとする場合に、ユーザ端末 10 の認証を行うことにより、かかるサイトへのアクセス制御を行う。

30

【0014】

判定装置 100 は、所定の認証手続きによって、ユーザ端末 10 の認証を行う。認証手続きでは、例えば、ユーザ端末 10 を利用するユーザ U01 から、ユーザ U01 本人であることを証明する情報を予め受け付け、認証の際には、登録済みの情報との照合を行う情報（以下、「認証情報」と表記する）の提示をユーザ端末 10 に求めるといった一連の手続きが行われる。例えば、判定装置 100 は、ユーザ U01 から事前に認証用の指紋データやパスワードの登録を受け付ける。そして、判定装置 100 は、認証の際には、認証情報として、ユーザ U01 に指紋データやパスワードの送信を求める。判定装置 100 は、登録済みの指紋データやパスワードと、送信された認証情報とが一致する場合に、ユーザ端末 10 を利用するユーザ U01 の本人性が確認できたものとして、ユーザ端末 10 を認証する。

40

【0015】

しかし、アクセス制限によって安全性が保たれる一方で、ユーザ U01 にとっては、サービスにアクセスを行う度に認証処理を求められるという、煩わしい処理が要求される。そこで、本願に係る判定装置 100 は、以下に説明する判定処理を行うことにより、ユーザ U01 の認証処理に対する手間を軽減させる。以下、図 1 を用いて、判定装置 100 が行う判定処理の一例の流れに沿って説明する。なお、図 1 の例において、判定装置 100 は、ユーザ U01 の本人性を確認する情報（例えば、ユーザ U01 の指紋データやパsw

50

ードなど)を予め受け付けているものとする。

【0016】

まず、判定装置100は、認証対象であるユーザ端末10から、判定処理に用いるコンテキスト(context)の登録を予め受け付ける(ステップS01)。判定装置100は、受け付けたコンテキストを記憶部120に記憶する。なお、実施形態において、コンテキストとは、ユーザ端末10が利用されている状況のことをいう。また、実施形態において、コンテキストを特定するための情報をコンテキスト情報という。コンテキスト情報には、例えば、ユーザ端末10自体のデバイス情報や、ユーザU01によってユーザ端末10が使用されている環境情報や、ユーザ端末10を所持するユーザU01が置かれている状態を示す情報や、ユーザU01およびユーザU01と関わりのある他のユーザに関する情報等が含まれる。なお、コンテキストの登録は、上述した、ユーザU01の本人性を確認する情報の登録と同時にも行われてもよい。

10

【0017】

図1に示す例では、ユーザ端末10は、コンテキストとして、「ユーザ端末10がユーザU01の自宅に所在」と、「ユーザ端末10と判定装置100との通信状態が確立」と、「ユーザ端末10とスピーカー20との通信状態が確立」という、3つのコンテキストの組み合わせを登録するものとする。ここで、スピーカー20は、ユーザU01の自宅に設置されている音響機器であり、所定の通信機能を有するものとする。具体的には、スピーカー20は、ユーザ端末10との近距離無線通信を確立させ、ユーザ端末10から送信される音声信号を音として出力する機能を有する。

20

【0018】

その後、判定装置100は、ユーザ端末10に対して所定の認証処理を行うものとする(ステップS02)。例えば、ユーザ端末10は、所定の認証処理(ユーザのログイン処理など)を有するサイトへアクセスし、アクセスの際に判定装置100から認証を受けるものとする。ステップS02における認証では、判定装置100は、ユーザ端末10から認証情報を受信し、登録済みの情報との一致を検証することで、ユーザ端末10を認証する。

【0019】

ユーザ端末10は、認証処理の後、ユーザ端末10のコンテキスト情報を定期的に判定装置100に送信する(ステップS03)。例えば、ユーザ端末10は、1分毎に、ユーザ端末10が検知する環境情報や、ユーザ端末10及びスピーカー20と判定装置100との通信状態に関する情報を判定装置100に送信する。具体的には、ユーザ端末10は、ステップS01で登録したコンテキストに関する情報として、「ユーザ端末10がユーザU01の自宅に所在」しているか否かを示す位置情報や、ユーザ端末10及びスピーカー20と、判定装置100との通信状態が確立しているか否かを示す通信情報を送信する。判定装置100は、送信されるコンテキスト情報を記憶部120に記憶する。

30

【0020】

その後、ユーザ端末10は、認証制限付きサイトへアクセスを要求する(ステップS04)。例えば、ユーザ端末10は、ステップS02の認証でアクセスが認められたサイトとは別のサイトへアクセスするものとする。アクセスの要求は、言い換えれば、判定装置100にユーザ端末10を認証することを求める認証の要求を示す。

40

【0021】

ここで、判定装置100は、記憶部120を参照し、ユーザ端末10のコンテキストの変化を検証する(ステップS05)。具体的には、判定装置100は、ステップS02の認証の時点でのコンテキスト情報と、ステップS03で定期的に取り得たコンテキスト情報と、ステップS04の認証の時点でのコンテキスト情報との変化を検証する。

【0022】

例えば、判定装置100は、ステップS02の認証の時点でのコンテキスト情報に基づき、ユーザ端末10のコンテキストとして、「ユーザ端末10がユーザU01の自宅に所在」と、「ユーザ端末10と判定装置100との通信状態が確立」と、「ユーザ端末10

50

とスピーカー 20 との通信状態が確立」という、3つのコンテキストの組み合わせが成立していると判定する。また、判定装置 100 は、ステップ S 0 3 及びステップ S 0 4 の時点でも、上記の3つのコンテキストの組み合わせが成立していると判定する。

【0023】

そして、判定装置 100 は、いずれのコンテキスト情報にも相違がないと判定した場合、すなわち、ステップ S 0 4 の時点においても予め登録を受け付けたコンテキストが成立している場合、ユーザ端末 10 はステップ S 0 2 の時点から変わらず、ユーザ U 0 1 によって操作されていると判定する。これにより、判定装置 100 は、ステップ S 0 4 での新たな認証を要しないと判定する(ステップ S 0 6)。言い換えれば、判定装置 100 は、ステップ S 0 4 の認証では、認証手続きを省いて、ユーザ端末 10 を認証する。そして、判定装置 100 は、ステップ S 0 4 で行われたアクセスの要求を承認する(ステップ S 0 7)。

10

【0024】

続いて、ユーザ U 0 1 が自宅を離れ、外出したとする(ステップ S 0 8)。この場合も、ユーザ端末 10 は、コンテキスト情報を定期的に判定装置 100 に送信し続ける(ステップ S 0 9)。

【0025】

そして、ユーザ端末 10 は、外出先において、認証制限付きサイトへアクセスを要求する(ステップ S 10)。判定装置 100 は、ユーザ端末 10 からアクセスの要求を受信した場合に、ユーザ端末 10 のコンテキストの変化を検証する(ステップ S 11)。具体的には、判定装置 100 は、ステップ S 0 2 ~ S 0 7 の時点でのコンテキスト情報と、ステップ S 0 9 で定期的に取得したコンテキスト情報と、ステップ S 10 の認証の時点でのコンテキスト情報との変化を検証する。

20

【0026】

そして、判定装置 100 は、ステップ S 0 2 ~ S 0 9 の時点でのコンテキスト情報と、ステップ S 10 の認証の時点でのコンテキスト情報とが変化していると判定する。具体的には、判定装置 100 は、ステップ S 10 の時点では、ステップ S 0 1 で登録されたコンテキストのうち、「ユーザ端末 10 が判定装置 100 との通信状態が確立」というコンテキストを示す情報は変わらず送信されているものの、「ユーザ端末 10 がユーザ U 0 1 の自宅に所在」及び「ユーザ端末 10 とスピーカー 20 との通信状態が確立」というコンテキストを示す情報は送信されていないことから、ユーザ端末 10 のコンテキストが変化したと判定する。

30

【0027】

そして、判定装置 100 は、ステップ S 10 の要求に対して、新たな認証を要すると判定する(ステップ S 12)。すなわち、判定装置 100 は、ユーザ端末 10 のコンテキストが変化していることにより、ユーザ端末 10 が変わらずユーザ U 0 1 によって操作されているという確認がとれないことから、再度の認証によりユーザ端末 10 を認証することを要すると判定し、認証を要求する(ステップ S 13)。

【0028】

この場合、判定装置 100 は、ユーザ端末 10 から送信されたアクセス要求に対して、通常の認証手続きを求める。すなわち、判定装置 100 は、ユーザ U 0 1 の本人性を確認する情報である認証情報の送信をユーザ端末 10 に要求する。要求に回答して、ユーザ端末 10 は、認証情報を送信する(ステップ S 14)。判定装置 100 は、認証情報の一致を判定し、ユーザ端末 10 を認証する。すなわち、判定装置 100 は、ステップ S 10 におけるアクセス要求を承認する(ステップ S 15)。

40

【0029】

このように、第1の実施形態に係る判定装置 100 は、ユーザ端末 10 を利用するユーザ U 0 1 の本人性の認証の要求を受信するとともに、ユーザ端末 10 のコンテキストを示す情報であるコンテキスト情報を取得する。そして、判定装置 100 は、取得されたコンテキスト情報に基づいて、ユーザ端末 10 から要求された認証に関する判定を行う。例え

50

ば、判定装置 100 は、以前に認証が行われたユーザ端末 10 に対して、再度の認証手続きを要求するか否かを判定する。

【0030】

すなわち、判定装置 100 は、認証の対象であるユーザ端末 10 のコンテキストに基づいて、認証手続きを行うか否かの判定を行う。例えば、判定装置 100 は、ユーザ端末 10 から予め受け付けたコンテキストと、認証時におけるコンテキストとが相違ない場合、新たな認証手続きを要しないと判定する。これにより、判定装置 100 は、新たな認証手続きを省いて、ユーザ端末 10 の認証を行うことができる。このように、判定装置 100 によれば、ユーザ U01 は、コンテキストから一定の信頼が得られる場合には、パスワード入力などの認証手続きを要求されることなく、認証を行わせることができる。このため、ユーザ U01 は、日常生活において実現され易いコンテキスト等を予め登録しておくことにより、認証に関する手間を軽減させることができる。結果として、判定装置 100 は、利便性に優れた本人認証を行うことができる。

10

【0031】

〔1-2. 判定処理システムの構成〕

次に、図 2 を用いて、第 1 の実施形態に係る判定装置 100 が含まれる判定処理システム 1 の構成について説明する。図 2 は、第 1 の実施形態に係る判定処理システム 1 の構成例を示す図である。図 2 に例示するように、第 1 の実施形態に係る判定処理システム 1 には、ユーザ端末 10 と、ユーザが利用する装置と、判定装置 100 と、ウェブサーバ 60 とが含まれる。なお、図 2 に示すように、ユーザから利用される装置には、スピーカ 20 等が含まれる。これらの各種装置は、ネットワーク N を介して、有線又は無線により通信可能に接続される。

20

【0032】

ユーザ端末 10 は、デスクトップ型 PC (Personal Computer) や、ノート型 PC や、タブレット端末や、スマートフォンを含む携帯電話機、PDA (Personal Digital Assistant) 等の情報処理端末である。また、ユーザ端末 10 には、眼鏡型や時計型の情報処理端末であるウェアラブルデバイス (wearable device) も含まれる。さらに、ユーザ端末 10 には、情報処理機能を有する種々のスマート機器が含まれてもよい。例えば、ユーザ端末 10 には、TV (Television) や冷蔵庫、掃除機などのスマート家電や、自動車などのスマートビークル (Smart vehicle) や、ドローン (drone)、家庭用ロボットなどが含まれてもよい。

30

【0033】

ユーザ端末 10 は、ユーザによる操作や、ユーザ端末 10 が有する機能に応じて、ユーザ端末 10 のコンテキストを示すコンテキスト情報を取得する。例えば、ユーザ端末 10 は、内蔵された各種センサにより、位置、加速度、温度、重力、回転 (角速度)、照度、地磁気、圧力、近接、湿度、回転ベクトルといった、種々の物理量をコンテキスト情報として取得する。また、ユーザ端末 10 は、内蔵する通信機能を利用して、各種装置との接続状況等のコンテキスト情報を取得する。

