(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2016-100007
(P2016-100007A)
(43)公開日　平成28年5月30日(2016.5.30)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/44	(2013.01)	G06F	21/44	
G06F 21/12	(2013.01)	G06F	21/12	

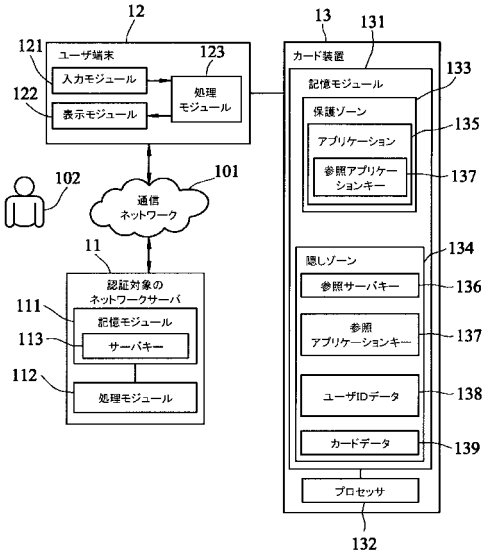
審査請求 有　請求項の数 13　ＯＬ　外国語出願　（全 14 頁）

(21)出願番号　特願2015-217335 (P2015-217335)
(22)出願日　平成27年11月5日 (2015.11.5)
(31)優先権主張番号　103141025
(32)優先日　平成26年11月26日 (2014.11.26)
(33)優先権主張国　台湾 (TW)

(71)出願人　509262068
周　宏建
台湾台中市南屯區永春東路１０００號之１９（１２樓）
(74)代理人　110000796
特許業務法人三枝国際特許事務所
(72)発明者　周　宏建
台湾台中市南屯區永春東路１０００號之１９（１２樓）

(54)【発明の名称】カード装置を用いたネットワーク認証方法

(57)【要約】　（修正有）
【課題】ネットワークトランザクションに関係するネットワークサーバおよびアプリケーションの安全な認証を保証する、ネットワーク認証方法を提供する。
【解決手段】ユーザ端末１２は、アプリケーションの実行を通じて、ネットワークサーバに接続し、ユーザ端末１２に接続されたカード装置１３にサーバ検証リクエストを送信する。カード装置１３は、サーバ検証コードに基づいてサーバ・ダイナミックリンクプログラムを生成し、さらに暗号化し、ユーザ端末１２を通じて、暗号化されたサーバ・ダイナミックリンクプログラムをネットワークサーバに送信する。ユーザ端末１２は、サーバ・ダイナミックリンクプログラムに基づいて、ネットワークサーバによって生成されるサーバコードデータを、ネットワークサーバから受け取ってカード装置１３に送信する。カード装置１３は、サーバコードデータとサーバ検証コードとに基づいて、ネットワークサーバを検証する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ユーザ端末(12)と前記ユーザ端末(12)に接続されたカード装置(13)とを含む端末装置を使用してインプリメントされる、少なくとも認証対象のネットワークサーバ(11)を認証するためのネットワーク認証方法であって、前記カード装置(13)が、特定のネットワークサーバと前記ユーザ端末(12)との間のネットワークトランザクションに関係しているアプリケーションと、前記特定のネットワークサーバに関係している参照サーバキー(136)とを格納しており、
前記ネットワーク認証方法が、
前記ユーザ端末(12)によるステップA)であり、前記アプリケーションの実行を通じて、通信ネットワーク(101)を越えて、前記認証対象のネットワークサーバ(11)と通信リンクを確立し、サーバ検証リクエストを前記カード装置(13)に送信する、ステップA)と、
前記カード装置(13)によるステップB)であり、前記ユーザ端末(12)からの前記サーバ検証リクエストを受け取ると、前記特定のネットワークサーバに対応するサーバ検証コードに少なくとも基づいて、サーバ・ダイナミックリンクプログラムを生成し、前記参照サーバキー(136)を用いて前記サーバ・ダイナミックリンクプログラムを暗号化し、それによって暗号化された前記サーバ・ダイナミックリンクプログラムを、前記ユーザ端末(12)に送信するステップB)と、
前記ユーザ端末(12)によるステップC)であり、前記アプリケーションの前記実行を通じて、前記カード装置(13)によって生成されて暗号化された前記サーバ・ダイナミックリンクプログラムを、前記通信ネットワーク(101)を介して前記ネットワークサーバに送信するステップC)と、
前記ユーザ端末(12)によるステップD)であり、前記サーバ・ダイナミックリンクプログラムに基づいて、前記認証対象のネットワークサーバ(11)によって生成されるサーバコードデータを、前記通信ネットワーク(101)を介して、前記認証対象のネットワークサーバ(11)から受け取ると、それによって受け取った前記サーバコードデータを、前記アプリケーションの前記実行を通じて、前記カード装置(13)に送信するステップD)と、
前記カード装置(13)によるステップE)であり、前記ユーザ端末(12)からの前記サーバコードデータと前記ステップB)における前記サーバ検証コードとの間の関係に基づいて、前記認証対象のネットワークサーバ(11)が前記特定のネットワークサーバか否かを検証するステップE)と、
を含む、ネットワーク認証方法。
【請求項２】
ステップB)において、前記サーバ検証コードはワンタイム・コードである、請求項1に記載のネットワーク認証方法。
【請求項３】
ステップE)において、前記カード装置(13)によって、前記サーバコードデータが前記サーバ検証コードに一致すると判定される場合、前記カード装置(13)によって、前記認証対象のネットワークサーバ(11)が前記特定のネットワークサーバであると検証される、請求項1に記載のネットワーク認証方法。
【請求項４】
ステップE)の後にさらに、
ステップF)であり、前記カード装置(13)によって、前記認証対象のネットワークサーバ(11)が前記特定のネットワークサーバであると検証される場合、前記通信ネットワーク(101)を介して、前記ユーザ端末(12)を通じて、前記認証対象のネットワークサーバ(11)の検証の成功を、前記認証対象のネットワークサーバ(11)に通知するステップF)を含む、請求項1に記載のネットワーク認証方法。
【請求項５】
ステップB)において、前記サーバ・ダイナミックリンクプログラムが、前記サーバ検証コードと、前記カード装置(13)によってランダムに提供されるワンタイム・サーバキーと

