(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6548667号
(P6548667)
(45)発行日　令和1年7月24日(2019.7.24)　(24)登録日　令和1年7月5日(2019.7.5)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/31
G06F 21/44 (2013.01)　　G06F 21/44

請求項の数 25　(全 40 頁)

(21)出願番号　特願2016-563918(P2016-563918)
(86)(22)出願日　平成27年5月21日(2015.5.21)
(65)公表番号　特表2017-521744(P2017-521744A)
(43)公表日　平成29年8月3日(2017.8.3)
(86)国際出願番号　PCT/US2015/031976
(87)国際公開番号　WO2015/179640
(87)国際公開日　平成27年11月26日(2015.11.26)
審査請求日　平成28年12月13日(2016.12.13)
(31)優先権主張番号　201410219868.0
(32)優先日　平成26年5月22日(2014.5.22)
(33)優先権主張国　中国(CN)
(31)優先権主張番号　14/717,545
(32)優先日　平成27年5月20日(2015.5.20)
(33)優先権主張国　米国(US)

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110000028
特許業務法人明成国際特許事務所

最終頁に続く

(54)【発明の名称】セキュリティチェックを提供するための方法、装置、および、システム

(57)【特許請求の範囲】
【請求項１】
コンピュータによって実行される方法であって、
端末から送信されたセキュリティ検証要求を受信し、
前記セキュリティ検証要求に少なくとも部分的に基づいて、第１検証要素情報を取得し、前記第１検証要素情報を取得することは、前記セキュリティ検証要求に関連する第１セキュリティ検証コードと、前記セキュリティ検証要求に関連する第１タイムスタンプとを生成することを含み、前記第１タイムスタンプは、現在のセキュリティチェックの期限を示し、前記第１検証要素情報は、前記端末に対応する第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含み、
前記第１検証要素情報に少なくとも部分的に基づいて、デジタルオブジェクト固有識別子を生成し、
前記デジタルオブジェクト固有識別子を前記端末に送信し、
第２検証要素情報を前記端末から受信し、
前記第１検証要素情報および前記第２検証要素情報が一致するとの決定に応答して、セキュリティチェック合格情報を前記端末に送信すること、
を備える、方法。
【請求項２】
請求項１に記載の方法であって、前記第２検証要素情報は、前記端末によって前記デジタルオブジェクト固有識別子から取得された前記第１検証要素情報に対応する、方法。

【請求項３】
請求項１に記載の方法であって、前記端末は、前記デジタルオブジェクト固有識別子を処理することによって、前記第２検証要素情報を取得する、方法。
【請求項４】
請求項１に記載の方法であって、さらに、
前記第１検証要素情報および前記第２検証要素情報が一致するか否かを判定する工程を備える、方法。
【請求項５】
請求項１に記載の方法であって、さらに、
ユーザ名と端末識別子との間の対応関係を格納することを備え、
前記セキュリティ検証要求に少なくとも部分的に基づいて、前記第１検証要素情報を取得することは、
前記セキュリティ検証要求に含まれる前記端末のユーザ名を用いて、ユーザ名と端末識別子との間の前記対応関係を検索して、前記端末に関連づけられている前記第１端末識別子を取得することを備える、方法。
【請求項６】
請求項５に記載の方法であって、前記第１検証要素情報に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成することは、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを組み合わせることによって、第１組み合わせ文字列を生成し、
前記第１組み合わせ文字列に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成すること、
を備える、方法。
【請求項７】
請求項６に記載の方法であって、前記第１組み合わせ文字列に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成することは、
前記第１組み合わせ文字列を暗号化することに少なくとも部分的に基づいて、暗号化文字列を生成し、
前記暗号化文字列をｂａｓｅ６４文字列に変換し、
クイックレスポンス（ＱＲ）符号化ルールに従って、前記ｂａｓｅ６４文字列を符号化し、
前記デジタルオブジェクト固有識別子に対応する二次元検証コードを生成すること、
を備える、方法。
【請求項８】
請求項５に記載の方法であって、さらに、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプの間の関係性を保存することを備え、
前記第２検証要素情報は、第２組み合わせ文字列を分解することによって取得された第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含み、前記第２組み合わせ文字列は、前記端末が前記デジタルオブジェクト固有識別子をスキャンすることによって取得され、前記第２検証要素情報は、前記端末が前記第２端末識別子を前記端末の前記第１端末識別子と比較して、前記第２端末識別子および前記端末の前記第１端末識別子が同じであると判定した場合に、前記端末から送信された情報に対応し、
前記セキュリティチェック合格情報を前記端末に送信することは、
前記第２端末識別子に少なくとも部分的に基づいて、複数の第１端末識別子、複数の第１セキュリティ検証コード、および、複数の第１タイムスタンプの間の複数の関係性を検索して、前記第２端末識別子にそれぞれ対応する前記第１セキュリティ検証コードおよび前記第１タイムスタンプを取得し、
前記第２セキュリティ検証コードおよび前記取得された第１セキュリティ検証コードが一致し、前記第２タイムスタンプおよび前記取得された第１タイムスタンプが一致し、

前記第２タイムスタンプが前記セキュリティ検証要求に関連する現在のセキュリティチェックの期限内にあるとの決定に応答して、セキュリティチェック合格情報を前記端末に送信すること、
を備える、方法。
【請求項９】
方法であって、
端末によってセキュリティ検証要求をサーバに送信し、
前記端末によってデジタルオブジェクト固有識別子を前記サーバから受信し、前記デジタルオブジェクト固有識別子は、前記サーバが前記セキュリティ検証要求に少なくとも部分的に基づいて取得した第１検証要素情報に少なくとも部分的に基づいて生成された固有識別子に対応し、前記第１検証要素情報は、前記セキュリティ検証要求に関連づけられている第１セキュリティ検証コード、前記端末に対応する第１端末識別子、および前記セキュリティ検証要求に関連付けられると共に、現在のセキュリティチェックの期限を示す第１タイムスタンプを含み、
前記端末によって前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて第２検証要素情報を取得し、
前記端末によって前記第２検証要素情報を前記サーバに送信し、
前記第１検証要素情報および前記第２検証要素情報が一致するとの決定に応答して、セキュリティチェック合格情報を前記サーバから受信すること、
を備える、方法。
【請求項１０】
請求項９に記載の方法であって、前記第２検証要素情報を取得することは、前記デジタルオブジェクト固有識別子を処理しと、前記デジタルオブジェクト固有識別子の前記処理に少なくとも部分的に基づいて前記第２検証要素情報を取得すること、を備える、方法。
【請求項１１】
請求項９に記載の方法であって、さらに、
前記第１検証要素情報の少なくとも一部および前記第２検証要素情報の少なくとも一部が一致するか否かを判定することを備える、方法。
【請求項１２】
請求項９に記載の方法であって、前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて前記第２検証要素情報を取得することは、
前記デジタルオブジェクト固有識別子をスキャンし、
前記デジタルオブジェクト固有識別子の前記スキャンに少なくとも部分的に基づいて第２組み合わせ文字列を取得し、前記デジタルオブジェクト固有識別子は、第１組み合わせ文字列に少なくとも部分的に基づいて生成され、前記第１組み合わせ文字列は、前記サーバが、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることによって生成され、前記第１検証要素情報は、前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含み、前記第１端末識別子は、前記端末のユーザ名に少なくとも部分的に基づいて取得された前記端末の端末識別子に対応し、前記端末の前記ユーザ名は、前記セキュリティ検証要求に含まれ、前記第１セキュリティ検証コードおよび前記第１タイムスタンプは、前記セキュリティ検証要求に関連して前記サーバによって生成された前記第１セキュリティ検証コードおよび前記第１タイムスタンプに対応し、
前記第２組み合わせ文字列を分解し、
前記第２組み合わせ文字列の前記分解に少なくとも部分的に基づいて、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含む前記第２検証要素情報を取得すること、
を備える、方法。
【請求項１３】
請求項１２に記載の方法であって、前記デジタルオブジェクト固有識別子の前記スキャ

ンに少なくとも部分的に基づいて前記第２組み合わせ文字列を取得することは、
クイックレスポンス（ＱＲ）復号ルールを用いて、前記デジタルオブジェクト固有識別子に対応する二次元検証コードを復号し、
前記二次元検証コードの前記復号に少なくとも部分的に基づいてｂａｓｅ６４文字列を生成し、
前記ｂａｓｅ６４文字列を暗号化文字列に変換し、
前記暗号化文字列を復号することに少なくとも部分的に基づいて前記第２組み合わせ文字列を取得すること、
を備える、方法。
【請求項１４】
請求項１２に記載の方法であって、さらに、
前記第２検証要素情報が前記サーバに送信される前に、前記第２端末識別子および前記端末の端末識別子を比較し、
前記第２端末識別子および前記端末の前記端末識別子がマッチするとの決定に応答して、前記第２検証要素情報を前記サーバに送信する工程を実行すること、
を備える、方法。
【請求項１５】
セキュリティチェックデバイスであって、
少なくとも１つのプロセッサであって、
端末から送信されたセキュリティ検証要求を受信し、
前記セキュリティ検証要求に少なくとも部分的に基づいて、第１検証要素情報を取得し、前記第１検証要素情報を取得することは、前記セキュリティ検証要求に関連する第１セキュリティ検証コードと、前記セキュリティ検証要求に関連する第１タイムスタンプとを生成することを含み、前記第１タイムスタンプは、現在のセキュリティチェックの期限を示し、前記第１検証要素情報は、前記端末に対応する第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含み、
前記第１検証要素情報に少なくとも部分的に基づいて、デジタルオブジェクト固有識別子を生成し、
前記デジタルオブジェクト固有識別子を前記端末に送信し、
第２検証要素情報を前記端末から受信し、
前記第１検証要素情報および前記第２検証要素情報が一致するとの決定に応答して、セキュリティチェック合格情報を前記端末に送信するよう構成されている、少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサに接続され、前記少なくとも１つのプロセッサに命令を提供するよう構成されているメモリと、
を備える、デバイス。
【請求項１６】
請求項１５に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
ユーザ名と端末識別子との間の対応関係を格納するよう構成されており、
前記少なくとも１つのプロセッサによって、前記セキュリティ検証要求に少なくとも部分的に基づいて、前記第１検証要素情報を取得することは、
前記セキュリティ検証要求に含まれる前記端末のユーザ名を用いて、ユーザ名と端末識別子との間の前記対応関係を検索して、前記端末に対応する前記第１端末識別子を取得し、
前記セキュリティ検証要求に関連する第１セキュリティ検証コードと、前記セキュリティ検証要求に関連する第１タイムスタンプとを生成すること、
を備え、
前記第１タイムスタンプは、現在のセキュリティチェックの期限を示し、前記第１検証要素情報は、前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含む、デバイス。

【請求項１７】
請求項１６に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを組み合わせることによって、第１組み合わせ文字列を生成し、
前記第１組み合わせ文字列に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成するよう構成されている、デバイス。
【請求項１８】
請求項１７に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記第１組み合わせ文字列を暗号化することに少なくとも部分的に基づいて、暗号化文字列を生成し、
前記暗号化文字列をｂａｓｅ６４文字列に変換し、
クイックレスポンス（ＱＲ）符号化ルールに従って、前記ｂａｓｅ６４文字列を符号化し、
前記デジタルオブジェクト固有識別子に対応する二次元検証コードを生成するよう構成されている、デバイス。
【請求項１９】
請求項１６に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプの間の関係性を保存するよう構成されており、
前記第２検証要素情報は、第２組み合わせ文字列を分解することによって取得された第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含み、前記第２組み合わせ文字列は、前記端末が前記デジタルオブジェクト固有識別子をスキャンすることによって取得され、前記第２検証要素情報は、前記端末が前記第２端末識別子を前記端末の前記第１端末識別子と比較して、前記第２端末識別子および前記端末の前記第１端末識別子が同じであると判定した場合に、前記端末から送信された情報に対応し、
前記少なくとも１つのプロセッサは、
前記第２端末識別子に少なくとも部分的に基づいて、複数の第１端末識別子、複数の第１セキュリティ検証コード、および、複数の第１タイムスタンプの間の前記関係性を検索して、前記第２端末識別子にそれぞれ対応する前記第１セキュリティ検証コードおよび前記第１タイムスタンプを取得し、
前記第２セキュリティ検証コードおよび前記取得されたセキュリティ検証コードが一致し、前記第２タイムスタンプおよび前記取得されたタイムスタンプが一致し、前記第２タイムスタンプが前記セキュリティ検証要求に関連する現在のセキュリティチェックの期限内にあるとの決定に応答して、セキュリティチェック合格情報を前記端末に送信することにより、
前記セキュリティチェック合格情報を前記端末に送信する、デバイス。
【請求項２０】
端末であって、
少なくとも１つのプロセッサであって、
セキュリティ検証要求をサーバに送信し、
デジタルオブジェクト固有識別子を前記サーバから受信し、
前記デジタルオブジェクト固有識別子は、前記サーバが前記セキュリティ検証要求に少なくとも部分的に基づいて取得した第１検証要素情報に少なくとも部分的に基づいて生成された固有識別子に対応し、前記第１検証要素情報は、前記セキュリティ検証要求に関連づけられている第１セキュリティ検証コード、前記端末に対応する第１端末識別子、および前記セキュリティ検証要求に関連付けられると共に、現在のセキュリティチェックの期限を示す第１タイムスタンプを含み、
前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて第２検証要素情報を取得し、
前記第２検証要素情報を前記サーバに送信し、

前記第１検証要素情報および前記第２検証要素情報が一致するとの決定に応答して、セキュリティチェック合格情報を前記サーバから受信するよう構成されている、少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサに接続され、前記少なくとも１つのプロセッサに命令を提供するよう構成されているメモリと、
を備える、端末。
【請求項２１】
請求項２０に記載の端末であって、前記少なくとも１つのプロセッサは、さらに、
前記デジタルオブジェクト固有識別子をスキャンし、
前記デジタルオブジェクト固有識別子の前記スキャンに少なくとも部分的に基づいて第２組み合わせ文字列を取得し、
前記デジタルオブジェクト固有識別子は、第１組み合わせ文字列に少なくとも部分的に基づいて生成され、前記第１組み合わせ文字列は、前記サーバが、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることによって生成され、前記第１検証要素情報は、前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含み、前記第１端末識別子は、端末のユーザ名に少なくとも部分的に基づいて取得された前記端末の端末識別子に対応し、前記端末の前記ユーザ名は、前記セキュリティ検証要求に含まれ、前記第１セキュリティ検証コードおよび前記第１タイムスタンプは、前記セキュリティ検証要求に関連して前記サーバによって生成された前記第１セキュリティ検証コードおよび前記第１タイムスタンプに対応し、
前記第２組み合わせ文字列を分解し、
前記第２組み合わせ文字列の前記分解に少なくとも部分的に基づいて、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含む前記第２検証要素情報を取得するよう構成されている、端末。
【請求項２２】
請求項２１に記載の端末であって、前記少なくとも１つのプロセッサは、さらに、
クイックレスポンス（ＱＲ）復号ルールを用いて、前記デジタルオブジェクト固有識別子に対応する二次元検証コードを復号し、
前記二次元検証コードの前記復号に少なくとも部分的に基づいてｂａｓｅ６４文字列を生成し、
前記ｂａｓｅ６４文字列を暗号化文字列に変換し、
前記暗号化文字列を復号することに少なくとも部分的に基づいて前記第２組み合わせ文字列を取得するよう構成されている、端末。
【請求項２３】
請求項２１に記載の端末であって、前記少なくとも１つのプロセッサは、さらに、
前記第２検証要素情報が前記サーバに送信される前に、前記第２端末識別子および前記端末の端末識別子を比較し、
前記第２端末識別子および前記端末の前記端末識別子がマッチするとの決定に応答して、前記第２検証要素情報を前記サーバに送信する工程を実行するよう構成されている、端末。
【請求項２４】
コンピュータプログラムであって、
端末から送信されたセキュリティ検証要求を受信するための機能と、
前記セキュリティ検証要求に少なくとも部分的に基づいて、第１検証要素情報を取得するための機能と、前記第１検証要素情報を取得する機能は、前記セキュリティ検証要求に関連する第１セキュリティ検証コードと、前記セキュリティ検証要求に関連する第１タイムスタンプとを生成する機能を含み、前記第１タイムスタンプは、現在のセキュリティチェックの期限を示し、前記第１検証要素情報は、前記端末に対応する第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含み、
前記第１検証要素情報に少なくとも部分的に基づいて、デジタルオブジェクト固有識別

