

明 細 書

発明の名称：通信制御装置および通信制御システム

技術分野

[0001] 本発明の実施形態は、通信制御装置および通信制御システムに関する。

背景技術

[0002] 監視カメラ等の社会インフラシステムにおいては、取り扱われるデータや機器の制御がマルウェア等の攻撃から防御される必要がある。しかしながら、社会インフラシステムを構成する機器類は頻繁に置換えることが難しい。このため、安全対策が不十分になってしまうという問題があった。

先行技術文献

特許文献

[0003] 特許文献1：特開2009-117887号公報

発明の概要

発明が解決しようとする課題

[0004] 本発明が解決しようとする課題は、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通信制御装置および通信制御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

[0005] 実施形態の通信制御装置は、通信部と、通報部とを持つ。通信部は、第1装置および第2装置と通信し、且つ、前記第1装置または前記第2装置の少なくとも一方とは無線で通信し、前記第1装置により取得されたデータを前記第2装置に送信する。通報部は、前記第1装置との通信状態が所定の状態あるいは自装置の挙動が所定の挙動である場合に、前記第2装置に向けて、前記通信部に所定情報を送信させる。

図面の簡単な説明

[0006] [図1]実施形態の通信制御システム1の構成例を示す図。

[図2]実施形態のクライアント装置10とサーバ装置20の機能構成例を示すブロック図。

[図3]実施形態のクライアント側通信制御装置30とサーバ側通信制御装置31の機能構成例を示すブロック図。

[図4]実施形態のICカード40のハードウェア構成の一例を示す図。

[図5]実施形態のICカード40の機能構成例を示すブロック図。

[図6]実施形態の通信制御管理装置50の機能構成の一例を示すブロック図。

[図7]実施形態の通信制御システム1が行う処理の一例を示すシーケンスチャート。

[図8]実施形態のクライアント側通信制御装置30による検知処理の一例を示すフローチャート。

[図9]第2実施形態の通信制御システム1Aの構成例を示す図。

[図10]第3実施形態の通信制御システム1Bの構成例を示す図。

発明を実施するための形態

[0007] 以下、実施形態の通信制御装置および通信制御システムを、図面を参照して説明する。

[0008] (第1実施形態)

図1は、実施形態の通信制御システム1の構成例を示す図である。通信制御システム1は、クライアント装置10(10-1~10-N)と、サーバ装置20と、クライアント側通信制御装置30(30-1~30-N)と、サーバ側通信制御装置31と、通信制御管理装置50と、を備える。

[0009] クライアント装置10とクライアント側通信制御装置30とは、近距離無線通信あるいは超近距離無線通信で通信する。近距離無線通信には、例えばWi-Fi網、Bluetooth(登録商標)などが含まれる。超近距離無線通信には、例えばTransferJet(登録商標)などが含まれる。超近距離無線通信を用いることにより、電波の干渉も起こりにくくなり、盗聴が困難になる。

[0010] クライアント側通信制御装置30とサーバ側通信制御装置31とは、近距

離無線通信で、ネットワークNWを介して通信する。サーバ側通信制御装置31とサーバ装置20とは、有線で通信する。

[0011] つまり、クライアント装置10は、クライアント側通信制御装置30を介してネットワークNWと接続する。サーバ装置20は、サーバ側通信制御装置31を介してネットワークNWと接続する。なお、クライアント装置10およびサーバ装置20の構成の詳細については後述する。

[0012] クライアント側通信制御装置30は、クライアント装置10とネットワークNWとの間に接続され、クライアント装置10とサーバ装置20との間の通信を仲介する。つまり、クライアント側通信制御装置30は、クライアント装置10の無線アクセスポイントとして機能する。クライアント側通信制御装置30は、クライアント装置10により取得されたデータをクライアント装置10から受信し、受信したデータをサーバ装置20に対して送信する。ここで、クライアント側通信制御装置30は、サーバ装置20に対してデータを送信する際に、クライアント装置10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20に対して送信する。

[0013] また、クライアント側通信制御装置30は、サーバ装置20からクライアント装置10に対して送信されるデータをサーバ側通信制御装置31から受信し、受信したデータをクライアント装置10に対して送信する。ここで、クライアント側通信制御装置30が受信するデータは、例えばサーバ側通信制御装置31により暗号化されたデータである。クライアント側通信制御装置30は、クライアント装置10にデータを送信する際に、サーバ側通信制御装置31を介してサーバ装置20から受信したデータを復号し、復号したデータをクライアント装置10に送信する。

[0014] サーバ側通信制御装置31は、サーバ装置20とネットワークNWとの間に接続され、クライアント装置10とサーバ装置20との間の通信を仲介する。サーバ側通信制御装置31は、サーバ装置20からクライアント装置10に対して送信されるデータをサーバ装置20から受信し、受信したデータをクライアント装置10に対して送信する。ここで、サーバ側通信制御装置

31は、クライアント装置10に対してデータを送信する際に、サーバ装置20から取得したデータを暗号化し、暗号化したデータをクライアント装置10に対して送信する。

[0015] また、サーバ側通信制御装置31は、クライアント装置10からサーバ装置20に対して送信されるデータをクライアント側通信制御装置30から受信し、受信したデータをサーバ装置20に対して送信する。ここで、サーバ側通信制御装置31が受信するデータは、例えばクライアント側通信制御装置30により暗号化されたデータである。サーバ側通信制御装置31は、サーバ装置20にデータを送信する際に、クライアント側通信制御装置30を介してクライアント装置10から受信したデータを復号し、復号したデータをサーバ装置20に送信する。

[0016] 本実施形態において、クライアント側通信制御装置30およびサーバ側通信制御装置31が行うデータの暗号化には、例えば、SSL (Secure Socket Layer) / TLS (Transport Layer Security) のプロトコルによる暗号化が行われる。クライアント側通信制御装置30およびサーバ側通信制御装置31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。

[0017] なお、クライアント側通信制御装置30およびサーバ側通信制御装置31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。クライアント側通信制御装置30およびサーバ側通信制御装置31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、クライアント側通信制御装置30およびサーバ側通信制御装置31は、FTP (File Transfer Protocol) をFTPS (FTP Secure) に置き換えてもよい。

[0018] 本実施形態においては、クライアント側通信制御装置30またはサーバ側通信制御装置31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、本実施形態においては、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」または「データを抜き取る行為」をいう。

[0019] 通信制御管理装置50は、クライアント側通信制御装置30に対し、クライアント証明書、および秘密鍵を発行する。例えば、通信制御管理装置50は、クライアント証明書、および秘密鍵を記憶させたICカードを発行する。また、通信制御管理装置50は、ICカードが装着されたクライアント側通信制御装置30に対し、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。

[0020] また、通信制御管理装置50は、サーバ側通信制御装置31に対し、サーバ証明書、および秘密鍵を発行する。例えば、通信制御管理装置50は、サーバ証明書、および秘密鍵を記憶させたICカードを発行する。また、通信制御管理装置50は、ICカードが装着されたサーバ側通信制御装置31に対し、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、クライアント側通信制御装置30とサーバ側通信制御装置31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。

