(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 603 094 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
07.12.2005 Bulletin 2005/49

(21) Application number: **04717766.2**

(22) Date of filing: **05.03.2004**

(51) Int Cl.[7]: **G08B 25/04**, G08B 25/10, G08B 23/00, G08B 13/22

(86) International application number:
PCT/JP2004/002819

(87) International publication number:
WO 2004/079687 (16.09.2004 Gazette 2004/38)

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **07.03.2003 US 452553 P**

(71) Applicant: **OMRON CORPORATION**
Kyoto-shi, Kyoto 600-8530 (JP)

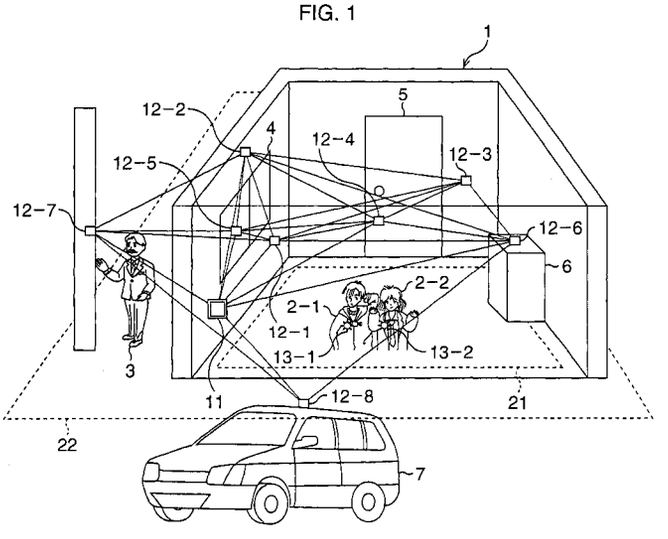
(72) Inventors:
- **HISANO, Atsushi, C/o Omron Corporation**
Shimogyo-ku, Kyoto 6008530 (JP)
- **KAMEYAMA, Masanori, C/o Omron Corporation**
Shimogyo-ku, Kyoto 6008530 (JP)

(74) Representative: **Calderbank, Thomas Roger et al**
Mewburn Ellis LLP
York House
23 Kingsway
London WC2B 6HP (GB)

(54) SECURITY SYSTEM, TERMINAL, INFORMATION PROCESSING DEVICE AND METHOD, PROGRAM, VEHICLE SECURITY SYSTEM, NETWORK SYSTEM, AND SETTING METHOD

(57) According to the present invention, specified processing for unauthorized intrusions can be executed in accordance with conditions in the object of security without requiring any bothersome operation. The distance measuring unit 43 detects the positions of authorized members using the object of security. The wireless transmitting and receiving unit 44 and data communications unit 46 detect the positions of unauthorized intrusions into the object of security. The white smoke generating modules 49 are disposed in a plurality of locations inside the object of security, and execute processing with respect to unauthorized intrusions. The control unit 41 selects the white smoke generating module 49 that executes processing in accordance with the relationship between the detected positions of the authorized members and the detected position of the unauthorized intrusion, and controls the execution of processing by the selected white smoke generating module 49. The present invention can be applied to a home security system.

FIG. 1



EP 1 603 094 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to a security system, a terminal device, an information processing device and method, a program, a vehicle security system, a network system and a setting method, and more particularly relates to a security system, a terminal device, an information processing device and method, a program, a vehicle security system and a setting method which detect the unauthorized invasion of an object constituting the object of security.

BACKGROUND ART

[0002] Various types of security systems have been proposed and utilized in the past.

[0003] In Japanese Patent Application Laid-Open No. 10-27292, a system is disclosed which is devised so that the final person to leave when a facility such as a shop or the like is closed can open a final exit door and return home only after doors that are the object of security are locked and a security mode is set. In this system, the system is devised so that during ordinary business hours up to five o'clock in the evening, the final exit door can be freely opened from the inside, while after five o'clock in the evening, the setting of the security mode is a condition for the opening of the door. As a result, the possibility that the setting of the security mode that notifies the security firm of the breaking of the door will be forgotten is prevented in advance.

[0004] In Japanese Patent Application Laid-Open No. 8-249550, a system is disclosed which is devised so that a monitoring mode is successively varied in loop form by pressing one setting button of a home security device for a time that is less than a first specified time within a second specified time. The monitoring mode is checked after the second specified time has elapsed, and the crime-prevention sensors of a plurality of systems are set in a monitoring state. In cases where the abovementioned setting button is pressed for a time that exceeds the first specified time, the monitoring state of the crime-prevention sensors of the plurality of systems is released by the operation of one setting button. In this home security device, the setting/release of the monitoring state of the closing of doors can be accomplished by the operation of a single setting button even in cases where the crime-prevention sensors of a plurality of systems are connected.

[0005] In Japanese Patent Application Laid-Open No. 2001-56887, a system is disclosed in which a first sensor that has a detection area on the object of security and on the front surface side of a part above the object of security, and a second sensor that has a detection area on the object of security and on the front surface side of a part below the object of security, are provided, a logic circuit equipped with a timer is disposed on at least one of the sensors, i. e., the first sensor or second sensor, and an output path that outputs a detection signal from the detection part within the sensor to the outside is disposed on at least the other sensor. The logic circuit equipped with a timer generates a warning signal when a detection signal from the detection part within the sensor on which the timer-equipped logic circuit is disposed and a detection signal that is extracted via the output path of the other sensor are received within a specified time. As a result, erroneous reports caused by small animals or external disturbing light can be avoided, and intrusion via openings such as (e. g.) windows, entrances and exits and the like of the building that is the object of security can be properly detected.

[0006] In Japanese Patent Application Laid-Open No. 5-114091, a system is disclosed which is devised so that when a window is opened so that the sensing signal of an indoor invasion sensor is input into a data processing part, a judgment is made as to whether or not a sensing signal indicating that an outdoor invasion sensor that monitors a specified position outside the window has sensed an intruder has been input into the data processing part in the past few seconds, and if conditions described previously are satisfied as a result of this judgment, an internal notification is made by means of a voice sounding action using an internal notification part and a speaker, and a higher system notification is made using a terminal that connects a higher system notification part and a telephone circuit, so that an actual warning is issued, while if the [abovementioned] conditions are not satisfied, this event is handled as an erroneous warning, and no internal notification or higher system notification is made. As a result, the warning can be judged to be an actual warning, and an intrusion warning can be issued, only when the [abovementioned] window is opened from the outside.

[0007] However, in the case of conventional home security systems, changing the mode of the home security system is bothersome, and mode change mistakes lead to erroneous warnings, failure to detect intrusions and the like.

[0008] In the invention disclosed in Japanese Patent Application Laid-Open No. 10-27292, the complicated operation of "the final person to leave being able to open the final exit door and return home only after locking the doors that are the object of security and setting the security mode" is required in order to solve the setting of the task of eliminating mistakes in the changing of the mode settings, so that the system is inconvenient. In the invention disclosed in Japanese Patent Application Laid-Open No. 8-249550, a button operation is required in order to change the mode settings, and if [the operator] forgets to perform this button operation, the mode settings cannot be changed. Furthermore, even if

an intruder is detected, only a simple voice warning is issued; accordingly, the intruder cannot be effectively repulsed.

[0009] The present applicant has analyzed the abovementioned problems; here, the "problem points" that are the causes of the problems will be indicated.

[0010] The following description will center on the home; however, this description may be applied to facilities (objects of security) such as homes, warehouses, offices, factories, hospitals, schools, vehicles and the like.

[0011] The following items are required in order to eliminate erroneous warnings with respect to intruder warnings in home security systems.

[0012] First, if the movement of a person inside the home or the opening or closing of a door of the home is detected during the absence of the person dwelling in the home, "caretaker guard processing" that judges whether or not an unauthorized intruder is present in this case must be started and stopped with an appropriate timing.

[0013] Second, in cases where a door or window of the home is opened or closed when the home dweller is present in a specified place inside the home, "at-home guard processing" that judges whether or not an unauthorized intruder is present must be appropriately started and stopped.

[0014] Third, the intruder must be repulsed with an appropriate timing and at an appropriate place.

DISCLOSURE OF THE INVENTION

[0015] The present invention was devised in light of the above facts; a first object of the present invention is to lower the frequency of erroneous warnings by setting and releasing the warning mode automatically without requiring the operation of a button or the like. Specifically, the present invention is devised so that specified processing with respect to unauthorized intrusions can be executed in accordance with the conditions inside the object of security without requiring any bothersome operation.

[0016] A second object of the present invention is to allow the simple execution of area settings for the purpose of setting and releasing the warning mode, i. e., to allow simple initial settings.

[0017] A third object of the present invention is to allow effective repulsion of intruders.

[0018] A fourth object of the present invention is to make it possible to provide appropriate evacuation guidance to authorized members.

[0019] The first security system of the present invention is characterized in that this security system comprises member position detection means that detect the positions of authorized members using the object of security, unauthorized intrusion position detection means that detect the positions of unauthorized intrusions into the object of security, execution means that are disposed in a plurality of locations inside the object of security, and that execute processing with respect to unauthorized intrusions, and execution control means that select the execution means that execute processing in accordance with the relationship between the positions of authorized members detected by the member position detection means and the positions of unauthorized intrusions detected by the unauthorized intrusion position detection means, and that control the execution of the processing of the selected execution means.

[0020] The execution control means can be devised so that in cases where the distance between the position of an unauthorized intrusion and the position of an authorized member is equal to or less than a specified threshold value, one or more execution means including the execution means closest to the position of the unauthorized intrusion are selected, and the execution of processing is controlled so that the processing for the unauthorized intrusion is executed by the selected execution means.

[0021] The execution control means can be devised so that the execution of processing is performed in such a manner that processing for the evacuation guidance of the authorized member is executed by execution means whose distance from the position of the authorized member is equal to or less than a specified threshold value, and which are located furthest from the position of the unauthorized intrusion.

[0022] The execution means can be devised so that these execution means execute processing that generates white smoke.

[0023] The member position detection means can be devised so that these member position detection means detect the positions of authorized members by detecting the positions of devices which are mounted on the authorized members, and which transmit by wireless transmission an ID code that corresponds to the object of security.

[0024] The member position detection means can be devised so that these member position detection means detect the positions of authorized members by detecting the positions of devices which are mounted on the authorized members, which transmit by wireless transmission an ID code that corresponds to the object of security, and in which the execution means are disposed.

[0025] The second security system of the present invention is characterized in that this security system comprises member position detection means that detect the positions of authorized members using the object of security, unauthorized intrusion position detection means that detect the positions of unauthorized intrusions into the object of security, external security surface memory means that store the position of an external security surface, internal security surface memory means that store the position of an internal security surface, execution control means that control the execution

of first guard processing or second guard processing on the basis of the positions of authorized members detected by the member position detection means so that the first guard processing is executed in cases where no authorized member is present inside the external security surface, and so that the second guard processing is executed in cases where an authorized member is present inside the internal security surface, and execution means which are disposed in a plurality of locations inside the object of security, and which execute processing for unauthorized intrusions when the positions of unauthorized intrusions into the object of security are detected by the unauthorized intrusion position detection means in cases where the first guard processing or second guard processing is executed.

[0026] The first guard processing can be set as caretaker guard processing that is guard processing for unauthorized intrusions into the inside of the external security surface, and the second guard processing can be set as at-home guard processing that is guard processing for unauthorized intrusions into the space between the external security surface and internal security surface.

[0027] The execution means can be devised so that these execution means execute processing that generates white smoke.

[0028] The member position detection means can be devised so that these means detect the positions of authorized members by detecting the positions of devices which are mount on the authorized members, and which transmit by wireless transmission ID codes that correspond to the object of security.

[0029] The member position detection means can be devised so that these means detect the positions of authorized members by detecting the positions of devices which are mounted on the authorized members, which transmit by wireless transmission an ID code that corresponds to the object of security, and in which the execution means are disposed.

[0030] The execution means disposed in the devices can be devised so that these means execute processing that generates white smoke.

[0031] The terminal device of the present invention is characterized in that this terminal device comprises an antenna unit, a wireless transmitting and receiving unit that transmits and receives information via the antenna unit, a distance measuring unit that measures the distance to the device constituting the wireless transmitting and receiving partner by transmitting and receiving signals modulated by a specified code via the antenna unit and wireless transmitting and receiving unit, a data communications unit which performs data communications with the devices by transmitting and receiving signals modulated by a code via the antenna unit and wireless transmitting and receiving unit, an actuator which executes specified processing with respect to unauthorized intrusions, and a control unit which performs overall control.

[0032] The actuator can be devised so that this actuator executes processing that generates white smoke.

[0033] The terminal device can be further equipped with human body detection means that detect a human body between the terminal device and another terminal device by analyzing the waveform of a wireless communications signal between the terminal device and another terminal device, and the actuator can be devised so that the actuator executes processing for an unauthorized intrusion in cases where the human body detection means detect a human body.

[0034] The second terminal device of the present invention is characterized in that this terminal device comprises distance measuring means that measure the distance between this second terminal device and a partner [terminal device], human body detection means that detect a human body between this second terminal device and this partner [terminal device], and transmitting means that transmit information indicating the measured distance between this second terminal device and partner [terminal device] or information indicating the detection of a human body.

[0035] The first information processing method of the present invention comprises a distance measurement step in which the distance between the terminal device and partner [terminal device] is measured, a human body detection step in which a human body between the terminal device and the partner [terminal device] is detected by the waveform analysis of a wireless communications signal, and a transmission control step in which the transmission of information indicating the measured distance between the terminal device and partner [terminal device] or information indicating the detection of a human body is controlled.

[0036] The first program of the present invention is characterized in that this program causes a computer to execute a distance measurement step in which the distance between the terminal device and partner [terminal device] is measured, a human body detection step in which a human body between the terminal device and the partner [terminal device] is detected by the waveform analysis of a wireless communications signal, and a transmission control step in which the transmission of information indicating the measured distance between the terminal device and partner [terminal device] or information indicating the detection of a human body is controlled.

[0037] The information processing device of the present invention is characterized in that this device comprises distance measuring means that measured the distances to respective terminal devices from this information processing device, receiving means for receiving information indicating the distances between terminal devices, which is transmitted from the respective terminal devices, and judgment means for judging whether or not there has been an unauthorized intrusion into the object of security on the basis of the distances to the respective terminal devices from the

information processing device or the distances between the respective terminal devices.

[0038] The information processing device can be further equipped with human body detection means that detect a human body between the information processing device and respective terminal devices by waveform analysis of a wireless communications signal, and the judgment means can be devised so that these means judge whether or not there has been an unauthorized intrusion into the object of security on the basis of the detection of a human body.

[0039] The receiving means can further receive information indicating the detection of a human body that is transmitted from the respective terminal devices, and the judgment means can be devised so that these means judge whether or not there has been an unauthorized intrusion into the object of security on the basis of information indicating the detection of a human body.

[0040] The second information processing method of the present invention is characterized in that this method comprises a distance measurement step in which the distances from the [information processing device] to respective terminal devices are measured, a reception control step in which the reception of information indicating the distances between terminal devices (which is transmitted from the respective terminal devices) is controlled, and a judgment step in which a judgment is made as to whether or not there has been an intrusion into the object of security on the basis of the distances from the information processing device to the respective terminal devices or the distances between the terminal devices.

[0041] The second program of the present invention is characterized in that this program causes a computer to execute a distance measurement step in which the distances from the [information processing device] to respective terminal devices are measured, a reception control step in which the reception of information indicating the distances between terminal devices (which is transmitted from the respective terminal devices) is controlled, and a judgment step in which a judgment is made as to whether or not there has been an intrusion into the object of security on the basis of the distances from the information processing device to the respective terminal devices or the distances between the terminal devices.

[0042] The vehicle security system of the present invention comprises fixed terminal devices which are disposed on the inside surfaces of the respective doors of the vehicle and which measure the distances between other fixed terminal devices and a control terminal device, a mobile terminal device which is held by a person that has proper authorization to enter and exit the vehicle, and a control terminal device which is disposed inside the vehicle, and is characterized in that the variations in the distance between the fixed terminal devices disposed inside the vehicle and the control terminal device and the mutual distances between the fixed terminal devices are monitored when the position of the mobile terminal device is located outside an external security surface that is set by the fixed terminal devices disposed inside the vehicle and the control terminal device, it is judged that an abnormality has occurred in cases where the variation in distance satisfies specified conditions, and processing for unauthorized intrusions is executed in cases where it is judged that an abnormality has occurred.

[0043] The processing for unauthorized intrusions can be devised so that white smoke is generated in this processing.

[0044] The network system of the present invention comprises sensing means in which fixed nodes sense the surrounding environment, first wireless communications means, an actuator which applies an action to the outside, and control means which control the first wireless communications means so that information relating to the surrounding environment sensed by the sensing means is transmitted to a control node, and so that the actuator is caused to operate in accordance with commands from the control node, and is characterized in that the control node comprises second wireless communications means and selection means that select the fixed node for which the actuator is to be operated on the basis of information relating to the surrounding environment that is received from the fixed nodes, and the second wireless communications means transmits a command that operates the actuator to the selected fixed node.

[0045] The second wireless communications means can be devised so that these means receive information relating to the surrounding environment (constituting information relating to the distances between fixed nodes) that is transmitted from the fixed nodes.

[0046] The first setting method of the present invention is a setting method for a three-dimensional coordinate system using a first terminal device, second terminal device, third terminal device and fourth terminal device which are terminal devices comprising an antenna unit, a wireless transmitting and receiving unit that transmits and receives information via the antenna unit, a distance measuring unit that measures the distance to the device constituting the wireless transmitting and receiving partner by transmitting and receiving signals modulated by a specified code via the antenna unit and wireless transmitting and receiving unit, a data communications unit which performs data communications with the devices by transmitting and receiving signals modulated by a code via the antenna unit and wireless transmitting and receiving unit, an actuator which executes specified processing with respect to unauthorized intrusions, and a control unit which performs overall control, this setting method being characterized in that the position of the first terminal device is taken as the origin of the three-dimensional coordinate system, the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device are respectively measured, the first axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to first measurement

results indicating the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device, the second axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to these first measurement results, the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device are respectively measured, and the third axis of the three-dimensional coordinate system is specified from second measurement results indicating the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device, the first axis and the second axis.

[0047] The second setting method of the present invention is the security surface setting method in the three-dimensional coordinate system set by the setting method according to claim 28, characterized in that the position of a fifth terminal device constituting a terminal device in the three-dimensional coordinate system is detected, the smallest rectangular solid in the three-dimensional coordinate system including a plurality of detected positions is determined, and the security surface is set on the basis of surface of the determined rectangular solid.

[0048] The system of the present invention relates to a security system using a sensor network constructed from nodes in which a plurality of nodes that can generate node ID information and that allow the measurement of the distances between nodes and the detection of any intrusion between nodes are disposed in facilities such as (for example) homes, warehouses, offices, factories, hospitals, schools, vehicles or the like, and nodes are also held by authorized members of these facilities, and further relates to a security system using an actuator network in which the nodes are equipped with actuators, and these actuators are appropriately operated in accordance with the position of an unauthorized intruder.

[0049] In the first security system of the present invention, the positions of authorized members using the object of security are detected, the position of any unauthorized intrusion into the object of security is detected, processing with respect to unauthorized intrusions is executed by execution means disposed in a plurality of locations inside the object of security, execution means that execute processing are selected in accordance with the relationship between the detected positions of authorized members and the detected position of any unauthorized intrusion, and the execution of the processing of the selected execution means is controlled.

[0050] In the second security system of the present invention, the positions of authorized members using the object of security are detected, the position of any unauthorized intrusion into the object of security is detected, the position of an external security surface is stored in memory, the position of an internal security surface is stored in memory, the execution of first guard processing or second guard processing is controlled on the basis of the detected positions of authorized members so that first guard processing is executed in cases where no authorized member is present inside the external security surface, and so that second guard processing is executed in cases where an authorized member is present inside the internal security surface; furthermore, in cases where first guard processing or second guard processing is executed, processing for an unauthorized intrusion is executed when the position of an unauthorized intrusion into the object of security is detected.

[0051] In the first terminal device of the present invention, information is transmitted and received via the antenna unit, signals modulated by a specified code are transmitted and received via the antenna unit and wireless transmitting and receiving unit, so that the distance to the device constituting the wireless transmitting and receiving partner is measured, data communications with devices are performed by transmitting and receiving signals modulated by a specified code via the antenna unit and wireless transmitting and receiving unit, specified processing for unauthorized intrusions is executed, and the device as a whole is controlled.

[0052] In the second terminal device, first information processing method and first program of the present invention, the distance to the partner [terminal device] is measured, a human body between this second terminal device and the partner [terminal device] is detected by the waveform analysis of a wireless communications signal, and information indicating the measured distance to the partner [terminal device] or information indicating the detection of a human body is transmitted.

[0053] In the information processing device, second information processing method and second program of the present invention, the distances to respective terminal devices from the information processing device are measured, information indicating the distances between terminal devices that is transmitted from the respective terminal devices is received, and a judgment as to whether or not there has been an unauthorized intrusion into the object of security is made on the basis of the distances from the information processing device to the respective terminal devices or the distances between terminal devices.

[0054] In the vehicle security system of the present invention, in cases where the position of the mobile terminal device is outside the external security surface that is set by the control terminal device and the fixed terminal devices that are disposed inside the vehicle, the variations in the distances between the control terminal device and the fixed terminal devices disposed inside the vehicle and the distances between the fixed terminal devices are monitored; furthermore, in cases where the variation in the distance satisfies specified conditions, it is judged that an abnormality

has occurred, and in cases where it is occurred that an abnormality has occurred, specified processing for an unauthorized intrusion is executed.

[0055] In the network system of the present invention, the surrounding environment is sensed, an action is applied to the outside, and information relating to the sensed surrounding environment is transmitted to the control node; furthermore, a control action is performed so that the actuator is operated in accordance with commands from the control node, the fixed node for which the actuator is to be operated is selected on the basis of the information relating to the surrounding environment that is received from the fixed nodes, and the actuator is caused to operate on the selected fixed node.

