(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2015-535362
(P2015-535362A)
(43)公表日　平成27年12月10日(2015.12.10)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/44	(2013.01)	G06F	21/44	5B084
G06F 13/00	(2006.01)	G06F	13/00	510A
G06F 21/33	(2013.01)	G06F	21/33	

審査請求 未請求　予備審査請求 未請求　（全 16 頁）

(21)出願番号　特願2015-532381 (P2015-532381)
(86)(22)出願日　平成25年9月16日 (2013.9.16)
(85)翻訳文提出日　平成27年5月18日 (2015.5.18)
(86)国際出願番号　PCT/EP2013/069178
(87)国際公開番号　WO2014/044641
(87)国際公開日　平成26年3月27日 (2014.3.27)
(31)優先権主張番号　12306126.9
(32)優先日　平成24年9月18日 (2012.9.18)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所

最終頁に続く

(54)【発明の名称】ウェブサービスに安全にアクセスするための方法および装置

(57)【要約】
本発明は、ユーザ装置上でウェブアプリケーションを実行するブラウザが、ネットワークを介して安全にウェブサービスにアクセスする方法に関する。ウェブサービスは、ユーザ装置がアクセスしているローカル装置を含む少なくとも１つの装置によってホストされている。ローカル装置は、ローカル装置を一意に識別するグローバル名と、グローバル名に関連付けられた証明書と、を含む。方法は、ウェブアプリケーションが、ウェブサービスをホストする任意の装置を識別する一般名を指定することによって、ウェブサービスへのアクセスを求める要求をネットワークに送信するステップと、ウェブアプリケーションが、ウェブサービスをホストするローカル装置を識別するグローバル名を含む、要求に対する応答をネットワークから受信するステップと、ウェブアプリケーションが、受信したグローバル名がリストに含まれることを検証するステップと、検証に成功した場合、グローバル名を指定することによってローカル装置に接続するステップと、ローカル装置から証明書を受信するステップと、ブラウザが、グローバル名に関連付けられた証

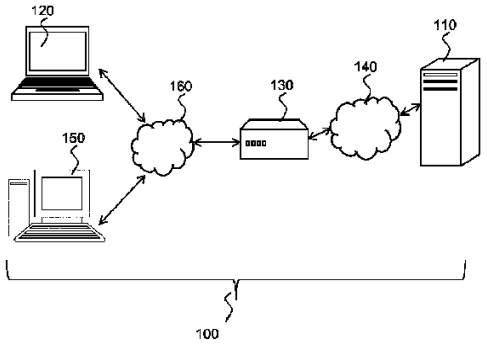


Figure 1

【特許請求の範囲】
【請求項１】
ユーザ装置（１２０）上でウェブアプリケーションを実行するブラウザが、前記ユーザ装置がアクセスしているローカル装置（１５０、１３０）を含む少なくとも１つによってホストされているウェブサービスに、ネットワーク（１６０）を介して安全にアクセスする方法であって、前記ローカル装置（１５０、１３０）は、前記ローカル装置を一意に識別するグローバル名（３０１）と、前記グローバル名に関連付けられた証明書と、を含み、
前記ウェブアプリケーションが、前記ウェブサービスをホストする任意の装置を識別する一般名（３００）を指定することにより、前記ウェブサービスへのアクセスの要求を前記ネットワーク（１６０）に送信するステップと、
前記ウェブアプリケーションが、前記要求への応答であって、前記ウェブサービスをホストする前記ローカル装置（１３０、１５０）を識別する前記グローバル名（３０１）を含む応答を、前記ネットワーク（１６０）から受信するステップと、
前記ウェブアプリケーションが、前記受信したグローバル名がリストに含まれていることを検証するステップと、
前記検証に成功した場合、前記グローバル名（３０１）を指定することによって、前記ローカル装置（１５０、１３０）に接続し、前記証明書を前記ローカル装置から受信し、前記ブラウザが、前記グローバル名に関連付けられた前記証明書を検証し、かつ、前記ウェブサービスに安全にアクセスするステップと、
をさらに含む、前記方法。
【請求項２】
前記リストは、前記ウェブサービスをホストする信頼できる装置のグローバル名を含む、請求項１に記載の方法。
【請求項３】
前記ローカル装置は、前記グローバル名と、前記グローバル名に関連付けられた前記証明書とを、信頼できるオペレータによって配信される、請求項１または２に記載の方法。
【請求項４】
前記リストは、前記ブラウザで実行している前記ウェブアプリケーションによって、前記信頼できるオペレータから動的に取得される、請求項３に記載の方法。
【請求項５】
前記リストは、前記ブラウザで実行している前記ウェブアプリケーションにハードコードされる、請求項３に記載の方法。
【請求項６】
前記グローバル名（３０１）を指定することによって前記ローカル装置（１５０、１３０）に接続するステップは、前記グローバル名（３０１）を指定することによって、前記ウェブサービスへのアクセスの第２の要求を外部のネットワーク（１４０）に送信するステップと、前記第２の要求に対する応答であって、前記ローカル装置（１３０、１５０）のローカルＩＰアドレスを含む応答を前記ネットワーク（１４０）から受信するステップと、をさらに含む、請求項１から５のいずれかに記載の方法。
【請求項７】
前記グローバル名に関連付けられた前記ローカル装置の前記ローカルＩＰアドレスを、信頼できるオペレータで公開する予備段階をさらに含む、請求項６に記載の方法。
【請求項８】
前記ローカル装置の前記ローカルＩＰアドレスと、前記グローバル名とのマッピングは、前記信頼できるオペレータによって実行されるＤＮＳサービスによって維持される、請求項６または７に記載の方法。
【請求項９】
一般名を指定することによる前記ウェブサービスへのアクセスの前記要求は、ＨＴＴＰ要求である、請求項１から８のいずれかに記載の方法。

