(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5081696号
(P5081696)
(45)発行日　平成24年11月28日(2012.11.28)　(24)登録日　平成24年9月7日(2012.9.7)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 21/20　131A
G06K 17/00 (2006.01)　　G06K 17/00　T
H04L 9/32 (2006.01)　　H04L 9/00　675D

請求項の数 11　(全 24 頁)

(21)出願番号　特願2008-93758(P2008-93758)
(22)出願日　平成20年3月31日(2008.3.31)
(65)公開番号　特開2009-245365(P2009-245365A)
(43)公開日　平成21年10月22日(2009.10.22)
審査請求日　平成22年10月26日(2010.10.26)

(73)特許権者　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(74)代理人　100095407
弁理士　木村　満
(72)発明者　板屋　一嗣
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　道坂　修
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　前田　秀介
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

最終頁に続く

(54)【発明の名称】情報処理システム、認証サーバ、サービス提供サーバ、認証方法、サービス提供方法、及び、プログラム

(57)【特許請求の範囲】
【請求項１】
ユーザ端末と、ユーザにサービスを提供するための複数の処理を実行するサービス提供サーバと、当該ユーザを認証する認証サーバとを有する情報処理システムにおいて、
前記ユーザ端末は、
当該ユーザを認証するための認証用データを取得する取得部と、
当該ユーザからの指示に基づいて、前記サービス提供サーバに当該複数の処理を開始する旨の開始要求と、前記取得された認証用データと、を前記サービス提供サーバに送信する開始要求送信部と、
を備え、
前記サービス提供サーバは、
当該複数の処理のそれぞれについて、前記認証サーバによる当該ユーザの認証が必要か否かを示す情報を記憶する認証要否情報記憶部と、
前記ユーザ端末から当該開始要求と当該認証用データを受信する開始要求受信部と、
前記受信した開始要求が示す当該複数の処理の中に、前記認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信部と、
を備え、
前記認証サーバは、

当該ユーザを認証するためのユーザ情報を予め記憶するユーザ情報記憶部と、
前記サービス提供サーバから当該認証要求と当該認証用データとを受信する認証要求受信部と、
前記認証要求受信部が当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定部と、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信部と、
前記認証要求受信部が当該認証要求を受信した場合、当該認証用データと前記ユーザ情報記憶部に記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証部と、
前記認証部による認証結果を前記サービス提供サーバに送信する認証結果送信部と、
を備え、
前記サービス提供サーバは、更に、
当該推定時間を前記認証サーバから受信する推定時間受信部と、
当該認証結果を前記認証サーバから受信する認証結果受信部と、
前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから、当該認証結果を受信するまで、当該処理群に含まれる処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該ユーザの認証に成功した旨の当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供部と、
を備えることを特徴とする情報処理システム。

【請求項２】
前記取得部は、当該認証用データとして、ＩＣ（Integrated Circuit）カードに予め記憶された個人情報を取得し、
前記認証部は、前記ユーザ端末から前記サービス提供サーバを介して送信された当該認証用データを用いて認証する、
ことを特徴とする、請求項１に記載の情報処理システム。

【請求項３】
前記認証要求送信部は、前記ＩＣカードの種類を示す情報を含む当該認証要求を前記認証サーバに送信し、
前記認証サーバは、前記ＩＣカードの種類に対応付けて、過去に当該認証要求を受信してから当該ユーザの認証を終了するまでにかかった時間を記憶する処理時間記憶部を更に備え、
前記推定部は、前記認証要求受信部が受信した認証要求が示す前記ＩＣカードの種類に対応付けられた時間に基づいて、当該推定時間を推定する、
ことを特徴とする、請求項２に記載の情報処理システム。

【請求項４】
前記認証部は、当該ユーザを認証する処理を開始してから終了するまでにかかった時間を用いて、前記処理時間記憶部に記憶されている時間のうち前記ＩＣカードの種類に対応する時間を更新する、
ことを特徴とする、請求項３に記載の情報処理システム。

【請求項５】
前記認証サーバは、前記認証部による認証結果を記憶する認証結果記憶部を更に備え、
前記認証結果受信部は、当該推定時間が所定値以上の場合、前記推定時間受信部が当該推定時間を受信してから当該推定時間が経過した後、当該認証結果を送信するよう前記認証サーバに要求し、当該認証結果を前記認証サーバから受信する、
ことを特徴とする、請求項１乃至４のいずれか１項に記載の情報処理システム。

【請求項６】
ユーザを認証するためのユーザ情報を予め記憶するユーザ情報記憶部と、
当該ユーザにサービスを提供するサービス提供サーバから、当該ユーザを認証する旨の

認証要求と、当該ユーザを認証するための認証用データとを受信する認証要求受信部と、
前記認証要求受信部が当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定部と、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信部と、
前記認証要求受信部が当該認証要求を受信した場合、当該認証用データと前記ユーザ情報記憶部に記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証部と、
前記認証部による認証結果を前記サービス提供サーバに送信する認証結果送信部と、
を備えることを特徴とする認証サーバ。
【請求項７】
ユーザにサービスを提供するための複数の処理のそれぞれについて、当該ユーザを認証する認証サーバによる当該ユーザの認証が必要か否かを示す情報を記憶する認証要否情報記憶部と、
当該複数の処理を開始する旨の開始要求と、当該ユーザを認証するための認証用データとを、当該ユーザが使用するユーザ端末から受信する開始要求受信部と、
前記受信した開始要求が示す複数の処理の中に、前記認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信部と、
前記認証サーバが当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる推定時間を、前記認証サーバから受信する推定時間受信部と、
当該ユーザの認証結果を前記認証サーバから受信する認証結果受信部と、
前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから当該認証結果を受信するまで、当該複数の処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該ユーザの認証に成功した旨の当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供部と、
を備えることを特徴とするサービス提供サーバ。
【請求項８】
ユーザにサービスを提供するサービス提供サーバから、当該ユーザを認証する旨の認証要求と、当該ユーザを認証するための認証用データとを受信する認証要求受信ステップと、
前記認証要求受信ステップが当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定ステップと、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信ステップと、
前記認証要求受信ステップが当該認証要求を受信した場合、当該認証用データと当該ユーザを認証するための予めメモリに記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証ステップと、
前記認証ステップによる認証結果を前記サービス提供サーバに送信する認証結果送信ステップと、
を備えることを特徴とする認証方法。
【請求項９】
複数の処理を開始する旨の開始要求と、ユーザを認証するための認証用データとを、当該ユーザが使用するユーザ端末から受信する開始要求受信ステップと、
前記受信した開始要求が示す複数の処理の中に、認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信ステップと、
前記認証サーバが当該認証要求を受信してから当該ユーザの認証を終了するまでにかか

る推定時間を、前記認証サーバから受信する推定時間受信ステップと、
当該ユーザの認証結果を前記認証サーバから受信する認証結果受信ステップと、
前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから当該認証結果を受信するまで、当該複数の処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該ユーザの認証に成功した旨の当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供ステップと、
を備えることを特徴とするサービス提供方法。
【請求項１０】
コンピュータを、
ユーザを認証するためのユーザ情報を予め記憶するユーザ情報記憶部、
当該ユーザにサービスを提供するサービス提供サーバから、当該ユーザを認証する旨の認証要求と、当該ユーザを認証するための認証用データとを受信する認証要求受信部、
前記認証要求受信部が当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定部、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信部、
前記認証要求受信部が当該認証要求を受信した場合、当該認証用データと前記ユーザ情報記憶部に記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証部、
前記認証部による認証結果を前記サービス提供サーバに送信する認証結果送信部、
として機能させることを特徴とするプログラム。
【請求項１１】
コンピュータを、
ユーザにサービスを提供するための複数の処理のそれぞれについて、当該ユーザを認証する認証サーバによる当該ユーザの認証が必要か否かを示す情報を記憶する認証要否情報記憶部、
当該複数の処理を開始する旨の開始要求と、当該ユーザを認証するための認証用データとを、当該ユーザが使用するユーザ端末から受信する開始要求受信部、
前記受信した開始要求が示す複数の処理の中に、前記認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信部、
前記認証サーバが当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる推定時間を、前記認証サーバから受信する推定時間受信部、
当該ユーザの認証結果を前記認証サーバから受信する認証結果受信部、
前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから当該認証結果を受信するまで、当該複数の処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供部、
として機能させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、行うべき処理群の中に多くの時間を要する処理がある場合にも処理群全体を効率よく実行するために好適な情報処理システム、認証サーバ、サービス提供サーバ、認証方法、サービス提供方法、及び、プログラムに関する。
【背景技術】
【０００２】

