

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5045131号
(P5045131)

(45) 発行日 平成24年10月10日(2012.10.10)

(24) 登録日 平成24年7月27日(2012.7.27)

(51) Int.Cl.		F I			
B6OR 16/02 (2006.01)			B6OR 16/02	66OU	
B6OR 16/023 (2006.01)			B6OR 16/02	66OC	
			B6OR 16/02	665P	

請求項の数 7 (全 28 頁)

(21) 出願番号	特願2007-25951 (P2007-25951)	(73) 特許権者	000005223 富士通株式会社
(22) 出願日	平成19年2月5日(2007.2.5)		神奈川県川崎市中原区上小田中4丁目1番1号
(65) 公開番号	特開2008-189163 (P2008-189163A)	(74) 代理人	110000040 特許業務法人池内・佐藤アンドパートナーズ
(43) 公開日	平成20年8月21日(2008.8.21)	(72) 発明者	北川 英志 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
審査請求日	平成21年11月6日(2009.11.6)	(72) 発明者	福岡 俊之 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

最終頁に続く

(54) 【発明の名称】 車載機、携帯端末およびそれらを含む車載機システム、ならびに、車載機のプログラム

(57) 【特許請求の範囲】

【請求項1】

特定のユーザに関する情報であって、車載機における処理に関わる情報であるユーザ固有情報を記録するデータ記録部を有する携帯端末と、当該携帯端末と互いに通信可能な車載機とを含む車載機システムであって、

前記車載機は、

携帯端末と有線または無線による通信を行う通信部と、

車載機での処理を行うためのデータを記録してある車載機用データ記録部と、

前記通信部が通信可能な前記携帯端末を検出する端末状態監視部と、

ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース部と、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行部と、

前記端末状態監視部によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス部とを備え、

前記実行部は、

前記端末状態監視部によって携帯端末が検出された場合は、

前記携帯端末の前記データ記録部から前記ユーザ固有情報の読み出しを、前記アクセス部に対して指示し、ユーザの指示に基づく前記処理に際して、読み出した前記ユーザ固有情報を用いて処理し、前記処理においてユーザ固有情報が生成または更新された場合に、

当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を前記アクセス部に対して指示し、前記アクセス部が前記ユーザ固有情報を前記携帯端末に書き込み・更新要求をした後、車載機上のユーザ固有情報を削除し、

前記端末状態監視部によって携帯端末が検出されない場合は、
前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行し、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上のユーザ固有情報を削除し、

前記携帯端末は、

車載機と有線または無線による通信を行う通信部と、

前記通信部が通信可能な車載機を検出する車載機状態監視部と、

前記車載機状態監視部が検出した車載機からの前記データ記録部に対するユーザ固有情報の読み出し要求、または書き込み・更新要求とユーザ固有情報を、前記通信部を介して受信し、当該読み出し要求または書き込み・更新要求に基づいて、前記データ記録部に対するユーザ固有情報の読み出し、または書き込み・更新処理を行い、当該処理結果を、前記車載機へ前記通信部を介して返信するアクセス制御部とを備える、車載機システム。

【請求項2】

データ記録部を有する携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部を備える車載機であって、

前記通信部が通信可能な前記携帯端末を検出する端末状態監視部と、

ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース部と、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行部と、

前記端末状態監視部によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス部とを備え、前記実行部は、

前記端末状態監視部によって携帯端末が検出された場合は、

前記携帯端末の前記データ記録部からの前記ユーザ固有情報の読み出しを、前記アクセス部に対して指示し、ユーザの指示に基づく前記処理に際して、読み出した前記ユーザ固有情報を用いて処理し、前記処理においてユーザ固有情報が生成または更新された場合に、当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を前記アクセス部に対して指示し、前記アクセス部が前記携帯端末へ前記ユーザ固有情報の書き込み・更新要求をした後、車載機上のユーザ固有情報を削除し、

前記端末状態監視部によって携帯端末が検出されない場合は、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行し、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上のユーザ固有情報を削除することを特徴とする車載機。

【請求項3】

特定の携帯端末のデータ記録部へアクセスするための認証情報を予め記録しておく車載機側認証情報記録部をさらに備え、

前記端末状態監視部によって携帯端末が検出された場合に、前記認証情報を、前記通信部を介して前記携帯端末に送信し、当該携帯端末のデータ記録部へのアクセス権限の有無の通知を、前記通信部を介して前記携帯端末から受信する権限判定部をさらに備え、

前記アクセス部は、前記権限判定部が、前記アクセス権限が有る旨の通知を受信した場合にのみ、前記携帯端末の前記データ記録部に対するユーザ固有情報の書き込み・更新要求、または読み出し要求を行う、請求項2に記載の車載機。

【請求項4】

前記ユーザ固有情報は、アクセス制限されたデータと、アクセス無制限のデータとを含み、

10

20

30

40

50

前記端末状態監視部は、前記通信部が前記携帯端末と通信可能な状態にあるか否かを監視する機能をさらに備え、

前記アクセス部が読み出しまたは書き込み・更新が可能なデータを記録する一時待避データ記録部と、

前記端末状態監視部が通信可能と判断しているときは、アクセス部による読み出し要求で読み出されたユーザ固有情報のうちアクセス無制限のデータを前記一時待避データ記録部に記録しておく一時待避データ更新部をさらに備え、

前記端末状態監視部が通信可能な状態にないことを検出した場合、前記アクセス部は、アクセス無制限のデータについては、前記一時待避データ記録部に対して読み出しや書き込みを行い、アクセス制限されたデータについては、前記実行部からの読み出しまたは書き込み・更新指示に対して不可能である旨の通知を返し、前記実行部は、書き込み・更新指示にかかるアクセス制限されたデータを所定のタイミングで削除し、

前記端末状態監視部が再び通信可能な状態になったことを検出した場合、前記アクセス部は、前回通信不可能な状態であることが検出されたとき以降に更新された一時待避データ記録部のデータを前記携帯端末の前記データ記録部に書き込む要求を行う、請求項 2 または 3 に記載の車載機。

【請求項 5】

車載機と有線または無線による通信を行う通信部と、

前記通信部が通信可能な車載機を検出する車載機状態監視部と、

特定のユーザに関する情報であって、車載機における処理に関わる情報であるユーザ固有情報を記録するデータ記録部と、

前記車載機状態監視部が検出した車載機からの前記データ記録部に対するユーザ固有情報の読み出し要求、または書き込み・更新要求とユーザ固有情報を、前記通信部を介して受信し、当該読み出し要求または書き込み要求に基づいて、前記データ記録部に対するユーザ固有情報の読み出し、または書き込み・更新処理を行い、当該処理結果を、前記車載機へ前記通信部を介して返信するアクセス制御部と、

所定のプログラムに基づいた所定の処理を実行し、当該所定の処理の結果を、前記通信部を介して車載機へ送信する実行部であって、当該所定の処理において、ユーザ固有情報を使用する場合に、前記アクセス制御部に対して当該ユーザ固有情報の読み出しを要求し、前記所定の処理において、ユーザ固有情報が生成または更新された場合は、前記アクセス制御部に対して当該ユーザ固有情報の書き込みを要求する実行部と、を備えた携帯端末

【請求項 6】

前記データ記憶部へのアクセスを認証するか否か判断するための認証情報を予め記録している端末側認証情報記録部と、

前記車載機が前記データ記録部へアクセスするための認証情報を、前記車載機から前記通信部を介して受信し、当該認証情報と前記端末側認証情報記録部の認証情報とを照会し、前記車載機が当該携帯端末に対して書き込み処理または読み出し処理をする権限があるか否かを認証判定し、前記通信部を介して前記車載機に認証判定結果を送信する認証部とをさらに備え、

前記アクセス制御部は、処理権限が認証された車載機からの要求に基づいて処理し、処理権限が認証されなかった車載機からの要求には権限がない旨の通知を、前記通信部を介して前記車載機に行うことを特徴とした、請求項 5 に記載の携帯端末。

【請求項 7】

データ記録部を有する携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部とを備える車載機に処理を実行させるプログラムであって、

前記通信部が通信可能な前記携帯端末を検出する端末状態監視処理と、

ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース処理と、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用

10

20

30

40

50

いて実行する実行処理と、

前記端末状態監視処理によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス処理とを車載機に実行させ、

前記端末状態監視処理によって携帯端末が検出された場合は、

前記実行処理において、前記アクセス処理で前記携帯端末の前記データ記録部から読み出された前記ユーザ固有情報を用いてユーザの指示に基づく前記処理が実行され、前記処理においてユーザ固有情報が生成または更新された場合に、前記アクセス処理で当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を要求が行われた後、車載機上の前記ユーザ固有情報が削除され、

10

前記端末状態監視処理によって携帯端末が検出されない場合は、

前記実行処理において、前記車載機用データ記録部に記録されたデータを用いて前記ユーザの指示に基づく処理が実行され、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上の前記ユーザ固有情報が削除されることを特徴とする、プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、互いに連携して情報処理を行う車載機および携帯端末、並びにそれらを含む車載機システムに関する。

20

【背景技術】

【0002】

従来の車載機では、個人にかかわる情報をすべて車載機内に記録していた。例えば、カーナビゲーション機能を持つ車載機には、利用経路や目的地の履歴、メモリ地点等が記録される。また、ハンズフリー通話機能を持つ車載機には、通話履歴、アドレス帳情報等が記録される。ところで、車は必ずしも一人で利用するとは限らない。例えば、家族や職場のメンバーなどで1台の車を共用する場合や、自分の車を友人に運転してもらった場合等がある。このため、車載機に保存された個人情報、意図せずに他人の目に触れることがあるという課題がある。また、車が盗難にあった場合でも、盗人が車載機を起動するだけで保存されていた個人情報が漏れてしまうという課題や、情報そのものが失われるという課題がある。

30

【0003】

これらの課題を解決するため、車内の個人情報を暗号化し、可搬媒体に復号のための情報を持たせて、その情報を利用して個人情報を復号化する方式が提案されている（例えば、特許文献1参照）。あるいは、生体情報を用いて個人認証を行い、車載機の利用を許可する方式が提案されている（例えば、特許文献2参照）。

【0004】

しかしながら、上記のいずれの手法でも、個人情報そのものは車載機に保持されているため、例えば、車が盗難に遭った場合等は、車とともに情報が失われる。このように、従来の車載機では、個人情報の漏洩および紛失の危険が依然として残っていた。

40

【特許文献1】特開2002-57664号公報

【特許文献2】国際公開第W02004/055302号パンフレット

【発明の開示】

【発明が解決しようとする課題】

【0005】

本発明は、上記の問題点に鑑みてなされたものであり、その目的は、車載機を通じた情報の漏洩と、車の紛失等による情報の紛失との危険をさけることができる車載機、携帯端末、車載機システム、車載機用のプログラムを提供することにある。

