

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号  
特開2018-165894  
(P2018-165894A)

(43) 公開日 平成30年10月25日(2018.10.25)

(51) Int.Cl.

F I

テーマコード (参考)

G O 6 F 21/31 (2013.01)

G O 6 F 21/32 (2013.01)

G O 6 F 21/31

G O 6 F 21/32

審査請求 未請求 請求項の数 10 O L (全 35 頁)

|           |                            |          |               |
|-----------|----------------------------|----------|---------------|
| (21) 出願番号 | 特願2017-62870 (P2017-62870) | (71) 出願人 | 000004237     |
| (22) 出願日  | 平成29年3月28日 (2017. 3. 28)   |          | 日本電気株式会社      |
|           |                            |          | 東京都港区芝五丁目7番1号 |
|           |                            | (74) 代理人 | 100109313     |
|           |                            |          | 弁理士 机 昌彦      |
|           |                            | (74) 代理人 | 100124154     |
|           |                            |          | 弁理士 下坂 直樹     |
|           |                            | (72) 発明者 | 岩上 智之         |
|           |                            |          | 東京都港区芝五丁目7番1号 |
|           |                            |          | 日本電気株式会社内     |

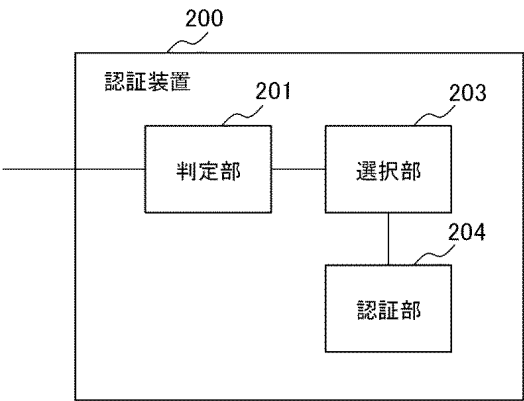
(54) 【発明の名称】 認証装置、認証方法およびプログラム

(57) 【要約】

【課題】 一台の計算機の中で効率良く認証を行う技術を提供する。

【解決手段】 認証装置は、サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、前記認証の実行の優先順位を示す第2の優先度を前記認証要求に付与する判定手段と、前記第2の優先度に応じて、前記認証の対象となる認証要求を選択する選択手段と、選択された認証要求に対し、前記認証を行う認証手段と、を備える。

【選択図】 図2 8



**【特許請求の範囲】****【請求項 1】**

サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第 1 の優先度に応じて、前記認証の実行の優先順位を示す第 2 の優先度を前記認証要求に付与する判定手段と、

前記第 2 の優先度に応じて、前記認証の対象となる認証要求を選択する選択手段と、  
選択された認証要求に対し、前記認証を行う認証手段と、を備える認証装置。

**【請求項 2】**

前記判定手段は、前記第 2 の優先度が付与された認証要求の数が閾値以下である場合、前記第 2 の優先度を、前記受け付けた認証要求に付与する請求項 1 に記載の認証装置。

10

**【請求項 3】**

前記判定手段は、前記認証要求に含まれるパスワードの安全性の度合いと前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する請求項 1 または 2 に記載の認証装置。

**【請求項 4】**

前記認証手段は、前記認証要求の要求元ごとに前記認証が連続して成功した回数を示す連続成功回数と、前記認証が連続して失敗した回数を示す連続失敗回数とをカウントし、

前記判定手段は、前記連続成功回数と前記連続失敗回数と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する請求項 1 または 2 に記載の認証装置。

20

**【請求項 5】**

前記判定手段は、前記認証要求の要求元が使用する IP ( Internet Protocol ) アドレスと前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する請求項 1 または 2 に記載の認証装置。

**【請求項 6】**

前記判定手段は、前記認証要求の要求元と前記認証要求の要求先との間でネットワーク通信が確立するまでに要する時間と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する請求項 1 または 2 に記載の認証装置。

**【請求項 7】**

前記判定手段は、前記認証要求の要求元が使用するアプリケーションに関する情報と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する請求項 1 または 2 に記載の認証装置。

30

**【請求項 8】**

前記判定手段は、前記サービスを利用するクライアントの行動的特徴を示すバイオメトリクス情報であって、予め登録されたバイオメトリクス情報と、受け付けた認証要求に含まれるバイオメトリクス情報とを用いて類似度を算出し、算出した類似度と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する請求項 1 または 2 に記載の認証装置。

**【請求項 9】**

サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第 1 の優先度に応じて、前記認証の実行順を示す第 2 の優先度を前記認証要求に付与し、

前記第 2 の優先度に応じて、前記認証の対象となる認証要求を選択し、  
選択された認証要求に対し、前記認証を行う認証方法。

**【請求項 10】**

サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第 1 の優先度に応じて、前記認証の実行順を示す第 2 の優先度を前記認証要求に付与する判定処理と、

前記第 2 の優先度に応じて、前記認証の対象となる認証要求を選択する選択処理と、

50

選択された認証要求に対し、前記認証を行う認証処理と、をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、認証装置、認証方法およびプログラムに関する。

【背景技術】

【0002】

インターネットの普及により、地理的な制約を受けずにサービスを提供する計算機システム、例えばサーバ等のリソースを利用できる環境が整いつつある。近年利用が増加しているクラウドサービスも、地理的制約から解放された計算機システムの利用方法の一例と考えられる。

10

【0003】

しかしながら、地理的制約からの解放により、例えばサーバ等のリソースを容易に使えるようになる一方で、悪意を持った利用者からのサーバに対する不正なアクセスが増加している。

【0004】

この不正なアクセスは、サーバが持つリソース、またはリソースに含まれる機密情報を入手する目的だけでなく、サーバが提供するサービスを妨害する目的で行われることもある。これらの不正アクセスからサーバ等のリソース、機密情報およびサービスを保護するために、認証の重要性が高まっている。

20

【0005】

サーバを保護するには、強固な認証の仕組みが必要となる。しかし、認証の仕組みが強固になればなるほど、認証の仕組みに要するサーバの計算機資源（CPU（Central Processing Unit）やメモリ）も増加する。

【0006】

さらに、地理的制約からの解放によるサーバの利用者の増加、および、サービスを妨害する意図でのアクセス（DoS（Denial of Services）攻撃）により、認証が行われる回数自体も増加傾向にある。

【0007】

30

これらの背景により、サーバが保有する計算機資源における認証のコストは増加傾向にあり、認証のコストが、サービスを提供するサーバに対して高負荷となる恐れがある。

【0008】

認証の負荷を分散する手段として、例えば、特許文献1には、認証を複数の計算機で分担して行う「スケールアウト」の手法が記載されている。特許文献1に記載の手法においては、認証を要求した利用者が使用するクライアント端末が、認証を行う夫々のサーバの優先度に基づき、夫々のサーバにアクセスすることで、夫々のサーバにおける認証のコストの均等化を行う。

【先行技術文献】

【特許文献】

40

【0009】

【特許文献1】特開平11-41252号公報

【発明の概要】

【発明が解決しようとする課題】

【0010】

しかしながら、例えば、一台の計算機でサービスを提供することを前提にしたメインフレーム等のサーバにおいて、複数の計算機を使用することができないため、特許文献1に記載の手法を用いることは難しい。

【0011】

本開示は、上記問題を鑑みたものであって、一台の計算機の中で効率良く認証を行う技

50

術を提供する。

【課題を解決するための手段】

【0012】

本開示の一形態に係る認証装置は、サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、前記認証の実行の優先順位を示す第2の優先度を前記認証要求に付与する判定手段と、前記第2の優先度に応じて、前記認証の対象となる認証要求を選択する選択手段と、選択された認証要求に対し、前記認証を行う認証手段と、を備える。

【0013】

本開示の一形態に係る認証方法は、サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、前記認証の実行順を示す第2の優先度を前記認証要求に付与し、前記第2の優先度に応じて、前記認証の対象となる認証要求を選択し、選択された認証要求に対し、前記認証を行う。

【0014】

本開示の一形態に係るプログラムは、サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、前記認証の実行順を示す第2の優先度を前記認証要求に付与する判定処理と、前記第2の優先度に応じて、前記認証の対象となる認証要求を選択する選択処理と、選択された認証要求に対し、前記認証を行う認証処理と、をコンピュータに実行させる。

【発明の効果】

【0015】

本開示によれば、一台の計算機の中で効率良く認証を行うことができる。

【図面の簡単な説明】

【0016】

【図1】第1実施形態に係る認証システムの構成の一例を示す機能ブロック図である。

【図2】各クライアント端末から送信される認証要求のデータ構造の一例を示す図である。

。

【図3】優先度判定データベースの一例を示す図である。

【図4】認証要求リストの一例を示す図である。

【図5】認証待機リストの一例を示す図である。

【図6】判定部の動作の一例を示すフローチャートである。

【図7】選択部の動作の一例を示すフローチャートである。

【図8】確認部の動作の一例を示すフローチャートである。

【図9】安全性リストの一例を示す図である。

【図10】変形例1における認証要求リストの一例を示す図である。

【図11】パスワード評価リストの一例を示す図である。

【図12】変形例2における判定部の動作の一例を示すフローチャートである。

【図13】変形例2における認証要求リストの一例を示す図である。

【図14】変形例3における認証装置の構成の一例を示す機能ブロック図である。

【図15】連続リストの一例を示す図である。

【図16】変形例3における認証要求リストの一例を示す図である。

【図17】アドレスリストの一例を示す図である。

【図18】変形例4における認証要求リストの一例を示す図である。

【図19】変形例5における認証要求リストの一例を示す図である。

【図20】変形例6における認証要求リストの一例を示す図である。

【図21】クライアント端末リストの一例を示す図である。

【図22】変形例7における認証要求リストを示す図である。

【図23】バイオメトリクスリストの一例を示す図である。

【図24】変形例8における認証要求リストの一例を示す図である。

10

20

30

40

50

【図 2 5】 利用情報リストの一例を示す図である。

【図 2 6】 優先度リストの一例を示す図である。

【図 2 7】 変形例 9 における認証要求リストの一例を示す図である。

【図 2 8】 第 2 実施形態に係る認証装置の構成の一例を示す機能ブロック図である。

【図 2 9】 第 2 実施形態に係る認証装置の動作の一例を示すフローチャートである。

【図 3 0】 本開示の各実施形態に係る認証装置または認証システムを実現する情報処理装置のハードウェア構成の一例を示すブロック図である。

【発明を実施するための形態】

【0017】

以下、本開示の実施形態について図面を参照して詳細に説明する。

10

【0018】

＜第 1 実施形態＞

図 1 は、認証システム 1 の構成の一例を示す機能ブロック図である。認証システム 1 は、認証装置 10 と、サーバ 20 と、サーバ 30 と、クライアント端末 40 と、クライアント端末 50 とを含む。

【0019】

サーバ 20 とサーバ 30 とは、有線または無線のネットワークを介し、クライアント端末 40 と、クライアント端末 50 とにサービスを提供する。サーバ 20 は、例えば、H T T P ( H y p e r T e x t T r a n s f e r P r o t o c o l ) サーバによって構成される。サーバ 30 は、例えば、メールサーバによって構成される。つまり、サーバ 20 は H T T P サービスを提供し、サーバ 30 はメールサービスを提供する。

20

【0020】

認証装置 10 は、クライアント端末 40 またはクライアント端末 50 が、サーバ 20 またはサーバ 30 から提供されるサービスを利用するための認証を行う装置である。言い換えると、認証装置 10 は、クライアント端末 40 と、クライアント端末 50 とがサーバ 20 またはサーバ 30 が提供するサービスを利用する権限を有しているか否か判定する装置である。

【0021】

また例えば、認証装置 10 は、L i n u x (登録商標)などで利用されている P A M ( P l u g g a b l e A u t h e n t i c a t i o n M o d u l e s ) によって実現される。認証装置 10 は、判定部 11 と、確認部 12 と、選択部 13 と、認証部 14 と、記憶部 15 とを備える。

30

【0022】

(記憶部 15)

記憶部 15 は、優先度が付与された認証要求が格納されている認証要求リスト 151 と、判定部 11 が認証要求に対して優先度を付与するために用いる情報が格納されている優先度判定データベース 152 と、認証待機リスト 153 と、認証要求量 154 とを記憶する。認証要求リスト 151 と、優先度判定データベース 152 と、認証待機リスト 153 と、認証要求量 154 とについては後述する。

【0023】

(判定部 11)

