(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 1 月 9 日(09.01.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/006733 A1

(51) 国際特許分類:
G08B 25/10 (2006.01) *G08B 25/08* (2006.01)
G08B 25/00 (2006.01)

(21) 国際出願番号: PCT/JP2012/067242

(22) 国際出願日: 2012 年 7 月 5 日(05.07.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 株式会社　テクノミライ (TECHNOMIRAI Co., Ltd.) [JP/JP]; 〒1690075 東京都新宿区高田馬場１－３３－１３ Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 三輪　和夫 (MIWA Kazuo) [JP/JP]; 〒1690075 東京都新宿区高田馬場１－３３－１３　株式会社　テクノミライ内 Tokyo (JP).

(74) 代理人: 中村　和男 (NAKAMURA Kazuo); 〒1440051 東京都大田区西蒲田七丁目５０番１０号　中村ビル２階　中村国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

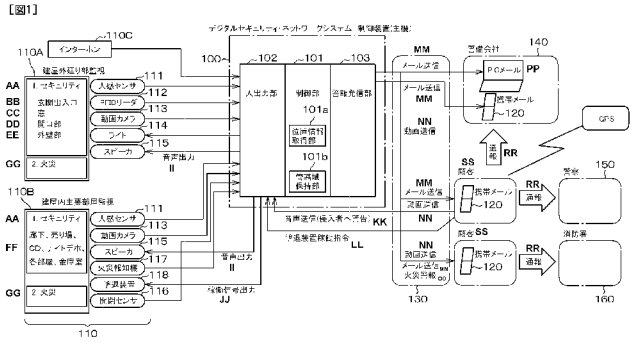
添付公開書類:

— 国際調査報告（条約第 21 条(3)）

(54) **Title**: DIGITAL SECURITY NETWORK SYSTEM AND METHOD

(54) 発明の名称 : デジタルセキュリティー・ネットワークシステム及び方法

[図1]



100 Control device (main device) in digital security network system
101 Control unit
101a Positional information acquisition section
101b Jurisdiction area holding section
102 Input and output unit
103 Alert issue unit
110A Outdoor periphery monitoring unit
110B Indoor main room monitoring unit
110C Intercom
111 Presence sensor
112 PFID reader
113 Video camera
114 Light
115 Speaker
116 Opening and closing sensor
117 Fire alarm
118 Repel device
120 Mobile phone email
140 Security agency
150 Police
160 Fire station

AA 1. Security
BB Entrance and gateways
CC Windows
DD Openings
EE Outer walls
FF Corridors, sales departments, CDs, night depositories, rooms, strongrooms
GG 2. Fire
II Voice output
JJ Activation signal output
KK Voice transmission (alert to intruder)
LL Repel device activation instruction
MM Email transmission
NN Video transmission
OO Fire alert
PP PC email
RR Report
SS Customer

(57) **Abstract**: A monitoring device (100) includes: a control unit (101) that has a positional information acquisition section (101a) for tracing the positions of communication terminals (120) and acquiring the positional information of the communication terminals (120), and a jurisdiction area holding section (101b) for holding the jurisdiction areas where a building for which security is provided is located and emergency calls are received; an input and output unit (102) for detecting an emergency on the basis of sensor outputs from an input and output device (110); and an alert issue unit (103) for sending email or video through telephone lines (130). When detecting an emergency, the control unit (101) refers to the jurisdiction area holding section (101b) to identify a communication terminal (120) that exists in the police station jurisdiction area or the fire station jurisdiction area and reports the emergency to the identified communication terminal (120) with priority. As a result, since the report is sent with priority to the mobile phone located in the jurisdiction area where the building for which security is provided is located, a report can be sent quickly when an emergency call is made from the mobile phone.

(57) 要約:

[続葉有]

WO 2014/006733 A1

監視装置１００は、通信端末装置１２０の存在位置を追跡し、通信端末装置１２０の位置情報を取得する位置情報取得部１０１ａと、警備対象建物が存在する、緊急通報用電話を受信する管轄域を保持する管轄域保持部１０１ｂとを有する制御部１０１と、入出力装置１１０からのセンサ出力に基づいて、緊急事態を検出する入出力部１０２と、電話回線１３０を介してメール送信又は映像を通報する警報発信部１０３と、を備える。制御部１０１は、緊急事態を検出した場合、管轄域保持部１０１ｂを参照して、警察の管轄域又は消防の管轄域に存在する通信端末装置１２０を特定し、特定した通信端末装置１２０に優先的に通報する制御を行う。これにより、警備する建物が存在する管轄内にある携帯電話に優先的に通報することによって携帯電話から緊急電話した場合に迅速に通報を行うことができる。

明　細　書

発明の名称 ：

デジタルセキュリティー・ネットワークシステム及び方法

技術分野

[0001] 本発明は、デジタルセキュリティー・ネットワークシステム及び方法に関する。

背景技術

[0002] 個別の住宅や敷地又は、商業施設、金融機関、法人建物等において、不審者の侵入に対して警戒を行う警備システムが一般的に知られている。例えば、住宅や敷地等に不審者が侵入した場合にはその不審者に警告等を発して威嚇したり、住人、職員や警備会社等に通報する。

[0003] 特許文献１には、操作者による切り替え操作の異常を検知した段階で、当該切り替え操作の異常をリカバリ可能にする警備システムが記載されている。特許文献１記載の警備システムは、監視領域における異常を検知して通報する制御装置が、利用者に付与された識別情報及び管理者に付与された識別情報と、電子メールアドレスとを各々対応付けて記憶し、警備モードの設定の切り替え操作を受け付け、これらの判断結果に応じて、特定した電子メールアドレスを含む電子メールを生成して送信する。

[0004] 特許文献２には、住宅分譲地を含む特定地域の警戒を行う地域警備システムが記載されている。特許文献２記載の警備システムは、非住人の存在位置と行動態様を判別し、非住人の存在位置に該当する地図情報上の箇所に、非住人の行動態様に応じた表示形式で非住人情報を表示する。

[0005] 一方、携帯電話機は、現在では広く普及し、基本となる音声通話に加えて電子メールによる通信や電子カメラによる画像取得とその画像の通信、更には測位システム（ＧＰＳ：Global Positioning System）を利用して位置情報を取得し現在位置を地図上に表示することができるものもある。携帯電話機は、その性格から個人単位の情報ツールとして外出時には常に持ち歩いて使

用されることから、携帯電話機を利用して個人の場所の検索サービスや緊急時における緊急通報サービスなどが一部実用化され、利用されている。また、携帯電話機を使用した緊急通報に関して各種の提案がなされている（例えば、特許文献３～５）。

[0006] すなわち、特許文献３には、異常が発生したときに簡易にそれを通報することのできる異常通報システムが記載されている。また、特許文献４には、サービス契約時に登録した様々なクライアント端末に対して地図情報を含めた緊急情報を手間を掛けずに通報する装置が記載されている。また、特許文献５には、異常時に通報者の位置情報等を迅速に伝える技術が記載されている。特許文献５記載のシステムは、通報者が、小型の発信装置を身に付け、携帯電話機は、小型の発信装置からのトリガ信号を受信したならば、ＧＰＳ信号を受信して携帯電話機の位置情報を計算し、電話番号等の情報と共に携帯電話網を経由して管理サーバに送信する。管理サーバでは、それらの情報をプッシュ型配信によって端末装置に送信する。

先行技術文献

特許文献

[0007] 特許文献1：特開２０１２－１１３４４６号公報

特許文献2：特開２０１１－１１３２５５号公報

特許文献3：特開２００１－１１８１７４号公報

特許文献4：特開２００２－１９７５７８号公報

特許文献5：特開２００２－２６１９８２号公報

発明の概要

発明が解決しようとする課題

[0008] しかしながら、このような従来の警備システムにあっては、管轄外にある携帯電話から緊急電話（例えば１１０番、１１９番）すると、電話受信署が一旦受けて、管轄署に連絡して、管轄署から折り返し電話をすることになる。例えば、警備したい自宅及び事業所が東京にあって、鹿児島から電話する

場合などは、電話受信署が一旦受けて、管轄署に連絡して、管轄署から折り返し電話をすることになる。そのため、通報が遅れるという課題があった。

[0009] 本発明の目的は、警備する建物が存在する管轄内にある携帯電話に優先的に通報することによって携帯電話から緊急電話した場合に迅速に通報を行うことができるデジタルセキュリティー・ネットワークシステム及び方法を提供することにある。

