(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4438199号
(P4438199)
(45)発行日　平成22年3月24日(2010.3.24)　(24)登録日　平成22年1月15日(2010.1.15)

(51)Int.Cl.　　F I
G06F 1/00 (2006.01)　　G06F 1/00 370E
G06F 1/16 (2006.01)　　G06F 1/00 312K

請求項の数 2　(全 13 頁)

(21)出願番号　特願2000-265549(P2000-265549)
(22)出願日　平成12年9月1日(2000.9.1)
(65)公開番号　特開2002-73197(P2002-73197A)
(43)公開日　平成14年3月12日(2002.3.12)
審査請求日　平成19年8月30日(2007.8.30)

(73)特許権者　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町２２番２２号
(74)代理人　100075557
弁理士　西教　圭一郎
(72)発明者　小柳　浩二
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内

審査官　小林　正明

最終頁に続く

(54)【発明の名称】携帯型電子機器の起動制御方法および携帯型電子機器

(57)【特許請求の範囲】
【請求項１】
識別情報が設定されている所定の電子鍵の挿入および挿入されている電子鍵に設定されている識別情報を出力するドッキングステーションを接続可能な携帯型電子機器の起動制御方法であって、
前記識別情報が設定されている所定の電子鍵が挿入されているか否かを検知する鍵検知ステップと、
前記ドッキングステーションとの接続を検出する接続検出ステップと、
前記鍵検知ステップにおいて、前記識別情報が設定されている所定の電子鍵が挿入されていることを検知したとき、当該挿入されている電子鍵に設定されている識別情報と、予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なうとともに、前記鍵検知ステップにおいて前記識別情報が設定されている所定の電子鍵が挿入されていないことを検知し、かつ前記接続検出ステップにおいてドッキングステーションとの接続を検出したとき、接続されているドッキングステーションから出力される識別情報と、予め登録されている識別情報と照合して、主回路への電力供給を行なうか否かの判断を行なう起動制御ステップとを、含むことを特徴とする携帯型電子機器の起動制御方法。
【請求項２】
識別情報が設定されている所定の電子鍵の挿入および挿入されている電子鍵に設定されている識別情報を出力するドッキングステーションを接続可能な携帯型電子機器であって

、
識別情報が設定されている所定の電子鍵が挿入可能で、当該電子鍵が挿入されているか否かを検知する検知手段と、
前記ドッキングステーションとの接続を検出する接続検出手段とを備え、
前記検知手段によって前記所定の電子鍵が挿入されていることを検知したとき、当該挿入されている電子鍵に設定されている識別情報と、予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なうとともに、前記所定の電子鍵が挿入されていないことを検知し、かつ前記接続検出手段によってドッキングステーションとの接続を検出したとき、接続されているドッキングステーションから出力される識別情報と、予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なう起動制御手段とを、含むことを特徴とする携帯型電子機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は単体でも使用可能な携帯型電子機器をドッキングステーションと接続して使用する場合の携帯型電子機器の起動制御方法および携帯型電子機器に関する。

【０００２】

【従来の技術】

従来から、ノートパソコンやＰＤＡ（Personal Digital Assistant）などと呼ばれる情報処理用の携帯型電子機器は、単体で使用することも可能であると同時に、ドッキングステーションと呼ばれる拡張ユニットと組合せての使用が可能にされている場合がある。たとえば特開２０００－１１２５８０号公報には、ノートパソコン、すなわちノートブック型のパーソナルコンピュータを機能拡張のためのドッキングステーションである拡張ユニットに装着すると、パーソナルコンピュータを自動的にパワーオンさせることができるコンピュータシステムについての先行技術が開示されている。この先行技術のドッキングステーションは、ＬＡＮ（Local Area Network）への接続を可能にするために設けられる。一般にドッキングステーションは、携帯型電子機器が携帯性を重視するために、充分なハードウエアを搭載することができない点を補うために用いられる。したがって、ドッキングステーションは、直接大容量の記憶装置が接続されていたり、ＬＡＮを通じて大容量の記憶装置に接続されていたりすることが多い。そのような記憶装置には、重要な情報が記憶され、正当な権限を有しない者が情報を読出したり情報を改変したりすることを防がなければならない。

【０００３】

一般に重要な業務などに用いるコンピュータ装置では、情報へのアクセスを正当な権限を有する者に限るために、セキュリティの確保が図られている。たとえばコンピュータ装置の使用を開始するにあたって行うログオン手続きで、操作者の資格を識別情報であるＩＤを入力させて確認したり、パスワードを入力させて確認するようにしている。さらに一層確実なセキュリティの確保のために、電子鍵を利用することも行われている。携帯型電子機器に対して電子鍵を用いるセキュリティシステムについては、本件出願人からも特願平１０－１８５１４１号として出願し、特開２０００－１７９１８号として出願公開されている。この特許出願では、固有の鍵データを送信する鍵データ送信部を内蔵する電子鍵と、その電子鍵を挿入するための鍵穴および鍵データ受信部を持つ携帯型電子機器から成るセキュリティシステムについての技術が開示されている。ただし、携帯型電子機器をドッキングステーションと組合せ、ドッキングステーションを含めたシステム全体としてのセキュリティ管理については何も示されていない。