判定部 11 は、クライアント端末 40 またはクライアント端末 50 からサーバ 20 またはサーバ 30 が受け取った認証の要求(以降、第 1 の認証要求と称す)を受け付ける。また、第 1 の認証要求は、サーバ 20 またはサーバ 30 が提供するサービスの利用に対する認証の要求である。

40

【0024】

図 2 は、判定部 11 が各サーバから受け付ける第 1 の認証要求のデータ構造の一例を示す図である。図 2 に示すテーブルの 1 つのエントリが、1 つの第 1 の認証要求を示す。第 1 の認証要求は、認証要求サービス 1511 と、認証 I D ( I d e n t i f i e r ) 1512 と、パスワード 1513 とを含む。

50

## 【0025】

認証要求サービス1511は、クライアント端末40またはクライアント端末50が認証要求を送信したサーバ20またはサーバ30が提供するサービスを表す。認証要求サービス1511はサービスを表すサービス名でもよいし、サービスを提供する各サーバのポート番号でもよい。

## 【0026】

認証ID1512は、各クライアント端末を利用する利用者（以降、クライアントと称する）を識別する識別子である。パスワード1513は、認証部14が行う認証に用いられるパスワードである。認証ID1512およびパスワード1513は、クライアントの特定および正当性を保証するために一般的に用いられる。

10

## 【0027】

判定部11は第1の認証要求に受け付けた順序を示す受領番号（順序情報）を付与する。以降、受領番号が付与された（受領番号を含む）第1の認証要求を第2の認証要求と称す。また、判定部11は、第2の認証要求に含まれる情報に応じて、第2の認証要求に優先度を付与するか否かを判定する。

## 【0028】

また判定部11は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度が閾値を超える第2の認証要求を認証待機リスト153に格納する。ここでは、一例として、閾値は優先度の所定の順位を表す数値に対応する。すなわち、認証待機リスト153は、優先度の順位（優先順位）が相対的に高く、判定部11が応答性が求められないサービスに対する認証要求であると判定した認証要求を一時的に格納するリストである。

20

## 【0029】

また判定部11は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度が所定の条件を満たす場合、第2の認証要求に優先度を付与する。所定の条件とは、例えば、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度が閾値以下であることである。

これ以降、相対的に高い優先順位の優先度が付与された（優先度を含む）第2の認証要求を第3の認証要求と称する。そして、判定部11は、第3の認証要求を認証要求リスト151に格納する。なお、判定部11が確認部12から第2の認証要求を受け付けた場合の動作については、図6と図8とに示すフローチャートを用いて後述する。

30

## 【0030】

図3は、記憶部15に記憶される優先度判定データベース152の一例を示す図である。優先度判定データベース152は、認証要求サービス1511と、優先度1522とを含む。認証要求サービス1511と、優先度1522とは紐づいている。優先度（第1の優先度）1522は、自身に紐づく認証要求サービス1511に対する優先順位を示す。

## 【0031】

具体的に、認証要求サービス1511が「メール」のサービス（メールサービスと呼ぶ）の優先度1522は「1」であり、認証要求サービス1511が「HTTP」のサービス（HTTPサービスと呼ぶ）の優先度1522は「2」である。本開示において、優先度1522の数値が小さいほど、優先順位は高くなるとする。よって、HTTPサービスの優先順位よりメールサービスの優先順位のほうが高くなるとする。

40

## 【0032】

第1の認証要求に含まれる認証要求サービス1511は、上述したように各サーバが提供するサービスでもある。そのため、判定部11は、第2の認証要求に含まれる認証要求サービス1151に紐づく優先度1522を確認するために、図3に示す優先度判定データベース152を参照する。

## 【0033】

ここで、図4と図5とを用いて、認証要求リスト151と認証待機リスト153とを説明する。

## 【0034】

50

図4は、認証要求リスト151の一例を示す図である。図4に示す認証要求リスト151の1つのエントリが、1つの第3の認証要求を示す。認証要求リスト151には、認証要求サービス1511、認証ID1512、パスワード1513、受領番号1514および優先度1515が夫々関連付けられている。つまり、第3の認証要求は、認証要求サービス1511、認証ID1512、パスワード1513、受領番号1514および優先度1515を含む。優先度（第2の優先度）1515は、認証要求に対して付与された、後述する認証部14が認証を実行する優先順位を示す。

#### 【0035】

図4に示す認証要求リスト151において、第3の認証要求に含まれる受領番号1514は、判定部11が認証要求を受け付けた時刻を示すタイムスタンプとなっている。また第1実施形態において、第3の認証要求に含まれる優先度1515は、夫々の第3の認証要求に含まれる認証要求サービス1511に紐づく優先度1522と等しい。そのため、図4に示すように、同一の優先度1515が付与された認証要求が存在する。

#### 【0036】

認証要求量154は、認証要求リスト151に格納されている認証要求の数を示す。例えば、図4に示す認証要求リスト151の場合、認証要求量154は「3」である。

#### 【0037】

図5は、認証待機リスト153の一例を示す図である。図5に示す認証待機リスト153の1つのエントリが、1つの第2の認証要求を示す。認証待機リスト153には、認証要求サービス1511、認証ID1512、パスワード1513および受領番号1514が関連付けられている。つまり、第2の認証要求は、認証要求サービス1511、認証ID1512、パスワード1513および受領番号1514を含む。

#### 【0038】

##### （選択部13）

選択部13は、認証部14が認証を行う第3の認証要求を選択する。具体的に選択部13は、認証要求リスト151に格納されている第3の認証要求のうち、最も高い優先度を含む第3の認証要求を選択し、選択した第3の認証要求を認証部14に送信する。

#### 【0039】

##### （認証部14）

認証部14は、選択部13から送信された第3の認証要求に対し認証を行う。具体的に、認証部14は、一般的な手法を用いて、クライアント端末40と、クライアント端末50とがサーバ20またはサーバ30が提供するサービスを利用する権限を有しているか否かを判定する。

#### 【0040】

##### （確認部12）

確認部12は、第2の認証要求を判定部11に送信する。上述したように、認証部14は、第3の認証要求に含まれる優先度1515に応じて認証を行う。第2の認証要求は優先度1515を含まないため、認証部14によって認証されない。そのため、確認部12は、再度判定部11が優先度1515を付与するか否かを判定するように、第2の認証要求を判定部11に送信する。

#### 【0041】

図6は、判定部11の動作の一例を示すフローチャートである。判定部11は、認証要求を受け付ける（ステップS401）。具体的に判定部11は、サーバ20またはサーバ30から第1の認証要求を受け付ける、または確認部12から第2の認証要求を受け付ける。

#### 【0042】

判定部11は、受け付けた認証要求に、受領番号1514が付与されているか否かを判定する（ステップS402）。具体的に、判定部11は、受け付けた認証要求が、第1の認証要求または第2の認証要求かを判定する。サーバ20またはサーバ30から受け付けた第1の認証要求は、図2に示すとおり受領番号1514を含まない。一方で、確認部12

10

20

30

40

50

から受け付けた第2の認証要求は、図5に示すとおり受領番号1514を含む。そのため、第1の認証要求の場合、処理はステップS402にてNOとなり、第2の認証要求の場合、処理はステップS402にてYESとなる。

【0043】

受け付けた認証要求に受領番号1514が付与されている場合（ステップS402にてYES）、すなわち、受け付けた認証要求が第2の認証要求の場合、処理はステップS404に進む。

【0044】

一方で、受け付けた認証要求に受領番号1514が付与されていない場合（ステップS402にてNO）、すなわち、判定部11が受け付けた認証要求が第1の認証要求の場合、処理はステップS403に進む。そして、判定部11は、受け付けた第1の認証要求に受領番号1514を付与する（ステップS403）。ステップS403の処理によって、第1の認証要求は第2の認証要求となる。

【0045】

判定部11は、優先度判定データベース152を参照し、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522を確認する（ステップS404）。そして、判定部11は、認証要求量154が閾値以下であるか否か判定する（ステップS405）。

【0046】

認証要求量154が閾値より多い場合（ステップS405にてNO）、判定部11は、ステップS404にて確認した認証要求サービス1511に紐づく優先度1522が閾値以下であるか否か判定する（ステップS409）。

【0047】

優先度1522が閾値以下である場合（ステップS409にてYES）、または認証要求量154が閾値以下である場合（ステップS405にてYES）、判定部11は、第2の認証要求に、ステップS404で確認した認証要求サービス1511に紐づく優先度1522を、認証要求に対する優先度1515として付与する（ステップS406）。ステップS406の処理によって、第2の認証要求は第3の認証要求となる。判定部11は、認証要求サービス1511に紐づく優先度1522を、認証要求に対する優先度1515として付与する。これにより、認証要求に対する優先度1515を新たに算出し、算出した優先度1515を認証要求に付与する場合に比べ、認証装置10は優先度1515を付与する処理の速度を上げることができる。

【0048】

そして、判定部11は、第3の認証要求を認証要求リスト151に格納する（ステップS407）。ステップS407の処理によって、認証要求リスト151に格納されている第3の認証要求の数が増えるため、判定部11は、認証要求量154を更新する（ステップS408）。そして、処理は終了する。

【0049】

優先度1522が閾値より大きい場合（ステップS409にてNO）、判定部11は、認証待機の応答をステップS401で受け付けた認証要求を送信した送信元に、返却する（ステップS410）。具体的に、ステップS401で受け付けた認証要求が第1の認証要求の場合、判定部11は、ステップS410において、サーバ20またはサーバ30に、認証待機の応答を返却する。また、ステップS401で受け付けた認証要求が第2の認証要求の場合、判定部11は、ステップS410において、確認部12に認証待機の応答を返却する。その後、判定部11は、第2の認証要求を認証待機リスト153に格納する（ステップS411）。そして、処理は終了する。

【0050】

図7は、選択部13の動作の一例を示すフローチャートである。選択部13は、以下に示す動作を定期的に行う。選択部13は、認証要求リスト151に第3の認証要求が格納されているか否か判定する（ステップS501）。認証要求リスト151に第3の認証要

10

20

30

40

50

求が格納されていない場合（ステップ S 5 0 1 にて N O）、処理は終了する。

【0051】

一方で、認証要求リスト 1 5 1 に第 3 の認証要求が格納されている場合（ステップ S 5 0 1 にて Y E S）、選択部 1 3 は、認証要求リスト 1 5 1 に格納されている第 3 の認証要求のうち、最も高い優先順位に対応する優先度（以下、最も高い優先度と呼ぶ）を含む第 3 の認証要求を選択する（ステップ S 5 0 2）。

【0052】

そして、選択部 1 3 は、ステップ S 5 0 2 にて選択した最も高い優先度を含む第 3 の認証要求が複数であるか否か判定する（ステップ S 5 0 3）。最も高い優先度を含む第 3 の認証要求が複数でない場合（ステップ S 5 0 3 にて N O）、つまり、最も高い優先度を含む第 3 の認証要求が 1 つである場合、処理はステップ S 5 0 5 に進む。

10

【0053】

一方で、最も高い優先度を含む第 3 の認証要求が複数である場合（ステップ S 5 0 3 にて Y E S）、選択部 1 3 は、最も高い優先度を含む複数の第 3 の認証要求のうち、最も古い受領番号 1 5 1 4 を含む第 3 の認証要求を選択する（ステップ S 5 0 4）。本実施形態において受領番号 1 5 1 4 はタイムスタンプであり、同一の番号となることはない。したがって、ステップ S 5 0 4 において、最も高い優先度を含む第 3 の認証要求が複数である場合でも、選択部 1 3 はタイムスタンプである受領番号 1 5 1 4 を参照することによって、1 つの第 3 の認証要求を選択することができる。そして処理はステップ S 5 0 5 に進む。

20

【0054】

選択部 1 3 は、ステップ S 5 0 2 またはステップ S 5 0 4 にて選択した 1 つの第 3 の認証要求を認証部 1 4 に送信する（ステップ S 5 0 5）。その後、処理はステップ S 5 0 1 に進む。

【0055】

以上の処理によって、ステップ S 5 0 5 にて選択部 1 3 から送信された第 3 の認証要求に対し、認証部 1 4 は認証を行う。

【0056】

例えば判定部 1 1 は、定期的に変換部 1 3 に図 7 に示す動作を行うように指示を送信してもよい。そして変換部 1 3 は、判定部 1 1 からの指示に基づき、図 7 に示す動作を行ってもよい。また、変換部 1 3 が定期的に変換部 7 に示す動作を実行してもよい。

30

【0057】

図 8 は、確認部 1 2 の動作の一例を示すフローチャートである。確認部 1 2 は、以下に示す動作を定期的に行う。確認部 1 2 は、認証待機リスト 1 5 3 に第 2 の認証要求が格納されているか否か判定する（ステップ S 6 0 1）。認証待機リスト 1 5 3 に第 2 の認証要求が格納されていない場合（ステップ S 6 0 1 にて N O）、処理は終了する。

