(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6947529号
(P6947529)
(45)発行日　令和3年10月13日(2021.10.13)　(24)登録日　令和3年9月21日(2021.9.21)

(51)Int.Cl.　F I
G06F 21/31 (2013.01)　G06F 21/31

請求項の数 12　(全 34 頁)

(21)出願番号　特願2017-83685(P2017-83685)
(22)出願日　平成29年4月20日(2017.4.20)
(62)分割の表示　特願2015-206280(P2015-206280)の分割
原出願日　平成27年10月20日(2015.10.20)
(65)公開番号　特開2017-157223(P2017-157223A)
(43)公開日　平成29年9月7日(2017.9.7)
審査請求日　平成30年9月14日(2018.9.14)
審判番号　不服2020-11969(P2020-11969/J1)
審判請求日　令和2年8月26日(2020.8.26)

(73)特許権者　319013263
ヤフー株式会社
東京都千代田区紀尾井町１番３号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　五味　秀仁
東京都千代田区紀尾井町１番３号　ヤフー株式会社内
(72)発明者　寺岡　照彦
東京都千代田区紀尾井町１番３号　ヤフー株式会社内

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に取得する取得部と、
前記認証を要求された場合は、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、今回の認証の要求に対する認証手続きを行うことを要求するか否かを判定する判定部と、
を備え、
前記判定部は、
前回の認証の要求時に取得されたコンテキスト情報が示すコンテキスト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示すコンテキストとの変化が所定の第１範囲内に収まり、かつ、前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキストの変化が所定の第２範囲内に収まる場合は、新たな認証手続きを要求しないと判定し、
前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキストの変化が前記第２範囲内に収まらない場合は、前回の認証の要求時に取得されたコンテキスト情報が示すコンテキスト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示すコンテキストとの変化が前記第１範囲内に収まる場合であっても、今回の認証においては新たな認証手続きを要求すると判定する

ことを特徴とする判定装置。
【請求項２】
前記判定部は
前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキスト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して新たな認証手続きを行うことを要求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、
前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキスト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して新たな認証手続きを行うことを要求するか否かを判定する、
ことを特徴とする請求項１または２に記載の判定装置。
【請求項４】
前記判定部は、
前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキスト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して新たな認証手続きを行うことを要求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して新たな認証手続きを要求しないと判定する、
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。
【請求項６】
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して新たな認証手続きを要求しないと判定する、
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。
【請求項７】
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６に記載の判定装置。
【請求項８】
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６又は７に記載の判定装置。
【請求項９】
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８に記載の判定装置。
【請求項１０】
前記判定部によって前記認証の要求に対して新たな認証手続きを要求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して新たな認証手続きを要求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１～９のいずれか一つに記載の判定装置。
【請求項１１】
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、
前記認証を要求された場合は、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、今回の認証の要求に対する認証手続きを行うことを要求するか否かを判定する判定工程と、
を含み、
前記判定工程は、
前回の認証の要求時に取得されたコンテキスト情報が示すコンテキスト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示すコンテキストとの変化が所定の第１範囲内に収まり、かつ、前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキストの変化が所定の第２範囲内に収まる場合は、新たな認証手続きを要求しないと判定し、
前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキストの変化が前記第２範囲内に収まらない場合は、前回の認証の要求時に取得されたコンテキスト情報が示すコンテキスト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示すコンテキストとの変化が前記第１範囲内に収まる場合であっても、今回の認証においては新たな認証手続きを要求すると判定する
ことを特徴とする判定方法。
【請求項１２】
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、
前記認証を要求された場合は、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、今回の認証の要求に対する認証手続きを行うことを要求するか否かを判定する判定手順と、
をコンピュータに実行させ、
前記判定手順は、
前回の認証の要求時に取得されたコンテキスト情報が示すコンテキスト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示すコンテキストとの変化が所定の第１範囲内に収まり、かつ、前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキストの変化が所定の第２範囲内に収まる場合は、新たな認証手続きを要求しないと判定し、
前回の認証の要求時から今回の認証の要求時までに定期的に取得されたコンテキスト情報が示すコンテキストの変化が前記第２範囲内に収まらない場合は、前回の認証の要求時

に取得されたコンテキスト情報が示すコンテキスト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示すコンテキストとの変化が前記第１範囲内に収まる場合であっても、今回の認証においては新たな認証手続きを要求すると判定する

