

## 明 細 書

発明の名称：通信制御装置および通信システム

### 技術分野

[0001] 本発明の実施形態は、通信制御装置および通信システムに関する。

### 背景技術

[0002] 通信システムは、取り扱うデータおよび機器の制御情報をマルウェア等の攻撃から防御される必要がある。例えば、社会インフラとして設置される監視カメラ等の機器は、通信するデータの安全性を確保することが必要である。しかしながら、監視カメラなどの社会インフラを構築する各機器は、一旦設置されると、頻繁に置換えることが難しいため、安全対策が不十分になってしまうという問題がある。

### 先行技術文献

#### 特許文献

[0003] 特許文献1：日本国特開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などに用いる通信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] 実施形態によれば、通信制御装置は、第1の装置とネットワーク通信網との間に並列に接続される複数の通信系統と分散制御器とを有する。分散制御器は、第1の装置またはネットワーク通信網と複数の通信系統との間に設け、第1の装置またはネットワーク通信網からのデータに対する処理の負荷に応じた数の通信系統で分散して通信処理を実行させる。複数の通信系統は、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た第2の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 の装置から前記第 2 の装置へ送信される情報を暗号化した情報を前記第 2 の通信制御装置へ送信し、前記第 2 の装置から前記第 1 の装置へ送信される情報を復号した情報を前記第 1 の装置に送信する通信処理を実行するコントローラを有する。

### 図面の簡単な説明

- [0006] [図1]図 1 は、各実施形態に係る通信システムの基本構成例を示す図である。
- [図2]図 2 は、各実施形態に係るクライアント装置およびサーバ装置の機能構成例を示すブロック図である。
- [図3]図 3 は、各実施形態に係るクライアント側の通信制御装置およびサーバ側の通信制御装置における機能構成例を示すブロック図である。
- [図4]図 4 は、各実施形態に係る通信制御装置における認証部の構成例としての IC カードのハードウェア構成例を示す図である。
- [図5]図 5 は、各実施形態に係る通信制御装置における認証部の構成例としての C カードにおける機能構成例を示すブロック図である。
- [図6]図 6 は、各実施形態に係る通信制御管理装置における機能構成例を示すブロック図である。
- [図7]図 7 は、図 1 に示す通信システムが行う処理の一例を示すシーケンスである。
- [図8]図 8 は、第 1 の実施形態に係る通信システムの第 1 の構成例を示す図である。
- [図9]図 9 は、第 1 の実施形態に係る通信システムの第 1 の構成例における通信制御装置の構成例を示すブロック図である。
- [図10]図 10 は、第 1 の実施形態の第 1 の構成例に係る通信システムの動作例を説明するためのシーケンスである。
- [図11]図 11 は、第 1 の実施形態に係る通信システムの第 2 の構成例を示す図である。
- [図12]図 12 は、第 1 の実施形態に係る通信システムの第 2 の構成例におけ

る通信制御装置の構成例を示すブロック図である。

[図13]図13は、第1の実施形態の第2の構成例に係る通信システムの動作例を説明するためのシーケンスである。

[図14]図14は、第2の実施形態に係る通信システムの構成例を示す図である。

[図15]図15は、第2の実施形態に係る通信システムの構成例における通信制御装置の構成例を示すブロック図である。

[図16]図16は、第2の実施形態に係る通信システムにおける分散制御器の動作例を説明するためのフローチャートである。

[図17]図17は、第3の実施形態に係る通信システムの構成例を示すブロック図である。

[図18]図18は、第3の実施形態に係る通信システムの第1の動作例を説明するためのシーケンスである。

[図19]図19は、第3の実施形態に係る通信システムの第2の動作例を説明するためのシーケンスである。

[図20]図20は、第4の実施形態に係る通信システムの第1の動作例を説明するためのシーケンスである。

[図21]図21は、第4の実施形態に係る通信システムの第2の動作例を説明するためのシーケンスである。

[図22]図22は、第4の実施形態に係る通信システムの第3の動作例を説明するためのシーケンスである。

## 実施形態

[0007] 以下、各実施形態について、図面を参照して説明する。

まず、各実施形態に係る通信システムのベースとなる基本的な構成例および動作例について説明する。

図1は、各実施形態に係る通信システムのベースとなる構成を有する通信システム1の構成例を示す図である。

通信システム1は、クライアント装置10（10-1～10-N）と、サ

サーバ装置20と、クライアント側の通信制御装置30（30-1～30-N）（「第1の通信制御装置」の一例）と、サーバ側の通信制御装置31（「第1の通信制御装置」の一例）と、通信制御管理装置5（「プライベート認証局」の一例）と、ネットワーク6と、ゲートウェイ7と、を備える。以下の説明においては、ネットワーク6と、ネットワーク6とクライアント装置10等とを接続するゲートウェイ7と、をまとめて「ネットワークNW」とも称する。

- [0008] クライアント装置10は、クライアント側の通信制御装置30を介してネットワークNWと接続する。サーバ装置20は、サーバ側の通信制御装置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。
- [0009] クライアント側の通信制御装置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。クライアント側の通信制御装置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、クライアント側の通信制御装置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。
- [0010] また、クライアント側の通信制御装置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、クライアント側の通信制御装置30が取得するデータは暗号化されたデータである。クライアント側の通信制御装置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からサーバ側の通信制御装置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。
- [0011] サーバ側の通信制御装置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。サーバ側の通信制御装置 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、サーバ側の通信制御装置 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。

[0012] また、サーバ側の通信制御装置 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、サーバ側の通信制御装置 31 が取得するデータは暗号化されたデータである。サーバ側の通信制御装置 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の通信制御装置 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。

[0013] クライアント側の通信制御装置 30 およびサーバ側の通信制御装置 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。クライアント側の通信制御装置 30 およびサーバ側の通信制御装置 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。

[0014] なお、クライアント側の通信制御装置 30 およびサーバ側の通信制御装置 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。クライアント側の通信制御装置 30 およびサーバ側の通信制御装置 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、クライアント側の通信制御装置 30 およびサーバ側の通信制御装置 31 は、FTP (File Transfer Protocol) を FTPS (FTP Secure) に置き換えてもよい。

- [0015] 通信システム 1 において、クライアント側の通信制御装置 30、またはサーバ側の通信制御装置 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、通信システム 1 におけるネットワーク NW を流れるデータは、暗号化されたデータであり。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。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。
- [0016] 通信制御管理装置 5 は、クライアント側の通信制御装置とサーバ側の通信制御装置とを用いた通信を管理するための通信管理サーバである。例えば、通信制御管理装置 5 は、クライアント側の通信制御装置 30 に対し、クライアント証明書、および秘密鍵を発行する。図 1 に示す構成例において、通信制御管理装置 5 は、クライアント側の通信制御装置 30 に装着する IC カードに記憶するクライアント証明書、および秘密鍵を発行する。また、通信制御管理装置 5 は、IC カードが装着されたクライアント側の通信制御装置 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。
- [0017] また、通信制御管理装置 5 は、サーバ側の通信制御装置 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 5 は、IC カードに記憶するサーバ証明書、および秘密鍵を発行する。また、通信制御管理装置 5 は、IC カードが装着されたサーバ側の通信制御装置 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、クライアント側の通信制御装置 30 とサーバ側の通信制御装置 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。
- [0018] ここでは、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。クライアント装置 10 とサーバ装置 20 とは、例えば、社会イン

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

[0019] 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。

[0020] 図２は、図１に示すクライアント装置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。

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。NW通信部１１は、クライアント側の通信制御装置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の通信制御装置３０に出力する。なお、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。

[0021] 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。

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。

[0022] サーバ装置２０は、NW（ネットワーク）通信部２１と、サーバ制御部２２と、撮像データ記憶部２３とを備える。NW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。NW通信部２１は、サーバ側の通信制御装置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の通信制御装置３１に出力する。なお、NW通信部２１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１０と通信を行う機能部に相当する。

[0023] 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。

[0024] クライアント装置１０とサーバ装置２０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２０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が用いられることがある。

[0025] この場合、クライアント装置１０、またはサーバ装置２０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１０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。

[0026] 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）を備えていないことが多い。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。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。

[0027] 通信システム１は、クライアント装置１０とネットワークNWとの間に接続されたクライアント側の通信制御装置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の通信制御装置３１は、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。

[0028] ここでは、クライアント側の通信制御装置３０、およびサーバ側の通信制御装置３１の構成について図３を用いて説明する。図３は、図１に示すクラ

クライアント側の通信制御装置３０、およびサーバ側の通信制御装置３１の機能構成例を示すブロック図である。クライアント側の通信制御装置３０、およびサーバ側の通信制御装置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、クライアント側の通信制御装置３０）の構成について説明し、他方（例えば、サーバ側の通信制御装置３１）の構成については説明を省略する。また、以下では、クライアント側の通信制御装置３０とサーバ側の通信制御装置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。

[0029] 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。

ここで、ＩＣカード４０は、「認証部」の一例である。認証部は、リーダライタ３５およびＩＣカード４０で実現するものに限定されない。認証部は、制御部３３が実現しても良いし、認証処理用の処理回路で実現しても良い。

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。

[0030] 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。また、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。また、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。

[0031] 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、クライアント側の通信制御装置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、サーバ側の通信制御装置 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。

[0032] リーダライタ 35 は、コンタクト部 36 を介して IC カード 40 に接続し、IC カード 40 との間の通信を行う。

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。また、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。

[0033] 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。

[0034] 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。

[0035] 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、図 3 に示す IC カード 40 のハードウェア構成例を示す図である。

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 (登録商標) (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。

[0036] 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。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端子を介して通信制御装置30(31)に出力する。UART43は、例えば、SIO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。また、UART43は、SIO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。

[0037] 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。

[0038] 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。

[0039] 次に、ICカード40の構成について、図5を用いて説明する。図5は、

図４に示す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５０と、制御部５１と、記憶部５４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。

[0040] 通信部５０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、通信制御装置３０（３１）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５０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５０は、ＵＡＲＴ４３を介して通信制御装置３０（３１）から受信した受信データをＲＡＭ４６に記憶させる。また、通信部５０は、ＲＡＭ４６に記憶されている送信データを、ＵＡＲＴ４３を介して通信制御装置３０（３１）に送信する。

[0041] 制御部５１は、例えば、ＣＰＵ４４と、ＲＡＭ４５と、ＲＯＭ４６又はＥＰＲＯＭ４７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５１は、コマンド処理部５２と暗号化復号部５３とを備える。

ここで、コマンド処理部５２が行う処理は、「認証処理」の一例である。

また、暗号化復号部５３が行う処理は、「暗号化復号処理」の一例である。

[0042] コマンド処理部５２は、各種コマンド処理を実行する。コマンド処理部５２は、例えば、後述するＨＴＴＰＳリクエストを要求するコマンド処理として、ＳＳＬ／ＴＬＳハンドシェイクを行う。ＳＳＬ／ＴＬＳハンドシェイクでは、暗号化された通信に必要な鍵情報等の交換、および通信先の装置との相互認証を行う。ここで、相互認証とは、クライアント側の通信制御装置３０とサーバ側の通信制御装置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。

