(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-75057
(P2014-75057A)
(43)公開日　平成26年4月24日(2014.4.24)

(51)Int.Cl.		F I			テーマコード（参考）
G08B 25/04	(2006.01)	G08B	25/04	E	5C084
G08B 25/10	(2006.01)	G08B	25/10	D	5C087
G08B 25/00	(2006.01)	G08B	25/00	520C	5K201
G08B 27/00	(2006.01)	G08B	27/00	A	
G08B 13/196	(2006.01)	G08B	13/196		

審査請求 未請求　請求項の数 18　ＯＬ　（全 27 頁）　最終頁に続く

(21)出願番号　特願2012-222559 (P2012-222559)
(22)出願日　平成24年10月4日 (2012.10.4)

（特許庁注：以下のものは登録商標）
１．ＨＤＭＩ

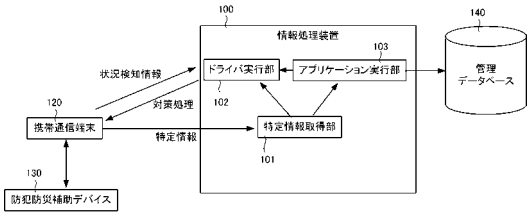
(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100134430
弁理士　加藤　卓士
(72)発明者　小林　佳和
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5C084 AA02 AA07 AA09 CC38 DD11 EE01 HH02 HH17
5C087 AA02 AA03 AA19 BB20 DD04 DD05 FF01 FF04 FF23 GG02 GG57 GG66 GG68 GG82 GG83 GG84

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理装置、情報処理方法、情報処理プログラム、携帯通信端末、その制御方法およびその制御プログラム

(57)【要約】
【課題】簡易かつ効果的に防犯、防災対策を講じること。
【解決手段】防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得手段と、前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行手段と、前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行手段と、を備えた情報処理装置を提供する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得手段と、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行手段と、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行手段と、
を備えた情報処理装置。
【請求項２】
前記防犯防災補助デバイスは、防犯ライト、スピーカ、防犯カメラ、ドアの開閉センサのいずれか少なくとも一つを含む、請求項１に記載の情報処理装置。
【請求項３】
前記アプリケーション実行手段は、前記携帯通信端末から、防犯時における、前記携帯通信端末の時刻情報を取得し、前記状況検知情報と共に前記管理データベースに蓄積する、請求項１または２に記載の情報処理装置。
【請求項４】
前記携帯通信端末は、前記防犯防災補助デバイスとしてのカメラおよびスピーカに接続され、
前記アプリケーション実行手段は、前記カメラの撮影画像中に不審者を発見した場合には、前記スピーカから威嚇音声を出力するように前記スピーカを制御する、請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記携帯通信端末は、前記防犯防災補助デバイスとしてのカメラおよびスピーカに接続され、
前記アプリケーション実行手段は、前記カメラの撮影画像中に不審者を発見した場合には、前記スピーカから指示メッセージを出力し、さらに、その指示メッセージに前記不審者が従わない場合に、店員待避を促す誘導音声を出力し、さらには威嚇音声を出力するように前記スピーカを制御する、請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項６】
前記携帯通信端末は、前記防犯防災補助デバイスとしてのカメラおよび釣銭引出に接続され、
前記アプリケーション実行手段は、前記カメラの撮影画像中に不審者を発見した場合には、前記釣銭引出を閉じて鍵をかける請求項１乃至５のいずれか１項に記載の情報処理装置。
【請求項７】
前記携帯通信端末は、前記防犯防災補助デバイスとしてのカメラおよびピッチングマシンに接続され、
前記アプリケーション実行手段は、前記カメラの撮影画像中に不審者を発見した場合には、不審者を追従するように前記カメラを制御し、前記ピッチングマシンを制御して前記不審者に向けてカラーボールを投射する請求項１乃至６のいずれか１項に記載の情報処理装置。
【請求項８】
前記携帯通信端末は、前記防犯防災補助デバイスとしてのディスプレイに接続され、
前記アプリケーション実行手段はさらに、前記防犯防災補助デバイスからの状況検知情報に基づいて、火災を検知した場合、前記ディスプレイに避難用メッセージを表示するよ

うに制御する、請求項１乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
前記アプリケーション実行手段は、前記防犯防災補助デバイスとしてのカメラが撮影した画像から、火災に伴って有害ガスが出ていると判断した場合には、前記ディスプレイに対し、袋で床の方の空気をいれて、それを吸いながら床をはって逃げるように避難用メッセージを表示するよう制御する、請求項８に記載の情報処理装置。
【請求項１０】
前記携帯通信端末は、前記防犯防災補助デバイスとして、スピーカ、店内の客の有無を検出する人感センサおよび前記店の扉を開閉するための開閉装置に接続され、
前記アプリケーション実行手段は、前記人感センサで店内に客がいると判断した場合には、不審者を追い出すべく威嚇音声を前記スピーカから出力し、前記人感センサで店内に客がいないと判断した場合には、前記開閉装置を用いて前記店の扉を閉じて施錠する、請求項１乃至９のいずれか１項に記載の情報処理装置。
【請求項１１】
前記アプリケーション実行手段は、防犯対策の効果を携帯通信端末に前記防犯防災補助デバイスが接続されたことを検知すると、前記防犯防災補助デバイスをどの位置にどのように設置すべきかを説明するメッセージを前記携帯通信端末に対して送信する、請求項１乃至１０のいずれか１項に記載の情報処理装置。
【請求項１２】
前記アプリケーション実行手段は、防犯対策効果計測者データベースに誰が防犯対策の効果を申告したかを属性として蓄積し、問題予防に利用する請求項１乃至１１のいずれか１項に記載の情報処理装置。
【請求項１３】
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得ステップと、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行ステップと、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行ステップと、
を含む情報処理方法。
【請求項１４】
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得ステップと、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行ステップと、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行ステップと、
をコンピュータに実行させる情報処理プログラム。
【請求項１５】
防犯防災補助デバイスに接続された場合に、自端末が該防犯防災補助デバイスを制御できるか否かを判定する判定手段と、
自端末が前記防犯防災補助デバイスを制御できないと判定した場合に、サーバにアクセ

スし、前記防犯防災補助デバイスの制御をリクエストする要求手段と、
前記防犯防災補助デバイスと前記サーバとの間の通信が確立して前記サーバが前記防犯防災補助デバイスから、前記防犯防災補助デバイスが検知した状況検知情報を取得できるように、前記防犯防災補助デバイスと前記サーバとの間の信号転送を制御する信号転送制御手段と、
前記サーバが前記防犯防災補助デバイスに対応する防犯防災アプリケーションプログラムを実行することにより生成された画面情報を前記サーバから受信する受信手段と、
を備えた携帯通信端末。
【請求項１６】
防犯防災補助デバイスに接続された場合に、自端末が該防犯防災補助デバイスを制御できるか否かを判定する判定ステップと、
自端末が前記防犯防災補助デバイスを制御できないと判定した場合に、サーバにアクセスし、前記防犯防災補助デバイスの制御をリクエストする要求ステップと、
前記防犯防災補助デバイスと前記サーバとの間の通信が確立して前記サーバが前記防犯防災補助デバイスから、前記防犯防災補助デバイスが検知した状況検知情報を取得できるように、前記防犯防災補助デバイスと前記サーバとの間の信号転送を制御する信号転送制御ステップと、
前記サーバが前記防犯防災補助デバイスに対応する防犯防災アプリケーションプログラムを実行することにより生成された画面情報を前記サーバから受信する受信ステップと、
を含む携帯通信端末の制御方法。
【請求項１７】
防犯防災補助デバイスに接続された場合に、自端末が該防犯防災補助デバイスを制御できるか否かを判定する判定ステップと、
自端末が前記防犯防災補助デバイスを制御できないと判定した場合に、サーバにアクセスし、前記防犯防災補助デバイスの制御をリクエストする要求ステップと、
前記防犯防災補助デバイスと前記サーバとの間の通信が確立して前記サーバが前記防犯防災補助デバイスから、前記防犯防災補助デバイスが検知した状況検知情報を取得できるように、前記防犯防災補助デバイスと前記サーバとの間の信号転送を制御する信号転送制御ステップと、
前記サーバが前記防犯防災補助デバイスに対応する防犯防災アプリケーションプログラムを実行することにより生成された画面情報を前記サーバから受信する受信ステップと、
をコンピュータに実行させる携帯通信端末の制御プログラム。
【請求項１８】
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得手段と、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行手段と、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行手段と、
を備えた情報処理装置と、
前記携帯通信端末と、
を含む情報処理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、防犯防災技術に関する。

【背景技術】
【０００２】
上記技術分野において、特許文献１の段落００２４、００２７、００２９に、監視装置は、観測部、対処部、監視計画実行部、一般監視知識記憶部より構成されていることが開示されている。ここで、監視計画実行部は、観測部を用いて監視対象の異常を検査し、異常検知時には最適な対処行動を決定し、対処行動を実行するよう対処部に指令する。また、一般監視知識記憶部は、監視対象のクラスごとに、監視態勢プロシージャ、異常検知プロシージャ、対処行動プロシージャを記憶している。
【０００３】
また、特許文献２には、その段落００４０、００４９に、ホストサーバー上では、仮想ＰＣソフトが起動しており、ホストサーバーは、グリッドコンピューティング技術により複数のＰＣで構築してもよい、と記載されている。また、段落００６０には、クライアント端末のハードウェアリソースは仮想ＰＣから利用できるように設定を行なう、と記載されている。
【０００４】
特許文献３の段落００１７には、シンクライアントシステムは、シンクライアント、シンクライアントのＵＳＢポートに接続されるＵＳＢデバイス、ネットワークを介して接続されたサーバからなり、シンクライアントは携帯通信端末が好例である、との記載がある。また、段落００２９には、ＵＳＢ仮想バスドライバは、サーバＯＳ部から見て、サーバ自身が備えるＵＳＢバスであるかのように振る舞うドライバである、と記載されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００３－２９６８５５号公報
【特許文献２】特開２００７－１９３４２９号公報
【特許文献３】特開２０１０－２１８３４７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記文献に記載の技術では、十分な記憶容量や処理能力を持つＰＣを店舗に持ち込まなければ、防犯システムを構成することができなかった。特に仮店舗や仮設住宅などで簡易的に導入できるものではなかった。
本発明の目的は、上述の課題を解決する技術を提供することにある。
【課題を解決するための手段】
【０００７】
上記目的を達成するため、本発明に係る情報処理装置は、
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得手段と、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行手段と、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行手段と、
を備えた。
【０００８】
上記目的を達成するため、本発明に係る情報処理方法は、
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デ

バイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得ステップと、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行ステップと、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行ステップと、
を含む。

