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

特許第5018103号
(P5018103)

(45)発行日　平成24年9月5日(2012.9.5)　(24)登録日　平成24年6月22日(2012.6.22)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 21/20 131D
G09C 1/00 (2006.01)　G09C 1/00 640E

請求項の数 8　(全 15 頁)

(21)出願番号　特願2007-12776(P2007-12776)
(22)出願日　平成19年1月23日(2007.1.23)
(65)公開番号　特開2008-181217(P2008-181217A)
(43)公開日　平成20年8月7日(2008.8.7)
審査請求日　平成21年12月21日(2009.12.21)

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳
(74)代理人　100085279
弁理士　西元　勝一
(74)代理人　100099025
弁理士　福田　浩志
(72)発明者　長村　徹
神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、画像処理装置、及び情報処理方法

(57)【特許請求の範囲】
【請求項１】
ユーザを識別する識別情報を含む複数の認証情報を予め記憶した記憶手段と、
入力された前記認証情報を、前記記憶手段に記憶された認証情報と照合する照合手段と、
前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定する居場所判定手段と、
前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記照合手段によって、前記入力された認証情報が照合され、かつ、前記居場所判定手段によって居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証する認証手段と、
を含む情報処理装置。
【請求項２】
ユーザを識別する識別情報を含む複数の認証情報を予め記憶した認証情報記憶装置に、入力された前記認証情報を照合させて、照合結果を受信する受信手段と、
前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場

合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定する居場所判定手段と、

前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記受信手段によって、前記入力された認証情報が照合されたことを示す照合結果を受信し、かつ、前記居場所判定手段によって居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証する認証手段と、

を含む情報処理装置。

【請求項３】

前記認証情報が自装置の設置場所において入力されたか、又は遠隔地に設置された端末装置からネットワークを介して入力されたかを判定する入力場所判定手段と、

前記スケジュール記憶装置に記憶された前記入力された認証情報の識別情報が示すユーザのスケジュール情報に基づいて、前記認証対象のユーザが、自装置を使用できる地域に存在しているか否かを判定する判定手段とを更に含み、

前記居場所判定手段は、前記入力場所判定手段によって前記遠隔地に設定された端末装置から入力されたと判定された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報に基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定し、

前記認証手段は、前記自端末の設置場所において入力されたと判定された場合には、前記入力された認証情報が照合され、かつ、前記判定手段によって前記認証対象のユーザが、自装置を使用できる地域に存在していると判定された場合に、前記認証対象のユーザが正当なユーザであると認証する請求項１記載の情報処理装置。

【請求項４】

前記認証情報が自装置の設置場所において入力されたか、又は遠隔地に設置された端末装置からネットワークを介して入力されたかを判定する入力場所判定手段と、

前記スケジュール記憶装置に記憶された前記入力された認証情報の識別情報が示すユーザのスケジュール情報に基づいて、前記認証対象のユーザが、自装置を使用できる地域に存在しているか否かを判定する判定手段とを更に含み、

前記居場所判定手段は、前記入力場所判定手段によって前記遠隔地に設定された端末装置から入力されたと判定された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報に基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定し、

前記認証手段は、前記自端末の設置場所において入力されたと判定された場合には、前記受信手段によって、前記入力された認証情報が照合されたことを示す照合結果を受信し、かつ、前記判定手段によって前記認証対象のユーザが、自装置を使用できる地域に存在していると判定された場合に、前記認証対象のユーザが正当なユーザであると認証する請求項２記載の情報処理装置。

【請求項５】

前記認証手段による認証において、前記居場所判定手段の判定結果を用いるか否かをユーザ毎に設定する設定手段を更に含み、

前記認証手段は、前記認証対象のユーザに対して前記判定結果を用いないと設定されている場合には、前記入力された認証情報が照合されると、前記認証対象のユーザが正当なユーザであると認証する請求項１～請求項４の何れか１項記載の情報処理装置。

【請求項６】

請求項１～請求項５の何れか１項記載の情報処理装置と、

画像データに基づいて、記録用紙に画像を形成する画像形成手段と、

を含む画像処理装置。
【請求項７】
ユーザを識別する識別情報を含む複数の認証情報を予め記憶した記憶手段を含む情報処理装置の情報処理方法であって、
入力された前記認証情報を、前記記憶手段に記憶された認証情報と照合し、
前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定し、
前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記入力された認証情報が照合され、かつ、居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証することを特徴とする情報処理方法。
【請求項８】
ユーザを識別する識別情報を含む複数の認証情報を予め記憶した認証情報記憶装置に、入力された前記認証情報を照合させて、照合結果を受信し、
前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定し、
前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記入力された認証情報が照合されたことを示す照合結果を受信し、かつ、居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証することを特徴とする情報処理方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、画像処理装置、及び情報処理方法に係り、特に、入力された識別情報及び認証情報に基づいて、ユーザを認証する情報処理装置、画像処理装置、及び情報処理方法に関する。
【背景技術】
【０００２】
従来、画像処理装置などの情報処理装置の内部または外部のサーバに保持した認証情報や権利情報を使って、情報処理装置の使用を制限する技術が知られている。画像処理装置における権利情報として、例えば、サービスごとの許可又は禁止、カラー又は白黒の許可又は禁止、サービスごとの使用量上限、当該画像処理装置の使用の許可又は禁止などが設定される。
【０００３】
また、認証情報としてユーザＩＤ及びパスワードを用い、入力されたユーザＩＤ及びパスワードと照合して認証判断を行っており、認証を行う画像処理装置として、外部のサーバにユーザＩＤ及びパスワードを対応させて記憶させ、外部のサーバを利用して認証処理を行う画像処理装置が知られている（特許文献１）。
【０００４】
また、Ｗｉｎｄｏｗｓ（登録商標）などのシステムでは、セキュリティの強度を向上させるために、認証情報として、ユーザＩＤごとに設定される使用可能な期日及び時間帯を

