(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6703539号
(P6703539)
(45)発行日　令和2年6月3日(2020.6.3)　(24)登録日　令和2年5月12日(2020.5.12)

(51)Int.Cl.　　F I
G06F 21/44 (2013.01)　　G06F 21/44
H04L 9/32 (2006.01)　　H04L 9/00 675B

請求項の数 13　(全 18 頁)

(21)出願番号　特願2017-532763(P2017-532763)
(86)(22)出願日　平成27年12月9日(2015.12.9)
(65)公表番号　特表2018-501567(P2018-501567A)
(43)公表日　平成30年1月18日(2018.1.18)
(86)国際出願番号　PCT/CN2015/096797
(87)国際公開番号　WO2016/095739
(87)国際公開日　平成28年6月23日(2016.6.23)
審査請求日　平成30年10月26日(2018.10.26)
(31)優先権主張番号　201410797833.5
(32)優先日　平成26年12月18日(2014.12.18)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　511050697
アリババ　グループ　ホウルディング　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ジョージ　タウン　ピーオーボックス　８４７　ワン　キャピタル　プレイス　フォース　フロア
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦

最終頁に続く

(54)【発明の名称】装置検証方法及び機器

(57)【特許請求の範囲】
【請求項１】
対象サービスの実行を要求する対象装置を検証するためにサーバによって実行される装置検証方法であって、
前記サーバが、前記対象装置によって送信された装置検証要求を受信することであって、前記装置検証要求が前記対象装置の装置証明書及び第１の装置属性情報を含み、前記装置証明書が第２の装置属性情報に従って生成された装置指紋を含むことと、
前記サーバが、前記装置指紋が前記第１の装置属性情報と一致するかどうかを判定することと、
前記サーバが、前記装置指紋が前記第１の装置属性情報と一致するとの判定に応じて、前記対象装置が前記対象サービスを実行できるようにすることと、
を含み、
前記対象装置によって送信された装置検証要求の前記受信の前に、前記方法が、
前記サーバが、前記対象装置によって送信された証明書申請要求を受信することであって、前記証明書申請要求が、前記対象装置によって収集された前記第２の装置属性情報を含むことと、
前記サーバが、前記第２の装置属性情報に従って前記装置指紋を生成することと、
前記サーバが、前記装置証明書を前記対象装置に送信することであって、前記装置証明書が前記装置指紋を含むことと、
を更に含み、

前記第２の装置属性情報が、前記対象装置によって収集された第１の数の属性値を含み、各属性値が前記対象装置の装置属性に対応し、
前記サーバが、前記第２の装置属性情報に従って前記装置指紋を生成することが、前記第１の数の属性値から第２の数の属性値を選択すること、及び前記装置指紋を生成するために前記第２の数の属性値を組み合わせることを更に含む、
装置検証方法。
【請求項２】
前記サーバが、前記装置指紋が前記第１の装置属性情報と一致すると判定することが、
前記サーバが、前記第１の装置属性情報が前記第２の装置属性情報の少なくともいくつかと一致すると判定すること、
又は、前記サーバが、前記第１の装置属性情報に従って別の装置指紋を生成し、前記別の装置指紋が前記装置証明書における前記装置指紋と一致すると判定すること、
を含む、請求項１に記載の方法。
【請求項３】
前記第１の装置属性情報が前記第２の装置属性情報の少なくともいくつかと一致することが、
前記第１の装置属性情報及び前記第２の装置属性情報における対応する属性値が同じであること、又は属性値の総数に対する同一属性値の数の比率が予め設定された比率閾値を満たすことを含む、請求項２に記載の方法。
【請求項４】
対象サービスの実行の要求がサーバに送信される場合に用いられる装置検証方法であって、
対象装置が、第１の装置属性情報を収集することと、
前記対象装置が、装置検証要求を前記サーバに送信することであって、前記装置検証要求が装置証明書及び前記第１の装置属性情報を含み、前記装置証明書が第２の装置属性情報に従って生成された装置指紋を含むことと、
前記対象装置が、前記装置指紋が前記第１の装置属性情報と一致するとの判定を前記サーバから受信した場合に、前記対象サービスを実行することと、
を含み、
第１の装置属性情報の前記収集の前に、前記方法が、
前記対象装置が、前記第２の装置属性情報を収集することと、
前記対象装置が、証明書申請要求を前記サーバに送信することであって、前記証明書申請要求が、前記装置指紋の生成に使用される前記第２の装置属性情報を含むことと、
前記対象装置が、前記サーバによって返された前記装置証明書を受信することと、
を更に含み、
前記第２の装置属性情報が、前記対象装置によって収集された第１の数の属性値を含み、各属性値が前記対象装置の装置属性に対応し、
前記装置指紋が、前記第１の数の属性値から前記サーバによって選択された第２の数の属性値の組み合わせに基づいて生成されている、
方法。
【請求項５】
証明書申請要求を前記サーバに送信する前に、前記方法が、
前記対象装置が、前記装置証明書がローカルに格納されていないことを確認すること、
又は、前記対象装置が、前記サーバによって返された検証失敗応答を受信すること、
を更に含む、請求項４に記載の方法。
【請求項６】
前記装置証明書が、トラステッド・プラットフォーム・モジュールＴＰＭに格納される、請求項４に記載の方法。
【請求項７】
装置検証機器であって、前記機器が、サーバに適用され、