【0058】

一方で、認証待機リスト 1 5 3 に第 2 の認証要求が格納されている場合（ステップ S 6 0 1 にて Y E S）、確認部 1 2 は、記憶部 1 5 から認証要求量 1 5 4 を取得する（ステップ S 6 0 2）。そして、確認部 1 2 は、認証要求量 1 5 4 が閾値以下であるか否か判定する（ステップ S 6 0 3）。認証要求量 1 5 4 が閾値より多い場合（ステップ S 6 0 3 にて N O）、処理は終了する。

40

【0059】

認証要求量 1 5 4 が閾値以下である場合（ステップ S 6 0 3 にて Y E S）、確認部 1 2 は、認証待機リスト 1 5 3 に格納されている第 2 の認証要求のうち、最も古い受領番号 1 5 1 4 を含む第 2 の認証要求を選択する（ステップ S 6 0 4）。そして、確認部 1 2 は、ステップ S 6 0 4 にて選択した第 2 の認証要求を、判定部 1 1 に送信する（ステップ S 6 0 5）。そして、処理はステップ S 6 0 1 に進む。

【0060】

なお、ステップ S 6 0 5 にて確認部 1 2 から送信された第 2 の認証要求に対し、判定部

50

1 1 は図 6 に示す処理を行う。

【0061】

第 2 の認証要求に含まれる認証要求サービス 1 5 1 1 に紐づく優先度が閾値を超える第 2 の認証要求は、優先度 1 5 1 5 が付与されることなく、認証待機リスト 1 5 3 に格納される。例えば、大量の認証要求を受け付けた場合、判定部 1 1 が受け付けた全ての認証要求に対し優先度 1 5 1 5 の付与を行ってから、認証要求を認証要求リスト 1 5 1 と認証待機リスト 1 5 3 とに振り分けると、認証装置 1 0 にとって優先度の付与が認証処理の応答性を低下させる場合がある。よって、認証装置 1 0 は、認証要求サービス 1 5 1 1 に紐づく優先度が閾値を超える第 2 の認証要求に優先度を付与することなく認証待機リスト 1 5 3 に格納することで、例えば、大量の認証要求を受け付けた場合でも、認証処理の応答性を低下させずに優先度の付与を行うことができる。

10

【0062】

判定部 1 1 は、認証要求量 1 5 4 が閾値以下の場合、第 2 の認証要求に含まれる認証要求サービス 1 5 1 1 に紐づく優先度 1 5 2 2 に関係なく、優先度 1 5 1 5 を付与する。例えば、判定部 1 1 が第 2 の認証要求に含まれる認証要求サービス 1 5 1 1 に紐づく優先度 1 5 2 2 が閾値より小さい場合にのみ、第 2 の認証要求に優先度 1 5 1 5 を付与するとする。例えば、すべての第 2 の認証要求に含まれる認証要求サービス 1 5 1 1 に紐づく優先度 1 5 2 2 が閾値より大きい場合、認証リスト 1 5 1 に第 3 の認証要求が 1 つもなくなる可能性がある。よって、判定部 1 1 が認証リスト 1 5 1 内の第 3 の認証要求の数である認証要求量 1 5 4 に応じて、第 2 の認証要求に優先度 1 5 1 5 を付与することで、認証部 1 4 は効率よく認証を行うことができる。

20

【0063】

認証システム 1 に含まれるサーバは、1 つでもよいし 3 つ以上でもよい。また、認証システム 1 に含まれるクライアント端末は、1 つでもよいし 3 つ以上でもよい。また、例えば、サーバ 2 0 またはサーバ 3 0 は 2 つ以上のサービスを提供してもよい。

【0064】

クライアント端末 4 0 またはクライアント端末 5 0 は、1 つまたは 2 つ以上のサービスを利用してもよい。

【0065】

また、認証装置 1 0 は、サービスを提供するサーバ 2 0 またはサーバ 3 0 に含まれるように構成されていてもよい。

30

【0066】

第 1 の認証要求に付与される受領番号 1 5 1 4 は、タイムスタンプでなくともよい。判定部 1 1 は、第 1 の認証要求を受け付けた順に 1、2、3、…、N（N：自然数）の番号を受領番号 1 5 1 4 として付与してもよい。受領番号 1 5 1 4 は、判定部 1 1 が受け付けた順序がわかるように付与されていればよい。

【0067】

この場合、確認部 1 2 はステップ S 6 0 4 にて、複数の第 2 の認証要求のうち、最も値の小さい受領番号 1 5 1 4 を含む第 2 の認証要求を選択すればよい。同様に選択部 1 3 は、ステップ S 5 0 4 にて、複数の第 3 の認証要求のうち、最も値の小さい受領番号 1 5 1 4 を含む第 3 の認証要求を選択すればよい。

40

【0068】

また、ステップ S 4 0 6 にて確認した認証要求サービス 1 5 1 1 に紐づく優先度 1 5 2 2 が閾値より大きい場合、判定部 1 1 は、ステップ S 4 1 0 の処理ではなく、ステップ S 4 1 1 の処理を先に行ってもよい。

【0069】

また、認証待機の応答をどのように扱うかは、各サーバまたは各クライアント端末側にて判断することができる。たとえば、各サーバは、認証待機の応答を受信した場合、各クライアント端末に対して一定時間待ち合わせる旨を示すメッセージを送信してもよい。そして、クライアント端末は受信した該メッセージを表示してもよい。

50

## 【0070】

また、認証部14は、認証が終了した場合、認証が終了したことを示す通知を、認証要求の要求元に送信してもよい。

## 【0071】

また、各サーバまたは各クライアント端末は、認証待機の応答を受信した場合、処理を中断（タイムアウト）してもよい。なお、ステップS409の処理は、必要に応じて、任意で実行することが可能である。

## 【0072】

このように判定部11が、受け付けた認証要求に受領番号1514を付与し、受け付けた認証要求に含まれる認証要求サービス1511に紐づく優先度1522を、該認証要求に対する優先度1515として、該認証要求に付与することで認証要求の認証の優先順位が設定される。これにより、選択部13は、認証の優先順位に基づき、認証部14が認証を行う認証要求を1つずつ選択し、認証部14に送信する。このため、認証部14は選択部13から送信された認証要求に対し、認証を行うことができる。これによって認証装置10は一台の計算機の中で効率良く認証を行うことができる。

## 【0073】

（変形例1）

ここで、第1実施形態に適用できる変形例を説明する。第1実施形態においては、判定部11は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522を、認証要求に対する優先度1515として第2の認証要求に付与する。変形例1では、判定部11は、登録パスワードの安全性を評価し、評価した結果を、認証要求に対する優先度付与に用いる。変形例1において、記憶部15は、パスワードの安全性に関する情報を含む安全性リスト155を記憶する。

## 【0074】

図9は、安全性リスト155の一例を示す図である。安全性リスト155は、認証ID1512と、パスワードの安全性に対する評価値であるパスワード評価値1552とを含む。そして、認証ID1512と、パスワード評価値1552とは紐づけられている。

## 【0075】

パスワード評価値1552は、各クライアントによって予め登録されたパスワードである登録パスワードの安全性を判定部11が評価し、評価した結果に基づいて付与された値である。例えば、登録パスワードは、各クライアントが登録パスワードを設定した際に、判定部11によって評価される。なお、判定部11が、登録パスワードの安全性を評価する方法は一般的な方法である。

## 【0076】

判定部11は、例えば、登録パスワードの文字数と閾値とを比較することによって登録パスワードの安全性を評価してもよい。図9に示す安全性リスト155においては、安全性が高いと評価された登録パスワードほど、小さい値が付与されているとする。

## 【0077】

変形例1において判定部11は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522の代わりに、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522と、安全性リスト155に格納されている、第2の認証要求に含まれる認証ID1512に紐づくパスワード評価値1552とを用いて、認証要求に対する優先度を付与する。

## 【0078】

例えば、判定部11は、安全性リスト155を参照する。そして、判定部11は、第2の認証要求に含まれる認証ID1512に紐づくパスワード評価値1552を取得する。その後、判定部11は、認証要求サービス1511に紐づく優先度1522と、認証ID1512に紐づくパスワード評価値1552とを掛け合わせるによって算出した値を認証要求に対する優先度として、第2の認証要求に付与する。なお認証要求に対する優先度は、小さい値となるほど、優先度が高くなるとする。

## 【0079】

図10は、変形例1における認証要求リスト251の一例を示す図である。認証要求リスト251は、変形例1において認証要求リスト151に代わり記憶部15に記憶されている。認証要求リスト251は、認証要求サービス1511、認証ID1512、パスワード1513、受領番号1514および認証要求に対する優先度2515を含む。

## 【0080】

優先度2515は、図3に示す優先度判定データベース152に格納されている認証要求サービス1511に紐づく優先度1522と、認証ID1512に紐づくパスワード評価値1552とを掛け合わせた値であり、認証要求に対する優先度を示す。

## 【0081】

また図9に示す安全性リスト155を参照すると、認証ID1512が「ID1」のパスワード評価値1552は「3」である。また、認証ID1512が「ID3」のパスワード評価値1552は「1」である。

## 【0082】

図3に示す優先度判定データベース152を参照すると、認証要求サービス1511の「メール」に紐づく優先度1522は「1」である。また、認証要求サービス1511の「HTTP」に紐づく優先度1522は「2」である。よって、認証ID1512が「ID1」の優先度2515は、パスワード評価値1552の「3」と優先度1522の「1」とを掛け合わせるによって算出された「3」である。また、認証ID1512が「ID3」の優先度2515は、パスワード評価値1552の「1」と優先度1522の「2」とを掛け合わせるによって算出された「2」となる。

## 【0083】

図9に示すとおり、パスワード評価値1552が「1」である認証ID1512が「ID3」の第3の認証要求は、パスワード評価値1552が「2」である認証ID1512が「ID2」の第3の認証要求よりも高い優先度となっている。選択部13は、第3の認証要求に含まれる優先度2525に応じて、認証部14に第3の認証要求を送信するため、第3の認証要求を受け付けた順序と、認証が行われる順序とが異なることとなる。

## 【0084】

パスワードは、複雑性や文字数等に応じて、安全性の高低が変化する。よって、安全性の低いパスワードは、悪意のあるクライアントによる総当たり攻撃であるブルートフォース

## 【0085】

このため、登録パスワードの安全性が低い認証要求に対し、低い優先度を付与することで、登録パスワードの安全性が低いクライアントが使用するクライアント端末からの認証要求は優先度が低くなる。これによって、各クライアントが優先的にサービスの提供を受けるために安全性が高い登録パスワードに設定することが期待できる。認証装置10は、各クライアントに安全性の高い登録パスワードにさせることで、悪意のあるクライアントによる総当たり攻撃の回数を低減させ、サービス不正利用の危険性を低減させることができる。また、登録パスワードの安全性が高い認証要求に対し、高い優先度を付与することで、安全性の高いパスワードを設定したクライアントが優先的に認証される。例えば、サービス提供者は、クライアントに安全性の高いパスワードを設定するように促すことで、安全性の低いパスワードを設定するクライアントを削減することができる。

## 【0086】

(変形例2)

変形例1では、判定部11は、登録パスワードの安全性を評価し、パスワード評価値1552を、認証要求に対する優先度付与に用いた。本変形例においては、判定部11は、第2の認証要求に含まれるパスワード1513（入力されたパスワード）の安全性を評価し、評価した結果と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対し優先度を付与する。ここで、判定部11がパスワード1513を評価し、評価した結果として出力する、パスワードの安全性を評価

10

20

30

40

50

した値について説明する。

【0087】

図11は、パスワード評価リスト111の一例を示す図である。パスワード評価リスト111は、パスワードの安全性1111と、安全値1112を含む。パスワードの安全性1111と、安全値1112とは紐づけられている。

【0088】

パスワードの安全性1111は、パスワード1513に対する安全性の高低の度合いを示す。安全値1112はパスワード1513に対する安全性の高低の度合いに応じて、パスワードの安全性1111に対して付与された値を示す。

【0089】

例えば判定部11が第2の認証要求に含まれるパスワード1513の安全性を評価した結果、第2の認証要求に含まれるパスワード1513の安全性が「高」である場合、判定部11は、パスワード評価リスト111からパスワードの安全性1111の「高」に紐づく安全値1112の「1」を取得する。また例えば判定部11が第2の認証要求に含まれるパスワード1513の安全性を評価した結果、第2の認証要求に含まれるパスワードの安全性が「低」である場合、判定部11は、パスワード評価リスト111からパスワードの安全性1111の「低」に紐づく安全値1112の「3」を取得する。判定部11は、図12に示すパスワード評価リスト111をあらかじめ記憶していてもよい。また判定部11は、パスワード1513の複雑性および／または文字数等に応じて、パスワード1513に対する安全性を評価してもよい。