【０００９】
上記目的を達成するため、本発明に係るプログラムは、
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得ステップと、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行ステップと、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行ステップと、
をコンピュータに実行させる。

【００１０】
上記目的を達成するため、本発明に係る携帯通信端末は、
防犯防災補助デバイスに接続された場合に、自端末が該防犯防災補助デバイスを制御できるか否かを判定する判定手段と、
自端末が前記防犯防災補助デバイスを制御できないと判定した場合に、サーバにアクセスし、前記防犯防災補助デバイスの制御をリクエストする要求手段と、
前記防犯防災補助デバイスと前記サーバとの間の通信が確立して前記サーバが前記防犯防災補助デバイスから、前記防犯防災補助デバイスが検知した状況検知情報を取得できるように、前記防犯防災補助デバイスと前記サーバとの間の信号転送を制御する信号転送制御手段と、
前記サーバが前記防犯防災補助デバイスに対応する防犯防災アプリケーションプログラムを実行することにより生成された画面情報を前記サーバから受信する受信手段と、
を備えた。

【００１１】
上記目的を達成するため、本発明に係る携帯通信端末の制御方法は、
防犯防災補助デバイスに接続された場合に、自端末が該防犯防災補助デバイスを制御できるか否かを判定する判定ステップと、
自端末が前記防犯防災補助デバイスを制御できないと判定した場合に、サーバにアクセスし、前記防犯防災補助デバイスの制御をリクエストする要求ステップと、
前記防犯防災補助デバイスと前記サーバとの間の通信が確立して前記サーバが前記防犯防災補助デバイスから、前記防犯防災補助デバイスが検知した状況検知情報を取得できるように、前記防犯防災補助デバイスと前記サーバとの間の信号転送を制御する信号転送制御ステップと、
前記サーバが前記防犯防災補助デバイスに対応する防犯防災アプリケーションプログラムを実行することにより生成された画面情報を前記サーバから受信する受信ステップと、
を含む。

【００１２】

上記目的を達成するため、本発明に係る携帯通信端末の制御プログラムは、
防犯防災補助デバイスに接続された場合に、自端末が該防犯防災補助デバイスを制御できるか否かを判定する判定ステップと、
自端末が前記防犯防災補助デバイスを制御できないと判定した場合に、サーバにアクセスし、前記防犯防災補助デバイスの制御をリクエストする要求ステップと、
前記防犯防災補助デバイスと前記サーバとの間の通信が確立して前記サーバが前記防犯防災補助デバイスから、前記防犯防災補助デバイスが検知した状況検知情報を取得できるように、前記防犯防災補助デバイスと前記サーバとの間の信号転送を制御する信号転送制御ステップと、
前記サーバが前記防犯防災補助デバイスに対応する防犯防災アプリケーションプログラムを実行することにより生成された画面情報を前記サーバから受信する受信ステップと、
をコンピュータに実行させる。

【００１３】

上記目的を達成するため、本発明に係るシステムは、
防犯防災補助デバイスが携帯通信端末に対して接続された場合に、前記防犯防災補助デバイスから、前記携帯通信端末を介して、前記防犯防災補助デバイスを特定する特定情報を取得する取得手段と、
前記特定情報に応じたドライバプログラムを実行して、前記防犯防災補助デバイスを制御するドライバ実行手段と、
前記特定情報に応じた防犯防災アプリケーションプログラムを実行して、前記携帯通信端末に接続された前記防犯防災補助デバイスが検知した状況検知情報を取得すると共に、取得した前記状況検知情報に対応する対策処理を、管理データベースを参照して特定し、前記携帯通信端末を介して、前記対策処理に基づいて前記防犯防災補助デバイスを制御するアプリケーション実行手段と、
を備えた情報処理装置と、
前記携帯通信端末と、
を含む。

【発明の効果】

【００１４】

本発明によれば、簡易かつ効果的に防犯、防災対策を講じることができる。

【図面の簡単な説明】

【００１５】

【図１】本発明の第１実施形態に係る情報処理装置の構成を示すブロック図である。
【図２Ａ】本発明の第２実施形態に係るクラウドサーバの利用方法を示す図である。
【図２Ｂ】本発明の第２実施形態に係るクラウドサーバの利用方法を示す図である。
【図２Ｃ】本発明の第２実施形態に係るクラウドサーバの利用方法を示す図である。
【図３】本発明の第２実施形態に係るクラウドサーバと共に用いられる防犯防災補助デバイスについて説明する図である。
【図４】本発明の第２実施形態に係るクラウドサーバの機能構成を示すブロック図である。
【図５】本発明の第２実施形態に係るスマートデバイスの機能構成を示すブロック図である。
【図６】本発明の第２実施形態に係るクラウドサーバを含むシステムの全体的な処理の流れを示すシーケンス図である。
【図７Ａ】本発明の第２実施形態に係るクラウドサーバで行なわれる処理の流れを示すフローチャートである。
【図７Ｂ】本発明の第２実施形態に係る情報処理システムでのパケット送受信処理の例を示す図である。
【図７Ｃ】本発明の第２実施形態に係る情報処理システムでのパケット送受信処理の他の例を示す図である。

【図７Ｄ】本発明の第２実施形態に係る情報処理システムでのパケット送受信処理のさらに他の例を示す図である。
【図７Ｅ】本発明の第２実施形態に係る情報処理システムで用いられるデバイスデータベースの構成を示す図である。
【図８Ａ】本発明の第２実施形態に係る情報処理システムでのサーバとデバイス間での通信確立処理の一例を示す図である。
【図８Ｂ】本発明の第２実施形態に係る情報処理システムでのサーバとデバイス間での通信確立処理の一例を示す図である。
【図８Ｃ】本発明の第２実施形態に係る情報処理システムでのサーバとデバイス間での通信確立処理の一例を示す図である。
【図８Ｄ】本発明の第２実施形態に係る情報処理システムでのサーバとデバイス間での通信確立処理の一例を示す図である。
【図９Ａ】本発明の第２実施形態においてスマートデバイスに表示される表示画面例を示す図である。
【図９Ｂ】本発明の第２実施形態においてスマートデバイスに表示される表示画面例を示す図である。
【図１０】本発明の第２実施形態に係る情報処理システムで用いられるデバイスデータベースの構成を示す図である。
【図１１】本発明の第２実施形態に係る情報処理システムで用いられる推奨防犯防災システムデータベースの構成を示す図である。
【図１２】本発明の第２実施形態に係る情報処理システムで用いられる防犯防災対策データベースの構成を示す図である。
【発明を実施するための形態】
【００１６】
以下に、図面を参照して、本発明の実施の形態について例示的に詳しく説明する。ただし、以下の実施の形態に記載されている構成要素はあくまで例示であり、本発明の技術範囲をそれらのみに限定する趣旨のものではない。
【００１７】
［第１実施形態］
本発明の第１実施形態としての情報処理装置１００について、図１を用いて説明する。情報処理装置１００は、特定情報取得部１０１と、ドライバ実行部１０２と、アプリケーション実行部１０３とを含む。
【００１８】
特定情報取得部１０１は、防犯防災補助デバイス１３０が携帯通信端末１２０に対して接続された場合に、防犯防災補助デバイス１３０から、携帯通信端末１２０を介して、防犯防災補助デバイス１３０を特定する特定情報を取得する。
【００１９】
ドライバ実行部１０２は、特定情報に応じたドライバプログラムを実行して、防犯防災補助デバイス１３０を制御する。さらに、アプリケーション実行部１０３は、特定情報に応じた防犯防災アプリケーションプログラムを実行して、携帯通信端末１２０に接続された防犯防災補助デバイス１３０が検知した状況検知情報を取得する。また、アプリケーション実行部１０３は、取得した状況検知情報に対応する対策処理を、管理データベース１４０を参照して特定し、携帯通信端末１２０を介して、対策処理に基づいて防犯防災補助デバイス１３０を制御する。
【００２０】
本実施形態によれば、携帯通信端末に接続された防犯防災デバイスを情報処理端末が、携帯通信端末にドライバやアプリケーションをダウンロードせずに制御でき、簡易かつ効果的に防犯、防災対策を講じることができる。
【００２１】
［第２実施形態］

本発明の第２実施形態に係る情報処理装置としてのクラウドサーバ２００について、図２乃至図１２を用いて説明する。

【００２２】

（全体構成）

図２Ａ、図２Ｂ、図２Ｃは、本実施形態に係るクラウドサーバ２００を含む情報処理システムの一種としての防犯防災システムの利用シーンを説明するための図である。

【００２３】

この防犯防災システムは、ネットワークに用意されたクラウドサーバ２００と、クラウドサーバ２００に対して無線通信ネットワークを介して通信可能な携帯通信端末としてのスマートデバイス２５０とを含む。スマートデバイス２５０は、防犯防災補助デバイスとしての、スピーカ２２１、カメラ２２２、人感センサ２２３、防犯ライト２２４、扉開閉センサ２２５、カラーボール自動ピッチングマシン２２６、接点制御装置（図３）などと接続されている。また、スマートデバイス２５０は、店舗内に設置されるＰＯＳ（Point of sale）端末２７０などとも接続されている。ここでは防犯防災補助デバイスをクラウドサーバ２００に中継接続するための携帯通信端末として、画面やマイクやカメラなどを備えたスマートデバイス２５０を例に挙げて説明しているが、本願発明はこれに限定されるものではない。例えばモバイルルータなど、通信機能をシンプルに備えた装置でもよい。

【００２４】

スピーカ２２１は、防犯音（威嚇音声）を出力するために用いられる。また、カメラ２２２は、不審者の侵入や火災の発生などを検知するほか、店内の客の性別や年齢まで判断するのに用いることができる。人感センサ２２３は、人の存在、その人数を感知する。防犯ライト２２４は、蓄積した電気で威圧的な明るさで周囲を照らすものである。また、扉開閉センサ２２５は、ドアの開け閉めや異常な振動（破壊での侵入による振動）を検知する。さらに、接点制御装置は、各種ドアやＰＯＳ端末２７０のロックや開閉、機器の電源ｏｎ／ｏｆｆ制御を行なう。カラーボール自動ピッチングマシン２２６は、逃亡する犯人に対してカラーボールをぶつけるための機械である。カラーボールとは、中に特殊染料が入った防犯用のボールである。スマートデバイス２５０は、その他にも、火災センサ（熱センサまたは煙センサ）、振動センサ、サイネージパネルなどと接続されてもよい。これらの防犯防災補助デバイスは、図３に示すようにＵＳＢハブ３０１を介して有線または無線で、スマートデバイス２５０に接続される。