課題を解決するための手段

[0010] 本発明に係るデジタルセキュリティー・ネットワークシステムは、複数の通信端末装置の存在位置を検出し、前記通信端末装置の位置情報を取得する位置情報取得手段と、警備対象建物が存在する、緊急通報用電話を受信する管轄域を保持する管轄域保持手段と、緊急事態を検出する緊急事態検出手段と、前記緊急事態検出手段が緊急事態を検出したことに応じて、前記管轄域保持手段を参照して、複数の前記通信端末装置のいずれかが前記管轄域に存在する場合に、該管轄域に存在する前記通信端末装置に優先的に通報する制御手段とを備えることを特徴とする。

[0011] 本発明に係るデジタルセキュリティー・ネットワーク方法は、複数の通信端末装置の存在位置を検出し、前記通信端末装置の位置情報を取得するステップと、警備対象建物が存在する、緊急通報用電話を受信する管轄域を保持するステップと、緊急事態を検出するステップと、緊急事態を検出したことに応じて、複数の前記通信端末装置のいずれかが前記管轄域に存在する場合に、該管轄域に存在する前記通信端末装置に優先的に通報するステップとを備えることを特徴とする。

発明の効果

[0012] 本発明によれば、警備する建物が存在する管轄内にある携帯電話に優先的に通報することによって携帯電話から緊急電話した場合に迅速に通報を行うことができる。

図面の簡単な説明

[0013] [図1]図１は、本発明の一実施の形態に係るデジタルセキュリティー・ネット

ワークシステムの構成を示すブロック図である。

[図2]図２は、上記実施の形態に係るデジタルセキュリティー・ネットワークシステムの屋外警備機能の手順・動作を示すフローチャートである。

[図3]図３は、上記実施の形態に係るデジタルセキュリティー・ネットワークシステムの屋外警備機能の手順・動作を示すフローチャートである。

[図4]図４は、上記実施の形態に係るデジタルセキュリティー・ネットワークシステムの屋内警備機能の手順・動作を示すフローチャートである。

[図5]図５は、上記実施の形態に係るデジタルセキュリティー・ネットワークシステムの火災予防機能の手順・動作を示すフローチャートである。

発明を実施するための形態

[0014] 以下、添付図面を参照しながら本発明を実施するための形態について詳細に説明する。

（実施の形態）

図１は、本発明の一実施の形態に係るデジタルセキュリティー・ネットワークシステムの構成を示すブロック図である。

[0015] 本デジタルセキュリティー・ネットワークシステムは、デジタルセキュリティ・ネットワークシステム機器本体である監視装置１００と、建物内外の各部に設置され、ケーブル等の有線又は近距離無線等の無線により監視装置１００に接続されて異常状態を検出し、また異常を報知する各種入出力装置１１０と、公衆回線である電話回線１３０を介して通信可能な複数の通信端末装置１２０と、を含んで構成される。

[0016] なお、デジタルセキュリティ・ネットワークシステムは、通信端末装置１２０に対して、セキュリティ契約のサービスを提供する場合、デジタルセキュリティ・ネットワークシステムから見て、通信端末装置１２０の使用者を顧客と呼ぶことができる。

[0017] ［監視装置１００］

監視装置１００は、制御部１０１、入出力部１０２、及び警報発信部１０３を備える。

[0018] 制御部１０１は、マイクロコンピュータ等により構成され、装置全体を制御するとともに、警備プログラムを実行して、デジタルセキュリティー・ネットワークシステムとして機能させる。制御部１０１は、情報を記憶するメモリ（図示略）を有する。メモリは、半導体メモリ、磁気記録デバイス、光ディスクデバイス又は光磁気ディスクデバイス等が挙げられる。

[0019] 制御部１０１は、通信端末装置１２０の存在位置を追跡し、通信端末装置１２０の位置情報を取得する位置情報取得部１０１ａと、携帯電話の受信管轄域としての警察の管轄域、及び消防の管轄域とをそれぞれ保持する管轄域保持部１０１ｂと、を備える。ここで、携帯電話の受信管轄域としての警察の管轄域と消防の管轄域とは必ずしも同じではなく、例えば日本における警察の管轄域は、都道府県単位を基本とし、消防の管轄域は警察よりも管轄域が細かい。したがって、仮にその両者が等しい国においては、その両方を保持する必要はない。制御部１０１は、緊急事態を検出した場合、管轄域保持部１０１ｂを参照して、その緊急事態の内容に応じて、警察の管轄域又は消防の管轄域に存在する通信端末装置１２０を特定し、特定した通信端末装置１２０に優先的に通報する制御を行う。

[0020] 制御部１０１は、通報を受けた通信端末装置１２０から送信された音声送信（侵入者へ警告）と、撃退装置稼働指令を判定し、これら指令が適合する場合に、入出力部１０２を介してスピーカ１１５に音声出力を出力し、撃退装置１１８に稼働信号を出力する。

[0021] 入出力部１０２は、入出力装置１１０からのセンサ出力に基づいて、緊急事態を検出する緊急事態検出手段としての機能を有する。入出力部１０２は、電話回線１３０を介して通信端末装置１２０から送信されてくる各通信端末装置１２０の位置情報を受信し、制御部１０１にこれらの信号を出力する。入出力部１０２は、電話回線１３０を介して通信端末装置１２０から送信されてくる音声送信（侵入者への警告）と撃退装置稼働指令を受信し、制御部１０１にこれらの信号を出力する。

[0022] 警報発信部１０３は、電話回線１３０を介して通信端末装置１２０及び警

備会社１４０にメール送信、動画を含む映像の送信又は火災警報を送信する。

[0023] ［入出力装置１１０］

入出力装置１１０は、各種センサ及び出力装置からなる建屋外廻り部監視１１０Ａ、建屋内主要部屋監視１１０Ｂ、及びインターホン１１０Ｃと、を備える。

[0024] 建屋外廻り部監視１１０Ａは、主に、玄関出入口、窓、開口部、外壁部を対象とするセキュリティと、火災防止とを目的とする。建屋外廻り部監視１１０Ａの入力装置には、例えば、人感センサ１１１、ＲＦＩＤ（Radio Frequency Identification）リーダ１１２、動画カメラ１１３があり、その出力装置にはライト１１４、スピーカ１１５がある。ＲＦＩＤは、電波を利用した認証技術である。ＲＦＩＤリーダ１１２は、ＩＣチップの情報を、ＲＷ（リーダ／ライタ）装置で読み取り、物体認識や個人認証を行う。動画カメラ１１３は、動画を撮像する。ライト１１４は、点灯又は点滅して不審者等に警告する。スピーカ１１５は、入出力部１０２からの音声出力信号に基づいてメッセージ又は警告音を放音して不審者等に警告する。

[0025] 建屋内主要部屋監視１１０Ｂは、主に、廊下、売場、キャッシュディスペンサ（ＣＤ）、ナイトデポ、各部屋、金庫室を対象とするセキュリティと、火災防止とを目的とする。建屋外廻り部監視１１０Ａの入力装置には、例えば、人感センサ１１１、動画カメラ１１３、開閉センサ１１６、火災報知器１１７があり、その出力装置にはスピーカ１１５、撃退装置１１８がある。開閉センサ１１６は、扉の開閉を感知する接触式センサ等である。撃退装置１１８は、例えば金庫室、主要部屋に設置された拡大音声装置、噴霧装置である。撃退装置１１８は、入出力部１０２からの稼働信号出力に基づいて作動し、拡大音声等により大音響で放音して不審者を撃退する。また、センサライト等の人の五感に訴える警報器でもよい。

[0026] インターホン１１０Ｃは、玄関に設置され、監視装置１００の入出力部１０２に訪問者の問合せなどの音声信号を入力する。また、監視装置１００の

遠隔制御機能によって、通信端末装置１２０からの音声信号をインターホン１１０Ｃに出力可能である。

[0027] ［通信端末装置１２０］

通信端末装置１２０は、携帯電話、ＰＨＳ（Personal Handy-Phone System）、ＰＤＡ（Personal Digital Assistants）又はスマートフォン等で構成され、電話回線１３０を介して監視装置１００に音声送信及び撃退装置稼働指令を送信する。本実施の形態では、通信端末装置１２０は、携帯電話、スマートフォンの利用を想定しており、各個人が様々な場所（すなわち存在位置）で使用可能である。通信端末装置１２０のうちの一つは、警備会社１４０にＰＣ（Personal Computer）とともに配置される。通信端末装置１２０は、電話回線１３０を介して監視装置１００からのメール又は動画を含む映像等を受信可能である。