【０００４】

図６は、前述の特許出願で示されている電子鍵を用いる携帯型電子機器で、ドッキングステーションへの接続を可能にする場合の電気的構成を示す。携帯型電子機器１は、セキュリティ管理のため電子鍵２を使用し、またドッキングステーション３と接続することもできる。電子鍵２を使用するセキュリティの管理は、マイクロコンピュータ６、フラッシュ

ＲＯＭ７、無線通信制御部８および送受信アンテナ９を含むセキュリティ機能関連回路１１によって行われる。電子鍵２が携帯型電子機器１の筐体に挿入されているか否かは、鍵入力スイッチ１２によって検出される。携帯型電子機器１の動作用の電源１３は、電子スイッチ１４を介して携帯型電子機器１としての主要な動作を行う主回路１５動作用の電力を供給する。ただし電子スイッチ１４は、セキュリティ機能関連回路１１のマイクロコンピュータ６によって、電子鍵２に基づくセキュリティが確保されているときのみ主回路１５に電力を供給することが可能となる。

【０００５】

ドッキングステーション３は、携帯型電子機器１側に設けられるインタフェース（以下、「Ｉ／Ｆ」と略称する）を受持つドッキングステーションＩ／Ｆ部１６と接続して用いる。前述の特許出願では、電子鍵２を用いて携帯型電子機器１の単体システムとしてセキュリティを管理しているけれども、ドッキングステーション３を含めたシステム全体としてのセキュリティ管理については示されていない。このため、携帯型電子機器１をドッキングステーション３と接続する場合に、組合せシステムとして有効に動作させるためには、ドッキングステーション３と携帯型電子機器１とを接続すれば、無条件で電子スイッチ１４を作動させ、電源１３から主回路１５に動作用の電力を供給しなければならない。

【０００６】

図７は、図６に示すシステムでセキュリティ管理の処理手順を示す。ステップｓ０から手順を開始し、ステップｓ１では電子鍵２が携帯型電子機器１の筐体の鍵穴に挿入され、鍵入力スイッチ１２が押されているか否かを判断する。鍵入力スイッチ１２が押されていると判断されるときには、鍵入力スイッチ１２を介して電源１３からセキュリティ機能関連回路１１に動作用の電力が供給される。このような動作は、鍵入力スイッチ１２が単なる機械的なスイッチであっても、可能であり電子鍵２を挿入したとき導通して、電源１３からの電力をセキュリティ機能関連回路１１に供給するようにすればよい。

【０００７】

ステップｓ３では、携帯型電子機器１のセキュリティ機能関連回路１１内に設けられる無線通信制御部８が電子鍵２から識別情報としてＩＤを受信する。次にステップｓ４で、セキュリティ機能関連回路１１内のマイクロコンピュータ６が無線通信制御部８で受信したＩＤと、フラッシュＲＯＭ７に予め登録されている登録ＩＤとを比較した結果として、受信ＩＤと登録ＩＤとが一致しているか否かを判断する。受信ＩＤと登録ＩＤとが一致していると判断されるときには、ステップｓ５でマイクロコンピュータ６は電子スイッチ１４を制御して、携帯型電子機器１の主回路１５に電源１３からの動作用電力を供給する。

【０００８】

なお、ステップｓ１で、電子鍵２によって鍵入力スイッチ１２が押されていないと判断されるときには、ステップｓ６でドッキングステーション３と接続されているか否かを判断する。ドッキングステーション３と接続されていないと判断されるときには、ステップｓ１に戻り、電子鍵が挿入されるかドッキングステーション３と接続されるかが行われるまでは、携帯型電子機器１を完全には動作させない。ステップｓ６で、ドッキングステーション３と接続されたと判断されるときには、ステップｓ５に移る。なおステップｓ４で、受信ＩＤと登録ＩＤとが一致しないと判断されるとき、またステップｓ６で主回路１５に電源供給が行われた後は、ステップｓ７で手順を終了する。

【０００９】

図７に示すように、電子鍵２が挿入された場合は、携帯型電子機器１のフラッシュＲＯＭ７に登録されているＩＤと、電子鍵２から受信するＩＤとを比較した結果、一致したときのみ携帯型電子機器１の主回路１５に電源１３からの動作用電力を供給するようになっている。しかしながら、ドッキングステーション３と接続する場合は、いつでも必ず携帯型電子機器１の主回路１５に動作用の電力を電源１３から供給するようになっている。

【００１０】

【発明が解決しようとする課題】

前述の特許出願で開示しているセキュリティシステムでは、電子機器単体システムとして

はセキュリティ管理を行うことができても、ドッキングステーション３を含めたシステム全体としてのセキュリティ管理は不充分である。パワーオンで動作中のドッキングステーション３と接続すると、携帯型電子機器１が自動的にセキュリティ管理を行うことができても、ドッキングステーション３を含めたシステム全体としてのセキュリティ管理を行うことはできない。

【００１１】

また、ドッキングステーション３を起動させるために電子鍵２が必要であるとすれば、携帯型電子機器１をドッキングステーション３と接続して使用する場合に、携帯型電子機器１に対する電子鍵２とドッキングステーション３に対する電子鍵２との両方の情報を用いる必要がある。このように、利用者が同一のＩＤを有する複数の電子鍵２を用いることは、利用者の負担を増大させてしまう。その一方で、携帯型電子機器１をドッキングステーション３と組合せた場合でも、全体のシステムしてのセキュリティ管理を有効に行う必要がある。

