(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2017-152013
(P2017-152013A)
(43)公開日　平成29年8月31日(2017.8.31)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/32	(2013.01)	G06F 21/32		5B043
G06T 7/00	(2017.01)	G06T 7/00	510F	

審査請求 有　請求項の数 5　ＯＬ　（全 27 頁）

(21)出願番号　特願2017-75259 (P2017-75259)
(22)出願日　平成29年4月5日 (2017.4.5)
(62)分割の表示　特願2013-245579 (P2013-245579)の分割
原出願日　平成25年11月28日 (2013.11.28)

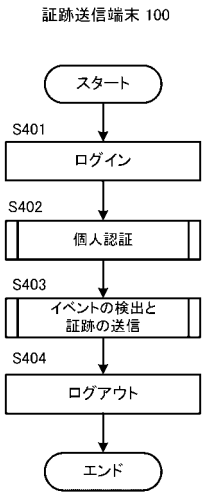
特許法第６４条第２項第４号の規定により図面の一部または全部を不掲載とする。

(71)出願人　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(71)出願人　592135203
キヤノンＩＴソリューションズ株式会社
東京都品川区東品川２丁目４番１１号
(74)代理人　100189751
弁理士　木村　友輔
(74)代理人　100208904
弁理士　伊藤　秀起
(72)発明者　深谷　大樹
東京都品川区東品川２丁目４番１１号　キヤノンＩＴソリューションズ株式会社内

Ｆターム(参考)　5B043 AA09　AA10　BA04　CA10　EA02
EA05　EA07　FA02　FA10

(54)【発明の名称】情報処理装置、情報処理方法、プログラム

(57)【要約】　（修正有）
【課題】管理者への負担を抑えつつ、テレワーカの労務状況やセキュリティインシデントの証跡を記録することが可能な仕組みを提供する。
【解決手段】撮像装置によって撮影されたユーザの顔画像を取得し、取得したユーザの顔画像から算出される特徴量と、あらかじめ登録された顔画像の特徴量との類似度を算出することで、個人認証をする。認証レベルに応じて、あらかじめ登録された顔画像の特徴量を用いてイベント検出をするか、テレワーク開始時に取得した顔画像の特徴量を用いてイベント検出をするかを決定する。
【選択図】図４



【特許請求の範囲】
【請求項１】
撮像装置によって撮影されたユーザの顔画像を取得する取得手段と、
前記取得手段により取得したユーザの顔画像から算出される特徴量と、あらかじめ登録された顔画像の特徴量との類似度を算出する類似度算出手段と、
前記撮像装置によって撮影された画像に基づきイベントを検出するイベント検出手段と、
前記検出手段により検出されたイベントを管理者に通知する通知手段と、
を備え、
前記イベント検出手段は、前記類似度算出手段により算出された類似度が第１の閾値を満たす場合、および、第１の閾値と第２の閾値とを満たさない場合、前記あらかじめ登録された顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出し、
前記類似度算出手段により算出された類似度が、第１の閾値を満たさず、第２の閾値を満たす場合、前記取得手段により取得した顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出することを特徴とする情報処理装置。
【請求項２】
前記類似度算出手段により算出された類似度が、第１の閾値を満たさず、第２の閾値を満たす場合、前記取得手段により取得した顔画像の特徴量を前記イベント検出手段によるイベント検出に用いるか否かの指示を管理者から受け付ける受付手段をさらに備え、
前記イベント検出手段は、前記受付手段により管理者から前記取得手段により取得した顔画像の特徴量を前記イベント検出手段によるイベント検出に用いる旨の指示を受け付けた場合、当該顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記類似度算出手段により算出された類似度が、第１の閾値および第２の閾値を満たさない場合、前記取得手段により取得した顔画像の特徴量を前記イベント検出手段によるイベント検出に用いるか否かの指示を管理者から受け付ける受付手段をさらに備え、
前記イベント検出手段は、前記受付手段により管理者から前記取得手段により取得した顔画像の特徴量を前記イベント検出手段によるイベント検出に用いる旨の指示を受け付けた場合、当該顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出することを特徴とする請求項１または２に記載の情報処理装置。
【請求項４】
情報処理装置の取得手段が、撮像装置によって撮影されたユーザの顔画像を取得する取得工程と、
前記情報処理装置の類似度算出手段が、前記取得工程により取得したユーザの顔画像から算出される特徴量と、あらかじめ登録された顔画像の特徴量との類似度を算出する類似度算出工程と、
前記情報処理装置のイベント検出手段が、前記撮像装置によって撮影された画像に基づきイベントを検出するイベント検出工程と、
前記情報処理装置の通知手段が、前記検出工程により検出されたイベントを管理者に通知する通知工程と、
を備え、
前記イベント検出工程は、前記類似度算出工程により算出された類似度が第１の閾値を満たす場合、および、第１の閾値と第２の閾値とを満たさない場合、前記あらかじめ登録された顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出し、
前記類似度算出工程により算出された類似度が、第１の閾値を満たさず、第２の閾値を満たす場合、前記取得工程により取得した顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出することを特徴とする情報処理方法。

【請求項５】
情報処理装置において実行可能なプログラムであって、
前記情報処理装置を、
撮像装置によって撮影されたユーザの顔画像を取得する取得手段と、
前記取得手段により取得したユーザの顔画像から算出される特徴量と、あらかじめ登録された顔画像の特徴量との類似度を算出する類似度算出手段と、
前記撮像装置によって撮影された画像に基づきイベントを検出するイベント検出手段と、
前記検出手段により検出されたイベントを管理者に通知する通知手段と、
して機能させ、
前記イベント検出手段を、前記類似度算出手段により算出された類似度が第１の閾値を満たす場合、および、第１の閾値と第２の閾値とを満たさない場合、前記あらかじめ登録された顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出し、
前記類似度算出手段により算出された類似度が、第１の閾値を満たさず、第２の閾値を満たす場合、前記取得手段により取得した顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出する手段として機能させることを特徴とするプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、テレワーク管理システムに関する。
【背景技術】
【０００２】
近年、ブロードバンドや情報セキュリティ技術の発達の他、災害時における事業継続性や節電対策への注目などを背景に、各企業でテレワークに対する関心が強まっている。テレワークを導入する上では、管理者から様子が見えにくいため、家族をはじめとする第三者による情報処理端末へのアクセスにより機密情報が漏えいするリスクや、労働管理がしにくい問題がある。
【０００３】
機密情報の漏えい予防手段としては、顔認識技術を用いて個人認証を行い、本人でない場合は情報処理端末をロックするといった先行技術が検討されている。顔認識技術は人などの顔を検出し、その属性情報を読み取る技術である。顔認識技術を用いた個人認証（顔認証）は、顔画像から算出した特徴量を学習した識別器によって他の顔画像から算出した特徴量との類似性を算出し、その顔の人物を識別する技術である。学習の際、同一人物を同じ識別子に関連付けて学習させる。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００９－２１１３８１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
前述の特許文献１のような顔認識を用いたテレワーク管理システムでは、予防機能に重点を置いており、何時から何時まで情報処理端末の前に在席していた、または離席していたといった、労務状況を管理者が知る仕組みが存在しない。また、顔認識の精度が高いこ

とが前提となっており、利用できる顔認識技術の精度が低い条件下については言及されていない。そのような条件下においては、本人であるにも関わらず情報処理端末を頻繁に利用できなくなる、または本人以外でも利用できてしまうことになりかねない。

【０００６】

顔認識技術は、照明条件や化粧、顔の向きやメガネの有無などによって、顔を検出できなかったり、うまく個人を認証できなかったりする。テレワークにおいては、特にこれらの条件の変動が頻繁に発生する可能性がある。

【０００７】

認証精度を高める最も単純な方法は、学習する顔画像（の特徴量）と認証対象の顔画像（の特徴量）との差異をなるべく取り除くことであり、テレワークを行うその日に同じ場所で撮影した顔画像を学習することは有用である。ただし、その顔画像がテレワーカ本人のものであることをテレワーカの労務管理者が保証する必要があるため、管理者の負担は大きくなる。

【０００８】

そこで、本発明は、管理者への負担を抑えつつ、テレワーカの労務状況やセキュリティインシデントの証跡を記録することが可能な仕組み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】

【０００９】

本発明の情報処理装置は、撮像装置によって撮影されたユーザの顔画像を取得する取得手段と、前記取得手段により取得したユーザの顔画像から算出される特徴量と、あらかじめ登録された顔画像の特徴量との類似度を算出する類似度算出手段と、前記撮像装置によって撮影された画像に基づきイベントを検出するイベント検出手段と、前記検出手段により検出されたイベントを管理者に通知する通知手段と、を備え、前記イベント検出手段は、前記類似度算出手段により算出された類似度が第１の閾値を満たす場合、および、第１の閾値と第２の閾値とを満たさない場合、前記あらかじめ登録された顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出し、前記類似度算出手段により算出された類似度が、第１の閾値を満たさず、第２の閾値を満たす場合、前記取得手段により取得した顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出することを特徴とする。

【００１０】

また、本発明の情報処理方法は、情報処理装置の取得手段が、撮像装置によって撮影されたユーザの顔画像を取得する取得工程と、前記情報処理装置の類似度算出手段が、前記取得工程により取得したユーザの顔画像から算出される特徴量と、あらかじめ登録された顔画像の特徴量との類似度を算出する類似度算出工程と、前記情報処理装置のイベント検出手段が、前記撮像装置によって撮影された画像に基づきイベントを検出するイベント検出工程と、前記情報処理装置の通知手段が、前記検出工程により検出されたイベントを管理者に通知する通知工程と、を備え、前記イベント検出工程は、前記類似度算出工程により算出された類似度が第１の閾値を満たす場合、および、第１の閾値と第２の閾値とを満たさない場合、前記あらかじめ登録された顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出し、前記類似度算出工程により算出された類似度が、第１の閾値を満たさず、第２の閾値を満たす場合、前記取得工程により取得した顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出することを特徴とする。

