

明 細 書

発明の名称： 通信制御システム、及び通信制御装置

技術分野

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

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システム、及び通信制御装置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システムは、第1の通信制御装置と、第2の通信制御装置と、を持つ。前記第1の通信制御装置は、クライアント装置とネットワーク通信網とに接続される。前記第2の通信制御装置は、サーバ装置とネットワーク通信網とに接続される。前記第1の通信制御装置は、第1の認証部と、第1の制御部を有する。前記第1の制御部は、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通信において行う第1の相互認証処理と、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クライアント装置により前記サーバ装置に対して送信される情報を暗号化するとともに、前記サーバ装置によ

り前記クライアント装置に対して送信された情報を復号する第１の暗号化復号処理とのうち少なくとも一方の処理を前記第１の認証部に依頼し、前記第１の認証部に前記第１の暗号化復号処理を依頼した場合、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クライアント装置に送信する。前記第２の通信制御装置は、第２の認証部と、第２の制御部を有する。前記第２の制御部は、プライベート認証局により発行された秘密鍵、及びサーバ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通信において行う第２の相互認証処理と、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サーバ装置により前記クライアント装置に対して送信される情報を暗号化するとともに、前記クライアント装置により前記サーバ装置に対して送信された情報を復号する第２の暗号化復号処理とのうち少なくとも一方の処理を前記第２の認証部に依頼し、前記第２の認証部に前記第２の暗号化復号処理を依頼した場合、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サーバ装置に送信する。

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、およびサーバ装置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、および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。

発明を実施するための形態

[0007] 以下、実施形態の通信制御システム、及び通信制御装置を、図面を参照し

て説明する。

[0008] 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)(「第1の通信制御装置」の一例)と、サーバ側通信制御装置31(「第1の通信制御装置」の一例)と、通信制御管理装置50(「プライベート認証局」の一例)と、ネットワーク60と、ゲートウェイ70と、を備える。以下の説明においては、ネットワーク60と、ネットワーク60とクライアント装置10等とを接続するゲートウェイ70と、をまとめて「ネットワークNW」とも称する。

[0009] 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。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。

[0010] 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とに接続され、クライアント装置10とサーバ装置20との通信を仲介する。クライアント側通信制御装置30は、クライアント装置10によりサーバ装置20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20に対して出力する。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。

[0011] クライアント側通信制御装置30は、サーバ装置20によりクライアント装置10に対して送信されるデータを取得し、取得したデータをクライアント装置10に対して出力する。ここで、クライアント側通信制御装置30が取得するデータは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にデータを出力する際に、サーバ装置20からサーバ側通信制御装置31を介して取得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に出力する。

- [0012] 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とに接続され、クライアント装置１０とサーバ装置２０との通信を仲介する。サーバ側通信制御装置３１は、サーバ装置２０によりクライアント装置１０に対して送信されるデータを取得し、取得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。
- [0013] サーバ側通信制御装置３１は、クライアント装置１０によりサーバ装置２０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２０に対して出力する。ここで、サーバ側通信制御装置３１が取得するデータは暗号化されたデータである。サーバ側通信制御装置３１は、サーバ装置２０にデータを出力する際に、クライアント装置１０からクライアント側通信制御装置３０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２０に出力する。
- [0014] 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。
- [0015] 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 F T P S (FTP Secure) に置き換えてもよい。

- [0016] 本実施形態においては、クライアント側通信制御装置 3 0、またはサーバ側通信制御装置 3 1 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り。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。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。
- [0017] 通信制御管理装置 5 0 は、クライアント側通信制御装置 3 0 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 5 0 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。通信制御管理装置 5 0 は、IC カードが装着されたクライアント側通信制御装置 3 0 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。
- [0018] 通信制御管理装置 5 0 は、サーバ側通信制御装置 3 1 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 5 0 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。通信制御管理装置 5 0 は、IC カードが装着されたサーバ側通信制御装置 3 1 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 3 0 とサーバ側通信制御装置 3 1 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。
- [0019] ここでは、クライアント装置 1 0、およびサーバ装置 2 0 の構成について説明する。クライアント装置 1 0 とサーバ装置 2 0 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。

