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

特許第5640060号
(P5640060)

(45)発行日　平成26年12月10日(2014.12.10)　(24)登録日　平成26年10月31日(2014.10.31)

(51)Int.Cl.　F I

G06F 21/62	(2013.01)	G06F	21/24	163G
G06Q 10/00	(2012.01)	G06Q	10/00	140
G08B 25/04	(2006.01)	G08B	25/04	F

請求項の数 5　(全 14 頁)

(21)出願番号　特願2012-237323(P2012-237323)
(22)出願日　平成24年10月26日(2012.10.26)
(65)公開番号　特開2014-86057(P2014-86057A)
(43)公開日　平成26年5月12日(2014.5.12)
審査請求日　平成26年8月19日(2014.8.19)

早期審査対象出願

(73)特許権者　000006150
京セラドキュメントソリューションズ株式会社
大阪府大阪市中央区玉造１丁目２番２８号
(74)代理人　100129997
弁理士　田中　米藏
(74)代理人　100121728
弁理士　井関　勝守
(72)発明者　杉原　宏
大阪市中央区玉造１丁目２番２８号　京セラドキュメントソリューションズ株式会社内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】機密情報管理システム

(57)【特許請求の範囲】

【請求項１】

管理区域へのユーザーの入退室を管理する入退室管理装置と、

アクセス制限された機密情報を保持する情報蓄積装置と、

ユーザーに対して当該電子機器へのログインの許可不許可を判定するユーザー認証部と、ユーザーが保持する携帯端末と通信する通信部とを有し、前記管理区域内に設置された電子機器と、

前記ユーザー認証部により前記ユーザーの前記電子機器へのログインが許可されたときに、前記通信部と通信する前記携帯端末を登録し、当該登録した携帯端末に対する前記情報蓄積部に保持された前記機密情報へのアクセスの許可不許可を判断するアクセス管理装置とを備え、

前記アクセス管理装置は、前記管理区域への前記ログインが許可されたユーザーの入室が前記入退室管理装置により認識されているときに、当該ログインが許可されたユーザーが保持する携帯端末の登録を認め、当該登録した携帯端末に前記機密情報へのアクセスを許可する機密情報管理システム。

【請求項２】

前記アクセス管理装置は、前記登録した携帯端末による前記機密情報へのアクセスとして、前記機密情報の閲覧を許可して保存を禁止する請求項１に記載の機密情報管理システム。

【請求項３】

前記アクセス管理装置は、前記登録した携帯端末に前記機密情報の保存を更に許可し、前記登録された前記携帯端末に前記機密情報の保存を許可するときは、前記機密情報に有効期限を設定する請求項１に記載の機密情報管理システム。
【請求項４】
前記アクセス管理装置は、前記ログインの許可されたユーザーが前記管理区域から退室したことが前記入退室管理装置から通知されたときに、前記携帯端末の登録を解除する請求項１乃至請求項３のいずれかに記載の機密情報管理システム。
【請求項５】
前記アクセス管理装置は、前記ログインの許可されたユーザーが前記電子機器からログオフしたときに、前記携帯端末の登録を解除する請求項１乃至請求項４のいずれかに記載の機密情報管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、機密情報管理システムに関し、特に、電子化された文書等からなる情報を印刷・閲覧等する場所を管理区域内に制限して、当該情報の機密性を担保する技術に関する。
【背景技術】
【０００２】
近年、文書の電子化に伴い、膨大な電子化文書が情報蓄積装置に蓄積され、任意の場所において電子化文書を自由に閲覧・印刷できるようになっている。このように、文書の電子化により文書利用の利便性が向上する反面、秘匿性のある電子化された文書、図面、写真等の機密情報については、どのように機密管理をするかが重要な課題である。機密情報にアクセス制限を設けることは機密管理の一つの有効な手段であるが、たとえアクセス制限をしたとしても、当該アクセス権を有するユーザーであれば、任意の場所において当該機密情報を閲覧・印刷することができるため、依然として情報漏えいの危険性を有する。
【０００３】
そこで、機密情報の閲覧・印刷等が可能な場所を、ユーザーの入退室が管理された管理区域内に制限して、機密情報の持ち出しを制限する技術が提案されている。例えば、下記特許文献１には、管理区域内に設置された端末装置のみで機密情報を閲覧することができる管理システムが示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００８－２７８０９３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ＰＤＡ（Personal Digital Assistant）やスマートフォン等の携帯端末の普及に伴い、電子化された文書を紙媒体に印刷するのではなく、携帯端末で閲覧するケースが増えている。従って、管理区域内でのみアクセス可能な機密情報についても、ユーザーが保持する携帯端末で閲覧したいという要請がある。しかしながら、上記特許文献１では、機密情報は特定された専用の端末装置でしか閲覧ができないため、機密情報を閲覧できるユーザー数が制限される。
【０００６】
本発明は、上記の問題を解決するためになされたもので、管理区域内でユーザーの携帯端末による機密情報のアクセスを可能にして利便性を向上するとともに、携帯端末による機密情報の不用意な持ち出しを制限して、当該機密情報の機密性を担保することを目的とする。
【課題を解決するための手段】

