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

特許第6704380号
(P6704380)

(45)発行日　令和2年6月3日(2020.6.3)　(24)登録日　令和2年5月14日(2020.5.14)

(51)Int.Cl.		F I		
H04Q 9/00	(2006.01)	H04Q	9/00	301D
H04M 11/00	(2006.01)	H04M	11/00	301
H04W 12/08	(2009.01)	H04W	12/08	
G08B 25/04	(2006.01)	G08B	25/04	H

請求項の数 15　(全 22 頁)

(21)出願番号　特願2017-186198(P2017-186198)
(22)出願日　平成29年9月27日(2017.9.27)
(65)公開番号　特開2019-62432(P2019-62432A)
(43)公開日　平成31年4月18日(2019.4.18)
審査請求日　平成31年3月11日(2019.3.11)

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100165179
弁理士　田▲崎▼　聡
(74)代理人　100175824
弁理士　小林　淳一
(74)代理人　100114937
弁理士　松本　裕幸
(72)発明者　飯田　恵介
東京都新宿区西新宿二丁目３番２号　ＫＤＤＩ株式会社内
(72)発明者　道畑　智也
東京都新宿区西新宿二丁目３番２号　ＫＤＤＩ株式会社内

最終頁に続く

(54)【発明の名称】外部サーバ、通信システムおよび通信方法

(57)【特許請求の範囲】
【請求項１】
宅外に配置された外部サーバであって、
前記外部サーバは、宅内ＩｏＴ（Internet of Things）機器を管理する宅内サーバおよび端末装置と、インターネットを介して通信可能であり、
前記宅内サーバと、前記端末装置とは、移動体通信網を介して通信可能であり、
前記端末装置は、
第１の場合に、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行い、
第２の場合に、前記移動体通信網を介して前記宅内サーバと通信を行い、
前記第１の場合とは、前記宅内ＩｏＴ機器が安全性を要さない機器である場合であって、通信される情報が秘匿情報でない場合であり、
前記第２の場合とは、前記宅内ＩｏＴ機器が安全性を要する機器である場合であるか、あるいは、通信される情報が秘匿情報である場合である、
外部サーバ。
【請求項２】
前記宅内ＩｏＴ機器には、ｅＳＩＭ（Embedded Subscriber Identity Module）が搭載されている、
請求項１に記載の外部サーバ。
【請求項３】

安全性を要する前記宅内ＩｏＴ機器は、鍵の施錠状態を検知する鍵センサである、
請求項１または請求項２に記載の外部サーバ。
【請求項４】
前記第２の場合に、前記宅内サーバは、前記ｅＳＩＭを用いたＳＳＬ（Secure Socket Layer）によって前記宅内ＩｏＴ機器に接続する、
請求項２に記載の外部サーバ。
【請求項５】
前記外部サーバは、前記端末装置からの問い合わせに応じて、前記第１の場合に該当するか、あるいは、前記第２の場合に該当するかを判定する、
請求項１から請求項４のいずれか一項に記載の外部サーバ。
【請求項６】
前記宅内サーバおよび前記外部サーバは、前記宅内ＩｏＴ機器が、安全性を要さない機器であるか、あるいは、安全性を要する機器であるかを示す第１情報を有し、
前記外部サーバは、前記第１情報に基づいて、前記第１の場合に該当するか、あるいは、前記第２の場合に該当するかを判定する、
請求項５に記載の外部サーバ。
【請求項７】
前記外部サーバは、前記外部サーバが有する前記第１情報を、前記宅内サーバが有する前記第１情報に同期させる、
請求項６に記載の外部サーバ。
【請求項８】
前記端末装置は、前記第２の場合に、ＬＴＥ（Long Term Evolution）を介して前記宅内サーバと通信を行う、
請求項１から請求項７のいずれか一項に記載の外部サーバ。
【請求項９】
前記外部サーバは、前記第２の場合における前記端末装置と前記宅内サーバとの間の通信内容についての事後報告を、前記宅内サーバから受ける、
請求項１から請求項８のいずれか一項に記載の外部サーバ。
【請求項１０】
前記宅内サーバは、複数の宅内ＩｏＴ機器の状態に基づいて、宅内に異常が発生したか否かを判定し、
宅内に異常が発生したと前記宅内サーバが判定した場合に、前記外部サーバは、異常が発生したことを示す情報を前記宅内サーバから受信し、
前記外部サーバは、宅内に発生した異常が、警告を要さない異常に該当するか、あるいは、警告を要する異常に該当するかを示す第２情報を有し、
宅内に発生した異常が、警告を要する異常に該当する場合に、前記外部サーバは、警告を要する異常が宅内に発生したことを示す情報を前記端末装置に送信し、前記端末装置は、アラートを出力する、
請求項１から請求項９のいずれか一項に記載の外部サーバ。
【請求項１１】
前記宅内サーバは、前記宅内ＩｏＴ機器と他の宅内ＩｏＴ機器とを含むメッシュネットワークの情報である第３情報を有し、
前記第２の場合であって、前記宅内サーバが前記ＳＳＬによって前記宅内ＩｏＴ機器に接続できない場合には、前記宅内サーバは、前記ＳＳＬによって前記他の宅内ＩｏＴ機器に接続し、次いで、前記他の宅内ＩｏＴ機器は、ＶＰＮ（Virtual Private Network）を介して前記宅内ＩｏＴ機器に接続する、
請求項４に記載の外部サーバ。
【請求項１２】
前記宅内サーバは、データ受信時の回線判別機能を備える、
請求項１から請求項１１のいずれか一項に記載の外部サーバ。

【請求項１３】
前記第２の場合であっても、防犯緊急時には、前記端末装置が、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行う、
請求項１から請求項１２のいずれか一項に記載の外部サーバ。
【請求項１４】
宅内ＩｏＴ機器を管理する宅内サーバと、
宅外に配置された外部サーバと、
端末装置とを備え、
前記宅内サーバと、前記外部サーバとは、インターネットを介して通信可能であり、
前記外部サーバと、前記端末装置とは、前記インターネットを介して通信可能であり、
前記宅内サーバと、前記端末装置とは、移動体通信網を介して通信可能であり、
前記端末装置は、
第１の場合に、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行い、
第２の場合に、前記移動体通信網を介して前記宅内サーバと通信を行い、
前記第１の場合とは、前記宅内ＩｏＴ機器が安全性を要さない機器である場合であって、通信される情報が秘匿情報でない場合であり、
前記第２の場合とは、前記宅内ＩｏＴ機器が安全性を要する機器である場合であるか、あるいは、通信される情報が秘匿情報である場合である、
通信システム。
【請求項１５】
宅内ＩｏＴ機器を管理する宅内サーバと、宅外に配置された外部サーバとが、インターネットを介して通信可能であり、
前記外部サーバと、端末装置とが、前記インターネットを介して通信可能であり、
前記宅内サーバと、前記端末装置とが、移動体通信網を介して通信可能な通信方法であって、
第１の場合に、前記端末装置が、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行うステップと、
第２の場合に、前記端末装置が、前記移動体通信網を介して前記宅内サーバと通信を行うステップとを含み、
前記第１の場合とは、前記宅内ＩｏＴ機器が安全性を要さない機器である場合であって、通信される情報が秘匿情報でない場合であり、
前記第２の場合とは、前記宅内ＩｏＴ機器が安全性を要する機器である場合であるか、あるいは、通信される情報が秘匿情報である場合である、
通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、外部サーバ、通信システムおよび通信方法に関する。
【背景技術】
【０００２】
従来より、インターネットには、パソコンやサーバ等のＩＴ（Information Technology）関連機器が接続されている。さらに、テレビやデジタルカメラ等のデジタル情報家電又は各種センサデバイス等もインターネットに直接接続されるようになり、このような機器はＩｏＴ（Internet of Things）機器と呼ばれる（例えば特許文献１参照）。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１６－１９２１２６号公報
【発明の概要】

【発明が解決しようとする課題】
【０００４】
一般的なＩｏＴサービスでは、ビックデータ等の処理や開発コスト低減を目的として、クラウドサーバとユーザ端末とが、インターネットを介して通信を行う。この場合、インターネットのセキュリティリスクにより、特に鍵センサなどの宅内ＩｏＴ機器を操作する際に、安全性が大きな課題となる。
本発明は、上記問題に鑑みて為されたものであり、宅内ＩｏＴ機器が安全性を要する機器であるか否かに応じて適切に端末装置が宅内サーバと通信することができる外部サーバ、通信システムおよび通信方法を提供することを目的とする。
【課題を解決するための手段】
【０００５】
本発明の一態様は、宅外に配置された外部サーバであって、前記外部サーバは、宅内ＩｏＴ（Internet of Things）機器を管理する宅内サーバおよび端末装置と、インターネットを介して通信可能であり、前記宅内サーバと、前記端末装置とは、移動体通信網を介して通信可能であり、前記端末装置は、第１の場合に、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行い、第２の場合に、前記移動体通信網を介して前記宅内サーバと通信を行い、前記第１の場合とは、前記宅内ＩｏＴ機器が安全性を要さない機器である場合であって、通信される情報が秘匿情報でない場合であり、前記第２の場合とは、前記宅内ＩｏＴ機器が安全性を要する機器である場合であるか、あるいは、通信される情報が秘匿情報である場合である、外部サーバである。
宅内サーバとは、物理的に宅内に配置されるサーバであるか否かを問わない。宅内サーバは、宅内ネットワークにアクセス可能であれば足りる。
【０００６】
本発明の一態様では、前記宅内ＩｏＴ機器には、ｅＳＩＭ（Embedded Subscriber Identity Module）が搭載されていてもよい。
【０００８】
本発明の一態様では、安全性を要する前記宅内ＩｏＴ機器は、鍵の施錠状態を検知する鍵センサであってもよい。
【０００９】
本発明の一態様では、前記第２の場合に、前記宅内サーバは、前記ｅＳＩＭを用いたＳＳＬ（Secure Socket Layer）によって前記宅内ＩｏＴ機器に接続してもよい。
【００１０】
本発明の一態様では、前記外部サーバは、前記端末装置からの問い合わせに応じて、前記第１の場合に該当するか、あるいは、前記第２の場合に該当するかを判定してもよい。
【００１１】
本発明の一態様では、前記宅内サーバおよび前記外部サーバは、前記宅内ＩｏＴ機器が、安全性を要さない機器であるか、あるいは、安全性を要する機器であるかを示す第１情報を有し、前記外部サーバは、前記第１情報に基づいて、前記第１の場合に該当するか、あるいは、前記第２の場合に該当するかを判定してもよい。
【００１２】
本発明の一態様では、前記外部サーバは、前記外部サーバが有する前記第１情報を、前記宅内サーバが有する前記第１情報に同期させてもよい。
【００１３】
本発明の一態様では、前記端末装置は、前記第２の場合に、ＬＴＥ（Long Term Evolution）を介して前記宅内サーバと通信を行ってもよい。
【００１４】
本発明の一態様では、前記外部サーバは、前記第２の場合における前記端末装置と前記宅内サーバとの間の通信内容についての事後報告を、前記宅内サーバから受けてもよい。
【００１５】
本発明の一態様では、前記宅内サーバは、複数の宅内ＩｏＴ機器の状態に基づいて、宅