[0028] 通信端末装置１２０は、位置情報の電波をＧＰＳ衛星等から受信するＧＰＳ機能部１２１（図３参照）を備え、ＧＰＳアンテナを介して受信した情報より、現在位置情報を、緯度／経度の２つのパラメータとして算出して位置情報を取得する。一般にＧＰＳによって高度情報も得られるが、本実施の形態では用いない。また、ＧＰＳ機能部１２１に代え、又は併用して、基地局及びネットワークを介して携帯電話会社サーバと情報の送受信を行い、通信端末装置１２０の現在位置情報を取得することもできる。取得した位置情報は、適時、監視装置１００に送信される。

[0029] 警備会社１４０は、本デジタルセキュリティー・ネットワークシステムからメール又は映像等を受信したときに、異常事態について調査を行う。なお、警備会社１４０は、本実施の形態に係るデジタルセキュリティー・ネットワークシステムの必須構成要素ではない。

[0030] 以下、上述のように構成されたデジタルセキュリティー・ネットワークシステムの警備動作について説明する。

まず、デジタルセキュリティー・ネットワークシステムの屋外警備機能についてセキュリティ動作を例に採り説明する。

[0031] 図２及び図３は、デジタルセキュリティー・ネットワークシステムの屋外警備機能の手順・動作を示すフローチャートである。本フローは、主に監視装置１００の制御部１０１により実行される。また、監視装置１００からの送信を受けた通信端末装置１２０の制御部（図示略）により実行される。図中、Ｓは監視装置１００の制御部１０１及び通信端末装置１２０の制御部により実行されるフローの各ステップを示す。

[0032] まず、ステップＳ１１では、制御部１０１は、各センサ入力により物体認識を行う。具体的には、監視装置１００の入出力部１０２は、建屋外廻り部監視１１０Ａのセキュリティ（図１参照）機能として玄関出入口、窓、開口部、外壁部等に設置された人感センサ１１１、ＲＦＩＤリーダ１１２、及びインターホン１１０Ｃの入力を受け付ける。制御部１０１は、これらのセンサ入力を基に物体（人等）が管轄の屋外に入ったことを認識する。ここで、制御部１０１は、ＲＦＩＤリーダ１１２のＩＤ情報を基に、物体が玄関から例えば１０ｍに達したときに物体判定を行う。

[0033] ステップＳ１２では、制御部１０１は、ＲＦＩＤの判定結果に基づいて認識した物体が不審者であるか否かを判断する。例えば、制御部１０１は、ＲＦＩＤのＩＤ情報がＩＤ登録者である場合は、正常者であると判断してステップＳ１３に進み、ＩＤ未登録者である場合は、物体が不審者の可能性があると判断してステップＳ１４に進む。

[0034] ステップＳ１３では、制御部１０１は、ＲＦＩＤの判定結果により警備監視を解除してステップＳ２２に進む。

上記ステップＳ１２でＩＤ未登録者の場合、ステップＳ１４で制御部１０１は、物体と玄関までの距離を判定する。

[0035] ステップＳ１５では、制御部１０１は、物体と玄関までの距離に応じた制御対応を行う。すなわち、(1)物体と玄関までの距離が１０ｍに到達した場合、制御部１０１は、ライト１１４（図１参照）に制御信号を出力し、ステップＳ１６でライト１１４を点灯させる。(2)物体と玄関までの距離が６ｍに到達した場合、制御部１０１は、スピーカ１１５（図１参照）に音声信号を出

力し、ステップＳ１６でスピーカ１１５から犬の鳴き声、人の話し声等を音声出力する。(3)物体と玄関までの距離が５ｍに到達した場合、制御部１０１は、室内のテレビ電源をＯＮ、又は部屋照明を点灯させる。ここまでの制御対応により、本デジタルセキュリティー・ネットワークシステムは、不審者に対して侵入を認識していることを知らしめる。

[0036] (4)物体と玄関までの距離が４ｍに到達した場合、ステップＳ１６で制御部１０１は、各通信端末装置１２０及び警備会社１４０のＰＣにメールを送信する。特に、各通信端末装置１２０は、移動通信可能な携帯電話・スマートフォンなどからなり、各個人の所在場所（すなわち存在位置）で使用される。また、これら通信端末装置１２０の存在位置は、監視装置１００によって予め追跡され、監視装置１００は、これらの通信端末装置１２０の存在位置を記憶しておくようにすることもできる。物体と玄関までの距離が４ｍに到達した場合、制御部１０１は、各通信端末装置１２０と警備会社１４０のＰＣにメールを送信することになる。

[0037] (5)監視装置１００の入出力部１０２（図１参照）には、動画カメラ１１３からの映像が入力されている。物体と玄関までの距離が３ｍに到達した場合、ステップＳ１５で制御部１０１は、動画カメラ１１３からの映像を取り込む。なお、物体と玄関までの距離が３ｍに到達した場合に、動画カメラ１１３を起動する態様でもよい。物体と玄関までの距離が３ｍに到達した場合、ステップＳ１６で制御部１０１は、各通信端末装置１２０及び警備会社１４０のＰＣに撮影した映像を送信する。物体と玄関までの距離が３ｍに到達した場合、制御部１０１は、メールに加えて映像を各通信端末装置１２０と警備会社１４０のＰＣに送信することになる。監視装置１００から送信された映像を受信する通信端末装置１２０の位置情報を用いた詳細動作については、図３のステップＳ２４以降において述べる。

[0038] (6)物体と玄関までの距離が２ｍに到達した場合、ステップＳ１５を抜け、不審者の最終判断処理に移行する。なお、建物に設置したレーザ又はレーダの信号を検出することで、物体と玄関までの距離をより正確に検出すること

ができる。

[0039] ステップＳ１７では、各通信端末装置１２０の使用者は、監視装置１００から受信した映像を確認する。

ステップＳ１８では、各通信端末装置１２０の使用者は、映像確認後、必要と判断した場合には、通信端末装置１２０を使用して監視装置１００に接続し、監視装置１００の遠隔制御機能によってインターホン１１０Ｃ経由で用件の問合せ等の通知を行う。

[0040] ステップＳ１９では、インターホン１１０Ｃによる確認及び後述するメール確認に基づいて、制御部１０１は、不審者か否かを判断する。不審者の場合は、ステップＳ２０で入出力部１０２は、スピーカ１１５により威嚇音声を発し、かつステップＳ２１で警報発信部１０３は、警備会社１４０へ通報する。

[0041] 一方、上記ステップＳ１９で不審者でない場合は、ステップＳ２２で制御部１０１は、玄関ドアの施錠を解錠し、ステップＳ２３で操作盤の警備実行警報を解除して本フローを終了する。

上記ステップＳ１６で監視装置１００から映像が送信された場合、図３のステップＳ２４に進む。

[0042] ステップＳ２４では、各通信端末装置１２０の使用者は、受信した映像を確認する。

ステップＳ２５では、通信端末装置１２０の制御部は、ＧＰＳ機能部１２１により検出した現在の位置情報を監視装置１００に送信する。

[0043] ステップＳ２６では、監視装置１００の制御部１０１は、入出力部１０２が通信端末装置１２０からの位置情報を受信する。

ステップＳ２７では、制御部１０１は、受信した通信端末装置１２０の位置情報に基づいて、警察緊急通報用電話受信管轄域である都道府県のいずれの所在かを判定する。

[0044] ステップＳ２８では、制御部１０１は、警備対象建物が存在する管轄域である該当都道府県に存在すると判定した通信端末装置１２０に対して優先的

に警察１５０への通報指示のメールを送信する。

ステップＳ２９では、通信端末装置１２０の制御部は、監視装置１００からの通報指示メールを受信する。通信端末装置１２０の使用者は、受信した通報指示メールに従い、リアルタイム動画を目視確認し、必要に応じて警察１５０へ通報する。

[0045] ステップＳ３０では、通信端末装置１２０の制御部は、監視装置１００に警察１５０へ通報した旨、又は警察１５０へ通知しなかった旨を返信する。

ステップＳ３１では、監視装置１００の制御部１０１は、他の通信端末装置１２０及び警備会社１４０に対して、警察１５０へ通報した結果メールを送信する。

[0046] ステップＳ３２では、警察１５０へ通報した通信端末装置１２０の使用者は、侵入者に対して警察１５０に通報したことを警告し、この警告により威嚇して退去させる。その後、上記ステップＳ１９に進む。

[0047] 次に、デジタルセキュリティー・ネットワークシステムの屋内警備機能についてセキュリティ動作を例に採り説明する。

図４は、デジタルセキュリティー・ネットワークシステムの屋内警備機能の手順・動作を示すフローチャートである。本フローは、不審者侵入に対する撃退フローに適用した例である。

