(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7145749号
(P7145749)

(45)発行日　令和4年10月3日(2022.10.3)

(24)登録日　令和4年9月22日(2022.9.22)

(51)国際特許分類			FI		
G06F	*21/62*	*(2013.01)*	G06F	21/62	
G06F	*21/31*	*(2013.01)*	G06F	21/31	
B60R	*16/02*	*(2006.01)*	B60R	16/02	660U
			B60R	16/02	660W

請求項の数　8　（全23頁）

(21)出願番号　特願2018-242136(P2018-242136)
(22)出願日　平成30年12月26日(2018.12.26)
(65)公開番号　特開2020-106888(P2020-106888A)
(43)公開日　令和2年7月9日(2020.7.9)
審査請求日　令和3年9月24日(2021.9.24)

(73)特許権者　000005348
株式会社ＳＵＢＡＲＵ
東京都渋谷区恵比寿一丁目２０番８号
(74)代理人　110001357弁理士法人つばさ国際特許事務所
(72)発明者　中曽　善朗
東京都渋谷区恵比寿一丁目２０番８号
株式会社ＳＵＢＡＲＵ内
審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】　データ検証装置

(57)【特許請求の範囲】

【請求項１】

第１のデータおよび第１のステータス情報を記憶する第１の記憶部と、第２のデータおよび第２のステータス情報を記憶する第２の記憶部とを有する記憶部と、

外部装置との間の通信により取得したデータに基づいて前記第１の記憶部に前記第１のデータを書き込んだ後に前記データに基づいて前記第２の記憶部に前記第２のデータを書き込む書込プロセスを制御するとともに、前記書込プロセスに応じて前記第１のステータス情報および前記第２のステータス情報を更新する管理部と、

前記通信が切断された状態において、前記第１のステータス情報および前記第２のステータス情報に基づいて前記第１のデータおよび前記第２のデータを検証する検証部と

を備え、

前記管理部は、

前記第１のデータを前記第１の記憶部に書き込む前に、前記第１のステータス情報を第１のステータスに設定し、

前記第１のデータを前記第１の記憶部に書き込んだ後に、前記第１のステータス情報を第２のステータスに設定し、

前記第２のデータを前記第２の記憶部に書き込み、前記第２の記憶部における前記第２のデータと、前記第１の記憶部における前記第１のデータとが一致した場合に、前記第１のステータス情報を第３のステータスに設定する

データ検証装置。

【請求項２】
　前記検証部は、前記通信が切断された状態において、前記第１のステータス情報、および前記第２のステータス情報に基づいて、前記書込プロセスが中断しているかどうかを確認し、前記書込プロセスが中断している場合には、どの段階で中断しているのかを確認し、それらの確認結果に基づいて前記第１のデータおよび前記第２のデータを検証する
　請求項１に記載のデータ検証装置。
【請求項３】
　前記検証部は、前記通信が切断された状態において、前記確認結果、前記第１のデータ、および前記第２のデータに基づいて、前記第１のデータおよび前記第２のデータのそれぞれに対して、データ不正または書込異常を判定する
　請求項２に記載のデータ検証装置。
【請求項４】
　前記検証部は、前記通信が切断された状態において、前記第１のステータス情報が前記第１のステータスである場合には、前記書込異常が生じたと判定する
請求項３に記載のデータ検証装置。
【請求項５】
　前記検証部は、前記通信が切断された状態において、前記第１のステータス情報が前記第２のステータスであり、かつ前記第１のデータにエラーがある場合には、前記データ不正が生じたと判定する
請求項３または請求項４に記載のデータ検証装置。
【請求項６】
　前記管理部は、
　前記第１のデータを前記第１の記憶部に書き込む前に、前記第２の記憶部にすでに書き込まれた前記第２のデータにエラーがある場合には前記第２のステータス情報を第４のステータスに設定し、
　前記第１のデータを前記第１の記憶部に書き込んだ後に、前記第２のステータス情報を第５のステータスに設定し、
　前記第２のデータを前記第２の記憶部に書き込み、前記第２の記憶部における前記第２のデータと、前記第１の記憶部における前記第１のデータとが一致した場合に、前記第２のステータス情報を第６のステータスに設定する
　請求項１から請求項５のいずれか一項に記載のデータ検証装置。
【請求項７】
　前記検証部は、前記通信が切断された状態において、前記第１の記憶部に書き込まれた前記第１のデータ、および前記第２の記憶部に書き込まれた前記第２のデータにエラーがあるかどうかを確認し、
　前記管理部は、前記第２のステータス情報が前記第５のステータスであり、前記第２のデータにエラーがあり、前記第１のデータにエラーがない場合には、前記第１の記憶部に書き込まれた前記第１のデータに基づいて、前記第２の記憶部に前記第２のデータを再度書き込む
請求項６に記載のデータ検証装置。
【請求項８】
第１のデータおよび第１のステータス情報を記憶する第１の記憶部と、第２のデータおよび第２のステータス情報を記憶する第２の記憶部とを有する記憶部と、
外部装置との間の通信により取得したデータに基づいて前記第１の記憶部に前記第１のデータを書き込んだ後に前記データに基づいて前記第２の記憶部に前記第２のデータを書き込む書込プロセスを制御するとともに、前記書込プロセスに応じて前記第１のステータス情報および前記第２のステータス情報を更新する管理部と、
前記通信が切断された状態において、前記第１のステータス情報および前記第２のステータス情報に基づいて前記第１のデータおよび前記第２のデータを検証する検証部と
　を備え、

前記管理部は、
前記第１のデータを前記第１の記憶部に書き込む前に、前記第２の記憶部にすでに書き込まれた前記第２のデータにエラーがある場合には前記第２のステータス情報を第４のステータスに設定し、
前記第１のデータを前記第１の記憶部に書き込んだ後に、前記第２のステータス情報を第５のステータスに設定し、
前記第２のデータを前記第２の記憶部に書き込み、前記第２の記憶部における前記第２のデータと、前記第１の記憶部における前記第１のデータとが一致した場合に、前記第２のステータス情報を第６のステータスに設定する
データ検証装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、データを検証するデータ検証装置に関する。
【背景技術】
【０００２】
自動車等の車両には、しばしば不揮発性の記憶装置が搭載される。その記憶装置には、車両で用いられる様々なデータが記憶される。例えば、特許文献１には、記憶装置への書換指令が正当でないことが確認された場合に、書換禁止指令を生成するデータ書換システムが開示されている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２００８－２７６６６３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
記憶装置に記憶されたデータは、一般に信頼性が高いことが望まれており、さらなる信頼性の向上が期待されている。
【０００５】
データの信頼性を高めることができるデータ検証装置を提供することが望ましい。
【課題を解決するための手段】
【０００６】
本開示の一実施の形態に係る第１のデータ検証装置は、記憶部と、管理部と、検証部とを備えている。記憶部は、第１のデータおよび第１のステータス情報を記憶する第１の記憶部と、第２のデータおよび第２のステータス情報を記憶する第２の記憶部とを有する。管理部は、外部装置との間の通信により取得したデータに基づいて第１の記憶部に第１のデータを書き込んだ後にデータに基づいて第２の記憶部に第２のデータを書き込む書込プロセスを制御するとともに、書込プロセスに応じて第１のステータス情報および第２のステータス情報を更新するように構成される。検証部は、通信が切断された状態において、第１のステータス情報および第２のステータス情報に基づいて第１のデータおよび第２のデータを検証する。上記管理部は、第１のデータを第１の記憶部に書き込む前に、第１のステータス情報を第１のステータスに設定し、第１のデータを第１の記憶部に書き込んだ後に、第１のステータス情報を第２のステータスに設定し、第２のデータを第２の記憶部に書き込み、第２の記憶部における第２のデータと、第１の記憶部における第１のデータとが一致した場合に、第１のステータス情報を第３のステータスに設定する。
本開示の一実施の形態に係る第２のデータ検証装置は、記憶部と、管理部と、検証部とを備えている。記憶部は、第１のデータおよび第１のステータス情報を記憶する第１の記憶部と、第２のデータおよび第２のステータス情報を記憶する第２の記憶部とを有する。管理部は、外部装置との間の通信により取得したデータに基づいて第１の記憶部に第１のデ

ータを書き込んだ後にデータに基づいて第２の記憶部に第２のデータを書き込む書込プロセスを制御するとともに、書込プロセスに応じて第１のステータス情報および第２のステータス情報を更新するように構成される。検証部は、通信が切断された状態において、第１のステータス情報および第２のステータス情報に基づいて第１のデータおよび第２のデータを検証する。上記管理部は、第１のデータを第１の記憶部に書き込む前に、第２の記憶部にすでに書き込まれた第２のデータにエラーがある場合には第２のステータス情報を第４のステータスに設定し、第１のデータを第１の記憶部に書き込んだ後に、第２のステータス情報を第５のステータスに設定し、第２のデータを第２の記憶部に書き込み、第２の記憶部における第２のデータと、第１の記憶部における第１のデータとが一致した場合に、第２のステータス情報を第６のステータスに設定する。

