

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2017-102758

(P2017-102758A)

(43) 公開日 平成29年6月8日 (2017. 6. 8)

(51) Int.Cl.		F I		テーマコード (参考)
G 0 6 F	21/40	(2013.01)	G 0 6 F	21/40
G 0 6 F	21/62	(2013.01)	G 0 6 F	21/62
G 0 6 F	1/00	(2006.01)	G 0 6 F	1/00

審査請求 未請求 請求項の数 6 O L (全 17 頁)

(21) 出願番号	特願2015-236152 (P2015-236152)	(71) 出願人	000102717
(22) 出願日	平成27年12月2日 (2015. 12. 2)		N T Tテクノクロス株式会社
			東京都港区港南二丁目16番4号
		(74) 代理人	100107766
			弁理士 伊東 忠重
		(74) 代理人	100070150
			弁理士 伊東 忠彦
		(72) 発明者	除楠 由紀子
			東京都港区港南二丁目16番4号 エヌ・
			ティ・ティ・ソフトウェア株式会社内
		(72) 発明者	田中 久子
			東京都港区港南二丁目16番4号 エヌ・
			ティ・ティ・ソフトウェア株式会社内

(54) 【発明の名称】 認証装置、認証方法及びプログラム

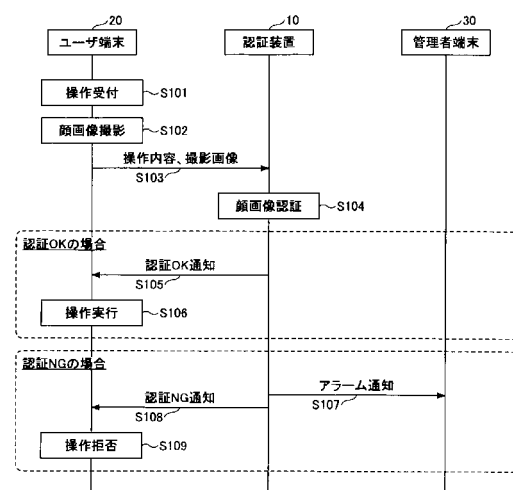
(57) 【要約】

【課題】 情報機器の操作が行われる際のセキュリティを高めることが可能な技術を提供する。

【解決手段】 操作を受け付ける端末と接続される認証装置であって、前記端末が受け付けた操作の内容と前記端末で撮影された撮影画像とを前記端末から受信する受信手段と、前記端末が受け付けた操作に対して認証を行う認証手段と、を有し、前記認証手段は、操作の内容と該操作を行う操作者と該操作を認証する認証者とが対応づけられた認証情報から、前記端末が受け付けた操作を行う操作者と認証者とを取得し、取得した操作者と認証者とが前記撮影画像に写っているか否かの判定を行うことで認証を行う。

【選択図】 図5

実施の形態に係るリアルタイム認証処理の一例を示すシーケンス図



【特許請求の範囲】

【請求項 1】

操作を受け付ける端末と接続される認証装置であって、
前記端末が受け付けた操作の内容と前記端末で撮影された第一の撮影画像とを前記端末から受信する受信手段と、
前記端末が受け付けた操作に対して認証を行う認証手段と、
を有し、
前記認証手段は、操作の内容と該操作を行う操作者と該操作を認証する認証者とが対応づけられた認証情報から、前記端末が受け付けた操作を行う操作者と認証者とを取得し、取得した操作者と認証者とが前記第一の撮影画像に写っているか否かの判定を行うことで認証を行う、認証装置。

10

【請求項 2】

前記端末が受け付けた操作の内容と前記第一の撮影画像に関する情報とをログ情報に記録する記録手段、を有し、
前記認証情報は、操作の内容に含まれる一連の操作のうち認証すべき操作の範囲を示す情報を更に含み、
前記認証手段は、前記ログ情報から前記操作の内容と前記第一の撮影画像に関する情報を取得し、取得した前記操作に内容に含まれる一連の操作のうち前記認証すべき操作の範囲に含まれる操作に対して前記判定を行うことで認証を行う、請求項 1 に記載の認証装置。

20

【請求項 3】

前記認証手段は、操作の内容と該操作を認証する認証者とが対応づけられた認証情報から、前記端末が受け付けた操作を認証する認証者を取得し、取得した認証者が前記第一の撮影画像に写っているか否かの判定を行うことで認証を行う、請求項 1 に記載の認証装置。

【請求項 4】

前記受信手段は、前記端末とは異なる他の端末で撮影された第二の撮影画像を前記他の端末から受信し、
前記認証手段は、操作の内容と該操作を行う操作者と該操作を認証する認証者とが対応づけられた認証情報から、前記端末が受け付けた操作を行う操作者と認証者とを取得し、取得した操作者と認証者とが前記第一の撮影画像又は前記第二の撮影画像に写っているか否かの判定を行うことで認証を行う、請求項 1 に記載の認証装置。

30

【請求項 5】

操作を受け付ける端末と接続される認証装置が行う認証方法であって、
前記端末が受け付けた操作の内容と前記端末で撮影された撮影画像とを前記端末から受信する受信ステップと、
前記端末が受け付けた操作に対して認証を行う認証ステップと、
を有し、
前記認証ステップは、操作の内容と該操作を行う操作者と該操作を認証する認証者とが対応づけられた認証情報から、前記端末が受け付けた操作を行う操作者と認証者とを取得し、取得した操作者と認証者とが前記撮影画像に写っているか否かの判定を行うことで認証を行う、認証方法。

40

【請求項 6】

コンピュータを、請求項 1 乃至 4 のいずれか一項に記載の認証装置の各手段として機能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、認証装置、認証方法及びプログラムに関する。

【背景技術】

50

【0002】

情報機器の操作に関するセキュリティの向上を目的として、操作者が情報機器を操作する際に操作者を撮影した撮影画像を分析し、操作者以外の第三者の立会いのもとで操作が行われていることが確認された場合に限り操作を認めることで、操作者が単独で情報機器を操作することを排除する技術が知られている（例えば、特許文献1参照）。

【先行技術文献】

【特許文献】

【0003】

【特許文献1】特開2015-036918号公報

【発明の概要】

10

【発明が解決しようとする課題】

【0004】

上述の技術は、撮影画像に複数人が写っている場合に情報機器の操作を許可するものであるが、管理者権限での情報機器の操作など、高いセキュリティが要求される操作については、単純に複数人が写っていることのみで操作が許可されてしまうのは好ましくないと考えられる。高いセキュリティが要求される操作については、例えば、適切な立会人のもとで操作が許可されることが望ましい。