【課題を解決するための手段】

50

【0006】

本発明にかかる車載機システムは、特定のユーザに関する情報であって、車載機における処理に関わる情報であるユーザ固有情報を記録するデータ記録部を有する携帯端末と、当該携帯端末と互いに通信可能な車載機とを含む車載機システムである。前記車載機は、携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部と、前記通信部が通信可能な前記携帯端末を検出する端末状態監視部と、ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース部と、前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行部と、前記端末状態監視部によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス部とを備える。前記実行部は、前記端末状態監視部によって携帯端末が検出された場合は、前記携帯端末の前記データ記録部から前記ユーザ固有情報の読み出しを、前記アクセス部に対して指示し、ユーザの指示に基づく前記処理に際して、読み出した前記ユーザ固有情報を用いて処理し、前記処理においてユーザ固有情報が生成または更新された場合に、当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を前記アクセス部に対して指示し、前記アクセス部が前記ユーザ固有情報を前記携帯端末に書き込み・更新要求をした後、車載機上のユーザ固有情報を削除する。前記実行部は、前記端末状態監視部によって携帯端末が検出されない場合は、前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行し、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上のユーザ固有情報を削除する。前記携帯端末は、車載機と有線または無線による通信を行う通信部と、前記通信部が通信可能な車載機を検出する車載機状態監視部と、前記車載機状態監視部が検出した車載機からの前記データ記録部に対するユーザ固有情報の読み出し要求、または書き込み・更新要求とユーザ固有情報を、前記通信部を介して受信し、当該読み出し要求または書き込み・更新要求に基づいて、前記データ記録部に対するユーザ固有情報の読み出し、または書き込み・更新処理を行い、当該処理結果を、前記車載機へ前記通信部を介して返信するアクセス制御部とを備える。

10

20

【0007】

上記構成により、車載器と通信可能な携帯端末が検出された場合、ユーザインタフェース部を介したユーザの指示に基づく実行部の処理で使用されるユーザ固有情報は、アクセス部によって携帯端末のデータ記録部から読み出される。また、実行部の処理において生成または更新したユーザ固有情報は、アクセス部により、携帯端末のデータ記録部に書き込まれる。一方、車載器と通信可能な携帯端末が検出されなかった場合、実行部は、ユーザの指示に基づく処理を車載機用データ記録部に記録されたデータを用いて実行し、この処理において、ユーザ固有情報が生成された場合は、所定のタイミングで削除する。そのため、実行部の処理に関わるユーザ固有情報は、通信可能な携帯端末が検出された場合および検出されない場合のいずれの場合であっても、車載機ではなく、携帯端末のデータ記録部に記録されることになる。すなわち、車載機にユーザ固有情報が残らない。その結果、車載機を通じてユーザ固有情報が漏洩する危険をさけることができ、かつ、車載機が搭載された車が盗難等により失われても、車とともにユーザ固有情報が失われるという危険もさけることができる。

30

40

【0008】

本発明にかかる車載機は、データ記録部を有する携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部を備える車載機であって、前記通信部が通信可能な前記携帯端末を検出する端末状態監視部と、ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース部と、前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行部と、前記端末状態監視部によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報で

50

あるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス部とを備える。前記実行部は、前記端末状態監視部によって携帯端末が検出された場合は、前記携帯端末の前記データ記録部からの前記ユーザ固有情報の読み出しを、前記アクセス部に対して指示し、ユーザの指示に基づく前記処理に際して、読み出した前記ユーザ固有情報を用いて処理し、前記処理においてユーザ固有情報が生成または更新された場合に、当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を前記アクセス部に対して指示し、前記アクセス部が前記携帯端末へ前記ユーザ固有情報の書き込み・更新要求をした後、車載機上のユーザ固有情報を削除する。前記実行部は、前記端末状態監視部によって携帯端末が検出されない場合は、前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて

10

【0009】

上記構成により、実行部の処理に関わるユーザ固有情報は、通信可能な携帯端末が検出された場合および検出されない場合のいずれの場合であっても、車載機ではなく、携帯端末のデータ記録部に記録されることになる。すなわち、車載機にユーザ固有情報が残らない。

【0010】

本発明にかかる車載機は、特定の携帯端末のデータ記録部へアクセスするための認証情報を予め記録しておく車載機側認証情報記録部をさらに備え、前記端末状態監視部によって携帯端末が検出された場合に、前記認証情報を、前記通信部を介して前記携帯端末に送信し、当該携帯端末のデータ記録部へのアクセス権限の有無の通知を、前記通信部を介して前記携帯端末から受信する権限判定部をさらに備え、前記アクセス部は、前記権限判定部が、前記アクセス権限が有る旨の通知を受信した場合にのみ、前記携帯端末の前記データ記録部に対するユーザ固有情報の書き込み・更新要求、または読み出し要求を行うことが好ましい。

20

【0011】

上記構成により、携帯端末が検出された場合、権限判定部は、予め記録された認証情報を使って、携帯端末のデータ記録部へのアクセス権限の有無を示す情報を得ることができる。そのため、アクセス部は、携帯端末のデータ記録部へのアクセス権限がある場合にのみ、当該データ記録部に対するユーザ固有情報の書き込み・更新要求、または読み出し要求を行うことができる。すなわち、携帯端末からアクセス権限が付与された場合にのみ、その携帯端末と車載機との間でユーザ固有データのやり取りが可能になる。そのため、ユーザ固有データの漏洩をより確実に防ぐことができる。

30

【0012】

本発明にかかる車載機は、ユーザの認証情報の入力を受け付け、当該ユーザの認証情報に基づいて、前記データ記録部内のデータのうち、アクセス可能な範囲を示すアクセスレベルを決定する車載機側レベル決定部をさらに備え、前記通信部は、前記車載機側レベル決定部が決定したアクセスレベルを、前記携帯端末に送信することが好ましい。

【0013】

上記構成により、データ記録部内のデータのうち、アクセス可能な範囲を示すアクセスレベルが、携帯端末に送信される。そのため、携帯端末では、データ記録部内のデータのうち、車載機のアクセス部がアクセス可能な範囲を、ユーザの認証情報に応じて設定することができる。その結果、アクセス部が携帯端末のデータ記録部に対してアクセスできるユーザ固有情報の範囲を、ユーザに応じて柔軟に調節することが可能になる。

40

【0014】

本発明にかかる車載機において、前記ユーザ固有情報は、アクセス制限されたデータと、アクセス無制限のデータとを含み、前記端末状態監視部は、前記通信部が前記携帯端末と通信可能な状態にあるか否かを監視する機能をさらに備える態様とすることができる。前記車載機は、前記アクセス部が読み出しまたは書き込み・更新が可能なデータを記録す

50

る一時待避データ記録部と、前記端末状態監視部が通信可能と判断しているときは、アクセス部による読み出し要求で読み出されたユーザ固有情報のうちアクセス無制限のデータを前記一時待避データ記録部に記録しておく一時待避データ更新部をさらに備えてもよく、前記端末状態監視部が通信可能な状態にないことを検出した場合、前記アクセス部はアクセス無制限のデータについては、前記一時待避データ記録部に対して読み出しや書き込みを行い、アクセス制限されたデータについては、前記実行部からの読み出しまたは書き込み・更新指示に対して不可能である旨の通知を返し、前記実行部は、書き込み・更新指示にかかるアクセス制限されたデータを所定のタイミングで削除する態様とすることができる。前記端末状態監視部が再び通信可能な状態になったことを検出した場合、前記アクセス部は、前回通信不可能な状態であることが検出されたとき以降に更新された一時待避データ記録部のデータを前記携帯端末の前記データ記録部に書き込む要求を行う態様とすることができる。

10

【0015】

上記構成により、通信部が携帯端末と通信不可能な状態になった場合は、アクセス制限されたユーザ固有情報について、アクセス部は、実行部からの読み出しまたは書き込み指示に対して、不可能である旨の通知を返す。そのため、実行部は、通信部が携帯端末と通信不可能な状態にある場合には、アクセス制限されたユーザ固有情報の読み出し、書き込み・更新が不可能であることを知ることができ、また、書き込もうとしたユーザ固有情報は削除される。その結果、通信部が携帯端末と通信不可能な状態である場合には、アクセス制限されたユーザ固有情報の使用およびユーザ固有情報の記録は行われず、ひいては、ユーザ固有情報が不正に使用される危険性が低くなる。さらに、アクセス無制限に設定されているユーザ固有情報については、車載機側の一時待避データ記録部に情報を記録しておき、携帯端末と接続されていない状態でも利用することができるため、利便性を確保することができる。また、携帯端末と再度接続されたときには、接続されていない間に更新されたユーザ固有情報を携帯端末に自動的に書き込むため、車両の盗難に伴う情報の紛失は最低限に抑えられる。

20

【0016】

本発明にかかる携帯端末は、車載機と有線または無線による通信を行う通信部と、前記通信部が通信可能な車載機を検出する車載機状態監視部と、特定のユーザに関する情報であって、車載機における処理に関わる情報であるユーザ固有情報を記録するデータ記録部と、前記車載機状態監視部が検出した車載機からの前記データ記録部に対するユーザ固有情報の読み出し要求、または書き込み・更新要求とユーザ固有情報を、前記通信部を介して受信し、当該読み出し要求または書き込み要求に基づいて、前記データ記録部に対するユーザ固有情報の読み出し、または書き込み・更新処理を行い、当該処理結果を、前記車載機へ前記通信部を介して返信するアクセス制御部とを備える。

30

【0017】

上記構成により、アクセス制御部が、携帯端末と通信可能な車載機からの要求に応じて、ユーザ固有情報の書き込み・更新または読み出しを行い、車載機に処理結果を返信する。そのため、例えば、車載機で使用されるユーザ固有情報や、車載機で生成または更新されたユーザ固有情報等を、携帯端末側で記録しておくことができる。その結果、車載機を通じてユーザ固有情報が漏洩する危険をさけることができ、かつ、車載機が搭載された車が盗難等により失われても、車とともにユーザ固有情報が失われるという危険もさけることができる。

40

【0018】

本発明にかかる携帯端末は、前記データ記憶部へのアクセスを認証するか否か判断するための認証情報を予め記録している端末側認証情報記録部と、前記車載機が前記データ記録部へアクセスするための認証情報を、前記車載機から前記通信部を介して受信し、当該認証情報と前記端末側認証情報記録部の認証情報とを照会し、前記車載機が当該携帯端末に対して書き込み処理または読み出し処理をする権限があるか否かを認証判定し、前記通信部を介して前記車載機に認証判定結果を送信する認証部とをさらに備え、前記アクセス

