(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2010-9530
(P2010-9530A)
(43)公開日　平成22年1月14日(2010.1.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B285
H04L 9/32	(2006.01)	H04L	9/00	675D	5J104

審査請求 未請求　請求項の数 32　ＯＬ　（全 34 頁）

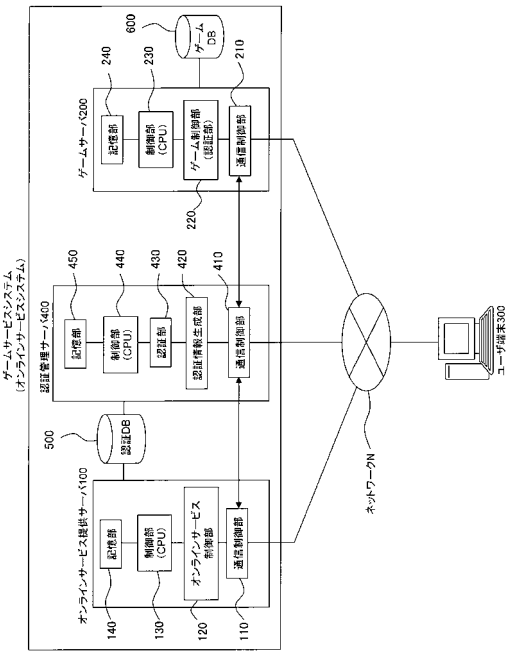
(21)出願番号　特願2008-171336 (P2008-171336)
(22)出願日　平成20年6月30日 (2008.6.30)

(71)出願人　505205812
エヌエイチエヌ　コーポレーション
大韓民国　キュンギード・４６３－８４４・ソンナム－シ・ブンダン－グ・ジョンジャードン・２５－１・ブンダン・ベンチャー・タウン
(71)出願人　501333021
ＮＨＮＪａｐａｎ株式会社
東京都品川区大崎二丁目１番１号
(74)代理人　100087398
弁理士　水野　勝文
(74)代理人　100067541
弁理士　岸田　正行
(74)代理人　100103506
弁理士　高野　弘晋

最終頁に続く

(54)【発明の名称】サービス提供方法及びオンラインサービスシステム

(57)【要約】
【課題】正当なユーザ以外のオンラインサービス利用を抑制し、正当なユーザが安全にオンラインサービスを利用することができるサービス提供方法及びオンラインサービスシステムを提供する。
【解決手段】本発明のオンラインサービスシステムのサービス提供方法は、オンラインサービス提供サーバでのユーザログイン情報に基づいて第１認証情報をユーザ端末に発行し保存するステップと、発行された第１認証情報を含む認証要求を認証管理サーバに送信するステップと、認証管理サーバが第１認証情報を用いて認証処理を遂行し、認証結果に基づいて第２認証情報をユーザ端末に発行し保存するステップと、ユーザ端末が第２認証情報を含むサービス接続要求をサービスサーバに送信するステップと、サービスサーバが第２認証情報を用いて認証管理サーバを通じた認証処理を遂行し、認証結果に基づいてユーザ端末へのオンラインサービスの提供を開始するステップとを含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
オンラインサービスを利用するためにユーザ端末が接続可能なオンラインサービス提供サーバと、前記オンラインサービスにおけるユーザの認証管理を行う認証管理サーバと、前記オンラインサービスを提供するサービスサーバとを備えるオンラインサービスシステムのサービス提供方法であって、
前記認証管理サーバが、前記オンラインサービス提供サーバでのユーザログイン情報に基づいて第１認証情報を前記ユーザ端末に発行し、保存する第１ステップと、
前記ユーザ端末が、発行された前記第１認証情報を含む認証要求を前記認証管理サーバに送信する第２ステップと、
前記認証管理サーバが、前記第１認証情報を用いて認証処理を遂行し、認証結果に基づいて第２認証情報を前記ユーザ端末に発行し、保存する第３ステップと、
前記ユーザ端末が、前記第２認証情報を含むサービス接続要求を前記サービスサーバに送信する第４ステップと、
前記サービスサーバが、前記第２認証情報を用いて前記認証管理サーバを通じた認証処理を遂行し、認証結果に基づいて前記ユーザ端末への前記オンラインサービスの提供を開始する第５ステップと、
を含むことを特徴とするサービス提供方法。
【請求項２】
前記第２認証情報は、認証有効期限情報を含み、
前記ユーザ端末が、前記認証有効期限情報と現在時間情報とに基づいて認証有効期限に対して所定の時間経過したか否かを判別し、前記所定の時間が経過したと判別された場合に、前記認証管理サーバに前記認証有効期限情報の更新要求を送信するステップと、
前記認証管理サーバが、前記更新要求に応答して前記第２認証情報の認証有効期限情報を更新するステップと、
を含むことを特徴とする請求項１に記載のサービス提供方法。
【請求項３】
前記認証要求及び前記サービス接続要求は、前記ユーザ端末の装置固有の識別情報を含んで構成され、
前記第３ステップは、発行された前記第２認証情報と前記認証要求に含まれる前記識別情報とを関連付けて保存し、
前記第５ステップは、前記識別情報及び前記第２認証情報を用いて前記認証管理サーバを通じた認証処理を遂行することを特徴とする請求項１又は２に記載のサービス提供方法。
【請求項４】
前記第５ステップは、
前記サービスサーバが、前記サービス接続要求に応答して前記第２認証情報を含む認証要求を前記認証管理サーバに送信するステップと、
前記認証管理サーバが、前記サービスサーバからの前記認証要求に基づく前記第２認証情報を用いた認証処理を遂行し、前記認証処理の認証結果を前記サービスサーバに送信するステップと、
前記サービスサーバが、前記認証管理サーバから受信した認証結果に基づいて前記ユーザ端末への前記オンラインサービスの提供を開始するステップと、
を含むことを特徴とする請求項１から３のいずれか１つに記載のサービス提供方法。
【請求項５】
前記第２認証情報を用いた認証処理を遂行し、認証結果を前記サービスサーバに送信するステップは、
前記認証結果が認証成功である場合に、前記第２認証情報に関連する第３認証情報を発行し、保存するステップと、
前記認証結果及び第３認証情報を前記サービスサーバに送信するステップと、を含み、

前記サービスサーバが前記オンラインサービスの提供を開始するステップは、
前記第３認証情報を前記ユーザ端末に送信するステップと、を含むことを特徴とする請求項４に記載のサービス提供方法。
【請求項６】
前記第３認証情報は、前記第２認証情報に含まれる認証有効期限情報及び発行シーケンス番号が異なる認証情報であることを特徴とする請求項５に記載のサービス提供方法。
【請求項７】
ブラウザを介してユーザ端末がオンラインサービスを利用するために接続するオンラインサービス提供サーバと、前記オンラインサービスにおけるユーザの認証管理を行う認証管理サーバと、前記ユーザ端末に設置された前記オンラインサービスを利用するためのサービスアプリケーションを通じて前記オンラインサービスを提供するサービスサーバと、を備えるオンラインサービスシステムのサービス提供方法であって、
前記認証管理サーバが、前記ブラウザを通じたサービス利用要求に応答し、前記オンラインサービス提供サーバでのユーザログイン情報に基づいて第１認証情報を前記ユーザ端末に発行し、保存する第１ステップと、
前記ブラウザが、発行された前記第１認証情報を含む認証要求を前記認証管理サーバに送信する第２ステップと、
前記認証管理サーバが、前記第１認証情報を用いて認証処理を遂行し、認証結果に基づいて第２認証情報を前記ユーザ端末に発行し、保存する第３ステップと、
前記ブラウザが、前記第２認証情報を前記サービスアプリケーションに受け渡す第４ステップと、
前記サービスアプリケーションが前記第２認証情報を含むサービス接続要求を前記サービスサーバに送信する第５ステップと、
前記サービスサーバが、前記第２認証情報を用いて前記認証管理サーバを通じた認証処理を遂行し、認証結果に基づいて前記サービスアプリケーションを通じた前記オンラインサービスの提供を開始する第６ステップと、
を含むことを特徴とするサービス提供方法。
【請求項８】
前記第２認証情報は、認証有効期限情報を含み、
前記サービスアプリケーションが、前記認証有効期限情報と現在時間情報とに基づいて認証有効期限に対して所定の時間経過したか否かを判別し、前記所定の時間が経過したと判別された場合に、前記認証管理サーバに前記認証有効期限情報の更新要求を送信するステップと、
前記認証管理サーバが、前記更新要求に応答して前記第２認証情報の認証有効期限情報を更新するステップと、
を含むことを特徴とする請求項７に記載のサービス提供方法。
【請求項９】
前記第２認証情報は、認証有効期限情報を含むとともに、前記ユーザ端末は、前記サービスアプリケーションの起動に必要な情報を所定のサーバから取得するための情報取得部を有し、
前記第４ステップは、
前記ブラウザが、発行された前記第２認証情報を前記情報取得部に受け渡すステップと、
前記情報取得部が、前記認証有効期限情報と現在時間情報とに基づいて認証有効期限に対して所定の時間経過したか否かを判別し、前記所定の時間が経過したと判別された場合に、前記認証管理サーバに前記認証有効期限情報の更新要求を送信するステップと、
前記認証管理サーバが、前記更新要求に応答して前記第２認証情報の認証有効期限情報を更新し、更新された認証期限情報を含む第２認証情報を前記情報取得部に提供するステップと、
前記情報取得部が、更新された認証期限情報を含む第２認証情報を、前記サービスアプ

リケーションに受け渡すステップと、
を含むことを特徴とする請求項７に記載のサービス提供方法。
【請求項１０】
前記認証要求及び前記サービス接続要求は、前記ユーザ端末の装置固有の識別情報を含んで構成され、
前記第３ステップは、発行された前記第２認証情報と前記認証要求に含まれる前記識別情報とを関連付けて保存し、
前記第６ステップは、前記識別情報及び前記第２認証情報を用いて前記認証管理サーバを通じた認証処理を遂行することを特徴とする請求項７から９のいずれか１つに記載のサービス提供方法。
【請求項１１】
前記第６ステップは、
前記サービスサーバが、前記サービス接続要求に応答して前記第２認証情報を含む認証要求を前記認証管理サーバに送信するステップと、
前記認証管理サーバが、前記サービスサーバからの前記認証要求に基づく前記第２認証情報を用いた認証処理を遂行し、前記認証処理の認証結果を前記サービスサーバに送信するステップと、
前記サービスサーバが、前記認証管理サーバから受信した前記認証結果に基づいて前記サービスアプリケーションを通じた前記オンラインサービスの提供を開始するステップと、を含むことを特徴とする請求項７から１０のいずれか１つに記載のサービス提供方法。
【請求項１２】
前記第２認証情報を用いた認証処理を遂行し、認証結果を前記サービスサーバに送信するステップは、
前記認証結果が認証成功である場合に、前記第２認証情報に関連する第３認証情報を発行し、保存するステップと、
前記認証結果及び第３認証情報を前記サービスサーバに送信するステップと、を含み、
前記サービスサーバが前記オンラインサービスの提供を開始するステップは、
前記第３認証情報を前記サービスアプリケーションに送信するステップと、を含むことを特徴とする請求項１１に記載のサービス提供方法。
【請求項１３】
前記第３認証情報は、前記第２認証情報に含まれる認証有効期限情報及び発行シーケンス番号が異なる認証情報であることを特徴とする請求項１２に記載のサービス提供方法。
【請求項１４】
ネットワークを通じて接続可能なユーザ端末にオンラインサービスを提供するオンラインサービスシステムであって、
前記ユーザ端末が前記オンラインサービスにログインした後、前記オンラインサービスを利用するための第１認証情報と、前記第１認証情報を用いた認証結果に基づいて前記ユーザ端末に発行される該第１認証情報と異なる第２認証情報と、を生成する認証情報生成部と、
前記ユーザ端末からの前記第１認証情報を含む認証要求に応答して前記第１認証情報を用いた第１認証処理を遂行するとともに、前記ユーザ端末からの前記第２認証情報を含むサービス接続要求に応答し、前記ユーザ端末への前記オンラインサービスの提供を開始するための該第２認証情報を用いた第２認証処理を遂行する認証部と、
前記第２認証処理の認証結果に基づいて、前記オンラインサービスを前記ユーザ端末に提供するオンラインサービス提供部と、
を有することを特徴とするオンラインサービスシステム。
【請求項１５】
前記第２認証情報は、認証有効期限情報を含み、
前記認証情報生成部は、
前記ユーザ端末からの前記認証有効期限情報の更新要求に基づいて、前記第２認証情報

の認証有効期限情報を更新する更新処理を遂行することを特徴とする請求項１４に記載のオンラインサービスシステム。
【請求項１６】
前記認証要求及び前記サービス接続要求は、前記ユーザ端末の装置固有の識別情報を含んで構成され、
前記認証情報生成部は、発行された前記第２認証情報と前記認証要求に含まれる前記識別情報とを関連付けて保存し、
前記認証部は、前記識別情報及び前記第２認証情報を用いて前記第２認証処理を遂行することを特徴とする請求項１４又は１５に記載のオンラインサービスシステム。
【請求項１７】
前記認証情報生成部は、前記第２認証処理の認証結果が認証成功である場合に、前記第２認証情報に関連する第３認証情報を生成することを特徴とする請求項１４から１６のいずれか１つに記載のオンラインサービスシステム。
【請求項１８】
前記第３認証情報は、前記第２認証情報に含まれる認証有効期限情報及び発行シーケンス番号が異なる認証情報であることを特徴とする請求項１７に記載のオンラインサービスシステム。
【請求項１９】
ネットワークを通じて接続可能なユーザ端末にオンラインサービスを提供するオンラインサービスシステムであって、
前記ユーザ端末がブラウザを通じて前記オンラインサービスにログインした後、前記オンラインサービスを利用するための第１認証情報と、前記第１認証情報を用いた認証結果に基づいて発行される該第１認証情報と異なる第２認証情報と、を生成する認証情報生成部と、
前記ブラウザを通じた前記第１認証情報を含む認証要求に応答して前記第１認証情報を用いた第１認証処理を遂行するとともに、前記ユーザ端末に設置される前記オンラインサービスを前記ユーザ端末で利用可能に動作させるサービスアプリケーションからの前記第２認証情報を含むサービス接続要求に応答し、前記ユーザ端末への前記オンラインサービスの提供を開始するための該第２認証情報を用いた第２認証処理を遂行する認証部と、
前記第２認証処理の認証結果に基づいて、前記サービスアプリケーションを通じて前記オンラインサービスを前記ユーザ端末に提供するオンラインサービス提供部と、
を有することを特徴とするオンラインサービスシステム。
【請求項２０】
前記第２認証情報は、認証有効期限情報を含み、
前記認証情報生成部は、
前記サービスアプリケーションからの前記認証有効期限情報の更新要求に基づいて、前記第２認証情報の認証有効期限情報を更新する更新処理を遂行することを特徴とする請求項１９に記載のオンラインサービスシステム。
【請求項２１】
前記第２認証情報は、認証有効期限情報を含むとともに、前記ユーザ端末は、前記サービスアプリケーションの起動に必要な情報を所定のサーバから取得するための情報取得部を有し、
前記認証情報生成部は、
前記情報取得部からの前記認証有効期限情報の更新要求に基づいて、対応する前記第２認証情報の認証有効期限情報を更新し、更新された認証期限情報を含む第２認証情報を前記情報取得部に提供することを特徴とする請求項１９に記載のオンラインサービスシステム。
【請求項２２】
前記認証要求及び前記サービス接続要求は、前記ユーザ端末の装置固有の識別情報を含んで構成され、