[0056] In the first setting method of the present invention, the position of the first terminal device is taken as the origin of the three-dimensional coordinate system, the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device are respectively measured, the first axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to first measurement results indicating the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device, the second axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to these first measurement results, the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device are respectively measured, and the third axis of the three-dimensional coordinate system is specified from second measurement results indicating the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device, the first axis and the second axis.

BRIEF DESCRIPTION OF THE DRAWINGS

[0057]

Fig. 1 is a diagram which shows one embodiment of the security system of the present invention;
Fig. 2 is a block diagram which shows an example of the construction of the control localizer;
Fig. 3 is a block diagram which shows an example of the construction of the fixed localizer;
Fig. 4 is a block diagram which shows an example of the construction of the mobile localizer;
Fig. 5 is a diagram which illustrates the calculation of positions in the coordinate system;
Fig. 6 is a diagram which illustrates the setting of the two internal security surfaces;
Fig. 7 is a flow chart which illustrates the processing of the execution mode;
Fig. 8 is a diagram which illustrates the position of the mobile localizer in a case where non-guard processing is performed;
Fig. 9 is a diagram which illustrates the position of the mobile localizer in a case where at-home guard processing is performed;
Fig. 10 is a diagram which illustrates the position of the mobile localizer in a case where caretaker guard processing is performed;
Fig. 11 is a flow chart which illustrates the details of non-guard processing;
Fig. 12 is a flow chart which illustrates the details of at-home guard processing;
Fig. 13 is a flow chart which illustrates the details of caretaker guard processing;
Fig. 14 is a diagram which illustrates the emission of white smoke; and
Fig. 15 is a diagram which shows one embodiment of the car security system of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

[0058] Fig. 1 is a diagram which shows one embodiment of the security system of the present invention. In Fig. 1, the security system of the present invention is disposed in a home 1 which constitutes one example of the object of security. Furthermore, in Fig. 1, the user 2-1 and user 2-2 are authorized members using the home 1. The security system detects the position of the unauthorized intrusion of an unauthorized intruder 3, and executes specified processing with respect to this unauthorized intrusion.

[0059] The security system of the present invention comprises a control localizer 11, fixed localizers 12-1 through 12-8, and mobile localizers 13-1 and 13-2.

[0060] Below, in cases where there is no need to make individual distinctions among the fixed localizers 12-1 through 12-8, these localizers will be referred to simply as the fixed localizers 12. Below, furthermore, in cases where there is no need to make an individual distinction between the mobile localizers 13-1 and 13-2, these localizers will be referred

to simply as the mobile localizers 13.

[0061] Furthermore, in the security system of the present invention, it is sufficient if the number of fixed localizers 12 is three or greater, and the number of mobile localizers 13 may be set at an arbitrary number.

[0062] Furthermore, in cases where there is no need to make individual distinctions among the control localizer 11, fixed localizers 12 and mobile localizers 13, these localizers will be referred to simply as localizers.

[0063] Here, the localizers are one example of terminal devices, and constitute a network system. Specifically, a specified ID code can be transmitted by wireless transmission, so that the distance between a given node and other nodes can be measured by wireless, or so that the position of a given node itself can be measured. Furthermore, a node which is devised so that if an intruding object (unauthorized intruder 3) is present between a given node and another node, the intrusion of this intruding object can be detected, and which further has a function that allows the wireless transmission of information detected by this node, is called a localizer.

[0064] Specifically, such a localizer detects unauthorized intrusions by means of the variation in the position of the localizer itself, or detects unauthorized intrusions by detecting a human body between localizers (i. e., in the sensing area).

[0065] The fixed localizers 12 are fastened to an object that constitutes the object of security, whose position basically does not vary (i. e., an object that does not move). The control localizer 11 is fastened to this object that constitutes the object of security whose position basically does not vary (i. e., an object that does not move), so that the position of the control localizer 11 does not vary. Furthermore, the control localizer 11 also has the function of communicating with the outside, and the control function of summarizing status information regarding all of the localizers in the system and storing this information in memory.

[0066] The control localizer 11 and fixed localizers 12 are fastened to fixed object in the home 1 such as window glasses, the vicinity of indoor window frames, the indoor surfaces of doors, the surfaces of indoor walls or ceilings, outdoor walls of the home, outdoor columns, gate posts or the like. Furthermore, the localizers are also fastened to outdoor vehicles 7, indoor electrical appliances, safes 6 or the like that are highly likely to be stolen.

[0067] However, mobile localizers 13 are mounted on vehicles 7, for which movement is a prerequisite. Even a mobile localizer 13 may be automatically incorporated as a fixed localizer 12 into a wireless network consisting of fixed localizers 12 if this mobile localizer 13 is stationary for a specified period of time or longer.

[0068] For example, as is shown in Fig. 1, the control localizer 11 is fastened to the inside of a wall of the home 1. The fixed localizer 12-1, fixed localizer 12-2 and fixed localizer 12-3 are fastened to the insides of walls of the home 1.

[0069] Furthermore, the fixed localizer 12-4 is fastened to the inside of a door 5 of the home 1. The fixed localizer 12-5 is fastened to the inside of a window 4 of the home 1. The fixed localizer 12-6 is fastened to a safe 6.

[0070] Furthermore, the fixed localizer 12-7 is fastened to the external structure of the home 1. Moreover, the fixed localizer 12-8 (or a mobile localizer 13) is fastened to a vehicle 7.

[0071] The position of the control localizer 11 is taken as the origin of a coordinate system (three-dimensional coordinate system) used for position measurement.

[0072] Then, three fixed localizers 12 centered on the control localizer 11 are disposed (for example) in the plus direction on the X axis, Y axis and Z axis, and a reference coordinate system (three-dimensional coordinate system) used to measure the positions of the fixed localizers 12 or mobile localizers 13 in terms of three-dimensional coordinates is set on the basis of the positions of the control localizer 11 and three fixed localizers 12.

[0073] Subsequently, the other fixed localizers 12 are further disposed in regions that are the object of monitoring inside and outside the home 1, and the positions of the fixed localizers 12 thus disposed in the three-dimensional coordinate system are registered (stored in memory).

[0074] The users 2-1 and 2-2 who are authorized members of the home 1 such as family members, cohabitants or the like hold mobile localizers 13 that are capable of transmitting an ID code by wireless transmission.

[0075] The control localizer 11 hypothetically sets an external security surface 22 on the outside of the home 1 so that this external security surface surrounds the home 1, and hypothetically sets one or more internal security surfaces 21 on the inside of the home 1 so that these internal security surfaces surround designated regions inside the home 1.

[0076] Specifically, the internal security surfaces 21 can be present only on the inside of the external security surface 22.

[0077] Caretaker guard processing is automatically executed in cases where all of the mobile localizers 13 have exited to the outside of the external security surface 22. At-home guard processing is automatically executed in cases where all of the mobile localizers 13 have entered the interiors of the internal security surfaces 21 from the interior of the external security surface 22.

[0078] Non-guard processing is automatically executed in cases where one or more mobile localizers 13 are present in the region between the internal security surfaces 21 and the external security surface 22.

[0079] As will be described later with reference to Fig. 15, in cases where no internal security surfaces 21 are set, e. g., in the case of use in a vehicle 7, caretaker guard processing is executed when all of the mobile localizers 13 have exited to the outside of the external security surface 22, and non-guard processing is executed in all other cases.

In such cases, the external security surface 22 is set with respect to the vehicle 7.

[0080] The setting of the internal security surfaces 21 and external security surface 22 is performed as follows. Specifically, after fixed localizers 12 are set inside and outside the home 1, the control localizer 11 is set in the external security surface setting mode.

[0081] Then, the users 2-1 and 2-2 holding the mobile localizers 13 (or on which the mobile localizers 13 are mounted) move through the area outside the home 1, and when these users reach positions that are to be registered as points on the external security surface 22, the users press the position registration buttons of the mobile localizers 13. Positions on the external security surface 22 in the three-dimensional coordinate system are registered by performing this operation in a number of positions sufficient to specify the external security surface 22. Parameters that determine the rectangular solids used to determine the external security surface 22 are determined from the positions on the external security surface 22 in the three-dimensional coordinate system thus registered.

[0082] Next, one or more internal security surfaces 21 are set. First, the control localizer 11 is set in the internal security surface setting mode by the operation of the control localizer 11. Then, the users 2-1 and 2-2 holding the mobile localizers 13 (or on which the mobile localizers 13 are mounted) press the position registration button in appropriate positions while moving in order to set the internal security surfaces 21, and register a plurality of positions of the mobile localizer 13 in the three-dimensional coordinate system when the position registration button is pressed, for each internal security surface 21 (each closed internal security region surface). The parameters of the rectangular solids used to determine the internal security surfaces 21 are determined from the plurality of points thus registered in the three-dimensional coordinate system. When all of the internal security surfaces 21 that are to be set have been set, the control localizer 11 is set in the execution mode.

[0083] As a result, the security system automatically switches between three types of processing, i. e., caretaker guard processing, at-home guard processing and non-guard processing, in accordance with the position of the mobile localizer 13 and the positional relationship of the internal security surfaces 21 and external security surface 22. In cases where an actuator (e. g., a speaker or white smoke generating unit) is contained in the localizers, the localizers that are close to the position of the unauthorized intruder 3 are caused to generate a warning sound or caused to generate white smoke when an unauthorized intrusion is detected in caretaker guard processing. When the unauthorized intruder 3 moves through the home, localizers that are nearby are caused to generate a warning sound or caused to generate white smoke in accordance with the position of the intruder; accordingly, a plurality of localizers are caused to generate a warning sound or caused to generate white smoke so as to follow the unauthorized intruder 3.

[0084] In the case of at-home guard processing, the operation of the actuators is controlled so that the unauthorized intruder 3 tends not to approach the internal security surfaces 21, or the actuators are controlled so that the users 2-1 and 2-2 inside the internal security surfaces 21 can escape away from the unauthorized intruder 3.

[0085] A wireless network system which detects abnormalities by comparing respective distances between nodes (i. e., a distance matrix) under ordinary circumstances and respective distances between nodes (i. e., a distance matrix) during monitoring has been named the "Hagoromo System" by the present applicant, and an outline of this system is displayed on the web site shown below. Below, a matrix which has the distances between nodes as elements will be called a distance matrix.

Internet URL:http://www.hagoromoweb.com/

[0086] Furthermore, the Hagoromo System is also described in the specification of United States Patent No. 10/200,522 (filing date: July 23, 2002), which was filed with one of the inventors of the present application as the inventor.

[0087] In the present invention, a distance matrix between localizers (a matrix in which the distance between a localizer s and a localizer t is taken as the distance (s, t)) is monitored in a security system constituting a wireless network system consisting of a control localizer 11 and fixed localizers 12.

[0088] Next, the localizers will be described in greater detail.

[0089] Preferably, the localizers contain batteries. The reason for this is as follows: namely, even if the unauthorized intruder 3 interrupts the power supply that is supplied to the home 1 (a so-called AC (alternating current) power supply) during the intrusion, the localizers can execute specified processing for the unauthorized intrusion if the localizers operate by means of an internal power supply. Various types of batteries such as fuel cells, lithium ion batteries or the like can be used as batteries in the localizers.

[0090] Furthermore, batteries that can be charged may be disposed in the localizers, and may be used together with an AC power supply. Moreover, solar batteries may be installed in localizers that are disposed outdoors. Furthermore, an AC power supply may be used for indoor localizers. As a result, the frequency of battery replacement can be reduced, so that the time and expense required for maintenance can be reduced.

[0091] For example, a surface fastener manufactured by Velcro Co. or Kurare K.K. can be used for the simple mounting of the localizers on objects (in more concrete terms, the walls of the home 1, doors, safes, glass or the like).

[0092] The technique disclosed in United States Patent No. 5748891 may be used in the localizers. In this technique, the localizers can measure the distances between localizers, and can detect variations in the waveforms of wireless

signals transmitted between localizers, which are generated by the presence of objects between the localizers. The control localizer 11 uses a communications function between localizers to gather information that indicates the distances between these localizers or that indicates whether or not objects are present in the spaces between the localizers.

[0093] Furthermore, the localizers may also be realized by using the technique disclosed in Japanese Patent Application Laid-Open No. 2002-228744 or Japanese Patent Application Laid-Open No. 2000-111638 together with a GPS (global positioning system) technique and a wireless communications technique. Specifically, in this case, the distances to objects between nodes are measured by a radar function, the positions of the nodes are measured by the function of GPS receivers held on the nodes, and information relating to the distances to objects detected between the nodes as well as information relating to the positions of the nodes is transmitted to other nodes by a wireless communications function.

[0094] Next, the constructions of various types of localizers will be described with reference to Figs. 2 through 4.

[0095] Fig. 2 is a block diagram which shows an example of the construction of the control localizer 11. For example, the control unit 41 comprises a built-in type microprocessor (MPU (micro-processing unit)), and controls and unifies the overall operation of the control localizer 11 by executing a control program. The memory 42 comprises a semiconductor memory that allows reading and writing. For example, this memory 42 stores various types of parameters such as parameters that specify the external security surface 22, a distance matrix that indicates the distances between the control localizer 11 and the fixed localizers 12 and the distances between the fixed localizers 12, and the like. The control unit 41 stores various types of data (including parameters) in the memory 42, and reads out data that is stored in the memory 42.

[0096] The distance measuring unit 43 transmits pulse sequences that are used to measure the distances to other localizers to the wireless transmitting and receiving unit 44 and antenna unit 45, and receives pulse sequences that are transmitted from other localizers. The distance measuring unit 43 calculates the distances between the control localizer 11 and the partner [localizers] from the time difference between the instant in time at which a pulse sequence is generated by another partner localizer and the instant in time at which the control localizer 11 receives a pulse sequence on the basis of the received pulse sequences that are supplied from the wireless transmitting and receiving unit 44. The distance measuring unit 43 supplies information indicating the distances between the control localizer 11 and the partner [localizers] to the control unit 41.

[0097] The wireless transmitting and receiving unit 44 modulates a signal supplied from the distance measuring unit 43 or data communications unit 46 using an ID that specifies the network system assigned in network system units which is supplied from an ID code processing unit 47, and transmits signals by supplying the modulated signal to the antenna unit 45. The wireless transmitting and receiving unit 44 modulates the signals received via the antenna unit 45 using the ID specifying the network system (assigned in network system units) that is supplied from the ID code processing unit 47. The wireless transmitting and receiving unit 44 supplies the modulated signals to the distance measuring unit 43 or data communications unit 46.

[0098] In this way, communication with localizers belonging to other network systems, i. e., the mixing of signals, is prevented.

[0099] In cases where signals from partners are received, the antenna unit 45 receives the electromagnetic waves from the partners, and supplies signals corresponding to the received electromagnetic waves to the wireless transmitting and receiving unit 44. Furthermore, in cases where signals are to be transmitted to partners, the antenna unit 45 radiates electromagnetic waves on the basis of the signals supplied from the wireless transmitting and receiving unit 44, and transmits signals to the partners by wireless transmission.

[0100] The data communications unit 46 communicates various types of data with other localizers via the wireless transmitting and receiving unit 44 and antenna unit 45 under the control of the control unit 41.

[0101] The ID code processing unit 47 stores an ID that is peculiar to the control localizer 11 (hereafter called the localizer ID) and an ID specifying the network system (hereafter referred to as the network ID) that is assigned in units of the network system to which the control localizer 11 belongs (for example, a network system in units of one home 1 in cases where the security system is installed as a home security system). The ID code processing unit 47 supplies the localizer ID and network ID to the wireless transmitting and receiving unit 44.

[0102] Furthermore, a speaker 48 which generates a warning sound and a white smoke generating module 49 which generates white smoke that is used to repulse the unauthorized intruder 3 are connected to the control unit 41. Moreover, a wireless notification unit 50 which is used to make a wireless notification to a communications device belonging to a specified external party (e. g., the telephone of a security firm or the mobile phone of the owner of the home) is connected to the control unit 41.

[0103] The input unit 51 comprises a mode changing switch or operating button, and supplies signals that designate the settings of the coordinate system, the setting of the external security surface 22, the settings of the internal security surface 21, or the selection of the mode such as the execution mode or the like to the control unit 41 in accordance with operations performed by the user 2-1 or 2-2. The display unit 52 comprises a liquid crystal display device, organic EL (electroluminescence) display device or the like, and displays the results of auto-diagnosis, the residual charges

of the batteries of the respective localizers, the residual amounts of the white smoke raw material of the white smoke generating modules and the like (indicated by data received from the respective localizers) under the control of the control unit 41.

[0104] The power supply unit 53 comprises a battery such as a primary cell or secondary cell, an AC (alternating current)-DC (direct current) converter or the like, and supplies a power source to respective parts of the control localizer 11.

[0105] Fig. 3 is a block diagram which shows an example of the construction of the fixed localizers 12. The construction of the fixed localizers 12 is substantially the same as the construction of the control localizer 11; however, no wireless notification unit or display unit is installed in the fixed localizers 12.

[0106] For example, the control unit 71 comprises a built-in type microprocessor (MPU), and controls and unifies the overall operation of the fixed localizers 12 by executing a control program. The memory 72 comprises a semiconductor memory that allows reading and writing, and stores various types of parameters that are required for various types of processing. The control unit 71 stores various types of data (including parameters) in the memory 72, and reads out data that is stored in the memory 72.

[0107] The distance measuring unit 73 transmits (emits) pulse sequences that are used to measure the distances to other localizers to the wireless transmitting and receiving unit 74 and antenna unit 75, and receives pulse sequences that are transmitted from other localizers. The distance measuring unit 73 measures the distances between fixed localizers 12 and partner [localizers] from the time difference between the instant in time at which a pulse sequence is generated by another partner localizer and the instant in time at which a fixed localizer 12 receives a pulse sequence on the basis of the received pulse sequences that are supplied from the wireless transmitting and receiving unit 74. The distance measuring unit 73 supplies information indicating the distances between fixed localizers 12 and partner [localizers] to the control unit 71.

[0108] The wireless transmitting and receiving unit 74 modulates a signal supplied from the distance measuring unit 73 or data communications unit 76 using a network ID which is supplied from an ID code processing unit 77, and transmits signals by supplying the modulated signal to the antenna unit 75. The wireless transmitting and receiving unit 74 demodulates the signals received via the antenna unit 75 using the network ID that is supplied from the ID code processing unit 77. The wireless transmitting and receiving unit 74 supplies the modulated signals to the distance measuring unit 73 or data communications unit 76.

[0109] In this way, communication with localizers belonging to other network systems, i. e., the mixing of signals, is prevented.

[0110] In cases where signals from partners are received, the antenna unit 75 receives the electromagnetic waves from the partners, and supplies signals corresponding to the received electromagnetic waves to the wireless transmitting and receiving unit 74. Furthermore, in cases where signals are to be transmitted to partners, the antenna unit 75 radiates electromagnetic waves on the basis of the signals supplied from the wireless transmitting and receiving unit 74, and transmits signals to the partners by wireless transmission.

[0111] The data communications unit 76 communicates various types of data with other localizers via the wireless transmitting and receiving unit 74 and antenna unit 75 under the control of the control unit 71.

[0112] The ID code processing unit 77 stores localizer IDs that are peculiar to the fixed localizers 12, and a network ID specifying the network system that is assigned in units of the network system to which the fixed localizers 12 belong. The ID code processing unit 77 supplies the localizer IDs and the network ID to the wireless transmitting and receiving unit 74.

[0113] Furthermore, a speaker 78 that generates a warning sound and a white smoke generating module 79 which generates white smoke that is used to repulse unauthorized intruders 3 are connected to the control unit 71.

[0114] The operating button 80 supplies signals that are used to select the mode such as coordinate system setting or the like to the control unit 71 in accordance with operations performed by the users 2-1 and 2-2. For example, when the operating button 80 is pressed, processing that sets the coordinate system with the control localizer 11 as the origin is executed. Details of the processing that sets the coordinate system will be described later.

[0115] The power supply unit 81 comprises a battery such as a primary cell, secondary cell or the like, an AC-DC converter or the like, and supplies a power source to respective parts of the fixed localizers 12.

[0116] Fig. 4 is a block diagram which shows an example of the construction of the mobile localizers 13. The construction of the mobile localizers 13 is substantially similar to the construction of the fixed localizers 12; however, no white smoke generating modules are installed in the mobile localizers 13. The mobile localizers 13 are constructed on the assumption that the users 2-1 and 2-2 constantly carry these localizes mounted in the form of a wristwatch or pendant.

[0117] For example, the control unit 101 comprises a built-in type microprocessor (MPU), and controls and unifies the overall operation of the mobile localizers 13 by executing a control program. The memory 102 comprises a semiconductor memory that allows reading and writing, and stores various types of parameters that are required for various types of processing. The control unit 101 stores various types of data (including parameters) in the memory 102, and

reads out data that is stored in the memory 102.

[0118] The distance measuring unit 103 transmits (emits) pulse sequences used to measure distances to other localizers to the wireless transmitting and receiving unit 104 and antenna unit 105, and receives pulse sequences that are transmitted from other localizers. The distance measuring unit 103 calculates the distances between the mobile localizers 13 and partners from the time difference between the instant in time at which a pulse sequence is generated by another partner localizer and the instant in time at which a mobile localizer 13 receives a pulse sequence on the basis of the received pulse sequences that are supplied from the wireless transmitting and receiving unit 104. The distance measuring unit 103 supplies information indicating the distances between mobile localizers 13 and partner [localizers] to the control unit 101.

[0119] The wireless transmitting and receiving unit 104 modulates a signal supplied from the distance measuring unit 103 or data communications unit 106 using a network ID which is supplied from an ID code processing unit 107, and transmits signals by supplying the modulated signal to the antenna unit 105. The wireless transmitting and receiving unit 104 modulates the signals received via the antenna unit 105 using the network ID that is supplied from the ID code processing unit 107. The wireless transmitting and receiving unit 104 supplies the modulated signals to the distance measuring unit 103 or data communications unit 106.

