

(19) 日本国特許庁 (JP)

## (12) 特 許 公 報 (B2)

(11) 特許番号

特許第4305146号  
(P4305146)

(45) 発行日 平成21年7月29日 (2009. 7. 29)

(24) 登録日 平成21年5月15日 (2009. 5. 15)

|                                |                       |
|--------------------------------|-----------------------|
| (51) Int. Cl.                  | F I                   |
| <b>G 0 6 F 15/00 (2006.01)</b> | G O 6 F 15/00 3 1 O E |
| <b>G 0 6 F 21/20 (2006.01)</b> | G O 6 F 15/00 3 3 O B |
| <b>G 0 6 F 13/00 (2006.01)</b> | G O 6 F 13/00 5 1 O A |
| <b>G 0 9 C 1/00 (2006.01)</b>  | G O 9 C 1/00 6 4 O E  |

請求項の数 4 (全 15 頁)

|           |                               |           |                       |
|-----------|-------------------------------|-----------|-----------------------|
| (21) 出願番号 | 特願2003-396541 (P2003-396541)  | (73) 特許権者 | 000005496             |
| (22) 出願日  | 平成15年11月27日 (2003. 11. 27)    |           | 富士ゼロックス株式会社           |
| (65) 公開番号 | 特開2005-157822 (P2005-157822A) |           | 東京都港区赤坂九丁目7番3号        |
| (43) 公開日  | 平成17年6月16日 (2005. 6. 16)      | (74) 代理人  | 100075258             |
| 審査請求日     | 平成18年10月20日 (2006. 10. 20)    |           | 弁理士 吉田 研二             |
|           |                               | (74) 代理人  | 100096976             |
|           |                               |           | 弁理士 石田 純              |
|           |                               | (72) 発明者  | 廣瀬 陽一                 |
|           |                               |           | 神奈川県川崎市高津区坂戸3丁目2番1号   |
|           |                               |           | K S P R & D ビジネスパークビル |
|           |                               |           | 富士ゼロックス株式会社内          |
|           |                               | 審査官       | 桑原 雅子                 |

最終頁に続く

(54) 【発明の名称】 通信制御装置、アプリケーションサーバ、およびプログラム

(57) 【特許請求の範囲】

## 【請求項 1】

利用者によりクライアント端末から送信された、指定したサービス処理装置が処理する処理対象データと、指定したサービス処理装置を特定するサービス識別子とを含む情報データを受信する受信手段と、

前記受信手段により受信された情報データを送信したクライアント端末の利用者が所定の認証装置の認証を受けていない場合、当該クライアント端末と当該情報データに含まれるサービス識別子とに関連づけて、当該情報データに含まれる処理対象データを保持する保持手段と、

前記受信手段により受信された情報データを送信したクライアント端末の利用者が前記認証装置の認証を受けていない場合、当該クライアント端末に対して、前記認証装置への認証要求を指示する認証要求指示手段と、

クライアント端末から前記認証要求の指示に対する認証が済んだことを示す通知を受けるのを待って、前記保持手段に保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該クライアント端末から送信されたデータとして、当該処理対象データに関連づけられたサービス識別子に基づき特定したサービス処理装置に提供する提供手段と、

を備える通信制御装置。

## 【請求項 2】

利用者によりクライアント端末から送信された、指定したアプリケーション処理装置が

10

20

処理する処理対象データがボディ領域に書き込まれ、かつ指定したアプリケーション処理装置のアドレスがヘッダ領域に書き込まれたPOSTメソッドを受信する受信手段と、

前記受信手段により受信されたPOSTメソッドを送信したクライアント端末の利用者が所定の認証サーバの認証を受けていない場合、当該クライアント端末と当該POSTメソッドのヘッダ領域に書き込まれたアプリケーション処理装置のアドレスとに関連づけて、当該POSTメソッドのボディ領域に書き込まれた処理対象データを保持する保持手段と、

前記受信手段により受信されたPOSTメソッドを送信したクライアント端末の利用者が所定の認証サーバの認証を受けていない場合、当該クライアント端末に対して、前記認証サーバへの認証要求を指示するリダイレクトを行うリダイレクト手段と、

クライアント端末から前記リダイレクト手段が行ったリダイレクトに対する認証が済んだことを示すGETメソッドによる通知を受けるのを待って、前記保持手段に保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該クライアント端末から送信されたデータとして、当該処理対象データに関連づけられたアドレスに基づき特定したアプリケーション処理装置に提供する提供手段と、

を備える通信制御装置。

#### 【請求項3】

クライアント端末からのアクセスを制御する通信制御手段と、アクセスしてきたクライアント端末によって指定されたアプリケーションサービスのサービス処理を実行するサービス処理手段と、を備えるアプリケーションサーバにおいて、

前記通信制御手段は、

利用者によりクライアント端末から送信された、前記サービス処理手段がサービス処理を実行する処理対象データと、指定されたアプリケーションサービスを特定するサービス識別子とを含む情報データを受信する受信手段と、

前記受信手段により受信された情報データを送信したクライアント端末の利用者が所定の認証サーバの認証を受けていない場合、当該クライアント端末と当該情報データに含まれるサービス識別子とに関連づけて、当該情報データに含まれる処理対象データを保持する保持手段と、

前記受信手段により受信された情報データを送信したクライアント端末の利用者が前記認証装置の認証を受けていない場合、当該情報データを送信したクライアント端末に対して、前記認証サーバへの認証要求を指示する認証要求指示手段と、

クライアント端末から前記認証要求の指示に対する認証が済んだことを示す通知を受けるのを待って、前記保持手段に保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該処理対象データに関連づけられたサービス識別子に基づき特定したアプリケーションサービスのサービス処理を実行させるために、当該処理対象データに関連づけられたクライアント端末から送信されたデータとして、前記サービス処理手段に提供する提供手段と、

を備えるアプリケーションサーバ。

#### 【請求項4】

利用者によりクライアント端末から送信された、指定したサービス処理装置が処理する処理対象データと、指定したサービス処理装置を特定するサービス識別子とを含む情報データを受信する受信手段、

