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

特許第6152767号
(P6152767)

(45)発行日　平成29年6月28日(2017.6.28)　(24)登録日　平成29年6月9日(2017.6.9)

(51)Int.Cl.		F I		
G06F 21/35	(2013.01)	G06F	21/35	
G06F 13/00	(2006.01)	G06F	13/00	５１０Ａ
G06K 19/07	(2006.01)	G06K	19/07	２３０
G06K 7/10	(2006.01)	G06K	7/10	
G06F 3/12	(2006.01)	G06F	3/12	３２２

請求項の数 10　(全 31 頁)　最終頁に続く

(21)出願番号　特願2013-205321 (P2013-205321)
(22)出願日　平成25年9月30日 (2013.9.30)
(65)公開番号　特開2015-69559 (P2015-69559A)
(43)公開日　平成27年4月13日 (2015.4.13)
審査請求日　平成28年3月10日 (2016.3.10)

(73)特許権者　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　110000110
特許業務法人快友国際特許事務所
(72)発明者　寺下　訓史
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】機能実行機器と可搬型デバイス

(57)【特許請求の範囲】
【請求項１】
機能実行機器であって、
特定機能を実行する機能実行部と、
ユーザによって操作される操作部と、
制御部と、を備え、
前記制御部は、
第１のユーザ認証情報が認証用メモリに登録されている状態で、第１のユーザによって前記操作部が操作されて、前記第１のユーザ認証情報が前記機能実行機器に入力される場合に、前記機能実行機器の状態を、前記第１のユーザに前記特定機能の利用を許可しない第１の不許可状態から、前記第１のユーザに前記特定機能の利用を許可する第１の許可状態へ移行させる状態移行部と、
第１の可搬型デバイスとの第１の接続が確立され、かつ、前記第１の可搬型デバイスから所定のアプリケーション情報が取得される場合に、前記第１のユーザ認証情報に関連付けて第１のデバイス認証情報を前記認証用メモリに登録する登録部であって、前記第１の可搬型デバイスとの前記第１の接続が確立され、かつ、前記第１の可搬型デバイスから前記所定のアプリケーション情報が取得されない場合に、前記第１のデバイス認証情報は、前記第１のユーザ認証情報に関連付けて前記認証用メモリに登録されず、前記所定のアプリケーション情報は、前記機能実行機器を利用するためのアプリケーションが前記第１の可搬型デバイスで起動中である場合に、前記第１の可搬型デバイスから前記機能実行機器

に供給される情報である、前記登録部と、
前記第１の可搬型デバイスとの前記第１の接続が確立される場合に、前記第１のデバイス認証情報を前記第１の可搬型デバイスに供給する供給部と、を備え、
前記状態移行部は、さらに、前記第１のデバイス認証情報が前記認証用メモリに登録された後に、前記第１の可搬型デバイスとの第２の接続が確立されて、前記第１の可搬型デバイスから前記第１のデバイス認証情報が取得される場合に、前記機能実行機器の状態を前記第１の不許可状態から前記第１の許可状態へ移行させる、
機能実行機器。
【請求項２】
機能実行機器であって、
特定機能を実行する機能実行部と、
ユーザによって操作される操作部と、
制御部と、
第１のモードと第２のモードとを含む複数のモードで動作可能な機器インターフェースと、を備え、
前記制御部は、
第１のユーザ認証情報が認証用メモリに登録されている状態で、第１のユーザによって前記操作部が操作されて、前記第１のユーザ認証情報が前記機能実行機器に入力される場合に、前記機能実行機器の状態を、前記第１のユーザに前記特定機能の利用を許可しない第１の不許可状態から、前記第１のユーザに前記特定機能の利用を許可する第１の許可状態へ移行させる状態移行部と、
第１の可搬型デバイスとの第１の接続が確立される場合に、前記第１のユーザ認証情報に関連付けて第１のデバイス認証情報を前記認証用メモリに登録する登録部であって、前記第１の接続は、前記機器インターフェースが前記第１のモードで動作するための接続である、前記登録部と、
前記第１の可搬型デバイスとの前記第１の接続が確立される場合に、前記第１のデバイス認証情報を前記第１の可搬型デバイスに供給する供給部と、を備え、
前記状態移行部は、さらに、前記第１のデバイス認証情報が前記認証用メモリに登録された後に、前記第１の可搬型デバイスとの第２の接続が確立されて、前記第１の可搬型デバイスから前記第１のデバイス認証情報が取得される場合に、前記機能実行機器の状態を前記第１の不許可状態から前記第１の許可状態へ移行させ、
前記第２の接続は、前記機器インターフェースが前記第２のモードで動作するための接続である、
機能実行機器。
【請求項３】
前記制御部は、さらに、
前記第１の可搬型デバイスとの接続が確立される場合に、前記確立済みの接続が、前記機器インターフェースが前記第１のモードで動作するための前記第１の接続であるのか、前記機器インターフェースが前記第２のモードで動作するための前記第２の接続であるのか、を判断し、前記確立済みの接続が前記第１の接続であると判断する場合に、第１種の処理を実行すべきことを決定し、前記確立済みの接続が前記第２の接続であると判断する場合に、第２種の処理を実行すべきことを決定する決定部を備え、
前記第１種の処理は、
前記登録部が、前記第１のユーザ認証情報に関連付けて前記第１のデバイス認証情報を前記認証用メモリに登録する処理と、
前記供給部が、前記第１のデバイス認証情報を前記第１の可搬型デバイスに供給する処理と、を含み、
前記第２種の処理は、
前記第１の可搬型デバイスから前記第１のデバイス認証情報が取得される場合に、前記状態移行部が、前記機能実行機器の状態を前記第１の不許可状態から前記第１の許可状

態へ移行させる処理を含む、請求項２に記載の機能実行機器。
【請求項４】
前記第２のモードは、ＮＦＣ（Near Field Communicationの略）方式のＲｅａｄｅｒ／Ｗｒｉｔｅｒモードを含む、請求項２又は３に記載の機能実行機器。
【請求項５】
前記登録部は、前記機能実行機器の状態が前記第１の許可状態である間に、前記第１の可搬型デバイスとの前記第１の接続が確立される場合に、前記第１のユーザ認証情報に関連付けて前記第１のデバイス認証情報を前記認証用メモリに登録する、請求項１から４のいずれか一項に記載の機能実行機器。
【請求項６】
前記登録部は、さらに、前記第１のデバイス認証情報が前記認証用メモリに登録された後に、前記機能実行機器の状態が前記第１の許可状態である間に、第２の可搬型デバイスとの第３の接続が確立される場合に、前記第１のユーザ認証情報に関連付けて、前記第１のデバイス認証情報に代えて、第２のデバイス認証情報を前記認証用メモリに登録し、
前記供給部は、さらに、前記第２の可搬型デバイスとの前記第３の接続が確立される場合に、前記第２のデバイス認証情報を前記第２の可搬型デバイスに供給し、
前記状態移行部は、さらに、前記第２のデバイス認証情報が前記認証用メモリに登録された後に、前記第２の可搬型デバイスとの第４の接続が確立されて、前記第２の可搬型デバイスから前記第２のデバイス認証情報が取得される場合に、前記機能実行機器の状態を前記第１の不許可状態から前記第１の許可状態へ移行させる、請求項５に記載の機能実行機器。
【請求項７】
前記状態移行部は、さらに、前記第１のユーザ認証情報とは異なる第２のユーザ認証情報が前記認証用メモリに登録されている状態で、第２のユーザによって前記操作部が操作されて、前記第２のユーザ認証情報が前記機能実行機器に入力される場合に、前記機能実行機器の状態を、前記第２のユーザに前記特定機能の利用を許可しない第２の不許可状態から、前記第２のユーザに前記特定機能の利用を許可する第２の許可状態へ移行させ、
前記登録部は、さらに、前記機能実行機器の状態が前記第２の許可状態である間に、第３のデバイス認証情報を予め記憶している第３の可搬型デバイスとの第５の接続が確立されて、前記第３の可搬型デバイスから前記第３のデバイス認証情報が取得される場合に、前記第２のユーザ認証情報に関連付けて前記第３のデバイス認証情報を前記認証用メモリに登録し、
前記状態移行部は、さらに、前記第３のデバイス認証情報が前記認証用メモリに登録された後に、前記機能実行機器の状態が前記第２の不許可状態である間に、前記第３の可搬型デバイスとの第６の接続が確立されて、前記第３の可搬型デバイスから前記第３のデバイス認証情報が取得される場合に、前記機能実行機器の状態を前記第２の不許可状態から前記第２の許可状態へ移行させる、請求項１から６のいずれか一項に記載の機能実行機器。
【請求項８】
前記登録部は、前記第１の可搬型デバイスとの前記第１の接続が確立される場合に、前記第１のデバイス認証情報を生成して、前記第１のユーザ認証情報に関連付けて前記第１のデバイス認証情報を前記認証用メモリに登録する、請求項１から７のいずれか一項に記載の機能実行機器。
【請求項９】
可搬型デバイスであって、
制御部と、
第３のモードと第４のモードとを含む複数のモードで動作可能なデバイスインターフェースと、を備え、
前記制御部は、
デバイスメモリと、

第１のデバイス認証情報が前記デバイスメモリに記憶されていない場合に、前記第３のモードで動作すべきことを前記デバイスインターフェースに指示し、前記第１のデバイス認証情報が前記デバイスメモリに記憶されている場合に、前記第４のモードで動作すべきことを前記デバイスインターフェースに指示するインターフェース制御部と、

前記第３のモードで動作する前記デバイスインターフェースを介して、特定機能を実行可能な機能実行機器との第１の接続が確立される場合に、前記機能実行機器から前記第１のデバイス認証情報を取得する取得部と、

前記機能実行機器から前記第１のデバイス認証情報が取得される場合に、前記第１のデバイス認証情報を前記デバイスメモリに記憶させる記憶制御部と、

前記第１のデバイス認証情報が前記デバイスメモリに記憶された後に、前記第４のモードで動作する前記デバイスインターフェースを介して、前記機能実行機器との第２の接続が確立される場合に、前記デバイスメモリ内の前記第１のデバイス認証情報を前記機能実行機器に供給して、前記機能実行機器の状態を、前記可搬型デバイスのユーザに前記特定機能の利用を許可しない不許可状態から、前記ユーザに前記特定機能の利用を許可する許可状態へ移行させる供給部と、

を備える、可搬型デバイス。

【請求項１０】

可搬型デバイスのためのコンピュータプログラムであって、

第１のデバイス認証情報がデバイスメモリに記憶されていない場合に、第３のモードで動作すべきことをデバイスインターフェースに指示し、前記第１のデバイス認証情報が前記デバイスメモリに記憶されている場合に、第４のモードで動作すべきことを前記デバイスインターフェースに指示するインターフェース制御処理であって、前記デバイスインターフェースは、前記第３のモードと前記第４のモードとを含む複数のモードで動作可能である、前記インターフェース制御処理と、

前記第３のモードで動作する前記デバイスインターフェースを介して、特定機能を実行可能な機能実行機器との第１の接続が確立される場合に、前記機能実行機器から第１のデバイス認証情報を取得する取得処理と、

前記機能実行機器から前記第１のデバイス認証情報が取得される場合に、前記第１のデバイス認証情報を前記可搬型デバイスのデバイスメモリに記憶させる記憶制御処理と、

前記第１のデバイス認証情報が前記デバイスメモリに記憶された後に、前記第４のモードで動作する前記デバイスインターフェースを介して、前記機能実行機器との第２の接続が確立される場合に、前記デバイスメモリ内の前記第１のデバイス認証情報を前記機能実行機器に供給して、前記機能実行機器の状態を、前記可搬型デバイスのユーザに前記特定機能の利用を許可しない不許可状態から、前記ユーザに前記特定機能の利用を許可する許可状態へ移行させる供給処理と、

を実行させるコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本明細書によって開示される技術は、特定機能を実行可能な機能実行機器と、当該特定機能を機能実行機器に実行させるために利用される可搬型デバイスと、に関する。

【背景技術】

【０００２】

特許文献１には、複合機が開示されている。複合機は、ユーザ情報が複合機に入力される場合に、ユーザ情報の認証を認証サーバに実行させる。複合機は、ユーザ情報の認証が成功した後に、複合機のカードリーダにタッチされるカードからカード情報を取得して、カード情報を認証サーバに供給する。認証サーバは、ユーザ情報に関連付けて、カード情報を登録する。これにより、ユーザは、ユーザ情報を複合機に入力しなくても、複合機のカードリーダにカードをタッチさせれば、複合機にログインすることができる。

【先行技術文献】

【特許文献】
【０００３】
【特許文献１】特開２０１０－１０８３４８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
上記の技術では、カード情報がカードに予め記憶されていることが前提となっている。従って、ユーザは、カード情報を予め記憶しているカードを準備しなければならない。本明細書では、ユーザが、デバイス認証情報を予め記憶していない可搬型デバイスを利用して、機能実行機器に特定機能を実行させ得る技術を提供する。
【課題を解決するための手段】
【０００５】
本明細書によって開示される機能実行機器は、特定機能を実行する機能実行部と、ユーザによって操作される操作部と、制御部と、を備える。制御部は、状態移行部と、登録部と、供給部と、を備える。状態移行部は、第１のユーザ認証情報が認証用メモリに登録されている状態で、第１のユーザによって操作部が操作されて、第１のユーザ認証情報が機能実行機器に入力される場合に、機能実行機器の状態を、第１のユーザに特定機能の利用を許可しない第１の不許可状態から、第１のユーザに特定機能の利用を許可する第１の許可状態へ移行させる。登録部は、第１の可搬型デバイスとの第１の接続が確立される場合に、第１のユーザ認証情報に関連付けて第１のデバイス認証情報を認証用メモリに登録する。供給部は、第１の可搬型デバイスとの第１の接続が確立される場合に、第１のデバイス認証情報を第１の可搬型デバイスに供給する。状態移行部は、さらに、第１のデバイス認証情報が認証用メモリに登録された後に、第１の可搬型デバイスとの第２の接続が確立されて、第１の可搬型デバイスから第１のデバイス認証情報が取得される場合に、機能実行機器の状態を第１の不許可状態から第１の許可状態へ移行させる。
【０００６】
上記の構成によると、機能実行機器は、第１のユーザによって操作部が操作されて、第１のユーザ認証情報が機能実行機器に入力される場合に、機能実行機器の状態を第１の許可状態へ移行させる。このために、第１のユーザは、機能実行機器に特定機能を実行させ得る。また、機能実行機器は、第１のユーザ認証情報に関連付けて第１のデバイス認証情報を認証用メモリに登録して、第１のデバイス認証情報を第１の可搬型デバイスに供給する。即ち、機能実行機器は、仮に、デバイス認証情報が第１の可搬型デバイスに予め記憶されていなくても、第１のデバイス認証情報を第１の可搬型デバイスに割り当てることができる。その後、機能実行機器は、第１の可搬型デバイスから第１のデバイス認証情報を取得する場合に、機能実行機器の状態を第１の許可状態へ移行させる。従って、第１のユーザは、デバイス認証情報を予め記憶していない第１の可搬型デバイスを利用して、機能実行機器に特定機能を実行させ得る。
【０００７】
登録部は、機能実行機器の状態が第１の許可状態である間に、第１の可搬型デバイスとの第１の接続が確立される場合に、第１のユーザ認証情報に関連付けて第１のデバイス認証情報を認証用メモリに登録してもよい。この構成によると、機能実行機器は、第１のユーザ情報に関連付けて第１のデバイス認証情報を認証用メモリに適切に登録することができる。
【０００８】
登録部は、さらに、第１のデバイス認証情報が認証用メモリに登録された後に、機能実行機器の状態が第１の許可状態である間に、第２の可搬型デバイスとの第３の接続が確立される場合に、第１のユーザ認証情報に関連付けて、第１のデバイス認証情報に代えて、第２のデバイス認証情報を認証用メモリに登録してもよい。供給部は、さらに、第２の可搬型デバイスとの第３の接続が確立される場合に、第２のデバイス認証情報を第２の可搬型デバイスに供給してもよい。状態移行部は、さらに、第２のデバイス認証情報が認証用