【００１１】

また、本発明のプログラムは、情報処理装置において実行可能なプログラムであって、前記情報処理装置を、撮像装置によって撮影されたユーザの顔画像を取得する取得手段と、前記取得手段により取得したユーザの顔画像から算出される特徴量と、あらかじめ登録された顔画像の特徴量との類似度を算出する類似度算出手段と、前記撮像装置によって撮影された画像に基づきイベントを検出するイベント検出手段と、前記検出手段により検出されたイベントを管理者に通知する通知手段と、して機能させ、前記イベント検出手段を

、前記類似度算出手段により算出された類似度が第１の閾値を満たす場合、および、第１の閾値と第２の閾値とを満たさない場合、前記あらかじめ登録された顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出し、前記類似度算出手段により算出された類似度が、第１の閾値を満たさず、第２の閾値を満たす場合、前記取得手段により取得した顔画像の特徴量と、前記撮像装置によって撮影された画像とに基づきイベントを検出する手段として機能させることを特徴とする。

【発明の効果】

【００１２】

本発明によれば、管理者への負担を抑えつつ、テレワーカの労務状況やセキュリティインシデントの証跡を記録することが可能な仕組みを提供することが可能となる。

【図面の簡単な説明】

【００１３】

【図１】本発明のテレワーク管理システムの構成の一例を示すシステム構成図である。

【図２】図１に示した証跡送信端末１００および証跡監査端末１１０，証跡管理サーバ１２０に適用可能な情報処理装置のハードウェア構成を示すブロック図である。

【図３】図１に示した証跡送信端末１００および証跡監査端末１１０，証跡管理サーバ１２０に必要な機能構成を示すブロック図である。

【図４】本発明におけるテレワーク管理システムにおける証跡送信装置の全体処理の一例を示すフローチャートである。

【図５】本発明におけるテレワーク管理システムにおける証跡送信装置の個人認証処理の一例を示すフローチャートである。

【図６】本発明におけるテレワーク管理システムにおける一時特徴量データの登録と承認の処理の一例を示すフローチャートである。

【図７】本発明におけるテレワーク管理システムにおけるイベントの検出とその証跡の送信の処理の一例を示すフローチャートである。

【図８】本発明におけるテレワーク管理システムにおける管理者情報が登録されたデータテーブルの一例を表すデータ構造図である。

【図９】本発明におけるテレワーク管理システムにおけるテレワーカ情報が登録されたデータテーブルの一例を表すデータ構造図である。

【図１０】本発明におけるテレワーク管理システムにおける識別子情報が登録されたデータテーブルの一例を表すデータ構造図である。

【図１１】本発明におけるテレワーク管理システムにおける特徴量データが登録されたデータテーブルの一例を表すデータ構造図である。

【図１２】本発明におけるテレワーク管理システムにおけるフレーム情報が登録されたデータテーブルの一例を表すデータ構造図である。

【図１３】本発明におけるテレワーク管理システムにおける顔検出結果が登録されたデータテーブルの一例を表すデータ構造図である。

【図１４】本発明におけるテレワーク管理システムにおける顔識別結果が登録されたデータテーブルの一例を表すデータ構造図である。

【図１５】本発明におけるテレワーク管理システムにおける証跡情報が登録されたデータテーブルの一例を表すデータ構造図である。

【図１６】本発明におけるテレワーク管理システムにおけるユーザが操作する画面の一例を示す画面イメージである。

【図１７】本発明におけるテレワーク管理システムにおけるユーザが操作する画面の一例を示す画面イメージである。

【図１８】本発明におけるテレワーク管理システムにおける認証レベルを求めるための第１の閾値、第２の閾値が登録されたデータテーブルの一例を示す図である。

【発明を実施するための形態】

【００１４】

まず、本発明の概要について説明する。

【００１５】
本発明のテレワーク管理システムは、顔認識技術を用いてテレワーカのイベント（”着席”や”離席”の労務イベントや、第三者による”なりすまし”や”覗き込み”のセキュリティインシデント）を検出・記録し、管理者が閲覧できるようにするシステムである。
【００１６】
テレワーカが勤務を開始する際、テレワーカの顔写真を撮影し、当該顔写真と、最初にテレワーカ本人であることが保証されている顔画像の特徴量とを用いて個人認証を行い、テレワーカ本人である可能性の度合い（認証レベル）を算出する（以降、顔画像とその特徴量をまとめて特徴量データ、個人認証に使用する特徴量データを認証特徴量データとする）。
【００１７】
たとえば、テレワーカ本人である可能性が極めて高い場合”高”、テレワーカ本人である可能性が高いが、第三者である可能性もある場合”中”、第三者である可能性が極めて高い場合”低”とする。なお、認証レベルについては、顔写真から算出される特徴量と、認証特徴量データとの類似度を算出し、予め定められた閾値と類似度とを用いることで、認証レベルを算出する。
【００１８】
認証レベルが”高”の場合、認証特徴量データと映像に写る人物の特徴量データとの差異が少ないので、認証特徴量データを使用してイベントの検出を行う。
【００１９】
認証レベルが”中”の場合、認証特徴量データと映像に写る人物の特徴量データに多少の差異がみられるため、現在の映像に写る顔から新たに特徴量データ（以降、一時特徴量データとする）を取得し、それを使ってイベントの検出を行う。これにより、管理者が保証した特徴量データ（認証特徴量データ）から多少の差異が見受けられたとしても正常にイベントを検出できるようになる。
【００２０】
ただし、一時特徴量データが第三者のものである可能性もあるので、その特徴量データを記録し、管理者に確認させる。管理者がその一時特徴量データを第三者のものであると判断した場合、速やかに一時特徴量データでのイベント検出を取りやめ、認証特徴量データを使用してイベントの検出を行うようにする。また、一時特徴量データが今後のテレワーカの認証にふさわしいと判断した場合、管理者はその一時特徴量データを認証特徴量データとして登録する。
【００２１】
認証レベルが”低”の場合、第三者である可能性が高いので、認証特徴量データを使用してイベントの検出を行う。この場合は”なりすまし”が頻発すると考えられる。ただし、例えば普段は化粧をしている人が化粧をしていなかったり、普段メガネをかけていない人がメガネをかけていたりする可能性もあるため、現在の映像から新たに一時特徴量データを取得して記録し、管理者に確認させる。管理者がその一時特徴量データをテレワーカのものと判断した場合、一時特徴量データを使用してイベントの検出を行うようにする。
【００２２】
以上が本発明におけるテレワーク管理システムの概要である。
【００２３】
以下、図面を参照して、本発明の実施形態を詳細に説明する。
【００２４】
図１は、本発明のテレワーク管理システムの構成の一例を示すシステム構成図である。
【００２５】
図１は、１又は複数の証跡送信端末１００、１又は複数の証跡監査端末１１０、１又は複数の証跡管理サーバ１２０が、ローカルエリアネットワーク（ＬＡＮ）１３０とルータ１４０、およびインターネット１５０を介して接続される構成となっている。
【００２６】

証跡送信端末１００は、使用するテレワーカの労務イベントおよびセキュリティインシデントを検出し、その証跡を証跡管理サーバ１２０に送信する。また、イベント検出に使用するテレワーカの特徴量データ（顔画像とそこから取得した特徴量）を証跡管理サーバ１２０に送信する。

【００２７】

証跡監査端末１１０は、証跡管理サーバ１２０に記録された特徴量データの承認操作と、証跡管理サーバ１２０に記録された証跡の監査操作を行う。

【００２８】

証跡管理サーバ１２０は、証跡送信端末１００から受信した証跡を記録し、その証跡に対する証跡監査端末１１０の監査操作を処理する。また、証跡送信端末１００から受信した特徴量データを記録し、その特徴量データに対する証跡監査端末１１０の承認操作を処理する。

【００２９】

以下、図２を用いて、図１に示した証跡送信端末１００、証跡監査端末１１０、証跡管理サーバ１２０に適用可能な情報処理装置のハードウェア構成について説明する。

【００３０】

図２は、図１に示した証跡送信端末１００、証跡監査端末１１０、証跡管理サーバ１２０に適用可能な情報処理装置のハードウェア構成を示すブロック図である。

【００３１】

図２において、２０１はＣＰＵで、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。また、ＲＯＭ２０３あるいは外部メモリ２１２には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　／　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）やオペレーティングシステムプログラム（以下、ＯＳ）や、各サーバ或いは各ＰＣの実行する機能を実現するために必要な後述する各種プログラム等が記憶されている。

【００３２】

２０３はＲＡＭで、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＯＭ２０３あるいは外部メモリ２１２からＲＡＭ２０２にロードして、該ロードしたプログラムを実行することで各種動作を実現するものである。

【００３３】

また、２０５は入力コントローラで、キーボード（ＫＢ）２０９やカメラデバイス２１０（撮像装置）、不図示のマウス等のポインティングデバイス等からの入力を制御する。２０６はビデオコントローラで、ＣＲＴディスプレイ（ＣＲＴ）２１１等の表示器への表示を制御する。なお、図２では、ＣＲＴ２１１と記載しているが、表示器はＣＲＴだけでなく、液晶ディスプレイ等の他の表示器であってもよい。これらは必要に応じて管理者が使用するものである。

【００３４】

２０７はメモリコントローラで、ブートプログラム，各種のアプリケーション，フォントデータ，ユーザファイル，編集ファイル，各種データ等を記憶する外部記憶装置（ハードディスク（ＨＤ））や、フレキシブルディスク（ＦＤ）、或いはＰＣＭＣＩＡカードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１２へのアクセスを制御する。