示す情報を更に利用し、認証判断を行っている。
【特許文献１】特開２００４－１２９２４７
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記のＷｉｎｄｏｗｓ（登録商標）などのシステムで使われている使用可能な期日及び時間帯を示す情報を認証判断で用いた場合、使用可能期日及び時間帯がユーザＩＤごとに固定的に設定されているため、設定された時間外では、正当なユーザであっても情報処理装置を使用できないという不都合が発生してしまう、という問題がある。
【０００６】
本発明は、上記の問題点を解決するためになされたもので、セキュリティの強度を高くすると共に、正当なユーザであるか否かを適切に認証判断することができる情報処理装置、画像処理装置、及び情報処理方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
上記の目的を達成するために第１の発明に係る情報処理装置は、ユーザを識別する識別情報を含む複数の認証情報を予め記憶した記憶手段と、入力された前記認証情報を、前記記憶手段に記憶された認証情報と照合する照合手段と、前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定する居場所判定手段と、前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記照合手段によって、前記入力された認証情報が照合され、かつ、前記居場所判定手段によって居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証する認証手段とを含んで構成されている。
【０００８】
また、第２の発明に係る情報処理方法は、ユーザを識別する識別情報を含む複数の認証情報を予め記憶した記憶手段を含む情報処理装置の情報処理方法であって、入力された前記認証情報を、前記記憶手段に記憶された認証情報と照合し、前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定し、前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記入力された認証情報が照合され、かつ、居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証することを特徴としている。
【０００９】
第１の発明及び第２の発明によれば、入力された認証情報を、記憶手段に記憶された認証情報と照合し、また、認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定する。
【００１０】
そして、遠隔地に設定された端末装置から前記認証情報が入力された場合に、入力された認証情報が照合され、かつ、居場所と所在地とが一致すると判定されたときに、認証対

象のユーザが正当なユーザであると認証する。

【００１１】

このように、認証情報が照合され、認証対象のユーザの居場所と端末装置の所在地とが一致すると判定されたときに、正当なユーザであると認証するため、セキュリティの強度を高くすると共に、正当なユーザであるか否かを適切に認証判断することができる。

【００１２】

第３の発明に係る情報処理装置は、ユーザを識別する識別情報を含む複数の認証情報を予め記憶した認証情報記憶装置に、入力された前記認証情報を照合させて、照合結果を受信する受信手段と、前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定する居場所判定手段と、前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記受信手段によって、前記入力された認証情報が照合されたことを示す照合結果を受信し、かつ、前記居場所判定手段によって居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証する認証手段とを含んで構成されている。

【００１３】

第４の発明に係る情報処理方法は、ユーザを識別する識別情報を含む複数の認証情報を予め記憶した認証情報記憶装置に、入力された前記認証情報を照合させて、照合結果を受信し、前記認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定し、前記遠隔地に設定された端末装置から前記認証情報が入力された場合に、前記入力された認証情報が照合されたことを示す照合結果を受信し、かつ、居場所と所在地とが一致すると判定されたときに、前記認証対象のユーザが正当なユーザであると認証することを特徴としている。

【００１４】

第３の発明及び第４の発明によれば、ユーザを識別する識別情報を含む複数の認証情報を予め記憶した認証情報記憶装置に、入力された認証情報を照合させて、照合結果を受信し、また、認証情報が、遠隔地に設置された端末装置からネットワークを介して入力された場合に、端末装置の所在地を示す所在地情報を管理する端末管理装置の前記端末装置の所在地情報と、ユーザの現在の居場所を示す居場所情報を含むスケジュール情報をユーザ毎に予め記憶したスケジュール記憶装置の前記スケジュール情報とに基づいて、前記入力された認証情報の識別情報が示すユーザの居場所情報の居場所と前記所在地情報が示す所在地とが一致するか否かを判定する。

【００１５】

そして、遠隔地に設定された端末装置から前記認証情報が入力された場合に、入力された認証情報が照合されたことを示す照合結果を受信し、かつ、居場所と所在地とが一致すると判定されたときに、認証対象のユーザが正当なユーザであると認証する。

【００１６】

このように、認証情報が照合され、認証対象のユーザの居場所と端末装置の所在地とが一致すると判定されたときに、正当なユーザであると認証するため、セキュリティの強度を高くすると共に、正当なユーザであるか否かを適切に認証判断することができる。

【００１７】

認証対象のユーザのスケジュール情報を利用して、ユーザの居場所と端末装置の所在地とが一致するか否かを判定することができるため、ユーザ操作が煩雑にならず、かつ、既

存のスケジュールを記憶している装置を利用して、コストを抑制することができる。

【００２０】

また、端末装置の所在地情報を管理する端末管理装置を利用して、遠隔地からのアクセスに対しても、セキュリティの強度を高くすることができる。

【００２１】

上記の情報処理装置は、認証手段による認証において、居場所判定手段の判定結果を用いるか否かをユーザ毎に設定する設定手段を更に含み、認証手段は、認証対象のユーザに対して判定結果を用いないと設定されている場合には、入力された認証情報が照合されると、認証対象のユーザが正当なユーザであると認証することができる。これにより、ユーザ毎に、認証において、ユーザの居場所と端末装置の所在地とが一致するか否かの判定を利用するか否かを設定できるため、利便性を向上させることができる。

