

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4829343号
(P4829343)

(45) 発行日 平成23年12月7日(2011.12.7)

(24) 登録日 平成23年9月22日(2011.9.22)

(51) Int.Cl.	F I
G06F 21/24 (2006.01)	G06F 12/14 520F
G06F 3/048 (2006.01)	G06F 12/14 520A
	G06F 12/14 560Z
	G06F 3/048 656A

請求項の数 8 (全 22 頁)

(21) 出願番号	特願2009-508736 (P2009-508736)	(73) 特許権者	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番1号
(86) (22) 出願日	平成19年3月16日(2007.3.16)	(74) 代理人	100101856 弁理士 赤澤 日出夫
(86) 国際出願番号	PCT/JP2007/055357	(72) 発明者	辻 健太郎 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(87) 国際公開番号	W02008/126185	(72) 発明者	瀬川 英吾 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(87) 国際公開日	平成20年10月23日(2008.10.23)	審査官	圓道 浩史
審査請求日	平成21年6月24日(2009.6.24)		

最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理プログラム、情報処理方法

(57) 【特許請求の範囲】

【請求項1】

情報を表示することができる表示装置の制御を行う情報処理装置であって、
前記表示装置を含む作業スペースに存在する人を検出し、前記検出された人と前記表示装置との位置関係を取得する位置関係取得部と、
前記作業スペース内に設置された認証装置を用いて、記憶部に予め記憶された人の認証情報に基づいて人を認証する認証部と、
前記位置関係と前記表示装置に表示させる表示態様との対応関係を保持し、前記認証部により人が認証された場合、前記記憶部に予め記憶された前記認証された人がアクセス可能な表示情報の種類を示す情報を取得し、前記認証された時点且つ前記認証装置の設置位置において前記位置関係取得部により検出された人である対象者と前記取得された情報とを対応付け、前記取得された情報と前記表示装置に表示される表示情報の種類を示す情報とを比較し、前記表示装置に表示される表示情報の種類が前記取得された情報に示される種類に含まれない場合、前記対応関係と前記位置関係とに基づいて前記表示装置に表示させる表示態様を制御する制御部と
を備える情報処理装置。

【請求項2】

請求項1に記載の情報処理装置において、
前記対応関係は、前記位置関係の範囲と前記表示装置に表示させる表示態様との対応付けを含み、

前記制御部は、前記表示装置に表示される表示情報の種類が前記取得された情報に含まれない場合、且つ、前記対象者に関する位置関係が所定の第1範囲内である場合、前記対象者の存在を前記表示装置に表示させることを特徴とする情報処理装置。

【請求項3】

請求項2に記載の情報処理装置において、

前記制御部は、前記対象者に関する位置関係が前記第1範囲と異なる第2範囲内である場合、前記表示装置における表示を中断させることを特徴とする情報処理装置。

【請求項4】

請求項1または請求項2に記載の情報処理装置において、

前記制御部は、前記表示装置に表示される表示情報の種類が前記取得された情報に示される種類に含まれない場合、前記対象者を前記表示情報へのアクセス権を持たない人と判断し、前記表示装置に表示される表示情報の種類が前記取得された情報に示される種類に含まれる場合、前記対象者を前記表示情報へのアクセス権を持つ人と判断し、

前記位置関係取得部は、検出された人のうち前記表示情報へのアクセス権を持たない人と前記表示情報へのアクセス権を持つ人と前記表示装置との位置関係を取得し、

前記対応関係は、該位置関係と前記表示情報が表示される前記表示装置上の位置との関係を含み、

前記制御部は、前記表示情報が前記表示情報へのアクセス権を持たない人から見て前記表示情報へのアクセス権を持つ人に遮られるように、前記表示情報の少なくとも位置を制御することを特徴とする情報処理装置。

【請求項5】

請求項1乃至請求項4のいずれかに記載の情報処理装置において、

前記位置関係は、前記位置関係取得部により検出された人と前記表示装置との距離を含み、

前記対応関係は、前記距離と前記表示装置に表示させる表示情報の大きさとの関係を含み、

前記制御部は、前記表示装置に表示される表示情報の種類が前記取得された情報に示される種類に含まれない場合、前記対象者に関する前記距離が小さくなるほど、前記表示装置に表示させる表示情報の大きさを小さくすることを特徴とする情報処理装置。

【請求項6】

請求項1乃至請求項4のいずれかに記載の情報処理装置において、

前記位置関係は、前記位置関係取得部により検出された人と前記表示装置との距離を含み、

前記対応関係は、前記距離と前記表示装置に表示させる表示情報のコントラストとの関係を含み、

前記制御部は、前記表示装置に表示される表示情報の種類が前記取得された情報に示される種類に含まれない場合、前記対象者に関する前記距離が小さくなるほど、前記表示装置に表示させる表示情報のコントラストを低くすることを特徴とする情報処理装置。

【請求項7】

情報を表示することができる表示装置の制御をコンピュータに実行させる情報処理プログラムであって、

前記表示装置を含む作業スペースに存在する人を検出し、前記検出された人と前記表示装置との位置関係を取得し、

前記作業スペース内に設置された認証装置を用いて、記憶部に予め記憶された人の認証情報に基づいて人を認証し、

前記位置関係と前記表示装置に表示させる表示態様との対応関係を保持し、

前記認証することにより人が認証された場合、前記記憶部に予め記憶された前記認証された人がアクセス可能な表示情報の種類を示す情報を取得し、前記認証された時点且つ前記認証装置の設置位置において前記位置関係を取得することにより検出された人である対象者と前記取得された情報とを対応付け、前記取得された情報と前記表示装置に表示され

10

20

30

40

50

る表示情報の種類を示す情報とを比較し、前記表示装置に表示される表示情報の種類が前記取得された情報に示される種類に含まれない場合、前記対応関係と前記位置関係とに基づいて前記表示装置に表示させる表示態様を制御する

ことをコンピュータに実行させる情報処理プログラム。

【請求項 8】

情報を表示することができる表示装置の制御を行う情報処理方法であって、

前記表示装置を含む作業スペースに存在する人を検出し、前記検出された人と前記表示装置との位置関係を取得し、

前記作業スペース内に設置された認証装置を用いて、記憶部に予め記憶された人の認証情報に基づいて人を認証し、

前記位置関係と前記表示装置に表示させる表示態様との対応関係を保持し、

前記認証することにより人が認証された場合、前記記憶部に予め記憶された前記認証された人がアクセス可能な表示情報の種類を示す情報を取得し、前記認証された時点且つ前記認証装置の設置位置において前記位置関係を取得することにより検出された人である対象者と前記取得された情報とを対応付け、前記取得された情報と前記表示装置に表示される表示情報の種類を示す情報とを比較し、前記表示装置に表示される表示情報の種類が前記取得された情報に示される種類に含まれない場合、前記対応関係と前記位置関係とに基づいて前記表示装置に表示させる表示態様を制御する

ことを行う情報処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報を表示することができる表示装置の制御を行う情報処理装置、情報処理プログラム、情報処理方法に関するものである。

【背景技術】

【0002】

PC (Personal Computer) 等、サービスを提供する端末において、パスワード、指紋、虹彩、静脈等を用いて、利用者の認証を行うことにより、権限のある利用者のみがサービスを利用できるようにする仕組みが広く普及している。

【0003】

また、サービスを提供する端末の周辺に複数の人がいる場合、利用者の後ろや隣にいる利用権限のない人がモニタに表示された情報を見ることができないようにするための技術がある (例えば、特許文献 1 参照)。この技術によれば、サービスを利用可能な範囲に存在する人をカメラやRFID (Radio Frequency Identification) 等で検出し、さらに顔認証等により各人を識別し、アクセスが許可された人以外が存在する場合は、サービス提供の中断や中止等の制御を行うことにより、セキュリティを高めることができる。

【0004】

同様に、情報表示装置の前にいる人を検出して情報表示を行うかどうかを判断するものがある (例えば、特許文献 2 参照)。この技術は、情報表示装置の操作者に向けてカメラを設置し、その映像中に事前に登録されていない顔が検出された場合、表示を中断するものである。これにより、登録されていない人が情報を覗いた場合にも、情報漏洩を防ぐことができる。

【0005】

これに対して、情報の正規利用者の作業効率を考慮した技術がある (例えば、特許文献 3 参照)。この技術は、液晶ディスプレイの前面に液晶のシャッターを設置することによって、液晶ディスプレイを見る方向ごとに、異なった映像を提示するものである。これにより、正規利用者のいる方向にのみ情報を表示することで、アクセス権がない人への情報漏えいを防ぐことができる。