【請求項１０】
前記グローバル名を指定することによる前記ウェブサービスへの安全なアクセスの要求は、ＨＴＴＰＳ要求である、請求項１から９のいずれかに記載の方法。
【請求項１１】
前記ローカル装置はゲートウェイである、請求項１から１０のいずれかに記載の方法。
【請求項１２】
ウェブアプリケーションを実行するブラウザが、ウェブサービスにネットワークを介して安全にアクセスするためのユーザ装置（１２０、４００）であって、前記ウェブサービスは、前記ユーザ装置がアクセスしているローカル装置を含む少なくとも１つの装置によってホストされ、
前記ウェブアプリケーションが、前記ウェブサービスをホストする任意の装置を識別する一般名を指定することによって、前記ウェブサービスへのアクセスの要求を前記ネットワークに送信する手段と、
前記ウェブアプリケーションが、前記ウェブサービスをホストする前記ローカル装置を一意に識別するグローバル名を含む、前記要求に対する応答を、前記ネットワークから受信する手段と、
前記ウェブアプリケーションが、前記ウェブサービスをホストする信頼できる装置のグローバル名を含むリストに前記受信したグローバル名が含まれていることを、検証する手段と、
前記ウェブアプリケーションが、前記グローバル名を指定することによって、前記ローカル装置に接続する手段と、前記ローカル装置から受信した証明書を受信する手段と、前記ブラウザが、前記グローバル名に関連付けられた前記証明書を検証する手段と、前記ウェブサービスに安全にアクセスする手段と、
を含むユーザ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的に、ウェブサービスへの安全なアクセスの分野に関する。より詳細には、本発明は、ユーザ装置上でウェブアプリケーションを実行しているブラウザが、ローカル装置によってホストされているウェブサービスに、ネットワークを介して安全にアクセスする方法に関する。
【背景技術】
【０００２】
この項は、当技術の様々な態様を読者に紹介するためのものであり、それらは、下記に記載、および／または、特許を請求する発明の様々な態様に関連すると思われる。この項の記載は、本発明の様々な態様をより良く理解するための背景情報を読者に提供する役に立つと考える。従って、この項の記載はこの観点で読むべきものであり、先行技術の承認でないことは理解されたい。
【０００３】
デジタルデータ（例えば、写真、ビデオ）は、ますます、携帯機器（例えば、スマートフォン、タブレット、ラップトップ）で生成され、管理されるようになっている。このデータは、また、インターネットを介して、共有、バックアップ、または、処理されることが多い。実際に、広範な「クラウド」サービスが、写真処理サービス、ソーシャルネットワーク、または、オンラインストレージの場合、クラウドサービスはユーザのコンテンツを扱う。これらのクラウドサービスの大半は、完全にウェブ技術に依存している。結果として、ユーザは、ＨＴＴＰを介して大量のコンテンツをウェブアプリケーションにアップロードする必要がある。しかしながら、アップロードの速度は、利用可能な回線容量の制約を受ける。実際に、レガシーインフラストラクチャ（ｘＤＳＬ）、または、共有媒体（セルラー）を使用するため、インターネットへの接続速度は限られている。
【０００４】

アップロード時間が長いことによって、ユーザは、自分のスタンドアロン装置を待機状態にしたり、電源を切ったりすることができず、インターネットを介した転送を行うために装置を接続したままにする必要がある。これらの問題を軽減するために、住居用ゲートウェイ等のネットワークに永続的に接続された第三者装置にＨＴＴＰを介してアップロードをオフロードする機構が提案されている。それと共に、オフロードウェブサービスを提供する第三者装置を検索する方法が提案されている。

【０００５】

しかしながら、タスクを第三者にオフロードするためには、この第三者を信頼する必要がある。言い換えれば、オフロードサービスをホストする第三者装置は、ユーザのスタンドアロン装置によって認証される必要がある。装置またはウェブサービスを認証する既知の解決法は、信頼機関による証明書に基づくものである。証明書は、ウェブサービスを所有している信頼できるオペレータ、または、ユーザの物理的装置に、信頼機関によって配信される。しかしながら、これらの解決法は、ウェブブラウザ等のレガシーソフトウェアや、処理環境が制限されている標準ウェブプロトコルには対応していない。言い換えれば、入力および出力という点でブラウザは制限を受ける。例えば、ブラウザは、ブラウザが実行されている装置の記憶媒体（ハードディスクドライブ等）にアクセスできず、ネットワークに直接アクセスできない。

【０００６】

従って、ユーザ装置上でウェブアプリケーションを実行しているブラウザが、ローカル装置によってホストされたウェブサービスにネットワークを介して安全にアクセスする解決法が必要とされている。その方法は、実施および使用が容易なように意図的に単純であって、レガシーソフトウェアに対応し、また、ＪａｖａＳｃｒｉｐｔ（登録商標）で実施でき、かつ、ブラウザで実行するように適合されていなければならない。