50

制御部は、処理権限が認証された車載機からの要求に基づいて処理し、処理権限が認証されなかった車載機からの要求には権限がない旨の通知を、前記通信部を介して前記車載機に行う態様としてもよい。

【0019】

上記構成において、認証部は、車載機から受信した認証情報を基に、車載機が当該携帯端末に対して書き込み・更新処理または読み出し処理をする権限があるか否かを認証判定して認証判定結果を車載機に送信する。そして、アクセス制御部は、認証された車載機からの要求に基づいてユーザ固有情報の書き込み・更新または読み出し処理を行う。そのため、車載機からデータ記録部に対するユーザ固有情報の書き込み、読み出しの可否が認証情報を基に制御される。

10

【0020】

本発明にかかる携帯端末は、所定のプログラムに基づいた所定の処理を実行し、当該所定の処理の結果を、前記通信部を介して車載機へ送信する実行部であって、当該所定の処理において、ユーザ固有情報を使用する場合に、前記アクセス制御部に対して当該ユーザ固有情報の読み出しを要求し、前記所定の処理において、ユーザ固有情報が生成または更新された場合は、前記アクセス部に対して当該ユーザ固有情報の書き込みを要求する実行部をさらに備える態様とすることができる。

【0021】

上記構成により、携帯端末が実行部を備えることにより、ユーザ固有情報を使用する処理、更新または生成する処理も携帯端末側で実行され、車載機には、その実行結果のみが送信されることになる。そのため、車載機側でユーザ固有情報を使用、更新または生成する処理を行う必要がなくなる。その結果、ユーザ固有情報を車載機側に送信する必要がなくなるため、より確実にユーザ固有情報の漏洩を防ぐことができる。

20

【0022】

本発明にかかる携帯端末は、ユーザの認証情報の入力を受け付け、当該ユーザの認証情報に基づいて、前記アクセス制御部が、前記データ記録部内のユーザ固有情報のうち書き込みまたは読み出しできるデータの範囲を示すアクセスレベルを決定する端末側レベル決定部をさらに備える態様とすることができる。

【0023】

上記構成により、端末側レベル決定部は、データ記録部内のユーザ固有情報のうちアクセス制御部がアクセス可能な範囲を、ユーザの認証情報に応じて設定することができる。すなわち、車載機からデータ記録部に対するアクセス可能なユーザ固有情報の範囲が、ユーザに応じて設定される。その結果、車載機がデータ記録部に対してアクセス可能なユーザ固有情報を、ユーザに応じて柔軟に調節することが可能になる。

30

【0024】

本発明にかかる携帯端末において、前記アクセス制御部は、前記端末側アクセスレベル決定部により決定されたアクセスレベルまたは、通信部が車載機から受信したアクセスレベルに基づいて、前記データ記録部内のユーザ固有情報のうち、前記アクセスレベルで示される範囲に対して、書き込み・更新、または読み出しを行う態様とすることができる。

【0025】

これにより、アクセス制御部は、認証されたユーザに適したアクセスレベル、または車載機に適したアクセスレベルに従って、ユーザ固有情報のアクセス制限の範囲を制御することができる。これにより、柔軟なユーザ固有情報のアクセス制限が可能になる。

40

【0026】

本発明にかかるプログラムは、データ記録部を有する携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部とを備える車載機に処理を実行させるプログラムであって、前記通信部が通信可能な前記携帯端末を検出する端末状態監視処理と、ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース処理と、前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行処理と、前記端末状態監視

50

処理によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス処理とを車載機に実行させる。前記端末状態監視処理によって携帯端末が検出された場合は、前記実行処理において、前記アクセス処理で前記携帯端末の前記データ記録部から読み出された前記ユーザ固有情報を用いてユーザの指示に基づく前記処理が実行され、前記処理においてユーザ固有情報が生成または更新された場合に、前記アクセス処理で当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を要求が行われた後、車載機上の前記ユーザ固有情報が削除される。前記端末状態監視処理によって携帯端末が検出されない場合は、前記実行処理において、前記車載機用データ記録部に記録されたデータを用いて前記ユーザの指示に基づく処理が実行され、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上の前記ユーザ固有情報が削除される。

10

【発明の効果】

【0027】

本発明によれば、車載機を通じた情報の漏洩と、車の紛失等による情報の紛失との危険をさけることができる車載機、携帯端末、車載機システム、車載機用のプログラムを提供することができる。

【発明を実施するための最良の形態】

【0028】

以下、本発明のより具体的な実施形態について図面を参照しながら詳細に説明する。

20

【0029】

(実施の形態1)

図1は、本実施形態にかかる車載機システムの構成を表す機能ブロック図である。図1に示す車載機システムは、車載機1と携帯端末2とを備える。車載機1は、車両に設けられる情報処理装置である。携帯端末は、携帯型の情報処理装置である。携帯端末の例として、例えば、携帯電話、PHS(Personal Handyphone System)、PDA(Personal Digital Assistance)、音楽プレーヤ、映像再生機、携帯ゲーム機等が挙げられる。

【0030】

車載機1と携帯端末2とは、互いに有線で接続することができ、接続されることによって互いに通信可能となる。なお、車載機1と携帯端末2とは、無線により通信を行う構成であってもよい。この場合の無線による通信には、例えば、IrDA(Infrared Data Association)規格のような赤外線通信技術や、無線LAN、Bluetooth、NFC(Near field Communication)等のような電波通信技術を用いることができる。

30

【0031】

本実施形態では、一例として、車載機1がカーナビゲーション機能およびハンズフリー通話機能を持ち、携帯端末2が携帯電話である場合について説明する。

【0032】

[車載機の構成]

図1に示す車載機1は、実行部11、UI(ユーザインタフェース)18、アクセス部12、通信部14、端末状態監視部17、車載機用データ記録部16を備える。

40

【0033】

車載機用データ記録部16には、車載機1のカーナビゲーション機能およびハンズフリー通話機能を実現するためのアプリケーションプログラムおよびデータが記録されている。実行部11は、車載機用データ記録部16に記録されたアプリケーションプログラムに従って所定の処理を実行する。これにより、カーナビゲーション機能およびハンズフリー通話機能が実現される。実行部11は、処理を実行する際に、UI18を介して、ユーザからの指示を受け付けたり、実行部11の処理結果をユーザに出力したりする。すなわち、UI18は、ボタン、コントローラ、マイク、タッチパネル等のユーザがデータを入力するための入力装置や、ディスプレイ、スピーカ等の出力装置を含む。

【0034】

50

本実施形態においては、実行部 11 の処理に関わるデータのうち、特定のユーザに関する情報であるユーザ固有情報は、車載機用データ記録部 16 には記録されないで、携帯端末 2 のデータ記録部 21 に記録される。そのために、実行部 11 は、ユーザ固有情報の読み出しや書き込み・更新をアクセス部 12 に対して指示する。アクセス部 12 は、実行部 11 からの要求に基づいて、携帯端末 2 のデータ記録部 21 に対するデータの書き込み・更新要求、または読み出し要求を、通信部 14 を介して行う。

【0035】

ここでは一例として、アクセス部 12 は、処理においてユーザ固有データを利用する際に、それに先立って、ユーザ固有データの読み出しの指示をするが、例えば、処理の最初に一括してユーザ固有データを読み込む指示を出してもよい。この場合、また、書き込み・更新指示も同様に、ユーザ固有データが生成または更新されたタイミングで行われてもよいし、処理の終了時、または車載機 1 が設けられた車両のキーのオフ時に一括して書き込み・更新を指示してもよい。

10

【0036】

なお、実行部 11 が、アクセス部 12 に対して出す要求は、上述の書き込み要求および読み出し要求に限られない。実行部 11 は、例えば、後述するように、携帯端末 2 の接続の状態や、携帯端末 2 へのアクセス権限の有無を問い合わせる要求を出してもよい。

【0037】

通信部 14 は、携帯端末 2 との通信を可能にするための通信インタフェースである。通信部 14 は、例えば、アクセス部 12 から、携帯端末 2 のデータ記録部 21 に対するデータの書き込み、または読み出しの要求を受け取って、携帯端末 2 へ送信する。また、通信部 14 は、携帯端末 2 から送信されたデータを受信して、アクセス部 12 または権限判定部 13 へ渡す。

20

【0038】

端末状態監視部 17 は、通信部 14 と通信可能な状態にあるが携帯端末 2 を検出し、検出結果をアクセス部 12 に通知する。アクセス部 12 は、通信可能な携帯端末がない場合には、実行部 11 からの読み出しまたは書き込み指示に対して不可能である旨の通知を返す。この場合、実行部 11 は、車載機用データ記録部 16 に記録されたデータを用いユーザの指示に基づく処理を実行する。この処理においてユーザ固有情報が生成または更新された場合は、所定のタイミングで、ユーザ固有情報を車載機上の記録媒体（例えば、メモリ等（図示せず））から削除する。実行部 11 は、例えば、生成または更新されたユーザ固有情報が処理において不要になった場合に削除してもよいし、車両のキーオフ時に一括して削除してもよい。

30

【0039】

端末状態監視部 17 は、有線通信の場合は、例えば、携帯端末 2 の接続および切断を検出することにより、通信可能な状態にあるか否かを判定することができる。端末状態監視部 17 は、無線通信の場合は、例えば、一定間隔で携帯端末 2 から送信される所定のメッセージ（例えば、ビーコンまたは死活監視メッセージ等）を受信することによって、通信可能な状態にあるか否かを判定することができる。

【0040】

[携帯端末の構成]

図 1 に示す携帯端末 2 は、データ記録部 21、データ読み出し部 22、データ書き込み部 23、アクセス制御部 24、車載機状態監視部 26、通信部 27 を備える。

40

【0041】

データ記録部 21 には、携帯端末 2 のユーザに関するユーザ固有情報が記録される。ユーザ固有情報は、ユーザに固有の情報であり、車載機 1 の機能の実現するための処理において使用、生成または更新される情報である。ユーザ固有情報には、例えば、ユーザ固有情報は、プライバシーの観点から保護されるべき情報や、ユーザ固有の情報であるために、紛失したらユーザが非常に困る情報等が含まれる。本実施形態においては、データ記録部 21 に記録されるユーザ固有情報に、車載機 1 のカーナビゲーション機能、およびハン

50

ズフリー通話機能で使用、生成または更新されるデータが含まれる。

【 0 0 4 2 】

図 2 は、データ記録部 2 1 に記録されるユーザ固有情報の一例を示す図である。図 2 に示す例は、カーナビゲーション機能で使用されるユーザ固有情報である。例えば、自宅位置、メモリ地点、目的地履歴、通過経路等を表すデータが記録される。

【 0 0 4 3 】

図 3 も、データ記録部 2 1 に記録されるユーザ固有情報の一例を示す図である。図 3 に示す例は、ハンズフリー通話機能で使用されるユーザ固有情報である。例えば、電話帳、発信履歴、着信履歴等を表すデータが記録される。

