(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5296726号
(P5296726)
(45)発行日　平成25年9月25日(2013.9.25)　(24)登録日　平成25年6月21日(2013.6.21)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/20 131A
G06F 21/62 (2013.01)　　G06F 21/24 163A
G06F 13/00 (2006.01)　　G06F 13/00 510A

請求項の数 8　(全 22 頁)

(21)出願番号　特願2010-52197(P2010-52197)
(22)出願日　平成22年3月9日(2010.3.9)
(65)公開番号　特開2011-186849(P2011-186849A)
(43)公開日　平成23年9月22日(2011.9.22)
審査請求日　平成24年2月13日(2012.2.13)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100147485
弁理士　杉村　憲司
(72)発明者　村井　健二
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　福田　希子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　堀　正弘
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】Ｗｅｂコンテンツ提供システム、Ｗｅｂサーバ、コンテンツ提供方法、及びこれらのプログラム

(57)【特許請求の範囲】
【請求項１】
ネットワーク上のＷｅｂサイトを提供するＷｅｂサーバと、前記Ｗｅｂサーバとネットワークを通じてＷｅｂプロトコル経由で通信する第１Ｗｅｂクライアント端末及び第２Ｗｅｂクライアント端末とを備えるＷｅｂコンテンツ提供システムであって、
前記Ｗｅｂサーバは、
前記第１Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するリクエスト情報解析手段と、
当該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認して、該アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であるか否かを判断するアクセス制御手段と、
アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であると判断される場合に、当該リクエスト情報に係るＷｅｂコンテンツを提示するＷｅｂコンテンツ提供手段と、を備え、
前記アクセス制御手段は、前記照合の結果として一致した場合に、アクセス履歴情報データベースに記録されているアクセス履歴情報に、前記第１Ｗｅｂクライアント端末の利用者を特定するアクセス元識別情報が存在しているか否かを確認して存在していない場合

に、前記利用者を特定するアクセス元識別情報を前記セッション情報、前記第１Ｗｅｂクライアント端末を特定するユーザエージェント情報、当該Ｗｅｂサイトのコンテンツを特定するコンテンツ識別情報、前記認証情報の種別を識別する認証手段識別情報、及び当該セッションに係るアクセス日時情報とともにアクセス履歴情報として前記アクセス履歴情報データベースに記録するアクセス履歴管理手段を有し、

前記Ｗｅｂコンテンツ提供手段は、前記アクセス履歴情報の確認後に、当該リクエスト情報に係るＷｅｂコンテンツを提示する手段を有し、

前記リクエスト情報解析手段は、前記第２Ｗｅｂクライアント端末から前記所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合する手段を有し、

前記アクセス制御手段は、該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、前記アクセス制御ポリシーに定められるアクセス優先順位に従って当該Ｗｅｂサイトのコンテンツを利用可能であるか否かを判別して利用可能であると判別する場合に、前記アクセス履歴情報データベースに記録されているアクセス履歴情報から前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報を抽出する手段を有し、

前記Ｗｅｂコンテンツ提供手段は、前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報に対応するＷｅｂコンテンツを前記第２Ｗｅｂクライアント端末へ提示する手段を有することを特徴とする、Ｗｅｂコンテンツ提供システム。

【請求項２】

前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で、同一のＷｅｂコンテンツが提示されている際に、

前記リクエスト情報解析手段が、前記第１Ｗｅｂクライアント端末から当該Ｗｅｂコンテンツをログアウトするリクエスト情報を受信した場合、該リクエスト情報に含まれるアカウントＩＤと、前記アクセス履歴情報データベース内のアクセス履歴情報のアクセス元識別情報と照合する手段を有し、

前記アクセス履歴管理手段が、該照合結果として一致すると判断される場合には、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を削除する手段を有することを特徴とする、請求項１に記載のＷｅｂコンテンツ提供システム。

【請求項３】

前記アクセス履歴管理手段は、前記アクセス制御ポリシー情報のアクセス優先順位にて前記第１Ｗｅｂクライアント端末が最も優先されている場合に、前記第２Ｗｅｂクライアント端末からのログイン時のリクエスト情報に含まれるアカウントＩＤと同一のアカウントＩＤによるセッション情報が存在しているか否かに関わらず、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を削除する手段を有することを特徴とする、請求項２に記載のＷｅｂコンテンツ提供システム。

【請求項４】

前記アクセス制御ポリシー情報は、

アクセス元識別情報とアカウントＩＤが一致する場合、別ポリシーに該当しない限り、同一のＷｅｂコンテンツを前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で同期して提示しないとするポリシーと、

前記ユーザエージェント情報に基づく認証情報ごとのアクセス優先順位に、前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末が該当する場合に、同一のＷｅｂコンテンツを前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で同期して提示可能とするポリシーと、

前記ユーザエージェント情報に基づく認証情報ごとのＷｅｂコンテンツの内容として全部又は一部で提示可能とする、Ｗｅｂクライアント端末毎のアクセス優先順位によるコンテンツ利用可否制限に対して、前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末が該当する場合に、同一のＷｅｂコンテンツの全部又は一部を前記第１Ｗｅ

ｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で同期して提示可能とするポリシーと、を含むことを特徴とする、請求項１～３のいずれか一項に記載のＷｅｂコンテンツ提供システム。

【請求項５】

前記第１Ｗｅｂクライアント端末の認証情報は、前記第２Ｗｅｂクライアント端末の認証情報よりも高度の認証として、前記アクセス制御ポリシー情報に規定されていることを特徴とする、請求項１～４のいずれか一項に記載のＷｅｂコンテンツ提供システム。

【請求項６】

第１Ｗｅｂクライアント端末及び第２Ｗｅｂクライアント端末とＷｅｂプロトコル経由で通信してネットワーク上のＷｅｂサイトを提供するＷｅｂサーバであって、

前記第１Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するリクエスト情報解析手段と、

当該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認して、該アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であるか否かを判断するアクセス制御手段と、

アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であると判断される場合に、当該リクエスト情報に係るＷｅｂコンテンツを提示するＷｅｂコンテンツ提供手段と、を備え、

前記アクセス制御手段は、前記照合の結果として一致した場合に、アクセス履歴情報データベースに記録されているアクセス履歴情報に、前記第１Ｗｅｂクライアント端末の利用者を特定するアクセス元識別情報が存在しているか否かを確認して存在していない場合に、前記利用者を特定するアクセス元識別情報を前記セッション情報、前記第１Ｗｅｂクライアント端末を特定するユーザエージェント情報、当該Ｗｅｂサイトのコンテンツを特定するコンテンツ識別情報、前記認証情報の種別を識別する認証手段識別情報、及び当該セッションに係るアクセス日時情報とともにアクセス履歴情報として前記アクセス履歴情報データベースに記録するアクセス履歴管理手段を有し、

前記Ｗｅｂコンテンツ提供手段は、前記アクセス履歴情報の確認後に、当該リクエスト情報に係るＷｅｂコンテンツを提示する手段を有し、

前記リクエスト情報解析手段は、前記第２Ｗｅｂクライアント端末から前記所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合する手段を有し、

前記アクセス制御手段は、該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、前記アクセス制御ポリシーに定められるアクセス優先順位に従って当該Ｗｅｂサイトのコンテンツを利用可能であるか否かを判別して利用可能であると判別する場合に、前記アクセス履歴情報データベースに記録されているアクセス履歴情報から前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報を抽出する手段を有し、

前記Ｗｅｂコンテンツ提供手段は、前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報に対応するＷｅｂコンテンツを前記第２Ｗｅｂクライアント端末へ提示する手段を有することを特徴とする、Ｗｅｂサーバ。

【請求項７】

第１Ｗｅｂクライアント端末及び第２Ｗｅｂクライアント端末とＷｅｂプロトコル経由で通信してネットワーク上のＷｅｂサイトを提供するＷｅｂサーバによるコンテンツ提供方法であって、

前記Ｗｅｂサーバの処理手順は、

前記第１Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン

時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するステップと、
当該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認するとともに、アクセス履歴情報データベースに記録されているアクセス履歴情報に、前記第１Ｗｅｂクライアント端末の利用者を特定するアクセス元識別情報が存在しているか否かを確認して存在していない場合に、前記利用者を特定するアクセス元識別情報を前記セッション情報、前記第１Ｗｅｂクライアント端末を特定するユーザエージェント情報、当該Ｗｅｂサイトのコンテンツを特定するコンテンツ識別情報、前記認証情報の種別を識別する認証手段識別情報、及び当該セッションに係るアクセス日時情報とともにアクセス履歴情報として前記アクセス履歴情報データベースに記録するステップと、
前記アクセス履歴情報の確認後に、当該リクエスト情報に係るＷｅｂコンテンツを提示するステップと、
前記第２Ｗｅｂクライアント端末から前記所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するステップと、
該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、前記アクセス制御ポリシーに定められるアクセス優先順位に従って当該Ｗｅｂサイトのコンテンツを利用可能であるか否かを判別して利用可能であると判別する場合に、前記アクセス履歴情報データベースに記録されているアクセス履歴情報から前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報を抽出するステップと、
前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報に対応するＷｅｂコンテンツを前記第２Ｗｅｂクライアント端末へ提示するステップと、
を含むことを特徴とするコンテンツ提供方法。
【請求項８】
第１Ｗｅｂクライアント端末及び第２Ｗｅｂクライアント端末とＷｅｂプロトコル経由で通信してネットワーク上のＷｅｂサイトを提供するＷｅｂサーバとして構成するコンピュータに、
前記第１Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するステップと、
当該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認するとともに、アクセス履歴情報データベースに記録されているアクセス履歴情報に、前記第１Ｗｅｂクライアント端末の利用者を特定するアクセス元識別情報が存在しているか否かを確認して存在していない場合に、前記利用者を特定するアクセス元識別情報を前記セッション情報、前記第１Ｗｅｂクライアント端末を特定するユーザエージェント情報、当該Ｗｅｂサイトのコンテンツを特定するコンテンツ識別情報、前記認証情報の種別を識別する認証手段識別情報、及び当該セッションに係るアクセス日時情報とともにアクセス履歴情報として前記アクセス履歴情報データベースに記録するステップと、
前記アクセス履歴情報の確認後に、当該リクエスト情報に係るＷｅｂコンテンツを提示するステップと、
前記第２Ｗｅｂクライアント端末から前記所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するステップと、
該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、前記アクセス制御ポリシーに定められるアクセス

