(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6967449号
(P6967449)
(45)発行日　令和3年11月17日(2021.11.17)　(24)登録日　令和3年10月27日(2021.10.27)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
G06F 21/31	(2013.01)	G06F	21/31	
G09C 1/00	(2006.01)	G09C	1/00	640E

請求項の数 17　(全 26 頁)

(21)出願番号	特願2017-518082(P2017-518082)
(86)(22)出願日	平成27年9月30日(2015.9.30)
(65)公表番号	特表2017-531951(P2017-531951A)
(43)公表日	平成29年10月26日(2017.10.26)
(86)国際出願番号	PCT/CN2015/091235
(87)国際公開番号	WO2016/054990
(87)国際公開日	平成28年4月14日(2016.4.14)
審査請求日	平成30年9月27日(2018.9.27)
審判番号	不服2020-5861(P2020-5861/J1)
審判請求日	令和2年4月30日(2020.4.30)
(31)優先権主張番号	201410532781.9
(32)優先日	平成26年10月10日(2014.10.10)
(33)優先権主張国・地域又は機関	中国(CN)

(73)特許権者　520015461
アドバンスド　ニュー　テクノロジーズ　カンパニー　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ケーワイ１－９００８　ジョージ　タウン　ホスピタル　ロード　２７　ケイマン　コーポレート　センター
(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】セキュリティチェックのための方法、デバイス、端末およびサーバ

(57)【特許請求の範囲】
【請求項１】
サーバにおいて行われるセキュリティチェックのモードであるオリジナルチェックモードのためのオリジナルチェック認証情報と、端末においてローカルで行われるセキュリティチェックのモードである更新チェックモードのための代用認証情報とを用いて、ネットワークアプリケーションにアクセスするためにセキュリティチェックを行うセキュリティチェック方法であって、
前記端末が、前記更新チェックモードが使用される場合に端末ユーザによって入力される、前記オリジナルチェックモードのオリジナルチェック認証情報を取得する工程であって、前記オリジナルチェック認証情報は、ユーザ登録時に前記サーバに登録される、工程と、
前記端末が、前記代用認証情報を生成する工程と、
前記端末が、前記端末ユーザのユーザ情報に対応する前記登録されたオリジナルチェック認証情報が前記入力されたオリジナルチェック認証情報と一致する場合に、前記ユーザ情報に対応づけて前記代用認証情報を前記サーバに格納させるために、前記入力されたオリジナルチェック認証情報、前記代用認証情報および前記ユーザ情報を前記サーバへ送信する工程と、
前記端末が、ローカルチェック結果を取得するために、前記更新チェックモードでローカルチェックを行う工程と、
前記端末が、前記代用認証情報に従って前記ローカルチェック結果を暗号化して、暗号

化チェック結果を取得する工程と、
前記端末が、前記暗号化チェック結果、前記ローカルチェック結果および前記ユーザ情報をサーバへ送信する工程と、
前記端末が、前記ユーザ情報に対応する代用認証情報に従った前記暗号化チェック結果の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程と、を含むセキュリティチェック方法。
【請求項２】
前記端末が、前記端末ユーザに関連付けられた信頼される記憶領域内に前記代用認証情報を格納する工程であって、前記信頼される記憶領域は、信頼される実行環境（ＴＥＥ）モジュールまたはセキュリティ環境（ＳＥ）モジュールを含む、工程をさらに含む、請求項１に記載の方法。
【請求項３】
前記代用認証情報は、公開鍵と秘密鍵とを含み、
前記端末が、前記代用認証情報を前記サーバへ送信する工程は、前記端末が、前記公開鍵を前記サーバへ送信する工程をさらに含み、
前記端末が、暗号化チェック結果を取得するために、格納された代用認証情報に従って前記ローカルチェック結果を暗号化する工程は、前記端末が、署名情報を取得するために、前記格納された秘密鍵に従って前記ローカルチェック結果にデジタル的に署名する工程をさらに含み、および
前記端末が、前記暗号化チェック結果を前記サーバへ送信する工程は、前記端末が、前記署名情報を前記サーバへ送信する工程をさらに含み、
前記端末が、前記ユーザ情報に対応する代用認証情報に従った前記暗号化チェック結果の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程は、前記端末が、前記ユーザ情報に対応する前記公開鍵に従った前記署名情報の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程を含む、請求項１に記載の方法。
【請求項４】
前記代用認証情報は、ランダムストリングであり、
前記端末が、前記代用認証情報を前記サーバへ送信する工程は、前記端末が、前記ランダムストリングを前記サーバへ送信する工程をさらに含み、
前記端末が、暗号化チェック結果を取得するために、格納された代用認証情報に従って前記ローカルチェック結果を暗号化する工程は、前記端末が、第１の暗号化データ結果を取得するために、メッセージアブストラクトアルゴリズムにより前記ランダムストリングと前記ローカルチェック結果とを暗号化する工程をさらに含み、および
前記端末が、前記暗号化チェック結果を前記サーバへ送信する工程は、前記端末が、第２の暗号化データ結果を取得するために前記第１の暗号化データ結果を前記サーバへ送信する工程をさらに含み、
前記端末が、前記ユーザ情報に対応する代用認証情報に従った前記暗号化チェック結果の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程は、前記端末が、前記第２の暗号化データ結果が前記第１の暗号化データ結果と一致する場合に、前記ネットワークアプリケーションへアクセスする工程を含む、請求項１に記載の方法。
【請求項５】
サーバが、端末により送信される暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信する工程であって、前記暗号化チェック結果は、格納された代用認証情報に従って前記ローカルチェック結果を暗号化することにより生成される情報であり、前記代用認証情報は、前記端末においてローカルで行われるセキュリティチェックのモードである更新チェックモードを使用することにより生成される情報であり、および前記ローカルチェック結果は、前記端末ユーザがセキュリティチェックを行う場合に、前記更新チェックモードでローカルチェックを行うことにより取得される情報である、工

程と、
前記サーバが、前記ユーザ情報に対応する代用認証情報を取得する工程と、
前記サーバが、前記ユーザ情報に対応する前記代用認証情報に従って前記暗号化チェック結果を検証し、かつ前記検証がパスすると、前記ローカルチェック結果が信頼できると判断する工程とを含むセキュリティチェック方法であって、
前記端末が前記更新チェックモードを使用する場合に、前記サーバが、前記端末により送信された、前記端末において前記端末ユーザにより入力されたオリジナルチェック認証情報、代用認証情報、および前記ユーザ情報を受信する工程であって、前記入力されたオリジナルチェック認証情報は、前記サーバにおいて行われるセキュリティチェックのモードであるオリジナルチェックモードのチェック認証情報であり、および前記代用認証情報は、前記更新チェックモードのために前記端末により生成される情報である、工程と、
前記サーバが、前記ユーザ情報に対応する、ユーザ登録時に登録されたオリジナルチェック認証情報を検索する工程と、
前記サーバが、前記入力されたオリジナルチェック認証情報が前記登録されたオリジナルチェック認証情報と一致するかどうかを判断する工程と、
前記サーバが、前記入力されたオリジナルチェック認証情報が前記登録されたオリジナルチェック認証情報と一致すると、前記代用認証情報と前記ユーザ情報との相関を格納する工程とをさらに含む、方法。
【請求項６】
前記代用認証情報は、公開鍵と秘密鍵とを含み、
前記サーバが、前記端末により送信された代用認証情報を受信する工程は、前記サーバが、前記端末により送信された前記公開鍵を受信する工程をさらに含み、
前記サーバが、前記端末により送信された暗号化チェック結果を受信する工程は、前記サーバが、前記端末により送信された署名情報を受信する工程であって、前記署名情報は、前記格納された秘密鍵に従って前記ローカルチェック結果にデジタル的に署名することにより取得される情報である、工程をさらに含み、
前記サーバが、前記ユーザ情報に対応する代用認証情報を取得する工程は、前記サーバが、前記相関を検索することにより、前記ユーザ情報に対応する公開鍵を取得する工程をさらに含み、および
前記サーバが、前記ユーザ情報に対応する前記代用認証情報に従って前記暗号化チェック結果を検証する工程は、前記サーバが、前記ユーザ情報に対応する前記公開鍵を介して前記署名情報を検証する工程をさらに含む、請求項５に記載の方法。
【請求項７】
前記代用認証情報は、ランダムストリングであり、
前記サーバが、前記端末により送信された代用認証情報を受信する工程は、前記サーバが、前記端末により送信された前記ランダムストリングを受信するさらに工程を含み、
前記サーバが、前記端末により送信された暗号化チェック結果を受信する工程は、前記サーバが、前記端末により送信された第１の暗号化データ結果を受信する工程であって、前記第１の暗号化データ結果は、メッセージアブストラクトアルゴリズムにより前記ランダムストリングと前記ローカルチェック結果とを暗号化することにより取得される情報である、工程をさらに含み、
前記サーバが、前記ユーザ情報に対応する代用認証情報を取得する工程は、前記サーバが、前記相関を検索することにより、前記ユーザ情報に対応するランダムストリングを取得する工程をさらに含み、および
前記サーバが、前記ユーザ情報に対応する前記代用認証情報に従って前記暗号化チェック結果を検証する工程は、前記サーバが、第２の暗号化データ結果を取得するために、前記ユーザ情報に対応するランダムストリングと前記ローカルチェック結果とを前記メッセージアブストラクトアルゴリズムにより暗号化する工程と、前記サーバが、前記第２の暗号化データ結果が前記第１の暗号化データ結果と一致するかどうかを判断する工程であって、前記第２の暗号化データ結果が前記第１の暗号化データ結果と一致する場合に前記検

