(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5889988号
(P5889988)

(45)発行日　平成28年3月22日(2016.3.22)　(24)登録日　平成28年2月26日(2016.2.26)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
G09C 1/00	(2006.01)	G09C	1/00	640D
H04W 12/02	(2009.01)	H04W	12/02	
H04W 12/06	(2009.01)	H04W	12/06	
G06F 21/33	(2013.01)	G06F	21/33	350

請求項の数 7　外国語出願　(全 25 頁)

(21)出願番号　特願2014-206285(P2014-206285)
(22)出願日　平成26年10月7日(2014.10.7)
(62)分割の表示　特願2012-510942(P2012-510942)の分割
原出願日　平成22年5月11日(2010.5.11)
(65)公開番号　特開2015-26391(P2015-26391A)
(43)公開日　平成27年2月5日(2015.2.5)
審査請求日　平成26年10月7日(2014.10.7)
(31)優先権主張番号　12/465,725
(32)優先日　平成21年5月14日(2009.5.14)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　98052-6399　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】ＨＴＴＰベースの認証

(57)【特許請求の範囲】
【請求項１】
要求者が使用するクライアントコンピュータと、サーバコンピュータとの間で交換されるメッセージを処理するコンピュータベースのシステムであって、前記システムは、動作を実行するように構成され、前記動作は、
前記クライアントコンピュータが、認証仕様を含む１または複数のＨＴＴＰヘッダを含むサーバメッセージに応答して、前記認証仕様に適合する要求メッセージを生成するステップと、
前記クライアントコンピュータが、前記要求メッセージ内に、前記認証仕様内のセキュリティトークン仕様に適合するセキュリティトークンを挿入するステップと、
前記クライアントコンピュータが、前記要求メッセージ内に、前記セキュリティトークンの配置を特定するＨＴＴＰトークン配置ヘッダを挿入するステップと、
前記クライアントコンピュータが、前記要求メッセージ内に、少なくとも１つのＨＴＴＰヘッダの暗号化表現を含む要約を含むＨＴＴＰ要約ヘッダを挿入するステップと、
前記クライアントコンピュータが、前記要求メッセージ内に、前記要求メッセージの少なくとも一部のデジタル署名を含むセキュリティヘッダを挿入するステップと
を含むことを特徴とするコンピュータベースのシステム。
【請求項２】
請求項１に記載のコンピュータベースのシステムであって、前記動作は、前記クライアントコンピュータが、前記セキュリティトークンのサイズに基づいて前記セキュリティト

ークンの配置を判定するステップをさらに含み、前記配置を判定するステップは、前記セキュリティトークンが１もしくは複数のＨＴＴＰヘッダ内にあるかまたはメッセージ本文内にあるかの判定を含むことを特徴とするコンピュータベースのシステム。

【請求項３】

請求項１に記載のコンピュータベースのシステムであって、前記要求メッセージはＨＴＴＰ　ＰＯＳＴメッセージであり、前記動作は、前記クライアントコンピュータが、前記セキュリティトークンをメッセージ本文内のＨＴＭＬフォームフィールド内に挿入するステップをさらに含むことを特徴とするコンピュータベースのシステム。

【請求項４】

請求項１に記載のコンピュータベースのシステムであって、前記動作は、前記クライアントコンピュータが、前記セキュリティトークンの配置を前記セキュリティトークンのサイズに基づいて判定するステップをさらに含み、前記配置を判定するステップは、前記セキュリティトークンが、正確に１つのＨＴＴＰヘッダの中にあるか、複数のＨＴＴＰヘッダの中にあるか、またはメッセージ本文内にあるかの判定を含むことを特徴とするコンピュータベースのシステム。

【請求項５】

請求項１に記載のコンピュータベースのシステムであって、前記要求メッセージは、前記サーバコンピュータによって受信され、前記セキュリティトークンは、前記サーバコンピュータによって、メッセージ本文から、前記ＨＴＴＰトークン配置ヘッダに基づいて選択的に抽出され、前記セキュリティトークンは、前記サーバコンピュータによって、正確に１つのＨＴＴＰヘッダから、前記ＨＴＴＰトークン配置ヘッダに基づいて選択的に抽出され、および前記セキュリティトークンの複数の断片は、前記サーバコンピュータによって、複数のＨＴＴＰヘッダから、前記ＨＴＴＰトークン配置ヘッダに基づいて選択的に抽出されることを特徴とするコンピュータベースのシステム。

【請求項６】

請求項１に記載のコンピュータベースのシステムであって、前記要求メッセージを生成するステップは、前記１または複数のＨＴＴＰヘッダを、ＨＴＴＰヘッダ名を使用することによって生成することを含み、前記ＨＴＴＰヘッダ名は、前記メッセージを認証することを、前記セキュリティトークンを抽出してかつ検証することによって、前記サーバコンピュータのＨＴＴＰスタックができるようにし、および前記サーバコンピュータの前記ＨＴＴＰスタックが前記セキュリティトークンを抽出してかつ検証するように構成されていない場合に、前記ＨＴＴＰヘッダ名は、前記メッセージを認証することを、前記セキュリティトークンを抽出してかつ検証することによって、前記サーバコンピュータのアプリケーションができるようにすることを特徴とするコンピュータベースのシステム。

【請求項７】

請求項１に記載のコンピュータベースのシステムであって、前記動作は、前記クライアントコンピュータが、前記セキュリティトークンをメッセージ本文内に挿入するステップをさらに含み、前記ＨＴＴＰトークン配置ヘッダは、前記メッセージ本文全体が前記セキュリティトークンを含むことを特定することを特徴とするコンピュータベースのシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般にネットワーク技術に関し、さらに具体的には、ネットワーク環境内の要求の認証のためのＨＴＴＰの使用に関する。

【背景技術】

【０００２】

コンピュータネットワークは、様々なセキュリティ欠陥にさらされている。このような欠陥のタイプの１つは、アクセスが許可されていないリソースにアクセスするためか、または要求に正しく関連付けられることを避けるために、ユーザまたはコンピュータシステ

ムが自身を偽って特定する際に発生する。要求認証を容易にするために、リソースまたはサービスを提供する団体（以下本明細書において「証明書利用者（relying party）」と称する）へのサービスに関する要求は、証明書利用者が身元の真偽を検証可能な態様における要求者の身元を含んでいる。要求認証は、要求の送信者の身元を検証する処理である。認証は、団体のＩＤ（identification）の各々が正確であるという、あるレベルのセキュリティをもたらす。要求者の身元は、証明書利用者によって行なわれるアクセス制御判定の基礎を形成する。

【０００３】

要求認証のタイプの１つは、ユーザ名およびパスワードの使用を含む。さらに強力なタイプの認証は、セキュリティトークンの使用を含む。あるタイプのセキュリティトークンは、信頼済みＩＤプロバイダ（identity provider）によって発行される。セキュリティトークンの所持は、所有団体に関する身元の証明を提供するのに役立つ。あるセキュリティトークンは、さらに強力なセキュリティのために埋め込まれた暗号化キーを有している。

【０００４】

やりとり（interaction）の１つのタイプにおいて、要求者は、ＩＤプロバイダからセキュリティトークンを取得する。要求者は、その後、サービス要求を伴ったセキュリティトークンを、リソースまたはサービスを提供する団体に提示する。リソースプロバイダは、ＩＤプロバイダとの信頼関係を有し、この信頼関係は、セキュリティトークンの信頼性を保証する役割を果たす。

【０００５】

ＲＥＳＴ（representation state transfer）は、ワールドワイドウェブ等の分散システムのソフトウェアアーキテクチャの様式である。ＲＥＳＴは、通常は、ドメイン特有のデータを、ＳＯＡＰ等の追加のメッセージ層無しにＨＴＴＰを介して伝送するインタフェースをいう。ＨＴＴＰは、“ＲＥＳＴに適合した（RESTful）”アーキテクチャに従った、ＧＥＴ、ＰＯＳＴ、ＵＰＤＡＴＥおよびＤＥＬＥＴＥ等のメソッドを含むインタフェースを提供する。ＲＥＳＴアーキテクチャの１つの態様は、ステートレスサーバ（stateless server）のサポートであり、当該態様において、各メッセージは、当該メッセージを理解するために必要な情報を含み、メッセージ間の通信状態を記憶する必要性からサーバを解放する。このことは、サーバファーム内等のサーバのスケーリング（scaling）を容易にする。

【０００６】

ＲＦＣ２６１７（http://www.ietf.org/rfc/rfc2617.txtにて取得可能）は、ＢＡＳＩＣ認証スキームを記載しており、当該スキームにおいて、ユーザ名およびパスワードを、ＨＴＴＰヘッダ領域内に送ることができる。このＲＦＣは、このスキームを「ユーザ名およびパスワードを非暗号化形式でネットワークを介して送るので、ユーザ認証の安全な方法としては考えられない」として記載している。ＲＦＣは「デジタルアクセス認証」スキームも記載しており、当該スキームにおいて、ユーザ名、パスワード、ノンス値（nonce value）、ＨＴＴＰメソッド、および要求されたＵＲＩのハッシュを使用する。ＲＦＣは、ダイジェストスキーム（digest scheme）が“．．．多くの既知の制限をうける”と記載している。

【発明の概要】

【０００７】

本概要を、発明を実施するための形態において以下にさらに詳細に説明される概念の選択を単純化された形式にて紹介するために提供する。本概要は、本発明の重要な特徴または本質的な特徴を特定することを意図しておらず、本発明の範囲を限定するために使用することも意図していない。

【０００８】

つまり、システム、メソッドおよびコンポーネントは、アプリケーションにＨＴＴＰ要求を認証することを可能にするＨＴＴＰメッセージ認証フレームワークを提供するために

機能する。このフレームワークは、様々な要求認証スキームを実装するための機構を有するアプリケーションを提供し、ＨＴＴＰスタックの実装を活用する。例示の実施形態は、ＨＴＴＰヘッダおよび関連するセマンティクスのセットを有するプロトコルを含む。ＨＴＴＰメッセージを生成して処理する方法を、要求者と証明書利用者との間の様々なやりとりとともに説明する。

【０００９】

例示の実施形態において、要求者は、サーバから、認証仕様を有する１または複数のＨＴＴＰヘッダを含むサーバメッセージを受信する。それに応じて、要求者は、認証仕様に適合する要求メッセージを生成することができる。一実施形態において、要求メッセージは、メッセージ本文、セキュリティトークン（ＳＴ）、セキュリティトークンの配置を特定するＨＴＴＰヘッダを含む。要求メッセージは、メッセージの要約を含むＨＴＴＰヘッダを含むことができる。セキュリティトークンを、１または複数のＨＴＴＰヘッダ内またはメッセージ本文内に配置することできる。セキュリティトークンを複数のＨＴＴＰヘッダ内に配置する場合、セキュリティトークンをヘッダに亘って断片化することができる。セキュリティトークンをメッセージ本文内に配置する場合、セキュリティトークンは、本文全体であるか、ＨＴＭＬフォームフィールドであるか、またはＸＭＬ要素内に在ることができる。一実施形態において、要約は、メッセージ本文および少なくとも１つのＨＴＴＰヘッダまたはそれらの一部の暗号化表現を含む。