対象装置によって送信された装置検証要求を受信するように構成された要求受信ユニットであって、前記装置検証要求が前記対象装置の装置証明書及び第１の装置属性情報を含み、前記装置証明書が第２の装置属性情報に従って生成された装置指紋を含む要求受信ユニットと、
前記装置指紋が前記第１の装置属性情報と一致するかどうかを判定するように、且つ前記装置指紋が前記第１の装置属性情報と一致するとの判定に応じて、前記対象装置が対象サービスを実行可能にするように構成された装置検証ユニットと、
を含み、
前記要求受信ユニットが、前記対象装置によって送信された証明書申請要求を受信するように更に構成され、前記証明書申請要求が前記対象装置によって収集された前記第２の装置属性情報を含み、
前記機器が証明書生成ユニット及び証明書送信ユニットを更に含み、
前記証明書生成ユニットが前記第２の装置属性情報に従って前記装置指紋を生成するように構成され、
前記証明書送信ユニットが前記装置証明書を前記対象装置に送信するように構成され、前記装置証明書が前記装置指紋を含み、
前記第２の装置属性情報が、前記対象装置によって収集された第１の数の属性値を含み、各属性値が前記対象装置の装置属性に対応し、
前記証明書生成ユニットが、前記第２の装置属性情報に従って前記装置指紋を生成する場合に、前記第１の数の属性値から第２の数の属性値を選択し、前記装置指紋を生成するために前記第２の数の属性値を組み合わせるように更に構成される、
装置検証機器。
【請求項８】
装置検証機器であって、前記機器が対象装置に適用され、
第１の装置属性情報を収集するように構成された情報取得ユニットと、
装置検証要求をサーバに送信するように構成された要求送信ユニットであって、前記装置検証要求が装置証明書及び前記第１の装置属性情報を含み、前記装置証明書が第２の装置属性情報に従って生成された装置指紋を含む、要求送信ユニットと、
を含み、
前記装置指紋が前記第１の装置属性情報と一致するとの判定に基づいて、対象サービスが実行され、
前記情報取得ユニットが前記第２の装置属性情報を収集するように更に構成され、
前記要求送信ユニットが証明書申請要求を前記サーバに送信するように更に構成され、前記証明書申請要求が、前記装置指紋の生成に使用される前記第２の装置属性情報を含み、
前記機器が、前記サーバによって返された前記装置証明書を受信するように構成された証明書受信ユニットを更に含み、
前記第２の装置属性情報が、前記情報取得ユニットによって収集された第１の数の属性値を含み、各属性値が前記対象装置の装置属性に対応し、
前記装置指紋が、前記第１の数の属性値から前記サーバによって選択された第２の数の属性値の組み合わせに基づいて生成されている、
装置検証機器。
【請求項９】
装置証明書がローカルに格納されていないことを確認した後に、又は前記サーバによって返された検証失敗応答を受信した後に、前記要求送信ユニットが前記証明書申請要求を送信するように更に構成される、請求項８に記載の機器。
【請求項１０】
前記装置指紋に基づいて前記装置証明書が有効であるかどうかを判定することを更に含む、請求項１に記載の方法。
【請求項１１】

命令のセットを格納する非一時的コンピュータ可読媒体であって、前記命令のセットは、対象装置を検証する方法を行うために装置検証機器の少なくとも一つのプロセッサによって実行可能であり、前記方法が、
対象サービスの実行を要求する対象装置を検証するための装置検証方法であって、
前記対象装置によって送信された装置検証要求を受信することであって、前記装置検証要求が前記対象装置の装置証明書及び第１の装置属性情報を含み、前記装置証明書が第２の装置属性情報に従って生成された装置指紋を含むことと、
前記装置指紋が前記第１の装置属性情報と一致するかどうかを判定することと、
前記装置指紋が前記第１の装置属性情報と一致するとの判定に応じて、前記対象装置が前記対象サービスを実行できるようにすることと、
を含み、
前記対象装置によって送信された装置検証要求の前記受信の前に、前記方法が、
前記対象装置によって送信された証明書申請要求を受信することであって、前記証明書申請要求が、前記対象装置によって収集された前記第２の装置属性情報を含むことと、
前記第２の装置属性情報に従って前記装置指紋を生成することと、
前記装置証明書を前記対象装置に送信することであって、前記装置証明書が前記装置指紋を含むことと、
を更に含み、
前記第２の装置属性情報が、前記対象装置によって収集された第１の数の属性値を含み、各属性値が前記対象装置の装置属性に対応し、
前記第２の装置属性情報に従って前記装置指紋を生成することが、前記第１の数の属性値から第２の数の属性値を選択すること、及び前記装置指紋を生成するために前記第２の数の属性値を組み合わせることを更に含む、
非一時的コンピュータ可読媒体。
【請求項１２】
前記装置指紋が前記第１の装置属性情報と一致すると判定することが、
前記第１の装置属性情報が前記第２の装置属性情報の少なくともいくつかと一致すると判定すること、
又は、前記第１の装置属性情報に従って別の装置指紋を生成し、別の装置指紋が前記装置証明書における前記装置指紋と一致すると判定すること、
を含む、請求項１１に記載の非一時的コンピュータ可読媒体。
【請求項１３】
命令のセットを格納する非一時的コンピュータ可読媒体であって、前記命令のセットは、対象装置を検証する方法を行うために装置検証機器の少なくとも一つのプロセッサによって実行可能であり、前記方法が、
第１の装置属性情報を収集することと、
装置検証要求をサーバに送信することであって、前記装置検証要求が装置証明書及び前記第１の装置属性情報を含み、前記装置証明書が第２の装置属性情報に従って生成された装置指紋を含むことと、
前記装置指紋が前記第１の装置属性情報と一致すると前記サーバが判定した場合に、当該判定に基づいて、対象サービスが実行されるようにすることと、
を含み、
第１の装置属性情報の前記収集の前に、前記方法が、
前記第２の装置属性情報を収集することと、
証明書申請要求を前記サーバに送信することであって、前記証明書申請要求が、前記装置指紋の生成に使用される前記第２の装置属性情報を含むことと、
前記サーバによって返された前記装置証明書を受信することと、
を更に含み、
前記第２の装置属性情報が第１の数の属性値を含み、各属性値が前記対象装置の装置属性に対応し、

前記装置指紋が、前記第１の数の属性値から前記サーバによって選択された第２の数の属性値の組み合わせに基づいて生成されている、
非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
技術分野
本発明は、ネットワークセキュリティ技術に関し、特に装置検証方法及び機器に関する。
【背景技術】
【０００２】
背景
ネットワーク技術の発展と共に、ネットワークセキュリティの問題により多くの注意が払われている。例えば、多くのウェブサイトサービスにおいて、サービス処理のセキュリティを保証するために、サービスを実行する装置が識別され、従って装置が安全な装置かどうかを判定する必要がある。しかしながら、現在の装置検証技術において、装置は、純粋に装置のハードウェア属性に従って識別され、偽造などのセキュリティハザードの事例が容易に発生し、検証方法の信頼性は低い。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
概要
これを考慮して、本発明は、装置検証の信頼性を改善するための装置検証方法及び機器を提供する。
【課題を解決するための手段】
【０００４】
具体的には、本発明は、以下の技術的解決法を通じて実施される。
【０００５】
第１の態様において、装置検証方法であって、対象サービスの実行を要求する対象装置を検証するために用いられ、
検証される対象装置によって送信された装置検証要求を受信することであって、装置検証要求が対象装置の装置証明書及び第１の装置属性情報を含み、装置証明書が第２の装置属性情報に従って生成された装置指紋を含むことと、
装置証明書が有効であることが装置指紋に従って確認され、且つ装置指紋が第１の装置属性情報と一致する場合に、装置証明書が対象装置の証明書であることを判定すること、及び対象装置が対象サービスを実行できるようにすることと、
を含む方法が提供される。
【０００６】
第２の態様において、装置検証方法であって、対象サービスを実行する要求をサーバに送信する場合に用いられ、
第１の装置属性情報を収集することと、
装置検証要求をサーバに送信することであって、装置検証要が装置証明書及び第１の装置属性情報を含み、装置証明書が第２の装置属性情報に従って生成された装置指紋を含み、その結果、装置指紋が第１の装置属性情報と一致することをサーバが判定した場合に、対象サービスが実行されることと、
を含む方法が提供される。
【０００７】
第３の態様において、装置検証機器であって、サーバに適用され、
検証される対象装置によって送信された装置検証要求を受信するように構成された要求受信ユニットであって、装置検証要求が対象装置の装置証明書及び第１の装置属性情報を

