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

特許第3772878号

(P3772878)

(45)発行日　平成18年5月10日(2006.5.10)　(24)登録日　平成18年2月24日(2006.2.24)

(51)Int.Cl.		F I		
G08B 25/04	(2006.01)	G08B	25/04	G
G08B 13/08	(2006.01)	G08B	13/08	Z
H04L 9/32	(2006.01)	H04L	9/00	673E

請求項の数 11　(全 25 頁)

(21)出願番号　特願2003-378808(P2003-378808)
(22)出願日　平成15年11月7日(2003.11.7)
(65)公開番号　特開2005-141571(P2005-141571A)
(43)公開日　平成17年6月2日(2005.6.2)
審査請求日　平成16年10月15日(2004.10.15)

前置審査

(73)特許権者　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町８０１番地
(74)代理人　110000338
特許業務法人原謙三国際特許事務所
(72)発明者　中村　明彦
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内
(72)発明者　大八木　雅之
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内
(72)発明者　山戸　雅貴
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内

最終頁に続く

(54)【発明の名称】サービス提供装置、サービス提供プログラム、コンピュータ読み取り可能な記録媒体、サービス提供方法、セキュリティ管理装置、およびセキュリティ管理方法

(57)【特許請求の範囲】

【請求項１】

ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、

上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、

当該サービス提供装置の動作を制御する制御手段とを備え、

上記制御手段は、

上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、

上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備え、

上記ＩＤ認証手段は、さらに、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行うものであり、

上記外部処理決定手段は、さらに、

下記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令するものであり、

下記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、下記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を行うよう上記外部装置に命令するものであることを特徴とするサービス提供装置。

（判断１）上記アクセスセンサによる、上記近傍領域内にユーザが存在するか否かに関する判断；

（判断２）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、ユーザが上記ＩＤ認証端末を有しているか否かに関して、上記無線通信手段が通信可能な通信エリア内における上記ＩＤ認証端末の有無に対応してなされる、上記無線通信手段による判断；

（判断３）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記アクセスポイントをユーザが操作したか否かに関する、上記操作検知センサによる判断；

（判断４）上記判断１および上記判断３において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記ＩＤ認証端末から上記許可ＩＤ情報に含まれるＩＤ情報を取得できたか否かに関する、上記ＩＤ認証手段による判断。

【請求項２】

上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、

上記操作検知センサは、上記ドアの開錠に用いられるキーが該ドアを開錠する動作を検知することを特徴とする請求項１に記載のサービス提供装置。

【請求項３】

上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、

上記操作検知センサは、上記ドアの開錠に用いられるキーが該ドアの鍵穴に差し込まれる際に、上記鍵穴から上記キーの方へ発生する力を検出する圧力センサであることを特徴とする請求項１に記載のサービス提供装置。

【請求項４】

上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、

上記操作検知センサは、上記ドアの開錠に用いられるキーを鍵穴に差し込み回転させる際に上記キーに発生するトルクを検出するトルクセンサであることを特徴とする請求項１に記載のサービス提供装置。

【請求項５】

上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、

上記操作検知センサは、

上記ドアノブに設けられるコイルと、

上記コイルにより誘導磁界を発生させる磁界発生手段と、

上記磁界発生手段により発生される誘導磁界の磁力変化を検知する検波手段とを備えていることを特徴とする請求項１に記載のサービス提供装置。

【請求項６】

上記無線通信手段は、通信に用いる電波の出力を切り替えることにより通信可能領域の広狭を切り替え可能なものであり、

上記ＩＤ認証手段は、上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断する際に、上記無線通信手段による狭域無線通信を用いるものである一方、

上記無線通信手段を介して正当なＩＤ情報を取得できない場合、上記無線通信手段を用

いて広域無線通信を行うことにより、正当なＩＤ情報を取得できないことを示す情報を外部装置に送信することを特徴とする請求項１ないし５のいずれか１項に記載のサービス提供装置。

【請求項７】

請求項１ないし６に記載のサービス提供装置における制御手段としてコンピュータを機能させることを特徴とするサービス提供プログラム。

【請求項８】

請求項７に記載のサービス提供プログラムを格納したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項９】

ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該サービス提供装置の動作を制御する制御手段とを備え、該制御手段が、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備えているサービス提供装置によるサービス提供方法であって、

上記ＩＤ認証手段が、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行う第１ステップと、

上記外部処理決定手段が、下記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令する第２ステップと、

上記外部処理決定手段が、下記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、下記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を上記外部装置に命令する第３ステップとを備えていることを特徴とするサービス提供方法。

（判断１）上記アクセスセンサによる、上記近傍領域内にユーザが存在するか否かに関する判断；

（判断２）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、ユーザが上記ＩＤ認証端末を有しているか否かに関して、上記無線通信手段が通信可能な通信エリア内における上記ＩＤ認証端末の有無に対応してなされる、上記無線通信手段による判断；

（判断３）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記アクセスポイントをユーザが操作したか否かに関する、上記操作検知センサによる判断；

（判断４）上記判断１および上記判断３において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記ＩＤ認証端末から上記許可ＩＤ情報に含まれるＩＤ情報を取得できたか否かに関する、上記ＩＤ認証手段による判断。

【請求項１０】

ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、

上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、

当該セキュリティ管理装置の動作を制御する制御手段とを備え、

上記制御手段は、

上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、

上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備え、

上記ＩＤ認証手段は、さらに、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記セキュリティ管理装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行うものであり、

上記外部処理決定手段は、さらに、

下記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令するものであり、

下記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、下記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を行うよう上記外部装置に命令するものであることを特徴とするセキュリティ管理装置。

（判断１）上記アクセスセンサによる、上記近傍領域内にユーザが存在するか否かに関する判断；

（判断２）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、ユーザが上記ＩＤ認証端末を有しているか否かに関して、上記無線通信手段が通信可能な通信エリア内における上記ＩＤ認証端末の有無に対応してなされる、上記無線通信手段による判断；

（判断３）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記アクセスポイントをユーザが操作したか否かに関する、上記操作検知センサによる判断；

（判断４）上記判断１および上記判断３において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記ＩＤ認証端末から上記許可ＩＤ情報に含まれるＩＤ情報を取得できたか否かに関する、上記ＩＤ認証手段による判断。

【請求項１１】

ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該セキュリティ管理装置の動作を制御する制御手段とを備え、該制御手段が、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備えているセキュリティ管理装置によるセキュリティ管理方法であって、

上記ＩＤ認証手段が、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記セキュリティ管理装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行う第１ステップと、

上記外部処理決定手段が、下記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令する第２ステップと、

上記外部処理決定手段が、下記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、下記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いこと

をユーザに知らせる処理である２次警報処理を上記外部装置に命令する第３ステップとを備えていることを特徴とするセキュリティ管理方法。

（判断１）上記アクセスセンサによる、上記近傍領域内にユーザが存在するか否かに関する判断；

（判断２）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、ユーザが上記ＩＤ認証端末を有しているか否かに関して、上記無線通信手段が通信可能な通信エリア内における上記ＩＤ認証端末の有無に対応してなされる、上記無線通信手段による判断；

（判断３）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記アクセスポイントをユーザが操作したか否かに関する、上記操作検知センサによる判断；

（判断４）上記判断１および上記判断３において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記ＩＤ認証端末から上記許可ＩＤ情報に含まれるＩＤ情報を取得できたか否かに関する、上記ＩＤ認証手段による判断。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ＩＤ認証を用いて、ユーザに最適なサービスを提供し得るサービス提供システムに関する。

【背景技術】

【０００２】

サービス提供システムの一例としての防犯システムに係る分野においては、様々な防犯手法が提案されている。その中でも特に多い手法は、監視カメラを用いて防犯を行う手法である。

【０００３】

たとえば、特許文献１においては、図８に示すように、撮影装置１００と、撮影装置１００で撮影された映像情報をインターネット１１０上に送信する住宅側端末１２０と、その映像情報をインターネット１１０上から受信して移動端末局１３０へ送信するホストコンピュータ１４０とを備え、住宅側端末１２０やホストコンピュータ１４０が訪問客などを捕捉すると、ホストコンピュータ１４０から移動端末局１３０に映像情報が送信される構成が開示されている。

【０００４】

また、特許文献２においては、図９に示すように、ドア２００に接近した来訪者を外部ユニット２１０に設けられた赤外線センサ等の人物検知装置が検知すると、撮像装置２２０がＯＮとなり、その旨および撮像された画像が録画されていることを、画像表示手段２３０を介して文字情報により、あるいはスピーカ２４０を介して音声情報により示す構成について開示されている。

【特許文献１】特開２００３－１９９０８８号公報（２００３年０７月１１日）

【特許文献２】特開２００２－３１２８６５号公報（２００２年１０月２５日）

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、上記従来技術には、家屋に近づく者が誰であるかを特定することなく撮像装置により監視領域の撮影を行うので、防犯が必要無いような状況においても不必要に防犯システムが動作してしまう問題がある。

【０００６】

具体的には、従来技術では、家屋に近づく者が誰であるかを判断しないので、家屋に近づく者がその家屋の家人、新聞等の配達者、近隣の住人であるか否かに関わらず防犯システムを動作させる。