【００２３】

第５の発明に係る画像形成装置は、上記の情報処理装置と、画像データに基づいて、記録用紙に画像を形成する画像形成手段とを含んで構成されている。

【００２４】

第５の発明に係る画像形成装置によれば、情報処理装置によって正当なユーザであると認証されたユーザによる画像形成装置の使用が許可され、ユーザの指示に従って、記録用紙に画像を形成する。

【発明の効果】

【００２５】

以上説明したように、本発明の情報処理装置、画像処理装置、及び情報処理方法によれば、認証情報が照合され、認証対象のユーザの居場所と端末装置の所在地とが一致すると判定されたときに、正当なユーザであると認証するため、セキュリティの強度を高くすると共に、正当なユーザであるか否かを適切に認証判断することができる、という効果が得られる。

【発明を実施するための最良の形態】

【００２６】

以下、本発明の実施の形態について図面を参照して説明する。なお、本実施の形態では、画像処理システムの画像形成装置に本発明を適用した場合について説明する。

【００２７】

図１に示すように、本発明の第１の実施の形態に係る画像処理システム１０は、画像データに基づいて記録用紙に画像を形成する画像形成装置１２と、ユーザのスケジュールを示すスケジュール情報を記憶し、管理するスケジュール情報管理サーバ１４と、複数のクライアントＰＣ１６と、画像形成装置１２、スケジュール情報管理サーバ１４、及びクライアントＰＣ１６を相互に接続するネットワーク１８とを備えている。なお、本実施の形態では、画像形成装置１２がユーザの勤務場所に設置されている場合を例に説明する。

【００２８】

画像形成装置１２は、各種プログラムやパラメータ等が記憶されたＲＯＭ２２、各種プログラムを実行するＣＰＵ２４、ＣＰＵ２４による各種プログラムの実行時におけるワークエリア等として用いられるＲＡＭ２６、画像データや後述する認証処理ルーチンを実行するためのプログラムなどが記憶されたＨＤＤ３２、及びこれらを相互に接続するためのバス３０が設けられている。

【００２９】

ＨＤＤ３２には、認証情報としてのユーザＩＤ及びパスワードを対応させて予め登録した認証管理情報データベースが記録されている。

【００３０】

また、画像形成装置１２には、さらに、原稿を読みとって画像データを生成するスキャナ３４と、画像データに基づいて感光体に静電潜像を記録し、静電潜像をモノクロトナーまたはカラートナーを用いて現像し、現像した画像を記録用紙に転写して出力する印字部３６と、画像形成装置１２の各種処理を指示するための操作ボタンや操作パネルからなる

操作パネル部３８と、ネットワーク１８を介して通信するためのネットワークインタフェース４０とが設けられており、これらもバス３０に接続されている。

【００３１】

なお、画像形成装置１２は、従来公知の画像形成装置の一般的構成を備えていればよく、本実施の形態では、画像形成装置１２の他の構成及び一般的処理の説明を省略する。

【００３２】

スケジュール情報管理サーバ１４に記憶されているスケジュール情報は、認証管理情報データベースに登録されているユーザＩＤと同じユーザＩＤと対応して記憶されており、スケジュール情報は、ユーザの勤怠情報（本日の出勤時刻及び退勤時刻）と居場所情報（本日の任意の時間帯におけるユーザの居場所）とから構成されている。例えば、スケジュール情報管理サーバ１４は、勤怠情報をユーザ毎に記憶した勤怠情報データベースを備えており、一般ユーザの操作によって、自分の出勤時刻及び退勤時刻の追加と、自分の勤務時間の集計と、自分の出勤時刻及び退勤時刻の問い合わせとを行うことができる。また、管理者の操作によって、各ユーザの出勤時刻及び退勤時刻の修正及び削除と、各ユーザの出勤時刻及び退勤時刻の問い合わせとを行うことができる。

【００３３】

また、スケジュール情報管理サーバ１４は、行動予定を共有するグループウェアと、居場所情報を記憶した居場所情報データベースとを備えており、一般ユーザがグループウェアを用いて、自分の居場所情報を含むスケジュールの追加、修正、及び削除と、自分と自分以外のスケジュールの問い合わせとを行うことができる。

【００３４】

スケジュール情報管理サーバ１４は、既存のそれぞれのシステムから、問合せを受けることができるインタフェースを備えており、ユーザＩＤを指定した問合せを受けると、指定されたユーザＩＤを用いて、勤怠情報データベースに対して、指定のユーザＩＤの出勤時刻及び退勤時刻を問い合わせ、出勤時刻がないときは出勤前、出勤時刻があり退勤時刻がないときは勤務中、出勤時刻及び退勤時刻の両方があるときは退勤後、と判断し、現在勤務中であるか否かを応答する。また、指定されたユーザＩＤを用いて、居場所情報データベースに対して、指定のユーザＩＤの本日の居場所情報を問い合わせ、得た居場所情報の中から現在の居場所を応答する。

【００３５】

クライアントＰＣ１６では、ユーザによって、画像データの作成及び編集を行い、画像データに基づく画像形成処理の要求を、ネットワーク１８を介して画像形成装置１２へ送信することができる。

【００３６】

次に、第１の実施の形態に係る画像処理システム１０の作用を説明する。

【００３７】

まず、管理者の操作によって、ユーザ毎にユーザＩＤ及びパスワードをＨＤＤ３２の認証管理情報データベースに登録しておく。また、スケジュール情報管理サーバ１４において、各ユーザの操作により、居場所情報データベースに自己のスケジュールとして時間帯及び居場所情報を予め登録しておき、また、各ユーザが出勤した場合には、出勤時刻を勤怠情報データベースに登録し、退勤した場合には、退勤時刻を勤怠情報データベースに登録する。