【0005】

本発明は上記に鑑みてなされたものであって、情報機器の操作が行われる際のセキュリティを高めることが可能な技術を提供することを目的とする。

20

【課題を解決するための手段】

【0006】

開示の技術の認証装置は、操作を受け付ける端末と接続される認証装置であって、前記端末が受け付けた操作の内容と前記端末で撮影された撮影画像とを前記端末から受信する受信手段と、前記端末が受け付けた操作に対して認証を行う認証手段と、を有し、前記認証手段は、操作の内容と該操作を行う操作者と該操作を認証する認証者とが対応づけられた認証情報から、前記端末が受け付けた操作を行う操作者と認証者とを取得し、取得した操作者と認証者とが前記撮影画像に写っているか否かの判定を行うことで認証を行う。

【発明の効果】

【0007】

30

開示の技術によれば、情報機器の操作が行われる際のセキュリティを高めることができる技術が提供される。

【図面の簡単な説明】

【0008】

【図1】実施の形態に係る認証システムの構成の一例を示す図である。

【図2】実施の形態に係る認証装置、ユーザ端末及び管理者端末の機能構成の一例を示す図である。

【図3】認証情報及びユーザ情報の一例を示す図である。

【図4】ログ情報の一例を示す図である。

【図5】実施の形態に係るリアルタイム認証処理の一例を示すシーケンス図である。

40

【図6】実施の形態に係る事後認証処理の一例を示すシーケンス図である。

【図7】実施の形態に係る認証処理の変形例その1を示すシーケンス図である。

【図8】実施の形態に係る認証処理の変形例その2を示すシーケンス図である。

【発明を実施するための形態】

【0009】

以下、図面を参照して本発明の実施の形態を説明する。なお、以下で説明する実施の形態は一例に過ぎず、本発明が適用される実施の形態は、以下の実施の形態に限られるわけではない。以下、本実施の形態に係る認証システムを企業内における認証管理に用いる場合を例に説明するが、本実施の形態に係る認証システムは、企業内に関わらず一般のユーザ間で認証管理を行う場合にも適用できる。

50

【0010】

<システム構成>

図1は、実施の形態に係る認証システムの構成の一例を示す図である。図1に示すように、実施の形態に係る認証システムは、認証装置10と、ユーザが利用するユーザ端末20₁～_Nと、管理者が利用する管理者端末30と、ユーザ端末20₁～_Nに接続される情報機器40とを有する。以下の説明において、ユーザ端末20₁～_Nのうち任意のユーザ端末は「ユーザ端末20」と表す。

【0011】

認証装置10は、ユーザがユーザ端末20を用いて行う各種操作を認証する機能を有する。認証装置10は、例えば、パーソナルコンピュータ、サーバ又は仮想サーバ等である。なお、ユーザがユーザ端末20を用いて行う各種操作とは、ユーザ端末20上で行われる操作（メール送信など）及びユーザ端末20に接続される情報機器40に対して行われる操作を含む。

10

【0012】

ユーザ端末20はカメラ（内蔵カメラ又は外付けカメラ）を備えており、ユーザから各種操作を受け付けた際に、各種操作の内容とカメラにより撮像した画像とを認証装置10に送信する機能を有している。ユーザ端末20は、例えば、パーソナルコンピュータ、携帯電話、スマートフォン又はタブレット端末等である。ユーザ端末20は、情報機器40をコントロールする専用のコンソール端末であってもよい。

【0013】

20

管理者端末30は、認証装置10から認証に失敗したとの通知を受けた場合に、管理画面等アラームを表示する機能を有する。管理者端末30は、例えば、パーソナルコンピュータ、携帯電話、スマートフォン又はタブレット端末等である。

【0014】

情報機器40は、ユーザ端末20により操作される情報機器であり、例えば、ネットワーク機器（ルータ、スイッチ等）、サーバ（クラウドサーバを含む）等である。また、サーバには、例えば、金融系の顧客管理サーバ等のように高いセキュリティが要求されるサーバが含まれるが、これに限られず、どのような用途のサーバであってもよい。

【0015】

以下の説明において、ユーザ端末20を用いて各種操作を行うユーザを「操作者」と呼び、操作者が行う各種操作を認証するユーザ（例えば、操作者が行う各種操作に立ち会うユーザ）を「認証者」と呼ぶ。

30

【0016】

<機能構成>

図2は、実施の形態に係る認証装置、ユーザ端末及び管理者端末の機能構成の一例を示す図である。

【0017】

（認証装置）

図2（a）に示すように、認証装置10は、通信部101と、ログ記録部102と、認証部103と、アラーム通知部104と、記憶部105とを有する。記憶部105には、各種操作の内容と各種操作を行う操作者と各種操作を認証する認証者とが対応づけられた認証情報と、ユーザ名と各ユーザの顔を特定するための情報等とが対応づけられたユーザ情報が格納される。記憶部105は、認証装置10が備えるメモリ又は認証装置10にネットワークを介して接続される記憶装置等を用いて実現可能である。

40

【0018】

通信部101は、ネットワークを介してユーザ端末20、管理者端末30と通信する機能を有する。また、通信部101は、ユーザ端末20が操作者から受け付けた操作の内容と、ユーザ端末20が備えるカメラで撮影された撮影画像とをユーザ端末20から受信する。

【0019】

50

ログ記録部102は、ユーザ端末20から受信した操作の内容と、認証部103により撮影画像から特定された操作者と認証者とをログ情報に記録する機能を有する。

【0020】

認証部103は、認証情報とユーザ情報とを用いて、操作者により行われる各種操作を認証する機能を有する。より具体的には、認証部103は、認証情報から、ユーザ端末20が受け付けた操作を行うことが許可されている操作者と当該操作を認証する認証者とを取得し、取得した操作者と認証者とが撮影画像に写っているか否かの判定を行うことで認証を行う。認証部103は、認証に失敗した場合、認証に失敗したことをアラーム通知部104に通知する。

【0021】

また、認証部103は、ログ情報から操作の内容と操作者と認証者とを取得し、取得した当該操作の内容に含まれる一連の操作のうち認証すべき操作の範囲に含まれる操作に対して認証を行うようにしてもよい。この場合、認証情報には、各種操作の内容に含まれる一連の操作のうち認証すべき操作の範囲を示す情報が含まれるようにしてもよい。

【0022】

アラーム通知部104は、認証部103から認証に失敗したとの通知を受けた場合、アラーム信号を管理者端末30に送信することで、認証に失敗したことを管理者に通知する。

【0023】

図3は、認証情報及びユーザ情報の一例を示す図である。図3を用いて、認証情報及びユーザ情報の具体例を説明する。

【0024】

図3(a)は認証情報の一例である。「操作内容」には、ユーザ端末20を用いて行われる様々な操作のうち、認証の対象である操作の内容を示す情報が格納される。なお、認証の対象である操作には、1つの操作手順で完結する操作と複数(一連)の操作手順からなる操作とが含まれる。