証はパスする、工程とをさらに含む、請求項５に記載の方法。
【請求項８】
プロセッサと前記プロセッサにより実行可能な命令を格納するためのメモリとを含む端末であって、前記命令は、前記端末の前記プロセッサに、サーバにおいて行われるセキュリティチェックのモードであるオリジナルチェックモードのためのオリジナルチェック認証情報と、前記端末においてローカルで行われるセキュリティチェックのモードである更新チェックモードのための代用認証情報とを用いて、ネットワークアプリケーションにアクセスするためにセキュリティチェックを行うセキュリティチェック方法を行わせるように構成され、前記方法は、
前記更新チェックモードが使用される場合に端末ユーザによって入力される、前記オリジナルチェックモードのオリジナルチェック認証情報を取得する工程であって、前記オリジナルチェック認証情報は、ユーザ登録時に前記サーバに登録される、工程と、
前記代用認証情報を生成する工程と、
前記端末ユーザのユーザ情報に対応する前記登録されたオリジナルチェック認証情報が前記入力されたオリジナルチェック認証情報と一致する場合に、前記ユーザ情報に対応づけて前記代用認証情報を前記サーバに格納させるために、前記入力されたオリジナルチェック認証情報、前記代用認証情報および前記ユーザ情報を前記サーバへ送信する工程と、
ローカルチェック結果を取得するために、前記更新チェックモードでローカルチェックを行う工程と、
前記代用認証情報に従って前記ローカルチェック結果を暗号化して、暗号化チェック結果を取得する工程と、
前記暗号化チェック結果、前記ローカルチェック結果および前記ユーザ情報をサーバへ送信する工程と、
前記ユーザ情報に対応する代用認証情報に従った前記暗号化チェック結果の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程と、を含む、
端末。
【請求項９】
プロセッサと前記プロセッサにより実行可能な命令を格納するためのメモリとを含むサーバであって、前記命令は、前記サーバの前記プロセッサにセキュリティチェック方法を行わせるように構成され、前記方法は、
端末により送信される暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信する工程であって、前記暗号化チェック結果は、格納された代用認証情報に従って前記ローカルチェック結果を暗号化することにより生成される情報であり、前記代用認証情報は、前記端末においてローカルで行われるセキュリティチェックのモードである更新チェックモードを使用することにより生成される情報であり、および前記ローカルチェック結果は、前記端末ユーザがセキュリティチェックを行う場合に、前記更新チェックモードでローカルチェックを行うことにより取得される情報である、工程と、
前記ユーザ情報に対応する代用認証情報を取得する工程と、
前記ユーザ情報に対応する前記代用認証情報に従って前記暗号化チェック結果を検証し、かつ前記検証がパスすると、前記ローカルチェック結果が信頼できると判断する工程とを含み、
前記端末が前記更新チェックモードを使用する場合に、前記端末により送信された、前記端末において前記端末ユーザにより入力されたオリジナルチェック認証情報、代用認証情報、および前記ユーザ情報を受信する工程であって、前記入力されたオリジナルチェック認証情報は、前記サーバにおいて行われるセキュリティチェックのモードであるオリジナルチェックモードのチェック認証情報であり、および前記代用認証情報は、前記更新チェックモードのために前記端末により生成される情報である、工程と、
前記ユーザ情報に対応する、ユーザ登録時に登録されたオリジナルチェック認証情報を検索する工程と、
前記入力されたオリジナルチェック認証情報が前記登録されたオリジナルチェック認証

情報と一致するかどうかを判断する工程と、
前記入力されたオリジナルチェック認証情報が前記登録されたオリジナルチェック認証情報と一致すると、前記代用認証情報と前記ユーザ情報との相関を格納する工程と
をさらに含む、
サーバ。
【請求項１０】
前記代用認証情報は、信頼される実行環境（ＴＥＥ）モジュールまたはセキュリティ環境（ＳＥ）モジュールに格納される、請求項８に記載の端末。
【請求項１１】
命令の組を記憶する非一時的コンピュータ可読媒体であって、前記命令の組は、端末装置に、サーバにおいて行われるセキュリティチェックのモードであるオリジナルチェックモードのためのオリジナルチェック認証情報と、前記端末装置においてローカルで行われるセキュリティチェックのモードである更新チェックモードのための代用認証情報とを用いて、ネットワークアプリケーションにアクセスするためにセキュリティチェックを行うセキュリティチェック方法を実行させるように、前記端末装置の少なくとも１つのプロセッサによって実行可能であり、前記方法は、
前記更新チェックモードが使用される場合に端末装置ユーザによって入力される、前記オリジナルチェックモードのオリジナルチェック認証情報を取得する工程であって、前記オリジナルチェック認証情報は、ユーザ登録時に前記サーバに登録される、工程と、
前記代用認証情報を生成する工程と、
前記端末装置ユーザのユーザ情報に対応する前記登録されたオリジナルチェック認証情報が前記入力されたオリジナルチェック認証情報と一致する場合に、前記ユーザ情報に対応づけて前記代用認証情報を前記サーバに格納させるために、前記入力されたオリジナルチェック認証情報、前記代用認証情報および前記ユーザ情報を前記サーバへ送信する工程と、
ローカルチェック結果を取得するために、前記更新チェックモードでローカルチェックを行う工程と、
前記代用認証情報に従って前記ローカルチェック結果を暗号化して、暗号化チェック結果を取得する工程と、
前記暗号化チェック結果、前記ローカルチェック結果および前記ユーザ情報をサーバへ送信する工程と、
前記ユーザ情報に対応する代用認証情報に従った前記暗号化チェック結果の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程と、を含む、
非一時的コンピュータ可読媒体。
【請求項１２】
前記命令の組は、前記端末装置に、
前記端末装置ユーザに関連付けられた信頼される記憶領域内に前記代用認証情報を格納する工程であって、前記信頼される記憶領域は、信頼される実行環境（ＴＥＥ）モジュールまたはセキュリティ環境（ＳＥ）モジュールを含む、工程
を実行させるように、前記端末装置の前記少なくとも１つのプロセッサによって実行可能である、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】
前記代用認証情報は、公開鍵と秘密鍵とを含み、
前記命令の組は、前記端末装置に、前記公開鍵を前記サーバへ送信することにより前記代用認証情報を前記サーバへ送信する工程を実行させるように、前記端末装置の前記少なくとも１つのプロセッサによって実行可能であり、
前記命令の組は、前記端末装置に、署名情報を取得すべく前記格納された秘密鍵に従って前記ローカルチェック結果にデジタル的に署名することにより、暗号化チェック結果を取得するために、格納された代用認証情報に従って前記ローカルチェック結果を暗号化する工程を実行させるように、前記端末装置の前記少なくとも１つのプロセッサによって実

行可能であり、
前記命令の組は、前記端末装置に、前記署名情報を前記サーバへ送信することにより前記暗号化チェック結果を前記サーバへ送信する工程を実行させるように、前記端末装置の前記少なくとも１つのプロセッサによって実行可能であり、
前記ユーザ情報に対応する代用認証情報に従った前記暗号化チェック結果の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程は、前記ユーザ情報に対応する前記公開鍵に従った前記署名情報の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程を含む、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１４】
前記代用認証情報は、ランダムストリングであり、
前記命令の組は、前記端末装置に、前記ランダムストリングを前記サーバへ送信することにより前記代用認証情報を前記サーバへ送信する工程を実行させるように、前記端末装置の前記少なくとも１つのプロセッサによって実行可能であり、
前記命令の組は、前記端末装置に、第１の暗号化データ結果を取得すべくメッセージアブストラクトアルゴリズムにより前記ランダムストリングと前記ローカルチェック結果とを暗号化することにより、暗号化チェック結果を取得するために、格納された代用認証情報に従って前記ローカルチェック結果を暗号化する工程を実行させるように、前記端末装置の前記少なくとも１つのプロセッサによって実行可能であり、
前記命令の組は、前記端末装置に、第２の暗号化データ結果を取得すべく前記第１の暗号化データ結果を前記サーバへ送信することにより、前記暗号化チェック結果を前記サーバへ送信する工程を実行させるように、前記端末装置の前記少なくとも１つのプロセッサによって実行可能であり、
前記ユーザ情報に対応する代用認証情報に従った前記暗号化チェック結果の検証がパスする場合に、前記ネットワークアプリケーションへアクセスする工程は、前記第２の暗号化データ結果が前記第１の暗号化データ結果と一致する場合に、前記ネットワークアプリケーションへアクセスする工程を含む、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１５】
命令の組を記憶する非一時的コンピュータ可読媒体であって、前記命令の組は、サーバにセキュリティチェック方法を実行させるように、前記サーバの少なくとも１つのプロセッサによって実行可能であり、前記方法は、
端末により送信される暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信する工程であって、前記暗号化チェック結果は、格納された代用認証情報に従って前記ローカルチェック結果を暗号化することにより生成される情報であり、前記代用認証情報は、前記端末においてローカルで行われるセキュリティチェックのモードである更新チェックモードを使用することにより生成される情報であり、および前記ローカルチェック結果は、前記端末ユーザがセキュリティチェックを行う場合に、前記更新チェックモードでローカルチェックを行うことにより取得される情報である、工程と、
前記ユーザ情報に対応する代用認証情報を取得する工程と、
前記ユーザ情報に対応する前記代用認証情報に従って前記暗号化チェック結果を検証し、かつ前記検証がパスすると、前記ローカルチェック結果が信頼できると判断する工程とを含み、
前記端末が前記更新チェックモードを使用する場合に、前記端末により送信された、前記端末において前記端末ユーザにより入力されたオリジナルチェック認証情報、代用認証情報、および前記ユーザ情報を受信する工程であって、前記入力されたオリジナルチェック認証情報は、前記サーバにおいて行われるセキュリティチェックのモードであるオリジナルチェックモードのチェック認証情報であり、および前記代用認証情報は、前記更新チェックモードのために前記端末により生成される情報である、工程と、
前記ユーザ情報に対応する、ユーザ登録時に登録されたオリジナルチェック認証情報を

