(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5122225号
(P5122225)
(45)発行日　平成25年1月16日(2013.1.16)　(24)登録日　平成24年11月2日(2012.11.2)

(51)Int.Cl.　F I
G06F 21/44 (2013.01)　G06F 21/20　144C

請求項の数 19　外国語出願　(全 16 頁)

(21)出願番号　特願2007-244239(P2007-244239)
(22)出願日　平成19年9月20日(2007.9.20)
(65)公開番号　特開2008-77664(P2008-77664A)
(43)公開日　平成20年4月3日(2008.4.3)
審査請求日　平成22年9月16日(2010.9.16)
(31)優先権主張番号　06121051.4
(32)優先日　平成18年9月21日(2006.9.21)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　500232617
イルデト・ベー・フェー
オランダ・ＮＬ－２１３２・ＬＳ・フーフドドープ・タウルサヴェンウー・１０５
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　アンドリュー・オーガスティン・ワイス
オランダ・２０２３・ＡＡ・ハーレム・ショッタージンゲル・９３
最終頁に続く

(54)【発明の名称】サーバとクライアント・システムとの間の通信セッションにおける状態追跡機構を履行する方法

(57)【特許請求の範囲】
【請求項１】
サーバ(1)とクライアント・システム(2)との間での通信セッションにおける状態追跡機構を履行する方法であって、
該クライアント・システムから第1リクエスト・メッセージを受信することであって、ここに該第1リクエスト・メッセージが第1データおよび第1状態値を含むことと、
該第1リクエスト・メッセージから該第1データを取り出すことと、
第2データを生成することと、
少なくとも該第2データおよび該第1状態値を入力として用いて第2状態値を計算することと、
第1サーバ応答を該クライアント・システムに送信することであって、ここに該第1サーバ応答が該第2データおよび該第2状態値を含むことと、
該第2状態値が第1クライアントの予想された状態値に等しいと該クライアント・システムが判断するとき、該クライアント・システムから第2リクエスト・メッセージを受信することであって、ここに該第2リクエスト・メッセージが第3状態値を含み、
該第1クライアントの予想された状態値が少なくとも該第1サーバ応答から取り出された該第2データおよび該第1状態値を入力として用いて計算され、
該第3状態値が少なくとも該第1データおよび該第2状態値を入力として用いて計算されることと、
少なくとも該第1データおよび該第2状態値を入力として用いて第1サーバの予想された

状態値を計算することと、
該第3状態値が該第1サーバの予想された状態値に等しいかどうかを判断することと、
該第3状態値が該第1サーバの予想された状態値に等しくないと判断された場合、該通信セッションを中断することと、
該第3状態値が該第1サーバの予想された状態値に等しいと判断された場合、少なくとも該第2データおよび該第3状態値を入力として用いて第4状態値を計算することと、
該クライアント・システムに第2サーバ応答を送信することであって、ここに該第2サーバ応答が該第4状態値を含むことと、
該第4状態値が第2クライアントの予想された状態値に等しいと該クライアント・システムが判断するとき、該クライアント・システムから第3リクエスト・メッセージを受信することであって、ここに該第3リクエスト・メッセージが第5状態値を含み、
該第2クライアントの予想された状態値が少なくとも該第2データおよび該第4状態値を入力として用いて計算され、
該第5状態値が少なくとも該第1データおよび該第4状態値を入力として用いて計算されることとを含む方法。

【請求項２】
該第1データはナンス(Nc)を含む請求項1に記載の方法。

【請求項３】
該クライアント・システム(2)には、それぞれの権限付与と関連した暗号化された情報を解読するために権限付与の識別子の組が与えられ、当該方法は、
該識別子の組に対応する該権限付与を反映する記録を維持し、そして
該クライアント・システム(2)に提供された組における識別子の各々の少なくとも部分に対応するデータをさらなる入力として用いて該第1サーバの予想された状態値を計算することをさらに含む請求項1または2のいずれか1項に記載の方法。

【請求項４】
該サーバ(1)と該クライアント・システム(2)との間で通信が行われるネットワーク(3)上で、該クライアント・システム(2)のネットワーク・アドレス、好ましくは該クライアント・システム(2)によって用いられる装備(4)に結線されたアドレスを用いて該第1サーバの予想された状態値を計算するステップをさらに含む請求項1乃至3のいずれか1項に記載の方法。

【請求項５】
該第3状態値が該第1サーバの予想された状態値に等しいと判断された場合、該クライアント・システム(2)にアプリケーション・データを提供するステップをさらに含む請求項1乃至4のいずれか1項に記載の方法。

【請求項６】
該アプリケーション・データは、該第2状態値が該第1クライアントの予想された状態値に等しいと該クライアント・システムが判断する場合には該第2状態値、該第4状態値が該第2クライアントの予想された状態値に等しいと該クライアント・システムが判断する場合には該第4状態値、または該第3状態値が該第1サーバの予想された状態値に等しいと判断される場合には該第3状態値の少なくとも部分を用いて導出可能なキーのもとで解読を許容するよう暗号化される、暗号化された形態で提供される請求項5に記載の方法。

【請求項７】
該第2リクエスト・メッセージを受信し、該第1サーバの予想された状態値を計算し、該第3状態値が該第1状態値に等しいかどうかを判断し、該第3状態値が該第1状態値に等しいと判断されたとき、該第4状態値を計算し、該クライアント・システムに該第2サーバ応答を送信するステップは、該クライアント・システム(2)が状態追跡情報の有効な値を有するかどうかを判断することを含み、当該方法は、
通信セッションの期間を通して、該クライアント・システム(2)が該状態追跡情報の有効な値を有するかどうかを判定するステップを繰り返し、そして
該クライアント・システム(2)が該状態追跡情報の有効な値を有すると判断されるとき

にのみ、該クライアント・システム(2)にアプリケーション・データを提供することをさらに含む請求項1乃至4のいずれか1項に記載の方法。

【請求項８】

クライアント・システム(2)には、キーのもとで解読を許容するよう暗号化されるコンテント・データの組が提供され、アプリケーション・データはキーの値を含む請求項5乃至7のいずれか1項に記載の方法。