[0021] また、通信制御管理装置50は、正当なクライアント装置10とクライアント側通信制御装置30とのペアを登録する。例えば、通信制御管理装置50は、クライアント装置10のアドレス情報と、クライアント側通信制御装置30のアドレス情報とを取得し、両アドレス情報を対応付けたホワイトリストを作成し、自装置の記憶部に格納する。アドレス情報には、例えば、IPアドレスやMACアドレスなどが含まれる。通信制御管理装置50は、作成したホワイトリストに基づいて、クライアント側通信制御装置30に対し

、ホワイトリストに登録されているアドレス情報のクライアント装置１０と接続するよう指示する。

[0022] 通信制御管理装置５０は、自装置の操作部を用いて管理者が入力することによりアドレス情報を取得してもよく、クライアント側通信制御装置３０からアドレス情報を取得してもよい。後者の場合、クライアント側通信制御装置３０は、初期設定の際に、クライアント装置１０と近距離無線通信を確立した時に取得したクライアント装置１０のアドレス情報と、自身のアドレス情報とを、ネットワークNWを介して通信制御管理装置５０に送信してもよい。

[0023] ここで、通信制御システム１の設置される環境の一例について説明する。クライアント装置１０とサーバ装置２０とは、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、例えば、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、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。以下においては、クライアント装置１０とサーバ装置２０とは、道路や公共設備などを監視する監視システムのコンポーネントである場合を例に説明する。この場合、クライアント装置１０は、道路の状況等が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）である。サーバ装置２０は、クライアント装置１０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。

[0024] なお、クライアント装置１０とサーバ装置２０とは、監視システムのコンポーネントに限定されることはない。例えば、クライアント装置１０とサーバ装置とは、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よいし、物流センタにおける配送状況を取得するシステム、あるい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よい。

- [0025] 次に、クライアント装置１０およびサーバ装置２０の構成について説明する。図２は、実施形態のクライアント装置１０とサーバ装置２０の機能構成例を示すブロック図である。
- [0026] クライアント装置１０は、通信部１１と、クライアント制御部１２と、撮像部１３とを備える。通信部１１は、例えば、クライアント側通信制御部３０と無線通信を確立する。
- なお、通信部１１は、従来のシステムであれば、ネットワークNWに接続され、ネットワークNWを介して、サーバ装置２０と通信を行う機能部に相当する。
- [0027] クライアント制御部１２は、例えば、CPU (Central Processing Unit) などを含むプロセッサであり、クライアント装置１０を統括的に制御する。クライアント制御部１２は、例えば、通信部１１を介してサーバ装置２０からコマンドを受信した場合、サーバ装置２０からの制御に従って撮像部１３に撮像を開始または停止させたり、撮像部１３に対し撮像するカメラの方向や、撮像する際の倍率等の撮像条件を設定したりする。
- [0028] 撮像部１３は、クライアント制御部１２の指示に従い、所定箇所における風景を撮像する。撮像部１３は、撮像したデータ（撮像データ）を、クライアント制御部１２に出力する。
- [0029] サーバ装置２０は、通信部２１と、サーバ制御部２２と、撮像データ記憶部２３と、出力部２４とを備える。通信部２１は、例えば、サーバ装置２０のイーサネット（登録商標）のポートである。本実施形態では、通信部２１は、有線ケーブルを介してサーバ側通信制御装置３１に接続され、サーバ装置２０からクライアント装置１０に対して送信されるデータをサーバ側通信制御装置３１に出力する。
- [0030] サーバ制御部２２は、例えば、CPUなどを含むプロセッサであり、サーバ装置２０を統括的に制御する。サーバ制御部２２は、例えば、クライアント装置１０に対して所定のコマンドを送信する。また、サーバ制御部２２は、例えば、クライアント装置１０により撮像された撮像データを、撮像デー

タ記憶部 2 3 に記憶させる。撮像データ記憶部 2 3 は、サーバ制御部 2 2 の指示に従い、撮像データを記憶する。

[0031] ここで、従来システムの一例について説明する。従来のシステムにおいて、クライアント装置とサーバ装置とが、互いの通信部およびネットワークを介して直接的に接続される場合、クライアント装置とサーバ装置との間の通信には、ネットワーク監視カメラにおける一般的な通信プロトコルである H T T P が用いられる。この場合、クライアント装置また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、容易に撮像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。

[0032] このような不正な攻撃に対する対策として、クライアント装置が、撮像データを暗号化させてネットワーク NW に出力させることが考えられる。しかしながら、そもそも監視カメラが備える C P U 等のプロセッサは、撮像データの圧縮や符号化の用途に用いられるために用いられる用途で用いられることが一般的であるため、さらに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。このような場合、クライアント装置が元々有する C P U では、撮像データを暗号化させることができない。クライアント装置に撮像データを暗号化させる場合には、撮像データを暗号化するためのプロセッサを、更にクライアント装置に搭載させる等、クライアント装置のハードウェア構成の変更や置換えが必要となることが考えられる。しかしながら、クライアント装置は、監視カメラ等の社会インフラを構成するコンポーネントであるため、ハードウェア構成を変更したり置換えたりすることが容易にはできない。このような事情を鑑みると、クライアント装置に変更を加えることなく、撮像データが暗号化されてネットワークに出力されることが望ましい。

[0033] 本実施形態において、クライアント装置 1 0 とネットワーク NW との間に接続されたクライアント側通信制御装置 3 0 が、クライアント装置 1 0 が送

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、サーバ装置20とネットワークNWとの間に接続されたサーバ側通信制御装置31が、サーバ装置20が送信する制御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、クライアント装置10、およびサーバ装置20を変更することなく、ネットワークNWを流れる撮像データの安全性を向上させる。

[0034] 次に、クライアント側通信制御装置30およびサーバ側通信制御装置31の構成について説明する。図3は、実施形態のクライアント側通信制御装置30の機能構成例を示すブロック図である。サーバ側通信制御装置31は、クライアント側通信制御装置30と同じ機能構成を有する。このため、以下では、クライアント側通信制御装置30の構成について説明し、サーバ側通信制御装置31の構成については説明を省略する。また、クライアント側通信制御装置30とサーバ側通信制御装置31とを区別しない場合には、単に、通信制御装置30（31）などと称する。

[0035] 図3に示すように、通信制御装置30は、NW（ネットワーク）通信部32と、制御部33と、装置通信部34と、リーダライタ35と、ICカード40とを備える。ここで、ICカード40は、「認証部」の一例である。

[0036] 通信部32は、ネットワークNWに接続され、ネットワークNWを介して、サーバ側通信制御装置31と通信を行う。

[0037] 制御部33は、例えば、CPUなどを含むプロセッサであり、クライアント側通信制御装置30を統括的に制御する。制御部33は、例えば、仲介処理部33Aと、検知部33Bと、通報部33Cと、機能制限部33Dと、設定部33Eと、通信制限部33Fとを備える。これらの機能部のうち一部または全部は、例えば、CPUなどのプロセッサが、記憶部に記憶されたプログラム（ソフトウェア）を実行することで実現される。また、これらの構成要素の機能のうち一部または全部は、LSI（Large Scale Integration）やASIC（Application Specific Integrated Circuit）、FPGA（Field-Programmable Gate Array）等のハードウェア（回路部：circuitryを含む）によって実現されていてもよいし、ソフトウェアとハードウェアの協働によ

って実現されていてもよい。

[0038] 仲介処理部33Aは、クライアント装置10とサーバ装置20との間の通信を仲介する。例えば、仲介処理部33Aは、装置通信部34を介してクライアント装置30から受信した情報に基づいて、リーダライタ35を介してICカード40にコマンドを送信する。