【００１２】

さらに、複数の利用者が携帯型電子機器をそれぞれ所有し、共通のドッキングステーション３を利用するような構成も考えられる。このように複数人がドッキングステーション３を利用する場合には、同じグループの利用者は携帯型電子機器１とドッキングステーション３とを組合せて利用可能であり、同じグループに属さない利用者は利用可能できなくするようなセキュリティの確保が望まれる。

【００１３】

本発明の目的は、携帯型電子機器の単体だけではなく、ドッキングステーションも含めた全体的なセキュリティを確保することができる携帯型電子機器の起動制御方法および携帯型電子機器を提供することである。

【００１４】

【課題を解決するための手段】

本発明は、識別情報が設定されている所定の電子鍵の挿入および挿入されている電子鍵に設定されている識別情報を出力するドッキングステーションを接続可能な携帯型電子機器の起動制御方法であって、

前記識別情報が設定されている所定の電子鍵が挿入されているか否かを検知する鍵検知ステップと、

前記ドッキングステーションとの接続を検出する接続検出ステップと、

前記鍵検知ステップにおいて、前記識別情報が設定されている所定の電子鍵が挿入されていることを検知したとき、当該挿入されている電子鍵に設定されている識別情報と、予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なうとともに、前記鍵検知ステップにおいて前記識別情報が設定されている所定の電子鍵が挿入されていないことを検知し、かつ前記接続検出ステップにおいてドッキングステーションとの接続を検出したとき、接続されているドッキングステーションから出力される識別情報と、予め登録されている識別情報と照合して、主回路への電力供給を行なうか否かの判断を行なう起動制御ステップとを、含むことを特徴とする携帯型電子機器の起動制御方法である。

【００１５】

本発明に従えば、単体またはドッキングステーションに接続して動作する携帯型電子機器のセキュリティ確保のため、電子鍵を使用する。携帯型電子機器は、識別情報が設定される電子鍵が挿入可能であって、電子鍵の挿入を検知したとき、挿入された電子鍵に設定されている識別情報、を予め登録されている識別情報とを照合して、主回路への電力供給を行うか否かを判断する。また、携帯型電子機器に前記識別情報が設定されている所定の電子鍵が挿入されていないことを検知したときには、携帯型電子機器にドッキングステーションが接続されたか否かを検出し、ドッキングステーションから出力される識別情報と、携帯型電子機器に予め登録されている識別情報とを照合し、この照合結果によって、携帯型電子機器へ電源電力を供給するか否かの判断が行われる。このように、携帯型電子機

器にドッキングステーションが接続されていない場合であっても、携帯型電子機器を起動して、セキュリティを確保することができる。

【００１６】

また本発明は、識別情報が設定されている所定の電子鍵の挿入および挿入されている電子鍵に設定されている識別情報を出力するドッキングステーションを接続可能な携帯型電子機器であって、

識別情報が設定されている所定の電子鍵が挿入可能で、当該電子鍵が挿入されているか否かを検知する検知手段と、

前記ドッキングステーションとの接続を検出する接続検出手段とを備え、

前記検知手段によって前記識別情報が設定されている所定の電子鍵が挿入されていることを検知したとき、当該挿入されている電子鍵に設定されている識別情報と、予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なうとともに、前記所定の電子鍵が挿入されていないことを検知し、かつ前記接続検出手段によってドッキングステーションとの接続を検出したとき、接続されているドッキングステーションから出力される識別情報と、予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なう起動制御手段とを、含むことを特徴とする。

【００１７】

本発明に従えば、携帯型電子機器は、電子鍵が挿入されているときは、その電子鍵の識別情報によって、また電子鍵が挿入されていないときは、ドッキングステーションに挿入されている電子鍵の識別情報によって、起動することができる。したがって、携帯型電子機器は、単に動作中のドッキングステーションに接続されるだけでは起動しない。そのため、携帯型電子機器は、電子鍵が挿入されているか否かを検知する検知手段と、ドッキングステーションとの接続の有無を検出する接続検出手段と、主回路への電力供給を行なうか否かの判断を行なう起動制御手段とを備える。

前記検知手段によって電子鍵が挿入されていることを検知されると、挿入された電子鍵に設定されている識別情報と、起動制御手段は、予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なう。また起動制御手段は、電子鍵が挿入されていないことを検知した状態で、接続検出手段によってドッキングステーションが接続されたことを検出すると、接続されているドッキングステーションから出力される識別情報と、携帯型電子機器に予め登録されている識別情報とを照合して、主回路への電力供給を行なうか否かの判断を行なう。

【００２８】

【発明の実施の形態】

図１は、本発明の実施の一形態として情報機器のセキュリティ確保方法を実現する電子機器の概略的な電気的構成を示す。本実施形態の情報機器は、携帯型電子機器２１、電子鍵２２およびドッキングステーション２３を含む。電子鍵２２は、基本的に図６に示す電子鍵２と同等である。ドッキングステーション２３については後述する。