【０００７】

たとえば、その家屋の家人が帰宅する場合には、撮像装置により家人を撮影して防犯体制をとる必要はあまりない。さらに、家人が帰宅した場合に防犯システムが動作していると、その家人は防犯システムを解除するか、あるいは在宅時の設定にするなどの必要があり、却って家人に煩わしささえ感じさせる場合もある。

【０００８】

また、新聞等の配達者、近隣の住人など、家屋内に不法侵入する可能性が低い者が、家屋のドアに近づいた場合にまで防犯システムを動作させることは、あまり効率的な防犯であるとはいえない。さらに、マンション等の集合住宅などにおいて、特許文献２に記載の技術のように撮像装置による撮影が行なわれていることをスピーカを用いて音声情報により示すと、近隣住人がドアの前を通過する度に音声メッセージが流れることとなり、却って近所迷惑である。

【０００９】

本発明は、上記従来の問題点に鑑みなされたものであって、より効率的な防犯を行うことを可能とし、さらには種々のサービス提供にも応用し得るサービス提供装置、サービス提供方法、サービス提供プログラム、コンピュータ読み取り可能な記録媒体、キーユニット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】

【００１０】

本発明のサービス提供装置は、上記課題を解決するために、ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該サービス提供装置の動作を制御する制御手段とを備え、上記制御手段は、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備え、上記ＩＤ認証手段は、さらに、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行うものであり、上記外部処理決定手段は、さらに、下記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令するものであり、下記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、下記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を行うよう上記外部装置に命令するものであることを特徴としている。

【００１１】

（判断１）上記アクセスセンサによる、上記近傍領域内にユーザが存在するか否かに関する判断；

（判断２）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、ユーザが上記ＩＤ認証端末を有しているか否かに関して、上記無線通信手段が通信可能な通信エリア内における上記ＩＤ認証端末の有無に対応してなされる、上記無線通信手段による判断；

（判断３）上記判断１において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記アクセスポイントをユーザが操作したか否かに関する、上記操作検知センサによる判断；

（判断４）上記判断１および上記判断３において「ＹＥＳ」の判断がなされた場合に実行される判断であって、上記ＩＤ認証端末から上記許可ＩＤ情報に含まれるＩＤ情報を取得できたか否かに関する、上記ＩＤ認証手段による判断。

【００１２】
さらに、上記構成のサービス提供装置において、上記ユーザによる操作の対象物を、家屋内へ入るためのドアとし、上記アクセスポイントを、上記ドアのドアノブとする一方、上記操作検知センサを、上記ドアの開錠に用いられるキーが該ドアを開錠する動作を検知するものとしてもよい。より具体的には、操作検知センサを、上記ドアの開錠に用いられるキーが該ドアの鍵穴に差し込まれる際に、上記鍵穴から上記キーの方へ発生する力を検出する圧力センサとすることができる。または、上記操作検知センサを、上記ドアの開錠に用いられるキーを鍵穴に差し込み回転させる際に上記キーに発生するトルクを検出するトルクセンサとしてもよい。または、上記操作検知センサを、上記ドアノブに設けられるコイルと、上記コイルにより誘導磁界を発生させる磁界発生手段と、上記磁界発生手段により発生される誘導磁界の磁力変化を検知する検波手段とを備えている構成としてもよい。

【００１３】
さらに、上記構成のサービス提供装置において、通信に用いる電波の出力を切り替えることにより通信可能領域の広狭を切り替え可能な無線通信手段を設けるとともに、上記ＩＤ認証手段を、ユーザにより携帯されるＩＤ認証端末と上記無線通信手段を用いて狭域無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行うように構成する一方、上記無線通信手段を介して正当なＩＤ情報を取得できない場合、上記無線通信手段を用いて広域無線通信を行うことにより、正当なＩＤ情報を取得できないことを示す情報を外部装置に送信する構成としてもよい。

【００１４】
また、本発明のサービス提供方法は、ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該サービス提供装置の動作を制御する制御手段とを備え、該制御手段が、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備えているサービス提供装置によるサービス提供方法であって、上記ＩＤ認証手段が、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行う第１ステップと、上記外部処理決定手段が、上記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令する第２ステップと、上記外部処理決定手段が、上記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、上記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を上記外部装置に命令する第３ステップとを備えていることを特徴としている。

【００１５】
また、本発明のサービス提供プログラムは、上記構成におけるサービス提供装置における制御手段としてコンピュータを機能させることを特徴としている。また、本発明のコンピュータ読み取り可能な記録媒体は、上記サービス提供プログラムを格納したことを特徴としている。

【００１６】
また、本発明のセキュリティ管理装置は、ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断す

るアクセスセンサと、当該セキュリティ管理装置の動作を制御する制御手段とを備え、上記制御手段は、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備え、上記ＩＤ認証手段は、さらに、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記セキュリティ管理装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行うものであり、上記外部処理決定手段は、さらに、上記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令するものであり、上記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、上記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を行うよう上記外部装置に命令するものであることを特徴としている。

【００１７】

また、本発明のセキュリティ管理方法は、ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該セキュリティ管理装置の動作を制御する制御手段とを備え、該制御手段が、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備えているセキュリティ管理装置によるセキュリティ管理方法であって、上記ＩＤ認証手段が、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記セキュリティ管理装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行う第１ステップと、上記外部処理決定手段が、上記の（判断１）において「ＹＥＳ」、（判断２）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令する第２ステップと、上記外部処理決定手段が、上記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、上記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を上記外部装置に命令する第３ステップとを備えていることを特徴としている。

【発明の効果】

【００１８】

本発明のサービス提供装置は、以上のように、ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該サービス提供装置の動作を制御する制御手段とを備え、上記制御手段は、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのＩＤ認証を行うＩＤ認証手段と、上記ＩＤ認証手段のＩＤ認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備え、上記ＩＤ認証手段は、さらに、ユーザにより携帯されるＩＤ認証端末と無線通信手段を用いて無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行うものであり、上記外部処理決定手段は、さらに、上記の（判断１）において「ＹＥＳ」、（判断２）に

おいて「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性があることをユーザに知らせる処理である１次警報処理を行うよう上記外部装置に命令するものであり、上記の（判断１）および（判断２）のいずれにおいても「ＹＥＳ」の判断がなされた後、または、上記１次警報処理が行われた後に、上記の（判断３）において「ＹＥＳ」、（判断４）において「ＮＯ」の判断がなされた場合に、不正侵入がなされようとしている可能性が上記１次警報処理により示される可能性よりも高いことをユーザに知らせる処理である２次警報処理を行うよう上記外部装置に命令するものである

上記構成によれば、操作検知センサによりユーザがアクセスポイントを操作したと判断判断される場合に、ＩＤ認証手段によりユーザのＩＤ認証を行うことができる。そして、ＩＤ認証手段によるＩＤ認証の結果に応じた外部処理を外部処理決定手段により外部装置に実行させることができる。

【００１９】

これにより、たとえば操作の対象物を家屋の玄関ドアとし、アクセスポイントを玄関のドアノブとすれば、家屋内に入る際には必ずドアノブを操作することが必要となるので、家屋内に入る者に対し確実にＩＤ認証を行うことが可能となる。そしてそのＩＤ認証の結果に応じて、家屋内に設けられた外部装置としての警報装置や通報装置に、サービスとしてＩＤ認証結果に基づく防犯処理を実行させることができる。

【００２０】

たとえば、ドアノブを操作した者からＩＤ認証により正当なＩＤ情報を得ることができなかった場合は、上記の警報装置により警報を鳴動させたり、通報装置により家屋への不正侵入がなされている可能性が高い旨を所定の通報先に通報したりできる。一方、ドアノブを操作した者からＩＤ認証の結果正当なＩＤ情報を得ることができた場合には、その家屋の家人が帰宅したものと判断し、外部装置としての警報装置や通報装置の動作を無効化するというサービスも外部処理決定手段により実行することができる。

【００２１】

このように、本発明によれば、ユーザが操作対象物を操作したことをトリガとしてＩＤ認証を行い、そのＩＤ認証結果に応じて外部装置により外部処理が実行されることとなる。したがって、本発明では、ユーザが単に操作対象物の前を通過するというだけでは外部処理は実行されない。よって、従来のように近隣住人等がドアの前を通過するだけで警報メッセージが流れてしまうという煩わしさを解消できるという効果を奏する。また、家人が帰宅した際には、本発明により自動的に防犯システムを解除することもできるので、従来のように帰宅する度に防犯システムを解除する必要があったという家人の煩わしさも解消することもできるという効果を奏する。

【００２２】

さらに、本発明では、ＩＤ認証手段がアクセスセンサの判断結果に基づいてユーザのＩＤ認証を行うので、アクセスセンサにより操作対象物の周辺にユーザが存在していると判断される場合にユーザのＩＤ認証を行うことができる。したがって、操作対象物の周辺にユーザが存在していないと判断されるような場合においてはＩＤ認証を行わないように構成できる。したがって、より効率的にユーザのＩＤ認証を行い、外部装置にサービスを実行させることが可能となる。

【００２３】

このように、本発明によれば、効率的に不正侵入者に対する防犯を行うことができる。さらに、本発明によれば、発明を実施するための形態において後述するように、操作対象物をユーザが操作したことをトリガとして、ユーザに応じた種々のサービスを実行することができ、操作対象物を操作する際のユーザの満足度を高めることもできるという効果も奏する。

