(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2017-72979
(P2017-72979A)
(43)公開日　平成29年4月13日(2017.4.13)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/31 (2013.01)	G06F 21/31	

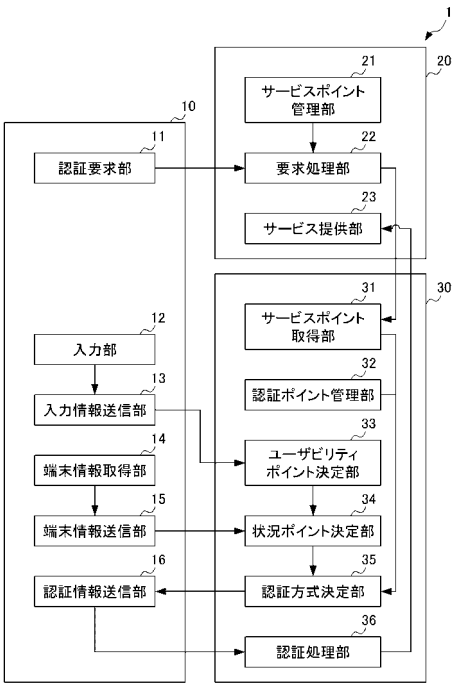
審査請求 未請求　請求項の数 12　ＯＬ　（全 20 頁）

(21)出願番号　特願2015-199273 (P2015-199273)
(22)出願日　平成27年10月7日 (2015.10.7)

(71)出願人　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100120891
弁理士　林　一好
(72)発明者　太田　陽基
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内
(72)発明者　渡辺　龍
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内
(72)発明者　清本　晋作
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ研究所内

(54)【発明の名称】認証システム、認証サーバ、事業者サーバ及び利用者端末

(57)【要約】
【課題】サービスに応じた認証方式の組み合わせを適切に決定できる認証システム、認証サーバ、事業者サーバ及び利用者端末を提供すること。
【解決手段】認証システム１において、利用者端末１０は、サービスの要求を行う認証要求部１１と、認証方式それぞれに対する認証情報を送信する認証情報送信部１６と、を備え、事業者サーバ２０は、サービスが必要とする認証の安全性を示すサービスポイントを管理するサービスポイント管理部２１を備え、認証サーバ３０は、認証方式の組み合わせにより得られる安全性を示す認証ポイントを管理する認証ポイント管理部３２と、認証ポイントがサービスポイント以上である認証方式の組み合わせのうち、認証ポイント及びサービスポイントの差分が小さい組み合わせを優先して決定する認証方式決定部３５と、決定された認証方式の組み合わせそれぞれに対して、認証情報を受信し、認証処理を行う認証処理部３６と、を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
サービスを利用する利用者端末、前記サービスを提供する事業者サーバ及び利用者の認証を行う認証サーバを有する認証システムであって、
前記利用者端末は、
前記サービスの要求を行う認証要求部と、
前記認証サーバにおいて決定された認証方式それぞれに対する認証情報を送信する認証情報送信部と、を備え、
前記事業者サーバは、
前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該被害内容の回収又は削除の困難性に基づく指標を統合して算出された、前記サービスが必要とする認証の安全性を示すサービスポイントを管理するサービスポイント管理部を備え、
前記認証サーバは、
前記認証方式毎の攻撃に対する安全性を示す安全性ポイントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された、前記認証方式の組み合わせにより得られる安全性を示す認証ポイントを管理する認証ポイント管理部と、
前記認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定する認証方式決定部と、
前記認証方式決定部により決定された認証方式の組み合わせそれぞれに対して、前記認証情報を受信し、認証処理を行う認証処理部と、を備える認証システム。
【請求項２】
前記利用者端末は、
認証実行時の時刻情報、位置情報、周辺情報及び移動手段情報のうち、少なくともいずれかの端末情報を取得する取得部と、
前記端末情報を送信する端末情報送信部と、を備え、
前記認証サーバは、
前記認証方式毎の利用者の利便性を示すユーザビリティポイント及び前記端末情報に基づいて、認証実行時における前記認証方式の組み合わせの優先度を示す状況ポイントを算出する状況ポイント決定部を備え、
前記認証方式決定部は、前記認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記状況ポイントが大きい組み合わせを優先して決定する請求項１に記載の認証システム。
【請求項３】
前記状況ポイント決定部は、前記端末情報をパラメータとする、前記認証方式毎に異なる関数を用いて前記状況ポイントを算出する請求項２に記載の認証システム。
【請求項４】
前記利用者端末は、
前記認証方式毎に、前記利用者が選択する優先順位若しくはポイント、登録・認証手続きに要する時間、及び登録・認証失敗の頻度に基づく指標のうち、少なくともいずれかの入力情報を受け付ける入力部と、
前記入力情報を送信する入力情報送信部と、を備え、
前記認証サーバは、
前記認証方式毎に、前記入力情報に基づいて、前記ユーザビリティポイントを算出するユーザビリティポイント決定部を備える請求項２又は請求項３に記載の認証システム。
【請求項５】
前記状況ポイント決定部は、前記認証方式の組み合わせがＡＮＤ、ＯＲ又は重み付けのいずれのパターンであるかに応じて、それぞれ異なる計算式を用いて前記状況ポイントを

算出する請求項２から請求項４のいずれかに記載の認証システム。
【請求項６】
前記認証方式の組み合わせにおいて、各認証方式の実行順は、前記パターン毎に当該認証方式の単独での状況ポイントの大きさにより決定される請求項５に記載の認証システム。
【請求項７】
前記安全性ポイントは、前記攻撃の種別毎の攻撃成功確率、攻撃に要する費用及び時間のうち、少なくともいずれかに基づいて算出される請求項１から請求項６のいずれかに記載の認証システム。
【請求項８】
前記安全性ポイントは、全数攻撃の成功確率に基づく指標と、前記全数攻撃以外の特殊攻撃のうち攻撃成功確率が最大の攻撃に関する当該攻撃成功確率、攻撃に要する費用及び時間に基づく指標とを統合して算出される請求項７に記載の認証システム。
【請求項９】
前記認証ポイントは、前記認証方式の組み合わせがＡＮＤ、ＯＲ又は重み付けのいずれであるかに応じて、それぞれ異なる計算式を用いて算出される請求項１から請求項８のいずれかに記載の認証システム。
【請求項１０】
事業者サーバにより提供されるサービスを利用する利用者の認証を行う認証サーバであって、
前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該被害内容の回収又は削除の困難性に基づく指標を統合して算出され前記事業者サーバにおいて管理されている、前記サービスが必要とする認証の安全性を示すサービスポイントを、利用者端末を経由して受信するサービスポイント取得部と、
認証方式毎の攻撃に対する安全性を示す安全性ポイントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された、前記認証方式の組み合わせにより得られる安全性を示す認証ポイントを管理する認証ポイント管理部と、
前記認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定する認証方式決定部と、
前記認証方式決定部により決定された認証方式の組み合わせそれぞれに対して、前記利用者端末から認証情報を受信し、認証処理を行う認証処理部と、を備える認証サーバ。
【請求項１１】
認証サーバにより認証された利用者端末にサービスを提供する事業者サーバであって、
前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該被害内容の回収又は削除の困難性に基づく指標を統合して算出された、前記サービスが必要とする認証の安全性を示すサービスポイントを管理するサービスポイント管理部と、
前記利用者端末からの前記サービスの要求に応じて、前記サービスポイントを提供し、前記認証サーバへリダイレクトさせる要求処理部と、
前記認証サーバにおいて、認証方式毎の攻撃に対する安全性を示す安全性ポイントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された前記認証方式の組み合わせにより得られる安全性を示す認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定した後、当該決定された認証方式の組み合わせに対して認証が成功したことを示す通知を受けたことに応じて、前記利用者端末へサービスの提供を開始するサービス提供部と、を備える事業者サーバ。
【請求項１２】
事業者サーバにより提供されるサービスを利用する利用者端末であって、
前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該