検索する工程と、
前記入力されたオリジナルチェック認証情報が前記登録されたオリジナルチェック認証情報と一致するかどうかを判断する工程と、
前記入力されたオリジナルチェック認証情報が前記登録されたオリジナルチェック認証情報と一致すると、前記代用認証情報と前記ユーザ情報との相関を格納する工程と
をさらに含む、
非一時的コンピュータ可読媒体。
【請求項１６】
前記代用認証情報は、公開鍵と秘密鍵とを含み、
前記命令の組は、前記サーバに、前記端末により送信された前記公開鍵を受信することにより、前記端末により送信された代用認証情報を受信する工程を実行させるように、前記サーバの前記少なくとも１つのプロセッサによって実行可能であり、
前記命令の組は、前記サーバに、前記端末により送信された署名情報を受信することにより、前記端末により送信された暗号化チェック結果を受信する工程を実行させるように、前記サーバの前記少なくとも１つのプロセッサによって実行可能であり、前記署名情報は、前記格納された秘密鍵に従って前記ローカルチェック結果にデジタル的に署名することにより取得される情報であり、
前記命令の組は、前記サーバに、前記相関を検索することによって前記ユーザ情報に対応する公開鍵を取得することにより、前記ユーザ情報に対応する代用認証情報を取得する工程を実行させるように、前記サーバの前記少なくとも１つのプロセッサによって実行可能であり、
前記命令の組は、前記サーバに、前記ユーザ情報に対応する前記公開鍵を介して前記署名情報を検証することにより、前記ユーザ情報に対応する前記代用認証情報に従って前記暗号化チェック結果を検証する工程を実行させるように、前記サーバの前記少なくとも１つのプロセッサによって実行可能である、請求項１５に記載の非一時的コンピュータ可読媒体。
【請求項１７】
前記代用認証情報は、ランダムストリングであり、
前記命令の組は、前記サーバに、前記端末により送信された前記ランダムストリングを受信することにより、前記端末により送信された代用認証情報を受信する工程を実行させるように、前記サーバの前記少なくとも１つのプロセッサによって実行可能であり、
前記命令の組は、前記サーバに、前記端末により送信された第１の暗号化データ結果を受信することにより、前記端末により送信された暗号化チェック結果を受信する工程を実行させるように、前記サーバの前記少なくとも１つのプロセッサによって実行可能であり、前記第１の暗号化データ結果は、メッセージアブストラクトアルゴリズムにより前記ランダムストリングと前記ローカルチェック結果とを暗号化することにより取得される情報であり、
前記ユーザ情報に対応する代用認証情報を取得する工程は、前記相関を検索することにより、前記ユーザ情報に対応するランダムストリングを取得する工程をさらに含み、
前記ユーザ情報に対応する前記代用認証情報に従って前記暗号化チェック結果を検証する工程は、第２の暗号化データ結果を取得するために、前記ユーザ情報に対応するランダムストリングと前記ローカルチェック結果とを前記メッセージアブストラクトアルゴリズムにより暗号化する工程と、前記第２の暗号化データ結果が前記第１の暗号化データ結果と一致するかどうかを判断する工程であって、前記第２の暗号化データ結果が前記第１の暗号化データ結果と一致する場合に前記検証はパスする、工程とを含む、請求項１５に記載の非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【発明の概要】
【０００１】
技術分野

本開示は、通信技術の分野に関し、特にセキュリティチェックのための方法、デバイス、端末およびサーバに関する。

【０００２】

背景

スマート端末およびネットワークアプリケーションの発展と共に、ユーザは、端末上にインストールされた様々なクライアントアプリケーションを介して様々なネットワークアプリケーションへアクセスし得る。アクセス中、ユーザは、通常、識別子認証、会員登録、ネットワークトランザクションなどを行う必要がある。一方、アプリケーションサーバは、ユーザ識別子を検証し得る。検証の伝統的モードは、アプリケーションサーバチェックである。すなわち、ユーザは、予め設定されたチェックパスワードを端末を介してアプリケーションサーバへ送信し、チェックパスワードがユーザ登録時のパスワードと一致するとアプリケーションサーバが検証すると、チェックはパスする。しかし、上記チェックモードにおけるチェックパスワードは、トロイプログラムを介して悪意のある第三者により容易に盗まれ得る。したがって、一般的に、チェック中、端末ローカルチェックがアプリケーションサーバチェックの代替となり得る。例えば、アプリケーションサーバにより送信されたチェック促進情報に基づき、端末は、ユーザ識別子チェックを完了し、チェック結果をサーバへ送信するために、ユーザ生体測定ベース指紋チェック（user-biometric-based fingerprint check）、動的識別ベースジェスチャチェック（dynamic-identifying-based gesture check）などをローカルで行う。

【０００３】

しかし、端末ローカルチェックがアプリケーションサーバチェックを置換するために使用される場合、悪意のある第三者がサーバと相互作用するために端末を装い、偽造された端末ローカルチェック結果をサーバへ送信すれば、サーバは、代用チェックモードとして機能する端末ローカルチェックモードの信用性を判断することができず、これにより既存セキュリティチェックモードの信頼性が不十分となり、かつネットワークアプリケーションのアクセス安全性が低下する。

【０００４】

概要

本開示の実施形態は、従来技術のセキュリティチェックモードの不十分な信頼性の問題に対処するためのセキュリティチェックのための方法、デバイス、端末およびサーバを提供する。

【０００５】

本開示の第１の態様は、セキュリティチェック方法を提供する。本方法は、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードを介してローカルチェックを行う工程と、格納された代用認証情報に従ってローカルチェック結果を暗号化して、暗号化チェック結果を取得する工程であって、代用認証情報は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合に生成される、工程と、暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報をサーバへ送信する工程であって、それにより、サーバは、ユーザ情報に対応する代用認証情報に従った暗号化チェック結果の検証がパスすると、ローカルチェック結果が信頼できると判断する、工程とを含む。

【０００６】

本開示の第２の態様は、セキュリティチェック方法をさらに提供する。本方法は、端末により送信される暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信する工程であって、暗号化チェック結果は、格納された代用認証情報に従って端末がローカルチェック結果を暗号化する場合に生成され、代用認証情報は、端末がオリジナルチェックモードを置換するために更新チェックモードを使用する場合に生成され、およびローカルチェック結果は、端末ユーザがセキュリティチェックを行う場合に、更新チェックモードを介してローカルチェックを行う端末により取得される、工程と、ユーザ情報に対応する代用認証情報を取得する工程と、ユーザ情報に対応する代用認証情報に従

って暗号化チェック結果を検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断する工程とを含む。

【０００７】

本開示の第３の態様は、セキュリティチェックデバイスをさらに提供する。本セキュリティチェックデバイスは、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードを介してローカルチェックを行うために使用されるチェックユニットと、格納された代用認証情報に従ってローカルチェック結果を暗号化して、暗号化チェック結果を取得するために使用される暗号化ユニットであって、代用認証情報は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合に生成される、暗号化ユニットと、暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報をサーバへ送信することであって、それにより、サーバは、ユーザ情報に対応する第２の代用認証情報に従った暗号化チェック結果の検証がパスすると、ローカルチェック結果が信頼できると判断する、送信することのために使用される第１の送信ユニットとを含む。

【０００８】

本開示の第４の態様は、セキュリティチェックデバイスをさらに提供する。本デバイスは、端末により送信される暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信するために使用される第１の受信ユニットであって、暗号化チェック結果は、格納された代用認証情報に従って端末がローカルチェック結果を暗号化する場合に生成され、代用認証情報は、端末がオリジナルチェックモードを置換するために更新チェックモードを使用する場合に生成され、およびローカルチェック結果は、端末ユーザがセキュリティチェックを行う場合に、更新チェックモードを介してローカルチェックを行う端末により取得される、第１の受信ユニットと、ユーザ情報に対応する代用認証情報を取得するために使用される取得ユニットと、ユーザ情報に対応する代用認証情報に従って暗号化チェック結果を検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断するために使用されるチェックユニットとを含む。

【０００９】

本開示の第５の態様は、端末をさらに提供する。本端末は、プロセッサとプロセッサにより実行可能な命令を格納するメモリとを含み、プロセッサは、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードを介してローカルチェックを行うことと、格納された代用認証情報に従ってローカルチェック結果を暗号化して、暗号化チェック結果を取得することであって、代用認証情報は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合に生成される、取得することと、暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報をサーバへ送信することであって、それにより、サーバは、ユーザ情報に対応する代用認証情報に従った暗号化チェック結果の検証がパスすると、ローカルチェック結果が信頼できると判断する、送信することとを行うように構成される。

【００１０】

本開示の第６の態様は、サーバを提供する。本サーバは、プロセッサとプロセッサにより実行可能な命令を格納するためのメモリとを含む。本プロセッサは、端末により送信される暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信することであって、暗号化チェック結果は、格納された代用認証情報に従って端末がローカルチェック結果を暗号化する場合に生成され、代用認証情報は、端末がオリジナルチェックモードを置換するために更新チェックモードを使用する場合に生成され、およびローカルチェック結果は、端末ユーザがセキュリティチェックを行う場合に、更新チェックモードを介してローカルチェックを行う端末により取得される、受信することと、ユーザ情報に対応する代用認証情報を取得することと、ユーザ情報に対応する代用認証情報に従って暗号化チェック結果を検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断することとを行うように構成される。

【００１１】

本開示の実施形態では、オリジナルチェックモードが更新チェックモードにより置換される場合、端末とサーバとの両方が更新チェックモード用に生成された代用認証情報を格納する。したがって、更新チェックモードがチェックに使用される場合、ローカルチェック結果は代用認証情報に従って暗号化され得る。また、対応するサーバは、端末により暗号化および送信された暗号化チェック結果を代用認証情報に従って検証し、次に検証がパスすると、ローカルチェック結果が信頼できると判断し得る。本開示の実施形態を適用することにより、悪意のある第三者は代用認証情報を取得することができず、およびセキュリティチェックは、悪意のある第三者がローカルチェック結果を取得する場合でも完了され得ない。したがって、本開示の実施形態は、セキュリティチェックの信頼性を改善し、かつネットワークアプリケーションのアクセスを安全にし得る。

【図面の簡単な説明】

【００１２】

【図１】本開示の実施形態によるセキュリティチェックシナリオの概略図である。

【図２Ａ】本開示の実施形態によるセキュリティチェック方法のフローチャートである。

【図２Ｂ】本開示の実施形態によるセキュリティチェック方法のフローチャートである。

【図３】本開示の実施形態による別のセキュリティチェック方法のフローチャートである。

【図４】本開示の実施形態による別のセキュリティチェック方法のフローチャートである。

【図５】セキュリティチェックのためのデバイスが本開示の実施形態に従って配置されるデバイスのハードウェア構造図である。

【図６】本開示の実施形態によるセキュリティチェックのためのデバイスのブロック図である。

【図７】本開示の実施形態によるセキュリティチェックのための別のデバイスのブロック図である。

【図８】本開示の実施形態によるセキュリティチェックのための別のデバイスのブロック図である。

【図９】本開示の実施形態によるセキュリティチェックのための別のデバイスのブロック図である。

【発明を実施するための形態】

【００１３】

詳細な説明

例示的実施形態が本明細書において詳細に説明され、実施形態の例を添付図面に示す。添付図面が以下に説明される場合、特記しない限り、様々な図面内の同じ参照符号は同じまたは同様の要素を示す。以下の例示的実施形態において説明される実施形態は、本開示に一致するすべての実施形態を表さない。逆に、これらは、本開示の特許請求の範囲において詳細に説明されるいくつかの態様に一致するデバイスおよび方法の単なる例である。

【００１４】

本開示において使用される用語は、本開示を限定するのではなく、むしろ特定の実施形態を単に説明するためのみのものである。本開示および特許請求の範囲において使用される「１つの」、「前記」、および「その」などの単数形式は、文脈内に別途明示しない限り、複数形式も含むように意図されている。本明細書で使用される用語「および／または」は、１つまたは複数の関連する列記項目のうちの任意のものまたはそのすべての可能な組み合わせを示し、かつ包含することも理解すべきである。

