【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成23年5月6日(2011.5.6)

【公表番号】特表2010-525448(P2010-525448A)
【公表日】平成22年7月22日(2010.7.22)
【年通号数】公開・登録公報2010-029
【出願番号】特願2010-504132(P2010-504132)
【国際特許分類】
Ｇ０６Ｆ　21/20　(2006.01)
Ｈ０４Ｌ　 9/32　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　３３０Ｂ
Ｈ０４Ｌ　 9/00　６７３Ａ
Ｈ０４Ｌ　 9/00　６７３Ｄ

【手続補正書】
【提出日】平成23年3月15日(2011.3.15)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
保護されたウェブサービスリソース（１０６）へのアクセスを制御するウェブサービスコンピュータシステム（１０４）であって、
通信ネットワーク（１１０）を経由して通信を行う通信装置（６１２）と、
前記通信装置（６１２）に通信接続されたプロセッサ（６０２）と、
コンピュータ実行可能命令を格納したメモリ（６０４）であって、前記コンピュータ実行可能命令が前記プロセッサ（６０２）によって実行されるときに、前記ウェブサービスコンピュータシステム（１０４）に、前記保護されたウェブサービスリソース（１０６）へのアクセスを制御する方法を実行させ、前記方法は、
（ｉ）前記通信ネットワーク（１１０）を通じてクライアントコンピュータシステム（１０２）から前記保護されたウェブサービスリソース（１０６）にアクセスする第１のリクエストを受信するステップと、
（ｉｉ）第１の要因に従って前記クライアントコンピュータシステム（１０２）が認証されたと判定するステップと、
（ｉｉｉ）前記第１の要因に従った認証に基づいて、前記第１のリクエストに、前記保護されたウェブサービスリソース（１０６）にアクセスするのを許可するステップと、
（ｉｖ）前記通信ネットワーク（１１０）を通じて前記クライアントコンピュータシステム（１０２）から前記保護されたウェブサービスリソース（１０６）にアクセスする第２のリクエストを受信するステップと、
（ｖ）前記第２のリクエストを許可するには不十分となる前記第１の要因に従った前記認証に基づいて、前記クライアントコンピュータシステムを第２の要因に従って認証する必要があると判定するステップと、
（ｖｉ）前記第２の要因に従って前記クライアントコンピュータシステム（１０２）が認証されたと判定するステップと、
（ｖｉｉ）前記第２の要因に従った認証に基づいて、前記保護されたウェブサービスリソース（１０６）にアクセスする前記第２のリクエストを許可するステップと

を備える、メモリ（６０４）と
を備えることを特徴とするウェブサービスコンピュータシステム（１０４）。
【請求項２】
前記第１の要因は、パスワード、セキュリティクエスチョンの回答、生体識別子、オブジェクト、およびクライアント特定情報を備えたグループから選択されることを特徴とする請求項１に記載のウェブサービスコンピュータシステム。
【請求項３】
前記第２の要因は、前記第１の要因とは異なることを特徴とする請求項１に記載のウェブサービスコンピュータシステム。
【請求項４】
前記方法は、
前記クライアントコンピュータシステムが前記第１の要因に従って認証サービスコンピュータシステムによって認証された後に、前記クライアントコンピュータシステムから第１の認証トークンを受信するステップ、および
前記第１の認証トークンを用いて、前記クライアントコンピュータシステムが前記第１の要因に従って認証されたと判定するステップ
をさらに備えることを特徴とする請求項１に記載のウェブサービスコンピュータシステム。
【請求項５】
前記クライアントコンピュータシステムが認証されたと判定するステップは、
前記認証サービスコンピュータシステムの公開キーを用いて前記第１の認証トークンを復号するステップと、
前記第１の認証トークンの前記認証サービスコンピュータシステムによって行われた申告がアクセスの条件を満たすと判定するステップと
を備えることを特徴とする請求項４に記載のウェブサービスコンピュータシステム。
【請求項６】
前記クライアントコンピュータシステムを第２の要因に従って認証する必要があると判定するステップは、前記クライアントコンピュータシステムを前記第２の要因に従って認証される認証サービスコンピュータシステムに導くメッセージを前記クライアントコンピュータシステムに送信するステップを備えることを特徴とする請求項１に記載のウェブサービスコンピュータシステム。
【請求項７】
前記クライアントコンピュータシステムが第２の要因に従って認証されたと判定するステップは、前記第２の要因に従って前記認証サービスコンピュータシステムによって認証された後に、前記クライアントコンピュータシステムから認証トークンを受信するステップを備えることを特徴とする請求項６に記載のウェブサービスコンピュータシステム。
【請求項８】
前記第２のリクエストに、前記保護されたウェブサービスリソースにアクセスするのを許可するステップは、認証トークンの評価に基づくことを特徴とする請求項６に記載のウェブサービスコンピュータシステム。
【請求項９】
ウェブサービスコンピュータシステム（１０４）がクライアントコンピュータシステム（１０２）に保護されたウェブサービスリソース（１０６）へのアクセスを認証する方法であって、
（ｉ）認証される前記クライアントコンピュータシステム（１０２）から前記保護されたウェブサービスリソース（１０６）にアクセスするリクエスト（５１６）を受信するステップと、
（ｉｉ）身元の確認のためのチャレンジメッセージ（５１８）を前記クライアントコンピュータシステム（１０２）に送信するステップと、
（ｉｉｉ）前記クライアントコンピュータシステム（１０２）から前記チャレンジメッ