【００２５】

クラウドサーバ２００は、防犯防災補助デバイスがユーザのスマートデバイス２５０に接続されたことを検知すると、それらのデバイスをどの位置にどのように設置すべきかをスマートデバイス２５０に対して送信する。これにより、ユーザは、専門的な知識がなくても、店舗の状況に応じた防犯防災体制を整えることが可能となる。また、来場の客層や、地域の犯罪履歴（高齢者への引ったくりが多い等の分析）にあわせて、防犯カメラを増やして来客者の安全を守るように、装置の組合せ提案をしてもよい。

【００２６】

ここでは、スマートデバイス２５０は、ＵＳＢ（Universal Serial Bus）インタフェースを介して、防犯防災補助デバイスと接続されている。また、しかし、本発明はこれに限定されるものではなく、他の通信インタフェース（例えばＩＥＥＥ１３９４、ＨＤＭＩ、Bluetooth（登録商標）、Wi-Fi（登録商標）など）で通信可能に接続されてもよい。

【００２７】

クラウドサーバ２００は、スマートデバイス２５０に接続された防犯防災補助デバイスを特定し、その防犯防災補助デバイスに合ったドライバプログラム２０２および防犯防災アプリケーションプログラム２０４を実行する。これにより、スマートデバイス２５０は、防犯防災補助デバイスを用いた監視体制に入る。クラウドサーバ２００は、ドライバプログラム２０２の実行により、防犯防災補助デバイスから状況検知情報を取得する。状況変化としては、不審者の侵入や火災の発生、ドアの開閉や異常振動などが挙げられる。取

得した状況検知情報に対応する対策処理を、管理データベース２１０を参照して特定する。そして、スマートデバイス２５０を介して、対策処理に基づいて防犯防災補助デバイスを制御する。

【００２８】

具体的には、図２Ｂに示すように、例えば、カメラ２２２で撮影した画像から、パターンマッチング等の画像処理技術を用いてヘルメット着用の不審者２９０を検知した場合、まずはヘルメットを脱ぐように指示する指示メッセージを、スピーカ２２１から流す。さらに、不審者２９０が一定時間ヘルメットを脱がない場合、次に、店員待避を促す（不審者から距離を置く）誘導音声をスピーカ２２１から流し、さらには威嚇音声をスピーカ２２１から流す。同時に、ＰＯＳ端末２７０の釣銭引出を閉じて鍵をかける。管理データベース２１０には、検知内容と、出力メッセージとの対応関係があらかじめ登録されており、防犯防災アプリケーションプログラム２０４が、管理データベース２１０を参照して対策処理を決定し、防犯防災補助デバイスを制御する。また、不審者２９０を追従するようにカメラ２２２を制御する。ＰＯＳ端末２７０の釣銭引出が開けられるなど、不審者２９０による犯罪行為を検出した場合には、入り口付近に設置したカラーボール自動ピッチングマシン２２６を動作させる。例えば、店舗から出た瞬間に、画像認識と連動させて、逃げようとする不審者にカラーボールを投射する。

【００２９】

防犯防災アプリケーションプログラム２０４は、店舗内の客層に応じて、対策処理を変更してもよい。例えば、カメラ２２２で撮影した画像から判断して、高齢者がいる場合や子供がいる場合には、店員に対し、ＰＯＳ端末２７０のディスプレイを介してそれらの客を優先的に誘導するように指示してもよい。

【００３０】

振動センサや接点制御装置などから検出された状況検知情報から、壁や窓を破っての店舗内への侵入があったと判断した場合には、スプリンクラーから水を出す、消火スプレーを噴射させるなどの防災時の対策処理により、侵入者をひるませる効果を狙ってもよい。一方、水をかけると火災になるような揚げ物を行なう装置が店舗内にあることが分かっている場合には、ボール型の防犯とカメラに注力することが望ましい。

【００３１】

火災センサが反応したら、図２Ｃに示すように、避難誘導のガイダンスが、スピーカ２２１から流れるようにすればよい。火災発生場所２８１を複数の火災センサの反応場所からわりだし、火災発生場所２８１から一番遠いところのドア２８２へ誘導する避難ルートをＰＯＳ端末２７０やサイネージパネル２８３を用いて案内してもよい。カメラ２２２が撮影した画像から、火災に伴って有害ガスが出ていると判断した場合には、スピーカ２２１やＰＯＳ端末２７０のディスプレイに対し、「ビニール袋で床の方の空気をいれて、それを吸いながら床をはって逃げてください」といった避難用メッセージを表示してもよい。

【００３２】

振動センサが振動を検知した場合には、その振動の大きさに応じて、店内にとどまるべきか、外に逃げられるタイミングかを、スピーカ２２１やサイネージパネルなどを通じてガイダンスしてもよい。そのガイダンスには、インターネット上の地震情報を連動させてもよい。その誘導は、スーパのような広い店舗から、コンビニのような狭い店舗、寿司屋、居酒屋、等の店舗の特性に合わせてナレッジ支援してもよい。

【００３３】

不法侵入者に対しては、外に早く威嚇してだすのか、閉じこめて捕まえやすくするのか、それを、人感センサ２２３で不法侵入者以外の客の有無と合わせて判断するようにしてもよい。つまり、客がいる場合には侵入者を追い出すべく、威嚇音声をスピーカ２２１から出力し、客がいなければ店員が待避した時点で入り口ドアを施錠して、閉じ込める。不審者に対する威嚇メッセージは、犯人の画像解析と連動して、凶器のパターンで変更してもよい。侵入者が１名で、包丁で店員を脅かそうとしているなら、「こっちにもいるよ」

と擬人音で後ろをむかせて、威嚇フラッシュで相手を目つぶしして、その間に店員が犯人から離れ、逃走等のみの安全確保をしてもよい。店舗を出ても犯人が逃亡しづらくする防犯ナレッジを提供してもよい。

【００３４】

防犯防災アプリケーションプログラム２０４は、スマートデバイス２５０に接続された駐車場のストッパを制御して、犯人が車で逃走できなくする指示を、接点制御装置から出すこともできる。また防犯防災アプリケーションプログラム２０４は、カメラ２２２で店内を撮影した画像や音声から、不審者に関する情報（性別、背丈、声の特徴）を割り出すことができる。さらに、防犯防災アプリケーションプログラム２０４は、カメラ２２２で店先を撮影した画像と、あらかじめ用意された車両データベースとの照合を行ない、逃亡者の車種、色、ナンバーを割り出すことができる。防犯防災アプリケーションプログラム２０４は、これらの犯人逮捕につながる情報を、自動的に警察の指定されたコンピュータに送信する。またその一方で、そのような情報をスマートデバイス２５０に接続された周辺機器に出力してもよい。

【００３５】

以上により、スマートデバイスに接続された防犯防災デバイスをクラウドサーバが、スマートデバイスにドライバやアプリケーションをダウンロードしなくても制御できる。したがって、店舗に用意された防犯防災補助デバイスをスマートデバイス２５０に接続するだけで、店舗内の防犯防災対策を構築できる。つまり、臨時的、または簡易的に防犯防災対策を施すことが非常に容易になる。

【００３６】

（クラウドサーバの機能構成）

図４は、クラウドサーバ２００の機能構成を示すブロック図である。クラウドサーバ２００は、ディスクリプタ受信部４０２を有する。ディスクリプタ受信部４０２は、防犯防災補助デバイスがスマートデバイス２５０に対して接続された場合に、スマートデバイス２５０を介して、防犯防災補助デバイスを特定する特定情報としてのディスクリプタを取得する。

【００３７】

デバイス判定部４０３は、ディスクリプタ受信部４０２が取得したディスクリプタを用いて、デバイスデータベース４２３（図７Ｅ参照）を検索することにより、防犯防災補助デバイスの製造元ＩＤおよび製品ＩＤを特定することができる。

【００３８】

ＵＳＢデバイスドライバ実行部４０７は、ディスクリプタに応じたドライバプログラムを実行して、防犯防災補助デバイスを制御する。複数種類のドライバプログラムが、ドライバプログラムデータベース４２４に用意されている。ドライバ選定部４０５は、デバイス判定部４０３が判定した製造元ＩＤおよび製品ＩＤを用いて、特定された防犯防災補助デバイスを駆動するのに必要なデバイスドライバをドライバプログラムデータベース４２４内から選定する。

【００３９】

ＵＳＢデバイスドライバ実行部４０７は、スマートデバイス２５０を中継して接続された防犯防災補助デバイスに対して送信すべきＵＳＢパケットを生成し、ＵＳＢパケットカプセリング部４０８に渡す。ＵＳＢパケットカプセリング部４０８は、ＵＳＢパケットをＩＰカプセリングして、スマートデバイス２５０に向けて送信する。一方、ＵＳＢパケットアンカプセリング部４０９は、ＩＰカプセリングされたデータをスマートデバイス２５０から受信して、そのデータをアンカプセリングしてＵＳＢパケットを取り出す。ＵＳＢデバイスドライバ実行部４０７は、受信したＵＳＢパケットを分析して、新たなＵＳＢパケットを生成して防犯防災補助デバイスに応答したり、アプリケーション実行部４１４に防犯防災補助デバイスのステータスを報告したりする。

【００４０】

防犯防災補助デバイス情報受信部４１０は、ＵＳＢデバイスドライバ実行部４０７で適

切なデバイスドライバを実行することにより、防犯防災補助デバイスからスマートデバイス２５０を介して状況検知情報を受信する。

【００４１】

アプリケーション実行部４１４は、ディスクリプタによって特定された製造元ＩＤおよび製品ＩＤを有する防犯防災補助デバイスに応じた防犯防災アプリケーションを実行する。アプリケーション選定部４０６は、デバイス判定部４０３が判定した製造元ＩＤおよび製品ＩＤに基づいて、スマートデバイス２５０において仮想的に実行されるべき防犯防災アプリケーションを、アプリケーションプログラムデータベース４２５から選定する。これにより、アプリケーション実行部４１４は、デバイス操作用画面送信部４１１および通信制御部４０１を介してスマートデバイス２５０に、デバイス操作用画面情報を送信する。つまり、スマートデバイス２５０では、接続された防犯防災補助デバイスの種類（組合せ）に応じて、異なる防犯防災アプリケーションの表示画面を表示することもできる。

【００４２】

アプリケーション実行部４１４は、スマートデバイス情報受信部４１３を介して、スマートデバイス２５０から取得した情報を取得し、管理データベース２１０に対して、店舗情報を蓄積する。例えばアプリケーション実行部４１４は、スマートデバイス２５０から、防犯時（犯行発生時や災害時を含む）における、時刻情報を取得し、状況検知情報と共に管理データベース２１０に蓄積する。

【００４３】

アプリケーション実行部４１４は、防犯防災補助デバイス情報受信部４１０を介して、防犯防災補助デバイスから状況検知情報を取得する。状況検知情報としては、不審者の侵入や火災の発生、ドアの開閉や異常振動などが挙げられる。