【００１０】

一実施形態において、要求者は、セキュリティトークンのサイズに基づいてセキュリティトークンの配置を判定する。１つのＨＴＴＰヘッダ内に収めるには長すぎる場合、セキュリティトークンを、複数のヘッダに亘って断片化することができる。複数のＨＴＴＰヘッダ内に収めるのに長すぎる場合、セキュリティトークンをメッセージ本文内に配置することができる。

【００１１】

一実施形態において、要求メッセージを受信するサーバは、セキュリティトークンを、トークン配置ヘッダ仕様に基づいて抽出することができる。セキュリティトークンは、１つのＨＴＴＰヘッダ内にあるか、複数のＨＴＴＰヘッダに亘って断片化されているか、またはメッセージ本文内に在ることができる。

【００１２】

一実施形態において、サーバは、要求者に署名仕様を送信し、および要求者は、セキュリティヘッダ内の署名仕様に適合するデジタル署名を含む。

一実施形態において、サーバは、コンテキストトークン（context token）を含むメッセージを用いて要求者に応答する。それに続く要求において、要求者は、セキュリティトークンを含む代わりにＨＴＴＰヘッダ内にコンテキストトークンを含むことができる。

【００１３】

上述および関連する目的の達成のために、システムのある例示の態様を、以下の説明および添付の図面とともに本明細書において説明する。しかし、これらの態様は、本発明の原理を使用することができる様々な方法のいくつかを示すものであり、本発明は、これら全ての態様およびそれらと均等なものを含むことを意図している。本発明の他の利点および新規な特徴は、図面と共に考慮される本発明の以下の詳細な説明から明らかになるだろう。

【００１４】

本発明の非限定的および非包括的な実施形態を、添付の図面を参照して説明する。図面において、同様の番号は、別途に特定されない限り、様々な図面を通じて同様の部分を参照する。

【００１５】

本発明の理解を助けるために、添付の図面とともに読まれるべき以下の発明を実施するための形態を参照する。

【図面の簡単な説明】

【００１６】
【図１】図１は、実施形態を実施することができる例示の環境のブロック図である。
【図２】図２は、証明書利用者を実装するために使用可能なコンピュータシステムの例示の実施形態を示すブロック図である。
【図３】図３は、実施形態を実施することができる例示の環境を示す図である。
【図４】図４は、要求者を認証するためにＨＴＴＰヘッダを使用する処理の例示の実施形態を示すフロー図である。
【図５】図５は、図４の動作のいくつかをさらに詳細に示すフロー図である。
【図６】図６は、例示の実施形態に従って、ＨＴＴＰメッセージ内にセキュリティトークンを挿入する処理を示すフロー図である。
【図７】図７は、例示の実施形態に従って、ＨＴＴＰメッセージからセキュリティトークンを抽出する処理を示すフロー図である。
【図８】図８は、例示の実施形態におけるＨＴＴＰメッセージを生成する処理を示すフロー図である。
【発明を実施するための形態】
【００１７】
本発明の例示の実施形態を、本明細書の一部を形成しかつ本発明を実施することができる特定の例示の実施形態を例示の目的で示す添付の図面を参照して、本明細書で以下にさらに十分に説明する。しかし、本発明を、多くの異なった形態にて実施することができ、本明細書にて説明されている実施形態に限定されるとして解釈するべきではない。むしろ、これらの実施形態を、本開示が完全かつ完璧となるように、ならびに本発明の範囲を当業者に十分に伝達するように提供する。様々ある中で、本発明を、方法またはデバイスとして実施することができる。従って、本発明を、完全なハードウェア実施形態、完全なソフトウェア実施形態またはソフトウェアおよびハードウェアの態様を組み合わせた実施形態の形式で実施することができる。従って、以下の詳細な説明を、限定するものとして理解すべきではない。
【００１８】
明細書および特許請求の範囲の請求項を通して、以下の用語は、文脈が明らかに他のことを記述していない限り、本明細書において明示的に関連付けられている意味を持つ。本明細書において用いられている「一実施形態において」という表現は、必ずしもそれまでの実施形態をいうわけではない。さらに、本明細書において用いられている「他の実施形態において」という表現は、必ずしも異なった実施形態をいうわけではない。従って、本発明の様々な実施形態を、本発明の範囲または趣旨から逸脱することなく容易に組み合わせることができる。同様に、本明細書において用いられている「１つの実装例において」という表現は、必ずしも同一の実装例を言うわけではないので、様々な実装例の技術を組み合わせることができる。
【００１９】
さらに、本明細書で用いられている用語「または」は、文脈が明らかに他のことを記述していない限り、包含的な「または」演算子であり、用語「および／または」と同等である。用語「に基づいて」は、排他的ではなく、文脈が明らかに他のことを記述していない限り、追加の要素に基づいていることを許容する。さらに、本明細書を通して、不定冠詞および定冠詞は複数のものを指すことができる。「内に」という語は、「内に」および「上に」の意味を含む。
【００２０】
本明細書で使用されている用語「認証する」は、許容可能な確度まで、事実または要求が真であることを確認することをいう。ユーザまたはユーザの身元を認証することを、ユーザの表明されている身元が、十分かつ正確であることを確認するために用いる。ユーザからの要求の認証は、要求に含まれる身元情報が正確であること、要求が特定されたユーザからのものであるかもしくは特定されたユーザによって許可されていること、要求が不適切に変更されていないこと、または要求内の他の情報が正確であることの確認を含むこ

とができる。認証は付随する確度を有しており、まだ不正確であるだろう場合でも、情報が認証されている状態を許容する。

【００２１】

本明細書で説明されているコンポーネントを、様々なデータ構造を有する様々なコンピュータ可読媒体から実行することができる。これらの構成要素は、１または複数のデータパケット（例えば、信号によって、ローカルシステム内もしくは分散システム内の他のコンポーネントとやりとりするか、またはインターネット等のネットワークを介して他のシステムとやりとりをする１つのコンポーネントからのデータ）を有する信号に従うようなローカルまたはリモート処理を介して通信することができる。ソフトウェアコンポーネントを、本発明の実施形態によって、例えば、限定するわけではないが、特定用途向け集積回路（ＡＳＩＣ）、ＣＤ（compact disk）、ＤＶＤ（digital versatile disk）ＲＡＭ（random access memory）、ＲＯＭ（read only memory）、フロッピー（登録商標）ディスク、ハードディスク、ＥＥＰＲＯＭ（electrically erasable programmable read only memory）、フラッシュメモリ、またはメモリスティックを含むコンピュータ可読記憶媒体に保存することができる。

【００２２】

本明細書において用いられるコンピュータ可読媒体という用語は、記憶媒体および通信媒体を含む。通信媒体は、通常は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータを搬送波または他の搬送メカニズム等の変調データ信号において表し、かつ任意の情報伝送媒体を含む。例示であり、限定するものではないが、通信媒体は、有線ネットワークおよび直接有線接続等の有線媒体、並びに音波、ラジオ、赤外線および他の無線媒体を含む。

【００２３】

図１は、実施形態を実施することができる環境１００のブロック図である。図１は、例示の環境の基本的な理解を提供するが、多くの構成を使用することができ、および多くの詳細は図１内に記載されていない。図１に示されているように、例示の環境１００は要求者１０２を含む。要求者１０２は、リモートサービスプロバイダからのリソースまたはサービスを要求するクライアントコンピュータデバイス、処理、または任意のコンポーネントとすることができる。例示の実施形態において、要求者１０２は、ＨＴＴＰスタック１０４を含む。ＨＴＴＰスタックは、ＨＴＴＰ規格および本明細書に記載されているメカニズムの少なくとも少なくともいくつかに従って、ＨＴＴＰ（hypertext protocol）メッセージを受信するか、処理するか、生成するかまたは送信することができる。

【００２４】

例示の環境１００は、証明書利用者１０６を含む。証明書利用者１０６は、コンピュータデバイス、サーバ、または複数のサーバを含むサーバファームとすることができる。図２は、証明書利用者１０６の実装例を示している。

【００２５】

図示された例示の実施形態において、証明書利用者はＨＴＴＰスタック１０８を含む。ＨＴＴＰスタック１０８は、ＨＴＴＰスタック１０４に説明されたような動作を実行するが、ＨＴＴＰスタック１０８およびＨＴＴＰスタック１０４の実装は異なってもよく、各々によって提供される機能が異なってもよい。

【００２６】

一実施形態において、要求者１０２は、証明書利用者１０６に１または複数の要求を送信する。要求は、いくつかのタイプの識別情報を含むことができる。要求は、リソースまたはサービスに対する要求とすることができる。本明細書で用いられているように、サービスに対する要求は、リソースに対する要求であるとみなされる。証明書利用者１０６は、要求を処理して、および要求が、当該要求または要求者１０２のユーザを十分に認証するための情報を含んでいるかを判定する。この情報は、特有の形式であってもよく、セキュリティ認証情報と称される。セキュリティ認証情報が含まれていないかまたは不十分である場合、証明書利用者１０６は、要求を拒否し、および十分なセキュリティ認証情報を

提供するように要求者１０２に命令することができる。この処理を、本明細書でさらに詳細に説明する。

【００２７】

例示の環境１００は、ＩＤプロバイダ１１０を含む。ＩＤプロバイダは、要求者１０２にセキュリティ認証情報を発行するネットワークエンティティとすることができる。セキュリティ認証情報は、証明書利用者１０６によって信頼可能な要求者１０２に関する要求を表すことができる。従って、ＩＤプロバイダ１１０は、証明書利用者１０６によって、信頼済みの団体とみなされる。一実施形態において、セキュリティ認証情報は、セキュリティトークン（ＳＴ）を含み、およびＩＤプロバイダ１１０は、セキュリティトークンを提供するセキュリティトークンサービス（ＳＴＳ）を含む。

【００２８】

１つのタイプのセキュリティトークンは、エンティティに関する１または複数の要求の一群を表すデータを含む。この要求を、要求者に関連する情報が正確であるアサーションとしてみなすことができる。これは、例えば、名前、識別子、キー、グループメンバシップ、特権、能力等を含むことができる。このタイプのセキュリティトークンは、本明細書において「ダイレクトセキュリティトークン」と称される。

【００２９】

第２のタイプのセキュリティトークンは、ダイレクトセキュリティトークンへの参照を含み、この参照はダイレクトセキュリティトークンへのアクセスを特定するかまたは可能にする。ダイレクトセキュリティトークンへのこのタイプの参照は、本明細書において非ダイレクトセキュリティトークンと称される。ＵＲＩ（uniform resource identifier）は、それがダイレクトセキュリティトークンを参照する場合、非ダイレクトセキュリティトークンの例である。本明細書で用いられているように、用語「セキュリティトークン」は、文脈が１つの特定のタイプを明確に指していない限り、ダイレクトセキュリティトークンまたは非ダイレクトセキュリティトークンをいう。

