(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5882833号
(P5882833)
(45)発行日　平成28年3月9日(2016.3.9)　(24)登録日　平成28年2月12日(2016.2.12)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/31
H04L 9/32 (2006.01)　　H04L 9/00 675A

請求項の数 14　(全 11 頁)

(21)出願番号　特願2012-122399(P2012-122399)
(22)出願日　平成24年5月29日(2012.5.29)
(65)公開番号　特開2013-246799(P2013-246799A)
(43)公開日　平成25年12月9日(2013.12.9)
審査請求日　平成27年5月29日(2015.5.29)

(73)特許権者　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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】認証装置、認証システム、認証方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
クライアントから受信したメッセージを認証する認証装置であって、
第１の認証処理を実行可能な第１認証手段であって、前記メッセージに第１の認証情報が含まれるかどうかに基づいて、および、前記第１の認証情報が含まれる場合に前記第１の認証処理を実行した結果に基づいて、第２の認証情報が前記メッセージに含まれているかどうかを解析することなく、前記メッセージに前記第１の認証処理に成功した前記第１の認証情報が含まれているかを示す認証結果を生成する第１認証手段と、
前記メッセージに第２の認証情報が含まれるかどうかを判断し、前記第２の認証情報が含まれると判断した場合、前記第２の認証情報に基づいて第２の認証処理を実行する第２認証手段と、を有し、
前記第２認証手段は、前記第１認証手段によって生成された認証結果および前記第２認証手段によって実行された前記第２の認証処理の認証結果に基づいて、前記メッセージの認証が成功したかどうかを決定する、
ことを特徴とする認証装置。
【請求項２】
前記第２認証手段は、前記メッセージに前記第２の認証情報が含まれず、かつ、前記第１認証手段によって生成された認証結果が、前記第１の認証処理に成功した前記第１の認証情報が含まれていることを示す場合、前記メッセージの認証が成功したと判定する、
ことを特徴とする請求項１に記載の認証装置。

【請求項３】
前記第２認証手段は、前記メッセージに前記第２の認証情報が含まれる場合であって、前記第２の認証処理に成功した場合に、前記メッセージの認証が成功したと判定する、
ことを特徴とする請求項１又は２に記載の認証装置。
【請求項４】
前記第１認証手段において前記メッセージに前記第１の認証情報が含まれている場合であって前記第１の認証処理に失敗した場合、又は、前記第２認証手段において前記第２の認証処理に失敗した場合に、前記クライアントへエラーを通知する通知手段をさらに有する、
ことを特徴とする請求項１から３のいずれか１項に記載の認証装置。
【請求項５】
前記第１認証手段は、前記メッセージに設定された認証方式が前記第１の認証情報を用いる認証方式であるかを判定し、前記メッセージに設定された認証方式が前記第１の認証情報を用いる認証方式でない場合、前記メッセージに前記第１の認証処理に成功した前記第１の認証情報が含まれないことを示す情報を、前記認証結果として生成する、
ことを特徴とする請求項１から４のいずれか１項に記載の認証装置。
【請求項６】
前記第１認証手段は、前記メッセージに認証方式が設定されていない場合、前記メッセージに前記第１の認証処理に成功した前記第１の認証情報が含まれないことを示す情報を、前記認証結果として生成する、
ことを特徴とする請求項５に記載の認証装置。
【請求項７】
前記第１の認証情報は、ＨＴＴＰダイジェスト認証の認証情報である、
ことを特徴とする請求項１から６のいずれか１項に記載の認証装置。
【請求項８】
前記第２の認証情報は、ＷＳ－Ｓｅｃｕｒｉｔｙ認証の認証情報である、
ことを特徴とする請求項１から７のいずれか１項に記載の認証装置。
【請求項９】
前記第２認証手段は、Ｗｅｂサービスの処理を実行するモジュールに含まれ、前記メッセージが、ユーザ認証が不要である前記Ｗｅｂサービスへのリクエストである場合、前記第２の認証情報を用いた認証を実行せずに、当該Ｗｅｂサービスの利用を許可する、
ことを特徴とする請求項１から８のいずれか１項に記載の認証装置。
【請求項１０】
前記第２認証手段は、Ｗｅｂサービスの処理を実行するモジュールに含まれ、前記クライアントのユーザが、前記Ｗｅｂサービスを利用する権限を有さない場合、前記第２の認証情報を用いた認証の結果によらずに、当該Ｗｅｂサービスの利用を許可しない、
ことを特徴とする請求項１から９のいずれか１項に記載の認証装置。
【請求項１１】
前記第１認証手段は、Ｗｅｂサーバの機能部に含まれる、
ことを特徴とする請求項１から１０のいずれか１項に記載の認証装置。
【請求項１２】
クライアントから受信したメッセージを認証する認証システムであって、
第１の認証処理を実行可能な第１認証手段であって、前記メッセージに第１の認証情報が含まれるかどうかに基づいて、および、前記第１の認証情報が含まれる場合に前記第１の認証処理を実行した結果に基づいて、第２の認証情報が前記メッセージに含まれているかどうかを解析することなく、前記メッセージに前記第１の認証処理に成功した前記第１の認証情報が含まれているかを示す認証結果を生成する第１認証手段と、
前記メッセージに第２の認証情報が含まれるかどうかを判断し、前記第２の認証情報が含まれると判断した場合、前記第２の認証情報に基づいて第２の認証処理を実行する第２認証手段と、を有し、

