(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7618979号
(P7618979)

(45)発行日　令和7年1月22日(2025.1.22)

(24)登録日　令和7年1月14日(2025.1.14)

(51)国際特許分類
Ｇ０６Ｆ　21/31　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/31

請求項の数　7　（全15頁）

(21)出願番号　特願2020-138610(P2020-138610)
(22)出願日　令和2年8月19日(2020.8.19)
(65)公開番号　特開2022-34755(P2022-34755A)
(43)公開日　令和4年3月4日(2022.3.4)
審査請求日　令和5年7月20日(2023.7.20)

(73)特許権者　000005496
富士フイルムビジネスイノベーション株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　110001519
弁理士法人太陽国際特許事務所
(74)代理人　110000039
特許業務法人アイ・ピー・ウィン
(72)発明者　鈴木　達郎
神奈川県横浜市西区みなとみらい六丁目１番　富士ゼロックス株式会社内
審査官　塩澤　如正

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理システムおよびプログラム

(57)【特許請求の範囲】

【請求項１】

メモリとプロセッサを備え、

前記プロセッサは、

離れた場所にいるユーザの認証情報を通信回線経由にて外部装置から取得する際に、当該認証情報の利用を制限するための制限情報を取得し、

前記認証情報を利用する際の条件が、前記制限情報により認証情報の利用が制限されないものである場合、前記認証情報を用いた認証装置に対する前記ユーザ以外の他のユーザによる代理認証処理の実行を、自装置を利用している利用者に対して許可するよう制御し、

取得した前記認証情報及び前記制限情報をメモリに記憶し、

離れた場所にいるユーザからの指示に基づいて、前記メモリに記憶されている前記認証情報の状態を有効状態から無効状態に、または無効状態から有効状態に切り替える、

情報処理装置。

【請求項２】

前記プロセッサは、離れた場所にいるユーザの認証情報を通信回線経由にて外部装置から取得する際に、当該認証情報の利用を許可する利用者を示す情報を取得し、

前記認証情報を利用しようとする利用者を特定して、特定した利用者が前記認証情報の利用が許可された利用者と一致した場合に、前記認証情報を用いた認証装置に対する前記ユーザ以外の他のユーザによる代理認証処理の実行を、自装置を利用している利用者に対して許可するよう制御する請求項１記載の情報処理装置。

【請求項３】
前記プロセッサは、自装置を利用しようとする利用者に対してログイン処理を要求することにより前記認証情報を利用しようとする利用者を特定する請求項２記載の情報処理装置。
【請求項４】
前記プロセッサは、前記制限情報として、前記認証情報を利用可能な期間または利用可能な回数の上限の情報を取得し、
当該期間の経過後または利用回数が上限に達した場合には前記認証情報を無効とする請求項１記載の情報処理装置。
【請求項５】
前記制限情報には、認証処理後に利用可能な機能を制限するための情報が含まれている請求項１から４のいずれか１項に記載の情報処理装置。
【請求項６】
前記プロセッサは、取得した認証情報の状態に関する情報を表示部に表示する請求項１から５のいずれか１項に記載の情報処理装置。
【請求項７】
離れた場所にいるユーザの認証情報を通信回線経由にて外部装置から取得する際に、当該認証情報の利用を制限するための制限情報を取得するステップと、
前記認証情報を利用する際の条件が、前記制限情報により認証情報の利用が制限されないものである場合、前記認証情報を用いた認証装置に対する前記ユーザ以外の他のユーザによる代理認証処理の実行を、自装置を利用している利用者に対して許可するよう制御するステップと、
取得した前記認証情報及び前記制限情報をメモリに記憶するステップと、
離れた場所にいるユーザからの指示に基づいて、前記メモリに記憶されている前記認証情報の状態を有効状態から無効状態に、または無効状態から有効状態に切り替えるステップと、
をコンピュータに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、情報処理装置、情報処理システムおよびプログラムに関する。
【背景技術】
【０００２】
特許文献１には、利用者の本人性を確認可能な情報を格納する格納媒体に、当該格納媒体を利用する利用者が他の利用者から委譲された権限に関する権限委譲情報を格納することにより、他の利用者からの権限を適切に委譲することができるようにした権限委譲システムが開示されている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２００９－２０５３４２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
本発明の目的は、離れた場所にいるユーザの認証情報を用いて、他のユーザがそのユーザの代理として認証処理を行う際に、その認証情報を使用した認証処理の実行を制限することが可能な情報処理装置、情報処理システムおよびプログラムを提供することである。
【課題を解決するための手段】
【０００５】
［情報処理装置］