[0043] 暗号化復号部５３は、データを暗号化する処理、および暗号化されたデータを復号する処理を実行する。暗号化復号部５３は、通信部５０を介して取

得した装置（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。また、暗号化復号部５３は、通信部５０を介して取得したネットワークNWからの暗号化されたデータを復号する。

[0044] 記憶部５４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５５と、秘密情報記憶部５６とを備える。証明書情報記憶部５５は、通信制御管理装置５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、クライアント側の通信制御装置３０に装着されるＩＣカード４０の証明書情報記憶部５５には、クライアント証明書を示す情報が記憶される。また、サーバ側の通信制御装置３１に装着されるＩＣカード４０の証明書情報記憶部５５には、サーバ証明書を示す情報が記憶される。

[0045] 秘密情報記憶部５６は、通信制御管理装置５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、クライアント側の通信制御装置３０に装着されるＩＣカード４０の秘密情報記憶部５６には、クライアント側の通信制御装置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、サーバ側の通信制御装置３１に装着されるＩＣカード４０の証明書情報記憶部５５には、サーバ側の通信制御装置３１に対して発行された秘密鍵を示す情報が記憶される。

[0046] ここでは、通信制御管理装置５の構成について、図６を用いて説明する。図６は、図１に示す通信制御管理装置５の構成例を示すブロック図である。通信制御管理装置５は、例えば、NW（ネットワーク）通信部６０と、制御部６１と、記憶部６６とを備える。

NW通信部６０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。

[0047] 制御部６１は、例えば、CPUなどのプロセッサを含む。制御部６１は、プロセッサがプログラムを実行することにより種々の処理を実現する。制御部６１は、通信制御管理装置５を統括的に制御する。また、制御部６１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

動作する。図6に示す例では、制御部61は、プロセッサがプログラムを実行することにより、鍵生成部62、証明書発行部63、証明書更新部64、証明書管理部65および管理部69としての機能を実現するための処理を実行する。

[0048] 鍵生成部62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。

[0049] 証明書発行部63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。

[0050] 証明書更新部64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64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。

[0051] 証明書管理部65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65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65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65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65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。

[0052] 管理部 6 9 は、通信制御装置 3 0 ( 3 1 ) を管理する。例えば、管理部 6 9 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。

記憶部 6 6 は、例えば、鍵情報記憶エリア 6 7 と、証明書情報記憶エリア 6 8 とを備える。鍵情報記憶エリア 6 7 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。証明書情報記憶エリア 6 8 は、例えば既に発行済みの証明書を示す情報を記憶する。鍵情報記憶エリア 6 7 と、証明書情報記憶エリア 6 8 とは、例えば、鍵生成部 6 2 が秘密鍵を発行する際、証明書発行部 6 3 が証明書を発行する際などに参照される。また、鍵情報記憶エリア 6 7 には、鍵生成部 6 2 が発行した秘密鍵を示す情報が記憶される。また、証明書情報記憶エリア 6 8 には、証明書発行部 6 3 が発行した証明書を示す情報が記憶される。

[0053] ここでは、通信システム 1 が行う処理の流れについて、図 7 を用いて説明する。

[0054] 図 7 は、通信システム 1 が行う処理の一例を示すシーケンスチャートである。

[0055] クライアント装置 1 0 は、撮像データをサーバ装置 2 0 に送信する場合、まずサーバ装置 2 0 に対する HTTP リクエストを送信する（ステップ S 1）。クライアント装置 1 0 が送信した HTTP リクエストは、クライアント側の通信制御装置 3 0 により取得される（ステップ S 2）。

[0056] クライアント側の通信制御装置 3 0 は、クライアント装置 1 0 により送信された HTTP リクエストを取得すると、サーバ側の通信制御装置 3 1 に対して、HTTPS のリクエスト (Client Hello) を送信する（ステップ S 3）。これにより、クライアント側の通信制御装置 3 0 とサーバ側の通信制御装置 3 1 との間のハンドシェイクが開始される（ステップ S 4）。

[0057] 具体的には、クライアント側の通信制御装置 3 0 が送信する Client Hello には、例えば、TLS のバージョン、および通信に用いる暗号方式やアルゴリズムのリストを示す情報が含まれる。サーバ側の通信制御装置 3 1 は、Cli

ent Helloに対する応答として、クライアント側の通信制御装置30に対しHTTPSのレスポンス (Server Hello) を送信する。サーバ側の通信制御装置31が送信するServer Helloには、例えばClient Helloで提示された選択肢の中でサーバ装置20が選択した情報が含まれる。換言すると、クライアント側の通信制御装置30からの提示に対し、サーバ側の通信制御装置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。

[0058] そして、サーバ側の通信制御装置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。クライアント側の通信制御装置30は、サーバ側の通信制御装置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。

[0059] クライアント側の通信制御装置30とサーバ側の通信制御装置31との間の相互認証は、例えば次のように行われる。クライアント側の通信制御装置30は、今までに受信したServer Hello等から署名を生成し、サーバ側の通信制御装置31に送信する。サーバ側の通信制御装置31は、クライアント側の通信制御装置30から受信した署名を、クライアント側の通信制御装置30から受信した証明書に基づいて検証する。サーバ側の通信制御装置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の通信制御装置30のものであると判定する。また、サーバ側の通信制御装置31は、今までに受信したClient Hello等から署名を生成し、クライアント側の通信制御装置30に送信する。クライアント側の通信制御装置30は、サーバ側の通信制御装置31から受信した署名を、サーバ側の通信制御装置31から受信した証明書に基づいて検証する。クライアント側の通信制御装置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の通信制御装置31のものであると判定する。

- [0060] クライアント側の通信制御装置30とサーバ側の通信制御装置31との間の相互認証が正しく行われると、クライアント側の通信制御装置30とサーバ側の通信制御装置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。
- [0061] サーバ側の通信制御装置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、クライアント側の通信制御装置30に許容される証明書であれば、サーバ側の通信制御装置31は、クライアント側の通信制御装置30から送付された公開鍵とその証明書が、サーバ側の通信制御装置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。
- [0062] サーバ側の通信制御装置31は、クライアント側の通信制御装置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。
- [0063] サーバ側の通信制御装置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に対しする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、サーバ側の通信制御装置31により取得される（ステップS8）。
- [0064] サーバ側の通信制御装置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）。サーバ側の通信制御装置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の通信制御装置30に受信される（ステップS10）。クライアント側の通信制御装置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）。クライアント側の通信制御装置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

S 1 2)。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 3）。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 4）。

[0065] クライアント装置 1 0 が送信した撮像データは、クライアント側の通信制御装置 3 0 により取得される（ステップ S 1 5）。クライアント側の通信制御装置 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 6）。クライアント側の通信制御装置 3 0 により暗号化された撮像データは、ネットワーク NW を介してサーバ側の通信制御装置 3 1 に受信される（ステップ S 1 7）。

[0066] サーバ側の通信制御装置 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 1 8）。サーバ側の通信制御装置 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 1 9）。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 0）。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。

[0067] なお、上記フローチャートのステップ S 4 において、クライアント側の通信制御装置 3 0 とサーバ側の通信制御装置 3 1 との間の相互認証が正しく行われなかった場合、クライアント側の通信制御装置 3 0 は、通信先との通信を許可しない。具体的には、クライアント側の通信制御装置 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、通信先がサーバ側の通信制御装置 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、クライアント側の通信制御装置 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 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 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の通信制御装置 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。

[0068] また、クライアント側の通信制御装置30は、上記フローチャートのステップS4において行われるハンドシェイクにおいて相互認証の代わりにクライアント装置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。クライアント側の通信制御装置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。

[0069] 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、クライアント側の通信制御装置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5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5は、クライアント側の通信制御装置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5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5が管理下にあるクライアント側の通信制御装置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。

[0070] また、クライアント側の通信制御装置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、クライアント側の通信制御装置3

0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5は、例えば、クライアント側の通信制御装置30およびサーバ側の通信制御装置31それぞれに検証鍵を送信するようにしてもよい。

[0071] 例えば、サーバ側の通信制御装置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、サーバ側の通信制御装置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、クライアント側の通信制御装置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。

[0072] また、クライアント側の通信制御装置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。クライアント側の通信制御装置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、クライアント側の通信制御装置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、クライアント側の通信制御装置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またはサーバ側の通信制御装置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して判定する。この場合、クライアント側の通信制御装置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。

[0073] 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に代わりサーバ側の通信制御装置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。

[0074] 以上説明したように、通信システム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の通信制御装置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の通信制御装置３１と、を備える。クライアント側の通信制御装置３０は、クライアント装置１０からの情報を暗号化してネットワークNW経由でサーバ側の通信制御装置３１へ送信し、ネットワークNWからの情報（通信制御装置３１で暗号化されたサーバ装置２０からの情報）を復号してクライアント装置１０へ送信する。サーバ側の通信制御装置３１は、サーバ装置２０からの情報を暗号化してネットワークNW経由でクライアント側の通信制御装置３０へ送信し、ネットワークNWからの情報（通信制御装置３０で暗号化されたクライアント装置からの情報）を復号してサーバ装置２０に送信する。

[0075] これにより、通信システム１は、社会インフラシステムを変更することなく、社会インフラシステムの安全性を向上させることができる。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、クライアント側の通信制御装置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、クライアント側の通信制御装置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。

[0076] また、通信システム１では、クライアント側の通信制御装置３０とサーバ側の通信制御装置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装置とにおいては、サーバ装置に対して不特定多数のクライアント端末が通信を行うため、当該不特定多数のクライアント端末に対して

正当なクライアント証明書を発行して管理し続けることは現実的ではない。しかしながら、通信システムを適用する社会インフラシステムなどにおいては、クライアント装置１０とサーバ装置２０との関係は明確に特定されている。このため、クライアント側の通信制御装置３０とサーバ側の通信制御装置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。

[0077] 一般に、クライアント証明書を有していないクライアント端末では、サーバ装置と通信を行うために、サーバ装置が発行したＩＤやパスワードの入力を求められることがある。このようなパスワード認証においては、安全性を維持するために、パスワードに対し文字と数字を組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。

[0078] これに対し、通信システム１では、クライアント側の通信制御装置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。

[0079] また、クライアント証明書を有していないクライアント端末がＩＤやパスワードによる認証に基づいてサーバ装置と通信を行うシステムでは、ＩＤとパスワードが正しく入力できてしまえば、だれでもサーバ装置と通信することができてしまう。このため、クライアント端末を不正に乗っ取り、サーバ装置へ不正にアクセスすることが可能となってしまう。例えば、不正に乗っ取られたサーバ装置によってクライアント端末の機能が制限され、解除するために身代金が要求されるといったランサムウェアに感染する可能性がある。

