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

特許第5500779号
(P5500779)

(45)発行日　平成26年5月21日(2014.5.21)　(24)登録日　平成26年3月20日(2014.3.20)

(51)Int.Cl.		F I		
H04W 4/00	(2009.01)	H04W	4/00	110
G06K 17/00	(2006.01)	G06K	17/00	F
G06K 19/07	(2006.01)	G06K	19/00	H
H04W 12/06	(2009.01)	H04W	12/06	
H04W 84/10	(2009.01)	H04W	84/10	110

請求項の数 6　(全 10 頁)　最終頁に続く

(21)出願番号　特願2008-95435(P2008-95435)
(22)出願日　平成20年4月1日(2008.4.1)
(65)公開番号　特開2009-253383(P2009-253383A)
(43)公開日　平成21年10月29日(2009.10.29)
審査請求日　平成23年3月31日(2011.3.31)
審判番号　不服2013-2535(P2013-2535/J1)
審判請求日　平成25年2月8日(2013.2.8)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】無線通信装置およびその制御方法、プログラム

(57)【特許請求の範囲】
【請求項１】
無線通信装置であって、
第１の無線通信手段と、
第２の無線通信手段と、
前記第１の無線通信手段の無線通信による他の装置との認証処理の認証結果を判定する判定手段と、
前記判定手段による判定結果に応じて、前記認証処理の認証が成功した場合には前記第２の無線通信手段による前記他の装置との無線通信を実行し、前記認証処理の認証が失敗した場合には前記第２の無線通信手段による無線通信を制限し、前記無線通信装置を当該無線通信装置に対する所定のユーザ操作以外の操作を拒否するロック状態にする制御手段と、を有することを特徴とする無線通信装置。
【請求項２】
前記他の装置から認証結果を受信する受信手段を有し、
前記判定手段は、受信した認証結果に基づいて、前記他の装置との認証結果を判定することを特徴とする請求項１に記載の無線通信装置。
【請求項３】
前記判定手段による判定結果に応じて、前記第２の無線通信手段の電力制御を行う制御手段と、を有することを特徴とする請求項１または請求項２に記載の無線通信装置。
【請求項４】

前記電力制御は、前記第２の無線通信手段への電力供給が行われないようにする制御であることを特徴とする請求項２に記載の無線通信装置。
【請求項５】
第１の無線通信手段と、第２の無線通信手段とを備えた無線通信装置の制御方法であって、
前記第１の無線通信手段の無線通信による他の装置との認証処理の認証結果を判定する判定工程と、
前記判定工程による判定結果に応じて、前記認証処理の認証が成功した場合には前記第２の無線通信手段による前記他の装置との無線通信を実行し、前記認証処理の認証が失敗した場合には前記第２の無線通信手段による無線通信を制限し、前記無線通信装置を当該無線通信装置に対する所定のユーザ操作以外の操作を拒否するロック状態にする制御工程と、を有することを特徴とする無線通信装置の制御方法。
【請求項６】
第１の無線通信手段と、第２の無線通信手段とを備えた無線通信装置のコンピュータに、
前記第１の無線通信手段の無線通信による他の装置との認証処理の認証結果を判定する判定工程と、
前記判定工程による判定結果に応じて、前記認証処理の認証が成功した場合には前記第２の無線通信手段による前記他の装置との無線通信を実行し、前記認証処理の認証が失敗した場合には前記第２の無線通信手段による無線通信を制限し、前記無線通信装置を当該無線通信装置に対する所定のユーザ操作以外の操作を拒否するロック状態にする制御工程と、を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えばいわゆる非接触通信により信号の送受信を行う機能を備えた無線通信端末に関する。
【背景技術】
【０００２】
近年ＲＦＩＤ（Radio Frequency-Identification：電波方式認識）回路を内蔵した非接触ＩＣカード（以下、ＲＦＩＤカード）は、簡易に機器間のアクセスが可能であることの利点を活かし、電車の乗車券として普及している。
【０００３】
また「TransferJET」と呼ばれる非接触転送技術が存在する。この転送技術は電源供給を必要とし、通信距離が最大３cmと短いながらもデータ転送速度が５６０Mbpsと高速である。「TransferJET」はノートＰＣや携帯電話、デジタルカメラ、プリンタ等に搭載することで機器間における高速通信が可能となり、ますますユーザの使い勝手が向上すると思われる。
【０００４】
これらの非接触転送技術においては簡易にデータ転送ができることの反面、そのセキュリティ管理が気にかかるところである。そこで特許文献１においては以下のような認証技術が提案されている。近距離無線通信機能を備えた認証端末と、所定範囲に存在する認証端末を検知する検知機能を備える携帯端末があるとする。携帯端末は、本人未確認の状態においては、キー入力等の第１の開始条件が成立した場合に、近傍の認証端末を探索し個人認証を行う。前記個人認証に成功した場合に本人確認済み状態に遷移して携帯端末の操作を可能にする。
【特許文献１】特開２００６－２２１４５２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】

