

(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2009-514262

(P2009-514262A)

(43) 公表日 平成21年4月2日(2009.4.2)

(51) Int.Cl. F I テーマコード (参考)
HO4L 9/32 (2006.01) HO4L 9/00 675B 5J104

審査請求 有 予備審査請求 有 (全 32 頁)

| | | | |
|---------------|------------------------------|----------|---|
| (21) 出願番号 | 特願2006-519925 (P2006-519925) | (71) 出願人 | 390009531 インターナショナル・ビジネス・マシーンズ・コーポレーション INTERNATIONAL BUSINESS MACHINES CORPORATION アメリカ合衆国10504 ニューヨーク州 アーモンク ニュー オーチャードロード |
| (86) (22) 出願日 | 平成16年7月9日 (2004.7.9) | (74) 代理人 | 100086243 弁理士 坂口 博 |
| (85) 翻訳文提出日 | 平成18年3月13日 (2006.3.13) | (74) 代理人 | 100091568 弁理士 市位 嘉宏 |
| (86) 国際出願番号 | PCT/EP2004/051435 | (74) 代理人 | 100108501 弁理士 上野 剛史 |
| (87) 国際公開番号 | W02005/015872 | | |
| (87) 国際公開日 | 平成17年2月17日 (2005.2.17) | | |
| (31) 優先権主張番号 | 10/621, 927 | | |
| (32) 優先日 | 平成15年7月17日 (2003.7.17) | | |
| (33) 優先権主張国 | 米国 (US) | | |

最終頁に続く

(54) 【発明の名称】 既存のSSLセッションを中断することなく証明書ベースの認証にステップアップするための方法及びシステム

(57) 【要約】

【課題】 以前に確立されたSSLセッションを終了又は再折衝することなく、非証明書ベースの認証手続きから証明書ベースの認証手続きにステップアップすることが可能な方法及びシステムを提供する。

【解決手段】

認証操作を実行するための方法が提示される。クライアントがサーバからのリソースを要求したときに、該サーバと該クライアントとの間のSSL(Secure Sockets Layer)セッションを介して、非証明書ベースの認証操作が実行される。クライアントが別のリソースを要求したときに、サーバは、より制限されたレベルの認証にステップアップすることを決定し、証明書ベースの認証操作が、該証明書ベースの認証操作の完了前にSSLセッションを終了又は再折衝することなく該SSLセッションを介して実行される。証明書ベースの認証手続きの間に、実行可能モジュールがSSLセッションを介してサーバからクライアントにダウンロードされ、その後、該サーバは、該クライアントでデジタル証明書を用いて該実行可能モジュールによって生成されたデジタル署名を、該SSLセッションを介して受信する。サーバにおけるデジタル署名の検証の成功に回答して、該サーバは、要求されたリソースへのアクセスを提供する。

【選択図】 図6

【特許請求の範囲】**【請求項 1】**

認証操作を実行するための方法であって、

サーバとクライアントとの間のSSL (Secure Sockets Layer) セッションを介して非証明書ベースの認証操作を実行するステップと、

前記非証明書ベースの認証操作を実行した後で、証明書ベースの認証操作を、前記証明書ベースの認証操作の完了前に前記SSLセッションを終了又は再折衝することなく前記サーバと前記クライアントとの間の前記SSLセッションを介して実行するステップと、を含む方法。

【請求項 2】

前記SSLセッションの折衝が、クライアントからの第1のデジタル証明書を用い、前記証明書ベースの認証操作が、前記クライアントからの第2のデジタル証明書を用い、前記第1のデジタル証明書と前記第2のデジタル証明書とは同一ではない、請求項1に記載の方法。

【請求項 3】

前記非証明書ベースの認証操作に関連するサーバによって、第1のリソースへのアクセスをクライアントに提供するステップをさらに含む、請求項1又は請求項2に記載の方法。

【請求項 4】

前記第1のリソースへのアクセスを提供するステップが、
前記クライアントからの第1のリソース要求を前記サーバで受信するステップと、
前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL (Secure Sockets Layer) セッションを確立するステップと、

前記SSLセッションを介して前記サーバと前記クライアントとの間で前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信するステップと、を含む、請求項3に記載の方法。

【請求項 5】

前記証明書ベースの認証操作に関連するサーバによって、第2のリソースへのアクセスをクライアントに提供するステップをさらに含む、請求項1から請求項4までのいずれか1つの請求項に記載の方法。

【請求項 6】

前記第2のリソースへのアクセスを提供するステップが、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信するステップと、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードするステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記サーバで受信するステップと、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信するステップと、を含む、請求項5に記載の方法。

【請求項 7】

前記第2のリソースへのアクセスを提供するステップが、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信するステップと、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応

10

20

30

40

50

答して、前記SSLセッションを介して前記サーバによって前記クライアントにおけるダウンロード可能ソフトウェア・モジュールの実行を開始させるステップと、

前記クライアントにおいてデジタル証明書を用いて前記ダウンロード可能ソフトウェア・モジュールの実行によって生成されたデジタル署名を、前記サーバで受信するステップと、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース要求を送信するステップと、

を含む、請求項5に記載の方法。

【請求項8】

前記証明書ベースの認証操作に関連して、クライアントがサーバにおける第2のリソースへのアクセスを取得するステップをさらに含む、請求項1から請求項7までのいずれか1つの請求項に記載の方法。

10

【請求項9】

前記第2のリソースへのアクセスを取得するステップが、

前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信するステップと、

証明書ベースの認証操作を行うための機能を備える実行可能モジュールを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信するステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信するステップと、

20

前記サーバからの第2のリソース応答を前記クライアントで受信するステップと、を含む、請求項8に記載の方法。

【請求項10】

前記第2のリソースへのアクセスを取得するステップが、

前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信するステップと、

関連するコンテンツ・タイプ標識を伴うコンテンツを有する応答メッセージを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信するステップと、

30

前記コンテンツのコンテンツ・タイプを決定したことに応答して、前記クライアントにおいてダウンロード可能ソフトウェア・モジュールを実行するステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信するステップと、

前記サーバからの第2のリソース応答を前記クライアントで受信するステップと、を含む、請求項8に記載の方法。

【請求項11】

認証操作を実行するための装置であって、

サーバとクライアントとの間のSSL(Secure Sockets Layer)セッションを介して非証明書ベースの認証操作を実行する手段と、

40

前記非証明書ベースの認証操作を実行した後で、証明書ベースの認証操作を、前記証明書ベースの認証操作の完了前に前記SSLセッションを終了又は再折衝することなく前記サーバと前記クライアントとの間の前記SSLセッションを介して実行する手段と、を備える装置。

【請求項12】

前記SSLセッションの折衝が、クライアントからの第1のデジタル証明書を用い、前記証明書ベースの認証操作が、前記クライアントからの第2のデジタル証明書を用い、前記第1のデジタル証明書と前記第2のデジタル証明書とは同一ではない、請求項11に記載の装置。

50

【請求項 13】

前記非証明書ベースの認証操作に関連するサーバによって、第1のリソースへのアクセスをクライアントに提供する手段をさらに備える、請求項11又は請求項12に記載の装置。

【請求項 14】

前記第1のリソースへのアクセスを提供する手段が、
前記クライアントからの第1のリソース要求を前記サーバで受信する手段と、
前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立する手段と、

10

前記SSLセッションを介して前記サーバと前記クライアントとの間で前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、
を備える、請求項13に記載の装置。

【請求項 15】

前記証明書ベースの認証操作に関連するサーバによって、第2のリソースへのアクセスをクライアントに提供する手段をさらに備える、請求項11から請求項14までのいずれか1つの請求項に記載の装置。

【請求項 16】

20

前記第2のリソースへのアクセスを提供する手段が、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信する手段と、
を備える、請求項15に記載の装置。

30

【請求項 17】

前記第2のリソースへのアクセスを提供する手段が、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバによって前記クライアントにおけるダウンロード可能ソフトウェア・モジュールの実行を開始させる手段と、

前記クライアントにおいてデジタル証明書を用いて前記ダウンロード可能ソフトウェア・モジュールの実行によって生成されたデジタル署名を、前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース要求を送信する手段と、
を備える、請求項15に記載の装置。

40

【請求項 18】

前記証明書ベースの認証操作に関連して、クライアントがサーバにおける第2のリソースへのアクセスを取得する手段をさらに備える、請求項11から請求項17までのいずれか1つの請求項に記載の装置。

【請求項 19】

前記第2のリソースへのアクセスを取得する手段が、
前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要

50

求を送信する手段と、

証明書ベースの認証操作を行うための機能を備える実行可能モジュールを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信する手段と、

前記サーバからの第2のリソース応答を前記クライアントで受信する手段と、

を備える、請求項18に記載の装置。

【請求項20】

前記第2のリソースへのアクセスを取得する手段が、

前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信する手段と、

関連するコンテンツ・タイプ標識を伴うコンテンツを有する応答メッセージを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信する手段と、

前記コンテンツのコンテンツ・タイプを決定したことに応答して、前記クライアントにおいてダウンロード可能ソフトウェア・モジュールを実行する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信する手段と、

前記サーバからの第2のリソース応答を前記クライアントで受信する手段と、
を備える、請求項18に記載の装置。

【請求項21】

データ処理システムにおいて用いるコンピュータ可読媒体内の、認証操作を実行するためのコンピュータ・プログラムであって、

サーバとクライアントの間のSSL(Secure Sockets Layer)セッションを介し、非証明書ベースの認証操作を実行する手段と、

前記非証明書ベースの認証操作を実行した後で、証明書ベースの認証操作の完了に先立つSSLセッションを終了又は再折衝することなく、サーバとクライアントの間のSSLセッションを介し、前記証明書ベースの認証操作を実行する手段と、

を含むコンピュータ・プログラム。

【請求項22】

前記SSLセッションの折衝が、クライアントからの第1のデジタル証明書を用い、前記証明書ベースの認証操作が、前記クライアントからの第2のデジタル証明書を用い、前記第1のデジタル証明書と前記第2のデジタル証明書とは同一ではない、請求項21に記載のコンピュータ・プログラム。

