(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2010-27028
(P2010-27028A)
(43)公開日　平成22年2月4日(2010.2.4)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330D	5B285
G06F 13/00	(2006.01)	G06F	13/00	510A	

審査請求 未請求　請求項の数 20　ＯＬ　（全 17 頁）

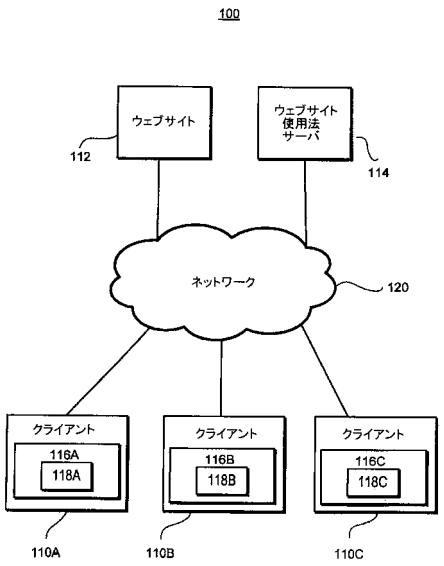
(21)出願番号　特願2009-40046(P2009-40046)
(22)出願日　平成21年2月23日(2009.2.23)
(31)優先権主張番号　12/175322
(32)優先日　平成20年7月17日(2008.7.17)
(33)優先権主張国　米国(US)

(71)出願人　504206263
シマンテック・コーポレーション
ＳＹＭＡＮＴＥＣ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　カリフォルニア州９５０１４　クパチーノ，スティーブンズ・クリーク・ブルバード，２０３３０
(74)代理人　100077539
弁理士　飯塚　義仁
(74)代理人　100114742
弁理士　林　秀男
(74)代理人　100125265
弁理士　貝塚　亮平

最終頁に続く

(54)【発明の名称】制限された認証証明書のオンラインストレージを介したウェブサイト使用の制御

(57)【要約】　（修正有）
【課題】ユーザが現在使っているコンピュータに無関係にウェブサイトへの該ユーザのアクセスを制御する。
【解決手段】クライアントは、ウェブサイトでアカウントにアクセスするためにネットワークを介してウェブサイト使用法サーバとコミュニケートする。クライアントは、ウェブサイト上のアカウントへのユーザアクセスが認められるかどうかの指示をリクエストする。ウェブサイト使用サーバは、ウェブサイト使用法がウェブサイトと利用者に関連するウェブサイト使用法規定の少なくとも一部に基づいて認められるかどうかを決定する。ウェブサイト使用法サーバは、アカウントへのアクセスが認められることを決定するのに応じて、ウェブサイトに限定された認証証明書を提供する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ウェブサイトへのユーザアクセスを制御するためのコンピュータによって実行される方法であって、
ウェブサイトの利用者に関連付けられたアカウントにアクセスするためにクライアントからリクエストを受け取ることと、
前記ウェブサイト及び前記利用者に関連付けられたウェブサイト使用法規定を特定することと、
前記アカウントへのアクセスがウェブサイト使用法規定の少なくとも一部に基づいて認められるかどうかを決定することと、
前記アカウントへのアクセスがウェブサイト使用法規定の少なくとも一部に基づいて認められるとの決定に応じて、前記利用者と前記ウェブサイトに関連付けられた制限された認証証明書をクライアントへ提供すること
を具える方法。
【請求項２】
前記アカウントへのアクセスが認められるかどうかを決定することは、
前記ウェブサイト使用法規定によって指定されたウェブサイト使用法パラメータを特定することと、
前記アカウントへのアクセスが認められるかどうかを決定するためにウェブサイト使用法パラメータを評価すること
を具える、コンピュータによって実行される請求項１の方法。
【請求項３】
前記ウェブサイト使用法パラメータは、前記アカウントへのユーザアクセスが認められる時刻を指定するものである、コンピュータによって実行される請求項２の方法。
【請求項４】
前記ウェブサイト使用法パラメータは、前記アカウントへのユーザアクセスが認められる割り当てられた時間を指定するものである、コンピュータによって実行される請求項２の方法。
【請求項５】
ウェブサイト使用法パラメータは、前記アカウントへのユーザアクセスが認められる離散的な時間の回数を指定するものである、コンピュータによって実行される請求項２の方法。
【請求項６】
さらに、
前記アカウントへのアクセスが前記ウェブサイト使用法規定の少なくとも一部に基づいて認められないとの決定に応じて、エラーメッセージをクライアントへ提供すること
を具える、コンピュータによって実行される請求項１の方法。
【請求項７】
前記制限された認証証明書は前記アカウントへのパスワードを含む、コンピュータによって実行される請求項１の方法。
【請求項８】
さらに、
前記アカウントへのアクセスが認められるとの決定に応じて、ウェブサイトに関連するログアウトメカニズムを決定することと、ここで、前記ログアウトメカニズムは前記アカウントから利用者をログアウトするための情報を含み、
前記クライアントに前記決定されたログアウトメカニズムを提供すること
を具える、コンピュータによって実行される請求項１の方法。
【請求項９】
クライアントからウェブサイトへのユーザアクセスを制御するためにコンピュータによって実行されるプログラムであって、

コンピュータに、
ウェブサイトでアカウントにアクセスするためのユーザリクエストを検出する手順と、
ウェブサイト使用法規定がウェブサイトで利用者が該アカウントにアクセスすることを認めるかどうかの指示を、ウェブサイト使用法サーバにリクエストする手順と、
ウェブサイト使用法規定が該アカウントへのアクセスを認めるとの前記ウェブサイト使用法サーバの決定に応じて、該ウェブサイト使用法サーバから当該アカウントのための制限された認証証明書を受け取る手順と
を実行させるためのモニタリングモジュールと、
前記ウェブサイトに関係するウェブサイト使用法規定を執行するように構成された執行モジュールであって、前記受け取った制限された認証証明書を前記ウェブサイトに提供する手順をコンピュータに実行させるように構成されたログインモジュールを具える前記執行モジュールと
を具えるコンピュータプログラム。
【請求項１０】
前記執行モジュールは、前記ウェブサイト使用法規定が前記アカウントへのアクセスを認めないとの前記ウェブサイト使用法サーバの決定に応じて、前記ウェブサイトにおける前記アカウントから利用者をログアウトする手順をコンピュータに実行させるように構成されたログアウトモジュールをさらに具える、請求項９のコンピュータプログラム。
【請求項１１】
前記ログアウトモジュールは、更に、前記ウェブサイト使用法規定の少なくとも一部に基づいて、一度に、前記ウェブサイトに関連するブラウザセションを終了させることあるいはログアウトウェブページをロードすることによって、前記ウェブサイトにおける前記アカウントから利用者をログアウトする手順をコンピュータに実行させるように構成されている、請求項１０のコンピュータプログラム。
【請求項１２】
前記ログアウトモジュールは、更に、利用者に前記制限された認証証明書を決定することを防ぐために、前記ウェブサイトのためのログアウト手順をコンピュータに実行させるように構成されている、請求項１０のコンピュータプログラム。
【請求項１３】
前記執行モジュールは、更に、利用者が前記アカウントにアクセスすることを中止することに応じて、前記ウェブサイトに関連するデータクリーンアップ行動をコンピュータに実行させるように構成されている、請求項９のコンピュータプログラム。
【請求項１４】
前記モニタリングモジュールは、更に、前記アカウントへのアクセスが認められないとの前記ウェブサイト使用法サーバの決定に応じて、該ウェブサイト使用法サーバからエラーメッセージを受け取る手順をコンピュータに実行させるように構成されている、請求項９のコンピュータプログラム。
【請求項１５】
前記モニタリングモジュールは、更に、
前記制限された認証証明書に関連する制限されたウェブページにアクセスしようと試みる利用者を検出する手順と、
前記制限されたウェブページへのアクセスを阻止する手順と
をコンピュータに実行させるように構成されている、請求項９のコンピュータプログラム。
【請求項１６】
前記ログインモジュールは、更に、利用者に前記認証証明書を決定するのを防ぐようなやり方で前記ウェブサイトに前記制限された認証証明書を自動的に提供する手順をコンピュータに実行させるように構成されている、請求項９のコンピュータプログラム。
【請求項１７】