【０００７】
本発明の一局面に係る機密情報管理システムは、管理区域へのユーザーの入退室を管理する入退室管理装置と、
アクセス制限された機密情報を保持する情報蓄積装置と、
ユーザーに対して当該電子機器へのログインの許可不許可を判定するユーザー認証部と、ユーザーが保持する携帯端末と通信する通信部とを有し、前記管理区域内に設置された電子機器と、
前記ユーザー認証部により前記ユーザーの前記電子機器へのログインが許可されたときに、前記通信部と通信する前記携帯端末を登録し、当該登録した携帯端末に対する前記情報蓄積部に保持された前記機密情報へのアクセスの許可不許可を判断するアクセス管理装置とを備え、
前記アクセス管理装置は、前記管理区域への前記ログインが許可されたユーザーの入室が前記入退室管理装置により認識されているときに、当該ログインが許可されたユーザーが保持する携帯端末の登録を認め、当該登録した携帯端末に前記機密情報へのアクセスを許可するものである。
【発明の効果】
【０００８】
本発明によれば、管理区域内でユーザーの携帯端末による機密情報のアクセスを可能にして利便性を向上するとともに、携帯端末による機密情報の不用意な持ち出しを制限して、当該機密情報の機密性を担保することができる。
【図面の簡単な説明】
【０００９】
【図１】本発明の一実施形態に係る機密情報管理システムの概略構成図である。
【図２】(Ａ)(Ｂ)は入退室管理テーブルの一例を示す図である。
【図３】画像形成装置の主要内部構成を示す機能ブロック図である。
【図４】(Ａ)(Ｂ)は端末管理テーブルの一例を示す図である。
【図５】機密情報管理システムによる機密情報管理を示すフローチャートである。
【発明を実施するための形態】
【００１０】
以下、本発明の一実施形態に係る機密情報管理システムについて図面を参照して説明する。図１は、本発明の一実施形態に係る機密情報管理システムの概略構成図である。
【００１１】
本発明の一実施形態に係る機密情報管理システム１は、アクセス制限された文書、図面、写真等の機密情報が不用意にアクセスされて持ち出されることのないように、管理区域２内でのみ、当該機密情報の印刷や閲覧等のアクセスを許可する管理を行うものである。
【００１２】
機密情報管理システム１は、入退室管理装置１２、情報蓄積装置１４、画像形成装置１６、及びアクセス管理装置１８を備える。これらは、例えばＬＡＮ（Local Area Network）等のネットワーク１００により、互いに通信可能に接続されている。
【００１３】
情報蓄積装置１４は、機密情報を保持する装置であり、例えばファイルサーバーである。情報蓄積装置１４に保持されている機密情報は、後述するアクセス管理装置１８による処理で、アクセス権限を有するユーザーのみがアクセス可能とされている。
【００１４】
情報蓄積装置１４は、例えば、図１に示したように、管理区域２とは別の箇所（例えば、厳重にセキュリティー管理されたサーバールーム内）に設置される。なお、情報蓄積装置１４は、管理区域２内に設置されてもよいし、情報蓄積装置１４をファイルサーバーで構成せずに、画像形成装置１６の構成要素の一つとして画像形成装置１６内に設けられてもよい。
【００１５】

入退室管理装置１２は、管理区域２へのユーザーの入退室を管理する。入退室管理装置１２は、入室用カードリーダー１２２、退室用カードリーダー１２４、管理区域２のドア２２の電気錠１２６、及び制御部１２８を備える。

【００１６】

管理区域２のドア２２は電気錠１２６により常時施錠されている。電気錠１２６は、ドア２２の施錠及び解錠を電気的に制御するものであり、例えば可動鉄心、固定鉄心、コイル等を有するソレノイド電気錠を用いることができる。

【００１７】

入室用カードリーダー１２２は、管理区域２外に設置されている。ユーザーが管理区域２への入室時に、ＩＤカード３を入室用カードリーダー１２２にかざすと、入室用カードリーダー１２２は、ＩＤカード３から当該ユーザーの識別情報を読み取り、当該識別情報を制御部１２８に送信する。制御部１２８は、当該識別情報から当該ユーザーが管理区域２に入室可能なユーザーであると判断すると電気錠１２６を解錠制御し、所定時間経過後に施錠制御する。

