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

特許第5521764号
(P5521764)

(45)発行日　平成26年6月18日(2014.6.18)　(24)登録日　平成26年4月18日(2014.4.18)

(51)Int.Cl.		F I		
G06F 21/34	(2013.01)	G06F	21/20	134
G06F 21/33	(2013.01)	G06F	21/20	133
G06F 21/43	(2013.01)	G06F	21/20	143
H04L 9/32	(2006.01)	H04L	9/00	673B
G06K 19/10	(2006.01)	H04L	9/00	673E

請求項の数 14　(全 19 頁)　最終頁に続く

(21)出願番号　特願2010-114958 (P2010-114958)
(22)出願日　平成22年5月19日 (2010.5.19)
(65)公開番号　特開2011-243017 (P2011-243017A)
(43)公開日　平成23年12月1日 (2011.12.1)
審査請求日　平成25年3月6日 (2013.3.6)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100147119
弁理士　篁　悟
(72)発明者　井上　赳
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】情報処理装置、認証システム、認証方法、認証プログラム及び記録媒体

(57)【特許請求の範囲】
【請求項１】
認証を条件として利用を許可する情報処理装置において、
利用者の認証情報及び該利用者に関連づけた他の携帯性を有する通信端末を識別する利用端末ＩＤを記憶するメモリを備え近距離通信を行う近距離通信デバイスと近距離通信する近距離通信手段と、
利用を許可する利用者の認証情報を登録認証情報として記憶する認証情報記憶手段と、
前記近距離通信手段が前記近距離通信デバイスから取得した前記認証情報を前記認証情報記憶手段の登録認証情報と照合して一次認証処理を行う一次認証手段と、
前記一次認証手段が前記一次認証に成功すると、前記近距離通信手段に近距離通信を行わせて通信端末から該通信端末の端末ＩＤを取得させ、該通信端末の端末ＩＤを前記利用端末ＩＤと照合して二次認証処理を行う二次認証手段と、
前記二次認証手段が認証に成功すると、利用を許可する制御手段と、
を備えていることを特徴とする情報処理装置。
【請求項２】
前記近距離通信デバイスは、前記メモリに、前記二次認証に利用する複数の前記通信端末の前記利用端末ＩＤを記憶し、
前記二次認証手段は、前記二次認証処理において、複数の前記利用端末ＩＤのうち１つ以上と一致する通信端末の端末ＩＤが前記近距離通信手段によって取得されると、二次認証成功とすることを特徴とする請求項１記載の情報処理装置。

【請求項３】
前記情報処理装置は、
前記一次認証手段による一次認証に成功することを条件として、前記近距離通信手段が近距離通信によって取得した通信端末の端末ＩＤを該一次認証した前記近距離通信デバイスに前記利用端末ＩＤとして登録するＩＤ登録手段を、さらに備えていることを特徴とする請求項１または請求項２記載の情報処理装置。
【請求項４】
前記情報処理装置は、
所定の警告手段を備え、
前記制御手段は、前記一次認証手段による一次認証に成功した後、所定時間内に、前記二次認証処理に失敗すると、前記警告手段に所定の警告を発生させることを特徴とする請求項１から請求項３のいずれかに記載の情報処理装置。
【請求項５】
前記制御手段は、
前記二次認証手段による二次認証に成功して、利用を許可した後、前記近距離通信手段に前記近距離通信デバイスまたは／及び前記通信端末と所定時間間隔で通信を行わせて、前記認証情報または／及び前記端末ＩＤを取得させ、取得された該認証情報または／及び該端末ＩＤに対する前記一次認証手段または前記二次認証手段による認証に失敗するか、該近距離通信デバイスまたは／及び該通信端末との通信に失敗すると、許可した利用を不許可とすることを特徴とする請求項１から請求項４のいずれかに記載の情報処理装置。
【請求項６】
前記情報処理装置は、
所定の警告手段を備え、
前記制御手段は、
前記所定時間間隔毎における前記認証に失敗するか、前記近距離通信デバイスまたは／及び前記通信端末との通信に失敗すると、前記警告手段に所定の警告を発生させることを特徴とする請求項５記載の情報処理装置。
【請求項７】
携帯性を有し内部メモリに端末ＩＤを記憶して近距離通信する通信端末と、
利用者の認証情報と該利用者に関連づけた前記通信端末を識別する利用端末ＩＤを記憶するメモリを備え近距離通信する近距離通信デバイスと、
前記近距離通信デバイス及び前記通信端末と近距離通信する近距離通信手段を備え所定の情報処理を行う情報処理装置と、
を備え、
前記情報処理装置は、
利用を許可する利用者の認証情報を登録認証情報として記憶する認証情報記憶手段と、
前記近距離通信手段によって前記近距離通信デバイスから認証情報を取得して、該認証情報を前記認証情報記憶手段の登録認証情報と照合して一次認証処理を行う一次認証手段と、
前記一次認証手段が前記一次認証に成功すると、前記近距離通信手段に近距離通信を行わせて通信端末から該通信端末の端末ＩＤを取得させ、該通信端末の端末ＩＤを前記利用端末ＩＤと照合して二次認証処理を行う二次認証手段と、
前記二次認証手段が認証に成功すると、利用を許可する制御手段と、
を備えていることを特徴とする認証システム。
【請求項８】
前記近距離通信デバイスは、前記メモリに、前記二次認証に利用する複数の前記通信端末の前記利用端末ＩＤを記憶し、
前記二次認証手段は、前記二次認証処理において、複数の前記利用端末ＩＤのうち１つ以上と一致する通信端末の端末ＩＤが前記近距離通信手段によって取得されると、二次認証成功とすることを特徴とする請求項７記載の認証システム。

【請求項９】
前記情報処理装置は、
前記一次認証手段による一次認証に成功することを条件として、前記近距離通信手段が近距離通信によって取得した通信端末の端末ＩＤを該一次認証した前記近距離通信デバイスに前記利用端末ＩＤとして登録するＩＤ登録手段を、さらに備えていることを特徴とする請求項７または請求項８記載の認証システム。
【請求項１０】
前記情報処理装置は、
所定の警告手段を備え、
前記制御手段は、前記一次認証手段による一次認証に成功した後、所定時間内に、前記二次認証処理に失敗すると、前記警告手段に所定の警告を発生させることを特徴とする請求項７から請求項９いずれかに記載の認証システム。
【請求項１１】
前記情報処理装置は、
前記制御手段が、前記二次認証手段による二次認証に成功して、利用を許可した後、前記近距離通信手段に前記近距離通信デバイスまたは／及び前記通信端末と所定時間間隔で通信を行わせて、前記認証情報または／及び前記端末ＩＤを取得させ、取得された該認証情報または／及び該端末ＩＤに対する前記一次認証手段または前記二次認証手段による認証に失敗するか、該近距離通信デバイスまたは／及び該通信端末との通信に失敗すると、許可した利用を不許可とすることを特徴とする請求項７から請求項１０のいずれかに記載の認証システム。
【請求項１２】
前記情報処理装置は、
所定の警告手段を備え、
前記制御手段が、前記所定時間間隔毎の前記認証に失敗するか、前記近距離通信デバイスまたは／及び前記通信端末との通信に失敗すると、前記警告手段に所定の警告を発生させることを特徴とする請求項１１記載の認証システム。
【請求項１３】
認証を条件として利用を許可する情報処理装置における認証プログラムであって、
コンピュータに、
利用者の認証情報及び該利用者に関連づけた他の携帯性を有する通信端末を識別する利用端末ＩＤを記憶するメモリを備えた近距離通信デバイスと近距離通信する近距離通信処理と、
前記近距離通信処理で前記近距離通信デバイスから認証情報を取得して、該認証情報を、利用を許可する利用者の認証情報を登録認証情報として記憶する認証情報記憶手段の該登録認証情報と照合して一次認証処理を行う一次認証処理と、
前記一次認証処理で前記一次認証に成功すると、前記近距離通信処理で近距離通信を行わせて通信端末から該通信端末の端末ＩＤを取得させ、該通信端末の端末ＩＤを前記利用端末ＩＤと照合して二次認証処理を行う二次認証処理と、
前記二次認証処理で認証に成功すると、前記情報処理装置の利用を許可する制御処理と、
を実行させるための認証プログラム。
【請求項１４】
請求項１３記載の認証プログラムを記録したことを特徴とするコンピュータが読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、認証システム、認証方法、認証プログラム及び記録媒体に関し、詳細には、近接無線通信を利用した個人認証を行う情報処理装置、認証システム、認