【００３８】

そして、ユーザが画像形成装置１２の利用を要求したときに、画像形成装置１２において、図２に示す認証処理ルーチンが実行される。

【００３９】

ステップ１００において、ユーザの認証情報としてユーザＩＤ及びパスワードが入力されたか否かを判定し、ユーザが操作パネル部３８を操作して、ユーザＩＤ及びパスワードが入力された場合や、ユーザがクライアントＰＣ１６を操作して、ネットワーク１８を介して画像形成装置１２にユーザＩＤ及びパスワードを入力した場合には、ステップ１００

からステップ１０２へ進み、照合処理を行い、入力されたユーザＩＤ及びパスワードと、ＨＤＤ３２の認証管理情報データベースに予め登録されたユーザＩＤ及びパスワードとを照合する。

【００４０】

そして、ステップ１０４において、ステップ１０２の照合処理で、照合されたか否かを判定し、照合されなかった場合には、ステップ１０６で、操作パネル部３８に認証失敗メッセージを表示して、認証処理ルーチンを終了するが、一方、照合された場合には、ステップ１０８で、リモートアクセスであるか否かを判定する。なお、ステップ１０６において、ネットワーク１８を介してクライアントＰＣ１６から画像形成装置１２にアクセスされた場合には、クライアントＰＣ１６に認証失敗メッセージを送信することにより、クライアントＰＣ１６において認証失敗メッセージを表示する。

【００４１】

ステップ１０８において、ユーザが操作パネル部３８を操作して、自装置に直接アクセスしている場合には、ステップ１１０へ移行するが、一方、遠隔地に設置されたクライアントＰＣ１６からネットワーク１８を介してアクセスされた場合には、スケジュール情報に基づく判定を行わずに、ステップ１１８へ移行する。

【００４２】

ステップ１１０では、入力されたユーザＩＤが示すユーザについて、スケジュール情報に基づく判定を行うように設定されているか否かを判定する。画像形成装置１２では、操作パネル部３８を操作して、認証情報に基づく判定の他に、スケジュール情報に基づく判定を用いてユーザ認証を行うか否かをユーザ毎に予め設定することができ、ここで、認証対象のユーザに対して、スケジュール情報の判定を行わないように予め設定されている場合には、スケジュール情報の判定を行わずに、ステップ１１８へ移行するが、スケジュール情報の判定を行うように設定されている場合には、ステップ１１２へ移行する。

【００４３】

ステップ１１２では、スケジュール情報管理サーバ１４に対して、入力されたユーザＩＤが示すユーザのスケジュール情報の問合せを行い、ステップ１１４において、スケジュール情報管理サーバ１４から、勤務中であるか否かと現在の居場所とを示すスケジュール情報を取得したか否かを判定し、スケジュール情報管理サーバ１４の勤怠情報データベースから、認証対象のユーザが勤務中であるか否かを示す応答メッセージを取得すると共に、居場所情報データベースから、認証対象のユーザの現在の居場所を示す応答メッセージを取得すると、ステップ１１６へ進む。

【００４４】

ステップ１１６では、スケジュール情報管理サーバ１４からの応答メッセージに基づいて、認証対象のユーザが勤務中であって、かつ、現在の居場所が、自装置を使用できる地域としての自装置の設置場所（本実施の形態の場合には、勤務場所）であるか否かを判定し、出勤前又は退勤後である場合や、現在の居場所が勤務場所以外である場合には、ステップ１０６へ移行して、認証失敗メッセージを表示するが、一方、ユーザが勤務中であり、現在勤務場所に存在している場合には、ユーザが正当なユーザであると認証して、ステップ１１８へ移行し、操作パネル部３８に認証成功メッセージを表示して、認証処理ルーチンを終了する。なお、ネットワーク１８を介してクライアントＰＣ１６からアクセスされている場合には、クライアントＰＣ１６に認証成功メッセージを送信することにより、クライアントＰＣ１６において認証成功メッセージを表示する。

【００４５】

そして、上記の認証処理ルーチンにおいて、認証が成功した場合には、ユーザによる画像形成装置１２の利用が許可され、ユーザの操作に基づいて、印刷ジョブが入力され、印字部３６において、印刷ジョブの画像データに基づいて、記録用紙に画像が形成される。一方、認証が失敗した場合には、ユーザによる画像形成装置１２の利用は禁止される。

【００４６】

以上説明したように、第１の実施の形態に係る画像形成システムによれば、認証情報が

照合され、かつ、認証対象のユーザが勤務中であり、自装置を使用できる勤務場所に存在していると判定されたときに、正当なユーザであると認証するため、セキュリティの強度を高くすると共に、正当なユーザであるか否かを適切に認証判断することができる。

【００４７】

また、認証対象のユーザのスケジュール情報を利用して、ユーザが現在自装置を使用できる地域に存在しているか否かを判定するため、既存のスケジュールを記憶している装置を利用して判定することができ、また、ユーザ操作をまったく従来方法と変更することなく、セキュリティの強度を高くすることができる。

【００４８】

スケジュール情報は既存の情報であり、スケジュール情報管理サーバの新規構築は不要であるため、発生するコストは連携にかかるものだけとなり、コストを抑えることができる。

【００４９】

認証において、スケジュール情報を問い合わせて、自装置を使用できる地域に存在しているか否かの判定を利用するか否かをユーザ毎に設定できるため、さまざま運用形態に対応することができ、利便性を向上させることができる。

【００５０】

また、遠隔地に設置された所在地が分からない端末装置からのリモートアクセスがあった場合には、認証判断において、自装置を使用できる地域に存在しているか否かの判定を行わずに、認証情報の照合のみによって、適切に認証を行うため、画像形成装置の利用形態に応じた適切なセキュリティ強化をすることができる。