【請求項９】

請求項1乃至8のいずれか1項に記載の方法を実行するよう配列されたデータ処理ユニットおよびメモリを含むサーバ・システム。

【請求項１０】

状態追跡機構を履行するサーバ(1)で通信セッションを行う方法であって、

第1データを生成することと、

第1状態値を生成することと、

該サーバ(1)に第1リクエスト・メッセージを送信することであって、ここに該第1リクエスト・メッセージが該第1データおよび該第1状態値を含むことと、

該サーバ(1)から該1サーバ応答を受信することであって、ここに該第1サーバ応答が第2データおよび第2状態値を含み、該第2状態値が少なくとも該第2データおよび該第1状態値を入力として用いて計算されることと、

該第1サーバ応答から該第2データを取り出すことと、

少なくとも該第1サーバ応答から取り出された該第2データおよび該第1状態値を入力として用いて第1クライアントの予想された状態値を計算することと、

該第2状態値が該第1クライアントの予想された状態値に等しいかどうかを判断することと、

該第2状態値が該第1クライアントの予想された状態値に等しくないと判断された場合、該通信セッションを中断することと、

該第2状態値が該第1クライアントの予想された状態値に等しいと判断された場合、少なくとも該第1データおよび該第2状態値を入力として用いて第3状態値を計算することと、

該サーバ(1)に第2リクエスト・メッセージを送信することであって、ここに該第2リクエスト・メッセージが該第3状態値を含むことと、

該第3状態値が第1サーバの予想された状態値に等しいと該サーバが判断するとき、該サーバ(1)から第2サーバ応答を受信することであって、ここに該第2サーバ応答が第4状態値を含み、

該第1サーバの予想された状態値が少なくとも該第1データおよび該第2状態値を入力として用いて計算され、

該第4状態値が少なくとも該第2データおよび該第3状態値を入力として用いて計算されることと、

少なくとも該第2データおよび該第4状態値を入力として用いて第2クライアントの予想された状態値を計算することと、

該第4状態値が該第2クライアントの予想された状態値に等しいかどうかを判断することと、

該第4状態値が該第2クライアントの予想された状態値に等しくないと判断された場合、該通信セッションを中断することと、

該第4状態値が該第2クライアントの予想された状態値に等しいと判断された場合、少なくとも該第1データおよび該第4状態値を入力として用いて第5状態値を計算することと、

該サーバ(1)に第3リクエスト・メッセージを送信することであって、ここに該第3リクエスト・メッセージが該第5状態値を含むこととを含む方法。

【請求項１１】

該第1データは該通信セッションの開始時に生成されたナンス(Nc)を含む請求項10に記載の方法。

【請求項１２】

それぞれの権限付与と関連した暗号化された情報を解読するために権限付与の識別子の組を維持し、そして該組における識別子の各々の少なくとも部分に対応するデータをさらなる入力として用いて該第3状態値を計算するステップをさらに含む請求項10または11のいずれか1項に記載の方法。

【請求項１３】

該サーバ(1)と該クライアント・システム(2)との間の通信がネットワーク(3)を介して行われ、該クライアント・システム(2)は、好ましくは、該クライアント・システム(2)によって用いられる装備(4)に結線された該ネットワーク(3)上のアドレスを有し、当該方法は、該ネットワーク・アドレスの少なくとも部分に対応するデータをさらなる入力として用いて該第3状態値を計算することをさらに含む請求項10乃至12のいずれか1項に記載の方法。

【請求項１４】

該第1状態値、該第3状態値または該第5状態値の少なくとも部分に対応するデータを含めて、該サーバ(1)にメッセージを送ることにより、アプリケーション・データの送信を要求するステップをさらに含む請求項10乃至13のいずれか1項に記載の方法。

【請求項１５】

暗号化された形態でアプリケーション・データを受信し、該暗号化されたアプリケーション・データを解読するためのキーを導出するために該第1状態値、該第3状態値および該第5状態値の少なくとも1つを使用するステップをさらに含む請求項10乃至14のいずれか1項に記載の方法。

【請求項１６】

暗号化されたコンテント・データのストリームを受信し、該サーバ(1)から受信されたアプリケーション・データから該暗号化されたコンテント・データを解読するためにキーを得るステップをさらに含む請求項10乃至15のいずれか1項に記載の方法。

【請求項１７】

第2サーバ応答を受信し、第2クライアントの予想された状態値を計算し、該第4状態値が該第2クライアントの予想された状態値に等しいかどうかを判断し、そして該第4状態値が該第2クライアントの予想された状態値に等しいと判断されたとき、第5状態値を計算し、該サーバ(1)に第3リクエスト・メッセージを送信するステップは、該クライアント・システム(2)が状態追跡情報の有効な値を有するかどうかを判断することを含み、当該方法は、

通信セッションの期間を通して、該クライアント・システム(2)が該状態追跡情報の有効な値を有するかどうかを判定するステップを繰り返し、そして

該クライアント・システム(2)が該状態追跡情報の有効な値を有すると判断されるときにのみ、該サーバ(1)からアプリケーション・データを受信することをさらに含む請求項10乃至13のいずれか1項に記載の方法。

【請求項１８】

請求項10乃至17のいずれか1項に記載の方法を実行するよう配列された、データ処理ユニット(6)およびメモリ(7、9)を含むクライアント・システム。

【請求項１９】

機械読取り可能な媒体に組み込まれたとき、情報処理能力を有するシステムに、請求項1乃至8または請求項10乃至17のいずれか1項に記載の方法を行わせることができる一組の命令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、サーバとクライアント・システムとの間の通信セッションにおける状態追跡機構を履行する方法であって、通信セッションの進行中に、状態追跡情報の有効値をクライアント・システムが有する場合にのみアクセス可能な形態でクライアント・システムにアプリケーション・データが提供され、クライアント・システムに状態追跡情報の新しい