近年、情報漏洩や不正利用を防止するために、ＩＣチップを搭載したカードが普及している。特許文献１には、例えば銀行のＡＴＭ（Automated Teller Machine）や窓口等で手続を行う際、ＩＣチップを搭載した運転免許証などの外部の機関が発行する身分証明書を用いて認証者（サーバ）が認証し、本人であるかを確認しつつサービスを提供するシステムが開示されている。

例えば、サービス提供側のシステムは、ＩＣカード等を用いたユーザ認証処理、入出金額の入力を受け付ける処理、振込先や振込元の入力を受け付ける処理、振り込みを実行する処理など、複数の処理のまとまり（以下「処理群」と呼ぶ。）を実行することによって、ユーザにサービスを提供する。

【特許文献１】特開２００７－２４１６４７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

ところで、ユーザを認証する処理など、サーバへの特定の処理の要求が集中すると、要求された処理の負荷が大きくなり、要求された処理ばかりか、処理群全体が完了するまでに多くの時間を要してしまうことがある。例えば、ユーザ認証処理を含む一連の処理群を実行する場合において、ユーザ認証処理に多くの時間を要すると、認証結果を受け取るまでの間、ユーザ認証処理が終わるまで処理群全体が待ち状態となり、結果的にシステムのレスポンスが悪くなったり、タイムアウトにより認証要求そのものが失敗したりしてしまう可能性がある。このように、行うべき処理群の中に多くの時間を要する処理があると、処理群全体のレスポンスが低下してしまう恐れがあるという問題があった。

【０００４】

本発明はこのような課題を解決するものであり、行うべき処理群の中に多くの時間を要する処理がある場合にも処理群全体を効率よく実行するために好適な情報処理システム、認証サーバ、サービス提供サーバ、認証方法、サービス提供方法、及び、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】

【０００５】

上記目的を達成するため、本発明の第１の観点に係る情報処理システムは、

ユーザ端末と、ユーザにサービスを提供するための複数の処理を実行するサービス提供サーバと、当該ユーザを認証する認証サーバとを有する情報処理システムにおいて、

前記ユーザ端末は、

当該ユーザを認証するための認証用データを取得する取得部と、

当該ユーザからの指示に基づいて、前記サービス提供サーバに当該複数の処理を開始する旨の開始要求と、前記取得された認証用データと、を前記サービス提供サーバに送信する開始要求送信部と、

を備え、

前記サービス提供サーバは、

当該複数の処理のそれぞれについて、前記認証サーバによる当該ユーザの認証が必要か否かを示す情報を記憶する認証要否情報記憶部と、

前記ユーザ端末から当該開始要求と当該認証用データを受信する開始要求受信部と、

前記受信した開始要求が示す当該複数の処理の中に、前記認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信部と、

を備え、

前記認証サーバは、

当該ユーザを認証するためのユーザ情報を予め記憶するユーザ情報記憶部と、

前記サービス提供サーバから当該認証要求と当該認証用データとを受信する認証要求受信部と、

前記認証要求受信部が当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定部と、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信部と、
前記認証要求受信部が当該認証要求を受信した場合、当該認証用データと前記ユーザ情報記憶部に記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証部と、
前記認証部による認証結果を前記サービス提供サーバに送信する認証結果送信部と、
を備え、
前記サービス提供サーバは、更に、
当該推定時間を前記認証サーバから受信する推定時間受信部と、
当該認証結果を前記認証サーバから受信する認証結果受信部と、
前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから、当該認証結果を受信するまで、当該処理群に含まれる処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該ユーザの認証に成功した旨の当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供部と、
を備えることを特徴とする。

【０００６】

前記取得部は、当該認証用データとして、ＩＣ（Integrated Circuit）カードに予め記憶された個人情報を取得してもよい。
そして、前記認証部は、前記ユーザ端末から前記サービス提供サーバを介して送信された当該認証用データを用いて認証してもよい。

【０００７】

前記認証要求送信部は、前記ＩＣカードの種類を示す情報を含む当該認証要求を前記認証サーバに送信してもよい。
また、前記認証サーバは、前記ＩＣカードの種類に対応付けて、過去に当該認証要求を受信してから当該ユーザの認証を終了するまでにかかった時間を記憶する処理時間記憶部を更に備えることができる。
そして、前記推定部は、前記認証要求受信部が受信した認証要求が示す前記ＩＣカードの種類に対応付けられた時間に基づいて、当該推定時間を推定してもよい。

【０００８】

前記認証部は、当該ユーザを認証する処理を開始してから終了するまでにかかった時間を用いて、前記処理時間記憶部に記憶されている時間のうち前記ＩＣカードの種類に対応する時間を更新してもよい。

【０００９】

前記認証サーバは、前記認証部による認証結果を記憶する認証結果記憶部を更に備えることができる。
また、前記認証結果受信部は、当該推定時間が所定値以上の場合、前記推定時間受信部が当該推定時間を受信してから当該推定時間が経過した後、当該認証結果を送信するよう前記認証サーバに要求し、当該認証結果を前記認証サーバから受信してもよい。

【００１０】

上記目的を達成するため、本発明の第２の観点に係る認証サーバは、
ユーザを認証するためのユーザ情報を予め記憶するユーザ情報記憶部と、
当該ユーザにサービスを提供するサービス提供サーバから、当該ユーザを認証する旨の認証要求と、当該ユーザを認証するための認証用データとを受信する認証要求受信部と、
前記認証要求受信部が当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定部と、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信部と、
前記認証要求受信部が当該認証要求を受信した場合、当該認証用データと前記ユーザ情

報記憶部に記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証部と、
前記認証部による認証結果を前記サービス提供サーバに送信する認証結果送信部と、
を備えることを特徴とする。
【００１１】
上記目的を達成するため、本発明の第３の観点に係るサービス提供サーバは、
ユーザにサービスを提供するための複数の処理のそれぞれについて、当該ユーザを認証する認証サーバによる当該ユーザの認証が必要か否かを示す情報を記憶する認証要否情報記憶部と、
当該複数の処理を開始する旨の開始要求と、当該ユーザを認証するための認証用データとを、当該ユーザが使用するユーザ端末から受信する開始要求受信部と、
前記受信した開始要求が示す複数の処理の中に、前記認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信部と、
前記認証サーバが当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる推定時間を、前記認証サーバから受信する推定時間受信部と、
当該ユーザの認証結果を前記認証サーバから受信する認証結果受信部と、
前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから当該認証結果を受信するまで、当該複数の処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該ユーザの認証に成功した旨の当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供部と、
を備えることを特徴とする。
【００１２】
上記目的を達成するため、本発明の第４の観点に係る認証方法は、
ユーザにサービスを提供するサービス提供サーバから、当該ユーザを認証する旨の認証要求と、当該ユーザを認証するための認証用データとを受信する認証要求受信ステップと、
前記認証要求受信ステップが当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定ステップと、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信ステップと、
前記認証要求受信ステップが当該認証要求を受信した場合、当該認証用データと当該ユーザを認証するための予めメモリに記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証ステップと、
前記認証ステップによる認証結果を前記サービス提供サーバに送信する認証結果送信ステップと、
を備えることを特徴とする。
【００１３】
上記目的を達成するため、本発明の第５の観点に係るサービス提供方法は、
複数の処理を開始する旨の開始要求と、ユーザを認証するための認証用データとを、当該ユーザが使用するユーザ端末から受信する開始要求受信ステップと、
前記受信した開始要求が示す複数の処理の中に、認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信ステップと、
前記認証サーバが当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる推定時間を、前記認証サーバから受信する推定時間受信ステップと、
当該ユーザの認証結果を前記認証サーバから受信する認証結果受信ステップと、

前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから当該認証結果を受信するまで、当該複数の処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該ユーザの認証に成功した旨の当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供ステップと、
を備えることを特徴とする。

【００１４】

上記目的を達成するため、本発明の第６の観点に係るプログラムは、コンピュータを、
ユーザを認証するためのユーザ情報を予め記憶するユーザ情報記憶部、
当該ユーザにサービスを提供するサービス提供サーバから、当該ユーザを認証する旨の認証要求と、当該ユーザを認証するための認証用データとを受信する認証要求受信部、
前記認証要求受信部が当該認証要求を受信した場合、当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる時間を推定する推定部、
前記推定された推定時間を前記サービス提供サーバに送信する推定時間送信部、
前記認証要求受信部が当該認証要求を受信した場合、当該認証用データと前記ユーザ情報記憶部に記憶されたユーザ情報とに基づいて、当該ユーザを認証する認証部、
前記認証部による認証結果を前記サービス提供サーバに送信する認証結果送信部、
として機能させることを特徴とする。