前記受信手段により受信された情報データを送信したクライアント端末の利用者が所定の認証装置の認証を受けていない場合、当該クライアント端末と当該情報データに含まれるサービス識別子とに関連づけて、当該情報データに含まれる処理対象データを保持部に保持させる保持手段、

前記受信手段により受信された情報データを送信したクライアント端末の利用者が前記認証装置の認証を受けていない場合、当該情報データを送信したクライアント端末に対して、前記認証装置への認証要求を指示する認証要求指示手段、

クライアント端末から前記認証要求の指示に対する認証が済んだことを示す通知を受け

10

20

30

40

50

るのを待って、前記保持部が保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該クライアント端末から送信されたデータとして、当該処理対象データに関連づけられたサービス識別子に基づき特定したサービス処理装置に提供する提供手段、

としてコンピュータを機能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、通信制御装置、特に、認証を受けたクライアント端末に対して、所定のサービスを提供するために、クライアント端末からのアクセスを制御する通信制御装置に関する。

10

【背景技術】

【0002】

従来、認証サーバのユーザ認証を受けたクライアント端末に対してのみ、HTTP通信により、各種サービスを提供するWebサーバが知られている。このようなWebサーバを含むネットワークシステムでは、クライアント端末からWebサーバに対してアクセスがあった場合、Webサーバは、まず、そのクライアント端末を操作するユーザがすでに認証サーバの認証を受けているか否かを判定する。判定の結果、未認証ユーザの場合は、クライアント端末に対して、認証サーバの認証を受けるように指示を出す。そして、クライアント端末から、認証サーバによるユーザ認証を受けた旨の通知を受けるのを待って、Webサーバは、そのクライアント端末との間にセッションを確立させ、そのクライアント端末に対して、各種サービスを提供する。

20

【0003】

このようなHTTP通信を利用して、Webサーバが、ユーザ認証を行ったクライアント端末に対して、各種サービスを提供するシステムとして、例えば、特開2003-296277号公報（以下、特許文献1）に開示された技術がある。

【0004】

この特許文献1では、HTTP通信として、HTTPのGETメソッドやPOSTメソッドを利用して通信を行い、HTTPの機能の一つであるリダイレクトを使用して、ユーザ認証を行っている。

30

【0005】

ここで、GETメソッドとは、サーバ等へアクセスする場合に使用するメソッドであり、HTTPメッセージ形式の一つである。具体的には、GETメソッドを構成するヘッダ領域に記述されるURL（Uniform Resource Identifier）に直接送信先へ送りたいデータを記述する形式のことをいう。例えば、ヘッダ領域に記述されるURLが、「http://test.fujixerox.co.jp/login?user=fuji&passwd=xerox」という記述の場合、「？」より前の記述が、データ送信先となるサーバ等のアクセス先（アドレス）を示し、「？」より後の記述が、送信先のサーバ等へ送信すべきデータを示す。つまり、GETメソッドを使用する場合、ヘッダ領域に記述されたデータのみ送信すれば、所望のデータを送信先のサーバ等へ送信することができる。しかし、GETメソッドのURLに書き込むことが可能なデータ量には、制限があり、大量のデータを送信する場合などには適さない。一方、POSTメソッドも、サーバ等へアクセスする場合に使用するメソッドの一つであり、HTTPメッセージ形式の一つである。しかし、ヘッダ領域とは別に定義されたボディ領域に、送信先のサーバ等へ送信すべきデータを記述する点で、GETメソッドとは異なる。POSTメソッドを利用する場合、ヘッダ領域のデータのほかに、HTTP通信において、ボディ領域のデータも送信先のサーバ等に送信する必要がある。POSTメソッドは、送信するデータ量が多かったり、メッセージにファイルを添付して送信する場合や、直接URLに書き込んで送信することで、サーバ上にデータをログとして残したくない場合などに使用されることが多い。また、リダイレクトとは、アクセスしてきた端末等に対して、別の接続先へアクセスするように指示を出すことをいう。

40

50

## 【0006】

このようなGETメソッド等を利用して、特許文献1では、次のように、ユーザ認証を行っている。

## 【0007】

まず、WWWブラウザは、GETメソッドを用いて、例えば、「GET url1 HTTP/1.X」といった要求メッセージを、WWWアプリケーションに送信する。ここで、「url1」は、WWWアプリケーションのURLを示す。WWWアプリケーションは、WWWブラウザからのアクセスを受けると、SSOサーバ（認証サーバ）の認証を受けたユーザからのアクセスか否かを判断する。そして、まだ認証が済んでいないユーザからのアクセスであった場合、WWWアプリケーションは、SSOサーバによるユーザ認証を受けるように、SSOサーバへのリダイレクトをWWWブラウザに対して指示する。

10

## 【0008】

そして、WWWアプリケーションからのリダイレクトを受信したWWWブラウザは、その要求に従い、指定されたURLを有するSSOサーバに対して、アクセスし、ユーザ認証要求を行う。SSOサーバは、ユーザ認証が成功すると、WWWアプリケーションにアクセスするように、WWWアプリケーションへのリダイレクトをWWWブラウザに対して指示する。リダイレクト指示を受けたWWWブラウザは、再度WWWアプリケーションにアクセスすることで、セッションが保持され、所望のサービスの提供を受ける。

## 【0009】

このように、HTTPのリダイレクトを利用して、ユーザ認証を行う場合、クライアント端末（WWWブラウザ）は、WWWアプリケーションに直接アクセスすれば、その後、リダイレクトの機能により、自動的に認証サーバにアクセスし、認証成功後は、さらにリダイレクトすることで、クライアント端末は、WWWアプリケーションとの間にセッションを確立できるため、クライアント端末は、認証サーバのURLを直接知らなくても、サービスの提供を受けることができる。

