(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3761477号

(P3761477)

(45)発行日　平成18年3月29日(2006.3.29)　(24)登録日　平成18年1月20日(2006.1.20)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
E05B 49/00	(2006.01)	E05B	49/00	K
E05B 65/12	(2006.01)	E05B	65/12	A

請求項の数 7　(全 26 頁)

(21)出願番号　特願2002-56778(P2002-56778)
(22)出願日　平成14年3月4日(2002.3.4)
(65)公開番号　特開2003-258794(P2003-258794A)
(43)公開日　平成15年9月12日(2003.9.12)
審査請求日　平成15年3月17日(2003.3.17)

(73)特許権者　390001395
エヌイーシーシステムテクノロジー株式会社
大阪府大阪市中央区城見１丁目４番２４号
(74)代理人　100097113
弁理士　堀　城之
(72)発明者　細谷　忠功
大阪府大阪市中央区城見１丁目４番２４号　エヌイーシーシステムテクノロジー株式会社内

審査官　中里　裕正

(56)参考文献　特開２０００－１２７８９２（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】移動体セキュリティシステム

(57)【特許請求の範囲】

【請求項１】

移動体の改造および盗難を防止する移動体セキュリティシステムであって、

前記移動体は、

情報を記憶する記憶手段と、

認証処理を実行する認証手段と、

前記移動体の作動を制御する制御手段と、

前記移動体を始動するための始動装置との通信を制御する通信手段と

を備え、

前記移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、

前記移動体の前記記憶手段に、第１の証明書と、第１の秘密鍵と、前記移動体を識別するための第１の識別データが登録され、

前記移動体の作動を制御する前記制御手段に、第２の証明書と、第２の秘密鍵と、前記第１の識別データと、前記移動体を利用する利用者を識別するための第２の識別データが登録され、

前記利用者が所持する前記始動装置に、第３の証明書と、第３の秘密鍵と、前記第２の識別データが登録され、

前記認証手段は、前記第１の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第１の証明書から前記記憶

手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記記憶手段に供給し、
前記記憶手段は、前記ランダムデータと前記第１の識別データを結合して前記第１の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、
前記認証手段は、前記第３の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第１の識別データを記憶し、
前記認証手段は、前記第２の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第２の証明書から前記制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記制御手段に供給し、
前記制御手段は、前記ランダムデータと前記第１の識別データと前記第２の識別データを結合して前記第２の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、
前記認証手段は、前記第４の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第１の識別データと、記憶しておいた前記第１の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第２の識別データを記憶し、
前記認証手段は、前記第３の証明書を前記第２の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第３の証明書から前記利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記始動装置に供給し、
前記始動装置は、前記ランダムデータと前記第２の識別データを結合して前記第３の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、
前記認証手段は、前記第５の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第２の識別データと、記憶しておいた前記第２の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記移動体を始動可能にする
ことを特徴とする移動体セキュリティシステム。

【請求項２】
前記第１の証明書は、前記記憶手段の前記第３の公開鍵を含み、第１の認証局の第４の秘密鍵でデジタル署名されたものであり、前記第２の証明書は、前記制御手段の前記第４の公開鍵を含み、前記第１の認証局の前記第４の秘密鍵でデジタル署名されたものであり、前記第３の証明書は、前記利用者の第５の公開鍵を含み、第２の認証局の第５の秘密鍵でデジタル署名されたものである
ことを特徴とする請求項１に記載の移動体セキュリティシステム。

【請求項３】
移動体の改造および盗難を防止する移動体セキュリティシステムであって、
前記移動体は、
情報を記憶する記憶手段と、
認証処理を実行する認証手段と、
前記移動体の作動を制御する制御手段と、
前記移動体を始動するための始動装置との通信を制御する通信手段と
を備え、
前記移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、
前記移動体の前記記憶手段に、第１の証明書と、第１の秘密鍵と、前記移動体を識別するための第１の識別データが登録され、

前記移動体の作動を制御する前記制御手段に、第２の証明書と、第２の秘密鍵と、前記第１の識別データと、前記移動体を利用する利用者を識別するための第２の識別データが登録され、

前記利用者が所持する前記始動装置に、利用者を識別するための利用者ＩＤと、第３の秘密鍵と、前記第２の識別データが登録され、

前記認証手段は、前記第１の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第１の証明書から前記記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、

前記記憶手段は、前記ランダムデータと前記第１の識別データを結合して前記第１の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、

前記認証手段は、前記第３の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、

前記第１の識別データを記憶し、

前記認証手段は、前記第２の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第２の証明書から前記制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記制御手段に供給し、

前記制御手段は、前記ランダムデータと前記第１の識別データと前記第２の識別データを結合して前記第２の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、

前記認証手段は、前記第４の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第１の識別データと、記憶しておいた前記第１の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第２の識別データを記憶し、

前記始動装置は、前記利用者ＩＤを前記通信手段を介して前記認証手段に供給し、

前記認証手段は、前記利用者ＩＤを前記第２の認証局に送信し、

前記第２の認証局は、前記利用者ＩＤの有効性を判定し、有効でないとき、前記認証装置を介して前記移動体を始動不可能にし、有効であるとき、第３の証明書を前記認証手段に送信し、

前記認証手段は、前記第３の証明書を前記第２の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第３の証明書から前記利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記始動装置に供給し、

前記始動装置は、前記ランダムデータと前記第２の識別データを結合して前記第３の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、

前記認証手段は、前記第５の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第２の識別データと、記憶しておいた前記第２の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記移動体を始動可能にする

ことを特徴とする移動体セキュリティシステム。

【請求項４】

情報を記憶する記憶手段と、認証処理を実行する認証手段と、前記移動体の作動を制御する制御手段と、前記移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防止方法であって、

前記移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、

前記移動体の前記記憶手段に、第１の証明書と、第１の秘密鍵と、前記移動体を識別するための第１の識別データが登録され、

前記移動体の作動を制御する前記制御手段に、第２の証明書と、第２の秘密鍵と、前記第１の識別データと、前記移動体を利用する利用者を識別するための第２の識別データが登録され、

前記利用者が所持する前記始動装置に、第３の証明書と、第３の秘密鍵と、前記第２の識別データが登録され、

前記認証手段は、前記第１の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第１の証明書から前記記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記記憶手段に供給し、

前記記憶手段は、前記ランダムデータと前記第１の識別データを結合して前記第１の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、

前記認証手段は、前記第３の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第１の識別データを記憶し、

前記認証手段は、前記第２の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第２の証明書から前記制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記制御手段に供給し、

前記制御手段は、前記ランダムデータと前記第１の識別データと前記第２の識別データを結合して前記第２の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、

前記認証手段は、前記第４の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第１の識別データと、記憶しておいた前記第１の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第２の識別データを記憶し、

前記認証手段は、前記第３の証明書を前記第２の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第３の証明書から前記利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記始動装置に供給し、

前記始動装置は、前記ランダムデータと前記第２の識別データを結合して前記第３の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、

前記認証手段は、前記第５の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第２の識別データと、記憶しておいた前記第２の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記移動体を始動可能にする

ことを特徴とする移動体盗難防止方法。

【請求項５】

情報を記憶する記憶手段と、認証処理を実行する認証手段と、前記移動体の作動を制御する制御手段と、前記移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防止方法であって、

前記移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、

前記移動体の前記記憶手段に、第１の証明書と、第１の秘密鍵と、前記移動体を識別するための第１の識別データが登録され、

前記移動体の作動を制御する前記制御手段に、第２の証明書と、第２の秘密鍵と、前記第１の識別データと、前記移動体を利用する利用者を識別するための第２の識別データが登録され、

前記利用者が所持する前記始動装置に、利用者を識別するための利用者ＩＤと、第３の

秘密鍵と、前記第２の識別データが登録され、
前記認証手段は、前記第１の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第１の証明書から前記記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、
前記記憶手段は、前記ランダムデータと前記第１の識別データを結合して前記第１の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、
前記認証手段は、前記第３の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第１の識別データを記憶し、
前記認証手段は、前記第２の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第２の証明書から前記制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記制御手段に供給し、
前記制御手段は、前記ランダムデータと前記第１の識別データと前記第２の識別データを結合して前記第２の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、
前記認証手段は、前記第４の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第１の識別データと、記憶しておいた前記第１の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第２の識別データを記憶し、
前記始動装置は、前記利用者ＩＤを前記通信手段を介して前記認証手段に供給し、
前記認証手段は、前記利用者ＩＤを前記第２の認証局に送信し、
前記第２の認証局は、前記利用者ＩＤの有効性を判定し、有効でないとき、前記認証装置を介して前記移動体を始動不可能にし、有効であるとき、第３の証明書を前記認証手段に送信し、
前記認証手段は、前記第３の証明書を前記第２の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第３の証明書から前記利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記始動装置に供給し、
前記始動装置は、前記ランダムデータと前記第２の識別データを結合して前記第３の秘密鍵でデジタル署名した署名データを前記認証手段に供給し、
前記認証手段は、前記第５の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第２の識別データと、記憶しておいた前記第２の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記移動体を始動可能にする
ことを特徴とする移動体盗難防止方法。

【請求項６】
情報を記憶する記憶手段と、認証処理を実行する認証手段と、前記移動体の作動を制御する制御手段と、前記移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防止プログラムであって、
前記移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とを登録し、
前記移動体の前記記憶手段に、第１の証明書と、第１の秘密鍵と、前記移動体を識別するための第１の識別データを登録し、
前記移動体の作動を制御する前記制御手段に、第２の証明書と、第２の秘密鍵と、前記第１の識別データと、前記移動体を利用する利用者を識別するための第２の識別データを登録し、
前記利用者が所持する前記始動装置に、第３の証明書と、第３の秘密鍵と、前記第２の