【００１５】

上記目的を達成するため、本発明の第７の観点に係るプログラムは、コンピュータを、ユーザにサービスを提供するための複数の処理のそれぞれについて、当該ユーザを認証する認証サーバによる当該ユーザの認証が必要か否かを示す情報を記憶する認証要否情報記憶部、
当該複数の処理を開始する旨の開始要求と、当該ユーザを認証するための認証用データとを、当該ユーザが使用するユーザ端末から受信する開始要求受信部、
前記受信した開始要求が示す複数の処理の中に、前記認証サーバによる当該ユーザの認証が必要な処理が含まれている場合、前記認証サーバに当該ユーザの認証を要求する旨の認証要求と、前記受信した認証用データと、を前記認証サーバに送信する認証要求送信部、
前記認証サーバが当該認証要求を受信してから当該ユーザの認証を終了するまでにかかる推定時間を、前記認証サーバから受信する推定時間受信部、
当該ユーザの認証結果を前記認証サーバから受信する認証結果受信部、
前記推定時間受信部が当該推定時間を受信した場合、
（ａ）当該開始要求を受信してから当該認証結果を受信するまで、当該複数の処理のうち前記認証サーバによる当該ユーザの認証が必要でない処理を優先して実行し、
（ｂ）当該認証結果を受信した後、前記認証サーバによる当該ユーザの認証が必要な処理を実行する、
ことによって、当該ユーザに当該サービスを提供するサービス提供部、
として機能させることを特徴とする。

【発明の効果】

【００１６】

本発明によれば、行うべき処理群の中に多くの時間を要する処理がある場合にも処理群全体を効率よく実行することができる。

【発明を実施するための最良の形態】

【００１７】

（実施形態）

本発明の実施形態を説明する。本実施形態では、情報処理システム１００として、インターネットを介した銀行のオンラインシステム（いわゆるインターネットバンキングシステム）を例にとって本発明を説明する。すなわち、サービス提供サーバ１２０は、インタ

ーネットバンキングサービスをユーザに提供する処理を実行するサーバである。ただし、本発明はインターネットバンキングサービスに限られず任意のサービスを提供するシステムに適用可能である。

【００１８】

図１は、本実施形態に係る情報処理システム１００の構成を示す図である。情報処理システム１００は、ユーザが操作する１つ以上のユーザ端末１１０（本図では１１０－１、１１０－２、１１０－ｉ等と記載）と、ユーザにサービスを提供する１つ以上のサービス提供サーバ１２０（本図では１２０－１、１２０－２、１２０－ｊ等と記載）と、ユーザを認証する認証サーバ１３０と、を備える。

【００１９】

サービス提供サーバ１２０は、ユーザに所定のサービスを提供する機関が設置したサーバである。例えばサービス提供サーバ１２０には、銀行が設置するインターネットバンキングサービス用のサーバ、行政機関が設置する行政サービス用のサーバ、病院など医療機関が設置する医療サービス用のサーバなど、様々なサーバがある。

【００２０】

認証サーバ１３０は、各サービス提供サーバ１２０が提供するサービスにおいて、ユーザが確かに本人であることを確認する処理（以下「ユーザ認証処理」という。）が必要な処理がある場合に、ユーザ認証処理を各サービス提供サーバ１２０に代わって実行することが可能である。そのため、認証サーバ１３０は、本人確認代行サーバと呼ばれることもある。認証サーバ１３０は、サービス提供サーバ１２０から認証要求を受信し、ユーザ認証処理を行い、認証要求があったサービス提供サーバ１２０に認証結果を送信する。

【００２１】

ユーザ端末１１０とサービス提供サーバ１２０は、インターネット、ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等の通信ネットワーク１４０で接続される。サービス提供サーバ１２０と認証サーバ１３０は、専用回線等の通信ネットワーク１５０で接続される。通信ネットワーク１５０として通信ネットワーク１４０と同様にインターネット、ＬＡＮ、ＷＡＮ等を用いることも可能である。

【００２２】

次に、ユーザ端末１１０、サービス提供サーバ１２０、認証サーバ１３０の各構成の詳細について、図２等を用いて説明する。

【００２３】

まず、ユーザ端末１１０の構成について説明する。ユーザ端末１１０は、記憶部１１１、入力受付部１１２、通信部１１３、出力部１１４、インタフェイス１１５、制御部１１６を備える。

【００２４】

記憶部１１１は、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Accsess Memory）、ハードディスク装置などから構成される。記憶部１１１には、インターネットバンキングシステムのユーザ端末１１０側の処理を実行するためのプログラムやオペレーティングシステム（ＯＳ）等が予め記憶される。また、各処理を実行する際の中間データや結果データ等も記憶する。

【００２５】

入力受付部１１２は、キーボードやマウス等の入力装置から構成され、ユーザからの様々な指示入力を受け付ける。指示入力には、例えば、新規口座の開設を依頼する指示入力、振り込みを依頼する指示入力などがある。

【００２６】

通信部１１３は、インターネットやＬＡＮ等の通信ネットワーク１４０に接続するためのＮＩＣ（Network Interface Card）やモデム等を備える。

【００２７】

出力部１１４は、ディスプレイ等の表示装置や、スピーカ等の出力装置から構成される。ユーザは、表示装置に表示される画面を見ながらユーザ端末１１０を操作できる。

【００２８】
インタフェイス１１５は、ＩＣカードリーダー・ライター（以下「ＩＣカードＲ／Ｗ」と呼ぶ）を備える。本実施形態では、ユーザ端末１１０は、ＩＣチップを搭載した運転免許証、健康保険証、社会保障カード、住民基本台帳カード、キャッシュカード、クレジットカード等の各種ＩＣカードに格納された情報を、ＩＣカードＲ／Ｗで読み取ることが可能である。ユーザは、情報処理システム１００のサービスを利用するために、ユーザとパスワードのチェックのほかに、ＩＣカードを用いて本人確認を行なわなければならない場合がある。
【００２９】
制御部１１６は、ＣＰＵ（Central Processing Unit）等から構成される。制御部１１６は、ユーザ端末１１０全体を制御し、各構成要素と接続され、制御信号やデータをやりとりする。例えば制御部１１６は、インターネットバンキングシステムのユーザ端末１１０側の処理を実行するためのプログラムを実行する。
【００３０】
ユーザ端末１１０として、公知のパーソナルコンピュータを用いることができる。
【００３１】
ＩＣカードには、ＣＰＵと、ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）あるいはフラッシュメモリ等の不揮発性メモリと、が内蔵されている。ＩＣカードの不揮発性メモリには、例えば口座番号や秘密鍵などの個人情報が格納されている。ＩＣカードのＣＰＵは、不揮発性メモリに格納された口座番号等の情報からハッシュ値を計算し、この計算されたハッシュ値を秘密鍵で暗号化して得られた暗号文を外部に出力することができる。ＩＣカードのＣＰＵは、任意のハッシュ関数を用いることができる。
【００３２】
次に、サービス提供サーバ１２０の構成について説明する。サービス提供サーバ１２０は、記憶部１２１、制御部１２２、通信部１２３を備える。
【００３３】
記憶部１２１は、ＲＯＭ、ＲＡＭ、ハードディスク装置などから構成される。記憶部１２１には、インターネットバンキングシステムのサービス提供サーバ１２０側の処理を実行するためのプログラムやＯＳ等が予め記憶される。
【００３４】
記憶部１２１は、図３に示すサービス一覧情報１２５を格納する。サービス一覧情報１２５は、処理群ごとに、サービスコードと処理の内容と本人確認の要否とを対応付けた情報である。
【００３５】
ここで、処理群とは、複数の異なる処理をグルーピングした、処理のまとまりのことである。例えば、あるユーザの銀行口座を新規に開設する場合、
・（処理１）ユーザの氏名、住所など、必要情報を記入する処理
・（処理２）口座番号を採番する処理
・（処理３）ユーザに許諾・契約内容を説明する処理
・（処理４）ユーザがカードデザインを選択する処理
・（処理５）申し込みを確定する処理
などといった複数の処理を実行する必要がある。つまり、処理１～５をすべて実行することにより、「新規口座開設」というサービスが完了する。処理１～５をまとめて処理群と呼ぶ。
【００３６】
１つの処理群には少なくとも１つ以上の処理が含まれる。処理群の数、及び、各処理群に含まれる処理の数は任意である。
【００３７】
サービスコードは、各処理に固有のコードであり、典型的には、文字、数字、記号等を用いて表現される。