20

## 【0010】

【特許文献1】特開2003-296277号公報

【発明の開示】

【発明が解決しようとする課題】

## 【0011】

30

上述したような認証サーバの認証成功により保持された、クライアント端末とWWWアプリケーションとのセッションは、永続的に確立しておくこと、WWWアプリケーションの処理を行うサーバのメモリ空間を圧迫したり、セキュリティ上の問題があるため、クライアント端末からのレスポンスが一定の期間なかった場合、強制的にセッションを切断するようにシステムも構成するのが一般的である。しかしながら、このように構成されたシステムにおいて、リダイレクトの機能を利用すると、リダイレクトのRFCの規定上、次のような課題が生じる。

## 【0012】

すなわち、リダイレクトは、RFC2616の規定されているとおり、GETメソッドのみ使用可能であり、リダイレクトを受け取った受信側は、リダイレクトに示されたURLに対して、GETメソッドを用いてアクセスを行う。POSTメソッドを使用して、アクセスした場合でも、RFCの規定上、リダイレクトは、GETメソッドによりアクセスが行われる。すると、GETメソッドには、上述のようにボディ領域について定義されていないため、POSTメソッドに対してリダイレクトが行われた場合、POSTメソッドのボディ領域に含まれるデータは、リダイレクトによって、失われてしまうこととなる。

40

## 【0013】

したがって、従来において、クライアント端末とWWWアプリケーションとの間にセッションが確立されてから一定期間経過後に、クライアント端末が、WWWアプリケーションに処理させたデータを作成して、POSTメソッドを用いて、そのデータをボディ領域に書き込み、WWWアプリケーションにアクセスしたとしても、すでにセッションが切断

50

され、上述したような認証に伴うリダイレクトが行われると、クライアント端末から送信されたPOSTメソッドのボディ領域に書き込まれたデータは失われてしまう。よって、クライアント端末は、先ほど作成したデータを、WWWアプリケーションに提供し処理してもらうためには、ユーザ認証が行われ、セッションが再確立された後に、同じデータを再度作成し、POSTメソッドにて再送する必要がある。

#### 【0014】

上記では、HTTP通信において、リダイレクトを用いた認証を行った後にアプリケーションを提供するシステムにおいて、タイムアウト等が原因で、一度確立されたセッションが切断してしまい、再認証が行われたことにより、POSTメソッドのボディ領域に書き込まれたデータが失われてしまうことを例として挙げた。しかし、このようなデータの喪失は、認証後に、タイムアウト等が原因で、一度確立されたセッションが切断してしまい、再度認証が行われるシステムでは、同様に起こる可能性がある。

#### 【0015】

本発明は、上記課題を鑑みてなされたものであり、認証を伴うアプリケーションを利用するシステムにおいて、アプリケーションの利便性の向上を図ることを目的とする。

#### 【課題を解決するための手段】

#### 【0016】

本発明に係る通信制御装置は、利用者によりクライアント端末から送信された、指定したサービス処理装置が処理する処理対象データと、指定したサービス処理装置を特定するサービス識別子とを含む情報データを受信する受信手段と、前記受信手段により受信された情報データを送信したクライアント端末の利用者が所定の認証装置の認証を受けていない場合、当該クライアント端末と当該情報データに含まれるサービス識別子とに関連づけて、当該情報データに含まれる処理対象データを保持する保持手段と、前記受信手段により受信された情報データを送信したクライアント端末の利用者が前記認証装置の認証を受けていない場合、当該クライアント端末に対して、前記認証装置への認証要求を指示する認証要求指示手段と、クライアント端末から前記認証要求の指示に対する認証が済んだことを示す通知を受けるのを待って、前記保持手段に保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該クライアント端末から送信されたデータとして、当該処理対象データに関連づけられたサービス識別子に基づき特定したサービス処理装置に提供する提供手段と、を備える。

#### 【0017】

本発明によれば、未認証のクライアント端末が送信した情報データであった場合でも、その情報データに含まれる処理対象データを、保持手段に保持しておき、そのクライアント端末からの認証済み報告通知を受けるのを待って、提供手段が、保持手段に保持した処理対象データを、そのサービス対象データに関連づけられたクライアント端末から送信されたデータとして、そのサービス対象データに関連づけられたサービス識別子に基づき特定したサービス処理装置に提供することができる。これにより、例えば、クライアント端末は、情報データを送信した際に、未認証であった場合でも、認証を受けた後、改めて同一の情報データを送信する手間が省け、利便性の向上を図ることができる。

#### 【0018】

本発明に係る通信制御装置は、利用者によりクライアント端末から送信された、指定したアプリケーション処理装置が処理する処理対象データがボディ領域に書き込まれ、かつ指定したアプリケーション処理装置のアドレスがヘッダ領域に書き込まれたPOSTメソッドを受信する受信手段と、前記受信手段により受信されたPOSTメソッドを送信したクライアント端末の利用者が所定の認証サーバの認証を受けていない場合、当該クライアント端末と当該POSTメソッドのヘッダ領域に書き込まれたアプリケーション処理装置のアドレスとに関連づけて、当該POSTメソッドのボディ領域に書き込まれた処理対象データを保持する保持手段と、前記受信手段により受信されたPOSTメソッドを送信したクライアント端末の利用者が所定の認証サーバの認証を受けていない場合、当該クライアント端末に対して、前記認証サーバへの認証要求を指示するリダイレクトを行うリダイ

レクト手段と、クライアント端末から前記リダイレクト手段が行ったリダイレクトに対する認証が済んだことを示すGETメソッドによる通知を受けるのを待って、前記保持手段に保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該クライアント端末から送信されたデータとして、当該処理対象データに関連づけられたアドレスに基づき特定したアプリケーション処理装置に提供する提供手段と、を備える。

#### 【0019】

本発明によれば、アプリケーション処理装置が処理する処理対象データがボディ領域に書き込まれたPOSTメソッドを送信したクライアント端末が、所定の認証サーバの認証を受けていなかった場合に、認証要求のためのリダイレクトがなされたとしても、保持手段が、POSTメソッドのボディ領域に書き込まれた処理対象データを一時保持し、提供手段が、クライアント端末からGETメソッドによる認証済み報告通知を受けるのを待って、その処理対象データをアプリケーション処理装置に提供する。よって、例えば、処理対象データがボディ領域に書き込まれたPOSTメソッドを送信したクライアント端末が、所定の認証サーバの認証を受けていなかった場合に、認証要求のためのリダイレクトがなされたとしても、その処理対象データは、破棄されることなく、アプリケーション処理装置に提供されるため、クライアント端末は、同じ処理対象データがボディ領域に書き込まれたPOSTメソッドを再度送信する手間が省け、利便性の向上につながる。