に基づいて、前記カード装置(13)によって生成され、
ステップE)の後にさらに、
ステップF')であり、前記カード装置(13)によって、前記サーバコードデータが前記サーバ検証コードに一致すると判定される場合、前記ワンタイム・サーバキーを用いて、そこに格納されている前記参照サーバキー(136)を更新し、前記通信ネットワーク(101)を介して、前記ユーザ端末(12)を通じて、前記ネットワークサーバの検証の成功を、前記認証対象のネットワークサーバ(11)に通知するステップF')を含む、請求項1に記載のネットワーク認証方法。
【請求項６】
前記認証対象のネットワークサーバ(11)の検証の成功の通知によって、前記認証対象のネットワークサーバ(11)が、前記ワンタイム・サーバキーを用いて、予めそこに格納されているサーバキー(113)を更新することが可能となる、請求項5に記載のネットワーク認証方法。
【請求項７】
前記カード装置(13)がさらに、特定のユーザ同一性に対応するユーザIDデータを格納し、
ステップE)の後にさらに、
ステップH)であり、前記カード装置(13)によって、前記サーバコードデータが前記サーバ検証コードに一致すると判定される場合、ユーザ同一性検証リクエストを前記ユーザ端末(12)に送信するステップH)と、
前記ユーザ端末(12)によるステップI)であり、前記カード装置(13)からの前記ユーザ同一性検証リクエストの受け取りに応じて、前記ユーザ端末(12)によって生成される、検証対象のユーザによって行なわれた入力操作に対応する入力データを前記カード装置(13)に送信するステップI)と、
前記カード装置(13)によるステップJ)であり、前記ユーザ端末(12)からの前記入力データと、そこに格納されている前記ユーザIDデータとの関係に基づいて、前記検証対象のユーザの前記同一性を検証するステップJ)と、
を含む、請求項1に記載のネットワーク認証方法。
【請求項８】
ステップJ)において、前記カード装置(13)によって、前記入力データが前記ユーザIDデータに一致すると判定される場合、前記検証対象のユーザの前記同一性が前記特定のユーザ同一性であると検証される、請求項7に記載のネットワーク認証方法。
【請求項９】
前記カード装置(13)がさらに、前記アプリケーション内に含まれている参照アプリケーションキー(137)を格納し、
ステップA)の前にさらに、
前記カード装置(13)によるステップi)であり、前記カード装置(13)内に格納されている前記アプリケーションに対応するアプリケーション検証コードに基づいて、アプリケーション・ダイナミックリンクプログラムを生成し、前記参照アプリケーションキーを用いて前記アプリケーション・ダイナミックリンクプログラムを暗号化するステップi)と、
ステップii)であり、アプリケーションキーを含んでおり、前記ネットワークトランザクションに関係しているアプリケーションの受け取りの後、前記ユーザ端末(12)によって、それによって受け取った前記アプリケーションの実行を通じて、前記カード装置(13)によって暗号化された前記アプリケーション・ダイナミックリンクプログラムを前記カード装置(13)から取得し、それによって実行される前記アプリケーションに含まれている前記アプリケーションキーと、それによって取得した前記アプリケーション・ダイナミックリンクプログラムとに基づいて、アプリケーションコードデータを生成し、それによって生成された前記アプリケーションコードデータを前記カード装置(13)に送信するステップii)と、
前記カード装置(13)によるステップiii)であり、前記ユーザ端末(12)からの前記アプリ

ケーションコードデータと前記アプリケーション検証コードとの前記関係に基づいて、前記ユーザ端末(12)によって実行された前記アプリケーションを検証するステップiii)と、を含み、

ステップA)は、ステップiii)において検証が成功した後にのみ行なわれる、請求項1に記載のネットワーク認証方法。

【請求項１０】

ステップi)において、前記アプリケーション検証コードはワンタイム・コードである、請求項9に記載のネットワーク認証方法。

【請求項１１】

ステップiii)において、前記アプリケーションコードデータが前記アプリケーション検証コードに一致する判定される場合、前記ユーザ端末(12)によって実行された前記アプリケーションが前記カード装置(13)内に格納されている前記アプリケーションであると成功裡に検証される、請求項9に記載のネットワーク認証方法。

【請求項１２】

ステップiii)とステップA)との間にさらに、

ステップiv)であり、前記カード装置(13)によって、前記アプリケーションコードデータが前記アプリケーション検証コードに一致すると判定される場合、ワンタイム・アプリケーションキーを用いて、そこに格納されており、そこに格納されている前記アプリケーションに含まれている前記参照アプリケーションキー(137)を更新するステップiv)を含む、請求項9に記載のネットワーク認証方法。

【請求項１３】

ステップii)が、

前記ユーザ端末(12)によって、前記アプリケーションキーを用いて、前記カード装置(13)から取得した前記アプリケーション・ダイナミックリンクプログラムを解読するサブステップと、