ウェブサイトへのユーザアクセスを制御するためのコンピュータによって実行されるシステムであって
コンピュータプロセッサと、
前記コンピュータプロセッサで実行するように構成されたコンピュータプログラムモジュールを記憶するコンピュータ読み取り可能な記憶媒体とを具えてなり、
コンピュータプログラムモジュールは、
ウェブサイトの利用者に関連付けられたウェブサイト使用法規定を定義するように構成された規定決定モジュールと、
前記ウェブサイト使用法規定を記憶するように構成された規定データベースと、
前記利用者及び前記ウェブサイトに関連付けられたアカウントのための制限された認証証明書を記憶するように構成された証明書データベースと、
前記ウェブサイトの利用者に関連付けられたアカウントにアクセスするためのリクエストをクライアントから受け取り、
前記ウェブサイト使用法規定の少なくとも一部に基づいて前記アカウントへのアクセスが認められるかどうかを決定し、そして
前記ウェブサイト使用法規定の少なくとも一部に基づいて前記アカウントへのアクセスが認められるとの決定に応じて、クライアントへアカウントのための制限された認証証明書を提供する、
ように構成された決定モジュールと
を具えることを特徴とするシステム。
【請求項１８】
前記決定モジュールは、更に、
前記ウェブサイト使用法規定によって指定されたウェブサイト使用法パラメータを確認し、そして、
前記アカウントへのアクセスが認められるかどうかを決定するために前記ウェブサイト使用法パラメータを評価する
ように構成されていることを特徴とする請求項１７のシステム。
【請求項１９】
前記ウェブサイト使用法パラメータを評価することは、前記アカウントへのユーザアクセスが認められる時刻を現時刻と比較することを含む、請求項１８のシステム。
【請求項２０】
前記決定モジュールは、さらに、
前記ウェブサイトに関連付けられたログアウトメカニズムを決定し、ここで、前記ログアウトメカニズムは、前記アカウントへのアクセスが認められるとの決定に応じて、利用者を該アカウントからログアウトするための情報を含み、そして、
クライアントへログアウトメカニズムを提供する
ように構成されている、請求項１７のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して、ウェブサイト使用法の分野に関し、特に、ウェブサイトへのアクセスを制御することに関する。
【背景技術】
【０００２】
典型的なインターネットユーザは一般に、いろいろなウェブサイトへ無制限にアクセスする。この無制限なアクセスのため、インターネットユーザはウェブサイトをブラウズするのに途方もない時間を費やすかもしれない。若干のユーザにとってウェブサイトをブラウズするのに１日を費やすことはすばらしいことかもしれないが、ウェブサイトへのユーザアクセスを制限するのが望ましい状況がある。
【０００３】

例えば、学校は、学校にいてネットワーク上の友達と付き合っていない間に、子供たちが学んでいることを保障するソーシャルネットワーキングウェブサイトのような特定のウェブサイトへのアクセスを制限することを望むかもしれない。同じく、会社においての従業員は、仕事をしている間に可能な限り能率的で生産的であることを保証する制限された特定のウェブサイトへアクセスするかもしれない。

【０００４】

最新のウェブサイトアクセスコントロールは典型的に一つのコンピュータにインストールされ、そして子供の親のようなシステム管理者に、利用者がそのコンピュータを使っている間、ウェブサイトへのユーザアクセスを制御することを認める。しかしながら、アプリケーションはそのアプリケーションがインストールされた特定の機器でウェブサイトへのユーザアクセスを制御できるだけであるから、このようなアプリケーションはウェブサイトへのユーザのアクセスについて制限された制御しか持たない。多くのインターネットユーザが１以上のコンピュータへアクセスするように、ユーザは異なるコンピュータを使うことによってアクセス制御を避けることができる。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

したがって、ユーザが現在使っているコンピュータに無関係にウェブサイトへの該ユーザのアクセスを制御するための方法が必要である。

【課題を解決するための手段】

【０００６】

上記のそしてその他の課題は、ユーザがウェブサイトをブラウズするのに現在使っているコンピュータに無関係に、ウェブサイトのユーザアクセスを制御するようにした方法、コンピュータによって実行されるシステム、若しくは、コンピュータプログラムによって処理される。方法の一実施例は、ウェブサイトの利用者に関連付けられたアカウントにアクセスするためのリクエストを、クライアントから受け取る。その方法は、ウェブサイトと利用者に関連するウェブサイト使用法規定を特定する。その方法は、アカウントへのアクセスがウェブサイト使用法規定の少なくとも一部に基づいて認められるかどうかをさらに決定する。アカウントへのアクセスがウェブサイト使用法規定の少なくとも一部に基づいて認められることを決定するのに応じて、その方法はクライアントへ利用者とウェブサイトに関連する制限された認証証明書を提供する。

【０００７】

コンピュータによって実行されるシステムの実施例は、コンピュータプロセッサと、コンピュータプロセッサで実行するように構成されたコンピュータプログラムモジュールを記憶するコンピュータ読み取り可能な記憶媒体とを具える。コンピュータプログラムモジュールは、ウェブサイトの利用者に関連したウェブサイト使用法規定を定義するように構成された規定決定モジュールを具える。コンピュータプログラムモジュールは、ウェブサイト使用法規定を記憶するための規定データベースをさらに具える。さらに、コンピュータプログラムモジュールは、利用者とウェブサイトに関連する制限された認証証明書を記憶するように構成された証明書データベースを具える。コンピュータプログラムモジュールは、クライアントからウェブサイトの利用者に関連するアカウントにアクセスするためのリクエストを受け取るように構成された決定モジュールをさらに具える。決定モジュールは、アカウントへのアクセスがウェブサイト使用法規定の少なくとも一部に基づいて認められるかどうかをさらに決定する。アカウントへのアクセスがウェブサイト使用法規定の少なくとも一部に基づいて認められることを決定するのに応じて、決定モジュールはクライアントへ利用者とウェブサイトに関連する制限された認証証明書を提供する。

