

(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2004-246489

(P2004-246489A)

(43) 公開日 平成16年9月2日(2004.9.2)

(51) Int.Cl.⁷

G06F 13/00

G06F 3/14

G06F 12/00

F I

G06F 13/00

G06F 3/14

G06F 12/00

540F

310C

515B

テーマコード (参考)

5B069

5B082

審査請求 未請求 請求項の数 10 O L (全 25 頁)

(21) 出願番号 特願2003-34020 (P2003-34020)

(22) 出願日 平成15年2月12日 (2003.2.12)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(74) 代理人 100092853

弁理士 山下 亮一

(72) 発明者 吉田 悦子

東京都大田区下丸子3丁目30番2号キヤ
ノン株式会社内

Fターム(参考) 5B069 AA01 KA02 LA03

5B082 EA11 GC06

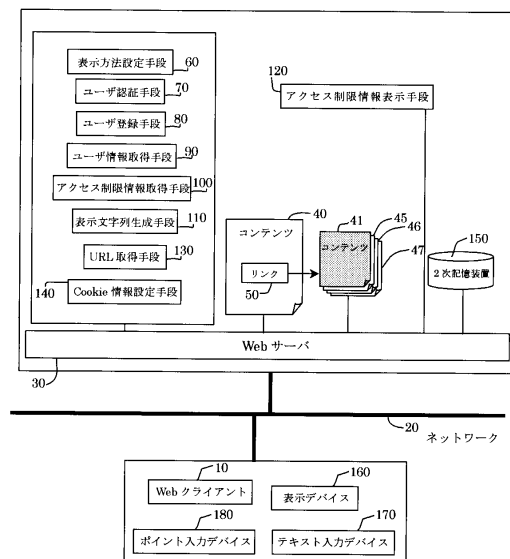
(54) 【発明の名称】 表示システム、表示方法及び記憶媒体

(57) 【要約】

【目的】 ユーザが予め登録したアクセス制限情報の表示システム、表示方法及び記憶媒体を提供すること。

【構成】 リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得手段によってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、表示方法設定手段によって登録された表示方法に従って表示文字列生成手段によって表示文字列を生成し、前記表示文字列生成手段によって生成された表示文字列とアクセス制限情報表示手段を受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示手段が起動し、サーバから送信された表示文字列を表示デバイスに表示する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

ネットワークに接続されたサーバとクライアントから成るシステムで、ユーザを登録するユーザ登録手段によってユーザを登録し、ユーザを認証するユーザ認証手段によってユーザが認証されるとアクセス制限情報の表示方法を設定する表示方法設定手段が起動し、表示方法が設定できるシステムにおいて、

リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得手段によってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、表示方法設定手段によって登録された表示方法に従って表示文字列生成手段によって表示文字列を生成し、前記表示文字列生成手段によって生成された表示文字列とアクセス制限情報表示手段を受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示手段が起動し、サーバから送信された表示文字列を表示デバイスに表示することを特徴とする表示システム。

10

【請求項 2】

前記サーバはWebサーバ、前記クライアントはWebブラウザであることを特徴とする請求項 1 記載の表示システム。

【請求項 3】

ネットワークに接続されたサーバとクライアントから成るシステムで、リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得手段によってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、クライアントの情報によって表示方法を決定し、前記表示方法に従って表示文字列生成手段によって表示文字列を生成し、前記表示文字列生成手段によって生成された表示文字列とアクセス制限情報表示手段を受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示手段が起動し、サーバから送信された表示文字列を表示デバイスに表示することを特徴とする表示システム。

20

【請求項 4】

前記サーバはWebサーバ、前記クライアントはWebブラウザであることを特徴とする請求項 3 記載の表示システム。

30

【請求項 5】

ネットワークに接続されたサーバとクライアントから成るシステムで、ユーザを登録するユーザ登録ステップによってユーザを登録し、ユーザを認証するユーザ認証ステップによってユーザが認証されるとアクセス制限情報の表示方法を設定する表示方法設定ステップが起動し、表示方法が設定できるシステムにおいて、

リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得ステップによってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、表示方法設定ステップによって登録された表示方法に従って表示文字列生成ステップによって表示文字列を生成し、前記表示文字列生成ステップによって生成された表示文字列とアクセス制限情報表示ステップを受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示ステップが起動し、サーバから送信された表示文字列を表示デバイスに表示することを特徴とする表示方法。

40

【請求項 6】

前記サーバはWebサーバ、前記クライアントはWebブラウザであることを特徴とする請求項 5 記載の表示方法。

【請求項 7】

ネットワークに接続されたサーバとクライアントから成るシステムで、リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得ステップによってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、

50

クライアントの情報によって表示方法を決定し、前記表示方法に従って表示文字列生成ステップによって表示文字列を生成し、前記表示文字列生成ステップによって生成された表示文字列とアクセス制限情報表示ステップを受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示ステップが起動し、サーバから送信された表示文字列を表示デバイスに表示することを特徴とする表示方法。

【請求項 8】

前記サーバは Web サーバ、前記クライアントは Web ブラウザであることを特徴とする請求項 7 記載の表示方法。

【請求項 9】

ネットワークに接続されたサーバとクライアントから成るシステムで、ユーザを登録するユーザ登録ステップによってユーザを登録し、ユーザを認証するユーザ認証ステップによってユーザが認証されるとアクセス制限情報の表示方法を設定する表示方法設定ステップが起動し、表示方法が設定できるシステムにおいて、

リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得ステップによってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、表示文字列生成ステップによって表示方法設定ステップによって登録された表示方法に従って表示文字列を生成し、前記表示文字列生成ステップによって生成された表示文字列とアクセス制限情報表示ステップを受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示ステップが起動し、サーバから送信された表示文字列を表示デバイスに表示する表示方法を含むプログラムが格納されている記憶媒体。

【請求項 10】

ネットワークに接続されたサーバとクライアントから成るシステムで、リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得ステップによってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、クライアントの情報によって表示方法を決定し、前記表示方法に従って表示文字列生成ステップによって表示文字列を生成し、前記表示文字列生成ステップによって生成された表示文字列とアクセス制限情報表示ステップを受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示ステップが起動し、サーバから送信された表示文字列を表示デバイスに表示する表示方法を含むプログラムが格納されている記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、Web クライアント上に表示されるリンクが指し示すコンテンツのアクセス制限情報をアクセス制限情報文字列として構成し、それを Window に表示する表示システム、表示方法及びそれらのプログラムが格納されている記憶媒体に関するものである。

【0002】

【従来の技術】

インターネットを利用した情報発信や情報を収集する方法として Web が挙げられる。Web 上では、HTML (Hyper Text Markup Language) で記述された文書 (ここでは“コンテンツ”と呼ぶ) を Web サーバが Web ブラウザ等のコンテンツを表示するためのプログラムである Web クライアントに HTTP (Hyper Text Transfer Protocol) で転送することにより、ユーザは情報にアクセスすることができる。

【0003】

コンテンツを指定するためには、URL (Unique Resource Location) を Web クライアントで指定することで、特定のコンテンツにアクセスすることができる。又、特定の URL へのリンクを含むコンテンツ (ここでは“リンク含

10

20

30

40

50

有コンテンツ”と呼ぶ)から、ユーザはリンクを選択することで別のコンテンツを指定することができる。

【0004】

又、Webサーバは、特定のコンテンツがWebクライアントから要求された際に、ユーザIDとパスワードをユーザに対して要求するフォームが記述されたコンテンツをWebクライアントに転送する。ユーザIDとパスワードをユーザに対して要求するダイアログを表示するという方法でコンテンツのアクセスを制限することができる。

【0005】

又、Webブラウザ上のある位置にカーソルを置くとWindow(例えば、バルーンヘルプ)が表示されるようにするためには、コンテンツ内のその場所に相当するテキスト部分にWindow表示のための関数を起動する命令を記述することでWindow表示される。Window内に表示するデータは、予め情報発信者が文字列や画像等を用意し、その文字列や画像等をWindow内に表示する。

【0006】

【発明が解決しようとする課題】

ユーザが前記アクセス制限情報を表示デバイス上に表示するとき、例えば携帯端末に組み込まれているWebブラウザである場合、Window表示する機能はサポートされていないことがある。又、モノクロの表示デバイスの場合、文字色を変更してアクセス制限が掛けられているコンテンツを強調することができない。このようにサポートされていない環境でユーザがアクセス制限情報を表示しようとした場合、ユーザはアクセス制限情報を表示することができず、無駄な処理を行なう時間を費やすこととなる。

