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

特許第4836675号
(P4836675)

(45)発行日　平成23年12月14日(2011.12.14)　(24)登録日　平成23年10月7日(2011.10.7)

(51)Int.Cl.		F I		
G08B 25/04	(2006.01)	G08B	25/04	H
G08B 25/00	(2006.01)	G08B	25/00	510E
G08B 25/08	(2006.01)	G08B	25/08	C
G08B 25/10	(2006.01)	G08B	25/10	D
H04M 11/04	(2006.01)	H04M	11/04	

請求項の数 13　(全 24 頁)

(21)出願番号　特願2006-161271 (P2006-161271)
(22)出願日　平成18年6月9日 (2006.6.9)
(65)公開番号　特開2007-328719 (P2007-328719A)
(43)公開日　平成19年12月20日 (2007.12.20)
審査請求日　平成21年6月4日 (2009.6.4)

(73)特許権者　000202361
綜合警備保障株式会社
東京都港区元赤坂１丁目６番６号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　小泉　さおり
東京都港区元赤坂１丁目６番６号　綜合警備保障株式会社内
(72)発明者　吉本　誠二
東京都港区元赤坂１丁目６番６号　綜合警備保障株式会社内
(72)発明者　横田　智美
東京都港区元赤坂１丁目６番６号　綜合警備保障株式会社内

最終頁に続く

(54)【発明の名称】警備装置、サーバ装置および監視システム

(57)【特許請求の範囲】

【請求項１】

監視領域における異常を検知し、検知された異常に関する情報をネットワークで接続された通報先端末に通報する警備装置において、

前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、

利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、

前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末にダイヤルすることにより、前記通報先端末を確認する通報先確認手段と、

前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、

を備えることを特徴とする警備装置。

【請求項２】

前記通報先確認手段は、さらにダイヤルに対する前記通報先端末からの応答により、前記通報先端末を確認すること、を特徴とする請求項１に記載の警備装置。

【請求項３】

監視領域における異常を検知し、検知された異常に関する情報をネットワークで接続された通報先端末に通報する警備装置において、

前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、

利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、

前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末に

確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、
前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、
を備えることを特徴とする警備装置。
【請求項４】
前記通報先確認手段は、さらに前記確認メールに対する前記通報先端末の返信メールを受信することにより、前記通報先端末を確認すること、を特徴とする請求項３に記載の警備装置。
【請求項５】
前記通報先格納手段は、さらに前記通報先確認手段によって前記通報先端末が確認されなかった場合に、前記通報先端末情報を前記通報先記憶手段に格納しないこと、を特徴とする請求項１～４のいずれか一つに記載の警備装置。
【請求項６】
前記通報先確認手段は、さらに前記通報先端末から通報の承諾を示す承諾情報を受信することによって前記通報先端末を確認すること、を特徴とする請求項１～５のいずれか一つに記載の警備装置。
【請求項７】
監視領域における異常を検知する警備装置が検知した異常に関する情報をネットワークで接続された通報先端末に送信するサーバ装置において、
前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、
利用者からの入力による前記通報先端末情報を受信する通報先受信手段と、
前記通報先受信手段によって受信された前記通報先端末情報を用いて前記通報先端末に確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、
前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、
を備えることを特徴とするサーバ装置。
【請求項８】
前記通報先確認手段は、さらに前記確認メールに対する前記通報先端末の返信メールを受信することにより、前記通報先端末を確認すること、を特徴とする請求項７に記載のサーバ装置。
【請求項９】
前記通報先格納手段は、さらに前記通報先確認手段によって前記通報先端末が確認されなかった場合に、前記通報先端末情報を前記通報先記憶手段に格納しないこと、を特徴とする請求項７または請求項８に記載のサーバ装置。
【請求項１０】
前記通報先確認手段は、さらに前記通報先端末から通報の承諾を示す承諾情報を受信することによって前記通報先端末を確認すること、を特徴とする請求項７～９のいずれか一つに記載のサーバ装置。
【請求項１１】
監視領域における異常を検知する警備装置と、前記警備装置とネットワークを介して接続され、異常を検知した旨が通報される通報先端末と、を備える監視システムにおいて、
前記警備装置は、
前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、
利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、
前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末にダイヤルすることにより、前記通報先端末を確認する通報先確認手段と、
前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、
を備えることを特徴とする監視システム。
【請求項１２】

監視領域における異常を検知する警備装置と、前記警備装置とネットワークを介して接続され、異常を検知した旨が通報される通報先端末と、を備える監視システムにおいて、
前記警備装置は、
前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、
利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、
前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末に確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、
前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、
を備えることを特徴とする監視システム。

【請求項１３】
監視領域における異常を検知する警備装置と、前記警備装置とネットワークを介して接続され、異常を検知した旨をメールで送信するサーバ装置と、前記サーバ装置とネットワークを介して接続され、前記メールを受信する通報先端末と、を備える監視システムにおいて、
前記サーバ装置は、
前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、
利用者からの入力による前記通報先端末情報を受信する通報先受信手段と、
前記通報先受信手段によって受信された前記通報先端末情報を用いて前記通報先端末に確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、
前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、
を備えることを特徴とする監視システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、警備装置、サーバ装置および監視システムに関するものであり、特に監視領域で検知された異常を通報する通報先の設定に関するものである。
【背景技術】
【０００２】
従来から、監視領域内で異常を検知した場合の警報を監視センタに送信する警備システムが一般に知られている。このシステムにおいては、監視センタでかかる監視装置から送信された警報を受信した場合に、警備会社は警備領域で発生した異常を確認するために、警備員を監視領域に出動させるようにしている。
【０００３】
一方、近年の家庭向け警備システムなどにおいては、通報先として家族の携帯電話や親戚の電話を指定し、異常が発生した際に自己で対処することが可能な警備モードを備えた警備システムや、警備会社に依存しない警備システムが知られている（特許文献１参照）。
【０００４】
【特許文献１】特開２００１－２９７３８４号公報
【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、上記特許文献１に記載された技術では、利用者が通報先を設定する際に誤って使用されていない電話番号や第三者の電話番号などを設定すると、異常の通報を行えなかったり、異常が無関係な第三者に通報されてしまい結果的に利用者が対応することができないという問題があった。
【０００６】
特に、このような警備システムでは、監視センタに通報する場合と異なり、通報先が確

実に通報を受信して対処できるとは限らないため、通報先を複数設定したり、通報先の事情により通報先を変更する場合が考えられることから、前述の問題が発生するおそれがある。

【０００７】

本発明は、上記に鑑みてなされたものであって、利用者が誤った通報先を設定することを防止することができる警備装置、サーバ装置および監視システム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】

【０００８】

上述した課題を解決し、目的を達成するために、請求項１にかかる発明は、監視領域における異常を検知し、検知された異常に関する情報をネットワークで接続された通報先端末に通報する警備装置において、前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末にダイヤルすることにより、前記通報先端末を確認する通報先確認手段と、前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、を備えることを特徴とする。

【０００９】

また、請求項２にかかる発明は、請求項１に記載の警備装置において、前記通報先確認手段は、さらにダイヤルに対する前記通報先端末からの応答により、前記通報先端末を確認すること、を特徴とする。

【００１０】

また、請求項３にかかる発明は、監視領域における異常を検知し、検知された異常に関する情報をネットワークで接続された通報先端末に通報する警備装置において、前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末に確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、を備えることを特徴とする。

【００１１】

また、請求項４にかかる発明は、請求項３に記載の警備装置において、前記通報先確認手段は、さらに前記確認メールに対する前記通報先端末の返信メールを受信することにより、前記通報先端末を確認すること、を特徴とする。

【００１２】

また、請求項５にかかる発明は、請求項１～４のいずれか一つに記載の警備装置において、前記通報先格納手段は、さらに前記通報先確認手段によって前記通報先端末が確認されなかった場合に、前記通報先端末情報を前記通報先記憶手段に格納しないこと、を特徴とする。

【００１３】

また、請求項６にかかる発明は、請求項１～５のいずれか一つに記載の警備装置において、前記通報先確認手段は、さらに前記通報先端末から通報の承諾を示す承諾情報を受信することによって前記通報先端末を確認すること、を特徴とする。

【００１４】

また、請求項７にかかる発明は、監視領域における異常を検知する警備装置が検知した異常に関する情報をネットワークで接続された通報先端末に送信するサーバ装置において、前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、利用者からの入力による前記通報先端末情報を受信する通報先受信手段と、前記通報先受信手段によって受信された前記通報先端末情報を用いて前記通報先端末に確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、前記通報先確認手段によって前記通

報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、を備えることを特徴とする。

【００１５】

また、請求項８にかかる発明は、請求項７に記載のサーバ装置において、前記通報先確認手段は、さらに前記確認メールに対する前記通報先端末の返信メールを受信することにより、前記通報先端末を確認すること、を特徴とする。