【００２９】

本実施形態の携帯型電子機器２１は、マイクロコンピュータ２６、フラッシュＲＯＭ２７、無線通信制御部２８および送受信アンテナ２９を含むセキュリティ機能関連回路３１と、鍵入力スイッチ３２、電源３３、電子スイッチ３４、主回路３５およびドッキングステーションＩ／Ｆ部３６を含む。これらの携帯型電子機器２１としての構成は、図６に示す携帯型電子機器１で、マイクロコンピュータ６、フラッシュＲＯＭ７、無線通信制御部８および送受信アンテナ９を含むセキュリティ機能関連回路１１と、鍵入力スイッチ１２、電源１３、電子スイッチ１４、主回路１５およびドッキングステーションＩ／Ｆ部１６とそれぞれ対応する。ただしマイクロコンピュータ２６およびフラッシュＲＯＭ２７は、無線通信制御部３８および送受信アンテナ３９とともに、接続時セキュリティ機能関連回路４０にも含まれる。

【００３０】

電子スイッチ３４は、主回路３５に対する電源３３からの電力供給を制御するために設け

られ、主回路３５へのメイン電源がＯＦＦの状態で、鍵入力手段としての鍵入力スイッチ３２に電子鍵２２が挿入されれば、電源３３からセキュリティ機能関連回路３１に動作用の電力を供給することができる。セキュリティ機能関連回路３１に動作用の電力が供給されると、電子鍵２２から固有の識別情報であるＩＤを識別情報入力手段としての無線通信制御部２８が送受信アンテナ２９を介して受信し、マイクロコンピュータ２６に受信ＩＤを入力する。起動制御手段としてのマイクロコンピュータ２６は、フラッシュＲＯＭ２７に予め登録されている電子鍵用ＩＤを参照し、参照した結果が一致すれば、電子スイッチ３４を制御して主回路３５に電源３３からのメイン電源を供給する。

【００３１】

また、接続検出手段としてのドッキングステーションＩ／Ｆ部３６にも、主回路３５にメイン電源をＯＦＦとしている状態で電源３３から動作用の電力を供給する。ドッキングステーションＩ／Ｆ部３６を動作中のドッキングステーション２３に接続すると、接続時セキュリティ機能関連回路４０に動作用電力が供給され、ドッキングステーション２３から伝送されるＩＤを無線通信制御部３８が送受信アンテナ３９を介して受信し、マイクロコンピュータ２６に入力してフラッシュＲＯＭ２７に予め登録されているＩＤと照合する。照合結果が一致すれば、マイクロコンピュータ２６が電子スイッチ３４を導通させ、電源３３からのメイン電源を主回路３５に供給して携帯型電子機器２１としての使用部分を動作させる。なお、電子鍵２２が挿入されることを鍵入力スイッチ３２によって検出すると、マイクロコンピュータ２６がその動作を認識し、電源３３からセキュリティ機能関連回路３１に電力が供給されるように制御するような構成も可能である。また、ドッキングステーションＩ／Ｆ部３６にドッキングステーション２３が接続されることを認識して、電源３３から接続時セキュリティ機能関連回路４０に電力が供給されるように制御することも可能である。

【００３２】

接続時セキュリティ機能関連回路４０の無線通信制御部３８は、電力が供給されると、ドッキングステーション２３に対してＩＤの送信指令を送り、ドッキングステーション２３からＩＤを受信する制御を行う。フラッシュＲＯＭ２７には、携帯型電子機器２１に登録されているＩＤが格納されている。マイクロコンピュータ２６は、ドッキングステーション２３から受信するＩＤと、携帯型電子機器２１に対して登録されているドッキングステーション用のＩＤとを比較した結果、一致する場合に電源３３から主回路３５に電力を供給するように電子スイッチ３４を制御する。

【００３３】

図２は、図１の電子鍵２２の概略的な電気的構成を示す。電子鍵２２は、ＩＣチップ４１を備える。ＩＣチップ４１は、無線通信制御部４２、メモリ４３、電源用コンデンサ４４および送受信アンテナ４５を含む。

【００３４】

送受信アンテナ４５は、無線通信のためのアンテナである。無線通信制御部４２は、携帯型電子機器２１からのＩＤの送信指令の受信、メモリ４３からのＩＤの読出し、およびそのＩＤの送信など、携帯型電子機器２１との送受信のための制御を行う。メモリ４３には、電子鍵２２としての固有のＩＤを格納している。電源用コンデンサ４４は、送受信アンテナ４５に受信する電波からの電力で充電され、無線通信制御部４２に電力を供給する。

【００３５】

図３は、本実施形態のドッキングステーション２３の概略的な電気的構成を示す。ドッキングステーション２３は、セキュリティ機能関連回路５１、鍵入力スイッチ５２、電源５３、電子スイッチ５４、主回路５５、マイクロコンピュータ５６、フラッシュＲＯＭ５７、無線通信制御部５８および送受信アンテナ５９を含む。マイクロコンピュータ５６、フラッシュＲＯＭ５７、無線通信制御部５８および送受信アンテナ５９は、セキュリティ機能関連回路５１内に含まれる。これらドッキングステーション２３で、セキュリティ機能関連回路５１、鍵入力スイッチ５２、電源５３、電子スイッチ５４、主回路５５、マイクロコンピュータ５６、フラッシュＲＯＭ５７、無線通信制御部５８および送受しアンテナ