【0007】

又、表示できないアクセス制限情報の送信が行なわれることで無駄な通信が発生し、通信効率を悪化させる。

【0008】

本発明は上記問題に鑑みてなされたもので、その目的とする処は、ユーザが予め登録したアクセス制限情報の表示システム、表示方法及び記憶媒体を提供することにある。

【0009】

【課題を解決するための手段】

本発明に係るアクセス制限情報表示システム及び表示方法は、以上のような課題を解決したもので、次のようなものである。

【0010】

即ち、サーバ/クライアント型のシステムで、ユーザを登録するユーザ登録手段によってユーザを登録し、ユーザを認証するユーザ認証手段によってユーザが認証されるとアクセス制限情報の表示方法を設定する表示方法設定手段が起動し、表示方法が設定できるシステムにおいて、リンク含有コンテンツがクライアントから要求されるとアクセス制限情報取得手段によってリンク含有コンテンツに記載されているリンクが指定するコンテンツのアクセス制限情報を取得し、表示文字列生成手段によって表示方法設定手段によって登録された表示法に従って表示文字列を生成し、前記表示文字列生成手段によって生成された表示文字列とアクセス制限情報表示手段を受信するクライアントにおいて、ユーザがカーソルをリンク含有コンテンツに記載されているリンク上に移動したときアクセス制限情報表示手段が起動し、サーバから送信された表示文字列を表示デバイスに表示することを特徴とする。

【0011】

【発明の実施の形態】

図1は本発明の代表的なシステム構成図であり、同図において、10はWebクライアント、30はWebサーバであり、Webクライアント10が保持するCookie情報にSession IDを設定する機能を持つ。

【0012】

図1中のリンク含有コンテンツ40は、コンテンツ41へのリンク50を含み、Session ID

i o n I D の有無によって判定するアクセス制限が掛けられたコンテンツである。

【0013】

図1中のコンテンツ41はアクセス制限が掛けられたアクセス制限付コンテンツである。コンテンツ45は表示方法選択フォームと送信ボタンを含む設定フォームコンテンツである。コンテンツ46はユーザID入力フォームとパスワード入力フォームと送信ボタンを含む認証コンテンツである。コンテンツ47はユーザID入力フォームとパスワード入力フォームと送信ボタンを含むユーザ登録フォームコンテンツである。

【0014】

図1中の表示方法設定手段60は、Webクライアント10に設定フォームコンテンツを送信し、ユーザの入力したデータを2次記憶装置150に保管する手段である。

10

【0015】

図1中のユーザ認証手段70は、Webクライアント10が保持するCookie値からSessionIDの有無を確認し、ユーザに対して認証処理を要求する手段である。

【0016】

図1中のユーザ登録手段80は、Webクライアント10にユーザ登録フォームコンテンツ47を送信し、ユーザの入力したユーザIDとパスワードを2次記憶装置150に保管する手段である。

【0017】

図1中のユーザ情報取得手段90は、2次記憶装置150からユーザが予め設定したユーザ情報を取得する手段である。

20

【0018】

図1中のアクセス制限情報取得手段100は、リンク含有コンテンツ40に記述されているリンク50が指し示すコンテンツ41にアクセス制限が掛けられているかを検出し、表示文字列生成手段110にその検出した情報に転送する手段である。アクセス制限が掛けられているかを検出する際に、各コンテンツにリンクが含まれているかを検出し、リンクが含まれているならば、そのリンクが指し示すコンテンツのアクセス制限情報も検出する手段である。

【0019】

図1中の表示文字列生成手段110は、アクセス制限情報取得手段100から転送されたアクセス制限情報とユーザ情報取得手段90から転送されたユーザ情報からユーザが設定した表示方法で表示するための表示文字列を生成する手段である。

30

【0020】

図1中のアクセス制限情報表示手段120は、表示文字列生成手段110が生成した表示文字列をWebクライアントの画面上に表示する手段である。

【0021】

図1中のURL取得手段130は、リンク含有コンテンツ40中に記載されているリンク50の情報からURLを取得する手段である。

【0022】

図1中のCookie情報設定手段140は、Webクライアント10が保持するCookie情報をアクセス権情報取得手段60が各コンテンツを要求する際に付加する手段である。

40

【0023】

上記手段を用いて本発明では以下のように処理を実施する。

【0024】

即ち、Webクライアント10は、リンク含有コンテンツ40をWebサーバ30に要求する。Webサーバ30は、ユーザ認証手段70を起動し、ユーザ認証を行う。次に、ユーザ情報取得手段90を起動し、ユーザが予め登録した表示方法を抽出する。この表示方法に従って表示文字列生成手段110が表示文字列を生成する。この生成された表示文字列とリンク含有コンテンツ40とアクセス制限情報表示手段120とをWebサーバ30はWebクライアント10に送信する。ユーザがカーソルをリンク50上に移動したとき

50

に、Webクライアント10は、アクセス制限情報表示手段120を起動し、表示文字列を表示デバイス上に表示する。

【0025】

以上の処理でユーザが選択した方法でアクセス制限情報を表示することができる。

【0026】

又、ここでユーザが表示方法を設定する処理は以下の通りである。

【0027】

即ち、Webクライアント10がWebサーバに設定フォームコンテンツ45を要求すると、Webサーバ30はユーザ認証手段70でユーザ認証を行う。次に、Webサーバ30は、設定フォーム45をWebクライアント10に送信し、ユーザは表示方法を設定フォームコンテンツ45から選択してWebサーバ30に送信する。表示方法設定手段60がユーザが選択した表示方法とユーザIDを2次記憶装置150に登録する。これにより、ユーザ毎に表示方法を設定することができる。

【0028】

<実施の形態1>

図13は本実施の形態の代表的なシステム構成図である。

【0029】

今、Webクライアント10は、Webブラウザプログラムであると仮定する。

【0030】

ネットワーク20は、TCP/IPを通信プロトコルとするインターネットであると仮定する。

【0031】

Webサーバ30は、アドレスwww.canon.co.jpを持ち、HTTPでコンテンツ等を提供するHTTPサーバプログラムであると仮定する。又、コンテンツ40, 41は、Cookie情報によるアクセス制限を掛けているコンテンツであり、Webクライアントから要求されたときにユーザ認証手段60を起動する機能を有すると仮定する。

【0032】

リンク含有コンテンツ40は、URLがhttp://www.canon.co.jp/index.htmlとしてアクセス可能であって、同一Webサーバ30が提供するコンテンツ41へのリンク50とネットワーク20に接続しているWebサーバ31が提供するコンテンツ42へのリンク51とネットワーク20に接続しているWebサーバ32が提供するコンテンツ43へのリンク52とを含むリンク含有コンテンツであると仮定する。

【0033】

Webサーバ31は、アドレスwww.canon.comを持つHTTPでコンテンツ等を提供するHTTPサーバプログラムであると仮定する。又、コンテンツ42がWebクライアントから要求された際に、ユーザIDとパスワードをユーザに要求し、Webサーバ30が保管するユーザID/パスワード情報と一致するかどうかを判定する認証機能を持つと仮定する。

【0034】

Webサーバ32は、アドレスwww2.canon.co.jpを持ち、HTTPでコンテンツ等を提供するHTTPサーバプログラムである。又、コンテンツ44は、Cookie情報によるアクセス制限を掛けているコンテンツであり、Webクライアントから要求されたときにユーザ認証手段61を起動する機能を有すると仮定する。

【0035】

CGI(Common Gateway Interface)プログラムは、表示方法設定手段60とユーザ認証手段70とユーザ登録手段80とユーザ情報取得手段90とアクセス制限情報取得手段100と表示文字列生成手段110とURL取得手段130とCookie情報設定手段140とを含むプログラムであると仮定する。

10

20

30

40

50

【0036】

J a v a S c r i p t プログラムは、アクセス制限情報表示手段120を含むプログラムであると仮定する。

【0037】

表示方法設定手段60は、Webクライアント10に設定フォームコンテンツ45を送信し、ユーザの入力したデータを2次記憶装置150に保管するC S I プログラムであると仮定する。ここで、設定フォームコンテンツ45は、URL “ h t t p : / / w w w . c a n o n . c o . j p / i n p u t . h t m l ” を持ち、表示方法設定フォーム220と送信ボタン210を含むHTMLで記述されたコンテンツであると仮定する。

【0038】

ユーザ認証手段70, 71は、Webクライアント10からコンテンツの要求があると、Webサーバ30, 32が発行するS e s s i o n I D の有無を確認し、ユーザに対して認証処理を要求するため認証コンテンツ46, 48をWebクライアント10に送信するC G I プログラムであると仮定する。ここで、認証コンテンツ46はURL “ h t t p : / / w w w . c a n o n . c o . j p / l o g i n . h t m l ” を持ち、ユーザID入力フォーム221とパスワード入力フォーム222と送信ボタン211と登録ボタン212を含むHTMLで記述されたコンテンツであり、認証コンテンツ48はURL “ h t t p : / / w w w 2 . c a n o n . c o . j p / l o g i n . h t m l ” を持つコンテンツであると仮定する。