本発明に係るアプリケーションサーバは、クライアント端末からのアクセスを制御する通信制御手段と、アクセスしてきたクライアント端末によって指定されたアプリケーションサービスのサービス処理を実行するサービス処理手段と、を備えるアプリケーションサーバにおいて、前記通信制御手段は、利用者によりクライアント端末から送信された、前記サービス処理手段がサービス処理を実行する処理対象データと、指定されたアプリケーションサービスを特定するサービス識別子とを含む情報データを受信する受信手段と、前記受信手段により受信された情報データを送信したクライアント端末の利用者が所定の認証サーバの認証を受けていない場合、当該クライアント端末と当該情報データに含まれるサービス識別子とに関連づけて、当該情報データに含まれる処理対象データを保持する保持手段と、前記受信手段により受信された情報データを送信したクライアント端末の利用者が前記認証装置の認証を受けていない場合、当該情報データを送信したクライアント端末に対して、前記認証サーバへの認証要求を指示する認証要求指示手段と、クライアント端末から前記認証要求の指示に対する認証が済んだことを示す通知を受けるのを待って、前記保持手段に保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該処理対象データに関連づけられたサービス識別子に基づき特定したアプリケーションサービスのサービス処理を実行させるために、当該処理対象データに関連づけられたクライアント端末から送信されたデータとして、前記サービス処理手段に提供する提供手段と、を備える。

本発明に係るプログラムは、利用者によりクライアント端末から送信された、指定したサービス処理装置が処理する処理対象データと、指定したサービス処理装置を特定するサービス識別子とを含む情報データを受信する受信手段、前記受信手段により受信された情報データを送信したクライアント端末の利用者が所定の認証装置の認証を受けていない場合、当該クライアント端末と当該情報データに含まれるサービス識別子とに関連づけて、当該情報データに含まれる処理対象データを保持部に保持させる保持手段、前記受信手段により受信された情報データを送信したクライアント端末の利用者が前記認証装置の認証を受けていない場合、当該情報データを送信したクライアント端末に対して、前記認証装置への認証要求を指示する認証要求指示手段、クライアント端末から前記認証要求の指示に対する認証が済んだことを示す通知を受けるのを待って、前記保持部が保持した処理対象データのうち、当該クライアント端末に関連づけられた処理対象データを、当該クライアント端末から送信されたデータとして、当該処理対象データに関連づけられたサービス識別子に基づき特定したサービス処理装置に提供する提供手段、としてコンピュータを機能させる。

10

20

30

40

50

【発明を実施するための最良の形態】

【0020】

本発明の実施の形態（以下、実施形態とする）について、以下、図面を用いて説明する。図1は、本実施形態におけるシステム構成を示す図である。図1において、WWWブラウザ10、WWWアプリケーション20、認証サーバ30は、ネットワーク40を介して相互にHTTPなどのプロトコルを使用して通信を行う。本実施形態では、WWWブラウザ、WWWアプリケーション、認証サーバは、それぞれ1つのみシステム上に存在するが、もちろん、多くのWWWブラウザ、WWWアプリケーション、認証サーバを含むシステムでもよい。

10

【0021】

WWWブラウザ10は、クライアント端末（図示せず）上で動作するソフトウェアであり、ネットワーク40を介して、HTTP通信により様々なサービスや情報の提供を受ける。クライアント端末は、例えば、デスクトップコンピュータ、ラップトップコンピュータ、PDA、携帯電話など、ネットワークに接続可能な端末であって、WWWブラウザが動作する環境を提供可能な端末であれば何でもよい。

【0022】

WWWアプリケーション20は、WWWブラウザ10に対して各種のサービスを提供する。また、WWWアプリケーション20は、コンピュータなどのネットワーク装置（サーバ）上でWWWブラウザ10にサービスを提供するソフトウェアである。また、WWWアプリケーション20は、ユーザ認証が行われたユーザにのみサービスを提供する。

20

【0023】

認証サーバ30は、WWWブラウザ10からのアクセスに対して、ユーザ認証を行うとともに、WWWアプリケーション20からの要求に応じてユーザ認証結果を返す。

【0024】

ここで、さらに、WWWアプリケーション20と認証サーバ30について説明する。

【0025】

WWWアプリケーション20は、通信制御部21と処理部22とを含み構成されている。通信制御部21は、ネットワーク40を介して、WWWブラウザ10からのアクセスを受け付けて、対応する処理を行う。例えば、未認証のWWWブラウザ10からのアクセスを受け付けた際には、WWWブラウザ10を利用しているユーザが認証済みであるか否かを判断する。そして、判断の結果、未認証であれば、認証の判断等に使用するリクエストIDを発行するとともに、WWWブラウザ10に対して、認証サーバ30へのリダイレクトを行う。これにより、WWWブラウザ10に対して、認証サーバ30による認証を受けさせる。また、認証済みのWWWブラウザ10からのアクセスであった場合には、先に発行したリクエストIDを受け取って、処理部22にサービスを行わせる。また、通信制御部21は、リダイレクトによりWWWブラウザ10から、認証済み報告通知を受けると、WWWブラウザ10との間のセッションを一定期間保持する。ただし、そのセッションは、一定期間経過後は、切断し、その後再度そのユーザからアクセスがあった場合は、再度WWWブラウザ10に対して、認証サーバ30へのリダイレクトを行う。