【0090】

パスワード1513は第1の認証要求に含まれるため、変形例2における記憶部15は、安全性リスト155を記憶しなくともよい。そのかわり判定部11が、第2の認証要求に含まれるパスワード1513の安全性を評価した値と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、認証要求に対する優先度を求める。具体的に図12を用いて、変形例2における判定部11の動作を説明する。

【0091】

図12は、変形例2における判定部11の動作の一例を示すフローチャートである。図12に示すステップS701～ステップS711の処理は、図6に示すステップS401～ステップS411の処理に対応するため、説明を省略する。本変形例ではステップS706の前に、第2の認証要求に含まれるパスワードを評価する。

【0092】

優先度1522が閾値以下である場合（ステップS709にてYES）または認証要求量154が閾値以下である場合（ステップS705にてYES）、判定部11は第2の認証要求に含まれるパスワード1513の安全性を評価する（ステップS712）。そして判定部11は、評価したパスワード1513の安全性を用いて、後述するパスワード評価リスト111を参照し、パスワード1513の安全性に紐づく値を取得する（ステップS713）。その後、判定部11は、ステップS713にて取得したパスワード1513の安全性に紐づく値と、認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対する優先度を算出する（ステップS714）。そして、判定部11はステップS714にて算出した優先度を付与する（ステップS706）。なお、判定部11は、ステップS712にて評価したパスワード1513の安全性を、第2の認証要求に付与してもよい。

【0093】

図13は、変形例2における認証要求リスト351の一例を示す図である。認証要求リスト351は、変形例2において認証要求リスト151に代わり記憶部15に記憶されている。認証要求リスト351は、認証要求サービス1511、認証ID1512、パスワード1513、パスワードの安全性1111、受領番号1514および認証要求に対する優先度3515を含む。パスワードの安全性1111は、判定部11によって評価されたパスワード1513の安全性である。

## 【0094】

優先度3515は、第2の認証要求に付与された優先度を示す。また、優先度3515は、第2の認証に含まれるパスワード1513（入力されたパスワード）の安全性を評価した値である安全値1112と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを掛け合わせた値である。

## 【0095】

図13に示す認証要求リスト351を参照すると、認証ID1512が「ID1」の第3の認証要求のパスワードの安全性1111は「低」である。また、認証ID1512が「ID2」の第3の認証要求のパスワードの安全性1111は「中」である。認証ID1512が「ID3」のパスワードの安全性1111が「高」である。

10

## 【0096】

したがって、認証ID1512が「ID1」の優先度3515は、パスワードの安全性1111の「低」に紐づく安全値1112の「3」と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522の「1」とを掛け合わせた「3」となる。また、認証ID1512が「ID2」の認証要求の優先度3515は、パスワードの安全性1111の「中」に紐づく安全値1112の「2」と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522の「2」とを掛け合わせた「4」となる。そして、認証ID1512が「ID3」の優先度3515は、パスワードの安全性1111の「高」に紐づく安全値1112の「1」と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522の「1」とを掛け合わせて算出された「1」となる。

20

## 【0097】

認証要求リスト351を参照すると、パスワードの安全性1111が低い認証ID1512が「ID1」の第3の認証要求は、パスワードの安全性1111が高い認証ID1512が「ID2」の第3の認証要求よりも低い優先度となる。これにより、認証要求を受け付けた順序と認証が行われる順序とが異なることとなる。

## 【0098】

このため、パスワードの安全性が低い認証要求に対し、低い優先度を付与することで、パスワードの安全性が低いクライアントが使用するクライアント端末からの認証要求は優先度が低くなる。これによって、クライアントが優先的にサービスの提供を受けるために安全性が高いパスワードに設定することが期待できる。認証装置10は、クライアントに安全性の高いパスワードにさせることで、悪意のあるクライアントによる総当たり攻撃の回数を低減させ、サービス不正利用の危険性を低減させることができる。また、パスワードの安全性が高い認証要求に対し、高い優先度を付与することで、安全性の高いパスワードを設定したクライアントが優先的に認証される。例えば、サービス提供者は、クライアントに安全性の高いパスワードを設定するように促すことで、安全性の低いパスワードを設定するクライアントを削減することができる。

30

## 【0099】

（変形例3）

変形例2においては、判定部11は、第2の認証要求に含まれるパスワード1513（入力されたパスワード）の安全性を評価し、評価した結果と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを認証要求に対する優先度の付与に用いた。変形例3においては、判定部11は、認証ID1512ごとの認証処理の結果を評価し、評価した結果と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対し優先度を付与する。

40

## 【0100】

図14は、変形例3に係る認証装置100の構成の一例を示す機能ブロック図である。認証装置100は、判定部21と、確認部12と、選択部13と、認証部24と、記憶部15とを備える。また認証装置100は、第1実施形態に係る認証装置10と比べて、判定部11に相当する判定部21と認証部14に相当する認証部24とが接続している。また、認証部24と記憶部15とが接続している。また記憶部15は、後述する連続リスト

50

156を記憶する。また、記憶部15は、認証要求リスト151に代わり認証要求リスト451を記憶する。

【0101】

認証部24は、認証部14の機能を有する。また認証部24は、第3の要求に対する認証処理が連続で成功した回数を認証ID1512ごとにカウントする。また認証部24は、第3の要求に対する認証処理が連続で失敗した回数を認証ID1512ごとにカウントする。そして、認証部24は、認証処理が連続で成功した回数と、認証処理が連続で失敗した回数とを記憶部15に記憶させる。判定部21は判定部11の機能を有する。

【0102】

図15は、連続リスト156の一例を示す図である。連続リスト156は、認証ID1512と、連続成功回数1562と、連続失敗回数1563と、連続評価値1564とを含む。

10

【0103】

第3の認証要求に対する認証部14の認証処理が連続で成功した回数を示す連続成功回数1562と、認証要求に対する認証部14の認証処理が連続で失敗した回数を示す連続失敗回数1563と、連続評価値1564とを含む。

【0104】

連続成功回数1562は、第3の要求に対する認証処理が連続で成功した回数を示す。連続失敗回数1563は、第3の要求に対する認証処理が連続で失敗した回数を示す。

【0105】

連続評価値1564は、連続成功回数1562と連続失敗回数1563とを用いて、判定部11が認証ID1512に紐づくクライアントの信頼度を評価した値である。具体的に、連続評価値1564は、基準値から連続成功回数1562を減算した値に、連続失敗回数1563を加算した値である。なお、図14に示す連続リスト156において、連続成功回数1562と連続失敗回数1563との初期値は「0」とする。また、基準値は「10」とする。

20

【0106】

連続評価値1564は、値が小さいほど信頼度の高いクライアントとする。そして連続評価値1564の値が小さいほど、判定部11によって、高い優先度が付与される。なお、基準値は「10」でなくともよく、判定部11が優先度1522と連続評価値1564とを掛け合わせて優先度を求められるように、連続評価値1564が負数とならないような値であればよい。

30

【0107】

図16は、変形例3における認証要求リスト451の一例を示す図である。認証要求リスト451は、変形例3において認証要求リスト151に代わり記憶部15に記憶されている。認証要求リスト451は、認証要求サービス1511、認証ID1512、パスワード1513、受領番号1514および優先度4515を含む。

【0108】

優先度4515は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522と、第2の認証要求に含まれる認証ID1512に紐づく連続評価値1564とを掛け合わせた値である。

40

【0109】

例えば、認証ID1512が「ID1」の場合、優先度4515は、第2の認証要求に含まれる認証要求サービス1511の「メール」に紐づく優先度1522の「1」と、認証ID1512が「ID1」に紐づく連続評価値1564の「12」とを掛け合わせることで算出された「12」となる。

【0110】

認証要求リスト451を参照すると、認証の失敗が連続している認証ID1512が「ID1」の第3の認証要求は、認証の成功が連続している認証ID1512が「ID3」の第3の認証要求よりも低い優先度4515となる。よって、認証要求を受け付けた順序

50

と認証が行われる順序が異なることとなる。

#### 【0111】

認証要求は正当な目的で利用される限り、認証が成功する回数が失敗する回数よりも多くなるという特性がある。この特性を利用して、認証が連続して成功した回数と連続して失敗した回数とを記録しておき、成功が続いているクライアントについては信頼度が高いとして、判定部11は高い優先度を付与する。

#### 【0112】

一方で失敗が続いているクライアントについては、悪意をもったクライアントである危険性があるため、判定部11は、低い優先度を付与する。判定部11は、このように優先度を付与することで、信頼度の高いクライアントからの認証要求の優先順位を高くし、信頼度の低いクライアントからの認証要求の優先順位を低くする。これにより、認証装置100は、不正利用の危険性を低減させることが出来る。

#### 【0113】

なお、認証部24は、一定期間、特定の認証ID1512を含む第3の認証要求に対し認証処理をしなかった場合、該特定の認証ID1512に紐づく連続成功回数と、連続失敗回数とのカウントをリセットしてもよい。

#### 【0114】

(変形例4)

変形例4においては、判定部11は、クライアント端末のIP(Internet Protocol)アドレスに対する優先度と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対し優先度を付与する。

#### 【0115】

変形例4において、判定部11が各サーバから受け付ける第1の認証要求には、認証要求サービス1511と、認証ID1512と、パスワード1513とに加え、クライアント端末のIPアドレスが含まれる。

#### 【0116】

また、変形例4において、記憶部15は、アドレスリスト157を記憶する。図17は、アドレスリスト157の一例を示す図である。アドレスリスト157には、IPアドレスのネットワークアドレス部1571と、ネットワークアドレス部1571に対する優先順位を示す優先度1572とが紐づいて格納されている。

#### 【0117】

具体的に、ネットワークアドレス部1571が「a. b. c」となるネットワークは信頼度が低いとして優先度1572を「3」と設定している。また、ネットワークアドレス部1571が「x. y. z」となるネットワークは信頼性が高いとして優先度1572を「1」と設定している。なお、ネットワークアドレス部1571が「a. b. c」と「x. y. z」とのどちらでもないネットワークは、優先度1572を「2」と設定している。つまり、ネットワークの信頼度が高いほど、優先度1572の値は小さくなるとする。

#### 【0118】

図18は、変形例4における認証要求リスト551の一例を示す図である。認証要求リスト551は、変形例4において認証要求リスト151に代わり記憶部15に記憶されている。認証要求リスト551は、認証要求サービス1511、認証ID1512、パスワード1513、クライアント端末のIPアドレス5511と、受領番号1514および認証要求に対する優先度5515を含む。IPアドレス5511は、上述したとおり、変形例4における第1の認証要求に含まれる。つまり第1の認証要求は、認証要求サービス1511、認証ID1512、パスワード1513およびIPアドレス5511を含む。そして、変形例4における第2の認証要求は、上述した第1の認証要求に受領番号1514が付与されたものである。

#### 【0119】

優先度5515は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522と、第2の認証要求に含まれるIPアドレス5511のネットワークアドレス

10

20

30

40

50

部 1 5 7 1 に紐づく優先度 1 5 7 2 とを掛け合わせた値である。

【0 1 2 0】

具体的に、認証 ID 1 5 1 2 が「ID 1」の IP アドレス 5 5 1 1 は「a. b. c. d」である。図 1 8 を参照すると、ネットワークアドレス部「a. b. c」に紐づく優先度 1 5 7 2 は「3」である。そのため、認証 ID 1 5 1 2 が「ID 1」の第 3 の認証要求の IP アドレス「a. b. c. d」に対する優先度 1 5 7 2 は「3」となる。

【0 1 2 1】

また、図 3 に示す優先度判定データベース 1 5 2 を参照すると、メールサービスに紐づく優先度 1 5 2 2 は「1」である。よって、ネットワークアドレス部「a. b. c」に紐づく優先度 1 5 7 2 は「3」とメールサービスに紐づく優先度 1 5 2 2 の「1」とを掛け合わせ算出された「3」が、認証 ID 1 5 1 2 が「ID 1」の第 3 の認証要求の優先度 5 5 1 5 となる。

10

【0 1 2 2】

このように信頼度の低いネットワークから接続されている認証 ID 1 5 1 2 が「ID 1」の第 3 の認証要求は、信頼度の高いネットワークから接続されている認証 ID 1 5 1 2 が「ID 3」の第 3 の認証要求よりも低い優先度となる。したがって、認証要求を受け付けた順序と認証が行われる順序とが異なることとなる。