【0006】

また、本発明に関連のある従来技術として、カメラを用いて撮影した画像上の物体を検

10

20

30

40

50

出する技術がある（例えば、特許文献4）。また、レーザスキャナを用いて歩行者を抽出する技術がある（例えば、非特許文献1参照）。また、逆投影法とカルマンフィルタを用いて移動物体の位置を追跡する技術がある（例えば、非特許文献2参照）。また、最小可読文字サイズを推定するための規格がある（例えば、非特許文献3参照）。

【特許文献1】特開平9-297735号公報

【特許文献2】特開2005-346307号公報

【特許文献3】特開2005-107306号公報

【特許文献4】特開2006-302115号公報

【非特許文献1】中村克行，“マルチレーザスキャナを用いた歩行者トラッキング，”電子情報通信学会論文誌 D-I I, vol. J88-D-I I, no. 7, pp. 1143-1152, 2005年7月。

10

【非特許文献2】早坂光晴，富永英義，小宮一三：“逆投影法とカルマンフィルタを用いた複数移動物体位置認識とその追跡，”PRMU2001-132, pp. 133-138, 2001年11月。

【非特許文献3】JIS S0032「高齢者・障害者配慮設計指針-視覚表示物-日本語文字の最小可読文字サイズ推定方法」

【発明の開示】

【発明が解決しようとする課題】

【0007】

しかしながら、特許文献1の技術のように、サービスの提供が可能な範囲のみを監視したのでは、サービスの利用権限のない人がその範囲に侵入した場合、侵入した人を検出した後で情報提供の制御が行われるため、侵入から制御までの間に情報が漏洩する可能性がある。また、人がRFID等の特殊な装置を携帯することを前提にすると、装置を持たない人を検出できないため、これらの人から情報漏えいの危険がある。また、特許文献2の技術では、登録されていない人が検出されると急に情報が表示されなくなるため、情報の利用者は準備する時間もなく突然作業の中断を余儀なくされ、作業効率が低下する。また、特許文献3の技術では、構造上、情報の正規利用者と近い視線方向からの覗き見は防止することができず、セキュリティが高いとは言えない。

20

【0008】

本発明は上述した問題点を解決するためになされたものであり、表示装置に表示される情報の漏洩を防止する情報処理装置、情報処理プログラム、情報処理方法を提供することを目的とする。

30

【課題を解決するための手段】

【0009】

上述した課題を解決するため、本発明は、情報を表示することができる表示装置の制御を行う情報処理装置であって、前記表示装置の周辺における所定のエリアに存在する人の検出を行い、該人と前記表示装置との位置関係を取得する位置関係取得部と、前記位置関係と前記表示装置に表示させる表示態様との対応関係を保持し、前記対応関係と前記位置関係取得部により取得された位置関係とに基づいて前記表示装置に表示させる表示態様を制御する制御部とを備える。

40

【0010】

また、本発明は、情報を表示することができる表示装置の制御をコンピュータに実行させる情報処理プログラムであって、前記表示装置の周辺における所定のエリアに存在する人の検出を行い、該人と前記表示装置との位置関係を取得する位置関係取得ステップと、前記位置関係と前記表示装置に表示させる表示態様との対応関係を保持し、前記対応関係と前記位置関係取得部により取得された位置関係とに基づいて前記表示装置に表示させる表示態様を制御する制御ステップとをコンピュータに実行させる。

【0011】

また、本発明は、情報を表示することができる表示装置の制御を行う情報処理方法であって、前記表示装置の周辺における所定のエリアに存在する人の検出を行い、該人と前記

50

表示装置との位置関係を取得する位置関係取得ステップと、前記位置関係と前記表示装置に表示させる表示態様との対応関係を保持し、前記対応関係と前記位置関係取得部により取得された位置関係とに基づいて前記表示装置に表示させる表示態様を制御する制御ステップとを実行する。

【図面の簡単な説明】

【0012】

【図1】実施の形態1に係る情報表示システムの構成の一例を示すブロック図である。

【図2】実施の形態1に係るサーバ及びアクセス端末の構成の一例を示すブロック図である。

【図3】実施の形態1に係る位置管理テーブルの一例を示す表である。

10

【図4】実施の形態1に係る予測時間管理テーブルの一例を示す表である。

【図5】実施の形態1に係るIDアクセス権管理テーブルの一例を示す表である。

【図6】実施の形態1に係る作業内容アクセス権管理テーブルの一例を示す表である。

【図7】実施の形態1に係るエリア管理テーブルの一例を示す表である。

【図8】実施の形態1に係る情報表示システムの動作の一例を示すフローチャートである。

【図9】実施の形態2に係る情報表示システムの構成の一例を示すブロック図である。

【図10】実施の形態2に係るサーバ及びアクセス端末の構成の一例を示すブロック図である。

【図11】実施の形態2に係る情報表示システムの別の構成の一例を示すブロック図である。

20

【図12】実施の形態3に係る情報表示システムの構成の一例を示すブロック図である。

【図13】実施の形態3に係るコンピュータの構成の一例を示すブロック図である。

【図14】実施の形態3に係るコンピュータによる検出処理の一例を示すフローチャートである。

【図15】実施の形態3に係るコンピュータによる表示処理の一例を示すフローチャートである。

【図16】実施の形態3に係る表示情報変更処理の一例を示す概念図である。

【図17】実施の形態3に係る表示文字サイズ選択テーブルの第1の例を示す表である。

【図18】実施の形態3に係る表示文字サイズ選択テーブルの第2の例を示す表である。

30

【図19】実施の形態3に係る表示文字サイズ選択テーブルの第3の例を示す表である。

【図20】実施の形態3に係る表示情報変更処理の第1の例を示す画面である。

【図21】実施の形態3に係る表示情報変更処理の第2の例を示す画面である。

【図22】実施の形態4に係る表示情報変更処理の一例を示す概念図である。

【図23】実施の形態4に係る表示コントラスト強度選択テーブルの第1の例を示す表である。

【図24】実施の形態4に係る表示コントラスト強度選択テーブルの第2の例を示す表である。

【図25】実施の形態4に係る表示コントラスト強度選択テーブルの第3の例を示す表である。

40

【図26】実施の形態4に係る表示情報変更処理の第1の例を示す画面である。

【図27】実施の形態4に係る表示情報変更処理の第2の例を示す画面である。

【図28】実施の形態5に係る表示情報変更処理の一例を示す概念図である。

【図29】実施の形態5に係る表示情報変更処理の一例を示すフローチャートである。

【発明を実施するための最良の形態】

【0013】

以下、本発明の実施の形態について図面を参照しつつ説明する。

【0014】

実施の形態1.

ここでは、本発明の情報処理装置を適用した情報表示システムの例について説明する。

50

また、本実施の形態に係る情報表示システムは、認証装置を有する。

【0015】

まず、本実施の形態に係る情報表示システムの構成について説明する。

【0016】

図1は、本実施の形態に係る情報表示システムの構成の一例を示すブロック図である。この情報表示システムは、サーバ(情報処理装置)101、アクセス端末(表示装置)102、一つまたは複数のカメラ103、認証装置104を備える。アクセス端末102は、利用者の操作に従って、文字、画像、音等の表示を行う。エリアAは、侵入者がアクセス端末102に表示された情報を見ることが出来るエリア、あるいは侵入者がアクセス端末102を操作できるエリアである。エリアBは、エリアAの外側である。エリアBの大きさは、侵入者がエリアBに入ってからエリアAに入るまでの時間に、アクセス端末102の利用者が作業の中断等の情報漏洩防止の処理を完了できるように決定される。

10

【0017】

カメラ103は、アクセス端末102を含む作業スペース(所定のエリア)を撮影し、連続する複数の画像を出力する。作業スペースは例えば、アクセス端末102が置かれた部屋全体である。認証装置104は作業スペースである部屋への入口等、作業スペース内に設置され、例えば、指紋照合等の生体認証により、認証動作を行った人が誰であるか認証する。なお、カメラ103とは別の認証装置104を設けず、カメラ103が人の顔を撮影することにより、サーバ101が顔認証を行い、人の認証を行っても良い。

【0018】

20

図2は、本実施の形態に係るサーバ及びアクセス端末の構成の一例を示すブロック図である。サーバ101は、位置検出部111、位置予測部112、アクセス制御部113を備える。アクセス端末102は、モニタやスピーカなどの表示部121、キーボードやマウスなどの入力部122を備える。