識別データを登録し、
前記認証手段に、前記第１の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第１の証明書から前記記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記記憶手段に供給する処理を実行させ、
前記記憶手段に、前記ランダムデータと前記第１の識別データを結合して前記第１の秘密鍵でデジタル署名した署名データを前記認証手段に供給する処理を実行させ、
前記認証手段に、前記第３の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第１の識別データを記憶する処理を実行させ、
前記認証手段に、前記第２の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第２の証明書から前記制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記制御手段に供給する処理を実行させ、
前記制御手段に、前記ランダムデータと前記第１の識別データと前記第２の識別データを結合して前記第２の秘密鍵でデジタル署名した署名データを前記認証手段に供給する処理を実行させ、
前記認証手段に、前記第４の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第１の識別データと、記憶しておいた前記第１の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第２の識別データを記憶する処理を実行させ、
前記認証手段に、前記第３の証明書を前記第２の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第３の証明書から前記利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記始動装置に供給する処理を実行させ、
前記始動装置に、前記ランダムデータと前記第２の識別データを結合して前記第３の秘密鍵でデジタル署名した署名データを前記認証手段に供給する処理を実行させ、
前記認証手段に、前記第５の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第２の識別データと、記憶しておいた前記第２の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記移動体を始動可能にする処理を実行させる
ことを特徴とする移動体盗難防止プログラム。
【請求項７】
情報を記憶する記憶手段と、認証処理を実行する認証手段と、前記移動体の作動を制御する制御手段と、前記移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防止プログラムであって、
前記移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とを登録し、
前記移動体の前記記憶手段に、第１の証明書と、第１の秘密鍵と、前記移動体を識別するための第１の識別データを登録し、
前記移動体の作動を制御する前記制御手段に、第２の証明書と、第２の秘密鍵と、前記第１の識別データと、前記移動体を利用する利用者を識別するための第２の識別データを登録し、
前記利用者が所持する前記始動装置に、利用者を識別するための利用者ＩＤと、第３の秘密鍵と、前記第２の識別データを登録し、
前記認証手段に、前記第１の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第１の証明書から前記記憶

手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶する処理を実行させ、

前記記憶手段に、前記ランダムデータと前記第１の識別データを結合して前記第１の秘密鍵でデジタル署名した署名データを前記認証手段に供給する処理を実行させ、

前記認証手段に、前記第３の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第１の識別データを記憶する処理を実行させ、

前記認証手段に、前記第２の証明書を前記第１の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第２の証明書から前記制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記制御手段に供給する処理を実行させ、

前記制御手段に、前記ランダムデータと前記第１の識別データと前記第２の識別データを結合して前記第２の秘密鍵でデジタル署名した署名データを前記認証手段に供給する処理を実行させ、

前記認証手段に、前記第４の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第１の識別データと、記憶しておいた前記第１の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記第２の識別データを記憶する処理を実行させ、

前記始動装置に、前記利用者ＩＤを前記通信手段を介して前記認証手段に供給する処理を実行させ、

前記認証手段に、前記利用者ＩＤを前記第２の認証局に送信する処理を実行させ、

前記第２の認証局に、前記利用者ＩＤの有効性を判定し、有効でないとき、前記認証装置を介して前記移動体を始動不可能にし、有効であるとき、第３の証明書を前記認証手段に送信する処理を実行させ、

前記認証手段に、前記第３の証明書を前記第２の公開鍵で検証し、検証が失敗したとき、前記移動体の始動を不可能にし、検証が成功したとき、前記第３の証明書から前記利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、前記始動装置に供給する処理を実行させ、

前記始動装置に、前記ランダムデータと前記第２の識別データを結合して前記第３の秘密鍵でデジタル署名した署名データを前記認証手段に供給する処理を実行させ、

前記認証手段に、前記第５の公開鍵で前記デジタル署名された前記署名データをデコードし、得られたランダムデータと、記憶しておいた前記ランダムデータとを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、得られた前記第２の識別データと、記憶しておいた前記第２の識別データを比較し、一致しないとき、前記移動体の始動を不可能にし、一致するとき、前記移動体を始動可能にする処理を実行させる

ことを特徴とする移動体盗難防止プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、移動体セキュリティシステムに関し、特に、移動体の盗難を防止する移動体セキュリティシステムに関する。

【０００２】

【従来の技術】

従来より、一般的に、車両等の移動体において利用者を特定するための認証方式は、固定された記憶情報に基づいて利用者のみの特定を行い、利用者の認証結果に応じて始動装置を制御する。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来の認証方式では、利用者のなりすましによる偽造データ入力、又は認証を行う前提となる記憶データの傍受を防ぐことができない。例えば、イモビライザシステム（特開平１０－２３８４４４）、車両用盗難防止システム（特開平１０－３１５９１５）、車両用盗難防止装置（特開平０８－３１８８２０）等のセキュリティ方式は、オンボードの認証用個人識別データが保護されず、不正に解読して偽の認証結果を元にシステムを利用することが可能である。

【０００４】

また、移動体がまるごと牽引車等によって盗難され、移動体の認証装置そのものが改竄されたり、移動体を分解して構成要素を再利用するような状況には対応できない。

【０００５】

また、盗難防止、及び改竄防止機能を有する自動車乗員保護装置、及びシステム（特開２０００－１２７８９２）は、エアバッグモジュール等の機能部品の盗難再利用を防ぐ方式に関するものであるが、メモリの中の同一性識別情報の改竄、及び盗難防止機能そのものの改竄を防ぐことができないため、盗難防止抑止の方式として不十分である。

【０００６】

本発明はこのような状況に鑑みてなされたものであり、公開鍵暗号方式により、利用者の認証と同時に、移動体を構成する必須要素のＥＣＵ（Ｅｌｅｃｔｒｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）と移動体本体についても識別認証を行い、盗難されても移動体を運行不能にすることで総合的にセキュリティを高めることができるようにするものである。

【０００７】

【課題を解決するための手段】

請求項１に記載の移動体セキュリティシステムは、移動体の改造および盗難を防止する移動体セキュリティシステムであって、移動体は、情報を記憶する記憶手段と、認証処理を実行する認証手段と、移動体の作動を制御する制御手段と、移動体を始動するための始動装置との通信を制御する通信手段とを備え、移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、移動体の記憶手段に、第１の証明書と、第１の秘密鍵と、移動体を識別するための第１の識別データが登録され、移動体の作動を制御する制御手段に、第２の証明書と、第２の秘密鍵と、第１の識別データと、移動体を利用する利用者を識別するための第２の識別データが登録され、利用者が所持する始動装置に、第３の証明書と、第３の秘密鍵と、第２の識別データが登録され、認証手段は、第１の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第１の証明書から記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、記憶手段に供給し、記憶手段は、ランダムデータと第１の識別データを結合して第１の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第３の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第１の識別データを記憶し、認証手段は、第２の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第２の証明書から制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、制御手段に供給し、制御手段は、ランダムデータと第１の識別データと第２の識別データを結合して第２の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第４の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第１の識別データと、記憶しておいた第１の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第２の識別データを記憶し、認証手段は、第３の証明書を第２の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第３の証明書から利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、始動装置に供給し、始動装置は、ランダムデータと第２の識別データを結合して第３の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第５の公

開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第２の識別データと、記憶しておいた第２の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、移動体を始動可能にすることを特徴とする。

また、第１の証明書は、記憶手段の第３の公開鍵を含み、第１の認証局の第４の秘密鍵でデジタル署名されたものであり、第２の証明書は、制御手段の第４の公開鍵を含み、第１の認証局の第４の秘密鍵でデジタル署名されたものであり、第３の証明書は、利用者の第５の公開鍵を含み、第２の認証局の第５の秘密鍵でデジタル署名されたものとすることができる。

請求項３に記載の移動体セキュリティシステムは、移動体の改造および盗難を防止する移動体セキュリティシステムであって、移動体は、情報を記憶する記憶手段と、認証処理を実行する認証手段と、移動体の作動を制御する制御手段と、移動体を始動するための始動装置との通信を制御する通信手段とを備え、移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、移動体の記憶手段に、第１の証明書と、第１の秘密鍵と、移動体を識別するための第１の識別データが登録され、移動体の作動を制御する制御手段に、第２の証明書と、第２の秘密鍵と、第１の識別データと、移動体を利用する利用者を識別するための第２の識別データが登録され、利用者が所持する始動装置に、利用者を識別するための利用者ＩＤと、第３の秘密鍵と、第２の識別データが登録され、認証手段は、第１の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第１の証明書から記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、記憶手段は、ランダムデータと第１の識別データを結合して第１の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第３の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第１の識別データを記憶し、認証手段は、第２の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第２の証明書から制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、制御手段に供給し、制御手段は、ランダムデータと第１の識別データと第２の識別データを結合して第２の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第４の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第１の識別データと、記憶しておいた第１の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第２の識別データを記憶し、始動装置は、利用者ＩＤを通信手段を介して認証手段に供給し、認証手段は、利用者ＩＤを第２の認証局に送信し、第２の認証局は、利用者ＩＤの有効性を判定し、有効でないとき、認証装置を介して移動体を始動不可能にし、有効であるとき、第３の証明書を認証手段に送信し、認証手段は、第３の証明書を第２の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第３の証明書から利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、始動装置に供給し、始動装置は、ランダムデータと第２の識別データを結合して第３の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第５の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第２の識別データと、記憶しておいた第２の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、移動体を始動可能にすることを特徴とする。

請求項４に記載の移動体盗難防止方法は、情報を記憶する記憶手段と、認証処理を実行する認証手段と、移動体の作動を制御する制御手段と、移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防