【０００７】

本発明は、このような解決法を提供する。

【発明の概要】

【０００８】

第１の態様において、本発明は、ユーザ装置上でウェブアプリケーションを実行しているブラウザがネットワークを介してウェブサービスに安全にアクセスする方法に関する。ウェブサービスは、ユーザ装置よってアクセスされているローカル装置を含む、少なくとも１つの装置によってホストされている。ローカル装置は、ウェブサービスをホストし、かつ、ユーザ装置に最も近接した装置であると好都合である。ローカル装置は、ローカル装置を一意に識別するグローバル名と、グローバル名に関連付けられた証明書と、を含む。方法は、ウェブアプリケーションが、ウェブサービスをホストする任意の装置を識別する一般名を指定することによって、ウェブサービスへのアクセスの要求をネットワークに送信するステップと、ウェブアプリケーションが、ウェブサービスをホストするローカル装置を識別する上記のグローバル名を含む要求に対する応答をネットワークから受信するステップと、ウェブアプリケーションが、受信したグローバル名がリストに含まれていることを検証するステップと、検証に成功した場合、グローバル名を指定することによってローカル装置に接続するステップと、ローカル装置から証明書を受信するステップと、ブラウザがグローバル名に関連付けられた証明書を検証するステップと、ウェブサービスに安全にアクセスするステップと、をさらに含む。一般名は、任意のローカル装置がアクセス可能な名前、すなわち、ウェブサービスをホストする全ての装置に共通の名前であると好都合である。ホワイトリストとも呼ばれるリストは、ウェブサービスをホストする信頼できる装置のグローバル名を含むと好都合である。グローバル名の数は、莫大になる可能性があるので、リストはウェブサービスをホストする信頼できるローカル装置のグローバル名の包括リストを含むのではなく、ローカル装置のグローバル名にマッチするパターンを含むと好都合である。

【０００９】

有利な特性によると、ローカル装置は、グローバル名と、グローバル名に関連付けられ

た証明書と、を信頼されたオペレータによって配信される。
【００１０】
別の有利な特性によると、ホワイトリストは、ブラウザで実行しているウェブアプリケーションによって、信頼されたオペレータから動的に取得される。変形形態においては、ホワイトリストは、ブラウザで実行しているウェブアプリケーション内に、ハードコードされる。
【００１１】
第１の好適実施形態においては、一般名を指定することによるウェブサービスへのアクセスの要求は、ＨＴＴＰ要求であり、グローバル名を指定することによるウェブサービスへの安全なアクセスの要求は、ＳＳＬ要求を含むＨＴＴＰＳ要求である。
【００１２】
変形形態によると、ローカル装置は、ゲートウェイ装置、セットトップボックス、ネットワーク接続ストレージ（ＮＡＳ）である。
【００１３】
第２の態様においては、本発明は、ウェブアプリケーションを実行しているブラウザが、ネットワークを介してウェブサービスに安全にアクセスするためのユーザ装置に関する。ウェブサービスは、ユーザ装置がアクセスしているローカル装置を含む少なくとも１つの装置によってホストされている。ローカル装置は、ウェブサービスをホストし、かつ、ユーザ装置に最も近接する装置であると好都合である。装置は、ウェブアプリケーションが、ウェブサービスをホストする任意の装置を識別する一般名を指定することによって、ウェブサービスへのアクセスの要求をネットワークに送信する手段と、ウェブアプリケーションが、ウェブサービスをホストするローカル装置を一意に識別するグローバル名を含む、要求への応答をネットワークから受信する手段と、ウェブアプリケーションが、ウェブサービスをホストする信頼できるローカル装置のグローバル名を含むホワイトリストとも呼ばれるリストに、受信したグローバル名が含まれていることを検証する手段と、ウェブアプリケーションが、グローバル名を指定することによってローカル装置に接続する手段と、ローカル装置から証明書を受信する手段と、グローバル名に関連付けられた証明書を検証する手段と、ウェブサービスに安全にアクセスする手段と、を含む。
【００１４】
ユーザ装置上でウェブアプリケーションを実行しているブラウザが、ローカル装置によってホストされているウェブサービスにネットワークを介して安全にアクセスする方法に関して記載された特性または実施形態はいずれも、開示された方法を実施するように適合されたユーザ装置またはローカル装置に対応している。
【００１５】
第１の実施形態による方法は、好都合なことに、現行のソフトウェアおよび標準ウェブプロトコルに対応している。従って、ユーザのブラウザや使用しているプロトコルを変更する必要なく採用することができる。
【図面の簡単な説明】
【００１６】
本発明の好ましい特徴を、添付の図面を参照しながら、制限目的ではない例を用いて説明する。
【図１】本発明を使用することができる例示的なネットワークを示す図である。
【図２】本発明の第１の実施形態に従った安全なアクセス方法のステップを示す図である。
【図３】本発明の好適実施形態に従った安全なアクセス方法のステップを示す図である。
【図４】本発明の好適実施形態に従った安全なアクセス方法を実施するローカル装置を示す図である。
【発明を実施するための形態】
【００１７】
図１は、本発明を使用することができる例示的なネットワーク１００を示す。ネットワ