【0025】

「操作A」は、メール送信ボタンを押下する操作を示す情報である。「操作B」は、添付ファイルをメールに添付してメール送信ボタンを押下するまでの一連の操作を示す情報である。「操作C」は、ルータ又はサーバ等のパスワードを変更するコマンドを入力する操作を示す情報である。「操作D」及び「操作E」は、ルータ又はサーバ等にパッチ(バグ修正用プログラム)をインストールする際の一連のコマンドを入力する操作を示す情報である。「操作F」は、経費を管理するデータベースを参照、更新する操作を示す情報である。

【0026】

「操作者」には、「操作内容」の操作を行うことが許可されているユーザを示す情報が格納される。図3(a)の例では「操作者」にはユーザの役職が格納されているが、具体的なユーザ名が格納されてもよい。「認証者」には、操作者が行う操作を監視することで操作者が不正な操作を行っていないかの認証(確認)を行う認証者、及び必要な認証者の人数を示す情報が格納される。例えば、「上司(1名)」とは、操作A又はBにおける認証者は、操作者の上司であるユーザ1名であることを意味している。また、例えば「経費管理(1名)、DB管理(1名)」とは、操作Fにおける認証者は、経費管理の権限を有するユーザ1名及びDB(データベース)管理の権限を有するユーザ1名であることを意味している。なお、「認証者」には具体的なユーザ名が格納されてもよい。「認証人数」には、「操作者」と「認証者」とを合計した人数が格納される。

【0027】

「認証範囲」には、「操作内容」に係る操作のうち、どの範囲の操作に対して認証者が監視していたことが確認された場合に、認証が成功したと判定すべきかを示す情報が格納される。「全体」とは、操作の開始から終了までの操作全体を認証者が監視していたことが確認された場合に認証が成功したと判定されることを示している。「一部(時間比率X

10

20

30

40

50

）」とは、操作の開始から終了までの一連の操作に要した時間のうち、所定の割合の時間（例えば $X = 70\%$ であれば、全ての操作時間のうち 70% の時間）において認証者が監視していたことが確認された場合に認証が成功したと判定されることを示している。「一部（特定操作）」とは、操作の開始から終了までの一連の操作のうち特定の操作が行われる際（例えば、ログインからパスワード変更までに投入される全てのコマンドのうち、パスワード変更コマンドが投入される際）に認証者が監視していたことが確認された場合に認証が成功したと判定されることを示している。なお、操作の開始から終了までの一連の操作のうち、所定の割合の操作（例えば、全体で5つの操作のうち2つの操作）が行われる際に認証者が監視していたことが確認された場合に認証が成功したと判定されるようにしてもよい。また、操作の開始と操作の終了については、それぞれ特定のキー操作又は特定の操作コマンド等により定義されるようにしてもよい。例えば、所定のコマンドAは操作の開始を意味し、所定のコマンドBは操作の終了を意味するということに予め定義されていてもよい。

【0028】

図3（b）は、ユーザ情報の一例である。「権限」には、そのユーザが有する管理権限が格納される。例えば、図3（b）の例では、ユーザAは経費管理に関する操作を管理（認証）する権限を有していることを意味しており、図3（a）の操作Fが行われる際の認証者に該当する。「上司」には、そのユーザの上司であるユーザ名が格納される。「顔情報」は、認証装置10の認証部103が、撮影画像に写っているユーザを特定する際に用いられる情報であり、例えばユーザの顔を撮影した画像データであってもよいし、顔の特徴を示すデータであってもよい。

【0029】

「位置情報」には、ユーザ端末20が備えるGPS又はその他ユーザの現在位置を特定することができる何れかの方法により取得されたユーザの現在位置が格納される。位置情報が取得されるタイミングは、定期的なタイミングであってもよいし、特定のタイミング（例えばユーザにより操作が開始されるタイミング）であってもよい。

【0030】

図4は、ログ情報の一例を示す図である。ログ情報には、時間ごとの操作内容と、当該時間帯における操作者及び認証者のユーザ名が格納される。なお、当該時間帯における操作者及び認証者のユーザ名には、ユーザ端末20から送信された撮影画像に写っていたユーザのユーザ名が格納される。図4の例では、10:14～10:20までの間に行われた操作Dのうち、10:16～10:17までの時間は認証者が不在であり、ユーザEが単独で操作していたことを示している。

【0031】

（ユーザ端末）

図2（b）に示すように、ユーザ端末20は、通信部201と、撮影部202と、UI（User Interface）制御部203とを有する。UI制御部203は、更に、操作受付部213と、操作記録部214と、認証要求部215と、操作実行部216とを有する。

【0032】

通信部201は、ネットワークを介して認証装置10と通信する機能を有する。

【0033】

撮影部202は、ユーザ端末20が備えるカメラ（内蔵カメラ又は外付けカメラ）を用いて撮影した撮影画像を、通信部201を介して認証装置10に送信する機能を有する。また、撮影部202は、操作者が操作を行う度に撮影画像を認証装置10に送信するようにしてもよいし、継続して動画像（又は周期的に撮影された撮影画像）を認証装置10に送信するようにしてもよい。

【0034】

UI制御部203は、入力デバイス（キーボード、マウス、タッチパネル等）を介してユーザ（操作者）から受け付けた操作に関する各種制御を行う機能、各種画面を表示する機能を有する。具体的には後述するが、本実施の形態に係る認証システムは、ユーザによ

り何らかの操作が行われる度に認証を行う「リアルタイム認証処理」と、ログ情報を用いて事後的に認証を行う「事後認証処理」とを実行することができる。UI制御部203は、リアルタイム認証手順が適用される場合、入力デバイスから入力された操作をすぐに実行するのではなく、認証装置10により認証が許可されてから当該操作を実行する。また、事後認証手順が適用される場合、UI制御部203は、入力デバイスから入力された操作をすぐに実行する。UI制御部203は、ユーザ端末20のディスプレイ等に表示されている操作画面を他のユーザ端末20との間で共有する機能を有していてもよい。

【0035】

操作受付部213は、入力デバイスを介してユーザから操作を受け付ける。また、操作受付部213は、リアルタイム認証処理が適用される場合、受け付けた操作を操作記録部214に通知する。操作記録部214は、操作受付部213から通知された操作を一時的に記憶する。

10

【0036】

認証要求部215は、操作受付部213に記憶された操作の内容を、通信部201を介して認証装置10に送信する。また、認証要求部215は、認証装置10から受信した認証結果を操作実行部216に通知する。操作実行部216は、認証要求部215から認証成功との通知を受けた場合、操作記録部214に一時的に記憶されている操作を実行する。一方、認証失敗との通知を受けた場合、操作実行部216は、操作記録部214に一時的に記憶されている操作を実行しない。