【請求項23】

前記非証明書ベースの認証操作に関連するサーバによって、第1のリソースへのアクセスをクライアントに提供する手段をさらに含む、請求項21又は請求項22に記載のコンピュータ・プログラム。

【請求項24】

前記第1のリソースへのアクセスを提供する手段が、

前記クライアントからの第1のリソース要求を前記サーバで受信する手段と、

前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立する手段と、

前記SSLセッションを介して前記サーバと前記クライアントとの間で前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、

を含む、請求項23に記載のコンピュータ・プログラム。

【請求項25】

前記証明書ベースの認証操作に関連するサーバによって、第2のリソースへのアクセス

10

20

30

40

50

をクライアントに提供する手段をさらに含む、請求項 2 1 から請求項 2 4 までのいずれか 1 つの請求項に記載のコンピュータ・プログラム。

【請求項 2 6】

前記第 2 のリソースへのアクセスを提供する手段が、
前記クライアントからの第 2 のリソース要求を、前記 SSL セッションを介して前記サーバで受信する手段と、

前記第 2 のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記 SSL セッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第 2 のリソース応答を送信する手段と、

を含む、請求項 2 5 に記載のコンピュータ・プログラム。

10

【請求項 2 7】

前記第 2 のリソースへのアクセスを提供する手段が、

前記クライアントからの第 2 のリソース要求を、前記 SSL セッションを介して前記サーバで受信する手段と、

前記第 2 のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記 SSL セッションを介して前記サーバによって前記クライアントにおけるダウンロード可能ソフトウェア・モジュールの実行を開始させる手段と、

20

前記クライアントにおいてデジタル証明書を用いて前記ダウンロード可能ソフトウェア・モジュールの実行によって生成されたデジタル署名を、前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第 2 のリソース要求を送信する手段と、

を含む、請求項 2 5 に記載のコンピュータ・プログラム。

【請求項 2 8】

前記証明書ベースの認証操作に関連して、クライアントがサーバにおける第 2 のリソースへのアクセスを取得する手段をさらに含む、請求項 2 1 から請求項 2 7 までのいずれか 1 つの請求項に記載のコンピュータ・プログラム。

30

【請求項 2 9】

前記第 2 のリソースへのアクセスを取得する手段が、

前記 SSL セッションを介して、前記クライアントから前記サーバに第 2 のリソース要求を送信する手段と、

証明書ベースの認証操作を行うための機能を備える実行可能モジュールを、前記クライアントにおいて、前記 SSL セッションを介して前記サーバから受信する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記 SSL セッションを介して前記サーバに送信する手段と、

前記サーバからの第 2 のリソース応答を前記クライアントで受信する手段と、

を含む、請求項 2 8 に記載のコンピュータ・プログラム。

40

【請求項 3 0】

前記第 2 のリソースへのアクセスを取得する手段が、

前記 SSL セッションを介して、前記クライアントから前記サーバに第 2 のリソース要求を送信する手段と、

関連するコンテンツ・タイプ標識を伴うコンテンツを有する応答メッセージを、前記クライアントにおいて、前記 SSL セッションを介して前記サーバから受信する手段と、

前記コンテンツのコンテンツ・タイプを決定したことに応答して、前記クライアントにおいてダウンロード可能ソフトウェア・モジュールを実行する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記 SSL セッションを介して前記サーバに送信する手段と、

50

前記サーバからの第2のリソース応答を前記クライアントで受信する手段と、
を含む、請求項28に記載のコンピュータ・プログラム。

【請求項31】

認証操作を実行するための方法であって、
クライアントからの第1のリソース要求をサーバで受信するステップと、
前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL (Secure Sockets Layer) セッションを確立するステップと、
前記SSLセッションを介して非証明書ベースの認証操作を実行するステップと、
前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信するステップと、
前記非証明書ベースの認証操作を実行した後で、前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信するステップと、
前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードするステップと、
前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバで受信するステップと、
前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信するステップと、
を含む方法。

10

20

【請求項32】

認証操作を実行するための装置であって、
クライアントからの第1のリソース要求をサーバで受信する手段と、
前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL (Secure Sockets Layer) セッションを確立する手段と、
前記SSLセッションを介して非証明書ベースの認証操作を実行する手段と、
前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、
前記非証明書ベースの認証操作を実行した後で、前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、
前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、
前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバで受信する手段と、
前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信する手段と、
を備える装置。

30

40

【請求項33】

データ処理システムにおいて用いるコンピュータ可読媒体内の、認証操作を実行するためのコンピュータ・プログラムであって、
クライアントからの第1のリソース要求をサーバで受信する手段と、
前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL (Secure Sockets Layer) セッションを確立する手段

50

と、

前記SSLセッションを介して非証明書ベースの認証操作を実行する手段と、

前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、

前記非証明書ベースの認証操作を実行した後で、前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信する手段と、

を含むコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、改良されたデータ処理システムに関し、具体的には、マルチコンピュータ・データ転送のための方法及び装置に関する。さらにより具体的には、本発明は、暗号を用いるマルチコンピュータ通信のための方法及び装置を提供する。

【背景技術】

【0002】

eコマース・ウェブ・サイト及びウェブ・アプリケーションは、ユーザに代わって、コンピュータ・ネットワーク上で取引を実行する。ユーザは、多くの場合、セキュリティの目的で、適切なレベルまで自分の身元を確実に証明するために、認証手続きを通過しなければならない。

【0003】

多くのコンピュータ・システムは、異なるセキュリティのレベルに合わせて異なるタイプの認証を有する。例えば、正しいユーザ名とパスワードとの組み合わせがユーザによって与えられる第1レベルの認証の完了に成功した後で、システムは、ウェブ・サイト上のリソースの特定の組へのアクセスを提供することができる。第2レベルの認証が、例えばスマートカードのようなハードウェア・トークンを提示することをユーザに対して求める場合があり、その後そのユーザには、より厳しく管理されたウェブ・サイト上のリソースへのアクセスが提供される。第3レベルの認証が、例えば指紋走査又は虹彩走査を通じて何らかの形式のバイオメトリック・データを提供することをユーザに対して求める場合があり、その後そのシステムは、ウェブ・サイト上の極めて重要なリソースまたは機密リソースへのアクセスを提供する。

【0004】

ある認証レベルから次のレベルに移行する処理は、「ステップアップ認証」と呼ばれる。すなわち、ユーザは、より重要なリソースへのアクセスを得るために、システムの要求に応じて、あるレベルの認証から上位レベルにステップアップする。

【0005】

eコマース・ウェブ・ベースの環境においては、コンピュータ・システムは、ウェブ・サイトにアクセスするための正面玄関すなわち監視ゲート(sentry gate)として、認証サービスを実装することが多い。これらの認証サービスは、ユーザがいずれかのリソースにアクセスする前に認証されることを確実にするように、アプリケーションの前、すなわちユーザとアプリケーションとの間に位置する。これらの認証サービスは、ウェブ・サーバ・プラグイン、リバース・プロキシ、又は他の同様な技術として実装することができる。これらの認証サービスに伴う潜在的な問題は、これらの認証サービスはユーザ名/パスワード認証を用いることが多く、クライアント・ベースの証明書を用いる認証

10

20

30

40

50

方法にステップアップすることができないという点である。証明書ベースの認証手続きは、一般に、ユーザ名/パスワードベースの認証手続きより上位レベルのセキュリティを達成すると考えられている。

【0006】

証明書ベースの認証は、公開鍵/秘密鍵からなる非対称暗号鍵対の使用を含むものである。デジタル証明書は、認証されたユーザの識別情報を公開暗号鍵と結びつける。証明書ベースの認証手続きの際、ユーザは、自分自身のデジタル証明書を認証サービスに提供し、自らが公開鍵に対応する秘密暗号鍵にアクセスできることを証明する必要がある。例えば、認証サービスは、何らかの形式のチャレンジ・データをユーザのクライアント・コンピュータに与え、次いでユーザのクライアント・コンピュータは、ユーザの秘密暗号鍵を用いてチャレンジ・データに署名し、認証サービスは、ユーザの公開鍵を用いてデジタル署名を検証することができる。秘密鍵は、識別情報が証明書に格納されたユーザによって常に秘密に保たれているはずであるため、認証サービスが、チャレンジ・データがユーザの秘密鍵を用いて適切に署名されたと判断したときは、該認証サービスは、ユーザの識別情報を高いレベルまで検証したことになる。

10

【発明の開示】

【発明が解決しようとする課題】

【0007】

証明書ベースの認証手続きにステップアップする操作は、不可能であることが多い。問題は、典型的には、相互認証されたSSLセッションが、ユーザ名/パスワードの組み合わせといった下位レベルの非証明書ベースの認証についてクライアントとサーバとの間にすでに確立されていることから生じる。ほとんどの市販製品の場合、例えばSSLスタックが何らかの方法でオペレーティング・システムに組み込まれている場合など、証明書ベースの認証手続きを必要とする認証サービスがSSLスタックを制御しない場合には、該認証サービスは、新たなSSLセッションを強制的に確立することができない。したがって、認証サービスは、アクティブなSSLセッション上ですでに行われたユーザ名/パスワードをベースとする認証手続きから、そのアクティブなSSLセッションを維持したまま証明書ベースの認証手続きにステップアップすることができない。

20

【0008】

したがって、何らかの目的で認証サービスによって要求される上位レベルのセキュリティを獲得するために、以前に確立されたSSLセッションを終了又は再折衝することなく、非証明書ベースの認証手続きから証明書ベースの認証手続きにステップアップすることが可能な方法及びシステムを有することは有益であろう。