【００５１】

また、認証情報としてユーザＩＤ及びパスワードを使う場合、単純にセキュリティの強度を高くしようとすると、パスワードの長さを長くしたり、大文字、小文字、数字、記号を組み合わせたりする必要があり、ユーザ操作が煩雑になるが、本実施の形態では、認証操作時にユーザが入力する必要のないユーザのスケジュール情報を認証判断に用いることにより、ユーザ操作を煩雑にすることなくセキュリティの強度を高くすることができる。

【００５２】

なお、上記の実施の形態では、スケジュール情報管理サーバに、勤怠情報データベースと居場所情報データベースとを備えている場合を例に説明したが、勤怠情報データベースを備えた勤怠情報管理サーバと、居場所情報データベースを備えた居場所情報管理サーバとを別々に設けるようにしてもよい。この場合には、画像形成装置は、認証処理において、勤怠情報管理サーバと居場所情報管理サーバとの各々に問合せを行えばよい。

【００５３】

また、認証対象のユーザが勤務中であるか否かの判定と現在の居場所が勤務場所であるか否かの判定との両方を用いて、正当なユーザであると認証する場合を例に説明したが、何れか一方の判定を用いて、認証処理を行うようにしてもよい。

【００５４】

また、スケジュール情報を用いて、認証対象のユーザが自装置を使用できる地域に存在しているか否かを判定する場合を例に説明したが、これに限定されるものではなく、ユーザがＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）対応携帯端末を所持している場合には、ＧＰＳシステムを利用して、認証対象のユーザの居場所を取得して、認証対象のユーザが自装置を使用できる地域に存在しているか否かを判定するようにしてもよい。

【００５５】

次に第２の実施の形態について説明する。なお、第１の実施の形態と同一構成となっている部分については、同一符号を付して説明を省略する。

【００５６】

第２の実施の形態では、画像形成装置とは別に設けられた認証情報管理サーバにおいて、ユーザＩＤ及びパスワードの認証を行うようになっている点が第１の実施の形態と異な

っている。

【００５７】

図３に示すように、第２の実施の形態に係る画像形成システム２１０には、認証管理情報データベースを備えた認証情報管理サーバ２５０が設けられており、認証情報管理サーバ２５０はネットワーク１８を介して、画像形成装置２１２と接続されている。また、認証情報管理サーバ２５０の認証管理情報データベースには、管理者の操作によって、ユーザ毎にユーザＩＤ及びパスワードが予め登録されている。

【００５８】

認証情報管理サーバ２５０は、ユーザＩＤ及びパスワードの照合依頼を受信すると、受信したユーザＩＤ及びパスワードを認証管理情報データベースに登録されているユーザＩＤ及びパスワードと照合し、照合結果を応答メッセージとして送信する。

【００５９】

なお、画像形成装置２１２のＨＤＤ２３２には、認証管理情報データベースが記憶されていない。

【００６０】

次に、第２の実施の形態に係る認証処理ルーチンについて、図４を用いて説明する。なお、第１の実施の形態と同一処理については、同一符号を付して詳細な説明を省略する。

【００６１】

まず、ステップ１００において、ユーザのユーザＩＤ及びパスワードが入力されたか否かを判定し、ステップ２７０において、認証情報管理サーバ２５０に対して、入力されたユーザＩＤ及びパスワードと共に、照合依頼を送信し、ステップ２７２において、認証情報管理サーバ２５０から照合結果を取得したか否かを判定し、認証情報管理サーバ２５０において、照合処理を行い、照合依頼対象のユーザＩＤ及びパスワードと、認証管理情報データベースに予め登録されたユーザＩＤ及びパスワードとを照合し、照合結果を示す応答メッセージを画像形成装置２１２に送信し、画像形成装置２１２で受信されると、ステップ２７４へ進む。

【００６２】

ステップ２７４では、ステップ２７２で取得された照合結果に基づいて、入力されたユーザＩＤ及びパスワードが照合されたか否かを判定し、照合されなかった場合には、ステップ１０６で、操作パネル部３８に認証失敗メッセージを表示して、認証処理ルーチンを終了するが、一方、照合された場合には、ステップ１０８で、リモートアクセスであるか否かを判定する。

【００６３】

ステップ１０８において、ユーザが自装置に直接アクセスしている場合には、ステップ１１０へ移行するが、一方、遠隔地に設置されたクライアントＰＣ１６からネットワーク１８を介してアクセスされた場合には、スケジュール情報に基づく判定を行わずに、ステップ１１８へ移行する。

【００６４】

ステップ１１０では、認証対象のユーザについて、スケジュール情報に基づく判定を行うように設定されているか否かを判定し、スケジュール情報の判定を行わないように設定されている場合には、スケジュール情報に基づく判定を行わずに、ステップ１１８へ移行するが、スケジュール情報の判定を行うように設定されている場合には、ステップ１１２へ移行する。

【００６５】

ステップ１１２では、スケジュール情報管理サーバ１４に対して、スケジュール情報の問合せを行い、ステップ１１４において、スケジュール情報管理サーバ１４からスケジュール情報を取得すると、ステップ１１６において、スケジュール情報管理サーバ１４から取得したスケジュール情報に基づいて、認証対象のユーザが勤務中であって、かつ、現在の居場所が自装置の設置場所であるか否かを判定し、出勤前又は退勤後である場合や、現在の居場所が勤務場所以外である場合には、ステップ１０６へ移行して、認証失敗メッセ

ージを表示するが、一方、ユーザが勤務中であり、現在勤務場所に存在している場合には、ステップ１１８へ移行し、操作パネル部３８に認証成功メッセージを表示して、認証処理ルーチンを終了する。