【００４４】

管理データベース２１０は、推奨防犯防災システムデータベース４５１、防犯防災対策データベース４５２、防犯課題シーンデータベース４５３、防犯対策効果計測者データベース４５４を含んでいる。

【００４５】

クラウドサーバ２００は、図１１に示すような推奨防犯防災システムデータベース４５１を参照することにより、スマートデバイス２５０に対して、どういった種類の防犯防災補助デバイスを接続すると有効かを提示することもできる。ユーザは、スマートデバイス２５０から、店舗の場所、店舗シーン（例：屋外常設店、屋内常設店（モールや商店街内の店舗）、イベント等での臨時店舗など）、店舗大きさ、店員数、予算などを入力する。クラウドサーバ２００は、これらの条件にあった防犯防災補助デバイスの組合せを、レンタル会社などに発注し、ユーザの店舗に届けさせる。

【００４６】

アプリケーション実行部４１４は、防犯防災対策データベース４５２（図１２参照）を参照して、取得した状況検知情報に対応する対策処理（例えば、防犯ライト点灯、威嚇音声出力、待避案内、避難案内、ＰＯＳ端末２７０のロック、スプリンクラーの作動など）を特定する。そして、スマートデバイス２５０を介して、対策処理に基づいて防犯防災補助デバイスを制御する。

【００４７】

また、アプリケーション実行部４１４は、防犯防災対策データベース４５２を参照して、その複数のセンサでの情報から、警備会社、警察、消防、会社の総務など、起きた事象に対応する通報先を決める。火事なら消防と会社の総務、不法侵入なら、警備会社と警察と会社への連絡というように使い分ける。

【００４８】

防犯防災対策データベース４５２は、上述したほか、発生した事象について、例えば、取得した不審者の音声や表情、犯人のひるみ度、店員の安全確保度を蓄積してもよい。また、防犯防災対策データベース４５２は、例えば揚げもの仮店舗では、水系の防犯対処は避けるべきといったナレッジを蓄積してもよい。

【００４９】
また、防犯課題シーンデータベース４５３においては、秋祭りでは老人の被害が多い、海祭りでは下着泥棒と盗撮が多いなどといった、季節や店舗の環境と犯罪履歴との関連性を蓄積する。
【００５０】
防犯対策効果計測者データベース４５４では、防犯対策の効果を誰が計測したかを蓄積する。例えば、社員、パート、派遣、お客様、の誰が申告したかを属性として蓄積し問題予防に利用する。また、性別、年代というパラメータや、報告者とその支援者の人数（１人、カップル、学生数名からの報告）、報告時の来客者と店員インの位置情報とを記録する。例えば、男性の方がより問題発見率が高いとか、女性とか店員とか、客の申しつけとか、データベース成長時の登録者の情報を蓄積する。２０代男性店員の方がより問題発生率が下がるとか、店員が２人や３人などの人数での問題発見率が高いとかいった関係性を蓄積する。問題発生時の他の客情報（位置や性別、年齢）や客の位置情報と外からの相関（窓側の見えるところにいたとか外から見えにくいところ何処にいた等）などを店員の問題報告として防犯対策効果計測者データベース４５４に蓄積する。これにより、問題予防効果や、問題発見効率や、担当者の年齢や男女の区別でどう動くと問題を予防しやすくなるかなどを後で導き出すことができる。
【００５１】
その他、管理データベース２１０には、火災の原因究明や犯人の逮捕につながるような証拠を蓄積してもよい。例えば、逃亡者の車種（車の種別、色、ナンバー）や犯人情報（性別、ドアを抜けたときの背丈情報、声の特徴）を撮影した画像から割り出して蓄積してもよい。それぞれの証拠について犯人逮捕に繋がったか否かを事後的に登録して、犯人逮捕に有効な情報は何かについてのデータベースも成長させてもよい。
【００５２】
（スマートデバイスの機能構成）
スマートデバイス２５０の機能構成について、図５を用いて説明する。スマートデバイス２５０は、ユーザからの指示や入力を受け付ける操作部５０１と、受け付けた指示情報や入力情報を送信する情報送信部５０２と通信制御部５０３とを備えている。通信制御部５０３は、ネットワークとのやり取りを制御する。
【００５３】
スマートデバイス２５０はまた、入出力部５０５として表示部５０６およびマイクやスピーカなどの音声入出力部５０７を備えている。画面受信部５０４は、通信制御部５０３を介して音声情報や画像情報を受信し、表示部５０６への画像出力や、音声入出力部５０７からの音声出力を行なう。
【００５４】
さらに、スマートデバイス２５０は、環境情報取得部５０８と位置検出部５２１と撮像部５２３と時刻検出部５２２とを備えている。ＧＰＳなどを利用した位置検出部５２１が検出した位置情報、デジタル時計などの時刻検出部５２２が検出した時刻情報、撮像部５２３を用いて撮影した画像情報などは、環境情報として、環境情報取得部５０８に送られる。環境情報取得部５０８が取得した環境情報は、情報送信部５０２および通信制御部５０３を介して、クラウドサーバ２００に送信される。
【００５５】
さらに、スマートデバイス２５０は、ＵＳＢコネクタ５２０と汎用ＵＳＢドライバ実行部５１１を備えており、ディスクリプタ取得部５１２は、接続されたＵＳＢデバイスから最低限のディスクリプタを取得できる構成となっている。取得されたディスクリプタは、ディスクリプタ送信部５１３にわたされて、通信制御部５０３を介してクラウドサーバ２００に送信される。
【００５６】
スマートデバイス２５０は、アンカプセリング部５１４およびカプセリング部５１５をさらに備えている。それらは、クラウドサーバ２００との通信時には、クラウドサーバ２

００との間でやり取りされるＵＳＢパケットについて、アンカプセリング処理やカプセリング処理を行なう。

【００５７】

アンカプセリング部５１４およびカプセリング部５１５は、信号転送制御部５１９として機能する。すなわち、信号転送制御部５１９は、防犯防災補助デバイスとクラウドサーバ２００との間の信号転送を制御する。

【００５８】

スマートデバイス２５０は、自端末にデバイスドライバを有するデバイスについてのデバイスディスクリプタと、インタフェースディスクリプタと、ベンダＩＤと、プロダクトＩＤとの対応関係を示すデバイスデータベース５２４を記憶する。デバイスデータベース５２４の構成は、図７Ｅに示す通りである。

【００５９】

スマートデバイス２５０は、防犯防災補助デバイスが接続された際に防犯防災補助デバイスから通知されたデバイスディスクリプタと、デバイスデータベース５２４内のデバイスディスクリプタとを比較する。防犯防災補助デバイスから通知されたデバイスディスクリプタがデバイスデータベース５２４内のデバイスディスクリプタと一致すれば、スマートデバイス２５０は、防犯防災補助デバイスが自端末で処理可能なデバイスであると判定する。一方、デバイスディスクリプタが一致しない場合には、スマートデバイス２５０は、自端末で処理不可能なデバイスであると判定する。

【００６０】

なお、防犯防災補助デバイスから通知されたデバイスディスクリプタ内のベンダＩＤとプロダクトＩＤとを抽出し、デバイスデータベース内のベンダＩＤおよびプロダクトＩＤと比較してもよい。その場合、デバイスデータベース５２４内に一致するベンダＩＤおよびプロダクトＩＤが存在する場合には、自端末で処理可能な防犯防災補助デバイスであると判定できる。逆に、ベンダＩＤおよびプロダクトＩＤが一致しない場合には、スマートデバイス２５０は、自端末で処理不可能な防犯防災補助デバイスであると判定できる。

【００６１】

（システム全体の処理の流れ）

次に、図６に示すシーケンス図を用いて、システム全体の処理の流れについて整理する。まず、防犯防災補助デバイスが、スマートデバイス２５０に接続される（Ｓ６０１）。すると、スマートデバイス２５０の汎用ＵＳＢドライバ実行部５１１およびディスクリプタ取得部５１２は、防犯防災補助デバイスから状況検知情報を取得するためのドライバプログラムなどが自端末に備わっているか否か判定する（Ｓ６０３）。

【００６２】

他種類にわたる防犯防災補助デバイスのドライバプログラムやアプリケーションプログラムを、ダウンロードしてインストールしていくと、スマートデバイス２５０の容量がいくらあっても足りない。そこで、汎用ＵＳＢドライバ実行部５１１は、図９Ａのような接続確認画面９０１を表示させてユーザに確認する。そして、ユーザからの指示に応じてスマートデバイス２５０からクラウドサーバ２００にログインする。さらに、ディスクリプタ送信部５１３を用いてディスクリプタをクラウドサーバ２００に送信し、クラウドサーバ２００主導で、防犯防災補助デバイスから状況検知情報を取得することをリクエストする（Ｓ６０５）。ただし、スマートデバイス２５０のユーザが、クラウドサーバ２００を運営するクラウドプロバイダの会員になっていることが必要となる。

【００６３】

クラウドサーバ２００は、スマートデバイス２５０を中継して（Ｓ６０７）、防犯防災補助デバイスとのやり取りを行ない、防犯防災補助デバイスを特定する（Ｓ６０９）。次に、その防犯防災補助デバイスに応じた防犯防災アプリケーションプログラム２０４を選定し、起動する（Ｓ６１１）。

【００６４】

次に、データベース選定部４１５は、図１０に示すような対応テーブル１００１を用い

て、接続された防犯防災補助デバイスに応じた管理データベースを決定する（Ｓ６１２）。対応テーブル１００１では、防犯防災補助デバイスを特定する情報が、その防犯防災補助デバイスを管理すべき企業や店舗と対応付けられ、さらに、その防犯防災補助デバイスからのデータを登録すべき管理データベースのアドレスに対応付けられている。これにより、防犯防災補助デバイスが特定された時点で、その防犯防災補助デバイスを用いて取得した状況検知情報をどの管理データベースに保存すべきか決定できる。ユーザは、防犯防災補助デバイスをスマートデバイスに接続するだけで、簡単に、防犯防災対策を実現できる。

【００６５】

クラウドサーバ２００は、ステップＳ６０９で特定したデバイスに対応するドライバを、ドライバプログラムデータベース４２４から選定し、そのドライバを駆動させる（Ｓ６１３）。これにより、クラウドサーバ２００は、スマートデバイス２５０を介して、防犯防災補助デバイスに対してアクセス可能となる。

【００６６】

防犯防災アプリケーションプログラム２０４は、まず、スマートデバイス２５０の表示部５０６に対して、図９Ｂに示すような防犯防災補助デバイスの確認画面９０２を表示させて、スマートデバイス２５０に接続された防犯防災補助デバイスを確認させる。なお、ここで、防犯防災アプリケーションプログラム２０４は、スマートデバイス２５０に接続された防犯防災補助デバイスが、あらかじめ接続を求めたデバイス（店舗として接続を望むデバイス）と同じデバイスか否かを判定してもよい。あらかじめ定めたデバイスと違うデバイスが繋がれた場合、本来繋ぐべきデバイスを、スマートデバイス２５０に対して、あらかじめ定めた画面や、音声により通知してもよい。つまり、これにより、つないで欲しい防犯防災補助デバイスをスマートデバイス２５０につなぐように誘導することができる。