前記ユーザ端末(12)によって、このように解読された前記アプリケーションを実行し、前記アプリケーションコードデータを生成するサブステップと、

を含む、請求項9に記載のネットワーク認証方法。

【発明の詳細な説明】

【技術分野】

【０００１】

（関連する出願の相互参照）

本出願は、2014年11月26日に出願された台湾出願第103141025号の優先権を主張し、その全開示は参照によって本明細書に組み込まれる。

【０００２】

本開示はネットワーク認証方法に関し、より詳細には、カード装置を用いたネットワーク認証方法に関する。

【背景技術】

【０００３】

技術の発展および進歩とともに、オンラインショッピングまたはエレクトロニック・コマース(電子商取引)は、近年、商品を購入する消費者にとってポピュラーかつ便利な方法になった。

【０００４】

購入者は、オンラインショッピングまたは電子商取引の支払処理をするために、典型的には、クレジットカードおよびデビットカードのような支払カードを使用する。しかしながら、そのような支払方法において、購入者によって入力されたクレジットカードまたはデビットカードの番号およびパスワードは、支払処理の間にハッカーによって盗まれる可能性がある。したがって、従来の支払カードにとって、セキュリティは大きな問題である。

【０００５】

関連する先行技術は特許文献１である。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】台湾特許第I465094号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
したがって、本開示の目的は、ネットワークトランザクションに関係しているネットワークサーバおよびアプリケーションの安全な認証を保証することができる、カード装置を用いたネットワーク認証方法を提供することである。
【課題を解決するための手段】
【０００８】
本開示によると、ユーザに関連したユーザ端末と、ユーザ端末に接続されたカード装置と、少なくともネットワークサーバを認証するためのネットワークサーバとを使用してインプリメントされるネットワーク認証方法が提供される。カード装置は、特定のネットワークサーバとユーザ端末との間のネットワークトランザクションに関係しているアプリケーションと、特定のネットワークサーバに関係している参照サーバキーとを格納している。ネットワーク認証方法は、
ユーザ端末によるステップA)であり、成功裡に検証されたアプリケーションの実行を通じて、通信ネットワークを越えて、ネットワークサーバと通信リンクを確立し、サーバ検証リクエストをカード装置に送信するステップA)と、
カード装置によるステップB)であり、ユーザ端末からのサーバ検証リクエストを受け取ると、特定のネットワークサーバに対応するサーバ検証コードに少なくとも基づいて、サーバ・ダイナミックリンクプログラムを生成し、参照サーバキーを用いてサーバ・ダイナミックリンクプログラムを暗号化し、それによって暗号化されたサーバ・ダイナミックリンクプログラムをユーザ端末に送信するステップB)と、
ユーザ端末によるステップC)であり、アプリケーションの実行を通じて、カード装置によって生成されて暗号化されたサーバ・ダイナミックリンクプログラムを、通信ネットワークを介してネットワークサーバに送信するステップC)と、
ネットワークサーバによるステップD)であり、通信ネットワークを介してサーバ・ダイナミックリンクプログラムを受け取ると、サーバキーとそれによって受け取ったサーバ・ダイナミックリンクプログラムとに基づいて、サーバコードデータを生成し、通信ネットワークを介して、サーバコードデータをユーザ端末に送信するステップD)と、
ユーザ端末によるステップE)であり、通信ネットワークを介してサーバコードデータを受け取ると、アプリケーションの実行を通じて、それによって受け取ったサーバコードデータをカード装置に送信するステップE)と、
カード装置によるステップF)であり、ユーザ端末からのサーバコードデータとステップB)におけるサーバ検証コードとの間の関係に基づいて、ネットワークサーバを検証するステップF)と、を含む。
【０００９】
本開示の他の特徴および利点は、添付の図面を参照する以下の実施形態の詳細な説明において明白になるであろう。
【図面の簡単な説明】
【００１０】
【図１】本開示に係るネットワーク認証方法の実施形態をインプリメントするために構成されるネットワーク認証装置を示す概略ブロック図である。
【図２】本開示の実施形態に係るネットワーク認証方法のアプリケーション検証手続を示すフローチャートである。
【図３Ａ】本開示の実施形態に係るネットワーク認証方法のネットワークサーバ検証手続

を示すフローチャートである。
【図３Ｂ】本開示の実施形態に係るネットワーク認証方法のネットワークサーバ検証手続を示すフローチャートである。
【図４】本開示の実施形態に係るネットワーク認証方法のユーザ同一性検証手続を示すフローチャートである。
【発明を実施するための形態】
【００１１】
図1を参照すると、本開示に係るネットワーク認証方法の実施形態をインプリメントするために端末装置が使用される。端末装置は、携帯電話やタブレットコンピュータ等のようなユーザ端末12と、カード装置13とを含んでいる。
【００１２】
ユーザ端末12は、インターネットのような通信ネットワーク101と接続することができ、入力モジュール121と、表示モジュール122と、入力モジュール121および表示モジュール122に接続された処理モジュール123とを含んでいる。
【００１３】
Secure Digital(SD)カードのようなカード装置13はユーザ端末12に接続され、記憶モジュール131と、記憶モジュール131に接続されたプロセッサ132とを含んでいる。
【００１４】
カード装置13の記憶モジュール131は、保護ゾーン133および隠しゾーン134を含んでいる。この実施形態では、ユーザ端末12の処理モジュール123には、保護ゾーン133への読み取り専用のアクセスが与えられ、プロセッサ132には、保護ゾーン133および隠しゾーン134への読み取りおよび書き込みアクセスが与えられる。保護ゾーン133は、ユーザ端末12により実行可能なアプリケーション135を格納するように構成される。アプリケーション135は、特定のネットワークサーバとユーザ端末12との間のネットワークトランザクションに関係している。アプリケーション135が参照アプリケーションキー137を含むことに注目されたい。隠しゾーン134は、特定のネットワークサーバに関連した参照サーバキー136と、参照アプリケーションキー137と、特定のユーザ同一性に対応するユーザIDデータ138と、クレジットカードまたはデビットカード番号のようなカードデータ139とを格納するように構成される。
【００１５】
なお、カード装置13の供給者と特定のネットワークサーバの所有者との間に協力関係があることに注目されたい。
【００１６】
次に、添付の図面を用いて、端末装置によってインプリメントされる本開示に係るネットワーク認証方法の実施形態を詳細に示す。ネットワーク認証方法の実施形態は、アプリケーション検証手続と、ネットワークサーバ検証手続と、ユーザ同一性検証手続とを連続して含んでいる。
【００１７】
図1および図2を参照すると、ユーザ端末12およびカード装置13は、本開示に係るネットワーク認証方法の実施形態に係るアプリケーション検証手続をインプリメントするために使用される。アプリケーション検証手続は、ユーザ端末12によって受け取られて実行されるアプリケーションを検証する方法に関係がある。アプリケーションはアプリケーションキーを含んでおり、ネットワークトランザクションに関係している。アプリケーション検証手続は次のステップを含んでいる。
【００１８】
ステップ201において、カード装置13のプロセッサ132は、カード装置13の記憶モジュール131の保護ゾーン133内に格納されているアプリケーション135に対応するアプリケーション検証コードに基づいて、アプリケーション・ダイナミックリンクプログラムを生成し、参照アプリケーションキー137を用いて、アプリケーション・ダイナミックリンクプログラムを暗号化する。この実施形態では、アプリケーション検証コードはワンタイム・コ