【００６６】

そして、上記の認証処理ルーチンにおいて、認証が成功した場合には、ユーザによる画像形成装置２１２の利用が許可されるが、一方、認証が失敗した場合には、ユーザによる画像形成装置２１２の利用は禁止される。

【００６７】

以上説明したように、第２の実施の形態に係る画像形成システムによれば、認証情報の照合を、画像形成装置の外部にある認証情報管理サーバに行わせるため、画像形成装置の処理負担を軽減して、認証におけるセキュリティの強度を高くすることができる。

【００６８】

次に第３の実施の形態について説明する。なお、第１の実施の形態と同様の構成となっている部分については、同一符号を付して、説明を省略する。

【００６９】

第３の実施の形態では、クライアントＰＣの所在地を管理する端末管理サーバから、リモートアクセスしてきたクライアントＰＣの所在地を取得して、リモートアクセスしてきたクライアントＰＣの所在地に認証対象のユーザが存在しているか否かを判定して、ユーザの認証を行う点が第１の実施の形態と異なっている。

【００７０】

図５に示すように、第３の実施の形態に係る画像形成システム３１０には、ネットワーク１８に接続されている複数のクライアントＰＣ１６の各々の所在地を管理している端末管理サーバ３５０が設けられ、ネットワーク１８を介して画像形成装置１２に接続されている。

【００７１】

端末管理サーバ３５０は、クライアントＰＣ１６の所在地の問合せを受けると、問合せ対象のクライアントＰＣ１６の所在地を示す応答メッセージを問合せ元に送信する。

【００７２】

次に、第３の実施の形態に係る認証処理ルーチンについて、図６を用いて説明する。なお、第１の実施の形態と同一処理については、同一符号を付して詳細な説明を省略する。

【００７３】

まず、ステップ１００において、ユーザのユーザＩＤ及びパスワードが入力されたか否かを判定し、ステップ１０２で、入力されたユーザＩＤ及びパスワードの照合処理を行う。そして、ステップ１０４において、ステップ１０２の照合処理で、照合されたか否かを判定し、照合されなかった場合には、ステップ１０６で、操作パネル部３８に認証失敗メッセージを表示して、認証処理ルーチンを終了するが、一方、照合された場合には、ステップ１１０において、入力されたユーザＩＤが示すユーザについて、スケジュール情報に基づく判定を行うように設定されているか否かを判定し、スケジュール情報の判定を行わないように予め設定されている場合には、ステップ１１８へ移行するが、スケジュール情報の判定を行うように設定されている場合には、ステップ１１２へ移行する。

【００７４】

ステップ１１２では、スケジュール情報管理サーバ１４に対して、スケジュール情報の問合せを行い、ステップ１１４において、スケジュール情報を取得したか否かを判定し、スケジュール情報管理サーバ１４からスケジュール情報を取得すると、ステップ３７０において、リモートアクセスであるか否かを判定し、ユーザが自装置に直接アクセスしている場合には、ステップ１１６へ移行するが、一方、遠隔地に設置されたクライアントＰＣ１６からネットワーク１８を介してアクセスされた場合には、ステップ３７２へ移行する。

【００７５】

ステップ１１６では、スケジュール情報管理サーバ１４から取得したスケジュール情報

に基づいて、認証対象のユーザが勤務中であって、かつ、現在の居場所が自装置の設置場所であるか否かを判定し、出勤前又は退勤後である場合や、現在の居場所が勤務場所以外である場合には、ステップ１０６へ移行して、認証失敗メッセージを表示するが、一方、ユーザが勤務中であり、現在勤務場所に存在している場合には、ステップ１１８へ移行し、操作パネル部３８に認証成功メッセージを表示し、又は、クライアントＰＣ１６に認証成功メッセージを送信して、認証処理ルーチンを終了する。

【００７６】

ステップ３７２では、端末管理サーバ３５０に対して、画像形成装置１２にリモートアクセスしているクライアントＰＣ１６の所在地を問合せ、ステップ３７４において、端末管理サーバ３５０からリモートアクセス元の所在地を取得したか否かを判定し、端末管理サーバ３５０が所在地の問合せを受けて、リモートアクセスしているクライアントＰＣ１６の所在地を示す応答メッセージを画像形成装置１２に送信すると、ステップ３７６へ進み、スケジュール情報管理サーバ１４から取得したスケジュール情報及び端末管理サーバ３５０から取得した所在地に基づいて、認証対象のユーザが勤務中であって、かつ、現在の居場所がアクセス元の所在地であるか否かを判定し、出勤前又は退勤後である場合や、現在の居場所がアクセス元の所在地以外である場合には、ステップ１０６へ移行して、認証失敗メッセージを表示するが、一方、ユーザが勤務中であり、現在アクセス元の所在地に存在している場合には、ステップ１１８へ移行し、操作パネル部３８に認証成功メッセージを表示し、又は、クライアントＰＣ１６に認証成功メッセージを送信して、認証処理ルーチンを終了する。

【００７７】

そして、上記の認証処理ルーチンにおいて、認証が成功した場合には、ユーザによる画像形成装置１２の利用が許可されるが、一方、認証が失敗した場合には、ユーザによる画像形成装置１２の利用は禁止される。

【００７８】

以上説明したように、第３の実施の形態に係る画像形成システムによれば、クライアントＰＣの所在地を管理する端末管理装置を合わせて利用することにより、遠隔地からのアクセスに対しても、セキュリティの強度を高くすることができる。