【0019】

位置検出部111は、カメラにより撮影された画像により作業スペースに入った人を検出する。位置検出部111は、例えば、特許文献3の技術を用いて画像から人を検出する。更に、位置検出部111は、予め画像内の位置と作業スペース内の位置とを対応付けておくことにより、作業スペースにおける人の位置を検出する。

【0020】

30

また、認証装置104で認証動作をした人が同定されると、位置検出部111は、同時に認証装置104の設置された位置に検出した人を認証済みの人として記録する。また、位置検出部111は、認証装置104で同定されなかった人、あるいは、認証動作をしていない人については、未認証の人として記録する。位置検出部111は、認証済の人については予め登録されているIDを、未認証の人については他の互いに異なるIDをそれぞれ割り当てる。

【0021】

位置予測部112は、位置管理テーブル、予測時間管理テーブル、IDアクセス権管理テーブル、作業内容アクセス権管理テーブル、エリア管理テーブルを管理する。図3は、本実施の形態に係る位置管理テーブルの一例を示す表である。位置予測部112は、位置検出部111により検出された人のIDと位置を取得し、この位置管理テーブルを用いて、人毎に、ID、現在の位置、所定時間(T秒)前の位置、予測時間(N秒)後の予測位置を管理する。また、位置検出部111は、現在の人の全身や一部の画像を過去の画像と対応付けることにより、人の位置の履歴を記録する。ここでは、T秒前の位置と現在の位置が記録される。ここで、位置検出部111は、例えば、2つの画像間の濃淡値の正規化相関を用いて最も相関値が高くなる部分を同一の部分(人)として対応付ける。

40

【0022】

図4は、本実施の形態に係る予測時間管理テーブルの一例を示す表である。想定される作業内容(表示情報の種類)毎に予測時間が設定され、予めこの予測時間管理テーブルに保持される。位置予測部112は、アクセス制御部113からアクセス端末102にお

50

る利用者の現在の作業内容を取得し、作業内容と予測時間管理テーブルにより、予測時間を決定する。

【0023】

位置予測部112は、上述した位置管理テーブルにおけるT秒前の位置と現在の位置からN秒後の位置を予測する。なお、位置検出部111は、より多くの過去の位置を記録しても良く、位置予測部112は、それらの位置を用いてN秒後の位置を予測しても良い。ここで、位置予測部112は例えば、人の過去から現在までの時間と位置との関係を一次式の関数で近似し、この関数により所定の予測時間後の人の位置を予測し、予測位置とする。なお、位置予測部112は、人の動きをモデル化しておき、モデルに基づいて位置の予測を行ってもよい。例えば、位置予測部112は、人の動きを等速運動でモデル化して

10

【0024】

図5は、本実施の形態に係るIDアクセス権管理テーブルの一例を示す表である。登録されているID毎にアクセス権(レベル)が設定され、予めこのIDアクセス権管理テーブルに保持される。図6は、本実施の形態に係る作業内容アクセス権管理テーブルの一例を示す表である。想定される作業内容毎に必要なアクセス権(レベル)が設定され、予めこの作業内容アクセス権管理テーブルに保持される。位置予測部112は、アクセス端末102における利用者の現在の作業内容と作業内容アクセス権テーブルにより、作業内容に必要なアクセス権を決定する。また、位置予測部112は、位置管理テーブルで管理された人のIDとIDアクセス権テーブルにより、人のアクセス権を決定する。また、位置

20

【0025】

また、位置予測部112は、作業内容(アクセス端末102により出力される情報の機密の度合い)に応じて、予測時間、エリアA及びエリアBの大きさを変更する。作業内容としては、例えば、動作させているアプリケーションの種類や数、作業開始からの経過時間、作業を開始してから追加あるいは変更されたデータの量がある。図7は、本実施の形態に係るエリア管理テーブルの一例を示す表である。想定される作業内容毎にエリアAの

30

【0026】

なお、予測時間、エリアA及びエリアBの大きさは、利用者が警報後に作業の中断等、情報漏洩防止のための必要な操作に要する時間を考慮して、予め固定値として設定されても良い。また、位置予測部112は、警報発報時の作業内容に応じてこれらの値を変更しても良い。情報漏洩防止のための必要な操作とは、作業内容を保存する操作やウィンドウを閉じる操作等が含まれる。

【0027】

位置予測部112は、侵入者の予測位置がエリアBの内部であれば、アクセス端末102に警告を発する。さらに、位置予測部112が予測した侵入者の予測位置がエリアAの内部であれば、アクセス端末102に作業の中断を指示する。アクセス制御部113から警告が発せられると、アクセス端末102は、表示部121により、人が近づいていることを文字、画像、音、振動等を用いて利用者に知らせる。また、アクセス制御部113から中断の指示が出された場合は、アクセス端末102は、表示部121における出力の中断、入力部122における入力

40

【0028】

このとき、アクセス端末102は、利用者に対してアクセスの中断の可否を問い合わせるようにしても良い。ここで、利用者がアクセスの中断をしないことを選択すると、アクセス端末102は、アクセスの中断を行わず、アクセス端末102は利用者の判断でアク

50

セスを継続したことを記録し、同時にその時点での状況を記録するために作業スペースを撮影したカメラの画像を保存する。この画像は、アクセスの権限の無い人を特定するための解析等に用いることができる。

【 0 0 2 9 】

次に、本実施の形態に係る情報表示システムの動作について説明する。

【 0 0 3 0 】

図8は、本実施の形態に係る情報表示システムの動作の一例を示すフローチャートである。まず、利用者がアクセス端末102の利用を開始すると(S11)、位置予測部112は、アクセス制御部113からアクセス端末102における利用者の現在の作業内容を取得する(S12)。次に、位置予測部112は、利用者の作業内容とエリア管理テーブルとによりエリアA及びエリアBの大きさを決定し、作業内容と予測時間管理テーブルとにより予測時間を決定する(S13)。次に、位置予測部112は、IDアクセス権管理テーブルにより作業スペース内にいる人のアクセス権を取得する(S14)。次に、位置予測部112は、アクセス権のない人を侵入者とし、侵入者の予測時間後の位置である予測位置(位置関係)を算出する(S15)。

10

【 0 0 3 1 】

次に、位置予測部112は、予測位置がエリアAの内部であるか(アクセス端末102から予測位置までの距離がエリアAの半径以内であるか)否かの判断を行う(S21)。エリアAの内部でなければ(S21, N)、処理S23へ移行し、エリアAの内部であれば(S21, Y)、アクセス制御部113は、アクセス端末102へ作業の中断を指示し、指示を受けたアクセス端末102は、利用者の作業(アクセス)を中断し(対応関係)(S22)、処理S25へ移行する。ここで、アクセス制御部113から作業の中断の指示を受けたアクセス端末102は、表示部121による出力を中断する、入力部122による入力を中断する等の処理を行う。

20

【 0 0 3 2 】

このとき、アクセス端末102は、利用者に対してアクセスの中断の可否を問い合わせるようにしても良い。この場合、利用者がアクセスの中断をしないことを選択すると、アクセス端末102は、以後、対象となった侵入者が接近してもアクセスの中断を行わず、アクセス制御部113は利用者の判断でアクセスを継続したことを記録し、同時にその時点での状況を記録するために作業スペースを撮影したカメラの画像を保存する。

30

【 0 0 3 3 】

次に、位置予測部112は、予測位置がエリアBの内部であるか(アクセス端末102から予測位置までの距離がエリアBの半径以内であるか)否かの判断を行う(S23)。エリアBの内部でなければ(S23, N)、処理S25へ移行し、エリアBの内部であれば(S23, Y)、アクセス制御部113は、アクセス端末102へ警告を発生し(対応関係)、警告を受けたアクセス端末102の出力部131は、利用者へ侵入者の接近を通知し(S24)、処理S25へ移行する。ここで、表示部121は、アクセス権を持たない人が近づいていることを文字、画像、音声、音、振動等を用いて利用者に知らせる。

【 0 0 3 4 】

次に、アクセス制御部113は、利用者がアクセス端末102の利用を終了したか否かの判断を行い(S25)、終了していない場合(S25, N)、処理S12へ戻り、終了した場合(S25, Y)、このフローは終了する。

40

【 0 0 3 5 】

なお、本実施の形態においては、予測位置算出の結果予測位置算出の結果、侵入者の位置が通知処理では間に合わない位置にある場合の危険性を考慮し、アクセス中断を行うエリアAの内部であるか否かから確認したが、作業スペースや認証装置の設置条件によっては、通知処理を行うエリアBから確認するようにしてもよい。

【 0 0 3 6 】

本実施の形態によれば、アクセス権を持たない人または未認証の人の位置を追跡し、位置を予測することにより、その人がアクセス端末102にアクセス可能になるまでに作業

50

を中断させることができ、覗き見等による情報漏洩の危険性を低下できる。また、その人がアクセス端末 102 にアクセス可能になる前に、情報漏洩が生じる可能性がある状況を事前に利用者に知らせ、利用者が適切な準備をするための時間を確保することにより、利便性を向上することができる。

【0037】

実施の形態 2 .

