【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成29年3月30日(2017.3.30)

【公表番号】特表2017-503427(P2017-503427A)
【公表日】平成29年1月26日(2017.1.26)
【年通号数】公開・登録公報2017-004
【出願番号】特願2016-544601(P2016-544601)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/35　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｈ０４Ｌ　9/00　６７３Ｅ
Ｇ０６Ｆ　21/35

【手続補正書】
【提出日】平成29年2月22日(2017.2.22)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保する認証装置であって、
秘密鍵を格納するように構成されたメモリーコンポーネントと、
前記秘密鍵と動的変数値とを暗号化して組み合わせることによって動的認証情報を生成するように構成されたデータ処理コンポーネントと、
前記認証装置を近距離無線通信（ＮＦＣ）転送装置に接続する近距離無線通信（ＮＦＣ）インターフェースと、
前記ユーザからの入力を取得するためのユーザ入力インターフェースと、
を有し、前記認証装置は、
近距離無線通信（ＮＦＣ）タグとして前記近距離無線通信転送装置に提供され、
近距離無線通信タグのデータコンテンツを読み出す近距離無線通信（ＮＦＣ）機構を用いて前記近距離無線通信転送装置により読み出し可能である、前記近距離無線通信タグの第一のデータコンテンツ内に前記生成された動的認証情報を含めることにより、該動的認証情報を前記近距離無線通信転送装置に利用可能とされ、前記認証装置が近距離無線通信タグとして前記近距離無線通信転送装置に提供される工程、前記データ処理コンポーネントが前記動的認証情報を生成する工程、または前記認証装置が前記生成された認証情報を前記近距離無線通信転送装置に利用可能とする工程のうち少なくとも１つに対する条件として前記ユーザからの特定の入力を要求するように構成されているものである、
認証装置。
【請求項２】
請求項１記載の認証装置において、さらに、
１型、２型、３型または４型の近距離無線通信（ＮＦＣ）フォーラムに準拠したタグとして提供され、
前記近距離無線通信転送装置が、近距離無線通信フォーラムに準拠したタグから近距離無線通信データ交換フォーマット（ＮＤＥＦ：ＮＦＣ　ｄａｔａ　Ｅｘｈａｎｇｅ　Ｆｏ

ｒｍａｔ）のメッセージを読み出す近距離無線通信（ＮＦＣ）機構を用いて、前記生成された動的認証情報を読み出すために、該動的認証情報を前記認証装置の近距離無線通信データ交換フォーマットファイルの該データ交換フォーマット（ＮＤＥＦ）メッセージにおける該データ交換フォーマット（ＮＤＥＦ）レコードに含めることによって該動的認証情報を前記転送装置に利用可能とするように構成されているものである、認証装置。
【請求項３】
請求項１記載の認証装置において、さらに、
クロックを有し、
前記動的変数は前記クロックによって提供される時刻値に基づくものである、認証装置。
【請求項４】
請求項１記載の認証装置において、前記動的変数は、前記メモリーコンポーネント内に格納され、特定のイベントが発生する毎に前記認証装置によって更新されるイベント関連値に基づくものである、認証装置。
【請求項５】
請求項４記載の認証装置において、前記特定のイベントは、前記動的認証情報の生成と同時に発生するものである、認証装置。
【請求項６】
請求項４記載の認証装置において、前記イベント関連値は、前記特定のイベントが発生する毎に前記認証によって単調増加または単調減少されるカウンタを有するものである、認証装置。
【請求項７】
請求項１記載の認証装置において、前記秘密鍵と前記動的変数値とを暗号化して組み合わせる工程は、前記動的変数値に対称暗号化アルゴリズムを適用する工程を有し、前記対称暗号化アルゴリズムは前記秘密鍵でパラメータ化されるものであり、前記秘密鍵は前記生成された動的認証情報を検証するための機関と共有されるものである、認証装置。
【請求項８】
請求項１記載の認証装置において、さらに、
ユーザ識別子を格納し、
近距離無線通信タグのデータコンテンツを読み出す近距離無線通信機構を用いて前記近距離無線通信転送装置により読み出し可能である、前記近距離無線通信タグのデータコンテンツ内に前記動的認証情報を含めることにより、前記ユーザ識別子を前記近距離無線通信転送装置に利用可能とするように構成されているものである、
認証装置。
【請求項９】
請求項１記載の認証装置において、前記ユーザ入力インターフェースはアクティベーションボタンを有し、前記特定の入力はユーザが前記アクティベーションボタンを押す工程を含むものである、認証装置。
【請求項１０】
請求項１記載の認証装置において、さらに、前記ユーザ入力インターフェースによって前記ユーザによりアクティベートされるように構成され、前記ユーザが前記ユーザ入力インターフェースを用いて前記認証装置をアクティベートさせた後にのみ、近距離無線通信タグとして前記近距離無線通信転送装置に提供されるものである、認証装置。
【請求項１１】
請求項１記載の認証装置において、さらに、前記近距離無線通信転送装置を有するアクセス装置に永久的または半永久的に固定されるように構成されているものである、認証装置。
【請求項１２】
請求項１１記載の認証装置において、さらに、前記近距離無線通信転送装置を有するアクセス装置への取り付け用に接着コンポーネントを有するものである、認証装置。