【００２４】

さらに、上記構成のサービス提供装置において、上記ユーザによる操作の対象物を家屋内へ入るためのドアし、上記アクセスポイントを上記ドアのドアノブとする一方、上記操作検知センサを、上記ドアの開錠に用いられるキーが該ドアを開錠する動作を検知する構

成とすることにより、以下の効果が奏される。

【００２５】

すなわち、家人が家屋へ入ろうとする際には、施錠されたドアの鍵穴にキーを差し込んでドアを開錠した後、ドアノブを操作することが必要になる。上記構成によれば、操作検知センサはキーがドアを開錠する動作を検知するので、ユーザがキーを用いてドアを開錠したことを的確に検知できる。したがって、ユーザがドアノブを操作することも的確に検知できる。

【００２６】

これにより、ＩＤ認証手段によるＩＤ認証処理、および外部処理決定手段による外部装置のサービス実行処理が、ユーザのドアノブ操作と確実に連動して行われることとなるので、より効率的な防犯を行うことができるという効果が奏される。

【００２７】

なお、キーがドアを開錠する動作を検知する操作検知センサは、たとえば、キーをドアの鍵穴に差し込んだ際にキーの方へ発生する力を検出する圧力センサや、ドアの開錠に用いられるキーを鍵穴に差し込み回転させる際に上記キーに発生するトルクを検出するトルクセンサにより、簡易に実現することができる。

【００２８】

さらに上記操作検知センサを、上記ドアノブに設けられるコイルと、上記コイルにより誘導磁界を発生させる磁界発生手段と、上記磁界発生手段により発生される誘導磁界の磁力変化を検知する検波手段とを備えている構成とすることにより、以下の効果が奏される。

【００２９】

すなわち、上記構成によれば、コイルおよび磁界発生手段により、ドアノブの周囲に誘導磁界を発生させることができる。そして、ユーザがドアノブを操作しようとしてドアノブに手を近づけた場合、ドアノブ周囲に発生された誘導磁界に磁力変化が生じるが、この磁力変化を検波手段により検知することができる。

【００３０】

このように、上記構成の操作検知センサによれば、ユーザのドアノブに対する操作を的確に検知することができる。したがって、ＩＤ認証手段によるＩＤ認証処理、および外部処理決定手段による外部装置のサービス実行処理が、ユーザのドアノブ操作と確実に連動して行われることとなるので、より効率的な防犯を行うことができるという効果が奏される。

【００３１】

さらに、上記構成のサービス提供装置において、通信に用いる電波の出力を切り替えることにより通信可能領域の広狭を切り替え可能な無線通信手段を設け、上記ＩＤ認証手段を、ユーザにより携帯されるＩＤ認証端末と上記無線通信手段を用いて狭域無線通信を行うことにより上記ＩＤ認証端末から取得されたＩＤ情報が、上記サービス提供装置に記録された許可ＩＤ情報に含まれているか否かを判断することによって、ユーザのＩＤ認証を行う一方、上記無線通信手段を介して正当なＩＤ情報を取得できない場合、上記無線通信手段を用いて広域無線通信を行うことにより、正当なＩＤ情報を取得できないことを示す情報を外部装置に送信する構成とすることにより、以下の効果が奏される。

【００３２】

すなわち、上記構成によれば、無線通信手段により狭域無線通信を行ってユーザのＩＤ認証端末からユーザのＩＤ情報を取得し、その情報がサービス提供装置に記録された許可ＩＤ情報に含まれているか否かという簡易な処理により、ユーザ認証を行うことができるという効果が奏される。なお、許可ＩＤ情報とは、操作対象物を操作することが許可されたユーザのＩＤが格納されている情報を意味する。また、狭域無線通信とは、数ｍ半径内の無線通信を指す意味において用いている。

【００３３】

また、ＩＤ認証端末から正当なＩＤ情報を取得できない場合には、無線通信手段により

広域無線通信を行って、外部装置に正当なＩＤ情報を取得できないことを示す情報を送信するので、操作対象物の操作を許可されていない者が操作対象物を不正に操作しようとしていることを外部装置に連絡することができる。これにより、外部装置においては、不正操作がなされようとしている場合における所定の処理、たとえば外部への通報処理や警報の鳴動処理を実行することができる。なお、広域無線通信とは、数ｋｍ半径内の無線通信を指す意味において用いている。

【００３４】

このように、本発明によれば、ＩＤ認証処理と、操作対象物に対する不正操作を外部装置に連絡する処理とを、無線通信手段により通信可能領域の広狭を切り替えて行うことができる。したがって、サービス提供装置の構成をより簡易にすることができるとともに、ユーザの利便性を高めることができるという効果が奏される。

【００３５】

さらに、本発明のサービス提供方法においては、第１ステップから第３ステップの各ステップにおいて、本発明のサービス提供装置と同一の処理が実現されている。よって、本発明のサービス提供装置と同様の作用効果を得ることができる。

【発明を実施するための最良の形態】

【００３６】

〔１．システムの概要〕

本発明のサービス提供装置の一実施形態としてのセキュリティ管理装置を用いる防犯システムの概要について、図２を用いて説明する。

【００３７】

図２に示すように、本実施形態の防犯システムは、セキュリティ管理装置１と、ＩＤ認証端末２と、操作検知センサ３と、アクセスセンサ４と、外部装置５とを含んでいる。

【００３８】

セキュリティ管理装置１は、家屋６内に設置されるとともに、ユーザにより携帯されるＩＤ認証端末２との間で近距離無線通信を行うことによって、ＩＤ認証端末２に記憶されたユーザのＩＤ情報や属性情報を取得し、ＩＤ認証を行うものである。上記の近距離無線通信としては、周波数が２．４ＧＨｚ（ギガヘルツ）の無線ＬＡＮ規格に基づく通信方式や、Ｂｌｕｅ－Ｔｏｏｔｈ（登録商標）規格の微弱電波を用いた通信方式を用いることができる。なお、セキュリティ管理装置１の構成および機能については後述する。

【００３９】

ＩＤ認証端末２は、上述のように、自身のユーザを認証するためのユーザ情報として、ユーザが誰であるのかを特定するためのＩＤ情報や、ユーザの属性を示す属性情報を記録するものである。このＩＤ認証端末２は、ユーザが簡易に携帯できるとともにユーザ情報を記録可能な媒体、たとえばＩＣカード、携帯電話機等を用いることが好ましい。

【００４０】

また、ＩＤ情報としては、ユーザの氏名そのものに関する情報、あるいはユーザの氏名を暗号化した情報を用いることができる。また、属性情報としては、ユーザの性別、年齢、身長、体重、体調等を示す情報を用いることができる。なお、ＩＤ認証端末２の構成および機能については後述する。

【００４１】

操作検知センサ３は、ユーザが玄関ドア７のドアノブ８（アクセスポイント）に手を触れたか否か、または手を近づけたか否かを検知するためのものである。操作検知センサ３としては、ユーザ操作によるドアノブ８の振動を検知する振動検知センサ、静電容量の変化を検知する接触センサなどを用いることができる。この操作検知センサ３により、ユーザのドアノブ８に対する操作が検知されたことがトリガとなって、セキュリティ管理装置１によるＩＤ認証が実行される。

【００４２】

アクセスセンサ４は、ユーザがドアノブ８を操作しているときに存在し得る領域（アクセスエリア、近傍領域）に接近したか否かを検知するためのものである。アクセスセンサ

４は、数ｍ半径の領域内における人体の存否を確認するセンサ、たとえば焦電センサ、マイクロ波センサ、超音波ドップラセンサを用いることができる。

【００４３】

外部装置５は、家屋内における警報装置、通報装置、テレビジョンなどの画像表示装置、エアコン等、セキュリティ管理装置１と独立した機器として構成されるものである。さらに、「外部装置」には、家屋外に設置された課金装置、ＰＣ端末、携帯電話等の機器も含まれる。

【００４４】

以上のような構成により、セキュリティ管理装置１は、操作検知センサ３によりドアノブ８にユーザが触れたことが検知された場合に、ユーザが有するＩＤ認証端末２を用いてＩＤ認証を行い、その結果に基づき、外部装置５に対し外部処理命令を与え、種々の処理を実行することを命令する。以下、上述した防犯システムを構成する要素のそれぞれについて、構成および機能を詳細に説明する。

【００４５】

〔２．ＩＤ認証端末の構成〕

先ず、ＩＤ認証端末２の構成および機能について説明する。図３に示すように、ＩＤ認証端末２は、通信部１０と、ユーザ情報記録部１１と、制御部１２とを備えている。

【００４６】

通信部１０は、外部装置との通信を行うためのインターフェース回路であり、セキュリティ管理装置１との通信を実現するものである。たとえば、ＩＤ認証端末２がＩＣカードであれば、リーダライタとしてのセキュリティ管理装置１が放出するエネルギーの一部を電源として利用するアンテナコイルにより通信部１０は実現される。また、ＩＤ認証端末２が携帯電話機であれば、通信部１０は、携帯電話機において携帯電話通信を実現する通信回路により実現される。

【００４７】

ユーザ情報記録部１１は、ＩＤ認証端末２のユーザを認証するためのユーザ情報として、上述したＩＤ情報および属性情報を記録するものである。ここで、ＩＤ情報は、ユーザが誰であるのかを特定することができる情報であるので、プライバシー保護および不正利用防止の観点から、一旦ユーザ情報記録部１１に書き込まれた後は変更できないようにしておくことが好ましい。したがって、ユーザ情報記録部１１のうちＩＤ情報を記録する部分は、フィールド・プログラマブルＲＯＭなどの１回のみ書込みが可能な記録媒体によって構成しておき、ＩＤ認証端末２を最初に使用開始する際にＩＤ情報の記憶処理を行う、という構成をとることが好ましい。