【００３０】

要求者１０２は、ネットワーク１２０を介して、証明書利用者１０６またはＩＤプロバイダ１１０と通信することができる。ネットワーク１２０は、ローカルエリアネットワーク、ワイドエリアネットワーク、またはこれらの組み合わせを含む。一実施形態にておいて、ネットワーク１２０は、ネットワークのネットワークであるインターネットを含む。ネットワーク１２０は、有線通信メカニズム、無線通信メカニズム、またはこれらの組み合わせを含む、要求者１０２、証明書利用者１０６、またはＩＤプロバイダ１１０間の通信、これらの互いのまたは他のコンピューティングデバイスとの通信は、ＩＰ、ＴＣＰ／ＩＰ、ＵＤＰ、ＨＴＴＰ、ＳＳＬ、ＴＬＳ、ＦＴＰ、ＳＭＴＰ、ＷＡＰ、ＢｌｕｅＴｏｏｔｈ（登録商標）、またはＷＬＡＮ等の１または複数の様々な有線または無線通信プロトコルを使用することができる。

【００３１】

図１は、適切な環境の単なる一実施例であり、および本発明の用途または機能の範囲に関する限定を提案するものではない。従って、様々なシステム構成を、本発明の範囲または趣旨から逸脱することなく用いることができる。例えば、証明書利用者１０６またはＩＤプロバイダ１１０の任意の機能を、様々な方法で複数のコンピュータデバイスの間に分散されているかまたは複製されている１または複数のコンピュータデバイス内で組み合わせることができる。同様に、要求者１０２の機能は、１または複数のコンピュータデバイス間で様々な方法で構成することができる。一実施形態において、証明書利用者１０６およびＩＤプロバイダ１１０の機能を、１または複数のコンピュータデバイス内に組み込むことができる。

【００３２】

一実施形態において、要求者１０２、証明書利用者１０６、およびＩＤプロバイダ１１０の各々を、１または複数のコンピュータデバイスによって実装する。コンピュータデバイスは、専用または汎用コンピュータデバイスとすることができる。簡単にいえば、使用

可能なコンピュータデバイスの一実施形態は、１または複数の処理ユニット、メモリ、ディスプレイ、キーボードおよびポインティングデバイス、並びに通信インタフェースを含む。１または複数の処理ユニットは、１または複数のマルチコアプロセッサを含むことができる。例示のコンピュータデバイスは、メインフレーム、サーバ、ブレードサーバ、パーソナルコンピュータ、ポータブルコンピュータ、通信デバイス、家電等を含む。コンピュータデバイスは、汎用または専用オペレーティングシステムを含むことができる。ワシントン州レドモンドのマイクロソフト社によるオペレーションシステムのＷｉｎｄｏｗｓ（登録商標）ファミリーは、開発システムのコンピュータデバイスにおいて実行することができるオペレーティングシステムの例である。

【００３３】

図２は、証明書利用者１０６を実装するために使用可能なコンピュータシステム２００の例示の実施形態またはこれらの一部を示すブロック図である。様々な実施形態において、システム２００を、様々な方法で構成されている１または複数のサーバまたは他のコンピュータデバイスを用いて実装することができる。

【００３４】

図示されているように、コンピュータシステム２００は、様々なコンピュータプログラムの命令を実行するために動作を実行する１または複数のプロセッサ２０２を含む。１つの構成において、プロセッサ２０２は、１または複数の中央演算ユニット、１または複数のプロセッサコア、ＡＳＩＣ、または他のハードウェア処理コンポーネント並びに関連するプログラムロジックを含むことができる。例示の実施形態において、コンピュータシステム２００は、揮発性または不揮発性メモリを含むことができるメモリ２０４を含むことができる。コンピュータシステム２００は、ネットワークを介してメッセージもしくは信号を離れたデバイスに送信するか、または当該デバイスから受信するように動作を実行するネットワーク通信ユニットを含むこともできる。

【００３５】

例示の実施形態において、コンピュータシステム２００は、メモリ内に保存されているＨＴＴＰスタック２０６および１または複数のアプリケーション２１０を含む。ＨＴＴＰスタック２０６は、ＨＴＴＰスタック１０８（図１）とすることができる。一実施形態において、ＨＴＴＰスタック２０６は、受信された要求を認証するように動作を実行する認証モジュール２０８を含む。ある実施形態において、ＨＴＴＰスタック２０６は、認証モジュール２０８を含まない。

【００３６】

一実施形態において、コンピュータシステム２００は、アプリケーション２１０を含む。アプリケーション２１０は、様々なサービスを実行するか、１または複数のリソースへのアクセスを提供するか、または要求に応じて他の動作を実行することができる。アプリケーション２１０の例は、ウェブサーバ、ＦＴＰサーバ、およびメールサーバを含む。アプリケーション２１０は、アプリケーション認証モジュール２１２を含むことができる。アプリケーション認証モジュール２１２は、受信された要求を認証するための動作を実行するが、認証モジュール２０８と同一の動作である必要はない。

【００３７】

図３は、実施形態を実施することができる例示の環境３００を示す。環境３００は、図１の環境１００またはこれらの変形例とともに存在することができる。図示されているように、環境３００は、要求者１０２、証明書利用者１０６、およびＩＤプロバイダ１１０を含む。要求者１０２は、証明書利用者１０６およびＩＤプロバイダ１１０の各々と直接的にまたは非直接的に通信する。この通信は、直接的、またはネットワーク１２０（図１）等のネットワークを介することができる。

【００３８】

図３内の矢印は、図示されたコンポーネント間で交換されるメッセージを表している。さらに、一実施形態において、メッセージの参照符号は、様々な実施形態において順序が異なるが、図面の頂部から底部方向の時系列に対応している。一実施形態において、図示

されているメッセージの各々は、ＨＴＴＰメッセージであり、ＨＴＴＰメッセージの内容を以下でさらに詳細に説明する。

【００３９】

図３のメッセージを、図４とともに説明する。図４は、要求者を認証するためのＨＴＴＰヘッダの使用の処理４００の例示の実施形態を示しているフロー図である。処理４００のいくつかの動作は、要求者１０２（図１）によって実行され、かつ図４の左側欄のヘッダ「要求者」の下に表されている。処理４００の他の動作は、証明書利用者１０６によって実行され、かつ図４の右側欄のヘッダ「証明書利用者」の下に表されている。処理４００のいくつかの動作は、図３に示されているメッセージの送信または受信に関連している。以下の説明は、図３のメッセージを参照する。

【００４０】

処理４００の図示されている部分を、ブロック４０２で開始することができ、ここで、要求者１０２は、要求メッセージを証明書利用者１０６に送信する（要求メッセージ３１０）。一実施形態において、要求メッセージ３１０は、アクセスを認証処理によって保護するリソースに対する要求である。この処理は、ブロック４０２から４０４に流れることができ、そこで、証明書利用者１０６は要求メッセージ３１０を受信する。処理４００は、ブロック４０４から判定ブロック４０６に流れることができ、そこで、要求が十分に認証されたかについて判定がなされる。一実施形態において、これは、要求が有効かつ十分なセキュリティ認証情報を含んでいるかの判定を含む。十分性の判定は、証明書利用者１０６の構成に基づくことができる。一実施形態において、ブロック４０６の判定は、要求がセキュリティトークンを含むこと、および設定されたスキームを守って実行しているかの判定を含む。この判定は、要求されたリソースの値、要求者の位置もしくは設定、時刻、または他の要素に基づくことができる。ブロック４０６の動作のさらなる詳細を、本明細書で説明する。

【００４１】

判定ブロック４０６において、要求が十分に認証されていると判定した場合、処理はブロック４０８に流れることができ、そこで、証明書利用者１０６が応答メッセージ３２０を要求者１０２に送信することができる。ある構成において、応答メッセージ３２０は、良好な応答（successful response）を示すことができる。応答は、リソース、リソースが利用可能であることの表示、サービスを提供しているかまたは提供することの表示、リソースの取得を容易にするデータ、または要求に従った他の応答を含むことができる。ある構成において、応答メッセージ３２０は、認証以外の理由で拒否された要求を示すことができる。例えば、要求を適切に認証したが、ユーザがリソースにアクセスすることを許可されていない場合がある。リソースは、他の理由で利用不可能とすることができる。処理は、ブロック４０８からプログラムの終了に流れるか、またはプログラムの呼び出しに戻ることができる。

【００４２】

判定ブロック４０６において、要求メッセージに含まれている十分なセキュリティ認証情報がないと判定した場合、処理４００は、ブロック４１０に流れることができ、そこでＨＴＴＰエラー応答メッセージを生成し、かつ証明書利用者１０６から要求者１０２に送信する。一実施形態において、ＨＴＴＰエラー応答メッセージは、ＨＴＴＰ「不許可」メッセージ３１２である。これは、「WWW-Authenticate」応答ヘッダを含む、ＨＴＴＰ４０１エラーメッセージとすることができる。このメッセージは、要求されたセキュリティ認証情報の仕様、または１もしくは複数のセキュリティ認証情報を送信する際に順守されるべきプロトコルを示すデータを含むことができる。このプロトコルは「スキーム」と称され、かつ１または複数のＨＴＴＰヘッダを使用するスキームの具体的な事例においては「ＨＴＴＰスキーム」と称される。

【００４３】

処理４００は、ブロック４１０からブロック４１２に流れることができ、そこで、要求者１０２は「不許可」メッセージ３１２を受信する。ある環境において、要求者１０２は

、十分なセキュリティ認証情報を保持するか、またはそれらを生成可能とすることができるが、例示した環境においては、「不許可」メッセージ３１２の受信に応答して、処理がブロック４１４に流れ、そこで、要求者１０２は、「不許可」メッセージ３１２にて証明書利用者１０６によって特定されたスキームに準ずる十分なセキュリティ認証情報を取得することを試行することができる。一実施形態では、ブロック４１４において、要求者１０２が、ＩＤプロバイダ１１０等の信頼済みＩＤプロバイダからのセキュリティトークンを要求することができる。この要求は、ＩＤプロバイダ１１０に送信される要求ＳＴメッセージ３１４の形式とすることができる。要求ＳＴメッセージ３１４は、要求者１０２のユーザを認証するために使用可能なセキュリティ認証情報または他のデータを含むことができる。