20

【0037】

また、操作受付部213は、事後認証処理が適用される場合、受け付けた操作を操作実行部216に直接通知する。操作実行部216は、直接通知された操作を実行する。

【0038】

(管理者端末)

図2(c)に示すように、管理者端末30は、アラーム受信部301と、表示部302とを有する。

【0039】

アラーム受信部301は、認証装置10から認証に失敗したとの通知を受けた場合、認証の失敗が発生したことを示すアラームを表示させるように表示部302に指示する。表示部302は、当該アラームを画面等に表示する。

30

【0040】

<システム動作例>

本実施の形態に係る認証システムは、操作が行われる度に認証を行う「リアルタイム認証処理」と、ログ情報を用いて事後的に認証を行う「事後認証処理」とを実行することができる。本認証システムにおいてリアルタイム認証処理が適用されるのか又は事後認証処理が適用されるのかは、認証装置10及びユーザ端末20にフラグを保持させておき、当該フラグに従っていずれか一方の認証処理に固定的に切替えられるようにしてもよい。また、認証の対象である操作毎にどちらの認証処理が適用されるのかを示す情報を認証装置10及びユーザ端末20に保持させておき、操作毎に認証処理が切替えられるようにしてもよい。例えば、図3(a)に示す操作A及び操作Bのように、短時間で操作が完了するような操作についてはリアルタイム認証処理が適用されるようにして、操作C～Fのように、ある程度の時間を要するような操作については事後認証処理が適用されるようにしてもよい。また、重要度の高い操作をリアルタイム認証にすることでもよい。

40

【0041】

(リアルタイム認証処理)

図5は、実施の形態に係るリアルタイム認証処理の一例を示すシーケンス図である。

【0042】

ステップS101で、ユーザ端末20の操作受付部213は、ユーザ(操作者)からの操作を受け付ける。受け付けた操作の内容は、操作記録部214に記憶される。

【0043】

50

ステップS102で、ユーザ端末20の撮影部202は、ユーザ端末20自身が備えるカメラを用いて画像の撮影を行う。

【0044】

ステップS103で、ユーザ端末20の認証要求部215及び撮影部202は、操作記録部214に記憶されている操作の内容を示す情報と、撮影画像とを認証装置10に送信する。

【0045】

ステップS104で、認証装置10の認証部103は、ステップS103の処理手順で受信した撮影画像を分析し、撮影画像に写っている複数のユーザの顔を抽出する。また、ユーザ情報の「顔情報」と抽出された複数のユーザの顔とを比較し、撮影画像に写っている複数のユーザを特定する。続いて、認証部103は、ステップS103の処理手順で受信した操作の内容に対応する「操作者」及び「認証者」を認証情報から抽出し、撮影画像に写っている複数のユーザが「操作者」及び「認証者」に該当するか否かを確認する。認証部103は、撮影画像に写っている複数のユーザが「操作者」及び「認証者」に該当する場合は認証成功と判定し、撮影画像に写っている複数のユーザが「操作者」及び「認証者」に該当しない場合は認証失敗と判定する。

【0046】

図3を用いて具体例を説明する。例えば、ユーザDが、ユーザB立会いの下でメール送信（操作A）を行う場合を想定する。ユーザDは、自身のユーザ端末20を用いてメール送信ボタンを押下する。ユーザ端末20は、ユーザD及びユーザBが写っている撮影画像と操作の内容を示す情報（メール送信ボタン押下）とを認証装置10に送信する（S103）。

【0047】

認証部103は、撮影画像を分析し、ユーザD及びユーザBが撮影画像に写っていることを特定する。続いて、認証部103は、ユーザ端末20から受信した操作の内容を示す情報（メール送信ボタン押下）をキーに認証情報を検索し、メール送信を行うことが許可されているのは役職が「担当」であるユーザであること、及びメール送信の認証者は操作者の上司であることを認識する。続いて、認証部103は、ユーザ情報を検索し、撮影画像に写っているユーザDの役職は「担当」であり、ユーザBはユーザDの上司であることを認識する。以上の処理により、撮影画像に写っている複数のユーザ（ユーザD及びユーザB）はメール送信時の「操作者」及び「認証者」に該当することが確認されるため、認証部103は認証成功と判定する。

【0048】

なお、認証部103は、ユーザ情報に格納されている操作者の位置情報と認証者の位置情報とを比較し、操作者の位置と認証者の位置とが所定の距離以上に離れている場合は、認証者が操作者の傍にいないことを特定して認証失敗と判定するようにしてもよい。また、認証部103は、撮影画像（動画像）から、認証者のまばたき又は表情の変化などを検出し、まばたき又は表情の変化などが検出されない場合は認証失敗と判定するようにしてもよい。これにより、操作者が、ユーザ端末20のカメラの前に認証者の顔写真をかざしながら操作を行うような不正行為を排除することができ、セキュリティを更に高めることが可能になる。また、認証部103は、撮影画像に写っているユーザを特定できない場合は、ユーザの特定が困難であることをユーザ端末20に通知するようにしてもよい。これにより、ユーザはカメラの位置を自身に近づけるなどの対応を行うことが可能になる。

【0049】

ステップS105で、認証装置10の認証部103は、認証成功をユーザ端末20に通知する。ステップS106で、ユーザ端末20の認証要求部215は、認証成功を操作実行部216に通知し、操作実行部216は、操作記録部214に記憶されている操作を実行する。

【0050】

ステップS107で、認証装置10のアラーム通知部104は、認証失敗が発生したこ

10

20

30

40

50

とを管理者に通知するため、アラーム通知信号を管理者端末 30 に送信する。管理者端末 30 の表示部 302 は、認証装置 10 から送信されたアラームを表示する。

【0051】

ステップ S108 で、認証装置 10 の認証部 103 は、認証失敗をユーザ端末 20 に通知する。ステップ S109 で、ユーザ端末 20 の認証要求部 215 は、認証失敗を操作実行部 216 に通知し、操作実行部 216 は、操作記録部 214 に記憶されている操作を実行せずに動作を終了する。なお、認証失敗の場合、ユーザ端末 20 の UI 制御部 203 は、認証に失敗したことをユーザ端末 20 の画面に表示するようにしてもよい。

【0052】

なお、図 3 (a) の操作 D などのように一連の操作手順を伴う場合、操作手順毎にステップ S101 乃至ステップ S109 の処理手順が繰り返されるようにしてもよい。例えば操作 D の場合、パッチのインストールに係る一連のコマンド入力操作において、コマンド入力が行われる度にステップ S101 乃至ステップ S109 の処理手順が繰り返されるようにしてもよい。この場合、図 3 (b) の「認証範囲」の設定に関わらず一連の操作全体に対して認証が行われることになる。