止方法であって、移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、移動体の記憶手段に、第１の証明書と、第１の秘密鍵と、移動体を識別するための第１の識別データが登録され、移動体の作動を制御する制御手段に、第２の証明書と、第２の秘密鍵と、第１の識別データと、移動体を利用する利用者を識別するための第２の識別データが登録され、利用者が所持する始動装置に、第３の証明書と、第３の秘密鍵と、第２の識別データが登録され、認証手段は、第１の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第１の証明書から記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、記憶手段に供給し、記憶手段は、ランダムデータと第１の識別データを結合して第１の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第３の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第１の識別データを記憶し、認証手段は、第２の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第２の証明書から制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、制御手段に供給し、制御手段は、ランダムデータと第１の識別データと第２の識別データを結合して第２の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第４の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第１の識別データと、記憶しておいた第１の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第２の識別データを記憶し、認証手段は、第３の証明書を第２の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第３の証明書から利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、始動装置に供給し、始動装置は、ランダムデータと第２の識別データを結合して第３の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第５の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第２の識別データと、記憶しておいた第２の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、移動体を始動可能にすることを特徴とする。

請求項５に記載の移動体盗難防止方法は、情報を記憶する記憶手段と、認証処理を実行する認証手段と、移動体の作動を制御する制御手段と、移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防止方法であって、移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とが登録され、移動体の記憶手段に、第１の証明書と、第１の秘密鍵と、移動体を識別するための第１の識別データが登録され、移動体の作動を制御する制御手段に、第２の証明書と、第２の秘密鍵と、第１の識別データと、移動体を利用する利用者を識別するための第２の識別データが登録され、利用者が所持する始動装置に、利用者を識別するための利用者ＩＤと、第３の秘密鍵と、第２の識別データが登録され、認証手段は、第１の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第１の証明書から記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、記憶手段は、ランダムデータと第１の識別データを結合して第１の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第３の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第１の識別データを記憶し、認証手段は、第２の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第２の証明書から制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、制御手段に供給し、制御手段は、ランダムデータと第１の識別データと第２の識別データを結合して第２の秘密鍵でデジタル署名した署名データを認証手段に供給し、

認証手段は、第４の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第１の識別データと、記憶しておいた第１の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第２の識別データを記憶し、始動装置は、利用者ＩＤを通信手段を介して認証手段に供給し、認証手段は、利用者ＩＤを第２の認証局に送信し、第２の認証局は、利用者ＩＤの有効性を判定し、有効でないとき、認証装置を介して移動体を始動不可能にし、有効であるとき、第３の証明書を認証手段に送信し、認証手段は、第３の証明書を第２の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第３の証明書から利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、始動装置に供給し、始動装置は、ランダムデータと第２の識別データを結合して第３の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第５の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第２の識別データと、記憶しておいた第２の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、移動体を始動可能にすることを特徴とする。

請求項６に記載の移動体盗難防止プログラムは、情報を記憶する記憶手段と、認証処理を実行する認証手段と、移動体の作動を制御する制御手段と、移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防止プログラムであって、移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とを登録し、移動体の記憶手段に、第１の証明書と、第１の秘密鍵と、移動体を識別するための第１の識別データを登録し、移動体の作動を制御する制御手段に、第２の証明書と、第２の秘密鍵と、第１の識別データと、移動体を利用する利用者を識別するための第２の識別データを登録し、利用者が所持する始動装置に、第３の証明書と、第３の秘密鍵と、第２の識別データを登録し、認証手段に、第１の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第１の証明書から記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、記憶手段に供給する処理を実行させ、記憶手段に、ランダムデータと第１の識別データを結合して第１の秘密鍵でデジタル署名した署名データを認証手段に供給する処理を実行させ、認証手段に、第３の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第１の識別データを記憶する処理を実行させ、認証手段に、第２の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第２の証明書から制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、制御手段に供給する処理を実行させ、制御手段に、ランダムデータと第１の識別データと第２の識別データを結合して第２の秘密鍵でデジタル署名した署名データを認証手段に供給する処理を実行させ、認証手段に、第４の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第１の識別データと、記憶しておいた第１の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第２の識別データを記憶する処理を実行させ、認証手段に、第３の証明書を第２の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第３の証明書から利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、始動装置に供給する処理を実行させ、始動装置に、ランダムデータと第２の識別データを結合して第３の秘密鍵でデジタル署名した署名データを認証手段に供給する処理を実行させ、認証手段に、第５の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第２の識別データと、記憶しておいた第

２の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、移動体を始動可能にする処理を実行させることを特徴とする。

請求項７に記載の移動体盗難防止プログラムは、情報を記憶する記憶手段と、認証処理を実行する認証手段と、移動体の作動を制御する制御手段と、移動体を始動するための始動装置との通信を制御する通信手段とを備える移動体の改造および盗難を防止する移動体盗難防止プログラムであって、移動体の認証手段に、第１の認証局の第１の公開鍵と、第２の認証局の第２の公開鍵とを登録し、移動体の記憶手段に、第１の証明書と、第１の秘密鍵と、移動体を識別するための第１の識別データを登録し、移動体の作動を制御する制御手段に、第２の証明書と、第２の秘密鍵と、第１の識別データと、移動体を利用する利用者を識別するための第２の識別データを登録し、利用者が所持する始動装置に、利用者を識別するための利用者ＩＤと、第３の秘密鍵と、第２の識別データを登録し、認証手段に、第１の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第１の証明書から記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶する処理を実行させ、記憶手段に、ランダムデータと第１の識別データを結合して第１の秘密鍵でデジタル署名した署名データを認証手段に供給する処理を実行させ、認証手段に、第３の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第１の識別データを記憶する処理を実行させ、認証手段に、第２の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第２の証明書から制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、制御手段に供給する処理を実行させ、制御手段に、ランダムデータと第１の識別データと第２の識別データを結合して第２の秘密鍵でデジタル署名した署名データを認証手段に供給する処理を実行させ、認証手段に、第４の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第１の識別データと、記憶しておいた第１の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第２の識別データを記憶する処理を実行させ、始動装置に、利用者ＩＤを通信手段を介して認証手段に供給する処理を実行させ、認証手段に、利用者ＩＤを第２の認証局に送信する処理を実行させ、第２の認証局に、利用者ＩＤの有効性を判定し、有効でないとき、認証装置を介して移動体を始動不可能にし、有効であるとき、第３の証明書を認証手段に送信する処理を実行させ、認証手段に、第３の証明書を第２の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第３の証明書から利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、始動装置に供給する処理を実行させ、始動装置に、ランダムデータと第２の識別データを結合して第３の秘密鍵でデジタル署名した署名データを認証手段に供給する処理を実行させ、認証手段に、第５の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第２の識別データと、記憶しておいた第２の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、移動体を始動可能にする処理を実行させることを特徴とする。

【０００８】

【発明の実施の形態】

本発明は、移動体を始動する際に必要となる始動装置、移動体本体、移動体の作動を制御する電子制御ユニット（Ｅｌｅｃｔｒｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ、以下では適宜、ＥＣＵと記載する）に、それぞれデジタル証明書（以下では適宜、証明書と記載する）と、秘密鍵と、識別データを登録し、認証装置にメーカー、及び販売店がそれぞれ個別に発行した公開鍵を登録し、デジタル署名（以下では適宜、署名と記載する）されたデータを公開鍵暗号方式により検証することで、利用者の厳密個人認証を行い、運行制限を設けるとともに、移動体本体の改造を防ぐことにより、移動体の盗難防止をはかるものである。

【０００９】
本発明の原理図を図１に示す。移動体１３のメーカー１１、販売店１２はそれぞれ個別にデジタル証明書を発行する認証局（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ、以下では適宜、ＣＡと記載する）として機能し、メーカー（ＣＡ１）１１は、メーカー公開鍵１１１及びメーカー秘密鍵１１２と、本体公開鍵を含む本体証明書１１３及び本体秘密鍵１１４と、ＥＣＵ公開鍵を含むＥＣＵ証明書１１５及びＥＣＵ秘密鍵１１６と、本体識別データ１１７を発行し、販売店（ＣＡ２）１２は、販売店公開鍵１２１及び販売店秘密鍵１２２と、利用者公開鍵を含む利用者証明書１２３及び利用者秘密鍵１２４と、利用者識別データ１２５を発行し、移動体１３の製造、及び販売の時点で移動体１３を構成する認証装置１４、移動体本体１５、ＥＣＵ１６、始動通信装置１７にそれぞれ登録格納する。

【００１０】
即ち、メーカー公開鍵１１１と販売店公開鍵１２１は認証装置１４に登録格納され、本体公開鍵を含む本体証明書１１３、本体秘密鍵１１４、及び本体識別データ１１７は移動体本体１５に登録格納され、ＥＣＵ公開鍵を含むＥＣＵ証明書１１５、ＥＣＵ秘密鍵１１６、本体識別データ１１７、及び利用者識別データ１２５はＥＣＵ１６に登録格納され、利用者公開鍵を含む利用者証明書１２３と利用者秘密鍵１２４は始動装置１８に登録格納される。

【００１１】
移動体本体１５とＥＣＵ１６は、それぞれ登録された証明書と秘密鍵と識別データを保持し、認証装置１４から認証を受けて初めて使用可能となる。

【００１２】
認証装置１４は、移動体本体１５、及びＥＣＵ１６との間で登録された公開鍵を使用して認証処理を行い、その結果によりＥＣＵ１６を活性化、又は不活性化することで移動体１３の始動可否を制御する。