30

40

【0026】

さらに、本実施形態における通信制御部21は、アクセスしてきたWWWブラウザ10が未認証であって、それがPOSTメソッドを用いたアクセスであった場合、リダイレクトに伴うGETメソッドを用いた認証済み報告の通知を受けるまでの間、そのPOSTメソッドのボディ領域に書き込まれたデータを一時保持することを特徴としている。そして、通信制御部21は、WWWブラウザ10からのGETメソッドを用いた認証済み報告を受けた後に、そのGETメソッドを、先ほど一時保持したデータがボディ領域に書き込まれたPOSTメソッドとなるようにエミュレートして、処理部22へ渡す。これにより、POSTメソッドを用いてアクセスしてきたWWWブラウザ10が、未認証ユーザからの

50

アクセスであった場合にも、POSTメソッドのボディ領域に書き込まれたデータは破棄されることなく、処理部22に提供される。

#### 【0027】

これにより、例えば、WWWブラウザ上に表示された各入力フォームに、ユーザが必要に応じて、データを入力して、WWWアプリケーションの管理するデータベースに登録するようなシステムでは、次のような効果がある。すなわち、WWWブラウザ10が、ユーザ認証を受けた後に、WWWアプリケーション20から、図2に示すようなブラウザ表示画面を受け取り、ユーザが、クライアント端末に備えられたキーボードなどを使用して、各入力フォームに必要な事項を入力する。ここで、入力フォームに入力されるデータとしては、テキストデータであったり、文書作成ツールなどの他のソフトウェアで作成した文書データや画像データ等の添付ファイルデータなどである。そして、データを入力した後、WWWブラウザ10が、その入力データのデータ形式変換を行い、その入力内容をボディ領域に書き込んでPOSTメソッドにより、WWWアプリケーション20へアクセスを試みる。その際に、例えば、ユーザが入力フォームに内容を入力する時間が多くかかったことなどが原因で、入力途中に、ユーザ認証によって確立されたWWWブラウザ10とWWWアプリケーション20との間のセッションがタイムアウトして、切断されてしまうことがある。その場合、WWWアプリケーション20は、リダイレクトにより、改めてWWWブラウザ10に対して認証を受けさせる。しかし、上述したように、リダイレクトは、RFCの規定上、GETメソッドを用いて行われるため、従来のWWWアプリケーションでは、先ほど、WWWブラウザ10より受け取ったPOSTメソッドのボディ領域に書き込まれたデータを破棄せざるを得なかった。一方、本実施形態におけるWWWアプリケーション20は、通信制御部21において、POSTメソッドのボディ領域に書き込まれたデータを一時保持しておき、認証の確認を行ったのちに、そのデータを処理部22に提供することができるため、認証が終了したのち、ユーザは改めて、各入力フォームに同じ内容を入力する必要がなく、WWWアプリケーションの利便性の向上を果たすことができる。

#### 【0028】

認証サーバ30は、認証部31と、個人情報管理データベース32とを含み構成されている。認証部31は、WWWブラウザ10からのアクセスに応じて認証処理を行うと伴に、WWWアプリケーション20からの問い合わせに応じて認証結果の返送などを行う。また、WWWブラウザ10からのアクセスを受けたとき、WWWブラウザ10のユーザが未認証である場合には、WWWブラウザ10に対して、図3に示すような認証フォームを送信してユーザによるユーザIDやパスワードなどの入力情報を受け取る。そして、その入力情報に基づいて、個人情報管理データベース32への問い合わせを行って、ユーザの認証を行う。認証済のユーザによるWWWブラウザ10からのアクセスに対しては、WWWブラウザに対して認証フォームを送信することはせずに、認証処理は行わない。

#### 【0029】

なお、この例では個人情報管理データベース32を認証サーバ30内に設けられるように図示しているが、これに限らず、認証サーバ30とは別のサーバにより構成することも可能である。また、それぞれの構成要素は実際の装置構成と一致しない場合もある。例えば、複数のWWWアプリケーションを一台のコンピュータに実装してもよいし、一台のコンピュータにおいて、WWWアプリケーションと認証サーバとを実現しても構わない。また、例えば、WWWアプリケーション20の通信制御部21と処理部22とを、別々の装置として構成しても構わない。

#### 【0030】

続いて、本実施形態において、未認証のWWWブラウザ10が、WWWアプリケーション20にアクセスしてきた場合の、ユーザ認証フローについて、図4に示すシーケンス図を元に説明する。

#### 【0031】

WWWブラウザ10を利用しているユーザは、WWWアプリケーション20を利用する場合には、WWWアプリケーション20のURL (url1) を入力し、アクセスを指示

する。するとWWWブラウザ10は、WWWアプリケーション20へのアクセスを行う（S101）。このときのHTTPの要求メッセージでは“GET”メソッドを用い、例えば“GET url1 HTTP/1.x”といった要求メッセージをWWWアプリケーション20へ送る。

#### 【0032】

WWWアプリケーション20の通信制御部21は、WWWブラウザ10からのアクセスを受けると、WWWブラウザ10との間にセッションが存在するか否か、すなわち認証済みか否かを判断する（S102）。セッションの有無は、WWWアプリケーション20内に保持しているセッションオブジェクトとして登録されているか否かを判断するなど、任意の方法によって行えばよい。ここではそれまでにWWWブラウザ10との間にセッションが存在しない。そこで、セッションを確立するために、まず新たに、そのWWWブラウザとWWWアプリケーションとを関連づけた固有の識別子であるリクエストIDを一時的に発行して、セッションオブジェクトとして登録しておく（S103）。 10

#### 【0033】

WWWアプリケーション20の通信制御部21は、WWWブラウザ10とのセッションが存在していなかったため、WWWブラウザ10に対して認証サーバ30による認証を行うように促すために、認証サーバ30へのリダイレクトをWWWブラウザ10に対して指示する（S104）。具体的には、認証サーバ30のURLをssoとすると、応答時のコード“302”を用い、応答メッセージとして例えば“HTTP/1.x 302 Moved Temporarily Location:sso+id”などとして、リダイレクトによりアクセスするように応答すればよい。なお、“sso+id”は、認証サーバ30のURL“sso”に、WWWアプリケーション20が一時的に発行したリクエストIDを付加したものである。さらに、WWWアプリケーション20のURLも付加しておくともよい。また、応答時にWWWアプリケーション20用の仮のクッキー(cookie)をWWWブラウザ10に送っておいてもよい。 20