請求項１に係る本発明は、メモリとプロセッサを備え、
前記プロセッサは、
離れた場所にいるユーザの認証情報を通信回線経由にて外部装置から取得する際に、当該認証情報の利用を制限するための制限情報を取得し、
前記認証情報を利用する際の条件が、前記制限情報により認証情報の利用が制限されないものである場合、前記認証情報を用いた認証装置に対する前記ユーザ以外の他のユーザによる代理認証処理の実行を、自装置を利用している利用者に対して許可するよう制御し、
取得した前記認証情報及び前記制限情報をメモリに記憶し、
離れた場所にいるユーザからの指示に基づいて、前記メモリに記憶されている前記認証情報の状態を有効状態から無効状態に、または無効状態から有効状態に切り替える情報処理装置である。
【０００６】
請求項２に係る本発明は、前記プロセッサが、離れた場所にいるユーザの認証情報を通信回線経由にて外部装置から取得する際に、当該認証情報の利用を許可する利用者を示す情報を取得し、
前記認証情報を利用しようとする利用者を特定して、特定した利用者が前記認証情報の利用が許可された利用者と一致した場合に、前記認証情報を用いた認証装置に対する前記ユーザ以外の他のユーザによる代理認証処理の実行を、自装置を利用している利用者に対して許可するよう制御する請求項１記載の情報処理装置である。
【０００７】
請求項３に係る本発明は、前記プロセッサが、自装置を利用しようとする利用者に対してログイン処理を要求することにより前記認証情報を利用しようとする利用者を特定する請求項２記載の情報処理装置である。
【０００８】
請求項４に係る本発明は、前記プロセッサが、前記制限情報として、前記認証情報を利用可能な期間または利用可能な回数の上限の情報を取得し、
当該期間の経過後または利用回数が上限に達した場合には前記認証情報を無効とする請求項１記載の情報処理装置である。
【０００９】
請求項５に係る本発明は、前記制限情報には、認証処理後に利用可能な機能を制限するための情報が含まれている請求項１から４のいずれか１項に記載の情報処理装置である。
【００１１】
請求項６に係る本発明は、前記プロセッサが、取得した認証情報の状態に関する情報を表示部に表示する請求項１から５のいずれか１項に記載の情報処理装置である。
【００１４】
［プログラム］
請求項７に係る本発明は、離れた場所にいるユーザの認証情報を通信回線経由にて外部装置から取得する際に、当該認証情報の利用を制限するための制限情報を取得するステップと、
前記認証情報を利用する際の条件が、前記制限情報により認証情報の利用が制限されないものである場合、前記認証情報を用いた認証装置に対する前記ユーザ以外の他のユーザによる代理認証処理の実行を、自装置を利用している利用者に対して許可するよう制御するステップと、
取得した前記認証情報及び前記制限情報をメモリに記憶するステップと、
離れた場所にいるユーザからの指示に基づいて、前記メモリに記憶されている前記認証情報の状態を有効状態から無効状態に、または無効状態から有効状態に切り替えるステップと、をコンピュータに実行させるためのプログラムである。
【発明の効果】
【００１６】
請求項１に係る本発明によれば、離れた場所にいるユーザの認証情報を用いて、他のユ

ーザがそのユーザの代理として認証処理を行う際に、その認証情報を使用した認証処理の実行を制限することが可能な情報処理装置を提供することができる。
また、請求項１に係る本発明によれば、認証情報全体を転送したり削除したりすることなく、その認証情報を有効化したり無効化したりすることが可能となる。
【００１７】
請求項２に係る本発明によれば、離れた場所にいるユーザの認証情報を用いて、他のユーザがそのユーザの代理として認証処理を行う際に、その認証情報を利用するユーザを制限することができる。
【００１８】
請求項３に係る本発明によれば、認証情報を利用するユーザを、ログイン処理を利用して特定することができる。
【００１９】
請求項４に係る本発明によれば、離れた場所にいるユーザの認証情報を用いて、他のユーザがそのユーザの代理として認証処理を行う際に、その認証情報を利用可能な回数を制限することができる。
【００２０】
請求項５に係る本発明によれば、その認証情報を利用して認証処理を実行した際に、利用可能な機能を制限することができる。
【００２２】
請求項６に係る本発明によれば、自装置の表示部を見ただけで認証情報が有効であるか否かを把握することが可能となる。
【００２５】
請求項７に係る本発明によれば、離れた場所にいるユーザの認証情報を用いて、他のユーザがそのユーザの代理として認証処理を行う際に、その認証情報を使用した認証処理の実行を制限することが可能なプログラムを提供することができる。
また、請求項７に係る本発明によれば、認証情報全体を転送したり削除したりすることなく、その認証情報を有効化したり無効化したりすることが可能となる。
【図面の簡単な説明】
【００２７】
【図１】本発明の一実施形態の情報処理システムのシステム構成を示す図である。
【図２】ユーザＡ、Ｂが、複合機２０に対して認証処理を実行する様子を説明するための図である。
【図３】本発明の一実施形態の移動端末１０を用いた代理認証の具体的な方法を説明するための図である。
【図４】本発明の一実施形態における移動端末１０のハードウェア構成を示すブロック図である。
【図５】本発明の一実施形態における移動端末１０の機能構成を示すブロック図である。
【図６】制限情報の構成の一例を説明するための図である。
【図７】移動端末１０において、代理認証を行おうとするユーザがログイン処理を行う際の表示画面例を示す図である。
【図８】認証情報が有効化されてユーザＡの権限が移譲されている状態であることを表示部３２に表示した場合の移動端末１０の表示画面例を示す図である。
【図９】代理認証が行われる際に、認証情報の使用可否をユーザＡに確認する際の端末装置６０、移動端末１０および複合機２０間で行われる情報の送受信の様子を説明するためのシーケンスチャートである。
【図１０】複数ユーザの認証情報を移動端末１０に書き込む際に、排他制御が行われる場合の移動端末１０の様子を示す図である。
【図１１】複数ユーザの認証情報を移動端末１０に書き込む際に、後優先制御が行われる場合の移動端末１０の様子を示す図である。
【発明を実施するための形態】