５９は、図１に示す携帯型電子機器２１でのセキュリティ機能関連回路３１、鍵入力スイッチ３２、電源３３、電子スイッチ３４、主回路３５、マイクロコンピュータ２６、フラッシュＲＯＭ２７、無線通信制御部２８および送受信アンテナ２９にそれぞれ対応する。ドッキングステーション２３には、さらに無線通信制御部６８および送受信アンテナ６９も含まれる。

【００３６】

マイクロコンピュータ５６は、電子鍵２２によって鍵入力スイッチ５２が押されたことを認識すると、電源５３からセキュリティ機能関連回路５１に電力が供給されるように制御する。すなわち鍵入力スイッチ５２は、セキュリティ機能関連回路５１の電源スイッチとして機能する。鍵入力スイッチ５２が機械的なスイッチで、直接電源５３からセキュリティ機能関連回路５１に電力を供給することもできる。

【００３７】

無線通信制御部５８は、セキュリティ機能関連回路５１に電力が供給されると、電子鍵２２に対してＩＤの送信指令を送り、電子鍵２２からＩＤを受信する制御を行う。マイクロコンピュータ５６は、電子鍵２２からＩＤを正常に受信したら電源５３から主回路５５に電力を供給するように電子スイッチ５４を制御する。マイクロコンピュータ５６は、さらに受信したＩＤから特定のＩＤに変換し、識別情報記憶手段としてのフラッシュＲＯＭ５７に書込みを行う。ＩＤの変換方法の例を、次の表１に示す。

【００３８】

【表１】

ユーザ名	電子鍵のＩＤ (ユーザＩＤ)	グループ名	ドッキングステーションに登録するＩＤ (グループＩＤ)
１	２０００５００１	Ａ	２０００１００１
２	２０００５００２		
３	２０００５００３	Ｂ	２０００１００２
４	２０００５００４		
５	２０００５００５	Ｃ	２０００１００３
６	２０００５００６		

【００３９】

この例では、同じグループの人のＩＤを全て或る特定のＩＤに変換する。たとえばユーザ名が１～６の６名に対し、グループ名Ａ，Ｂ，Ｃの３組に分ける場合を想定する。各ユーザに対応する電子鍵２２のＩＤ２０００５００１～２０００５００６を、２０００１００１～２０００１００３のドッキングステーションに登録するＩＤとしてのグループＩＤに変換する。この結果、ドッキングステーション２３に接続する携帯型電子機器２１は、パワーオン可能な場合と可能でない場合が生じる。次の表２は、表１に示すようなグループ分けで、パワーオンが可能な場合を○印で示し、可能でない場合を×印で示す。

【００４０】

【表２】

			ドッキングステーション起動したユーザ					
			1	2	3	4	5	6
		グループ	A		B		C	
携帯型電子機器のユーザ	1	A	○	○	×	×	×	×
	2		○	○	×	×	×	×
	3	B	×	×	○	○	×	×
	4		×	×	○	○	×	×
	5	C	×	×	×	×	○	○
	6		×	×	×	×	○	○

【００４１】
表２に示すように、ドッキングステーション２３を起動したユーザと同じグループのユーザが携帯型電子機器２１のユーザである場合にのみ動作中のドッキングステーション２３に携帯型電子機器２１を接続するだけで、携帯型電子機器２１をパワーオンして起動させることが可能となる。これによって、グループ間でセキュリティ管理を図ることが可能となる。グループ内のメンバがドッキングステーション２３を起動していれば、携帯型電子機器２１には電子鍵２２を挿入しなくても起動が可能となるので、利便性を向上させることができる。
【００４２】
ドッキングステーション２３から、グループＩＤあるいはユーザＩＤを携帯型電子機器２１に伝送するために、識別情報伝送手段としての無線通信制御部６８および送受信アンテナ６９が設けられる。無線通信制御部６８は、携帯型電子機器２１からの送信指令を受信し、フラッシュＲＯＭ５７からＩＤを読出し、およびそのＩＤの送信など、携帯型電子機器２１との送受信のための制御を行う。
【００４３】
図４は、本実施形態で携帯型電子機器２１がセキュリティ確保のための制御を行う手順を示す。ステップａ０から手順を開始し、ステップａ１では電子鍵２２によって鍵入力スイッチ３２が押されているか否かを判断する。鍵入力スイッチ３２が押されていると判断されるときには、ステップａ２で携帯型電子機器のセキュリティ機能関連回路３１に電源を供給する。次にステップａ３では、携帯型電子機器の無線通信制御部２８が電子鍵２２からＩＤを受信する。ステップａ４では、受信したＩＤとフラッシュＲＯＭ２７に登録されているＩＤとを比較した結果、一致するか否かを判断する。一致していると判断されるときには、ステップａ５で携帯型電子機器２１の主回路３５に電源供給を行う。
【００４４】
ステップａ１で、電子鍵２２によって鍵入力スイッチ２２が押されていないと判断されるときには、ステップａ６でドッキングステーション２３と接続されているか否かを判断する。ドッキングステーション２３とも接続されていないと判断されるときには、ステップａ１に戻る。ステップａ６でドッキングステーション２３と接続されたと判断されるときには、ステップａ７で携帯型電子機器２１の接続時セキュリティ機能関連回路４０に電源供給を行う。ステップａ８では、携帯型電子機器２１の無線通信制御部３８がドッキングステーション２３からＩＤを受信する。ステップａ９では、受信したＩＤとフラッシュＲＯＭ２７にドッキングステーション用に登録されているＩＤとを比較した結果、一致しているか否かを判断する。一致していると判断されるときには、ステップａ５で携帯型電子機器２１の主回路３５に電源供給を行う。ステップａ５で主回路３５に電源供給を行った後、またはステップａ４やステップａ９で受信ＩＤと登録ＩＤとが一致しないと判断され