【００１８】

ＩＤカード３は、例えばＲＦＩＤ（Radio Frequency IDentification）を用いて非接触認証が可能なＩＣカードである。なお、ユーザー認証にはＩＤカード３に更にパスワード入力を併用してもよい。

【００１９】

一方、ユーザーが管理区域２から退室する場合には、ユーザーがＩＤカード３を管理区域２内に設置されている退室用カードリーダー１２４にかざすと、当該退室用カードリーダー１２４は、ＩＤカード３から当該ユーザーの識別情報を読み取り、当該識別情報を制御部１２８に送信する。制御部１２８は、当該識別情報から当該ユーザーが管理区域２から退室可能なユーザーであると判断すると電気錠１２６を解錠制御し、所定時間経過後に施錠制御する。

【００２０】

制御部１２８は、カードリーダー１２２，１２４からの識別情報の受信、当該識別情報に基づくユーザーの管理区域２への入退出許可の判断、電気錠１２６の施錠及び解錠制御を行うと共に、ユーザーの管理区域２への入退室履歴を記憶する。具体的には、制御部１２８は、図示しないデータベースに入退室管理テーブルを保存しており、ユーザーの管理区域２への入退室履歴を当該入退室管理テーブルに記録する。

【００２１】

図２(Ａ)(Ｂ)は入退室管理テーブルの一例を示す。図２（Ａ）は、ユーザーが管理区域２に入室したときの入退室管理テーブルの例を示す。図２（Ａ）に示す入退室管理テーブルは、例えば、ユーザーＩＤ“１００１”のユーザーが、２０１２年１０月４日１５時５分１０秒（入室日時“121004150510”）に入室し、ユーザーＩＤ“１００２”のユーザーが２０１２年１０月４日１５時１３分４秒（入出日時“121004151304”）に、それぞれ管理区域２に入室した場合を示している。当該入退室管理テーブルにおいては、ユーザーＩＤ“１００１”及び“１００２”のユーザーが管理区域２内に滞在中であるとき、退出日時がいずれも情報無し(null)とされる。

【００２２】

図２（Ｂ）は、ユーザーが管理区域２から退出したときの入退室管理テーブルの例を示す。当該入退室管理テーブルは、ユーザーＩＤ“１００１”のユーザーが２０１２年１０月４日１７時３０分５秒（退出日時“121004173005”）に管理区域２から退室したことを表している。このように、ユーザーが管理区域２から退室すると、制御部１２８は、同じレコードの退出日時フィールドに当該ユーザーの退出日時を記録する。

【００２３】

再び図１を参照して説明する。画像形成装置１６は、例えば、コピー機能、プリンター機能、スキャナー機能、およびファクシミリ機能のような複数の機能を兼ね備えた複合機である。画像形成装置１６は、カードリーダー８０(図３)を備え、ユーザーが上記のＩＤ

カード３をカードリーダー８０にかざすと、カードリーダー８０は、ＩＤカード３から当該ユーザーの識別情報を読み取り、当該識別情報をユーザー認証部１０２(図３)に送信する。ユーザー認証部１０２は、当該識別情報に基づいて、当該ユーザーが、画像形成装置１６の操作を許可された正規のユーザーであるか否かを判定し、正規のユーザーである場合には、当該ユーザーに画像形成装置１６へのログインを許可する。なお、このログインに用いられるＩＤカード３は、管理区域２（図１）への入退室に用いるＩＤカード３である。

【００２４】

また、画像形成装置１６は、無線通信のホットスポット（登録商標）を提供する機能を備える。ログインユーザーが保持する携帯端末４は当該ホットスポット（登録商標）を介して画像形成装置１６に接続可能とされている。携帯端末４は、ＰＤＡ、スマートフォン、タブレット型ＰＣ等である。ログインユーザーは、一定条件の下で、携帯端末４により、情報蓄積装置１４に保持されている機密情報を閲覧可能とされている。

【００２５】

図３は、画像形成装置１６の主要内部構成を示す機能ブロック図である。画像形成装置１６は、制御ユニット１０、操作部４７、原稿給送部６、原稿読取部５、画像処理部３１、画像メモリー３２、画像形成部３３、定着部３４、駆動モーター７０、ファクシミリ通信部７１、ネットワークインターフェイス部９１、ＨＤＤ９２、カードリーダー８０、通信部９０等を備える。

【００２６】

制御ユニット１０は、ＣＰＵ(Central Processing Unit)、ＲＡＭ、ＲＯＭ及び専用のハードウェア回路等から構成され、画像形成装置１６の全体的な動作制御を司る。制御ユニット１０は、制御部１０１、ユーザー認証部１０２を備える。

【００２７】

制御部１０１は、操作部４７、原稿給送部６、原稿読取部５、画像処理部３１、画像メモリー３２、画像形成部３３、定着部３４、駆動モーター７０、ファクシミリ通信部７１、ネットワークインターフェイス部９１、ＨＤＤ９２、カードリーダー８０、通信部９０等と接続され、これら各部の駆動制御を行う。