【００２８】
次に、本発明の実施の形態について図面を参照して詳細に説明する。
【００２９】
図１は本発明の一実施形態の情報処理システムのシステム構成を示す図である。
【００３０】
本発明の一実施形態の情報処理システムは、図１に示されるように、在宅勤務を行うテレワーク利用者の端末装置６０と、オフィス内において使用される移動端末１０とが、無線ＬＡＮターミナル７０、インターネット５０、ルータ３０、社内ネットワーク、無線ＬＡＮターミナル４０を経由して相互に接続された構成となっている。
【００３１】
移動端末１０は、Ｗｉ－Ｆｉ（登録商標）等の無線通信回線を介して無線ＬＡＮターミナル４０と接続可能なスマートフォン等の情報処理装置である。
【００３２】
図１に示した情報処理システムでは、ユーザＡが自宅において在宅勤務を行う様子が示されている。そして、ユーザＡは、在宅勤務を行う際に自身の移動端末１０を、オフィス内において勤務するユーザＢに託しているものとして説明する。つまり、ユーザＢは、オフィスにおいて勤務していないユーザＡから権限を移譲され、ユーザＡの代理人として移動端末１０を保持している。
【００３３】
なお、オフィス内の社内ネットワークには、複合機２０が接続されている。この複合機２０は、印刷機能、スキャン機能、コピー機能、ファクシミリ機能等の複数の機能を有する画像形成装置である。
【００３４】
複合機２０はオフィス内に設置されており、数多くのユーザにより使用されるようになっている。しかし、近年セキュリティ意識の高まりから、各ユーザが認証処理を実行しなければ複合機２０の各機能を使用することができないようになっている。この認証処理を実行する際には、社員証等のＩＣカードを複合機２０のＩＣカードリーダにタッチすることにより、ＩＣカード内に保持されている認証情報が読み出されて認証処理が実行され、そのユーザが特定されるようになっている。このＩＣカードは、ＮＦＣ（Near Field Communicationの略）と呼ばれる近距離無線通信によって、内蔵されたＩＣチップ内に書き込まれた情報を用いて外部の通信機器との間でデータの送受信を行う機能を有している。
【００３５】
例えば、図２に示すように、ユーザＡが自身のＩＣカード８０Ａを複合機２０のＩＣカードリーダにタッチすることによりユーザＡとしての認証が行われ、ユーザＢが自身のＩＣカード８０Ｂを複合機２０のＩＣカードリーダにタッチすることによりユーザＢとしての認証が行われる。
【００３６】
このような認証制御を行うことにより、本人がパーソナルコンピュータ等から転送した印刷ジョブのみを印刷するような機能や、あるユーザはカラー印刷が可能だが他のユーザはモノクロ印刷しかできない等のユーザ毎に利用可能なサービスを制限したりする機能を実現することができる。さらに、このような認証制御によれば、ユーザ毎に毎月のコピー枚数の上限を設けることや、所属組織毎にコピー枚数等の利用実績を集計する機能や、ユーザ毎にＦＡＸの宛先帳や、スキャンしたデータの送信先としてのメールアドレス等の設定を自動的に行う等の様々な機能を実現することができる。
【００３７】
しかし、上述したように自宅にて勤務を行うテレワーク利用者がオフィス内に設置されている複合機２０を使用したい場合がある。例えば、ある書類を複合機２０によりスキャンして、スキャンされた電子化データをユーザＡのメールアドレスに送信して欲しい場合がある。
【００３８】

このような場合、オフィス内に勤務しているユーザＢに、ユーザＡのＩＣカード８０Ａを渡しておけば、ユーザＢがユーザＡの代理として認証処理を実行することが可能である。しかし、ＩＣカード８０Ａがユーザの社員証も兼ねている場合、自分の社員証を他人に貸与することは問題がある。さらに、ユーザＢにユーザＡのＩＣカード８０Ａを渡してしまった場合、無制限に全ての機能が使用できてしまうと、ユーザＡが意図していない範囲までユーザＢが使用できてしまうという問題がある。

【００３９】

そこで、本実施形態では、図１に示した移動端末１０をＩＣカード８０Ａの代わりとして使用して、下記のような制御を行うことにより、離れた場所にいるユーザＡの認証情報を用いて、他のユーザＢがそのユーザＡの代理として認証処理を行う際に、その認証情報を使用した認証処理の実行を制限することができるようにしている。なお、以下において、あるユーザの認証情報を用いて他のユーザが認証処理を行うことを代理認証と称する。

【００４０】

本実施形態の移動端末１０を用いた代理認証の具体的な方法を図３に示す。図３では、ユーザＡは端末装置６０を操作することにより、移動端末１０にユーザＡの認証情報を書き込むことにより、ユーザＢに権限を移譲する。すると、ユーザＢは、ユーザＡの認証情報が書き込まれた移動端末１０を複合機１０のＩＣカードリーダにタッチすることにより、ユーザＡとしてログインする代理認証を行う。

【００４１】

このようにユーザＢが、ユーザＡとして複合機２０に対して代理人認証を行うことにより、ユーザＡから依頼された各種操作を実行することが可能となる。

【００４２】

ただし、ユーザＡが認証情報を移動端末１０に書き込む際に、この認証情報の使用を制限するための制限情報も同時に移動端末１０に書き込む。そのため、ユーザＢが移動端末１０に書き込まれた認証情報を利用して行うユーザＡの代理認証は、この制限情報の範囲内において制限されることになる。この制限情報の詳細については後述する。

【００４３】

なお、ここでは移動端末１０にユーザＡの認証情報を書き込むことにより、ユーザＡの権限を移譲するものとして説明したが、以下において説明する本実施形態の説明では、ユーザＡの認証情報が移動端末１０に予め記憶されているものとして説明する。この場合には、ユーザＡがユーザＢに対して、ユーザＡの権限を移譲する際に、ユーザＡが端末装置６０から移動端末１０にアクセスして、記憶されている認証情報を有効化することにより使用可能とする。そして、移譲した権限を無効にする場合には、ユーザＡが端末装置６０から移動端末１０にアクセスして、有効状態の認証情報を無効化する。しかし、端末装置６０から移動端末１０に認証情報を実際に転送したり、移動端末１０に記憶されている認証情報を実際に削除したりするような方法により、ユーザＡがユーザＢに対して、ユーザＡの権限を移譲したり移譲した権限を無効化するようにしても良い。

【００４４】

次に、本実施形態の情報処理システムにおける移動端末１０のハードウェア構成を図４に示す。

【００４５】

移動端末１０は、図４に示されるように、ＣＰＵ１１、メモリ１２、フラッシュメモリ等の記憶装置１３、ネットワークを介して外部の装置等との間でデータの送信及び受信を行う通信インタフェース（ＩＦと略す。）１４、タッチパネル又は液晶ディスプレイ等のユーザインタフェース（ＵＩと略す。）装置１５を有する。これらの構成要素は、制御バス１６を介して互いに接続されている。