ことを特徴とする判定プログラム。

【発明の詳細な説明】

【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定期的に取得する取得部と、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から、新たに前記受信部によって認証の要求が受信されるまでの期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。

【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。
【図１１】図１１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１２】図１２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１３】図１３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１４】図１４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。
【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。
【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。
【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。

【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を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の指紋データやパスワードなど）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行われてもよい。

【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。

【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。

【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。

【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で定期的に取得し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Ｓ０３及びステップＳ０４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Ｓ０４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Ｓ０２の時点から変わらず、ユーザＵ０１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Ｓ０４での新たな認証を要しないと判定する（ステップＳ０６）。言い換えれば、判定装置１００は、ステップＳ０４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Ｓ０４で行われたアクセスの要求を承認する（ステップＳ０７）。
【００２４】
続いて、ユーザＵ０１が自宅を離れ、外出したとする（ステップＳ０８）。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Ｓ０９）。
【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Ｓ１０）。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Ｓ１１）。具体的には、判定装置１００は、ステップＳ０２～Ｓ０７の時点でのコンテキスト情報と、ステップＳ０９で定期的に取得したコンテキスト情報と、ステップＳ１０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。
【００２６】
そして、判定装置１００は、ステップＳ０２～Ｓ０９の時点でのコンテキスト情報と、ステップＳ１０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Ｓ１０の時点では、ステップＳ０１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Ｕ０１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。
【００２７】
そして、判定装置１００は、ステップＳ１０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Ｓ１２）。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Ｕ０１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Ｓ１３）。
【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Ｕ０１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。要求に応答して、ユーザ端末１０は、認証情報を送信する（ステップＳ１４）。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Ｓ１０におけるアクセス要求を承認する（ステップＳ１５）。

【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Ｕ０１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。

【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、スピーカー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。

【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。

【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、例えばスピーカー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。

【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（株価）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。

【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】

〔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。

【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）

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。

【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】

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。

【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。

【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の実施形態に係る認証ログ記憶部１２３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１２３は、「ユーザＩＤ」、「認証日時」、「認証手段」といった項目を有する。

【００５２】

「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。

【００５３】

すなわち、図６では、ユーザＩＤ「Ｕ０１」で識別されるユーザＵ０１に対して、「２０１５年１１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１１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１２１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Ｕ０１は、「２０１５年１１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。

【００５４】

なお、認証ログ記憶部１２３には、認証が行われた際のユーザ端末１０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。

【００５５】

（コンテキストログ記憶部１２４について）

コンテキストログ記憶部１２４は、判定装置１００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１２４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１２４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１２４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。

【００５６】

「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。

【００５７】

「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１２４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「Ｒ０１」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。

【００５８】

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「Ｒ０１」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Ｇ０１」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１０（と、判定装置１００との）通信」や、「スピーカー２０（と、ユーザ端末１０との）通信」が取得

されたか否かの正否が記憶される。
【００５９】
例えば、図７では、「２０１５年１１月１日　７：００」におけるコンテキスト情報として、「位置情報Ｇ０１」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１０」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２０」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。
【００６０】
一方で、「２０１５年１１月１日　９：００」におけるコンテキスト情報として、「位置情報Ｇ０３」が取得され、登録されたコンテキストを示す「位置情報Ｇ０１」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２０」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Ｕ０１が自宅（位置情報Ｇ０１で示される）から外出し、ユーザ端末１０とスピーカー２０との通信も途絶えたことを示している。なお、「ユーザ端末１０」は、変わらず判定装置１００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。
【００６１】
このように、コンテキストログ記憶部１２４では、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「Ｒ０１」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１２４には、登録ＩＤ「Ｒ０２」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。
【００６２】
（制御部１３０について）
制御部１３０は、例えば、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）等によって、判定装置１００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１３０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される。
【００６３】
図３に示すように、制御部１３０は、登録部１３１と、受信部１３２と、認証部１３３と、取得部１３４と、判定部１３５と、送信部１３６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１３０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１３０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。
【００６４】
（登録部１３１について）
登録部１３１は、ユーザ端末１０が認証される際のユーザ端末１０のコンテキストについて登録を受け付ける。例えば、登録部１３１は、ユーザ端末１０を利用するユーザＵ０１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１３１が受け付けたコンテキストは、判定部１３５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１０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１３１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。
【００６５】
登録部１３１は、受け付けたコンテキストを登録情報記憶部１２１に記憶する。また、登録部１３１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。

