

明 細 書

発明の名称： 情報処理装置および通信システム

技術分野

[0001] 本発明の実施形態は、情報処理装置および通信システムに関する。

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] 従来、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に、既存のデバイスとネットワークとの間に接続される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、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、従来の情報処理装置は、既存のデバイスやシステムの可用性を重視した設計となるため、起動時において通信許可設定が反映されるまでの間に情報処理装置の全ての通信ポートがリンクアップされる。つまり、

従来の情報処理装置は、起動時などにおいて通信許可設定が反映されずに全ての通信ポートがリンクアップされることで通信許可されていない通信経路での通信が可能になってしまう可能性があるという問題がある。このため、システム全体の可用性を担保しながら、完全なセキュリティ対策を実現できる情報処理装置および通信システムが要望されている。

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、通信設定を遵守できる情報処理装置および通信システム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、情報処理装置は、端末装置と前記端末装置とネットワークを介して通信するサーバ装置との間に接続される。情報処理装置は、第1通信部と第2通信部と制御部とを有する。第1通信部は、サーバ装置にネットワークを介して接続する。第2通信部は、端末装置に接続する。制御部は、第1通信部により通信管理装置にリンクアップし、端末装置と他の端末装置との通信可否を示す通信設定情報に基づく通信設定が完了した後に第2通信部により端末装置にリンクアップする。

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制御装置における認証部の構成例としてのＣカードにおける機能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7]図７は、実施形態に係る通信システムにおけるデバイス側の情報処理装置による第１の通信設定処理を説明するためのフローチャートである。

[図8]図８は、実施形態に係る通信システムにおけるデバイス側の情報処理装置による第２の通信設定処理を説明するためのフローチャートである。

[図9]図９は、実施形態に係る通信システムにおけるデバイス側の情報処理装置による第３の通信設定処理を説明するためのフローチャートである。

[図10]図１０は、実施形態に係る通信システムにおけるデバイス側の情報処理装置による第４の通信設定処理を説明するためのフローチャートである。

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）１１（１１Ａ、１１Ｂ、１１Ｃ）、サーバ装置１２、情報処理装置１３（１３Ａ、１３Ｂ、１３Ｃ、１３Ｄ）、通信管理装置１４、スイッチ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、スイッチ１５、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（１１Ａ、１１Ｂ、１１Ｃ）、サーバ装置１２、通信管理装置１４、スイッチ１５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で通信システム1を構築するように設置される。情報処理装置13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ポート（例えば、第1のLANポート）21と第2ポート（例えば、第2のLANポート）22とを備える。例えば、情報処理装置13Aは、第1ポート21Aをスイッチ15に接続し、第2ポート22AをIoTデバイス11Aに接続することにより、IoTデバイス11Aとスイッチ15との間に接続される。
- [0013] 各IoTデバイス11A、11B、11Cは、それぞれに接続されるデバイス側の情報処理装置13A、13B、13Cを介してネットワークNWと接続する。サーバ装置12は、サーバ側の情報処理装置13Dを介してネットワークNWと接続する。すなわち、各IoTデバイス11A、11B、11Cとサーバ装置12とは、それぞれに接続された情報処理装置13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。
- [0014] IoTデバイス11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、IoTデバイス11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。IoTデバイス11は、取得したなデータをサーバ装置12へ送信する。また、IoTデバイス11は、サーバ装置12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あっても良い。
- [0015] 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。
- [0016] デバイス側の情報処理装置13A、13B、13Cは、IoTデバイス11A、11B、11CとネットワークNWのスイッチ15との間に接続される。デバイス側の情報処理装置13A、13B、13C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ポート21A、21B

、 2 1 C とデバイス側のインターフェース接続部としての第 2 ポート 2 2 A 、 2 2 B 、 2 2 C とを有する。第 1 ポート 2 1 A 、 2 1 B 、 2 1 C および第 2 ポート 2 2 A 、 2 2 B 、 2 2 C 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 ポート 2 1 A 、 2 1 B 、 2 1 C には、スイッチ 1 5 が接続され、第 2 ポート 2 2 A 、 2 2 B 、 2 2 C には、それぞれ IoT デバイス 1 1 A 、 1 1 B 、 1 1 C が接続される。

[0017] デバイス側の情報処理装置 1 3 A 、 1 3 B 、 1 3 C は、IoT デバイス 1 1 A 、 1 1 B 、 1 1 C 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 、 1 3 B 、 1 3 C は、IoT デバイス 1 1 A 、 1 1 B 、 1 1 C 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 、 1 3 B 、 1 3 C は、サーバ装置 1 2 に対してデータを送信する際に、IoT デバイス 1 1 A 、 1 1 B 、 1 1 C 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。

[0018] また、情報処理装置 1 3 A 、 1 3 B 、 1 3 C は、サーバ装置 1 2 により IoT デバイス 1 1 A 、 1 1 B 、 1 1 C 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 1 1 A 、 1 1 B 、 1 1 C に対して出力する。ここで、情報処理装置 1 3 A 、 1 3 B 、 1 3 C 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 、 1 3 B 、 1 3 C は、IoT デバイス 1 1 A 、 1 1 B 、 1 1 C 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 D を介して取得したデータを復号し、復号したデータを IoT デバイス 1 1 A 、 1 1 B 、 1 1 C に出力する。

[0019] さらに、デバイス側の情報処理装置 1 3 A 、 1 3 B 、 1 3 C は、スイッチ 1 5 を介してデバイス側の他の情報処理装置 1 3 A 、 1 3 B 、 1 3 C と通信可能な構成を備える。デバイス側の各情報処理装置 1 3 A 、 1 3 B 、 1 3 C 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 、 1 3 B 、 1 3 C との通信の可否が設定される。

[0020] サーバ側の情報処理装置 1 3 D 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 13 D 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 ポート 21 D とサーバ側のインターフェース接続部としての第 2 ポート 22 D とを有する。第 1 ポート 21 D には、ネットワーク 18 が接続され、第 2 ポート 22 D には、サーバ装置 12 が接続される。

[0021] サーバ側の情報処理装置 13 D は、各 IoT デバイス 11 とサーバ装置 12 との間の通信を仲介する。サーバ側の情報処理装置 13 D 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 13 D 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。

[0022] また、サーバ側の情報処理装置 13 D 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 13 D 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 13 D 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 13 A、13 B、13 C 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。