【0 1 2 3】

夫々のクライアントがサービスをインターネット経由で利用する場合、認証装置 1 0 は、夫々のクライアント端末が持つ IP アドレス 5 5 1 1 に基づき、夫々のクライアント端末が存在する国または所属するネットワークを識別することができる。よって、認証システム 1 は、危険性の高い国またはネットワークに属する IP アドレスを持つクライアント端末を特定し、特定したクライアント端末から送信された認証要求に対する優先度を低くすることによって、不正利用の危険性を低減させることが出来る。

20

【0 1 2 4】

(変形例 5)

変形例 5 においては、判定部 1 1 は、R T T (Round Trip Time) に関する情報と、第 2 の認証要求に含まれる認証要求サービス 1 5 1 1 に紐づく優先度 1 5 2 2 とを用いて、第 2 の認証要求に対し優先度を付与する。

【0 1 2 5】

本変形例において、R T T とは、T C P / I P (Transmission Control Protocol / Internet Protocol) において、ネットワーク通信の接続を確立するための手順であるスリーウェイ・ハンドシェイクに要した時間を示す。

30

【0 1 2 6】

変形例 5 において、判定部 1 1 が各サーバから受け付ける第 1 の認証要求には、認証要求サービス 1 5 1 1 と、認証 ID 1 5 1 2 と、パスワード 1 5 1 3 とに加え、R T T に関する情報が含まれる。

【0 1 2 7】

図 1 9 は、変形例 5 における認証要求リスト 6 5 1 の一例を示す図である。認証要求リスト 6 5 1 は、変形例 5 において認証要求リスト 1 5 1 に代わり記憶部 1 5 に記憶されている。認証要求リスト 6 5 1 は、認証要求サービス 1 5 1 1、認証 ID 1 5 1 2、パスワード 1 5 1 3、R T T 6 5 1 1、受領番号 1 5 1 4 および認証要求に対する優先度 6 5 1 5 を含む。

40

【0 1 2 8】

R T T 6 5 1 1 は、クライアント端末と、サーバ 2 0 またはサーバ 3 0 とのネットワーク通信の接続を確立するための手順であるスリーウェイ・ハンドシェイクに要した時間を示す。また R T T 6 5 1 1 は、変形例 5 における第 1 の認証要求に、R T T に関する情報として含まれる。つまり変形例 5 における第 1 の認証要求は、認証要求サービス 1 5 1 1、認証 ID 1 5 1 2、パスワード 1 5 1 3 および R T T 6 5 1 1 を含む。そして、変形例

50

5における第2の認証要求は、上述した第1の認証要求に受領番号1514が付与されたものである。

【0129】

優先度6515は、第2の認証要求に付与された優先度である。具体的に、優先度6515は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522と、第2の認証要求に含まれるRTT6511の値とを掛け合わせた値である。

【0130】

例えば、認証ID1512が「ID1」の場合、判定部11は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522の「1」と、第2の認証要求に含まれるRTT6511の値「15」とを掛け合わせて優先度6515を求める。よって、認証ID1512が「ID1」の第3の認証要求に含まれる優先度6515は「15」となる。

10

【0131】

また認証ID1512が「ID3」の場合、判定部11は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522の「1」と、第2の認証要求に含まれるRTT6511の値「5」とを掛け合わせて優先度6515を求める。よって、認証ID1512が「ID3」の第3の認証要求に含まれる優先度6515は「5」となる。

【0132】

このように、RTT6511が「15ms」を含む認証ID1512が「ID1」の第3の認証要求は、RTT6511が「5ms」を含む認証ID1512が「ID3」の第3の認証要求よりも低い優先度となる。よって、認証要求を受け付けた順序と認証が行われる順序が異なることとなる。

20

【0133】

クライアントがインターネットを介してサーバが提供するサービスを利用する場合、ネットワークの距離に応じて、サービスを提供するサーバとクライアント端末とのネットワーク通信が確立するまでに要する時間(RTT)は変化する。判定部11が、より短いRTTで接続が確立するクライアント端末の認証要求に対し、高い優先度を付与することによって、ネットワークの応答性が、サービスの応答性に反映される。よって変形例5に係る認証システム1によれば、高い応答性をもつネットワークを利用するクライアント端末に対し、高い応答性を持つサービスを提供することができる。

30

【0134】

(変形例6)

変形例6においては、判定部11は、パスワード入力のレイテンシと、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対し優先度を付与する。

【0135】

変形例6において、パスワード入力のレイテンシとは、各サーバが各クライアント端末に対してパスワードの入力を要求してから、実際にクライアント端末から各サーバにパスワードが送信されるまでの時間を示す。判定部11は、各サーバが各クライアント端末にパスワードの入力を要求する際、各サーバが各クライアント端末にパスワードを要求した時刻と、各クライアント端末から各サーバにパスワードが送信された時刻とを測定し、夫々の時刻の差分を求めることによってパスワード入力のレイテンシを取得できる。

40

【0136】

また、変形例6において、判定部11が各サーバから受け付ける第1の認証要求には、認証要求サービス1511と、認証ID1512と、パスワード1513とに加え、上述したパスワード入力のレイテンシが含まれる。

【0137】

図20は、変形例6における認証要求リスト751の一例を示す図である。認証要求リスト751は、変形例6において認証要求リスト151に代わり記憶部15に記憶されている。認証要求リスト751は、認証要求サービス1511、認証ID1512、パsw

50

ード1513、パスワード入力のレイテンシ7511、受領番号1514および優先度7515を含む。パスワード入力のレイテンシ7511は、上述したとおり、変形例6における第1の認証要求に含まれる。つまり第1の認証要求は、認証要求サービス1511、認証ID1512、パスワード1513およびパスワード入力のレイテンシ7511を含む。そして、変形例6における第2の認証要求は、上述した第1の認証要求に受領番号1514が付与されたものである。

#### 【0138】

優先度7515は、認証要求に対する優先度を示す。また優先度7515は、認証要求サービス1511に紐づく優先度1522と、パスワード入力のレイテンシ7511の値とを用いて掛け合わせた値である。

10

#### 【0139】

具体的に、認証ID1512が「ID1」の第3の認証要求は、パスワード入力のレイテンシ7511が「150ms」である。また認証ID1512が「ID1」の認証要求サービス1511は、メールサービスのため、サービスに紐づく優先度1522は「1」となる。したがって、認証ID1512が「ID1」の認証要求に対する優先度7515は、パスワード入力のレイテンシ7511の値「150」と認証要求サービス1511に紐づく優先度1522の「1」とを掛け合わせることで算出された「150」となる。

#### 【0140】

認証要求リスト751を参照すると、パスワード入力のレイテンシ7511が「150ms」の認証ID1512が「ID1」の第3の認証要求は、パスワード入力のレイテンシ7511が「50ms」の認証ID1512が「ID3」の第3の認証要求よりも低い優先度となっている。よって、認証要求を受け付けた順序と認証が行われる順序とが異なることとなる。

20

#### 【0141】

このように、判定部11は、より短時間でパスワード入力された認証要求に対し高い優先度7515を付与する。これによって、クライアントは、より短時間でパスワード入力を行うことで、応答性の高いサービスを利用することが可能となる。

#### 【0142】

(変形例7)

変形例7においては、判定部11は、各クライアント端末が使用しているアプリケーションのバージョンの情報に対する優先度と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対し優先度を付与する。

30

#### 【0143】

変形例7において、判定部11が各サーバから受け付ける第1の認証要求には、認証要求サービス1511と、認証ID1512と、パスワード1513に加え、各クライアント端末が使用しているアプリケーションのバージョンの情報が含まれる。

#### 【0144】

変形例7において、記憶部15は、クライアント端末リスト158を記憶する。図21は、クライアント端末リスト158の一例を示す図である。クライアント端末リスト158は、各クライアント端末が使用しているアプリケーションのバージョンの情報であるクライアント情報1581と、クライアント情報1581に対する優先順位を示す優先度1582とを格納している。クライアント情報1581と、クライアント情報1581に対する優先度1582とは夫々関連付けられている。

40

#### 【0145】

具体的に、クライアント情報1581の「Version2」は、優先度1582の「1」が対応付けられ、クライアント情報1581の「Version1」は、優先度1582の「2」が対応付けられている。また、「Version2」および「Version1」以外のクライアント情報1581は、優先度1582の「3」が対応付けられている。なお、クライアント情報1581に対応付けられている優先度1582は、値が小さいほど優先度が高いことを示すとする。

50

## 【0146】

図22は、変形例7における認証要求リスト851を示す図である。認証要求リスト851は、変形例7において認証要求リスト151に代わり記憶部15に記憶されている。認証要求リスト851は、認証要求サービス1511、認証ID1512、パスワード1513、クライアント情報1581、受領番号1514および認証要求に対する優先度8515を含む。クライアント情報1581は、上述したとおり、変形例7における第1の認証要求に含まれる。つまり第1の認証要求は、認証要求サービス1511、認証ID1512、パスワード1513およびクライアント情報1581を含む。そして、変形例7における第2の認証要求は、上述した第1の認証要求に受領番号1514が付与されたものである。

10

## 【0147】

優先度8515は、認証要求に対する優先度を示す。また、優先度8515は、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522と、第2の認証要求に含まれるクライアント情報1581に対応する優先度1582とを掛け合わせた値である。

## 【0148】

具体的に、認証ID1512が「ID1」の認証要求は、クライアント情報1581の「Version1」と、認証要求サービス1511の「メール」とを含む。したがって、認証ID1512が「ID1」の優先度8515は、クライアント情報1581の「Version1」に紐づく優先度1582の「2」と、認証要求サービス1511の「メール」に紐づく優先度1522の「1」とを掛け合わせた「2」となる。また、認証ID1512が「ID3」の認証要求は、クライアント情報1581の「Version2」と、認証要求サービス1511の「メール」とを含む。したがって、認証ID1512が「ID3」の優先度8515は、クライアント情報1581の「Version2」に紐づく優先度1582の「1」と、認証要求サービス1511の「メール」に紐づく優先度1522の「1」とを掛け合わせるによって算出された「1」となる。

20

## 【0149】

よって、認証要求リスト851に示すとおり、「Version1」を使用している認証ID1512が「ID1」の第3の認証要求は、「Version2」を使用している認証ID1512が「ID3」の第3の認証要求よりも低い優先度となる。よって、認証要求を受け付けた順序と認証が行われる順序とが異なることとなる。

30

## 【0150】

サービスを利用するクライアント端末には様々なアプリケーションやアプリケーションのバージョンが混在することが一般的である。また、様々なアプリケーションやアプリケーションの様々なバージョンによって、応答性やセキュリティの強度は異なる。

## 【0151】

例えば、最新のバージョンのアプリケーションを使用しているクライアント端末であれば、高い応答性および／または強固なセキュリティを持つ可能性が高い。よって、判定部11は、より高い応答性および／または強固なセキュリティを持つ可能性の高いバージョンのアプリケーションを使用するクライアント端末からの接続に対し、より高い優先度を付与する。これによって、変形例7に係る認証システム1によれば、高い応答性の維持および不正利用の危険性を低減させることが出来る。

40

## 【0152】

(変形例8)

変形例8においては、クライアントのバイオメトリクス情報に応じた情報と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対し優先度を付与する。

## 【0153】

変形例8において、クライアントのバイオメトリクス情報は、認証ID1512が示すクライアントの行動的特徴の情報を示す。クライアントの行動的特徴の情報とは、例えば

50

、パスワード入力時におけるタイピングの速度またはタイミングである。クライアントが各クライアント端末に対し、パスワードを設定する際、同じパスワードを何回か入力することで、そのパスワード入力時におけるタイピングの速度またはタイミングを定量化することができる。

#### 【0154】

また、変形例8において、判定部11が各クライアント端末から受け付ける第1の認証要求には、認証要求サービス1511と、認証ID1512と、パスワード1513とに加え、パスワード入力時に取得したクライアントのバイオメトリクス情報が含まれる。

#### 【0155】

変形例8において、記憶部15は、バイオメトリクスリスト159を記憶する。図23は、バイオメトリクスリスト159の一例を示す図である。バイオメトリクスリスト159は、認証ID1512に、予め登録されたバイオメトリクス情報である登録バイオメトリクス情報1592が紐づいている。