値を担持するメッセージを送信することを含む方法に関する。
【０００２】
本発明は、また、状態追跡機構を履行するサーバと通信セッションを行なう方法であって、
通信セッションを行うクライアント・システムにおいて状態追跡情報を維持することを含み、それにおいて、通信セッションの進行中に、クライアント・システムに維持された状態追跡情報が値において有効値に対応する場合のみ、アプリケーション・データがサーバから受信されかつクライアント・システム上の目標アプリケーションにアクセス可能とされ、そして
サーバからメッセージにおける状態追跡情報の新しい値を受信することを含む方法に関する。
【０００３】
本発明は、また、サーバ、クライアント・システム、及びコンピュータ・プログラムにも関する。
【背景技術】
【０００４】
このような方法の例は、Kristol, D. 及びMontulli, L. の“ＨＴＴＰ状態管理機構”ＲＦＣ　２９６５、インターネット・ササイアティ、２０００年１０月から知られている。この公報は、発信源（オリジン）サーバがユーザ・エージェントに状態情報を送る方法、並びにユーザ・エージェントが発信源サーバに状態情報を戻す方法を記載している。該公報は、参加している発信源サーバとユーザ・エージェントとの間で状態情報を運ぶ、３つのヘッダ、クッキー（Ｃｏｏｋｉｅ）、クッキー２（Ｃｏｏｋｉｅ２）、及びセット－クッキー２（Ｓｅｔ－Ｃｏｏｋｉｅ２）を記載している。ユーザ・エージェントは、各発信源サーバからセット－クッキー２（Ｓｅｔ－Ｃｏｏｋｉｅ２）の応答ヘッダを介して到着した状態情報の別々の追跡を保つ。状態情報の値（“Ｃｏｏｋｉｅ”）は、発信源サーバが送るために選択する何かであり得る。セット－クッキー２（Ｓｅｔ－Ｃｏｏｋｉｅ２）の応答ヘッダの内容は、セット－クッキー２（Ｓｅｔ－Ｃｏｏｋｉｅ２）のヘッダを調べる誰かによって読み取り可能であり得る。もし、ユーザ・エージェントが、前以って記憶されていたクッキー（Ｃｏｏｋｉｅ）のものと名前が同じであるセット－クッキー２（Ｓｅｔ－Ｃｏｏｋｉｅ２）の応答ヘッダを受信したならば、新しいクッキー（Ｃｏｏｋｉｅ）は古いものに取って代わる。それが発信源サーバにリクエストを送ったとき、ユーザ・エージェントは、リクエストに適用可能なクッキーを記憶していたならば、クッキー・リクエスト・ヘッダを含んでいる。
【０００５】
この既知の方法の問題は、クライアント・システムが、サーバによって送られたクッキーの新しい値を傍受するエンティティ（存在者）によってなりすまされるのを阻止するための装備を持たないということである。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明の目的は、クライアント・システムになりすますことを試みる何等かのシステムが、発信源のクライアント・システムと同じ状態を維持するのを阻止するのを助けるための特徴を有する上述した型の方法、サーバ、クライアント・システム、及びコンピュータ・プログラムを提供することである。
【課題を解決するための手段】
【０００７】
この目的は、少なくともメッセージに担持された新しい値及びクライアント・システムに維持されるデータを入力として用いて、メッセージの送信後に有効な状態追跡情報の値を計算するようにしたことを特徴とする、本発明による状態追跡機構を履行する方法によって達成される。

【０００８】
該通信セッションの進行中において、クライアント・システムが状態追跡情報の有効値を有する場合にのみクライアント・システムにアクセス可能な形態でアプリケーション・データが提供され、そしてメッセージの送信後に有効な値がクライアント・システムに維持されたデータを入力として用いて計算されるので、該データは、クライアントがアプリケーション・データにアクセスし続けることを必要とされない。アプリケーション・データは、例えば、条件付アクセス・システムによって配分されている暗号化されたコンテントを解読するためのキーを含み得る。データはクライアント・システムに維持されるので、それは状態追跡情報の新しい値を担持するメッセージにおいて送信される必要がなく、従って、新しい値を担持するメッセージの傍受は全く取るに足らないことである。送信後に有効な状態追跡情報の値がクライアント・システムへのメッセージに担持される新しい値も入力として用いて計算されるので、クライアントの状態はサーバによって決定されるものとして展開する。このことは、リプレイ・アタック（replay attacks）に対抗するのを助ける。

【０００９】
本方法の実施形態は、ナンスの形態でクライアント・システムに維持されるデータを得ることを含む。

【００１０】
ナンス、もしくは一度使用されたナンバは、クライアント・システムの認可されないクローン化に対抗するのを助ける。クライアント・システムに維持されるデータもクローンに利用可能であるように、クライアント・システムがクローン化されるすなわち複製されたとしても、次に、クローンはセッションの終りで作用するのをやめる。ナンスのような新しいデータは、サーバとクライアント・システムとの間の新しい通信セッションの開始時に創設され得る。代替的には、ナンスのようなデータは、通信セッションが創設される前にクライアントにおいて予め発生される。

【００１１】
一実施形態においては、ナンスはサーバによって知られている。サーバは、例えば、通信セッションの開始時に、クライアント・システムからのナンスを受信し得る。代替的には、サーバは、通信セッションの開始前にクライアントのナンスに気付いているかも知れない。ナンスは、例えば、ナンスが導出され得るシード（seed：発生源）によってサーバにより知られるかもしれない。

【００１２】
その効果は、ナンスが、クライアント・システムによって発生され得るので、サーバからクライアント・システムに通信される必要がない、ということである。サーバは、クライアント・システムからのナンスに気付いており、それ故、双方の側は、状態追跡情報の有効な値を計算することができる。特に状態追跡情報が一方向性関数もしくは一方向作用である場合に、サーバからクライアント・システムへのメッセージだけを監視することによって状態追跡情報の有効値を得ることは可能ではない。これらのメッセージは、人が、クライアント・システムに維持されるデータを得ることを許容しない。

【００１３】
本方法の実施形態は、計算を実行する際に有効な少なくとも状態追跡情報の値を入力として用いて、メッセージの送信後に有効な状態追跡情報の値及びメッセージに担持された新しい値のうちの少なくとも１つを計算することを含む。