るときには、ステップａ１０で手順を終了する。

【００４５】

図５は、図１のドッキングステーション２３でのセキュリティ確保のための処理手順を示す。ステップｂ０から手順を開始し、ステップｂ１では電子鍵２２によって鍵入力スイッチ５２が押されるのを待つ。鍵入力スイッチ５２が押されると、ステップｂ２でドッキングステーション２３のセキュリティ機能関連回路５１に電源供給を行う。ステップｂ３では、ドッキングステーション２３の無線通信制御部５８が電子鍵２２からＩＤを受信する。ステップｂ４では、電子鍵２２からＩＤを正常に受信しているか否かを判断する。ＩＤを正常に受信すると、ステップｂ５で、ドッキングステーション２３の主回路５５に電源供給を行う。ステップｂ６では、受信ＩＤから特定のＩＤへの変換を行う。ステップｂ７では、変換後のＩＤをドッキングステーション２７のフラッシュＲＯＭ５７に書込む。

【００４６】

ステップｂ８では、ドッキングステーション２３に携帯型電子機器２１が接続されて、ＩＤ送信要求が受信されるか否かを判断する。ＩＤ送信要求が受信されると、ステップｂ９でフラッシュＲＯＭに書込まれたＩＤを携帯型電子機器２１に送信する。ステップｂ８でＩＤ送信要求が受信されないとき、またはステップｂ９の後、ステップｂ１０に移る。ステップｂ１０では、電源スイッチなどがＯＦＦに操作されて、ドッキングステーション２３の使用が終了されているか否かを判断する。使用の終了でないと判断されるときには、ステップｂ１１で電子鍵２２が新たに挿入されているか否かを判断する。電子鍵２２が挿入されなければ、ステップｂ８に戻る。ステップｂ１１で新たに電子鍵２２が挿入されていると判断されれば、ステップｂ３に戻る。ステップｂ１０で使用終了と判断されるとき、またはステップｂ４で電子鍵２２からＩＤを正常に受信していないと判断されるときには、ステップｂ１２で手順を終了する。

【００４７】

以上説明した図５に示す処理手順では、ドッキングステーション２３を起動した電子鍵２２のＩＤをフラッシュＲＯＭ５７に書込む。ドッキングステーション２３は、起動時のみ電子鍵２２を必要とし、起動が終了すれば電子鍵２２は除去可能である。ただし動作中に他の電子鍵２２を挿入すると、最後に挿入した電子鍵２２に設定されているＩＤを正常に受信することができれば、そのＩＤをフラッシュＲＯＭ５７に書込むようにすることができる。このようにすると、最後に使用した電子鍵２２に従って、ドッキングステーション２３と接続するだけで起動することができる携帯型電子機器２１を変えることができる。

【００４８】

また、本実施形態で用いるＩＤは、固定した一定のデータを用いることができるばかりではなく、日時などの変化する情報に基づいて一定の関数で変化するデータを用いるようにすることもできる。

【００４９】

【発明の効果】

以上のように本発明によれば、ドッキングステーションを起動するためにも電子鍵が必要となるため、ドッキングステーションはセキュリティが確保された状態で動作中となり、携帯型電子機器は単体で動作するときに電子鍵でセキュリティの確保を図り、ドッキングステーションと接続するときには動作中のドッキングステーションに接続するだけでセキュリティを確保しながら携帯型電子機器を起動することができる。電子鍵を持たない利用者は、動作中のドッキングステーションと接続するときのみ携帯型電子機器を起動させることができ、ドッキングステーション側でセキュリティを確保した状態で携帯型電子機器の利用を図ることができる。電子鍵を有する利用者は、携帯型電子機器を単体で起動して利用することができる。

【００５０】

また本発明によれば、携帯型電子機器に電子鍵が挿入されたときには、挿入された電子鍵の識別情報の照合によって起動制御し、携帯型電子機器に電子鍵が挿入されていないときには、ドッキングステーションに挿入された電子鍵の携帯型電子機器の単体だけではな

く、ドッキングステーションも含めた全体的なセキュリティを確保することができる。

【図面の簡単な説明】

【図１】本発明の実施の一形態としての情報機器のセキュリティ確保方法を実行するために必要な概略的な電気的構成を示すブロック図である。

【図２】図１の電子鍵２２の概略的な電気的構成を示すブロック図である。

【図３】図１のドッキングステーション２３の概略的な電気的構成を示すブロック図である。

【図４】図１の携帯型電子機器２１でのセキュリティ確保のための処理手順を示すフローチャートである。

【図５】図１のドッキングステーション２３でのセキュリティ確保のための処理手順を示すフローチャートである。

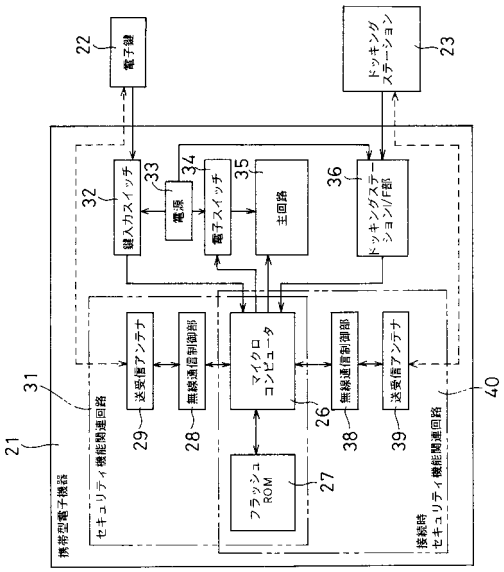
【図６】従来技術でセキュリティ確保を図っている携帯型電子機器をドッキングステーションに接続している時の概略的な電気的構成を示すブロック図である。