【００４６】

ＣＰＵ１１は、メモリ１２または記憶装置１３に格納された制御プログラムに基づいて所定の処理を実行して、移動端末１０の動作を制御するプロセッサである。なお、本実施形態では、ＣＰＵ１１は、メモリ１２または記憶装置１３内に格納された制御プログラム

を読み出して実行するものとして説明するが、当該プログラムをＣＤ－ＲＯＭ等の記憶媒体に格納してＣＰＵ１１に提供することも可能である。

【００４７】

図５は、上記の制御プログラムが実行されることにより実現される移動端末１０の機能構成を示すブロック図である。

【００４８】

本実施形態の移動端末１０は、図５に示されるように、操作入力部３１と、表示部３２と、データ取得部３３と、制御部３４と、データ記憶部３５とを備えている。

【００４９】

表示部３２は、制御部３４により制御され、ユーザに各種情報を表示する。操作入力部３１は、ユーザにより行われた各種操作情報を入力する。

【００５０】

データ取得部３３は、無線通信回線を介して外部の装置との間でデータの送受信を行って、各種情報を取得する。

【００５１】

制御部３４は、移動端末１０の全体動作を制御している。データ記憶部３５は、データ取得部３３により取得されたデータ等の各種データを格納する。

【００５２】

そして、データ取得部３３は、離れた場所である自宅にいるユーザＡの認証情報を、Ｗｉ－Ｆｉ（登録商標）等の無線通信回線経由にて外部装置である端末装置６０から取得する際に、その認証情報の利用を制限するための制限情報を取得する。なお、このデータ取得部３３により取得された認証情報や制限情報はデータ記憶部３５に記憶される。

【００５３】

この認証情報は、例えば、ログインＩＤとパスワードとから構成されており、複合機２０において認証処理を実行する際に必要となる情報である。そして、制限情報とは、認証情報の利用を制限するための制限内容が設定された情報であり、例えば、図６に示すような構成となっている。

【００５４】

図６に示した制限情報例では、制限項目として、許可ユーザ、使用可能期間、使用可能回数、使用可能機能、認証時の確認要否等が設定されている。なお図６に示した制限情報例では、許可ユーザとしてユーザＢが設定されており、認証情報を使用することが許可されているユーザがユーザＢのみであることを意味している。また、使用可能期間として１日が設定されており、認証情報を使用可能な期間が、この認証情報が有効状態となってから１日以内であることを意味している。また、使用可能数として１０回が設定されており、この認証情報を用いた認証処理を実行可能な回数が１０回までであることを意味している。

【００５５】

さらに、図６に示した制限情報例では、使用可能機能として、コピー、スキャン、ＦＡＸ、プリントのそれぞれに対して、使用可、使用不可、使用可、使用可が設定されており、この認証情報を用いて認証を行った場合には、コピー、ＦＡＸ、プリントの機能を使用することはできるが、スキャンの機能は使用することができないことを意味している。

【００５６】

さらに、図６に示した制限情報例では、認証時の確認要否については、不要と設定されており、この認証情報を用いて認証処理を行って複合機２０の機能を使用する際に、認証情報の所有者であるユーザＡに確認を行う必要は無いことを意味している。

【００５７】

そして、制御部３４は、認証情報を利用する際の条件が、制限情報により認証情報の利用が制限されないものである場合、認証情報を用いた認証処理の実行を許可するよう制御する。

【００５８】

例えば、データ取得部３３、自宅にいるユーザＡの認証情報を通信回線経由にて外部装置から取得する際に、この認証情報の利用を許可するユーザを示す情報を制限情報として取得する。

【００５９】

そして、制御部３４は、認証情報を利用しようとするユーザを特定して、特定したユーザが、この認証情報の利用が許可されたユーザと一致した場合に、この認証情報を用いた認証処理の実行を許可するよう制御する。

【００６０】

具体的には、制御部３４は、自装置を利用しようとするユーザに対してログイン処理を要求することにより、データ記憶部３５に記憶された認証情報を利用しようとするユーザを特定する。

【００６１】

例えば、制御部３４は、図７に示すように、代理認証を行おうとするユーザに対してログイン処理を要求して、ログインしたユーザがユーザＢである場合にのみ、認証情報を有効化して代理人認証を許可する。ここで、ログインしたユーザが許可されていないユーザＣである場合には、制御部３４は、認証情報を有効化せず無効状態のままとする。

【００６２】

そして、ログインしたユーザがユーザＢであることが確認されると、制御部３４は、図８に示すように、認証情報が有効化されてユーザＡの権限が移譲されている状態であることを表示部３２に表示する。

【００６３】

このように、制御部３４は、取得した認証情報の状態に関する情報を表示部３２に表示するようにしても良い。

【００６４】

さらに、制御部３４は、認証情報を利用可能な期間または利用可能な回数の上限の情報を制限情報として取得した場合、その期間の経過後または利用回数が上限に達した場合には認証情報を無効とする。

【００６５】

例えば、認証情報の利用可能な期間が１日の場合には、認証情報を取得した時点から１日が経過した場合、制御部３４は、有効状態だった認証情報を無効化する。また、認証情報の利用可能な回数の上限が１０回の場合には、認証情報を利用して行った代理認証の回数が１０回に到達した場合、制御部３４は、有効状態だった認証情報を無効化する。

【００６６】

さらに、認証処理後に利用可能な機能を制限するための情報が制限情報に含まれている場合には、制御部３４は、代理人認証を行う際に利用可能な機能の情報を複合機２０に転送する。その結果、複合機２０では、利用可能として設定されている機能のみを利用可能とする。例えば、制限情報において図６に示したように、コピー、ＦＡＸ、プリントのみが使用可に設定され、スキャンについては使用不可に設定されている場合、この認証情報により認証が行われた複合機２０では、コピー、ＦＡＸ、プリントのみを利用可能として、スキャンについては利用不可とする。