【発明の効果】

【０００７】

本開示の一実施の形態に係る第１および第２のデータ検証装置によれば、データの信頼性を高めることができる。

【図面の簡単な説明】

【０００８】

【図１】本開示の一実施の形態に係る充電システムの一構成例を表すブロック図である。

【図２】図１に示したデータセクションの一例を表す説明図である。

【図３】図１に示した更新データセクションの一例を表す説明図である。

【図４Ａ】図１に示した車両の一動作例を表すフローチャートである。

【図４Ｂ】図１に示した車両の一動作例を表す他のフローチャートである。

【図５Ａ】図１に示した車両の一動作例を表す他のフローチャートである。

【図５Ｂ】図１に示した車両の一動作例を表す他のフローチャートである。

【図６Ａ】図１に示した車両の一動作例を表す表である。

【図６Ｂ】図１に示した車両の一動作例を表す他の表である。

【図７Ａ】図１に示した車両の一動作例を表す他の表である。

【図７Ｂ】図１に示した車両の一動作例を表す他の表である。

【発明を実施するための形態】

【０００９】

以下、本開示の実施の形態について、図面を参照して詳細に説明する。

【００１０】

＜実施の形態＞

［構成例］

図１は、一実施の形態に係るデータ検証装置が適用された充電システム１の一構成例を表すものである。充電システム１は、車両１０と、充電ステーション３０と、管理装置４０と、サーバ５０とを備えている。

【００１１】

車両１０は、例えば電動車両である。車両１０のドライバ（ユーザ）は、車両１０のバッテリ１４（後述）を充電したい場合には、車両１０を充電ステーション３０に移動させ、車両１０を充電ステーション３０にケーブルで接続する。充電ステーション３０は、車両１０との間でケーブルを介して通信を行い、車両１０に記憶された証明書データＤＴに基づいて認証処理を行い、認証処理が成功した場合に、車両１０のバッテリ１４に電力を供給する。サーバ５０は、ユーザ情報データベース５２（後述）を利用して、その証明書データＤＴに含まれるユーザ識別子ＵＩＤ（後述）に対応する、課金処理に必要な情報を特定し、この情報に基づいて、ユーザに対して課金処理を行う。

【００１２】

車両１０に記憶された証明書データＤＴは、例えば、定期的に更新される。この例では、車両１０は、充電ステーション３０との間でケーブルを介して通信を行うことにより、充電ステーション３０から新しい証明書データＤＴを取得し、この証明書データＤＴを用いて車両１０に記憶された証明書データＤＴを更新する。証明書データＤＴを更新する際

、例えば車両１０において書込異常が生じるおそれがある。この場合には、車両１０は、例えば充電ステーション３０と通信を行うことにより、証明書データＤＴを再度更新することができる。

【００１３】

ところで、例えば、車両１０の部品の故障により、証明書データＤＴにエラーが生じた場合があり得る。また、悪意者が、証明書データＤＴを不正に改変するおそれもある。車両１０は、車両１０に記憶されたステータス情報（後述するデータステータスＳＴＤおよび更新ステータスＳＴＵ）および証明書データＤＴに基づいて、部品故障またはデータ不正が生じたと判定し、ステータス情報を書き換える。この場合、車両１０は、ロック状態になり、充電ステーション３０により電力が供給されず、充電ステーション３０と通信を行っても、証明書データＤＴを更新しない。そこで、ユーザは、例えば、車両１０をディーラに持ち込む。部品故障である場合には、ディーラがその部品を交換し、そのディーラが管理する管理装置４０が、車両１０と通信を行うことにより、車両１０に記憶された証明書データＤＴを強制的に更新するとともにステータス情報をリセットすることができる。また、データ不正である場合には、ディーラが管理する管理装置４０は、車両１０と通信を行うことにより、車両１０に記憶された証明書データＤＴを強制的に更新するとともにステータス情報をリセットすることができる。このように、管理装置４０は、車両１０がロック状態である場合でも、証明書データＤＴを車両１０に強制的に書き込むことができ、これにより、車両１０のロックを解除することができるようになっている。

【００１４】

車両１０は、ゲートウェイ１１と、セキュリティ制御部２０と、表示部１３と、バッテリ１４と、インバータ１５と、モータ１６とを有している。

【００１５】

ゲートウェイ１１は、中継部１１Ａ，１１Ｂを有している。中継部１１Ａは、セキュリティ制御部２０および充電ステーション３０の間の通信を中継するように構成される。セキュリティ制御部２０および充電ステーション３０は、例えばケーブルにより接続され、ＴＬＳ（Transport Layer Security）を用いて通信を行うようになっている。中継部１１Ｂは、セキュリティ制御部２０および管理装置４０の間の通信を中継するように構成される。セキュリティ制御部２０および管理装置４０は、例えばケーブルにより接続され、例えば専用規格を用いたセキュリティ通信を行うようになっている。

【００１６】

セキュリティ制御部２０は、例えばセキュリティＥＣＵ（Electronic Control Unit）を含んで構成される。セキュリティＥＣＵは、例えば、１または複数の半導体チップを含んで構成される。セキュリティ制御部２０は、通信部２１と、セクション管理部２２と、記憶部２３と、電源監視部２４と、監視部２５とを有している。

【００１７】

通信部２１は、車両１０が充電ステーション３０に接続された場合には、ゲートウェイ１１の中継部１１Ａを介して充電ステーション３０との間で通信を行い、車両１０が管理装置４０に接続された場合には、ゲートウェイ１１の中継部１１Ｂを介して管理装置４０との間で通信を行うように構成される。

【００１８】

セクション管理部２２は、記憶部２３に対するデータの書込プロセス、および記憶部２３からのデータの読出プロセスを管理することにより、記憶部２３のデータセクションＳＥＣＤおよび更新データセクションＳＥＣＵを管理するように構成される。

【００１９】

記憶部２３は、例えばフラッシュメモリなどの不揮発性メモリを含んで構成される。記憶部２３は、ファイアウォールＦＷと、データセクションＳＥＣＤと、更新データセクションＳＥＣＵとを有している。

【００２０】

ファイアウォールＦＷは、セクション管理部２２との間の通信を監視し、記憶部２３に

記憶されたデータを保護するため、望まれない通信を防ぐように構成される。
【００２１】
データセクションＳＥＣＤは、車両１０で用いられる様々なデータを記憶するメモリ領域である。
【００２２】
図２は、データセクションＳＥＣＤの一例を表すものである。データセクションＳＥＣＤは、複数のデータセットＤＳ（データセットＤＳ１，ＤＳ２，…）が記憶される。複数のデータセットＤＳのうちのいずれか１つ（この例では１番目のデータセットＤＳ１）に、証明書データＤＴが格納される。このデータセットＤＳ１は、データステータスＳＴＤと、データ番号ＮＤと、証明書データＤＴ（証明書データＤＴＤ）と、ＳＵＭ値とを含んでいる。説明の便宜上、データセクションＳＥＣＤに記憶された証明書データＤＴを、証明書データＤＴＤとも呼ぶ。
【００２３】
データステータスＳＴＤは、セキュリティ制御部２０における書込プロセスのステータスについての情報を含む。データステータスＳＴＤは、この例では、後述するように、例えば、“正常”、“要更新”、または“不正”に設定可能である。
【００２４】
データ番号ＮＤは、データセクションＳＥＣＤに記憶された複数のデータセットＤＳのうちの、このデータセットＤＳ１を識別する番号である。このデータ番号ＮＤは、データセクションＳＥＣＤにおいて、このデータセットＤＳ１が記憶されたメモリ領域を示すアドレスに対応している。
【００２５】
証明書データＤＴＤは、暗号化された電子証明書である。証明書データＤＴＤは、例えば、車両１０を識別可能な識別子（車両識別子ＶＩＤ）、ユーザを識別可能な識別子（ユーザ識別子ＵＩＤ）などについての情報を含んでいる。
【００２６】
ＳＵＭ値は、誤り検出符号の符号値である。この例では、ＳＵＭ値は、このデータセットＤＳ１に含まれる、データステータスＳＴＤ、データ番号ＮＤ、および証明書データＤＴＤに基づいて算出された値である。セキュリティ制御部２０は、このＳＵＭ値を用いて、データセットＤＳ１におけるデータエラーの有無を検証することができるようになっている。
【００２７】
なお、この例ではＳＵＭ値を用いたが、これに限定されるものではなく、これに代えて、例えば、データステータスＳＴＤ、データ番号ＮＤ、および証明書データＤＴＤのミラーデータであってもよい。この場合には、セキュリティ制御部２０は、データエラーの有無に加え、例えばデータエラーの場所を検出することができる。
【００２８】
更新データセクションＳＥＣＵ（図１）は、例えば、データセクションＳＥＣＤに記憶された証明書データＤＴを更新する前に、そのデータセクションＳＥＣＤに記憶すべき新しい証明書データＤＴを一時的に記憶するメモリ領域である。すなわち、セキュリティ制御部２０は、証明書データＤＴを更新する際、まず、更新データセクションＳＥＣＵに証明書データＤＴを書き込み、その後に、データセクションＳＥＣＤに証明書データＤＴを書き込むようになっている。
【００２９】
図３は、更新データセクションＳＥＣＵの一例を表すものである。この例では、更新データセクションＳＥＣＵに記憶されたデータは、更新ステータスＳＴＵと、データ番号ＮＵと、証明書データＤＴ（証明書データＤＴＵ）と、ＳＵＭ値とを含んでいる。説明の便宜上、更新データセクションＳＥＣＵに記憶された証明書データＤＴを、証明書データＤＴＵと呼ぶ。
【００３０】

更新ステータスＳＴＵは、セキュリティ制御部２０における書込プロセスのステータスについての情報を含む。更新ステータスＳＴＵは、この例では、後述するように、例えば、“更新中”、“書換中”、または“未使用”に設定可能である。