被害内容の回収又は削除の困難性に基づく指標を統合して算出され前記事業者サーバにおいて管理されている、前記サービスが必要とする認証の安全性を示すサービスポイントを取得し、認証サーバに対して認証要求を行う認証要求部と、
前記認証サーバにおいて、認証方式毎の攻撃に対する安全性を示す安全性ポイントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された前記認証方式の組み合わせにより得られる安全性を示す認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定した後、当該決定された認証方式それぞれに対する認証情報を送信する認証情報送信部と、を備える利用者端末。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サービスを利用する際の認証を行う認証システムに関する。
【背景技術】
【０００２】
従来、通信ネットワークを介して様々なサービスが提供されている。これらのサービスには、なりすまし等を防ぐため、利用者の本人性を確認する本人認証技術が採用されている。本人認証技術には、多種多様な認証方式が存在するが、いずれの認証方式を採用するかは、通常、サービス提供事業者が決定している。
【０００３】
特許文献１では、セキュリティ対象毎にセキュリティレベルを設定・管理し、このレベルに応じて認証時に使用する認証方式を選択する技術が提案されている。
特許文献２では、利用者自身が選択した認証方式を用いて認証を行い、この認証方式の認証ポイントがサービス事業者の要求する認証レベルに達しているか否かを判定する技術が提案されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００５－２２７９３４号公報
【特許文献２】特開２０１０－６７１２４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ところで、提供されるサービスのそれぞれにおいて、必要とする認証のレベルは様々であり、これらを適切に設定することは難しかった。また、必要とする認証のレベルに応じて、適切な認証方式の組み合わせを選択することは難しかった。
【０００６】
本発明は、サービスに応じた認証方式の組み合わせを適切に決定できる認証システム、認証サーバ、事業者サーバ及び利用者端末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】
本発明に係る認証システムは、サービスを利用する利用者端末、前記サービスを提供する事業者サーバ及び利用者の認証を行う認証サーバを有する認証システムであって、前記利用者端末は、前記サービスの要求を行う認証要求部と、前記認証サーバにおいて決定された認証方式それぞれに対する認証情報を送信する認証情報送信部と、を備え、前記事業者サーバは、前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該被害内容の回収又は削除の困難性に基づく指標を統合して算出された、前記サービスが必要とする認証の安全性を示すサービスポイントを管理するサービスポイント管理部を備え、前記認証サーバは、前記認証方式毎の攻撃に対する安全性を示す安全性ポイ

ントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された、前記認証方式の組み合わせにより得られる安全性を示す認証ポイントを管理する認証ポイント管理部と、前記認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定する認証方式決定部と、前記認証方式決定部により決定された認証方式の組み合わせそれぞれに対して、前記認証情報を受信し、認証処理を行う認証処理部と、を備える。

【０００８】

前記利用者端末は、認証実行時の時刻情報、位置情報、周辺情報及び移動手段情報のうち、少なくともいずれかの端末情報を取得する取得部と、前記端末情報を送信する端末情報送信部と、を備え、前記認証サーバは、前記認証方式毎の利用者の利便性を示すユーザビリティポイント及び前記端末情報に基づいて、認証実行時における前記認証方式の組み合わせの優先度を示す状況ポイントを算出する状況ポイント決定部を備え、前記認証方式決定部は、前記認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記状況ポイントが大きい組み合わせを優先して決定してもよい。

【０００９】

前記状況ポイント決定部は、前記端末情報をパラメータとする、前記認証方式毎に異なる関数を用いて前記状況ポイントを算出してもよい。

【００１０】

前記利用者端末は、前記認証方式毎に、前記利用者が選択する優先順位若しくはポイント、登録・認証手続きに要する時間、及び登録・認証失敗の頻度に基づく指標のうち、少なくともいずれかの入力情報を受け付ける入力部と、前記入力情報を送信する入力情報送信部と、を備え、前記認証サーバは、前記認証方式毎に、前記入力情報に基づいて、前記ユーザビリティポイントを算出するユーザビリティポイント決定部を備えてもよい。

【００１１】

前記状況ポイント決定部は、前記認証方式の組み合わせがＡＮＤ、ＯＲ又は重み付けのいずれのパターンであるかに応じて、それぞれ異なる計算式を用いて前記状況ポイントを算出してもよい。

【００１２】

前記認証方式の組み合わせにおいて、各認証方式の実行順は、前記パターン毎に当該認証方式の単独での状況ポイントの大きさにより決定されてもよい。

【００１３】

前記安全性ポイントは、前記攻撃の種別毎の攻撃成功確率、攻撃に要する費用及び時間のうち、少なくともいずれかに基づいて算出されてもよい。

【００１４】

前記安全性ポイントは、全数攻撃の成功確率に基づく指標と、前記全数攻撃以外の特殊攻撃のうち攻撃成功確率が最大の攻撃に関する当該攻撃成功確率、攻撃に要する費用及び時間に基づく指標とを統合して算出されてもよい。

【００１５】

前記認証ポイントは、前記認証方式の組み合わせがＡＮＤ、ＯＲ又は重み付けのいずれであるかに応じて、それぞれ異なる計算式を用いて算出されてもよい。

【００１６】

本発明に係る認証サーバは、事業者サーバにより提供されるサービスを利用する利用者の認証を行う認証サーバであって、前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該被害内容の回収又は削除の困難性に基づく指標を統合して算出され前記事業者サーバにおいて管理されている、前記サービスが必要とする認証の安全性を示すサービスポイントを、利用者端末を経由して受信するサービスポイント取得部と、認証方式毎の攻撃に対する安全性を示す安全性ポイントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された、前記認証方式の組み合わせにより得られる安全性を示す認証ポイントを管理する認証ポイン

ト管理部と、前記認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定する認証方式決定部と、前記認証方式決定部により決定された認証方式の組み合わせそれぞれに対して、前記利用者端末から認証情報を受信し、認証処理を行う認証処理部と、を備える。

【００１７】

本発明に係る事業者サーバは、認証サーバにより認証された利用者端末にサービスを提供する事業者サーバであって、前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該被害内容の回収又は削除の困難性に基づく指標を統合して算出された、前記サービスが必要とする認証の安全性を示すサービスポイントを管理するサービスポイント管理部と、前記利用者端末からの前記サービスの要求に応じて、前記サービスポイントを提供し、前記認証サーバへリダイレクトさせる要求処理部と、前記認証サーバにおいて、認証方式毎の攻撃に対する安全性を示す安全性ポイントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された前記認証方式の組み合わせにより得られる安全性を示す認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定した後、当該決定された認証方式の組み合わせに対して認証が成功したことを示す通知を受けたことに応じて、前記利用者端末へサービスの提供を開始するサービス提供部と、を備える。