【００６６】
（受信部１３２について）
受信部１３２は、各種情報を受信する。例えば、受信部１３２は、ユーザ端末１０から送信される各種要求を受信する。具体的には、受信部１３２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１０から受信する。また、受信部１３２は、ユーザ端末１０の認証の要求を受信する。また、受信部１３２は、認証手続きにおいて、ユーザ端末１０から送信される認証情報を受信する。
【００６７】
上記の処理において、受信部１３２は、所定の制限付きサイトへのアクセス要求や、ユーザ端末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）に関する情報等を取得する。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。

【００８２】

例えば、判定部１３５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１３５は、数種類のコンテキスト情報のうち、いくつ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１３５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１３５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１０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１３５は、取得された位置情報Ｇ０１が位置情報Ｇ０２に変化した場合であっても、位置情報Ｇ０１と位置情報Ｇ０２とがごく近い範囲を示す情報であれば、ユーザ端末１０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１００の管理者等によって人為的に設定されてもよい。

【００８３】

そして、判定部１３５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１０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１３５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１０への新たな認証手続きを要しないと判定する。

【００８４】

また、判定部１３５は、前回の認証の要求時から今回の認証の要求時までに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１３５は、定期的に取得部１３４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１３５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１３５は、ユーザ端末１０とスピーカー２０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１０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１３５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１０に要求すると判定してもよい。

【００８５】

また、判定部１３５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１３５は、受信部１３２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してもよい。

【００８６】

（送信部１３６について）

送信部１３６は、各種情報を送信する。例えば、送信部１３６は、認証の要求を行った

ユーザ端末１０に対して、認証部１３３が行った認証処理の結果を送信する。例えば、認証部１３３がユーザ端末１０を認証した場合、送信部１３６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１０に送信する。

【００８７】

〔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１０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１０の構成例を示す図である。図８に示すように、ユーザ端末１０は、通信部１１と、入力部１２と、表示部１３と、検知部１４と、記憶部１５と、制御部１６とを有する。

【００８８】

（通信部１１について）

通信部１１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２０や、判定装置１００や、ウェブサーバ６０との間で情報の送受信を行う。例えば、通信部１１は、ＮＩＣ等によって実現される。

【００８９】

（入力部１２及び表示部１３について）

入力部１２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１２は、ユーザ端末１０に備えられた操作キー等によって実現される。表示部１３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１３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１０にタッチパネルが採用される場合には、入力部１２の一部と表示部１３とは一体化される。

【００９０】

（検知部１４について）

検知部１４は、ユーザ端末１０に関する各種情報を検知する。具体的には、検知部１４は、ユーザ端末１０に対するユーザＵ０１の操作や、ユーザ端末１０の所在する位置情報や、ユーザ端末１０と接続されている機器に関する情報や、ユーザ端末１０における環境等を検知する。図８に示す例では、検知部１４は、操作検知部１４１と、位置検知部１４２と、外部装置検知部１４３と、環境検知部１４４とを有する。

【００９１】

（操作検知部１４１について）

操作検知部１４１は、ユーザ端末１０に対するユーザＵ０１の操作を検知する。例えば、操作検知部１４１は、入力部１２に入力された情報に基づいて、ユーザＵ０１の操作を検知する。すなわち、操作検知部１４１は、入力部１２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１４１は、ユーザＵ０１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１０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１４１は、ユーザＵ０１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１４１は、ユーザ端末１０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１０自体が動かされているといった操作を検知してもよい。

【００９２】

（位置検知部１４２について）

位置検知部１４２は、ユーザ端末１０の現在位置を検知する。具体的には、位置検知部１４２は、ＧＰＳ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１０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。

【００９３】

位置検知部１４２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１０が駅改札や商店等で使用される非接触型ＩＣ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１０が非接触型ＩＣ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１０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１４２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１４２は、ユーザ端末１０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１０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。

【００９４】

（外部装置検知部１４３について）

外部装置検知部１４３は、ユーザ端末１０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１４３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１４３は、検知した外部装置をユーザ端末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）。

【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。

【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。

【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）。

【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）。

【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、認証にかけ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。

【０１３５】

〔２－１．判定処理の一例〕

まず、図１１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１１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１１に示した判定装置２００は、ユーザ端末１０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。