証方法、認証プログラム及び記録媒体に関する。
【背景技術】
【０００２】
近年、情報の機密を確保することが重要な課題となってきており、また、近接無線通信（ＮＦＣ：Near Field Communications、以下、ＮＦＣという。）が普及し、例えば、複写装置、プリンタ装置、複合装置、コンピュータ等の情報処理装置においても、ＮＦＣを利用したＩＣカード（Integrated Circuit Card）等にユーザのＩＤを記憶するとともに、情報処理装置がＮＦＣリード／ライタを搭載して、情報処理装置を利用しようとするユーザの携帯するＩＣカードのユーザＩＤを読み取って情報処理装置の利用の可否を制御することが行われている。
【０００３】
ところが、このようなＩＣカードを用いた認証方法においては、盗難等によって悪意の第３者にＩＣカードがわたると、情報処理装置が不正利用されるおそれがある。すなわち、従来の機密保持技術にあっては、ＩＣカード等のＮＦＣデバイスの利用者が、証明書情報等の登録者であるとみなしているため、ＮＦＣデバイスの盗難・紛失時に悪意のあるユーザが不正利用を行おうとした場合、該ＮＦＣを利用して、本来の登録者になりすまして、情報処理装置に簡単にアクセスすることができ、情報処理装置内部の情報の盗難・改ざんが容易に行われるおそれがあった。
【０００４】
そこで、従来、電子バリューを記憶するＩＣカード及びＩＣカード機能付き携帯端末を利用してサービス端末の利用や保守操作を行うシステムにおいて、保守操作を行うための権限情報を記憶するＩＣカード機能付き携帯端末が、権限情報発行サーバから該権限情報を取得して、サービス端末が、ＩＣカード機能付き携帯端末と通信して該権限情報を取得して照合し、保守操作を許可した場合にのみ、扉を開錠して保守操作モードで動作する技術が提案されている（特許文献１参照）。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記従来技術にあっては、ＩＣカード機能付き携帯端末の権限情報を確認するために権限情報発行サーバと連携する必要がある。その結果、複雑な基幹ネットワークシステムを構築する必要があるとともに、該基幹ネットワークに接続する必要があり、コストが高くなるとともに、情報の機密を保持するためのシステムとして大型で利用性が悪いという問題があった。
【０００６】
そこで、本発明は、利用を要求している利用者の認証を安価にかつ確実に行う情報処理装置、認証システム、認証方法、認証プログラム及び記録媒体を提供することを目的としている。
【課題を解決するための手段】
【０００７】
本発明は、上記目的を達成するために、利用者の認証情報及び該利用者に関連づけた他の携帯性を有する通信端末を識別する利用端末ＩＤを記憶するメモリを備えた近距離通信デバイスと近距離通信し、該近距離通信デバイスから認証情報を取得して、該認証情報を、利用を許可する利用者の認証情報を登録認証情報として記憶する認証情報記憶手段の該登録認証情報と照合して一次認証処理を行って、該一次認証に成功すると、近距離通信を行って通信端末から該通信端末の端末ＩＤを取得して、該通信端末の端末ＩＤを該利用端末ＩＤと照合して二次認証処理を行って、該二次認証処理で認証に成功すると、情報処理装置の利用を許可することを特徴としている。
【発明の効果】
【００１３】
本発明によれば、利用を要求している利用者の認証を安価にかつ確実に行うことができ

る。
【図面の簡単な説明】
【００１４】
【図１】本発明の一実施例を適用した認証システムのシステム構成図。
【図２】他の認証システムのシステム構成図。
【図３】ＮＦＣデバイスのブロック構成図。
【図４】複合装置のブロック構成図。
【図５】複合装置の要部機能ブロック構成図。
【図６】認識処理に関する機能ブロック構成図。
【図７】認識処理を示すフローチャート。
【図８】通知画面の一例を示す図。
【図９】初回登録処理を示すフローチャート。
【発明を実施するための形態】
【００１５】
以下、本発明の好適な実施例を添付図面に基づいて詳細に説明する。なお、以下に述べる実施例は、本発明の好適な実施例であるので、技術的に好ましい種々の限定が付されているが、本発明の範囲は、以下の説明によって不当に限定されるものではなく、また、本実施の形態で説明される構成の全てが本発明の必須の構成要件ではない。
【実施例１】
【００１６】
図１～図９は、本発明の情報処理装置、認証システム、認証方法、認証プログラム及び記録媒体の一実施例を示す図であり、図１は、本発明の情報処理装置、認証システム、認証方法、認証プログラム及び記録媒体の一実施例を適用した認証システム１のシステム構成図である。
【００１７】
図１において、認証システム１は、複合装置（情報処理装置）２がＮＦＣリーダ／ライタ（ＮＦＣ　Ｒ／Ｗ）３を備えており、ＮＦＣリーダ／ライタ（近距離通信手段）３は、通信可能な近距離に存在するＮＦＣデバイス４と通信を行うとともに、近距離にあるＮＦＣ対応の通信端末である携帯通信端末５（図３に示すＲＦＩＤ（Radio Frequency-Identification：電波方式認識）５ａ、ＩＣカード５ｂ等）と通信を行う。
【００１８】
また、認証システム１は、図２に示すように、複合装置２が、インターネット、ＷＡＮ（Wide Area Network ）、ＬＡＮ（Local Area Network）等の有線／無線のネットワークＮＷに接続されていて、ネットワークＮＷには、アクセスポイント装置６、電子メールサーバ７及びＣＡ（認証局）８等が接続されていてもよい。図２の場合、複合装置２は、１台のみが接続されている状態を示しているが、複数台が接続されていてもよい。
【００１９】
認証局（ＣＡ）８は、複合装置２を使用する利用者からの要求に応じて、該利用者を認証する認証情報を発行する。
【００２０】
電子メールサーバ７は、複合装置２の利用者、認証局（ＣＡ）８、認証システム１の管理者等の間の電子メールの授受を行う。
【００２１】
アクセスポイント装置６は、ネットワークＮＷへの無線／有線のアクセスポイントである。
【００２２】
ＮＦＣデバイス４は、図３に示すように、通信部１１、ＮＦＣコントローラ部１２及びアンテナ部１３等を備えており、ＮＦＣコントローラ部１２は、制御部１４と複数のメモリ１５ａ～１５ｎ等を備えている。メモリ１５ａ～１５ｎは、ネットワーク設定に必要なアソシエーション情報、個人毎またはデバイス毎の証明書情報（認証情報）及び複合装置

２を操作する利用者を特定するための携帯通信端末５の利用端末ＩＤ等が格納されており、通信部１１がアンテナ１３を介して周辺のＮＦＣリーダ／ライタ３等と通信を行って、ＮＦＣコントローラ部１２がメモリ１５ａ～１５ｎ内のデータを読み取ってＮＦＣリーダ／ライタ３等に送信したり、通信相手のＮＦＣリーダ／ライタ３から受け取ったデータをメモリ１５ａ～１５ｎに書き込む。

【００２３】

複合装置２は、図４に示すように、コントローラ１００、操作部１０１、ファックス制御ユニットファックス制御ユニット１０２、プロッタ１０３、スキャナ１０４、これら以外のハードウェアリソースであるその他のハードウェアリソース１０５等を備えているとともに、上記ＮＦＣリーダ／ライタ３がコントローラ１００に接続されている。

【００２４】

コントローラ（制御手段）１１０は、ＣＰＵ（Central Processing Unit）１１１、タイマ１１２、ＲＯＭ（Read Only Memory）１１３、ＲＡＭ（Random Access Memory）１１４、ＡＳＩＣ（Application Specific Integrated Circuit）１１５、ＲＡＭ１１６、ＨＤＤ（Hard Disk Drive）１１７、シリアルバスＩ／Ｆ１１８、ＮＩＣ（Network Interface Card）１１９、ＷＬＡＮ　Ｉ／Ｆ１２０、ＵＳＢ（Universal Serial Bus）デバイスＩ／Ｆ１２１、ＵＳＢホスト１２２、メモリカードＩ／Ｆ１２３等を備えている。