【0034】

ユーザが利用する装置とは、ユーザ端末 10 の他に、ユーザが利用する機器の総称を示す。例えば、ユーザが利用する装置は、上述したユーザ端末 10 と同様、情報処理機能を有する種々のスマート機器である。第 1 の実施形態では、ユーザによって利用される装置は、例えばスピーカ 20 である。これらの装置は、例えば、ユーザ端末 10 のコンテキストを表すために利用される。

40

【0035】

判定装置 100 は、上述のように、ユーザ端末 10 のコンテキスト情報を取得し、取得されたコンテキスト情報に基づいて、ユーザ端末 10 の認証に関する判定を行うサーバ装置である。

【0036】

ウェブサーバ 60 は、ユーザ端末 10 からアクセスされた場合に、各種ウェブページを

50

提供するサーバ装置である。ウェブサーバ60は、例えば、ニュースサイト、天気予報サイト、ショッピングサイト、ファイナンス(株値)サイト、路線検索サイト、地図提供サイト、旅行サイト、飲食店紹介サイト、ウェブブログなどに関する各種ウェブページや、アプリで表示されるコンテンツ等を提供する。

【0037】

ウェブサーバ60は、サービスの提供にあたり、ユーザの本人認証を要求する場合がある。例えば、ウェブサーバ60が決済サービスを提供する際に、ユーザ端末10を利用しているユーザが間違いなくユーザU01本人であると認証できないときには、ウェブサーバ60は、ユーザ端末10による決済サービスの実行を制限することができる。ウェブサーバ60は、ユーザ端末10に関する認証を行う判定装置100による認証結果に応じて、ユーザ端末10からのアクセスを認めるか否かを判定する。例えば、判定装置100がユーザ端末10を認証した場合、ウェブサーバ60は、ユーザ端末10による認証制限付きサイトへのアクセスを承認する。

10

【0038】

すなわち、ウェブサーバ60は、判定装置100がユーザU01を認証したことを示す情報を判定装置100から受信した場合に、ユーザ端末10を利用しているユーザがユーザU01であると信頼する。ユーザ端末10の認証後は、ウェブサーバ60は、ユーザ端末10による決済処理など、本人認証後でなければ許可しないような操作について受け付けることができる。

【0039】

20

〔1-3. 判定装置の構成〕

次に、図3を用いて、第1の実施形態に係る判定装置100の構成について説明する。図3は、第1の実施形態に係る判定装置100の構成例を示す図である。図3に示すように、判定装置100は、通信部110と、記憶部120と、制御部130とを有する。なお、判定装置100は、判定装置100を利用する管理者等から各種操作を受け付ける入力部(例えば、キーボードやマウス等)や、各種情報を表示するための表示部(例えば、液晶ディスプレイ等)を有してもよい。

【0040】

(通信部110について)

通信部110は、例えば、NIC(Network Interface Card)等によって実現される。かかる通信部110は、ネットワークNと有線又は無線で接続され、ネットワークNを介して、ユーザ端末10等との間で情報の送受信を行う。

30

【0041】

(記憶部120について)

記憶部120は、例えば、RAM、フラッシュメモリ(Flash Memory)等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。記憶部120は、登録情報記憶部121と、認証情報記憶部122と、認証ログ記憶部123と、コンテキストログ記憶部124とを有する。

【0042】

(登録情報記憶部121について)

40

登録情報記憶部121は、ユーザ端末10によって登録された登録情報に関する情報を記憶する。ここで、図4に、第1の実施形態に係る登録情報記憶部121の一例を示す。図4は、第1の実施形態に係る登録情報記憶部121の一例を示す図である。図4に示した例では、登録情報記憶部121は、「ユーザID」、「登録ID」、「コンテキスト」といった項目を有する。

【0043】

「ユーザID」は、コンテキストを登録するユーザを識別する識別情報である。なお、ユーザIDは、ユーザ端末10を操作するユーザの参照符号と一致するものとする。例えば、ユーザID「U01」によって識別されるユーザは、ユーザU01を示す。また、ユーザIDは、ユーザIDによって識別されるユーザが使用する端末装置を識別する情報と

50

して扱われてもよい。

【0044】

「登録ID」は、登録されたコンテキストを識別する情報である。「コンテキスト」は、予めユーザから登録されるコンテキストであり、上述した判定処理に用いられるコンテキストを示す。例えば、コンテキストは、ユーザ端末10が所在する位置を示す位置情報や、ユーザ端末10と判定装置100とが通信状態であるという通信情報によって特定される。

【0045】

すなわち、図4では、ユーザID「U01」で識別されるユーザU01は、登録ID「R01」で識別されるコンテキストとして、「位置情報G01」、「ユーザ端末10と通信」、「ユーザ端末10とスピーカー20との通信」といったコンテキストを登録していることを示している。

10

【0046】

なお、図4の例において、「位置情報」は、ユーザ端末10の位置情報を示しており、「位置情報」が示す値に「G01」といった概念的な情報が格納される例を示したが、実際には、位置情報としては、「緯度及び経度」や「住所（例えば、都道府県や市区町村）」等を示す情報が記憶される。例えば、位置情報G01は、ユーザU01の自宅を示す位置情報であるものとする。ユーザ端末10は、例えば、GPS（Global Positioning System）等を利用して位置情報をコンテキスト情報として取得する。

【0047】

20

また、「通信」は、インターネット等の広域ネットワークのみならず、外部のネットワーク機器等を介さずにユーザ端末10とスピーカー20との間のみで成立する近距離通信（例えば、Bluetooth（登録商標）などによる通信の確立）であってもよい。

【0048】

（認証情報記憶部122について）

認証情報記憶部122は、判定装置100が行う認証に関する情報を記憶する。ここで、図5に、第1の実施形態に係る認証情報記憶部122の一例を示す。図5は、第1の実施形態に係る認証情報記憶部122の一例を示す図である。図5に示した例では、認証情報記憶部122は、「ユーザID」、「認証手段」、「正解データ」といった項目を有する。

30

【0049】

「ユーザID」は、図4で示した同一の項目に対応する。「認証手段」は、ユーザの認証に用いられる認証の手段を示す。例えば、認証手段は、指紋や、パスワードや、音声や、虹彩や、顔認識等である。「正解データ」は、認証手段に対応して、ユーザの本人性を認証するために用いられる正解データを示す。図5では、「正解データ」が示す値に、「X01」といった概念的な情報が格納される例を示したが、実際には、正解データとして、ユーザの指紋データや、パスワードとなる文字列や、音声の声紋情報等が記憶される。

【0050】

すなわち、図5では、判定装置100が認証する対象のユーザであって、ユーザID「U01」で識別されるユーザU01は、認証手段として、「指紋」、「パスワード」、「音声」を登録しており、それぞれの正解データは、「X01」、「X02」、「X03」である例を示している。なお、図5での図示は省略したが、ユーザU01は、例えば、利用するサイト毎に認証手段を登録してもよい。例えば、ユーザU01は、銀行のサイトで認証を行う場合には「指紋」を認証情報として利用し、他のサイトで認証を行う場合には「パスワード」を認証情報として利用する等の設定を行ってもよい。この場合、判定装置100は、かかる設定を認証情報記憶部122に記憶する。

40

【0051】

（認証ログ記憶部123について）

認証ログ記憶部123は、判定装置100が行う認証に関するログを記憶する。ここで、図6に、第1の実施形態に係る認証ログ記憶部123の一例を示す。図6は、第1の実

50

施形態に係る認証ログ記憶部 1 2 3 の一例を示す図である。図 6 に示した例では、認証ログ記憶部 1 2 3 は、「ユーザ ID」、「認証日時」、「認証手段」といった項目を有する。

【 0 0 5 2 】

「ユーザ ID」は、図 4 で示した同一の項目に対応する。「認証日時」は、認証が行われた日時を示す。「認証手段」は、認証で用いられた認証手段を示す。

【 0 0 5 3 】

すなわち、図 6 では、ユーザ ID 「U 0 1」で識別されるユーザ U 0 1 に対して、「2015 年 1 1 月 1 日 7 時」に、「指紋」を認証手段として認証が行われたことを示している。また、「2015 年 1 1 月 1 日 7 時 10 分」には、「登録データ」を認証手段として認証が行われたことを示している。「登録データ」とは、登録情報記憶部 1 2 1 に登録されたコンテキストを示している。すなわち、ユーザ U 0 1 は、「2015 年 1 1 月 1 日 7 時 10 分」の認証時には、通常の認証手続きによる認証がスキップされ、登録されたコンテキストによって認証されている例を示している。

【 0 0 5 4 】

なお、認証ログ記憶部 1 2 3 には、認証が行われた際のユーザ端末 1 0 のコンテキスト情報が、認証に関する情報と対応付けられて記憶されてもよい。

【 0 0 5 5 】

(コンテキストログ記憶部 1 2 4 について)

コンテキストログ記憶部 1 2 4 は、判定装置 1 0 0 が取得したコンテキストに関するログを記憶する。ここで、図 7 に、第 1 の実施形態に係るコンテキストログ記憶部 1 2 4 の一例を示す。図 7 は、第 1 の実施形態に係るコンテキストログ記憶部 1 2 4 の一例を示す図である。図 7 に示した例では、コンテキストログ記憶部 1 2 4 は、「ユーザ ID」、「取得日時」、「コンテキスト情報」といった項目を有する。

【 0 0 5 6 】

「ユーザ ID」は、図 4 で示した同一の項目に対応する。「取得日時」は、コンテキスト情報が取得された日時を示す。

【 0 0 5 7 】

「コンテキスト情報」は、ユーザが利用する端末装置のコンテキストを示すための各種情報を示す。コンテキスト情報は、端末装置の利用状況を示す情報であるため、種々の情報が含まれる。図 7 に示した一例では、コンテキストログ記憶部 1 2 4 は、予めユーザから登録されたコンテキストに関して、その登録されたコンテキストが取得されたか否かを示す情報を記憶するものとする。具体的には、図 7 では、図 4 に示した登録情報のうち、登録 ID 「R 0 1」で示されるコンテキストに関するコンテキスト情報のログが記憶されている例を示す。

【 0 0 5 8 】

例えば、コンテキスト情報には、「取得情報」と「正否」といった小項目が含まれる。「取得情報」は、登録 ID 「R 0 1」で示されるコンテキストに関するコンテキスト情報が対応する。例えば、図 7 に示す例では、取得情報として、「位置情報 G 0 1」が取得されたか否かの正否が記憶される。同様に、取得情報として、「ユーザ端末 1 0 (と、判定装置 1 0 0 との) 通信」や、「スピーカー 2 0 (と、ユーザ端末 1 0 との) 通信」が取得されたか否かの正否が記憶される。

【 0 0 5 9 】

例えば、図 7 では、「2015 年 1 1 月 1 日 7 : 0 0」におけるコンテキスト情報として、「位置情報 G 0 1」が取得されたため、その正否は「正 (1)」であることが記憶される。同様に、「ユーザ端末 1 0」において「通信あり」が取得されたため、その正否は「正 (1)」であることが記憶される。同様に、「スピーカー 2 0」において「通信あり」が取得されたため、その正否は「正 (1)」であることが記憶される。

【 0 0 6 0 】

一方で、「2015 年 1 1 月 1 日 9 : 0 0」におけるコンテキスト情報として、「位

10

20

30

40

50

置情報 G 0 3」が取得され、登録されたコンテキストを示す「位置情報 G 0 1」と相違している。このため、その正否には「否(0)」が記憶される。同様に、「スピーカー 2 0」において「通信なし」が取得されたため、その正否は「否(0)」が記憶される。このことは、ユーザ U 0 1 が自宅(位置情報 G 0 1 で示される)から外出し、ユーザ端末 1 0 とスピーカー 2 0 との通信も途絶えたことを示している。なお、「ユーザ端末 1 0」は、変わらず判定装置 1 0 0 との通信を保っているため、「通信あり」が取得され、その正否は「正(1)」が記憶される。

【 0 0 6 1 】

このように、コンテキストログ記憶部 1 2 4 では、ユーザ端末 1 0 のコンテキストを示すコンテキスト情報を記憶するとともに、登録されたコンテキストを満たしているか否かの情報がログとして記憶される。図 7 の一例では、登録 ID 「R 0 1」で示されるコンテキストに関する情報を例として示したが、コンテキストログ記憶部 1 2 4 には、登録 ID 「R 0 2」で示されるコンテキストに関する情報も同時に記憶されているものとする。