前記認証情報生成部は、発行された前記第２認証情報と前記認証要求に含まれる前記識別情報とを関連付けて保存し、
前記認証部は、前記識別情報及び前記第２認証情報を用いて前記第２認証処理を遂行することを特徴とする請求項１９から２１のいずれか１つに記載のオンラインサービスシステム。
【請求項２３】
前記認証情報生成部は、前記第２認証処理の認証結果が認証成功である場合に、前記第２認証情報に関連する第３認証情報を生成することを特徴とする請求項１９から２２のいずれか１つに記載のオンラインサービスシステム。
【請求項２４】
前記第３認証情報は、前記第２認証情報に含まれる認証有効期限情報及び発行シーケンス番号が異なる認証情報であることを特徴とする請求項２３に記載のオンラインサービスシステム。
【請求項２５】
ネットワークを通じて接続可能なユーザ端末にオンラインサービスを提供するオンラインサービスシステムのユーザ認証管理を行う認証管理装置であって、
前記ユーザ端末が前記オンラインサービスにログインした後に前記オンラインサービスを利用するための第１認証情報と、前記第１認証情報を用いた認証結果に基づいて発行される該第１認証情報と異なる第２認証情報と、を生成する認証情報生成部と、
前記ユーザ端末からの前記第１認証情報を含む認証要求に応答して前記第１認証情報を用いた第１認証処理を遂行するとともに、前記ユーザ端末からの前記第２認証情報を含むサービス接続要求に応答し、前記ユーザ端末への前記オンラインサービスの提供を開始するための該第２認証情報を用いた第２認証処理を遂行する認証部と、を有することを特徴とする認証管理装置。
【請求項２６】
前記ユーザ端末から送信される前記認証要求及び前記サービス接続要求は、前記ユーザ端末の装置固有の識別情報を含み、
前記認証情報生成部は、前記第１及び第２認証情報を記憶する記憶部に前記識別情報と前記第２認証情報とを関連付けて保存し、
前記認証部は、前記サービス接続要求に含まれる前記識別情報と前記第２認証情報とを用いた前記第２認証処理を遂行することを特徴とする請求項２５に記載の認証管理装置。
【請求項２７】
前記認証情報生成部は、認証有効期限を含んだ前記第２認証情報を生成するとともに、
前記ユーザ端末からの前記認証有効期限の更新要求に基づいて、前記認証有効期限を延長する更新処理を遂行することを特徴とする請求項２５又は２６に記載の認証管理装置。
【請求項２８】
前記認証情報生成部は、前記第２認証処理の認証結果が認証成功である場合に、前記第２認証情報に関連する第３認証情報を生成することを特徴とする請求項２５から２７のいずれか１つに記載の認証管理装置。
【請求項２９】
前記第３認証情報は、前記第２認証情報に含まれる認証有効期限情報及び発行シーケンス番号が異なる認証情報であることを特徴とする請求項２８に記載の認証管理装置。
【請求項３０】
オンラインサービスを提供するオンラインサービスシステムにネットワークを通じて接続可能であって、前記オンラインサービスの提供を受けるコンピュータに、
前記オンラインサービスシステムのサービス利用に伴って該オンラインシステムが発行する第１認証情報を含む認証情報発行要求を前記オンラインサービスシステムに送信する機能と、
前記第１認証情報を用いた前記オンラインサービスシステム側の認証結果に基づいて発行される認証情報であって、前記オンラインサービスシステムからのサービス提供の開始

に際する認証処理に用いられる第２認証情報を含むサービス接続要求を、前記オンラインサービスシステムに送信する機能と、
を実現させるためのプログラム。
【請求項３１】
前記第２認証情報は、認証有効期限情報を含み、
前記認証有効期限情報と現在時間情報とに基づいて認証有効期限に対して所定の時間経過したか否かを判別し、前記所定の時間が経過したと判別された場合に、前記オンラインシステムに前記認証有効期限情報の更新要求を送信する機能を、さらに含むことを特徴とする請求項３０に記載のプログラム。
【請求項３２】
当該コンピュータの装置固有の識別情報を取得する機能をさらに含み、
認証情報発行要求を前記オンラインシステムに送信する機能、及びサービス接続要求を、前記オンラインシステムに送信する機能は、
前記認証要求及び前記サービス接続要求に前記識別情報を含ませて前記オンラインシステムに送信することを特徴とする請求項３０又は３１に記載のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザの正当性を保証したオンラインサービスのサービス提供方法及びオンラインサービスシステムに関する。
【背景技術】
【０００２】
近年、インターネットを通じたゲームサービス等の様々なオンラインサービスが提供されている。これらのインターネットを通じたサービスでは、サービス加入者に予め付与又は登録したユーザＩＤ及びパスワードを用いて認証処理を行い、サービス利用時の本人確認が行われる。サービス提供側は、この本人確認に基づいてゲームサービス等を提供する。
【０００３】
図１７は、ゲームサービスにおけるゲームサービス提供方法（ゲーム起動方法）を示す図であり、ゲームサービスを提供するオンラインサービス提供サイト（ＷＥＢサイト）にユーザがアクセスして、所望のゲームを開始するまでの過程を示している。
【０００４】
図１７に示すように、オンラインサービス提供サーバ１００は、ネットワークＮを通じて接続するユーザ端末３００に、サービスログイン画面を提供する。ユーザは、ユーザ端末３００のブラウザに表示されたサービスログイン画面にユーザＩＤ及びパスワードを入力する。ユーザ端末３００のブラウザは、当該画面に入力されたユーザＩＤ及びパスワードをオンラインサービス提供サーバ１００に送信するとともにユーザＩＤ及びパスワードを保持する。
【０００５】
そして、オンラインサービス提供サーバ１００では、受信したユーザＩＤ及びパスワードを用いて所定の認証処理を遂行し、認証結果（認証ＯＫ／認証ＮＧ）をユーザ端末３００に送信する。オンラインサービス提供サーバ１００は、ユーザ端末３００を介したユーザの操作によりゲームサービス提供画面（ゲーム選択画面）を提供する。
【０００６】
ユーザは、ゲームを開始するためにサービスにログイン後、ブラウザに表示されたゲーム選択画面から所望するゲームを選択する。オンラインサービス提供サーバ１００は、このゲーム選択に応答してユーザ端末３００に選択したゲームのゲーム起動画面を提供し、ユーザによりゲーム起動が選択されると（ゲーム起動ボタンが押下されると）、ブラウザは、オンラインサービス提供サーバ１００にゲーム起動要求を送信し、オンラインサービ

ス提供サーバ１００は、ゲーム起動要求に応答してブラウザにゲーム起動指示を送信する。

【０００７】

ブラウザは、ゲーム起動指示に基づいて、選択されたゲームに対応する予めユーザ端末３００に設置されたゲームクライアント（ゲームプログラム）を起動させるとともに、該ブラウザが保持していたユーザＩＤ及びパスワードを該ゲームクライアントに受け渡す。ゲームクライアントは、ゲームを開始するための処理として、ゲームサーバ２００にゲームセッション接続要求とともに、ブラウザから受け取ったユーザＩＤ及びパスワードをゲームサーバ２００に送信する。

【０００８】

ゲームサーバ２００では、ゲームクライアントからのゲームセッション接続要求に応答して受信したユーザＩＤ及びパスワードを用い、ゲームサーバ２００側でのユーザ認証処理を遂行する。認証処理が成功であれば、ゲームサーバ２００は、ゲームクライアント（ユーザ端末３００）との間のゲームセッション確立処理を遂行し、ゲームクライアントとの間でゲーム制御を遂行する。

【０００９】

【特許文献１】特開２００３－１８８７３号公報

【特許文献２】特開２００７－１０９１２２号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

上述のように従来のオンラインサービスシステムでは、ブラウザを介したサービスログイン認証と、サービスに伴いユーザ端末で起動するサービスアプリケーション機能（プログラム）の起動に際するサービス起動認証とが行われ、サービスログイン認証とサービス起動認証とが、同じユーザＩＤ及びパスワードのみを用いて行われる。このため、パスワード等の詐取、盗聴等に対するセキュリティが低い問題があった。

【００１１】

つまり、従来のオンラインサービスシステムでは、ブラウザでのサービスログイン後でなければ、ゲームサーバに接続できない（ゲームを起動して開始することができない）が、ゲームサーバ側での認証処理は、ユーザＩＤ及びパスワードによるサービスログインが正常に完了したことを前提に、オンラインサービス提供サーバでのサービスログイン結果に関係なくゲームクライアント（サービスアプリケーション）からのゲームセッション接続要求とユーザＩＤ及びパスワードに基づいて行われていた。

【００１２】

例えば、Cookie技術を用いてサービスログイン状態を管理している場合、ユーザ端末とオンラインサービス提供サーバとの間のHTTP通信等においてCookie情報のやり取りが行われ、サービスへのログイン／ログアウトの情報がCookie情報に含まれてユーザ端末で保持される。そして、ユーザ端末は、ユーザのゲーム起動要求に応答して当該ユーザ端末側において保持しているCookie情報を参照してサービスログイン／ログアウトをチェックし、ゲーム起動要求をオンラインサービス提供サーバに送信できないように構成しているが、ゲームサーバでは、オンラインサービス提供サーバでのサービスログインの有無に関係なく（Cookie情報等を用いたサービスへのログイン／ログアウトをチェックせずに）、同じユーザＩＤ及びパスワードを用いた個別の認証処理を行ってユーザにゲームサービスを提供していた。

【００１３】

したがって、サービスログインを行うユーザ端末（ブラウザ）とゲームセッション接続要求を行うユーザ端末（ゲームクライアント）との間で同一性が保証されない個別の認証が行われていたため、パケットキャプチャー（スニファ／ダンプ）等によってパスワードが詐取、盗聴された場合、ブラウザを介してサービスにログインしなくても、盗聴等されたユーザＩＤ及びパスワードを用いて他人が直接ゲームサーバに接続してゲームを利用で

きてしまう問題があった。

【００１４】

また、ブラウザと該ブラウザ以外のサービスアプリケーションとを用いてサービスを提供する従来のオンラインサービスシステムでは、ブラウザからサービスアプリケーションにユーザＩＤ及びパスワードが受け渡されるため、ユーザ端末に悪意あるパケットスニファ等が設置されている場合には、オンラインサービス提供サーバ及びゲームサーバとの間の通信以外にも、ブラウザとサービスアプリケーションとの間でユーザＩＤ及びパスワードが漏洩する危険性があり、サービスログインを行うブラウザとゲームセッション接続要求を行うゲームクライアントとの間で同一性が保証されない従来のオンラインサービスシステムの認証方法では、パスワード等の詐取、盗聴等に対するサービスの不正使用を抑制することができなかった。

【００１５】

そこで、本発明の目的は、正当なユーザ以外のオンラインサービス利用を抑制し、正当なユーザが安全にオンラインサービスを利用することができるサービス提供方法及びオンラインサービスシステムを提供することにある。

【課題を解決するための手段】

【００１６】

本発明の１つの観点としての、オンラインサービスを利用するためにユーザ端末が接続可能なオンラインサービス提供サーバと、オンラインサービス提供サービスにおけるユーザの認証管理を行う認証管理サーバと、オンラインサービスを提供するサービスサーバとを備えるオンラインサービスシステムのサービス提供方法は、上記認証管理サーバが、オンラインサービス提供サーバでのユーザログイン情報に基づいて第１認証情報をユーザ端末に発行し、保存する第１ステップと、上記ユーザ端末が、発行された第１認証情報を含む認証要求を認証管理サーバに送信する第２ステップと、上記認証管理サーバが、第１認証情報を用いて認証処理を遂行し、認証結果に基づいて第２認証情報をユーザ端末に発行し、保存する第３ステップと、上記ユーザ端末が、第２認証情報を含むサービス接続要求を上記サービスサーバに送信する第４ステップと、上記サービスサーバが、第２認証情報を用いて認証管理サーバを通じた認証処理を遂行し、認証結果に基づいてユーザ端末へのオンラインサービスの提供を開始する第５ステップと、を含むことを特徴とする。

【００１７】

また、上記第２認証情報は、認証有効期限情報を含むように構成され、上記ユーザ端末は、認証有効期限情報と現在時間情報とに基づいて認証有効期限に対して所定の時間経過したか否かを判別し、所定の時間が経過したと判別された場合に上記認証管理サーバに認証有効期限情報の更新要求を送信するステップと、上記認証管理サーバが、上記更新要求に応答して上記第２認証情報の認証有効期限情報を更新するステップと、を含むように構成することができる。

【００１８】

また、上記ユーザ端末は、第１認証情報を含む認証要求を認証管理サーバに送信する際、該ユーザ端末の装置固有の識別情報（コンピュータ名やＭＡＣアドレス、ＩＰアドレス等）を共に送信するように構成することができ、認証管理サーバが、第２認証処理と識別情報とを関連付けて保存し、上記サービスサーバが、識別情報及び第２認証情報を用いて認証管理サーバを通じた認証処理を遂行するように構成することができる。

【００１９】

また、上記第５ステップは、上記サービスサーバがサービス接続要求に応答して第２認証情報を含む認証要求を認証管理サーバに送信するステップと、上記認証管理サーバが、サービスサーバからの認証要求に基づく第２認証情報を用いた認証処理を遂行し、認証処理の認証結果をサービスサーバに送信するステップと、上記サービスサーバが、認証管理サーバから受信した認証結果に基づいてユーザ端末へのオンラインサービスの提供を開始するステップと、を含むことができる。また、上記第２認証情報を用いた認証処理を遂行し、認証結果をサービスサーバに送信するステップにおいて、認証管理サーバが、認証結

果が認証成功である場合、第２認証情報に関連する第３認証情報を発行し、保存するステップと、認証結果及び第３認証情報をサービスサーバに送信するステップと、を含むように構成することができ、さらに、上記サービスサーバがオンラインサービスの提供を開始するステップは、上記第３認証情報をユーザ端末に送信するステップと、を含むことができる。

【００２０】

また、上記第３認証情報は、上記第２認証情報に含まれる認証有効期限情報及び発行シーケンス番号が異なる認証情報として生成することができる。

【００２１】

また、本発明の他の観点としての、ブラウザを介してユーザ端末がオンラインサービスを利用するために接続するオンラインサービス提供サーバと、オンラインサービスにおけるユーザの認証管理を行う認証管理サーバと、ユーザ端末に設置されたオンラインサービスを利用するためのサービスアプリケーションを通じてオンラインサービスを提供するサービスサーバと、を備えるオンラインサービスシステムのサービス提供方法は、上記認証管理サーバが、ブラウザを通じたサービス利用要求に応答し、オンラインサービス提供サーバでのユーザログイン情報に基づいて第１認証情報をユーザ端末に発行し、保存する第１ステップと、ブラウザが、発行された前記第１認証情報を含む認証要求を認証管理サーバに送信する第２ステップと、認証管理サーバが、第１認証情報を用いて認証処理を遂行し、認証結果に基づいて第２認証情報をユーザ端末に発行し、保存する第３ステップと、ブラウザが、発行された第２認証情報をサービスアプリケーションに受け渡す第４ステップと、サービスアプリケーションが第２認証情報を含むサービス接続要求をサービスサーバに送信する第５ステップと、サービスサーバが、第２認証情報を用いて認証管理サーバを通じた処理を遂行し、認証結果に基づいてサービスアプリケーションを通じたオンラインサービスの提供を開始する第６ステップと、を含むことを特徴とする。

【００２２】

また、本発明のさらに他の観点としてのネットワークを通じて接続可能なユーザ端末にオンラインサービスを提供するオンラインサービスシステムは、ユーザ端末がオンラインサービスにログインした後オンラインサービスを利用するための第１認証情報と、該第１認証情報を用いた認証結果に基づいてユーザ端末に発行される第１認証情報と異なる第２認証情報と、を生成する認証情報生成部と、ユーザ端末からの第１認証情報を含む認証要求に応答して第１認証情報を用いた第１認証処理を遂行するとともに、ユーザ端末からの第２認証情報を含むサービス接続要求に応答し、ユーザ端末へのオンラインサービスの提供を開始するための該第２認証情報を用いた第２認証処理を遂行する認証部と、第２認証処理の認証結果に基づいて、オンラインサービスをユーザ端末に提供するオンラインサービス提供部と、を有することを特徴とする。

【００２３】

また、本発明のさらに他の観点としてのネットワークを通じて接続可能なユーザ端末にオンラインサービスを提供するオンラインサービスシステムは、ユーザ端末がブラウザを通じてオンラインサービスにログインした後、オンラインサービスを利用するための第１認証情報と、第１認証情報を用いた認証結果に基づいてユーザ端末に発行される第１認証情報と異なる第２認証情報と、を生成する認証情報生成部と、ブラウザを通じた第１認証情報を含む認証要求に応答して第１認証情報を用いた第１認証処理を遂行するとともに、ユーザ端末に設置されるオンラインサービスをユーザ端末で利用可能に動作させるサービスアプリケーションからの第２認証情報を含むサービス接続要求に応答し、ユーザ端末へのオンラインサービスの提供を開始するための該第２認証情報を用いた第２認証処理を遂行する認証部と、第２認証処理の認証結果に基づいて、サービスアプリケーションを通じてオンラインサービスをユーザ端末に提供するオンラインサービス提供部と、を有することを特徴とする。