子を生成するための機能と、
前記デジタルオブジェクト固有識別子を前記端末に送信するための機能と、
第２検証要素情報を前記端末から受信するための機能と、
前記第１検証要素情報および前記第２検証要素情報が一致するとの決定に応答して、セキュリティチェック合格情報を前記端末に送信するための機能と、
をコンピュータによって実現させる、コンピュータプログラム。
【請求項２５】
コンピュータプログラムであって、
セキュリティ検証要求をサーバに送信するための機能と、
デジタルオブジェクト固有識別子を前記サーバから受信するための機能と、前記デジタルオブジェクト固有識別子は、前記サーバが前記セキュリティ検証要求に少なくとも部分的に基づいて取得した第１検証要素情報に少なくとも部分的に基づいて生成された固有識別子に対応し、前記第１検証要素情報は、前記セキュリティ検証要求に関連づけられている第１セキュリティ検証コード、端末に対応する第１端末識別子、および前記セキュリティ検証要求に関連付けられると共に、現在のセキュリティチェックの期限を示す第１タイムスタンプを含み、
前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて第２検証要素情報を取得するための機能と、
前記第２検証要素情報を前記サーバに送信するための機能と、
前記第１検証要素情報および前記第２検証要素情報が一致するとの決定に応答して、セキュリティチェック合格情報を前記サーバから受信するための機能と、を端末によって実現させる、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
他の出願の相互参照
本願は、発明の名称を「Ａ ＭＥＴＨＯＤ， Ａ ＤＥＶＩＣＥ， Ａ ＳＥＲＶＥＲ ＡＮＤ Ａ ＴＥＲＭＩＮＡＬ ＦＯＲ ＳＥＣＵＲＩＴＹ ＣＨＥＣＫＳ」とする、２０１４年５月２２日出願の中国特許出願第２０１４１０２１９８６８．０号に基づく優先権を主張しており、当該出願は、すべての目的のために参照により本明細書に組み込まれる。
【０００２】
本願は、ネットワーク通信セキュリティ技術の分野に関し、特に、セキュリティを検証するための方法、デバイス、サーバ、システム、および、端末に関する。
【背景技術】
【０００３】
スマート端末およびインターネットアプリケーションの発展の結果として、ユーザは、端末にインストールされた様々なアプリケーションクライアントを用いて様々なインターネットアプリケーションにアクセスできるようになっている。ユーザが様々なインターネットアプリケーションにアクセスするための処理に関連して、ユーザは、一般に、ＩＤを認証する、メンバーとして登録する、ネットワーク取引に参加することなどを求められる。或る関連技術によると、アプリケーションサーバが、動的検証コードを含む検証テキストメッセージをユーザの所有する端末に送信する。ユーザは、一般に、検証テキストメッセージに含まれる動的検証コードを入力することを求められる。ユーザは、動的検証コードを入力すると、アプリケーションサーバのセキュリティチェックを合格し、インターネットアプリケーションへのアクセスを認められる。
【０００４】
しかしながら、検証テキストメッセージで伝えられる動的検証コードは、一般に、簡単な数字からなる。例えば、インターネット取引が実行されている場合、インターネット取引に関連するオンラインバンキングサーバが、６桁の数からなる検証テキストメッセージ

をユーザ登録端末に送信する。ユーザは、検証テキストメッセージに含まれる６桁の数字を正確に入力すると、オンラインバンキング取引を完了することを許可される。しかしながら、或る関連技術で用いられる検証テキストメッセージは、単純な書かれた数字情報を含むだけなので、悪意のある第三者が、トロイの木馬プログラムを用いて検証キストメッセージまたは検証テキストメッセージに含まれる数字情報を比較的容易に盗むことができる。悪意のある第三者は、書かれた数字情報を安全な検証インターフェースに入力することにより、セキュリティチェックを完了することができる。したがって、既存のセキュリティチェック方法で送信される数字検証コードは、比較的信頼性が低く、インターネットアプリケーションのためのアクセスセキュリティが低くなる。

【０００５】

そのため、より効果的なセキュリティチェックを提供するための方法、デバイス、サーバ、システム、および、端末が求められている。

【図面の簡単な説明】

【０００６】

以下の詳細な説明と添付の図面において、本発明の様々な実施形態を開示する。

【０００７】

これらの図面は、記載に組み込まれ、記載の一部を構成する。図面は、本願に従った実施形態を図示し、本願の原理を説明するために記載と共に用いられる。

【０００８】

【図１】本願の本開示の様々な実施形態に従って、アプリケーション背景を示す図。

【０００９】

【図２】本願の本開示の様々な実施形態に従って、セキュリティチェック方法を示すフローチャート。

【００１０】

【図３】本願の本開示の様々な実施形態に従って、セキュリティチェック方法を示すフローチャート。

【００１１】

【図４】本願の本開示の様々な実施形態に従って、セキュリティチェック方法を示すフローチャート。

【００１２】

【図５】本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図。

【００１３】

【図６】本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図。

【００１４】

【図７】本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図。

【００１５】

【図８】本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図。

【００１６】

【図９】本願の本開示の様々な実施形態に従って、サーバの一実施形態を示すブロック図。

【００１７】

【図１０】本願の本開示の様々な実施形態に従って、端末を示すブロック図。

【００１８】

【図１１】本開示の様々な実施形態に従って、セキュリティを提供するためのシステムを示す構造ブロック図。

【００１９】

【図１２】本開示の様々な実施形態に従って、セキュリティを提供するためのコンピュータシステムを示す機能図。
【発明を実施するための形態】
【００２０】
本発明は、処理、装置、システム、物質の組成、コンピュータ読み取り可能な格納媒体上に具現化されたコンピュータプログラム製品、および／または、プロセッサ（プロセッサに接続されたメモリに格納および／またはそのメモリによって提供される命令を実行するよう構成されたプロセッサ）を含め、様々な形態で実装されうる。本明細書では、これらの実装または本発明が取りうる任意の他の形態を、技術と呼ぶ。一般に、開示された処理の工程の順序は、本発明の範囲内で変更されてもよい。特に言及しない限り、タスクを実行するよう構成されるものとして記載されたプロセッサまたはメモリなどの構成要素は、ある時間にタスクを実行するよう一時的に構成された一般的な構成要素として、または、タスクを実行するよう製造された特定の構成要素として実装されてよい。本明細書では、「プロセッサ」という用語は、１または複数のデバイス、回路、および／または、コンピュータプログラム命令などのデータを処理するよう構成された処理コアを指すものとする。
【００２１】
本願は「第１」、「第２」、「第３」などの用語を用いて様々な情報を記載するが、この情報は、これらの用語によって限定されることはない。これらの用語は、単に、同じカテゴリの情報を区別するよう機能する。例えば、それらの情報が本願の範囲内にある限りは、第１情報を第２情報と呼ぶこともできる。同様に、第２情報を第１情報と呼ぶこともできる。例えば、本明細書で用いられる「ｉｆ（～の場合）」という用語は、文脈に応じて、「ｗｈｅｎ（～の時）」または「ｕｐｏｎ　ｂｅｉｎｇ　ｃｏｎｆｉｒｍｅｄ（確認後）」と解釈されうる。
【００２２】
端末とは、一般に、ネットワークシステム内で（例えば、ユーザによって）利用され、１または複数のサーバと通信するために利用されるデバイスのことである。本開示の様々な実施形態によれば、端末は、通信機能を備えてよい。例えば、端末は、スマートフォン、タブレットコンピュータ、携帯電話、ビデオ電話、電子書籍リーダ、デスクトップパーソナルコンピュータ（ＰＣ）、ラップトップＰＣ、ネットブックＰＣ、パーソナルデジタルアシスタント（ＰＤＡ）、携帯型マルチメディアプレーヤ（ＰＭＰ）、ｍｐ３プレーヤ、携帯型メディカルデバイス、カメラ、ウェアラブルデバイス（例えば、ヘッドマウントデバイス（ＨＭＤ）、電子衣服、電子装具、電子ネックレス、電子アクセサリ、電子タトゥー、または、スマートウォッチ）などであってよい。
【００２３】
本開示のいくつかの実施形態によれば、端末は、通信機能を備えたスマート家電を含む。スマート家電は、例えば、テレビ、デジタルビデオディスク（ＤＶＤ）プレーヤ、オーディオ装置、冷蔵庫、エアコン、掃除機、オーブン、電子レンジ、洗濯機、ドライヤー、空気清浄機、セットトップボックス、ＴＶボックス（例えば、ＳａｍｓｕｎｇのＨｏｍｅＳｙｎｃ（商標）、アップルＴＶ（商標）、または、Ｇｏｏｇｌｅ　ＴＶ（商標））、ゲーム機、電子辞書、電子キー、ビデオカメラ、電子写真フレームなどであってよい。
【００２４】
本開示の様々な実施形態によれば、端末は、上述の端末の任意の組み合わせであってもよい。さらに、本開示の様々な実施形態に従った端末は上述の端末に限定されないことが、当業者にとって明らかである。
【００２５】
本開示の様々な実施形態は、セキュリティを提供するための方法、デバイス、サーバ、システム、および、端末を含む。例えば、本開示の様々な実施形態は、セキュリティチェックを提供するための方法、デバイス、サーバ、システム、および、端末を含む。セキュリティチェックは、アクセスイベント（例えば、ユーザがウェブベースサービスなどのネ

ットワークサービスまたはアプリケーションへのアクセスを試みること）に関連して提供されうる。

【００２６】

図１は、本願の本開示の様々な実施形態に従って、アプリケーション背景を示す図である。

【００２７】

図１を参照すると、セキュリティ検証を用いるための背景（環境とも呼ぶ）１００が提供されている。いくつかの実施形態では、図２～図４の処理２００～４００が、環境１００内で実施されうる。

【００２８】

図に示すように、環境１００は、端末１１０およびサーバ１２０を含む。ユーザは、端末１１０にインストールされた様々なアプリケーションクライアントを通して様々なインターネットアプリケーションにアクセスできる。例えば、端末１１０は、インターネットを用いて、サーバ１２０によってホストされたウェブサイトまたはサービスにアクセスできる。アクセス処理中、ユーザは、ユーザのＩＤを認証する、メンバーとして登録する、オンライン取引に参加することなどを求められうる。アクセス処理のセキュリティを保証するために、サーバ１２０は、ユーザのＩＤに対するセキュリティチェックを実行できる。

【００２９】

ある関連技術によると、ユーザがインターネットアプリケーションへのアクセスを試みる場合、ユーザが、書かれた数字情報をセキュリティ検証インターフェースに入力することにより、セキュリティチェックが実行されうる。ユーザは、モバイルネットワークでユーザの端末に送信されたテキストメッセージから数字情報を取得できる。

【００３０】

本願の様々な実施形態によれば、セキュリティチェックは、インターネットに基づく端末１１０およびサーバ１２０の間の検証処理を含む。検証処理は、デジタルオブジェクト固有識別子（ＤＯＵＩ）ベースの技術（１３０）を用いる。後に詳述するように、セキュリティ処理に関連するＤＯＵＩベースの検証処理は、検証の信頼性およびセキュリティを向上させる。

【００３１】

図２は、本願の本開示の様々な実施形態に従って、セキュリティチェック方法を示すフローチャートである。

【００３２】

図２を参照すると、セキュリティチェックを実行するための方法２００が提供されている。いくつかの実施形態において、処理２００は、図５のデバイス５００、図６のデバイス６００、または、図９のデバイス９００によって実施できる。

【００３３】

工程２１０では、セキュリティ検証要求が受信される。いくつかの実施形態では、サーバが、セキュリティ検証要求を受信する。セキュリティ検証要求は、端末から送信されうる。端末は、アクセスイベント、オンライン取引などに関連してセキュリティ検証要求を送信できる。ユーザは、アクセスイベント、オンライン取引などに関連してセキュリティチェックを実行させることを選択できる。例えば、端末がユーザインターフェース（例えば、端末にインストールされたブラウザによって表示されたウェブサイトのウェブページ）を用いてオンライン取引を実行するために用いられる場合、その端末は、（例えば、ダイアログボックス、選択ボックスなどを介して）セキュリティ検証要求を実行するオプションを提供できる。ユーザは、インターフェース上でセキュリティ検証要求オプションを実行することを選択でき、セキュリティ検証要求オプションを実行する選択に関連して、セキュリティ検証要求が通信される。

【００３４】

いくつかの実施形態によると、セキュリティチェックは、端末上のクライアントインタ

ーフェースで提供されうる。例えば、ユーザは、端末上のクライアントを通してインターネットアプリケーション（例えば、サーバ上で実行するアプリケーション）にアクセスする場合、インターネットアプリケーションのクライアントインターフェースに入り（例えば、ブラウザを介してクライアントインターフェースを含む特定のページをロードするか、または、クライアント側のアプリケーションを用いてクライアントインターフェースを呼び出し）、クライアントインターフェースにおいてセキュリティチェックを受けることができる。例えば、セキュリティチェックは、オンライン取引に関連して（例えば、オンライン取引中に）提供されうる。この場合、ユーザは、クライアントインターフェース上でセキュリティ検証要求オプションを選択（例えば、クリック）できる。セキュリティ検証要求オプションが選択されると、サーバは、端末によって送信されたセキュリティ検証要求を受信する。

【００３５】

いくつかの実施形態において、識別子が、セキュリティ検証要求に関連して通信される。例えば、識別子は、ユーザ名、端末識別子など、または、それらの任意の組み合わせに対応しうる。識別子は、セキュリティ検証要求に含められてよい。例えば、端末を利用もしくは端末にログインしているユーザのユーザ名が、セキュリティ検証要求で通信されてよい。いくつかの実施形態において、端末識別子は、メディアアクセス制御（ＭＡＣ）アドレス、電話番号（例えば、携帯電話のＳＩＭカードまたはＵＩＭカードから読み取った電話番号）、加入者識別モジュール（ＳＩＭ）カード番号、インターネットプロトコル（ＩＰ）アドレス、国際移動体装置識別番号（ＩＭＥＩ）、移動体装置識別子（ＭＥＩＤ）、トークン、または、端末を識別する別の識別子でありうる。

【００３６】

工程２２０では、第１検証要素情報が取得される。いくつかの実施形態では、サーバが、第１検証要素情報を取得する。例えば、サーバは、セキュリティ検証要求に従って第１検証要素情報を取得できる。

【００３７】

いくつかの実施形態において、サーバは、ユーザ名と端末情報との間の対応関係を格納できる。例えば、サーバは、ユーザ名と、ユーザによって用いられる端末の端末識別子との間の関連を格納できる。端末によって送信されたセキュリティ検証要求が受信されると、ユーザ名と端末情報との間の保存済みの対応関係が、（セキュリティ検証要求に含まれる）端末所有者のユーザ名で検索されて、端末ユーザに対応する端末の端末識別子が取得されうる。端末識別子は、第１端末識別子と呼ぶことができる。