【００３８】
また、サービスコードは、処理群に含まれる各処理を実行するときの望ましい実行順を示す。例えばサービスコードの特定の桁に数字を用い、数字の小さい順に処理を実行することが望ましい旨の情報を格納することができる。
【００３９】
望ましい実行順とは、処理群に含まれる各処理を実行する際の典型的な順番のことであり、必ずしもこの順に各処理を実行しなければならないというわけではない。
【００４０】
例えば図３において、「新規口座開設」というサービスを提供するには、制御部１２２は、既定の順として、サービスコードＡ１，Ａ２，Ａ３，Ａ４，Ａ５の順に、処理を実行する。しかし、「口座番号の採番（サービスコードＡ２）」の処理に時間が長くかかってしまう場合、あるいは、時間が長くかかってしまうことが推測される場合、制御部１２２は、サービスコードＡ１の処理の終了後、サービスコードＡ２の処理をスキップしてサービスコードＡ３の処理を開始し、サービスコードＡ３の処理が完了した後にサービスコードＡ２の処理を開始してもよい。
【００４１】
あるいは、制御部１２２は、サービスコードＡ１の処理の後、サービスコードＡ２の処理を開始し、サービスコードＡ２の処理が完了する前にサービスコードＡ３の処理を（例えばマルチタスクで）開始してもよい。
【００４２】
本人確認の要否は、各々の処理が、ＩＣカードを用いて本人であることを認証サーバ１３０によって認証する必要がある処理であるか否かを示す情報である。例えば図３の「口座番号の採番（サービスコードＡ２）」の処理を実行するためには、ＩＣカードを用いて認証する必要がある。一方、「必要情報の記入（サービスコードＡ１）」の処理を実行するためには、ＩＣカードを用いて認証していなくてもよい。
【００４３】
つまり、本人確認が必要な処理を制御部１２２が実行する場合には、処理を開始する前、あるいは、処理の開始後であって完了する前に、認証サーバ１３０による認証を行い、正常に本人確認を完了する（ユーザが本人であると認証される）必要がある。
【００４４】
本実施形態では、ユーザから要求されたサービスを提供する際、まず制御部１２２は、要求されたサービスを提供するための処理群の中に、認証サーバ１３０による認証が必要な処理が含まれているか否かを判別する。そして、認証サーバ１３０による認証が必要な処理が含まれている場合、制御部１２２は、ユーザにＩＣカードの提示を要求し、ＩＣカードから認証に必要な情報を読み出し、認証サーバ１３０に認証を要求する。図３のサービスコードＡ２，Ａ５の２つの処理のように、１つの処理群の中に本人確認が必要な処理が複数存在する場合、ユーザが本人であると一度正常に認証されたセッション又はトランザクションにおいては、再び認証サーバ１３０に認証処理を要求しないようにしてもよい。
【００４５】
また、記憶部１２１は、それぞれのユーザについて、ユーザ名とパスワードを対応付けて格納する、簡易認証データベース１２６を記憶する。制御部１２２は、例えば、ユーザによって入力されたパスワードと、予め登録されたパスワードとが一致するか否かを判断することによって、ＩＣカードを用いない簡易的なユーザ認証処理を実行することができる。
【００４６】
制御部１２２は、ＣＰＵ等から構成される。制御部１２２は、サービス提供サーバ１２０全体を制御し、各構成要素と接続され、制御信号やデータをやりとりする。例えば、制御部１２２は、ユーザによって提示されたＩＣカードから読み出した情報をユーザ端末１１０から受け取り、受け取った情報を認証サーバ１３０に送信して、ＩＣカードを用いた

より詳細なユーザ認証を要求する。また例えば、制御部１２２は、認証サーバ１３０から認証結果を受信し、ユーザ端末１１０に通知する。

【００４７】

通信部１２３は、インターネット等の通信ネットワーク１４０に接続するためのＮＩＣと、専用回線等の通信ネットワーク１５０に接続するためのＮＩＣとを備える。制御部１２２は、通信部１２３により通信ネットワーク１４０を介してユーザ端末１１０とデータを送受信することができる。また、制御部１２２は、通信部１２３により通信ネットワーク１５０を介して認証サーバ１３０とデータを送受信することもできる。

【００４８】

次に、認証サーバ１３０の構成について説明する。認証サーバ１３０は、記憶部１３１、制御部１３２、通信部１３３を備える。

【００４９】

記憶部１３１は、ＲＯＭ、ＲＡＭ、ハードディスク装置などから構成される。記憶部１３１には、ユーザ認証処理を実行するためのプログラムやＯＳ等が予め記憶される。

【００５０】

記憶部１３１は、認証データベース１３５を予め格納する。図４に示すように、認証データベース１３５には、カード種別と認証強度とを対応付けた情報が格納される。

【００５１】

カード種別とは、例えば、運転免許証、健康保険証、社会保障カード、住民基本台帳カード、キャッシュカードなどの種別のことである。

【００５２】

認証強度は、いわゆるセキュリティレベルであり、ユーザ認証にあたり、具体的にどのような認証方式により認証するのかを規定する。

【００５３】

本実施形態では、ユーザ認証方式として、「内部」と「外部」を採用している。制御部１３２は、ユーザによって提示されたＩＣカードのカード種別と、要求されたサービス（又は処理群又は処理）に応じて予め決められた認証強度とに基づいて、ユーザ認証方式を選択する。

【００５４】

ここで、「内部」とは、次に述べるステップＡ１～Ａ３の一連の処理によって認証する方式である。

（Ａ１）認証サーバ１３０の制御部１３２は、乱数を生成し、サービス提供サーバ１２０を経由して、生成した乱数をＩＣカードに送信する。ＩＣカードのＣＰＵは、サービス提供サーバ１２０を経由して、乱数を受信する。

（Ａ２）ＩＣカードのＣＰＵは、受信した乱数を秘密鍵で暗号化し、サービス提供サーバ１２０を経由して、得られた暗号文を認証サーバ１３０に送信する。認証サーバ１３０の制御部１３２は、サービス提供サーバ１２０を経由して、暗号文を受信する。

（Ａ３）認証サーバ１３０の制御部１３２は、受信した暗号文を公開鍵を用いて復号し、復号して得られたデータと、上記ステップＡ１で送信した乱数と、を照合する。制御部１３２は、照合の結果、一致すれば認証成功と判断し、一致しなければ認証失敗と判断する。

【００５５】

あるいは、上記の「内部」の認証方式の変形例として、次のステップＢ１～Ｂ４のように認証してもよい。

（Ｂ１）ＩＣカードのＣＰＵは、ＩＣカード内の不揮発性メモリに格納された情報をハッシュ化し、得られたハッシュ値を、秘密鍵を用いて暗号化し、得られた暗号文を出力する。