【００６７】

なお、本実施形態の移動端末１０では、データ記憶部３５に、ユーザＡの認証情報が予め記憶されている。そして、制御部３４は、離れた場所にいるユーザＡからの指示に基づいて、データ記憶部３５に記憶されている認証情報の状態を有効状態または無効状態の間で切り替える。

【００６８】

上記の説明では、ユーザＢは、認証情報が有効化された状態の移動端末１０を用いて複合機２０の認証処理を行うことにより、制限情報の範囲内で複合機２０の各種機能を実行することが可能となる。しかし、認証情報が有効化された状態の移動端末１０がユーザＡの意図しない範囲で使用される場合も発生してしまう可能性がある。そのため、移動端末

１０により複合機２０に対する認証を実行する際に、ユーザＡに確認を求め、ユーザＡが許可した場合にのみ移動端末１０による代理人認証を可能とするようにしても良い。

【００６９】

具体的には、図６に示した制限情報において、認証時の確認要否において「必要」と設定されており、この認証情報を用いて認証処理を行って複合機２０の機能を使用する際に、認証情報の所有者であるユーザＡに確認を行う必要があると設定されている場合に上記のような制御が行われる。以下において、このような制御を行う場合について説明する。

【００７０】

この場合には、データ取得部３３は、離れた場所にいるユーザＡの認証情報を通信回線経由にて外部装置から取得する際に、その認証情報が複製されたものであることを示す情報とともに取得する。

【００７１】

そして、制御部３５は、この認証情報を用いた認証処理を実行する際に、認証情報が複製されたものであることを示す情報を含めた認証情報を複合機２０に提示する。なお、本実施形態では、認証処理を実行する認証装置として複合機２０を用いた場合について説明するが、提示された認証情報に基づいて認証処理を実行するような認証装置であれば同様な制御を実現することが可能である。

【００７２】

そして、複合機２０は、移動端末１０から認証情報を取得して認証処理を行う際に、取得した認証情報にこの認証情報が複製されたものであることを示す情報が含まれている場合、その認証情報の所有者であるユーザＡに認証情報の使用可否の確認を行い、認証情報の使用を許可する旨の回答を受信した場合に、その認証情報を用いた認証処理を実行する。

【００７３】

このような処理が実行される際の端末装置６０、移動端末１０および複合機２０間で行われる情報の送受信の様子を図９のシーケンスチャートを参照して説明する。

【００７４】

まず、移動端末１０が、ステップＳ１０１において、複合機２０に認証情報を提示して認証処理を要求する際に、この認証情報が複製であることを示す情報も一緒に提示する。

【００７５】

すると、複合機２０は、ステップＳ１０２において、認証情報の所有者であるユーザＡの端末装置６０に対して、複製された認証情報を用いた代理認証を行っても良いか否かを確認する通知を送信する。

【００７６】

そして、この複合機２０からの確認通知に対して、ステップＳ１０３において、端末装置６０から代理認証を許可する旨が複合機２０に返信された場合、複合機２０は、ステップＳ１０４において、この認証情報を用いた認証処理を実行する。

【００７７】

このような制御とすることにより、複合機２０からの確認通知を受けたユーザＡが、代理認証を依頼していないはずであると不審に思って、代理認証を許可する旨を返信しなければ、複合機２０において代理認証が実行されないことになる。

【００７８】

さらに、上記で説明した実施形態では、移動端末１０にユーザＡの認証情報を書き込んで使用する場合について説明したが、複数のユーザの認証情報を移動端末１０に書き込んで使用することができるようにしても良い。

【００７９】

例えば、ユーザＡとユーザＣの認証情報をそれぞれ移動端末１０に書き込んで、ユーザＢが移動端末１０を使用して代理認証を行うようにしても良い。

【００８０】

ただし、このような場合には、複数のユーザの認証情報を同時に書き込んだり有効化したりしたのでは、複合機２０では、どちらの認証情報により認証処理を実行して良いのか

分からなくなってしまう。そのため、移動端末１０内において書き込まれる認証情報または有効化される認証情報は１人のユーザのものに限定する必要がある。

【００８１】

そして、このような条件を実現するためには、移動端末１０では、あるユーザの認証情報が書き込まれている場合には、その認証情報が消去されるまで他のユーザの認証情報の書き込みを拒絶する排他制御か、あるユーザの認証情報が書き込まれている状態で他のユーザの認証情報が書き込まれた場合には、後から書き込まれた認証情報を優先して古い認証情報については消去する後優先制御を実行する必要がある。

【００８２】

このような排他制御が行われる場合の移動端末１０の様子を図１０に示す。

【００８３】

この図１０に示される場合では、時刻Ｔ１において、いずれの認証情報も書き込まれていない状態である無効状態の移動端末１０にユーザＡによる認証情報の書き込みが行われると、移動端末１０には、このユーザＡの認証情報が書き込まれた状態となる。そして、この状態において時刻Ｔ２に、ユーザＣにより認証情報の書き込みが行われた場合、既にユーザＡの認証情報が書き込まれた状態であるため、ユーザＣによる認証情報の書き込みは拒絶される。

【００８４】

その結果、その後にユーザＢが移動端末１０を用いて複合機２０に対して認証処理を実行した場合には、ユーザＡの権限により認証処理が実行されることになる。

【００８５】

そして、時刻Ｔ３においてユーザＡによる認証情報の消去が行われると、移動端末１０に記憶されていたユーザＡの認証情報は削除され、移動端末１０は、いずれの認証状態も書き込まれていない無効状態となる。