【００１４】
効果は、状態追跡情報の新しい値を担持するメッセージの送信後に有効な状態追跡情報の値が、状態追跡情報の先の有効な値に依存するということである。このことは、通信セッションが、メッセージの送信までのその全期間の間に通信セッションに参加したそれらのシステムの間だけで続くのを確実にするのを助ける。

【００１５】
クライアント・システムには、それぞれの権限付与と関連した暗号化された情報を解読

するために権限付与の識別子の組が与えられるという実施形態は、
識別子の組に対応する権限付与を反映する記録を維持し、そして
クライアント・システムに提供された組における識別子の各々の少なくとも部分に対応するデータをさらなる入力として用いてメッセージの送信後に有効な状態追跡情報の値を計算することを含む。

【００１６】

権限付与の組は、状態追跡機構を履行するサーバによってクライアント・システムに通信される必要が必ずしもない。権限付与は、アプリケーション・データに含まれ得る。クライアント・システムには、状態追跡情報の有効な値を有する場合にアクセス可能な形態でアプリケーション・データが提供されるだけであるということが思い起こされる。従って、この実施形態においては、クライアント・システムは、それに提供される組における識別子の各々の少なくとも部分に対応するデータをさらなる入力として用いてメッセージの送信後に有効な状態追跡情報の値をも計算しなければならない。効果は、クライアント・システムに提供される識別子の組が、サーバに維持される記録の対応の修正なしでは変更されることができないということである。

【００１７】

本方法の実施形態は、サーバとクライアント・システムとの間で通信が行なわれるネットワーク上で、クライアント・システムのネットワーク・アドレスを用いて、好ましくはクライアント・システムによって用いられる装備に結線されたアドレスを用いて、メッセージの送信後に有効な状態追跡情報の値を計算することを含む。

【００１８】

このことは、状態追跡情報の値がサーバのネットワーク場所に関連しているので、中間の人によるアタック（man-in-middle attacks）に対抗するのを助ける。通常の通信プロトコルは、この場所のチェックを許容する。

【００１９】

本方法の実施形態は、サーバによって創設されかつ維持された少なくともナンスを入力として用いてメッセージに担持された新しい値を計算することを含み、ここに、ナンスは通信セッションの開始においてクライアント・システムに送信されるものである。

【００２０】

効果は、クライアント・システムが、ナンスを最初に発生したサーバとだけの通信セッションを維持することを相対的に確かなものにすることができるということである。このことは、クライアント・システムをだましてもう１つのサーバに情報を露出させる試みを未然に防ぐのを助ける。

【００２１】

一実施形態において、アプリケーション・データは、状態追跡情報の有効な値に対応するデータを担持するクライアント・システムからのリクエスト・メッセージの受信時にクライアント・システムに提供される。

【００２２】

従って、クライアント・システムが未だに状態追跡情報の有効値を有しているという１つのチェックの後にアプリケーション・データの複数の送信が行なわれ得る。

【００２３】

一実施形態において、アプリケーション・データは、状態追跡情報の有効な値の少なくとも部分を用いて導出可能なキーのもとで解読を許容するよう暗号化される、暗号化された形態で提供される。

【００２４】

効果は、クライアントによって維持される状態追跡情報の値の継続的なより強いチェックを提供することである。クライアント・システムが、それによって維持される状態追跡情報の値を含むメッセージを送信しない変形例も可能である。クライアントによって維持される状態追跡情報の値の有効性のチェックは、事実上、アプリケーション・データを解読する試みが為されるとき、クライアント・システムにおいて実行される。さらなる効果

は、アプリケーション・データへのアクセスが、クライアント・システムが或る状態にある間隔に制限され得るということである。

【００２５】

一実施形態において、クライアント・システムには、キーのもとで解読を許容するよう暗号化されるコンテント・データの組が提供され、アプリケーション・データはキーの値を含む。

【００２６】

効果は、クライアントが有する状態追跡情報の値の有効性に関するチェックが、コンテント・データの送信ごとには行われる必要がなく、アクセス可能な形態でキーを提供するためにのみ行なわれるということである。このことは、比較的効率的なことであり、なおかつコンテント・データへのアクセスを或る状態におけるクライアント・システムに制限する。

【００２７】

もう１つの態様でよれば、本発明によるサーバ・システムは、データ処理ユニット及びメモリを含み、そして、本発明による状態追跡機構を履行する方法を実行するよう配列されている。

【００２８】

もう１つの態様によれば、本発明による状態追跡機構を履行するサーバで通信セッションを行なう方法は、クライアント・システムに記憶されたデータ及びメッセージにおける少なくとも新しい値を入力として用いて状態追跡情報のさらなる値を計算することと、クライアント・システムに維持された状態追跡情報を該さらなる値によって置き換えることと、を特徴とする。

【００２９】

効果は、サーバからのメッセージにおける状態追跡情報の新しい値の受信時に、状態追跡情報の有効な値が、該データをも記憶するクライアント・システムにおいてのみ得られ得るということである。該データは、メッセージ内には含まれておらず、それ故、サーバからのメッセージを監視することによっては、次の有効な値を得ることができない。

【００３０】

本方法の実施形態は、通信セッションの開始時にナンスの形態でクライアント・システムに記憶されたデータを得ることを含む。

【００３１】

効果は、もしクライアント・システムがデータでクローン化されているならば、該クローンは、現在の通信セッションの終りまで単に機能的なままであるということである。

【００３２】

一実施形態は、好ましくは、通信セッションの開始時に乱数を発生しかつサーバにナンスを通信することにより、クライアント・システムにナンスを発生することを含む。

【００３３】

従って、状態追跡情報の有効な値は、サーバとクライアント・システムとの間の引き続く通信だけを、またはサーバからクライアント・システムへのすべてのメッセージを監視することによって得られることができる。

【００３４】

一実施形態においては、クライアント・システムが、それぞれの権限付与と関連した暗号化された情報を解読するよう権限付与の識別子の組を維持する場合において、当該方法は、

