

明 細 書

発明の名称： 通信システム、情報処理装置および監視方法

技術分野

[0001] 本発明の実施形態は、通信システム、情報処理装置および監視方法に関する。

背景技術

[0002] 近年、ＩｏＴ技術を活用して様々なデバイスをネットワークにつなげるシステムが提案されている。例えば、工場、発電所あるいは鉄道などで運転や点検時の様々な稼働データを収集してＡＩ（人工知能）にて分析することによって事前に故障の兆候などを検知する予防保全や設備の効率運用を実現するための通信システムが提案されている。

[0003] このような通信システムを新たに構築するには、様々なデータをネットワーク経由で収集する必要があるために、既存の独自ネットワーク内で運用していたシステムをオープンなネットワークにつなげる必要性が生じることがある。既存の独自ネットワークで運用していたシステムをオープンなネットワークに接続する場合、不正なアクセスに対応するために、新たにオープンなネットワークに接続するデバイス自体にセキュリティ対策を組み込むことでセキュリティを強化することが考えられる。ただし、既に稼働している既存のデバイスに変更を加えることは、デバイス自体の取り替えなどの必要が生じるためコストや可用性の点で実現困難な場合が多い。

[0004] 既存のデバイスに変更を加えずに通信経路の機密性および完全性を担保するためのセキュリティデバイスとして情報処理装置が開発されている。このような情報処理装置は、既存のデバイスとネットワークとの間に接続される。既存のデバイスとネットワークとの間に接続する情報処理装置は、既存のデバイスにおける通信の振る舞いを観察することによりデバイスへの攻撃やウイルス感染などを検知した場合に攻撃者の通信を遮断する機能を備えている。

[0005] しかしながら、既存のデバイスには、ネットワーク以外にローカルに外部機器が接続される可能性があるインターフェースとしてのポートを有するものがある。従来の情報処理装置は、ネットワークを経由する通信経路におけるセキュリティを確保するものであるが、既存のデバイスに設けられる空きポートに対する不正なアクセスを監視する術がないという問題がある。

先行技術文献

特許文献

[0006] 特許文献1：日本国特開2019-50485号公報

発明の概要

発明が解決しようとする課題

[0007] 本発明が解決しようとする課題は、保護対象機器におけるポートへの不正なアクセスを監視できる通信システム、情報処理装置および監視方法を提供することである。

課題を解決するための手段

[0008] 実施形態によれば、通信システムは、情報処理装置と無線器とを有する。無線器は、接触部と第1無線通信部とを有する。情報処理装置は、第1通信インターフェースと第2通信インターフェースと第2無線通信部と制御部とを有する。接触部は、保護対象機器のポートに装着する。第1無線通信部は、接触部が保護対象機器のポートに装着された状態において情報処理装置と無線通信する。第1通信インターフェースは、保護対象機器に接続する。第2通信インターフェースは、ネットワークに接続する。第2無線通信部は、無線器と無線通信する。制御部は、無線器との通信不可状態が異常検知期間以上継続した場合、保護対象機器のネットワークを介した通信を遮断する。

図面の簡単な説明

[0009] [図1]図1は、実施形態に係る通信システムの構成例を示す図である。

[図2]図2は、実施形態に係る通信システムにおける情報処理装置の構成例を示すブロック図である。

[図3]図3は、実施形態に係る情報処理装置に装着されるＩＣカードの構成例を示すブロック図である。

[図4]図4は、実施形態に係る情報処理装置に装着されるＩＣカードにおける機能の構成例としてのＩＣカードのハードウェア構成例を示す図である。

[図5]図5は、実施形態に係る通信システムにおいてＩｏＴデバイスのポートに装着される dongle の構成例を示すブロック図である。

[図6]図6は、実施形態に係る通信システムにおける通信管理装置の構成例を示すブロック図である。

[図7]図7は、実施形態に係る通信システムにおけるＩｏＴデバイス（端末装置）とサーバ装置との間における通信制御の流れを説明するためのシーケンスである。

[図8]図8は、実施形態に係る通信システムにおける情報処理装置、dongle および通信管理装置による処理の例を説明するためのシーケンスである。

実施形態

[0010] 以下、実施形態について、図面を参照して説明する。

図1は、実施形態に係る情報処理装置13を有する通信システムの構成例を示す図である。

通信システム1は、ＩｏＴデバイス（端末装置、保護対象機器）11、サーバ装置12、情報処理装置13（13A、13B）、通信管理装置14、無線dongle（無線器）15およびゲートウェイ17を備える。図1に示す構成例においては、ゲートウェイ17およびネットワーク18をまとめてネットワークNWとも称するものとする。

[0011] 通信システム1において、各情報処理装置13は、既存の通信システムに接続されることが想定される。すなわち、各情報処理装置13は、ＩｏＴデバイス11、サーバ装置12、通信管理装置14、およびゲートウェイ17を備える既存のシステムにおいて図1に示すような位置に接続される。

[0012] 各情報処理装置13は、既存のシステムを各装置の構成を変更せずに可用性を維持したまま通信システム1を構築するように設置される。情報処理

装置 1 3 は、図 1 に示すように、既存のシステムにおける通信経路に接続するための第 1 通信ポート（例えば、第 1 の L A N ポート） 2 1 と第 2 通信ポート（例えば、第 2 の L A N ポート） 2 2 とを備える。例えば、情報処理装置 1 3 は、第 1 通信ポート 2 1 A をゲートウェイ 1 7 に接続し、第 2 通信ポート 2 2 A を I o T デバイス 1 1 に接続することにより、I o T デバイス 1 1 とゲートウェイ 1 7 との間に接続される。

[0013] また、本実施形態に係る情報処理装置 1 3 は、無線通信部 3 5 およびスイッチ 3 6 などを有する。無線通信部 3 5 は、I o T デバイス 1 1 のポート 1 6 に装着される無線ドングル 1 5 と無線通信を行うように構成される。なお、無線通信部 3 5 およびスイッチ 3 6 は、デバイス側の情報処理装置 1 3 A だけでなく、サーバ側の情報処理装置 1 3 B が具備するものでも良い。本実施形態において、無線通信部 3 5 およびスイッチ 3 6 は、保護対象機器とする I o T デバイス 1 1 に接続するデバイス側の情報処理装置 1 3 A に設けるものとして説明する。

[0014] I o T デバイス 1 1 は、様々なデータを取得するデバイス（端末装置、クライアント端末）である。例えば、I o T デバイス 1 1 は、センサなどでデータを取得するデバイスであっても良いし、オペレータが入力するデータを取得するデバイスであっても良い。I o T デバイス 1 1 は、取得したなデータをサーバ装置 1 2 へ送信する。また、I o T デバイス 1 1 は、サーバ装置 1 2 の制御情報に応じて動作を制御する機能を有するものでも良い。

[0015] I o T デバイス 1 1 は、それぞれに接続されるデバイス側の情報処理装置 1 3 A を介してネットワーク NW と接続する。サーバ装置 1 2 は、サーバ側の情報処理装置 1 3 B を介してネットワーク NW と接続する。すなわち、各 I o T デバイス 1 1 とサーバ装置 1 2 とは、それぞれに接続された情報処理装置 1 3 およびネットワーク NWなどを介して通信するように構成される。

[0016] さらに、I o T デバイス 1 1 は、外部機器を接続するポート 1 6 を有する。ポート 1 6 は、汎用のポートであり、例えば、U S B（U n i v e r s a l S e r i a l B u s）ポートである。ポート 1 6 は、外部機器の接続

部が物理的に接続されるコネクタを備え、装着された外部機器とＩｏＴデバイス１１とがデータの入出力を行えるようにするものであれば良い。例えば、ポート１６は、データの入出力を行うカード状の電子機器を接続するスロットであって良い。本実施形態において、ポート１６には、後述する無線ドングル１５が接続されるものとする。

[0017] 無線ドングル１５は、ＩｏＴデバイス１１のポート１６に物理的に装着される無線器である。無線ドングル１５は、ポート１６から供給される電力によって動作する。無線ドングル１５は、情報処理装置１３と無線通信する。ＩｏＴデバイス１１のポート１６から供給される電力によって駆動する無線ドングル１５は、デバイス側の情報処理装置１３Ａの無線通信部３５と無線通信する。

[0018] 無線ドングル１５は、ＩｏＴデバイス１１のポート１６に装着されていれば、情報処理装置１３Ａの無線通信部３５と無線通信を継続的に実行する。無線ドングル１５は、ポート１６から取り外されると、電力の供給が途絶えるために動作を停止する。これにより、デバイス側の情報処理装置１３Ａは、無線ドングル１５との通信が継続できているか否かにより、ＩｏＴデバイス１１のポート１６に無線ドングル１５が装着されているか否かを特定できる。

[0019] サーバ装置１２は、ＩｏＴデバイス１１が取得したデータを収集する。例えば、サーバ装置１２は、各ＩｏＴデバイス１１から収集したデータを管理したり分析したりする。また、サーバ装置１２は、ＩｏＴデバイス１１に対して制御情報を送信するようにしても良い。

[0020] デバイス側の情報処理装置１３Ａは、ＩｏＴデバイス１１とネットワークNWのゲートウェイ１７との間に接続される。デバイス側の情報処理装置１３Ａは、それぞれネットワークNW側のインターフェース接続部としての第１通信ポート２１Ａとデバイス側のインターフェース接続部としての第２通信ポート２２Ａとを有する。第１通信ポート２１Ａおよび第２通信ポート２２Ａは、例えば、ＬＡＮポートである。図１に示す構成例において、第１通

信ポート 2 1 A には、ゲートウェイ 1 7 が接続され、第 2 通信ポート 2 2 A には、それぞれ I o T デバイス 1 1 A が接続される。

[0021] デバイス側の情報処理装置 1 3 A は、I o T デバイス 1 1 とサーバ装置 1 2 との間の通信を仲介する。情報処理装置 1 3 A は、I o T デバイス 1 1 によりサーバ装置 1 2 に対して送信されるデータを取得し、取得したデータをサーバ装置 1 2 に対して出力する。ここで、情報処理装置 1 3 A は、サーバ装置 1 2 に対してデータを送信する際に、I o T デバイス 1 1 から取得したデータを暗号化し、暗号化したデータをサーバ装置 1 2 に対して送信する。

[0022] また、情報処理装置 1 3 A は、サーバ装置 1 2 により I o T デバイス 1 1 に対して送信されるデータを取得し、取得したデータを I o T デバイス 1 1 に対して出力する。ここで、情報処理装置 1 3 A が取得するデータは暗号化されたデータである。情報処理装置 1 3 A は、I o T デバイス 1 1 にデータを出力する際に、サーバ装置 1 2 からサーバ側の情報処理装置 1 3 B を介して取得したデータを復号し、復号したデータを I o T デバイス 1 1 に出力する。