メモリに登録された後に、第２の可搬型デバイスとの第４の接続が確立されて、第２の可搬型デバイスから第２のデバイス認証情報が取得される場合に、機能実行機器の状態を第１の不許可状態から第１の許可状態へ移行させてもよい。この構成によると、例えば、第１のユーザが第１の可搬型デバイスに代えて第２の可搬型デバイスを利用することを望む場合に、機能実行機器は、第１のユーザ認証情報に関連付けて、第１のデバイス認証情報に代えて、第２のデバイス認証情報を認証用メモリに登録して、第２のデバイス認証情報を第２の可搬型デバイスに供給することができる。従って、第１のユーザは、第１の可搬型デバイスに代えて第２の可搬型デバイスを利用して、機能実行機器に特定機能を実行させ得る。

【０００９】

状態移行部は、さらに、第１のユーザ認証情報とは異なる第２のユーザ認証情報が認証用メモリに登録されている状態で、第２のユーザによって操作部が操作されて、第２のユーザ認証情報が機能実行機器に入力される場合に、機能実行機器の状態を、第２のユーザに特定機能の利用を許可しない第２の不許可状態から、第２のユーザに特定機能の利用を許可する第２の許可状態へ移行させてもよい。登録部は、さらに、機能実行機器の状態が第２の許可状態である間に、第３のデバイス認証情報を予め記憶している第３の可搬型デバイスとの第５の接続が確立されて、第３の可搬型デバイスから第３のデバイス認証情報が取得される場合に、第２のユーザ認証情報に関連付けて第３のデバイス認証情報を認証用メモリに登録してもよい。状態移行部は、さらに、第３のデバイス認証情報が認証用メモリに登録された後に、機能実行機器の状態が第２の不許可状態である間に、第３の可搬型デバイスとの第６の接続が確立されて、第３の可搬型デバイスから第３のデバイス認証情報が取得される場合に、機能実行機器の状態を第２の不許可状態から第２の許可状態へ移行させてもよい。この構成によると、機能実行機器は、機能実行機器の状態が第２の許可状態である間に、第３の可搬型デバイスから第３のデバイス認証情報を取得する場合に、第２のユーザ認証情報に関連付けて第３のデバイス認証情報を認証用メモリに登録する。そして、機能実行機器は、第３の可搬型デバイスから第３のデバイス認証情報を取得する場合に、機能実行機器の状態を第２の許可状態へ移行させる。従って、第２のユーザは、第３のデバイス認証情報を予め記憶している第３の可搬型デバイスを利用して、機能実行機器に特定機能を実行させ得る。

【００１０】

登録部は、第１の可搬型デバイスとの第１の接続が確立され、かつ、第１の可搬型デバイスから所定のアプリケーション情報が取得される場合に、第１のユーザ認証情報に関連付けて第１のデバイス認証情報を認証用メモリに登録してもよく、第１の可搬型デバイスとの第１の接続が確立され、かつ、第１の可搬型デバイスから所定のアプリケーション情報が取得されない場合に、第１のユーザ認証情報に関連付けて第１のデバイス認証情報を認証用メモリに登録しなくてもよい。所定のアプリケーション情報は、機能実行機器を利用するためのアプリケーションが第１の可搬型デバイスで起動中である場合に、第１の可搬型デバイスから機能実行機器に供給されてもよい。この構成によると、機能実行機器は、機能実行機器を利用するためのアプリケーションが第１の可搬型デバイスで起動中でない場合、即ち、第１のデバイス認証情報の登録が目的ではない状況で、第１の可搬型デバイスとの第１の接続が確立される場合に、第１のデバイス認証情報を認証用メモリに登録せずに済む。

【００１１】

登録部は、第１の可搬型デバイスとの第１の接続が確立される場合に、第１のデバイス認証情報を生成して、第１のユーザ認証情報に関連付けて第１のデバイス認証情報を認証用メモリに登録してもよい。

【００１２】

機能実行機器は、さらに、第１のモードと第２のモードとを含む複数のモードで動作可能な機器インターフェースを備えていてもよい。第１の接続は、機器インターフェースが第１のモードで動作するための接続であってもよい。第２の接続は、機器インターフェー

スが第２のモードで動作するための接続であってもよい。

【００１３】

制御部は、さらに、第１の可搬型デバイスとの接続が確立される場合に、確立済みの接続が、機器インターフェースが第１のモードで動作するための第１の接続であるのか、機器インターフェースが第２のモードで動作するための第２の接続であるのか、を判断し、確立済みの接続が第１の接続であると判断する場合に、第１種の処理を実行すべきことを決定し、確立済みの接続が第２の接続であると判断する場合に、第２種の処理を実行すべきことを決定する決定部を備えていてもよい。第１種の処理は、登録部が、第１のユーザ認証情報に関連付けて第１のデバイス認証情報を認証用メモリに登録する処理と、供給部が、第１のデバイス認証情報を第１の可搬型デバイスに供給する処理と、を含んでいてもよい。第２種の処理は、第１の可搬型デバイスから第１のデバイス認証情報が取得される場合に、状態移行部が、機能実行機器の状態を第１の不許可状態から第１の許可状態へ移行させる処理を含んでいてもよい。この構成によると、機器実行機器は、確立済みの接続の種類（即ち第１の接続又は第２の接続）に応じて、適切な処理を実行し得る。

【００１４】

第２のモードは、ＮＦＣ（Near Field Communicationの略）方式のＲｅａｄｅｒ／Ｗｒｉｔｅｒモードを含んでいてもよい。

【００１５】

本明細書によって開示される可搬型デバイスは、制御部を備える。制御部は、デバイスメモリと、取得部と、記憶制御部と、供給部と、を備える。取得部は、特定機能を実行可能な機能実行機器との第１の接続が確立される場合に、機能実行機器から第１のデバイス認証情報を取得する。記憶制御部は、機能実行機器から第１のデバイス認証情報が取得される場合に、第１のデバイス認証情報をデバイスメモリに記憶させる。供給部は、第１のデバイス認証情報がデバイスメモリに記憶された後に、機能実行機器との第２の接続が確立される場合に、デバイスメモリ内の第１のデバイス認証情報を機能実行機器に供給して、機能実行機器の状態を、可搬型デバイスのユーザに特定機能の利用を許可しない不許可状態から、ユーザに特定機能の利用を許可する許可状態へ移行させる。

【００１６】

上記の構成によると、可搬型デバイスは、デバイス認証情報を予め記憶していなくても、機能実行機器から第１のデバイス認証情報を取得して、第１のデバイス認証情報をデバイスメモリに記憶させることができる。その後、可搬型デバイスは、第１のデバイス認証情報を機能実行機器に供給して、機能実行機器の状態を許可状態へ移行させることができる。従って、ユーザは、デバイス認証情報を予め記憶していない可搬型デバイスを利用して、機能実行機器に特定機能を実行させ得る。

【００１７】

可搬型デバイスは、さらに、第３のモードと第４のモードとを含む複数のモードで動作可能なデバイスインターフェースを備えていてもよい。制御部は、さらに、第１のデバイス認証情報がデバイスメモリに記憶されていない場合に、第３のモードで動作すべきことをデバイスインターフェースに指示し、第１のデバイス認証情報がデバイスメモリに記憶されている場合に、第４のモードで動作すべきことをデバイスインターフェースに指示するインターフェース制御部を備えていてもよい。取得部は、第３のモードで動作するデバイスインターフェースを介して、機能実行機器との第１の接続が確立される場合に、機能実行機器から第１のデバイス認証情報を取得してもよい。供給部は、第４のモードで動作するデバイスインターフェースを介して、機能実行機器との第２の接続が確立される場合に、第１のデバイス認証情報を機能実行機器に供給して、機能実行機器の状態を不許可状態から許可状態へ移行させてもよい。この構成によると、可搬型デバイスは、第１のデバイス認証情報がデバイスメモリに記憶されているのか否かに応じて、デバイスインターフェースが動作すべきモードを決定する。従って、可搬型デバイスは、第１のデバイス認証情報がデバイスメモリに記憶されているのか否かに応じて、適切な処理を実行し得る。

【００１８】

なお、上記の機能実行機器又は可搬型デバイスを実現するための制御方法、コンピュータプログラム、及び、当該コンピュータプログラムを格納するコンピュータ読取可能記録媒体も、新規で有用である。また、上記の機能実行機器と可搬型デバイスとを含む通信システムも、新規で有用である。

【図面の簡単な説明】

【００１９】

【図１】通信システムの構成を示す。

【図２】多機能機とＮＦＣ機器との間でＮＦＣ方式の接続が確立される様子を示す。

【図３】多機能機のログイン管理処理のフローチャートを示す。

【図４】図３の続きのフローチャートを示す。

【図５】携帯端末のアプリケーション処理のフローチャートを示す。

【図６】多機能機及び携帯端末によって実行される各処理のシーケンス図を示す。

【図７】多機能機及び携帯端末によって実行される各処理のシーケンス図を示す。

【図８】多機能機及び認証カードによって実行される各処理のシーケンス図を示す。

【発明を実施するための形態】

【００２０】

（通信システム２の構成）

図１に示すように、通信システム２は、多機能機１０と、複数個の携帯端末ＰＴ１，ＰＴ２と、認証カードＡＣと、を備える。

【００２１】

（多機能機１０の構成）

多機能機１０は、印刷機能、スキャン機能、コピー機能等の多機能を実行可能な周辺機器（即ち、図示省略のＰＣ（Personal Computerの略）等の周辺機器）である。多機能機１０は、操作部１２と、表示部１４と、印刷実行部１６と、スキャン実行部１８と、ＮＦＣ（Near Field Communicationの略）インターフェース２０と、ＬＡＮ（Local Area Networkの略）インターフェース２２と、制御部３０と、を備える。各部１２～３０は、バス線（符号省略）に接続されている。以下では、インターフェースのことを「Ｉ／Ｆ」と記載する。

【００２２】

操作部１２は、複数のキーを備える。ユーザは、操作部１２を操作することによって、様々な指示を多機能機１０に入力することができる。表示部１４は、様々な情報を表示するためのディスプレイである。印刷実行部１６は、インクジェット方式、レーザ方式等の印刷機構である。スキャン実行部１８は、ＣＣＤ、ＣＩＳ等のスキャン機構である。

【００２３】

ＮＦＣＩ／Ｆ２０は、ＮＦＣ方式に従ったＮＦＣ通信を実行するためのＩ／Ｆである。ＮＦＣ方式は、例えば、ＩＳＯ／ＩＥＣ２１４８１又は１８０９２の国際標準規格に従って、近距離無線通信を実行するための無線通信方式である。ＮＦＣＩ／Ｆ２０は、Ｐ２Ｐ（Peer to Peerの略）モードとＲ／Ｗ（Reader/Writerの略）モードとで動作可能である。

【００２４】

ＬＡＮＩ／Ｆ２２は、Ｗｉ－Ｆｉ方式に従った無線通信（即ちＷｉ－Ｆｉ通信）を実行するためのＩ／Ｆである。ただし、変形例では、ＬＡＮＩ／Ｆ２２は、有線通信を実行するためのＩ／Ｆであってもよい。Ｗｉ－Ｆｉ方式は、例えば、ＩＥＥＥ（The Institute of Electrical and Electronics Engineers, Inc.の略）の８０２．１１の規格、及び、それに準ずる規格（例えば、８０２．１１ａ，１１ｂ，１１ｇ，１１ｎ等）に従って、無線通信を実行するための無線通信方式である。

【００２５】

ここでは、ＮＦＣＩ／Ｆ２０を介した無線通信と、ＬＡＮＩ／Ｆ２２を介した無線通信と、の相違点を説明しておく。ＬＡＮＩ／Ｆ２２を介した無線通信の通信速度（例えば、最大の通信速度が１１～６００Ｍｂｐｓ）は、ＮＦＣＩ／Ｆ２０を介した無線通信の通信

速度（例えば、最大の通信速度が１００～４２４Ｋｂｐｓ）よりも速い。また、ＬＡＮＩ／Ｆ２２を介した無線通信における搬送波の周波数（例えば、２．４ＧＨｚ帯、５．０ＧＨｚ帯）は、ＮＦＣＩ／Ｆ２０を介した無線通信における搬送波の周波数（例えば、１３．５６ＭＨｚ帯）とは異なる。また、多機能機１０がＬＡＮＩ／Ｆ２２を介して外部機器と無線通信を実行可能な最大の距離（例えば最大で１００ｍ）は、多機能機１０がＮＦＣＩ／Ｆ２０を介して外部機器と無線通信を実行可能な最大の距離（例えば最大で１０ｃｍ）よりも大きい。

【００２６】

制御部３０は、ＣＰＵ３２とメモリ３４とを備える。ＣＰＵ３２は、メモリ３４に格納されているプログラム３６に従って、様々な処理を実行する。メモリ３４は、上記のプログラム３６の他に、認証テーブルＡＴを格納する。

【００２７】

認証テーブルＡＴは、複数のユーザに対応する複数の組合せ情報を記憶可能である。各組合せ情報は、ユーザＩＤと、パスワードと、デバイスＩＤと、コピー許可情報と、スキャン許可情報と、送信先情報と、が関連付けられた情報である。ユーザＩＤ及びパスワードは、ユーザを認証するためのユーザ認証情報である。デバイスＩＤは、多機能機１０とは異なるデバイス（即ち、携帯端末ＰＴ１，ＰＴ２、認証カードＡＣ等）を認証するためのデバイス認証情報である。コピー許可情報、スキャン許可情報は、それぞれ、コピー機能、スキャン機能の実行をユーザに許可するのか否かを示す情報であり、「ＯＫ」及び「ＮＧ」のどちらかの値を示す。「ＯＫ」は、機能（コピー機能又はスキャン機能）の実行をユーザに許可することを示し、「ＮＧ」は、機能の実行をユーザに許可しないことを示す。送信先情報は、スキャン機能が実行されて生成されるスキャンデータの送信先を示す情報であり、例えば、ＰＣ等の外部機器のＩＰアドレスを示す。

【００２８】

通信システム２の管理者は、例えば、多機能機１０の操作部１２を操作して、又は、図示省略のＰＣを利用して多機能機１０にアクセスして、認証テーブルＡＴに情報を登録する。具体的には、管理者は、ユーザＩＤ（例えば「Ｕ１」、「Ｕ２」）、パスワード（例えば「Ｐ１」、「Ｐ２」）、コピー許可情報（即ち「ＯＫ」又は「ＮＧ」）、及び、スキャン許可情報（即ち「ＯＫ」又は「ＮＧ」）を、多機能機１０に入力する。管理者は、スキャン許可情報「ＯＫ」を入力する場合には、さらに、送信先情報（例えば「ＩＰ１」）を多機能機１０に入力する。これにより、多機能機１０のＣＰＵ３２は、入力された各情報を認証テーブルＡＴに登録する。

【００２９】

管理者は、デバイスＩＤを多機能機１０に入力しない。従って、管理者によってユーザＩＤ等の各情報が認証テーブルＡＴに登録される段階では、デバイスＩＤが認証テーブルＡＴに登録されない。ＣＰＵ３２は、例えば、携帯端末ＰＴ１，ＰＴ２とのＮＦＣ接続が確立される場合に、デバイスＩＤを生成して、当該デバイスＩＤを認証テーブルＡＴに登録する。また、ＣＰＵ３２は、例えば、認証カードＡＣとのＮＦＣ接続が確立される場合に、認証カードＡＣからデバイスＩＤを取得して、当該デバイスＩＤを認証テーブルＡＴに登録する。

【００３０】

（携帯端末ＰＴ１，ＰＴ２の構成）

各携帯端末ＰＴ１，ＰＴ２は、携帯電話（例えばスマートフォン）、ＰＤＡ（Personal Digital Assistantの略）、ノートＰＣ、タブレットＰＣ、携帯型音楽再生装置、携帯型動画再生装置等の可搬型のデバイスである。