内に異常が発生したか否かを判定し、宅内に異常が発生したと前記宅内サーバが判定した場合に、前記外部サーバは、異常が発生したことを示す情報を前記宅内サーバから受信し、前記外部サーバは、宅内に発生した異常が、警告を要さない異常に該当するか、あるいは、警告を要する異常に該当するかを示す第２情報を有し、宅内に発生した異常が、警告を要する異常に該当する場合に、前記外部サーバは、警告を要する異常が宅内に発生したことを示す情報を前記端末装置に送信し、前記端末装置は、アラートを出力してもよい。

【００１６】

本発明の一態様では、前記宅内サーバは、前記宅内ＩｏＴ機器と他の宅内ＩｏＴ機器とを含むメッシュネットワークの情報である第３情報を有し、前記第２の場合であって、前記宅内サーバが前記ＳＳＬによって前記宅内ＩｏＴ機器に接続できない場合には、前記宅内サーバは、前記ＳＳＬによって前記他の宅内ＩｏＴ機器に接続し、次いで、前記他の宅内ＩｏＴ機器は、ＶＰＮ（Virtual Private Network）を介して前記宅内ＩｏＴ機器に接続してもよい。

【００１７】

本発明の一態様では、前記宅内サーバは、データ受信時の回線判別機能を備えてもよい。

【００１８】

本発明の一態様では、前記第２の場合であっても、防犯緊急時には、前記端末装置が、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行ってもよい。

【００１９】

本発明の一態様は、宅内ＩｏＴ機器を管理する宅内サーバと、宅外に配置された外部サーバと、端末装置とを備え、前記宅内サーバと、前記外部サーバとは、インターネットを介して通信可能であり、前記外部サーバと、前記端末装置とは、前記インターネットを介して通信可能であり、前記宅内サーバと、前記端末装置とは、移動体通信網を介して通信可能であり、前記端末装置は、第１の場合に、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行い、第２の場合に、前記移動体通信網を介して前記宅内サーバと通信を行い、前記第１の場合とは、前記宅内ＩｏＴ機器が安全性を要さない機器である場合であって、通信される情報が秘匿情報でない場合であり、前記第２の場合とは、前記宅内ＩｏＴ機器が安全性を要する機器である場合であるか、あるいは、通信される情報が秘匿情報である場合である、通信システムである。

【００２０】

本発明の一態様は、宅内ＩｏＴ機器を管理する宅内サーバと、宅外に配置された外部サーバとが、インターネットを介して通信可能であり、前記外部サーバと、端末装置とが、前記インターネットを介して通信可能であり、前記宅内サーバと、前記端末装置とが、移動体通信網を介して通信可能な通信方法であって、第１の場合に、前記端末装置が、前記インターネットおよび前記外部サーバを介して前記宅内サーバと通信を行うステップと、第２の場合に、前記端末装置が、前記移動体通信網を介して前記宅内サーバと通信を行うステップとを含み、前記第１の場合とは、前記宅内ＩｏＴ機器が安全性を要さない機器である場合であって、通信される情報が秘匿情報でない場合であり、前記第２の場合とは、前記宅内ＩｏＴ機器が安全性を要する機器である場合であるか、あるいは、通信される情報が秘匿情報である場合である、通信方法である。

【発明の効果】

【００２１】

本発明によれば、宅内ＩｏＴ機器が安全性を要する機器であるか否かに応じて適切に端末装置が宅内サーバと通信することができる外部サーバ、通信システムおよび通信方法を提供することができる。

【図面の簡単な説明】

【００２２】

【図１】第１実施形態の外部サーバが適用された通信システムの構成の一例を示す図であ

る。
【図２】図１に示す宅内サーバ、外部サーバ、端末装置などの概要を示す図である。
【図３】図１に示す宅内サーバおよび端末装置の機能構成の一例を示す図である。
【図４】図１に示す外部サーバの機能構成の一例を示す図である。
【図５】第１の場合に実行される処理を説明するためのシーケンス図である。
【図６】第２の場合に実行される処理を説明するためのシーケンス図である。
【図７】第２実施形態の外部サーバが適用された通信システムにおいて図６のステップＳ３０４の前に実行される処理を説明するためのシーケンス図である。
【図８】第３実施形態の外部サーバが適用された通信システムにおいて図６のステップＳ３１１の後に実行される処理を説明するためのシーケンス図である。
【発明を実施するための形態】
【００２３】
以下、図面を参照して本発明の外部サーバ、通信システムおよび通信方法の実施形態について説明する。
【００２４】
［第１実施形態］
図１は、第１実施形態の外部サーバ１３が適用された通信システム１の構成の一例を示す図である。図１に示す例では、通信システム１が、宅内サーバ１２と、外部サーバ１３と、端末装置１４とを備えている。宅内サーバ１２は、例えば通信システム１のユーザの例えば自宅である住宅Ａの宅内に配置されている。宅内サーバ１２は、住宅Ａの宅内に配置された宅内ＩｏＴ（Internet of Things）機器１１、１１－１を管理する。ＩｏＴ機器１１、１１－１は、インターネットＩＮに接続可能な機器であり、例えば照明、テレビ、デジタルカメラ等のデジタル情報家電、例えば鍵センサ等の各種センサデバイスなどである。宅内サーバ１２は、物理的に住宅Ａの宅内に配置されていても、住宅Ａの宅外に配置されていてもよい。宅内サーバ１２とは、宅内ネットワークにアクセス可能であり、住宅Ａの宅内に配置された宅内ＩｏＴ機器１１、１１－１を管理できるものである。
【００２５】
図１に示す例では、ｅＳＩＭ（Embedded Subscriber Identity Module）１１Ａが宅内ＩｏＴ機器１１に搭載されており、ｅＳＩＭ１１Ａ－１が宅内ＩｏＴ機器１１－１に搭載されている。他の例では、宅内ＩｏＴ機器１１、１１－１がｅＳＩＭを搭載していなくてもよい。つまり、ｅＳＩＭが宅内ＩｏＴ機器の全部又は一部に搭載されていてもよいし、搭載されていなくてもよい。
【００２６】
図１に示す例では、外部サーバ１３は、住宅Ａの宅外に配置されているクラウドサーバである。他の例では、外部サーバ１３が、住宅Ａの宅外に配置されているクラウドサーバ以外のサーバであってもよい。
宅内サーバ１２と、外部サーバ１３とは、インターネットＩＮを介して通信可能である。つまり、図１に示す例では、宅内ＩｏＴ機器１１、１１－１が、宅内サーバ１２を介してインターネットＩＮに接続可能である。
【００２７】
端末装置１４は、例えば通信システム１のユーザによって携帯される。外部サーバ１３と、端末装置１４とは、インターネットＩＮを介して通信可能である。また、宅内サーバ１２と、端末装置１４とは、インターネットＩＮを介することなく、移動体通信網ＭＮを介することによっても通信可能である。
【００２８】
図２は、図１に示す宅内サーバ１２、外部サーバ１３、端末装置１４などの概要を示す図である。宅内サーバ１２は、端末装置１４から受信するデータ（例えば、音楽、写真及び動画等）を管理する。宅内サーバ１２は、ハードディスクドライブやＲＯＭ（Read Only Memory）などの記憶部１２Ｅを備えている。この記憶部１２Ｅには、端末装置１４から送信される写真や動画、音楽などのデータが保存される。この記憶部１２Ｅに記憶され

るデータは、端末装置１４が読み出すことも可能である。この場合、宅内サーバ１２は、端末装置１４のファイルサーバとして機能する。また、記憶部１２Ｅには、宅内ＩｏＴ機器１１、１１－１のリストＩＦ１が第１情報として登録され、記憶されている。

宅内サーバ１２および外部サーバ１３には、同期により、全部又は一部の同一のデータが記憶されていてもよい。

【００２９】

宅内サーバ１２は、端末装置１４との間のデータの送受信を、通信によって行う。この宅内サーバ１２が行う通信には、さまざまな方式がある。例えば、宅内サーバ１２が行う通信には、ＢＬＥ（Bluetooth（登録商標） Low Energy）やＷｉ－Ｆｉ（登録商標）による近距離無線通信、ＬＴＥ（Long Term Evolution）などの移動体通信網ＭＮを介した無線通信、赤外線による無線通信、インターネットＩＮおよび外部サーバ１３を介した通信などの方式がある。