【００６７】

以上が前処理となり、ここから、防犯防災処理に移る。クラウドサーバ２００において防犯防災アプリケーションプログラム２０４を起動したアプリケーション実行部４１４は、防犯防災補助デバイスのそれぞれに対して、スマートデバイス２５０を介して駆動指示を送る。このとき、ステップＳ６１７として、スマートデバイス２５０の表示画面には、各種の防犯防災補助デバイスに応じたメッセージを表示する。例えば、「防犯カメラを駆動します」「人感センサを駆動しました。現在お客様は○名です」「スピーカからの威嚇音声出力をテストします」「カラーボール自動ピッチングマシンにカラーボールがセットされていません。セットして下さい」等である。

【００６８】

防犯防災補助デバイスは、クラウドサーバ２００からの指示に応じて、駆動を開始すると（Ｓ６１９）、監視対象となっている店舗内、または店舗外の状況を検知し（Ｓ６２１）、定期的に、または、異常発生時に、状況検知情報をスマートデバイス２５０に向けて送信する。

【００６９】

スマートデバイス２５０では、受信した状況検知情報を表示すると共に状況検知情報をクラウドサーバ２００に転送する。例えば「不審者がいます」「揺れを検知しました」「煙がでています」などといったメッセージを表示することができる。

【００７０】

クラウドサーバ２００は、状況検知情報を受信すると、ステップＳ６２７に進んで、管理データベース２１０を参照して、どのような対策処理が必要かを判定する。

【００７１】

何らかの対策処理が必要な場合には、ステップＳ６２９に進み、クラウドサーバ２００は、スマートデバイス２５０に対して、対策処理の指示を送る。スマートデバイス２５０は、その指示を中継して防犯防災補助デバイスに送信する（Ｓ６３１）。防犯防災補助デバイスは、クラウドサーバ２００からの指示に応じて対策処理を行なう。

【００７２】
以上、ステップＳ６１５～Ｓ６３３の一連の処理が防犯防災処理であり、防犯防災アプリケーションプログラムが駆動中は繰り返し、この防犯防災処理を行なう。
【００７３】
以上の一連の処理により、クラウドサーバ２００は、防犯防災システムを構築することができる。
【００７４】
（クラウドサーバ２００での処理の流れ）
図７Ａを用いて、クラウドサーバ２００におけるより詳しい処理の流れを説明する。ステップＳ７１１において、スマートデバイス２５０から、デバイス接続リクエストを受信したと判断すると、ステップＳ６０９に進み、デバイス特定処理を行なう。ステップＳ６１１では、すでに説明したとおり、特定したデバイスに基づいて、防犯防災アプリケーションプログラムを選定し、起動する。さらに、ステップＳ６１２では管理データベース２１０を特定し、ステップＳ６１３ではデバイスドライバを選定して起動する。
【００７５】
一方、ステップＳ７２１において、状況検知情報を受信したと判断すると、ステップＳ６２５において、管理データベース２１０への状況検知情報の蓄積処理を行なう。そしてさらに、ステップＳ６２７において、管理データベース２１０を参照して、どのような対策処理が必要かを判定する。さらに、対策処理が必要と判定すると、ステップＳ６２９でその対策処理指示をＵＳＢパケットとして送信する処理に移る。
【００７６】
ステップＳ７３１において、ＵＳＢパケットの送信を行なうと判定した場合には、ステップＳ７３３に進み、送信用ＵＳＢパケットを生成し、さらにステップＳ７３５においてＩＰカプセリングしてデバイス宛に送信する。その後、デバイスからの受信を待ち（Ｓ７３７）、受信するとＩＰアンカプセリングを行ない（Ｓ７３９）、さらに受信ＵＳＢパケットのアンカプセリング処理を行なう（Ｓ７４１）。このステップＳ７３１～Ｓ７４１の処理により防犯防災補助デバイスからスマートデバイス２５０を介して所望の情報を受信することができる。
【００７７】
〈ディスクリプタの取得方法〉
図７Ｂ、図７Ｃ、図７Ｄは、ステップＳ６０１～Ｓ６０９で説明したデバイス特定のための処理についてより詳しく説明する図である。これらの図は、クラウドサーバ２００とスマートデバイス２５０と防犯防災補助デバイスとの間でやり取りされるパケットデータについて示している。
【００７８】
図７Ｂにおいて、スマートデバイス２５０に防犯防災補助デバイスが接続されると、セットアップ・ステージＳ７５１において、トークン・パケットとデータ・パケットとを、スマートデバイス２５０から防犯防災補助デバイスに送信する。防犯防災補助デバイスは、これに応えてハンドシェイク・パケットをスマートデバイス２５０に送信する。スマートデバイス２５０は、まず、適正なハンドシェイク・パケットが返ってくるか否かにより、自端末で防犯防災補助デバイスを制御できるか判断できる。
【００７９】
例えば、スマートデバイス２５０に接続されることがあらかじめ想定されているデバイスであれば、適正なハンドシェイク・パケットが返り、データ・ステージ、ステータス・ステージを続ける。それにより取得したデバイスディスクリプタに対応して、スマートデバイス２５０内に用意されたデバイスドライバを駆動することでデバイスを制御できる。しかし、スマートデバイス２５０が接続を想定されているデバイスは非常に数が少ない。セットアップ・ステージＳ７０１においてハンドシェイク・パケットが返ってこない場合、ここで、ＵＳＢ切断処理を行ない（Ｓ７５２）、スマートデバイス２５０はクラウドサーバ２００に対してデータ取得のリクエストを行なう（Ｓ６０５）。

【００８０】
次にクラウドサーバ２００は、スマートデバイス２５０を介して、防犯防災補助デバイスとの間で、セットアップ・ステージＳ７５３を再度行ない、データ・ステージＳ７５４に進むことにより、デバイスディスクリプタといったデバイス情報を取得する。クラウドサーバ２００は、世の中に存在する様々な防犯防災補助デバイスとも接続可能となるように数多くのドライバおよびデータ変換モジュールをあらかじめ備えている。そのため、クラウドサーバ２００と防犯防災補助デバイスとの間では、セットアップ・ステージＳ７５３、データ・ステージＳ７５４、ステータス・ステージＳ７５５と順調に進み、防犯防災補助デバイスとの通信が適正に確立する。
【００８１】
図７Ｃは、防犯防災補助デバイスがハンドシェイク・パケットを返すものの、スマートデバイス２５０が防犯防災補助デバイスから取得したデバイスディスクリプタに対応するドライバを有していない場合のシーケンスを示す。この場合、スマートデバイス２５０と防犯防災補助デバイスとの間でセットアップ・ステージＳ７６１、データ・ステージＳ７６２、ステータス・ステージＳ７６３を行なう。この３つのステージによって取得したデバイスディスクリプタに対応するデバイスドライバをスマートデバイス２５０が有していないと判断すると、ＵＳＢ切断処理Ｓ７６４を行なう。そして、スマートデバイス２５０はクラウドサーバ２００に対してデータ取得のリクエストを行なう（Ｓ６０５）。
【００８２】
そして、スマートデバイス２５０は、クラウドサーバ２００に対して防犯防災補助デバイスとの通信確立を要求する。スマートデバイス２５０と防犯防災補助デバイスとの間のＵＳＢ接続を切断後、クラウドサーバ２００において、再度、セットアップ・ステージＳ７６５、データ・ステージＳ７６６、ステータス・ステージＳ７６７を行なう。これによりクラウドサーバ２００は、防犯防災補助デバイスから直接デバイスディスクリプタを取得して、デバイスにあったドライバを駆動できる。
【００８３】
図７Ｄは、スマートデバイス２５０と防犯防災補助デバイスとの間のセットアップ・ステージＳ７７１およびデータ・ステージＳ７７２において取得したデバイスディスクリプタを、スマートデバイス２５０の内部にキャッシュする場合の処理を示している。ＵＳＢ切断処理を行なう前に、取得したデバイスディスクリプタを、スマートデバイス２５０の内部にキャッシュし（Ｓ７７４）、スマートデバイス２５０はクラウドサーバ２００に対してデータ取得のリクエストを行なう（Ｓ６０５）。
【００８４】
そして、スマートデバイス２５０と防犯防災補助デバイスとの間の接続を一度切断した後に、クラウドサーバ２００主導で、防犯防災補助デバイスとの通信確立処理を開始する（Ｓ７７５～Ｓ７７７）。この場合、セットアップ・ステージＳ７７５において、スマートデバイス２５０は、セットアップ用のトークン・パケットおよびデータ・パケットを防犯防災補助デバイスに送らず、ハンドシェイク・パケットを生成し、クラウドサーバ２００に送信する。また、データ・ステージＳ７７６では、スマートデバイス２５０は、トークン・パケットとデータ・パケットとをクラウドサーバ２００から受信する。そして、それらを防犯防災補助デバイスに送らずに、キャッシュからデバイスディスクリプタを読出し、クラウドサーバ２００に送信する。すなわち、防犯防災補助デバイスからデバイスディスクリプタを取得する処理を省略することが可能となるため、防犯防災補助デバイスとの通信切断後の再開を効率良く行なうことが可能となる。
【００８５】
（デバイス特定テーブル）
デバイスデータベース４２３は、図７Ｅに示したデバイスデータベース５２４と同様に、デバイスディスクリプタと、インタフェースディスクリプタと、ベンダＩＤと、プロダクトＩＤとの対応関係を記憶する。
【００８６】

クラウドサーバ２００は、防犯防災補助デバイスがスマートデバイス２５０に接続された際に、防犯防災補助デバイスからスマートデバイス２５０を介して取得したデバイスディスクリプタを、デバイスデータベース４２３内で検索する。そして、そのベンダＩＤおよびプロダクトＩＤを特定する。そしてそのベンダＩＤおよびプロダクトＩＤに対応するデバイスドライバを、ドライバプログラムデータベース４２４から選択して、実行する。

【００８７】

なお、デバイスデータベース４２３は、デバイスディスクリプタと、インタフェースディスクリプタと、ベンダＩＤと、プロダクトＩＤとの対応関係を記憶しているが、本発明はこれに限定するものではない。例えば、さらに、デバイスディスクリプタと商品名との対応関係を記憶してもよい。その場合、このデバイスデータベース４２３を用いてデバイスディスクリプタから防犯防災補助デバイスの商品名を特定し、その商品名を、スマートデバイス２５０の画面に表示させてもよい。そうすれば、スマートデバイス２５０のユーザは、「自分が接続した防犯防災補助デバイスをクラウドサーバ２００が認識したこと」を確認することができ、大きな安心感を得ることができる。