ードであるがこれに制限されない。

【００１９】

ステップ202において、アプリケーションの受け取りの後、ユーザ端末12の処理モジュール123は、それによって受け取ったアプリケーションの実行を通じて、プロセッサ132によって暗号化されたアプリケーション・ダイナミックリンクプログラムをカード装置13から取得し、それによって実行されたアプリケーションに含まれているアプリケーションキーと、それによって取得されたアプリケーション・ダイナミックリンクプログラムとに基づいて、アプリケーションコードデータを生成し、それによって生成されたアプリケーションコードデータをカード装置13に送信する。

【００２０】

理想的には、ユーザ端末12が、悪意のあるいかなる第三者からの悪意のある攻撃を受けない場合、ユーザ端末12の処理モジュール123によって実行されるアプリケーションは、カード装置13の記憶モジュール131内に格納されているアプリケーション135と同一のはずであることに言及することは有益である。しかしながら、実際には、ユーザ端末12によって受け取られて実行されたアプリケーションは、ハッカーからの悪意のあるプログラムによって改ざんされている可能性がある。悪意のあるプログラムは、フィッシングサイトにユーザ端末12を誘導することができるか、または、例えばユーザIDデータ138やカードデータ139などのデータをカード装置13から盗むために、ユーザ端末12内に潜伏することができる。したがって、ユーザ端末12の処理モジュール123によって実行されたアプリケーションが、カード装置13の記憶モジュール131内に格納されているアプリケーション135と同一か否かを確認すること、すなわち、ユーザ端末12の処理モジュール123によって受け取られて実行されたアプリケーションが改ざんされているか否かを確認することが、カード装置13について必要である。

【００２１】

ステップ202は、ユーザ端末12の処理モジュール123によって行なわれる次のサブステップを含んでいる:アプリケーションに含まれているアプリケーションキーを用いて、カード装置13から取得したアプリケーション・ダイナミックリンクプログラムを解読するサブステップ;このように解読されたアプリケーション・ダイナミックリンクプログラムの実行を通じて、アプリケーションコードデータを生成するサブステップ。

【００２２】

ステップ202において、ユーザ端末12によって受け取られて実行されたアプリケーションが改ざんされていない場合、すなわち、ユーザ端末12によって受け取られて実行されたアプリケーションが、記憶モジュール131の保護ゾーン133内に格納されているアプリケーション135と同一である場合、アプリケーションに含まれているアプリケーションキーは、したがって、アプリケーション135に含まれておりカード装置13の記憶モジュール131の隠しゾーン134内に格納されている参照アプリケーションキー137と同じである。したがって、カード装置13から取得したアプリケーション・ダイナミックリンクプログラムは、アプリケーションキーを用いて、ユーザ端末12の処理モジュール123によって成功裡に解読される。ユーザ端末12の処理モジュール123によって生成されたアプリケーションコードデータは、アプリケーション検証コードと同じである。

【００２３】

ステップ202において、ユーザ端末12によって受け取られて実行されたアプリケーションが改ざんされている場合、アプリケーションに含まれているアプリケーションキーは、アプリケーション135に含まれておりカード装置13の記憶モジュール131の隠しゾーン134内に格納されている参照アプリケーションキー137と異なっている可能性がある。その結果、カード装置13から取得したアプリケーション・ダイナミックリンクプログラムは、アプリケーションキーを用いて、ユーザ端末12の処理モジュール123によって成功裡に解読されない可能性がある。したがって、ユーザ端末12の処理モジュール123によって生成されたアプリケーションコードデータは、アプリケーション検証コードと異なっている可能性がある。