ここでは、宅内サーバ１２が、端末装置１４との間においてＢＬＥ、Ｗｉ－Ｆｉ、ＬＴＥおよびインターネットＩＮによって通信が可能である場合について説明する。

【００３０】

この一例では、宅内サーバ１２は、Ｗｉ－Ｆｉによる近距離無線通信を行うルータＲＴがユーザの宅内に設置されているか否かによって、端末装置１４との間の通信方式を選択する。宅内サーバ１２は、ユーザの宅内にルータＲＴが設置されている場合には、Ｗｉ－Ｆｉによってデータの授受を行う。宅内サーバ１２は、ユーザの宅内にルータＲＴが設置されていない場合には、ＬＴＥまたはインターネットＩＮによってデータの授受を行う。

【００３１】

端末装置１４は、可搬型の装置であり、ユーザの操作に応じて無線通信を行う。端末装置１４とは、例えば、携帯電話、スマートフォン及びタブレット型のコンピュータ（タブレットＰＣ）等の携帯型のパーソナルコンピュータなどである。

【００３２】

宅内サーバ１２および端末装置１４は、移動体通信網ＭＮを利用するサービスに加入する加入者を識別するための識別チップを備える。この識別チップとは、例えば、ＳＩＭ（Subscriber Identity Module）である。このＳＩＭには、ＩＭＳＩ（International Mobile Subscriber Identity）が、加入者を識別する加入者識別子ＩＤとして記憶されている。

ＬＴＥなどの移動体通信網ＭＮを介した通信サービスは、通信事業者によって提供される。通信事業者は、ＩＭＳＩ（加入者識別子ＩＤ）と、電話番号とを対応付けて加入者の装置による通信を管理する。宅内サーバ１２及び端末装置１４は、ＳＩＭを装着することにより、移動体通信網ＭＮを介した相互の通信が可能になる。

【００３３】

宅内サーバ１２に装着されているＳＩＭの加入者識別子は、識別子ＩＤ１である。また、端末装置１４に装着されているＳＩＭの加入者識別子は、識別子ＩＤ２である。

【００３４】

「ルータ経由無線ＬＡＮ方式」では、宅内サーバ１２がルータＲＴを経由して端末装置１４とデータの授受を行う。ルータＲＴが宅内サーバ１２に備えられていてもよい。

「ＬＴＥ経由方式」では、宅内サーバ１２がルータＲＴを経由せずに、ＬＴＥなどの移動体通信網ＭＮを介して端末装置１４とデータの授受を行う。

また、宅内サーバ１２は、ルータＲＴを経由せずに、インターネットＩＮおよび外部サーバ１３を介して端末装置１４とデータの授受を行うこともできる。

【００３５】

宅内サーバ１２や端末装置１４を使用するすべてのユーザがＷｉ－Ｆｉ等の通信設定に詳しいとは限らない。通信設定に詳しくないユーザの場合、ユーザは、宅内にルータＲＴが設置されているか否かを把握していない場合がある。また、このようなユーザの場合、ユーザは、宅内にルータＲＴが設置されていることを把握していても、ルータＲＴと宅内サーバ１２との間の通信設定や、ルータＲＴと端末装置１４との間の通信設定を滞りなく

行えるとは限らない。
宅内サーバ１２は、宅内サーバ１２と端末装置１４との間の通信設定を自動的に行うことにより、上述したような通信設定に詳しくないユーザに対する支援を行う。
【００３６】
図３は、図１に示す宅内サーバ１２および端末装置１４の機能構成の一例を示す図である。図３に示す例では、端末装置１４は、Ｗｉ－Ｆｉ無線通信部１４Ａと、ＢＬＥ無線通信部１４Ｂと、ＬＴＥ無線通信部１４Ｃと、操作部１４Ｄと、表示部１４Ｅと、ＣＰＵ（Central Processing Unit）１４Ｆと、記憶部１４Ｇと、ＳＩＭ１４Ｈとを備える。これら各部は、内部バスによって相互に接続される。
Ｗｉ－Ｆｉ無線通信部１４Ａは、他の通信機器との間においてＷｉ－Ｆｉ方式によって無線通信を行う。
ＢＬＥ無線通信部１４Ｂは、他の通信機器との間においてＢＬＥ方式によって無線通信を行う。
ＬＴＥ無線通信部１４Ｃは、他の通信機器との間においてＬＴＥ方式によって無線通信を行う。
【００３７】
操作部１４Ｄは、入力デバイスを備え、ユーザの操作を受け付ける。この入力デバイスには、キーボード等の文字情報を入力するデバイス、マウス、タッチパネル等のポインティングデバイス、ボタン、ダイヤル、ジョイスティック、タッチセンサ、タッチパッド等が含まれる。
表示部１４Ｅは、ＣＰＵ１４Ｆによって制御され、画像、ＧＵＩ（Graphical User Interface）等を表示する。この一例では、操作部１４Ｄとは、タッチパネルである。
【００３８】
記憶部１４Ｇは、例えば、ハードディスクドライブやＲＯＭ等を備え、記憶部１４Ｇには、端末装置１４を制御するためのプログラムなどが記憶されている。
ルータ経由方式の場合、記憶部１４Ｇには、端末装置１４がルータＲＴにアクセスするための鍵情報ＫＹＲが記憶される。鍵情報ＫＹＲとは、例えば、ＷＥＰ（Wired Equivalent Privacy）等の暗号化キーである。
ここで、宅内サーバ１２と、端末装置１４とがルータ経由無線ＬＡＮ方式の通信によってデータの授受を行う場合、端末装置１４は、ルータＲＴが提供する無線通信にアクセスするための鍵情報ＫＹＲを用いる。この一例では、端末装置１４は、ルータＲＴが提供する無線通信に予め接続される。このため、端末装置１４は、記憶部１４Ｇに鍵情報ＫＹＲが記憶される。
【００３９】
ＣＰＵ１４Ｆは、記憶部１４Ｇに格納されるプログラムを実行し、端末装置１４の各部を制御する。例えば、ＣＰＵ１４Ｆは、Ｗｉ－Ｆｉ無線通信部１４Ａ、ＢＬＥ無線通信部１４Ｂ、及びＬＴＥ無線通信部１４Ｃを制御することにより、他の機器との間において無線通信を行う。また、例えば、ＣＰＵ１４Ｆは、インターネットＩＮへのアクセスによって得られた画像、音声などのデータを、記憶部１４Ｇに記憶させる。また、ＣＰＵ１４Ｆは、記憶部１４Ｇに記憶させたこれらのデータを、無線通信を介して宅内サーバ１２に送信する。
【００４０】
宅内サーバ１２は、Ｗｉ－Ｆｉ無線通信部１２Ａと、ＢＬＥ無線通信部１２Ｂと、ＬＴＥ無線通信部１２Ｃと、ＣＰＵ１２Ｄと、記憶部１２Ｅと、ＳＩＭ１２Ｆとを備える。これら各部は、内部バスによって相互に接続される。
【００４１】
Ｗｉ－Ｆｉ無線通信部１２Ａは、他の通信機器との間においてＷｉ－Ｆｉ方式によって無線通信を行う。
ＢＬＥ無線通信部１２Ｂは、他の通信機器との間においてＢＬＥ方式によって無線通信を行う。

ＬＴＥ無線通信部１２Ｃは、他の通信機器との間においてＬＴＥ方式によって無線通信を行う。

【００４２】

記憶部１２Ｅは、例えば、ハードディスクドライブやＲＯＭ等を備え、記憶部１２Ｅには、宅内サーバ１２を制御するためのプログラムなどが記憶されている。

ルータ経由方式の場合、記憶部１２Ｅには、宅内サーバ１２がルータＲＴにアクセスするための鍵情報ＫＹＲが記憶される。この鍵情報ＫＹＲとは、端末装置１４に記憶されている鍵情報ＫＹＲと同一の鍵情報であり、例えば、ＷＥＰ等の暗号化キーである。この一例では、宅内サーバ１２は、ルータＲＴが提供する無線通信に予め接続されていない。このため、宅内サーバ１２は、端末装置１４から鍵情報ＫＹＲを取得し、記憶部１２Ｅに記憶させる。

【００４３】

ＣＰＵ１２Ｄは、記憶部１２Ｅに格納されるプログラムを実行し、宅内サーバ１２の各部を制御する。例えば、ＣＰＵ１２Ｄは、Ｗｉ－Ｆｉ無線通信部１２Ａ、ＢＬＥ無線通信部１２Ｂ、及びＬＴＥ無線通信部１２Ｃを制御することにより、他の機器との間において無線通信を行う。

【００４４】

また、ＣＰＵ１２Ｄは、選択部１２Ｄ１をその機能部として備える。

選択部１２Ｄ１は、端末装置１４との間の無線通信の接続状態を示す情報（接続状態情報ＣＤ１）に基づいて、宅内サーバ１２と端末装置１４との間の通信方式を選択する。接続状態情報ＣＤ１とは、端末装置１４が受信可能な無線通信の無線通信識別情報の一覧を示す情報である。この無線通信識別情報の一例として、無線ＬＡＮのアクセスポイントを識別するＳＳＩＤ（Service Set Identifier）がある。

【００４５】

アクセスポイントには、固有のＳＳＩＤが割り当てられている。アクセスポイントは、周囲の無線通信装置に対してＳＳＩＤを通知する。端末装置１４は、アクセスポイントからＳＳＩＤを受信すると、受信したＳＳＩＤを一覧にした接続状態情報ＣＤ１を生成する。端末装置１４は、ＢＬＥ方式の無線通信によって、接続状態情報ＣＤ１を宅内サーバ１２に通知する。