【００１５】

「第１」、「第２」、「第３」などの用語が様々な要素を説明するために本開示において使用され得るが、これらの要素は、これらの用語により限定されるものではないことも理解すべきである。これらの用語は同じタイプの要素を単に識別するために使用される。例えば、本開示の範囲から逸脱することなく、第１の要素は第２の要素とも呼ばれ得る。同様に、第２の要素は第１の要素とも呼ばれ得る。文脈により、本明細書で使用されるよ

うに、用語「～場合」は、「～のとき」、「～すると」、または「～と判断することに応じて」と解釈され得る。

【００１６】

インターネットに基づく通信のシナリオでは、ユーザは、ユーザにより保持される端末上にインストールされた様々なクライアントアプリケーションを介して様々なネットワークアプリケーションへアクセスし得、アクセス中、ユーザは、通常、識別子認証、会員登録、ネットワークトランザクションなどを行う必要がある。上記アクセスを安全にするために、サーバはユーザ識別子に関するセキュリティチェックを行う必要がある。端末ローカルチェックモードがサーバエンドチェックモードを徐々に置換している。しかし、悪意のある第三者が置換中に端末ローカルチェック結果を容易に偽造し、サーバと相互作用し得るため、セキュリティチェックの信頼性が悪化する。本開示の実施形態に従ってセキュリティチェックを実施するためのアプリケーションシナリオの概略図である図１を参照すると、端末とサーバとの間のチェックのすべてがインターネットに基づいて行われる。オリジナルチェックモードを更新チェックモードで置換中、端末とサーバとの両方が更新チェックモード用に生成された代用認証情報を格納するため、更新チェックモードがチェックに使用される場合、ローカルチェック結果は、代用認証情報に従って暗号化され得、対応するサーバは、端末により暗号化および送信された暗号化チェック結果を代用認証情報に従って検証し得る。また、セキュリティチェックの信頼性を改善し、かつネットワークアプリケーションのアクセスを安全にするために、ローカルチェック結果は、検証がパスすると、信頼できるとさらに判断され得る。本開示の実施形態について以下に詳細に説明する。

【００１７】

図２Ａは、本開示の実施形態によるセキュリティチェック方法のフローチャートである。本方法の実施形態は、セキュリティチェックが行われる端末側から説明する。本方法は工程２０１～２０３を含む。

【００１８】

工程２０１において、端末ユーザがセキュリティチェックを行うと、ローカルチェック結果を取得するためにローカルチェックが更新チェックモードを介して行われる。

【００１９】

例えば、サーバ側において行われるセキュリティチェックのモードは、オリジナルチェックモードと呼ばれ得、オリジナルチェックモードは、通常、端末ユーザ登録時に格納されたチェックパスワードによりサーバがチェックを行う工程を含む。端末においてローカルで行われるセキュリティチェックのモードは、更新チェックモードと呼ばれ得る。更新チェックモードは、指紋チェックモード、ジェスチャチェックモード、顔ポーズチェックモードなどを含み得る。

【００２０】

例えば、更新チェックモードがオリジナルチェックモードを置換するために使用される場合、端末は、オリジナルチェックモードに関する第１のオリジナルチェック認証情報を取得し得、第１のオリジナルチェック認証情報は、端末ユーザ登録時に設定されたチェックパスワードであり得る。端末は、更新チェックモードのための代用認証情報を生成し、第１のオリジナルチェック認証情報、代用認証情報および端末ユーザのユーザ情報をサーバへ送信し、代用認証情報は、鍵またはランダムストリングであり得、ユーザ情報は、端末ユーザのユーザ名であり、端末の端末識別子をさらに含み得る。端末ユーザは、ユーザ情報により一意的に識別され得る。一方、端末は、生成された代用認証情報をローカルに格納し得る。例えば、代用認証情報は、信頼実行環境（ＴＥＥ）モジュールまたはセキュリティ環境（ＳＥ）モジュール内に格納され得る。第１のオリジナルチェック認証情報、代用認証情報および端末ユーザのユーザ情報を受信した後、サーバは、ユーザ情報に対応する第２のオリジナルチェック認証情報を検索し得る。第２のオリジナルチェック認証情報は、端末ユーザ登録時に端末ユーザにより設定され、端末によりサーバへ送信されるチェックパスワードであり得る。サーバは、比較後に第２のオリジナルチェック認証情報が

第１のオリジナルチェック認証情報と一致した場合に、代用認証情報とユーザ情報との相関を格納し得る。

【００２１】

端末は、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードに従ってローカルチェックを行い得る。更新チェックモードがローカルチェックを行うために使用される場合、サーバは、通常、チェック促進情報を端末へ送信し得、端末は、例えばチェック促進情報に従ってリアルタイムでローカルチェック結果を取得する。

【００２２】

工程２０２において、ローカルチェック結果は、暗号化チェック結果を取得するために、格納された代用認証情報に従って暗号化される。代用認証情報は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合に生成される情報である。

【００２３】

例えば、端末は、ローカルチェック結果を取得した後、格納されておりかつ更新チェックモード用に生成される代用認証情報を取得し得、暗号化チェック結果を取得するために代用認証情報に従ってローカルチェック結果を暗号化し得る。様々なタイプの代用認証情報により、様々な暗号化モードが適用され得る。図３および図４に示す実施形態は、鍵とランダムストリングとをそれぞれ例として取り上げる詳細な説明を提供するが、鍵とランダムストリングとの詳細はここでは省略される。

【００２４】

工程２０３において、暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報がサーバへ送信され、サーバは、暗号化チェック結果がユーザ情報に対応する代用認証情報に従って検証されると、ローカルチェック結果が信頼できると判断する。

【００２５】

上記実施形態から以下のことが分かる。オリジナルチェックモードを更新チェックモードで置換する間に、端末とサーバとの両方が更新チェックモード用に生成された代用認証情報を格納するため、更新チェックモードがチェックに使用される場合、ローカルチェック結果は、代用認証情報に従って暗号化され得、対応するサーバは、端末により暗号化および送信された暗号化チェック結果を代用認証情報に従って検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断し得る。本開示の実施形態を適用することにより、悪意のある第三者は代用認証情報を取得することができず、およびセキュリティチェックは、悪意のある第三者がローカルチェック結果を取得する場合でも完了され得ない。したがって、本方法の実施形態は、セキュリティチェックの信頼性を改善し、かつネットワークアプリケーションのアクセスを安全にし得る。

【００２６】

図２Ｂは、本開示の実施形態による別のセキュリティチェック方法のフローチャートであり、この方法は、どのようにサーバ側からセキュリティチェックを実施するかを説明する。本方法は工程２１１～２１３を含む。

【００２７】

工程２１１において、端末により送信された暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報が受信され得る。

【００２８】

先の工程２０１における説明を参照すると、更新チェックモードがオリジナルチェックモードを置換するために使用される場合、端末は、オリジナルチェックモードの第１のオリジナルチェック認証情報を取得し、更新チェックモードのための代用認証情報を生成し、第１のオリジナルチェック認証情報、代用認証情報および端末ユーザのユーザ情報をサーバへ送信し得る。第１のオリジナルチェック認証情報、代用認証情報および端末ユーザのユーザ情報を受信した後、サーバは、ユーザ情報に対応する第２のオリジナルチェック認証情報を検索し得、サーバは、比較後に第２のオリジナルチェック認証情報が第１のオリジナルチェック認証情報と一致した場合に、代用認証情報とユーザ情報との相関を格納

し得る。

【００２９】

端末ユーザがセキュリティチェックを行う場合、端末は、更新チェックモードに従って取得されるローカルチェック結果、格納された代用認証情報に従ってローカルチェック結果を暗号化することにより生成される暗号化チェック結果、および端末ユーザのユーザ情報をサーバへ送る。

【００３０】

工程２１２において、ユーザ情報に対応する代用認証情報が取得される。

【００３１】

例えば、暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信した後、サーバは、格納された代用認証情報とユーザ情報との相関を検索し、ユーザ情報に対応する代用認証情報を取得し得る。

【００３２】

工程２１３において、暗号化チェック結果は、ユーザ情報に対応する代用認証情報に従って検証され、ローカルチェック結果は、検証がパスすると信頼できると判断される。

【００３３】

例えば、サーバが代用認証情報に従って暗号化チェック結果を検証する場合、様々なタイプの代用認証情報に従って様々な検証モードが使用され得、後の図３および図４に示す実施形態は、鍵とランダムストリングとをそれぞれ例として取り上げた詳細な説明を提供するが、鍵とランダムストリングとの詳細はここでは省略される。暗号化チェック結果の検証がパスすると、サーバは、端末により送信されたローカルチェック結果が信頼できるチェック結果であると判断し得る。

【００３４】

上記実施形態から以下のことが分かる。オリジナルチェックモードを更新チェックモードで置換する間、端末とサーバとの両方が更新チェックモード用に生成された代用認証情報を格納するため、更新チェックモードがチェックに使用される場合、ローカルチェック結果は、代用認証情報に従って暗号化され得、対応するサーバは、端末により暗号化および送信された暗号化チェック結果を代用認証情報に従って検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断し得る。本開示の実施形態の適用では、悪意のある第三者は代用認証情報を取得することができず、およびセキュリティチェックは、悪意のある第三者がローカルチェック結果を取得する場合でも完了され得ず、したがって、この実施形態は、セキュリティチェックの信頼性を改善し、かつネットワークアプリケーションのアクセスを安全にし得る。

【００３５】

図３は、本開示のいくつかの実施形態による別のセキュリティチェック方法のフローチャートである。本実施形態は、端末とサーバとの間の相互作用の観点からセキュリティチェックのプロセスを詳細に説明するために、公開鍵および秘密鍵である代用認証情報を一例として挙げる。本方法は工程３０１～３１２を含み得る。

【００３６】

工程３０１において、端末は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合、オリジナルチェックモードの第１のオリジナルチェック認証情報を取得する。

【００３７】

例えば、サーバ側において行われるセキュリティチェックのモードは、オリジナルチェックモードと呼ばれ得、オリジナルチェックモードは、通常、端末ユーザ登録時に格納されたチェックパスワードを使用してサーバがチェックを行う。端末においてローカルで行われるセキュリティチェックのモードは、更新チェックモードと呼ばれ得、更新チェックモードは、指紋チェックモード、ジェスチャチェックモード、顔ポーズチェックモードなどを含み得る。