【００３８】

いくつかの実施形態において、サーバは、セキュリティ検証要求に少なくとも部分的に基づいて、現在のセキュリティチェックに関連する第１セキュリティ検証コードおよび第１タイムスタンプを生成できる。第１タイムスタンプは、現在のセキュリティチェックの期限を示すために利用されうる。第１セキュリティ検証コードは、テキスト、数字、キャプション、画像、リンクなど、または、それらの任意の組み合わせでありうる。第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプは、集合的に第１検証要素情報と呼ぶことができる。第１検証コードは、ランダムに生成されうる。例えば、第１検証コードは、ランダム化計算関数（ＲａｎｄｏｍＳｔｒｉｎｇＵｔｉｌｓ．ｒａｎｄｏｍＡｌｐｈａｎｕｍｅｒｉｃ（ｉｎｔ　ｌｅｎｇｔｈ）など）を用いて生成できる。

【００３９】

工程２３０では、デジタルオブジェクト固有識別子が生成される。いくつかの実施形態では、サーバが、デジタルオブジェクト固有識別子を生成する。デジタルオブジェクト固有識別子は、第１検証要素情報に少なくとも部分的に基づいて生成されうる。例えば、デジタルオブジェクト固有識別子は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを用いて生成されうる。

【００４０】

いくつかの実施形態において、デジタルオブジェクト固有識別子は、数字情報を識別す

るために用いられるツールである。デジタルオブジェクト固有識別子は、二次元コード、バーコード、クイックレスポンス（ＱＲコード（登録商標））コードなど、または、それらの任意の組み合わせを含みうる。デジタルオブジェクト固有識別子は、デジタルオブジェクト固有識別子が用いられるアプリケーション環境に従って構成されうる。例えば、デジタルオブジェクト固有識別子は、アプリケーション環境に従って、二次元コード、バーコード、ＱＲコードなどを含むよう構成されうる。いくつかの実施形態において、サーバは、セキュリティチェックの信頼性を高めるために、デジタルオブジェクト固有識別子を用いて検証情報を伝えることができる。サーバは、第１検証要素情報を取得すると、第１組み合わせ文字列を生成できる。サーバは、それに含まれる第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを用いて、組み合わせ文字列を生成できる。例えば、サーバは、それに含まれる第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせて、第１組み合わせ文字列を生成できる。サーバは、組み合わせ文字列を生成すると、第１組み合わせ文字列を入力として受け入れる生成関数を実行することにより、第１組み合わせ文字列を用いてデジタルオブジェクト固有識別子を生成できる。第１組み合わせ文字列を用いてデジタル固有識別子を生成するために、文字列を用いてデジタルオブジェクト固有識別子を生成するための様々な周知の方法（例えば、ｉＯＳライブラリを提供されたｃｒｅａｔｅＱＲＦｏｒＳｔｒｉｎｇ　関数）を利用できる。

【００４１】

工程２４０では、デジタルオブジェクト固有識別子が通信される。いくつかの実施形態では、サーバが、デジタルオブジェクト固有識別子を通信する。例えば、サーバは、デジタルオブジェクト固有識別子を端末へ送信できる。デジタルオブジェクト固有識別子に対応する画像（例えば、２Ｄバーコード、ＱＲコードなど）が、サーバが端末に送信するメッセージに含まれうる。

【００４２】

いくつかの実施形態では、端末とサーバとの間の検証処理全体が、インターネットベースである。したがって、サーバは、オンライン通信を介して、デジタルオブジェクト固有識別子を端末へ送信できる。デジタルオブジェクト固有識別子は、電子メールへの添付、インスタントメッセージへの添付として、ウェブページに関連して、ＨＴＴＰセッションに関連して、などの方法で、端末に送信されうる。

【００４３】

工程２５０では、第２検証要素情報が受信される。いくつかの実施形態では、サーバが、第２検証要素情報を受信する。例えば、サーバは、第２検証要素情報を端末から受信できる。端末は、デジタルオブジェクト固有識別子を受信するよう構成されたコードを含み、デジタルオブジェクト固有識別子を受信したことに応答して、第２検証要素情報をサーバへ通信する。第２検証要素情報は、デジタルオブジェクト固有識別子を用いて端末によって取得された検証要素情報を含むか、もしくは、他の方法で対応しうる。例えば、端末は、デジタルオブジェクト固有識別子から第１検証要素情報を抽出し、デジタルオブジェクト固有識別子から抽出した第１検証要素情報を用いて第２検証要素情報を生成できる。

【００４４】

いくつかの実施形態において、端末は、サーバから受信したデジタルオブジェクト固有識別子をスキャン、または、他の方法で処理（例えば、解析）する。端末は、受信したデジタルオブジェクト固有識別子をスキャンするか、または、他の方法で処理すると、第２組み合わせ文字列を取得する。端末は、第２組み合わせ文字列を分解または他の方法で処理できる。端末は、第２組み合わせ文字列を分解することにより、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを取得できる。第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプは、第２検証要素情報に属するか、または、他の方法で集合的に対応する。例えば、第２検証要素情報は、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含みうる。いくつかの実施形態において、端末は、サーバから受信したデジタルオブジェクト固有識別子から

取得した第２端末識別子が、端末の端末識別子と同じであるか否かを判定できる。端末は、サーバから受信したデジタルオブジェクト固有識別子から取得した第２端末識別子が、端末の端末識別子と同じであると判定した場合、第２検証要素情報をサーバへ送信できる。

【００４５】

端末は、端末に接続されたカメラによって取り込まれたデジタルオブジェクト固有識別子の画像を処理することにより、デジタルオブジェクト固有識別子をスキャンできる。いくつかの実施形態において、デジタルオブジェクト固有識別子のスキャンは、端末に接続されたカメラでデジタルオブジェクト固有識別子の画像を取り込むことを含む。

【００４６】

いくつかの実施形態において、端末は、第１端末によって表示されたデジタルオブジェクト固有識別子（例えば、２ＤコードまたはＱＲコード）を取り込むために端末のカメラを起動するアプリケーションをインストールされている。端末は、画像認識を用いて、画像から幾何学的画像を抽出し、それに従って画像を復号する画像処理コードを含む。

【００４７】

いくつかの実施形態において、端末は、電子メールメッセージ、ショートメッセージサービス（ＳＭＳ）メッセージ、マルチメディアメッセージサービス（ＭＭＳ）メッセージなどからデジタルオブジェクト固有識別子を取得する。端末は、デジタルオブジェクト固有識別子（例えば、２ＤコードまたはＱＲコード）またはその画像を電子メールメッセージから抽出し、画像処理コードを用いて（例えば、実行することによって）デジタルオブジェクト固有識別子を変換できる。画像処理コードは、デジタルオブジェクト固有識別子に含まれた（例えば、埋め込まれた）情報を取得するために、デジタルオブジェクト固有識別子を逆変換できる。デジタルオブジェクト固有識別子に含まれる情報（例えば、セキュリティ検証コード、携帯電話番号、タイムスタンプなど）は、所定の文字（例えば、ハイフン）によって分離されうる。

【００４８】

工程２６０では、セキュリティチェック合格情報が通信される。いくつかの実施形態では、サーバが、セキュリティチェック合格情報を端末に通信する。サーバは、第２検証要素情報が第１検証要素情報と一致するか否かを判定できる。例えば、サーバは、第２検証要素情報が第１検証要素情報とマッチするか否かを判定できる。サーバは、第１検証要素情報および第２検証要素情報が一致することを確認すると（例えば、第１検証コードが第２検証コードと比較され、第１タイムスタンプおよび第２タイムスタンプがサーバに従った現在時刻と比較されると）、セキュリティチェック合格情報を端末に送り返すことができる。セキュリティチェック合格情報は、端末がセキュリティチェックを合格したことを示しうる。サーバは、第１検証要素情報および第２検証要素情報が一致しない（例えば、マッチしない）と判定した場合、端末へのセキュリティチェックが不合格であった旨の示唆を送信し、ドメイン（例えば、サーバ）への端末アクセスを拒否する、もしくは、セキュリティチェックに関連する取引を拒否または他の方法で防止できる。

【００４９】

いくつかの実施形態において、サーバは、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを格納する。例えば、サーバは、第１検証要素情報を取得すると、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプの間の関係性（例えば、関連）を格納できる。関係性は、テーブルまたはデータベースに格納されうる。第２検証要素情報を受信したことに応答して、サーバは、第２端末識別子（例えば、第２検証要素情報に含まれる端末識別子）を用いて、端末識別子、セキュリティ検証コード、および、タイムスタンプの格納済みの関係性を検索することで、第２端末識別子に対応するセキュリティ検証コードおよびタイムスタンプを取得できる。サーバは、第２セキュリティ検証コードおよび取得したセキュリティ検証コードが同じであること、第２タイムスタンプおよび取得したタイムスタンプが同じであること、ならびに、第２タイムスタンプが（例えば、サーバの現在時刻に対応すると決定されうる）現在のセキュ

リティチェックの期限（例えば、６０秒）内にあることを決定（例えば、確認）した場合に、セキュリティチェック合格情報を端末に送信する。

【００５０】

デジタルオブジェクト固有識別子は、セキュリティチェック中に検証情報を送信するために利用できる。デジタルオブジェクト固有識別子に関連して、数字だけを含むテキストメッセージを実施する或る連技術に従ったセキュリティチェックよりも豊富かつ信頼性の高い確認情報が送信されうる。数値と比較すると、デジタルオブジェクト固有識別子に関連して送信される確認情報は、盗んで利用することが比較的困難である。したがって、書かれた数字の通信に関連したテキストメッセージではなく、確認情報の通信にデジタルオブジェクト固有識別子を用いることによって、インターネットアプリケーションのアクセスセキュリティを強化できる。様々な実施形態によれば、デジタルオブジェクト固有識別子は、インターネットトラフィックを介して送信されるため、検証コードがテキストメッセージを介して送信される場合に生じる通信費が避けられる。結果として、様々な実施形態において、セキュリティチェックの実行に必要なモバイル通信リソースが削減される。いくつかの実施形態によれば、端末は、デジタルオブジェクト固有識別子またはデジタルオブジェクト固有識別子に含まれる情報を認識したことに応答して、認識情報をサーバへ自動的に送り返すことができる。したがって、様々な実施形態に従ったセキュリティチェック処理は、ユーザによる手入力を必要とせず、手動での確認情報の不正の可能性を避ける。

【００５１】

図３は、本願の本開示の様々な実施形態に従って、セキュリティチェック方法を示すフローチャートである。

【００５２】

図３を参照すると、セキュリティチェックを実行するための方法３００が提供されている。いくつかの実施形態において、処理３００は、図７のデバイス７００、図８のデバイス８００、または、図１０の端末１０００によって実施できる。

【００５３】

工程３１０では、セキュリティ検証要求が通信される。いくつかの実施形態では、端末が、セキュリティ検証要求をサーバへ送信できる。端末は、アクセスイベント、オンライン取引などに関連してセキュリティ検証要求を送信できる。ユーザは、アクセスイベント、オンライン取引などに関連してセキュリティチェックを実行させることを選択できる。例えば、端末がユーザインターフェース（例えば、端末にインストールされたブラウザによって表示されたウェブサイトのウェブページ）を用いてオンライン取引を実行するために用いられる場合、その端末は、（例えば、ダイアログボックス、選択ボックスなどを介して）セキュリティ検証要求を実行するオプションを提供できる。ユーザは、インターフェース上でセキュリティ検証要求オプションを実行することを選択でき、セキュリティ検証要求オプションを実行する選択に関連して、セキュリティ検証要求が通信される。

【００５４】

いくつかの実施形態によると、セキュリティチェックは、端末上のクライアントインターフェースで提供されうる。例えば、ユーザは、端末上のクライアントを通してインターネットアプリケーション（例えば、サーバ上で実行するアプリケーション）にアクセスする場合、インターネットアプリケーションのクライアントインターフェースに入り（例えば、ブラウザを介してクライアントインターフェースを含む特定のページをロードするか、または、クライアント側のアプリケーションを用いてクライアントインターフェースを呼び出し）、クライアントインターフェースにおいてセキュリティチェックを受けることができる。例えば、セキュリティチェックは、オンライン取引に関連して提供されうる。ユーザがクライアントインターフェース上の要求オプションを選択（例えば、クリック）すると、セキュリティ検証要求が、端末を通してサーバへ送信されうる。

【００５５】

いくつかの実施形態において、識別子が、セキュリティ検証要求に関連して通信される

。例えば、識別子は、ユーザ名、端末識別子など、または、それらの任意の組み合わせに対応しうる。識別子は、セキュリティ検証要求に含められてよい。例えば、端末を利用もしくは端末にログインしているユーザのユーザ名が、セキュリティ検証要求で通信される。

【００５６】

工程３２０では、デジタルオブジェクト固有識別子が受信される。いくつかの実施形態では、端末が、デジタルオブジェクト固有識別子を受信する。端末は、デジタルオブジェクト固有識別子をサーバから受信できる。例えば、デジタルオブジェクト固有識別子は、サーバがセキュリティ検証要求を受信したこと（および処理したこと）に応答して、サーバによって送り返されうる。デジタルオブジェクト固有識別子は、サーバがセキュリティ検証要求に従って第１検証要素情報を取得した後に、第１検証要素情報に従って生成される識別子である。例えば、デジタルオブジェクト固有識別子は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを用いて生成されうる。第１セキュリティ検証コードは、セキュリティ検証要求に含まれるか、または、セキュリティ検証要求に関連して通信される端末識別子（例えば、第１端末識別子）に従って、決定されうる。第１タイムスタンプは、現在のセキュリティチェックの期限を示すために利用されうる。

【００５７】

工程３３０では、第２検証要素情報が取得される。いくつかの実施形態では、端末が、第２検証要素情報を取得する。端末は、デジタルオブジェクト固有識別子を用いて第２検証要素情報を取得できる。端末は、端末がデジタルオブジェクト固有識別子を受信したことに応答して、第２検証要素情報をサーバへ通信できる。第２検証要素情報は、デジタルオブジェクト固有識別子を用いて端末によって取得された検証要素情報を含むか、もしくは、他の方法で対応しうる。例えば、端末は、デジタルオブジェクト固有識別子から検証要素情報を抽出し、デジタルオブジェクト固有識別子から抽出した検証要素情報を用いて第２検証要素情報を生成できる。

【００５８】

デジタルオブジェクト固有識別子は、サーバによって生成されうる。例えば、デジタルオブジェクト固有識別子は、第１組み合わせ文字列に少なくとも部分的に基づいて生成されうる。第１組み合わせ文字列は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを用いて生成されうる。例えば、サーバは、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることによって、第１組み合わせ文字列を生成できる。第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプは、第１検証要素情報に属するか、または、含まれうる。第１端末識別子は、端末の端末識別子に対応しうる。端末の端末識別子は、セキュリティ検証要求に含まれる情報に少なくとも部分的に基づいて決定されうる。例えば、端末の端末識別子は、セキュリティ検証要求で伝えられる端末ユーザ名に従って決定されうる。第１セキュリティチェックは、現在のセキュリティチェックに関連してサーバによって生成されたセキュリティ検証コードに対応し、第１タイムスタンプは、現在のセキュリティチェックに関連してサーバによって生成されたタイムスタンプに対応しうる。

【００５９】

いくつかの実施形態において、端末は、サーバから受信したデジタルオブジェクト固有識別子をスキャン、または、他の方法で処理（例えば、解析）する。端末は、受信したデジタルオブジェクト固有識別子をスキャンするか、または、他の方法で処理すると、第２組み合わせ文字列を取得できる。例えば、端末は、デジタルオブジェクト固有識別子をスキャンすることによって、第２組み合わせ文字列を取得できる。端末は、第２組み合わせ文字列を分解または他の方法で処理できる。端末は、第２組み合わせ文字列を分解することにより、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを取得できる。第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプは、第２検証要素情報に属するか、または、他の方法で集合的に対応する。例えば、