【 0 0 4 4 】

なお、図 2、3 に示すユーザ固有情報は、一例であり、データの内容はこれに限られない。例えば、特定場所の滞在時間や、特定地点の訪問回数、特定施設の利用回数、有料道路の利用回数、利用料金、利用日時等もユーザ固有情報に含まれても良い。データ記録部 2 1 に記録されるユーザ固有情報の項目は予め決められていてもよいし、車載機 1 の実行部 1 1 において生成または更新されたデータが自動的にユーザ固有情報としてデータ記録部 2 1 に記録されるようにしてもよい。

【 0 0 4 5 】

データ書き込み部 2 3 は、アクセス制御部 2 4 の指示に従って、データ記録部 2 1 へデータを書き込む処理を行い、データ読み出し部 2 2 は、データ記録部 2 1 からデータを読み出す処理を行う。

【 0 0 4 6 】

アクセス制御部 2 4 は、データ読み出し部 2 2 およびデータ書き込み部 2 3 を制御することにより、データ記録部 2 1 に対するデータの書き込みおよび読み出しを制御する。アクセス制御部 2 4 は、通信部 2 7 を介して送られてくるユーザ固有情報の読み出しまたは書き込み要求に応じて、データ記録部 2 1 に対するデータの書き込みおよび読み出しを行う。

【 0 0 4 7 】

通信部 2 7 は、車載機 1 との通信を可能にするための通信インタフェースである。通信部 2 7 は、例えば、携帯端末 2 のデータ記録部 2 1 に対するデータの書き込み要求、または読み出し要求を、車載機 1 から受信してアクセス制御部 2 4 へ渡す。このように、通信部 2 7 は、車載機 1 と携帯端末 2 との間で通信されるデータを中継する。なお、通信部 2 7 が中継するデータは、上記の書き込みまたは読み出し要求およびその処理結果に限られない。

【 0 0 4 8 】

車載機状態監視部 2 6 は、通信部 2 7 が通信可能な車載機 1 を検出し、検出結果をアクセス制御部 2 4 および認証部 2 5 に通知する。通信可能な状態にある車載機 1 があるか否かは、有線通信の場合は、例えば、携帯端末 2 の接続および切断を検出することにより判定できる。無線通信の場合は、例えば、車載機 1 からの通信開始要求等の所定のメッセージを受信することにより、通信可能な状態にあるか否かを判定することができる。

【 0 0 4 9 】

以上、図 1 に示した車載機 1 および携帯端末の構成は、一例であって、これに限られない。例えば、上記構成では、車載機 1 で生成または更新されたユーザ固有情報が、データ記録部 2 1 に書き込まれる構成になっているが、例えば、携帯端末 2 も、ユーザがデータを入力するためのユーザインタフェースを備え、ユーザインタフェースを介して入力されたユーザ固有情報が、データ記録部 2 1 に書き込まれる構成となってもよい。これにより、ユーザが、車載機 1 での処理に関わるユーザ固有情報を閲覧したり、編集したりすることができるようになる。

【 0 0 5 0 】

[車載機 1 の動作例]

次に車載機 1 の動作について説明する。図 4 は、車載機 1 のアクセス部 1 2 の動作例を

10

20

30

40

50

示すフローチャートである。図 4 に示す例は、アクセス部 1 2 が、実行部 1 1 から、ユーザ固有情報の読み出しまたは書き込みの要求を受ける動作から始まる (Op 1 1)。

【0051】

ここで、実行部 1 1 が、ユーザ情報の読み出しまたは書き込み要求する場合の例を説明する。例えば、実行部 1 1 が、カーナビゲーション機能の処理を実行している際に、ユーザから、これまでに行った目的地の履歴を表示する指示が、UI 1 8 を介して入力された場合、携帯端末 2 のデータ記録部 2 1 から目的地履歴を読み込むことをアクセス部 1 2 に対して要求する。また、ユーザが、自宅位置を、UI 1 8 を介して入力した場合、実行部 1 1 は、データ記録部 2 1 に自宅位置を書き込むことをアクセス部 1 2 に要求する。

【0052】

アクセス部 1 2 は、実行部 1 1 からユーザ固有情報の読み出しまたは書き込みの要求を受けると、端末状態監視部 1 7 に、通信部 1 4 が携帯端末 2 と通信可能な状態になっているか否かを問い合わせる (Op 1 2)。携帯端末 2 との通信が不可能であれば (Op 1 2 で No)、アクセス部 1 2 は、読み出しまたは書き込み不可能である旨の通知を実行部 1 1 へ返し、処理を終了する (Op 1 7)。

【0053】

携帯端末 2 との通信が可能であれば (Op 1 2 で Yes)、アクセス部 1 2 は、ユーザ固有情報の読み出し要求または書き込み要求を通信部 1 4 に渡し、携帯端末 2 へ送信させる。

【0054】

ユーザ固有情報の読み出し要求または書き込み要求を受信した携帯端末 2 は、受信した要求に基づいて、ユーザ固有情報の読み出しまたは書き込み処理を行い、その処理結果を車載機 1 へ返信する。携帯端末 2 側の動作については、後述する。

【0055】

書き込み要求の処理結果は、例えば、書き込みに成功したか否かを示すデータであり、読み出し要求の処理結果は、読み出したユーザ固有情報そのものである。通信部 1 4 は、携帯端末 2 からの処理結果を受信すると、アクセス部 1 2 へ渡す (Op 1 5)。アクセス部 1 2 は、通信部 1 4 から渡された処理結果を、実行部 1 1 へ返す (Op 1 6)。

【0056】

以上、図 4 に示した処理により、実行部 1 1 が処理を実行する際に生成または更新したユーザ固有情報を、携帯端末 2 のデータ記録部 2 1 に記録することができる。また、実行部 1 1 が、ユーザ固有情報を、データ記録部 2 1 から読み出して、処理に使用することができる。例えば、実行部 1 1 が、カーナビゲーション機能の処理を実行する際に、自宅位置、目的地履歴等を、携帯端末 2 のデータ記録部 2 1 から読み出して、車載機 1 の UI 1 8 を介してユーザに表示することができる。また、ユーザが UI 1 8 を介して、目的地、メモリ地点を入力した場合や、自動的に生成される車の通過経路等のユーザ固有情報は、携帯端末 2 のデータ記録部 2 1 に書き込まれることになる。

【0057】

なお、通信不可能な状態である場合は、アクセス部 1 2 が、読み出しまたは書き込み不可能である通知を実行部 1 1 に返す (Op 1 7)。実行部 1 1 は、読み出し不可能であった場合には、ユーザ固有情報を使わずに、車載機用データ記録部 1 6 に記録されたデータを用いて処理を進める。実行部 1 1 は、例えば、自宅位置、目的地履歴等のユーザ固有情報を用いなくても、ユーザから目的地の入力を受け付けて、目的地まで誘導するというカーナビゲーションの基本的な処理は実行することができる。また、実行部 1 1 は、ユーザ固有情報を書き込み不可能であった場合には、書き込もうとしたユーザ固有情報を、車載機 1 に記録せず、破棄することができる。これにより、ユーザ固有情報が車載機 1 に残ることが避けられる。

【0058】

[携帯端末 2 の動作例]

次に、携帯端末 2 の動作について説明する。図 5 は、携帯端末 2 のアクセス制御部 2 4

10

20

30

40

50

の動作例を示すフローチャートである。図5に示す例では、まず、アクセス制御部24が、通信部27を介して、車載機1からユーザ固有情報の読み出しまたは書き込み要求を受信する(Op21)。

【0059】

アクセス制御部24は、読み出しまたは書き込み要求を受信すると、車載機状態監視部26に、通信部27が車載機1と通信可能な状態になっているか否かを問い合わせる(Op22)。車載機1との通信が不可能であれば(Op22でNo)、認証部25が、車載機1のデータ記録部21へのアクセス権限を解除する(Op27)。アクセス制御部24は、読み出しまたは書き込み不可能である旨の通知を通信部27へ渡し、車載機1への返信を試みさせる(Op28)。

10

【0060】

車載機1との通信が可能であれば、アクセス制御部24は、受信した要求が読み出し要求か書き込み要求かを判定する(Op24)。読み出し要求である場合、アクセス制御部24は、データ読み出し部22に読み出し処理を実行させる(Op25b)。書き込み要求である場合、アクセス制御部24は、データ書き込み部23に、書き込み処理を実行させる(Op25a)。

【0061】

アクセス制御部24は、データ書き込み部23からは、データ書き込み処理の処理結果として、書き込みに成功したか否かを示すデータを受け取り、データ読み出し部22からは、データ読み出し処理の処理結果として、読み出したユーザ固有情報を受け取る。アクセス制御部24は、受け取った処理結果を通信部27へ渡し、携帯端末へ送信させる(Op26)。これにより、アクセス制御部24は、車載機1から受信した書き込み要求または読み出し要求を実行し、その処理結果を車載機に返すことができる。

20

【0062】

以上、図4および図5に示した処理により、ユーザ固有情報を全て車載機1ではなく携帯端末2に記録することが可能になる。そのため、ユーザは、車載機1を介したユーザ固有情報の漏洩や、車の紛失等による個人情報の紛失を心配しなくてもよくなる。また、本実施形態では、ユーザ固有情報の移動範囲が、車載機1と携帯端末2に限られるため、ユーザ固有情報が、通信網やサーバ等を通じて流出する危険性も少なくなる。さらに、セキュリティのためのデータセンタやサーバ等の大規模な情報処理施設を設ける必要がないので、運用コストが安くてすむ。

30

【0063】

(実施の形態2)

図6は、本実施形態にかかる車載機システムの構成を表す機能ブロック図である。図6において、図1と同じ部分には同じ番号を付し、詳細な説明を省略する。図6に示す車載機システムにおいて、車載機1cは、図1に示した車載機1に、車載機側認証情報記録部15および権限判定部13を追加した構成になっている。携帯端末2cは、図1に示した携帯端末2に、認証部25および端末側認証情報記録部211を追加した構成になっている。

【0064】

車載機1cにおいて、車載機側認証情報記録部15には、車載機1cが携帯端末2cのデータ記録部21に対するアクセス権限を得るための認証情報が記録される。権限判定部13は、車載機側認証情報記録部15に記録された認証情報を、通信部14を介して携帯端末2cに送信し、携帯端末2cのデータ記録部21へのアクセス権限の有無の通知を、通信部14を介して携帯端末2cから受信する。

40

【0065】

権限判定部13は、アクセス権限の有無をアクセス部12に通知する。これにより、アクセス部12は、アクセス権限があるか否かを示す情報を得ることができる。アクセス部12は、アクセス権限がある場合にのみ、実行部11の要求に応じて、携帯端末2cのデータ記録部21に対するユーザ固有情報の書き込み、または読み出しを行う。