【００３８】

いくつかの実施形態において、更新チェックモードがオリジナルチェックモードを置換するために使用される場合、端末は、オリジナルチェックモードの第１のオリジナルチェック認証情報を取得し得、第１のオリジナルチェック認証情報は、端末ユーザ登録時に設定されたチェックパスワードであり得る。オリジナルチェックモードがセキュリティチェックに使用される場合、端末ユーザは、登録時に設定されたユーザ名およびチェックパスワードを端末のセキュリティチェックインターフェース上で入力する。端末は、セキュリティチェック要求内にユーザ名およびチェックパスワードを保持し、セキュリティチェック要求をサーバへ送信し得る。サーバは、ユーザ登録情報内に格納されたユーザ名に対応するチェックパスワードを検索し、取り出されたチェックパスワードが端末により送信されたチェックパスワードと同じであれば、端末ユーザがセキュリティチェックをパスしたと判断し得、端末ユーザにより実行されるサービスオペレーションがリリースされ得る。

【００３９】

工程３０２において、端末は、更新チェックモードの公開鍵と秘密鍵とを生成する。

【００４０】

例えば、オリジナルチェックモードを置換するために更新チェックモードを使用すると判断されると、端末は、更新されたチェックモード用の代用認証情報として機能する鍵（公開鍵と秘密鍵とを含む）を生成し得る。鍵を生成するための任意の鍵生成アルゴリズムが使用され得、アルゴリズムの説明はここでは省略される。

【００４１】

工程３０３において、端末は、端末ユーザに関連付けられた信頼される記憶領域内に秘密鍵を格納する。

【００４２】

例えば、信頼される記憶領域は、ＴＥＥモジュールまたはＳＥモジュールを含み得る。公開鍵と秘密鍵とが生成された後、端末は、秘密鍵を信頼される記憶領域内に格納し得る。

【００４３】

工程３０４において、端末は、第１のオリジナルチェック認証情報、公開鍵および端末ユーザのユーザ情報をサーバへ送信する。

【００４４】

いくつかの実施形態では、ユーザ情報は、端末ユーザのユーザ名（例えば端末ユーザ登録時のユーザ名セット）であり得る。ユーザ情報は、端末の端末識別子（例えば端末のメディアアクセス制御（ＭＡＣ）アドレス）をさらに含み得る。端末ユーザは、ユーザ情報に従って一意的に識別され得る。端末は、取得された第１のオリジナルチェック認証情報、生成された公開鍵、および端末ユーザのユーザ情報をサーバへさらに送信し、サーバは、第１のオリジナルチェック認証情報を検証し得る。

【００４５】

工程３０５において、サーバは、ユーザ情報に対応する第２のオリジナルチェック認証情報を検索する。

【００４６】

サーバ上に登録したすべての端末ユーザに関し、サーバは、これらの端末ユーザのユーザ情報とチェックパスワードとの相関を格納する。チェックパスワードは、チェック認証情報である。いくつかの実施形態では、端末により送信された第１のオリジナルチェック認証情報、公開鍵、および端末ユーザのユーザ情報を受信すると、サーバは、ユーザ情報とチェックパスワードとの相関を検索し、受信したユーザ情報に対応するチェックパスワードを取得し得る。チェックパスワードは、いくつかの実施形態において第２のオリジナルチェック認証情報と呼ばれる。

【００４７】

工程３０６において、サーバは、第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致するかどうかを比較する。

【００４８】

例えば、サーバは、受信された第１のオリジナルチェック認証情報が、発見された第２のオリジナルチェック認証情報と一致するかどうかを比較する。すなわち、サーバにより格納された端末ユーザのチェックパスワードが、端末により送信されたチェックパスワードと同じかどうかを比較することが判断され得、その結果、セキュリティチェックモードを現在置換している対象が端末ユーザ自身かどうかが、さらに判断される。

【００４９】

工程３０７において、サーバは、第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致すると、公開鍵とユーザ情報との相関を格納する。

【００５０】

比較結果に基づき第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致すると判断された場合、サーバは、セキュリティチェックモードを現在置換している対象が端末ユーザ自身であると判断し得る。次に、サーバは、受信された公開鍵とユーザ情報との相関を格納し得る。

【００５１】

工程３０８において、端末は、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードを介してローカルチェックを行う。

【００５２】

端末は、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードを介してローカルチェックを行い得る。更新チェックモードがローカルチェックに使用される場合、チェック促進情報は、通常、サーバにより端末へ送信され、端末は、チェック促進情報に従ってローカルチェック結果をリアルタイムで取得する。例えば、更新チェックモードがジェスチャチェックモードである場合、サーバにより端末へ戻されたジェスチャチェック促進情報が「２」であると仮定すると、端末ユーザは、ジェスチャチェック促進情報に従って２本の指を示し得る。２本の指が画像認識処理技術により認識された後、端末は、ローカルチェック結果として「２」の認識結果を取る。

【００５３】

工程３０９において、端末は、署名情報を取得するために、信頼される記憶領域内に格納された秘密鍵に従ってローカルチェック結果にデジタル的に署名する。

【００５４】

例えば、ローカルチェック結果を取得した後、端末は、格納された秘密鍵を信頼される記憶領域から取得し、ローカルチェック結果にデジタル的に署名するために秘密鍵を使用し得る。デジタル署名技術は、アブストラクト情報が送信側の秘密鍵により暗号化され、オリジナルテキストと共に受信器へ送信され得る暗号化技術である。受信側は、送信側の公開鍵により暗号化アブストラクト情報を解読し、次に、受信されたオリジナルテキストのアブストラクト情報をハッシュ関数により生成し、生成されたアブストラクト情報と解読されたアブストラクト情報とを比較し得る。生成されたアブストラクト情報と解読されたアブストラクト情報とが同じであれば、受信情報が修正されていないことが示され、したがって、情報の完全性が、デジタル署名により検証され得る。本実施形態において、ローカルチェック結果にデジタル的に署名する具体的方法に関し、既存のデジタル署名技術の実施プロセスが参照され得、デジタル署名技術の詳細はここでは省略される。

【００５５】

工程３１０において、端末は、署名情報、ローカルチェック結果および端末ユーザのユーザ情報をサーバへ送信する。

【００５６】

工程３１１において、サーバは、格納された相関を検索することにより、受信されたユーザ情報に対応する公開鍵を取得する。

【００５７】

再び工程３０７を参照すると、更新チェックモードがローカルチェックモードを置換す

るために使用される場合、サーバは、公開鍵とユーザ情報との相関を格納する。この工程において、サーバは、受信されたユーザ情報に対応する公開鍵を取得するために、署名情報、ローカルチェック結果および端末ユーザのユーザ情報を受信した後に上記相関を検索し得る。

【００５８】

工程３１２において、サーバは、取り出された公開鍵により、受信された署名情報を検証し、かつ検証がパスすると、受信されたローカルチェック結果が信頼できると判断する。

【００５９】

工程３０９で端末においてローカルで行われるデジタル署名プロセスに対応して、署名情報の検証は解読プロセスである。署名情報の検証中、サーバは、取り出された公開鍵により署名情報を検証し得、特定の検証プロセスは、既存デジタル署名技術に一致し、デジタル署名技術の詳細はここでは省略される。検証がパスすると、サーバは、受信されたローカルチェック結果が信頼できるチェック結果であると判断し得る。

【００６０】

さらに、サーバは、チェック結果の精度を判断し得る。チェック結果が正確であれば、端末ユーザの現在のオペレーションがリリースされ得、チェック結果が不正確であれば、端末ユーザは、現在のオペレーションを実行することを禁じられる。

【００６１】

上記実施形態から以下のことが分かる。更新チェックモードがオリジナルチェックモードを置換するために使用される場合、端末が更新チェックモード用に生成された秘密鍵を格納し、サーバが更新チェックモード用に生成された公開鍵を格納するため、更新チェックモードがチェックに使用される場合、端末は、秘密鍵によりローカルチェック結果にデジタル的に署名し得、対応するサーバは、端末により送信された署名情報を公開鍵を介して検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断し得る。本開示の実施形態の適用では、悪意のある第三者は秘密鍵と公開鍵とを取得することができず、およびセキュリティチェックは、悪意のある第三者がローカルチェック結果を取得する場合でも完了され得ず、したがって、この実施形態は、セキュリティチェックの信頼性を改善し、かつネットワークアプリケーションのアクセスを安全にし得る。

【００６２】

図４は、本開示の実施形態による別のセキュリティチェック方法のフローチャートである。本方法の実施形態は、端末とサーバとの相互作用の観点からセキュリティチェックのプロセスを詳細に説明すべく、ランダムストリングである代用認証情報を一例として挙げる。本方法は４０１～４１３を含む。

【００６３】

工程４０１において、端末は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合、オリジナルチェックモードの第１のオリジナルチェック認証情報を取得する。

【００６４】

工程４０１の説明は工程３０１と一致しており、詳細はここでは省略される。

【００６５】

工程４０２において、端末は、更新チェックモードのランダムストリングを生成する。

【００６６】

図３における鍵を代用認証情報として生成することと異なり、端末は、本実施形態においてオリジナルチェックモードを置換するために更新チェックモードを使用すると判断された後、代用認証情報として機能する更新チェックモードのランダムストリングを生成し得る。ランダムストリングを生成するための特定のアルゴリズムは、本開示の実施形態により限定されない。

【００６７】

工程４０３において、端末は、端末ユーザに関連付けられた信頼される記憶領域内にラ

ンダムストリングを格納する。
【００６８】
例えば、信頼される記憶領域は、ＴＥＥモジュールまたはＳＥモジュールを含み得、ランダムストリングが生成された後、端末は、信頼される記憶領域内にランダムストリングを格納し得る。
【００６９】
工程４０４において、端末は、第１のオリジナルチェック認証情報、ランダムストリングおよび端末ユーザのユーザ情報をサーバへ送信する。
【００７０】
工程３０４の説明に一致して、例えば、ユーザ情報は、端末ユーザが一意的に識別され得る唯一の情報である。ユーザ情報は、端末ユーザのユーザ名であり得る。
【００７１】
工程４０５において、サーバは、ユーザ情報に対応する第２のオリジナルチェック認証情報を検索する。
【００７２】
工程４０６において、サーバは、第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致するかどうかを判断する。
【００７３】
工程４０５、４０６の説明は工程３０５、３０６と一致しており、詳細はここでは省略される。
【００７４】
工程４０７において、サーバは、第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致すると、ランダムストリングとユーザ情報との相関を格納する。
【００７５】
判断結果に従って第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致すると判断された場合、サーバは、セキュリティチェックモードを現在置換している対象が端末ユーザ自身であると判断し得、このとき、サーバは、受信されたランダムストリングとユーザ情報との相関を格納し得る。
【００７６】
工程４０８において、端末は、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードに従ってローカルチェックを行う。
【００７７】
工程４０８の説明は工程３０８と一致しており、詳細はここでは省略される。
【００７８】
工程４０９において、端末は、第１の暗号化データ結果を取得するために、サーバとの間で予め取り決められるメッセージアブストラクトアルゴリズムにより、信頼される記憶領域内に格納されたランダムストリングおよびローカルチェック結果を暗号化する。
【００７９】
例えば、端末とサーバとは、メッセージアブストラクトアルゴリズムを予め取り決め得る。メッセージアブストラクトアルゴリズムは、例えばハッシュベースメッセージ認証コード（ＨＭＡＣ）であり得る。ＨＭＡＣは、ハッシュアルゴリズムを使用し、入力として鍵とメッセージを用い、出力としてメッセージアブストラクトを生成し得る。
【００８０】
例えば、ローカルチェック結果が取得された後、端末は、第１の暗号化データ結果を生成するために、格納されたランダムストリングを信頼される記憶領域から取得し、ランダムストリングを鍵として、およびローカルチェック結果をメッセージとして用い、ランダムストリングとローカルチェック結果とをＨＭＡＣアルゴリズムにより暗号化し得る。
【００８１】