[0023] 各情報処理装置 13 (13 A、13 B、13 C、13 D) は、例えば、SSL (Secure Socket Layer) / TLS (Transport Layer Security) のプロトコルによる暗号化を実行する。デバイス側の情報処理装置 13 A、13 B、13 C およびサーバ側の情報処理装置 13 D は、例えば、SSL / TLS プロトコルを、HTTP 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。

[0024] なお、デバイス側の情報処理装置 13 A、13 B、13 C およびサーバ側の情報処理装置 13 D 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。情報処理装置13およびサーバ側の情報処理装置13Dは、SSL/TLSプロトコルを種々の通信プロトコル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プロトコル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、13B、13Cおよびサーバ側の情報処理装置13Dは、FTP (File Transfer Protocol) をFTPS (FTP Secure) に置き換えてもよい。

[0025] 通信システム1において、デバイス側の情報処理装置13A、13B、13C又はサーバ側の情報処理装置13D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。

[0026] 通信管理装置14は、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13D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14は、プライベート認証局としても機能する。通信管理装置14は、各情報処理装置13に対し、クライアント証明書および秘密鍵を発行する。

[0027] 図1に示す構成例において、通信管理装置14は、情報処理装置13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13A、13B、13C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14は、情報処理装置13A、13B、13C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。

[0028] また、通信管理装置14は、サーバ側の情報処理装置13D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13D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１４は、サーバ側の情報処理装置１３Ｄ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１３Ａ、１３Ｂ、１３Ｃとサーバ側の情報処理装置１３Ｄ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。

[0029] ここで、ＩｏＴデバイス１１およびサーバ装置１２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。

[0030] 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。

[0031] 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。

[0032] 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。

[0033] 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、１３Ｂ、１３Ｃ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１３Ｄすることで構築できるシステムである。

[0034] 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。

[0035] 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１１Ａ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１３Ｄを介してサーバ装置１２と通信する。

- [0036] また、本実施形態に係る通信システム１において、各ＩｏＴデバイス１１は、ゲートウェイ１７よりも手間で他のＩｏＴデバイス１１と通信可能に設定できる。すなわち、各ＩｏＴデバイス１１は、自機に接続した情報処理装置１３、スイッチ１５および他機に接続した情報処理装置を介して他のＩｏＴデバイスとも通信可能に設定できる。例えば、ＩｏＴデバイス１１Ａは、情報処理装置１３Ａ、スイッチ１５および情報処理装置１３Ｂを介してＩｏＴデバイス１１Ｂと通信可能に設定することも可能である。デバイス側の各情報処理装置１３Ａ、１３Ｂ、１３Ｃは、通信許可設定に従って、ＩｏＴデバイス間の通信可否を設定する。
- [0037] 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。
- [0038] 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１３Ｄに接続され、情報処理装置１３Ｄ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１３Ｄを接続することで構築できるシステムである。
- [0039] 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。

[0040] 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。

[0041] 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。

[0042] 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 I o T デバイスにハードウェア構成を変更したり既存の I o T デバイスを新たな I o T デバイスに置き換えたりすることなく、既存の I o T 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。

[0043] すなわち、通信システム 1 において、I o T デバイス 1 1 とネットワーク NW との間に接続された情報処理装置 1 3 は I o T デバイス 1 1 がサーバ装置 1 2 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 1 2 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 1 3 D はサーバ装置 1 2 からの I o T デバイス 1 1 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、I o T デバイス 1 1 およびサーバ装置 1 2 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。

[0044] また、図 1 に示す通信システム 1 において、ゲートウェイ 1 7 を介してネットワーク 1 8 に接続されるスイッチ 1 5 は、デバイス側の各情報処理装置 1 3 A、1 3 B、1 3 C を介して I o T デバイス 1 1 A、1 1 B、1 1 C 同士で通信可能なローカルなシステムを構成する。すなわち、通信システム 1 は、I o T デバイス 1 1 A、1 1 B、1 1 C がスイッチ 1 5 とデバイス側の各情報処理装置 1 3 A、1 3 B、1 3 C を介して他の I o T デバイスと通信可能な構成を備える。スイッチ 1 5 を介した I o T デバイス 1 1 A、1 1 B、1 1 C 間の通信は、情報処理装置 1 3 A、1 3 B、1 3 C によって制御される。

[0045] 例えば、I o T デバイス 1 1 A と I o T デバイス 1 1 B との通信を不可とする場合、情報処理装置 1 3 A および 1 3 B には、I o T デバイス 1 1 A と I o T デバイス 1 1 B との通信を不可とする設定（通信許可設定）を含む通信設定が適用される。本実施形態に係る情報処理装置 1 3 A、1 3 B、1 3 C は、通信許可設定が適用されたことを確認した後に、スイッチ 1 5 を介した I o T デバイス 1 1 A、1 1 B、1 1 C 間の通信を実行する。

[0046] 換言すれば、情報処理装置13A、13B、13Cは、通信許可設定が反映（適用）された状態でスイッチ15を介したIoTデバイス11A、11B、11C間の通信を許可し、通信許可設定が反映されていない状態ではスイッチ15を介したIoTデバイス11A、11B、11C間の通信を不可とする。これにより、各情報処理装置13は、通信設定を遵守でき、起動処理などにおいて通信許可設定で通信が不可に設定されているIoTデバイス11間の通信が許可されることがないようにできる。

[0047] 次に、実施形態に係る情報処理装置13（13A、13B、13C、13D）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（13A、13B、13C、13D）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（13A、13B、13C、13D）は、制御部30、第1通信部31、第2通信部32、リーダライタ33、および、ICカード34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であり、情報処理装置13（13A、13B、13C、13D）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（13A、13B、13C、13D）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（13A、13B、13C、13D）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に接続される第1ポート21（21A、21B、21C）を備える。第1通信部31は、ネットワークNWを介

して、他方の情報処理装置 13 (13 A、13 B、13 C、13 D) と通信を行う。具体的には、デバイス側の情報処理装置 13 A、13 B、13 C の第 1 通信部 31 は、第 1 ポート 21 A、21 B、21 C に接続されるスイッチ 15 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スイッチ 15 を介してゲートウェイ 17 へ出力する。また、サーバ側の情報処理装置 13 D の第 1 通信部 31 は、第 1 ポート 21 D 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。