50

【 0 0 6 6 】

携帯端末 2 c において、例えば、車載機状態監視部 2 6 が、車載機 1 c が通信可能な状態になったことを検出した時に、認証部 2 5 が、その車載機 1 c のデータ記録部 2 1 へのアクセス権限の認証を行い、その後、車載機状態監視部 2 6 が、車載機 1 c が通信不可能な状態になったことを検出した時に、認証部 2 5 がそのアクセス権限を解除することができる。これにより、特定の組み合わせの車載機と携帯端末とが接続されている間にだけ、車載機からデータ記録部 2 1 へのアクセスを可能とする構成になる。認証部 2 5 は、アクセス権限の認証の有無を示すデータを、例えば、端末側認証情報記録部 2 1 1 に記録することができる。

【 0 0 6 7 】

認証部 2 5 は、携帯端末 2 c に接続された車載機 1 c が、データ記録部 2 1 に対してアクセス権限を持っていることを認証する。具体的には、認証部 2 5 は、車載機 1 c からの送信された認証情報を通信部 2 7 より受け取り、当該認証情報に基づいて、車載機 1 c のデータ記録部 2 1 に対するアクセス権限の有無を判断する。例えば、認証部 2 5 は、車載機 1 c から送信された認証情報と、端末側認証情報記録部 2 1 1 に予め記録された認証データとを照合し、両者が適合する場合に、車載機 1 c はアクセス権限を持っていると判断することができる。認証部 2 5 は、アクセス権限の有無を示すデータを、通信部 2 7 に渡して、車載機 1 c へ送信させる。

【 0 0 6 8 】

また、認証部 2 5 は、車載機 1 c によるアクセス権限の有無に基づいて、アクセス制御部 2 4 によるデータ記録部 2 1 に対する、車載機 1 c の要求に基づく書き込みまたは読み出しの可否を設定する。認証部 2 5 は、車載機 1 c によるアクセス権限がないと判断した場合は、アクセス制御部 2 4 の書き込みまたは読み出し動作を制限する。認証部 2 5 は、例えば、アクセス制御部 2 4 によるデータ読み出し部 2 2 およびデータ書き込み部 2 3 への指示が可能である旨のフラグ等のデータを端末側認証情報記録部 2 1 1 に記録する。

【 0 0 6 9 】

車載機 1 c から送信される認証情報の具体例として、例えば、ID とパスワードが挙げられる。この場合、端末側認証情報記録部 2 1 1 には、認証データとして、アクセス権限を有する車載機の ID とパスワードを示すデータのリストが記録される。携帯端末 2 c の認証部 2 5 は、車載機 1 c から送信される ID とパスワードを、端末側認証情報記録部 2 1 1 に記録された認証データと照合することにより認証を行う。なお、車載機 1 c の ID とパスワードが携帯端末 2 c 以外の端末への漏洩を防ぐために、例えば、電子割符と呼ばれる技術を用いることによって、ID とパスワードを暗号化し、携帯端末 2 c の認証データとその ID とパスワードが揃って初めて復号できる構成としてもよい。

【 0 0 7 0 】

[車載機 1 c の動作例]

次に車載機 1 c の動作例を、図 7 を参照して説明する。図 7 は、車載機 1 c のアクセス部 1 2 の動作例を示すフローチャートである。図 7 に示す処理において、図 4 に示した処理と同じステップには同じ番号を付し、詳細な説明を省略する。図 7 における Op 1 1、Op 1 2 は、図 4 の Op 1 1、Op 1 2 と同様である。

【 0 0 7 1 】

携帯端末 2 c との通信が可能であれば (Op 1 2 で Yes)、アクセス部 1 2 は、権限判定部 1 3 へ、携帯端末 2 c のデータ記録部 2 1 へのアクセスが許されているか否かを問い合わせる (Op 1 3)。

【 0 0 7 2 】

権限判定部 1 3 は、携帯端末 2 c の車載機 1 c への接続時に、車載機側認証情報記録部 1 5 の認証情報を携帯端末 2 c へ送信して、データ記録部 2 1 へのアクセス権限の有無を問い合わせることにより、携帯端末 2 c より権限の有無を示すデータを取得しておく。その権限の有無を示すデータは、接続が切断されるまで権限判定部 1 3 により保持される。アクセス部 1 2 から問い合わせに対して、権限判定部 1 3 は、保持している権限の有無を示

10

20

30

40

50

すデータを返す。

【 0 0 7 3 】

なお、権限判定部 1 3 は、アクセス部 1 2 から問い合わせが来た時に、車載機側認証情報記録部 1 5 の認証情報を携帯端末 2 c へ送信して、データ記録部 2 1 へのアクセス権限の有無を問い合わせることにより、携帯端末 2 c より権限の有無を示すデータを取得してもよい。

【 0 0 7 4 】

アクセス権限がない場合 (O p 1 3 で N o)、アクセス部 1 2 は、読み出しまたは書き込み不可能である旨の通知を実行部 1 1 へ返し、処理を終了する (O p 1 7)。アクセス権限がある場合 (O p 1 3 で Y e s)、アクセス部 1 2 は、ユーザ固有情報の読み出し要求または書き込み要求を通信部 1 4 に渡し、携帯端末 2 c へ送信させる (O p 1 4)。以降 O p 1 4 ~ O p 1 7 の処理は、図 4 の O p 1 4 ~ O p 1 7 と同様である。

[携帯端末 2 c の動作例]

次に、携帯端末 2 c の動作例について、図 8 を参照して説明する。図 8 は、車載機 1 c のアクセス制御部 2 4 の動作例を示すフローチャートである。図 8 に示す処理において、図 5 に示した処理と同じステップには同じ番号を付し、詳細な説明を省略する。図 8 における O p 2 1、O p 2 2 は、図 5 の O p 2 1、O p 2 2 と同様である。

【 0 0 7 5 】

車載機 1 c との通信が不可能であれば (O p 2 2 で N o)、認証部 2 5 が、車載機 1 c のデータ記録部 2 1 へのアクセス権限を解除する (O p 2 7)。アクセス制御部 2 4 は、読み出しまたは書き込み不可能である旨の通知を通信部 2 7 へ渡し、車載機 1 c への返信を試みさせる (O p 2 8)。

【 0 0 7 6 】

車載機 1 c との通信が可能であれば、アクセス制御部 2 4 は、認証部 2 5 へ、車載機 1 c がデータ記録部 2 1 へのアクセス権限を有しているか否かを問い合わせる (O p 2 3)。認証部 2 5 は、携帯端末 2 c の車載機 1 c への接続時に、車載機 1 c から送信される認証情報と、端末側認証情報記録部 2 1 1 に予め記録された認証データとを照合することにより、車載機 1 c のアクセス権限の有無を判定する。その車載機 1 c のアクセス権限の有無を示すデータは、接続が切断されるまで端末側認証情報記録部 2 1 1 により保存される。アクセス制御部 2 4 から問い合わせに対して、認証部 2 5 は、保存されている車載機 1 c のアクセス権限の有無を示すデータを返す。

【 0 0 7 7 】

アクセス権限がない場合 (O p 2 3 で N o)、アクセス制御部 2 4 は、読み出しまたは書き込み不可能である旨の通知を通信部 2 7 へ渡して、車載機 1 c への返信を試みさせる (O p 2 8)。アクセス権限がある場合 (O p 2 3 で Y e s)、アクセス制御部 2 4 は、受信した要求が読み出し要求か書き込み要求かを判定する (O p 2 4)。以降の O p 2 4 ~ O p 2 6 の処理は図 5 の O p 2 4 ~ O p 2 6 と同様である。

【 0 0 7 8 】

以上、本実施の形態では、携帯端末 2 c が認証した車載機 1 c のみが、ユーザ固有情報のデータ記録部 2 1 へアクセス可能となる。そのため、ユーザ固有データの漏洩をより確実に防ぐことができる。

【 0 0 7 9 】

(実施の形態 3)

図 9 は、本実施形態にかかる車載機システムの構成を表す機能ブロック図である。図 9 において、図 6 と同じ部分には同じ番号を付し、詳細な説明を省略する。図 9 に示す車載機システムにおいて、車載機 1 c は、図 6 に示した車載機 1 c と同じである。携帯端末 2 a は、図 1 に示した携帯端末 2 に、レベル決定部 2 8 およびユーザ認証デバイス 2 9 を追加した構成になっている。

【 0 0 8 0 】

ユーザ認証デバイス 2 9 は、ユーザの認証情報の入力を受け付けて、携帯端末 2 a のユ

10

20

30

40

50

ーザを認証するデバイスである。ユーザの認証情報は、それにより、ユーザを特定できる情報である。例えば、ユーザの認証情報として、予め決められたユーザのパスワード、または指紋等のユーザの生体情報等が挙げられる。ユーザ認証デバイス 29 の例として、例えば、指紋認証装置等が挙げられる。

【 0 0 8 1 】

レベル決定部 28 は、ユーザ認証デバイス 29 で特定されたユーザに基づいて、データ記録部 21 のデータのうち、アクセス可能な範囲を示すアクセスレベルを決定する。レベル決定部 28 は、例えば、ユーザ認証デバイス 29 で特定されたユーザが、携帯端末 2a に対してどの程度の権限を有しているかを判断し、判断結果に基づいてアクセスレベルを決定する。ユーザ認証デバイス 29 で特定されたユーザの権限を判断するには、例えば、
10 携帯端末 2a において、ユーザとアクセスレベルとを対応付けるデータを予め記録しておく、そのデータを用いて判断することができる。さらに、認証されたユーザに与えられたアクセスレベルを上限として、どのレベルまで公開するかを携帯端末 2a でユーザが明示的に指定できるようにしても良い。

【 0 0 8 2 】

アクセス制御部 24 は、レベル決定部 28 が決定したアクセスレベルで示される範囲のデータのみアクセスするように、データ書き込み部 23、データ読み出し部 22 を制御する。

【 0 0 8 3 】

アクセスレベルの定義の一例を下記表 1 に示す。下記表 1 は、例えば、レベル値 = 5 の
20 データは、携帯端末 2a の持ち主本人だけが利用可能であることを示している。

【 0 0 8 4 】

【表 1】

レベル値	アクセス可能なユーザ
5	本人だけ利用可能
4	家族でも利用可能
3	友人でも利用可能
2	知り合い程度の人でも利用可能
1	電話と接続できていればだれでも利用可能
0	制限なし