優先順位に従って当該Ｗｅｂサイトのコンテンツを利用可能であるか否かを判別して利用可能であると判別する場合に、前記アクセス履歴情報データベースに記録されているアクセス履歴情報から前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報を抽出するステップと、

前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報に対応するＷｅｂコンテンツを前記第２Ｗｅｂクライアント端末へ提示するステップと、

を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、或る利用者が複数のクライアント端末を用いてクライアント端末間でセッションを維持しながら、Ｗｅｂサーバにアクセスする際のアクセス制御技術に関し、特に、複数のＷｅｂクライアント端末間でセッションを継続したままコンテンツを提供するＷｅｂコンテンツ提供システム、Ｗｅｂサーバ、コンテンツ提供方法、及びこれらのプログラムに関する。

【背景技術】

【０００２】

利用者がその利用環境に応じて複数のＷｅｂクライアント端末を利用したい場合に、セッションを継続したままシームレスにＷｅｂクライアント端末間の切り替えを行い、この切り替えの際、Ｗｅｂサーバでは複数のＷｅｂクライアント端末間でのテンポラリーな認証情報によるセキュアな利用者認証を行う技術がある（例えば、特許文献１参照）。

【０００３】

また、複数のＷｅｂクライアント端末からのアクセスを制御する方法として、ＨＴＴＰによるリクエスト情報に含まれるログインＩＤを元に、Ｗｅｂサーバが、アクセス履歴情報等に識別情報を記録し、同一のログインＩＤを含む別のリクエストを拒否する、いわゆる２重ログインを防止する技術も知られている。更に、ＨＴＴＰによるリクエスト情報に含まれるユーザエージェント情報を、Ｗｅｂサーバが識別し、特定のユーザエージェントを拒否するアクセス制御技術も知られている。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００５－１２２６５１号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

複数のクライアント端末間におけるセッションを維持しながら、Ｗｅｂサーバにアクセスする、従来から知られているＷｅｂコンテンツ提供システムでは、例えば、或る利用者が、ＩＣカード認証のような比較的高度な認証手段を具備するＷｅｂクライアント端末（例えば、認証専用ＩＣチップを搭載した携帯電話機）を用いた場合でも、ＩＤ／パスワードのような比較的低度な認証手段を具備するＷｅｂクライアント端末（例えば、デジタルテレビ端末）を用いた場合でも、全く同じＷｅｂコンテンツを利用することになり、Ｗｅｂサーバ側で、Ｗｅｂクライアント端末のセッション状態やＷｅｂコンテンツの内容に応じた、複数のＷｅｂクライアント端末の各々に対する個別のアクセス制御を実現することができない。

【０００６】

換言すれば、従来から知られているＷｅｂコンテンツ提供システムでは、複数のＷｅｂクライアント端末間のセッション維持とＷｅｂコンテンツへのアクセス制御を、同一のＷｅｂサーバに対して同時に行うことができないので、利用者は、同一のＷｅｂサーバに対して、複数のＷｅｂクライアント端末の双方で利用可能な全く同じＷｅｂコンテンツのサービス提供しか受けることができない。

【０００７】
本発明の目的は、上述の問題に鑑みて為されたものであり、複数のＷｅｂクライアント端末間のセッション維持とＷｅｂコンテンツへのアクセス制御を、同一のＷｅｂサーバに対して同時に行うことを可能とする、Ｗｅｂクライアント端末間でセッションを継続したままコンテンツを提供するＷｅｂコンテンツ提供システム、Ｗｅｂクライアント端末、Ｗｅｂサーバ、コンテンツ提供方法、及びこれらのプログラムを提供することにある。
【課題を解決するための手段】
【０００８】
本発明のＷｅｂコンテンツ提供システムでは、Ｗｅｂサーバにおいて、予め設定登録したアクセス制御ポリシー情報に基づき、複数のＷｅｂクライアント端末間のセッション維持とＷｅｂコンテンツへのアクセス制御を同一Ｗｅｂサーバに対して同時に実現することができ、アクセス制御ポリシーの定義内容に応じて、細かなアクセス制御を実現する。
【０００９】
例えば、利用者が、パーソナルコンピュータ、携帯電話機、デジタルテレビ端末等の、Ｗｅｂサーバにアクセス可能な認証手段の異なる複数のＷｅｂクライアント端末を用いて、Ｗｅｂサーバの提供するＷｅｂコンテンツを利用する際、Ｗｅｂサーバにて予め定めたアクセス制御ポリシーに従い、各Ｗｅｂクライアント端末の具備する認証手段に応じたアクセス制御を、Ｗｅｂサーバの実装部分で実現する。
【００１０】
より具体的には、ＩＤ／パスワードのような比較的低度な認証手段のみを具備するＷｅｂクライアント（例として、デジタルテレビ端末）を用いた場合でも、ＩＣカード認証のような比較的高度な認証手段を具備するＷｅｂクライアント（例として、ＩＣチップを搭載した携帯電話機）による別のログイン済みセッションが有効な場合に、携帯電話機からのみ利用可能なＷｅｂコンテンツを、デジタルテレビからも利用可能にする。これにより、利便性を損なうことなくセキュリティを維持したアクセス制御を実現する。
【００１１】
本発明に係るＷｅｂサーバは、ネットワークを介して、複数のＷｅｂクライアント端末からＨＴＴＰ等によりアクセスされ、通信処理部によってＨＴＴＰ等のログインに係るリクエスト情報を解析し、解析して得られる情報をもとに、アクセス制御部によって予めデータベースに記録したアクセス制御ポリシー情報と照合し、照合結果に応じて、コンテンツ画面生成部によるＷｅｂコンテンツの生成、及び通信処理部によるＨＴＴＰ等のレスポンス（ＷＥＢコンテンツ）の送信の可否を制御する。
【００１２】
アクセス制御ポリシー情報には、ＨＴＴＰヘッダ等のログインに係るリクエスト情報に含まれる、ユーザエージェント情報（各Ｗｅｂクライアント端末が利用するアプリケーションの情報であり、利用環境情報として関連付けられる情報）等に対応したアクセス優先順位情報のポリシーや、このリクエスト情報に含まれるアクセス元識別情報等を当該セッション情報及びログインの情報に対応させて利用制限するポリシー等があり、アクセス履歴は、アクセス制御部によりアクセス履歴情報データベースにて参照され、又は更新される。
【００１３】
即ち、本発明のＷｅｂコンテンツ提供システムは、ネットワーク上のＷｅｂサイトを提供するＷｅｂサーバと、前記Ｗｅｂサーバとネットワークを通じてＷｅｂプロトコル経由で通信する第１Ｗｅｂクライアント端末及び第２Ｗｅｂクライアント端末とを備えるＷｅｂコンテンツ提供システムであって、前記Ｗｅｂサーバは、前記第１Ｗｅｂクライアント端末及び／又は前記第２Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するリクエスト情報解析手段と、当該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報デー

タベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認して、該アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であるか否かを判断するアクセス制御手段と、アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であると判断される場合に、当該リクエスト情報に係るＷｅｂコンテンツを提示するＷｅｂコンテンツ提供手段と、を備えることを特徴とする。

【００１４】

また、本発明のＷｅｂコンテンツ提供システムにおいて、前記リクエスト情報解析手段は、前記第１Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合する手段を有し、前記アクセス制御手段は、該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認するとともに、アクセス履歴情報データベースに記録されているアクセス履歴情報に、前記第１Ｗｅｂクライアント端末の利用者を特定するアクセス元識別情報が存在しているか否かを確認して存在していない場合に、前記利用者を特定するアクセス元識別情報を前記セッション情報、前記第１Ｗｅｂクライアント端末を特定するユーザエージェント情報、当該Ｗｅｂサイトのコンテンツを特定するコンテンツ識別情報、前記認証情報の種別を識別する認証手段識別情報、及び当該セッションに係るアクセス日時情報とともにアクセス履歴情報として前記アクセス履歴情報データベースに記録するアクセス履歴管理手段を有し、前記Ｗｅｂコンテンツ提供手段は、前記アクセス履歴情報の確認後に、当該リクエスト情報に係るＷｅｂコンテンツを提示する手段を有することを特徴とする。