【００２８】

ユーザー認証部１０２は、カードリーダー８０によってＩＤカード３から取得された当該カード保有者の識別情報から、当該ユーザーが画像形成装置１６の使用権限があるか否かを判定し、使用権限があると判定した場合、当該ユーザーをログインユーザーとして、画像形成装置１６の操作を許可する。

【００２９】

原稿読取部５は、制御ユニット１０による制御の下、光照射部及びＣＣＤセンサー等を有する読取機構を備える。画像形成装置１６が原稿読取動作を行う場合、原稿読取部５は、原稿給送部６により給送されてくる原稿、又は原稿載置ガラスに載置された原稿に光照射部により光を照射し、その反射光をＣＣＤセンサーで受光することにより、原稿から画像を読み取る。

【００３０】

画像処理部３１は、原稿読取部５で読み取られた画像の画像データを必要に応じて画像処理する。例えば、画像処理部３１は、原稿読取部５により読み取られた画像が画像形成部３３により画像形成された後の品質を向上させるために、シェーディング補正等の予め定められた画像処理を行う。

【００３１】

画像メモリー３２は、原稿読取部５による読取で得られた原稿画像のデータを一時的に記憶したり、画像形成部３３のプリント対象となるデータを一時的に保存する領域である。

【００３２】

画像形成部３３は、原稿読取部５で読み取られた印刷データ、ネットワーク接続された

情報蓄積装置１４（図１）から受信した印刷データ等の画像形成を行う。
【００３３】
操作部４７は、画像形成装置１６が実行可能な各種動作及び処理について操作者からの指示を受け付ける。操作部４７は、表示部４７３を備える。
【００３４】
ファクシミリ通信部７１は、図略の符号化／復号化部、変復調部及びＮＣＵ（Network Control Unit）を備え、公衆電話回線網を用いてのファクシミリの送信を行うものである。
【００３５】
ネットワークインターフェイス部９１は、ＬＡＮボード等の通信モジュールから構成され、当該ネットワークインターフェイス部９１に接続されたＬＡＮ等を介して、ローカルエリア内の情報蓄積装置１４（図１）等と種々のデータの送受信を行う。
【００３６】
ＨＤＤ（ハードディスクドライブ）９２は、原稿読取部５によって読み取られた原稿画像等を記憶する大容量の記憶装置である。
【００３７】
定着部３４は、画像形成部３３で形成された画像を、加熱及び加圧によって記録紙に定着させる。
【００３８】
駆動モーター７０は、画像形成部３３の各回転部材及び搬送ローラー対等に回転駆動力を付与する駆動源である。
【００３９】
カードリーダー８０は、管理区域２（図１）への入退室に用いるＩＤカード３から、当該ＩＤカード３保有者であるユーザーの識別情報を読み取り、当該識別情報を制御ユニット１０に送信する。制御ユニット１０におけるユーザー認証部１０２は、上述したユーザー認証処理を行う。
【００４０】
通信部９０は、Ｗｉ－Ｆｉ（登録商標）やブルートゥース（登録商標）等の近距離無線通信手段によるホットスポット（登録商標）を提供する。通信部９０は、携帯端末４からの要求に応じて携帯端末４との間でセッションを確立して携帯端末４と通信することができる。
【００４１】
図１に戻って、アクセス管理装置１８は、画像形成装置１６のユーザー認証部１０２によりユーザーの当該画像形成装置１６へのログインが許可されたときに、通信部９０とセッションを確立している携帯端末４を登録する。
【００４２】
アクセス管理装置１８は、管理区域２へのログインユーザーの入室が入退室管理装置１２により認識されているときに、当該ログインユーザーが保持する携帯端末４の登録を認め、当該登録した携帯端末４に、情報蓄積装置１４に保持された機密情報へのアクセスを許可する制御を行う。
【００４３】
更に、アクセス管理装置１８は、入退室管理装置１２から、ログインユーザーが管理区域２から退室したことが通知されたとき、携帯端末４の登録を解除する。これにより、アクセス管理装置１８は、当該携帯端末４による以降の機密情報へのアクセスを不可とする。すなわち、アクセス管理装置１８は、携帯端末４による上記機密情報へのアクセス可否を管理する。具体的には、アクセス管理装置１８は、図示しないデータベースに端末管理テーブルを有し、機密情報へのアクセスが許可された端末としての携帯端末４の登録を、当該端末管理テーブルに記録し、記録された携帯端末４にのみ情報蓄積装置１４に保持された機密情報へのアクセスを許可する。
【００４４】