仲介処理部33Aは、ICカード40からレスポンスを受信し、ICカード40から受信したレスポンスに基づく情報を、NW通信部32を介してサーバ装置20に送信する。また、仲介処理部33Aは、NW通信部32を介してサーバ側通信制御装置31から受信した情報に基づいて、リーダライタ35を介してICカード40にコマンドを送信する。仲介処理部33Aは、ICカード40からレスポンスを受信し、ICカード40から受信したレスポンスに基づく情報を、装置通信部34を介してクライアント装置10に送信する。

[0039] 検知部33Bは、クライアント装置10との通信状態が所定の状態である場合、あるいは自装置の挙動が所定の挙動である場合に、クライアント装置10とサーバ装置20との間の通信を仲介する仲介環境に異変が発生したことを検知する。

[0040] 例えば、検知部33Bは、装置通信部34による通信状態に基づいてクライアント装置10との通信状態の変化が認識された場合、クライアント装置10との通信状態が所定の状態であるとして、異変が発生したことを検知する。クライアント装置10との通信状態が所定の状態である場合には、例えば、クライアント装置10との通信が切断された場合、クライアント装置10との通信における電波強度が閾値以下である場合、クライアント装置10との通信が断続的に切断される回数が閾値以上である場合、クライアント装置10との通信が連続的に切断されている時間が閾値以上である場合、クライアント装置10との通信状態が悪い（例えば、通信レベルが閾値以下）場合などが含まれる。

[0041] クライアント装置10との通信状態が所定の状態である場合、検知部33

Bは、クライアント装置10に対して何らかの不正行為が行われていることや、自装置とクライアント装置10との相対的な位置関係に変化が発生したことを検知できる。前者の場合、例えば、クライアント装置10とサーバ装置20との通信を不正の目的で仲介する装置に取って代わられた状況などが考えられる。後者の場合、例えば、超近距離無線通信で通信している状況において、クライアント装置10とサーバ装置20との相対的な位置関係が変化することにより、通信が切断される状況であることが考えられる。

[0042] また、検知部33Bは、挙動センサ37からの出力に基づいて自装置の挙動の変化が認識された場合、自装置の挙動が所定の挙動であるとして、異変が発生したことを検知する。自装置の挙動が所定の状態にある場合には、例えば、自装置の位置が変化した場合、自装置の加速度が変化した場合、自装置が振動した場合などが含まれる。また、自装置の挙動が所定の状態にある場合には、自装置の位置や加速度の変化量、自装置の振動量、変化した頻度などが閾値を超えた場合であってもよい。

[0043] こうすることにより、検知部33Bは、不正行為自体を検知でき、また、不正行為の前段階における異変も検知することができる。例えば、クライアント装置10との間に遮蔽板が置かれた場合、クライアント装置10との通信状態が切断されるため、検知部33Bは、その後に不正行為が行われるかもしれない状況であることを検知することができる。

また、クライアント側通信制御装置30よりも強い電波強度でクライアント装置10と通信しようとする不正装置がある場合、クライアント装置10との通信状態が悪くなるため、検知部33Bは、その後に不正行為が行われるかもしれない状況であることを検知することができる。

[0044] 通報部33Cは、検知部33Bにより異常の発生が検知された場合、検知結果をサーバ装置20に通報する。例えば、通報部33Cは、NW通信部32に指示して、サーバ装置20に向けて所定情報を送信させる。所定情報には、異常の発生を通知する情報、異常の種類を通報する情報、異常の発生時刻や発生地点を示す情報などが含まれる。また、通報部33Cは、出力部3

8に指示して、異常の発生を通知する警報音や光を点滅させてもよい。これに限られず、通報部33Cは、検知部33Bにより異常の発生が検知された場合、検知結果を通信制御管理装置50に通報してもよい。

[0045] 機能制限部33Dは、検知部33Bにより異常の発生が検知された場合、クライアント装置10の機能を停止または制限させる。例えば、機能制限部33Dは、クライアント装置10の電源をOFFにするように指示するコマンドや、クライアント装置10から送信されるデータに不正取得であることを示す画像を重畳させるよう指示するコマンドなどをクライアント装置10に送信する。また、機能制限部33Dは、クライアント装置10から受信したデータをサーバ装置20に転送しないようにしてもよいし、サーバ装置20にデータを転送する頻度や回数を通常よりも減らしてもよい。

[0046] 設定部33Eは、通信が許可されたクライアント装置10のアドレス情報を設定する。

例えば、設定部33Eは、通信制御管理装置50の指示に従って、ホワイトリストに登録されているクライアント装置10のアドレス情報を、記憶部39に登録する。これに限られず、設定部33Eは、NW通信部32あるいは装置通信部34を用いて接続された他の端末の指示に従って、他の端末から受信した情報に基づいて、通信が許可されたクライアント装置10のアドレス情報を記憶部39に登録してもよい。

[0047] 通信制限部33Fは、記憶部39を参照し、例えばホワイトリストに登録されているクライアント装置10との通信を許可し、ホワイトリストに登録されていないクライアント装置10との通信を制限する。例えば、通信制限部33Fは、記憶部39において登録されているアドレス情報のクライアント装置10から受信したリクエストに基づいて、サーバ装置20に対する相互認証によるハンドシェイクを実行するが、記憶部39に登録されていない装置からリクエストを受信した場合には、サーバ装置20に対する相互認証によるハンドシェイクを実行しない。

[0048] また、通信制限部33Fは、記憶部39において登録されているアドレス

情報のクライアント装置 10 から受信したデータは、サーバ装置 20 に送信するが、記憶部 39 に登録されていない装置から受信したデータはサーバ装置 20 に送信せずに破棄する。こうすることにより、クライアント側通信制御装置 30 を、特定のアドレスの機器でしか作動しないようにすることができる。よって、セキュアな通信を確立することが期待できる。

[0049] 装置通信部 34 は、装置（クライアント装置 10、またはサーバ装置 20）に接続され、装置と通信を行う。具体的には、クライアント側通信制御装置 30 の装置通信部 34 は、クライアント装置 10 に接続され、クライアント装置 10 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クライアント装置 10 に出力する。また、サーバ側通信制御装置 31 の装置通信部 34 は、サーバ装置 20 に接続され、サーバ装置 20 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 20 に出力する。

[0050] リーダライタ 35 は、ＩＣカード 40 のコンタクト部 36 を介して、ＩＣカード 40 の間の通信を行う。

[0051] 挙動センサ 37 は、自装置の挙動の変化を検出する。挙動センサ 37 は、例えば、加速度センサ、ＧＮＳＳセンサ、振動検知センサなどを含む。加速度センサを用いることで、挙動センサ 37 は、加速度の変化を検知する。ＧＮＳＳセンサを用いることで、挙動センサ 37 は、自装置の設置位置の変化を検知する。振動検知センサを用いることで、挙動センサ 37 は、自装置に何かが接触したことなどを検知する。

[0052] 出力部 38 は、例えば、スピーカ、発光ダイオード、ディスプレイなどを含む。

[0053] 記憶部 39 は、例えば、ＲＡＭ、ＲＯＭなどによって実現される。記憶部 39 は、プロセッサが実行するプログラムを格納する他、設定部 33 E により設定されたクライアント装置 10 のアドレス情報を格納する。