【００２４】

また、本発明のさらに他の観点としてのネットワークを通じて接続可能なユーザ端末に

オンラインサービスを提供するオンラインサービスシステムの当該オンラインサービスにおけるユーザの認証管理を行う認証管理装置は、ユーザ端末がオンラインサービスにログインした後にオンラインサービスを利用するための第１認証情報と、第１認証情報を用いた認証結果に基づいてユーザ端末に発行される該第１認証情報と異なる第２認証情報と、を生成する認証情報生成部と、ユーザ端末からの第１認証情報を含む認証要求に応答して該第１認証情報を用いた第１認証処理を遂行するとともに、ユーザ端末からの第２認証情報を含むサービス接続要求に応答し、ユーザ端末へのオンラインサービスの提供を開始するための該第２認証情報を用いた第２認証処理を遂行する認証部と、を有することを特徴とする。

【００２５】

また、本発明のさらに他の観点としてプログラムは、オンラインサービスを提供するオンラインサービスシステムにネットワークを通じて接続可能であって、オンラインサービスの提供を受けるコンピュータに、オンラインサービスシステムのサービス利用に伴って該オンラインサービスシステムが発行する第１認証情報を含む認証情報発行要求をオンラインサービスシステムに送信する機能と、第１認証情報を用いたオンラインサービスシステム側の認証結果に基づいて発行される認証情報であって、オンラインサービスシステムからのサービス提供の開始に際する認証処理に用いられる第２認証情報を含むサービス接続要求を、オンラインサービスシステムに送信する機能と、を実現させることを特徴とする。

【発明の効果】

【００２６】

本発明によれば、正当なユーザ以外のオンラインサービス利用を抑制し、セキュリティ性の高い安全なオンラインサービスの提供が可能となる。

【００２７】

すなわち、オンラインサービス提供サーバでのユーザログインに基づいて発行される第１認証情報を用いた認証処理を遂行し、該認証処理の認証結果に基づいて第１認証情報と異なるオンラインサービスの提供を開始するための第２認証情報をユーザ端末に発行する。

【００２８】

したがって、オンラインサービスにサービスログインせずに不正にサービスを利用することを抑制できるとともに、第１認証情報の認証結果に基づいて発行される第２認証情報によりオンラインサービスの提供を開始するための認証処理を遂行するので、オンラインサービスを利用するユーザの同一性を保証することができ、パスワード等の詐取・盗難による不正なサービス利用を抑制することができる。このため、オンラインサービスにおけるユーザ認証におけるセキュリティ性が向上し、正当なユーザによる安全なオンラインサービスの利用が確保される。

【発明を実施するための最良の形態】

【００２９】

以下、本発明の好適な実施形態を、図面を参照しながら説明する。

【００３０】

（第１実施形態）

図１は、本発明のオンラインサービスシステムの構成図である。本実施形態のオンラインサービスシステムは、サービス提供サイト（ＷＥＢサイト）を提供するＷＥＢサーバとしてのオンラインサービス提供サーバ１００、オンラインサービスにおけるユーザの認証管理を行う認証管理サーバ４００、及びオンラインサービスを提供するサービスサーバとしてのゲームサーバ２００とを備える。本実施形態では、オンラインサービスとしてゲームサービスを一例に説明する。各サーバは、ユーザ端末３００とインターネット等のネットワークＮを通じて接続可能に構成され、かつ各サーバ間は、ネットワークＮ又は専用回線等の通信回線で接続されている。ユーザ端末３００は、パーソナルコンピュータやＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）、携帯電話機等の移動通

信端末装置などの通信機能及び演算機能を備えた端末装置である。

【００３１】

オンラインサービス提供サーバ１００は、ネットワークＮを介した複数のユーザ端末３００との通信制御及び認証管理サーバ４００との通信制御を行う通信制御部１１０、ユーザ端末３００にオンラインサービス（ゲームサービス）を提供するための所定の画面を提供するオンラインサービス制御部１２０、オンラインサービス提供サーバ１００全体の制御を司る制御部（ＣＰＵ）１３０、及び画面（ページ）データ等を記憶する記憶部１４０を含む。

【００３２】

ゲームサーバ２００は、ネットワークＮを介した複数のユーザ端末３００との通信制御及び認証管理サーバ４００との通信制御を行う通信制御部２１０、ユーザ端末３００との間の所定のゲームセッションを通じて後述するユーザ端末３００に設置（インストール）されたゲームクライアント３４０との間でゲーム制御を遂行するゲーム制御部２２０、ゲームサーバ２００全体の制御を司る制御部（ＣＰＵ）２３０、及び記憶部２４０を含む。また、ゲームサーバ２００と個別に構成されたゲームＩＤ毎に各ユーザのゲーム情報を格納するゲームＤＢ（ゲームデータベース）６００が、当該ゲームサーバ２００に接続されており、ゲーム制御部２２０は、ゲームＤＢ６００との間で情報の格納、更新、削除等の制御も行う。なお、ゲームＤＢ６００は、ゲームサーバ２００に含まれるように一体に構成することも可能である。

【００３３】

認証管理サーバ４００は、ネットワークＮを介した複数のユーザ端末３００、オンラインサービス提供サーバ１００及びゲームサーバ２００との通信制御を行う通信制御部４１０、ゲームサービスをユーザが利用する際にユーザ端末３００に発行する認証情報を生成する認証情報生成部４２０、認証情報生成部４２０で生成された認証情報を用いた認証処理を遂行する認証部４３０、認証管理サーバ４００全体の制御を司る制御部（ＣＰＵ）４４０、及び記憶部４５０を含む。そして、認証管理サーバ４００と個別に構成された認証情報生成部４２０で生成された認証情報及びユーザＩＤ等を格納する認証ＤＢ（認証データベース）５００が、当該認証管理サーバ４００に接続され、認証情報生成部４２０は、認証ＤＢ５００との間での情報の格納、更新、削除等を行うとともに、認証部４３０は、認証処理に際して、認証ＤＢ５００に格納されている認証情報を参照する。なお、認証ＤＢ５００は、認証管理サーバ４００に含まれるように一体に構成することも可能である。

【００３４】

図２は、本実施形態のユーザ端末３００の構成ブロック図である。図２に示すように、本実施形態のユーザ端末３００は、ネットワークＮを介したオンラインサービス提供サーバ１００、認証管理サーバ４００、及びゲームサーバ２００との通信制御を行う通信制御部３１０、ユーザ端末３００全体の制御を司る制御部（ＣＰＵ）３２０、オンラインサービス提供サーバ１００から提供される各画面（ページ）を表示する表示制御部としてのブラウザ３３０、ユーザ端末３００側のゲーム処理を行うゲームクライアント３４０を備えるとともに、記憶部（メモリ）３５０、外部インターフェース３６０、操作部３７０（キーボード、マウス、コントローラ等）、表示インターフェース３８０、表示部３９０（表示ディスプレイ）を備える。なお、ブラウザ３３０は、インターネットエクスプローラ等の各種のＷＥＢブラウザが適用される。

【００３５】

ゲームクライアント３４０は、ゲームサービスを利用するためのサービスアプリケーションプログラムであり、一般的なオンラインゲームにおいて適用される技術である。ゲームクライアント３４０は、ゲームを行うユーザ端末３００に予め（若しくはゲーム開始時に）インストールされ、ユーザ端末３００側のゲーム処理全般を担う。本実施形態のゲームクライアント３４０は、ゲームサーバ２００から送信されるゲーム制御情報に応じて表示インターフェース３８０を介した表示部３９０へのゲーム表示処理（ゲーム画面の表示処理を含む）及びゲーム制御を行うゲーム処理部３４１、ゲームに使用される多様なグラ

フィックデータ、ゲームルールが定義されたゲーム基本ファイル、及び更新ファイルなどの情報（ゲーム情報）が格納されるゲームデータ格納部３４２を備える。ゲームデータ格納部３４２に格納されるデータは、ゲーム開始時、ゲーム終了時、又はゲーム進行中にゲームサーバ２００との通信により適宜更新される情報が含まれる。

【００３６】

また、ブラウザ３３０及びゲームクライアント３４０は、第１認証制御部３３１及び第２認証制御部３４３を各々含み、第１及び第２認証制御部３３１、３４３は、認証管理サーバ４００との間での認証情報の制御を遂行する。なお、ブラウザ３３０の第１認証制御部３３１は、ＡｃｔｉｖｅＸコントロール等で実現することができ、第１認証制御部３３２は、ブラウザにプラグインされる形態で実現することが可能である。また、第２認証制御部３４３は、ゲームクライアント３４０を構成するゲームプログラムの一部として実現することができ、ゲームクライアント３４０に内的に又は外的に付加される形態で実現することが可能である。

【００３７】

ここで、図３及び図４を参照しながら、本実施形態のゲームサービスシステムのサービス提供方法（サービス起動方法）について詳細に説明する。

【００３８】

本実施形態のサービス提供方法は、認証管理サーバ４００を通じた認証処理を遂行し、ゲームサーバ２００を通じてゲームサービスをユーザ端末３００に提供する。認証管理サーバ４００は、オンラインサービスサイトでのサービスログイン認証に用いられるパスワードと異なる認証情報（第２認証情報）をユーザ端末３００に発行し、ゲームサーバ２００は、認証管理サーバ４００が発行した認証情報を用いた認証結果に応じてユーザ端末３００へのゲームサービスの提供を開始する。

【００３９】

さらに、本実施形態のサービス提供方法は、ゲームサーバ２００によるゲームサービスの提供を開始するための認証処理（サービス起動認証処理）に用いられる第２認証情報の発行に際して、認証発行チケット（第１認証情報）をさらにユーザ端末３００に発行し、セキュリティ性の高い認証情報の生成処理を遂行する。つまり、ゲームサーバ２００によるゲームサービスの提供を開始するための認証処理に用いられる第２認証情報は、認証発行チケットによる認証処理を経て発行され、認証発行チケットを有しない第２認証情報の発行要求（認証発行チケットによる認証処理が認証ＮＧである第２認証情報の発行要求）は、不正な処理要求として判別されてゲームを開始することができない。つまり、認証発行チケットによりゲームを起動するユーザ端末３００と認証情報が発行されるユーザ端末３００との同一性を保証した認証を行う。

【００４０】

図３に示すように、オンラインサービス提供サーバ１００は、ネットワークＮを通じて接続するユーザ端末３００に、サービスログイン画面を提供する。ユーザは、ユーザ端末３００のブラウザ３３０に表示されたサービスログイン画面に、予め登録されたユーザＩＤ及びパスワードを入力する。ユーザ端末３００のブラウザ３３０は、当該画面に入力されたユーザＩＤ及びパスワードをオンラインサービス提供サーバ１００に送信する。

【００４１】

オンラインサービス提供サーバ１００では、受信したユーザＩＤ及びパスワードを用い、認証ＤＢ５００に格納された不図示のユーザＩＤ－パスワードテーブルを参照してサービスログイン認証処理を遂行し、認証結果（認証ＯＫ（ログイン）／認証ＮＧ（ログアウト））を含むCookie情報とともに、ゲームサービス提供画面（ゲーム選択画面）をユーザ端末３００に提供する。上述のように、本実施形態は、Cookie技術を用いてサービスログイン状態を管理している。なお、Cookie情報は、最終ログイン日時、最終ログアウト日時、ログイン／ログアウト状態等を含むことができる。また、Cookie技術を用いたサービスへのログイン／ログアウト情報の管理以外の技術も適用することできる。例えば、オンラ

インサービス提供サーバでのサービスログイン認証時にユーザのサービスログイン状態を示す情報を別途保存して管理することも可能である。

【００４２】

オンラインサービスにログイン後（サービスログイン後）、ユーザは、ゲームを開始するためにブラウザ３３０に表示されたゲーム選択画面から所望するゲームを選択する。オンラインサービス提供サーバ１００は、このゲーム選択に応答してユーザ端末３００に選択したゲームのゲーム起動画面を提供し、ユーザによりゲーム起動が選択されると（ゲーム起動ボタンが押下されると）、ブラウザ３３０は、ユーザ端末３００において保存されているサービスログインの認証結果（認証ＯＫ／認証ＮＧ）を含むCookie情報を参照して、当該ユーザのログイン状態をチェックする。Cookie情報のログイン状態を示す情報が認証ＯＫであると判別された場合、ブラウザ３３０は、オンラインサービス提供サーバ１００にゲーム起動要求（起動されるゲームＩＤ、ユーザＩＤを含む）を送信する。このゲーム起動要求を受信したオンラインサービス提供サーバ１００は、ゲーム起動要求に応答して、認証管理サーバ４００に対して認証発行チケットである第１認証情報の発行要求を送信する。一方、ブラウザ３３０は、Cookie情報のログイン状態を示す情報が認証ＮＧ（ログアウト）であると判別された場合、オンラインサービス提供サーバ１００に対してゲーム起動要求を送信せずに、所定のメッセージ、例えば「サービスにログインしてからゲームを起動してください」などのメッセージを表示する。

【００４３】

認証管理サーバ４００は、オンラインサービス提供サーバ１００からの第１認証情報の発行要求を受信すると、認証有効期限情報を含む第１認証情報を生成し、ゲーム起動要求をしたユーザＩＤと関連付けて生成した第１認証情報を認証ＤＢ５００に格納する。図４（ａ）は、発行された第１認証情報が格納される第１認証情報テーブルの一例である。第１認証情報テーブルは、発行するユーザＩＤ毎に、ゲーム起動要求（ゲーム選択）に含まれるゲームＩＤ、オンラインサービス提供サーバ１００がユーザ端末３００からゲーム起動要求を受信した日時（又は認証管理サーバ４００がオンラインサービス提供サーバ１００から第１認証情報の発行要求を受信した日時）、第１認証情報、シーケンス番号、認証有効期限を格納する。

【００４４】

第１認証情報は、所定のアルゴリズムで生成される文字及び数字が混在した認証番号と、第１認証情報が発行される度に所定の数だけインクリメントされるシーケンス番号とで構成される。すなわち、同一のユーザに対して一度第１認証情報を生成すると、シーケンス番号が１インクリメントされ、次回に生成される第１認証情報は、シーケンス番号が異なり、前回に発行された第１認証情報とは異なる認証情報となる。言い換えれば、一度認証処理に用いられた認証情報は、次回又は他の認証処理で使用することができず、認証処理が遂行される毎にシーケンス番号が異なる認証情報が生成されることになる。したがって、一度発行された第１認証情報は、一度切りしか使用できない使い捨ての認証情報（ワンタイムパスワード；ＯＴＰ）として生成される。また、第１認証情報は、認証情報としての時間的な制限（認証有効期限）があり、例えば、第１認証情報の発行から１分以内でなければ、第１認証情報を用いた認証処理において、認証情報としての有効性が消失することになる。

【００４５】

このように認証管理サーバ４００で生成された第１認証情報は、オンラインサービス提供サーバ１００を介してユーザ端末３００に提供される。第１認証情報を受信したブラウザ３３０の第１認証制御部３３１は、ユーザ端末３００の装置固有の識別情報（以下、ＰＣ識別情報と称す）を当該装置から取得する。ＰＣ識別情報としては、ユーザ端末３００のＭＡＣアドレス、ユーザ端末３００に登録されているコンピュータ名やユーザ名がある。第１認証制御部３３１は、受信した第１認証情報及び取得したＰＣ識別情報を含む認証情報発行要求を認証管理サーバ４００に送信する。なお、ＰＣ識別情報は、ＭＡＣアドレスやコンピュータ名等を組み合わせたり、ＭＡＣアドレスやコンピュータ名の一部を抽出

して組み合わせて用いることも可能であり、ＭＡＣアドレス等をそのままＰＣ識別情報として使用する以外にも、任意に各識別情報を組み合わせてＰＣ識別情報として使用することもできる。また、ＭＡＣアドレスの一部を抽出してＰＣ識別情報として使用することも可能である。