図４(Ａ)(Ｂ)は、端末管理テーブルの一例を示す図である。図４（Ａ）は、ログインユーザーが保持する携帯端末４が登録されているときの端末管理テーブルの例を示す。当該端末管理テーブルは、携帯端末４の端末ＩＤ“12-34-56-78-9A-BC”をユーザーＩＤ“１００１”と対応付けて記録し、更に２０１２年１０月４日１５時２２分４１秒（登録日時“121004152241”）に当該携帯端末４が登録されたことを記憶している例を示す。なお、端末ＩＤは、携帯端末４に固有の識別記号であり、例えば、ＭＡＣアドレスやBluetooth(登録商標)アドレスが用いられる。

【００４５】

図４（Ｂ）は、ログインユーザーが管理区域２から退出したときの端末管理テーブルの例を示す。当該端末管理テーブルは、端末ＩＤ“12-34-56-78-9A-BC”の携帯端末４が２０１２年１０月４日１７時３０分５秒（解除日時“121004173005”）に登録解除されたことを記憶した例を示している。アクセス管理装置１８は、入退室管理装置１２から、管理区域２から退出したユーザーＩＤ及び退出日時の情報を受けた時に、当該ユーザーの携帯端末４の登録を解除するように処理する。アクセス管理装置１８は、入退室管理装置１２から、管理区域２から退出したユーザーＩＤ及び退出日時の情報を受け、端末管理テーブルにおいて当該ユーザーＩＤに一致するすべてのレコードの解除日時フィールドに当該退出日時を記録する。図４(Ｂ)に示す解除日時は、図２（Ｂ）に示した退出日時と一致する例を示している。

【００４６】

次に、機密情報管理システム１による機密情報管理について説明する。図５は、機密情報管理システム１による機密情報管理を示すフローチャートである。

【００４７】

ユーザーは、管理区域２への入室時に、ＩＤカード３を入室用カードリーダー１２２にかざす。入室用カードリーダー１２２は、ＩＤカード３から当該ユーザーの識別情報を読み取り、当該識別情報を制御部１２８に送信する。制御部１２８は、当該識別情報から当該ユーザーが管理区域２に入室可能なユーザーであると判断すると電気錠１２６を解錠する(Ｓ１)。これにより、ユーザーは入室が許可され、ドア２２を開けて管理区域２に入室することができる。

【００４８】

管理区域２に入室したユーザーは、同じＩＤカード３を使用して画像形成装置１６にログインする（Ｓ２）。すなわち、ユーザーが、ＩＤカード３をカードリーダー８０にかざすと、カードリーダー８０は、ＩＤカード３から、当該ＩＤカード３の保有者であるユーザーの識別情報を読み取り、当該識別情報を制御ユニット１０に送信する。制御ユニット１０のユーザー認証部１０２は、当該識別情報から当該ユーザーが画像形成装置１６の使用権限があるか否かを判定し、使用権限があると判定した場合、当該ユーザーをログインユーザーとして認識して画像形成装置１６の操作を許可する。

【００４９】

ログインユーザーによる画像形成装置１６の操作部４７の操作により、当該ログインユーザー所有(保有)の携帯端末４を登録する旨の要求があれば、画像形成装置１６の通信部９０は、当該ログインユーザーが保持する携帯端末４との間でセッションを確立する。アクセス管理装置１８は、機密情報へのアクセスが許可された端末として、当該接触が確立された携帯端末４を登録する（Ｓ３）。

【００５０】

続いて、アクセス管理装置１８により、当該携帯端末４による情報蓄積装置１４に蓄積されている機密情報へのアクセスが許可される（Ｓ４）。例えば、情報蓄積装置１４は、その制御部が、当該携帯端末４に組み込まれているブラウザーからの要求に応じて、保持している文書等のうち、当該要求の示す文書等へのアクセスを許可し、携帯端末４による当該文書等の閲覧を可能にする。

【００５１】

この後、ユーザーはＩＤカード３等を使用して管理区域２から退室する。ユーザーがＩ

Ｄカード３を管理区域２内に設置されている退室用カードリーダー１２４にかざすと、当該退室用カードリーダー１２４は、ＩＤカード３から当該ユーザーの識別情報を読み取り、当該識別情報を制御部１２８に送信する。制御部１２８は、当該識別情報から当該ユーザーが管理区域２から退室可能なユーザーであると判断すると電気錠１２６を解錠する(Ｓ５)。これにより、ユーザーは入退室管理装置１２により退室が許可され、ドア２２を開けて管理区域２から退室することができる。

【００５２】

このとき、アクセス管理装置１８は、入退室管理装置１２からユーザー退室の通知を受け、当該ユーザーが保持していた携帯端末４の登録を解除する（Ｓ６）。この後は、アクセス管理装置１８は、ログインユーザーは携帯端末４による機密情報へのアクセスを禁止する（Ｓ７）。これにより、以降は、情報蓄積装置１４に保持された文書を携帯端末４で閲覧することは不可能となる。