【０１３６】

図１１に示すユーザＵ０１は、ユーザ端末１０と、時計型端末５０とを利用するユーザである。例えば、ユーザＵ０１は、ユーザ端末１０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２００に認証を要求する。ユーザＵ０１は、認証の要求とともに、ユーザ端末１０に関するコンテキスト情報を送信する（ステップＳ４１）。この場合、ユーザ端末１０から送信されるコンテキスト情報は、例えば、「ユーザ端末１０と時計型端末５０との近距離通信が確立」等である。

【０１３７】

判定装置２００は、取得したコンテキストログを記憶部１２０に蓄積する（ステップＳ４２）。そして、判定装置２００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Ｓ４３）。詳細は後述するが、判定装置２００は、例えば、ユーザ端末１０の認証を行う際には、高い確率で「ユーザ端末１０と時計型端末５０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２００は、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２００は、認証で用いるコンテキストとして、「ユーザ端末１０と時計型端末５０との近距離通信が確立」を推定する。

【０１３８】

その後、ユーザ端末１０は、定期的にコンテキスト情報を判定装置２００に送信する（ステップＳ４４）。そして、あるタイミングで、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Ｓ４５）。このとき、判定装置２００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Ｓ４６）。これは、第１の実施形態において、判定装置１００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。

【０１３９】

そして、判定装置２００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２００は、通常、「ユーザ端末１０と時計型端末５０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１０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１０は通常認証を行っているユーザＵ０１により操作されているものと判定する。

【０１４０】

そして、判定装置２００は、ステップＳ４５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Ｓ４７）。そして、判定装置２００は、新たな認証手続きを省いて、ユーザ端末１０のアクセス要求を承認する（ステップＳ４８）。

【０１４１】

このように、第２の実施形態に係る判定装置２００は、コンテキストの推定手段を有する。そして、判定装置２００は、推定したコンテキストの変化に基づいて、ユーザＵ０１の認証に関する判定処理を行う。これにより、判定装置２００は、予めユーザＵ０１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２００は、ユーザＵ０１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。

【０１４２】

〔２－２．判定装置の構成〕

次に、図１２を用いて、第２の実施形態に係る判定装置２００の構成について説明する。図１２は、第２の実施形態に係る判定装置２００の構成例を示す図である。図１２に示すように、判定装置２００は、推定ルール記憶部２２５と、推定部２３７とを有する。

【０１４３】

（推定ルール記憶部２２５について）

推定ルール記憶部２２５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２２５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２２５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２２５が記憶する推定ルールは、例えば、判定装置２００の管理者等により人為的に設定され、記憶される。

【０１４４】

（推定部２３７について）

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。この場合、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、推定部２３７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。

【０１４５】

推定部２３７は、推定ルール記憶部２２５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２３７は、取得部１３４によって取得されたコンテキスト情報から、ユーザ端末１０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。

【０１４６】

すなわち、推定部２３７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２３７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２３７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。

【０１４７】

第１の実施形態で説明したように、取得部１３４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１３４は、ユーザ端末１０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２３７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２００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できる。

【０１４８】

〔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２００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推定部２３７を備える。また、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、推定部２３７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。

【０１４９】

このように、第２の実施形態に係る判定装置２００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２００によれば、事前の登録処理を要せずに、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。

【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。

【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。

【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。

【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て行われてもよい。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。
【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。
【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。
【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。