【００１３】
始動装置１８は、利用者証明書１２３と利用者秘密鍵１２４を保持し、利用者識別データ入力装置１８１を有する。

【００１４】
利用者が利用開始する時点で、認証装置１４は始動通信装置１７を介して始動装置１８との間で利用者の認証を行い、始動装置１８から送られてきた利用者識別データ１２５と、ＥＣＵ１６の保持する利用者識別データ１２５とが一致する場合、移動体１３を始動する。

【００１５】
このように、偽造できないデータを用いてメーカー１１、販売店１２、正規に組み合わされた移動体１３、及び利用者が全て認証されて初めて、移動体１３が始動可能となる。

【００１６】
図２は、本実施の形態の構成例を示すブロック図である。図２において、メーカー（ＣＡ１）２１、販売店（ＣＡ２）２２、移動体２３、認証装置２４、移動体本体２５、ＥＣＵ２６、始動通信装置２７、始動装置２８、利用者識別データ入力装置２２１、利用者識別データ入力装置２８２は、図１のメーカー１１、販売店１２、移動体１３、認証装置１４、移動体本体１５、ＥＣＵ１６、始動通信装置１７、始動装置１８、利用者識別データ入力装置１２６、利用者識別データ入力装置１８１にそれぞれ対応している。

【００１７】
メーカー２１は、移動体２３の製造、及びメーカー公開鍵１１１、メーカー秘密鍵１１２、本体証明書１１３、本体秘密鍵１１４、ＥＣＵ証明書１１５、ＥＣＵ秘密鍵１１６、本体識別データ１１７の発行登録と管理を行う。

【００１８】
販売店２２は、メーカー２１が製造した移動体２３を利用者に販売する際、メーカー２１が発行したものとは別に、販売店公開鍵１２１、販売店秘密鍵１２２、利用者証明書１２３、利用者秘密鍵１２４、及び利用者識別データ１２５の発行登録と管理を行う。

【００１９】
移動体２３は、認証装置２４、移動体本体２５、ＥＣＵ２６、始動通信装置２７により構成される。
【００２０】
認証装置２４に搭載されたＩＣチップ２４１には、メーカー２１が発行したメーカー公開鍵１１１と、販売店２２が発行した販売店公開鍵１２１がそれぞれ登録格納され、移動体本体２５に搭載されたＩＣチップ２５１には、メーカー２１が発行した本体証明書１１３と本体秘密鍵１１４と本体識別データ１１７が格納され、ＥＣＵ２６に搭載されたＩＣチップ２６１には、メーカー２１が発行したＥＣＵ証明書１１５とＥＣＵ秘密鍵１１６と本体識別データ１１７と販売店２２が発行した利用者識別データ１２５が格納される。
【００２１】
認証装置２４は、移動体本体２５のＩＣチップ２５１、及びＥＣＵ２６のＩＣチップ２６１、及び始動装置２８のＩＣチップ２８１との間で、格納された各証明書と署名データを送受信する機能を有し、始動通信装置２７を介して始動装置２８とデータを送受信する機能を有し、各証明書と各署名データを元に、各構成要素を認証する機能を有し、認証結果によりＥＣＵ２６を活性化、又は不活性化する機能を有する。
【００２２】
始動通信装置２７は、始動装置２８と認証装置２４の間で利用者に関するデータ通信を可能にする機能を有する。
【００２３】
始動装置２８は、利用者により所持管理され、移動体２３を始動する際に使用され、搭載されたＩＣチップ２８１は販売店２２が発行した利用者証明書１２３と利用者秘密鍵１２４を保持し、始動通信装置２７とデータ通信を可能にする機能を有し、利用者識別データを入力するための利用者識別データ入力装置２８２を有する。
【００２４】
移動体本体２５に搭載されたＩＣチップ２５１は、認証装置２４に本体証明書１１３を送信する機能を有する。また、認証装置２４から送信されたランダムデータと本体識別データ１１７を結合し、本体秘密鍵１１４で署名した署名データを認証装置２４に送信する機能を有する。
【００２５】
ＥＣＵ２５に搭載されたＩＣチップ２６１は、認証装置２４にＥＣＵ証明書１１５を送信する機能を有する。また、認証装置２４から送信されたランダムデータと、本体識別データ１１７と、利用者識別データ１２５とを結合し、ＥＣＵ秘密鍵１１６で署名した署名データを認証装置２４に送信する機能を有する。
【００２６】
始動装置２８に搭載されたＩＣチップ２８１は、認証装置２４に利用者証明書１２３を送信する機能を有する。また、利用者識別データ入力装置２８２から入力された利用者識別データ１２５を利用者秘密鍵１２４で署名し、始動通信装置２７を介して認証装置２４に送信する機能を有する。
【００２７】
ＩＣチップ２５１，２６１，２８１は、本体秘密鍵１１４、本体識別データ１１７、ＥＣＵ秘密鍵１１６、利用者識別データ１２５を直接読み出せない機能を有し、本体証明書１１３、本体秘密鍵１１４、ＥＣＵ証明書１１５、ＥＣＵ秘密鍵１１６、本体識別データ１１７は、移動体２３の製造時に、おのおの１個ずつ１回限り登録可能とする機能を有する。
【００２８】
利用者識別データ入力装置２８２は、利用者を一意に特定するための識別データを入力する機能を有する。販売店２２は、同じ方式でデータ入力を行う利用者識別データ入力装置２２１を有し、利用者識別データ１２５を生成する際に使用する。
【００２９】

移動体本体２５は、単一の部品で構成されるもの、或いは複数の部品で構成されるものであって良い。また、移動体本体２５が複数の部品で構成される場合、ＩＣチップがそれぞれの部品毎に搭載され、それぞれの部品がＥＣＵ２６、認証装置２４とデータを送受信する機能を有していても良い。

【００３０】

ＩＣチップ２８１は、複数の利用者を登録可能とするために、利用者識別データ１２５と利用者証明書１２３と利用者秘密鍵１２４の組み合わせを複数保持しても良く、また、再登録を可能としても良い。同様に、ＩＣチップ２６１は、利用者識別データ１２５を複数保持してもよく、再登録を可能としても良い。

【００３１】

また、各構成要素間のデータの送受信は、有線、又は無線のいずれの方式によっても良い。

【００３２】

本体識別データ１１７は、移動体１４の製造番号、動作音の声紋データなどの任意の形式、及び任意の長さで数値化されるデータを使用しても良い。

【００３３】

利用者識別データ１２５としては、パスワード方式、指紋、虹彩、声紋等の生体情報を利用する生体情報方式、動作パターン抽出方式などにより、利用者を特定するための識別情報が任意の形式、及び任意の長さで数値化されたデータを使用して良い。

【００３４】

ここで、デジタル証明書について説明しておく。一般的に、公開鍵はそれ単独で流通するのではなくデジタル証明書の形で流通する。デジタル証明書を入手すれば、このデジタル証明書から公開鍵を取り出して、対応する秘密鍵でデジタル署名された電子データの正当性を検証することができる。しかしながら、デジタル証明書自体が改竄、捏造されている可能性があるため、デジタル証明書を検証無しで無制限に信用することはできない（例えば、改竄されたデータを偽の秘密鍵で署名して、偽の公開鍵を含んだ証明書とともに送りつけられた場合など）。そこで、デジタル証明書はその正当性を保証するために、発行した認証局（ＣＡ）によってデジタル署名された署名データが含まれた形で作成される。

【００３５】

このデジタル証明書に対するデジタル署名は、ＣＡの秘密鍵によって行われるので、ＣＡの証明書を入手すれば、その証明書から取り出したＣＡ公開鍵により、誰でもデジタル証明書の検証を行うことができる。検証作業は、まず、デジタル証明書のうち、デジタル署名以外の部分（ここに公開鍵や発行者名などが含まれる）をＭＤ５やＳＨＡ－１などの一方向ハッシュ関数により、復号化不能な一定の長さのハッシュデータに変換する。次に、デジタル証明書に含まれるデジタル署名データをＣＡ公開鍵により復号化し、得られたデータを先に計算したハッシュデータと比較する。このとき、改竄されていれば、ハッシュ値は必ず変化するので、これにより証明書のいかなる部分も改竄や捏造がされていないことが確認できる。その際に使用すべきハッシュ関数や暗号／復号化方式は、デジタル証明書そのものに記述されている。

【００３６】

なお、当然、ＣＡ証明書そのものも検証しなければならないことがあるので、ＣＡ証明書をデジタル署名したルートＣＡのルートＣＡ証明書を使って検証する場合もあり得る。また、複数のルートＣＡがお互いを認証し合うこともある。このように、デジタル証明書はいくつもの中間証明機関やルート証明機関により階層的に正当性がチェックされる仕組みになっている。これらの仕組みは全て規約により標準化されている。

【００３７】

次に、図２の構成図、及び図３乃至図７のフローチャートを参照して、本実施の形態の動作について詳細に説明する。まず最初に、図３のフローチャートを参照して、メーカー２１の処理手順について説明する。メーカー２１は、まず、メーカー公開鍵１１１とメーカー秘密鍵１１２を生成する（ステップＳ３１）。次に、移動体２３を製造し（ステップＳ

３２）、移動体２３に組み込んだ認証装置２４のＩＣチップ２４１に、メーカー公開鍵１１１を格納し（ステップＳ３３）、移動体２３の本体識別データ１１７を生成する（ステップＳ３４）。