含み、装置証明書が第２の装置属性情報に従って生成された装置指紋を含む要求受信ユニットと、
装置証明書が有効であることが装置指紋に従って検証され、且つ装置指紋が第１の装置属性情報と一致する場合に、装置証明書が対象装置の証明書であることを判定するように、且つ対象装置が対象サービスを実行可能にするように構成された装置検証ユニットと、
を含む機器が提供される。
【０００８】
第４の態様において、装置検証機器であって、対象装置に適用され、
第１の装置属性情報を収集するように構成された情報取得ユニットと、
装置検証要求をサーバに送信するように構成された要求送信ユニットであって、装置検証要求が装置証明書及び第１の装置属性情報を含み、装置証明書が第２の装置属性情報に従って生成された装置指紋を含み、その結果、装置指紋が第１の装置属性情報と一致することをサーバが判定した場合に、対象サービスが実行される要求送信ユニットと、
を含む機器が提供される。
【０００９】
本発明の実施形態の装置検証方法及び機器において、対象装置は、検証を要求する場合に装置証明書を伝達し、装置証明書は装置属性に従って生成された装置指紋を含む。対象装置は装置証明書及び装置指紋に従って検証され、対象装置は、装置指紋が対象装置の装置属性と一致し、且つ証明書が対象装置の証明書であることを判定された場合にのみ、サービスにアクセスすることが許され、その結果、不正なアクセス装置は、より効率的に識別され得、装置検証は、より信頼できる。
【図面の簡単な説明】
【００１０】
図面の簡単な説明
【図１】本発明の実施形態による装置検証方法の適用シナリオ図である。
【図２】本発明の実施形態による装置検証方法の概略シグナリング図である。
【図３】本発明の実施形態による別の装置検証方法の概略シグナリング図である。
【図４】本発明の実施形態による装置検証機器の概略構造図である。
【図５】本発明の実施形態による別の装置検証機器の概略構造図である。
【図６】本発明の実施形態による更に別の装置検証機器の概略構造図である。
【図７】本発明の実施形態による更に別の装置検証機器の概略構造図である。
【発明を実施するための形態】
【００１１】
詳細な説明
図１は、本発明の実施形態による装置検証方法の適用シナリオを概略的に示す。図１に示されているように、例として、ウェブサイト上で決済サービスを実行するユーザを取り上げると、決済サービスは、例えば、ユーザが、自分自身の口座を用いることによってサービスの支払いをするなどのサービス業務である。ユーザは、一般に、決済サービスを実行するために、自分のコンピュータ１１を用いる。サービスが、より高いセキュリティを要求するので、サーバ１２は、ユーザの口座とユーザによって通常用いられるコンピュータ１１との間の対応関係を記録してもよく、ユーザの口座が、コンピュータ１１上で用いられる場合に、サーバ１２は、サービスが安全に行われると見なしてもよい。決済サービスの実行を要求する場合に、口座が、ユーザによって通常用いられるコンピュータではなく、コンピュータ１３を用いることをサーバ１２が知った場合に、サーバ１２は、ユーザの口座が、ハッカーによって不正に入手されたかどうか、及びハッカーが、コンピュータ１３を用いることによって不正に動いているかどうかを疑ってもよく、その結果、サーバ１２は、サービスの履行を拒否してもよい。
【００１２】
上記の例は、装置検証の適用シナリオである。即ち、ウェブサイトサーバは、サービスが安全に行われるかどうかを検証するために、サービスのセキュリティを保証するように

装置（例えばコンピュータ）を識別する。続いて説明される本発明の実施形態による装置検証方法は、検証結果がより正確でより信頼できることを保証するために、サーバがどのように装置を検証するかを説明する。明らかに、装置検証の例は、図１に示されているシナリオに限定されず、他の同様のシナリオがまた、本発明の実施形態による装置検証方法を採用してもよい。

【００１３】

図２は、本発明の実施形態による装置検証方法の概略シグナリング図である。図２に示されているように、方法は、装置とサーバとの間で実行される装置検証フローを概略的に示す。例えば、ユーザは、決済サービスを行う装置を用いている。サーバ側は、サービスのセキュリティを保証するために、検証を行うように装置に指示してもよく、サーバは、検証が成功した後にだけ装置がサービスを再開できるようにしてもよい。

【００１４】

以下のプロセスは、装置が検証されることを要求するサーバの指示を、装置が受信した後で実行される処理を説明する。検証される装置は、対象装置と呼ばれてもよく、装置によって実行されるサービスは、対象サービスと呼ばれる。

【００１５】

２０１．対象装置は、第１の装置属性情報を収集する。

【００１６】

検証される対象装置が、サーバによって送信された、装置の検証を要求する指示を受信した後で、対象装置は、対象装置自体に対応する第１の装置属性情報を収集する（「第１の」は、続く実施形態に現れる他の属性情報から区別されるためにのみ用いられ、他の限定的な意味を有しない）。具体的には、第１の装置属性情報は、対象装置のハードウェア固有属性である。

【００１７】

例えば、例として、コンピュータである対象装置を取り上げると、コンピュータは、ネットワークカード、表示カード、ＣＰＵ及びメモリチップなどの様々なハードウェアを有しており、そのようなハードウェアの属性情報が、収集される必要がある。例えば、表示カードに関し、表示カードの属性は、例えば型、名称、配送ＩＤ、解像度などを含んでもよい。これらは、全て、ハードウェア、この場合には表示カードの属性情報と呼ばれてもよい。どの属性（単複）が特に収集されるか、例えば型又は配送ＩＤが収集されるかどうかは、この実施形態において限定されていない。しかしながら、取得されるハードウェア属性用の要件が存在する。属性は、ハードウェアの固有属性、即ちハードウェア用の不変の属性である。例えば、例としてやはり表示カードを用いると、配送ＩＤ又は型は、収集されてもよい。これらの属性は、固定され不変である。一方で解像度は、表示カードの属性であるが、変化する可能性がある。例えば、コンピュータ構成が調整された後で、解像度は、増加又は低減される可能性があり、かかる可変属性情報は、第１の装置属性情報として収集することができない。