[0023] さらに、デバイス側の情報処理装置 1 3 A は、ゲートウェイ 1 7 を介してデバイス側の他の情報処理装置 1 3 A と通信可能な構成を備えるようにしても良い。この場合、デバイス側の各情報処理装置 1 3 A は、それぞれに設定される通信許可設定に従ってデバイス側の他の情報処理装置 1 3 A との通信の可否が設定されるようにしても良い。

[0024] サーバ側の情報処理装置 1 3 B は、サーバ装置 1 2 とネットワーク NW との間に接続される。サーバ側の情報処理装置 1 3 B は、ネットワーク NW 側のインターフェース接続部としての第 1 通信ポート 2 1 B とサーバ側のインターフェース接続部としての第 2 通信ポート 2 2 B とを有する。第 1 通信ポート 2 1 B には、ネットワーク 1 8 が接続され、第 2 通信ポート 2 2 B には、サーバ装置 1 2 が接続される。

[0025] サーバ側の情報処理装置 1 3 B は、各 I o T デバイス 1 1 とサーバ装置 1 2 との間の通信を仲介する。サーバ側の情報処理装置 1 3 B は、サーバ装置

12によりIoTデバイス11に対して送信されるデータを取得し、取得したデータをIoTデバイス11に対して送信する。ここで、サーバ側の情報処理装置13Bは、IoTデバイス11に対してデータを送信する際に、サーバ装置12から取得したデータを暗号化し、暗号化したデータをIoTデバイス11に対して送信する。

[0026] また、サーバ側の情報処理装置13Bは、IoTデバイス11によりサーバ装置12に対して送信されるデータを取得し、取得したデータをサーバ装置12に対して出力する。ここで、サーバ側の情報処理装置13Bが取得するデータは暗号化されたデータである。サーバ側の情報処理装置13Bは、サーバ装置12にデータを出力する際に、IoTデバイス11からデバイス側の情報処理装置13Aを介して取得したデータを復号し、復号したデータをサーバ装置12に出力する。

[0027] 各情報処理装置13(13A、13B)は、例えば、SSL(Secure Socket Layer)/TLS(Transport Layer Security)の Protokolによる暗号化を実行する。デバイス側の情報処理装置13Aおよびサーバ側の情報処理装置13Bは、例えば、SSL/TLS Protokolを、HTTP(Hypertext Transfer Protocol)と組み合わせることで、HTTPに含まれるデータを暗号化し、安全性を向上させたHTTPS(HTTP Secure)に置き換える。

[0028] なお、デバイス側の情報処理装置13Aおよびサーバ側の情報処理装置13Bが行うデータの暗号化は、HTTPをHTTPSとすることに限定されない。デバイス側の情報処理装置13Aおよびサーバ側の情報処理装置13Bは、SSL/TLS Protokolを種々の通信 Protokolと組み合わせることにより、安全性を向上させたセキュアな通信 Protokolに置き換えてもよい。例えば、デバイス側の情報処理装置13Aおよびサーバ側の情報処理装置13Bは、FTP(File Transfer Protocol)をFTPS(FTP Secure)に置き換えてもよい。

- [0029] 通信システム 1 において、デバイス側の情報処理装置 1 3 A 又はサーバ側の情報処理装置 1 3 B により暗号化されたデータがネットワーク NW に出力される。換言すると、通信システム 1 におけるネットワーク NW を流れるデータは、暗号化されたデータである。このため、ネットワーク NW で送受信されるデータに対し、外部から悪意をもってアクセスされデータが盗聴されてしまうような危険を回避し、安全性を向上させる。なお、ここでいうデータの盗聴とは、「データを盗み見る行為」又は「データを抜き取る行為」をいう。
- [0030] 通信管理装置 1 4 は、デバイス側の情報処理装置 1 3 A とサーバ側の情報処理装置 1 3 B とを用いた通信を管理するためのサーバ装置である。例えば、通信管理装置 1 4 は、プライベート認証局としても機能する。通信管理装置 1 4 は、各情報処理装置 1 3 に対し、クライアント証明書および秘密鍵を発行する。
- [0031] 図 1 に示す構成例において、通信管理装置 1 4 は、情報処理装置 1 3 に装着する IC カードに記憶するクライアント証明書および秘密鍵を発行する。デバイス側の情報処理装置 1 3 A に認証部およびセキュアな記憶部を備える IC カードが装着される場合、通信管理装置 1 4 は、情報処理装置 1 3 A に対して IC カードに記憶させるクライアント証明書および秘密鍵をネットワーク NW を介して送信する。
- [0032] また、通信管理装置 1 4 は、サーバ側の情報処理装置 1 3 B に対して、サーバ証明書、および秘密鍵を発行する。サーバ側の情報処理装置 1 3 B に認証部およびセキュアな記憶部を備える IC カードが装着される場合、通信管理装置 1 4 は、サーバ側の情報処理装置 1 3 B に対して IC カードに記憶させるサーバ証明書および秘密鍵をネットワーク NW を介して送信する。クライアント証明書、サーバ証明書および秘密鍵のそれぞれは、デバイス側の情報処理装置 1 3 A とサーバ側の情報処理装置 1 3 B とが暗号化通信を行う場合に用いる共通鍵（セッション鍵）を決定するために必要な情報である。
- [0033] ここで、IoT デバイス 1 1 およびサーバ装置 1 2 の例について説明する

。

ＩｏＴデバイス１１とサーバ装置１２とは、例えば、社会インフラシステムを構築する構成要素（コンポーネント）である。社会インフラとは、道路交通網、発電設備、配送電設備、水処理設備、又はガス配給設備等などの社会基盤を整えるために必要な設備である。社会インフラシステムとは、例えば、社会インフラを監視し、状況の変化を把握し、その変化に対応することにより、社会インフラを安定的に動作させる仕組みである。

[0034] 具体例として、道路や公共設備などを映像で監視する監視システムである場合、ＩｏＴデバイス１１は、道路の状況等を監視するために撮像された撮像データをネットワークNWを介して送信する装置（ネットワーク監視カメラ）であり、サーバ装置１２は、ＩｏＴデバイス１１により送信された撮像データをネットワークNWを介して受信する装置である。また、ＩｏＴデバイス１１とサーバ装置１２とは、発電設備や配送電設備における電力状況をモニタリングするシステムのコンポーネントであっても良い。また、ＩｏＴデバイス１１とサーバ装置１２とは、物流センタにおける配送状況を取得するシステムのコンポーネントであっても良い。また、ＩｏＴデバイス１１とサーバ装置１２とは、工場や研究機関における設備の稼働状況を取得するシステム等のコンポーネントであっても良い。

[0035] なお、監視システムやモニタリングシステムなどの社会インフラシステムは、ＩｏＴデバイス１１とサーバ装置１２をコンポーネントとする通信システムの例であり、ＩｏＴデバイス１１とサーバ装置１２は、社会インフラシステムのコンポーネントに限定されるものではない。

[0036] ＩｏＴデバイス１１は、NW（ネットワーク）通信部、デバイス制御部およびデータ取得部を有する。NW通信部は、データ通信を行うための通信インターフェースである。NW通信部は、ネットワークを介して外部装置と通信可能とするイーサネット（登録商標）などの通信インターフェースである。言い換えると、ＩｏＴデバイス１１は、NW通信部によりネットワークに接続される装置と通信可能な構成を備えるデバイスである。

- [0037] 本実施形態に係る通信システム1においては、IoTデバイス11のNW通信部は、情報処理装置13に接続され、情報処理装置13を介してネットワークNWに接続されるサーバ装置12と通信する構成となっている。すなわち、本実施形態に係る通信システム1は、IoTデバイス11とサーバ装置12とがネットワークを介して通信可能に構成される既存のシステムに対して、後付でIoTデバイス11とネットワークNWとの間に情報処理装置13Aを接続し、サーバ装置12とネットワークNWとの間に情報処理装置13Bを接続することで構築できるシステムである。
- [0038] デバイス制御部は、例えば、CPUなどを含むプロセッサであり、IoTデバイス11を統括的に制御する。デバイス制御部は、例えば、サーバ装置12からの制御に従い、データ取得部によるデータの取得を開始又は停止させたり、データ取得部に対する動作設定などを実行したりする。データ取得部は、デバイス制御部の指示に従って動作することにより、データを取得し、取得したデータを制御部に出力する。デバイス制御部は、データ取得部で取得したデータをNW通信部により送信（出力）する。
- [0039] 本実施形態に係る通信システム1においては、IoTデバイス11のNW通信部は、情報処理装置13に接続される。このため、各IoTデバイス11は、情報処理装置13を介してデータの入出力を行う。例えば、IoTデバイス11は、デバイス側の情報処理装置13A、ネットワークNW、および、サーバ側の情報処理装置13Bを介してサーバ装置12と通信する。
- [0040] サーバ装置12は、NW（ネットワーク）通信部、サーバ制御部およびデータ記憶部などを備える。NW通信部は、データ通信を行うための通信インターフェースである。NW通信部は、ネットワークを介して外部装置と通信可能とするイーサネット（登録商標）などの通信インターフェースである。言い換えると、サーバ装置12は、NW通信部によりネットワークに接続される装置と通信可能な構成を備える装置である。
- [0041] 本実施形態に係る通信システム1においては、サーバ装置12のNW通信部は、情報処理装置13Bに接続され、情報処理装置13Bを介してネット

ワークNWに接続される機器と通信する構成となっている。すなわち、本実施形態に係る通信システム1は、IoTデバイス11とサーバ装置12とがネットワークを介して通信可能に構成される既存のシステムに対して、後付でサーバ装置12とネットワークとの間に情報処理装置13Bを接続することで構築できるシステムである。

[0042] サーバ制御部は、例えば、CPUなどを含むプロセッサであり、サーバ装置を統括的に制御する。サーバ制御部は、例えば、NW通信部により各IoTデバイス11からデータを取得し、IoTデバイス11から取得したデータをデータ記憶部に記憶させる。データ記憶部は、サーバ制御部の指示に従い、IoTデバイス11から取得したデータを記憶する。また、サーバ制御部は、NW通信部により通信する各IoTデバイス11に動作指示などの制御命令を出力したりする。