[0048] まず、ステップＳ４１は、制御部１０１は、各センサ入力により物体認識を行う。具体的には、監視装置１００の入出力部１０２は、建屋内主要部屋監視１１０Ｂのセキュリティ（図１参照）機能として廊下、売場、キャッスディスペンサ、ナイトデポ、各部屋、金庫室等に設置された人感センサ１１１、ＲＦＩＤリーダ１１２、及び開閉センサ１１６の入力を受け付ける。制御部１０１は、これらのセンサ入力を基に物体（人等）が屋内に入ったことを認識する。ここで、制御部１０１は、ＲＦＩＤリーダ１１２のＩＤ情報を基に判定を行う。

[0049] ステップＳ４２では、制御部１０１は、ＲＦＩＤの判定結果に基づいて認識した物体が不審者であるか否かを判断する。制御部１０１は、ＲＦＩＤの

ＩＤ情報がＩＤ登録者である場合は、正常者であると判断してステップＳ４３に進み、ＩＤ未登録者である場合は、物体が不審者の可能性があると判断してステップＳ４４に進む。

[0050] ステップＳ４３では、制御部１０１は、警備監視を解除してステップＳ２３（図３参照）に進む。

上記ステップＳ４２でＩＤ未登録者の場合、ステップＳ４４で制御部１０１は、不審者侵入と判断して動画カメラ１１３からの映像を取り込むとともに、該当通信端末装置１２０及び警備会社１４０にメール・映像を送信してステップＳ４５に進む。また、監視装置１００からメール・映像が送信された通信端末装置１２０は、図３のステップＳ２４を実行する。すなわち、ステップＳ２４（図３参照）では、通信端末装置１２０の使用者は、受信した映像を確認する。

[0051] ステップＳ４５では、制御部１０１は、警備実行モードを実行する。警備実行モードは、具体的にはスピーカ１１５への音声出力、及び撃退装置の電源ＯＮである。

一方、ステップＳ４６では、通信端末装置１２０の使用者は、受信した映像を確認し、通報が必要と判断した場合は、ステップＳ４７で警察１５０に通報する。

[0052] ステップＳ４８では、制御部１０１は、警察１５０に通報したことと警告メッセージをスピーカ１１５により侵入者に通知し、侵入者を威嚇・退去させる。

ステップＳ４９では、制御部１０１は、人感センサ１１１等により侵入者が主要警戒エリアである２ｍに到達したことを検出する。

[0053] ステップＳ５０では、通信端末装置１２０の制御部は、ＧＰＳ機能部１２１により検出した現在の位置情報を監視装置１００に送信する。

ステップＳ５１では、監視装置１００の制御部１０１は、入出力部１０２が通信端末装置１２０からの位置情報を受信する。

[0054] ステップＳ５２では、制御部１０１は、受信した通信端末装置１２０の位

置情報に基づいて、警察緊急通報用電話受信管轄域である都道府県のいずれの所在かを判定する。

ステップＳ５３では、制御部１０１は、警備対象建物が存在する管轄域である該当都道府県に所在すると判定した通信端末装置１２０に対して優先的に警察１５０への通報指示のメールを送信する。

[0055] ステップＳ５４では、通信端末装置１２０の制御部は、監視装置１００からの通報指示メールを受信する。通信端末装置１２０の使用者は、受信した通報指示メールに従い、リアルタイム動画を目視確認し、必要に応じて警察１５０へ通報する。

ステップＳ５５では、制御部１０１は、再度、異常発生と警告メッセージをスピーカ１１５により侵入者に通知し、侵入者を威嚇・退去させる。

[0056] ステップＳ５６では、制御部１０１は、所定時間（例えば３０秒）経過を計時する。

一方、ステップＳ５７では、通信端末装置１２０の使用者は、受信した動画映像を確認する。ステップＳ５８では、通信端末装置１２０の使用者は、必要に応じて撃退装置稼働指示を出す。具体的には、予め準備されたメニューに従ってボタン操作することで、撃退装置稼働指示を実行する。通信端末装置１２０の制御部は、この撃退装置稼働指令（図１参照）を電話回線１３０を介して監視装置１００に送信する。監視装置１００の入出力部１０２は、受信した撃退装置稼働指令を制御部１０１に出力する。

[0057] ステップＳ５９では、制御部１０１は、上記ステップＳ５５の再度の警告メッセージ通知から３０秒経過し、かつ通信端末装置１２０から撃退装置稼働指令を受信したことを判別する。前記３０秒経過し、かつ前記撃退装置稼働指令を受信した場合、ステップＳ６０で制御部１０１は、撃退装置１１８を作動させる。撃退装置１１８は、例えば拡大音声装置、噴霧装置である。撃退装置１１８を作動させることで、侵入者を威嚇・撃退させる。

[0058] ステップＳ６１では、制御部１０１は、該当通信端末装置１２０及び警備会社１４０に、撃退装置１１８を作動させたことを通知する。

ステップＳ６２では、制御部１０１は、上記侵入者の侵入判定と同様の方法によって侵入者の退去を確認し、侵入者が退去した場合、警戒・警備を通常モードにして本フローを終了する。

[0059] 次に、デジタルセキュリティー・ネットワークシステムの火災予防機能について説明する。

図５は、デジタルセキュリティー・ネットワークシステムの火災予防機能の手順・動作を示すフローチャートである。

[0060] まず、ステップＳ７１では、監視装置１００は、火災警報監視を行う。具体的には、監視装置１００の入出力部１０２は、火災報知器１１７からの警報アラームを常時監視する。

ステップＳ７２では、制御部１０１は、入出力部１０２により火災報知器１１７からの警報アラーム、又は各部屋等に設置された温度計が異常（例えば８０℃）を感知したか否かを判別する。

[0061] 上記警報アラーム又は温度異常を感知した場合、ステップＳ７５で制御部１０１は、消火装置１１９の作動指示を出力する。消火装置１１９は、作動指示に従って作動する。また、ステップＳ７４で制御部１０１は、火災予防モードに移行し、動画映像を開始する。

ステップＳ７５では、制御部１０１は、動画カメラ１１３からの映像を取り込むとともに、該当通信端末装置１２０及び警備会社１４０にメール・映像を送信してステップＳ７６に進む。

[0062] ステップＳ７６では、監視装置１００からメール・映像が送信された通信端末装置１２０の使用者は、受信した映像を確認する。

ステップＳ７７では、通信端末装置１２０の制御部は、ＧＰＳ機能部１２１により検出した現在の位置情報を監視装置１００に送信する。

[0063] ステップＳ７８では、監視装置１００の制御部１０１は、入出力部１０２が通信端末装置１２０からの位置情報を受信する。

ステップＳ７９では、制御部１０１は、受信した通信端末装置１２０の位置情報に基づいて、消防緊急通報用電話受信管轄域のいずれの所在かを判定

する。

[0064] ステップＳ８０では、制御部１０１は、警備対象建物が存在する管轄域に存在すると判定した通信端末装置１２０に対して消防署１６０への通報指示のメールを送信する。

ステップＳ８１では、通信端末装置１２０の制御部は、監視装置１００からの通報指示メールを受信する。通信端末装置１２０の使用者は、受信した通報指示メールに従い、リアルタイム動画を目視確認し、消防署１６０へ通報する。

[0065] ステップＳ８２では、制御部１０１は、スピーカ１１５により近隣に火災警報を通知する。

ステップＳ８３では、制御部１０１は、該当通信端末装置１２０及び警備会社１４０に、消防署１６０への通報と消火装置１１９の作動と近隣への火災警報を通知した旨を通知する。

[0066] ステップＳ８４では、制御部１０１は、上記警報アラーム又は温度異常の判定と同様の方法によって消火を確認し、消火した場合、消火機能と発報を停止して本フローを終了する。

[0067] 以上詳細に説明したように、本実施の形態によれば、監視装置１００は、通信端末装置１２０の存在位置を追跡し、通信端末装置１２０の位置情報を取得する位置情報取得部１０１ａと、警備対象建物が存在する、緊急通報用電話を受信する警察管轄域及び消防管轄域を保持する管轄域保持部１０１ｂとを有する制御部１０１と、入出力装置１１０からのセンサ出力に基づいて、緊急事態を検出する入出力部１０２と、電話回線１３０を介してメール送信又は映像を通報する警報発信部１０３と、を備える。制御部１０１は、緊急事態を検出した場合、管轄域保持部１０１ｂを参照して、警察の管轄域又は消防の管轄域に存在する通信端末装置１２０を特定し、特定した通信端末装置１２０に優先的に通報する制御を行う。