[0054] ＩＣカード 40 は、例えば、プラスチックのカード基材に、ＩＣモジュール 41 を実装して形成されている。すなわち、ＩＣカード 40 は、ＩＣモジ

ジュール41と、ICモジュール41が埋め込まれたカード基材とを備える。

[0055] ICモジュール41は、コンタクト部36と、ICチップ42とを備える。コンタクト部36は、ICカード40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通信制御装置30(31)から供給を受ける端子、及び、通信制御装置30(31)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。

[0056] ICカード40は、クライアント側通信制御装置30に着脱可能に装着され、コンタクト部36を介してクライアント側通信制御装置30と通信可能である。例えば、ICカード40は、クライアント側通信制御装置30が送信したコマンド(処理要求)を、コンタクト部36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。そして、ICカード40は、コマンド処理の実行結果であるレスポンス(処理応答)をクライアント側通信制御装置30にコンタクト部36を介して送信する。

[0057] 次に、ICカード40のハードウェア構成の一例について説明する。図4は、実施形態のICカード40のハードウェア構成の一例を示す図である。

[0058] 上述した通り、ICカード40は、コンタクト部36と、ICチップ42とを備えたICモジュール41を備えている。そして、ICチップ42は、UART(Universal Asynchronous Receiver Transmitter)43と、CPU44と、ROM(Read Only Memory)45と、RAM(Random Access Memory)46と、EEPROM(Electrically Erasable Programmable ROM)47とを備える。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。

[0059] UART43は、上述したSIO端子を介して、クライアント側通信制御装置30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

B Sを介して取得したデータをシリアル変換して、S I O端子を介してクライアント側通信制御装置3 0に出力する。U A R T 4 3は、例えば、S I O端子を介してコマンドをクライアント側通信制御装置3 0から受信する。また、U A R T 4 3は、S I O端子を介してレスポンスをクライアント側通信制御装置3 0に送信する。

[0060] C P U 4 4は、R O M 4 5又はE E P R O M 4 7に記憶されているプログラムを実行して、I Cカード4 0の各種処理を行う。C P U 4 4は、例えば、コンタクト部3 6を介して、U A R T 4 3が受信したコマンドに応じたコマンド処理を実行する。

[0061] R O M 4 5は、例えば、マスクR O Mなどの不揮発性メモリであり、I Cカード4 0の各種処理を実行するためのプログラム、及びコマンドテーブルなどのデータを記憶する。

R A M 4 6は、例えば、S R A M (Static RAM) などの揮発性メモリであり、I Cカード4 0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 4 7は、例えば、電氣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 4 7は、I Cカード4 0が利用する各種データを記憶する。E E P R O M 4 7は、例えば、I Cカード4 0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。

[0062] 次に、I Cカード4 0の構成の一例について説明する。図5は、実施形態のI Cカード4 0の機能構成例を示すブロック図である。I Cカード4 0は、通信部4 0 Aと、制御部4 0 Bと、記憶部4 0 Cとを備える。ここで、図5に示されるI Cカード4 0の各部は、図4に示されるI Cカード4 0のハードウェアを用いて実現される。

[0063] 通信部4 0 Aは、例えば、U A R T 4 3と、C P U 4 4と、R O M 4 5に記憶されているプログラムとにより実現され、コンタクト部3 6を介して、例えば、クライアント側通信制御装置3 0との間でコマンド及びレスポンスの送受信を行う。すなわち、通信部4 0 Aは、所定の処理を要求するコマンド（処理要求）をクライアント側通信制御装置3 0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）をクライアント側通信制御装置 30 に送信する。通信部 40A は、UART 43 を介してクライアント側通信制御装置 30 から受信した受信データを RAM 46 に記憶させる。また、通信部 40A は、RAM 46 に記憶されている送信データを、UART 43 を介してクライアント側通信制御装置 30 に送信する。

[0064] 制御部 40B は、例えば、CPU 44 と、RAM 45 と、ROM 46 又は EEPROM 47 とにより実現され、IC カード 40 を統括的に制御する。制御部 40B は、コマンド処理部 41B と、暗号化復号部 42B とを備える。

[0065] ここで、コマンド処理部 41B が行う処理は、「認証処理」の一例である。また、暗号化復号部 42B 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 41B は、各種コマンド処理を実行する。コマンド処理部 41B は、例えば、後述する HTTP S 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、クライアント側通信制御装置 30 とサーバ側通信制御装置 31 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認証処理である。

[0067] 暗号化復号部 42B 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 42B は、通信部 40A を介してクライアント装置 10（サーバ側通信制御装置 31 の場合はサーバ装置 20）から受信したデータを暗号化する。また、暗号化復号部 42B は、通信部 40A を介してサーバ装置 20（サーバ側通信制御装置 31 の場合はクライアント装置 10）からネットワーク NW を介して受信した暗号化されたデータを復号する。

[0068] 記憶部 40C は、例えば、EEPROM 47 により構成された記憶部であり、証明書情報記憶部 41C と、秘密情報記憶部 42C とを備える。証明書

情報記憶部 4 1 C は、通信制御管理装置 5 0 が発行したクライアント装置 1 0（サーバ側通信制御装置 3 1 の場合はサーバ装置 2 0）に対する証明書を記憶する。具体的には、クライアント側通信制御装置 3 0 に装着される IC カード 4 0 の証明書情報記憶部 4 1 C には、クライアント証明書を示す情報が記憶される。また、サーバ側通信制御装置 3 1 に装着される IC カード 4 0 の証明書情報記憶部 4 1 C 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 4 2 C は、通信制御管理装置 5 0 が発行したクライアント装置 1 0（サーバ側通信制御装置 3 1 の場合はサーバ装置 2 0）に対する秘密鍵を記憶する。具体的には、クライアント側通信制御装置 3 0 に装着される IC カード 4 0 の秘密情報記憶部 4 2 C には、クライアント側通信制御装置 3 0 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、サーバ側通信制御装置 3 1 に装着される IC カード 4 0 の証明書情報記憶部 4 1 C には、サーバ側通信制御装置 3 1 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、通信制御管理装置 5 0 の構成の一例について説明する。図 6 は、実施形態の通信制御管理装置 5 0 の機能構成の一例を示すブロック図である。通信制御管理装置 5 0 は、例えば、NW（ネットワーク）通信部 5 0 A と、制御部 5 0 B と、記憶部 5 0 C とを備える。

[0071] NW 通信部 5 0 A は、ネットワーク NW に接続され、ネットワーク NW を介して、通信制御装置 3 0（3 1）と通信を行う。

[0072] 制御部 5 0 B は、例えば、CPU などを含むプロセッサであり、通信制御管理装置 5 0 を統括的に制御する。制御部 5 0 B は、主に通信制御装置 3 0（3 1）の正当性を認めるプライベート認証局として機能する。制御部 5 0 B は、鍵生成部 5 1 B と、証明書発行部 5 2 B と、証明書更新部 5 3 B と、証明書管理部 5 4 B と、管理部 5 5 B と、リスト作成部 5 6 B とを備える。

[0073] 鍵生成部 5 1 B は、例えば、通信制御装置 3 0（3 1）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。