ーク１００は、写真共有アプリケーション等のウェブアプリケーションをホストするサーバ装置１１０を含む。ユーザは、電池式装置（タブレット、ラップトップコンピュータ、携帯電話）またはコンピュータ等の個人用の装置１２０を所有し、そこで、ウェブブラウザを利用することができる。ウェブアプリケーション、例えば、写真共有アプリケーションのクライアント側は、ユーザ装置１２０のブラウザで実行されており、ウェブアプリケーションは、ウェブアプリケーションのサーバ側にアクセスする。ウェブアプリケーションのクライアント側は、オフロードサービス等のウェブサービスにもアクセスすることができる。ユーザ装置は、インターネットルータ、セットトップボックス、別のユーザコンピュータ、住居用ゲートウェイ、ＮＡＳ１５０等のローカル装置上で実行しているウェブサービスにローカルエリアネットワーク１６０によって接続する。ウェブアプリケーションのクライアント側、および、ウェブサービスは、無線インターネットルータまたは住居用ゲートウェイ等のネットワークアクセス装置１３０を通してウェブアプリケーションのサーバ側にアクセスすることができる。従って、住居用ゲートウェイは、速度の速いローカルエリアネットワーク１６０と比較的遅いブロードバンドネットワーク１４０間の境界であり、ここでの遅いブロードバンドネットワークへのアクセスが、ウェブアプリケーションのサーバ側へデータをアップロードするために問題となる。好適実施形態においては、ネットワークアクセス装置は常に電源が入っているので、ネットワークアクセス装置１３０がローカル装置である。変形形態においては、例えば、このようなネットワークアクセス装置１３０はオフロード機能をサポートしておらず、ローカル装置は、好ましくは上述のように常に電源が入っている種類のローカルネットワーク１４０の任意の種類の装置、例えば、ＮＡＳ１５０である。本発明は、ローカル装置１３０、１５０、または、より正確には、ローカル装置１３０、１５０上で実行しているウェブサービスを認証する解決法を提供することによって、ローカル装置に成り済ます攻撃者を避けて、ローカル装置に一時的に収容されているアップロードデータを攻撃者から保護する。

【００１８】

本発明の最も重要な発明的着想は、ウェブアプリケーションで用いるローカルウェブサービスをブラウザから検索し、そのローカルサービスを認証するということである。その方法を用いて、オフロードサービスを検索することができるが、ＤＬＮＡ／ＵＰＮＰリレーへのＷｅｂを検索する等の他のアプリケーションに対応していると好都合である。ＤＬＮＡ／ＵＰＮＰリレーへのＷｅｂでは、ウェブアプリケーションがＤＬＮＡ／ＵＰＮＰリレーへのウェブサービスを介してユーザの装置を制御する許可を得られる。

【００１９】

好適実施形態においては、方法は、ＪａｖａＳｃｒｉｐｔ言語によって実行されるよう適合される。従って、方法は、ウェブブラウザが提供した制約された実行環境に合致するように適合されると好都合である。これらの制約は、ブラウザが、悪意のコードの影響を非常に限られたものにするのを支援する。

【００２０】

さらに、ウェブサービスに安全にアクセスする方法は、サービスの存在と、そのアドレスの両方を動的に判定する。その機構は、再配置されたサービスの認証も担当する。その機構によって、サービスの存在に応じて、クライアント側においてウェブアプリケーションを動的に適合することができる。

【００２１】

図２は、本発明の第１の実施形態による安全なアクセス法のステップを示す。

【００２２】

ブラウザは、いわゆるブラウザネットワークＡＰＩで実施されるＸＭＬＨｔｔｐＲｅｑを用いてのみ、ネットワークにアクセスすることができる。ブラウザは、ＪａｖａＳｃｒｉｐｔマシンをさらに含む。ブラウザに存在する認証／証明機構は、ＴＬＳ／ＳＳＬ機構である。

【００２３】

図２には示していないが、予備段階においては、信頼できるオペレータが、ドメイン（

ｏｆｆｌｏａｄ．ｏｒｇ）を購入し、そのドメインのＳＳＬ証明書を要求する。サービスを実行する信頼できる各装置は、一意の名前（例えば、ａｆ３４ａ）と、その名前に対応する証明書（ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ）とを受信する。信頼できるオペレータは、（インターネットで利用可能な）ＤＮＳサービスを実行する。そのＤＮＳサービスは信頼できる装置によって更新できるので、名前ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇは常に、正しいローカルＩＰアドレスにマッピングされる。

【００２４】

検索／認証手順の第１のステップ２１０において、ローカルにホストされたウェブサービスにアクセスを試みるブラウザは、ネットワークの一般名（ｏｆｆｌｏａｄ．ｌｏｃａｌ）に要求を送信する。より正確には、ＪａｖａＳｃｒｉｐｔは、ブラウザネットワークＡＰＩを介して、任意のローカルネットワーク上のサービスを実行する任意の装置に共通な何らかの固定アドレス（ｏｆｆｌｏａｄ．ｌｏｃａｌ）にローカルクエリを出す。ゲートウェイに存在するＤＮＳは、ローカルＩＰアドレスでＤＮＳクエリに答え、ブラウザネットワークＡＰＩは、安全対策が施されていないＨＴＴＰプロトコルを用いて、このＩＰアドレス、すなわち、ウェブサービスをホストするローカル装置のＩＰアドレスに接続する。「ｏｆｆｌｏａｄ．ｌｏｃａｌ」という名前は何にも属さず、どの証明機関もその証明書を発行していないので、「ｏｆｆｌｏａｄ．ｌｏｃａｌ」の証明書を取得できないという問題がある。

【００２５】

従って、第２ステップ２２０において、ブラウザは、ローカル装置がホストし、かつ、ローカル装置のＩＰアドレスに関連付けられたウェブサービスの、グローバル名と呼ばれる完全修飾名（ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ）を取得する。しかしながら、既に説明したように、完全修飾名は破損しているかもしれない。

【００２６】

第３のステップ２３０において、ブラウザは、取得したグローバル名（ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ）は、何らかの信頼できるオペレータによって管理されていることを確認する。実際、何者かがｈａｃｋｅｒ．ｏｒｇに対して有効な証明書を有しているものの、これは、十分な条件ではない。さらなる要件は、証明書の所有者が信頼できることである。従って、ブラウザは、取得したグローバル名をホワイトリストで検証して、下位証明書（ｓｕｂ－ｃｅｒｔｉｆｉｃａｔｅ）（ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ）が信頼できるオペレータ（ｏｆｆｌｏａｄ．ｏｒｇ）からのものであることを確認する。ホワイトリストは、信頼できる各装置のグローバル名の包括的なリストではなく、グローバル名の検証に用いられるパターンマッチング方式を含めばよいことを、当業者は理解されよう。