【００５３】

なお、アクセス管理装置１８は、ログインユーザーが画像形成装置１６からログオフしたときに、上記携帯端末４の登録を解除するようにしてもよい。これによれば、ユーザーによる画像形成装置１６へのログイン毎に、機密情報へのアクセスが許可される端末としての携帯端末４の登録が改めて行われる。従って、一度登録されたことのある携帯端末４であっても、それを保持するユーザーが画像形成装置１６にログインしているか否かに応じて、すなわち、ログインユーザーのアクセス権に応じて、機密情報へのアクセスが制限されるため、携帯端末４による機密情報へのアクセスを厳密に管理可能となり、機密情報の取り扱い利便性を確保しつつ、機密情報の機密性を更に確実に担保することが可能になる。

【００５４】

上記のように、本実施形態では、管理区域２内に画像形成装置１６が設置され、当該画像形成装置１６のログインユーザーが保持する携帯端末４は当該画像形成装置１６の通信部９０と通信可能になっている。そして、アクセス管理装置１８により、当該管理区域２内にいる当該ログインユーザーが保持する携帯端末４が、情報蓄積装置１４に保持されたアクセス制限された機密情報へのアクセスが許可された端末として登録され、当該登録した携帯端末４による機密情報へのアクセスが許可される。

【００５５】

従って、上記実施形態によれば、上記登録された携帯端末４であれば、情報蓄積装置１４に蓄積されている機密情報にアクセス可能とされるため、管理区域２内においては、当該携帯端末４による機密情報へのアクセスを可能にして、機密情報取り扱い時の利便性を向上できる。そして、アクセス管理装置１８は、管理区域２内におり、かつログインが許可されたログインユーザーの携帯端末４にのみ、当該機密情報へのアクセスを許可するため、携帯端末４による機密情報の不用意な持ち出しを制限して、当該機密情報の機密性を担保することができる。

【００５６】

また、例えば、管理システムに、各ユーザーが保持する携帯端末を、機密情報へのアクセス時よりも前に登録しておき、当該事前に登録されている各携帯端末に対して機密情報へのアクセスを許可する処理も考えられるが、ユーザー毎に保持する携帯端末が異なる上、同じユーザーであっても複数の携帯端末を所持し、毎回異なる携帯端末を用いることもあるため、機密情報へのアクセス時よりも前に管理システムに事前に携帯端末を登録することは非常に煩雑であり実用的ではない。しかしながら、上記実施形態に示したアクセス管理装置１８による携帯端末４の登録、及び機密情報の取り扱いによれば、機密情報へのアクセス時に携帯端末４を登録するため、多種多様な携帯端末に対して機密情報の取り扱いを認めて利便性を確保しつつ、機密情報の機密性も同時に担保可能である。

【００５７】

また、上記実施形態では、画像形成装置１６のログインユーザーが管理区域２から退室した場合、アクセス管理装置１８によって、当該ログインユーザーが保持する携帯端末４

の登録が解除される。従って、当該ログインユーザーが管理区域２から退室し、当該携帯端末４が管理区域２外から当該画像形成装置１６と引き続き通信できる状態であっても、当該携帯端末４から機密情報へアクセスが禁止され、携帯端末４による機密情報への不用意なアクセスを制限することができる。

【００５８】

アクセス管理装置１８は、登録した携帯端末４による機密情報へのアクセスとして、機密情報の閲覧のみを許可して保存を禁止してもよい。この場合、より厳格に携帯端末４による機密情報の持ち出しを制限することができる。

【００５９】

また、アクセス管理装置１８は、上記登録した携帯端末４に機密情報の保存を更に許可するものとし、上記登録された携帯端末４に機密情報の保存を許可するときは、機密情報に有効期限を設定するようにしてもよい。この場合、当該機密情報がユーザーにより管理区域２外に持ち出された場合であっても、一定期間後に当該機密情報にアクセス不可能とできるため、当該機密情報の漏洩及び拡散を有効に防止することができる。

【００６０】

なお、本発明は上記実施の形態の構成に限られず種々の変形が可能である。例えば、上記実施形態では、電子機器の一例として、画像形成装置を用いて説明しているが、他の電子機器、例えば、情報表示装置、情報処理装置等であっても構わない。さらには、画像形成装置１６の場合であっても、上記複合機に限定されるものではなく、他の電子機器、例えば、プリンター、コピー機、ファクシミリ装置等の他の画像形成装置でもよい。