30

【課題を解決するための手段】

【0009】

認証操作を実行するための方法が提示される。クライアントがサーバからのリソースを要求したときに、該サーバと該クライアントとの間のSSL(Secure Sockets Layer)セッションを介して、非証明書ベースの認証操作が実行される。クライアントが別のリソースを要求したときに、サーバは、より制限されたレベルの認証にステップアップすることを決定し、証明書ベースの認証操作が、該証明書ベースの認証操作の完了前にSSLセッションを終了又は再折衝することなく該SSLセッションを介して実行される。証明書ベースの認証手続きの間に、実行可能モジュールがSSLセッションを介してサーバからクライアントにダウンロードされ、その後、該サーバは、該クライアントにおいてデジタル証明書を用いて該実行可能モジュールによって生成されたデジタル署名を、該SSLセッションを介して受信する。サーバにおけるデジタル署名の検証の成功に応答して、該サーバは、要求されたリソースへのアクセスを提供する。

40

【発明を実施するための最良の形態】

【0010】

本発明の特性と考えられる新規な特徴は、特許請求の範囲に記載される。発明自体、更なる目的、及びその利点は、添付の図面を参照して読んだ時に、以下の詳細な説明を参照

50

することによって最も良く理解されるであろう。

【0011】

一般に、本発明が備えるか又は本発明に関連する装置は、様々なデータ処理技術を含む。したがって、本発明をより詳細に説明する前に、背景技術として、分散データ処理システム内のハードウェア・コンポーネント及びソフトウェア・コンポーネントの典型的な構成を説明する。

【0012】

ここで図を参照すると、図1は、各々が本発明の一部を実装することができるデータ処理システムの典型的なネットワークを示す。分散データ処理システム100はネットワーク101を含み、ネットワーク101は、分散データ処理システム100内で相互に接続された種々の装置及びコンピュータ間に通信リンクを提供するために用いることができる媒体である。ネットワーク101は、電線又は光ファイバ・ケーブルなどの永久的な接続、又は、電話回線若しくは無線通信を通じて形成される一時的な接続を含むことができる。図示された例においては、サーバ102及びサーバ103は、ストレージ・ユニット104と共にネットワーク101に接続される。さらに、クライアント105～107もまた、ネットワーク101に接続される。クライアント105～107及びサーバ102～103は、メインフレーム、パーソナル・コンピュータ、携帯情報端末(PDA)などといった種々のコンピューティング装置によって表すことができる。分散データ処理システム100は、図示されていない付加的なサーバ、クライアント、ルータ、他の装置、及びピアツーピア・アーキテクチャを含むことができる。

10

20

【0013】

図示された例においては、分散データ処理システム100は、Lightweight Directory Access Protocol(LDAP)、Transport Control Protocol/Internet Protocol(TCP/IP)、Hypertext Transport Protocol(HTTP)、Wireless Application Protocol(WAP)などといった、相互に通信するための種々のプロトコルを用いるネットワーク及びゲートウェイの世界規模の集合体を表すネットワーク101を有するインターネットを含むことができる。当然のことながら、分散データ処理システム100は、例えば、イントラネット、ローカル・エリア・ネットワーク(LAN)、又は広域エリア・ネットワーク(WAN)などの、多くの異なるタイプのネットワークを含むこともできる。例えば、サーバ102は、クライアント109と、無線通信リンクを組み込んだネットワーク110とを直接サポートする。ネットワーク対応電話111は、無線リンク112を介してネットワーク110に接続し、PDA113は、無線リンク114を介してネットワーク110に接続する。電話111及びPDA113はまた、Bluetooth(商標)無線技術などの適切な技術を用いる無線リンク115を介して互いの間で直接データを転送し、いわゆるパーソナル・エリア・ネットワーク(PAN)又はパーソナル・アドホック・ネットワークを形成することができる。同様の方法で、PDA113は、無線通信リンク116を介してPDA107にデータを転送することができる。

30

40

【0014】

本発明は、種々のハードウェア・プラットフォーム上に実装することができる、すなわち、図1は、異種コンピューティング環境の一例であり、本発明についてのアーキテクチャ上の制限として意図するものではない。

【0015】

ここで図2を参照すると、図は、図1において示されるシステムのような、本発明を実装することができるデータ処理システムの典型的なコンピュータ・アーキテクチャを示す。データ処理システム120は、内部システム・バス123に接続された1つ又は複数の中央演算処理装置(CPU)122を含み、内部システム・バス123は、ランダム・アクセス・メモリ(RAM)124と、読み取り専用メモリ126と、プリンタ130、ディスク・ユニット132、又は音声出力システムなどのような図示されない他の装置とい

50

った種々のI/O装置をサポートする入力/出力アダプタ128とを、相互接続する。システム・バス123はまた、通信リンク136へのアクセスを提供する通信アダプタ134を接続する。ユーザ・インターフェース・アダプタ148は、キーボード140及びマウス142、又はタッチ・スクリーン、スタイラス、マイクロフォンなどのような図示されない他の装置といった種々のユーザ装置を接続する。ディスプレイ・アダプタ144は、システム・バス123をディスプレイ装置146に接続する。

【0016】

当業者であれば、図2のハードウェアは、システム実装に応じて変えることができることが分かるであろう。例えば、システムは、Intel(商標)Pentium(商標)ベースのプロセッサ及びデジタル信号プロセッサ(DSP)などの1つ又は複数のプロセッサと、1つ又は複数のタイプの揮発性メモリ及び不揮発性メモリとを有するものとすることができる。図2に示されるハードウェアに加えて、又はこれに代えて、他の周辺装置を用いることができる。図示された例は、本発明に関してアーキテクチャ上の制限を意味することを意図するものではない。

10

【0017】

本発明は、種々のハードウェア・プラットフォーム上に実装することができることに加えて、種々のソフトウェア環境において実装することができる。典型的なオペレーティング・システムを用いて、各々のデータ処理システム内のプログラム実行を制御することができる。例えば、1つのデバイスがUnix(商標)オペレーティング・システムを動作させることができる一方で、別のデバイスは、単純なJava(商標)ランタイム環境を含む。代表的なコンピュータ・プラットフォームは、画像ファイル、ワード・プロセッシング・ファイル、Extensible Markup Language(XML)、Hypertext Markup Language(HTML)、Handheld Device Markup Language(HDML)、Wireless Markup Language(WML)などの様々なフォーマット、並びに、他の様々なフォーマット及びファイル・タイプを持つハイパーテキスト文書にアクセスするための周知のソフトウェア・アプリケーションであるブラウザを含むことができる。

20

【0018】

本発明は、図1及び図2に関して上述したように、種々のハードウェア・プラットフォーム及びソフトウェア・プラットフォーム上に実装することができる。しかしながら、本発明は、より特定のには、改良された認証サービスに向けられる。改良された認証サービスをより詳細に説明する前に、典型的な認証サービスを説明する。

30

【0019】

本明細書における図の説明は、クライアント装置又は該クライアント装置のユーザによる特定の動作を伴う。当業者であれば、クライアントとの間の応答及び/又は要求は、時にはユーザによって開始され、時には、多くの場合クライアントのユーザに代わって、該クライアントによって自動的に開始されることが分かるであろう。したがって、図の説明においてクライアント又はクライアントのユーザというときには、「クライアント」及び「ユーザ」という用語は、説明される処理の意味に大きな影響を与えることなく交換可能に用いることができることを理解すべきである。

40

【0020】

ここで図3を参照すると、データ・フロー図は、クライアントがサーバにおける保護リソースへのアクセスを試みる際に用いることができる典型的な認証処理を示す。図示されるように、クライアント・ワークステーション150のユーザは、該クライアント・ワークステーション上で実行する該ユーザのウェブ・ブラウザを通じ、コンピュータ・ネットワークを介して、サーバ151上の保護リソースへのアクセスを求める。保護リソースとは、アクセスが制御又は制限されているリソース(アプリケーション、オブジェクト、文書、ページ、ファイル、実行可能コード、又は他のコンピュータ・リソース、通信形式リソースなど)である。保護リソースは、認証され且つ許可されたユーザによってのみアクセス可能な、Uniform Resource Locator(URL)、又はよ

50

り一般的には、Uniform Resource Identifier (URI) によって特定される。コンピュータ・ネットワークは、図1又は図2に示されるように、インターネット、イントラネット、又は他のネットワークとすることができ、サーバは、ウェブ・アプリケーション・サーバ (WAS)、サーバ・アプリケーション、サーバレット・プロセスなどとすることができる。

【0021】

処理は、ユーザが、「ibm.com」ドメイン内のウェブ・ページのようなサーバ・サイドの保護リソースを要求したときに開始される (ステップ152)。「サーバ・サイド」及び「ユーザ・サイド」という用語は、それぞれ、ネットワーク環境内のサーバ及びクライアントにおける動作又はエンティティを指す。ウェブ・ブラウザ (又は、関連するアプリケーション若しくはアプレット) は、「ibm.com」ドメインをホスティングするウェブ・サーバに送信されるHTTP要求を生成する (ステップ153)。「要求」及び「応答」という用語は、メッセージ、通信プロトコル情報、又は他の関連情報などの、特定の操作に必要とされる情報の転送に適したデータ・フォーマット設定を含むことが理解されるべきである。

10

【0022】

サーバは、このクライアントについてアクティブなセッションがないものと判断し (ステップ154)、そのため、サーバは、該サーバと該クライアントとの間に、該クライアントと該サーバとの間の多数の情報転送を伴うSSL (Secure Sockets Layer) セッションの確立を開始し、完了する。SSLセッションが確立された後は、該SSLセッション内でその後の通信メッセージが転送されるが、該SSLセッション内の通信メッセージは暗号化されているため、いずれの秘密情報も安全に保たれる。

20

【0023】

しかしながら、サーバは、ユーザが保護リソースにアクセスすることが可能になる前に該ユーザの識別情報を判断する必要があるため、該サーバは、何らかのタイプの認証チャレンジをクライアントに送信することによって認証処理を実行するようにユーザに要求する (ステップ156)。認証チャレンジは、HTML形式などの様々なフォーマットとすることができる。次いで、ユーザは、ユーザ名又は他のタイプのユーザ識別子などの要求された情報又は必要な情報を、関連するパスワード又は他の形式の秘密情報と共に提供する (ステップ157)。