【００３５】

２０８は通信Ｉ／Ｆコントローラで、ネットワーク（例えば、図１に示したＬＡＮ１３０）を介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰを用いた通信等が可能である。

【００３６】

なお、ＣＰＵ２０１は、例えばＲＡＭ２０２内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ＣＲＴ２１１上での表示を可能と

している。また、ＣＰＵ２０１は、ＣＲＴ２１１上の不図示のマウスカーソル等でのユーザ指示を可能とする。

【００３７】

本発明を実現するための後述する各種プログラムは、外部メモリ２１２に記録されており、必要に応じてＲＡＭ２０２にロードされることによりＣＰＵ２０１によって実行されるものである。さらに、上記プログラムの実行時に用いられる定義ファイル及び各種情報テーブル等も、外部メモリ２１２に格納されており、これらについての詳細な説明も後述する。

【００３８】

次に、図３を用いて、本発明の証跡送信端末１００、証跡監査端末１１０および証跡管理サーバ１２０の機能ブロック図について説明する。

【００３９】

尚、各機能ブロックが処理する詳細な制御については、後述するフローチャートにて説明する。

【００４０】

まず、証跡送信端末１００の機能構成について説明する。

【００４１】

映像入力部１０１は、カメラデバイス２１０より映像を取得し、個人認証部１０２にその映像を送信する。個人認証部１０２の処理が完了したら、イベント検出部１０６にその映像を送信する。

【００４２】

個人認証部１０２は、映像入力部１０１から送られてきた映像のフレーム（静止画）と特徴量データ記憶部１０４から取得した特徴量データの特徴量を顔認識部１０３に与え、顔認識部１０３から得られた顔識別結果から映像に写っているのがテレワーカ本人である可能性（認証レベル）を”高”、”中”、”低”として算出する。認証レベルが”高”の場合、イベントの検出に使用する特徴量として認証に使用した特徴量を指定する。”中”、”低”の場合、フレームから顔画像とその一時特徴量を取得し、特徴量データ記憶部１０４に記憶する。

【００４３】

顔認識部１０３は、個人認証部１０２またはイベント検出部１０６から送られてきたフレームに対して顔検出を行う。さらに検出された顔に対して、指定された特徴量との類似度を算出する。

【００４４】

特徴量データ記憶部１０４は、顔画像とその特徴量からなる特徴量データを記憶する。

【００４５】

特徴量データ送信部１０５は、個人認証部１０２から送られてきた特徴量データを、通信Ｉ／Ｆコントローラ２０８を介して証跡管理サーバ１２０の特徴量データ受信部１２１に送信する。

【００４６】

イベント検出部１０６は、映像入力部１０１から取得した映像のフレームと個人認証部で指定された特徴量データを顔認識部１０３に与え、顔認識部１０３から得られた顔識別結果をもとに、着席、離席、なりすまし、覗き込み等のイベントを検出する。検出したイベントの証跡は、証跡制御部１０７に送信する。

【００４７】

証跡制御部１０７は、イベント検出部１０６から得られた証跡を証跡記憶部１０８に記憶する。特定の送信条件が満たされた場合（たとえば、離席イベントが発生してから３分経過等）、証跡記憶部１０８に記録された証跡を証跡送信部１０９に送信する。さらに、送信の済んだ、または送信の必要がなくなった（たとえば、離席イベントが発生してから３分以内に着席イベントが発生した等）証跡を証跡記憶部１０８から消去する。

【００４８】

証跡記憶部１０８は、イベントの証跡を記憶する。
【００４９】
証跡送信部１０９は、証跡制御部１０７から得られた証跡を、通信Ｉ／Ｆコントローラ２０８を介して証跡管理サーバ１２０の証跡受信部１２５に送信する。
【００５０】
特徴量データ更新部１０Ａは、証跡管理サーバ１２０の特徴量データ管理操作処理部１２４の結果を受けて、特徴量データ記憶部１０４の特徴量データを更新する。
【００５１】
次に、証跡監査端末１１０の機能構成について説明する。
【００５２】
特徴量データ管理操作部１１１は、証跡管理サーバ１２０の特徴量データ管理操作処理部１２４を介して、特徴量データの閲覧と、その承認状況（承認待ち、承認、否認、差戻し）および識別子との関連（識別ＩＤ）の更新を行う。
【００５３】
証跡監査操作部１１２は、証跡管理サーバ１２０の証跡監査操作処理部１２７を介して、イベントの証跡と、イベントから導かれる労務状況の統計情報を閲覧する。
【００５４】
更新通知受信部１１３は、証跡管理サーバ１２０の更新通知送信部からの更新通知を受信する。
【００５５】
最後に、証跡管理サーバ１２０の機能構成について説明する。
【００５６】
特徴量データ受信部１２１は、証跡送信端末１００の特徴量データ送信部１０５から送られてくる特徴量データを受信し、特徴量データ記憶部１２２に記憶する。また、更新通知送信部１２３に、新しい特徴量データの登録があったことを通知するよう要求する。
【００５７】
特徴量データ記憶部１２２は、特徴量データ受信部１２１で受信した特徴量データを記憶する。また、特徴量データの識別ＩＤに紐づいた識別子の情報を記憶する。
【００５８】
更新通知送信部１２３は、特徴量データおよび証跡を受信した際に、証跡監査端末１１０の更新通知受信部１１３に更新通知を送信する。
【００５９】
特徴量データ管理操作受信部１２４は、証跡監査端末１１０の特徴量データ管理操作部１１１の命令を受けて、特徴量データ記憶部１２２の特徴量データを画面に表示したり、特徴量データへの操作を処理したりする。
【００６０】
証跡受信部１２５は、証跡送信端末１００の証跡送信部１０９から送信された証跡を受信し、証跡記憶部１２６に記憶する。また、証跡のイベントが”なりすまし”や”覗き込み”であった場合、更新通知送信部１２３に、セキュリティインシデントの証跡の登録があったことを通知するよう要求する。
【００６１】
証跡記憶部１２６は、”着席”、”離席”等の労務イベントや”なりすまし”、”覗き込み”等のセキュリティインシデントの証跡を記憶する。
【００６２】
証跡監査操作処理部１２７は、証跡監査端末１１０の証跡監査操作部１１２の命令を受けて、証跡記憶部１２６の証跡や、証跡から算出した労務の統計情報を画面に表示したり、証跡に対する操作を処理したりする。
【００６３】
アカウント記憶部１２８は、テレワーカおよび管理者のアカウント情報を記憶する。
【００６４】

なお、テレワーカおよび管理者がシステムを利用する際に必要なアカウント認証を行う機能および、それらのアカウント情報を登録する機能についても備えているが、本発明の趣旨から外れるため詳細な説明は省略する。

【００６５】

以下、本実施形態におけるテレワーク管理システムの全体の流れを、個人認証による認証レベルごとに説明する。

【００６６】

まず、認証レベルが”高”の場合について説明する。

【００６７】

証跡送信端末１００は、カメラデバイス２１０から取得した映像に対して認証特徴量データを使って個人認証を行い、認証レベルを算出する。認証レベルが”高”の場合、認証特徴量データを使ってイベントの検出を開始する。イベントが検出されたら、その証跡を証跡管理サーバ１２０に送信する。

【００６８】

証跡管理サーバ１２０は、証跡送信端末１００から受け取った証跡を記憶し、セキュリティインシデントの証跡である場合は、証跡監査端末１１０にセキュリティインシデントの証跡の登録に関する更新通知を送信する。

【００６９】

証跡監査端末１１０は、証跡管理サーバ１２０からの更新通知を受けて証跡を表示し、必要に応じてその証跡に対する操作を受け付ける。また、労務イベントの統計情報を表示する。

【００７０】

次に、認証レベルが”中”の場合について説明する。

【００７１】

証跡送信端末１００は、カメラ映像に対して認証特徴量データを使って個人認証を行い、認証レベルを算出する。認証レベルが”中”の場合、現在の映像から一時特徴量データを算出し、証跡管理サーバ１２０に送信し、その一時特徴量データでイベントの検出を開始する。

【００７２】

証跡管理サーバ１２０は、証跡送信端末１００から受け取った一時特徴量データを記憶し、証跡監査端末１１０に特徴量データ登録に関する更新通知を送信する。

【００７３】

証跡監査端末１１０は、証跡管理サーバ１２０からの更新通知を受けて、一時特徴量データの承認操作を行う。特に問題がない場合は承認状況を”承認”にし、さらに今後認証に使用する特徴量データとする場合、関連する識別子を設定する。特徴量データが第三者のものである場合は承認状況を”否認”にする。特徴量データがテレワーカ本人のものであるが、認証にふさわしいものとみなせない場合、承認状況を”差戻し”にする。

【００７４】

証跡管理サーバ１２０は、証跡監査端末１１０から受け取った特徴量データ操作を処理する。

【００７５】

証跡操作端末１００は、証跡管理サーバ１２０の特徴量データの変更を受けて、端末に記憶された特徴量データを更新する。

【００７６】

証跡送信端末１００は、イベント検出に使用している一時特徴量データの承認状況が”否認”になっている場合、イベント検出に使用する特徴量データを認証特徴量データに置き換える。必要であれば、情報処理端末にロックをかける。また、イベント検出に使用している一時特徴量データの承認状況が”差戻し”になっている場合、再度個人認証を行い、イベント検出に使用する特徴量データを更新する。

【００７７】

次に、認証レベルが”低”の場合について説明する。

【００７８】

証跡送信端末１００は、カメラ映像に対して登録済の認証特徴量データを使って個人認証を行い、認証レベルを算出する。認証レベルが”低”の場合、認証特徴量データを使ってイベントの検出を開始する。また、現在の映像から一時特徴量データを算出し、証跡管理サーバ１２０に送信する。