【００３８】

メーカー２１は、さらに本体公開鍵と本体秘密鍵１１４を生成し（ステップＳ３５）、本体公開鍵を元に、メーカー秘密鍵１１２で署名した本体公開鍵を含む本体証明書１１３を発行し（ステップＳ３６）、本体証明書１１３と本体秘密鍵１１４を、本体識別データ１１７とともに移動体本体２５のＩＣチップ２５１に格納する（ステップＳ３７）。次に、ＥＣＵ公開鍵とＥＣＵ秘密鍵１１６を生成し（ステップＳ３８）、同様に、ＥＣＵ公開鍵を元に、メーカー秘密鍵１１２で署名したＥＣＵ公開鍵を含むＥＣＵ証明書１１５を発行し（ステップＳ３９）、ＥＣＵ証明書１１５とＥＣＵ秘密鍵１１６を、本体識別データ１１７とともにＥＣＵ２６のＩＣチップ２６１に格納する（ステップＳ３ａ）。

【００３９】

また、メーカー２１は、生成した全ての鍵ペア（メーカー公開鍵１１１とメーカー秘密鍵１１２、本体公開鍵と本体秘密鍵１１４、ＥＣＵ公開鍵とＥＣＵ秘密鍵１１６）、本体識別データ１１７、各種証明書（本体証明書１１３、ＥＣＵ証明書１１５）を保存して、保守用に備えることができる。

【００４０】

また、移動体本体２５が、複数のモジュールで構成される場合、本体証明書１１３と本体秘密鍵１１４を個別に発行しても良い。

【００４１】

次に、図４のフローチャートを参照して、販売店１２の処理手順について説明する。メーカー２１から移動体２３の供給を受けた販売店２２は、まず、販売店公開鍵１２１と販売店秘密鍵１２２を生成する（ステップＳ４１）。

【００４２】

次に、認証装置２４のＩＣチップ２４１に、販売店公開鍵１２１を格納し（ステップＳ４２）、移動体２３を運行する利用者の数（＝ｎ（ｎは任意の自然数））だけ利用者証明書１２３と利用者秘密鍵１２４を発行し、始動装置２８に格納する（ステップＳ４４乃至ステップＳ４ａ）。

【００４３】

次に、ステップＳ４４乃至ステップＳ４ａの手順について詳細に説明する。まず、ステップＳ４４において、利用者数（＝ｎ）が０より多いか否かが判定される。その結果、利用者数が０より多いと判定された場合、ステップＳ４５に進む。一方、利用者数が０であると判定された場合、処理を終了する。

【００４４】

ステップＳ４５においては、利用者識別データ入力装置２２１から利用者固有の情報を入力して利用者識別データ１２５を生成し、その利用者に対応する利用者公開鍵と利用者秘密鍵１２４を生成し（ステップＳ４６）、利用者公開鍵を含み、販売店秘密鍵１２２で署名した利用者証明書１２３を発行する（ステップＳ４７）。また、利用者識別データ１２５をＥＣＵ２６のＩＣチップ２６１に格納し（ステップＳ４８）、利用者証明書１２３と利用者秘密鍵１２４を始動装置２８のＩＣチップ２８１に格納する（ステップＳ４９）。次に、ステップＳ４ａにおいて、利用者数（＝ｎ）を１だけデクリメントし、ステップＳ４４に戻る。その後、ｎの値が０になるまで、即ち、利用者の数だけ、各利用者について、ステップＳ４４以降の処理が繰り返し実行される。

【００４５】

次に、図５のフローチャートを参照して、移動体２３を始動するまでの認証動作について説明する。図５は、移動体本体２５の認証手順を示すフローチャートである。

【００４６】

移動体２３に、運行に必要なバッテリーを接続するなどして通電した（ステップＳ５１）時点で、移動体本体２５は、認証装置２４に本体証明書１１３を送信する（ステップＳ５

２）。認証装置２４は、受信した本体証明書１１３を自身の保持するメーカー公開鍵１１１で検証を行い（ステップＳ５３）、検証失敗なら移動体２３を始動不能にする（ステップＳ５４のＮＯ）。

【００４７】

一方、検証成功すると、次に、認証装置２４は、本体証明書１１３から取り出した本体公開鍵を記憶しておき（ステップＳ５５）、任意長のランダムデータを生成、記憶し（ステップＳ５６）、このランダムデータを移動体本体２５に送信する（ステップＳ５７）。

【００４８】

移動体本体２５は、受信したランダムデータと本体識別データ１１７を結合し（ステップＳ５８）、結合データを本体秘密鍵１１４で署名し（ステップＳ５９）、署名データを認証装置２４に送信する（ステップＳ５ａ）。認証装置２４は、受信した署名データをステップＳ５５において記憶しておいた本体公開鍵でデコードし（ステップＳ５ｂ）、その結果得られた結合データのうち、ランダムデータ部分とステップＳ５６で記憶しておいたランダムデータを比較する（Ｓ５ｃ）。比較の結果、両者が一致しなければ認証失敗となり（Ｓ５ｄのＮＯ）、移動体２３を始動不能にする。一方、両者が一致したら（Ｓ５ｄのＹＥＳ）、結合データのうち、本体識別データ１１７を記憶しておく（Ｓ５ｅ）。その後、処理を終了する。

【００４９】

次に、図６のフローチャートを参照して、ＥＣＵ認証手順について説明する。図６は、ＥＣＵを認証する認証手順を示すフローチャートである。移動体２３に、運行に必要なバッテリーを接続するなどして通電した時点で、ＥＣＵ２６は認証装置２４にＥＣＵ証明書１１５を送信する（ステップＳ６１）。認証装置２４は、受信したＥＣＵ証明書１１５を自身の保持するメーカー公開鍵１１１で検証を行い（ステップＳ６２）、検証失敗なら移動体を始動不能にする（ステップＳ６３のＮＯ）。

【００５０】

一方、検証成功ならば（ステップＳ６３のＹＥＳ）、次に、ＥＣＵ証明書１１５から取り出したＥＣＵ公開鍵を記憶しておき（ステップＳ６４）、任意長のランダムデータを生成、記憶し（ステップＳ６５）、ランダムデータをＥＣＵ２６に送信する（ステップＳ６６）。

【００５１】

ＥＣＵ２６は、受信したランダムデータと本体識別データ１１７と利用者識別データ１２５を結合し（ステップＳ６７）、結合データをＥＣＵ秘密鍵１１６で署名し（ステップＳ６８）、署名データを認証装置２４に送信する（ステップＳ６９）。認証装置２４は、受信した署名データをステップＳ６４で記憶しておいたＥＣＵ公開鍵でデコードし（ステップＳ６ａ）、その結果得られた結合データのうち、ランダムデータ部分とステップＳ６５で記憶しておいたランダムデータを比較する（ステップＳ６ｂ）。

【００５２】

その結果、両者が一致しなければ認証失敗となり（ステップＳ６ｃのＮＯ）、移動体２３を始動不能にする。一方、両者が一致したら（ステップＳ６ｃのＹＥＳ）、結合データのうち、本体識別データ１１７をステップＳ５ｅで記憶した本体識別データ１１７と比較する（ステップＳ６ｄ）。その結果、両者が一致しなければ、認証失敗となり（ステップＳ６ｅのＮＯ）、移動体２３を始動不能にする。一方、両者が一致したら、結合データのうち、利用者識別データ１２５を記憶しておく（ステップＳ６ｆ）。

【００５３】

図７は、利用者を認証する手順を示すフローチャートである。利用者は、始動装置２８を移動体２３の始動通信装置２７に接続すると（ステップＳ７１）、利用者識別データ入力装置２８２は、利用者識別データ１２５を読み込んで記憶し（ステップＳ７２）、始動装置２８は、利用者証明書１２３を始動通信装置２７を介して認証装置２４に送信する（ステップＳ７３）。認証装置２４は、受信した利用者証明書１２３を自身の保持する販売店公開鍵１２１で検証を行い（ステップＳ７４）、検証失敗なら（ステップＳ７５のＮＯ）

、移動体２３を始動不能にする。
【００５４】
一方、検証成功すると（ステップＳ７５のＹＥＳ）、次に、認証装置２４は、利用者証明書１２３から取り出した利用者公開鍵を記憶しておき（ステップＳ７６）、任意長のランダムデータを生成、記憶し（ステップＳ７７）、ランダムデータを始動装置２８に送信する（ステップＳ７８）。
【００５５】
始動装置２８は、受信したランダムデータとステップＳ７２で読み込んだ利用者識別データ１２５を結合し（ステップＳ７９）、結合データを利用者秘密鍵１２４で署名し（ステップＳ７ａ）、署名データを認証装置２４に送信する（ステップＳ７ｂ）。
【００５６】
認証装置２４は、受信した署名データをステップＳ７６で記憶しておいた利用者公開鍵でデコードし（ステップＳ７ｃ）、その結果得られた結合データのうち、ランダムデータ部分とステップＳ７７で記憶しておいたランダムデータを比較する（ステップＳ７ｄ）。その結果、両者が一致しなければ認証失敗となり（ステップＳ７ｅのＮＯ）、移動体２３を始動不能にする。一方、両者が一致したら（ステップＳ７ｅのＹＥＳ）、結合データのうち、利用者識別データ１２５をステップＳ６ｆで記憶した利用者識別データ１２５と比較する（ステップＳ７ｆ）。
【００５７】
その結果、両者が一致しなければ認証失敗となり（ステップＳ７ｇのＮＯ）、移動体２３を始動不能にする。一方、両者が一致したら（ステップＳ７ｇのＹＥＳ）、移動体２３を始動可能状態にする（ステップＳ７ｈ）。その後、処理を終了する。
【００５８】
図５のフローチャートを参照して上述した移動体本体２５の認証と、図６のフローチャートを参照して上述したＥＣＵ２６の認証は、任意の順に実施して良い。その場合、本体識別データ１１７は、一番最初に実施された認証手順で記憶されれば良い。また、移動体本体２５、及びＥＣＵ２６の認証は、利用者が始動装置２８を接続した時点で認証を開始しても良い。
【００５９】
本実施の形態は、例えば、乗用自動車、建設機械、飛行機、電車、船舶などの移動体と、メーカーと、運行利用者の関係に適用が可能である。
【００６０】
また、移動体以外の、特定の利用者にのみ操作を許可する据え付け型の機械にも適用可能である。
【００６１】
本実施の形態により、次のような効果を得ることができる。第１の効果は、移動体２３を運行利用できる利用者を特定することにより、移動体２３の不正な使用を抑制することができることである。その理由は、証明書を用いた厳密個人認証により、始動装置２８の偽造、利用者のなりすましが不可能であり、始動装置２８の偽造も販売店２２の保持する鍵ペア無しでは不可能だからである。
【００６２】
第２の効果は、移動体２３の構成要素の盗難再利用を不能にすることができることである。その理由は、移動体本体２５、及びＥＣＵ２６を一意に特定する証明書を用いた認証により、他の移動体の構成要素と組み合わせても使用不能になるからである。
【００６３】
図８は、本発明を応用した他の実施の形態の原理図を示している。図９は本発明を応用した他の実施の形態の構成例を示している。図１０、図１１は、本発明を応用した他の実施の形態の認証手順を示すフローチャートである。以下、図８乃至図１１を参照して、本発明を応用した他の実施の形態の構成及び動作について詳細に説明する。
【００６４】