[0050] 第 2 通信部 32 は、通信を実行する装置 (IoT デバイス 11、又はサーバ装置 12) に接続される第 2 ポート 22 (22 A、22 B、22 C) を備える。第 2 通信部 32 は、IoT デバイス 11、又はサーバ装置 12 と通信を行う。具体的には、デバイス側の情報処理装置 13 A、13 B、13 C の第 2 通信部 32 は、第 2 ポート 22 A、22 B、22 C に接続される IoT デバイス 11 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 13 D の第 2 通信部 32 は、第 2 ポート 22 D 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。

[0051] また、本実施形態の構成によれば、デバイス側の情報処理装置 13 A、13 B、13 C は、スイッチ 15 を介して他のデバイス側の各情報処理装置と通信可能である。デバイス側の各情報処理装置 13 A、13 B、13 C は、通信許可設定に従って他のデバイス側の各情報処理装置 13 A、13 B、13 C との通信可否が設定される。本実施形態に係る情報処理装置 13 は、通信許可の設定 (セキュリティモード) 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 (リンクアップする)。

[0052] すなわち、第 1 通信部 31 は、第 1 ポート 21 A (21 B、21 C) を介して通信管理装置 14 と通信するためにリンクされる。第 2 通信部 32 は、

第1通信部31が第1ポート21A(21B、21C)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(13B、13C)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ポート22A(22B、22C)を介してIoTデバイス11A(11B、11C)にリンクアップされる。

[0053] 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。

[0054] 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、13C、13D)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、13C、13D)と通信する。

[0055] ICカード34は、例えば、情報処理装置13(13A、13B、13C、13D)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、13C、13D)にコンタクト部41を介して送信する。

[0056] 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、13C、13D)から供給を受ける端子、および、情報処理装置13(13A、13B、13C

、13D)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。

[0057] 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 Transmitter)43、CPU44と、ROM(Read Only Memory)45、RAM(Random Access Memory)46、および、EEPROM(登録商標)(Electrically Erasable Programmable ROM)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。

[0058] UART43は、上述したSIO端子を介して、情報処理装置13(13A、13B、13C、13D)とシリアルデータ通信を行う。UART43は、SIO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、UART43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、SIO端子を介して情報処理装置13(13A、13B、13C、13D)に出力する。UART43は、例えば、SIO端子を介してコマンドを情報処理装置13(13A、13B、13C、13D)から受信する。また、UART43は、SIO端子を介してレスポンスを情報処理装置13(13A、13B、13C、13D)に送信する。

[0059] CPU44は、ROM45又はEEPROM47に記憶されているプログラムを実行して、ICカード34の各種処理を行う。CPU44は、例えば、コンタクト部41を介して、UART43が受信したコマンドに応じたコ

マンド処理を実行する。

[0060] ROM45は、例えば、マスクROMなどの不揮発性メモリであり、IC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。RAM46は、例えば、SRAM(Static RAM)などの揮発性メモリであり、IC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。EEPROM47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。EEPROM47は、ICカード34が利用する各種データを記憶する。EEPROM47は、例えば、IC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。

[0061] 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。

[0062] 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、13C、13D)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、13C、13D)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、13C、13D)に送信する。通信部50は、UART43を介して情報処理装置13(13A、13B、13C、13D)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、13C、13D)に送信する。

- [0063] 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RAM45とROM46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。
- [0064] 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、13B又は13Cとサーバ側の情報処理装置13D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。
- [0065] 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。
- [0066] 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13D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。
- [0067] 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 1 3 に装着される I C カード 3 4 の秘密情報記憶部 5 6 には、情報処理装置 1 3 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 1 3 D に装着される I C カード 3 4 の証明書情報記憶部 5 5 には、サーバ側の情報処理装置 1 3 D に対して発行された秘密鍵を示す情報が記憶される。

[0068] 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 1 4 の構成について説明する。

図 5 は、図 1 に示す通信管理装置 1 4 の構成例を示すブロック図である。

通信管理装置 1 4 は、NW（ネットワーク）通信部 6 0、制御部 6 1 および記憶部 6 2 を備える。

NW 通信部 6 0 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 1 3（1 3 A、1 3 B、1 3 C、1 3 D）と通信を行う。

[0069] 制御部 6 1 は、例えば、CPU などのプロセッサを含む。制御部 6 1 は、プロセッサが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 6 1 は、通信管理装置 1 4 を統括的に制御する。制御部 6 1 は、情報処理装置 1 3 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 6 1 は、主に情報処理装置 1 3（1 3 A、1 3 B、1 3 C、1 3 D）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 6 に示す例において、制御部 6 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。

[0070] 鍵生成部 7 1 は、例えば、情報処理装置 1 3（1 3 A、1 3 B、1 3 C、1 3 D）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。

[0071] 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、1 3 C、1 3 D）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、1 3 C、1 3 D）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 13（13A、13B、13C、13D）の所有者を示す情報とが含まれる。

[0072] 証明書更新部 73 は、有効期限が渡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 73 は、例えば、情報処理装置 13（13A、13B、13C、13D）からの更新申請に基づいて、当該情報処理装置 13（13A、13B、13C、13D）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 13（13A、13B、13C、13D）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 13（13A、13B、13C、13D）により受信され、情報処理装置 13（13A、13B、13C、13D）の IC カード 34 の証明書情報記憶部 55 に記憶されることで、情報処理装置 13（13A、13B、13C、13D）の証明書の有効期限が延長される。

[0073] 証明書管理部 74 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 74 は、例えば、情報処理装置 13（13A、13B、13C、13D）に装着された IC カード 34 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 13（13A、13B、13C、13D）に対して発行した証明書を無効化する処理を行う。

[0074] また、証明書管理部 74 は、情報処理装置 13（13A、13B、13C、13D）からの問い合わせに基づいて、情報処理装置 13（13A、13B、13C、13D）、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 72 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 74 は、定期的に、発行済みの証明書が正当な情報処理装置 13（13A、13B、13C、13D）に使用されているかを確認するようにしてもよい。

[0075] 管理部 75 は、情報処理装置 13（13A、13B、13C、13D）を管理する。例えば、管理部 75 は、情報処理装置 13（13A、13B、13C、13D）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 6 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。