【００４８】

また、属性情報のうち、ユーザの性別を示す情報は基本的に一生変わることはないが、ユーザの年齢、身長、体重、体調等を示す情報は時々刻々と変化するものであるので、属性情報は書き換え可能にＩＤ認証端末２に記録されていることが好ましい。したがって、ユーザ情報記録部１１のうち属性情報を記録する部分は、書き換え可能な記録媒体、たとえばＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）により構成しておくことが好ましい。

【００４９】

制御部１２は、ＩＤ認証端末２における処理を統括的に制御するものである。特に、制御部１２は、ユーザ情報記録部１１からＩＤ情報または属性情報を取得するユーザ情報取得部１３を備えている。なお、ユーザ情報取得部１３によるユーザ情報の取得は、セキュリティ管理装置１からの通信部１０を介したユーザ情報取得要求に基づき実行され、取得されたユーザ情報は、通信部１０によりセキュリティ管理装置１に送信される。

【００５０】

上記構成により、ＩＤ認証端末２は、通信部１０によりセキュリティ管理装置１との通信を行うとともに、その通信内容に基づき、ユーザ情報記録部１１に記録されたＩＤ情報または属性情報をユーザ情報取得部１３により読み出す。さらに、ＩＤ認証端末２は、通

信部１０を用いて、ＩＤ情報または属性情報をセキュリティ管理装置１に送信する。

【００５１】

〔３．セキュリティ管理装置の構成〕

次に、セキュリティ管理装置１の構成および機能について説明する。セキュリティ管理装置１は図１に示すように、通信処理部（無線通信手段）１４と、制御部（制御手段）１５と、記録部１６とを備えている。

【００５２】

通信処理部１４は、外部機器との通信を行うためのインターフェース回路であり、ＩＤ認証端末２との通信を実現するＩＤ認証端末通信部（無線通信手段）１７と、外部装置との通信を実現する外部装置通信部（無線通信手段）１８とを備えている。

【００５３】

ここで、ＩＤ認証端末通信部１７とセキュリティ管理装置１との通信は、上述のように近距離無線通信によって実現されているので、ＩＤ認証端末通信部１７としては、数ｍ程度の近距離無線通信を実現するものであればよい。

【００５４】

一方、外部装置通信部１８は、通常のケーブルを用いた有線通信を採用しても、近距離の無線通信を採用しても構わない。特に、外部装置が家屋外に設定されたＰＣ端末、携帯電話等の機器である場合、外部装置通信部は、インターネット網や携帯電話網等の広域通信を実現するものであることが好ましい。

【００５５】

なお、ＩＤ認証端末通信部１７と、外部装置通信部１８とは図１において別ブロックとして記載したが、必ずしもこれらの通信部は別個のものとして構成されている必要はない。すなわち、通信に用いる電波の出力を切り替えることにより通信領域の広狭を切り替え可能な無線通信手段に、ＩＤ認証端末通信部１７および外部装置通信部１８の役割を負わせることも可能である。

【００５６】

つまり、上述のような無線通信手段により低パワーの電波を出力することにより、数ｍ半径内の領域における狭域無線通信を実現すれば、ＩＤ認証端末通信部１７の機能を同無線通信手段に担保させることができる。一方、同無線通信手段により高パワーの電波を出力することにより、数ｋｍ半径内の領域における広域通信を実現すれば、外部装置通信部１８の役割を同無線通信手段に担保させることも可能である。

【００５７】

制御部１５は、セキュリティ管理装置１内部の処理を統括的に制御するものである。特に、制御部１５は、操作有無判断部１９と、アクセス判断部２０と、ＩＤ認証処理部（ＩＤ認証手段）２１と、外部処理決定部（外部処理決定手段）２２とを備えている。

【００５８】

操作有無判断部１９は、ドアノブ８に対するユーザの操作が操作検知センサ３により検知されたか否かを判断するものである。また、アクセス判断部２０は、ドアノブ８の近辺における人物の存在がアクセスセンサ４により検知されたか否かを判断するものである。

【００５９】

ＩＤ認証処理部２１は、通信処理部１４を介してＩＤ認証端末２と通信を行うことにより、ＩＤ認証処理を実行するものである。具体的には、ＩＤ認証処理部２１は、ＩＤ認証端末２のユーザ情報記録部１１に格納されたＩＤ情報を取得し、そのＩＤ情報と、セキュリティ管理装置１の記録部１６に記録された許可ＩＤ情報とを比較することによってＩＤ認証処理を行う。

【００６０】

すなわち、セキュリティ管理装置１の記録部１６に記録された許可ＩＤ情報は、家屋内における居住者およびその友人、親戚等、家屋内に居ることが許可された者のＩＤを示す情報である。したがって、ＩＤ認証処理部２１は、ＩＤ認証端末通信部１７を介して取得したＩＤ情報が許可ＩＤ情報に含まれているか否かを判断することによって、ＩＤ認証端

末２が正当なＩＤ情報を有しているか否かを判断することができる。

【００６１】

なお、ユーザのＩＤ認証処理は、上述のようにＩＤ認証端末２におけるＩＤ情報を取得して行う方式に限定されるものではない。たとえば、バイオメトリックな手段、すなわち指紋認識、顔面認識、網膜認識、虹彩認識、音声認識などの手段をセキュリティ管理装置１に設け、これによってユーザの認証を行うことも可能である。

【００６２】

外部処理決定部２２は、操作有無判断部１９による判断結果、アクセス判断部２０による判断結果、およびＩＤ認証処理部２１によるＩＤ認証結果に基づき、外部装置通信部１８を介して、外部装置に外部処理命令を付与するものである。具体的には、外部処理決定部２２は、操作有無判断部１９によりユーザがドアノブ８を操作したことを判断し、さらにアクセス判断部２０によりドアノブ８の近辺に人物が存在すると判断された場合において、ＩＤ認証処理部２１により得られたＩＤ情報や属性情報に応じた処理を実行するよう、外部機器に動作命令を付与する。外部機器が行う動作の詳細については後述する。

【００６３】

以上のように、セキュリティ管理装置１は、ユーザが携帯するＩＤ認証端末２からユーザのＩＤ情報や属性情報を取得してＩＤ認証処理部２１によりＩＤ認証処理を行うとともに、操作有無判断部１９およびアクセス判断部２０の判断結果を考慮して、外部装置が行う処理を決定するものである。

【００６４】

〔４．好適なＩＤ認証端末の構成〕

次に、ＩＤ認証端末の好適な実施形態であるキーユニットの構成について説明する。図４に示すように、本実施形態のキーユニット２３は、通信部（ＩＤ情報送信手段）２４と、制御部２５と、記録部（記録手段）２６と、表示部（表示手段）２７とを備えている。さらに、キーユニット２３は、鍵穴に差し込まれる鍵部（キー部分）２８と、鍵部２８を鍵穴に差し込んで開錠・施錠する場合に鍵部２８に発生するトルクを検出するトルクセンサ（操作検知センサ）２９と、鍵部２８を鍵穴に差し込む際に鍵部がキーユニットに付与する力を検出する圧力センサ（操作検知センサ）３０とを備えている。

【００６５】

通信部２４は、キーユニット２３と外部機器との通信を行うためのインターフェース回路である。特に、通信部２４は、セキュリティ管理装置１との通信を実現するものであるので、近距離無線通信方式を採用することが好ましい。

【００６６】

制御部２５は、キーユニット内部の処理を統括的に制御するものである。特に制御部２５は、ユーザ情報取得部３１と、本体側情報取得部３２と、使用検知部３３とを備えている。

【００６７】

ユーザ情報取得部３１は、記録部２６に記録されたＩＤ情報や属性情報を取得するものである。さらに、ユーザ情報取得部３１は、記録部２６から取得したＩＤ情報や属性情報を、セキュリティ管理装置１のＩＤ認証処理部２１がＩＤ認証に用いることができるよう、これらの情報をセキュリティ管理装置１のＩＤ認証処理部２１に送信する。

【００６８】

本体側情報取得部３２は、過去の家屋内における異常履歴を示す異常履歴情報や、現在家屋内に居る者を示す在宅者情報などを、通信部２４を介してセキュリティ管理装置１の記録部１６から取得するものである。

【００６９】

なお、異常履歴情報は、セキュリティ管理装置１の制御部１５により作成されるものである。具体的には、ＩＤ認証処理部２１がドアノブ８を操作するユーザから正当なＩＤ情報を取得できない場合に、家屋内に不正侵入がなされた可能性が高い時刻を示す情報が、異常履歴情報として作成される。