[0120] In this way, communication with localizers belonging to other network systems, i. e., the mixing of signals, is prevented.

[0121] In cases where signals transmitted to partners, the antenna unit 105 receives the electromagnetic waves from the partners, and supplies signals corresponding to the received electromagnetic waves to the wireless transmitting and receiving unit 104. Furthermore, in cases where signals are to be received by partners, the antenna unit 105 radiates electromagnetic waves on the basis of the signals supplied from the wireless transmitting and receiving unit 104, and transmits signals to the partners by wireless transmission.

[0122] The data communications unit 106 communicates various types of data with other localizers via the wireless transmitting and receiving unit 104 and antenna unit 105 under the control of the control unit 101.

[0123] The ID code processing unit 107 stores localizer IDs that are peculiar to the mobile localizers 13, and a network ID specifying the network system that is assigned in units of the network system to which the mobile localizers 13 belong. The ID code processing unit 107 supplies the localizer IDs and the network ID to the wireless transmitting and receiving unit 104.

[0124] Furthermore, a speaker 108 used to generate a warning sound is connected to the control unit 101.

[0125] The operating button 109 supplies signals that are used to select the mode to the control unit 101 in accordance with operations performed by the users 2-1 and 2-2.

[0126] The power supply unit 110 comprises a battery or the like, and supplies a power source to various parts of the mobile localizers 13.

[0127] Next, the setting of the three-dimensional coordinate system in the security system of the present invention used as a network system will be described.

[0128] When the input unit 51 is operated by the user 2-1 or 2-2 (constituting the operator), the mode of the control localizer 11 shifts to the coordinate system setting mode. Then, the operator selects a fixed localizer 12-1 among the fixed localizers 12 that are already attached, and presses the operating button 80 of this fixed localizer 12-1.

[0129] Consequently, the control localizer 11 and fixed localizer 12-1 measure the distance between the two localizers, and the control localizer 11 sets the fixed localizer 12-1 in a one-dimensional coordinate system (with the X axis as the positive direction) using the control localizer 11 as the origin.

[0130] Next, the operator selects the fixed localizer 12-2 which is on the same plane as the control localizer 11 and fixed localizer 12-1, and presses the operating button 80 that is disposed on this fixed localizer 12-2. As a result, the control localizer 11 and fixed localizer 12-1 measure the respective distances to the fixed localizer 12-2. The fixed localizer 12-1 transmits information indicating the distance from the fixed localizer 12-1 to the fixed localizer 12-2 to the control localizer 11.

[0131] Here, the distance between the control localizer 11 and fixed localizer 12-1 is expressed as the distance a, and the distance between the control localizer 11 and the fixed localizer 12-2 is expressed as the distance b. Furthermore, the distance between the fixed localizer 12-1 and fixed localizer 12-2 is expressed as the distance c.

[0132] As is shown in Fig. 5, Equations (1) and (2) hold true for the position (x2, y2) of the fixed localizer 12-2 in the two-dimensional coordinate system.

$$x2=(c^2-b^2-a^2)/2a \tag{1}$$

$$y2=(b^2-x2^2)^{1/2} \tag{2}$$

[0133] In this coordinate system, the control localizer 11 is present at the origin, so that the position of the control localizer 11 in the three-dimensional coordinate system is (0, 0, 0). The position of the fixed localizer 12-1 in the three-dimensional coordinate system is (a, 0, 0). Furthermore, the position of the fixed localizer 12-2 in the three-dimensional coordinate system is (x2, y2, 0).

[0134] Next, as is shown in Fig. 1, the operator selects the fixed localizer 12-3 which is not on the plane formed by the control localizer 11, fixed localizer 12-1 and fixed localizer 12-2 (i. e., which is in a position that is removed from this plane), and presses the operating button 80 that is disposed on this fixed localizer 12-3.

[0135] After the three-dimensional coordinates determined by the positions of the control localizer 11, fixed localizer 12-1 and fixed localizer 12-2 have been set, the distance between the control localizer 11 and the fixed localizer 12-3, the distance between the fixed localizer 12-1 and the fixed localizer 12-3 and the distance between the fixed localizer 12-2 and the fixed localizer 12-3 are measured by this operation. The fixed localizers 12-1 through 12-3 transmit information indicating the distance between the control localizer 11 and the fixed localizer 12-3, the distance between the fixed localizer 12-1 and the fixed localizer 12-3 and the distance between the fixed localizer 12-2 and the fixed localizer 12-3 to the control localizer 11.

[0136] On the basis of the received information indicating the distance between the control localizer 11 and the fixed localizer 12-3, the distance between the fixed localizer 12-1 and the fixed localizer 12-3 and the distance between the fixed localizer 12-2 and the fixed localizer 12-3, the control localizer 11 determines the position (x3, y3, z3) of the fixed localizer 12-3 in the three-dimensional coordinate system by solving simultaneous equations with the position of the fixed localizer 12-3 in the three-dimensional coordinate system as the unknown quantity.

[0137] The control localizer 11 stores information indicating the positions of the respective fixed localizers 12 in the three-dimensional coordinate system in association with the localizer IDs of these fixed localizers 12.

[0138] Thus, if the distances to fixed localizers 12 or mobile localizers 13 focused on three more localizers, i. e., the control localizer 11 and fixed localizers 12, whose positions in the three-dimensional coordinate system are known are determined, the positions of the fixed localizers 12 or mobile localizers 13 (in the three-dimensional coordinate system) on which attention is focused can be determined by solving simultaneous equations.

[0139] When a state which is such that the positions of desired fixed localizers 12 or mobile localizers 13 in the three-dimensional coordinate system can be determined as described above is obtained, it can be said that the setting of the three-dimensional coordinate system is completed.

[0140] When the setting of the three-dimensional coordinate system of the network system has been completed, the respective fixed localizers 12 within the network system measure the distances to the fixed localizers 12 whose three-dimensional coordinates have already been registered, and measured distance transmission information in the format shown below, which includes the measured distances, is transmitted to the control localizer 11.

Measured distance transmission information:

(Own node number, partner node number, distance between own node and partner node)

[0141] Here, the localizer IDs can be used as the "own node number" and "partner node number". Furthermore, in the network system, for example, node numbers indicating the order of registration which are assigned at the time of registration can be used as the "own node number" and "partner node number".

[0142] The control localizer 11 stores a distance matrix between localizers or a list of the position coordinates of localizers as a fingerprint constituting specific information relating to the network system consisting of the control localizer 11 and fixed localizers 12. If the elements of the inter-localizer distance matrix indicating the distances between localizers s and localizers t are designated as M(s, t), then M(s, t) can be expressed by Equation (3).

$$M(s,t)=\begin{cases}\text{Distance}(s,t): & \text{if distance mesuring was successful.}\\ -1: & \text{if distance measuring failed.}\end{cases} \quad (3)$$

[0143] Here, distance(s, t) is a value that indicates the distance between a localizer s and a localizer t.

[0144] Next, the setting of the external security surface 22 and internal security surfaces 21 will be described.

[0145] First, the setting of the external security surface 22 is performed.

[0146] When the setting of the three-dimensional coordinate system is completed, the user 2-1 or 2-2 (constituting the operator) operates the input unit 51 of the control localizer 11, so that the mode of the control localizer 11 is shifted to the setting mode for the external security surface 22.

[0147] Then, while carrying one of the mobile localizers 13, the operator sets the external security surface 22 as follows:

[0148] As a first step, the operator moves the mobile localizer 13 to the presumed vicinity of the external security surface 22. As a second step, the operator presses the operating button 109 (as a position registration button) of the mobile localizer 13. Then, as a third step, the fixed localizers 12 respectively measure the distances from themselves to the mobile localizer 13 in this case, and the measured distances are transmitted to the control localizer 11 as measured distance transmission information in the format described above. The control localizer 11 calculates the position of the mobile localizer 13 in the three-dimensional coordinate system on the basis of the distances between the respective fixed localizers 12 and the mobile localizer 13 contained in the measured distance transmission information that is transmitted from the respective fixed localizers 12, and stores the calculated position of the mobile localizer 13 in the three-dimensional coordinate system as a registration point.

[0149] The processing of the first step through third step is repeated until the number of registration points reaches a specified number, e. g., 10 points. However, the operator registers the positions in the three-dimensional coordinate system so that lines connecting the registration points are present on all of the planes of the envisioned external security surface 22.

[0150] As a fourth step, the control localizer 11 determines the smallest rectangular solid that surrounds the registered registration points. Here, the floor surface of this smallest rectangular solid is set as a plane that is 1 meter lower than the mean value of the z coordinate positions (positions in the vertical direction of the three-dimensional coordinate system) of the respective registration points. The reason for this is that the positioning of the mobile localizer 13 in the vicinity of the floor surface or the vicinity of the ceiling surface is in most cases either difficult to accomplish, or else requires an unreasonable physical attitude on the part of the operator.

[0151] As a fifth step, the control localizer 11 enlarges the smallest rectangular solid determined by the processing of the fourth step by a specified factor (e. g., 150%) about the center point of this smallest rectangular solid, and registers (stores in memory) the surface of the enlarged rectangular solid as the external security surface 22. The reason for this is as follows: namely, it may be envisioned that there will be cases in which it is difficult to move around the outside of the home 1 while holding the mobile localizer 13 in order to provide registration points outside the home 1; accordingly, the system is devised so that the external security surface 22 can be set outside the home 1 by movement only inside the home 1.

[0152] Next, the setting of the internal security surfaces 21 is performed.

[0153] Such internal security surfaces 21 are set in cases where a warning of intrusions from the outside is to be made even in cases where authorized members such as the users 2-1, 2-2 and the like are present inside the home, as in a home security system. In cases where no authorized member (holder of a mobile localizer 13) is present between the internal security surfaces 21 and external security surface 22, there is no person monitoring unauthorized intrusions beyond the external security surface 22; accordingly, by setting internal security surfaces 21, the security system can be devised so that monitoring processing between the internal security surfaces 21 and external security surface 22 can be automatically executed.

[0154] The user 2-1 or 2-2 (constituting the operator) operates the input unit 51 of the control localizer 11 so that the mode of the control localizer 11 is shifted to the setting mode for the internal security surfaces 21. Then, the operator sets the internal security surfaces 21 as follows while carrying one of the mobile localizers 13.

[0155] As a first step, the operator moves the mobile localizer 13 to the presumed vicinity of the internal security surface 21. As a second step, the operator presses the operating button 109 (as a position registration button) of the mobile localizer 13. Then, as a third step, the fixed localizers 12 respectively measure the distances from themselves to the mobile localizer 13 in this case, and the measured distances are transmitted to the control localizer 11 as measured distance transmission information in the format described above. The control localizer 11 calculates the position of the mobile localizer 13 in the three-dimensional coordinate system on the basis of the distances between the respective fixed localizers 12 and the mobile localizer 13 contained in the measured distance transmission information that is transmitted from the respective fixed localizers 12, and stores the calculated position of the mobile localizer 13 in the three-dimensional coordinate system as a registration point.

[0156] The processing of the first step through third step is repeated until the number of registration points reaches a specified number, e. g., 10 points. However, the operator registers the positions in the three-dimensional coordinate system so that lines connecting the registration points are present on all of the planes of the envisioned internal security surfaces 21.

[0157] As a fourth step, the control localizer 11 determines the smallest rectangular solid that surrounds the registered registration points. Here, the floor surface of this smallest rectangular solid is set as a plane that is 1 meter lower than the mean value of the z coordinate positions (positions in the vertical direction of the three-dimensional coordinate system) of the respective registration points, the ceiling surface of the smallest rectangular solid is set as a place that is 1 meter upper than the mean value of the z coordinate positions (positions in the vertical direction of the three-dimensional coordinate system) of the respective registration points. The reason for this is that the positioning of the mobile localizer 13 in the vicinity of the floor surface or the vicinity of the ceiling surface is in most cases either difficult to accomplish, or else requires an unreasonable physical attitude on the part of the operator.

[0158] As a fifth step, the control localizer 11 registers (stores in memory) the smallest rectangular solid determined by the processing of the fourth step as an internal security surface 21.

[0159] In cases where non-guard processing is performed with an authorized person present inside, as in a vehicle 7, the processing that sets the internal security surfaces 21 is omitted.

[0160] A concrete example of application to a home security system will be described with reference to Fig. 1.

[0161] In the example shown in Fig. 1, the control localizer 11 is disposed on the inside wall of a home 1 constituting one example of an object of security. Furthermore, a fixed localizer 12-1 and a fixed localizer 12-2 are disposed on the wall on which the control localizer 11 is disposed. Moreover, a fixed localizer 12-3 is disposed on a different wall from the wall on which the control localizer 11 is disposed.

[0162] The respective localizers are fastened to these objects by means of surface fasteners.

[0163] A three-dimensional coordinate system with the control localizer 11 as the origin is set by the processing described above, the positions of all of the fixed localizers 12 in the three-dimensional coordinate system are measured, and the control localizer 11 stores the positions of the respective localizers in the three-dimensional coordinate system in memory in association with the localizers IDS of the respective localizers.

[0164] Then, the external security surface 22 and internal security surfaces 21 are set. In this case, the users 2-1 and 2-2 who are authorized members (inhabitants) of this home 1 have mobile localizers 13 mounted on their bodies as pendants or wristwatches.

[0165] Here, one internal security surface 21 may be set inside one external security surface 22 as shown in Fig. 1, or two internal security surfaces 21, i. e., an internal security surface 21-1 and an internal security surface 21-2, may be set inside one external security surface 22 as shown in Fig. 6.
In this latter case, the processing that sets an internal security surface 21 is performed twice. Furthermore, the number of internal security surfaces 21 may be an arbitrary number.

[0166] When the external security surface 22 is registered, and the internal security surfaces 21 are registered (if necessary), the processing of the execution mode is performed on the basis of the registered external security surface 22 or internal security surfaces 21.

[0167] Even during the execution of this execution mode, a shift to another mode (e. g., the setting mode for the external security surface 22) can be effected if the switch of the input unit 51 of the control localizer 11 is operated. Specifically, the processing of the execution mode is ended, and the execution of the processing of another mode that is to be started is initiated, by the processing of step S7 in Fig. 7 described later.

[0168] In this execution mode, the processing that is started is automatically switched in accordance with the positional relationship of the mobile localizer 13, external security surface 22 and internal security surfaces 21. Specifically, one of three types of processing, i. e., caretaker guard processing, at-home guard processing or non-guard processing, is automatically started at an appropriate time.

[0169] Next, the processing of the execution mode will be described with reference to the flow chart shown in Fig. 7.

[0170] In step S1, the control localizer 11 and fixed localizers 12 measure the positions of all of the mobile localizers 13 that issue ID codes (network IDs) for authorized members.

[0171] Specifically, the control localizer 11 transmits instructions to measure and report the distances to the mobile localizers 13 to the respective fixed localizers 12 in the network system. The distance measuring units 73 of the respective fixed localizers 12 receiving these instructions measure the distances to the respective mobile localizers 13.

[0172] Each of the fixed localizers 12 notifies the control localizer 11 of the distances to the mobile localizers 13 by transmitting measured distance transmission information in the abovementioned format that indicates the distances between itself and the respective mobile localizers 13 to the control localizer 11.

[0173] Furthermore, the distance measuring unit 43 of the control localizer 11 measures the distances to the mobile localizers 13. The control localizer 11 calculates and stores in memory the positions of the respective mobile localizers 13 on the basis of the results of the measurement of the distances to the mobile localizers 13 and the notification from the respective fixed localizers 12.

[0174] In step S2, the control unit 41 of the control localizer 11 judges whether or not there are mobile localizers 13 for which position measurement has been successful. Specifically, if there are absolutely no mobile localizers 13 in places that allow measurement of the distance between these mobile localizers and fixed localizers 12, or in cases where such mobile localizers are present, but comprise only mobile localizers 13 whose distance cannot be measured because of loss of the battery power supply, the control localizer 11 judges that there are no mobile localizers 13 allowing successful position measurement. Furthermore, in cases where the control localizer 11 and fixed localizers 12 cannot communicate with other mobile localizers 13 belonging to the network system so that mutual distances cannot be measured, and only mobile localizers 13 belonging to other networks are in positions that allow communication and distance measurement, the control localizer 11 judges that there are no mobile localizers 13 allowing successful position measurement.

[0175] The mobile localizers 13 communicate or judge mutual distances by means of signals modulated using a network ID which is a code peculiar to the network system to which these mobile localizers 13 belong. In cases where

there are one or more mobile localizers 13 allowing successful position measurement belonging to the network system to which a given mobile localizer 13 belongs, it is judged that there are mobile localizers 13 allowing successful position measurement.

[0176] In cases where it is judged in step S2 that there are mobile localizers 13 allowing successful position measurement, the processing proceeds to step S3, and the control unit 41 of the control localizer 11 judges whether or not mobile localizers 13 are present inside the external security surface 22. The control localizer 11 judges whether or not mobile localizers 13 are present inside the external security surface 22 by comparing the coordinate positions indicating the scope of the external security surface 22 and the coordinate positions of the mobile localizers 13.

[0177] In cases where it is judged in step S3 that there are mobile localizers 13 present inside the external security surface 22, the processing proceeds to step S4, and the control unit 41 of the control localizer 11 judges whether or not internal security surface 21 have been set.

[0178] For example, in cases where authorized members using the home 1 are sleeping in the bedroom at night, the bedroom region is taken as an internal security surface 21. As a result, the network system of the bedroom is appropriately controlled, and the operation of the actuators (e. g. white smoke generating modules 49) can be controlled so that unauthorized intruders 3 do not approach the internal security surface 21 (e. g., bedroom).

[0179] In cases where it is judged in step S4 that an internal security surface 21 has been set, the processing proceeds to step S5.

[0180] In step S5, the control unit 41 of the control localizer 11 judges whether or not all of the mobile localizers 13 allowing successful position measurement are positioned inside the internal security surface 21. For example, in cases where the internal security surface 21 is the bedroom, it is judged whether or not [all of] the authorized members using the home 1 are in the bedroom.

[0181] In cases where it is judged in step S5 that not all of the mobile localizers 13 allowing successful position measurement are positioned inside the internal security surface 21, the processing proceeds to step S6, the control localizer 11 executes non-guard processing, and the processing proceeds to step S7. The details of non-guard processing will be described later.

[0182] In cases where it is judged in step S5 that not all of the mobile localizers 13 allowing successful position measurement are positioned inside the internal security surface 21, since it has been judged in step S3 that mobile localizers 13 positioned inside the external security surface 22 are present, and since it has been judged in step S4 that an internal security surface 21 has been set, this means that (for example) either the mobile localizer 13-1 or the mobile localizer 13-3 is positioned on the outside of the internal security surface 21 and on the inside of the external security surface 22 as shown in Fig. 8. In such cases, since there is no need to perform guard processing, non-guard processing is performed.

[0183] In step S7, the control unit 41 of the control localizer 11 judges whether or not mode switching has been instructed. For example, in step S7, the control localizer 11 checks in order to ascertain whether or not an operation shifting to another mode such as the setting of an internal security surface 21, the setting of an external security surface 22 or the like has been applied to the input unit 51.

[0184] In cases where it is judged in step S7 that no mode change has been instructed, the processing returns to step S1, and the abovementioned processing is repeated.

[0185] In cases where it is judged in step S7 that a mode change has been instructed, the processing of the execution mode is ended.

[0186] In cases where it is judged in step S5 that all of the mobile localizers 13 allowing successful position judgment are positioned inside the internal security surface 21, the processing proceeds to step S8, the control localizer 11 executes at-home guard processing, and the processing proceeds to step S7. The details of at-home guard processing will be described later.

[0187] In cases where it is judged in step S5 that all of the mobile localizers 13 allowing successful position judgment are positioned inside the internal security surface 21, since it has been judged in step S3 that mobile localizers 13 positioned inside the external security surface 22 are present, and since it has been judged in step S4 that an internal security surface 21 has been set, this means that (for example) both of the mobile localizers 13-1 and 13-2 are positioned inside the internal security surface 21 as shown in Fig. 9.
In such cases, since it is necessary to protect the authorized members inside the internal security surface 21, at-home guard processing is executed.

[0188] In cases where it is judged in step S4 that no internal security surface 21 has been set, the processing proceeds to step S9, the control localizer 11 executes non-guard processing, and the processing then proceeds to step S7.

[0189] In cases where it is judged in step S3 that no mobile localizers 13 positioned inside the external security surface 22 are present, or in cases where it is judged in step S2 that there are no mobile localizers 13 allowing successful position measurement, i. e., in cases where the positions of all of the mobile localizers 13 allowing successful position judgment are outside the external security surface 22, the processing proceeds to step S10, the control localizer 11 executes caretaker guard processing, and the processing then proceeds to step S7.

[0190] For example, this means that the security system automatically executes caretaker guard processing immediately after the authorized members on which the mobile localizers 13 are mounted leave this home 1 as shown in Fig. 10.

[0191] In a conventional home security system, when the home is to be guarded in the absence of the inhabitants, a button operation must be performed in order to switch to the caretaker guard mode. If this is forgotten, the painstakingly devise home security system usually does not operate at the most important time. The home security system of the present invention does not require a bothersome operation, and can securely perform processing that securely protects the object of security.

[0192] Next, the details of non-guard processing will be described.

[0193] Fig. 11 is a flow chart which illustrates the details of non-guard processing corresponding to the processing of step S6 or step S9 in Fig. 7.

[0194] In step S21, the control localizer 11 and respective fixed localizers 12 measure the distances between the control localizer 11 and the fixed localizers 12, and the distances between the respective fixed localizers 12.

[0195] For example, under the control of the control unit 41, the distance measuring unit 43 of the control localizer 11 measures the distances between the control localizer 11 and the respective fixed localizers 12, and supplies the measurement results to the control unit 41. Under the control of the control units 71, the distance measuring units 73 of the respective fixed localizers 12 measure the distances between themselves and the other fixed localizers 12. The control units 71 of the respective fixed localizers 12 cause the wireless transmitting and receiving units 74 to transmit measured distance transmission information indicating the distances between themselves and other fixed localizers 12 obtained by this measurement to the control localizer 11.