【００３１】

携帯端末ＰＴ１の構成を説明する。携帯端末ＰＴ２は、携帯端末ＰＴ１と同様の構成を備える。携帯端末ＰＴ１は、操作部７２と、表示部７４と、ＮＦＣＩ／Ｆ８０と、ＬＡＮＩ／Ｆ８２と、制御部９０と、を備える。各部７２～９０は、バス線（符号省略）に接続されている。

【００３２】
操作部７２は、複数のキーを備える。ユーザは、操作部７２を操作することによって、様々な指示を携帯端末ＰＴ１に入力することができる。表示部７４は、様々な情報を表示するためのディスプレイである。ＮＦＣＩ／Ｆ８０、ＬＡＮＩ／Ｆ８２は、それぞれ、多機能機１０のＮＦＣＩ／Ｆ２０、ＬＡＮＩ／Ｆ２２とほぼ同様である。従って、携帯端末ＰＴ１は、ＮＦＣ通信とＷｉ－Ｆｉ通信とのそれぞれを実行可能である。ただし、ＮＦＣＩ／Ｆ８０は、Ｐ２Ｐモード及びＲ／Ｗモードのみならず、ＣＥ（Card Emulationの略）モードで動作可能である。
【００３３】
制御部９０は、ＣＰＵ９２とメモリ９４とを備える。ＣＰＵ９２は、メモリ９４に格納されている各プログラム９６，９８に従って、様々な処理を実行するプロセッサである。
【００３４】
ＯＳ（Operation Systemの略）プログラム９６は、携帯端末ＰＴ１の基本的な動作を実現するためのプログラムである。アプリケーション９８は、多機能機１０を利用するためのプログラムであり、より具体的には、携帯端末ＰＴ１が多機能機１０からデバイスＩＤを取得する処理と、携帯端末ＰＴ１を利用して多機能機１０にログインする処理と、を実現するためのプログラムである。アプリケーション９８は、多機能機１０のベンダによって提供されるアプリケーションであり、インターネット上のサーバから携帯端末ＰＴ１にインストールされてもよいし、多機能機１０と共に出荷されるメディアから携帯端末ＰＴ１にインストールされてもよい。
【００３５】
メモリ９４は、上記の各プログラム９６，９８の他に、デバイスＩＤを記憶可能である。デバイスＩＤは、多機能機１０から取得される情報である。従って、メモリ９４は、多機能機１０からデバイスＩＤが取得される前に、デバイスＩＤを記憶しておらず、多機能機１０からデバイスＩＤが取得された後に、デバイスＩＤを記憶する。
【００３６】
（認証カードＡＣの構成）
認証カードＡＣは、多機能機１０のベンダから通信システム２の管理者に与えられる可搬型のカードである。通信システム２の管理者は、認証カードＡＣをユーザに与えることができる。これにより、ユーザは、認証カードＡＣを利用して、多機能機１０にログインすることができる。
【００３７】
認証カードＡＣは、図示省略のＮＦＣＩ／Ｆを備えており、ＮＦＣ通信を実行可能である。認証カードＡＣのＮＦＣＩ／Ｆは、ＮＦＣ規格のカードとして機能するＩ／Ｆである。ＮＦＣ規格のカードは、上記のＣＥモードと同様の動作を実行し、Ｐ２Ｐモード及びＲ／Ｗモードの動作を実行不可能である。
【００３８】
また、認証カードＡＣは、図示省略のメモリを備えており、当該メモリは、複数個のアルファベット及び／又は数字の組み合わせであるデバイスＩＤ「Ｄ３」を予め記憶している。認証カードＡＣのデバイスＩＤ「Ｄ３」は、予め決められている文字数を有する。
【００３９】
（ＮＦＣ方式の接続；図２）
続いて、図２を参照して、多機能機１０のＮＦＣＩ／Ｆ２０とＮＦＣ機器のＮＦＣＩ／Ｆとの間に確立されるＮＦＣ方式の接続について説明する。図２の「ＮＦＣ機器」は、多機能機１０とのＮＦＣ接続を確立可能な機器であり、例えば、携帯端末ＰＴ１，ＰＴ２、認証カードＡＣ等である。
【００４０】
（ケース１）
ケース１は、多機能機１０のＮＦＣＩ／Ｆ２０がＰ２Ｐモード及びＲ／Ｗモードで動作しており、かつ、ＮＦＣ機器のＮＦＣＩ／ＦがＰ２Ｐモードのみで動作しているケースを

示す。多機能機１０のＮＦＣＩ／Ｆ２０は、Ｐｏｌｌ動作を実行し、次いで、Ｌｉｓｔｅｎ動作を実行するという１セットの動作を繰り返し実行する。また、Ｐ２Ｐモードのみで動作しているＮＦＣ機器も、上記の１セットの動作を繰り返し実行する。

【００４１】

Ｐｏｌｌ動作は、ポーリング信号を送信して、レスポンス信号を受信することを監視する動作である。Ｌｉｓｔｅｎ動作は、ポーリング信号を受信することを監視して、ポーリング信号を受信する場合に、レスポンス信号を送信する動作である。ケース１では、多機能機１０のＮＦＣＩ／Ｆ２０がＰｏｌｌ動作を実行する期間と、ＮＦＣ機器のＮＦＣＩ／ＦがＬｉｓｔｅｎ動作を実行する期間と、が一致する。この結果、多機能機１０は、ポーリング信号をＮＦＣ機器に送信して、ＮＦＣ機器からレスポンス信号を受信する。

【００４２】

多機能機１０は、ＮＦＣ機器からレスポンス信号を受信する場合に、ＮＦＣ機器がＰ２Ｐモードで動作しているのか否かを確認するためのＳＮＥＰ（Simple NDEF Exchange Protocolの略）コマンドをＮＦＣ機器に送信する。なお、ＮＤＥＦは、NFC Data Exchange Formatの略である。

【００４３】

ＮＦＣ機器は、Ｐ２Ｐモードで動作しているので、多機能機１０からＳＮＥＰコマンドを受信する場合に、ＯＫ信号を多機能機１０に送信する。

【００４４】

多機能機１０は、ＮＦＣ機器からＯＫ信号を受信する場合に、Ｐ２Ｐモード及びＲ／Ｗモードでのうちの Ｐ２Ｐモードで動作するための接続を確立すべきことを決定する。そして、多機能機１０は、ＡｃｔｉｖａｔｉｏｎコマンドをＮＦＣ機器に送信する。Ａｃｔｉｖａｔｉｏｎコマンドは、Ｐｏｌｌ動作を実行した機器からＬｉｓｔｅｎ動作を実行した機器に送信されるコマンドである。次いで、多機能機１０は、ＮＦＣ機器からＯＫ信号を受信する。これにより、多機能機１０のＮＦＣＩ／Ｆ２０とＮＦＣ機器のＮＦＣＩ／Ｆとの間に、それらのＮＦＣＩ／Ｆの双方がＰ２Ｐモードで動作するＰ２Ｐ接続が確立される。

【００４５】

多機能機１０及びＮＦＣ機器は、Ｐ２Ｐ接続を利用して、様々なデータの双方向通信を実行することができる。

【００４６】

（ケース２）

ケース２でも、ケース１と同様に、多機能機１０のＮＦＣＩ／Ｆ２０がＰ２Ｐモード及びＲ／Ｗモードで動作しており、かつ、ＮＦＣ機器のＮＦＣＩ／ＦがＰ２Ｐモードのみで動作している。ケース２では、多機能機１０のＮＦＣＩ／Ｆ２０がＬｉｓｔｅｎ動作を実行する期間と、ＮＦＣ機器のＮＦＣＩ／ＦがＰｏｌｌ動作を実行する期間と、が一致する。この結果、多機能機１０は、ＮＦＣ機器からポーリング信号を受信して、レスポンス信号をＮＦＣ機器に送信する。

【００４７】

次いで、多機能機１０は、ＮＦＣ機器からＳＮＥＰコマンドを受信する。これにより、多機能機１０は、ＮＦＣ機器がＰ２Ｐモードで動作していることを知ることができ、ＯＫ信号をＮＦＣ機器に送信する。そして、多機能機１０は、Ｐ２Ｐモード及びＲ／Ｗモードのうちの Ｐ２Ｐモードで動作するための接続を確立すべきことを決定する。多機能機１０は、ＮＦＣ機器からＡｃｔｉｖａｔｉｏｎコマンドを受信して、ＯＫ信号をＮＦＣ機器に送信する。これにより、多機能機１０のＮＦＣＩ／Ｆ２０とＮＦＣ機器のＮＦＣＩ／Ｆとの間に、Ｐ２Ｐ接続が確立される。

【００４８】

（ケース３）

ケース３は、多機能機１０のＮＦＣＩ／Ｆ２０がＰ２Ｐモード及びＲ／Ｗモードで動作しており、かつ、ＮＦＣ機器のＮＦＣＩ／ＦがＣＥモードのみで動作しているケースを示

す。ＣＥモードのみで動作しているＮＦＣ機器は、Ｐｏｌｌ動作を実行せずに、Ｌｉｓｔｅｎ動作のみを実行する。従って、多機能機１０は、ポーリング信号をＮＦＣ機器に送信して、ＮＦＣ機器からレスポンス信号を受信する。

【００４９】

多機能機１０は、ＮＦＣ機器からレスポンス信号を受信する場合に、ＳＮＥＰコマンドをＮＦＣ機器に送信する。ＮＦＣ機器は、Ｐ２Ｐモードで動作していないので（即ちＣＥモードのみで動作しているので）、多機能機１０からＳＮＥＰコマンドを受信しても、ＯＫ信号を多機能機１０に送信しない。

【００５０】

多機能機１０は、ＮＦＣ機器からＯＫ信号を受信しない場合に、Ｐ２Ｐモード及びＲ／ＷモードのうちのＲ／Ｗモードで動作するための接続を確立すべきことを決定する。そして、多機能機１０は、ＡｃｔｉｖａｔｉｏｎコマンドをＮＦＣ機器に送信して、ＮＦＣ機器からＯＫ信号を受信する。これにより、多機能機１０のＮＦＣＩ／Ｆ２０とＮＦＣ機器のＮＦＣＩ／Ｆとの間に、Ｒ／Ｗ－ＣＥ接続が確立される。Ｒ／Ｗ－ＣＥ接続は、多機能機１０のＮＦＣＩ／Ｆ２０がＲ／Ｗモードで動作すると共に、ＮＦＣ機器のＮＦＣＩ／ＦがＣＥモードで動作する接続である。

【００５１】

例えば、多機能機１０のＮＦＣＩ／Ｆ２０がＲ／ＷモードのうちのＲｅａｄｅｒとして動作する場合には、多機能機１０は、Ｒ／Ｗ－ＣＥ接続を利用して、ＮＦＣ機器からデータを読み出すことができる（即ちデータを取得することができる）。また、例えば、多機能機１０のＮＦＣＩ／Ｆ２０がＲ／ＷモードのうちのＷｒｉｔｅｒとして動作する場合には、多機能機１０は、Ｒ／Ｗ－ＣＥ接続を利用して、ＮＦＣ機器にデータを書き込むことができる（即ちデータを供給することができる）。

【００５２】

上記のケース１～ケース３に示されるように、多機能機１０は、通信相手のＮＦＣ機器の動作に応じて、Ｐ２Ｐ接続を確立すべきか、Ｒ／Ｗ－ＣＥ接続を確立すべきか、を決定することができる。

【００５３】

（多機能機１０のログイン管理処理；図３）

続いて、図３を参照して、多機能機１０のＣＰＵ３２が実行するログイン管理処理を実行する。ログイン管理処理では、ＣＰＵ３２は、Ｓ１０、Ｓ２０、及び、Ｓ４０の各監視処理を繰り返し実行する。

【００５４】

Ｓ１０では、ＣＰＵ３２は、ユーザＩＤ及びパスワードを入力するための操作が操作部１２に実行されることを監視している。ＣＰＵ３２は、当該操作が実行される場合に、Ｓ１０でＹＥＳと判断して、Ｓ１２に進む。以下では、Ｓ１０で入力されたユーザＩＤのことを「対象ユーザＩＤ」と呼び、Ｓ１０で入力されたユーザＩＤ及びパスワードのセットのことを「対象セット」と呼び、対象セットを入力したユーザのことを「対象ユーザ」と呼ぶ。

【００５５】

Ｓ１２では、ＣＰＵ３２は、対象セットの認証を実行して、当該認証が成功したのか否かを判断する。ＣＰＵ３２は、対象セットが認証テーブルＡＴに登録されていないと判断する場合（Ｓ１２でＮＯ）には、Ｓ１３に進む。

【００５６】

Ｓ１３では、ＣＰＵ３２は、多機能機１０の状態を非ログイン状態に維持したまま、認証失敗を示すエラーメッセージを表示部１４に表示させる。Ｓ１３が終了すると、Ｓ１０に戻る。

【００５７】

また、Ｓ１２において、ＣＰＵ３２は、対象セットが認証テーブルＡＴに登録済みであると判断する場合（Ｓ１２でＹＥＳ）には、Ｓ１４に進む。

【００５８】
Ｓ１４では、ＣＰＵ３２は、多機能機１０の状態を、非ログイン状態から、対象ユーザＩＤに対応するログイン状態へ移行させる。非ログイン状態は、コピー機能及び／又はスキャン機能の実行を、対象ユーザを含むいずれのユーザにも許可しない状態である。また、対象ユーザＩＤに対応するログイン状態は、対象ユーザＩＤに関連付けられているコピー許可情報及び／又はスキャン許可情報が「ＯＫ」を示すことを条件として、コピー機能及び／又はスキャン機能の実行を、対象ユーザに許可する状態である。Ｓ１４が終了すると、Ｓ１０に戻る。
【００５９】
Ｓ２０では、ＣＰＵ３２は、コピー機能又はスキャン機能の実行を指示するための操作（以下では「機能実行操作」と呼ぶ）が操作部１２に実行されることを監視している。ＣＰＵ３２は、機能実行操作が実行される場合に、Ｓ２０でＹＥＳと判断して、Ｓ２２に進む。以下では、機能実行操作で指示された機能のことを「指定機能」と呼ぶ。
【００６０】
Ｓ２２では、ＣＰＵ３２は、多機能機１０の状態が、いずれかのユーザＩＤに対応するログイン状態であるのか否かを判断する。ＣＰＵ３２は、多機能機１０の状態が非ログイン状態であると判断する場合（Ｓ２２でＮＯ）には、Ｓ２３に進む。
【００６１】
Ｓ２３では、ＣＰＵ３２は、多機能機１０の状態を非ログイン状態に維持したまま、非ログイン状態であることに起因して、指定機能を実行不可能であることを示すエラーメッセージを、表示部１４に表示させる。Ｓ２３が終了すると、Ｓ１０に戻る。
【００６２】
また、Ｓ２２において、ＣＰＵ３２は、多機能機１０の状態がログイン状態であると判断する場合（Ｓ２２でＹＥＳ）には、Ｓ２６に進む。以下では、Ｓ２２でＹＥＳと判断されたユーザＩＤ（即ち多機能機１０にログインしているユーザＩＤ）のことを「対象ユーザＩＤ」と呼ぶ。
【００６３】
Ｓ２６では、ＣＰＵ３２は、指定機能を実行可能であるのか否かを判断する。具体的には、ＣＰＵ３２は、認証テーブルＡＴから、対象ユーザＩＤに関連付けられている指定機能（例えばコピー）の許可情報（例えばコピー許可情報）を取得する。そして、ＣＰＵ３２は、対象ユーザＩＤに関連付けられている指定機能の許可情報が「ＮＧ」を示すと判断する場合（Ｓ２６でＮＯ）には、Ｓ２７に進む。
【００６４】
Ｓ２７では、ＣＰＵ３２は、許可情報が「ＮＧ」を示すことに起因して、指定機能を実行不可能であることを示すエラーメッセージを、表示部１４に表示させる。Ｓ２７が終了すると、Ｓ３２に進む。
【００６５】
また、Ｓ２６において、ＣＰＵ３２は、対象ユーザＩＤに関連付けられている指定機能の許可情報が「ＯＫ」を示すと判断する場合（Ｓ２６でＹＥＳ）には、Ｓ２８に進む。
【００６６】
Ｓ２８では、ＣＰＵ３２は、指定機能を実行する。例えば、指定機能がコピー機能である場合には、ＣＰＵ３２は、原稿のスキャンをスキャン実行部１８に実行させる。次いで、ＣＰＵ３２は、スキャンデータを印刷実行部１６に供給する。これにより、印刷実行部１６は、スキャンデータによって表わされる画像を印刷媒体に印刷する。また、例えば、指定機能がスキャン機能である場合には、ＣＰＵ３２は、原稿のスキャンをスキャン実行部１８に実行させる。次いで、ＣＰＵ３２は、認証テーブルＡＴから、対象ユーザＩＤに関連付けられている送信先情報（例えば「ＩＰ１」）を取得する。次いで、ＣＰＵ３２は、取得済みの送信先情報を利用して、ＬＡＮＩ／Ｆ２２を介して、スキャンデータを送信する。Ｓ２８が終了すると、Ｓ３２に進む。
【００６７】