【 0 0 6 2 】

(制御部 1 3 0 について)

制御部 1 3 0 は、例えば、CPU (Central Processing Unit) や MPU (Micro Processing Unit) 等によって、判定装置 1 0 0 内部の記憶装置に記憶されている各種プログラムが RAM (Random Access Memory) を作業領域として実行されることにより実現される。また、制御部 1 3 0 は、例えば、ASIC (Application Specific Integrated Circuit) や FPGA (Field Programmable Gate Array) 等の集積回路により実現

【 0 0 6 3 】

図 3 に示すように、制御部 1 3 0 は、登録部 1 3 1 と、受信部 1 3 2 と、認証部 1 3 3 と、取得部 1 3 4 と、判定部 1 3 5 と、送信部 1 3 6 とを有し、以下に説明する情報処理の機能や作用を実現または実行する。なお、制御部 1 3 0 の内部構成は、図 3 に示した構成に限られず、後述する情報処理を行う構成であれば他の構成であってもよい。また、制御部 1 3 0 が有する各処理部の接続関係は、図 3 に示した接続関係に限られず、他の接続関係であってもよい。

【 0 0 6 4 】

(登録部 1 3 1 について)

登録部 1 3 1 は、ユーザ端末 1 0 が認証される際のユーザ端末 1 0 のコンテキストについて登録を受け付ける。例えば、登録部 1 3 1 は、ユーザ端末 1 0 を利用するユーザ U 0 1 から、認証を行う際に頻繁に観測されるコンテキストについて、予め登録を受け付ける。登録部 1 3 1 が受け付けたコンテキストは、判定部 1 3 5 による判定処理に用いられ、所定の条件下において、ユーザ端末 1 0 に要求される認証手続きがスキップされる。このように、登録部 1 3 1 は、予めコンテキストの登録を行うことにより、その後の認証処理における利便性を向上させることができる。

【 0 0 6 5 】

登録部 1 3 1 は、受け付けたコンテキストを登録情報記憶部 1 2 1 に記憶する。また、登録部 1 3 1 は、既にコンテキストを登録したユーザから、登録されたコンテキストの変更や更新を受け付けてもよい。

【 0 0 6 6 】

(受信部 1 3 2 について)

受信部 1 3 2 は、各種情報を受信する。例えば、受信部 1 3 2 は、ユーザ端末 1 0 から送信される各種要求を受信する。具体的には、受信部 1 3 2 は、所定の制限付きサイトへのアクセス要求をユーザ端末 1 0 から受信する。また、受信部 1 3 2 は、ユーザ端末 1 0 の認証の要求を受信する。また、受信部 1 3 2 は、認証手続きにおいて、ユーザ端末 1 0 から送信される認証情報を受信する。

【 0 0 6 7 】

上記の処理において、受信部 1 3 2 は、所定の制限付きサイトへのアクセス要求や、ユ

10

20

30

40

50

ーザ端末10の認証の要求を、ウェブサーバ60を経由して受信してもよい。すなわち、ユーザ端末10がウェブサーバ60の管理するサイトへアクセスした場合、ウェブサーバ60は、アクセス要求があった旨、また、アクセスを承認するためにユーザ端末10を認証することを要する旨を判定装置100に送信する。受信部132は、ウェブサーバ60から送信された要求を受信し、受信した要求に関する情報について、適宜制御部130の各処理部に送る。

【0068】

また、受信部132は、認証において用いられる認証手段や、認証手段に対応した正解データを受信する。受信部132は、受信した情報を認証情報記憶部122に記憶する。

【0069】

(認証部133について)

認証部133は、ユーザ端末10を利用するユーザU01の本人性を認証する。具体的には、認証部133は、認証情報記憶部122に記憶された情報に基づいて、認証対象となるユーザ端末10に対する認証手続きを行う。すなわち、認証部133は、ユーザ端末10から認証情報を受け付け、受け付けた認証情報と正解データとの一致を検証する。そして、認証部133は、受け付けた認証情報と正解データとの一致が検証された場合に、ユーザ端末10を利用するユーザU01の本人性が確認できたと判定し、ユーザ端末10を認証する。

【0070】

例えば、認証部133は、ユーザ端末10が所定のサービスを利用するために制限付きサイトにアクセスする場合や、サービス利用のためのログイン処理を行う場合等に、ユーザ端末10に対する認証処理を実行する。

【0071】

また、認証部133は、後述する判定部135による判定が行われたときには、判定部135による判定に応じて、認証手続きを行うか否かを判定する。具体的には、認証部133は、判定部135によって認証の要求に対する認証手続きを行うことを要すると判定された場合には、ユーザ端末10に対する認証手続きを行う。一方、認証部133は、判定部135によって認証の要求に対する認証手続きを行うことを要しないと判定された場合には、認証手続きを省いて、ユーザ端末10を認証する。この場合、認証部133は、ユーザ端末10から送信される認証情報ではなく、ユーザ端末10のコンテキストに基づいてユーザ端末10を認証する。

【0072】

(取得部134について)

取得部134は、各種情報を取得する。例えば、取得部134は、ユーザ端末10のコンテキストを示す情報であるコンテキスト情報を取得する。具体的には、取得部134は、コンテキスト情報として、ユーザ端末10によって検知される環境情報や、ユーザ端末10自体のデバイス情報、ユーザ端末10を利用するユーザU01に関するユーザ情報、ユーザ端末10と通信する外部装置に関する情報等を取得する。

【0073】

取得部134は、ユーザ端末10によって検知されるコンテキスト情報として、例えば、ユーザ端末10が所在する位置を示す位置情報、ユーザ端末10の周囲の温度、湿度情報、環境光の強さを示す光情報、ユーザ端末10の周囲の騒音レベルを示す音情報等を取得する。また、取得部134は、ユーザ端末10が備えるカメラで撮影された写真や映像に基づいて、ユーザ端末10の周囲の環境情報を取得してもよい。例えば、取得部134は、カメラで撮影された画像情報や、画像情報に含まれる位置情報、撮影された日時等に基づいて、ユーザ端末10の周囲の環境情報を取得する。

【0074】

また、取得部134は、ユーザ端末10自体のデバイス情報として、ユーザ端末10のCPUや、OS(Operating System)、メモリ等に関する情報、アンテナ等のネットワーク機能、インストールされたソフトウェア、使用されるブラウザソフトウェア、対応す

10

20

30

40

50

る認証手段（例えば、指紋データを取得する機能や虹彩を取得する機能を備えているか否か）等の情報を取得する。

【0075】

また、取得部134は、ユーザ端末10の動作状況を取得してもよい。例えば、取得部134は、ユーザ端末10が起動状態にあるか否か、また、起動状態であれば、画面のON/OFFの状態や、ユーザ端末10が移動/静止している状態か等の情報を取得する。かかる情報は、例えば、ユーザ端末10にインストールされた所定のセンシング（sensing）機能を有するアプリによって取得され、ユーザ端末10内部に保持される。

【0076】

また、取得部134は、コンテキスト情報の取得対象となるユーザ、又は当該ユーザと関わりのある他のユーザに関する情報として、これらユーザの属性情報、現在の行動情報、ネットワーク上の行動履歴、興味関心、他のユーザとの関係（物理的に近くにいることや、同じ組織にいることや、ソーシャル的なつながりを有することなど）に関する情報を取得する。かかるユーザ情報は、例えば、ユーザ端末10内に記憶されたブラウザのログ等を参照することで取得される。

【0077】

また、取得部134は、ユーザ端末10と通信する外部装置に関する情報として、ユーザ端末10と相互の通信状態にある外部装置を識別する情報や、確立している通信の種類や周波数帯域等を取得する。

【0078】

取得部134は、ユーザ端末10から定期的にコンテキスト情報を受け付けることにより、上述した情報を取得する。また、取得部134は、ユーザ端末10からの送信によらず、所定時間ごとにユーザ端末10等と所定の通信を行い、ユーザ端末10内部に保持されたコンテキスト情報をクロール（crawl）することにより、コンテキスト情報を取得してもよい。取得部134は、取得した情報を認証ログ記憶部123や、コンテキストログ記憶部124に記憶する。

【0079】

（判定部135について）

判定部135は、取得部134によって取得されたコンテキスト情報に基づいて、ユーザ端末10から要求された認証に関する判定を行う。例えば、判定部135は、受信部132によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化に基づいて、受信部132によって受信された認証の要求に対する認証手続きを行うことを要するか否かを判定する。より具体的には、判定部135は、前回の認証の要求時に取得されたコンテキスト情報と、今回の認証の要求時に取得されたコンテキスト情報との変化に基づいて、今回の要求に対する認証手続きを行うことを要するか否かを判定する。

【0080】

判定部135は、コンテキスト情報の変化として、コンテキスト情報の存在そのものが変化するか、あるいは、コンテキスト情報が示す値が変化するか等を検証する。コンテキスト情報の存在そのものが変化するとは、例えば、「ユーザ端末10とスピーカー20との相互の通信が確立している」といったコンテキスト情報が、ある時点を境に観測されなくなったこと、すなわち、コンテキスト情報の「ある/なし」が変化すること等をいう。また、コンテキスト情報が示す値が変化するとは、例えば、「ユーザ端末10の位置情報はG01である」といったコンテキスト情報が、ある時点を境に、「ユーザ端末10の位置情報はG02である」といったコンテキスト情報に変化すること等をいう。

【0081】

判定部135は、コンテキスト情報の存在または値の変化について、所定の閾値を設定し、ユーザ端末10のコンテキスト情報の変化を判定する。すなわち、判定部135は、コンテキスト情報の変化率又は変化量に基づいて、今回の認証の要求に対する認証手続きを行うことを要するか否かを判定する。

10

20

30

40

50

【 0 0 8 2 】

例えば、判定部 1 3 5 は、前回の認証時において取得された数種類のコンテキスト情報を判定するものとする。この場合、判定部 1 3 5 は、数種類のコンテキスト情報のうち、いくつかの情報の存在が変化したかを示す変化量を判定する。また、判定部 1 3 5 は、コンテキスト情報が数値を示す情報である場合、その数値がどのくらいの割合だけ変化したかを示す変化率を判定する。例えば、判定部 1 3 5 は、判定対象とする数種類のコンテキスト情報のうち、一つだけが変化している場合には、ユーザ端末 1 0 のコンテキストに変化がないと判定してもよい。あるいは、判定部 1 3 5 は、取得された位置情報 G 0 1 が位置情報 G 0 2 に変化した場合であっても、位置情報 G 0 1 と位置情報 G 0 2 とがごく近い範囲を示す情報であれば、ユーザ端末 1 0 のコンテキストに変化がないと判定してもよい。なお、コンテキスト情報が変化したと判定する変化量や変化率の閾値については、例えば、処理の繰り返しによる既知の学習処理等を経て適宜設定されてもよいし、判定装置 1 0 0 の管理者等によって人為的に設定されてもよい。

10

【 0 0 8 3 】

そして、判定部 1 3 5 は、所定の閾値を超えてコンテキスト情報が変化したと判定した場合に、ユーザ端末 1 0 への新たな認証手続きを要すると判定する。一方で、判定部 1 3 5 は、所定の閾値を超えてコンテキスト情報が変化していないと判定した場合には、ユーザ端末 1 0 への新たな認証手続きを要しないと判定する。

【 0 0 8 4 】

また、判定部 1 3 5 は、前回の認証の要求時から今回の認証の要求時までを取得されたコンテキスト情報の変化のパターンに基づいて、今回の認証の要求に対する認証手続きを行うことを要するか否かを判定してもよい。例えば、判定部 1 3 5 は、定期的に取得部 1 3 4 によって取得されるコンテキストのログを参照する。そして、判定部 1 3 5 は、コンテキストのログの変化パターンに応じて、新たな認証手続きを要するか否かを判定する。例えば、判定部 1 3 5 は、ユーザ端末 1 0 とスピーカー 2 0 との通信が確立したり途絶えたりしているコンテキスト情報が取得された場合であっても、かかる変化を繰り返すのみで、前回の認証時と今回の認証時においてユーザ端末 1 0 のコンテキストに大きな変化がないと想定される場合には、新たな認証手続きを要しないと判定してもよい。一方で、判定部 1 3 5 は、前回の認証の要求時と今回の認証の要求時に取得されたコンテキスト情報が一致する場合であっても、その間に定期的に取得されるコンテキストログに、通常観測される変化とは異なる変化パターンが観測された場合などは、今回の認証においては、新たな認証手続きをユーザ端末 1 0 に要求すると判定してもよい。