【００３１】

データ番号ＮＵは、この更新データセクションＳＥＣＵのデータが書き込まれるべきデータセクションＳＥＣＤにおけるデータセット（この例ではデータセットＤＳ１）のデータ番号ＮＤである。なお、例えば、データセクションＳＥＣＤにおけるデータセットＤＳ２に証明書データＤＴを格納する場合には、この更新データセクションＳＥＣＵのデータ番号ＮＵは、このデータセットＤＳ２に含まれるデータ番号ＮＤである。

【００３２】

証明書データＤＴＵは、データセクションＳＥＣＤに証明書データＤＴＤとして書き込まれるべき、暗号化された電子証明書である。

【００３３】

ＳＵＭ値は、誤り検出符号の符号値であり、更新ステータスＳＴＵ、データ番号ＮＵ、および証明書データＤＴＵに基づいて算出された値である。セキュリティ制御部２０は、このＳＵＭ値を用いて、更新データセクションＳＥＣＵに記憶されたデータのデータエラーの有無を検証することができるようになっている。

【００３４】

なお、この例ではＳＵＭ値を用いたが、これに限定されるものではなく、これに代えて、例えば、更新ステータスＳＴＵ、データ番号ＮＵ、および証明書データＤＴＵのミラーデータであってもよい。この場合には、セキュリティ制御部２０は、エラーの有無に加え、データエラーの場所を検出することができる。

【００３５】

この構成により、セキュリティ制御部２０では、セクション管理部２２は、例えば、充電ステーション３０からの読出要求に基づいて、記憶部２３のデータセクションＳＥＣＤから証明書データＤＴ（証明書データＤＴＤ）を読み出し、通信部２１は、この証明書データＤＴを中継部１１Ａを介して充電ステーション３０に送信する。また、セクション管理部２２は、例えば、充電ステーション３０から送信された、更新すべき新しい証明書データＤＴを受け取った場合には、まず、この新しい証明書データＤＴを、証明書データＤＴＵとして更新データセクションＳＥＣＵに書き込む。そして、その後に、セクション管理部２２は、この新しい証明書データＤＴを、証明書データＤＴＤとしてデータセクションＳＥＣＤに書き込む。また、セクション管理部２２は、その書込プロセスに応じて、更新データセクションＳＥＣＵに更新ステータスＳＴＵを書き込むとともに、データセクションＳＥＣＤにデータステータスＳＴＤを書き込むようになっている。

【００３６】

電源監視部２４は、セキュリティ制御部２０に供給される電源電圧を監視するように構成される。電源監視部２４は、電源供給が停止した後に電源供給が復旧したときに、その電源供給の停止についての情報を、監視部２５に供給するようになっている。

【００３７】

監視部２５は、記憶部２３に記憶されたデータを監視するように構成される。監視部２５は、例えば、車両１０が起動する度に、記憶部２３に記憶された更新ステータスＳＴＵおよびデータステータスＳＴＤに基づいて、セキュリティ制御部２０における書込プロセスが中断しているかどうかを確認する。そして、監視部２５は、書込プロセスが中断している場合には、どの段階で中断しているのかを確認し、その確認結果と、記憶部２３に記憶された証明書データＤＴＵおよび証明書データＤＴＤとに基づいて、部品故障またはデータ不正が生じているのか、あるいはデータの書込異常が生じているのかを判定する。また、監視部２５は、電源監視部２４から供給された情報に基づいて、書込プロセスが中断した原因を判定する機能をも有している。

【００３８】

表示部１３は、例えばインストルメントパネルなどに設けられ、例えば液晶ディスプレ

イを含んで構成される。表示部１３は、監視部２５からの指示に基づいて、データの不正やデータの書込異常などについての情報をユーザに通知するようになっている。

【００３９】

バッテリ１４は、電力を蓄えるとともに、インバータ１５に直流電力を供給するように構成される。バッテリ１４は、充電ステーション３０から供給された電力を蓄えることができるようになっている。インバータ１５は、バッテリ１４から供給された直流電力に基づいて交流電力を生成し、生成した交流電力をモータ１６に供給するように構成される。モータ１６は、インバータ１５から供給された交流電力に基づいて、機械的エネルギーである駆動力を生成する動力源である。このようにして、車両１０は、モータの駆動力に基づいて走行を行うことができるようになっている。

【００４０】

充電ステーション３０（図１）は、車両１０のバッテリ１４に電力を供給することができるように構成される。充電ステーション３０は、例えば充電事業を行う事業者により管理される。なお、この例では充電ステーションの例で説明するが、これに限定されるものではなく、これに代えて、例えばＶ２Ｈ（Vehicle to Home）により家庭に電力供給を行うことが可能な装置であってもよい。充電ステーション３０は、認証部３１と、給電部３２と、証明書更新部３３とを有している。

【００４１】

認証部３１は、車両１０から取得した証明書データＤＴに基づいて認証処理を行うように構成される。具体的には、認証部３１は、車両１０から取得した証明書データＤＴに基づいて、サーバ５０のユーザ情報データベース５２（後述）に問い合わせを行うことにより、認証処理を行うようになっている。

【００４２】

給電部３２は、認証部３１における認証処理が成功した場合に、車両１０のバッテリ１４に電力を供給するように構成される。そして、充電ステーション３０は、証明書データＤＴに含まれるユーザ識別子ＵＩＤについての情報、およびバッテリ１４への電力供給量についての情報をサーバ５０に供給するようになっている。

【００４３】

証明書更新部３３は、車両１０の証明書データＤＴを更新するように構成される。具体的には、証明書更新部３３は、サーバ５０により生成され送信された、新しい証明書データＤＴを車両１０の記憶部２３に書き込むことにより、車両１０の証明書データＤＴを更新するようになっている。

【００４４】

管理装置４０は、例えばディーラにより管理される装置である。管理装置４０は、証明書更新部４１を有している。証明書更新部４１は、充電ステーション３０の証明書更新部３３と同様に、証明書データＤＴを更新するように構成される。そして、管理装置４０は、この証明書データＤＴを、車両１０の記憶部２３に強制的に書き込むようになっている。

【００４５】

サーバ５０は、証明書生成部５１と、ユーザ情報データベース５２と、課金処理部５３とを有している。

【００４６】

証明書生成部５１は、充電ステーション３０や管理装置４０からの依頼に基づいて、車両１０の証明書データＤＴを生成するように構成される。そして、サーバ５０は、証明書生成部５１が生成した証明書データＤＴを、その依頼元である充電ステーション３０や管理装置４０に送信するようになっている。

【００４７】

ユーザ情報データベース５２は、車両識別子ＶＩＤ、ユーザ識別子ＵＩＤ、そのユーザ識別子ＵＩＤに対応するユーザに対する課金処理に必要な情報などを、互いに関連づけて管理するように構成される。課金処理に必要な情報は、例えば、クレジットカード情報や、銀行の口座情報である。

【００４８】
課金処理部５３は、充電ステーション３０から送信されたユーザ識別子ＵＩＤについての情報および電力供給量についての情報に基づいて、課金処理を行うように構成される。具体的には、課金処理部５３は、充電ステーション３０から送信されたユーザ識別子ＵＩＤに基づいて、ユーザ情報データベース５２を用いて、そのユーザ識別子ＵＩＤに対応するユーザに対する課金処理に必要な情報を特定する。そして、課金処理部５３は、充電ステーション３０から送信された電力供給量についての情報に基づいて、金額を算出し、算出した金額、および特定された課金処理に必要な情報に基づいて、課金処理を行うようになっている。
【００４９】
ここで、セキュリティ制御部２０は、本開示における「データ検証装置」の一具体例に対応する。記憶部２３は、本開示における「記憶部」の一具体例に対応する。更新データセクションＳＥＣＵは、本開示における「第１の記憶部」の一具体例に対応する。データセクションＳＥＣＤは、本開示における「第２の記憶部」の一具体例に対応する。セクション管理部２２は、本開示における「管理部」の一具体例に対応する。監視部２５は、本開示における「検証部」の一具体例に対応する。
【００５０】
［動作および作用］
続いて、本実施の形態の充電システム１の動作および作用について説明する。
【００５１】
（全体動作概要）
まず、図１を参照して、充電システム１の全体動作概要を説明する。車両１０のドライバ（ユーザ）は、車両１０のバッテリ１４を充電したい場合には、車両１０を充電ステーション３０に移動させ、車両１０を充電ステーション３０にケーブルで接続する。充電ステーション３０は、車両１０との間でケーブルを介して通信を行うことにより、記憶部２３のデータセクションＳＥＣＤに記憶された証明書データＤＴ（証明書データＤＴＤ）を読み出す。充電ステーション３０の認証部３１は、読み出した証明書データＤＴに基づいて、サーバ５０のユーザ情報データベース５２に問い合わせを行うことにより、認証処理を行う。そして、認証処理が成功した場合には、給電部３２は、車両１０のバッテリ１４に電力を供給する。充電ステーション３０は、証明書データＤＴに含まれるユーザ識別子ＵＩＤについての情報およびバッテリ１４への電力供給量についての情報をサーバ５０に送信する。サーバ５０の課金処理部５３は、これらのユーザ識別子ＵＩＤについての情報および電力供給量についての情報に基づいて、ユーザ情報データベース５２を利用して、課金処理を行う。
【００５２】
また、車両１０は、充電ステーション３０との間でケーブルを介して通信を行うことにより、充電ステーション３０から新しい証明書データＤＴを取得し、この証明書データＤＴを用いて車両１０に記憶された証明書データＤＴを更新する。セクション管理部２２は、記憶部２３に対するデータの書込プロセス、および記憶部２３からのデータの読出プロセスを管理することにより、記憶部２３のデータセクションＳＥＣＤおよび更新データセクションＳＥＣＵを管理する。セクション管理部２２は、まず、取得した新しい証明書データＤＴを証明書データＤＴＵとして更新データセクションＳＥＣＵに書き込み、その後に、新しい証明書データＤＴを証明書データＤＴＤとしてデータセクションＳＥＣＤに書き込む。また、セクション管理部２２は、その書込プロセスに応じて、更新データセクションＳＥＣＵに更新ステータスＳＴＵを書き込むとともに、データセクションＳＥＣＤにデータステータスＳＴＤを書き込む。
【００５３】
監視部２５は、記憶部２３に記憶されたデータを監視する。そして、表示部１３は、監視部２５からの指示に基づいて、データの不正やデータの書込異常などについての情報をユーザに通知する。