[0068] この構成により、複数の携帯電話（通信端末装置１２０）の存在位置を追跡しておくことで、緊急事態を検出した場合、警察又は消防の管轄域に存在

する携帯電話に優先的に通報することができる。この通報は、例えばメール送信及び映像である。通報を受けた携帯電話を所持する人は、受信したメール及び映像を見て、管轄域から警察又は消防に電話することができる。従来例では、管轄外にある携帯電話から緊急電話（１１０番、１１９番）すると（警備したい自宅が東京にあって、鹿児島から電話する場合など）、電話受信署が一旦受けて、管轄署に連絡して、管轄署から折り返し電話をするので、通報が遅れるという、一刻を争う局面においては問題があった。本実施の形態では、例えば警察の管轄域で監視装置１００からの通報を受け、通報を受けた携帯電話を所持する人が、その管轄域内で警察に通報するので、迅速に通報することができる。

[0069] 特に、警察の管轄域は、都道府県単位であり、消防の管轄域は警察よりも管轄域が細かい。すなわち、警察と消防とでは、広狭を含め管轄域が異なっている。本実施の形態では、不審者侵入・接近か火災かによって、管轄域を異ならせることができる。

[0070] また、管轄域の境界の近くでは位置検出を誤ることがあり得るので、管轄域の境界から所定距離以上離れた内部に存在する通信端末装置がある場合に、更に優先して該通信端末装置に通報することによって、より確実に管轄域内にある携帯電話から迅速に緊急通報を行うことができる。

[0071] また、本実施の形態のデジタルセキュリティー・ネットワークシステムによれば、既存の公衆回線である電話回線１３０を介して、携帯電話等の汎用の通信端末装置をデジタルセキュリティー・ネットワークシステムの端末装置として利用することができるため、デジタルセキュリティー・ネットワークシステム専用の端末装置が必要なくなり、デジタルセキュリティー・ネットワークシステムの導入コストを低く抑えることができる。

[0072] また、本実施の形態のデジタルセキュリティー・ネットワークシステムによれば、公衆回線を利用しても、通報の確認ができるため、デジタルセキュリティー・ネットワークシステムの安全性を高めることができる。

[0073] 以上の説明は本発明の好適な実施の形態の例証であり、本発明の範囲はこ

れに限定されることはない。例えば、本実施の形態では、公衆回線として電話回線１２０を使用する場合について説明したが、本発明はこの場合に限定されるものではなく、例えば公衆回線として無線通信回線、インターネット又はＬＡＮ等を使用してもよい。また、この公衆回線の種類に応じて、公衆回線が無線通信の場合は通信端末装置としてトランシーバーを、公衆回線がインターネット又はＬＡＮの場合は通信端末装置としてパーソナルコンピュータ又はパームトップコンピュータを利用してもよい。このように既存の公衆回線を利用してデジタルセキュリティー・ネットワークシステムを構築することにより、デジタルセキュリティー・ネットワークシステムの利用態様を拡げることができ、かつ、デジタルセキュリティー・ネットワークシステムの構築コストを抑えることができる。

[0074] また、本実施の形態ではデジタルセキュリティー・ネットワークシステム及び方法という名称を用いたが、これは説明の便宜上であり、セキュリティシステム、防犯システム、セキュリティ方法等であってもよい。

[0075] さらに、緊急事態の検出には、公知のすべてが含まれる。例えば緊急事態には、不審者侵入・接近、火災である。なお、本実施の形態では、接近距離も通報している。また、通報は、メールに限らずどのようなものでもよい。

[0076] また、本発明のデジタルセキュリティー・ネットワークシステム及び方法は、コンピュータを本デジタルセキュリティー・ネットワークシステム又は方法として機能させるためのプログラムでも実現される。このプログラムは、コンピュータで読み取り可能な記録媒体に格納されていてもよい。

[0077] このプログラムを記録した記録媒体は、本デジタルセキュリティー・ネットワークシステムのＲＯＭそのものであってもよいし、また、外部記憶装置としてＣＤ－ＲＯＭドライブ等のプログラム読取装置が設けられ、そこに記録媒体を挿入することで読み取り可能なＣＤ－ＲＯＭ等であってもよい。

また、上記記録媒体は、磁気テープ、カセットテープ、フレキシブルディスク、ハードディスク、ＭＯ／ＭＤ／ＤＶＤ等、又は半導体メモリであってもよい。

[0078] 本明細書で引用したすべての刊行物、特許及び特許出願は、そのまま参考として、ここにとり入れるものとする。

産業上の利用可能性

[0079] 本発明に係るデジタルセキュリティー・ネットワークシステム及び方法は、ホームセキュリティ・ネットワークシステム及び法人・商業施設、事務所等、リアルタイムで対応し、財産、生命と経済損失を未然に防止して利用効果は大きい。

符号の説明

[0080] １００　監視装置
１０１　制御部
１０１ａ　位置情報取得部
１０１ｂ　管轄域保持部
１０２　入出力部
１０３　警報発信部
１１０　入出力装置
１１０Ｃ　インターホン
１１１　人感センサ
１１２　ＲＦＩＤリーダ
１１３　動画カメラ
１１４　ライト
１１５　スピーカ
１１６　開閉センサ
１１７　火災報知器
１１８　撃退装置
１１９　消火装置
１２０　通信端末装置
１２１　ＧＰＳ機能部
１３０　電話回線

１４０　警備会社

請求の範囲

［請求項1］ 複数の通信端末装置の存在位置を検出し、前記通信端末装置の位置情報を取得する位置情報取得手段と、

警備対象建物が存在する、緊急通報用電話を受信する管轄域を保持する管轄域保持手段と、

緊急事態を検出する緊急事態検出手段と、

前記緊急事態検出手段が緊急事態を検出したことに応じて、前記管轄域保持手段を参照して、複数の前記通信端末装置のいずれかが前記管轄域に存在する場合に、該管轄域に存在する前記通信端末装置に優先的に通報する制御手段と

を備えることを特徴とするデジタルセキュリティー・ネットワークシステム。

［請求項2］ 前記通報する手段がメール送信及び映像送信であることを特徴とする請求項１記載のデジタルセキュリティー・ネットワークシステム。

［請求項3］ 前記管轄域保持手段は、警察の管轄域及び消防の管轄域の両方の管轄域を保持し、前記制御手段は、前記緊急事態が警察に関することである場合には警察の管轄域を参照し、前記緊急事態が消防に関することである場合には消防の管轄域を参照することを特徴とする請求項１又は２記載のデジタルセキュリティー・ネットワークシステム。

［請求項4］ 前記制御手段は、前記管轄域の境界から所定距離以上離れた内部に存在する前記通信端末装置がある場合に、更に優先して該通信端末装置に通報することを特徴とする請求項１乃至３いずれかに記載のデジタルセキュリティー・ネットワークシステム。