20

30

【 0 0 8 5 】

また、判定部 1 3 5 は、上述のように、予め登録されたコンテキストに基づいて、判定を行ってもよい。すなわち、判定部 1 3 5 は、受信部 1 3 2 によって認証の要求が受信された場合に取得されたコンテキスト情報が、登録部 1 3 1 によって登録済みのコンテキストを示すものである場合には、当該認証の要求に対する認証手続きを行うことを要しないと判定してもよい。

【 0 0 8 6 】

(送信部 1 3 6 について)

送信部 1 3 6 は、各種情報を送信する。例えば、送信部 1 3 6 は、認証の要求を行ったユーザ端末 1 0 に対して、認証部 1 3 3 が行った認証処理の結果を送信する。例えば、認証部 1 3 3 がユーザ端末 1 0 を認証した場合、送信部 1 3 6 は、認証が成功し、所定のサイトへの接続が許可されたこと等を示す情報をユーザ端末 1 0 に送信する。

40

【 0 0 8 7 】

[1 - 4 . ユーザ端末の構成]

次に、図 8 を用いて、第 1 の実施形態に係るユーザ端末 1 0 の構成について説明する。図 8 は、第 1 の実施形態に係るユーザ端末 1 0 の構成例を示す図である。図 8 に示すように、ユーザ端末 1 0 は、通信部 1 1 と、入力部 1 2 と、表示部 1 3 と、検知部 1 4 と、記憶部 1 5 と、制御部 1 6 とを有する。

50

【 0 0 8 8 】

(通信部 1 1 について)

通信部 1 1 は、ネットワーク N と有線又は無線で接続され、スピーカー 2 0 や、判定装置 1 0 0 や、ウェブサーバ 6 0 との間で情報の送受信を行う。例えば、通信部 1 1 は、N I C 等によって実現される。

【 0 0 8 9 】

(入力部 1 2 及び表示部 1 3 について)

入力部 1 2 は、ユーザから各種操作を受け付ける入力装置である。例えば、入力部 1 2 は、ユーザ端末 1 0 に備えられた操作キー等によって実現される。表示部 1 3 は、各種情報を表示するための表示装置である。例えば、表示部 1 3 は、液晶ディスプレイ等によって実現される。なお、ユーザ端末 1 0 にタッチパネルが採用される場合には、入力部 1 2 の一部と表示部 1 3 とは一体化される。

10

【 0 0 9 0 】

(検知部 1 4 について)

検知部 1 4 は、ユーザ端末 1 0 に関する各種情報を検知する。具体的には、検知部 1 4 は、ユーザ端末 1 0 に対するユーザ U 0 1 の操作や、ユーザ端末 1 0 の所在する位置情報や、ユーザ端末 1 0 と接続されている機器に関する情報や、ユーザ端末 1 0 における環境等を検知する。図 8 に示す例では、検知部 1 4 は、操作検知部 1 4 1 と、位置検知部 1 4 2 と、外部装置検知部 1 4 3 と、環境検知部 1 4 4 とを有する。

【 0 0 9 1 】

20

(操作検知部 1 4 1 について)

操作検知部 1 4 1 は、ユーザ端末 1 0 に対するユーザ U 0 1 の操作を検知する。例えば、操作検知部 1 4 1 は、入力部 1 2 に入力された情報に基づいて、ユーザ U 0 1 の操作を検知する。すなわち、操作検知部 1 4 1 は、入力部 1 2 に画面をタッチする操作の入力があったことや、音声の入力があったこと等を検知する。また、操作検知部 1 4 1 は、ユーザ U 0 1 によって所定のアプリが起動されたことを検知してもよい。かかるアプリがユーザ端末 1 0 内の撮像装置を動作させるアプリである場合、操作検知部 1 4 1 は、ユーザ U 0 1 によって撮像機能が利用されていることを検知する。また、操作検知部 1 4 1 は、ユーザ端末 1 0 内に備えられた加速度センサやジャイロセンサ等で検知されたデータに基づき、ユーザ端末 1 0 自体が動かされているといった操作を検知してもよい。

30

【 0 0 9 2 】

(位置検知部 1 4 2 について)

位置検知部 1 4 2 は、ユーザ端末 1 0 の現在位置を検知する。具体的には、位置検知部 1 4 2 は、G P S 衛星から送出される電波を受信し、受信した電波に基づいてユーザ端末 1 0 の現在位置を示す位置情報 (例えば、緯度及び経度) を取得する。

【 0 0 9 3 】

位置検知部 1 4 2 は、種々の手法により位置情報を取得することができる。例えば、ユーザ端末 1 0 が駅改札や商店等で使用される非接触型 I C カードと同等の機能を備えている場合 (もしくは、ユーザ端末 1 0 が非接触型 I C カードの履歴を読み取る機能を備えている場合)、ユーザ端末 1 0 によって駅での乗車料金の決済等が行われた情報とともに、使用された位置が記録される。位置検知部 1 4 2 は、かかる情報を検知し、位置情報として取得する。また、位置検知部 1 4 2 は、ユーザ端末 1 0 が特定のアクセスポイントと通信を行う際には、アクセスポイントから取得可能な位置情報を検知してもよい。また、位置情報は、ユーザ端末 1 0 が備える光学式センサや、赤外線センサや、磁気センサ等によって取得されてもよい。

40

【 0 0 9 4 】

(外部装置検知部 1 4 3 について)

外部装置検知部 1 4 3 は、ユーザ端末 1 0 に接続される外部装置を検知する。例えば、外部装置検知部 1 4 3 は、外部装置との相互の通信パケットのやり取りなどに基づいて、外部装置を検知する。そして、外部装置検知部 1 4 3 は、検知した外部装置をユーザ端末

50

10と接続される端末として認識する。また、外部装置検知部143は、外部装置との接続の種類を検知してもよい。例えば、外部装置検知部143は、外部装置と有線で接続されているか、無線通信で接続されているかを検知する。また、外部装置検知部143は、無線通信で用いられている通信方式等を検知してもよい。また、外部装置検知部143は、外部装置が発する電波を検知する電波センサや、電磁波を検知する電磁波センサ等によって取得される情報に基づいて、外部装置を検知してもよい。

【0095】

(環境検知部144について)

環境検知部144は、ユーザ端末10における環境を検知する。環境検知部144は、ユーザ端末10に備えられた各種センサや機能を利用し、環境に関する情報を検知する。例えば、環境検知部144は、ユーザ端末10の周囲の音を収集するマイクロフォンや、ユーザ端末10の周囲の照度を検知する照度センサや、ユーザ端末10の物理的な動きを検知する加速度センサ(又は、ジャイロセンサなど)や、ユーザ端末10の周囲の湿度を検知する湿度センサや、ユーザ端末10の所在位置における磁場を検知する地磁気センサ等を利用する。そして、環境検知部144は、各種センサを用いて、種々の情報を検知する。例えば、環境検知部144は、ユーザ端末10の周囲における騒音レベルや、ユーザ端末10の周囲がユーザU01の虹彩を撮像に適する照度であるか等を検知する。さらに、環境検知部144は、カメラで撮影された写真や映像に基づいて周囲の環境情報を検知してもよい。

【0096】

(記憶部15について)

記憶部15は、各種情報を記憶する。記憶部15は、例えば、RAM、フラッシュメモリ等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。例えば、記憶部15は、検知部14によって検知された各種情報を、検知された日時と対応付けて記憶する。

【0097】

(制御部16について)

制御部16は、例えば、CPUやMPU等によって、ユーザ端末10内部の記憶装置に記憶されている各種プログラムがRAMを作業領域として実行されることにより実現される。また、制御部16は、例えば、ASICやFPGA等の集積回路により実現される。

【0098】

図8に示すように、制御部16は、取得部161と、受信部162と、認証制御部163と、送信部164とを有し、以下に説明する情報処理の機能や作用を実現または実行する。なお、制御部16の内部構成は、図8に示した構成に限られず、後述する情報処理を行う構成であれば他の構成であってもよい。

【0099】

(取得部161について)

取得部161は、各種情報を取得する。例えば、取得部161は、検知部14を制御することにより、検知部14によって検知される各種情報を、ユーザ端末10のコンテキストを示すコンテキスト情報として取得する。具体的には、取得部161は、位置検知部142を制御することにより、ユーザ端末10の位置情報と、位置情報が検知された時間に対応する時間情報を取得する。

【0100】

取得部161は、所定の時間毎にコンテキスト情報を取得するようにしてもよい。例えば、取得部161は、定期的(1分毎や、3分毎や、5分毎等)に、上述した検知部14を制御すること等により、コンテキスト情報を取得する。なお、取得部161がコンテキスト情報を取得するタイミングは、判定装置100によって設定されてもよい。

【0101】

(受信部162について)

受信部162は、各種情報を受信する。例えば、受信部162は、判定装置100から

送信される認証情報の要求を受信する。受信部 162 は、受信した情報を、制御部 16 の各処理部へ送る。

【0102】

(認証制御部 163 について)

認証制御部 163 は、判定装置 100 に対する認証処理を制御する。例えば、認証制御部 163 は、判定装置 100 から認証情報の要求が送信された場合に、要求された認証情報に対応する認証手続きに関する処理を行う。例えば、認証制御部 163 は、要求された認証情報に対応する認証手段を特定する。そして、認証制御部 163 は、認証手段に応じた処理を実行する。

【0103】

例えば、認証制御部 163 は、要求された認証情報がユーザ U01 の指紋データである場合には、指紋の入力画面を表示部 13 に表示させる。そして、認証制御部 163 は、ユーザ U01 から指紋データの入力を受け付けた場合に、受け付けた指紋データを判定装置 100 に送信するための処理を行う。そして、認証制御部 163 は、送信するデータを送信部 164 に送る。

【0104】

(送信部 164 について)

送信部 164 は、取得部 161 によって取得されたコンテキスト情報を判定装置 100 に送信する。また、送信部 164 は、認証制御部 163 によって取得された認証情報を判定装置 100 に送信する。

【0105】

[1-5. 処理手順]

次に、図 9 を用いて、第 1 の実施形態に係る判定装置 100 による処理の手順について説明する。図 9 は、第 1 の実施形態に係る判定処理手順を示すフローチャートである。

【0106】

図 9 に示すように、認証部 133 は、ユーザ端末 10 を利用するユーザ U01 の認証を行う(ステップ S101)。その後、取得部 134 は、定期的にユーザ端末 10 のコンテキスト情報を取得する(ステップ S102)。

【0107】

そして、受信部 132 は、ユーザ端末 10 から新たな認証の要求を受信したか否かを判定する(ステップ S103)。新たな認証の要求を受信しない場合(ステップ S103; No)、取得部 134 は、コンテキスト情報を取得する処理を継続する。

【0108】

一方、新たな認証の要求を受信した場合(ステップ S103; Yes)、判定部 135 は、ユーザ端末 10 のコンテキストの変化を検出したか否かを判定する(ステップ S104)。コンテキストの変化を検出しない場合(ステップ S104; No)、判定部 135 は、ユーザ端末 10 に対する新たな認証手続きを要しないと判定する(ステップ S105)。

【0109】

一方、コンテキストの変化を検出した場合(ステップ S104; Yes)、判定部 135 は、ユーザ端末 10 に対する新たな認証手続きを要すると判定する(ステップ S106)。この場合には、認証部 133 は、ユーザ端末 10 に対して認証情報を要求する(ステップ S107)。そして、受信部 132 は、ユーザ端末 10 から送信される認証情報を受信する(ステップ S108)。

【0110】

ステップ S105 の場合には、認証部 133 は、取得されたコンテキスト情報により、ユーザ端末 10 を認証する(ステップ S109)。すなわち、認証部 133 は、ユーザ端末 10 から認証情報を送信させるといった認証手続きを省いて、ユーザ端末 10 を認証することができる。また、ステップ S108 の場合には、認証部 133 は、送信された認証情報との一致を判定することで、ユーザ端末 10 を認証する(ステップ S109)。

10

20

30

40

50

【0111】

なお、ステップS104におけるコンテキストの変化に関する判定は、予め登録されたコンテキストとの比較により行われてもよいし、前回の認証時からのコンテキストとの比較により行われてもよい。

