

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、妨害制御部とを持つ。通信部は、第1装置と無線で通信し、前記第1装置から取得した情報をネットワークを介して第2装置にアップロードする。妨害制御部は、前記第1装置の使用する通信帯域で無線通信をしようとする装置のうち自装置以外の装置と前記第1装置との無線通信を、妨害電波を出力させることにより妨害する。

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による妨害処理の一例を示すフローチャート。

[図9]実施形態のクライアント側通信制御装置30による妨害処理の他の例を示すフローチャート。

[図10]第2実施形態の通信制御システム1A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、少なくとも一以上のクライアント装置10と、サーバ装置20と、少なくとも一以上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と、通信制御管理装置50と、ゲートウェイ60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、無線通信で通信する。

無線通信には、例えばWi-Fi網、Bluetooth(登録商標)などが含まれる。

[0010] クライアント側通信制御装置30は、ゲートウェイ60と無線通信あるいは有線通信で通信する。ゲートウェイ60は、ネットワークNWを介して、

無線通信あるいは有線通信でサーバ側通信制御装置 31 と通信する。サーバ側通信制御装置 31 は、ネットワーク NW を介して、有線通信でクライアント側通信制御装置 30 と通信する。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 とゲートウェイ 60 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 1

0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、I

P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] ここで、クライアント装置１０の通信相手として他の通信制御装置７０が出現した場合の一例について説明する。例えば、クライアント装置１０の設定を変更することにより、あるいは、クライアント側通信制御装置３０よりも電波強度の強い電波で無線通信することなどにより、通信相手が、クライアント側通信制御装置３０から他の通信制御装置７０に変更されたとする。あるいは、クライアント装置１０が、クライアント側通信制御装置３０と並行して、他の通信制御装置７０と無線通信で接続されたとする。この場合、他の通信制御装置７０が、クライアント装置１０の無線アクセスポイントとなり、セキュアな通信環境が確保されなくなる。実施形態のクライアント側通信制御装置３０は、妨害電波を出力することなどにより、他の通信制御装置７０とクライアント装置１０との通信を妨害する。なお、クライアント側通信制御装置３０は、自装置以外の装置とクライアント装置１０との無線通信を制限させることにより、他の通信制御装置７０とクライアント装置１０との通信を妨害してもよい。詳細については後述する。これにより、クライアント装置１０の通信相手をクライアント側通信制御装置３０に限定することが可能となり、安全性を向上させたセキュアな通信環境を確保することができる。

[0026] 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。

[0027] 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。

通信部１１は、クライアント装置１０の使用可能な通信帯域で無線通信する。クライアント装置１０の使用可能な通信帯域は、自装置により設定されてもよく、外部装置からの指示に従って設定されてもよい。また、クライアン

ト装置 10 の使用可能な通信帯域は、外部装置からの指示に従って変更されてもよい。

[0028] 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。

[0029] 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。

[0030] 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。

[0031] 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 23 に記憶させる。撮像データ記憶部 23 は、サーバ制御部 22 の指示に従い、撮像データを記憶する。

[0032] ここで、従来システムの一例について説明する。従来システムにおいて、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 HTTP 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。

[0033] 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CPU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CPU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。

[0034] 本実施形態において、クライアント装置10とネットワークNWとの間に接続されたクライアント側通信制御装置30が、クライアント装置10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。

[0035] 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。

[0036] 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。

[0037] 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。

[0038] 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、妨害制御部33B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。

[0039] 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10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。

[0040] 妨害制御部 33B は、クライアント装置 10 の使用する通信帯域で無線通信をしようとする装置のうち、クライアント側通信制御装置 30 以外の装置とクライアント装置 10 との無線通信を、妨害電波を出力することなどにより妨害する。妨害制御部 33B は、妨害電波の周波数帯や出力期間を決定する。妨害制御部 33B は、決定した周波数帯の妨害電波を出力するよう妨害電波出力部 37 を制御する。また、妨害制御部 33B は、決定した出力期間において妨害電波を出力するよう妨害電波出力部 37 を制御する。また、妨害制御部 33B は、決定した妨害電波の周波数帯や出力期間を記憶部 38 に格納してもよい。