第２検証要素情報は、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含みうる。

【００６０】

工程３４０では、第２検証要素情報が通信される。いくつかの実施形態では、端末が、第２検証要素情報を通信する。例えば、端末は、第２検証要素情報をサーバに送信できる。

【００６１】

いくつかの実施形態において、端末は、サーバから受信したデジタルオブジェクト固有識別子から取得した第２端末識別子が、端末の端末識別子と同じであるか否かを判定できる。端末は、サーバから受信したデジタルオブジェクト固有識別子から取得した第２端末識別子が、端末の端末識別子と同じであると判定した場合、第２検証要素情報をサーバへ送信できる。

【００６２】

工程３５０では、セキュリティチェックの結果が受信される。いくつかの実施形態では、端末が、セキュリティチェックの結果をサーバから受信する。例えば、セキュリティチェックが成功した場合、端末は、セキュリティチェック合格情報をサーバから受信できる。

【００６３】

サーバは、第２検証要素情報が第１検証要素情報と一致するか否かを判定できる。例えば、サーバは、第２検証要素情報が第１検証要素情報とマッチするか否かを判定できる。サーバが、第１検証要素情報および第２検証要素情報が一致（例えば、マッチ）することを確認した場合、サーバは、セキュリティチェック合格情報を端末に送信することができ、端末は、セキュリティチェック合格情報を受信できる。セキュリティチェック合格情報は、端末がセキュリティチェックを合格したこと（例えば、セキュリティチェックが成功したこと）を示しうる。サーバは、第１検証要素情報および第２検証要素情報が一致しない（例えば、マッチしない）と判定した場合、端末へのセキュリティチェックが不合格であった旨の示唆を送信し、ドメイン（例えば、サーバ）への端末アクセスを拒否する、もしくは、セキュリティチェックに関連する取引を拒否または他の方法で防止できる。

【００６４】

いくつかの実施形態において、サーバは、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを格納できる。例えば、サーバは、第１検証要素情報を取得すると、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプの間の関係性を格納できる。関係性は、テーブルまたはデータベースに格納されうる。第２検証要求情報を受信したことに応答して、サーバは、端末識別子、セキュリティ検証コード、および、タイムスタンプの格納済みの関係性を検索して、第２端末識別子（例えば、第２検証要素情報に含まれる端末識別子）に対応するセキュリティ検証コードおよびタイムスタンプを取得できる。サーバは、第２セキュリティ検証コードおよび取得したセキュリティ検証コードが同じであること、第２タイムスタンプおよび取得したタイムスタンプが同じであること、ならびに、第２タイムスタンプが現在のセキュリティチェックの期限内にあることを決定（例えば、確認）した場合に、セキュリティチェック合格情報を端末に送信できる。

【００６５】

デジタルオブジェクト固有識別子は、セキュリティチェック中に検証情報を送信するために利用できる。デジタルオブジェクト固有識別子に関連して、書かれた数字を含むテキストメッセージを実施する或る連技術に従ったセキュリティチェックよりも豊富かつ信頼性の高い確認情報が送信されうる。いくつかの実施形態では、デジタルオブジェクト固有識別子に関連して送信される確認情報は、盗んで利用することが比較的困難である。したがって、書かれた数字の通信に関連したテキストメッセージではなく、確認情報の通信にデジタルオブジェクト固有識別子を用いることによって、インターネットアプリケーションのアクセスセキュリティを強化できる。様々な実施形態によれば、デジタルオブジェク

ト固有識別子は、インターネットトラフィックを介して送信されるため、検証コードがテキストメッセージを介して送信される場合に生じる通信費が避けられる。結果として、様々な実施形態において、セキュリティチェックの実行に必要なモバイル通信リソースがの削減が実現する。いくつかの実施形態によれば、端末は、デジタルオブジェクト固有識別子またはデジタルオブジェクト固有識別子に含まれる情報を認識したことに応答して、認識情報をサーバへ自動的に送り返すことができる。したがって、様々な実施形態に従ったセキュリティチェック処理は、ユーザによる手入力を必要とせず、手動での確認情報の不正の可能性を避ける。

【００６６】

様々な実施形態によれば、セキュリティチェック処理は、端末およびサーバの間のやり取りに関連して実行されうる。セキュリティチェック処理に関連して用いられるデジタルオブジェクト固有識別子は、二次元コードでありうる。

【００６７】

図４は、本願の本開示の様々な実施形態に従って、セキュリティチェック方法を示すフローチャートである。

【００６８】

図４を参照すると、セキュリティチェックを実行するための方法４００が提供されている。いくつかの実施形態において、処理４００の少なくとも一部は、図５～図１０のデバイス５００、６００、７００、８００、９００、および、１０００によって実施できる。

【００６９】

工程４１０では、サーバ４０２が、ユーザ識別子および端末識別子の間の対応関係を格納する。例えば、サーバ４０２は、ユーザ名および端末識別子の間の対応関係を格納する。サーバ４０２は、ユーザ識別子および端末識別子の間の対応関係を、テーブル、データベースなど、または、それらの任意の組み合わせに格納できる。

【００７０】

いくつかの実施形態において、セキュリティチェックを受ける端末は、モバイル通信機能を持つ携帯デバイス（例えば、携帯電話）である。したがって、端末識別子は、携帯電話番号、ＳＩＭカード番号などでありうる。サーバは、具体的なセキュリティチェックシナリオでセキュリティチェックを実施できるように、ユーザのユーザ名とユーザそれぞれの端末識別子（例えば、携帯電話番号）との間の対応関係を予め保存できる。例えば、ユーザが特定のインターネットアプリケーションに登録されると、そのユーザは、一般に、ユーザの認証情報（例えば、ユーザ名、パスワード、携帯電話番号、および、その他の情報）を入力することを求められる。アプリケーションサーバは、ユーザの認証情報を受信すると、かかる情報の対応関係を保存できる。別の例において、ユーザがインターネットバンキングを開始する場合、取引サーバは、かかる情報の対応関係を保存でき、支払いウェブサイトの支払いサーバと情報の対応関係を同期することができる。

【００７１】

工程４１２では、端末４０１が、セキュリティ検証要求をサーバ４０２へ送信する。

【００７２】

いくつかの実施形態によると、セキュリティチェックは、端末上のクライアントインターフェースで提供されうる。例えば、ユーザがユーザの端末４０１のクライアントを通してインターネットアプリケーションにアクセスすると、そのユーザは、インターネットアプリケーションのクライアントインターフェースに入り（例えば、ロードし）、クライアントインターフェースでセキュリティチェックを受けることができる。例えば、セキュリティチェックは、オンライン取引に関連して提供されうる。ユーザがクライアントインターフェース上の要求オプションを選択（例えば、クリック）した後、セキュリティ検証要求が、端末４０１を通してサーバ４０２へ送信されうる。

【００７３】

工程４１４では、サーバ４０２が、端末４０１に対応する第１端末識別子を取得する。例えば、サーバ４０２は、セキュリティ検証要求で伝えられた、または、それに関連して

通信された端末のユーザ名を用いて、対応関係を検索することができ、端末４０１のユーザ名に対応する端末４０１と関連づけられている第１端末識別子を取得する。

【００７４】

サーバは、セキュリティ検証要求から端末のユーザ名を取得し、対応関係（たとえば、工程４１０において保存された対応関係）の検索に端末のユーザ名を用いることで、ユーザ名に対応する端末４０１の端末識別子を取得できる。端末４０１の端末識別子は、第１端末識別子に対応する。

【００７５】

工程４１６では、サーバ４０２が、第１セキュリティ検証コードおよび第１タイムスタンプを生成する。サーバ４０２は、セキュリティ検証要求を受信すると、第１セキュリティ検証コードおよび第１タイムスタンプを生成する。例えば、第１セキュリティ検証コードおよび第１タイムスタンプは、セキュリティ検証要求に関連づけられる。

【００７６】

サーバは、現在のセキュリティチェックに関連して、第１セキュリティ検証コードおよび第１タイムスタンプを自動的に生成できる。第１タイムスタンプは、現在のセキュリティチェックの期限を示すために利用されうる。第１セキュリティ検証コードは、具体的には、テキスト、数字、キャプション、画像、リンクなど、または、それらの任意の組み合わせであってよい。第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプは、集合的に第１検証要素情報と呼ぶことができる。

【００７７】

工程４１８では、サーバ４０２が、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプの間の関係性を保存する。サーバは、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプの間の関係性を保存する。

【００７８】

いくつかの実施形態において、関係テーブルが、各セキュリティチェックの端末識別子、セキュリティ検証コード、および、タイムスタンプの間の関係性を保存するために、サーバ内に構成される。

【００７９】

工程４２０では、第１組み合わせ文字列が生成される。いくつかの実施形態では、サーバ４０２が、第１組み合わせ文字列を生成する。第１組み合わせ文字列は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプに少なくとも部分的に基づいて生成されうる。例えば、第１組み合わせ文字列は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることによって生成されうる。

【００８０】

様々な実施形態によれば、様々な組み合わせ方法を用いて、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることができる。例えば、第１端末識別子が端末ユーザ携帯電話番号「１３０００００１２３４」に対応し、第１セキュリティ検証コードが「Ａｊ８９」であり、第１タイムスタンプが「５－１２－２０１４　１４：０６　１８９」であると仮定すると、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプは、ダブルスラッシュまたはその他の区切り文字を用いて組み合わせられ、１３０００００１２３４／／５－１２－２０１４　１４：０６　１８９／／Ａｊ８９などの第１組み合わせ文字列を形成しうる。

【００８１】

工程４２２では、検証コードが生成される。いくつかの実施形態では、サーバ４０２が、検証コードを生成する。検証コードは、第１組み合わせ文字列に少なくとも部分的に基づいて生成されうる。一例として、検証コードは、二次元コード、バーコード、ＱＲコードなどを含むよう構成されてよい。いくつかの実施形態において、検証コードは、デジタルオブジェクト固有識別子に対応しうる。例えば、サーバ４０２は、第１組み合わせ文字列を用いて、二次元検証コードを生成できる。第１組み合わせ文字列は、二次元検証コー

ドを生成するために処理および利用されうる。

【００８２】

二次元検証コードが生成される場合、第１組み合わせ文字列を暗号化して、暗号化文字列を生成することができる。暗号化文字列は、二次元検証コードを生成するために利用できる。暗号化文字列の中の文字は通例は長いので、暗号化文字列は、ｂａｓｅ６４文字列に変換されうる。ｂａｓｅ６４文字列を符号化して、二次元検証コードを生成することができる。様々な実施形態によれば、暗号化文字列は、ｎ進数文字列に変換可能であり、ここでｎは正の整数である。第１組み合わせ文字列は、様々な暗号化方法に従って暗号化できる。例えば、第１組み合わせ文字列は、ハッシュ暗号化法、対称暗号化法、非対称暗号化法、ＭＤ５など、周知の暗号化技術を用いて生成できる。いくつかの実施形態では、任意の文字列暗号化が利用されうる。例えば、６４ビットのキーを用いて６４ビット文字列を暗号化するデータ暗号化規格（ＤＥＳ）が、暗号化された６４ビット値を生成するために利用されうる。

【００８３】

いくつかの実施形態において、二次元検証コードは、個々のパターンに従って幾何学図形の平面にわたって分布された交互の黒白を含むグラフィック図である。端末は、二次元検証コードスキャンソフトウェアで二次元コード情報を読み取る（例えば、スキャンする）ことができる。例えば、端末は、二次元検証コードの画像を取り込み、取り込んだ画像を処理して、二次元コードに埋め込まれるかまたは他の方法で含まれた情報を抽出できる。一例として、端末は、端末のカメラを用いて二次元検証コードの画像を取り込む画像キャプチャコードを呼び出すことにより、二次元検証コードの画像を取り込むことができる。別の例として、端末は、電子メール、ＳＭＳメッセージ、ＭＭＳメッセージ、インスタントメッセージなどのメッセージから、二次元検証コードの画像すなわち二次元検証コード自体を抽出することによって、二次元検証コードの画像を取り込むことができる。二次元検証コードは、ＱＲルールに従って符号化および生成されたＱＲコードであってよい。ＱＲコードは、テキスト、画像、および、その他の異なるタイプの符号化用のデータなど、より多くの情報を迅速に読み取りおよび保存できる。いくつかの実施形態において、ＱＲコードは、正方形であり、黒および白の２色のみを有する。ＱＲコードは、４つの角の内の３つに印刷されたより小さい正方形を含みうる。これら３つの正方形は、ユーザが、任意の角度からＱＲコードをスキャンすることを可能にする。例えば、３つの角に含まれる小さい正方形は、所定の向きに従ってＱＲコードを処理できるようにＱＲコードの相対位置を決定することを可能にする。

【００８４】

いくつかの実施形態において、第１組み合わせ文字列が対称暗号化アルゴリズムを用いて暗号化される場合、同じ暗号化キーが、サーバ４０２および端末４０１（例えば、端末４０１にインストールされたクライアントプログラム）に別個に保存される。第１組み合わせ文字列が非対称暗号化アルゴリズムを用いて暗号化される場合、暗号化キーが、サーバ４０２に保存され、復号キーが端末４０１（例えば、端末４０１にインストールされたクライアントプログラム）に保存されうる。いくつかの実施形態において、第１組み合わせ文字列の暗号化に用いられる暗号化アルゴリズムのタイプにかかわらず、サーバ４０２は、保存された暗号化キーを用いて第１組み合わせ文字列を暗号化する。

【００８５】

工程４２４では、サーバ４０２が、二次元検証コード（例えば、検証コード）を端末４０１へ送信する。サーバ４０２は、インターネットを介して二次元検証コードを端末４０１へ送信できる。

【００８６】

いくつかの実施形態では、端末とサーバ４０２との間の検証処理全体が、インターネットベースである。したがって、サーバ４０２は、二次元検証コードをオンライン送信で端末４０１へ送信できる。

【００８７】

工程４２６では、第２組み合わせ文字列が取得される。いくつかの実施形態では、端末４０１が、第２組み合わせ文字列を取得する。端末４０１は、検証コードを用いて（例えば、検証コードから）第２組み合わせ文字列を取得できる。例えば、端末４０１は、二次元検証コードをスキャン（および処理）することによって、第２組み合わせ文字列を取得する。いくつかの実施形態において、第２組み合わせ文字列を生成するために用いられる情報が、二次元検証コードから抽出されうる。

【００８８】

端末４０１が二次元検証コードを受信すると、二次元検証コードは、二次元組み合わせ文字列を取得するために、二次元コードスキャンソフトウェアでスキャンされうる。サーバ４０２が工程４２２で二次元コードを生成するための処理に対応して、端末４０１は、二次元コードスキャン処理において、ＱＲ復号ルールに従って、二次元検証コードを復号して、ｂａｓｅ６４文字列を生成できる。ｂａｓｅ６４文字列は、暗号化文字列に変換され、暗号化文字列は、第２組み合わせ文字列を取得するために復号されうる。端末４０１は、復号を実行すると、サーバ４０２によって保存された暗号化キーに対応する復号キーを用いて、暗号化文字列を復号する。

【００８９】

工程４２８では、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプが取得される。いくつかの実施形態では、端末４０１が、第２組み合わせ文字列を用いて（例えば、第２組み合わせ文字列から）、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを取得する。例えば、いくつかの実施形態において、端末４０１は、第２組み合わせ文字列を分解して、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを取得できる。

【００９０】

いくつかの実施形態において、端末４０１は、第１組み合わせ文字列が（例えば、サーバ４０２によって）生成された時に適用された組み合わせルールに対応する逆のルールを用いて第２組み合わせ文字列を分解することにより、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを取得する。第２組み合わせ文字列の分解の結果は、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプでありうる。