しかしこれらの方法には以下のような課題が存在する。

【０００６】

例えば今後、非接触転送技術を具備するノートＰＣ、デジタルカメラ、プリンタ等の登場が予測される。ここで仮にノートＰＣを主にデータの取り込み機器、デジタルカメラをデータの転送機器とし、デジタルカメラ内の画像データをノートＰＣへデータ転送する処理を実行する場合を想定してみる。これらの機器においては非接触転送技術によるインタフェースを具備しているので、ノートＰＣにデジタルカメラをかざすだけ、またはノートＰＣにデジタルカメラを乗せるだけで容易にデータ転送を実行することが可能になる。つまりキー入力、パスワード確認等のユーザによる実行意思を確認するフェーズが省略される。従って誰でも簡単かつ短時間でデジタルカメラ内の画像データを取得できるという反面、画像データを取り扱う上でセキュリティ上の課題が生じる。

【０００７】

仮に上記デジタルカメラを悪意の第３者が一瞬でも操作可能な状態になる、または悪意の第三者の前で一瞬でも目を離すなどしてしまうと、上記手順で容易にデジタルカメラのデータを盗難されてしまうということが考えられる。

【０００８】

本発明は上記の課題に鑑みてなされたものであり、非接触転送を行う無線通信において、非接触転送の特徴である簡易性を損なうことなく、セキュリティ性を併せ持つ無線通信を提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記の目的を達成するための本発明の一態様による無線通信装置は以下の構成を備有する。即ち、

無線通信装置であって、

第１の無線通信手段と、

第２の無線通信手段と、

前記第１の無線通信手段の無線通信による他の装置との認証処理の認証結果を判定する判定手段と、

前記判定手段による判定結果に応じて、前記認証処理の認証が成功した場合には前記第２の無線通信手段による前記他の装置との無線通信を実行し、前記認証処理の認証が失敗した場合には前記第２の無線通信手段による無線通信を制限し、前記無線通信装置を当該無線通信装置に対する所定のユーザ操作以外の操作を拒否するロック状態にする制御手段と、を有する。

【発明の効果】

【００１３】

本発明によれば、非接触転送を行う無線通信において、非接触転送の特徴である簡易性を損なうことなく、セキュリティ性を併せ持つ無線通信を提供することが可能となる。従って、本発明の無線通信システムによれば、非接触転送機能を有する機器が盗難にあっても、容易に該機器からデータを盗られない、また利用させないことを実現することができる。

【発明を実施するための最良の形態】

【００１４】

以下、添付図面に従って本発明に係る実施形態を説明する。

【００１５】

本実施形態の特徴点並びに目的は、以下の通りである。すなわち本発明の無線端末は認証用の第１の無線通信手段として「ＲＦＩＤ」機能を具備する。さらにはデータ通信用の第２の無線通信手段として、ＲＦＩＤとは異なる電源供給を必要とする近接非接触通信機能（以後：無線データ通信機能）を具備する。この無線端末においてデータ転送の簡易性を保ったまま、取り扱うデータにおけるセキュリティ維持を提供することである。

【００１６】

本発明の説明に用いる無線システムは、「ＲＦＩＤ」機能、「無線データ通信」機能を具備したデジタルスチルカメラ（以後ＤＳＣ）と、同様の機能を具備したノートＰＣで構成される。そして、このＤＳＣをノートＰＣにかざすだけで、当該ＤＳＣとノートＰＣとの間でセキュリティを考慮したデータ（本実施形態では画像データ）の転送を実現することである。