図８のメーカー８１、販売店８２、移動体８３、認証装置８４、移動体本体８５、ＥＣＵ８６、始動通信装置８７、始動装置８８、利用者識別データ入力装置８２６、利用者識別データ入力装置８８１は、図１のメーカー１１、販売店１２、移動体１３、認証装置１４、移動体本体１５、ＥＣＵ１６、始動通信装置１７、始動装置１８、利用者識別データ入力装置１２６、利用者識別データ入力装置１８１にそれぞれ対応している。

【００６５】

また、図９のメーカー９１、販売店９２、移動体９３、認証装置９４、移動体本体９５、ＥＣＵ９６、始動通信装置９７、始動装置９８、利用者識別データ入力装置９２１、利用者識別データ入力装置９８２は、図８のメーカー８１、販売店８２、移動体８３、認証装置８４、移動体本体８５、ＥＣＵ８６、始動通信装置８７、始動装置８８、利用者識別データ入力装置８２６、利用者識別データ入力装置８８１にそれぞれ対応している。

【００６６】

また、図９のメーカー公開鍵８１１、メーカー秘密鍵８１２、本体証明書８１３、本体秘密鍵８１４、ＥＣＵ証明書８１５、ＥＣＵ秘密鍵８１６、本体識別データ８１７、販売店公開鍵８２１、販売店秘密鍵８２２、利用者証明書８２３、利用者秘密鍵８２４、利用者識別データ８２５は、図１のメーカー公開鍵１１１、メーカー秘密鍵１１２、本体証明書１１３、本体秘密鍵１１４、ＥＣＵ証明書１１５、ＥＣＵ秘密鍵１１６、本体識別データ１１７、販売店公開鍵１２１、販売店秘密鍵１２２、利用者証明書１２３、利用者秘密鍵１２４、利用者識別データ１２５にそれぞれ対応している。

【００６７】

そして、図８及び図９に示した実施の形態の場合、図１に示した認証装置１４のＩＣチップ２４１に格納されるメーカー公開鍵１１１と販売店公開鍵１２１に加えて、移動体本体８５の場合と同様に、本体証明書８１３（本体証明書１１３に対応する）と本体秘密鍵８１４（本体秘密鍵１１４に対応する）と本体識別データ８１７（本体識別データ１１７に対応する）が認証装置８４のＩＣチップ９４１（図９）に格納される点が異なる。

【００６８】

また、ＩＣチップ９４１は、認証装置９４により生成され、転送されてきたランダムデータと本体識別データ８１７を結合し、本体秘密鍵８１４で署名した署名データを認証装置９４に転送する機能を有する点が異なる。また、図１において、始動装置１８に格納される利用者証明書１２３の代わりに、利用者ＩＤ８２６が始動装置８８に格納される点が異なる。さらに、図２に示された販売店２２の利用者識別データ入力装置２２１に加えて、利用者ＩＤ／証明書送受信装置９２２が販売店９２に備わる点が異なる。

【００６９】

また、新たに利用者ＩＤ／証明書送受信装置９４２が認証装置９４に備わる点が異なる。また、利用者ＩＤ／証明書送受信装置９２２、及び利用者ＩＤ／証明書送受信装置９４２は、販売店９２と認証装置９４の間で利用者ＩＤ８２６、及び対応する利用者証明書８２３を無線や有線などの任意の伝送手段を介して送受信する機能を有する。

【００７０】

次に、本実施の形態の動作について説明する。本実施の形態においては、図５のフローチャートを参照して上述した移動体本体８５の認証過程に加えて、図１０のフローチャートに示した認証手順により、認証装置８４が自身の認証を行うことで、認証装置８４の正当性を検証する処理が追加される。

【００７１】

以下、図１０のフローチャートを参照して、認証装置８５の認証手順について説明する。移動体９３に、運行に必要なバッテリーを接続するなどして通電した（ステップＳ１１１）時点で、認証装置９４に搭載されたＩＣチップ９４１内の本体証明書８１３を認証装置９４に転送する（ステップＳ１１２）。認証装置９４は、転送されてきた本体証明書８１３を自身の保持するメーカー公開鍵８１１で検証を行い（ステップＳ１１３）、検証失敗なら移動体９３を始動不能にする（ステップＳ１１４のＮＯ）。

【００７２】

一方、検証成功すると（ステップＳ１１４のＹＥＳ）、次に、認証装置９４は、本体証明書８１３から取り出した本体公開鍵を記憶しておき（ステップＳ１１５）、任意長のランダムデータを生成、記憶し（ステップＳ１１６）、このランダムデータを認証装置９４に搭載されたＩＣチップ９４１に転送する（ステップＳ１１７）。

【００７３】

認証装置９４に搭載されたＩＣチップ９４１は、転送されてきたランダムデータと本体識別データ８１７を結合し（ステップＳ１１８）、結合データを本体秘密鍵８１４で署名し（ステップＳ１１９）、署名データを認証装置９４に転送する（ステップＳ１１ａ）。認証装置９４は、転送されてきた署名データをステップＳ１１５において記憶しておいた本体公開鍵でデコードし（ステップＳ１１ｂ）、その結果得られた結合データのうち、ランダムデータ部分とステップＳ１１６で記憶しておいたランダムデータを比較する（Ｓ１１ｃ）。比較の結果、両者が一致しなければ認証失敗となり（Ｓ１１ｄのＮＯ）、移動体２３を始動不能にする。一方、両者が一致したら（Ｓ１１ｄのＹＥＳ）、結合データのうち、本体識別データ８１７を記憶しておく（Ｓ１１ｅ）。その後、処理を終了する。

【００７４】

また、利用者の認証については、図４のフローチャートを参照して上述した利用者登録手順とは異なり、販売店８２は、移動体８３を販売したときに、利用者証明書８２３を発行するとともに、対応する利用者ＩＤ８２６を発行し、利用者証明書８２３に代えて始動装置８８に格納しておく。

【００７５】

図１１は、利用者を認証する手順を示すフローチャートである。利用者は始動装置９８を移動体９３の始動通信装置９７に接続すると（ステップＳ１０１）、利用者識別データ入力装置９８２は入力された利用者識別データ８２５を読み込んで記憶し（ステップＳ１０２）、始動装置９８は、認証装置９４に利用者ＩＤ８２６を送信する（ステップＳ１０３）。認証装置９４は、受信した利用者ＩＤ８２６を利用者ＩＤ／証明書送受信装置９４２を使用して販売店９２に送信する（ステップＳ１０４）。

【００７６】

販売店９２は、利用者ＩＤ／証明書送受信装置９２２を介して受信した利用者ＩＤ８２６の有効性をチェックし、有効な利用者ＩＤと認められない場合（ステップＳ１０５のＮＯ）は、利用者ＩＤ／証明書送受信装置９２２から受信した利用者ＩＤ８２６をそのまま移動体９３の認証装置９４に送信して返す（ステップＳ１０６）。この場合、利用者の認証は失敗となり、認証装置９４は移動体９３を始動不能にする。

【００７７】

一方、販売店９２が、受信した利用者ＩＤ８２６を有効な利用者ＩＤと認めると（ステップＳ１０５のＹＥＳ）、次に、利用者ＩＤ／証明書送受信装置９２２から利用者証明書８２３を移動体９３の認証装置９４に送信して返す（ステップＳ１０７）。利用者証明書８２３を利用者ＩＤ／証明書送受信装置９４２を介して受信した認証装置９４は、自身の保持する販売店公開鍵８２１で検証を行い（ステップＳ１０８）、検証失敗なら（ステップＳ１０９のＮＯ）、移動体９３を始動不能にする。

【００７８】

一方、検証成功すると（ステップＳ１０９のＹＥＳ）、以下、説明は省略するが、図７のフローチャートのステップＳ７６に続く利用者認証処理を継続して行う。その後、処理を終了する。

【００７９】

本実施の形態は、移動体９３に加えて、認証装置９４自身の改竄を防ぐことができるという効果を有する。また、利用者証明書８２３を販売店９２から取得するようにすることにより、盗難届が販売店９２に通知された時点で、販売店９２は盗難に遭った利用者の利用者ＩＤ８２６に対応する利用者証明書８２３を移動体９３に送信しないようにして、その利用者ＩＤ８２６を無効にすることができるという効果も有する。さらに、利用者ＩＤ８２６の送受信の際に、ＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）