（Ｂ２）ユーザ端末１１０の制御部１１６は、暗号文をＩＣカードＲ／Ｗで読み取ってサービス提供サーバ１２０に送信する。

（Ｂ３）サービス提供サーバ１２０の制御部１２２は、暗号文を受信して認証サーバ１３

０に送信する。認証サーバ１３０の制御部１３２は、暗号文を受信する。
（Ｂ４）認証サーバ１３０の制御部１３２は、予め記憶部１３１に記憶した公開鍵で、受信した暗号文を復号し、復号して得られるデータと、後述するユーザ情報データベース１３６に格納された情報をハッシュ化して得られたハッシュ値と、を照合する。制御部１３２は、照合の結果、一致すれば認証成功と判断し、一致しなければ認証失敗と判断する。
【００５６】
また、「外部」とは、次に述べるステップＸ１～Ｘ４の一連の処理によって認証する方式である。
（Ｘ１）認証サーバ１３０の制御部１３２は、サービス提供サーバ１２０を経由して、外部認証用の公開鍵をＩＣカードに送信する。ＩＣカードのＣＰＵは、サービス提供サーバ１２０を経由して、公開鍵を受信する。
（Ｘ２）ＩＣカードのＣＰＵは、乱数を生成し、サービス提供サーバ１２０を経由して、生成した乱数を認証サーバ１３０に送信する。認証サーバ１３０の制御部１３２は、サービス提供サーバ１２０を経由して、乱数を受信する。
（Ｘ３）認証サーバ１３０の制御部１３２は、受信した乱数を、予め記憶部１３２に記憶した外部認証用の秘密鍵で暗号化し、サービス提供サーバ１２０を経由して、得られた暗号文をＩＣカードに送信する。ＩＣカードのＣＰＵは、サービス提供サーバ１２０を経由して、暗号文を受信する。
（Ｘ４）ＩＣカードのＣＰＵは、ステップＸ３で受信した暗号文を、ステップＸ１で受信した公開鍵を用いて復号し、復号して得られたデータと、ステップＸ２で送信した乱数と、を照合する。ＩＣカードのＣＰＵは、照合の結果、一致すれば認証成功と判断し、一致しなければ認証失敗と判断する。
【００５７】
あるいは、上記の「外部」の認証方式を応用して、次のステップＹ１～Ｙ４のように認証してもよい。
（Ｙ１）認証サーバ１３０の制御部１３２は、ユーザ情報データベース１３６に格納された情報をハッシュ化し、得られたハッシュ値を記憶部１３１に予め記憶した公開鍵で暗号化し、暗号文をサービス提供サーバ１２０に送信する。
（Ｙ２）サービス提供サーバ１２０の制御部１２２は、暗号文を受信してユーザ端末１１０に送信する。ユーザ端末１１０の制御部１１６は、暗号文を受信する。
（Ｙ３）ユーザ端末１１０の制御部１１６は、暗号文をＩＣカードに送信する。ＩＣカードのＣＰＵは、暗号文を受信する。
（Ｙ４）ＩＣカードのＣＰＵは、予め不揮発性メモリに格納した秘密鍵で、受信した暗号文を復号し、復号して得られるデータと、不揮発性メモリに予め格納された情報をハッシュ化して得られたハッシュ値と、を照合する。照合の結果、一致すればＩＣカードのＣＰＵは認証成功と判断し、一致しなければ認証失敗と判断する。
【００５８】
なお、上記以外の認証方式を採用することも可能である。また、カード種別と認証強度との対応付けを自由に変更することも可能である。
【００５９】
記憶部１３１は、ユーザ情報データベース１３６を更に格納する。ユーザ情報データベース１３６は、図５に示すように、各ユーザについて、ユーザごとに固有のユーザＩＤ、登録済カードＩＤ、氏名、住所等の各項目の情報を対応付けて格納する。
【００６０】
記憶部１３１は、処理時間テーブル１３７を格納する。処理時間テーブル１３７は、カード種別ごとに、１回のユーザ認証処理を開始してから終了するまでにかかる時間（実際にかかった時間）を示す情報である。例えば、制御部１３２は、１回のユーザ認証処理を開始してから終了するまでの経過時間の、所定時間内における平均時間あるいは所定回数分の平均時間を計算して、処理時間テーブル１３７に格納する。処理時間テーブル１３７に格納された時間は、新たにユーザ認証処理を開始する際に、ユーザ認証処理を完了する

までにかかる時間を推定するために用いられる。詳細は後述する。

【００６１】

制御部１３２は、あるユーザＵＳＲ１の認証を要求され、認証方式として「内部」が指定されている場合、ＩＣカードから送信された暗号文をユーザＵＳＲ１の公開鍵で復号して得られたデータと、ユーザ情報データベース１３６に格納された情報のうちＩＣカードがハッシュ値を計算するために用いた項目のデータ（又はＩＣカードに送信した乱数）をハッシュ化して得られたハッシュ値と、を照合して、認証結果をサービス提供サーバ１２０に送信する。なお、制御部１３２は、照合結果をユーザ情報データベース１３６にログとして格納するようにしてもよい。

【００６２】

また、制御部１３２は、あるユーザＵＳＲ１の認証を要求され、認証方式として「外部」が指定されている場合、ユーザ情報データベース１３６に格納された情報のうち所定の項目の情報を公開鍵を用いて暗号文を生成して、サービス提供サーバ１２０に送信する。なお、ＩＣカード側による認証結果をサービス提供サーバ１２０から受信し、照合結果をユーザ情報データベース１３６にログとして格納するようにしてもよい。

【００６３】

制御部１３２は、ＣＰＵ等から構成される。制御部１３２は、認証サーバ１３０全体を制御し、各構成要素と接続され、制御信号やデータをやりとりする。例えば、制御部１３２は、サービス提供サーバ１２０からユーザを認証する旨の要求を受信すると、認証データベース１３５を参照して認証方式を決定し、決定した認証方式でユーザを認証する。

【００６４】

サービス提供サーバ１２０から送信される情報の内容は、例えば、ユーザ端末１１０のＩＣカードＲ／Ｗにより読み取られたカード識別情報などのＩＣカードの情報や、ユーザによりユーザ端末１１０に入力されたユーザ名、パスワード、暗証番号、等である。

【００６５】

通信部１３３は、通信ネットワーク１５０に接続するためのＮＩＣを備える。制御部１３２は、通信部１３３により通信ネットワーク１５０を介してサービス提供サーバ１２０とデータを送受信することができる。

【００６６】

次に、情報処理システム１００にて実行されるサービス提供処理の流れについて、図６乃至図８を用いて説明する。以下の説明では、インターネットバンキングサービスにおいて、情報処理システム１００が「口座新規開設」のサービスを実行する場合を例にとって説明する。サービス提供サーバ１２０はユーザにインターネットバンキングサービスを提供し、認証サーバ１３０はユーザの本人確認を行う処理（ユーザ認証処理）を代行する。

【００６７】

まず、ユーザ端末１１０の制御部１１６は、サービスの提供を開始する指示入力が入力受付部１１２により受け付けられたか否かを判別する。サービスの提供を開始する指示入力を受け付けた場合、制御部１１６は、サービスを開始するようサービス提供サーバ１２０に要求する（ステップＳ６０１）。サービスの提供を開始する指示入力を受け付けていない場合、指示入力があるまで待機する。

【００６８】

サービス提供サーバ１２０の制御部１２２は、要求されたサービスのための処理群に、ユーザ認証処理が必要な処理が含まれているか否か、すなわち要求されたサービスを提供するためにユーザ認証（本人確認）が必要か否かを判別する（ステップＳ６０２）。

【００６９】

例えば、処理群と処理が図３に示す内容であり、「口座新規開設」のサービスが要求された場合、制御部１２２は、サービスコードＡ１乃至Ａ６の処理に対応する本人確認要否を参照する。その結果、処理群にユーザ認証が必要とされている処理（サービスコードＡ２とＡ５の２つ）が含まれているため、ユーザ認証が必要であると判別する。

【００７０】

ユーザ認証が必要でない場合（ステップＳ６０２；ＮＯ）、後述のステップＳ８０１に進む。一方、ユーザ認証が必要である場合（ステップＳ６０２；ＹＥＳ）、制御部１２２は、サービスの提供にあたりユーザ認証が必要である旨をユーザ端末１１０に通知する（ステップＳ６０３）。

【００７１】

ユーザ端末１１０の制御部１１６は、ユーザ認証が必要である旨の通知を受け取ると、ユーザにＩＣカードの提示と、ＰＩＮ（Personal Identification Number)、ユーザ名、パスワード等の入力とを求める（ステップＳ６０４）。例えば、制御部１１６は、ユーザにＩＣカードの提示とＰＩＮ等の入力とを求める画面を表示する。制御部１１６は、ＩＣカードＲ／Ｗを読み取り可能状態に設定する。また、制御部１１６は、ＰＩＮ等の入力を受け付けるユーザインタフェイスを備えた画面を出力部１１４に表示させ、ＰＩＮ等の入力を受け付ける。

【００７２】

制御部１１６は、ＩＣカードＲ／ＷによりＩＣカードからカード識別情報を読み取る。また、制御部１１６は、ＰＩＮ等を取得する（ステップＳ６０５）。制御部１１６は、ユーザがＩＣカードの所有者であるか否かをＰＩＮを用いて認証（ＰＩＮ認証）する。

【００７３】

ここで、カード識別情報とは、カードを一意に識別できる情報（例えば運転免許登録番号やクレジットカード番号など）である。ＩＣカードは、サービス（処理群）が終了するまで、ＩＣカードＲ／Ｗがデータを読み取れるように固定されたままであることが望ましい。

【００７４】

制御部１１６は、取得したカード識別情報、ユーザ名、パスワード等をサービス提供サーバ１２０に送信する（ステップＳ６０６）。制御部１１６は、所定の暗号化アルゴリズムによって暗号化した上で送信することが望ましい。

【００７５】

サービス提供サーバ１２０の制御部１２２は、カード識別情報とＰＩＮ等を受信する（ステップＳ６０７）。制御部１２２は、ステップＳ６０６で用いられた暗号化アルゴリズムに対応する復号アルゴリズムによって復号することができる。