【０００８】

コンピュータプログラムの実施例は、クライアントからウェブサイトへのユーザアクセスを制御するためのコンピュータが実行可能なコードを記憶したコンピュータが読み取り可能な記憶媒体を持ち、モニタリングモジュールを具えたコードはウェブサイトでアカウ

ントにアクセスするためのユーザリクエストを検出するように構成される。モニタリングモジュールは、ウェブサイト使用法規定がウェブサイトで利用者が該アカウントにアクセスすることを認めるかどうかの指示を、ウェブサイト使用法サーバにリクエストし、そして、ウェブサイト使用法規定が該アカウントへのアクセスを認めるとの前記ウェブサイト使用法サーバの決定に応じて、該ウェブサイト使用法サーバから当該アカウントのための制限された認証証明書を受け取る物。プログラムは、ウェブサイトに関連するウェブサイト使用法規定を実施するように構成された執行モジュール、受け取った制限された認証証明書をウェブサイトへ提供するように構成されたログインモジュールを含んでなる執行モジュールをさらに具える。

【図面の簡単な説明】

【０００９】

【図１】一実施例に基づくコンピュータ環境の高レベルのブロックダイアグラム。

【００１０】

【図２】ウェブサイト使用法サーバ、クライアント、及び／又はウェブサイトを提供しているウェブサーバとして使用するための主要なコンピュータを示す高レベルのブロックダイアグラム。

【００１１】

【図３】一実施例に基づくウェブサイト使用法サーバの詳細な概要を示す高レベルのブロックダイアグラム。

【００１２】

【図４】一実施例に基づく制御モジュールの詳細な概要を示す高レベルのブロックダイアグラム。

【００１３】

【図５】ウェブサイトへのユーザアクセスをコントロールするために制御モジュールにより実行されるステップを示すフローチャート。

【００１４】

【図６】ウェブサイトへのユーザアクセスを制御するためにウェブサイト使用法サーバにより実行されるステップを示すフローチャート。

【００１５】

上記図面は、説明の目的のためだけにこの発明の実施例を描写する。当業者は、ここで説明する発明の本質から逸脱せずに、図解及び記述された階層構造、方法、機能について他の実施例を用いることが可能であることを、以下の説明から容易に理解するであろう。

【発明を実施するための形態】

【００１６】

図１は、一実施例に基づくコンピュータ環境１００の高レベルのブロックダイアグラムである。図１は、ネットワーク１２０によってウェブサイト１１２とウェブサイト使用法サーバ１１４に接続された３つのクライアント１１０を示す。３つのクライアント１１０と１つのウェブサイト１１２だけが、説明を単純にそして明確にするために図１に示される。コンピュータ環境１００の実施例は、ネットワーク１２０へ接続された何千あるいは何百万というクライアント１１０及び／又はウェブサイト１１２を持つことができる。説明を簡略化するために、図で示した「ウェブサイト」は一つのウェブサイトまたは複数のウェブサイトのどちらかを表す。

【００１７】

図１とその他の図は、同様の構成を特定するために類似の参照数字を使う。「１１０Ａ」のような、参照数字の後の文字は本文が明確にその特定の参照数字を持つ構成を参照することを示す。「１１０」のような、次の文字がない本文中の参照数字は、その参照数字を生み出す図中における要素のいずれかすべてを参照する（例えば、本文中の「１１０」は図中の参照数字「１１０Ａ」、「１１０Ｂ」及び／又は「１１０Ｃ」を参照する）。

【００１８】

一般に、ウェブサイト１１２はウェブサーバに記憶された１以上のウェブページの蓄積

物を含む。図示されたウェブサイト１１２は、ネットワーク１２０で利用可能な種々のウェブサイトを表す。例えば、ウェブサイト１１２はユーザが相互に作用する社会ネットワーキングウェブサイト、ユーザがビデオを見る映像エンターテイメントウェブサイト、あるいは異なるスポーツの話題に関係したスポーツウェブサイトであるかもしれない。ユーザは、ウェブサイト１１２でアカウントを持つことができる。サービスにアクセスするための（すなわち認証する）彼または彼女のアカウント内のユーザログは、ウェブサイト１１２によって提供される。ログインするために、ユーザはユーザ名とパスワードのような認証証明書を提供しなくてはならない。これらの証明書なしでは、ユーザはウェブサイト１１２によって提供された限定されたサービスのセットだけにアクセスすることが可能であるかもしれない。

【００１９】

クライアント１１０は、ネットワーク１２０のウェブサイト１１２にアクセス（ブラウズ）するためにユーザによって使われる。クライアント１１０は、例えば、パーソナルコンピュータ、パーソナルデジタルアシスタント（ＰＤＡ）、あるいは携帯電話であり得る。一実施例において、ウェブサイト１１２へのユーザのアクセスは、ウェブサイト使用法管理者（「アドミニストレータ」）によって管理される。１つの例で、ユーザは子供でありそして管理者はその子供の親である。他の例で、ユーザは会社の従業員あるいは企業の他のメンバーでありそして管理者はユーザのボスである。同様に、ユーザは学生でありそして管理者は教師であり得る。

【００２０】

一実施例において、クライアント１１０は、ネットワーク１２０のウェブサイト１１２からウェブページや他のコンテンツを検索し表示することをユーザに許可するマイクロソフトインターネットエクスプローラのようなウェブブラウザ１１６を実行する。クライアント１１０は、ユーザの管理者によって確立されたウェブサイト使用法規定に従ってウェブサイトへのユーザのアクセスを制限する制御モジュール１１８を実行する。例えば、制御モジュール１１８はブラウザプラグイン、ブラウザヘルパーオブジェクト（ＢＨＯ）、スタンドアローンアプリケーション、他のアプリケーションの一部であってよく、あるいはオペレーティングシステムへ組み込まれていてもよい。

【００２１】

ウェブサイト使用法サーバ１１４は、アドミニストレータによって確立されたウェブサイト使用法規定を記憶し、そしてクライアント１１０の制御モジュール１１８へその規定と関連情報とを提供する。ウェブサイト使用法規定は、制限されたウェブサイト１１２へのユーザのアクセスをコントロールするウェブサイトアクセスパラメータの１セットである。ウェブサイト使用法規定は、時間、離散的なアクセス数に基づいた制限事項、及び／又はこれらの基準あるいは他の基準の組み合わせを指定することができる。例えば、アクセスが許可されたとき、規定は時間間隔、許可されたアクセスの合計時間、及び／又は与えられた時間間隔内で認められた離散的なアクセス合計数を提示することができる。所定の規定は、１以上のユーザ及び／又は１以上のウェブサイト１１２に関連付けられ得る。