- [0080] これに対し、上述した通信システム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、通信システム１では、ランサムウェアに対する対策も可能となる。
- [0081] また、例えば、ネットワーク内に管理者が不在の端末（野良デバイスともいう）がある場合、その端末が不正に乗っ取られることにより、その端末がマルウェア等の攻撃を行う不正な端末として利用されてしまう場合がある。これに対し、上述した通信システム１では、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。
- [0082] また、上述した通信システム１では、サーバ装置２０がサーバ側の通信制御装置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、サーバ側の通信制御装置３１に接続されたサーバ装置２０が通信制御管理装置５の管理下であることが明確となる。サーバ装置２０がすでにサーバ側の通信制御装置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との間にサーバ側の通信制御装置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の通信制御装置３１に相当する機能部により、クライアント側の通信制御装置３０との間の認証処理が行われる。
- [0083] また、通信システム１では、ＩＣカード４０の制御部４０１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。
- [0084] また、通信システム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、通信システム１は、相互認証および暗号化複合化処理を行う構成がＩＣカードに限定されるものではない。また、上述したＩＣカード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し、カードの形態を採用しなくてもよい。

[0085] また、通信システム１においては、クライアント側の通信制御装置３０のＩＣカード４０は、クライアント側の通信制御装置３０に対して着脱可能に装着される。これにより、通信システム１においては、ＩＣカード４０とクライアント側の通信制御装置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とクライアント側の通信制御装置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、クライアント側の通信制御装置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、通信システム１では、クライアント側の通信制御装置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。

[0086] また、通信システム１は、通信制御管理装置５を更に備え、通信制御管理装置５は、クライアント側の通信制御装置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の通信制御装置３０に送信し、サーバ側の通信制御装置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の通信制御装置３１に送信する。これにより、通信システム１は、通信制御管理装置５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。

[0087] なお、通信システム１の構成は、上述した例に限定されない。例えば、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。つまり、通信制御装置 30 (31) は、セキュアな処理が可能な限り、必ずしも IC カードを装着する構成に限らず、上記通信制御装置 30 (31) の機能を実現できる IC チップや IC モジュールを用いた構成としてもよい。

[0088] また、通信システム 1 においては、SSL/TLS プロトコルを用いたセキュアな通信を常時行うようにしてもよいし、SSL/TLS プロトコルを用いた通信を行うか否かを選択可能にしてもよい。また、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。

[0089] 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。

[0090] また、通信システム 1 においては、SSL/TLS プロトコルを用いた通信を常時行い、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 5 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 5 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。

[0091] また、通信システム 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５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５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５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。

[0092] また、通信システム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。

[0093] また、通信システム１においては、サーバ装置２０や通信制御管理装置５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、例えばサーバ側の通信制御装置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、クライアント側の通信制御装置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。

- [0094] 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 5 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。
- [0095] また、通信システム 1 においては、サーバ装置 20 や通信制御管理装置 5 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。
- [0096] また、通信システム 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、クライアント側の通信制御装置 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。
- [0097] なお、上述した通信システム 1 において、クライアント側の通信制御装置 30 がサーバ側の通信制御装置 31 と通信を行う例を説明したが、クライアント側の通信制御装置 30 の通信先はこれに限定されることはない。例えば、クライアント側の通信制御装置 30-1 は、クライアント側の通信制御装置 30-2 と通信を行ってもよい。クライアント側の通信制御装置 30-1 は、クライアント側の通信制御装置 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の通信制御装置 30-2 との間で相互認証を行い、クライアント側の通信制御装置 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、クライアント側の通信制御装置30-1は、クライアント側の通信制御装置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、通信システム1においては、クライアント側の通信制御装置30とサーバ側の通信制御装置31との通信、及びクライアント側の通信制御装置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。

[0098] (第1の実施形態)

次に、第1の実施形態に係る通信システムについて説明する。

図8は、第1の実施形態に係る通信システム100の第1構成例を示す図である。図8に示す通信システム100は、図1に示すシステム構成において通信制御装置30を通信制御装置101に置き換えたものである。また、図8に示す構成例において、通信制御装置101は、ネットワークNWとクライアント装置10との間に、並列に設けた複数の通信デバイス111A、111Bを有する。

[0099] 図8に示す構成において、通信システム100における通信制御装置101以外の各装置は、図1に示す装置と同様な構成で実現することができる。このため、以下、通信制御装置101以外の構成については、詳細な説明を省略するものとする。

なお、通信システム100においては、通信制御装置31についても、通信制御装置101と同様に、ネットワークNWとサーバ装置20との間に、並列に設けた複数の通信デバイスを具備する構成としても良い。

図9は、第1の実施形態に係る通信システム100の第1の構成例における通信制御装置101の構成例を示すブロック図である。

図9に示す構成例において、通信制御装置101は、複数の通信デバイス111として並列に配置した第1通信デバイス111Aと第2通信デバイス111Bとを有する。第1通信デバイス111Aと第2通信デバイス111

Bとは、通信制御装置101において、ネットワークNW側に接続するハブ114とクライアント側に接続するハブ115との間に並列に接続する。第1通信デバイス111Aおよび第2通信デバイス111Bは、それぞれが上述した図1に示す通信制御装置30と同等の通信処理を実行する構成を有する。

[0100] また、図9に示す構成例において、通信制御装置101は、第1通信デバイス111Aと第2通信デバイス111Bとが共用する電源116およびメモリ／F117とを有するものとする。電源116は、外部電源に接続され、外部電源からの電力を各通信デバイス111A、111Bへ供給する。メモリ／F117は、メモリカードなどのメモリデバイス118をセットするインターフェースである。例えば、メモリ／F117には、初期設定情報などの通信デバイス111A、111Bに適用する情報を記憶したメモリデバイス118がセットされる。メモリ／F117にセットするメモリデバイス118は、通信デバイス111A、111Bから供給されるデータ（例えば、ログデータ）を記憶するようにしても良い。

[0101] ただし、第1実施形態に係る通信制御装置101は、通信制御装置30と同様な構成を有する複数の通信デバイスを並列に配置したシステムとして実現しても良い。このようなシステムでは、各通信デバイスがそれぞれ電源およびメモリ／Fなどを具備する構成として良い。また、通信制御装置101において、第1通信デバイス111Aと第2通信デバイス111Bとは、ネットワークNWとクライアント装置10との間に並列に配置するものであれば良い。例えば、通信制御装置101は、ハブ114及び115を設けずに、第1通信デバイス111Aと第2通信デバイス111Bとが、それぞれネットワークNWおよびクライアント装置10に接続するインターフェースを具備した構成であっても良い。

[0102] 各通信制御装置101において、第1通信デバイス111Aおよび第2通信デバイス111Bは、ネットワークNWとクライアント装置10との間に並列に配置され、何れか一方が通常通信モード（第1の通信モード）による

通信処理を実行する。通信制御装置１０１は、通常通信モードで通信する通信デバイス１１１Ａ、１１１Ｂを切り替えることによりネットワークNWとクライアント装置１０との間における通信制御を実現する。

[0103] ここで、通常通信モードは、上述したようなサーバ側の通信制御装置３１との相互認証に基づく共通鍵を用いた送受信データの暗号化および復号化を伴う通信を行う動作モードであるものとする。また、本実施形態において、通信制御装置１０１は、通常通信モードにおいて、後述するホワイトリストにある宛先との通信を許可するホワイトリスト運用モードで通信を実行するものとする。

[0104] なお、通信制御装置１０１において並列に設ける第１通信デバイス１１１Ａおよび第２通信デバイス１１１Ｂは、それぞれが独立した２つの通信処理用のソフトウェアで実現するものであっても良い。この場合、ハードウェアとしては１つの通信デバイスを２つのソフトウェアで実現する並列に配置した２つの通信デバイスとして動作するようにしても良い。

[0105] 各通信デバイス１１１（第１通信デバイス１１１Ａおよび１１１Ｂ）は、自身の故障、不正アクセス、あるいは、マルウェア感染などを検知する機能を有する。例えば、通信デバイス１１１は、故障、不正アクセス又はマルウェア感染などを示す故障や通信障害などの不具合を示す情報を通信制御管理装置（デバイス管理サーバ）５へ送信する。また、各通信デバイス１１１は、通信制御管理装置５からの指示に応じて動作モードを切り替える。例えば、各通信デバイス１１１は、通信制御管理装置５からの指示に応じて未通信状態から通常通信モードに切り替えたり、通常通信モードから未通信状態に切り替えたりする。

[0106] 各通信デバイス１１１（１１１Ａ、１１１Ｂ）は、図９に示すように、コントローラ１２０、ブリッジ１３２、ハブ１３３、ブリッジ１３４、リーダーライタ１３５およびＩＣカード１４０を有する。

コントローラ１２０は、通信デバイス１１１を制御するものである。図９に示す構成例において、コントローラ１２０は、ＭＰＵ１２１、ＲＡＭ１２

2、SAM 123およびデータメモリ 124などを有する。

[0107] MPU 121は、コントローラ 120の制御を司るプロセッサの一例である。MPU 121は、データメモリ 124などに記憶したプログラムを実行することで種々の処理を実現する。例えば、コントローラ 120は、MPU 121がプログラムを実行することにより、通信制御、故障検知、通信障害の検知、自己診断、および、ログ情報の収集などの処理を実行する。

[0108] また、コントローラ 120は、MPU 121がプログラムを実行することにより、サーバ側の通信制御装置 31との相互認証処理、クライアント装置 10からネットワークNWへ送出するデータの暗号化処理、ネットワークNWを経由してクライアント装置へ送信される暗号化されたデータの復号化処理などを行うようにしても良い。また、コントローラ 120は、リーダライタ 135を介して接続するICカード 140に対して、相互認証処理、暗号化処理および復号化処理の少なくとも何れか1つを依頼するようにしても良い。

[0109] RAM 122は、ランダムアクセスメモリである。RAM 122は、作業用のデータを保持するワーキングメモリとして機能する。SAM 123は、シリアルアクセスメモリである。データメモリ 124は、書き換え可能な不揮発性のメモリである。

データメモリ 124は、プログラムおよび設定情報などを記憶する。例えば、データメモリ 124は、通信を許可する宛先のリストを示すホワイトリストを記憶する。コントローラ 120は、通信モードがホワイトリストにある宛先との通信を行うホワイトリスト運用モード（通常通信モード、第1の通信モード）である場合、データメモリ 124に記憶するホワイトリストを参照して通信を実行する。また、コントローラ 120は、データメモリ 124にあるホワイトリストを通信制御管理装置 5からの指示に応じて書き換えるようにしても良い。例えば、通信デバイス 111は、ホワイトリストにある宛先をすべて削除することにより未通信状態とするようにしても良い。また、データメモリ 124は、当該通信デバイスの動作状態を示すログ情報を

記憶するようにしても良い。データメモリ 124 に蓄積したログ情報は、通信制御管理装置（デバイス管理サーバ）5 へ送ったり、自己診断処理などに用いたりする。

[0110] ブリッジ 132、134 は、通信インターフェース（通信部）として機能する。ブリッジ 132 および 134 は、ハブ 133 を介してコントローラ 120 に接続される。

ブリッジ 132 は、通信デバイス 111 におけるネットワーク NW 側の通信を実行する。ブリッジ 132 は、図 3 に示す NW 通信部 32 としての通信を実現する。ブリッジ 132 は、ネットワーク NW から受信するデータをハブ 133 を介してコントローラ 120 へ供給する。また、ブリッジ 134 は、コントローラ 120 または IC カード 140 で暗号化したデータをネットワーク NW へ送出する。