【００１８】

本発明に係る利用者端末は、事業者サーバにより提供されるサービスを利用する利用者端末であって、前記サービスにおいて想定される被害内容の種別毎の、当該被害内容の数量、及び当該被害内容の回収又は削除の困難性に基づく指標を統合して算出され前記事業者サーバにおいて管理されている、前記サービスが必要とする認証の安全性を示すサービスポイントを取得し、認証サーバに対して認証要求を行う認証要求部と、前記認証サーバにおいて、認証方式毎の攻撃に対する安全性を示す安全性ポイントに加えて、ワンタイム性、所有物認証性及び多要素性の指標のうち、少なくともいずれかに基づいて算出された前記認証方式の組み合わせにより得られる安全性を示す認証ポイントが前記サービスポイント以上である前記認証方式の組み合わせのうち、前記認証ポイント及び前記サービスポイントの差分が小さい組み合わせを優先して決定した後、当該決定された認証方式それぞれに対する認証情報を送信する認証情報送信部と、を備える。

【発明の効果】

【００１９】

本発明によれば、サービスに応じた認証方式の組み合わせを適切に決定できる。

【図面の簡単な説明】

【００２０】

【図１】実施形態に係る認証システムの構成を示す図である。

【図２】実施形態に係る認証方式の組み合わせを決定する手順を示す図である。

【図３】実施形態に係る認証方式の組み合わせ決定処理の一例を示すフローチャートである。

【図４】実施形態に係る入力情報の登録処理を示すシーケンス図である。

【図５】実施形態に係る認証方式を利用するための照合情報登録処理を示すシーケンス図である。

【図６】実施形態に係る認証方式の選定及び認証の処理を示すシーケンス図である。

【発明を実施するための形態】

【００２１】

以下、本発明の実施形態の一例について説明する。

図１は、本実施形態に係る認証システム１の構成を示す図である。

【００２２】

認証システム１は、サービスを利用する利用者端末１０と、サービスを提供する事業者

サーバ２０と、利用者の認証を行う認証サーバ３０とを備える。
【００２３】
利用者端末１０、事業者サーバ２０及び認証サーバ３０は、互いにネットワークを介して接続されている。利用者端末１０において利用者がサービスを利用する際に、サービス要求は認証サーバ３０へリダイレクトされ、利用者の正当性が認証された後、事業者サーバ２０によりサービスが提供される。
【００２４】
利用者端末１０は、認証要求部１１と、入力部１２と、入力情報送信部１３と、端末情報取得部１４と、端末情報送信部１５と、認証情報送信部１６とを備える。
【００２５】
認証要求部１１は、事業者サーバ２０に対してサービスの要求を行う。
入力部１２は、認証方式毎に、利用者が選択する優先順位若しくはポイント、登録・認証手続きに要する時間、及び登録・認証失敗の頻度に基づく指標のうち、少なくともいずれかの入力情報を受け付ける。
入力情報送信部１３は、入力部１２により受け付けられた入力情報を、認証方式毎の利用者の利便性を示すユーザビリティポイント算出のために認証サーバ３０へ送信する。
【００２６】
端末情報取得部１４は、認証実行時の時刻情報、位置情報、周辺情報及び移動手段情報のうち、少なくともいずれかの端末情報を取得する。
端末情報送信部１５は、端末情報取得部１４により取得された端末情報を、認証実行時における認証方式の組み合わせの優先度を示す状況ポイント算出のために認証サーバ３０へ送信する。
【００２７】
認証情報送信部１６は、認証サーバ３０において決定された認証方式それぞれに対する認証情報を送信する。
【００２８】
事業者サーバ２０は、サービスポイント管理部２１と、要求処理部２２と、サービス提供部２３とを備える。
【００２９】
サービスポイント管理部２１は、認証サーバ３０において後述のサービスポイント決定処理により算出された、サービスが必要とする認証の安全性を示すサービスポイントを記憶、管理する。
【００３０】
要求処理部２２は、利用者端末１０からのサービスの要求に応じて、サービスポイント管理部２１により管理されているサービスポイントを提供し、認証サーバ３０へリダイレクトさせる。
【００３１】
サービス提供部２３は、認証サーバ３０において認証方式の組み合わせが決定された後、この決定された認証方式の組み合わせに対して認証が成功したことを示す通知を受けたことに応じて、利用者端末１０へサービスの提供を開始する。
【００３２】
認証サーバ３０は、サービスポイント取得部３１と、認証ポイント管理部３２と、ユーザビリティポイント決定部３３と、状況ポイント決定部３４と、認証方式決定部３５と、認証処理部３６とを備える。
【００３３】
サービスポイント取得部３１は、事業者サーバ２０において管理されているサービスポイントを、利用者端末１０を経由して受信する。
【００３４】
認証ポイント管理部３２は、後述の認証ポイント決定処理により算出した、認証方式の組み合わせにより得られる安全性を示す認証ポイントを記憶、管理する。

【００３５】
ユーザビリティポイント決定部３３は、認証方式毎に、利用者端末１０から受信した入力情報に基づいて、後述のユーザビリティポイント決定処理によりユーザビリティポイントを算出する。
状況ポイント決定部３４は、ユーザビリティポイント、及び利用者端末１０から受信した端末情報に基づいて、後述の状況ポイント決定処理により状況ポイントを算出する。
【００３６】
認証方式決定部３５は、認証ポイント、サービスポイント及び状況ポイントに基づいて、後述の認証方式決定処理により認証方式の組み合わせを決定する。
認証処理部３６は、認証方式決定部３５により決定された認証方式の組み合わせそれぞれに対して、利用者端末１０から認証情報を受信し、認証処理を行う。
【００３７】
図２は、本実施形態に係る認証システム１において、多種多様に存在する認証方式の中から最適な認証方式の組み合わせを自動的に決定する手順を示す図である。
ここで、本実施形態において対象とする認証方式は、例えば以下が挙げられるが、これらには限られず、様々な認証方式が用いられてよい。
・パスワード認証
・４桁の暗証番号認証
・８桁の暗証番号認証
・パターン認証
・秘密の質問を用いた認証
・ワンタイムパスワード認証
・ワンタイムパターン認証
・ＳＩＭ認証
・機器認証
・秘密鍵を用いた署名による認証
・乱数表による認証
・掌紋認証
・指紋認証
・顔認証
・てのひら静脈認証
・指静脈認証
・虹彩認証
・音声認証
・署名認証
・多要素認証
・画像認証（ＣＡＰＴＣＨＡ）
・位置認証
・リスクベース認証
・多経路認証
【００３８】
（サービスポイント決定処理）
サービスポイント決定処理では、認証サーバ３０又は事業者サーバ２０の管理者が入力する次の３種類の項目から、対象となるサービスがどの程度の安全性を必要とするのかが決定される。
【００３９】
（ａ）被害内容の種別
サービス事業者の提供するサービスにおいて、不正者によるなりすましが行われた場合、どのような種類の被害を受けるかを想定し、被害内容の種別として、金銭、個人情報等の項目が入力される。