【００７０】
また、在宅者情報も、セキュリティ管理装置１の制御部１５により作成されるものである。具体的には、制御部１５は、ドアノブ８を操作するユーザから正当なＩＤ情報を取得できた場合には、その履歴を在宅者情報として作成する。
【００７１】
表示部２７は、液晶パネル等の画像表示装置により構成されるものであり、本体側情報取得部３２が取得した異常履歴情報や在宅者情報を表示するものである。表示部２７にてこれらの情報を表示することにより、ユーザは、家屋内における過去の異常履歴や、現在家屋内にいる者を確認することができる。
【００７２】
使用検知部３３は、トルクセンサ２９または圧力センサ３０の出力を判断することにより、現在キーユニット２３の鍵部２８が鍵穴に差し込まれて開錠または施錠に用いられているか否かを判断するものである。
【００７３】
すなわち、キーユニット２３の鍵部２８を鍵穴に挿入して開錠する際には、鍵部２８が鍵穴を回転させることになるので、鍵部２８にはトルクが発生することになる。したがって、トルクセンサ２９によりキーユニット２３が使用されているか否かを判断することができる。また、キーユニット２３を鍵穴に挿入する際には、鍵部２８を鍵穴に押し当てる力が発生するので、その反力を圧力センサ３０により検出すれば、キーユニット２３が使用されているか否かを判断することができる。
【００７４】
この使用検知部３３は、上述した操作検知センサ３としても機能するものである。すなわち、キーユニット２３の鍵部２８を鍵穴に差し込む際には、同時にドアノブに手を近づけることにもなる。したがって、使用検知部３３によりキーユニット２３の使用があったか否かを判断すれば、ユーザがドアノブ８に手を近づけたか否かを判断することができる。
【００７５】
このようにキーユニット２３に使用検知部３３を設けることにより、キーユニット２３は、ＩＤ認証端末２としての機能と、操作検知センサ３としての機能とを有することとなる。つまり、本実施形態のキーユニット２３では、ＩＤ認証端末２と操作検知センサ３とが一体的に構成されているので、特にドアノブ８に操作検知センサ３を設ける必要がなくなる。したがって、本実施形態の防犯システムをより低コストにて提供することができる。
【００７６】
〔５．ドアノブセンサ〕
次に、操作検知センサの好適な実施形態であるドアノブセンサの構成について説明する。図５に示すように、本実施形態のドアノブセンサ４０は、ドア４１のドアノブ４２に取り付けられるコイル４３と、発振部（磁界発生手段）４４と、検波部（検波手段）４５と、判定部４６とを備えている。
【００７７】
発振部４４は、ドアノブ４２に取り付けられたコイル４３に電流を付与することにより、誘導磁界を発生させるものである。このように発振部４４により発せられる誘導磁界の磁力は、ユーザがドアノブ４２に手を近づけると変化する。検波部４５は、このように生じる磁力の変化を検知するものである。
【００７８】
そして、判定部４６は、検波部４５が所定レベル以上の磁力変化を検知したか否かを判断することにより、ユーザがドアノブに手を近づけたか否かを判断するものである。すなわち、ユーザがドアノブに手を近づければ近づけるほど、コイル４３により発生される磁界には大きな変化が生じる。したがって、判定部４６においては、検波部４５が所定レベル以上の磁力変化を検知した場合に、ユーザがドアノブに手を近づけたと判断される。

【００７９】
このように、本実施形態のドアノブセンサ４０によれば、ドアノブ４２にコイル４３を引っ掛けるという簡易な構成により、ユーザがドアノブに手を近づけたか否かを判断できる。したがって、ドアに穴を開けて振動検知センサや接触センサを設けることなく、操作検知センサ３をドアに設けることができるので、低コストにて本実施の形態の防犯システムを提供することができる。
【００８０】
〔６．処理フロー〕
次に、本実施の形態のセキュリティ管理装置１により実行される処理フローについて説明する。なお、セキュリティ管理装置１が実行する処理フローには、アクセスセンサ４の検知結果を用いない場合と用いる場合との２通りの処理フローがあるので、これらの処理フローを順番に説明する。
【００８１】
（６－１．アクセスセンサの検知結果を用いない場合）
先ず、アクセスセンサの検知結果を用いない場合の処理フローを説明する。図６に示すように、セキュリティ管理装置１の制御部２５により、セキュリティモードがＯＮに設定される（ステップ１、以下各ステップを単にＳと記載する）。
【００８２】
なお、セキュリティモードとは、後述するように、ＩＤ認証端末２に記録されたＩＤ情報に基づき、セキュリティを解除したり外部処理を実行したりするモードのことを意味する。
【００８３】
その後、玄関ドア７が開いたか否かが、操作検知センサ３により検知される（Ｓ２）。Ｓ２において玄関ドアが開いていないと判断された場合、再度Ｓ２に戻り玄関ドアが開いたか否かの判断が行われる。
【００８４】
Ｓ２において玄関ドア７が開いたと判断された場合、ＩＤ認証端末通信部１７により、ユーザがＩＤ認証端末２を有しているか否かが判断される（Ｓ３）。具体的には、ＩＤ認証端末通信部１７が通信可能な通信エリア内にＩＤ認証端末２が存在するか否かを判断することにより、Ｓ２の判断が行われる。
【００８５】
Ｓ３においてユーザがＩＤ認証端末を有していないと判断された場合、ＩＤ認証端末を有していない者が玄関ドア７を開けたことになるので、家屋への不正侵入がなされている可能性が高い。そこで、外部処理決定部２２は、その判断結果に基づき、外部装置としての警報装置に対し、警報を鳴動する処理を外部処理として行うよう命令する（Ｓ４）。
【００８６】
なお、Ｓ４において、外部処理決定部２２は、外部装置としての通報装置に対して、不正侵入がなされようとしている旨を所定の通報先へ通報する処理を外部処理として行うよう命令してもよい。特に、不正侵入がなされようとしている旨を通報する際には、上述した通信領域の広狭を切り替え可能な無線通信手段によりＩＤ認証端末通信部１７と外部装置通信部１８との役割を担保させることが有利である。すなわち、当該無線通信手段により、広域の無線通信を行えば、数ｋｍ先にいるユーザのＩＤ認証端末にも不正侵入がなされようとしている旨を通報することができる。これにより、ユーザにより迅速に家屋への不正侵入を知らせることができる。
【００８７】
Ｓ４の後、Ｓ５において、制御部１５は記録部１６における異常履歴情報を更新する。具体的は、ＩＤ認証端末を有していない者が玄関ドアを開けたことと、その者により玄関ドアが開けられた時刻とを異常履歴情報に追加する。この異常履歴情報は、上述したキーユニット２３をユーザが携帯している場合に有効に活用される。
【００８８】

すなわち、ユーザがキーユニット２３（図４参照）を携帯している場合には、異常履歴情報が表示部２７において表示されるので、ユーザは家屋内に入る前に、家屋への不正侵入があったか否かを確認できる。したがって、家人と不正侵入者とが鉢合わせして不正侵入者から暴力を受けるというような事故を未然に防止できる。

【００８９】

一方、Ｓ３においてユーザがＩＤ認証端末を有していると判断された場合、ＩＤ認証処理部２１により、ＩＤ認証端末が正当なＩＤ情報を有しているか否かが判断される（Ｓ６）。Ｓ６においては、たとえば上述したように、ＩＤ認証処理部２１が、ＩＤ認証端末通信部１７を介して取得したＩＤ情報が許可ＩＤ情報に含まれているか否かを判断することによって、ＩＤ認証端末が正当なＩＤ情報を有しているか否かを判断することができる。

【００９０】

Ｓ６においてＩＤ認証端末が正当なＩＤ情報を有していないと判断された場合には、上述したＳ４における警報の鳴動処理を実行した後、Ｓ５において異常履歴情報の更新処理が実行される。

【００９１】

また、Ｓ６においてＩＤ認証端末が正当なＩＤ情報を有していると判断された場合には、制御部１５により、セキュリティの解除処理が実行される。セキュリティの解除処理とは、家屋内の窓やドアに取り付けられた不正侵入検知用の振動センサや、家屋内に取り付けられた人体検知センサ等の防犯センサの動作を停止させる処理を意味している。

【００９２】

Ｓ７においてセキュリティの解除処理が行われた後、Ｓ８において、外部処理決定部２２は、ＩＤ認証端末２のＩＤ情報に応じた各種の処理を実行するよう、外部装置に外部処理命令を付与する。

【００９３】

たとえば、ＩＤ認証端末のＩＤ情報が子供のものであると判断された場合には、外部処理決定部２２は、外部装置としての防犯センサを起動したり、家屋内の玄関、扉、窓等に取り付けられた外部装置としての鍵が施錠されるように、外部処理命令を付与する。これにより、子供が家屋内への不正侵入者に暴行を受ける被害を未然に防ぐことが可能となる。また、ＩＤ認証端末のＩＤ情報が老人のものである場合にも、同様の外部処理命令が外部処理決定部２２により付与される。

【００９４】

また、家屋内において各個人に部屋が割り当てられている場合には、ＩＤ認証端末のＩＤ情報からその個人に割り当てられた部屋を判断し、外部装置としてのその部屋の照明が点灯されるよう、外部処理決定部２２により外部処理命令を付与してもよい。さらには、外部装置としてのその部屋のエアコンが作動するよう、外部処理決定部２２から外部処理命令を付与してもよい。

【００９５】

（６－２．アクセスセンサの検知結果を用いる場合）

次に、アクセスセンサの検知結果を用いる場合の処理フローを説明する。図７に示すように、セキュリティ管理装置１の制御部２５により、セキュリティモードがＯＮに設定される（Ｓ１１）。

【００９６】

その後、玄関ドア７の前にユーザが居るか否かが、アクセスセンサ４により判断される（Ｓ１２）。Ｓ１２において玄関ドア７の前にユーザが居ないと判断された場合には、再度Ｓ１２において玄関ドア７の前にユーザが居るか否かが判断される。