【００９１】

工程４３０では、第２端末識別子が端末４０１の端末識別子に対応するか否かについて判定がなされる。いくつかの実施形態では、端末４０１が、第２端末識別子を端末４０１の端末識別子（例えば、第１端末識別子）と比較して、第２端末識別子および端末４０１の端末識別子が一致するか（例えば、合致するか）否かを判定する。

【００９２】

いくつかの実施形態において、セキュリティチェックの第１再検証が、端末４０１において完了されうる。例えば、端末４０１は、（端末４０１が第２組み合わせ文字列の分解を通して取得した）第２端末識別子を、自身の第１端末識別子と比較することができる。第２端末識別子および第１端末識別子が同じである場合、第２端末識別子および第１端末識別子の一致は、端末４０１がセキュリティチェックを受けているユーザの指定端末であることを示すと見なされうる。第２端末識別子および第１端末識別子が同じでない場合、第２端末識別子および第１端末識別子の不一致は、端末４０１がユーザの指定端末ではないことを示すと見なされうる。例えば、端末４０１の所有者が、セキュリティチェックを受けることを望むユーザではない場合がある。それにより、セキュリティチェックの検出の有効性が向上する。

【００９３】

いくつかの実施形態において、端末がマルチカードマルチモード携帯電話である場合、端末４０１は、分解を通して取得した携帯電話番号を端末４０１の携帯電話番号と比較する時に、端末４０１のすべての携帯電話番号を網羅してよい。端末４０１の任意の携帯電話が分解を通して得られた携帯電話番号と同じである場合、マッチする端末４０１が、ユ

ーザの指定携帯電話であると確定されうる。

【００９４】

第２端末識別子が端末４０１の端末識別子と一致しない（例えば、マッチしない）場合、工程４３２において、セキュリティチェックは不合格となる。端末４０１は、セキュリティチェックが不合格であった旨の示唆をユーザに提供できる。例えば、端末４０１は、ポップアップダイアログボックス、振動、音声、スクリーンの明るさの変化、インジケータライトなど、または、それらの任意の組み合わせによって、示唆を提供できる。第２端末識別子が端末４０１の端末識別子と一致しない（例えば、マッチしない）場合、セキュリティチェック処理は終了しうる。

【００９５】

第２端末識別子が端末４０１の端末識別子と一致（例えば、マッチ）する場合、工程４３４において、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプが通信されうる。いくつかの実施形態では、端末４０１が、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプをサーバ４０２へ送信する。

【００９６】

端末４０１は、第２端末識別子を端末４０１の端末識別子を比較し、第２端末識別子が端末４０１の端末識別子（例えば、第１端末識別子）と同じであると判定した場合、サーバ４０２が、さらに、セキュリティチェックインターネット動作の信頼性を検証して、効果的にさらなる検証を実行できるように、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプをサーバ４０２へ送信できる。例えば、端末４０１は、サーバ４０２の通信インターフェース（例えば、ハイパーテキスト・トランスファー・プロトコル（ＨＴＴＰ）接続またはハイパーテキスト・トランスファー・プロトコル・オーバー・セキュア・ソケット・レイヤ（ＨＴＴＰＳ）接続）で通信チャネルを確立し、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを送信できる。例えば、端末４０１は、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプが、サーバ４０２へのインターフェースの３つのパラメータであるかのように、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを送信できる。したがって、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプをサーバ４０２へ送信するために、手動の操作は必要はない。実施形態において、セキュリティチェック処理は、セキュリティチェックを完了させるために、端末４０１のユーザからの手動操作を必要としない。

【００９７】

工程４３６では、サーバ４０２が、関係性の中から、第２端末識別子に対応する関係性を検索する。例えば、サーバ４０２は、端末識別子、セキュリティ検証コード、および、タイムスタンプの間の対応関係の記録（例えば、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプの記録）を検索する。サーバ４０２は、第２端末識別子に対応する記録を見つけると、第２端末識別子に対応する検証コード（例えば、第１検証コード）およびタイムスタンプ（例えば、第１タイムスタンプ）を取得する。

【００９８】

サーバは、受信した第２端末識別子をインデックスとすることにより、工程４１８において保存された関係性を検索し、第２端末識別子に対応するセキュリティ検証コードおよびタイムスタンプを取得できる。

【００９９】

工程４３８において、サーバは、取得したセキュリティ検証コードおよび取得したタイムスタンプ（例えば、第２端末識別子に関連する記録に対応するセキュリティ検証コードおよびタイムスタンプ）が、第２セキュリティ検証コード（例えば、工程４３４で受信された第２検証コード）および第２タイムスタンプ（例えば、工程４３４において受信された第２タイムスタンプ）とマッチするか否かを判定する。いくつかの実施形態において、サーバは、第２セキュリティ検証コードおよび第２タイムスタンプが、第２端末識別子に従って取得されたセキュリティ検証コードおよびタイムスタンプと同じであるか否か、な

らびに、第２タイムスタンプが現在のセキュリティチェックの期限内であるか否かを判定する。

【０１００】

工程４３８において、サーバ４０２は、（例えば、工程４１８で格納された第１セキュリティ検証コードに対応する）第２セキュリティ検証コードおよび工程４３４で取得されたセキュリティ検証コードが同じであり、（例えば、工程４１８において格納された第１タイムスタンプに対応する）第２タイムスタンプおよび工程４３４において取得されたタイムスタンプが同じでり、現在時刻が第２タイムスタンプによって規定された時間範囲を外れていないと判定した場合、端末がセキュリティチェックを合格したと確定できる。

【０１０１】

取得したセキュリティ検証コードおよび取得したタイムスタンプ（例えば、第２端末識別子に関連する記録に対応するセキュリティ検証コードおよびタイムスタンプ）が、第２セキュリティ検証コード（例えば、工程４３４において受信された第２検証コード）および第２タイムスタンプ（例えば、工程４３４において受信された第２タイムスタンプ）とマッチしないと、サーバが判定した場合、セキュリティチェックは不合格になる。セキュリティチェックが不合格であった場合、工程４４０において、サーバ４０２は、セキュリティチェック不合格情報を端末４０１へ送信できる。端末４０１は、サーバ４０２からセキュリティチェック不合格情報を受信すると、セキュリティチェックが不合格であった旨の示唆をユーザに提供できる。例えば、端末４０１は、ポップアップダイアログボックス、振動、音声、スクリーンの明るさの変化、インジケータライトなど、または、それらの任意の組み合わせによって、示唆を提供できる。セキュリティチェックが不合格であった場合、セキュリティチェック処理を終了しうる。

【０１０２】

いくつかの実施形態において、第２セキュリティ検証コードおよび第２タイムスタンプは、第２端末識別子に従って取得されたセキュリティ検証コードおよびタイムスタンプと同じであるが、第２タイムスタンプが現在のセキュリティチェックの期限内でないと、サーバが判定した場合、セキュリティチェックは不合格になる。例えば、セキュリティチェックは、第２セキュリティ検証コードおよび第２タイムスタンプが、閾値期限内に第２端末識別子に従って取得されたセキュリティ検証コードおよびタイムスタンプと同じであると判定されない場合には、タイムアウト（例えば、失効）しうる。

【０１０３】

セキュリティチェック合格の場合、工程４４２において、サーバ４０２は、セキュリティチェック合格情報を端末へ送信する。セキュリティチェック合格情報は、端末がセキュリティチェックを合格したことを示しうる。セキュリティチェック不合格の場合、セキュリティチェック処理は終了しうる。

【０１０４】

上述の例からわかるように、二次元検証コードは、セキュリティチェック中に検証情報を送信するために利用できる。二次元検証コードは、書かれた数字を含むテキストメッセージを通して実施されるセキュリティチェックを用いる或る関連技術よりも豊富かつ信頼性の高い確認情報を伝えることができる。様々な実施形態によれば、確認情報は、盗んで利用することが難しいため、インターネットアプリケーションのアクセスセキュリティを強化する。いくつかの実施形態において、二次元検証コードは、インターネットトラフィックを介して送信されるため、検証コードがテキストメッセージを介して送信される場合に生じる通信費が避けられる。結果として、様々な実施形態において、セキュリティチェックの実行に必要なモバイル通信リソースがの削減が実現する。いくつかの実施形態によれば、端末が二次元検証コードを認識したことに応答して、その端末は、認識情報をサーバへ自動的に送り返すことができる。したがって、様々な実施形態に従ったセキュリティチェック処理は、ユーザによる手入力を必要とせず、手動での確認情報の不正の可能性を避ける。さらに、端末が端末識別子を確認することによってセキュリティチェック処理における第１再検証を実施できるので、セキュリティチェックの効率が効果的に高められる

。
【０１０５】
図５は、本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図である。
【０１０６】
図５を参照すると、セキュリティチェックを実行するためのデバイス５００が提供されている。いくつかの実施形態において、デバイス５００は、図２の処理２００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス５００は、図３の処理３００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス５００は、図４の処理４００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス５００は、図１０の端末１０００によって実装されうる。いくつかの実施形態において、デバイス５００は、図１１のシステム１１００によって実装されうる。
【０１０７】
いくつかの実施形態において、デバイス５００は、サーバに実装されうる。デバイス５００は、受信モジュール５１０、取得モジュール５２０、生成モジュール５３０、送信モジュール５４０、および、確認モジュール５５０を備えてよい。
【０１０８】
受信モジュール５１０は、端末から送信されたセキュリティ検証要求を受信するよう構成されうる。
【０１０９】
取得モジュール５２０は、受信モジュール５１０によって受信されたセキュリティ検証要求に従って第１検証要素情報を取得するよう構成されうる。
【０１１０】
生成モジュール５３０は、取得モジュール５２０によって取得された第１検証要素情報を用いて、デジタルオブジェクト固有識別子を生成するよう構成されうる。
【０１１１】
送信モジュール５４０は、生成モジュール５３０によって生成されたデジタルオブジェクト固有識別子を送信するよう構成されうる。送信モジュール５４０は、デジタルオブジェクト固有識別子を端末に送信できる。
【０１１２】
受信モジュール５１０は、さらに、端末によって送信された第２検証要素情報を受信するよう構成されうる。第２検証要素情報は、送信モジュール５４０によって送信されたデジタルオブジェクト固有識別子を用いて端末によって取得された検証要素情報に対応しうる。
【０１１３】
確認モジュール５５０は、セキュリティチェックの結果を送信するよう構成されうる。例えば、取得モジュール５２０によって取得された第１検証要素情報および受信ユニットによって受信された第２検証要素情報が合致（例えば、一致）することを確認すると、確認モジュール５５０は、セキュリティチェック合格情報を端末に送り返すことができる。
【０１１４】
図６は、本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図である。
【０１１５】
図６を参照すると、セキュリティチェックを実行するためのデバイス６００が提供されている。いくつかの実施形態において、デバイス６００は、図２の処理２００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス６００は、図３の処理３００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス６００は、図４の処理４００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス６００は、図１０の端末１０００によって実装されうる。いくつかの実施形態において、デバイス６００は、図１１のシステム１１００によって実装されうる。

【０１１６】
いくつかの実施形態において、デバイス６００は、サーバに実装されうる。デバイス６００は、保存モジュール６１０、受信モジュール６２０、取得モジュール６３０、生成モジュール６４０、送信モジュール６５０、および、確認モジュール６６０を備えてよい。
【０１１７】
保存モジュール６１０は、ユーザ識別子と端末識別子との間の対応関係を格納するよう構成されうる。保存モジュール６１０は、テーブル、データベースなどに対応関係を格納できる。保存モジュール６１０は、ユーザが、ユーザ名を登録するかまたは既存のユーザ名に対応する記録の登録を変更するかした場合に、対応関係を更新できる。
【０１１８】
受信モジュール６２０は、端末から送信されたセキュリティ検証要求を受信するよう構成されうる。
【０１１９】
取得モジュール６３０は、識別子検索サブモジュール６３０および情報生成サブモジュール６３２を備えてよい。
【０１２０】
識別子検索サブモジュール６３１は、端末に関連するユーザ名を用いて、保存モジュール６１０によって保存された対応関係を検索し、端末のユーザ名に関連する端末に対応する第１端末識別子を取得するよう構成されうる。端末に関連するユーザ名は、受信モジュール６２０によって受信されたセキュリティ検証要求で伝えられうる。
【０１２１】
情報生成サブモジュール６３２は、第１セキュリティ検証コードおよび第１タイムスタンプを生成するよう構成されうる。情報生成サブモジュール６３２は、受信モジュール６２０によって受信されたセキュリティ検証要求に関連して、第１セキュリティ検証コードおよび第１タイムスタンプを生成できる。第１タイムスタンプは、現在のセキュリティチェックの期限を示すことができる。第１検証要素情報は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを含みうる。
【０１２２】
保存モジュール６１０は、さらに、識別子検索サブモジュール６３１によって取得された第１端末識別子と、情報生成サブモジュール６３２によって生成された第１セキュリティ検証コードおよび第１タイムスタンプとの間の関係性を保存するよう構成されうる。
【０１２３】
生成モジュール６４０は、文字列生成サブモジュール６４１および識別子生成サブモジュール６４２を備えてよい。
【０１２４】
文字列生成サブモジュール６４１は、第１組み合わせ文字列を生成するよう構成されうる。文字列生成サブモジュール６４１は、識別子検索サブモジュール６３１によって取得された第１端末識別子ならびに情報生成サブモジュール６３２によって生成された第１セキュリティ検証コードおよび第１タイムスタンプを組み合わせることによって、第１組み合わせ文字列を生成するよう構成されうる。
【０１２５】
識別子生成サブモジュール６４２は、文字列生成サブモジュール６４１によって生成された第１組み合わせ文字列を用いて、デジタルオブジェクト固有識別子を生成するよう構成されうる。
【０１２６】
送信モジュール６５０は、識別子生成サブモジュール６４２によって生成されたデジタルオブジェクト固有識別子を端末に送信するよう構成されうる。
【０１２７】
受信モジュール６２０は、さらに、端末によって送信された第２検証要素情報を受信するよう構成されうる。第２検証要素情報は、送信モジュール６５０によって送信されたデ

ジタルオブジェクト固有識別子を用いて端末によって取得された検証要素情報に対応しうる。受信ユニット６２０によって受信された第２検証要素情報は、第２組み合わせ文字列を分解することによって取得された第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含みうる。第２組み合わせ文字列は、デジタルオブジェクト固有識別子をスキャンすることにより端末によって取得されうる。端末は、第２端末識別を端末の端末識別子と比較して、第２端末識別子が端末の端末識別子とマッチする（例えば、同じである）と判定した場合に、第２検証要素情報を送り返すことができる。

【０１２８】

確認モジュール６６０は、情報検索サブモジュール６６１および確認実行サブモジュール６６２を備えてよい。

【０１２９】

情報検索サブモジュール６６１は、保存モジュール６１０によって保存された関係性（例えば、関係性の記録）を検索し、受信モジュール６２０によって受信された第２検証要素情報内の第２端末識別子にそれぞれ対応するセキュリティ検証コードおよびタイムスタンプを取得するよう構成されうる。

【０１３０】

確認実行サブモジュール６６２は、セキュリティチェック結果の結果の示唆を送信するよう構成されうる。確認実行サブモジュール６６２は、第２セキュリティ検証コードおよび情報検索サブモジュール６６１によって取得されたセキュリティ検証コードがマッチする（例えば、同じである）か否か、第２タイムスタンプおよび情報検索サブモジュール６６１によって取得されたタイムスタンプがマッチする（例えば、同じである）か否か、ならびに、第２タイムスタンプが現在のセキュリティチェックの期限内にあるか否かを判定できる。確認実行サブモジュール６６２は、第２セキュリティ検証コードおよび情報検索サブモジュール６６１によって取得されたセキュリティ検証コードがマッチし（例えば、同一であり）、第２タイムスタンプおよび情報検索サブモジュール６６１によって取得されたタイムスタンプがマッチし（例えば、同じであり）、第２タイムスタンプが現在のセキュリティチェックの期限内にあると判定した場合、セキュリティチェック合格情報を端末に送り返す。