[0041] 妨害制御部 33B は、以下に説明する妨害手法のうち少なくとも一つを採用する。

[0042] 初めに、第 1 妨害手法の一例について説明する。妨害制御部 33B は、クライアント側通信制御装置 30 とクライアント装置 10 との通信が可能な電波強度であって、且つ、クライアント装置 10 の使用可能な通信帯域の全域の周波数帯で、妨害電波を出力させる。

妨害制御部 33B は、例えば、クライアント装置 10 とクライアント側通信制御装置 30 との相対的な位置関係に基づいて、電波強度を決定する。例えば、妨害制御部 33B は、クライアント装置 10 とクライアント側通信制御装置 30 との距離に関する距離情報を、自身が備える距離計測部（図示は省略）による計測結果から取得してもよく、利用者が外部装置を用いて入力することにより外部装置から取得してもよい。こうすることにより、他の通信制御装置 70 の通信強度がクライアント側通信制御装置 30 の電波強度よりも弱い場合、他の通信制御装置 70 とクライアント装置 10 との通信を妨害

し、且つ、クライアント側通信制御装置 30 とクライアント装置 10 との通信を確保することができる。

[0043] 次に、第 2 妨害手法の一例について説明する。妨害制御部 33B は、クライアント装置 10 の使用する通信帯域のうちクライアント側通信制御装置 30 が使用可能な周波数帯以外の帯域で、妨害電波を出力させる。こうすることにより、他の通信制御装置 70 がクライアント装置 10 の使用する通信帯域以外の帯域でクライアント装置 10 と通信しようとする場合、他の通信制御装置 70 とクライアント装置 10 との通信を妨害し、且つ、クライアント側通信制御装置 30 とクライアント装置 10 との通信を確保することができる。

[0044] 次に、第 3 妨害手法の一例について説明する。妨害制御部 33B は、クライアント装置 10 とクライアント側通信制御装置 30 とが通信する期間を除いて、クライアント装置 10 の使用可能な全ての通信帯域で、妨害電波を出力させる。例えば、妨害制御部 33B は、クライアント装置 10 とクライアント側通信制御装置 30 とが通信する期間以外の全てを、出力期間に決定する。こうすることにより、クライアント側通信制御装置 30 とクライアント装置 10 との通信とが妨害電波の影響を受けることなく、他の通信制御装置 70 とクライアント装置 10 との通信を妨害することができる。

[0045] 次に、第 4 妨害手法の一例について説明する。妨害制御部 33B は、クライアント装置 10 の使用可能な通信帯域を、クライアント側通信制御装置 30 との通信帯域に制限する。言い換えると、妨害制御部 33B は、クライアント側通信制御装置 30 以外の装置（例えば、他の通信制御装置 70）とクライアント装置 10 との無線通信を制限させることにより、例えば他の通信制御装置 70 とクライアント装置 10 との無線通信を妨害する。

[0046] 第 4 妨害手法において、妨害制御部 33B は、クライアント装置 10 の使用可能な通信帯域の設定を、クライアント装置 10 に対して指示する。例えば、妨害制御部 33B は、クライアント装置 10 の使用可能な通信帯域のうちクライアント装置 10 が使用する第 1 通信帯域を、クライアント装置 10

の使用可能な通信帯域に設定するよう、クライアント装置１０に対して指示する。ここで、妨害制御部３３Ｂは、クライアント装置１０に対して第１通信帯域以外で無線通信しないように制限する指示をしてもよい。また、妨害制御部３３Ｂは、第１通信帯域でクライアント装置１０と通信するよう装置通信部３４に対して指示する。こうすることにより、クライアント装置１０の使用可能な通信帯域が制限され、他の通信制御装置７０とクライアント装置１０との通信を制限された通信帯域において妨害することができる。

