

(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2021-89575

(P2021-89575A)

(43) 公開日 令和3年6月10日(2021.6.10)

(51) Int. Cl.	F I	テーマコード (参考)
G06F 21/40 (2013.01)	G06F 21/40	3C707
B25J 9/22 (2006.01)	B25J 9/22	Z
B25J 19/06 (2006.01)	B25J 19/06	
G06F 21/32 (2013.01)	G06F 21/32	

審査請求 未請求 請求項の数 3 O L (全 5 頁)

(21) 出願番号	特願2019-219568 (P2019-219568)	(71) 出願人	501428545 株式会社デンソーウェーブ
(22) 出願日	令和1年12月4日 (2019.12.4)	(74) 代理人	110000567 特許業務法人 サトー国際特許事務所
		(72) 発明者	植山 剛 愛知県知多郡阿久比町大字草木字芳池1 株式会社デンソーウェーブ内
		(72) 発明者	澤田 洋祐 愛知県知多郡阿久比町大字草木字芳池1 株式会社デンソーウェーブ内
		Fターム(参考)	3C707 JU14 KT01 KT06 KV11 KX00 KX11 LS05 LW03 MS27 MS29

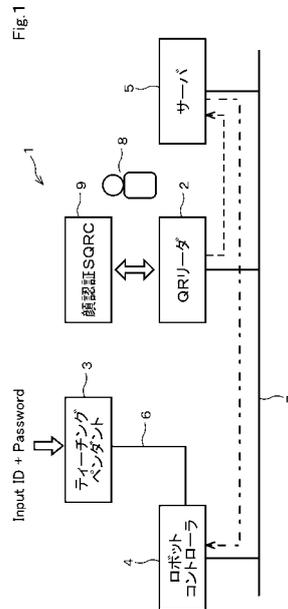
(54) 【発明の名称】 ロボット教示用認証システム

(57) 【要約】

【課題】ユーザの成りすましをより高いレベルで防止できるロボット教示用認証システムを提供する。

【解決手段】、認証システム1におけるロボットコントローラ4は、ユーザ8がティーチングペンダント3に自身のID及びパスワードを入力すると、その情報の認証処理を行う。QRリーダ2は、ユーザ8に付与されている顔認証SQRC9を読み取ると、読み取ってデコードした情報をサーバ5に転送する。コントローラ4は、転送されたIDがティーチングペンダント3の操作権限を有する者のIDであれば、ユーザ8を認証してそのIDをサーバ5に転送する。サーバ5は、QRリーダ2、コントローラ4よりそれぞれ転送された情報を照合する。照合結果が同一のユーザ8を示すものであればティーチングペンダント3にログイン処理の許可を与え、ティーチングペンダント3はその許可を受けてログイン処理を開始する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

ユーザがロボットに教示を行うために入力操作を行う教示装置と、
 前記ユーザに付与されているセキュリティコードを読み取るコード読み取り装置と、
 前記ユーザが前記教示装置に、操作者としての権限を認証する個人認証情報を入力すると、前記情報の認証処理を行う認証処理部と、
 前記コード読み取り装置が読み取ったセキュリティコードと、前記個人認証情報との照合処理を行う照合処理部とを備え、
 前記認証処理部は、前記個人認証情報により対応するユーザを認証すると、当該情報を前記照合処理部に転送し、
 前記照合処理部は、転送された個人認証情報と前記セキュリティコードとを照合した結果が同一のユーザを示すものであれば、前記教示装置にログイン処理の許可を与え、
 前記教示装置は、前記許可を受けてログイン処理を開始するロボット教示用認証システム。

10

【請求項 2】

前記セキュリティコードは、QRコードである請求項 1 記載のロボット教示用認証システム。

【請求項 3】

前記セキュリティコードは、SQRCである請求項 2 記載のロボット教示用認証システム。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ユーザがロボットに教示を行うために入力操作を行う教示装置について、個人認証を行うシステムに関する。

【背景技術】

【0002】

ロボットの教示装置である例えばティーチングペンダントの操作をユーザが開始する際には、一般に操作者としての権限を確認するためにユーザの個人認証情報を入力して、認証結果がOKであれば操作の開始を許可するようになっている。

30

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2010 - 198465 号公報

【特許文献 2】特開 2008 - 221363 号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、従来の認証システムはセキュリティレベルが低く、ユーザの成りすましを十分に排除できるものとは言えなかった。