【００１６】

また、請求項９にかかる発明は、請求項７または請求項８に記載のサーバ装置において、前記通報先格納手段は、さらに前記通報先確認手段によって前記通報先端末が確認されなかった場合に、前記通報先端末情報を前記通報先記憶手段に格納しないこと、を特徴とする。

【００１７】

また、請求項１０にかかる発明は、請求項７～９のいずれか一つに記載のサーバ装置において、前記通報先確認手段は、さらに前記通報先端末から通報の承諾を示す承諾情報を受信することによって前記通報先端末を確認すること、を特徴とする。

【００１８】

また、請求項１１にかかる発明は、監視領域における異常を検知する警備装置と、前記警備装置とネットワークを介して接続され、異常を検知した旨が通報される通報先端末と、を備える監視システムにおいて、前記警備装置は、前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末にダイヤルすることにより、前記通報先端末を確認する通報先確認手段と、前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、を備えることを特徴とする。

【００１９】

また、請求項１２にかかる発明は、監視領域における異常を検知する警備装置と、前記警備装置とネットワークを介して接続され、異常を検知した旨が通報される通報先端末と、を備える監視システムにおいて、前記警備装置は、前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、利用者からの入力により前記通報先端末情報を取得する通報先取得手段と、前記通報先取得手段によって取得された前記通報先端末情報を用いて前記通報先端末に確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、を備えることを特徴とする。

【００２０】

また、請求項１３にかかる発明は、監視領域における異常を検知する警備装置と、前記警備装置とネットワークを介して接続され、異常を検知した旨をメールで送信するサーバ装置と、前記サーバ装置とネットワークを介して接続され、前記メールを受信する通報先端末と、を備える監視システムにおいて、前記サーバ装置は、前記通報先端末を識別する通報先端末情報を記憶する通報先記憶手段と、利用者からの入力による前記通報先端末情報を受信する通報先受信手段と、前記通報先受信手段によって受信された前記通報先端末情報を用いて前記通報先端末に確認メールを送信することにより、前記通報先端末を確認する通報先確認手段と、前記通報先確認手段によって前記通報先端末が確認された場合に、前記通報先端末情報を前記通報先記憶手段に格納する通報先格納手段と、を備えることを特徴とする。

【発明の効果】

【００２１】

請求項１にかかる発明によれば、通報先取得手段によって、利用者からの入力により通報先端末を識別する通報先端末情報を取得し、通報先確認手段によって、通報先端末情報を用いて通報先端末にダイヤルすることにより通報先端末を確認し、通報先格納手段によ

って、通報先端末が確認された場合に、通報先端末情報を、通報先端末情報を記憶する通報先記憶手段に格納することにより、事前に通報先端末が使用可能な状態であることが確認された上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００２２】

また、請求項２にかかる発明によれば、通報先確認手段は、さらにダイヤルに対する前記通報先端末からの応答により通報先端末を確認することにより、事前に通報先端末の応答があった上で通報先が登録されるため、利用者が誤った通報先を設定することを防止するという効果を奏する。

【００２３】

また、請求項３にかかる発明によれば、通報先取得手段によって、利用者からの入力により通報先端末を識別する通報先端末情報を取得し、通報先確認手段によって、通報先端末情報を用いて通報先端末に確認メールを送信することにより通報先端末を確認し、通報先格納手段によって、通報先端末が確認された場合に、通報先端末情報を、通報先端末情報を記憶する通報先記憶手段に格納することにより、事前に通報先端末が使用可能な状態であることが確認された上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００２４】

また、請求項４にかかる発明によれば、通報先確認手段は、さらに確認メールに対する通報先端末の返信メールを受信することにより通報先端末を確認することにより、事前に通報先端末の返信メールを受信した上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００２５】

また、請求項５にかかる発明によれば、通報先格納手段は、さらに通報先端末が確認されなかった場合に、通報先端末情報を通報先記憶手段に格納しないことにより、事前に通報先端末が使用可能な状態にない場合や第三者のものである場合などに通報先が登録されることがないため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００２６】

また、請求項６にかかる発明によれば、通報先確認手段は、さらに通報先端末から通報の承諾を示す承諾情報を受信することによって通報先端末を確認することにより、通報先から異常検知時に通報することを承諾された場合にのみ通報先が登録されるため、利用者が誤った通報先を設定することを防止するとともに、利用者が事前に確認を取っていない親戚等を通報先として設定することを防止することができるという効果を奏する。

【００２７】

また、請求項７にかかる発明によれば、通報先受信手段によって、利用者からの入力による通報先端末を識別する通報先端末情報を受信し、通報先確認手段によって、通報先端末情報を用いて通報先端末に確認メールを送信することによって通報先端末を確認し、通報先格納手段によって、通報先端末が確認された場合に、通報先端末情報を、通報先端末情報を記憶する通報先記憶手段に格納することにより、事前に通報先端末が使用可能な状態にあることが確認された上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００２８】

また、請求項８にかかる発明によれば、通報先確認手段は、さらに確認メールに対する通報先端末の返信メールを受信することによって通報先端末を確認することにより、事前に通報先端末の返信メールを受信した上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００２９】

また、請求項９にかかる発明によれば、通報先格納手段は、さらに通報先端末が確認されなかった場合に、通報先端末情報を通報先記憶手段に格納しないことにより、事前に通

報先端末が使用可能な状態にない場合や第三者のものである場合に通報先が登録されることがないため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００３０】

また、請求項１０にかかる発明によれば、通報先確認手段は、さらに通報先端末から通報の承諾を示す承諾情報を受信することによって通報先端末を確認することにより、通報先から異常検知時に通報することを承諾された場合にのみ通報先が登録されるため、利用者が誤った通報先を設定することを防止するとともに、利用者が事前に確認を取っていない親戚等を通報先として設定することを防止することができるという効果を奏する。

【００３１】

また、請求項１１にかかる発明によれば、通報先取得手段によって、利用者からの入力により通報先端末を識別する通報先端末情報を取得し、通報先確認手段によって、通報先端末情報を用いて通報先端末にダイヤルすることにより通報先端末を確認し、通報先格納手段によって、通報先端末が確認された場合に、通報先端末情報を、通報先端末情報を記憶する通報先記憶手段に格納することにより、事前に通報先端末が使用可能な状態にあることが確認された上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００３２】

また、請求項１２にかかる発明によれば、通報先取得手段によって、利用者からの入力により通報先端末を識別する通報先端末情報を取得し、通報先確認手段によって、通報先端末情報を用いて通報先端末に確認メールを送信することにより通報先端末を確認し、通報先格納手段によって、通報先端末が確認された場合に、通報先端末情報を、通報先端末情報を記憶する通報先記憶手段に格納することにより、事前に通報先端末が使用可能な状態にあることが確認された上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【００３３】

また、請求項１３にかかる発明によれば、通報先受信手段によって、利用者からの入力による、通報先端末を識別する通報先端末情報を受信し、通報先確認手段によって、通報先端末情報を用いて通報先端末に確認メールを送信することによって通報先端末を確認し、通報先格納手段によって、通報先端末が確認された場合に、通報先端末情報を、通報先端末情報を記憶する通報先記憶手段に格納することにより、事前に通報先端末が使用可能な状態にあることが確認された上で通報先が登録されるため、利用者が誤った通報先を設定することを防止することができるという効果を奏する。

【発明を実施するための最良の形態】

【００３４】

以下に添付図面を参照して、本発明にかかる警備装置、サーバ装置および監視システムの最良な実施の形態を詳細に説明する。なお、本発明はこれらの実施の形態に限定されるものではない。

【００３５】

（第１の実施の形態）

第１の実施の形態について、添付図面を参照して説明する。第１の実施の形態にかかる警備装置は、監視領域で異常を検知した場合に通報する通報先として、確実に通報可能で、かつ承諾を得た通報先のみを登録するものである。

【００３６】

まず、本発明が適用される警備装置を含む監視システムの構成例について説明する。図１は、第１の実施の形態にかかる監視システムの構成を示すブロック図である。

【００３７】

本実施の形態にかかる監視システム１０は、警備装置１００と、通報先端末２０１～２０３と、監視センタ３００と、を備えており、警備装置１００と、通報先端末２０１～２０３と、監視センタ３００とは電話回線、無線ネットワーク、インターネットなどのネッ

トワーク４００を介して接続されている。

【００３８】

通報先端末２０１～２０３は、図示しない送受信部、制御部、表示部、操作部、音声通話部などから構成されており、公知の携帯電話や固定電話と同様の構成である。送受信部は、ネットワーク４００から無線または有線でデータの送受信を行う。制御部は通報先端末２０１～２０３の各種の制御を行う。表示部は、送信されたデータまたは入力されたデータの表示を行い、操作部は、データの入力を行う。音声通話部は、警備装置１００から送信される通報先を確認する情報を音声データとして受信し出力するとともに、在宅者との音声通話またはデータ入力を行う。なお、通報先端末２０１～２０３は、公知のＰＤＡ（Personal Digital Assistants）を用いてもよい。