ここでは、本発明の情報処理装置を適用した情報表示システムの例について説明する。また、本実施の形態に係る情報表示システムは、認証装置を必要としない。

【0038】

まず、本実施の形態に係る情報表示システムの構成について説明する。

10

【0039】

図9は、本実施の形態に係る情報表示システムの構成の一例を示すブロック図である。この図において、図1と同一符号は図1に示された対象と同一又は相当物を示しており、ここでの説明を省略する。図1と比較するとこの図は、サーバ101の代わりにサーバ201を備え、認証装置104を必要としない。

【0040】

図10は、本実施の形態に係るサーバ及びアクセス端末の構成の一例を示すブロック図である。この図において、図2と同一符号は図2に示された対象と同一又は相当物を示しており、ここでの説明を省略する。サーバ101と比較するとサーバ201は、位置検出部111の代わりに位置検出部211を備え、位置予測部112の代わりに位置予測部212を備える。

20

【0041】

位置検出部211は、位置検出部111と同様、カメラ103により撮影された画像により作業スペースに入った人を検出する。更に、位置検出部211は、予め画像内の位置と作業スペース内の位置とを対応付けておくことにより、作業スペースにおける人の位置を検出する。また、位置検出部211は、予め設定されたアクセス端末102の位置からアクセス端末102の利用者を検出する。更に、位置検出部211は、利用者以外の検出された全ての人を侵入者として扱い、それぞれ異なるIDを割り当てる。

【0042】

位置予測部212は、位置予測部112と同様に侵入者の位置である予測位置を算出し、予測位置と作業内容とエリア管理テーブルにより、警告や中断の判断を行う。本実施の形態においては、利用者以外の検出された全ての人を侵入者として扱うため、IDアクセス権管理テーブル及び作業内容アクセス権管理テーブルは不要であり、位置予測部212は、全ての侵入者の予測位置を算出し、全ての侵入者の予測位置についてエリアA及びエリアBに入ったか否かの判断を行う。以降、実施の形態1と同様、アクセス制御部113は、この判断の結果に基づいて、作業の中断や警告を行う。

30

【0043】

なお、カメラの代わりにレーザスキャナを用いて人の位置を検出しても良い。

【0044】

図11は、本実施の形態に係る情報表示システムの別の構成の一例を示すブロック図である。この図において、図9と同一符号は図9に示された対象と同一又は相当物を示しており、ここでの説明を省略する。図9と比較するとこの図は、カメラ103の代わりに一つまたは複数のレーザスキャナ105を備える。レーザスキャナ105は、アクセス端末102を含む作業スペースを計測する。位置検出部211は、レーザスキャナ105の計測データから作業スペースへの人を検出する。位置検出部211は、例えば、非特許文献1の技術を用いてレーザスキャナ105の計測データから人の位置を検出する。

40

【0045】

本実施の形態によれば、作業スペースに入った人の認証を不要とすることができる。

【0046】

実施の形態 3 .

50

ここでは、本発明の情報処理装置を適用した情報表示システムの例について説明する。本実施の形態に係る情報表示システムは、不正利用者の位置（位置関係）に応じて表示情報のサイズ（表示態様）を制御する。

【0047】

図12は、本実施の形態に係る情報表示システムの構成の一例を示すブロック図である。この情報表示システムはPCなどのコンピュータ（情報処理装置）301を有し、コンピュータ301からの情報を表示するためのディスプレイ（表示装置）302、コンピュータ301への各種入力のためのキーボード303およびマウス304、認証を行うための認証装置305、そして、コンピュータ301の周辺にいる人の位置を把握するためのカメラ306が、コンピュータ301に接続されている。

10

【0048】

カメラ306は、コンピュータ301の周辺を撮影するように設置される。なお、カメラ306は、例えばレーザーセンサやRFIDリーダなど人の位置を検出できるものであれば代用可能である。

【0049】

図13は、本実施の形態に係るコンピュータの構成の一例を示すブロック図である。コンピュータ301は、認証情報データベース321、表示情報データベース322を備える。認証情報データベース321は利用者のID、名前、認証用情報、情報の閲覧権限など、利用者認証処理を行うための情報が登録されたものである。表示情報データベース322は、ディスプレイ302において閲覧される表示情報ごとに、ファイル名、表示情報を閲覧するために必要なアクセス権や表示情報の機密度などが登録されたものである。

20

【0050】

更に、コンピュータ301は、カメラ306によって得られた画像から人を検出し、その人の位置の追跡を行う位置検出部311、認証情報データベース321に基づいて認証を行う認証部312、認証部312による認証結果と位置検出部311により検出された人の位置に応じて表示情報を変化させるか否かの判定を行う表示情報変更判定部313、表示情報の変更を行い、表示情報をディスプレイ302へ表示させる表示情報変更部314を備える。

【0051】

次に、コンピュータ301による検出処理について説明する。

30

【0052】

図14は、本実施の形態に係るコンピュータによる検出処理の一例を示すフローチャートである。

【0053】

まず、位置検出部311は、カメラ306により撮影された画像からディスプレイ302周辺の監視範囲（作業スペース）にいる人の位置を検出する（S31）。例えば、複数のカメラを用いて人の位置を認識する方法としては、非特許文献2のように逆投影法とカルマンフィルタを用いる方法がある。また、レーザー光を使う方法としては、例えば非特許文献1のようなマルチレーザースキャナを用いて人の足を計測するものがある。

【0054】

40

認証部312は、表示情報の閲覧者およびディスプレイ302周辺の人がコンピュータ301へログインするとき、ディスプレイ302が設置されている部屋への入室のときなど、認証装置305を用いて認証を実行し、人が認証されたか否かの判断を行う（S32）。具体的には、静脈や指紋等の生体認証を用いた認証装置305を利用して認証情報データベース321との照合を行うことにより人を特定し、その人の個人情報を出力する。なお、認証部312がディスプレイ302上に利用者認証用のダイアログを表示し、ユーザとパスワードを用いて認証する方法でも良い。この場合、認証装置305は不要となる。

【0055】

人が認証された場合（S32，Y）、表示情報変更判定部313は、認証部312によ

50

り認証された人のアクセス権を取得し（S 3 3）、認証部 3 1 2 により認証が行われた場所（認証装置 3 0 5 の場所）とその認証が行われた時点で位置検出部 3 1 1 により検出された人の位置と認証部 3 1 2 により認証された人のアクセス権とから、人の位置とアクセス権を対応付け（S 3 5）、このフローは終了する。人が認証されなかった場合（S 3 2, N）、表示情報変更判定部 3 1 3 は、認証が行われていない人を、表示情報へのアクセス権がない人と設定し、位置検出部 3 1 1 により検出された人の位置とアクセス権を対応付け（S 3 5）、このフローは終了する。

【 0 0 5 6 】

次に、コンピュータ 3 0 1 による表示処理について説明する。

【 0 0 5 7 】

図 1 5 は、本実施の形態に係るコンピュータによる表示処理の一例を示すフローチャートである。まず、位置検出部 3 1 1 は、カメラ 3 0 6 により撮影された画像からディスプレイ 3 0 2 周辺の監視範囲（作業スペース）にいる人の位置を検出する（S 4 0）。次に、表示情報変更判定部 3 1 3 は、閲覧者が表示情報を閲覧している際に、その表示情報へのアクセス権を持たない人（不正利用者）が表示情報を見ることができる位置に存在するか否かの判断を行う（S 4 1）。

【 0 0 5 8 】

表示装置付近に存在しない場合（S 4 1, N）、表示情報変更部 3 1 4 は、閲覧者によるキーボード 3 0 3 やマウス 3 0 4 の操作に従って、表示情報を取得し（S 4 2）、ディスプレイ 3 0 2 上に表示し（S 4 4）、このフローは終了する。このとき、表示情報を表示しようとしている人に表示情報を閲覧する権限がない場合、ディスプレイ 3 0 2 に表示情報を表示しない。