【００２７】

最後のステップ２４０において、検証に成功すると、ブラウザは、グローバル名への安全なアクセスを求める要求を送信する。より正確には、ブラウザネットワークＡＰＩは、完全修飾名（ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ）に新しいクエリを行う。信頼できるオペレータによって運営されるＤＮＳは、ローカルＩＰアドレスで答える。ブラウザは、このローカルＩＰアドレスにＨＴＴＰＳで接続し、ブラウザの証明書のコレクションを用いて、グローバル名に関連付けられた証明書が、ブラウザが接続する装置に対応していることと、その証明書が有効で、取り消されていないこと、とを確認する。ステップ２４０でローカル装置が認証されていることが認められ、ステップ２３０でローカル装置が信頼できるオペレータによって承認されたものであることを認められると好都合である。

【００２８】

このようにして、ｈｔｔｐｓ：／／ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇで利用可能なウェブサービスは安全確実に用いられる。

【００２９】

何れかのステップで失敗するということは、そのサービスが利用できないこと、または、何らかの認証問題でそのサービスが信頼できないこと、を意味する。よって、そのサー

ビスは用いるべきではない。

【００３０】

図３は、本発明の好適実施形態による安全なアクセスのステップを示す。既に説明したように、好適実施形態においては、ウェブサービスは、アップロードをオフロードするためのウェブサービスである。

【００３１】

検索サービスは、固定のＵＲＬ、ｈｔｔｐ：／／ｏｆｆｌｏａｄ．ｌｏｃａｌ／ｔｅｓｔで利用可能である。分かり易いように、全ての記述においてポート番号を省略している。しかしながら、既存のサービスとのコンフリクトを避けるために、非標準のＨＴＴＰ／ＨＴＴＰＳポート（例えば、ＨＴＴＰ用の８７８７と、ＨＴＴＰＳ用の８７８８）を用いる。完全修飾名とポートは、固定で、全てのゲートウェイに共通である。結果として、ブラウザで実行しているウェブアプリケーションは、ＸＭＬＨｔｔｐＲｅｑｕｅｓｔのみを使用してネットワークにアクセスできるアプリケーションであるが、そのサービスにアクセスできる。ブラウザは、ゲートウェイのＩＰアドレスへの一般的な完全修飾名（ｏｆｆｌｏａｄ．ｌｏｃａｌ３００）を解決し、ゲートウェイに接続する。接続エラー（ＤＮＳ解決に失敗、接続タイムアウト４０４、４０３．．．）はどれも、サービスが利用できないことを示す。オフロードサービスが実行中で、オフロード要求を受け入れることができる場合、ブラウザは、答えとしてＯＫを受信する。

【００３２】

検索サービスは、ＬＡＮ上でサービスをサポートする装置のＩＰアドレスの固定の名前を解決するにあたって、ＤＮＳに大きく依存する。大抵のゲートウェイは、独自のＤＮＳサーバを実行しているので、それ自体で、ｏｆｆｌｏａｄ．ｌｏｃａｌとして登録することができる。オフロードサービスが別の装置によって提供される場合、この装置は、ＤＨＣＰプロトコルによって、ゲートウェイのＤＮＳに名前ｏｆｆｌｏａｄ．ｌｏｃａｌを登録することができる。ＤＮＳ解決は、ＤＨＣＰを用いてｏｆｆｌｏａｄ．ｌｏｃａｌに登録している同一ＬＡＮ上のものの影響を受けやすいので、ウェブ開発者は、解決によって（ブラウザのＳＳＬ証明書に従った）信頼できるゲートウェイにつながることを確実にしようとするであろう。この解決法は、ＨＴＴＰＳ認証機構に依存することである。この目的を達成するために、各ゲートウェイは、独自の自己署名証明書を有し、ユーザは、自分が信頼するゲートウェイからの証明書を、自分のブラウザの証明書リストに手動で追加する。要求は、ｈｔｔｐ：／／ｏｆｆｌｏａｄ．ｌｏｃａｌ／ではなく、ｈｔｔｐｓ：／／ｏｆｆｌｏａｄ．ｌｏｃａｌ／に送信される。ゲートウェイが信頼されない場合、検索サービスへの要求の結果は接続エラーとなる。よって、オフロードは有効化されない。しかしながら、このプロセスでは、ユーザは、自分のブラウザに適切な証明書を追加することによって、自分が使用する新しい各ゲートウェイを手動で承認する必要がある。このプロセスは、込み入ったものになり得るので、完全に透過的なユーザ体験を阻害する可能性がある。

【００３３】

このプロセスを途切れのないものにするために、好適実施形態による方法は、好都合にも、ゲートウェイの認証も担当する強化された検索方法を提供する。この方法は、信頼されたソフトウェアを実行し、コピーできない証明書を有する組み込み装置と共に用いられるように意図されている。図３は、検索および認証プロセス全体を示す。このプロセスは、上記で述べた認証されていない検索サービスを強化するものである。この場合、各ゲートウェイは、一意の名前（例えば、ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ３０１）に関連付けられており、また、信頼できる認証機関に署名された対応する証明書を有する。各ゲートウェイは、信頼できるドメインｏｆｆｌｏａｄ．ｏｒｇに対して実行している動的なＤＮＳサービス上に、そのゲートウェイのローカルＩＰアドレスを公表する。