【００２４】
上記のものを考慮して、ステップ203において、カード装置13のプロセッサ132は、ユーザ端末12から受け取ったアプリケーションコードデータが、ユーザ端末12の処理モジュール123によって実行されたアプリケーションを検証するためのアプリケーション検証コードに一致するか否かを判定する。カード装置13のプロセッサ132が、アプリケーションコードデータがアプリケーション検証コードに一致すると判定する場合、アプリケーションは、カード装置13によって、記憶モジュール131の保護ゾーン133内に格納されているアプリケーション135であると成功裡に検証される。それゆえにフローはステップ204に移る。一方で、カード装置13のプロセッサ132が、アプリケーションコードデータがアプリケーション検証コードに一致しないと判定する場合、カード装置13は、アプリケーションの検証が失敗したと判定する。それゆえにフローはステップ205に移る。
【００２５】
ステップ204において、アプリケーションがアプリケーション135であると成功裡に検証されている場合、カード装置13のプロセッサ132は、アプリケーションの検証の成功を処理モジュール123に通知し、例えばプロセッサ132によってランダムに提供されるワンタイム・アプリケーションキーを用いて、記憶モジュール131の隠しゾーン134内に格納されており、かつ、記憶モジュール131の保護ゾーン133内に格納されているアプリケーション135にも含まれている、参照アプリケーションキー137を更新する。
【００２６】
ステップ205において、アプリケーションの検証が失敗した場合、カード装置13のプロセッサ132は、アプリケーションの検証の失敗を示すエラーメッセージをユーザ端末12に送信する。
【００２７】
ステップ206において、カード装置13からのエラーメッセージを受け取ると、ユーザ端末12の処理モジュール123は、表示モジュール122上にエラーメッセージを表示する。
【００２８】
図1、図3Aおよび図3Bを参照すると、アプリケーションが成功裡に検証された後、ネットワーク認証装置1は、本開示に係るネットワーク認証方法の実施形態に係るネットワークサーバ検証手続をインプリメントする。ネットワークサーバ検証手続は、認証対象の（to-be-authenticated）ネットワークサーバ11を検証する方法に関係がある。ネットワークサーバ11は、通信ネットワーク101と接続することができる。ネットワークサーバ11は、サーバキー113を予め格納した記憶モジュール111と、記憶モジュール111に接続された処理モジュール112とを含んでいる。ネットワークサーバ11は、ネットワークトランザクションに関連したウェブページ(図示せず)を提供することができる。ネットワークサーバ検証手続は次のステップを含んでいる。
【００２９】
ステップ301において、アプリケーションの実行を通じて、アプリケーションの検証が成功した旨の通知を受け取ると、ユーザ端末12の処理モジュール123は、通信ネットワーク101を越えて、認証対象のネットワークサーバ11と通信リンクを確立し、サーバ検証リクエストをカード装置13に送信する。
【００３０】
ステップ302において、ユーザ端末12からのサーバ検証リクエストを受け取ると、カード装置13のプロセッサ132は、特定のネットワークサーバに対応するサーバ検証コードと、例えばカード装置13のプロセッサ132によってランダムに提供されるワンタイム・サーバキーとに基づいて、サーバ・ダイナミックリンクプログラムを生成し、記憶モジュール131の隠しゾーン134内に格納されている参照サーバキー136を用いてサーバ・ダイナミックリンクプログラムを暗号化し、それによって暗号化されたサーバ・ダイナミックリンクプログラムをユーザ端末12に送信する。この実施形態では、サーバ検証コードはワンタイム・コードであるがこれに制限されない。
【００３１】

ステップ303において、アプリケーションの実行を通じて、ユーザ端末12は、通信ネットワーク101を介して、カード装置13からの暗号化されたサーバ・ダイナミックリンクプログラムを、認証対象のネットワークサーバ11に送信する。

【００３２】

ステップ304において、通信ネットワーク101を介してサーバ・ダイナミックリンクプログラムを受け取ると、認証対象のネットワークサーバ11の処理モジュール112は、記憶モジュール111内に予め格納されているサーバキー113とそれによって受け取ったサーバ・ダイナミックリンクプログラムとに基づいて、サーバコードデータを生成し、通信ネットワーク101を介して、サーバコードデータをユーザ端末12に送信する。

【００３３】

ステップ304は、認証対象のネットワークサーバ11の処理モジュール112によって行なわれる次のサブステップを含んでいる:サーバキー113を用いて、それによって受け取ったサーバ・ダイナミックリンクプログラムを解読するサブステップ; このように解読されたサーバ・ダイナミックリンクプログラムの実行を通じて、サーバコードデータを生成するサブステップ。

【００３４】

理想的には、ユーザ端末12と認証対象のネットワークサーバ11との間の通信リンクが、悪意のあるいかなる第三者からの悪意のある攻撃を受けない場合、ユーザ端末12にリンクされたネットワークサーバ11は特定のネットワークサーバのはずであることに言及することは有益である。しかしながら、実際には、ユーザ端末12と認証対象のネットワークサーバ11との間の通信リンクは、中間者(man-in-the-middle: MITM)攻撃のような悪意のある攻撃を受けている可能性がある。MITM攻撃は、特定のネットワークサーバによって提供されるウェブページのIPアドレスとは異なる、例えばフィッシングサイトのIPアドレスへ、ユーザ端末12を誘導し直すことができる。したがって、ユーザ端末12に接続されている、認証対象のネットワークサーバ11が、特定のネットワークサーバであるか否かを確認することが必要である。

【００３５】

ユーザ端末12と認証対象のネットワークサーバ11との間の通信リンクが、悪意のある攻撃を受けない場合、すなわち、認証対象のネットワークサーバ11が確かに特定のネットワークサーバである場合、認証対象のネットワークサーバ11の記憶モジュール111内に予め格納されているサーバキー113は、カード装置13の記憶モジュール131の隠しゾーン134内に格納されている参照サーバキー136と同一であろう。また、認証対象のネットワークサーバ11によって受け取られたサーバ・ダイナミックリンクプログラムは、ステップ302においてカード装置13のプロセッサ132によって生成されて暗号化されたサーバ・ダイナミックリンクプログラムと同じになるであろう。したがって、ステップ304において、認証対象のネットワークサーバ11の処理モジュール112は、サーバキー113を用いて、それによって受け取ったサーバ・ダイナミックリンクプログラムを成功裡に解読し、それによって解読されたサーバ・ダイナミックリンクプログラムの実行を通じて、サーバコードデータを生成および同様にワンタイム・サーバキーを生成するであろう。この場合、認証対象のネットワークサーバ11によって生成されたサーバコードデータは、ステップ302でのサーバ検証コードと同じである。