【００５４】
（証明書データＤＴの更新について）
図４Ａ，４Ｂは、証明書データＤＴを更新する際の車両１０の動作を表すものである。車両１０のセクション管理部２２は、充電ステーション３０から取得した新しい証明書データＤＴを証明書データＤＴＵとして更新データセクションＳＥＣＵに書き込み、その後に、新しい証明書データＤＴを証明書データＤＴＤとしてデータセクションＳＥＣＤに書き込む。また、セクション管理部２２は、その書込プロセスに応じて、更新データセクションＳＥＣＵに更新ステータスＳＴＵを書き込むとともに、データセクションＳＥＣＤにデータステータスＳＴＤを書き込む。以下に、この動作について詳細に説明する。
【００５６】
まず、セキュリティ制御部２０の通信部２１は、充電ステーション３０から送信された新しい証明書データＤＴを受信する（ステップＳ１０１）。
【００５７】
次に、セクション管理部２２は、データセクションＳＥＣＤにおける、更新対象であるデータセットＤＳを確認する（ステップＳ１０２）。この例では、図２に示したように、証明書データＤＴ（証明書データＤＴＤ）は１番目のデータセットＤＳ１に格納されているので、セクション管理部２２は、更新対象であるデータセットＤＳは１番目のデータセットＤＳ１である旨を確認する。
【００５８】
次に、セクション管理部２２は、更新対象であるデータセットＤＳにおけるＳＵＭ値が正常であるかどうかを確認する（ステップＳ１０３）。セクション管理部２２は、この例では、１番目のデータセットＤＳ１に含まれるデータステータスＳＴＤ、データ番号ＮＤ、および証明書データＤＴＤに基づいてＳＵＭ値を算出し、このＳＵＭ値がデータセットＤＳ１に含まれるＳＵＭ値と一致した場合に正常と判定する。
【００５９】
ステップＳ１０３において、ＳＵＭ値が正常ではない場合（ステップＳ１０３において“Ｎ”）には、セクション管理部２２は、データセクションＳＥＣＤに“不正”を示すデータステータスＳＴＤを書き込むことにより、データステータスＳＴＤを“不正”に設定する（ステップＳ１０４）。すなわち、この場合には、データセクションＳＥＣＤにおける証明書データＤＴ（証明書データＤＴＤ）にデータエラーが生じているので、セクション管理部２２は、部品が故障しているか、あるいはデータが不正に改変された可能性が高いと判定し、データステータスＳＴＤを“不正”に設定する。
【００６０】
そして、監視部２５は、このデータステータスＳＴＤが“不正”である旨を確認し、表示部１３は、監視部２５からの指示に基づいて、部品故障またはデータ不正が生じた旨を表示する（ステップＳ１０５）。
【００６１】
そして、通信部２１は、セクション管理部２２からの指示に基づいて、部品故障またはデータ不正が生じた旨を充電ステーション３０に通知する（ステップＳ１０６）。
【００６２】
このようにデータステータスＳＴＤが“不正”である場合には、車両１０はロック状態になり、これ以降において、充電ステーション３０は、車両１０の証明書データＤＴを更新することができず、車両１０のバッテリ１４を充電することができない。この場合には、ユーザは、例えば、車両１０をディーラに持ち込む。部品故障である場合には、ディーラはその部品を交換し、管理装置４０は、車両１０と通信を行うことにより、車両１０に記憶された証明書データＤＴを更新するとともにデータステータスＳＴＤをリセットする。また、データ不正である場合には、ディーラが管理する管理装置４０は、車両１０と通信を行うことにより、車両１０に証明書データＤＴを強制的に書き込むとともにデータステータスＳＴＤをリセットする。このようにして、管理装置４０は車両１０のロックを解除することができる。

【００６３】
一方、ステップＳ１０３において、ＳＵＭ値が正常である場合（ステップＳ１０３において“Ｙ”）には、セクション管理部２２は、更新データセクションＳＥＣＵに、“書換中”を示す更新ステータスＳＴＵを書き込むことにより、更新ステータスＳＴＵを“書換中”に設定する（ステップＳ１０７）。
【００６４】
次に、セクション管理部２２は、ステップＳ１０１において通信部２１が受信した新しい証明書データＤＴを証明書データＤＴＵとして更新データセクションＳＥＣＵに書き込む（ステップＳ１０８）。
【００６５】
次に、セクション管理部２２は、更新データセクションＳＥＣＵに書き込まれた証明書データＤＴＵに基づいてＳＵＭ値を算出し、そのＳＵＭ値を更新データセクションＳＥＣＵに書き込む（ステップＳ１０９）。具体的には、セクション管理部２２は、ステップＳ１０８により更新データセクションＳＥＣＵに書き込まれた証明書データＤＴＵを読み出し、読み出された証明書データＤＴＵに基づいてＳＵＭ値を算出することができる。なお、これに限定されるものではなく、図示しないバッファメモリが、例えば、ステップＳ１０１において通信部２１が受信した証明書データＤＴを一旦記憶し、セクション管理部２２が、そのバッファメモリに記憶された証明書データＤＴに基づいてＳＵＭ値を算出し、そのＳＵＭ値を更新データセクションＳＥＣＵに書き込んでもよい。
【００６６】
次に、セクション管理部２２は、更新データセクションＳＥＣＵに、“更新中”を示す更新ステータスＳＴＵを書き込むことにより、更新ステータスＳＴＵを“更新中”に設定する（ステップＳ１１０）。
【００６７】
次に、セクション管理部２２は、データセクションＳＥＣＤに、“要更新”を示すデータステータスＳＴＤを書き込むことにより、データステータスＳＴＤを“要更新”に設定する（ステップＳ１１１）。
【００６８】
次に、セクション管理部２２は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する更新処理を行う（ステップＳ１１２）。具体的には、セクション管理部２２は、更新データセクションＳＥＣＵに記憶されたデータ番号ＮＵおよび証明書データＤＴ（証明書データＤＴＵ）を読み出し、読み出した証明書データＤＴを、データセクションＳＥＣＤにおけるそのデータ番号ＮＵに対応するデータセットＤＳ（この例では１番目のデータセットＤＳ１）に証明書データＤＴＤとして書き込む。また、セクション管理部２２は、更新データセクションＳＥＣＵに記憶されたＳＵＭ値を読み出し、読み出したＳＵＭ値をそのデータセットＤＳ（この例ではデータセットＤＳ１）に書き込む。
【００６９】
次に、セクション管理部２２は、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致するかどうかを確認する（ステップＳ１１３）。具体的には、セクション管理部２２は、データセクションＳＥＣＤにおける、証明書データＤＴが格納されたデータセットＤＳ（この例では１番目のデータセットＤＳ１）のデータ番号ＮＤ、証明書データＤＴＤ、およびＳＵＭ値と、更新データセクションＳＥＣＵのデータ番号ＮＵ、証明書データＤＴＵ、およびＳＵＭ値が互いにそれぞれ一致するかどうかを確認する。
【００７０】
ステップＳ１１３において、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致する場合（ステップＳ１１３において“Ｙ”）には、セクション管理部２２は、データセクションＳＥＣＤに、“正常”を示すデータステータスＳＴＤを書き込むことにより、データステータスＳＴＤを“正常”に設定する（ステップＳ１