【００３９】

監視センタ３００は、警備装置１００のセンサ１０１が異常を検知し、警報が送信された場合に、待機中の警備員に対して異常が検知された監視領域へ向かう旨の指示を出すとともに、必要に応じて警察や消防など関係機関への通報を行うセンタである。

【００４０】

本実施の形態にかかる警備装置１００は、センサ１０１と、操作部１０２と、出力部１０３と、制御部１１０と、認証データベース１２０と、通報先データベース１３０とを備えている。

【００４１】

センサ１０１は、人感センサであり、たとえば赤外線の受光量の変化をもとに人の存在を検出する赤外線センサ、赤外線などの受信が遮断されることで人の存在を検出する遮断センサ、電磁波の乱れで人の存在を検知する気配センサ、およびマグネットにより扉の開閉を検出するマグネットセンサなどの監視領域の異常を検出する各種センサであり、監視領域への侵入者を検知するなどの目的で設置されたものである。

【００４２】

操作部１０２は、利用者ＩＤやパスワードなどの認証情報や通報先の電話番号やメールアドレスを入力するものである。例えば、テンキー、タッチパネル、カードリーダ、指紋照合装置などの生体認証装置などが必要に応じて設けられている。また、操作部１０２は、警備装置１００に対する警備モードを設定するものである。警備モードとは、監視領域において異常を検知したときの警備装置１００の動作を決定するモードである。具体的には、警備状態、在宅警備状態、セルフ警備状態、警備解除状態があり、操作部１０２によって、いずれかの状態に設定される。

【００４３】

ここで、警備状態とは、センサ１０１によって異常を検知したときに発せられる検知情報を警備装置１００が取得した場合に、異常を知らせる警報を監視センタ３００に通報する状態である。在宅警備状態とは、センサ１０１によって異常を検知したときに発せられる検知情報を警備装置１００が取得した場合に、監視領域、例えば警備装置が設定されている住宅やオフィス等で異常を検知したことを報知する状態である。また、監視領域だけではなく警報を監視センタ３００に報知する場合もある。

【００４４】

セルフ警備状態とは、センサ１０１によって異常を検知したときに発せられる検知情報を警備装置が取得した場合に、携帯電話や固定電話などの通報先端末に異常を検知したことを通報する状態である。

【００４５】

警備解除状態とは、センサ１０１によって異常を検知したときに発せられる検知情報を警備装置１００が取得した場合でも、監視センタ３００への警報の通報、監視領域における異常の報知、通報先端末への異常の通報のいずれも行わない状態である。なお、上述したモードのいずれであっても、検知された異常が火災やガス漏れの場合、または、非常ボタンが操作された場合は、監視センタ３００への通報を行い、必要に応じて監視領域における異常の検知、通報先端末への異常の通報などを行う。

【００４６】
出力部１０３は、通報先の承認状況等を文字で表示し、音声で出力するものである。例えば、液晶パネルやスピーカなどが必要に応じて設けられている。
【００４７】
認証データベース１２０は、警備装置１００における認証情報を規定する。図２は、認証データベースのデータ構成の一例を示す説明図である。認証データベース１２０は、利用者ＩＤと、パスワードとを対応付けて記憶している。例えば、図２に示すように、利用者ＩＤとして“００１”、その利用者ＩＤに対応するパスワードとして“１２３４”が格納されている。
【００４８】
通報先データベース１３０は、警備装置１００が異常を検知した場合に通報する通報先情報を規定する。図３は、通報先データベースのデータ構成の一例を示す説明図である。通報先データベース１３０は、通報先情報を記憶している。例えば、通報先情報として通報先端末の電話番号“０９０－ＸＸＸＸ－○○○○”が格納されている。
【００４９】
制御部１１０は、さらに検知情報取得部１１１と、操作情報取得部１１２と、出力制御部１１３と、警備モード切替部１１４と、認証部１１５と、通報先情報記憶部１１６と、警備モード記憶部１１７と、通報先確認部１１８と、警報送信部１１９と、を備えている。
【００５０】
検知情報取得部１１１は、センサ１０１によって異常を検知したときに発せられる検知情報を取得するものである。操作情報取得部１１２は、操作部１０２によって入力された利用者ＩＤやパスワード等の認証情報や通報先の電話番号やメールアドレス、警備モードなどの操作情報を取得するものである。出力制御部１１３は、文字メッセージや音声メッセージを出力部１０３に出力する制御を行うものである。
【００５１】
警備モード切替部１１４は、操作部１０２によって設定された警備モードに従って、現在の警備モードを警備状態、在宅警備状態、セルフ警備状態または警備解除状態のいずれかに切替えるものである。
【００５２】
認証部１１５は、操作部１０２によって入力された利用者ＩＤおよびパスワードの認証情報と認証データベース１２０に登録されている認証情報とを照合することにより、操作を行っている利用者を認証するものである。
【００５３】
通報先情報記憶部１１６は、操作部１０２から入力された通報先情報を一時的に記憶するメモリなどの記憶媒体である。警備モード記憶部１１７は、現在の警備モードを記憶するメモリなどの記憶媒体である。
【００５４】
通報先確認部１１８は、操作部１０２から入力された通報先情報または通報先情報記憶部１１６に一時的に記憶されている通報先情報が示す通報先に対して、電話回線が接続されるか否かを確認するとともに、異常検知時に通報されることを承諾するか否かの確認を行い、承諾されたと判断した場合に通報先情報を通報先データベース１３０に格納するものである。通報先確認部１１８は、本発明における通報先確認手段および通報先格納手段を構成するものである。
【００５５】
警報送信部１１９は、検知情報取得部１１１によって検知情報が検知されたときに、警備モード記憶部１１７に記憶された現在の警備モードが“警備状態”の場合に警報を監視センタに送信するものである。
【００５６】
次に、以上のように構成されている警備装置１００による通報承諾確認処理について説

明する。図４－１、図４－２は、操作情報取得部、出力制御部、認証部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。

【００５７】

まず、操作情報取得部１１２は、操作部１０２によって入力された認証情報、すなわち利用者ＩＤとパスワードを取得する（ステップＳ４０１）。図５は、認証情報が入力される操作部の画面の一例を示す説明図である。例えば、図５に示すような画面を液晶パネルに表示し、テンキーの液晶表示から利用者ＩＤ“００１”と、パスワード“１２３４”を入力する。上述したように液晶パネルで文字メッセージを表示するほか、操作ガイドを音声で出力してもよい。また、操作部１０２を液晶パネルではなくテンキーボタンとし、音声メッセージによる操作ガイドに従って、テンキーを押下して利用者ＩＤとパスワードを入力するようにしてもよい。

【００５８】

認証部１１５は、操作部１０２によって入力された利用者ＩＤとパスワードと、認証データベース１２０に格納されている認証情報、すなわち利用者ＩＤとパスワードとを照合する（ステップＳ４０２）。認証部１１５は、照合結果が一致するか否か、すなわち認証されたか否かを判断する（ステップＳ４０３）。認証されていないと判断した場合には（ステップＳ４０３：Ｎｏ）、ステップＳ４０１に戻る。

【００５９】

認証されたと判断した場合には（ステップＳ４０３：Ｙｅｓ）、操作情報取得部１１２は操作部１０２によって入力された通報先情報である通報先電話番号を取得する（ステップＳ４０４）。図６は、通報先設定の画面の一例を示す説明図である。上述したように操作部１０２をテンキーとして、操作ガイドを音声で出力してもよい。通報先確認部１１８は、取得された通報先電話番号にダイヤルする（ステップＳ４０５）。通報先確認部１１８は、通報先にダイヤルできたか否かを判断する（ステップＳ４０６）。

【００６０】

通報先にダイヤルできないと判断した場合には（ステップＳ４０６：Ｎｏ）、出力制御部１１３を制御し、出力部１０３から通報先にダイヤルできなかった旨を出力する（ステップＳ４０７）。その後、ステップＳ４１６に進む。ここで、通話先にダイヤルできない場合とは、発呼できずに通話先電話番号が使用されていない旨のメッセージが出力される場合や、都合により回線を接続できない旨のメッセージが出力された場合をいう。通報先にダイヤルができたと判断した場合には（ステップＳ４０６：Ｙｅｓ）、通報先確認部１１８は通報先から応答があるか否かを判断する（ステップＳ４０８）。通報先から応答がないと判断した場合は（ステップＳ４０８：Ｎｏ）、出力制御部１１３を制御し、出力部１０３から通報先から応答がなかった旨を出力する（ステップＳ４０９）。その後、ステップＳ４１６に進む。ここで、通報先から応答がなかった場合とは、発呼したが通報先との回線が接続されない場合や、通報先の携帯電話の電源がＯＦＦにされている、または通報先の携帯電話に電波が届かない旨のメッセージが出力され、回線が接続されない場合をいう。なお、通報先の応答がない場合、適当な時間をおいて再ダイヤルするようにしてもよい。通報先から応答があったと判断した場合は（ステップＳ４０８：Ｙｅｓ）、通報先確認部１１８は異常検知時に異常を通報することの承諾を求める音声メッセージを送信する（ステップＳ４１０）。例えば、“承諾の場合は１を、不承諾の場合は２を入力してください”との音声情報を送信する。