【００４６】

認証管理サーバ４００は、受信した認証情報発行要求に含まれる第１認証情報を用いて認証ＤＢ５００を参照し、認証処理（第１認証処理）を遂行する。この第１認証処理において認証ＯＫであれば、ゲームサーバ２００によるユーザ端末３００へのゲームサービスの提供を開始するための認証処理に用いられる第２認証情報を生成する。

【００４７】

図４（ｂ）は、発行された第２認証情報が格納される第２認証情報テーブルの一例である。第２認証情報テーブルは、発行するユーザＩＤ毎に、ゲームＩＤ、認証管理サーバ４００がユーザ端末３００から認証情報発行要求を受信した日時、ＰＣ識別情報、第２認証情報、シーケンス番号、認証有効期限を格納する。

【００４８】

第２認証情報は、ゲームＩＤ、認証有効期限、ＰＣ識別情報及びシーケンス番号（第２シーケンス番号）で構成され、第２シーケンス番号は、第２認証情報が発行される度に所定の数だけインクリメントされる。当該第２認証情報も上述した第１認証情報と同様に、同一のユーザに対して一度第２認証情報を生成すると、シーケンス番号が１インクリメントされ、次回に生成される第２認証情報は、シーケンス番号が異なり、前回に発行された第２認証情報とは異なる認証情報となる。つまり、一度認証処理に用いられた認証情報は、次回又は他の認証処理で使用することができず、認証処理が遂行される毎にシーケンス番号が異なる第２認証情報が生成されることになる。したがって、一度発行された第２認証情報は、一度切りしか使用できない使い捨ての認証情報（ワンタイムパスワード；ＯＴＰ）として生成される。また、第２認証情報も、認証情報としての時間的な制限（認証有効期限）を含み、例えば、第２認証情報の発行タイムスタンプから５分以内（認証有効期限＝発行タイムスタンプ＋所定時間）でなければ、第２認証情報を用いた認証処理において、認証情報としての有効性が消失することになる。

【００４９】

また、第２認証情報は、第１認証情報とは異なり、ユーザ端末３００のＭＡＣアドレス等のＰＣ識別情報を含んで構成されている。

【００５０】

このように認証管理サーバ４００で生成された第２認証情報は、ユーザ端末３００に直接提供される。第２認証情報を受信したブラウザ３３０は、ゲームクライアント３４０を起動させ、受信した第２認証情報を当該ゲームクライアント３４０に受け渡す（出力する）。

【００５１】

ゲームクライアント３４０は、第２認証制御部３４３による上記第１認証制御部３３１と同様のＰＣ識別情報取得処理を遂行し、ブラウザ３３０から受け取った第２認証情報とともに改めて取得したＰＣ識別情報を含むゲーム接続要求をゲームサーバ２００に送信する。ゲームサーバ２００は、ユーザ端末３００からのゲーム接続要求に応答して、ＰＣ識別情報及び第２認証情報を含む認証要求を認証管理サーバ４００に送信する。認証管理サーバ４００は、第２認証情報に基づく認証結果及び第３認証情報をゲームサーバ２００に送信し、ゲームサーバ２００は、受信した認証結果に基づいて、ゲームクライアント３４０との間のゲームセッション確立処理及びゲーム制御を遂行するとともに、第３認証情報をゲームクライアント３４０に送信する。なお、この第３認証情報については、後述する。

【００５２】

また、本実施形態のＰＣ識別情報は、ゲームクライアント３４０の第２認証制御部３４３が、第１認証制御部３３１と同様にユーザ端末３００の装置固有のＰＣ識別情報を当該

装置から改めて取得し、ブラウザ３３０からＰＣ識別情報を受け取らない構成としている。これは第１認証制御部３３１（ブラウザ３３０）と第２認証制御部３４３（ゲームクライアント３４０）が同一のユーザ端末３３０で動作しているか否か、言い換えれば、ＰＣの同一性をより保証するために、第１及び第２認証制御部３３１、３４３の各々が、個別に当該ユーザ端末３３０からＰＣ固有情報を取得するように構成している。なお、第１認証制御部３３１において一度取得したＰＣ固有情報を第２認証制御部３４３に受け渡すように構成し、第２認証制御部３４３においてＰＣ固有情報を取得しないように構成することも可能である。

【００５３】

次に、図５Ａ及び図５Ｂを参照して、本実施形態のゲームサービスシステムのサービス提供方法の処理遷移について説明する。

【００５４】

まず、ユーザ端末３００は、ゲームを開始するためにゲームサービスを提供するオンラインサービスサイトであるオンラインサービス提供サーバ１００に、ブラウザ３３０を介して接続する（ステップＳ３０１）。オンラインサービス提供サーバ１００は、ネットワークＮを通じて接続したユーザ端末３００に、サービスログイン画面を提供する（ステップＳ１０１）。ユーザは、ユーザ端末３００のブラウザ３３０に表示されたサービスログイン画面に、予め登録されたユーザＩＤ及びパスワードを入力し、ユーザ端末３００のブラウザ３３０は、当該画面に入力されたユーザＩＤ及びパスワードをオンラインサービス提供サーバ１００に送信する（ステップＳ３０２）。

【００５５】

オンラインサービス提供サーバ１００は、ユーザ端末３００からのユーザＩＤ及びパスワードの受信に応答して、これらユーザＩＤ及びパスワードを用いて認証ＤＢ５００を参照してサービスログイン認証を遂行する（ステップＳ１０２）。オンラインサービス提供サーバ１００は、サービスログインの認証結果（認証ＯＫ／認証ＮＧ等のサービスログイン／ログアウト状態を示す情報）を含むCookie情報をユーザ端末３００に送信する。

【００５６】

オンラインサービスにログイン後、ユーザが、ゲームを開始するためにブラウザ３３０に表示されたゲーム選択画面から所望するゲームを選択すると、オンラインサービス提供サーバ１００は、このゲーム選択に応答してユーザ端末３００に選択したゲームのゲーム起動画面を提供する。そして、ユーザによりゲーム起動が選択されると（ゲーム起動ボタンが押下されると）、ブラウザ３３０は、ユーザ端末３００に保存されているCookie情報を参照して、当該ユーザのログイン状態をチェックする。ブラウザ３３０は、Cookie情報のログイン状態を示す情報が認証ＯＫであると判別された場合、オンラインサービス提供サーバ１００にゲーム起動要求（起動されるゲームＩＤ、ユーザＩＤを含む）を送信する。Cookie情報のログイン状態を示す情報が認証ＮＧ（ログアウト）であると判別された場合は、オンラインサービス提供サーバ１００に対してゲーム起動要求を送信しない（ステップＳ３０３）。そして、ユーザ端末３００からゲーム起動要求を受信したオンラインサービス提供サーバ１００は、認証管理サーバ４００に認証発行チケットである第１認証情報の発行要求を送信する。

【００５７】

認証管理サーバ４００は、オンラインサービス提供サーバ１００から第１認証情報の発行要求を受信した場合、すなわち、ユーザ端末３００からのゲーム起動要求に応答して認証チケット発行処理を遂行する。具体的には、認証部４３０は、認証情報生成部４２０に第１認証情報の生成処理を指示し、認証情報生成部４２０は、認証有効期限を含む第１認証情報を生成するとともに、生成した第１認証情報、発行要求（ゲーム起動要求）に含まれるゲームＩＤ、認証有効期限情報等をユーザＩＤと関連付けて認証ＤＢ５００の第１認証情報テーブルに格納する。生成された第１認証情報は、オンラインサービス提供サーバ１００を介してユーザ端末３００に送信される（ステップＳ４０１，Ｓ４０２）。

【００５８】

ブラウザ３３０の第１認証制御部３３１は、第１認証情報を受信すると、ユーザ端末３００の装置固有のＰＣ識別情報を該端末装置から取得し、受信した第１認証情報及び取得したＰＣ識別情報を含む認証情報発行要求を生成して、認証管理サーバ４００に送信する（ステップＳ３０４）。

【００５９】

認証管理サーバ４００の認証部４３０は、受信した認証情報発行要求に含まれる第１認証情報を用いて認証ＤＢ５００を参照し、第１認証処理を遂行する。具体的には、第１認証情報の一致性を判別するとともに、第１認証情報テーブルに格納されている認証有効期限と認証情報発行要求を受信したタイムスタンプを比較し、認証情報発行要求を受信したタイムスタンプが、認証有効期限を越えているか否かを判別する（ステップＳ４０３）。本実施形態では、これら２つの認証を満足する場合に、第１認証情報を用いた認証処理が成功した（認証ＯＫ）と判断する。

【００６０】

第１認証情報を用いた第１認証処理の認証結果が認証ＯＫである場合、認証部４３０は、認証情報生成部４２０に第２認証情報の生成処理を指示する。認証情報生成部４４０は、第２認証情報を生成するとともに、生成した第２認証情報、認証情報発行要求に含まれるＰＣ識別情報、認証有効期限情報等をユーザＩＤ毎に認証ＤＢ５００の第２認証情報テーブルに格納する。生成された第２認証情報は、ユーザ端末３００に送信される（ステップＳ４０４，Ｓ４０５）。なお、第１認証処理の認証結果が認証ＮＧである場合、第２認証情報を発行せずにユーザ端末３００に対してゲームサーバ２００に接続できない旨、サービス利用ができない旨等のメッセージを送信する。

【００６１】

ユーザ端末３００のブラウザ３３０は、図５Ｂに示すように、認証管理サーバ４００で生成された第２認証情報を受信すると、当該受信に応答してゲームクライアント３４０を起動させ、受信した第２認証情報、ユーザＩＤ、ゲームＩＤ等を当該ゲームクライアント３４０に受け渡す。また、ゲームクライアント３４０は、ブラウザ３３０と同様に該端末装置からＰＣ識別情報を改めて取得し、ブラウザ３３０から受け取った第２認証情報、ユーザＩＤ、ゲームＩＤ、及び改めた取得したＰＣ識別情報等を含むゲーム接続要求を生成してゲームサーバ２００に送信する（ステップＳ３０５）。

【００６２】

ゲームサーバ２００は、ユーザ端末３００（ゲームクライアント３４０）からのゲーム接続要求を受信すると、ゲーム制御部２２０が、受信したゲーム接続要求に含まれる第２認証情報、ユーザＩＤ、ゲームＩＤ、ＰＣ識別情報を抽出して、認証管理サーバ４００に抽出したこれらの情報を含む認証要求を送信する（ステップＳ２０１）。認証管理サーバ４００の認証部４３０は、認証要求とともに受信した第２認証情報、ユーザＩＤ、ゲームＩＤ、ＰＣ識別情報と用いた第２認証処理を遂行する。認証ＤＢ５００の第２認証情報テーブルを参照して、受信した第２認証情報及びＰＣ識別情報の一致性を判別し、かつ第２認証情報テーブルに格納されている認証有効期限と認証情報発行要求を受信したタイムスタンプを比較して認証情報発行要求を受信したタイムスタンプが、認証有効期限を越えているか否かを判別する。これら２つの認証を満足する場合に、第２認証情報を用いた認証処理が成功した（認証ＯＫ）と判断する。（ステップＳ４０６）。そして、認証管理サーバ４００の認証部４３０は、第２認証情報を用いた第２認証処理が認証ＯＫである場合、認証結果情報を生成するとともに、認証情報生成部４２０に対して第３認証情報の生成指示を出力する。認証情報生成部４２０は、第３認証情報を生成するとともに、生成した第３認証情報を認証ＤＢ５００に保存する（ステップＳ４０７）。その後、認証部４３０又は認証情報生成部４２０は、生成された認証結果と第３認証情報をゲームサーバ２００に送信する（ステップＳ４０８）。なお、第２認証情報を用いた第２認証処理の結果が認証ＮＧの場合は、第３認証情報は生成されない。

【００６３】

ゲームサーバ２００のゲーム制御部２２０は、認証管理サーバ４００からの認証結果及

び第３認証情報を受信し、認証ＯＫ／認証ＮＧを判別する。認証ＯＫであると判別された場合には、ゲームクライアント３４０との間のゲームセッション確立処理及びゲーム制御を遂行するとともに、第３認証情報をゲームクライアント３４０に送信する（ステップＳ２０２）。なお、第２認証処理の認証結果が認証ＮＧである場合、ユーザ端末３００に対してゲームサーバ２００に接続できない旨、サービス利用ができない旨等のメッセージを送信する。

【００６４】

第３認証情報を受信したゲームクライアント３４０の第２認証制御部３４３は、該第３認証情報を保存し、第３認証情報に含まれる認証有効期限と現在時刻とに基づいて、認証有効期限に対して所定の時間が経過したか否かを判別し、所定の時間が経過したと判別された場合に、第３認証情報の認証有効期限の更新要求を認証管理サーバ４００に送信する（ステップＳ３０６）。認証管理サーバ４００は、この更新要求を受信すると、対応する第３認証情報の認証有効期限を所定時間延長する更新処理を遂行し、更新結果として、認証有効期限が更新された第３認証情報を、ゲームクライアント３４０に送信する（ステップＳ４０９）。

【００６５】

ここで、第３認証情報について詳細に説明する。本実施形態のオンラインサービスシステムは、ゲームサーバ２００との間でゲームセッションが確立されてゲームが開始された後、ゲーム進行に伴うゲームサービスを構成する他のサーバが、本実施形態のゲームサーバ２００と同様の認証処理を行うために、第３認証情報を発行する。なお、ゲームサーバ２００が複数のサーバで構成されている場合は、複数の各ゲームサーバへのアクセス毎に認証管理サーバ４００を通じた認証処理が遂行されるように構成することができ、サービスを提供するために構成された各サーバの各々の認証に対する第４認証情報、第５認証情報・・・が、認証処理の度に発行される。

【００６６】

つまり、ゲーム進行中のアイテム購入時のポイント支払やアイテム購入のためのポイント購入などの処理は、ゲームサーバ２００と別個に構成される課金サーバ等で遂行される。したがって、ゲームクライアント３４０が課金サーバに接続する際に、課金サーバ側での認証管理サーバ４００を通じた認証を遂行するための第３認証情報を、第２認証情報を用いた第２認証処理後（ゲームクライアント３４０との間のゲームセッション確立処理及びゲーム制御開始後）に、ゲームクライアント３４０に発行する。したがって、ゲームクライアント３４０は、ゲームサーバ２００と同様に、課金サーバ等にユーザＩＤ，第３認証情報，アイテムコード等を含むアイテム購入要求やポイント購入要求等を送信し、課金サーバは、第３認証情報を含む認証要求を認証管理サーバ４００に送信し、認証結果に基づいて課金処理を遂行する。

【００６７】

この第３認証情報は、第２認証情報と同様に認証有効期限を含み、図４（ｂ）に示した第２認証情報と同様の構成を有するが、ゲーム接続要求に用いられる第２認証情報とは、認証有効期限とシーケンス番号とが異なる。

【００６８】

すなわち、本実施形態の第３認証情報は、第２認証情報のシーケンス番号が所定数インクリメントされた、該第２認証情報とは異なる認証情報として生成されつつ、第２認証情報に関連した認証情報として生成される。このため、ＰＣ識別情報が第３認証情報に引き継がれて、第２認証情報を用いた認証処理と同様のユーザの同一性を担保した認証処理が遂行される。

【００６９】

また、第３認証情報は、同様に認証有効期限を含むが、ゲーム進行中のどの時点でユーザがアイテムを購入するか、言い換えれば、第３認証情報を用いた認証処理（第３認証処理）が遂行されるかは、ユーザのゲーム進行に依存し、判別することができない。そこで、本実施形態の第２認証制御部３４３は、受信した第３認証情報の認証有効期限と現在時

刻とを比較チェックし、認証有効期限に対して所定の時間が経過したか否かを判別し、第３認証情報の認証有効期限の更新を認証管理サーバ４００に要求する。例えば、認証有効期限が１９：０５で、現在時刻が１９：００である場合の残り時間が５分である場合に、更新が必要であると判別したり、第３認証情報を受信した時点から、認証有効期限までの有効時間を算出し、有効時間が半分の時間が経過した場合に、更新が必要であると判別し、第３認証情報の認証有効期限の更新要求を認証管理サーバ４００に送信する。