[0020] 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。

[0021] 図２は、実施形態のクライアント装置１０、およびサーバ装置２０の機能構成例を示すブロック図である。

[0022] クライアント装置１０は、NW（ネットワーク）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。NW通信部１１は、例えば、クライアント装置１０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、NW通信部１１は、クライアント側通信制御装置３０に接続され、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に出力する。NW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。

[0023] クライアント制御部１２は、例えば、CPU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、サーバ装置２０からの制御に従い、撮像部１３に撮像を開始または

停止させたり、撮像部 1 3 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。

[0024] 撮像部 1 3 は、クライアント制御部 1 2 の指示に従い、所定箇所における風景を撮像する。撮像部 1 3 は、撮像したデータ（撮像データ）を、クライアント制御部 1 2 に出力する。

[0025] サーバ装置 2 0 は、NW（ネットワーク）通信部 2 1 と、サーバ制御部 2 2 と、撮像データ記憶部 2 3 とを備える。NW通信部 2 1 は、例えば、サーバ装置 2 0 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、NW通信部 2 1 は、サーバ側通信制御装置 3 1 に接続され、サーバ装置 2 0 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側通信制御装置 3 1 に出力する。NW通信部 2 1 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、クライアント装置 1 0 と通信を行う機能部に相当する。

[0026] サーバ制御部 2 2 は、例えば、CPU などを含むプロセッサであり、サーバ装置 2 0 を統括的に制御する。サーバ制御部 2 2 は、例えば、クライアント装置 1 0 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。

[0027] 従来のシステムにおいて、クライアント装置 1 0 とサーバ装置 2 0 とが、互いの NW 通信部およびネットワーク NW を介して接続された場合、クライアント装置とサーバ装置 2 0 との通信には、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。

[0028] この場合、クライアント装置 1 0、またはサーバ装置 2 0 によりネットワーク NW 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 NW を流れる。この場合、外部から悪意をもってネットワーク NW 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。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 1 0 には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。例えば、クライアント装置10のクライアント制御部12は、撮像データを暗号化し、暗号化した撮像データをネットワークNWに出力する。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、クライアント制御部12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。クライアント制御部12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、更にクライアント制御部12に搭載させる等、クライアント制御部12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10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10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NWに出力されることが望ましい。

[0029] 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。サーバ装置20とネットワークNWと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。

[0030] ここでは、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の構成について図3を用いて説明する。図3は、実施形態のクライアント側通信制御装置30、および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である。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の機能構成は同じである。このため、以下では、一方（例えば、クライアント側通信制御装置30）の構成について説明し、他方（例

例えば、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。以下では、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。

[0031] 図 3 に示すように、通信制御装置 30 (31) 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。

[0032] ここで、IC カード 40 は、「認証部」の一例である。

[0033] NW 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、他方の通信制御装置 30 (31) と通信を行う。

[0034] 制御部 33 は、例えば、CPU などを含むプロセッサであり、通信制御装置 30 (31) を統括的に制御する。制御部 33 は、例えば、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とともに、IC カード 40 からレスポンスを受信する。制御部 33 は、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、他方の通信制御装置 30 (31) に送信する。制御部 33 は、NW 通信部 32 を介して、他方の通信制御装置 30 (31) から受信した情報に基づいて、IC カード 40 にコマンドを送信する。

[0035] 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。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。

[0036] 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。

[0037] 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。

ICカード40は、通信制御装置30(31)に着脱可能に装着され、コンタクト部36を介して通信制御装置30(31)と通信可能である。

[0038] ICカード40は、例えば、通信制御装置30(31)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)を通信制御装置30(31)にコンタクト部36を介して送信する。

[0039] 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。

[0040] ここでは、ICカード40のハードウェア構成について図4を用いて説明する。図4は、実施形態のICカード40のハードウェア構成例を示す図である。

[0041] 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。各構成(43から47)は、内部バスBSを介して接続されている。