の位置情報を含めるようにすることも可能であり、移動体９３の地理的な利用制限を行うことができるという新たな効果も有する。

【００８０】

なお、上記実施の形態の構成及び動作は例であって、本発明の趣旨を逸脱しない範囲で適宜変更することができることは言うまでもない。

【００８１】

【発明の効果】

以上の如く、本発明に係る移動体セキュリティシステムによれば、認証手段は、第１の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第１の証明書から記憶手段の第３の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、記憶手段に供給し、記憶手段は、ランダムデータと第１の識別データを結合して第１の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第３の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第１の識別データを記憶し、認証手段は、第２の証明書を第１の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第２の証明書から制御手段の第４の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、制御手段に供給し、制御手段は、ランダムデータと第１の識別データと第２の識別データを結合して第２の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第４の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第１の識別データと、記憶しておいた第１の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、第２の識別データを記憶し、認証手段は、第３の証明書を第２の公開鍵で検証し、検証が失敗したとき、移動体の始動を不可能にし、検証が成功したとき、第３の証明書から利用者の第５の公開鍵を取得して記憶し、所定のランダムデータを生成、記憶し、始動装置に供給し、始動装置は、ランダムデータと第２の識別データを結合して第３の秘密鍵でデジタル署名した署名データを認証手段に供給し、認証手段は、第５の公開鍵でデジタル署名された署名データをデコードし、得られたランダムデータと、記憶しておいたランダムデータとを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、得られた第２の識別データと、記憶しておいた第２の識別データを比較し、一致しないとき、移動体の始動を不可能にし、一致するとき、移動体を始動可能にするようにしたので、移動体を運行利用可能な利用者を特定することができ、移動体の不正使用を抑制することができる。また、移動体の構成要素を改竄したり、不正に再利用することを抑制することができる。

【図面の簡単な説明】

【図１】本発明が適用される実施の形態の原理図である。

【図２】本発明が適用される実施の形態の構成例を示すブロック図である。

【図３】メーカーの処理手順を説明するためのフローチャートである。

【図４】販売店の処理手順を説明するためのフローチャートである。

【図５】移動体本体を認証する手順を説明するためのフローチャートである。

【図６】ＥＣＵを認証する手順を説明するためのフローチャートである。

【図７】利用者を認証する手順を説明するためのフローチャートである。

【図８】本発明が適用される他の実施の形態の原理図である。

【図９】本発明が適用される他の実施の形態の構成例を示すブロック図である。

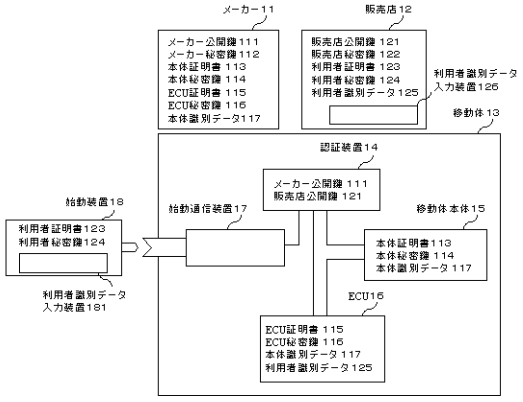
【図１０】図８及び図９に示した実施の形態において認証装置を認証する手順を説明するためのフローチャートである。

【図１１】図８及び図９に示した実施の形態において利用者を認証する手順を説明するためのフローチャートである。

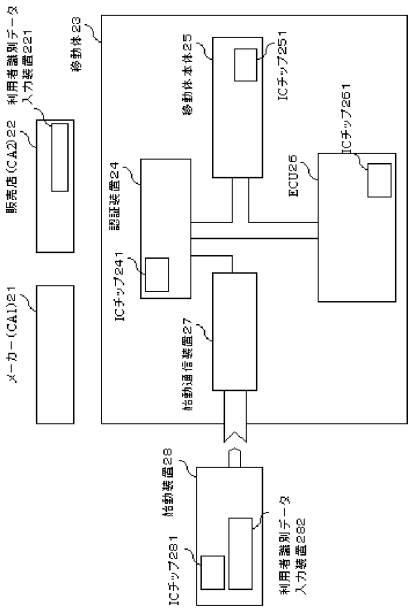
【符号の説明】

１１，２１，８２，９２　メーカー（ＣＡ１）
１２，２２，８２，９２　販売店（ＣＡ２）
１３，２３，８３，９３　移動体
１４，２４，８４，９４　認証装置
１５，２５，８５，９５　移動体本体
１６，２６，８６，９６　ＥＣＵ
１７，１７，８７，９７　始動通信装置
１８，２８，８８，９８　始動装置
１２５，１８１，２２１，２８２　８２５，８８１，９２１，９８２　利用者識別データ入力装置
２４１，２５１，２６１，２８１，９４１，９５１，９６１，９８１　ＩＣチップ
９２２，９４２　利用者ＩＤ／証明書送受信装置
１１，８１１　メーカー公開鍵
１１２，８１２　メーカー秘密鍵
１１３，８１３　本体証明書
１１４，８１４　本体秘密鍵
１１５，８１５　ＥＣＵ証明書
１１６，８１６　ＥＣＵ秘密鍵
１１７，８１７　本体識別データ
１２１，８２１　販売店公開鍵
１２２，８２２　販売店秘密鍵
１２３，８２３　利用者証明書
１２４，８２４　利用者秘密鍵
１２５，８２５　利用者識別データ

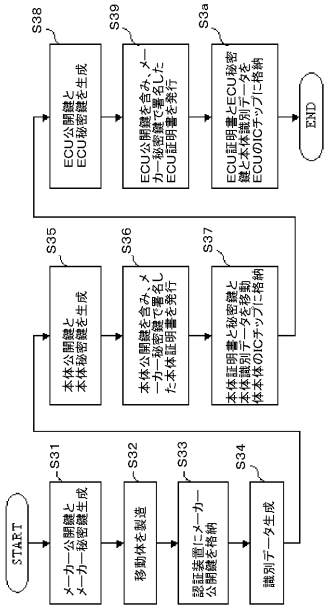
【図１】



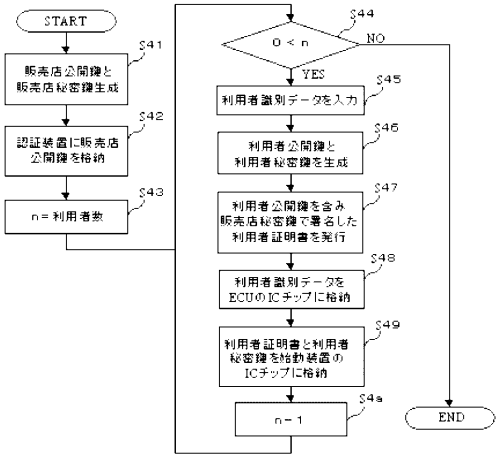
【図２】



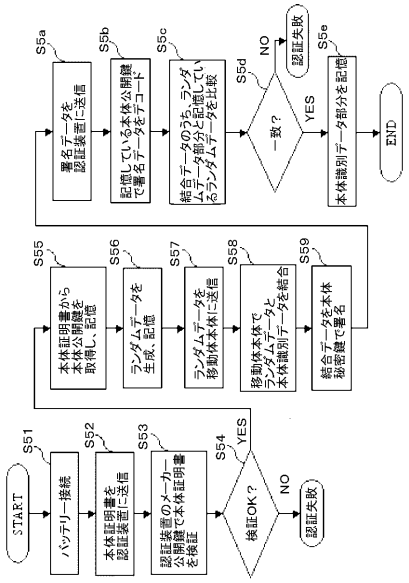
【図３】


START
メーカー公開鍵と
メーカー秘密鍵生成
S31
移動体を製造
S32
認証装置にメーカー
公開鍵を格納
S33
識別データ生成
S34
本体公開鍵と
本体秘密鍵を生成
S35
本体公開鍵を含み、メ
ーカー秘密鍵で署名し
た本体証明書を発行
S36
本体証明書と秘密鍵と
本体識別データを移動
体本体のICチップに格納
S37
ECU公開鍵と
ECU秘密鍵を生成
S38
ECU公開鍵を含み、メー
カー秘密鍵で署名した
ECU証明書を発行
S39
ECU証明書とECU秘密
鍵と本体識別データを
ECUのICチップに格納
S3a
END

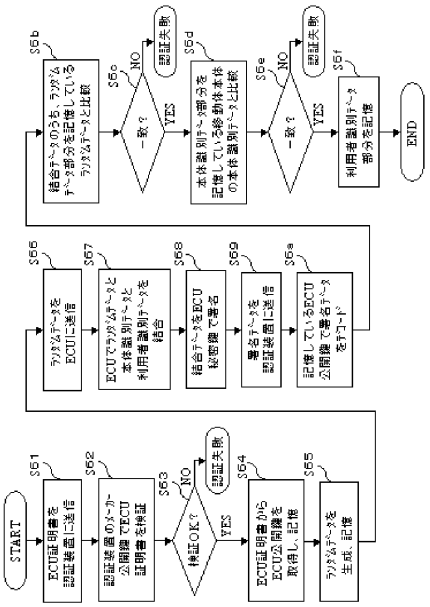
【図４】


START
販売店公開鍵と
販売店秘密鍵生成
S41
認証装置に販売店
公開鍵を格納
S42
n＝利用者数
S43
0 < n
S44
NO
YES
利用者識別データを入力
S45
利用者公開鍵と
利用者秘密鍵を生成
S46
利用者公開鍵を含み
販売店秘密鍵で署名した
利用者証明書を発行
S47
利用者識別データを
ECUのICチップに格納
S48
利用者証明書と利用者
秘密鍵を移動装置の
ICチップに格納
S49
n－1
S4a
END