[0196] The control unit 41 of the control localizer 11 causes the wireless transmitting and receiving unit 44 to receive the measured distance transmission information indicating the distances between the fixed localizers 12 that is transmitted from the respective fixed localizers 12. The control unit 41 of the control localizer 11 acquires the measured distance transmission information indicating the distances between the fixed localizers 12 that is received by the wireless transmitting and receiving unit 44 via the data communications unit 46.

[0197] In step S22, the control localizer 11 produces an inter-localizer distance matrix that indicates the distances between the control localizer 11 and the fixed localizers 12, and the distances between the respective fixed localizers 12. For example, the control unit 41 of the control localizer 11 produces an inter-localizer distance matrix whose elements are the distances between the control localizer 11 and fixed localizers 12 and the distances between the respective fixed localizers 12 by arranging values that indicate the distances between the control localizer 11 and the respective fixed localizers 12 and values that indicate the distances between the respective fixed localizers 12 in the order of the values of the localizer IDs on the basis the measured distance transmission information indicating the distances between the control localizer 11 and the respective fixed localizers 12 and the distances between the respective fixed localizers 12 acquired by the processing of step S21.

[0198] In step S23, the control localizer 11 stores the inter-localizer distance matrix in memory. For example, in step S23, the control unit 41 of the control localizer 11 stores the inter-localizer distance matrix in the memory 42.

[0199] In step S24, the control localizer 11 and respective fixed localizers 12 perform an auto-diagnosis. For example, in step S24, the control localizer 11 and respective fixed localizers 12 respectively diagnose the respective units that constitute these localizers themselves.

[0200] To describe this in greater detail, for example, in step S24, the control localizer 11 and respective fixed localizers 12 perform an auto-diagnosis by investigating the residual charge of the batteries of the power supply unit 53 or power supply unit 81, and the residual amount of the raw materials of the white smoke or the like of the white smoke generating modules 49 or white smoke generating modules 79. In greater detail, the control localizer 11 and respective fixed localizers 12 perform an auto-diagnosis by comparing the residual charge of the batteries of the power supply unit 53 or power supply unit 81 with a specified threshold value, or comparing the residual amount of the raw materials of the white smoke or the like of the white smoke generating modules 49 or white smoke generating modules 79 with another specified threshold value. The fixed localizers 12 notify the control localizer 11 of the results of this auto-diagnosis.

[0201] In step S25, the control unit 41 of the control localizer 11 judges whether or not there is any trouble on the basis of the results of the auto-diagnosis of the control localizer 11 and the results of the auto-diagnosis of the respective fixed localizers 12 (of which the control localizer 11 has been notified by the respective fixed localizers 12).

[0202] In cases where it is judged in step S25 that trouble has occurred, the processing proceeds to step S26, the control unit 41 of the control localizer 11 operates the speaker 48 or the display unit 52, thus notifying the users 2-1 and 2-2 of the trouble, and the non-guard processing is ended. For example, in step S26, the control unit 41 causes the speaker to output a sound that indicates the content of the trouble. Alternatively, for example, in step S26, the control unit 41 causes the display device 52 to display an image or characters that indicate the content of the trouble.

[0203] In cases where it is judged in step S25 that there is no trouble, since there is no need for notification of trouble, the processing of step S26 is skipped, and the non-guard processing is ended.

[0204] Furthermore, the processing of steps S21 through S26 may be repeated.

[0205] Next, the details of at-home guard processing will be described.

[0206] Fig. 12 is a flow chart illustrating the details of at-home guard processing, which corresponds to the processing of step S8 in Fig.7.

[0207] In step S41, the control localizer 11 and respective fixed localizers 12 measure the distances between the control localizer 11 and the fixed localizers 12, and the distances between the respective fixed localizers 12.

[0208] For example, under the control of the control unit 41, the distance measuring unit 43 of the control localizer 11 measures the distances between the control localizer 11 and the respective fixed localizers 12, and supplies the measurement results to the control unit 41. Furthermore, under the control of the control units 71, the distance measuring units 73 of the respective fixed localizers 12 measure the distances between themselves and other fixed localizers 12. The control units 71 of the respective fixed localizers 12 cause the wireless transmitting and receiving units 74 to transmit measured distance transmission information indicating the distances between themselves and other fixed localizers 12 (acquired by the abovementioned measurements) to the control localizer 11.

[0209] The control unit 41 of the control localizer 11 causes the wireless transmitting and receiving unit 44 to receive measured distance transmission information indicating the distances between respective fixed localizers 12 that is transmitted from the respective fixed localizers 12. The control unit 41 of the control localizer 11 acquires the measured distance transmission information indicating the distances between the respective fixed localizers 12 that is received by the wireless transmitting and receiving unit 44 via the data communications unit 46.

[0210] In step S42, the control localizer 11 produces an inter-localizer distance matrix that indicates the distances between the control localizer 11 and fixed localizers 12, and the distances between the respective fixed localizers 12. For example, the control unit 41 of the control localizer 11 produces an inter-localizer distance matrix whose elements are the distances between the control localizer 11 and fixed localizers 12 and the distances between the respective fixed localizers 12 by arranging values that indicate the distances between the control localizer 11 and the respective fixed localizers 12 and values that indicate the distances between the respective fixed localizers 12 in the order of the values of the localizer IDs on the basis the measured distance transmission information indicating the distances between the control localizer 11 and the respective fixed localizers 12 and the distances between the respective fixed localizers 12 acquired by the processing of step S41.

[0211] In step S43, the control unit 41 of the control localizer 11 judges whether or not there are any differences between the inter-localizer distance matrix that is produced and an inter-localizer distance matrix stored in memory for the control localizer 11 and fixed localizers 12 that are inside the external security surface 22 and outside the internal security surface 21.

[0212] In non-guard processing, the inter-localizer distance matrix that is stored in memory is further updated to values that indicated the distances between the localizers at that point in time (i. e., the point in time at which the non-guard processing is executed). Accordingly, in step S43, differences between the last updated inter-localizer distance matrix and the current inter-localizer distance matrix are detected. These differences are calculated as the sum of the absolute values of the differences for each corresponding element in the range in which distance measurement is possible within the inter-localizer distance matrix that is stored in memory and the inter-localizer distance matrix at the current point in time.

[0213] However, in order to prevent the detection of abnormalities due to the movement of authorized members such as the users 2-1 and 2-2 of the home 1 or the like inside the internal security surface 21 (i. e., in order to prevent erroneous detection), differences generated by the movement of the localizers themselves inside the internal security surface 21 are not used in the calculation of this sum.

[0214] The control units 41 judge that there is an abnormality (i. e., "abnormality present") if the abovementioned sum exceeds a predetermined threshold value. If the fixed localizers 12 are mounted on the window 4, door 5 or safe 6 as shown in Fig. 1, then the distances between the localizers mounted on the window 4 and door 5 and other localizers will vary if the window 4 moves (is opened), or if the door 5 moves (is opened). The same is true if the safe 6 moves. As a result, the inter-localizer distance matrix varies.

[0215] In cases where it is judged in step S43 that there are no differences between the inter-localizer distance matrix that is produced and the inter-localizer distance matrix that is stored in memory for the control localizer 11 and fixed localizers 12 that are inside the external security surface 22 and outside the internal security surface 21, the processing proceeds to step S44, and the control localizer 11 and fixed localizers 12 analyze the wireless signals communicating with the outside of the internal security surface 21.

[0216] In cases where a human being is present between localizers, the waveform of the wireless signals exchanged between the localizers varies as a result of being affected by this human body; accordingly, the control localizer 11 and fixed localizers 12 detect the presence of a human body between the control localizer 11 and fixed localizers 12, or between the respective fixed localizers 12, by waveform analysis. A fixed localizer 12 that has detected the presence of a human body then notifies the control localizer 11 of the detection of this human body by transmitting human body detection information in the format shown below to the control localizer 11.

Human body detection information:

(Own node number, partner node number, parameter indicating human body detection)

[0217] Here, the localizer IDs can be used as the "own node number" and "partner node number". Furthermore, in the network system, for example, node numbers indicating the order of registration which are assigned at the time of registration can be used as the "own node number" and "partner node number".

[0218] The human body detection information indicates that a human body has been detected between the localizer indicated by the "own node number" and the localizer indicated by the "partner node number". A flag indicating the presence or absence of a human body or a parameter indicating the thickness of the human body may be used as a detection parameter in this case.

[0219] Thus, the respective fixed localizers 12 transmit human body detection information indicating the results of the waveform analysis of the wireless signal to the control localizer 11.

[0220] In step S45, the control unit 41 of the control localizer 11 judges whether or not a human body is present between the control localizer 11 and fixed localizers 12 or between the respective fixed localizers 12 inside the external security surface 22 and outside the internal security surface 21 on the basis of the human body detection information that is transmitted from the respective fixed localizers 12, or the results of human body detection by the control localizer 11 itself.

[0221] In cases where it is judged in step S45 that no human being is present between the control localizer 11 and fixed localizers 12 or between the respective fixed localizers 12 on the inside of the external security surface 22 and on the outside of the internal security surfaces 21, the processing proceeds to step S46, and the control unit 41 of the control localizer 11 judges whether or not other guard processing has been executed.

[0222] In step S46, in cases where it is judged that other guard processing is not being performed, the processing returns to step S41, and the abovementioned processing is repeated.

[0223] In step S46, in cases where it is judged that other guard processing has been performed, the at-home guard processing is ended.

[0224] In cases where it is judged in step S43 that there are differences between the inter-localizer distance matrix that is produced and the inter-localizer distance matrix that is stored in memory for the control localizer 11 and fixed localizers 12 that are inside the external security surface 22 and outside the internal security surface 21, or in cases where it is judged in step S45 that a human being is present between the control localizer 11 and fixed localizers 12 or between the respective fixed localizers 12 that are inside the external security surface 22 and outside the internal security surface 21, an unauthorized intrusion has occurred; accordingly, the procedure proceeds to step S47.

[0225] In step S47, the control unit 41 causes the wireless communications unit 50 to notify a specified reporting destination of the occurrence of an abnormality. For example, the wireless communications unit 50 reports the occurrence of an abnormality by wireless transmission to the communications device of a specified outside party such as the mobile telephone of the homeowner, the telephone of a security firm or the like.

[0226] Furthermore, as a result of the processing of steps S48 through S50, authorized members such as the users 2-1 and 2-2 of the home 1 inside the internal security surface 21 are informed of the presence of an unauthorized intruder; furthermore, the unauthorized intruder 3 tends not to approach the internal security surface 21. In addition, if possible, the authorized members such as the users 2-1 and 2-2 of the home 1 are given evacuation guidance in a direction away from the position of the unauthorized intruder 3.

[0227] Specifically, in step S48, the control unit 41 of the control localizer 11 causes the white smoke generating module 49 or the white smoke generating modules 79 of the fixed localizers 12 to emit white smoke.

[0228] The white smoke generating module 49 or white smoke generating modules 79 generate white smoke that is harmless to the human body or to various types of equipment by heating a mixture of propylene glycol and water to a temperature of approximately 200°C. If localizers are thus prepared beforehand so that these localizers contain a white smoke generating module 49 or white smoke generating modules 79, white smoke can be generated when an unauthorized intruder 3 is detected.

[0229] For example, the control unit 41 of the control localizer 11 specifies the position (range) of the unauthorized intruder 3 in the three-dimensional coordinate system from elements in which differences are generated between the inter-localizer distance matrix that is produced and the inter-localizer distance matrix that is stored in memory, or from the spaces between the control localizer 11 and fixed localizers 12 or the spaces between respective fixed localizers 12 in which a human body is judged to be present. Furthermore, the control unit 41 of the control localizer 11 selects the control localizer 11 (itself) or a fixed localizer 12 that is close to the position of the unauthorized intruder 3 in the three-dimensional coordinate system.

[0230] In cases where the control unit 41 of the control localizer 11 selects the control localizer 11 itself, the white smoke generating module 49 is caused to emit white smoke.

[0231] In cases where the control unit 41 of the control localizer 11 selects a fixed localizer 12, the data communi-

cations unit is caused to transmit a command that causes the emission of white smoke to the selected fixed localizer 12 via the wireless transmitting and receiving unit 44. For example, this command that causes the emission of white smoke contains the localizer ID that is peculiar to the selected fixed localizer 12.

[0232] When such a command that causes the emission of white smoke is transmitted via wireless transmission, the control units 71 of the fixed localizers 12 cause the wireless transmitting and receiving units 74 to receive this command, and cause the data communications units 76 to extract the localizer ID contained in this command. The control units 71 of the fixed localizers 12 make a judgment as to whether or not the extracted localizer ID is the same as their own localizer ID. In cases where the control unit 71 of the fixed localizer 12 judges that the extracted localizer ID is the same as its own localizer ID, a command causing the mission of white smoke is transmitted to this fixed localizer 12 itself; accordingly, the white smoke generating module 79 is caused to generate white smoke.

[0233] In cases where the control units 71 of the fixed localizers 12 judge that the extracted localizer ID is not the same as their own localizer ID, these control units 71 do not emit white smoke.

[0234] In step S49, the control unit 41 of the control localizer 11 causes the speaker 48 or the speakers 78 of the fixed localizers 12 to generate a warning sound.

[0235] For example, the control unit 41 of the control localizer 11 specifies the position (range) of the unauthorized intruder 3 in the three-dimensional coordinate system from elements in which differences are generated between the inter-localizer distance matrix that is produced and the inter-localizer distance matrix that is stored in memory, or from the spaces between the control localizer 11 and fixed localizers 12 or spaces between the respective fixed localizers 12 in which it is judged that a human being is present. Then, the control unit 41 of the control localizer 11 selects a control localizer 11 (i. e., itself) or fixed localizer 12 that is close to the position of the unauthorized intruder 3 in the three-dimensional coordinate system.

[0236] In cases where the control unit 41 of the control localizer 11 selects the control localizer 11 (i. e., itself), the speaker 48 is caused to generate a warning sound.

[0237] In cases where the control unit 41 of the control localizer 11 selects a fixed localizer 12, the data communications unit is caused to transmit a command that generates a warning sound to the selected fixed localizer 12 via the wireless transmitting and receiving unit 44. For example, the command that generates a warning sound contains a localizer ID that is peculiar to the selected fixed localizers 12.

[0238] When a command that generates a warning sound is transmitted via wireless transmission, the control unit 71 of the fixed localizer 12 causes the wireless transmitting and receiving unit 74 to receive the command, and causes the data communications unit 76 to extract the localizer ID that is contained in the command. The control unit 71 of the fixed localizer 12 judges whether or not the extracted localizer ID is the same as its own localizer ID. In cases where the control unit 71 of the fixed localizer 12 judges that the extracted localizer ID is the same as its own localizer ID, since a command that generates a warning sound is transmitted to this fixed localizer 12 itself, the speaker 78 is caused to generate a warning sound.

[0239] In cases where the control unit 71 of the fixed localizer 12 judges that the extracted localizer ID is not the same as its own localizer ID, a warning sound is not generated.

[0240] Thus, in step S48 and step S49, a warning sound is generated and white smoke is generated from a fixed localizer 12 in the location where the unauthorized intruder is detected (i. e., a fixed localizer 12 whose coordinate position varies or a fixed localizer 12 that has detected a human body between itself and another fixed localizer 12).

[0241] As was described above, the control localizer 11 can transmit commands to respective fixed localizers 12 by wireless communications so that a warning sound is generated and white smoke is generated only from localizers that have detected a human body or localizers whose three-dimensional coordinate position has varied (and surrounding localizers). Consequently, a warning sound and white smoke are generated in various movement destinations within the home 1 in the vicinity of the intrusion of the unauthorized intruder 3. Here, in other words, actuators which have the effect of generating white smoke and actuators which have the effect of generating a warning sound are spatially dispersed, and a wireless communications network is formed, so that this system acts as an actuator network system in which actuators that are suitable for responding to abnormalities on the spot act in accordance with the locations in which such abnormalities occur.

[0242] Thus, fixed localizers 12 which are located outside the internal security surface 21 and within a specified distance from the position of the unauthorized intruder 3 generate a warning sound and generate white smoke.

[0243] In cases where the distance between the mobile localizer 13 and the unauthorized intruder equal to or less than a specified distance, the fixed localizer 12 that is closest to the unauthorized intruder 3 may contain another repelling function, and may activate this repelling function. Examples of such other repelling functions include the emission of a tear agent spray, an increase in the sound volume of the warning sound and the like. As a result, authorized members of the home 1 can be protected from unauthorized intruders 3 who have approached these authorized members of the home 1.

[0244] In step S50, the control unit 41 of the control localizer 11 causes the speaker 48 or the speakers 78 of the fixed localizers 12 to generate a sound that provides evacuation guidance.

[0245] Authorized members of the home 1 who are located inside the internal security surface 21 are notified of the presence of an unauthorized intruder 3 by this warning sound.

[0246] For example, the control localizer 11 measures the distance to the mobile localizer 13. Furthermore, the control localizer 11 transmits commands that cause the respective fixed localizers 12 to measure the distances from these fixed localizers 12 to the mobile localizer 13. The respective fixed localizers 12 measure the distances to the mobile localizer 13 and transmit the measurement results to the control localizer 11.

[0247] The control localizer 11 calculates the position of the mobile localizer 13 in the three-dimensional coordinate system on the basis of information indicating the distance to the mobile localizer 13 measured by the control localizer 11 itself, and information indicating the distances from the respective fixed localizers 12 to the mobile localizer 13 transmitted from the respective fixed localizers 12.

[0248] Then, the control unit 41 of the control localizer 11 selects the control localizer 11 (i. e., itself) or fixed localizer 12 in the position that is closest to the position of the mobile localizer 13 in the three-dimensional coordinate system.

[0249] In cases where the control unit 41 of the control localizer 11 selects the control localizer 11 (i. e., itself), the speaker 48 is caused to generate a sound that provides evacuation guidance.

[0250] In cases where the control unit 41 of the control localizer 11 selects a fixed localizer 12, the data communications unit is caused to transmit a command that generates a sound providing evacuation guidance to the selected fixed localizer 12 via the wireless transmitting and receiving unit 44. For example, the command that generates a warning sound contains a localizer ID that is peculiar to the selected fixed localizer 12.

When a command that generates a sound providing evacuation guidance is transmitted via wireless transmission, the control unit 71 of the fixed localizer 12 causes the wireless transmitting and receiving unit 74 to receive the command, and causes the data communications unit 76 to extract the localizer ID that is contained in the command. The control unit 71 of the fixed localizer 12 judges whether or not the extracted localizer ID is the same as its own localizer ID.

In cases where the control unit 71 of the fixed localizer 12 judges that the extracted localizer ID is the same as its own localizer ID, since a command that generates a sound providing evacuation guidance is transmitted to the fixed localizer 12 itself, the speaker 78 is caused to generate a sound providing evacuation guidance.

[0251] For example, a fixed localizer 12 which is located at a specified distance or less from the mobile localizer 13, and which is furthest from the unauthorized intruder 3 generates a sound (evacuation guidance sound) that differs from the warning sound. The authorized members of the home 1 can automatically move away from the unauthorized intruder 3 by moving toward this evacuation guidance sound.

[0252] Following the processing of step S50, the procedure returns to step S41. As a result, the position of the unauthorized intruder 3 in the three-dimensional coordinate system is repeatedly detected, and in cases where the unauthorized intruder 3 is present inside the external security surface 22, the processing of steps S47 through S50 is repeated on the basis of the position of the unauthorized intruder 3 in the three-dimensional coordinate system.

[0253] Next, the details of caretaker guard processing will be described.

[0254] Fig. 12 is a flow chart showing the details of caretaker guard processing, corresponding to the processing of step S10 in Fig. 7.

[0255] The processing of step S71 and the processing of step S72 are respectively similar to the processing of step S41 and the processing of step S42 in Fig. 12; accordingly, a description of these steps is omitted.

[0256] In step S73, a judgment is made as to whether or not there are differences between the inter-localizer distance matrix that is produced and the inter-localizer distance matrix that is stored in memory for the control localizer 11 and fixed localizers 12 inside the external security surface 22.

[0257] In non-guard processing, the inter-localizer distance matrix that is stored in memory is updated to values indicating the distances between the localizers at that point in time (the point in time at which non-guard processing is executed). Accordingly, in step S73, the differences between the last updated inter-localizer distance matrix and the current inter-localizer distance matrix are detected. These differences are calculated as the sum of the absolute values of the differences for each corresponding element in the range in which distance measurement is possible within the inter-localizer distance matrix that is stored in memory and the inter-localizer distance matrix at the current point in time.

[0258] The control unit 41 judges that there is an abnormality (i. e., "abnormality present") if the abovementioned sum exceeds a predetermined threshold value. If the fixed localizers 12 are mounted on the window 4, door 5 or safe 6 as shown in Fig. 1, then the distances between the localizers mounted on the window 4 and door 5 and other localizers will vary if the window 4 moves (is opened), or if the door 5 moves (is opened). The same is true if the safe 6 moves. As a result, the inter-localizer distance matrix varies.

[0259] In cases where it is judged in step S73 that there are no differences between the inter-localizer distance matrix that is produced and the inter-localizer distance matrix that is stored in memory for the control localizer 11 and fixed localizers 12 that are inside the external security surface 22, the processing proceeds to step S74, and the control localizer 11 and fixed localizers 12 analyze the waveform of the wireless signals communicating with the inside of the external security surface 22 by processing similar to the processing of step S44.

[0260] In step S75, the control unit 41 of the control localizer 11 judges whether or not a human body is present

between the control localizer 11 and fixed localizers 12 or between the respective fixed localizers 12 inside the external security surface 22 on the basis of the human body detection information that is transmitted from the respective fixed localizers 12, or the results of human body detection by the control localizer 11 itself.