【００７６】

制御部１２２は、受信したユーザ名、パスワード等を用いて、簡易的なユーザ認証を実行する（ステップＳ６０８）。例えば、制御部１２２は、受信したＰＩＮ、ユーザ名、パスワードと、簡易認証データベース１２６に予め格納されているＰＩＮ、ユーザ名、パスワードと、を照合することにより、簡易的なユーザ認証を実行する。照合の結果、一致した場合、簡易認証成功と判断してサービス提供処理を続行する。一致しない場合、簡易認証失敗と判断してサービス提供処理を終了する。

【００７７】

更に、制御部１２２は、ＩＣカードを用いたユーザ認証を実行するよう認証サーバ１３０に要求する（ステップＳ６０９）。制御部１２２は、受信したカード識別情報を認証サーバ１３０に送信する。

【００７８】

認証サーバ１３０の制御部１３２は、受信したカード識別情報が、ユーザ情報データベース１３６の登録済みカードＩＤに、登録済みとして記録されているか否かを確認する。登録済みでない場合、制御部１３２は、受信したカード識別情報を登録済みとしてユーザ情報データベース１３６に格納する。

【００７９】

制御部１３２は、ユーザ認証にかかる時間を推定する（ステップＳ６１０）。

【００８０】

具体的には、制御部１３３は、図９に示すような処理時間テーブル１３７を参照し、受信したカード識別情報に対応するカード種別の平均処理時間を取得する。制御部１３２は

、取得した平均処理時間と、ユーザ認証処理を実行するための待ち行列（キュー）に現在登録されているジョブ数との積を、要求されたユーザ認証にかかる時間として推定する。つまり、計算される推定時間は、待ち行列に登録してから、要求されたユーザ認証処理の順番が回ってきてそのユーザ認証処理を終了するまで、にかかると推定される時間である。

【００８１】

待ち行列には、例えば図１０に示すようなデータが格納される。番号は、待ち行列に登録された順を表す。受付時刻は、待ち行列に登録された時刻である。

【００８２】

図１０では、待ち行列を１つだけにしているが、カード種別ごとに待ち行列を定義してもよい。例えば、運転免許証を用いたユーザ認証処理用の待ち行列と、住民基本台帳カードを用いたユーザ認証処理用の待ち行列と、を別々に用意し、運転免許証を用いたユーザ認証処理と、住民基本台帳カードを用いたユーザ認証処理とを平行して実行できるようにしてもよい。

【００８３】

制御部１３２は、ユーザ認証処理にかかる推定時間をサービス提供サーバ１２０に送信する。また、制御部１３２は、要求されたユーザ認証を、ユーザ認証処理を実行するための待ち行列に登録する（ステップＳ６１１）。待ち行列は、ＦＩＦＯ（ First In First Out）のリスト構造で保持される。

【００８４】

待ち行列に登録された（キューイングされた）ユーザ認証要求は、処理順が回ってくると直ちに実行される。完了したユーザ認証に対応するジョブは待ち行列から削除される。したがって、待ち行列に登録されているデータ数が少なければ、要求されたユーザのユーザ認証処理はすぐに開始されるし、待ち行列に登録されているデータ数が多ければ、要求を受け取ってから実際に開始するまでに比較的長いタイムラグが発生することもある。

【００８５】

サービス提供サーバ１２０の制御部１２２は、ユーザ認証処理にかかる推定時間を受信する。制御部１２２は、要求されたサービスに対応する処理群の中から、ユーザ認証処理を終了していなくても実行可能な処理を選択して優先的に実行する（ステップＳ６１２）。つまり、制御部１２２は、サービス一覧情報１２５を参照し、本人確認要否が必要ないとされている処理を選択する。例えば図３において、制御部１２２は、新規口座開設の処理群の中から、サービスコードＡ１，Ａ３，Ａ４の３つの処理を選択して実行する。

【００８６】

このとき、制御部１２２は、選択した処理を、既定順になるべく近い順に実行することが望ましい。例えば、選択された処理が、サービスコードＡ１，Ａ３，Ａ４の３つの処理なのであれば、既定順（Ａ１，Ａ２，Ａ３，Ａ４，Ａ５の順）に最も近い順である、Ａ１，Ａ３，Ａ４の順に、各処理を実行する。ただし、制御部１２２は、任意の順番で各処理を実行してもよい。

【００８７】

また、制御部１２２は、推定時間が所定値未満であれば、既定順通りに処理群を実行し、所定値以上であれば、ユーザ認証処理を終了していなくても実行可能な処理を選択して優先的に実行するようにしてもよい。

【００８８】

また、制御部１２２は、推定時間が所定値以上である場合、所定の待機時間が経過してから再びユーザ認証処理を要求し直すようにサービス提供処理に通知するようにしてもよい。この通知を受けたサービス提供処理は、ユーザ認証処理用に認証サーバ１３０との間に開いたポートが占有され続けることなく、早期にポートを開放できるので、サービス提供サーバ１２０への負荷を低減することができる。

【００８９】

後述するように、認証サーバ１３０による認証結果は、記憶部１３１の所定記憶領域に

格納される。そこで、推定時間が所定値以上である場合、制御部１２２は、ユーザ認証処理を要求して認証結果を取得する第１のセッションを終了し、推定時間が経過した後、認証結果を認証サーバ１３０に問い合わせて取得する第２のセッションを開始し、認証結果を取得するようにしてもよい。なお、第１のセッションが終了した場合にも、認証サーバ１３０の制御部１３２は、当該ユーザ認証処理のジョブを待ち行列から削除せず、当該ユーザ認証処理を終了してから削除するものとする。

【００９０】

ユーザ端末１１０の制御部１１６は、サービス提供サーバ１２０の制御部１２２が実行している（サービス提供サーバ１２０側の）処理に対応する、ユーザ端末１１０側の処理を実行する（ステップＳ６１３）。

【００９１】

例えば図３では、「必要情報の記入（サービスコードＡ１）」は、本人確認が必要ない処理とされている。そこで、サービス提供サーバ１２０の制御部１２２は、サービスコードＡ１の処理を開始する。ユーザ端末１１０の制御部１１６は、ＩＣカードから氏名、住所などの情報を読み取り、所定の暗号化アルゴリズムで暗号化した後、サービス提供サーバ１２０に送信する。サービス提供サーバ１２０の制御部１２２は、新規口座開設に必要な情報であってＩＣカードから取得可能な情報を収集する。

【００９２】

ところで、認証サーバ１３０ではユーザ認証処理がキューイングされており、処理順が回ってくると、ステップＳ６１２乃至Ｓ６１３と平行して、ユーザ認証処理が開始される。上述のように、認証方式には２種類あるが、ここでは認証方式として「内部」を選択した場合を例にとって説明する。

【００９３】

制御部１３２は、ユーザ認証処理を開始し（図７；ステップＳ７０１）、サービス提供サーバ１２０に通知する。

【００９４】

サービス提供サーバ１２０の制御部１２２は、カード情報の読み取りをユーザ端末１１０に要求する（ステップＳ７０２）。

【００９５】

ユーザ端末１１０の制御部１１６は、ＩＣカードＲ／Ｗを用いて、ＩＣカードのＣＰＵが生成した暗号文を読み取る（ステップＳ７０３）。

【００９６】

制御部１１６は、読み取った暗号文をサービス提供サーバ１２０に送信する。サービス提供サーバ１２０は、受信した暗号文を認証サーバ１３０に送信する（ステップＳ７０４）。

【００９７】

なお、認証サーバ１３０の制御部１３２は、ステップＳ７０３において、カード識別情報を合わせて取得するようにし、ステップＳ６０５で取得したカード識別情報と一致するか否かをチェックすることとする。一致すれば、ステップＳ７０５に進み、一致しなければ、新たにカード識別情報を登録済みカードＩＤに登録した後ステップＳ７０５に進む。

【００９８】

制御部１３２は、受信した暗号文を所定の復号アルゴリズムで復号し、復号されて得られたデータと、ユーザ情報データベース１３６に格納された情報から生成したハッシュ値（又は送信した乱数）と、を照合する（ステップＳ７０５）。制御部１３２は、両者が一致する場合には認証成功と判断し、一致しない場合には認証失敗と判断する。

【００９９】

制御部１３２は、認証結果を記憶部１３１の所定記憶領域（例えばユーザ情報データベース１３６等）に格納する。

【０１００】

制御部１３２は、ステップＳ７０５における認証結果をサービス提供サーバ１２０に送

信する。また、制御部１３２は、ユーザ認証処理にかかった時間を記憶部１３１にログ情報として記録する（ステップＳ７０６）。制御部１３２は、ユーザ認証処理にかかった時間を用いて、処理時間テーブル１３７を更新する。例えば、制御部１３２は、平均処理時間を再計算し、処理時間テーブル１３７に格納する。