【００２２】

一実施例において、制限されたウェブサイト１１２へのアクセスは、ウェブサイト１１２のための認証証明書のいくつかあるいはすべてをユーザが知ることを防ぐことによって制御される。ユーザに知られていない証明書は、「制限された証明書」として参照される。例えば、ウェブサイト１１２においてユーザのアカウントのためのパスワードは制限され得る。そのために、ユーザは制限された証明書を知ることなくアカウントにログインすることは不可能である。

【００２３】

ウェブサイト使用法サーバ１１４は、制限された証明書を記憶する。ユーザがブラウザ１１６を制限されたウェブサイト１１２にアクセスするために使うとき、制御モジュール１１８はウェブサイト使用法サーバ１１４と連絡を取り、そしてウェブサイトの使用法規定に従ってアクセスが認められるかどうかを決定する。もしアクセスが認められるなら、

ウェブサイト使用法サーバ１１４と制御モジュール１１８は、制限された証明書を使ってユーザをウェブサイト１１２にログインするために動作する。さらに、一旦ユーザがウェブサイトを去ると、自発的にまたは使用法規定に基づいて、使用法サーバ１１４と制御モジュール１１８は、クッキーのような、制限された証明書を学ぶためにユーザが使うかもしれないクライアント１１０に記憶されたどんな情報をも削除するために動作する。

【００２４】

ウェブサイト使用法サーバ１１４にウェブサイト使用法規定と制限された証明書を記憶することは、どこにユーザが位置づけられたかにかかわらず、ウェブサイト１１２へのユーザアクセス制御を認める。ユーザは家にある、学校にある、友達の家にある、あるいは他のいかなる場所にあるクライアント１１０を使用できる、そしてユーザは制限されたウェブサイト１１２へのアクセスを得るためにウェブサイト使用法サーバ１１４と相互に作用しなければならない。

【００２５】

ネットワーク１２０はクライアント１１０、ウェブサイト使用法サーバ１１４とウェブサイト１１２の間に情報伝達経路を表す。一実施例において、ネットワーク１２０はインターネットである。ネットワーク１２０はまた、必ずしもインターネットの一部でない専用のあるいは私的な通信回線を活用することができる。一実施例において、ネットワーク１２０は標準的な通信技術及び／又はプロトコルを使う。それで、ネットワーク１２０は、イーサネット（登録商標）、８０２.１１、総合ディジタル通信網サービス（ISDN）、ディジタル加入者線（DSL）、非同期転送モード（ATM）、その他のような技術を使った経路を含み得る。同様に、ネットワーク１２０で使用されるネットワーク通信プロトコルは、転送制御プロトコル/インターネットプロトコル（TCP/IP）、ハイパテキスト転送プロトコル（HTTP）、簡易メール転送プロトコル（SMTP）、ファイル転送プロトコル（FTP）などを含み得る。ネットワーク１２０で交換されたデータは、ハイパテキストマーク付け言語（HTML）、拡張マーク付け言語（XML）などを含んでなる技術及び／又はフォーマットを使って表される。さらに、すべてあるいは若干の経路は、セキュアソケットレイヤー（SSL）、セキュアHTTP及び／又はバーチャルプライベートネットワーク（VPNs）のような従来の暗号化技術を使って暗号化され得る。他の実施例において、構成要素は上記したものの代わりにあるいは上記したものに加えてカスタム及び／又は専用のデータ通信技術を使うことができる。

【００２６】

図２は、ウェブサイト使用法サーバ１１４、クライアント１１０、及び／又はウェブサイト１１２を提供しているウェブサーバとして使用するための主要なコンピュータ２００を説明する高レベルのブロックダイアグラムである。図は、バス２０４へつながれたプロセッサ２０２である。同じくバス２０４につながれるのは、メモリ２０６、記憶媒体２０８、キーボード２１０、グラフィックスアダプタ２１２、ポインティングデバイス２１４、そしてネットワークアダプタ２１６である。ディスプレイ２１８は、グラフィックスアダプタ２１２につながれる。

【００２７】

プロセッサ２０２は、インテル x86 互換ＣＰＵのような汎用プロセッサであるかもしれない。記憶媒体２０８は、一実施例において、ハードディスク装置また書き込み可能なコンパクトディスク（ＣＤ）あるいはＤＶＤ、又は半導体メモリデバイスのような、データを記憶することができる他のいかなるデバイスであり得る。メモリ２０６は、例えば、ファームウェア、読出し専用メモリ（ROM）、不揮発性ランダムアクセスメモリ（NVRAM）、及び／又はＲＡＭであるかもしれず、そしてプロセッサ２０２によって使用された命令とデータを保留する。ポインティングデバイス２１４はマウス、トラックボール、あるいは他のタイプのポインティングデバイスであるかもしれず、そしてコンピュータ２００にデータを入力するためのキーボード２１０と組み合わされて使われる。グラフィックアダプタ２１２は、ディスプレイ２１８に画像と他の情報を表示する。ネットワークアダプタ２１６は、ネットワーク１２０にコンピュータ２００をつなげる。