１４）。
【００７１】
次に、セクション管理部２２は、更新データセクションＳＥＣＵに、“未使用”を示す更新ステータスＳＴＵを書き込むことにより、更新ステータスＳＴＵを“未使用”に設定する（ステップＳ１１５）。
【００７２】
次に、監視部２５は、データステータスＳＴＤが“正常”であり更新ステータスＳＴＵが“未使用”である旨を確認し、表示部１３は、監視部２５からの指示に基づいて、証明書データＤＴの更新が正常に終了した旨を表示する（ステップＳ１１６）。
【００７３】
そして、通信部２１は、セクション管理部２２からの指示に基づいて、証明書データＤＴの更新が正常に終了した旨を充電ステーション３０に通知する（ステップＳ１１７）。
【００７４】
一方、ステップＳ１１３において、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致しない場合（ステップＳ１１３において“Ｎ”）には、セクション管理部２２は、データセクションＳＥＣＤのデータステータスＳＴＤを“要更新”に維持し（ステップＳ１１８）、ステップＳ１１２と同様に、再度、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する更新処理を行い（ステップＳ１１９）、ステップＳ１１３と同様に、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致するかどうかを確認する（ステップＳ１２０）。ステップＳ１２０において、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致する場合（ステップＳ１２０において“Ｙ”）には、ステップＳ１１４に進む。一方、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致しない場合（ステップＳ１２０において“Ｎ”）には、所定回数、ステップＳ１１９，Ｓ１２０を繰り返す。
【００７５】
繰り返し回数が所定回数に達した場合（ステップＳ１２１において“Ｙ”）には、監視部２５は、データステータスＳＴＤが“要更新”であり更新ステータスＳＴＵが“更新中”である旨を確認し、表示部１３は、監視部２５からの指示に基づいて、書込異常が生じた旨を表示する（ステップＳ１２２）。
【００７６】
そして、通信部２１は、セクション管理部２２からの指示に基づいて、書込異常が生じた旨を充電ステーション３０に通知する（ステップＳ１２３）。
【００７７】
以上で、このフローは終了する。ここで、証明書データＤＴＵは、本開示における「第１のデータ」の一具体例に対応する。更新ステータスＳＴＵは、本開示における「第１のステータス情報」の一具体例に対応する。更新ステータスＳＴＵの“書込中”は、本開示における「第１のステータス」の一具体例に対応する。更新ステータスＳＴＵの“更新中”は、本開示における「第２のステータス」の一具体例に対応する。更新ステータスＳＴＵの“未使用”は、本開示における「第３のステータス」の一具体例に対応する。証明書データＤＴＤは、本開示における「第２のデータ」の一具体例に対応する。データステータスＳＴＤは、本開示における「第２のステータス情報」の一具体例に対応する。データステータスＳＴＤの“不正”は、本開示における「第４のステータス」の一具体例に対応する。データステータスＳＴＤの“要更新”は、本開示における「第５のステータス」の一具体例に対応する。データステータスＳＴＤの“正常”は、本開示における「第６のステータス」の一具体例に対応する。
【００７８】
（バッテリ１４を充電する動作について）
図５Ａ，５Ｂは、証明書データＤＴを使用してバッテリ１４を充電する際の車両１０の動作を表すものである。車両１０のセクション管理部２２は、データセクションＳＥＣＤ

から、証明書データＤＴ（証明書データＤＴＤ）を含むデータセットＤＳを読み出し、そのデータセットＤＳに基づいて、その証明書データＤＴが正常であるかどうかを判定する。そして、充電ステーション３０は、その証明書データＤＴが正常である場合に、車両１０のバッテリ１４を充電する。以下に、この動作について詳細に説明する。

【００７９】

まず、セクション管理部２２は、データセクションＳＥＣＤから、証明書データＤＴ（証明書データＤＴＤ）を含むデータセットＤＳを読み出す（ステップＳ１３１）。この例では、１番目のデータセットＤＳ１が証明書データＤＴを含むので、セクション管理部２２は、１番目のデータセットＤＳ１を読み出す。

【００８０】

次に、セクション管理部２２は、読み出したデータセットＤＳに含まれるデータステータスＳＴＤが“不正”であるかどうかを確認する（ステップＳ１３２）。

【００８１】

ステップＳ１３２において、データステータスＳＴＤが“不正”である場合（ステップＳ１３２において“Ｙ”）には、監視部２５は、このデータステータスＳＴＤが“不正”である旨を確認し、表示部１３は、監視部２５からの指示に基づいて、部品故障またはデータ不正が生じた旨を表示する（ステップＳ１３３）。

【００８２】

そして、通信部２１は、ステップＳ１０６と同様に、セクション管理部２２からの指示に基づいて、部品故障またはデータ不正が生じた旨を充電ステーション３０に通知する（ステップＳ１３４）。この場合には、充電ステーション３０は、車両１０のバッテリ１４に電力を供給しない。

【００８３】

一方、ステップＳ１３２において、データステータスＳＴＤが“不正”ではない場合（ステップＳ１３２において“Ｎ”）には、セクション管理部２２は、このデータステータスＳＴＤが“要更新”であるかどうかを確認する（ステップＳ１３５）。

【００８４】

ステップＳ１３５において、データステータスＳＴＤが“要更新”である場合（ステップＳ１３５において“Ｙ”）には、セクション管理部２２は、データセクションＳＥＣＤのデータステータスＳＴＤを“要更新”に維持し（ステップＳ１３６）、再度、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する更新処理を行い（ステップＳ１３７）、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致するかどうかを確認する（ステップＳ１３８）。ステップＳ１３８において、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致する場合（ステップＳ１３８において“Ｙ”）には、ステップＳ１４２に進む。一方、データセクションＳＥＣＤのデータと更新データセクションＳＥＣＵのデータとが互いに一致しない場合（ステップＳ１３８において“Ｎ”）には、所定回数、ステップＳ１３７，Ｓ１３８を繰り返す。

【００８５】

繰り返し回数が所定回数に達した場合（ステップＳ１３９において“Ｙ”）には、監視部２５は、データステータスＳＴＤが“要更新”である旨を確認し、表示部１３は、監視部２５からの指示に基づいて、書込異常が生じた旨を表示する（ステップＳ１４０）。

【００８６】

そして、通信部２１は、セクション管理部２２からの指示に基づいて、書込異常が生じた旨を充電ステーション３０に通知する（ステップＳ１４１）。この場合には、充電ステーション３０は、車両１０のバッテリ１４に電力を供給しない。

【００８７】

一方、ステップＳ１３５において、データステータスＳＴＤが“要更新”ではない場合（ステップＳ１３５において“Ｎ”）には、セクション管理部２２は、ステップＳ１３１において読み出したデータセットＤＳのＳＵＭ値が正常であるかどうかを確認する（ステップ

Ｓ１４２）。セクション管理部２２は、この例では、１番目のデータセットＤＳ１に含まれるデータステータスＳＴＤ、データ番号ＮＤ、および証明書データＤＴＤに基づいてＳＵＭ値を算出し、このＳＵＭ値がデータセットＤＳ１に含まれるＳＵＭ値と一致した場合に正常と判定する。

【００８８】

ステップＳ１４２において、データセットＤＳのＳＵＭ値が正常ではない場合（ステップＳ１４２において“Ｎ”）には、セクション管理部２２は、データセクションＳＥＣＤに、“不正”を示すデータステータスＳＴＤを書き込むことにより、データステータスＳＴＤを“不正”に設定する（ステップＳ１４３）。

【００８９】

そして、監視部２５は、このデータステータスＳＴＤが“不正”である旨を確認し、表示部１３は、監視部２５からの指示に基づいて、部品故障またはデータ不正が生じた旨を表示する（ステップＳ１４４）。

【００９０】

そして、通信部２１は、セクション管理部２２からの指示に基づいて、部品故障またはデータ不正が生じた旨を充電ステーション３０に通知する（ステップＳ１４５）。この場合には、充電ステーション３０は、車両１０のバッテリ１４に電力を供給しない。

【００９１】

一方、ステップＳ１４２において、データセットＤＳのＳＵＭ値が正常である場合（ステップＳ１４２において“Ｙ”）には、セクション管理部２２は、そのデータセットＤＳに含まれる証明書データＤＴ（証明書データＤＴＤ）は正常であると判定し、通信部２１は、この証明書データＤＴを充電ステーション３０に送信する（ステップＳ１４６）。

【００９２】

充電ステーション３０の認証部３１は、車両１０から送信された証明書データＤＴに基づいて認証処理を行い、認証処理が成功した場合には、給電部３２が、車両１０のバッテリ１４に電力を供給する。このようにして、車両１０のバッテリ１４に電力が供給される（ステップＳ１４７）。

【００９３】

（車両１０におけるデータ検証動作について）

セキュリティ制御部２０の監視部２５は、例えば、車両１０が起動する度に、記憶部２３に記憶された更新ステータスＳＴＵおよびデータステータスＳＴＤに基づいて、セキュリティ制御部２０における書込プロセスが中断しているかどうかを確認する。そして、監視部２５は、書込プロセスが中断している場合には、どの段階で中断しているのかを確認し、その確認結果と、記憶部２３に記憶された証明書データＤＴＵおよび証明書データＤＴＤとに基づいて、部品故障またはデータ不正が生じているのか、あるいはデータの書込異常が生じているのかを判定する。以下に、更新データセクションＳＥＣＵのデータに基づくデータ検証、およびデータセクションＳＥＣＤのデータに基づくデータ検証について、順に説明する。

【００９４】

図６Ａ，６Ｂは、更新データセクションＳＥＣＵのデータに基づく監視部２５におけるデータ検証動作の一例を表すものである。図６において、“データエラー無し”は、ＳＵＭ値が正常であることを示し、“データエラー有り”は、ＳＵＭ値が正常ではないことを示す。

【００９５】

例えば、更新ステータスＳＴＵが“未定義”である場合には、監視部２５は、部品故障またはデータ不正が生じたと判定する。すなわち、この例では、“更新中”、“書換中”、および“未使用”の３つが、更新ステータスＳＴＵとして設定できるように定義されている。よって、更新ステータスＳＴＵがこれらのいずれでもないことは、更新ステータスＳＴＵ自体が変化してしまったことを意味している。よって、監視部２５は、部品故障またはデータ不正が生じたと判定する。

【００９６】

この場合には、セクション管理部２２は、データステータスＳＴＤを“不正”に設定することにより車両１０をロックする。そして、表示部１３は、監視部２５からの指示に基づいて、部品故障またはデータ不正が生じた旨を表示する。ロック状態では、車両１０は、更新データセクションＳＥＣＵのデータの消去や充電ステーション３０による再度の証明書データＤＴの更新を行うことはできない。充電ステーション３０は、車両１０のロックを解除することはできず、管理装置４０のみが車両１０のロックを解除することができる。よって、車両１０のドライバ（ユーザ）は、車両１０をディーラに持ち込む。部品故障である場合には、ディーラはその部品を交換する。そして、管理装置４０は、車両１０と通信を行うことにより、車両１０に記憶された証明書データＤＴを更新するとともにデータステータスＳＴＤをリセットする。また、データ不正である場合には、管理装置４０は、車両１０と通信を行うことにより、車両１０に記憶された証明書データＤＴを更新するとともにデータステータスＳＴＤをリセットする。管理装置４０は、このように車両１０に強制的に証明書データＤＴを書き込むことにより、車両１０のロックを解除する。