40

本発明は、上記実情に鑑みてなされたものであり、その目的は、ユーザの成りすましをより高いレベルで防止できるロボット教示用認証システムを提供することにある。

【課題を解決するための手段】

【0005】

請求項 1 記載のロボット教示用認証システムによれば、コード読み取り装置は、ユーザに付与されているセキュリティコードを読み取る。認証処理部は、ユーザが教示装置に個人認証情報を入力すると、その情報の認証処理を行う。照合処理部は、読み取り装置が読み取ったセキュリティコードと個人認証情報との照合処理を行う。そして、認証処理部は、個人認証情報により対応するユーザを認証すると当該情報を前記照合処理部に転送し、

50

照合処理部は、転送された個人認証情報とセキュリティコードとを照合した結果が同一のユーザを示すものであれば教示装置にログイン処理の許可を与え、教示装置はその許可を受けてログイン処理を開始する。

【0006】

すなわち、ユーザの認証を、個人認証情報に併せてユーザに付与されているセキュリティコードも用いて行うので、認証処理を2段階で行うことによりセキュリティレベルを向上させて、ユーザの成りすましを防止できる。

【0007】

請求項2記載のロボット教示用認証システムによれば、セキュリティコードにQRコード（（株）デンソーウェーブの登録商標）を用いる。QRコードは、リーダによって2次元コードを光学的に読み取るものであるから、ユーザ個人に付与されているQRコード自体を取得しなければ認証処理を行うことができない。したがって、セキュリティレベルを確実に向上させることができる。また、QRコードを読み取るコードリーダは、ロボット等の生産設備が設置されている工場等で使用されることが多いので、認証処理を行うために特殊な装置を用いる必要がなくなる。

10

【0008】

請求項3記載のロボット教示用認証システムによれば、セキュリティコードにSQRC（（株）デンソーウェーブの登録商標）を用いる。SQRCは、QRコードにユーザの顔の特徴点の情報をコード化して重畳したものであるから、他人がSQRCを取得しても、顔の特徴点が不一致となることで認証結果は不可となる。したがって、ユーザの成りすましを確実に防止できる。

20

【図面の簡単な説明】

【0009】

【図1】一実施形態であり、認証システムの構成を示す機能ブロック図

【図2】認証システムにおける各装置間の動作を示すシーケンス図

【発明を実施するための形態】

【0010】

以下、一実施形態について図面を参照して説明する。図1は、認証システムの構成を示す機能ブロック図である。認証システム1は、QRリーダ2、ティーチングペンダント3、ロボットコントローラ4及びサーバ5を備えている。ティーチングペンダント3とロボットコントローラ4とは、ケーブル6により接続されている。QRリーダ2、ティーチングペンダント3、ロボットコントローラ4及びサーバ5とは、例えばLAN等のネットワーク7を介して接続されている。尚、ネットワーク7は、無線通信ネットワークでも良い。QRリーダ2は、ユーザ8に付与されているセキュリティコードである顔認証SQRC9の読み取りにも対応しているコードリーダである。尚、SQRCに関する技術の詳細については、例えば特許第6124124号公報等が開示されている。

30

【0011】

ティーチングペンダント3とロボットコントローラ4とは、図示しないロボット本体が生産設備として設置されている工場等に配置されている。QRリーダ2は、例えばユーザ8がロボットを動作させる際に、QRコード化されている様々な情報を読み取って入力するために携帯しているものである。また、QRリーダ2は、例えば教示対象であるロボットが設置されている工場にユーザ8が入場する際の入場門に配置されているものでも良い。ティーチングペンダント3は教示装置の一例であり、コントローラ4は認証処理部の一例である。QRリーダ2はコード読み取り装置の一例であり、サーバ5は照合処理部の一例である。

40

【0012】

次に、本実施形態の作用について図2を参照して説明する。図2は、認証システム1における各装置間の動作を示すシーケンス図である。ユーザ8は、ティーチングペンダント3を用いて作業を開始する際に、自身に付与されている顔認証SQRC9をQRリーダ2に読み取らせる。この段階で、QRリーダ2は、顔認証SQRC9に重畳されているコー

50

ド化されたユーザ 8 の顔の特徴点と、その読み取りの際に QR リーダ 2 がカメラ等により取得したユーザ 8 の顔の画像とが一致するか否かが判定される。

【 0 0 1 3 】

尚、上述したように QR リーダ 2 が工場の入場門に配置されている際には、ユーザ 8 が入場する際に顔認証 S Q R C 9 を QR リーダ 2 に読み取らせるようにする。判定が OK でありユーザ 8 を認証すると、読み取られてデコードされた情報はサーバ 5 に転送される。前記情報がサーバ 5 に転送されることで、ユーザ 8 がティーチングペンダント 3 を用いてロボットの教示を開始する意思の表示となる。