【0039】

ユーザ登録手段80は、Webクライアント10にユーザ登録フォームコンテンツ47を送信し、ユーザの入力したユーザIDとパスワードを2次記憶装置150に保管するC G I プログラムであると仮定する。ここで、ユーザ登録フォームコンテンツ47は、ユーザID入力フォーム23とパスワード入力フォーム224と送信ボタン213を含むHTMLで記述されたコンテンツであると仮定する。

【0040】

ユーザ情報取得手段90は、2次記憶装置150からユーザが予め設定したユーザ情報を取得するC G I プログラムであると仮定する。

【0041】

アクセス制限情報取得手段100は、コンテンツ40に記載されているリンク50, 51, 52からコンテンツ41, 42, 43を各Webサーバ30, 31, 32に要求し、Webサーバから送信されたコンテンツの情報からアクセス制御情報を検出、保管するC G I プログラムであると仮定する。

【0042】

アクセス制限情報表示手段120は、ユーザがカーソルをリンク上に移動したことをきっかけとして起動し、アクセス制限情報取得手段60が保管したアクセス制御情報を表示デバイス上に表示するJ a v a S c r i p t プログラムであると仮定する。

【0043】

URL取得手段130は、リンク含有コンテンツ40, 43に記述されているリンクからURLを抽出するC G I プログラムであると仮定する。

【0044】

C o o k i e 情報設定手段140は、Webクライアント10が保持するC o o k i e 情報をアクセス制限情報取得手段が送信するG E T メソッド242のヘッダ情報に追加するプログラムであると仮定する。

【0045】

又、2次記憶装置150は、ユーザIDテーブル230と表示方法テーブル231とユーザ設定テーブル232と認証URLテーブル233を保管するデータベース装置であると仮定する。

【0046】

先ず、表示方法設定手段60について図2を用いて具体的に説明する。

10

20

30

40

50

[STEP 1-1]

Webクライアント10は、Webサーバ30に以下のGETメソッド240を送信することで、ファイル名がinput.htmlである設定フォームコンテンツ45の提供を要求する。

【0047】

GET /input.html HTTP/1.0

ここで、上記GETメソッド240は“メソッド ファイル名 プロトコル”という形式で記述されており、「input.htmlファイルを要求するGETメソッドがHTTP/1.0で定義されているプロトコルでwww.canon.co.jp に送信された」ことを示す。

10

[STEP 1-2]

Webサーバ30は、ユーザ認証手段70を起動する。

[STEP 1-3]

ユーザ認証手段70は、図3の処理を実行する。

[STEP 1-4]

Webサーバ30は、設定フォームコンテンツ45をWebクライアントに送信する。

[STEP 1-5]

Webクライアント10は、設定フォームコンテンツ45を表示し、ユーザは表示方法を選択して送信ボタンを選択する。今、ユーザは表示方法を以下のように選択したと仮定する。

20

【0048】

Window表示する、リンク表示しない、強調する、強調タイプ=マーク、複数表示する。

【0049】

上記の表示方法は表示方法テーブル231と照らし合わせてみると表示方法IDが18となる。

[STEP 1-6]

表示方法設定手段60は、STEP 1-5で送信された表示方法とユーザIDを以下のデータを2次記憶装置150のユーザ設定テーブル232に登録する。

【0050】

canon, 1, 18

ここで、上記データは「ID：表示の有無：選択した表示方法ID」という形式で記述されているものとする。IDはユーザIDと一致する任意の文字列であり、表示の有無は0の場合アクセス情報を表示しない。1の場合表示するという意味を持つ。又、表示方法IDは2次記憶装置150に図のように保管されている表示方法テーブル231の表示方法IDと一致する数値である。

30

【0051】

ここで、ユーザ認証手段70は以下の通りである。

[STEP 1-3-1]

Webクライアント10が保持するCookie情報を取得し、Webサーバ30が発行したSessionIDが含まれているかどうかを確認する。含まれているならば、STEP 1-4に進む。含まれていないならば、STEP 1-3-2に進む。

40

[STEP 1-3-2]

Webサーバ30は、認証コンテンツ46をWebクライアント10に送信する。

[STEP 1-3-3]

Webクライアント10は、認証コンテンツ46を表示する。ユーザは既にユーザ登録しているならば、キーボード等のテキスト入力デバイス170でユーザID入力フォーム221にユーザIDをパスワード入力フォーム222にパスワードを入力し、マウス等のポインタ入力デバイス180で送信ボタン211を選択し、STEP 1-3-4に進む。ユーザ登録していないのならば、登録ボタン212を選択し、STEP 1-3-5に進む。

50

[STEP 1-3-4]

2次記憶装置150に図21のように登録されているユーザIDテーブルからSTEP 1-3-3で送信されたユーザIDとパスワードの組が一致しているか確認する。一致していたら、Webクライアント10のCookieにSessionID をセットしてSTEP 1-3-1に戻る。一致していない場合は、STEP 1-3-5に進む。ここで、SessionID はユーザIDの値と一致するものとする。

[STEP 1-3-5]

Webサーバ30は、ユーザ登録手段80を起動する。

【0052】

ここで、ユーザ登録手段80の処理は以下の通りである。

10

[STEP 1-3-5-1]

Webサーバ30は、ユーザ登録フォームコンテンツ47をWebクライアント10に送信する。

[STEP 1-3-5-2]

Webクライアント10は、ユーザ登録フォームコンテンツ47を表示する。

[STEP 1-3-5-3]

ユーザは、ユーザID入力フォーム223とパスワード入力フォーム224に任意の文字列を入力して送信ボタン213を選択する。今、ユーザはユーザ入力フォーム223に“ canon ”、パスワード入力フォーム224に“ passwd ”を入力したとする。

[STEP 1-3-5-4]

20

ユーザ登録手段80は、STEP 1-3-5-3で送信されたデータから、ユーザIDを抽出し、2次記憶装置150のユーザIDテーブル230にユーザIDが登録されていないかを確認する。既に登録されている場合は、STEP 1-3-5-1に戻り、ユーザに異なるユーザIDを要求する。そうでない場合は、2次記憶装置150に保管されているユーザIDテーブル230にSTEP 1-3-5-3で入力されたユーザIDとパスワードを登録する。今、ユーザIDテーブル230にはユーザID“ canon ”は登録されていないので、ユーザID“ canon ”、パスワード“ passwd ”をユーザIDテーブル230に登録する。

【0053】

又、Webクライアント10が直接ユーザ登録フォームコンテンツ47を要求することで、STEP 1-1の処理に入る前にユーザ登録処理80を実行することができる。

30

【0054】

次に、ユーザが表示方法設定手段60によって予め設定した表示方法でアクセス制限情報を表示する処理について図5及び図6を用いて説明する。

[STEP 2-1]

Webクライアント10は、アドレスがwww. canon. co. jp であるWebサーバ30に以下のGETメソッド241を送信することでファイル名がindex. htmlであるリンク含有コンテンツ40の提供を要求する。

【0055】

GET /index. html HTTP/1.0

40

[STEP 2-2]

Webサーバ30は、ユーザ認証手段70を起動し処理を実行する。

[STEP 2-3]

ユーザ情報取得手段90が起動する。

[STEP 2-4]

ユーザ情報取得手段90は、Webクライアント10が保持するCookie情報からSessionID を抽出する。ここで、SessionID はユーザIDと一致するため、2次記憶装置150が保管するユーザIDテーブルからSessionID と一致するユーザIDのデータを抽出する。ここで、抽出されたデータ250は以下のように記述されているものとする。

50

【0056】

canon, 1, 18

[STEP 2-5]

表示の有無が1である場合、アクセス制限情報取得手段100を起動し、STEP 2-7に進む。0の場合、STEP 2-6に処理を進める。本実施の形態では表示の有無が1であるため、STEP 2-7に進む。

[STEP 2-7]

アクセス制限情報取得手段100は図7～図9の処理を実行し、取得したアクセス制限情報を表示文字列生成手段110に渡す。

[STEP 2-8]

表示文字列生成手段110は、STEP 2-4で抽出したデータ250の表示方法と表示手段IDが一致するデータを抽出する。ここで、2次記憶装置150には図22のように表示方法テーブル231が保管されているものとする。今、データの表示方法IDは18であるので、表示方法IDが一致するデータは、

18, 1, 0, 1, マーク, 1

である。ここで、上記データは「表示方法ID、Window表示の有無、リンク表示の有無、強調表示の有無、強調タイプ、複数Window表示の有無」という順で記述されているものとする。

[STEP 2-9]

表示文字列生成手段110は、STEP 4-1からの処理を実行し、表示文字列260を生成する。

[STEP 2-10]

Webサーバ30は、リンク含有コンテンツ40とSTEP 2-9で生成した表示文字列260とアクセス制限情報表示手段120をWebクライアント10に送信する。

[STEP 2-11]