セージ（５１８）に対する確認応答（５２０）を受信するステップと、
（ｉｖ）前記確認応答が、所定の基準に合うと判定するステップと、
（ｖ）前記リクエストを許可するには、前記チャレンジメッセージ（５１８）、前記確認応答（５２０）、および前記所定の基準を用いた（ｉｉ）から（ｉｖ）までの認証が十分ではなく、認証される前記リクエストが、追加的な認証を要求すると判定するステップと、
（ｖｉ）第２のチャレンジメッセージ（５２２）、第２の確認応答（５２４）、および第２の所定の基準を用いて（ｉｉ）から（ｉｖ）までを繰り返して前記追加的な認証を行うステップと、
（ｖｉｉ）認証メッセージ（５３０）を前記クライアントコンピュータシステム（１０２）に送信するステップと
を備えることを特徴とする方法。
【請求項１０】
認証される前記リクエストが追加的な認証を要求すると判定するステップは、前記リクエストからのデータを読み出すステップ、および前記リクエストからの前記データを、前記チャレンジメッセージと関連付けられた認証レベルと比較するステップを備えることを特徴とする請求項９に記載の方法。
【請求項１１】
前記認証メッセージを前記クライアントコンピュータシステムに送信するステップは、認証トークンを前記クライアントコンピュータシステムに送信するステップを備えることを特徴とする請求項９に記載の方法。
【請求項１２】
前記認証トークンは、前記クライアントコンピュータシステムを認証するのに用いられた要因に関連する認証サービスコンピュータシステムからの申告を含むことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記認証メッセージを前記クライアントコンピュータシステムに送信する前に、第３のチャレンジメッセージ、第３の確認応答、および第３の所定の基準を用いて（ｉｉ）から（ｉｖ）までを繰り返すステップをさらに備えることを特徴とする請求項９に記載の方法。
【請求項１４】
ウェブサービスコンピュータ（１０４）に保護されたウェブサービスリソース（１０６）へのアクセスを制御する方法を実行させるためのコンピュータ実行可能命令を記録したコンピュータ読み取り可能な記憶媒体（６０８）であって、前記方法は、
クライアントコンピュータシステム（１０２）から、前記保護されたウェブサービスリソース（１０６）を特定するリクエスト（５１２）を受信するステップと、
認証サービスコンピュータシステム（１０８）に認証を要求する応答（５１４）を前記クライアントコンピュータシステム（１０２）に送信するステップと、
前記認証サービスコンピュータシステム（１０８）から認証された後に、前記クライアントコンピュータシステム（１０２）から認証（５３２）を受信するステップと、
前記認証が、前記リクエストを許可するのに十分であるかどうかを判定するステップと、
前記認証が十分である場合、前記リクエストを許可するステップと、
前記認証が前記リクエストを許可するのに十分ではない場合、前記リクエストを拒否するステップと
を備えることを特徴とするコンピュータ読み取り可能な記憶媒体。
【請求項１５】
前記認証は、認証トークンであることを特徴とする請求項１４に記載のコンピュータ読み取り可能な記憶媒体。
【請求項１６】

前記認証トークンは、公開キー暗号化を用いて暗号化されることを特徴とする請求項１５に記載のコンピュータ読み取り可能な記憶媒体。

【請求項１７】

前記方法は、前記認証が十分である場合、前記リクエストを許可した後に前記ウェブサービスコンピュータシステムの前記保護されたウェブサービスリソースへのアクセスを許可するステップをさらに備えることを特徴とする請求項１４に記載のコンピュータ読み取り可能な記憶媒体。

【請求項１８】

前記リクエストを拒否するステップは、前記拒否を、メッセージを用いて前記クライアントコンピュータシステムに送るステップを備え、前記メッセージは、前記クライアントコンピュータシステムを認証するように構成された前記認証サービスコンピュータシステムについての情報を含むことを特徴とする請求項１４に記載のコンピュータ読み取り可能な記憶媒体。

【請求項１９】

前記方法は、

前記ウェブサービスコンピュータシステムの前記保護されたウェブサービスリソースを特定する第２のリクエストを前記クライアントコンピュータシステムから受信するステップであって、前記第２のリクエストが前記認証を含む、ステップと、

前記認証が前記第２のリクエストを許可するのに十分であるかどうかを判定するステップと、

前記認証が前記第２のリクエストを許可するのに十分である場合、前記第２のリクエストを許可するステップと、

前記認証が前記第２のリクエストを許可するのに十分ではない場合、前記第２のリクエストを拒否するステップと

をさらに備えることを特徴とする請求項１４に記載のコンピュータ読み取り可能な記憶媒体。

【請求項２０】

前記リクエストを拒否するステップは、Ｓｉｍｐｌｅ　Ｏｂｊｅｃｔ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌに従ってフォルトメッセージを送信するステップを備え、認証を受信するステップは、Ｗｅｂ　Ｓｅｒｖｉｃｅｓ　Ｔｒｕｓｔ仕様書に従ってＷｅｂ　Ｓｅｒｖｉｃｅｓ　Ｔｒｕｓｔ　Ｒｅｑｕｅｓｔ　Ｓｅｃｕｒｉｔｙ　Ｔｏｋｅｎ　Ｒｅｓｐｏｎｓｅ　Ｍｅｓｓａｇｅを受信するステップを備えることを特徴とする請求項１４に記載のコンピュータ読み取り可能な記憶媒体。