【００９７】

また、例えば、更新ステータスＳＴＵが“書換中”であり、証明書データＤＴＵにデータエラーがある場合には、監視部２５は、更新データセクションＳＥＣＵに対するデータの書込中に書込異常が生じたと判定する。

【００９８】

この場合には、セクション管理部２２は、データステータスＳＴＤを“要更新”に設定する。そして、表示部１３は、監視部２５からの指示に基づいて、書込異常が生じた旨を表示する。すなわち、この場合には、更新データセクションＳＥＣＵへの証明書データＤＴの書き込みが終了していない段階で書込プロセスが中断したので、例えば、証明書データＤＴが不正に改変されたおそれはないため、車両１０はロックされない。よって、セクション管理部２２は、更新データセクションＳＥＣＵのデータの消去や充電ステーション３０による再度の証明書データＤＴの更新を行うことができる。

【００９９】

また、例えば、更新ステータスＳＴＵが“更新中”であり、証明書データＤＴＵにデータエラーがある場合には、監視部２５は、部品故障またはデータ不正が生じたと判定する。すなわち、この場合には、更新データセクションＳＥＣＵへの証明書データＤＴの書き込みが終了した後に書込プロセスが中断したので、例えば、証明書データＤＴＵが不正に改変されたおそれがある。よって、監視部２５は、部品故障またはデータ不正が生じたと判定する。

【０１００】

この場合には、セクション管理部２２は、データステータスＳＴＤを“不正”に設定することにより車両１０をロックする。そして、表示部１３は、監視部２５からの指示に基づいて、部品故障またはデータ不正が生じた旨を表示する。ロック状態では、車両１０は、更新データセクションＳＥＣＵのデータの消去や充電ステーション３０による再度の証明書データＤＴの更新を行うことはできない。充電ステーション３０は、車両１０のロックを解除することはできず、管理装置４０のみが車両１０のロックを解除することができる。

【０１０１】

また、例えば、更新ステータスＳＴＵが“未使用”であり、証明書データＤＴＵにデータエラーがある場合には、監視部２５は、問題ないと判定する。すなわち、更新ステータスＳＴＵが“未使用”であるので、証明書データＤＴＵのデータエラーは、証明書データＤＴの更新後に生じている。よって、監視部２５は、問題ないと判定する。

【０１０２】

この場合には、セクション管理部２２は、更新データセクションＳＥＣＵに記憶された証明書データＤＴＵを消去することができる。また、例えば、セクション管理部２２は、充電ステーション３０による再度の証明書データＤＴの更新を行うことができる。

【０１０３】

また、例えば、更新ステータスＳＴＵが“書換中”であり、証明書データＤＴＵにデータ

エラーがない場合には、監視部２５は、更新データセクションＳＥＣＵに対するデータの書込中に書込異常が生じたと判定する。

【０１０４】

この場合には、セクション管理部２２は、データステータスＳＴＤを“要更新”に設定する。そして、表示部１３は、監視部２５からの指示に基づいて、書込異常が生じた旨を表示する。すなわち、この場合には、更新データセクションＳＥＣＵへの証明書データＤＴの書き込みが終了していない段階で書込プロセスが中断したので、例えば、証明書データＤＴが不正に改変されたおそれはないため、車両１０はロックされない。よって、セクション管理部２２は、更新データセクションＳＥＣＵのデータの消去や充電ステーション３０による再度の証明書データＤＴの更新を行うことができる。

【０１０５】

また、例えば、更新ステータスＳＴＵが“更新中”であり、証明書データＤＴＵにデータエラーがない場合には、監視部２５は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する際に書込異常が生じたと判定する。

【０１０６】

この場合には、更新データセクションＳＥＣＵの証明書データＤＴＵにデータエラーがないので、セクション管理部２２は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する更新処理を行う。その結果、データセクションＳＥＣＤには、証明書データＤＴが正常に書き込まれ、更新ステータスＳＴＵは“未使用”に設定されることにより、証明書データＤＴの更新は正常に終了する。

【０１０７】

また、例えば、更新ステータスＳＴＵが“未使用”であり、証明書データＤＴＵにデータエラーがない場合には、証明書データＤＴの更新は正常に終了しているので、監視部２５は、問題ないと判定する。

【０１０８】

この場合には、セクション管理部２２は、例えば、更新データセクションＳＥＣＵに記憶された証明書データＤＴＵを消去することができる。

【０１０９】

図７Ａ，７Ｂは、データセクションＳＥＣＤのデータに基づく監視部２５におけるデータ検証動作の一例を表すものである。

【０１１０】

例えば、データステータスＳＴＤが“正常”であり、証明書データＤＴＤにデータエラーがある場合には、監視部２５は、書込異常が生じたと判定する。

【０１１１】

この場合には、証明書データＤＴＤにデータエラーがあるため、セクション管理部２２は、この証明書データＤＴＤを使用不可にする。これにより、充電ステーション３０は車両１０のバッテリ１４に電力を供給することはできない。そして、表示部１３は、監視部２５からの指示に基づいて、書込異常が生じた旨を表示する。更新データセクションＳＥＣＵにデータエラーがない場合には、セクション管理部２２は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する更新処理を行うことができる。これにより、充電ステーション３０は、車両１０のバッテリ１４を充電することができるようになる。

【０１１２】

また、例えば、データステータスＳＴＤが“要更新”であり、証明書データＤＴＤにデータエラーがある場合には、監視部２５は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する際に書込異常が生じたと判定する。

【０１１３】

この場合には、表示部１３は、書込異常が生じた旨を表示する。セクション管理部２２は、充電ステーション３０による再度の証明書データＤＴの更新を行うことができる。更新データセクションＳＥＣＵの証明書データＤＴＵにデータエラーがなく、更新ステータ

ＳＳＴＵが"更新中"である場合には、セクション管理部２２は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する更新処理を行うことができる。

【０１１４】

また、例えば、データステータスＳＴＤが“不正”であり、証明書データＤＴＤにデータエラーがある場合には、監視部２５は、部品故障またはデータ不正が生じたと判定する。

【０１１５】

この場合には、データステータスＳＴＤがすでに“不正”であるため、車両１０はロック状態である。表示部１３は、監視部２５からの指示に基づいて、部品故障またはデータ不正が生じた旨を表示する。ロック状態では、車両１０は、更新データセクションＳＥＣＵのデータの消去や充電ステーション３０による再度の証明書データＤＴの更新を行うことはできない。充電ステーション３０は、車両１０のロックを解除することはできず、管理装置４０のみが車両１０のロックを解除することができる。

【０１１６】

例えば、データステータスＳＴＤが“正常”であり、証明書データＤＴＤにデータエラーがない場合には、証明書データＤＴの更新は正常に終了しているので、監視部２５は、問題ないと判定する。

【０１１７】

この場合には、証明書データＤＴを使用することができる。例えば、充電ステーション３０は、車両１０のバッテリ１４に電力を供給することができる。

【０１１８】

また、例えば、データステータスＳＴＤが“要更新”であり、証明書データＤＴＤにデータエラーがない場合には、監視部２５は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する際に書込異常が生じたと判定する。

【０１１９】

この場合には、表示部１３は、書込異常が生じた旨を表示する。セクション管理部２２は、充電ステーション３０による再度の証明書データＤＴの更新を行うことができる。更新データセクションＳＥＣＵの証明書データＤＴＵにデータエラーがなく、更新ステータスＳＴＵが"更新中"である場合には、セクション管理部２２は、更新データセクションＳＥＣＵに基づいてデータセクションＳＥＣＤのデータを更新する更新処理を行うことができる。

【０１２０】

また、例えば、データステータスＳＴＤが“不正”であり、証明書データＤＴＤにデータエラーがある場合には、監視部２５は、部品故障またはデータ不正が生じたと判定する。

【０１２１】

この場合には、データステータスＳＴＤがすでに“不正”であるため、車両１０はロック状態である。表示部１３は、監視部２５からの指示に基づいて、部品故障またはデータ不正が生じた旨を表示する。ロック状態では、車両１０は、更新データセクションＳＥＣＵのデータの消去や充電ステーション３０による再度の証明書データＤＴの更新を行うことはできない。充電ステーション３０は、車両１０のロックを解除することはできず、管理装置４０のみが車両１０のロックを解除することができる。

【０１２２】

このように、セキュリティ制御部２０では、更新データセクションＳＥＣＵおよびデータセクションＳＥＣＤを設け、更新データセクションＳＥＣＵに更新ステータスＳＴＵを記憶させるとともに、データセクションＳＥＣＤにデータステータスＳＴＤを記憶させるようにした。そして、監視部２５は、更新ステータスＳＴＵおよびデータステータスＳＴＤに基づいて、書込プロセスの中断を確認するようにした。そして、監視部２５は、書込プロセスが中断している場合には、どの段階で中断しているのかを確認し、その確認結果と、記憶部２３に記憶された証明書データＤＴＵおよび証明書データＤＴＤとに基づいて、部品故障またはデータ不正が生じているのか、あるいはデータの書込異常が生じている