【００９７】

Ｓ１２においてドアの前にユーザがいると判断された場合には、ＩＤ認証端末通信部１７により、ユーザがＩＤ認証端末２を有しているか否かが判断される（Ｓ１３）。Ｓ１３においてユーザがＩＤ認証端末２を有していないと判断された場合には、外部処理決定部２２は、外部装置としての警報装置に対し、１次警報処理を行うよう命令する（Ｓ１４）

。

【００９８】

ここで、１次警報処理とは、家屋への不正侵入がなされようとしている可能性があることを、警報装置により警報を鳴動させることによってユーザに知らせる処理のことをいう。すなわち、Ｓ１３において玄関ドアの前に居るユーザがＩＤ認証端末２を有していないと判断されたことは、その家屋の家人以外の者が玄関ドアの前に立っているということなので、家屋への不正侵入がなされようとしている可能性が高いと判断できる。

【００９９】

ただし、新聞や郵便の配達者が玄関ドアの前に立っている場合に大音量の警報が鳴動されてしまっては、近所迷惑となってしまう場合がある。したがって、１次警報処理においては、比較的小音量の警報を鳴動させることが好ましい。また、Ｓ１２においてドアの前にユーザが居ると判断されてから所定時間を経過するまでに、Ｓ１３においてユーザのＩＤ認証端末が認識されない場合に、Ｓ１４において１次警報処理を実行するようにしてもよい。

【０１００】

一方、Ｓ１３においてユーザがＩＤ認証端末を有していると判断された場合は、Ｓ１５において、そのユーザが玄関ドア７を開けたか否かが操作検知センサ３により判断される（Ｓ１５）。Ｓ１５においてドアを開けていないと判断される場合は、再度Ｓ１２において玄関ドアの前にユーザがいるか否かの判断が行われる。

【０１０１】

一方、Ｓ１５においてユーザが玄関ドアを開けたと判断された場合には、Ｓ１６において、ＩＤ認証処理部２１により、ＩＤ認証端末が正当なＩＤ情報を有しているか否かが判断される。Ｓ１６は、図６のＳ６と同様の処理であるので、その詳細な説明は省略する。

【０１０２】

Ｓ１６においてＩＤ認証端末が正当なＩＤ情報を有していないと判断された場合、Ｓ１７において、外部処理決定部２２は、外部装置としての警報装置に対し、２次警報処理を行うよう命令する（Ｓ１７）。

【０１０３】

Ｓ１７における２次警報処理とは、図６のＳ４と同様の処理である。すなわち、２次警報処理とは、外部装置としての警報装置が警報を鳴動させる処理や、通報装置が所定の通報先に不正侵入がなされようとしている旨を通報する処理のことを意味している。

【０１０４】

なお、この２次警報処理が行われる場合は、正当なＩＤ認証端末を有していないユーザが既に家屋内に入ってきている場合なので、家屋への不正侵入が行われている可能性が非常に高い。したがって、２次警報処理においては、より大音量で警報を鳴動させたり、所定の通報先に不正侵入を通報する処理を行うことにより、不正侵入した者に対する威嚇をより効果的に行うことができる。

【０１０５】

さらに、Ｓ１７の後、Ｓ１８において、制御部１５は記録部１６における異常履歴情報を更新する。Ｓ１８の処理は、図６のＳ５の処理と同様であるのでその詳細な説明は省略する。

【０１０６】

一方、Ｓ１６においてＩＤ認証端末が正当なＩＤ情報を有していると判断された場合、Ｓ１９において、制御部１５により、セキュリティの解除処理が実行された後、Ｓ２０において、外部処理決定部２２により、ＩＤ認証端末２のＩＤ情報に応じた各種の処理を実行する命令が外部装置に対してなされる。Ｓ１９は図６のＳ７と同一の処理であり、Ｓ２０は図６のＳ８と同一の処理であるので、その詳細な説明は省略する。

【０１０７】

〔７．他のサービスへの適用例〕

上述の実施形態では、玄関ドアのドアノブをアクセスポイントとし、そのアクセスポイ

ントをユーザが操作した場合、すなわちアクセスポイントにユーザがアクセスした場合に、ユーザのＩＤ認証を行い、そのＩＤ認証結果に基づき外部処理が行われる。しかしながら、本発明のサービス提供装置の適用範囲は上述したような防犯システムのみに限られるものではない。

【０１０８】

たとえば、本発明のサービス提供装置は、工作機械の操作説明システムにも用いることができる。すなわち、工作機械の操作部をアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、そのアクセスポイントにユーザがアクセスした場合にユーザのＩＤ認証を行い、ユーザのＩＤに応じた外部処理を行うことができる。

【０１０９】

具体的には、工作機械の操作部に上述したような操作検知センサを設けておき、その操作検知センサによりユーザが操作部を操作したと判断される場合にユーザのＩＤ認証を行う。そして、ユーザのＩＤ情報からその工作機械の操作についてユーザがどの程度習熟しているかを判断し、その習熟度に応じた操作説明を工作機械のディスプレイから行う処理を外部処理として実行することができる。たとえば、初心者に対しては、工作機械のディスプレイに操作方法を逐一表示するとともに、音声による操作案内を行うという処理を行うことにより、工作機械の操作について説明することができる。一方、熟練者に対しては、全く操作説明を行わないという処理を行うこともできる。

【０１１０】

また、本発明のサービス提供装置は、ＰＣ（Personal Computer）に用いることもできる。すなわち、ＰＣを操作するにあたってユーザが必ずアクセスする箇所、たとえば電源スイッチ、マウス、キーボード等をアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、以下のような外部処理を行うことができる。

【０１１１】

具体的には、ＰＣの電源スイッチに操作検知センサを設けておき、その操作検知センサによりユーザが電源スイッチを押下したと判断される場合に、ユーザのＩＤ認証を行う。そのＩＤ認証により得られたユーザのＩＤ情報に基づいて、各ユーザについて設定された起動画面を表示する処理を外部処理として行うことができる。さらに、ＰＣ起動時に実行されるプログラムについて、各ユーザが異なる設定をしている場合には、ＩＤ認証により得られたユーザのＩＤ情報に基づき、そのユーザが設定したプログラムを自動的に実行する処理を外部処理として行うことができる。

【０１１２】

さらに、本発明のサービス提供装置は、料理提供サービスにも用いることができる。すなわち、ユーザが料理をするにあたって必ずユーザがアクセスする箇所、たとえば冷蔵庫の開閉ハンドルをアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、以下のような外部処理を行うことができる。

【０１１３】

具体的には、冷蔵庫の開閉ハンドルに操作検知センサを設けておき、その操作検知センサによりユーザが開閉ハンドルを操作したと判断される場合にユーザのＩＤ認証を行う。そして、ユーザのＩＤ情報からユーザの健康状態を判断し、そのユーザの健康状態に最適な食材を選択して冷蔵庫のディスプレイに表示する処理を外部処理として行うことができる。

【０１１４】

また、本発明のサービス提供システムは、レンタカーを利用する際の課金システムに用いることもできる。すなわち、レンタカーを利用するにあたってユーザが必ずアクセスする箇所、たとえばドアハンドルやステアリング等をアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、以下のような外部処理を行うことができる。

【０１１５】

具体的には、上述のアクセスポイントに操作検知センサを設けておき、その操作検知センサによりユーザがドアハンドル等を操作したと判断される場合、ユーザのＩＤ認証を行

う。そして、そのＩＤ認証により得られるＩＤ情報をレンタカー利用料金を管理する管理サーバに送信し、各ユーザについての利用料金を自動課金するということが可能である。

【０１１６】

〔８．補足〕

最後に、上記セキュリティ管理装置１の各ブロックは、ハードウェアロジックによって構成してもよいし、次のようにＣＰＵを用いてソフトウェアによって実現してもよい。

【０１１７】

すなわち、セキュリティ管理装置１は、各機能を実現する制御プログラムの命令を実行するＣＰＵ（central processing unit）、上記プログラムを格納したＲＯＭ（read only memory）、上記プログラムを展開するＲＡＭ（random access memory）、上記プログラムおよび各種データを格納するメモリ等の記憶装置（記録媒体）などを備えている。そして、本発明の目的は、上述した機能を実現するソフトウェアであるセキュリティ管理装置１の制御プログラムのプログラムコード（実行形式プログラム、中間コードプログラム、ソースプログラム）をコンピュータで読み取り可能に記録した記録媒体を、セキュリティ管理装置１に供給し、そのコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に記録されているプログラムコードを読み出し実行することによっても、達成可能である。

【０１１８】

上記記録媒体としては、たとえば、磁気テープやカセットテープ等のテープ系、フロッピー（登録商標）ディスク／ハードディスク等の磁気ディスクやＣＤ－ＲＯＭ／ＭＯ／ＭＤ／ＤＶＤ／ＣＤ－Ｒ等の光ディスクを含むディスク系、ＩＣカード（メモリカードを含む）／光カード等のカード系、あるいはマスクＲＯＭ／ＥＰＲＯＭ／ＥＥＰＲＯＭ／フラッシュＲＯＭ等の半導体メモリ系などを用いることができる。