【請求項１３】
請求項１１記載の認証装置において、前記近距離無線通信転送装置を有するアクセス装置の保護シェルまたは保護カバー内に含まれるものである、認証装置。
【請求項１４】
請求項１記載の認証装置において、
前記動的変数は外部データに基づいており、
前記認証装置は、さらに、近距離無線通信タグのデータコンテンツを更新する近距離無線通信機構を用いて前記近距離無線通信転送装置により更新された、前記近距離無線通信タグの第二のデータコンテンツから外部データを抽出することにより、前記近距離無線通信転送装置から該外部データを受信するように構成されているものである、認証装置。
【請求項１５】
請求項１４記載の認証装置において、さらに、
ユーザ出力インターフェースを有し、
前記外部データは取引データを有し、
前記認証装置は、さらに、前記取引データをユーザに提示し、前記提示された取引データに対する前記ユーザによる承諾または拒否を前記入力インターフェースで取得し、前記ユーザが前記提示された取引データを承諾した場合にのみ、前記動的認証情報を生成し、および／または、前記生成された動的認証情報を前記近距離無線通信転送装置に利用可能にするように構成されていものである、認証装置。
【請求項１６】
請求項１５記載の認証装置において、前記ユーザ入力インターフェースは、前記承諾を取得するための承諾ボタンと、前記拒否を取得するための拒否ボタンを有するものである、認証装置。
【請求項１７】
請求項１５記載の認証装置において、さらに、
前記認証装置は、前記近距離無線通信転送装置から前記外部データを受信した後、所定の期間、近距離無線通信タグとして前記近距離無線通信転送装置に提供されないように構成されており、かつ前記ユーザが前記提示された取引データを承諾または拒否した後にのみ、前記近距離無線通信転送装置に再び提供されるように構成されているものである、認証装置。
【請求項１８】
請求項１記載の認証装置において、さらに、
近距離無線通信タグのデータコンテンツを更新する近距離無線通信機構を用いて前記近距離無線通信転送装置により更新された、前記近距離無線通信タグの第三のデータコンテンツからパスワード値を抽出することにより、前記近距離無線通信転送装置から該パスワード値を受信し、
前記受信したパスワード値が正しいかどうかを検証し、
前記パスワード値を受信し、かつ該パスワード値が正しいと検証した場合にのみ、前記動的認証情報を生成し、および／または前記生成した認証情報を前記近距離無線通信転送装置に利用可能にするように構成されているものである、
認証装置。
【請求項１９】
ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保するシステムであって、
動的認証情報を生成する認証装置と、
前記コンピュータベースのアプリケーションのサーバ部をホストし、前記認証装置によって生成された前記動的認証情報を検証するアプリケーションサーバと、
前記ユーザによる前記コンピュータ・ベース・アプリケーションへのアクセスを許可するためのアクセス装置であって、コンピュータネットワークによって前記アプリケーションサーバに接続され、前記認証装置から前記動的認証情報を取得し、かつ前記取得した動