Ｓ３２では、ＣＰＵ３２は、多機能機１０の状態を、対象ユーザＩＤに対応するログイン状態から非ログイン状態へ移行させる。Ｓ３２が終了すると、Ｓ１０に戻る。

【００６８】

Ｓ４０では、ＣＰＵ３２は、ＮＦＣＩ／Ｆ２０を介したＮＦＣ接続が確立されることを監視している。ＣＰＵ３２は、ＮＦＣ機器からＡｃｔｉｖａｔｉｏｎ信号に対するＯＫ信号を受信する場合（図２のケース１又はケース３）、又は、Ａｃｔｉｖａｔｉｏｎ信号に対するＯＫ信号をＮＦＣ機器に送信する場合（図２のケース２）に、Ｓ４０でＹＥＳと判断して、図４のＳ５０に進む。以下では、多機能機１０とのＮＦＣ接続が確立されたＮＦＣ機器のことを「対象機器」と呼ぶ。

【００６９】

（ログイン管理処理の続き；図４）

Ｓ５０では、ＣＰＵ３２は、確立済みのＮＦＣ接続が、Ｐ２Ｐ接続であるのか、Ｒ／Ｗ－ＣＥ接続であるのかを判断する。ＣＰＵ３２は、ＮＦＣ接続が確立される過程で、Ｐ２Ｐ接続を確立すべきことを決定した場合（即ち図２のケース１又はケース２）には、確立済みのＮＦＣ接続がＰ２Ｐ接続であると判断して（Ｓ５０でＹＥＳ）、Ｓ５２～Ｓ６４の各処理を実行すべきことを決定する。

【００７０】

Ｓ５２では、ＣＰＵ３２は、多機能機１０の状態が、いずれかのユーザＩＤに対応するログイン状態であるのか否かを判断する。ＣＰＵ３２は、多機能機１０の状態が非ログイン状態であると判断する場合（Ｓ５２でＮＯ）には、Ｓ５３に進む。

【００７１】

Ｓ５３では、ＣＰＵ３２は、多機能機１０の状態を非ログイン状態に維持したまま、非ログイン状態であることに起因して、以降の処理を実行不可能であることを示すエラーメッセージを、表示部１４に表示させる。Ｓ５３が終了すると、図３のＳ１０に戻る。

【００７２】

また、Ｓ５２において、ＣＰＵ３２は、多機能機１０の状態がログイン状態であると判断する場合（Ｓ５２でＹＥＳ）には、Ｓ５６に進む。以下では、Ｓ５２でＹＥＳと判断されたユーザＩＤ（即ち多機能機１０にログインしているユーザＩＤ）のことを「対象ユーザＩＤ」と呼ぶ。

【００７３】

Ｓ５６では、ＣＰＵ３２は、ＮＦＣＩ／Ｆ２０を介して（即ちＰ２Ｐ接続を利用して）、対象機器からアプリＩＤを取得したのか否かを判断する。アプリＩＤは、対象機器でアプリケーション９８（図１参照）が起動中である場合に、対象機器から多機能機１０に供給される。ＣＰＵ３２は、対象機器からアプリＩＤを取得しなかったと判断する場合（Ｓ５６でＮＯ）には、Ｓ５７に進む。

【００７４】

Ｓ５７では、ＣＰＵ３２は、アプリＩＤが取得されないことに起因して、以降の処理を実行不可能であることを示すエラーメッセージを、表示部１４に表示させる。Ｓ５７が終了すると、Ｓ６４に進む。

【００７５】

また、Ｓ５６において、ＣＰＵ３２は、対象機器からアプリＩＤを取得したと判断する場合（Ｓ５６でＹＥＳ）には、Ｓ６０に進む。

【００７６】

Ｓ６０では、ＣＰＵ３２は、デバイスＩＤを新たに生成する。具体的には、ＣＰＵ３２は、アルファベット及び／又は数字をランダムに選択して、予め決められている文字数を有するデバイスＩＤを生成する。当該文字数は、認証カードＡＣのデバイスＩＤ「Ｄ３」（図１参照）の文字数に一致する。ＣＰＵ３２は、生成済みのデバイスＩＤが、認証テーブルＡＴに現在登録されているいずれかのデバイスＩＤに一致する場合には、デバイスＩＤを再び生成する。これにより、ＣＰＵ３２は、認証テーブルＡＴに現在登録されていないユニークなデバイスＩＤを生成することができる。そして、ＣＰＵ３２は、対象ユーザ

ＩＤに関連付けて、生成済みのデバイスＩＤを認証テーブルＡＴに登録する。
【００７７】
なお、Ｓ６０の処理を開始する際に、対象ユーザＩＤに関連付けられているデバイスＩＤが認証テーブルＡＴに既に登録されている場合には、Ｓ６０では、ＣＰＵ３２は、認証テーブルＡＴから登録済みのデバイスＩＤを削除した後に、対象ユーザＩＤに関連付けて、生成済みのデバイスＩＤを登録する。即ち、ＣＰＵ３２は、対象ユーザＩＤに関連付けて、登録済みのデバイスＩＤに代えて、生成済みのデバイスＩＤを登録する。
【００７８】
上述したように、本実施例によると、多機能機１０は、対象機器からアプリＩＤを取得する場合（Ｓ５６でＹＥＳ）には、対象ユーザＩＤに関連付けてデバイスＩＤを認証テーブルＡＴに登録し（Ｓ６０）、対象機器からアプリＩＤを取得しない場合（Ｓ５６でＮＯ）には、対象ユーザＩＤに関連付けてデバイスＩＤを登録しない（Ｓ５７）。従って、多機能機１０は、多機能機１０を利用するためのアプリケーション９８が対象機器で起動中でない場合、即ち、デバイスＩＤの登録が目的ではない状況で、対象機器とのＰ２Ｐ接続が確立される場合に、デバイスＩＤを認証テーブルＡＴに登録せずに済む。
【００７９】
次いで、Ｓ６２では、ＣＰＵ３２は、ＮＦＣＩ／Ｆ２０を介して（即ちＰ２Ｐ接続を利用して）、生成済みのデバイスＩＤを対象機器に供給する。これにより、ＣＰＵ３２は、生成済みのデバイスＩＤを対象機器に割り当てることができる。上述したように、ＣＰＵ３２は、認証カードＡＣのデバイスＩＤ「Ｄ３」の文字数に一致する文字数を有するデバイスＩＤを対象機器に割り当てる。従って、ＣＰＵ３２は、デバイスＩＤを対象機器に割り当てることによって、対象機器（例えば携帯端末ＰＴ１）を認証カードとして機能させることができる。
【００８０】
次いで、Ｓ６４では、ＣＰＵ３２は、多機能機１０の状態を、対象ユーザＩＤに対応するログイン状態から非ログイン状態へ移行させる。Ｓ６４が終了すると、Ｓ１０に戻る。
【００８１】
一方、ＣＰＵ３２は、ＮＦＣ接続が確立される過程で、Ｒ／Ｗ－ＣＥ接続を確立すべきことを決定した場合（即ち図２のケース３）には、確立済みのＮＦＣ接続がＲ／Ｗ－ＣＥ接続であると判断して（Ｓ５０でＮＯ）、Ｓ７０～Ｓ８０の各処理を実行すべきことを決定する。
【００８２】
Ｓ７０では、ＣＰＵ３２は、ＮＦＣＩ／Ｆ２０を介して（即ちＲ／Ｗ－ＣＥ接続を利用して）、対象機器からデバイスＩＤを取得する。以下では、Ｓ７０で取得されたデバイスＩＤのことを「対象デバイスＩＤ」と呼ぶ。
【００８３】
次いで、Ｓ７２では、ＣＰＵ３２は、多機能機１０の状態が、いずれかのユーザＩＤに対応するログイン状態であるのか否かを判断する。ＣＰＵ３２は、多機能機１０の状態がログイン状態であると判断する場合（Ｓ７２でＹＥＳ）には、Ｓ７４に進む。以下では、Ｓ７２でＹＥＳと判断されたユーザＩＤ（即ち多機能機１０にログインしているユーザＩＤ）のことを「対象ユーザＩＤ」と呼ぶ。
【００８４】
Ｓ７４では、ＣＰＵ３２は、対象ユーザＩＤに関連付けて、対象デバイスＩＤを認証テーブルＡＴに登録する。
【００８５】
次いで、Ｓ７６では、ＣＰＵ３２は、多機能機１０の状態を、対象ユーザＩＤに対応するログイン状態から非ログイン状態へ移行させる。Ｓ７６が終了すると、Ｓ１０に戻る。
【００８６】
一方、Ｓ７２において、ＣＰＵ３２は、多機能機１０の状態が非ログイン状態であると判断する場合（Ｓ７２でＮＯ）には、Ｓ７８に進む。

【００８７】
Ｓ７８では、ＣＰＵ３２は、対象デバイスＩＤの認証を実行して、当該認証が成功したのか否かを判断する。ＣＰＵ３２は、対象デバイスＩＤが認証テーブルＡＴに登録されていないと判断する場合（Ｓ７８でＮＯ）には、Ｓ７９に進む。
【００８８】
Ｓ７９では、ＣＰＵ３２は、多機能機１０の状態を非ログイン状態に維持したまま、認証失敗を示すエラーメッセージを表示部１４に表示させる。Ｓ７９が終了すると、Ｓ１０に戻る。
【００８９】
また、Ｓ７８において、ＣＰＵ３２は、対象デバイスＩＤが認証テーブルＡＴに登録済みであると判断する場合（Ｓ７８でＹＥＳ）には、Ｓ８０に進む。
【００９０】
Ｓ８０では、ＣＰＵ３２は、多機能機１０の状態を、非ログイン状態から、対象デバイスＩＤに関連付けられているユーザＩＤに対応するログイン状態へ移行させる。Ｓ８０が終了すると、Ｓ１０に戻る。
【００９１】
（携帯端末ＰＴ１のアプリケーション処理；図５）
続いて、図５を参照して、携帯端末ＰＴ１のＣＰＵ９２が実行するアプリケーション処理を実行する。携帯端末ＰＴ２は、携帯端末ＰＴ１と同様に、図５の処理を実行する。
【００９２】
携帯端末ＰＴ１のユーザは、多機能機１０から割り当てられるデバイスＩＤ（図４のＳ６２参照）を携帯端末ＰＴ１に記憶させることを望む場合に、操作部７２を操作して、アプリケーション９８を起動させる。また、ユーザは、携帯端末ＰＴ１にデバイスＩＤが記憶されている状態で、携帯端末ＰＴ１を利用して多機能機１０にログインすることを望む場合にも、操作部７２を操作して、アプリケーション９８を起動させる。携帯端末ＰＴ１のＣＰＵ９２は、アプリケーション９８が起動されることをトリガとして、アプリケーション９８に従って、図５の処理を実行する。
【００９３】
Ｓ１００では、ＣＰＵ９２は、デバイスＩＤがメモリ９４に記憶済みであるのか否かを判断する。ＣＰＵ９２は、デバイスＩＤがメモリ９４に記憶済みでないと判断する場合（Ｓ１００でＮＯ）には、Ｓ１０２に進み、デバイスＩＤがメモリ９４に記憶済みであると判断する場合（Ｓ１００でＹＥＳ）には、Ｓ１２０に進む。
【００９４】
Ｓ１０２では、ＣＰＵ９２は、Ｐ２Ｐモードのみで動作するように、ＮＦＣＩ／Ｆ８０に指示を供給する。これにより、ＮＦＣＩ／Ｆ８０は、Ｒ／Ｗモード及びＣＥモードで動作せずに、Ｐ２Ｐモードで動作する。
【００９５】
次いで、Ｓ１０４では、ＣＰＵ９２は、多機能機１０にログインすることをユーザに促すメッセージと、多機能機１０にログインした後に、携帯端末ＰＴ１を多機能機１０に近づけることをユーザに促すメッセージと、を表示部７４に表示させる。これにより、ユーザは、ユーザＩＤ及びパスワードを多機能機１０に入力して、多機能機１０にログインする（図３のＳ１０でＹＥＳ、Ｓ１２でＹＥＳ、Ｓ１４参照）。その後、ユーザは、携帯端末ＰＴ１を多機能機１０に近づける。これにより、携帯端末ＰＴ１のＮＦＣＩ／Ｆ８０と多機能機１０のＮＦＣＩ／Ｆ２０との間の距離が、ＮＦＣ通信を実行可能な距離（例えば１０ｃｍ）未満になり、この結果、これらのＮＦＣＩ／Ｆ８０，２０の間にＮＦＣ接続が確立される。
【００９６】
ＣＰＵ９２は、ＮＦＣ接続が確立される場合に、Ｓ１０６でＹＥＳと判断して、Ｓ１０８に進む。携帯端末ＰＴ１のＮＦＣＩ／Ｆ８０がＰ２Ｐモードのみで動作しているので（Ｓ１０２参照）、図２のケース１又はケース２に示されるように、Ｐ２Ｐ接続が確立され