【００１８】

更に、通常、このステップで収集される複数の第１の装置属性情報が存在してもよい。例えば、３つの属性情報又は５つの属性情報が収集されてもよい。複数の属性情報が、１つのハードウェアに対応する複属性であってよく、且つ複数個のハードウェアにそれぞれ対応する複属性であってもよいことに留意されたい。

【００１９】

例えば、３つの属性情報、即ち属性Ａ、属性Ｂ、及び属性Ｃが収集されることを仮定する。その場合に、３つの属性は、表示カードなどの同じハードウェアピースに対応し、それぞれ表示カードの型、配送ＩＤ及び名称である。又は３つの属性は、相異なるハードウェアピースにそれぞれ対応し、例えば、属性Ａは、ネットワークカードの型であり、属性Ｂは、表示カードの配送ＩＤであり、属性Ｃは、ＣＰＵなどの型である等である。明らかに他の例が存在するが、それらは、ここで詳細には説明されない。

【００２０】

２０２．対象装置は、装置検証要求をサーバに送信する。要求は、対象装置の装置証明書及び第１の装置属性情報を含み、装置証明書は、第２の装置属性情報に従って生成された装置指紋を含む。

【００２１】

第１の装置属性情報を収集した後で、対象装置は、対象装置に対して装置検証を実行するようにサーバに要求するために、装置検証要求をサーバに送信する。検証要求は、２０１において収集された第１の装置属性情報を含むだけでなく、装置証明書も含む。

【００２２】

一般に、対象装置が、正当なユーザ機器であると仮定すると、装置証明書は、この装置検証プロセスの前に、サーバによって対象装置へと発行され、対象装置は、サーバによって送信された装置証明書を格納する。対象装置は、このステップにおいて検証要求で装置証明書を伝達するように要求されるだけである。この時点で、第２の装置属性情報に従って生成される、且つ装置証明書に保持される装置指紋は、その属性、例えば２０１で挙げられた属性に従って、対象装置によって生成される指紋である。

【００２３】

検証される対象装置が、ハッカーによって使用される不正な装置であると仮定すると、装置証明書は、ハッカーによって盗まれた正当なユーザの装置証明書であり得、装置証明書に保持される装置指紋は、やはり、対象装置の属性に従って対象装置によって生成された指紋である。ハッカーは、装置証明書に含まれる装置指紋を修正することができない。何故なら、装置証明書の内容に対してなされるどんな修正も、証明書を無効にするからである。

【００２４】

任意選択的に、装置証明書は、対象装置のトラステッド・プラットフォーム・モジュールＴＰＭに格納されてもよく、ＴＰＭハードウェアは、より信頼できるセキュリティ保証を証明書の格納用に提供することができる。

【００２５】

２０３．サーバは、第１の装置属性情報が、装置証明書における装置指紋と一致するかどうかを判定する。

【００２６】

このステップにおいて、第１の装置属性情報が、装置証明書における装置指紋と一致するかどうかをサーバが判定する前に、サーバは、装置指紋に従って、装置証明書が有効かどうかを更に判定する。例えば、証明書が有効であることを判定した場合に、サーバは、装置指紋が破損されたかどうかをチェックしてもよい。例えば、サーバは、装置指紋が破損されているかどうかを判定するために、証明書における装置指紋を、前にサーバに格納された指紋と比較してもよい。サーバはまた、証明書の内容が完全かどうかを判定する完全性試験を実行するために、装置指紋を用いてもよい等である。

【００２７】

証明書が有効であると判定された後で、サーバは、２０２において対象装置によって提示された第１の装置属性情報を証明書における装置指紋と比較して、２つが互いに一致するかどうかを判定する。

【００２８】

任意選択的に、第１の装置属性情報が、証明書における装置指紋と一致する２つの方法が存在し得る。例えば、第１の装置属性情報は、第２の装置属性情報と一致する。例えば、対象装置によって収集された第１の装置属性情報は、属性Ａ、属性Ｂ及び属性Ｃを含み、証明書における装置指紋を生成するための第２の装置属性情報もまた、属性Ａ、属性Ｂ及び属性Ｃを含む。即ち、装置指紋もまた、３つの属性によって生成される。その場合には、第１の装置属性情報は、第２の装置属性情報と一致する。換言すれば、第１の装置属性情報は、証明書における装置指紋と一致する。別の例では、別の装置指紋がまた、対象装置によって収集された第１の装置属性情報に従って生成されてもよく、その別の装置指紋が、装置証明書における装置指紋と同じである場合に、それは、第１の装置属性情報が