Webクライアント10は、リンク含有コンテンツ40と表示文字列260とアクセス制限情報表示手段120を受信し、リンク含有コンテンツ40を表示する。

[STEP 2-12]

ユーザは、カーソル190をリンク50上に移動する。

[STEP 2-13]

アクセス制限情報表示手段120が起動し、以下の処理を行う。

[STEP 2-13-1]

STEP 2-11で受信したアクセス制限情報表示手段120にWindow生成手段が存在するならば、表示文字列260を読み込み、表示デバイス160上にWindow 200を出力する。

【0057】

(1) カーソル190が現在表示デバイス160上のどの位置にあるか、X軸方向とY軸方向の位置情報を取得し、各々変数x, yに格納する。

【0058】

(2) (1)で格納した変数x, yの値に任意の値を各々加える。ここで値を加えるのは、Window 200をカーソルの位置からずらして表示させるためである。

【0059】

(3) 表示文字列を読み込み、表示デバイス160上に(2)で求めたx, yの位置にWindow 200を表示する。

【0060】

STEP 2-10で受信したアクセス制限情報表示手段120にWindow生成手段が存在しないならば、表示文字列260をWebクライアント10に転送する。Webクライアント10は、表示文字列260を読み込み、表示デバイス160上に表示する。

【0061】

以上の処理により、ユーザが予め選択した表示方法でアクセス制限情報を表示することが

10

20

30

40

50

できる。

【0062】

ここで、アクセス制限取得手段100がコンテンツ41のアクセス制限情報を取得する処理の流れを図7～図9を用いて具体的に説明する。

[STEP3-1]

アクセス制限情報取得手段100は、URL取得手段130を起動する。

[STEP3-2]

URL取得手段130は、次の処理を実行する。

[STEP3-2-1]

リンク含有コンテンツ40に記載されているリンク50, 51, 52を抽出する。ここで、各リンクはHTMLで定義されているアンカータグに記載されているものとする。 10

[STEP3-2-2]

STEP3-2-1で抽出したリンク50, 51, 52からURLを抽出し、配列url[x]に代入する。ここで、変数xは $0 \leq x < n$ であり、変数nはリンク含有コンテンツ40に記載されているリンクの数である。今、 $n = 3$ である。

【0063】

先ず、リンク含有コンテンツ40に記載されているリンク50は下記のようなアンカー文字列で記載されていると仮定する。

【0064】

コンテンツ40 20

アンカー文字列からURLを抽出し、配列url[0]に代入する。同様に、リンク51, 52からURLを抽出し、各々を配列url[1], url[2]に代入する。更に、 $x = 0$ としてSTEP3-3に進む。

[STEP3-3]

アクセス制限情報取得手段100はCookie情報設定手段140を起動する。

[STEP3-4]

Cookie情報設定手段140は次の処理を実行する。

[STEP3-4-1]

Cookie情報設定手段140は、Webクライアント10から送信されたGETメソッド400のヘッダから環境変数HTTP-COOKIEが存在するか確認する。 30

【0065】

今、環境変数HTTP-COOKIEは存在しないものとする。

【0066】

従って、Cookie情報設定手段140の処理を終了し、STEP3-5に進む。

[STEP3-5]

アクセス制限情報取得手段100はurl[x]が指し示すコンテンツを要求する。今、 $x = 0$ なので、url[0]が指し示すコンテンツ41を持つWebサーバ30に以下のGETメソッド242を送信することで、ファイル名がcontent.htmlであるコンテンツ41の提供を要求する。 40

【0067】

GET /content.html HTTP/1.0

[STEP3-6]

Webサーバ30はコンテンツ41をアクセス制限情報取得手段100にHTTPプロトコルで送信する。

【0068】

今、コンテンツ41はコンテンツ40と同様の方法でアクセス制限が掛けられているものとする。ここで、Cookie情報が存在しないため、コンテンツ41はユーザが認証を受けていないと判断し、認証コンテンツ46をアクセス制限情報取得手段100に送信する。

[STEP 3-7]

アクセス制限情報取得手段100は、コンテンツ41のアクセス制限情報270を検出する。

[STEP 3-7-1]

アクセス制限情報取得手段100は、2次記憶装置150に保管されている認証コンテンツURLとSTEP 3-6で送信された認証コンテンツ46のURLが一致するかを確認する。

【0069】

今、2次記憶装置150の認証URLテーブル233には図24のように認証URLが保管されている。ここで、認証コンテンツURLと認証コンテンツ45のURLが一致するため、アクセス制御フラグを1に設定し、STEP 3-8に進む。 10

[STEP 3-8]

アクセス制御フラグが1なので、STEP 3-9に処理を進める。

[STEP 3-9]

アクセス制限情報取得手段100は、アクセス制限情報270を配列access_info[x]に保管する。ここで変数xは配列url[x]で用いている変数xと同一の値であり、今x=0である。従って、コンテンツ41のアクセス制限情報270をaccess_info[0]に保管する。

ここで、アクセス制限情報270は“URL、アクセス制御フラグ、親URL、子フラグ”という形式で記述されているものとし、コンテンツ41のアクセス制限情報270 access_info[0] は以下のように記述されるものとする。 20

【0070】

http://www.canon.co.jp/content.html, 1, null, 0

ここで、アクセス制御フラグは1又は0の値を持つものとし、アクセス制限が掛かっている場合は1、掛かっていない場合は0とする。又、親URLとはリンク含有コンテンツ40に記載されているリンクではなく、他のリンクからアクセスされるコンテンツの場合に、リンクが記載されているリンク含有コンテンツのURLを記述する。例えば、コンテンツ44の場合であり、この場合親URLはリンク含有コンテンツ43のURLとなる。そうでない場合は“null”を記述する。 30

【0071】

又、子フラグとは、同一サーバで保管されているコンテンツへのリンクを含むリンク含有コンテンツの場合1とする。そうでない場合は0とする。

[STEP 3-10]

コンテンツ41中からリンクの記述を抽出する。抽出手段はURL取得手段130を用いる。

[STEP 3-11]

コンテンツ41にはリンクの記述が存在しないため、x=x+1としてSTEP 3-3に戻る。

【0072】

ここまででアクセス制限情報取得手段100はコンテンツ41のアクセス制限情報270を取得することができる。次に、url[1]に保管されているURLが指し示すコンテンツ42のアクセス制限情報271を取得する処理の流れについて説明する。ここで、コンテンツ42のアクセス制限情報271の取得がコンテンツ41のアクセス制限情報270の取得する処理と異なるのはSTEP 3-6, 7である。従って、以下でSTEP 3-6, 7のコンテンツ42の場合について説明する。 40

[STEP 3-6]

Webサーバ31は、コンテンツ42をアクセス制限情報取得手段100にHTTPプロトコルで送信する。ここで、Webサーバ31から送信されたデータは図14のような記述である。 50

[STEP 3-7]

アクセス制限情報取得手段100は、コンテンツ42のアクセス制限情報271を検出する。

[STEP 3-7-1]

アクセス制限情報取得手段100は、2次記憶装置150に保管されているURL認証テーブルにSTEP 3-6で送信されたコンテンツ42のURLが存在するかを確認する。

【0073】

今、コンテンツ42のURLが存在しないため、STEP 3-7-2に進む。[STEP 3-7-2]

アクセス制限情報取得手段100は、コンテンツ42の環境変数WWW-Authenticateの有無をチェックする。今、図14の記述には環境変数WWW-Authenticateの記述が存在するため、アクセス制御フラグを1に設定し、STEP 3-8の処理に進む。

【0074】

これまでの処理でアクセス制限情報取得手段100は、コンテンツ42のアクセス制限情報271を取得することができる。次に、url[2]に保管されているURLが指し示すリンク含有コンテンツ43に記載されているリンク53が指し示すコンテンツ44のアクセス制限情報273を取得する処理の流れについて説明する。ここで、コンテンツ41、42の場合と異なるのは、STEP 3-11の処理でSTEP 3-3に戻るのではなく、STEP 3-12以降に進む点である。従って、以下でSTEP 3-11以降の処理について説明する。

[STEP 3-11]

URL取得手段130は処理を実行する。ここで、処理はSTEP 3-2と同様である。

【0075】

取得したURLを配列url2[x]に格納する。今、リンク含有コンテンツからはリンク53が検出されたため、配列url2[0]の値は、

url2[0] = http://www2.canon.co.jp/content.html

となる。

【0076】

又、リンクが存在するので、コンテンツ43が保管されているサーバ名280を検出する。ここで、url[2]に保管されているURLは、

http://www2.canon.co.jp/index.html

であると仮定する。上記URLは“プロトコル名：//サーバ名/ファイル名”と記述されている。従って、コンテンツ43が保管されているサーバ名は、

www2.canon.co.jp

であり、アクセス制限情報取得手段100は、上記サーバ名280を変数server_nameに格納する。

【0077】

server_name = www2.canon.co.jp

今、URLが存在するので、STEP 3-14に処理を進める。

[STEP 3-12]