【００１７】

図１は、本実施形態の無線端末におけるシステムの構成例を示す図である。

【００１８】

１０１は認証用の無線通信を実現する「ＲＦＩＤ」機能部、電源供給することでデータ転送用の無線通信を実現する「無線データ通信」機能部を具備したデジタルカメラ（以後ＤＳＣ）である。このＤＳＣ１０１におけるＲＦＩＤ機能部は主にタグやラベル状に加工されたアンテナ付ＩＣチップから成り、チップに情報を記憶させる「ＲＦＩＤタグ」として機能する。

【００１９】

ＰＣ１０２は同様に認証用の無線通信を実現する「ＲＦＩＤ」機能部、データ転送用の無線通信を実現する「無線データ通信」機能部を具備したノートＰＣ（以後ＰＣ）である。このＰＣ１０２におけるＲＦＩＤ機能部は主にＲＦＩＤタグに情報を書き込み及び読み出したりする「リーダ／ライタ」として機能する。

【００２０】

１０３はＤＳＣ１０１をかざすことでＲＦＩＤリーダ／ライタ部及び無線データ通信部を介して認証またはデータ送受を実現する近接非接触通信機能用インタフェースである。なお、近接非接触通信機能用インタフェースは別体で用意し、ＰＣ１０２とＵＳＢ等のインターフェースを介して接続するようにしてもよい。

【００２１】

まずＤＳＣ１０１の構成について説明する。図２は、本実施形態におけるＤＳＣ１０１の機能構成例を示すブロック図である。

【００２２】

無線データ通信機能部２０１は電源部２０４より電源を供給されることで上述したデータ転送用の無線通信を実現するブロックであり、他の無線通信機器との間で無線信号の送受信を行う。

【００２３】

ＲＦＩＤタグ部２０２も上記の通り認証用の無線通信を実現するために用いられる。例えばＰＣ１０２のＲＦＩＤリーダ／ライタ機能部３０２（図３により後述する）によって、認証情報を書き込むことができる。本実施形態の無線システムは、このＲＦＩＤに書き込まれた情報をＰＣ１０２のＲＦＩＤリーダ／ライタ機能部３０２で確認することで認証処理を実現する。

【００２４】

認証結果処理機能部２０３はＲＦＩＤタグ部２０２より通知される認証結果に応じて、適した処理を施す。またはロック状態となったＤＳＣ１０１のロック解除のための条件判定を行う。これらの具体的な処理に関しては後述する。

【００２５】

電源部２０４はＤＳＣ機能部２０７、無線データ通信機能部２０１、ＣＰＵ２０６等、電源供給を必要とする各ブロックに駆動電源を供給する。

【００２６】

ロック機能部２０５は認証結果処理機能部２０３の指示に応じて無線データ通信機能部２０１への電源供給を停止し、またＤＳＣ機能部２０７の操作をロックする。

ＣＰＵ２０６は以上の動作を指示及び制御するためのブロックである。

ＤＳＣ機能部２０７は実際に画像を撮像するなどＤＳＣとしての機能を処理するブロックである。

【００２７】

次にＰＣ１０２の構成について説明する。図３は本実施形態におけるＰＣ１０２の機能構成例を示すブロック図である。

【００２８】

無線データ通信機能部３０１は電源部３０６より電源を供給されることで上記したデータ転送用の無線通信を実現するブロックであり、他の無線通信機器との間で無線信号の送受信を行う。

ＲＦＩＤリーダ／ライタ機能部３０２は、上記したように認証処理に用いられる。

【００２９】

ディスプレイ機能部３０３はＰＣ１０２において各種表示を行うディスプレイである。メモリ３０４は、ＰＣ１０２のＣＰＵ（不図示）が各種処理を実行するための制御プログラムや、各種データを記憶する。