[0111] ブリッジ 134 は、通信デバイス 111 におけるクライアント装置 10 側の通信を実行する。ブリッジ 134 は、図 3 に示す装置通信部 34 としての通信を実現する。ブリッジ 134 は、クライアント装置 10 からのデータをハブ 133 を介してコントローラ 120 へ供給する。例えば、ブリッジ 134 は、ネットワーク NW からの暗号化されたデータをコントローラ 110 または IC カード 140 で復号化したデータをクライアント装置 10 へ送出する。

[0112] リーダライタ 135 および IC カード 140 は、上述した図 3 に示すリーダライタ 35 および IC カード 40 に相当するものである。IC カード 140 は、上述した図 4 に示す IC カード 40 と構成を有するもので実現できる。また、IC カード 140 は、上述した図 5 に示す IC カード 40 と同様な処理機能を有し、通信制御装置 101 における認証部の一例として機能する。

[0113] 次に、第 1 の実施形態に係る図 8 に示す構成の通信システム 100 における第 1 の動作例について説明する。

図 10 は、図 8 に示す構成の通信システム 100 における動作例を説明す

るためのシーケンスである。

まず、通信制御装置 101 は、第 1 通信デバイス 111 A がホワイトリストに基づく通常の運用モード（通常通信モード、第 1 の通信モード）で通信を実行し（ステップ S 101）、第 2 通信デバイス 111 B が未通信状態であるものとする（ステップ S 102）。

[0114] 第 1 通信デバイス 111 A のコントローラ 120 は、通常通信モードにおいて、通信データ量、通信速度、通信時間、エラーの検出頻度などの動作状態を監視し、当該第 1 通信デバイスにおける故障または通信障害の有無を検知する（ステップ S 103）。また、コントローラ 120 は、設定されたタイミングで自己診断を実行することにより当該通信デバイス 111 A 内における不具合の有無を検知するようにしても良い。また、各通信デバイス 111 は、不具合を検知する検知器を設け、検知器による検知結果をコントローラ 120 が取得する構成としても良い。

[0115] 第 1 通信デバイス 111 A のコントローラ 120 は、不具合を検知しなければ（ステップ S 103、NO）、通常通信モードでの通信を継続して実行する。また、第 1 通信デバイス 111 A のコントローラ 120 は、通常通信モードで通信を実行中に不具合を検知すると（ステップ S 103、YES）、不具合を示す情報を通信制御管理装置 5 へ送信する。

[0116] 通信制御装置 101 の第 1 通信デバイス 111 A が送信した不具合を示す情報は、通信制御管理装置 5 により取得される（ステップ S 105）。通信制御管理装置 5 の制御部 61 は、通信制御装置 101 の第 1 通信デバイス 111 A からの不具合を示す情報に応じて、当該通信制御装置 101 の第 2 通信デバイス 111 B を通常通信モードとし、第 1 通信デバイス 111 A を未通信状態するように制御する。

[0117] すなわち、第 1 通信デバイス 111 A からの不具合を示す情報を受信すると、通信制御管理装置 5 の制御部 61 は、不具合を示す情報の発信元である通信制御装置 101 の第 2 通信デバイス 111 B に対して通常通信モードへの切替を指示する（ステップ S 106）。この通信制御管理装置 5 からの通

常通信モードへの切替を指示は、不具合を示す情報の発信元である通信制御装置 101 の第 2 通信デバイス 111 B により取得される（ステップ S 107）。これにより、第 2 通信デバイス 111 B のコントローラ 120 は、通信制御管理装置 5 からの通常通信モードへの切替指示に応じて動作モードを通常通信モードに切り替える（ステップ S 108）。

[0118] また、第 1 通信デバイス 111 A からの不具合を示す情報を受信すると、通信制御管理装置 5 の制御部 61 は、不具合を示す情報の発信元である通信制御装置 101 の第 1 通信デバイス 111 A に対して未通信状態となることを指示する（ステップ S 109）。この通信制御管理装置 5 からの未通信状態への切替指示は、不具合を示す情報の発信元である第 1 通信デバイス 111 B により取得される（ステップ S 110）。これにより、第 1 通信デバイス 111 A のコントローラ 120 は、通信制御管理装置 5 からの未通信状態への切替指示に応じて動作モードを未通信状態に切り替える（ステップ S 111）。

[0119] ここで、第 1 通信デバイスと第 2 通信デバイスとの動作モードの切り替えは、通信制御装置 101 としての通信が途切れることが無いように切り替えられる。例えば、通信制御管理装置（デバイス管理サーバ）5 は、第 2 通信デバイス 111 B における通常通信モードへの切り替えが完了した後に第 1 通信デバイス 111 A を未通信状態にするようにする。これにより、通信制御管理装置 5 は、通信制御装置 101 における通信の可用性を確実に確保することができる。

[0120] なお、通信制御装置 101 は、通常通信モードで通信を実行中の一方の通信デバイスに不具合が発生した場合に、他方の通信デバイスで通常通信モードでの通信を実行するように切り替える制御を通信制御装置 101 内で実現するようにしても良い。例えば、通常通信モードで通信を実行中の第 1 通信デバイスが不具合を検知した場合、第 1 通信デバイス 111 A のコントローラ 120 が第 2 通信デバイス 111 B に対して通常通信モードへの切替を要求するようにしても良い。これにより、第 2 通信デバイス 111 B は要求に

応じて通常通信モードで起動し、第1通信デバイス111Aが未通信状態に移移するようにできる。この場合、第1通信デバイスと第2通信デバイスとは互いのアドレスによって通信することが可能である。

[0121] 次に、第1の実施形態に係る通信システムの第2の構成例について説明する。

図11は、第1の実施形態に係る通信システム100'の第2の構成例を示す図である。図11に示す通信システム100'は、図1に示すシステム構成において通信制御装置30を通信制御装置101'に置き換えたものである。また、図11に示す構成例において、通信制御装置101'は、ネットワークNWとクライアント装置10との間に、直列に配置した複数の通信デバイス111C、111Dを有する。

[0122] 図11に示す構成において、通信システム100'における通信制御装置101'以外の各装置は、図1に示す装置と同様な構成で実現することができる。このため、以下、通信制御装置101'以外の各装置の構成については、詳細な説明を省略するものとする。

なお、通信システム100'においては、通信制御装置31についても、通信制御装置101'と同様に、ネットワークNWとサーバ装置20との間に、直列に配置した複数の通信デバイスを具備する構成としても良い。

図12は、第1の実施形態に係る通信システム100'の第2の構成例における通信制御装置101'の構成例を示すブロック図である。

図12に示す構成例において、通信制御装置101'は、複数の通信デバイス111として、直列に配置した第1通信デバイス111Cと第2通信デバイス111Dとを有する。図12に示す例では、通信制御装置101'において、ネットワークNWに接続する第1通信デバイス111Cとクライアント装置10に接続する第2通信デバイス111Dとが直列に接続される。

[0123] また、図12に示す構成例において、通信制御装置101'は、第1通信デバイス111Cと第2通信デバイス111Dとが共用する電源116およびメモリI/F117とを有するものとする。電源116は、図9と同様に

、外部電源に接続され、外部電源からの電力を各通信デバイス111C、111Dへ供給するものである。また、メモリ117は、図9と同様に、メモリカードなどのメモリデバイス118をセットするインターフェースである。

ただし、通信制御装置101'は、通信制御装置30と同様な構成を有する複数の通信デバイスを直列に配置したシステムとして実現しても良い。このようなシステムでは、複数の通信デバイス111'がそれぞれ電源およびメモリ117などの構成を具備するものとして良い。

[0124] 第1通信デバイス111Cおよび第2通信デバイス111Dは、それぞれが上述した図1に示す通信制御装置30と同等の通信処理を実行する構成を有する。すなわち、各通信制御装置101内において、ネットワークNWとクライアント装置10との間に直列に配置された第1通信デバイス111Cおよび第2通信デバイス111Dは、何れか一方が通常通信モード（第1の通信モード）による通信を行い、他方がパススルーモード（第2の通信モード）で通信を行う。

[0125] ここで、パススルーモード（第2の通信モード）は、入力する情報をそのまま通過させて出力する通信モードである。また、通常通信モードは、上述したようにサーバ側の通信制御装置31との相互認証に基づく共通鍵を用いた送受信データの暗号化および復号化を伴う通信を行う動作モードであるものとする。また、本実施形態において、通信制御装置101'は、通常運用モードにおいて、上述したようなホワイトリストにある宛先との通信を許可するホワイトリスト運用モードで通信を実行するものとする。

[0126] なお、通信制御装置101'において直列に設ける第1通信デバイス111Cおよび第2通信デバイス111Dは、それぞれが独立した2つの通信処理のソフトウェアで実現するものであっても良い。この場合、ハードウェアとしては1つの通信デバイスを2つのソフトウェアで実現する並列に配置した2つの通信デバイスとして動作するようにしても良い。

[0127] 各通信デバイス111'（第1通信デバイス111Cおよび111D）は

、自身の故障、不正アクセス、あるいは、マルウェア感染などを検知する機能を有する。例えば、通信デバイス１１１'は、故障、不正アクセス又はマルウェア感染などを示す故障や通信障害などの不具合を示す情報を通信制御管理装置（デバイス管理サーバ）５へ通知する。また、各通信デバイス１１１'は、通信制御管理装置５からの指示に応じて動作モードを切り替える。例えば、各通信デバイス１１１'は、通信制御管理装置５からの指示に応じてパススルーモードから通常通信モードに切り替えたり、通常通信モードからパススルーモードに切り替えたりする。

[0128] 図１２に示すように、各通信デバイス１１１'（１１１Ｃ、１１１Ｄ）は、図９に示す構成と同様に、コントローラ１２０、ブリッジ１３２、ハブ１３３、ブリッジ１３４、リーダライタ１３５およびＩＣカード１４０などを有するものとする。また、コントローラ１２０は、ＭＰＵ１２１、ＲＡＭ１２２、ＳＡＭ１２３およびデータメモリ１２４などを有するものとする。これらの各構成は、図９に示す各構成と同様なもので実現できるため、詳細な説明を省略するものとする。

[0129] 次に、第１の実施形態に係る図１１に示す構成の通信システム１００'における動作例（第２の動作例）について説明する。

図１３は、図１１に示す構成の通信システム１００'における動作例を説明するためのシーケンスである。

まず、通信制御装置１０１'は、第１通信デバイス１１１Ｃがホワイトリストに基づく通常の運用モード（通常通信モード）で通信を実行し（ステップＳ１２１）、第２通信デバイス１１１Ｄがパススルーモードで動作するものとする（ステップＳ１２２）。

[0130] 第１通信デバイス１１１Ｃのコントローラ１２０は、通常通信モードにおいて、通信データ量、通信速度、通信時間、エラーの検出頻度などの動作状態を監視し、当該第１通信デバイスにおける故障または通信障害の有無を検知する（ステップＳ１２３）。また、コントローラ１２０は、設定されたタイミングで自己診断を実行することにより当該通信デバイス１１１Ａ内にお