【００４４】

ある実施形態において、要求ＳＴメッセージ３１４に応答して、ＩＤプロバイダ１１０が、要求者１０２が十分な識別情報を提供していないこと、またはそうでなければセキュリティトークンを受信することを許可されていないことを判定する。この動作を、図４には記載しない。例示の処理４００は、ＩＤプロバイダ１１０が、要求されたセキュリティトークンを要求者１０２に返信する環境を示している。示されているように、処理４００は、ブロック４１６に流れ、そこで要求者１０２がセキュリティトークン３２５を含むＳＴ応答メッセージ３１６を受信する。ある実施形態において、セキュリティトークンは、１または複数の暗号化キーを含む。キーベアリング（key-bearing）セキュリティトークンの例は、セッションキーを用いたケロベロスｖ５チケット、およびホルダー－オブ－キー（holder-of-key）サブジェクト確認を用いたＳＡＭＬｖ１．１もしくはｖ２．０トークンを含む。

【００４５】

一実施形態において、要求ＳＴメッセージ３１４およびＳＴ応答メッセージ３１６は、本明細書において説明されているメッセージプロトコルの少なくともいくつかに従っている。例えば、要求者は、ＳＴ要求メッセージ３１４内に、本明細書において説明されているトークン配置ヘッダおよびトークンヘッダを挿入することができる。このメッセージは、さらに、要約ヘッダおよびデジタル署名を含むことができる。これらのメッセージの例を、本明細書において提供する。

【００４６】

ブロック４１６におけるセキュリティトークンの受信に応答して、処理はブロック４１８に流れることができ、そこで、要求者１０２は要求メッセージ３１８を生成し、かつ証明書利用者１０６に送信することができる。要求メッセージ３１８は、要求メッセージ３１０の要求と同様の要求を含むことができる。しかし、要求メッセージ３１８は、ＩＤプロバイダ１１０から受信されたセキュリティトークン３２５を含むことができる。一実施形態において、要求メッセージ３１８は、追加のＨＴＴＰヘッダを有しかつ認証データを提供する要求メッセージ３１０と同様である。処理は、ブロック４１８からブロック４０４に流れることができ、そこで、証明書利用者１０６は要求メッセージ３１８を受信する。

【００４７】

ブロック４０４において、要求メッセージ３１８の受信に応答して、証明書利用者１０６は、当該メッセージを処理して、当該要求が十分な識別認証情報を含みかつ要求メッセージ３１０に関して説明されたような設定された認証スキームに従っているかを判定することができる。識別認証情報が不十分であるとみなされる場合、処理４００は、ブロック４１０に流れることができ、そこで証明書利用者は他の不許可メッセージ３１２を送信することができる。判定ブロック４０６において、セキュリティ認証情報が十分であると判定された場合、処理はブロック４０８に流れることができ、上述のように、そこで応答を送信する。図３は、メッセージの例示のシーケンスを示しており、この場合第１の要求メッセージは不十分であり、第２の要求メッセージは十分である。このメッセージの例示のシーケンスは、以下のメッセージのシーケンスを示している。

要求メッセージ３１０。
不許可メッセージ３１２。
要求ＳＴメッセージ３１４。
ＳＴ応答メッセージ３１６。
（セキュリティトークンを伴う）要求メッセージ３１８。
応答メッセージ３２０。
【００４８】
一実施形態において、環境は以下のメッセージのシーケンスをもたらすことができる。
要求ＳＴメッセージ３１４。
ＳＴ応答メッセージ３１６。
（セキュリティトークンを伴う）要求メッセージ３１８。
応答メッセージ３２０。
【００４９】
上述の例示のシーケンスにおいて、要求者１０２は、ブロック４１４において、要求ＳＴメッセージ３１４を送信することができ；ブロック４１６において、要求者１０２は、セキュリティＳＴ応答メッセージ３１６を受信することができ；それに応じて、ブロック４１８において、要求者１０２は、要求メッセージ３１８を生成し、かつ送信することができる。証明書利用者１０６は、その後、ブロック４０８において応答メッセージ３２０を送信することができる。例えば、要求者１０２が、事前の要求に応答して事前に受信した不許可メッセージ３１２を有している環境か、またはそうでなければ、要求者１０２が、適切なセキュリティトークンを取得して要求メッセージ内の適切なスキームを用いてそれを送信する環境において、このシーケンスは生じる場合がある。さらに他のシーケンスにおける例示されたメッセージまたはそれら一部の送信を含む、処理４００のバリエーションが生じる場合がある。
【００５０】
図５は、図４の判定ブロック４０６の実装例を示すフロー図である。判定ブロックの動作のいくつかを、証明書利用者１０６（図１）のＨＴＴＰスタック２０６（図２）によって実行することができ、かつ図５の左側欄のヘッダ「ＨＴＴＰスタック」の下に表す。判定ブロック４０６の他の動作を、アプリケーション２１０の認証モジュール２１２によって実行することができ、かつ右側欄のヘッダ「アプリケーション」の下に表す。図５は、前後関係に関して、破線にて図４のブロック４０４、４１０および４０８を含んでいるが、これらは、示されている実施形態における判定ブロック４０６の動作には含まれない。図５に示されている判定ブロック４０６の動作は、本明細書において処理５００と称される。
【００５１】
図５に示されているように、処理は、ブロック４０４からブロック５０４に流れることができ、そこで、認証スキームの仕様を、ＨＴＴＰメッセージのＨＴＴＰヘッダから抽出することができる。要求メッセージ３１８は、このようなＨＴＴＰメッセージの一例である。一実施形態において、この仕様は、証明書利用者１０６において設定された任意のスキーム名とすることができる。
【００５２】
処理５００は、ブロック５０４から判定ブロック５０６に流れることができ、そこで、ＨＴＴＰスタック２０６を、特定された認証スキームに対応しているハンドラ（handler）を用いて設定しているかの判定を行なう。本明細書において説明されているフレームワークは、処理５００を、証明書利用者において、特定された認証スキームに対応するＨＴＴＰスタックハンドラを用いて、またはそのように構成されていないＨＴＴＰスタックを用いて実行することを可能にする。
【００５３】
判定ブロック５０６において、ＨＴＴＰスタック２０６が対応するハンドラを用いて設

定されていると判定した場合、処理はブロック５０８に流れることができ、そこで、セキュリティトークンを、受信されたメッセージから抽出することができる。本明細書で説明されているように、本明細書において説明されているフレームワークは、セキュリティトークンを、１または複数のＨＴＴＰヘッダ内、または要求メッセージ本文内に配置することを可能にする。ブロック５０６の動作は、セキュリティトークンの配置を判定するステップ、セキュリティトークンを抽出するステップ、および２以上ある場合にセキュリティトークンの断片を組み合わせるステップを含む。図７は、ブロック５０８の動作のいくつかをさらに詳細に示している。

【００５４】

この処理は、ブロック５０８からブロック５１０に流れることができ、ここでセキュリティトークンの検証を実行することができる。一実施形態において、ブロック５１０の動作は、セキュリティトークンを、セキュリティトークンを含んで受信された要求に適切に関連付けていることを検証するステップを含む。一実施形態において、メッセージは、要求メッセージの要約、またはその一部を含むことができる。当該メッセージは、メッセージ本文、セキュリティトークン、およびＨＴＴＰヘッダの選択された部分を含むことができる。要約は、メッセージの指定された部分のハッシュを含むことができる。ブロック５１０の動作は、要約がメッセージ本文およびＨＴＴＰヘッダの選択された部分を正確に表していることの検証を含むことができる。セキュリティトークンの検証は、要約の生成および当該要約がセキュリティトークンに含まれている要約と一致していることの検証を含むことができる。一実施形態において、ブロック５１０の動作は、少なくとも要約をカバーするデジタル署名の検証を含む。この署名は、セキュリティトークン内に埋め込まれている暗号化キーを使用することができる。このことは、セキュリティトークンとメッセージとの強い関連付けをもたらす。

【００５５】

セキュリティトークンの検証は、セキュリティトークンを、図１のＩＤプロバイダ１１０等の信頼済みＩＤプロバイダによって発行したことを検証することを含む。ブロック５１０の動作は、証明書利用者の構成に基づいて、セキュリティトークンによって表された要求が十分であることを検証すること、または設定されているセキュリティトークンデータの追加の検証を含むことができる。

【００５６】

処理は、判定ブロック５１２に流れることができ、そこで、セキュリティトークンおよび関連するデータを適切に検証したかを判定する。検証が失敗している場合、処理は処理４００のブロック４１０に流れることができ、かつ本明細書に記載されているように継続する。検証が成功している場合、処理はブロック５１４に流れることができ、そこで、要求メッセージまたはその一部をアプリケーション２１０に送る。アプリケーション２１０は、ブロック４０８を含む処理４００の様々な方法でメッセージを処理することができ、処理は本明細書において説明されているように継続することができる。

【００５７】

一実施形態において、ＨＴＴＰスタックを、特定された認証スキームに従ってセキュリティトークンを抽出し、かつ確認するように構成していなくともよい。判定ブロック５０６において、ＨＴＴＰスタックを、特定された認証スキームに対するハンドラを用いて構成していないと判定した場合、処理はブロック５２６に流れることができ、そこで、要求メッセージまたはその一部をアプリケーション２１０に送る。このことは、アプリケーション２１０に、受信されたメッセージの認証を実行するメカニズムを提供する。

【００５８】

処理は、ブロック５１６からブロック５１８に流れることができ、そこで、セキュリティトークンを、受信されたメッセージから抽出することができる。一実施形態において、アプリケーション２１０を、要求メッセージの認証に関連してＨＴＴＰスタック２０６の動作の少なくともいくつかを実行するように構成することができる。特に、ブロック５１８および５２０、並びに判定ブロック５２２は、本明細書に説明されているように、対応

するブロック５０８、５１０および５１２の動作をそれぞれ含むことができる。従って、処理は、対応するブロックに関して上述されているように、ブロック５１８からブロック５２０、ブロック５２２に流れ、その後、ブロック４１０またはブロック４０８に流れることができる。一実施形態において、判定ブロック５２２において失敗した認証は、本明細書に記載されているようにＨＴＴＰエラーの注入をもたらすことができる。

【００５９】

本明細書に記載されているメカニズムの少なくともいくつかは、証明書利用者１０６が、受信された要求メッセージに関連する様々な構成を有することを可能にする。１つの構成において、ＨＴＴＰスタック２０６の認証モジュール２０８を、受信された要求の認証を実行するように構成することができる。１つの構成において、認証モジュール２０８を、そのように構成しなくともよく、およびメッセージを、アプリケーション２１０に送り、そこでアプリケーションモジュール２１２は認証を実行する。１つの構成において、認証モジュール２０８は、認証動作の一部を実行することができ、および認証モジュール２１２は、他の部分を実行することができる。従って、アプリケーション２１０を、様々なコンピュータシステム２００にインストールし、かつ様々なＨＴＴＰスタック構成とともに動作することができる。