【００６１】

通報先確認部１１８は、通報先から承諾または不承諾の情報を受信する（ステップＳ４１１）。例えば、相手先の携帯電話から“１”または“２”が入力されることにより、警備装置１００側は承諾または不承諾の情報を受信することになる。なお、文字入力によるほか、“承諾します”または“承諾しません”という音声の入力を受付け、音声判定により承諾または不承諾を判断してもよい。また、携帯電話で何も操作されず電話回線を切断された場合は不承諾と判断するようにしてもよい。

【００６２】

通報先確認部１１８は、承諾されたか否かを判断する（ステップＳ４１２）。上述した場合を例とすると、“１”が受信された場合は承諾されたと判断し、“２”が受信された場合には承諾されていないと判断する。承諾されたと判断した場合には（ステップＳ４１２：Ｙｅｓ）、通報先データベース１３０に通報先電話番号を格納する（ステップＳ４１３）。出力部１０３は、通報先設定完了のメッセージを出力する（ステップＳ４１４）。図７は、通報先が設定された場合の出力画面の一例を示す説明図である。図７に示すような文字表示に代えて、または文字表示とともに音声出力してもよい。

【００６３】

承諾されていないと判断した場合には（ステップＳ４１２：Ｎｏ）、出力制御部１１３を制御し、通報先に承認を得られなかった旨を出力部１０３から出力する（ステップＳ４１５）。その後、ステップＳ４１６に進む。

【００６４】

通報先確認部１１８は、通報先の設定が終了したか否かを判断する（ステップＳ４１６）。通報先の設定が終了したと判断した場合には（ステップＳ４１６：Ｙｅｓ）、例えば操作部１０２で終了のボタンが押下された場合には、処理を抜ける。通報先の設定が終了していないと判断した場合には（ステップＳ４１６：Ｎｏ）、ステップＳ４０４に戻り、さらに通報先電話番号を取得する。

【００６５】

このように、利用者が登録しようとする通報先に対しダイヤルできた場合であって、なおかつダイヤルに対して応答があり、通報先の登録につき、承諾された場合にのみ通報先情報が登録されるため、誤った通報先情報が登録されることを防止することができる。また、利用者が事前に確認を取っていない親戚等を通報先として設定することを防止することができる。

【００６６】

なお、本実施の形態では、通報先の登録を行うために、ダイヤルできたか否か、ダイヤルに対して応答があったか否か、通報先の登録につき承諾されたか否かを段階に分けて判断しているが、適宜いずれか一つまたは二つの判断のみを行うようにしてもよい。

【００６７】

また、他の例として、通報先を複数入力した場合の通報承諾確認処理について説明する。図８－１、図８－２は、操作情報取得部、出力制御部、認証部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。

【００６８】

まず、認証処理については、上述した図４のステップＳ４０１～ステップＳ４０３の処理と同様であるため、上述した説明を参照し、ここでの説明を省略する。

【００６９】

ステップＳ８０３において、認証されたと判断した場合には（ステップＳ８０３：Ｙｅｓ）、操作情報取得部１１２は操作部１０２によって入力された通報先情報である通報先電話番号を取得し、通報先情報記憶部１１６に格納する（ステップＳ８０４）。操作情報取得部１１２は、通報先情報の設定が終了したか否かを判断する（ステップＳ８０５）。通報先情報の設定が終了していないと判断した場合には（ステップＳ８０５：Ｎｏ）、ステップＳ８０４に戻り、さらに通報先情報を取得する。

【００７０】

通報先情報の設定が終了したと判断した場合には（ステップＳ８０５：Ｙｅｓ）、通報先確認部１１８は通報先情報記憶部１１６に格納された通話先電話番号を取得する（ステップＳ８０６）。通報先確認部１１８は、通報先情報記憶部１１６から取得された通報先電話番号にダイヤルする（ステップＳ８０７）。通報先確認部１１８は、通報先にダイヤルできたか否かを判断する（ステップＳ８０８）。

【００７１】

通報先にダイヤルできないと判断した場合には（ステップＳ８０８：Ｎｏ）、ステップＳ８１４に進む。通報先にダイヤルできたと判断した場合には（ステップＳ８０８：Ｙｅ

ｓ）、通報先確認部１１８は通報先から応答があるか否かを判断する（ステップＳ８０９）。通報先から応答がないと判断した場合は（ステップＳ８０９：Ｎｏ）、ステップＳ８１５に進む。なお、通報先の応答がない場合には、上述した場合と同様に、適当な時間をおいて再ダイヤルするようにしてもよい。通報先から応答があると判断した場合は（ステップＳ８０９：Ｙｅｓ）、通報先確認部１１８は通報先としての承諾を求める音声メッセージを送信する（ステップＳ８１０）。

【００７２】

通報先確認部１１８は、通報先から承諾または不承諾の情報を受信する（ステップＳ８１１）。通報先確認部１１８は、承認されたか否かを判断する（ステップＳ８１２）。承認されたと判断した場合には（ステップＳ８１２：Ｙｅｓ）、通報先データベース１３０に通報先電話番号を格納する（ステップＳ８１３）。通報先確認部１１８は、通報先情報記憶部１１６に格納された通報先電話番号が終了したか否かを判断する（ステップＳ８１４）。通報先情報記憶部１１６に格納された通報先電話番号が終了していないと判断した場合には（ステップＳ８１４：Ｎｏ）、ステップＳ８０６に戻り、さらに通報先情報記憶部１１６に格納された通報先電話番号を取得する。

【００７３】

通報先情報記憶部１１６に格納された通報先電話番号が終了したと判断した場合には（ステップＳ８１４：Ｙｅｓ）、出力制御部１１３を制御し、出力部１０３に通報先設定状況を出力する（ステップＳ８１５）。例えば、複数の通報先情報を設定した場合に、通報先電話番号ごとに設定されたか否かを音声または画面表示によって出力する。さらに、通報先電話番号が設定されなかった場合に、回線が接続されなかったため設定されなかったのかまたは承諾されなかったため設定されなかったのか等の情報を出力してもよい。

【００７４】

通報先確認部１１８は、通報先の設定が終了したか否かを判断する（ステップＳ８１６）。通報先の設定が終了したと判断した場合には（ステップＳ８１６：Ｙｅｓ）、例えば操作部１０２で終了のボタンが押下された場合には、処理を抜ける。通報先の設定が終了していないと判断した場合には（ステップＳ８１６：Ｎｏ）、ステップＳ８０４に戻り、さらに通報先電話番号を取得する。

【００７５】

（第２の実施の形態）

第２の実施の形態について、添付図面を参照して説明する。第２の実施の形態にかかるサーバ装置は、警備装置が検知した異常の通報を、通報先にサーバ装置を介してメールで行う場合に、通報先として確実に通報可能でかつ承諾を得た通報先のみを登録するものである。

【００７６】

本発明が適用されるサーバ装置を含む監視システムの構成例について、第１の実施の形態を異なる部分を説明する。他の部分については第１の実施の形態と同様であるので、上述した説明を参照し、ここでの説明を省略する。図９は、第２の実施の形態にかかる監視システムの構成を示すブロック図である。

【００７７】

本実施の形態にかかる監視システム２０は、警備装置１００と、通報先端末２０１、２０３、２０４と、監視センタ３００と、サーバ装置５００とを備えており、警備装置１００と、通報先端末２０１、２０３、２０４と、監視センタ３００と、サーバ装置５００とは電話回線、無線ネットワーク、インターネットなどのネットワーク４００を介して接続されている。なお、本実施の形態では、通報先端末２０１、２０３、２０４と通報先を設定する端末を兼ねているが、必ずしも通報先端末２０１、２０３、２０４で通報先を設定する必要はなく、通報先端末２０１、２０３、２０４以外の端末から設定してもよい。

【００７８】

ここで、警備装置１００と、通報先端末２０１、２０３と、監視センタ３００の構成、機能は、第１の実施の形態と同様であるので、説明を省略する。また、本実施の形態では

、監視領域内での異常を通報するためにメールを利用するので、通報先端末は図９の通報先端末２０４に示すようなパーソナルコンピュータでもよい。なお、警備装置１００は、上述した通報承諾確認設定処理を行う部分を備えない警備装置でもよい。