、証明書における装置指紋と一致することを示す。
【００２９】
更に、第１の装置属性情報が、第２の装置属性情報と一致する場合に、属性情報間の一致は、例えば、第１の装置属性情報及び第２の装置属性情報における対応する属性値が同じであること、又は属性値の総数に対する同一属性値の数の比率が、予め設定された比率閾値に達することを指す。
【００３０】
例えば、４つの属性、即ち属性Ａ、属性Ｂ、属性Ｃ及び属性Ｄが存在すると仮定すると、サーバは、対象装置によって収集された４つの属性が、装置証明書における４つの対応する属性と同一かどうかを比較してもよい。例としてネットワークカードを取り上げると、装置証明書における属性Ａは、ネットワークカードの配送ＩＤであり、対象装置によって収集された第１の装置属性情報もまた、対象装置のネットワークカードの配送ＩＤを有し、サーバは、２つの配送ＩＤが同じかどうか、即ち同じハードウェアの対応するタイプの属性が同じかどうかを比較してもよい。上記の比較は、証明書における各属性に対して必要とされる。
【００３１】
比較中に、３つの場合が存在し得る。例えば、１つの場合において、属性値（属性値は、例えばネットワークカードの配送ＩＤである）は同じである。例えば配送ＩＤが同一である。別の場合において、属性値は異なる。例えば、配達ＩＤが異なるか又は表示カードの型が異なる。更に別の場合において、収集された属性値はヌルである。例えば、装置証明書における１つの属性は、ネットワークカードの型であるが、しかし対象装置によって収集された第１の装置属性情報において、ネットワークカード型はヌルである。即ち、ネットワークカード型は収集されない。これは、収集中に収集環境又は他の要因によって影響を受けた可能性があり、その場合、属性は取得されない。
【００３２】
上記の３つの比較の場合に基づいて、属性情報間の一致は、次のように定義されてもよい。
【００３３】
例えば、第１の装置属性情報、及び第２の装置属性情報における対応する属性値は、完全に同じである必要がある。即ち、対象装置は、証明書における全ての属性値を収集する必要があり、属性値は、同じである必要がある。その場合に、サーバは、第１の装置属性情報が第２の装置属性情報と一致することを判定することができる。
【００３４】
別の例では、第１の装置属性情報、及び第２の装置属性情報における対応する属性値は、完全に同じである必要があり、その場合に、幾つかの収集された対応する属性値がヌルであることは許され得るが、しかし全ての収集された属性値がヌルであることは許されない。証明書における属性値が、対象装置によって収集されず、それらが全てヌルである場合に、サーバは、第１の装置属性情報が、第２の装置属性情報と一致しないことを判定する。４つの属性Ａ、Ｂ、Ｃ及びＤに関し、属性Ｂだけが対象装置によって収集されず、他の属性値が同じである場合に、属性Ａは無視されてもよく、第１の装置属性情報が、第２の装置属性情報と一致することが判定される。
【００３５】
別の例では、第１の装置属性情報、及び第２の装置属性情報における対応する属性値間で、属性値の総数に対する同一属性値の数の比率は、予め設定された比率閾値に達する。例えば、上記の４つの属性において、１つの対応する属性だけが比較において異なり、他の３つが同じである場合に、属性値の総数に対する同一属性値の数の比率は３／４であり、予め設定された比率閾値１／２より大きく、そのとき、それらが互いに一致することが判定される。３つの属性の属性値が異なる場合に、属性値の総数に対する同一属性値の数の比率は、１／４であり、予め設定された比率閾値１／２未満であり、そのとき、それらが互いに一致しないことが判定される。

【００３６】
前述において説明された一致条件の例が、単に例であり、網羅的ではなく、特定の実装形態において、一致条件が、装置検証によって要求されるセキュリティ制御の厳格さの程度に従って柔軟に設定されてもよいことに留意されたい。
【００３７】
このステップにおける属性比較は、図１に示されている適用シナリオの例と組み合わせて示されており、装置が安全かどうか、及び装置が安全な装置か又は不正な装置かをサーバがどのように判定するかが説明される。
【００３８】
図１において、ユーザが、正当なユーザであり、サーバ１２にアクセスするために自分のコンピュータ１１を用いると仮定すると、コンピュータ１１が、装置検証要求を送信する場合に、そこに保持された装置証明書は、コンピュータ１１へとサーバ１２によって発行された証明書であり、証明書における第２の装置属性情報は、コンピュータ１１に対応する属性、例えば、コンピュータ１１の表示カード属性及びネットワークカード属性である。装置検証要求が送信される場合に、コンピュータ１１の表示カード及びネットワークカード属性もまた、コンピュータ１１によって収集された第１の属性情報に存在し、２つの属性情報は、サーバ側によって判定される場合に、一般に一貫している。
【００３９】
対して、図１において、ユーザが、不正なユーザ、即ち正当なユーザのコンピュータ１１に対応する装置証明書を盗み、コンピュータ１３を介してサーバ１２にアクセスする不正なユーザであると仮定し、且つコンピュータ１３が、装置検証要求を送信する場合に、そこに保持される装置証明書が、サーバ１２によってコンピュータ１１に発行された証明書であると仮定すると、証明書における装置指紋は、コンピュータ１１の属性によって生成され、一方でコンピュータ１３によって収集された第１の装置属性情報は、コンピュータ１３に対応するハードウェア情報であり、従って、サーバ側が判定する場合に、装置指紋及び第１の装置属性情報が互いに一致しないことが判定されることになる。
【００４０】
このステップにおいて、装置証明書が装置指紋に従って有効であると判定され、且つ判定結果によれば、装置証明書における装置指紋が第１の装置属性情報と一致する場合に、それは、装置証明書が対象装置の証明書であることを示し、２０４が実行される。そうでなければ、２０５が実行される。
【００４１】
２０４．サーバは、対象装置が対象サービスを実行できるようにする。
【００４２】
このステップにおいて、サーバは、検証成功応答を対象装置に返すか、又は成功応答を返さずに、対象装置が後続のサービス動作を直接実行できるようにしてもよい。
【００４３】
２０５．サーバは、対象装置が対象サービスを実行できないようにする。
【００４４】
例えば、サーバは、検証失敗応答を対象装置に返す。例えば、不正なユーザが、上記で説明したように、サーバにアクセスするためにコンピュータ１３を用いた場合に、ユーザは、サーバによって、サービスを実行できないようにされることになる。
【００４５】
この実施形態の装置検証方法において、装置属性情報に従って生成された装置指紋は、装置用に発行された装置証明書に保持され、装置の検証中に、装置は、装置属性が証明書における装置指紋と一致する場合にのみサービスを実行できるようにされ、それによって、装置検証のセキュリティ及び信頼性を改善する。
【００４６】
上記の例において、装置検証方法を実行するプロセスは、対象装置が装置証明書を格納したことに基づいて実行され、対象装置は、装置検証要求を送信する場合に、装置証明書

を伝達する必要があるだけである。実際には、装置証明書は、サーバによって対象装置に発行され、装置検証のプロセスを実行する前に、サーバに申請することを通して、対象装置によって取得される。証明書の申請は、以下で詳細に説明される。

【００４７】

図３は、本発明の実施形態による別の機器検証方法の概略シグナリング図であり、その図は、装置が証明書をサーバに申請する場合のプロセス及びサーバが証明書を生成する方法を説明するために用いられ、以下のステップを含む。

【００４８】

３０１．対象装置は、第２の装置属性情報を収集し、且つ公開鍵－秘密鍵ペアを生成する。

【００４９】

装置証明書が、サーバによって作成される場合に、装置のハードウェア属性もまた、証明書に設定され、従って、対象装置が、証明書を申請する場合に、第２の装置属性情報と呼ばれてもよい装置のハードウェア属性の収集が、実行される必要があり、その結果、それらは、サーバに提出され、それに応じてサーバが証明書を生成できるようにすることができる。