【０１０１】

サービス提供サーバ１２０の制御部１２２は、認証サーバ１３０から認証結果を受信する（ステップＳ７０７）。

【０１０２】

なお、上述のように、サービス提供サーバ１２０の制御部１２２は、ステップＳ６１２で推定時間を受信した時刻から、推定時間が経過した後、認証結果を送信するよう認証サーバ１３０に要求してもよい。そして、認証サーバ１３０の制御部１３２は、当該要求を受信すると、記憶部１３１の所定記憶領域に格納した認証結果をサービス提供サーバ１２０に送信し、サービス提供サーバ１２０の制御部１２２は、認証サーバ１３０から認証結果を受信するようにしてもよい。

【０１０３】

認証失敗の場合（ステップＳ７０８；ＮＯ）、制御部１２２は、認証に失敗した旨をユーザ端末１１０に通知して、サービス提供処理を終了する。制御部１２２は、実行していた処理群をロールバックする。ユーザ端末１１０の制御部１１６は、サービスの提供を続行できない旨をユーザに通知する。

【０１０４】

あるいは、ステップＳ７０１に戻り、ユーザ認証処理を所定回数だけリトライする。待ち行列に登録し直してユーザ認証処理をリトライしてもよい。

【０１０５】

認証成功の場合（ステップＳ７０８；ＹＥＳ）、制御部１２２は、認証に成功した旨をユーザ端末１１０に通知する。また、制御部１２２は、ステップＳ６１２で選択しなかった処理、すなわち、ユーザ認証処理でユーザ認証に成功しなければ実行できないと定められている処理を実行する（ステップＳ７０９）。

【０１０６】

このとき、制御部１２２は、既定順になるべく近い順に処理を実行することが望ましい。例えば、ステップＳ６１２で選択された処理がサービスコードＡ１，Ａ３，Ａ４の３つであり、この順に処理群を進行中であり、認証に成功した旨が通知されたときサービスコードＡ３の処理を実行中であるならば、サービスコードＡ３の処理の終了後、サービスコードＡ４の処理ではなく、サービスコードＡ２の処理を先に実行する。すなわち、制御部１２２は、結果的に、Ａ１，Ａ３，Ａ２，Ａ４，Ａ５の順に処理を実行する。ただし、制御部１２２は、任意の順番で各処理を実行してもよい。

【０１０７】

ユーザ端末１１０の制御部１１６は、サービス提供サーバ１２０の制御部１２２が実行している（サービス提供サーバ１２０側の）処理に対応する、ユーザ端末１１０側の処理を実行する（ステップＳ７１０）。

【０１０８】

サービス提供サーバ１２０の制御部１２２は、ユーザに要求されたサービスに対応する処理群に含まれるすべての処理を終了したか否かを判別する（ステップＳ７１１）。

【０１０９】

まだ終了していない処理が残っている場合（ステップＳ７１１；ＮＯ）、制御部１２２は処理を続行する。すべての処理を終了した場合（ステップＳ７１１；ＹＥＳ）、サービスの提供を終了する。

【０１１０】

以上のように、情報処理システム１００は、ユーザ認証処理にかかる時間を推定し、ユーザ認証処理が終わっていなくても提供可能な処理を優先的に実行することにより、処理群全体を効率よく実行できるようになる。例えば、ユーザ認証処理に比較的長い時間を要

してしまう時間帯（アクセスが集中して混み合っている時間帯）では、ユーザ認証処理が必要ない処理を先に進め、一方でユーザ認証処理をバックグラウンドで平行して行い、本人確認ができた後に残りの処理を行えるようにする。また、ユーザ認証処理をすぐに終えることができる時間帯（アクセスが少なく空いている時間帯）では、既定順通りに処理を進める。どちらにしても、ユーザは結果的に行うべき手続きを効率の良い順番で行うことができるので、ユーザーフレンドリーなシステム設計が可能になる。また、ユーザの立場から見れば、ユーザ認証処理に時間がかかっていることが容易には分からず粛々と手続きが進んでいるように見えるので、ストレスを感じさせないという効果がある。

【０１１１】

本実施形態では、情報処理システム１００が提供するサービスとしてインターネットバンキングサービスを想定した。しかし、他のサービスを提供するシステムにも応用可能である。例えば、行政機関が行う行政サービスにおいて、住民票発行などの処理の際に本人確認を行うケースや、病院など医療機関が行う医療サービスにおいて、診療受付の際に本人確認を行うケースなど、様々な分野で本発明を利用できる。

【０１１２】

本実施形態では、インターネットバンキングサービスにおけるユーザ認証処理を、サービス提供サーバ１２０とは異なる認証サーバ１３０が実行するものとして説明した。すなわち、情報処理システム１００全体のうち、多くの時間を要する可能性のある処理（ボトルネックとなる可能性のある処理）として、ユーザ認証処理を想定した。しかし、認証サーバ１３０を、他の任意の処理を実行する運用サーバに置き換えた実施形態を採用することもできる。

【０１１３】

例えば、獲得ポイントを決済に利用できるインターネット上のショッピングサイトにおいて、情報処理システム１００は、ユーザが商品を購入できるサービスを提供する。ユーザの獲得ポイントや購買履歴等を取得してユーザ端末１１０のモニターに表示する処理が、比較的多くの時間を要する可能性のある処理であると仮定する。このとき、上述の説明において、認証サーバ１３０を、ユーザの獲得ポイントや購買履歴等を管理する運用サーバに置き換えた実施形態を採用して、本発明を適用することが可能である。

【０１１４】

つまり、アクセスが少なく空いている時間帯では、既定の処理順として、（処理Ａ）現在の獲得ポイント数を取得して表示する処理、（処理Ｂ）商品を選択する処理、（処理Ｃ）発送方法を指定する処理、（処理Ｄ）決済方法を指定する処理、（処理Ｅ）注文の確定処理、を順に実行する。

【０１１５】

一方、アクセスが集中して混み合っている時間帯であって処理Ａが重い場合、サービス提供サーバ１２０は、処理Ｂ，Ｃを優先的に実行し、処理Ａのうち現在の獲得ポイント数を取得する処理部分を運用サーバがバックグラウンドで実行する。獲得ポイントの取得後、サービス提供サーバ１２０は、処理Ａ，処理Ｄ，処理Ｅを実行する。

【０１１６】

このように、本発明は、行うべき処理群の中に多くの時間を要する可能性のある処理がある場合に、処理群全体を効率よく実行できるようにするために利用することができる。

【０１１７】

本発明は、上述した実施形態に限定されず、種々の変形及び応用が可能である。

【０１１８】

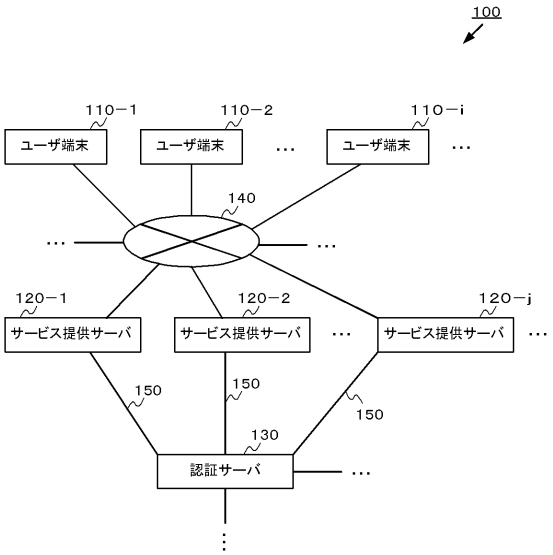
以上説明したように、本発明によれば、行うべき処理群の中に多くの時間を要する処理がある場合にも処理群全体を効率よく実行するために好適な情報処理システム、認証サーバ、サービス提供サーバ、認証方法、サービス提供方法、及び、プログラムを提供することができる。