【0112】

〔1-6. 判定処理のバリエーション〕

上記第1の実施形態では、例えば、ユーザ端末10が所定の制限付きサイトにアクセスする例を用いて、判定装置100が行う処理を説明した。そして、所定の判定がなされた際には、コンテキストそのものが認証情報となり、認証手続きを省いてユーザ端末10を認証する例を示した。このように、コンテキストそのものが認証情報となる処理について、様々な状況に応用されてもよい。この点について、図10を用いて説明する。

10

【0113】

図10は、第1の実施形態に係る判定処理の変形例を示す図である。図10では、ユーザU01、及び、端末装置30を利用するユーザU02という複数のユーザが、共有ファイル40を利用する例を示している。安全性の確保のため、共有ファイル40には所定のアクセス制限が付されており、限られたユーザしか閲覧することができないものとする。また、共有ファイル40へのアクセスは、判定装置100により制御されているものとする。

【0114】

図10の例において、ユーザU01は、判定装置100に予めコンテキストを登録する(ステップS21)。例えば、ユーザU01は、「ユーザ端末10と端末装置30との近距離通信が確立」していることをコンテキストとして登録する。

20

【0115】

ユーザU01は、判定装置100に対して認証の要求を行い、認証処理を実行させる(ステップS22)。これにより、ユーザU01は、判定装置100によって認証された状態となる。また、この際には、「ユーザ端末10と端末装置30との近距離通信が確立」というコンテキストが実現されているものとする。

【0116】

その後、ユーザ端末10は、コンテキスト情報を定期的に送信する(ステップS23)。所定時間後、ユーザU01は、共有ファイル40の閲覧を判定装置100に要求する(ステップS24)。判定装置100は、送信されていた情報に基づいて、コンテキストを検証する(ステップS25)。そして、判定装置100は、「ユーザ端末10と端末装置30との近距離通信が確立」というコンテキストが変わらず維持されていることを判定する。この場合、判定装置100は、登録されたコンテキストによりユーザU01の認証を行う(ステップS26)。これにより、ユーザU01は、共有ファイル40の閲覧要求が承認される(ステップS27)。

30

【0117】

その後、ユーザU02が移動し(ステップS28)、ユーザ端末10と端末装置30との近距離通信が途絶えたとする。ユーザ端末10は、このようなコンテキスト情報を定期的に判定装置100に送信する(ステップS29)。その後、ユーザ端末10は、共有ファイル40の閲覧を判定装置100に要求する(ステップS30)。

40

【0118】

判定装置100は、送信されていた情報に基づいて、コンテキストの変化を検出する(ステップS31)。すなわち、判定装置100は、「ユーザ端末10と端末装置30との近距離通信が確立」というコンテキストが変化していると判定する。この場合、判定装置100は、登録されたコンテキストでの認証ができないことを判定する(ステップS32)。これにより、ユーザU01は、共有ファイル40の閲覧要求が否認される(ステップS33)。

【0119】

図10の例のように、判定装置100は、コンテキストの変化について、認証手続きを

50

行うか否かといった判定のみならず、コンテキストの変化を認証情報として利用することができる。この場合、事前に判定装置100に登録されていた「ユーザ端末10と端末装置30との近距離通信が確立」というコンテキストが実現されない場合、ユーザU01は、共有ファイル40を利用することができなくなる。このように、判定装置100によれば、ある時点からのコンテキストの変化を判定することで、既に認めていたアクセス権を認めないようにすること等ができる。これにより、例えば特定のユーザによって共有ファイル40が改竄されること等を防止できるため、判定装置100は、より安全性に優れた認証をユーザに提供することができる。

【0120】

〔1-7.効果〕

上述してきたように、第1の実施形態に係る判定装置100は、受信部132と、取得部134と、判定部135とを有する。受信部132は、ユーザ端末10を利用するユーザU01の本人性の認証の要求を受信する。取得部134は、ユーザ端末10のコンテキストを示す情報であるコンテキスト情報を取得する。判定部135は、取得部134によって取得されたコンテキスト情報に基づいて、ユーザ端末10から要求された認証に関する判定を行う。

【0121】

このように、第1の実施形態に係る判定装置100は、認証の対象であるユーザ端末10のコンテキストに基づいて、認証手続きを行うか否かの判定を行う。例えば、判定装置100は、ユーザ端末10から予め受け付けたコンテキストと、認証時におけるコンテキストとが相違ない場合、新たな認証手続きを要しないと判定する。すなわち、判定装置100は、新たな認証手続きを省いてユーザ端末10を認証できるため、認証にかかる手間を省くことができ、ユーザの利便性を向上させる。

【0122】

また、判定部135は、受信部132によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化に基づいて、受信部132によって受信された認証の要求に対する認証手続きを行うことを要するか否かを判定する。

【0123】

このように、第1の実施形態に係る判定装置100は、過去に行われた認証の際（例えば、前回の認証時）のコンテキスト情報と、今回の認証時のコンテキスト情報の変化に基づいて判定処理を行う。これにより、判定装置100は、認証機会ごとのタイミングにおいてコンテキスト情報を検証することができるため、適切な判定処理を行うことができる。

【0124】

また、判定部135は、受信部132によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化率に基づいて、受信部132によって受信された認証の要求に対する認証手続きを行うことを要するか否かを判定する。

【0125】

このように、第1の実施形態に係る判定装置100は、今回の認証と要求時と、以前に行われた認証の要求時とのコンテキスト情報の変化率に基づいて判定処理を行う。これにより、判定装置100は、多少のコンテキスト情報の変化であれば、変わらず同一のユーザにユーザ端末10が利用されていると判定するなど、柔軟な処理を行うことができる。

【0126】

また、判定部135は、受信部132によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化量に基づいて、認証手続きを行うことを要するか否かを判定する。

【0127】

このように、第1の実施形態に係る判定装置100は、コンテキスト情報の変化量に基

10

20

30

40

50

づいて判定処理を行ってもよい。例えば、判定装置100は、コンテキスト情報が数値で示される場合には、数値の変化量に所定の閾値を設ける。そして、判定装置100は、閾値を超えたか否かを判定することで、ユーザ端末10（もしくは、ユーザU01）のコンテキストが変化したか否かを判定することができる。すなわち、判定装置100は、閾値の設定を調整すること等により、柔軟な判定処理を行うことができる。

【0128】

また、判定部135は、受信部132によって認証の要求が受信された際に取得されたコンテキスト情報と、以前に認証の要求が受信された際に取得されたコンテキスト情報との変化のパターンに基づいて、認証手続きを行うことを要するか否かを判定する。

【0129】

このように、第1の実施形態に係る判定装置100は、コンテキスト情報の変化のパターンに基づいて判定処理を行ってもよい。これにより、判定装置100は、例えば認証のタイミングで類似するコンテキストが観測されたとしても、他のユーザによってユーザ端末10が使用されている可能性があること等を判定し、認証手続きを要求することができる。このため、判定装置100は、より高い安全性を確保することができる。

【0130】

また、第1の実施形態に係る判定装置100は、ユーザ端末10が認証される際の当該ユーザ端末10のコンテキストについて登録を受け付ける登録部131をさらに備える。判定部135は、認証の要求が受信された場合に取得されたコンテキスト情報が、登録部131によって登録済みのコンテキストを示すものである場合には、当該認証の要求に対する認証手続きを行うことを要しないと判定する。

【0131】

このように、第1の実施形態に係る判定装置100は、予めコンテキストの登録を受け付け、登録されたコンテキストとの比較に基づいて、判定処理を行うことができる。ユーザは、認証が発生しやすいコンテキスト等を予め登録することで、登録されたコンテキストが観測された場合には、認証手続きを省略させることができる。これにより、判定装置100は、認証の利便性を向上させることができる。

【0132】

また、第1の実施形態に係る判定装置100は、判定部135によって認証の要求に対する認証手続きを行うことを要すると判定された場合には、ユーザ端末10に対する認証手続きを行い、判定部135によって認証の要求に対する認証手続きを行うことを要しないと判定された場合には、認証手続きを省いてユーザ端末10を認証する認証部133をさらに備える。

【0133】

このように、第1の実施形態に係る判定装置100は、判定処理に応じて、認証手続きを行うか否かを決定することができる。このため、判定装置100は、コンテキスト情報に信頼性がある場合には、認証手続きを省略することでユーザの利便性を高めることができ、また、コンテキスト情報に信頼性がない場合には、認証手続きを行うことで、認証の安全性を高めることができる。このように、判定装置100は、安全性を確保したうえで、利便性のよい認証処理を行うことができる。

【0134】

〔2. 第2の実施形態〕

上記第1の実施形態では、前回の認証時におけるコンテキスト情報と、新たな認証要求があった際のコンテキスト情報との変化に基づいて、認証手続きを要するか否かを判定する例を示した。また、判定処理において、ユーザから、予め認証に用いるコンテキストの登録を受け付け、登録されたコンテキストと、新たな認証要求があった際のコンテキストとの変化に基づいて、認証手続きを要するか否かを判定する例を示した。ここで、本願発明は、予め登録を受け付けるのではなく、判定に用いるコンテキストを推定して、判定処理を行ってもよい。この点について、第2の実施形態として説明する。なお、第1の実施形態において説明した事項と同様の事項については、説明を省略する。

10

20

30

40

50

【 0 1 3 5 】

〔 2 - 1 . 判定処理の一例 〕

まず、図 1 1 を用いて、第 2 の実施形態に係る判定処理の一例について説明する。図 1 1 は、第 2 の実施形態に係る判定処理の一例を示す図である。図 1 1 に示した判定装置 2 0 0 は、ユーザ端末 1 0 に関する所定のコンテキストを推定し、推定したコンテキストに基づいて、判定処理を行う。

【 0 1 3 6 】

図 1 1 に示すユーザ U 0 1 は、ユーザ端末 1 0 と、時計型端末 5 0 とを利用するユーザである。例えば、ユーザ U 0 1 は、ユーザ端末 1 0 を利用して、所定の制限付きサイトへアクセスする場合に、判定装置 2 0 0 に認証を要求する。ユーザ U 0 1 は、認証の要求と
10 ともに、ユーザ端末 1 0 に関するコンテキスト情報を送信する（ステップ S 4 1 ）。この場合、ユーザ端末 1 0 から送信されるコンテキスト情報は、例えば、「ユーザ端末 1 0 と時計型端末 5 0 との近距離通信が確立」等である。

【 0 1 3 7 】

判定装置 2 0 0 は、取得したコンテキストログを記憶部 1 2 0 に蓄積する（ステップ S 4 2 ）。そして、判定装置 2 0 0 は、所定の推定ルールに従い、認証で用いるコンテキストを推定する（ステップ S 4 3 ）。詳細は後述するが、判定装置 2 0 0 は、例えば、ユーザ端末 1 0 の認証を行う際には、高い確率で「ユーザ端末 1 0 と時計型端末 5 0 との近距離通信が確立」というコンテキスト情報を取得するものとする。また、判定装置 2 0 0 は、
20 所定回数の認証のうち、一定回数だけ同じコンテキスト情報が取得された場合に、かかるコンテキスト情報が示すコンテキストを、認証で用いるコンテキストとして推定する、といったルールを有するものとする。この場合、判定装置 2 0 0 は、認証で用いるコンテキストとして、「ユーザ端末 1 0 と時計型端末 5 0 との近距離通信が確立」を推定する。

【 0 1 3 8 】

その後、ユーザ端末 1 0 は、定期的にコンテキスト情報を判定装置 2 0 0 に送信する（ステップ S 4 4 ）。そして、あるタイミングで、ユーザ端末 1 0 は、認証制限付きサイトへアクセスを要求する（ステップ S 4 5 ）。このとき、判定装置 2 0 0 は、定期的に送信されたコンテキスト情報が示すコンテキスト、及び、アクセスが要求された際のコンテキスト情報が示すコンテキストと、推定されたコンテキストとの一致を検証する（ステップ S 4 6 ）。これは、第 1 の実施形態において、判定装置 1 0 0 が、予め登録されたコンテキスト情報や定期的に送信されたコンテンツ情報と、アクセスが要求された際のコンテキスト情報との一致を検証する処理と同様の処理といえる。
30