【００８６】

次に、上記で説明した後優先制御が行われる場合の移動端末１０の様子を図１１に示す。

【００８７】

この図１１に示される場合では、時刻Ｔ１において、いずれの認証情報も書き込まれていない状態である無効状態の移動端末１０にユーザＡによる認証情報の書き込みが行われると、移動端末１０には、このユーザＡの認証情報が書き込まれた状態となる。そして、この状態において時刻Ｔ２に、ユーザＣにより認証情報の書き込みが行われた場合、既にユーザＡの認証情報が書き込まれた状態であるが、後優先制御が行われることにより、ユーザＣによる認証情報の書き込みが行われユーザＡの認証情報は削除される。

【００８８】

その結果、その後にユーザＢが移動端末１０を用いて複合機２０に対して認証処理を実行した場合には、ユーザＣの権限により認証処理が実行されることになる。

【００８９】

そして、時刻Ｔ３においてユーザＣによる認証情報の消去が行われると、移動端末１０に記憶されていたユーザＣの認証情報は削除され、移動端末１０は、いずれの認証状態も書き込まれていない無効状態となる。

【００９０】

上記のような制御が行われることにより、１台の移動端末１０に対して複数のユーザの認証情報の書き込みを行っても、有効な認証情報は１人のユーザのみのものとなる。

【００９１】

上記各実施形態において、プロセッサとは広義的なプロセッサを指し、汎用的なプロセッサ（例えばＣＰＵ：Central Processing Unit、等）や、専用のプロセッサ（例えばＧＰＵ：Graphics Processing Unit、ＡＳＩＣ：Application Specific Integrated Circuit、ＦＰＧＡ：Field Programmable Gate Array、プログラマブル論理デバイス等）を含むものである。

【００９２】

また上記各実施形態におけるプロセッサの動作は、１つのプロセッサによって成すのみでなく、物理的に離れた位置に存在する複数のプロセッサが協働して成すものであってもよい。また、プロセッサの各動作の順序は上記各実施形態において記載した順序のみに限定されるものではなく、適宜変更してもよい。

【００９３】

[変形例]

上記実施形態では、ユーザ毎の認証情報を用いて複合機２０に対する認証処理を実行する場合を用いて説明したが、本発明はこれに限定されるものではなく、使用される際に認証処理を要求する様々な認証装置に対する認証処理を実行するような場合でも本発明を同様に適用することができるものである。

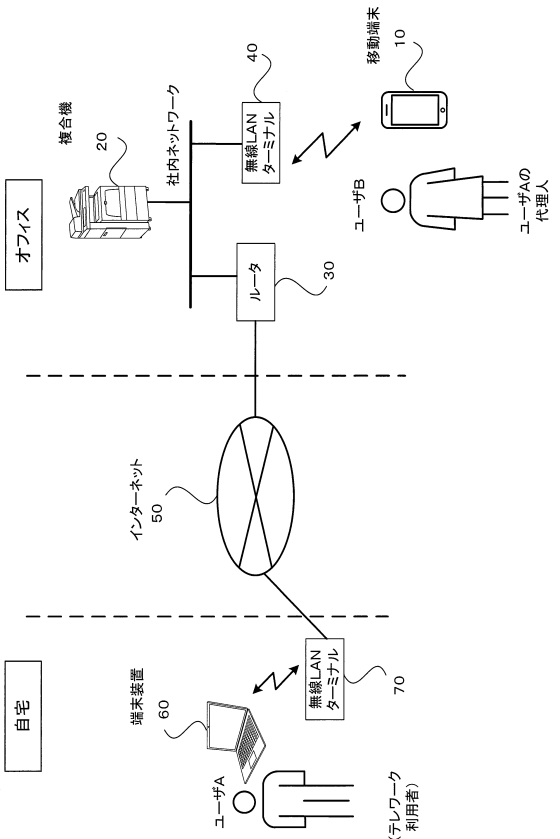
【符号の説明】

【００９４】

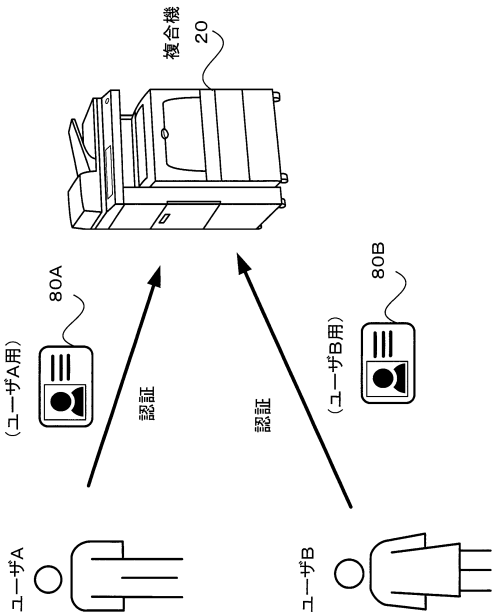
１０　移動端末
１１　ＣＰＵ
１２　メモリ
１３　記憶装置
１４　通信インタフェース
１５　ユーザインタフェース装置
１６　制御バス
２０　複合機
３０　ルータ
３１　操作入力部
３２　表示部
３３　データ取得部
３４　制御部
３５　データ記憶部
４０　無線ＬＡＮターミナル
５０　インターネット
６０　端末装置
７０　無線ＬＡＮターミナル
８０Ａ、８０Ｂ　ＩＣカード