【００３４】

プロセスは、ゲートウェイ検索し、そのゲートウェイを認証することにある。この目的のために、ｈｔｔｐ：／／ｏｆｆｌｏａｄ．ｌｏｃａｌ／ａｕｔｈへの要求を発する。こ

の要求は、ゲートウェイの一意の完全修飾名（例えば、ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ３０１）を返す。この完全修飾名をドメインのホワイトリストとマッチさせて、証明書は、適切な認証機関によって発行されたものであることを保証する。有効なＳＳＬドメイン（すなわち、ブラウザ証明書リストに従って証明された）の全てが、信頼できるゲートウェイにマッピングされている、というわけではない。ほんのわずかなドメイン（例えば、ｏｆｆｌｏａｄ．ｏｒｇ）が、この目的のために信頼され、ホワイトリストにリストされる。この時点まで、ゲートウェイは、信頼できず、取得された情報は、操作されているかもしれない。しかし、完全修飾名は、信頼できるゲートウェイの組にマッピングされる。次に、ｈｔｔｐｓ：／／ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ／ｔｅｓｔへの要求が出される。ブラウザは、ゲートウェイの証明書を確認して、乗っ取りを防止する。証明書が正当な場合、オフロード機構を有効化することができ、要求を、ｈｔｔｐｓ：／／ａｆ３４ａ．ｏｆｆｌｏａｄ．ｏｒｇ／ｕｐｌｏａｄ／にポストすることができる。

【００３５】

ここでも、基本的な検索プロセスにおいてと同様に、いかなるエラーも、オフロード機構を有効化できないことを意味する。各装置は、独自の証明書を持っているので、証明書が盗まれた場合、または、装置のサブセットでセキュリティ問題が発見された場合、個々の証明書を無効にすることができる。攻撃者が、ＤＮＳエントリを改ざんして検索サービスを中断させることに成功したとしても、ウェブアプリケーションは、単に、オフロード機能のない通常サービスに戻るだけで、オフロードがアクティブでないことを除いては、ユーザへのサービスに影響はない。

【００３６】

方法は、特別な機器を必要とすることなく容易に実施することができるので、ＰＣ、携帯電話、ホームネットワークのゲートウェイなど、「普通の」ユーザ装置で実施されてよいことを、当業者は理解されよう。本発明は、８０２．１１通信（Ｗｉ－Ｆｉ）、または、Ｂｌｕｅｔｏｏｔｈ(登録商標)もしくはＵＷＢなどの任意の有線もしくは無線アクセスにさらに対応している。本発明は、好都合なことに、無線ネットワークのホットスポットに配置されたウェブサービスに対応している。

【００３７】

図４は、本発明の好適実施形態による例示的なユーザ装置を示す。ユーザ装置４００は、ブラウザまたはウェブブラウザと呼ばれるソフトウェアモジュールを含む。ブラウザは、ネットワークを介してウェブサービスに安全にアクセスしようとするウェブアプリケーションを実行する。異なる変形形態によると、ユーザ装置は、コンピュータ、携帯装置、タブレットで実施されてよい。

【００３８】

ユーザ装置４００は、８０２．１１無線カードなどのネットワークインタフェース４１０と、少なくとも１つのプロセッサ４２０（以下「プロセッサ」と呼ぶ）と、メモリ４３０と、を含む。ネットワークインタフェース４１０は、ユーザ装置をネットワークに接続するように適合され、従って、ユーザ装置をローカル装置に接続するように適合される。ネットワークインタフェース４１０は、例えば、遠隔ウェブサービスへのアクセスを求める要求を物理的に送信し、その要求への応答を物理的に受信する。変形形態においては、ネットワークインタフェース４１０は、Ｅｔｈｅｒｎｅｔ(登録商標)等の有線のインタフェースである。プロセッサ４２０は、ウェブブラウザと呼ばれるソフトウェアモジュールを実施する命令を実行するよう適合される。ウェブブラウザは、ウェブアプリケーションを実行するよう適合される。本発明の理解に必要な特徴のみを以下に記載する。ウェブアプリケーションは、ウェブサービスをホストする任意の装置を識別する一般名を指定することにより、ウェブサービスへのアクセスの要求を、ネットワークインタフェース４１０を介して送信する。ウェブアプリケーションは、ネットワークインタフェース４１０を介して要求への応答を受信する。応答は、ウェブサービスをホストするローカル装置を一意に識別し、かつ、ユーザ装置が安全にアクセスできるグローバル名を含む。ウェブアプリケーションは、ウェブサービスをホストする信頼できる装置のグローバル名を含むリスト

に、受信したグローバル名が含まれていることを検証する。リストはメモリ４３０に記憶されると好都合である。ウェブアプリケーションが、グローバル名を指定することによって、ネットワークインタフェース４１０を介してローカル装置への接続を確立すると、ブラウザは、そのローカル装置のグローバル名に関連付けられた、受信した証明書を検証する。このようにして、ウェブアプリケーションは、ウェブサービスに安全にアクセスする。変形態様においては、安全機能は、安全なプロセッサ等のハードウェアの一部で実施される。