【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。

【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。

【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。

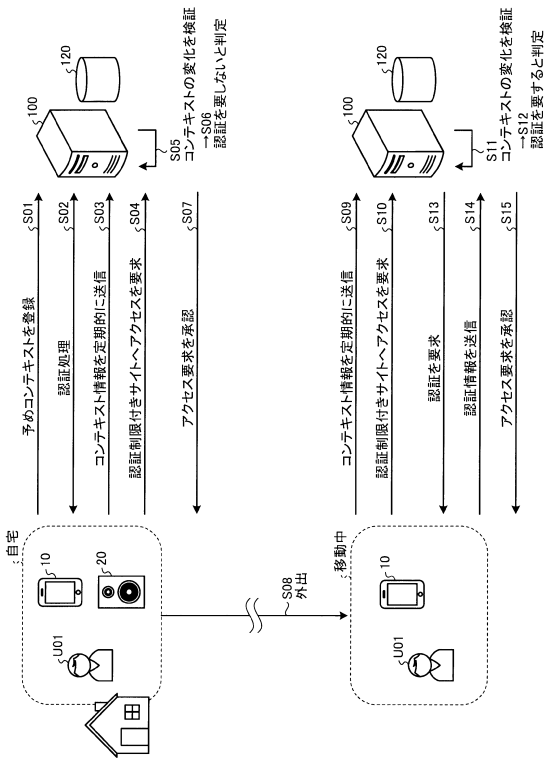
【符号の説明】

【０１８８】

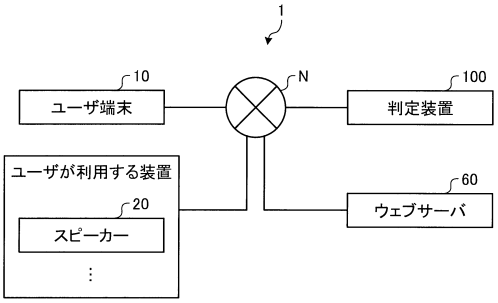
１　判定処理システム
１０　ユーザ端末
２０　スピーカー
３０　端末装置
４０　共有ファイル
５０　時計型端末
６０　ウェブサーバ
１００　判定装置
１１０　通信部

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
１３４　取得部
１３５　判定部
１３６　送信部
２００　判定装置
２２５　推定ルール記憶部
２３７　推定部
３００　判定装置
３３８　学習部

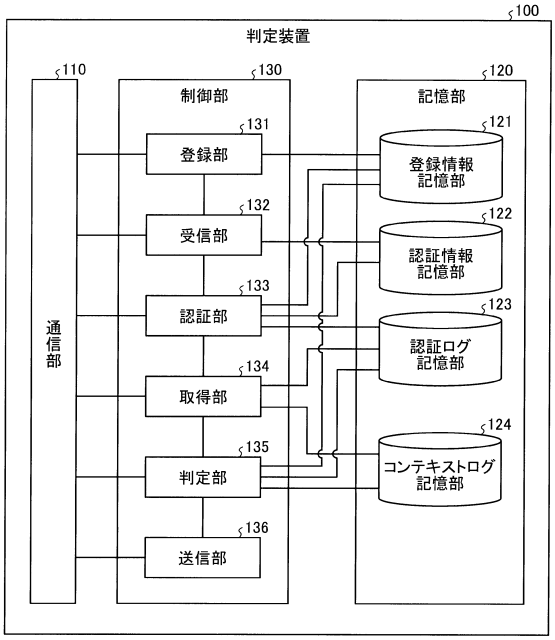
【図１】



【図２】



【図３】



【図４】

121

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】

122

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６】

123

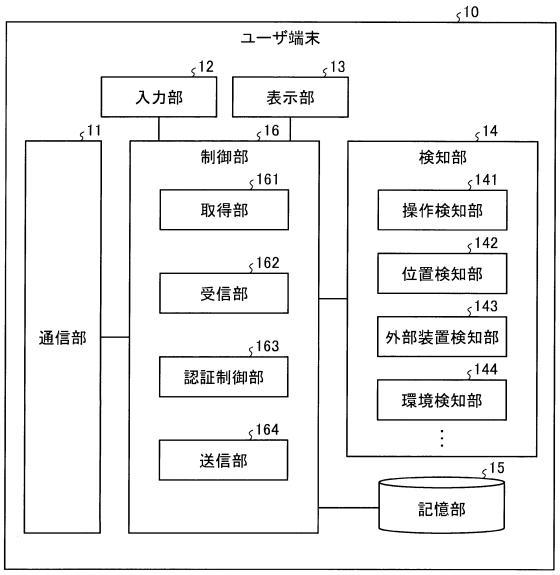
ユーザID	認証日時	認証手段	…
…	…	…	…
U01	2015/11/1 7:00	指紋	…
	2015/11/1 7:10	登録データ	…
	…	…	…
	2015/11/1 9:10	指紋	…
	…	…	…
…	…	…	…