#### 【0034】

WWWブラウザ10は、上述のようなWWWアプリケーション20からの応答メッセージを受けると、自動的に認証サーバ30に対して、認証要求をするためにアクセスを行う（S105）。このようなリダイレクトを利用することによって、ユーザは認証サーバ30のURL等を知らなくても、利用したいWWWアプリケーションにアクセスすれば、初回は認証サーバ30へ自動的にアクセスされるので、利便性を向上させることができる。 30

#### 【0035】

また、自動的に行われるWWWブラウザ10から認証サーバ30へのアクセス時の要求メッセージは、具体的には“GET”メソッドを用い、アドレス部分はS104で渡された“Location:”以降の部分、すなわち“sso+id”である。例えば“GET sso+id HTTP/1.x”といった要求メッセージがWWWブラウザ10から認証サーバ30へ渡される。なお、アドレス部分にWWWアプリケーション20のURLが含まれる場合もある。

#### 【0036】

認証サーバ30では、WWWブラウザ10からのアクセスを受けた場合、この時点ではいまだにWWWブラウザ10とのセッションはなく、認証を行っていない。従って、認証サーバの認証部31が、新規にセッションを生成し、内部にセッションオブジェクトとして登録しておく。このとき、アドレス部分で渡された、通信制御部21で生成したリクエストIDを用いることができる。また、アドレス部分にWWWアプリケーション20のURLが含まれる場合、そのURLも保持しておく。 40

#### 【0037】

新たにWWWブラウザ10からアクセスされた場合、認証部31は、認証を行うための認証フォームをWWWブラウザ10へ送る（S106）。具体的には応答コード“200”を用い、例えば応答ヘッダ“HTTP/1.x 200 OK”と、認証フォームのデータを応答メッセージとしてWWWブラウザ10に送信すればよい。このとき、認証サーバ 50

30用の仮のクッキーを送信しておいてもよい。

#### 【0038】

ユーザが、認証フォームに表示された欄にユーザID及びパスワードを入力したのち、そのユーザが入力したユーザID及びパスワードがWWWブラウザ10から認証サーバ30へ送られる(S107)。

#### 【0039】

WWWブラウザ10から認証サーバ30へユーザID及びパスワードを送信する場合の具体的な要求メッセージは、“POST”メソッドを用い、例えばリクエストラインとして“POST sso HTTP/1.x”、ボディ領域にユーザが入力したユーザID及びパスワードを含めればよい。

10

#### 【0040】

認証部31は、WWWブラウザ10からユーザIDおよびパスワードを受け取ると、個人情報管理データベース32への問い合わせを行い、ユーザの認証を行う(S108)。ユーザIDとパスワードが正しくなければ、認証できなかった旨をWWWブラウザ10に通知し、再入力を受けるかあるいは処理を終了する。

#### 【0041】

受け取ったユーザIDとパスワードが正しければ、WWWブラウザ10のユーザを正規のユーザとして認証する。このとき、認証サーバ30へのログインが行われ、認証済である状態がユーザのユーザIDとともにセッションオブジェクトとして登録される。

#### 【0042】

認証サーバ30の認証部31での認証が行われたら、認証部31はWWWブラウザ10に対してWWWアプリケーション20へのリダイレクトをするように、応答メッセージを返す(S109)。具体的には、応答コード“302”を使用し、例えば“HTTP/1.x 302 Moved Temporarily Location:url1”とし、WWWアプリケーション20のURL(“url1”)を指定したリダイレクトをWWWブラウザ10に指示すればよい。

20

#### 【0043】

認証サーバ30からのリダイレクトを受けたWWWブラウザ10は、GETメソッドを用いて、認証サーバ30によるユーザ認証が済んだことを通知するために、WWWアプリケーション20にアクセスする(S110)。WWWブラウザ10からのアクセスを受けたWWWアプリケーション20の通信制御部21は、認証サーバ30に対して、先ほど発行したリクエストIDをキーとして、認証されたユーザ名を要求し(S111)、その要求に応じて、認証サーバ30の認証部31は、認証されたユーザ名をWWWアプリケーション20に送信する(S112)。要求したユーザ名を受信した通信制御部21は、ユーザ認証が適正に行われたユーザからのアクセスであると判断して、WWWブラウザ10からの受信したデータを処理部22へ渡し、WWWブラウザ10からの要求に応じたサービスを提供する(S113)。例えば、処理部22は、通信制御部21を介して、図2に示す表示画面フォームをWWWブラウザ10に送信する。

30

#### 【0044】

このように、ユーザ認証を受けたユーザに対してのみ、サービスを提供するWWWアプリケーションにおいて、リダイレクトを用いて、自動的にWWWブラウザに対して、認証要求を行わせることで、WWWブラウザは、直接認証サーバのURL等を知ることなしに、ユーザ認証を受けて、サービスの提供を受けることができる。

40

#### 【0045】

しかしながら、認証を受けた後、図2に示すような表示画面フォームが提供されたWWWブラウザ10において、ユーザが各入力フォームに必要な事項の入力を行っている間に、一定時間が経過してしまうことなどが原因で、ユーザ認証に伴い確立されたセッションが切断されてしまうことがある。すると、WWWブラウザ10が、ユーザによるデータ入力が完了した時点で、その入力データをデータベースに登録する処理をWWWアプリケーション20に行ってもらうために、その入力データを、ボディ領域に書き込んで、POST

50

メソッドを用いて、WWWアプリケーション20にアクセスしたとしても、セッションが切断されているために、再度、リダイレクトにより認証が行われる。しかし、リダイレクトは、GETメソッドでのみ行われるため、POSTメソッドのボディ領域に書き込まれたデータは、破棄されてしまう。

#### 【0046】

そこで、本実施形態では、ユーザ認証が済んだものの、一定期間が経過してしまったことなどが原因により、セッションが切断された時点で、WWWブラウザ10が、POSTメソッドを用いて、WWWアプリケーション20にアクセスしてきた場合に、図5に示すようなシーケンスを実行することで、そのPOSTメソッドのボディ領域に書き込まれたデータが破棄されてしまうことを防いでいる。