のかを判定するようにした。これにより、セキュリティ制御部２０では、車両１０と、外部装置との間で通信を行うことなく、部品故障またはデータ不正が生じているのか、あるいはデータの書込異常が生じているのかを判定することができる。その結果、セキュリティ制御部２０では、証明書データＤＴの信頼性を高めることができる。

【０１２３】

すなわち、例えば、車両と外部装置との間で通信を行い、車両が、記憶している証明書データＤＴと、外部装置から送信された証明書データＤＴとを比較することにより、証明書データＤＴを検証する方法があり得る。しかしながら、例えば、悪意のある第３者がこの外部装置を用意した場合には、証明書データＤＴを正確に検証することができない。

【０１２４】

一方、本実施の形態に係るセキュリティ制御部２０では、更新ステータスＳＴＵおよびデータステータスＳＴＤに基づいて、書込プロセスの中断を確認し、この確認結果と、記憶部２３に記憶された証明書データＤＴＵおよび証明書データＤＴＤとに基づいて、証明書データＤＴを検証するようにした。これにより、本実施の形態では、車両１０と外部装置との間で通信を行うことなく、車両１０のセキュリティ制御部２０自体が、証明書データＤＴを検証することができる。その結果、セキュリティ制御部２０では、証明書データＤＴを正確に検証することができるので、データ（証明書データＤＴ）の信頼性を高めることができる。

【０１２５】

また、セキュリティ制御部２０では、部品故障またはデータ不正が生じているのか、あるいはデータの書込異常が生じているのかを判定するようにした。これにより、例えば部品故障またはデータ不正が生じている場合には、車両１０をディーラに持ち込むことにより、部品の交換などの適切な処置を受けることができる。また、例えば、データの書込異常の場合には、車両１０をディーラに持ち込むことなく、正常な状態に復帰することができる。その結果、セキュリティ制御部２０では、ユーザの利便性を高めることができる。

【０１２６】

［効果］

以上のように本実施の形態では、更新データセクションおよびデータセクションを設け、更新データセクションに更新ステータスを記憶させるとともに、データセクションにデータステータスを記憶させるようにした。そして、更新ステータスおよびデータステータスに基づいて、書込プロセスの中断を確認し、書込プロセスが中断している場合には、どの段階で中断しているのかを確認し、その確認結果と、記憶部２３に記憶された証明書データとに基づいて、部品故障またはデータ不正が生じているのか、あるいはデータの書込異常が生じているのかを判定するようにした。これにより、証明書データの信頼性を高めることができる。

【０１２７】

本実施の形態では、部品故障またはデータ不正が生じているのか、あるいはデータの書込異常が生じているのかを判定するようにしたので、ユーザの利便性を高めることができる。

【０１２８】

以上、実施の形態を挙げて本技術を説明したが、本技術はこれらの実施の形態等には限定されず、種々の変形が可能である。

【０１２９】

例えば、上記実施の形態では、本技術を証明書データＤＴに適用したが、これに限定されるものではなく、様々なデータに適用することができる。

【０１３０】

また、例えば、上記実施の形態では、本技術を充電システムに適用したが、これに限定されるものではなく、充電以外の用途に適用してもよい。

【０１３１】

なお、本明細書中に記載された効果はあくまで例示であって限定されるものではなく、

また、他の効果があってもよい。

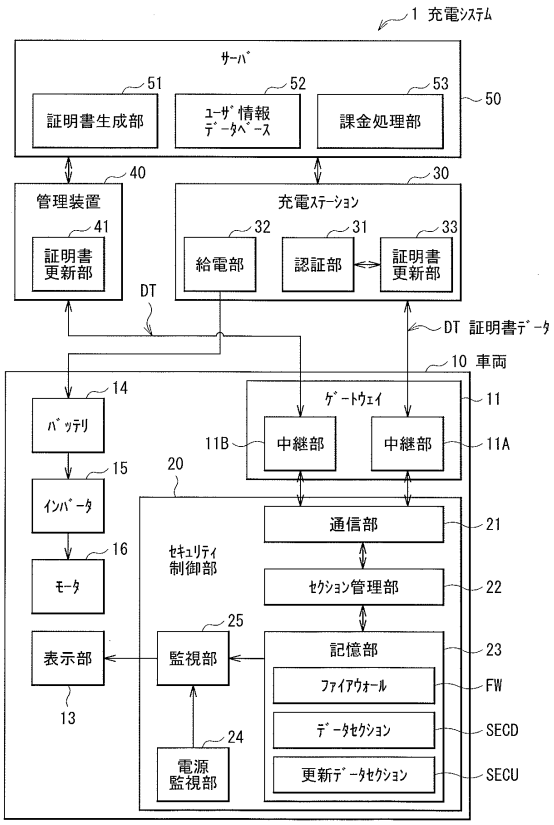
【符号の説明】

【０１３２】

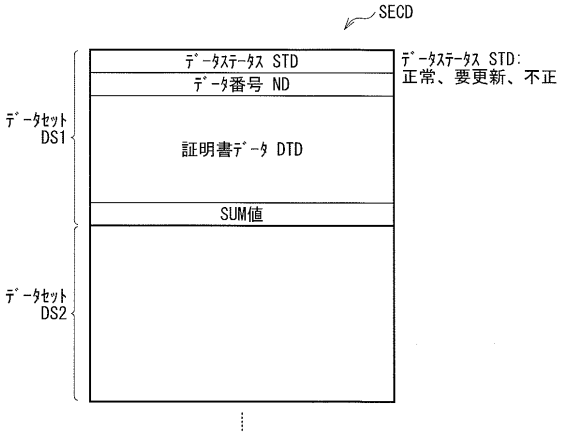
１…充電システム、１０…車両、１１…ゲートウェイ、１１Ａ，１１Ｂ…中継部、１３…表示部、１４…バッテリ、１５…インバータ、１６…モータ、２０…セキュリティ制御部、２１…通信部、２２…セクション管理部、２３…記憶部、２４…電源監視部、２５…監視部、ＤＳ，ＤＳ１，ＤＳ２…データセット、ＤＴ，ＤＴＤ，ＤＴＵ…証明書データ、ＦＷ…ファイアウォール、ＮＤ，ＮＵ…データ番号、ＳＥＣＤ…データセクション、ＳＥＣＵ…更新データセクション、ＳＴＤ…データステータス、ＳＴＵ…更新ステータス。