【 0 0 5 9 】

表示装置付近に存在する場合（S 4 1, Y）、表示情報変更部 3 1 4 は、不正利用者の位置と予め設定されたディスプレイ 3 0 2 との位置から不正利用者とディスプレイ 3 0 2 との距離を計算し、その距離に応じて表示情報を変更する表示情報変更処理を行い（S 4 3）、表示情報変更処理により加工された表示情報をディスプレイ 3 0 2 に表示し（S 4 4）、このフローは終了する。

【 0 0 6 0 】

以後、閲覧者が表示情報の閲覧を行っている間、表示処理を繰り返す。また、不正利用者がディスプレイ 3 0 2 の表示情報を見ることができない位置へ移動したことを検出した場合、表示情報変更部 3 1 4 は、表示情報変更処理により変更された表示情報を元の表示情報に戻す。

【 0 0 6 1 】

次に、本実施の形態に係る表示情報変更処理について説明する。

【 0 0 6 2 】

図 1 6 は、本実施の形態に係る表示情報変更処理の一例を示す概念図である。X, Y, Z は、それぞれ不正利用者の位置を示す。また、これらの位置に対応して、X から見た表示情報、Y から見た表示情報、Z から見た表示情報を示す。不正利用者が表示情報を見ようとして X から Y へ移動した場合、不正利用者からディスプレイ 3 0 2 までの距離は近くなるが、表示情報の大きさが小さくなるため、不正利用者は表示情報を認識することができない。同様に、不正利用者が Y から Z へ移動した場合、不正利用者からディスプレイ 3 0 2 までの距離は更に近くなるが、表示情報の大きさが更に小さくなるため、不正利用者は表示情報を認識することができない。

【 0 0 6 3 】

表示情報変更処理において、表示情報変更部 3 1 4 は、正規利用者からは見え、不正利用者からは見えないように、表示情報（文字や画像）の大きさを変更してディスプレイ 3 0 2 に表示させる。つまり、不正利用者がディスプレイ 3 0 2 に近づくほど、ディスプレイ 3 0 2 に表示される表示情報の大きさが小さくなることにより、不正利用者は表示情報を認識することができない。

10

20

30

40

50

【 0 0 6 4 】

ディスプレイ 3 0 2 から不正利用者までの距離とディスプレイ 3 0 2 に表示される表示情報の大きさとの関係は、予め表示文字サイズ選択テーブル（対応関係）に設定される。図 1 7 は、本実施の形態に係る表示文字サイズ選択テーブルの第 1 の例を示す表である。この表示文字サイズ選択テーブルによれば、不正利用者に表示情報を見せないようにするため、不正利用者とディスプレイ 3 0 2 との距離（ L_1, L_2, \dots ）が小さくなるほど、表示情報の文字の大きさ（ F_1, F_2, \dots ）が小さくなるように設定されている。文字サイズは、ポイントまたは標準サイズに対する比率で表される。距離と表示文字サイズの関係は、非特許文献 3 のような基準を用いて決定する。表示情報変更部 3 1 4 は、不正利用者距離と表示文字サイズ選択テーブルにより表示文字サイズを決定し、ディスプレイ 3 0 2 により表示される文字サイズを変更する。ここでは、文字サイズの変更のみを示したが、画像やウィンドウ等のサイズも同様にして変更されても良い。これにより、不正利用者が表示情報を認識する可能性を低くすることができる。

10

【 0 0 6 5 】

なお、ディスプレイ 3 0 2 から不正利用者までの距離と、表示情報の機密度と、ディスプレイ 3 0 2 に表示される表示情報の大きさとの関係が、予め表示文字サイズ選択テーブルに設定されても良い。図 1 8 は、本実施の形態に係る表示文字サイズ選択テーブルの第 2 の例を示す表である。表示情報データベース 3 2 2 には、予め表示情報毎に、機密度（必要なアクセス権のレベル）が設定される。この場合の表示文字サイズ選択テーブルによれば、表示情報の機密度（ S_1, S_2, \dots ）が高くなるほど、表示情報の文字の大きさ（ F_{11}, F_{21}, \dots ）が小さくなるように設定される。更に、不正利用者とディスプレイ 3 0 2 との距離（ L_1, L_2, \dots ）が小さくなるほど、表示情報の文字の大きさ（ F_{11}, F_{12}, \dots ）が小さくなるように設定される。これにより、機密度が高いほど不正利用者が表示情報を見る可能性を低くすることができる。

20

【 0 0 6 6 】

また、ディスプレイ 3 0 2 から不正利用者までの距離と、表示情報の機密度と、人毎のアクセス権のレベルと、ディスプレイ 3 0 2 に表示される表示情報の大きさとの関係が、予め表示文字サイズ選択テーブルに設定されても良い。図 1 9 は、本実施の形態に係る表示文字サイズ選択テーブルの第 3 の例を示す表である。この場合の表示文字サイズ選択テーブルによれば、表示文字サイズ選択テーブルの第 2 の例による効果に加え、表示情報の機密度（ S_1, S_2, \dots ）に対してディスプレイ 3 0 2 に近づいた不正利用者のアクセス権のレベル（ a, b, \dots ）が低くなるほど、表示情報の文字の大きさ（ $F_{11-a}, F_{11-b}, \dots$ ）が小さくなるように設定される。これにより表示情報へのアクセス権の無い人が表示情報を見る可能性を低くすることができる。

30

【 0 0 6 7 】

次に、本実施の形態に係る表示情報変更処理の結果について説明する。まず、表示情報変更処理の第 1 の例として、表示情報全体のサイズを小さくする場合について説明する。図 2 0 は、本実施の形態に係る表示情報変更処理の第 1 の例を示す画面である。左の画面は、表示情報変更処理前の表示情報を示す。右の画面は、表示情報変更処理後の表示情報を示す。この表示情報変更処理によれば、表示情報全体の文字サイズが距離に応じて小さくなる。

40

【 0 0 6 8 】

次に、表示情報変更処理の第 2 の例として、特定の種類の情報のサイズを小さくする場合について説明する。図 2 1 は、本実施の形態に係る表示情報変更処理の第 2 の例を示す画面である。左の画面は、表示情報変更処理前の表示情報を示す。右の画面は、表示情報変更処理後の表示情報を示す。この表示情報変更処理によれば、漏洩が許されない個人情報の項目など、予め設定された項目の文字サイズが小さくなる。

【 0 0 6 9 】

また、表示情報データベース 3 2 2 において、名前、住所、電話番号などの項目ごとに異なる機密度を予め設定しておき、項目ごとに異なる比率で表示情報の大きさを変更して

50

も良い。

【 0 0 7 0 】

実施の形態 4 .

ここでは、本発明の情報処理装置を適用した情報表示システムの例について説明する。本実施の形態に係る情報表示システムは、不正利用者の位置に応じて表示情報のコントラスト（表示態様）を制御する。

【 0 0 7 1 】

本実施の形態に係る情報表示システム及びコンピュータの構成は、実施の形態 3 と同様である。また、本実施の形態に係る検出処理及び表示処理は、実施の形態 3 と同様であるが、表示情報変更処理のみが異なる。

【 0 0 7 2 】

次に、本実施の形態に係る表示情報変更処理について説明する。

【 0 0 7 3 】

図 2 2 は、本実施の形態に係る表示情報変更処理の一例を示す概念図である。X , Y , Z は、それぞれ不正利用者の位置を示す。また、これらの位置に対応して、X から見た表示情報、Y から見た表示情報、Z から見た表示情報を示す。不正利用者が表示情報を見ようとして X から Y へ移動した場合、不正利用者からディスプレイ 3 0 2 までの距離は近くなるが、表示情報のコントラストが低くなるため、不正利用者は表示情報を認識することができない。同様に、不正利用者が Y から Z へ移動した場合、不正利用者からディスプレイ 3 0 2 までの距離は更に近くなるが、表示情報のコントラストが更に低くなるため、不正利用者は表示情報を認識することができない。

【 0 0 7 4 】

表示情報変更処理において、表示情報変更部 3 1 4 は、この図のように正規利用者からは見え、不正利用者からは見えないように、表示情報（文字や画像）のコントラストを変更してディスプレイ 3 0 2 に表示させる。つまり、不正利用者がディスプレイ 3 0 2 に近づくほど、ディスプレイ 3 0 2 に表示される表示情報のコントラストが低くなることにより、不正利用者は表示情報を認識することができない。