配列url2[0]からサーバ名281を検出する。検出方法はSTEP 3-11と同様である。検出したサーバ名281を変数server_name2に格納する。

【0078】

server_name2 = www2.canon.co.jp

次に、変数server_nameと変数server_name2を比較する。ここで、変数server_nameと変数server_name2は値が一致するため、STEP 3-3以降の処理と同様の処理を行う。

【0079】

10

20

30

40

50

更に、配列 `u r l 2` に格納されている値が無くなるまで `S T E P 3 - 1 2` を繰り返し、無くなったら `S T E P 3 - 2` に戻る。

【0080】

次に、表示文字列生成手段 110 について図 18 を用いて具体的に説明する。

【0081】

今、ここで Web サーバ 30 から送信されたコンテンツ 41 のアクセス権情報 270 は以下に示す記述である。

【0082】

`h t t p : / / w w w . c a n o n . c o . j p / c o n t e n t . h t m l , 1 , n u l l , 0`

10

又、コンテンツ 42 のアクセス制限情報 271 は以下に示す記述であり、

`h t t p : / / w w w . c a n o n . c o m / i n d e x . h t m l , 1 , n u l l , 0`
コンテンツ 43 のアクセス制限情報 272 は以下に示す記述であるものとする。

【0083】

`h t t p : / / w w w 2 . c a n o n . c o . j p / i n d e x . h t m l , 0 , n u l l , 1`

更に、`S T E P 2 - 8` で抽出した表示方法データは、

`1 8 , 1 , 0 , 1 , マーク , 1`

である。

[STEP 4-1]

20

変数 `d i s p l a y` に “`h t t p : / / w w w . c a n o n . c o . j p / c o n t e n t . h t m l`” を代入する。

[STEP 4-2]

強調フラグが 1 ならば、`S T E P 4 - 2 - 1` を実行する。

[STEP 4-2-1]

強調タイプデータを抽出し、以下の処理を実行する。

【0084】

(1) 強調タイプ=大きさならば、変数 `d i s p l a y` の先頭に「`< b i g >`」を挿入し、末尾に「`< / b i g >`」を挿入する。

【0085】

30

(2) 強調タイプ=色ならば、変数 `d i s p l a y` の先頭に「`< f o n t c o l o r = " r e d " >`」と挿入し、末尾に「`< / f o n t >`」と挿入する。本実施の形態では、文字色を赤に設定している。

【0086】

(3) 強調タイプ=フォントタイプならば、変数 `d i s p l a y` の先頭に「`< B >`」と挿入し、末尾に「`< / B >`」と挿入する。

【0087】

(4) 強調タイプ=マークならば、変数 `d i s p l a y` の先頭にマーク「`×`」を挿入する。ここで、マーク「`×`」はアクセス制限が掛かっていることを示すマークであるものとする。

40

【0088】

(5) 強調タイプ=イメージならば、変数 `d i s p l a y` の先頭に「`< i m g s r c = " k e y . g i f " >`」を挿入する。ここで、`k e y . g i f` とはイメージ図のファイルであり、上記の記述により `k e y . g i f` を表示することができる。

【0089】

(6) 強調タイプ=メッセージならば、変数 `d i s p l a y` を「認証が必要です。事前に登録されたユーザのみ閲覧できます。」と設定する。ここで、変数 `d i s p l a y` に設定したメッセージは予め 2 次記憶装置 150 に保管しているものとする。

[STEP 4-3]

50

アクセス制限情報の子フラグが1ならば、STEP 4-3-1を実行する。本実施の形態では、コンテンツ43の場合に該当する。

[STEP 4-3-1]

親URLがアクセス制限情報のURLと一致するアクセス制限情報を抽出し、配列access_info_tmp[y]に代入する。ここで、yは $0 \leq y < m$ の整数で、mは抽出されたアクセス制限情報の数を表わす。

【0090】

(1) y = 0 に設定する。

【0091】

(2) y < m ならば、(3)に進む。そうでないならば、STEP 4-5に進む。 10

【0092】

(3) access_info_tmp[y]のアクセス制御フラグが1ならば、STEP 4-3-1の処理を実行する。但し、変数displayではなく、変数display_tmpに値を設定するものとする。

【0093】

(4) 複数表示フラグが0ならば(1)を、1ならば(2)を実行する。

【0094】

(4-1) 変数displayに“
<P>display_tmp</P>”を追加する。ここで、“
”は改行を表わすタグである。又、<P> , </P>はこれらで囲まれた文字列をインデントを付けて表示するように予め設定したタグである 20

【0095】

(4-2) STEP 5-1の処理を実行する。

【0096】

(5) y = y + 1 とし、(2)の処理に戻る。

[STEP 4-4]

リンクフラグが1ならば、STEP 4-4-1を実行する。

[STEP 4-4-1]

変数displayの先頭にを挿入し、末尾にを挿入する。 30

[STEP 4-5]

Window表示フラグの値に応じて以下の処理を実行する。

【0097】

(1) Window表示フラグ=1ならば、STEP 2-9実行時にWindow生成手段をWebクライアント10に送信する。

【0098】

(2) Window表示フラグ=2ならば、STEP 2-9実行時にスクロール関数をWebクライアント10に送信する。

【0099】

(3) Window表示フラグ=3ならば、変数displayの先頭に「<html 40
><body>」を挿入し、末尾に「</body></html>」を挿入する。

[STEP 4-7]

変数display 又は配列class を表示文字列としてSTEP 2-9に進む。

【0100】

以上が表示文字列生成手段110の処理である。

【0101】

ここで、STEP 4-4-1 (4-2)の処理について以下に説明する。

[STEP 5-1]

配列class[n]に変数displayの末尾に「▼」を挿入した値を代入する。ここで、「▼」は子階層が存在することを示し、ユーザが「▼」をカーソルで選択すると 50

、配列 `class[n+1]` を表示する関数を呼び出す。今、`n=0` とする。

【STEP 5-2】

アクセス制限情報から、アクセス制限情報のURLと同一URLを親URLに持つアクセス制限情報を抽出する。今、以下のアクセス制限情報が抽出されたものとする。

```
http://www2.canon.co.jp/a.html, 0, http://www2.canon.co.jp/index.html, 1
http://www2.canon.co.jp/b.html, 0, http://www2.canon.co.jp/index.html, 0
```

【STEP 5-3】

抽出されたアクセス制限情報 275 からURLとアクセス制御フラグと子フラグを呼び出し、配列 `class[n+1]` に代入する。ここで、アクセス制御フラグが1ならば、STEP 4-3-1 の処理を実行する。 10

【0102】

以上の処理により、リンク含有コンテンツ 40 に記載されているリンク上にユーザがカーソルを移動したときに、予めユーザが選択した表示方法でアクセス権情報を表示デバイス上で表示することができる。

【0103】

<実施の形態 2>

実施の形態 2 が前記実施の形態と異なるのはユーザが直接表示方法を設定するのではなく、Webサーバにリンク含有コンテンツを要求してきたWebクライアントの情報から、Webクライアントに適した表示方法で表示文字列を生成する点である。 20

【0104】

これは、実施の形態 1 のSTEP 2-4 のユーザ情報取得手段 90 の処理を以下のように変更すると実施できる。

(2-1)

ユーザ情報取得手段 90 は、Webクライアント 10 から送信されたGETメソッド 241 のヘッダに記述されているUSER-AGENT情報を取得する。ここで、USER-AGENT情報は以下のように記述されているとする。

【0105】

USER-AGENT : Mozilla/4.06 [ja] (WinNT; I 30)

(2-2)

USER-AGENT情報からWebクライアントの種類とバージョン、Webクライアントが動作しているオペレーティングシステム（以下、“OS”と記述する）を取得する。本実施の形態では、USER-Agent情報よりWebクライアントの種類は“Mozilla”でバージョンは“4.06”，OSは“WinNT”である。

(2-3)

ユーザ情報取得手段 90 は、2次記憶装置 150 が保管するクライアント情報テーブル 234 から、Webクライアントの種類とバージョン、OSが一致するデータを抽出する。

【0106】

ここで、以下のデータが抽出されたものとする。 40

【0107】

null, 0, 0, 0, 1

ここで、上記データは図 25 における表示方法IDの順と同じ順序で並んでおり、表示できるIDの場合は1、表示できない場合は0で示している。又、“null”は表示できる方法ではあるが、更に上位の表示方法IDで表示できる方法があるため、nullとしている。

(2-4)

2-3 で抽出されたデータより、Webクライアント 10 で表示できる表示方法は表示方法ID 5 である。この表示方法IDを表示文字列生成手段 110 に渡し、STEP 2-8 50