【図面】

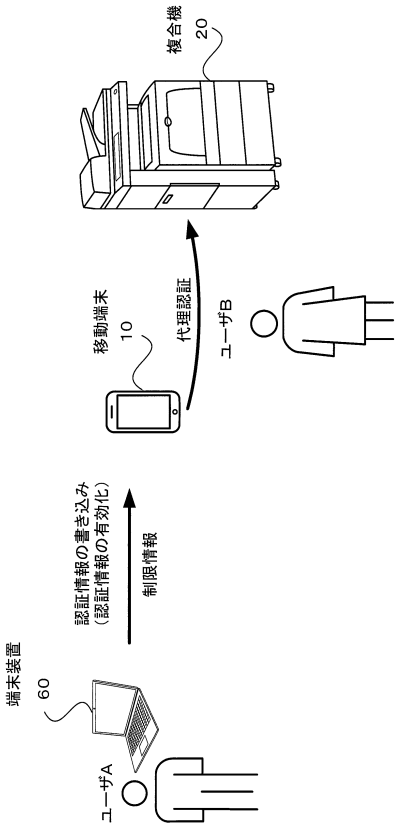
【図１】


オフィス
自宅
複合機
20
社内ネットワーク
40
無線LAN
ターミナル
移動端末
10
ユーザB
ユーザAの
代理人
ルータ
30
インターネット
50
端末装置
60
無線LAN
ターミナル
70
ユーザA
（テレワーク
利用者）

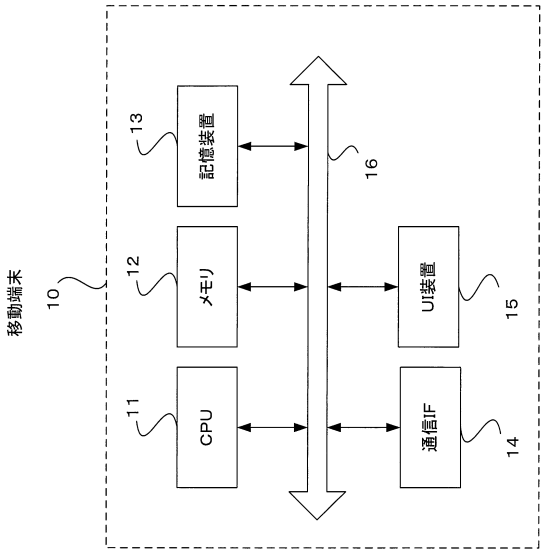
【図２】


複合機
20
80A
（ユーザA用）
認証
認証
80B
（ユーザB用）
ユーザA
ユーザB

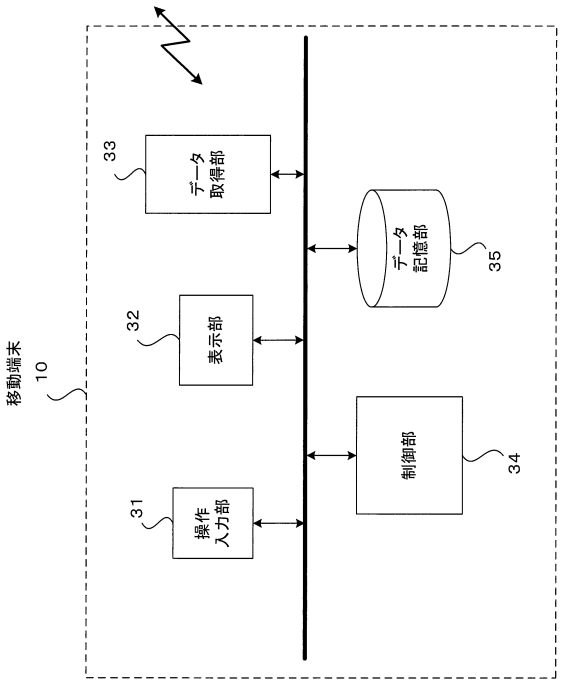
【図３】


複合機
20
移動端末
10
代理認証
ユーザB
認証情報の書き込み
（認証情報の有効化）
制限情報
端末装置
60
ユーザA

【図４】


移動端末
10
CPU
11
メモリ
12
記憶装置
13
通信IF
14
UI装置
15
16

【図５】

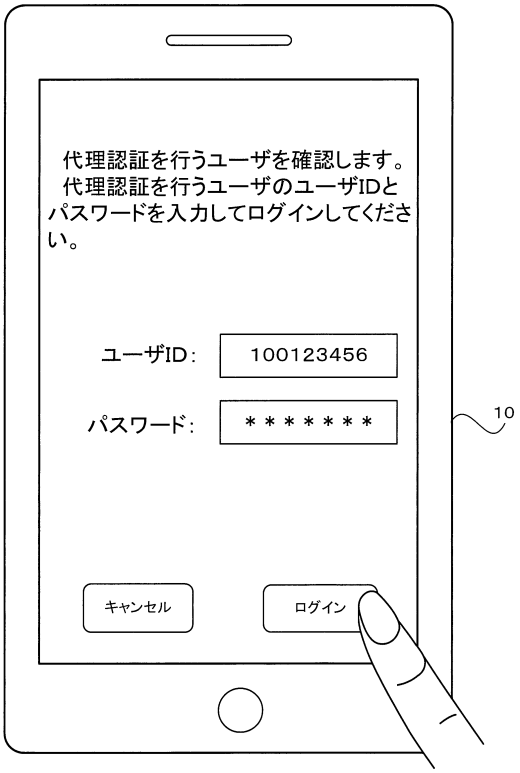


【図６】

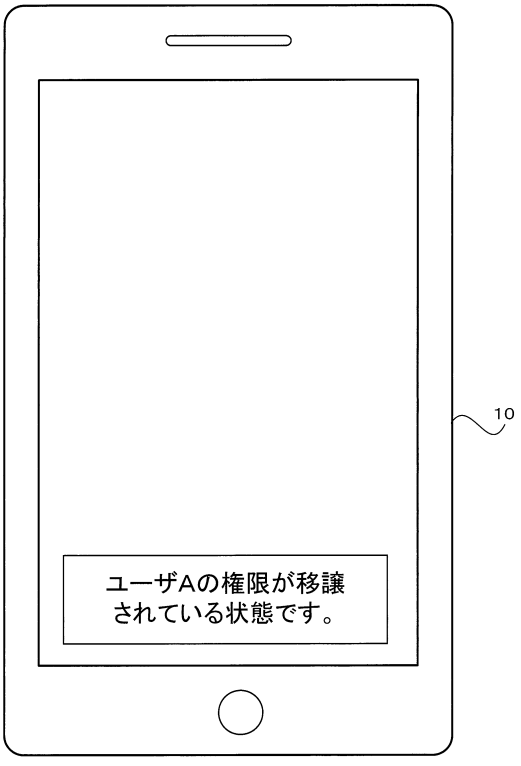
制限情報例

制限項目		制限内容
許可ユーザ		ユーザB
使用可能期間		1日
使用可能回数		10回
使用可能機能	コピー	使用可
	スキャン	使用不可
	FAX	使用可
	プリント	使用可
認証時の確認要否		不要