#### 【0156】

図24は、変形例8における認証要求リスト951の一例を示す図である。認証要求リスト951は、変形例8において認証要求リスト151に代わり記憶部15に記憶されている。認証要求リスト951は、認証要求サービス1511、認証ID1512、パスワード1513、入力バイオメトリクス情報9511、受領番号1514、類似度9512および認証要求に対する優先度9515を含む。入力バイオメトリクス情報9511は、上述したようにパスワード入力時に取得したクライアントのバイオメトリクス情報を示す。すなわち、変形例8における第1の認証要求は認証要求サービス1511、認証ID1512、パスワード1513および入力バイオメトリクス情報9511を含む。また、変形例8における第2の認証要求は、上述した第1の認証要求に受領番号1514が付与されたものである。

#### 【0157】

類似度9512は、入力バイオメトリクス情報9511と登録バイオメトリクス情報1592とが類似している度合いを示す。また、類似度9512は、判定部11によって、認証ID1512ごとに入力バイオメトリクス情報9511と、登録バイオメトリクス情報1592とを照合することによって算出された値である。すなわち、判定部11は、入力バイオメトリクス情報9511と登録バイオメトリクス情報1592とを照合し、類似度9512を認証ID1512ごとに算出する。そして判定部11は、算出した類似度9512を第2の認証要求に付与する。なお、判定部11は、算出した類似度9512を第2の認証要求に付与しなくともよい。なお、変形例8において、類似度9512は値が小さいほど、入力バイオメトリクス情報9511と登録バイオメトリクス情報1592とが類似していることを示すとする。

#### 【0158】

優先度9515は、認証要求に対する優先度を示す。また、優先度9515は、認証要求サービス1511に紐づく優先度1522と、各認証ID1512に紐づく類似度9512とを掛け合わせた値である。

#### 【0159】

具体的に、認証ID1512が「ID1」に紐づく類似度9512は「3」である。また認証ID1512が「ID1」に紐づく認証要求サービス1511はメールサービスのため、認証要求サービス1511に紐づく優先度1522は「1」となる。したがって、認証ID1512が「ID1」に紐づく優先度9515は、類似度9512の「3」と認証要求サービス1511に紐づく優先度1522の「1」とを掛け合わせた「3」となる。また、認証ID1512が「ID3」に紐づく類似度9512は「1」である。また認証ID1512が「ID3」に紐づく認証要求サービス1511はメールサービスのため、認証要求サービス1511に紐づく優先度1522は「1」となる。したがって、認証ID1512が「ID3」に紐づく優先度9515は、類似度9512の「1」と認証要求サービス1511に紐づく優先度1522の「1」とを掛け合わせた「1」となる。

## 【0160】

認証要求リスト951を参照すると、認証ID1512が「ID1」を含む第3の認証要求は、認証ID1512が「ID3」を含む第3の認証要求よりも低い優先度9515となっている。よって、認証要求の受け付けた順序と認証が行われる順序が異なることとなる。

## 【0161】

変形例8に係る認証システム1は、類似度が低い認証要求に対し、優先順位の低い優先度を付与する。これによって、例えば、クライアント本人ではなくクライアントに成りすました他人から不正利用の危険性を低減させることができる。

## 【0162】

(変形例9)

変形例9においては、クライアント情報1581、パスワードの安全性1111等に応じた重要度と、第2の認証要求に含まれる認証要求サービス1511に紐づく優先度1522とを用いて、第2の認証要求に対し優先度を付与する。

## 【0163】

変形例9において、判定部11が各サーバから受け付ける第1の認証要求には、認証要求サービス1511と、認証ID1512と、パスワード1513とに加え、クライアント情報1581が含まれる。また、変形例9における第2の認証要求は、パスワードの安全性1111と受領番号1514とが付与されたものである。

## 【0164】

変形例9において、記憶部15は利用情報リスト160を記憶する。図25は、利用情報リスト160の一例を示す図である。利用情報リスト160は、認証要求に対する優先度の付与に利用する情報である利用情報1601と、各利用情報の重要性の高低の度合いを示す重要度1602とが紐づいて格納されている。

## 【0165】

また、重要度1602は、値が小さいほど重要性が高いことを示す。したがって、図25に示す利用情報リスト160を参照すると、変形例9において、クライアント情報1581よりもパスワードの安全性1111の重要性が高いことがわかる。なお、利用情報1601は、パスワード入力のレイテンシ7511、RTT6511等でもよい。

## 【0166】

また、変形例9において、記憶部15は、優先度リスト161を記憶する。図26は、優先度リスト161の一例を示す図である。優先度リスト161は、認証ID1512、パスワード優先度1612、第1中間値1613、クライアント優先度1614、第2中間値1615および総合優先度1616を含む。認証ID1512と、パスワード優先度1612と、クライアント優先度1614と、総合優先度1616とは紐づいている。第1中間値1613および第2中間値1615については後述する。

## 【0167】

パスワード優先度1612は、図12に示すパスワード評価リスト111に基づき、各認証ID1512に紐づく認証要求に含まれるパスワードを判定部11が評価し、評価した結果に対して付与された優先度である。

## 【0168】

クライアント優先度1614は、図21に示すクライアント端末リスト158に基づき、各認証ID1512に紐づくクライアント端末のクライアント情報1581に対して付与された優先度である。

## 【0169】

総合優先度1616は、パスワード優先度1612と、クライアント優先度1614との組み合わせに対する優先度を示す。また、総合優先度1616は、パスワード優先度1612とクライアント優先度1614と重要度1602とを掛け合わせた値である。

## 【0170】

具体的に、認証ID1512が「ID1」の総合優先度1616の求め方について説明

10

20

30

40

50

する。まず、判定部 11 は、第 2 の認証要求に含まれるパスワード 1513 が「PW1」の安全性を評価し、パスワード優先度 1612 の「3」を取得する。

#### 【0171】

そして、判定部 11 は、優先度リスト 161 を参照し、パスワードの安全性に対する重要度 1602 の「1」と、パスワード優先度 1612 の「3」とを掛け合わせ、第 1 中間値 1613 の「3」を算出する。

#### 【0172】

また、判定部 11 は、利用情報リスト 160 を参照し、第 2 の認証要求に含まれるクライアント情報 1581 の「Version1」を用いて、クライアント優先度 1614 の「2」を取得する。その後、判定部 11 は、優先度リスト 161 を参照し、クライアント情報に対する重要度 1602 が持つ「2」と、クライアントと優先度 1614 の「2」とを掛け合わせ、第 2 中間値 1615 「4」を算出する。そして、判定部 11 は、パスワードの安全性に対する第 1 中間値 1613 と、クライアント情報に対する第 2 中間値 1615 を掛け合わせ、総合優先度 1616 の「12」を算出する。その後、優先度判定データベース 152 から認証 ID 1512 が「ID1」の認証要求サービス 1511 に紐づく優先度 1522 の「1」を取得する。そして、判定部 11 は、総合優先度 1616 の「12」と優先度 1522 の「1」とを掛け合わせて、認証要求に対する優先度の「12」を算出する。

#### 【0173】

図 27 は、変形例 9 における認証要求リスト 1051 の一例を示す図である。認証要求リスト 1051 は、変形例 9 において認証要求リスト 151 に代わり記憶部 15 に記憶されている。認証要求リスト 1051 は、認証要求サービス 1511、認証 ID 1512、パスワード 1513、クライアント情報 1581、受領番号 1514 および認証要求に対する優先度 1015 を含む。

#### 【0174】

優先度 1015 は、上述したように、認証要求サービス 1511 に紐づく優先度 1522 と、総合優先度 1616 とを掛け合わせた値である。

#### 【0175】

認証要求リスト 1051 を参照すると、パスワードの安全性が低く、「Version1」のアプリケーションを使用している認証 ID 1512 が「ID1」の優先度 1015 は、メールサービスに比べ優先度が低い HTTP サービスに対する認証要求である、認証 ID 1512 が「ID2」の優先度 1015 より低くなる。変形例 9 に係る認証システム 1 によれば、判定部 11 は、複数の利用情報と、利用情報に基づく重要度および優先度に応じて、第 2 の認証要求に優先度 1015 を付与することができる。

#### 【0176】

なお、本変形例において、認証要求に対する優先度は、総合優先度 1616 と認証要求サービス 1511 に紐づく優先度 1522 とを用いて決定される。そのため、記憶部 15 は、総合優先度 1616 自体を記憶しなくてもよい。本変形例において、記憶部 15 は、パスワード評価リスト 111、優先度判定データベース 152、クライアント端末リスト 158 および利用情報リスト 160 を記憶すればよい。判定部 11 は、第 1 または第 2 の認証要求を用いて、パスワード評価リスト 111、優先度判定データベース 152、クライアント端末リスト 158 および利用情報リスト 160 に基づき、総合優先度 1616 を求めればよい。また、第 1 中間値 1613 および第 2 中間値 1615 とは、優先度リスト 161 に格納しなくともよい。

#### 【0177】

##### <第 2 実施形態>

図 28 は第 2 実施形態に係る認証装置 200 の構成の一例を示す機能ブロック図である。認証装置 200 は、判定部 201 と、選択部 203 と、認証部 204 とを備える。第 2 実施形態に係る認証装置 200 は、本開示が解決しようとする課題を解決するための基本の構成である。

10

20

30

40

50

## 【0178】

判定部201は、判定部11の機能を有する。また判定部201はサービスの利用に対する認証の要求である認証要求を受け付け、受け付けた認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、認証の実行の優先順位を示す第2の優先度を受け付けた認証要求に付与する。

## 【0179】

選択部203は、選択部13の機能を有する。また選択部203は、第2の優先度に応じて、認証の対象となる認証要求を選択する。認証部204は、認証部14の機能を有する。また認証部204は、選択部203によって選択された認証要求に対し、認証を行う。

10

## 【0180】

図29は第2実施形態に係る認証装置200の動作の一例を示すフローチャートである。

## 【0181】

判定部201は、サービスの利用に対する認証の要求である認証要求を受け付ける（ステップS801）。そして、判定部201は、受け付けた認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、認証の実行の優先順位を示す第2の優先度を受け付けた認証要求に付与する（ステップS802）。

## 【0182】

選択部203は、第2の優先度に応じて、認証の対象となる認証要求を選択する（ステップS803）。そして、認証部204は、選択部203によって選択された認証要求に対し、認証を行う（ステップS804）。

20

## 【0183】

以上のように、認証装置200は、受け付けた認証要求含まれる認証要求サービスの優先順位を示す第1の優先度に応じて、認証の優先順位を示す第2の優先度を、受け付けた認証要求に付与し、第2の優先度に基づき認証要求を選択し、選択した認証要求に対し認証を行うことで、一台の計算機の中で効率良く認証を行うことができる。

## 【0184】

<ハードウェア構成>

本開示の各実施形態において、各装置または各システムの各構成要素は、機能単位のブロックを示している。各装置または各システムの各構成要素の一部又は全部は、例えば図30に示すような情報処理装置900とプログラムとの任意の組み合わせにより実現される。情報処理装置900は、一例として、以下のような構成を含む。

30

## 【0185】

- ・CPU901
- ・ROM (Read Only Memory) 902
- ・RAM (Random Access Memory) 903
- ・RAM903にロードされるプログラム904
- ・プログラム904を格納する記憶装置905
- ・記録媒体906の読み書きを行うドライブ装置907
- ・通信ネットワーク909と接続する通信インターフェース908
- ・データの入出力を行う入出力インターフェース910
- ・各構成要素を接続するバス911

40

各実施形態における各装置の各構成要素は、これらの機能を実現するプログラム904をCPU901が取得して実行することで実現される。各装置の各構成要素の機能を実現するプログラム904は、例えば、予め記憶装置905やROM902に格納されており、必要に応じてCPU901が読み出す。なお、プログラム904は、通信ネットワーク909を介してCPU901に供給されてもよいし、予め記録媒体906に格納されており、ドライブ装置907が当該プログラムを読み出してCPU901に供給してもよい。

## 【0186】

50

各装置の実現方法には、様々な変形例がある。例えば、各装置は、構成要素毎に夫々別個の情報処理装置 900 とプログラムとの任意の組み合わせにより実現されてもよい。また、各装置またはが備える複数の構成要素が、一つの情報処理装置 900 とプログラムとの任意の組み合わせにより実現されてもよい。

【0187】

また、各装置の各構成要素の一部又は全部は、その他の汎用または専用の回路、プロセッサ等やこれらの組み合わせによって実現される。これらは、単一のチップによって構成されてもよいし、バスを介して接続される複数のチップによって構成されてもよい。