【００２５】

操作部１０１は、コントローラ１００のＡＳＩＣ１１５に接続されており、ファックス制御ユニット１０２、プロッタ１０３、スキャナ１０４及びその他のハードウェアリソース１０５は、コントローラ１００のＡＳＩＣ１１５にＰＣＩ（Peripheral Component Interconnect）バスで接続されている。また、シリアルバスＩ／Ｆ１１８、ＮＩＣ１１９、ＷＬＡＮ１２０、ＵＳＢデバイス１２１、ＵＳＢホスト１２２及びメモリカードＩ／Ｆ１２３は、コントローラ１００のＡＳＩＣ１１５にＰＣＩバスで接続されている。

【００２６】

コントローラ１１０は、ＣＰＵ１１１が、ＲＯＭ１１３やＨＤＤ１１７内のプログラムに基づいて、ＲＡＭ１１４をワークメモリとして利用して、複合装置２の各部を制御して、複合装置２としての基本処理を実行するとともに、後述する本発明の認証制御処理を実行する。

【００２７】

すなわち、複合装置２は、ＲＯＭ、ＥＥＰＲＯＭ（Electrically Erasable and Programmable Read Only Memory ）、ＥＰＲＯＭ、フラッシュメモリ、フレキシブルディスク、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory ）、ＣＤ－ＲＷ（Compact Disc Rewritable ）、ＤＶＤ（Digital Versatile Disk）、ＳＤ（Secure Digital）カード、ＭＯ（Magneto-Optical Disc）等のコンピュータが読み取り可能な記録媒体に記録されている本発明の認証方法を実行する認証プログラムを読み込んでＲＯＭ１１３やハードディスク１１７等に導入することで、後述する複合装置２の操作を許可された利用者を確実に認証する認証方法を実行する情報処理装置として構築されている。この認証プログラムは、アセンブラ、Ｃ、Ｃ＋＋、Ｃ＃、Ｊａｖａ（登録商標）等のレガシープログラミング言語やオブジェクト指向ブログラミング言語等で記述されたコンピュータ実行可能なプログラムであり、上記記録媒体に格納して頒布することができる。

【００２８】

タイマ１１２は、発振器や分周器等を備え、現在時刻を計時して、ＣＰＵ１１１に通知するとともに、複合装置２の各部の動作タイミングをとるためのクロックを生成する。

【００２９】

ＡＳＩＣ１１５は、画像処理用のハードウェア要素を有する画像処理用途向けのＩＣであり、各デバイスを接続するブリッジの役割をも有している。

【００３０】

ＲＡＭ１１６は、ＡＳＩＣ１１５が処理を行う際にプログラムや中間処理データを一時的に記憶するのに使用され、ＨＤＤ（認証情報記憶手段）１１７は、ＣＰＵ１１１が実行

する制御プログラム及び画像データ、文書データ、フォントデータ、フォームデータ等の各種データを保管するとともに、後述するＮＦＣを利用した利用者認証（一次認証）における利用者認証情報（証明証情報）等を登録認証情報として保管する。

【００３１】

シリアルバスＩ／Ｆ１１８は、複合装置２と図示しない周辺機器をシリアル接続し、ＮＩＣ１１９は、図示しない拡張スロット等に接続された拡張カードであってＬＡＮ接続のインターフェイスであって、ネットワーク上の他の複合装置やサーバ等と通信を行う。

【００３２】

ＵＳＢデバイスＩ／Ｆ１２１は、複合装置２と図示しないＵＳＢ対応の周辺機器をＵＳＢケーブルにより接続して、該周辺機器との通信を行う。

【００３３】

ＵＳＢホスト１２２には、ＵＳＢケーブルによりＮＦＣリーダ／ライタ３が接続され、ＵＳＢホスト１２２は、該ＮＦＣリーダ／ライタ３と通信するための物理的・電気的Ｉ／Ｆを制御する機能及びＵＳＢプロトコルを制御する機能を有して、ＮＦＣリーダ／ライタ３と通信する。

【００３４】

メモリカードＩ／Ｆ１２３には、コンパクトフラッシュメモリ（登録商標）、メモリスティック（ＭＳ）、スマートメディア等の図示しないメモリカードが接続され、メモリカードＩ／Ｆ１２３は、接続されたメモリカードへのデータの書き込み及びメモリカードからのデータの読み出しのインターフェイスを行う。

【００３５】

操作部（警告手段）１０１は、各種操作キーやディスプレイ等を備え、利用者による各種操作キーからの入力操作を受け付けるとともに、利用者に対してディスプレイに各種情報の表示を行う。操作部１０１は、特に、後述する認証処理において利用者情報等の入力操作等が行われる。

【００３６】

ファックス制御ユニット１０２には、電話回線等が接続され、Ｇ３、Ｇ４の通信プログラムに基づいて、相手ファクシミリ装置等のファクシミリ通信機能を備えた装置との間でファクシミリ文書の送受信を行う。

【００３７】

プロッタ１０３は、所定の印刷方式、例えば、電子写真方式で印刷対象の画像データに基づいて画像を用紙に記録出力する。プロッタ１０３は、電子写真方式の場合、図示しないが、レーザを用いた電子写真方式で用紙に画像データを記録出力するのに必要な部品、例えば、感光体、光書込部、現像部、帯電部及びクリーニング部等を備えている。プロッタ１０３は、画像データ及び制御信号により光書込部を動作させて感光体上に静電潜像を形成し、現像部によりトナーを感光体上に供給して現像してトナー画像を形成する。プロッタ１０３は、給紙部から用紙搬送路を経由させて用紙を感光体と転写部との間に給紙して、感光体上のトナー画像を用紙に転写させ、トナー画像の転写された用紙を定着部に搬送して、定着部で加熱・加圧して用紙上のトナー画像を定着させることで、画像を用紙に印刷出力する。

【００３８】

スキャナ１０４は、原稿の画像を主走査及び副走査して、該原稿の画像を所定の解像度で読み取って、画像データを取得する。

【００３９】

その他のハードウェアリソース１０５は、外付けハードウェア等である。

【００４０】

上記ＮＦＣリーダ／ライタ３は、ＵＳＢホスト１２２に接続され、該ＵＳＢホスト１２２を介してＣＰＵ１１１の制御下で、ＮＦＣ規格に基づいて所定の近距離にある上記ＮＦＣデバイス４や携帯通信端末５と通信して、データの転送・交換を行う。複合装置２は、このＮＦＣリーダ／ライタ３とＮＦＣデバイス４との間の通信によって、ＮＦＣデバイス

４のメモリ１５ａ～１５ｎに格納されているネットワーク設定に必要なアソシエーション情報、複合装置２の操作が許可されている利用者の証明証情報等の認証情報（利用者認証情報）、該利用者の携帯通信端末５を特定する利用端末ＩＤ及び利用者認証情報にアクセスするための鍵情報等のデータを取得したり、該データを更新したりする。

【００４１】

また、ＮＦＣリーダ／ライタ３は、ＣＰＵ１１１の制御下で、所定時間各毎に、ＮＦＣ規格に基づいて所定の近距離にあるＮＦＣ機能を搭載する携帯通信端末５と通信し、該携帯通信端末５のメモリに格納されている該携帯通信端末５の利用端末ＩＤを取得して、コントローラ１００のＣＰＵ１１１に渡す。

【００４２】

ＣＰＵ１１１は、ＮＦＣリーダ／ライタ３が取得した端末ＩＤが上記ＮＦＣデバイス４に登録されている利用端末ＩＤと一致するか否かチェックして、一致するときには二次認証に成功したとして、該ＮＦＣデバイス４を所持する利用者による複合装置２の操作を許可し、両端末ＩＤが一致しないか、携帯通信端末５から端末ＩＤを取得できない時間が所定時間継続すると、複合装置２の操作を禁止する認証処理を行う。