【図面の簡単な説明】

【００７９】

【図１】本発明の第１の実施の形態に係る画像形成システムの構成を示す概略図である。

【図２】本発明の第１の実施の形態に係る画像形成装置の認証処理ルーチンの内容を示すフローチャートである。

【図３】本発明の第２の実施の形態に係る画像形成システムの構成を示す概略図である。

【図４】本発明の第２の実施の形態に係る画像形成装置の認証処理ルーチンの内容を示すフローチャートである。

【図５】本発明の第３の実施の形態に係る画像形成システムの構成を示す概略図である。

【図６】本発明の第３の実施の形態に係る画像形成装置の認証処理ルーチンの内容を示すフローチャートである。

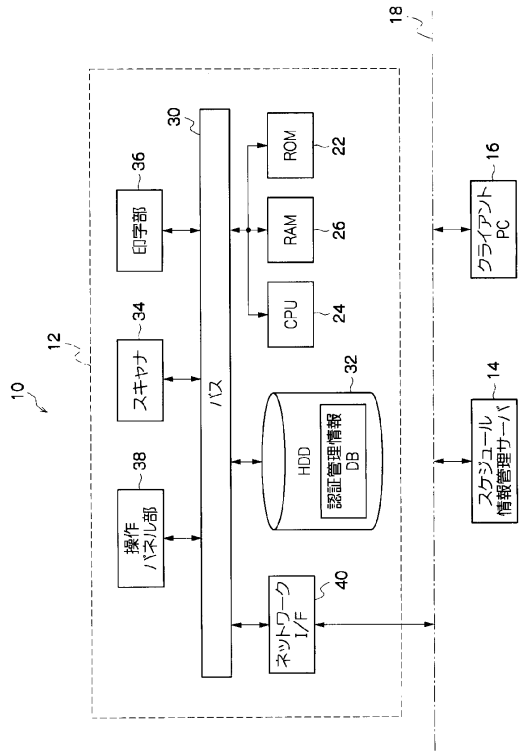
【符号の説明】

【００８０】

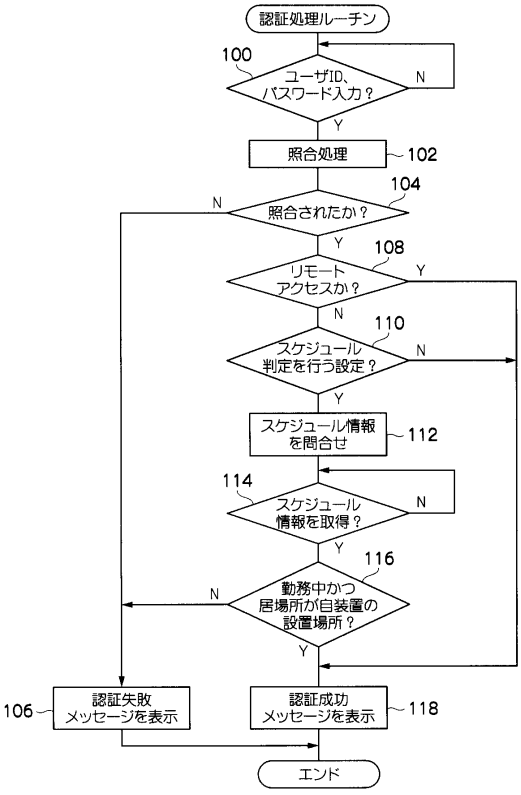
１０、２１０、３１０　画像処理システム
１２、２１２　画像形成装置
１４　スケジュール情報管理サーバ
１６　クライアントＰＣ
１８　ネットワーク
２２　ＲＯＭ
２４　ＣＰＵ
２６　ＲＡＭ
３２　ＨＤＤ