【図７】

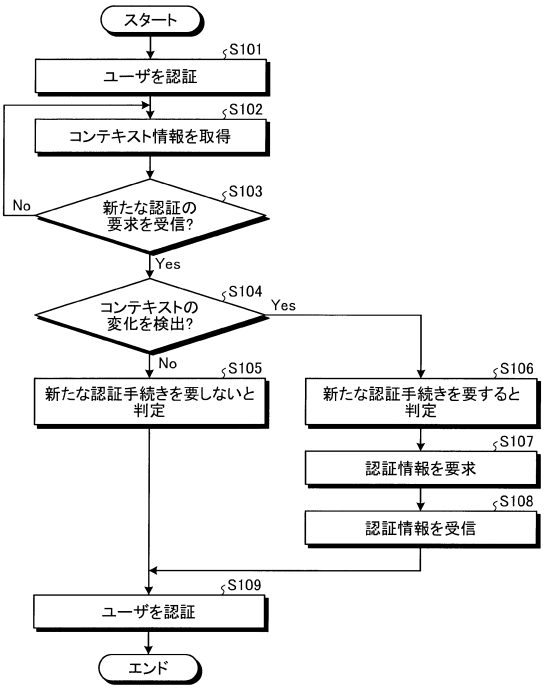
124

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	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	スピーカー20/通信あり	1	…	…	…	…
	2015/11/1 7:10	位置情報G01	1	ユーザ端末10/通信あり	1	スピーカー20/通信あり	1	…	…	…	…
	2015/11/1 7:20	位置情報G01	1	ユーザ端末10/通信あり	1	スピーカー20/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	0	…	…	…	…
	2015/11/1 9:00	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	0	…	…	…	…
	2015/11/1 9:10	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	0	…	…	…	…
	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…

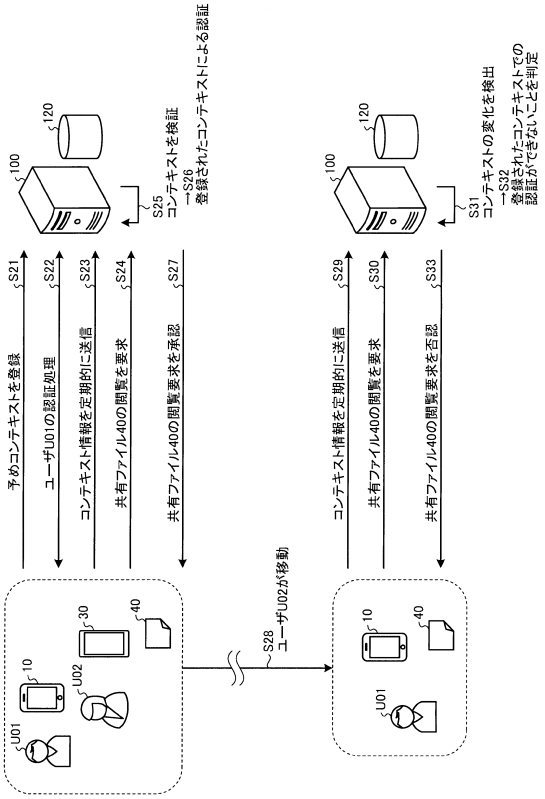
【図８】


10
ユーザ端末
12
入力部
13
表示部
11
16
制御部
14
検知部
161
取得部
162
受信部
163
認証制御部
164
送信部
141
操作検知部
142
位置検知部
143
外部装置検知部
144
環境検知部
通信部
15
記憶部

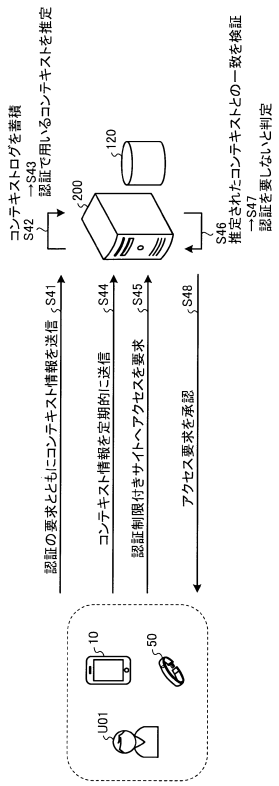
【図９】


スタート
S101
ユーザを認証
S102
コンテキスト情報を取得
S103
新たな認証の要求を受信?
No
Yes
S104
コンテキストの変化を検出?
Yes
No
S105
新たな認証手続きを要しないと判定
S106
新たな認証手続きを要すると判定
S107
認証情報を要求
S108
認証情報を受信
S109
ユーザを認証
エンド