る。
【００９７】
Ｓ１０８では、ＣＰＵ９２は、ＮＦＣＩ／Ｆ８０を介して（即ちＰ２Ｐ接続を利用して）、多機能機１０からデバイスＩＤを取得する（図４のＳ６２参照）。
【００９８】
次いで、Ｓ１１０では、ＣＰＵ９２は、取得済みのデバイスＩＤをメモリ９４に記憶させる。これにより、携帯端末ＰＴ１を利用した多機能機１０へのログインを実現することができる状態になる。Ｓ１１０が終了すると、図５の処理が終了する。
【００９９】
一方、Ｓ１２０（即ちデバイスＩＤが記憶済みである場合）では、ＣＰＵ９２は、ＣＥモードのみで動作するように、ＮＦＣＩ／Ｆ８０に指示を供給する。これにより、ＮＦＣＩ／Ｆ８０は、Ｐ２Ｐモード及びＲ／Ｗモードで動作せずに、ＣＥモードで動作する。
【０１００】
次いで、Ｓ１２２では、ＣＰＵ９２は、携帯端末ＰＴ１を多機能機１０に近づけることをユーザに促すメッセージを表示部７４に表示させる。これにより、ユーザは、携帯端末ＰＴ１を多機能機１０に近づける。この結果、携帯端末ＰＴ１のＮＦＣＩ／Ｆ８０と多機能機１０のＮＦＣＩ／Ｆ２０との間にＮＦＣ接続が確立される。
【０１０１】
ＣＰＵ９２は、ＮＦＣ接続が確立される場合に、Ｓ１２４でＹＥＳと判断して、Ｓ１２６に進む。携帯端末ＰＴ１のＮＦＣＩ／Ｆ８０がＣＥモードのみで動作しているので（Ｓ１２０参照）、図２のケース３に示されるように、Ｒ／Ｗ－ＣＥ接続が確立される。
【０１０２】
Ｓ１２６では、ＣＰＵ９２は、ＮＦＣＩ／Ｆ８０を介して（即ちＲ／Ｗ－ＣＥ接続を利用して）、メモリ９４内のデバイスＩＤを多機能機１０に供給する（図４のＳ７０参照）。これにより、多機能機１０へのログインが実現される（図４のＳ８０参照）。Ｓ１２６が終了すると、図５の処理が終了する。
【０１０３】
（ケースＡ；図６）
続いて、図３～図５のフローチャートに従って実現される具体的なケースを説明する。まず、図６を参照して、多機能機１０及び携帯端末ＰＴ１によって実現されるケースＡを説明する。
【０１０４】
図６のケースＡの初期状態では、多機能機１０の認証テーブルＡＴには、図１に示されるように、ユーザＩＤ「Ｕ１」、パスワード「Ｐ１」、コピー「ＯＫ」、及び、スキャン「ＮＧ」を含む組合せ情報が登録されている。ただし、認証テーブルＡＴでは、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」に関連付けて、デバイスＩＤが登録されていない。また、携帯端末ＰＴ１のメモリ９４には、デバイスＩＤが記憶されていない。
【０１０５】
通信システム２の管理者は、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」を携帯端末ＰＴ１のユーザ（以下では「第１のユーザ」と呼ぶ）に通知済みである。従って、Ｔ１０では、第１のユーザは、多機能機１０の操作部１２を操作して、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」のセットを入力することができる（図３のＳ１０でＹＥＳ）。この場合、Ｔ１２では、多機能機１０は、入力済みのセットが認証テーブルＡＴに登録済みであると判断し（Ｓ１２でＹＥＳ）、ユーザＩＤ「Ｕ１」に対応するログイン状態へ移行する（Ｓ１４）。
【０１０６】
Ｔ１４では、第１のユーザは、コピー機能のための機能実行操作を多機能機１０の操作部１２に実行する（図３のＳ２０でＹＥＳ）。この場合、Ｔ１６では、多機能機１０は、ユーザＩＤ「Ｕ１」に対応するログイン状態であると判断し（Ｓ２２でＹＥＳ）、ユーザＩＤ「Ｕ１」に関連付けられているコピー許可情報が「ＯＫ」であると判断し（Ｓ２６で

ＹＥＳ）、コピー機能を実行する（Ｓ２８）。そして、Ｔ１８では、多機能機１０は、非ログイン状態へ移行する（Ｓ３２）。

【０１０７】

第１のユーザは、多機能機１０から割り当てられるデバイスＩＤを携帯端末ＰＴ１に記憶させることを望んでいる。従って、Ｔ２０では、第１のユーザは、携帯端末ＰＴ１の操作部７２を操作して、アプリケーション９８を起動させる（図５の処理のトリガ）。この場合、Ｔ２２では、携帯端末ＰＴ１は、ＮＦＣＩ／Ｆ８０をＰ２Ｐモードのみで動作させる（Ｓ１００でＮＯ、Ｓ１０２）。そして、Ｔ２４では、携帯端末ＰＴ１は、多機能機１０にログインすることをユーザに促すメッセージと、携帯端末ＰＴ１を多機能機１０に近づけることをユーザに促すメッセージと、を表示する（Ｓ１０４）。

【０１０８】

Ｔ３０では、第１のユーザは、多機能機１０の操作部１２を操作して、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」のセットを入力する（図３のＳ１０でＹＥＳ）。この場合、Ｔ３２では、多機能機１０は、入力済みのセットが認証テーブルＡＴに登録済みであると判断し（Ｓ１２でＹＥＳ）、ユーザＩＤ「Ｕ１」に対応するログイン状態へ移行する（Ｓ１４）。

【０１０９】

Ｔ３４では、第１のユーザが携帯端末ＰＴ１を多機能機１０に近づけることに起因して、多機能機１０と携帯端末ＰＴ１との間にＰ２Ｐ接続が確立される（図３のＳ４０でＹＥＳ、図４のＳ５０でＹＥＳ、図５のＳ１０６でＹＥＳ）。この場合、Ｔ３６では、多機能機１０は、デバイスＩＤ「Ｄ１」を新たに生成して、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」に関連付けて、デバイスＩＤ「Ｄ１」を認証テーブルＡＴに登録する（図４のＳ６０）。そして、Ｔ３８では、多機能機１０は、デバイスＩＤ「Ｄ１」を携帯端末ＰＴ１に供給する（Ｓ６２）。次いで、Ｔ４０では、多機能機１０は、非ログイン状態へ移行する（Ｓ６４）。

【０１１０】

Ｔ３８では、携帯端末ＰＴ１は、多機能機１０からデバイスＩＤ「Ｄ１」を取得する（図５のＳ１０８）。そして、Ｔ５０では、携帯端末ＰＴ１は、デバイスＩＤ「Ｄ１」を記憶する（Ｓ１１０）。

【０１１１】

第１のユーザは、携帯端末ＰＴ１がデバイスＩＤ「Ｄ１」を記憶した後に、携帯端末ＰＴ１を利用して多機能機１０にログインすることを望んでいる。従って、Ｔ６０では、第１のユーザは、携帯端末ＰＴ１の操作部７２を操作して、アプリケーション９８を起動させる（図５の処理のトリガ）。この場合、Ｔ６２では、携帯端末ＰＴ１は、ＮＦＣＩ／Ｆ８０をＣＥモードのみで動作させる（Ｓ１００でＹＥＳ、Ｓ１２０）。そして、Ｔ６４では、携帯端末ＰＴ１は、携帯端末ＰＴ１を多機能機１０に近づけることをユーザに促すメッセージを表示する（Ｓ１２２）。

【０１１２】

Ｔ６６では、第１のユーザが携帯端末ＰＴ１を多機能機１０に近づけることに起因して、多機能機１０と携帯端末ＰＴ１との間にＲ／Ｗ－ＣＥ接続が確立される（図３のＳ４０でＹＥＳ、図４のＳ５０でＮＯ、図５のＳ１２４でＹＥＳ）。この場合、Ｔ６８では、携帯端末ＰＴ１は、デバイスＩＤ「Ｄ１」を多機能機１０に供給する（Ｓ１２６）。

【０１１３】

Ｔ６８では、多機能機１０は、携帯端末ＰＴ１からデバイスＩＤ「Ｄ１」を取得する（図４のＳ７０）。そして、Ｔ７２では、多機能機１０は、非ログイン状態であると判断し（Ｓ７２でＮＯ）、デバイスＩＤ「Ｄ１」が認証テーブルＡＴに登録済みであると判断し（Ｓ７８でＹＥＳ）、デバイスＩＤ「Ｄ１」に関連付けられているユーザＩＤ「Ｕ１」に対応するログイン状態へ移行する（Ｓ８０）。

【０１１４】

Ｔ７４では、第１のユーザは、コピー機能のための機能実行操作を多機能機１０の操作

部１２に実行する（図３のＳ２０でＹＥＳ）。この場合、Ｔ７６では、多機能機１０は、ユーザＩＤ「Ｕ１」に対応するログイン状態であると判断し（Ｓ２２でＹＥＳ）、ユーザＩＤ「Ｕ１」に関連付けられているコピー許可情報が「ＯＫ」であると判断し（Ｓ２６でＹＥＳ）、コピー機能を実行する（Ｓ２８）。そして、Ｔ７８では、多機能機１０は、非ログイン状態へ移行する（Ｓ３２）。

【０１１５】

（ケースＡの効果）

上述したように、多機能機１０は、第１のユーザによって操作部１２が操作されて、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」が多機能機１０に入力される場合（Ｔ１０）に、多機能機１０の状態をユーザＩＤ「Ｕ１」に対応するログイン状態へ移行させる（Ｔ１２）。このために、第１のユーザは、多機能機１０にコピー機能を実行させることができる（Ｔ１４、Ｔ１６）。また、多機能機１０は、多機能機１０の状態がユーザＩＤ「Ｕ１」に対応するログイン状態である間に、携帯端末ＰＴ１とのＰ２Ｐ接続が確立される場合（Ｔ３４）に、デバイスＩＤ「Ｄ１」を生成して、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」に関連付けて、デバイスＩＤ「Ｄ１」を認証テーブルＡＴに登録する（Ｔ３６）。そして、多機能機１０は、デバイスＩＤ「Ｄ１」を携帯端末ＰＴ１に供給する（Ｔ３８）。このように、多機能機１０は、デバイスＩＤが携帯端末ＰＴ１に予め記憶されていなくても、携帯端末ＰＴ１が認証カードとして機能するように、デバイスＩＤ「Ｄ１」を携帯端末ＰＴ１に割り当てることができる。即ち、携帯端末ＰＴ１は、多機能機１０からデバイスＩＤ「Ｄ１」を取得して（Ｔ３８）、デバイスＩＤ「Ｄ１」を記憶することができる（Ｔ５０）。これにより、携帯端末ＰＴ１は、認証カードとして機能することができ、デバイスＩＤ「Ｄ１」を多機能機１０に供給して（Ｔ６８）、多機能機１０の状態をユーザＩＤ「Ｄ１」に対応するログイン状態へ移行させることができる（Ｔ７２）。換言すると、多機能機１０は、携帯端末ＰＴ１からデバイスＩＤ「Ｄ１」を取得する場合（Ｔ６８）に、多機能機１０の状態をユーザＩＤ「Ｄ１」に対応するログイン状態へ移行させることができる（Ｔ７２）。このために、第１のユーザは、多機能機１０にコピー機能を実行させることができる（Ｔ７４、Ｔ７６）。本実施例によると、第１のユーザは、デバイスＩＤを予め記憶していない携帯端末ＰＴ１を利用して、所望の機能を多機能機１０に実行させることができる。

【０１１６】

また、上述したように、認証カードＡＣのＮＦＣＩ／Ｆ（図示省略）は、ＮＦＣ規格のカード（即ちＣＥモードと同様）として動作する。そして、多機能機１０は、認証カードＡＣとのＲ／Ｗ－ＣＥ接続を利用して、認証カードＡＣからデバイスＩＤを取得する場合（図４のＳ７０）に、認証処理を実行する（Ｓ７８）。このような認証カードＡＣの動作に合わせて、携帯端末ＰＴ１は、デバイスＩＤ「Ｄ１」がメモリ９４に記憶されている場合、即ち、携帯端末ＰＴ１が認証カードとして機能すべき場合には、ＮＦＣＩ／Ｆ８０をＣＥモードのみで動作させる（図６のＴ６２）。この結果、多機能機１０は、携帯端末ＰＴ１とのＲ／Ｗ－ＣＥ接続を利用して、携帯端末ＰＴ１からデバイスＩＤ「Ｄ１」を取得する場合（Ｔ６８、図４のＳ７０）に、認証処理を実行する（Ｔ７２、図４のＳ７８）。即ち、本実施例によると、認証カードＡＣのＮＦＣＩ／Ｆの動作と、認証カードとして機能すべき携帯端末ＰＴ１のＮＦＣＩ／Ｆ８０の動作と、が一致するので、多機能機１０は、認証カードＡＣ及び携帯端末ＰＴ１のいずれとのＲ／Ｗ－ＣＥ接続が確立されても、認証処理を適切に実行することができる。

【０１１７】

また、携帯端末ＰＴ１は、デバイスＩＤ「Ｄ１」がメモリ９４に記憶されていない場合、即ち、多機能機１０からデバイスＩＤ「Ｄ１」を取得すべき場合には、ＮＦＣＩ／Ｆ８０をＰ２Ｐモードのみで動作させる（Ｔ２２）。この結果、多機能機１０は、携帯端末ＰＴ１とのＰ２Ｐ接続が確立される場合（Ｔ３４）には、デバイスＩＤ「Ｄ１」の生成及び登録を実行し（Ｔ３６）、デバイスＩＤ「Ｄ１」を携帯端末ＰＴ１に供給する（Ｔ３８）。このように、本実施例によると、多機能機１０は、多機能機１０と携帯端末ＰＴ１との

間に確立される接続の種類（即ちＰ２Ｐ接続又はＲ／Ｗ－ＣＥ接続）に応じて、適切な処理を実行することができる。

【０１１８】

（ケースＢ；図７）

続いて、図７を参照して、多機能機１０が携帯端末ＰＴ１にデバイスＩＤ「Ｄ１」を割り当てた後に、多機能機１０及び携帯端末ＰＴ２によって実現されるケースＢを説明する。多機能機１０の認証テーブルＡＴには、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」に関連付けて、デバイスＩＤ「Ｄ１」が登録されている。

【０１１９】

第１のユーザは、携帯端末ＰＴ１に代えて、携帯端末ＰＴ２を利用して、多機能機１０にログインすることを望んでいる。この場合、Ｔ１２０では、第１のユーザは、携帯端末ＰＴ２の操作部（図示省略）を操作して、アプリケーション（即ち図１のアプリケーション９８と同一のアプリケーション）を起動させる（図５の処理のトリガ）。この後のＴ１２２～Ｔ１３４は、携帯端末ＰＴ１ではなく携帯端末ＰＴ２が利用される点を除くと、図６のＴ２２～Ｔ３４と同様である。

【０１２０】

Ｔ１３６では、多機能機１０は、デバイスＩＤ「Ｄ２」を新たに生成して、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」に関連付けて、デバイスＩＤ「Ｄ１」に代えて、デバイスＩＤ「Ｄ２」を認証テーブルＡＴに登録する（図４のＳ６０）。これにより、認証テーブルＡＴでは、携帯端末ＰＴ１に割り当てられていたデバイスＩＤ「Ｄ１」に代えて、携帯端末ＰＴ２に割り当てられるべきデバイスＩＤ「Ｄ２」が登録される。この後のＴ１３８～Ｔ１７８は、携帯端末ＰＴ１ではなく携帯端末ＰＴ２が利用される点と、デバイスＩＤ「Ｄ１」ではなくデバイスＩＤ「Ｄ２」が利用される点と、を除くと、図６のＴ３８～Ｔ７８と同様である。

【０１２１】

（ケースＢの効果）

上述したように、第１のユーザが携帯端末ＰＴ１に代えて携帯端末ＰＴ２を利用することを望む場合に、多機能機１０は、デバイスＩＤ「Ｄ１」に代えてデバイスＩＤ「Ｄ２」を認証テーブルＡＴに登録して（Ｔ１３６）、デバイスＩＤ「Ｄ２」を携帯端末ＰＴ２に供給することができる（Ｔ１３８）。従って、第１のユーザは、携帯端末ＰＴ１に代えて携帯端末ＰＴ２を利用して、多機能機１０にログインすることができ（Ｔ１６０～Ｔ１７２）、この結果、所望の機能を多機能機１０に実行させることができる（Ｔ１７４、Ｔ１７６）。

【０１２２】

（ケースＣ；図８）

続いて、図８を参照して、多機能機１０及び認証カードＡＣによって実現されるケースＣを説明する。

【０１２３】

図８のケースＣの初期状態では、多機能機１０の認証テーブルＡＴには、図１に示されるように、ユーザＩＤ「Ｕ２」、パスワード「Ｐ２」、コピー「ＮＧ」、スキャン「ＯＫ」、及び、送信先「ＩＰ１」を含む組合せ情報が登録されている。ただし、認証テーブルＡＴでは、ユーザＩＤ「Ｕ２」及びパスワード「Ｐ２」に関連付けて、デバイスＩＤが登録されていない。また、認証カードＡＣは、デバイスＩＤ「Ｄ３」を予め記憶している。