［請求項5］ 複数の通信端末装置の存在位置を検出し、前記通信端末装置の位置情報を取得するステップと、

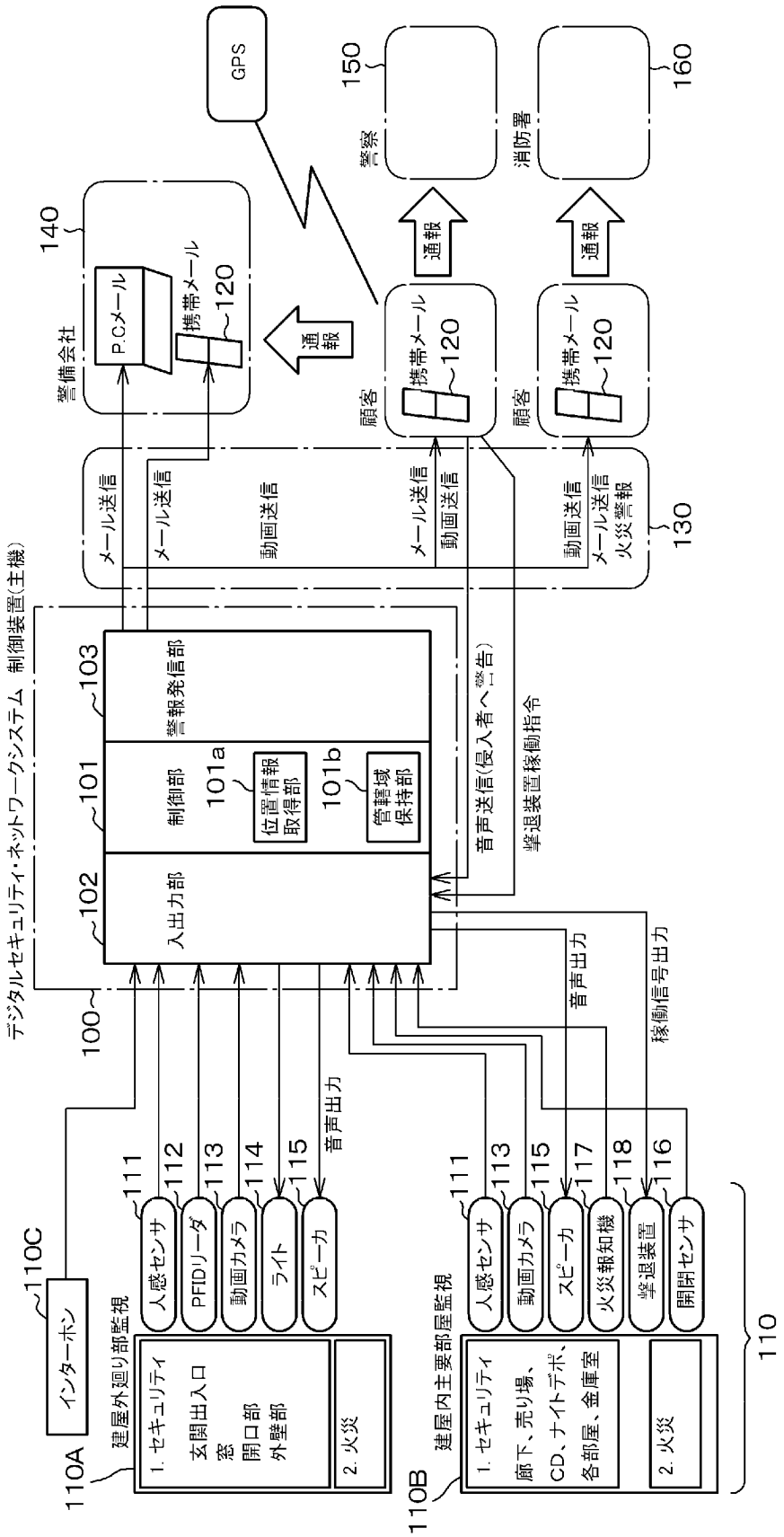
警備対象建物が存在する、緊急通報用電話を受信する管轄域を保持するステップと、

緊急事態を検出するステップと、

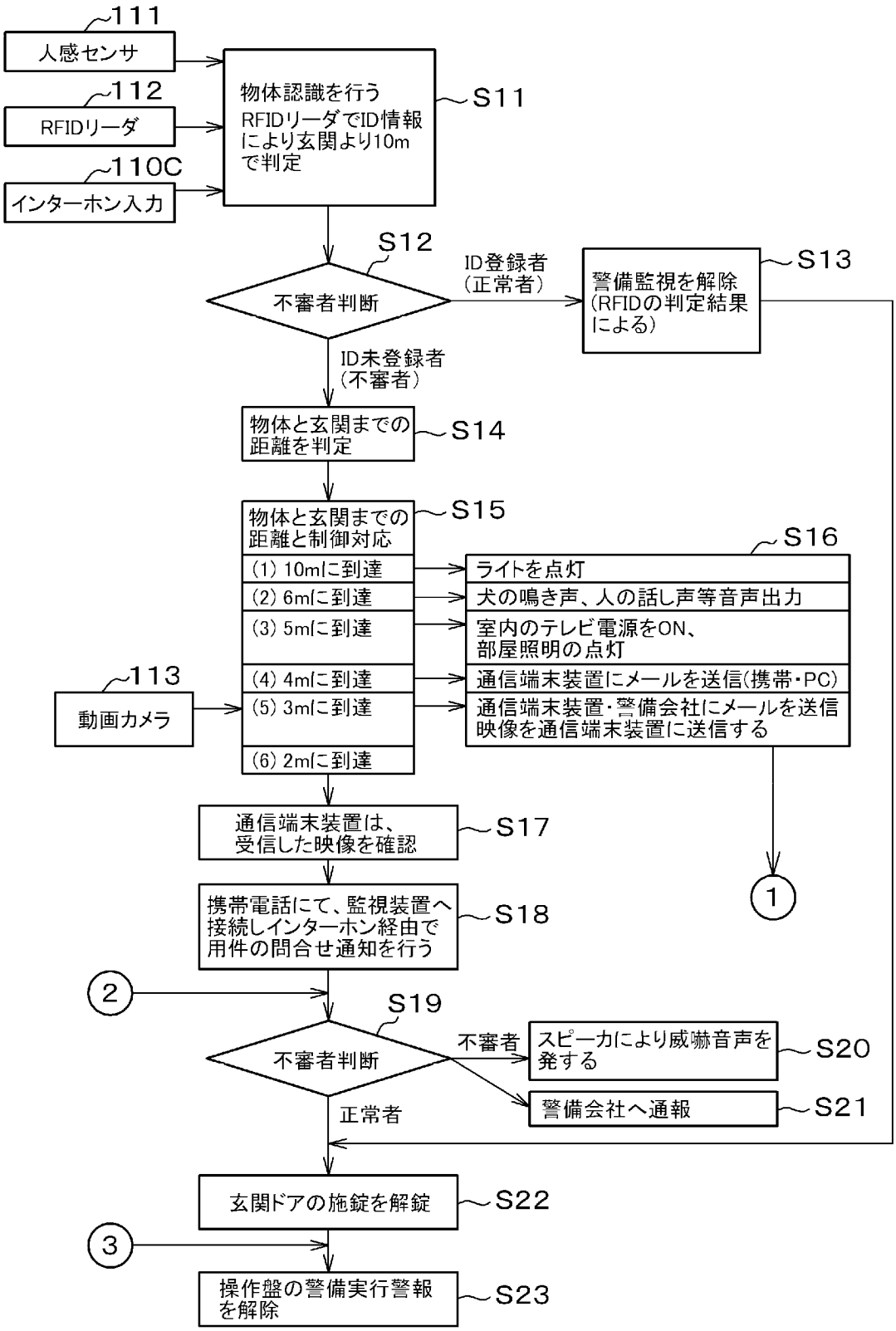
緊急事態を検出したことに応じて、複数の前記通信端末装置のいずれかが前記管轄域に存在する場合に、該管轄域に存在する前記通信端末装置に優先的に通報するステップと

を備えることを特徴とするデジタルセキュリティー・ネットワーク方法。

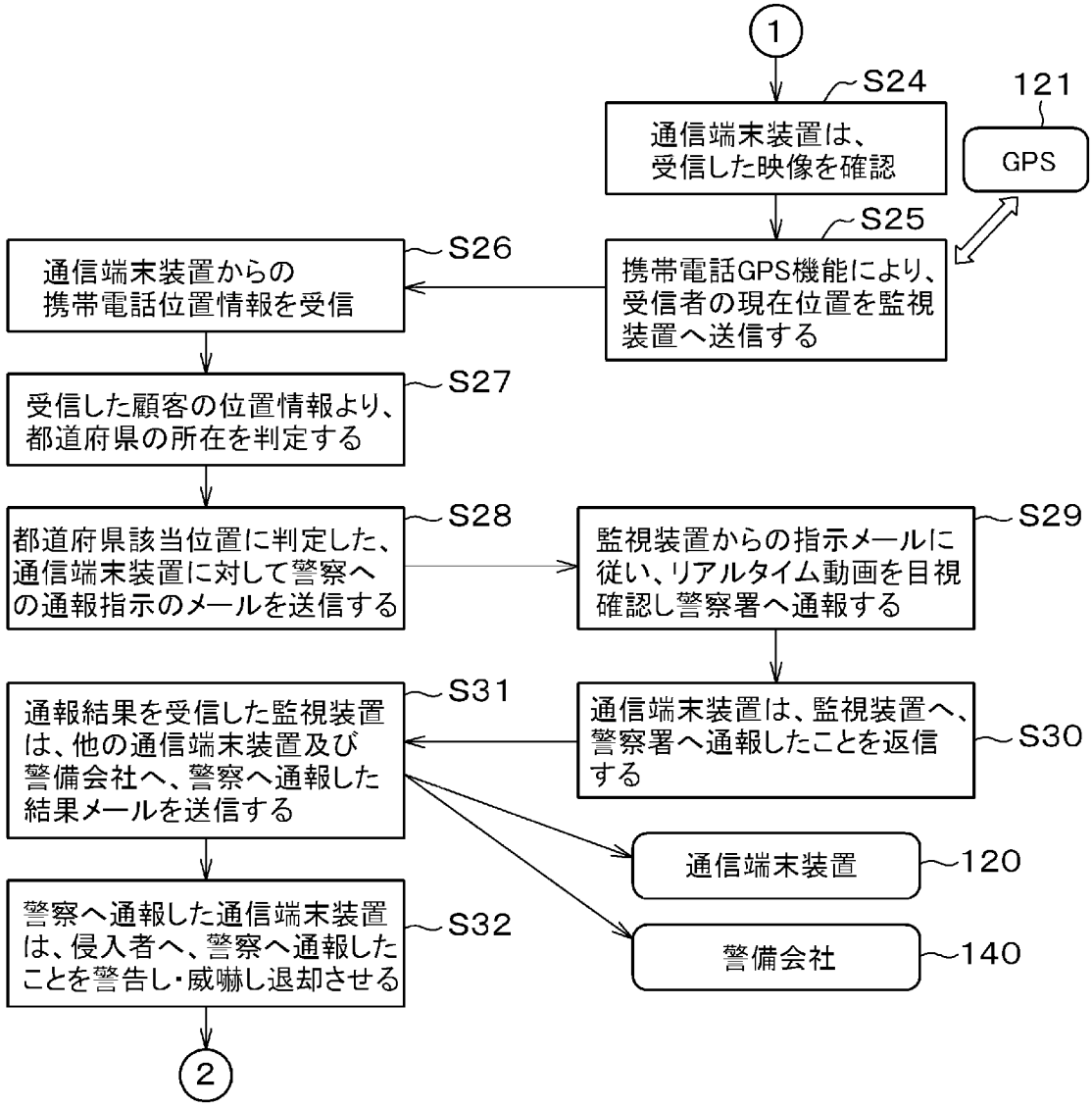
[図1]