30

【0024】

認証応答情報はサーバに送信され (ステップ158)、その時点で、サーバは、例えば以前に提出された登録情報を検索し、提示された認証情報をユーザの格納済み情報と照合することによって、ユーザ又はクライアントを認証する (ステップ159)。認証が成功した場合には、認証されたユーザ又はクライアントについてアクティブなセッションが確立される。

【0025】

次いで、サーバは、初めに要求されたウェブ・ページを検索して、HTTP応答メッセージをクライアントに送信し (ステップ160)、それにより、保護リソースについてのユーザの当初要求を実現する。この時点で、ユーザは、ブラウザ・ウィンドウ内のハイパーテキスト・リンクをクリックすることによって「ibm.com」内の別のページを要求することができ、該ブラウザは、別のHTTP要求メッセージをサーバに送信する (ステップ162)。この時点で、サーバは、ユーザがアクティブなセッションを有していることを認識し (ステップ163)、該サーバは、別のHTTP応答メッセージにおいて、要求されたウェブ・ページをクライアントに返信する (ステップ164)。

40

【0026】

ここで図4を参照すると、ブロック図は、複数の認証サーバを含むエンタープライズ・ドメインについての典型的なデータ処理システムを示す。典型的な企業コンピューティング環境又はインターネット・ベースのコンピューティング環境の場合と同様に、エンタープライズ・ドメイン170は、ユーザ171が、例えばクライアント装置173上のブラ

50

ウザ・アプリケーション 172 を用いることによってネットワーク 174 を介してアクセスすることが可能な制御されたリソースのホストとして機能する。アプリケーション・サーバ 175 は、ウェブ・ベースのアプリケーションを介して、又はレガシ・アプリケーションを含む他のタイプのアプリケーションを介してアクセス可能なリソースをサポートする。認証サーバ 176 は、ユーザ名 / パスワード、X.509 証明書、又はセキュア・トークンなどの様々な認証機構をサポートする。エンタープライズ・ドメイン 170 は、複数のサーバをサポートする。プロキシ・サーバ 177 は、エンタープライズ・ドメイン 170 に代わって、広範囲の機能を実行する。プロキシ・サーバ 177 は、例えばアプリケーション・サーバのコンテンツをミラーリングするためにウェブ・ページをキャッシュすること、又は、入力データストリーム・フィルタ・ユニット 179 及び出力データストリーム・フィルタ・ユニット 180 を通して、着信及び発信するデータストリームにフィルタをかけることなどのプロキシ・サーバ 177 の機能を制御するために、管理上、設定ファイル及びエンタープライズ・ポリシー・データベース 178 を介して設定することができる。入力データストリーム・フィルタ・ユニット 179 は、要求が着信したときに複数の検査を実行することができ、一方、出力データストリーム・フィルタ・ユニット 180 は、応答を発信するときに複数の検査を実行することができ、各々の検査は、種々のエンタープライズ・ポリシー内に指定された目標及び条件に従って実行することができる。

10

【0027】

エンタープライズ・ドメイン 170 は、許可サーバ 181 を含む。許可サーバ 181 の許可ポリシー管理ユニット 182 は、ユーザ・レジストリ 183 及びアクセス制御リスト (ACL) データベース 184 内の情報を管理する。ポリシー管理ユニット 182 は、ユーザがドメイン 170 内のアプリケーション・サーバ 175 によって提供される特定のサービスにアクセスすることを許可されるかどうかを、これらのサービスについてのユーザ要求に対するポリシーを検査することによって判断する。本明細書の例は、ユーザが、認証された後に全ての制御されたリソースにアクセスすることを許可されるものと仮定するが、本発明の様々な実施形態は、本発明の範囲に影響を与えることなく代替的な許可処理を組み込むことができることに注意すべきである。

20

【0028】

エンタープライズ・ドメイン 170 内の上記のエンティティは、多くのコンピューティング環境内の典型的なエンティティを表す。図 3 に関して示されたように、ウェブ・ベースのアプリケーションは、種々の手段を利用して、多くの場合は HTML 形式内のユーザ名 / パスワードの組み合わせとして認証情報を入力するように、ユーザに指示することができる。図 4 に示される例においては、ユーザ 171 は、クライアント 173 がリソースにアクセスする前に認証されることを要求される場合があり、その後、図 3 において上述されたものと同様の方法で、クライアント 173 についてのセッションが確立される。図 4 においては、入力データストリーム・フィルタ・ユニット 179 は、クライアント 173 からの着信要求を受信した後で、クライアント 173 がすでにセッションを確立済みであるかどうかを判断することができ、確立されていない場合には、ユーザ 171 を認証するために認証サーバ 176 上の認証サービスを呼び出すことができる。クライアント 173 がすでにセッションを確立済みである場合には、制御されたリソースへのアクセスを承諾する前に着信要求に対して付加的な検査を実行することができ、この付加的な検査は、エンタープライズ認証ポリシーの中で指定することができる。

30

40

【0029】

ここで本発明に焦点を移すと、幾つかのシステムはステップアップ認証手続きを実行する必要があることが上記された。しかしながら、ユーザ名 / パスワードの組み合わせといった下位レベルの非証明書ベースの認証手続きについてクライアントとサーバとの間に SSL セッションが確立された場合に、認証サービスと該ユーザのブラウザ又は同様のクライアント・アプリケーションとの間で相互認証されたアクティブな SSL セッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップする操作は不可能であることもまた指摘された。本発明は、

50

既存のSSLセッションを介してユーザ又はユーザのクライアント装置についての証明書ベースの認証手続きを実行するサーバ・サイドの認証サービスを持つことによって、この問題への解決策を提供する。本発明は、残りの図面に関連して以下により詳細に説明される。

【0030】

ここで図5を参照すると、ブロック図は、本発明に係るステップアップ認証処理を含むように拡張された認証サービスを示す。クライアント200は、図4に関して上述されたものと同様の方法で、様々なウェブ・アプリケーションからリソース及びサービスにアクセスするためのウェブ・ブラウザ・アプリケーション202又は同様のクライアント・アプリケーションを実行する。ブラウザ202は、仮想マシンを含むことができるランタイム環境204をサポートし、ランタイム環境204は、アプレット又はプラグインなどの、様々なタイプのダウンロード可能な実行可能ソフトウェア・モジュールを実行することができる。ブラウザ202及びサポートされたアプレット/プラグインは、クライアントがユーザのデジタル証明書及び/又は暗号鍵を保持する鍵データストア206にアクセスすることができる。さらに、ブラウザ202及びサポートされた実行可能モジュールは、クライアント200において生成された署名のログを収める署名ログ208にアクセスすることができる。署名ログ208はまた、クライアント200からの署名の提出に回答してウェブ・サーバから戻された署名記録/受け取りを収めることができる。

10

【0031】

ドメイン210は、アプリケーション・サーバ及び認証サーバを備え、そのうちの少なくとも1つは、本発明のステップアップ認証機能を実装するためのステップアップ認証処理ユニット214を含む認証サービス212をサポートする。認証サービス212はまた、以下により詳細に説明されるように、クライアントから受信するデジタル署名を検証するためのデジタル署名検証ユニット216と、認証サービス212からの要求に回答してクライアントから戻された受信済み署名の記録を格納するための署名ログ218とをサポートする。

20

【0032】

ここで図6を参照すると、フローチャートは、相互認証されたアクティブなSSLセッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップするための処理を示す。図3に関して上述されたように、保護リソースにアクセスするためのユーザ要求を受信したことに回答して、例えばクライアント装置上のブラウザ・アプリケーションにおけるユーザ動作に回答して生成されたHTTP要求メッセージの形式のウェブ・ページ要求の結果として、サーバにおいて典型的な非証明書ベースの認証操作を行うことができる(ステップ302)。相互認証されたSSLセッションをクライアントとサーバとの間に確立した後で、該サーバは、該SSLセッションを介して、非証明書ベースの認証操作、例えば有効なユーザ名/パスワードの組み合わせ又は他の何らかの秘密情報を提供するためのクライアント/ユーザに対するチャレンジを実行する(ステップ304)。非証明書ベースの認証操作の完了が成功した場合には、サーバは、例えば応答メッセージを戻すか又は他の何らかの動作を実行することによって、初めに要求されたリソースをクライアントに提供する(ステップ306)。

30

40

【0033】

しかしながら、図3が非証明書ベースの認証操作のみを示すのに対して、図6は、本発明が証明書ベースの認証操作によってもたらされるような上位レベルのセキュリティにステップアップするための処理を提供する方法を示すことにより続けられるという点で、図6は図3と異なる。

【0034】

非証明書ベースの認証操作が完了し、以前の非証明書ベースの認証操作によって保護されるクライアント・セッションの間にサーバが保護リソースを提供した後のある時点で、該サーバは、上位レベルのセキュリティによって制御される保護リソース、すなわちその

50

特定のリソースへのアクセスがより制限される保護リソースについての要求を受信する（ステップ308）。それに応答して、サーバは、該サーバとクライアントとの間に以前に確立されたSSLセッションを介して、該クライアントについての証明書ベースの認証操作を実行する（ステップ310）が、これは、その時点のSSLセッションを中断すること、その時点のSSLセッションを再折衝すること、又はその時点のSSLセッションを終了することなく行われる。証明書ベースの認証操作の完了が成功した場合には、サーバは、例えば応答メッセージを戻すか又は他の何らかの動作を実行することによって、より制限されたリソースをクライアントに提供し、処理は終了する。このように、非証明書ベースの認証操作のために以前に用いられたものと同じSSLセッションを介して、証明書ベースの認証操作が行われる。