【 0 0 8 5 】

上記表 1 のようにアクセスレベルのレベル値が定義されている場合、レベル決定部 28 は、例えば、ユーザ認証デバイス 29 で特定されたユーザが、本人、家族、友人、知り合い、それ以外のいずれであるかによって、レベル値を決定することができる。ユーザ認証デバイス 29 が、入力されたユーザの認証情報から、本人、家族、友人、知り合い、それ以外のいずれであるかを特定するには、例えば、認証情報と、ユーザ属性（本人、家族、友人、知り合い、またはそれ以外）との対応関係を示すデータを予め携帯端末 2a に記録しておくことよ
40 い。レベル決定部 28 は、そのデータを用いてユーザ属性を判定することができる。

【 0 0 8 6 】

アクセスレベルは、例えば、データ記録部 21 に記録されるユーザ固有情報に付加して記録することができる。図 10 は、アクセスレベルのレベル値が付加されたユーザ固有情報の一例を示す図である。図 10 に示す例では、ユーザ固有情報は階層構造になって記録されている。すなわち、上位項目である各保存項目の下位に 1 項目以上の保存データが記録され、各保存データの下位にさらに 1 項目以上のデータが記録されている。例えば、保存項目「自宅位置」の下位の保存データの項目として「位置」があり、「位置」の下位の項目として「緯度」、「経度」がある。

【 0 0 8 7 】

10

20

30

40

50

図10に示す例では、各階層の項目ごとにレベル値が設定されている。なお、図中「-」は、上位項目のレベル値を継承していることを示している。例えば、「メモリ地点」の項目のレベル値は「4」であり、その下位項目の「データ1」のレベル値は「3」である。「データ2」のレベル値「-」は、上位項目の「メモリ地点」のレベル値「4」を継承していることを示している。

【0088】

例えば、保存項目「メモリ地点」のデータは、レベル値「4」なので、携帯端末2aの持ち主本人か、その家族は利用可能だが、友人は利用できない。また、「メモリ地点」の下位の「データ1」に含まれるデータは、レベル値「3」なので、友人でも利用できる。

【0089】

アクセス制御部24は、レベル決定部28が決定したレベル値が、書き込みまたは読み出そうとするデータの項目のレベル値と等しいか、大きい場合にのみ、そのデータにアクセスすることが可能となる。例えば、レベル決定部28が決定したレベル値が「3」（友人）であった場合に、アクセス制御部24が、「メモリ地点」の下位のデータを読み出そうとすると、レベル値「3」である「データ1」に含まれる項目「名称」「読み仮名」・・・のデータを読み出すことはできるが、レベル値「4」である「データ2」に含まれるデータは読み出すことができない。そのため、アクセス制御部24は、「メモリ地点」の読み出し要求を受けた場合は、「データ1」に含まれるデータのみを読み出すことになる。

【0090】

このように本実施形態では、ユーザの属性によって、アクセスできるユーザ固有情報の範囲を柔軟に変えることができる。なお、本実施形態では、レベル決定部28およびユーザ認証デバイス29は、携帯端末2aに設けられる構成について説明したが、この構成に限られない。例えば、レベル決定部28およびユーザ認証デバイス29は、車載機1に設けられてもよい。この場合、レベル決定部が決定したアクセスレベルは、通信部14、29を介して携帯端末2aへ送信される。

【0091】

また、レベル決定部28は、ユーザ認証デバイス29による認証結果を用いてアクセスレベルを決定する代わりに、ユーザからアクセスレベルの入力を受け付けてもよい。これにより、ユーザが、アクセスレベルを指定したり、変更したりすることが可能になる。例えば、車載機1に接続された携帯端末2aの持ち主は、車に同乗者がいる場合、その同乗者に合わせて公開するユーザ固有情報を制限することができる。その結果、大切な情報を意図せず他人の目にさらす危険が少なくなる。

【0092】

(実施の形態4)

図11は、本実施形態にかかる車載機システムの構成を表す機能ブロック図である。図11において、図1と同じ部分には同じ番号を付し、詳細な説明を省略する。図11に示す携帯端末2bは、図6に示した携帯端末2cに、実行部11bおよびアプリケーションデータ記録部16bを追加した構成になっている。車載機1bは、図6に示した車載機1cから実行部11、アクセス部12、権限判定部13、端末状態監視部17、車載機用データ記録部16を除いた構成になっている。

【0093】

実行部11bは、図1に示した実行部11と同様の機能を持ち、アプリケーションデータ記録部16bは、図1に示した車載機用データ記録部16と同様の機能を持つ。すなわち、図11に示す車載機システムは、図1に示した車載機1の実行部11、アプリケーションデータ記録部16bの機能を、携帯端末2へ移した構成になっている。これにより、実行部11bは、直接アクセス制御部24に対して、ユーザ固有情報の書き込みまたは読み出し要求を出すようになっている。

【0094】

認証部25、端末側認証情報記録部211、車載機状態監視部26の機能も図1と同様

10

20

30

40

50

である。このため、実施の形態 1 と同様に、アクセス権限のある車載機 1 b が携帯端末 2 b と接続されている間のみ、アクセス制御部 2 4 はデータ記録部 2 1 に対するアクセスが可能になる。

【 0 0 9 5 】

実行部 1 1 b によって実行された処理結果は、通信部 2 7 を介して車載機 1 b に送信される。車載機 1 b の通信部 1 4、UI 1 8 を通じて出力される。実行部 1 1 b の処理の例として、例えば、カーナビゲーション機能、ハンズフリー通話機能等を実現するための処理が挙げられる。

【 0 0 9 6 】

本実施形態によれば、車載機 1 b で提供される機能の処理を、携帯端末 2 b において実行するので、車載機 1 b に新たな機能を追加しなくても、携帯端末 2 b を接続するだけで、車載機 1 b で新たな機能を実現することができる。また、例えば、明示的に許可されていない車載機と接続する場合には認証が成立しないので、携帯電話が盗難されて他の車載機に接続された場合のユーザ固有情報の漏洩を防ぐことができる。また、上記実施の形態 1 と同様に、ユーザ固有情報が携帯端末 2 b のみに記録されるため、ユーザ固有情報の漏洩、紛失の危険性が少なくなる効果も奏する。

【 0 0 9 7 】

(実施の形態 5)

図 1 2 は、本実施形態にかかる車載機システムの構成を表す機能ブロック図である。図 1 2 において、図 1 と同じ部分には同じ番号を付し、詳細な説明を省略する。図 9 に示す車載機システムにおいて、携帯端末 2 は、図 1 に示した携帯端末 2 と同じである。車載機 1 d は、図 1 に示した車載機 1 に、一時待避データ更新部 1 1 0 および一時待避データ記録部 1 9 を追加した構成になっている。

【 0 0 9 8 】

本実施形態において、携帯端末 2 のデータ記録部 2 1 に記録されるユーザ固有情報は、アクセス制限されたデータと、アクセス無制限のデータとを含んでいる。例えば、上記実施の形態 3 の図 1 0 で示したように、データ記録部 2 1 に記録されるユーザ固有情報にアクセスレベルを表わすデータが付加して記録される。なお、図 1 0 では、アクセスレベルを表わすデータの例として、レベル値が 2 ~ 5 までが付加されていたデータが示されているが、本実施形態では、レベル値は、少なくとも、アクセス制限があるかないかの 2 段階のアクセスレベルを表わすものであれば足りる。以下、ユーザ固有情報には、アクセス無制限のデータと、アクセス制限されたデータとが含まれる場合について説明する。

【 0 0 9 9 】

図 1 2 において、一時待避データ記録部 1 9 に記録されるデータは、アクセス部 1 2 および一時待避データ更新部 1 1 0 が読み出したまたは書き込み・更新が可能となっている。一時待避データ更新部 1 1 0 は、端末状態監視部 1 7 が通信可能と判断しているときは、アクセス部 1 2 による読み出し要求で読み出されたユーザ固有情報のうちアクセス無制限のデータを前記一時待避データ記録部に記録しておく。この際、一時待避データ更新部 1 1 0 は、実行部 1 1 の処理が開始されたタイミングで、データ記録部 2 1 から一括して読み出されたアクセス無制限のデータを、一時待避データ記録部 1 9 に記録しておいてもよい。これにより、突然、携帯端末 2 との通信が不可能な状態になった場合でも、アクセス部 1 2 が、一時待避データ記録部 1 9 に記録されたアクセス無制限のデータを読み出すことができる。

【 0 1 0 0 】

端末状態監視部 1 7 が通信可能な状態にないことを検出した場合、アクセス部 1 2 はアクセス無制限のデータについては、一時待避データ記録部 1 9 に対して読み出しや書き込みを行い、アクセス制限されたデータについては、実行部 1 1 からの読み出したまたは書き込み・更新指示に対して不可能である旨の通知を返す。この通知を受けた実行部 1 1 は、書き込み・更新指示にかかるアクセス制限されたデータを所定のタイミングで削除する。例えば、実行部 1 1 は、データの使用后、すぐに削除してもよいし、車両のキーオフ時に

10

20

30

40

50

削除してもよい。これにより、実行部 11 は、携帯端末 2 との通信が不可能な場合、アクセス権限のないユーザ固有情報の読み出しは行わない。また、アクセス権限のないユーザ固有情報を生成または更新した場合にも、そのようなアクセス制限されたユーザ固有情報が車載機 1d 側に残らないようになる。

【0101】

端末状態監視部 17 が再び通信可能な状態になったことを検出した場合、アクセス部 12 は、前回通信不可能な状態であることが検出されたとき以降に更新された一時待避データ記録部 19 のデータを携帯端末 2 のデータ記録部 21 に書き込む要求を出す。これにより、通信不可能になっていた期間に生成または更新されたユーザ固有データをデータ記録部 21 へ記録することができる。

10

【0102】

このように、本実施形態では、携帯端末との通信が途絶えた場合であっても、アクセス無制限のユーザ固有情報に関してはアクセスすることができるようになる。

【0103】

以上、実施の形態 1 ~ 5 において述べた車載機システムは、本発明の実施例であり、本発明は、上記実施の形態に限られるものではない。例えば、車載機が持つ機能は、カーナビゲーション機能、ハンズフリー通話機能に限られない。車載機が持ちうるその他の機能として、例えば、音楽再生、TV・ラジオ受信、交通情報案内、メンテナンス情報の通知等が挙げられる。

【0104】

20

以上の実施の形態に関し、更に以下の付記を開示する。

【0105】

(付記 1)

特定のユーザに関する情報であって、車載機における処理に関わる情報であるユーザ固有情報を記録するデータ記録部を有する携帯端末と、当該携帯端末と互いに通信可能な車載機とを含む車載機システムであって、

前記車載機は、

携帯端末と有線または無線による通信を行う通信部と、

車載機での処理を行うためのデータを記録してある車載機用データ記録部と、

前記通信部が通信可能な前記携帯端末を検出する端末状態監視部と、

30

ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース部と、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行部と、