[0076] 通信設定記憶部 8 3 は、各情報処理装置 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 に記憶する通信設定情報は、デバイス側の各情報処理装置 1 3 に設定する通信許可設定を含む。制御部 6 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 6 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。また、制御部 6 1 は、通信設定情報を予め各情報処理装置 1 3 に予め供給しておき、各情報処理装置 1 3 が記憶部 5 4 などに記憶しておくようにしても良い。ただし、通信システム 1 が通信設定情報を必要に応じて通信管理装置 1 4 からダウンロード（取得）する実施形態とする場合、記憶部 6 2 には、通信設定情報を保存する通信設定記憶部 8 3 を設けなくても良い。

[0077] 次に、通信システム 1 における IoT デバイス 1 1 とサーバ装置 1 2 との間における通信処理について説明する。

図 6 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。

[0078] IoT デバイス 1 1 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 1 2 に送信する場合、まずサーバ装置 1 2 に対する HTTP リクエストを送信する（ステップ S 1）。IoT デバイス 1

1 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、13B、13C) により取得される (ステップ S2)。

[0079] 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 13D に対して、HTTPS のリクエスト (Client Hello) 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 13D との間のハンドシェイクが開始される (ステップ S4)。

[0080] 具体的には、デバイス側の情報処理装置 13 が送信する Client Hello 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 13D は、Client Hello 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 (Server Hello) を送信する。サーバ側の情報処理装置 13D が送信する Server Hello には、例えば Client Hello 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 13D 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。

[0081] そして、サーバ側の情報処理装置 13D 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 13 は、サーバ側の情報処理装置 13D 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。

[0082] 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 13D 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 13 は、今までに受信した Server Hello 等から署名を生成し、サーバ側の情報処理装置 13D に送信する。サーバ側の情報処理装置 13D は、デバ

イス側の情報処理装置 13 から受信した署名をデバイス側の情報処理装置 13 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 13 D 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 13 のものであると判定する。また、サーバ側の情報処理装置 13 D は、今までに受信した Client Hello 等から署名を生成し、デバイス側の情報処理装置 13 に送信する。デバイス側の情報処理装置 13 は、サーバ側の情報処理装置 13 D から受信した署名を、サーバ側の情報処理装置 13 D 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 13 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 13 D のものであると判定する。

[0083] 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 13 D 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 13 とサーバ側の情報処理装置 13 D 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。

[0084] サーバ側の情報処理装置 13 D から送付されたサーバ装置 12 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 13 に許容される証明書であれば、サーバ側の情報処理装置 13 D は、デバイス側の情報処理装置 13 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 13 D 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。

[0085] サーバ側の情報処理装置 13 D は、デバイス側の情報処理装置 13 とのハンドシェイクが確立されると、サーバ装置 12 に対し、HTTP リクエストを送信する（ステップ S5）。HTTP リクエストは、ステップ S1 において IoT デバイス 11 から送信される HTTP リクエストである。

[0086] サーバ側の情報処理装置 13 D により送信された HTTP リクエストは、サーバ装置 12 により受信される（ステップ S6）。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 に対しする 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

Pレスポンスは、サーバ側の情報処理装置13Dにより取得される（ステップS8）。

[0087] サーバ側の情報処理装置13D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13D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13に受信される（ステップS10）。デバイス側の情報処理装置13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13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）。

[0088] 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13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13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13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13Dに受信される（ステップS17）。

[0089] サーバ側の情報処理装置13D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13D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。

[0090] なお、上記フローチャートのステップS4において、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13D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 13 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 13 は、通信先から送信された情報を IoT デバイス 11 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 13 D 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 13 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 14 に送信するようにしてもよい。これより、通信管理装置 14 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 13 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。

[0091] また、デバイス側の情報処理装置 13 は、上記フローチャートのステップ S4 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 IoT デバイス 11 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 13 の制御部 30 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。

[0092] また、制御部 30 は、送信先リストを更新するようにしてもよい。制御部 30 は、例えば、一定期間に IoT デバイス 11 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 30 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 と通信を行った通信先 URL

L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と通信する通信機器を一括して管理することができる。

[0093] また、デバイス側の情報処理装置13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およびサーバ側の情報処理装置13Dそれぞれに検証鍵を送信するようにしてもよい。

[0094] 例えば、サーバ側の情報処理装置13D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13D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。

[0095] また、デバイス側の情報処理装置13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13は、復号した情報（平文）をIoTデバイス11に出力する。一方、デバイス側の情報処理装置13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、IoTデバイス11に対して送信された情報は、サーバ装置12又はサーバ側の情報処理装置13D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13は、復号した情報（平文）をIoTデバイス11に出力しない。

[0096] これにより、IoTデバイス11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、IoTデバイス11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、IoTデバイス11に代わりサーバ側の情報処理装置13DがIoTデバイス11に対して送信された情報の内容を検証することにより、IoTデバイス11の処理負担を軽減させることが可能となる。

[0097] 以上説明したように、通信システム1は、IoTデバイス11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13と、サーバ装置12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13Dと、を備える。デバイス側の情報処理装置13は、IoTデバイス11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13Dへ送信し、ネットワークNWからの情報（情報処理装置13Dで暗号化されたサーバ装置12からの情報）を復号してIoTデバイス11へ送信する。サーバ側の情報処理装置13Dは、サーバ装置12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13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で暗号化されたIoTデバイスからの情報）を復号してサーバ装置12に送信する。

[0098] 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。IoTデバイス11からサーバ装置12に対して送信されたHTTP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が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。

[0099] また、通信システム 1 では、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 13D 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 とサーバ側の情報処理装置 13D 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。

[0100] 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たと、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。

[0101] 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 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。

- [0102] 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。
- [0103] 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13D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。
- [0104] 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13D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。
- [0105] 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13D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12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13Dに接続されたサーバ装置12が通信管理装置14の管理下であることが明確となる。サーバ装置12が既にサーバ側の情報処理装置13D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 D 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 D 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 との間の認証処理が行われる。

[0106] また、通信システム 1 では、ＩＣカード 3 4 の制御部 4 0 1 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、1 3 C、1 3 D) の装置コストを抑制することができる。

[0107] 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、1 3 C、1 3 D) 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。

[0108] 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。

[0109] 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 D 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 D 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。