10

【0035】

「非証明書ベースの認証操作」という用語の使用は、ユーザ/クライアントの識別情報を判断するための第1の認証操作がデジタル証明書を使用しないという事実を指すことに留意すべきである。（非証明書ベースの認証操作において使用される秘密情報、例えばパスワードを安全に伝送するために用いられる場合がある）SSLセッションを確立するためにクライアント・サイドのデジタル証明書を用いることは、本明細書では、非証明書ベースの認証操作における証明書の使用とは見なされない。

【0036】

ここで図7を参照すると、フローチャートは、本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、サーバにおける具体的な処理の更なる詳細を示す。図7に示される処理は、主として、図6におけるステップ308～312についての更なる詳細を提供するものである。図7の処理におけるステップは、サーバ・サイドのデータ処理システム、例えば図5において示される分散データ処理システムと同様のシステム内で行われ、説明を容易にするために、処理をその全体が1つのサーバ内で行われるよう説明するが、処理は、複数のサーバ、アプリケーション、及び/又は装置にわたって実装することができるであろう。本例は、HTTPメッセージ及びHTMLページの使用を説明するが、本発明は、他のプロトコル及びメッセージ/文書フォーマットをサポートするように実装することができる。

20

【0037】

処理は、非証明書ベースの認証操作、例えば図6におけるステップ302～306に示されるような非証明書ベースの認証操作がSSLセッションを介して行われた後で、サーバがクライアントからのリソース要求を受信することによって始まる（ステップ402）。したがって、サーバは、すでに該サーバとアクティブなセッションを確立したクライアントからリソース要求を受信したことを認識し、図3とは対照的に、該サーバは、認証操作を完了するように直ちにクライアントに求めるのではなく、該要求に応答することに進む。

30

【0038】

次いで、サーバは、要求されたリソースへのアクセスが、クライアントとの間ですでに完了した非証明書ベースの認証操作によって提供された下位レベルのセキュリティではなく、証明書ベースの認証操作によって提供することができる上位レベルのセキュリティを必要とすることを決定する（ステップ404）。サーバは、本発明の範囲に影響を与えることなく、種々の処理を通じてこの決定を行うことができる。1つの例として、着信リソース要求は、図4におけるサーバ177などのプロキシ・サーバによって、フィルタをかけるか又は走査することができる。要求されたURIを着信要求メッセージから抽出した後で、抽出されたURIは、該抽出されたURIに関連するポリシーと照合される。関連するポリシーは、いずれかの認証要件又は他のセキュリティ手順を含む、URIに適切に応答するために実行されるべき適切な動作を示す。ポリシーが、要求に応答する前に証明書ベースの認証操作の完了が成功しなければならないことを示す場合、及び、要求しているクライアントとの間で証明書ベースの認証操作がまだ完了していない場合には、図7において示される処理の残りのステップに示すように、認証のレベルをステップアップする

40

50

ための手続きが開始される。この例においては、アプリケーション・サーバは、認証要件を認識していないが、他の実施形態は、本発明の範囲に影響を与えることなく、何らかの方法でアプリケーション・サーバを関与させることができる。

【0039】

次いで、サーバは、ソフトウェア・モジュールをサーバからクライアントにダウンロードすること、及び/又は、クライアントにおいてソフトウェア・モジュールの実行を開始させることに進む(ステップ406)。ソフトウェア・モジュールをダウンロードする方法又は実行を開始させる方法は、変えることができる。第1の実施形態においては、サーバは、例えばクライアントからの初めの要求、すなわち証明書ベースの認証操作を必要とすることが決定された要求に対するHTTP応答メッセージのコンテンツ・ペイロードとして戻されるHTMLウェブ・ページ内にJavaアプレットを埋め込むことによって、アプレット又はプラグインをブラウザなどのクライアント・アプリケーションにダウンロードする。それに応答して、ブラウザは、そのアプレットをウェブ・ページの通常の解釈及び処理の一部として読み込む。

10

【0040】

代替的な実施形態においては、サーバは、特定のMIME(Multipurpose Internet Mail Extension)タイプを有するコンテンツを含むことを示すメッセージ本文をクライアントに戻すことができる。それに応答して、クライアントのブラウザ・アプリケーションは、特定のMIMEタイプを処理することができるものとして以前にブラウザに登録された適切なプラグインを読み込む。幾つの場合においては、特定のMIMEタイプについてのプラグインが登録されていない場合には、ブラウザは、適切なプラグインを探すようにユーザに指示する。このように、ブラウザは、サーバがソフトウェア・モジュールをクライアントにダウンロードする必要がないように、後述される処理ステップを行うことができるソフトウェア・モジュールを予め持つことができる。

20

【0041】

いずれの場合においても、保護リソースについての要求を送信するクライアント・アプリケーションは、以前にアクティブにされたSSLセッションを維持し、サーバは、証明書ベースの認証手続きについてのクライアント・サイドのステップを行うソフトウェア・モジュールを該クライアント・アプリケーションに実行させるために、該SSLセッションを介して適切なメッセージを該クライアント・アプリケーションに送信するが、幾つの場合においては、サーバはソフトウェア・モジュールをダウンロードすることもでき、別の場合においては、ソフトウェア・モジュールはすでにクライアントに存在しているものとすることができる。本発明は、標準的なインターネット関連プロトコル及び仕様に準拠するため、本発明は、クライアント・アプリケーションがサーバ・サイドの認証要件に応答するためのビルトイン機能を持つことを前提としないステップアップ認証操作の方法を提供する。サーバは、周知のインターネット関連技術及びワールド・ワイド・ウェブ関連技術を通じて、ブラウザ及び同様のクライアント・アプリケーションの拡張性を利用することによって、必要な機能を持つソフトウェア・モジュールを提供することができる。

30

【0042】

引き続き図7を参照すると、サーバは、次に、ソフトウェア・モジュールによってデジタル署名されることになるチャレンジ・データをダウンロードする(ステップ408)。チャレンジ・データは、クライアントにおけるアプレット、プラグイン、又は他のソフトウェア・モジュール内にあり、該チャレンジ・データ上にデジタル署名を生成するデジタル署名アルゴリズムへの入力として用いることができる何らかのタイプのデータ項目である。チャレンジ・データのフォーマットは、使用されるデジタル署名アルゴリズムによって決まるものとすることができ、本発明は、1つ又は複数の標準的な又は専用のデジタル署名アルゴリズムをサポートすることができる。

40

【0043】

サーバは、ダウンロードされるアプレットと共にチャレンジ・データをダウンロードす

50

ることができ、又は、チャレンジ・データは、後のメッセージに入れて送信することができる。代替的には、クライアントにおけるアプレット、プラグイン、又は他のソフトウェア・モジュールは、チャレンジ・データを要求することができ、サーバは、それに応答してチャレンジ・データを戻す。代替的には、クライアントは、例えばサーバによって以前にクライアントに戻されたキャッシュ済みウェブ・ページなどのチャレンジ・データをすでに持っている場合がある。

【0044】

その後のいずれかの時点において、サーバは、クライアントからデジタル署名を受信し（ステップ410）、該サーバは、ユーザ/クライアントの適切な公開鍵証明書を用いて該デジタル署名を検証する（ステップ412）。サーバは、ディレクトリから公開鍵証明書を検索することができ、又は、公開鍵証明書は、クライアントからのデジタル署名を伴うメッセージを添付することができ、公開鍵証明書の信頼性は、認証局及び種々の証明書取り消し機構を通じて検証可能である。有効な公開鍵証明書に示される個人/エンティティのみが、公開鍵に対応する秘密鍵を所有するはずであるため、デジタル署名が検証された場合には、クライアントは、非対称の公開暗号鍵/秘密暗号鍵の対における公開鍵に対応する秘密鍵を所有しており、それによってクライアント/ユーザの識別情報を立証することを示している。デジタル署名の検証に成功した場合には、サーバは、否認防止を目的として、例えば、該デジタル署名の複製、検証可能なタイムスタンプ、及び該デジタル署名を受信したIPアドレスと共にデータベース記録を生成することによって、デジタル署名の受信を記録することができる（ステップ414）。デジタル署名の検証に成功することによって、証明書ベースの認証操作が完了し、結果として、サーバは、該サーバが証明書ベースの認証操作を試みる前にクライアントによって要求されたりソースへのアクセスを提供し（ステップ416）、それによって、図7に示される処理を終了する。

10

20

【0045】

ここで図8を参照すると、フローチャートは、本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、クライアントにおける処理を示す。サーバ・サイドの処理を示す図7とは対照的に、図8は、クライアント・サイドの処理を示す。処理は、クライアントがサーバとの間でSSLセッションをすでに確立し、該サーバとの間で非証明書ベースの認証操作を完了することに成功した後で、該クライアントがリソースについての要求メッセージを該サーバに送信することによって始まる（ステップ502）。要求に応答して、クライアントは、証明書ベースの認証操作をサポートするソフトウェア・モジュールを含むか、又はそのようなソフトウェア・モジュールの実行を開始させる、応答メッセージを受信する（ステップ504）。クライアントは、ブラウザなどのクライアント・アプリケーションによってサポートされる仮想マシン内で実行可能なJavaアプレットなどのアプレットを受信することができる。代替的に、クライアントは、特定のMIMEタイプのコンテンツを含むメッセージを受信し、それにより、クライアント・アプリケーションを起動させて、示されるMIMEタイプを有するオブジェクトを処理するプラグインを起動することができる。

30

【0046】

さらに、クライアント・アプリケーションは、デジタル署名を生成する時に用いられるチャレンジ・データを受信することができる（ステップ506）。代替的に、クライアント・アプリケーションは、デジタル署名アルゴリズムへの入力として用いることができるデータ項目をすでに持っている場合もある。いずれの場合においても、クライアントによって用いられるデジタル署名アルゴリズムへの入力データは、該入力データ上に生成されるデジタル署名をサーバが検証するために、該サーバに知られていなければならない。したがって、デジタル署名アルゴリズムへの入力データは、クライアントによって選択され、それに続いて、例えば生成されたデジタル署名と共にSSLセッションを介してサーバに送ることができる。