ルータＲＴが宅内に設置されている場合、端末装置１４は、ルータＲＴのＳＳＩＤを受信する。この場合、端末装置１４が生成する接続状態情報ＣＤ１には、ルータＲＴのＳＳＩＤが含まれている。したがって、ルータＲＴが宅内に設置されている場合、端末装置１４が宅内サーバ１２に通知する接続状態情報ＣＤ１には、ルータＲＴのＳＳＩＤが含まれている。

つまり、端末装置１４は、接続状態情報ＣＤ１によって、ルータＲＴが宅内に設置されているか否かを宅内サーバ１２に通知する。

【００４６】

ＢＬＥ無線通信部１２Ｂは、接続状態情報ＣＤ１をＢＬＥ方式の無線通信によって受信する。選択部１２Ｄ１は、ＢＬＥ無線通信部１２Ｂが受信した接続状態情報ＣＤ１に基づいて、宅内サーバ１２の通信方式を選択する。

ルータＲＴが宅内に設置されている場合、接続状態情報ＣＤ１には、ルータＲＴのＳＳＩＤが含まれる。この場合、選択部１２Ｄ１は、ルータ経由方式を、宅内サーバ１２と端末装置１４との間の無線通信方式として選択する。

【００４７】

上述したように、宅内サーバ１２がルータＲＴとの通信を行う場合、鍵情報ＫＹＲが必要である。

ルータ経由方式が選択される場合、宅内サーバ１２は、ＢＬＥ方式の無線通信によって、端末装置１４から鍵情報ＫＹＲを受信する。宅内サーバ１２は、受信した鍵情報ＫＹＲに基づいて、ルータＲＴとの通信設定を行う。これにより、宅内サーバ１２は、端末装置１４との間において、ルータ経由方式によってデータの送受信を行う。

上記設定方法はあくまで一例である。この一例に従った場合、つまり、ルータ経由方式が選択される場合、ネットワーク設定が不得手なユーザであっても、ルータ経由方式によってデータの送受信を行うことができる。

【００４８】

図４は、図１に示す外部サーバ１３の機能構成の一例を示す図である。

図４に示す例では、外部サーバ１３が、通信部１３Ａと、記憶部１３Ｂと、ＣＰＵ１３Ｃとを備えている。通信部１３Ａは、インターネットＩＮを介して宅内サーバ１２および端末装置１４との通信を行う。記憶部１３Ｂは、例えば、ＲＯＭ及びＲＡＭ（Random Access Memory）等により構成される。記憶部１３Ｂは、外部サーバ１３を機能させるための各種プログラムを記憶する。記憶部１３Ｂは、インターネットＩＮを介して外部機器からダウンロードされたプログラムを記憶してもよい。記憶部１３Ｂは、例えば、宅内サーバ１２の記憶部１２Ｅに記憶されているリストＩＦ１に同期させて、リストＩＦ１を第１情報として記憶する。

【００４９】

ＣＰＵ１３Ｃは、記憶部１３Ｂに記憶されている各種プログラムを実行することにより、外部サーバ１３に係る機能を統括的に制御する。ＣＰＵ１３Ｃは、例えば、受信処理部１３Ｃ１と、送信処理部１３Ｃ２と、登録処理部１３Ｃ３と、判定処理部１３Ｃ４とを備えている。受信処理部１３Ｃ１は、通信部１３Ａを介してインターネットＩＮから各種情報を受信する。受信処理部１３Ｃ１は、インターネットＩＮを介してリストＩＦ１を宅内サーバ１２から定期的に受信する。その結果、外部サーバ１３は、宅内サーバ１２が有するリストＩＦ１の情報に同期するリストＩＦ１の情報を有することができる。

【００５０】

送信処理部１３Ｃ２は、通信部１３Ａを介してインターネットＩＮに各種情報を送信する。登録処理部１３Ｃ３は、例えば受信処理部１３Ｃ１が受信したリストＩＦ１を登録し、記憶部１３Ｂに記憶させる。判定処理部１３Ｃ４は、後述する第１の場合であるか、あるいは、第２の場合であるか等の判定を行う。

【００５１】

図５は、第１の場合に実行される処理を説明するためのシーケンス図である。

第１の場合とは、端末装置１４と宅内サーバ１２との間で通信される情報が、例えば照明機器のＯＮ／ＯＦＦ情報などのような安全性を要さない宅内ＩｏＴ機器１１に関する情報であって、秘匿情報ではない情報の場合である。

【００５２】

図５に示す例では、宅内ＩｏＴ機器１１（例えば照明機器）を含むリストＩＦ１が、宅内サーバ１２の記憶部１２Ｅに登録され、記憶されている。

ステップＳ２０１では、外部サーバ１３のＣＰＵ１３Ｃの受信処理部１３Ｃ１が、宅内サーバ１２の記憶部１２Ｅに登録されているリストＩＦ１を定期的に受信し、リストＩＦ１の同期を行う。

ステップＳ２０２では、外部サーバ１３のＣＰＵ１３Ｃの登録処理部１３Ｃ３は、受信処理部１３Ｃ１が受信したリストＩＦ１の登録を行い、記憶部１３ＢがリストＩＦ１を記憶する。

ステップＳ２０３では、端末装置１４が、外部サーバ１３に対して宅内ＩｏＴ機器１１のＩＤの問い合わせを行う。その問い合わせには、宅内ＩｏＴ機器１１がどの宅に存在するものであるかも含まれる。端末装置１４と外部サーバ１３との間では、インターネットＩＮを介する通信が行われる。他の例では、端末装置１４と外部サーバ１３との間において、例えばＬＴＥまたはＷｉ－Ｆｉによる通信が行われてもよい。

【００５３】

ここで、宅内サーバ１２が、例えば宅内ＩｏＴ機器１１に搭載されたｅＳＩＭ１１Ａを用いたＳＳＬ（Secure Socket Layer）によって宅内ＩｏＴ機器１１に接続してもよい。他の例では、宅内サーバ１２がＳＳＬ以外の手法によって宅内ＩｏＴ機器１１に接続してもよい。

【００５４】
ステップＳ２０４では、外部サーバ１３のＣＰＵ１３Ｃの判定処理部１３Ｃ４が、記憶部１３Ｂに記憶されているリストＩＦ１を参照する。
ステップＳ２０５では、外部サーバ１３のＣＰＵ１３Ｃの判定処理部１３Ｃ４が、リストＩＦ１に基づいて、第１の場合に該当するか、あるいは、第２の場合に該当するかを判定する。詳細には、判定処理部１３Ｃ４は、問い合わせ対象の宅内ＩｏＴ機器１１（例えば照明機器）に関する情報が秘匿情報ではなく、問い合わせ対象の宅内ＩｏＴ機器１１が安全性を要さない宅内ＩｏＴ機器であり、第１の場合に該当すると判定する。
ステップＳ２０６では、外部サーバ１３が、ステップＳ２０５の判定結果（つまり、問い合わせ対象の宅内ＩｏＴ機器１１が安全性を要さない宅内ＩｏＴ機器である旨）を端末装置１４に回答する。
【００５５】
ステップＳ２０７では、端末装置１４が、端末装置１４による操作対象の宅内ＩｏＴ機器１１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１の操作内容（操作指示）を、外部サーバ１３に対してインターネットＩＮを介して送信する。
ステップＳ２０８では、外部サーバ１３が、端末装置１４による操作対象の宅内ＩｏＴ機器１１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１の操作内容（操作指示）を、宅内サーバ１２に対してインターネットＩＮを介して送信する。
このように宅内サーバ１２を介させることにより、宅内ＩｏＴ機器１１などに複数のプロトコル（例えばWi-Fi Halow（登録商標）、Z-Waveなど）が濫立していても、一元的にプロトコル変換することにより、ユーザ目線ではプロトコルに関係なく使えて利便性が高まる。
ステップＳ２０８において、外部サーバ１３が、それらを（宅内サーバ１２を介することなく）インターネットＩＮ及びＬＴＥ経由で宅内ＩｏＴ機器１１に直接送信することもできる。
【００５６】
ステップＳ２０９では、宅内サーバ１２のＣＰＵ１２Ｄが、記憶部１２Ｅに記憶されているリストＩＦ１を参照する。
ステップＳ２１０では、宅内サーバ１２のＣＰＵ１２Ｄが、インターネットプロトコルからＳＳＬプロトコルへのプロトコル変換を行う。
ステップＳ２１１では、宅内サーバ１２が、例えば宅内ＩｏＴ機器１１に搭載されたｅＳＩＭ１１Ａを用いたＳＳＬによって、端末装置１４による操作対象の宅内ＩｏＴ機器１１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１の操作内容（操作指示）を宅内ＩｏＴ機器１１に送信する。その結果、端末装置１４による操作指示に基づいて、宅内ＩｏＴ機器１１が操作される（例えば、照明装置がＯＮからＯＦＦに切り替えられる）。他の例では、ステップＳ２１１において、宅内サーバ１２がＳＳＬ以外の手法によって宅内ＩｏＴ機器１１に宅内ＩｏＴ機器１１のＩＤおよび操作内容（操作指示）を宅内ＩｏＴ機器１１に送信してもよい。
【００５７】
図６は、第２の場合に実行される処理を説明するためのシーケンス図である。
第２の場合とは、端末装置１４と宅内サーバ１２との間で通信される情報が、例えば鍵センサが検知した鍵の解錠状態／施錠状態の情報などのような安全性を要する宅内ＩｏＴ機器１１－１に関する情報であって、秘匿情報の場合である。
【００５８】
図６に示す例では、宅内ＩｏＴ機器１１－１（例えば鍵センサ）を含むリストＩＦ１が、宅内サーバ１２の記憶部１２Ｅに登録され、記憶されている。
ステップＳ３０１では、外部サーバ１３のＣＰＵ１３Ｃの受信処理部１３Ｃ１が、宅内サーバ１２の記憶部１２Ｅに登録されているリストＩＦ１を定期的に受信し、リストＩＦ１の同期を行う。
ステップＳ３０２では、外部サーバ１３のＣＰＵ１３Ｃの登録処理部１３Ｃ３は、受信