10

#### 【0047】

すなわち、図5において、ユーザによるデータ入力済みのWWWブラウザ10は、POSTメソッドを用いて、そのボディ領域に入力されたデータを書き込んで、WWWアプリケーション20にアクセスする(S201)。WWWアプリケーション20の通信制御部21は、そのアクセスを受けて、そのWWWブラウザ10がユーザ認証を受けているか否かを判断する(S202)。ここでは、タイムアウト等のために一度ユーザ認証が成功し、確立されていたセッションが切断されてしまった場合を想定しているため、通信制御部21は、そのWWWブラウザ10について、未認証と判断する。そこで、新たにユーザ認証を行うために、改めて、一時的なリクエストIDを発行して(S203)、セッションオブジェクトとして登録しておく。さらに、本実施形態の特徴として、通信制御部21は、そのWWWブラウザとWWWアプリケーションとを関連づけた固有の識別子であるリクエストIDに関連づけて、WWWブラウザから受け取ったPOSTメソッドのボディ領域に書き込まれたデータを、通信制御部21が保有するRAM等の記憶部(図示せず)に一時保持する(S204)。

20

#### 【0048】

続いて、通信制御部21は、WWWブラウザ10に対して認証サーバ30による認証を行うように促すために、認証サーバ30へのリダイレクトをWWWブラウザ10に対して指示する(S205)。この指示は、リダイレクトのため、上述したように、RFCの規定により、GETメソッドにより行われる。したがって、従来であれば、WWWブラウザ10からのPOSTメソッドのボディ領域に書き込まれたデータは、WWWアプリケーションによるリダイレクトにより破棄されてしまう。しかし、本実施形態によれば、S205において、POSTメソッドのボディ領域に書き込まれたデータは、リクエストIDと関連づけられて一時保持されるため、破棄されずに済む。

30

#### 【0049】

そして、WWWアプリケーション20からのリダイレクトを受けたWWWブラウザ10は、認証サーバ30との間で、図4に示すシーケンスのS105～S109と同様の処理をS206～S210において、実行する。さらに、認証サーバ30による認証に成功すると、認証サーバ30の認証部31からのリダイレクトにより、WWWブラウザ10は、WWWアプリケーション20に、認証サーバ30による認証が済んだことを通知するために、GETメソッドを用いてアクセスする(S211)。WWWブラウザ10からのアクセスを受けて、WWWアプリケーション20の通信制御部21は、図4に示すシーケンスのS111～S112と同様の処理をS212～S213において、実行することで、正式にユーザ認証が済んだことを認証サーバ30に対して確認する。

40

#### 【0050】

認証サーバ30への認証確認の後、本実施形態において、特徴的な処理として、通信制御部21は、リクエストIDと関連づけられ、一時保持しているデータが存在するか否かを判断する(S214)。ここでは、先ほど一時保持したデータが存在するため、WWWアプリケーション20は、その一時保持したデータを復元し、POSTメソッド後のrequestオブジェクトをエミュレートするようなラッパーを作成し、処理部22へ渡す(S215)。処理部22は、通信制御部21によって一時保持したデータを復元し、エ

50

ミュレートされたPOSTメソッドを用いて処理を行うため、S201において、POSTメソッドを用いてアクセスした際の、そのPOSTメソッドのボディ領域に書き込まれたデータは破棄されることなく、処理部22において処理されて、その処理結果が、通信制御部21を介してWWWブラウザ10に提供される（S216）。

#### 【0051】

よって、たとえ、図2に示すような表示画面フォームが提供されたWWWブラウザ10において、ユーザが各入力フォームに必要事項の入力を行っている間に、一定時間が経過してしまうことなどが原因で、ユーザ認証に伴い確立されたセッションが切断されてしまい、改めて、リダイレクトにより認証が行われたとしても、通信制御部21が、そのリダイレクトの前にPOSTメソッドを用いてアクセスされた際のデータを復元し、処理部22に提供するため、ユーザは、認証後に再度同じデータを、入力する手間を省くことができ、WWWアプリケーションの利便性の向上につながる。

10

#### 【0052】

なお、本実施形態において、説明したユーザ認証方法は、一例に過ぎず、リダイレクトを用いた認証を行うWWWアプリケーションを含むシステムであれば、どのような認証方法でもよい。また、本実施形態では、ユーザ認証の際に用いるリクエストIDを、POSTメソッドのボディ領域に書き込まれたデータを一時保持する際に、併用している。しかし、リクエストIDとは別に、固有のIDを発行して、そのIDに基づいて、データの保持及び復元を行っても構わない。

#### 【0053】

20

また、本実施形態では、HTTP通信において、リダイレクトを用いた認証を行った後にアプリケーションを提供するシステムにおいて、タイムアウト等が原因で、一度確立されたセッションが切断してしまい、再認証が行われたことにより、POSTメソッドのボディ領域に書き込まれたデータが失われてしまうことを例として挙げた。しかし、HTTP通信でのPOSTメソッドを利用したシステムでなくとも、認証後に、タイムアウト等が原因で、一度確立されたセッションが切断してしまい、再度認証が行われるシステムであれば、同様に、認証前に受信したいデータを一時保持しておき、認証確認後に、その認証前のデータを復元することで、実現可能である。

#### 【0054】

さらに、本実施形態では、WWWブラウザ10とWWWアプリケーション20との間に確立された1つのセッションに対して、1つのPOSTメソッドのボディ領域に書き込まれたデータを関連づけて一時保持するのではなく、WWWブラウザ10とWWWアプリケーション20とに関連づけて発行されるリクエストIDに関連づけて、POSTメソッドのボディ領域に書き込まれたデータを一時保持する。よって、確立された1つのセッションに対して、POSTメソッドのボディ領域に書き込まれたデータを、複数保持することができる。

30

#### 【0055】

加えて、1つのセッションに、POSTメソッドのボディ領域に書き込まれたデータを、複数保持することができるため、図2に示すような、フレームで複数の入力フォームに分割された画面において、複数のPOSTメソッドにより複数のデータが入力された場合でも、データの競合をすることなく、個々のフレームに入力されたデータを適切に管理し、復元することが可能である。