【００４０】
（ｂ）被害内容の数量
サービス事業者の提供するサービスにおいて、不正者によるなりすましが行われた場合、どの程度の被害を受けるかを想定し、被害内容の数量として、金額（金銭の場合）、件数（個人情報の場合）等の項目が入力される。
【００４１】
（ｃ）被害内容の回収・削除困難性
サービス事業者の提供するサービスにおいて、不正者によるなりすましが行われた場合、受けた被害の回収又は削除がどの程度困難であるかを想定し、被害内容の回収・削除困難性として、回収困難率（金銭の場合）、削除困難率（個人情報の場合）等の項目が入力される。
【００４２】
このとき、サービスポイントは下記の数式により算出される。
サービスポイント
＝「金銭」における「金額」×「回収困難率」×Ｐｓｒ１
＋「個人情報」における「件数」×「削除困難率」×Ｐｓｒ２
＋「その他」における「数量」×「回収・削除困難率」×Ｐｓｒ３
【００４３】
ただし、Ｐｓｒ１、Ｐｓｒ２、Ｐｓｒ３は、以下を意味している。
・Ｐｓｒ１：「金銭」に関する被害内容を正規化するためのパラメータ
・Ｐｓｒ２：「個人情報」に関する被害内容を正規化するためのパラメータ
・Ｐｓｒ３：「その他」に関する被害内容を正規化するためのパラメータ
【００４４】
（ユーザビリティポイント決定処理）
ユーザビリティポイント決定処理では、サービスの利用者が入力する次の３種類の項目から、利用者がどの認証方式を優先的に使用したいのかが決定される。
【００４５】
（ａ）利用者選択の優先順位又はポイント
サービス事業者の提供するサービスを利用する上で、利用者がどの認証方式を優先的に選択したいのかを示す項目として、選択可能な認証方式と、その優先順位又はポイント（例えば、０～１００）等が入力される。
なお、優先順位が入力された場合には、所定の規則によりポイントに変換されてもよい。例えば、４種類の認証方式に１位から４位までの優先順位が指定された場合、１位が１００ポイント、２位が７５ポイント、３位が５０ポイント、４位が２５ポイントのように変換されてもよい。
また、特定の認証方式のみが優先される場合、例えば、この認証方式に対して１００ポイントが入力され、他の認証方式には０ポイントが入力されてもよい。
【００４６】
（ｂ）登録・認証経過時間
サービス事業者の提供するサービスを使用する上で、利用者が選択可能な認証方式において、パスワード又は生体情報等の認証に用いる情報の登録、及び認証処理にどのくらいの時間を要するかを示す項目として、選択可能な認証方式における登録・認証経過時間が入力される。
入力されるデータは、具体的な時間（分又は秒）でもよいし、段階的なレベル値でもよい。
【００４７】
（ｃ）登録・認証失敗回数
サービス事業者の提供するサービスを使用する上で、利用者が選択可能な認証方式において、登録・認証に成功するまでにどのくらいの回数失敗したのかを示す想定項目として、選択可能な認証方式における登録・認証失敗回数が入力される。

【００４８】
このとき、ユーザビリティポイントは、主観的な指標である利用者選択のポイントと、客観的な指標である登録・認証経過時間及び登録・認証失敗回数とを用いて、例えば下記の数式により算出される。
ユーザビリティポイント
＝認証方式における「利用者選択のポイント」×Ｐｕｓ１
＋Ｐｕｓ２／（当該認証方式における「登録・認証経過時間」）
＋Ｐｕｓ３／（当該認証方式における「登録・認証失敗回数」）
【００４９】
ただし、Ｐｕｓ１、Ｐｕｓ２、Ｐｕｓ３は、以下を意味している。
・Ｐｕｓ１：「利用者選択のポイント」を正規化するためのパラメータ
・Ｐｕｓ２：「登録・認証経過時間」を正規化するためのパラメータ
・Ｐｕｓ３：「登録・認証失敗回数」を正規化するためのパラメータ
【００５０】
（状況ポイント決定処理）
状況ポイント決定処理では、次の５種類の入力項目から、利用者が現在どのような状況に置かれているのかに応じて、どの認証方式の組み合わせを優先的に使用すべきかが決定される。
【００５１】
（ａ）ユーザビリティポイント
選択可能な認証方式と、この認証方式に対してユーザビリティポイント決定処理により算出されたユーザビリティポイントとが入力される。
【００５２】
（ｂ）時間情報
サービス事業者の提供するサービスを使用する上で、利用者が対象の認証方式をいつ使用しようとしているのかを示す時間情報が入力される。
【００５３】
（ｃ）位置情報
サービス事業者の提供するサービスを使用する上で、利用者が対象の認証方式をどこで使用しようとしているのかを示す位置情報が入力される。
【００５４】
（ｄ）周辺情報
サービス事業者の提供するサービスを使用する上で、利用者が対象の認証方式をどのような状況で使用しようとしているのかを示す周辺情報が入力される。
周辺情報は、例えば、明るい場所なのか暗い場所なのか、静かな場所なのか騒がしい場所なのか、近くに人がいるのかいないのか等、選択される認証方式によって好都合又は不都合となり得る状況を表す項目である。
【００５５】
（ｅ）移動手段情報
サービス事業者の提供するサービスを使用する上で、利用者が対象の認証方式をどのように移動しながら使用しようとしているのかを示す移動手段情報が入力される。
移動手段情報は、例えば、電車、歩き、静止等の種別を表す。
【００５６】
このとき、１つの認証方式における状況ポイントは、下記の数式により算出される。
１つの認証方式における状況ポイント
＝「ユーザビリティポイント」
×ｆ（Ｐｓｔ１，Ｐｓｔ２，Ｐｓｔ３，Ｐｓｔ４）×Ｐｓｔ５
【００５７】
ただし、ｆ、Ｐｓｔ１、Ｐｓｔ２、Ｐｓｔ３、Ｐｓｔ４、Ｐｓｔ５は、以下を意味している。

・ｆ：時間情報、位置情報、周辺情報、移動手段情報をパラメータとする関数
・Ｐｓｔ１：対象の認証方式が使用される時間情報を表すパラメータ
・Ｐｓｔ２：対象の認証方式が使用される位置情報を表すパラメータ
・Ｐｓｔ３：対象の認証方式が使用される周辺情報を表すパラメータ
・Ｐｓｔ４：対象の認証方式が使用される移動手段情報を表すパラメータ
・Ｐｓｔ５：対象の認証方式における状況ポイントを正規化するためのパラメータ

【００５８】

なお、ｆは、認証方式毎に異なる関数である。

例えば、音声認証であれば周辺情報としての周囲の音量（静かな場所なのか騒がしい場所なのか）が重要であるし、パスワード認証であれば、近くに人がいるかいないか（覗き見のリスクがあるかないか）が重要である。また、認証方式によって、時間情報、位置情報、周辺情報、移動手段情報それぞれの重要度が異なる。

このため、認証方式毎に、各情報の重み付けが適宜設定され、それぞれ異なる関数が設けられる。

【００５９】

ここで、複数の認証方式を組み合わせる方法として、ＡＮＤ、ＯＲ、重み付けの３種類がある。認証方式の組み合わせに対する状況ポイントの算出方法、及び認証方式の実行順は次のようになる。

なお、以降の数式中で、Ｍ、ｎ、Ｗｉは、以下を意味している。

・Ｍ：状況ポイントを正規化する際の最大値
・ｎ：認証方式を複数組み合わせた場合の認証方式の個数
・Ｗｉ：認証方式ｉにおける重み

【００６０】

（ア）ＡＮＤの場合

組み合わせ方法がＡＮＤの場合における状況ポイントの算出方法は以下の通りである。

【数１】

$$\text{ANDの場合における状況ポイント} = M \times \prod_{i=1}^{n} \left(\text{認証方式}i\text{の状況ポイント}/M\right)$$

【００６１】

ＡＮＤの場合における複数の認証方式は、状況ポイントが低い認証方式から順に、すなわち、利便性の低い認証方式から順に実行され、認証失敗時に要した手間が最小となるようにしてよい。