- [0074] 証明書発行部 5 2 B は、例えば、通信制御装置 3 0 (3 1) からの認証申請に基づいて、通信制御装置 3 0 (3 1) の正当性を認める証明書の発行を行う。証明書には、公開鍵と、通信制御装置 3 0 (3 1) の所有者を示す情報が含まれる。
- [0075] 証明書更新部 5 3 B 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 5 3 B は、例えば、通信制御装置 3 0 (3 1) からの更新申請に基づいて、当該通信制御装置 3 0 (3 1) 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、発行した証明書を通信制御装置 3 0 (3 1) に対して送信する。発行した証明書を示す情報が通信制御装置 3 0 (3 1) により受信され、通信制御装置 3 0 (3 1) の I C カード 4 0 の証明書情報記憶部 4 1 C に記憶されることで、通信制御装置 3 0 (3 1) の証明書の有効期限が延長される。
- [0076] 証明書管理部 5 4 B 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 5 4 B は、例えば、通信制御装置 3 0 (3 1) に装着された I C カード 4 0 の改ざん、また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、通信制御装置 3 0 (3 1) に対して発行した証明書を無効化する処理を行う。また、証明書管理部 5 4 B は、通信制御装置 3 0 (3 1) からの問い合わせに基づいて、通信制御装置 3 0 (3 1) 、および他の通信装置に対して発行した証明書が証明書管理部 5 4 B 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 5 4 B は、定期的に、発行済みの証明書が正当な通信制御装置 3 0 (3 1) に使用されているかを確認するようにしてもよい。
- [0077] 管理部 5 5 B は、通信制御装置 3 0 (3 1) を管理する。例えば、管理部 5 5 B は、通信制御装置 3 0 (3 1) 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。
- [0078] リスト作成部 5 6 B は、クライアント装置 1 0 のアドレス情報と、クライアント側通信制御装置 3 0 のアドレス情報とを取得し、両アドレス情報を対応付けたホワイトリストを作成し、リスト記憶部 5 3 C に格納する。また、

リスト作成部 56B は、サーバ装置 20 のアドレス情報と、サーバ側通信制御装置 31 のアドレス情報とを取得し、両アドレス情報を対応付けたホワイトリストを作成し、リスト記憶部 53C に格納してもよい。

[0079] 記憶部 50C は、例えば鍵情報記憶部 51C と、証明書情報記憶部 52C と、リスト記憶部 53C とを備える。鍵情報記憶部 51C 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 52C 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 51C と、証明書情報記憶部 52C とは、例えば、鍵生成部 51B が秘密鍵を発行する際、証明書発行部 52B 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 51C には、鍵生成部 51B 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 52C には、証明書発行部 52B が発行した証明書を示す情報が記憶される。リスト記憶部 53C には、リスト作成部 56B により作成されるホワイトリストが記憶される。

[0080] 次に、通信制御システム 1 が行う処理の一例について説明する。図 7 は、実施形態の通信制御システム 1 が行う処理の一例を示すシーケンスチャートである。

[0081] クライアント装置 10 は、撮像データをサーバ装置 20 に送信する場合、まずサーバ装置 20 に対する HTTP リクエストを送信する（ステップ S1）。クライアント装置 10 が送信した HTTP リクエストは、クライアント側通信制御装置 30 により取得される（ステップ S2）。

[0082] クライアント側通信制御装置 30 は、クライアント装置 10 により送信された HTTP リクエストを取得すると、HTTP とともに受信したアドレス情報に基づいて、事前にホワイトリストに登録されているクライアント装置 10 であるか否かを判定する（ステップ S3）。受信したアドレス情報がホワイトリストに登録されている場合、サーバ側通信制御装置 31 に対して、HTTPS のリクエスト (ClientHello) を送信する（ステップ S4）。これにより、クライアント側通信制御装置 30 とサーバ側通信制御装置 31 との間のハンドシェイクが開始される（ステップ S5）。

- [0083] 具体的には、クライアント側通信制御装置30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。サーバ側通信制御装置31は、ClientHelloに対する応答として、クライアント側通信制御装置30に対しHTTPSのレスポンス (ServerHello) を送信する。サーバ側通信制御装置31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20が選択した情報が含まれる。換言すると、クライアント側通信制御装置30からの提示に対し、サーバ側通信制御装置31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。
- [0084] そして、サーバ側通信制御装置31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20に対して発行された公開鍵とその証明書を示す情報、およびクライアント装置10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。クライアント側通信制御装置30は、サーバ側通信制御装置31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、及び暗号化通信に用いる共通鍵に必要な情報を送る。
- [0085] クライアント側通信制御装置30とサーバ側通信制御装置31との間の相互認証は、例えば次のように行われる。クライアント側通信制御装置30は、今までに受信したServerHello等から署名を生成し、サーバ側通信制御装置31に送信する。サーバ側通信制御装置31は、クライアント側通信制御装置30から受信した署名を、クライアント側通信制御装置30から受信した証明書に基づいて検証する。サーバ側通信制御装置31は、検証が成功すると、その証明書が間違いなくクライアント側通信制御装置30のものであると判定する。また、サーバ側通信制御装置31は、今までに受信したClientHello等から署名を生成し、クライアント側通信制御装置30に送信する。クライアント側通信制御装置30は、サーバ側通信制御装置31から受信した署名を、サーバ側通信制御装置31から受信した証明書に基づいて検証する。クライアント側通信制御装置30は、検証が成功すると、その証明書が間

違いなくサーバ側通信制御装置 31 のものであると判定する。

[0086] クライアント側通信制御装置 30 とサーバ側通信制御装置 31 との間の相互認証が正しく行われると、クライアント側通信制御装置 30 とサーバ側通信制御装置 31 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。

[0087] サーバ側通信制御装置 31 から送付されたサーバ装置 20 に対して発行された公開鍵とその証明書が、クライアント側通信制御装置 30 に許容される証明書であれば、サーバ側通信制御装置 31 は、クライアント側通信制御装置 30 から送付された公開鍵とその証明書が、サーバ側通信制御装置 31 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。

[0088] サーバ側通信制御装置 31 は、クライアント側通信制御装置 30 とのハンドシェイクが確立されると、サーバ装置 20 に対し、HTTP リクエストを送信する（ステップ S6）。ここで送信される HTTP リクエストは、ステップ S2 においてクライアント装置 10 から受信した HTTP リクエストである。

[0089] サーバ側通信制御装置 31 により送信された HTTP リクエストは、サーバ装置 20 により受信される（ステップ S7）。このとき、サーバ装置 20 は、クライアント装置 10 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 20 は、クライアント装置 10 に対して HTTP レスポンスを応答する（ステップ S8）。サーバ装置 20 が送信した HTTP レスポンスは、サーバ側通信制御装置 31 により取得される（ステップ S9）。

[0090] サーバ側通信制御装置 31 は、取得したサーバ装置 20 からの HTTP レスポンスを、ステップ S5 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 S10）。サーバ側通信制御装置 31 により暗号化された HTTP レスポンスは、ネットワーク NW を介してクライアント側通信制御装置 30 に受信される（ステップ S11）。

クライアント側通信制御装置 30 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 S12）。クライアント側通信制御装置 30

により復号されたHTTPレスポンスは、クライアント装置10に取得される(ステップS13)。クライアント装置10は、復号されたHTTPレスポンスを受信する(ステップS14)。このとき、クライアント装置10は、サーバ装置20からHTTPレスポンスが応答されたと認識する。このため、クライアント装置10は、サーバ装置20に対し、撮像データを送信する(ステップS15)。