【図面の簡単な説明】

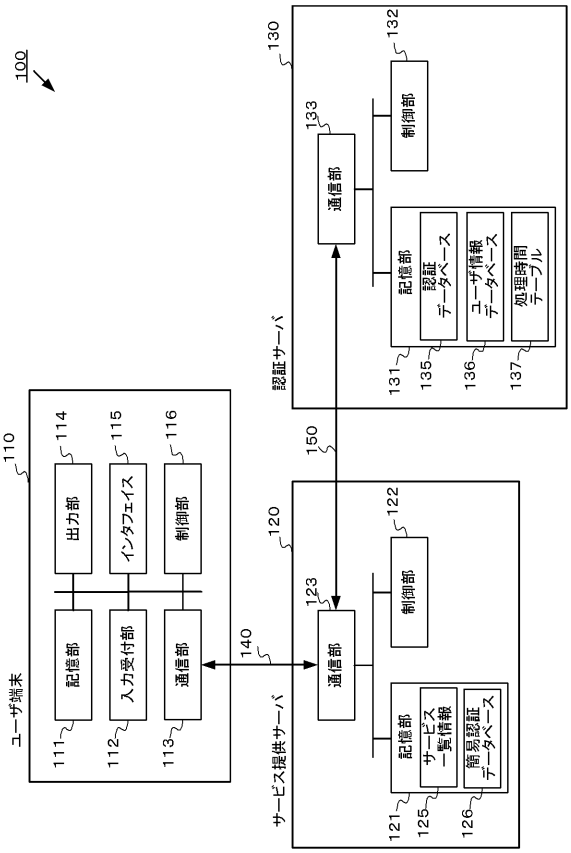
【０１１９】

【図１】情報処理システムの構成を説明するための図である。
【図２】ユーザ端末、サービス提供サーバ、認証サーバの各構成を説明するための図である。
【図３】サービス一覧情報に格納されるデータの構成例である。
【図４】認証データベースに格納されるデータの構成例である。
【図５】ユーザ情報データベースに格納されるデータの構成例である。
【図６】サービス提供処理の流れを説明するための図である。
【図７】サービス提供処理の流れを説明するための図（続き）である。
【図８】サービス提供処理の流れを説明するための図（続き）である。
【図９】処理時間テーブルに格納されるデータの構成例である。
【図１０】待ち行列に格納されるデータの構成例である。
【符号の説明】
【０１２０】
１００　情報処理システム
１１０　ユーザ端末
１１１　記憶部
１１２　入力受付部
１１３　通信部
１１４　出力部
１１５　インタフェイス
１１６　制御部
１２０　サービス提供サーバ
１２１　記憶部
１２２　制御部
１２３　通信部
１２５　サービス一覧情報
１２６　簡易認証データベース
１３０　認証サーバ
１３１　記憶部
１３２　制御部
１３３　通信部
１３５　認証データベース
１３６　ユーザ情報データベース
１３７　処理時間テーブル
１４０，１５０　通信ネットワーク

【図１】



【図２】

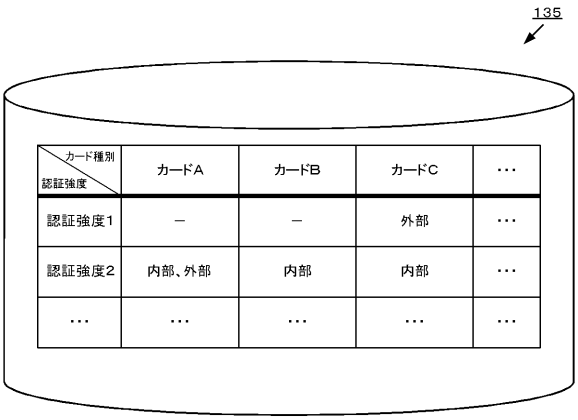


【図３】

125

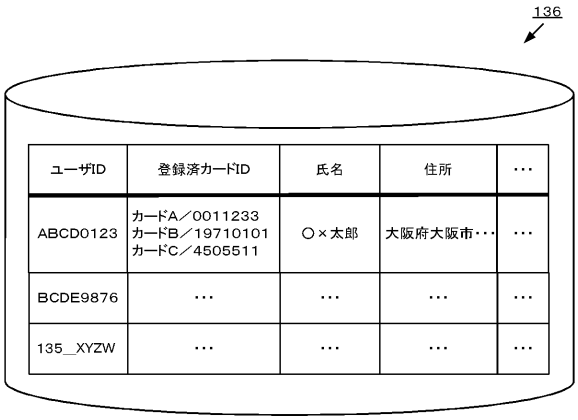
処理群の名称	サービスコード	処理の内容	本人確認要否
A. 新規口座開設	A1	必要情報の記入	否
	A2	口座番号の採番	要
	A3	許諾・契約内容の説明	否
	A4	カードデザインの選択	否
	A5	申し込みの確定	要
B. 残高照会	B1	残高照会	否
C. 振り込み	C1	登録済み振込先の読み出し	要
	C2	金額の指定	否
	C3	振込元の情報の入力	否
	C4	振り込みの実行	要
…	…	…	…

【図４】

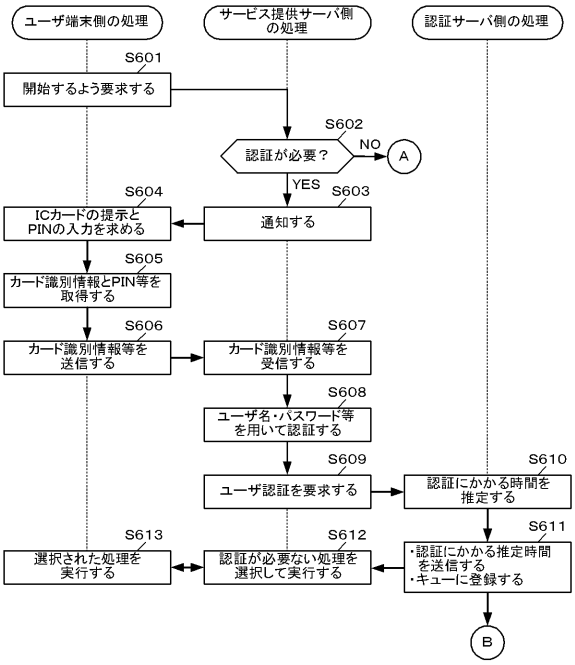


認証強度＼カード種別	カードA	カードB	カードC	…
認証強度1	−	−	外部	…
認証強度2	内部、外部	内部	内部	…
…	…	…	…	…

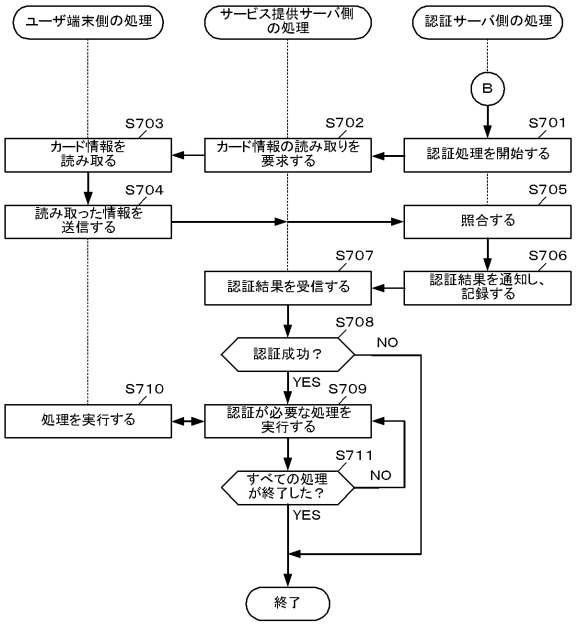
【図５】



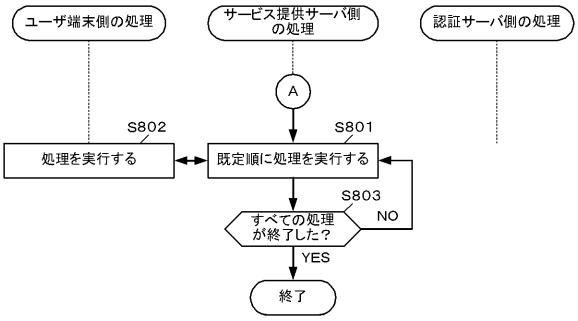
【図６】



【図７】



【図８】



【図９】

137

カード種別	平均処理時間（秒）
IC運転免許証	3．5
住民基本台帳カード	2．1
在留外国人カード	4．2

【図１０】

順番	カード識別番号	カード種別	受付時刻
1	xxxxxxxxxxxxx	IC運転免許証	yyyymmdd hh:mm:ss:xx
2	yyyyyyyyyyyyy	住民基本台帳カード	yyyymmdd hh:mm:ss:xx
3	zzzzzzzzzzzzz	IC運転免許証	yyyymmdd hh:mm:ss:xx
…	…	…	…

フロントページの続き

審査官　平井　誠

(56)参考文献　特開２００５－０９２６７１（ＪＰ，Ａ）
特開２０００－１０５８４９（ＪＰ，Ａ）
再公表特許第２００４／０９２９６７（ＪＰ，Ａ１）
特開２００２－２９７９００（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｋ　１７／００
Ｈ０４Ｌ　９／３２