【００７９】

証跡管理サーバ１２０は、証跡送信端末１００から受け取った一時特徴量データを記憶し、証跡監査端末１１０に特徴量データ登録に関する更新通知を送信する。

【００８０】

証跡監査端末１１０は、証跡管理サーバ１２０からの更新通知を受けて、一時特徴量データの承認操作を行う。特に問題がない場合は承認状況を”承認”にし、さらに今後認証に使用する特徴量データとする場合、関連する識別子を設定する。特徴量データが第三者のものである場合は承認状況を”否認”にする。特徴量データがテレワーカ本人のものであるが、認証にふさわしいものとみなせない場合は承認状況を”差戻し”にする。

【００８１】

証跡管理サーバ１２０は、証跡監査端末１１０から受け取った特徴量データ操作を処理する。

【００８２】

証跡操作端末１００は、証跡管理サーバ１２０の特徴量データの変更を受けて、端末に記憶された特徴量データを更新する。

【００８３】

証跡送信端末１００は、送信した一時特徴量データの承認状況が”承認”になっている場合、イベント検出に使用する特徴量データを一時特徴量データに置き換える。また、送信した一時特徴量データの承認状況が”否認”になっている場合、必要であれば情報処理端末にロックをかける。また、イベント検出に使用している一時特徴量データの承認状況が”差戻し”になっている場合、再度個人認証を行い、イベント検出に使用する特徴量データを更新する。

【００８４】

以下、図４を参照して、本実施形態のテレワーク管理システムにおける、テレワーカが利用する証跡送信端末１００上で動作する常駐アプリケーションでの処理について説明する。

【００８５】

図４のフローチャートで示す処理は、証跡送信端末１００のＣＰＵ２０１が所定の制御プログラムを読み出して実行する処理である。

【００８６】

ステップＳ４０１では、ユーザが証跡送信端末１００にログインすることにより、証跡送信端末１００が常駐アプリケーションを起動し、バックグラウンドで証跡管理サーバ１２０にテレワーカのアカウントＩＤとパスワードによってログインする。証跡管理サーバ１２０は、アカウント記憶部１２８に記憶されたテレワーカの情報（図９）と比較し、一致すればログインを許可する。アカウントＩＤとパスワードは、常駐アプリケーションの初回起動時にユーザが設定し、以降は設定された値を使用するものとする。

【００８７】

ステップＳ４０２では、証跡送信端末１００を使用しているユーザが証跡管理サーバ１２０に登録されたテレワーカである可能性を算出し、その結果次第でステップＳ４０３のイベント検出で使用する特徴量データを決定する。詳細については図５で説明する。

【００８８】

ステップＳ４０３では、イベント（”着席”、”離席”といった労務イベントや、”なりすまし”、”覗き込み”といったセキュリティインシデント）を検出し、その証跡を証跡管理サーバ１２０に送信する。詳細については図６で説明する。

【００８９】
ステップＳ４０４では、ユーザが証跡送信端末１００からログアウトすることにより、証跡送信端末１００がバックグラウンドで証跡管理サーバ１２０からログアウトする。
【００９０】
以下、図５を参照して、図４の４０２の個人認証処理の詳細について説明する。図５のフローチャートで示す処理は、証跡送信端末１００のＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムをＲＡＭ２０２に記憶することで実行される。
【００９１】
ステップＳ５０１では、ステップＳ５０２－Ｓ５１５で発生する処理以外のユーザ操作をロックする。また、顔の認証を行うことをユーザに通知し、通常業務を行う姿勢でＣＲＴ２１１の中央を見てもらえるよう促す。すなわち、業務を行う際の通常の姿勢を取ってもらうように促す。
【００９２】
ステップＳ５０２－Ｓ５０７では、ＲＡＭ２０２にＮ件のフレームに対する顔識別結果（図１４）が記憶されるまで、カメラデバイスに写るフレームに対して顔識別を繰り返す。このように複数のフレームに対して顔識別処理を行うのは、１つのフレームに対する１度の顔識別結果だけでは、たまたま良いまたは悪い結果が得られてしまう可能性があることから、適切な判断をするために行うものである。ただし、必ずしも複数にする必要はなく、１つのフレームに対して１度の顔識別処理を行うようにしても良い。
【００９３】
なおＮ件の具体的な数値については、予め定められているものとし、例えば５件や１０件といった値である。
【００９４】
ステップＳ５０３では、カメラデバイス２１０からフレームの入力を受け付け、その情報（図１２）をＲＡＭ２０２に記憶する。
【００９５】
ステップＳ５０４では、ステップＳ５０３で取得したフレームに対して顔検出を行う。得られた顔検出結果（図１３）を、ＲＡＭ２０２に記憶する。
【００９６】
ステップＳ５０５では、ステップＳ５０４で検出された顔が１つであるかを判断する。
【００９７】
検出された顔が１つである場合（ステップＳ５０５：ＹＥＳ）は、処理をステップＳ５０６に移行し、それ以外の場合はステップＳ５０２に遷移する。
【００９８】
ステップＳ５０６では、ステップＳ５０４で得られた顔検出結果をもとにフレームから顔画像を取得する。そして、その顔画像について、認証特徴量データ（の特徴量）を学習させた識別器を使って顔識別を行う。
【００９９】
得られた顔識別結果（図１４）はＲＡＭ２０２に記憶する。同じ識別子に関連付けられる認証特徴量データが複数ある場合は、それらを同じ識別対象として識別器に学習させる。
【０１００】
複数の識別子が存在する場合、それらを別の識別対象として学習させる。ここでいう識別対象とは、対象がテレワーカ本人であることは同じなのだが、メガネや化粧の有無、業務を実行する環境の違い（による照明環境やカメラと顔の位置関係など）など、テレワーカの業務環境をカテゴライズしたものとなる。初回はここで使用する認証特徴量データが存在しないと考えられるが、その場合はステップＳ５０８において認証レベル“中”と算出されることになる類似度を設定した顔識別結果を生成し、ＲＡＭ２０２に記憶する。
【０１０１】
そして、撮影回数がＮ件に達したかを判断し、Ｎ件に達している場合は、ステップＳ５

０８へ処理を進める。Ｎ件に達していない場合は、再度ステップＳ５０３からＳ５０６の処理を繰り返す（ステップＳ５０７）。

【０１０２】

ステップＳ５０８では、ＲＡＭ２０２に記憶された顔識別結果から、その代表となる顔識別結果を選出し、そこから一時特徴量データ（図１１）を生成し、ＲＡＭ２０２に記憶する。

【０１０３】

代表となる顔識別結果の選出の一例としては、Ｎ件の顔識別結果の類似度の平均値に最も近い類似度をもつ顔識別結果を選出する方法がある。

【０１０４】

生成した一時特徴量データと、認証用特徴量データとの類似度が閾値Ａ（第１の閾値）を超えていたら、テレワーカ本人であると認証されたものとし、生成した一時特徴量データの認証レベルを”高”にする。類似度が閾値Ａ未満で閾値Ｂ（第２の閾値）を超えていたら、認証レベルを“中”に、閾値Ｂを下回っていたら認証レベルを“低”にする。

【０１０５】

ここで、閾値Ａは認証特徴量データによる認証において、類似度がその値以上であればほぼ同一人物であることが保証される類似度の値であり、閾値Ｂは、類似度がその値以上であれば本人である可能性が高いと考えられる類似度の値である。この閾値は、使用する顔認識技術等によって異なる。

【０１０６】

識別器に複数の識別子が登録されていた場合、別々に類似度の平均値を算出し、最もその値が大きい識別子の顔識別結果から選出するものとする。一時特徴量データの生成後、ＲＡＭ２０２に記憶されたフレーム、顔検出結果、顔識別結果をすべて消去する。

【０１０７】

ステップＳ５０９では、ステップＳ５０８で算出した一時特徴量データの認証レベルを判定する。

【０１０８】

判定の結果、一時特徴量データの認証レベルが“高”であれば処理をステップＳ５１０に移行する。

【０１０９】

それ以外（認証レベルが中、低）であれば処理をステップＳ５１１に遷移する。

【０１１０】

ステップＳ５１０では、イベントの検出を行う際に使用する特徴量データとして、ステップＳ５０６で使用した認証特徴量データをＲＡＭ２０２に記憶する。

【０１１１】

複数の識別子が存在する場合、ステップＳ５０８で算出した、類似度の平均値が最も大きい識別子の認証特徴量データをイベントの検出を行う際に使用する特徴量データとして設定する。なお、イベント検出において複数の識別子の登録を許可するのであれば、すべての認証特徴量データをイベント検出に使用するよう設定してもかまわない。

【０１１２】

複数の識別子が存在する場合とは、認証用特徴量データが複数登録されている場合をいう。たとえばメガネをかけている顔の認証用特徴量データと、メガネをかけていない顔の認証特徴量データの２通りが登録されている場合である。

【０１１３】

そして、処理をステップＳ５１６に移行する。ステップＳ５１６の処理は後述する。

【０１１４】

ステップＳ５０９において認証レベル中または低と判断された場合の処理について説明する。

【０１１５】

ステップＳ５１１では、認証結果と一時特徴量データの顔画像をユーザに確認させるべ

く、表示する。認証レベルが“中”の場合、一時特徴量データを使ってイベントの検出を行うこと、また、その特徴量データを管理サーバに記録することを確認させる。認証レベルが“低”の場合、認証がうまくいかなかったこと、一時特徴量データを使ってイベントの検出を行えるよう管理者に承認してもらえるよう通知することを確認させる。