[0043] 次に、IoTデバイス11とサーバ装置12との間の通信について説明する。

一般に、通信機能を有するIoTデバイス（クライアント端末、通信デバイス）とサーバ装置とが互いのNW通信部およびネットワークを介して接続された場合、IoTデバイスとサーバ装置との間の通信には、一般的な通信プロトコルであるHTTPが用いられることがある。この場合、通信デバイス又はサーバ装置によりネットワークに出力された暗号化されていない情報（いわゆる、平文）がネットワークを流れる。この場合、外部から悪意をもってネットワーク上のデータが取得されてしまうと、容易にデータが盗聴されたり、改ざんされたりする危険性がある。このような不正な攻撃に対する対策としては、通信デバイスがデータを暗号化してネットワークに出力させることが考えられる。

[0044] しかしながら、既存のシステムに用いられている既存のIoTデバイス（クライアント端末）は、暗号化のための処理を行うだけの資源（リソース）を備えていないことが多い。例えば、IoTデバイスの一例としての監視カメラは、撮像データの圧縮や符号化を行うためのCPU等のプロセッサを備

えるが、さらに暗号化のための処理を行うだけのリソースを備えていないことが多い。従って、既存のシステムにおいて、IoTデバイスがネットワークに出力するデータを暗号化させるためには、データを暗号化するためのプロセッサをさらにIoTデバイスに搭載させる必要があり、IoTデバイスのハードウェア構成の変更や置き換えが必要となることが考えられる。監視システム等の社会インフラシステムを構成するコンポーネントとしての既存のIoTデバイスは、ハードウェア構成を変更したり置き換えたりすることが容易にはできない。

[0045] 上述したような事情を鑑みると、既存のIoTデバイスに変更を加えることなく、IoTデバイスからのデータが暗号化されてネットワークNWに伝送されるように構成できる通信システムが望ましい。本実施形態に係る通信システム1は、既存のシステムにおける既存のIoTデバイスにハードウェア構成を変更したり既存のIoTデバイスを新たなIoTデバイスに置き換えたりすることなく、既存のIoTデバイスおよびサーバ装置に情報処理装置を接続することでデータを安全に伝送できるものである。

[0046] すなわち、通信システム1において、IoTデバイス11とネットワークNWとの間に接続された情報処理装置13はIoTデバイス11がサーバ装置12宛に送信するデータを暗号化してネットワークNWに出力する。また、通信システム1において、サーバ装置12とネットワークNWとの間に接続されたサーバ側の情報処理装置13Bはサーバ装置12からのIoTデバイス11宛の制御データなどのデータを暗号化してネットワークNWに出力する。これにより、本実施形態に係る通信システム1によれば、IoTデバイス11およびサーバ装置12を変更することなく、ネットワークNWを流れるデータの安全性を向上できる。

[0047] 次に、実施形態に係る情報処理装置13の構成について説明する。

図2は、図1に示す情報処理装置13の構成例を示すブロック図である。

図2に示すように、情報処理装置13は、制御部30、第1通信部31、第2通信部32、リーダライタ33、ICカード34、無線通信部35およ

びスイッチ 36 を備える。ここで、リーダライタ 33、および、ＩＣカード 34 は、「認証部」の一例である。認証部は、リーダライタ 33 および ＩＣカード 34 で実現するものに限定されない。認証部は、制御部 30 が実現しても良いし、認証処理用の処理回路で実現しても良い。

[0048] 制御部 30 は、例えば、ＣＰＵなどを含むプロセッサを有する。制御部 30 は、情報処理装置 13 を統括的に制御する。制御部 30 は、例えば、リーダライタ 33 を介して、ＩＣカード 34 にコマンドを送信するとともに、ＩＣカード 34 からレスポンスを受信する。また、制御部 30 は、ＩＣカード 34 から受信したレスポンスに基づく情報を、第 1 通信部 31 を介して、他方の情報処理装置 13 に送信する。また、制御部 30 は、第 1 通信部 31 を介して、他方の情報処理装置 13 から受信した情報に基づいて、ＩＣカード 34 にコマンドを送信する。

[0049] 第 1 通信部 31 は、ネットワーク NW を介して接続される各装置と通信するためのネットワーク通信部である。第 1 通信部 31 は、ネットワーク NW に接続される第 1 通信ポート 21 (21A、21B) を備える。第 1 通信部 31 は、例えば、NIC (Network Interface Card) により構成される。例えば、情報処理装置 13A は、第 1 通信部 31 によりネットワーク NW を介して、通信管理装置 14 と通信したり、サーバ側の情報処理装置 13B と通信したりする。

[0050] 具体的には、デバイス側の情報処理装置 13A の第 1 通信部 31 は、第 1 通信ポート 21A に接続されるゲートウェイ 17 からのデータを取得するとともに、サーバ装置 12 宛のデータを暗号化してゲートウェイ 17 を介してネットワーク 18 へ出力する。また、サーバ側の情報処理装置 13B の第 1 通信部 31 は、第 1 通信ポート 21B に接続されるネットワーク 18 からの暗号化されたデータを取得するとともに、取得したデータを復号してサーバ装置 12 へ出力する。

[0051] 第 2 通信部 32 は、端末装置としての IoT デバイス 11 又はサーバ装置 12 と通信するためのデバイス通信部である。第 2 通信部 32 は、通信を実

行する端末装置（ＩｏＴデバイス１１、又はサーバ装置１２）に接続される第２通信ポート２２（２２Ａ、２２Ｂ）を備える。例えば、第２通信部３２は、ＮＩＣ（Network Interface Card）により構成される。

[0052] 具体的には、デバイス側の情報処理装置１３Ａの第２通信部３２は、第２通信ポート２２Ａに接続されるＩｏＴデバイス１１としてのカメラからの撮像データを取得するとともに、復号された制御データをＩｏＴデバイス１１に出力する。また、サーバ側の情報処理装置１３Ｂの第２通信部３２は、第２通信ポート２２Ｂに接続されるサーバ装置１２からの制御データを取得するとともに、復号された撮像データをサーバ装置１２に出力する。

[0053] また、本実施形態に係る情報処理装置１３は、通信管理装置１４による通信許可の設定が有効になったことが確認された後に、ＩｏＴデバイス１１と第２通信部３２とを通信可能な状態にするようにしても良い。すなわち、第１通信部３１は、ネットワークＮＷを介して通信管理装置１４と通信するためにリンクアップされる。第２通信部３２は、第１通信部３１がネットワークＮＷを介して通信管理装置１４にリンクアップされ、当該情報処理装置１３Ａにおける通信許可の設定が有効となったことが確認された後、第２通信ポート２２Ａを介してＩｏＴデバイス１１にリンクアップされるようにしても良い。

[0054] 無線通信部３５は、無線ドングル１５と無線通信するためのインターフェースである。無線通信部３５は、例えば、近距離無線通信によってＩｏＴデバイス１１のポート１６に装着した無線ドングル１５と通信する。

スイッチ３６は、ユーザが指示を入力するための操作部である。スイッチ３６は、例えば、ＩｏＴデバイス１１の電源をオンした場合に入力される。

[0055] リーダライタ３３は、ＩＣカード３４との間の通信を行う。リーダライタ３３は、ＩＣカード３４の通信方式に対応するインターフェースを備える。ＩＣカード３４が接触式のＩＣカードである場合、リーダライタ３３は、図２に示すように、ＩＣカード３４のコンタクト部に接続するインターフェー

スを備え、インターフェースを介してデータの送受信を行う。

[0056] ICカード34は、例えば、プラスチックのカード基材に、ICモジュール40を実装して形成されている。ICカード34は、ICモジュール40とICモジュール40が埋め込まれたカード基材（本体）とを備える。図2に示す構成例において、ICカード34は、情報処理装置13（13A、13B）のリーダライタ33に着脱可能に構成される。ICカード34は、リーダライタ33に装着された状態でコンタクト部41を介して情報処理装置13（13A、13B）と通信する。

[0057] ICカード34は、例えば、情報処理装置13（13A、13B）が送信したコマンド（処理要求）をコンタクト部41を介して受信し、受信したコマンドに応じた処理（コマンド処理）を実行する。ICカード34は、コマンド処理の実行結果であるレスポンス（処理応答）を情報処理装置13（13A、13B）にコンタクト部41を介して送信する。

[0058] ICモジュール40は、コンタクト部41とICチップ42とを備える。コンタクト部41は、ICカード34が動作するために必要な各種信号の端子を有している。ここで、各種信号の端子は、電源電圧、クロック信号、リセット信号などを情報処理装置13（13A、13B）から供給を受ける端子、および、情報処理装置13（13A、13B）と通信するためのシリアルデータ入出力端子（SIO端子）を有する。ICチップ42は、例えば、1チップのマイクロプロセッサなどのLSI（Large Scale Integration）である。

[0059] ここで、実施形態に係る情報処理装置13が備える認証部の構成例としてのICカード34のハードウェア構成について説明する。

図3は、図2に示すICカード34のハードウェア構成例を示す図である。

ICカード34は、コンタクト部41とICチップ42とを備えたICモジュール40を有する。ICチップ42は、図3に示すように、UART（Universal Asynchronous Receiver T

r a n s m i t t e r) 43、CPU44と、ROM (R e a d O n l y M e m o r y) 45、RAM (R a n d o m A c c e s s M e m o r y) 46、および、EEPROM (登録商標) (E l e c t r i c a l l y E r a s a b l e P r o g r a m m a b l e R O M) 47を備える。

また、各構成(43から47)は、内部バスBSを介して接続されている。

[0060] U A R T 43は、上述したS I O端子を介して、情報処理装置13(13A、13B)とシリアルデータ通信を行う。U A R T 43は、S I O端子を介して受信したシリアルデータ信号をパラレル変換したデータ(例えば、1バイトのデータ)を内部バスBSに出力する。また、U A R T 43は、内部バスBSを介して取得したデータをシリアル変換して、S I O端子を介して情報処理装置13(13A、13B)に出力する。U A R T 43は、例えば、S I O端子を介してコマンドを情報処理装置13(13A、13B)から受信する。また、U A R T 43は、S I O端子を介してレスポンスを情報処理装置13(13A、13B)に送信する。

[0061] C P U 44は、ROM45又はEEPROM47に記憶されているプログラムを実行して、I Cカード34の各種処理を行う。C P U 44は、例えば、コンタクト部41を介して、U A R T 43が受信したコマンドに応じたコマンド処理を実行する。