【００１５】

また、本発明のＷｅｂコンテンツ提供システムにおいて、前記リクエスト情報解析手段は、前記第２Ｗｅｂクライアント端末から前記所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合する手段を有し、前記アクセス制御手段は、該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、前記アクセス制御ポリシーに定められるアクセス優先順位に従って当該Ｗｅｂサイトのコンテンツを利用可能であるか否かを判別して利用可能であると判別する場合に、前記アクセス履歴情報データベースに記録されているアクセス履歴情報から前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報を抽出する手段を有し、前記Ｗｅｂコンテンツ提供手段は、前記第１Ｗｅｂクライアント端末へ提示した最も直近のコンテンツ識別情報に対応するＷｅｂコンテンツを前記第１Ｗｅｂクライアント端末へ提示する手段を有することを特徴とする。

【００１６】

また、本発明のＷｅｂコンテンツ提供システムにおいて、前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で、同一のＷｅｂコンテンツが提示されている際に、前記リクエスト情報解析手段が、前記第１Ｗｅｂクライアント端末から当該Ｗｅｂコンテンツをログアウトするリクエスト情報を受信した場合、該リクエスト情報に含まれるアカウントＩＤと、前記アクセス履歴情報データベース内のアクセス履歴情報のアクセス元識別情報と照合する手段を有し、

前記アクセス履歴管理手段が、該照合結果として一致すると判断される場合には、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を削除する手段を有することを特徴とする。

【００１７】

また、本発明のＷｅｂコンテンツ提供システムにおいて、前記アクセス履歴管理手段は、前記アクセス制御ポリシー情報のアクセス優先順位にて前記第１Ｗｅｂクライアント端末が最も優先されている場合に、前記第２Ｗｅｂクライアント端末からのログイン時のリ

クエスト情報に含まれるアカウントＩＤと同一のアカウントＩＤによるセッション情報が存在しているか否かに関わらず、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を削除する手段を有することを特徴とする。

【００１８】

また、本発明のＷｅｂコンテンツ提供システムにおいて、前記アクセス制御ポリシー情報は、アクセス元識別情報とアカウントＩＤが一致する場合、別ポリシーに該当しない限り、同一のＷｅｂコンテンツを前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で同期して提示しないとするポリシーと、前記ユーザエージェント情報に基づく認証情報ごとのアクセス優先順位に、前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末が該当する場合に、同一のＷｅｂコンテンツを前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で同期して提示可能とするポリシーと、前記ユーザエージェント情報に基づく認証情報ごとのＷｅｂコンテンツの内容として全部又は一部で提示可能とする、Ｗｅｂクライアント端末毎のアクセス優先順位によるコンテンツ利用可否制限に対して、前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末が該当する場合に、同一のＷｅｂコンテンツの全部又は一部を前記第１Ｗｅｂクライアント端末及び前記第２Ｗｅｂクライアント端末の双方で同期して提示可能とするポリシーと、を含むことを特徴とする。

【００１９】

また、本発明のＷｅｂコンテンツ提供システムにおいて、前記第１Ｗｅｂクライアント端末の認証情報は、前記第２Ｗｅｂクライアント端末の認証情報よりも高度の認証として、前記アクセス制御ポリシー情報に規定されていることを特徴とする。

【００２０】

また、本発明のＷｅｂサーバは、第１Ｗｅｂクライアント端末及び第２Ｗｅｂクライアント端末とＷｅｂプロトコル経由で通信してネットワーク上のＷｅｂサイトを提供するＷｅｂサーバであって、前記第１Ｗｅｂクライアント端末及び／又は前記第２Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するリクエスト情報解析手段と、当該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認して、該アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であるか否かを判断するアクセス制御手段と、アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であると判断される場合に、当該リクエスト情報に係るＷｅｂコンテンツを提示するＷｅｂコンテンツ提供手段と、を備えることを特徴とする。

【００２１】

更に、本発明は、第１Ｗｅｂクライアント端末及び第２Ｗｅｂクライアント端末とＷｅｂプロトコル経由で通信してネットワーク上のＷｅｂサイトを提供するＷｅｂサーバによるコンテンツ提供方法、Ｗｅｂサーバとして構成するコンピュータに、上記コンテンツ提供方法の各ステップを実行させるためのプログラムとして構成される。

【発明の効果】

【００２２】

本発明によれば、Ｗｅｂサーバにおいて、複数のＷｅｂクライアント端末間のセッション維持とＷｅｂコンテンツへのアクセス制御を同一のＷｅｂサーバに対して同時に実現するため、デジタルテレビ端末のような比較的低度な認証手段のみを具備する第２Ｗｅｂクライアント端末を用いた場合でも、ＩＣカード認証のような比較的高度な認証手段を具備する第１Ｗｅｂクライアント端末（例えば、認証専用ＩＣチップを搭載した携帯電話機）による別のログイン済みセッションが有効な場合に、第１Ｗｅｂクライアント端末からのみ利用可能なＷｅｂコンテンツを、第２Ｗｅｂクライアント端末からも利用可能となる。

【図面の簡単な説明】

【００２３】
【図１】本発明による一実施例のＷｅｂコンテンツ提供システムの典型例を示す図である。
【図２】本発明による一実施例のＷｅｂコンテンツ提供システムにおける第１Ｗｅｂクライアント端末の機能ブロック図である。
【図３】本発明による一実施例のＷｅｂコンテンツ提供システムにおける第２Ｗｅｂクライアント端末１２の機能ブロック図である。
【図４】本発明による一実施例のＷｅｂコンテンツ提供システムにおけるＷｅｂサーバの機能ブロック図である。
【図５】本発明による一実施例のＷｅｂコンテンツ提供システムの動作フローを示す図である。
【図６】本発明による一実施例のＷｅｂコンテンツ提供システムの動作フローを示す図である。
【図７】本発明による一実施例のＷｅｂコンテンツ提供システムの動作フローを示す図である。
【図８】本発明による一実施例のＷｅｂコンテンツ提供システムに係るアクセス制御ポリシー情報の一例を示す図である。
【図９】本発明による一実施例のＷｅｂコンテンツ提供システムに係るアクセス履歴情報テーブルの一例を示す図である。
【図１０】（ａ）（ｂ）は、本発明による一実施例のＷｅｂコンテンツ提供システムに係るアカウント情報テーブルの一例を示す図である。
【発明を実施するための形態】
【００２４】
以下、本発明による一実施例のＷｅｂコンテンツ提供システムを説明する。本発明に係るＷｅｂクライアント端末、Ｗｅｂサーバ及びこれらのプログラム、並びに、本発明に係るコンテンツ提供方法は、本発明による一実施例のＷｅｂコンテンツ提供システムの説明から明らかになる。
【００２５】
〔システム構成〕
図１は、本発明による一実施例のＷｅｂコンテンツ提供システムの典型例を示す図である。本実施例のＷｅｂコンテンツ提供システム１は、Ｗｅｂサーバ１３に対して予め登録した複数のクライアント端末毎のアクセス制御ポリシー情報を管理することで、複数のＷｅｂクライアント端末間のセッション維持とＷｅｂコンテンツへのアクセス制御を同一のＷｅｂサーバ１３に対して同時に実現する。従って、利用者は、デジタルテレビ端末のような比較的低度な認証手段のみを具備する第２Ｗｅｂクライアント端末を用いた場合でも、ＩＣカード認証のような比較的高度な認証手段を具備する第１Ｗｅｂクライアント端末（例えば、認証専用ＩＣチップを搭載した携帯電話機）による別のログイン済みセッションが有効な場合に、第１Ｗｅｂクライアント端末１１からのみ利用可能なＷｅｂコンテンツを、第２Ｗｅｂクライアント端末１２からも利用可能とする。
【００２６】
図１に例示する本実施例のＷｅｂコンテンツ提供システム１では、ＩＣカード認証のような比較的高度な認証手段（Ｗｅｂアプリで規定される認証手段）でＷｅｂアクセスを行う機能を有する第１Ｗｅｂクライアント端末１１（例えば、携帯電話機）と、比較的低度な認証手段（Ｗｅｂブラウザで規定される認証手段）のみを有する第２Ｗｅｂクライアント端末１２（例えば、デジタルテレビ端末）と、認証の必要なＷｅｂサイトのサービスを提供するＷｅｂサーバ１３から構成され、第１Ｗｅｂクライアント端末１１、第２Ｗｅｂクライアント端末１２及びＷｅｂサーバ１３は、インターネットなどＷＡＮ経由で接続される。
【００２７】
第１Ｗｅｂクライアント端末１１及び第２Ｗｅｂクライアント端末１２は、セッション

維持のための特別なコンポーネントの実装は不要であり、多くのクライアント端末（携帯電話機やデジタルテレビ端末）で装備されているため、特別なハードウェアの追加なしで、ファームウェアの変更のみで本実施例のＷｅｂコンテンツ提供システム１を実現可能である。また、各Ｗｅｂクライアント端末は、多くのＷｅｂブラウザなどのユーザエージェントがサポートする、セッションクッキーやスクリプト機能（Ｗｅｂプロトコル処理部）を具備しているものとする。ＨＴＴＰのようなステートレスなプロトコル通信においても、セッションクッキーやスクリプト機能を活用してセッション維持が行われている。