工程４１０において、端末は、第１の暗号化データ結果、ローカルチェック結果および端末ユーザのユーザ情報をサーバへ送信する。

【００８２】

工程４１１において、サーバは、格納された相関を検索することにより、受信されたユーザ情報に対応するランダムストリングを取得する。

【００８３】

上の工程４０７を参照すると、更新チェックモードがローカルチェックモードを置換するために使用される場合、サーバは、ランダムストリングとユーザ情報との相関を格納する。この工程において、サーバは、第１の暗号化データ結果、ローカルチェック結果および端末ユーザのユーザ情報を受信した後、受信されたユーザ情報に対応するランダムストリングを取得するために相関を検索し得る。

【００８４】

工程４１２において、サーバは、第２の暗号化データ結果を取得するために、発見されたランダムストリングおよびローカルチェック結果を、端末との間で予め取り決められる暗号化アブストラクトアルゴリズムにより暗号化する。

【００８５】

端末における工程４０９のメッセージアブストラクトアルゴリズムによりローカルチェック結果およびランダムストリングをローカルで暗号化するプロセスに対応して、この工程において、サーバは、第２の暗号化データ結果を取得するために、端末との間で予め取り決められるメッセージアブストラクトアルゴリズムを取得し、次に、受信されたローカルチェック結果と、発見されたランダムストリングとをメッセージアブストラクトアルゴリズムにより暗号化し得る。

【００８６】

工程４１３において、サーバは、第２の暗号化データ結果が第１の暗号化データ結果と一致するかどうかを判断し、一致する場合にローカルチェック結果は信頼できると判断され得る。

【００８７】

例えば、第２の暗号化データ結果が第１の暗号化データ結果と一致すると判断されると、サーバは、ローカルチェック結果が信頼できると判断し得る。さらに、サーバは、チェック結果の精度を判断し得、チェック結果が正確であれば、端末ユーザの現在のサービスオペレーションがリリースされ得、チェック結果が不正確であれば、端末ユーザは、現在のサービスオペレーションを実行することを禁じられる。

【００８８】

上記実施形態から以下のことが分かる。更新チェックモードがオリジナルチェックモードを置換するために使用される場合、端末とサーバとが更新チェックモード用に生成されたランダムストリングを格納することから、更新チェックモードがチェックに使用される場合、端末は、ランダムストリングとローカルチェック結果とを予め取り決められるメッセージアブストラクトアルゴリズムにより暗号化し得る。対応するサーバは、ランダムストリングと、端末により送信されたローカルチェック結果とを同じメッセージアブストラクトアルゴリズムにより暗号化し、２つの暗号化データ結果が互いに一致する場合に、ローカルチェック結果が信頼できると判断し得る。本開示の実施形態を適用することにより、悪意のある第三者は、ランダムストリングと、サーバと端末とにより予め取り決められるメッセージアブストラクトアルゴリズムとを取得することができず、およびセキュリティチェックは、悪意のある第三者がローカルチェック結果を取得する場合でも完了され得ない。したがって、本実施形態は、セキュリティチェックの信頼性を改善し、かつネットワークアプリケーションのアクセスを安全にし得る。

【００８９】

本開示のセキュリティチェック方法の実施形態に対応し、本開示は、セキュリティチェックのためのデバイス、端末およびサーバの実施形態をさらに提供する。

【００９０】

本開示のセキュリティチェックのためのデバイスの実施形態は、端末およびサーバへそれぞれ適用され得る。デバイスの実施形態は、ソフトウェア、ハードウェアまたはそれらの組み合せを介して実現され得る。例えば、ソフトウェア実施形態は、論理的意味におけるデバイスとして、本デバイスが配置される装置のプロセッサが不揮発性メモリ内の対応コンピュータプログラム命令を実行用メモリへ読み出すことにより形成される。ハードウェアの観点から、図５は、セキュリティチェックデバイスが本開示の実施形態に従って配置される装置のハードウェア構造図である。図５に示すようなプロセッサ、メモリ、ネットワークインターフェースおよび不揮発性メモリの他に、デバイスが配置される装置は、通常、デバイスの実際の機能に従って他のハードウェアをさらに含み得る。例えば、端末は、カメラ、タッチスクリーン、通信部品などを含み得る。サーバは、パケットを処理する責任を負う送受信器チップを含み得る。

【００９１】

図６は、本開示のいくつかの実施形態によるセキュリティチェックデバイスのブロック図である。セキュリティチェックデバイスは端末へ適用され得る。本デバイスは、チェックユニット６１０、暗号化ユニット６２０および第１の送信ユニット６３０を含み得る。

【００９２】

チェックユニット６１０は、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するためにローカルチェックを更新チェックモードにより行うために使用される。

【００９３】

暗号化ユニット６２０は、暗号化チェック結果を取得するために、格納された代用認証情報に従ってローカルチェック結果を暗号化するために使用される。代用認証情報は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合に生成される情報である。

【００９４】

第１の送信ユニット６３０は、暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報をサーバへ送信することのために使用され、それにより、サーバは、ユーザ情報に対応する代用認証情報に従った暗号化チェック結果の検証がパスすると、ローカルチェック結果が信頼できると判断する。

【００９５】

図７は、本開示のいくつかの実施形態によるセキュリティチェックデバイスのブロック図である。セキュリティチェックデバイスは端末へ適用され得る。本デバイスは、取得ユニット７１０、生成ユニット７２０、第２の送信ユニット７３０、格納ユニット７４０、チェックユニット７５０、暗号化ユニット７６０および第１の送信ユニット７７０を含む。

【００９６】

取得ユニット７１０は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合に、オリジナルチェックモードの第１のオリジナルチェック認証情報を取得するために使用される。

【００９７】

生成ユニット７２０は、更新チェックモードのための代用認証情報を生成するために使用される。

【００９８】

第２の送信ユニット７３０は、第１のオリジナルチェック認証情報、代用認証情報およびユーザ情報をサーバへ送信することのために使用され、それにより、サーバは、ユーザ情報に対応する第２のオリジナルチェック認証情報を取り出し、第２のオリジナルチェック認証情報が第１のオリジナルチェック認証情報と一致すると、代用認証情報とユーザ情報との相関を格納する。

【００９９】

格納ユニット７４０は、端末ユーザに関連付けられた信頼される記憶領域内に代用認証

情報を格納するために使用され、信頼される記憶領域は、ＴＥＥモジュールまたはＳＥモジュールを含む。

【０１００】

チェックユニット７５０は、端末ユーザがセキュリティチェックを行う場合に、ローカルチェック結果を取得するために更新チェックモードを介してローカルチェックを行うために使用される。

【０１０１】

暗号化ユニット７６０は、暗号化チェック結果を取得するために、格納された代用認証情報に従ってローカルチェック結果を暗号化するために使用される。代用認証情報は、更新チェックモードがオリジナルチェックモードを置換するために使用される場合に生成される情報である。

【０１０２】

第１の送信ユニット７７０は、暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報をサーバへ送信することのために使用され、それにより、サーバは、ユーザ情報に対応する代用認証情報に従った暗号化チェック結果の検証がパスすると、ローカルチェック結果が信頼できると判断する。

【０１０３】

別の実施形態では、代用認証情報は、公開鍵と秘密鍵とを含み得、第２の送信ユニット７３０は、特に、公開鍵をサーバへ送信するために使用され得、暗号化ユニット７６０は、特に、署名情報を取得するために、格納された秘密鍵に従ってローカルチェック結果にデジタル的に署名するために使用され得、第１の送信ユニット７７０は、特に、署名情報をサーバへ送信することのために使用され得、それにより、サーバは、ユーザ情報に対応する公開鍵に従った署名情報の検証がパスすると、ローカルチェック結果が信頼できると判断する。

【０１０４】

別の代替案実施形態では、代用認証情報は、ランダムストリングを含み得、第２の送信ユニット７３０は、特に、ランダムストリングをサーバへ送信するために使用され得、暗号化ユニット７６０は、特に、第１の暗号化データ結果を取得するために、サーバとの間で予め取り決められるメッセージアブストラクトアルゴリズムによりランダムストリングとローカルチェック結果とを暗号化するために使用され得、第１の送信ユニット７７０は、特に、第１の暗号化データ結果をサーバへ送信するために使用され得、サーバは、第２の暗号化データ結果を取得するために、ユーザ情報に対応するランダムストリングを取得して、ユーザ情報に対応するランダムストリングと、ローカルチェック結果とをメッセージアブストラクトアルゴリズムにより暗号化し、かつ第２の暗号化データ結果が第１の暗号化データ結果と一致すると、ローカルチェック結果が信頼できると判断する。

【０１０５】

図８は、本開示の実施形態によるセキュリティチェックデバイスの別の実施形態のブロック図である。セキュリティチェックデバイスはサーバへ適用され得、本デバイスは、第１の受信ユニット８１０、取得ユニット８２０およびチェックユニット８３０を含み得る。

【０１０６】

第１の受信ユニット８１０は、端末により送信される暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信するために使用され、暗号化チェック結果は、格納された代用認証情報に従って端末がローカルチェック結果を暗号化する場合に生成される暗号化チェック結果であり、代用認証情報は、端末がオリジナルチェックモードを置換するために更新チェックモードを使用する場合に生成される情報であり、およびローカルチェック結果は、端末ユーザがセキュリティチェックを行う場合に、更新チェックモードを介してローカルチェックを行う端末により取得されるチェック結果である。