【０１１９】

また、セキュリティ管理装置１を通信ネットワークと接続可能に構成し、上記プログラムコードを通信ネットワークを介して供給してもよい。この通信ネットワークとしては、特に限定されず、たとえば、インターネット、イントラネット、エキストラネット、ＬＡＮ、ＩＳＤＮ、ＶＡＮ、ＣＡＴＶ通信網、仮想専用網（virtual private network）、電話回線網、移動体通信網、衛星通信網等が利用可能である。また、通信ネットワークを構成する伝送媒体としては、特に限定されず、たとえば、ＩＥＥＥ１３９４、ＵＳＢ、電力線搬送、ケーブルＴＶ回線、電話線、ＡＤＳＬ回線等の有線でも、ＩｒＤＡやリモコンのような赤外線、Ｂｌｕｅｔｏｏｔｈ、８０２．１１無線、ＨＤＲ、携帯電話網、衛星回線、地上波デジタル網等の無線でも利用可能である。なお、本発明は、上記プログラムコードが電子的な伝送で具現化された搬送波あるいはデータ信号列の形態でも実現され得る。

【０１２０】

なお、本発明のキーユニットは、以上のように、ドアの鍵穴に差し込まれるキー部分と、ユーザのＩＤ情報を記録する記録手段と、上記キー部分が上記ドアの鍵穴に差し込まれることを検知する操作検知センサと、上記操作検知センサの検知結果に基づき、上記記録手段からユーザのＩＤ認証を行う外部のＩＤ認証手段に、上記ユーザのＩＤ情報を送信するＩＤ情報送信手段とを備えていることにより、以下の効果を奏する。

【０１２１】

すなわち、上記構成によれば、ユーザがドアを開錠するためにキー部分を差し込むと、操作検知センサによりキー部分が鍵穴に差し込まれたことが検知され、ＩＤ情報送信手段により記録手段からユーザのＩＤ情報が送信される。

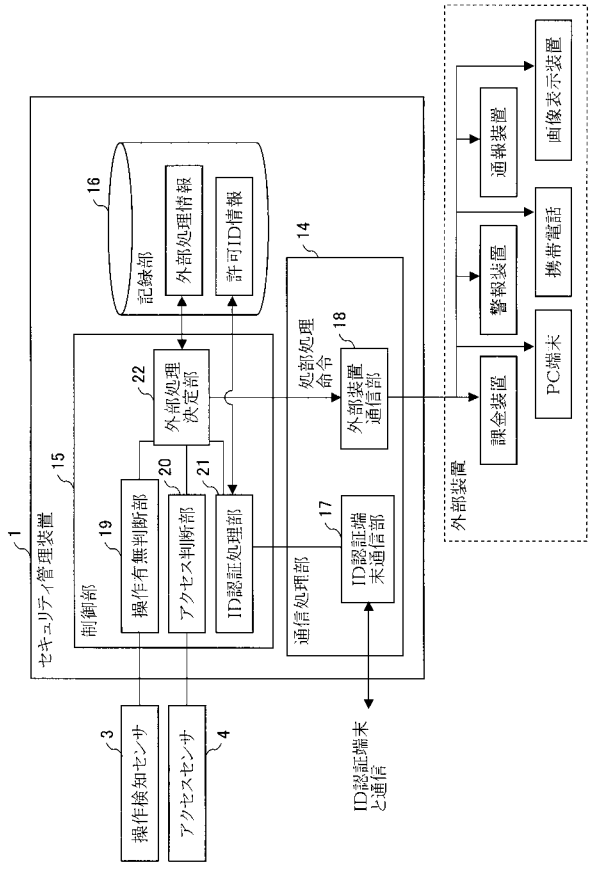
【０１２２】

ここで、上記のＩＤ認証手段を、上述した本発明のサービス提供装置におけるものとすることにより、ユーザがドアを開錠するための一連の動作において、自動的にＩＤ情報がキーユニットからＩＤ認証手段に送信され、ＩＤ認証が行われることとなる。したがって、ユーザにおいては、ドアを開錠する以外に余分な動作を行わなくても、サービス提供装置にＩＤ認証を実行させることができる。よって、本発明のサービス提供装置に用いるのに適したキーユニットを提供することができるという効果が奏される。

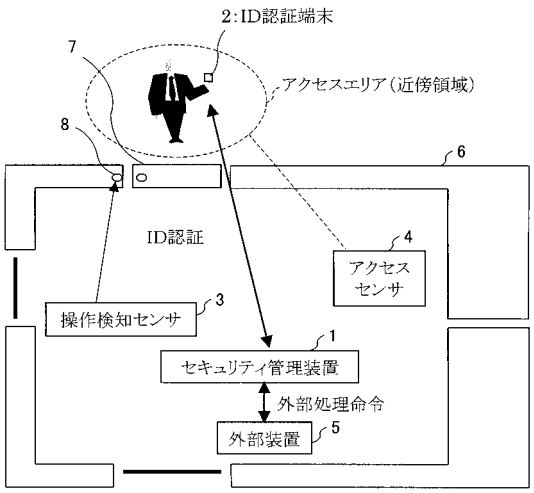
【０１２３】
さらに、上記構成のキーユニットにおいて、上記ＩＤ認証手段が行ったＩＤ認証の結果に基づき作成される、家屋への不正侵入がなされた可能性が高い時刻を示す異常履歴情報および家屋内に在宅している者を示す在宅者情報の少なくとも一方を、上記ＩＤ認証手段から取得し表示する表示手段を備えることにより、以下の効果が奏される。
【０１２４】
すなわち、上記構成によれば、ユーザは、キーユニットの表示手段に表示された異常履歴情報または在宅者情報を確認することにより、家屋への不正侵入がなされた可能性や、現在家屋内に在宅している者を知ることができる。なお、異常履歴情報は、ＩＤ認証手段がキーユニットの記録手段から正当なＩＤ情報を取得できなかった場合、その履歴を記録しておくことにより作成される。また、在宅者情報はＩＤ認証手段がキーユニットの記録手段から正当なＩＤ情報を取得した場合、その履歴を記録しておくことにより作成される。
【０１２５】
したがって、ユーザは、家屋に入る前に、現在家屋内にどのような者が居るのかを判断することができるので、不正侵入者と鉢合わせして暴行を受けてしまうという事故を防止することができるという効果が奏される。
【産業上の利用可能性】
【０１２６】
以上のように、本発明のサービス提供装置な、効率的に不正侵入者に対する防犯を行うのに適している。さらに、本発明のサービス提供装置は、防犯システムのみならず、工作機械の操作説明サービス、自動的にＰＣの起動時設定を変更するサービス、料理提供サービス、レンタカーの課金サービスなど、種々のサービス分野においてユーザに適したサービスを提供するのにも適している。
【図面の簡単な説明】
【０１２７】
【図１】本発明のサービス提供装置の一実施形態に係るセキュリティ管理装置の構成を示すブロック図である。
【図２】図１のセキュリティ管理装置を用いる防犯システムの概要を示す図である。
【図３】図２の防犯システムにおいて用いられるＩＤ認証端末の構成を示すブロック図である。
【図４】ＩＤ認証端末の好適な構成の一例であるキーユニットの構成を示すブロック図である。
【図５】図１のセキュリティ管理装置における操作検知センサの好適な構成としてのドアノブセンサの構成を示すブロック図である。
【図６】図１のセキュリティ管理装置により実行される処理の流れを示すフローチャートである。
【図７】図１のセキュリティ管理装置により実行される処理の流れを示すフローチャートである。
【図８】従来の防犯システムの一例を示す図である。
【図９】従来の防犯システムの他の例を示す図である。
【符号の説明】
【０１２８】
１　　セキュリティ管理装置（サービス提供装置）
２　　ＩＤ認証端末
３　　操作検知センサ
４　　アクセスセンサ
５　　外部装置
７　　玄関ドア
８　　ドアノブ

１４　通信処理部（無線通信手段）
１５　制御部（制御手段）
１７　ＩＤ認証端末通信部（無線通信手段）
１８　外部装置通信部（無線通信手段）
２１　ＩＤ認証処理部（ＩＤ認証手段）
２２　外部処理決定部（外部処理決定手段）
２３　キーユニット
２４　通信部（ＩＤ情報送信手段）
２６　記録部（記録手段）
２７　表示部（表示手段）
２８　鍵部（キー部分）
２９　トルクセンサ（操作検知センサ）
３０　圧力センサ（操作検知センサ）
４３　コイル
４４　発振部（磁界発生手段）
４５　検波部（検波手段）