【００７９】

サーバ装置５００は、制御部５１０と、認証データベース５２０と、通報先データベース５３０とを備える。認証データベース５２０は、通報先端末２０１、２０３、２０４からの通報先の設定を可能とする認証情報を規定する。図１０は、認証データベースのデータ構成の一例を示す説明図である。認証データベース５２０は、利用者ＩＤと、パスワードと、警備装置ＩＤとを対応付けて記憶している。例えば、利用者ＩＤとして“００１”、パスワードとして“ＰＷ１２３４”、警備装置ＩＤとして“Ｋ００１”が格納されている。

【００８０】

通報先データベース５３０は、警備装置１００が異常を検知した場合に通報する通報先情報を規定する。図１１は、通報先データベースのデータ構成の一例を示す説明図である。通報先データベース５３０は、警備装置ＩＤと、通報先情報とを対応付けて記憶している。例えば、警備装置ＩＤとして“Ｋ００１”、通報先情報として通報先端末のメールアドレス“ｍａｉｌ０１@ｘｘｘ．ｎｅ．ｊｐ”が格納されている。

【００８１】

制御部５１０は、さらにデータ送受信部５１１と、メール送受信部５１２と、タイマ部５１３と、認証部５１４と、メール生成部５１５と、通報先確認部５１６とを備える。

【００８２】

データ送受信部５１１は、通報先端末２０１、２０３、２０４によって送信された認証情報を受信し、認証部５１４での認証結果を通報先端末２０１、２０３、２０４に送信するものである。また、データ送受信部５１１は、通報先端末２０１、２０３、２０４によって送信されたメールアドレスを受信するものである。データ送受信部５１１は、通報先確認部５１６による通報承諾結果を通報先端末２０１、２０３、２０４に送信するものである。

【００８３】

メール送受信部５１２は、メール生成部５１５によって生成された通報承諾確認メールを通報先情報が示す通報先に送信し、通報先から送信された通報承諾返信メールを受信するものである。

【００８４】

タイマ部５１３は、メール送受信部５１２によって通報承諾確認メールが送信された時点からの時間を計測するものである。認証部５１４は、通報先端末２０１、２０３、２０４から送信された認証情報と認証データベース５２０とを照合することによって利用者を認証するとともに、認証情報に対応する警備装置を特定するものである。

【００８５】

メール生成部５１５は、データ送受信部５１１によって受信されたメールアドレスに対する通報承諾確認メールを生成するものである。通報先確認部５１６は、メール送受信部５１２によって受信された通報先からの通報承諾返信メールに基づいて、通報先が通報を承諾したか否かを判断し、承諾した場合は通報先データベース５３０にメールアドレスを通報先情報として格納するものである。通報先確認部５１６は、本発明における通報先確認手段および通報先格納手段を構成するものである。

【００８６】

次に、以上のように構成されているサーバ装置５００による通報承諾確認処理について説明する。図１２－１、図１２－２、図１２－３は、データ送受信部、メール送受信部、タイマ部、認証部、メール生成部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。ここでは、通報先端末である携帯電話２０１から通報先を設定する場合を一例として説明する。

【００８７】

まず、携帯電話２０１からサーバ装置５００のホームセキュリティのＷｅｂサイトにアクセスする（ステップＳ１２０１）。サーバ装置５００は、携帯電話２０１にＷｅｂサイトの画面データを送信する（ステップＳ１２０２）。携帯電話２０１は、入力部によって入力された認証情報を取得する（ステップＳ１２０３）。図１３は、認証情報入力画面の一例を示す説明図である。例えば、図１３に示すように、利用者ＩＤとして“００１”、パスワードとして“ＰＷ１２３４”を入力する。携帯電話２０１は、認証情報をサーバ装置５００に送信する（ステップＳ１２０４）。

【００８８】

サーバ装置５００において、データ送受信部５１１は、携帯電話２０１から送信された認証情報を受信する（ステップＳ１２０５）。認証部５１４は、送信された認証情報と、認証データベース５２０に格納された認証情報とを照合する（ステップＳ１２０６）。認証部５１４は、照合結果が一致するか否かにより、認証されたか否かを判断する（ステップＳ１２０７）。認証されなかったと判断した場合には（ステップＳ１２０７：Ｎｏ）、処理を終了する。なお、携帯電話２０１に認証されなかった旨のメッセージを送信し、携帯電話２０１側でメッセージを表示してもよい。

【００８９】

認証されたと判断した場合には（ステップＳ１２０７：Ｙｅｓ）、データ送受信部５１１はメールアドレス入力画面を送信する（ステップＳ１２０８）。携帯電話２０１は、メールアドレス入力画面を受信し、表示する（ステップＳ１２０９）。携帯電話２０１は、入力されたメールアドレスを取得する（ステップＳ１２１０）。図１４は、メールアドレス入力画面の一例を示す説明図である。なお、メールアドレスの取得は、１つずつでも複数でもよい。携帯電話２０１は、メールアドレスをサーバ装置５００に送信する（ステップＳ１２１１）。

【００９０】

サーバ装置５００において、データ送受信部５１１は、携帯電話２０１から送信されたメールアドレスを受信する（ステップＳ１２１２）。メール生成部５１５は、受信したメールアドレスに対して異常検知時の通報を承諾するか否かの通報承諾確認メールを生成する（ステップＳ１２１３）。なお、携帯電話２０１自体を通報先とする場合は、通報承諾確認メールを送信することなく、通報先としてもよい。メール送受信部５１２は、メール生成部５１５によって生成された通報承諾確認メールを送信する（ステップＳ１２１４）。メール送受信部５１２は、通報承諾確認メールを送信できたか否かを判断する（ステップＳ１２１５）。通報承諾確認メールを送信できなかったと判断した場合は（ステップＳ１２１５：Ｎｏ）、ステップＳ１２２１に進む。ここで、通報承諾確認メールを送信できなかった場合とは、図示しないメールサーバから応答するメールアドレスが存在しない旨のメール、またはメールの受信を拒否された旨のメールが返信された場合をいう。通報承諾確認メールを送信できたと判断した場合は（ステップＳ１２１５：Ｙｅｓ）、タイマ部５１３は所定時間が経過したか否かを判断する（ステップＳ１２１６）。所定時間が経過していないと判断した場合には（ステップＳ１２１６：Ｎｏ）、ステップＳ１２１６に戻り、所定時間が経過するまで計測を繰り返す。

【００９１】

所定時間が経過したと判断した場合には（ステップＳ１２１６：Ｙｅｓ）、通報承諾確認メールに対する通報承諾返信メールを受信したか否かを判断する（ステップＳ１２１７）。通報承諾返信メールか否かは、通報承諾返信メールの宛先アドレスが通報承諾確認メールの送信元アドレスであり、通報承諾返信メールの送信元アドレスが通報承諾確認メールの宛先アドレスであることによって確認することができる。通報承諾確認メールに対する通報承諾返信メールを受信したと判断した場合には（ステップＳ１２１７：Ｙｅｓ）、通報先確認部５１６は通報承諾返信メールの本文から通報承諾の有無を判断する（ステップＳ１２１８）。例えば、承諾ならば“１”を入力し、承諾しないならば“２”を入力するように指示した場合には、その値で判断することができる。なお、通報承諾確認メールに対して返信することによって、承諾と判断するようにしてもよい。ステップＳ１２１７

において、通報承諾確認メールに対する通報承諾返信メールが１つも受信されていないと判断した場合には（ステップＳ１２１７：Ｎｏ）、ステップＳ１２２１に進む。なお、通報承諾返信メールが受信されない場合、適当な時間をおいて再度通報承諾確認メールを送信するようにしてもよい。

【００９２】

通報先から送信された通報承諾返信メールから異常検知時の通報が承諾されたと判断した場合には（ステップＳ１２１９：Ｙｅｓ）、通報先確認部５１６は警備装置ＩＤごとにメールアドレスを通報先データベース５３０に格納する（ステップＳ１２２０）。警備装置ＩＤは、認証データベース５２０に格納されているため、認証時に認証情報によって特定することができる。通報先として承諾されていないと判断した場合には（ステップＳ１２１９：Ｎｏ）、ステップＳ１２２１に進む。データ送受信部５１１は、異常検知時の通報先の承諾結果を携帯電話２０１に送信する（ステップＳ１２２１）。

【００９３】

携帯電話２０１は、サーバ装置５００から送信された異常検知時の通報先の承諾結果を受信する（ステップＳ１２２２）。携帯電話２０１は、異常検知時の通報先の承諾結果を音声や画面表示によって出力する（ステップＳ１２２３）。