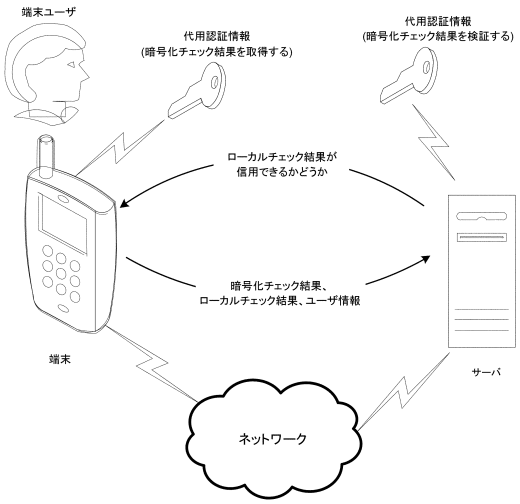
【０１０７】

取得ユニット８２０は、ユーザ情報に対応する代用認証情報を取得するために使用され

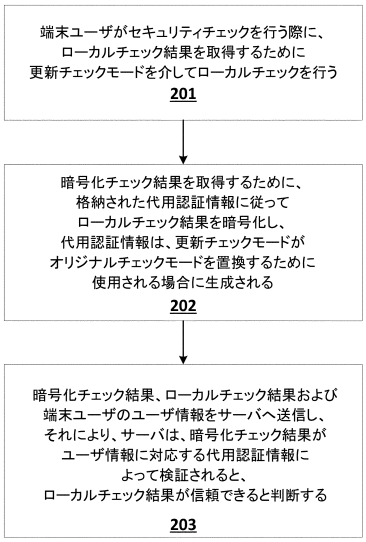
る。
【０１０８】
チェックユニット８３０は、ユーザ情報に対応する代用認証情報に従って暗号化チェック結果を検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断するために使用される。
【０１０９】
図９は、本開示の実施形態による別のセキュリティチェックデバイスのブロック図である。セキュリティチェックデバイスはサーバへ適用され得、本デバイスは、第２の受信ユニット９１０、検索ユニット９２０、比較ユニット９３０、格納ユニット９４０、第１の受信ユニット９５０、取得ユニット９６０およびチェックユニット９７０を含む。
【０１１０】
第２の受信ユニット９１０は、端末がオリジナルチェックモードを置換するために更新チェックモードを使用する場合に、端末により送信された第１のオリジナルチェック認証情報、代用認証情報、およびユーザ情報を受信するために使用される。第１のオリジナルチェック認証情報は、オリジナルチェックモードのチェック認証情報である。代用認証情報は、更新チェックモードの端末により生成される代用認証情報である。
【０１１１】
検索ユニット９２０は、ユーザ情報に対応する第２のオリジナルチェック認証情報を検索するために使用される。
【０１１２】
比較ユニット９３０は、第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致するかどうかを判断するために使用される。
【０１１３】
格納ユニット９４０は、第１のオリジナルチェック認証情報が第２のオリジナルチェック認証情報と一致すると、代用認証情報とユーザ情報との相関を格納するために使用される。
【０１１４】
第１の受信ユニット９５０は、端末により送信された暗号化チェック結果、ローカルチェック結果および端末ユーザのユーザ情報を受信するために使用され、暗号化チェック結果は、格納された代用認証情報に従って端末がローカルチェック結果を暗号化する場合に生成される暗号化チェック結果であり、代用認証情報は、端末がオリジナルチェックモードを置換するために更新チェックモードを使用する場合に生成される情報であり、およびローカルチェック結果は、端末ユーザがセキュリティチェックを行う場合に、更新チェックモードを介してローカルチェックを行う端末により取得されるチェック結果である。
【０１１５】
取得ユニット９６０は、ユーザ情報に対応する代用認証情報を取得するために使用される。
【０１１６】
チェックユニット９７０は、ユーザ情報に対応する代用認証情報に従って暗号化チェック結果を検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断するために使用される。
【０１１７】
別の実施形態では、代用認証情報は、公開鍵と秘密鍵とを含み得る。第２の受信ユニット９１０は、特に、端末により送信された公開鍵を受信するために使用され得る。第１の受信ユニット９５０は、特に、端末により送信された署名情報を受信するために使用され得、署名情報は、格納された秘密鍵に従ってローカルチェック結果にデジタル的に署名する端末により取得される署名情報である。取得ユニット９６０は、特に、相関を検索することにより、ユーザ情報に対応する公開鍵を取得するために使用され得る。チェックユニット９７０は、特に、ユーザ情報に対応する公開鍵を介して署名情報を検証するために使用され得る。

【０１１８】
別の代替案実施形態では、代用認証情報は、ランダムストリングを含み、第２の受信ユニット９１０は、特に、端末により送信されたランダムストリングを受信するために使用され得、第１の受信ユニット９５０は、特に、端末により送信された第１の暗号化データ結果を受信するために使用され得、第１の暗号化データ結果は、サーバとの間で予め取り決められるメッセージアブストラクトアルゴリズムによりランダムストリングとローカルチェック結果とを暗号化する端末により取得される暗号化データ結果であり、取得ユニット９６０は、特に、相関を検索することにより、ユーザ情報に対応するランダムストリングを取得するために使用され得る。
【０１１９】
チェックユニット９７０は、第２の暗号化データ結果を取得するために、ユーザ情報に対応するランダムストリングとローカルチェック結果とを暗号化アブストラクトアルゴリズムにより暗号化するために使用される結果暗号化副ユニットと、第２の暗号化データ結果が第１の暗号化データ結果と一致するかどうかを判断するために使用され、一致する場合に検証がパスする、結果判断副ユニットとを含み得る（図９に図示せず）。
【０１２０】
上記デバイスのユニットの機能の実施プロセスおよび効果に関して、これまで述べた方法における対応する工程実施プロセスを参照されたい。その詳細はここでは省略される。
【０１２１】
デバイス実施形態に関し、これらは方法実施形態にほぼ対応するため、方法実施形態の関連部分を参照されたい。上に説明したデバイス実施形態は単に例示的であり、別個部分として説明したユニットは互いに物理的に分離されてもされなくてもよく、ユニットとして示された部分は、１つの位置に配置されてもよく、または複数のネットワークユニット全体にわたって分散されてもよい物理的ユニットであってもなくてもよい。モジュールの一部またはすべては、本開示の解決策の目的を達成するために実際的な要件に従って選択され得る。当業者は、独創的努力なしに本解決策を理解および実施し得る。
【０１２２】
上記実施形態から以下のことが分かる。更新チェックモードがオリジナルチェックモードを置換するために使用される場合、端末とサーバとの両方が更新チェックモード用に生成された代用認証情報を格納するため、更新チェックモードがチェックに使用される場合、ローカルチェック結果は、代用認証情報を介して暗号化され得、対応するサーバは、端末により暗号化および送信された暗号化チェック結果を代用認証情報を介して検証し、かつ検証がパスすると、ローカルチェック結果が信頼できると判断し得る。本開示の実施形態の適用では、悪意のある第三者は代用認証情報を取得することができず、およびセキュリティチェックは、悪意のある第三者がローカルチェック結果を取得したとしても完了され得ず、したがって、本開示の実施形態は、セキュリティチェックの信頼性を改善し、かつネットワークアプリケーションのアクセスセキュリティを確実にし得る。
【０１２３】
当業者は、本明細書を考察し、および本発明を実施した後、本発明の他の実施形態を容易に想到するであろう。本開示は、本発明のいかなる変形形態、使用または適応形態も包含するように意図されており、これらの変形形態、使用または適応形態は、本発明の一般的原理に従い、本開示において開示されない当該技術分野における常識または慣習的な技術的手段を含む。本明細書と実施形態とは単に例示的であると見なされ、本開示の真の範囲および趣旨は以下の特許請求の範囲により示される。
【０１２４】
本開示は、上に説明され添付図面に示される正確な構造に限定されず、様々な修正形態および変更形態が本発明の範囲から逸脱することなくなされ得ることを理解すべきである。本開示の範囲は、添付特許請求範囲のみにより限定される。

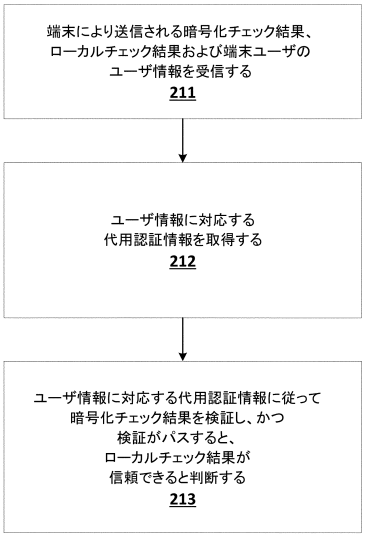
【図１】


端末ユーザ
代用認証情報
(暗号化チェック結果を取得する)
代用認証情報
(暗号化チェック結果を検証する)
ローカルチェック結果が
信用できるかどうか
暗号化チェック結果、
ローカルチェック結果、ユーザ情報
端末
サーバ
ネットワーク

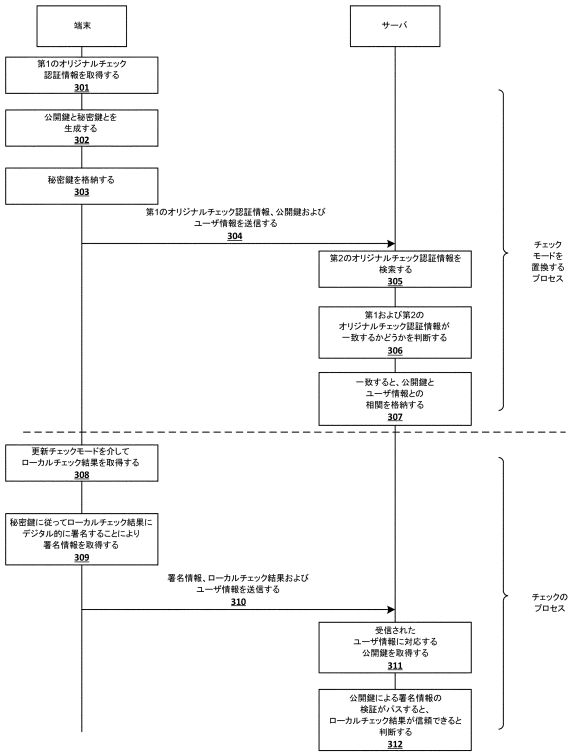
【図２Ａ】


端末ユーザがセキュリティチェックを行う際に、
ローカルチェック結果を取得するために
更新チェックモードを介してローカルチェックを行う
201
暗号化チェック結果を取得するために、
格納された代用認証情報に従って
ローカルチェック結果を暗号化し、
代用認証情報は、更新チェックモードが
オリジナルチェックモードを置換するために
使用される場合に生成される
202
暗号化チェック結果、ローカルチェック結果および
端末ユーザのユーザ情報をサーバへ送信し、
それにより、サーバは、暗号化チェック結果が
ユーザ情報に対応する代用認証情報に
よって検証されると、
ローカルチェック結果が信頼できると判断する
203