的認証情報を検証のために前記アプリケーションサーバに転送するように構成されているものである、前記アクセス装置と、
を有し、
前記アクセス装置は近距離無線通信（ＮＦＣ）転送装置を有し、
前記認証装置は、
秘密鍵を格納するように構成されたメモリーコンポーネントと、
前記秘密鍵と第一の動的変数の第一の値とを暗号化して組み合わせることによって前記動的認証情報を生成するように構成されたデータ処理コンポーネントと、
前記認証装置を前記近距離無線通信転送装置に接続する近距離無線通信（ＮＦＣ）インターフェースと、
前記ユーザからの入力を取得するためのユーザ入力インターフェースと、
を有し、
前記認証装置は、
近距離無線通信（ＮＦＣ）タグとして前記近距離無線通信転送装置に提供され、
近距離無線通信タグのデータコンテンツを読み出す近距離無線通信（ＮＦＣ）機構を用いて前記近距離無線通信転送装置により読み出し可能である、前記近距離無線通信タグの第一のデータコンテンツ内に前記生成された動的認証情報を含めることにより、該動的認証情報を前記近距離無線通信転送装置に利用可能とされ、
前記認証装置が近距離無線通信タグとして前記近距離無線通信転送装置に提供される工程、前記データ処理コンポーネントが前記動的認証情報を生成する工程、または前記認証装置が前記生成された認証情報を前記近距離無線通信転送装置に利用可能とする工程のうち少なくとも１つに対する条件として前記ユーザからの特定の入力を要求するように構成されているものであり、
前記アクセス装置は、近距離無線通信タグのデータコンテンツを読み出す近距離無線通信機構を用いて前記近距離無線通信転送装置により読み出し可能である、前記近距離無線通信タグの前記第一のデータコンテンツから前記動的認証情報を抽出することにより、前記動的認証情報を取得するものであり、
前記アプリケーションサーバは、前記認証装置により生成され、前記アクセス装置により取得および転送された前記動的認証情報を受信し、前記受信した動的変数を第二の動的変数の第二の値と共に暗号化アルゴリズムを用いて検証するように構成されているものである、
システム。
【請求項２０】
請求項１９記載のシステムにおいて、前記秘密鍵と前記第一の動的変数の前記第一の値とを暗号化して組み合わせる工程は、前記第一の動的変数の前記第一の値に対称暗号化アルゴリズムを実行する工程を有し、該対称暗号化アルゴリズムは前記秘密鍵でパラメータ化され、前記秘密鍵は前記認証装置と前記アプリケーションサーバとの間で共有され、前記アプリケーションサーバは前記秘密鍵のサーバコピーを用いて前記動的認証情報を検証するものである、システム。
【請求項２１】
請求項１９記載のシステムにおいて、
前記認証装置および前記アクセス装置は結合用の秘密（ｂｉｎｄｉｎｇ　ｓｅｃｒｅｔ）を共有し、
前記アクセス装置は、さらに、前記近距離無線通信転送装置が、近距離無線通信タグのデータコンテンツを更新する近距離無線通信機構を用いて、前記近距離無線通信タグの第二のデータコンテンツを更新することにより前記結合用の秘密から導き出された結合値を前記認証装置に通信するように構成され、
前記認証装置は、さらに、
近距離無線通信タグのデータコンテンツを更新する前記近距離無線通信機構を用いて前記近距離無線通信転送装置により更新された、前記近距離無線通信タグの前記第二のデ