該組内の識別子の各々の少なくとも部分に対応するデータをさらなる入力として用いて状態追跡情報のさらなる値を計算することを含む。

【００３５】

効果は、識別子の組が、状態追跡情報の無効な値に導くことなく変更されることができないということである。状態追跡情報の値が展開するので、このことは、通信セッション全体を通してその場合のままである。

【００３６】
一実施形態において、サーバとクライアント・システムとの間の通信がネットワークを介して行なわれ、クライアント・システムは、好ましくは、クライアント・システムによって用いられる装備に結線されたネットワーク上のアドレスを有する場合において、当該方法は、
ネットワーク・アドレスの少なくとも部分に対応するデータをさらなる入力として用いて状態追跡情報のさらなる値を計算することを含む。
【００３７】
従って、クライアント・システムの状態は、サーバと通信するよう用いられるネットワーク・アドレスに関連している。
【００３８】
本方法の実施形態は、通信セッションの開始時にサーバによって創設されるナンスを担持するメッセージを受信することと、
サーバによって創設された少なくともナンスを入力として用いてサーバからのメッセージにおいて受信された状態追跡情報の新しい値の予想された値を計算することと、
を含み、ここに、状態追跡情報のさらなる値は、予想された値がサーバからのメッセージにおいて受信された値と一致するということを判断したときにのみ計算される。
【００３９】
効果は、通信セッションが同じサーバと共に留まるということを確認するためにチェックが行なわれるということである。
【００４０】
本方法の実施形態は、メッセージの受信時にクライアント・システムに維持された状態追跡情報の少なくとも値を入力として用いてサーバからのメッセージにおいて受信された状態追跡情報の新しい値の予想された値を計算することを含み、
ここに、状態追跡情報のさらなる値は、予想された値がサーバからのメッセージにおいて受信された値と一致するということを判断したときにのみ計算される。
【００４１】
効果は、サーバから表面的に受信されたメッセージがクライアント・システムの状態の展開の追跡を保つサーバと同じサーバからのものであるということをクライアント・システムがチェックすることができるということである。
【００４２】
本方法の実施形態は、クライアント・システムに維持された状態追跡情報の少なくとも部分に対応するデータを含むメッセージを送ることにより、アプリケーション・データの送信を要求することを含む。
【００４３】
効果は、クライアント・システムが、アプリケーション・データを受信するために正しい状態にあるということをサーバに対して立証するということである。そのときだけアプリケーション・データは送信され、このことは、認可されないクライアント・システムに対する不必要な送信を避けるのを助ける。
【００４４】
本方法の実施形態は、
暗号化された形態でアプリケーション・データを受信することと、
暗号化されたアプリケーション・データを解読するためのキーを導出するためにクライアント・システムに維持された状態追跡情報を用いることと、を含む。
【００４５】
効果は、クライアント・システムがアクセス可能な形態でアプリケーション・データを得ることを試みる度にクライアント・システムの状態に関するチェックがクライアント・システムにおいて行なわれることである。
【００４６】
一実施形態は、

暗号化されたコンテント・データのストリームを受信することと、
サーバから受信されたアプリケーション・データから暗号化されたコンテント・データを解読するためにキーを得ることと、を含む。

【００４７】

該実施形態は、条件付アクセス・システムまたはディジタル権利管理システムにおける状態追跡機構の履行を表わす。

【００４８】

もう１つの態様によれば、本発明によるクライアント・システムは、データ処理ユニット及びメモリを含み、そして本発明によるサーバとの通信セッションを行なう方法を行うよう配列されている。

【００４９】

本発明のもう１つの態様によれば、機械読取り可能な媒体に組み込まれたとき、情報処理能力を有するシステムに、本発明による方法を行なわせることができる一組の命令を含むコンピュータ・プログラムが提供される。

【００５０】

以下、添付部面を参照して本発明を一層詳細に説明する。

【発明を実施するための最良の形態】

【００５１】

サーバ・システム１は、クライアント・システム２との通信セッションにおいて状態追跡機構を履行する。データは、ネットワーク３、代表的にはワイド・エリア・ネットワーク（ＷＡＮ）を介して交換される。ネットワーク３は、幾つかの異なった種類のネットワーク、例えば、光、ワイアレス、衛星または公衆交換電話網のネットワークを含み得る。状態追跡機構は、サーバ・システム１からクライアント・システム２に通信が一方向である形態で履行され得る。ここに説明する最も入念な実施形態においては、データは双方向に送信される。

【００５２】

例において、クライアント・システム２には、ネットワーク・インターフェース４と、バスへのインターフェース５とが設けられ、バスは、中央処理装置６と主メモリ７と記憶媒体９へのインターフェース８とを相互接続する。インターフェース５は、さらに、ビデオ・プロセッサ１０及びオーディオ・プロセッサ１１への接続を提供する。クライアント・システム２は、パーソナル・コンピュータ、ゲーム・コンソール、セットトップ・ボックス、または同様の装置を表わし得る。それには、スマート・カードのようなアクセス・トークンへのインターフェース（図示せず）が提供され得る。代替的には、クライアント・システム２にインストールされるまたは一時的に記憶されるソフトウェアのセキュア（保証）ピースがアクセス・トークンとして機能し得る。ソフトウェアのこのようなセキュア（保証）ピースは、エンジニアを入れ替えるのが困難な、分かりにくくされたコンピュータ・プログラム・コードの形態で提供され得る。

【００５３】

クライアント・システム２には、さらに、該クライアント・システム２がサーバ・システム１と通信セッションを行なうのを可能とするクライアント・ソフトウェア・モジュールが設けられる。該クライアント・ソフトウェア・モジュールは、サーバ・システム１が状態追跡の形態を履行するのを可能とするサーバ・システム１で走行するソフトウェアと協働する。クライアント・システム２は、クライアント・システム上で走行するコンテント・データ・デコーディング・アプリケーションのためのアプリケーション・データを得るためにかかる通信セッションをセットアップする。アプリケーション・データは、クライアント・システム２が、サーバ・システム１から、ネットワーク２に属されたもう１つのサーバから、または携帯記憶媒体から受信し得る、オーディオ及び／またはビデオ・データの或るストリームを解読し、かつデコーディングするための権利の付与の識別子を含む。権利の付与のこのような識別子は、アクセス・トークンとして機能する装置またはソフトウェア・モジュールに記憶される。アプリケーション・データは、さらに、コンテン