[0062] R O M 45は、例えば、マスクROMなどの不揮発性メモリであり、I Cカード34の各種処理を実行するためのプログラム、およびコマンドテーブルなどのデータを記憶する。R A M 46は、例えば、S R A M (S t a t i c R A M)などの揮発性メモリであり、I Cカード34の各種処理を行う際に利用されるデータを一時記憶する。E E P R O M 47は、例えば、電気的に書き換え可能な不揮発性メモリである。E E P R O M 47は、I Cカード34が利用する各種データを記憶する。E E P R O M 47は、例えば、I Cカード34を利用した各種サービス(アプリケーション)に使用される情報を記憶する。

[0063] 次に、実施形態に係る情報処理装置13における認証部の構成例としての

ＩＣカード３４が備える機能について説明する。

図４は、図３に示すＩＣカード３４の機能構成例を示すブロック図である。ＩＣカード３４は、通信部５０と、制御部５１と、記憶部５４とを備える。ここで、図４に示されるＩＣカード３４の各部は、図３に示されるＩＣカード３４のハードウェアを用いて実現される。

[0064] 通信部５０は、コンタクト部４１を介して、情報処理装置１３（１３Ａ、１３Ｂ）との間でコマンドおよびレスポンスの送受信を行う。通信部５０は、ＣＰＵ４４がＲＯＭ４５に記憶されているプログラムを実行することによりＵＡＲＴ４３を用いてデータの送受信を実行する機能である。通信部５０は、所定の処理を要求するコマンド（処理要求）を情報処理装置１３（１３Ａ、１３Ｂ）から受信するとともに、コマンドに対するレスポンス（処理応答）を情報処理装置１３（１３Ａ、１３Ｂ）に送信する。通信部５０は、ＵＡＲＴ４３を介して情報処理装置１３（１３Ａ、１３Ｂ）から受信した受信データをＲＡＭ４６に記憶させる。また、通信部５０は、ＲＡＭ４６に記憶されている送信データを、ＵＡＲＴ４３を介して情報処理装置１３（１３Ａ、１３Ｂ）に送信する。

[0065] 制御部５１は、ＩＣカード３４の動作を制御する。制御部５１は、ＣＰＵ４４とＲＡＭ４６とＲＯＭ４５又はＥＥＰＲＯＭ４７とにより実現される。制御部５１は、コマンド処理部５２および暗号化復号部５３を備える。ここで、コマンド処理部５２が行う処理は、「認証処理」の一例である。また、暗号化復号部５３が行う処理は、「暗号化復号処理」の一例である。

[0066] コマンド処理部５２は、各種コマンド処理を実行する。コマンド処理部５２は、例えば、後述するＨＴＴＰＳリクエストを要求するコマンド処理として、ＳＳＬ／ＴＬＳハンドシェイクを行う。ＳＳＬ／ＴＬＳハンドシェイクでは、暗号化された通信に必要な鍵情報等の交換、および通信先の装置との相互認証を行う。ここで、相互認証とは、デバイスが側の情報処理装置１３Ａとサーバ側の情報処理装置１３Ｂとが通信を行う前に、互いに正当に認証された装置であることを相互に確認する処理である。

[0067] 暗号化復号部53は、データを暗号化する処理、および暗号化されたデータを復号する処理を実行する。暗号化復号部53は、通信部50を介して取得した装置（IoTデバイス11又はサーバ装置12）により出力されたデータを暗号化する。また、暗号化復号部53は、通信部50を介して取得したネットワークNWからの暗号化されたデータを復号する。

[0068] 記憶部54は、データを記憶する。記憶部54は、制御部51の制御によってデータのリードおよびライトが実行されるEEPROM47により実現される。記憶部54は、証明書情報記憶部55と秘密情報記憶部56とを有する。証明書情報記憶部55は、通信管理装置14が発行した装置（IoTデバイス11又はサーバ装置12）に対する証明書を記憶する。具体的には、情報処理装置13に装着されるICカード34の証明書情報記憶部55には、クライアント証明書を示す情報が記憶される。また、サーバ側の情報処理装置13Bに装着されるICカード34の証明書情報記憶部55には、サーバ証明書を示す情報が記憶される。

[0069] 秘密情報記憶部56は、通信管理装置14が発行した装置（IoTデバイス11又はサーバ装置12）に対する秘密鍵を記憶する。具体的には、情報処理装置13に装着されるICカード34の秘密情報記憶部56には、情報処理装置13に対して発行された秘密鍵を示す情報が記憶される。また、サーバ側の情報処理装置13Bに装着されるICカード34の証明書情報記憶部55には、サーバ側の情報処理装置13Bに対して発行された秘密鍵を示す情報が記憶される。

[0070] 次に、実施形態に係る通信システム1における無線ドングル15の構成について説明する。

図5は、実施形態に係る通信システム1における無線ドングル15の構成例を示すブロック図である。

図5に示す構成例において、無線ドングル15は、マイコン61、無線通信部62、電源部63および接続部64を有する。

マイコン61は、無線ドングル15の制御を司る制御部である。マイコン

61は、例えば、CPUなどのプロセッサとROM、RAMおよびNVMなどのシステムメモリとを含む。マイコン61は、プロセッサがシステムメモリなどに記憶したプログラムを実行することにより種々の処理を実現する。例えば、マイコン61は、通信相手と相互認証を行う機能を有するセキュアマイコンである。マイコン61は、情報処理装置13Aの無線通信部35と相互認証を行った後に無線通信部62を用いた無線通信を実行する。

[0071] 無線通信部62は、無線通信を行う通信インターフェースである。無線通信部62は、情報処理装置13が備える無線通信部35に対応する無線通信方式の通信インターフェースで構成する。

[0072] 電源部63は、接続部64を介して供給される電力を各部に供給する電源として機能する。接続部64は、IoTデバイス11のポート16に装着可能な仕様で構成される。無線ドングル15がポート16に装着された場合、接続部64は、IoTデバイス11のポート16内のコンタクト部に接触し、ポート16からの電力供給を受ける。電源部63は、接続部64に供給される電力を各部（マイコン61および無線通信部62）が動作するための電力に変換することにより各部への動作用の電力を供給する。

[0073] 次に、実施形態に係る通信システム1における通信管理装置14の構成について説明する。

図6は、図1に示す通信管理装置14の構成例を示すブロック図である。

通信管理装置14は、NW（ネットワーク）通信部90、制御部91、および記憶部92を備える。

NW通信部90は、ネットワークNWに接続され、ネットワークNWを介して、情報処理装置13（13A、13B）と通信を行う。

[0074] 制御部91は、例えば、CPUなどのプロセッサとROMおよびRAMなどのシステムメモリとを含む。制御部91は、プロセッサがシステムメモリなどの記憶部に記憶したプログラムを実行することにより種々の処理を実現する。制御部91は、通信管理装置14を統括的に制御する。制御部91は、情報処理装置13と他の装置との通信に用いるセキュリティ情報を管理す

る。例えば、制御部 9 1 は、主に情報処理装置 1 3 (1 3 A、1 3 B) の正当性を認めるプライベート認証局として動作する。図 7 に示す例において、制御部 9 1 は、プロセッサがプログラムを実行することにより、鍵生成部 7 1、証明書発行部 7 2、証明書更新部 7 3、証明書管理部 7 4 および管理部 7 5 としての機能を実現するための処理を実行する。

[0075] 鍵生成部 7 1 は、例えば、情報処理装置 1 3 (1 3 A、1 3 B) からの認証申請に基づいて、後述する証明書に含まれる公開鍵に対応する秘密鍵の発行を行う。

[0076] 証明書発行部 7 2 は、例えば、情報処理装置 1 3 (1 3 A、1 3 B) からの認証申請に基づいて、情報処理装置 1 3 (1 3 A、1 3 B) の正当性を認める証明書の発行を行う。証明書には、例えば、公開鍵と情報処理装置 1 3 (1 3 A、1 3 B) の所有者を示す情報とが含まれる。

[0077] 証明書更新部 7 3 は、有効期限が経過した証明書に対して新たな有効期限を設定することにより、証明書の更新を行う。証明書更新部 7 3 は、例えば、情報処理装置 1 3 (1 3 A、1 3 B) からの更新申請に基づいて、当該情報処理装置 1 3 (1 3 A、1 3 B) に対して発行した証明書の有効期限を延長させた証明書を発行し、発行した証明書を情報処理装置 1 3 (1 3 A、1 3 B) に対して送信する。発行した証明書を示す情報が情報処理装置 1 3 (1 3 A、1 3 B) により受信され、情報処理装置 1 3 (1 3 A、1 3 B) の IC カード 3 4 の証明書情報記憶部 5 5 に記憶されることで、情報処理装置 1 3 (1 3 A、1 3 B) の証明書の有効期限が延長される。

[0078] 証明書管理部 7 4 は、既に発行済みの証明書に対する管理を行う。証明書管理部 7 4 は、例えば、情報処理装置 1 3 (1 3 A、1 3 B) に装着された IC カード 3 4 の改ざん、又は盗難等により相互認証において互いの正当性が証明されない場合に、情報処理装置 1 3 (1 3 A、1 3 B) に対して発行した証明書を無効化する処理を行う。

[0079] また、証明書管理部 7 4 は、情報処理装置 1 3 (1 3 A、1 3 B) からの問い合わせに基づいて、情報処理装置 1 3 (1 3 A、1 3 B)、および他の

通信装置に対して発行した証明書が証明書発行部 7 2 により発行されたものか否か応答するようにしてもよい。また、証明書管理部 7 4 は、定期的に、発行済みの証明書が正当な情報処理装置 1 3 (1 3 A、1 3 B) に使用されているかを確認するようにしてもよい。

[0080] 管理部 7 5 は、情報処理装置 1 3 (1 3 A、1 3 B) を管理する。例えば、管理部 7 5 は、情報処理装置 1 3 (1 3 A、1 3 B) が行う相互認証を、ネットワーク NW を介して遠隔制御する。

記憶部 9 2 は、例えば、不揮発性の記憶装置で構成される。記憶部 9 2 は、鍵情報記憶部 8 1、証明書情報記憶部 8 2 および通信設定記憶部 8 3 を備える。鍵情報記憶部 8 1 は、例えば既に発行済みの公開鍵や秘密鍵を示す情報を記憶する。証明書情報記憶部 8 2 は、例えば既に発行済みの証明書を示す情報を記憶する。鍵情報記憶部 8 1 と証明書情報記憶部 8 2 とは、例えば、鍵生成部 7 1 が秘密鍵を発行する際、証明書発行部 7 2 が証明書を発行する際などに参照される。また、鍵情報記憶部 8 1 には、鍵生成部 7 1 が発行した秘密鍵を示す情報が記憶される。また、証明書情報記憶部 8 2 には、証明書発行部 7 2 が発行した証明書を示す情報が記憶される。