【００６２】

（イ）ＯＲの場合

組み合わせ方法がＯＲの場合における状況ポイントの算出方法は以下の通りである。

【数２】

$$\begin{aligned}&\text{OR の場合における状況ポイント}\\&= M\\&\times \sum_{i=1}^{n} \left[\left(\text{認証方式}i\text{の状況ポイント}/M\right)\right.\\&\left.\times \prod_{j=1}^{j<i} \left\{1 - \left(\text{認証方式}j\text{の状況ポイント}/M\right)\right\} \right]\end{aligned}$$

【００６３】

ＯＲの場合における複数の認証方式は、状況ポイントが高い認証方式から順に、すなわ

ち、利便性の高い認証方式から順に実行され、認証成功時に要した手間が最小となるようにしてよい。

【００６４】

（ウ）重み付けの場合

重み付けとは、例えば、以下のような方式である。

２種類の認証方式Ａ及びＢにおいて、認証方式Ａの閾値に対して９０％の照合率で認証失敗し、認証方式Ｂの閾値Ｂに対して１５０％の照合率で認証成功している場合を想定する。このとき、認証方式Ａを０．６、認証方式Ｂを０．４の重み付けとした場合、照合率は、それぞれ５４％及び６０％に重み付けされ、両方共に重み付けされた平均の閾値５０％を超え、認証成功となる。

【００６５】

組み合わせ方法が重み付けの場合における状況ポイントの算出方法は以下の通りである。

【数３】

重み付けの場合における状況ポイント

$$= M \times \prod_{i=1}^{n} \left[\left(\text{認証方式}i\text{の状況ポイント} / M \right) \times Wi \Big/ \left\{ \left(\sum_{j=1}^{n} Wj \right) \Big/ n \right\} \right]$$

【００６６】

重み付けの場合における複数の認証方式は、状況ポイントが低い認証方式から順に、すなわち、利便性の低い認証方式から順に実行され、認証失敗時に要した手間が最小となるようにしてよい。

【００６７】

（安全性ポイント決定処理）

安全性ポイント決定処理では、認証サーバ３０の管理者が入力する次の４種類の項目から、各認証方式が単独で使用される場合にどの程度の安全性を有するのかが決定される。

【００６８】

（ａ）全数攻撃の成功確率

各認証方式が単独で使用される場合、攻撃者が全数攻撃にどの程度の確率で成功するのかを示す全数攻撃の成功確率が入力される。全数攻撃とは、例えば、パスワード認証に対して、入力可能な全てのパスワードのパターンを試行する攻撃である。

【００６９】

（ｂ）特殊攻撃の成功確率

各認証方式が単独で使用される場合、攻撃者が全数攻撃以外の特殊攻撃にどの程度の確率で成功するのかを示す特殊攻撃の成功確率が特殊攻撃の種別と共に入力される。

【００７０】

（ｃ）攻撃費用

各認証方式が単独で使用される場合、攻撃者が各攻撃にどの程度の費用を要するのかを示す攻撃費用が攻撃の種別と共に入力される。

【００７１】

（ｄ）攻撃時間

各認証方式が単独で使用される場合、攻撃者が各攻撃にどの程度の時間を要するのかを示す攻撃時間が攻撃の種別と共に入力される。

【００７２】

このとき、安全性ポイントは、下記の数式により算出される。

１つの認証方式における安全性ポイント

＝Ｐｓｃ１／「全数攻撃の成功確率」

＋Ｐｓｃ２／ｍａｘ（「特殊攻撃の種別」に対する「特殊攻撃の成功確率」）

＋（上記の「特殊攻撃の種別」に対する「攻撃費用」）×Ｐｓｃ３
＋（上記の「特殊攻撃の種別」に対する「攻撃時間」）×Ｐｓｃ４
【００７３】
ただし、Ｐｓｃ１、Ｐｓｃ２、Ｐｓｃ３、Ｐｓｃ４は、以下を意味している。
・Ｐｓｃ１：「全数攻撃の成功確率」を正規化するためのパラメータ
・Ｐｓｃ２：「特殊攻撃の成功確率」を正規化するためのパラメータ
・Ｐｓｃ３：「攻撃費用」を正規化するためのパラメータ
・Ｐｓｃ４：「攻撃時間」を正規化するためのパラメータ
【００７４】
なお、成功確率が最も高い特殊攻撃が複数存在する場合には、安全性ポイント決定処理では、以下の順序で、特殊攻撃の絞込みが行われる。
（１）「攻撃費用」が少ない特殊攻撃。
（２）（１）において「攻撃費用」が同じ特殊攻撃が存在する場合、「攻撃時間」が短い特殊攻撃。
（３）（２）において「攻撃時間」も同じ特殊攻撃が存在する場合、最初に記述されている特殊攻撃。
【００７５】
（認証ポイント決定処理）
認証ポイント決定処理では、認証サーバ３０の管理者が入力する次の４種類の項目から、各認証方式が他の方式と組み合わされて使用される場合にどの程度の安全性を有するのかが決定される。
【００７６】
（ａ）安全性ポイント
選択可能な認証方式と、この認証方式に対して安全性ポイント決定処理により算出された安全性ポイントとが入力される。
【００７７】
（ｂ）ワンタイム性
各認証方式が一時的な情報を使用するか固定された情報を使用するかを示すワンタイム性が入力される。ワンタイム性は、例えば０～１の値であり、情報が複数回使用される場合は０と１との間の値となる。
【００７８】
（ｃ）所有物認証性
各認証方式が利用者の所有物による認証であるか否かを示す所有物認証性が入力される。
所有物による認証では、利用者が対象物を持っているか否かにより本人性を確認するので、対象物を盗まれるリスクがあるが、他の認証方式と組み合わせることにより安全性が高まる。そこで、認証ポイント決定処理では、この所有物認証性により、認証方式の組み合わせに対する安全性ポイントが調整される。
【００７９】
（ｄ）多要素性
各認証方式が複数の認証方式を組み合わせて使用されるか否かを示す多要素性が入力される。
【００８０】
このとき、認証方式ｉ（認証ポイントｉ）と認証方式ｊ（認証ポイントｊ）とを組み合わせた場合の認証ポイント（ｉ，ｊ）は、下記の数式により算出される。
（ア）認証方式ｉ∧認証方式ｊの場合
認証ポイント（ｉ，ｊ）＝ｍａｘ（認証ポイントｉ，認証ポイントｊ）
（イ）認証方式ｉ∨認証方式ｊの場合
認証ポイント（ｉ，ｊ）＝ｍｉｎ（認証ポイントｉ，認証ポイントｊ）
（ウ）各認証方式に重みがある場合

認証ポイント（ｉ，ｊ）＝認証ポイントｉ×Ｗｉ＋認証ポイントｊ×Ｗｊ

【００８１】

なお、各認証方式における認証ポイントｋ（ｋ＝ｉのときｋ’＝ｊ、ｋ＝ｊのときｋ’＝ｉとする）の算出方法は、以下の通りである。

認証ポイントｋ

＝「安全性ポイント」

×（１＋「ワンタイム性」）

×（１＋「所有物認証性」×Ｐａｕ１）

×（１＋「多要素性」×Ｐａｕ２）

×Ｐａｕ３

【００８２】

ただし、Ｐａｕ１、Ｐａｕ２、Ｐａｕ３は、以下を意味している。

・Ｐａｕ１：認証方式ｋが所有物認証であり、かつ認証方式ｋ’が所有物認証でない場合のみ１になるパラメータ

・Ｐａｕ２：認証方式ｋが多要素認証可能であり、かつ、認証方式ｋ’も多要素認証可能である場合のみ１になるパラメータ

・Ｐａｕ３：各認証方式における認証ポイントを正規化するためのパラメータ

【００８３】

（認証方式決定処理）

認証方式決定処理では、サービスポイント、状況ポイント及び認証ポイントの各ポイントを入力として、利便性及び安全性に関して最もバランスのとれた認証方式の組み合わせが決定される。