【0188】

各装置の各構成要素の一部又は全部は、上述した回路等とプログラムとの組み合わせによって実現されてもよい。

10

【0189】

各装置の各構成要素の一部又は全部が複数の情報処理装置や回路等により実現される場合には、複数の情報処理装置や回路等は、集中配置されてもよいし、分散配置されてもよい。例えば、情報処理装置や回路等は、クライアント端末アンドサービスシステム、クラウドコンピューティングシステム等、各々が通信ネットワークを介して接続される形態として実現されてもよい。

【0190】

以上、各実施形態を参照して本開示を説明したが、本開示は上記各実施形態に限定されたものではない。本開示の構成や詳細には、本開示の範囲内で当業者が理解し得る様々な変更をすることができる。

20

【0191】

上記の各実施形態の一部又は全部は、以下の付記のようにも記載されうるが、以下には限定されない。

【0192】

(付記 1)

サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第 1 の優先度に応じて、前記認証の実行の優先順位を示す第 2 の優先度を前記認証要求に付与する判定手段と、

前記第 2 の優先度に応じて、前記認証の対象となる認証要求を選択する選択手段と、  
選択された認証要求に対し、前記認証を行う認証手段と、を備える認証装置。

30

【0193】

(付記 2)

前記判定手段は、前記第 2 の優先度が付与された認証要求の数が閾値以下である場合、前記第 2 の優先度を、前記受け付けた認証要求に付与する付記 1 に記載の認証装置。

【0194】

(付記 3)

前記判定手段は、前記サービスを利用するクライアントごとに予め設定されたパスワードの安全性の度合いと前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を、前記受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

40

【0195】

(付記 4)

前記判定手段は、前記認証要求に含まれるパスワードの安全性の度合いと前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

【0196】

(付記 5)

前記認証手段は、前記認証要求の要求元ごとに前記認証が連続して成功した回数を示す連続成功回数と、前記認証が連続して失敗した回数を示す連続失敗回数とをカウントし、

50

前記判定手段は、前記連続成功回数と前記連続失敗回数と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

【0197】

(付記 6)

前記判定手段は、前記認証要求の要求元が使用する IP (Internet Protocol) アドレスと前記第 1 の優先度とに基づき前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

【0198】

(付記 7)

前記判定手段は、前記認証要求の要求元と前記認証要求の要求先との間でネットワーク通信が確立するまでに要する時間と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

【0199】

(付記 8)

前記判定手段は、前記認証要求の要求元が使用するアプリケーションに関する情報と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

【0200】

(付記 9)

前記判定手段は、前記サービスを利用するクライアントの行動的特徴を示すバイOMETRICS 情報であって、予め登録されたバイOMETRICS 情報と、受け付けた認証要求に含まれるバイOMETRICS 情報とを用いて類似度を算出し、算出した類似度と前記第 1 の優先度とに基づき、前記第 2 の優先度を算出し、算出した第 2 の優先度を受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

【0201】

(付記 10)

前記判定手段は、前記第 1 の優先度を前記第 2 の優先度として受け付けた認証要求に付与する付記 1 または 2 に記載の認証装置。

【0202】

(付記 11)

前記判定手段は、前記第 1 の優先度が所定の条件を満たす場合、前記第 2 の優先度を受け付けた認証要求に付与する付記 1 から 10 のいずれか 1 項に記載の認証装置。

【0203】

(付記 12)

前記判定手段は、受け付けた順序を示す順序情報を受け付けた認証要求に付与し、

前記選択手段は、最も高い前記第 2 の優先度が付与された前記認証要求が複数である場合、前記順序情報に応じて、前記認証の対象となる認証要求を選択する付記 11 に記載の認証装置。

【0204】

(付記 13)

前記順序情報が付与された認証要求を記憶する記憶手段と、

前記第 2 の優先度が付与された認証要求の数が閾値以下である場合、前記記憶手段に記憶された認証要求から、前記順序情報に基づき認証要求を選択し、選択した認証要求を前記判定手段に送信する確認手段と、を備え、

前記判定手段は、前記第 1 の優先度が前記所定の条件を満たさない場合、受け付けた認証要求を前記記憶手段に記憶させる付記 12 に記載の認証装置。

【0205】

(付記 14)

10

20

30

40

50

サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、前記認証の実行順を示す第2の優先度を前記認証要求に付与し、

前記第2の優先度に応じて、前記認証の対象となる認証要求を選択し、  
選択された認証要求に対し、前記認証を行う認証方法。

#### 【0206】

(付記15)

サービスの利用に対する認証の要求である認証要求を受け付け、前記認証要求に関連するサービスの優先順位を示す第1の優先度に応じて、前記認証の実行順を示す第2の優先度を前記認証要求に付与する判定処理と、

前記第2の優先度に応じて、前記認証の対象となる認証要求を選択する選択処理と、  
選択された認証要求に対し、前記認証を行う認証処理と、をコンピュータに実行させるプログラム。

#### 【符号の説明】

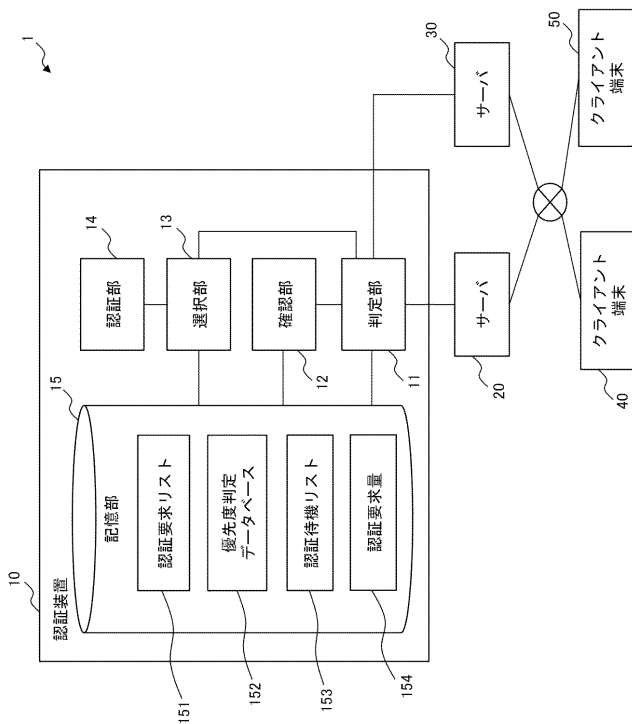
#### 【0207】

|     |             |    |
|-----|-------------|----|
| 1   | 認証システム      |    |
| 10  | 認証装置        |    |
| 11  | 判定部         |    |
| 12  | 確認部         |    |
| 13  | 選択部         | 20 |
| 14  | 認証部         |    |
| 15  | 記憶部         |    |
| 20  | サーバ         |    |
| 21  | 判定部         |    |
| 24  | 認証部         |    |
| 30  | サーバ         |    |
| 40  | クライアント端末    |    |
| 50  | クライアント端末    |    |
| 100 | 認証装置        |    |
| 111 | パスワード評価リスト  | 30 |
| 151 | 認証要求リスト     |    |
| 152 | 優先度判定データベース |    |
| 153 | 認証待機リスト     |    |
| 155 | 安全性リスト      |    |
| 156 | 連続リスト       |    |
| 157 | アドレスリスト     |    |
| 158 | クライアント端末リスト |    |
| 159 | バイオメトリクスリスト |    |
| 160 | 利用情報リスト     |    |
| 161 | 優先度リスト      | 40 |
| 200 | 認証装置        |    |
| 201 | 判定部         |    |
| 203 | 選択部         |    |
| 204 | 認証部         |    |
| 251 | 認証要求リスト     |    |
| 351 | 認証要求リスト     |    |
| 451 | 認証要求リスト     |    |
| 551 | 認証要求リスト     |    |
| 651 | 認証要求リスト     |    |
| 751 | 認証要求リスト     | 50 |

8 5 1 認証要求リスト  
 9 0 0 情報処理装置  
 9 0 1 C P U  
 9 0 2 R O M  
 9 0 3 R A M  
 9 0 4 プログラム  
 9 0 5 記憶装置  
 9 0 6 記録媒体  
 9 0 7 ドライブ装置  
 9 0 8 通信インターフェース  
 9 0 9 通信ネットワーク  
 9 1 0 入出力インターフェース  
 9 1 1 バス  
 9 5 1 認証要求リスト  
 1 0 5 1 認証要求リスト

10

【図 1】



【図 2】

| 1511<br>認証要求サービス | 1512<br>認証ID | 1513<br>パスワード |
|------------------|--------------|---------------|
| メール              | ID1          | PW1           |
| HTTP             | ID2          | PW2           |
| メール              | ID3          | PW3           |
| ⋮                | ⋮            | ⋮             |
| メール              | ID7          | PW7           |
| HTTP             | ID8          | PW8           |
| メール              | ID9          | PW9           |

【図 3】

| 1511<br>認証要求サービス | 1522<br>優先度 |
|------------------|-------------|
| メール              | 1           |
| HTTP             | 2           |

【図 4】

151

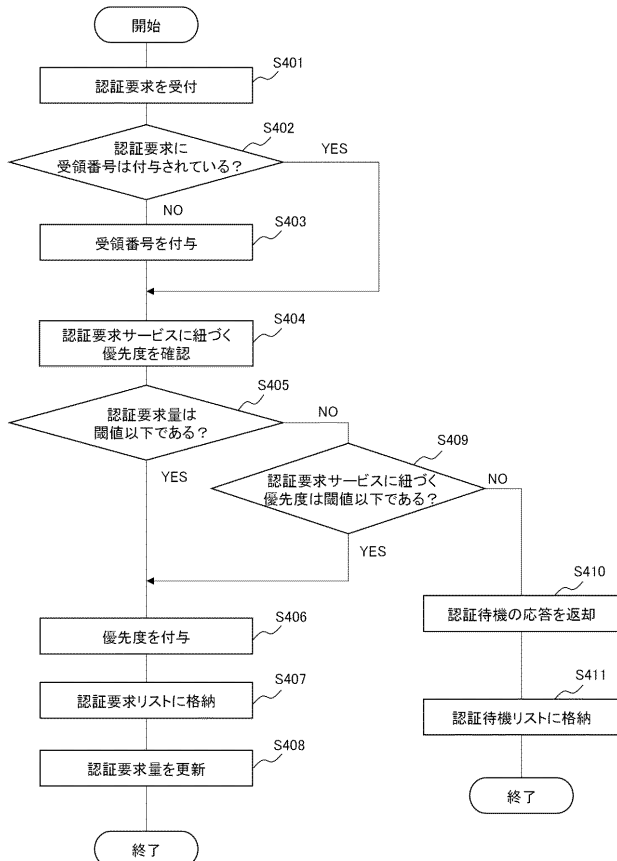
| 1511     | 1512 | 1513  | 1514    | 1515 |
|----------|------|-------|---------|------|
| 認証要求サービス | 認証ID | パスワード | 受領番号    | 優先度  |
| メール      | ID1  | PW1   | 1000:00 | 1    |
| HTTP     | ID2  | PW2   | 1000:43 | 2    |
| メール      | ID3  | PW3   | 1001:12 | 1    |

【図 5】

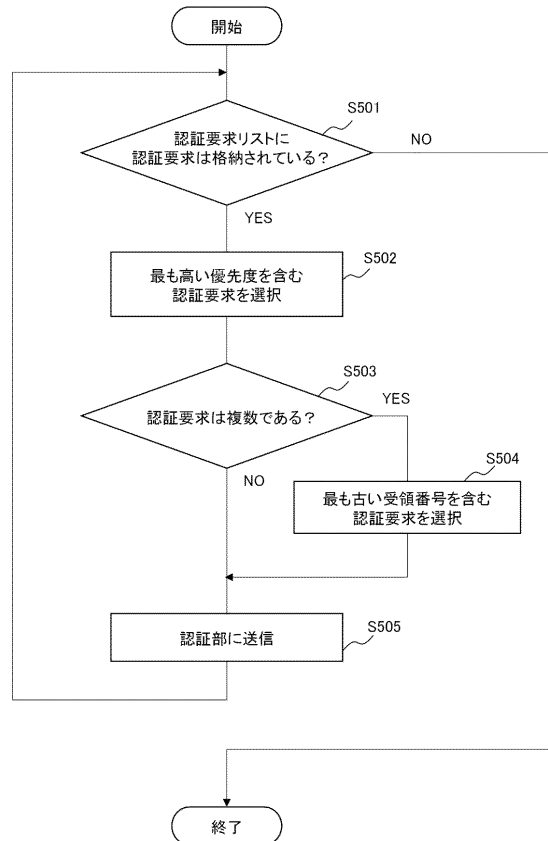
153

| 1511     | 1512 | 1513  | 1514     |
|----------|------|-------|----------|
| 認証要求サービス | 認証ID | パスワード | 受領番号     |
| メール      | ID7  | PW7   | 11:00:00 |
| HTTP     | ID8  | PW8   | 11:00:13 |
| メール      | ID9  | PW9   | 11:01:22 |