ータコンテンツから前記結合値を抽出することにより、前記アクセス装置から前記結合値を受信し、
前記結合用の秘密を用いて前記受信した結合値を検証し、
前記受信した結合値が正しいと検証した場合にのみ、前記動的認証情報を生成し、および／または、前記生成した動的認証情報を前記近距離無線通信転送装置に利用可能にするものである、
システム。
【請求項２２】
ユーザとコンピュータベースのアプリケーションとのインタラクションにおける安全性を確保する方法であって、
前記ユーザからの入力を取得するためのユーザ入力インターフェースと近距離無線通信転送装置に接続するための近距離無線通信（ＮＦＣ）インターフェースを有する認証装置で、第一の動的変数の第一の値と、前記認証装置に格納されかつ前記アプリケーションのサーバ部をホストするアプリケーションサーバと共有する秘密鍵とを暗号化して組み合わせることにより動的認証情報を生成する工程であって、前記認証装置は近距離無線通信タグとして前記近距離無線通信転送装置に提供されるものである、前記生成する工程と、
近距離無線通信タグとして前記近距離無線通信転送装置に提供される工程、前記データ処理コンポーネントが前記動的認証情報を生成する工程、または前記認証装置が前記生成された認証情報を前記近距離無線通信転送装置に利用可能とする工程のうち少なくとも１つに対する条件として前記ユーザからの特定の入力を要求するものである前記認証装置で、近距離無線通信タグのデータコンテンツを読み出す近距離無線通信機構を用いて前記近距離無線通信転送装置により読み出し可能である、前記近距離無線通信タグの第一のデータコンテンツに前記動的認証情報に含めることにより、前記生成した動的認証情報を前記近距離無線通信転送装置に利用可能にする工程と、
前記近距離無線通信転送装置を有し、コンピュータネットワークによって前記アプリケーションサーバに接続されたアクセス装置を用いて、前記ユーザが前記コンピュータベースのアプリケーションにアクセスするのを許可する工程と、
前記アクセス装置で、近距離無線通信タグのデータコンテンツを読み出す前記近距離無線通信転送装置を用いて前記近距離無線通信転送装置により読み出された、前記近距離無線通信タグの前記データコンテンツから動的認証情報を抽出することにより、前記動的認証情報を取得する工程と、
前記アクセス装置で、前記動的認証情報を前記アプリケーションサーバに転送する工程と、
前記アプリケーションサーバで、前記認証装置で生成され、前記アクセス装置で取得された前記動的認証情報を受信する工程と、
前記アプリケーションサーバで、前記受信した動的認証情報を検証する工程と、
を有する、方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００４
【補正方法】変更
【補正の内容】
【０００４】
近年、リモートアプリケーションにアクセスするために、ＰＣ（パーソナルコンピュータ）よりむしろスマートフォンを使用することが益々普及してきている。これは、ユーザがスマートフォンを使用中に、リモートアプリケーションと安全にインタラトすることを保障するための解決策が求められていることを意味する。元来ＰＣに使用するために開発された既存の解決策は、様々な理由でスマートフォンに使用するにはあまり満足できるものではない。動的なパスワードおよび署名を生成するソフトウェアアプリケーションのような純粋なソフトウェア解決策は、ＰＣと同様にスマートフォンが、益々あらゆる種類の

マルウェアの標的になってきているので、攻撃に対して脆弱である。スマートカードまたはＵＳＢトークンのようなハードウェア解決策は、しばしばスマートフォンにサポートされていない特定の通信用インターフェース（スマートカードリーダ、ＵＳＢポート等）を必要とする。ユーザが変換されるべきデータ（ワン・タイム・パスワードなど）をコピーすることに依存する強力な認証トークンのような他のハードウェア解決策は、文字通りスマートフォンで手一杯のユーザにはしばしば煩わしいものとして認識される可能性がある。

この出願の発明に関連する先行技術文献情報としては、以下のものがある（国際出願日以降国際段階で引用された文献及び他国に国内移行した際に引用された文献を含む）。

（先行技術文献）

（特許文献）

（特許文献１）　米国特許第８，７８９，１４６号明細書
（特許文献２）　米国特許出願公開第２００９／００４８９７１号明細書
（特許文献３）　米国特許出願公開第２００９／０１４３１０４号明細書
（特許文献４）　米国特許出願公開第２０１０／０１７８８６８号明細書
（特許文献５）　米国特許出願公開第２０１２／００２３５６７号明細書
（特許文献６）　米国特許出願公開第２０１２／０１６７１９４号明細書
（特許文献７）　米国特許出願公開第２０１２／０２６５９８８号明細書
（特許文献８）　米国特許出願公開第２０１３／０３４３５４２号明細書
（特許文献９）　米国特許出願公開第２０１４／０１８１９５５号明細書
（特許文献１０）　米国特許第８，９４３，３１１号明細書
（特許文献１１）　米国特許第９，１０４，８５３号明細書
（特許文献１２）　国際公開第２０１３／０３４６８１号
（特許文献１３）　国際公開第２０１０／０４３９７４号

（非特許文献）

（非特許文献１）　Ｐａｒｄｉｓ　Ｐｏｕｒｇｈｏｍｉ；　Ｍａｎａｇｉｎｇ　ＮＦＣ　Ｐａｙｍｅｎｔ　Ａｐｐｌｉｃａｔｉｏｎｓ　ｔｈｒｏｕｇｈ　Ｃｌｏｕｄ　Ｃｏｍｐｕｔｉｎｇ；　ＩＥＥＥ；　Ｙｅａｒ：２０１２；　ｐａｇｅ：　７７２－７７７