デジタルセキュリティ・ネットワークシステム 制御装置(主機)
100
101
制御部
101a
位置情報取得部
101b
管轄域保持部
102
入出力部
103
警報発信部
110
110A
建屋外廻り部監視
1. セキュリティ
玄関出入口
窓
開口部
外壁部
2. 火災
110B
建屋内主要部屋監視
1. セキュリティ
廊下、売り場、
CD、ナイトデポ、
各部屋、金庫室
2. 火災
110C
インターホン
111
人感センサ
112
PFIDリーダ
113
動画カメラ
114
ライト
115
スピーカ
116
開閉センサ
117
スピーカ
118
火災報知機
音声出力
稼働信号出力
音声送信(侵入者へ警告)
撃退装置稼働指令
130
メール送信
メール送信
動画送信
メール送信
動画送信
動画送信
メール送信
火災警報
140
警備会社
P.Cメール
携帯メール
120
通報
GPS
150
警察
通報
160
消防署
通報
顧客
携帯メール
120
顧客
携帯メール
120

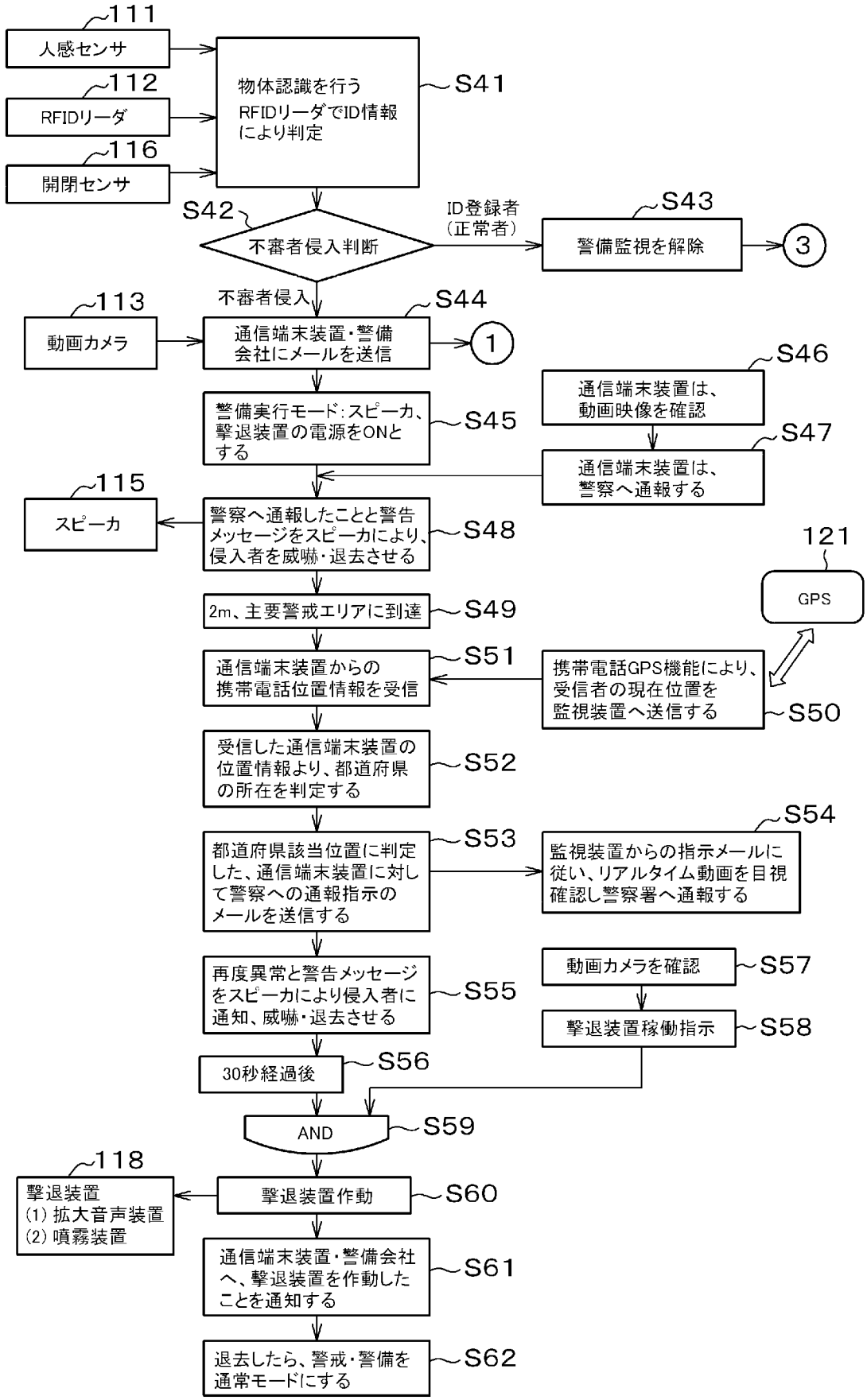
[図2]


111
人感センサ
112
RFIDリーダ
110C
インターホン入力
物体認識を行う
RFIDリーダでID情報により玄関より10mで判定
S11
S12
不審者判断
ID登録者（正常者）
警備監視を解除（RFIDの判定結果による）
S13
ID未登録者（不審者）
物体と玄関までの距離を判定
S14
物体と玄関までの距離と制御対応
S15
S16
(1) 10mに到達
ライトを点灯
(2) 6mに到達
犬の鳴き声、人の話し声等音声出力
(3) 5mに到達
室内のテレビ電源をON、部屋照明の点灯
(4) 4mに到達
通信端末装置にメールを送信(携帯・PC)
(5) 3mに到達
通信端末装置・警備会社にメールを送信映像を通信端末装置に送信する
(6) 2mに到達
113
動画カメラ
通信端末装置は、受信した映像を確認
S17
携帯電話にて、監視装置へ接続しインターホン経由で用件の問合せ通知を行う
S18
①
②
S19
不審者判断
不審者
スピーカにより威嚇音声を発する
S20
警備会社へ通報
S21
正常者
玄関ドアの施錠を解錠
S22
③
操作盤の警備実行警報を解除
S23