[0081] 通信設定記憶部 8 3 は、情報処理装置 1 3 に適用（設定）する通信設定を示す通信設定情報を記憶する。通信設定記憶部 8 3 が記憶する情報処理装置 1 3 の通信設定情報には、端末装置としての IoT デバイス 1 1 との通信の可否を指定する通信許可設定を含むようにしても良い。また、制御部 9 1 は、通信設定記憶部 8 3 に記憶する通信設定情報を情報処理装置 1 3 からの要求に応じて供給するようにしても良い。例えば、制御部 9 1 は、情報処理装置 1 3 が起動した場合に情報処理装置 1 3 へ通信設定情報を供給するようにしても良い。

[0082] 次に、通信システム 1 における情報処理装置 1 3 A および 1 3 B を介した IoT デバイス 1 1 とサーバ装置 1 2 との通信処理について説明する。

図 7 は、通信システム 1 が行う処理の一例を示すシーケンスチャートである。

- [0083] IoTデバイス11は、データ（IoTデバイスが検出したデータや撮像したデータなど）をサーバ装置12に送信する場合、まずサーバ装置12に対するHTTPリクエストを送信する（ステップS1）。IoTデバイス11が送信したHTTPリクエストは、デバイス側の情報処理装置13（13A）により取得される（ステップS2）。
- [0084] デバイス側の情報処理装置13は、IoTデバイス11により送信されたHTTPリクエストを取得すると、サーバ側の情報処理装置13Bに対して、HTTPSのリクエスト（ClientHello）を送信する（ステップS3）。これにより、デバイス側の情報処理装置13とサーバ側の情報処理装置13Bとの間のハンドシェイクが開始される（ステップS4）。
- [0085] 具体的には、デバイス側の情報処理装置13が送信するClientHelloには、例えば、TLSのバージョン、および通信に用いる暗号方式やアルゴリズムのリストを示す情報が含まれる。サーバ側の情報処理装置13Bは、ClientHelloに対する応答として、デバイス側の情報処理装置13に対しHTTPSのレスポンス（ServerHello）を送信する。サーバ側の情報処理装置13Bが送信するServerHelloには、例えばClientHelloで提示された選択肢の中でサーバ装置12が選択した情報が含まれる。換言すると、デバイス側の情報処理装置13からの提示に対し、サーバ側の情報処理装置13Bが選択を行うことで、通信における具体的な暗号化アルゴリズムが決定される。
- [0086] そして、サーバ側の情報処理装置13Bは、暗号化通信に用いる共通鍵に必要な情報を送る。共通鍵に必要な情報には、例えば、サーバ装置12に対して発行された公開鍵とその証明書を示す情報、およびIoTデバイス11の公開鍵とその証明書を送ることを要求する情報が含まれる。デバイス側の情報処理装置13Aは、サーバ側の情報処理装置13Bに対して、自装置に対して発行された公開鍵とその証明書、および暗号化通信に用いる共通鍵に必要な情報を送る。
- [0087] デバイス側の情報処理装置13Aとサーバ側の情報処理装置13Bとの間

の相互認証は、例えば次のように行われる。デバイス側の情報処理装置 1 3 A は、今までに受信した S e r v e r H e l l o 等から署名を生成し、サーバ側の情報処理装置 1 3 B に送信する。サーバ側の情報処理装置 1 3 B は、デバイス側の情報処理装置 1 3 A から受信した署名をデバイス側の情報処理装置 1 3 から受信した証明書に基づいて検証する。サーバ側の情報処理装置 1 3 B は、検証が成功すると、その証明書が間違いなくデバイス側の情報処理装置 1 3 A のものであると判定する。また、サーバ側の情報処理装置 1 3 B は、今までに受信した C l i e n t H e l l o 等から署名を生成し、デバイス側の情報処理装置 1 3 A に送信する。デバイス側の情報処理装置 1 3 A は、サーバ側の情報処理装置 1 3 B から受信した署名を、サーバ側の情報処理装置 1 3 B から受信した証明書に基づいて検証する。デバイス側の情報処理装置 1 3 A は、検証が成功すると、その証明書が間違いなくサーバ側の情報処理装置 1 3 B のものであると判定する。

[0088] デバイス側の情報処理装置 1 3 A とサーバ側の情報処理装置 1 3 B との間の相互認証が正しく行われると、デバイス側の情報処理装置 1 3 A とサーバ側の情報処理装置 1 3 B とは、それぞれ暗号化に用いる共通鍵を生成して交換する。

[0089] サーバ側の情報処理装置 1 3 B から送付されたサーバ装置 1 2 に対して発行された公開鍵とその証明書が、デバイス側の情報処理装置 1 3 A に許容される証明書であれば、サーバ側の情報処理装置 1 3 B は、デバイス側の情報処理装置 1 3 A から送付された公開鍵とその証明書が、サーバ側の情報処理装置 1 3 B に許容される証明書であれば、ハンドシェイクを終了する。

[0090] サーバ側の情報処理装置 1 3 B は、デバイス側の情報処理装置 1 3 A とのハンドシェイクが確立されると、サーバ装置 1 2 に対し、H T T P リクエストを送信する（ステップ S 5）。H T T P リクエストは、ステップ S 1 において I o T デバイス 1 1 から送信される H T T P リクエストである。

[0091] サーバ側の情報処理装置 1 3 B により送信された H T T P リクエストは、サーバ装置 1 2 により受信される（ステップ S 6）。このとき、サーバ装置

12は、IoTデバイス11からHTTPリクエストが要求されたと認識する。このため、サーバ装置12は、IoTデバイス11に対するHTTPレスポンスを応答する（ステップS7）。サーバ装置12が送信したHTTPレスポンスは、サーバ側の情報処理装置13Bにより取得される（ステップS8）。

[0092] サーバ側の情報処理装置13Bは、取得したサーバ装置12からのHTTPレスポンスを、ステップS4のハンドシェイクにおいて決定された共通鍵を用いて暗号化する（ステップS9）。サーバ側の情報処理装置13Bにより暗号化されたHTTPレスポンスは、ネットワークNWを介してデバイス側の情報処理装置13Aに受信される（ステップS10）。デバイス側の情報処理装置13Aは、受信したHTTPレスポンスを、共通鍵を用いて復号する（ステップS11）。デバイス側の情報処理装置13Aにより復号されたHTTPレスポンスは、IoTデバイス11に取得される（ステップS12）。IoTデバイス11は、復号されたHTTPレスポンスを受信する（ステップS13）。このとき、IoTデバイス11は、サーバ装置12からHTTPレスポンスが応答されたと認識する。このため、IoTデバイス11は、サーバ装置12に対し、データを送信する（ステップS14）。

[0093] IoTデバイス11が送信した撮像データは、デバイス側の情報処理装置13Aにより取得される（ステップS15）。デバイス側の情報処理装置13Aは、IoTデバイス11により送信されたデータを、共通鍵を用いて暗号化する（ステップS16）。デバイス側の情報処理装置13Aにより暗号化されたデータは、ネットワークNWを介してサーバ側の情報処理装置13Bに受信される（ステップS17）。

[0094] サーバ側の情報処理装置13Bは、受信したデータを、共通鍵を用いて復号する（ステップS18）。サーバ側の情報処理装置13Bにより復号されたデータは、サーバ装置12にとり取得される（ステップS19）。サーバ装置12は、復号されたデータを受信する（ステップS20）。このとき、サーバ装置12は、IoTデバイス11からのデータを受信したと認識する。

。

[0095] なお、上記フローチャートのステップS 4において、デバイス側の情報処理装置1 3 Aとサーバ側の情報処理装置1 3 Bとの間の相互認証が正しく行われなかった場合、デバイス側の情報処理装置1 3 Aは、通信先との通信を許可しない。具体的には、デバイス側の情報処理装置1 3 Aは、通信先から送信された情報をI o Tデバイス1 1に出力しない。相互認証が正しく行われなかった場合、通信先がサーバ側の情報処理装置1 3 Bに見せかけた不正な通信装置である可能性があるためである。この場合、デバイス側の情報処理装置1 3 Aは、例えば、相互認証が正しく行われなかった場合の通信記録を通信管理装置1 4に送信するようにしてもよい。これより、通信管理装置1 4は相互認証が正しく行われなかった場合の通信記録を取得することができ、管理下にあるデバイス側の情報処理装置1 3 Aに対する不正な通信のパターンや頻度を把握することで、ネットワークの異常を監視することができる。

[0096] また、デバイス側の情報処理装置1 3 Aは、上記フローチャートのステップS 4において行われるハンドシェイクにおいて相互認証の代わりにI o Tデバイス1 1に対する通信を許可する通信機器の情報を示す送信先リストに基づいて、通信先との通信を許可するか否かを判定するようにしてもよい。送信先リストに示される通信機器の情報は、例えばURL (Uniform Resource Locator) である。デバイス側の情報処理装置1 3 Aの制御部3 0は、通信先のURLが送信先リストに登録されているURLである場合に当該通信先との通信を許可し、送信先リストに登録されていない場合には通信を許可しない。

[0097] また、制御部3 0は、送信先リストを更新するようにしてもよい。制御部3 0は、例えば、一定期間にI o Tデバイス1 1に対する通信を許可された通信先のURL、および許可されなかった通信先URLを記憶させる。そして、制御部3 0は、例えば、送信先リストに登録されたURLのうち、一定期間に通信が行われた通信先のURLを再度登録する等することにより送信

先リストを更新する。あるいは、デバイス側の情報処理装置 13 は、一定期間に通信を許可された通信先 URL、および許可されなかった通信先 URL を通信管理装置 14 に送信するようにしてもよい。この場合、例えば、通信管理装置 14 は、デバイス側の情報処理装置 13 A と通信を行った通信先 URL に基づいて、送信先リストを更新するようにしてもよい。通信管理装置 14 により送信先リストが更新されることで、通信管理装置 14 が管理下にあるデバイス側の情報処理装置 13 A と通信する通信機器を一括して管理することができる。

[0098] また、デバイス側の情報処理装置 13 A は、ステップ S4 において行われるハンドシェイクが確立した後に IoT デバイス 11 に対して送信された情報（例えば、ファームウェアの更新プログラム）の内容が正しいか否かの検証を行うようにしてもよい。例えば、デバイス側の情報処理装置 13 A の制御部 30 は、ネットワーク NW を介して IoT デバイス 11 のファームウェアの更新プログラムが送信された場合、検証用の鍵（検証鍵）を用いて検証する。この場合、通信管理装置 14 は、例えば、デバイス側の情報処理装置 13 A およびサーバ側の情報処理装置 13 B それぞれに検証鍵を送信するようにしてもよい。