３６　印字部
３８　操作パネル部
２５０　認証情報管理サーバ
３５０　端末管理サーバ

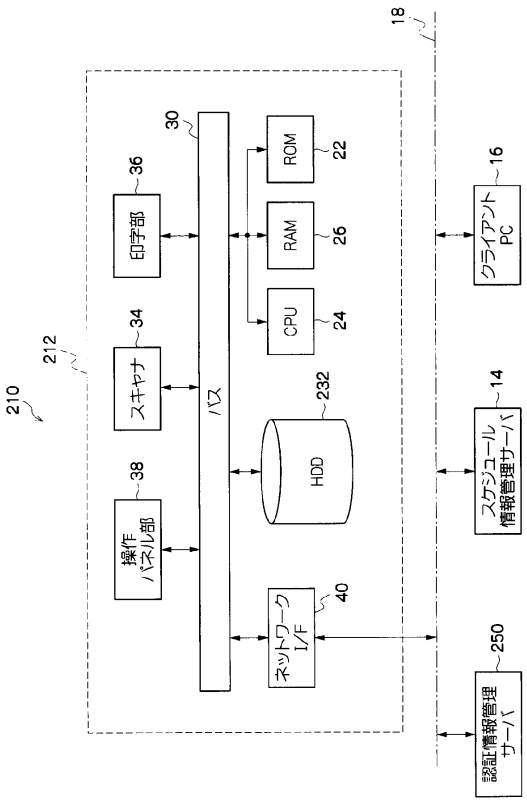
【図１】



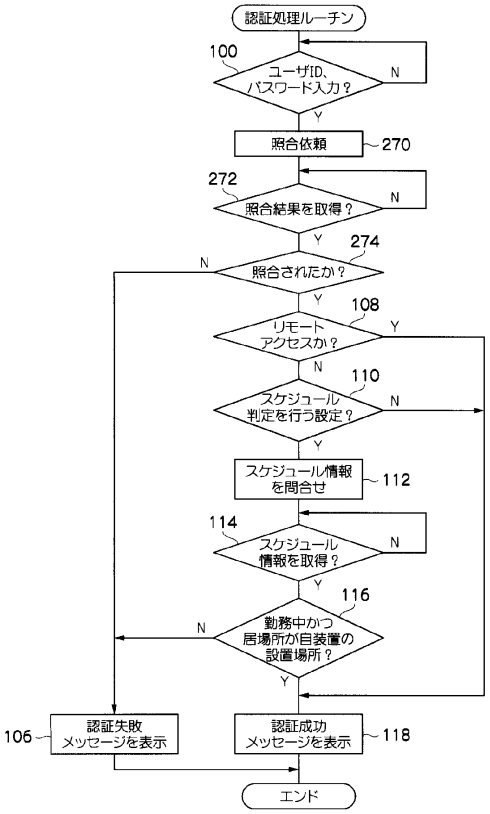
【図２】



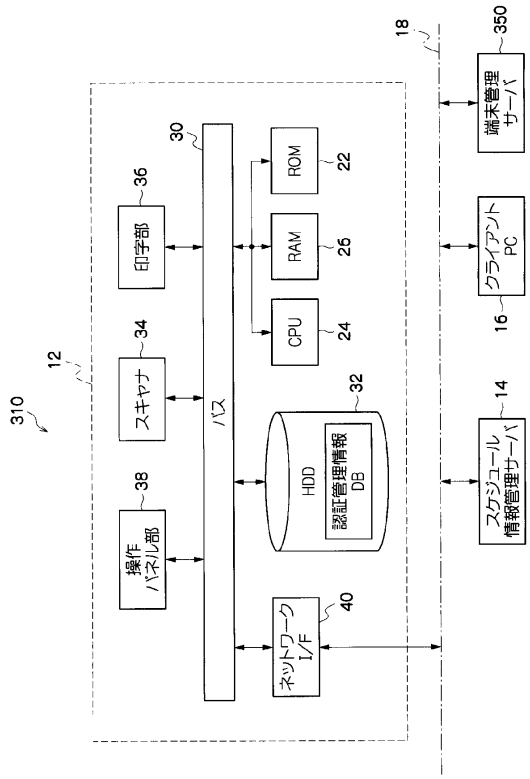
【図３】


18
30
ROM
22
印字部
36
RAM
26
クライアントPC
16
CPU
24
212
スキャナ
34
バス
232
HDD
スケジュール情報管理サーバ
14
210
操作パネル部
38
ネットワークI/F
40
250
認証情報管理サーバ

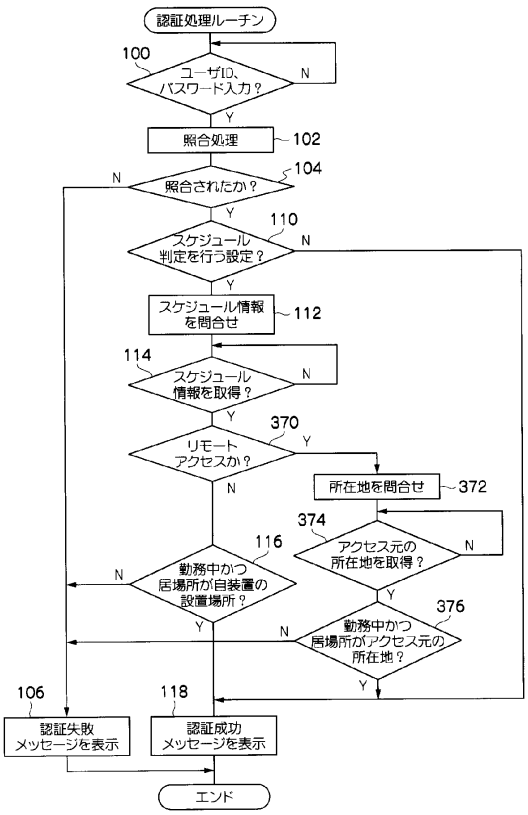
【図４】


認証処理ルーチン
100
ユーザID、パスワード入力？
N
Y
照合依頼
270
272
照合結果を取得？
N
Y
274
照合されたか？
N
Y
108
リモートアクセスか？
Y
N
110
スケジュール判定を行う設定？
N
Y
スケジュール情報を問合せ
112
114
スケジュール情報を取得？
N
Y
116
勤務中かつ居場所が目装置の設置場所？
N
Y
106
認証失敗メッセージを表示
認証成功メッセージを表示
118
エンド

【図５】


18
350
端末管理サーバ
30
ROM
22
印字部
36
RAM
26
クライアントPC
16
CPU
24
12
スキャナ
34
バス
32
HDD
認証管理情報DB
スケジュール情報管理サーバ
14
310
操作パネル部
38
ネットワークI/F
40

【図６】


認証処理ルーチン
100
ユーザID、パスワード入力？
N
Y
照合処理
102
104
照合されたか？
N
Y
110
スケジュール判定を行う設定？
N
Y
スケジュール情報を問合せ
112
114
スケジュール情報を取得？
N
Y
370
リモートアクセスか？
Y
N
所在地を問合せ
372
374
アクセス元の所在地を取得？
N
Y
116
勤務中かつ居場所が目装置の設置場所？
N
Y
376
勤務中かつ居場所がアクセス元の所在地？
N
Y
106
認証失敗メッセージを表示
118
認証成功メッセージを表示
エンド

フロントページの続き

(72)発明者　田邊　滋
神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内

審査官　石田　信行

(56)参考文献　特開２００３－１４０９６８（ＪＰ，Ａ）
特開２００６－２４４４８２（ＪＰ，Ａ）
特表２００２－５１８７２０（ＪＰ，Ａ）
特開２００５－０１８５６６（ＪＰ，Ａ）
特開２００４－１２９２４７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０９Ｃ　１／００