【 0 1 3 9 】

そして、判定装置 2 0 0 は、推定したコンテキストと、アクセスが要求された際のコンテキストとが一致すると判定する。すなわち、判定装置 2 0 0 は、通常、「ユーザ端末 1 0 と時計型端末 5 0 との近距離通信が確立」というコンテキスト情報とともに認証を行っているユーザ端末 1 0 から、今回においても同一のコンテキスト情報とともに認証の要求があったことから、高い確率で、ユーザ端末 1 0 は通常認証を行っているユーザ U 0 1 により操作されているものと判定する。

【 0 1 4 0 】

そして、判定装置 2 0 0 は、ステップ S 4 5 におけるアクセス要求に際して、新たな認証手続きを要しないと判定する（ステップ S 4 7 ）。そして、判定装置 2 0 0 は、新たな認証手続きを省いて、ユーザ端末 1 0 のアクセス要求を承認する（ステップ S 4 8 ）。
40

【 0 1 4 1 】

このように、第 2 の実施形態に係る判定装置 2 0 0 は、コンテキストの推定手段を有する。そして、判定装置 2 0 0 は、推定したコンテキストの変化に基づいて、ユーザ U 0 1 の認証に関する判定処理を行う。これにより、判定装置 2 0 0 は、予めユーザ U 0 1 からコンテキストの登録を受け付けることなく、コンテキストの一致を判定することができる。このため、判定装置 2 0 0 は、ユーザ U 0 1 に煩雑な処理を負わせることなく、適切な判定処理を行うことができる。
50

【 0 1 4 2 】

〔 2 - 2 . 判定装置の構成 〕

次に、図 1 2 を用いて、第 2 の実施形態に係る判定装置 2 0 0 の構成について説明する。図 1 2 は、第 2 の実施形態に係る判定装置 2 0 0 の構成例を示す図である。図 1 2 に示すように、判定装置 2 0 0 は、推定ルール記憶部 2 2 5 と、推定部 2 3 7 とを有する。

【 0 1 4 3 】

(推定ルール記憶部 2 2 5 について)

推定ルール記憶部 2 2 5 は、コンテキストを推定するルールを記憶する。例えば、推定ルール記憶部 2 2 5 は、コンテキストを推定するために用いられるコンテキストの類似度の算出等のルールを記憶する。また、推定ルール記憶部 2 2 5 には、例えば、所定回数以上のコンテキストログが蓄積された場合に、判定処理に用いるコンテキストとして推定するといったルールが記憶されてもよい。推定ルール記憶部 2 2 5 が記憶する推定ルールは、例えば、判定装置 2 0 0 の管理者等により人為的に設定され、記憶される。

10

【 0 1 4 4 】

(推定部 2 3 7 について)

推定部 2 3 7 は、取得部 1 3 4 によって取得されたコンテキスト情報に基づいて、ユーザ端末 1 0 が認証される際のユーザ端末 1 0 のコンテキストを推定する。この場合、判定部 1 3 5 は、認証の要求が受信された場合に取得されたコンテキスト情報が、推定部 2 3 7 によって推定されたコンテキストを示すものである場合には、当該認証の要求に対する認証手続きを行うことを要しないと判定してもよい。

20

【 0 1 4 5 】

推定部 2 3 7 は、推定ルール記憶部 2 2 5 に記憶された推定ルールに基づいて、判定処理に用いるコンテキストを推定する。また、推定部 2 3 7 は、取得部 1 3 4 によって取得されたコンテキスト情報から、ユーザ端末 1 0 のコンテキストが確定的に判断できない場合に、コンテキストを推定する処理を行ってもよい。

【 0 1 4 6 】

すなわち、推定部 2 3 7 は、コンテキストが確定的に判定できなかった場合に、得られている限りのコンテキスト情報を用いてコンテキストの類似度を算出する。具体的には、推定部 2 3 7 は、コンテキストログと認証ログ、及び、認証ログに含まれるコンテキスト情報を参照することにより、類似するコンテキストを導出する。そして、推定部 2 3 7 は、導出した類似するコンテキストを、コンテキスト情報が示すコンテキストと推定する。

30

【 0 1 4 7 】

第 1 の実施形態で説明したように、取得部 1 3 4 は、コンテキスト情報として多様な情報を取得する。その一方で、取得部 1 3 4 は、ユーザ端末 1 0 のコンテキストを確定させるコンテンツ情報が常に取得できるとは限らない。この場合、推定部 2 3 7 は、所定のルールに従い、取得できたコンテキスト情報に基づいて、コンテキストを推定する処理を行う。これにより、判定装置 2 0 0 は、比較的少ないコンテキスト情報しか取得されない状況であっても、適切に判定処理を行うことができる。

【 0 1 4 8 】

〔 2 - 3 . 効果 〕

上述してきたように、第 2 の実施形態に係る判定装置 2 0 0 は、取得部 1 3 4 によって取得されたコンテキスト情報に基づいて、ユーザ端末 1 0 が認証される際のユーザ端末 1 0 のコンテキストを推定する推定部 2 3 7 を備える。また、判定部 1 3 5 は、認証の要求が受信された場合に取得されたコンテキスト情報が、推定部 2 3 7 によって推定されたコンテキストを示すものである場合には、当該認証の要求に対する認証手続きを行うことを要しないと判定する。

40

【 0 1 4 9 】

このように、第 2 の実施形態に係る判定装置 2 0 0 は、判定処理で用いるコンテキストを推定することができる。例えば、判定装置 2 0 0 によれば、事前の登録処理を要せず、ユーザの認証時に発生しやすいコンテキストを推定し、推定されたコンテキストを用い

50

た判定処理を行う。これにより、ユーザは、事前の登録等の手間をかけずとも、コンテキストによって本人確認が確保されるような場合には、認証手続きを省略することができる。すなわち、判定装置 200 は、ユーザの利便性を向上させることができる。

【0150】

また、推定部 237 は、取得部 134 によって取得されたコンテキスト情報のログと、ユーザ端末 10 が以前に認証された際のコンテキスト情報のログとの類似度に基づいて、ユーザ端末 10 が認証される際のユーザ端末 10 のコンテキストを推定する。

【0151】

このように、第 2 の実施形態に係る判定装置 200 は、コンテキストのログに基づいてユーザ端末 10 のコンテキストを推定する。これにより、判定装置 200 は、コンテキストの推定精度を向上させ、適切な判定処理を行うことができる。

10

【0152】

〔3. 第 3 の実施形態〕

上記第 2 の実施形態では、判定装置 200 が推定部 237 と、推定ルール記憶部 225 とを備える例を示した。ここで、本願発明は、推定部 237 による推定処理に基づいて所定の学習を行い、推定ルールを学習により更新させていく学習部を備える構成であってもよい。この点について、第 3 の実施形態として説明する。なお、第 1 及び第 2 の実施形態において説明した事項と同様の事項については、説明を省略する。

【0153】

〔3-1. 判定装置の構成〕

図 13 を用いて、第 3 の実施形態に係る判定装置 300 の構成について説明する。図 13 は、第 3 の実施形態に係る判定装置 300 の構成例を示す図である。図 13 に示すように、判定装置 300 は、学習部 338 を有する。

20

【0154】

（学習部 338 について）

学習部 338 は、推定部 237 によってコンテキストが推定される際に用いられる推定ルールに関する学習を行う。第 2 の実施形態で説明したように、推定部 237 は、所定の推定ルールに基づき、例えば、コンテキスト情報のログと、ユーザ端末 10 が以前に認証された際のコンテキスト情報のログとの類似度に基づいて、ユーザ端末 10 が認証される際のコンテキストを推定する。学習部 338 は、推定部 237 による推定処理の結果に基づいて、推定ルールを更新することで、推定部 237 による推定処理の精度を向上させる。

30

【0155】

例えば、学習部 338 は、推定部 237 による推定処理ののちにコンテキストが判定された場合や、認証が行われる際に新たに取得されたコンテキスト情報に基づきコンテキストが判定された場合等に、コンテキストの推定の正否を学習する。そして、学習部 338 は、推定処理の結果の蓄積に応じて、コンテキストの推定ルールを学習する。例えば、学習部 338 は、特定のユーザであるユーザ U01 に関する推定処理が繰り返されることで蓄積される、ユーザ U01 に関するコンテキストの推定結果に基づき学習を行う。これにより、学習部 338 は、ユーザ U01 が常時利用する環境、デバイス情報などに基づく推定ルールを精度よく更新することができるため、推定処理の精度を高めることができる。また、学習部 338 は、ログとしての情報のないコンテキストにユーザ端末 10 が置かれた場合等に、過去の既存の推定ルールを用いて新たなルールを生成してもよい。

40

【0156】

また、推定部 237 は、学習部 338 によって学習された推定ルールであって、ユーザ端末 10 を利用するユーザ U01 以外のユーザに対応して学習された推定ルールに基づいて、ユーザ端末 10 のコンテキストを推定してもよい。すなわち、学習部 338 は、ユーザ U01 以外のユーザに関する学習の結果として得られた推定ルールを、メタルールとしてユーザ U01 に応用することができる。すなわち、学習部 338 は、学習の結果として生成された推定ルールを、特定のユーザのみならず、一般的なユーザにも応用することが

50

できる。これにより、推定部 237 は、よりコンテキストの推定精度を向上させることができる。なお、上記のような学習部 338 による学習処理は、既知の学習処理手法を組み合わせられてもよい。

【0157】

〔3-2. 効果〕

上述してきたように、第 3 の実施形態に係る判定装置 300 は、推定部 237 によってコンテキストが推定される際に用いられる推定ルールに関する学習を行う学習部 338 を備える。また、推定部 237 は、学習部 338 によって学習された推定ルールであって、ユーザ端末 10 を利用するユーザ U01 に対応して学習された推定ルールに基づいて、ユーザ端末 10 のコンテキストを推定する。

10

【0158】

このように、第 3 の実施形態に係る判定装置 300 は、推定処理に用いるルールを学習により得ることができる。このため、判定装置 300 は、処理が進むにつれて、精度の高いコンテキストの推定を行うことができるようになる。これにより、判定装置 300 は、ユーザに認証手続きを行わせるか否かの判定を適切に行うことができるため、ユーザの利便性を向上させることができる。

【0159】

また、推定部 237 は、学習部 338 によって学習された推定ルールであって、ユーザ端末 10 を利用するユーザ U01 以外のユーザに対応して学習された推定ルールに基づいて、ユーザ端末 10 のコンテキストを推定する。

20

【0160】

このように、第 3 の実施形態に係る判定装置 300 は、所定のユーザに対応して学習されたデータをメタデータとして他のユーザに応用することができる。このため、判定装置 300 は、未知のコンテキスト情報が取得された場合であっても、高い精度でコンテキストを推定することができるので、判定装置 300 が実行する各処理の精度を向上させることができる。

【0161】

〔4. 変形例〕

上述した判定装置 100 は、上記実施形態以外にも種々の異なる形態にて実施されてよい。そこで、以下では、判定装置 100 (判定装置 200、判定装置 300 も含む) の他の実施形態について説明する。

30

【0162】

〔4-1. 端末内での認証〕

上記実施形態では、判定装置 100 は、ユーザ端末 10 から送信される認証情報に基づいて、ユーザ端末 10 の認証を行う例を示した。ここで、ユーザ端末 10 は、認証情報自体を判定装置 100 に送信するのではなく、ユーザ端末 10 内部でユーザ U01 の認証を実行し、かかる結果のみを判定装置 100 に送信するような手法を採用してもよい。

【0163】

この場合、ユーザ端末 10 は、ユーザ U01 を認証するために正解データをユーザ端末 10 内部に記憶する。そして、ユーザ端末 10 は、認証手続きの要求を受け付けた際には、所定の認証手段により、ユーザ U01 を認証する。例えば、ユーザ端末 10 は、ユーザ U01 の指紋データの正解データを予め保持しておき、認証の際には、ユーザ U01 に対して指紋データの入力を求める。そして、ユーザ端末 10 は、ユーザ端末 10 内部で認証が完了したことを示した情報のみを判定装置 100 に送信する。これにより、ユーザ端末 10 は、指紋データやパスワード等の認証情報そのものをネットワーク上に送信することなく、認証手続きを行うことができる。これにより、判定装置 100 による処理は、より安全性が保たれる。