前記端末状態監視部によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス部とを備え、

前記実行部は、

前記端末状態監視部によって携帯端末が検出された場合は、

前記携帯端末の前記データ記録部から前記ユーザ固有情報の読み出しを、前記アクセス部に対して指示し、ユーザの指示に基づく前記処理に際して、読み出した前記ユーザ固有情報を用いて処理し、前記処理においてユーザ固有情報が生成または更新された場合に、当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を前記アクセス部に対して指示し、前記アクセス部が前記ユーザ固有情報を前記携帯端末に書き込み・更新要求をした後、車載機上のユーザ固有情報を削除し、

40

前記端末状態監視部によって携帯端末が検出されない場合は、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行し、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上のユーザ固有情報を削除し、

前記携帯端末は、

車載機と有線または無線による通信を行う通信部と、

50

前記通信部が通信可能な車載機を検出する車載機状態監視部と、

前記車載機状態監視部が検出した車載機からの前記データ記録部に対するユーザ固有情報の読み出し要求、または書き込み・更新要求とユーザ固有情報を、前記通信部を介して受信し、当該読み出し要求または書き込み・更新要求に基づいて、前記データ記録部に対するユーザ固有情報の読み出し、または書き込み・更新処理を行い、当該処理結果を、前記車載機へ前記通信部を介して返信するアクセス制御部とを備える、車載機システム。

【0106】

(付記2)

データ記録部を有する携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部を備える車載機であって

10

、
前記通信部が通信可能な前記携帯端末を検出する端末状態監視部と、
ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース部と、
前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行部と、前記端末状態監視部によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス部とを備え、

前記実行部は、

前記端末状態監視部によって携帯端末が検出された場合は、

20

前記携帯端末の前記データ記録部からの前記ユーザ固有情報の読み出しを、前記アクセス部に対して指示し、ユーザの指示に基づく前記処理に際して、読み出した前記ユーザ固有情報を用いて処理し、前記処理においてユーザ固有情報が生成または更新された場合に、当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を前記アクセス部に対して指示し、前記アクセス部が前記携帯端末へ前記ユーザ固有情報の書き込み・更新要求をした後、車載機上のユーザ固有情報を削除し、

前記端末状態監視部によって携帯端末が検出されない場合は、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行し、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上のユーザ固有情報を削除することを特徴とする車載機。

30

【0107】

(付記3)

特定の携帯端末のデータ記録部へアクセスするための認証情報を予め記録しておく車載機側認証情報記録部をさらに備え、

前記端末状態監視部によって携帯端末が検出された場合に、前記認証情報を、前記通信部を介して前記携帯端末に送信し、当該携帯端末のデータ記録部へのアクセス権限の有無の通知を、前記通信部を介して前記携帯端末から受信する権限判定部をさらに備え、

前記アクセス部は、前記権限判定部が、前記アクセス権限が有る旨の通知を受信した場合にのみ、前記携帯端末の前記データ記録部に対するユーザ固有情報の書き込み・更新要求、または読み出し要求を行う、付記2に記載の車載機。

40

【0108】

(付記4)

ユーザの認証情報の入力を受け付け、当該ユーザの認証情報に基づいて、前記データ記録部内のデータのうち、アクセス可能な範囲を示すアクセスレベルを決定する車載機側レベル決定部をさらに備え、

前記通信部は、前記車載機側レベル決定部が決定したアクセスレベルを、前記携帯端末に送信する、付記2または3に記載の車載機。

【0109】

(付記5)

前記ユーザ固有情報は、アクセス制限されたデータと、アクセス無制限のデータとを含

50

み、

前記端末状態監視部は、前記通信部が前記携帯端末と通信可能な状態にあるか否かを監視する機能をさらに備え、

前記アクセス部が読み出したまたは書き込み・更新が可能なデータを記録する一時待避データ記録部と、

前記端末状態監視部が通信可能と判断しているときは、アクセス部による読み出し要求で読み出されたユーザ固有情報のうちアクセス無制限のデータを前記一時待避データ記録部に記録しておく一時待避データ更新部をさらに備え、

前記端末状態監視部が通信可能な状態にないことを検出した場合、前記アクセス部は、アクセス無制限のデータについては、前記一時待避データ記録部に対して読み出しや書き込みを行い、アクセス制限されたデータについては、前記実行部からの読み出したまたは書き込み・更新指示に対して不可能である旨の通知を返し、前記実行部は、書き込み・更新指示にかかるアクセス制限されたデータを所定のタイミングで削除し、

前記端末状態監視部が再び通信可能な状態になったことを検出した場合、前記アクセス部は、前回通信不可能な状態であることが検出されたとき以降に更新された一時待避データ記録部のデータを前記携帯端末の前記データ記録部に書き込む要求を行う、付記 2 ~ 4 のいずれか 1 項に記載の車載器。

【 0 1 1 0 】

(付記 6)

車載機と有線または無線による通信を行う通信部と、

前記通信部が通信可能な車載機を検出する車載機状態監視部と、

特定のユーザに関する情報であって、車載機における処理に関わる情報であるユーザ固有情報を記録するデータ記録部と、

前記車載機状態監視部が検出した車載機からの前記データ記録部に対するユーザ固有情報の読み出し要求、または書き込み・更新要求とユーザ固有情報を、前記通信部を介して受信し、当該読み出し要求または書き込み要求に基づいて、前記データ記録部に対するユーザ固有情報の読み出し、または書き込み・更新処理を行い、当該処理結果を、前記車載機へ前記通信部を介して返信するアクセス制御部とを備えた携帯端末。

【 0 1 1 1 】

(付記 7)

前記データ記憶部へのアクセスを認証するか否か判断するための認証情報を予め記録している端末側認証情報記録部と、

前記車載機が前記データ記録部へアクセスするための認証情報を、前記車載機から前記通信部を介して受信し、当該認証情報と前記端末側認証情報記録部の認証情報とを照会し、前記車載機が当該携帯端末に対して書き込み処理または読み出し処理をする権限があるか否かを認証判定し、前記通信部を介して前記車載機に認証判定結果を送信する認証部とをさらに備え、

前記アクセス制御部は、処理権限が認証された車載機からの要求に基づいて処理し、処理権限が認証されなかった車載機からの要求には権限がない旨の通知を、前記通信部を介して前記車載機に行うことを特徴とした、付記 6 に記載の携帯端末。

【 0 1 1 2 】

(付記 8)

所定のプログラムに基づいた所定の処理を実行し、当該所定の処理の結果を、前記通信部を介して車載機へ送信する実行部であって、当該所定の処理において、ユーザ固有情報を使用する場合に、前記アクセス制御部に対して当該ユーザ固有情報の読み出しを要求し、前記所定の処理において、ユーザ固有情報が生成または更新された場合は、前記アクセス部に対して当該ユーザ固有情報の書き込みを要求する実行部をさらに備える、付記 6 に記載の携帯端末。

【 0 1 1 3 】

(付記 9)

10

20

30

40

50

ユーザの認証情報の入力を受け付け、当該ユーザの認証情報に基づいて、前記アクセス制御部が、前記データ記録部内のユーザ固有情報のうち書き込みまたは読み出しできるデータの範囲を示すアクセスレベルを決定する端末側レベル決定部をさらに備える、付記6に記載の携帯端末。

【0114】

(付記10)

前記アクセス制御部は、前記端末側アクセスレベル決定部により決定されたアクセスレベルまたは、通信部が車載機から受信したアクセスレベルに基づいて、前記データ記録部内のユーザ固有情報のうち、前記アクセスレベルで示される範囲に対して、書き込み・更新、または読み出しを行う、付記9に記載の携帯端末。

10

【0115】

(付記11)

データ記録部を有する携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部とを備える車載機に処理を実行させるプログラムであって、

前記通信部が通信可能な前記携帯端末を検出する端末状態監視処理と、

ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェース処理と、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行処理と、

前記端末状態監視処理によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセス処理とを車載機に実行させ、

20

前記端末状態監視処理によって携帯端末が検出された場合は、

前記実行処理において、前記アクセス処理で前記携帯端末の前記データ記録部から読み出された前記ユーザ固有情報を用いてユーザの指示に基づく前記処理が実行され、前記処理においてユーザ固有情報が生成または更新された場合に、前記アクセス処理で当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を要求が行われた後、車載機上の前記ユーザ固有情報が削除され、

前記端末状態監視処理によって携帯端末が検出されない場合は、

前記実行処理において、前記車載機用データ記録部に記録されたデータを用いて前記ユーザの指示に基づく処理が実行され、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上の前記ユーザ固有情報が削除されることを特徴とする、プログラム。

30

【0116】

(付記12)

データ記録部を有する携帯端末と有線または無線による通信を行う通信部と、車載機での処理を行うためのデータを記録してある車載機用データ記録部とを備える車載機が実行する情報処理方法であって、

前記通信部が通信可能な前記携帯端末を検出する端末状態監視ステップと、

ユーザからの処理の指示を入力し、処理結果を出力するユーザインタフェースステップと、

前記ユーザの指示に基づく処理を、前記車載機用データ記録部に記録されたデータを用いて実行する実行ステップと、前記端末状態監視処理によって検出された携帯端末の前記データ記録部に対して、特定のユーザに固有の情報であって、車載機での処理に関わる情報であるユーザ固有情報の書き込み・更新要求、または読み出し要求を、前記通信部を介して行うアクセスステップとを含み、

40

前記端末状態監視ステップで携帯端末が検出された場合は、

前記実行ステップにおいて、前記アクセスステップで前記携帯端末の前記データ記録部から読み出された前記ユーザ固有情報を用いてユーザの指示に基づく前記処理が実行され

50

、前記処理においてユーザ固有情報が生成または更新された場合に、前記アクセスステップで当該生成または更新されたユーザ固有情報の前記携帯端末の前記データ記録部への書き込み・更新を要求が行われた後、車載機上の前記ユーザ固有情報が削除され、

前記端末状態監視ステップによって携帯端末が検出されない場合は、

前記実行処理において、前記車載機用データ記録部に記録されたデータを用いて前記ユーザの指示に基づく処理が実行され、前記処理においてユーザ固有情報が生成された場合は、所定のタイミングで、車載機上の前記ユーザ固有情報が削除されることを特徴とする、情報処理方法。