【００３６】

ユーザ端末12と認証対象のネットワークサーバ11との間の通信リンクが、悪意のある攻撃を受けている場合、例えば、認証対象のネットワークサーバ11がMITM攻撃ノードである場合、ステップ304において使用されるサーバキー113は、記憶モジュール131の隠しゾーン134内に格納されている参照サーバキー136ではない可能性がある。その結果、認証対象のネットワークサーバ11の処理モジュール112によって受け取られたサーバ・ダイナミックリンクプログラムは、サーバキー113を用いて解読されなくてもよい。したがって、解読されていないサーバ・ダイナミックリンクプログラムの実行を通じて、認証対象のネットワークサーバ11によって生成されたサーバコードデータは、ステップ302におけるサー

バ検証コードとは異なっており、ワンタイム・サーバキーは、ネットワークサーバ11によって生成されなくてもよい。

【００３７】

ステップ305において、通信ネットワーク101を介してサーバコードデータを受け取ると、ユーザ端末12の処理モジュール123は、アプリケーションの実行を通じて、それによって受け取ったサーバコードデータをカード装置13のプロセッサ132に送信する。

【００３８】

ステップ306において、カード装置13のプロセッサ132は、ユーザ端末12からのサーバコードデータが、認証対象のネットワークサーバ11を検証するための、ステップ302におけるサーバ検証コードに一致するか否かを判定する。カード装置13のプロセッサ132が、サーバコードデータがサーバ検証コードに一致すると判定する場合、認証対象のネットワークサーバ11は、カード装置13によって、特定のネットワークサーバであると成功裡に検証される。それゆえにフローはステップ307に移る。一方で、カード装置13のプロセッサ132が、サーバコードデータがサーバ検証コードに一致しないと判定する場合、カード装置13は、認証対象のネットワークサーバ11の検証が失敗したと判定する。それゆえにフローはステップ309に移る。

【００３９】

ステップ307において、認証対象のネットワークサーバ11が特定のネットワークサーバであると成功裡に検証されている場合、カード装置13のプロセッサ132は、通信ネットワーク101を介してユーザ端末12を通じて、認証対象のネットワークサーバ11の検証の成功を、認証対象のネットワークサーバ11に通知し、ステップ302において使用したワンタイム・サーバキーを用いて、記憶モジュール131の隠しゾーン134内に格納されている参照サーバキー136を更新する。

【００４０】

ステップ308において、認証対象のネットワークサーバ11の検証の成功の通知をカード装置13から受け取ると、認証対象のネットワークサーバ11の処理モジュール112は、ユーザ端末12の表示モジュール122上にウェブページを表示するようにユーザ端末12をウェブページに誘導し、ステップ304において生成されたワンタイム・サーバキーを用いて、記憶モジュール111内に予め格納されているサーバキー113を更新する。

【００４１】

ステップ309において、認証対象のネットワークサーバ11の検証が失敗した場合、カード装置13のプロセッサ132は、認証対象のネットワークサーバ11の検証の失敗を示すエラーメッセージをユーザ端末12に送信する。

【００４２】

ステップ310において、カード装置13からのエラーメッセージを受け取ると、ユーザ端末12の処理モジュール123は、表示モジュール122上にエラーメッセージを表示する。

【００４３】

図1および図4を参照すると、ネットワーク認証装置1のユーザ端末12およびカード装置13は、本開示に係るネットワーク認証方法の実施形態に係るユーザ同一性検証手続をインプリメントするために使用される。ユーザ同一性検証手続は、ユーザ端末12を操作している、検証対象のユーザ102の同一性を検証する方法に関係があり、次のステップを含んでいる。

【００４４】

ステップ401において、アプリケーションおよび認証対象のネットワークサーバ11の検証が成功した後、カード装置13のプロセッサ132は、ユーザ同一性検証リクエストをユーザ端末12に送信する。

【００４５】

ステップ402において、カード装置13からのユーザ同一性検証リクエストの受け取りに応じて、ユーザ端末12の処理モジュール123は、ユーザ端末12の入力モジュール121によって生成される、検証対象のユーザ102によって行なわれた入力操作に対応する入力データ

を、カード装置13のプロセッサ132に送信する。

【００４６】

ステップ403において、カード装置13のプロセッサ132は、ユーザ端末12からの入力データが、検証対象のユーザ102の同一性を検証するための、記憶モジュール131の隠しゾーン134内に格納されているユーザIDデータ138に一致するか否かを判定する。カード装置13のプロセッサ132が、入力データがユーザIDデータ138に一致すると判定する場合、検証対象のユーザ102の同一性は、カード装置13によって、特定のユーザ同一性であると成功裡に検証される。それゆえにフローはステップ404に移る。一方で、カード装置13のプロセッサ132が、入力データがユーザIDデータ138に一致しないと判定する場合、検証対象のユーザ102の同一性の検証は失敗したと判定される。それゆえにフローはステップ406に移る。

【００４７】

ステップ404において、検証対象のユーザ102の同一性が特定のユーザ同一性であると成功裡に検証されている場合、カード装置13のプロセッサ132は、記憶モジュール131の隠しゾーン134内に格納されているカードデータ139を、ユーザ端末12の処理モジュール123に送信する。

【００４８】

ステップ405において、アプリケーションの実行を通じて、ユーザ端末12の処理モジュール123は、通信ネットワーク101を介して、カード装置13からのカードデータ139をネットワークサーバ11の処理モジュール112に送信する。その後、ネットワークサーバ11は、ユーザ端末12からのカードデータ139に基づいて、ネットワークトランザクションに関連した支払手続を行う。