【００２８】

以下、より具体的に、第１Ｗｅｂクライアント端末１１、第２Ｗｅｂクライアント端末１２、及びＷｅｂサーバ１３の構成について説明する。

【００２９】

図２に、本発明による一実施例のＷｅｂコンテンツ提供システムにおける第１Ｗｅｂクライアント端末１１の機能ブロック図を示す。第１Ｗｅｂクライアント端末１１は、制御部（Ｗｅｂアプリ部）１１１と、Ｗｅｂサーバ１３とのＷｅｂ通信を行うインターフェースを構成する通信制御部１１２と、利用者が操作するユーザＩ／Ｆ１１３ａからの入力を制御するユーザＩ／Ｆ制御部１１３と、Ｗｅｂサーバ１３が提供するＷｅｂコンテンツを表示するための表示装置１１４ａを制御する表示制御部１１４と、記憶部１１５とを備える。尚、通信制御部１１２は、Ｗｅｂサーバ１３とのセッションで非同期通信を可能とする非同期通信部１１２１を有する。制御部１１１は、Ｗｅｂプロトコル処理部１１１１と、認証情報処理部１１１２と、リクエスト情報生成部１１１３と、Ｗｅｂ表示制御部１１１４とを備える。尚、本発明に係る制御部１１１の各機能を説明するが、第１Ｗｅｂクライアント端末１１が備える他の機能を排除することを意図したものではないことに留意する。第１Ｗｅｂクライアント端末１１は、コンピュータとして構成することができ、制御部１１１の各機能を実現する処理内容を記述したプログラムを、当該コンピュータの記憶部１１５に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。

【００３０】

Ｗｅｂプロトコル処理部１１１１は、Ｗｅｂサーバ１３とのＷｅｂ通信を確立する機能を有する。特に、Ｗｅｂプロトコル処理部１１１１は、Ｗｅｂアプリを起動させて、ネットワークを通じてＷｅｂサーバ１３に対し、認証処理を実行する機能を有する。

【００３１】

認証情報処理部１１１２は、例えばＩＣカード認証のような比較的高度な認証手段を実現するための認証情報を処理する機能を有する。

【００３２】

リクエスト情報生成部１１１３は、Ｗｅｂアプリを通じて入力されるログインＩＤ／パスワードをＷｅｂサーバ１３に送信する際のリクエスト情報を生成する機能、及びログアウト時のアカウントＩＤを含むリクエスト情報を生成する機能を有する。

【００３３】

Ｗｅｂ表示制御部１１１４は、Ｗｅｂサーバ１３によって認証処理が行われた後に該当ＵＲＬのＷｅｂコンテンツを、表示制御部１１４を介して表示装置１１４ａに表示させる機能を有する。

【００３４】

図３に、本発明による一実施例のＷｅｂコンテンツ提供システムにおける第２Ｗｅｂクライアント端末１２の機能ブロック図を示す。第２Ｗｅｂクライアント端末１２は、制御部１２１と、Ｗｅｂサーバ１３に対してＷｅｂ通信を行うインターフェースを構成する通信制御部１２２と、利用者が操作するユーザＩ／Ｆ１２３ａからの入力を制御するユーザＩ／Ｆ制御部１２３と、Ｗｅｂサーバ１３が提供するＷｅｂコンテンツを表示するための表示装置１２４ａを制御する表示制御部１２４と、記憶部１２５とを備える。尚、通信制御部１２２は、Ｗｅｂサーバ１３とのセッションで非同期通信を可能とする非同期通信部１２２１を有する。制御部（Ｗｅｂブラウザ）１２１は、Ｗｅｂプロトコル処理部１２１

１と、認証情報処理部１２１２と、リクエスト情報生成部１２１３と、Ｗｅｂ表示制御部１２１４とを備える。尚、本発明に係る制御部１２１の各機能を説明するが、第２Ｗｅｂクライアント端末１２が備える他の機能を排除することを意図したものではないことに留意する。第２Ｗｅｂクライアント端末１２は、コンピュータとして構成することができ、制御部１２１の各機能を実現する処理内容を記述したプログラムを、当該コンピュータの記憶部１２５に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。

【００３５】

Ｗｅｂプロトコル処理部１２１１、リクエスト情報生成部１２１３、及びＷｅｂ表示制御部１２１４は、それぞれ第１Ｗｅｂクライアント端末１１におけるＷｅｂプロトコル処理部１１１１、リクエスト情報生成部１２１３、及びＷｅｂ表示制御部１２１４と同様の機能を有する。ただし、本実施例では、認証情報処理部１２１２が、ＩＤ／パスワードのような比較的低度な認証手段を実現するための認証情報を処理する機能を有する例を説明する。

【００３６】

図４に、本発明による一実施例のＷｅｂコンテンツ提供システムにおけるＷｅｂサーバ１３の機能ブロック図を示す。Ｗｅｂサーバ１３は、制御部１３１と、第１Ｗｅｂクライアント端末１１及び／又は第２Ｗｅｂクライアント端末１２に対してＷｅｂ通信を行うインターフェースを構成する通信制御部１３２と、所定のアカウント情報テーブル（図１０）を格納するアカウント情報データベース１３３と、所定のアクセス制御ポリシー情報（図８）を格納するアクセス制御ポリシー情報データベース１３４と、所定のアクセス履歴情報テーブル（図９）を格納するアクセス履歴情報データベース１３５と、各ＵＲＬのＷｅｂコンテンツの情報を保持するコンテンツデータベース１３６と、記憶部１３７とを備える。制御部１３１は、通信処理部（Ｗｅｂプロトコル処理部１３１１及びリクエスト情報解析部１３１２からなる）と、アクセス制御部１３１３（アクセス履歴管理部１３１４を有する）と、コンテンツ画面生成部１３１５とを備える。尚、本発明に係る制御部１３１の各機能を説明するが、Ｗｅｂサーバ１３が備える他の機能を排除することを意図したものではないことに留意する。Ｗｅｂサーバ１３は、コンピュータとして構成することができ、制御部１３１の各機能を実現する処理内容を記述したプログラムを、当該コンピュータの記憶部１３７に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。

【００３７】

通信処理部におけるＷｅｂプロトコル処理部１３１１は、第１Ｗｅｂクライアント端末１１及び／又は第２Ｗｅｂクライアント端末１２とのＷｅｂ通信を確立する機能を有する。特に、Ｗｅｂプロトコル処理部１３１１は、リクエスト情報に基づくセッション情報を生成する機能を有する。また、Ｗｅｂプロトコル処理部１３１１は、特定のＷｅｂコンテンツのみ通常のセッションタイムアウト時間以上に継続して利用できるように設定して、各Ｗｅｂクライアント端末に対して、ポーリング実行スクリプト情報を送信することで非同期スクリプトを実現する機能を有する。

【００３８】

通信処理部におけるリクエスト情報解析部１３１２は、ログインＩＤ／パスワードを含むリクエスト情報やログアウトのリクエスト情報を解析して、アカウント情報データベース１３３のアカウント情報に予め登録され記録されているログインＩＤ／パスワードの情報と照合する機能を有する。

【００３９】

尚、リクエスト情報に含まれるアカウント情報に関して、同一のアカウントＩＤに対して、複数のログインを許可することができ、例えば、第１Ｗｅｂクライアント端末１１に対するログイン１と第２Ｗｅｂクライアント端末１２に対するログイン２という例を図１０（ａ）に示す。更には、アカウント情報データベース１３３にて、同一のアカウントＩＤに対して、利用環境情報として識別される第１Ｗｅｂクライアント端末１１のＷｅｂア

プリや第２Ｗｅｂクライアント端末１２のＷｅｂブラウザを、それぞれのパスワードと認証情報（例えば、ＩＣカード等の認証手段の種別に応じた利用環境情報）で予め登録しておくことができる（図１０（ｂ））。

【００４０】

アクセス制御部１３１３は、リクエスト情報の解析結果のログインＩＤ／パスワードを基に、アクセス制御ポリシー情報データベース１３４内のアクセス制御ポリシー情報を参照してポリシーを確認し、さらに、アクセス履歴情報データベース１３５内のアクセス履歴情報テーブルに、利用者Ａを特定するアクセス元識別情報が存在しているか否かを確認し、アクセス制御部１３１３内のアクセス履歴管理部１３１４によって、アクセス履歴情報としてアクセス履歴情報データベース１３５内のアクセス履歴情報テーブルに記録させる機能を有する。また、アクセス制御部１３１３は、ログアウト時のアカウントＩＤを含むリクエスト情報の解析結果を基に、アクセス履歴管理部１３１４によって、アクセス履歴情報データベース１３５内のアクセス履歴情報テーブルを参照させ、該当セッション情報を含むアクセス履歴情報を削除させる機能を有する。

【００４１】

尚、アクセス制御ポリシー情報は、アクセス元識別情報とアカウントＩＤが一致する場合、別ポリシーに該当しない限り、同一のＷｅｂコンテンツを複数のＷｅｂクライアント端末で同期して提示しないとするポリシーと、ユーザエージェント情報に基づく認証情報ごとのアクセス優先順位に、複数のＷｅｂクライアント端末が該当する場合に、同一のＷｅｂコンテンツを複数のＷｅｂクライアント端末で同期して提示可能とするポリシーと、ユーザエージェント情報に基づく認証情報ごとのＷｅｂコンテンツの内容として全部又は一部で提示可能とする、Ｗｅｂクライアント端末毎のアクセス優先順位によるコンテンツ利用可否制限に対して、複数のＷｅｂクライアント端末が該当する場合に、同一のＷｅｂコンテンツの全部又は一部を複数のＷｅｂクライアント端末で同期して提示可能とするポリシーと、を含むように構成することができる（図８）。また、第１Ｗｅｂクライアント端末１１の認証情報は、第２Ｗｅｂクライアント端末１２の認証情報よりも高度の認証として、アクセス制御ポリシー情報にて規定することもできる。