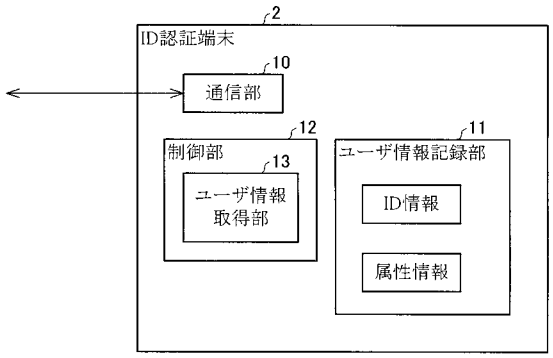
【図１】



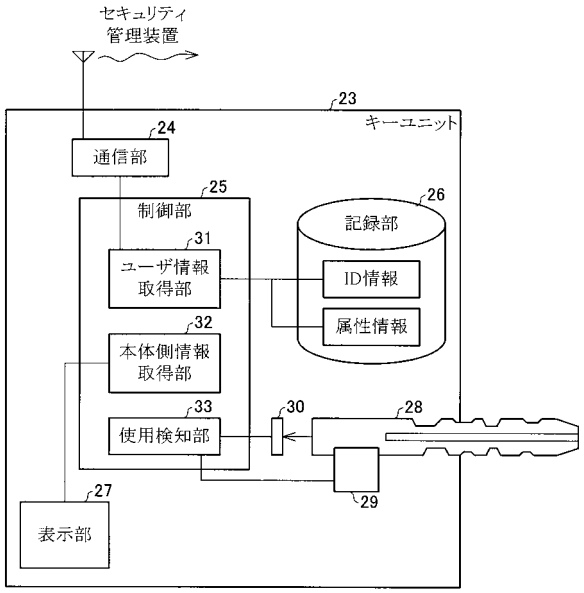
【図２】



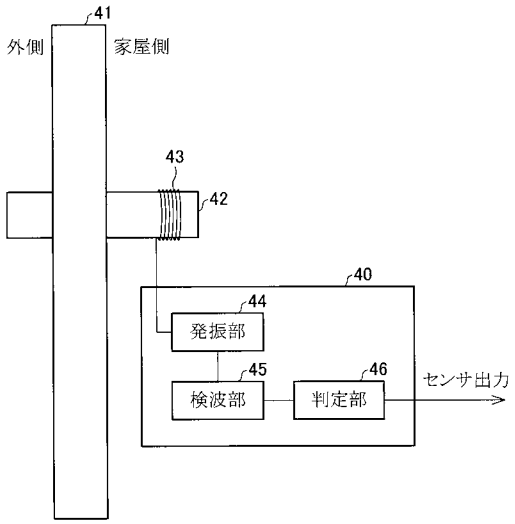
【図３】


2
ID認証端末
10
通信部
12
制御部
13
ユーザ情報取得部
11
ユーザ情報記録部
ID情報
属性情報

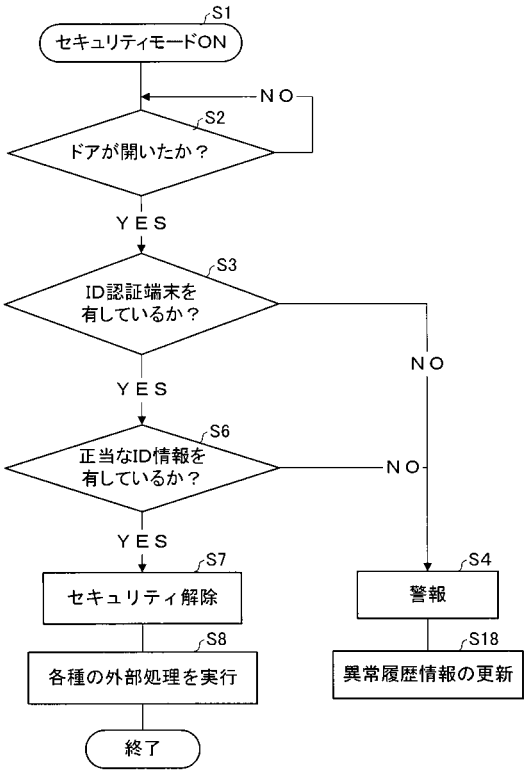
【図４】


セキュリティ管理装置
23
キーユニット
24
通信部
25
制御部
26
記録部
31
ユーザ情報取得部
ID情報
属性情報
32
本体側情報取得部
33
使用検知部
30
28
29
27
表示部

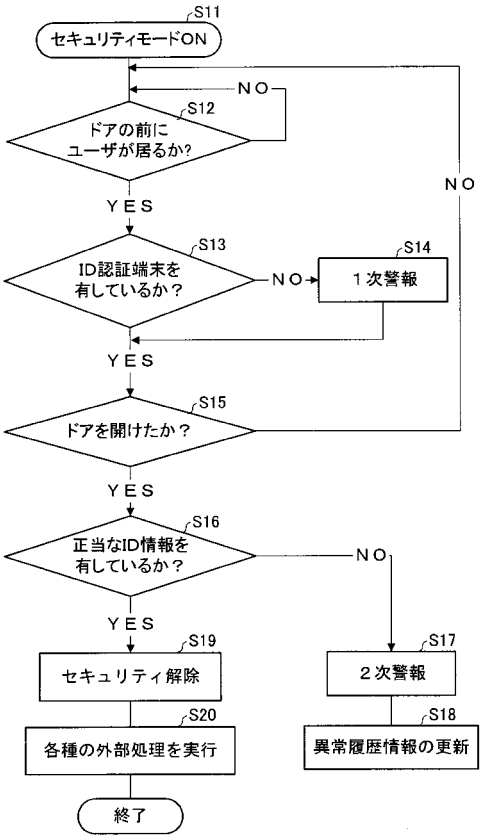
【図５】


41
外側
家屋側
43
42
40
44
発振部
45
検波部
46
判定部
センサ出力

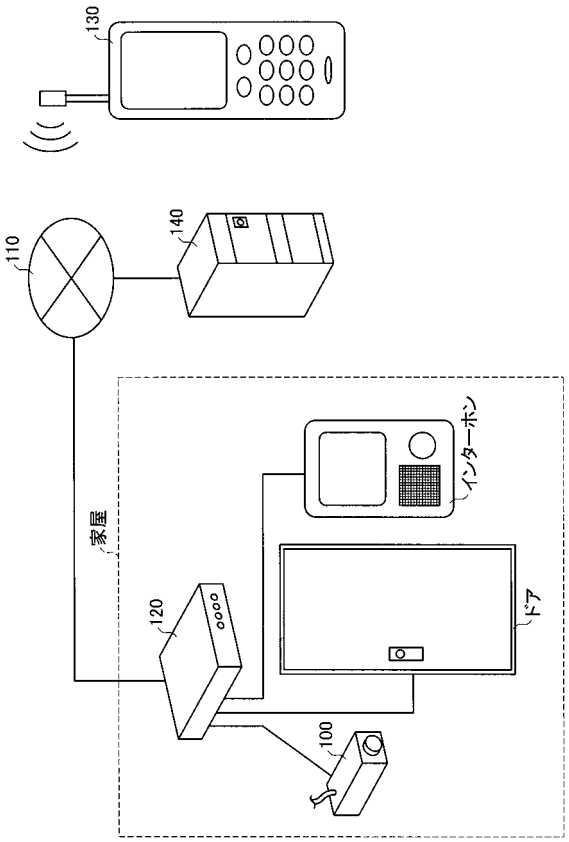
【図６】


S1
セキュリティモードON
NO
S2
ドアが開いたか？
YES
S3
ID認証端末を有しているか？
NO
YES
S6
正当なID情報を有しているか？
NO
YES
S7
セキュリティ解除
S8
各種の外部処理を実行
終了
S4
警報
S18
異常履歴情報の更新

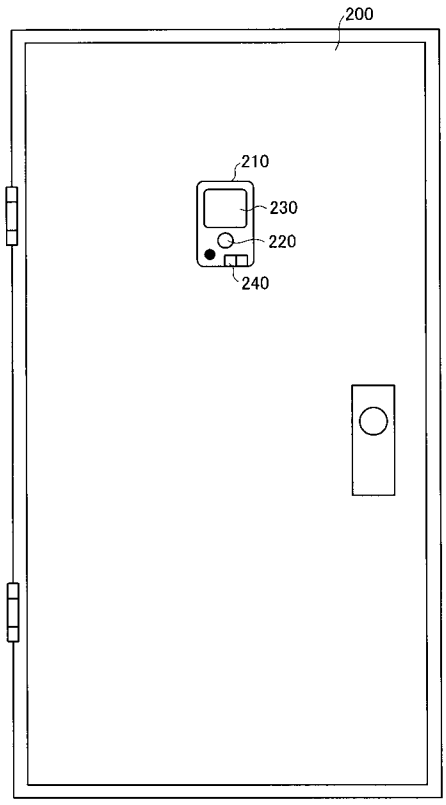
【図７】


S11
セキュリティモードON
NO
S12
ドアの前に
ユーザが居るか?
YES
NO
S13
ID認証端末を
有しているか？
NO
S14
１次警報
YES
S15
ドアを開けたか？
YES
S16
正当なID情報を
有しているか？
NO
YES
S19
セキュリティ解除
S20
各種の外部処理を実行
S17
２次警報
S18
異常履歴情報の更新
終了

【図８】


130
110
140
家屋
インターホン
120
ドア
100

【図９】


200
210
230
220
240

フロントページの続き

(72)発明者　久野　敦司
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内
(72)発明者　小林　秀行
京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内

審査官　▲高▼木　真顕

(56)参考文献　特開昭５６－１２３０９５（ＪＰ，Ａ）
特開２００３－１３８８１７（ＪＰ，Ａ）
特開２００２－３１２８６５（ＪＰ，Ａ）
特開２００２－３２７５６１（ＪＰ，Ａ）
特開２０００－２８５３４２（ＪＰ，Ａ）
実開昭６１－１４６３５８（ＪＰ，Ｕ）
特開２００１－２７９９９９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０８Ｂ１３／００～１５／０２
Ｇ０８Ｂ１９／００～３１／００
Ｈ０４Ｌ　９／００