【００９４】

このように、警備装置１００において監視領域で異常を検知した場合に、サーバ装置を介して通報先にメールで通報する監視システムにおいても、利用者が登録しようとするメールアドレスに対し、通報承諾確認メールが送信できた場合であって、なおかつ通報承諾確認メールに対する通報確認返信メールを受信し、通報承諾があった場合にのみ通報先情報が登録されるため、利用者が誤った通報先を登録することを防止することができる。また、利用者が事前に確認を取っていない親戚等を通報先として設定することを防止することができる。

【００９５】

なお、本実施の形態では、通報先の登録を行うために、通報承諾確認メールを送信できたか否か、通報承諾確認メールに対する通報承諾返信メールを受信したか否か、通報先の登録につき承諾されたか否かを段階を分けて判断しているが、適宜いずれか一つまたは二つの判断のみ行うようにしてもよい。

【００９６】

（第３の実施の形態）

第３の実施の形態について、添付図面を参照して説明する。第３の実施の形態にかかる警備装置は、上述した第２の実施の形態におけるサーバ装置が行っていたメールによる通報承認確認処理を警備装置が行うものである。

【００９７】

本発明が適用される警備装置を含む監視システムの構成例について、上述した実施の形態と異なる部分を説明する。他の部分については第１または第２の実施の形態と同様であるので、上述した説明を参照し、ここでの説明を省略する。図１５は、第３の実施の形態にかかる監視システムの構成を示すブロック図である。

【００９８】

本実施の形態にかかる監視システム３０は、警備装置１５００と、通報先端末２０１、２０３、２０４と、監視センタ３００と、を備えており、警備装置１５００と、通報先端末２０１、２０３、２０４と、監視センタ３００とは電話回線、無線ネットワーク、インターネットなどのネットワーク４００を介して接続されている。

【００９９】

本実施の形態にかかる警備装置１５００は、センサ１０１と、操作部１０２と、出力部１０３と、制御部１５１０と、認証データベース１２０と、通報先データベース１５３０とを備えている。ここで、センサ１０１と、操作部１０２と、出力部１０３と、認証データベース１２０の構成、機能は、第１の実施の形態と同様であるので、説明を省略する。

【０１００】

通報先データベース１５３０は、警備装置１５００が異常を検知した場合に通報する通報先情報を規定する。図１６は、通報先データベースのデータ構成の一例を示す説明図である。通報先データベース１５３０は、通報先情報を記憶している。例えば、通報先情報として通報先端末のメールアドレス“ｍａｉｌ０１@ｘｘｘ．ｎｅ．ｊｐ”が格納されている。

【０１０１】

制御部１５１０は、さらに検知情報取得部１１１と、操作情報取得部１１２と、出力制御部１１３と、警備モード切替部１１４と、認証部１１５と、通報先情報記憶部１１６と、警備モード記憶部１１７と、警報送信部１１９と、メール送受信部５１２と、タイマ部５１３と、メール生成部５１５と、通報先確認部５１６と、を備えている。ここで、各部の構成、機能は、第１または第２の実施の形態と同様であるので、上述した説明を参照し、ここでの説明を省略する。

【０１０２】

次に、以上のように構成されている警備装置１５００による通報承諾確認処理について説明する。図１７－１、図１７－２は、操作情報取得部、認証部、メール送受信部、タイマ部、メール生成部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。

【０１０３】

まず、認証処理であるステップＳ１７０１～ステップＳ１７０３の処理は、上述した図４のステップＳ４０１～ステップＳ４０３の処理と同様であるため、上述した説明を参照し、ここでの説明を省略する。

【０１０４】

操作情報取得部１１２は、操作部１０２によって入力されたメールアドレスを取得する（ステップＳ１７０４）。次に、メール生成部５１５は、取得されたメールアドレスに対して異常検知時に通報されることを承諾するか否かの通報承諾確認メールを生成する（ステップ１７０５）。メール送受信部５１２は、メール生成部５１５によって生成された通報承諾確認メールを送信する（ステップＳ１７０６）。メール送受信部５１２は、通報承諾確認メールを送信できたか否かを判断する（ステップＳ１７０７）。通報承諾確認メールを送信できなかったと判断した場合は（ステップＳ１７０７：Ｎｏ）、ステップＳ１７１３に進む。通報承諾確認メールを送信できたと判断した場合は（ステップＳ１７０７：Ｙｅｓ）、タイマ部５１３は所定時間が経過したか否かを判断する（ステップＳ１７０８）。所定時間が経過していないと判断した場合には（ステップＳ１７０８：Ｎｏ）、ステップＳ１７０８に戻り、所定時間が経過するまで計測を繰り返す。

【０１０５】

所定時間が経過したと判断した場合には（ステップＳ１７０８：Ｙｅｓ）、通報承諾確認メールに対する通報承諾返信メールが受信されたか否かを判断する（ステップＳ１７０９）。通報承諾確認メールに対する通報承諾返信メールが受信されたと判断した場合には（ステップＳ１７０９：Ｙｅｓ）、通報先確認部５１６は通報承諾返信メールの本文から通報先承諾の有無を判断する（ステップＳ１７１０）。ステップＳ１７０９において、通報承諾確認メールに対する通報承諾返信メールが１つも受信されていないと判断した場合には（ステップＳ１７０９：Ｎｏ）、ステップＳ１７１３に進む。なお、通報承諾返信メールを受信しない場合は、上述した実施の形態と同様に、適当な時間をおいて再度通報承諾確認メールを送信するようにしてもよい。

【０１０６】

通報先から送信された通報承諾返信メールによって異常検知時に通報することを承諾されたと判断した場合には（ステップＳ１７１１：Ｙｅｓ）、通報先確認部５１６はメールアドレスを通報先データベース１５３０に格納する（ステップＳ１７１２）。異常検知時に通報することを承諾されていないと判断した場合には（ステップＳ１７１１：Ｎｏ）、ステップＳ１７１３に進む。出力部１０３は、異常検知時の通報先の承諾結果を出力する（ステップＳ１７１３）。

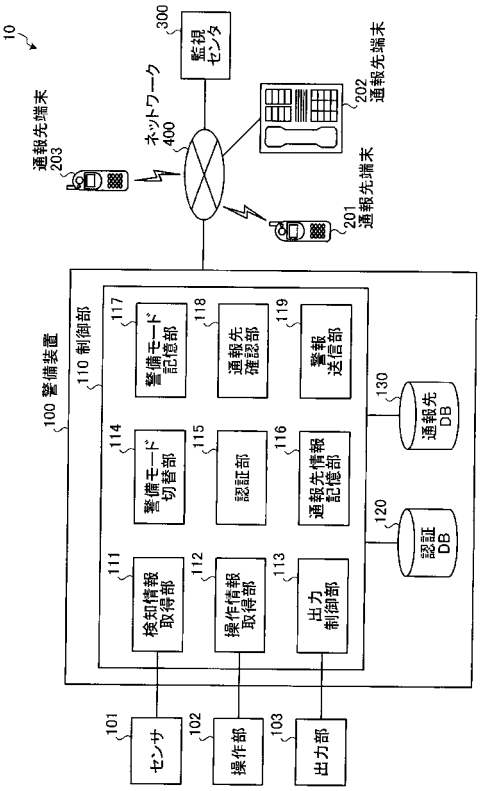
【０１０７】
このように、警備装置１００において監視領域で異常を検知した場合に、警備装置からメールで通報先に異常検知を通報する監視システムにおいても、利用者が登録しようとするメールアドレスに対し、通報承諾確認メールが送信できた場合であって、なおかつ通報承諾確認メールに対する通報承諾返信メールを受信し、通報承諾があった場合にのみ通報先情報が登録されるため、利用者が誤った通報先を登録することを防止することができる。また、利用者が事前に確認を取っていない親戚等を通報先として設定することを防止することができる。
【０１０８】
なお、本実施の形態では、通報先の登録を行うために、通報承諾確認メールを送信できたか否か、通報承諾確認メールに対する通報承諾返信メールを受信したか否か、通報先の登録につき承諾されたか否かを段階に分けて判断しているが、適宜いずれか一つまたは二つの判断のみを行うようにしてもよい。
【０１０９】
以上、本発明を第１～第３の実施の形態を用いて説明してきたが、上述した実施の形態に多様な変更または改良を加えることができる。また、上述した第１～第３の実施の形態において説明した構成や機能は、自由に組み合わせることができる。
【図面の簡単な説明】
【０１１０】
【図１】第１の実施の形態にかかる監視システムの構成を示すブロック図である。
【図２】認証データベースのデータ構成の一例を示す説明図である。
【図３】通報先データベースのデータ構成の一例を示す説明図である。
【図４－１】操作情報取得部、出力制御部、認証部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図４－２】操作情報取得部、出力制御部、認証部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図５】認証情報が入力される操作部の画面の一例を示す説明図である。
【図６】通報先設定の画面の一例を示す説明図である。
【図７】通報先が設定された場合の出力画面の一例を示す説明図である。
【図８－１】操作情報取得部、出力制御部、認証部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図８－２】操作情報取得部、出力制御部、認証部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図９】第２の実施の形態にかかる監視システムの構成を示すブロック図である。
【図１０】認証データベースのデータ構成の一例を示す説明図である。
【図１１】通報先データベースのデータ構成の一例を示す説明図である。
【図１２－１】データ送受信部、メール送受信部、タイマ部、認証部、メール生成部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図１２－２】データ送受信部、メール送受信部、タイマ部、認証部、メール生成部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図１２－３】データ送受信部、メール送受信部、タイマ部、認証部、メール生成部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図１３】認証情報入力画面の一例を示す説明図である。
【図１４】メールアドレス入力画面の一例を示す説明図である。
【図１５】第３の実施の形態にかかる監視システムの構成を示すブロック図である。
【図１６】通報先データベースのデータ構成の一例を示す説明図である。
【図１７－１】操作情報取得部、認証部、メール送受信部、タイマ部、メール生成部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。
【図１７－２】操作情報取得部、認証部、メール送受信部、タイマ部、メール生成部、通報先確認部が行う通報承諾確認処理手順を示すフローチャートである。