ける不具合の有無を検知するようにしても良い。また、各通信デバイス 111 は、不具合を検知する検知器を設け、検知器による検知結果をコントローラ 120 が取得する構成としても良い。

[0131] 第 1 通信デバイス 111 C のコントローラ 120 は、不具合を検知しなければ（ステップ S 123、NO）、通常通信モードでの通信を継続して実行する。また、第 1 通信デバイス 111 C のコントローラ 120 は、通常通信モードで通信を実行中に不具合を検知すると（ステップ S 123、YES）、不具合を示す情報を通信制御管理装置 5 へ通知する（ステップ S 124）。

[0132] 通信制御装置 101' の第 1 通信デバイス 111 C が通知する不具合を示す情報は、通信制御管理装置 5 により取得される（ステップ S 125）。通信制御管理装置 5 の制御部 61 は、通信制御装置 101' の第 1 通信デバイス 111 C からの不具合を示す情報に応じて、当該通信制御装置 101' の第 2 通信デバイス 111 D を通常通信モードとし、第 1 通信デバイス 111 C をパススルーモードとするように制御する。

[0133] すなわち、第 1 通信デバイス 111 C からの不具合を示す情報を受信すると、通信制御管理装置 5 の制御部 61 は、不具合を示す情報の発信元である通信制御装置 101' の第 2 通信デバイス 111 D に対して通常通信モードへの切替を指示する（ステップ S 126）。この通信制御管理装置 5 からの通常通信モードへの切替を指示は、不具合を示す情報の発信元である通信制御装置 101' における第 2 通信デバイス 111 D により取得される（ステップ S 127）。これにより、第 2 通信デバイス 111 D のコントローラ 120 は、通信制御管理装置 5 からの通常通信モードへの切替指示に応じて動作モードを通常通信モードに切り替える（ステップ S 128）。

[0134] また、第 1 通信デバイス 111 C からの不具合を示す情報を受信すると、通信制御管理装置 5 の制御部 61 は、不具合を示す情報の発信元である通信制御装置 101' の第 1 通信デバイス 111 C に対してパススルーモードとなることを指示する（ステップ S 129）。この通信制御管理装置 5 からの

パススルーモードへの切替指示は、不具合を示す情報の発信元である第1通信デバイス111Cにより取得される（ステップS130）。これにより、第1通信デバイス111Cのコントローラ120は、通信制御管理装置5からのパススルーモードへの切替指示に応じて動作モードをパススルーモードに切り替える（ステップS131）。

[0135] 以上のような第1の実施形態に係る通信システムによれば、通信制御装置において複数の通信デバイスを設けた冗長構成とする。これにより、第1の実施形態によれば、ネットワークを介したデータ通信におけるセキュリティ性を確保するための通信制御装置に故障や通信障害が発生しても通信が途切れることなく継続することができるような確実な可用性をもった通信の運用を実現できる。

[0136] （第2の実施形態）

次に、第2の実施形態に係る通信システムについて説明する。

図14は、第2の実施形態に係る通信システム200の構成例を示す図である。図14に示す通信システム200は、図1に示すシステム構成においてクライアント側の通信制御装置30を通信制御装置201に置き換えたものである。また、図14に示す構成例において、通信制御装置201は、ネットワークNWとクライアント装置10との間に、分散制御器212Aおよび212Bを介して並列に配置した複数の通信デバイス211A、211B、211Cを有する。

[0137] 図14に示す構成において、通信システム200における通信制御装置201以外の各装置は、図1に示す装置と同様な構成で実現することができる。このため、通信制御装置200以外の構成については、詳細な説明を省略するものとする。

なお、通信システム200においては、サーバ側の通信制御装置31についても、通信制御装置201と同様に、ネットワークNWとサーバ装置20との間に、分散制御器を介して並列に配置した複数の通信デバイスを具備する構成としても良い。

[0138] 図15は、第2の実施形態に係る通信システム200の構成例における通信制御装置201の構成例を示すブロック図である。

図15に示す構成例において、通信制御装置201は、複数の通信デバイス211として並列に配置した3つの通信デバイス211A、211B、211Cを有する。複数の通信デバイス211A～211Cは、通信制御装置201において、ネットワークNWに接続する分散制御器212Aとクライアント装置10に接続する分散制御器212Bとの間に並列に接続する。複数の通信デバイス211A～211Cは、それぞれが上述した図1に示す通信制御装置30と同等の通信処理を実行する構成を有する。また、分散制御器212A、212Bは、通信処理の負荷を複数の通信デバイス211A～211Cに分散する制御を行う。したがって、暗号化復号処理や、証明書による相互認証処理も、それぞれの通信デバイス211A～211Cが有するコントローラが処理を行うことができる。

[0139] また、図15に示す構成例において、通信制御装置201は、複数の通信デバイス211A～211C、分散制御器212A、212Bが共用する電源216を有する。また、通信制御装置201は、複数の通信デバイス211A～211Cが共用するおよびメモリI/F217も有する。電源216は、外部電源に接続され、外部電源からの電力を各通信デバイス211A～211Cおよび分散制御器212A、212Bへ供給する。メモリI/F217は、メモ리카ードなどのメモリデバイス218をセットするインターフェースである。例えば、メモリI/F217には、各通信デバイス211に対する設定情報などを記憶したメモリデバイス218がセットされる。

[0140] なお、第2の実施形態に係る通信制御装置201において、並列に配置される通信デバイス211の個数は、3個に限定されるものではなく、複数であれば良い。また、通信制御装置201において、並列に配置される各通信デバイス211は、同内容の通信処理を行うものであれば良く、処理能力が異なるものであっても良い。さらには、通信制御装置201において、並列に配置される各通信デバイス211は、処理能力が異なるもの置き換えても良

い。

[0141] また、第2の実施形態に係る通信制御装置201は、通信制御装置30と同様な構成を有する複数の通信デバイスを2つの分散制御器212A、212B間に並列に配置した分散デバイスシステムとして実現しても良い。この場合、分散デバイスシステムを構成する各通信デバイスは、それぞれ電源およびメモリI/Fなどを具備し、独立して動作することができる装置として構成されるものとして良い。

[0142] 各通信デバイス211(211A~211C)は、図15に示すように、コントローラ220、ブリッジ232、ハブ233、ブリッジ234、リーダライタ235およびICカード240を有する。

コントローラ220は、通信デバイス211を制御するものである。図15に示す構成例において、コントローラ220は、MPU221、RAM222、SAM223およびデータメモリ224などを有する。

[0143] MPU221は、コントローラ220の制御を司るプロセッサの一例である。MPU221は、データメモリ224などに記憶したプログラムを実行することで種々の処理を実現する。例えば、コントローラ220は、MPU221がプログラムを実行することにより、通信制御、故障検知、通信障害の検知、通信状態の監視、自己診断、および、ログ情報の収集などの処理を実行する。

[0144] また、コントローラ220は、MPU221がプログラムを実行することにより、サーバ側の通信制御装置31との相互認証処理、クライアント装置10からネットワークNWへ送出するデータの暗号化処理、ネットワークNWを経由してクライアント装置へ送信される暗号化されたデータの復号化処理などを行うようにしても良い。また、コントローラ220は、相互認証処理、暗号化処理および復号化処理の少なくとも何れか1つをICカード240に対して依頼するようにして良い。

[0145] RAM222は、ランダムアクセスメモリである。RAM222は、作業用のデータを保持するワーキングメモリとして機能する。SAM223は、

シリアルアクセスメモリである。データメモリ 224 は、書き換え可能な不揮発性のメモリである。

データメモリ 224 は、プログラムおよび設定情報などを記憶する。例えば、データメモリ 224 は、通信を許可する宛先のリストを示すホワイトリストを記憶する。コントローラ 220 は、データメモリ 224 に記憶するホワイトリストを参照して通常通信モード（第 1 の通信モード）での通信を実行する。また、データメモリ 224 は、当該通信デバイスの動作状態を示すログ情報を記憶するようにしても良い。また、データメモリ 224 は、当該通信デバイスにおける通信量を示す情報を記憶するようにしても良い。また、データメモリ 224 は、ログデータの分析などによる自己診断処理などを実行したりする。

[0146] ブリッジ 232、234 は、通信インターフェース（通信部）として機能する。ブリッジ 232 および 234 は、ハブ 233 を介してコントローラ 220 に接続される。

ブリッジ 232 は、通信デバイス 211 におけるネットワーク NW 側の通信を実行する。ブリッジ 232 は、図 3 に示す NW 通信部 32 としての通信を実現する。ブリッジ 232 は、ネットワーク NW から受信するデータをハブ 233 を介してコントローラ 220 へ供給する。また、ブリッジ 234 は、コントローラ 220 または IC カード 240 で暗号化したデータをネットワーク NW へ送出する。

[0147] ブリッジ 234 は、通信デバイス 211 におけるクライアント装置 10 側の通信を実行する。ブリッジ 234 は、図 3 に示す装置通信部 34 としての通信を実現する。ブリッジ 234 は、クライアント装置 10 からのデータをハブ 233 を介してコントローラ 220 へ供給する。また、ブリッジ 234 は、ネットワーク NW からの暗号化されたデータをコントローラ 220 または IC カード 240 で復号化したデータをクライアント装置 10 へ送出する。

[0148] リーダライタ 235 および IC カード 240 は、上述した図 3 に示すリー

ドライタ 35 および IC カード 40 に相当するものである。IC カード 240 は、上述した図 4 に示す IC カード 40 と構成を有するもので実現できる。また、IC カード 240 は、上述した図 5 に示す IC カード 40 と同様な処理機能を有し、通信制御装置 201 における認証部の一例として機能する。

[0149] 各分散制御器 212 (212A、212B) は、図 15 に示すように、コントローラ 251、メモリ 252、ハブ 253 およびインターフェース (I/F) 254 を有する。

コントローラ 251 は、分散制御器 212 を制御するものである。コントローラ 251 は、プロセッサおよび各種のメモリなどを有する。コントローラ 251 においては、プロセッサがプログラムを実行することで種々の処理を実現する。例えば、コントローラ 251 は、プロセッサがプログラムを実行することにより各通信デバイス 211A~211C への通信負荷の分散制御を行う。

[0150] メモリ 252 は、設定情報などを記憶する。例えば、メモリ 252 は、通信負荷の分散を判断するための閾値などを記憶する。コントローラ 251 は、メモリ 252 に記憶した閾値などの設定情報に基づいて通信負荷に応じて複数の通信デバイスから通信処理を実行させる通信デバイスを決定する。

ハブ 253 は、ネットワーク NW またはクライアント装置 10 と複数の通信デバイス 211A~211C とを接続させるインターフェースである。ハブ 253 は、コントローラ 251 によって接続先する通信デバイスが制御される。