【００８８】

（ＵＳＢ接続処理）

図８Ａ～図８Ｄを用いて、ＵＳＢでの通信を確立するまでにクラウドサーバ２００とスマートデバイス２５０と防犯防災補助デバイスとの間でやり取りされる信号をより詳細に説明する。特に、ここでは、図７Ｄに示したように、デバイスディスクリプタをキャッシュに保存する例について説明する。

【００８９】

ステップＳ８０１において、防犯防災補助デバイスをスマートデバイス２５０に接続し、電源を投入する。次に、ステップＳ８０２において、スマートデバイス２５０は防犯防災補助デバイスに対するＵＳＢ接続処理を開始し、リセット信号を送信する。次に、ステップＳ８０３において、スマートデバイス２５０は、防犯防災補助デバイスに対してアドレスを指定する。この後においてスマートデバイス２５０と防犯防災補助デバイスとの間でやり取りされるパケットにはそのアドレスが付加される。

【００９０】

ステップＳ８０４において、スマートデバイス２５０は防犯防災補助デバイスからディスクリプタを取得するために「ＧＥＴ　ＤＥＳＤＣＲＩＰＴＯＲ」の処理を行なう。「ＧＥＴ　ＤＥＳＤＣＲＩＰＴＯＲ」の処理は、図７Ｄで説明したステップＳ７２１～Ｓ７２３と同様であるため、詳細は説明しない。ディスクリプタのリクエストを防犯防災補助デバイスに送信すると（Ｓ８０５）、防犯防災補助デバイスは、エンドポイント０領域に記憶されたデバイスディスクリプタをスマートデバイス２５０に送信する（Ｓ８０６、Ｓ８０７）。スマートデバイス２５０は、ステータス・ステージＳ７２３において、その確認信号（ACK）を防犯防災補助デバイスに送信する。

【００９１】

この時点でデバイスディスクリプタを取得したスマートデバイス２５０は、そのデバイスディスクリプタをキャッシュに保存する（Ｓ７７４）。また、そのデバイスディスクリプタを用いて、スマートデバイス２５０が制御可能なデバイスか判定する（Ｓ６０３）。制御不可能と判断すると、ステップＳ８１１に進み、ＵＳＢ切断処理を行ない、同時に、クラウドサーバ２００に対し、防犯防災補助デバイスの制御依頼を行なう（Ｓ８１２）。

【００９２】

次に、ステップＳ８１３において、クラウドサーバ２００は、防犯防災補助デバイスの制御を行なうべく処理を開始し、リセット信号を、スマートデバイス２５０を介して防犯防災補助デバイスに送信する。次に、ステップＳ８１５において、クラウドサーバ２００は、セットアドレスを行ない、防犯防災補助デバイスに対してアドレスを指定する。

【００９３】

さらに、クラウドサーバ２００は、ゲットディスクリプタ（Ｓ８１６）と、ゲットコンフィギュレーション（Ｓ８２４）とを、スマートデバイス２５０を介して防犯防災補助デ

バイスに対して行なう（Ｓ８２３）。具体的には、ステップＳ８１７において、クラウドサーバ２００は、ゲットディスクリプタをスマートデバイス２５０に送る。ステップＳ８１８において、スマートデバイス２５０は、キャッシュに保存されたデバイスディスクリプタを読み出し、クラウドサーバ２００に送信する（Ｓ８１９）。

【００９４】

ステップＳ８２５において、防犯防災補助デバイスは、エンドポイント０領域に記憶されたコンフィギュレーションディスクリプタを送信する。次に、クラウドサーバ２００は、スマートデバイス２５０を介して防犯防災補助デバイスに対してＢＵＬＫ　ＴＲＡＮＳＦＥＲを行なう（Ｓ８２６）。すると、防犯防災補助デバイスは、状況検知情報を読み出して（Ｓ８２７）、スマートデバイス２５０を介してクラウドサーバ２００に送信する。

【００９５】

ステップＳ６０３において、防犯防災補助デバイスのデバイスディスクリプタに基づいて、制御可能なデバイスではないと判定すると、図８Ｂのステップ８２８に進む。ステップＳ８２８、Ｓ８２９では、コンフィギュレーションディスクリプタ取得処理を行ない、防犯防災補助デバイスは、それに応じてコンフィギュレーションディスクリプタをスマートデバイス２５０に送信する。スマートデバイス２５０は、ステップＳ８３２において、取得したコンフィギュレーションディスクリプタをキャッシュに保存する。そして、ステップＳ６０３において、スマートデバイス２５０は、コンフィギュレーションディスクリプタに基づいて、防犯防災補助デバイスがスマートデバイス２５０にとって制御可能なデバイスか否か判定する。制御可能ではないと判定すると、ステップＳ８３３に進んでスマートデバイス２５０と防犯防災補助デバイスとの間のＵＳＢ接続を切断する。

【００９６】

ＵＳＢ接続を切断後、スマートデバイス２５０は、クラウドサーバ２００に対して、防犯防災補助デバイスの制御を依頼する。クラウドサーバ２００は、その制御依頼に応じて、ＵＳＢ制御を開始すると共にリセット信号を、スマートデバイス２５０を介して防犯防災補助デバイスに送信する（Ｓ８３５）。そして続けてセットアドレスを行ない（Ｓ８３６）、アドレスを防犯防災補助デバイスに指定する。さらに、ＧＥＴ　ＤＥＳＣＲＩＰＴＯＲ（Ｓ８３７）で、スマートデバイス２５０に対して、ディスクリプタを要求する。スマートデバイス２５０は、その要求を防犯防災補助デバイスに中継する代わりに、デバイスディスクリプタをキャッシュから読出して（Ｓ８３９）、クラウドサーバ２００に返す（Ｓ８４０）。

【００９７】

さらに、クラウドサーバ２００は、スマートデバイス２５０を介して防犯防災補助デバイスに対してＧＥＴ　ＣＯＮＦＩＧＵＲＡＴＩＯＮを実行する（Ｓ８４１）。スマートデバイス２５０は、そのコマンドを防犯防災補助デバイスに送信する代わりに、キャッシュに記憶されたコンフィギュレーションディスクリプタを読み出し、クラウドサーバ２００に送信する（Ｓ８４３）。次に、クラウドサーバ２００は、スマートデバイス２５０を介して防犯防災補助デバイスに対してＢＵＬＫ　ＴＲＡＮＳＦＥＲを行なう（Ｓ８４４）。防犯防災補助デバイスは状況検知情報を読み出して（Ｓ８４５）、スマートデバイス２５０を介してクラウドサーバ２００に送信する。

【００９８】

ステップＳ６０３において、コンフィギュレーションディスクリプタに基づいて、制御可能なデバイスであると判定すると（Ｂ）、図８Ｃのステップ８４６に示すＢＵＬＫ　ＴＲＡＮＳＦＥＲに進む。ＢＵＬＫ　ＴＲＡＮＳＦＥＲでも、セットアップ・ステージ、データ・ステージ、ステータス・ステージを行なうことにより、防犯防災補助デバイスから状況検知情報を読出して、スマートデバイス２５０に送信する（Ｓ８４９）。スマートデバイス２５０は、読出された状況検知情報を受信すると、キャッシュに保存して（Ｓ８５１）、図８Ｄのステップ８５６に進む。

【００９９】

図８Ｄのステップ８５６では、スマートデバイス２５０は、クラウドサーバ２００に

対して防犯防災補助デバイスの制御依頼を行なう。クラウドサーバ２００は、その制御依頼に応じて、ＵＳＢ制御を開始すると共にリセット信号を、スマートデバイス２５０を介して防犯防災補助デバイスに送信する（Ｓ８５７）。そして続けてセットアドレスを行ない（Ｓ８５９）、アドレスを防犯防災補助デバイスに指定する。さらに、ＧＥＴ　ＤＥＳＣＲＩＰＴＯＲ（Ｓ８６１）で、スマートデバイス２５０に対して、ディスクリプタを要求する。すると、スマートデバイス２５０は、その要求を防犯防災補助デバイスに中継する代わりに、デバイスディスクリプタをキャッシュから読出して（Ｓ８６３）、クラウドサーバ２００に返す。

【０１００】

さらに、クラウドサーバ２００は、スマートデバイス２５０を介して防犯防災補助デバイスに対してＧＥＴ　ＣＯＮＦＩＧＵＲＡＴＩＯＮを実行する（Ｓ８６５）。すると、スマートデバイス２５０は、そのコマンドを中継する代わりに、キャッシュに保存されたコンフィギュレーションディスクリプタを読出して、クラウドサーバ２００に送信する（Ｓ８６７）。

【０１０１】

次に、クラウドサーバ２００は、スマートデバイス２５０を介して防犯防災補助デバイスに対してＢＵＬＫ　ＴＲＡＮＳＦＥＲを行なう（Ｓ８６９）。すると、スマートデバイス２５０は、キャッシュに保存された情報を読み出して（Ｓ８７１）、クラウドサーバ２００に送信する。

【０１０２】

以上のシーケンスにより、スマートデバイス２５０のキャッシュをうまく使って、クラウドサーバ２００と防犯防災補助デバイスとの通信を効率的に行なうことが可能となる。

以上、本実施形態によれば、防犯防災補助デバイスの特定情報を、スマートデバイスを介して取得して、ドライバおよびアプリケーションを特定して実行する。したがって、防犯防災補助デバイスをスマートデバイスに接続するだけで、簡単に、防犯防災対策を実現できる。つまり、防犯防災補助デバイスとスマートデバイスとを用いて、非常に簡易に、臨時店舗などに防犯防災システムを構築できる。

【０１０３】

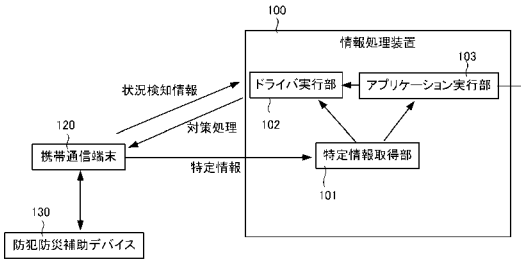
［他の実施形態］

以上、実施形態を参照して本願発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。また、それぞれの実施形態に含まれる別々の特徴を如何様に組み合わせたシステムまたは装置も、本発明の範疇に含まれる。