前記第２認証手段は、前記第１認証手段によって生成された認証結果および前記第２認証手段によって実行された前記第２の認証処理の認証結果に基づいて、前記メッセージの認証が成功したかどうかを決定する、
ことを特徴とする認証システム。
【請求項１３】
クライアントから受信したメッセージを認証する認証方法であって、
第１の認証処理を実行可能な第１認証手段が、前記メッセージに第１の認証情報が含まれるかどうかに基づいて、および、前記第１の認証情報が含まれる場合に前記第１の認証処理を実行した結果に基づいて、第２の認証情報が前記メッセージに含まれているかどうかを解析することなく、前記メッセージに前記第１の認証処理に成功した前記第１の認証情報が含まれているかを示す認証結果を生成する第１認証工程と、
第２認証手段が、前記メッセージに第２の認証情報が含まれるかどうかを判断し、前記第２の認証情報が含まれると判断した場合、前記第２の認証情報に基づいて第２の認証処理を実行する第２認証工程と、
前記第２認証手段が、前記第１認証工程において生成された認証結果および前記第２認証工程において実行された前記第２の認証処理の認証結果に基づいて、前記メッセージの認証が成功したかどうかを決定する工程と、
を有することを特徴とする認証方法。
【請求項１４】
コンピュータを請求項１から１１のいずれか１項に記載の認証装置が備える各手段として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、複数の認証方式を用いた認証技術に関する。
【背景技術】
【０００２】
複数の認証情報を用いてユーザや機器を認証する仕組みがある。例えば、複数の認証情報を用いることでより高いセキュリティを確保する技術や、複数の認証の過程を１度経ることにより以降は最初の認証だけ行い利便性を高める技術がある。
【０００３】
特許文献１には、携帯端末ごとに固有の第１の認証情報と、携帯端末ごとに生成した第２の認証情報とを用いて、第１の認証情報を用いた認証が成功した場合に携帯端末との通信を許可し、第２の認証情報を用いた認証処理を行うシステムが記載されている。また、特許文献２には、端末装置に搭載されたアプリケーションを使用するための第１の認証手段と、外部サービスを使用するための第２の認証手段とを備える認証装置が記載されている。引用文献２に記載の認証装置は、第１の認証と第２の認証の両方の認証に成功した場合に得られる認証子を用いてユーザのログイン操作を簡略化する。
【０００４】
また、非特許文献１ではＨＴＴＰダイジェスト認証とＷＳ－Ｓｅｃｕｒｉｔｙの２つの認証を用いて、過去に公開されたＯＮＶＩＦの仕様において使用されていた認証方式と互換性を保つ方法が開示されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００９－１２３０５９号公報
【特許文献２】特開２００９－２２３７３９号公報
【非特許文献】
【０００６】
【非特許文献１】ＯＮＶＩＦ　Ｃｏｒｅ　Ｓｐｅｃ．　Ｖｅｒ．　２．２　ｐｐ．　３０

－３１
【発明の概要】
【発明が解決しようとする課題】
【０００７】
また、非特許文献１の技術では、Ｗｅｂサーバにおいて、ＨＴＴＰダイジェストの認証情報とＷＳＳ（ＷＳ－Ｓｅｃｕｒｉｔｙ）の両方の認証情報の有無を調べることが要求される。そして、非特許文献１の技術では、ＷＳＳの認証情報が含まれていた場合は、ＨＴＴＰダイジェスト認証の認証情報が含まれていなくても、ＨＴＴＰダイジェスト認証は行わずにＷＳＳの認証情報だけで認証処理を行う。しかしながら、Ｗｅｂサーバ内でＷＳＳの認証情報の有無を調べるには、ＨＴＭＬボディ内の解析が必要で処理の負荷が大きいという課題があった。なお、非特許文献１に記載の認証方法において、認証の利便性を高めるために特許文献１又は特許文献２に記載の技術を適用することは困難である。
【０００８】
本発明は上記課題に鑑みなされたものであり、非特許文献１に記載の認証方式と同様の能力を有する認証方式を実現する際に、Ｗｅｂサーバの認証処理の負荷を軽減する技術を提供することを目的とする。
【課題を解決するための手段】
【０００９】
上記目的を達成するため、本発明による認証装置は、クライアントから受信したメッセージを認証する認証装置であって、第１の認証処理を実行可能な第１認証手段であって、前記メッセージに第１の認証情報が含まれるかどうかに基づいて、および、前記第１の認証情報が含まれる場合に前記第１の認証処理を実行した結果に基づいて、第２の認証情報が前記メッセージに含まれているかどうかを解析することなく、前記メッセージに前記第１の認証処理に成功した前記第１の認証情報が含まれているかを示す認証結果を生成する第１認証手段と、前記メッセージに第２の認証情報が含まれるかどうかを判断し、前記第２の認証情報が含まれると判断した場合、前記第２の認証情報に基づいて第２の認証処理を実行する第２認証手段と、を有し、前記第２認証手段は、前記第１認証手段によって生成された認証結果および前記第２認証手段によって実行された前記第２の認証処理の認証結果に基づいて、前記メッセージの認証が成功したかどうかを決定する、ことを特徴とする。