[0261] In cases where it is judged in step S75 that no human being is present between the control localizer 11 and fixed localizers 12 or between the respective fixed localizers 12 on the inside of the external security surface 22, the processing proceeds to step S76, and the control unit 41 of the control localizer 11 judges whether or not other guard processing has been executed.

[0262] In cases where it is judged in step S76 that no other guard processing has been executed, the processing returns to step S71, and the abovementioned processing is repeated.

[0263] In cases where it is judged in step S76 that other guard processing has been executed, the at-home guard processing is ended.

[0264] In cases where it is judged in step S73 that there are differences between the inter-localizer distance matrix that is produced and the inter-localizer distance matrix that is stored in memory for the control localizer 11 and fixed localizers 12 inside the external security surface 22, or in cases where it is judged in step S75 that a human being is present between the control localizer 11 and fixed localizers 12 or between the respective fixed localizers 12 inside the external security surface 22, this means that there has been an unauthorized intrusion; accordingly, the procedure proceeds to step S77.

[0265] The processing of steps S77 through S79 is similar to the processing of steps S47 through S49 in Fig. 12; accordingly, a description of this processing will be omitted.

[0266] Following the processing of step S80, the procedure returns to step S71. As a result, the position of the unauthorized intruder 3 in the three-dimensional coordinate system is repeatedly detected, and in cases where an unauthorized intruder 3 is present inside the external security surface 22, the processing of steps S77 through S79 is repeated on the basis of the position of the unauthorized intruder 3 in the three-dimensional coordinate system.

[0267] Fig. 14 is a diagram which illustrates the emission of white smoke.

[0268] In the example shown in Fig. 14, the security system comprises a control localizer 11, fixed localizers 12-1 through 12-18, and a mobile localizer 13. The control localizer 11, fixed localizers 12-1 through 12-18 and mobile localizer 13 are disposed in various locations in the rooms 201-1 through 201-3 of a home 1, and on the outside of this home 1.

[0269] For example, the fixed localizer 12-4 is attached to a window 4-1. The fixed localizer 12-8 is attached to a window 4-2. The fixed localizer 12-16 is attached to a window 4-3.

[0270] The fixed localizer 12-6 is attached to a door 5-1. The fixed localizers 12-1 and 12-7 are attached to a door 5-2. The fixed localizer 12-11 is attached to a door 5-3. The fixed localizers 12-12 and 12-13 are attached to a door 5-4.

[0271] As is shown in Fig. 14, when the window 4-1 of the home 1 is opened, and an unauthorized intruder 3 makes an unauthorized intrusion into the room 201-1 of the home 1, white smoke is emitted from the fixed localizer 12-4 that is attached to the window 4-1, and from the nearby fixed localizers 12-3 and 12-7.

[0272] Specifically, when an unauthorized intruder 3 intrudes from the window 4-1 of the room 201-1, an unauthorized intruder 3 is considered to be present in the vicinity of the fixed localizer 12-4 whose position in the three-dimensional coordinate system moves as a result of the opening of the window 4-1, and the fixed localizer 12-4 attached to this window generates a warning sound and emits a stream of white smoke. White smoke is also emitted from the fixed localizers 12-3 and 12-7 located near the fixed localizer 12-4 that is attached to the window 4-1 of the room 201-1.

[0273] In at-home guard processing, the fixed localizers 12-15 and 12-16 which are positioned near the mobile localizers 13 and positioned in a direction away from the position of the unauthorized intruder 3 provide evacuation guidance to the authorized members (on which the mobile localizers 13 positioned inside the internal security surface 21 are mounted) in a direction away from the position of the unauthorized intruder 3 by outputting a sound.

[0274] Next, a case in which the present invention is applied to a car security system will be described with reference to Fig. 15.

[0275] A control localizer 11 is disposed in an arbitrary location in the interior of a vehicle 7 (other than the doors 301-1 through 301-4). One or more fixed localizers 12 are disposed on the insides of the respective doors 301-1 through 301-4.

[0276] For example, a fixed localizer 12-1 is disposed on the inside of the door 301-1, a fixed localizer 12-2 is disposed on the inside of the door 301-2, a fixed localizer 12-3 is disposed on the inside of the door 301-3, and a fixed localizer 12-4 is disposed on the inside of the door 301-4.

[0277] Authorized members using this vehicle 7 have mobile localizer 13.

[0278] The setting of a three-dimensional coordinate system, the setting of the positions of all of the fixed localizers in this three-dimensional coordinate system and the setting of an external security surface 22 are performed by processing similar to that described above.

[0279] Subsequently, the car security system executes processing of the execution mode. The processing of this execution mode is similar to the processing that was described with reference to Fig. 7. Since no internal security

surface 21 is set, at-home guard processing is not started (executed). Accordingly, in this car security system, only two types of guard processing, i. e., caretaker guard processing and non-guard processing, are executed. Such caretaker guard processing and non-guard processing are respectively similar to the processing that was described with reference to Fig. 13 and the processing that was described with reference to Fig. 11.

[0280] In the case of caretaker guard processing, if the fixed localizers 12 contain speakers 78 (used to generate a warning sound) as actuators, and also contain white smoke generating modules, then the fixed localizers 12 will emit a warning sound and will also emit a stream of white smoke throughout the interior of the vehicle when any of the doors 301-1 through 301-4 are opened.

[0281] As a result, even if there is an attempted unauthorized intrusion into the interior of the vehicle 7, the unauthorized intruder 3 cannot utilize his visual sense in the vehicle interior, so that criminal behavior is prevented.

[0282] Thus, in the present invention, automatic switching between guard processing and non-guard processing is possible, so that the problem of forgetting to switch [modes] can be prevented, thus making it possible to prevent erroneous operation of the security system.

[0283] Furthermore, unauthorized intruders can be repulsed by the operation of the actuators in response to the positions of the unauthorized intruders.

[0284] Moreover, unauthorized intruders can be prevented from approaching authorized members who are present with a [given] region, and authorized members located within this region can be given evacuation guidance while these members avoid such unauthorized intruders. Furthermore, security surfaces whose setting is required for the automatic switching between guard processing and non-guard processing can be simply set and registered using mobile localizers 13.

[0285] Thus, in cases where the system is devised so that the positions of authorized members using the object of security can be detected, the positions of unauthorized intrusions into the object of security can be detected, processing with respect to unauthorized intrusions can be executed with [the system] disposed in a plurality of locations within the object of security, the execution means that execute processing can be selected in accordance with the relationship between the detected positions of the authorized members and the detected positions of unauthorized intrusions, and the execution of processing by the selected execution means is controlled, specified processing with respect to unauthorized intrusions can be executed in accordance with conditions in the object of security without any need for a bothersome operation.

[0286] In cases where the system is devised so that the positions of authorized members using the object of security can be detected, the positions of unauthorized intrusions into the object of security can be detected, the position of an external security surface can be stored in memory, the position of an internal security surface can be stored in memory, the execution of first guard processing or second guard processing is controlled so that first guard processing is executed on the basis of the detected positions of the authorized members in cases where there are no authorized members inside the external security surface, and so that second guard processing is executed in cases where there are authorized members inside the internal security surface, and processing with respect to unauthorized intrusions is executed when the position of an unauthorized intrusion into the object of security is detected in cases where first guard processing or second guard processing is executed, specified processing with respect to unauthorized intrusions can be executed in accordance with conditions in the object of security without any need for a bothersome operation.

[0287] In cases where the system is devised so that information is transmitted and received, signals modulated by a specified code are transmitted and received, the distances to devices constituting partners in wireless transmission and reception are measured, signals modulated by a code are transmitted and received, data communications with the devices are performed, specified processing with respect to unauthorized intrusions is executed, and overall control is performed, unauthorized intrusions can be detected, and specified processing with respect to unauthorized intrusions can be executed.

[0288] In cases where the system is devised so that the distances to partners are measured, human bodies between the system itself and partners are detected by the waveform analysis of wireless transmission signals, and information indicating the measured distances to partners or information indicating the detection of human bodies is transmitted, unauthorized intrusions can be detected, and specified processing with respect to unauthorized intrusions can be executed.

[0289] In cases where the system is devised so that the distances from the system itself to respective terminal devices are measured, information indicating the distances between respective terminal devices that is transmitted from these respective terminal devices is received, and a judgment is made as to whether or not there has been an unauthorized intrusion into object of security on the basis of the distances from the system itself to respective terminal devices or the distances between respective terminal devices, unauthorized intrusions can be detected, and specified processing with respect to unauthorized intrusions can be executed.

[0290] In cases where a vehicle security system is constructed from fixed terminal devices which are disposed on the inside surfaces of the respective doors of a vehicle, and which measure the distances from these terminal devices to other terminal devices and a control terminal device, a mobile terminal device held by a person have the proper

authorization to enter and exit this vehicle, and a control terminal device which is disposed inside the vehicle, and this system is devised so that variations in the distances between fixed terminal devices and a control terminal device and the distances between respective terminal devices disposed inside the vehicle are monitored in cases where the position of the mobile terminal device is outside an external security surface set by fixed terminal devices and a control terminal device disposed inside the vehicle, it is judged that an abnormality has occurred in cases where the variation in distances satisfies specified conditions, and specified processing with respect to unauthorized intrusions is executed in cases where it is judged that an abnormality has occurred, unauthorized intrusions can be detected, and specified processing with respect to unauthorized intrusions can be executed.

[0291] In cases where the system is devised so that fixed nodes sense the surrounding environment, wireless communications are performed, an action is applied to the outside, information relating to the sensed surrounding conditions is transmitted to a control node, a control action is performed so that actuators are operated in response to commands from the control node, the control node performs wireless communications, the fixed node that is to operate the actuator is selected on the basis of information relating to the surrounding environment that is received from the fixed nodes, and commands that are used to operate the actuator are transmitted to the selected fixed node, unauthorized intrusions can be detected, and specified processing with respect to unauthorized intrusions can be executed.

[0292] In cases where the system is devised so that the position of a first terminal device is taken as the origin of a three-dimensional coordinate system, the distance between a first terminal device and a second terminal device, the distance between a first terminal device and a third terminal device and the distance between a second terminal device and a third terminal device are respectively measured, the first axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to first measurement results that indicate the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device, the second axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to the first measurement results, the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device are respectively measured, and the third axis of the three-dimensional coordinate system is specified from second measurement results indicating the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device, the first axis and the second axis.

INDUSTRIAL APPLICABILITY

[0293] The first invention makes it possible to detect unauthorized intrusions. Furthermore, by using the first invention, it is possible to execute specified processing with respect to unauthorized intrusions in accordance with conditions in the object of security without any need for a bothersome operation.

[0294] The second invention makes it possible to detect unauthorized intrusions. Furthermore, by using the second invention, it is possible to execute specified processing with respect to unauthorized intrusions in accordance with conditions in the object of security without any need for a bothersome operation.

[0295] The third invention makes it possible to detect unauthorized intrusions. By using the third invention, it is possible to detect unauthorized intrusions and to execute specified processing with respect to unauthorized intrusions.

[0296] The fourth invention makes it possible to detect unauthorized intrusions. By using the fourth invention, it is possible to detect unauthorized intrusions and to execute specified processing with respect to unauthorized intrusions.

[0297] The fifth invention makes it possible to detect unauthorized intrusions. By using the fifth invention, it is possible to detect unauthorized intrusions and to execute specified processing with respect to unauthorized intrusions.

[0298] The sixth invention makes it possible to detect unauthorized intrusions. By using the sixth invention, it is possible to detect unauthorized intrusions and to execute specified processing with respect to unauthorized intrusions.

[0299] The seventh invention makes it possible to detect unauthorized intrusions. By using the seventh invention, it is possible to detect unauthorized intrusions and to execute specified processing with respect to unauthorized intrusions.

[0300] The eighth invention makes it possible to execute area setting for the setting and release of guard modes in a simple manner.

Claims

1. A security system which executes specified processing with respect to an unauthorized intrusion into an object of security in cases where such an unauthorized intrusion is detected, comprising:

member position detection means which detect the positions of authorized members using said object of security;
unauthorized intrusion position detection means which detect the position of said unauthorized intrusion into said object of security;
execution means which are disposed in a plurality of locations inside said object of security, and which execute said processing with respect to said unauthorized intrusion; and
execution control means which select said execution means that execute said processing in accordance with the relationship of the positions of said authorized members detected by said member position detection means and the position of said unauthorized intrusion detected by said unauthorized intrusion position detection means, and which control the execution of said processing by said selected execution means.

2. The security system according to claim 1, **characterized in that** said execution control means select one or more execution means including said execution means closest to the position of said unauthorized intrusion in cases where the distance between the position of said unauthorized intrusion and the positions of said authorized members is equal to or less than a specified threshold value, and control the execution of said processing so as to cause the selected execution means to execute said processing with respect to said unauthorized intrusion.

3. The security system according to claim 1, **characterized in that** said execution control means control the execution of said processing so that said processing for guiding the evacuation of said authorized members is executed by said execution means whose distance from the position of said authorized members is equal to or less than a specified threshold value, and whose distance from the position of said unauthorized intrusion is maximal.

4. The security system according to claim 1, **characterized in that** said execution means execute said processing that generates white smoke.

5. The security system according to claim 1, **characterized in that** said member position detection detect the positions of said authorized members by detecting the positions of devices which are mounted on said authorized members, and which transmit by wireless transmission an ID code that corresponds to the object of security.

6. The security system according to claim 1, **characterized in that** said member position detection means detect the positions of said authorized members by detecting the positions of devices which are mounted on said authorized members, which transmit by wireless transmission an ID code that corresponds to the object of security, and on which said execution means are disposed.

7. A security system which executes specified processing with respect to an unauthorized intrusion into an object of security in cases where such an unauthorized intrusion is detected, comprising:

member position detection means which detect the positions of authorized members using said object of security;
unauthorized intrusion position detection means which detect the position of said unauthorized intrusion into said object of security;
external security surface memory means which store the position of an external security surface;
internal security surface memory means which store the position of an internal security surface;
execution control means which control the execution of first guard processing or second guard processing on the basis of the positions of said authorized members detected by said member position detection means so that said first guard processing is executed in cases where there are no authorized members inside said external security surface, and so that said second guard processing is executed in cases where said authorized members are present inside said internal security surface; and
execution means which are disposed in a plurality of locations inside said object of security, and which execute said processing with respect to said unauthorized intrusion when the position of said unauthorized intrusion into said object of security is detected by said unauthorized intrusion position detection means in cases where said first guard processing or said second guard processing is executed.

8. The security system according to claim 7, **characterized in that** said first guard processing is caretaker guard processing which is guard processing for said unauthorized intrusion into the inside of said external security surface, and said second guard processing is at-home guard processing which is guard processing for said unauthorized intrusion between said external security surface and said internal security surface.

9. The security system according to claim 7, **characterized in that** said execution means execute said processing that generates white smoke.

10. The security system according to claim 7, **characterized in that** said member position detection means detect the positions of said authorized members by detecting the positions of devices which are mounted on said authorized members, and which transmit by wireless transmission an ID code that corresponds to the object of security.

11. The security system according to claim 7, **characterized in that** said member position detection means detect the positions of said authorized members by detecting the positions of devices which are mounted on said authorized members, which transmit by wireless transmission an ID code that corresponds to the object of security, and on which said execution means are disposed.

12. The security system according to claim 11, **characterized in that** said execution means disposed on said devices execute said processing that generates white smoke.

13. A terminal device comprising:

an antenna unit;
a wireless transmitting and receiving unit which transmits and receives information via said antenna unit;
a distance measuring unit which transmits and receives signals modulated by a specified code via said antenna unit and said wireless transmitting and receiving unit, and which measures the distances to devices constituting partners in this wireless transmission and reception;
a data communications unit which transmits and receives signals modulated by said code via said antenna unit and said wireless transmitting and receiving unit, and which performs data communications with said devices;
an actuator which executes specified processing with respect to unauthorized intrusions; and
a control unit which performs overall control.

14. The terminal device according to claim 13, **characterized in that** said actuator executes said processing that generates white smoke.

15. The terminal device according to claim 13, **characterized in that** this device further comprises human body detection means which detect a human body between this terminal device itself and other terminal devices by the waveform analysis of wireless signals between this terminal device itself and the other terminal devices, and said actuator executes said processing for said unauthorized intrusion in cases where said human body detection means detects said human body.

16. A terminal device comprising:

distance measuring means which measure the distance between the terminal device itself and partners;
human body detection means which detect a human body between the terminal device itself and partners by the waveform analysis of wireless transmission signals; and
transmitting means which transmit information indicating the measured distance between the terminal device itself and said partners or information indicating the detection of said human body.

17. An information processing method for a terminal device comprising:

a distance measurement step in which the distance between said terminal device and a partner is measured;
a human body detection step in which a human body between said terminal device and a partner is detected by the waveform analysis of a wireless transmission signal; and
a transmission control step in which the transmission of information indicating the measured distance between said terminal device and said partner or information indicating the detection of said human body is controlled.

18. A program which is used to cause the computer of a terminal device to perform information processing, comprising:

a distance measurement step in which the distance between said terminal device and a partner is measured;
a human body detection step in which a human body between said terminal device and the partner is detected by the waveform analysis of a wireless transmission signal; and

a transmission control step in which the transmission of information indicating the measured distance between said terminal device and said partner or information indicating the detection of said human body is controlled.

19. An information processing device which processes information that is transmitted from a plurality of terminal devices, comprising:

distance measuring means which measure the distances from said information processing device itself to said respective terminal devices;
receiving means which receive information indicating the distances between said respective terminal devices that is transmitted from each of said terminal devices; and
judgment means which judge whether or not there has been an unauthorized intrusion into the object of security on the basis of the distances from said information processing device itself to said respective terminal devices or the distances between said respective terminal devices.

20. The information processing device according to claim 19, further comprising human body detection means which detect a human body between the information processing device itself and said respective terminal devices by the waveform analysis of a wireless transmission signal, **characterized in that** said judgment means judge whether or not there has been an unauthorized intrusion into said object of security on the basis of the detection of said human body.

21. The information processing device according to claim 19, **characterized in that** the receiving means further receive information indicating the detection of a human body that is transmitted from each of said terminal devices, and said judgment means judge whether or not there has been an unauthorized intrusion into said object of security on the basis of said information indicating the detection of said human body.

22. An information processing method which processes information that is transmitted from a plurality of terminal devices, comprising:

a distance measurement step in which the distances from the device itself to said respective terminal devices are measured;
a reception control step in which the reception of information indicating the distances between said respective terminal devices that is transmitted from each of said terminal devices is controlled; and
a judgment step in which it is judged whether or not there has been an unauthorized intrusion into the object of security on the basis of the distances from the device itself to said respective terminal devices or the distances between said respective terminal devices.

23. A program which causes a computer to perform information processing that processes information transmitted from a plurality of terminal devices, comprising:

a distance measurement step in which the distances from the device itself to said respective terminal devices are measured;
a reception control step in which the reception of information indicating the distances between said respective terminal devices that is transmitted from each of said terminal devices is controlled; and
a judgment step in which it is judged whether or not there has been an unauthorized intrusion into the object of security on the basis of the distances from the device itself to said respective terminal devices or the distances between said respective terminal devices.

24. A vehicle security system comprising:

fixed terminal devices which are disposed on the inside surfaces of the respective doors of the vehicle, and which measure the distances to other fixed terminal devices and a control terminal device;
a mobile terminal device which is held by a person having authorization to enter and exit said vehicle; and
a control terminal device which is disposed inside said vehicle;

characterized in that the variation in the distances between said fixed terminal devices and said control terminal device disposed inside said vehicle and the distances between said respective fixed terminal devices is monitored when the position of said mobile terminal device is outside an external security surface 22 that is set by said fixed terminal devices and said control terminal device disposed inside said vehicle, and it is judged that

an abnormality has occurred in cases where the variation in distance satisfies specified conditions; and specified processing for an unauthorized intrusion is executed in cases where it is judged that an abnormality has occurred.

25. The vehicle security system according to claim 24, **characterized in that** said processing for an unauthorized intrusion is processing that generates white smoke.

26. A network system comprising a plurality of fixed nodes and a control node, **characterized in that** said fixed nodes [each] comprise sensing means which sense the surrounding environment, first wireless communications means, an actuator which applies an action to the outside, and control means which cause said first wireless communications means to transmit information relating to said surrounding environment sensed by said sensing means to said control node, and which perform a control action so that said actuator is operated in response to commands from said control node, said control node comprises second wireless communications means, and selection means which select said fixed node that are to operate said actuator on the basis of said information relating to the surrounding environment that is received from said fixed nodes, and said second wireless communications means transmit said commands that operate said actuator to said selected fixed node.

27. The network system according to claim 26, **characterized in that** said second wireless communications means receive information relating to said surrounding environment which is information relating to the distances between said fixed nodes that is transmitted from said fixed nodes.

28. A three-dimensional coordinate system setting method using a first terminal device, second terminal device, third terminal device and fourth terminal device which are terminal devices comprising an antenna unit, a wireless transmitting and receiving unit that transmits and receives information via the antenna unit, a distance measuring unit that measures the distance to the device constituting the wireless transmitting and receiving partner by transmitting and receiving signals modulated by a specified code via the antenna unit and wireless transmitting and receiving unit, a data communications unit which performs data communications with the devices by transmitting and receiving signals modulated by a code via the antenna unit and wireless transmitting and receiving unit, an actuator which executes specified processing with respect to unauthorized intrusions, and a control unit which performs overall control, this setting method being **characterized in that** the position of the first terminal device is taken as the origin of the three-dimensional coordinate system, the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device are respectively measured, the first axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to first measurement results indicating the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device, the second axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to these first measurement results, the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device are respectively measured, and the third axis of the three-dimensional coordinate system is specified from second measurement results indicating the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device, the first axis and the second axis.

29. The security surface setting method in said three-dimensional coordinate system set by the setting method according to claim 28, **characterized in that** the position of a fifth terminal device which is one of said terminal devices in said three-dimensional coordinate system is detected, the smallest rectangular solid in said three-dimensional coordinate system that includes a plurality of said detected positions is determined, and said security surface is set on the basis of the surfaces of said determined rectangular solid.