【００４３】

そして、ＮＦＣ対応の携帯通信端末５は、何ら限定されるものではないが、携帯性に富み、悪意の第３者から通信していることがわからない程度の大きさ等であることが望ましい。このような携帯通信端末５としては、例えば、ＮＦＣ対応のＩＣカード５ａ、ＲＦＩＤ端末５ｂ、ＮＦＣ搭載携帯電話等を用いることができる。

【００４４】

そして、複合装置２は、ＣＰＵ１１１がＵＳＢホスト１２２を介してＮＦＣリーダ／ライタ３に対してコマンドを送信することで、ＮＦＣデバイス４及び携帯通信端末５とのＮＦＣによる通信を行うが、ＵＳＢホスト１２２とＮＦＣリーダ／ライタ３とはＵＳＢケーブルで接続されているため、このＵＳＢの通信系路における上記ネットワークアソシエーション情報、個別の証明書情報、利用者認証情報、端末ＩＤ及び利用者認証情報にアクセスするための鍵情報等のデータが、ＵＳＢバスがモニターされることによって漏洩することを防止するために、ＵＳＢバス上のコマンド及びデータの送受信を暗号化している。なお、暗号化するためには、ＵＳＢホスト１２２とＮＦＣリーダ／ライタ３との間の認証が必要であるため、暗号化を行う前に、まず、ＵＳＢホスト１２２とＮＦＣリーダ／ライタ３との間の認証を行い、認証結果に基づいて共通鍵を生成して、この共通鍵を利用して暗号化（及び復号化）を行うことで、ＵＳＢバスを利用した通信の安全を確保している。

【００４５】

そして、複合装置２は、基本プログラム及び本発明の認証プログラムが導入されて実行されることで、図５に示すような機能ブロックが構築される。

【００４６】

図５において、複合装置２は、ＵＮＩＸ（登録商標）等のオペレーティングシステム（以下、ＯＳという）２００上に起動されているアプリケーションモジュール層２１０とサービスモジュール層２２０及びハードウェア層３００を備えている。アプリケーションモジュール層２１０とサービスモジュール層２２０とはＡＰＩ（Application Program Interface ）によって機能接続されており、ＯＳ２００とハードウェア層３００とは、エンジンＩ／Ｆによって情報の授受が可能となっている。

【００４７】

アプリケーションモジュール層２１０は、コピー、ファックス、プリンタ、スキャナ及びＷｅｂ等の画像形成に関連するそれぞれ固有の処理を行うプログラムを含んでおり、コピーに係る機能を実現するコピーアプリケーション２１１、ファックス送受信に係る機能を実現するファックスアプリケーション２１２、プリンタ出力に係る機能を実現するプリンタアプリケーション２１３及びウェブ（Ｗｅｂ）通信に係る機能を実現するウェブアプリケーション２１４等を含んでいる。

【００４８】

サービスモジュール層２２０は、システム制御サービス２２１、ファックス制御サービス２２２、エンジン制御サービス２２３、メモリ制御サービス２２４、操作部制御サービス２２５、ネットワーク制御サービス２２６及び認証制御サービス２２７等のサービスモジュールを含んでいる。

【００４９】

サービスモジュール層２２０は、アプリケーションモジュール層２１０からの処理要求を解釈してハードウェア資源３００の獲得要求を発生する。

【００５０】

ハードウェア資源３００には、上記プロッタエンジン１０３、スキャナエンジン１０４、その他のハードウェアリソース１０５等を備えているとともに、これらのハードウェアを確保して制御するエンジン制御ボード３０１を備えている。

【００５１】

ＯＳ２００は、アプリケーションモジュール層２１０及びサービスモジュール層２２０の各ソフトウェアをプロセスとして並列実行する。

【００５２】

システム制御サービス２２１は、アプリケーション２１１～２１４の管理、操作部１０１の制御、システム画面表示、ＬＥＤ（Light Emitting Diode）の表示、ハードウェア資源３００の管理、割り込みアプリケーション制御等の処理を行い、ファックス制御サービス２２２は、ファクシミリ機能を実現するモジュールである。エンジン制御サービス２２３は、プロッタエンジン１０３、スキャナエンジン１０４及びその他のハードウェアリソース１０５を制御するモジュールである。

【００５３】

メモリ制御サービス２２４は、メモリ制御を行うモジュールであり、操作部制御サービス２２５は、操作部１０１を制御するモジュールである。

【００５４】

ネットワーク制御サービス２２６は、ネットワークＩ／Ｏを必要とするアプリケーションに対して共通に利用できるサービスを提供するものであり、ネットワーク側から各プロトコルによって受信したデータを各アプリケーション２１１～２１４に振り分けを行い、また、各アプリケーション２１１～２１４からのデータをネットワーク側に送信する際の仲介を行う。例えば、ネットワーク制御サービス２２６は、ネットワークを介して接続されるネットワーク機器、例えば、ホスト装置やサーバ等とのデータ通信を制御する。

【００５５】

認証制御サービス２２７は、上記各アプリケーション２１１～２１４を利用するための利用者認証を行い、具体的には、ＮＦＣリーダ／ライタ３を用いたＮＦＣデバイス４及び携帯通信端末５との認証情報と端末ＩＤによる利用者認証処理を実行する。

【００５６】

そして、複合装置２は、認証処理に関しては、さらに、詳細には、図６に示すような機能ブロックが構築される。すなわち、複合装置２は、アプリケーションモジュール層２１０の各アプリケーション２１１～２１４を利用するために、認証制御サービス２２７によるＮＦＣを用いた認証を必要とし、この認証制御サービス２２７による認証処理を実行するために、ＮＦＣリソースマネージャ２３１、ＮＦＣリーダ／ライタ（ＮＦＣ　Ｒ／Ｗ）デバイスドライバ２３２、ＵＳＢホストデバイスドライバ２３３、ネットワークライブラリ２３４、無線ドライバ２３５、アドレス帳データベース（ＤＢ）２３６、ファイルシステム２３７、ＨＤＤドライバ２３８、描画処理モジュール２３９及びグラフィックドライバ２４０等を利用する。

【００５７】

すなわち、ＮＦＣを利用した認証制御サービス２２７は、上記各アプリケーション２１１～２１４から認証要求やＮＦＣデバイス４及び携帯通信端末５とのペアリングまたはアソシエーション要求を受け付けると、描画処理モジュール２３９及びグラフィックドライバ２４０を経由して操作部（オペレーションパネル）１０１へ所定の認証関連情報の表示

処理を行う。認証制御サービス２２７は、ＮＦＣリソースマネージャ２３１を介して、ＵＳＢ接続されたＮＦＣリーダ／ライタ３を制御するＮＦＣ　Ｒ／Ｗデバイスドライバ２３２及びＵＳＢホストデバイスドライバ２３３を通じて、ＮＦＣデバイス４及び携帯通信端末５と通信して、アソシエーションまたはペアリングのための設定情報や証明書情報及び携帯通信端末５を識別するための端末ＩＤを取得し、取得した証明書情報を、ＨＤＤ１１７に設けられた認証用のアドレス帳ＤＢ（図示せず）に対して、このアドレス帳ＤＢを管理するアドレス帳ＤＢモジュール２３６を利用して、ファイルシステム２３７及びＨＤＤドライバ２３８を通じて問い合わせ、または、ネットワークライブラリ２３４を利用して、ＷＬＡＮ　Ｉ／Ｆ１２０やＮＩＣ１１９等の無線ドライバ２３５を用いてアクセスポイント装置６を介して、または、直接、ネットワークＮＷに接続された外部の認証局（ＣＡ）８に対して問い合わせを行う。認証制御サービス２２７は、問い合わせ途中の詳細情報や問い合わせた結果として、一次認証が成功したか、失敗したかをアプリケーション２１１～２１４へ出力する。