【００４９】

ステップ406において、ユーザ102の同一性の検証が失敗した場合、カード装置13のプロセッサ132は、検証対象のユーザ102の同一性の検証の失敗を示すエラーメッセージをユーザ端末12に送信する。

【００５０】

ステップ407において、カード装置13からのエラーメッセージを受け取ると、ユーザ端末12の処理モジュール123は、表示モジュール122上にエラーメッセージを表示する。

【００５１】

なお、カード装置13からユーザ端末12内にアプリケーション135を再取得する度に、ネットワーク認証装置1によって、本開示に係るネットワーク認証方法が再度完全に実行されること、すなわち、アプリケーション検証手続、ネットワークサーバ検証手続およびユーザ同一性検証手続が、連続して行なわれることに注目されたい。

【００５２】

各アプリケーション検証手続では、カード装置13のプロセッサ132は、以前のアプリケーション検証手続におけるものとは好ましくは異なっているアプリケーション検証コードに基づいて、アプリケーション・ダイナミックリンクプログラムを生成し、以前のアプリケーション検証手続（図2のステップ201）のステップ204において更新されている参照アプリケーションキー137を用いて、アプリケーション・ダイナミックリンクプログラムを暗号化する。同様に、各ネットワークサーバ検証手続では、カード装置13のプロセッサ132は、以前のサーバ検証手続におけるものとは好ましくは異なっているサーバ検証コードおよびワンタイム・サーバキーに基づいて、サーバ・ダイナミックリンクプログラムを生成し、以前のサーバ検証手続（図3Aのステップ302）のステップ307において更新されている参照サーバキー136を用いて、サーバ・ダイナミックリンクプログラムを暗号化する。

【００５３】

各アプリケーション／ネットワークサーバ検証手続において使用されているアプリケーション／サーバ検証コードが、以前のアプリケーション／ネットワークサーバ検証手続において使用されているものとは異なっており、各アプリケーション／ネットワークサーバ検証手続において、アプリケーション／サーバ・ダイナミックリンクプログラムを暗号化するために使用される参照アプリケーション／サーバキー137/136が、以前のアプリケー

ション／ネットワークサーバ検証手続において更新されているので、たとえ、アプリケーション検証／サーバ検証コードおよび参照アプリケーション／サーバキー137/136を取得するために、例えば総当たり（brute-force）攻撃方法を使用して、以前のアプリケーション／サーバ検証手続においてアプリケーション／サーバ・ダイナミックリンクプログラムが盗まれているとしても、ネットワークサーバ11およびアプリケーションの安全な認証を、依然として保証することができる。

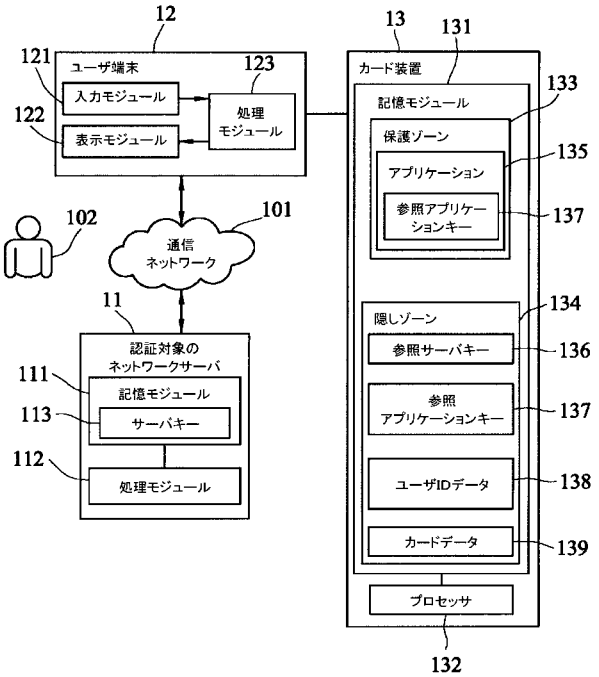
【００５４】

上記のものを考慮して、本開示に係るネットワーク認証方法は、ネットワークトランザクションに関係している、認証対象のネットワークサーバ11の、アプリケーションの、および検証対象のユーザ102の同一性の、安全な認証を保証することができる。

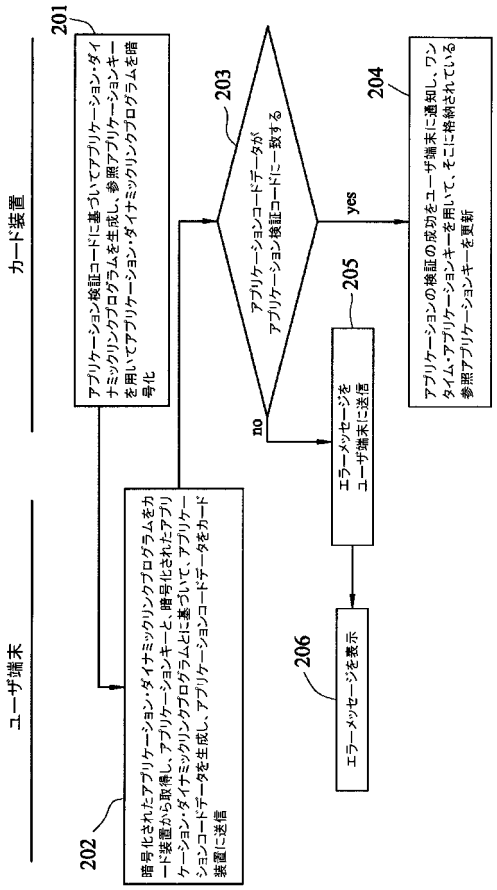
【００５５】

以上、本開示を典型的な実施形態と考えられるものに関して記述してきたが、本開示は、開示した実施形態に制限されることなく、同様の修正および等価なアレンジのすべてを包含するような、最も広い解釈の精神および範囲内に含まれる様々なアレンジをカバーするように意図されることが理解される。