ＰＣ制御部３０５は、ＣＰＵ（不図示）を具備し、各ブロックの動作を制御する。

電源部３０６は、ＰＣ１０２内の各ブロックに電源を供給する。

キーボード／マウス処理部３０７はキーボードの入力制御、ポインティングデバイス（本例ではマウス）の動作制御を行う。

【００３０】

以上、図１の無線システムを構成する各機器について説明した。図１のシステムにおいてはＤＳＣ１０１に保存されている静止画データ及び動画データを、ＤＳＣ１０１をＰＣ１０２にかざすだけで、データをＰＣ１０２に取り込むという使用方法が考えられる。またはＤＳＣ１０１に保存されている静止画データ及び動画データを、ＤＳＣ１０１をＰＣ１０２にかざすだけでＰＣ１０２のディスプレイ機能部３０３に出力する、といった使用方法も考えられる。ユーザが意図したＤＳＣ１０１からＰＣ１０２へデータ転送が行われる場合には問題はない。しかしながら、ユーザが意図しない機器間でのデータ伝送、例えばＰＣ１０２が悪意の第３者が用意したＰＣである場合のデータ転送は阻止されなければならない。以下にその具体的な方法を図４乃至図６のフローチャート図を用いて説明する。図４は、ＤＳＣ１０１における無線データ転送処理を説明するフローチャートである。また、図５はＤＳＣ１０１におけるロック状態の解除処理を説明するフローチャートである。更に、図６はＰＣ１０２における無線データ転送処理を説明するフローチャートである。

【００３１】

ユーザは図１に示すようにＤＳＣ１０１をＰＣ１０２の近接非接触通信機能用インタフェース１０３上に乗せる、または通信可能な距離まで近づけるようにしてかざす。この操作によりＲＦＩＤタグ部２０２とＲＦＩＤリーダ／ライタ機能部３０２との間でＲＦＩＤによる通信が行われる（ステップＳ４０１）。ＰＣ１０２では、ＲＦＩＤリーダ／ライタ機能部３０２がＲＦＩＤタグ部２０２から読み取った認証情報に基づいて認証処理を行う（ステップＳ４２１、Ｓ４２２）。こうして、ＤＳＣ１０１とＰＣ１０２との間の認証処理が行われる。そして、ＰＣ１０２は、認証に成功した場合にのみ、無線データ通信機能部３０１と無線データ通信機能部２０１を用いたデータの通信を開始する（ステップＳ４２３、Ｓ４２４）。従って、ＤＳＣ１０１において、ＣＰＵ２０６は、ＲＦＩＤタグ部２０２による通信が実行された後、所定時間内に無線データ通信機能部２０１によるデータの通信が開始されたか否かで認証の成否を判定することができる（ステップＳ４０２）。データの通信の開始は、ＰＣ１０２からデータ通信の要求を受信することにより判断することができる。なお、無線データ通信機能部２０１を介してＰＣ１０２から認証の成否を示す情報を受け取って、認証処理の成否を判定するようにしてもよい。

【００３２】

上記した通り、ＤＳＣ１０１のＲＦＩＤタグ部２０２には、ＰＣ１０２のＲＦＩＤリーダ／ライタ機能部３０２によって何かしらの認証情報が書き込まれている必要性がある。そして、例えば、ＤＳＣ１０１のＲＦＩＤタグ部２０２に書き込み済みの認証情報をＰＣ１０２のＲＦＩＤリーダ／ライタ機能部３０２で照合し、認証情報の合致を確認することで認証処理を成功とする。本実施形態においてはＤＳＣ１０１と、ユーザが意図しないＰ

Ｃ１０２、つまり認証処理が成功しないようなＰＣ１０２とのデータ転送処理について説明する。従ってＤＳＣ１０１のＲＦＩＤタグ部２０２には、ＰＣ１０２のＲＦＩＤリーダ／ライタ機能部３０２による認証処理が成功しないような認証情報が書き込まれている、または何も認証情報が書き込まれていないとする。