【００４２】

尚、アクセス履歴管理部１３１４は、各Ｗｅｂクライアント端末によるアクセスごとに繰り返されるアクセス履歴を、アクセス履歴情報データベース１３５内のアクセス履歴情報テーブルに更新する機能を有する。また、アクセス履歴管理部１３１４は、アクセス履歴情報データベース１３５に、利用者を特定するアクセス元識別情報を、セッション情報、Ｗｅｂクライアント端末を特定するユーザエージェント情報、ＷｅｂサイトのＷｅｂコンテンツを特定するコンテンツ識別情報、認証情報（認証手段）の種別を識別する認証手段識別情報、及び当該セッションに係るアクセス日時情報とともにアクセス履歴情報として記録する（図９）。

【００４３】

コンテンツ画面生成部１３１５は、アクセス制御部１３１３からの指示により、コンテンツデータベース１３６から、要求される該当ＵＲＬのＷｅｂコンテンツを読み出し、各Ｗｅｂクライアント端末へのログイン画面又はサービス提供画面を生成して通信処理部（Ｗｅｂプロトコル処理部１３１１）経由で提示する機能を有する。また、コンテンツ画面生成部１３１５は、アクセス制御部１３１３によるアクセス履歴情報のアクセス元識別情報に基づく照合結果で存在しない場合に、アクセス制御部１３１３からの指示により、Ｗｅｂコンテンツのサービス不能画面を生成して通信処理部（Ｗｅｂプロトコル処理部１３１１）経由で提示する機能を有する。

【００４４】

以下、本発明による一実施例のＷｅｂコンテンツ提供システムの動作を説明する。

【００４５】

〔システム動作〕

図５乃至図７は、本発明による一実施例のＷｅｂコンテンツ提供システムの動作フロー

を示す図である。まず、図５を参照するに、利用者Ａは、第１Ｗｅｂクライアント端末１１（例として携帯電話機）のユーザＩ／Ｆ１１３ａを介してＷｅｂアプリを起動させ、Ｗｅｂサーバ１３）が提供するＷｅｂコンテンツのＵＲＬを入力してアクセスする（ステップＳ１）。

【００４６】

Ｗｅｂサーバ１３は、コンテンツ画面生成部１３１５により、レスポンスのＷｅｂコンテンツをコンテンツデータベース１３６から読み出して、ログイン画面を、第１Ｗｅｂクライアント端末１１に提示する（ステップＳ２）。

【００４７】

利用者Ａは、第１Ｗｅｂクライアント端末１１のユーザＩ／Ｆ１１３ａを介してログインＩＤ／パスワードをログイン画面の所定の入力フィールドに入力し、送信ボタンを押下し、ログインＩＤ／パスワードを含むリクエスト情報をＷｅｂサーバ１３に送信する（ステップＳ３）。

【００４８】

尚、利用者認証の例としてＩＣカード等を用いて読み取られたＩＤ及びパスワードの組み合わせで入力することや、ログインＩＤを操作入力することもできる。また、ログインＩＤ／パスワードの登録は、利用者Ａが、第１Ｗｅｂクライアント端末１１を用いて、Ｗｅｂサーバ１３の提供するログインＩＤ／パスワード登録方法に従い、事前に実施済みとする。ログインＩＤ／パスワードは、使用する第１Ｗｅｂクライアント端末１１に関連付けて個別に登録するか、又は複数のＷｅｂクライアント端末で共通に利用することができ、このどちらでもよい。

【００４９】

Ｗｅｂサーバ１３は、通信処理部のリクエスト情報解析部１３１２によって、第１Ｗｅｂクライアント端末１１からのリクエスト情報を解析し、予めアカウント情報データベース１３３のアカウント情報に記録されているログインＩＤ／パスワードの情報と照合する（ステップＳ４，Ｓ５）。

【００５０】

Ｗｅｂサーバ１３は、この照合の結果、一致したと判断した場合（ステップＳ６）、Ｗｅｂプロトコル処理部１３１１によって、セッション情報を生成し（ステップＳ７）、アクセス制御部１３１３によって、リクエスト情報の解析結果のアクセス元識別情報及びログインＩＤ／パスワードを基に、アクセス制御ポリシー情報データベース１３４内のアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認し、アクセス履歴情報データベース１３５内のアクセス履歴情報テーブルに、利用者Ａを特定するアクセス元識別情報が存在しているか否かを確認する（ステップＳ８，Ｓ９）。アクセス元識別情報とリクエスト解析結果との対応については予め登録され、アクセス制御ポリシー情報内に定義されている。

【００５１】

Ｗｅｂサーバ１３は、アクセス元識別情報の確認の結果、初めてのアクセスであると判断される場合（ステップＳ１０）、アクセス制御部１３１３内のアクセス履歴管理部１３１４によって、図９に示すような、該当するアクセス元識別情報、セッション情報、ユーザエージェント情報、コンテンツ識別情報、認証手段識別情報、及び当該セッションに係るアクセス日時情報を、アクセス履歴情報としてアクセス履歴情報データベース１３５に記録する（ステップＳ１１）。初めてのアクセスでないと判断される場合には該当するアクセス日時情報を更新する。

【００５２】

続いて、Ｗｅｂサーバ１３は、コンテンツ画面生成部１３１５によって、コンテンツデータベース１３６から、要求される該当ＵＲＬのＷｅｂコンテンツを読み出し、第１Ｗｅｂクライアント端末１１へのレスポンスのＷｅｂコンテンツ（サービス提供画面）を生成し、アクセス制御部１３１３によって、Ｗｅｂコンテンツの識別情報をアクセス履歴情報データベース１３５内のアクセス履歴情報テーブルに追加して記録する。

【００５３】
Ｗｅｂサーバ１３は、Ｗｅｂプロトコル処理部１３１１によって、セッション情報とともに、第１Ｗｅｂクライアント端末１１へのレスポンスのＷｅｂコンテンツ（サービス提供画面）を第１Ｗｅｂクライアント端末１１に提示して、当該リクエスト情報に係るＷｅｂサイトへのアクセスを許可する（ステップＳ１２）。
【００５４】
利用者Ａが、Ｗｅｂコンテンツを利用する間、第１Ｗｅｂクライアント端末１１とＷｅｂサーバ１３の間で繰り返されるアクセスは、アクセス履歴管理部１３１４によって管理され（ステップＳ１３）、即ちＷｅｂコンテンツを利用する際のリクエストとレスポンスが繰り返されるたびに、アクセス履歴情報データベース１３５内のアクセス履歴情報テーブルは更新される（ステップＳ１４乃至Ｓ１５）。また、Ｗｅｂサーバ１３は、特定のＷｅｂコンテンツのみ通常のセッションタイムアウト時間以上に継続して利用できるように設定することができ、この場合、レスポンス情報の送信の際、第１Ｗｅｂクライアント端末１１の非同期通信部１１２１に対して、ポーリング実行スクリプト情報を送信することで非同期スクリプトが実現される（ステップＳ１６）。
【００５５】
このようにして、利用者Ａは、第１Ｗｅｂクライアント端末１１を利用して、Ｗｅｂサーバ１３が提供するＷｅｂコンテンツを利用することができる。
【００５６】
引き続き、利用者Ａは、Ｗｅｂコンテンツの利用上、例えば第１Ｗｅｂクライアント端末１１の画面が小さく閲覧しづらい等の理由で、第２Ｗｅｂクライアント端末１２（例としてデジタルテレビ端末）を用いて、Ｗｅｂサーバ１３にアクセスする例を説明する。
【００５７】
図６を参照するに、利用者Ａは、第２Ｗｅｂクライアント端末１２のユーザＩ／Ｆ１２３ａを介してＷｅｂブラウザを起動させ、Ｗｅｂサーバ１３が提供するＷｅｂコンテンツのＵＲＬを入力してアクセスする（ステップＳ２１）。
【００５８】
Ｗｅｂサーバ１３は、コンテンツ画面生成部１３１５により、レスポンスのＷｅｂコンテンツをコンテンツデータベース１３６から読み出して、ログイン画面を、第１Ｗｅｂクライアント端末１１に提示する（ステップＳ２２）。
【００５９】
利用者Ａは、第２Ｗｅｂクライアント端末１２のユーザＩ／Ｆ１２３ａを介してログインＩＤ／パスワードをログイン画面の所定の入力フィールドに入力し、送信ボタンを押下し、ログインＩＤ／パスワードを含むリクエスト情報を送信する（ステップＳ２３）。
【００６０】
尚、利用者認証の例としてログインＩＤを操作入力することや、ＩＣカード等を用いて読み取られたＩＤ及びパスワードの組み合わせとすることができる。また、ログインＩＤ／パスワードの登録は、利用者Ａが、第１Ｗｅｂクライアント端末１１を用いて、Ｗｅｂサーバ１３の提供するログインＩＤ／パスワード登録方法に従い、事前に実施済みとする。ログインＩＤ／パスワードは、使用する第１Ｗｅｂクライアント端末１１に関連付けて個別に登録するか、又は複数のＷｅｂクライアント端末で共通に利用することができ、このどちらでもよい。
【００６１】
Ｗｅｂサーバ１３は、アクセス制御部１３１３内のリクエスト情報解析部１３１２によって、第１Ｗｅｂクライアント端末１１からのリクエスト情報を解析し、予めアカウント情報データベース１３３のアカウント情報に記録されているログインＩＤ／パスワードの情報と照合する（ステップＳ２４,Ｓ２５）。
【００６２】
Ｗｅｂサーバ１３は、この照合の結果、一致すると判断した場合（ステップＳ２６）、通信処理部（Ｗｅｂプロトコル処理部１３１１）によって、セッション情報を生成し（ス