【0053】

また、図 3 (a) の操作 D などのように一連の操作手順を伴う場合、一連の操作手順全体に対してステップ S101 乃至ステップ S109 の処理手順がまとめて行われるようにしてもよい。この場合、ステップ S103 の処理手順において、ユーザ端末 20 の認証要求部 215 及び撮影部 202 は、一連の操作手順に係る操作の内容を示す情報と一連の操作手順の各々に対応する撮影画像とを認証装置 10 に送信する。また、ステップ S104 の処理手順において、認証部 103 は、一連の操作手順について、認証情報の「認証範囲」の設定値に従って認証を行うようにする。

【0054】

以上、リアルタイム認証処理について説明した。リアルタイム認証処理が行われることで、認証者の立会いの下でのみ、ユーザ端末 20 を用いて行われる各種操作を許可することが可能になり、セキュリティを高めることが可能になる。

【0055】

(事後認証処理)

図 6 は、実施の形態に係る事後認証処理の一例を示すシーケンス図である。

【0056】

ステップ S201 で、ユーザ端末 20 の操作受付部 213 は、ユーザ（操作者）からの操作を受け付ける。なお、受け付けた操作は、操作記録部 214 に記憶される。

【0057】

ステップ S202 で、ユーザ端末 20 の撮影部 202 は、ユーザ端末 20 自身が備えるカメラを用いて画像の撮影を行う。

【0058】

ステップ S203 で、ユーザ端末 20 の認証要求部 215 及び撮影部 202 は、操作記録部 214 に記憶されている操作の内容を示す情報と、撮影画像とを認証装置 10 に送信する。

【0059】

ステップ S204 で、ユーザ端末 20 の操作実行部 216 は、操作記録部 214 に記憶されている操作を実行する。

【0060】

ステップ S205 で、認証装置 10 の認証部 103 は、ステップ S203 の処理手順で受信した撮影画像を分析し、撮影画像に写っているユーザの顔を抽出する。また、ユーザ情報の「顔情報」と抽出されたユーザの顔とを比較し、撮影画像に写っているユーザのユーザ名を特定する。続いて、認証部 103 は、ステップ S203 の処理手順で受信した操作の内容に対応する「操作者」及び「認証者」を認証情報から抽出し、撮影画像に写っているユーザが「操作者」及び「認証者」のどちらに該当するかを特定する。なお、認証部

10

20

30

40

50

103は、ユーザ端末20のログインアカウントをユーザ端末20から取得し、撮影画像に写っているユーザのうち、取得したログインアカウントに該当するユーザを「操作者」として特定し、他方を「認証者」として特定するようにしてもよい。

【0061】

認証装置10のログ記録部102は、認証部103により特定された「操作者」のユーザ名及び「認証者」のユーザ名と、ステップS203の処理手順で受信した操作の内容とをログ情報に記録する。また、ステップS203の処理手順で受信した撮影画像から認証部103が「操作者」又は／及び「認証者」を特定できない場合（例えば、撮影画像に1人しか写っていないような場合で、かつ、そのユーザが認証情報の「操作者」及び「認証者」のどちらにも該当しないような場合）、ログ記録部102は、「操作者」又は／及び「認証者」を特定できないことをログ情報に記録するようにしてもよい。

10

【0062】

ステップS206で、ユーザ端末20の操作受付部213は、操作の終了を検出する。操作受付部213は、ユーザからの明示的な指示（例えば、ログオフなど）により操作の終了を検出するようにしてもよい。ステップS207で、ユーザ端末20の操作受付部213は、操作が終了したことを認証装置10に通知する。

【0063】

ステップS208で、認証装置10の認証部103は、ログ情報の各レコードに含まれる「操作内容」、「操作者」及び「認証者」と、認証情報とを比較することで認証を行う。

20

【0064】

ここで、認証部103は、認証情報の「認証範囲」の設定値に従って認証を行うようにする。図4を用いて具体例を説明する。例えば、10:14~10:20には操作Dが行われ、操作者はユーザAであることが記録されている。また、10:14~10:16及び10:17~10:20の認証者はユーザCであるものの、10:16~10:17の認証者は不在であることが記録されている。また、認証情報によれば、操作Dの認証範囲は「一部（時間比率X）」である。この場合、認証部103は、10:14~10:20のうち、時間比率Xの時間で正しい認証者が記録されている場合に認証成功であると判定する。例えばX=50%に設定されている場合、認証部103は、操作Dについては認証成功であると判定することになる。また、例えばX=10%に設定されている場合、認証部103は、操作Dについては認証失敗であると判定することになる。

30

【0065】

ステップS209は、図5のステップS107の処理手順と同一であるため説明は省略する。

【0066】

なお、図3(a)の操作Dなどのように一連の操作手順を伴う場合、操作手順毎にステップS201乃至ステップS205の処理手順が繰り返し行われるようにしてもよいし、一連の操作手順全体に対してステップS201乃至ステップS205の処理手順がまとめて行われるようにしてもよい。後者の場合、ステップS203の処理手順において、ユーザ端末20の認証要求部215及び撮影部202は、一連の操作手順に係る操作の内容を示す情報と一連の操作手順の各々に対応する撮影画像とを認証装置10に送信する。

40

【0067】

以上、事後認証処理について説明した。事後認証処理が適用されることで、リアルタイム認証処理よりもユーザ端末20における操作レスポンスを向上させることができる。

【0068】

（認証処理の変形例その1）

図5及び図6で説明したリアルタイム認証処理及び事後認証処理では、操作者は、認証者の立会いの下で操作を行っている前提で説明したが、認証者が操作者の傍に立ち会うことが出来ない場合も想定される。そこで、以下の処理手順では、操作者が用いるユーザ端末20と認証者が用いるユーザ端末20との間で操作画面を共有し、認証者は共有された

50

操作画面を参照することで操作者が行う操作を監視することを可能にする。また、認証装置 10 は、操作者のユーザ端末 20₁ 及び認証者のユーザ端末 20₂ の各々から受信した撮影画像を用いて認証を行うようにする。

【0069】

図 7 は、実施の形態に係る認証処理の変形例その 1 を示すシーケンス図である。本処理手順をリアルタイム認証処理に適用する場合、図 5 のステップ S 101 乃至ステップ S 103 の処理手順を、図 7 の処理手順に置き換えればよい。また、本処理手順を事後認証処理に適用する場合、図 6 のステップ S 201 乃至 S 203 の処理手順を、図 7 の処理手順に置き換えればよい。