【発明の効果】
【００１０】
本発明によれば、複数の認証方式を用いて認証を実行する際に、Ｗｅｂサーバの処理の負荷を軽減することができる。
【図面の簡単な説明】
【００１１】
【図１】Ｗｅｂサービスシステムの構成図。
【図２】実施形態１のＷｅｂサーバの認証処理を示すフローチャート。
【図３】実施形態１のＷｅｂサービス処理部の処理を示すフローチャート。
【図４】実施形態２のＷｅｂサーバの認証処理を示すフローチャート。
【図５】実施形態２のＷｅｂサービス処理部の処理を示すフローチャート。
【図６】ネットワーク装置を実装するコンピュータを示す概略ブロック図。
【発明を実施するための形態】
【００１２】
以下、添付図面を参照して本発明の実施の形態を詳細に説明する。
【００１３】
＜＜実施形態１＞＞
（システム構成）

本実施形態に係るＷｅｂサービスシステムの構成を図１に示す。Ｗｅｂサービスシステムは、ネットワーク装置１００と、ユーザクライアント１３とを含む。ネットワーク装置１００は、例えばネットワークカメラやネットワーク上のコンピュータである。また、ユーザクライアント１３は例えばパーソナルコンピュータ（ＰＣ）であり、インターネットやＬＡＮなどのネットワークを介してネットワーク装置１００と通信を行う。

【００１４】

ネットワーク装置１００の以下に説明する機能は、例えば、図６に示すような、ＣＰＵ１０１、ＲＯＭ１０２、ＲＡＭ１０３、二次記憶装置１０４、及び通信部１０５を備える、ネットワーク装置１００に内蔵されるコンピュータにより実現される。コンピュータにおいては、ＲＯＭ１０２に記録された本方法に係るプログラムをＣＰＵ１０１により実行する。そして、例えば、ＳＯＡＰメッセージや認証結果情報１６などの情報をＲＡＭ１０３や二次記憶装置１０４に記憶させる。そして、通信部１０５を用いてユーザクライアント１３などと通信を行う。なお、ネットワーク装置１００は、以下に説明する各機能を実行する専用のハードウェアを備えてもよいし、一部をハードウェアで実行し、その他の部分をコンピュータにより実行させてもよい。

【００１５】

ネットワーク装置１００は、Ｗｅｂサービスを提供する装置であり、例えば、図１に示すように、Ｗｅｂサーバ機能部であるＷｅｂサーバ１１と、Ｗｅｂサービスを提供する機能部であるＷｅｂサービス処理部１２とを含む。そして、Ｗｅｂサーバ１１の第１認証処理部１とＷｅｂサービス処理部１２の第２認証処理部２とは、ユーザ認証システムを構築する。Ｗｅｂサーバ１１は、ユーザクライアント１３から、インターネットやＬＡＮなどのネットワークを介してＨＴＭＬメッセージ１４によるＷｅｂサービスのリクエストを受け付ける。

【００１６】

第１認証処理部１は、ＨＴＭＬのユーザ認証の仕組みであるＨＴＭＬダイジェスト認証（第１の認証処理）を実行する。第１認証処理部１は、第１の認証情報であるＨＴＭＬダイジェスト認証の認証情報の有無の判定と認証処理とを実行し、認証結果情報１６を生成する。そして、Ｗｅｂサーバ１１は、不図示の送信部により、ＳＯＡＰメッセージ１５をＷｅｂサービス処理部１２へ送信する。なお、ＳＯＡＰメッセージ１５には、ＨＴＭＬメッセージ１４を構成する少なくとも一部の情報（例えばボディ部分）が含まれ、Ｗｅｂサーバ１１は、ＳＯＡＰメッセージ（ＨＴＭＬメッセージ１４のボディ）の解析は行わない。

【００１７】

Ｗｅｂサービス処理部１２はＷｅｂサービスの処理を行うモジュールで、Ｗｅｂサービスのユーザ認証の仕組みであるＷＳ－Ｓｅｃｕｒｉｔｙ（ＷＳＳ）認証（第２の認証処理）を行う第２認証処理部２を含む。第２認証処理部２は、ＸＭＬで記載されたＳＯＡＰメッセージ１５を解析するエンジンを備え、第２の認証情報であるＷＳＳ認証の認証情報の有無の判定と認証処理とを実行する。Ｗｅｂサービス処理部１２は、ユーザクライアント１３からのＷｅｂサービスの要求を処理し、処理結果をＷｅｂサーバ１１を通してユーザクライアント１３へ送信する。