【００６０】

図６は、例示の実施形態において、セキュリティトークンをＨＴＴＰメッセージ内に挿入する処理６００を示すフロー図である。処理６００は、上述のように、ブロック４１８の動作の少なくともいくつかを示している。処理６００の示されている部分を、ブロック６０２において開始することができ、そこで、セキュリティトークンの１または複数の配置を判定することができる。一実装において、セキュリティトークンを、１または複数のＨＴＴＰヘッダ内にあるように構成することができ、またはメッセージ本文における３つの配置のうちの１つの配置とするように構成することができる。判定ブロック６０４において、処理は、配置オプションのそれぞれを取り扱うために４つのブロックのうちの１つに分岐することができる。このような配置の１つは、１または複数のＨＴＴＰヘッダ内にある配置である。これがセキュリティトークンの配置であると判定すると、処理は判定ブロック６０６に流れることができ、そこで、セキュリティトークンを断片化するかの判定を行なう。一実施形態において、この判定を、セキュリティトークンのサイズに基づいて行なう。判定ブロック６０６において、セキュリティトークンを１つのヘッダに挿入することができることを判定すると、この処理はブロック６０８に流れることができ、そこで、セキュリティトークンを１つのＨＴＴＰヘッダ内に挿入する。この処理は、ブロック６２０に流れることができる。一実施形態にて、ブロック６２０において、ＨＴＴＰトークン配置ヘッダを、セキュリティトークンの配置の仕様とともに生成する。処理は、その後、終了ブロック６２２に流れて終了し、またはブロック４１８等の呼び出しプログラムに戻ることができる。判定ブロック６０６において、断片化を行なうべきと判定した場合、処理は、ブロック６１０に流れることができ、そこで、セキュリティトークンの断片化を実行し、複数のＨＴＴＰトークンヘッダを生成し、セキュリティトークンの断片を、各ヘッダに挿入する。処理は、その後、ブロック６２０に流れることができ、そこでトークン配置ヘッダを生成することができる。ブロック６２０において、セキュリティトークンを断片化している場合、トークン配置ヘッダは、断片の数および各断片のサイズを特定することができる。この処理は、終了ブロック６２２に流れることができる。

【００６１】

判定ブロック６０４において。ＨＴＴＰメッセージの本文全体がセキュリティトークンを含むべきであることを判定することができる。このように判定すると、この処理は、ブロック６１２に流れることができ、そこで、セキュリティトークンを本文内に挿入する。処理は、その後、ブロック６２０において継続することができ、そこで、トークン配置ヘッダを生成することができる。

【００６２】

判定ブロック６０４において、セキュリティトークンを、受信されたメッセージのＨＴ

ＭＬフォームフィールド内に配置するべきであることを判定することができる。このように判定すると、処理は、ブロック６１４に流れることができ、そこで、特定のフォームフィールドを生成することができ、かつセキュリティトークンをその中に挿入する。処理は、その後、ブロック６２０において継続することができ、そこで、トークン配置ヘッダを生成することができる。

【００６３】

判定ブロック６０４において、セキュリティトークンを、メッセージ本文内の特定のＸＭＬ要素内に配置するべきであることを判定することができる。このように判定すると、処置はブロック６１６に流れることができ、そこで、特定のＸＭＬ要素を生成し、かつセキュリティトークンをその中に挿入する。処理は、その後、ブロック６２０において継続することができ、そこでトークン配置ヘッダを生成することができる。

【００６４】

図７は、例示の実施形態における、ＨＴＴＰメッセージからセキュリティトークンを抽出する処理７００を示すフロー図である。処理７００は、上述のように、ブロック５０８および５１８の動作の少なくともいくつかの動作を示す。処理７００の示された部分を、ブロック７０２で開始することができ、そこで、セキュリティトークンの１または複数の配置を判定することができる。このことは、トークンの配置を特定し、およびトークンを断片化する場合、断片の数を特定するトークン配置ヘッダの分析を含むことができる。一実装において、セキュリティトークンを、４つの配置のいずれかにて構成することができる。判定ブロック７０４において、処理は、４つのブロックのうちの１つに分岐し、それぞれ配置オプションを取り扱うことができる。このような配置の１つは、１または複数のＨＴＴＰヘッダ内にある配置である。この配置であると判定した場合、処理はブロック７０６に流れることができ、そこで、セキュリティトークンの断片を、ヘッダの各々から抽出する。２以上の断片が２以上の対応するヘッダ内にある場合、これらを組み合わせて、セキュリティトークンを形成する。この処理は、その後、図５のブロック５１０または５２０において継続することができる。

【００６５】

判定ブロック７０４において、ＨＴＴＰメッセージの本文全体がセキュリティトークンを含んでいると判定することができる。このように判定した場合、処理はブロック７０８に流れることができ、そこで、セキュリティトークンを本文から抽出する。この処理は、その後、ブロック５１０または５２０において継続することができる。

【００６６】

判定ブロック７０４において、セキュリティトークンを、受信されたメッセージの特定のＨＴＭＬフォームフィールド内に配置していることを判定することができる。このように判定した場合、処理はブロック７１０に流れることができ、そこで、セキュリティトークンを特定のフォームフィールドから抽出する。この処理は、その後、ブロック５１０または５２０において継続することができる。

【００６７】

判定ブロック７０４において、セキュリティトークンを、メッセージ本文内の特定のＸＭＬ要素内に配置していることを判定することができる。このように判定した場合、処理はブロック７１２に流れることができ、そこでセキュリティトークンをＸＭＬ要素から抽出する。一実施形態において、ＸＭＬ要素の抽出を、トークン配置ヘッダフィールド内で特定されているクエリを用いて実行することができる。この処理は、その後、ブロック５１０または５２０において継続することができる。

【００６８】

処理６００および７００は、セキュリティトークンの配置に関する多数のオプションを可能にする。例えば、セキュリティトークンが、特定のＨＴＴＰヘッダサイズ制約に基づいて、単一のＨＴＴＰヘッダ内に収めるには長すぎる場合、セキュリティトークンを、複数のＨＴＴＰヘッダ内に配置することができる。セキュリティトークンが、全体ヘッダサイズにおけるＨＴＴＰ制約に基づいて、複数のＨＴＴＰヘッダ内に収めるには長すぎる場

合、セキュリティトークンを、メッセージ本文内に配置することができる。この処理は、さらに、ＨＴＭＬまたはＸＭＬを含む異なったプロトコルのメッセージ本文に適応する。例えば、要求は、ＨＴＴＰ　ＰＯＳＴメッセージの形式とすることができる。

例示のメッセージ

この節は、環境３００において説明されたメッセージまたは他のメッセージを実装するために使用することができるメッセージ内容の例を説明する。これらの説明を、実施例のセットとして理解すべきである。様々な実施形態において、これらの実施例を、それら全体としてまたはそれらのサブセットとして使用し、これにより認証スキームまたはプロトコルを形成することができる。様々な実施形態において、キーワードまたはパラメータは異なってもよく、およびその上、キーワードまたはパラメータを使用し、本明細書に記載されているメカニズムの少なくともいくつかを実行することができる。一実施形態において、これらの実施例を１つも使用しない。

【００６９】

一実施形態において、本明細書に記載されているメッセージを使用し、ＲＦＣ２６１７の認証プロトコルの拡張部であるプロトコルを形成する。名称「ＷＳＳＥＣ」を、本明細書において、このプロトコルに関する呼称として使用する。本明細書で説明されているプロトコルは、ＨＴＴＰ要求を認証する様々なスキームを容易にする。このプロトコルはまた、ＷＳＳＥＣプロトコルと共に使用するそのセマンティクス、および新しいＨＴＴＰ拡張ヘッダのセットを、このプロトコルをスタック内のＨＴＴＰ層においてまたはＨＴＴＰ層の上のアプリケーション内で実装することができるような方法にて定義することができる。

【００７０】

本明細書において上述されているように、本明細書内に記載されている様々な動作を、アプリケーション２１０のアプリケーション認証モジュール２１２（図２）、またはＨＴＴＰスタック２０６の認証モジュール２０８によって実行することができる。一実施形態において、メッセージおよびメッセージヘッダを、アプリケーション２１０またはＨＴＴＰスタック２０６による実装を提供するように設計し、アプリケーションは、ＨＴＴＰスタックがヘッダまたはパラメータの少なくともいくつかを認識せずまたは処理しない環境においてこれらのメカニズムの少なくともいくつかを実装することができる。例えば、いくつかのウェブサーバを、特定されている認証スキームをウェブサーバが認識しない場合に、標準のＨＴＴＰ認証ヘッダを取り除くように構成する。このような環境において、本明細書において定義されているカスタムヘッダは、アプリケーションにまだ使用可能であり、認証プロトコルを成立させる。

【００７１】

ある環境において、ＨＴＴＰスタックを、本明細書において説明されている認証スキームを認識し、かつ処理するように構成することができ、アプリケーションを、これらのタスクを実行することから解放する。従って、証明書利用者が本明細書に記載されているヘッダを認識するかまたは実装するＨＴＴＰスタックを有するかに関わらず、要求者は、同一の態様にて様々な証明書利用者とやりとりをすることができる。同様に、証明書利用者は、要求者の各ＨＴＴＰスタックが本明細書に記載されているＨＴＴＰヘッダを実装しているかに関わらず、様々な要求者とやりとりすることができる。さらに、アプリケーションは、ＨＴＴＰスタックを、認証スキームを処理しない環境において展開することができる。ＨＴＴＰスタックを更新し、認証スキームを処理する場合、アプリケーションは、機能し続けて、ＨＴＴＰスタックが認証動作を実行することを可能にする。

【００７２】

表１は、記載されたメッセージの各々において使用可能なＨＴＴＰヘッダを示す。各メッセージにおいて、記載されていない追加のＨＴＴＰヘッダを含むことができる。

【００７３】

【表１】

表1

	認証ヘッダ
不許可メッセージ 312	WWW-Authenticate X-WSS-Authenticate
リクエストメッセージ 318	Authorization X-WSS-Security X-WSS-TokenLoc X-WSS-Token X-WSS-Digest
応答メッセージ 320	X-WSS-AuthInfo

【００７４】

表２は、表１の各ＨＴＴＰヘッダに関して、ヘッダに包含可能なパラメータのセットを示す。例示の実施形態において、パラメータの多くが、パラメータ名を表すキーワードの後にパラメータの値が続く「name=value」形式である。一実施形態において、様々な実施形態においてプロトコルが異なり得るが、角括弧内に列挙されているパラメータは任意的であるとみなされる。

【００７５】

以下の説明において、ヘッダを使用し、ヘッダの記述の特定を補助するが、ヘッダの使用は、関連するテキストをヘッダに限定すること、またはヘッダの記述を付随するテキストに限定することを示唆しない。