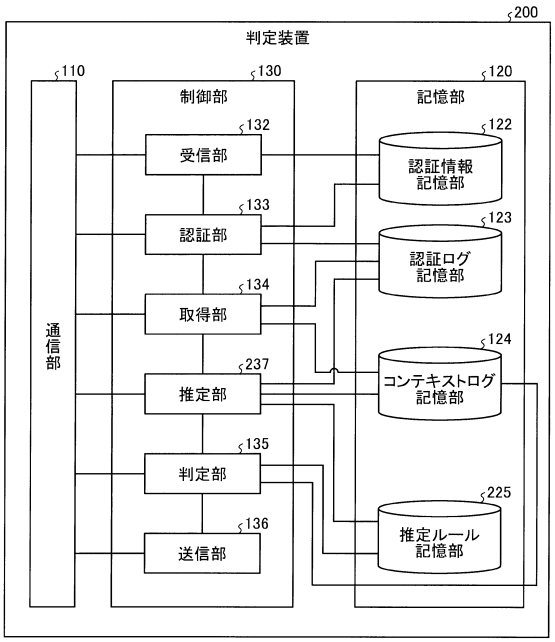
【図１０】


120
100
S25
コンテキストを検証
S26
登録されたコンテキストによる認証
S21
予めコンテキストを登録
S22
ユーザU01の認証処理
S23
コンテキスト情報を定期的に送信
S24
共有ファイル40の閲覧を要求
S27
共有ファイル40の閲覧要求を承認
S28
ユーザU02が移動
S29
コンテキスト情報を定期的に送信
S30
共有ファイル40の閲覧を要求
S33
共有ファイル40の閲覧要求を否認
S31
コンテキストの変化を検出
S32
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
10
30
40
50
U01
U02

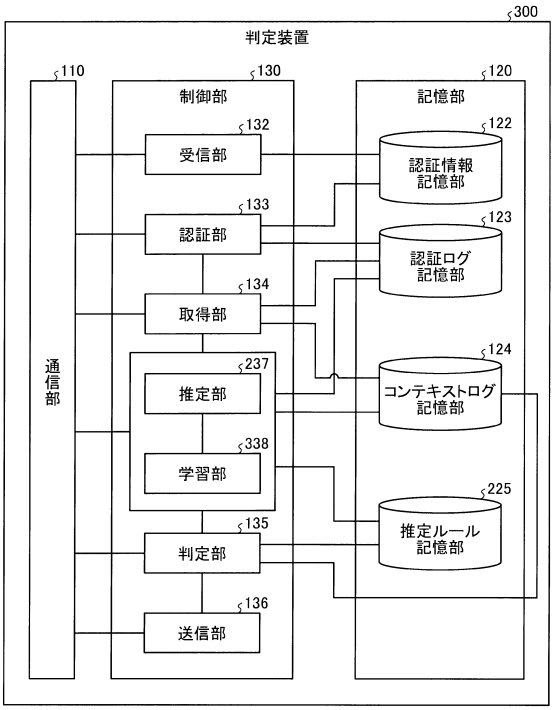
【図１１】


コンテキストログを蓄積
S43
認証で用いるコンテキストを推定
S42
120
200
S46
推定されたコンテキストとの一致を検証
S47
認証を要しないと判定
S41
認証の要求とともにコンテキスト情報を送信
S44
コンテキスト情報を定期的に送信
S45
認証制限付きサイトへアクセスを要求
S48
アクセス要求を承認
10
50
U01

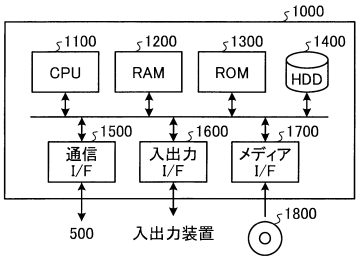
【図１２】


200
判定装置
110
通信部
130
制御部
132
受信部
133
認証部
134
取得部
237
推定部
135
判定部
136
送信部
120
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
225
推定ルール記憶部

【図１３】


300
判定装置
110
通信部
130
制御部
132
受信部
133
認証部
134
取得部
237
推定部
338
学習部
135
判定部
136
送信部
120
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
225
推定ルール記憶部

【図１４】


1000
1100
CPU
1200
RAM
1300
ROM
1400
HDD
1500
通信I/F
1600
入出力I/F
1700
メディアI/F
500
入出力装置
1800

フロントページの続き

合議体
審判長　田中　秀人
審判官　山崎　慎一
審判官　塚田　肇

(56)参考文献　特開２００４－１１８４５６（ＪＰ，Ａ）
特開２００４－３１０２０７（ＪＰ，Ａ）
特開２０１５－９０５８９（ＪＰ，Ａ）
特開２０１１－６１７１４（ＪＰ，Ａ）
特開２０１０－２７７１４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F21/31