処理部１３Ｃ１が受信したリストＩＦ１の登録を行い、記憶部１３Ｂがリスト
ＩＦ１を記憶する。
ステップＳ３０３では、宅内サーバ１２が、例えば宅内ＩｏＴ機器１１－１に搭載されたｅＳＩＭ１１Ａ－１を用いたＳＳＬによって宅内ＩｏＴ機器１１－１に接続する。
【００５９】
ステップＳ３０４では、端末装置１４が、外部サーバ１３に対して宅内ＩｏＴ機器１１－１のＩＤの問い合わせを行う。端末装置１４と外部サーバ１３との間では、インターネットＩＮを介する通信が行われる。他の例では、端末装置１４と外部サーバ１３との間において、例えばＬＴＥまたはＷｉ－Ｆｉによる通信が行われてもよい。
【００６０】
ステップＳ３０５では、外部サーバ１３のＣＰＵ１３Ｃの判定処理部１３Ｃ４が、記憶部１３Ｂに記憶されているリストＩＦ１を参照する。
ステップＳ３０６では、外部サーバ１３のＣＰＵ１３Ｃの判定処理部１３Ｃ４が、リストＩＦ１に基づいて、第１の場合に該当するか、あるいは、第２の場合に該当するかを判定する。詳細には、判定処理部１３Ｃ４は、問い合わせ対象の宅内ＩｏＴ機器１１－１（例えば鍵センサ）に関する情報が秘匿情報であり、問い合わせ対象の宅内ＩｏＴ機器１１－１が安全性を要する宅内ＩｏＴ機器であり、第２の場合に該当すると判定する。
ステップＳ３０７では、外部サーバ１３が、ステップＳ３０６の判定結果（つまり、問い合わせ対象の宅内ＩｏＴ機器１１－１が安全性を要する宅内ＩｏＴ機器である旨）を端末装置１４に回答する。
【００６１】
ステップＳ３０８では、端末装置１４が、例えば端末装置１４にインストールされたアプリにより、通信接続先を外部サーバ１３から宅内サーバ１２に切り替える。
ステップＳ３０９では、端末装置１４が、端末装置１４による操作対象の宅内ＩｏＴ機器１１－１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１－１の操作内容（操作指示）を、宅内サーバ１２に対して移動体通信網ＭＮ（詳細にはＬＴＥ）を介して送信する。
【００６２】
ステップＳ３１０では、宅内サーバ１２のＣＰＵ１２Ｄが、記憶部１２Ｅに記憶されているリストＩＦ１を参照する。
ステップＳ３１１では、宅内サーバ１２のＣＰＵ１２Ｄが、ＬＴＥプロトコルからＳＳＬプロトコルへのプロトコル変換を行う。
ステップＳ３１２では、宅内サーバ１２が、宅内ＩｏＴ機器１１－１に搭載されたｅＳＩＭ１１Ａ－１を用いたＳＳＬによって、端末装置１４による操作対象の宅内ＩｏＴ機器１１－１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１－１の操作内容（操作指示）を宅内ＩｏＴ機器１１－１に送信する。その結果、端末装置１４による操作指示に基づいて、宅内ＩｏＴ機器１１－１が操作され、例えば鍵センサの検知対象の鍵が解錠状態から施錠状態に切り替えられる。
【００６３】
ステップＳ３１３では、宅内サーバ１２が、ステップＳ３０９における端末装置１４から宅内サーバ１２への通信データ（通信内容）を、外部サーバ１３に定期的に事後報告として送信する。
【００６４】
＜第１実施形態のまとめ＞
第１実施形態の外部サーバ１３が適用された通信システム１では、図１に示すように、宅内ＩｏＴ機器１１、１１－１を管理する宅内サーバ１２と、宅外に配置された外部サーバ１３と、端末装置１４とが備えられている。また、宅内サーバ１２と、外部サーバ１３とは、インターネットＩＮを介して通信可能である。外部サーバ１３と、端末装置１４とは、インターネットＩＮを介して通信可能である。また、宅内サーバ１２と、端末装置１４とは、インターネットＩＮを介することなく、移動体通信網ＭＮを介して通信可能であ

る。端末装置１４は、第１の場合に、インターネットおよび外部サーバ１３を介して宅内サーバ１２と通信を行う。また、端末装置１４は、第２の場合に、移動体通信網ＭＮ（詳細には例えばＬＴＥ）を介して宅内サーバ１２と通信を行う。

図５を参照して説明したように、第１の場合とは、宅内ＩｏＴ機器１１が安全性を要さない機器（例えば照明機器）である場合であって、通信される情報（例えば照明機器のＯＮ／ＯＦＦ情報）が秘匿情報でない場合である。

図６を参照して説明したように、第２の場合とは、宅内ＩｏＴ機器１１－１が安全性を要する機器（例えば鍵の施錠状態を検知する鍵センサ）である場合であるか、あるいは、通信される情報（例えば鍵センサが検知した鍵の解錠状態／施錠状態の情報）が秘匿情報である場合である。

第１の場合／第２の場合の振り分け方は、一例であり、任意に決めることができる。また、第１の場合・第２の場合は例示であり、これに限定されない。つまり、第１の場合にも、第２の場合にも該当しない第３の場合を設け、第３の場合に別のアクションをとってもよい。

図１に示すように、宅内ＩｏＴ機器１１には、ｅＳＩＭ１１Ａが搭載されており、宅内ＩｏＴ機器１１－１には、ｅＳＩＭ１１Ａ－１が搭載されている。

そのため、第１実施形態の外部サーバ１３が適用された通信システム１では、端末装置１４は、宅内ＩｏＴ機器１１、１１－１が安全性を要する機器であるか否かに応じて適切に宅内サーバ１２と通信することができる。宅内ＩｏＴ機器１１－１が安全性を要する場合（第２の場合）には、高度の安全性を確保した通信を行うことによって、ユーザの安心感を獲得することができる。

【００６５】

第１実施形態の外部サーバ１３が適用された通信システム１では、第２の場合に、図６のステップＳ３１２において、宅内サーバ１２が、ｅＳＩＭ１１Ａ－１を用いたＳＳＬによって宅内ＩｏＴ機器１１－１に接続する。

そのため、第１実施形態の外部サーバ１３が適用された通信システム１では、なりすましによる宅内ＩｏＴ機器１１－１の操作を抑制することができる。

【００６６】

第１実施形態の外部サーバ１３が適用された通信システム１では、外部サーバ１３が、図５のステップＳ２０３または図６のステップＳ３０４における端末装置１４からの問い合わせに応じて、図５のステップＳ２０５または図６のステップＳ３０６において、第１の場合に該当するか、あるいは、第２の場合に該当するかを判定する。

そのため、第１実施形態の外部サーバ１３が適用された通信システム１では、第１の場合に該当するか、あるいは、第２の場合に該当するかの判定が宅内サーバ１２によって行われる場合よりも、宅内サーバ１２を簡略化することができる。

【００６７】

第１実施形態の外部サーバ１３が適用された通信システム１では、図５および図６を参照して説明したように、宅内ＩｏＴ機器１１（例えば照明機器）および宅内ＩｏＴ機器１１－１（例えば鍵センサ）を含むリストＩＦ１が、宅内サーバ１２の記憶部１２Ｅに登録され、記憶されている。つまり、宅内サーバ１２は、宅内ＩｏＴ機器１１、１１－１が、安全性を要さない機器であるか、あるいは、安全性を要する機器であるかを示すリストＩＦ１（第１情報）を有する。

また、宅内ＩｏＴ機器１１（例えば照明機器）および宅内ＩｏＴ機器１１－１（例えば鍵センサ）を含むリストＩＦ１が、図５のステップＳ２０２または図６のステップＳ３０２において、外部サーバ１３のＣＰＵ１３Ｃの登録処理部１３Ｃ３により登録され、記憶部１３Ｂに記憶されている。つまり、外部サーバ１３は、宅内ＩｏＴ機器１１、１１－１が、安全性を要さない機器であるか、あるいは、安全性を要する機器であるかを示すリストＩＦ１（第１情報）を有する。