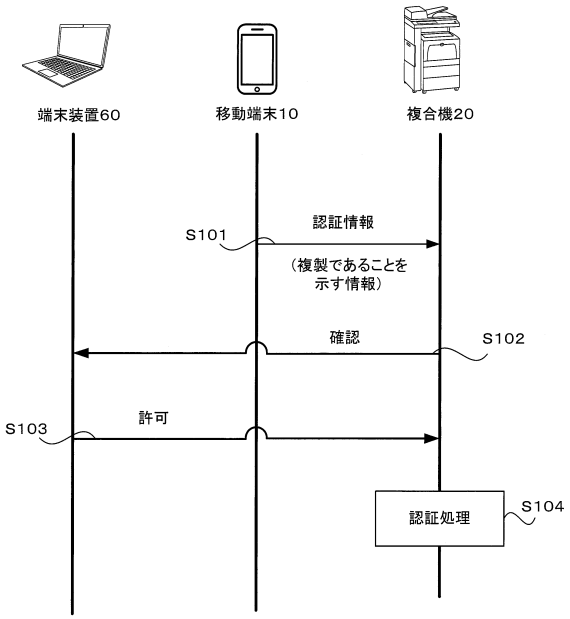
【図７】



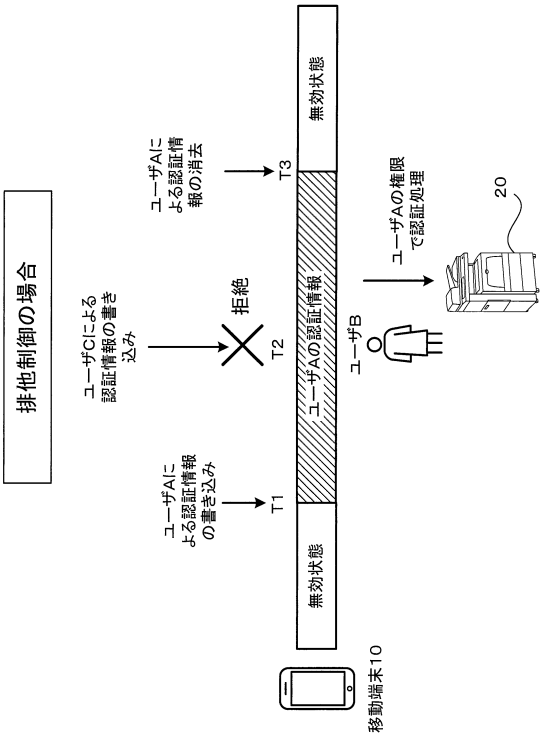
【図８】



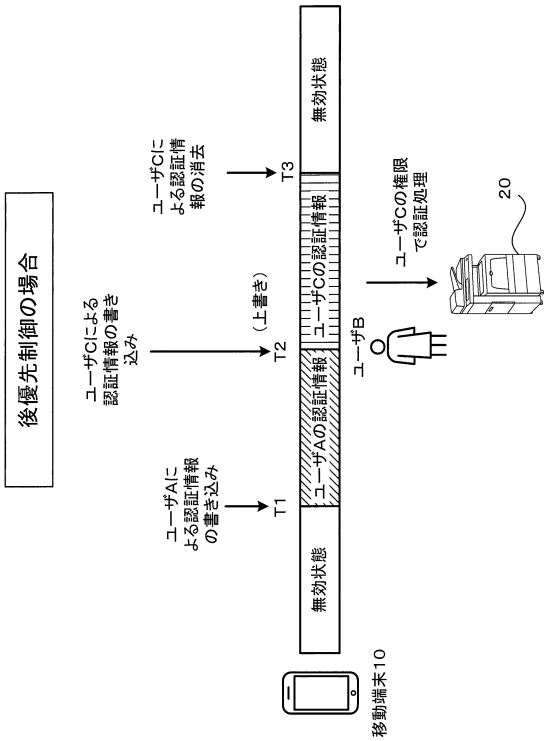
【図９】


端末装置60
移動端末10
複合機20
S101
認証情報
（複製であることを示す情報）
確認
S102
許可
S103
認証処理
S104

【図１０】


排他制御の場合
ユーザCによる認証情報の書き込み
拒絶
T2
ユーザAによる認証情報の消去
T3
ユーザAによる認証情報の書き込み
T1
無効状態
ユーザAの認証情報
無効状態
ユーザB
ユーザAの権限で認証処理
20
移動端末10

【図１１】


後優先制御の場合
ユーザCによる認証情報の書き込み
（上書き）
T2
ユーザCによる認証情報の消去
T3
ユーザAによる認証情報の書き込み
T1
無効状態
ユーザAの認証情報
ユーザCの認証情報
無効状態
ユーザB
ユーザCの権限で認証処理
20
移動端末10

フロントページの続き

(56)参考文献 特開２００６－２２１５０６（ＪＰ，Ａ）
特開２００５－１８２１３９（ＪＰ，Ａ）
特開２０１０－０２６７５８（ＪＰ，Ａ）
特開２００４－０３２２２０（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１