テップＳ２７）、アクセス制御部１３１３によって、リクエスト情報の解析結果のログインＩＤ／パスワードを基に、上記と同様に、アクセス制御ポリシー情報データベース１３４内のアクセス制御ポリシー情報を参照してポリシーを確認し、アクセス履歴情報データベース１３５内のアクセス履歴情報テーブルに、利用者Ａを特定するアクセス元識別情報が存在しているか否かを確認する（ステップＳ２８，Ｓ２９）。

【００６３】

Ｗｅｂサーバ１３は、アクセス制御部１３１３によって、アクセス制御ポリシー情報の確認の結果、アクセス元識別情報がログインＩＤに関連付けられたアカウントＩＤ、と定義されていると判断した場合、Ｗｅｂサーバ１３における利用者Ａのアカウント ＩＤはユニークであると判断し（同一のアクセス元識別情報が存在すると判断し）、即ち、２つのＷｅｂクライアント端末で同期して利用不可と判断した場合、アクセス制御ポリシー情報にて、その他のポリシーの照合がないかを確認する（ステップＳ３０）。

【００６４】

その他のポリシーとして、ユーザエージェント情報によるアクセス優先順位が、アクセス制御情報ポリシーに設定されている場合で、第１Ｗｅｂクライアント端末１１が第２Ｗｅｂクライアント端末１２に優先するとして設定されている場合に、第１Ｗｅｂクライアント端末１１からのセッション情報が存在して維持されている状況下で、さらにその他のポリシーの照合がないかを確認する（ステップＳ３１）。

【００６５】

更に、その他のポリシーとして、Ｗｅｂクライアント端末毎のアクセス優先順位によるコンテンツ利用可否制限が、アクセス制御ポリシーに設定されている場合で、このアクセス制御ポリシーの結果、アクセス履歴情報に記録されているコンテンツ識別情報のＷｅｂコンテンツが、第２Ｗｅｂクライアント端末１２のアクセス優先順位で利用可能であると判断される場合（ステップＳ３２）、アクセス制御部１３１３は、第１Ｗｅｂクライアント端末１１からのセッション情報が存在して維持されている状況下で、第２Ｗｅｂクライアント端末１２に対して、当該ポリシーに従うＷｅｂコンテンツの提供が可能であると判断する。コンテンツ提供ができないと判断される場合は、その都度、第２Ｗｅｂクライアント端末１２に対してその旨を知らせる。

【００６６】

Ｗｅｂサーバ１３は、アクセス制御部１３１３により、アクセス履歴情報テーブルに記録されているＷｅｂコンテンツのコンテンツ識別情報のうちの第１Ｗｅｂクライアント端末１１へ送信した最も直近のコンテンツ識別情報を抽出し、このコンテンツ識別情報を元に、コンテンツ画面生成部１３１５に対して、ポリシーに従うコンテンツ生成を要求する。コンテンツ画面生成部１３１５は、コンテンツ識別情報を基に、最も直近に第１Ｗｅｂクライアント端末１１へ送信したものと同様のレスポンス情報のＷｅｂコンテンツ（サービス提供画面）を生成し、アクセス制御部１３１３に返却する。

【００６７】

Ｗｅｂサーバ１３は、アクセス制御部１３１３からの要求により、Ｗｅｂプロトコル処理部１３１１によって、セッション情報とともに、当該レスポンス情報のＷｅｂコンテンツ（サービス提供画面）を、第２Ｗｅｂクライアント端末１２に送信する（ステップＳ３３）。

【００６８】

このようにして、利用者Ａは、第２Ｗｅｂクライアント端末１２のＷｅｂブラウザを用いて、Ｗｅｂサーバ１３が送信する、前述の第１Ｗｅｂクライアント端末１１におけるレスポンス情報のＷｅｂコンテンツ（サービス提供画面）を利用し、前述と同様に第２Ｗｅｂクライアント端末１２の非同期通信部１２２１に対して非同期スクリプトも実行することができる（ステップＳ３４）。

【００６９】

利用者Ａが、Ｗｅｂコンテンツを利用する間、第２Ｗｅｂクライアント端末１２とＷｅｂサーバ１３の間で繰り返されるアクセスは、アクセス履歴管理部１３１４によって管理

され、即ちＷｅｂコンテンツを利用する際のリクエストとレスポンスが繰り返されるたびに、アクセス履歴情報データベース１３５内のアクセス履歴情報テーブルは更新される（ステップＳ３５乃至Ｓ３７）。

【００７０】

続いて、第１Ｗｅｂクライアント端末１１及び第２Ｗｅｂクライアント端末１２の双方で、同一のＷｅｂコンテンツが提示されている際に、利用者Ａが、第１Ｗｅｂクライアント端末１１のＷｅｂアプリを用いて、ログアウト操作もしくはＷｅｂアプリを終了する場合を説明する。

【００７１】

図７を参照するに、Ｗｅｂサーバ１３は、通信処理部内のリクエスト情報解析部１３１２によって、利用者Ａの第１Ｗｅｂクライアント端末１１から当該Ｗｅｂコンテンツをログアウトするリクエスト情報を受信した場合、アカウントＩＤを含むこのリクエスト情報を解析し（ステップＳ４１，Ｓ４２）、アクセス制御部１３１３によって、アクセス履歴情報データベース１３５内のアクセス履歴情報のアクセス元識別情報と照合し（ステップＳ４３，Ｓ４４）、アクセス制御部１３１３内のアクセス履歴管理部１３１４によって、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を更新（削除）する（ステップＳ４５）。さらに、アクセス制御ポリシー情報のアクセス優先順位にて、第１Ｗｅｂクライアント端末１１が最も優先されている場合には、第２Ｗｅｂクライアント端末１２からのログイン時のリクエスト情報に含まれるアカウントＩＤと同一のアカウントＩＤによるセッション情報が存在しているか否かに関わらず、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を削除する（ステップＳ４６）。これにより、再び、図５及び図６に示される処理が繰り返される場合にも同様に動作する。Ｗｅｂサーバ１３は、コンテンツ画面生成部１３１５によって、当該セッションのＷｅｂコンテンツのサービス終了画面を第１Ｗｅｂクライアント端末１１に提示する（ステップＳ４７）。

【００７２】

また、Ｗｅｂサーバ１３は、Ｗｅｂプロトコル処理部１３１１により、第１Ｗｅｂクライアント端末１１の通信制御部１１２からのポーリングのタイムアウトあるいは通常セッションのタイムアウトの発生を検知した場合も、アクセス制御部１３１３によりアクセス履歴管理部１３１４に指示して、前述と同様、該当セッション情報を含むアクセス履歴情報を削除する（ステップＳ４８）。

【００７３】

続いて、利用者Ａが、第２Ｗｅｂクライアント端末１２のＷｅｂブラウザを用いて、画面操作を行うと（ステップＳ５１）、Ｗｅｂサーバ１３のリクエスト情報解析部１３１２が対応するリクエスト情報を解析して（ステップＳ５２）、アクセス制御部１３１３が、アクセス履歴情報のアクセス元識別情報と照合し（ステップＳ５３，Ｓ５４）、該当情報が存在しないため（ステップＳ５５）、コンテンツ画面生成部１３１５が当該レスポンスのＷｅｂコンテンツ（サービス不能画面）を生成し、Ｗｅｂプロトコル処理部１３１１経由で第２Ｗｅｂクライアント端末１２に提示する（ステップＳ５６）。従って、第１Ｗｅｂクライアント端末１１に対するサービス終了に伴い、第２Ｗｅｂクライアント端末１２に対するサービス提供も終了され、予め定めたアクセス制御ポリシーの利用制限が維持される。

【００７４】

このように、上記の実施例によれば、複数のＷｅｂクライアント端末間のセッション維持とＷｅｂコンテンツへのアクセス制御を同一のＷｅｂサーバに対して同時に実現することができる。このため、デジタルテレビ端末のような比較的低度な認証手段のみを具備する第２Ｗｅｂクライアント端末１２を用いた場合でも、ＩＣカード認証のような比較的高度な認証手段を具備する第１Ｗｅｂクライアント端末１１（例えば、認証専用ＩＣチップを搭載した携帯電話機）による別のログイン済みセッションが有効な場合に、第１Ｗｅｂクライアント端末１１からのみ利用可能なＷｅｂコンテンツを、第２Ｗｅｂクライアント端末１２からも利用可能となる。