【００５０】

このステップにおいて、対象装置によって収集された第２の装置属性情報が、装置証明書における属性情報と必ずしも完全に同一でなくてもよいことに留意されたい。例えば、３つの属性Ａ、Ｂ及びＣが、装置証明書に存在すると仮定すると、このステップにおける第２の装置属性情報は、対象装置が、対象装置自体の全てのハードウェア固有属性を収集するか又は５つの属性を収集する等であってよく、それは、要するに、装置証明書に含まれる属性より多くてもよく、装置証明書における属性は、複属性から選択された幾つかの属性である。詳しくは、後続の３０３の説明を参照されたい。明らかに、第２の装置属性情報はまた、証明書における属性と同一であってもよい。例えば、３つのＡ、Ｂ及びＣが収集され、３つの属性はまた、証明書が作成される場合に証明書に設定される。

【００５１】

更に、このステップにおいて第２の装置属性情報を収集することに加えて、対象装置は、公開鍵及び秘密鍵を含む公開鍵－秘密鍵ペアを更に生成する。公開鍵は、３０４において証明書を生成するために用いられ、秘密鍵は、証明書が申請される場合にはサーバに送信されない。例えば、秘密鍵は、検証が成功した後で、情報伝送中に情報を暗号化するために用いられてもよい。例えば、対象装置によってサーバ送信される情報は、秘密鍵によって暗号化され、サーバは、公開鍵を用いることによって情報を解読する。

【００５２】

３０２．対象装置は、証明書申請要求をサーバに送信し、証明書申請要求は、第２の装置属性情報、及び公開鍵－秘密鍵ペアにおける公開鍵を含む。

【００５３】

対象装置が、証明書申請要求をサーバに送信する場合に、３０１において収集された第２の装置属性情報、及び生成された公開鍵－秘密鍵ペアにおける公開鍵が伝達される。

【００５４】

任意選択的に、対象装置は、装置証明書をサーバに申請し、申請は、次のように列挙される２つの場合において、サーバに対して開始されてもよい。

【００５５】

１つの場合において、対象装置は、それが装置証明書を格納していないことを知る。証明書がサーバによって装置に送信されるので、証明書は装置に格納され、装置が装置検証を実行するようにサーバに要求した場合に、証明書は装置検証要求において伝達される。装置証明書がローカルに格納されていないことを対象装置が確認した場合に、装置検証は、続いて実行することはできない。従って、対象装置は、証明書申請を開始することになる。

【００５６】

もう１つの場合に、対象装置が、サーバによって返された検証失敗応答を受信した場合に、換言すれば、今回の対象装置による証明書の申請の前に、対象装置は、恐らくサーバに検証を要求するために別の装置の証明書を用いた可能性があり、その結果、サーバは、属性情報が一致しないことを判定し、装置証明書が、その装置の証明書ではないことを示す検証失敗を返す。従って、対象装置は、再びそれ自体の装置証明書を申請する必要がある。

【００５７】

３０３．サーバは、第２の装置属性情報に従って装置指紋を生成する。

【００５８】

このステップにおいて、対象装置によって収集された第２の装置属性情報における属性数が、装置指紋が生成される場合に基づく必要のある属性情報の数より多い場合に、属性は、第２の装置属性情報から選択されてもよく、対象装置によって収集された第２の装置属性情報における属性数が、装置指紋が生成される場合に基づく必要のある属性数と同じである場合に、指紋は、それらの全てに基づいて生成されてもよい。

【００５９】

前述において、装置指紋が生成される際に基づく第２の装置属性情報の取得は、属性数の点から説明され、収集される第２の装置属性情報が、属性Ａ（例えばＣＰＵ型）、属性Ｂ（例えばネットワークカード型）、属性Ｃ（例えば表示カードの配送ＩＤ）、及び属性Ｄ（例えばメモリの名称）を含むと仮定すると、それに応じて指紋が生成される際に基づく属性を取得する場合に、指紋は、例えば、次に示す方法で、更に処理される必要がある。

【００６０】

【表１】

表1 属性値用に取られたハッシュ値

属性	ハッシュ値
属性A	属性Aのハッシュ値
属性B	属性Bのハッシュ値
属性C	属性Cのハッシュ値
属性D	属性Dのハッシュ値

【００６１】

上記の表１に示されているように、表１は、対象装置が、伝送のセキュリティを保証するために、収集された４つの属性情報の属性値用のハッシュ値を取ることを示す。実際には、収集された属性値のハッシュ値は、サーバに送信される。サーバ側において、これらの属性のハッシュ値は、対象装置を識別するための装置指紋を形成するために組み合わされる必要がある。

【００６２】

例えば、例として、第２の装置属性情報から幾つかの属性を選択する。第２の装置属性情報は複属性値を含み、各属性値、例えば上記の表１における４つの属性値は、対象装置の装置固有属性に対応する。サーバは、４つの属性から、予め設定された数の属性値を選択する。例えば、この実施形態において、３つの属性値Ａ、Ｂ及びＣが選択され、これらの属性値は、装置の指紋情報を生成するために組み合わされる。組み合わせは、次の方法に従って実行されてもよい。即ち、上記の表１における属性Ａ、属性Ａのハッシュ値、属性Ｂ、属性Ｂのハッシュ値、属性Ｃ、及び属性Ｃのハッシュ値は、全て、装置指紋情報として働くために、ハッシュを取るように統合される。明らかに、３つの属性の関連情報が含まれる限り、他の組み合わせ方法が存在してもよいが、それらは、詳細には説明されない。

【００６３】
前述のように、第２の装置属性情報から幾つかの属性を選択することによって装置指紋を生成する方法が、装置検証の方法をより信頼でき且つより安全にできることに留意されたい。その理由は、対象装置が、その全てのハードウェア固有属性を収集すると仮定すると、対象装置は、それらの全ての属性からどの属性が、それに応じて装置指紋を生成するために、サーバによって選択されるかを知ることができず、ハッカーなどの不正なユーザは、どの属性が装置証明書に含まれるかが分からず、その結果、ハッカーは、自分自身で属性を捏造しようとさえ目論むが（例えばハッカーは、装置検証要求を報告する場合に、正当な装置のハードウェア属性を改竄し、それらをハッカー自身のハードウェアと取り替える）、ハッカーは、どの属性が捏造される必要があるかが分からず、それは、ハッカーの不正行為の困難さを増加させ、その結果、検証方法は、より高い信頼性を有する。
【００６４】
更に、対象装置は、証明書を申請する場合に、対象装置によって収集されるハードウェア固有属性を記録してもよい。このようにして、同じ装置属性はまた、続いて装置検証が要求される場合に、収集されることができる。このようにしてのみ、収集された属性情報が、装置証明書における対応する属性を含むことが保証され得、サーバは、属性を照合し、比較することができる。
【００６５】
３０４．サーバは、装置指紋及び公開鍵を含む装置証明書を生成する。
【００６６】
以下の表２は、単純化された方法で、このステップにおいて生成される装置証明書の構造を示す。
【００６７】
【表２】