【０１１６】

具体的には、図１６に示す画面を表示することで、ユーザに確認させる。そして、ユーザからの確認結果を受け付ける。

【０１１７】

ステップＳ５１２では、ステップＳ５１１においてユーザから受け付けた確認結果が“ＯＫ”の場合、ステップＳ５１３に遷移する。

【０１１８】

確認結果がＯＫの場合とは、認証レベルが中の場合は、一時特徴量データを使ってイベントの検出を行うこと、また、その特徴量データを管理サーバに記録することに対して承認する旨の結果を受け付けた場合である。認証レベルが低の場合は、認証がうまくいかなかったこと、一時特徴量データを使ってイベントの検出を行えるよう管理者に承認してもらえるよう通知することについて承認する旨の結果を受け付けた場合である。

【０１１９】

確認結果として再認証をする旨を受け付けた場合は、処理をＳ５０２に遷移して再度顔認証を行う。

【０１２０】

確認結果としてキャンセルする旨を受け付けた場合、処理をステップＳ５１０に遷移する。

【０１２１】

ステップＳ５１３では、ステップＳ５０８で算出した一時特徴量データを証跡管理サーバ１２０に登録する。この処理の詳細は図６のフローチャートを用いて説明する。

【０１２２】

ステップＳ５１４では、一時特徴量データの認証レベルが“中”の場合ステップＳ５１５に遷移し、“低”の場合ステップＳ５１０に遷移する。

【０１２３】

ステップＳ５１５では、イベントの検出を行う際に使用する特徴量データとして、ステップＳ５０８で算出した一時特徴量データをＲＡＭ２０２に記憶する。なお、イベント検出において複数の識別子の登録を許可するのであれば、一時特徴量データに加えてすべての認証特徴量データを使用するように設定してもかまわない。

【０１２４】

このように、一時特徴量データをイベント検出に用いることで、過去に取得した認証特徴量データをイベント検出に使うよりも認証精度がよくなり、“着席”および“なりすまし”などのイベントを精度よく検出できるようになる。

【０１２５】

ステップＳ５１６では、ステップＳ５０１で行ったユーザ操作のロックを解除する。そして本フローチャートの処理を終了する。

【０１２６】

個人認証処理においてユーザが操作する画面の一例を図１６に示す。

【０１２７】

図１６（Ａ）は、ステップＳ５０１において証跡送信端末１００の表示部に表示される画面の一例である。

【０１２８】

図１６（Ｂ）は、ステップＳ５０９において認証レベルが高であると判断された場合に、証跡送信端末１００の表示部に表示される画面の一例である。

【０１２９】

図１６（Ｃ）は、ステップＳ５０９において認証レベルが低であると判断された場合に

、証跡送信端末１００の表示部に表示される画面の一例である。図１６（Ｃ）にあるように、ＯＫボタン、キャンセルボタン、再認証ボタンが含まれ、ユーザにより押下されたボタンに応じて、ステップＳ５１２の処理（判定）が行われる。

【０１３０】

図１６（Ｄ）は、ステップＳ５０９において認証レベルが中であると判断された場合に、証跡送信端末１００の表示部に表示される画面の一例である。図１６（Ｄ）も図１６（Ｃ）と同様にＯＫボタン、キャンセルボタン、再認証ボタンが含まれ、ユーザにより押下されたボタンに応じて、ステップＳ５１２の処理（判定）が行われる。

【０１３１】

次に図６を参照して、図５のステップＳ５１２の一時特徴量データの登録およびその承認処理の詳細について説明する。

【０１３２】

図６のフローチャートで示す処理のうち証跡送信端末１００の処理は、証跡送信端末１００のＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムをＲＡＭ２０２に記憶することで実行される。また証跡監査端末１１０の処理は、証跡監査端末１１０のＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムをＲＡＭ２０２に記憶することで実行される。また証跡管理サーバ１２０の処理は、証跡管理サーバ１２０のＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムをＲＡＭ２０２に記憶することで実行される。

【０１３３】

ステップＳ６０１では、証跡送信端末１００が、ステップＳ５０８で算出した一時特徴量データを証跡管理サーバ１２０に送信する。同時に、特徴量データ記憶部１０４にその一時特徴量データを記憶する。

【０１３４】

ステップＳ６０２では、証跡管理サーバ１２０が、証跡送信端末１００が送信した一時特徴量データを受信し、特徴量データ記憶部１２２に記憶する。そして、証跡送信端末１００と証跡管理サーバ１２０は非同期に動作し、証跡送信端末１００は、個人認証処理（図５）のステップＳ５１４の処理に遷移し、証跡管理サーバ１２０はステップＳ６０３の処理に遷移する。証跡送信端末１００の処理（Ｓ５１４以降）については、上述の通りである。

【０１３５】

ステップＳ６０３では、証跡管理サーバ１２０が、一時特徴量データ１００のテレワーカＩＤに対応するテレワーカの管理者の情報（図８）をアカウント記憶部１２８から取得する。そして、その管理者の証跡監査端末１１０に、新しく登録された一時特徴量データの承認依頼通知を送信する。代表的な送信手段としては、電子メールがあげられるが、いずれの方法であってもよい。送信後、証跡管理サーバ１２０は新たな命令があるまで待機する。

【０１３６】

ステップＳ６０４では、証跡監査端末１１０が、証跡管理サーバ１２０から送信された承認依頼通知を受信する。

【０１３７】

ステップＳ６０５では、証跡監査端末１１０は、表示部に図１７に示す画面を表示し、証跡管理サーバ１２０上の一時特徴量データ（図１１）の顔画像を管理者に確認させ、管理者による承認操作を受け付ける。

【０１３８】

管理者が、表示部に表示された顔画像の持ち主がテレワーカ本人であると判断し、一時特徴量データによるイベント検出を認める場合（すなわち、管理者から承認する旨の指示を受け付けた場合）、承認状況を“承認”に変更する。

【０１３９】

管理者が、顔画像の持ち主がテレワーカ本人であるが、イベント検出に使用することは

認められないと判断した場合（すなわち、承認をキャンセルする旨の指示を受け付けた場合）、承認状況を“差戻し”に変更する。

【０１４０】

管理者が、顔画像の持ち主がテレワーカ以外の第三者であると判断した場合（すなわち、管理者から否認する旨の指示を受け付けた場合）、承認状況を“否認”に変更する。

【０１４１】

管理者が、顔画像の持ち主がテレワーカ本人であると判断し、今後個人認証で使用する認証特徴量データとして当該顔画像を登録する場合、承認状況を“承認”に変更し、識別子（図１０）の指定を受け付ける。識別子を指定する際、既存の識別子だけでなく、新しい識別子を指定することもできる。既存の識別子を指定する際、その識別子が設定された他の特徴量データの識別子をクリアして、編集中の特徴量データのみをその識別子の認証特徴量データとすることもできる。特徴量データの更新においてユーザが操作する画面の一例を図１７に示す。

【０１４２】

ここで図１７に示す画面について説明する。

【０１４３】

図１７（Ａ）は、ステップＳ６０４において証跡監査端末１１０の表示部に表示される画面である。管理者により承認状況が「登録」となっているデータが選択されると、図１７（Ｂ）に示す画面が表示される。

【０１４４】

図１７（Ｂ）の画面では、管理者から（Ａ）の画面で選択された特徴量データを承認するか（イベント検出に用いる特徴量データとして承認するか）の指示を受け付ける。

【０１４５】

承認する旨の指示を受け付けると、図１７（Ｃ）に示す画面を表示する。図１７（Ｃ）に示す画面においては、認証用の特徴量データとして使うことを承認するかの指示を受け付ける。

【０１４６】

認証用の特徴量データとして使うことを承認する旨の指示がなされると、図１７（Ｄ）に示す画面を表示し、識別子の選択を受け付ける。

【０１４７】

識別子の選択を受け付け、ＯＫボタンが押下されると、図１７（Ｅ）に示す画面を表示する。

【０１４８】

図１７（Ｅ）に示す画面は、識別子に対応付ける特徴量データの設定をする画面である。

【０１４９】

以上が図１７に示す画面の説明である。

【０１５０】

ステップＳ６０６では、証跡管理サーバ１２０が、ステップＳ６０５において受け付けた管理者による承認操作に従い、特徴量データを更新する。

【０１５１】

ステップＳ６０７では、証跡送信端末１００が、証跡管理サーバ１２０によるステップＳ６０６での一時特徴量データの更新に応じて、特徴量データ記憶部１０４に記憶された、対応する一時特徴量データを更新する。すなわち、証跡管理サーバ１２０に記憶されたデータと証跡送信端末１００に記憶されたデータとを同期する処理である。

【０１５２】

なお、ステップＳ６０６で更新された一時特徴量データが特徴量データ記憶部１０４になかった場合、その情報を証跡管理サーバ１２０から取得する。また、ステップＳ６０６で更新されたものが認証特徴量データであった場合も、その特徴量データの更新を行う。