【００７０】

そして、認証管理サーバ４００は、この更新要求を受信すると、対応する第３認証情報の認証有効期限を所定時間、例えば、５分延長する更新処理を遂行し、認証有効期限が更新された第３認証情報をゲームクライアント３４０（第２認証制御部３４３）に送信する。また、上述のように、この第２認証制御部３４３による更新処理は、第３認証情報が認証処理に使用されるまで、言い換えれば、第３認証情報を含む所定の処理要求を所定の処理を行うサーバに送信するまで、繰り返し遂行され、また、第３認証情報を用いた認証処理を遂行した認証管理サーバ４００は、第３認証情報のシーケンス番号が所定数インクリメントされた第３認証情報とは異なる第４認証情報、すなわち、第２及び第３認証情報のシーケンス番号及び認証有効期限が異なる認証情報を生成して、ゲームクライアント３４０に送信する。

【００７１】

図６Ａ及び図６Ｂは、本実施形態のゲーム起動方法におけるユーザ端末３００の処理遷移を示したフローチャートである。

【００７２】

ユーザ端末３００のブラウザ３３０は、ユーザ操作に基づいてゲームサービスサイトであるオンラインサービス提供サーバ１００にアクセスし、オンラインサービス提供サーバ１００から提供されるサービスログイン画面を表示する（ステップＳ６０１）。ユーザは、ユーザ端末３００のブラウザ３３０に表示されたサービスログイン画面に、予め登録されたユーザＩＤ及びパスワードを入力し、ログインボタン等が選択されると、ブラウザ３３０は、当該画面に入力されたユーザＩＤ及びパスワードをオンラインサービス提供サーバ１００に送信する（ステップＳ６０２）。

【００７３】

オンラインサービスへのログイン後、ブラウザ３３０は、オンラインサービス提供サーバ１００から提供されるゲーム選択画面を表示し（ステップＳ６０３）、ユーザは、ゲーム選択画面に表示されたゲームの中から所望するゲームを選択する。オンラインサービス提供サーバ１００は、このゲーム選択に応答してユーザ端末３００に選択したゲームのゲーム起動画面を提供する。ユーザによりゲーム起動が選択されると（ゲーム起動ボタンが押下されると）、ブラウザ３３０は、ユーザのゲーム起動アクションに基づいて、ユーザ端末３００に保存されているCookie情報を参照し、当該ユーザのログイン状態をチェックする。ブラウザ３３０は、Cookie情報のログイン状態を示す情報が認証ＯＫであると判別された場合、オンラインサービス提供サーバ１００にゲーム起動要求（起動されるゲームＩＤ、ユーザＩＤを含む）を送信する（ステップＳ６０４）。

【００７４】

ブラウザ３３０の第１認証制御部３３１は、ゲーム起動要求に対して認証管理サーバ４００から発行される第１認証情報（認証発行チケット）を受信すると（ステップＳ６０５）、ユーザ端末３００の装置固有のＰＣ識別情報を該端末装置から取得する（ステップＳ６０６）。そして、第１認証制御部３３１は、受信した第１認証情報及び取得したＰＣ識別情報を含む認証情報発行要求を生成して、認証管理サーバ４００に送信する（ステップＳ６０７）。

【００７５】

ユーザ端末３００のブラウザ３３０は、認証管理サーバ４００で生成（発行）された第２認証情報を受信すると、当該受信に応答してゲームクライアント３４０を起動させ（ステップＳ６０８）、受信した第２認証情報、ユーザＩＤ、ゲームＩＤ等を当該ゲームクラ

イアント３４０に受け渡す（ステップＳ６０９）。ゲームクライアント３４０は、ブラウザ３３０と同様に、改めて個別にユーザ端末３００のＰＣ識別情報を取得し（ステップＳ６１０）、受け取った第２認証情報、ユーザＩＤ、ゲームＩＤ、ＰＣ識別情報等を含むゲーム接続要求を生成してゲームサーバ２００に送信する（ステップＳ６１１）。

【００７６】

ゲームクライアント３４０は、ゲームサーバ２００からのゲームセッション確立処理に応答して、ゲームサーバ２００との間のゲームセッションを確立し、ゲームクライアント３４０のゲーム処理部３４１は、ゲームサーバ２００のゲーム制御部２２０のゲーム制御に基づいてユーザ端末３００側でのゲーム処理を遂行する（ステップＳ６１１）。このとき、ゲームクライアント３４０は、ゲームサーバ２００から第３認証情報を受信し（ステップＳ６１２）、第３認証情報の認証有効期限の更新処理を開始する。ゲームクライアント３４０の第２認証制御部３４３は、受信した第３認証情報の認証有効期限と現在時刻とを比較チェックし、認証有効期限に対して所定の時間が経過したか否かを判別する（ステップＳ６１３）。そして、判別の結果、更新が必要であると判別された場合には、第３認証情報の認証有効期限の更新要求を認証管理サーバ４００に送信する（ステップＳ６１４）。その後、認証管理サーバ４００から認証有効期限が更新された第３認証情報を受信し（ステップＳ６１５）、第３認証情報を含む所定の処理要求を所定の処理を行うサーバに送信するまで、ステップＳ６１３からステップＳ６１５を繰り返し遂行し（ステップＳ６１６）、第３認証情報を含む処理要求が所定のサーバに送信する際に（ステップＳ６１７）、当該更新処理を終了する。

【００７７】

図７及び図８は、本実施形態の認証管理サーバ４００の処理遷移を示すフローチャートである。

【００７８】

認証管理サーバ４００の認証部４３０は、サービスログイン認証に伴ってオンラインサービス提供サーバ１００から送信される第１認証情報の発行要求、言い換えれば、ユーザ端末３００からのゲーム起動要求の受信有無を判別し（ステップＳ７０１）、ゲーム起動要求を受信したと判別した場合に、認証情報生成部４２０に第１認証情報の生成処理を指示する。

【００７９】

認証情報生成部４２０は、認証有効期限を含む第１認証情報を生成するとともに、生成した第１認証情報、発行要求（ゲーム起動要求）に含まれるゲームＩＤ、認証有効期限情報等をユーザＩＤと関連付けて認証ＤＢ５００の第１認証情報テーブルに格納する。また、生成された第１認証情報は、オンラインサービス提供サーバ１００を介してユーザ端末３００に送信される（ステップＳ７０２）。

【００８０】

次に、認証部４３０は、発行した第１認証情報及びユーザ端末３００のＰＣ識別情報を含む認証情報発行要求を受信すると（ステップＳ７０３）、受信した認証情報発行要求に含まれる第１認証情報を用いて認証ＤＢ５００を参照し、第１認証情報の一致性及び第１認証情報テーブルに格納されている認証有効期限と認証情報発行要求を受信したタイムスタンプを比較し、認証情報発行要求を受信したタイムスタンプが認証有効期限を越えているか否かを判別する第１認証処理を遂行する（ステップＳ７０４）。

【００８１】

認証部４３０は、第１認証処理の認証結果を判別し（ステップＳ７０５）、認証情報生成部４２０に第２認証情報の生成処理を指示する。認証情報生成部４４０は、第２認証情報を生成してユーザ端末３００に送信するとともに（ステップＳ７０７）、生成した第２認証情報、認証情報発行要求に含まれるＰＣ識別情報、認証有効期限情報等をユーザＩＤ毎に認証ＤＢ５００の第２認証情報テーブルに格納する（ステップＳ７０８）。一方、ステップＳ７０５において、第１認証処理の認証結果が認証ＮＧであると判別された場合、認証部４３０は、第２認証情報の生成指示を認証情報生成部４２０に出力せずに、ユーザ

端末３００に対して認証ＮＧである旨（ゲームサーバ２００に接続できない旨、サービス利用ができない旨等）のメッセージを送信する（ステップＳ７０６）。

【００８２】

その後、認証管理サーバ４００の認証部４３０は、ゲームサーバ２００からの第２認証情報を用いた認証要求の受信有無を判別し（ステップＳ８０１）、認証要求を受信したと判別した場合に、認証要求に含まれる第２認証情報及びＰＣ識別情報を用いた第２認証処理を遂行する（ステップＳ８０２）。認証ＤＢ５００の第２認証情報テーブルを参照して、受信した第２認証情報及びＰＣ識別情報の一致性の判別し、かつ第２認証情報テーブルに格納されている認証有効期限と認証情報発行要求を受信したタイムスタンプを比較して認証情報発行要求を受信したタイムスタンプが、認証有効期限を越えているか否かを判別する（ステップＳ８０３）。これら２つの認証を満足する場合に、第２認証情報を用いた認証処理が成功した（認証ＯＫ）と判断し、いずれか一方が満足されない場合には、認証処理が失敗した（認証ＮＧ）と判断する。認証部４３０は、認証ＯＫである場合、第２認証情報に基づく認証結果を生成し、認証情報生成部４２０に第３認証情報の生成指示を出力し、認証情報生成部４２０は、第２認証情報に基づいて第３認証情報を生成する（ステップＳ８０４）。そして、認証部４３０は、認証結果及び第３認証情報をゲームサーバ２００に送信する（ステップＳ８０５）。その後、認証部４３０は、第１認証情報又は／及び第２認証情報を用いた認証処理を終了する（ステップＳ８０８）。一方、ステップ８０３において、第２認証処理が認証ＮＧである場合、認証部４３０は、認証結果のみを生成し（ステップＳ８０６）、生成した認証結果をゲームサーバ２００に送信する（ステップＳ８０７）。

【００８３】

図９は、本実施形態のゲームサーバ２００の処理遷移を示すフローチャートである。

【００８４】

ゲームサーバ２００のゲーム制御部２２０は、ユーザ端末３００のゲームクライアント３４０からのゲーム接続要求があったか否かを判別し（ステップＳ９０１）、ゲーム接続要求があったと判別された場合、認証管理サーバ４００に対して受信したゲーム接続要求に含まれる第２認証情報、ＰＣ識別情報等を含む認証要求を送信する（ステップＳ９０２）。

【００８５】

ゲームサーバ２００のゲーム制御部２２０は、送信した認証要求に対する認証管理サーバ４００での認証結果を受信し（ステップＳ９０３）、認証結果を判別する（ステップＳ９０４）。認証結果が認証ＮＧであると判別された場合には、ゲームクライアント３４０との間のゲームセッション確立処理を遂行せずに、ユーザ端末３００に対して認証ＮＧである旨（サービス利用ができない旨等）のメッセージを送信する（ステップＳ９０５）。

【００８６】

一方、認証結果が認証ＯＫであると判別される場合には、ステップＳ９０３において認証結果とともに第３認証情報を受信し、認証ＯＫの認証結果に基づいてゲーム制御部２２０は、ゲームクライアント３４０との間のゲームセッション確立処理を遂行し、ゲーム制御を遂行するとともに、第３認証情報をゲームクライアント４３０に送信する（ステップＳ９０６）。なお、このゲーム制御部２２０によるゲーム制御についての説明は、省略する。

【００８７】

その後、ゲームサーバ２００のゲーム制御部２２０は、ユーザにより又はゲーム進行に応じてゲームが終了するまでゲーム制御を遂行し、ゲームが終了したと判別された場合に（ステップＳ９０７）、ゲーム終了処理（ゲームセッションの切断処理、ゲームデータの更新・格納等）を遂行してゲームを終了させる（ステップＳ９０８）。

【００８８】

このように本実施形態のゲームサービスシステムは、オンラインサービス提供サーバでのユーザログイン認証に基づいて発行される認証発行チケット（第１認証情報）により、

サービスログインせずにゲームサーバ２００に接続してゲームを不正に開始することを抑制できるとともに、ユーザログイン認証に使用されるユーザＩＤ及びパスワードと異なる第２認証情報によりゲームサービス（オンラインサービス）の提供を開始するための認証処理を遂行するので、パスワード等の詐取・盗難による不正なサービス利用を抑制することができる。

【００８９】

したがって、オンラインサービスのユーザ認証セキュリティが向上し、正当権限のあるユーザによる安全なオンラインサービスの提供が実現される。

【００９０】

さらに、第２認証情報を用いた認証処理の際、ユーザ端末３００のＰＣ識別情報に基づくユーザ識別を行っているため、認証情報が詐取、盗難等された場合であっても、ユーザの正当性を好適に判別することができる。

【００９１】

つまり、ブラウザ３３０から認証管理サーバ４００に送信されるＰＣ固有情報と、ゲームクライアント３４０から認証管理サーバ４００に送信されるＰＣ固有情報とが、同一であることを保証する、言い換えれば、第２認証情報の認証情報発行要求を送信したユーザ端末３００と、ゲームサーバ２００にゲーム接続要求を送信したゲームクライアント３４０が設置されたユーザ端末３００との同一性を、ＰＣ識別情報により保証する。

【００９２】

したがって、サービスログインしたユーザ端末３００のブラウザ３３０とゲームクライアント３４０との間でユーザ端末３００のＰＣ識別情報が引き継がれることで、ユーザの同一性を保証しつつ、認証有効期限を有する第１認証情報及び第２認証情報を用いた認証処理を遂行するため、パスワード等の詐取、盗難による他のユーザによるサービス不正利用を好適に抑制することができる。特に、ブラウザ３３０及びゲームクライアント３４０において個別にＰＣ識別情報を取得するように構成することで、よりユーザの同一性の高い認証を実現することが可能となる。

【００９３】

また、ゲーム開始後においても第２認証情報に基づく第３認証情報を用い、認証管理サーバ４００を通じた認証処理が遂行されるため、ゲームサービスに含まれる全ての処理において、パスワード等の詐取・盗難による不正なサービス利用を好適に抑制することができる。

【００９４】

（第２実施形態）

図１０は、本発明の第２実施形態におけるオンラインサービスシステムの構成図である。本実施形態のオンラインサービスシステムは、上記第１実施形態に対して、ゲームクライアント３４０やその他のユーザ端末３００にゲームを提供するに際し、必要な情報を格納するゲームデータ提供サーバ（ダウンロードサーバ）７００を有している。

【００９５】

通常、ゲームサービスシステムでは、ゲームクライアント３４０をユーザ端末３００にダウンロードさせ、ゲームクライアント３４０により所定のゲーム画面の表示、操作制御等のゲーム処理が遂行される。このため、ゲームサービスシステムにおいて初めてゲームを行う場合は、ユーザ端末３００は、ゲームクライアント３４０をゲームデータ提供サーバ７００からダウンロードする必要がある。また、初めて行う場合でなくとも、ゲームプログラムが更新されたり、新しいゲームシナリオ、表示画像、アイテム等が追加された場合は、ゲームを起動させる際にこれら更新データをユーザ端末３００にダウンロードさせて、ゲームクライアント３４０のゲームデータ格納部３４２に格納されるゲームデータを最新の状態にする必要がある。

【００９６】

一方、データのダウンロードは、ダウンロードするデータ容量及び通信性能に応じてユーザ端末３００毎に異なる。したがって、上記第１実施形態のように認証情報に認証有効

期限情報などの時間制限がある場合、認証情報が発行された時点からゲームクライアント３４０がゲームサーバ２００にゲーム接続要求するまでに必要な時間が、データの取得時間（ダウンロード時間）により長くなり、正当なユーザによるゲーム接続要求であっても、認証有効期限が超過することにより第２認証情報の有効性が消失し、ユーザ端末３００は、ゲームサービスを利用することができない。

【００９７】

そこで、本実施形態のユーザ端末３００は、図１１に示すように、第３認証制御部３４３ａを含む情報取得制御部３４０ａが設けられ、認証管理サーバ４００に格納されている第２認証情報の認証有効期限を更新する。なお、上記第１実施形態と同様の構成等については、同符号を付して説明を省略するとともに、上記第１実施形態と相違する部分を中心に本実施形態のゲームサービスシステムを説明する。

【００９８】

本実施形態のゲームサービスシステムは、オンラインサービスサイトであるオンラインサービス提供サーバ１００、オンラインサービスにおけるユーザの認証管理を行う認証管理サーバ４００、オンラインサービス提供サービスを提供するサービスサーバとしてのゲームサーバ２００、及びゲームサービスを利用するために必要な情報を格納し、ユーザ端末３００にゲームデータ等を提供するゲームデータ提供サーバ７００を備える。

【００９９】

ゲームデータ提供サーバ７００は、ネットワークＮを介した複数のユーザ端末３００との通信制御を行う通信制御部７１０、ゲームデータ格納部７３０に格納されたゲームデータをユーザ端末３００に提供する提供制御部７２０と、ゲームデータ提供サーバ７００全体の制御を司る制御部（ＣＰＵ）７４０を含む。