[0151] インターフェース 254 は、設定情報などを取得するためのインターフェースである。閾値などの設定情報を通信制御管理装置 (デバイス管理サーバ) 5 から取得する運用形態とする場合、インターフェース 254 は、通信制御管理装置 5 と通信するための通信部として構成される。また、インターフェース 254 は、閾値などの設定情報を記憶したメモリカードなどのメモリデバイスから情報を読み取るメモリリーダで構成しても良い。また、インタ

ーフェース 254 は、閾値などの設定情報を供給する外部装置を接続するためのインターフェースであっても良い。

[0152] 次に、第2実施形態に係る図14及び図15に示す構成の通信システム200の動作例について説明する。

図16は、図14及び図15に示す構成の通信システム200における分散制御器212（212A、212B）の動作例を説明するためのフローチャートである。

まず、分散制御器212は、インターフェース254などにより入力される複数の通信デバイス211A～211Cによる分散処理のための設定情報を受け付ける（S201）。分散処理のための設定情報を取得した場合（ステップS201、YES）、分散制御器212（212A又は212B）のコントローラ251は、入力される設定情報に基づいて複数の通信デバイス211A～211Cによる分散処理を決定するための閾値を設定する（ステップS202）。ここでは、1つの通信制御装置201において並列に配置される通信デバイスが3つである場合を想定するものとし、コントローラ251は、第1閾値と第2閾値とをメモリ252に保存するものとする。

[0153] 例えば、第1閾値は、通信処理を1つの通信デバイスで実施するか否かを判定するための通信制御装置201全体での処理の負荷に対する判定基準値である。分散制御器212のコントローラ251は、通信制御装置201全体での処理の負荷が第1閾値未満であれば1つの通信デバイスで通信処理を実行し、第1閾値以上であれば複数の通信デバイスで分散して通信処理を実行するものとする。

[0154] さらに、第2閾値は、通信処理を3つの通信デバイスで実施するか否かを判定するための通信制御装置201全体での処理の負荷に対する判定基準値である。分散制御器212のコントローラ252は、通信制御装置201全体での処理の負荷が第2閾値以上であれば3つの通信デバイスで分散して通信処理を実行し、第1閾値以上かつ第2閾値未満であれば2つの通信デバイスで分割して通信処理を実行するものとする。分散処理を実施するための設

定情報としての閾値は、適宜設定できるようにしても良い。

[0155] また、分散制御器 2 1 2 A、2 1 2 B のコントローラ 2 5 1 は、通信量などに基づく通信デバイスにおける処理の負荷を監視する（ステップ S 2 0 3）。例えば、ネットワーク NW 側から入力する情報に対して通信デバイス 2 1 1 が復号化処理を実行するため、分散制御器 2 1 2 A のコントローラ 2 5 1 は、ネットワーク NW 側から入力するデータ量を処理の負荷として監視する。また、クライアント装置 1 0 から入力する情報に対しては通信デバイス 2 1 1 が暗号化処理を実行するため、分散制御器 2 1 2 B のコントローラ 2 5 1 は、クライアント装置 1 0 から入力するデータ量を処理の負荷として監視する。

[0156] 分散制御器 2 1 2 のコントローラ 2 5 1 は、監視している処理の負荷が第 1 閾値未満であれば（ステップ S 2 0 4、YES）、1 つの通信デバイス 2 1 1 により通信処理を実行させる（ステップ S 2 0 5）。

例えば、複数の通信デバイスが動作している状態であれば、コントローラ 2 5 1 は、監視している処理の負荷が第 1 閾値未満となった場合に 1 つの通信デバイスだけで通信を実行し、通信を実行しない通信デバイスを未通信状態（スリープ状態）へ遷移させる。

これにより、分散制御器 2 1 2 は、処理の負荷が第 1 閾値未満である場合に、1 つの通信デバイスだけで通信処理を実行し、その他の通信デバイスを未通信状態とすることで無駄な電力消費を抑制できる。

[0157] また、分散制御器 2 1 2 のコントローラ 2 5 1 は、監視している処理の負荷が第 1 閾値以上であれば（ステップ S 2 0 4、NO）、処理の負荷が第 2 閾値未満であるかを判定する（ステップ S 2 0 6）。コントローラ 2 5 1 は、処理の負荷が第 1 閾値以上かつ第 2 閾値未満である場合（ステップ S 2 0 6、YES）、2 つの通信デバイスに分散して通信処理を実行させる（ステップ S 2 0 7）。

[0158] 例えば、1 つの通信デバイス 2 1 1 A だけが動作している状態であれば、コントローラ 2 5 1 は、監視している処理の負荷が第 1 閾値以上かつ第 2 閾

値未満となった場合、2つの目の通信デバイス211Bを通信可能な状態とする。通信デバイス211Aに加えて通信デバイス211Bが通信可能な状態となると、コントローラ251は、ハブ253から出力する情報を通信デバイス211Aと通信デバイス211Bとへ振り分ける。

[0159] これにより、分散制御器212は、処理の負荷が第1閾値以上かつ第2閾値未満である場合に2つの通信デバイスで分散して処理を実行することができる。この結果として、分散制御器212は、処理が負荷に応じて動作させる複数の通信デバイスで分散して通信処理を実行でき、処理能力の不足によってデータ遅延などが発生することを防止できる。

[0160] また、分散制御器212のコントローラ251は、監視している処理の負荷が第2閾値以上であれば（ステップS206、NO）、3つの通信デバイスに分散して通信処理を実行させる（ステップS208）。例えば、2つの通信デバイス211A及び211Bが動作している状態であれば、コントローラ251は、監視している処理の負荷が第2閾値以上となった場合、3つの目の通信デバイス211Aを通信可能な状態とする。通信デバイス211A及び211Bに加えて通信デバイス211Cが通信可能な状態となると、コントローラ251は、ハブ253から出力する情報を通信デバイス211Aと通信デバイス211Bと通信デバイス211Cへ振り分ける。

[0161] これにより、分散制御器212は、処理の負荷が第2閾値以上である場合に3つの通信デバイス（最大数の通信デバイス）で分散して処理を実行することができる。この結果として、分散制御器212は、処理が負荷に応じて動作させる複数の通信デバイスで分散して通信処理を実行でき、処理能力の不足によってデータ遅延などが発生することを防止できる。

[0162] なお、上述した動作例は、複数の通信デバイスが正常に動作することを前提して説明したものであるが、分散制御器は、各通信デバイスにおける故障あるいは通信障害などの不具合を検知し、不具合が発生した通信デバイス以外で上述した分散制御を行うようにしても良い。また、全ての通信デバイスにおいて不具合が発生した場合には、分散制御器は、何れかの1つの通信デ

バイスをパススルーモードとして動作させてデータ通信を確実に継続させるようにしても良い。

[0163] また、上述した通信制御装置は、同等な複数の通信デバイスを並列に配置するものとしたが、処理能力が異なる複数の通信デバイスを並列に配置するようにしても良い。また、1つの通信デバイスをメインの処理デバイスとし、それ以外の通信デバイスをスレーブの処理デバイスとしてメインの通信デバイスの処理を補助するような運用としても良い。さらに、通信デバイスが実施する処理内容を分けて実施するようにしても良い。

[0164] 以上のように、第2実施形態に係る通信システムは、ネットワークとクライアント装置との間に分散制御器を介して複数の通信デバイスを並列に配置した通信制御装置を有する。分散制御器は、通信制御装置における処理の負荷を監視し、処理の負荷に応じた台数の通信デバイスで通信処理を分散して実行する。

[0165] これにより、1つの通信デバイスの最大通信許容量を超えたデータの通信を行う場合であっても、通信制御装置としてデータ遅延を起こす確率を減らすことができる。また、処理の負荷に応じた台数の通信デバイスで通信を実行するように制御するため、負荷が少ない状態で多数の通信デバイスを起動させることがなく、省電力化を図ることもできる。

[0166] (第3の実施形態)

次に、第3の実施形態に係る通信システムについて説明する。

図17は、第3の実施形態に係る通信システム300および通信制御装置301の構成例を示す図である。図17に示す通信システム300は、図1に示すシステム構成においてクライアント側の通信制御装置30を通信制御装置301に置き換えたものである。ただし、通信システム300において、ネットワークNWとサーバ装置20との間に配置されるサーバ側の通信制御装置31についても、通信制御装置301と同様の構成を有するものとして良い。なお、図17に示す構成において、通信システム300における通信制御装置301以外の各装置は、図1に示す装置と同様な構成で実現する

ことができるため、詳細な説明を省略するものとする。

[0167] 図17に示す構成例において、通信制御装置301は、電源316、メモリI/F317、コントローラ320、ブリッジ332、ハブ333、ブリッジ334、リーダーライタ335、ICカード340などを有する。

コントローラ320は、通信デバイス211を制御するものである。図17に示す構成例において、コントローラ320は、MPU321、RAM322、SAM323およびデータメモリ324などを有する。

[0168] MPU321は、コントローラ320の制御を司るプロセッサの一例である。MPU321は、データメモリ324などに記憶したプログラムを実行することで種々の処理を実現する。例えば、コントローラ320は、MPU321がプログラムを実行することにより、通信制御、故障検知、通信障害の検知、通信量の分析、自己診断、ログ情報の保存およびログ情報の送信などの処理を実行する。

[0169] また、コントローラ320は、MPU321がプログラムを実行することにより、サーバ側の通信制御装置31との相互認証処理、クライアント装置10からネットワークNWへ送出するデータの暗号化処理、ネットワークNWを経由してクライアント装置10へ送信される暗号化されたデータの復号化処理などを行うようにしても良い。また、コントローラ320は、相互認証処理、暗号化処理および復号化処理の少なくとも何れか1つをICカード340に対して依頼するようにして良い。

[0170] RAM322は、ランダムアクセスメモリである。RAM322は、作業用のデータを保持するワーキングメモリとして機能する。SAM323は、シリアルアクセスメモリである。データメモリ324は、書き換え可能な不揮発性のメモリである。

データメモリ324は、プログラムおよび設定情報などを記憶する。例えば、データメモリ324は、通信を許可する宛先のリストを示すホワイトリストを記憶する。コントローラ320は、データメモリ324に記憶するホワイトリストを参照して通常通信モード（第1の通信モード）での通信を実

行する。また、データメモリ 324 は、当該通信制御装置の動作状態を示すログ情報を記憶するようにしても良い。また、データメモリ 324 は、コントローラ 320 による当該通信制御装置における通信量の分析情報を記憶する。

[0171] ブリッジ 332、334 は、通信インターフェース（通信部）として機能する。ブリッジ 332 および 334 は、ハブ 333 を介してコントローラ 320 に接続される。

ブリッジ 332 は、通信制御装置 301 におけるネットワーク NW 側の通信を実行する。ブリッジ 332 は、図 3 に示す NW 通信部 32 としての通信を実現する。ブリッジ 332 は、ネットワーク NW から受信するデータをハブ 333 を介してコントローラ 320 へ供給する。また、ブリッジ 334 は、コントローラ 320 または IC カード 340 で暗号化したデータをネットワーク NW へ送出する。