40

#### 【0056】

また、本実施形態は、WWWアプリケーション20の通信制御部21で行う処理内容に改良を加えるだけで、実現可能なため、処理部22での処理内容や、WWWブラウザ10での処理内容は、従来と同一でよい。したがって、本実施形態を実現するために、WWWアプリケーションのシステム変更を大幅に行ったり、WWWブラウザの仕様を変更する必要がなく、容易に現状のシステムに導入することが可能である。

#### 【図面の簡単な説明】

#### 【0057】

50

【図１】本実施形態におけるシステム構成図である。

【図２】本実施形態のWWWアプリケーションがWWWブラウザに提供する表示画面の一例を示す図である。

【図３】本実施形態の認証サーバが、ユーザ認証を行なうためにWWWブラウザに提供する認証フォームの一例である。

【図４】本実施形態におけるユーザ認証のシーケンスを示す図である。

【図５】本実施形態において、POSTメソッドを送信したWWWブラウザが認証を受けていなかった場合のシーケンスを示す図である。

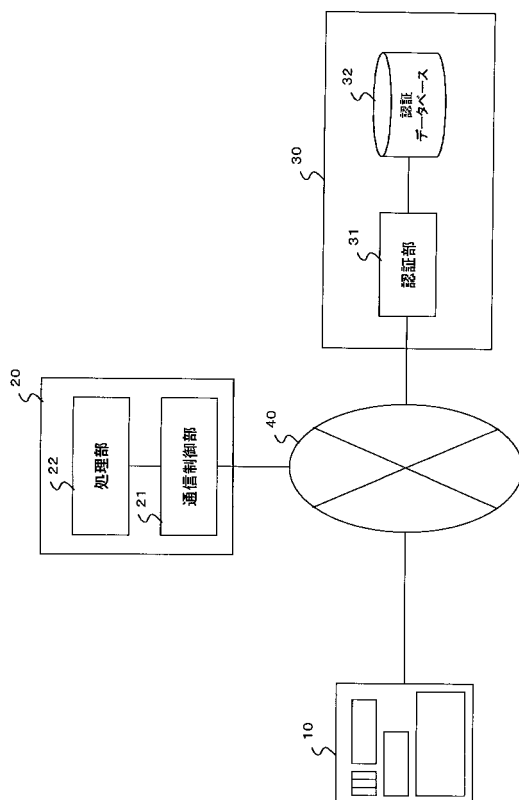
【符号の説明】

【００５８】

１０ WWWブラウザ、２０ WWWアプリケーション、２１ 通信制御部、２２ 処理部、３０ 認証サーバ、３１ 認証部、３２ 個人情報管理データベース、４０ ネットワーク。

10

【図１】



【図２】

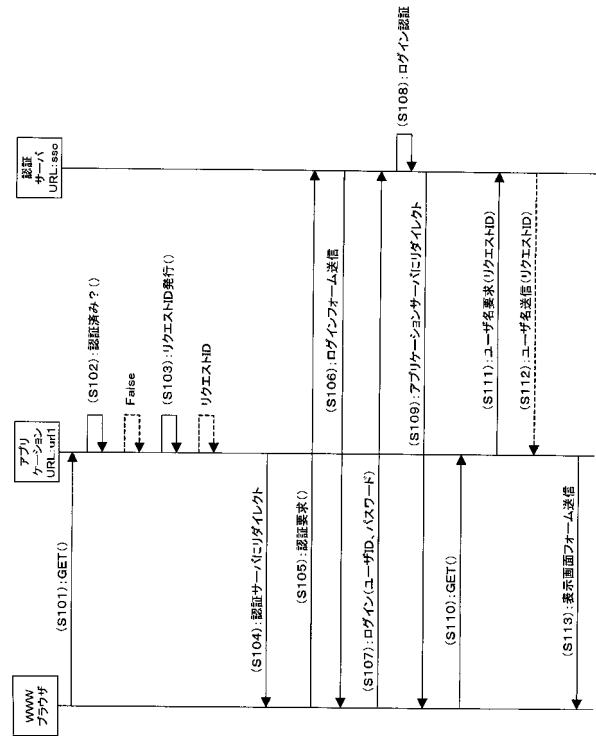
【図 3】

ログイン

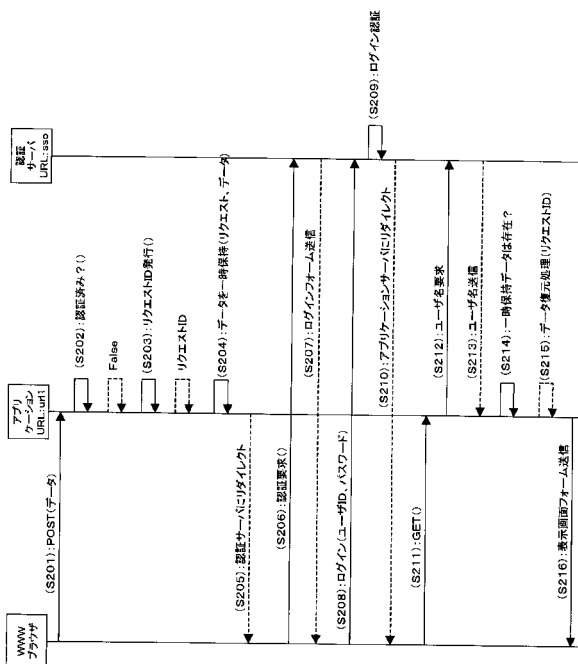
ユーザ名

パスワード

【図 4】



【図 5】



---

フロントページの続き

- (56)参考文献 特開平11-282804 (JP, A)  
特開2003-330865 (JP, A)  
特開平09-265443 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
- |         |           |
|---------|-----------|
| G 0 6 F | 1 5 / 0 0 |
| G 0 6 F | 1 3 / 0 0 |
| G 0 6 F | 2 1 / 2 0 |
| G 0 9 C | 1 / 0 0   |