ト・データを解読するための暗号化キーを含む。クライアント・システムは、また、コンテント・データの暗号化されたセットへのアクセスを得るためにディジタル権利管理（ＤＲＭ）システムを履行するためのアプリケーションをも含み得ることに留意されたし。このようなアプリケーションに向けられるアプリケーション・データは、暗号化されたディジタル権利対象を含み、その各々は、クライアント・システムがアクセスするための権限を与えられた一組のコンテント・データを識別する。

【００５４】

クライアント・システム２には、それが状態追跡情報の有効値、この例においては状態変数ＳＶを有するならば、アクセス可能な形態でアプリケーション・データが提供される。クライアント・システムの容易なクローニングを避けるために、状態変数ＳＶは、クライアント・システム２のセキュア（保証）要素、例えば、アクセス・トークンに記憶され得る。クライアント・システム２には、クライアント・システムが現在の有効な状態変数ＳＶを有するか否かにかかわらず、暗号化された形態でアプリケーション・データが提供され得、該アプリケーション・データは、有効状態変数ＳＶが存在する場合にのみ解読可能である。さらにもしくは代替的には、アプリケーション・データは、クライアント・システム２が現在の有効状態変数を有するということを立証した場合にのみ、サーバ・システム１からクライアント・システム２に転送され得る。

【００５５】

状態変数ＳＶは、サーバ・システム１の命令で一定の間を置いて変化される。このため、それは、状態変数ＳＶの新しい値を担持するメッセージをクライアント・システム２に送る。状態変数の値における変化の後、クライアント・システム２の任意のコピーが中止して、アクセス可能な形態でアプリケーション・データが提供されるであろう。このようなコピーも状態変数の新しい値を担持するメッセージを受信するべきであるとしても、クライアント・システム２に維持されたデータの値をも有さなければならないであろう。これは、状態変数ＳＶの新しい値を担持するメッセージの送信後に有効な状態変数の値が、少なくともメッセージに担持された新しい値及びクライアント・システム２に維持されたデータを入力として用いて、クライアント・システム２によって計算されるからである。

【００５６】

クライアント・システム２に維持されたデータは、各通信セッションの開始において新たに創設される。それは、１つの通信セッションに対してのみ有効であり、当該の通信セッションに対して独特の値を有する。それは、ワンタイム・パッド（一回限り暗号帳）から得られ得る。クライアント・システムのクローニングに対する追加された保護のために、クライアント・システムは、例えば乱数としてデータを発生し得る。

【００５７】

図２Ａ及び図２Ｂは、状態追跡機構を一層詳細に示す。示された動作が実行される間、クライアント・システム２には、クライアント・システムが状態追跡情報の有効値を有する場合にのみ、アクセス可能な形態でアプリケーション・データが連続的に提供されるということを、図は示していない。

【００５８】

クライアント・システム２は、第１のステップ１２において、クライアント・ナンスＮｃ、上述で言及したデータ、を発生する。それは、次に（ステップ１３）、状態変数ＳＶの第１の値を発生する。状態変数ＳＶの第１の値は、クライアント・システム２によって選択された任意値であって良い。それは、また、クライアント・システム２によってランダムに選択された値の関数であっても良く、そして特にクライアント・ナンスＮｃを含む１つ以上の他の変数であっても良い。

【００５９】

クライアント・システム２は、新しい通信セッションを創設するために、サーバ・システム１にリクエスト・メッセージを送る（ステップ１４）。リクエスト・メッセージは、クライアント・ナンスＮｃ及び状態変数ＳＶの第１の値を含む。

【００６０】

サーバ・システム１は、リクエスト・メッセージを受信する（ステップ１５）。クライアント・ナンスＮｃは、通信セッションの開始時にクライアント・システム２からサーバ・システム１によって受信され、その理由は、それが、リクエスト・メッセージに含まれており、このメッセージからサーバ・システム１によって検索される（ステップ１６）からである。リクエスト・メッセージは、さらに、サーバ・システムが、リクエストされたアプリケーション・データを受信するために、クライアントの権限の初期の確認を実行するのを可能とするデータを含み得る。

【００６１】

リクエスト・メッセージの受信後、サーバ・システム１は、サーバ・システム１によって創設され（ステップ１８）かつ維持された少なくともサーバ・ナンスＮｓを入力として用いて新しい状態変数値を計算する（ステップ１７）。サーバ・ナンスＮｓは、通信セッションの期間の間サーバ・システム１におけるメモリ内に保持されるが、引き続いては用いられない。サーバ・ナンスＮｓは、乱数に基づき得る。サーバ・ナンスＮｓは、通信セッションの開始時に、すなわち、クライアント・システムのリクエスト・メッセージに応答して送られた（ステップ１９）応答メッセージにおいて、クライアント・システム２に通信される。応答メッセージに担持された新しい状態変数値は、計算を行なうときに有効な少なくとも状態追跡情報の値、すなわち、リクエスト・メッセージにおいて受信された値を、さらなる入力として用いて計算される。このことは、現在有効な値が常にすべての先の値、並びにサーバ・ナンスＮｓ及びクライアント・ナンスＮｃに依存しているという意味において、状態変数値を連鎖させる。

【００６２】

上述したように、クライアント・システム２は、それぞれの権限と関連した暗号化された情報を解読するために、利用可能な一組の権限の識別子を有する。サーバ・システム１は、クライアント・システム２によって格納された一組の識別子に対応する権限を反映する記録を維持する。応答メッセージに含まれるべき新しい状態変数値を計算する際、サーバ・システム１は、クライアント・システム２に提供される一組内の識別子の各々の少なくとも部分に対応するデータをさらなる入力として用いる。

【００６３】

サーバ・システム１は、また、クライアント・システム２のネットワーク・アドレス、好ましくはＭＡＣアドレスのようなネットワーク・インターフェース４内にハード結線されたアドレスを、新しい状態変数値を計算するために用いられるアルゴリズムへの入力として用いる。アドレス値は、代替的には、インターネット・プロトコル（ＩＰ）であって良い。