[0172] ブリッジ 334 は、通信制御装置 301 におけるクライアント装置 10 側の通信を実行する。ブリッジ 334 は、図 3 に示す装置通信部 34 としての通信を実現する。ブリッジ 334 は、クライアント装置 10 からのデータをハブ 333 を介してコントローラ 320 へ供給する。また、ブリッジ 334 は、ネットワーク NW からの暗号化されたデータをコントローラ 320 または IC カード 340 で復号化したデータをクライアント装置 10 へ送出する。

[0173] リーダライタ 335 および IC カード 340 は、上述した図 3 に示すリーダライタ 35 および IC カード 40 に相当するものである。IC カード 340 は、上述した図 4 に示す IC カード 40 と構成を有するもので実現できる。また、IC カード 340 は、上述した図 5 に示す IC カード 40 と同様な処理機能を有し、通信制御装置 301 における認証部の一例として機能する。

[0174] また、電源 316 は、外部電源に接続され、外部電源からの電力を当該通信制御装置 301 内の各部へ供給する。メモリ I/F 317 は、メモリーカー

ドなどのメモリデバイス318をセットするインターフェースである。例えば、メモリ1/F317には、通信制御装置301に対する設定情報などを記憶したメモリデバイス318がセットされる。

[0175] 次に、第3実施形態に係る図17に示す構成の通信システム300の動作例について説明する。

図18は、図17に示す通信システム300における第1の動作例を説明するためのシーケンスである。

まず、通信制御装置301は、通常の運用において通信量を含むログ情報を蓄積する。例えば、通信制御装置301のコントローラ320は、通信インターフェースとしてのブリッジ332および334を通過するデータを監視することにより、当該通信制御装置301の通信量を示す情報をデータメモリ324に保存する。

[0176] 通信制御装置301のコントローラ320は、データメモリ324にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ324に記憶する（ステップS301）。例えば、コントローラ320は、所定の周期で通信量の分析を行って通信量の分析情報をデータメモリ324に記録する。通信量の分析情報は、例えば、時間当たりの通信量を示すものであっても良いし、時間帯ごとの通信量および通信量の増減傾向などを示すものであっても良いし、通信量が所定閾値未満となる時間帯あるいは通信量が最小となる時間帯を示す情報でも良い。第3の実施形態においては、通信量の分析情報は、当該通信制御装置301が自己診断を実施する時刻を決めるための情報であれば良い。

[0177] 通信制御装置301のコントローラ320は、データメモリ324に記憶した通信量の分析情報を通信制御管理装置（デバイス管理サーバ）5へ送信する（ステップS302）。コントローラ320は、例えば、所定のタイミングで通信量の分析情報を送信するようにしても良いし、通信制御管理装置5からの要求に応じて送信するようにしても良い。また、コントローラ320は、当該通信制御管理装置5における通信量が少ない時間帯を自己判断し

、通信量が少ないと判断した時間帯に通信量の分析情報を通信制御管理装置 5 へ送信するようにしても良い。

[0178] 通信制御装置 301 から送信される通信量の分析情報は、通信制御管理装置 5 に取得される（ステップ S303）。通信制御管理装置 5 の制御部 61 は、NW通信部 60 により受信した通信量の分析情報を送信元の通信制御装置 301 を示す識別情報に対応づけて記憶部 66 に記憶する。制御部 61 は、受信した通信量の分析情報に基づいて当該通信制御装置 301 が自己診断を実行すべき時刻または時間帯を決定する（ステップ S304）。例えば、制御部 301 は、通信量の分析情報に基づいて通信量が所定閾値未満となる時間帯のうち自己診断処理の要する時間が確保できる時刻を自己診断の実施時刻（実施予定時刻）として特定する。また、夜中等、長時間通信量が低くなるような使用状況下においては、所定閾値未満であるかどうかにかかわらず、自己診断処理の要する時間が確保できる時刻を自己診断の実施時刻（実施予定時刻）として特定してもよい。

[0179] 自己診断の実施時刻を決定した後、制御部 61 は、自己診断の実施時刻になると、当該通信制御装置 301 に対して生死確認クエリを送信する（ステップ S305）。生死確認クエリは、正常に動作中であるか否かの応答を要求するものである。通信制御装置 301 のコントローラ 320 は、通信制御管理装置 5 からの生死確認クエリを受信すると（ステップ S306）、正常動作中であれば正常であることを示す応答を送信する（ステップ S307）。また、通信制御装置 301 は、生死確認クエリに対して前回の自己診断を実施した日時などを応答するようにしても良い。

[0180] 通信制御管理装置 5 の制御部 61 は、通信制御装置 301 からの応答に基づいて自己診断を実施させるか否かを判断する（ステップ S308）。例えば、制御部 61 は、通信制御装置から応答がない場合、あるいは、前回の自己診断を実施したに日時から所定期間以上経過している場合、当該通信制御装置 301 に自己診断を実施させるものと判断する。また、制御部 61 は、通信制御装置 301 からの応答内容にかかわらず、自己診断を実施させるよ

うにしても良い。自己診断を実施させる場合、通信制御管理装置5の制御部61は、当該通信制御装置301に対して自己診断の実施を要求する（ステップS309）。

[0181] 通信制御管理装置5のコントローラ320は、通信制御管理装置5からの自己診断の実施要求を受信すると、現在、自身が自己診断を実施できる状況であるかを判断する（ステップS311）。例えば、コントローラ320は、現在の通信量が所定の閾値未満であれば自己診断を実施するものとする。

[0182] これは、通信制御管理装置5が指定する自己診断の実施時刻は、過去の通信量（通信量の分析情報）に基づくものであって、実際には設定した時刻に通信量が多い可能性があるためである。第3実施形態に係るシステムは、通信制御装置や通信システム全体にできるだけ、負荷をかけずに自己診断を実行させるための制御を行うものである。このため、通信制御装置のコントローラは、実際の通信量が多くなっている場合には自己診断を実施しない（延期する）と判断するものとする。

[0183] 自己診断を実施する場合（ステップS311、YES）、コントローラ320は、自己診断を実施し（ステップS312）、自己診断の実行結果を示す情報を通信制御管理装置5へ送信する。この場合、自己診断の実行結果を示す情報は、通信制御装置301から送信され、通信制御管理装置5が取得する（ステップS313）。

また、自己診断を実施しない場合（ステップS311、NO）、コントローラ320は、自己診断を実施していないことを示す通知を通信制御管理装置5へ送信する（ステップS314）。この場合、自己診断を実施していないことを示す通知が、自己診断の実施要求に対する応答として通信制御管理装置5により取得される（ステップS315）。

[0184] 自己診断の実施要求に対する結果を取得すると、通信制御管理装置5の制御部61は、自己診断の結果を記憶部66に保存する（ステップ316）。例えば、通信制御装置30で自己診断が実施された場合、制御部61は、自己診断の実行結果を示す情報を実施日時と共に当該通信制御装置301の識

別情報に対応づけて記憶部 66 に記憶する。また、通信制御装置 30 で自己診断が実施されなかった場合、制御部 61 は、自己診断が実施できなかった旨の情報を当該通信制御装置 301 の識別情報に対応づけて記憶部 66 に記憶する。

[0185] また、通信制御管理装置 5 の制御部 61 は、取得した自己診断の実行結果に対して異常の有無を検証する。自己診断の実行結果から異常と判断される項目がある場合（ステップ S317、YES）、制御部 61 は、通信制御装置 301 または通信システム 300 に異常があることを示すアラートを報知する（ステップ S318）。また、生死確認クエリに対して通信制御装置 301 から応答がない場合も、制御部 61 は、通信制御装置 301 または通信システム 300 に異常があることを報知するようにしても良い。

[0186] 以上のように、第 3 実施形態の第 1 の動作例では、通信制御装置における通信量の分析情報を通信制御管理装置が取得し、通信制御管理装置が通信量の分析情報に基づいて通信制御装置に自己診断を実施させる時刻を設定する。

これにより、通信制御管理装置は、通信制御装置に対して、通信量が少なく、自己診断を行っても通常の通信処理に影響がない時間に自己診断を実施させることができる。この結果として、通信制御装置の状態を確認したり、故障や通信障害などを早期に発見したりするための自己診断を本来の通信システムに負荷をかけずに効率よく実施させることができる。

[0187] 次に、第 3 の実施形態に係る通信システム 300 の第 2 の動作例について説明する。

図 19 は、図 17 に示す通信システム 300 における第 2 の動作例を説明するためのシーケンスである。

通信制御装置 301 のコントローラ 320 は、上述した第 1 の動作例と同様に、データメモリ 324 にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ 324 に記憶する（ステップ S321）。

[0188] 通信制御装置 301 のコントローラ 320 は、所定のタイミングでデータメモリ 324 に記憶した通信量の分析情報に基づいて自己診断を実行する予定の実施予定時刻を決定する（ステップ S322）。例えば、コントローラ 320 は、通信量の分析情報に基づいて通信量が所定閾値未満となる時間帯のうち自己診断処理の要する時間が確保できる時刻を自己診断の実施時刻（実施予定時刻）として特定する。

[0189] 自己診断の実施予定時刻を決定した場合、コントローラ 320 は、自己診断の実施予定時刻を通信制御管理装置 5 へ通知する（S323）。この場合、通信制御管理装置 5 の制御部 61 は、通信制御装置 301 から通知される自己診断の実施予定時刻を示す情報を当該通信制御装置 301 の識別情報に対応づけて記憶しておくようにしても良い。ただし、コントローラ 320 は、自己診断の実施予定時刻を通信制御管理装置 5 へ通知しなくても良い。

[0190] 自己診断の実施予定時刻を決定した後、制御部 61 は、自己診断の実施予定時刻になると、自身が自己診断を実施できる状況であるかを判断する（ステップ S324）。例えば、コントローラ 320 は、現在の通信量が所定の閾値未満であれば自己診断を実施する。

自己診断を実施する場合（ステップ S324、YES）、コントローラ 320 は、自己診断を実施し（ステップ S325）、自己診断の実行結果を示す情報を通信制御管理装置 5 へ送信する。自己診断の実行結果を示す情報は、通信制御装置 301 から送信され、通信制御管理装置 5 が取得する（ステップ S326）。

また、自己診断を実施しない場合（ステップ S324、NO）、コントローラ 320 は、自己診断を実施していないことを示す通知を通信制御管理装置 5 へ送信する（ステップ S327）。この場合、自己診断を実施していないことを示す通知が、自己診断の実施要求に対する応答として通信制御管理装置 5 により取得される（ステップ S328）。

[0191] 自己診断の実施要求に対する結果を取得すると、通信制御管理装置 5 の制御部 61 は、自己診断の結果を記憶部 66 に保存する（ステップ 329）。

また、通信制御装置 30 で自己診断が実施されなかった場合、制御部 61 は、自己診断が実施できなかった旨の情報を当該通信制御装置 301 の識別情報に対応づけて記憶部 66 に記憶する。

[0192] また、通信制御管理装置 5 の制御部 61 は、取得した自己診断の実行結果に対して異常の有無を検証する（ステップ S 330）。自己診断の実行結果から異常と判断される項目がある場合（ステップ S 330、YES）、制御部 61 は、通信制御装置 301 または通信システム 300 に異常があることを示すアラートを報知する（ステップ S 331）。