【０１００】

ゲームデータ格納部７３０には、ゲームＩＤ毎にゲームクライアント３４０、更新プログラム、新しいゲームシナリオ、表示画像、アイテム等のゲームデータが格納されている。ゲームデータ提供サーバ７００は、更新プログラムや新しいアイテム等の更新追加情報（更新追加リスト）をゲームＩＤ毎に保存（記憶）しており、ユーザ端末３００からのゲームＩＤを含むゲームデータ取得要求に応答して、対応する更新プログラム等をユーザ端末３００に提供する。

【０１０１】

ユーザ端末３００の情報取得部３４０ａは、ブラウザ３００により起動（実行）され、ゲームデータ提供サーバ７００にアクセスし、ゲームデータ取得要求をゲームデータ提供サーバ７００に送信する。また、情報取得制御部３４０ａの第３認証制御部３４３ａは、認証管理サーバ４００に第２認証情報の認証有効期限の更新要求を送信する。

【０１０２】

ここで、図１２を参照しながら、本実施形態のゲームサービスシステムのサービス提供方法（サービス起動方法）について詳細に説明する。

【０１０３】

認証管理サーバ４００で生成された第２認証情報は、ユーザ端末３００に提供され、第２認証情報を受信したブラウザ３３０は、情報取得制御部３４０ａを起動する。この情報取得制御部３４０ａは、例えば、ゲームランチャが適用される。そして、ブラウザ３３０は、第２認証情報を情報取得制御部３４０ａに受け渡すとともに、ゲームデータの取得指示を出力する。当該情報取得制御部３４０ａには、ブラウザ３３０から第２認証情報、ゲームＩＤ、ユーザＩＤが受け渡される。

【０１０４】

情報取得制御部３４０ａは、ゲームデータ提供サーバ７００にネットワークＮを通じて接続するために、該ゲームデータ提供サーバ７００との間の通信セッションを確立し、ゲームＩＤを含むゲームデータ取得要求をゲームデータ提供サーバ７００に送信する。ゲームデータ提供サーバ７００は、受信したゲームデータ取得要求に含まれるゲームＩＤに基づいて、対応するゲームデータをユーザ端末３００に提供する。

【０１０５】
このとき、情報取得制御部３４０ａの第３認証制御部３４３ａは、上記第１実施形態と同様に、ブラウザ３３０から取得した第２認証情報の認証有効期限と現在時刻とを比較チェックし、認証有効期限に対して所定の時間が経過したか否かを判別し、第３認証情報の認証有効期限の更新要求（認証有効期限を延長する旨の更新要求）を認証管理サーバ４００に送信する。この更新要求には、ブラウザ３３０から受け取った第２認証情報及び当該第３認証制御部３４３ａにおいて改めて個別に取得した当該ユーザ端末３００のＰＣ識別情報が含まれ、認証管理サーバ４００は、第２認証情報及びＰＣ識別情報を用いて認証処理を遂行し、認証結果がＯＫである場合に、予め設定された延長時間を現在の認証有効期限情報に加算したり、別途新たな認証有効期限を設定する更新処理を遂行する。

【０１０６】
なお、第３認証制御部３４３ａの第２認証情報の認証有効期限の更新判別処理及び更新要求処理は、ゲームデータ提供サーバ７００から所定のゲームデータをダウンロードしている間、繰り返し行い、その都度、認証管理サーバ４００に更新要求を送信する。このように構成することで、ユーザ端末３００の通信状態の変化に対して適切な認証有効期限の更新を行うことができる。また、通信状態の変化を考慮して通信状態に応じた各々異なる認証有効期限の更新を行うことも可能である。

【０１０７】
情報取得制御部３４０ａは、ゲームデータ提供サーバ７００からのデータ取得が完了した後に、ゲームクライアント３４０に起動指示を出力するとともに、保持していた第２認証情報を当該ゲームクライアント３４０に受け渡す。そして、ゲームクライアント３４０は、情報取得制御部３４０ａから受け取った第２認証情報とブラウザ３３０及び情報取得制御部３４０ａと同様に、改めて個別に取得したユーザ端末３００のＰＣ識別情報を含むゲーム接続要求をゲームサーバ２００に送信し、ゲームサーバ２００との間で確立したゲームセッションを通じてゲーム処理を遂行する。

【０１０８】
次に、図１３及び図１４を参照して、本実施形態のゲームサービスシステムのサービス提供方法の処理遷移について説明する。

【０１０９】
第２認証情報を受信したブラウザ３３０は、情報取得制御部３４０ａを起動して当該情報取得制御部３４０ａに対してゲームデータの取得指示を出力するとともに、当該情報取得制御部３４０ａに対して受信した第２認証情報、ゲームＩＤ、ユーザＩＤを出力する。情報取得制御部３４０ａは、ゲームＩＤを含むゲームデータ取得要求をゲームデータ提供サーバ７００に送信する（ステップＳ３０４ａ）。ゲームデータ提供サーバ７００は、ネットワークＮを通じて接続するために、ユーザ端末３００との間の通信セッションを確立し、受信したゲームデータ取得要求に含まれるゲームＩＤに基づいて、対応するゲームデータをユーザ端末３００に提供するダウンロード処理を開始する（ステップＳ５０１）。

【０１１０】
そして、情報取得制御部３４０ａの第３認証制御部３４３ａは、第２認証情報の認証有効期限と現在時刻とを比較チェックし、認証有効期限に対して所定の時間が経過したか否かを判別し（ステップＳ３０４ｂ）、所定の時間が経過したと判別された場合に、ユーザ端末３００のＰＣ識別情報を改めて取得し、認証管理サーバ４００に対して第２認証情報の認証有効期限を延長するための更新要求を送信する（ステップＳ３０４ｃ）。この更新要求には、ブラウザ３３０から受け取った第２認証情報及び改めて取得したＰＣ識別情報が含まれ、認証管理サーバ４００は、第２認証情報及びＰＣ識別情報を用いて認証処理を遂行し、認証結果がＯＫである場合に、認証有効期限を延長する有効期限更新処理を遂行する（ステップＳ４０５ａ）。その後、認証管理サーバ４００は、更新された第２認証情報をゲームクライアント３４０に送信し（ステップＳ４０５ｂ）、情報取得制御部３４０ａは、ゲームデータ提供サーバ７００からのデータ取得が完了した後に、ゲームクライアント３４０に起動指示を出力するとともに、更新された第２認証情報を当該ゲームクライ

アント３４０に受け渡す。

【０１１１】

図１５は、本実施形態の情報取得制御部３４０ａ及び第３認証制御部３４３ａの処理遷移を示すフローチャートであり、図６Ａのステップ６０８及びステップＳ６０９に対応している。

【０１１２】

ユーザ端末３００のブラウザ３３０は、認証管理サーバ４００で生成（発行）された第２認証情報を受信すると、情報取得制御部３４０ａを起動させるとともに、当該情報取得制御部３４０ａにゲームデータ取得指示を出力する。そして、受信した第２認証情報、ユーザＩＤ、ゲームＩＤ等を当該情報取得制御部３４０ａに受け渡す（ステップＳ１５０１）。

【０１１３】

情報取得制御部３４０ａは、ゲームデータ提供サーバ７００からのデータダウンロード処理を開始する（ステップＳ１５０２）。情報取得制御部３４０ａは、ゲームＩＤを含むゲームデータ取得要求をゲームデータ提供サーバ７００に送信し、ゲームデータ提供サーバ７００は、ネットワークＮを通じて接続するために、ユーザ端末３００との間の通信セッションを確立し、受信したゲームデータ取得要求に含まれるゲームＩＤに基づいて、対応するゲームデータをユーザ端末３００に提供するダウンロード処理を開始する。

【０１１４】

そして、情報取得制御部３４０ａは、第２認証情報の認証有効期限と現在時刻とに基づいて認証有効期限に対して所定の時間が経過したか否かを判別し（ステップＳ１５０３）、所定の時間が経過したと判別された場合に、ユーザ端末３００のＰＣ識別情報を取得し（ステップＳ１５０４）、認証管理サーバ４００に対して第２認証情報の認証有効期限を延長する旨の更新要求を送信し（ステップＳ１５０５）、認証有効期限が更新された第２認証情報を認証管理サーバ４００から受信する（ステップＳ１５０６）。その後、情報取得制御部３４０ａは、ゲームデータ提供サーバ７００からのデータ取得が完了したか否かを判別し（ステップＳ１５０７）、ダウンロード処理が完了していない場合は、ステップＳ１５０３に戻り、認証有効期限の更新判別処理及び更新要求処理を繰り返し行う。一方、ステップＳ１５０７において、ダウンロード処理が完了されたと判別された場合には、情報取得制御部３４０ａは、ゲームクライアント３４０に起動指示を出力するとともに（ステップＳ１５０８）、更新された第２認証情報を当該ゲームクライアント３４０に受け渡す（ステップＳ１５０９）。

【０１１５】

図１６は、本実施形態の認証管理サーバ４００の認証有効期限情報の更新処理を示したフローチャートであり、図７及び図８のステップ７０９及びステップＳ８０１の間で遂行される。

【０１１６】

認証管理サーバ４００は、第２認証情報の認証有効期限を延長するための更新要求をユーザ端末３００から受信したか否かを判別し（ステップＳ１６０１）、受信したと判別された場合は、認証部４３０は、該更新要求に含まれる第２認証情報及びＰＣ識別情報に基づいて認証処理を遂行する。この認証処理において、認証結果が認証ＮＧの場合は、ユーザ端末３００にゲームサービスを利用できない旨等のメッセージを送信し、当該更新処理を終了する。

【０１１７】

一方、第２認証情報及びＰＣ識別情報に基づいた認証処理の結果が認証ＯＫである場合に、認証情報生成部４２０は、予め設定された延長時間等に基づいて第２認証情報テーブルの対応する認証有効期限を更新する（ステップＳ１６０２，Ｓ１６０３）。

【０１１８】

このように本実施形態では、ゲームサービスを利用するために必要な情報を取得する場合においても、認証情報の認証有効期限を適宜更新するため、ゲームサービスを好適に提

供することが可能となる。

【０１１９】

また、ブラウザ３３０、情報取得制御部３４０ａは、及びゲームクライアント３４０の各モジュールにおいて個別に取得されたＰＣ識別情報を用いた認証処理が遂行されるため、よりユーザの同一性の高い認証を実現することが可能となる。

【０１２０】

以上、本発明を好適な実施形態を一例に説明したが、本発明は、ゲームサービスシステム以外にも、音楽提供サービスやアバター提供サービス等に適用することが可能である。例えば、アバター提供サービスにおいてユーザがサービスにログインした後に、アバターアイテム（洋服等）を購入する場合に、アイテム購入のための課金サーバにユーザ端末３００が接続する際に、本発明のサービス提供方法を適用して、ユーザの正当性を保証した安全なサービス提供を実現することができる。また、音楽提供サービスにおいても、音楽データのダウンロードサーバ等に接続する際、第２認証情報を用いた認証処理を適用することができる。

【０１２１】

なお、アバター提供サービスや音楽提供サービスの場合、ゲームクライアント等のサービスアプリケーションを別途ユーザ端末３００に設置する必要がない場合がある。この場合、本発明のサービス提供方法は、ブラウザの第１認証制御部３３１が、上記実施形態の第２認証制御部３４３の機能を備えるように構成し、サービスサーバ（課金サーバやダウンロードサーバ）が認証管理サーバ４００を通じて第２認証情報を用いた認証処理を遂行するように構成することができる。つまり、ゲームクライアント等のユーザ端末３００に設置されるサービスアプリケーションを介さずに、ブラウザのみで本発明のユーザ端末３００側の処理を遂行するように構成することができる。

【０１２２】

また、本発明のサービス提供方法は、基本的にゲームクライアントをインストールせずにゲームが遂行されるＦｌａｓｈ（登録商標）ゲームにも適用することが可能である。この場合、ＦｌａｓｈＰｌａｙｅｒ（ＳＷＦファイル）が第２認証制御部３４３の機能を担うように構成される。

【０１２３】

また、上記実施形態におけるゲームサービスシステムは、上述のように第１認証制御部３３１をブラウザ３３０にプラグインされるＡｃｔｉｖｅＸコントロール等のプログラムモジュールでユーザ端末３００に提供し、ゲームクライアント３４０をサービスアプリケーションプログラムとしてユーザ端末３００に提供する。ユーザ端末３００は、記憶部３５０に展開された各プログラムを読み込むことで、上記実施形態のユーザ端末３００での機能を実現させることができる。また、これらの各プログラムは、コンピュータ読取可能な記録媒体に記録された状態で、又はインターネット等のネットワークＮを通じてユーザ端末３００に提供される。コンピュータ読取可能な記録媒体としては、ＣＤ－ＲＯＭ等の光ディスク、ＤＶＤ－ＲＯＭ等の相変化型光ディスク、ＭＯ（Ｍａｇｎｅｔ　Ｏｐｔｉｃａｌ）やＭＤ（Ｍｉｎｉ　Ｄｉｓｋ）などの光磁気ディスク、フロッピー（登録商標）ディスクやリムーバブルハードディスクなどの磁気ディスク、コンパクトフラッシュ（登録商標）、スマートメディア、ＳＤメモリカード、メモリスティック等のメモリカードが挙げられる。

【０１２４】

また、上記実施形態における各サーバは、ハードウェア構成として上述以外にも、キーボード、マウス、スキャナー等の操作入力手段、液晶ディスプレイ等の表示手段、プリンタ、スピーカなどの出力手段、主記憶装置（メモリ）、補助記憶装置（ハードディスク等）等を備えることが可能であり、ユーザ端末においてもこれらの手段を備えることができる。各手段に制御は、サーバ又はコンピュータ全体の制御を司る制御手段（ＣＰＵ）により遂行される。

【０１２５】

なお、本発明の詳細な説明では具体的な実施形態について説明したが、本発明の要旨から逸脱しない範囲内で多様に変形できる。よって、本発明の範囲は、上述の実施形態に限定されるものではなく、特許請求の範囲の記載及びこれと均等なものに基づいて定められるべきである。