【００３３】

認証処理に成功したと判定された場合は、認証結果処理機能部２０３は、ＤＳＣ１０１の無線データ通信機能部２０１とＰＣ１０２の無線データ通信機能部３０１によるデータ転送処理を開始する（ステップＳ４０３、ステップＳ４０４）。一方、認証処理に失敗した場合は、処理はステップＳ４０３からステップＳ４０５へ進む。なお、認証処理の失敗の判定においてはユーザが誤って操作した場合を考慮して１回だけで判定するのでなく、予め決められた規定の回数だけ連続して認証に失敗したことをもって認証処理の失敗と判断するようにしてもよい。認証処理の失敗の結果を受けた認証結果処理機能部２０３は、ロック機能部２０５を介して電源部２０４から無線データ通信機能部２０１への電源供給を停止する（ステップＳ４０５）。

【００３４】

近年のＤＳＣは本体におけるメイン電源をオフにしていても電源部２０４より一部のブロックには電源が供給されている。従って機器によっては本体におけるメイン電源をオフにしていても、無線データ通信機能部２０１には電源が供給されているためＰＣ等に対してデータ転送が可能な場合もある。そこで、上記ステップＳ４０５の処理の目的には、これらのデータ転送も阻止することも含まれる。

【００３５】

さらに認証結果処理機能部２０３はロック機能部２０５を介して、当該ＤＳＣ１０１の本体への操作を拒否するべく動作をロックする（ステップＳ４０６）。例えば、当該ロック状態を解除するための操作以外のＤＳＣ１０１に対する操作を拒否するようにする。この処理によりＵＳＢケーブルなどを用いた他のデータ転送機能の禁止、またＤＳＣ１０１内の画像データの消去などを防ぐことができる。

【００３６】

以上の処理によって、ユーザが意図しない、近接非接触通信機能によるデータ転送を防ぐことが可能となる。

【００３７】

次に、不正なＰＣとの認証処理或いはユーザの誤操作によって、ロック機能部２０５によってＤＳＣ１０１の操作がロックされてしまった場合の解除方法について述べる。ロック状態のＤＳＣ１０１はユーザからのあらゆる操作に対して、ロックを解除するための処理を要求することになる。例えば、再生ボタン、撮影ボタンのいずれが操作された場合でも、ＤＳＣ機能部２０７におけるＤＳＣのディスプレイ等へ、ロックを解除するための認証データ（例えばパスワード）の入力を促す表示を行う（ステップＳ５０１）。英数字を入力するためのユーザインターフェースとしては、例えば、ジョグダイヤル、ソフトキーボードなど、周知の技術を採用することができる。ＤＳＣ１０１はユーザによって入力されたパスワードと、予め設定済みのパスワードを認証結果処理機能部２０３にて比較する（ステップＳ５０２）。この比較の結果、パスワードが合致すればロック機能部２０５を介して無線データ通信機能への電源供給の停止を解除し（ステップＳ５０３）、さらには本体の操作ロック状態を解除する（ステップＳ５０４）。

【００３８】

以上のようにＤＳＣ１０１は、ＲＦＩＤタグを用いてＰＣ１０２との間で認証処理を実施する。そして、ＤＳＣ１０１は、認証処理が成功した場合は通常のデータ転送を行うが、認証処理が失敗した場合は本体電源からの無線データ通信機能への電源供給を停止する。さらに、ＤＳＣ１０１は、ユーザによる当該ＤＳＣ１０１への各種操作（ロック状態を解除するためのパスワード入力以外の操作）をロックする。

【００３９】

これらの機能により、近接非接触通信機能を具備した機器において、セキュリティ性を

保ちつつ、容易なデータ転送を提供することができる。

【００４０】

以上、実施形態を詳述したが、本発明は、例えば、システム、装置、方法、プログラムもしくは記憶媒体等としての実施態様をとることが可能である。具体的には、複数の機器から構成されるシステムに適用しても良いし、また、一つの機器からなる装置に適用しても良い。

【００４１】

尚、本発明は、ソフトウェアのプログラムをシステム或いは装置に直接或いは遠隔から供給し、そのシステム或いは装置のコンピュータが該供給されたプログラムコードを読み出して実行することによって前述した実施形態の機能が達成される場合を含む。この場合、供給されるプログラムは実施形態で図に示したフローチャートに対応したコンピュータプログラムである。

【００４２】

従って、本発明の機能処理をコンピュータで実現するために、該コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明は、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。