外部サーバ１３は、図５のステップＳ２０５または図６のステップＳ３０６において、リストＩＦ１（第１情報）に基づいて、第１の場合に該当するか、あるいは、第２の場合

に該当するかを判定する。
　また、外部サーバ１３は、図５のステップＳ２０１または図６のステップＳ３０１において、外部サーバ１３が有するリストＩＦ１（第１情報）を、宅内サーバ１２が有するリストＩＦ１（第１情報）に同期させる。
　そのため、第１実施形態の外部サーバ１３が適用された通信システム１では、外部サーバ１３は、第１の場合に該当するか、あるいは、第２の場合に該当するかを正確に判定することができる。
【００６８】
　第１実施形態の外部サーバ１３が適用された通信システム１では、宅内サーバ１２が、図６のステップＳ３１３において、ステップＳ３０９における端末装置１４から宅内サーバ１２への通信データ（通信内容）を事後報告として、外部サーバ１３に送信する。つまり、外部サーバ１３は、第２の場合における端末装置１４と宅内サーバ１２との間の通信内容についての事後報告を、宅内サーバ１２から受ける。
　そのため、第１実施形態の外部サーバ１３が適用された通信システム１では、外部サーバ１３が、外部サーバ１３を介さない図６のステップＳ３０９における通信内容をビッグデータ化することができる。つまり、外部サーバ１３は、宅内サーバ１２よりも高いスペックを有し、例えばビッグデータの分析等の能力が、宅内サーバ１２に勝っている。
【００６９】
　上述したように、第１実施形態の外部サーバ１３が適用された通信システム１では、鍵センサなどの安全性が求められる宅内ＩｏＴ機器１１－１に、ｅＳＩＭ１１Ａ－１が導入される。そして、端末装置１４と宅内サーバ１２との間が、そもそもインターネットＩＮを介することなく、通信事業者の例えばセルラー回線（ＬＴＥ）のような移動体通信網ＭＮによって接続される。また、宅内サーバ１２と鍵センサ等の宅内ＩｏＴ機器１１－１との間が、ｅＳＩＭ１１Ａ－１を用いたＳＳＬによって接続される。その結果、端末装置１４と宅内ＩｏＴ機器１１－１との間で安全なデータ通信が可能になる。
　このように、第１実施形態の外部サーバ１３が適用された通信システム１によれば、インターネットＩＮのセキュリティリスクを回避することができ、高度の安全性を確保した通信を行うことができる。その結果、通信システム１のユーザの安心感を獲得することができる。
【００７０】
　また、第１実施形態の外部サーバ１３が適用された通信システム１では、第１の場合に外部サーバ１３を介した通信が行われると共に、外部サーバ１３を介した通信が行われない第２の場合においても、端末装置１４から宅内サーバ１２への通信データ（通信内容）が、外部サーバ１３に定期的に事後報告として送信される。そのため、第１実施形態の外部サーバ１３が適用された通信システム１では、拡張性を向上させることができ、ビッグデータに対応する（つまり、外部サーバ１３を介さない通信内容もビッグデータ化する）ことができる。
【００７１】
［第２実施形態］
　図７は、第２実施形態の外部サーバ１３が適用された通信システム１において図６のステップＳ３０４の前に実行される処理を説明するためのシーケンス図である。
　図６に示す例では、宅内サーバ１２が、住宅Ａの宅内に配置された宅内ＩｏＴ機器１１、１１－１を管理するが、図７に示す例では、宅内サーバ１２が、住宅Ａの宅内に配置された宅内ＩｏＴ機器１１、１１－１、１１－２を管理する。宅内ＩｏＴ機器１１は、例えば照明機器であり、宅内ＩｏＴ機器１１－１は、例えば鍵センサであり、宅内ＩｏＴ機器１１－２は、例えばデジタルカメラである。
【００７２】
　図７に示す例では、宅内ＩｏＴ機器１１、１１－１、１１－２を含むリストＩＦ１が、宅内サーバ１２の記憶部１２Ｅに登録され、記憶されている。
　ステップＳ４０１では、外部サーバ１３のＣＰＵ１３Ｃの受信処理部１３Ｃ１が、宅内

サーバ１２の記憶部１２Ｅに登録されているリストＩＦ１を定期的に受信し、リストＩＦ１の同期を行う。

ステップＳ４０２では、外部サーバ１３のＣＰＵ１３Ｃの登録処理部１３Ｃ３は、受信処理部１３Ｃ１が受信したリストＩＦ１の登録を行い、記憶部１３ＢがリストＩＦ１を記憶する。

ステップＳ４０３では、外部サーバ１３のＣＰＵ１３Ｃの登録処理部１３Ｃ３は、警告パターンの登録を行う。例えば宅内ＩｏＴ機器１１－１（鍵センサ）が、鍵の施錠状態を検知し続けているにもかかわらず、宅内ＩｏＴ機器１１（照明機器）がＯＦＦ状態からＯＮ状態に切り替わった場合（つまり、不審者が宅内に侵入したおそれがある場合）などが、警告パターンとして登録される。

【００７３】

ステップＳ４０４では、宅内サーバ１２が、宅内ＩｏＴ機器１１－２（デジタルカメラ）に搭載されたｅＳＩＭを用いたＳＳＬによって宅内ＩｏＴ機器１１－２（デジタルカメラ）に接続する。

ステップＳ４０５では、宅内サーバ１２が、宅内ＩｏＴ機器１１（照明機器）に搭載されたｅＳＩＭ１１Ａを用いたＳＳＬによって宅内ＩｏＴ機器１１（照明機器）に接続する。

ステップＳ４０６では、宅内サーバ１２が、宅内ＩｏＴ機器１１－１（鍵センサ）に搭載されたｅＳＩＭ１１Ａ－１を用いたＳＳＬによって宅内ＩｏＴ機器１１－１（鍵センサ）に接続する。

ステップＳ４０７では、宅内サーバ１２が、宅内ＩｏＴ機器１１（照明機器）のＯＮ／ＯＦＦ状態の情報を宅内ＩｏＴ機器１１（照明機器）から受信する。

ステップＳ４０８では、宅内サーバ１２が、宅内ＩｏＴ機器１１－１（鍵センサ）が検知した鍵の解錠状態／施錠状態の情報を宅内ＩｏＴ機器１１－１（鍵センサ）から受信する。

【００７４】

ステップＳ４０９では、ステップＳ４０７において宅内サーバ１２が宅内ＩｏＴ機器１１（照明機器）から受信した宅内ＩｏＴ機器１１（照明機器）のＯＮ／ＯＦＦ状態の情報、および、ステップＳ４０８において宅内サーバ１２が宅内ＩｏＴ機器１１－１（鍵センサ）から受信した宅内ＩｏＴ機器１１－１（鍵センサ）が検知した鍵の解錠状態／施錠状態の情報を外部サーバ１３に送信する。その送信タイミングは、定期的な同期タイミングでもよく、任意に設定されてもよい。

ステップＳ４１０では、外部サーバ１３が、警告パターンを参照する。

ステップＳ４０９において外部サーバ１３が宅内サーバ１２から受信した情報が、警告パターンに該当する場合、つまり、例えば宅内ＩｏＴ機器１１－１（鍵センサ）が鍵の施錠状態を検知し続けているにもかかわらず、宅内ＩｏＴ機器１１（照明機器）がＯＦＦ状態からＯＮ状態に切り替わった場合には、ステップＳ４１１において、外部サーバ１３が端末装置１４にアラートを送信する。

ステップＳ４１２では、端末装置１４の表示部１４Ｅが、アラートのポップアップ画面を表示する。ステップＳ３０４、Ｓ３０５、Ｓ３０６以降の処理は、図６を参照して説明したステップＳ３０４、Ｓ３０５、Ｓ３０６以降の処理と同様である。例えば、操作指示により、宅内ＩｏＴ機器１１－２（デジタルカメラ）をＯＮ状態に切り替え、宅内の様子を確認することができる。

【００７５】

＜第２実施形態のまとめ＞

第２実施形態の外部サーバ１３が適用された通信システム１では、ステップＳ４０７、Ｓ４０８において受信した複数の宅内ＩｏＴ機器１１、１１－１の状態の情報に基づいて、宅内サーバ１２は、宅内に異常が発生したか否かを判定する。

宅内に異常が発生したと宅内サーバ１２が判定した場合に、外部サーバ１３は、ステップＳ４０９において異常が発生したことを示す情報を宅内サーバ１２から受信する。

外部サーバ１３には、宅内に発生した異常が、警告を要さない異常に該当するか、あるいは、警告を要する異常に該当するかを示す第２情報としての警告パターンが、ステップＳ４０３において登録されている。外部サーバ１３は、ステップＳ４１０において、警告パターンと、宅内ＩｏＴ機器１１、１１－１の状態（例えばＯＮ／ＯＦＦ状態など）とを照合する。

宅内に発生した異常が、警告を要する異常に該当する場合に、外部サーバ１３は、ステップＳ４１１において、警告を要する異常が宅内に発生したことを示す情報をアラートとして端末装置１４に送信する。端末装置１４は、ステップＳ４１２において、ポップアップ画面を表示することによって、アラートを出力する。また、端末装置１４は、必要に応じて、宅内ＩｏＴ機器１１、１１－１、１１－２のうちの所定の宅内ＩｏＴ機器に対して操作指示を送信する。

そのため、第２実施形態の外部サーバ１３が適用された通信システム１では、通信システム１のユーザの安心感および満足度を向上させることができる。

【００７６】

［第３実施形態］

図８は、第３実施形態の外部サーバ１３が適用された通信システム１において図６のステップＳ３１１の後に実行される処理を説明するためのシーケンス図である。

図６に示す例では、宅内サーバ１２が、住宅Ａの宅内に配置された宅内ＩｏＴ機器１１、１１－１を管理するが、図７に示す例では、宅内サーバ１２が、住宅Ａの宅内に配置された宅内ＩｏＴ機器１１－１、１１－３を管理する。宅内ＩｏＴ機器１１－１は、例えば鍵センサであり、宅内ＩｏＴ機器１１－３は、例えば無線メッシュネットワークにおけるリーダー宅内ＩｏＴ機器である。リーダー宅内ＩｏＴ機器は、一又は複数の宅内ＩｏＴ機器にデータを転送する機能を有する。これにより、一度特定の宅内ＩｏＴ機器に送信できなくても、当該特定の宅内ＩｏＴ機器に送信できるリーダー宅内ＩｏＴ機器を介することで、再度データを送ることができる。

低消費無線通信規格「Ｔｈｒｅａｄ」においては、家庭やオフィスに無線メッシュネットワークが形成され、インターネットに対する接続が行われる。

「Ｔｈｒｅａｄ」では、無線機器を網目のようにつなぐメッシュネットワークが自己形成され、通常では電波が届かない場所への通信が可能になる。このメッシュネットワークは、ネットワーク内のどの機器が故障しても、バックアップする仕組みを有し、堅牢である。