40

【0164】

〔4-2. 認証手段の判定〕

上記実施形態では、判定装置 100 は、新たな認証手続きを行うか否かを判定する点に

50

ついて説明した。ここで、判定装置100は、認証に関する判定として、新たな認証手続きを行うか否かを判定するのみならず、他の判定を行ってもよい。

【0165】

例えば、判定装置100は、認証手続きに用いる認証手段の判定を行ってもよい。具体的には、判定装置100は、ユーザ端末10が利用する各種センサから取得される情報に基づいてユーザ端末10のコンテキストを推測し、コンテキストに適した認証手段を判定するようにしてもよい。例えば、判定装置100は、ユーザ端末10の周辺の照度が虹彩を撮像するには不足している場合、虹彩による認証手段ではなく、他の認証手段を用いて認証手続きを行うことを判定する。あるいは、判定装置100は、ユーザ端末10の周辺の騒音レベルが、ユーザ端末10のマイクで音声を認識するには適していないほど高い場合、音声による認証手段ではなく、他の認証手段を用いて認証手続きを行うことを判定する。また、判定装置100は、認証ログやコンテキストログ等に基づいて、以前の認証時と類似するコンテキストにおいて認証が行われる場合には、以前の認証時に利用された認証手段による認証手続きを行うと判定してもよい。このように、判定装置100は、ユーザ端末10のコンテキスト情報に基づいて、最適な認証手段を判定する処理を行ってもよい。

10

【0166】

〔4-3. ユーザ端末の識別〕

上記第1の実施形態では、判定装置100は、複数のユーザ端末10の識別において、ユーザIDを取得する例を示した。ここで、判定装置100は、複数のユーザ端末10の識別に関して、必ずしも他の機器にも共通するようなグローバルな識別子を取得することを要さない。すなわち、判定装置100は、実行する処理において、ユーザ端末10を一意に識別することが可能な識別子を取得しさえすればよく、必ずしも永続的に定まる識別子を取得しなくてもよい。

20

【0167】

また、図1及び図10で示したような、ユーザ端末10と他の端末装置との通信など、1対1の通信によるコンテキスト情報に基づいて判定処理が行われる場合には、必ずしもユーザIDやデバイスIDを取得することを要さない。また、3台以上の機器同士の通信により判定処理が行われる場合であっても、判定装置100は、各々の端末を一意に識別することが可能な識別子を取得しさえすればよく、例えば、一時的な識別子を適宜発行するような形式で識別子を取得してもよい。

30

【0168】

〔4-4. ユーザ端末の構成〕

上記第1の実施形態では、ユーザ端末10の構成例について図8を用いて説明した。しかし、ユーザ端末10は、図8で例示した全ての処理部を備えることを必ずしも要しない。例えば、ユーザ端末10は、表示部13や検知部14を必ずしも備えていなくてもよい。また、ユーザ端末10は、2以上の機器に分離されて図8を示す構成が実現されてもよい。例えば、ユーザ端末10は、少なくとも検知部14を有する検知装置と、少なくとも通信部11を有する通信装置とが分離された構成を有する、2台以上の機器により実現されてもよい。

40

【0169】

〔4-5. サービスを提供する装置〕

上記実施形態では、ユーザ端末10がアクセスする認証制限付きサイトを提供する装置として、ウェブサーバ60を例示して説明した。しかし、このようなサービスを提供する装置は、ウェブサーバ60に限られない。例えば、サービスを提供する装置は、ウェブサービスに限らず、HTTP (Hypertext Transfer Protocol) ではない種類のプロトコルを扱うネットワークサービスや、IoT (Internet of Things) を扱う通信やアプリケーションを提供する装置であってもよい。すなわち、サービスを提供する装置は、判定装置100やユーザ端末10等と通信可能であり、判定装置100による判定処理や認証処理を利用する機能を有する装置であれば、ウェブサーバ60に限られず、どのような装

50

置によって実現されてもよい。

【0170】

〔4-6. 判定処理〕

上記実施形態では、判定装置100は、例えば図9に示したように、認証手続きを行うか否かの判定を行う例を示した。ここで、判定装置100は、認証手続きの強度に関する判定を行ってもよい。

【0171】

例えば、判定装置100は、コンテキスト情報の変化に基づいて、認証手続きの強度に関する判定を行う。認証強度の判定とは、例えば、多要素認証を実施するか否かなどの、認証処理において、本人確認のためにどのような認証情報を要求するかを判定する処理をいう。

10

【0172】

例えば、判定装置100は、通常、パスワードと指紋による多要素認証をユーザに要求しているとする。そして、判定装置100は、ユーザから取得されたコンテキスト情報の変化が所定の閾値以内である場合には、変わらず同一のユーザに端末が操作されている可能性が高いと判定し、認証手続きの強度を弱めることができる。具体的には、判定装置100は、パスワードによる認証手続きのみでユーザを認証する、といったように、認証処理の強度を変更することができる。あるいは、判定装置100は、以前の認証時と同一コンテキストが想定されるものの、認証自体が一年ぶりのユーザに関しては、パスワードと指紋に加えて、声紋を認証情報として要求するなど、認証処理の強度を強めることができる。

20

【0173】

また、判定装置100は、上記のような認証処理の強度の判定について、学習処理を行ってもよい。例えば、判定装置100は、所定のユーザに対して、「登録されたコンテキスト」と「三重の認証手段（例えば、パスワードと指紋と声紋）」とを認証処理の条件としている場合があるとする。そして、判定装置100は、当該ユーザが、例えば3か月間にわたり、「登録されたコンテキスト」と「三重の認証手段」とを用いて認証処理を行っているという履歴を取得する。判定装置100は、このような履歴に基づいて、当該ユーザの認証に関して、「三重の認証手段」であった認証手段を「二重の認証手段」や、「単独の認証手段」や、「認証手段なし」などに変更することができる。すなわち、判定装置100は、所定期間以上にわたり同一のコンテキストで認証処理が正確になされているユーザに関しては、信頼性が高いものと学習することで、認証手段を変更するなどの判定を適宜行うことができる。言い換えれば、判定装置100は、「毎日3か月間も同一コンテキストで認証を続けている」というコンテキスト自体を、判定要素として用いることができる。

30

【0174】

〔4-7. 取得処理〕

上記実施形態では、判定装置100は、定期的にコンテキスト情報をユーザ端末10から取得する例を示した。しかし、判定装置100は、必ずしも定期的にコンテキスト情報を取得し続けることを要さず、判定処理に用いるコンテキスト情報のみを取得するようにしてもよい。

40

【0175】

例えば、判定装置100は、今回の認証時と前回の認証時とにおけるコンテキスト情報の差異のみを判定要素としてもよい。この場合、判定装置100は、認証の間のユーザの行動に関わらず、認証時のタイミングで認証手続きの有無を判定してもよい。また、判定装置100は、第1の実施形態で説明したように、認証の間のコンテキスト情報を定期的に取得してもよい。この場合、判定装置100は、認証の間のコンテキスト情報の変化に応じて、認証時のタイミングで同一のコンテキストが観測されたとしても、認証手続きを要求するようにしてもよい。具体例を挙げて説明する。判定装置100は、会議室において、所定のユーザを認証したとする。その後、当該ユーザは、途中で一度会議室から退室

50

し、再び会議室にて認証を試みるとする。この場合、判定装置100は、ユーザに対して、認証手続きを要求してもよいし、しなくてもよい。このように、判定装置100は、ユーザが認証を試みるタイミングにおいて、同一のコンテキストが観測される場合であっても、認証を要求するか否かを判定することができる。これにより、判定装置100は、ユーザにとって煩雑になりすぎず、適切なレベルでのアクセスコントロールを実現することができる。

【0176】

〔5.ハードウェア構成〕

上述してきた各実施形態に係る判定装置は、例えば図14に示すような構成のコンピュータ1000によって実現される。以下、判定装置100を例に挙げて説明する。図14は、判定装置の機能を実現するコンピュータ1000の一例を示すハードウェア構成図である。コンピュータ1000は、CPU1100、RAM1200、ROM1300、HDD1400、通信インターフェイス(I/F)1500、入出力インターフェイス(I/F)1600、及びメディアインターフェイス(I/F)1700を有する。

10

【0177】

CPU1100は、ROM1300又はHDD1400に記憶されたプログラムに基づいて動作し、各部の制御を行う。ROM1300は、コンピュータ1000の起動時にCPU1100によって実行されるブートプログラムや、コンピュータ1000のハードウェアに依存するプログラム等を記憶する。

【0178】

HDD1400は、CPU1100によって実行されるプログラム、及び、かかるプログラムによって使用されるデータ等を記憶する。通信インターフェイス1500は、通信網500(図2に示したネットワークNに対応)を介して他の機器からデータを受信してCPU1100へ送り、CPU1100が生成したデータを、通信網500を介して他の機器へ送信する。

20

【0179】

CPU1100は、入出力インターフェイス1600を介して、ディスプレイやプリンタ等の出力装置、及び、キーボードやマウス等の入力装置を制御する。CPU1100は、入出力インターフェイス1600を介して、入力装置からデータを取得する。また、CPU1100は、入出力インターフェイス1600を介して生成したデータを出力装置へ出力する。

30

【0180】

メディアインターフェイス1700は、記録媒体1800に記憶されたプログラム又はデータを読み取り、RAM1200を介してCPU1100に提供する。CPU1100は、かかるプログラムを、メディアインターフェイス1700を介して記録媒体1800からRAM1200上にロードし、ロードしたプログラムを実行する。記録媒体1800は、例えばDVD(Digital Versatile Disc)、PD(Phase change rewritable Disk)等の光学記録媒体、MO(Magneto-Optical disk)等の光磁気記録媒体、テープ媒体、磁気記録媒体、または半導体メモリ等である。

【0181】

例えば、コンピュータ1000が第1の実施形態に係る判定装置100として機能する場合、コンピュータ1000のCPU1100は、RAM1200上にロードされたプログラムを実行することにより、制御部130の機能を実現する。また、HDD1400には、記憶部120内のデータが記憶される。コンピュータ1000のCPU1100は、これらのプログラムを記録媒体1800から読み取って実行するが、他の例として、他の装置から通信網500を介してこれらのプログラムを取得してもよい。

40

【0182】

〔6.その他〕

また、上記実施形態において説明した各処理のうち、自動的に行われるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行われるもの

50

として説明した処理の全部または一部を公知の方法で自動的に行うこともできる。この他、上記文書中や図面中で示した処理手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。例えば、各図に示した各種情報は、図示した情報に限られない。

【0183】

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。例えば、図3に示した認証部133と、取得部134とは統合されてもよい。また、例えば、記憶部120に記憶される情報は、ネットワークNを介して、外部に備えられた記憶装置に記憶されてもよい。

10

【0184】

また、例えば、上記実施形態では、判定装置100が、ユーザ端末10のコンテキスト情報を取得する取得処理と、認証の必要性を判定する判定処理と、ユーザを認証する認証処理とを行う例を示した。しかし、上述した判定装置100は、取得処理を行う取得装置と、判定処理を行う判定装置と、認証処理を行う認証装置に分離されてもよい。この場合、例えば、第1の実施形態に係る判定装置100による処理は、取得装置と、判定装置と、認証装置といった各装置を有する判定処理システム1によって実現される。

【0185】

また、上述してきた各実施形態及び変形例は、処理内容を矛盾させない範囲で適宜組み合わせることが可能である。

20

【0186】

以上、本願の実施形態のいくつかを図面に基づいて詳細に説明したが、これらは例示であり、発明の開示の欄に記載の態様を始めとして、当業者の知識に基づいて種々の変形、改良を施した他の形態で本発明を実施することが可能である。

【0187】

また、上述してきた「部(section、module、unit)」は、「手段」や「回路」などに読み替えることができる。例えば、取得部は、取得手段や取得回路に読み替えることができる。