【００６１】

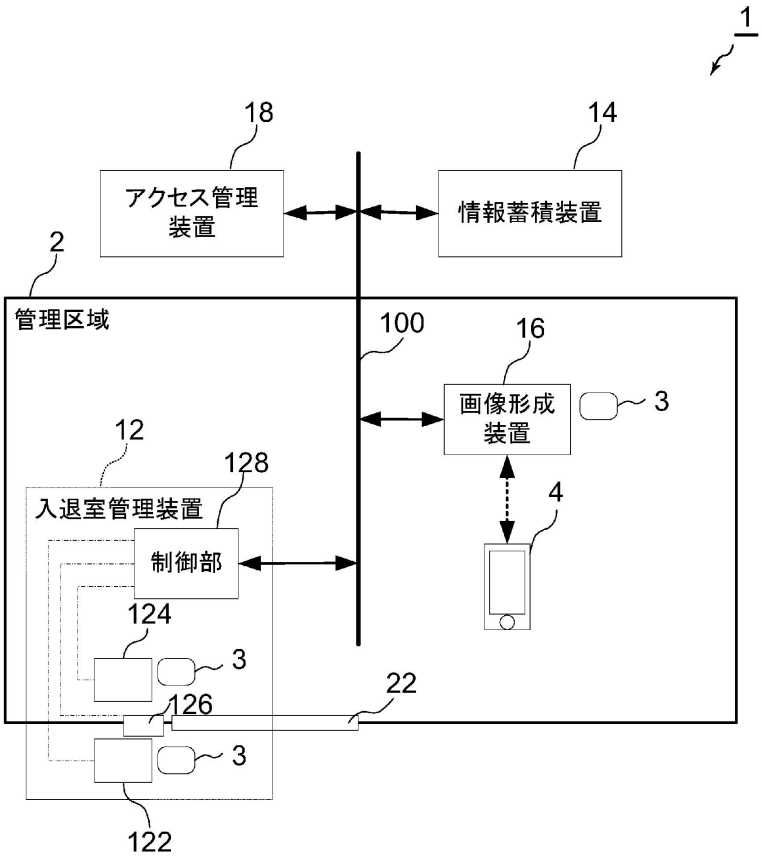
また、上記実施形態では、図１乃至図５を用いて上記実施形態により示した構成及び処理は、本発明の一実施形態に過ぎず、本発明を当該構成及び処理に限定する趣旨ではない。