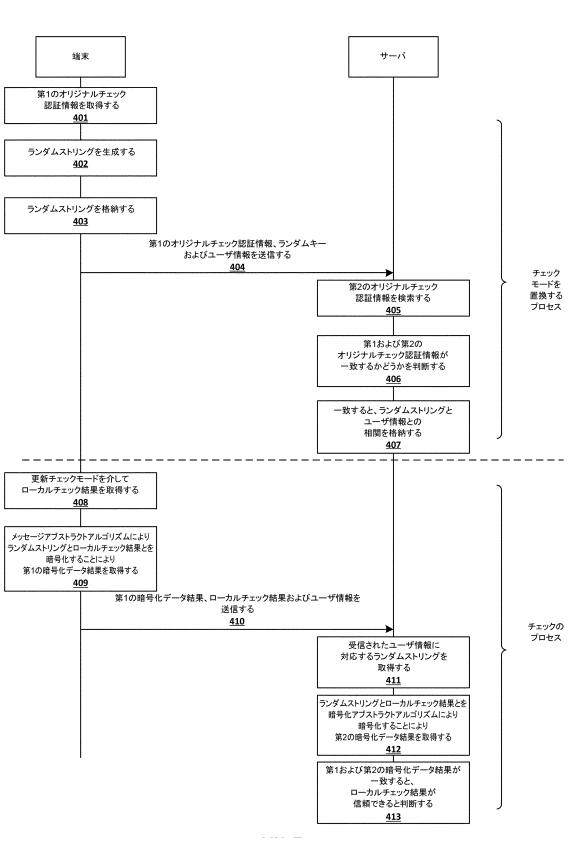
【図２Ｂ】


端末により送信される暗号化チェック結果、
ローカルチェック結果および端末ユーザの
ユーザ情報を受信する
211
ユーザ情報に対応する
代用認証情報を取得する
212
ユーザ情報に対応する代用認証情報に従って
暗号化チェック結果を検証し、かつ
検証がパスすると、
ローカルチェック結果が
信頼できると判断する
213

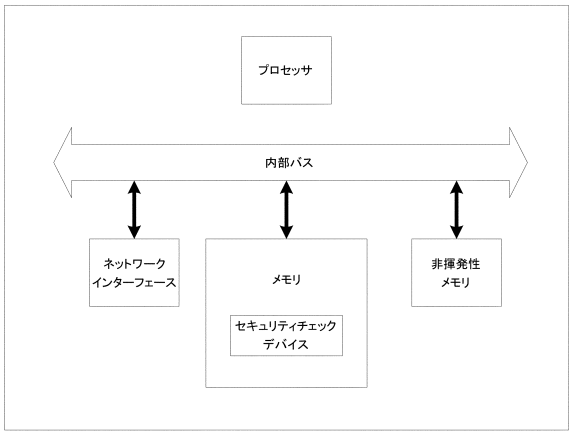
【図３】


端末
サーバ
第1のオリジナルチェック
認証情報を取得する
301
公開鍵と秘密鍵とを
生成する
302
秘密鍵を格納する
303
第1のオリジナルチェック認証情報、公開鍵および
ユーザ情報を送信する
304
第2のオリジナルチェック認証情報を
検索する
305
第1および第2の
オリジナルチェック認証情報が
一致するかどうかを判断する
306
一致すると、公開鍵と
ユーザ情報との
相関を格納する
307
チェック
モードを
置換する
プロセス
更新チェックモードを介して
ローカルチェック結果を取得する
308
秘密鍵に従ってローカルチェック結果に
デジタル的に署名することにより
署名情報を取得する
309
署名情報、ローカルチェック結果および
ユーザ情報を送信する
310
受信された
ユーザ情報に対応する
公開鍵を取得する
311
公開鍵による署名情報の
検証がパスすると、
ローカルチェック結果が信頼できると
判断する
312
チェックの
プロセス

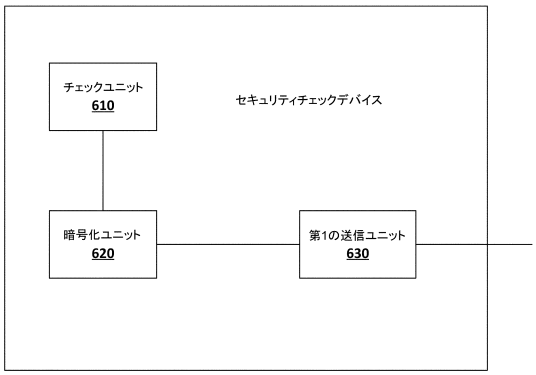
【図４】


端末
サーバ
第1のオリジナルチェック
認証情報を取得する
401
ランダムストリングを生成する
402
ランダムストリングを格納する
403
第1のオリジナルチェック認証情報、ランダムキー
およびユーザ情報を送信する
404
第2のオリジナルチェック
認証情報を検索する
405
第1および第2の
オリジナルチェック認証情報が
一致するかどうかを判断する
406
一致すると、ランダムストリングと
ユーザ情報との
相関を格納する
407
チェック
モードを
置換する
プロセス
更新チェックモードを介して
ローカルチェック結果を取得する
408
メッセージアブストラクトアルゴリズムにより
ランダムストリングとローカルチェック結果とを
暗号化することにより
第1の暗号化データ結果を取得する
409
第1の暗号化データ結果、ローカルチェック結果およびユーザ情報を
送信する
410
受信されたユーザ情報に
対応するランダムストリングを
取得する
411
ランダムストリングとローカルチェック結果とを
暗号化アブストラクトアルゴリズムにより
暗号化することにより
第2の暗号化データ結果を取得する
412
第1および第2の暗号化データ結果が
一致すると、
ローカルチェック結果が
信頼できると判断する
413
チェック
のプロセス

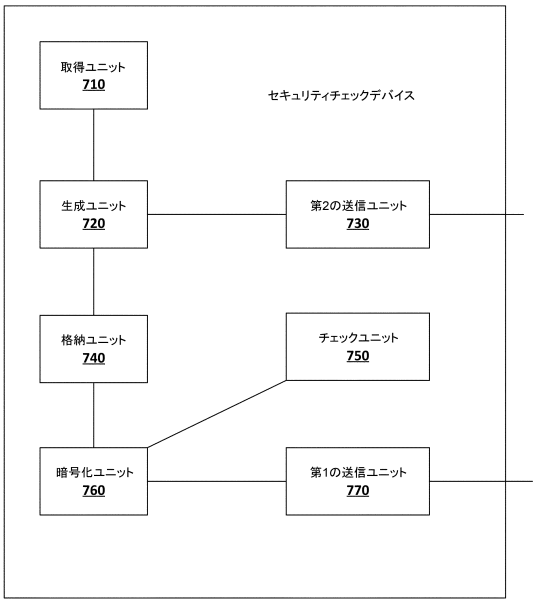
【図５】


プロセッサ
内部バス
ネットワーク
インターフェース
メモリ
セキュリティチェック
デバイス
非揮発性
メモリ

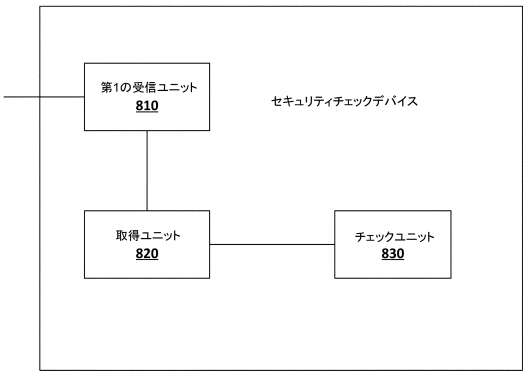
【図６】


チェックユニット
610
セキュリティチェックデバイス
暗号化ユニット
620
第1の送信ユニット
630

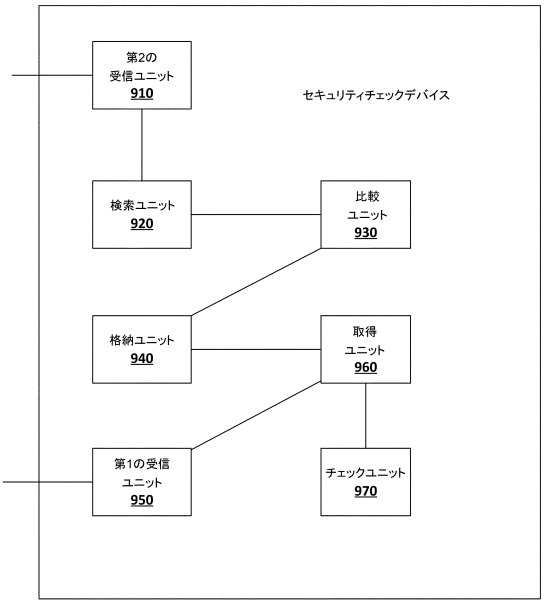
【図７】


取得ユニット
710
セキュリティチェックデバイス
生成ユニット
720
第2の送信ユニット
730
格納ユニット
740
チェックユニット
750
暗号化ユニット
760
第1の送信ユニット
770

【図８】


第1の受信ユニット
810
セキュリティチェックデバイス
取得ユニット
820
チェックユニット
830

【図９】


第2の
受信ユニット
910
セキュリティチェックデバイス
検索ユニット
920
比較
ユニット
930
格納ユニット
940
取得
ユニット
960
第1の受信
ユニット
950
チェックユニット
970

フロントページの続き

(72)発明者　リン，ジュンスイ
中華人民共和国，浙江省　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

合議体
審判長　石井　茂和
審判官　山崎　慎一
審判官　塚田　肇

(56)参考文献　特開２０１１－０５９７４９（ＪＰ，Ａ）
特開２０１１－１７６４３５（ＪＰ，Ａ）
国際公開第２００８／０９９７５６（WO，Ａ１）
特開２００７－２２００７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L9/32
G06F21/31
G09C1/00