[0047] また、第４妨害手法は、上述の第１～３の妨害手法を組み合わせることにより、他の通信制御装置７０がクライアント装置１０と通信する可能性を低減させることができる。

[0048] 次に、第５妨害手法の一例について説明する。妨害制御部３３Ｂは、クライアント装置１０の使用可能な通信帯域を、クライアント側通信制御装置３０との通信帯域に制限するとともに、その通信帯域を切り替える。例えば、妨害制御部３３Ｂは、クライアント装置１０の使用可能な通信帯域を、第２通信帯域に変更するようクライアント装置１０に対して指示する。妨害制御部３３Ｂは、例えば、クライアント装置１０と無線通信を開始した時に変更指示をしてもよく、定期的に変更指示をしてもよい。また、妨害制御部３３Ｂは、第２通信帯域でクライアント装置１０と通信するよう装置通信部３４に対して指示する。こうすることにより、クライアント装置１０の使用可能な通信帯域が制限され、且つ、使用可能な通信帯域が固定されないため、他の通信制御装置７０とクライアント装置１０との通信をより効果的に妨害することができる。

[0049] また、上述した第１～５妨害手法において、妨害制御部３３Ｂは、クライアント装置１０の通信機能に関する情報（以下、機能情報と記す）の送信をクライアント装置１０に指示し、取得した機能情報に基づいて、クライアント装置１０の使用可能な通信帯域や、妨害電波の周波数帯または妨害電波の出力期間のうち少なくとも一つを決定してもよい。機能情報には、例えば、クライアント装置１０の使用可能な通信帯域、現時点において設定されてい

るクライアント装置１０の使用可能な通信帯域、クライアント装置１０に設定可能な通信チャンネルに関する情報、現時点においてクライアント装置１０に設定されている通信チャンネルに関する情報などが含まれる。

[0050] また、上述した第１～５妨害手法において、妨害制御部３３Ｂは、過去にクライアント装置１０と無線通信した他の通信制御装置に関する情報（以下、通信履歴情報と記す）の送信をクライアント装置１０に指示し、取得した通信履歴情報に基づいて、クライアント装置１０の使用可能な通信帯域や、妨害電波の周波数帯または妨害電波の出力期間のうち少なくとも一つを決定してもよい。通信履歴情報には、例えば、過去にクライアント装置１０が他の通信制御装置との無線通信に使用した通信帯域やチャンネルを示す情報、過去にクライアント装置１０が他の通信制御装置との無線通信に使用した通信タイミングを示す情報などが含まれる。なお、通信履歴情報は、クライアント側通信制御装置３０において決定された過去の履歴が記憶部３８に格納されており、この情報に基づくものであってもよい。例えば、妨害制御部３３Ｂは、通信履歴情報に基づいて、過去にクライアント装置１０が他の通信制御装置との無線通信に使用した通信帯域（あるいはチャンネル）を妨害電波の周波数帯に決定する。また、妨害制御部３３Ｂは、通信履歴情報に基づいて、過去にクライアント装置１０が他の通信制御装置との無線通信に使用した通信タイミングを妨害電波の出力期間に決定する。

[0051] 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。

[0052] 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。

- [0053] 妨害電波出力部３７は、妨害制御部３３Ｂにより指示された周波数帯や電波強度の電波を出力する。また、妨害電波出力部３７は、妨害制御部３３Ｂにより指示された出力期間に継続して、妨害電波を出力する。妨害電波は、例えば、指定された周波数帯において通信をジャミングするためのノイズを含む電波である。
- [0054] 記憶部３８は、例えば、ＲＡＭ、ＲＯＭなどによって実現される。記憶部３８は、プロセッサが実行するプログラムを格納する他、妨害制御部３３Ｂにより決定された妨害電波の周波数帯や出力期間などを格納する。
- [0055] 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。
- [0056] 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。
- [0057] 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。
- [0058] 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。