40

【0047】

クライアント・アプリケーションは、デジタル署名を生成することを開始させられた後

50

、又はデジタル署名を生成することを決定した後のいずれかの時点において、デジタル署名を生成し（ステップ508）、該デジタル署名をサーバに送信する（ステップ510）。さらに、クライアント・アプリケーションは、タイムスタンプ、及び場合によっては否認防止手続きに役立つ他の情報と共に、デジタル署名の生成を記録することができる（ステップ512）。デジタル署名が適切に生成された場合には、クライアントは、以前に確立されたSSLセッションを介してステップアップした証明書ベースの認証操作を完了することに成功したことになり、次いでクライアントは、例えばウェブ・ページを受信することによって要求したリソースへのアクセスを受け（ステップ514）、それによりクライアント・サイドの処理を終了する。

【0048】

デジタル署名を生成し、検証する方法は、本発明の範囲に影響を与えることなく、周知の規格又は専用の処理に従って変えることができる。例えば、以前に確立されたSSLセッションを介してステップアップした証明書ベースの認証処理を実行するというサーバの決定に応答して、クライアントのブラウザが、埋め込まれたアプレットを持つHTMLページを受信した時に、クライアント・サイドの処理を行うことができる。ブラウザは、ウェブ・ページを処理し、クライアント上のファイルなどの鍵データストアの識別子を、その鍵データストアのロックを解除するパスワードと共に入力するようにユーザに指示するアプレットを実行する。アプレットがユーザに指示する機構又は他の方法で作動する機構は、本発明の実装形態に応じて変えることができる。アプレットは、保留中の要求についてデジタル署名を作成する必要性を説明するブラウザ・ウィンドウ内のウェブ・ページを提示することによってユーザに指示することができ、提示されたウェブ・ページは、ユーザがデジタル署名についての要求を承認又は非承認とすることができるようにするOKボタン及びキャンセル・ボタンを有することができる。さらに、提示されたウェブ・ページは、ユーザがチャレンジ・データを見直すことができるように、署名されている該チャレンジ・データを確認表示することができる。

【0049】

典型的には、鍵データストアは、非対称暗号機能のための秘密鍵/公開鍵対のうちの秘密鍵を保持する。鍵データストアは、ブラウザ・アプリケーション、アプレット、又はクライアント・オペレーション・システムといった種々のエンティティによって管理することができる。ブラウザは、暗号情報の使用に関する種々の規格に準拠するものとしてすることができる。例えば、「PKCS#7: Cryptographic Message Syntax」、RFC (Request for Comments) 2315、Internet Engineering Task Force (IETF) は、デジタル署名及びデジタル・エンベロープなどのデータに適用される暗号方式を有するデータについての一般的な構文を記述するPKCS (Public Key Cryptographic System) 仕様である。別の例として、「PKCS#11: Cryptographic Token Interface Standard」、RSA Security, Inc. は、暗号情報を保持し、暗号機能を実行する装置のためのアプリケーション・プログラミング・インターフェース (API) を記述するPKCS仕様である。

【0050】

ユーザが、要求された情報を入力し、該ユーザの秘密鍵の使用を承認することを示した後で、アプレットは、好ましくはWorld Wide Web Consortium (W3C) によって標準化されたXMLデジタル署名の形式で、デジタル署名を生成する。デジタル署名は、続いて検証されることになるデータ項目の組、すなわちいわゆる「署名情報」に適切な署名アルゴリズムを適用することによって作成され、このシナリオにおいては、署名されたデータは、最低限は、チャレンジ・データを含むことになる。XML署名は、デジタル署名を検証するのに用いられるべきユーザの公開鍵証明書を含むことができる、いわゆる「キー情報」も含む。次いで、アプレットは、XML署名をウェブ・サーバに送信し、デジタル署名を生成する処理が完了する。

10

20

30

40

50

【 0 0 5 1 】

本発明の利点は、上述された詳細な説明を考慮すれば明らかとなるはずである。本発明は、ユーザ名/パスワードの組み合わせといった下位レベルの非証明書ベースの認証手続きについてクライアントとサーバとの間にSSLセッションが確立された場合に、認証サービスとユーザのブラウザ又は同様のクライアント・アプリケーションとの間で相互認証されたアクティブなSSLセッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップするための認証操作を提供する。

【 0 0 5 2 】

本発明は、既存のSSLセッションを介してユーザ又はユーザのクライアント装置についての証明書ベースの認証手続きを実行するサーバ・サイドの認証サービスを持つことによって、この問題への解決策を提供する。認証サービスは、必要に応じて、既存のSSLセッションを介して実行可能モジュールをクライアントにダウンロードする。次いで、実行可能モジュールは、クライアント・サイドのデジタル証明書を用いてデジタル署名を生成し、該デジタル署名は、以前に確立されたSSLセッションを介して戻される。認証サービスがデジタル署名を検証した後、証明書ベースの認証手続きは完了する。このようにして、認証サービスは、既存のSSLセッションを終了又は再折衝する必要なく、証明書ベースの認証にステップアップすることができる。

10

【 0 0 5 3 】

完全に機能するデータ処理システムを背景として本発明を説明したが、当業者であれば、本発明の処理は、配布を行うのに実際に用いられる特定のタイプの信号支持媒体に関わらず、コンピュータ可読媒体内の命令の形態で、及び他の様々な形態で、配布できることが分かるであろうということに留意することが重要である。コンピュータ可読媒体の例には、EPROM、ROM、テープ、紙、フロッピー（商標）ディスク、ハード・ディスク・ドライブ、RAM、及びCD-ROMなどの媒体、並びに、デジタル通信リンク及びアナログ通信リンクなどの伝送タイプの媒体が含まれる。

20

【 0 0 5 4 】

方法は、一般に、所望の結果に至る自己矛盾のない一連のステップであると理解される。これらのステップは、物理量の物理的な操作を必要とする。必須ではないが通常は、これらの量は、格納するか、転送するか、組み合わせるか、比較するか、又は他の方法で操作することが可能な電気的信号又は磁気的信号の形態をとる。時には、主に一般的な用法であるという理由で、これらの信号を、ビット、値、パラメータ、項目、要素、記号、文字、語、数などと呼ぶのが都合がよい。しかしながら、これらの用語の全て及び同様の用語は、適切な物理量と関連付けられるものであり、これらの量に付される都合の良いレベルに過ぎないことに留意されたい。

30

【 0 0 5 5 】

本発明の説明は、例示の目的で提示されたものであって、包括的であること、又は、開示された実施形態に限定されることを意図するものではない。当業者であれば、多くの修正及び変形が明らかであろう。本実施形態は、本発明の原理及びその実際の用途を説明するために、並びに、考え得る他の用途に適合するような種々の修正を伴う種々の実施形態を実施するために当業者以外の者が本発明を理解することが可能になるように、選択されたものである。

40

【 図面の簡単な説明 】

【 0 0 5 6 】

【 図 1 】 各々が本発明を実装することができるデータ処理システムの典型的なネットワークを示す。

【 図 2 】 本発明を実装することができるデータ処理システム内で用いることができる典型的なコンピュータ・アーキテクチャを示す。

【 図 3 】 クライアントがサーバにおける保護リソースへのアクセスを試みる際に用いることができる典型的な認証処理を説明するデータ・フロー図を示す。

50

【図4】複数の認証サーバを含むエンタープライズ・ドメインについての典型的なデータ処理システムを示すブロック図を示す。

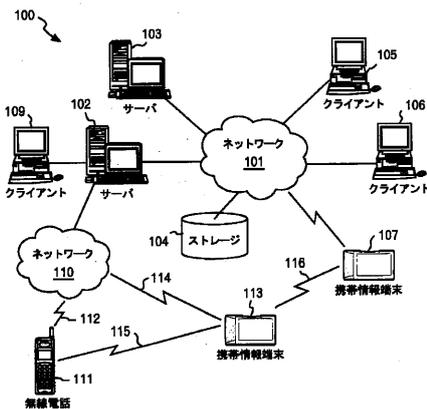
【図5】本発明に係るステップアップ認証処理を含むように拡張された認証サービスを示すブロック図を示す。

【図6】相互認証されたアクティブなSSLセッションを維持しながら、下位レベルの非証明書ベースの認証手続きから上位レベルの証明書ベースの認証手続きにステップアップするための処理を示すフローチャートを示す。

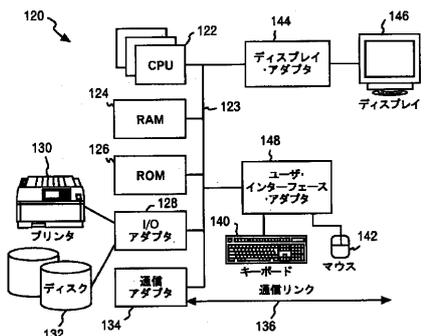
【図7】本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、サーバにおける具体的な処理の更なる詳細を説明するフローチャートを示す。