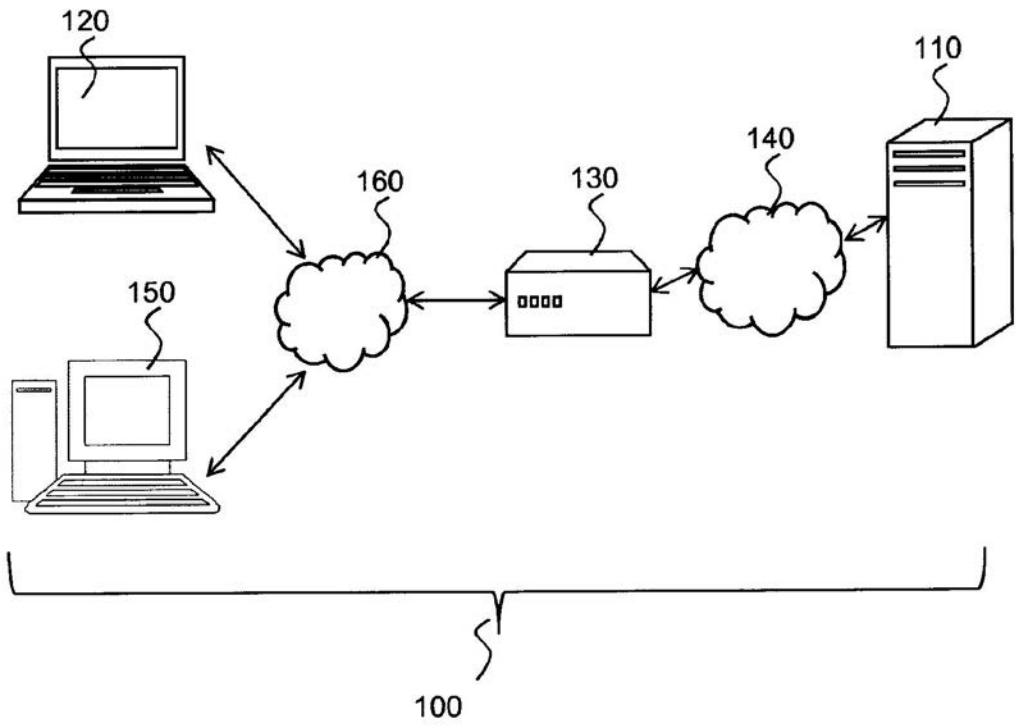
【００３９】

記載は、ウェブアプリケーションへのアップロードに集中しているが、本発明は、ウェブサービスがローカルで提供される機構に対応している。

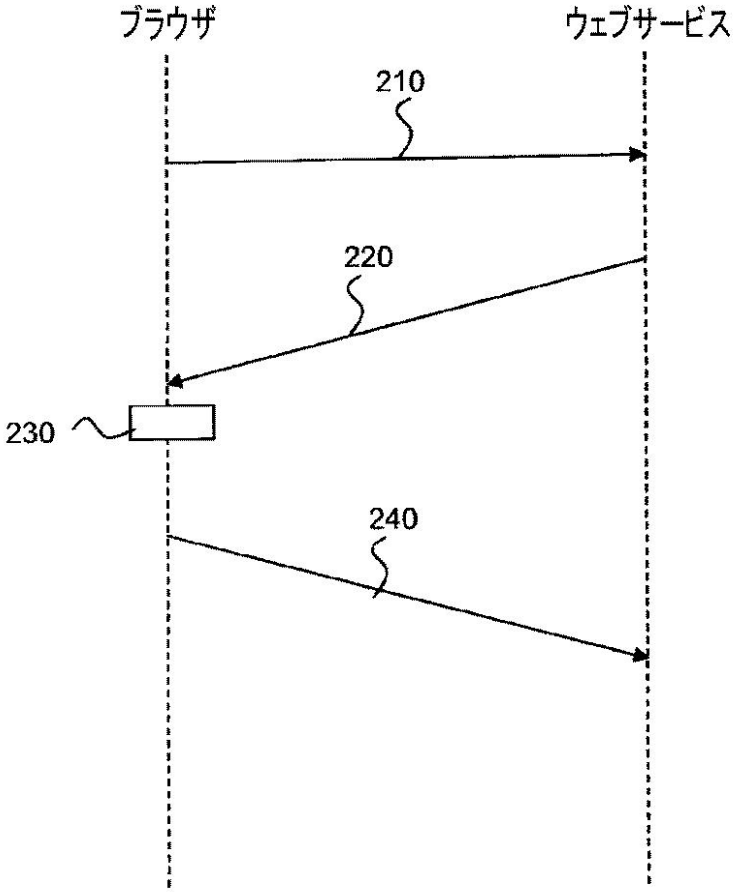
【００４０】

明細書、（必要に応じて）請求項、および、図面で開示した各特徴は、個別で、または、任意の適切な組み合わせで提供してよい。ソフトウェアで実施されているとして記載した特徴は、ハードウェアで実施してもよく、逆もまた同様である。請求項で用いられる参照番号は、例証のためであり、請求項の範囲に制限を課すものではない。