[0099] 例えば、サーバ側の情報処理装置 13 B は、IoT デバイス 11 へ送信する情報（平文）からハッシュ値を生成し、生成したハッシュ値を検証鍵で暗号化する。そして、サーバ側の情報処理装置 13 B は、平文と暗号化したハッシュ値をさらに秘密鍵で暗号して IoT デバイス 11 へ送信する。また、デバイス側の情報処理装置 13 は共通鍵を用いて情報を復号化し、平文と暗号化されたハッシュ値とを取得する。

[0100] また、デバイス側の情報処理装置 13 A は、取得した平文からハッシュ値を生成するとともに、暗号化されたハッシュ値を検証鍵で復号する。デバイス側の情報処理装置 13 A は、平文から生成したハッシュ値と、復号化したハッシュ値とが等しい値である場合、IoT デバイス 11 に対して送信された情報は正しい内容であると判定する。この場合、デバイス側の情報処理装

置 1 3 A は、復号した情報（平文）を I o T デバイス 1 1 に出力する。一方、デバイス側の情報処理装置 1 3 A は、平文から生成したハッシュ値と復号化したハッシュ値が等しい値でない場合、I o T デバイス 1 1 に対して送信された情報は、サーバ装置 1 2 又はサーバ側の情報処理装置 1 3 B に見せかけた不正な通信装置から送信された不正な情報である可能性があると判定する。この場合、デバイス側の情報処理装置 1 3 A は、復号した情報（平文）を I o T デバイス 1 1 に出力しない。

[0101] これにより、I o T デバイス 1 1 は、検証済みである正しい内容であることが検証された情報のみを受け取ることができる。また、通常、I o T デバイス 1 1 がファームウェアを更新する際の更新プログラムの内容が正しいか否かの判定を行うと考えられるが、I o T デバイス 1 1 に代わりサーバ側の情報処理装置 1 3 B が I o T デバイス 1 1 に対して送信された情報の内容を検証することにより、I o T デバイス 1 1 の処理負担を軽減させることが可能となる。

[0102] 以上説明したように、通信システム 1 は、I o T デバイス 1 1 とネットワーク NW との間に接続されるデバイス側の情報処理装置 1 3 A と、サーバ装置 1 2 とネットワーク NW との間に接続されるサーバ側の情報処理装置 1 3 B と、を備える。デバイス側の情報処理装置 1 3 A は、I o T デバイス 1 1 からの情報を暗号化してネットワーク NW 経由でサーバ側の情報処理装置 1 3 B へ送信し、ネットワーク NW からの情報（情報処理装置 1 3 B で暗号化されたサーバ装置 1 2 からの情報）を復号して I o T デバイス 1 1 へ送信する。サーバ側の情報処理装置 1 3 B は、サーバ装置 1 2 からの情報を暗号化してネットワーク NW 経由でデバイス側の情報処理装置 1 3 へ送信し、ネットワーク NW からの情報（デバイス側の情報処理装置 1 3 A で暗号化された I o T デバイスからの情報）を復号してサーバ装置 1 2 に送信する。

[0103] これにより、通信システム 1 は、社会インフラシステムを変更することなく、社会インフラシステムの安全性を向上させることができる。I o T デバイス 1 1 からサーバ装置 1 2 に対して送信された H T T P プロトコルのデー

タ（いわゆる平文）が、デバイス側の情報処理装置 13 により、例えば、SSL/TLS プロトコルと組み合わせられて、安全性が向上された HTTPS に置き換えられるためである。また、サーバ装置 12 か IoT デバイス 11 に対して送信された制御データは、暗号化されるが、デバイス側の情報処理装置 13 により復号されて、IoT デバイス 11 に受信されるため、IoT デバイス 11 に復号させる処理を行わせる必要がなく、既存の装置を変更することなくそのまま利用することができる。

[0104] また、通信システム 1 では、デバイス側の情報処理装置 13 A とサーバ側の情報処理装置 13 B とが相互認証を行うため、いずれか一方方向のみの認証を行う場合よりも安全性を向上させることができる。一般的なクライアント端末とサーバ装置とにおいては、サーバ装置に対して不特定多数のクライアント端末が通信を行うため、当該不特定多数のクライアント端末に対して正当なクライアント証明書を発行して管理し続けることは現実的ではない。しかしながら、通信システムを適用する社会インフラシステムなどにおいては、IoT デバイス 11 とサーバ装置 12 との関係は明確に特定されている。このため、デバイス側の情報処理装置 13 A とサーバ側の情報処理装置 13 B とが相互認証を行うことが可能であり、安全性を向上させることができる。

[0105] 一般に、クライアント証明書を有していないクライアント端末では、サーバ装置と通信を行うために、サーバ装置が発行した ID やパスワードの入力を求められることがある。このようなパスワード認証においては、安全性を維持するために、パスワードに対し文字と数字を組み合わせた長文の文字列が要求されたり、定期的なパスワードの変更等が求められたりすることがある。しかしながら、覚えなければならないパスワードが増えると、管理が面倒になってしまい、パスワードをメモに残したり、ウェブブラウザに記録させたりするなど、かえってパスワードが漏洩してしまう場合があった。

[0106] これに対し、通信システム 1 では、デバイス側の情報処理装置 13 A がクライアント（デバイス）証明書を有することにより、サーバ装置 12 との間

で確実に相互認証を行うことができる。このため、パスワード認証が不要となる。このため、パスワードを入力する手間や定期的に変更して管理する手間がなくなり、ユーザの利便性が向上する。つまり、ユーザに負担をかけることなく安全性を維持することができる。

[0107] また、クライアント証明書を有していないクライアント端末がIDやパスワードによる認証に基づいてサーバ装置と通信を行うシステムでは、IDとパスワードが正しく入力できてしまえば、だれでもサーバ装置と通信することができてしまう。このため、クライアント端末を不正に乗っ取り、サーバ装置へ不正にアクセスすることが可能となってしまう。例えば、不正に乗っ取られたサーバ装置によってクライアント端末の機能が制限され、解除するために身代金が要求されるといったランサムウェアに感染する可能性がある。

[0108] これに対し、上述した通信システム1では、IoTデバイス11とサーバ装置12との間で、デバイス側の情報処理装置13Aとサーバ側の情報処理装置13Bとを介した相互認証が行われることにより、IoTデバイス11やサーバ装置12が不正に乗っ取られることがない。つまり、通信システム1では、ランサムウェアに対する対策も可能となる。

[0109] また、例えば、ネットワーク内に管理者が不在の端末（野良デバイスともいう）がある場合、その端末が不正に乗っ取られることにより、その端末がマルウェア等の攻撃を行う不正な端末として利用されてしまう場合がある。これに対し、上述した通信システム1では、IoTデバイス11とサーバ装置12との間で、デバイス側の情報処理装置13A（13B、13C）とサーバ側の情報処理装置13Bとを介した相互認証が行われることにより、ネットワークNWの内部にある管理者が不在の端末が不正に乗っ取られて攻撃に利用された場合であっても、マルウェア等に感染することを防止することができる。

[0110] また、上述した通信システム1では、サーバ装置12がサーバ側の情報処理装置13Bに接続されており、サーバ装置12の内部で認証処理を行わな

い。このため、サーバ装置 1 2 の内部で証明書等を保持する必要がなく、サーバ側の情報処理装置 1 3 B に接続されたサーバ装置 1 2 が通信管理装置 1 4 の管理下であることが明確となる。サーバ装置 1 2 が既にサーバ側の情報処理装置 1 3 B に相当する機能部を有している場合には、必ずしもサーバ装置 1 2 とネットワーク NW との間にサーバ側の情報処理装置 1 3 B が物理的に接続される必要はない。この場合、サーバ装置 1 2 が元々有するサーバ側の情報処理装置 1 3 B に相当する機能部により、デバイス側の情報処理装置 1 3 A との間の認証処理が行われる。

[0111] また、通信システム 1 では、IC カード 3 4 において、相互認証と暗号化復号処理とのうち少なくともいずれか一方を行わせる。このため、情報処理装置 1 3 (1 3 A、1 3 B) の装置コストを抑制することができる。

[0112] また、通信システム 1 においては、情報処理装置 1 3 (1 3 A、1 3 B) に装着された IC カード 3 4 が相互認証と暗号化復号処理とのうち少なくともいずれか一方の処理を行う例を説明したが、通信システム 1 は、相互認証および暗号化複合化処理を行う構成が IC カードに限定されるものではない。また、上述した IC カード 3 4 としては、秘密鍵およびクライアント証明書（あるいは、サーバ証明書）を記憶する記憶機能と、相互認証と暗号化復号処理とのうち少なくともいずれか一方を行う処理機能を有している機能部であればよく、例えば、IC チップが搭載された SIM カードであってもよいし、カードの形態を採用しなくてもよい。

[0113] また、通信システム 1 においては、情報処理装置 1 3 の IC カード 3 4 は、情報処理装置 1 3 に対して着脱可能に装着される。これにより、通信システム 1 においては、IC カード 3 4 と情報処理装置 1 3 とが分離可能であるため、どちらか一方を交換する場合には、当該一方のデバイスを交換すればよい。例えば、IC カード 3 4 と情報処理装置 1 3 とが一体化された場合には、IC カード 3 4 に相当する部分を交換する場合には、情報処理装置 1 3 全体を交換しなければならないが、この場合と比較して、通信システム 1 では、情報処理装置 1 3 が有する IC カード 3 4 等の特定の部分を交換する場

合のメンテナンスコストを抑制することができる。

- [0114] また、通信システム 1 は、通信管理装置 1 4 をさらに備え、通信管理装置 1 4 は、情報処理装置 1 3 に装着された IC カード 3 4 に記憶させる秘密鍵、およびクライアント証明書を情報処理装置 1 3 に送信し、サーバ側の情報処理装置 1 3 B に装着された IC カード 3 4 に記憶させる秘密鍵、およびサーバ証明書をサーバ側の情報処理装置 1 3 B に送信する。これにより、通信システム 1 は、通信管理装置 1 4 により発行された正当な秘密鍵、証明書を用いて、ハンドシェイクを行い、共通鍵を決定することができ、上述した効果を奏する他、社会インフラシステムの安全性をさらに向上させることができる。
- [0115] なお、通信システム 1 の構成は、上述した例に限定されない。例えば、情報処理装置 1 3 は、処理の負荷に基づき、ハードウェアにより情報処理装置 1 3 の機能を実現する HSM (Hardware Security Module) を用いてもよい。つまり、情報処理装置 1 3 は、セキュアな処理が可能な限り、必ずしも IC カードを装着する構成に限らず、上記情報処理装置 1 3 の機能を実現できる IC チップや IC モジュールを用いた構成としてもよい。
- [0116] また、通信システム 1 においては、SSL/TLS プロトコルを用いたセキュアな通信を常時行うようにしてもよいし、SSL/TLS プロトコルを用いた通信を行うか否かを選択可能にしてもよい。また、IoT デバイス 1 1 とサーバ装置 1 2 との間における双方向の通信のうち一方の方向の通信のみを SSL/TLS プロトコルを用いた通信としてもよい。また、SSL/TLS プロトコルを用いたセキュアな通信を常時行うようにしてもよいし、SSL/TLS プロトコルを用いた通信を行うか否かを選択可能にしてもよい。
- [0117] SSL/TLS プロトコルを用いた通信を常時行うようにすることで、情報処理装置 1 3 により認証された正当な情報処理装置 1 3 とは異なる装置からの通信を遮断することができる。このため、IoT デバイス 1 1 やサーバ