【図面の簡単な説明】

【０１２６】

【図１】本発明の第１実施形態におけるオンラインサービスシステムの構成図であり、各サーバの構成ブロック図を示す図である。

【図２】本発明の第１実施形態におけるユーザ端末の構成ブロック図である。

【図３】本発明の第１実施形態におけるサービス提供方法を示す図である。

【図４】本発明の第１実施形態における認証ＤＢの各テーブルの一例を示す図である。

【図５Ａ】本発明の第１実施形態におけるオンラインシステムの処理遷移を示すフローチャートである。

【図５Ｂ】図５Ａに続く本発明の第１実施形態におけるオンラインシステムの処理遷移を示すフローチャートである。

【図６Ａ】本発明の第１実施形態におけるユーザ端末の処理遷移を示すフローチャートである。

【図６Ｂ】図６Ａに続く本発明の第１実施形態におけるユーザ端末の処理遷移を示すフローチャートである。

【図７】本発明の第１実施形態における認証管理サーバの処理遷移を示すフローチャートである。

【図８】図７に続く本発明の第１実施形態における認証管理サーバの処理遷移を示すフローチャートである。

【図９】本発明の第１実施形態におけるゲームサーバの処理遷移を示すフローチャートである。

【図１０】本発明の第２実施形態におけるオンラインサービスシステムの構成図であり、ゲームデータ提供サーバの構成ブロック図を示す図である。

【図１１】本発明の第２実施形態におけるユーザ端末の構成ブロック図である。

【図１２】本発明の第２実施形態におけるサービス提供方法を示す図である。

【図１３】本発明の第２実施形態におけるオンラインサービスシステムの処理遷移を示すフローチャートである。

【図１４】図１３に続く本発明の第２実施形態におけるオンラインサービスシステムの処理遷移を示すフローチャートである。

【図１５】本発明の第２実施形態におけるユーザ端末の処理遷移を示すフローチャートである。

【図１６】本発明の第２実施形態における認証管理サーバの処理遷移を示すフローチャートである。

【図１７】従来のゲームサービスにおけるゲームサービス提供方法を示す図である。

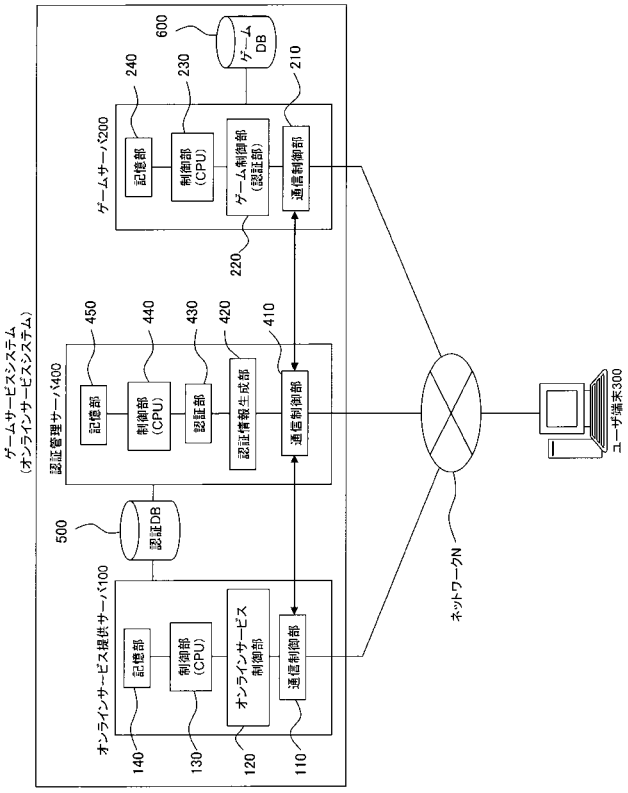
【符号の説明】

【０１２７】

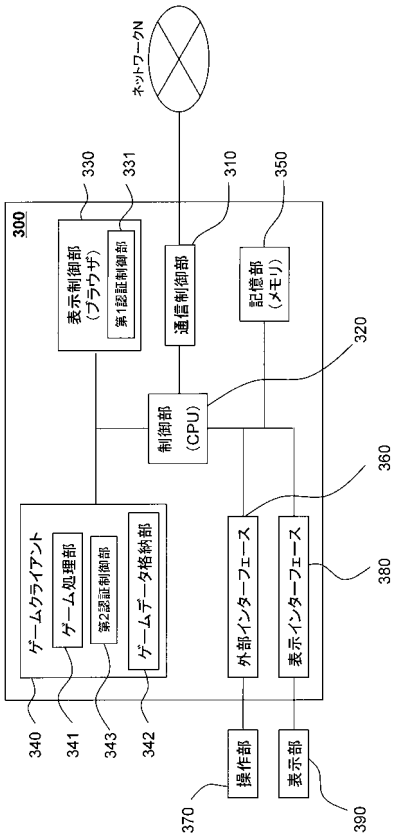
１００　オンラインサービス提供サーバ
１１０　通信制御部
１２０　オンラインサービス制御部
１３０　制御部（ＣＰＵ）
１４０　記憶部
２００　ゲームサーバ
２１０　通信制御部
２２０　ゲーム制御部
２３０　制御部（ＣＰＵ）
２４０　記憶部

３００　ユーザ端末
３１０　通信制御部
３２０　制御部（ＣＰＵ）
３３０　表示制御部（ブラウザ）
３３１　第１認証制御部
３４０　ゲームクライアント（サービスアプリケーション）
３４０ａ　情報取得制御部
３４１　ゲーム処理部
３４２　ゲームデータ格納部
３４３　第２認証制御部
３４３ａ　第３認証制御部
３５０　記憶部（メモリ）
３６０　外部インターフェース
３７０　操作部
３８０　表示インターフェース
３９０　表示部
４００　認証管理サーバ
４１０　通信制御部
４２０　認証情報発行部
４３０　認証部
４４０　制御部（ＣＰＵ）
４５０　記憶部
５００　認証ＤＢ
６００　ゲームＤＢ
７００　ゲームデータ提供サーバ
７１０　通信制御部
７２０　提供制御部
７３０　ゲームデータ格納部
７４０　制御部（ＣＰＵ）

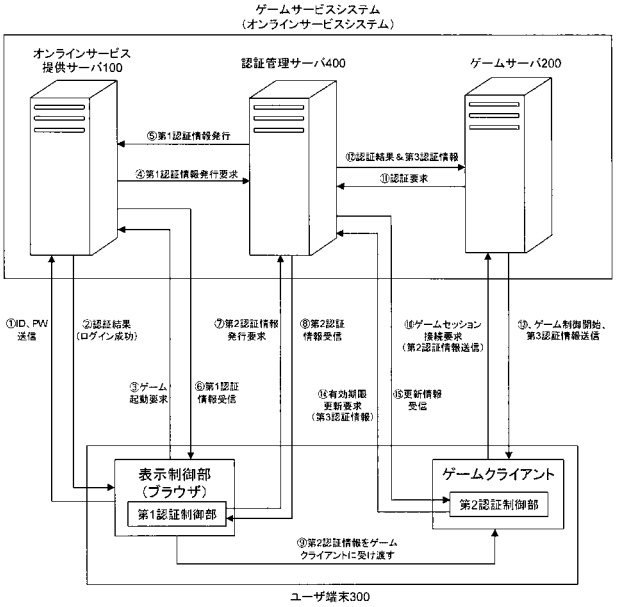
【図１】



【図２】



【図３】



【図４】

(a)

第1認証情報テーブル

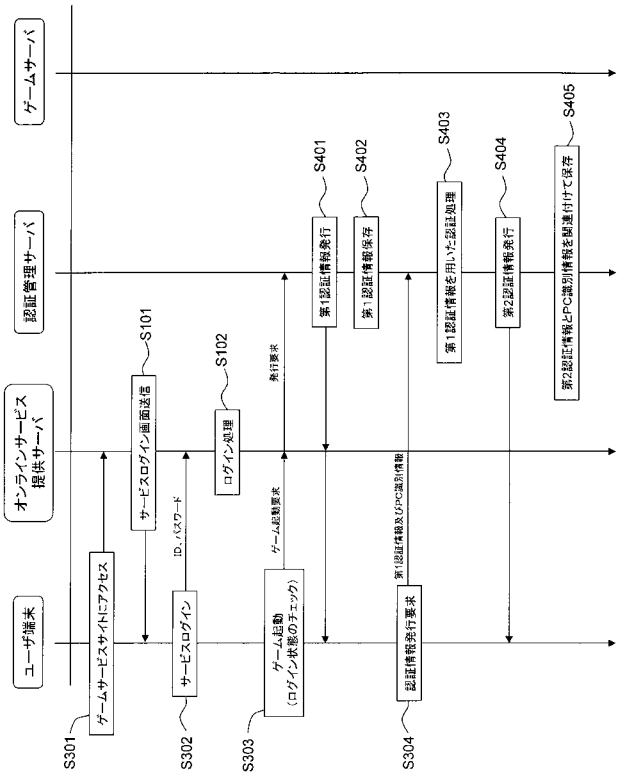
ユーザID	起動要求	ゲームID	第1認証情報	第1シーケンス番号	認証有効期限
A0001	2008/5/10 19:35	G0001	SI001+第1シーケンス番号	1	起動要求から1分以内
…	…	…	…	…	…

(b)

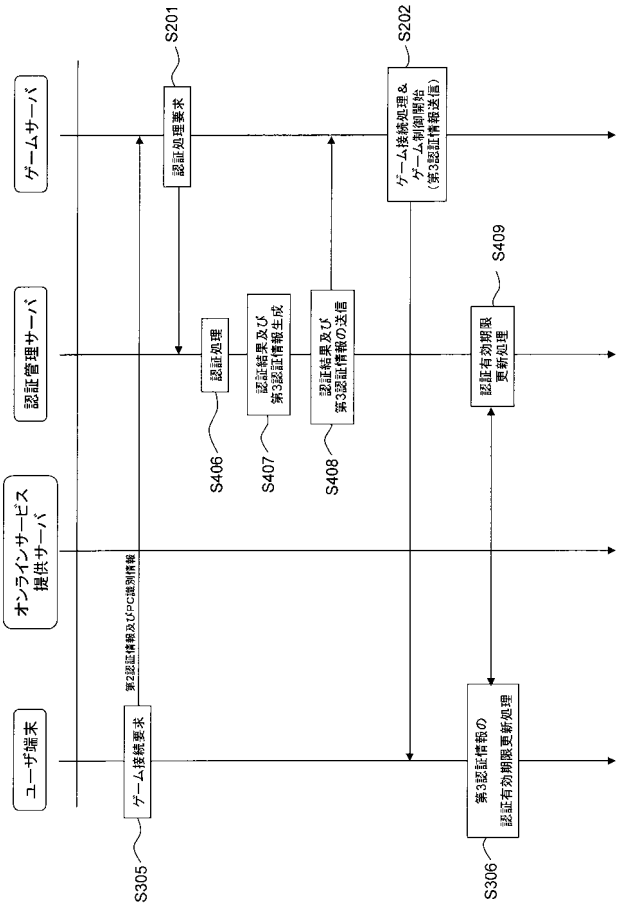
第2認証情報テーブル

ユーザID	発行要求	ゲームID	第1認証情報	PC識別情報	第2認証情報	第2シーケンス番号	認証有効期限
A0001	2008/5/10 19:36	G001	SI001_1	MACアドレス等	ゲームID+認証有効期限+PC識別情報+第2シーケンス番号	1	発行タイムスタンプ+5分以内
…	…	…	…	…	…	…	…

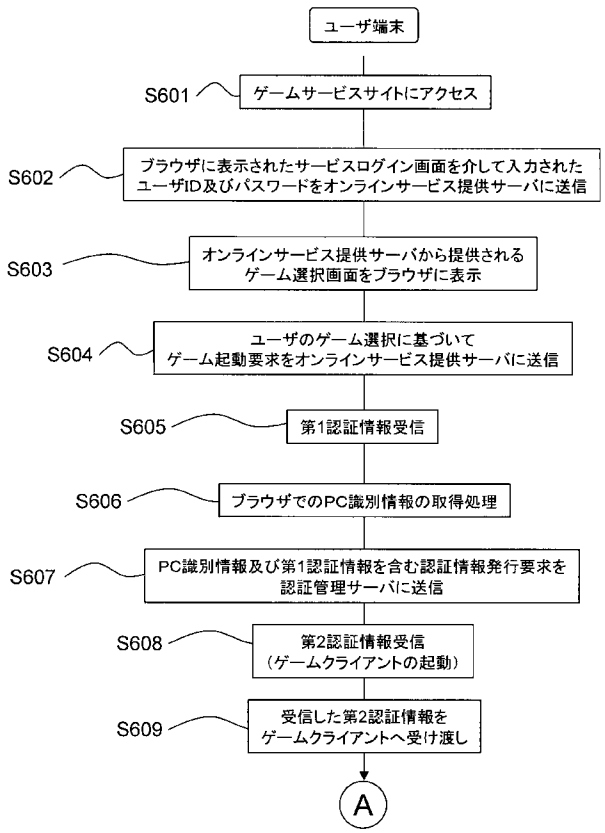
【図５Ａ】



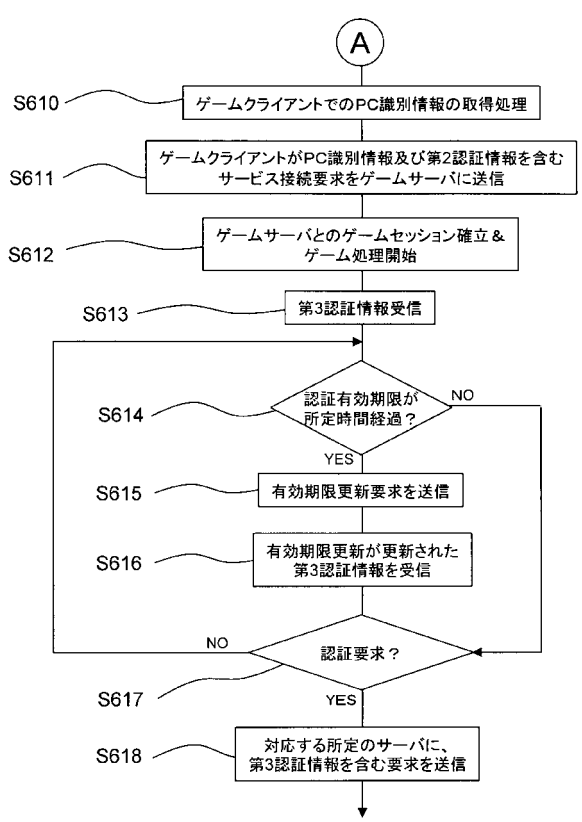
【図５Ｂ】



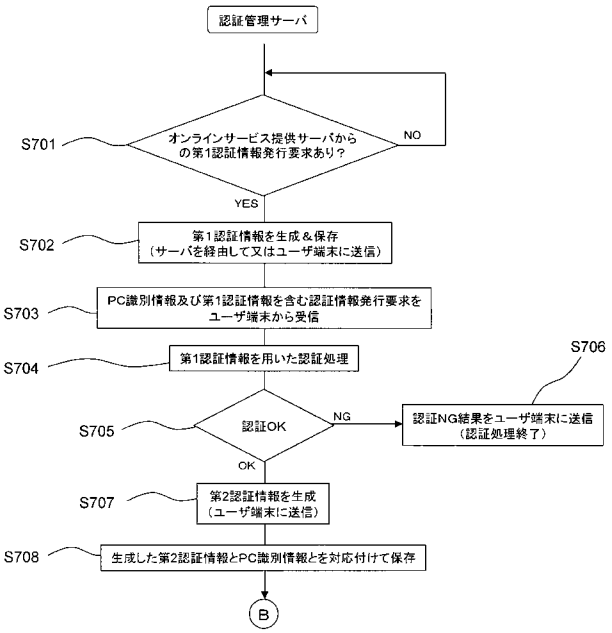
【図６Ａ】



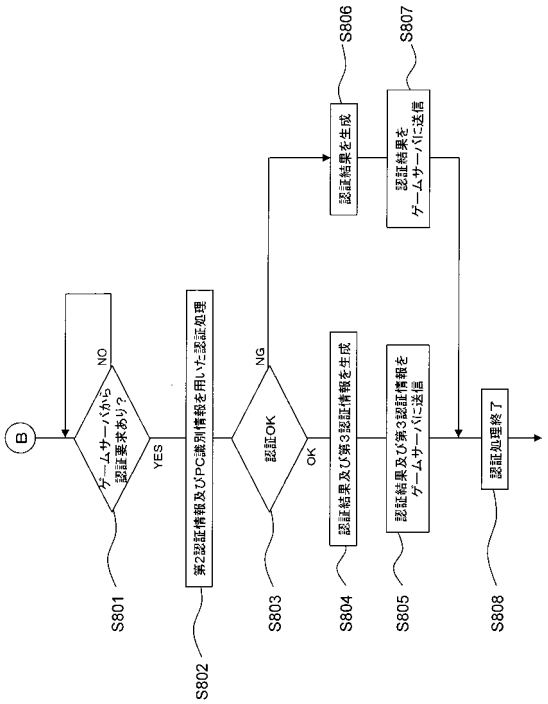
【図６Ｂ】



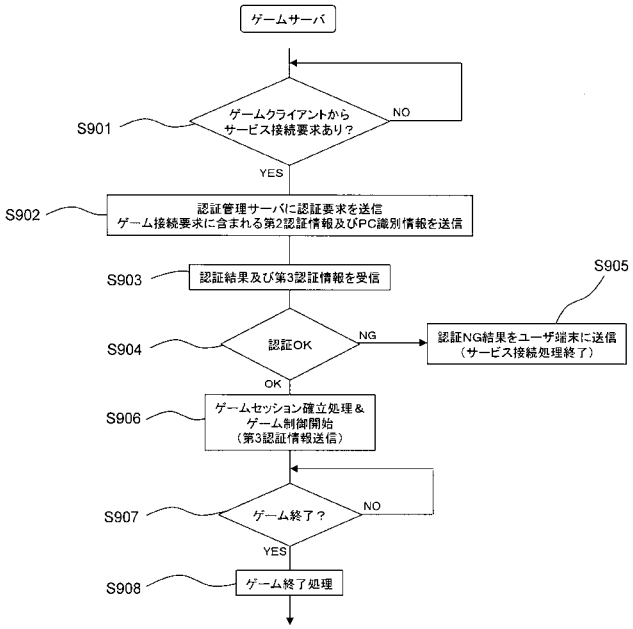
【図７】


認証管理サーバ
S701
オンラインサービス提供サーバから
の第1認証情報発行要求あり？
NO
YES
S702
第1認証情報を生成＆保存
（サーバを経由して又はユーザ端末に送信）
S703
PC識別情報及び第1認証情報を含む認証情報発行要求を
ユーザ端末から受信
S704
第1認証情報を用いた認証処理
S705
認証OK
NG
S706
認証NG結果をユーザ端末に送信
（認証処理終了）
OK
S707
第2認証情報を生成
（ユーザ端末に送信）
S708
生成した第2認証情報とPC識別情報とを対応付けて保存
B