【産業上の利用可能性】

【0117】

以上のように、本発明は、車載機を通じた情報の漏洩と、盗難等による、情報の紛失との危険をさけることができる車載機、携帯端末、車載機システムとして有用である。

【図面の簡単な説明】

【0118】

【図1】実施の形態1にかかる車載機システムの構成を表す機能ブロック図

【図2】データ記録部に記録されるユーザ固有情報の一例を示す図

【図3】データ記録部に記録されるユーザ固有情報の他の一例を示す図

【図4】車載機のアクセス部の動作例を示すフローチャート

【図5】携帯端末のアクセス制御部の動作例を示すフローチャート

【図6】実施の形態2にかかる車載機システムの構成を表す機能ブロック図

【図7】実施の形態2における車載機のアクセス部の動作例を示すフローチャート

【図8】実施の形態2における携帯端末のアクセス制御部の動作例を示すフローチャート

【図9】実施の形態3にかかる車載機システムの構成を表す機能ブロック図

【図10】アクセスレベルのレベル値が付加されたユーザ固有情報の一例を示す図

【図11】実施の形態4にかかる車載機システムの構成を表す機能ブロック図

【図12】実施の形態5にかかる車載機システムの構成を表す機能ブロック図

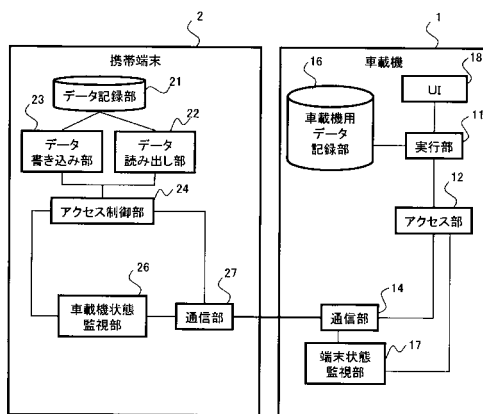
【符号の説明】

【0119】

- | | | |
|-----------|-----------------|----|
| 1、1 b | 車載機 | |
| 2、2 a、2 b | 携帯端末 | 30 |
| 1 1、1 1 b | 実行部 | |
| 1 1 0 | 一時待避データ更新部 | |
| 1 2 | アクセス部 | |
| 1 3 | 権限判定部 | |
| 1 4 | 通信部 | |
| 1 5 | 車載機側認証情報記録部 | |
| 1 6 | 車載機用データ記録部 | |
| 1 6 b | アプリケーションデータ記録部 | |
| 1 7 | 端末状態監視部 | |
| 1 8 | UI (ユーザインタフェース) | 40 |
| 1 9 | 一時待避データ記録部 | |
| 2 1 | データ記録部 | |
| 2 2 | データ読み出し部 | |
| 2 3 | データ書き込み部 | |
| 2 4 | アクセス制御部 | |
| 2 5 | 認証部 | |
| 2 1 1 | 端末側認証情報記録部 | |
| 2 6 | 車載機状態監視部 | |
| 2 7 | 通信部 | |
| 2 8 | レベル決定部 | 50 |

2 9 認証デバイス

【図 1】



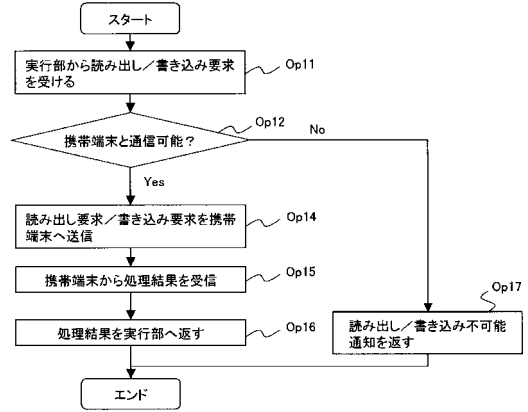
【図 2】

保存項目	保存データ	
自宅位置	位置	緯度
		経度
メモリ地点	データ1	名称
		読み仮名
		緯度
		経度
		電話番号
	:	
	データ2	
:		
目的地履歴	履歴1	名称
		読み仮名
	緯度	
	経度	
	利用日時	
履歴2		
:		
通過経路	通過位置1	緯度
		経度
	通過位置2	
:		

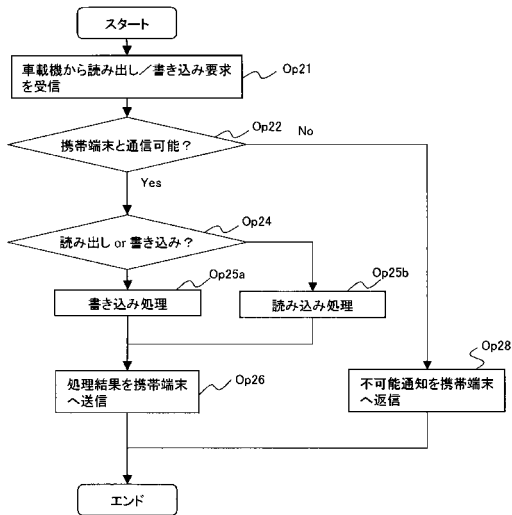
【図3】

保存項目	保存データ	
電話帳	データ1	名前
		読み仮名
	データ2	電話番号
		住所
		:
発信履歴	履歴1	名前
		電話番号
	履歴2	日時
		:
		:
着信履歴	履歴1	名前
		電話番号
	履歴2	日時
		:
		:

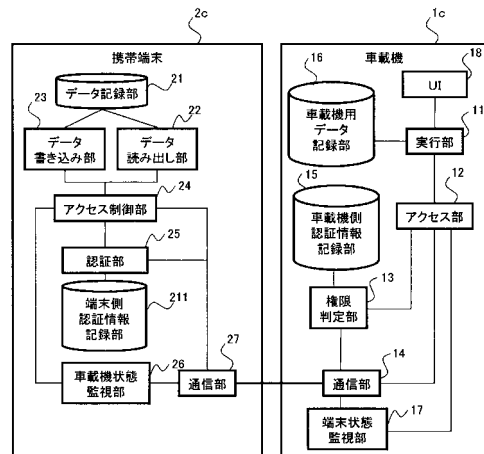
【図4】



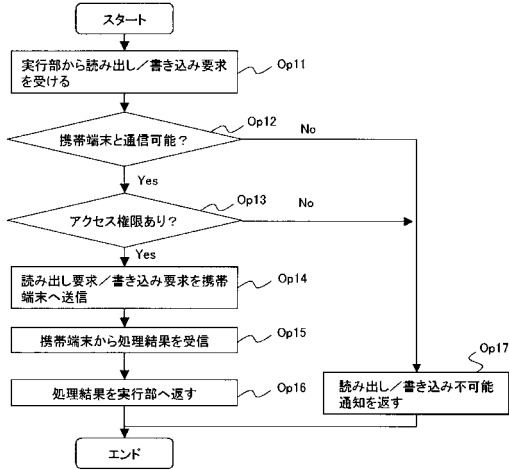
【図5】



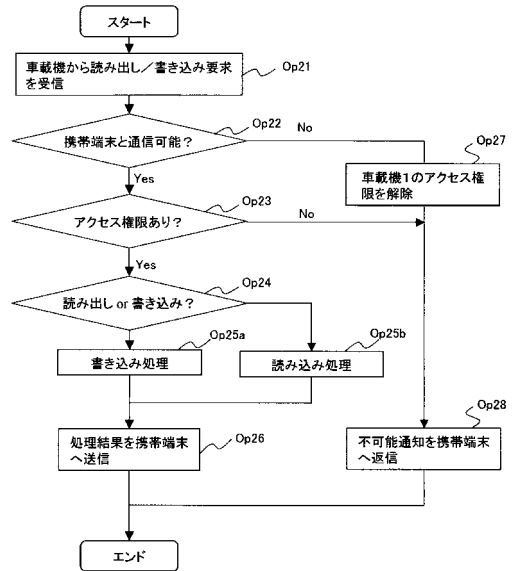
【図6】



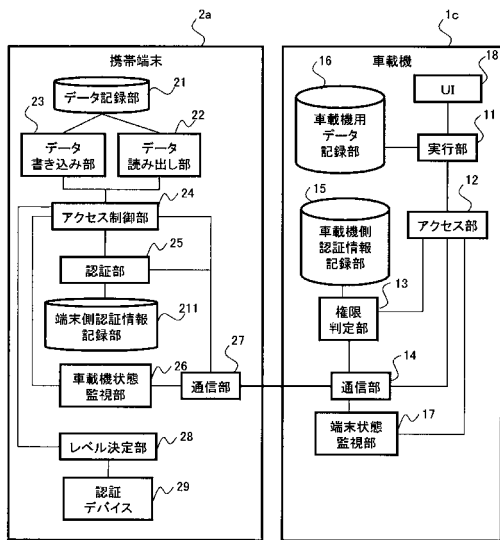
【図7】



【図8】



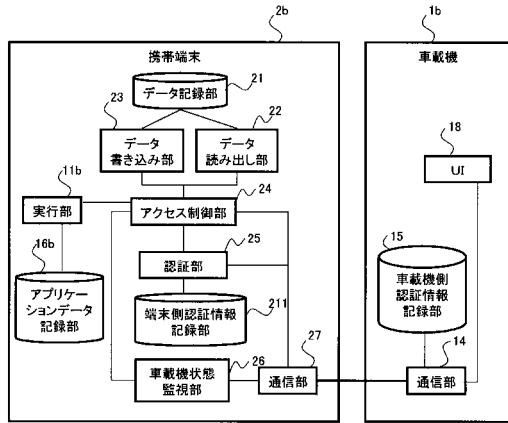
【図9】



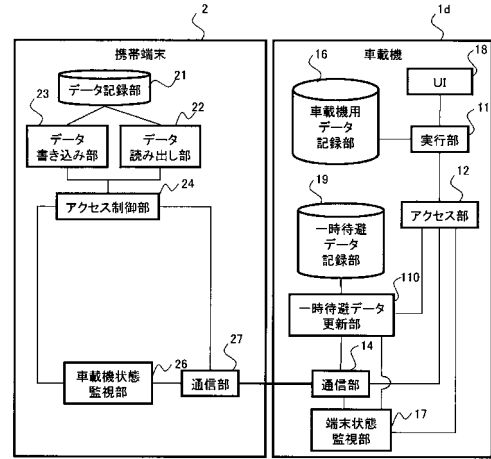
【図10】

保存項目	保存データ		
2 自宅位置	- 位置	- 緯度	
		- 経度	
4 メモリ地点	3 データ1	- 名称	
		- 読み仮名	
		- 緯度	
		- 経度	
		- 電話番号	
		- :	
4 目的地履歴	- 履歴1	- 名称	
		- 読み仮名	
		- 緯度	
		- 経度	
		5 利用日時	
		- 履歴2	
5 通過経路	- 通過位置1	- 緯度	
		- 経度	
	- 通過位置2		
		- :	

【図 1 1】



【図 1 2】



フロントページの続き

- (72)発明者 奥山 鏡子
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
- (72)発明者 宮田 亮介
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
- (72)発明者 池田 拓郎
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

審査官 加藤 信秀

- (56)参考文献 特開2003-216261(JP,A)
特開2001-338358(JP,A)
特開2003-250181(JP,A)

- (58)調査した分野(Int.Cl., DB名)
B60R 16/02
B60R 16/023