【 0 0 1 4 】

次に、ユーザ 8 は、ティーチングペンダント 3 に、ユーザ 8 に付与されている個人認証情報である ID 及びパスワードを入力する。入力された情報は、コントローラ 4 に転送される。コントローラ 4 には、ティーチングペンダント 3 の操作権限を有しているユーザの ID 及びパスワードの情報が予め登録されている。そして、コントローラ 4 は、転送された ID 及びパスワードが、操作権限を有しているユーザ 8 のものであるか否かを認証する。

10

【 0 0 1 5 】

ID とパスワードとが対応しており、且つその ID が操作権限を有しているユーザ 8 のものでありユーザ 8 を認証すると、コントローラ 4 は、サーバ 5 に前記 ID を転送することで、ユーザ 8 が教示を開始しようとしている否かの問い合わせを行う。サーバ 5 は、コントローラ 4 からの問い合わせがあると、転送された ID と顔認証 S Q R C 9 の情報とが同一のユーザ 8 を示しているか否かを照合する。その照合結果が OK であれば、サーバ 5 は、コントローラ 4 を介してティーチングペンダント 3 にログイン処理を許可する指令を送信する。すると、ティーチングペンダント 3 は、その許可指令を受けてユーザ 8 のログイン処理を開始する。

20

【 0 0 1 6 】

以上のように本実施形態によれば、認証システム 1 におけるロボットコントローラ 4 は、ユーザ 8 がティーチングペンダント 3 に自身の ID 及びパスワードを入力すると、その情報の認証処理を行う。QR リーダ 2 は、ユーザ 8 に付与されている顔認証 S Q R C 9 を読み取ると、読み取ってデコードした情報をサーバ 5 に転送する。コントローラ 4 は、転送された ID がティーチングペンダント 3 の操作権限を有する者の ID であれば、ユーザ 8 を認証してその ID をサーバ 5 に転送する。サーバ 5 は、QR リーダ 2 , コントローラ 4 よりそれぞれ転送された情報を照合する。そして、照合結果が同一のユーザ 8 を示すものであればティーチングペンダント 3 にログイン処理の許可を与え、ティーチングペンダント 3 はその許可を受けてログイン処理を開始する。

30

【 0 0 1 7 】

すなわち、ユーザ 8 の認証を、ID 及びパスワードに併せてユーザ 8 に付与されている顔認証 S Q R C 9 も用いて行うので、認証処理を 2 段階で行うことによりセキュリティレベルを向上させて、ユーザの成りすましを防止できる。そして、セキュリティコードに QR コードを用いるので、各ユーザ個人に付与されている QR コード自体を取得しなければ認証処理を行うことができないからセキュリティレベルを確実に向上させることができる。また、QR リーダ 2 は、ロボット等の生産設備が設置されている工場等で使用されることが多いので、認証処理を行うために特殊な装置を用いる必要がなくなる。加えて、セキュリティコードに顔認証 S Q R C 9 を用いるので、他人が顔認証 S Q R C 9 を取得しても、顔の特徴点が不一致となることで認証結果は NG , 不可となる。したがって、ユーザの成りすましを確実に防止できる。

40

【 0 0 1 8 】

本発明は上記した、又は図面に記載した実施形態にのみ限定されるものではなく、以下のような変形又は拡張が可能である。

セキュリティコードは S Q R C 9 に限ることなく、一般的な QR コードやバーコード等を用いても良い。

50

認証処理部はコントローラ4に限ることなく、ティーチングペンダント3の内部機能としても良い。

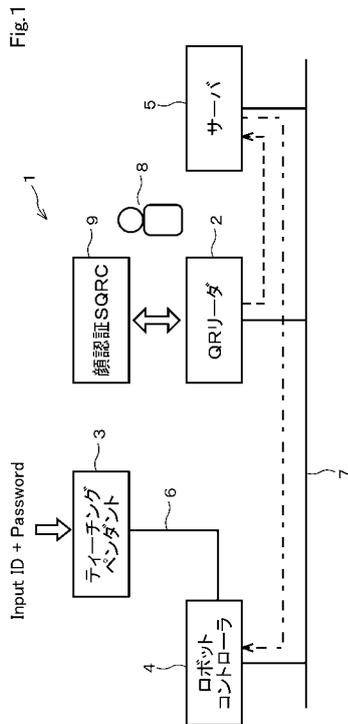
照合処理部はサーバ5に限ることなく、同じくティーチングペンダント3の内部機能としても良い。

【符号の説明】

【0019】

図面中、1は認証システム、2はQRリーダー、3はティーチングペンダント、4はロボットコントローラ、5はサーバ、8はユーザ、9は顔認証SQRCである。

【図1】



【図2】