- [0059] 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。
- [0060] 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端子を介してクライアント側通信制御装置３０に出力する。ＵＡＲＴ４３は、例えば、ＳＩＯ端子を介してコマンドをクライアント側通信制御装置３０から受信する。また、ＵＡＲＴ４３は、ＳＩＯ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３０に送信する。
- [0061] 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４０の各種処理を行う。ＣＰＵ４４は、例えば、コンタクト部３６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。
- [0062] 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４０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。
- ＲＡＭ４６は、例えば、ＳＲＡＭ（Static RAM）などの揮発性メモリであり、ＩＣカード４０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、電氣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４０が利用する各種データを記憶する。ＥＥＰＲＯＭ４７は、例えば、ＩＣカード４０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、ＩＣカード４０の構成の一例について説明する。図５は、実施形態のＩＣカード４０の機能構成例を示すブロック図である。ＩＣカード４０は、通信部４０Ａと、制御部４０Ｂと、記憶部４０Ｃとを備える。ここで、図５に示されるＩＣカード４０の各部は、図４に示されるＩＣカード４０のハードウェアを用いて実現される。

[0064] 通信部４０Ａは、例えば、ＵＡＲＴ４３と、ＣＰＵ４４と、ＲＯＭ４５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３６を介して、例えば、クライアント側通信制御装置３０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４０Ａ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３０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、ＵＡＲＴ４３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ＲＡＭ４６に記憶させる。また、通信部４０Ａは、ＲＡＭ４６に記憶されている送信データを、ＵＡＲＴ４３を介してクライアント側通信制御装置３０に送信する。

[0065] 制御部４０Ｂは、例えば、ＣＰＵ４４と、ＲＡＭ４５と、ＲＯＭ４６又はＥＥＰＲＯＭ４７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。

[0066] 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。

[0067] 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、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。

[0068] 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。

[0069] 記憶部４０Ｃは、例えば、EEPROM４７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４１Ｃは、通信制御管理装置５０が発行したクライアント装置１０（サーバ側通信制御装置３１の場合はサーバ装置２０）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３０に装着されるＩＣカード４０の証明書情報記憶部４１Ｃ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３１に装着されるＩＣカード４０の証明書情報記憶部４１Ｃには、サーバ証明書を示す情報が記憶される。

[0070] 秘密情報記憶部４２Ｃは、通信制御管理装置５０が発行したクライアント装置１０（サーバ側通信制御装置３１の場合はサーバ装置２０）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３０に装着されるＩＣカード４０の秘密情報記憶部４２Ｃには、クライアント側通信制御装置３０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３１に装着されるＩＣカード４０の証明書情報記憶部４１Ｃには、サーバ側通信制御装置３１に対して発行された秘密鍵を示す情報が記憶される。

[0071] 次に、通信制御管理装置５０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５０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５０は、例えば、NW（ネットワーク）通信部５０Ａと、

制御部50Bと、記憶部50Cとを備える。

[0072] NW通信部50A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30(31)と通信を行う。

[0073] 制御部50B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50を統括的に制御する。制御部50Bは、主に通信制御装置30(31)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50Bは、鍵生成部51Bと、証明書発行部52Bと、証明書更新部53Bと、証明書管理部54Bと、管理部55Bとを備える。

[0074] 鍵生成部51Bは、例えば、通信制御装置30(31)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。

[0075] 証明書発行部52Bは、例えば、通信制御装置30(31)からの認証申請に基づいて、通信制御装置30(31)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30(31)の所有者を示す情報が含まれる。

[0076] 証明書更新部53B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53Bは、例えば、通信制御装置30(31)からの更新申請に基づいて、当該通信制御装置30(31)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30(31)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30(31)により受信され、通信制御装置30(31)のICカード40の証明書情報記憶部41Cに記憶されることで、通信制御装置30(31)の証明書の有効期限が延長される。

[0077] 証明書管理部54B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54Bは、例えば、通信制御装置30(31)に装着されたICカード40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30(31)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54Bは、通信制御装置30(31)

1)からの問い合わせに基づいて、通信制御装置30(31)、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54B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54Bは、定期的に、発行済みの証明書が正当な通信制御装置30(31)に使用されているかを確認するようにしてもよい。