Amended claims under Art. 19.1 PCT

the positions of devices which are mounted on said authorized members, and which transmit by wireless transmission an ID code that corresponds to the object of security.

11. The security system according to claim 7, **characterized in that** said member position detection means detect the positions of said authorized members by detecting the positions of devices which are mounted on said author-

ized members, which transmit by wireless transmission an ID code that corresponds to the object of security, and on which said execution means are disposed.

12. The security system according to claim 11, **characterized in that** said execution means disposed on said devices execute said processing that generates white smoke.

13. (Amended) A terminal device comprising:

an antenna unit;
a wireless transmitting and receiving unit which transmits and receives information via said antenna unit;
a distance measuring unit which transmits and receives signals modulated by a specified code via said antenna unit and said wireless transmitting and receiving unit, and which measures the distances to other terminal devices constituting partners in this wireless transmission and reception;
a data communications unit which transmits and receives signals modulated by said code via said antenna unit and said wireless transmitting and receiving unit, and which performs data communications with said other terminal devices;
an actuator which executes specified processing with respect to unauthorized intrusions; and
a control unit which performs overall control, and which controls said actuator on the basis of signals from said other terminal devices so that said processing is executed,
and controls said data communications unit so that commands that cause the execution of said processing are transmitted to said other terminal devices.

14. The terminal device according to claim 13, **characterized in that** said actuator executes said processing that generates white smoke.

15. (Amended) The terminal device according to claim 13, **characterized in that** this device further comprises human body detection means which detect a human body between this terminal device itself and said other terminal devices by the waveform analysis of wireless signals between this terminal device itself and said other terminal devices, and said actuator executes said processing for said unauthorized intrusion in cases where said human body detection means detects said human body.

16. (Amended) A terminal device comprising:

distance measuring means which measure the distances between this terminal device itself and other terminal devices;
human body detection means which detect a human body between this terminal device itself and said other terminal devices by waveform analysis of a wireless transmission signal;
communications means which receive information indicating the distances between this terminal device itself and said other terminal devices or information indicating the detection of said human body that is transmitted from said other terminal devices; and
control means which control said communications means on the basis of the results of the measurement of the distances between this terminal device itself and said other terminal devices or the results of the detection of said human body, or on the basis of received information indicating the distances between this terminal device itself and said other terminal devices or information indicating the detection of said human body, so that commands that cause the execution of specified processing are transmitted to said other terminal devices.

17. (Amended) An information processing method for a terminal device comprising:

a distance measurement step in which the distances between said terminal device and other terminal devices are measured;
a human body detection step in which a human body between said terminal device and said other terminal devices is detected by the waveform analysis of a wireless transmission signal;
a communications control step in which the reception of information indicating the distances between said terminal device itself and said other terminal devices or information indicating the detection of said human body that is transmitted from said other terminal devices is controlled; and
a control step in which commands that cause the execution of specified processing are transmitted to said other terminal devices in said communications control step on the basis of the results of the measurement of the distances between this terminal device itself and said other terminal devices or the results of the detection of said human body, or on the basis of received information indicating the distances between this terminal device itself and said other terminal devices or information indicating the detection of said human body.

18. (Amended) A program which causes the computer of a terminal device to perform information processing,

comprising:

a distance measurement step in which the distances between said terminal device and other terminal devices are measured;
a human body detection step in which a human body between said terminal device and said other terminal devices is detected by the waveform analysis of a wireless transmission signal;
a communications control step in which the reception of information indicating the distances between said terminal device itself and said other terminal devices or information indicating the detection of said human body that is transmitted from said other terminal devices is controlled; and
a control step in which commands that cause the execution of specified processing are transmitted to said other terminal devices in said communications control step on the basis of the results of the measurement of the distances between this terminal device itself and said other terminal devices or the results of the detection of said human body, or on the basis of received information indicating the distances between this terminal device itself and said other terminal devices or information indicating the detection of said human body.

19. An information processing device which processes information that is transmitted from a plurality of terminal devices, comprising:

distance measuring means which measure the distances from said information processing device itself to said respective terminal devices;
receiving means which receive information indicating the distances between said respective terminal devices that is transmitted from each of said terminal devices; and
judgment means which judge whether or not there has been an unauthorized intrusion into the object of security on the basis of the distances from said information processing device itself to said respective terminal devices or the distances between said respective terminal devices.

20. The information processing device according to claim 19, further comprising human body detection means which detect a human body between the information processing device itself and said respective terminal devices by the waveform analysis of a wireless transmission signal, **characterized in that** said judgment means judge whether or not there has been an unauthorized intrusion into said object of security on the basis of the detection of said human body.

21. The information processing device according to claim 19, **characterized in that** the receiving means further receive information indicating the detection of a human body that is transmitted from each of said terminal devices, and said judgment means judge whether or not there has been an unauthorized intrusion into said object of security on the basis of said information indicating the detection of said human body.

22. An information processing method which processes information that is transmitted from a plurality of terminal devices, comprising:

a distance measurement step in which the distances from the device itself to said respective terminal devices are measured;
a reception control step in which the reception of information indicating the distances between said respective terminal devices that is transmitted from each of said terminal devices is controlled; and
a judgment step in which it is judged whether or not there has been an unauthorized intrusion into the object of security on the basis of the distances from the device itself to said respective terminal devices or the distances between said respective terminal devices.

23. A program which causes a computer to perform information processing that processes information transmitted from a plurality of terminal devices, comprising:

a distance measurement step in which the distances from the device itself to said respective terminal devices are measured;
a reception control step in which the reception of information indicating the distances between said respective terminal devices that is transmitted from each of said terminal devices is controlled; and
a judgment step in which it is judged whether or not there has been an unauthorized intrusion into the object of security on the basis of the distances from the device itself to said respective terminal devices or the distances between said respective terminal devices.

24. (Amended) A vehicle security system comprising:

fixed terminal devices which are disposed on the inside surfaces of the respective doors of the vehicle, and which measure the distances to other fixed terminal devices and a control terminal device;
a mobile terminal device which is held by a person having authorization to enter and exit said vehicle; and
a control terminal device which is disposed inside said vehicle;

characterized in that a judgment is made as to whether or not there has been an unauthorized intrusion into said vehicle on the basis of the distances between said fixed terminal devices and said control terminal device disposed inside said vehicle or the distances between said respective fixed terminal devices in cases where the position of said mobile terminal device is outside the external security surface set by said fixed terminal devices and said control terminal device disposed inside said vehicle, and specified processing for unauthorized intrusions is executed in cases where it is judged that there has been an unauthorized intrusion.

25. The vehicle security system according to claim 24, **characterized in that** said processing for an unauthorized intrusion is processing that generates white smoke.

26. (Amended) A network system comprising a plurality of fixed nodes and one control node, **characterized in that** said fixed nodes [each] comprise sensing means which sense the surrounding environment, first wireless communications means, an actuator which applies an action to the outside, and control means which cause said first wireless communications means to transmit information relating to said surrounding environment sensed by said sensing means to said control node, and which perform a control action so that said actuator is operated in response to commands from said control node, said control node comprises second wireless communications means, and selection means which select one or a plurality of fixed nodes that are to operate said actuator from said plurality of fixed nodes on the basis of said information relating to the surrounding environment that is received from each of said plurality of fixed nodes, and said second wireless communications means transmit said commands that operate said actuator to said one or the plurality of fixed nodes that are selected.

27. The network system according to claim 26, **characterized in that** said second wireless communications means receive information relating to said surrounding environment which is information relating to the distances between said fixed nodes that is transmitted from said fixed nodes.

28. (Amended) The network system according to claim 26, **characterized in that** said information relating to the surrounding environment indicates the presence or absence of any unauthorized intrusion, and the action that is applied to the outside by said actuator is an action that generates white smoke.

29. (Amended) A three-dimensional coordinate system setting method using a first terminal device, second terminal device, third terminal device and fourth terminal device which are terminal devices comprising an antenna unit, a wireless transmitting and receiving unit that transmits and receives information via the antenna unit, a distance measuring unit that measures the distance to the device constituting the wireless transmitting and receiving partner by transmitting and receiving signals modulated by a specified code via the antenna unit and wireless transmitting and receiving unit, a data communications unit which performs data communications with the devices by transmitting and receiving signals modulated by a code via the antenna unit and wireless transmitting and receiving unit, an actuator which executes specified processing with respect to unauthorized intrusions, and a control unit which performs overall control, this setting method being **characterized in that** the position of said first terminal device is taken as the origin of the three-dimensional coordinate system, the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device are respectively measured, the first axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to first measurement results indicating the distance between the first terminal device and second terminal device, the distance between the first terminal device and third terminal device and the distance between the second terminal device and third terminal device, the second axis of the three-dimensional coordinate system is specified by applying a specified mathematical operation to these first measurement results, the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device are respectively measured, and the third axis of the three-dimensional coordinate system is specified from second measurement results indicating the distance between the first terminal device and fourth terminal device, the distance between the second terminal device and fourth terminal device and the distance between the third terminal device and fourth terminal device, the first axis and the second axis.

30. (Added) The security surface setting method in said three-dimensional coordinate system set by the setting method according to claim 29, **characterized in that** the position of a fifth terminal device which is one of said terminal devices in said three-dimensional coordinate system is detected, the smallest rectangular solid in said three-dimensional coordinate system that includes a plurality of said detected positions is determined, and said security surface is set on the basis of the surfaces of said determined rectangular solid.

31. (Added) A terminal device comprising:

an antenna unit;
a wireless transmitting and receiving unit which transmits and receives information via said antenna unit;
a distance measuring unit which transmits and receives signals modulated by a specified code via said antenna unit and said wireless transmitting and receiving unit, and which measures the distances to other terminal devices constituting partners in this wireless transmission and reception;
a data communications unit which transmits and receives signals modulated by said code via said antenna unit and said wireless transmitting and receiving unit, and which performs data communications with said other terminal devices;
an actuator which executes specified processing with respect to unauthorized intrusions; and
a control unit which performs overall control, and which controls said actuator on the basis of signals from said other terminal devices so that said processing is executed.

32. (Added) The terminal device according to claim 31, **characterized in that** said actuator executes said processing that generates white smoke.

33. (Added) The terminal device according to claim 31, further comprising human body detection means which detect a human body between this terminal device itself and the other terminal devices by the waveform analysis of a wireless signal between this terminal device itself and said other terminal devices, **characterized in that** said actuator executes said processing with respect to said unauthorized intrusions in cases where said human body detection means detects said human body.

34. (Added) A terminal device comprising:

distance measuring means which measure the distances between this terminal device itself and other terminal devices
human body detection means which detect a human body between this terminal device itself and said other terminal devices by the waveform analysis of a wireless transmission signal;
communications means which transmit information indicating the measured distances between this terminal device itself and said other terminal devices, or information indicating the detection of said human body, and which receive commands that cause the execution of specified processing for unauthorized intrusions;
an actuator which executes said processing for unauthorized intrusions; and
control means which control said actuator on the basis of said received commands so that said processing is executed.

35. (Added) An information processing method for a terminal device comprising an actuator which executes specified processing for unauthorized intrusions, comprising:

a distance measurement step in which the distance between said terminal device and a partner is measured;
a human body detection step in which a human body between said terminal device and the partner is detected by the waveform analysis of a wireless transmission signal;
a communications control step in which the transmission of information indicating the measured distance between said terminal device and said partner or information indicating the detection of said human body is controlled, and the reception of commands that cause the execution of said processing for unauthorized intrusions is controlled; and
a control step in which said actuator is controlled on the basis of said received commands so that said processing is executed.

36. (Added) A program which causes the computer of a terminal device comprising an actuator that executes specified processing for unauthorized intrusions to perform information processing, comprising:

a distance measurement step in which the distance between said terminal device and a partner is measured;
a human body detection step in which a human body between said terminal device and the partner is detected by the waveform analysis of a wireless transmission signal;
a communications control step in which the transmission of information indicating the measured distance between said terminal device and said partner or information indicating the detection of said human body is controlled, and the reception of commands that cause the execution of said processing for unauthorized intrusions is controlled; and
a control step in which said actuator is controlled on the basis of said received commands so that said processing is executed.

FIG. 1

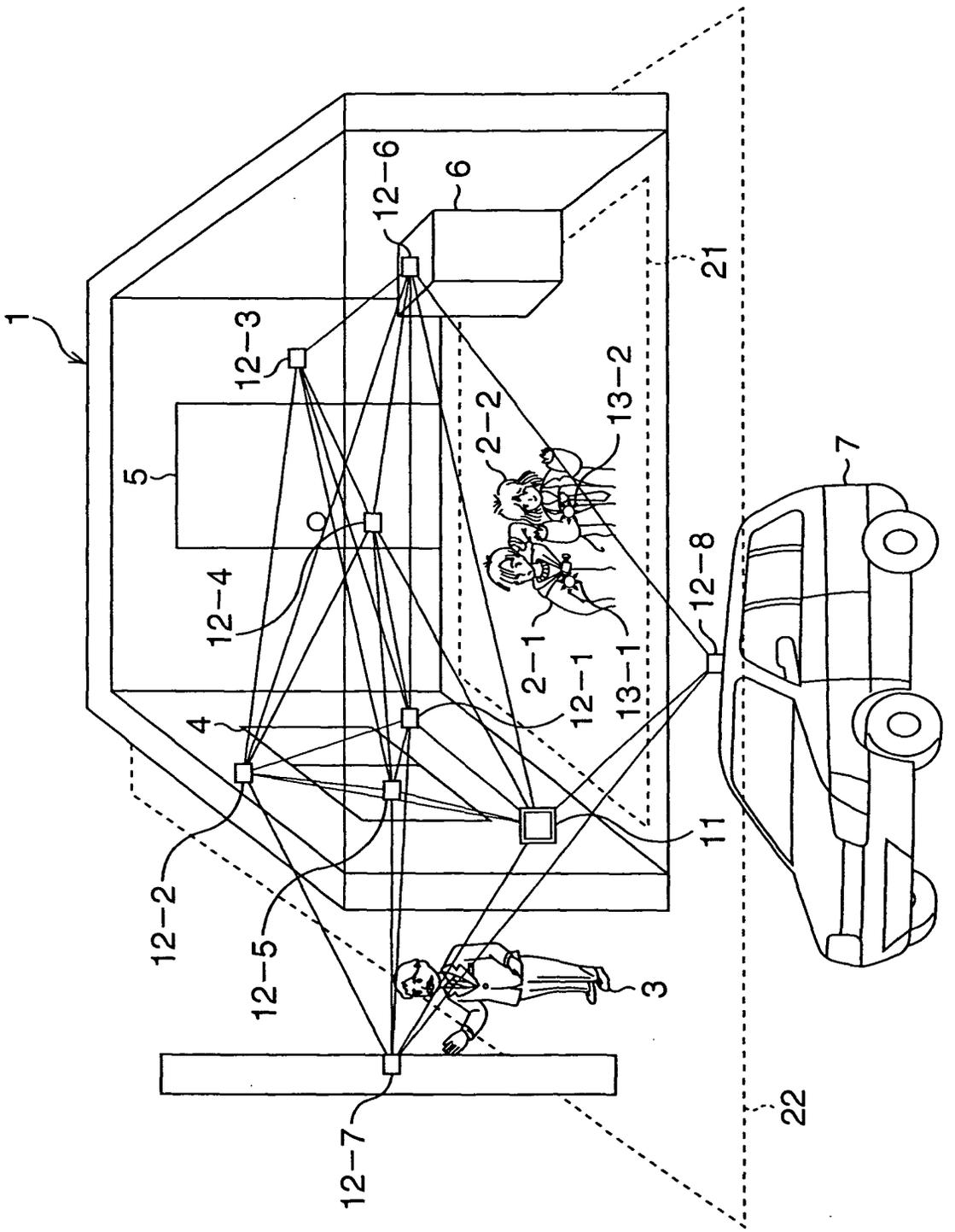


FIG. 2

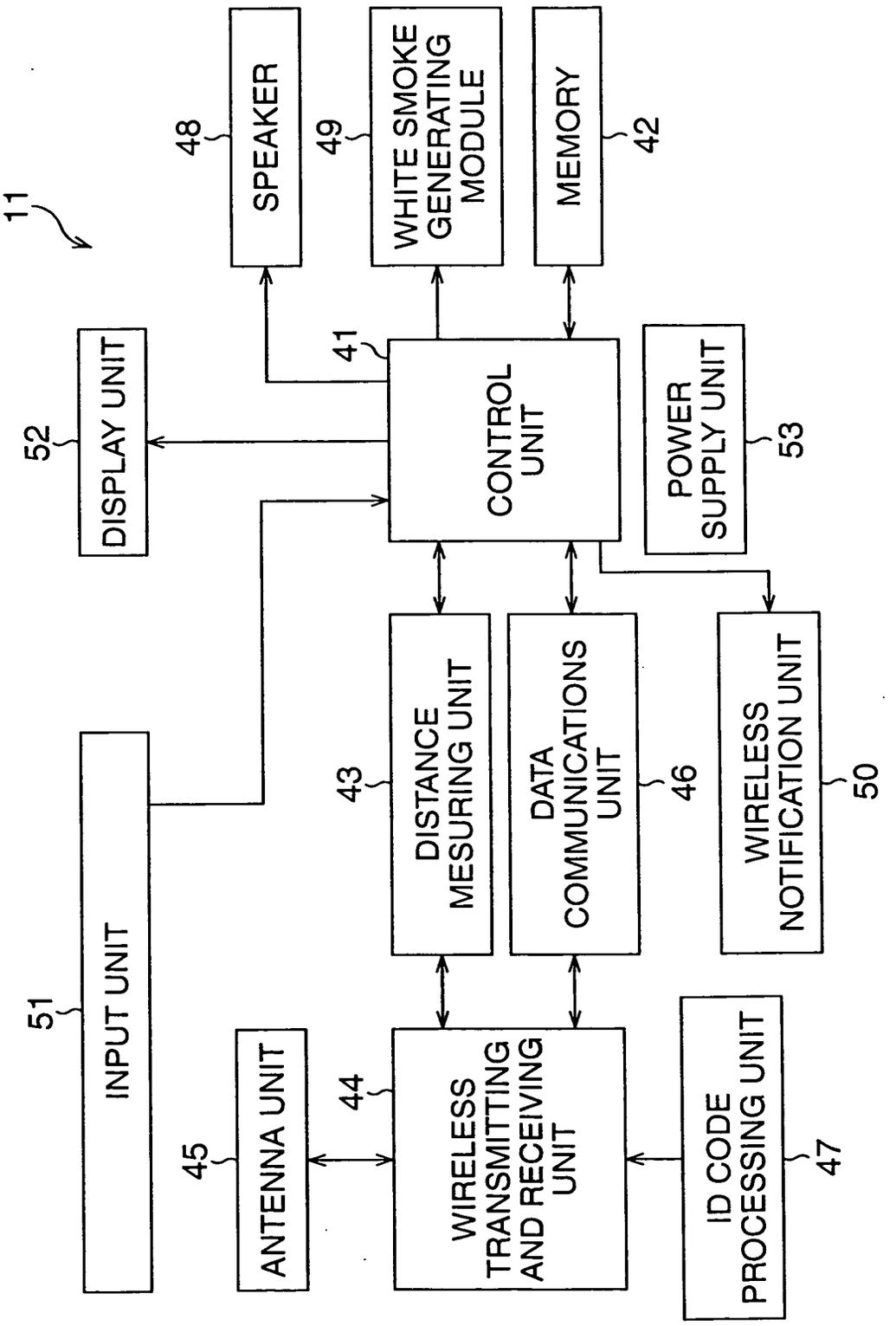

11
48
SPEAKER
49
WHITE SMOKE GENERATING MODULE
42
MEMORY
41
CONTROL UNIT
52
DISPLAY UNIT
53
POWER SUPPLY UNIT
43
DISTANCE MESURING UNIT
46
DATA COMMUNICATIONS UNIT
50
WIRELESS NOTIFICATION UNIT
51
INPUT UNIT
45
ANTENNA UNIT
44
WIRELESS TRANSMITTING AND RECEIVING UNIT
47
ID CODE PROCESSING UNIT