【符号の説明】

【０１１１】

１０　２０　３０　監視システム
１００　１５００　警備装置
１０１　センサ
１０２　操作部
１０３　出力部
１１０　５１０　１５１０　制御部
１１１　検知情報取得部
１１２　操作情報取得部
１１３　出力制御部
１１４　警備モード切替部
１１５　５１４　認証部
１１６　通報先情報記憶部
１１７　警備モード記憶部
１１８　５１６　通報先確認部
１１９　警報送信部
１２０　５２０　認証データベース
１３０　５３０　１５３０　通報先データベース
２０１　２０２　２０３　２０４　通報先端末
３００　監視センタ
４００　ネットワーク
５００　サーバ装置
５１１　データ送受信部
５１２　メール送受信部
５１３　タイマ部
５１５　メール生成部

【図１】



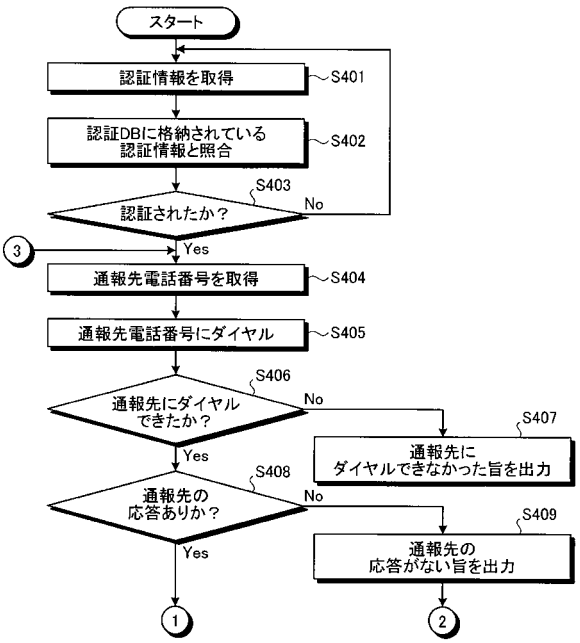
【図２】

利用者ID	パスワード
001	1234
002	5678
003	9012
⋮	⋮

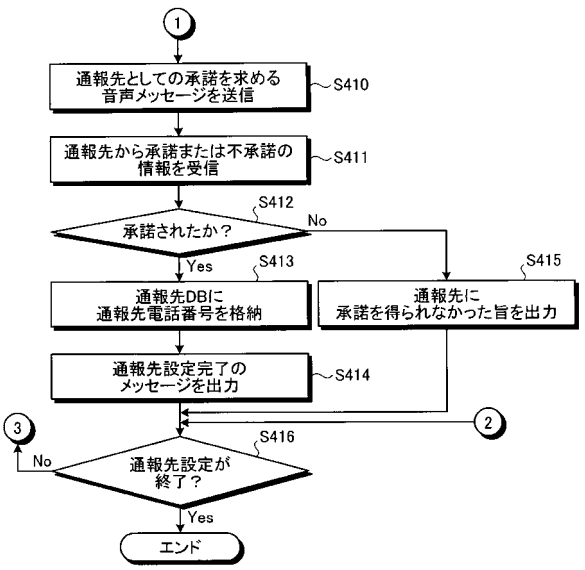
【図３】

通報先情報
090-XXXX-○○○○
03-XXXX-△△△△
090-XXXX-□□□□
⋮

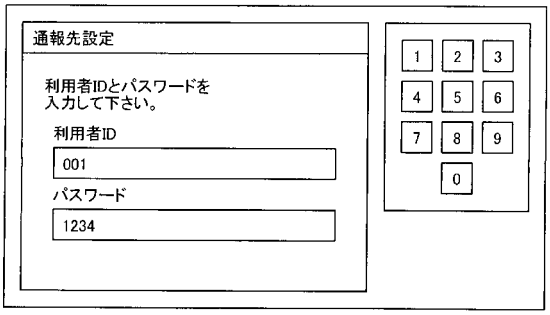
【図４－１】



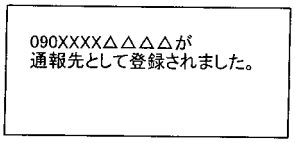
【図４－２】



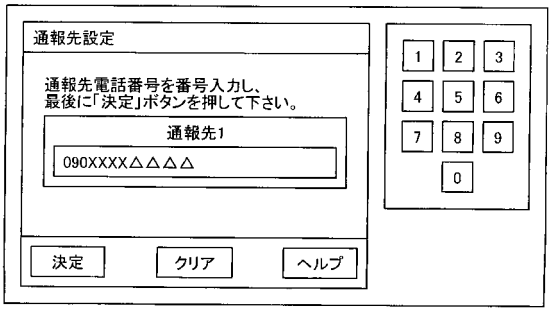
【図５】



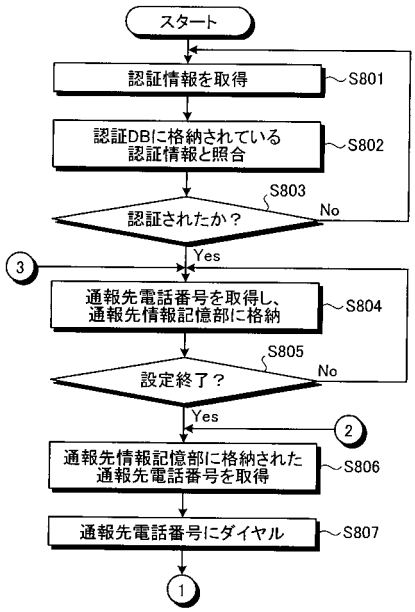
【図７】



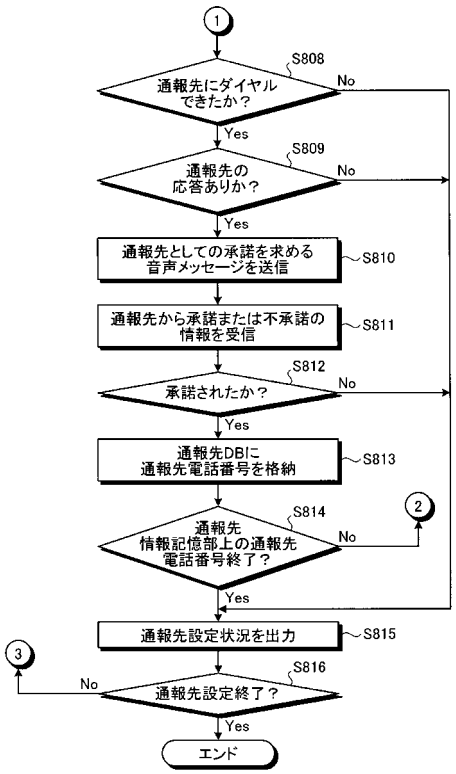
【図６】



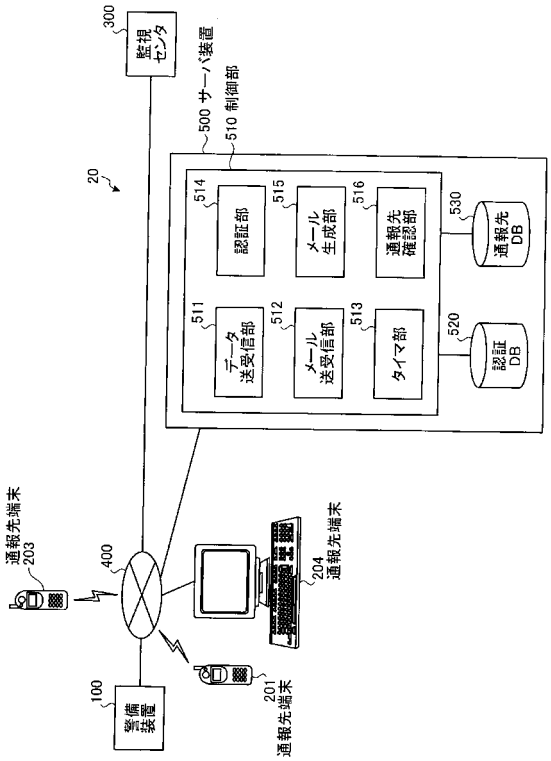
【図８－１】



【図８－２】



【図９】



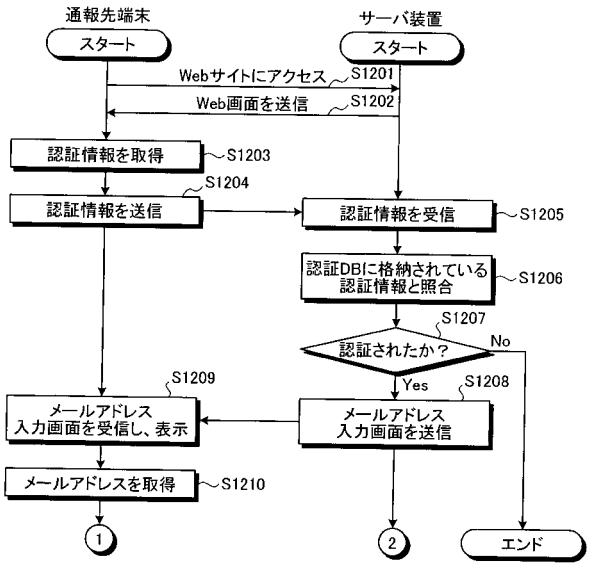
【図１０】

利用者ID	パスワード	警備装置ID
001 011	PW1234 PW4321	K001 K002
⋮	⋮	⋮

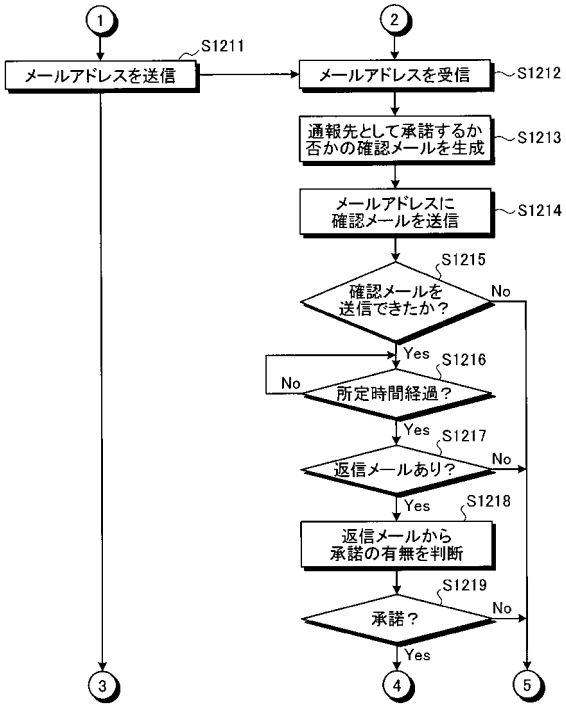