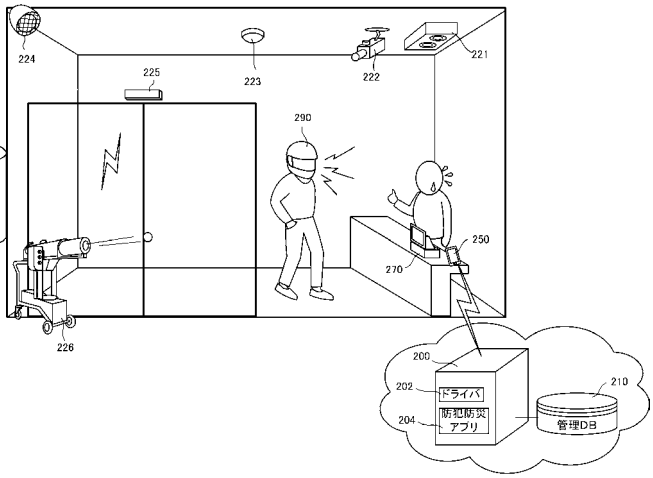
【０１０４】

また、本発明は、複数の機器から構成されるシステムに適用されてもよいし、単体の装置に適用されてもよい。さらに、本発明は、実施形態の機能を実現する情報処理プログラムが、システムあるいは装置に直接あるいは遠隔から供給される場合にも適用可能である。したがって、本発明の機能をコンピュータで実現するために、コンピュータにインストールされるプログラム、あるいはそのプログラムを格納した媒体、そのプログラムをダウンロードさせるＷＷＷ（World Wide Web)サーバも、本発明の範疇に含まれる。

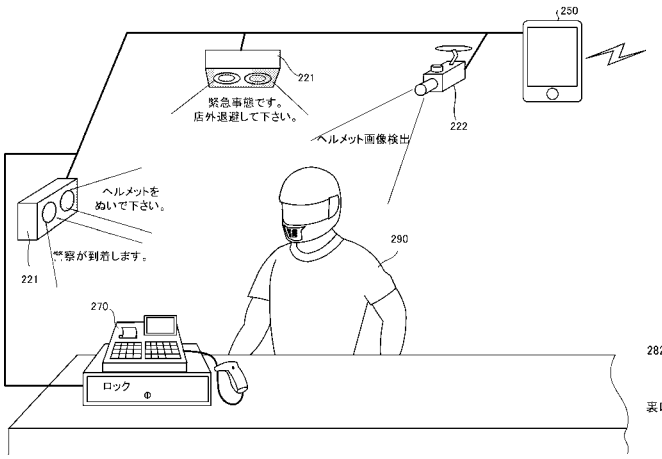
【図１】



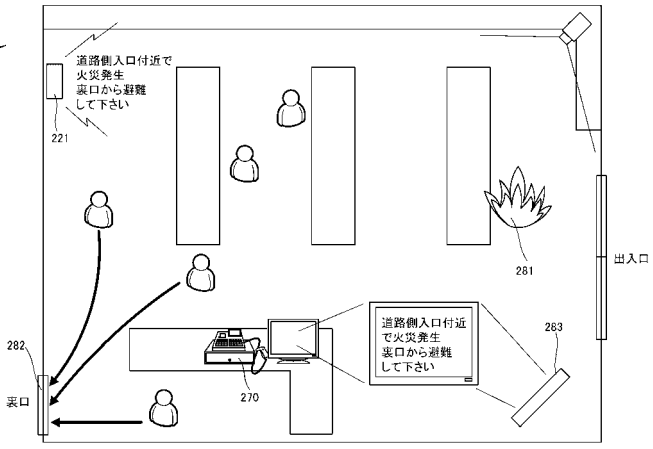
【図２Ａ】



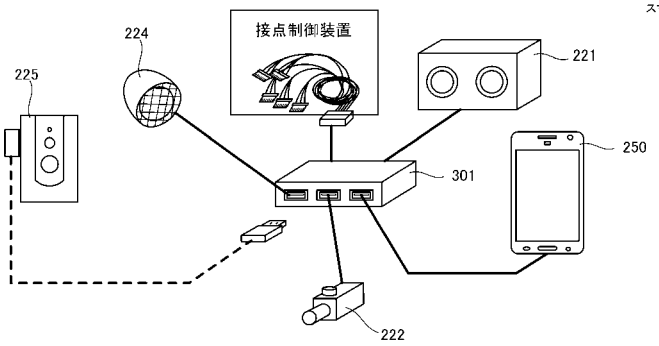
【図２Ｂ】



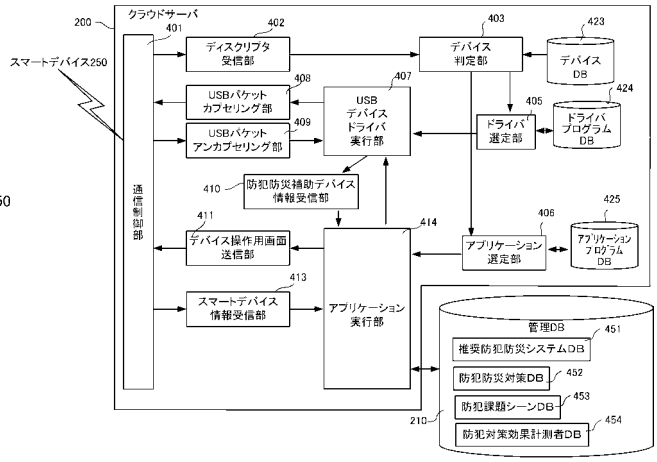
【図２Ｃ】



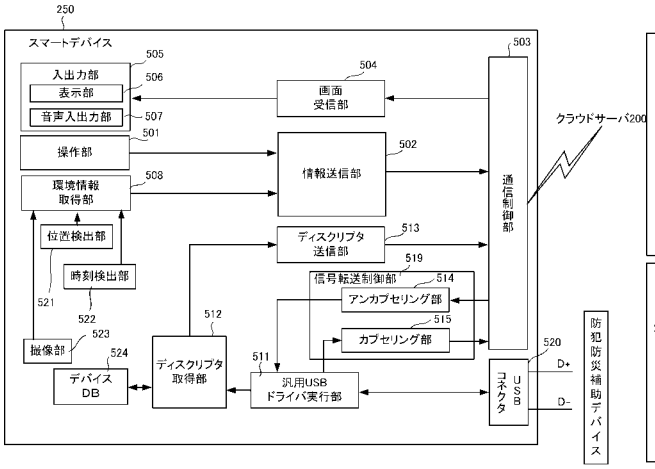
【図３】


接点制御装置
224
225
221
250
301
222

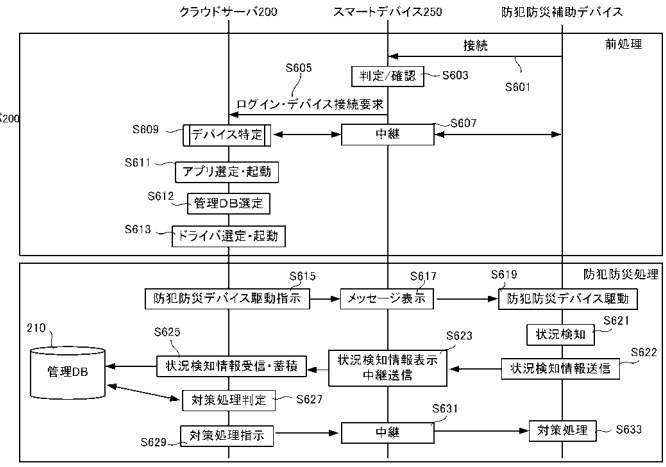
【図４】


クラウドサーバ
200
401
スマートデバイス250
通信制御部
ディスクリプタ受信部
402
デバイス判定部
403
デバイスDB
423
USBパケットカプセリング部
408
USBパケットアンカプセリング部
409
USBデバイスドライバ実行部
407
ドライバ選定部
405
ドライバプログラムDB
424
防犯防災補助デバイス情報受信部
410
デバイス操作用画面送信部
411
アプリケーション選定部
406
アプリケーションプログラムDB
425
スマートデバイス情報受信部
413
アプリケーション実行部
414
管理DB
451
推奨防犯防災システムDB
防犯防災対策DB
452
防犯課題シーンDB
453
防犯対策効果計測者DB
454
210

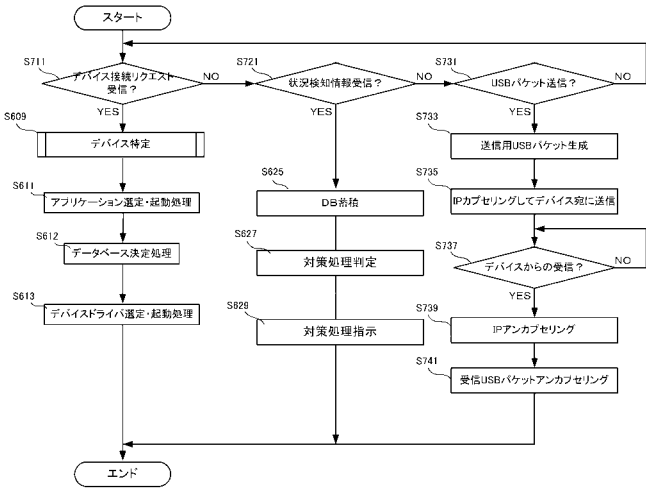
【図５】


250
スマートデバイス
入出力部
505
表示部
506
音声入出力部
507
操作部
501
環境情報取得部
508
位置検出部
時刻検出部
521
522
撮像部
523
デバイスDB
524
ディスクリプタ取得部
512
511
汎用USBドライバ実行部
画面受信部
504
情報送信部
502
ディスクリプタ送信部
513
519
信号転送制御部
アンカプセリング部
514
カプセリング部
515
503
通信制御部
USBコネクタ
520
D+
D-
クラウドサーバ200
防犯防災補助デバイス

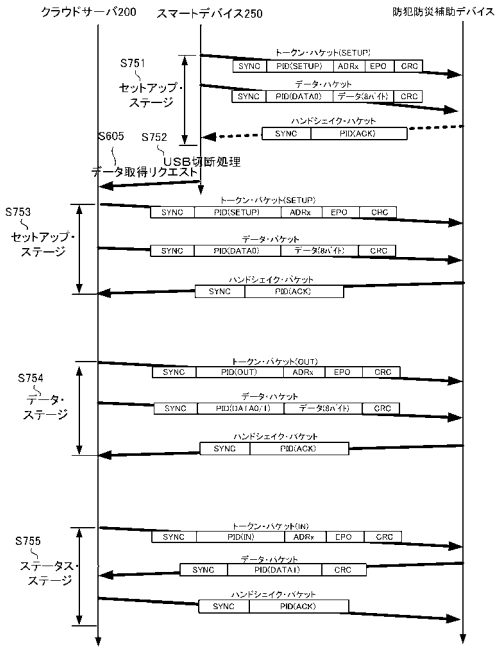
【図６】


クラウドサーバ200
スマートデバイス250
防犯防災補助デバイス
前処理
接続
S601
判定/確認
S603
S605
ログイン・デバイス接続要求
デバイス特定
S609
中継
S607
アプリ選定・起動
S611
管理DB選定
S612
ドライバ選定・起動
S613
防犯防災処理
防犯防災デバイス駆動指示
S615
メッセージ表示
S617
防犯防災デバイス駆動
S619
状況検知
S621
状況検知情報送信
S622
状況検知情報表示中継送信
S623
状況検知情報受信・蓄積
S625
管理DB
210
対策処理判定
S627
対策処理指示
S629
中継
S631
対策処理
S633