【００４３】

その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等の形態であっても良い。

【００４４】

コンピュータプログラムを供給するためのコンピュータ読み取り可能な記憶媒体としては以下が挙げられる。例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）などである。

【００４５】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続し、該ホームページから本発明のコンピュータプログラムをハードディスク等の記録媒体にダウンロードすることが挙げられる。この場合、ダウンロードされるプログラムは、圧縮され自動インストール機能を含むファイルであってもよい。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明に含まれるものである。

【００４６】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布するという形態をとることもできる。この場合、所定の条件をクリアしたユーザに、インターネットを介してホームページから暗号を解く鍵情報をダウンロードさせ、その鍵情報を使用して暗号化されたプログラムを実行し、プログラムをコンピュータにインストールさせるようにもできる。

【００４７】

また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される他、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどとの協働で実施形態の機能が実現されてもよい。この場合、ＯＳなどが、実際の処理の一部または全部を行ない、その処理によって前述した実施形態の機能が実現される。

【００４８】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれて前述の実施形態の機能の一部或いは全てが実現されてもよい。この場合、機能拡張ボードや機

能拡張ユニットにプログラムが書き込まれた後、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行なう。

【図面の簡単な説明】

【００４９】

【図１】実施形態による無線通信システムの構成例を示す図である。

【図２】実施形態におけるＤＳＣの機能構成例を示すブロック図である。

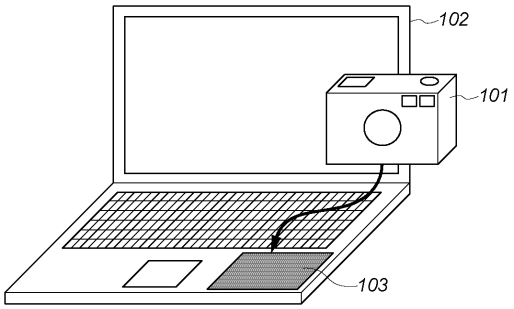
【図３】実施形態におけるＰＣの機能構成例を示すブロック図である。

【図４】実施形態のＤＳＣ１０１による無線データ転送の処理を示すフローチャートである。

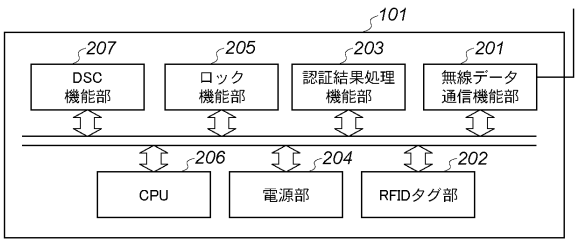
【図５】実施形態のＤＳＣ１０１による、ロック解除処理を示すフローチャートである。