【００８４】

図３は、本実施形態に係る認証方式の組み合わせ決定処理の一例を示すフローチャートである。

なお、予め対象サービスのサービスポイントと、想定される認証方式の組み合わせ毎の状況ポイント及び認証ポイントとが決定されているものとする。

【００８５】

ステップＳ１において、認証サーバ３０は、状況ポイントが０より大きい認証方式の組み合わせを抽出する。

【００８６】

ステップＳ２において、認証サーバ３０は、ステップＳ１で抽出された組み合わせのうち、認証ポイントがサービスポイント以上である認証方式の組み合わせを抽出する。

【００８７】

ステップＳ３において、認証サーバ３０は、ステップＳ２で抽出された組み合わせのうち、認証ポイントとサービスポイントとの差が最小のもの、すなわち、サービスポイントに比べて認証ポイントが高過ぎない認証方式の組み合わせを抽出する。

【００８８】

ステップＳ４において、認証サーバ３０は、ステップＳ３で抽出された組み合わせのうち、状況ポイントが最大のもの、すなわち、利用者の利便性が高い認証方式の組み合わせを抽出する。

【００８９】

本処理では、認証サーバ３０は、ステップＳ３において、「認証ポイントとサービスポイントとの差が最小」という条件で認証方式の絞り込みを行ったが、これには限られず、例えば、差が所定以内の認証方式の組み合わせを複数抽出してもよい。

【００９０】

次に、認証システム１において利用者端末１０がサービスの提供を受けるまでに、各装置（利用者端末１０、事業者サーバ２０、認証サーバ３０）間で連携される処理の流れを詳述する。

【００９１】

図４は、本実施形態に係る入力情報の登録処理を示すシーケンス図である。
本処理では、利用者端末１０に対応する前述のユーザビリティポイントを決定するために、利用者端末１０が認証方式の優先順位若しくはポイント、登録・認証経過時間及び登録・認証失敗回数の少なくともいずれかを含む入力情報を認証サーバ３０に登録する。
【００９２】
ステップＳ１１において、利用者端末１０は、認証サーバ３０に認証方式の優先順位登録要求を送信する。
【００９３】
ステップＳ１２において、認証サーバ３０は、ステップＳ１１で受け取った要求に対して、認証方式の優先順位登録応答を利用者端末１０に送信する。
【００９４】
ステップＳ１３において、利用者端末１０は、各認証方式に対する優先順位又はポイント、登録・認証経過時間及び登録・認証失敗回数の入力情報を受け付ける。
【００９５】
ステップＳ１４において、利用者端末１０は、ステップＳ１３で受け付けた入力情報の記載ファイルを認証サーバ３０に送信する。
【００９６】
ステップＳ１５において、認証サーバ３０は、ステップＳ１４で受信したファイルのフォーマット及び数値データの範囲等の正当性を検証し、検証ＯＫならば入力情報を登録し、検証ＮＧならば登録しない。
【００９７】
ステップＳ１６において、認証サーバ３０は、ステップＳ１５の検証及び登録の結果（ＯＫ／ＮＧ）を利用者端末に送信する。
【００９８】
ステップＳ１７において、利用者端末１０は、ステップＳ１６で受信した登録結果に対し、登録ＯＫならばステップＳ１４で送信したファイルを保存し、登録ＮＧならば当該ファイルを保存しない。
【００９９】
図５は、本実施形態に係る認証方式を利用するための照合情報登録処理を示すシーケンス図である。
本処理では、認証サーバ３０で認証を実施するために、利用者端末１０が認証方式毎のパスワード又は生体情報等の照合情報を認証サーバ３０に登録する。
【０１００】
ステップＳ２１において、利用者端末１０は、認証サーバ３０に認証方式の情報登録要求を送信する。
【０１０１】
ステップＳ２２において、認証サーバ３０は、ステップＳ２１で受信した要求に対して、認証方式の情報登録応答と認証方式リスト要求とを利用者端末１０に送信する。
【０１０２】
ステップＳ２３において、利用者端末１０は、ステップＳ２２で受信した要求に対し、情報を登録する認証方式のリストを認証サーバ３０に送信する。
【０１０３】
ステップＳ２４において、認証サーバ３０は、ステップＳ２３で受信した認証方式リストに応じて、認証方式の登録情報要求を利用者端末１０に送信する。
【０１０４】
ステップＳ２５において、利用者端末１０は、各認証方式に対する登録情報の入力を受け付ける。
【０１０５】
ステップＳ２６において、利用者端末１０は、ステップＳ２５で受け付けた登録情報を認証サーバ３０に送信する。

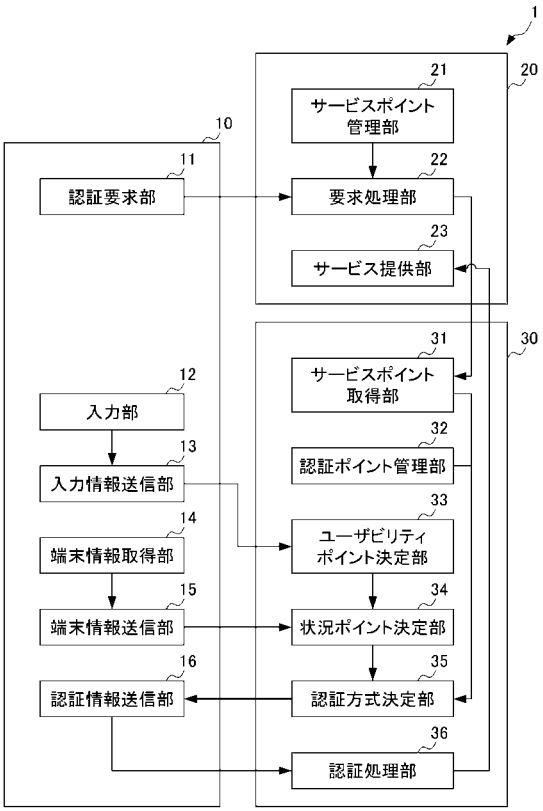
【０１０６】
ステップＳ２７において、認証サーバ３０は、ステップＳ２６で受信した登録情報が有効なデータであることを検証し、検証ＯＫならば登録情報を登録し、検証ＮＧならば当該情報を登録しない。
【０１０７】
ステップＳ２８において、認証サーバ３０は、ステップＳ２７の登録結果（ＯＫ／ＮＧ）を利用者端末１０に送信する。認証サーバ３０は、ステップＳ２３で受信した認証方式リストに記載されている全ての認証方式の情報が登録されていればステップＳ２９に処理を進め、登録されていなければステップＳ２４～Ｓ２８を繰り返す。
【０１０８】
ステップＳ２９において、認証サーバ３０は、登録完了応答を利用者端末１０に送信する。
【０１０９】
図６は、本実施形態に係る認証方式の選定及び認証の処理を示すシーケンス図である。
本処理では、利用者端末１０、事業者サーバ２０及び認証サーバ３０の３者間の連携により、認証方式の選定と選定された方式による認証とが実施される。
【０１１０】
ステップＳ３１において、利用者端末１０は、事業者サーバ２０にサービス要求を送信する。
【０１１１】
ステップＳ３２において、事業者サーバ２０は、ステップＳ３１で受信した要求に対して、サービス応答と前述のサービスポイントとを利用者端末１０に送信する。
【０１１２】
ステップＳ３３において、利用者端末１０は、ステップＳ３２で受信した応答に対して、認証サーバ３０にサービスリダイレクト応答と共にサービスポイントを送信する。
【０１１３】
ステップＳ３４において、認証サーバ３０は、ステップＳ３３で受信した応答に対して、利用者端末１０に端末情報要求を送信する。
【０１１４】
ステップＳ３５において、利用者端末１０は、端末情報として、前述の状況ポイントを算出するための時間情報、位置情報、周辺情報及び移動手段情報を取得する。
【０１１５】
ステップＳ３６において、利用者端末１０は、ステップＳ３４で受信した要求に対して、認証サーバ３０に端末情報を送信する。
【０１１６】
ステップＳ３７において、認証サーバ３０は、ステップＳ３３で受信したサービスポイント、ステップＳ３６で受信した端末情報に基づいて算出される状況ポイント、及び認証ポイントから認証方式を自動的に選定する。
【０１１７】
ステップＳ３８において、認証サーバ３０は、ステップＳ３７で選定した認証方式毎に、利用者端末１０に認証要求を送信する。
なお、複数の認証方式を組み合わせる場合には、組み合わせ方として、ＡＮＤ、ＯＲ、重み付けの３種類がある。ＡＮＤ又は重み付けの場合は、状況ポイントが低い認証方式から順に実施し、ＯＲの場合は、状況ポイントが高い認証方式から実施する。
【０１１８】
ステップＳ３９において、利用者端末１０は、各認証方式に対する認証情報の入力を受け付ける。
【０１１９】
ステップＳ４０において、利用者端末１０は、ステップＳ３９で受け付けた認証情報を認証サーバ３０に送信する。