【図8】本発明の実施形態に係るステップアップした証明書ベースの認証操作のための、クライアントにおける処理を説明するフローチャートを示す。

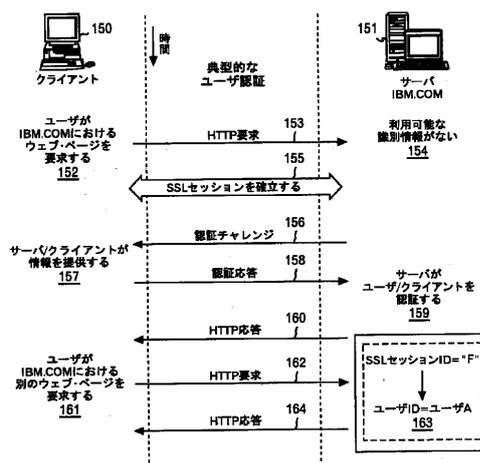
【図1】



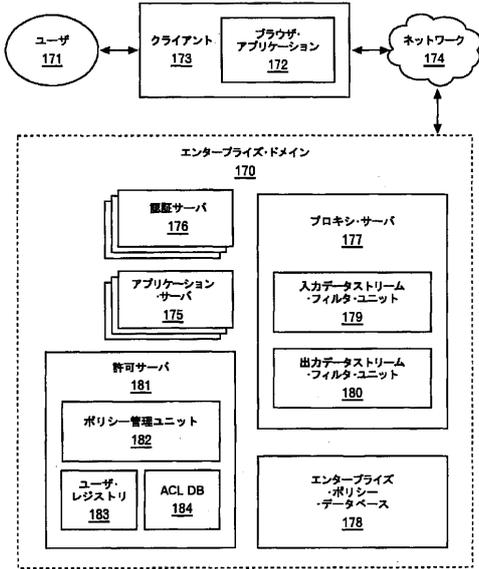
【図2】



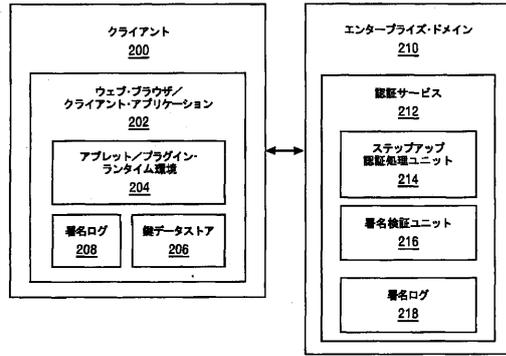
【図3】



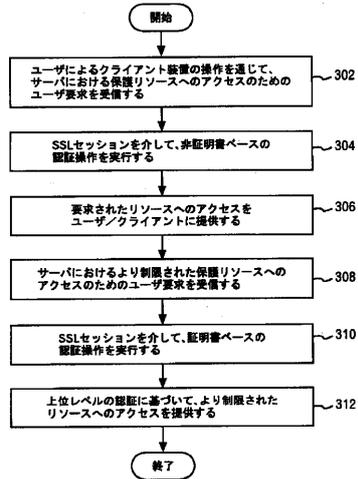
【 図 4 】



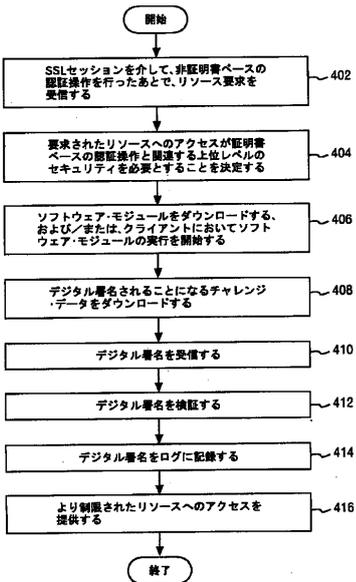
【 図 5 】



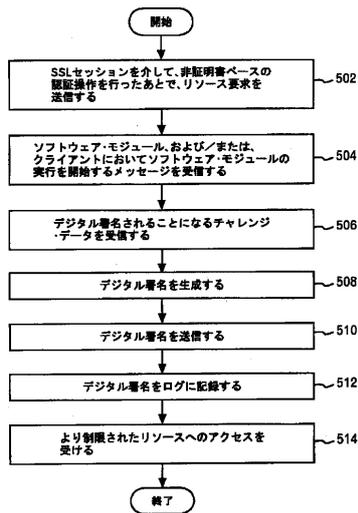
【 図 6 】



【 図 7 】



【 図 8 】



【手続補正書】

【提出日】平成17年5月17日(2005.5.17)

【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】

認証操作を実行するための方法であって、

サーバとクライアントとの間のSSL(Secure Sockets Layer)セッションを介して非証明書ベースの認証操作を実行するステップと、

前記非証明書ベースの認証操作を実行した後で、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードするステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を前記サーバで受信するステップと、

証明書ベースの認証操作を、前記証明書ベースの認証操作の完了前に前記SSLセッションを終了又は再折衝することなく、前記サーバと前記クライアントとの間の前記SSLセッションを介して実行するステップと、

を含む方法。

【請求項2】

前記SSLセッションの折衝が、クライアントからの第1のデジタル証明書を用い、前記証明書ベースの認証操作は、前記クライアントからの第2のデジタル証明書を用い、前記第1のデジタル証明書と前記第2のデジタル証明書とは同一ではない、請求項1に記載の方法。

【請求項3】

前記非証明書ベースの認証操作に関連するサーバによって、第1のリソースへのアクセスをクライアントに提供するステップをさらに含む、請求項2に記載の方法。

【請求項4】

前記第1のリソースへのアクセスを提供する前記ステップが、

前記クライアントからの第1のリソース要求を前記サーバで受信するステップと、

前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立するステップと、

前記SSLセッションを介して前記サーバと前記クライアントとの間で前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信するステップと、

をさらに含む、請求項3に記載の方法。

【請求項5】

前記証明書ベースの認証操作に関連するサーバによって、第2のリソースへのアクセスをクライアントに提供するステップをさらに含む、請求項3又は請求項4に記載の方法。

【請求項6】

前記第2のリソースへのアクセスを提供する前記ステップが、

前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信するステップと、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに前記実行可能モジュールをダウンロードするステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生

成されたデジタル署名を、前記サーバで受信するステップと、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信するステップと、
をさらに含む、請求項5に記載の方法。

【請求項7】

前記第2のリソースへのアクセスを提供する前記ステップが、

前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信するステップと、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバによって前記クライアントにおけるダウンロード可能ソフトウェア・モジュールの実行を開始させるステップと、

前記クライアントにおいてデジタル証明書を用いて前記ダウンロード可能ソフトウェア・モジュールの実行によって生成されたデジタル署名を、前記サーバで受信するステップと、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース要求を送信するステップと、
をさらに含む、請求項5に記載の方法。

【請求項8】

前記証明書ベースの認証操作に関連して、クライアントがサーバにおける第2のリソースへのアクセスを取得するステップをさらに含む、請求項1から請求項7までのいずれか1つの請求項に記載の方法。

【請求項9】

前記第2のリソースへのアクセスを取得する前記ステップが、

前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信するステップと、

証明書ベースの認証操作を行うための機能を備える実行可能モジュールを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信するステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信するステップと、

前記サーバからの第2のリソース応答を前記クライアントで受信するステップと、
をさらに含む、請求項8に記載の方法。

【請求項10】

前記第2のリソースへのアクセスを取得する前記ステップが、

前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信するステップと、

関連するコンテンツ・タイプ標識を伴うコンテンツを有する応答メッセージを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信するステップと、

前記コンテンツのコンテンツ・タイプを決定したことに応答して、前記クライアントにおいてダウンロード可能ソフトウェア・モジュールを実行するステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信するステップと、

前記サーバからの第2のリソース応答を前記クライアントで受信するステップと、
をさらに含む、請求項8に記載の方法。

【請求項11】

認証操作を実行するための装置であって、

サーバとクライアントとの間のSSL (Secure Sockets Layer) セッションを介して非証明書ベースの認証操作を実行する手段と、

前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を前記サーバで受信する手段と、

前記非証明書ベースの認証操作を実行した後で、証明書ベースの認証操作を、前記証明書ベースの認証操作の完了前に前記SSLセッションを終了又は再折衝することなく前記サーバと前記クライアントとの間の前記SSLセッションを介して実行する手段と、
を備える装置。

【請求項12】

前記SSLセッションの折衝が、クライアントからの第1のデジタル証明書を用い、前記証明書ベースの認証操作は、前記クライアントからの第2のデジタル証明書を用い、前記第1のデジタル証明書と前記第2のデジタル証明書とは同一ではない、請求項11に記載の装置。

【請求項13】

前記非証明書ベースの認証操作に関連するサーバによって、第1のリソースへのアクセスをクライアントに提供する手段をさらに備える、請求項12に記載の装置。

【請求項14】

前記第1のリソースへのアクセスを提供する前記手段が、
前記クライアントからの第1のリソース要求を前記サーバで受信する手段と、
前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立する手段と、

前記SSLセッションを介して前記サーバと前記クライアントとの間で前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、
をさらに備える、請求項13に記載の装置。

【請求項15】

前記証明書ベースの認証操作に関連するサーバによって、第2のリソースへのアクセスをクライアントに提供する手段をさらに備える、請求項13又は請求項14に記載の装置。

【請求項16】

前記第2のリソースへのアクセスを提供する前記手段が、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、
前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに前記実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信する手段と、
をさらに備える、請求項15に記載の装置。

【請求項17】

前記第2のリソースへのアクセスを提供する前記手段が、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバによって前記クライアントにおけるダウンロード可能ソフトウェア・モジュールの実行を開始させる手段と、

前記クライアントにおいてデジタル証明書を用いて前記ダウンロード可能ソフトウェア・モジュールの実行によって生成されたデジタル署名を、前記サーバで受信する手段と、前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース要求を送信する手段と、をさらに備える、請求項15に記載の装置。

【請求項18】

前記証明書ベースの認証操作に関連して、クライアントがサーバにおける第2のリソースへのアクセスを取得する手段をさらに備える、請求項11から請求項17までのいずれか1つの請求項に記載の装置。

【請求項19】

前記第2のリソースへのアクセスを取得する前記手段が、前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信する手段と、

証明書ベースの認証操作を行うための機能を備える実行可能モジュールを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信する手段と、

前記サーバからの第2のリソース応答を前記クライアントで受信する手段と、をさらに備える、請求項18に記載の装置。

【請求項20】

前記第2のリソースへのアクセスを取得する前記手段が、前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信する手段と、

関連するコンテンツ・タイプ標識を伴うコンテンツを有する応答メッセージを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信する手段と、

前記コンテンツのコンテンツ・タイプを決定したことに応答して、前記クライアントにおいてダウンロード可能ソフトウェア・モジュールを実行する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信する手段と、