装置 1 2 に対する不正なアクセスや、IoT デバイス 1 1 やサーバ装置 1 2 がマルウェアに感染することを抑止することができる。

[0118] また、通信システム 1 においては、SSL/TLS プロトコルを用いた通信を常時行い、IoT デバイス 1 1 やサーバ装置 1 2 に対する不正なアクセスを記憶するようにしてもよい。この場合、通信管理装置 1 4 に不正なアクセスの記録が送信されるようにしてもよい。通信管理装置 1 4 は、不正なアクセスの有無を認識することができ、システム全体に対する大規模攻撃が開始される前の予兆の段階を検出して対策することが可能となる。

[0119] また、通信システム 1 においては、情報処理装置 1 3 は、定期的に、自装置が接続されている IoT デバイス 1 1 又はサーバ装置 1 2 との接続が維持されているか否かを確認するようにしてもよい。この場合、通信管理装置 1 4 に接続状態を示す情報が送信されるようにしてもよい。通信管理装置 1 4 は、情報処理装置 1 3 から接続状態を示す情報が受信できない場合などには、情報処理装置 1 3 が IoT デバイス 1 1 又はサーバ装置 1 2 から切り離された判断し、当該切り離された情報処理装置 1 3 を無効とする。こうすることで通信管理装置 1 4 は、切り離された情報処理装置 1 3 が不正な装置に接続されてなりすましに悪用されることを抑制する。

[0120] また、通信システム 1 においては、情報処理装置 1 3 に装着する IC カード 3 4 に、CC (Common Criteria/ISO 15408) 認証を取得したセキュアエレメントと呼ばれる耐タンパ性の高いチップを搭載してもよい。このチップを用いて、秘密鍵や公開鍵を含む証明書を記憶させることにより、非常に高い安全性を維持することができる。

[0121] また、通信システム 1 においては、サーバ装置 1 2 や通信管理装置 1 4 等から、情報処理装置 1 3 を介して、IoT デバイス 1 1 のプログラムを更新させるようにしてもよい。情報処理装置 1 3 を介してプログラムの更新（ファームウェアのアップデート）が行われることにより、安全に IoT デバイス 1 1 の機能を更新させることができる。このようにサーバ装置 1 2 から IoT デバイス 1 1 に対してファームウェアが送信される場合、サーバ装置 1

2から送信されるファームウェアには、例えばサーバ側の情報処理装置13Bにより暗号化されたサーバ装置12の署名が付与される。この場合、IoTデバイス11では、情報処理装置13により署名が復号されることにより、送信されたファームウェアが間違いなくサーバ装置12から送信されたファームウェアであると判定することができる。これにより、あたかもサーバ装置12であるかのように装う不正な端末から、不正なファームウェアがIoTデバイス11に送信されてしまった場合であっても、IoTデバイス11に対し不正なファームウェアに基づく誤った更新がなされてしまうことを排除することができる。

[0122] また、このように情報処理装置13を介して通信が行われることにより、サーバ装置12や通信管理装置14等からIoTデバイス11にファームウェアを安全に更新することができるため、作業員が複数のIoTデバイス11に対して物理的に各々のIoTデバイス11が設置されている場所まで移動してファームウェアのアップデート作業を行う場合と比較して、作業コストを低減させることも可能である。

[0123] また、通信システム1においては、サーバ装置12や通信管理装置14等から、情報処理装置13を介して、IoTデバイス11の起動や停止を行ってもよい。情報処理装置13を介して起動や停止（リモートアクティベーション）が行われることにより、安全にIoTデバイス11の機能を更新させることができ、セキュアな遠隔制御を実現させることができる。

[0124] また、通信システム1においては、IoTデバイス11、およびサーバ装置12が有線により通信する場合を例に説明したが、これに限定されることはない。IoTデバイス11、およびサーバ装置12のうち少なくともいずれかが無線LAN等により無線通信を行う装置であってもよい。例えば、IoTデバイス11が無線通信によりサーバ装置12と通信を行う場合、情報処理装置13は、無線による通信機能を有し、IoTデバイス11により送信されるデータを暗号化し、暗号化したデータを、無線通信によりサーバ装置12に送信する。

[0125] 上述した例では、通信システム 1 において、情報処理装置 1 3 がサーバ側の情報処理装置 1 3 B と通信を行う例を説明したが、情報処理装置 1 3 の通信先はこれに限定されることはない。例えば、情報処理装置 1 3 A は、情報処理装置 1 3 B と通信を行ってもよい。情報処理装置 1 3 A は、情報処理装置 1 3 B から通信開始の合図を受信した場合、まず情報処理装置 1 3 B との間で相互認証を行い、情報処理装置 1 3 B が正当な通信端末であることを確認する。そして、相互認証が正しく行われた場合、情報処理装置 1 3 A は、情報処理装置 1 3 B から受信した情報を IoT デバイス 1 1 に出力する。暗号を使用して送信データに認証子が付与されることにより、通信情報の改ざんの検出および送信者の特定が可能となる。

[0126] 以上のように、通信システム 1 においては、デバイス側の情報処理装置 1 3 とサーバ側の情報処理装置 1 3 B との通信、およびデバイス側の情報処理装置 1 3 同士の通信において、「正しい相手から」、「改ざんされていないデータを受け取る」ことを確実にすることができる。

[0127] 次に、実施形態に係る通信システム 1 による IoT デバイス 1 1 おけるポート 1 6 に対する監視処理について説明する。

図 8 は、実施形態に係る通信システム 1 による IoT デバイス 1 1 のポート 1 6 に対する監視処理の動作例を説明するためのシーケンスである。

ここで、図 1 に示すような構成において、通信システム 1 では、IoT デバイス 1 1 における特定の機器が接続されていないポート（空きポート）1 6 に無線ドングル 1 5 が装着されるものとする。すなわち、IoT デバイス 1 1 において空き状態となっているポート 1 6 には、管理者の操作などによって無線ドングル 1 5 がセットされる（ステップ S 4 1）。

[0128] ポート 1 6 にセットされた無線ドングル 1 5 は、接続部 6 4 を介してポート 1 6 から電力が供給される。無線ドングル 1 5 の電源部 6 3 は、接続部 6 4 を介してポート 1 6 から供給される電力を各部へ供給する。これにより、無線ドングル 1 5 のマイコン 6 1 は、電源部 6 3 から供給される電力によって起動する（ステップ S 4 2）。

[0129] 無線ドングル15のマイコン61は、起動すると、無線通信部62を用いて無線通信により情報処理装置13Aへ接続要求を送信する。

デバイス側の情報処理装置13Aは、無線通信部35により無線ドングル15から接続要求を受信する。情報処理装置13Aの制御部30は、無線通信部35により無線ドングル15から接続要求を受信すると、無線ドングル15との相互認証を行う（ステップ43）。

[0130] 情報処理装置13Aの制御部30は、無線ドングル15との相互認証が成功すると、通信部32により無線ドングル15との相互認証が成功したことを通信管理装置14へ通知する（ステップ44）。ここで、情報処理装置13Aの制御部30は、無線ドングル15がどのIoTデバイス11のどのポート16に接続されているかを示す情報なども通信管理装置14へ通知するようにしても良い。

[0131] 通信管理装置14は、NW通信部90により情報処理装置13Aから無線ドングル15との相互認証が成功したことを示す通知を受信する。通信管理装置14の制御部91は、情報処理装置13Aから無線ドングル15との相互認証が成功したことを示す通知を受信すると、当該無線ドングル15がセットされたIoTデバイス11のポート16を監視するための監視設定情報を含む管理情報を設定する（ステップS45）。

[0132] 例えば、通信管理装置14の制御部91は、無線ドングル15がセットされたIoTデバイス11のポート16を監視するために、情報処理装置13Aが無線ドングル15と通信する間隔（監視間隔）などを示す監視設定情報を含む管理情報を設定する。また、通信管理装置14の制御部91は、IoTデバイス11の識別情報、無線ドングル15の識別情報および情報処理装置13Aの識別情報などを対応づけて記憶部92に保存して管理するようにしても良い。

通信管理装置14の制御部91は、監視設定情報を含む管理情報を設定すると、監視設定情報を情報処理装置13Aへ送信する（ステップS46）。

[0133] 情報処理装置13Aは、通信部32により通信管理装置14から監視設定

情報を受信する。情報処理装置 13 A の制御部 30 は、監視設定情報を受信すると、受信した監視設定情報に基づいて無線ドングル 15 がセットされた I o T デバイス 11 のポート 16 に対する監視設定を行う（ステップ S 47）。例えば、情報処理装置 13 A の制御部 30 は、監視設定として、無線ドングル 15 と通信する間隔（監視間隔）、および、異常と判定する通信不可の期間（異常検知期間）などを設定する。

[0134] 情報処理装置 13 A の制御部 30 は、監視設定が完了すると、監視設定に従って無線ドングル 15 との通信を行う（ステップ S 48）。例えば、情報処理装置 13 A の制御部 30 は、無線通信部 35 により監視設定で設定される監視間隔で無線ドングル 15 へ応答要求を送信する。無線ドングル 15 は、無線通信部 62 により情報処理装置 13 A からの応答要求を受信し、応答要求に対する応答（レスポンス）を情報処理装置 13 A へ送信する。これにより、情報処理装置 13 A は、監視間隔ごとに無線ドングル 15 が I o T デバイス 11 のポート 16 にセットされていることを確認できる。