【００５８】

また、認証制御サービス２２７は、所定時間間隔で、ＮＦＣリソースマネージャ２３１、ＮＦＣリーダ／ライタ（ＮＦＣ　Ｒ／Ｗ）デバイスドライバ２３２及びＵＳＢホストデバイスドライバ２３３を介して、近距離の携帯通信端末５と通信を試行して、上記ＮＦＣデバイス４から取得した利用端末ＩＤと一致する端末ＩＤを有する携帯通信端末５と通信が可能であるか否かによって、ＮＦＣデバイス４を所持している利用者が正規の利用者であるか否かの二次認証処理を行う。

【００５９】

ここで、ＮＦＣリソースマネージャ２３１は、ＮＦＣに対応したリソース管理機能を提供し、優先順位に応じて複数のアプリケーション間での各種ハードウェアリソースの割り当てを可能にする。ＵＳＢホストデバイスドライバ２３３は、ＵＳＢ接続されたデバイスを制御対象とするのか否かを判断し、ＮＦＣ　Ｒ／Ｗデバイスドライバ２３２は、ＵＳＢ接続されたＮＦＣリーダ／ライタ３を初期化したり、所定の設定を行ったりする。ＨＤＤドライバ２３８は、ＨＤＤ１１７を駆動制御するデバイスドライバであって、ファイルシステム２３７は、ＨＤＤ１１７に格納されるファイルを管理し、そのセキュリティや信頼性確保などの機能も有するプログラムである。なお、認証用のアドレス帳ＤＢには、登録された証明書情報（認証情報）と、利用者毎に証明書情報が設けられている場合は、その証明書情報に利用者の電子メールアドレスが対応付けられて格納され、また、ＮＦＣデバイス４と対応づけられた携帯通信端末５の利用端末ＩＤが格納される。

【００６０】

次に、本実施例の作用について説明する。本実施例の認証システム１は、複合装置２を利用しようとする利用者が、ＮＦＣデバイス４と携帯通信端末５の双方がそろっていることを条件に利用が許可される。

【００６１】

すなわち、複合装置２は、ＮＦＣを利用したＮＦＣデバイス４による利用者認証（一次認証）と、該ＮＦＣデバイス４の所有者が正規の所有者であるかを、ＮＦＣデバイス４に登録されている端末ＩＤの携帯通信端末５を該利用者が所持しているか否かの二次認証によって確認する。

【００６２】

そこで、複合装置２は、複合装置２を利用しようとする利用者が、ネットワーク設定に必要なアソシエーション情報、個人毎またはデバイス毎の証明書情報がメモリ１５ａ～１５ｎに登録されているＮＦＣデバイス４を所持して、複合装置２の利用に先立って、ＮＦＣリーダ／ライタ３にかざすと、複合装置２は、ＣＰＵ１１の制御下で、認証プログラムに基づいて、ＵＳＢホスト１２２を介してＮＦＣリーダ／ライタ３を動作させて、ＮＦＣデバイス４との間で、通信を開始して、ネットワークアソシエーションまたはペアリングや一次認証処理を行う（ステップＳ１０１）。

【００６３】

複合装置２は、一次認証が正常に完了すると、認証したＮＦＣデバイス４のメモリ１１５ａ～１５ｎに保管されている携帯通信端末５の利用端末ＩＤを取得する。ＮＦＣデバイス４は、利用端末ＩＤを、メモリ１５ａ～１５ｎの容量に応じて複数保管することができる。

【００６４】

複合装置２は、ＮＦＣデバイス４のメモリ１５ａ～１５ｎに保管されているか否か、または、データベース（ＤＢ）のアクセス情報等を参照して、ＮＦＣデバイス４が初回の利用であって、メモリ１５ａ～１５ｎに利用端末ＩＤが登録されていないかを判定する（ステップＳ１０２）。

【００６５】

ＮＦＣデバイス４が初回の利用（一度目の利用）であると（ステップＳ１０２で、ＮＯの場合）には、携帯通信端末５の利用端末ＩＤの初回登録処理を行い（ステップＳ１０３）、ＮＦＣデバイス４から登録済みの利用端末ＩＤを取得可能であるかチェックする（ステップＳ１０４）。なお、初回登録処理については、後述する。

【００６６】

ステップＳ１０４で、ＮＦＣデバイス４から利用端末ＩＤを取得できないときには、複合装置２は、不正なＮＦＣデバイスであると判断して、処理を終了する。

【００６７】

この場合、複合装置２は、例えば、図８に示すような通知画面Ｇを操作部１０１のディスプレイに表示する。

【００６８】

ステップＳ１０４で、ＮＦＣデバイス４に登録されている利用端末ＩＤを該ＮＦＣデバイス４から取得できたときには、複合装置２は、取得した利用端末ＩＤをＨＤＤ１１７等に保管し、ＮＦＣリーダ／ライタ３から周辺の携帯通信端末５に向けて信号を飛ばして、予め設定されている設定期間内に携帯通信端末５からの信号を取得できたか判断する（ステップＳ１０５）。

【００６９】

ステップＳ１０５で、設定期間内に信号を受信すると、複合装置２は、受信した信号をエンコードして、該信号から携帯通信端末５の端末ＩＤを取得して、携帯通信端末５から取得した端末ＩＤが、ＮＦＣデバイス４から取得した利用端末ＩＤと一致するかチェックする（ステップＳ１０６）。

【００７０】

複合装置２は、携帯通信端末５から暗号化された端末ＩＤを取得すると、セキュリティを向上させるために、携帯通信端末５の端末ＩＤが、暗号化されているので、暗号化されている該端末ＩＤを、ＨＤＤ１１７等に保管管理している暗号鍵を用いて復号化し、この携帯通信端末５から受信して復号化した端末ＩＤとＮＦＣデバイス４から取得してＨＤＤ１１７等に保管している利用端末ＩＤが一致するかチェックする。

【００７１】

ステップＳ１０６で、両端末ＩＤが一致しないときには、複合装置２は、ステップＳ１０５に戻って、設定期間内に携帯通信端末５から端末ＩＤを受信したかのチェックから上記同様に処理し（ステップＳ１０５、Ｓ１０６）、一致する端末ＩＤを受信することなく、ステップＳ１０５で、設定期間内に信号を携帯通信端末５からの信号を取得しないときには、ＮＦＣ４による認証が不正な認証であるとして、処理を終了する。

【００７２】

この場合、複合装置２は、例えば、図８に示したような通知画面Ｇを操作部１０１のディスプレイに表示する。

【００７３】

また、この場合の利用者は、ＮＦＣデバイス４の正規の所有者ではない者（悪意の第３者等）である可能性があるため、警告音で周辺の人に通知し、また、ネットワークＮＷを通して複合装置２の管理者やデータベース等に登録されたＮＦＣデバイス４の所有者に電

子メール等で連絡する等の警報処理を行ってもよい。この場合、音を発生させる機構及び電子メールを送信する機構が警告手段として機能する。

【００７４】

ステップＳ１０６で、両端末ＩＤが一致すると、複合装置２は、コントローラ１００の制御下で、複合装置２のアプリケーションの利用を可能とし（ステップＳ１０７）、アプリケーションの利用を許可すると、予め設定されている監視期間毎に、ＮＦＣリーダ／ライタ３からＮＦＣデバイス４に信号を飛ばして、ＮＦＣデバイス４と通信が可能かチェックする（ステップＳ１０８）。

【００７５】

ステップＳ１０８で、ＮＦＣデバイス４と通信可能であると、複合装置２は、複合装置２の利用許可を継続して、再度、監視期間毎にＮＦＣデバイス４との通信が可能かのチェックを繰り返し行い（ステップＳ１０７、Ｓ１０８）。

【００７６】

ステップＳ１０８で、ＮＦＣデバイス４との通信が不可能な状態が監視期間以上経過すると、認証した利用者による複合装置２の利用が終了したと判断して、複合装置２のセキュリティを確保するために、複合装置２のアプリケーション２１１～２１４の利用を禁止して、処理を終了する。

【００７７】

なお、ステップＳ１０８でセキュリティ向上のために、利用者の確認を行うのは、ＮＦＣデバイス４との通信確認に限るものではなく、例えば、ＮＦＣデバイス４に予め登録されている携帯通信端末５がＮＦＣによる通信圏内にあるか、すなわち、携帯通信端末５を所持した利用者が近くにいるかを確認してもよいし、ＮＦＣデバイス４と携帯通信端末５の両方と通信して、一次認証と二次認証の両方を行ってもよい。