【００１８】

（第１の認証処理）

図２は、Ｗｅｂサーバ１１内の第１認証処理部１の処理の詳細を示すフローチャートである。Ｗｅｂサーバ１１は、ユーザクライアント１３からＨＴＭＬメッセージ１４を受信すると、ＨＴＭＬを解析してＨＴＴＰダイジェスト認証の認証ヘッダが含まれるかどうかを判定する（Ｓ２１）。Ｗｅｂサーバ１１は、ＨＴＴＰダイジェスト認証の認証ヘッダが含まれていない場合（Ｓ２１でＮｏ）は、認証結果情報１６を「認証情報無し」に設定して生成する（Ｓ２２）。そして、Ｗｅｂサーバ１１は、認証結果情報１６とＳＯＡＰメッセージ１５とを、例えばネットワーク装置１００内のバスを介して、Ｗｅｂサービス処理部１２へ送信する（Ｓ２３）。

【００１９】
ＨＴＴＰダイジェスト認証ヘッダが含まれると判定された場合（Ｓ２１でＹｅｓ）は、Ｗｅｂサーバ１１は、ＨＴＴＰダイジェスト認証の処理を実行する（Ｓ２４）。次に、Ｗｅｂサーバ１１は、ＨＴＴＰダイジェスト認証の結果を判定し（Ｓ２５）、成功していれば（Ｓ２５でＹｅｓ）、認証結果情報１６を「認証情報有り」に設定して生成する（Ｓ２６）。そして、認証結果情報１６とＳＯＡＰメッセージ１５とが、例えばネットワーク装置１００内のバスを介して、Ｗｅｂサービス処理部１２へ送信される（Ｓ２７）。一方、ＨＴＴＰダイジェスト認証に失敗した場合（Ｓ２５でＮｏ）は、Ｗｅｂサーバ１１は、ユーザクライアント１３へＨＴＴＰ４０１エラー（Ｕｎａｕｔｈｏｒｉｚｅｄ）を返し、ＨＴＴＰダイジェスト認証が失敗したことを通知する（Ｓ２８）。

【００２０】
通常のＷｅｂサーバは、ＨＴＴＰダイジェスト認証の認証情報（第１の認証情報）がない場合は、ＨＴＴＰ４０１エラーをユーザクライアント１３へ通知し、ＨＴＴＰダイジェスト認証情報を付加するように促す。しかし、本実施形態においては、Ｓ２３で示した通り、ＨＴＴＰダイジェスト認証は行わず、以下で説明するＷｅｂサービス処理部１２による処理を実行し、ＨＴＴＰ４０１エラーを通知するかの判定はＷｅｂサービス処理部１２が行う。また、Ｗｅｂサーバ１１は、第２の認証情報であるＷＳＳ認証の認証情報の解析は実行しない。すなわち、Ｗｅｂサーバ１１は、ＨＴＴＰダイジェスト認証の認証ヘッダがないか、又は第１の認証情報であるＨＴＴＰダイジェスト認証の認証情報が存在する場合の認証の成否のみを判定し、認証結果情報の内容としてＷｅｂサービス処理部１２へ送信する。

【００２１】
（第２の認証処理）
続いて、Ｗｅｂサービス処理部１２における認証処理を説明する。図３は、Ｗｅｂサービス処理部１２内の第２認証処理部２の処理の詳細を示すフローチャートである。Ｗｅｂサービス処理部１２は、Ｗｅｂサーバ１１から取得したＳＯＡＰメッセージ１５を解析し、第２の認証情報であるＷＳ－Ｓｅｃｕｒｉｔｙ認証情報（ＷＳＳ認証情報）が含まれているかを判定する（Ｓ３１）。ＷＳＳ認証情報がない場合（Ｓ３１でＮｏ）は、Ｗｅｂサービス処理部１２は、Ｗｅｂサーバ１１から取得した認証結果情報１６が「認証情報有り」であるかを判定する（Ｓ３２）。認証結果情報１６が「認証情報有り」であった場合（Ｓ３２でＹｅｓ）は、Ｗｅｂサーバ１１においてＨＴＴＰダイジェスト認証が成功していることになる。このため、Ｗｅｂサービス処理部１２は、ＷＳＳ認証は行わずにＷｅｂサービスの利用を許可し、Ｗｅｂサービスの処理を実行する（Ｓ３４）。認証結果情報１６が「認証情報無し」であった場合（Ｓ３２でＮｏ）は、第１の認証情報であるＨＴＴＰダイジェストの認証情報と、第２の認証情報であるＷＳＳの認証情報との両方が存在しないことになるため、ＨＴＴＰ４０１エラーを返答する（Ｓ３３）。これにより、ユーザクライアント１３へ、ＨＴＴＰダイジェスト認証の認証情報をＨＴＭＬ中に含めてリクエストを送るよう促すことができる。