【 0 0 7 5 】

ディスプレイ 3 0 2 から不正利用者までの距離とディスプレイ 3 0 2 に表示される表示情報のコントラストとの関係は、予め表示コントラスト強度選択テーブル（対応関係）に設定される。図 2 3 は、本実施の形態に係る表示コントラスト強度選択テーブルの第 1 の例を示す表である。この表示コントラスト強度選択テーブルによれば、不正利用者に表示情報を見せないようにするため、不正利用者とディスプレイ 3 0 2 との距離（L 1 , L 2 , ...）が小さくなるほど、表示情報のコントラスト（コントラストの強さ、C 1 , C 2 ...）が低くなるように設定される。コントラストは、階調数または標準のコントラストに対する比率で表される。コントラストが低くなるほど、文字色の輝度は低くなり、背景色の輝度は高くなり、それぞれ所定の中間の輝度に近づく。これにより、不正利用者が表示情報を認識する可能性を低くすることができる。なお、不正利用者とディスプレイ 3 0 2 との距離が小さくなった場合、表示情報変更部 3 1 4 は、表示情報の輝度を低くする、文字色と背景色をより目立たない組み合わせの色に変更する、表示情報への網掛けを増加させる、等の処理を行っても良い。

【 0 0 7 6 】

なお、ディスプレイ 3 0 2 から不正利用者までの距離と、表示情報の機密度と、ディスプレイ 3 0 2 に表示される表示情報のコントラストとの関係が、予め表示コントラスト強度選択テーブルに設定されても良い。図 2 4 は、本実施の形態に係る表示コントラスト強度選択テーブルの第 2 の例を示す表である。表示情報データベース 3 2 2 には、予め表示情報毎に、機密度（必要なアクセス権のレベル）が設定される。この場合の表示コントラスト強度選択テーブルによれば、表示情報の機密度（S 1 , S 2 , ...）が高くなるほど、表示情報のコントラスト（C 1 1 , C 2 1 , ...）が小さくなるように設定される。更に、不正利用者とディスプレイ 3 0 2 との距離（L 1 , L 2 , ...）が小さくなるほど、表示情

10

20

30

40

50

報のコントラスト (C 1 1 , C 1 2 , ...) が低くなるように設定される。これにより、機密度が高いほど、不正利用者が表示情報を見る可能性を低くすることができる。

【 0 0 7 7 】

また、ディスプレイ 3 0 2 から不正利用者までの距離と、表示情報の機密度と、人毎のアクセス権のレベルと、ディスプレイ 3 0 2 に表示される表示情報のコントラストとの関係が、予め表示コントラスト強度選択テーブルに設定されても良い。図 2 5 は、本実施の形態に係る表示コントラスト強度選択テーブルの第 3 の例を示す表である。この場合の表示コントラスト強度選択テーブルによれば、表示コントラスト強度選択テーブルの第 2 の例による効果に加え、表示情報の機密度 (S 1 , S 2 ...) に対してディスプレイ 3 0 2 に近づいた不正利用者のアクセス権のレベル (a , b ...) が低くなるほど、表示情報のコントラスト (C 1 1 - a , C 1 1 - b ...) が低くなるように設定される。これにより表示情報へのアクセス権の無い人が表示情報を見る可能性を低くすることができる。

10

【 0 0 7 8 】

次に、本実施の形態に係る表示情報変更処理の結果について説明する。まず、表示情報変更処理の第 1 の例として、表示情報全体のコントラストを低くする場合について説明する。図 2 6 は、本実施の形態に係る表示情報変更処理の第 1 の例を示す画面である。左の画面は、表示情報変更処理前の表示情報を示す。右の画面は、表示情報変更処理後の表示情報を示す。この表示情報変更処理によれば、表示情報全体のコントラストが距離に応じて低くなる。

【 0 0 7 9 】

20

次に、表示情報変更処理の第 2 の例として、特定の種類の情報のコントラストを低くする場合について説明する。図 2 7 は、本実施の形態に係る表示情報変更処理の第 2 の例を示す画面である。左の画面は、表示情報変更処理前の表示情報を示す。右の画面は、表示情報変更処理後の表示情報を示す。この表示情報変更処理によれば、漏洩が許されない個人情報項目など、予め設定された項目のコントラストが低くなる。

【 0 0 8 0 】

また、表示情報データベース 3 2 2 において、名前、住所、電話番号などの項目ごとに異なる機密度を予め設定しておき、項目ごとに異なる比率で表示情報のコントラストを変更しても良い。

【 0 0 8 1 】

30

上述した実施の形態 3 及び実施の形態 4 によれば、アクセス権の無い人が近づいた場合でも表示の大きさやコントラストが変化しただけであることから、表示情報の正規利用者は、作業を突然中断されることなく、続行することができる。さらに、正規利用者は文字の大きさやコントラストの変化から、ディスプレイと不正利用者との距離を知ることができるため、作業をしながら情報漏洩の危険度を認識することができる。よって、作業効率の低下を防ぎつつ情報の漏洩を防止することが可能となる。

【 0 0 8 2 】

実施の形態 5 .

ここでは、本発明の情報処理装置を適用した情報表示システムの例について説明する。本実施の形態に係る情報表示システムは、不正利用者の位置に応じて表示情報の位置を制御する。

40

【 0 0 8 3 】

本実施の形態に係る情報表示システム及びコンピュータの構成は、実施の形態 3 と同様である。また、本実施の形態に係る検出処理及び表示処理は、実施の形態 3 と同様であるが、表示情報変更処理のみが異なる。

【 0 0 8 4 】

次に、本実施の形態に係る表示情報変更処理について説明する。

【 0 0 8 5 】

図 2 8 は、本実施の形態に係る表示情報変更処理の一例を示す概念図である。この図は、ディスプレイ 3 0 2 の位置、コンピュータ 3 0 1 の正規利用者 (閲覧者) の位置 A、不

50

正利用者（アクセス権がない人）の移動前の位置 B 及び移動後の位置 C を上から見た図である。不正利用者が B にいるとき、表示情報変更部 3 1 4 は、ディスプレイ 3 0 2 上の表示情報のウィンドウの位置を D に設定する。また、不正利用者が C へ移動すると、表示情報変更部 3 1 4 は、ディスプレイ 3 0 2 上の表示情報のウィンドウの位置を E に設定する。

【 0 0 8 6 】

このように、表示情報変更部 3 1 4 は、正規利用者からは見る事ができるが、不正利用者からは見る事ができないような位置に、表示情報のウィンドウの位置を設定する。例えば、表示情報変更部 3 1 4 は、正規利用者と不正利用者とを結んだ直線上に表示情報のウィンドウの位置を設定することにより、不正利用者は正規利用者に遮られて表示情報を見ることができなくなる。

10

【 0 0 8 7 】

図 2 9 は、本実施の形態に係る表示情報変更処理の一例を示すフローチャートである。まず、表示情報変更部 3 1 4 は、位置検出部 3 1 1 により得られた人の位置からその人の頭部の位置を推定する（S 5 1）。次に、表示情報変更部 3 1 4 は、ディスプレイ 3 0 2 の位置と正規利用者の頭部の位置と不正利用者の頭部の位置と（位置関係）から、不正利用者が視認不可能なディスプレイ 3 0 2 上の範囲である視認不可能範囲を計算する（対応関係）（S 5 2）。次に、表示情報変更部 3 1 4 は、表示情報のウィンドウの位置を視認不可能範囲内に設定する（S 5 3）。次に、表示情報変更部 3 1 4 は、表示情報のウィンドウが視認不可能範囲内に収まらないか否かの判断を行い、視認不可能範囲内に収まる場合（S 5 4 , N）、このフローは終了し、視認不可能範囲内に収まらない場合（S 5 4 , Y）、表示情報のウィンドウの大きさが視認不可能範囲内に収まるまで小さくするように変更し（S 5 5）、このフローは終了する。

20

【 0 0 8 8 】

本実施の形態によれば、表示情報の正規利用者は不正利用者が近づいた場合でも、不正利用者の位置によって作業を続けることが可能であり、作業効率の低下を防ぐことができる。

【 0 0 8 9 】

なお、上述した実施の形態 3、実施の形態 4、実施の形態 5 のいずれかを組み合わせた形態も可能である。例えば、表示情報のウィンドウの位置を変化させつつ、表示情報中の文字の大きさも変えるような形態である。このような組み合わせにより、更にセキュリティ性能を高められる。

30

【 0 0 9 0 】

また、上述した実施の形態 1、実施の形態 2、実施の形態 3、実施の形態 4、実施の形態 5 のいずれかを組み合わせた形態も可能である。例えば、侵入者がエリア B に入った場合、侵入者の位置に基づいて表示情報の位置を変更し、侵入者がエリア A に入った場合、作業を中断させるような形態である。このような組み合わせにより、更にセキュリティ性能を高められる。