【０１３１】

いくつかの実施形態において、識別子生成サブモジュール６４２は、文字列生成サブモジュール６４１によって生成された第１組み合わせ文字列を暗号化して、暗号化文字列を生成し、暗号化文字列をｂａｓｅ６４文字列に変換するよう構成される。識別子生成サブモジュール６４２は、ＱＲ符号化ルールに従ってｂａｓｅ６４文字列を符号化し、デジタルオブジェクト固有識別子に対応する二次元検証コードを生成するよう構成されうる。

【０１３２】

図７は、本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図である。

【０１３３】

図７を参照すると、セキュリティチェックを実行するためのデバイス７００が提供されている。いくつかの実施形態において、デバイス７００は、図２の処理２００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス７００は、図３の処理３００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス７００は、図４の処理４００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス７００は、図１０の端末１０００によって実装されうる。いくつかの実施形態において、デバイス７００は、図１１のシステム１１００によって実装されうる。

【０１３４】

デバイス７００は、端末に実装されうる。デバイス７００は、送信モジュール７１０、受信モジュール７２０、取得モジュール７３０、および、確認モジュール７４０を備えてよい。

【０１３５】

送信モジュール７１０は、セキュリティ検証要求をサーバに送信するよう構成されうる。

【０１３６】

受信モジュール７２０は、サーバによって送信されたデジタルオブジェクト固有識別子を受信するよう構成されうる。デジタルオブジェクト固有識別子は、送信モジュール７１０によって送信されたセキュリティ検証要求に従ってサーバが第１検証要素情報を取得した後に、第１検証要素情報に従って（例えば、少なくとも部分的に基づいて）生成された固有識別子でありうる。

【０１３７】

取得モジュール７３０は、受信ユニット７２０によって受信されたデジタルオブジェクト固有識別子を用いて第２検証要素情報を取得するよう構成されうる。

【０１３８】

送信モジュール７１０は、さらに、取得モジュール７３０によって取得された第２検証要素情報をサーバへ送信するよう構成されうる。

【０１３９】

確認モジュール７４０は、セキュリティチェックの結果を受信するよう構成されうる。確認モジュール７４０は、サーバによって送信されたセキュリティチェック合格情報を受信できる。サーバは、第１検証要素情報および送信モジュール７１０によって送信された第２検証要素情報が合致することを確認すると、セキュリティチェック合格情報を送信できる。

【０１４０】

図８は、本願の本開示の様々な実施形態に従って、セキュリティ検証デバイスを示すブロック図である。

【０１４１】

図８を参照すると、セキュリティチェックを実行するためのデバイス８００が提供されている。いくつかの実施形態において、デバイス８００は、図２の処理２００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス８００は、図３の処理３００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス８００は、図４の処理４００の一部またはすべてを実施できる。いくつかの実施形態において、デバイス８００は、図１０の端末１０００によって実装されうる。いくつかの実施形態において、デバイス８００は、図１１のシステム１１００によって実装されうる。

【０１４２】

デバイス８００は、端末に実装されうる。デバイス８００は、送信モジュール８１０、受信モジュール８２０、取得モジュール８３０、比較モジュール８４０　および、確認モジュール８５０を備えてよい。

【０１４３】

送信モジュール８１０は、セキュリティ検証要求をサーバに送信するよう構成されうる。

【０１４４】

受信モジュール８２０は、サーバによって送信されたデジタルオブジェクト固有識別子を受信するよう構成されうる。デジタルオブジェクト固有識別子は、送信モジュール８１０によって送信されたセキュリティ検証要求に従ってサーバが第１検証要素情報を取得した後に、第１検証要素情報に従って（例えば、少なくとも部分的に基づいて）生成された固有識別子に対応しうる。

【０１４５】

取得モジュール８３０は、識別子スキャンサブモジュール８３１および文字列分解サブモジュール８３２を備えてよい。

【０１４６】

識別子スキャンサブモジュール８３１は、受信モジュール８２０によって受信されたデジタルオブジェクト固有識別子をスキャンすることによって第２組み合わせ文字列を取得

できる。デジタルオブジェクト固有識別子は、第１組み合わせ文字列から生成されたデジタルオブジェクト固有識別子に対応しうる。第１組み合わせ文字列は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることによりサーバによって生成されうる。第１検証要素情報は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを含みうる。第１端末識別子は、端末の端末識別子に対応しうる。第１端末識別子は、セキュリティ検証要求で伝えられた端末ユーザ名に従って取得されうる。第１セキュリティ検証コードおよび第１タイムスタンプは、セキュリティ検証要求に関連してサーバによって生成されたセキュリティ検証コードおよびタイムスタンプにそれぞれ対応しうる。

【０１４７】

文字列分解サブモジュール８３２は、識別子スキャンサブモジュール８３１によって取得された第２組み合わせ文字列を分解するよう構成されうる。文字列分解サブモジュール８３２は、第２組み合わせ文字列を分解することによって第２検証要素情報を取得するよう構成されうる。第２検証要素情報は、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含みうる。

【０１４８】

比較モジュール８４０は、文字列分解サブモジュール８３２によって取得された第２端末識別子と、端末の端末識別子とを比較するよう構成されうる。

【０１４９】

送信モジュール８１０は、さらに、第２検証要素情報をサーバに送信するよう構成されうる。例えば、送信モジュールは、第２端末識別子および端末の端末識別子がマッチする（例えば、同じである）ことを比較モジュール８４０からの比較結果が示す場合に、第２検証要素情報をサーバに送信できる。

【０１５０】

確認モジュール８５０は、セキュリティチェックの結果を受信するよう構成されうる。確認モジュール８５０は、サーバによって送信されたセキュリティチェック合格情報を受信できる。サーバは、第１検証要素情報および送信モジュール８１０によって送信された第２検証要素情報が合致することを確認すると、セキュリティチェック合格情報を送信できる。

【０１５１】

いくつかの実施形態において、識別子スキャンサブモジュール８３１は、ＱＲ復号ルールに従って、デジタルオブジェクト固有識別子に対応し、受信ユニット８２０によって受信された二次元検証コードを復号するよう構成されうる。識別子スキャンサブモジュール８３１は、さらに、ｂａｓｅ６４文字列を生成し、ｂａｓｅ６４文字列を暗号化文字列に変換し、暗号化文字列を復号して第２組み合わせ文字列を取得するよう構成されうる。

【０１５２】

図５～図８に関連して上述したモジュールは、物理的に分離していても分離していなくてもよい別個の構成要素であってよい。モジュールは、１つの場所に配置されてもよいし、複数のネットワークユニットにわたって分散されてもよい。本願のスキームは、実際のニーズに従って、モジュールの一部または全部を選択することによって実現されうる。

【０１５３】

図９は、本願の本開示の様々な実施形態に従って、サーバの一実施形態を示すブロック図である。

【０１５４】

図９を参照すると、セキュリティチェックを実行するためのサーバ９００が提供されている。いくつかの実施形態において、サーバ９００は、図２の処理２００の一部またはすべてを実施できる。いくつかの実施形態において、サーバ９００は、図３の処理３００の一部またはすべてを実施できる。いくつかの実施形態において、サーバ９００は、図４の処理４００の一部またはすべてを実施できる。いくつかの実施形態において、サーバ９００は、図１０の端末１０００によって実装されうる。いくつかの実施形態において、サー

バ９００は、図１１のシステム１１００によって実装されうる。
【０１５５】
サーバ９００は、プロセッサ９１０と、プロセッサ９１０によって実行可能なコマンドを格納するためのストレージデバイス９２０と、入出力インターフェース（図示せず）と、インターネットインターフェース（図示せず）と、様々なハードウエア（図示せず）と、を備えてよい。
【０１５６】
プロセッサ９１０は、端末から送信されたセキュリティ検証要求を受信し、セキュリティ検証要求に従って第１検証要素情報を取得し、第１検証要素情報を用いてデジタルオブジェクト固有識別子を生成し、デジタルオブジェクト固有識別子を端末に送信し、端末によって送信された第２検証要素情報を受信するよう構成されうる。第２検証要素情報は、デジタルオブジェクト固有識別子を通して（例えば、用いて）端末によって取得された検証要素情報に対応しうる。
【０１５７】
いくつかの実施形態において、プロセッサ９１０は、セキュリティチェック結果の結果の示唆を送信するよう構成されうる。プロセッサ９１０は、第１検証要素情報および第２検証要素情報が合致するか（例えば、マッチするか）否かを判定できる。プロセッサ９１０は、第１検証要素情報および第２検証要素情報が合致する（例えば、マッチする）と判定した場合に、セキュリティチェック合格情報を端末に送信する。
【０１５８】
ストレージデバイス９２０は、ユーザ識別子と端末識別子との間の対応関係を格納できる。ストレージデバイス９２０は、ユーザ識別子および端末識別子の間の対応関係を、テーブル、データベースなど、または、それらの任意の組み合わせに格納できる。ストレージデバイス９２０は、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプの間の関係性を格納できる。
【０１５９】
図１０は、本願の本開示の様々な実施形態に従って、端末を示すブロック図である。
【０１６０】
図１０を参照すると、セキュリティチェックを実行するための端末１０００が提供されている。いくつかの実施形態において、端末１０００は、図２の処理２００の一部またはすべてを実施できる。いくつかの実施形態において、端末１０００は、図３の処理３００の一部またはすべてを実施できる。いくつかの実施形態において、端末１０００は、図４の処理４００の一部またはすべてを実施できる。いくつかの実施形態において、端末１０００は、図１１のシステム１１００によって実装されうる。
【０１６１】
端末１０００は、プロセッサ１０１０と、プロセッサ１０１０によって実行可能なコマンドを格納するストレージデバイス１０２０と、入出力インターフェース（図示せず）と、インターネットインターフェース（図示せず）と、様々なハードウエア（図示せず）と、を備えてよい。
【０１６２】
プロセッサ１０１０は、セキュリティ検証要求をサーバに送信するよう構成されうる。プロセッサ１０１０は、さらに、サーバによって送り返されたデジタルオブジェクト固有識別子を受信するよう構成されうる。デジタルオブジェクト固有識別子は、サーバがセキュリティ検証要求に従って第１検証要素情報を取得した後に、第１検証要素情報に従って生成される固有識別子に対応しうる。プロセッサ１０１０は、さらに、デジタルオブジェクト固有識別子を通して第２検証要素情報を取得するよう構成されうる。プロセッサ１０１０は、さらに、第２検証要素情報をサーバに送信するよう構成されうる。
【０１６３】
いくつかの実施形態において、プロセッサ１０１０は、セキュリティチェックの結果を受信するよう構成されうる。プロセッサ１０１０は、サーバによって送信されたセキュリ

ティチェック合格情報を受信できる。サーバは、第１検証要素情報および第２検証要素情報が合致することを確認すると、セキュリティチェック合格情報を送信できる。

【０１６４】

ストレージデバイス１０２０は、識別子を格納できる。例えば、識別子は、ユーザ名、端末識別子など、または、それらの任意の組み合わせに対応しうる。

【０１６５】

デジタルオブジェクト固有識別子は、セキュリティチェック中に検証情報を送信するために利用できる。デジタルオブジェクト固有識別子に関連して、書かれた数字を含むテキストメッセージを実施する或る連技術に従ったセキュリティチェックよりも豊富かつ信頼性の高い確認情報が送信されうる。いくつかの実施形態では、デジタルオブジェクト固有識別子に関連して送信される確認情報は、盗んで利用することが比較的困難である。したがって、書かれた数字の通信に関連したテキストメッセージではなく、確認情報の通信にデジタルオブジェクト固有識別子を用いることによって、インターネットアプリケーションのアクセスセキュリティを強化できる。様々な実施形態によれば、デジタルオブジェクト固有識別子は、インターネットトラフィックを介して送信されるため、検証コードがテキストメッセージを介して送信される場合に生じる通信費が避けられる。結果として、様々な実施形態において、セキュリティチェックの実行に必要なモバイル通信リソースがの削減が実現する。いくつかの実施形態によれば、端末は、デジタルオブジェクト固有識別子またはデジタルオブジェクト固有識別子に含まれる情報を認識したことに応答して、認識情報をサーバへ自動的に送り返すことができる。したがって、様々な実施形態に従ったセキュリティチェック処理は、ユーザによる手入力を必要とせず、手動での確認情報の不正の可能性を避ける。さらに、端末が端末識別子を確認することによってセキュリティチェック処理における第１再検証を実施できるので、セキュリティチェックの効率が効果的に高められる。

【０１６６】

図１１は、本開示の様々な実施形態に従って、セキュリティを提供するためのシステムを示す構造ブロック図である。

【０１６７】

図１１を参照すると、セキュリティを提供するためのシステム１１００が提供されている。いくつかの実施形態において、システム１１００は、図２の処理２００の一部またはすべてを実施できる。いくつかの実施形態において、システム１１００は、図３の処理３００の一部またはすべてを実施できる。いくつかの実施形態において、システム１１００は、図４の処理４００の一部またはすべてを実施できる。いくつかの実施形態では、図５のデバイス５００が、システム１１００によって実装されうる。いくつかの実施形態では、図６のデバイス６００が、システム１１００によって実装されうる。いくつかの実施形態では、図７のデバイス７００が、システム１１００によって実装されうる。いくつかの実施形態では、図８のデバイス８００が、システム１１００によって実装されうる。いくつかの実施形態では、図９のサーバ９００が、システム１１００によって実装されうる。いくつかの実施形態では、図１０の端末１０００が、システム１１００によって実装されうる。

【０１６８】

セキュリティチェックを提供するためのシステム１１００は、端末１１１０およびサーバ１１２０を備える。システム１１００は、端末１１１０およびサーバ１１２０が通信するネットワーク１１３０を備えてよい。端末１１１０からセキュリティ検証要求を受信したことに応答して、サーバ１１２０は、端末１１１０（例えば、端末１１１０を用いるまたは他の方法で端末１１１０に関連するユーザ）のセキュリティチェックを提供できる。

【０１６９】

図１２は、本開示の様々な実施形態に従って、セキュリティを提供するためのコンピュータシステムを示す機能図である。

【０１７０】

図１２を参照すると、セキュリティを提供するためのコンピュータシステム１２００が提供されている。明らかに、セキュリティを提供するために、他のコンピュータシステムアーキテクチャおよび構成を用いることも可能である。以下に述べるような様々なサブシステムを備えるコンピュータシステム１２００は、少なくとも１つのマイクロプロセッササブシステム（プロセッサまたは中央処理装置（ＣＰＵ）とも呼ばれる）１２０２を備える。例えば、プロセッサ１２０２は、シングルチッププロセッサまたはマルチプロセッサによって実装できる。いくつかの実施形態において、プロセッサ１２０２は、コンピュータシステム１２００の動作を制御する汎用デジタルプロセッサである。メモリ１２１０から読み出された命令を用いて、プロセッサ１２０２は、入力データの受信および操作、ならびに、出力デバイス（例えば、ディスプレイ１２１８）上でのデータの出力および表示を制御する。