【００２８】
当該技術分野で周知であるように、コンピュータ２００はコンピュータプログラムモジュールを実行することに適応している。ここに使われるように、用語「モジュール」は指定の相関関係を提供するためのコンピュータプログラムロジック及び／又はデータを示す。モジュールはハードウェア、ファームウェア、及び／又はソフトウェアに実装され得る。一実施例において、モジュールは記憶装置２０８に記憶されて、メモリ２０６にロードされ、そしてプロセッサ２０２により実行される。
【００２９】
図１の構成要素によって利用されたコンピュータ２００のタイプは、実施例と構成要素により利用された処理能力によって異ならせることができる。例えば、典型的には移動電話であるクライアント１１０は限定的な処理能力、小さなディスプレイ２１８を持ち、そしてポインティングデバイス２１４を欠いているかもしれない。ウェブサイト使用法サーバ１１４は、対照的に、ここに記述された相関関係を提供するために一緒に動作する複数のブレードサーバを具えるかもしれない。
【００３０】
図３は、一実施例に基づくウェブサイト使用法サーバの詳細な概要を説明する高レベルのブロックダイアグラムである。図３に示されるように、ウェブサイト使用法サーバ１１４は複数のモジュールを含む。ウェブサイト使用法サーバ１１４の他の実施例は、ここで説明されたものより異なった及び/又は他のモジュールを持つことができ、そして相関関係は異なる方法でモジュール間に分配され得る。
【００３１】
規定決定モジュール３００は、ユーザとウェブサイト１１２とを関連付けるウェブサイト使用法規定を決定する。上述したように、ウェブサイト使用法規定は、１つ以上の制限されたウェブサイト１１２へのユーザのアクセス条件を指定する。規定は、アクセスが許されている又は許されていない時を指定することによる時間に基づいてウェブサイト１１２へのアクセスを制限することができる。例えば、ウェブサイト使用法規定は、週末の午後１時００分から午後５時００分までの間、及び／又は平日の午後７時００分から午後８時００分までの間にウェブサイト１１２にユーザはアクセスすることが認められているだけであることを示唆することができる。
【００３２】
さらに、規定は許可されたアクセスの合計時間に基づいてアクセスを制限できる。許可されたアクセスの合計時間は、ユーザがウェブサイト１１２へのアクセスを許可された割り当て時間を示す。例えば、ウェブサイト使用法規定は、ユーザが毎日２時間だけウェブサイト１１２にアクセスしてもよい、あるいはユーザが平日に２時間だけそして週末に無制限の時間ウェブサイト１１２にアクセスしてもよいことを示すことができる。
【００３３】
規定はまた、多くの許可されたアクセスに基づいてアクセスを制限することができる。許可されたアクセスの数は、ユーザがウェブサイト１１２へのアクセスを認められた個々の回数を示す。例えば、ウェブサイト使用法規定は、ユーザが１日に合計３回又は１週間に７回ウェブサイト１１２へアクセスすることを単に認められるだけであることを明示することができる。ウェブサイト使用法規定はまた、これらの基準の組み合わせに基づきアクセスを制限することができる。例えば、ウェブサイト使用法規定は、平日の午後５時から午後９時まで、ただし２時間の合計割り当て時間の間だけ、ユーザはウェブサイト１１２にアクセスできるだけであることを示すことができる。
【００３４】
さらなる実施例において、ウェブサイト使用法規定は、ユーザがアクセスを許可されていないウェブサイト１１２の制限されたウェブページを指定することができる。規定は、ユーザがアクセスできない特定のページ及び／又はページの特性を識別できる。例えば、規定は、制限された認証証明書を変更することをユーザに表示するかあるいは認めるウェブサイト１１２の特定ページにアクセスすることを認められていないユーザを指定できる

。同じく、規定は、ページに現れるときに、そのページを利用者にアクセスできなくするべきである特定の用語を指定できる。一実施例において、規定定義モジュール３００は、管理者によって設定されたウェブサイト使用法規定を記憶する規定データベース３０１を含む。

【００３５】

証明書データベース３０７は、ユーザの制限された認証証明書を記憶する。一実施例において、制限された証明書はパスワードである。それで、制限された証明書データベース３０７は、関連したウェブサイト使用法規定を持つユーザのためにウェブサイトにおけるアカウントのためのパスワードを記憶する。他の実施態様において他の制限された証明書が記憶される。さらに、ユーザ名のような制限されていない証明書もまた、一実施例において証明書データベース３０７に記憶される。

【００３６】

ユーザインタフェース（ＵＩ）モジュール３０２は、ユーザ及び／又は管理者にウェブサイト使用法サーバ１１４と相互にやりとりすることを許可する。一実施例において、ＵＩモジュール３０２は１以上のウェブページを供給するウェブサーバを含む。これらのページは、例えば使用規定が関係するウェブサイトとユーザを指定すること、ウェブサイトとユーザのためのウェブサイト使用法規定を規定すること、制限されたそして無制限の認証証明書を見ることそして編集すること等のような機能を実行するのを許可する。例えば、ウェブサイト使用法管理者は、使用規定が適用されるユーザを識別する、そのユーザのために制限されたウェブサイトを識別する、そして制限されたウェブサイトのために認証証明書を供給するといったような行動を実行するためにＵＩモジュール３０２によって提供されたＵＩを使うことができる。

【００３７】

一実施例において、ウェブサイト使用法管理者とユーザのいずれもが、ウェブサイト１１２のための制限された認証証明書を知らない。このような実施例で、管理者は制限された証明書を生成し記憶するためにＵＩモジュール３０２を使うことができる。これらの証明書は新しいアカウントが確立されるか、または証明書変更プロセスを経由したときにウェブサイト１１２へ供給される、故にユーザの認証証明書はウェブサイト使用法サーバ１１４によって生成された証明書を含んでいる。

【００３８】

ログアウトデータベース３０９は、ウェブサイト１１２のためのログアウトメカニズムを記述しているデータを記憶する。ログアウトメカニズムは、ウェブサイト１１２上のアカウントからユーザをログアウトするためのテクニック及び関連する情報である。したがって、ログアウトメカニズムは、ユーザのログアウトに関係しているウェブサイトの特定のウェブページの参照を含むことができる。さらに、ログアウトメカニズムは、例えばログアウトの際に消去するためにユーザのブラウザによって記憶された身元及び／又はクッキーの記載のような、ユーザがアカウントからログアウトするときに実行すべきデータ掃除の行動を指定できる。データ掃除の行動は、ユーザが制限された認証証明書を突き止めるためにクライアント１１０の残りのデータを調べることを防ぐことができる。一実施例において、ログアウトデータベース３０９の情報は、ウェブサイト使用法サーバ１１４のシステム管理者によって提供され維持される。

【００３９】

決定モジュール３０５は、規定がユーザに所定のウェブサイトへのアクセスを認めるかどうかを決定する。一実施例において、決定モジュール３０５は、クライアントの利用者がウェブサイト１１２にアクセスするのを認めるために、制限された認証証明書のためのリクエストをクライアント１１０における制御モジュール１１８から受け取る。決定モジュール３０５は、規定データベース３０１で適用できる規定を識別して、例えば現時刻、前のアクセス量及び／又は回数のような変数を考慮して規定を評価する。一実施例において、決定モジュール３０５はまた、ユーザの使用法規定を評価するために必要であるかもしれないということで、ユーザによって過去のウェブサイト使用法に関する情報を記憶す

る。

【００４０】

一実施例において、ウェブサイトアクセスが許可されることを決定するのに応じて、決定モジュール３０５は、ユーザがウェブサイト１１２でアカウントにログインできるように、規定データベース３０７から制御モジュール１１８までユーザの制限された認証証明書を伝える。一実施例において、ウェブサイト１１２に関連するウェブサイト使用法規定に従ってウェブサイト使用が認められないとの決定に応じて、決定モジュール３０５はユーザのクライアント１１０にエラーメッセージを供給する。エラーメッセージは、なぜウェブサイトへのアクセスが拒否されたかという理由を示す。例えば、エラーメッセージはユーザが規定によって許可されない時間にウェブサイト１１２でアカウントにアクセスしようと試みていることを提示することができる。