「Ｔｈｒｅａｄ」では、インターネットのＩＰ通信網が、そのまま無線通信に使用される。また、ネットワークに新しい機器が参加する際のプロセスが工夫されており、ＩｏＴでは特に重要度を増しているセキュリティ対策も施されている。Ｔｈｒｅａｄのエンドデバイスは自己の都合でスリープ状態に居ることができるため、長期の電池駆動が可能である。

「Ｔｈｒｅａｄ」は、第３実施形態の外部サーバ１３を適用可能な無線メッシュネットワークの一例であり、第３実施形態の外部サーバ１３は、他の任意の無線メッシュネットワークに適用可能である。

【００７７】

図８に示す例では、宅内サーバ１２が、宅内ＩｏＴ機器１１－１と、メッシュネットワークのリーダー機器である宅内ＩｏＴ機器１１－３とを含む第３情報としてのメッシュネットワーク情報を有する。つまり、宅内サーバ１２が、メッシュネットワークに含まれる宅内ＩｏＴ機器１１－１、１１－３の情報を有する。

【００７８】

図８に示す例では、ステップＳ５０１において、宅内サーバ１２が、メッシュネットワークのリーダー機器である宅内ＩｏＴ機器１１－３を認識する。好適には、宅内サーバ１２の記憶部１２Ｅ（および外部サーバ１３の記憶部１３Ｂ）に、宅内ＩｏＴ機器１１－１、１１－３のうちのどれがリーダー機器であるかの情報が、リストとして記憶されている。

ステップＳ３１２において、宅内サーバ１２が、宅内ＩｏＴ機器１１－１に搭載されたｅＳＩＭ１１Ａ－１を用いたＳＳＬによって、端末装置１４による操作対象の宅内ＩｏＴ機器１１－１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１－１の操作内容（操作指示）を宅内ＩｏＴ機器１１－１に送信し、宅内ＩｏＴ機器１１－１の操作を試みるが、失敗する。

ステップＳ５０２において、宅内サーバ１２が、端末装置１４による操作対象の宅内ＩｏＴ機器１１－１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１－１の操作内容（操作指示）を、宅内ＩｏＴ機器１１－１の代わりに、宅内ＩｏＴ機器１１－３にＳＳＬによって送信する。

ステップＳ５０３では、宅内ＩｏＴ機器１１－３が、端末装置１４による操作対象の宅内ＩｏＴ機器１１－１のＩＤ、および、端末装置１４による宅内ＩｏＴ機器１１－１の操作内容（操作指示）を宅内ＩｏＴ機器１１－１にＶＰＮ（Virtual Private Network）を介して送信する。

【００７９】

＜第３実施形態のまとめ＞

第３実施形態の外部サーバ１３が適用された通信システム１では、第２の場合であって、宅内サーバ１２がＳＳＬによって宅内ＩｏＴ機器１１－１に接続できない場合に、宅内サーバ１２は、ステップＳ５０２において、ＳＳＬによって宅内ＩｏＴ機器１１－３に接続する。次いで、宅内ＩｏＴ機器１１－３は、ステップＳ５０２において、ＶＰＮを介して宅内ＩｏＴ機器１１－１に接続する。

そのため、第３実施形態の外部サーバ１３が適用された通信システム１では、宅内サーバ１２がＳＳＬによって宅内ＩｏＴ機器１１－１に接続できない場合であっても、端末装置１４が宅内ＩｏＴ機器１１－１を操作することができる。その結果、通信システム１の安全性および確実性を向上させることができる。

【００８０】

＜第１変形例＞

第１から第３実施形態の外部サーバ１３が適用された通信システム１の第１変形例では、宅内サーバ１２が、データ受信時の回線判別機能を備える。そのため、セキュリティを向上させることができる。

具体的には、第１変形例では、宅内ＩｏＴ機器１１－１の操作指示がどの回線を経由して送られてきたかを、宅内サーバ１２が判別する。安全性を要する宅内ＩｏＴ機器１１－１の操作指示は、本来であれば、移動体通信網ＭＮ（例えばＬＴＥ回線）を経由して宅内サーバ１２に送られてくる。その安全性を要する宅内ＩｏＴ機器１１－１の操作指示が、移動体通信網ＭＮ（例えばＬＴＥ回線）ではなく、インターネットＩＮを経由して宅内サーバ１２に送られてきた場合、宅内サーバ１２は、その操作指示が不正な操作指示であると検知する。また、その場合に、宅内サーバ１２は、宅内ＩｏＴ機器１１－１に対するその操作指示を無効化する。

【００８１】

＜第２変形例＞

防犯緊急時には緊急性が最優先事項となり、セキュリティの必要性が下がる。従って、防犯緊急時には、図６に示す例のように、ステップＳ３０９において移動体通信網ＭＮ（詳細にはＬＴＥ）を介する通信を行う必要はなく、ステップＳ３１２においてＳＳＬによる通信を行う必要はない。

そこで、第１から第３実施形態の外部サーバ１３が適用された通信システム１の第２変形例では、第２の場合であっても、防犯緊急時には、端末装置１４が、インターネットＩＮおよび外部サーバ１３を介して宅内サーバ１２と通信を行う。そのため、防犯緊急時の要望を満足させることができる。

一方、防犯緊急時ではない時（平時）に例えば宅内ＩｏＴ機器１１－２（デジタルカメラ）が撮像した子どもの顔写真のデータを端末装置１４に送信する場合には、子どもの顔写真のデータがセンシティブな情報であり、セキュリティの必要性が高い通信に該当する

。従って、図６に示す例のように、ステップＳ３０９において移動体通信網ＭＮ（詳細にはＬＴＥ）を介する通信を行う必要があり、ステップＳ３１２においてＳＳＬによる通信を行う必要がある。

【００８２】

＜第３変形例＞

第１から第３実施形態の外部サーバ１３が適用された通信システム１の第３変形例では、外部サーバ１３のビッグデータ処理により、例えば宅内ＩｏＴ機器１１（照明機器）のＯＮ／ＯＦＦ状態の情報（センサ情報）によっては（つまり、例えばユーザの在宅時間などの個人情報の漏えいのおそれがある場合には）、本来セキュリティが不要な宅内ＩｏＴ機器１１（照明機器）であっても、「セキュリティ必要」に動的に変更され、図６に示す処理と同様の処理が実行される。

【００８３】

なお、上記の各実施形態における宅内サーバ１２、外部サーバ１３、及び端末装置１４が備える各部は、専用のハードウェアにより実現されるものであってもよく、また、メモリおよびマイクロプロセッサにより実現させるものであってもよい。

【００８４】

なお、宅内サーバ１２、外部サーバ１３、及び端末装置１４が備える各部は、メモリおよびＣＰＵ（中央演算装置）により構成され、宅内サーバ１２、外部サーバ１３、及び端末装置１４が備える各部の機能を実現するためのプログラムをメモリにロードして実行することによりその機能を実現させるものであってもよい。

【００８５】

また、宅内サーバ１２、外部サーバ１３、及び端末装置１４が備える各部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。

【００８６】

また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであってもよく、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであってもよい。

【００８７】

以上、本発明の実施形態を、図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更を加えることができる。上述した各実施形態に記載の構成を組み合わせてもよい。

【符号の説明】

【００８８】

１…通信システム、１１…宅内ＩｏＴ機器、１１Ａ…ｅＳＩＭ、１１－１…宅内ＩｏＴ機器、１１Ａ－１…ｅＳＩＭ、１１－２…宅内ＩｏＴ機器、１１－３…宅内ＩｏＴ機器、１２…宅内サーバ、１２Ａ…Ｗｉ－Ｆｉ無線通信部、１２Ｂ…ＢＬＥ無線通信部、１２Ｃ…ＬＴＥ無線通信部、１２Ｄ…ＣＰＵ、１２Ｄ１…選択部、１２Ｅ…記憶部、１２Ｆ…ＳＩＭ、１３…外部サーバ、１３Ａ…通信部、１３Ｂ…記憶部、１３Ｃ…ＣＰＵ、１３Ｃ１…

受信処理部、１３Ｃ２…送信処理部、１３Ｃ３…登録処理部、１３Ｃ４…判定処理部、１４…端末装置、１４Ａ…Ｗｉ－Ｆｉ無線通信部、１４Ｂ…ＢＬＥ無線通信部、１４Ｃ…ＬＴＥ無線通信部、１４Ｄ…操作部、１４Ｅ…表示部、１４Ｆ…ＣＰＵ、１４Ｇ…記憶部、１４Ｈ…ＳＩＭ、Ａ…住宅、ＣＤ１…接続状態情報、ＩＤ１…識別子、ＩＤ２…識別子、ＩＦ１…第１情報、ＩＮ…インターネット、ＫＹＲ…鍵情報、ＭＮ…移動体通信網、ＲＴ…ルータ