前記サーバからの第2のリソース応答を前記クライアントで受信する手段と、をさらに備える、請求項18に記載の装置。

【請求項21】

データ処理システムにおいて用いるコンピュータ可読媒体内の、認証操作を実行するためのコンピュータ・プログラムであって、

サーバとクライアントの間のSSL(Secure Sockets Layer)セッションを介し、非証明書ベースの認証操作を実行する手段と、

前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を前記サーバで受信する手段と、

前記非証明書ベースの認証操作を実行した後で、証明書ベースの認証操作の完了に先立つSSLセッションを終了又は再折衝することなく、サーバとクライアントの間のSSLセッションを介し、前記証明書ベースの認証操作を実行する手段と、を含むコンピュータ・プログラム。

【請求項22】

前記SSLセッションの折衝が、クライアントからの第1のデジタル証明書を用い、前記証明書ベースの認証操作は、前記クライアントからの第2のデジタル証明書を用い、前記第1のデジタル証明書と前記第2のデジタル証明書とは同一ではない、請求項21に記載のコンピュータ・プログラム。

【請求項23】

前記非証明書ベースの認証操作に関連するサーバによって、第1のリソースへのアクセスをクライアントに提供する手段をさらに含む、請求項21又は請求項22に記載のコンピュータ・プログラム。

【請求項24】

前記第1のリソースへのアクセスを提供する前記手段が、
前記クライアントからの第1のリソース要求を前記サーバで受信する手段と、
前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立する手段と、

前記SSLセッションを介して前記サーバと前記クライアントとの間で前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、
をさらに含む、請求項23に記載のコンピュータ・プログラム。

【請求項25】

前記証明書ベースの認証操作に関連するサーバによって、第2のリソースへのアクセスをクライアントに提供する手段をさらに含む、請求項21から請求項24までのいずれか1つの請求項に記載のコンピュータ・プログラム。

【請求項26】

前記第2のリソースへのアクセスを提供する前記手段が、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに前記実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信する手段と、
をさらに含む、請求項25に記載のコンピュータ・プログラム。

【請求項27】

前記第2のリソースへのアクセスを提供する前記手段が、
前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバによって前記クライアントにおけるダウンロード可能ソフトウェア・モジュールの実行を開始させる手段と、

前記クライアントにおいてデジタル証明書を用いて前記ダウンロード可能ソフトウェア・モジュールの実行によって生成されたデジタル署名を、前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース要求を送信する手段と、
をさらに含む、請求項25に記載のコンピュータ・プログラム。

【請求項28】

前記証明書ベースの認証操作に関連して、クライアントがサーバにおける第2のリソースへのアクセスを取得する手段をさらに含む、請求項21から請求項27までのいずれか1つの請求項に記載のコンピュータ・プログラム。

【請求項29】

前記第2のリソースへのアクセスを取得する前記手段が、
前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信する手段と、

証明書ベースの認証操作を行うための機能を備える実行可能モジュールを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信する手段と、
前記サーバからの第2のリソース応答を前記クライアントで受信する手段と、
をさらに含む、請求項28に記載のコンピュータ・プログラム。

【請求項30】

前記第2のリソースへのアクセスを取得する前記手段が、

前記SSLセッションを介して、前記クライアントから前記サーバに第2のリソース要求を送信する手段と、

関連するコンテンツ・タイプ標識を伴うコンテンツを有する応答メッセージを、前記クライアントにおいて、前記SSLセッションを介して前記サーバから受信する手段と、

前記コンテンツのコンテンツ・タイプを決定したことに応答して、前記クライアントにおいてダウンロード可能ソフトウェア・モジュールを実行する手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバに送信する手段と、

前記サーバからの第2のリソース応答を前記クライアントで受信する手段と、
をさらに含む、請求項28に記載のコンピュータ・プログラム。

【請求項31】

認証操作を実行するための方法であって、

クライアントからの第1のリソース要求をサーバで受信するステップと、

前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立するステップと、

前記SSLセッションを介して非証明書ベースの認証操作を実行するステップと、

前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信するステップと、

前記非証明書ベースの認証操作を実行した後で、前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信するステップと、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードするステップと、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバで受信するステップと、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信するステップと、
を含む方法。

【請求項32】

認証操作を実行するための装置であって、

クライアントからの第1のリソース要求をサーバで受信する手段と、

前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立する手段と、

前記SSLセッションを介して非証明書ベースの認証操作を実行する手段と、

前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、

前記非証明書ベースの認証操作を実行した後で、前記クライアントからの第2のリソース

ス要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信する手段と、
を備える装置。

【請求項33】

データ処理システムにおいて用いるコンピュータ可読媒体内の、認証操作を実行するためのコンピュータ・プログラムであって、

クライアントからの第1のリソース要求をサーバで受信する手段と、

前記第1のリソース要求に応答する前に前記第1のリソース要求が非証明書ベースの認証操作の完了を必要とすると決定したことに応答して、前記サーバと前記クライアントとの間にSSL(Secure Sockets Layer)セッションを確立する手段と、

前記SSLセッションを介して非証明書ベースの認証操作を実行する手段と、

前記非証明書ベースの認証操作を実行することに成功したことに応答して、前記サーバから前記クライアントに第1のリソース応答を送信する手段と、

前記非証明書ベースの認証操作を実行した後で、前記クライアントからの第2のリソース要求を、前記SSLセッションを介して前記サーバで受信する手段と、

前記第2のリソース要求が証明書ベースの認証手続きを必要とすると決定したことに応答して、前記SSLセッションを介して前記サーバから前記クライアントに実行可能モジュールをダウンロードする手段と、

前記クライアントにおいてデジタル証明書を用いて前記実行可能モジュールによって生成されたデジタル署名を、前記SSLセッションを介して前記サーバで受信する手段と、

前記サーバにおいて前記デジタル署名を検証することに成功したことに応答して、前記サーバから前記クライアントに第2のリソース応答を送信する手段と、
を含むコンピュータ・プログラム。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正の内容】

【0009】

本発明の第1の態様によれば、認証操作を実行するための方法であって、サーバとクライアントとの間のSSL(Secure Sockets Layer)セッションを介して非証明書ベースの認証操作を実行するステップと、該非証明書ベースの認証操作を実行した後で、該SSLセッションを介して該サーバから該クライアントに実行可能モジュールをダウンロードするステップと、該クライアントにおいてデジタル証明書を用いて該実行可能モジュールによって生成されたデジタル署名を該サーバで受信するステップと、証明書ベースの認証操作を、該証明書ベースの認証操作の完了前に該SSLセッションを終了又は再折衝することなく、該サーバと該クライアントとの間の該SSLセッションを介して実行するステップと、を含む方法が提供される。

【 国際調査報告 】

INTERNATIONAL SEARCH REPORT

 International Application No
 PCT/EP2004/051435

| | | |
|--|---|---|
| A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04L29/06 H04L9/00 | | |
| 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) IPC 7 H04L G06F | | |
| 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 practical, 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. |
| X | WO 01/11451 A (SUN MICROSYSTEMS INC) 15 February 2001 (2001-02-15) abstract page 2, line 27 - line 34 page 5, line 1 - page 8, line 26 page 9, line 2 - page 10, line 20 page 12, line 22 - page 16, line 10 page 19, line 9 - page 20, line 31 page 21, line 17 - page 22, line 24 | 1-33 |
| A | WO 00/27089 A (LOCKSTAR INC) 11 May 2000 (2000-05-11) the whole document | 1-33 |
| A | WO 02/39237 A (IBM DEUTSCHLAND ; IBM (US)) 16 May 2002 (2002-05-16) page 10, line 8 - page 29, line 6 --- -/-- | 1-33 |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. | | <input checked="" type="checkbox"/> Patent family members are listed in 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 document 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. *Z* document member of the same patent family |
| Date of the actual completion of the international search 28 October 2004 | | Date of mailing of the international search report 05/11/2004 |
| Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016 | | Authorized officer Apostolescu, R |

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051435

| C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT | | |
|--|---|-----------------------|
| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| A | EP 1 280 317 A (HEWLETT PACKARD CO) 29 January 2003 (2003-01-29) paragraph '0003! - paragraph '0005! paragraph '0011! paragraph '0015! - paragraph '0018! paragraph '0027! | 1-33 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2004/051435

| Patent document cited in search report | | Publication date | Patent family member(s) | Publication date |
|--|---|------------------|-------------------------|------------------|
| WO 0111451 | A | 15-02-2001 | US 6609198 B1 | 19-08-2003 |
| | | | AU 6617000 A | 05-03-2001 |
| | | | EP 1204912 A1 | 15-05-2002 |
| | | | WO 0111451 A1 | 15-02-2001 |
| | | | US 2004210771 A1 | 21-10-2004 |
| WO 0027089 | A | 11-05-2000 | AU 1236800 A | 22-05-2000 |
| | | | WO 0027089 A1 | 11-05-2000 |
| WO 0239237 | A | 16-05-2002 | AU 1234502 A | 21-05-2002 |
| | | | WO 0239237 A2 | 16-05-2002 |
| | | | EP 1368722 A2 | 10-12-2003 |
| | | | TW 528957 B | 21-04-2003 |
| EP 1280317 | A | 29-01-2003 | GB 2378010 A | 29-01-2003 |
| | | | EP 1280317 A1 | 29-01-2003 |
| | | | US 2003023880 A1 | 30-01-2003 |

フロントページの続き

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

(74)代理人 100112690

弁理士 太佐 種一

(72)発明者 アシュレー、ポール、アンソニー

オーストラリア国 4 0 6 5 クイーンズランド州 バードン ボウマン・パレード 4 9

(72)発明者 マピディ、スリダール

アメリカ合衆国 7 8 7 5 9 テキサス州 オースチン ヤーボン・ドライブ 6 6 2 3

(72)発明者 バンデンバウバー、マーク

アメリカ合衆国 7 8 6 8 1 テキサス州 ラウンドロック ウィットワース・レーン 8 0 1 3

Fターム(参考) 5J104 AA07 AA09 KA01 KA04 LA03 LA06 NA02 NA05 NA27 NA37

NA38 PA07