表2 装置証明書の構造

証明書の主情報	証明書の拡張情報
署名付き公開鍵	装置指紋

【００６８】
上記の表２に示されているように、装置証明書は、証明書の拡張情報に含まれる装置指紋を有するデジタル証明書であり、デジタル証明書は、例えばＸ．５０９Ｖ３フォーマットにおける証明書である。装置指紋の生成の説明は、３０３の説明に見い出し得る。装置証明書はＣＡ署名付き公開鍵を更に含み、公開鍵は、対象装置によって生成された公開鍵－秘密鍵ペアにおける公開鍵である。情報の破損は、証明書を無効にする。
【００６９】
更に、装置証明書が生成される場合に、証明書通し番号もまた、証明書の固有属性として生成される。サーバ側は、生成された装置証明書と装置指紋との間の対応関係を記録してもよい。具体的には、次の表３に示されているように、サーバ側は、例えば、証明書の証明書通し番号と装置指紋との間の対応関係、及び同様に装置固有属性（属性は、指紋が生成される際に基づく属性を指す）を記録してもよい。
【００７０】

【表３】

表3 装置証明書の対応関係

証明書通し番号	装置指紋	装置固有属性	証明書生成時刻	証明書使用時刻
		属性A	#####	****
		属性B		
		属性C		

【００７１】
表３の対応関係が記録された後で、サーバが、続いて対象装置によって送信された装置検証要求で伝達された装置証明書、即ち証明書通し番号の証明書属性を含む装置証明書を受信した場合に、サーバは、装置証明書に対応する装置指紋に対応する属性Ａ、属性Ｂ、及び属性Ｃを取得するために、証明書通し番号に従って表３を調べ、且つ対象装置によって収集された第１の装置属性情報と属性を比較し、それらが互いに一致するかどうかを判定してもよい。
【００７２】
証明書通し番号がまた、装置検証をより信頼できるものにすることができることに留意されたい。例えば、２つの装置の属性が同じである、例えば、ネットワークカードの型及び表示カードの配送ＩＤが全て同じであると仮定すると、２つの装置が、装置証明書を申請する場合に、サーバは、２つの装置用の装置証明書を発行する可能性があり、装置証明書に保持される装置指紋は、同じである可能性がある。しかしながら、各証明書は、一意の証明書通し番号に対応し、２つの装置証明書の証明書通し番号は、相異なり、サーバは、やはり２つの装置を区別することができる。
【００７３】
換言すれば、対象装置の装置検証要求を受信した場合に、サーバは、上記の例で説明された装置属性情報を照合し比較する必要があるだけでなく、また証明書の通し番号が、同じかどうか、証明書が、有効期限内かどうか、証明書情報が、完全か又は破損されているかどうか等を確かめるために、例えばある基本的な証明書検証を実行する必要がある。
【００７４】
３０５．サーバは、装置証明書を対象装置に送信する。
【００７５】
本発明のこの実施形態における装置検証方法は、デジタル証明書及び装置指紋を組み合わせる機構を用い、その結果、証明書における装置指紋は、デジタル証明書が偽造不可能であるように偽造不可能である。一方で、デジタル証明書の一意性もまた利用され、それによって装置検証の信頼性を大いに改善する。
【００７６】
装置検証機器が、上記で説明された装置検証方法を機器を通して実行するために、以下のように更に提供される。
【００７７】
図４は、本発明の実施形態による装置検証機器の概略構造図であり、機器は、サーバに適用されてもよく、例えば、ソフトウェアは、サーバ端末に設定される。図４に示されているように、機器は、要求受信ユニット４１及び装置検証ユニット４２を含んでもよい。
要求受信ユニット４１は、検証される対象装置によって送信された装置検証要求を受信するように構成され、装置検証要求は対象装置の装置証明書及び第１の装置属性情報を含み、装置証明書は第２の装置属性情報に従って生成された装置指紋を含む。
装置検証ユニット４２は、装置証明書が有効であることが装置指紋に従って確認され、且つ装置指紋が第１の装置属性情報と一致する場合に、装置証明書が対象装置の証明書で

あることを判定し、且つ対象装置が対象サービスを実行可能にするように構成される。

【００７８】

図５は、本発明の実施形態による別の装置検証機器の概略構造図である。図４に示されている構造に基づいて、機器は、証明書生成ユニット４３及び証明書送信ユニット４４を更に含む。

要求受信ユニット４１は、対象装置によって送信された証明書申請要求を受信するように更に構成され、証明書申請要求は、対象装置によって収集された第２の装置属性情報を含む。

証明書生成ユニット４３は、第２の装置属性情報に従って装置指紋を生成するように、且つ生成された装置証明書に装置指紋を設定するように構成される。

証明書送信ユニット４４は、装置証明書を対象装置に送信するように構成される。

【００７９】

更に、証明書生成ユニット４３は、第２の装置属性情報に従って装置指紋を生成する場合に、第２の装置属性情報に含まれる複属性値から予め設定された数の属性値を選択するように、且つ対象装置を識別するための装置指紋を生成するために予め設定された数の属性値を組み合わせるように更に構成される。各属性値は、対象装置の装置固有属性に対応する。

【００８０】

図６は、本発明の実施形態による更に別の装置検証機器の概略構造図である。機器は、対象装置に適用されてもよい。例えば、クライアント端末ソフトウェアは、対象装置側に設定される。図６に示されているように、機器は、情報取得ユニット６１及び要求送信ユニット６２を含んでもよい。

情報取得ユニット６１は、第１の装置属性情報を収集するように構成される。

要求送信ユニット６２は、装置検証要求をサーバに送信するように構成され、装置検証要求は装置証明書及び第１の装置属性情報を含み、装置証明書は第２の装置属性情報に従って生成された装置指紋を含み、その結果、対象サービスは、装置指紋が第１の装置属性情報と一致することをサーバが判定した場合に実行される。

【００８１】

図７は、本発明の実施形態による更に別の装置検証機器の概略構造図である。図６に示されている構造に基づいて、機器は、証明書受信ユニット６３を更に含む。

情報取得ユニット６１は、第２の装置属性情報を収集するように更に構成される。

要求送信ユニット６２は、証明書申請要求をサーバに送信するように更に構成され、証明書申請要求は第２の装置属性情報を含み、その結果、サーバは、第２の装置属性情報に従って装置指紋を生成し、且つ装置証明書に装置指紋を設定する。