【００７８】

この携帯通信端末５は、上述のように、小型で、ウェアラブルなもの（携帯性に富んだもの）であることが望ましい。すなわち、携帯通信端末５が、ウェアラブルなものであれば、利用者が複合装置２の利用を終了時に、ＮＦＣデバイス４を複合装置２の上等に置き忘れてその場を去ってしまって、悪意の第３者がＮＦＣデバイス４を持ち去っても、携帯通信端末５を携帯した利用者が複合装置２からの信号を受信できない距離まで離れていると、携帯通信端末５との通信が途絶えるため、悪意の第３者が複合装置２のアプリケーションを利用することができなくなる。複合装置２を利用することができなくなると、ＮＦＣデバイス４のメモリ１５ａ～１５ｎの暗号化された端末ＩＤを復号化することができず、ＮＦＣデバイス４のメモリ１５ａ～１５ｎに登録されている携帯通信端末５を特定することがでいない。また、携帯通信端末５が、小型であれば、複合装置２を利用するための認証を行っているところを他人に見られても、視覚によっては、認証に用いられた携帯通信端末５を特定することができず、セキュリティをより一層向上させることができる。

【００７９】

そして、複合装置２は、上記ステップＳ１０３の初回登録処理を、図９に示すように実行する。すなわち、利用者は、複合装置２を利用して、ＮＦＣ４に対して携帯通信端末５の登録を行うには、ＮＦＣデバイス４をＮＦＣリーダ／ライタ３にかざしてＮＦＣデバイス４を認証させ、ＮＦＣデバイス４の認証が完了すると、認証プログラムによる携帯通信端末５の登録要求を行う。複合装置２は、ＮＦＣデバイス４への携帯通信端末５の端末ＩＤの初回登録が要求されると、ＣＰＵ１１１がＵＳＢホスト１２２を介してＮＦＣリーダ／ライタ３から周辺の携帯通信端末５との間で信号の送受信を行い（ステップＳ２０１）、携帯通信端末５から受信した携帯ＩＤを操作部１０１のディスプレイに表示させて、利用者による登録対象の端末ＩＤの選択を要求する（ステップＳ２０２）。この場合、利用者は、複数の携帯通信端末５から受信すると、利用者の意図する携帯通信端末以外を登録してしまう恐れがあるので、受信できるのは一つの携帯通信端末５からのみという環境で行うことが望ましい。

【００８０】

複合装置２は、登録対象の端末ＩＤが選択されると、選択された端末ＩＤを暗号化した後、ＮＦＣデバイス４に利用者端末ＩＤとして書き込んで登録処理を完了する。複合装置２は、この暗号化鍵をＨＤＤ１１７等で管理する。

【００８１】

なお、複合装置２は、ＮＦＣデバイス４の認証が完了した状態であれば、ＮＦＣデバイス４に登録されている携帯通信端末５の利用端末ＩＤを、削除、追加、変更等のＩＤ更新処理を行うことができ、また、利用端末ＩＤを、複数登録することもできる。また、複合装置２は、ＮＦＣデバイス４の使用していた利用端末ＩＤを削除するときには、新しい端末ＩＤを利用端末ＩＤとして登録した後に、使用していた利用端末ＩＤを削除することで、複合装置２の利用を継続しながら端末ＩＤの変更を行うことができる。

【００８２】

また、ＮＦＣデバイス４の盗難、紛失、破損等で複合装置２の利用を行うことができなくなった場合には、新たにＮＦＣデバイス４を用意し、複合装置２のＨＤＤ１１７データベースの書き換えを管理者が行う。また、通信装置の盗難、紛失、破損等で複合装置２が使用できなくなった場合には、管理者がＨＤＤ１１７のデータベースを書き換えて、該当するＮＦＣデバイス４を初回利用の状態にすることで、携帯通信端末５の再登録が可能となる。

【００８３】

このように、本実施例の認証システム１は、複合装置２が、利用者の認証情報及び該利用者に関連づけた他の携帯性を有する携帯通信端末５を識別する利用端末ＩＤを記憶するメモリ１５ａ～１５ｎを備えた近距離通信デバイスであるＮＦＣデバイス４と、ＮＦＣリーダ／ライタ３によって近距離通信し、該ＮＦＣデバイス４から認証情報を取得して、該認証情報を、利用を許可する利用者の認証情報を登録認証情報として記憶するＨＤＤ（認証情報記憶手段）１１７の該登録認証情報と照合して一次認証処理を行って、該一次認証に成功すると、ＮＦＣリーダ／ライタ３によって近距離通信を行って通信端末から該通信端末のＩＤを取得して、該通信端末の端末ＩＤを該利用端末ＩＤと照合して二次認証処理を行って、該二次認証処理で認証に成功すると、複合装置２の利用を許可している。

【００８４】

したがって、ＮＦＣデバイス４と携帯通信端末５の両方が揃った状態でないと、複合装置２の利用を開始することができず、複合装置２のセキュリティを向上させることができるとともに、携帯性を有する携帯通信端末５を利用しているため、悪意の第３者から認証に利用していることが知られにくく、セキュリティ性をより一層向上させることができる。

【００８５】

すなわち、正規の利用者がＮＦＣデバイス４を複合装置２の上に置き忘れる等によって、悪意の第３者がＮＦＣデバイス４を入手しても、該第３者は該ＮＦＣデバイス４に端末ＩＤの登録されている携帯通信端末５を携帯していないため、複合装置２を利用することができず、ＮＦＣデバイス４を用いてのなりすましによる複合装置２の不正利用、情報の漏洩、改ざん等を防止して、複合装置２のセキュリティを確保することができる。

【００８６】

また、本実施例の認証システム１は、ＮＦＣデバイス４が、メモリ１５ａ～１５ｎに、二次認証に利用する複数の携帯通信端末５の利用端末ＩＤを記憶し、二次認証処理において、複数の利用端末ＩＤのうち１つ以上と一致する携帯通信端末５の端末ＩＤがＮＦＣリーダ／ライタ３によって取得されると、二次認証成功としている。

【００８７】

したがって、１つの携帯通信端末５が破損、紛失、盗難等となっても、簡単に他の携帯通信端末５を利用して、複合装置２を利用することができ、利用性を向上させることができるとともに、複合装置２の利用を行えることで、破損等した携帯通信端末５のＨＤＤ１１７に登録されている利用端末ＩＤの削除等の対応を適切に行うことができる。

【００８８】

さらに、本実施例の認証システム１は、複合装置２が、ＮＦＣデバイス４から取得した認証情報（ＮＦＣ）による一次認証に成功することを条件として、ＮＦＣリーダ／ライタ３を使用した近距離通信によって取得した携帯通信端末５の端末ＩＤを該一次認証したＮＦＣデバイス４に端末ＩＤとして登録している。

【００８９】

したがって、二次認証に利用する形態通信端末５を適切かつセキュリティが保たれた状態で登録することができ、利用性を向上させることができるとともに、セキュリティを向上させることができる。

【００９０】

また、本実施例の認証システム１は、複合装置２が、一次認証に成功した後、所定時間内に、携帯通信端末５を利用した二次認証処理に失敗すると、通知画面Ｇ１を操作部１０１に表示したり、管理者に電子メールを送信する等の所定の警告を発生している。

【００９１】

したがって、利用者がＮＦＣデバイス４を複合装置２上に置き忘れてしまった場合等に、その事実を瞬時に利用者に知らせることができ、利用性を向上させることができるとともに、第３者にＮＦＣデバイス４が持ち去られることを防止して、セキュリティを向上させることができる。

【００９２】

さらに、本実施例の認証システム１は、携帯通信端末５を利用した二次認証に成功して、利用を許可した後、ＮＦＣデバイス４または／及び携帯通信端末５と所定時間間隔で通信を行って、前記認証情報または／及び前記端末ＩＤを取得して、取得した該認証情報または／及び該端末ＩＤに対する一次認証または二次認証に失敗するか、該ＮＦＣデバイス４または／及び該携帯通信端末５との通信に失敗すると、許可した利用を不許可としている。