に処理を進める。

【0108】

以上の処理により、Webクライアントの種類やバージョン、Webクライアントが動作しているOSによって表示方法を変更することができる。これにより、ユーザが自分で使用しているWebクライアントの種類に合わせて表示方法を設定することなく、Webクライアントに適した表示方法を提供することができる。

【0109】

＜実施の形態3＞

実施の形態3が前記実施の形態と異なるのはユーザが複数の表示方法を設定できる点である。これは、実施の形態1のSTEP1-6を(3-1)に、STEP2-4を(3-2) 10

(3-1)

(3-1-1)

表示方法設定手段60は、Webクライアント10の種類とバージョン、Webクライアントが動作しているOSを取得する。

【0110】

ここで、取得方法は実施の形態2の2-1, 2-2と同様である。

【0111】

(3-1-2)

3-1-1で取得したWebクライアント10の種類とバージョン、OSとSTEP1- 20
5で送信されたユーザIDのデータが2次記憶装置150の保管するユーザ設定テーブル235に登録されていないかを確認する。本実施の形態では、図26に示すように、ユーザ設定テーブル235に登録されていないため、下記データを登録する。

【0112】

Canon, 5, Mozilla/4.06, WinNT

ここで、上記データは「ユーザID、表示方法ID、Webクライアントの種類／バージョン、OS」という形式で記述されているものとする。

【0113】

以上の処理により、ユーザはWebクライアントの種類／バージョン、OS毎に表示方法を設定することができる。 30

【0114】

次に、リンク含有コンテンツ40を要求したWebクライアント10の種類／バージョン、OSとユーザIDからユーザ設定テーブル235に登録されたデータを抽出し、それに合わせた表示文字列を生成する処理について説明する。

(3-2)

(3-2-1)

ユーザ情報取得手段90は、Webクライアント10が保持するCookie情報からSessionIDを抽出する。ここで、SessionID とユーザIDは一致するものとする。

【0115】

又、Webクライアント10の種類とバージョン情報をUSER-AGENT情報から取得する。ここで取得されたSessionID は「canon」 40

であり、Webクライアント10の種類／バージョンはMozilla/4.06, OSはWinNT であるとする。

【0116】

(3-2-2)

3-2-1で取得したSessionID とWebクライアント10の種類／バージョン、OS情報のデータと一致するデータを2次記憶装置150が保管するユーザ設定テーブル235から抽出する。ここで抽出されたデータは以下のように記述されているものとする。 50

【0117】

canon, 5, Mozilla/4.06, WinNT
(3-2-3)

表示方法手段110に3-2-2で抽出したデータに記述されている表示方法IDを渡し、STEP2-8に進む。

【0118】

以上の処理により、ユーザが複数の種類が異なるWebクライアントからリンク含有コンテンツを要求しても、そのWebクライアントに合わせた表示方法であり、且つ、ユーザが望む表示方法で表示することができる。

【0119】

10

<実施の形態4>

実施の形態4が前記実施の形態と異なるのは設定フォームコンテンツのフォーム内容をWebクライアントに合わせて変更させている点である。これは、実施の形態1のSTEP1-4の処理を以下の処理に変更することで実施できる。

(4-1)

Webクライアント10の種類/バージョン、OS情報を取得する。取得方法は実施の形態2の2-1, 2-2と同様である。ここで、種類はMozilla、バージョンは4.06、OSはWinNTが取得されたものとする。

(4-2)

20

クライアント情報テーブル234から4-1で取得したWebクライアント10の種類/バージョン、OSで表示することが可能な表示方法のIDを取得する。ここで、表示方法ID5が取得されたものとする。

(4-3)

4-2で取得した表示方法IDで設定できる表示方法のみの設定フォームを生成する。ここで、表示方法ID5は、「Window表示は可能、リンク表示は不可、強調表示は可能、強調タイプは『大きさ』である、複数Window表示は不可」という表示方法であるため、設定フォームは図27のようになる。

(4-4)

30

4-3で生成した設定フォームをWebクライアント10に送信する。

【0120】

以上の処理により、Webクライアント10が表示できる方法のみを設定する設定フォームを送信することができる。これにより、ユーザは使用中のWebクライアントが表示できない方法を選ぶという無駄な処理を削除することができる。

【0121】

【発明の効果】

以上の説明で明らかなように、本発明によればユーザは自分の好む表示方法やWebブラウザの種類、Webブラウザが動作しているOSといった環境に合わせたアクセス制限の表示方法で表示することができ、Webサーバから送られてきたアクセス制限情報を表示できないというエラーを排除することができるという効果が得られる。

40

【図面の簡単な説明】

【図1】本発明のシステム構成図である。

【図2】表示方法設定手段の処理の流れ図である。

【図3】ユーザ認証手段の処理の流れ図である。

【図4】ユーザ登録手段の処理の流れ図である。

【図5】アクセス制限情報を表示するまでの処理の流れ図である。

【図6】アクセス制限情報を表示するまでの処理の流れ図である。

【図7】アクセス制限情報取得手段の処理の流れ図である。

【図8】アクセス制限情報取得手段の処理の流れ図である。

【図9】アクセス制限情報取得手段の処理の流れ図である。

50

- 【図 1 0】 U R L 取得手段の処理の流れ図である。
- 【図 1 1】 C o o k i e 情報設定手段の処理の流れ図である。
- 【図 1 2】 本発明を実施した結果の例を示す図である。
- 【図 1 3】 実施例 1 のシステム構成図である。
- 【図 1 4】 アクセス制限が掛かっているコンテンツの送信例を示す図である。
- 【図 1 5】 設定フォームコンテンツの例を示す図である。
- 【図 1 6】 認証コンテンツの例を示す図である。
- 【図 1 7】 ユーザ登録フォームの例を示す図である。
- 【図 1 8】 表示文字列生成手段の処理の流れ図である。
- 【図 1 9】 表示文字列生成手段の処理の流れ図である。
- 【図 2 0】 複数 W i n d o w 生成の処理の流れ図である。
- 【図 2 1】 ユーザ I D テーブルの例を示す図である。
- 【図 2 2】 表示方法テーブルの例を示す図である。
- 【図 2 3】 ユーザ設定テーブルの例を示す図である。
- 【図 2 4】 認証 U R L テーブルの例を示す図である。
- 【図 2 5】 クライアント情報テーブルの例を示す図である。
- 【図 2 6】 ユーザ設定テーブルの例を示す図である。
- 【図 2 7】 設定フォームの例を示す図である。

10

【符号の説明】

- 1 0 W e b クライアント
- 2 0 ネットワーク
- 3 0 ~ 3 2 W e b サーバ
- 4 0 , 4 3 リンク含有コンテンツ
- 4 1 , 4 2 , 4 4 アクセス制限が掛けられたコンテンツ
- 4 5 設定フォームコンテンツ
- 4 6 認証コンテンツ
- 4 7 ユーザ登録フォームコンテンツ
- 5 0 ~ 5 3 リンク
- 6 0 表示方法設定手段
- 7 0 ユーザ認証手段
- 8 0 ユーザ登録手段
- 9 0 ユーザ情報取得手段
- 1 0 0 アクセス制限情報取得手段
- 1 1 0 表示文字列生成手段
- 1 2 0 アクセス制限情報表示手段
- 1 3 0 U R L 取得手段
- 1 4 0 C o o k i e 情報設定手段
- 1 5 0 2 次記憶装置
- 1 6 0 表示デバイス
- 1 7 0 テキスト入力デバイス
- 1 8 0 ポイント入力デバイス
- 1 9 0 カーソル
- 2 0 0 W i n d o w
- 2 1 0 ~ 2 1 2 送信ボタン
- 2 1 2 , 2 1 3 登録ボタン
- 2 2 0 , 2 2 1 表示方法設定フォーム
- 2 2 1 , 2 2 3 ユーザ I D 入力フォーム
- 2 2 2 , 2 2 4 パスワード入力フォーム
- 2 3 0 ユーザ I D テーブル
- 2 3 1 表示方法テーブル