【図７】図６の携帯型電子機器でのセキュリティ確保のための処理手順を示すフローチャートである。

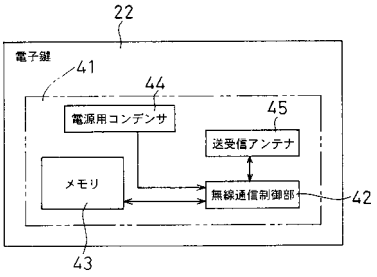
【符号の説明】

２１　携帯型電子機器
２２　電子鍵
２３　ドッキングステーション
２６，５６　マイクロコンピュータ
２７，５７　フラッシュＲＯＭ
２８，３８，５８，６８　無線通信制御部
２９，３９，４５，５９，６９　送受信アンテナ
３１，５１　セキュリティ機能関連回路
３２，５２　鍵入力スイッチ
３３，５３　電源
３４，５４　電子スイッチ
３５，５５　主回路
３６　ドッキングステーションＩ／Ｆ部
４０　接続時セキュリティ機能関連回路
４１　ＩＣチップ
４３　メモリ
４４　電源用コンデンサ

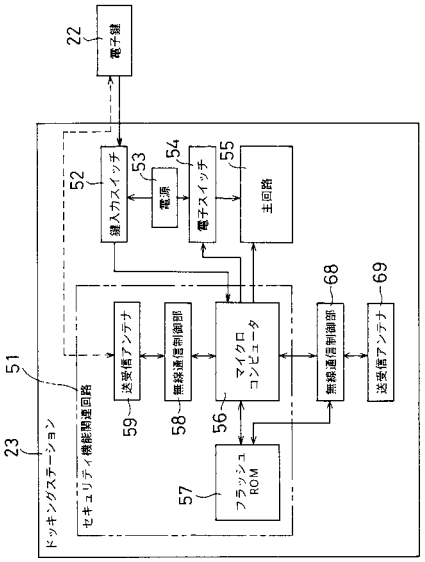
【図１】


携帯型電子機器
21
セキュリティ機能関連回路
31
電子鍵
22
ドッキングステーション
23
接続時
セキュリティ機能関連回路
40
鍵入力スイッチ
32
電源
33
電子スイッチ
34
主回路
35
ドッキングステーション/I/F部
36
送受信アンテナ
29
無線通信制御部
28
マイクロコンピュータ
26
フラッシュROM
27
無線通信制御部
38
送受信アンテナ
39

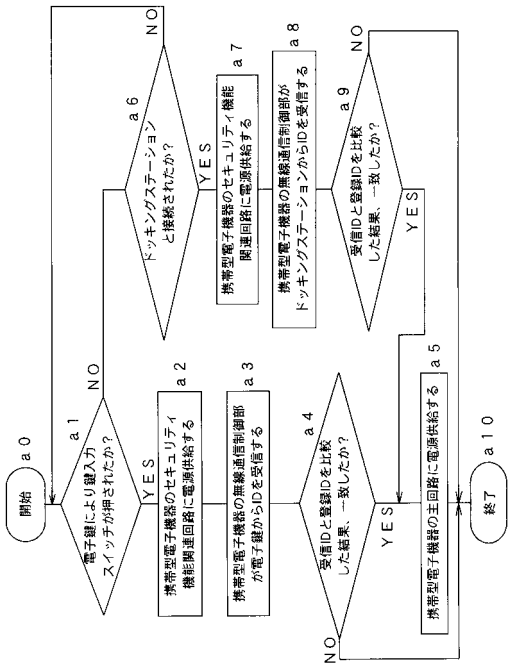
【図２】


電子鍵
22
41
44
電源用コンデンサ
45
送受信アンテナ
メモリ
無線通信制御部
42
43

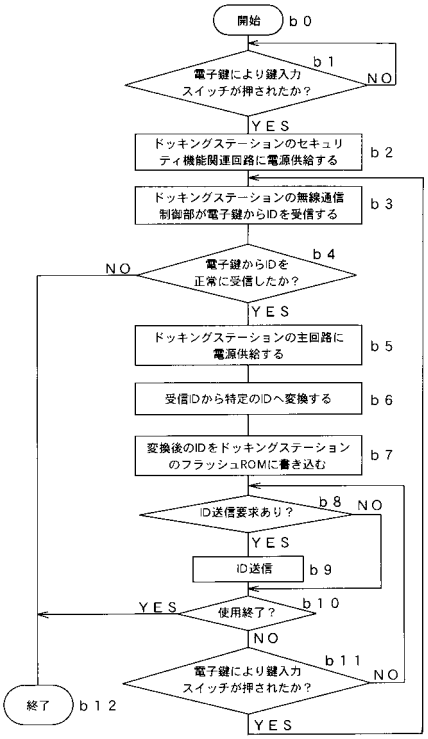
【図３】


ドッキングステーション
23
セキュリティ機能関連回路
51
電子鍵
22
鍵入力スイッチ
52
電源
53
電子スイッチ
54
主回路
55
送受信アンテナ
59
無線通信制御部
58
マイクロコンピュータ
56
フラッシュROM
57
無線通信制御部
68
送受信アンテナ
69