[0110] 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。

[0111] 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。

[0112] 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。

[0113] 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11やサーバ装置12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14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14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。

[0114] また、通信システム1においては、情報処理装置13は、定期的に、自装置が接続されているIoTデバイス11又はサーバ装置12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14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14は、情報処理装置13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13がIoTデバイス11又はサーバ装置12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13を無効とする。こうすることで通信管理装置14は、切り離された情報処理装置13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。

[0115] また、通信システム1においては、情報処理装置13に装着するICカード34に、CC (Common Criteria/ISO15408) 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。

[0116] 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13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11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12からIoTデバイス11に対してファームウェアが送信される場合、サーバ装置12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13D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 1 2 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 1 2 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 I o T デバイス 1 1 に送信されてしまった場合であっても、I o T デバイス 1 1 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。

[0117] また、このように情報処理装置 1 3 を介して通信が行われることにより、サーバ装置 1 2 や通信管理装置 1 4 等から I o T デバイス 1 1 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 I o T デバイス 1 1 に対して物理的に各々の I o T デバイス 1 1 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。

[0118] 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、I o T デバイス 1 1 の起動や停止を行ってもよい。情報処理装置 1 3 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 I o T デバイス 1 1 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。

[0119] また、通信システム 1 においては、I o T デバイス 1 1、およびサーバ装置 1 2 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。I o T デバイス 1 1、およびサーバ装置 1 2 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、I o T デバイス 1 1 が無線通信によりサーバ装置 1 2 と通信を行う場合、情報処理装置 1 3 は、無線による通信機能を有し、I o T デバイス 1 1 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 1 2 に送信する。

[0120] 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 D 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 13B と通信を行ってもよい。情報処理装置 13A は、情報処理装置 13B から通信開始の合図を受信した場合、まず情報処理装置 13B との間で相互認証を行い、情報処理装置 13B 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 13A は、情報処理装置 13B から受信した情報を IoT デバイス 11 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。

[0121] 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 13 とサーバ側の情報処理装置 13D との通信、およびデバイス側の情報処理装置 13 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。

[0122] 次に、実施形態に係る通信システム 1 における情報処理装置 13 の通信設定処理について説明する。

上記したように、実施形態に係る通信システム 1 は、不正な攻撃を検知し、攻撃者の通信を遮断する機能を備えている。さらに、デバイス側の各情報処理装置 13 は、通信許可設定に従って通信を可能するデバイスが設定される。情報処理装置 13 は、起動処理において通信許可設定を反映（設定）させる処理を実行する。

[0123] 仮に、情報処理装置 13 が通信許可設定を反映する前に（通信許可設定が設定されていない状態で）全ての通信ポートのリンクアップを実行すると、情報処理装置 13 に接続するデバイスは、通信許可設定が反映されるまでの時間に通信許可設定で通信を許可していないデバイスとの通信ができる状態になってしまう可能性がある。通信許可設定が反映されるまでの時間が短時間であっても通信を許可していないデバイスとの通信ができる状態になってしまうことは、セキュリティの脆弱性が生じてしまう可能性があることを意味する。

[0124] このため、本実施形態に係る通信システム 1 は、情報処理装置 13 の起動処理中であっても、情報処理装置 13 が常に通信許可設定を遵守できるよう

にする。以下、情報処理装置 1 3 が通信許可設定を遵守しつつ通信設定を行う通信設定処理の第 1 ～第 4 の例について説明するものとする。

[0125] まず、実施形態に係る通信システム 1 におけるデバイス側の情報処理装置 1 3 による第 1 の通信設定処理について説明する。

図 7 は、実施形態に係る通信システム 1 におけるデバイス側の情報処理装置 1 3 による第 1 の通信設定処理を説明するためのフローチャートである。

まず、情報処理装置 1 3 の制御部 3 0 は、電源の投入に応じて起動処理を開始する（ステップ S 3 1）。例えば、オペレータは、通信システム 1 の稼働時間外になると情報処理装置 1 3 へ供給する電源をオフし、稼働時間になると情報処理装置 1 3 への電源供給をオンとする。この場合、制御部 3 0 は、電源の投入に応じて各部を動作させるための起動処理を実行する。

[0126] 制御部 3 0 は、起動処理を開始すると、通信管理装置 1 4 側の通信（LAN）ポートである第 1 ポート 2 1 をリンクアップする（S 3 2）。制御部 3 0 は、第 1 ポート 2 1 を含む第 1 通信部 3 1 により、スイッチ 1 5、ゲートウェイ 1 7 およびネットワーク 1 8 を介して通信管理装置 1 4 に通信接続する。

[0127] 通信管理装置 1 4 の制御部 6 1 は、NW通信部 6 0 により起動処理を実行する情報処理装置 1 3 と通信を確立する。制御部 6 1 は、NW通信部 6 0 により情報処理装置 1 3 との通信が確立すると、当該情報処理装置 1 3 の認識完了を示す通知を送信する。

[0128] 情報処理装置 1 3 の制御部 3 0 は、通信管理装置 1 4 からの通知により当該情報処理装置が通信管理装置 1 4 によって認識されたことを確認する（S 3 3）。制御部 3 0 は、当該情報処理装置 1 3 が通信管理装置 1 4 によって認識されたことを確認すると、当該情報処理装置 1 3 に適用される通信設定情報を通信管理装置 1 4 からダウンロードする（S 3 4）。

[0129] 第 1 の通信設定処理において、通信管理装置 1 4 は、管理下にある各情報処理装置に適用すべき通信可否の設定を含む通信設定情報を通信設定記憶部 8 3 に保持しているものとする。例えば、通信管理装置 1 4 の制御部 6 1 は

、ある情報処理装置 1 3 との通信接続が確立した場合に認識完了の通知と共に当該情報処理装置 1 3 に適用すべき通信設定情報を送信する。また、通信管理装置 1 4 の制御部 6 1 は、認識完了の通知を送信した後に情報処理装置 1 3 からの要求に応じて通信設定情報を送信するようにしても良い。この場合、情報処理装置 1 3 の制御部 3 0 は、通信管理装置 1 4 からの認識完了の通知を受けた後に通信設定情報を通信管理装置 1 4 に要求するようにすれば良い。