【００９３】

したがって、ＮＦＣデバイス４と携帯通信端末５の一方を置き忘れて複合装置２から離れても、第３者によって複合装置２が利用されることを防止することができ、セキュリティを向上させることができる。

【００９４】

また、本実施例の認証システム１は、所定時間間隔毎における認証に失敗するか、ＮＦＣデバイス４または／及び携帯通信端末５との通信に失敗すると、通知画面Ｇ１を操作部１０１に表示したり、管理者に電子メールを送信するとの所定の警告を発生している。

【００９５】

したがって、利用者がＮＦＣデバイス４を複合装置２上に置き忘れてしまった場合等に、その事実を瞬時に利用者に知らせることができ、利用性を向上させることができるとともに、第３者にＮＦＣデバイス４が持ち去られることを防止して、セキュリティを向上させることができる。

【００９６】

以上、本発明者によってなされた発明を好適な実施例に基づき具体的に説明したが、本発明は上記実施例で説明したものに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【産業上の利用可能性】

【００９７】

本発明は、セキュリティを向上させた複合装置、ファクシミリ装置、画像形成装置、コンピュータ等の情報処理装置、認証システム、認証方法、認証プログラム及び記録媒体に利用することができる。

【符号の説明】

【００９８】

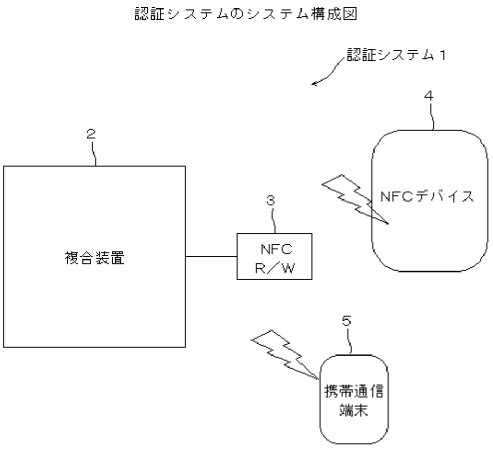
１　認証システム

２　複合装置

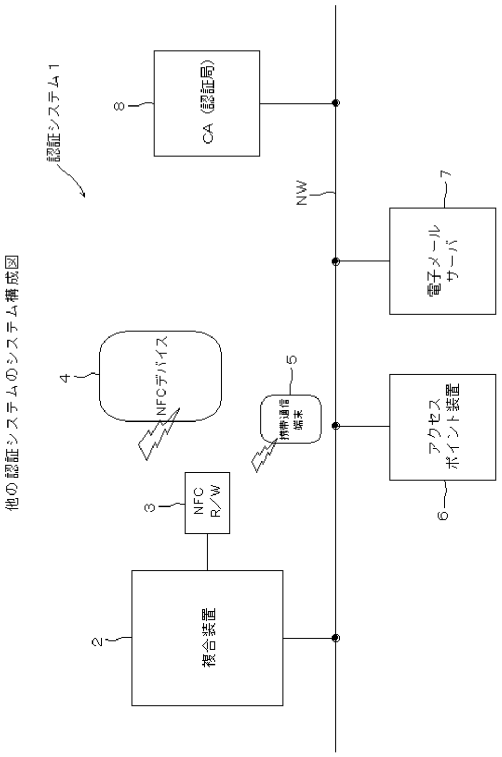
３　ＮＦＣリーダ／ライタ（ＮＦＣ　Ｒ／Ｗ）
４　ＮＦＣデバイス
５　携帯通信端末
５ａ　ＲＦＩＤ
５ｂ　ＩＣカード
ＮＷ　ネットワーク
６　アクセスポイント装置
７　電子メールサーバ
８　認証局
１１　通信部
１２　ＮＦＣコントローラ部
１３　アンテナ部
１４　制御部
１５ａ～１５ｎ　メモリ
１００　コントローラ
１０１　操作部
１０２　ファックス制御ユニットファックス制御ユニット
１０３　プロッタ
１０４　スキャナ
１０５　その他のハードウェアリソース
１１１　ＣＰＵ
１１２　タイマ
１１３　ＲＯＭ
１１４　ＲＡＭ
１１５　ＡＳＩＣ
１１６　ＲＡＭ
１１７　ＨＤＤ
１１８　シリアルバスＩ／Ｆ
１１９　ＮＩＣ
１２０　ＷＬＡＮ　Ｉ／Ｆ
１２１　ＵＳＢデバイスＩ／Ｆ
１２２　ＵＳＢホスト
１２３　メモリカードＩ／Ｆ
２００　オペレーティングシステム（ＯＳ）
２１０　アプリケーションモジュール層
２１１　コピーアプリケーション
２１２　ファックスアプリケーション
２１３　プリンタアプリケーション
２１４　ウェブアプリケーション
２２０　サービスモジュール層
２２１　システム制御サービス
２２２　ファックス制御サービス
２２３　エンジン制御サービス
２２４　メモリ制御サービス
２２５　操作部制御サービス
２２６　ネットワーク制御サービス
２２７　認証制御サービス
２３１　ＮＦＣリソースマネージャ
２３２　ＮＦＣリーダ／ライタ（ＮＦＣ　Ｒ／Ｗ）デバイスドライバ
２３３　ＵＳＢホストデバイスドライバ

２３４　ネットワークライブラリ
２３５　無線ドライバ
２３６　アドレス帳データベース（ＤＢ）
２３７　ファイルシステム
２３８　ＨＤＤドライバ
２３９　描画処理モジュール
２４０　グラフィックドライバ
３００　ハードウェア層
【先行技術文献】
【特許文献】
【００９９】
【特許文献１】特開２００６－９９２００号公報