【 0 0 9 1 】

なお、位置関係取得部は、実施の形態における位置検出部 1 1 1 及び位置予測部 1 1 2、または位置検出部 3 1 1 及び表示情報変更判定部 3 1 3 に対応する。また、制御部は、実施の形態におけるアクセス制御部 1 1 3、または表示情報変更部 3 1 4 に対応する。また、認証部は、実施の形態における認証装置 1 0 4、または認証部 3 1 2 に対応する。

40

【 0 0 9 2 】

また、位置関係取得ステップは、実施の形態における処理 S 1 2 ~ S 1 5、または処理 S 3 1 ~ S 3 5 に対応する。また、制御ステップは、実施の形態における処理 S 2 1 ~ S 2 4、または処理 S 4 3 に対応する。また、認証ステップは、実施の形態における認証装置 1 0 4 の処理、または認証部 3 1 2 の処理に対応する。

【 0 0 9 3 】

更に、情報処理装置を構成するコンピュータにおいて上述した各ステップを実行させる

50

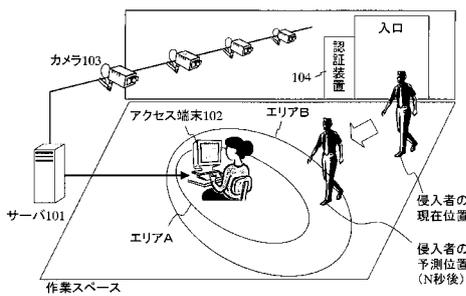
プログラムを、情報処理プログラムとして提供することができる。上述したプログラムは、コンピュータにより読取り可能な記録媒体に記憶させることによって、情報処理装置を構成するコンピュータに実行させることが可能となる。ここで、上記コンピュータにより読取り可能な記録媒体としては、ROMやRAM等のコンピュータに内部実装される内部記憶装置、CD-ROMやフレキシブルディスク、DVDディスク、光磁気ディスク、ICカード等の可搬型記憶媒体や、コンピュータプログラムを保持するデータベース、或いは、他のコンピュータ並びにそのデータベースや、更に回線上の伝送媒体をも含むものである。

【産業上の利用可能性】

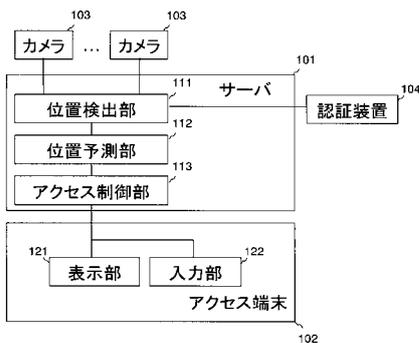
【0094】

以上説明したように、表示装置に表示される情報の漏洩を防止することができる。

【図1】



【図2】



【図3】

ID	現在の位置	T秒前の位置	N秒後の予測位置
001	(X11, Y11, Z11)	(X12, Y12, Z12)	(X13, Y13, Z13)
002	(X21, Y21, Z21)	(X22, Y22, Z22)	(X23, Y23, Z23)
...

【図4】

作業内容	予測時間N
ファイルAの閲覧	T1
ファイルAの編集	T2
ファイルBの閲覧	T3
ファイルBの編集	T4
アプリケーションAの実行	T5
...	...

【図5】

ID	アクセス権
001	レベル1
002	レベル1
003	レベル2
...	...

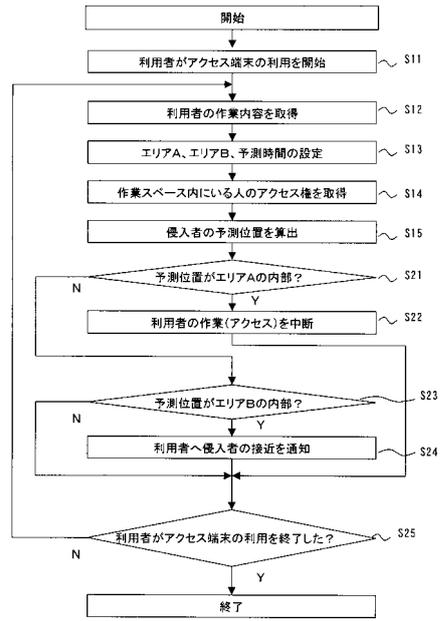
【図6】

作業内容	必要なアクセス権
ファイルAの閲覧	レベル1
ファイルAの編集	レベル2
アプリケーションAの実行	レベル3
...	...

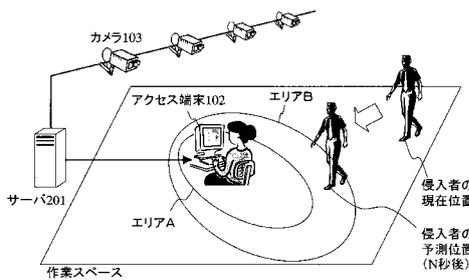
【図7】

作業内容	エリアA	エリアB
ファイルAの閲覧	半径RA1の円	半径RB1の円
ファイルAの編集	半径RA1の円	半径RB1の円
ファイルBの閲覧	半径RA2の円	半径RB2の円
ファイルBの編集	半径RA2の円	半径RB3の円
アプリケーションAの実行	半径RA3の円	半径RB3の円
...

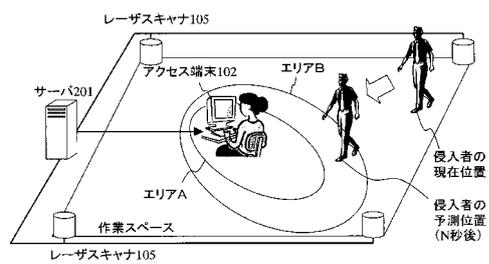
【図8】



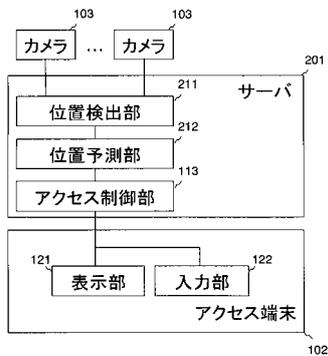
【図9】



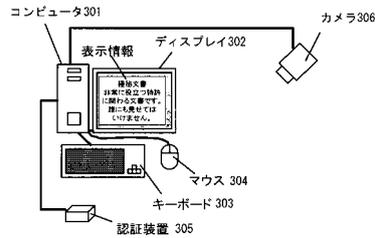
【図11】



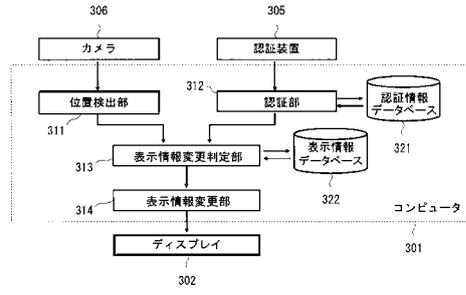
【図10】



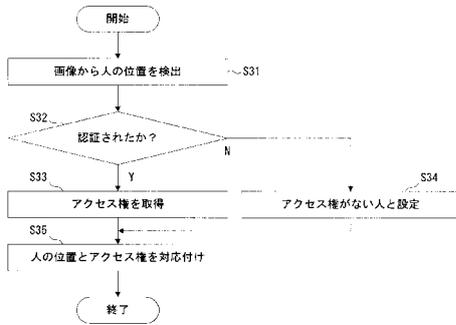
【図12】



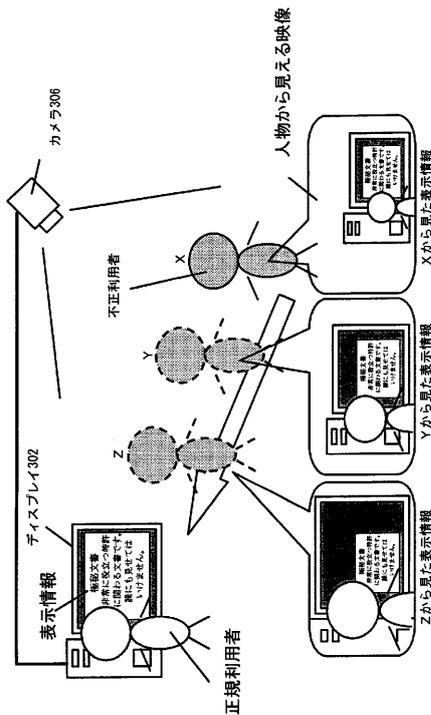
【図13】



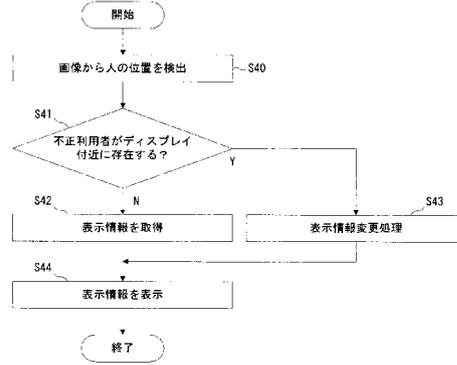
【図14】



【図16】



【図15】



【図17】

距離	L1	L2	L3	...	L9
文字の大きさ	F1	F2	F3	...	F9

距離 $L1 < L2 < L3 \dots < L9$
 文字の大きさ $F1 < F2 < F3 \dots < F9$

【図18】

		距離				
		L1	L2	L3	...	L9
情報の機密度	S1	F11	F12	F13	...	F19
	S2	F21	F22	F23	...	F29
	S3	F31	F32	F33	...	F39
	⋮	⋮	⋮	⋮	⋮	⋮
	S9	F91	F92	F93	...	F99