FIG. 3

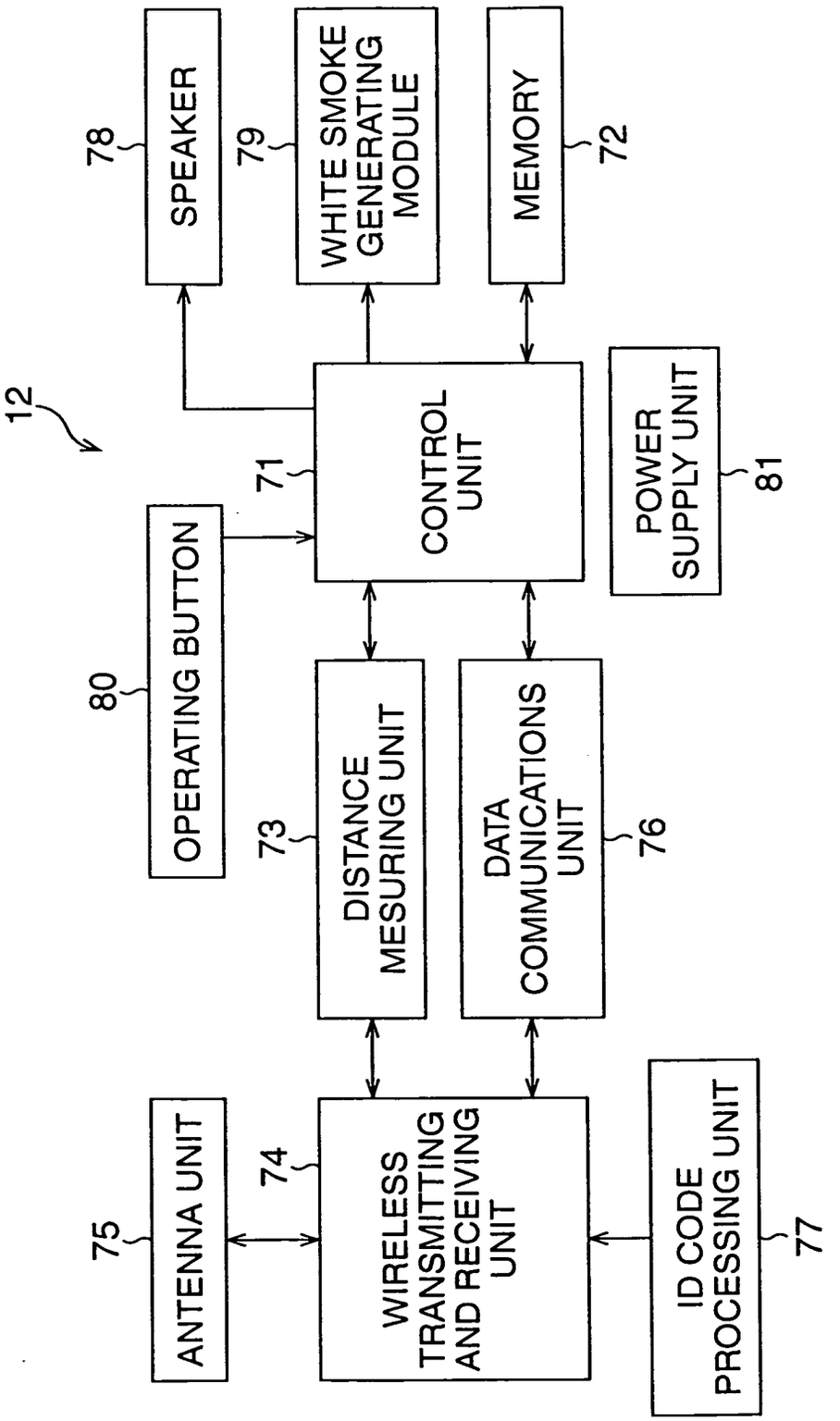

12
78
SPEAKER
79
WHITE SMOKE GENERATING MODULE
72
MEMORY
71
CONTROL UNIT
81
POWER SUPPLY UNIT
80
OPERATING BUTTON
73
DISTANCE MESURING UNIT
76
DATA COMMUNICATIONS UNIT
75
ANTENNA UNIT
74
WIRELESS TRANSMITTING AND RECEIVING UNIT
77
ID CODE PROCESSING UNIT

FIG. 4

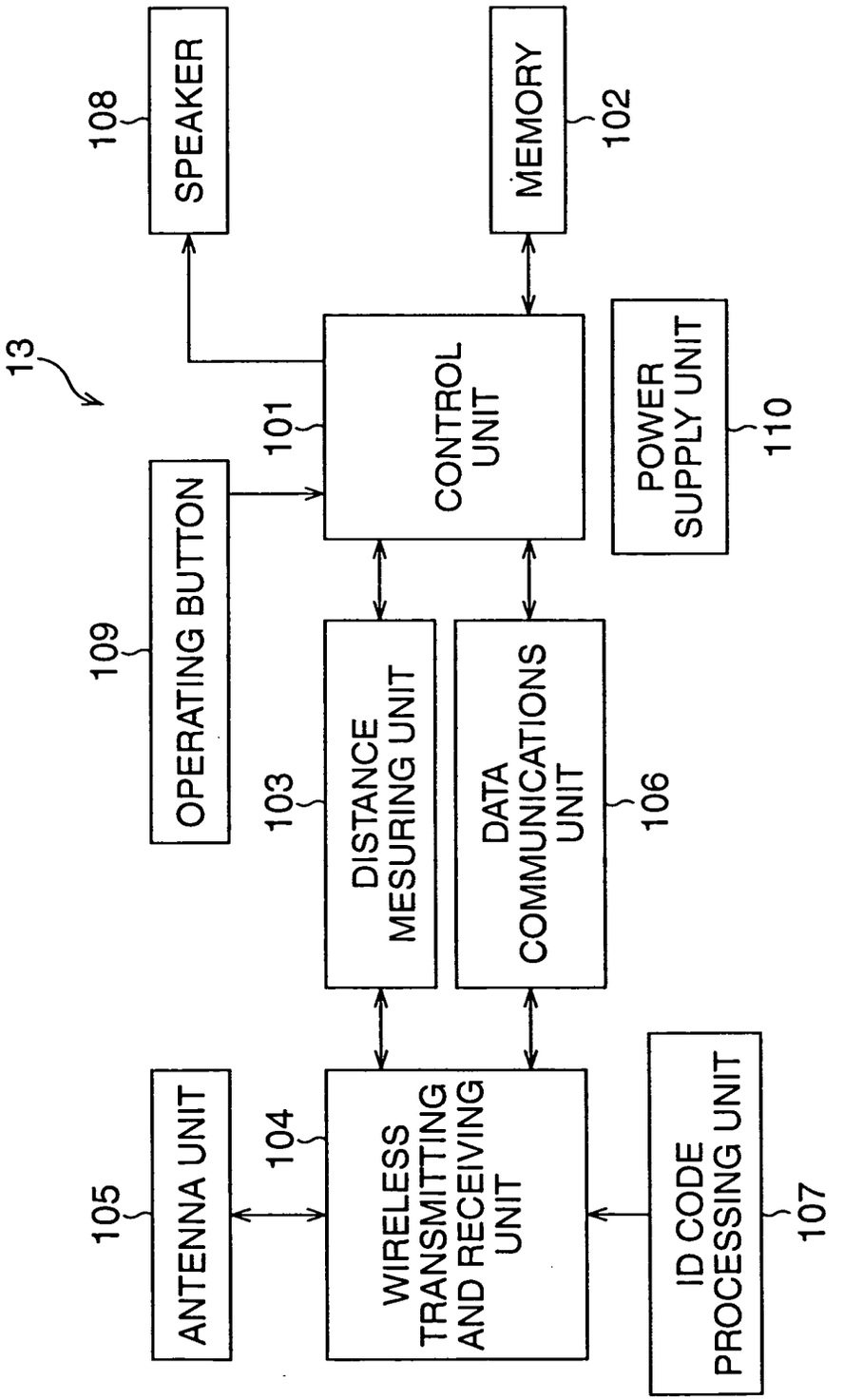

13
108
SPEAKER
MEMORY
102
CONTROL UNIT
101
POWER SUPPLY UNIT
110
OPERATING BUTTON
109
DISTANCE MESURING UNIT
103
DATA COMMUNICATIONS UNIT
106
ANTENNA UNIT
105
104
WIRELESS TRANSMITTING AND RECEIVING UNIT
ID CODE PROCESSING UNIT
107

FIG. 5

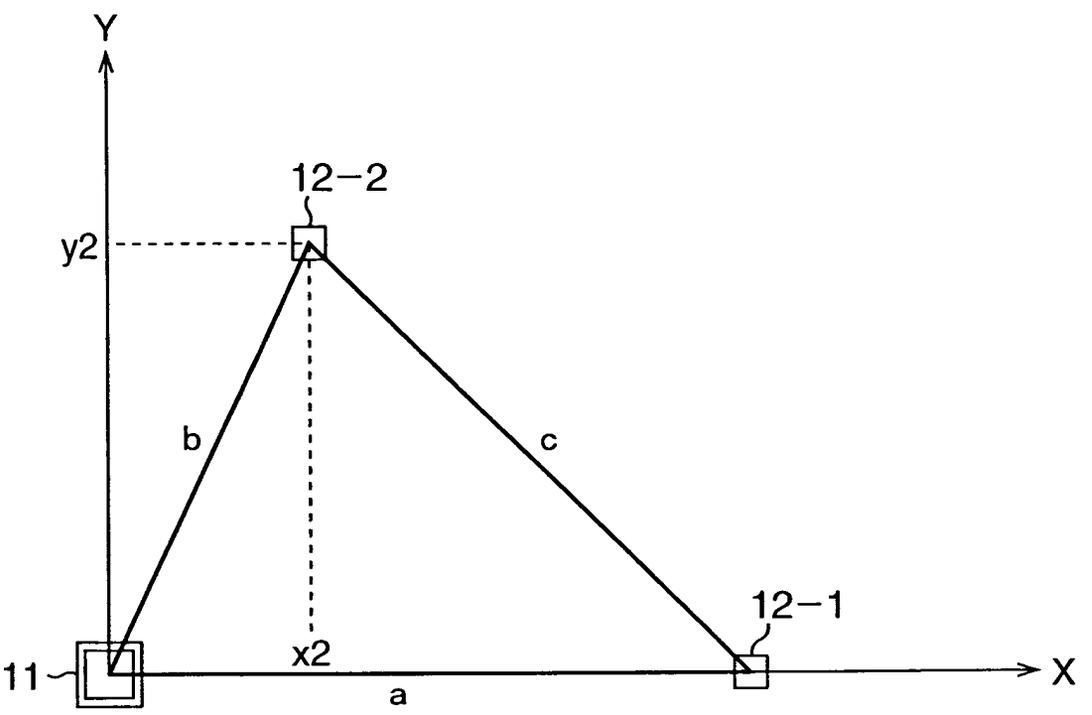


FIG. 6

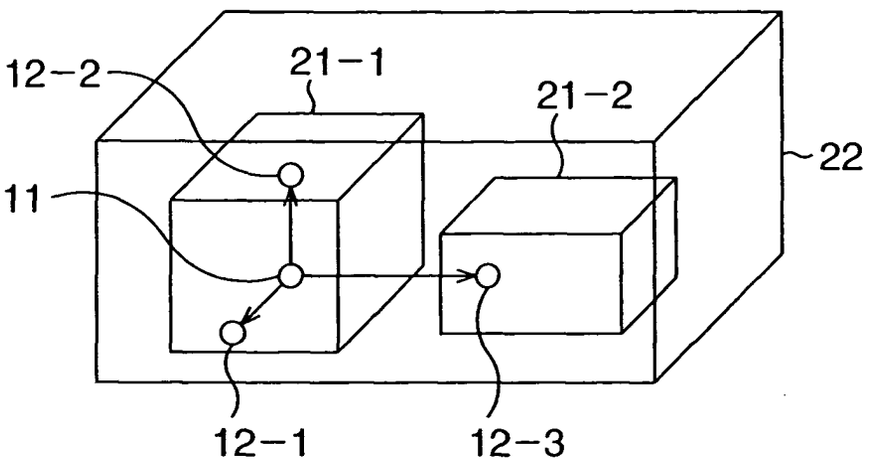


FIG. 7

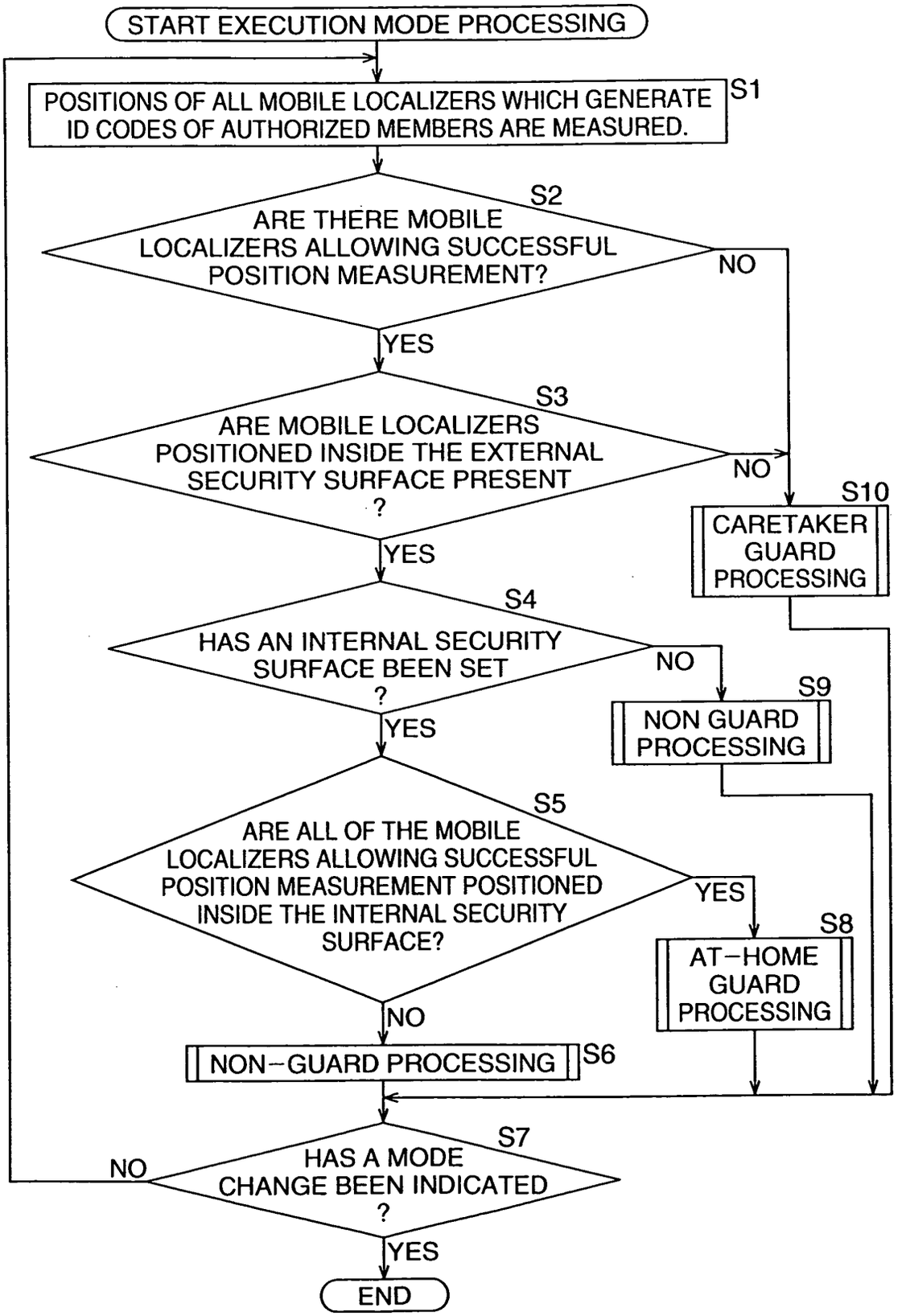

START EXECUTION MODE PROCESSING
POSITIONS OF ALL MOBILE LOCALIZERS WHICH GENERATE ID CODES OF AUTHORIZED MEMBERS ARE MEASURED.
S1
ARE THERE MOBILE LOCALIZERS ALLOWING SUCCESSFUL POSITION MEASUREMENT?
S2
NO
YES
ARE MOBILE LOCALIZERS POSITIONED INSIDE THE EXTERNAL SECURITY SURFACE PRESENT ?
S3
NO
YES
CARETAKER GUARD PROCESSING
S10
HAS AN INTERNAL SECURITY SURFACE BEEN SET ?
S4
NO
YES
NON GUARD PROCESSING
S9
ARE ALL OF THE MOBILE LOCALIZERS ALLOWING SUCCESSFUL POSITION MEASUREMENT POSITIONED INSIDE THE INTERNAL SECURITY SURFACE?
S5
YES
NO
AT-HOME GUARD PROCESSING
S8
NON-GUARD PROCESSING
S6
HAS A MODE CHANGE BEEN INDICATED ?
S7
NO
YES
END

FIG. 8

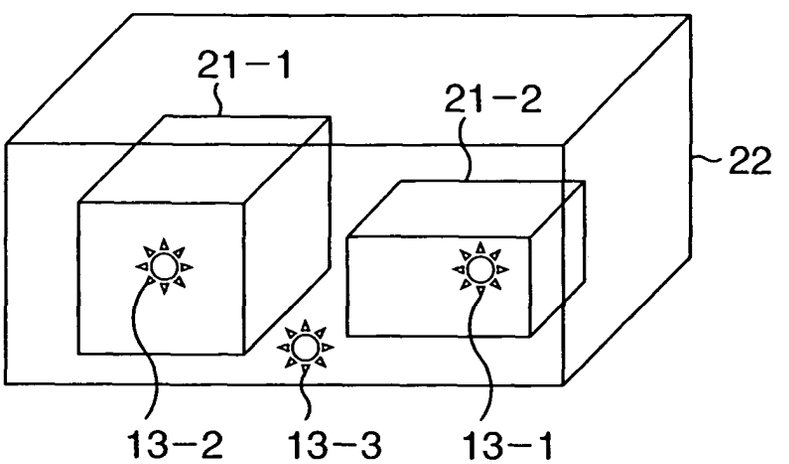


FIG. 9

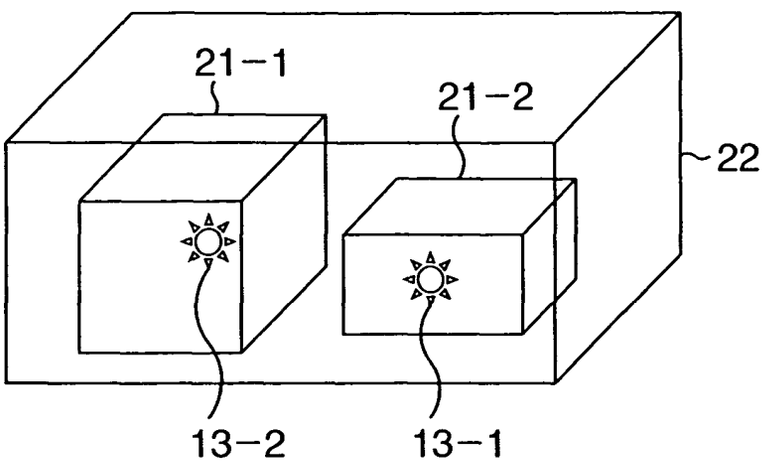


FIG. 10

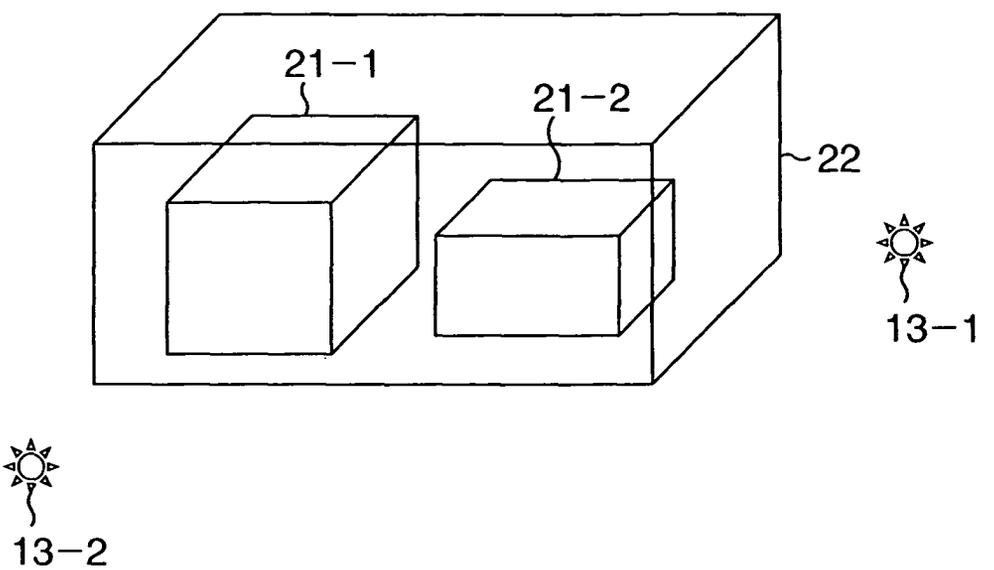


FIG. 11

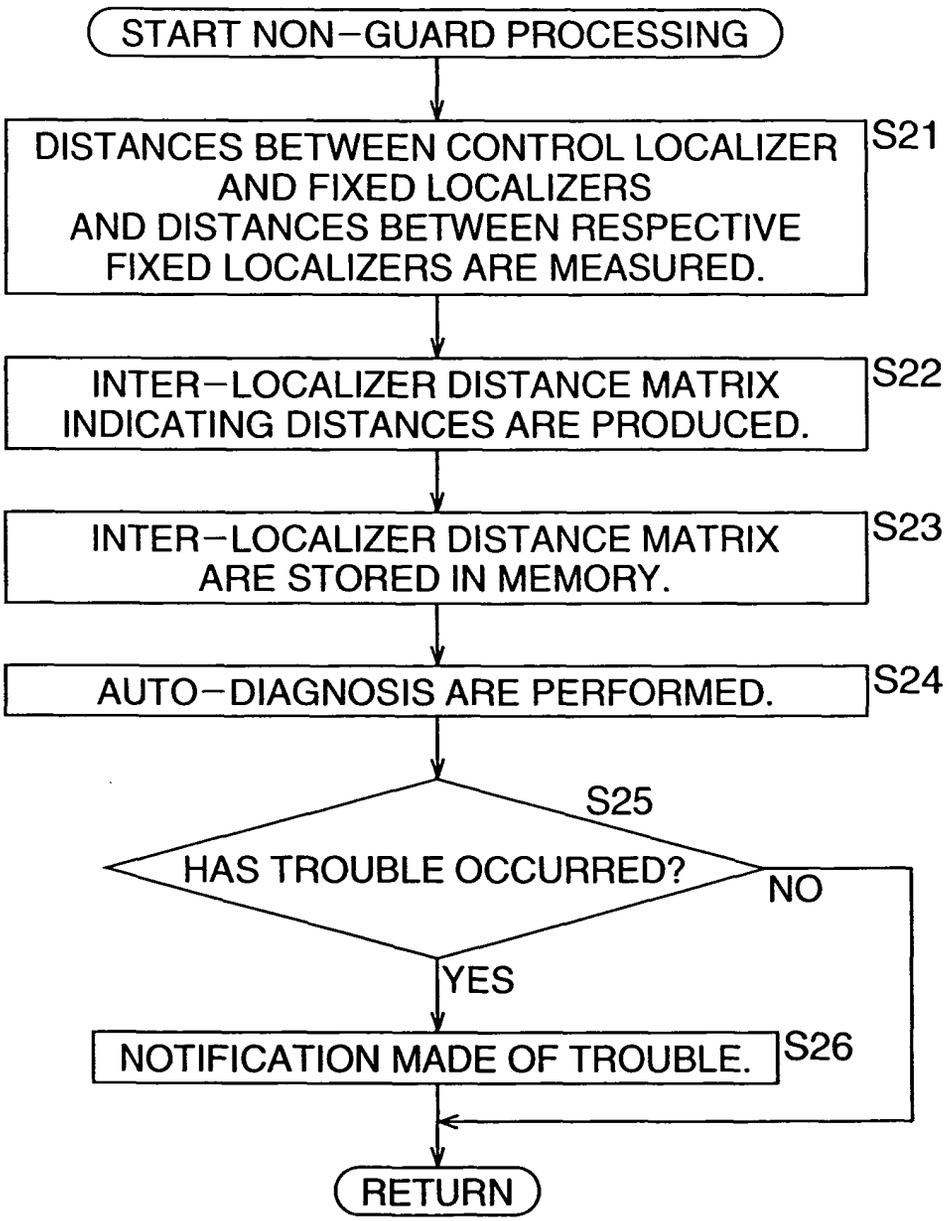

START NON-GUARD PROCESSING
DISTANCES BETWEEN CONTROL LOCALIZER AND FIXED LOCALIZERS AND DISTANCES BETWEEN RESPECTIVE FIXED LOCALIZERS ARE MEASURED.
S21
INTER-LOCALIZER DISTANCE MATRIX INDICATING DISTANCES ARE PRODUCED.
S22
INTER-LOCALIZER DISTANCE MATRIX ARE STORED IN MEMORY.
S23
AUTO-DIAGNOSIS ARE PERFORMED.
S24
S25
HAS TROUBLE OCCURRED?
NO
YES
NOTIFICATION MADE OF TROUBLE.
S26
RETURN