[0078] 管理部55Bは、通信制御装置30(31)を管理する。例えば、管理部55Bは、通信制御装置30(31)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。

[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。

[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)。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、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）。

[0082] 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。

[0083] 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。

[0084] 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。

[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。

[0086] 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。

[0087] 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。

[0088] 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)。

[0089] 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S 1 2）。クライアント側通信制御装置3 0により復号されたH T T Pレスポンスは、クライアント装置1 0に取得される（ステップS 1 3）。クライアント装置1 0は、復号されたH T T Pレスポンスを受信する（ステップS 1 4）。このとき、クライアント装置1 0は、サーバ装置2 0からH T T P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1 0は、サーバ装置2 0に対し、撮像データを送信する（ステップS 1 5）。

[0090] クライアント装置1 0が送信した撮像データは、クライアント側通信制御装置3 0により取得される（ステップS 1 6）。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S 1 8）。

クライアント側通信制御装置3 0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3 1に受信される（ステップS 1 9）。

[0091] サーバ側通信制御装置3 1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S 2 0）。サーバ側通信制御装置3 1により復号された撮像データは、サーバ装置2 0にとり取得される（ステップS 2 1）。サーバ装置2 0は、復号された撮像データを受信する（ステップS 2 2）。このとき、サーバ装置2 0は、クライアント装置1 0からの撮像データを受信したと認識する。

[0092] なお、上記フローチャートのステップS 5において、クライアント側通信制御装置3 0とサーバ側通信制御装置3 1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3 0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3 0は、通信先から送信された情報をクライアント装置1 0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3 1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3 0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。

[0093] 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。

[0094] 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。

[0095] 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。

[0096] 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。

[0097] 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。

[0098] 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。

[0099] 次に、クライアント側通信制御装置 30 による妨害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 による妨害処理の一例を示すフローチャートである。ここでは、上述した様々な妨害手法を合わせて説明する。

[0100] まず、妨害制御部 33B は、クライアント装置 10 の使用可能な通信帯域を示す情報などを取得する（ステップ S101）。妨害制御部 33B は、クライアント装置 10 と通信して情報を取得してもよく、他の外部装置と通信して情報を取得してもよい。また、妨害制御部 33B は、上述した機能情報や通信履歴情報をクライアント装置 10 から取得してもよい。

[0101] 次いで、妨害制御部 33B は、取得した情報に基づいて妨害電波の周波数帯や電波強度を決定する（ステップ S102）。例えば、第 1 妨害手法では、クライアント装置 10 との通信が可能な範囲で妨害電波の電波強度が決定され、第 2 妨害手法では、クライアント側通信制御装置 30 が使用可能な通信周波数帯以外の帯域で、妨害電波の周波数帯が決定される。また、第 4、5 妨害手法によって決定された周波数帯に基づいて妨害電波の周波数帯が決定されてもよい。そして、例えば第 1、2 妨害手法のように、出力期間を設定しない場合（ステップ S103-NO）、妨害制御部 33B は、妨害電波の出力を開始させる（ステップ S104）。妨害制御部 33B は、通信制御管理装置 50、クライアント装置 10、または他の外部装置からの妨害電波出力停止要求受信時（ステップ S105-YES）に、妨害電波の出力を停止する（ステップ S106）。

[0102] 一方、例えば第 3 妨害手法のように、出力期間を設定する場合（ステップ S103-YES）、妨害制御部 33B は、例えば、クライアント装置 10

とクライアント側通信制御装置30とが通信する期間以外の全ての期間を、出力期間に決定する(ステップS107)。そして、開始タイミングになった場合(ステップS108-YES)、妨害制御部33Bは、妨害電波出力部37を制御して、妨害電波の出力を開始させ(ステップS109)、終了タイミングになるまで妨害電波を継続的に出力させる。終了タイミングになった場合(ステップS110-YES)、妨害制御部33Bは、妨害電波の出力を停止させる(ステップS106)。