【0070】

ステップ S 301 で、操作者のユーザ端末 20₁ の UI 制御部 203 と認証者のユーザ端末 20₂ の UI 制御部 203 との間で、操作者のユーザ端末 20₁ の画面に表示されている操作画面が共有される。具体的には、操作者のユーザ端末 20 の画面に表示されている操作画面と同一の操作画面が、認証者のユーザ端末 20₂ の画面に表示される。なお、ユーザ端末 20₁ の UI 制御部 203 は、どのユーザ端末 20 との間で操作画面を共有すべきかを、操作者の明示的な指示により判断してもよいし、操作の内容と操作者のユーザ名（例えば、ユーザ端末 20 のログインアカウントを用いて特定）とを認証装置 10 に通知し、認証装置 10 から指示されたユーザ端末 20 に呼出し信号を送信するようにしてもよい。この場合、認証装置 10 に格納されているユーザ情報に、予めユーザごとのユーザ端末 20 の IP アドレス等を格納するようにしておく。

【0071】

ステップ S 302 の処理手順は、図 5 のステップ S 101、又は図 6 のステップ S 201 と同一であるため説明は省略する。

【0072】

ステップ S 303 で、ユーザ端末 20₁ の UI 制御部 203 は、ユーザ端末 20₂ に対して撮影指示信号を送信する。

【0073】

ステップ S 304 で、ユーザ端末 20₁ の撮影部 202 は、ユーザ端末 20₁ 自身が備えるカメラを用いて画像の撮影を行う。ステップ S 305 で、ユーザ端末 20₂ の撮影部 202 は、ユーザ端末 20₂ 自身が備えるカメラを用いて画像の撮影を行う。

【0074】

ステップ S 306 で、ユーザ端末 20₁ の認証要求部 215 及び撮影部 202 は、操作記録部 214 に記憶されている操作の内容と、撮影画像とを認証装置 10 に送信する。ステップ S 307 で、ユーザ端末 20₂ の撮影部 202 は、撮影画像を認証装置 10 に送信する。

【0075】

以上、認証処理の変形例その 1 によれば、認証者が操作者の傍に立ち会うことが出来ない場合であっても認証処理を行うことが可能になり、ユーザの利便性を高めることが可能になる。

【0076】

（認証処理の変形例その 2）

認証処理の変形例その 2 は、認証処理の変形例その 1 と異なり、予め認証者のユーザ端末 20 との間で操作画面を共有するのではなく、操作の都度、操作者から認証者のユーザ端末 20 を呼出すようにする。特に言及しない点は認証処理の変形例その 1 と同一でよい。

【0077】

図 8 は、実施の形態に係る認証処理の変形例その 2 を示すシーケンス図である。本処理手順をリアルタイム認証処理に適用する場合、図 5 のステップ S 101 乃至ステップ S 103 の処理手順を、図 8 の処理手順に置き換えればよい。また、本処理手順を事後認証処理に適用する場合、図 6 のステップ S 201 乃至 S 203 の処理手順を、図 8 の処理手順

に置き換えればよい。

【0078】

ステップS401の処理手順は、図5のステップS101、又は図6のステップS201と同一であるため説明は省略する。

【0079】

ステップS402で、ユーザ端末20₁のUI制御部203は、ユーザ端末20₂に対して呼出し信号を送信する。なお、UI制御部203は、どのユーザ端末20に呼出し信号を送信すべきかを、操作者の明示的な指示により判断してもよいし、操作の内容と操作者のユーザ名とを認証装置10に通知し、認証装置10から指示されたユーザ端末20に呼出し信号を送信するようにしてもよい。また、呼出し信号には、ステップS401で受け付けた操作の内容が含まれていてもよい。認証者は、操作者がどのような操作を行おうとしているのかを事前に把握することができる。

10

【0080】

ステップS403乃至S406の処理手順は、それぞれ図7のステップS304乃至ステップS307の処理手順と同一であるため説明は省略する。

【0081】

なお、以上の処理手順において、ユーザ端末20₁のUI制御部203は、連続して操作が行われる際、呼出し信号を送信するユーザ端末20を認証者が変わる度に切替えるようにしてもよい。例えば、ユーザEが操作Aを行う際、ユーザ端末20₁のUI制御部203はユーザCのユーザ端末20₂に呼出し信号を送信し、続けてユーザEが操作Cを行う際、ユーザ端末20₁のUI制御部203はユーザBのユーザ端末20₂に呼出し信号を送信するようにしてもよい。これにより、認証装置10には適切な認証者の撮影画像が届くことになる。

20

【0082】

以上、認証処理の変形例その2によれば、認証者が操作者の傍に立ち会うことが出来ない場合であっても認証処理を行うことが可能になり、ユーザの利便性を高めることが可能になる。

【0083】

(認証処理の変形例その3)

以上説明した実施の形態では、認証部103は、認証情報からユーザ端末20が受け付けた操作を行うことが許可されている操作者と当該操作を認証する認証者とを取得し、取得した操作者と認証者とは撮影画像に写っているか否かの判定を行うことで認証を行うようにした。一方、認証処理の変形例その3では、操作者を限定せずに認証を行うようにする。なお、本変形例では、認証情報に「操作者」を格納しないようにしてもよい。また、本変形例は、上述の変形例その1又は変形例その2と組み合わせるようにしてもよい。

30

【0084】

具体的には、図5のステップS104において、認証装置10の認証部103は、撮影画像に「操作者」が写っていることを確認せずに「認証者」が写っていることのみを確認することで認証を行うようにしてもよい。

【0085】

同様に、図6のステップS208において、認証装置10の認証部103は、ログ情報の各レコードに含まれる「操作者」と認証情報とを比較せずに、ログ情報の各レコードに含まれる「操作内容」及び「認証者」と、認証情報とを比較することで認証を行うようにしてもよい。ログ記録部102は、ログ情報に「操作者」を記録しないようにしてもよい。

40

【0086】

また、他の具体例として、図5のステップS104において、認証装置10の認証部103は、撮影画像に最低2人以上のユーザが写っていることを確認すると共に、撮影画像に写っているユーザのうち少なくとも1人が「認証者」であることを確認することで認証を行うようにしてもよい。

50

【0087】

同様に、図6のステップS205の処理手順において、認証装置10の認証部103は、撮影画像に最低2人以上のユーザが写っていることを確認すると共に、撮影画像に写っているユーザのうち少なくとも1人が「認証者」に該当するかを特定し、ログ記録部102は、撮影画像に最低2人以上のユーザが写っているか否かを示すフラグ、及び、特定された「認証者」をログ情報に記録するようにしてもよい。また、認証部103は、図6のステップS208において、ログ情報の各レコードに含まれる「操作内容」及び「認証者」と、認証情報とを比較すると共に、ログ情報の各レコードに撮影画像に最低2人以上のユーザが写っていることを示すフラグが付与されていることを確認することで認証を行うようにしてもよい。