【００７６】

【表２】

表2

	ヘッダパラメータ
WWW-Authenticate: WSSEC	[**realm**="realm-spec",] [**profile**="token-profile"]
X-WSS-Authenticate:	**nonce**="nonce-value", [**sigmethod**="signature-method",] [**sigusage**="signature-usage",] [**version**="protocol-version"]
Authorization: WSSEC	[**realm**="realm-spec",] [**profile**="token-profile"]
X-WSS-Security: "token-profile"	**timestamp**="timestamp-value", **nonce**="nonce-value" [**sigmethod**="signature-method",] [**sigusage**="signature-usage",] [**signature**="signature-value",] [**version**="protocol-version"]
X-WSS-TokenLoc: "location-type"	[**frags**="fragment-count",][**fragsize**="fragment-size"] **fieldname**="form-field-name" | [**querytype**="query-type",]**query**="query-string"
X-WSS-Token<*n*>:	"*token-fragment-content*"
X-WSS-Digest:	[**method**="*digest-method*",] **digest**="*content-digest*"
X-WSS-AuthInfo:	[**nextnonce**="nonce-value",] [**ctxtoken**="context-token", **ctxtokensecret**="context-token-secret"]

【００７７】
ＷＷＷ－Ａｕｔｈｅｎｔｉｃａｔｅヘッダ
一実施形態において、不許可メッセージ３１２内のキーワード「ＷＳＳＥＣ」を伴うＷＷＷ－Ａｕｔｈｅｎｔｉｃａｔｅヘッダの使用は、本明細書内に記載されているメカニズムの少なくともいくつかに関するサポートを示す。
【００７８】
ＷＷＷ－Ａｕｔｈｅｎｔｉｃａｔｅヘッダは、１または複数の認証仕様を含む。このＨＴＴＰヘッダにおいて、「realm-spec」は、保護領域を特定することができる。セキュリティトークンプロファイルは、ダイレクトセキュリティトークンの生成の形式および対応するアルゴリズムを特定する。トークンプロファイルの例は、仕様ケロベロスｖ．５サービスチケットプロファイル、ｘ．５０９ｖ３認証プロファイル、ＳＡＭＬｖ１．１アサーション、ＳＡＭＬｖ２．０アサーション、または証明書利用者によって発行されたセキュリティコンテキストトークンを含む。
Ｘ－ＷＳＳ－Ａｕｔｈｅｎｔｉｃａｔｅヘッダ
一実施形態において、Ｘ－ＷＳＳ－Ａｕｔｈｅｎｔｉｃａｔｅヘッダを、不許可メッセージ３１２の中で証明書利用者によって使用し、認証仕様および、さらに具体的には、要求者を指示し、後に続くメッセージで使用するという署名仕様を送ることができる。パラメータを以下のように定義する。
【００７９】
nonce-value：Ｂａｓｅ６４でエンコードされたノンス値。
signature-method：要求を署名するために使用される署名アルゴリズムの任意的な仕様。
【００８０】
signature-usage：証明書利用者が要求内の署名を介して要求者に伝達したい意味論的使用法または目的（semantic usage or purpose）の任意的な仕様。
version；プロトコルバージョンの任意的な仕様。
【００８１】
以下は、ＷＷＷ－ＡｕｔｈｅｎｔｉｃａｔｅおよびＸ－ＷＳＳ－Ａｕｔｈｅｎｔｉｃａｔｅヘッダを含む不許可メッセージ３１２の少なくとも一部の例示の実施形態である：
【００８２】
【表３】

```
HTTP/1.1 401 Unauthorized
        WWW-Authenticate: WSSEC realm="contoso.com", profile="samlv1.1"
        X-WSS-Authenticate: nonce="uV3F3YluFJax1c",
                            sigmethod="hmac-sha1",
                            sigusage="auth-int",
                            version="1.0"
```

【００８３】
許可ヘッダ
一実施形態において、許可ヘッダを、要求者によって要求メッセージ３１８内に含め、認証に関するＷＳＳＥＣプロトコルへの準拠を示す。「realm-spec」および「token-profile」パラメータは、各々任意的とすることができる。一実施形態において、これらのフィールドの各々は、許可ヘッダを含む場合、不許可メッセージ３１２において証明書利用者から受信されるＷＷＷ－Ａｕｔｈｅｎｔｉｃａｔｅヘッダ内の対応するフィールドに合致する。
Ｘ－ＷＳＳ－Ｓｅｃｕｒｉｔｙヘッダ
一実施形態において、Ｘ－ＷＳＳ－Ｓｅｃｕｒｉｔｙヘッダを要求メッセージ３１８内で使用し、デジタル署名に関連するセキュリティ情報を提供し、および証明書利用者から受信された署名仕様への準拠を示すことができる。このヘッダは、要求認証に使用される

セキュリティトークンの所有の証明を提供することを要求者に可能にするプロトコルパラメータを有する。さらに具体的にいうと、このヘッダは、トークンを要求に暗号的に結び付ける認証トークン内にある暗号化キー（key material）を使用するデジタル署名を含むことができる。一実施形態において、パラメータを以下のように定義する。

【００８４】

「timestamp-value」、これは、整数のタイムスタンプ値を特定する。

「nonce-value」、これは、Ｂａｓｅ６４でエンコードされたノンス値とすることができる。

【００８５】

「signature-method」、これは、要求を署名するために使用される署名アルゴリズムを任意的に特定する。

「signature-usage」、これは、要求者が要求内の署名を介して伝達したいと望む意味論的使用方法または目的の任意的な仕様である。

【００８６】

「signature-value」、これは、要求のデジタル署名の任意的な値である。

「protocol-version」、これは、プロトコルバージョンの任意的な仕様である。

ノンスおよびタイムスタンプは、要求リプレイ攻撃の阻止の前に、要求を提示しなかったことの保証を提供する。このノンスは、同一のタイムスタンプを有する複数のメッセージをリプレイするかまたは複製するかを判定することを証明書利用者に可能とさせる乱数とすることができる。以下は、認証およびＸ－ＷＳＳ－Ｓｅｃｕｒｉｔｙヘッダを含む要求メッセージ３１８の部分の一例である。

【００８７】

【表４】

```
POST /resource/add.aspx HTTP/1.1
Host: www.contoso.com
Content-Type: application/xml
Authorization: WSSEC realm="contoso.com", profile="samlv1.1"
X-WSS-Security:      samlv1.1
                     nonce="uV3F3YluFJax1c",
                     timestamp="1288542340",
                     sigmethod="hmac-sha1",
                     sigusage="auth-int",
                     signature="gU53F679YHluax2dcJH...",
                     version="1.0"
```

【００８８】

Ｘ－ＷＳＳ－ＴｏｋｅｎＬｏｃ

一実施形態において、Ｘ－ＷＳＳ－ＴｏｋｅｎＬｏｃヘッダは、ＨＴＴＰメッセージ内のセキュリティトークンの配置を特定する。このセキュリティトークンは、ダイレクトまたは非ダイレクトセキュリティトークンとすることができる。これらのパラメータを、以下のように定義する。

【００８９】

「location-type」、これは、トークンの配置を特定する。これは、キーワード「header」「body」「body-form」または「body-xml」のうちの１つとすることができる。

「fragment-count」および「fragment-size」、これらのパラメータを、「header」配置と共に使用し、ならびにそれぞれ、断片の数および各断片のサイズを特定する。

【００９０】

「form-field-name」、これを、「body-form」配置と共に使用する。これは、ＨＴＭＬ

フォーム内のフィールド名を特定する。
「query-type」および「query-string」、これらのパラメータは、「body-xml」配置と共に使用され、およびクエリを特定し、ｘｍｌ要素を抽出することができる。
Ｘ－ＷＳＳ－Ｔｏｋｅｎヘッダ
一実施形態において、本明細書において説明されているように、Ｘ－ＷＳＳ－ＴｏｋｅｎＬｏｃヘッダの「location-type」パラメータの値を「header」として特定する場合、Ｘ－ＷＳＳ－Ｔｏｋｅｎヘッダを使用し、セキュリティトークンを送信する。ダイレクトセキュリティトークンの仕様を、認証ヘッダ内の「token-profile」パラメータによって特定することができ、かつ証明書利用者から受信された認証仕様に準拠することができる。
【００９１】
セキュリティトークンは１つの断片内にあるか、または複数の断片内に分割可能であり、各断片を、異なったＸ－ＷＳＳ－Ｔｏｋｅｎヘッダフィールドによって保持する。断片の数を、Ｘ－ＷＳＳ－ＴｏｋｅｎＬｏｃヘッダの「fragment-count」フィールドによって示すことができる。
【００９２】
一実施形態において、各Ｘ－ＷＳＳ－Ｔｏｋｅｎヘッダの名前を、基本の「X-WSS-Token」に、整数値の添え字　Ｎ＝１，．．．，断片数　を付けることによって生成し、ここで断片数は、Ｘ－ＷＳＳ－ＴｏｋｅｎＬｏｃヘッダの「fragment-count」フィールドによって特定されるような、トークンを分割して入れる断片の数である。例えば、「X-WSS-Token1」と名付けられたヘッダは、第１のトークン断片を保持することができ、「X-WSS-Token2」と名付けられたヘッダは、第２のトークン断片を保持することができる、等である。一実施形態において、このヘッダによって送信されたトークンの受信者は、基本名「XWSS-Token」を有する全てのヘッダを収集して、およびそれらの内容を、順番に結び付けてトークン全部の内容を再構築する。
Ｘ－ＷＳＳ－Ｄｉｇｅｓｔヘッダ
一実施形態において、Ｘ－ＷＳＳ－Ｄｉｇｅｓｔヘッダを使用し、メッセージ内に保持されている本文の要約を送信することができる。少なくともいくつかのＨＴＴＰヘッダの一部を、要約内に含むことができる。特に、認証に関連するＨＴＴＰヘッダの少なくともいくつかを含むことができる。これは、表２に列挙されている「Ｘ－ＷＳＳ」ヘッダを含むことができる。要約を処理する前に、処理すべき内容を、正規化形式に変換することができる。内容の正規化は、全ての文字を小文字にすること、空白スペースを除去すること、ヘッダまたはパラメータをアルファベット順にソートすること、ＵＲＬを正規化すること等の変換を含むことができる。この要約は、完全性保護を提供して、かつメッセージ本文またはヘッダの検証を容易にする。一実施形態において、このヘッダを、「sigusage」パラメータによって示されるメッセージ本文をカバーする署名を有するＸ－ＷＳＳ－セキュリティヘッダとともに使用する。一実施形態において、このメッセージのパラメータを以下のように使用する。
【００９３】
「digest-method」、この文字列は、本文の要約を処理するために使用されるハッシュアルゴリズムを特定する。
「content-digest」、これはＢａｓｅ６４でエンコードされた要約値を特定するバイナリ値パラメータである。
【００９４】
以下は、ＳＨＡ－１要約方法を特定する際に使用することができるＸ－ＷＳＳ－要約ヘッダの一例である。
X-WSS-Digest: method=”sha1” digest=”3F679YHluax2dc”
Ｘ－ＷＳＳ－ＡｕｔｈＩｎｆｏヘッダ
一実施形態においてＸ－ＷＳＳ－ＡｕｔｈＩｎｆｏヘッダを、証明書利用者によって応答メッセージ３２０内で使用し、要求認証が成功した後に、追加のパラメータを、認証に