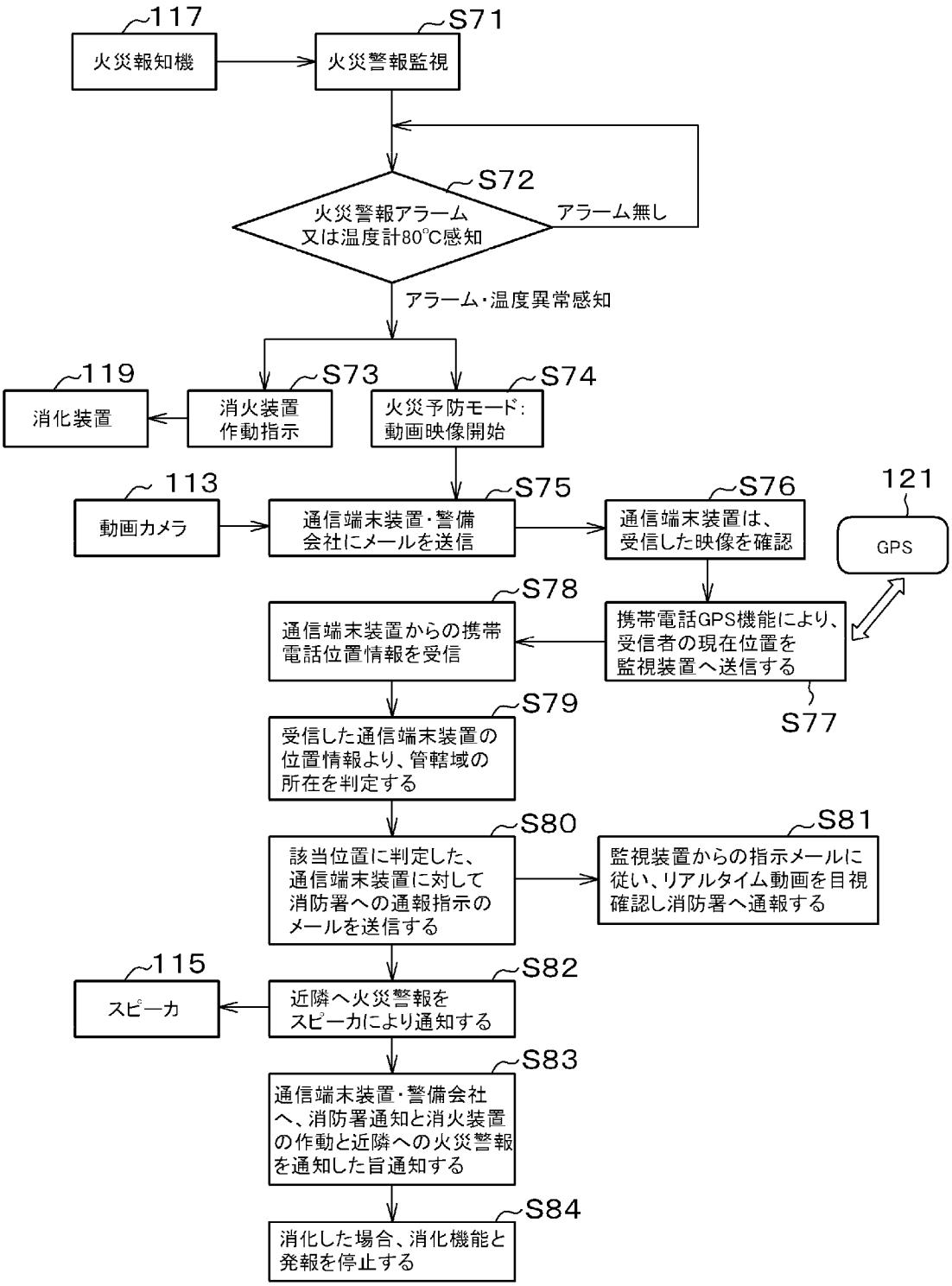
[図3]


1
S24
通信端末装置は、
受信した映像を確認
121
GPS
S25
携帯電話GPS機能により、
受信者の現在位置を監視
装置へ送信する
S26
通信端末装置からの
携帯電話位置情報を受信
S27
受信した顧客の位置情報より、
都道府県の所在を判定する
S28
都道府県該当位置に判定した、
通信端末装置に対して警察へ
の通報指示のメールを送信する
S29
監視装置からの指示メールに
従い、リアルタイム動画を目視
確認し警察署へ通報する
S30
通信端末装置は、監視装置へ、
警察署へ通報したことを返信
する
S31
通報結果を受信した監視装置
は、他の通信端末装置及び
警備会社へ、警察へ通報した
結果メールを送信する
通信端末装置
120
警備会社
140
S32
警察へ通報した通信端末装置
は、侵入者へ、警察へ通報した
ことを警告し・威嚇し退却させる
2

[図4]


111
人感センサ
112
RFIDリーダ
116
開閉センサ
物体認識を行う
RFIDリーダでID情報により判定
S41
S42
不審者侵入判断
ID登録者（正常者）
S43
警備監視を解除
3
不審者侵入
113
動画カメラ
S44
通信端末装置・警備会社にメールを送信
1
S46
通信端末装置は、動画映像を確認
警備実行モード：スピーカ、撃退装置の電源をONとする
S45
S47
通信端末装置は、警察へ通報する
115
スピーカ
警察へ通報したことと警告メッセージをスピーカにより、侵入者を威嚇・退去させる
S48
121
GPS
2m、主要警戒エリアに到達
S49
通信端末装置からの携帯電話位置情報を受信
S51
携帯電話GPS機能により、受信者の現在位置を監視装置へ送信する
S50
受信した通信端末装置の位置情報より、都道府県の所在を判定する
S52
S54
都道府県該当位置に判定した、通信端末装置に対して警察への通報指示のメールを送信する
S53
監視装置からの指示メールに従い、リアルタイム動画を目視確認し警察署へ通報する
再度異常と警告メッセージをスピーカにより侵入者に通知、威嚇・退去させる
S55
動画カメラを確認
S57
撃退装置稼働指示
S58
30秒経過後
S56
AND
S59
118
撃退装置
(1) 拡大音声装置
(2) 噴霧装置
撃退装置作動
S60
通信端末装置・警備会社へ、撃退装置を作動したことを通知する
S61
退去したら、警戒・警備を通常モードにする
S62

[図5]


117
火災報知機
S71
火災警報監視
S72
火災警報アラーム
又は温度計80℃感知
アラーム無し
アラーム・温度異常感知
119
消化装置
S73
消火装置
作動指示
S74
火災予防モード:
動画映像開始
113
動画カメラ
S75
通信端末装置・警備
会社にメールを送信
S76
通信端末装置は、
受信した映像を確認
121
GPS
S78
通信端末装置からの携帯
電話位置情報を受信
携帯電話GPS機能により、
受信者の現在位置を
監視装置へ送信する
S77
S79
受信した通信端末装置の
位置情報より、管轄域の
所在を判定する
S80
該当位置に判定した、
通信端末装置に対して
消防署への通報指示の
メールを送信する
S81
監視装置からの指示メールに
従い、リアルタイム動画を目視
確認し消防署へ通報する
115
スピーカ
S82
近隣へ火災警報を
スピーカにより通知する
S83
通信端末装置・警備会社
へ、消防署通知と消火装置
の作動と近隣への火災警報
を通知した旨通知する
S84
消化した場合、消化機能と
発報を停止する

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/067242

A. CLASSIFICATION OF SUBJECT MATTER
G08B25/10(2006.01)i, *G08B25/00*(2006.01)i, *G08B25/08*(2006.01)i

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)
G08B25/10, G08B25/00, G08B25/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

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.
A	JP 2011-228919 A (Kabushiki Kaisha Guard I), 10 November 2011 (10.11.2011), paragraph [0022] (Family: none)	1-5
A	JP 2004-265191 A (NEC Access Technica, Ltd.), 24 September 2004 (24.09.2004), entire text; all drawings (Family: none)	1-5
A	JP 2001-36645 A (Toyo Communication Equipment Co., Ltd.), 09 February 2001 (09.02.2001), paragraph [0016] (Family: none)	1-5

☒ 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
03 August, 2012 (03.08.12)	21 August, 2012 (21.08.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/067242

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-152867 A (NEC Corp.), 23 May 2003 (23.05.2003), entire text; all drawings (Family: none)	1-5

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０６７２４２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G08B25/10(2006.01)i, G08B25/00(2006.01)i, G08B25/08(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G08B25/10, G08B25/00, G08B25/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2011-228919 A（株式会社ガードアイ）2011.11.10,　【００２２】（ファミリーなし）	１－５
A	JP 2004-265191 A（ＮＥＣアクセステクニカ株式会社）2004.09.24,　全文全図（ファミリーなし）	１－５
A	JP 2001-36645 A（東洋通信機株式会社）2001.02.09,　【００１６】（ファミリーなし）	１－５

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０３．０８．２０１２	国際調査報告の発送日 ２１．０８．２０１２
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　３Ｇ　９４３０ 神山　茂樹 電話番号　０３－３５８１－１１０１　内線　３３５５

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Ａ	JP 2003-152867 A（日本電気株式会社）2003.05.23，全文全図（ファミリーなし）	１－５