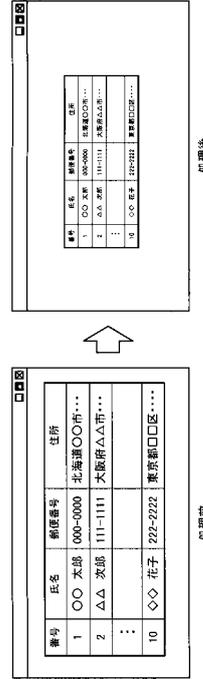
距離 $L1 < L2 < L3 \dots < L9$
 機密度 $S1 < S2 < S3 \dots < S9$
 文字の大きさ $F1x > F2x > F3x \dots > F9x$
 $Fx1 < Fx2 < Fx3 \dots < Fx9$

【図 19】

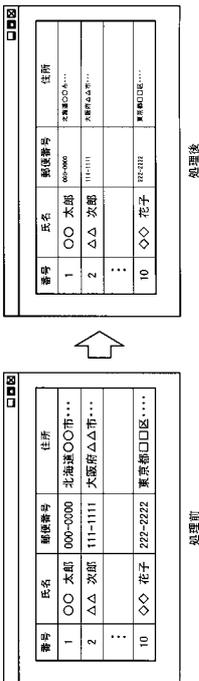
		距離				
		L1	L2	L3	...	L9
S1	F11-a	F12-a	F13-a	...	F19-a	
	F11-b	F12-b	F13-b	...	F19-b	
	F11-c	F12-c	F13-c	...	F19-c	
S2	F21-a	F22-a	F23-a	...	F29-a	
	F21-b	F22-b	F23-b	...	F29-b	
	F21-c	F22-c	F23-c	...	F29-c	
S3	F31-a	F32-a	F33-a	...	F39-a	
	F31-b	F32-b	F33-b	...	F39-b	
	F31-c	F32-c	F33-c	...	F39-c	
...	
S9	F91-a	F92-a	F93-a	...	F99-a	
	F91-b	F92-b	F93-b	...	F99-b	
	F91-c	F92-c	F93-c	...	F99-c	

距離 L1 < L2 < L3 ... < L9
 機密度 S1 < S2 < S3 ... < S9
 文字の大きさ F1x > F2x > F3x ... > F9x
 Fx1 < Fx2 < Fx3 ... < Fx9
 不正利用者のアクセス権 a < b < c
 文字の大きさ Fxx-a < Fxx-b < Fxx-c

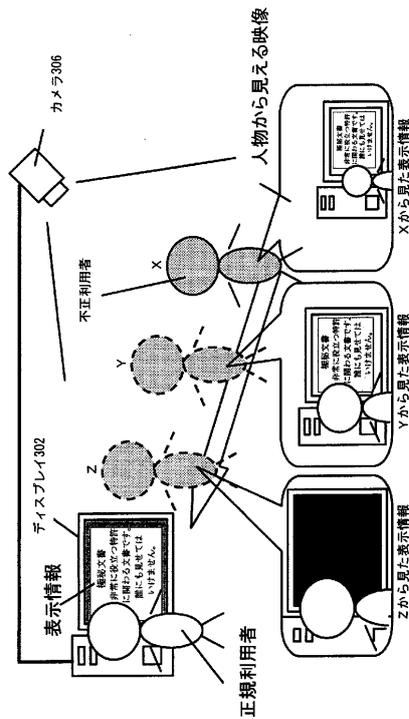
【図 20】



【図 21】



【図 22】



【図 2 3】

距離	L1	L2	L3	...	L9
コントラストの強さ	C1	C2	C3	...	C9

距離 $L1 < L2 < L3 \dots < L9$
 コントラストの強さ $C1 < C2 < C3 \dots < C9$

【図 2 4】

		距離				
機密性の強さ	S1	C11	C12	C13	...	C19
	S2	C21	C22	C23	...	C29
	S3	C31	C32	C33	...	C39

	S9	C91	C92	C93	...	C99

距離 $L1 < L2 < L3 \dots < L9$
 機密性 $S1 < S2 < S3 \dots < S9$
 コントラストの強さ $C1x > C2x > C3x \dots > C9x$
 $Cx1 < Cx2 < Cx3 \dots < Cx9$

【図 2 5】

		不正利用者と表示装置の距離				
機密性の強さ	S1	C11-a	C12-a	C13-a	...	C19-a
		C11-b	C12-b	C13-b	...	C19-b
		C11-c	C12-c	C13-c	...	C19-c
	S2	C21-a	C22-a	C23-a	...	C29-a
		C21-b	C22-b	C23-b	...	C29-b
		C21-c	C22-c	C23-c	...	C29-c
	S3	C31-a	C32-a	C33-a	...	C39-a
		C31-b	C32-b	C33-b	...	C39-b
		C31-c	C32-c	C33-c	...	C39-c

S9	C91-a	C92-a	C93-a	...	C99-a	
	C91-b	C92-b	C93-b	...	C99-b	
	C91-c	C92-c	C93-c	...	C99-c	

距離 $L1 < L2 < L3 \dots < L9$
 機密性 $S1 < S2 < S3 \dots < S9$
 コントラストの強さ $C1x > C2x > C3x \dots > C9x$
 $Cx1 < Cx2 < Cx3 \dots < Cx9$
 不正利用者のアクセス権 $a < b < c$
 コントラストの強さ $Cxx-a < Cxx-b < Cxx-c$

【図 2 6】

番号	氏名	郵便番号	住所
1	〇〇 太郎	000-0000	北海道〇〇市...
2	△△ 次郎	111-1111	大蔵府△△市...
...
10	◇◇ 花子	222-2222	東京都〇〇区...

処理後

番号	氏名	郵便番号	住所
1	〇〇 太郎	000-0000	北海道〇〇市...
2	△△ 次郎	111-1111	大蔵府△△市...
...
10	◇◇ 花子	222-2222	東京都〇〇区...

処理前

【図 2 7】

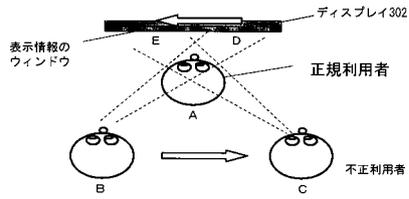
番号	氏名	郵便番号	住所
1	〇〇 太郎	000-0000	北海道〇〇市...
2	△△ 次郎	111-1111	大蔵府△△市...
...
10	◇◇ 花子	222-2222	東京都〇〇区...

処理後

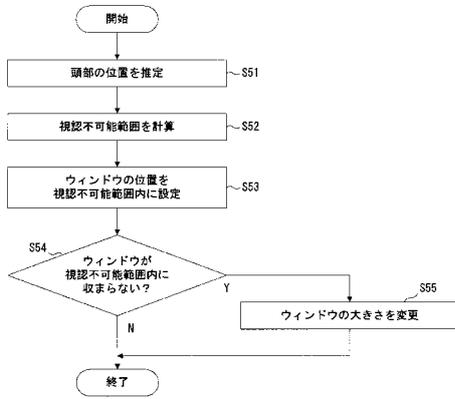
番号	氏名	郵便番号	住所
1	〇〇 太郎	000-0000	北海道〇〇市...
2	△△ 次郎	111-1111	大蔵府△△市...
...
10	◇◇ 花子	222-2222	東京都〇〇区...

処理前

【図28】



【図29】



フロントページの続き

(56)参考文献 特開平06-059042(JP,A)
特開平09-297735(JP,A)
特開2005-346307(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/24

G06F 3/00-3/048