[0103] 次に、クライアント側通信制御装置30による妨害処理の他の例について説明する。図9は、実施形態のクライアント側通信制御装置30による妨害処理の他の例を示すフローチャートである。ここでは、上述した第4、5妨害手法を合わせて説明する。妨害制御部33Bは、クライアント装置10が外部装置からの指示に従って使用可能な通信帯域を設定あるいは変更することが可能である場合に、以下の処理を実行する。図9に示す妨害処理は、図8に示す妨害処理よりも前に実行されてもよく、並行して実行されてもよい。

[0104] まず、妨害制御部33Bは、クライアント装置10の使用可能な通信帯域を示す情報、機能情報、通信履歴情報などをクライアント装置10から取得する(ステップS201)。妨害制御部33Bは、取得した情報に基づいて、クライアント装置10の使用可能な通信帯域を決定する(ステップS202)。妨害制御部33Bは、例えば、クライアント側通信制御装置30と通信するために必要な最低限の範囲で、クライアント側通信制御装置30の使用する通信帯域を決定し、決定した通信帯域を、クライアント装置10の使用可能な通信帯域に決定する。そして、妨害制御部33Bは、装置通信部34を用いて、クライアント装置10に対して、決定した通信帯域だけで通信するよう指示する(ステップS203)。そして、妨害制御部33Bは、クライアント側通信制御装置30の使用する通信帯域で通信するよう、装置通信部34に指示する(ステップS204)。ここで、妨害制御部33Bは、ステップS201において取得した情報に基づいて、妨害電波の周波数帯や

出力期間を決定してもよい（ステップS 2 0 5）。

[0105] 次いで、妨害制御部3 3 Bは、設定したクライアント装置1 0の使用可能な通信帯域を変更するか否かを判定する（ステップS 2 0 6）。例えば、前回の設定から所定時間が経過した場合、変更すると判定する。変更する場合、妨害制御部3 3 Bは、取得した情報に基づいて、少なくとも前回と異なる帯域を、クライアント装置1 0の使用可能な通信帯域に決定する（ステップS 2 0 7）。なお、過去の使用可能な通信帯域を示す情報は、クライアント装置1 0から取得してもよく、自装置における記録から取得してもよい。そして、妨害制御部3 3 Bは、クライアント装置1 0の使用可能な通信帯域を、ステップS 2 0 7において決定した通信帯域に変更するようクライアント装置1 0に指示する（ステップS 2 0 8）。そして、妨害制御部3 3 Bは、ステップS 2 0 7で変更したクライアント側通信制御装置3 0の使用する通信帯域で通信するよう、装置通信部3 4に指示する（ステップS 2 0 9）。ここで、妨害制御部3 3 Bは、ステップS 2 0 1において取得した情報や変更結果などに基づいて、妨害電波の周波数帯や出力期間を決定してもよい（ステップS 2 1 0）。

[0106] （第2実施形態）

図1 0は、第2実施形態の通信制御システム1 Aの構成例を示す図である。通信制御システム1 Aは、妨害電波出力装置3 0 A、3 0 Bを備える点で、通信制御システム1 と異なる。妨害電波出力装置3 0 A、3 0 Bは、クライアント側通信制御装置3 0と有線あるいは無線で接続されている。妨害電波出力装置3 0 A、3 0 Bは、クライアント側通信制御装置3 0の指示に従って、指示された周波数帯や電波強度の妨害電波を、指定された出力期間に出力する。妨害電波出力装置3 0 A、3 0 Bは、例えば、クライアント側通信制御装置3 0とクライアント装置1 0との通信を妨害しない位置に設置される。両者の通信を妨害しない位置は、例えば、クライアント側通信制御装置3 0に対して、クライアント装置1 0と遠くなる方向の位置などである。