10

【0088】

また、他の具体例として、認証情報において「操作者」と「認証者」に同一のユーザが設定されることを許容し、図5のステップS104において、認証装置10の認証部103は、撮影画像に「操作者」及び「認証者」の両方に該当するユーザが写っていることを確認することで認証を行うようにしてもよい。

【0089】

同様に、図6のステップS205の処理手順において、認証装置10の認証部103は、撮影画像に写っているユーザが「操作者」及び「認証者」の両方に該当する場合を許容し、ログ記録部102は、特定された「操作者」及び「認証者」として同一のユーザ名をログ情報に記録するようにしてもよい。また、認証部103は、図6のステップS208において、ログ情報の各レコードに含まれる「操作内容」、「操作者」及び「認証者」と、認証情報とを比較することで認証を行うようにしてもよい。

20

【0090】

（認証処理の変形例その4）

以上説明した事後認証処理では、認証装置10は、ログ情報に操作者と認証者とを記録するようにしたが、認証処理の変形例その4では、認証装置10は、操作者と認証者に代えて（又は加えて）撮影画像をログ情報に記録しておき、ログ情報に記録された撮影画像から操作者及び認証者を特定して認証を行うようにしてもよい。なお、本変形例は、上述の変形例その1又は変形例その2と組み合わせるようにしてもよい。

【0091】

具体的には、図6のステップS205の処理手順で、認証装置10のログ記録部102は、ステップS203の処理手順で受信した操作の内容と撮影画像とをログ情報に記録する。つまり、ログ情報には、図4に示す「操作者」及び「認証者」のカラムに代えて（又は加えて）「撮影画像」が格納される。

30

【0092】

続いて、ステップS208の処理手順で、認証装置10の認証部103は、ログ情報の各レコードに記録された撮影画像を分析し、撮影画像に写っているユーザの顔を抽出する。また、ユーザ情報の「顔情報」と抽出されたユーザの顔とを比較し、撮影画像に写っているユーザのユーザ名を特定する。続いて、認証部103は、当該レコードに記録された「操作内容」に対応する「操作者」及び「認証者」を認証情報から抽出し、撮影画像に写っているユーザが「操作者」及び「認証者」のどちらに該当するかを特定する。なお、認証部103は、ユーザ端末20のログインアカウントをユーザ端末20から取得し、撮影画像に写っているユーザのうち、取得したログインアカウントに該当するユーザを「操作者」として特定し、他方を「認証者」として特定するようにしてもよい。

40

【0093】

続いて、認証装置10の認証部103は、ログ情報の各レコードに含まれる「操作内容」と、当該レコードの撮影画像より特定された「操作者」及び「認証者」と、認証情報とに基づいて、認証情報の「認証範囲」の設定値に従って認証を行う。

【0094】

なお、本変形例は、上述の認証処理の変形例その3と組み合わせるようにしてもよい。

50

【0095】

具体的には、図6のステップS208の処理手順で、認証装置10の認証部103は、ログ情報の各レコードに記録された撮影画像に最低2人以上のユーザが写っていることを確認すると共に、当該レコードの「操作内容」と認証情報とを参照し、撮影画像に写っているユーザのうち少なくとも1人が、「操作内容」に対応する「認証者」に該当するかを確認することで認証を行うようにしてもよい。なお、認証情報には「操作者」が格納されていなくてもよい。

【0096】

また、他の具体例として、認証部103は、認証情報において「操作者」と「認証者」に同一のユーザが設定されることを許容してもよい。この場合、図6のステップS208の処理手順で、認証部103は、ログ情報の各レコードに含まれる「操作内容」と認証情報とを比較し、当該レコードの撮影画像に写っているユーザが「操作者」及び「認証者」の両方に該当するかを確認すると共に、「認証範囲」の設定値を満たすか否かを確認することで認証を行うようにしてもよい。

【0097】

<実施形態の補足>

本発明は、上記の実施の形態に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。実施の形態で述べたシーケンスは、矛盾の無い限り順序を入れ替えてもよい。

【0098】

実施の形態において、認証装置10はクラウドサーバであってもよい。すなわち、図2(a)に示す各機能部は、クラウドサーバ上に実装されるようにしてもよい。

【0099】

実施の形態において、認証装置10とユーザ端末20は一体であってもよい。すなわち、認証装置10が有する各機能部がユーザ端末20に含まれていてもよい。また、管理者端末30は、ユーザ端末20と一体であってもよい。すなわち、管理者端末30が有する各機能部がユーザ端末20に含まれていてもよい。

【0100】

実施の形態に係る認証装置10、ユーザ端末20及び管理者端末30が有する各機能部は、これらが備えるCPU及びメモリなどのハードウェア資源を用いて、認証装置10、ユーザ端末20及び管理者端末30の各々で実施される処理に対応するプログラムを実行することによって実現することが可能である。また、当該プログラムは、記憶媒体に格納することができる。また、実施の形態に係る認証装置10、ユーザ端末20及び管理者端末30の各々は複数のコンピュータ等の組み合わせにより実現されてもよい。

【0101】

実施の形態において、ユーザ端末20は端末の一例である。通信部101は受信手段の一例である。認証部103は認証手段の一例である。ログ記録部102は記録手段の一例である。認証情報に含まれる認証範囲は、「操作の内容に含まれる一連の操作のうち認証すべき操作の範囲を示す情報」の一例である。「撮影画像に写っている操作者及び認証者」又は／及び「撮影画像」は、撮影画像に関する情報の一例である。

【符号の説明】

【0102】

- 10 認証装置
- 20 ユーザ端末
- 30 管理者端末
- 40 情報機器
- 101 通信部
- 102 ログ記録部
- 103 認証部
- 104 アラーム通知部

10

20

30

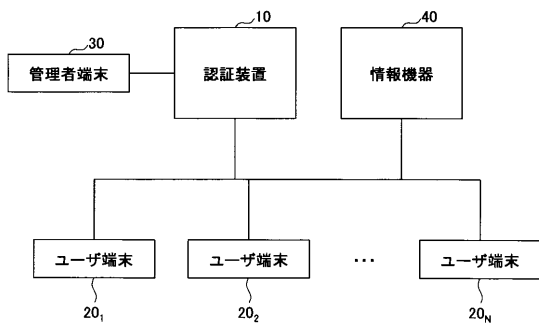
40

50

- 1 0 5 記憶部
- 2 0 1 通信部
- 2 0 2 撮影部
- 2 0 3 U I 制御部
- 2 1 3 操作受付部
- 2 1 4 操作記録部
- 2 1 5 認証要求部
- 2 1 6 操作実行部
- 3 0 1 アラーム受信部
- 3 0 2 表示部

