【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６部門第３区分
【発行日】平成17年11月24日(2005.11.24)

【公開番号】特開2005-38411(P2005-38411A)
【公開日】平成17年2月10日(2005.2.10)
【年通号数】公開・登録公報2005-006
【出願番号】特願2004-179562(P2004-179562)
【国際特許分類第７版】
　Ｇ０６Ｆ　15/00
　Ｈ０４Ｌ　 9/32
【ＦＩ】
　Ｇ０６Ｆ　15/00　　３３０Ｃ
　Ｈ０４Ｌ　 9/00　　６７３Ｃ

【手続補正書】
【提出日】平成17年9月30日(2005.9.30)
【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】
　提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、
　前記取得した元情報から機器認証情報を生成する生成手段と、
　機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、
　を具備したことを特徴とする端末機器。
【請求項２】
　前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、
　前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求項１に記載の端末機器。
【請求項３】
　前記生成手段で生成した機器認証情報を暗号化して記憶する記憶手段を具備し、
　前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信することを特徴とする請求項１に記載の端末機器。
【請求項４】
　前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備したことを特徴とする請求項３に記載の端末機器。
【請求項５】
　前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去手段を具備したことを特徴とする請求項４に記載の端末機器。
【請求項６】
　前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得手段と、
　前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、

前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、
を具備したことを特徴とする請求項１に記載の端末機器。
【請求項７】
前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、
前記算出した変換値を前記提供サーバに提供する変換値提供手段と、
を具備したことを特徴とする請求項６に記載の端末機器。
【請求項８】
前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、
前記算出した変換値を前記提供サーバに提供する変換値提供手段と、
を具備したことを特徴とする請求項１に記載の端末機器。
【請求項９】
前記取得した元情報を記憶する記憶手段を具備し、
前記機器認証情報送信手段は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求項１に記載の端末機器。
【請求項１０】
元情報取得手段と、生成手段と、機器認証情報送信手段と、を備えたコンピュータで構成された端末機器において、
提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、
前記取得した元情報から機器認証情報を、前記生成手段で生成する生成ステップと、
機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、
から構成されたことを特徴とする機器認証情報処理方法。
【請求項１１】
提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、
前記取得した元情報から機器認証情報を生成する生成機能と、
機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、
をコンピュータで実現する機器認証情報処理プログラム。
【請求項１２】
端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、
前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、
前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、
前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、
前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、
を具備したことを特徴とする提供サーバ。
【請求項１３】
前記判断手段で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信手段を具備したことを特徴とする請求項１２に記載の提供サーバ。
【請求項１４】
元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、判断手段と、を備えたコンピュータにおいて、
端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する

元情報提供ステップと、
前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、
前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、
前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出ステップと、
前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、
から構成されたことを特徴とする機器認証情報提供方法。
【請求項１５】
前記コンピュータは、判断結果送信手段を備え、
前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えたことを特徴とする請求項１４に記載の機器認証情報提供方法。
【請求項１６】
端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、
前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、
前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、
前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、
前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、
をコンピュータで実現する機器認証情報提供プログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】端末機器、機器認証情報処理方法、機器認証情報処理プログラム、提供サーバ、機器認証情報提供方法、および機器認証情報提供プログラム
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正の内容】
【０００９】
本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、前記取得した元情報から機器認証情報を生成する生成手段と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、を具備したことを特徴とする端末機器を提供する（第１の構成）。
また、第１の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することもできる（第２の構成）。
更に、第１の構成において、前記生成手段で生成した機器認証情報を暗号化して記憶する記憶手段を具備し、前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信するように構成することもできる（第３の構成）。
また、第３の構成において、前記記憶手段に記憶する機器認証情報の暗号化、及び復号

化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備するように構成することもできる（第４の構成）。

また、第４の構成において、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去手段を具備するように構成することもできる（第５の構成）。

また、第１の構成において、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得手段と、前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備するように構成することもできる（第６の構成）。

また、第６の構成において、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第７の構成）。

また、第１の構成において、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第８の構成）。

また、第１の構成において、前記取得した元情報を記憶する記憶手段を具備し、前記機器認証情報送信手段は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することもできる（第９の構成）。

また、本発明は、前記目的を達成するために、元情報取得手段と、生成手段と、機器認証情報送信手段と、を備えたコンピュータで構成された端末機器において、提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、前記取得した元情報から機器認証情報を、前記生成手段で生成する生成ステップと、機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、から構成されたことを特徴とする機器認証情報処理方法を提供する（第１０の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、前記取得した元情報から機器認証情報を生成する生成機能と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、をコンピュータで実現する機器認証情報処理プログラムを提供する（第１１の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備したことを特徴とする提供サーバを提供する（第１２の構成）。

第１２の構成において、前記判断手段で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信手段を具備するように構成することができる（第１３の構成）。

また、本発明は、前記目的を達成するために、元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、判断手段と、を備えたコンピュータにおいて、端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する元情報提供ステップと、前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出ステップと、前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、から構成されたことを特徴とする機器

認証情報提供方法を提供する（第１４の構成）。

第１４の構成において、前記コンピュータは、判断結果送信手段を備え、前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えるように構成することができる（第１５の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現する機器認証情報提供プログラムを提供する（第１６の構成）。