【００４１】

図４は、一実施例に基づく制御モジュールの詳細な概要を説明する高レベルのブロックダイアグラムである。図４に示されるように、制御モジュール１１８は複数のモジュールを含む。制御モジュール１１８の他の実施例は、ここで記述したものより異なった及び／又は他のモジュールを持つことができ、そしてその機能は異なった方法でモジュール間で分散され得る。

【００４２】

一実施例において、管理者はユーザが制限されたウェブサイト１１２を訪れようと試みる前に、クライアント１１０に制御モジュール１１８をインストールする。例えば、管理者は、クライアント１１０に制御モジュール１１８をダウンロードするために、ウェブサイト使用法サーバ１１４及び／又はネットワーク１２０上の他のサーバに接続するためにブラウザ１１６を使うことができる。こうして、ユーザは、管理者がそのクライアントについてまず最初に制御モジュール１１８をインストールするという用意がなされた、いずれかのクライアントから制限されたウェブサイト１１２にアクセスすることができる。

【００４３】

一実施例において、制御モジュール１１８は、例えば、ユーザに問い合わせることによって、ユーザの身元を得る。制御モジュール１１８は、その利用者のために制限されたウェブサイト１１２を識別するためにウェブサイト使用法サーバ１１４と相互に作用する。制御モジュール１１８内のモニタリングモジュール４００は、クライアント１１０でブラウザ使用法をモニターする。モニタリングモジュール４００は、あるユーザが制限されたウェブサイト１１２でアカウントにログインしたいという指示を検出する。一実施例において、モニタリングモジュール４００は、ウェブページがログインフォームを含んでいるかどうかを決定するために、ブラウザ１１６によって制限されたウェブサイト１１２からダウンロードされるウェブページを調べる。一実施例において、モニタリングモジュール４００は、「ユーザ名」と「パスワード」のようなフォームの中で特定のキーワードを検出することによってログインフォームを検出する。他の実施例において、モニタリングモジュール４００は、ウェブサイト１１２を支援するためのログインフォームのＵＲＬのリストを含み、かつ、該モジュールは、ブラウザがリストされたＵＲＬからページをダウンロードするときを検出する。

【００４４】

ユーザが制限されたウェブサイト１１２でアカウントにログインしたいという指示を検出すると、モニタリングモジュール４００は、当該ユーザのためのウェブサイト使用法規定が該ウェブサイトにアクセスを認めるかどうかを決定するためにウェブサイト使用法サーバ１１４と通信する。一実施例において、モニタリングモジュール４００は、ユーザの身元とユーザがアクセスしているウェブサイトの身元をウェブサイト使用法サーバ１１４に提供する。応答中に、モニタリングモジュール４００は、ウェブサイトのための制限された認証証明書（そして随意的に無制限の証明書）か、ウェブサイトへのアクセスが認められないことを示しているエラーメッセージのいずれかを受け取る。さらに、モニタリングモジュール４００は、使用法規定及び／又は制限されたウェブサイトに関する情報を受

け取る。この情報は、規定に従うアクセスの条件、例えば、次の９０分間許可されるアクセス、そして制限されたウェブサイトに適切などんなログアウトメカニズム、を含み得る。

【００４５】

もしエラーメッセージが受け取られるならば、モニタリングモジュール４００の実施例は、ウェブサイト１１２へのアクセスがなぜ否定されたかの説明を提供するためにユーザへエラーメッセージを提示する。例えば、エラーメッセージは、ユーザがウェブサイト１１２にアクセスを試みている時間がウェブサイト使用法規定に従っていないことをユーザに示すかもしれません。

【００４６】

モニタリングモジュール４００は、受け取った制限された認証証明書のどれをも、執行モジュール４０１に提供する。執行モジュール４０１は、当該規定によって認められたときにアクセスを許可することにより、また、当該規定によって指示されたときに既に許可されているアクセスを終わらせることにより、当該ウェブサイト使用法規定を執行する。例えば、ウェブサイト使用法規定が午後７時００分より前のウェブサイト使用を許可していると仮定して、午後６時３０分にユーザがアクセスをリクエストすることを想定する。その場合、執行モジュール４０１は最初の３０分間アクセスを許可し、それから午後７時００分にアクセスを終了する。

【００４７】

一実施例において、執行モジュール４０１はアクセスがウェブサイト使用法規定によって許可されるときに、ユーザを制限されたウェブサイト１１２にログインさせるためのログインモジュール４０２を含む。ログインモジュール４０２は、制限された証明書を含めて、ウェブサイト１１２のためのログインフォームに自動的に書き込むために、ユーザの認証証明書を使う。一実施例において、ログインモジュール４０２は、ユーザが制限された証明書を覚えるのを妨げるような方法で、ログインフォームに書き込む。例えば、ログインモジュール４０２は、制限された証明書をアステリスク（＊）であるいはユーザから情報を隠す他のキャラクタで表示させるようにしてよい。同様に、ログインモジュール４０２はブラウザ１１６と相互に作用して、そして利用者へログインフォーム（あるいは認証証明書）を示すことなく、直接ウェブサイト１１２へ認証証明書を提供することができる。

【００４８】

執行モジュール４０１は、アクセスがウェブサイト使用法規定によって許可されないときに、制限されたウェブサイト１１２からユーザをログアウトさせるためのログアウトモジュール４０３をさらに含む。一実施例において、ログアウトモジュール４０３は、執行モジュール４０１によってそうするように指示されたときに、ウェブサイト１１２のためにログアウトメカニズムを実行する。ログアウトメカニズムを実行することは、ユーザのブラウザ１１６に前記制限されたウェブサイトに対してログアウトページをリクエストさせることと、それによってウェブサイトからユーザを効果的にログアウトすることを含んでいてよい。ログアウトメカニズムを実行することはまた、ブラウザセションを終了すること及び／又はユーザをログアウトする他の行動を実行することを含み得る。一実施例において、ログアウトモジュール４０３は例えばウェブサイト１１２に関連したすべてのブラウザクッキーを消去するような、ログアウトの際の制限されたウェブサイトに関連したクリーンアップ行動を実行する。クリーンアップ行動は、ユーザが制限された認証証明書を割り出すことを防ぐ。

【００４９】

一実施例において、モニタリング４００と執行モジュール４０１は、ユーザがアクセスを得たウェブサイトでユーザが制限されたウェブページにアクセスするのを防ぐために相互作用する。モニタリングモジュール４００は、ユーザが制限されたウェブページにアクセスを試みていることを検出し、執行モジュール４０１に通知する。執行モジュール４０１は、順番に、ブラウザ１１６が制限されたページを表示するのを妨げて、その代わりに

それにエラーメッセージを表示させる。この方法で、モジュールは表示することができるウェブページにユーザがアクセスすることを防ぐか、あるいはユーザが制限された認証証明書を変えることを許可する。