【０１５３】

ステップＳ６０８では、一時特徴量データの承認状況を判断する。
【０１５４】
承認状況が「差し戻し」である場合は、処理をステップＳ６０９に移行する。
【０１５５】
承認状況が「否認」である場合は、処理をステップＳ６１０に移行する。
【０１５６】
承認状況が「承認」である場合は、処理をステップＳ６１１に移行する。
【０１５７】
ステップＳ６０９では、証跡送信端末１００が、一時特徴量データが差戻されたことを受け、再度ステップＳ４０２と同様の個人認証処理を行いイベント検出に使用する特徴量データの決定を行う。
【０１５８】
ステップＳ６１０では、証跡送信端末１００が、一時特徴量データが否認されたことを受け、情報端末の画面ロック等の処理を行う。すなわち、管理者により一時特徴量データにおける顔画像がテレワーカ本人の顔画像ではないと判断されたことになるため、画面ロックなどを行うことで、テレワーカ本人以外による証跡送信端末の操作などを防ぎセキュリティ対策を行う。
【０１５９】
なお、ここで実行される画面ロック等の処理は、画面ロックでなくとも、エラー音を鳴らすなどの警告を通知したり、カメラ映像を動画として保存したりするなどのセキュリティ対策を行うことを想定している。画面ロックの解除の詳細な内容説明については本発明の趣旨から外れるため省略する。
【０１６０】
ステップＳ６１１では、変更された一時特徴量データの認証レベルが“低”の場合（ステップＳ６１１：ＴＲＵＥ）はステップＳ６１２に遷移してイベント検出に使用する特徴量データを、当該一時特徴量データで更新を行う。すなわち、ステップＳ５１０の処理で設定された内容を更新する。
【０１６１】
認証レベルが“中”の場合（ステップＳ６１１：ＦＡＬＳＥ）は、既に承認された一時特徴量データでイベントの検出を行っている（ステップＳ５１５）ので処理を終了する。
【０１６２】
ステップＳ６１２では、証跡送信端末１００が、イベント検出に使用する特徴量データを、ステップＳ５１０で設定した認証特徴量データから当日に取得した一時特徴量データに更新する。なお、イベント検出において複数の識別子の登録を許可するのであれば、使用中の認証特徴量データに加えて一時特徴量データを使用するように設定してもかまわない。
【０１６３】
これにより、認証特徴量データを使用していた状態に比べてなりすましが起こりにくい状態になる。
【０１６４】
以下、図７を参照して、図４のステップＳ４０３のイベント検出の詳細について説明する。この処理は、証跡送信端末１００のＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムをＲＡＭ２０２に記憶することで実行される。ステップＳ７０１－ステップＳ７０９のイベント検出処理と、ステップＳ７１０－ステップＳ７１３の証跡送信処理は非同期で動作する。この処理は、すべてバックエンドで実行され、ユーザ操作を介さない。
【０１６５】
まず、ステップＳ７０１－ステップＳ７０９のイベント検出処理について説明する。
【０１６６】
ステップＳ７０１では、アプリケーションの終了命令があるか確認し、なければ（ステップＳ７０１：ＮＯ）ステップＳ７０２に遷移する。アプリケーションの終了命令がある

場合（ステップＳ７０１：ＹＥＳ）は、本フローチャートの処理を終了し、処理をステップＳ４０４に移行する。

【０１６７】

ステップＳ７０２では、カメラデバイス２１０からフレーム（画像）の入力を受け付け、その情報（図１２）をＲＡＭ２０２に記憶する。

【０１６８】

ステップＳ７０７でイベントを検出する際には所定の件数（Ｍ件）のフレームの顔検出および顔識別結果を利用するため、ＲＡＭ２０２にフレームがＭ件記憶されていたら、最も古いフレームと、それに関連づいた顔検出結果および顔識別結果をＲＡＭ２０２から消去する。

【０１６９】

ステップＳ７０３では、ステップＳ７０２で取得したフレームに対して顔検出を行う。得られた顔検出結果（図１３）は、ＲＡＭ２０２に記憶する。

【０１７０】

ステップＳ７０４－ステップＳ７０６では、ステップＳ７０３で検出された顔に対して顔識別を行う。完了したらステップＳ７０７に遷移する。

【０１７１】

ステップＳ７０５では、ステップＳ７０３で得られた顔検出結果をもとにフレームから一つの顔画像を取得し、その顔画像に対して個人認証処理（図４）で算出したイベント検出に使う特徴量データ（の特徴量）を学習させた識別器を使って顔識別を行う。得られた顔識別結果（図１４）はＲＡＭ２０２に記憶する。同じ識別子に関連付けられる特徴量データが複数ある場合は、それらを同じ識別対象として識別器に学習させる。複数の識別子が存在する場合、それらを別の識別対象として学習させる。ここでいう識別対象とは、対象がテレワーカ本人であることは同じなのだが、メガネや化粧の有無、業務を実行する環境の違い（による照明環境やカメラと顔の位置関係など）など、テレワーカの業務環境をカテゴライズしたものとなる。

【０１７２】

ステップＳ７０７では、ＲＡＭ２０２に記憶された複数のフレームの顔検出結果および顔識別結果から、現在のイベント（着席、離席、なりすまし、覗き込み）を算出し、証跡をＲＡＭ２０２に記憶する。

【０１７３】

単純な例としては、複数のフレームについて、各フレームの顔検出結果の数を調べ、検出された顔の数が０件のフレームが最も多い場合は“離席”（顔が映っていない時間が長いといえるため、離席していると判断）、顔の数が２件のフレームが最も多い場合“覗き込み”（顔を２つ以上検知しているため、覗き込みされていると判断）とする。

【０１７４】

また、顔検出数が１件のフレームが最も多い場合、顔識別結果の類似度が一定値以上のフレーム数と一定値未満のフレーム数を調べ、前者が多い場合“着席”（テレワーカ本人だけが映っている）、後者が多い場合“なりすまし”（テレワーカ以外の人物だけが映っている）とする。

【０１７５】

この算出方法は顔検出および顔識別の結果の精度および傾向によりどのように設定してもよい。また、イベントの発生傾向を学習させた識別器によって判定させてもよい。

【０１７６】

ステップＳ７０８では、ステップＳ７０７で算出した証跡のイベントと、直前に検出された証跡のイベントが同じ値（すなわち、状況に変化がない場合）であればステップＳ７０１に遷移し、異なる場合（すなわち、状況に変化があった、何らかのイベントが発生した場合）は、ステップＳ７０９に遷移する。

【０１７７】

ステップＳ７０９では、証跡を証跡記憶部１０８に記憶し、ステップＳ７０１に遷移す

る。
【０１７８】
続いて、ステップＳ７１０－ステップＳ７１３の証跡送信処理について説明する。
【０１７９】
ステップＳ７１０では、アプリケーションの終了命令があるか確認し、なければ（ステップＳ７１０：ＮＯ）ステップＳ７１１に遷移する。アプリケーションの終了命令がある場合（ステップＳ７１０：ＹＥＳ）は、本フローチャートの処理を終了し、処理をステップＳ４０４に移行する。
【０１８０】
ステップＳ７１１では、証跡記憶部１０８に記憶された最新の証跡を確認し、証跡の送信条件が満たされているか判定する。
【０１８１】
送信条件の一例としては、最新の証跡が最後に送信した証跡のイベントと異なり、証跡の検出日時から一定時間経過していたらその証跡の送信が必要であるとし、ＲＡＭ２０２に記憶する。一定時間経過していなければ、送信不要と判定する。
【０１８２】
この経過時間は、顔認識の精度によって、イベント毎に設定する。たとえば、なりすましを誤検出しやすく、覗き込みを高精度に検出できるのであれば、なりすましを３０秒間検出した場合になりすましイベントの証跡を送信し、覗き込みを５秒間検出した場合に覗き込みイベントの証跡を送信する、といったように、イベントによってその証跡を送信するまでの時間を異ならせて設定する。
【０１８３】
なお、最後に送信した証跡はＲＡＭ２０２に記憶されており、初期値は“離席”となっている。これにより、本人が着席しているが“なりすまし”や“離席”が頻繁に誤検出されてしまう場合にも、そのあとすぐに“着席”を検出できればそれまでに起きたイベントはノイズとして管理サーバに送信、記憶されることがなくなる。
【０１８４】
ステップＳ７１２では、最後に証跡を送信したあとに検出された証跡の履歴から、送るべき証跡があるかどうか判定する。
【０１８５】
たとえば、“なりすまし”と“離席”が短期間（たとえば１秒ごと）に交互に複数回以上発生している場合、“なりすまし”が発生していると推定できる（１秒間の間に離席と着席とを繰り返すのは不自然であるため、離席の検知は誤検知であると考えられ、なりすましが続いていると判断できる）ので、その初回の“なりすまし”のイベントを送信が必要と判断し、ＲＡＭ２０２に記憶する。
【０１８６】
また、離席イベントと離席イベントの間に“なりすまし”が発生した場合、第三者がテレワーカの離席中にちょっと覗き込んですぐ去っていったものと推定できるので、証跡を送信が必要であるとし、ＲＡＭ２０２に記憶する。
【０１８７】
ステップＳ７１２のように証跡の履歴から送信の要否を判断することで、ステップＳ７１１で見逃された送信が必要な証跡を掘り起すことができる。
【０１８８】
ステップＳ７１３では、ステップＳ７１１およびステップＳ７１２で送信が必要と判断した証跡を管理サーバ１２０に送信する。この際、検出日時の新しい証跡を最後に送信した証跡としてＲＡＭ２０２に記憶する。
【０１８９】
以上のように、図７のフローチャートで示す処理は、アプリケーションが終了するまで継続して実行される処理である。
【０１９０】

図８－１５は、本実施形態のテレワーク管理システムにおけるデータテーブルの一例を示すデータ構成図である。

【０１９１】

図８は、管理者情報が登録されたデータテーブルの一例を示す図であり、管理者の情報（ＩＤ、名前、メールアドレス等）が格納されている。

【０１９２】

図９は、テレワーカ情報が登録されたデータテーブルの一例を示す図であり、テレワーカＩＤ、テレワーカの名前、テレワーカのメールアドレス、当該テレワーカに対応する管理者のＩＤなどの情報が格納されている。ここに登録された管理者に対して、一時特徴量データの承認依頼などが通知される（Ｓ５１３）。

【０１９３】

図１０は、識別子情報が登録されたデータテーブルの一例を示す図であり、テレワーカＩＤと識別ＩＤと名前などの情報が格納されている。図１０の例では、テレワーカＩＤが「１」のテレワーカには、２種類の認証用特徴量データが登録されていることを示している。

【０１９４】

図１１は、特徴量データが登録されたデータテーブルの一例を示す図である。図１１の例では、テレワーカＩＤ「１」のテレワーカの特徴量データが４つ登録されている。特徴量データＩＤ「１」とＩＤ「２」とＩＤ「３」の特徴量データについては、管理者による承認がなされている。また、ＩＤ「１」とＩＤ「２」の特徴量データについては、識別ＩＤが登録されているため、認証用特徴量データとして個人認証に用いられているものである。