FIG. 12

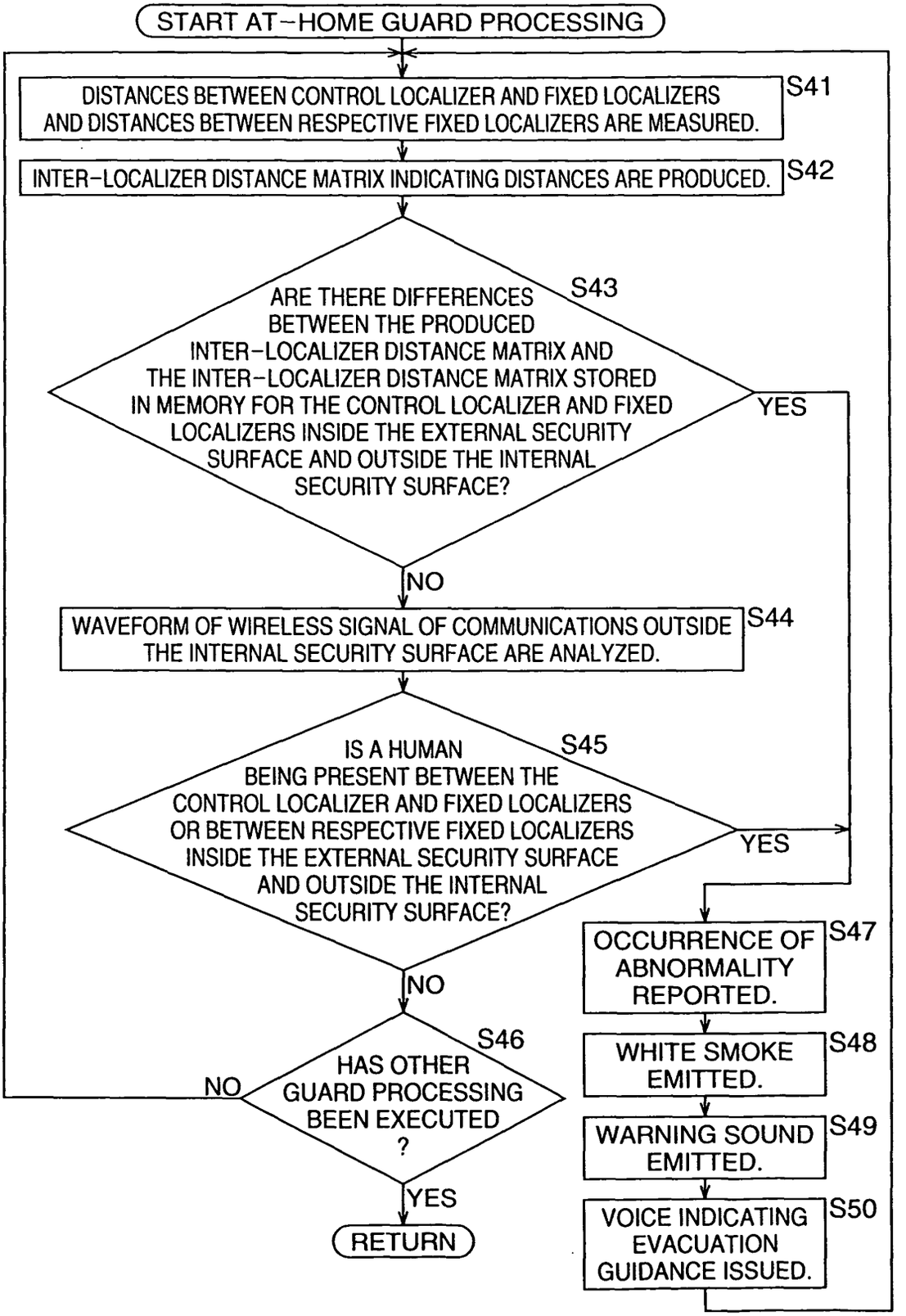

START AT-HOME GUARD PROCESSING
DISTANCES BETWEEN CONTROL LOCALIZER AND FIXED LOCALIZERS AND DISTANCES BETWEEN RESPECTIVE FIXED LOCALIZERS ARE MEASURED.
S41
INTER-LOCALIZER DISTANCE MATRIX INDICATING DISTANCES ARE PRODUCED.
S42
ARE THERE DIFFERENCES BETWEEN THE PRODUCED INTER-LOCALIZER DISTANCE MATRIX AND THE INTER-LOCALIZER DISTANCE MATRIX STORED IN MEMORY FOR THE CONTROL LOCALIZER AND FIXED LOCALIZERS INSIDE THE EXTERNAL SECURITY SURFACE AND OUTSIDE THE INTERNAL SECURITY SURFACE?
S43
YES
NO
WAVEFORM OF WIRELESS SIGNAL OF COMMUNICATIONS OUTSIDE THE INTERNAL SECURITY SURFACE ARE ANALYZED.
S44
IS A HUMAN BEING PRESENT BETWEEN THE CONTROL LOCALIZER AND FIXED LOCALIZERS OR BETWEEN RESPECTIVE FIXED LOCALIZERS INSIDE THE EXTERNAL SECURITY SURFACE AND OUTSIDE THE INTERNAL SECURITY SURFACE?
S45
YES
NO
HAS OTHER GUARD PROCESSING BEEN EXECUTED ?
S46
NO
YES
RETURN
OCCURRENCE OF ABNORMALITY REPORTED.
S47
WHITE SMOKE EMITTED.
S48
WARNING SOUND EMITTED.
S49
VOICE INDICATING EVACUATION GUIDANCE ISSUED.
S50

FIG. 13

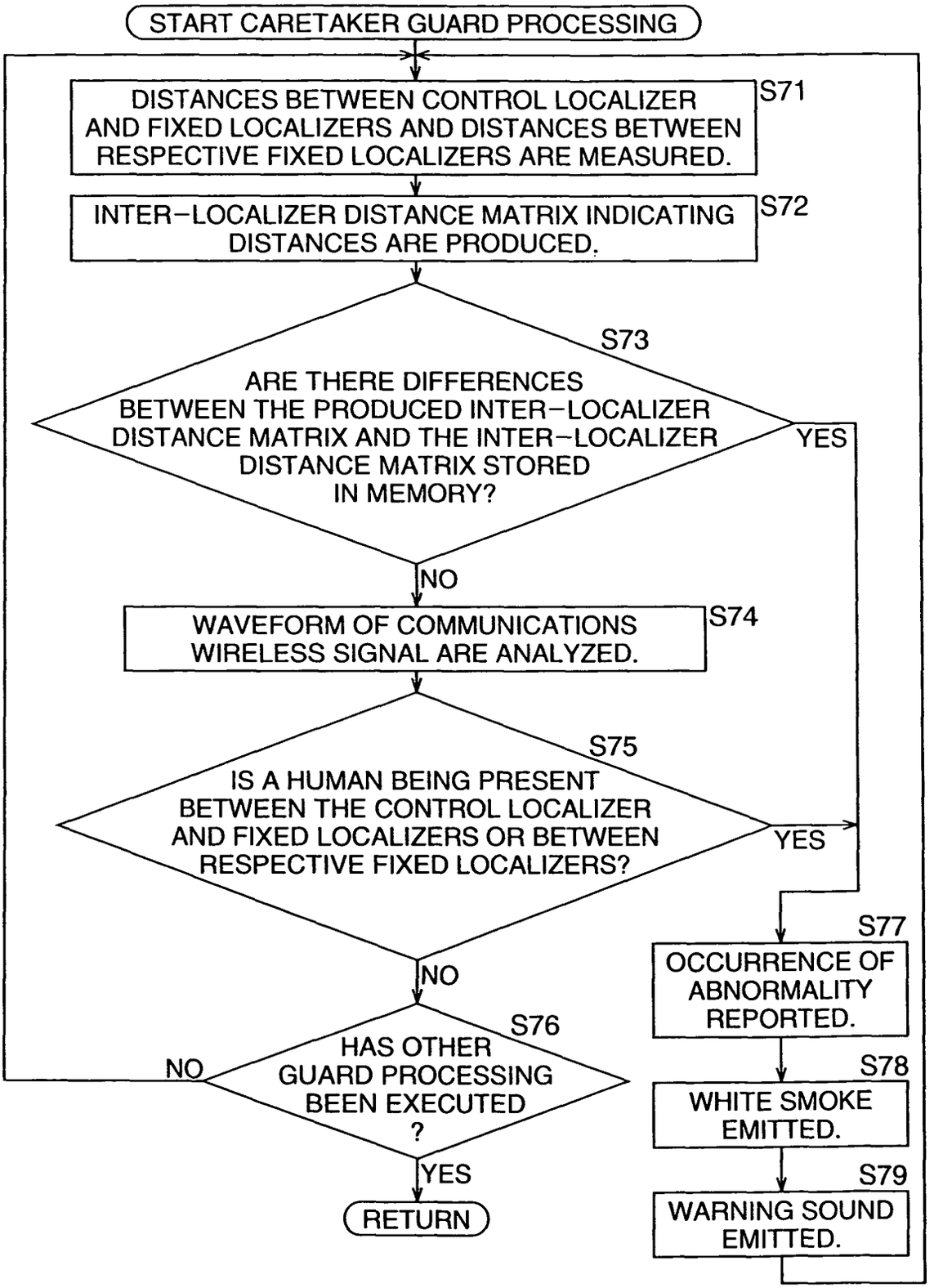

START CARETAKER GUARD PROCESSING
DISTANCES BETWEEN CONTROL LOCALIZER AND FIXED LOCALIZERS AND DISTANCES BETWEEN RESPECTIVE FIXED LOCALIZERS ARE MEASURED.
S71
INTER-LOCALIZER DISTANCE MATRIX INDICATING DISTANCES ARE PRODUCED.
S72
S73
ARE THERE DIFFERENCES BETWEEN THE PRODUCED INTER-LOCALIZER DISTANCE MATRIX AND THE INTER-LOCALIZER DISTANCE MATRIX STORED IN MEMORY?
YES
NO
WAVEFORM OF COMMUNICATIONS WIRELESS SIGNAL ARE ANALYZED.
S74
S75
IS A HUMAN BEING PRESENT BETWEEN THE CONTROL LOCALIZER AND FIXED LOCALIZERS OR BETWEEN RESPECTIVE FIXED LOCALIZERS?
YES
NO
S76
HAS OTHER GUARD PROCESSING BEEN EXECUTED ?
NO
YES
RETURN
S77
OCCURRENCE OF ABNORMALITY REPORTED.
S78
WHITE SMOKE EMITTED.
S79
WARNING SOUND EMITTED.

FIG. 14

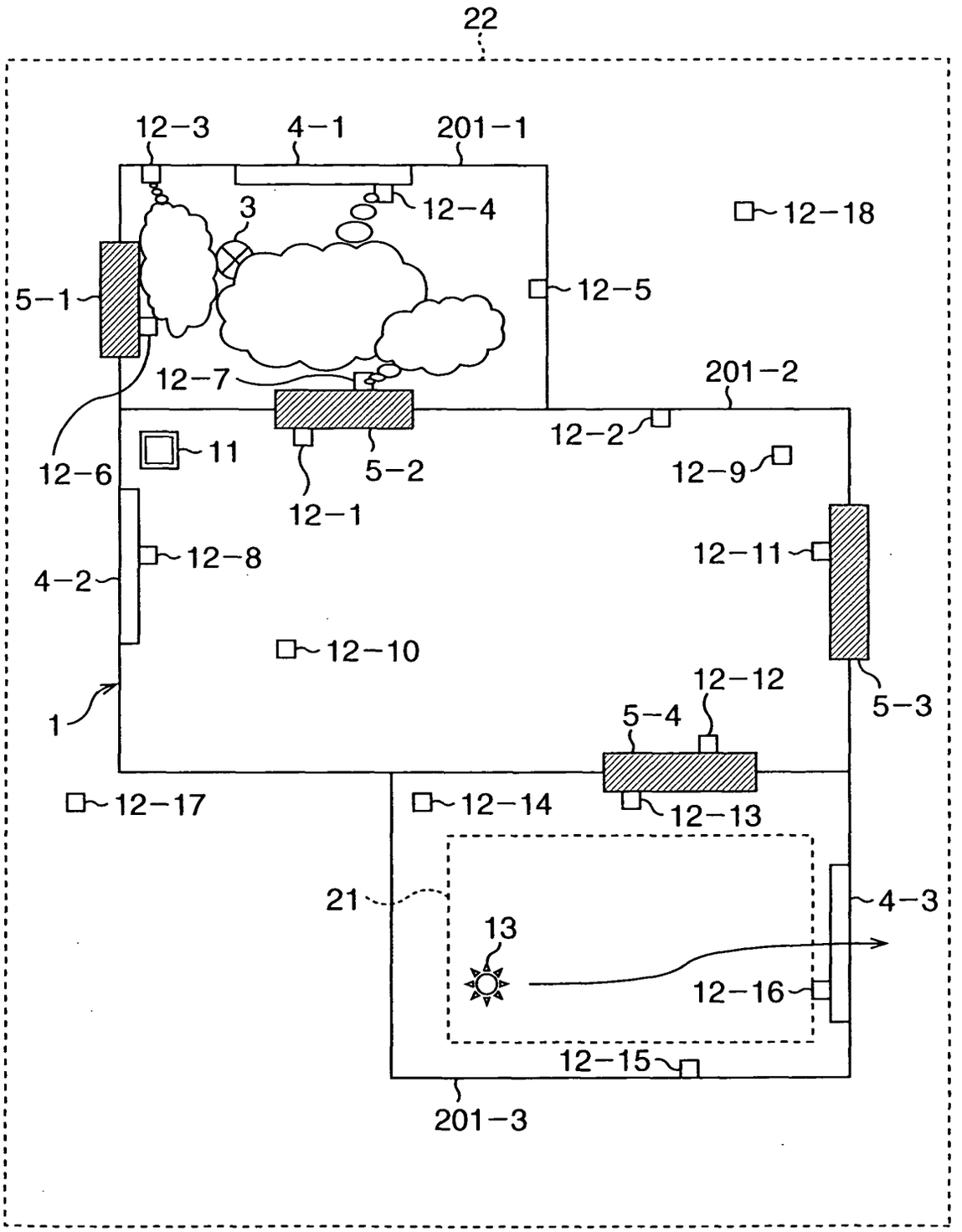
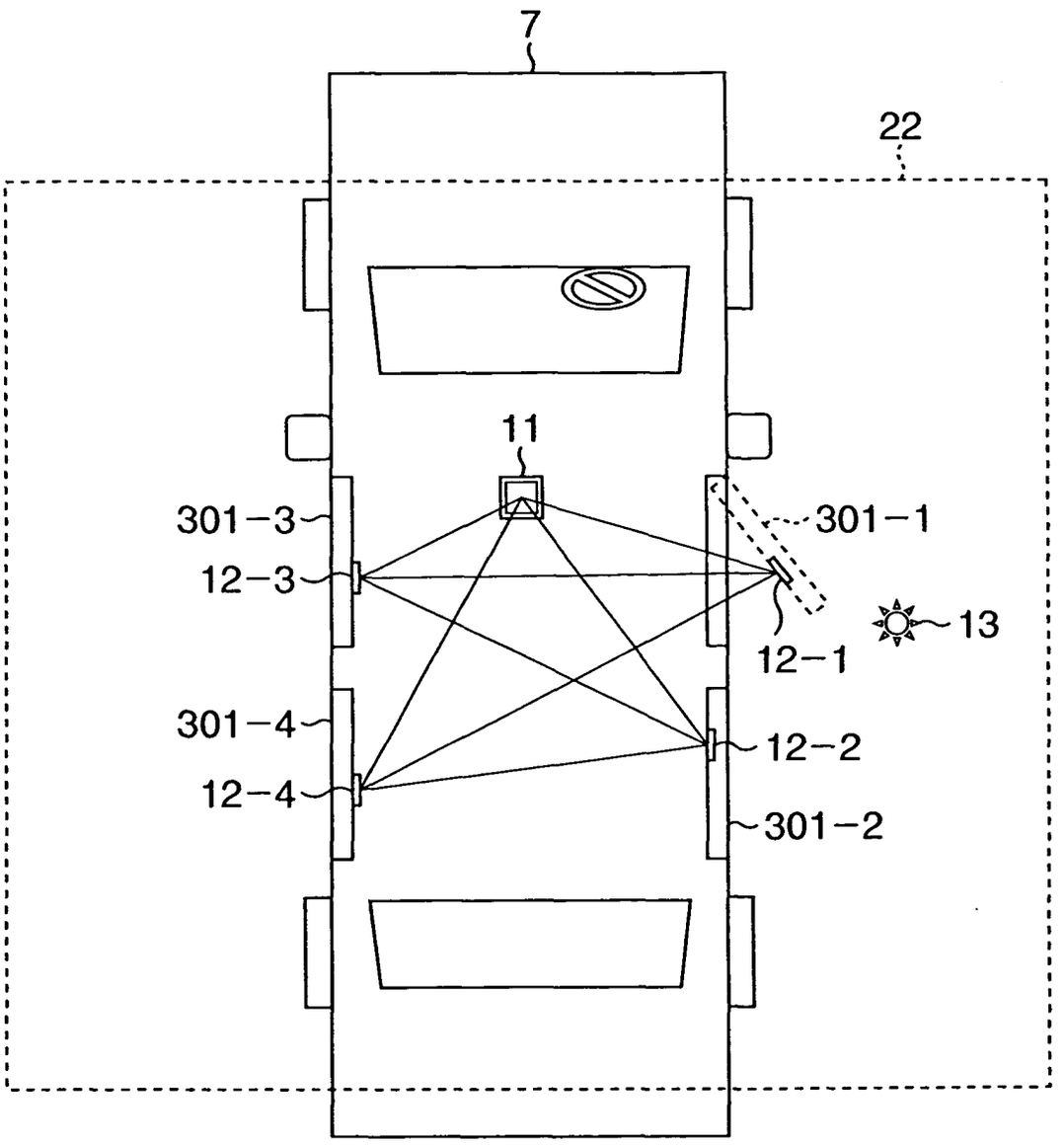

22
12-3
4-1
201-1
3
12-4
12-18
5-1
12-5
12-7
201-2
12-2
11
12-6
5-2
12-9
12-1
12-8
12-11
4-2
12-10
12-12
5-4
5-3
1
12-17
12-14
12-13
21
4-3
13
12-16
12-15
201-3

FIG. 15



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/002819

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G08B25/04, G08B25/10, G08B23/00, G08B13/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G08B25/04, G08B25/10, G08B23/00, G08B13/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2001/307251 A (Fenwal Co., Ltd.), 02 November, 2001 (02.11.01), Par. Nos. [0037] to [0049]; Figs. 1 to 2 (Family: none)	26 27,4,9,12, 14,25
Y A	JP 2000-76574 A (Victor Company Of Japan, Ltd.), 14 March, 2000 (14.03.00), Par. Nos. [0016] to [0021]; Figs. 1 to 3 (Family: none)	13-15,16-18, 24-25 19-23,26-29
Y A	JP 2001-14558 A (Victor Company Of Japan, Ltd.), 19 January, 2001 (19.01.01), Par. No. [0013]; Figs. 1 to 4 (Family: none)	13-15,24-25 26-29

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 June, 2004 (01.06.04)	15 June, 2004 (15.06.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/002819

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 9-180070 A (Obayashi Corp.), 11 July, 1997 (11.07.97), Par. Nos. [0024] to [0025] (Family: none)	15,16-18 20-21
A	JP 2001-355361 A (Kabushiki Kaisha Nakamura Gijutsu Kenkyusho), 26 December, 2001 (26.12.01) Claims; Figs 1 to 6 (Family: none)	1-12
P,A	JP 2003-288657 A (Sanyo Electric Co., Ltd.), 10 October, 2003 (10.10.03), Par. Nos. [0012] to [0017]; Figs 1 to 4 (Family: none)	1-12

Form PCT/ISA/210 (continuation of second sheet) (January 2004)