[0135] すなわち、情報処理装置 13 A の制御部 30 は、無線ドングル 15 との通信が不可であった場合（ステップ S 49、NO）、通信不可が継続している期間が異常と判定するための期間（異常検知期間）以上であるか否かを判断する（ステップ S 50）。例えば、監視間隔を 500 m s とし、異常検知期間を 10 s とした場合、制御部 30 は、監視間隔ごとの通信が 20 回連続で通信不可となると、異常を検知する。

[0136] 情報処理装置 13 A の制御部 30 は、無線ドングル 15 との正常に通信できた場合（ステップ S 49、NO）、又は、通信不可が継続している期間が異常検知期間未満である場合（ステップ S 50、NO）、監視間隔ごとの無線ドングル 15 との通信を繰り返す。

[0137] 情報処理装置 13 A の制御部 30 は、通信不可が継続している期間が異常検知期間以上である場合（ステップ S 50、YES）、無線ドングル 15 とセットした I o T デバイス 11 のネットワーク通信を遮断する（ステップ S 51）。

- [0138] さらに、情報処理装置 13 A の制御部 30 は、通信不可が継続している期間が異常検知期間以上である場合（ステップ S50、YES）、IoT デバイス 11 のポート 16 にセットした無線ドングル 15 が通信不可となった旨の異常通知を通信部 32 により通信管理装置 14 へ送信する（ステップ S52）。
- [0139] 通信管理装置 14 は、NW 通信部 90 により情報処理装置 13 A からの異常通知を受信する。通信管理装置 14 の制御部 91 は、情報処理装置 13 A から異常通知を受信すると、予め設定されている管理者に異常を報知する（ステップ S53）。
- [0140] 例えば、通信管理装置 14 の制御部 91 は、通知先として予め設定されている管理者の通知先（管理者の端末機器あるいは管理者のメールアドレス）に IoT デバイス 11 のポート 16 にセットした無線ドングル 15 との通信が不可となった旨又は無線ドングル 15 との通信不可によって IoT デバイス 11 のネットワーク通信を遮断した旨の通知を送信する。例えば、管理者は、ネットワークに接続する自身の端末機器（コンピュータ）で通信管理装置 14 からの通知を受ける。
- [0141] また、通信管理装置 14 の制御部 91 は、IoT デバイス 11 のポート 16 にセットした無線ドングル 15 との通信が不可となった旨又は無線ドングル 15 との通信不可によって IoT デバイス 11 のネットワーク通信を遮断した旨を通信管理装置 14 に接続した表示装置に表示することにより、管理者に異常を報知するようにしても良い。
- [0142] 通信管理装置 14 の制御部 91 は、無線ドングル 15 との通信不可によって IoT デバイス 11 のネットワーク通信を遮断したことを管理者に異常を報知した場合、管理者からの IoT デバイス 11 によるネットワーク通信の再開指示を受け付ける（ステップ S54）。例えば、管理者は、ネットワークに接続する自身の端末機器（コンピュータ）で通信管理装置 14 にログインし、IoT デバイス 11 の状態を確認したり、IoT デバイスの通信再開を指示したりする。

- [0143] 通信管理装置 14 の制御部 91 は、管理者から IoT デバイス 11 のネットワーク通信の再開が指示されると、NW 通信部 90 により情報処理装置 13 A へネットワーク通信の再開指示を送信する（ステップ S55）。
- [0144] 情報処理装置 13 A は、通信部 32 により通信管理装置 14 からの IoT デバイス 11 のネットワーク通信の再開指示を受信する。情報処理装置 13 A の制御部 30 は、IoT デバイス 11 のネットワーク通信が再開指示を受けた場合、IoT デバイス 11 のネットワーク通信を許可（再開）する。情報処理装置 13 A の制御部 30 は、ネットワーク通信を再開した場合、上記ステップ S43 と同様に無線ドングル 15 との相互認証を再度実行することにより、IoT デバイス 11 における無線ドングル 15 がセットされたポート 16 の監視を行うようにしても良い。
- [0145] なお、情報処理装置 13 A は、IoT デバイス 11 を電源オフした場合にも無線ドングル 15 との通信が不可となる。このため、情報処理装置 13 A は、IoT デバイス 11 の電源のオンオフ状態を検出し、IoT デバイス 11 の電源がオフであれば、無線ドングル 15 との無線通信によるポート 16 の監視（異常検知）を中止するようにしても良い。また、情報処理装置 13 A は、電源オフした IoT デバイス 11 の再び電源オンとなったことを検出した場合、無線ドングル 15 との無線通信を再開して上述したようなポート 16 の監視を実行するようにしても良い。
- [0146] また、情報処理装置 13 A が IoT デバイス 11 の電源のオンオフ状態が検出できない場合、情報処理装置 13 A は、上述した動作によって IoT デバイス 11 のネットワーク通信を遮断する。この場合、情報処理装置 13 A は、管理者やオペレータによるスイッチ 36 への指示に応じて IoT デバイス 11 のポート 16 に装着した無線ドングル 15 との通信を再開することによりポート 16 の監視を行うようにしても良い。
- [0147] すなわち、情報処理装置 13 A は、スイッチ 36 への指示に応じて無線ドングル 15 を装着した IoT デバイス 11 のポート 16 の監視を行うようにしても良い。例えば、情報処理装置 13 A の制御部 30 は、スイッチ 36 が

指示されると、図8のステップS43へ進み、IoTデバイス11のポート16に装着した無線ドングル15との相互認証を実行するようにしても良い。この場合、情報処理装置13Aは、スイッチ36への指示に応じて無線ドングルとの通信を開始することができ、無線ドングルとの通信によるIoTデバイス11のポート16の監視を行える。

[0148] 以上のように、実施形態に係る通信システムによれば、情報処理装置に接続されるIoTデバイスの空きポートには無線ドングルがセットされる。IoTデバイスが接続される情報処理装置は、通信管理装置から指示される監視設定情報に従ってIoTデバイスのポートにセットされた無線ドングルと定期的（継続的）に無線通信する。情報処理装置は、無線ドングルとの通信不可状態が異常検知期間以上継続した場合、通信管理装置へ異常を通知し、IoTデバイスをネットワークから遮断する。

[0149] これにより、情報処理装置および通信管理装置は、IoTデバイスの空きポートの状態を監視できる。また、無線ドングルがIoTデバイスの空きポートを物理的に塞ぐことにより、IoTデバイスの空きポートに任意の不特定な外部機器が接続されることを防止できる。

[0150] また、IoTデバイスの空きポートを物理的に塞ぐ無線ドングルが取り外されると、IoTデバイスの空きポートに外部機器が接続される可能性が高まるが、情報処理装置は、無線ドングルとの通信が不可となった場合にIoTデバイスをネットワークから遮断して通信管理装置に異常を通知することで、IoTデバイスの空きポートに任意の外部機器が接続されることで生じるリスクを低減できる。例えば、通信システムとしては、IoTデバイスが空きポートに無線ドングル以外の不正な外部機器が接続された状態でネットワーク通信を行うことを防止できる。

[0151] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことが

できる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

- [請求項1] 情報処理装置と無線器とを有する通信システムにおいて、
前記無線器は、
保護対象機器のポートに装着する接触部と、
前記接触部が前記保護対象機器のポートに装着された状態において
前記情報処理装置と無線通信する第1無線通信部と、を有し、
前記情報処理装置は、
前記保護対象機器に接続する第1通信インターフェースと、
ネットワークに接続する第2通信インターフェースと、
前記無線器と無線通信する第2無線通信部と、
前記無線器との通信不可状態が異常検知期間以上継続した場合、前
記保護対象機器の前記ネットワークを介した通信を遮断する制御部と
、を有する、
通信システム。
- [請求項2] 前記制御部は、前記無線器との通信不可状態が異常検知期間以上継
続した場合、前記保護対象機器の前記第1通信インターフェース及び
前記第2通信インターフェースを介した前記ネットワークとの通信の
みを遮断する、
請求項1に記載の通信システム。
- [請求項3] 前記情報処理装置の前記制御部は、前記第2通信インターフェース
により前記ネットワークを介して通信する通信管理装置から指定され
る監視設定情報に従って前記無線器と通信する間隔を設定する、
請求項1に記載の通信システム。
- [請求項4] 前記情報処理装置の前記制御部は、前記通信管理装置から指定され
る監視設定情報に従って前記異常検知期間を設定する、
請求項3に記載の通信システム。
- [請求項5] 前記無線器は、さらに、前記第1無線通信部により無線通信する前
記情報処理装置との相互認証を実行するマイコンを有し、

前記情報処理装置の前記制御部は、前記第2無線通信部により無線通信する前記無線器との相互認証が成功した後に前記保護対象機器のポートに装着された前記無線器との通信を開始する、

請求項1に記載の通信システム。

[請求項6]

前記情報処理装置の前記制御部は、前記無線器との通信不可状態が異常検知期間以上継続した場合、前記第2通信インターフェースにより前記ネットワークを介して通信管理装置へ前記保護対象機器における前記無線器を装着したポートの異常を通知する、

請求項1に記載の通信システム。

[請求項7]

さらに、前記通信システムは、前記通信管理装置を有し、

前記通信管理装置は、

前記情報処理装置と前記ネットワークを介して通信するネットワーク通信部と、

前記ネットワーク通信部により前記情報処理装置から前記保護対象機器における前記無線器を装着したポートの異常通知を受信した場合、前記保護対象機器における異常を管理者に報知する制御部と、を有する、

請求項6に記載の通信システム。

[請求項8]

前記通信管理装置の制御部は、前記管理者から前記保護対象機器のネットワークを介した通信の再開が指示された場合、前記ネットワーク通信部により前記情報処理装置に前記保護対象機器のネットワークを介した通信の再開を指示し、

前記情報処理装置の前記制御部は、前記通信管理装置から前記保護対象機器のネットワーク通信の再開指示を受信した場合、前記保護対象機器のネットワークを介した通信を再開する、

請求項7に記載の通信システム。

[請求項9]

保護対象機器に接続する第1通信インターフェースと、

ネットワークに接続する第2通信インターフェースと、

保護対象機器のポートに装着された状態で動作する無線器と無線通信する無線通信部と、

前記無線器との通信不可状態が異常検知期間以上継続した場合、前記保護対象機器の前記ネットワークを介した通信を遮断する制御部と、を有する、

情報処理装置。

[請求項10]

保護対象機器の状態を監視する監視方法であって、

保護対象機器とネットワークとの間に接続される情報処理装置と前記保護対象機器のポートに装着された無線器とが無線通信し、

前記情報処理装置と前記無線器との通信不可状態が異常検知期間以上継続した場合、情報処理装置が前記保護対象機器の前記ネットワークを介した通信を遮断する、

監視方法。