【符号の説明】

【００６２】

１　機密情報管理システム
２　管理区域
４　携帯端末
１２　入退室管理装置
１４　情報蓄積装置
１６　画像形成装置
１８　アクセス管理装置
９０　通信部

【図１】



【図２】

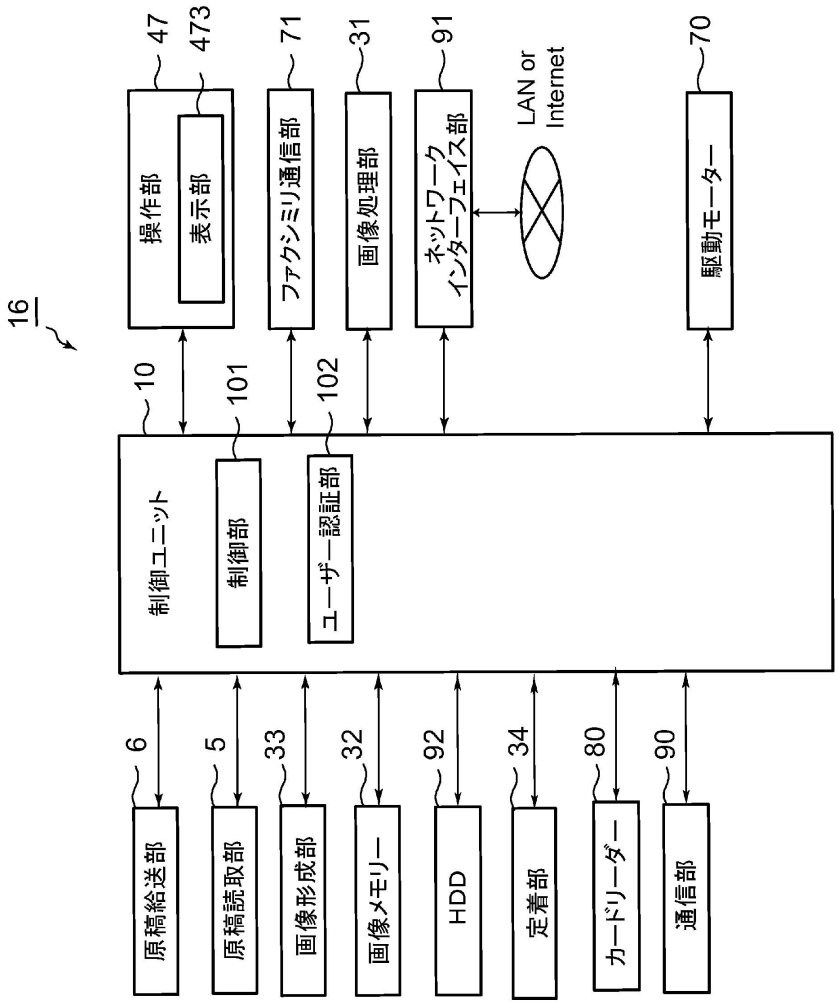
（A）

利用者ID	入室日時	退室日時
1001	121004150510	
1002	121004151304	
…	…	…

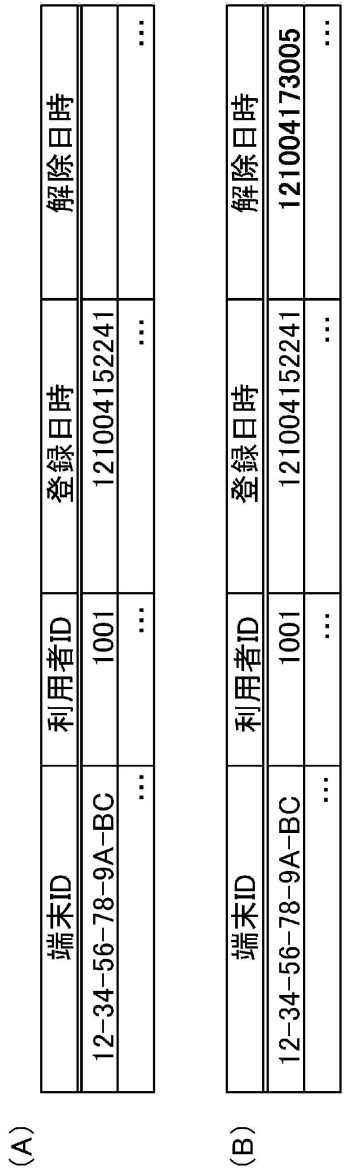
（B）

利用者ID	入室日時	退室日時
1001	121004150510	**121004173005**
1002	121004151304	
…	…	…

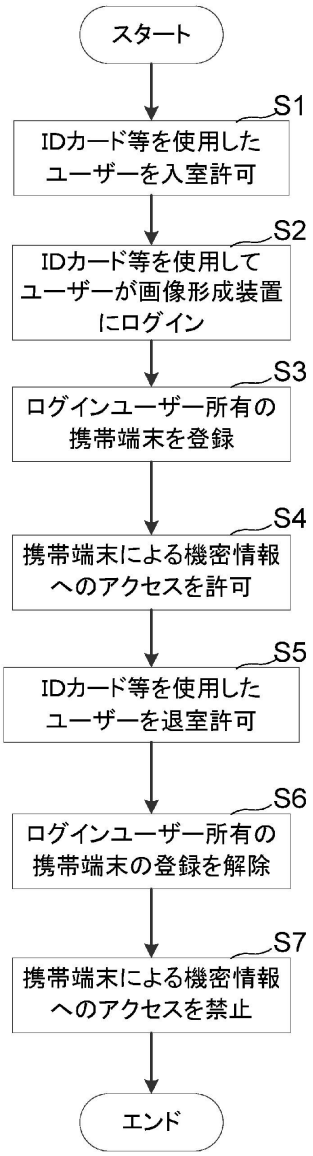
【図３】


16
制御ユニット
10
操作部
47
表示部
473
101
制御部
102
ユーザー認証部
ファクシミリ通信部
71
画像処理部
31
ネットワーク
インターフェイス部
91
LAN or
Internet
駆動モーター
70
6
原稿給送部
5
原稿読取部
33
画像形成部
32
画像メモリー
92
HDD
34
定着部
80
カードリーダー
90
通信部

【図４】


(A)
端末ID
利用者ID
登録日時
解除日時
12-34-56-78-9A-BC
1001
121004152241
…
…
…
(B)
端末ID
利用者ID
登録日時
解除日時
12-34-56-78-9A-BC
1001
121004152241
121004173005
…
…
…

【図５】


スタート
S1
IDカード等を使用したユーザーを入室許可
S2
IDカード等を使用してユーザーが画像形成装置にログイン
S3
ログインユーザー所有の携帯端末を登録
S4
携帯端末による機密情報へのアクセスを許可
S5
IDカード等を使用したユーザーを退室許可
S6
ログインユーザー所有の携帯端末の登録を解除
S7
携帯端末による機密情報へのアクセスを禁止
エンド

フロントページの続き

(56)参考文献 特開２００６－２２１２１２（ＪＰ，Ａ）
特開２００６－１２７１３５（ＪＰ，Ａ）
特開２００９－０２０８６８（ＪＰ，Ａ）
特開２００６－１５５１３８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｑ　１０／００
Ｇ０８Ｂ　２５／０４