【００７５】
包括的には、本発明に係るＷｅｂサーバ１３は、第１Ｗｅｂクライアント端末及び／又は前記第２Ｗｅｂクライアント端末から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合するリクエスト情報解析部１３１２と、当該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベースに登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認して、該アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であるか否かを判断するアクセス制御部１３１３と、アクセス制御ポリシーに応じたＷｅｂコンテンツが提供可能であると判断される場合に、当該リクエスト情報に係るＷｅｂコンテンツを提示するコンテンツ画面生成部１３１５と、を備える。
【００７６】
特に、リクエスト情報解析部１３１２は、第１Ｗｅｂクライアント端末１１から所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合する手段を有し、アクセス制御部１３１３は、該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、予めアクセス制御ポリシー情報データベース１３３に登録されているアクセス制御ポリシー情報を参照して認証情報に応じたアクセス制御ポリシーを確認するとともに、アクセス履歴情報データベース１３５に記録されているアクセス履歴情報に、第１Ｗｅｂクライアント端末１１の利用者を特定するアクセス元識別情報が存在しているか否かを確認して存在していない場合に、利用者を特定するアクセス元識別情報をセッション情報、第１Ｗｅｂクライアント端末１１を特定するユーザエージェント情報、当該Ｗｅｂサイトのコンテンツを特定するコンテンツ識別情報、認証情報の種別を識別する認証手段識別情報、及び当該セッションに係るアクセス日時情報とともにアクセス履歴情報としてアクセス履歴情報データベース１３５に記録するアクセス履歴管理部１３５を備える。
【００７７】
ここで、本発明に係るＷｅｂサーバ１３のリクエスト情報解析部１３１２は、第２Ｗｅｂクライアント端末１２から該所定のＷｅｂサイトへアクセスする際のログイン時の認証情報を含むリクエスト情報を受信して、予めアカウント情報データベースに登録されているアカウント情報に記録される認証情報と照合する手段を有し、アクセス制御部１３１３は、該照合の結果として一致した場合に、当該アクセスのセッション情報を生成し、該リクエスト情報に含まれる認証情報を基に、アクセス制御ポリシーに定められるアクセス優先順位に従って当該Ｗｅｂサイトのコンテンツを利用可能であるか否かを判別して利用可能であると判別する場合に、アクセス履歴情報データベース１３５に記録されているアクセス履歴情報から第１Ｗｅｂクライアント端末１１へ提示した最も直近のコンテンツ識別情報を抽出し、コンテンツ画面生成部１３１５は、第１Ｗｅｂクライアント端末１１へ提示した最も直近のコンテンツ識別情報に対応するＷｅｂコンテンツを第１Ｗｅｂクライアント端末１１へ提示する画面を生成する。
【００７８】
また、第１Ｗｅｂクライアント端末１１及び第２Ｗｅｂクライアント端末１２の双方で、同一のＷｅｂコンテンツが提示されている際に、リクエスト情報解析部１３１２が、第１Ｗｅｂクライアント端末１１から当該Ｗｅｂコンテンツをログアウトするリクエスト情報を受信した場合、該リクエスト情報に含まれるアカウントＩＤと、アクセス履歴情報データベース１３５内のアクセス履歴情報のアクセス元識別情報と照合し、アクセス履歴管理部１３１４が、該照合結果として一致すると判断される場合には、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を削除する。更に、アクセス履歴管理部１３１４は、アクセス制御ポリシー情報のアクセス優先順位にて第１Ｗｅｂクライアント端末１１が最も優先されている場合に、第２Ｗｅｂクライアント端末１２からのログイン時

のリクエスト情報に含まれるアカウントＩＤと同一のアカウントＩＤによるセッション情報が存在しているか否かに関わらず、アクセス元識別情報とアカウントＩＤが一致するアクセス履歴情報を削除する手段を有する。

【００７９】

これらの本発明に係る第１Ｗｅｂクライアント端末１１、第２Ｗｅｂクライアント端末１２、及びＷｅｂサーバ１３をコンピュータで構成した場合、各機能を実現する処理内容を記述したプログラムを、当該コンピュータの内部又は外部の記憶部に格納しておき、当該コンピュータの中央演算処理装置（ＣＰＵ）によってこのプログラムを読み出して実行させることで実現することができる。また、このようなプログラムは、例えばＤＶＤ又はＣＤ－ＲＯＭなどの可搬型記録媒体の販売、譲渡、貸与等により流通させることができるほか、そのようなプログラムを、例えばネットワーク上にあるサーバの記憶部に記憶しておき、ネットワークを介してサーバから他のコンピュータにそのプログラムを転送することにより、流通させることができる。また、そのようなプログラムを実行するコンピュータは、例えば、可搬型記録媒体に記録されたプログラム又はサーバから転送されたプログラムを、一旦、自己の記憶部に記憶することができる。また、このプログラムの別の実施態様として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、更に、このコンピュータにサーバからプログラムが転送される度に、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。従って、本発明は、前述した実施例に限定されるものではなく、その主旨を逸脱しない範囲において種々変更可能である。

【産業上の利用可能性】

【００８０】

本発明によれば、複数のＷｅｂクライアント端末間のセッション維持とＷｅｂコンテンツへのアクセス制御を同一のＷｅｂサーバに対して同時に実現することができるため、利用者のサービス利用度が向上するため、Ｗｅｂコンテンツを提供するサービスの方式に有用である。

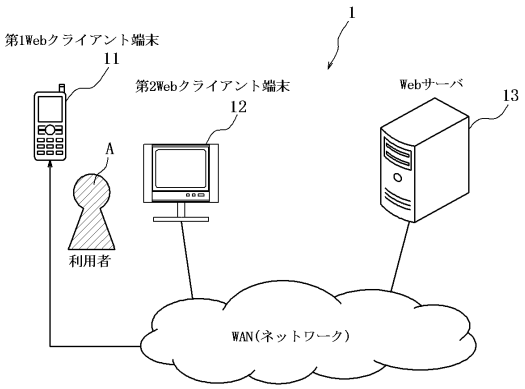
【符号の説明】

【００８１】

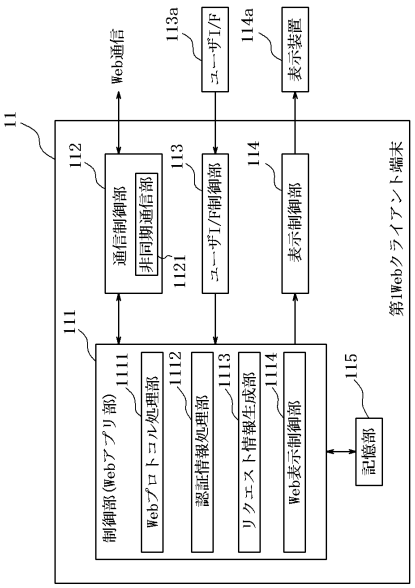
１　Ｗｅｂコンテンツ提供システム
１１　第１Ｗｅｂクライアント端末
１２　第２Ｗｅｂクライアント端末
１３　Ｗｅｂサーバ
１１１　制御部（Ｗｅｂアプリ部）
１１２　通信制御部
１１３　ユーザＩ／Ｆ制御部
１１３ａ　ユーザＩ／Ｆ
１１４　表示制御部
１１４ａ　表示装置
１１５　記憶部
１２１　制御部（Ｗｅｂブラウザ部）
１２２　通信制御部
１２３　ユーザＩ／Ｆ制御部
１２４　表示制御部
１２５　記憶部
１３１　制御部
１３２　通信制御部
１３３　アカウント情報データベース
１３４　アクセス制御ポリシー情報データベース
１３５　アクセス履歴情報データベース
１３６　コンテンツデータベース

１３７　記憶部
１１１１　Ｗｅｂプロトコル処理部
１１１２　認証情報処理部
１１１３　リクエスト情報生成部
１１１４　Ｗｅｂ表示制御部
１１２１　非同期通信部
１２１１　Ｗｅｂプロトコル処理部
１２１２　認証情報処理部
１２１３　リクエスト情報生成部
１２１４　Ｗｅｂ表示制御部
１２２１　非同期通信部
１３１１　Ｗｅｂプロトコル処理部
１３１２　リクエスト情報解析部
１３１３　アクセス制御部
１３１４　アクセス履歴管理部
１３１５　コンテンツ画面生成部

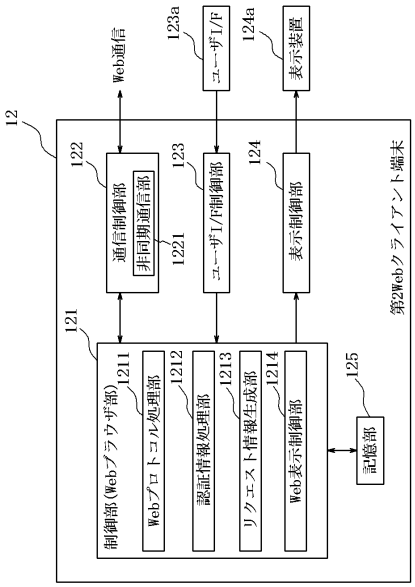
【図１】



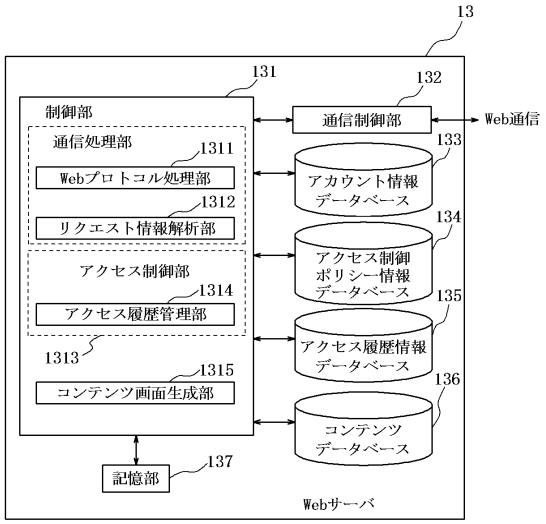
【図２】



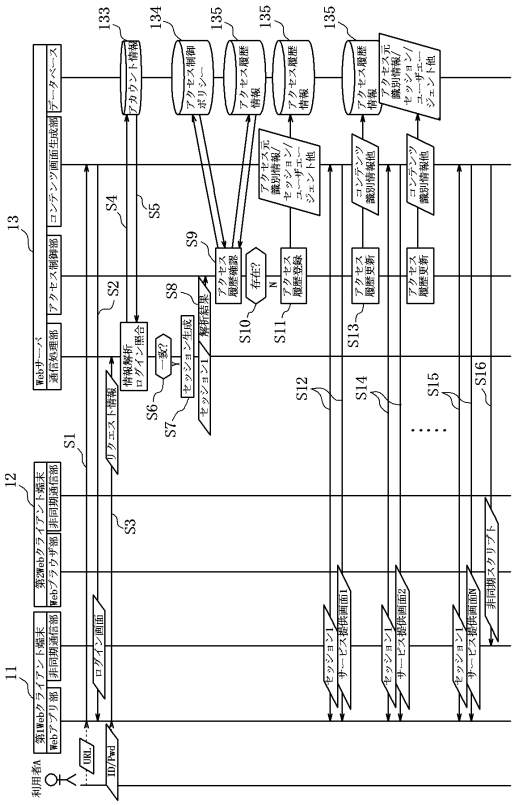
【図３】


12
第2Webクライアント端末
Web通信
123a
ユーザI/F
124a
表示装置
122
通信制御部
非同期通信部
1221
123
ユーザI/F制御部
124
表示制御部
121
制御部(Webブラウザ部)
1211
Webプロトコル処理部
1212
認証情報処理部
1213
リクエスト情報生成部
1214
Web表示制御部
125
記憶部