【０１９５】

図１２は、フレーム情報が登録されたデータテーブルの一例を示す図である。本テーブルは、ステップＳ５０３やＳ７０２の処理において登録されるデータである。フレームＩＤ、画像、大きさ、取得日時などのデータから構成される。

【０１９６】

図１３は、顔検出結果が登録されたデータテーブルの一例を示す図である。図１２に登録された各フレームから検出された顔の情報が登録される。

【０１９７】

図１４は、顔識別結果が登録されたデータテーブルの一例を示す図である。

【０１９８】

図１５は、証跡情報が登録されたデータテーブルの一例を示す図である。ステップＳ７０９において登録されるデータである。検出日時、証跡画像、イベント内容などにより構成されている。

【０１９９】

図１８は、認証レベルを求めるための第１の閾値、第２の閾値が登録されたデータテーブルの一例を示す図である。

【０２００】

図１６、図１７は、本実施形態のテレワーク管理システムにおけるユーザが操作する画面の一例を示す画面イメージである。

【０２０１】

以上のように、本発明においては、テレワークを開始する際に撮影された顔画像とあらかじめ管理者により承認された認証用の顔画像との類似度が高い場合（類似度が第１の閾値よりも高い場合）、すなわち本実施形態における認証レベルが高の場合は、当該認証用の顔画像を用いてイベントを検出する。これにより、管理者はテレワーカがテレワークを開始する度に、本人であるかの判断をする必要がなくなり、管理者の負担を低減させることが可能となる。また、テレワーカにとっても、管理者に対して承認依頼を出す必要がなく、負担が低減される。

【０２０２】

テレワークを開始する際に撮影された顔画像とあらかじめ管理者により承認された認証用の顔画像との類似度が中程度（類似度が第１の閾値よりも低く、第２の閾値よりも高い場合）、すなわち本実施形態における認証レベルが中の場合は、当該テレワーク開始時に撮影された顔画像を用いてイベント検出を行う。また、テレワーク開始時に撮影された顔画像を管理者に確認させ、当該顔画像を引き続きイベント検出に用いるかの指示を受け付ける。また、今後の認証用の顔画像として、当該テレワーク開始時に撮影した顔画像を用いるかの選択を受け付け、今後の認証用に当該顔画像を用いる旨の指示があった場合は、当該顔画像を認証用の顔画像として登録する。

【０２０３】

このように、類似度が中程度の場合にはテレワーカ本人である可能性は一定程度あるため、テレワーク開始時に撮影された顔画像によりイベント検出を行うことで、なりすましの誤検出を低減させることが可能となる。また、当該テレワーク開始時に撮影された顔画像を管理者に確認させ、引き続きイベント検出に用いても良いかの選択を受け付けることで、仮にテレワーカ本人でなかった場合におけるセキュリティインシデントの影響を小さく抑えることが可能となる。

【０２０４】

また、管理者がテレワーカ本人であり認証用に用いてよいと判断した場合は、当該テレワーク開始時に撮影された顔画像を認証用の顔画像にすることで、年月の経過による顔の変化に対応した認証用顔画像を登録することが可能となる。

【０２０５】

テレワークを開始する際に撮影された顔画像とあらかじめ管理者により承認された認証用の顔画像との類似度が低い（類似度が第２の閾値よりも低い場合）、すなわち本実施形態における認証レベルが低の場合は、認証用の顔画像を用いてイベント検出を行う。またテレワーク開始時に撮影された顔画像を管理者に確認させ、イベント検出に用いる顔画像として承認を得られた場合は、当該テレワーク開始時に撮影された顔画像をイベント検出に用いる。また、今後の認証用に当該顔画像を用いる旨の指示があった場合は、当該顔画像を認証用の顔画像として登録する。

【０２０６】

このように、類似度が低い場合にはテレワーカ本人である可能性は低いため、まずは認証用の顔画像でイベントを検知することで、セキュリティインシデント等の影響を小さく抑えることが可能となる。また、管理者による承認があった場合には当該テレワーク開始時に撮影された顔画像によりイベント検出を行うことで、誤検出による利便性低下を抑えることが可能となる。

【０２０７】

また、管理者がテレワーカ本人であり認証用に用いて良いと判断した場合は、当該テレワーク開始時に撮影された顔画像を認証用の顔画像にすることで、年月の経過による顔の変化に対応した認証用顔画像を登録することが可能となる。

【０２０８】

なお、上述した各種データの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な構成や内容で構成されることは言うまでもない。

【０２０９】

また、本発明におけるプログラムは、図４～図７の処理をコンピュータに実行させるプログラムである。なお、本発明におけるプログラムは、図４～図７の各処理ごとのプログラムであってもよい。

【０２１０】

以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムを読み出し、実行することによっても本発明の目的が達成されることは言うまでもない。

【０２１１】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記録した記録媒体は本発明を構成することになる。

【０２１２】

プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク等を用いることが出来る。

【０２１３】

また、コンピュータが読み出したプログラムを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２１４】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２１５】

また、本発明は、複数の機器から構成されるシステムに適用しても、ひとつの機器から成る装置に適用しても良い。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０２１６】

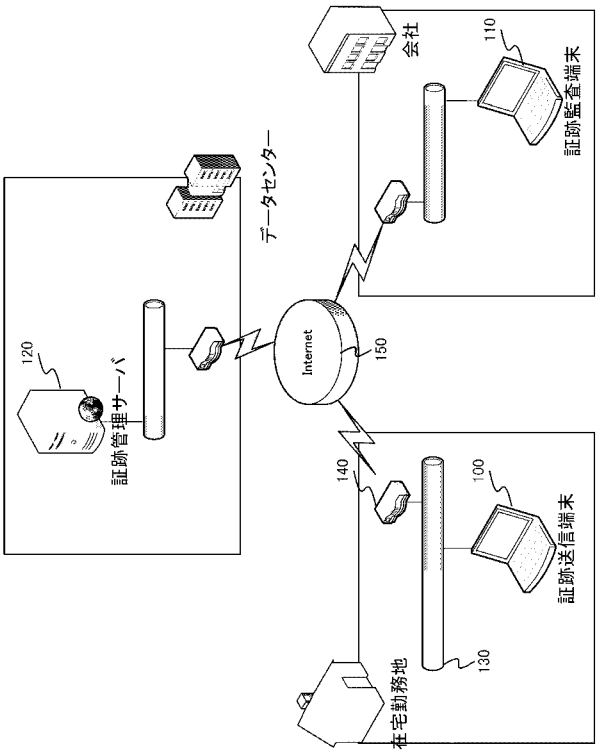
さらに、本発明を達成するためのプログラムをネットワーク上のサーバ、データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【符号の説明】

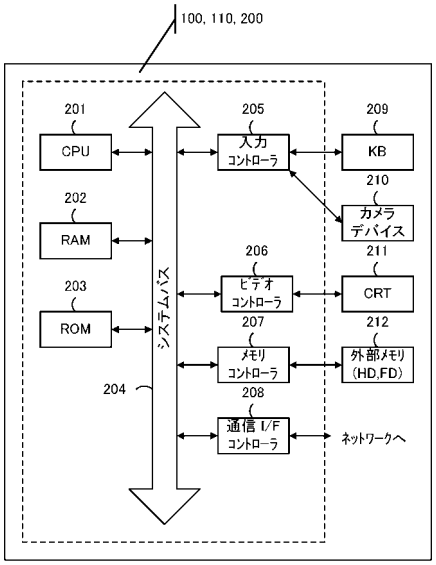
【０２１７】

１００　証跡送信端末
１１０　証跡監査端末
１２０　証跡管理サーバ

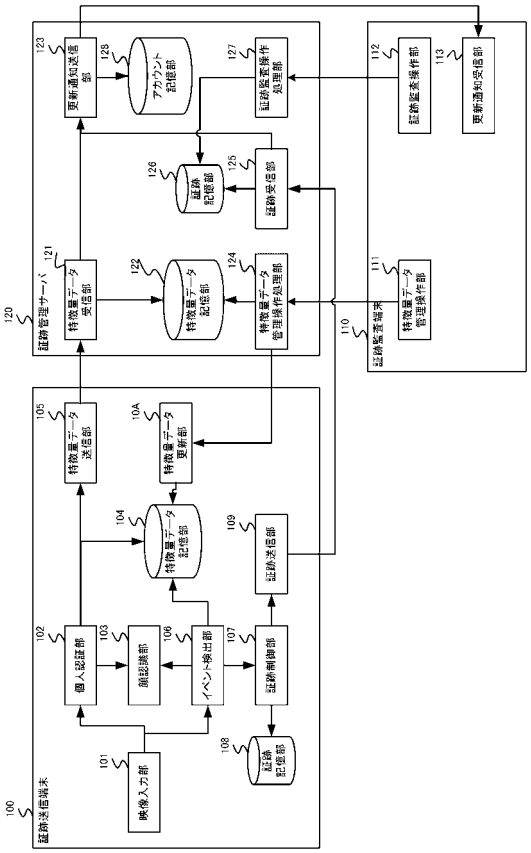
【図１】


会社
110
証跡監査端末
データセンター
120
証跡管理サーバ
Internet
150
140
100
証跡送信端末
130
在宅勤務地

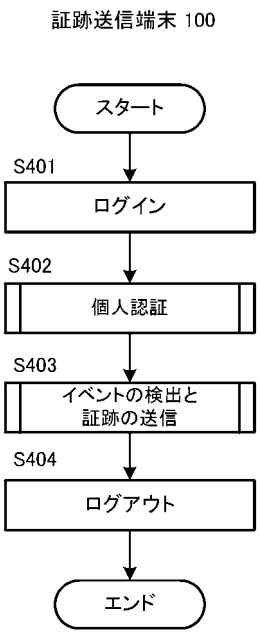
【図２】


100, 110, 200
201
CPU
202
RAM
203
ROM
204
システムバス
205
入力コントローラ
206
ビデオコントローラ
207
メモリコントローラ
208
通信 I/F コントローラ
209
KB
210
カメラデバイス
211
CRT
212
外部メモリ (HD,FD)
ネットワークへ