証明書受信ユニット６３は、サーバによって返された装置証明書を受信するように構成される。

【００８２】

更に、要求送信ユニット６２は、装置証明書がローカルに格納されていないことが確認された場合に、又はサーバによって返された検証失敗応答が受信された場合に、証明書申請要求を送信するように更に構成される。

【００８３】

上記は、単に本発明の好ましい実施形態であり、本発明を限定するようには意図されていない。本発明の趣旨及び原理内で行われる任意の修正、等価な交換、改良等は、全て、本発明の保護範囲内に入るものとする。

【図１】

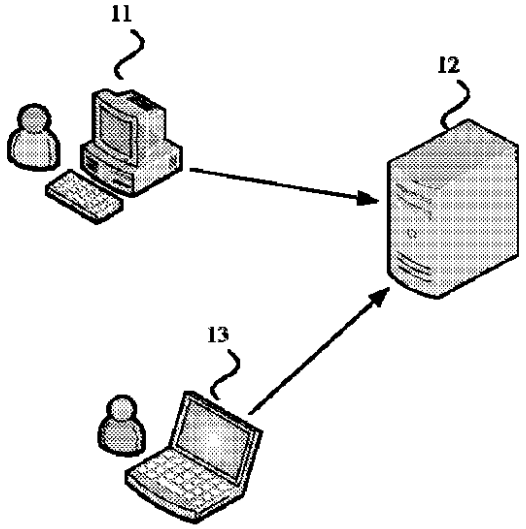
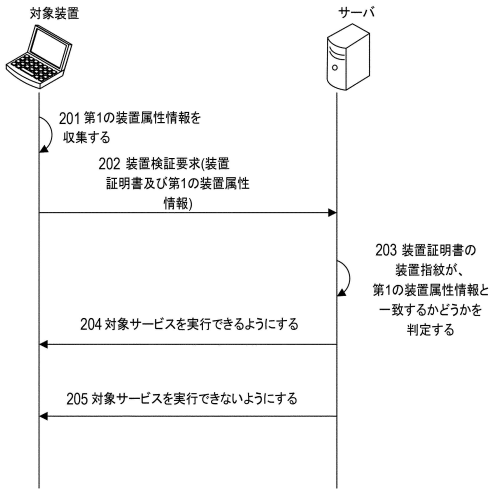
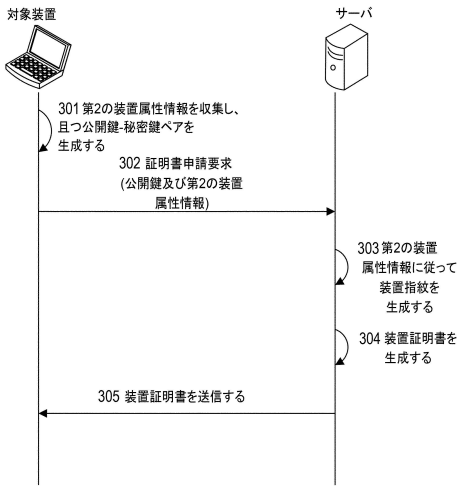

11
12
13

図 1

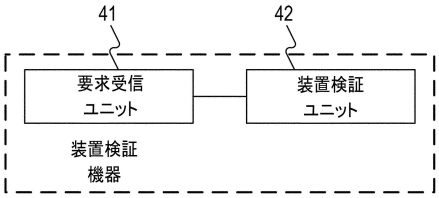
【図２】


対象装置
サーバ
201 第1の装置属性情報を収集する
202 装置検証要求(装置証明書及び第1の装置属性情報)
203 装置証明書の装置指紋が、第1の装置属性情報と一致するかどうかを判定する
204 対象サービスを実行できるようにする
205 対象サービスを実行できないようにする

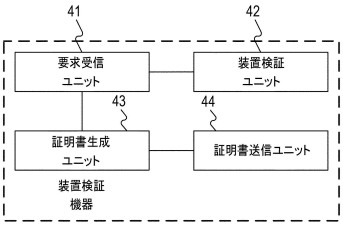
【図３】


対象装置
サーバ
301 第2の装置属性情報を収集し、且つ公開鍵-秘密鍵ペアを生成する
302 証明書申請要求(公開鍵及び第2の装置属性情報)
303 第2の装置属性情報に従って装置指紋を生成する
304 装置証明書を生成する
305 装置証明書を送信する

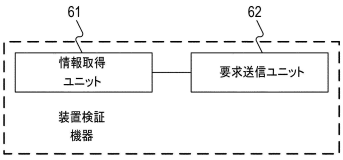
【図４】


41
42
要求受信ユニット
装置検証ユニット
装置検証機器

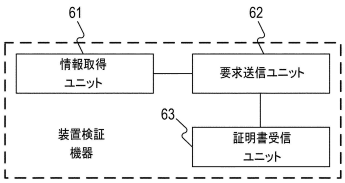
【図５】


41
42
要求受信
ユニット
装置検証
ユニット
43
44
証明書生成
ユニット
証明書送信ユニット
装置検証
機器

【図６】


61
62
情報取得
ユニット
要求送信ユニット
装置検証
機器

【図７】


61
62
情報取得
ユニット
要求送信ユニット
63
装置検証
機器
証明書受信
ユニット

フロントページの続き

(72)発明者　グオ，ホンハイ
中華人民共和国，ジャージャン　３１１１２１，ハンチョウ，ユハン　ディストリクト，ウェスト　ウェン　イ　ロード　ナンバー　９６９，ビルディング　３，５／エフ，アリババ　グループ　リーガル　デパートメント
(72)発明者　リ，シャオフェン
中華人民共和国，ジャージャン　３１１１２１，ハンチョウ，ユハン　ディストリクト，ウェスト　ウェン　イ　ロード　ナンバー　９６９，ビルディング　３，５／エフ，アリババ　グループ　リーガル　デパートメント

審査官　宮司　卓佳

(56)参考文献　特開平１０－２６０９３９（ＪＰ，Ａ）
特開２００２－２３６５２２（ＪＰ，Ａ）
特開２００６－３２３８６０（ＪＰ，Ａ）
特開２０１４－１７４５６０（ＪＰ，Ａ）
米国特許出願公開第２０１１／００９３９２０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４
Ｈ０４Ｌ　９／３２