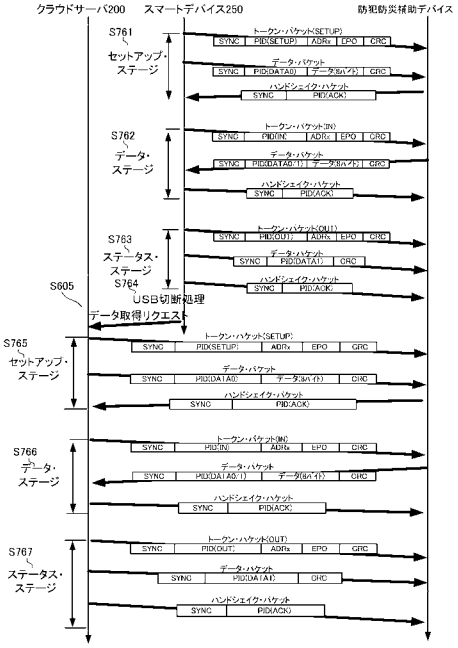
【図７Ａ】



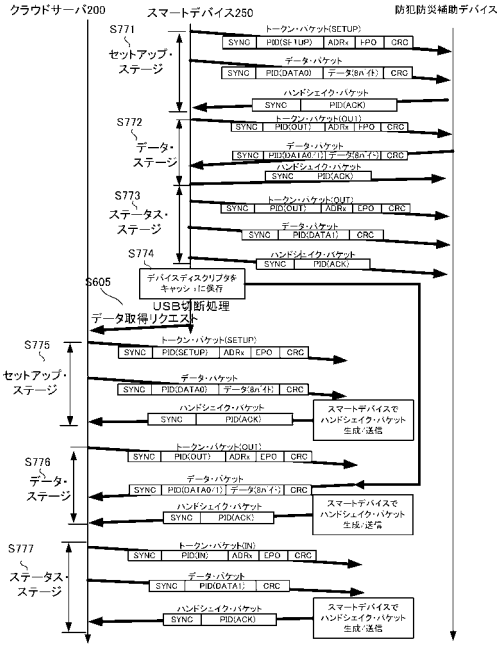
【図７Ｂ】



【図７Ｃ】



【図７Ｄ】

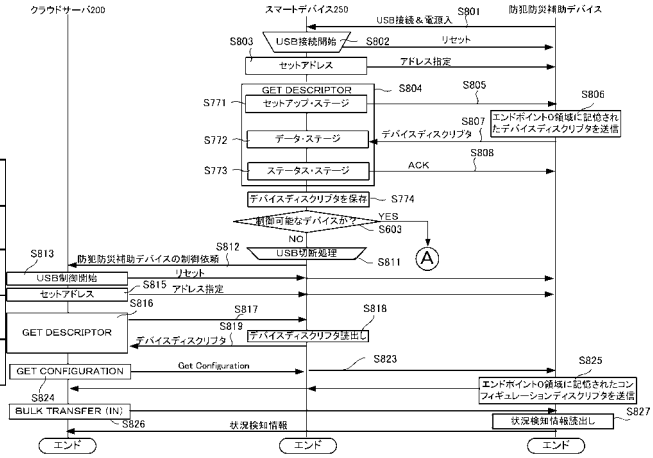


【図７Ｅ】

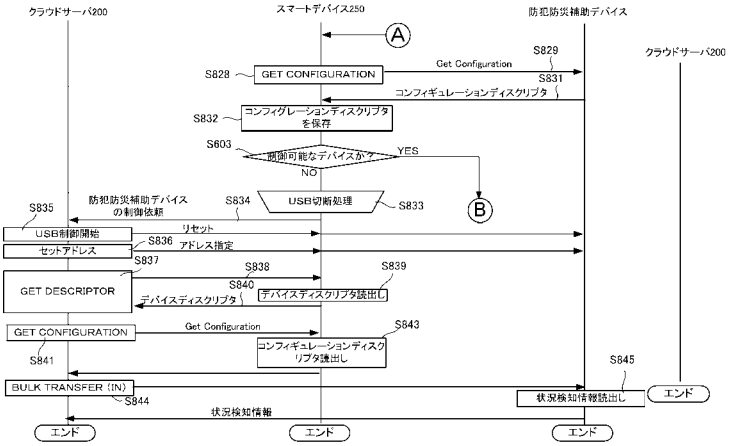
524

デバイス ディスクリプタ	インタフェース ディスクリプタ	ベンダID	プロダクトID
AAAAAA	XXXXXX	○○○○	●●●●
BBBBBB	YYYYYY	△△△△	▲▲▲▲
CCCCCC	ZZZZZZ	□□□□	■■■■
⋮	⋮	⋮	⋮

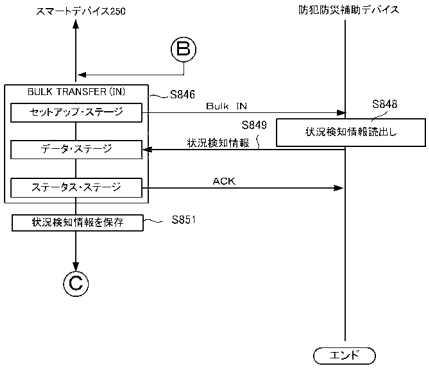
【図８Ａ】



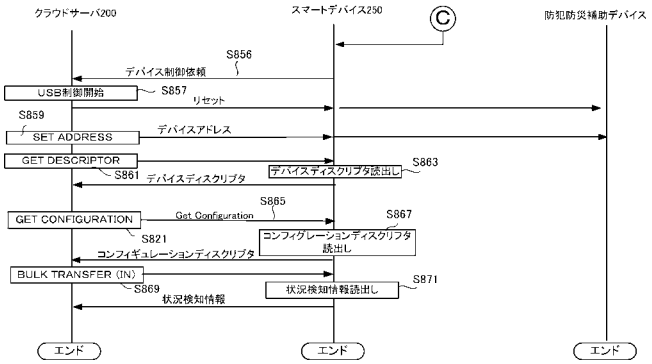
【図８Ｂ】



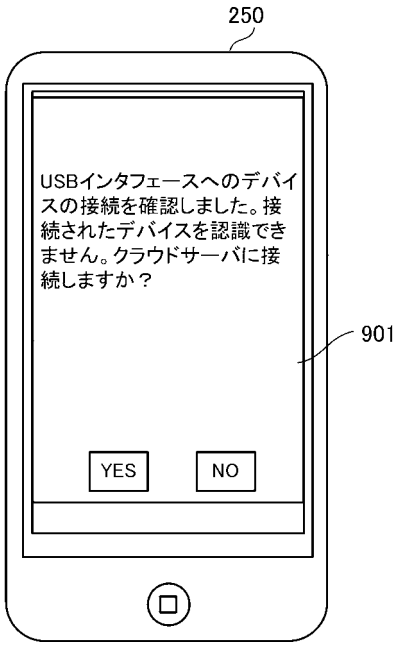
【図８Ｃ】



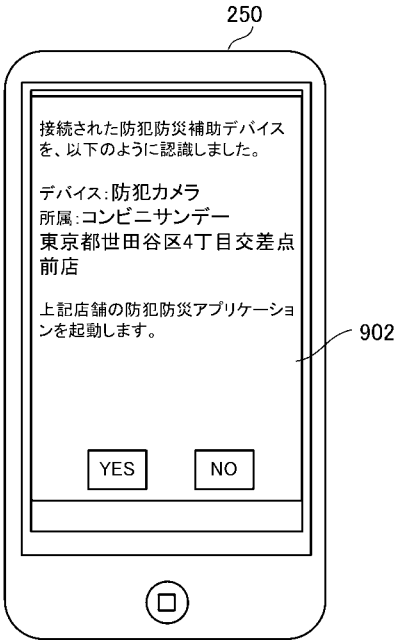
【図８Ｄ】



【図９Ａ】



【図９Ｂ】



【図１０】

1001

ベンダID	プロダクトID	シリアルNo.	商品名	使用企業	店舗	DBアドレス

【図１１】

451

店舗シーン	店舗大きさ		
	～30m²	30～60m²	60m²～
屋外常設店	ビデオカメラ1台・スピーカ・防犯ライト・火災センサ・開閉センサ・接点制御装置	ビデオカメラ2台・スピーカ2台・防犯ライト・火災センサ・開閉センサ・接点制御装置	ビデオカメラ3台・スピーカ2台・防犯ライト・火災センサ・開閉センサ・ピッチングマシン・接点制御装置
屋内常設店	ビデオカメラ1台・スピーカ・防犯ライト・火災センサ	ビデオカメラ2台・スピーカ・防犯ライト・火災センサ	ビデオカメラ3台・スピーカ・防犯ライト・火災センサ
屋外臨時店	ビデオカメラ1台・スピーカ・防犯ライト・火災センサ	ビデオカメラ2台・スピーカ・防犯ライト・火災センサ	ビデオカメラ3台・スピーカ・防犯ライト・火災センサ
屋内臨時店	ビデオカメラ1台・防犯ライト	ビデオカメラ2台・スピーカ・防犯ライト	ビデオカメラ3台・スピーカ・防犯ライト

【図１２】

452

状況検知情報	対策処理	通報先
煙検出・火の画像認識	スプリンクラー作動・避難ガイダンス音声出力・避難路表示・ドア開放	消防署 会社(xxx-xxxx-xxxx)
自動ドア開放検出・不審者の侵入認識	防犯ライト点灯・避難ガイダンス音声出力・威嚇放送・ドア開放（店員及び客避難後ドア施錠）	警備会社(yy-yyyy-yyyy)・警察・ 会社(xxx-xxxx-xxxx)
自動ドア開放検出・不審者の退店認識	不審者に対してカラーボール発射	警備会社(yy-yyyy-yyyy)・警察・ 会社(xxx-xxxx-xxxx)
揺れの画像認識	避難ガイダンス音声出力・避難路表示・非常食位置表示	会社(xxx-xxxx-xxxx)

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
Ｈ０４Ｍ 11/04	*(2006.01)*	Ｈ０４Ｍ 11/04		

Ｆターム(参考) 5K201 AA07 BA03 CA04 CA06 DC05 DC06 EA05 EC06 ED05 EF04
EF08