20

30

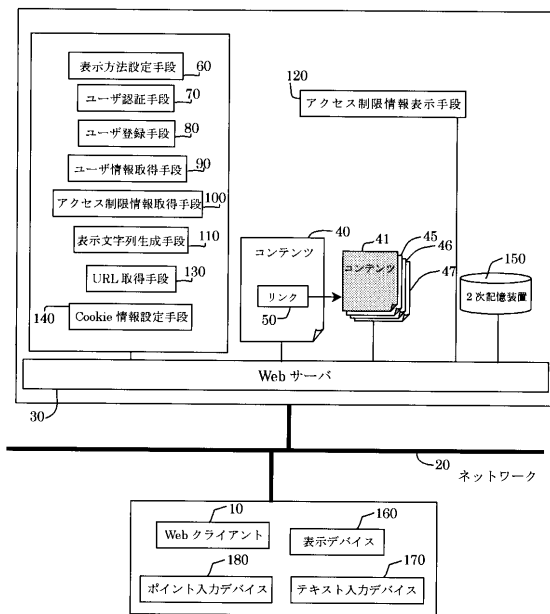
40

50

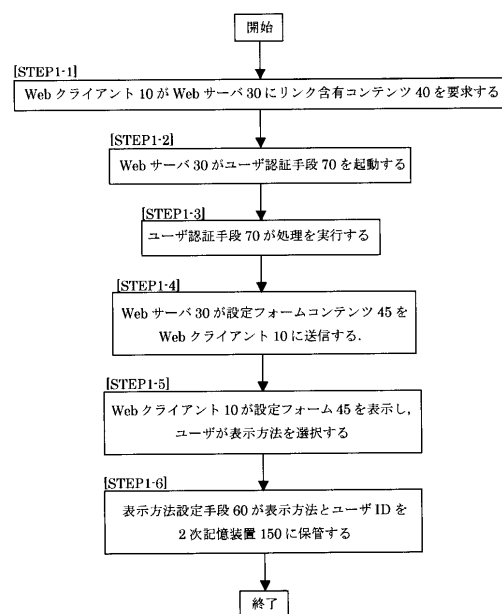
232, 235 ユーザ設定テーブル
 233 認証URLテーブル
 234 クライアント情報テーブル
 240～242 GETメソッド
 250 登録データ
 260 表示文字列
 270～273 アクセス制限情報
 280, 281 サーバ名
 290 CGIプログラム
 291 JavaScriptプログラム