【００２２】
一方、Ｓ３１において、ＷＳＳ認証情報が含まれていると判定された場合（Ｓ３１でＹｅｓ）は、Ｗｅｂサービス処理部１２は、ＷＳＳ認証処理を行う（Ｓ３５）。Ｗｅｂサービス処理部１２は、次に、ＷＳＳ認証に成功したかどうかを判定し（Ｓ３６）、ＷＳＳ認証に成功した場合（Ｓ３６でＹｅｓ）、ＨＴＴＰダイジェスト認証とＷＳＳ認証の両方に成功したことになる。このため、Ｗｅｂサービス処理部１２は、Ｗｅｂサービスの利用を許可し、Ｗｅｂサービスの処理を実行する（Ｓ３４）。一方、ＷＳＳ認証に失敗したと判定された場合（Ｓ３６でＮｏ）は、ＨＴＴＰダイジェスト認証には成功したがＷＳＳ認証には失敗した場合である。この場合は、Ｗｅｂサービス処理部１２は、ＷＳＳ認証に失敗したことを示すＨＴＴＰ４００エラー（Ｂａｄ　Ｒｅｑｕｅｓｔ）をユーザクライアント１３へ通知する。

【００２３】

なお、Ｓ３３ではＨＴＴＰ４０１エラーを通知しているが、ＨＴＴＰ４０１エラーに加えてＳＯＡＰメッセージでもエラー（４０１　Ｕｎａｕｔｈｏｒｉｚｅｄ）を通知してもよい。このエラー通知もＨＴＴＰダイジェスト認証に失敗したことを示すが、ＳＯＡＰメッセージのエラーまで解釈するかはユーザクライアント１３次第である。

【００２４】

また、Ｓ３７ではＨＴＴＰ４００エラーを通知しているが、ＨＴＴＰ４００エラーに加えてＳＯＡＰメッセージでもエラー（ｔｅｒ：Ｕｎａｕｔｈｏｒｉｚｅｄ）を通知してもよい。このエラー通知もＷＳＳ認証に失敗したことを示すが、ＳＯＡＰメッセージのエラーまで解釈するかはユーザクライアント１３次第である。

【００２５】

非特許文献１によれば、ＷＳＳの認証情報が含まれているかどうかをＨＴＴＰダイジェスト認証を行う前後に判定しなければならず、Ｗｅｂサーバ内にＷＳＳの認証情報をチェックする仕組みが必要である。しかし本実施形態によれば、ＨＴＴＰダイジェスト認証を行うＷｅｂサーバではＷＳＳの認証情報が含まれるかどうかは判定せず、認証結果情報１６を生成してＷｅｂサービス処理部１２へ送る。これにより、Ｗｅｂサーバ内でＷＳＳの認証情報の有無を調べるために、ＨＴＭＬボディ内を解析する必要がなくなり、Ｗｅｂサーバの負荷を軽減することができる。

【００２６】

＜＜実施形態２＞＞

続いて、図４及び図５を参照して、第２の実施形態について説明する。本実施形態におけるシステムの構成は、図１に示す実施形態１の構成と同様であるが、Ｗｅｂサーバ１１とＷｅｂサービス処理部１２に付加機能を設ける。付加機能により、Ｗｅｂサーバ１１とＷｅｂサービス処理部１２は、ＨＴＴＰとＷＳＳの認証の設定や、特定のユーザ権限を有するユーザクライアントの考慮、特定のサービスにおける認証処理の迂回を実行する。特に、本実施形態のＷｅｂサーバ１１の第１認証処理部１は、ＨＴＴＰ認証方式がダイジェスト認証でない場合、ユーザ認証はＷＳＳの認証に任せるため、認証結果情報１６を「認証情報無し」に設定して生成する。

【００２７】

（第１の認証処理）

図４は、Ｗｅｂサーバ１１で、ダイジェスト認証以外のＨＴＴＰ認証方式に対応するために図２に示すフローチャートを拡張した、第１認証処理部１の処理を示すフローチャートである。対応するＨＴＴＰ認証方式は、あらかじめネットワーク装置１００の管理者が、Ｗｅｂサーバ１１の設定として決めておく。

【００２８】

処理が開始されると、Ｗｅｂサーバ１１は、ＨＴＭＬメッセージ１４に設定されたＨＴＴＰ認証の認証方式を判定する（Ｓ４１）。Ｗｅｂサーバ１１は、ＨＴＭＬ認証方式が、第１の認証情報を用いる認証方式である「ダイジェスト認証」であると判定した場合は処理をＳ２１へ進め、以降は実施形態１で示した認証処理と同様の処理を実行する。

【００２９】

一方、Ｗｅｂサーバ１１は、Ｓ４１において、ＨＴＴＰ認証方式を「認証無し」と判定した場合は、認証結果情報１６を「認証情報無し」に設定して生成する（Ｓ２２）。そして、Ｗｅｂサーバ１１は、認証結果情報１６とＳＯＡＰメッセージ１５とを、例えばネットワーク装置１００内のバスを介して、Ｗｅｂサービス処理部１２へ送信する（Ｓ２３）。この場合、Ｗｅｂサービス処理部１２におけるＷＳＳ認証のみが認証処理として実行される。

【００３０】

また、Ｗｅｂサーバ１１は、Ｓ４１において、ＨＴＴＰ認証方式が「ベーシック認証」であると判定した場合、ＨＴＴＰベーシック認証処理を実行し（Ｓ４２）、ＨＴＴＰベーシック認証が成功したかどうかを判定する（Ｓ４３）。そして、Ｗｅｂサーバ１１は、ＨＴＴＰベーシック認証が成功した場合（Ｓ４３でＹｅｓ）は、認証結果情報１６を「認証