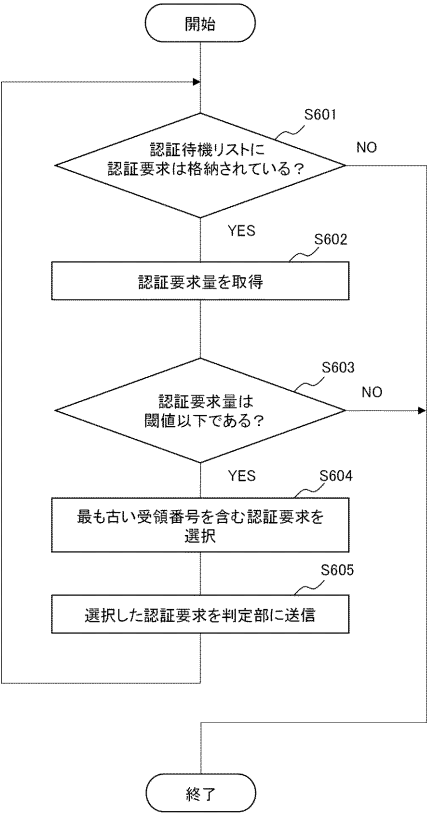
【図 6】



【図 7】



【図 8】



【図 9】

155

| 1512<br>認証ID | 1552<br>パスワード評価値 |
|--------------|------------------|
| ID1          | 3                |
| ID2          | 2                |
| ID3          | 1                |

【図 10】

251

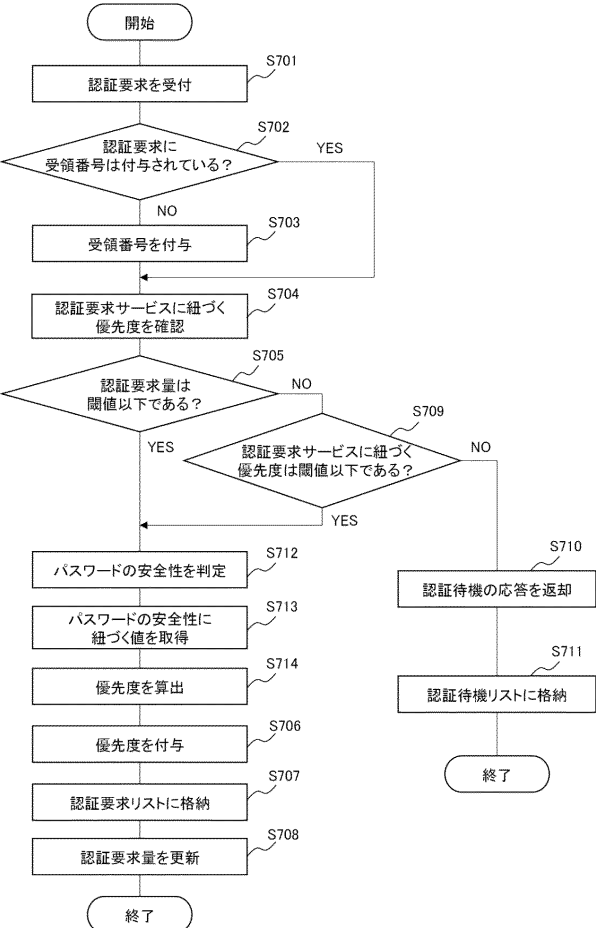
| 1511<br>認証要求サービス | 1512<br>認証ID | 1513<br>パスワード | 1514<br>受領番号 | 2515<br>優先度 |
|------------------|--------------|---------------|--------------|-------------|
| メール              | ID1          | PW1           | 10:00:00     | 3           |
| HTTP             | ID2          | PW2           | 10:00:43     | 4           |
| メール              | ID3          | PW3           | 10:01:12     | 1           |

【図 11】

111

| 1111<br>パスワードの安全性 | 1112<br>安全値 |
|-------------------|-------------|
| 高                 | 1           |
| 中                 | 2           |
| 低                 | 3           |

【図 1 2】

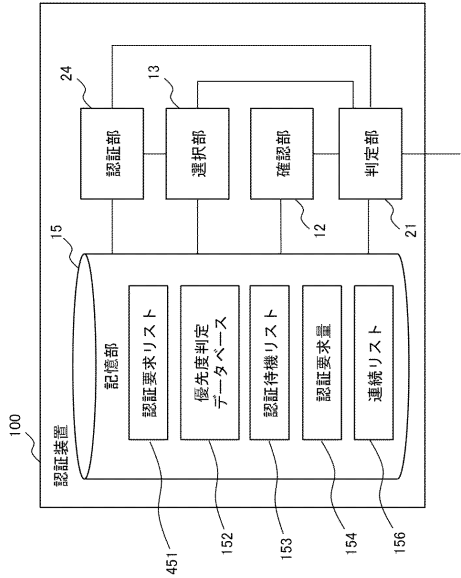


【図 1 3】

351

| 1511     | 1512 | 1513  | 1111      | 1514   | 3515 |
|----------|------|-------|-----------|--------|------|
| 認証要求サービス | 認証ID | パスワード | パスワードの安全性 | 受領番号   | 優先度  |
| メール      | ID1  | PW1   | 低         | 100000 | 3    |
| HTTP     | ID2  | PW2   | 中         | 100043 | 4    |
| メール      | ID3  | PW3   | 高         | 100112 | 1    |

【図 1 4】



【図 1 5】

| 156  |        |        |                  |  |
|------|--------|--------|------------------|--|
| 1512 | 1562   | 1563   | 1564             |  |
| 認証ID | 連続成功回数 | 連続失敗回数 | 連続評価値 (10=成功+失敗) |  |
| ID1  | 0      | 2      | 12               |  |
| ID2  | 1      | 0      | 9                |  |
| ID3  | 3      | 0      | 7                |  |

【図 16】

451

|          |      |       |         |      |
|----------|------|-------|---------|------|
| 1511     | 1512 | 1513  | 1514    | 4515 |
| 認証要求サービス | 認証ID | パスワード | 受領番号    | 優先度  |
| メール      | ID1  | PW1   | 1000:00 | 12   |
| HTTP     | ID2  | PW2   | 1000:43 | 18   |
| メール      | ID3  | PW3   | 1001:12 | 7    |
| ⋮        | ⋮    | ⋮     | ⋮       | ⋮    |

【図 17】

157

|             |      |
|-------------|------|
| 1571        | 1572 |
| ネットワークアドレス部 | 優先度  |
| x.y.z       | 1    |
| a.b.c       | 3    |
| *           | 2    |

【図 18】

551

|          |      |       |         |         |      |
|----------|------|-------|---------|---------|------|
| 1511     | 1512 | 1513  | 5511    | 1514    | 5515 |
| 認証要求サービス | 認証ID | パスワード | IPアドレス  | 受領番号    | 優先度  |
| メール      | ID1  | PW1   | a.b.c.d | 1000:00 | 3    |
| HTTP     | ID2  | PW2   | h.i.j.k | 1000:43 | 4    |
| メール      | ID3  | PW3   | x.y.z.w | 1001:12 | 1    |

【図 19】

651

|          |      |       |         |         |      |
|----------|------|-------|---------|---------|------|
| 1511     | 1512 | 1513  | 6511    | 1514    | 6515 |
| 認証要求サービス | 認証ID | パスワード | RTT(ms) | 受領番号    | 優先度  |
| メール      | ID1  | PW1   | 15      | 1000:00 | 15   |
| HTTP     | ID2  | PW2   | 10      | 1000:43 | 20   |
| メール      | ID3  | PW3   | 5       | 1001:12 | 5    |

【図 2 0】

751

|          |      |       |                  |        |      |
|----------|------|-------|------------------|--------|------|
| 1511     | 1512 | 1513  | 7511             | 1514   | 7515 |
| 認証要求サービス | 認証ID | パスワード | パスワード入力レイテンシ(ms) | 受領番号   | 優先度  |
| メール      | ID1  | PW1   | 150              | 100000 | 150  |
| HTTP     | ID2  | PW2   | 100              | 100043 | 200  |
| メール      | ID3  | PW3   | 50               | 100112 | 50   |

【図 2 1】

158

|           |      |
|-----------|------|
| 1581      | 1582 |
| クライアント情報  | 優先度  |
| Version 2 | 1    |
| Version 1 | 2    |
| その他       | 3    |

【図 2 2】

851

|          |      |       |           |        |      |
|----------|------|-------|-----------|--------|------|
| 1511     | 1512 | 1513  | 1581      | 1514   | 8515 |
| 認証要求サービス | 認証ID | パスワード | クライアント情報  | 受領番号   | 優先度  |
| メール      | ID1  | PW1   | Version1  | 100000 | 2    |
| HTTP     | ID2  | PW2   | Version 2 | 100043 | 2    |
| メール      | ID3  | PW3   | Version 2 | 100112 | 1    |

【図 2 3】

159

|      |                |
|------|----------------|
| 1512 | 1592           |
| 認証ID | 登録バイOMETRICS情報 |
| ID1  | 情報A            |
| ID2  | 情報B            |
| ID3  | 情報C            |

【図 2 4】

951

| 1511     | 1512 | 1513  | 9511         | 1514   | 9512 | 9515 |
|----------|------|-------|--------------|--------|------|------|
| 認証要求サービス | 認証ID | パスワード | 入力バイオメトリクス情報 | 受領番号   | 類似度  | 優先度  |
| メール      | ID1  | PW1   | 情報X          | 100000 | 3    | 3    |
| HTTP     | ID2  | PW2   | 情報B          | 100043 | 2    | 4    |
| メール      | ID3  | PW3   | 情報C          | 100112 | 1    | 1    |

【図 2 6】

161

| 1512 | 1612     | 1613  | 1614      | 1615  | 1616  |
|------|----------|-------|-----------|-------|-------|
| 認証ID | パスワード優先度 | 第1中間値 | クライアント優先度 | 第2中間値 | 総合優先度 |
| ID1  | 3        | 3     | 2         | 4     | 12    |
| ID2  | 2        | 2     | 1         | 2     | 4     |
| ID3  | 1        | 1     | 1         | 2     | 2     |

【図 2 5】

160

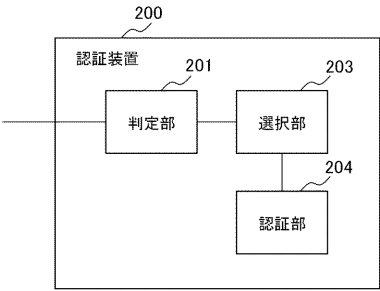
| 1601      | 1602 |
|-----------|------|
| 利用情報      | 重要度  |
| パスワードの安全性 | 1    |
| クライアント情報  | 2    |

【図 2 7】

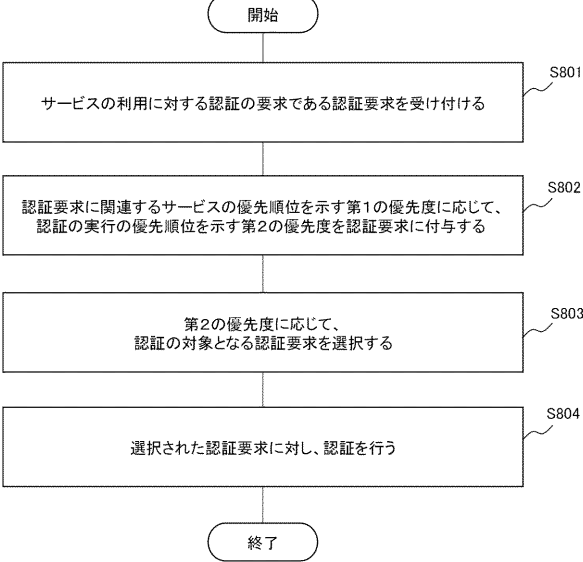
1051

| 1511     | 1512 | 1513  | 1581      | 1111      | 1514   | 1015 |
|----------|------|-------|-----------|-----------|--------|------|
| 認証要求サービス | 認証ID | パスワード | クライアント情報  | パスワードの安全性 | 受領番号   | 優先度  |
| メール      | ID1  | PW1   | Version1  | 低         | 100000 | 12   |
| HTTP     | ID2  | PW2   | Version 2 | 中         | 100043 | 8    |
| メール      | ID3  | PW3   | Version 2 | 高         | 100112 | 2    |

【図 28】



【図 29】



【図 30】