10

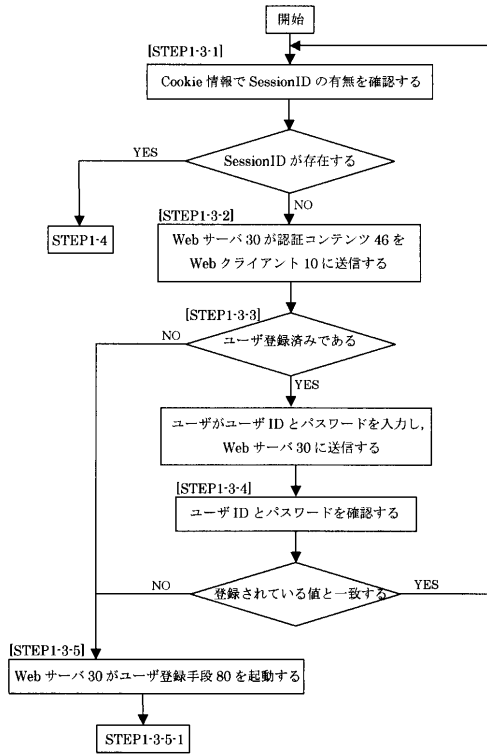
【図1】



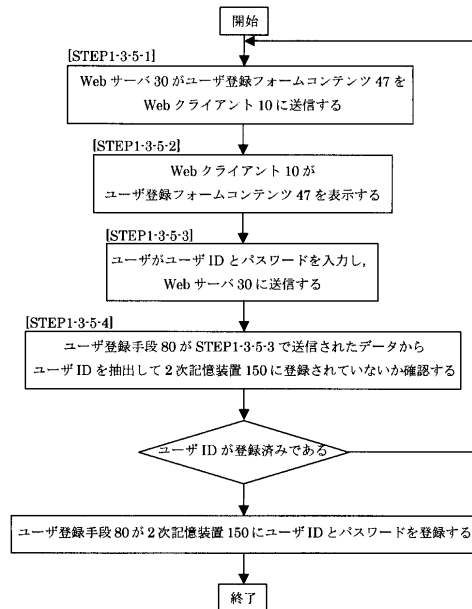
【図2】



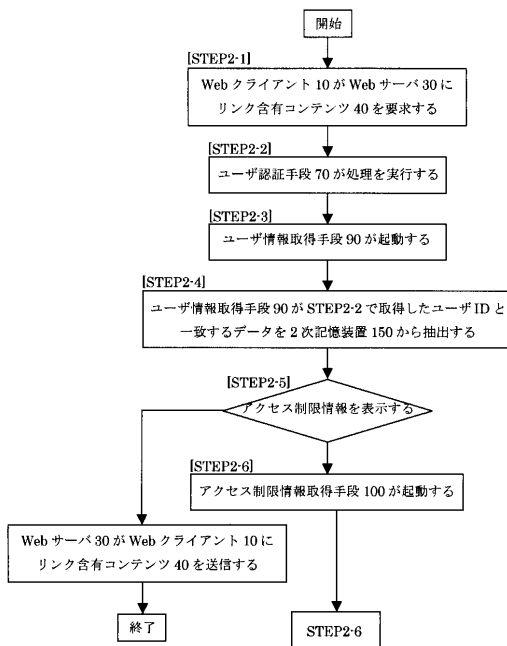
【図 3】



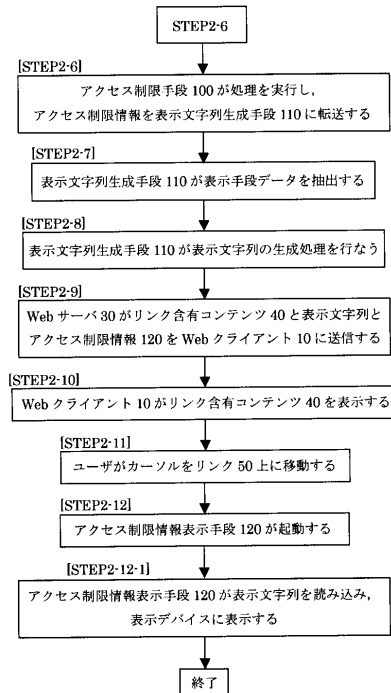
【図 4】



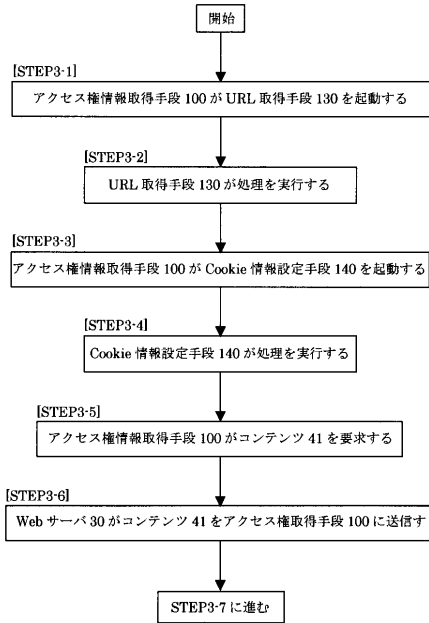
【図 5】



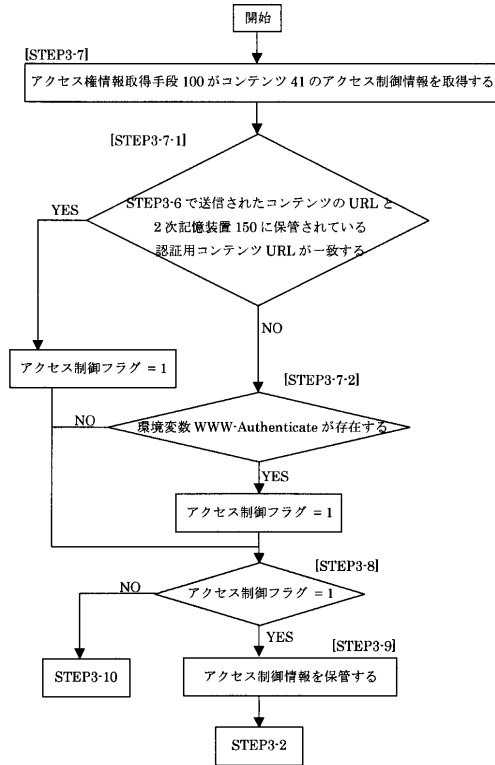
【図 6】



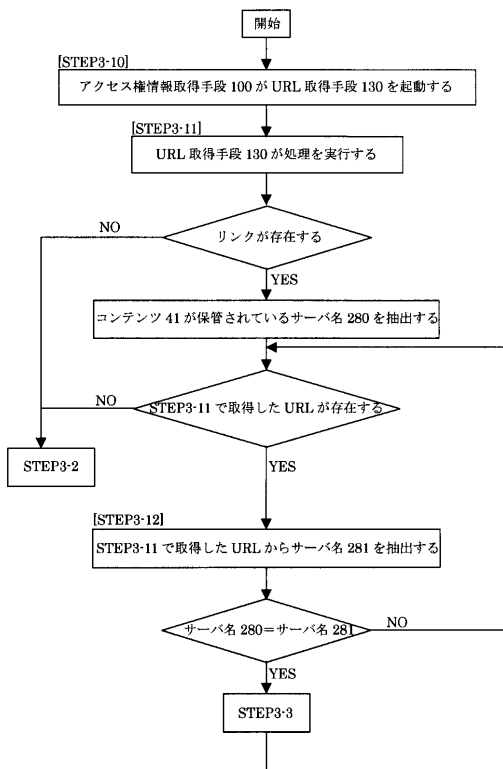
【図 7】



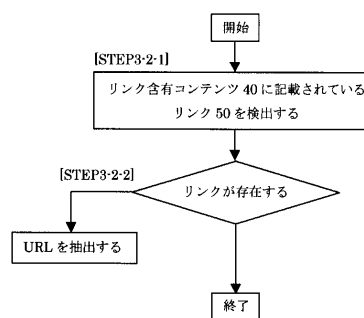
【図 8】



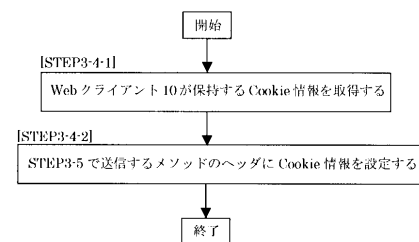
【図 9】



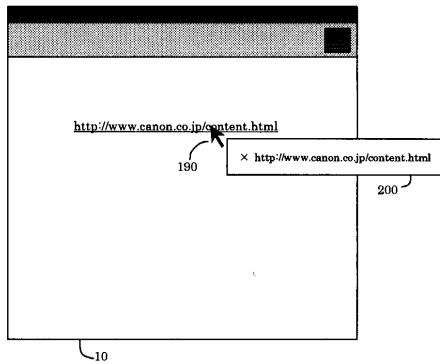
【図 10】



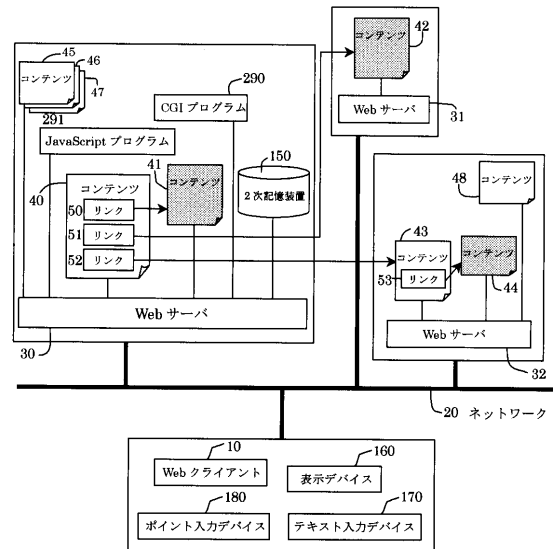
【図 11】



【図 12】



【図 13】

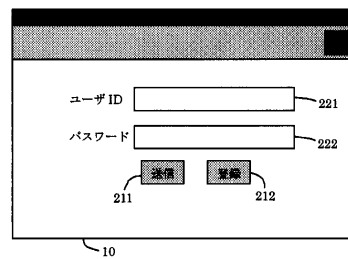


【図 14】

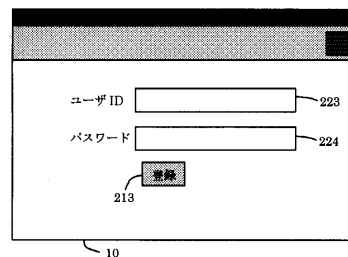
HTTP/1.1 401 Authorization Required
 Date: Fri, 15 Dec 2000 05:49:13 GMT
 Server: Apache/1.3.9 (Unix)
 WWW-Authenticate: Basic realm="ByPassword"
 Connection: close
 Content-Type: text/html

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>401 Authorization Required</TITLE>
</HEAD><BODY>
<H1>Authorization Required</H1>
This server could not verify that you are authorized to access the
document requested. Either you supplied the wrong credentials (e.g.,
bad password), or your browser doesn't understand how to supply the
credentials required.<p>
</BODY></HTML>
```

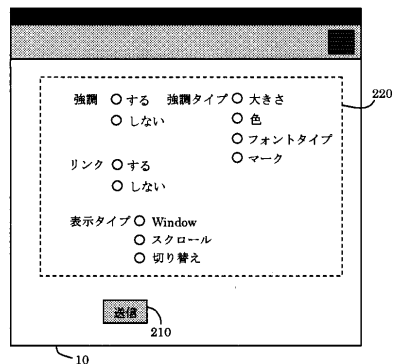
【図 16】



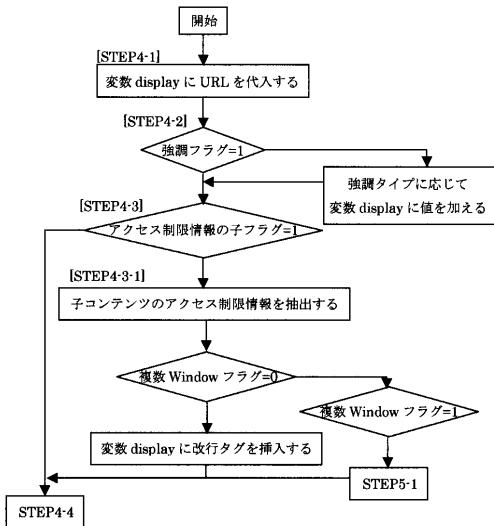
【図 17】



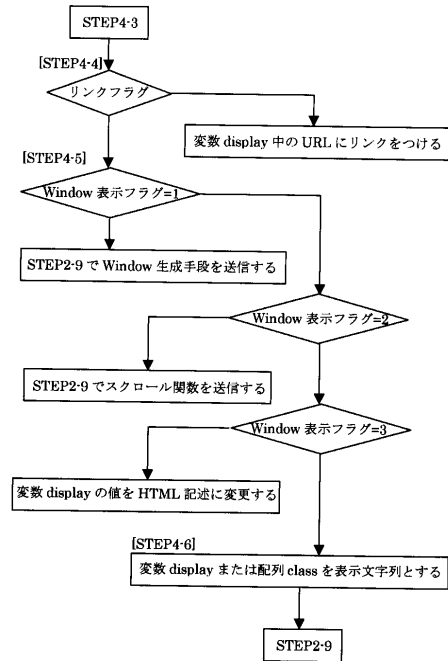
【図 15】



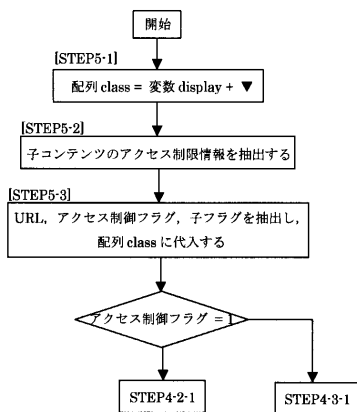
【図 18】



【図 19】



【図 20】



【図 22】

表示方法 ID	Window 表示	リンク	強調	強調タイプ	複数 Window
1	1	0	0		0
2	1	0	0		1
3	1	1	0		0
4	1	1	0		1
5	1	0	1	大きさ	0
6	1	0	1	大きさ	1
7	1	1	1	大きさ	0
8	1	1	1	大きさ	1
9	1	0	1	色	0
10	1	0	1	色	1
11	1	1	1	色	0
12	1	1	1	色	1
13	1	0	1	フォントタイプ	0
14	1	0	1	フォントタイプ	1
15	1	1	1	フォントタイプ	0
16	1	1	1	フォントタイプ	1
17	1	0	1	マーク	0
18	1	0	1	マーク	1
19	1	1	1	マーク	0
20	1	1	1	マーク	1
21	2	0	0		0
31	3	0	0		0

【図 21】

ユーザ ID	パスワード
sato	pass1
suzuki	pass2
yamada	pass3

【図 23】

ユーザ ID	表示	表示方法 ID
sato	0	
suzuki	1	10
yamada	1	13

【図 24】

認証 URL
http://www.canon.co.jp/login.html
http://www2.canon.co.jp/login.html

【図 2 5】

種類/Version, OS	表示方法 ID				
	1	2	3	4	5
Mozilla/3.2, Win95	1	0	0	0	0
Mozilla/4.0, WinNT	1	0	0	0	0
Mozilla/4.06 WinNT	null	0	0	0	1
MSIE/4.0, WinNT	null	0	1	0	0
MSIE/5.0, WinNT	null	0	0	0	1

【図 2 6】

ユーザ ID	表示方法 ID	種類/Version, OS
canon	1	MSIE/5.0, Win95
suzuki	3	Mozilla/4.05, Win98
suzuki	1	MSIE/5.0, WinNT

【図 2 7】

Window 表示 ☐ する
☐ しない

強調 ☐ する 強調タイプ: 大きさ
☐ しない

送信 (212)

10

221