【０１２０】
ステップＳ４１において、認証サーバ３０は、ステップＳ４０で受信した認証情報と、事前に登録した登録情報とを照合する。
【０１２１】
ステップＳ４２において、認証サーバ３０は、ステップＳ４１で行った照合の結果（ＯＫ／ＮＧ）を利用者端末１０に送信する。認証サーバ３０は、ステップＳ３７で選定された認証方式による認証が完了していればステップＳ４３に処理を進め、完了していなければステップＳ３８～Ｓ４２を繰り返す。
【０１２２】
ステップＳ４３において、認証サーバ３０は、ステップＳ３８～Ｓ４２で繰り返し行った照合結果から得られた認証結果（ＯＫ／ＮＧ）を利用者端末１０に送信する。
【０１２３】
ステップＳ４４において、利用者端末１０は、ステップＳ４３で得られた認証結果が認証ＯＫならば事業者サーバ２０に認証成功リダイレクト応答を送信し、認証ＮＧならば強制終了する。
【０１２４】
ステップＳ４５において、事業者サーバ２０は、ステップＳ４４で受信した応答を検証し、検証ＯＫならば認証サーバ３０にトークン要求を送信し、検証ＮＧならば強制終了する。
【０１２５】
ステップＳ４６において、認証サーバ３０は、ステップＳ４５で受信した要求を検証し、要求元が認証に成功した利用者端末１０である（検証ＯＫ）ならばトークンを発行し、検証ＮＧならば強制終了する。
【０１２６】
ステップＳ４７において、認証サーバ３０は、ステップＳ４６で発行したトークンを事業者サーバ２０に送信する。
【０１２７】
ステップＳ４８において、事業者サーバ２０は、ステップＳ４７で受信した応答を検証し、検証ＯＫならば利用者端末１０にサービスを提供し、検証ＮＧならば強制終了する。
【０１２８】
本実施形態によれば、利用者端末１０、事業者サーバ２０、認証サーバ３０の３者間において、多種多様に存在する認証方式を統合するための認証システム１を実現した。
認証システム１は、サービス毎にサービスポイントを管理し、認証方式の組み合わせ毎に認証ポイントを管理する。そして、認証システム１は、認証ポイントがサービスポイント以上である認証方式の組み合わせのうち、認証ポイント及びサービスポイントの差分が小さい組み合わせを優先して決定する。したがって、認証システム１は、サービスに応じて必要とされる安全性を満たし、かつ、サービスポイントに比べて認証ポイントが高過ぎない認証方式の組み合わせを適切に決定できる。
【０１２９】
また、認証システム１は、認証方式の組み合わせ毎に状況ポイントを算出し、この状況ポイントが大きい組み合わせを優先して決定する。したがって、認証システム１は、サービスに応じて必要とされる安全性を満たし、かつ、サービスポイントに比べて認証ポイントが高過ぎない、さらに、利用者の利便性が高いものを優先して、認証方式の組み合わせを適切に決定できる。
このとき、認証システム１は、時刻情報、位置情報、周辺情報及び移動手段情報をパラメータとする認証方式毎に異なる関数を用いて状況ポイントを算出するので、認証時点におけるユーザの状況を認証方式に応じて適切に評価し、認証方式の組み合わせを適切に決定できる。
【０１３０】
また、認証システム１は、ユーザの入力情報に基づいてユーザビリティポイントを算出