【図面】

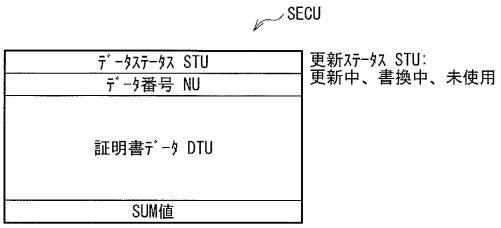
【図１】



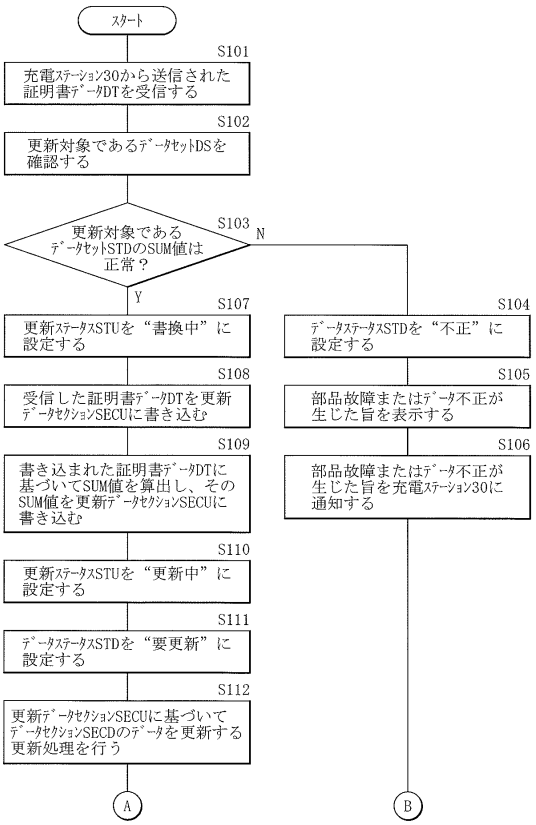
【図２】



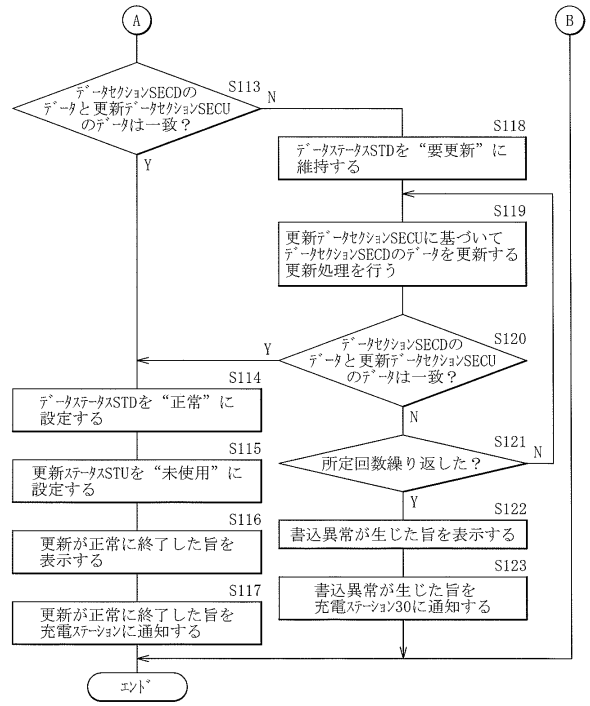
【図３】



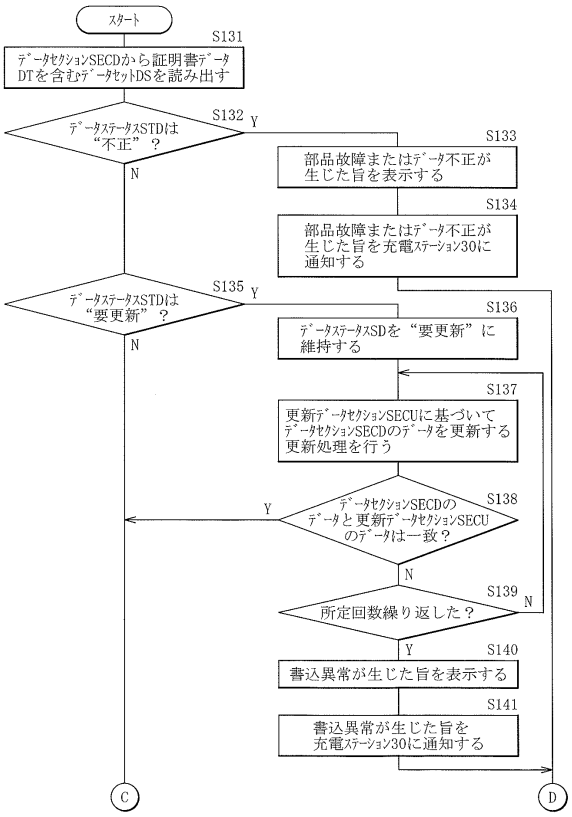
【図４Ａ】



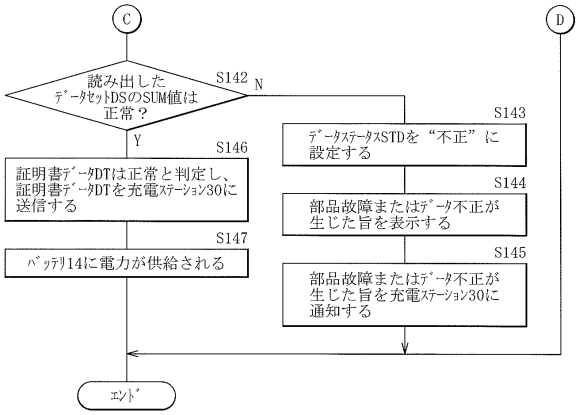
【図４Ｂ】



【図５Ａ】



【図５Ｂ】



【図６Ａ】

更新データセクション SECU		判定	対応例
更新ステータス STU	証明書データ DTU		
未定義	データエラー有り/データエラー無し	部品故障またはデータ不正が生じたと判定する。	セクション管理部22は、データステータスSTDを“不正”に設定することにより車両10をロックする。表示部13は、部品故障またはデータ不正が生じた旨を表示する。
書換中	データエラー有り	更新データセクションSECUに対するデータの書込中に書込異常が生じたと判定する。	セクション管理部22は、データステータスSTDを“要更新”に設定する。表示部13は、書込異常を表示する。セクション管理部22は、更新データセクションSECUのデータの消去や充電ステーション30による再度の証明書データDTの更新を行う。
更新中	データエラー有り	部品故障またはデータ不正が生じたと判定する。	セクション管理部22は、データステータスSTDを“不正”に設定することにより車両10をロックする。表示部13は、部品故障またはデータ不正が生じた旨を表示する。
未使用	データエラー有り	問題ないと判定する。	セクション管理部22は、証明書データDTUを消去する。セクション管理部22は、充電ステーション30による再度の証明書データDTの更新を行う。

【図６Ｂ】

更新ﾃﾞｰﾀｾｸｼｮﾝ SECU		判定	対応例
更新ｽﾃｰﾀｽ STU	証明書ﾃﾞｰﾀ DTU		
書換中	ﾃﾞｰﾀｴﾗｰ無し	更新ﾃﾞｰﾀｾｸｼｮﾝSECUに対するﾃﾞｰﾀの書込中に書込異常が生じたと判定する。	ｾｸｼｮﾝ管理部22は、ﾃﾞｰﾀｽﾃｰﾀｽSTDを“要更新”に設定する。 表示部13は、書込異常を表示する。 ｾｸｼｮﾝ管理部22は、更新ﾃﾞｰﾀｾｸｼｮﾝSECUのﾃﾞｰﾀの消去や充電ｽﾃｰｼｮﾝ30による再度の証明書ﾃﾞｰﾀDTUの更新を行う。
更新中	ﾃﾞｰﾀｴﾗｰ無し	更新ﾃﾞｰﾀｾｸｼｮﾝSECUに基づいてﾃﾞｰﾀｾｸｼｮﾝSECDのﾃﾞｰﾀを更新する際に書込異常が発生したと判定する。	ｾｸｼｮﾝ管理部22は、更新ﾃﾞｰﾀｾｸｼｮﾝSECUに基づいてﾃﾞｰﾀｾｸｼｮﾝSECDのﾃﾞｰﾀの更新する更新処理を行う。
未使用	ﾃﾞｰﾀｴﾗｰ無し	問題ないと判定する。	ｾｸｼｮﾝ管理部22は、証明書ﾃﾞｰﾀDTUを消去する。

【図７Ａ】

ﾃﾞｰﾀｾｸｼｮﾝ SECD		判定	対応例
ﾃﾞｰﾀｽﾃｰﾀｽ STD	証明書ﾃﾞｰﾀ DTD		
正常	ﾃﾞｰﾀｴﾗｰ有り	書込異常が生じたと判定する。	ｾｸｼｮﾝ管理部22は、証明書ﾃﾞｰﾀDTDを使用不可にする。 表示部13は、書込異常を表示する。 ｾｸｼｮﾝ管理部22は、更新ﾃﾞｰﾀｾｸｼｮﾝSECUの証明書ﾃﾞｰﾀDTUにﾃﾞｰﾀｴﾗｰがない場合には、更新ﾃﾞｰﾀｾｸｼｮﾝSECUに基づいてﾃﾞｰﾀｾｸｼｮﾝSECDのﾃﾞｰﾀを更新する更新処理を行う。
要更新	ﾃﾞｰﾀｴﾗｰ有り	更新ﾃﾞｰﾀｾｸｼｮﾝSECUに基づいてﾃﾞｰﾀｾｸｼｮﾝSECDのﾃﾞｰﾀを更新する際に書込異常が発生したと判定する。	表示部13は、書込異常が生じた旨を表示する。 ｾｸｼｮﾝ管理部22は、充電ｽﾃｰｼｮﾝ30による再度の証明書ﾃﾞｰﾀDTUの更新を行う。 ｾｸｼｮﾝ管理部22は、更新ﾃﾞｰﾀｾｸｼｮﾝSECUの証明書ﾃﾞｰﾀDTUにﾃﾞｰﾀｴﾗｰがなく、更新ｽﾃｰﾀｽSTUが“更新中”である場合には、更新ﾃﾞｰﾀｾｸｼｮﾝSECUに基づいてﾃﾞｰﾀｾｸｼｮﾝSECDのﾃﾞｰﾀを更新する更新処理を行う。
不正	ﾃﾞｰﾀｴﾗｰ有り	部品故障またはﾃﾞｰﾀ不正が生じたと判定する。	表示部13は、部品故障またはﾃﾞｰﾀ不正が生じた旨を表示する。

【図７Ｂ】

ﾃﾞｰﾀｾｸｼｮﾝ SECD		判定	対応例
ﾃﾞｰﾀｽﾃｰﾀｽ STD	証明書ﾃﾞｰﾀ DTD		
正常	ﾃﾞｰﾀｴﾗｰ無し	問題ないと判定する。	証明書ﾃﾞｰﾀDTDを使用することができる。
要更新	ﾃﾞｰﾀｴﾗｰ無し	更新ﾃﾞｰﾀｾｸｼｮﾝSECUに基づいてﾃﾞｰﾀｾｸｼｮﾝSECDのﾃﾞｰﾀを更新する際に書込異常が発生したと判定する。	表示部13は、書込異常が生じた旨を表示する。 ｾｸｼｮﾝ管理部22は、充電ｽﾃｰｼｮﾝ30による再度の証明書ﾃﾞｰﾀDTUの更新を行う。 ｾｸｼｮﾝ管理部22は、更新ﾃﾞｰﾀｾｸｼｮﾝSECUの証明書ﾃﾞｰﾀDTUにﾃﾞｰﾀｴﾗｰがなく、更新ｽﾃｰﾀｽSTUが“更新中”である場合には、更新ﾃﾞｰﾀｾｸｼｮﾝSECUに基づいてﾃﾞｰﾀｾｸｼｮﾝSECDのﾃﾞｰﾀを更新する更新処理を行う。
不正	ﾃﾞｰﾀｴﾗｰ無し	部品故障またはﾃﾞｰﾀ不正が生じたと判定する。	表示部13は、部品故障またはﾃﾞｰﾀ不正が生じた旨を表示する。

フロントページの続き

(56)参考文献 特開平０４－０３３０３０（ＪＰ，Ａ）
特開２００５－１１５６１４（ＪＰ，Ａ）
特開２００９－２１２８９６（ＪＰ，Ａ）
特開２０１２－１０３１８１（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ ２１／３１
Ｂ６０Ｒ １６／０２