【０１７１】

プロセッサ１２０２は、メモリ１２１０と双方向的に接続されており、メモリ１２１０は、第１のプライマリストレージ（通例は、ランダムアクセスメモリ（ＲＡＭ））および第２のプライマリストレージ領域（通例は、読み出し専用メモリ（ＲＯＭ））を含みうる。当業者に周知のように、プライマリストレージは、一般的な記憶領域として、および、スクラッチパッドメモリとして利用可能であり、また、入力データおよび処理済みデータを格納するために利用可能である。プライマリストレージは、さらに、プロセッサ１２０２上で実行される処理のための他のデータおよび命令に加えて、データオブジェクトおよびテキストオブジェクトの形態で、プログラミング命令およびデータを格納できる。また、当業者に周知のように、プライマリストレージは、通例、機能（例えば、プログラムされた命令）を実行するためにプロセッサ１２０２によって用いられる基本的な動作命令、プログラムコード、データ、および、オブジェクトを備える。例えば、メモリ１２１０は、例えば、データアクセスが双方向である必要があるか、単方向である必要があるかに応じて、後述する任意の適切なコンピュータ読み取り可能な記憶媒体を含みうる。例えば、プロセッサ１２０２は、頻繁に必要になるデータをキャッシュメモリ（図示せず）に直接的かつ非常に迅速に格納し取り出すことができる。メモリは、持続性のコンピュータ読み取り可能な記憶媒体であってよい。

【０１７２】

着脱可能マスストレージデバイス１２１２が、コンピュータシステム１２００にさらなるデータ記憶容量を提供しており、プロセッサ１２０２に対して双方向（読み出し／書き込み）または単方向（読み出しのみ）に接続されている。例えば、ストレージ１２１２は、磁気テープ、フラッシュメモリ、ＰＣカード、携帯型マスストレージデバイス、ホログラフィックストレージデバイス、および、その他のストレージデバイスなどのコンピュータ読み取り可能な媒体も含みうる。固定マスストレージ１２２０も、例えば、さらなるデータ記憶容量を提供しうる。マスストレージ１２２０の最も一般的な例は、ハードディスクドライブである。マスストレージデバイス１２１２および固定マスストレージ１２２０は、一般に、プロセッサ１２０２によって通例はあまり利用されないさらなるプログラミング命令、データなどを格納する。マスストレージデバイス１２１２および固定マスストレージ１２２０に保持された情報は、必要であれば、仮想メモリとしてのメモリ１２１０（例えば、ＲＡＭ）の一部に標準的な方式で組み込まれうることが理解される。

【０１７３】

プロセッサ１２０２がストレージサブシステムにアクセスできるようにすることに加えて、バス１２１４が、その他のサブシステムおよびデバイスへのアクセスを可能にするために用いられてもよい。図に示すように、これらは、ディスプレイモニタ１２１８、ネットワークインターフェース１２１６、キーボード１２０４、および、ポインティングデバイス１２０６、ならびに、必要に応じて、補助入力／出力デバイスインターフェース、サウンドカード、スピーカ、および、その他のサブシステムを含みうる。例えば、ポインティングデバイス１２０６は、マウス、スタイラス、トラックボール、または、タブレットであってよく、グラフィカルユーザインターフェースと相互作用するのに有用である。

【０１７４】
ネットワークインターフェース１２１６は、図に示すように、ネットワーク接続を用いて、別のコンピュータ、コンピュータネットワーク、または、遠隔通信ネットワークにプロセッサ１２０２を接続することを可能にする。例えば、ネットワークインターフェース１２１６を通して、プロセッサ１２０２は、方法／処理ステップを実行する過程で、別のネットワークから情報（例えば、データオブジェクトまたはプログラム命令）を受信したり、別のネットワークに情報を出力したりすることができる。情報は、しばしば、プロセッサ上で実行される一連の命令として表され、別のネットワークから受信されたり、別のネットワークへ出力されたりしうる。インターフェースカード（または同様のデバイス）と、プロセッサ１２０２によって実装（例えば、実行／実施）される適切なソフトウェアとを用いて、コンピュータシステム１２００を外部ネットワークに接続し、標準プロトコルに従ってデータを転送することができる。例えば、本明細書に開示された様々な処理の実施形態は、プロセッサ１２０２上で実行されてもよいし、処理の一部を共有するリモートプロセッサと共に、ネットワーク（インターネット、イントラネットワーク、または、ローカルエリアネットワークなど）上で実行されてもよい。さらなるマスストレージデバイス（図示せず）が、ネットワークインターフェース１２１６を通してプロセッサ１２０２に接続されてもよい。
【０１７５】
補助Ｉ／Ｏデバイスインターフェース（図示せず）が、コンピュータシステム１２００と共に用いられてよい。補助Ｉ／Ｏデバイスインターフェースは、プロセッサ１２０２がデータを送信すること、ならびに、より典型的には、他のデバイス（マイクロフォン、タッチセンサ方式ディスプレイ、トランスデューサカードリーダ、テープリーダ、音声または手書き認識装置、バイオメトリクスリーダ、カメラ、携帯型マスストレージデバイス、および、他のコンピュータなど）からデータを受信することを可能にする汎用インターフェースおよびカスタマイズされたインターフェースを含みうる。
【０１７６】
図１２に示したコンピュータシステムは、本明細書に開示された様々な実施形態と共に利用するのに適切なコンピュータシステムの一例にすぎない。かかる利用に適した他のコンピュータシステムは、より多いまたは少ないサブシステムを含みうる。さらに、バス１２１４は、サブシステムをつなぐよう機能する任意の相互接続スキームの例である。異なる構成のサブシステムを有する他のコンピュータアーキテクチャが利用されてもよい。
【０１７７】
以上は、本願の実施形態にすぎず、本願を限定することはない。当業者にとって、本願は、様々な変形例および変更例を有しうる。本願の精神および原理の範囲内でなされた任意の変形、等価的な置換、または、改良はすべて、本願の請求項の範囲内に含まれる。
【０１７８】
上述の実施形態は、理解しやすいようにいくぶん詳しく説明されているが、本発明は、提供された詳細事項に限定されるものではない。本発明を実施する多くの代替方法が存在する。開示された実施形態は、例示であり、限定を意図するものではない。
適用例１：方法であって、
端末から送信されたセキュリティ検証要求を受信し、
前記セキュリティ検証要求に少なくとも部分的に基づいて、第１検証要素情報を取得し、
前記第１検証要素情報に少なくとも部分的に基づいて、デジタルオブジェクト固有識別子を生成し、
前記デジタルオブジェクト固有識別子を前記端末に送信し、
第２検証要素情報を前記端末から受信し、
前記第１検証要素情報および前記第２検証要素情報が一致する場合に、セキュリティチェック合格情報を前記端末に送信すること、
を備える、方法。

適用例２：適用例１に記載の方法であって、前記第２検証要素情報は、前記端末によって前記デジタルオブジェクト固有識別子から取得された前記第１検証要素情報に対応する、方法。
適用例３：適用例１に記載の方法であって、前記端末は、前記デジタルオブジェクト固有識別子を処理することによって、前記第２検証要素情報を取得する、方法。
適用例４：適用例１に記載の方法であって、さらに、
前記第１検証要素情報および前記第２検証要素情報が一致するか否かを判定する工程を備える、方法。
適用例５：適用例１に記載の方法であって、さらに、
ユーザ名と端末識別子との間の対応関係を格納することを備え、
前記セキュリティ検証要求に少なくとも部分的に基づいて、前記第１検証要素情報を取得すること、
前記セキュリティ検証要求に含まれる前記端末のユーザ名を用いて、ユーザ名と端末識別子との間の前記対応関係を検索して、前記端末に関連づけられている第１端末識別子を取得し、
前記セキュリティ検証要求に関連する第１セキュリティ検証コードと、前記セキュリティ検証要求に関連する第１タイムスタンプとを生成し、前記第１タイムスタンプは、現在のセキュリティチェックの期限を示し、前記第１検証要素情報は、前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含むこと、
を備える、方法。
適用例６：適用例５に記載の方法であって、前記第１検証要素情報に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成することは、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを組み合わせることによって、第１組み合わせ文字列を生成し、
前記第１組み合わせ文字列に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成すること、
を備える、方法。
適用例７：適用例６に記載の方法であって、前記第１組み合わせ文字列に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成することは、
前記第１組み合わせ文字列を暗号化することに少なくとも部分的に基づいて、暗号化文字列を生成し、
前記暗号化文字列をｂａｓｅ６４文字列に変換し、
クイックレスポンス（ＱＲ）符号化ルールに従って、前記ｂａｓｅ６４文字列を符号化し、
前記デジタルオブジェクト固有識別子に対応する二次元検証コードを生成すること、
を備える、方法。
適用例８：適用例５に記載の方法であって、さらに、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプの間の関係性を保存することを備え、
前記第２検証要素情報は、第２組み合わせ文字列を分解することによって取得された第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含み、前記第２組み合わせ文字列は、前記端末が前記デジタルオブジェクト固有識別子をスキャンすることによって取得され、前記第２検証要素情報は、前記端末が前記第２端末識別子を前記端末の前記第１端末識別子と比較して、前記第２端末識別子および前記端末の前記第１端末識別子が同じであると判定した場合に、前記端末から送信された情報に対応し、
前記セキュリティチェック合格情報を前記端末に送信することは、
前記第２端末識別子に少なくとも部分的に基づいて、複数の第１端末識別子、複数の第１セキュリティ検証コード、および、複数の第１タイムスタンプの間の複数の関係性を検索して、前記第２端末識別子にそれぞれ対応する前記セキュリティ検証コードおよび前記タイムスタンプを取得し、

前記第２セキュリティ検証コードおよび前記取得されたセキュリティ検証コードが一致し、前記第２タイムスタンプおよび前記取得されたタイムスタンプが一致し、前記第２タイムスタンプが前記セキュリティ検証要求に関連する現在のセキュリティチェックの期限内にある場合に、セキュリティチェック合格情報を前記端末に送信すること、
を備える、方法。
適用例９：方法であって、
端末によってセキュリティ検証要求をサーバに送信し、
前記端末によってデジタルオブジェクト固有識別子を前記サーバから受信し、前記デジタルオブジェクト固有識別子は、前記サーバが前記セキュリティ検証要求に少なくとも部分的に基づいて取得した第１検証要素情報に少なくとも部分的に基づいて生成された固有識別子に対応し、
前記端末によって前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて第２検証要素情報を取得し、
前記端末によって前記第２検証要素情報を前記サーバに送信し、
前記第１検証要素情報および前記第２検証要素情報が一致する場合に、セキュリティチェック合格情報を前記サーバから受信すること、
を備える、方法。
適用例１０：適用例９に記載の方法であって、前記第２検証要素情報を取得することは、前記デジタルオブジェクト固有識別子を処理しと、前記デジタルオブジェクト固有識別子の前記処理に少なくとも部分的に基づいて前記第２検証要素情報を取得すること、を備える、方法。
適用例１１：適用例９に記載の方法であって、さらに、
前記第１検証要素情報の少なくとも一部および前記第２検証要素情報の少なくとも一部が一致するか否かを判定することを備える、方法。
適用例１２：適用例９に記載の方法であって、前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて前記第２検証要素情報を取得することは、
前記デジタルオブジェクト固有識別子をスキャンし、
前記デジタルオブジェクト固有識別子の前記スキャンに少なくとも部分的に基づいて第２組み合わせ文字列を取得し、前記デジタルオブジェクト固有識別子は、第１組み合わせ文字列に少なくとも部分的に基づいて生成され、前記第１組み合わせ文字列は、前記サーバが、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることによって生成され、前記第１検証要素情報は、前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含み、前記第１端末識別子は、前記端末のユーザ名に少なくとも部分的に基づいて取得された前記端末の端末識別子に対応し、前記端末の前記ユーザ名は、前記セキュリティ検証要求に含まれ、前記第１セキュリティチェックおよび前記第１タイムスタンプは、前記セキュリティ検証要求に関連して前記サーバによって生成された前記第１セキュリティ検証コードおよび前記第１タイムスタンプに対応し、
前記第２組み合わせ文字列を分解し、
前記第２組み合わせ文字列の前記分解に少なくとも部分的に基づいて、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含む前記第２検証要素情報を取得すること、
を備える、方法。
適用例１３：適用例１２に記載の方法であって、前記デジタルオブジェクト固有識別子の前記スキャンに少なくとも部分的に基づいて前記第２組み合わせ文字列を取得することは、
クイックレスポンス（ＱＲ）復号ルールを用いて、前記デジタルオブジェクト固有識別子に対応する二次元検証コードを復号し、
前記二次元検証コードの前記復号に少なくとも部分的に基づいてｂａｓｅ６４文字列を生成し、

前記ｂａｓｅ６４文字列を暗号化文字列に変換し、
前記暗号化文字列を復号することに少なくとも部分的に基づいて前記第２組み合わせ文字列を取得すること、
を備える、方法。
適用例１４：適用例１２に記載の方法であって、さらに、
前記第２検証要素情報が前記サーバに送信される前に、前記第２端末識別子および前記端末の端末識別子を比較し、
前記第２端末識別子および前記端末の前記端末識別子がマッチする場合に、前記第２検証要素情報を前記サーバに送信する工程を実行すること、
を備える、方法。
適用例１５：セキュリティチェックデバイスであって、
少なくとも１つのプロセッサであって、
端末から送信されたセキュリティ検証要求を受信し、
前記セキュリティ検証要求に少なくとも部分的に基づいて、第１検証要素情報を取得し、
前記第１検証要素情報に少なくとも部分的に基づいて、デジタルオブジェクト固有識別子を生成し、
前記デジタルオブジェクト固有識別子を前記端末に送信し、
第２検証要素情報を前記端末から受信し、
前記第１検証要素情報および前記第２検証要素情報が一致する場合に、セキュリティチェック合格情報を前記端末に送信するよう構成されている、少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサに接続され、前記少なくとも１つのプロセッサに命令を提供するよう構成されているメモリと、
を備える、デバイス。
適用例１６：適用例１５に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
ユーザ名と端末識別子との間の対応関係を格納するよう構成されており、
前記少なくとも１つのプロセッサによって、前記セキュリティ検証要求に少なくとも部分的に基づいて、前記第１検証要素情報を取得することは、
前記セキュリティ検証要求に含まれる前記端末のユーザ名を用いて、ユーザ名と端末識別子との間の前記対応関係を検索して、前記端末に関連づけられている第１端末識別子を取得し、
前記セキュリティ検証要求に関連する第１セキュリティ検証コードと、前記セキュリティ検証要求に関連する第１タイムスタンプとを生成すること、
を備え、
前記第１タイムスタンプは、現在のセキュリティチェックの期限を示し、前記第１検証要素情報は、前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含む、デバイス。
適用例１７：適用例１６に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを組み合わせることによって、第１組み合わせ文字列を生成し、
前記第１組み合わせ文字列に少なくとも部分的に基づいて、前記デジタルオブジェクト固有識別子を生成するよう構成されている、デバイス。
適用例１８：適用例１７に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記第１組み合わせ文字列を暗号化することに少なくとも部分的に基づいて、暗号化文字列を生成し、
前記暗号化文字列をｂａｓｅ６４文字列に変換し、