[0091] クライアント装置10が送信した撮像データは、クライアント側通信制御装置30により取得される(ステップS16)。クライアント側通信制御装置30は、撮像データとともに受信したアドレス情報に基づいて、事前にホワイトリストに登録されているクライアント装置10であるか否かを判定する(ステップS17)。受信したアドレス情報がホワイトリストに登録されている場合、クライアント側通信制御装置30は、クライアント装置10により送信された撮像データを、共通鍵を用いて暗号化する(ステップS18)。

クライアント側通信制御装置30により暗号化された撮像データは、ネットワークNWを介してサーバ側通信制御装置31に受信される(ステップS19)。

[0092] サーバ側通信制御装置31は、受信した撮像データを、共通鍵を用いて復号する(ステップS20)。サーバ側通信制御装置31により復号された撮像データは、サーバ装置20にとり取得される(ステップS21)。サーバ装置20は、復号された撮像データを受信する(ステップS22)。このとき、サーバ装置20は、クライアント装置10からの撮像データを受信したと認識する。

[0093] なお、上記フローチャートのステップS5において、クライアント側通信制御装置30とサーバ側通信制御装置31との間の相互認証が正しく行われなかった場合、クライアント側通信制御装置30は、通信先との通信を許可しない。具体的には、クライアント側通信制御装置30は、通信先から送信された情報をクライアント装置10に出力しない。相互認証が正しく行われ

なかった場合、通信先がサーバ側通信制御装置 31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、クライアント側通信制御装置 30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制御管理装置 50に送信するようにしてもよい。これにより、通信制御管理装置 50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、管理下にあるクライアント側通信制御装置 30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。

[0094] また、クライアント側通信制御装置 30は、上記フローチャートのステップ S5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クライアント装置 10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。クライアント側通信制御装置 30の制御部 33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。

[0095] また、制御部 33は、送信先リストを更新するようにしてもよい。制御部 33は、例えば、一定期間にクライアント装置 10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 33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、クライアント側通信制御装置 30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を通信制御管理装置 50に送信するようにしてもよい。この場合、例えば、通信制御管理装置 50は、クライアント側通信制御装置 30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。通信制御管理装置 50により送信先リストが更新されることで、通信制御管

理装置 50 が管理下にあるクライアント側通信制御装置 30 と通信する通信機器を一括して管理することができる。

[0096] また、クライアント側通信制御装置 30 は、ステップ S5 において行われるハンドシェイクが確立した後にクライアント装置 10 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、クライアント側通信制御装置 30 の制御部 33 は、ネットワーク NW を介してクライアント装置 10 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、通信制御管理装置 50 は、例えば、クライアント側通信制御装置 30 およびサーバ側通信制御装置 31 それぞれに検証鍵を送信するようにしてもよい。

[0097] 例えば、サーバ側通信制御装置 31 は、クライアント装置 10 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、サーバ側通信制御装置 31 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クライアント装置 10 へ送信する。また、クライアント側通信制御装置 30 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。

[0098] また、クライアント側通信制御装置 30 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。クライアント側通信制御装置 30 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、クライアント装置 10 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、クライアント側通信制御装置 30 は、復号した情報（平文）をクライアント装置 10 に出力する。一方、クライアント側通信制御装置 30 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、クライアント装置 10 に対して送信された情報は、サーバ装置 20 またはサーバ側通信制御装置 31 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、クライアント側通信制御装置 30 は、復号した情報（平

文)をクライアント装置10に出力しない。

[0099] これにより、クライアント装置10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、クライアント装置10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、クライアント装置10に代わりサーバ側通信制御装置31がクライアント装置10に対して送信された情報の内容を検証することにより、クライアント装置10の処理負担を軽減させることが可能となる。

[0100] 次に、クライアント側通信制御装置30による検知処理の一例について説明する。図8は、実施形態のクライアント側通信制御装置30による検知処理の一例を示すフローチャートである。まず、検知部33Bは、挙動センサ37からの出力を取得し(ステップS101)、自装置の挙動が所定の状態にあるか否かを判定する(ステップS102)。自装置の挙動が所定の状態である場合、検知部33Bは、異常の発生を検知し(ステップS103)、通報部33Cが、検知結果をサーバ装置20(あるいは通信制御管理装置50)に通報する(ステップS104)。

[0101] 次いで、検知部33Bにより異常の発生が検知された場合にはクライアント装置10の機能を停止または制限させることが事前に設定されている場合(ステップS105)、機能制限部33Dは、クライアント装置10の機能を停止または制限させる(ステップS106)。そして、処理を終了する。

[0102] 一方、ステップS102において、自装置の挙動が所定の状態でない場合、検知部33Bは、装置通信部34による通信状態を示す情報を取得し(ステップS107)、クライアント装置10との通信状態が所定の状態であるか否かを判定する(ステップS108)。クライアント装置10との通信状態が所定の状態である場合、ステップS103の処理に移行し、クライアント装置10との通信状態が所定の状態でない場合、処理を終了する。

[0103] (第2実施形態)

図9は、第2実施形態の通信制御システム1Aの構成例を示す図である。

通信制御システム 1 A は、クライアント側通信制御装置 3 0 がクライアント装置 1 0 と電氣的に接続されている点で、通信制御システム 1 と異なる。クライアント側通信制御装置 3 0 は、例えば、USB ドングルのような形状であって、クライアント装置 1 0 の USB ポートに接続されている。なお、クライアント側通信制御装置 3 0 が USB トングルのような形状でなく USB ポートを備える場合、USB ケーブルを介してクライアント装置 1 0 の USB ポートと接続されてもよい。これらに限られず、クライアント側通信制御装置 3 0 は、SD カードのような形状であって、クライアント装置 1 0 の SD カードのスロットに挿入されることでクライアント装置 1 0 と接続されてもよい。

[0104] このような構成とすることで、クライアント装置 1 0 に無線通信の機能が無い場合であっても、サーバ装置 2 0 との無線通信を簡単に実現することができる。

[0105] 本実施形態のクライアント側通信制御装置 3 0 は、クライアント装置 1 0 との電氣的な接続が切断された場合、その旨を示す情報（切断情報）をサーバ装置 2 0 に送信してよい。こうすることにより、サーバ装置 2 0 は、異常の発生を検知することができる。例えば、なお、クライアント側通信制御装置 3 0 がクライアント装置 1 0 からの電力により動作している場合、切断された後に切断情報をサーバ装置 2 0 に送信できない場合がある。この場合、クライアント側通信制御装置 3 0 は、クライアント装置 1 0 に対して切断情報をサーバ装置 2 0 に送信するように依頼してもよく、次に接続された時に切断情報をサーバ装置 2 0 に送信してもよい。

[0106] また、クライアント側通信制御装置 3 0 は、クライアント装置 1 0 と電氣的に接続されている状態において、その旨を示す情報（接続情報）を定期的にサーバ装置 2 0 に送信するようにしてもよい。こうすることにより、サーバ装置 2 0 は、接続情報を受信しない場合に、異常の発生を検知することができる。

[0107] （第 3 実施形態）

図 10 は、第 3 実施形態の通信制御システム 1 B の構成例を示す図である。通信制御システム 1 B は、クライアント側通信制御装置 30 が有線通信で、ゲートウェイ 70 とネットワーク NW を介してサーバ側通信制御装置 31 と通信する点で、通信制御システム 1 と異なる。このような構成とすることで、クライアント装置 10 に無線通信の機能が無い場合であっても、サーバ装置 20 との無線通信を簡単に実現することができる。