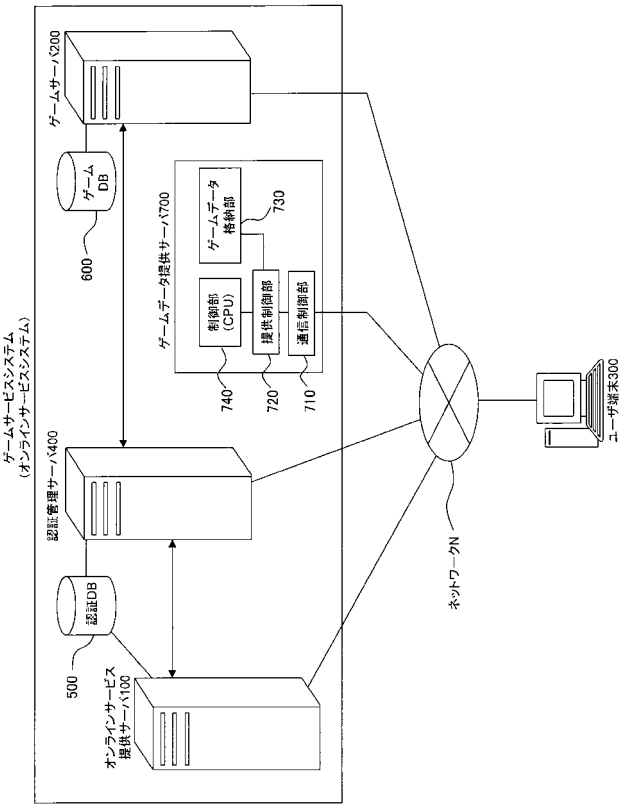
【図８】


S806
S807
認証結果を生成
認証結果を
ゲームサーバに送信
B
ゲームサーバから
認証要求あり？
NO
YES
第2認証情報及びPC識別情報を用いた認証処理
認証OK
NG
OK
認証結果及び第3認証情報を生成
認証結果及び第3認証情報を
ゲームサーバに送信
認証処理終了
S801
S802
S803
S804
S805
S808

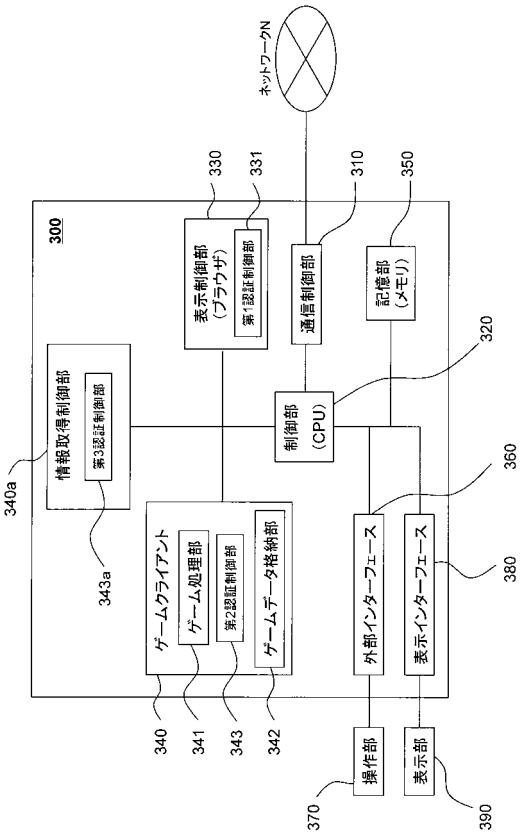
【図９】


ゲームサーバ
S901
ゲームクライアントから
サービス接続要求あり？
NO
YES
S902
認証管理サーバに認証要求を送信
ゲーム接続要求に含まれる第2認証情報及びPC識別情報を送信
S903
認証結果及び第3認証情報を受信
S905
S904
認証OK
NG
認証NG結果をユーザ端末に送信
（サービス接続処理終了）
OK
S906
ゲームセッション確立処理＆
ゲーム制御開始
（第3認証情報送信）
S907
ゲーム終了？
NO
YES
S908
ゲーム終了処理

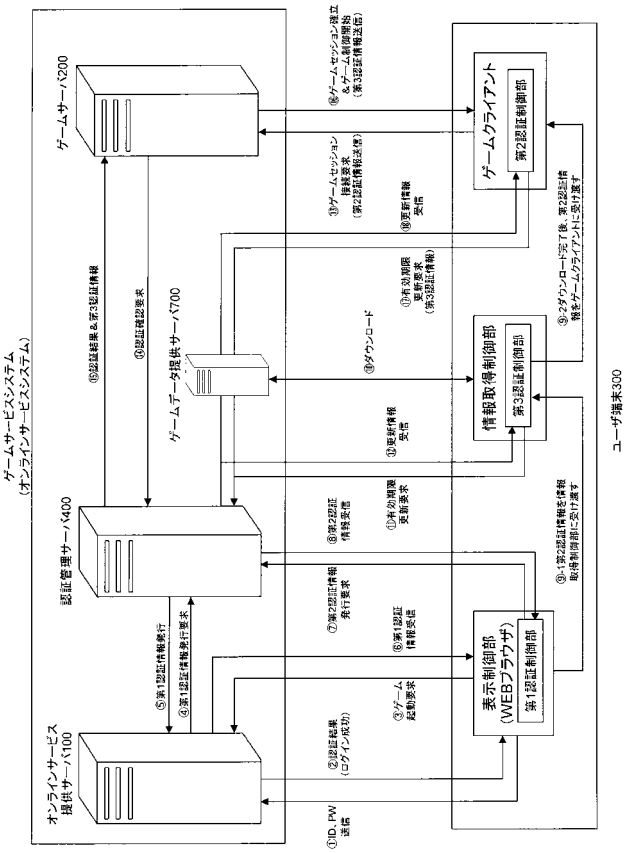
【図１０】


ゲームサービスシステム
（オンラインサービスシステム）
ゲームサーバ200
ゲーム
DB
600
ゲームデータ提供サーバ700
ゲームデータ
格納部
730
制御部
（CPU）
提供制御部
通信制御部
740
720
710
認証管理サーバ400
認証DB
500
オンラインサービス
提供サーバ100
ネットワークN
ユーザ端末300

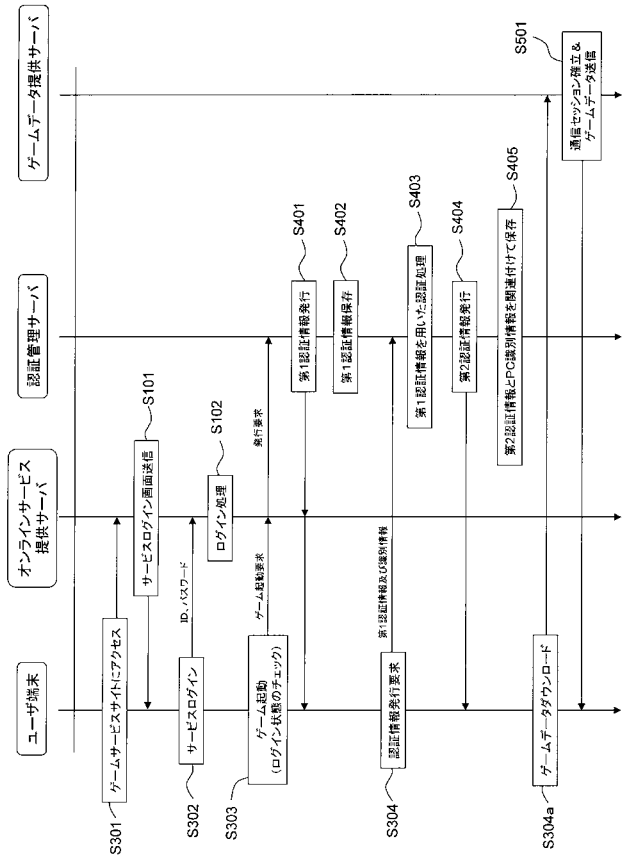
【図１１】



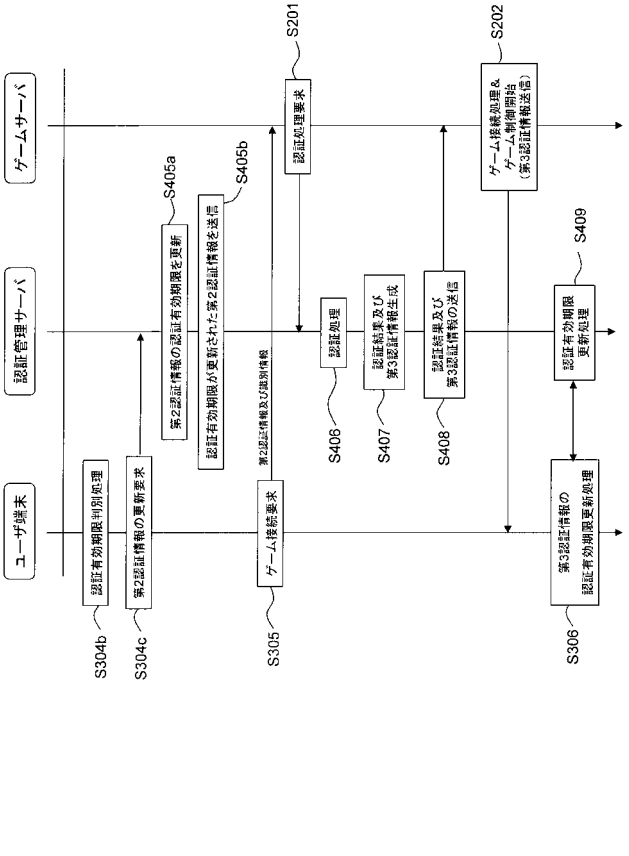
【図１２】



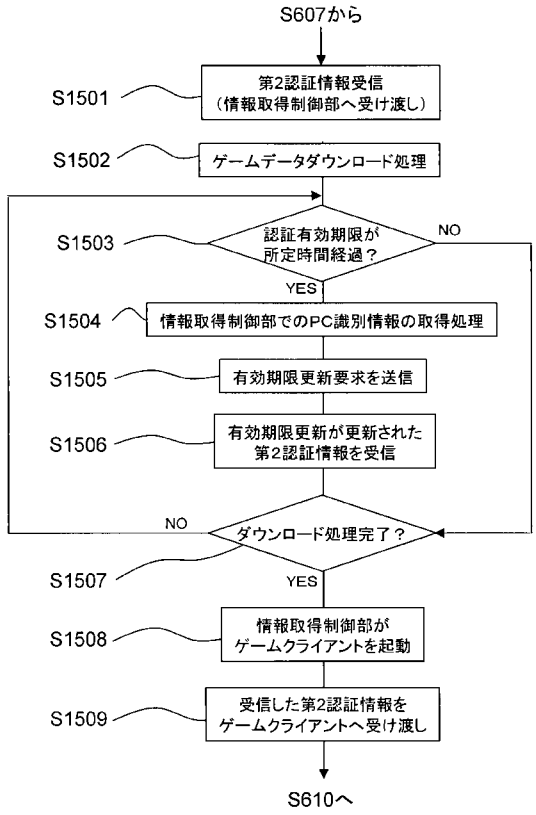
【図１３】



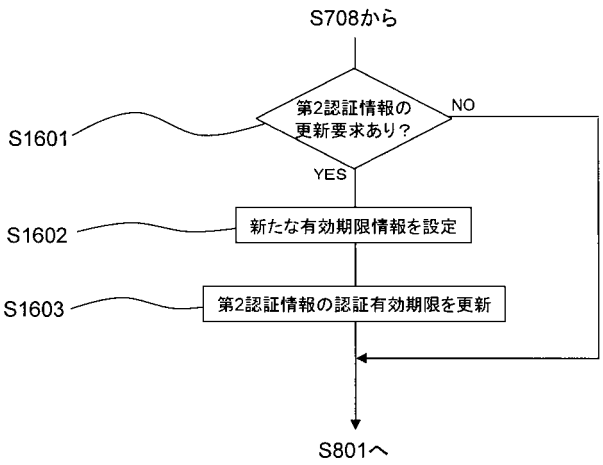
【図１４】



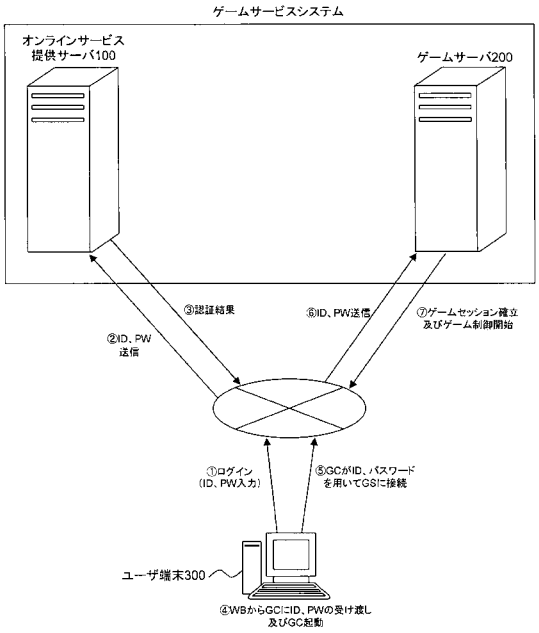
【図１５】


S607から
S1501
第2認証情報受信
（情報取得制御部へ受け渡し）
S1502
ゲームデータダウンロード処理
S1503
認証有効期限が
所定時間経過？
NO
YES
S1504
情報取得制御部でのPC識別情報の取得処理
S1505
有効期限更新要求を送信
S1506
有効期限更新が更新された
第2認証情報を受信
NO
ダウンロード処理完了？
S1507
YES
S1508
情報取得制御部が
ゲームクライアントを起動
S1509
受信した第2認証情報を
ゲームクライアントへ受け渡し
S610へ

【図１６】


S708から
S1601
第2認証情報の
更新要求あり？
NO
YES
S1602
新たな有効期限情報を設定
S1603
第2認証情報の認証有効期限を更新
S801へ

【図１７】


ゲームサービスシステム
オンラインサービス
提供サーバ100
ゲームサーバ200
③認証結果
⑥ID、PW送信
⑦ゲームセッション確立
及びゲーム制御開始
②ID、PW
送信
①ログイン
（ID、PW入力）
⑤GCがID、パスワード
を用いてGSに接続
ユーザ端末300
④WBからGCにID、PWの受け渡し
及びGC起動

フロントページの続き

(74)代理人　100105072
弁理士　小川　英宣
(72)発明者　イ・ジュンヨン
東京都品川区大崎２丁目１番１号　ＮＨＮＪａｐａｎ株式会社内
(72)発明者　宅間啓
東京都品川区大崎２丁目１番１号　ＮＨＮＪａｐａｎ株式会社内
(72)発明者　李燦宗
東京都品川区大崎２丁目１番１号　ＮＨＮＪａｐａｎ株式会社内
(72)発明者　金東燮
東京都品川区大崎２丁目１番１号　ＮＨＮＪａｐａｎ株式会社内
(72)発明者　申東權
東京都品川区大崎２丁目１番１号　ＮＨＮＪａｐａｎ株式会社内
(72)発明者　沈正載
東京都品川区大崎２丁目１番１号　ＮＨＮＪａｐａｎ株式会社内

Ｆターム(参考)　5B285 AA01 BA03 CB02 CB47 CB52 CB55 CB62 CB72 CB83 CB85
5J104 AA07 KA01 KA04 MA01 NA05 NA38 PA07