【図６】実施形態のＰＣ１０２による、無線データ転送の処理を示すフローチャートである。

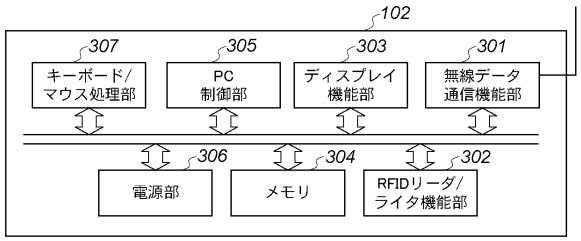
【図１】



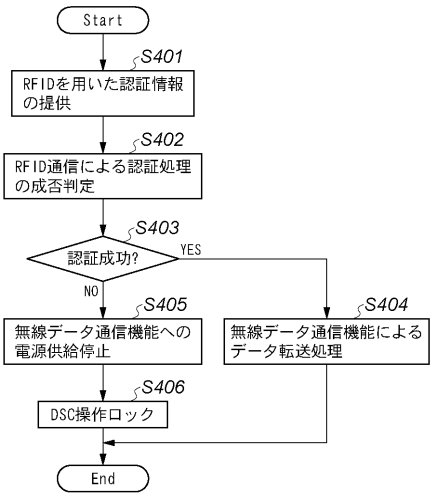
【図２】



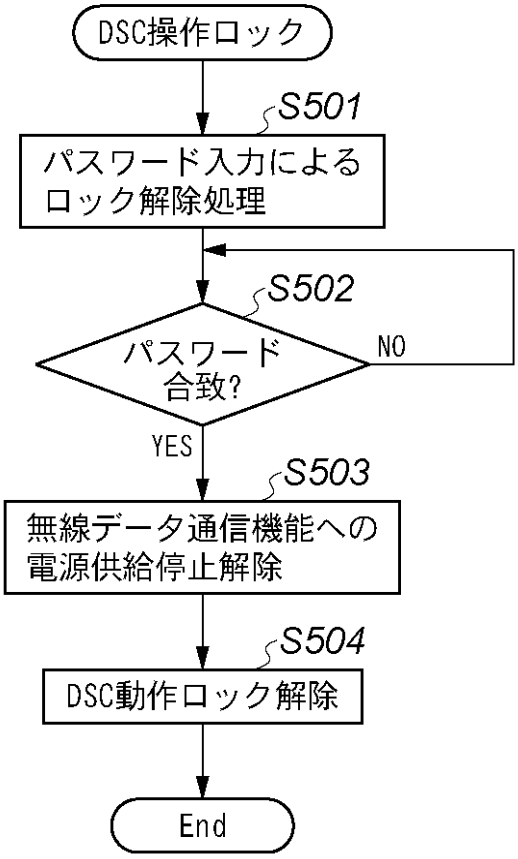
【図３】



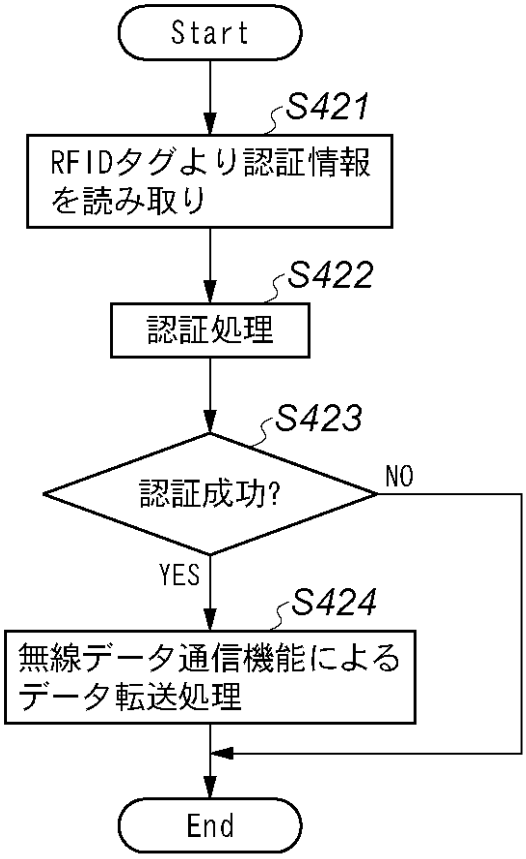
【図４】



【図５】


DSC操作ロック
S501
パスワード入力による
ロック解除処理
S502
パスワード
合致?
NO
YES
S503
無線データ通信機能への
電源供給停止解除
S504
DSC動作ロック解除
End

【図６】


Start
S421
RFIDタグより認証情報
を読み取り
S422
認証処理
S423
認証成功?
NO
YES
S424
無線データ通信機能による
データ転送処理
End

フロントページの続き

(51)Int.Cl. ＦＩ
Ｈ０４Ｗ 88/06 (2009.01) Ｈ０４Ｗ 88/06

(72)発明者 森友 和夫
東京都大田区下丸子３丁目３０番２号 キヤノン株式会社内

合議体
審判長 加藤 恵一
審判官 佐藤 聡史
審判官 吉田 隆之

(56)参考文献 特開２００８－６５７７４（ＪＰ，Ａ）
特開２００５－３３３１８４（ＪＰ，Ａ）
特開２００５－１６７９４６（ＪＰ，Ａ）
特開２００６－９３９３４（ＪＰ，Ａ）
特開２００７－１６６５３８（ＪＰ，Ａ）
特開２００６－２４６３９２（ＪＰ，Ａ）
特開２００３－２８４１４１（ＪＰ，Ａ）