【００５０】

一実施例において、モニタリングモジュール４００、執行モジュール４０１とウェブサイト使用法サーバ１１４は、ユーザとユーザの管理者にウェブサイト１１２でアカウントを確立することを許可するために相互作用する。モニタリングモジュール４００は、ウェブサイト使用法サーバ１１４に知られていないウェブサイト１１２のための新しいアカウントを確立するためにロードされたウェブページを検出する。次いで、執行モジュール４０１はブラウザ１１６がウェブページを表示することを許可する。ユーザと管理者は、パスワードのような制限された証明書以外のアカウントを作るために必要な情報を提供することができる。一実施例において、ウェブサイト使用法サーバ１１４は、アカウントの登録手続きを完了するために、ユーザと管理者の依頼により制限された証明書を自動的に生成し記憶する。生成された制限された証明書は、ユーザと管理者から秘密にしておくことができる。アカウントが作られた途端に、管理者は新しいアカウントと結びつくウェブサイト使用法規定を確立するため、あるいはサーバ生成証明書を変えるために、ウェブサイト使用法サーバ１１４と相互に作用することができる。

【００５１】

図５は、一実施例によるところのユーザのウェブサイト使用法をコントロールするための制御モジュール１１８（図１）により実行されるステップを説明するフローチャートである。他の実施例は、異なった命令で図示のステップを実行する、及び／又は異なるあるいは付加的なステップを実行する。さらに、ステップのいくつかあるいはすべてが制御モジュール１１８以外の構成要素によって実行され得る。

【００５２】

制御モジュール１１８は、クライアント１１０のウェブサイトブラウザ使用法をモニターする（５００）。制御モジュール１１８は、ユーザがブラウザ使用法からの制限されたウェブサイト１１２のアカウントにログインしたいという指示を検出する（５０１）。例えば、ブラウザ使用法は、ユーザがウェブサイト１１２でアカウントへアクセスしたいことを示すログインフォームと一緒に、ユーザがウェブページをロードしたことを示すことができる。制御モジュール１１８は、使用法規定に従って制限されたウェブサイトにユーザがアクセスすることを認められるかどうかをウェブサイト使用法サーバ１１４が決定するために、ユーザの身元証明（ＩＤ）と該ユーザがアクセスしている当該制限されたウェブサイト１１２の身元証明（ＩＤ）のような、身元証明（ＩＤ）情報をウェブサイト使用法サーバ１１４に提供する（５０３）。身元証明（ＩＤ）情報の提供に応じて、制御モジュール１１８はウェブサイト使用法サーバ１１４から応答を受け取る（５０５）。一実施例において、制御モジュール１１８はウェブサイトのために制限された認証証明書を受け取ることができる。さらに、制御モジュール１１８はウェブサイトと結びつくウェブサイト使用法規定に従うアクセスの条件を受け取ることができる。制御モジュール１１８は、それからウェブサイト使用法規定を執行する（５０７）。一実施例において、制御モジュール１１８は、規定によって認められたときにウェブサイト１１２へのアクセスを認めることにより、該ウェブサイト使用法規定を執行する。制御モジュール１１８は、ユーザが制限された証明書を突き止めることを妨げるような方法で、ウェブサイト１１２のためのログインフォームに自動的に書き込むために、ユーザの認証証明書を使うことができる。一実施例において、制御モジュール１１８は、アクセスがウェブサイト使用法規定によってもはや認められないとき、制限されたウェブサイト１１２からユーザをログアウトすることによって、ウェブサイト使用法規定を執行する。制御モジュール１１８の実行は、ユーザがウェブサイト１１２にアクセスすることを許可されないことを示しているエラーメッセージを提供することができる。

【００５３】

図６は、一実施例によるところのウェブサイト１１２（図１）へのユーザアクセスをコ

ントロールするためにウェブサイト使用法サーバ１１４（図１）により実行されるステップを説明するフローチャートである。他の実施例は、異なった命令で図示のステップを実行する、及び／又は異なるあるいは付加的なステップを実行する。さらに、ステップのいくつかあるいはすべてがブラウザ１１６以外の構成要素によって実行され得る。

【００５４】

ウェブサイト使用法サーバ１１４は、制御モジュール１１８からウェブサイト１１２にアクセスするためのリクエストを受け取る（６００）。一実施例において、ウェブサイト使用法サーバ１１４は、制御モジュール１１８からユーザの身元証明（ＩＤ）とウェブサイト１１２の身元証明（ＩＤ）を受け取る。身元証明（ＩＤ）情報は、制御モジュール１１８がウェブサイト１１２へのアクセスをリクエストしているという指示である。ウェブサイト使用法サーバ１１４は、ユーザとウェブサイトのための適切なウェブサイト使用法規定を特定する（６０１）。ウェブサイト使用法サーバ１１４は、ウェブサイト使用法がウェブサイト使用法規定により許可されるかどうかを決定する（６０３）。一実施例において、ウェブサイト使用法サーバ１１４は、現時刻あるいは前のアクセスの量及び／又は数のような変数に鑑みて規定を評価する。例えば、ウェブサイト使用法サーバ１１４は、リクエストの時間を決定し、その時間をウェブサイト使用法規定で指定された許可されたアクセスの時間と比較することができる。ウェブサイト使用法サーバ１１４がウェブサイト使用が認められることを決定するのに応じて、ウェブサイト使用法サーバ１１４はウェブサイトへのアクセスを認める（６０７）。一実施例において、ウェブサイト使用法サーバ１１４は、ウェブサイト１１２のログインフォームに自動で書き入れるために制御モジュール１１８に制限された認証証明書を伝える。ウェブサイト使用法サーバ１１４がウェブサイト使用法が認められないことを決定するのに応じて、ウェブサイト使用法サーバ１１４はウェブサイト１１２へのアクセスを認めない（６０５）。一実施例において、ウェブサイト使用法サーバはなぜそのユーザがウェブサイト１１２へのアクセスを認められなかったかを示しているブラウザ１１６にエラーメッセージを送る。

【００５５】

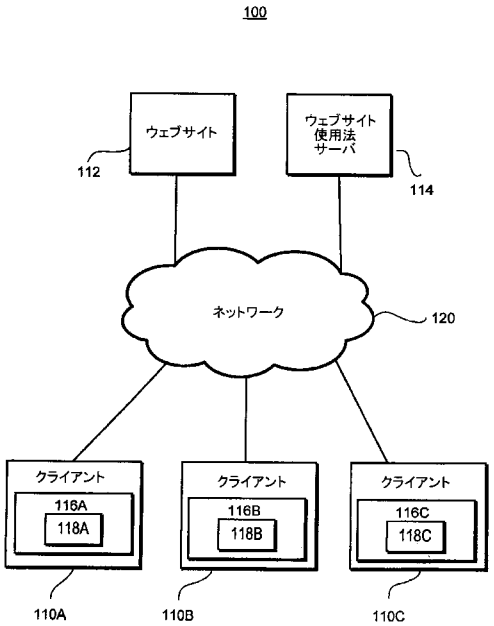
上述の記述は、特定の実施例の動作を示すことが含まれており、そして発明の範囲を制限することを意味するものではない。発明の範囲は次のクレームによってのみ制限されるはずである。上の議論から、多くの変形物が本発明の精神と範囲によってまだ含まれているであろうことが当業者によって明らかになるでしょう。例えば、一実施例において、ユーザがウェブサイト１１２にアクセスしたいことを自動的に検出するブラウザ１１６よりむしろ、ユーザはウェブサイト１１２へのアクセスを手作業でリクエストするためにウェブサイト使用法サーバ１１４によって提供されたユーザインタフェースを使うことができる。上述した実施例は、ウェブサイト１１２へのアクセスが認められるべきであるかどうかを決定するために適用されるであろう。