クイックレスポンス（ＱＲ）符号化ルールに従って、前記ｂａｓｅ６４文字列を符号化し、
前記デジタルオブジェクト固有識別子に対応する二次元検証コードを生成するよう構成されている、デバイス。
適用例１９：適用例１６に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプの間の関係性を保存するよう構成されており、
前記第２検証要素情報は、第２組み合わせ文字列を分解することによって取得された第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含み、前記第２組み合わせ文字列は、前記端末が前記デジタルオブジェクト固有識別子をスキャンすることによって取得され、前記第２検証要素情報は、前記端末が前記第２端末識別子を前記端末の前記第１端末識別子と比較して、前記第２端末識別子および前記端末の前記第１端末識別子が同じであると判定した場合に、前記端末から送信された情報に対応し、
前記少なくとも１つのプロセッサは、
前記第２端末識別子に少なくとも部分的に基づいて、複数の第１端末識別子、複数の第１セキュリティ検証コード、および、複数の第１タイムスタンプの間の前記関係性を検索して、前記第２端末識別子にそれぞれ対応する前記セキュリティ検証コードおよび前記タイムスタンプを取得し、
前記第２セキュリティ検証コードおよび前記取得されたセキュリティ検証コードが一致し、前記第２タイムスタンプおよび前記取得されたタイムスタンプが一致し、前記第２タイムスタンプが前記セキュリティ検証要求に関連する現在のセキュリティチェックの期限内にある場合に、セキュリティチェック合格情報を前記端末に送信することにより、
前記セキュリティチェック合格情報を前記端末に送信する、デバイス。
適用例２０：デバイスであって、
少なくとも１つのプロセッサであって、
セキュリティ検証要求をサーバに送信し、
デジタルオブジェクト固有識別子を前記サーバから受信し、
前記デジタルオブジェクト固有識別子は、前記サーバが前記セキュリティ検証要求に少なくとも部分的に基づいて取得した第１検証要素情報に少なくとも部分的に基づいて生成された固有識別子に対応し、
前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて第２検証要素情報を取得し、
前記第２検証要素情報を前記サーバに送信し、
前記第１検証要素情報および前記第２検証要素情報が一致する場合に、セキュリティチェック合格情報を前記サーバから受信するよう構成されている、少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサに接続され、前記少なくとも１つのプロセッサに命令を提供するよう構成されているメモリと、
を備える、デバイス。
適用例２１：適用例２０に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記デジタルオブジェクト固有識別子をスキャンし、
前記デジタルオブジェクト固有識別子の前記スキャンに少なくとも部分的に基づいて第２組み合わせ文字列を取得し、
前記デジタルオブジェクト固有識別子は、第１組み合わせ文字列に少なくとも部分的に基づいて生成され、前記第１組み合わせ文字列は、前記サーバが、第１端末識別子、第１セキュリティ検証コード、および、第１タイムスタンプを組み合わせることによって生成され、前記第１検証要素情報は、前記第１端末識別子、前記第１セキュリティ検証コード、および、前記第１タイムスタンプを含み、前記第１端末識別子は、前記端末のユーザ

名に少なくとも部分的に基づいて取得された前記端末の端末識別子に対応し、前記端末の前記ユーザ名は、前記セキュリティ検証要求に含まれ、前記第１セキュリティチェックおよび前記第１タイムスタンプは、前記セキュリティ検証要求に関連して前記サーバによって生成された前記第１セキュリティ検証コードおよび前記第１タイムスタンプに対応し、
前記第２組み合わせ文字列を分解し、
前記第２組み合わせ文字列の前記分解に少なくとも部分的に基づいて、第２端末識別子、第２セキュリティ検証コード、および、第２タイムスタンプを含む前記第２検証要素情報を取得するよう構成されている、デバイス。
適用例２２：適用例２１に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
クイックレスポンス（ＱＲ）復号ルールを用いて、前記デジタルオブジェクト固有識別子に対応する二次元検証コードを復号し、
前記二次元検証コードの前記復号に少なくとも部分的に基づいてｂａｓｅ６４文字列を生成し、
前記ｂａｓｅ６４文字列を暗号化文字列に変換し、
前記暗号化文字列を復号することに少なくとも部分的に基づいて前記第２組み合わせ文字列を取得するよう構成されている、デバイス。
適用例２３：適用例２３に記載のデバイスであって、前記少なくとも１つのプロセッサは、さらに、
前記第２検証要素情報が前記サーバに送信される前に、前記第２端末識別子および前記端末の端末識別子を比較し、
前記第２端末識別子および前記端末の前記端末識別子がマッチする場合に、前記第２検証要素情報を前記サーバに送信する工程を実行するよう構成されている、デバイス。
適用例２４：コンピュータプログラム製品であって、持続性のコンピュータ読み取り可能な記憶媒体内に具現化され、
端末から送信されたセキュリティ検証要求を受信するためのコンピュータ命令と、
前記セキュリティ検証要求に少なくとも部分的に基づいて、第１検証要素情報を取得するためのコンピュータ命令と、
前記第１検証要素情報に少なくとも部分的に基づいて、デジタルオブジェクト固有識別子を生成するためのコンピュータ命令と、
前記デジタルオブジェクト固有識別子を前記端末に送信するためのコンピュータ命令と、
第２検証要素情報を前記端末から受信するためのコンピュータ命令と、
前記第１検証要素情報および前記第２検証要素情報が一致する場合に、セキュリティチェック合格情報を前記端末に送信するためのコンピュータ命令と、
を備える、コンピュータプログラム製品。
適用例２５：コンピュータプログラム製品であって、持続性のコンピュータ読み取り可能な記憶媒体内に具現化され、
セキュリティ検証要求をサーバに送信するためのコンピュータ命令と、
デジタルオブジェクト固有識別子を前記サーバから受信するためのコンピュータ命令と、前記デジタルオブジェクト固有識別子は、前記サーバが前記セキュリティ検証要求に少なくとも部分的に基づいて取得した第１検証要素情報に少なくとも部分的に基づいて生成された固有識別子に対応し、
前記デジタルオブジェクト固有識別子に少なくとも部分的に基づいて第２検証要素情報を取得するためのコンピュータ命令と、
前記第２検証要素情報を前記サーバに送信するためのコンピュータ命令と、
前記第１検証要素情報および前記第２検証要素情報が一致する場合に、セキュリティチェック合格情報を前記サーバから受信するためのコンピュータ命令と、を備える、コンピュータプログラム製品。

【図１】

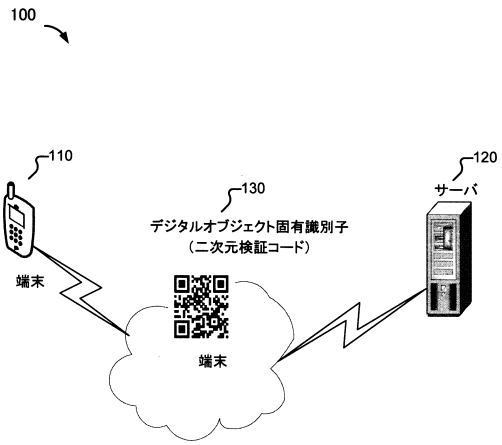
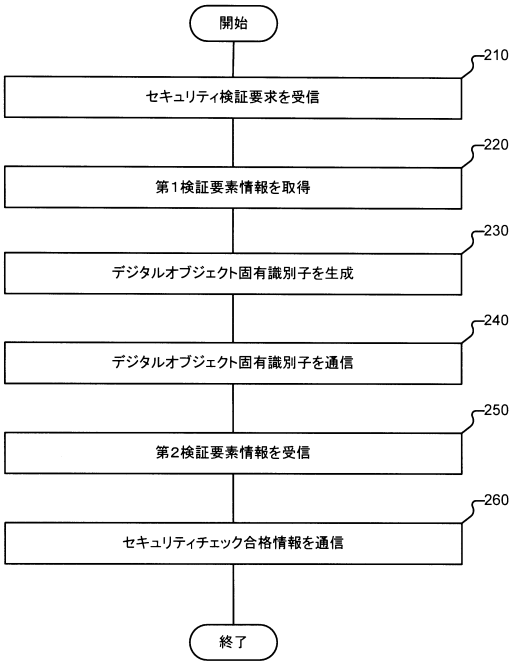


FIG. 1

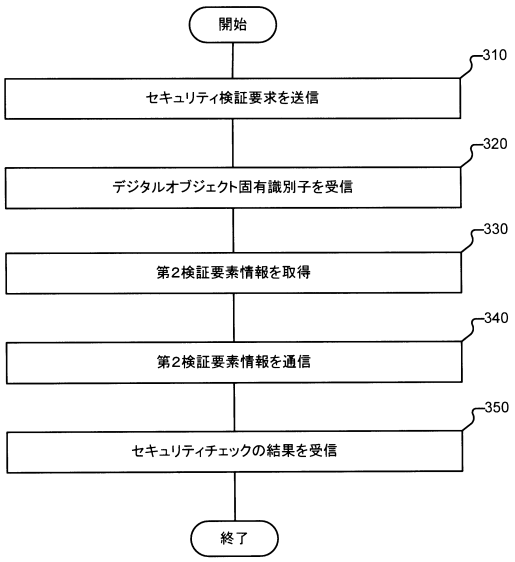
【図２】



200

FIG. 2

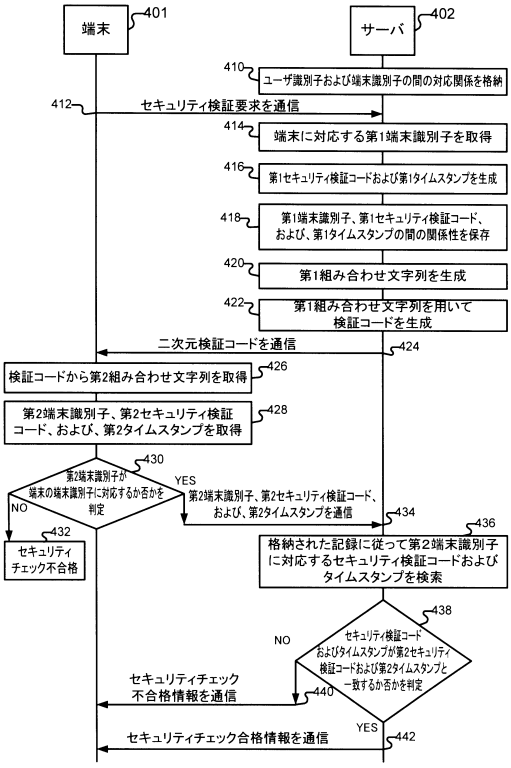
【図３】



300

FIG. 3

【図４】



400

FIG. 4

【図５】

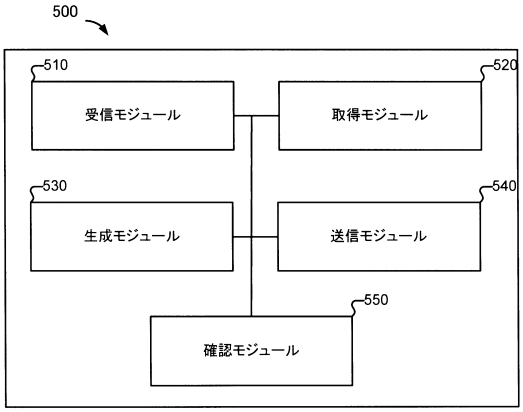


FIG. 5

【図６】

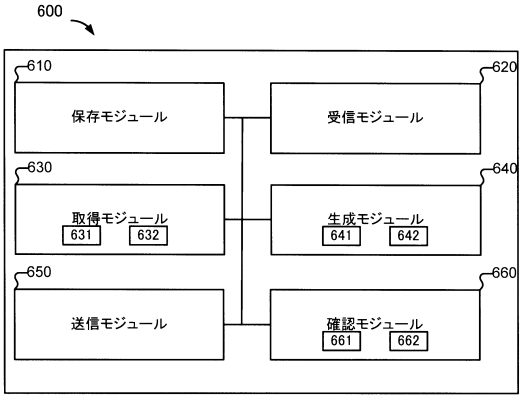


FIG. 6

【図７】

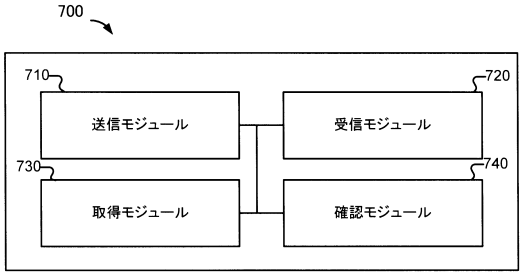


FIG. 7

【図８】

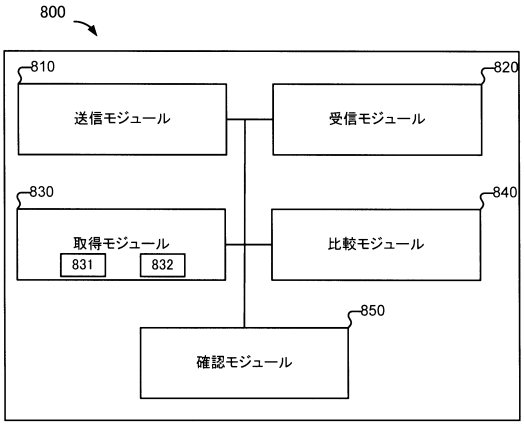


FIG. 8

【図９】

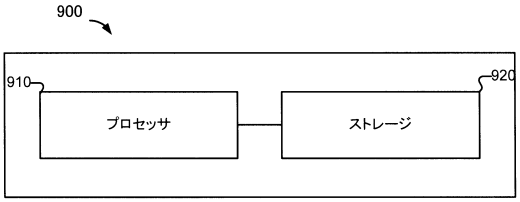


FIG. 9

【図１０】

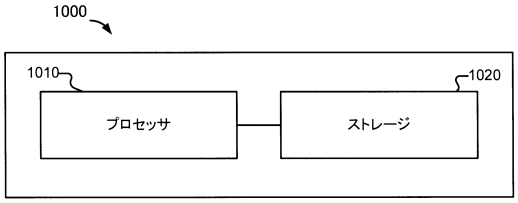


FIG. 10

【図１１】

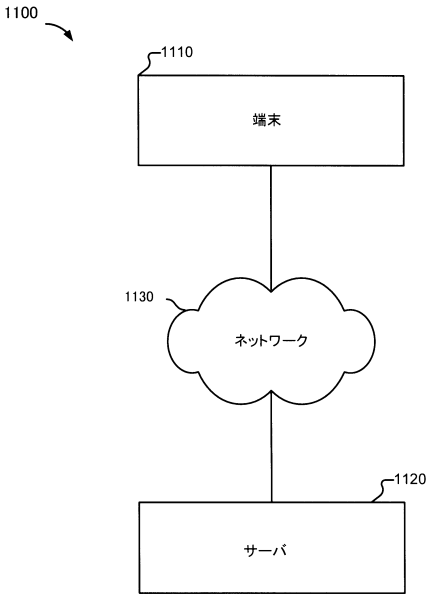


FIG.11

【図１２】

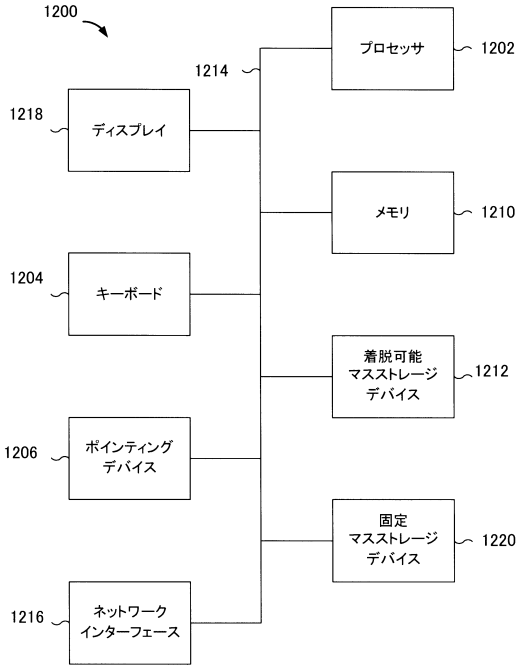


FIG. 12

フロントページの続き

(72)発明者　フェン・ジンガン
中華人民共和国　ハンチョウ３１１１２１，ユ・ハン・ディストリクト，ウェスト・ウェン・イー・ロード，ビルディング　３，５階，ナンバー９６９，アリババ・グループ・リーガル・デパートメント内

審査官　岸野　徹

(56)参考文献　特表２０１３－５０９８４０（ＪＰ，Ａ）
米国特許出願公開第２００３／００２３５６６（ＵＳ，Ａ１）
国際公開第２００９／０１１４３６（WO，Ａ１）
特開２００１－３１８８９４（ＪＰ，Ａ）
国際公開第２００９／０５６８９７（WO，Ａ１）
特開２０１０－２１１２９４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／４４