関連する要求者に送信することができる。これらのパラメータは、任意の後の要求認証の動作に影響を与えるか、または当該動作を変更することができる。一実施形態において、このメッセージのパラメータを以下のように使用する。

【００９５】

「nonce-value」、これは、次の要求認証に使用されるべき新しいノンス値を特定する。このパラメータが存在する場合、このパラメータは、この証明書利用者への次の要求メッセージのＸ－ＷＳＳ－Ｓｅｃｕｒｉｔｙヘッダ内で、この値を使用するように要求者に指示する。

【００９６】

「context-token」、このパラメータは、証明書利用者によって要求者のために設定されるセキュリティコンテキストを表す暗号化クッキー等のセキュリティコンテキストトークンを含む。このパラメータは、そのセキュリティコンテキストトークンを、将来の要求において使用すべきことを要求者に指示する。セキュリティコンテキストの保持の証明を提供するために使用される暗号化キーを、「context-token」パラメータ内で特定する。

【００９７】

「context-token-secret」、このパラメータを、「context-token」パラメータと共に使用する。このパラメータは、「context-token」パラメータによって表されたセキュリティコンテキストの所有権を証明するために要求者によって使用可能な秘密対称暗号化キーを特定する。

【００９８】

証明書利用者は、ワンタイム・ノンスを実装する手段として「nonce-value」パラメータを送信することができる。証明書利用者は、「context-token」および「context-token-secret」パラメータの組み合わせを使用して、要求者のためのセキュリティコンテキストを構築し、そのコンテキスト内の将来の認証は、（例えば、トークンサイズが大きい場合、）最初の要求と共に提示されるセキュリティトークンを含む必要は無い。一実施形態において、要求者および証明書利用者は、ＳＳＬまたはＴＬＳ等のトランスポート層セキュリティを使用して、このやりとりの機密性を保護する。

【００９９】

以下は、セキュリティコンテキストトークンおよび対応する証明キーを有するＸ－ＷＳＳ－ＡｕｔｈＩｎｆｏヘッダを含む応答メッセージ３２０の例である。

X-WSS-AuthInfo: ctxtoken=”fg75kVB890Uwstm…”,ctxtokensecret=”gU59cJH…”

図８は、実施形態の一例における、ＨＴＴＰメッセージの生成の処理８００を示すフロー図である。処理８００は、上述されるようなブロック４１８の動作の少なくともいくつかを示している。処理８００の示されている部分を、ブロック８０２で開始することができ、そこで、セキュリティトークンを、メッセージ本文または１もしくは複数のＨＴＴＰヘッダに挿入する。ブロック８０２の動作は、図６において説明されている。

【０１００】

ブロック８０４において、セキュリティトークンの配置の仕様を含むトークン説明ヘッダを生成する。ブロック８０４の動作は、図６において説明されている。表２および関連する説明は、トークン配置ヘッダの一実施形態を説明している。

【０１０１】

ブロック８０６において、デジタル署名を生成し、かつセキュリティヘッダ内に挿入することができる。表２および関連する説明は、セキュリティヘッダの一実施形態を説明している。

【０１０２】

ブロック８０８において、許可ヘッダを生成することができる。表２および関連する説明は、許可ヘッダの一実施形態を説明している。

ブロック８１０において、要約を生成し、かつ要約ヘッダ内に挿入することができる。表２および関連する説明は、要約ヘッダの一実施形態を説明している。処理８００は、ブロック８２０に流れて終了するか、またはプログラム呼び出しに戻ることができる。

【０１０３】
一実施形態では、ブロック８１０の動作を実行せず、および要約ヘッダを生成しない。様々な実施形態において、本明細書において説明されている他のヘッダを、要求ヘッダから除外することができる。図８のブロックおよび関連する動作の順序は、様々な順序でなされてもよく、およびこの処理を図示された順序に限定しない。
【０１０４】
本明細書において上述されたように、一実施形態において、要求者は、本明細書において説明されたメカニズムおよびプロトコルの少なくともいくつかを使用して、ＩＤプロバイダからのトークンを要求することができる。以下は、このような使用法の一例であり、この例は、要求ＳＴメッセージ３１４の少なくとも一部を形成することができる。この例において、ＨＴＴＰ　ＰＯＳＴメソッドを要求に使用している。
【０１０５】
【表５】

```
POST /sts/issue HTTP/1.1
Host: contoso.com
Authorization: WSSEC profile=samlv1.1”
Content-Type: application/xml
X-WSS-Security:      nonce=”uV3F3YluFJax1c”, timestamp=”1288542340”,
        sigmethod=”hmac-sha1”, sigusage=”auth-int”,
        signature=”gU53F679YHluax2dcJH...”, version=”1.0”
X-WSS-Digest: method=”sha1” digest=”3F679YHluax2dc”
X-WSS-TokenLoc: header
X-WSS-Token1: w87xzV6Flm53KluDJay3d...

<RequestSecurityToken>
        <AppliesTo> xyz </AppliesTo>
</RequestSecurityToken>
```

【０１０６】
他の例において、ＰＯＳＴ本文内のＸＭＬベースのペイロードの代わりに、ＸＭＬタグ名とフォームフィールド名との間のマッピングを定義することによって、フォームベース（form-based）のペイロードを使用することができる。例えば、フォームベースのペイロードを使用する上述の要求を、以下に示す。
【０１０７】
【表６】

```
POST /sts/issue HTTP/1.1
Host: contoso.com
Authorization: WSSEC profile=samlv1.1”
Content-Type: application/xml
X-WSS-Security:      nonce=”uV3F3YluFJax1c”, timestamp=”1288542340”,
        sigmethod=”hmac-sha1”, sigusage=”auth-int”,
        signature=”gU53F679YHluax2dcJH...”, version=”1.0”
X-WSS-Digest: method=”sha1” digest=”3F679YHluax2dc”
X-WSS-TokenLoc: header
X-WSS-Token1: w87xzV6Flm53KluDJay3d...

AppliesTo=xyz
```

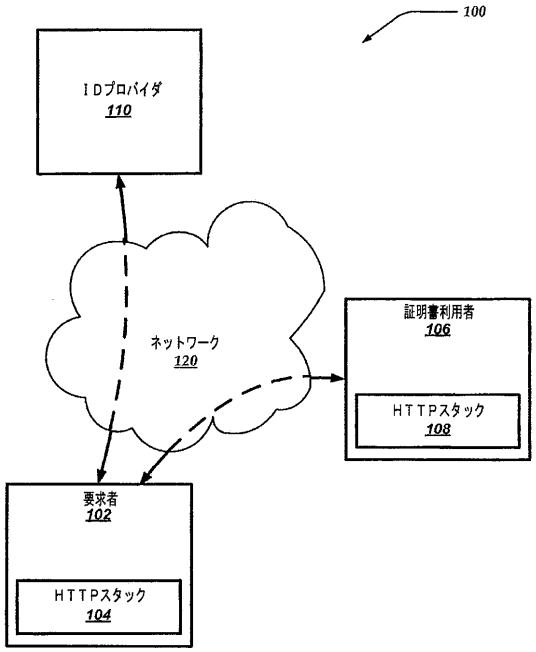
【０１０８】

図４－８のフローチャート図の各ブロック、およびフローチャート図内のブロックの組み合わせを、ソフトウェア命令によって実装することができることを理解されたい。これらのプログラム命令を、プロセッサに提供し、プロセッサ上で実行される命令が、フローチャートのブロック（１または複数）内で特定される動作を実装する手段を生成するようなマシンをもたらすことができる。ソフトウェア命令をプロセッサによって実行し、フローチャートのブロック（１または複数）内で特定される動作を実装するステップをもたらすことができる。さらに、フローチャート図内の１もしくは複数のブロックまたはブロックの組み合わせを、本発明の範囲または趣旨から逸脱することなく、他のブロックもしくはブロックの組み合わせと同時に実行することができ、または図示されているのと異なる順序で実行することができる。

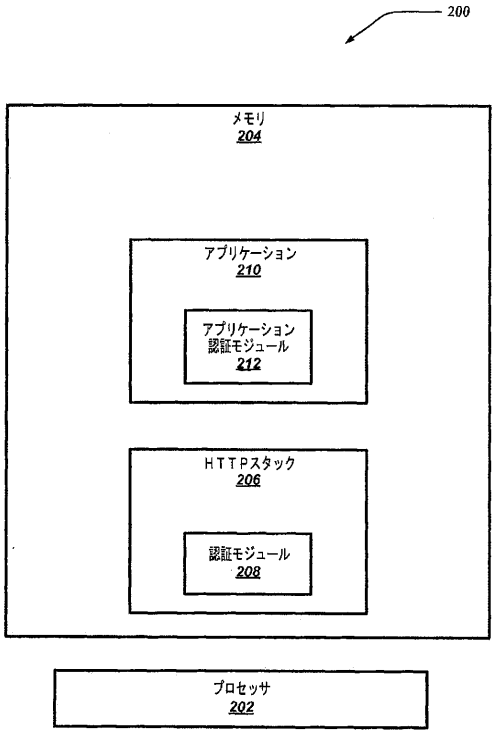
【０１０９】

上述の明細書、例示、およびデータは、本発明の製品および本発明の構成の使用法の完全な説明を提供する。従って、本発明の多くの実施形態を、本発明の趣旨および範囲から逸脱することなく行なうことができ、本発明は添付の特許請求の範囲内にある。