[0130] 情報処理装置 1 3 の制御部 3 0 は、通信管理装置 1 4 から通信設定情報を取得すると、取得した通信設定情報に基づく通信設定を実行する（S 3 5）。例えば、制御部 3 0 は、通信設定情報が示す通信不可とする I o T デバイス（I o T デバイスに接続される情報処理装置）との通信を不可とする設定を実行する。情報処理装置 1 3 の制御部 3 0 は、他のデバイスとの通信可否を含む設定が完了すると、セキュリティモードがオンとなったことを通信管理装置 1 4 へ通知する。

[0131] 通信管理装置 1 4 の制御部 6 1 は、通信設定情報を送信した情報処理装置 1 3 からセキュリティモードのオンを示す通知を受信すると、当該情報処理装置 1 3 にセキュリティモードがオンとなったことを認識した旨の通知を送信する。

[0132] 情報処理装置 1 3 の制御部 3 0 は、通信管理装置 1 4 から通知によって当該情報処理装置 1 3 がセキュリティモードがオンとなったことを通信管理装置 1 4 が認識したことを確認する（S 3 6）。情報処理装置 1 3 の制御部 3 0 は、セキュリティモードがオンとなったことを通信管理装置 1 4 が認識したことを確認すると、I o T デバイス 1 1 側の通信（L A N）ポートである第 2 ポート 2 2 をリンクアップする（S 3 7）。ここで、情報処理装置 1 3 の制御部 3 0 は、各デバイスとの通信可否を含む設定の完了に応じて第 2 ポート 2 2 をリンクアップし、セキュリティモードがオンとなったことを通信管理装置 1 4 へ通知するようにしても良い。

[0133] 以上のような第 1 の通信設定処理によれば、情報処理装置は、起動時に通

信管理装置から通信設定情報を取得し、通信管理装置から取得した通信設定情報に従って通信を不可するデバイスを設定した後にデバイス側のポートをリンクアップする。これにより、情報処理装置は、起動時であっても通信不可に設定されている通信先と通信可能となるタイミングが発生することなく通信可否などの通信設定を遵守した運用が可能となる。

[0134] 次に、実施形態に係る通信システム 1 におけるデバイス側の情報処理装置 13 による第 2 の通信設定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 におけるデバイス側の情報処理装置 13 による第 2 の通信設定処理を説明するためのフローチャートである。

第 2 の通信設定処理において、情報処理装置 13 は、各デバイスとの通信可否を示す設定情報を含む通信設定情報を記憶部 54 に記憶しているものとする。例えば、情報処理装置 13 は、稼働中に通信管理装置 14 からダウンロードする通信設定情報を記憶部 54 に記憶しておくようにしても良い。また、IC カードリーダーライタなどを用いて通信設定情報を書き込んだ IC カード 34 を情報処理装置 13 に装着するようにしても良い。

[0135] 情報処理装置 13 の制御部 30 は、電源の投入に応じて起動処理を開始する（ステップ S41）。制御部 30 は、起動処理を開始すると、通信管理装置 14 側の通信（LAN）ポートである第 1 ポート 21 をリンクアップする（S42）。制御部 30 は、第 1 ポート 21 を含む第 1 通信部 31 により、スイッチ 15、ゲートウェイ 17 およびネットワーク 18 を介して通信管理装置 14 に通信接続する。

[0136] 通信管理装置 14 の制御部 61 は、NW 通信部 60 により起動処理を実行する情報処理装置 13 と通信を確立する。制御部 61 は、NW 通信部 60 により情報処理装置 13 との通信が確立すると、当該情報処理装置 13 へ認識完了を示す通知を送信する。

情報処理装置 13 の制御部 30 は、通信管理装置 14 からの通知により当該情報処理装置が通信管理装置 14 によって認識されたことを確認する（S43）。制御部 30 は、当該情報処理装置 13 が通信管理装置 14 によって

認識したことを確認すると、記憶部54に記憶している通信設定情報を読み出す(S44)。

[0137] 情報処理装置13の制御部30は、記憶部54から通信設定情報を読み出すと、読み出した通信設定情報に基づく通信設定を実行する(S45)。例えば、制御部30は、通信設定情報が示す通信不可とするIoTデバイス(IoTデバイスに接続される情報処理装置)との通信を不可にする設定を実行する。制御部30は、通信設定情報に基づく他のデバイスとの通信可否を含む設定が完了すると、セキュリティモードがオンとなったことを通信管理装置14へ通知する。

[0138] 通信管理装置14の制御部61は、通信設定情報を送信した情報処理装置13からセキュリティモードのオンを示す通知を受信すると、当該情報処理装置13にセキュリティモードがオンとなったことを認識した旨の通知を送信する。

[0139] 情報処理装置13の制御部30は、通信管理装置14からの通知によってセキュリティモードがオンとなったことを通信管理装置14が認識したことを確認する。

情報処理装置13の制御部30は、セキュリティモードがオンとなったことを通信管理装置14が認識したことを確認すると、IoTデバイス11側の通信(LAN)ポートである第2ポート22をリンクアップする(S47)。ここで、情報処理装置13の制御部30は、通信可否を含む通信設定情報に基づく設定が完了した場合に第2ポート22をリンクアップし、セキュリティモードがオンとなったことを通信管理装置14へ通知するようにしても良い。

[0140] 以上のような第2の通信設定処理によれば、情報処理装置は、起動時に記憶部に記憶した通信設定情報を取得に従って通信を不可するデバイスを設定した後にデバイス側のポートをリンクアップする。これにより、情報処理装置は、起動時であっても通信不可に設定されている通信先と通信可能となるタイミングが発生することなく通信可否などの通信設定を遵守した運用が可能

能となる。

[0141] 次に、実施形態に係る通信システム 1 におけるデバイス側の情報処理装置 1 3 による第 3 の通信設定処理について説明する。

図 9 は、実施形態に係る通信システム 1 におけるデバイス側の情報処理装置 1 3 による第 3 の通信設定処理を説明するためのフローチャートである。

第 3 の通信設定処理において、複数の情報処理装置 1 3 が一括した通信設定の管理対象となるものとする。1 つの管理対象となる複数の情報処理装置 1 3 は、例えば、電源が一斉にオンオフされるような運用を想定するものとする。通信管理装置 1 4 は、一括した通信設定の管理対象とする複数の情報処理装置 1 3 を示す情報を管理するものとする。また、第 3 の通信設定処理では、通信設定の管理対象とする複数の情報処理装置 1 3 の通信設定情報は通信管理装置 1 4 からダウンロードされるものとする。