[0108] 以上説明したように、実施形態の通信制御システム 1 は、第 1 装置および第 2 装置と通信し、且つ、前記第 1 装置または前記第 2 装置の少なくとも一方とは無線で通信し、前記第 1 装置により取得されたデータを前記第 2 装置に送信する通信部（NW 通信部 32）と、前記第 1 装置との通信状態が所定の状態あるいは自装置の挙動が所定の挙動である場合に、前記第 2 装置に向けて、前記通信部に所定情報を送信させる通報部（通報部 33C）と、を備えることにより、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通信制御装置を提供することができる。

[0109] また、実施形態の通信制御システム 1 は、クライアント装置 10 とネットワーク NW との間に接続されるクライアント側通信制御装置 30 と、サーバ装置 20 とネットワーク NW との間に接続されるサーバ側通信制御装置 31 と、を備える。クライアント側通信制御装置 30 は、IC カード 40 と、制御部 33 を有する。制御部 33 は、IC カード 40 に、相互認証と暗号化復号処理とのうち少なくとも一方の処理を依頼し、暗号化された情報をサーバ側通信制御装置 31 に送信し、復号された情報をクライアント装置 10 に送信する。サーバ側通信制御装置 31 は、IC カード 40 と、制御部 33 を有する。制御部 33 は、IC カード 40 に、相互認証と暗号化復号処理とのうち少なくとも一方の処理を依頼し、暗号化された情報をクライアント側通信制御装置 30 に送信し、復号された情報をサーバ装置 20 に送信する。この場合、通信制御装置 30（31）の制御部 33 は、IC カード 40 に相互認証の処理のみをさせてもよいし、暗号化復号処理のみをさせてもよいし、相

互認証と暗号化復号処理との両方の処理をさせてもよい。

[0110] これにより、実施形態の通信制御システム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。クライアント装置10からサーバ装置20に対して送信されたHTTPプロトコルの撮像データ（いわゆる平文）が、クライアント側通信制御装置30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20からクライアント装置10らに対して送信された制御データは、暗号化されるが、クライアント側通信制御装置30により復号されて、クライアント装置10に受信されるため、クライアント装置10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。

[0111] また、実施形態の通信制御システム1では、クライアント側通信制御装置30とサーバ側通信制御装置31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端末においては、サーバ端末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、社会インフラシステムにおいては、クライアント装置10とサーバ装置20の関係は明確に特定されている。このため、クライアント側通信制御装置30とサーバ側通信制御装置31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。

[0112] クライアント証明書を有していないクライアント端末の場合、サーバ端末と通信を行うために、サーバ端末が発行した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合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。

[0113] これに対し、実施形態の通信制御システム 1 では、クライアント側通信制御装置 30 がクライアント証明書を持有することにより、サーバ装置 20 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。

[0114] また、クライアント証明書を持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端末と通信を行う場合、ID とパスワードが正しく入力できてしまえば、だれでもサーバ端末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、サーバ端末へ不正にアクセスすることが可能となってしまう。このため例えば、不正に乗っ取られたサーバ端末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った。

[0115] これに対し、実施形態の通信制御システム 1 では、クライアント装置 10 とサーバ装置 20 との間で、通信制御装置 30 (31) を介した相互認証が行われることや、アドレス情報に基づいて通信相手のクライアント装置 10 が制限されることなどにより、クライアント装置 10 やサーバ装置 20 が不正に乗っ取られることがない。つまり、実施形態の通信制御システム 1 では、ランサムウェアに対する対策も可能となる。

[0116] 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った。これに対し、実施形態の通信制御システム 1 では、クライアント装置 10 とサーバ装置 20 との間で、通信制御装置 30 (31) を介した相互認証が行われることや、アドレス情報に基づいて通信相手のクライアント装置 10

が制限されることなどにより、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。

[0117] また、実施形態の通信制御システム1では、サーバ装置20がサーバ側通信制御装置31に接続されており、サーバ装置20の内部で認証処理を行わない。このため、サーバ装置20の内部で証明書等を保持する必要がなく、サーバ側通信制御装置31に接続されたサーバ装置20が通信制御管理装置50の管理下であることが明確となる。もっとも、サーバ装置20が、すでにサーバ側通信制御装置31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20とネットワークNWとの間にサーバ側通信制御装置31が物理的に接続される必要はない。この場合、サーバ装置20が元々有するサーバ側通信制御装置31に相当する機能部により、クライアント側通信制御装置30との間の認証処理が行われる。

[0118] また、実施形態の通信制御システム1では、ICカード40の制御部40B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、通信制御装置30（31）の装置コストを抑制することができる。

[0119] なお、実施形態の通信制御システム1においては、通信制御装置30（31）に装着されたICカード40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、当該処理を行う機能部がICカードに限定されることはない。

実施形態のICカード40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。

[0120] また、実施形態の通信制御システム1においては、クライアント側通信制御装置30のICカード40は、クライアント側通信制御装置30に対して着脱可能に装着される。これにより、実施形態の通信制御システム1におい

ては、ＩＣカード４０とクライアント側通信制御装置３０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４０とクライアント側通信制御装置３０とが一体化された場合には、ＩＣカード４０に相当する部分を交換する場合には、クライアント側通信制御装置３０全体を交換しなければならないが、この場合と比較して、実施形態の通信制御システム１では、クライアント側通信制御装置３０が有するＩＣカード４０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。

[0121] また、実施形態の通信制御システム１は、通信制御管理装置５０を更に備え、通信制御管理装置５０は、クライアント側通信制御装置３０に装着されたＩＣカード４０に記憶させる秘密鍵、及びクライアント証明書をクライアント側通信制御装置３０に送信し、サーバ側通信制御装置３１に装着されたＩＣカード４０に記憶させる秘密鍵、及びサーバ証明書をサーバ側通信制御装置３１に送信する。これにより、実施形態の通信制御システム１は、通信制御管理装置５０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更に向上させることができる。

[0122] 以上、実施形態の通信制御システム１について説明したが、実施形態の構成は、上記例に限定されない。例えば、通信制御装置３０（３１）は、処理の負荷に基づき、ハードウェアにより通信制御装置３０（３１）の機能を実現するＨＳＭ（Hardware Security Module）を用いてもよい。

[0123] また、実施形態の通信制御システム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、クライアント装置１０とサーバ装置２０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。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、通信制御装置30(31)により認証された正当な通信制御装置30(31)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、クライアント装置10やサーバ装置20に対する不正なアクセスや、クライアント装置10やサーバ装置20がマルウェアに感染することを抑止することができる。

[0124] また、実施形態の通信制御システム1においては、SSL/TLSプロトコルを用いた通信を常時行い、クライアント装置10やサーバ装置20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、通信制御管理装置50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。通信制御管理装置50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。

[0125] また、実施形態の通信制御システム1においては、通信制御装置30(31)に装着するICカード40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。