【００６４】

新しい状態変数値を計算するために用いられるアルゴリズムは、落とし戸関数（トラップドア（ｔｒａｐｄｏｏｒ）関数）としても知られている、強いまたは弱い一方向性関数であって良い。効果は、サーバ・システム１とクライアント・システム２との間で交換される状態変数値だけから、サーバ・ナンスＮｓ及びクライアント・ナンスＮｃを計算するのが困難であるということである。該アルゴリズムは、ハッシュ関数を含み得る。

【００６５】

クライアント・システム２は、サーバ・システム１から応答メッセージにおける状態変数ＳＶの新しい値を受信する（ステップ２０）。状態変数ＳＶの新しい値は、応答メッセージから検索される（ステップ２１）。しかしながら、それは、クライアント・システム２における有効値として先に維持された状態変数の値を直接には交換しない。

【００６６】

クライアント・システム２によって受信された応答メッセージは、また、通信セッションの開始時にサーバによって創設されたサーバ・ナンスＮｓを担持する。クライアント・システム２は、応答メッセージからサーバ・ナンスＮｓを検索する（ステップ２２）。それは、入力として少なくともサーバ・ナンスＮｓを用いてサーバ・システム１から応答メッセージにおいて受信された状態変数の新しい値の予想される値を計算する（ステップ２

３）が、また、ステップ１３において発生されクライアント・システム２において維持された状態変数値、並びにクライアント・システム２のネットワーク・アドレス及び権限付与識別子の組も計算する（ステップ２３）。

【００６７】

計算され予想された値が、サーバ・システム１からの応答メッセージにおいて受信された状態変数値と一致するならば、次に、クライアント・システム２は、応答メッセージにおける新しい値及びクライアント・システムにおいて格納されたデータ、すなわち、クライアント・ナンスＮｃ、並びにクライアント・システム２のネットワーク・アドレス及び権限付与識別子の組を入力として用いて、状態追跡情報のさらなる値を計算するよう進行する。さらなる値は、クライアント・システム２に維持された状態変数値を置換え、そしてクライアント・システム２がアクセス可能な形態でアプリケーション・データを受信するよう権限付けられるということを確定するように用いられる。

【００６８】

サーバ・システム１は、また、少なくともメッセージ内に担持された新しい値及びクライアント・ナンスＮｃを入力として用いる応答メッセージの送信の後に有効な状態追跡情報の値を計算する（ステップ２５）。このことは、サーバ・システム１が、クライアント・システム２にアクセス可能形態でアプリケーション・データを提供する際、クライアント・システム２の状態をチェックするのを許容する。

【００６９】

通信セッションの進行中、クライアント・システム２はさらなるリクエスト・メッセージを送り得る（ステップ２６）。これらは、クライアント・システム２において維持された状態変数ＳＶの値の少なくとも部分に対応するデータを含む。リクエスト・メッセージの各々または幾つかだけに応答して、サーバ・システム１は、図２Ｂに示されたステップを実行するであろう。

【００７０】

リクエスト・メッセージを受信する（ステップ２７）と、サーバ・システム１は、リクエスト・メッセージに担持された状態変数の値を検索する（ステップ２８）。検索された値が、ステップ２５で計算された予想された値と一致するならば、サーバ・システム１は、新しい状態変数の値を発生する（ステップ２９）。

【００７１】

新しい状態変数の値は、今まで有効な状態変数の値、サーバ・ナンスＮｓ、権限付与識別子の組、及びクライアント・システム２のネットワーク・アドレスを入力として用いて、以前のように計算され得る。新しい状態変数の値は、クライアント・システム２にさらなる応答メッセージにおいて送られる（ステップ３０）。再度、状態変数の次の有効な値は、ステップ３０で送られた新しい状態変数の値及びクライアント・ナンスＮｃ、並びにクライアント・システム２に提供される識別子の組に対応する暗号化された情報を解読するために権限付与に反映する記録に基づくデータを入力として用いて計算される（ステップ３１）。

【００７２】

サーバ・システム１は、アプリケーション・データのための引き続くリクエストが、次の有効な値として計算される状態変数ＳＶの値を含む場合にのみ、アプリケーション・データを提供するよう配列され得る。さらにまたは代替的に、サーバ・システム１は、次の有効な値を有するクライアント・システムだけがアプリケーション・データを解読することができるように、状態変数の次の有効な値に基づくキーでアプリケーション・データを暗号化するためのシステムを提供し得る。

【００７３】

クライアント・システム２は、さらなる応答メッセージを受信する（ステップ３２）。それは、入力として少なくともサーバ・ナンスＮｓ及び予め有効な状態変数値を用いてサーバ・システム１からさらなる応答メッセージにおいて受信された状態追跡情報の新しい値の予想された値を計算する（ステップ３３）。それは、また、サーバ・システム１から

さらなる応答メッセージにおいて実際に受信された状態変数ＳＶの新しい値を検索する（ステップ３４）。予想された値が、サーバ・システム１からメッセージにおいて受信された値と一致することを決定すると、状態追跡情報のさらなる値が計算される（ステップ３５）。これは、クライアント・システム２へのさらなる応答メッセージの送信後に有効である状態変数の値である。

【００７４】

さらなる値が、クライアント・ナンスＮｓ、並びにさらなる応答メッセージに担持される値に基づいているので、さらなる応答メッセージに担持された値をコピーすることは、オリジナルのクライアント・システム２と同じ状態にクライアント・システム２の違法のクローンを置くためには充分でない。

【００７５】

本発明は、上述の実施形態に制限されるものではなく、特許請求の範囲内で変化し得るものである。例えば、サーバ・システム１によって計算され、応答メッセージにおいてクライアント・システム１に送信される状態変数の新しい値は、状態変数の次の有効な値を計算するためにクライアント・システム２によって用いられる入力に必ずしも基づく必要はない。リクエスト・メッセージ及び／または応答メッセージは、例えば、当該のメッセージの受信前に有効である状態変数の値から導出されるキーのもとに暗号化され得る。