[0142] ここで、図 1 に示す構成例においてスイッチ 1 5 に接続されるデバイス側の複数の情報処理装置 1 3 A、1 3 B、1 3 C が一括した通信設定の管理対象となる場合を想定して説明するものとする。通信管理装置 1 4 は、情報処理装置 1 3 A、1 3 B、1 3 C を一括した通信設定の管理対象として管理し、さらに、各情報処理装置 1 3 A、1 3 B、1 3 C に設定する通信設定情報を保持しているものとする。

[0143] 各情報処理装置 1 3 (1 3 A、1 3 B、1 3 C) の制御部 3 0 は、電源の投入に応じて起動処理を開始する(ステップ S 5 1)。制御部 3 0 は、起動処理を開始すると、通信管理装置 1 4 側の通信(LAN)ポートである第 1 ポート 2 1 をリンクアップする(S 5 2)。制御部 3 0 は、第 1 ポート 2 1 を含む第 1 通信部 3 1 により、スイッチ 1 5、ゲートウェイ 1 7 およびネットワーク 1 8 を介して通信管理装置 1 4 に通信接続する。

[0144] 通信管理装置 1 4 の制御部 6 1 は、NW通信部 6 0 により起動処理を実行する情報処理装置 1 3 と通信を確立する。制御部 6 1 は、NW通信部 6 0 により情報処理装置 1 3 との通信が確立すると、当該情報処理装置 1 3 へ認識完了を示す通知を送信する。

各情報処理装置 13 の制御部 30 は、通信管理装置 14 からの通知により当該情報処理装置が通信管理装置 14 によって認識されたことを確認する（S53）。制御部 30 は、当該情報処理装置 13 が通信管理装置 14 によって認識されたことを確認すると、当該情報処理装置 13 に適用される通信設定情報を通信管理装置 14 からダウンロードする（S54）。

[0145] 各情報処理装置 13 の制御部 30 は、通信管理装置 14 から通信設定情報を取得すると、取得した通信設定情報に基づく通信設定を実行する（S55）。例えば、制御部 30 は、通信設定情報が示す通信不可とする IoT デバイス（IoT デバイスに接続される情報処理装置）との通信を不可にする設定を実行する。制御部 30 は、通信設定情報に基づく他のデバイスとの通信可否を含む設定が完了すると、セキュリティモードがオンとなったことを通信管理装置 14 へ通知する。

[0146] 通信管理装置 14 の制御部 61 は、管理対象とする各情報処理装置 13 に通信設定情報を送信し、各情報処理装置 13 による通信設定の完了（セキュリティモードのオン）となった旨の通知を受信する。通信管理装置 14 の制御部 61 は、一括した通信設定の管理対象とする全ての情報処理装置 13 から通知設定の完了（セキュリティモードのオン）の通知を受信すると、一括した通信設定の管理対象となる各情報処理装置 13 へ全ての情報処理装置 13 のセキュリティモードがオンとなったことを認識した旨の通知を送信する。

[0147] 各情報処理装置 13 の制御部 30 は、通信管理装置 14 からの通知によって自装置を含む一括した通信設定の管理対象となる全ての情報処理装置 13 のセキュリティモードがオンとなったことを通信管理装置 14 が認識したことを確認する（S56）。各情報処理装置 13 の制御部 30 は、全ての情報処理装置 13 のセキュリティモードがオンとなったことを通信管理装置 14 が認識したことを確認すると、IoT デバイス 11 側の通信（LAN）ポートである第 2 ポート 22 をリンクアップする（S57）。

[0148] 以上のような第 3 の通信設定処理によれば、情報処理装置は、起動時に通

信管理装置から通信設定情報を取得し、通信管理装置から取得した通信設定情報に従って通信を不可するデバイスを設定し、さらに自身を含む管理対象となる全ての情報処理装置における通信設定が完了した後にデバイス側のポートをリンクアップする。

[0149] これにより、管理対象となる各情報処理装置は、起動時であっても通信不可に設定されている通信先と通信可能となるタイミングが発生することなく通信可否などの通信設定を遵守した運用が可能となる。また、管理対象となる複数の情報処理装置が全て通信設定を完了した後に管理対象となる各情報処理装置がデバイス側のポートをリンクアップするため、管理対象とする複数の情報処理装置の全体でセキュリティを遵守することができ、セキュリティ性を向上できる。

[0150] 次に、実施形態に係る通信システム 1 におけるデバイス側の情報処理装置 13 による第 4 の通信設定処理について説明する。

図 10 は、実施形態に係る通信システム 1 におけるデバイス側の情報処理装置 13 による第 4 の通信設定処理を説明するためのフローチャートである。

第 4 の通信設定処理は、第 3 の通信設定処理の説明と同様に複数の情報処理装置 13 が一括した通信設定の管理対象となるものとする。ただし、第 4 の通信設定処理では、通信設定情報は、各情報処理装置 13 の記憶部 54 に記憶されているものとする。

[0151] 以下の図 10 の説明として、図 1 に示す構成例においてスイッチ 15 に接続されるデバイス側の複数の情報処理装置 13 A、13 B、13 C が一括した通信設定の管理対象となり、各情報処理装置 13 A、13 B、13 C が自装置に適用（設定）する通信設定情報を保持しているものとする。

[0152] 管理対象となる各情報処理装置 13（13 A、13 B、13 C）の制御部 30 は、それぞれ電源の投入に応じて起動処理を開始する（ステップ S 61）。制御部 30 は、起動処理を開始すると、通信管理装置 14 側の通信（LAN）ポートである第 1 ポート 21 をリンクアップする（S 62）。制御部

30は、第1ポート21を含む第1通信部31により、スイッチ15、ゲートウェイ17およびネットワーク18を介して通信管理装置14に通信接続する。

[0153] 通信管理装置14の制御部61は、NW通信部60により起動処理を実行する情報処理装置13と通信を確立する。制御部61は、NW通信部60により情報処理装置13との通信が確立すると、当該情報処理装置13へ認識完了を示す通知を送信する。