【０１２４】

通信システム２の管理者は、認証カードＡＣを第２のユーザに付与済みである。また、管理者は、ユーザＩＤ「Ｕ２」及びパスワード「Ｐ２」を第２のユーザに通知済みである。従って、Ｔ２１０では、第２のユーザは、多機能機１０の操作部１２を操作して、ユーザＩＤ「Ｕ２」及びパスワード「Ｐ２」のセットを入力することができる（図３のＳ１０でＹＥＳ）。この場合、Ｔ２１２では、多機能機１０は、入力済みのセットが認証テーブルＡＴに登録済みであると判断し（Ｓ１２でＹＥＳ）、ユーザＩＤ「Ｕ２」に対応するロ

グイン状態へ移行する（Ｓ１４）。

【０１２５】

Ｔ２１４では、第２のユーザは、スキャン機能のための機能実行操作を多機能機１０の操作部１２に実行する（図３のＳ２０でＹＥＳ）。この場合、Ｔ２１６では、多機能機１０は、ユーザＩＤ「Ｕ２」に対応するログイン状態であると判断し（Ｓ２２でＹＥＳ）、ユーザＩＤ「Ｕ２」に関連付けられているスキャン許可情報が「ＯＫ」であると判断し（Ｓ２６でＹＥＳ）、スキャン機能を実行する（Ｓ２８）。そして、Ｔ２１８では、多機能機１０は、非ログイン状態へ移行する（Ｓ３２）。

【０１２６】

第２のユーザは、認証カードＡＣのデバイスＩＤ「Ｄ３」を多機能機１０の認証テーブルＡＴに登録することを望んでいる。従って、Ｔ２３０では、第２のユーザは、多機能機１０の操作部１２を操作して、ユーザＩＤ「Ｕ２」及びパスワード「Ｐ２」のセットを入力する（図３のＳ１０でＹＥＳ）。この場合、Ｔ２３２では、多機能機１０は、入力済みのセットが認証テーブルＡＴに登録済みであると判断し（Ｓ１２でＹＥＳ）、ユーザＩＤ「Ｕ２」に対応するログイン状態へ移行する（Ｓ１４）。

【０１２７】

Ｔ２３４では、第２のユーザが認証カードＡＣを多機能機１０に近づけることに起因して、多機能機１０と認証カードＡＣとの間にＲ／Ｗ－ＣＥ接続が確立される（図３のＳ４０でＹＥＳ、図４のＳ５０でＮＯ）。この場合、Ｔ２３６では、多機能機１０は、認証カードＡＣからデバイスＩＤ「Ｄ３」を取得する（Ｓ７０）。そして、Ｔ２３８では、多機能機１０は、ユーザＩＤ「Ｕ２」に対応するログイン状態であると判断し（Ｓ７２でＹＥＳ）、ユーザＩＤ「Ｕ２」及びパスワード「Ｐ２」に関連付けて、デバイスＩＤ「Ｄ３」を認証テーブルＡＴに登録する（Ｓ７４）。次いで、Ｔ２４０では、多機能機１０は、非ログイン状態へ移行する（Ｓ７６）。

【０１２８】

第２のユーザは、認証カードＡＣを利用して多機能機１０にログインすることを望んでいる。Ｔ２６６では、第２のユーザが認証カードＡＣを多機能機１０に近づけることに起因して、多機能機１０と認証カードＡＣとの間にＲ／Ｗ－ＣＥ接続が確立される（図３のＳ４０でＹＥＳ、図４のＳ５０でＮＯ）。この場合、Ｔ２６８では、多機能機１０は、認証カードＡＣからデバイスＩＤ「Ｄ３」を取得する（Ｓ７０）。そして、Ｔ２７２では、多機能機１０は、非ログイン状態であると判断し（Ｓ７２でＮＯ）、デバイスＩＤ「Ｄ３」が認証テーブルＡＴに登録済みであると判断し（Ｓ７８でＹＥＳ）、デバイスＩＤ「Ｄ３」に関連付けられているユーザＩＤ「Ｕ２」に対応するログイン状態へ移行する（Ｓ８０）。この後のＴ２７４～Ｔ２７８は、Ｔ２１４～Ｔ２１８と同様である。

【０１２９】

（ケースＣの効果）

多機能機１０は、多機能機１０の状態がユーザＩＤ「Ｄ２」に対応するログイン状態である間に、認証カードＡＣからデバイスＩＤ「Ｄ３」を取得する場合（Ｔ２３６）に、ユーザＩＤ「Ｄ２」及びパスワード「Ｐ２」に関連付けて、デバイスＩＤ「Ｄ３」を認証テーブルＡＴに登録する（Ｔ２３８）。その後、多機能機１０は、多機能機１０の状態が非ログイン状態である間に、認証カードＡＣからデバイスＩＤ「Ｄ３」を取得する場合（Ｔ２６８）に、多機能機１０の状態をユーザＩＤ「Ｄ２」に対応するログイン状態へ移行させる（Ｔ２７２）。従って、第２のユーザは、認証カードＡＣを利用して、多機能機１０にログインすることができ、この結果、所望の機能を多機能機１０に実行させることができる（Ｔ２７４、Ｔ２７６）。

【０１３０】

また、本実施例によると、第２のユーザは、認証カードＡＣのデバイスＩＤ「Ｄ３」を多機能機１０の認証テーブルＡＴに登録することを望む場合に、認証カードＡＣを多機能機１０に近づけるだけでよい。即ち、第２のユーザ（あるいは通信システム２の管理者）は、デバイスＩＤ「Ｄ３」を認証テーブルＡＴに登録するために、例えば、多機能機１０

の操作部１２を操作したり、ＰＣ等を利用して多機能機１０にアクセスしたりせずに済む。従って、ユーザの利便性が高い。

【０１３１】

（対応関係）

多機能機１０、携帯端末ＰＴ１が、それぞれ、「機能実行機器」、「可搬型デバイス」の一例である。携帯端末ＰＴ１、携帯端末ＰＴ２、認証カードＡＣが、それぞれ、「第１の可搬型デバイス」、「第２の可搬型デバイス」、「第３の可搬型デバイス」の一例である。コピー機能及び／又はスキャン機能が、「特定機能」の一例である。印刷実行部１６及びスキャン実行部１８が、「機能実行部」の一例である。認証テーブルＡＴが、「認証用メモリ」の一例である。ＮＦＣＩ／Ｆ２０、ＮＦＣＩ／Ｆ８０が、それぞれ、「機器インターフェース」、「デバイスインターフェース」の一例である。アプリＩＤが、「所定のアプリケーション情報」の一例である。Ｐ２Ｐモード、Ｒ／Ｗモードが、それぞれ、「第１のモード」、「第２のモード」の一例である。Ｐ２Ｐモード、ＣＥモードが、それぞれ、「第３のモード」、「第４のモード」の一例である。図４のＳ６０及びＳ６２の処理が、「第１種の処理」の一例であり、Ｓ８０の処理が、「第２種の処理」の一例である。

【０１３２】

図６のケースＡでは、ユーザＩＤ「Ｕ１」及びパスワード「Ｐ１」が、「第１のユーザ認証情報」の一例である。デバイスＩＤ「Ｄ１」が、「第１のデバイス認証情報」の一例である。非ログイン状態、ユーザＩＤ「Ｕ１」に対応するログイン状態が、それぞれ、「第１の不許可状態」、「第１の許可状態」の一例である。Ｔ３４のＰ２Ｐ接続、Ｔ６６のＲ／Ｗ－ＣＥ接続が、それぞれ、「第１の接続」、「第２の接続」の一例である。

【０１３３】

図７のケースＢでは、デバイスＩＤ「Ｄ２」が、「第２のデバイス認証情報」の一例である。Ｔ１３４のＰ２Ｐ接続、Ｔ１６６のＲ／Ｗ－ＣＥ接続が、それぞれ、「第３の接続」、「第４の接続」の一例である。

【０１３４】

図８のケースＣでは、ユーザＩＤ「Ｕ２」及びパスワード「Ｐ２」が、「第２のユーザ認証情報」の一例である。デバイスＩＤ「Ｄ３」が、「第３のデバイス認証情報」の一例である。非ログイン状態、ユーザＩＤ「Ｕ２」に対応するログイン状態が、それぞれ、「第２の不許可状態」、「第２の許可状態」の一例である。Ｔ２３４のＲ／Ｗ－ＣＥ接続、Ｔ２６６のＲ／Ｗ－ＣＥ接続が、それぞれ、「第５の接続」、「第６の接続」の一例である。

【０１３５】

以上、本発明の具体例を詳細に説明したが、これらは例示にすぎず、特許請求の範囲を限定するものではない。特許請求の範囲に記載の技術には以上に例示した具体例を様々に変形、変更したものが含まれる。上記の実施例の変形例を以下に列挙する。

【０１３６】

（変形例１）

上記の実施例では、多機能機１０のＣＰＵ３２は、ログイン状態である間に、携帯端末ＰＴ１とのＰ２Ｐ接続が確立される場合（図４のＳ５０でＹＥＳ、Ｓ５２でＹＥＳ）に、デバイスＩＤの生成及び登録を実行する（Ｓ６０）。これに代えて、ＣＰＵ３２は、非ログイン状態である間に、携帯端末ＰＴ１とのＰ２Ｐ接続が確立される場合に、ユーザＩＤ及びパスワードの入力をユーザに促してもよい。そして、ＣＰＵ３２は、ユーザによってユーザＩＤ及びパスワードが入力される場合に、デバイスＩＤの生成及び登録を実行してもよい。一般的に言うと、登録部は、機能実行機器の状態が第１の許可状態であるのか否かに関わらず、第１の接続が確立される場合に、第１のデバイス認証情報を登録してもよい。

【０１３７】

（変形例２）

上記の実施例では、多機能機１０のＣＰＵ３２は、携帯端末ＰＴ１とのＰ２Ｐ接続が確

立される場合（図４のＳ５０でＹＥＳ）に、デバイスＩＤを生成する（Ｓ６０）。これに代えて、ＣＰＵ３２は、携帯端末ＰＴ１とのＰ２Ｐ接続が確立される前に、ユニークなデバイスＩＤを予め生成しておき、携帯端末ＰＴ１とのＰ２Ｐ接続が確立される場合に、生成済みのデバイスＩＤの登録を実行してもよい。一般的に言うと、登録部は、第１の接続が確立される前に、第１のデバイス認証情報を生成してもよいし、第１の接続が確立された後に、第１のデバイス認証情報を生成してもよい。

【０１３８】

（変形例３）

上記の実施例では、多機能機１０のＣＰＵ３２は、携帯端末ＰＴ１からアプリＩＤを取得する場合（図４のＳ５６でＹＥＳ）に、デバイスＩＤの生成及び登録を実行する（Ｓ６０）。これに代えて、ＣＰＵ３２は、携帯端末ＰＴ１からアプリＩＤを取得するのか否かに関わらず（即ちＳ５６でＹＥＳでもＮＯでも）、デバイスＩＤの生成及び登録を実行してもよい。一般的に言うと、登録部は、所定のアプリケーション情報が取得されるのか否かに関わらず、第１の接続が確立される場合に、第１のデバイス認証情報を登録してもよい。

【０１３９】

（変形例４）

上記の実施例では、多機能機１０のＣＰＵ３２は、認証カードＡＣのデバイスＩＤ「Ｄ３」を登録する処理を実行可能である（図４のＳ７４、Ｓ７６）。これに代えて、ＣＰＵ３２は、認証カードＡＣのデバイスＩＤ「Ｄ３」を登録する処理を実行不可能であってもよい。例えば、通信システム２の管理者は、多機能機１０の操作部１２を操作して、認証カードＡＣのデバイスＩＤ「Ｄ３」を認証テーブルＡＴに登録してもよい。一般的に言うと、登録部は、第２のユーザ認証情報に関連付けて第３のデバイス認証情報を登録する処理を実行不可能であってもよい。

【０１４０】

（変形例５）

上記の実施例では、多機能機１０のＣＰＵ３２は、ログイン状態である間に、機能実行操作が操作部１２に実行される場合（図３のＳ２０でＹＥＳ、Ｓ２２でＹＥＳ）に、指定機能を実行する（Ｓ２８）。これに代えて、ＣＰＵ３２は、例えば、非ログイン状態である間に、機能実行操作が実行される場合に、ログインの実行をユーザに促してもよい。そして、ＣＰＵ３２は、ユーザによってログインのための動作（例えばユーザＩＤ及びパスワードの入力等）が実行されて、ログイン状態へ移行した後に、指定機能を実行してもよい。一般的に言うと、機能実行部は、機能実行機器の状態が第１の許可状態である間に、特定機能の利用の指示が入力される場合に、特定機能を実行してもよいし、機能実行機器の状態が第１の不許可状態である間に、特定機能の利用の指示が入力されて、その後、機能実行機器の状態が第１の許可状態へ移行する場合に、特定機能を実行してもよい。

【０１４１】

（変形例６）

例えば、図５において、携帯端末ＰＴ１のＣＰＵ９２は、デバイスＩＤがメモリ９４に記憶済みである場合（Ｓ１００でＹＥＳ）に、Ｐ２ＰモードのみでＮＦＣＩ／Ｆ８０を動作させ、デバイスＩＤがメモリ９４に記憶済みでない場合（１００でＮＯ）に、ＣＥモードのみでＮＦＣＩ／Ｆ８０を動作させてもよい。そして、ＣＰＵ９２は、多機能機１０とのＲ／Ｗ－ＣＥ接続が確立される場合に、多機能機１０からデバイスＩＤを取得して、デバイスＩＤをメモリ９４に記憶させてもよい。また、ＣＰＵ９２は、多機能機１０とのＰ２Ｐ接続が確立される場合に、多機能機１０にデバイスＩＤを供給して、多機能機１０の状態をログイン状態へ移行させてもよい。また、多機能機１０のＣＰＵ３２は、携帯端末ＰＴ１とのＲ／Ｗ－ＣＥ接続が確立される場合に、デバイスＩＤを登録して、当該デバイスＩＤを携帯端末ＰＴ１に供給してもよい。また、ＣＰＵ３２は、携帯端末ＰＴ１とのＰ２Ｐ接続が確立される場合に、携帯端末ＰＴ１からデバイスＩＤを取得して、多機能機１０の状態をログイン状態へ移行させてもよい。本変形例では、Ｒ／Ｗモード、Ｐ２Ｐモー

ドが、それぞれ、「第１のモード」、「第２のモード」の一例である。ＣＥモード、Ｐ２Ｐモードが、それぞれ、「第３のモード」、「第４のモード」の一例である。また、「第１のモード」～「第４のモード」は、上記の実施例及び本変形例の各モードに限定されない。例えば、多機能機１０のＮＦＣＩ／Ｆ２０が、Ｐ２Ｐモード及びＲ／Ｗモードのみならず、ＣＥモードで動作可能である場合には、以下の変形例を採用してもよい。例えば、Ｐ２Ｐモード、ＣＥモードが、それぞれ、「第１のモード」、「第２のモード」の一例であり、さらに、Ｐ２Ｐモード、Ｒ／Ｗモードが、それぞれ、「第３のモード」、「第４のモード」の一例であってもよい。また、例えば、ＣＥモード、Ｐ２Ｐモードが、それぞれ、「第１のモード」、「第２のモード」の一例であり、さらに、Ｒ／Ｗモード、Ｐ２Ｐモードが、それぞれ、「第３のモード」、「第４のモード」の一例であってもよい。また、例えば、Ｒ／Ｗモード、ＣＥモードが、それぞれ、「第１のモード」、「第２のモード」の一例であり、さらに、ＣＥモード、Ｒ／Ｗモードが、それぞれ、「第３のモード」、「第４のモード」の一例であってもよい。例えば、ＣＥモード、Ｒ／Ｗモードが、それぞれ、「第１のモード」、「第２のモード」の一例であり、さらに、Ｒ／Ｗモード、ＣＥモードが、それぞれ、「第３のモード」、「第４のモード」の一例であってもよい。