[0126] また、実施形態の通信制御システム1においては、サーバ装置20や通信制御管理装置50等から、通信制御装置30(31)を介して、クライアント装置10のプログラムを更新させるようにしてもよい。通信制御装置30(31)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、安全にクライアント装置10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20からクライアント装置10に対してファームウェアが送信される場合、サーバ装置20から送信されるファームウェアには、例えばサーバ側通信制御装置31により暗号化されたサーバ装置20の署名が付与される。この場合、クライアント装置10では、クライアント側通信制御装置30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20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20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クライアント装置10に送信されてしまった場合であっても、クライアント装置10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。

[0127] また、このように通信制御装置30(31)を介して通信が行われることにより、サーバ装置20や通信制御管理装置50等からクライアント装置10にファームウェアを安全に更新することができるため、作業員が複数のクライアント装置10に対して物理的に各々のクライアント装置10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。

[0128] また、実施形態の通信制御システム1においては、サーバ装置20や通信制御管理装置50等から、通信制御装置30(31)を介して、クライアント装置10の起動や停止を行ってもよい。通信制御装置30(31)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、安全にクライアント装置10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。

[0129] なお、上述した実施形態の通信制御システム1において、クライアント側通信制御装置30-1がサーバ側通信制御装置31-1と通信を行う例を説明したが、クライアント側通信制御装置30の通信先はこれに限定されることはない。例えば、クライアント側通信制御装置30-1は、クライアント側通信制御装置30-2と通信を行ってもよい。クライアント側通信制御装置30-1は、クライアント側通信制御装置30-2から通信開始の合図を受信した場合、まずクライアント側通信制御装置30-2との間で相互認証を行い、クライアント側通信制御装置30-2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、クライアント側通信制御装置30-1は、クライアント側通信制御装置30-2から受信した情

報をクライアント装置 10 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及び送信者の特定が可能となる。このため、本実施形態の通信制御システム 1 においては、クライアント側通信制御装置 30 とサーバ側通信制御装置 31 との通信、及びクライアント側通信制御装置 30 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。

[0130] 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同様に、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ものである。

符号の説明

[0131] 1…通信制御システム、10…クライアント装置、20…サーバ装置、30…クライアント側通信制御装置、31…サーバ側通信制御装置、33A…仲介処理部、33B…検知部、33C…通報部、33D…機能制限部、33E…設定部、33F…通信制限部 33

請求の範囲

- [請求項1] 第1装置および第2装置と通信し、且つ、前記第1装置または前記第2装置の少なくとも一方とは無線で通信し、前記第1装置により取得されたデータを前記第2装置に送信する通信部と、
- 前記第1装置との通信状態が所定の状態あるいは自装置の挙動が所定の挙動である場合に、前記第2装置に向けて、前記通信部に所定情報を送信させる通報部と、
- を備える通信制御装置。
- [請求項2] 前記通報部は、前記第1装置との通信状態に基づいて通信状態の変化が認識された場合に、前記第1装置との通信状態が所定の状態であるとして、前記所定情報を前記第2装置に向けて送信させる、
- 請求項1に記載の通信制御装置。
- [請求項3] 前記通信制御装置と前記第1装置とは無線通信で接続されており、
- 前記通報部は、前記第1装置との通信が切断された場合に、前記第1装置との通信状態が所定の状態であるとして、前記所定情報を前記第2装置に向けて送信させる、
- 請求項2に記載の通信制御装置。
- [請求項4] 前記通信制御装置と前記第1装置とは物理的に接続されており、
- 前記通報部は、前記第1装置との物理的な接続が切断された場合に、前記第1装置との通信状態が所定の状態であるとして、前記所定情報を前記第2装置に向けて送信させる、
- 請求項2に記載の通信制御装置。
- [請求項5] 前記通信制御装置の挙動を検出するセンサをさらに備え、
- 前記通報部は、前記センサの出力に基づいて前記自装置の挙動に変化が認識された場合、前記自装置の挙動が所定の挙動であるとして、前記所定情報を前記第2装置に向けて送信させる、
- 請求項1から4のうちいずれか一項に記載の通信制御装置。
- [請求項6] 前記第1装置との通信状態あるいは自装置の挙動が所定の状態であ

る場合に、前記第 1 装置の機能を停止または制限させる機能制限部をさらに備える、

請求項 1 から 5 のうちいずれか一項に記載の通信制御装置。

[請求項7]

前記通報部は、前記第 1 装置との通信状態が所定の状態あるいは自装置の挙動が所定の挙動である場合に、前記第 2 装置と異なる第 3 装置に向けて、前記通信部に所定情報を送信させる、

請求項 1 から 6 のうちいずれか一項に記載の通信制御装置。

[請求項8]

前記通信部は、

前記第 1 装置とネットワーク通信網との間に接続され、前記第 2 装置とネットワーク通信網との間に接続される第 2 の通信制御装置との間で通信を行い、

第 1 の認証部と、

前記第 1 の認証部に、プライベート認証局により発行された秘密鍵、及びクライアント証明書を用いる相互認証を前記第 2 の通信制御装置との間で行う相互認証処理と、前記相互認証処理により決定された共通鍵を用いて前記第 1 装置により前記第 2 装置に対して送信される情報を暗号化するとともに、前記第 2 装置により前記第 1 装置に対して送信された情報を復号する暗号化復号処理とのうち少なくとも一方の処理を依頼し、前記暗号化された情報を前記第 2 の通信制御装置に送信し、前記復号された情報を前記第 1 装置に送信する第 1 の制御部をさらに有する、

請求項 1 から 7 のうちいずれか一項に記載の通信制御装置。

[請求項9]

第 1 装置とネットワーク通信網との間に接続される第 1 の通信制御装置と、

第 2 装置とネットワーク通信網との間に接続される第 2 の通信制御装置と、

を備え、

前記第 1 の通信制御装置は、

前記第 1 装置および前記第 2 装置と通信し、且つ、前記第 1 装置または前記第 2 装置の少なくとも一方とは無線で通信し、前記第 1 装置により取得されたデータを前記第 2 装置に送信する通信部と、

自装置の挙動あるいは前記第 1 装置との通信状態が所定の状態である場合に、前記第 2 装置に向けて、前記通信部に所定情報を送信させる通報部と、

第 1 の認証部と、

前記第 1 の認証部に、プライベート認証局により発行された秘密鍵、及び第 1 証明書を用いる相互認証を前記第 2 の通信制御装置との間で行う相互認証処理と、前記相互認証処理により決定された共通鍵を用いて前記第 1 装置により前記第 2 装置に対して送信される情報を暗号化するとともに、前記第 2 装置により前記第 1 装置に対して送信された情報を復号する暗号化復号処理とのうち少なくとも一方の処理を依頼し、前記暗号化された情報を前記第 2 の通信制御装置に送信し、前記復号された情報を前記第 1 装置に送信する第 1 の制御部を有し、

前記第 2 の通信制御装置は、

第 2 の認証部と、

前記第 2 の認証部に、前記プライベート認証局により発行された秘密鍵、及び第 2 証明書を用いる相互認証を前記第 1 の通信制御装置との間で行う相互認証処理と、前記相互認証処理により決定された共通鍵を用いて前記第 2 装置により前記第 1 装置に対して送信される情報を暗号化するとともに、前記第 1 装置により前記第 2 装置に対して送信された情報を復号する暗号化復号処理とのうち少なくとも一方の処理を依頼し、前記暗号化された情報を前記第 1 の通信制御装置に送信し、前記復号された情報を前記第 2 装置に送信する第 2 の制御部を有する

通信制御システム。