各情報処理装置13の制御部30は、通信管理装置14からの通知により当該情報処理装置が通信管理装置14によって認識されたことを確認する(S63)。制御部30は、当該情報処理装置13が通信管理装置14によって認識されたことを確認すると、記憶部54に記憶している通信設定情報を読み出す(S64)。

[0154] 各情報処理装置13の制御部30は、記憶部54から通信設定情報を読み出すと、読み出した通信設定情報に基づく通信設定を実行する(S65)。例えば、制御部30は、通信設定情報が示す通信不可とするIoTデバイス(IoTデバイスに接続される情報処理装置)との通信を不可にする設定を実行する。制御部30は、通信設定情報に基づく他のデバイスとの通信可否を含む設定が完了すると、セキュリティモードがオンとなったことを通信管理装置14へ通知する。

[0155] 通信管理装置14の制御部61は、管理対象とする各情報処理装置13に通信設定情報を送信し、各情報処理装置13から通信設定が完了した(セキュリティモードがオンとなった)旨の通知を受信する。通信管理装置14の制御部61は、一括した通信設定の管理対象となる全ての情報処理装置13からセキュリティモードのオンの通知を受信すると、各情報処理装置13へ全ての情報処理装置13のセキュリティモードがオンとなったことを認識した旨の通知を送信する。

[0156] 各情報処理装置13の制御部30は、通信管理装置14からの通知によって自装置を含む一括した通信設定の管理対象となる全ての情報処理装置13

のセキュリティモードがオンとなったことを通信管理装置 14 が認識したことを確認する (S 66)。各情報処理装置 13 の制御部 30 は、全ての情報処理装置 13 のセキュリティモードがオンとなったことを通信管理装置 14 が認識したことを確認すると、IoT デバイス 11 側の通信 (LAN) ポートである第 2 ポート 22 をリンクアップする (S 67)。

[0157] 以上のような第 4 の通信設定処理によれば、情報処理装置は、起動時に記憶部に記憶した通信設定情報に従って通信を不可するデバイスを設定し、さらに自身を含む管理対象となる全ての情報処理装置における通信設定が完了した後にデバイス側の通信ポートをリンクアップする。

[0158] これにより、情報処理装置は、起動時であっても通信不可に設定されている通信先と通信可能となるタイミングが発生することなく通信可否などの通信設定を遵守した運用が可能となる。また、管理対象となる複数の情報処理装置が全て通信設定を完了した後に管理対象となる各情報処理装置がデバイス側のポートをリンクアップするため、管理対象とする複数の情報処理装置の全体でセキュリティを遵守することができ、セキュリティ性を向上できる。

[0159] 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] 端末装置と前記端末装置とネットワークを介して通信するサーバ装置との間に接続される情報処理装置において、
- 前記サーバ装置にネットワークを介して接続する第1通信部と、
- 前記端末装置に接続する第2通信部と、
- 前記第1通信部により通信管理装置にリンクアップし、前記端末装置と他の端末装置との通信可否を示す通信設定情報に基づく通信設定が完了した後に前記第2通信部により前記端末装置にリンクアップする制御部と、を有する、
- 情報処理装置。
- [請求項2] 前記制御部は、前記第1通信部によりリンクアップした前記通信管理装置から当該情報処理装置に適用する通信設定情報を取得し、前記通信管理装置から取得する通信設定情報に基づいて通信設定を実行する、
- 請求項1に記載の情報処理装置。
- [請求項3] さらに、当該情報処理装置に適用する通信設定情報を記憶する記憶部を有し、
- 前記制御部は、前記記憶部に記憶した通信管理装置に基づいて通信設定を実行する、
- 請求項1に記載の情報処理装置。
- [請求項4] 前記制御部は、管理対象とする複数の端末装置に接続される全ての情報処理装置における通信設定が完了した後に前記第2通信部により前記端末装置にリンクアップする、
- 請求項1乃至3の何れか1項に記載の情報処理装置。
- [請求項5] 前記制御部は、前記通信管理装置から管理対象とする複数の端末装置に接続される全ての情報処理装置における通信設定が完了したことを示す通知を受けた後に前記第2通信部により前記端末装置にリンクアップする、

請求項 4 に記載の情報処理装置。

[請求項6] 複数の情報処理装置と通信管理装置とを含む通信システムにおいて、

、

前記各情報処理装置は、

サーバ装置にネットワークを介して接続する第 1 通信部と、

前記サーバ装置への情報を出力する端末装置に接続する第 2 通信部と、

、

前記第 1 通信部により前記通信管理装置にリンクアップし、前記端末装置と他の端末装置との通信可否を示す通信設定情報に基づく通信設定を完了した後に前記第 2 通信部により前記端末装置にリンクアップする第 1 の制御部と、を有する、

前記通信管理装置は、

前記ネットワークを介して各情報処理装置と通信する NW 通信部と

、

前記 NW 通信部により通信する各情報処理装置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第 2 の制御部と、を有する、

通信システム。

[請求項7] 前記通信管理装置は、さらに、前記各情報処理装置に適用する通信設定情報を記憶する記憶部を有し、

前記通信管理装置の前記第 2 の制御部は、前記 NW 通信部による通信が確立した情報処理装置に適用する通信設定情報を読み出して当該情報処理装置へ送信し、

前記各情報処理装置の前記第 1 の制御部は、前記第 1 通信部によりリンクアップした前記通信管理装置から通信設定情報を取得し、前記通信管理装置から取得する通信設定情報に基づく通信設定を実行する

、

請求項 6 に記載の通信システム。

[請求項8] 前記各情報処理装置は、さらに、自装置に適用する通信設定情報を

記憶する記憶部を有し、

前記各情報処理装置の前記第 1 の制御部は、前記記憶部が記憶する通信設定情報に基づく通信設定を実行する、

請求項 6 に記載の通信システム。

[請求項 9]

前記通信管理装置の前記第 2 の制御部は、管理対象とする複数の端末装置に接続される全ての情報処理装置における通信設定が完了したことを認識した場合に前記管理対象とする各情報処理装置へ通信設定の完了通知を送信し、

前記各情報処理装置の前記第 1 の制御部は、前記管理対象とする複数の端末装置に接続される全ての情報処理装置における通信設定が完了したことを示す通信設定の完了通知を前記通信管理装置から受信した後に前記第 2 通信部により前記端末装置にリンクアップさせる、

請求項 6 乃至 8 の何れか 1 項に記載の通信システム。