【０１４２】

（変形例７）

また、上記の実施例では、「第１の接続」において、多機能機１０のＮＦＣＩ／Ｆ２０が動作するモード（即ちＰ２Ｐモード）と、「第２の接続」において、ＮＦＣＩ／Ｆ２０が動作するモード（即ちＲ／Ｗモード）と、が異なる。また、「第１の接続」において、携帯端末ＰＴ１のＮＦＣＩ／Ｆ８０が動作するモード（即ちＰ２Ｐモード）と、「第２の接続」において、ＮＦＣＩ／Ｆ８０が動作するモード（即ちＣＥモード）と、が異なる。これに代えて、「第１の接続」において、多機能機１０のＮＦＣＩ／Ｆ２０が動作するモードと、「第２の接続」において、ＮＦＣＩ／Ｆ２０が動作するモードと、が同じであってもよい（例えばＰ２Ｐモード）。同様に、「第１の接続」において、携帯端末ＰＴ１のＮＦＣＩ／Ｆ８０が動作するモードと、「第２の接続」において、ＮＦＣＩ／Ｆ８０が動作するモードと、が同じであってもよい。

【０１４３】

（変形例８）

例えば、携帯端末ＰＴ１は、デバイスＩＤ「Ｄ１」をメモリ９４に予め記憶していてもよい。即ち、多機能機１０の認証テーブルＡＴにデバイスＩＤ「Ｄ１」が登録されていない状態で、例えば、ユーザがデバイスＩＤ「Ｄ１」を携帯端末ＰＴ１に入力して、携帯端末ＰＴ１にデバイスＩＤ「Ｄ１」を割り当ててもよい。この場合、多機能機１０のＣＰＵ３２は、図８のケースＣにおいて認証カードＡＣのデバイスＩＤ「Ｄ３」を認証テーブルＡＴに登録する場合と同様に、携帯端末ＰＴ１からデバイスＩＤ「Ｄ１」を取得して、デバイスＩＤ「Ｄ１」を認証テーブルＡＴに登録してもよい。本変形例では、携帯端末ＰＴ１が「第３の可搬型デバイス」の一例である。

【０１４４】

（変形例９）

多機能機１０の操作部１２及び表示部１４は、いわゆるタッチパネルであってもよい。即ち、多機能機１０の操作部１２及び表示部１４は、上記の実施例のように、別々に構成されているハードウェアによって実現されてもよいし、本変形例のように、一体に構成されているハードウェアによって実現されてもよい。同様に、携帯端末ＰＴ１の操作部７２及び表示部７４は、別々に構成されているハードウェアによって実現されてもよいし、一体に構成されているハードウェアによって実現されてもよい。

【０１４５】

（変形例１０）

認証テーブルＡＴは、多機能機１０のメモリ３４に記憶されていなくてもよく、多機能機１０とは別体に構成されている特定機器（例えばサーバ）に記憶されていてもよい。この場合、多機能機１０のＣＰＵ３２は、例えば、図３のＳ１２、Ｓ２６、図４のＳ６０、

Ｓ７４、Ｓ７８等を実行する際に、特定機器と通信を実行して、特定機器内の認証テーブルＡＴにアクセスしてもよい。一般的に言うと、「認証用メモリ」は、機能実行機器の内部に存在していてもよいし、機能実行機器の外部に存在していてもよい。

【０１４６】

（変形例１１）

多機能機１０及び携帯端末ＰＴ１は、ＮＦＣＩ／Ｆ２０，８０に代えて、ＴｒａｎｓｆｅｒＪｅｔ（登録商標）、ＢｌｕｅＴｏｏｔｈ（登録商標）、赤外線等の他の近距離無線通信を実行するためのＩ／Ｆを備えていてもよい。即ち、「機器インターフェース」及び「デバイスインターフェース」は、ＮＦＣＩ／Ｆに限られず、他の種類のＩ／Ｆであってもよい。

【０１４７】

（変形例１２）

「機能実行機器」は、多機能機１０に限られず、印刷機能のみを実行可能なプリンタであってもよいし、スキャン機能のみを実行可能なスキャナであってもよいし、電話機能を実行可能な電話機でもよいし、ファクシミリ機能を実行可能なＦＡＸ機であってもよいし、通信機能を実行可能なＰＣ等であってもよい。即ち、「特定機能」は、コピー機能及びスキャン機能に限られず、他の機能であってもよい。

【０１４８】

（変形例１３）上記の各実施例では、図３～図５の各処理がソフトウェア（即ちプログラム３６，９８）によって実現されるが、図３～図５の各処理のうちの少なくとも１つが論理回路等のハードウェアによって実現されてもよい。

【０１４９】

また、本明細書または図面に説明した技術要素は、単独であるいは各種の組合せによって技術的有用性を発揮するものであり、出願時請求項記載の組合せに限定されるものではない。また、本明細書または図面に例示した技術は複数目的を同時に達成するものであり、そのうちの一つの目的を達成すること自体で技術的有用性を持つものである。

以下に、本明細書に記載の技術の特徴を列挙する。

（項目１）

機能実行機器であって、

特定機能を実行する機能実行部と、

ユーザによって操作される操作部と、

制御部と、を備え、

前記制御部は、

第１のユーザ認証情報が認証用メモリに登録されている状態で、第１のユーザによって前記操作部が操作されて、前記第１のユーザ認証情報が前記機能実行機器に入力される場合に、前記機能実行機器の状態を、前記第１のユーザに前記特定機能の利用を許可しない第１の不許可状態から、前記第１のユーザに前記特定機能の利用を許可する第１の許可状態へ移行させる状態移行部と、

第１の可搬型デバイスとの第１の接続が確立される場合に、前記第１のユーザ認証情報に関連付けて第１のデバイス認証情報を前記認証用メモリに登録する登録部と、

前記第１の可搬型デバイスとの前記第１の接続が確立される場合に、前記第１のデバイス認証情報を前記第１の可搬型デバイスに供給する供給部と、を備え、

前記状態移行部は、さらに、前記第１のデバイス認証情報が前記認証用メモリに登録された後に、前記第１の可搬型デバイスとの第２の接続が確立されて、前記第１の可搬型デバイスから前記第１のデバイス認証情報が取得される場合に、前記機能実行機器の状態を前記第１の不許可状態から前記第１の許可状態へ移行させる、

機能実行機器。

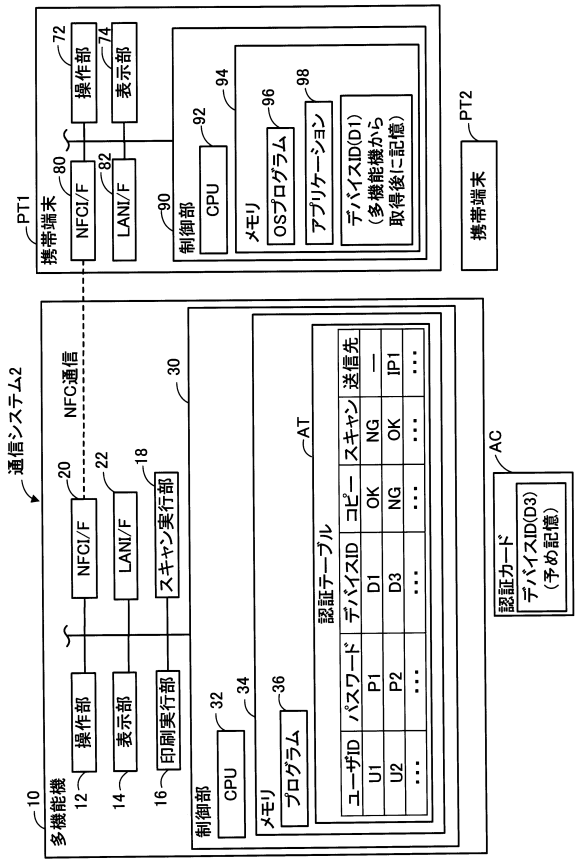
（項目２）

前記登録部は、前記機能実行機器の状態が前記第１の許可状態である間に、前記第１の可搬型デバイスとの前記第１の接続が確立される場合に、前記第１のユーザ認証情報に関

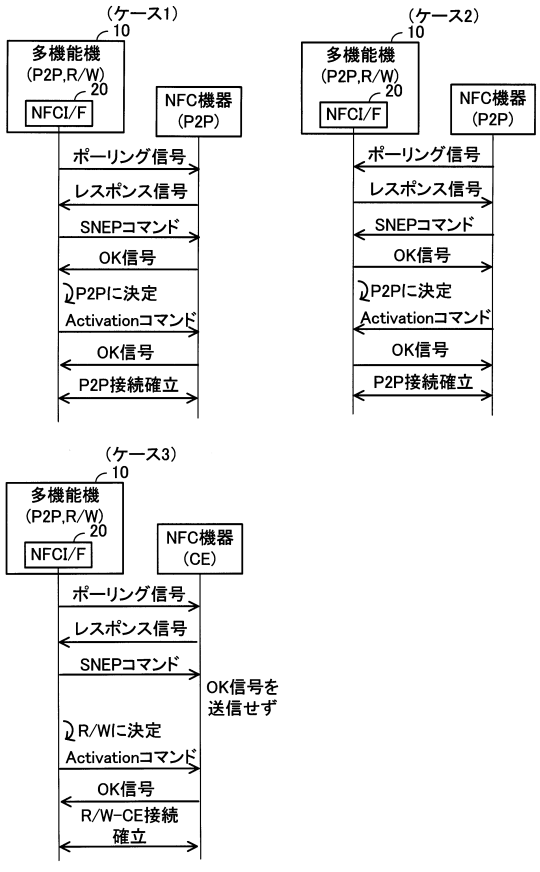
連付けて前記第１のデバイス認証情報を前記認証用メモリに登録する、項目１に記載の機能実行機器。
（項目３）
前記登録部は、さらに、前記第１のデバイス認証情報が前記認証用メモリに登録された後に、前記機能実行機器の状態が前記第１の許可状態である間に、第２の可搬型デバイスとの第３の接続が確立される場合に、前記第１のユーザ認証情報に関連付けて、前記第１のデバイス認証情報に代えて、第２のデバイス認証情報を前記認証用メモリに登録し、
前記供給部は、さらに、前記第２の可搬型デバイスとの前記第３の接続が確立される場合に、前記第２のデバイス認証情報を前記第２の可搬型デバイスに供給し、
前記状態移行部は、さらに、前記第２のデバイス認証情報が前記認証用メモリに登録された後に、前記第２の可搬型デバイスとの第４の接続が確立されて、前記第２の可搬型デバイスから前記第２のデバイス認証情報が取得される場合に、前記機能実行機器の状態を前記第１の不許可状態から前記第１の許可状態へ移行させる、項目２に記載の機能実行機器。
（項目４）
前記状態移行部は、さらに、前記第１のユーザ認証情報とは異なる第２のユーザ認証情報が前記認証用メモリに登録されている状態で、第２のユーザによって前記操作部が操作されて、前記第２のユーザ認証情報が前記機能実行機器に入力される場合に、前記機能実行機器の状態を、前記第２のユーザに前記特定機能の利用を許可しない第２の不許可状態から、前記第２のユーザに前記特定機能の利用を許可する第２の許可状態へ移行させ、
前記登録部は、さらに、前記機能実行機器の状態が前記第２の許可状態である間に、第３のデバイス認証情報を予め記憶している第３の可搬型デバイスとの第５の接続が確立されて、前記第３の可搬型デバイスから前記第３のデバイス認証情報が取得される場合に、前記第２のユーザ認証情報に関連付けて前記第３のデバイス認証情報を前記認証用メモリに登録し、
前記状態移行部は、さらに、前記第３のデバイス認証情報が前記認証用メモリに登録された後に、前記機能実行機器の状態が前記第２の不許可状態である間に、前記第３の可搬型デバイスとの第６の接続が確立されて、前記第３の可搬型デバイスから前記第３のデバイス認証情報が取得される場合に、前記機能実行機器の状態を前記第２の不許可状態から前記第２の許可状態へ移行させる、項目１から３のいずれか一項に記載の機能実行機器。
（項目５）
前記登録部は、
前記第１の可搬型デバイスとの前記第１の接続が確立され、かつ、前記第１の可搬型デバイスから所定のアプリケーション情報が取得される場合に、前記第１のユーザ認証情報に関連付けて前記第１のデバイス認証情報を前記認証用メモリに登録し、
前記第１の可搬型デバイスとの前記第１の接続が確立され、かつ、前記第１の可搬型デバイスから前記所定のアプリケーション情報が取得されない場合に、前記第１のユーザ認証情報に関連付けて前記第１のデバイス認証情報を前記認証用メモリに登録せず、
前記所定のアプリケーション情報は、前記機能実行機器を利用するためのアプリケーションが前記第１の可搬型デバイスで起動中である場合に、前記第１の可搬型デバイスから前記機能実行機器に供給される、項目１から４のいずれか一項に記載の機能実行機器。
（項目６）
前記登録部は、前記第１の可搬型デバイスとの前記第１の接続が確立される場合に、前記第１のデバイス認証情報を生成して、前記第１のユーザ認証情報に関連付けて前記第１のデバイス認証情報を前記認証用メモリに登録する、項目１から５のいずれか一項に記載の機能実行機器。
（項目７）
前記機能実行機器は、さらに、
第１のモードと第２のモードとを含む複数のモードで動作可能な機器インターフェースを備え、

前記第１の接続は、前記機器インターフェースが前記第１のモードで動作するための接続であり、
前記第２の接続は、前記機器インターフェースが前記第２のモードで動作するための接続である、項目１から６のいずれか一項に記載の機能実行機器。
（項目８）
前記制御部は、さらに、
前記第１の可搬型デバイスとの接続が確立される場合に、前記確立済みの接続が、前記機器インターフェースが前記第１のモードで動作するための前記第１の接続であるのか、前記機器インターフェースが前記第２のモードで動作するための前記第２の接続であるのか、を判断し、前記確立済みの接続が前記第１の接続であると判断する場合に、第１種の処理を実行すべきことを決定し、前記確立済みの接続が前記第２の接続であると判断する場合に、第２種の処理を実行すべきことを決定する決定部を備え、
前記第１種の処理は、
前記登録部が、前記第１のユーザ認証情報に関連付けて前記第１のデバイス認証情報を前記認証用メモリに登録する処理と、
前記供給部が、前記第１のデバイス認証情報を前記第１の可搬型デバイスに供給する処理と、を含み、
前記第２種の処理は、
前記第１の可搬型デバイスから前記第１のデバイス認証情報が取得される場合に、前記状態移行部が、前記機能実行機器の状態を前記第１の不許可状態から前記第１の許可状態へ移行させる処理を含む、項目７に記載の機能実行機器。
（項目９）
前記第２のモードは、ＮＦＣ（Near Field Communicationの略）方式のＲｅａｄｅｒ／Ｗｒｉｔｅｒモードを含む、項目７又は８に記載の機能実行機器。
（項目１０）
可搬型デバイスであって、
制御部を備え、
前記制御部は、
デバイスメモリと、
特定機能を実行可能な機能実行機器との第１の接続が確立される場合に、前記機能実行機器から第１のデバイス認証情報を取得する取得部と、
前記機能実行機器から前記第１のデバイス認証情報が取得される場合に、前記第１のデバイス認証情報を前記デバイスメモリに記憶させる記憶制御部と、
前記第１のデバイス認証情報が前記デバイスメモリに記憶された後に、前記機能実行機器との第２の接続が確立される場合に、前記デバイスメモリ内の前記第１のデバイス認証情報を前記機能実行機器に供給して、前記機能実行機器の状態を、前記可搬型デバイスのユーザに前記特定機能の利用を許可しない不許可状態から、前記ユーザに前記特定機能の利用を許可する許可状態へ移行させる供給部と、
を備える、可搬型デバイス。
（項目１１）
前記可搬型デバイスは、さらに、
第３のモードと第４のモードとを含む複数のモードで動作可能なデバイスインターフェースを備え、
前記制御部は、さらに、
前記第１のデバイス認証情報が前記デバイスメモリに記憶されていない場合に、前記第３のモードで動作すべきことを前記デバイスインターフェースに指示し、前記第１のデバイス認証情報が前記デバイスメモリに記憶されている場合に、前記第４のモードで動作すべきことを前記デバイスインターフェースに指示するインターフェース制御部を備え、
前記取得部は、前記第３のモードで動作する前記デバイスインターフェースを介して、前記機能実行機器との前記第１の接続が確立される場合に、前記機能実行機器から前記第