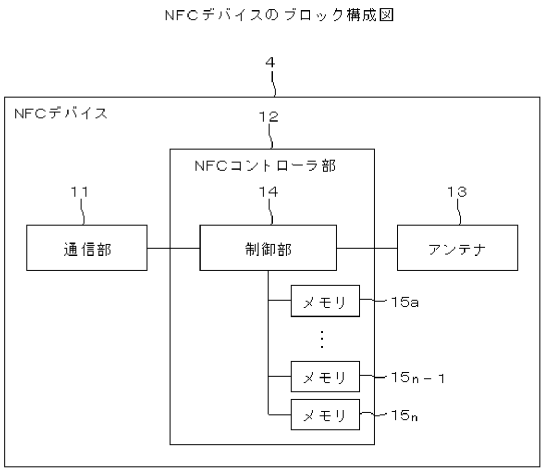
【図１】



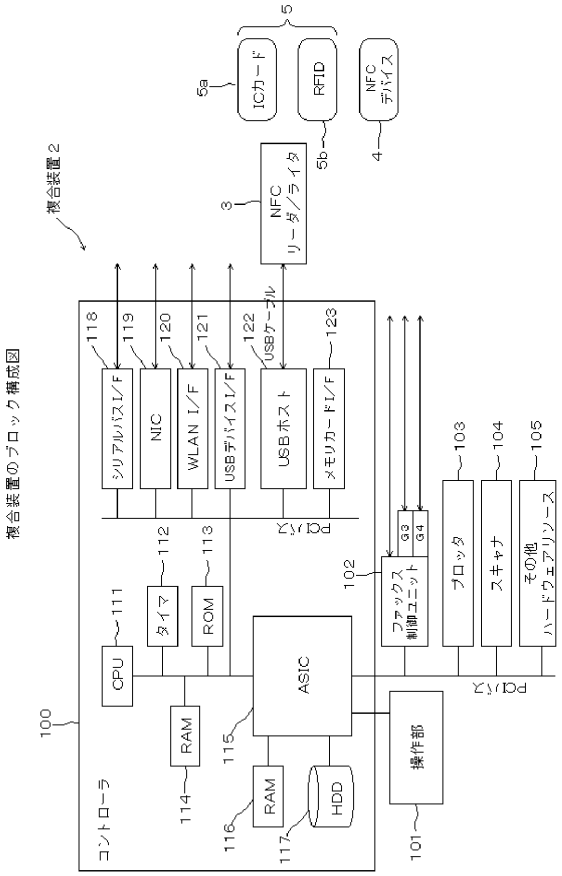
【図２】



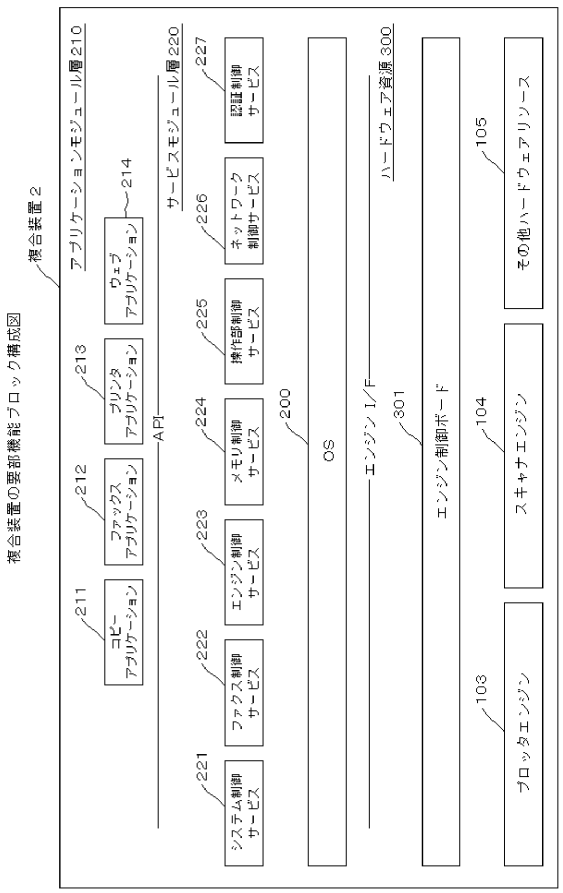
【図３】


NFCデバイスのブロック構成図
4
NFCデバイス
12
NFCコントローラ部
11
通信部
14
制御部
13
アンテナ
メモリ
15a
メモリ
15n－1
メモリ
15n

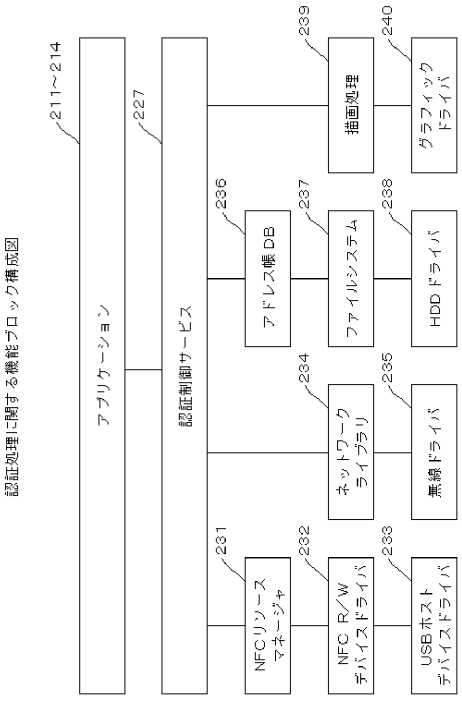
【図４】


複合装置のブロック構成図
複合装置2
5
5a
ICカード
RFID
NFC デバイス
5b
4
3
NFC リーダ／ライタ
USBケーブル
118
119
120
121
122
123
シリアルバスI/F
NIC
WLAN I/F
USBデバイスI/F
USB ホスト
メモリカードI/F
PCIバス
G3
G4
ファックス 制御ユニット
102
103
104
105
プロッタ
スキャナ
その他 ハードウェアリソース
112
113
タイマ
ROM
111
CPU
RAM
114
ASIC
115
RAM
116
HDD
117
操作部
101
100
コントローラ

【図５】

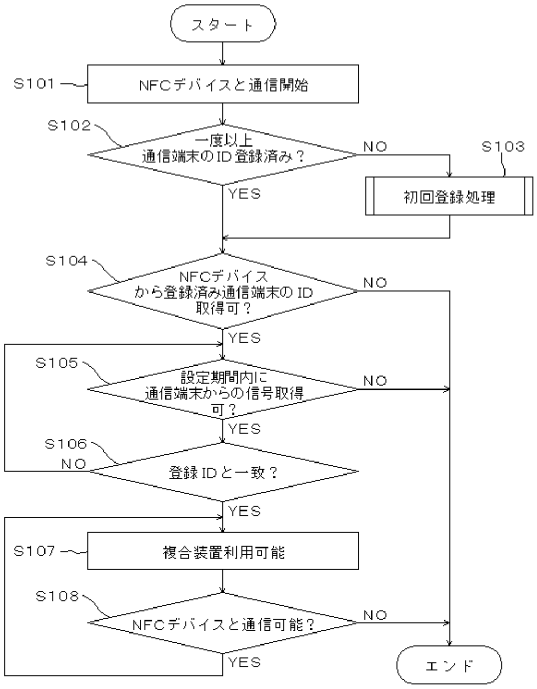

複合装置の要部機能ブロック構成図
複合装置2
アプリケーションモジュール層210
サービスモジュール層220
API
211
コピー アプリケーション
212
ファックス アプリケーション
213
プリンタ アプリケーション
214
ウェブ アプリケーション
221
システム制御 サービス
222
ファクス制御 サービス
223
エンジン制御 サービス
224
メモリ制御 サービス
225
操作部制御 サービス
226
ネットワーク 制御サービス
227
認証制御 サービス
200
OS
エンジン I/F
ハードウェア資源300
301
エンジン制御ボード
103
プロッタエンジン
104
スキャナエンジン
105
その他ハードウェアリソース

【図６】


認証処理に関する機能ブロック構成図
211～214
アプリケーション
227
認証制御サービス
231
NFCリソース マネージャ
232
NFC R／W デバイスドライバ
233
USB ホスト デバイスドライバ
234
ネットワーク ライブラリ
235
無線ドライバ
236
アドレス帳 DB
237
ファイルシステム
238
HDD ドライバ
239
描画処理
240
グラフィック ドライバ

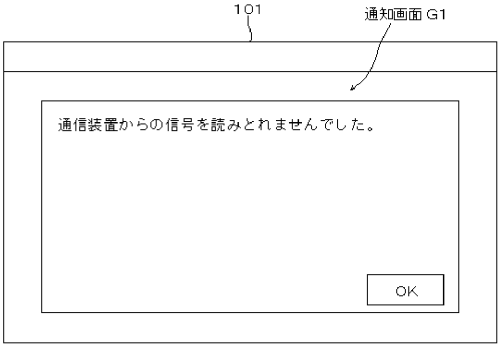
【図７】

認証処理を示すフローチャート



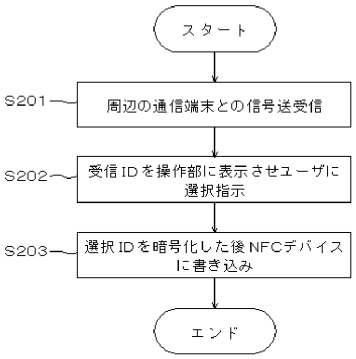
【図８】

通知画面の一例を示す図



【図９】

初回登録処理を示すフローチャート



フロントページの続き

(51)Int.Cl.		FI		
G06K 19/07	***(2006.01)***	G06K	19/00	R
G06K 17/00	***(2006.01)***	G06K	19/00	H
		G06K	17/00	F
		G06K	17/00	T

(56)参考文献 特開２００７－２０７１８７（ＪＰ，Ａ）
特開２００４－２３４６３３（ＪＰ，Ａ）
特開２００６－１０７３１６（ＪＰ，Ａ）
特開２００７－０４８３１２（ＪＰ，Ａ）
特開２００７－３１０４２６（ＪＰ，Ａ）
特開２００８－１２３３３５（ＪＰ，Ａ）
特開２００７－０２６０３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３４
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／４３
Ｇ０６Ｋ　１７／００
Ｇ０６Ｋ　１９／０７
Ｇ０６Ｋ　１９／１０
Ｈ０４Ｌ　９／３２