情報無し」に設定して生成する（Ｓ２２）。そして、Ｗｅｂサーバ１１は、認証結果情報１６とＳＯＡＰメッセージ１５とを、例えばネットワーク装置１００内のバスを介して、Ｗｅｂサービス処理部１２へ送信する（Ｓ２３）。一方、Ｗｅｂサーバ１１は、ＨＴＴＰベーシック認証が失敗したと判定した場合（Ｓ４３でＮｏ）は、ユーザクライアント１３へＨＴＴＰ４０１エラーを通知し（Ｓ４４）、認証情報の付与を促す。

【００３１】

なお、上述の処理では、ＨＴＭＬメッセージ１４に設定された認証方式が、ＨＴＴＰベーシック認証である場合に、ＨＴＴＰベーシック認証を実行するが、この認証を実行しなくてもよい。例えば、第１の認証情報を用いる認証方式であるＨＴＴＰダイジェスト認証以外の認証方式がＨＴＭＬメッセージ１４に設定されている場合は、その後の認証を行わずに、認証結果情報１６を「認証情報無し」に設定してもよい。また、ＨＴＴＰベーシック認証以外の認証方式が設定されていた場合は、Ｗｅｂサーバ１１は、その設定された認証方式に対応している場合に、その認証方式で認証を実行し、認証に成功した場合に認証結果情報１６を「認証情報無し」に設定してもよい。

【００３２】

（第２の認証処理）

図５は、Ｗｅｂサービス処理部１２で、特定のサービスに対する処理や、ユーザレベル、ＷＳＳの認証を設定ができることを考慮して図３のフローチャートを拡張した、第２認証処理部２の処理を示すフローチャートである。

【００３３】

Ｗｅｂサービス処理部１２は、ＳＯＡＰメッセージを解析し、特定のサービスへのリクエストであるかどうかを判定する（Ｓ５１）。ここで、特定のサービスとは、例えば、ネットワーク装置１００の時刻情報や機能の情報など、ユーザ認証が不要とされるサービスである。ユーザ認証が不要とされるサービスへのリクエストであった場合（Ｓ５１でＹｅｓ）は、Ｗｅｂサービス処理部１２は、第１認証処理部１での認証結果情報１６やＷＳＳの認証情報によらず、Ｗｅｂサービスの利用を許可して処理を実行する（Ｓ５３）。

【００３４】

ＳＯＡＰメッセージがユーザ認証が不要とされるサービスへのリクエストでなく、ユーザ認証が必要なサービスと判定された場合（Ｓ５１でＮｏ）は、Ｗｅｂサービス処理部１２は、ネットワーク装置１００でＷＳＳ認証が有効かを判定する（Ｓ５２）。ＷＳＳ認証の有効または無効の設定は、あらかじめネットワーク装置１００の管理者が設定しておく。Ｗｅｂサービス処理部１２は、ＷＳＳ認証が有効と判定した場合（Ｓ５２でＹｅｓ）は、処理をＳ３１へ進め、以降は実施形態１の図３で示した処理と同様の処理を実行する。

【００３５】

なお、上述の説明では、ＷＳＳの認証情報が含まれており、ＷＳＳの認証情報が誤っている場合であっても、Ｗｅｂサービス処理部１２はＷｅｂサービスを提供するが、これに限られない。例えば、Ｗｅｂサービス処理部１２は、ＷＳＳの認証が有効であってＷＳＳの認証情報が含まれている場合には、ＷＳＳの認証処理を実行して、認証情報が誤っている場合には、ＨＴＴＰ４００エラーを通知するようにしてもよい。

【００３６】

次に、ユーザがサービスを受ける権限を持っていない場合、またはユーザが特定のユーザである場合に、ＷＳＳの認証処理の結果によらず、ユーザ認証を不可と判定する機能について説明する。ネットワークの設定など、ネットワーク装置１００の重要な設定を変更するサービスの場合、特定のユーザ又は権限を持ったユーザだけにサービスを提供したい要求がある。そのため、Ｓ３４又はＷＳＳ認証が無効の時のＳ５３の処理の前に、ユーザクライアント１３がＷｅｂサービスを実行する権限を有するかを判定するようにしてもよい。ユーザに権限がない場合、Ｗｅｂサービスの利用を許可せず、処理を実行せずにＨＴＴＰ４００エラーを通知する。

【００３７】

非特許文献１には、ＷＳＳの認証情報が含まれているかどうかに加え、特定のサービス

へのリクエストや、ユーザ権限によってサービスを制限するアクセス制御機能が記載されている。これを実行するには、Ｗｅｂサーバ１１においてＳＯＡＰメッセージを解析し、どのサービスへのリクエストなのかをチェックし、またはＷＳＳの認証情報をチェックする仕組みが必要である。しかし本実施形態によれば、ＨＴＴＰダイジェスト認証やＨＴＴＰベーシック認証を行うＷｅｂサーバでは、どのサービスへのリクエストか、またはＷＳＳの認証情報が含まれるかの判定は実行せず、認証結果情報１６をＷｅｂサービス処理部１２へ送信する。これにより、Ｗｅｂサーバ１１において、どのサービスへのリクエストか、またはＷＳＳの認証情報を有するかを調べるために、ＨＴＭＬボディ内を解析する必要が無くなり、Ｗｅｂサーバの負荷を軽減することができる。