[0042] UART43は、上述したSIO端子を介して、通信制御装置30(31)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。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、S I O端子を介して通信制御装置30(31)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通信制御装置30(31)から受信する。U A R T 4 3は、S I O端子を介してレスポンスを通信制御装置30(31)に送信する。

[0043] 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40の各種処理を行う。C P U 4 4は、例えば、コンタクト部36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。

[0044] 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。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。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40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。

[0045] 次に、I Cカード40の構成について、図5を用いて説明する。図5は、実施形態のI Cカード40の機能構成例を示すブロック図である。I Cカード40は、通信部400と、制御部401と、記憶部404とを備える。ここで、図5に示されるI Cカード40の各部は、図4に示されるI Cカード40のハードウェアを用いて実現される。

[0046] 通信部400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36を介して、例えば、通信制御装置30(31)と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400は、所定の処理を要求するコマンド(処理要求)を通信制御装置30(31)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)を通信制御装置30(31)に送信する。通信部40

0は、UART 43を介して通信制御装置30（31）から受信した受信データをRAM 46に記憶させる。通信部400は、RAM 46に記憶されている送信データを、UART 43を介して通信制御装置30（31）に送信する。

[0047] 制御部401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401は、コマンド処理部402と、暗号化復号部403とを備える。

[0048] ここで、コマンド処理部402が行う処理は、「第1の相互認証処理」及び「第2の相互認証処理」の一例である。暗号化復号部403が行う処理は、「第1の暗号化復号処理」及び「第2の暗号化復号処理」の一例である。

[0049] コマンド処理部402は、各種コマンド処理を実行する。コマンド処理部402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。

[0050] 暗号化復号部403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403は、通信部400を介して取得した装置（クライアント装置10、またはサーバ装置20）により出力されたデータを暗号化する。暗号化復号部403は、通信部400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。

[0051] 記憶部404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405と、秘密情報記憶部406とを備える。証明書情報記憶部405は、通信制御管理装置50が発行した装置（クライアント装置10、またはサーバ装置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405には、クライアント証明書を示す情報が記憶される。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405には、サーバ証明書を示す情報が記憶される。

[0052] 秘密情報記憶部406は、通信制御管理装置50が発行した装置（クライアント装置10、またはサーバ装置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406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。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405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。

[0053] ここでは、通信制御管理装置50の構成について、図6を用いて説明する。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500と、制御部501と、記憶部506とを備える。

[0054] NW通信部500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。

[0055] 制御部501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501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501は、鍵生成部502と、証明書発行部503と、証明書更新部504と、証明書管理部505と、管理部509とを備える。

[0056] 鍵生成部502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。

証明書発行部503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。

- [0057] 証明書更新部504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504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405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。
- [0058] 証明書管理部505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505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。証明書管理部505は、通信制御装置30(31)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505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。証明書管理部505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。
- [0059] 管理部509は、通信制御装置30(31)を管理する。例えば、管理部509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。
- [0060] 記憶部506は、例えば鍵情報記憶部507と、証明書情報記憶部508とを備える。鍵情報記憶部507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508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507と、証明書情報記憶部508とは、例えば、鍵生成部502が秘密鍵を発行する際、証明書発行部503が証明書を発行する際などに参照される。鍵情報記憶部507には、鍵生成部502が発行した秘密鍵を示す情報が記憶される。証明書情報記憶

部508には、証明書発行部503が発行した証明書を示す情報が記憶される。

[0061] ここでは、通信制御システム1が行う処理の流れについて、図7を用いて説明する。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。

[0062] 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）。

[0063] 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、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S3）。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との通信においてハンドシェイクが開始される（ステップS4）。

[0064] 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。

[0065] 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。

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との通信における相互認証は、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。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。

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との通信における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。

- [0066] 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との通信においてハンドシェイクが確立される。
- [0067] 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S5）。HTTPリクエストは、ステップS1においてクライアント装置10から送信されるHTTPリクエストである。
- [0068] 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S6）。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に対するHTTPレスポンスを応答する(ステップS7)。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S8)。

[0069] 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S10)。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S11)。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S12)。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S13)。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S14)。

[0070] 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S15)。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S16)。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S17)。