【図１１】

警備装置ID	通報先情報
K001	mail01@xxx.ne.jp mail02@yyy.ne.jp ⋮
K002	mail21@zzz.ne.jp ⋮
⋮	⋮

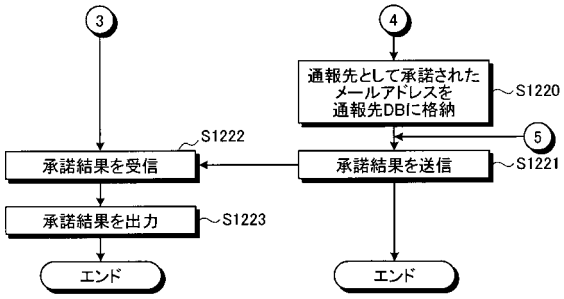
【図１２－１】



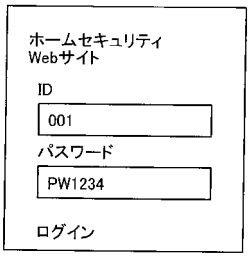
【図１２－２】



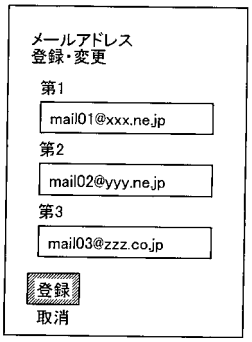
【図１２－３】



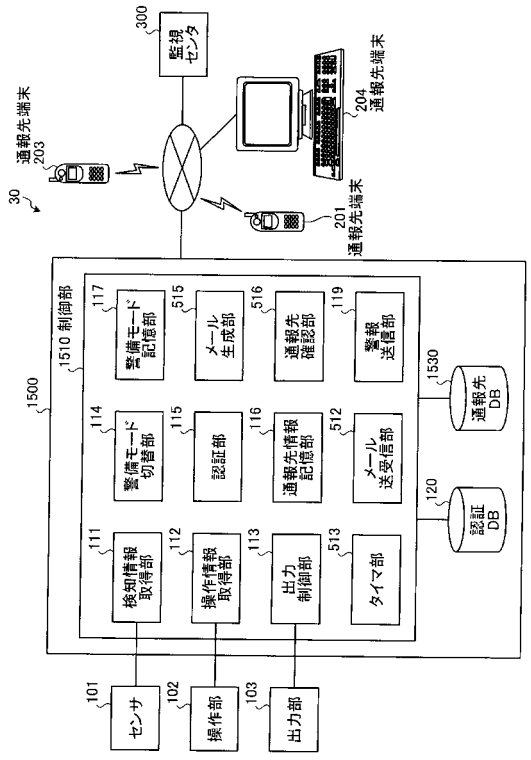
【図１３】



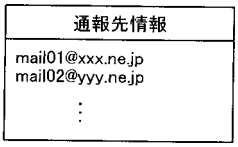
【図１４】



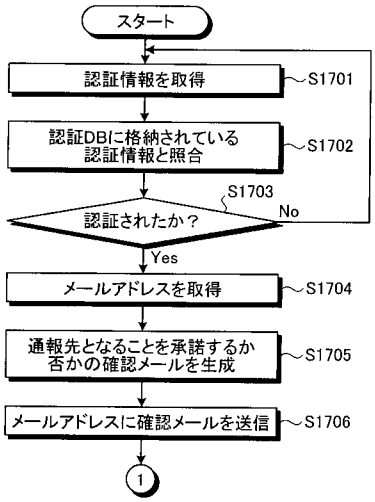
【図１５】



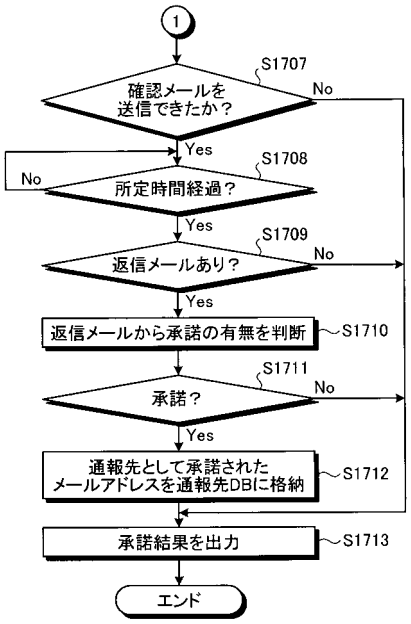
【図１６】



【図１７－１】


スタート
認証情報を取得
S1701
認証DBに格納されている
認証情報と照合
S1702
S1703
認証されたか？
No
Yes
メールアドレスを取得
S1704
通報先となることを承諾するか
否かの確認メールを生成
S1705
メールアドレスに確認メールを送信
S1706
1

【図１７－２】


1
S1707
確認メールを
送信できたか？
No
Yes
S1708
No
所定時間経過？
Yes
S1709
返信メールあり？
No
Yes
返信メールから承諾の有無を判断
S1710
S1711
承諾？
No
Yes
通報先として承諾された
メールアドレスを通報先DBに格納
S1712
承諾結果を出力
S1713
エンド

フロントページの続き

審査官　二之湯　正俊

(56)参考文献　特開２００５－３１１８３１（ＪＰ，Ａ）
特開２０００－２８７２４９（ＪＰ，Ａ）
特開２００３－０７８９０４（ＪＰ，Ａ）
特開２００２－３５２３４９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０８Ｂ　２３／００－３１／００
Ｇ０８Ｂ　１９／００－２１／２４
Ｇ０８Ｂ　１３／００－１５／０２
Ｈ０４Ｍ　１１／０４