【００３８】

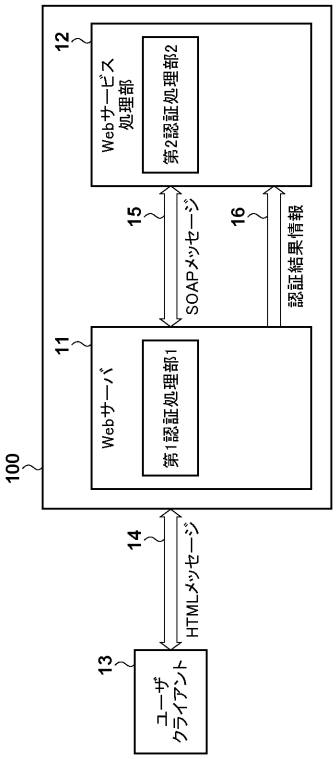
以上、本発明の好ましい実施形態について説明したが、本発明はこれらの実施形態に限定されず、その要旨の範囲内で種々の変形及び変更が可能である。例えば、上述の説明では、Ｗｅｂサーバ１１とＷｅｂサービス処理部１２とを１つネットワーク装置１００に含むものとして説明したが、それぞれ別の装置に実装されてもよい。すなわち、第１認証処理部１を有するＷｅｂサーバ１１に相当する第１認証装置と、第２認証処理部２を有するＷｅｂサービス処理部１２に相当する第２認証装置とを含むネットワークシステムとして実装されてもよい。