30

【符号の説明】

【0188】

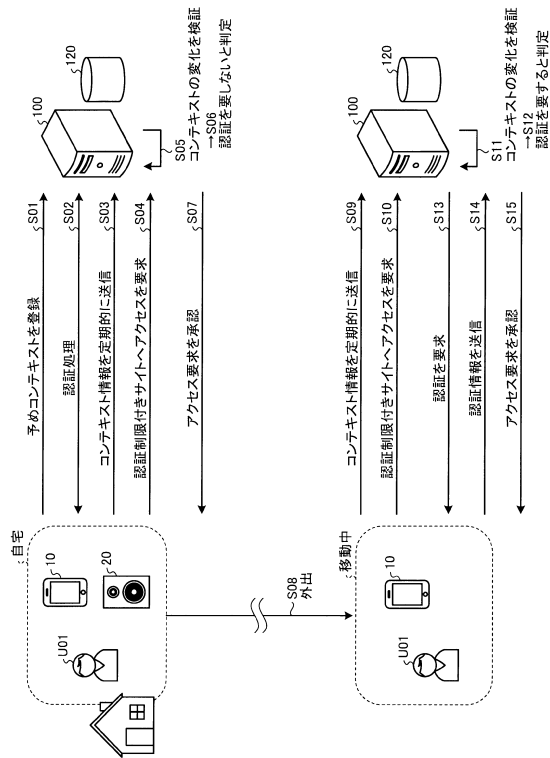
- 1 判定処理システム
- 10 ユーザ端末
- 20 スピーカー
- 30 端末装置
- 40 共有ファイル
- 50 時計型端末
- 60 ウェブサーバ
- 100 判定装置
- 110 通信部
- 120 記憶部
- 121 登録情報記憶部
- 122 認証情報記憶部
- 123 認証ログ記憶部
- 124 コンテキストログ記憶部
- 130 制御部
- 131 登録部
- 132 受信部
- 133 認証部

40

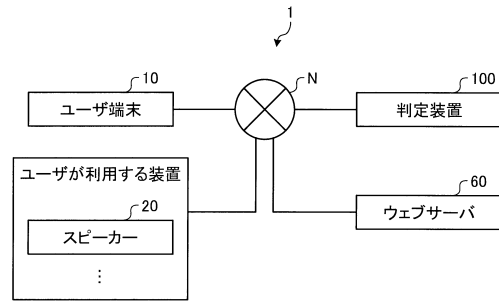
50

- 1 3 4 取得部
- 1 3 5 判定部
- 1 3 6 送信部
- 2 0 0 判定装置
- 2 2 5 推定ルール記憶部
- 2 3 7 推定部
- 3 0 0 判定装置
- 3 3 8 学習部

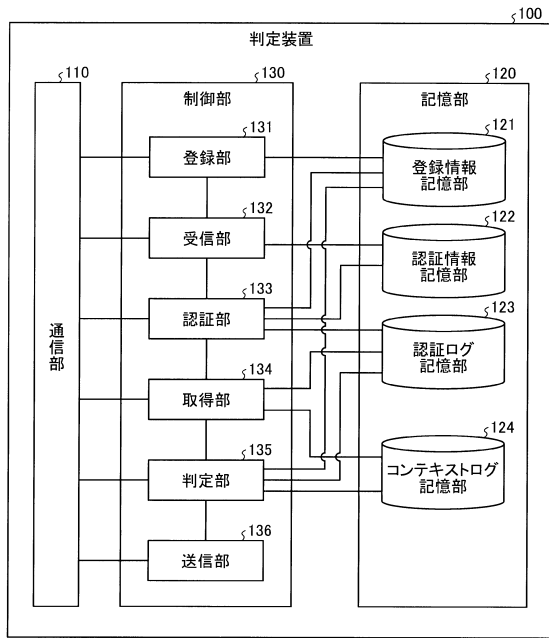
【 図 1 】



【 図 2 】



【図3】



【図4】

ユーザID	登録ID	コンテキスト	...
...
U01	R01	位置情報G01	...
		ユーザ端末10と通信	
		ユーザ端末10とスピーカー20との通信	
	
	R02	ユーザ端末10と通信	...
		端末装置30と通信	
ユーザ端末10と端末装置30との通信			
...
...

【図5】

ユーザID	認証手段	正解データ	...
...
U01	指紋	X01	...
	パスワード	X02	...
	音声	X03	...
...

【図7】

ユーザID	取得日時	コンテキスト情報		取得情報	正否	
		取得情報	正否			
U01	2015/11/1 7:00	位置情報G01	1	ユーザ端末10/通信あり	1	
		位置情報G01	1	ユーザ端末10/通信あり	1	
		位置情報G01	1	ユーザ端末10/通信あり	1	
		
	2015/11/1 8:50	位置情報G02	0	ユーザ端末10/通信あり	1	スピーカー20/通信なし
		位置情報G03	0	ユーザ端末10/通信あり	1	スピーカー20/通信なし
		位置情報G04	0	ユーザ端末10/通信あり	1	スピーカー20/通信なし
		
	2015/11/1 9:10
	
	
	

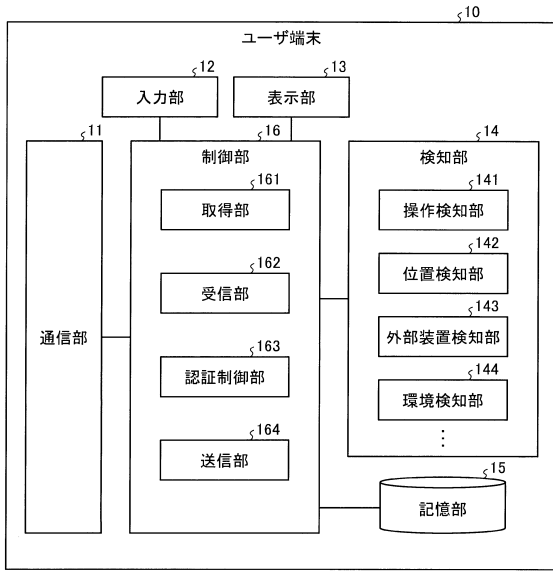
【図6】

ユーザID	認証日時	認証手段	...
...
U01	2015/11/1 7:00	指紋	...
	2015/11/1 7:10	登録データ	...

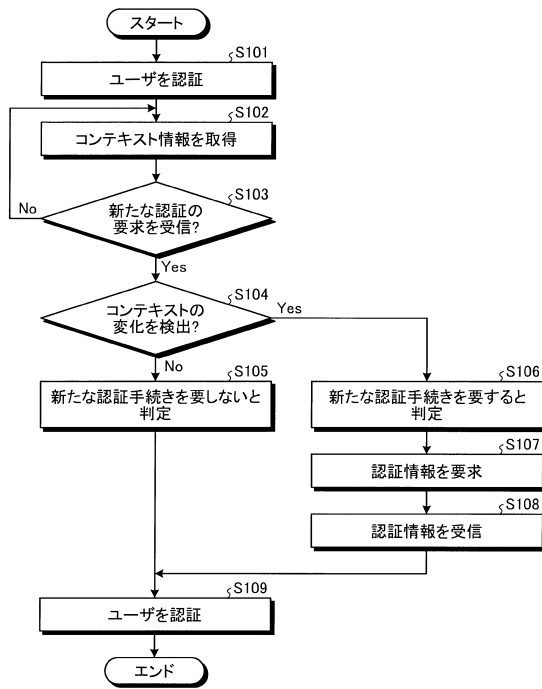
	2015/11/1 9:10	指紋	...

...

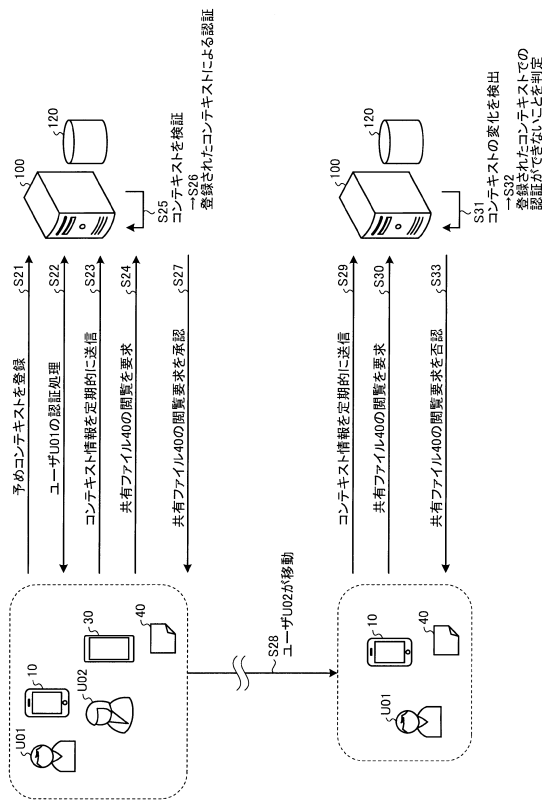
【図 8】



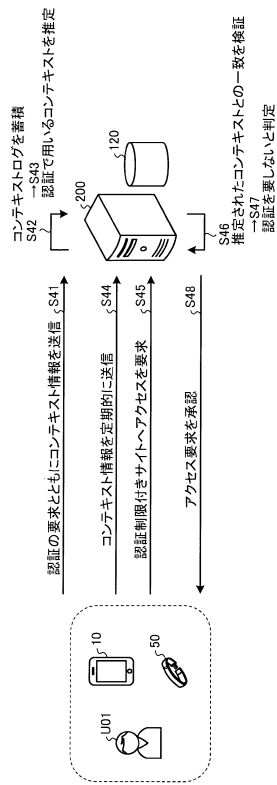
【図 9】



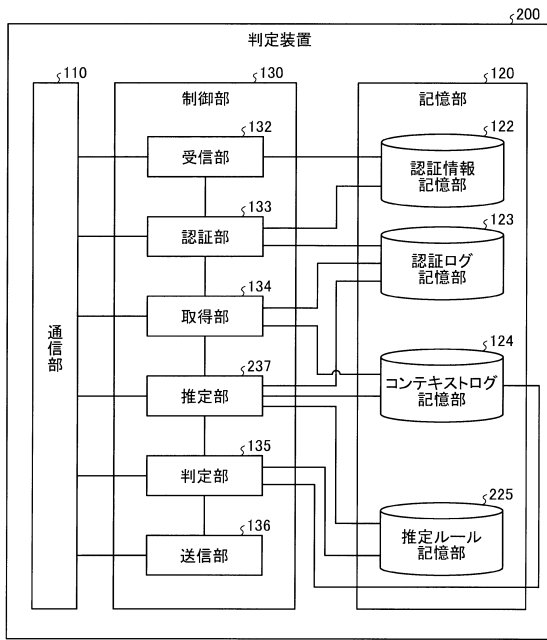
【図 10】



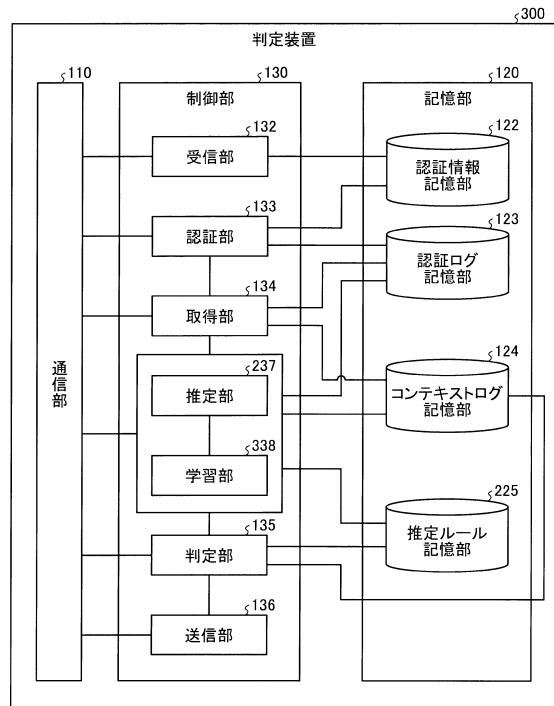
【図 11】



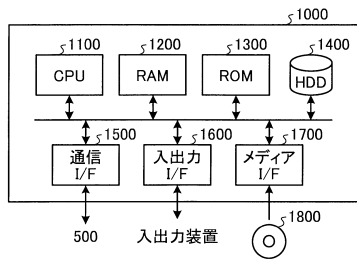
【図12】



【図13】



【図14】



フロントページの続き

(56)参考文献 特開2010-204808(JP,A)

特許第5731726(JP,B2)

特開2012-202747(JP,A)

特開2014-123277(JP,A)

Android 5.0 Lollipop クイックスタートガイド(日本語版), Google Inc., 2015年 3月
31日, pp.26-28

(58)調査した分野(Int.Cl., DB名)

G06F 21/31

G06F 21/50