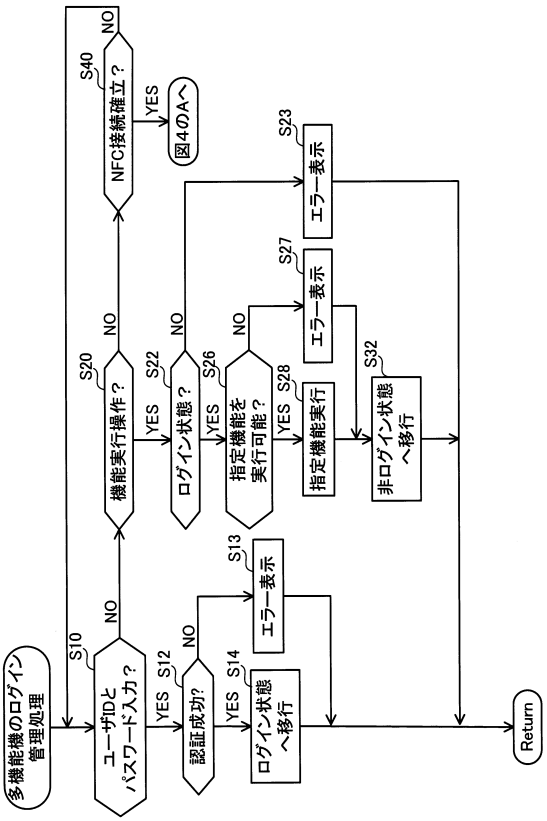
１のデバイス認証情報を取得し、
　前記供給部は、前記第４のモードで動作する前記デバイスインターフェースを介して、前記機能実行機器との前記第２の接続が確立される場合に、前記第１のデバイス認証情報を前記機能実行機器に供給して、前記機能実行機器の状態を前記不許可状態から前記許可状態へ移行させる、項目１０に記載の可搬型デバイス。
（項目１２）
　可搬型デバイスのためのコンピュータプログラムであって、
　特定機能を実行可能な機能実行機器との第１の接続が確立される場合に、前記機能実行機器から第１のデバイス認証情報を取得する取得処理と、
　前記機能実行機器から前記第１のデバイス認証情報が取得される場合に、前記第１のデバイス認証情報を前記可搬型デバイスのデバイスメモリに記憶させる記憶制御処理と、
　前記第１のデバイス認証情報が前記デバイスメモリに記憶された後に、前記機能実行機器との第２の接続が確立される場合に、前記デバイスメモリ内の前記第１のデバイス認証情報を前記機能実行機器に供給して、前記機能実行機器の状態を、前記可搬型デバイスのユーザに前記特定機能の利用を許可しない不許可状態から、前記ユーザに前記特定機能の利用を許可する許可状態へ移行させる供給処理と、
　を実行させるコンピュータプログラム。
【符号の説明】
【０１５０】
２：通信システム、１０：多機能機、１２：操作部、１４：表示部、１６：印刷実行部、１８：スキャン実行部、２０：ＮＦＣインターフェース、２２：ＬＡＮインターフェース、３０：制御部、３２：ＣＰＵ、３４：メモリ、３６：プログラム、ＡＴ：認証テーブル、ＰＴ１，ＰＴ２：携帯端末、７２：操作部、７４：表示部、８０：ＮＦＣインターフェース、８２：ＬＡＮインターフェース、９０：制御部、９２：ＣＰＵ、９４：メモリ、９６：ＯＳプログラム、９８：アプリケーション、ＡＣ：認証カード
【図１】



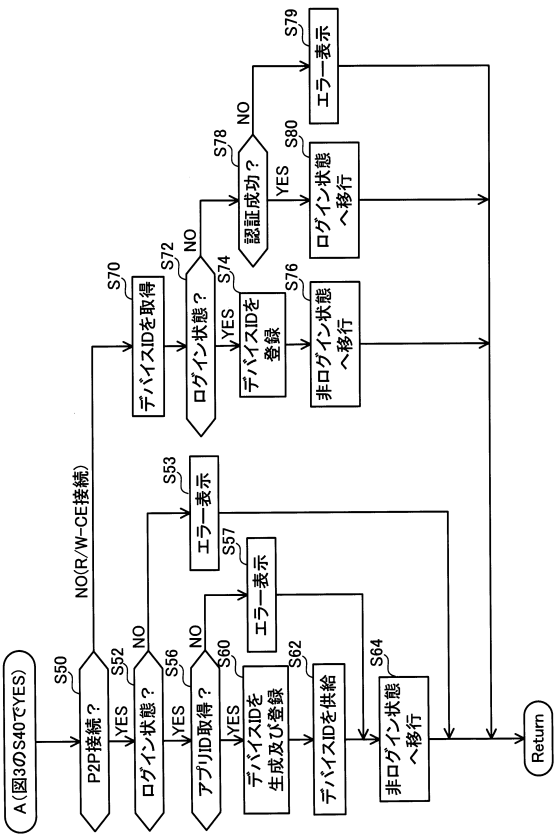
【図２】



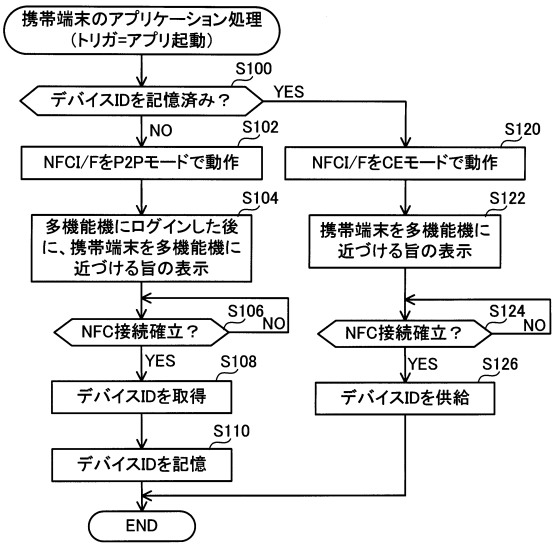
【図３】


多機能機のログイン管理処理
S10
ユーザIDとパスワード入力？
NO
YES
S12
認証成功?
NO
YES
S13
エラー表示
S14
ログイン状態へ移行
S20
機能実行操作？
NO
YES
S22
ログイン状態？
NO
YES
S26
指定機能を実行可能？
NO
YES
S27
エラー表示
S28
指定機能実行
S23
エラー表示
S32
非ログイン状態へ移行
S40
NFC接続確立？
NO
YES
図4のAへ
Return

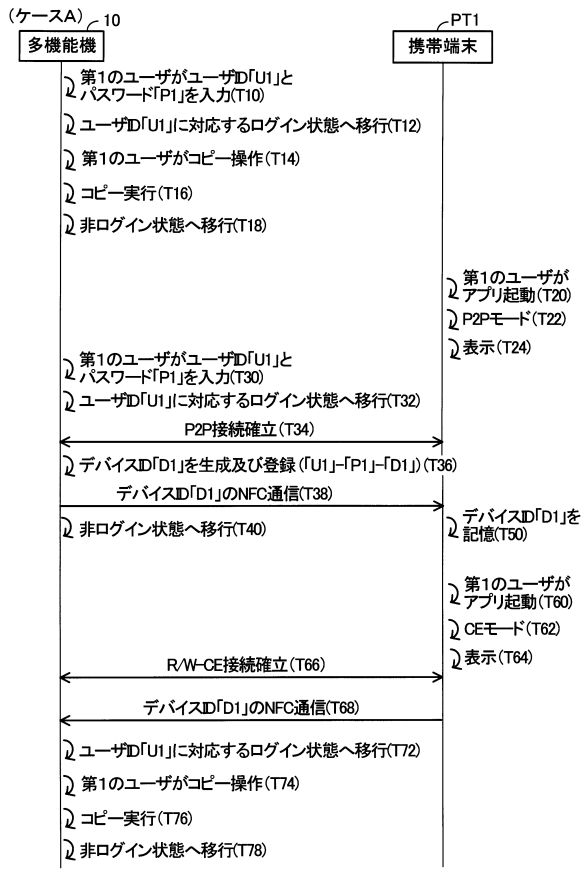
【図４】


A（図3のS40でYES）
S50
P2P接続？
NO(R/W-CE接続)
YES
S52
ログイン状態？
NO
YES
S56
アプリID取得？
NO
YES
S60
デバイスIDを生成及び登録
S57
エラー表示
S53
エラー表示
S62
デバイスIDを供給
S64
非ログイン状態へ移行
S70
デバイスIDを取得
S72
ログイン状態？
NO
YES
S74
デバイスIDを登録
S76
非ログイン状態へ移行
S78
認証成功？
NO
YES
S80
ログイン状態へ移行
S79
エラー表示
Return

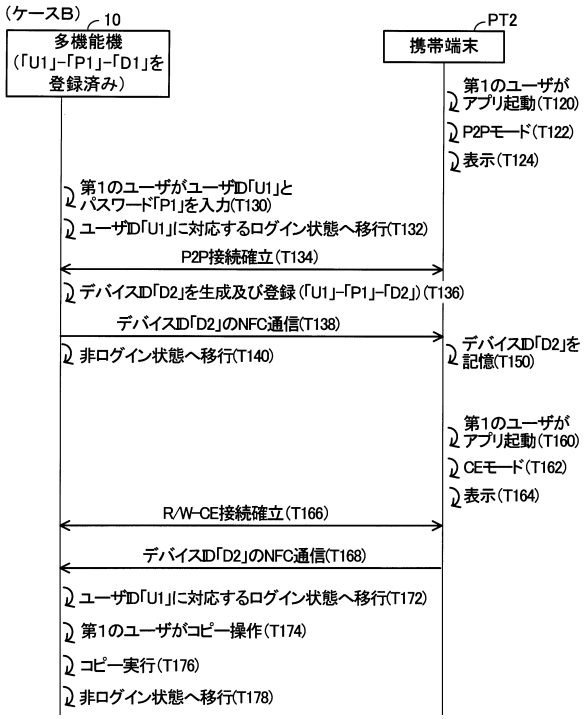
【図５】


携帯端末のアプリケーション処理（トリガ=アプリ起動）
S100
デバイスIDを記憶済み？
YES
NO
S102
NFCI/FをP2Pモードで動作
S104
多機能機にログインした後に、携帯端末を多機能機に近づける旨の表示
S106
NFC接続確立？
NO
YES
S108
デバイスIDを取得
S110
デバイスIDを記憶
S120
NFCI/FをCEモードで動作
S122
携帯端末を多機能機に近づける旨の表示
S124
NFC接続確立？
NO
YES
S126
デバイスIDを供給
END

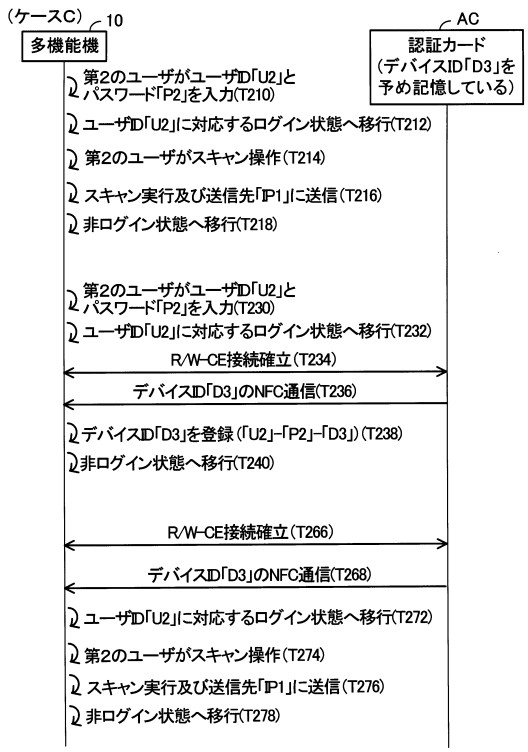
【図６】


（ケースA）
10
多機能機
PT1
携帯端末
第1のユーザがユーザID「U1」とパスワード「P1」を入力(T10)
ユーザID「U1」に対応するログイン状態へ移行(T12)
第1のユーザがコピー操作(T14)
コピー実行(T16)
非ログイン状態へ移行(T18)
第1のユーザがアプリ起動(T20)
P2Pモード(T22)
表示(T24)
第1のユーザがユーザID「U1」とパスワード「P1」を入力(T30)
ユーザID「U1」に対応するログイン状態へ移行(T32)
P2P接続確立(T34)
デバイスID「D1」を生成及び登録（「U1」-「P1」-「D1」）(T36)
デバイスID「D1」のNFC通信(T38)
非ログイン状態へ移行(T40)
デバイスID「D1」を記憶(T50)
第1のユーザがアプリ起動(T60)
CEモード(T62)
表示(T64)
R/W-CE接続確立(T66)
デバイスID「D1」のNFC通信(T68)
ユーザID「U1」に対応するログイン状態へ移行(T72)
第1のユーザがコピー操作(T74)
コピー実行(T76)
非ログイン状態へ移行(T78)

【図７】


（ケースB）
10
多機能機
（「U1」-「P1」-「D1」を
登録済み）
PT2
携帯端末
第1のユーザが
アプリ起動(T120)
P2Pモード(T122)
表示(T124)
第1のユーザがユーザID「U1」と
パスワード「P1」を入力(T130)
ユーザID「U1」に対応するログイン状態へ移行(T132)
P2P接続確立(T134)
デバイスID「D2」を生成及び登録（「U1」-「P1」-「D2」）(T136)
デバイスID「D2」のNFC通信(T138)
非ログイン状態へ移行(T140)
デバイスID「D2」を
記憶(T150)
第1のユーザが
アプリ起動(T160)
CEモード(T162)
表示(T164)
R/W-CE接続確立(T166)
デバイスID「D2」のNFC通信(T168)
ユーザID「U1」に対応するログイン状態へ移行(T172)
第1のユーザがコピー操作(T174)
コピー実行(T176)
非ログイン状態へ移行(T178)

【図８】


（ケースC）
10
多機能機
AC
認証カード
（デバイスID「D3」を
予め記憶している）
第2のユーザがユーザID「U2」と
パスワード「P2」を入力(T210)
ユーザID「U2」に対応するログイン状態へ移行(T212)
第2のユーザがスキャン操作(T214)
スキャン実行及び送信先「IP1」に送信(T216)
非ログイン状態へ移行(T218)
第2のユーザがユーザID「U2」と
パスワード「P2」を入力(T230)
ユーザID「U2」に対応するログイン状態へ移行(T232)
R/W-CE接続確立(T234)
デバイスID「D3」のNFC通信(T236)
デバイスID「D3」を登録（「U2」-「P2」-「D3」）(T238)
非ログイン状態へ移行(T240)
R/W-CE接続確立(T266)
デバイスID「D3」のNFC通信(T268)
ユーザID「U2」に対応するログイン状態へ移行(T272)
第2のユーザがスキャン操作(T274)
スキャン実行及び送信先「IP1」に送信(T276)
非ログイン状態へ移行(T278)

フロントページの続き

(51)Int.Cl.			FI		
G06F	***1/00***	***(2006.01)***	G06F	3/12	338
H04N	***1/00***	***(2006.01)***	G06F	1/00	370E
			H04N	1/00	107Z

(56)参考文献 特開2007－310426（JP，A）
特開2013－016201（JP，A）
特開2011－243017（JP，A）
特開2013－157736（JP，A）

(58)調査した分野(Int.Cl.，DB名)

G06F 21／30－G06F 21／46
G06F 3／12
G06K 7／10
G06K 19／07
H04N 1／00