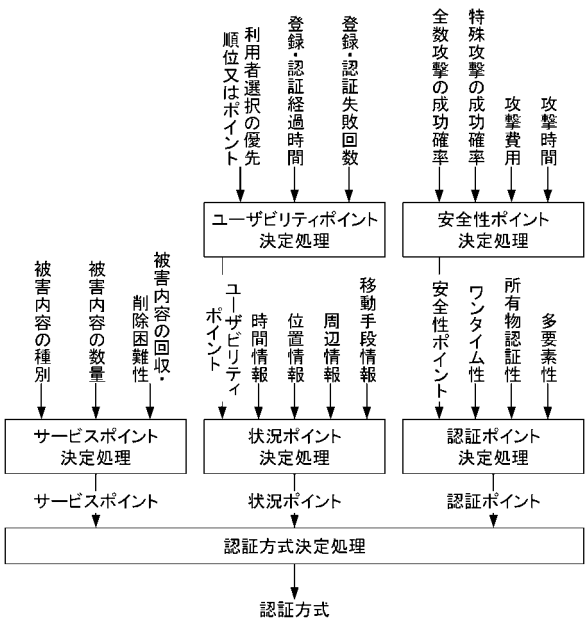
することにより、ユーザの利便性をより適切に評価して、認証方式の組み合わせを適切に決定できる。
さらに、認証システム１は、認証方式の組み合わせのパターン（ＡＮＤ、ＯＲ又は重み付け）に応じて、それぞれ異なる計算式により状況ポイント及び認証ポイントを算出する。したがって、認証システム１は、認証方式の組み合わせ方を区別して、各ポイントをより適切に求めることができ、認証方式の組み合わせを適切に決定できる。
【０１３１】
また、認証システム１は、状況ポイントの大きさにより認証方式の実行順を決定するので、複数の認証方式を組み合わせた際の利用者の負担を低減できる。
【０１３２】
また、認証システム１は、攻撃の種別毎の成功確率、費用又は時間に基づいて安全性ポイントを算出するので、様々な攻撃を想定して認証方式の安全性をより適切に評価し、認証方式の組み合わせを適切に決定できる。
このとき、認証システム１は、全数攻撃と特殊攻撃とを区別し、さらに、攻撃成功確率が最大の特殊攻撃の情報を用いて安全性ポイントを算出するので、認証方式毎の安全性をより適切に評価でき、この結果、認証方式の組み合わせを適切に決定できる。
【０１３３】
以上、本発明の実施形態について説明したが、本発明は前述した実施形態に限るものではない。また、本実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、本実施形態に記載されたものに限定されるものではない。
【０１３４】
本実施形態では、利用者端末１０から受信した情報に基づいて認証サーバ３０がユーザビリティポイント及び状況ポイントを算出したが、これには限られない。例えば、利用者端末１０がユーザビリティポイント及び状況ポイントを算出し、認証サーバ３０へ提供してもよい。
【０１３５】
本実施形態では、事業者サーバ２０により提供されるサービスについての認証を認証サーバ３０が実施したが、事業者サーバ２０と認証サーバ３０とが同一、すなわち事業者サーバ２０が認証サーバ３０の機能を備えていてもよい。
【０１３６】
認証システム１による認証方法は、ソフトウェアにより実現される。ソフトウェアによって実現される場合には、このソフトウェアを構成するプログラムが、情報処理装置（利用者端末１０、事業者サーバ２０、認証サーバ３０）にインストールされる。また、これらのプログラムは、ＣＤ－ＲＯＭのようなリムーバブルメディアに記録されてユーザに配布されてもよいし、ネットワークを介してユーザのコンピュータにダウンロードされることにより配布されてもよい。さらに、これらのプログラムは、ダウンロードされることなくネットワークを介したＷｅｂサービスとしてユーザのコンピュータ（利用者端末１０、事業者サーバ２０、認証サーバ３０）に提供されてもよい。
【符号の説明】
【０１３７】
１　認証システム
１０　利用者端末
１１　認証要求部
１２　入力部
１３　入力情報送信部
１４　端末情報取得部
１５　端末情報送信部
１６　認証情報送信部
２０　事業者サーバ

２１　サービスポイント管理部
２２　要求処理部
２３　サービス提供部
３０　認証サーバ
３１　サービスポイント取得部
３２　認証ポイント管理部
３３　ユーザビリティポイント決定部
３４　状況ポイント決定部
３５　認証方式決定部
３６　認証処理部

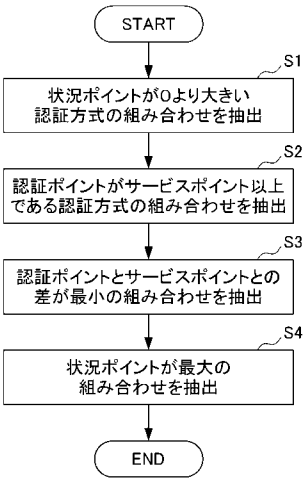
【図１】



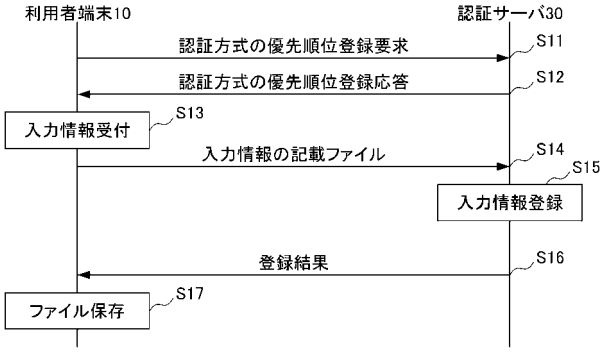
【図２】



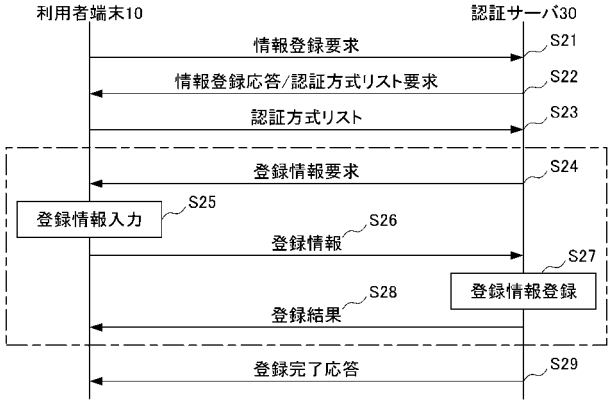
【図３】


START
S1
状況ポイントが0より大きい
認証方式の組み合わせを抽出
S2
認証ポイントがサービスポイント以上
である認証方式の組み合わせを抽出
S3
認証ポイントとサービスポイントとの
差が最小の組み合わせを抽出
S4
状況ポイントが最大の
組み合わせを抽出
END

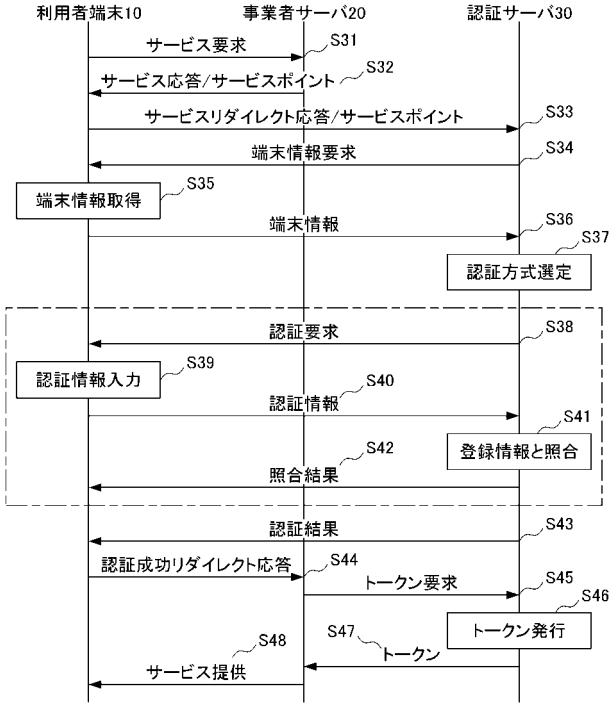
【図４】


利用者端末10
認証サーバ30
認証方式の優先順位登録要求
S11
認証方式の優先順位登録応答
S12
入力情報受付
S13
入力情報の記載ファイル
S14
S15
入力情報登録
登録結果
S16
ファイル保存
S17

【図５】


利用者端末10
認証サーバ30
情報登録要求
S21
情報登録応答/認証方式リスト要求
S22
認証方式リスト
S23
登録情報要求
S24
登録情報入力
S25
登録情報
S26
S27
登録情報登録
登録結果
S28
登録完了応答
S29

【図６】


利用者端末10
事業者サーバ20
認証サーバ30
サービス要求
S31
サービス応答/サービスポイント
S32
サービスリダイレクト応答/サービスポイント
S33
端末情報要求
S34
端末情報取得
S35
端末情報
S36
S37
認証方式選定
認証要求
S38
認証情報入力
S39
認証情報
S40
S41
登録情報と照合
照合結果
S42
認証結果
S43
認証成功リダイレクト応答
S44
トークン要求
S45
S46
トークン発行
S47
トークン
S48
サービス提供