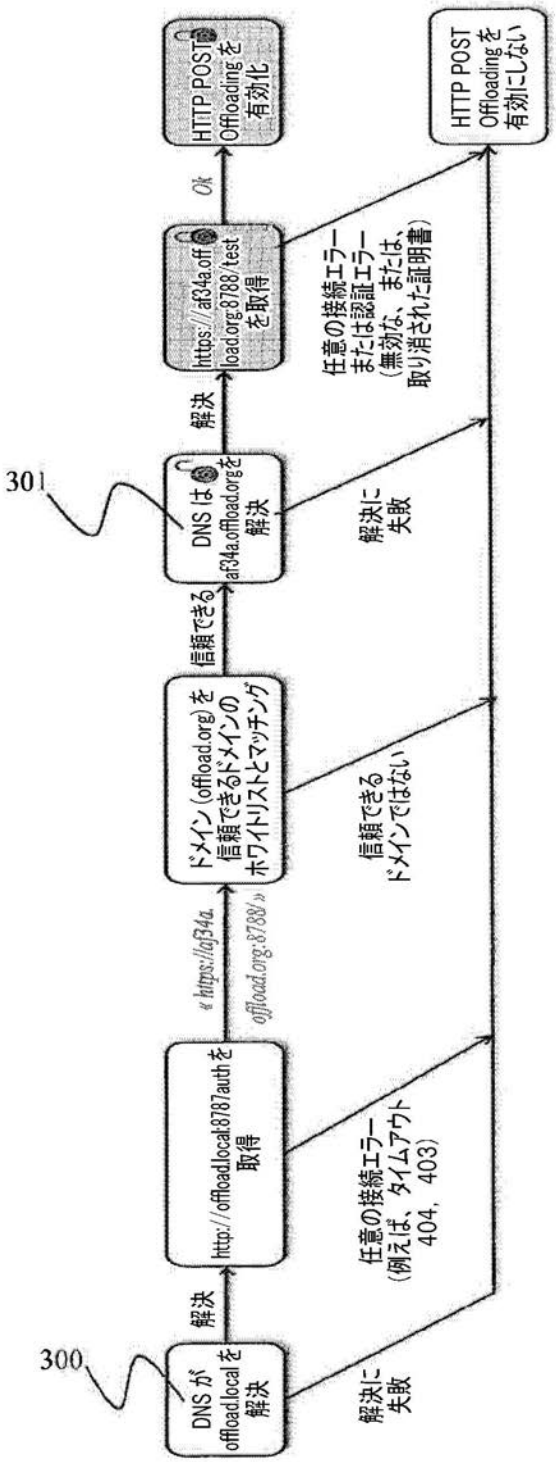
【図１】



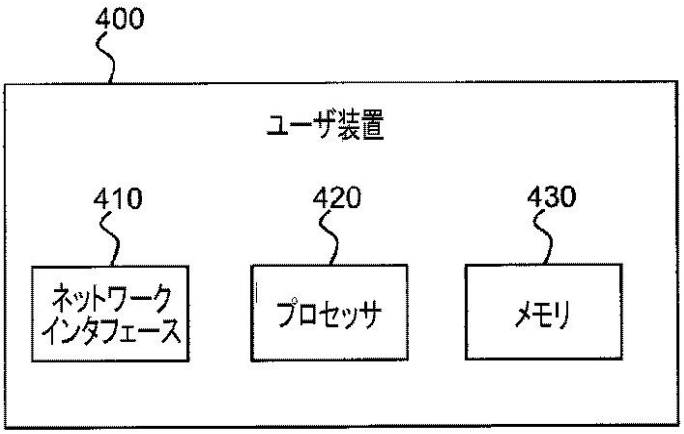
【図２】



【図３】


300
DNS が offload.local を解決
解決
http://offload.local:8787/auth を取得
« https://af34a.
offload.org:8787/ »
ドメイン（offload.org）を信頼できるドメインのホワイトリストとマッチング
信頼できる
301
DNS は af34a.offload.org を解決
解決
https://af34a.offload.org:8787/test を取得
Ok
HTTP POST Offloading を有効化
解決に失敗
任意の接続エラー（例えば、タイムアウト 404、403）
信頼できるドメインではない
解決に失敗
任意の接続エラーまたは認証エラー（無効な、または、取り消された証明書）
HTTP POST Offloading を有効にしない

【図４】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/069178

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08 H04L29/06 H04W28/08 H04W36/22
ADD. H04W88/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2011/098660 A1 (NOTAVA OY [FI]; LAPPETELAEINEN ANTTI [FI]; TUUPOLA JUHA-MATTI [FI]; ER) 18 August 2011 (2011-08-18) paragraph [0004] page 6, line 20 - line 23 page 7, line 8 - line 18 page 8, line 43 - line 46 page 11, line 36 - line 41 figures 2,7	1-12
A	US 7 181 506 B1 (VIGUE CHARLES L [US] ET AL) 20 February 2007 (2007-02-20) column 2, line 24 - line 39 page 11, lines 9-19,42-62 figures 1,9	1-12

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 January 2014	06/02/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pajatakis, Emmanouil

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/069178

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2011098660 A1	18-08-2011	CN 102783218 A	14-11-2012
		EP 2534889 A1	19-12-2012
		US 2013042316 A1	14-02-2013
		WO 2011098660 A1	18-08-2011
US 7181506 B1	20-02-2007	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ

（特許庁注：以下のものは登録商標）
１．ＤＬＮＡ

(72)発明者 ニコラス ル スコウアルネック
フランス ３５ ５７６ セソン セヴィニェ シーエス １７６ １６ ゼットエーシー デ シャン ブラン アベニュー デ シャン ブラン ９７５ テクニカラー アールアンドディー フランス内
(72)発明者 エルワン ル メレル
フランス ３５ ５７６ セソン セヴィニェ シーエス １７６ １６ ゼットエーシー デ シャン ブラン アベニュー デ シャン ブラン ９７５ テクニカラー アールアンドディー フランス内
(72)発明者 ギレス シュトラウブ
フランス ３５ ５７６ セソン セヴィニェ シーエス １７６ １６ ゼットエーシー デ シャン ブラン アベニュー デ シャン ブラン ９７５ テクニカラー アールアンドディー フランス内

Ｆターム(参考) 5B084 AA01 AA12 AA22 AB26 AB36 BB16 DA12 DB02 DC02 DC03

【要約の続き】
明書を検証するステップと、ウェブサービスに安全にアクセスするステップ、とをさらに含む。一般名は、任意のローカル装置がアクセス可能な名前、すなわち、ウェブサービスをホストする全ての装置に共通の名前である。リストは、ウェブサービスをホストする信頼できる装置のグローバル名を含む。