【図１】

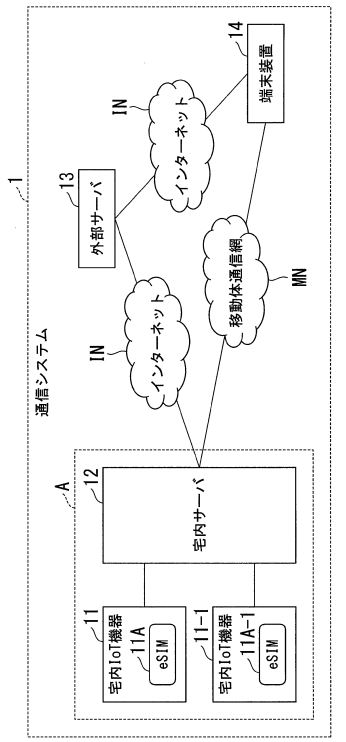


図１

【図２】

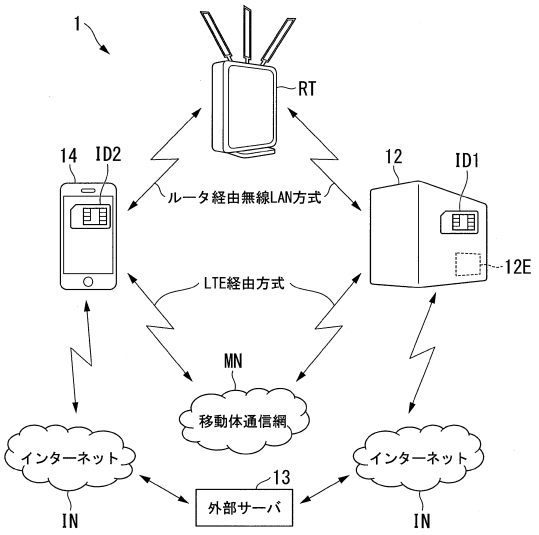
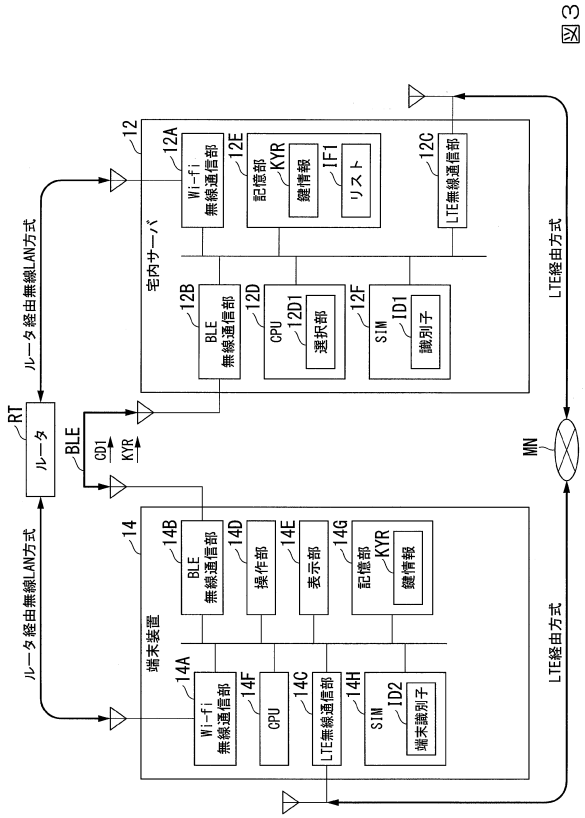


図２

【図３】



【図４】

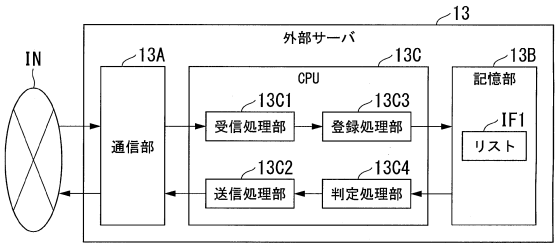


図4

【図５】

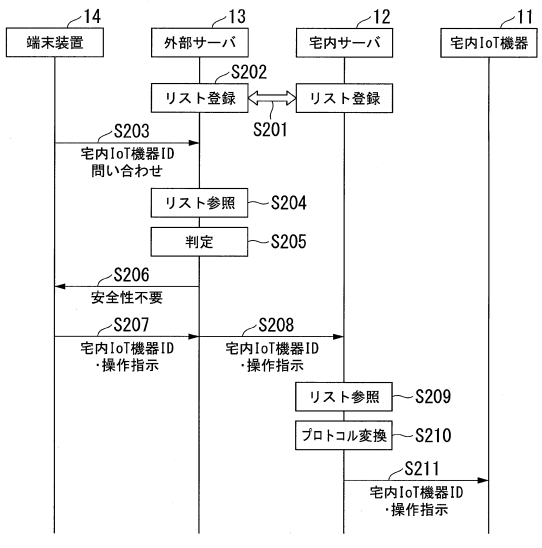


図5

【図６】

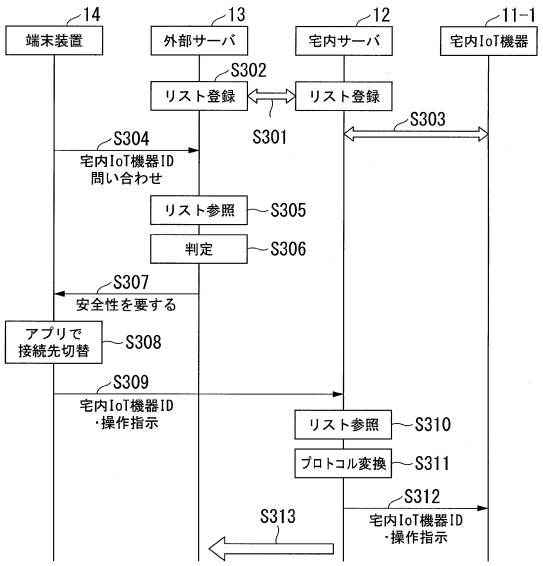


図6

【図７】

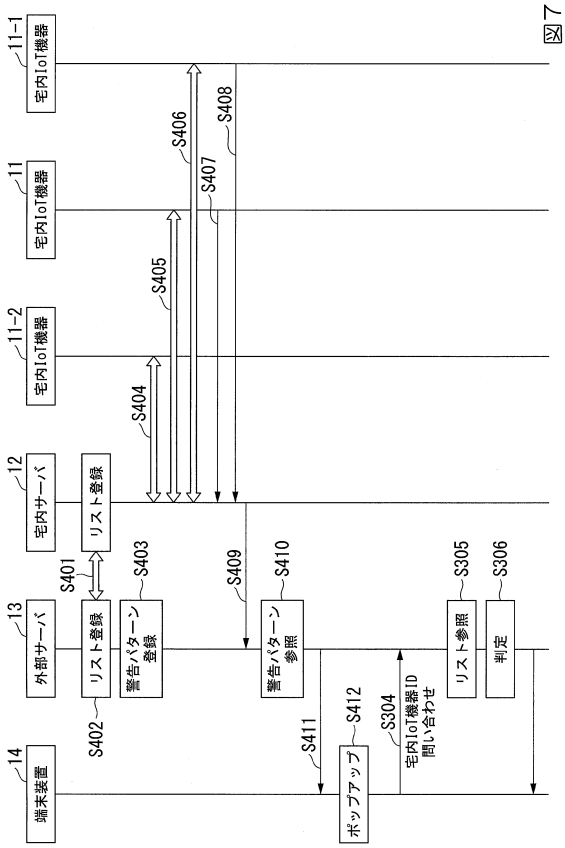

11-1
宅内IoT機器
11
宅内IoT機器
11-2
宅内IoT機器
12
宅内サーバ
13
外部サーバ
14
端末装置
リスト登録
リスト登録
警告パターン登録
警告パターン参照
リスト参照
判定
ポップアップ
S401
S402
S403
S404
S405
S406
S407
S408
S409
S410
S411
S412
S304
宅内IoT機器ID問い合わせ
S305
S306

図７

【図８】

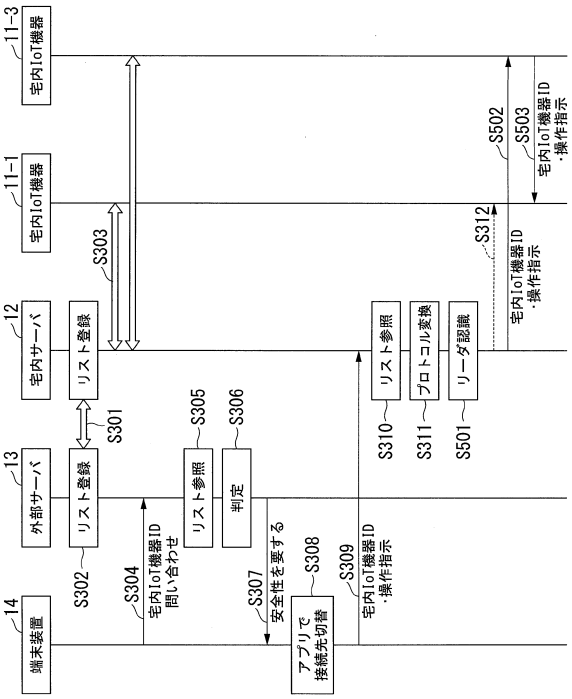

11-3
宅内IoT機器
11-1
宅内IoT機器
12
宅内サーバ
13
外部サーバ
14
端末装置
リスト登録
リスト登録
リスト参照
判定
リスト参照
プロトコル変換
リーダ認識
アプリで接続先切替
S301
S302
S303
S304
宅内IoT機器ID問い合わせ
S305
S306
S307
安全性を要する
S308
S309
宅内IoT機器ID・操作指示
S310
S311
S312
宅内IoT機器ID・操作指示
S501
S502
S503
宅内IoT機器ID・操作指示

図８

フロントページの続き

審査官　藤江　大望

(56)参考文献　特開２００８－１２４９６０（ＪＰ，Ａ）
国際公開第０２／０２８０８３（WO，Ａ１）
特開２０１３－０７０３７４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０８Ｂ２３／００－３１／００
Ｈ０３Ｊ９／００－９／０６
Ｈ０４Ｂ７／２４－７／２６
Ｈ０４Ｍ３／００
３／１６－３／２０
３／３８－３／５８
７／００－７／１６
１１／００－１１／１０
Ｈ０４Ｑ９／００－９／１６
Ｈ０４Ｗ４／００－９９／００