[0107] このような構成とすることで、クライアント装置1 0とクライアント側通

信制御装置 30 との通信が、妨害電波の影響を受けにくくなる。

[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、クライアント装置 10 と無線で通信し、クライアント装置 10 から取得した情報をネットワーク NW を介してサーバ装置 20 にアップロードする NW 通信部 32 と、クライアント装置 10 の使用する通信帯域で無線通信をしようとする装置のうち自装置以外の装置とクライアント装置 10 との無線通信を、妨害電波を出力させることにより妨害する妨害制御部 33B 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がクライアント装置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。

[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っ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る。

[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/IS015408）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…妨害制御部

請求の範囲

- [請求項1] 第1装置と無線で通信し、前記第1装置から取得した情報をネットワークを介して第2装置にアップロードする通信部と、
前記第1装置の使用する通信帯域で無線通信をしようとする装置のうち自装置以外の装置と前記第1装置との無線通信を、妨害電波を出力させることにより妨害する妨害制御部と、
を備える通信制御装置。
- [請求項2] 前記妨害制御部は、
前記通信制御装置が前記第1装置と通信が可能な電波強度であって、前記第1装置の使用可能な通信帯域の全域の周波数帯で、前記妨害電波を出力させる、
請求項1に記載の通信制御装置。
- [請求項3] 前記妨害制御部は、
前記第1装置の使用可能な通信帯域のうち前記通信制御装置が使用する通信帯域以外の帯域で、前記妨害電波を出力させる、
請求項1または2に記載の通信制御装置。
- [請求項4] 前記妨害制御部は、
前記第1装置と前記通信制御装置とが通信する期間を除いて、前記第1装置の使用可能な通信帯域で、前記妨害電波を出力させる、
請求項1から3のうちいずれか一項に記載の通信制御装置。
- [請求項5] 前記妨害制御部は、
前記第1装置の使用可能な通信帯域のうち前記第1装置が使用する第1通信帯域を、前記第1装置の使用可能な通信帯域として設定するよう前記第1装置に対して指示し、前記第1通信帯域で前記第1装置と通信するよう前記通信部に対して指示する、
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] 前記妨害制御部は、
前記第1装置の使用可能な通信帯域を第2通信帯域に変更するよう

前記第 1 装置に対して指示し、前記第 2 通信帯域で前記第 1 装置と通信するよう前記通信部に対して指示する、

請求項 5 に記載の通信制御装置。

[請求項 7] 前記通信部は、前記第 1 装置の通信機能に関する機能情報を前記第 1 装置から受信し、

前記妨害制御部は、前記機能情報に基づいて前記妨害電波の周波数帯または前記妨害電波の出力期間のうち少なくとも一方を決定する、

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] 第 1 装置と無線で通信し、前記第 1 装置から取得した情報をネットワークを介して第 2 装置にアップロードする通信部と、

妨害電波を出力させること、または、自装置以外の装置と前記第 1 装置との無線通信を制限させることの少なくとも一方により、前記第 1 装置の使用する通信帯域で無線通信をしようとする装置のうち自装置以外の装置と前記第 1 装置との無線通信を妨害する妨害制御部と、
を備える通信制御装置。

[請求項 9] 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 8 のうちいずれか一項に記載の通信制御装置。

[請求項10] 通信制御装置と少なくとも一つの妨害電波出力装置とを備える通信制御システムにおいて、

前記通信制御装置は、

第 1 装置と無線で通信し、前記第 1 装置と第 2 装置との通信を仲介する通信部と、

前記妨害電波出力装置に妨害電波を出力させることにより、前記第 1 装置の使用する通信帯域で無線通信をしようとする装置のうち自装置以外の装置と前記第 1 装置との無線通信を妨害する妨害制御部と、

を備える通信制御システム。

[請求項11] 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、

第 1 装置と無線で通信し、前記第 1 装置から取得した情報をネットワークを介して第 2 装置にアップロードする通信部と、

前記第 1 装置の使用する通信帯域で無線通信をしようとする装置のうち自装置以外の装置と前記第 1 装置との無線通信を、妨害電波を出力させることにより妨害する妨害制御部と、

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の制御部とを有し、

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の制御部とを有する

通信制御システム。