[0071] 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S18)。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S19)。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S20)。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。

- [0072] 上記フローチャートのステップS 4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との通信における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5 0に送信するようにしてもよい。これより、通信制御管理装置5 0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3 0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。
- [0073] クライアント側通信制御装置3 0は、上記フローチャートのステップS 4において行われるハンドシェイクにおいて相互認証の代わりにクライアント装置1 0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3 0の制御部3 3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。
- [0074] 制御部3 3は、送信先リストを更新するようにしてもよい。制御部3 3は、例えば、一定期間にクライアント装置1 0に対する通信を許可された通信先のURL、および許可されなかった通信先URLを記憶させる。そして、制御部3 3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3 0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。

[0075] クライアント側通信制御装置30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。

[0076] 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。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。

[0077] 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。

[0078] 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。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のが一般的である。このため、ファームウェアが更新される場合、クライアント装置10の負担が増大すると考えられる。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。これにより、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。

[0079] 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とネットワークNWと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。

[0080] 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。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。

[0081] 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。

[0082] 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。

[0083] 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と通信において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。

[0084] 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。

[0085] 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との通信において、通信制御装置３０（３１）を介した相互認証が行われることにより、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。

[0086] 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との通信において、通信制御装置３０（３１）を介した相互認証が行われる。これにより、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。

[0087] 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 3 1 に接続されており、サーバ装置 2 0 の内部で認証処理を行わない。このため、サーバ装置 2 0 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 3 1 に接続されたサーバ装置 2 0 が通信制御管理装置 5 0 の管理下であることが明確となる。もっとも、サーバ装置 2 0 が、すでにサーバ側通信制御装置 3 1 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 2 0 とネットワーク NW とにサーバ側通信制御装置 3 1 が物理的に接続される必要はない。この場合、サーバ装置 2 0 が元々有するサーバ側通信制御装置 3 1 に相当する機能部により、クライアント側通信制御装置 3 0 との通信において認証処理が行われる。

[0088] 実施形態の通信制御システム 1 では、ＩＣカード 4 0 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、通信制御装置 3 0 (3 1) の装置コストを抑制することができる。

[0089] 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 3 0 (3 1) に装着されたＩＣカード 4 0 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 4 0 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。

[0090] 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 3 0 のＩＣカード 4 0 は、クライアント側通信制御装置 3 0 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 4 0 とクライアント側通信制御装置 3 0 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 4 0 とクライアント側通信制御装置 3 0 とが一体化された場合には、ＩＣカード 4 0 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。しかしながら、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。

[0091] 実施形態の通信制御システム 1 では、通信制御管理装置 50 が、通信制御装置 30 (31) 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通信制御装置 30 (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。

[0092] 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。

[0093] 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。クライアント装置 10 とサーバ装置 20 との通信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。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。

。

- [0094] 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。
- [0095] 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）は、定期的に、自装置が接続されているクライアント装置１０またはサーバ装置２０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、通信制御管理装置５０に接続状態を示す情報が送信されるようにしてもよい。通信制御管理装置５０は、通信制御装置３０（３１）から接続状態を示す情報が受信できない場合などには、通信制御装置３０（３１）がクライアント装置１０またはサーバ装置２０から切り離された判断し、当該切り離された通信制御装置３０（３１）を無効とする。こうすることで通信制御管理装置５０は、切り離された通信制御装置３０（３１）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。
- [0096] 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。
- [0097] 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。

[0098] 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。このため、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。

[0099] 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。

[0100] 実施形態の通信制御システム１においては、クライアント装置１０、およびサーバ装置２０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。クライアント装置１０、およびサーバ装置２０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、クライアント装置１０が無線通信によりサーバ装置２０と通信を

行う場合、クライアント側通信制御装置 30 は、無線による通信機能を有し、クライアント装置 10 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 20 に送信する。

[0101] 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 がサーバ側通信制御装置 31 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 との通信において相互認証を行い、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。

[0102] 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

[0103] 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、40…ICカ

ード、４０２…コマンド処理部、４０３…暗号化復号部、４０５…証明書情報記憶部、４０６…秘密情報記憶部。