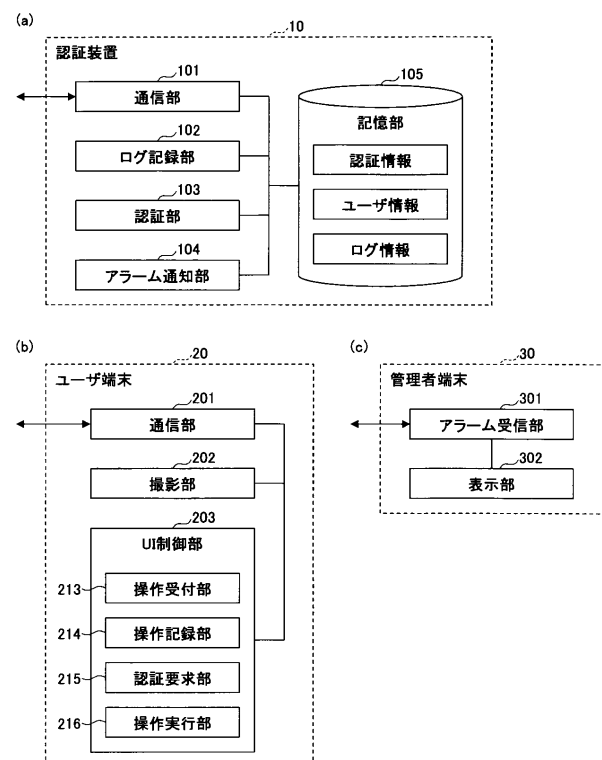
【図 1】

実施の形態に係る認証システムの構成の一例を示す図



【図 2】

実施の形態に係る
認証装置、ユーザ端末及び管理者端末の機能構成の一例を示す図



【図 3】

認証情報及びユーザ情報の一例を示す図

認証情報					
操作内容	操作者	認証者	認証人数	認証範囲	
操作A(メール送信)	担当	上司(1名)	2	全体	
操作B(メール送信(添付有))	担当・課長	上司(1名)	2	全体	
操作C(NW/スワート変更)	担当・課長	NW管理(1名)	2	全体	
操作D(NW/タッチ1)	担当・課長	NW管理(1名)	2	一部(時間比率X)	
操作E(NW/タッチ2)	担当・課長	NW管理(1名)	2	一部(特定操作)	
操作F(経費DB更新)	課長	経費管理(1名)、DB管理(1名)	3	全体	

(a)

ユーザ情報				
ユーザ名	役職	権限	顔情報	位置情報
A	部長	経費管理	-	A.jpg
B	課長	NW管理	A	B.jpg
C	課長	-	A	C.jpg
D	担当	DB管理	B	D.jpg
E	担当	-	C	E.jpg

(b)

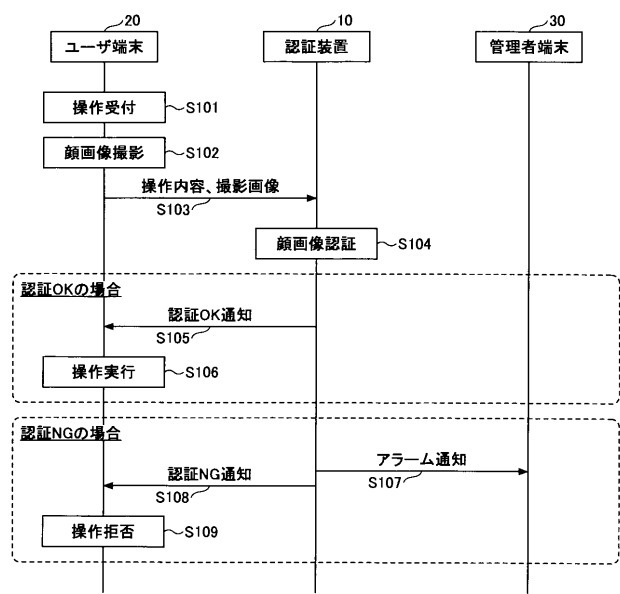
【図 4】

ログ情報の一例を示す図

ログ情報				
時間	操作内容	操作者	認証者	認証者
10:00～10:05	操作なし	E		
10:05～10:08	操作A	E	C	
10:08～10:14	操作なし	E		
10:14～10:16	操作D	E	B	
10:16～10:17	操作D	E		
10:17～10:20	操作D	E	B	
10:20～10:21	操作なし	C		
10:21～10:28	操作F	C	D	A

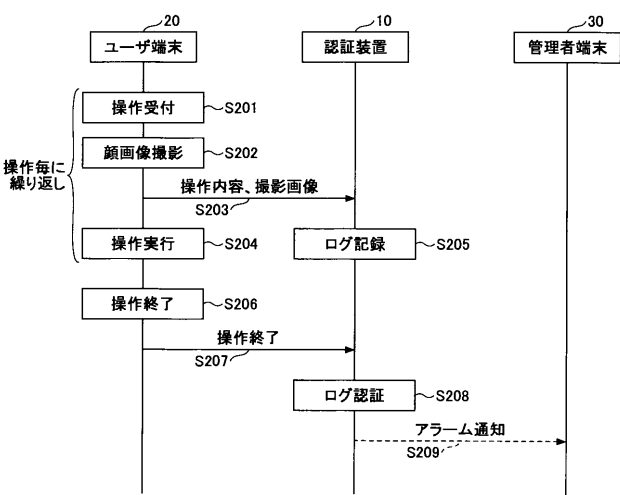
【図 5】

実施の形態に係るリアルタイム認証処理の一例を示すシーケンス図



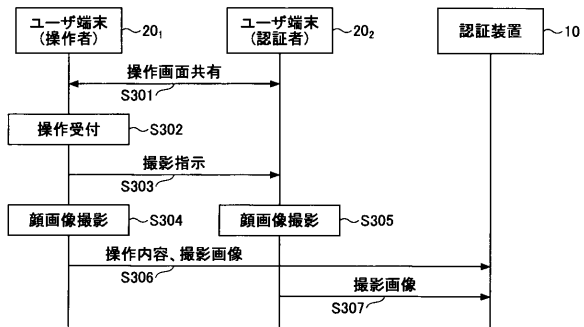
【図 6】

実施の形態に係る事後認証処理の一例を示すシーケンス図



【図 7】

実施の形態に係る認証処理の変形例その1を示すシーケンス図



【図 8】

実施の形態に係る認証処理の変形例その2を示すシーケンス図