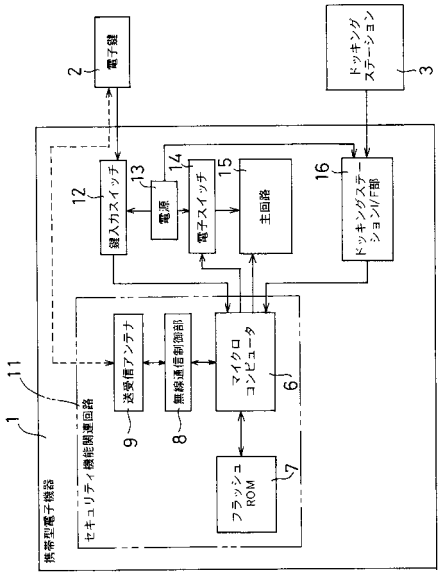
【図４】


開始
a0
電子鍵により鍵入力スイッチが押されたか？
a1
NO
YES
携帯型電子機器のセキュリティ機能関連回路に電源供給する
a2
携帯型電子機器の無線通信制御部が電子鍵からIDを受信する
a3
受信IDと登録IDを比較した結果、一致したか？
a4
NO
YES
携帯型電子機器の主回路に電源供給する
a5
ドッキングステーションと接続されたか？
a6
NO
YES
携帯型電子機器のセキュリティ機能関連回路に電源供給する
a7
携帯型電子機器の無線通信制御部がドッキングステーションからIDを受信する
a8
受信IDと登録IDを比較した結果、一致したか？
a9
NO
YES
終了
a10

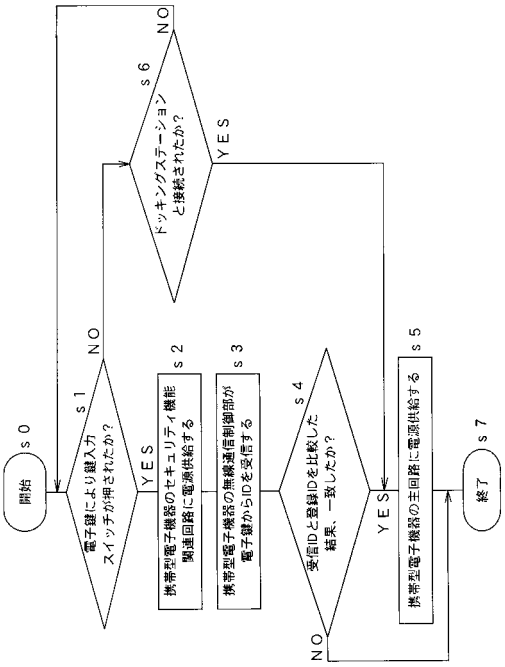
【図５】


開始
b０
電子鍵により鍵入力スイッチが押されたか？
b１
NO
YES
ドッキングステーションのセキュリティ機能関連回路に電源供給する
b２
ドッキングステーションの無線通信制御部が電子鍵からIDを受信する
b３
電子鍵からIDを正常に受信したか？
b４
NO
YES
ドッキングステーションの主回路に電源供給する
b５
受信IDから特定のIDへ変換する
b６
変換後のIDをドッキングステーションのフラッシュROMに書き込む
b７
ID送信要求あり？
b８
NO
YES
ID送信
b９
使用終了？
b１０
YES
NO
電子鍵により鍵入力スイッチが押されたか？
b１１
NO
YES
終了
b１２

【図６】


携帯型電子機器
1
電子鍵
2
ドッキングステーション
3
鍵入力スイッチ
12
電源
13
電子スイッチ
14
主回路
15
ドッキングステーションI/F部
16
セキュリティ機能関連回路
11
送受信アンテナ
9
無線通信制御部
8
マイクロコンピュータ
6
フラッシュROM
7

【図７】


開始
s０
電子鍵により鍵入力スイッチが押されたか？
s１
NO
YES
携帯型電子機器のセキュリティ機能関連回路に電源供給する
s２
携帯型電子機器の無線通信制御部が電子鍵からIDを受信する
s３
受信IDと登録IDを比較した結果、一致したか？
s４
NO
YES
携帯型電子機器の主回路に電源供給する
s５
ドッキングステーションと接続されたか？
s６
NO
YES
終了
s７

フロントページの続き

(56)参考文献 特開平９－３０５２４９（ＪＰ，Ａ）
特開平１１－３４５２０７（ＪＰ，Ａ）
特開平１０－３１６２７（ＪＰ，Ａ）
特開平９－１９８３５１（ＪＰ，Ａ）
特開平５－２０４４８３（ＪＰ，Ａ）
特開平５－２０４４８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 1/00
G06F 1/16