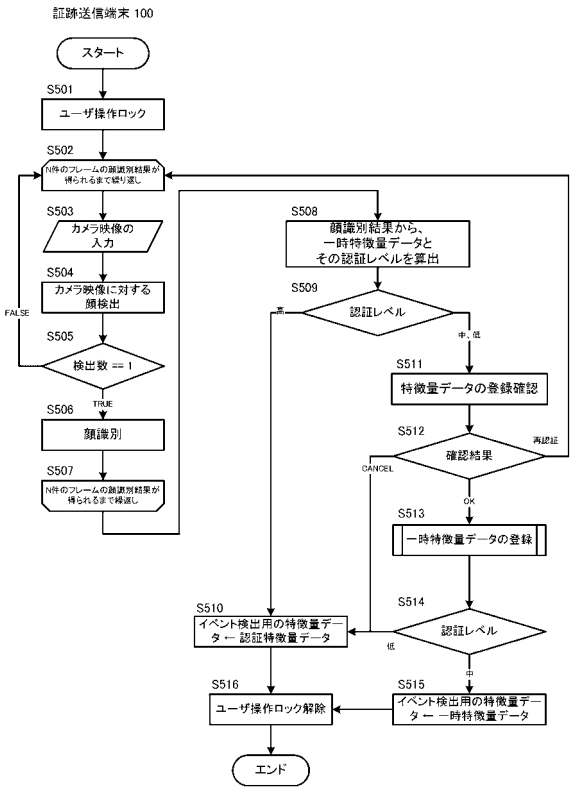
【図３】


証跡送信端末
証跡管理サーバ
証跡監査端末
映像入力部
個人認証部
顔認識部
イベント検出部
証跡制御部
特徴量データ送信部
特徴量データ更新部
特徴量データ記憶部
証跡送信部
証跡記憶部
特徴量データ受信部
特徴量データ記憶部
特徴量データ管理操作処理部
更新通知送信部
アカウント記憶部
証跡監査操作処理部
証跡受信部
証跡記憶部
特徴量データ管理操作部
証跡監査操作部
更新通知受信部

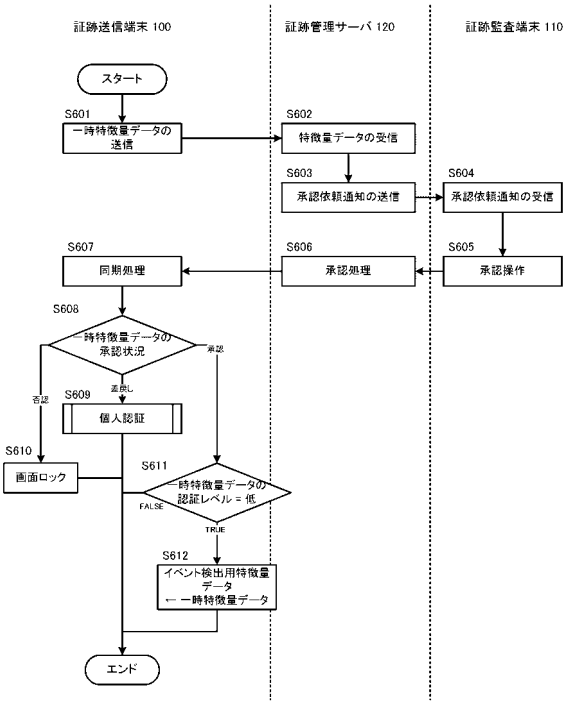
【図４】


証跡送信端末 100
スタート
S401
ログイン
S402
個人認証
S403
イベントの検出と証跡の送信
S404
ログアウト
エンド

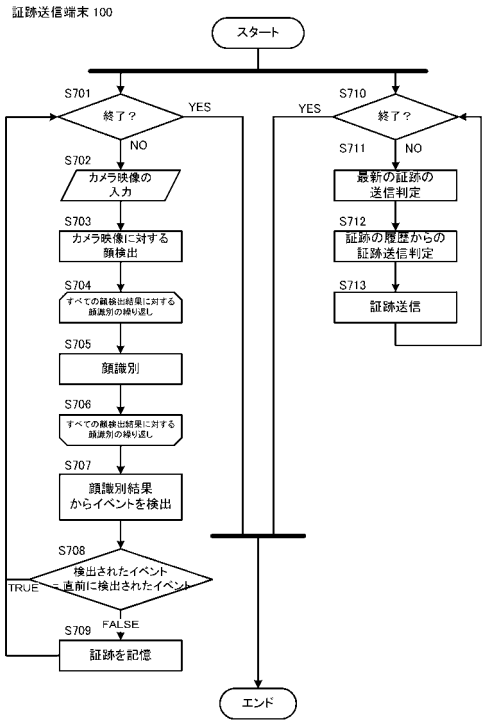
【図５】



【図６】



【図７】



【図８】

この図は公序良俗違反のため不掲載とする

【図９】

この図は公序良俗違反のため不掲載とする

【図１０】

テレワーカID	1	1
識別ID	1	2
名前	標準	メガネ

【図１１】

テレワーカID	1	1	1	1
特徴量データID	1	2	3	4
顔画像	…	…	…	…
特徴量	…	…	…	…
承認状況	承認	承認	承認	登録
認証レベル	中	低	中	中
識別ID	1	2		
登録日時	2013／04／02 08:55:43	2013／04／03 08:55:43	2013／04／09 08:55:43	2013／04／10 08:55:43
承認日時	2013／04／02 09:05:12	2013／04／03 09:05:12	2013／04／09 09:05:12	

【図１２】

フレームID	1	2	3	4
画像	…	…	…	…
大きさ	640,480	640,480	640,480	640,480
取得日時	2013／04／10 08:55:20	2013／04／10 08:55:25	2013／04／10 08:55:30	2013／04／10 08:55:35

【図１３】

フレームID	1	2	3	4
顔検出ID	1	2	3	4
位置	234,123	234,123	440,222	234,123
大きさ	120,150	120,150	10,20	120,150
傾き	0	0	30	0

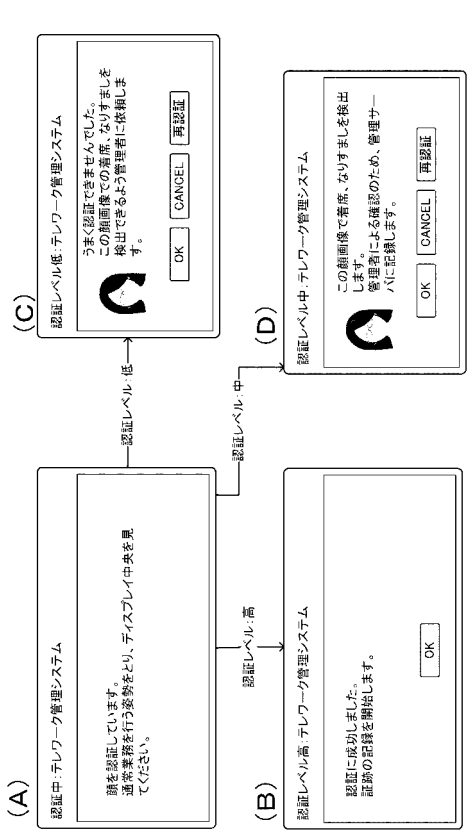
【図１４】

顔検出ID	1	1	4	4
識別ID	1	2	7	8
類似度	0.85	0.8	0.84	0.79

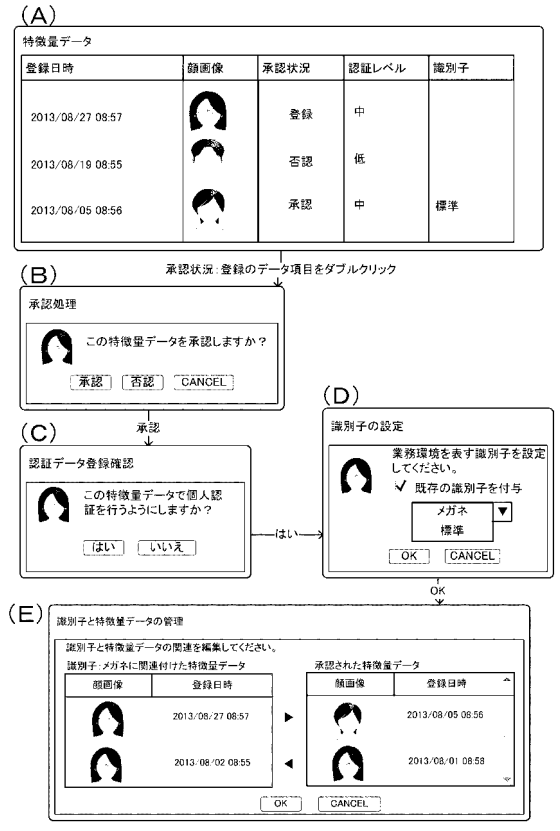
【図１５】

テレワークID	1	1	1	1
証跡ID	1	2	3	4
証跡画像	…	…	…	…
イベント	着席	誰き込み	着席	着席
検出日時	2013/04/10 08:55:50	2013/04/10 11:43:54	2013/04/10 11:50:32	2013/04/10 12:04:42

【図１６】



【図１７】



【図１８】

第1の閾値	0.8
第2の閾値	0.7