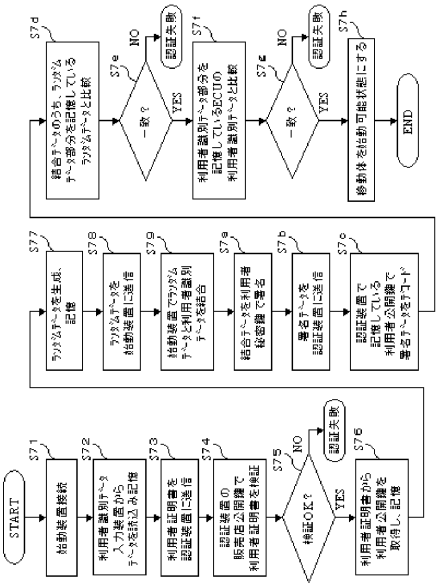
【図５】


START
バッテリー接続
S51
本体証明書を
認証装置に送信
S52
認証装置でメーカー公開鍵で本体証明書
を検証
S53
検証OK？
S54
YES
NO
認証失敗
本体公開鍵と
本体秘密鍵を取得し、記憶
S55
ランダムデータを
生成、記憶
S56
ランダムデータを
移動体本体に送信
S57
移動体本体で
ランダムデータと
本体識別データを結合
S58
結合データを本体
秘密鍵で署名
S59
署名データを
認証装置に送信
S5a
記憶している本体公開鍵
で署名データをデコード
S5b
結合データのうち、ランダ
ムデータ部分と記憶してい
るランダムデータを比較
S5c
一致？
S5d
NO
YES
認証失敗
本体識別データ部分を記憶
S5e
END

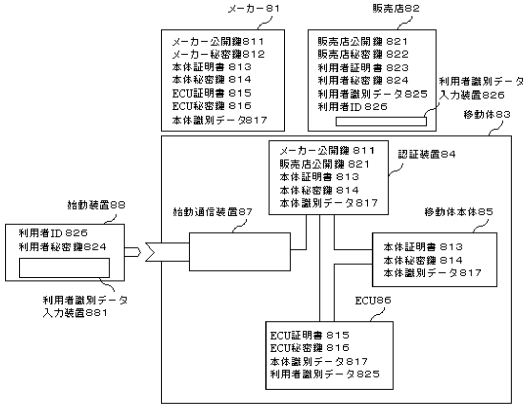
【図６】


START
ECU証明書を
認証装置に送信
S61
認証装置のメーカー
公開鍵でECU
証明書を検証
S62
検証OK？
S63
YES
NO
認証失敗
ECU証明書から
ECU公開鍵を
取得し、記憶
S64
ランダムデータを
生成、記憶
S65
ランダムデータを
ECUに送信
S66
ECUでランダムデータと
本体識別データと
利用者識別データを
結合
S67
結合データを
ECU
秘密鍵で署名
S68
署名データを
認証装置に送信
S69
記憶している
ECU
公開鍵で署名データ
をデコード
S6a
結合データのうち、ランダム
データ部分を記憶している
ランダムデータと比較
S6b
一致？
S6c
NO
YES
認証失敗
本体識別データ部分を記憶
している移動体本体
の本体識別データと比較
S6d
一致？
S6e
NO
YES
認証失敗
利用者識別データ
部分を記憶
S6f
END

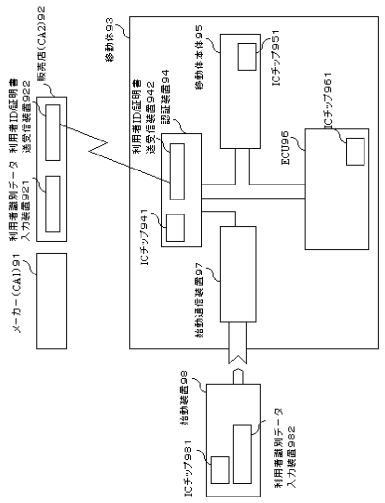
【図７】


START
始動装置接続
利用者識別データ入力装置から データを読込み記憶
利用者証明書を認証装置に送信
認証装置の販売店公開鍵で利用者証明書を検証
検証OK？
NO
認証失敗
YES
利用者証明書から利用者公開鍵を取得し、記憶
ランダムデータを生成、記憶
ランダムデータを始動装置に送信
始動装置でランダムデータと利用者識別データを結合
結合データを利用者秘密鍵で署名
署名データを認証装置に送信
認証装置で記憶している利用者公開鍵で署名データをデコード
結合データのうち、ランダムデータ部分を記憶しているECUの利用者識別データと比較
一致？
NO
認証失敗
YES
利用者識別データ部分を記憶している本体識別データと比較
一致？
NO
認証失敗
YES
移動体を始動可能状態にする
END

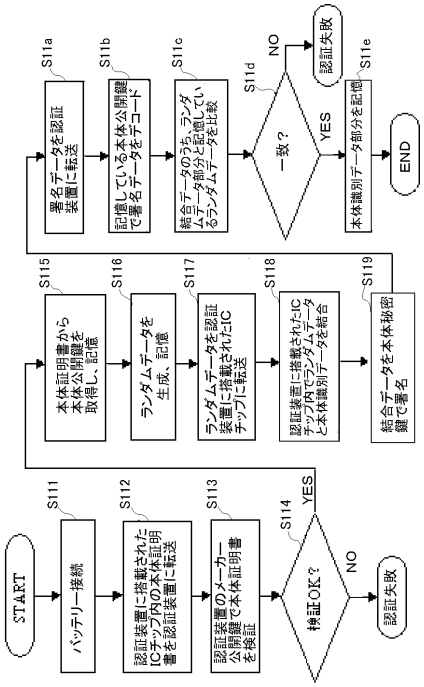
【図８】


メーカー81
メーカー公開鍵811
メーカー秘密鍵812
本体証明書813
本体秘密鍵814
ECU証明書815
ECU秘密鍵816
本体識別データ817
販売店82
販売店公開鍵821
販売店秘密鍵822
利用者証明書823
利用者秘密鍵824
利用者識別データ825
利用者ID826
利用者識別データ入力装置826
移動体83
メーカー公開鍵811
販売店公開鍵821
本体証明書813
本体秘密鍵814
本体識別データ817
認証装置84
移動体本体85
本体証明書813
本体秘密鍵814
本体識別データ817
ECU85
ECU証明書815
ECU秘密鍵816
本体識別データ817
利用者識別データ825
始動装置88
利用者ID825
利用者秘密鍵824
利用者識別データ入力装置881
始動通信装置87

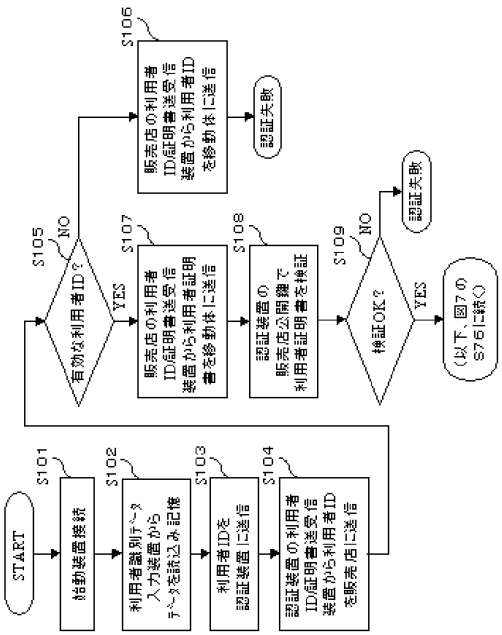
【図９】


メーカー(CA1)91
利用者識別データ入力装置921
利用者ID証明書送受信装置922
販売店(CA2)92
移動体93
利用者ID証明書送受信装置942
認証装置94
移動体本体95
ICチップ951
ECU96
ICチップ961
ICチップ941
始動通信装置97
始動装置98
ICチップ981
利用者識別データ入力装置982

【図１０】


START
S111
バッテリー接続
S112
認証装置に搭載された ICチップ内の本体証明書を認証装置に転送
S113
認証装置のメーカー公開鍵で本体証明書を検証
S114
検証OK？
YES
NO
認証失敗
S115
本体証明書から本体公開鍵を取得、記憶
S116
ランダムデータを生成、記憶
S117
ランダムデータを認証装置に搭載されたICチップに転送
S118
認証装置に搭載されたICチップ内でランダムデータと本体識別データを結合
S119
結合データを本体秘密鍵で署名
S11a
署名データを認証装置に転送
S11b
記憶している本体公開鍵で署名データをデコード
S11c
結合データのうち、ランダムデータ部分と記憶しているランダムデータを比較
S11d
一致？
NO
認証失敗
YES
本体識別データ部分を記憶
S11e
END

【図１１】


START
S101
始動装置接続
S102
利用者識別データ入力装置からデータを読込み記憶
S103
利用者IDを認証装置に送信
S104
認証装置の利用者ID/証明書送受信装置から利用者IDを販売店に送信
S105
有効な利用者ID？
NO
YES
S106
販売店の利用者ID/証明書送受信装置から利用者IDを移動体に送信
認証失敗
S107
販売店の利用者ID/証明書送受信装置から利用者証明書を移動体に送信
S108
認証装置の販売店公開鍵で利用者証明書を検証
S109
検証OK？
NO
認証失敗
YES
（以下、図7のS751に続く）

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)

H04L 9/32

E05B 49/00

E05B 65/12