【図面の簡単な説明】

【００７６】

【図１】状態追跡機構を履行するためのクライアント・システム及びサーバを示す概略図である。

【図２Ａ】状態追跡機構の実施形態における動作及び目的フローを示す能動的な図である。

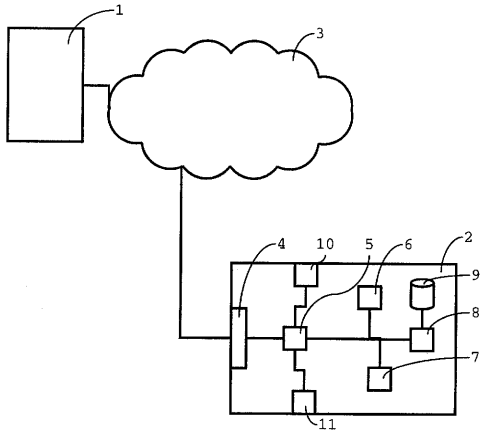
【図２Ｂ】状態追跡機構の実施形態における動作及び目的フローを示す能動的な図である。

【符号の説明】

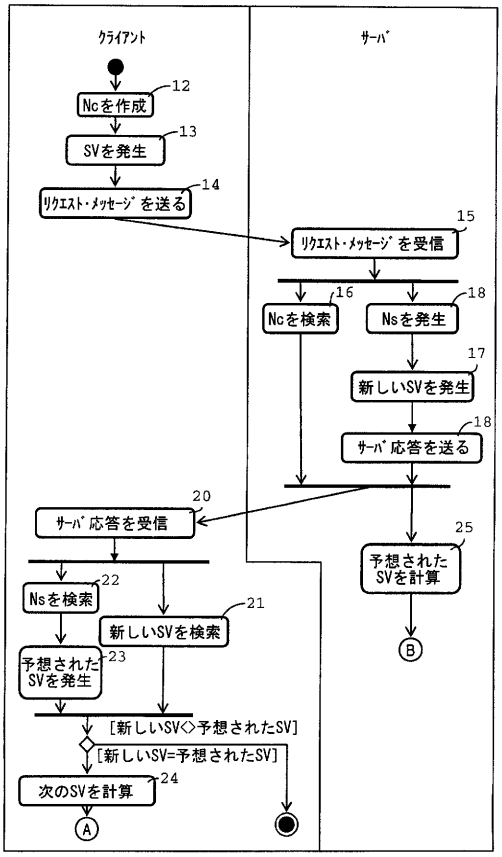
【００７７】

１　サーバ・システム
２　クライアント・システム
３　ネットワーク
４　ネットワーク・インターフェース
５　インターフェース
６　中央処理装置
７　主メモリ
８　インターフェース
９　記憶媒体
１０　ビデオ・プロセッサ
１１　オーディオ・プロセッサ

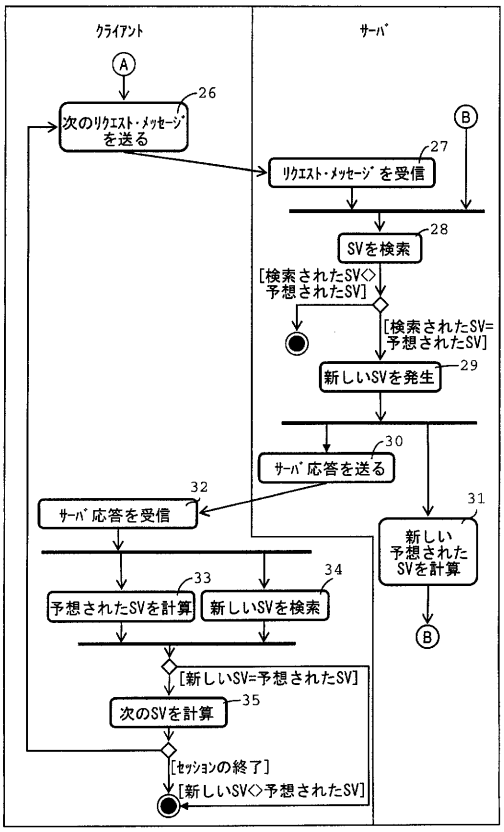
【図１】


1
3
4
10
5
6
2
9
8
7
11

【図２Ａ】


ｸﾗｲｱﾝﾄ
ｻｰﾊﾞ
Ncを作成
12
SVを発生
13
ﾘｸｴｽﾄ･ﾒｯｾｰｼﾞを送る
14
ﾘｸｴｽﾄ･ﾒｯｾｰｼﾞを受信
15
Ncを検索
16
Nsを発生
18
新しいSVを発生
17
ｻｰﾊﾞ応答を送る
18
ｻｰﾊﾞ応答を受信
20
予想された
SVを計算
25
Nsを検索
22
新しいSVを検索
21
予想された
SVを発生
23
[新しいSV◇予想されたSV]
[新しいSV=予想されたSV]
次のSVを計算
24
A
B

【図２Ｂ】


ｸﾗｲｱﾝﾄ
ｻｰﾊﾞ
A
次のﾘｸｴｽﾄ･ﾒｯｾｰｼﾞ
を送る
26
B
ﾘｸｴｽﾄ･ﾒｯｾｰｼﾞを受信
27
SVを検索
28
[検索されたSV◇
予想されたSV]
[検索されたSV=
予想されたSV]
新しいSVを発生
29
ｻｰﾊﾞ応答を送る
30
ｻｰﾊﾞ応答を受信
32
新しい
予想された
SVを計算
31
予想されたSVを計算
33
新しいSVを検索
34
B
[新しいSV=予想されたSV]
次のSVを計算
35
[ｾｯｼｮﾝの終了]
[新しいSV◇予想されたSV]

フロントページの続き

審査官　▲吉▼田　耕一

(56)参考文献　特開２００５－３０１４４９（ＪＰ，Ａ）
特開２００５－１０２１６３（ＪＰ，Ａ）
特表２００１－５０９２９５（ＪＰ，Ａ）
特開平１０－０５１４８９（ＪＰ，Ａ）
特開２００６－１１５３１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０