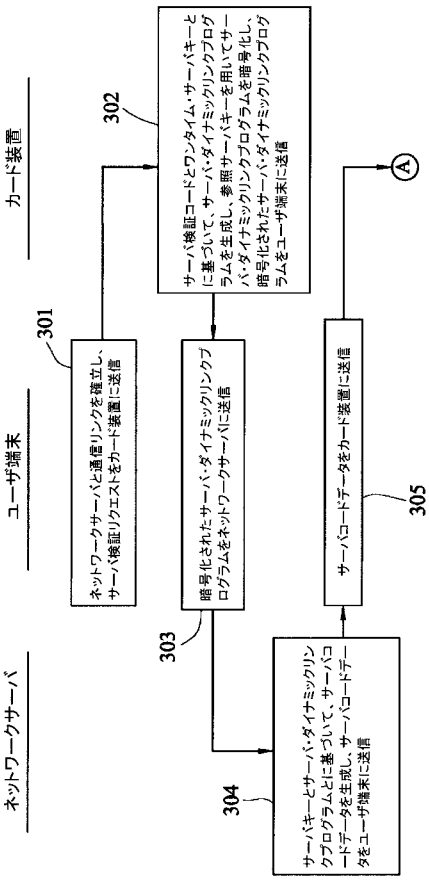
【図１】



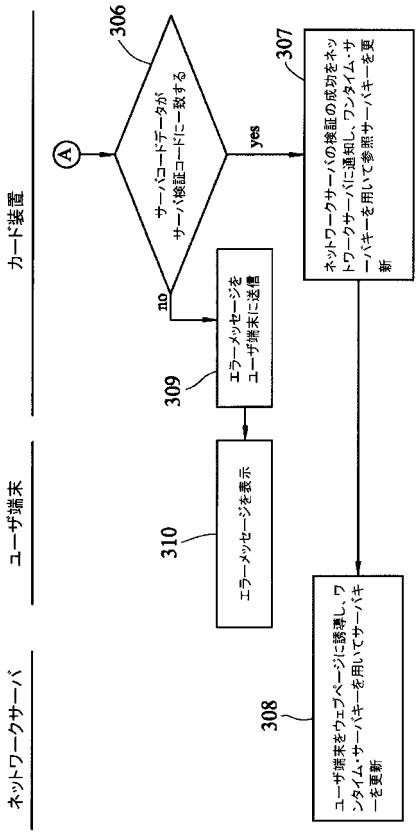
【図２】



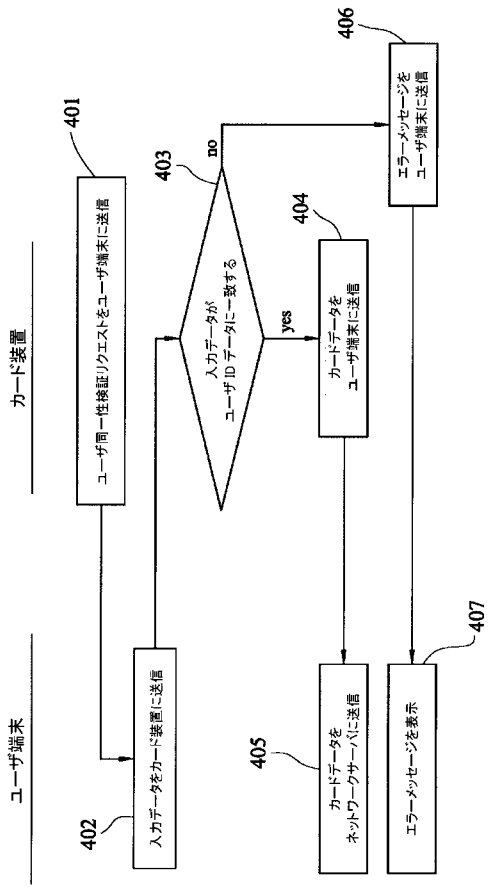
【図３Ａ】


ネットワークサーバ
ユーザ端末
カード装置
301
302
303
304
305
ネットワークサーバと通信リンクを確立し、サーバ検証リクエストをカード装置に送信
サーバ検証コードとワンタイム・サーバキーとに基づいて、サーバ・ダイナミックリンクプログラムを生成し、参照サーバキーを用いてサーバ・ダイナミックリンクプログラムを暗号化し、暗号化されたサーバ・ダイナミックリンクプログラムをユーザ端末に送信
暗号化されたサーバ・ダイナミックリンクプログラムをネットワークサーバに送信
サーバキーとサーバ・ダイナミックリンクプログラムに基づいて、サーバコードデータを生成し、サーバコードデータをユーザ端末に送信
サーバコードデータをカード装置に送信
A

【図３Ｂ】


ネットワークサーバ
ユーザ端末
カード装置
306
307
308
309
310
A
サーバコードデータがサーバ検証コードに一致する
yes
no
ネットワークサーバの検証の成功をネットワークサーバに通知し、ワンタイム・サーバキーを用いて参照サーバキーを更新
エラーメッセージをユーザ端末に送信
エラーメッセージを表示
ユーザ端末をウェブページに誘導し、ワンタイム・サーバキーを用いてサーバキーを更新

【図４】


ユーザ端末
カード装置
401
402
403
404
405
406
407
ユーザ同一性検証リクエストをユーザ端末に送信
入力データをカード装置に送信
入力データがユーザIDデータに一致する
yes
no
カードデータをユーザ端末に送信
エラーメッセージをユーザ端末に送信
カードデータをネットワークサーバに送信
エラーメッセージを表示

【外国語明細書】
2016100007000001.pdf
2016100007000002.pdf
2016100007000003.pdf
2016100007000004.pdf