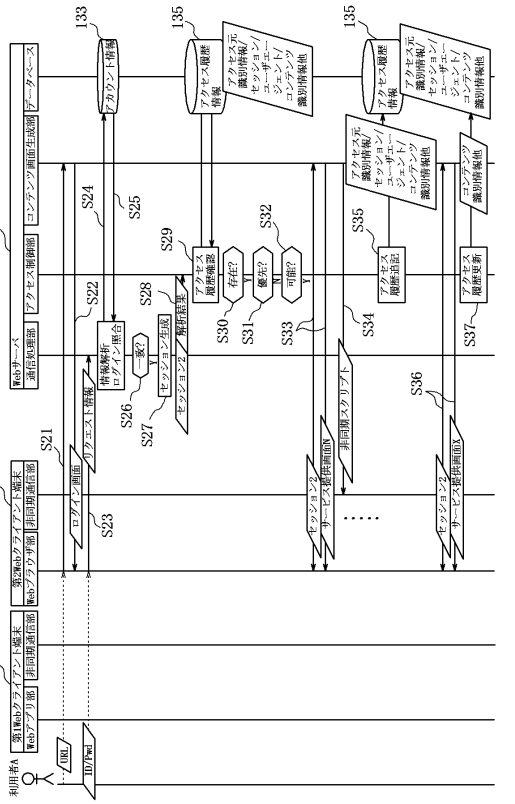
【図４】


13
131
制御部
通信処理部
1311
Webプロトコル処理部
1312
リクエスト情報解析部
アクセス制御部
1314
アクセス履歴管理部
1313
1315
コンテンツ画面生成部
132
通信制御部
Web通信
133
アカウント情報データベース
134
アクセス制御ポリシー情報データベース
135
アクセス履歴情報データベース
136
コンテンツデータベース
記憶部
137
Webサーバ

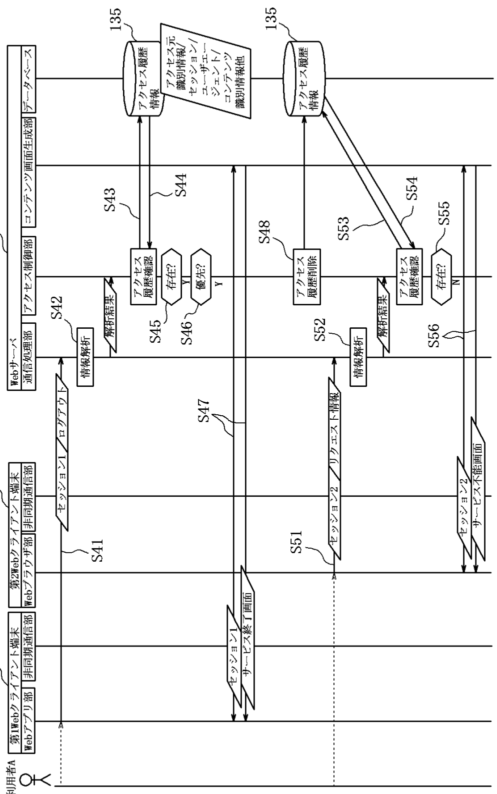
【図５】


利用者A
11
第1Webクライアント端末
Webアプリ部
非同期通信部
ID/Pwd
URL
12
第2Webクライアント端末
Webブラウザ部
非同期通信部
13
Webサーバ
通信処理部
アクセス制御部
コンテンツ画面生成部
データベース
ログイン画面
S1
S2
S3
S4
S5
S6
S7
S8
S9
S10
S11
S12
S13
S14
S15
S16
133
アカウント情報
134
アクセス制御ポリシー
135
アクセス履歴情報
情報解析ログイン照合
一致?
セッション生成
セッションID
解析結果
アクセス履歴登録
存在?
アクセス履歴登録
アクセス履歴更新
アクセス元識別情報/セッションID/ユーザエージェント/コンテンツ識別情報他
コンテンツ識別情報他
セッションID
サービス提供画面1
サービス提供画面2
サービス提供画面N
非同期スクリプト

【図６】


利用者A
11
第1Webクライアント端末
Webアプリ部
非同期通信部
ID/Pwd
URL
12
第2Webクライアント端末
Webブラウザ部
非同期通信部
13
Webサーバ
通信処理部
アクセス制御部
コンテンツ画面生成部
データベース
ログイン画面
S21
S22
S23
S24
S25
S26
S27
S28
S29
S30
S31
S32
S33
S34
S35
S36
S37
133
アカウント情報
135
アクセス履歴情報
情報解析ログイン照合
一致?
セッション生成
セッションID
解析結果
アクセス履歴登録
存在?
Y
N
要元?
可能?
アクセス履歴登記
アクセス履歴更新
アクセス元識別情報/セッションID/ユーザエージェント/コンテンツ識別情報他
コンテンツ識別情報他
セッションID
サービス提供画面1
サービス提供画面2
非同期スクリプト

【図７】



【図８】

アクセス制御ポリシー情報

アクセス元識別情報＝アカウントＩＤ、
#
#　※アクセス元識別情報＝アカウントＩＤ.ユーザエージェント情報　あるいは、ログインＩＤ(共通ＩＤでない)　の場合、
#　　ＷＥＢクライアント１および２のアクセス元識別情報は異なる。よって両者でＷＥＢコンテンツを区別して利用することはできない

アクセス優先順位＝ユーザエージェント情報:"WEB-Browser1">"WEB-App1">"WEB-Browser2",認証手段識別情報:"01">"02"
#
#　例)
#　１位：パソコン(WEB-Browser1)＋ＩＣカード認証(1)
#　２位：携帯電話(WEB-App1)＋ＩＣカード認証(1)
#　３位：携帯電話(WEB-App1)＋ＩＤ／パスワード認証(2)
#　４位：デジタルテレビ(WEB-Browser2)＋ＩＤ／パスワード認証(2)

コンテンツ利用可否制限＝allow("Service[0-9A-Z] [0-9] [0-9]*"@1),allow("Service[N] [0-9] [0-9]*"@4),allow("Service[0-9X-Z] [0-9] [0-9]*"@.),deny("Service[0-9A-Z] [0-9] [0-9]*"@.)
#
#　allow | deny(コンテンツ識別情報(正規表現)@アクセス優先順位(正規表現)),…
#　例) 利用可能なコンテンツ
#　パソコン＋ＩＣカード認証　　　　：全てのＷＥＢコンテンツ
#　携帯電話＋ＩＣカード認証　　　　：全てのＷＥＢコンテンツ
#　携帯電話＋ＩＤ／パスワード認証　：一部のＷＥＢコンテンツ
#　デジタルテレビ＋ＩＤ／パスワード認証：一部のＷＥＢコンテンツ

【図９】

アクセス履歴情報

アクセス履歴ＩＤ	アクセス元識別情報	セッション情報	ユーザエージェント情報	コンテンツ識別情報	認証手段識別情報	アクセス日時情報
UserA2010000000	UserA	Session1	WEB-App1	ServiceNxxxxxxx	01	Fri. 1-Jan 2010 00:00:00 GM
UserA2010001000	UserA	Session2	WEB-Browser2	ServiceXxxxxxxx	02	Fri. 1-Jan 2010 00:10:00 GM

【図１０】

（ａ）

アカウント情報

アカウントＩＤ	ログイン１	ログイン２
UserA	UserA-Login1	UserA-Login2
・・・	・・・	・・・

（ｂ）

アカウントＩＤ	ログインＩＤ	パスワード	利用環境情報	認証手段
UserA	UserA-Login1	UserA-Login1-Pwd	WEB-App1xxxxxxxxx	01
UserA	UserA-Login2	UserA-Login2-Pwd	WEB-Browser2xxxxxxxx	02

フロントページの続き

審査官　平井　誠

(56)参考文献　特開２００３－０３０１５４（ＪＰ，Ａ）
特開２００５－１８２２９１（ＪＰ，Ａ）
特開２００７－００４６５０（ＪＰ，Ａ）
特開２００７－２４１５９０（ＪＰ，Ａ）
特開２００５－１２２６５１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１