【符号の説明】

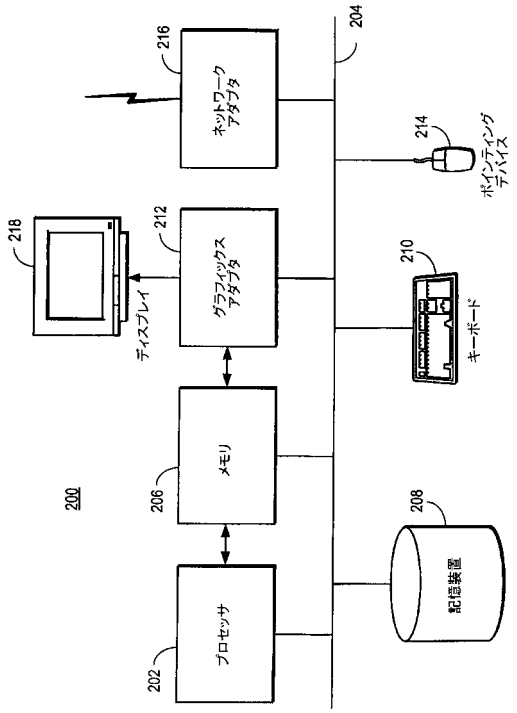
【００５６】

１１０　クライアント
１１２　ウェブサイト
１１４　ウェブサイト使用法サーバ

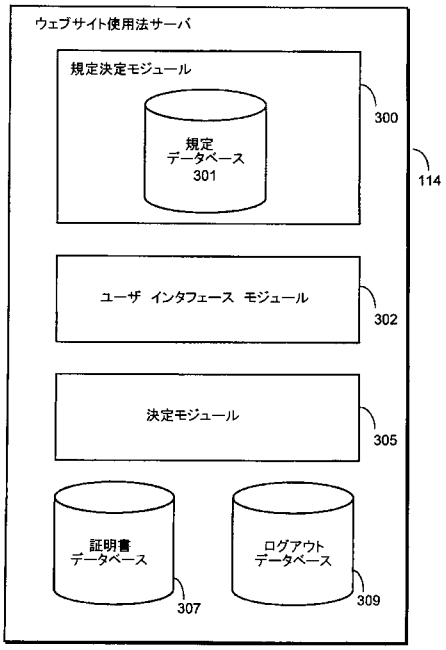
【図１】


100
ウェブサイト
112
ウェブサイト使用法サーバ
114
ネットワーク
120
クライアント
116A
118A
110A
クライアント
116B
118B
110B
クライアント
116C
118C
110C

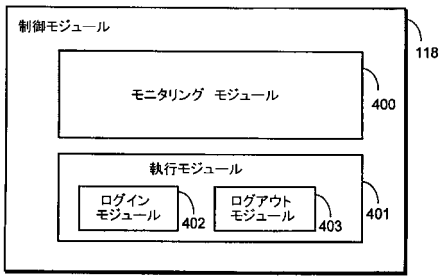
【図２】


200
204
216
ネットワークアダプタ
214
ポインティングデバイス
218
ディスプレイ
212
グラフィックスアダプタ
210
キーボード
206
メモリ
208
記憶装置
202
プロセッサ

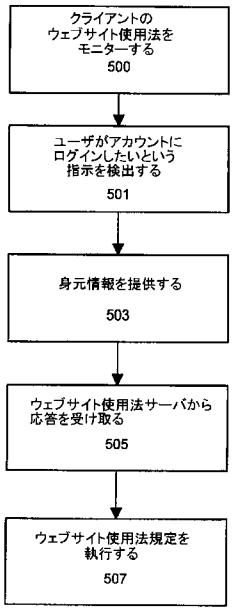
【図３】


ウェブサイト使用法サーバ
規定決定モジュール
300
規定データベース 301
114
ユーザ インタフェース モジュール
302
決定モジュール
305
証明書データベース
307
ログアウトデータベース
309

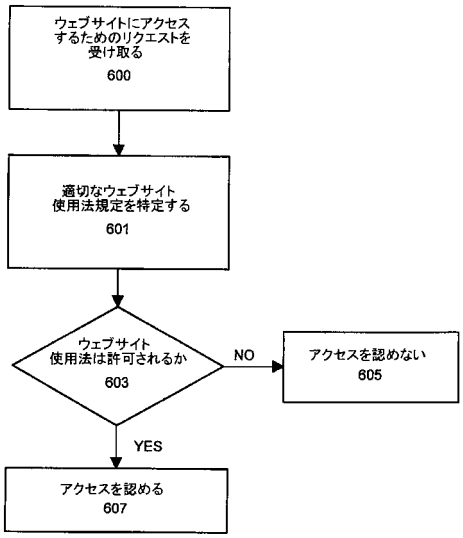
【図４】


制御モジュール
118
モニタリング モジュール
400
執行モジュール
ログインモジュール
402
ログアウトモジュール
403
401

【図５】


クライアントの
ウェブサイト使用法を
モニターする
500
ユーザがアカウントに
ログインしたいという
指示を検出する
501
身元情報を提供する
503
ウェブサイト使用法サーバから
応答を受け取る
505
ウェブサイト使用法規定を
執行する
507

【図６】


ウェブサイトにアクセス
するためのリクエストを
受け取る
600
適切なウェブサイト
使用法規定を特定する
601
ウェブサイト
使用法は許可されるか
603
NO
アクセスを認めない
605
YES
アクセスを認める
607

フロントページの続き

(72)発明者　ケイス　ニュースタッヅ
アメリカ合衆国　カリフォルニア　９５０１４，クパチーノ，スティーブンス　クリーク　ブールバード　２０３３０，　シマンテック　コーポレーション内
(72)発明者　ショーン　ピー．　クーレイ
アメリカ合衆国　カリフォルニア　９５０１４，クパチーノ，スティーブンス　クリーク　ブールバード　２０３３０，　シマンテック　コーポレーション内

Ｆターム(参考) 5B285 AA01 BA09 CA06 CA17 CA18 CA32 CA41 CB47 CB62 CB72
CB85 DA03 DA05