【００３９】

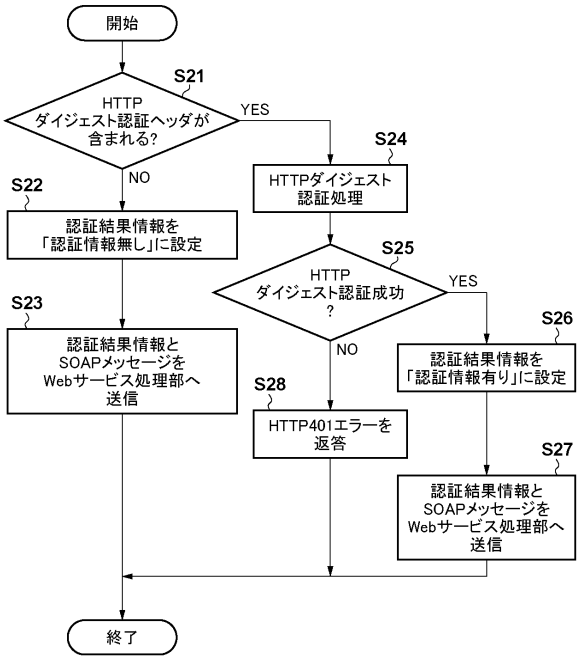
＜＜その他の実施形態＞＞

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

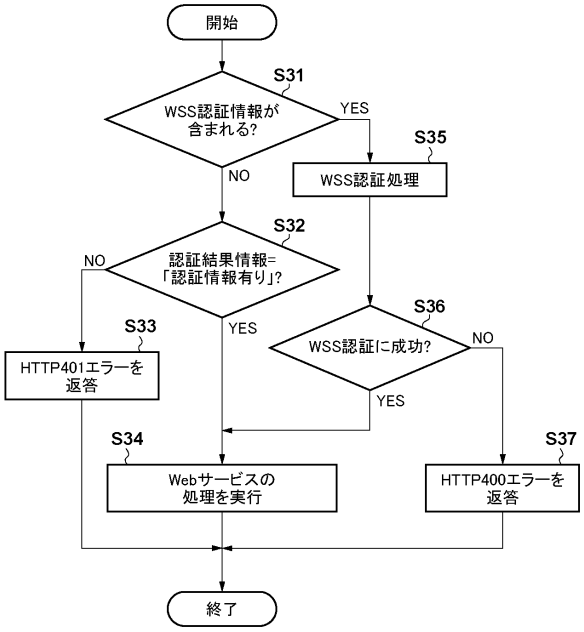
【図１】



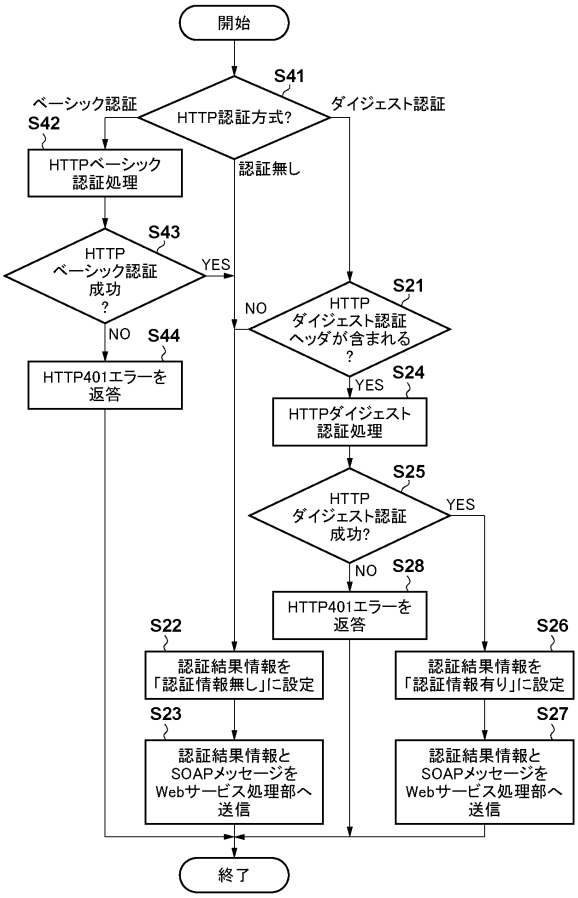
【図２】



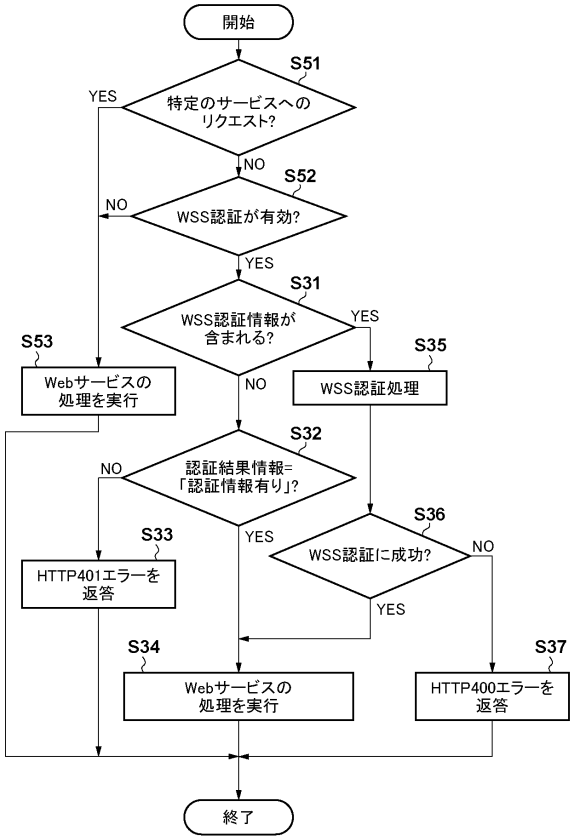
【図３】


開始
S31
WSS認証情報が含まれる?
YES
NO
S35
WSS認証処理
S32
認証結果情報=「認証情報有り」?
NO
YES
S33
HTTP401エラーを返答
S36
WSS認証に成功?
NO
YES
S34
Webサービスの処理を実行
S37
HTTP400エラーを返答
終了

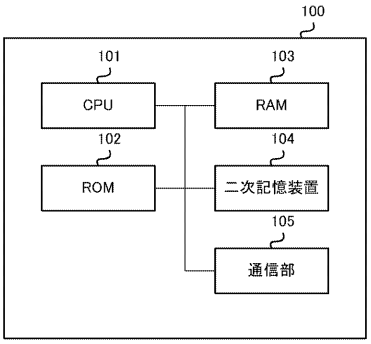
【図４】


開始
S41
HTTP認証方式?
ベーシック認証
ダイジェスト認証
S42
HTTPベーシック認証処理
認証無し
S43
HTTPベーシック認証成功?
YES
NO
S44
HTTP401エラーを返答
S21
HTTPダイジェスト認証ヘッダが含まれる?
NO
YES
S24
HTTPダイジェスト認証処理
S25
HTTPダイジェスト認証成功?
YES
NO
S28
HTTP401エラーを返答
S22
認証結果情報を「認証情報無し」に設定
S23
認証結果情報とSOAPメッセージをWebサービス処理部へ送信
S26
認証結果情報を「認証情報有り」に設定
S27
認証結果情報とSOAPメッセージをWebサービス処理部へ送信
終了

【図５】


開始
S51
特定のサービスへのリクエスト?
YES
NO
S52
WSS認証が有効?
NO
YES
S31
WSS認証情報が含まれる?
YES
NO
S53
Webサービスの処理を実行
S35
WSS認証処理
S32
認証結果情報=「認証情報有り」?
NO
YES
S33
HTTP401エラーを返答
S36
WSS認証に成功?
NO
YES
S34
Webサービスの処理を実行
S37
HTTP400エラーを返答
終了

【図６】


100
101
CPU
103
RAM
102
ROM
104
二次記憶装置
105
通信部

フロントページの続き

(72)発明者　淺野　歩
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

審査官　宮司　卓佳

(56)参考文献　特開２０１０－９２４０７（ＪＰ，Ａ）
特開２００４－３２３１１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３０－Ｇ０６Ｆ　２１／４６
Ｈ０４Ｌ　９／３２