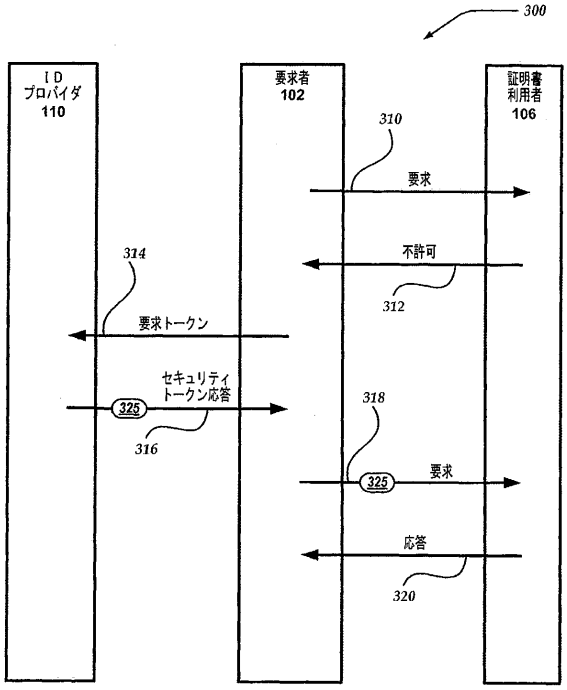
【図１】



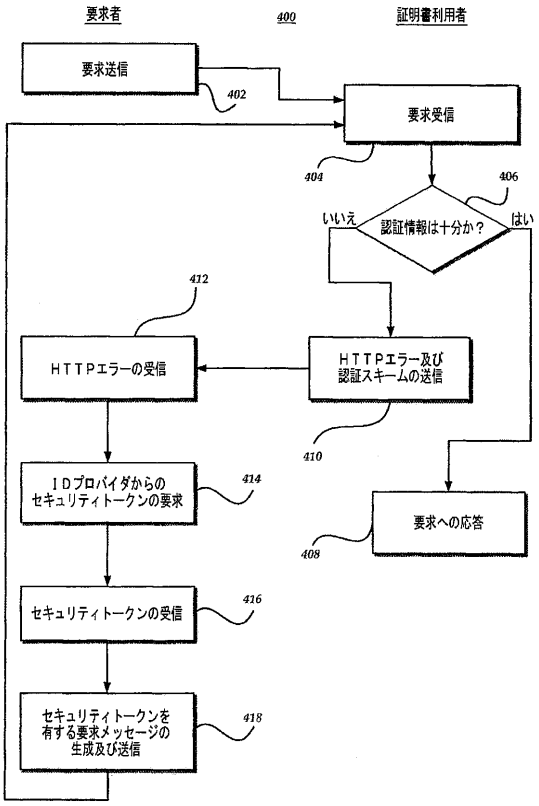
【図２】



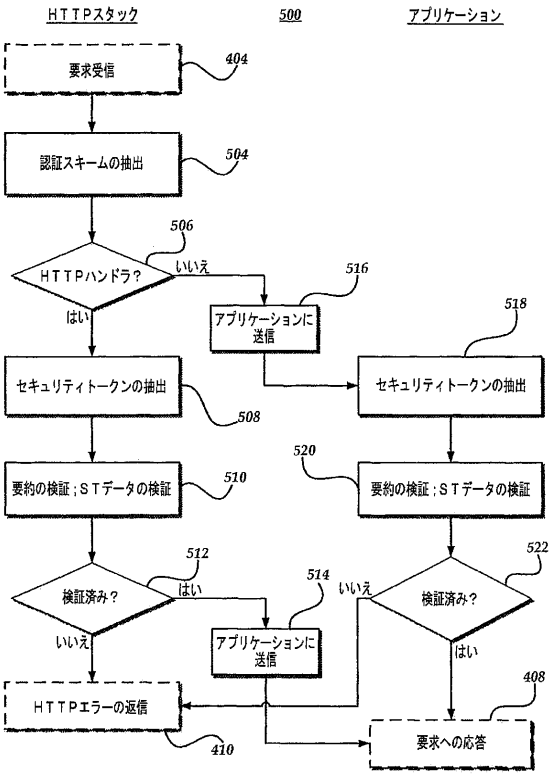
【図３】


300
IDプロバイダ 110
要求者 102
証明書利用者 106
310
要求
不許可
312
314
要求トークン
セキュリティトークン応答
325
316
318
325
要求
応答
320

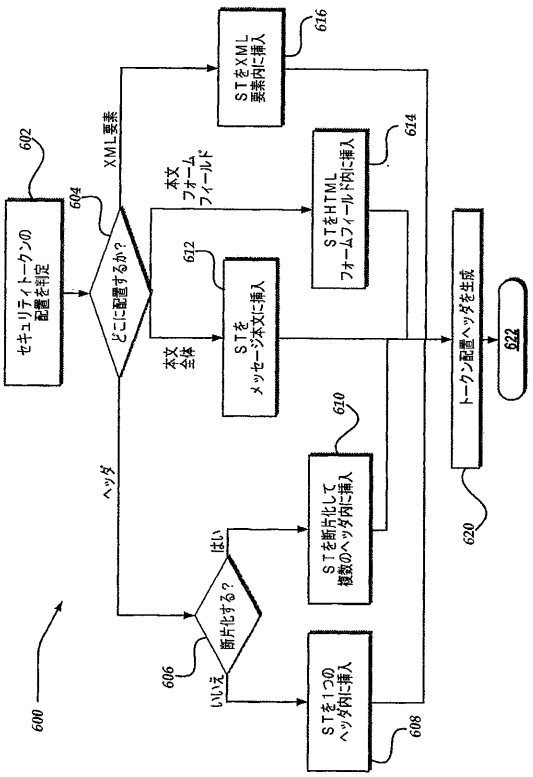
【図４】


要求者
400
証明書利用者
要求送信
402
要求受信
404
406
いいえ
認証情報は十分か？
はい
412
HTTPエラーの受信
HTTPエラー及び認証スキームの送信
410
IDプロバイダからのセキュリティトークンの要求
414
要求への応答
408
セキュリティトークンの受信
416
セキュリティトークンを有する要求メッセージの生成及び送信
418

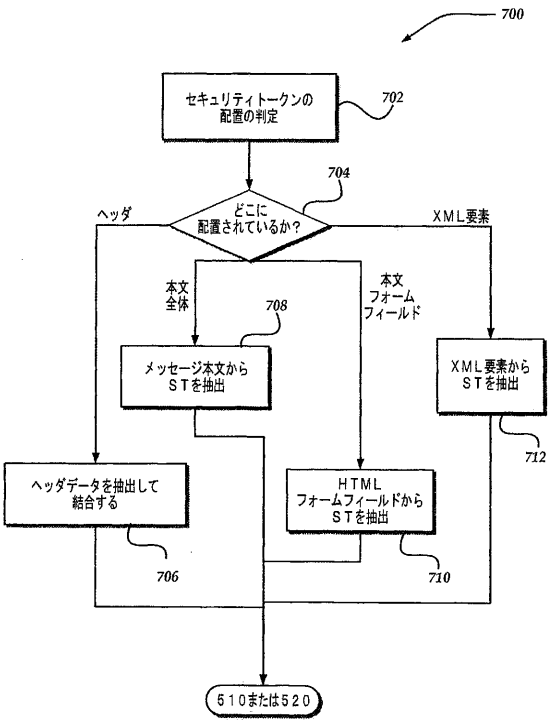
【図５】


HTTPスタック
500
アプリケーション
要求受信
404
認証スキームの抽出
504
HTTPハンドラ？
506
いいえ
はい
516
アプリケーションに送信
518
セキュリティトークンの抽出
508
セキュリティトークンの抽出
要約の検証；STデータの検証
510
520
要約の検証；STデータの検証
検証済み？
512
はい
いいえ
514
アプリケーションに送信
検証済み？
522
いいえ
はい
HTTPエラーの返信
410
408
要求への応答

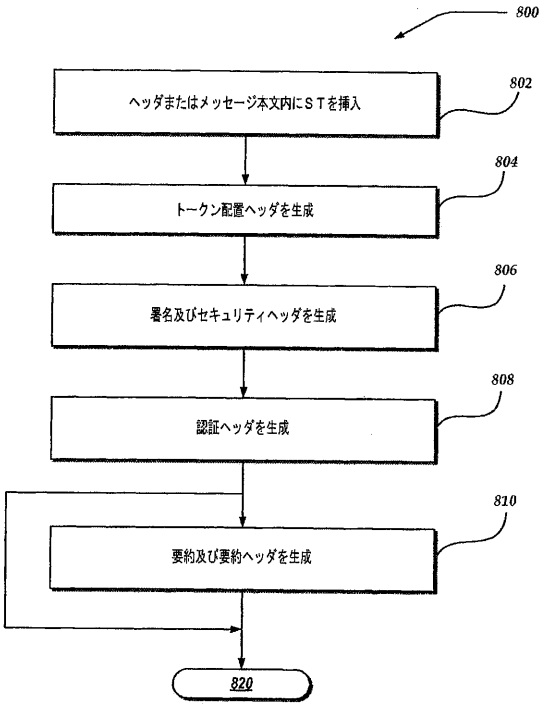
【図６】


600
セキュリティトークンの配置を判定
602
どこに配置するか？
604
XML要素
本文フォームフィールド
本文全体
ヘッダ
STをXML要素内に挿入
616
STをHTMLフォームフィールド内に挿入
614
STをメッセージ本文に挿入
612
STを断片化して複数のヘッダ内に挿入
610
断片化する？
606
はい
いいえ
STを1つのヘッダ内に挿入
608
トークン配置ヘッダを生成
620
622

【図７】


700
セキュリティトークンの配置の判定
702
704
どこに配置されているか？
ヘッダ
XML要素
本文全体
本文フォームフィールド
708
メッセージ本文からSTを抽出
XML要素からSTを抽出
712
ヘッダデータを抽出して結合する
HTMLフォームフィールドからSTを抽出
706
710
510または520

【図８】


800
ヘッダまたはメッセージ本文内にSTを挿入
802
804
トークン配置ヘッダを生成
806
署名及びセキュリティヘッダを生成
808
認証ヘッダを生成
810
要約及び要約ヘッダを生成
820

フロントページの続き

(72)発明者 アルン ケー. ナンダ
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 ハーヴェイ ウィルソン
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内

審査官 青木 重徳

(56)参考文献 特開２００８－２７６７２４（ＪＰ，Ａ）
特開２００５－３２２２３４（ＪＰ，Ａ）
特開２００３－１０８４５５（ＪＰ，Ａ）
特開２０００－０５７１１２（ＪＰ，Ａ）
特表２００９－５１４０５０（ＪＰ，Ａ）
特表２００６－５２５５９２（ＪＰ，Ａ）
米国特許出願公開第２００７／０１４０４９３（ＵＳ，Ａ１）
米国特許出願公開第２００７／０００５８０１（ＵＳ，Ａ１）
太田 純 他，最先端のXML＆Ｊａｖａ技術を身につけよう！ “本気”で学ぶＷｅｂサービス 第2回，Ｊａｖａ ＷＯＲＬＤ，日本，（株）ＩＤＧジャパン，２００３年１２月 1日，第7巻，第１２号，ｐ．１５５－１６２
高瀬 俊郎，ＳＯＡＰ入門及び最新動向，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００３年 1月 9日，Ｖｏｌ．１０２，Ｎｏ．５６４，ｐ．５３－５８
原 陽亮，ＧＴＤタスク管理ツール ｔｕｇｂｏａｔ．ＧＴＤ ＡＩＲ Ｅｄｉｔｉｏｎ紹介，ＳｏｆｔｗａｒｅＤｅｓｉｇｎ，日本，（株）技術評論社，２００８年 1月１８日，Ｎｏ．２０７，ｐ．１０８－１１８
山本 陽平，ＲＥＳＴレシピ クールなＷｅｂシステムへの道しるべ 第9回，ＷＥＢ＋ＤＢ ＰＲＥＳＳ，日本，（株）技術評論社，２００８年 9月２５日，Ｖｏｌ．４６ 初版，ｐ．２０４－２０９

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３３
Ｇ０９Ｃ １／００
Ｈ０４Ｗ １２／０２
Ｈ０４Ｗ １２／０６