[0193] 以上のように、第 3 実施形態の第 2 の動作例では、通信制御装置自身が通信量の分析情報に基づいて自己診断を実施する予定時刻を設定する。これにより、通信制御装置は、通信量が少なく自己診断を行っても通常の通信処理に影響がない時間に自己診断を実施するように計画することができる。この結果として、通信制御管理装置が通信制御装置の状態を確認したり故障や通信障害などを早期に発見したりするための自己診断を通信システムに負荷をかけずに効率よく実施させることができる。

[0194] （第 4 の実施形態）

次に、第 4 の実施形態に係る通信システムについて説明する。

第 4 の実施形態に係る通信システムは、上述した第 3 の実施形態に係る通信システム 300 と同様な構成を有するものとする。従って、第 4 の実施形態については、第 3 の実施形態で説明した図 17 に示す通信システム 300 に適用する例として説明する。

[0195] 以下、第 4 実施形態に係る通信システム 300 の動作例として第 1 ～第 4 の動作例について説明する。

図 20 は、第 4 の実施形態に係る通信システム 300 における第 1 の動作例を説明するためのシーケンスである。

まず、通信制御装置 301 は、動作状態を示すログ情報をデータメモリ 324 に蓄積する。ここで、データメモリ 324 に蓄積するログ情報は、通信制御装置 301 の動作履歴を示す情報である。ただし、不正アクセスなどの

緊急に通信制御管理装置 5 へ通知すべき情報は、ログ情報として保存しても良いが、直ちに通信制御管理装置 5 へ通知される。

[0196] また、通常の運用における通信量を示す情報は、ログ情報としてデータメモリ 324 に蓄積するようにしても良い。例えば、通信制御装置 301 のコントローラ 320 は、通信インターフェースとしてのブリッジ 332 および 334 を通過するデータを監視することにより、当該通信制御装置 301 の通信量を示す情報をデータメモリ 324 に保存する。

[0197] 通信制御装置 301 のコントローラ 320 は、データメモリ 324 にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ 324 に記憶する（ステップ S401）。例えば、コントローラ 320 は、所定の周期で通信量の分析を行って通信量の分析情報をデータメモリ 324 に記録する。通信量の分析情報は、例えば、時間当たりの通信量を示すものであっても良いし、時間帯ごとの通信量および通信量の増減傾向などを示すものであっても良いし、通信量が所定閾値未満となる時間帯あるいは通信量が最小となる時間帯を示す情報でも良い。第 4 の実施形態において、通信量の分析情報は、当該通信制御装置 301 がログ情報を通信制御管理装置（デバイス管理サーバ）5 へ送信する時刻を決めるための情報であれば良い。

[0198] 通信制御装置 301 のコントローラ 320 は、データメモリ 324 に記憶した通信量の分析情報を通信制御管理装置（デバイス管理サーバ）5 へ送信する（ステップ S402）。コントローラ 320 は、例えば、所定のタイミングで通信量の分析情報を送信するようにしても良いし、通信制御管理装置 5 からの要求に応じて送信するようにしても良い。また、コントローラ 320 は、当該通信制御管理装置 5 における通信量が少ない時間帯を自己判断し、通信量が少ないと判断した時間帯に通信量の分析情報を通信制御管理装置 5 へ送信するようにしても良い。

[0199] 通信制御装置 301 から送信される通信量の分析情報は、通信制御管理装置 5 に取得される（ステップ S403）。通信制御管理装置 5 の制御部 61

は、NW通信部60により受信した通信量の分析情報を送信元の通信制御装置301を示す識別情報に対応づけて記憶部66に記憶する（ステップS404）。制御部61は、記憶部66に記憶した各通信制御装置301からの通信量の分析情報に基づいて、各通信制御装置301がログ情報を送信するスケジュール（ログ収集のスケジュール）を決定する（ステップS405）。例えば、制御部301は、当該通信システムにおける各通信制御装置からの通信量の分析情報に基づいて、ネットワークNW全体における通信量が所定閾値未満となるように、各通信制御装置301がログ情報を送信できる時刻（時間帯）をスケジューリングする。

[0200] ログ収集のスケジュールを作成すると、制御部61は、個々の通信制御装置301に対してログ情報を送信する時刻（送出時刻）を通知する（ステップS406）。通信制御装置301のコントローラ320は、通信制御管理装置5からログ情報の送出時刻の通知を受信すると（ステップS407）、ログ情報の送出時刻をデータメモリ324に記憶する（ステップS408）。コントローラ320は、通信制御管理装置5から指示されたログ情報の送出時刻になると、データメモリ324に蓄積したログ情報を通信制御管理装置5へ送信する（ステップS409）。

[0201] 通信制御装置301から送信されるログ情報は、ネットワークNWを経由して通信制御管理装置5へ伝送され、通信制御管理装置5に受信される（ステップS410）。通信制御管理装置5の制御部61は、通信制御装置301から受信したログ情報を記憶部66に保存する（ステップ411）。例えば、制御部61は、受信したログ情報を実施日時と共に当該通信制御装置301の識別情報に対応づけて記憶部66に記憶する。

[0202] 上述した第4の実施形態に係る第1の動作例は、クライアント装置に接続する通信制御装置が自身の通信量の分析情報を通信制御管理装置へ送信し、通信制御管理装置は、通信システムにおける各通信制御装置からの通信量の分析情報に基づいて、個々の通信制御装置がログ情報を送信する時刻をスケジューリングする。

[0203] これにより、各通信制御装置 301 が通信量の分析情報に基づいてログ情報を送信する時刻を判断する必要がなく、通信制御管理装置は、通信システム全体の各通信制御装置における通信量を加味して各通信制御装置がログ情報の送出を決定できる。この結果、個々の通信制御装置だけでなく、ネットワーク全体に発生すると予測される負荷も考慮して各通信制御装置がログ情報を送出する時刻をコントローラでできる。

[0204] 次に、第4の実施形態に係る通信システム 300 における第2の動作例について説明する。

図21は、第4の実施形態に係る通信システム 300 における第2の動作例を説明するためのシーケンスである。

まず、通信制御装置 301 のコントローラ 320 は、上述の第1の動作例と同様に、データメモリ 324 にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ 324 に記憶する（ステップ S421）。

通信制御装置 301 のコントローラ 320 は、データメモリ 324 に記憶した通信量の分析情報に基づいて、当該通信制御装置 301 がログ情報を送信する送出時刻の候補を選出する（ステップ S422）。送出時刻の候補は、1つであっても良いし、複数であっても良いし、時間帯で示しても良い。

[0205] 例えば、コントローラ 320 は、当該通信制御装置における通信量の分析情報に基づき、通信量が最も少ない時間帯で当該通信制御装置 301 がログ情報を送信できる時刻を送出時刻の候補として選出する。また、制御部 301 は、当該通信制御装置における通信量の分析情報に基づき、通信量が所定閾値未満となる時間帯から当該通信制御装置 301 がログ情報を送信できる時刻（送出時刻）を選出しても良い。

[0206] ログ情報の送出時刻の候補を選出すると、コントローラ 3210 は、選出したログ情報の送出時刻の候補を通信制御管理装置 5 へ送信する（ステップ S424）。これにより、通信制御装置 301 が選出するログ情報の送出時刻の候補は、通信制御管理装置 5 が取得する。

- [0207] 通信制御管理装置5の制御部61は、NW通信部60により受信したログ情報の送出時刻の候補を示す情報を送信元の通信制御装置301を示す識別情報に対応づけて記憶部66に記憶する（ステップS425）。これにより、記憶部66には、通信システムにおける各通信制御装置301からログ情報の送出時刻の候補を示す情報が蓄積される。
- [0208] 通信制御管理装置5の制御部61は、記憶部66に記憶した各通信制御装置301のログ情報の送出時刻の候補に基づいてシステム全体の各通信制御装置31がログ情報を送出する時刻のスケジュール（ログ収集のスケジュール）を作成する（ステップS426）。例えば、制御部301は、ネットワークNW全体における通信量が所定閾値未満となるように、各通信制御装置からのログ情報の送出時刻の候補をスケジューリングする。
- [0209] ログ情報の送出時刻のスケジュールを作成すると、制御部61は、個々の通信制御装置301に対してログ情報を送信する送出時刻を通知する（ステップS427）。通信制御装置301のコントローラ320は、通信制御管理装置5からログ情報の送出時刻の通知を受信すると（ステップS428）、ログ情報の送出時刻をデータメモリ324に記憶する（ステップS429）。コントローラ320は、通信制御管理装置5から指示されたログ情報の送出時刻になると、データメモリ324に蓄積したログ情報を通信制御管理装置5へ送信する（ステップS430）。
- [0210] 通信制御装置301から送信されるログ情報は、ネットワークNWを経由して通信制御管理装置5へ伝送され、通信制御管理装置5に受信される（ステップS431）。通信制御管理装置5の制御部61は、通信制御装置301から受信したログ情報を記憶部66に保存する（ステップ432）。例えば、制御部61は、受信したログ情報を実施日時と共に当該通信制御装置301の識別情報に対応づけて記憶部66に記憶する。
- [0211] 以上のように、第4の実施形態に係る第2の動作例は、通信制御装置301が自身の通信量の分析情報に基づいてログ情報の送出時刻の候補を選出する。通信制御管理装置5は、通信システム300における各通信制御装置3

01から取得するログ情報の送出時刻の候補をネットワークNWに対する負荷が少なくなるようにスケジューリングする。

[0212] これにより、各通信制御装置301は、ログ情報を通信制御管理装置へ送信する場合におけるネットワーク全体に対する負荷を軽減することができる。また、ログ情報の送出時刻の候補を各通信制御装置がそれぞれ選出するため、通信制御管理装置5にかかる処理の負荷は軽減できる。この結果として、例えば、通信制御装置の数が大量となるような通信システムにおいても効率良く、各通信制御装置がログ情報を送信する時刻をコントローラできる。

[0213] 次に、第4の実施形態に係る通信システム300における第3の動作例について説明する。

図22は、第4の実施形態に係る通信システム300における第3の動作例を説明するためのシーケンスである。

まず、通信制御装置301のコントローラ320は、上述の第1の動作例と同様に、データメモリ324にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ324に記憶する（ステップS441）。

通信制御装置301のコントローラ320は、データメモリ324に記憶した通信量の分析情報に基づいて、当該通信制御装置301がログ情報を送信する送出予定時刻を決定する（ステップS442）。例えば、コントローラ320は、当該通信制御装置における通信量の分析情報に基づき、通信量が最も少ない時間帯で当該通信制御装置301がログ情報を送信できる時刻を送出予定時刻として選定する。

[0214] ログ情報の送出予定時刻を選定すると、コントローラ320は、選定したログ情報の送出予定時刻になると、ネットワークの混雑度を推定する（ステップS443）。例えば、コントローラ320は、ネットワークの混雑度を確認するための問合せを通信制御管理装置5へ送信してから通信制御管理装置5からの応答を受信するまでの時間からネットワークの混雑度を推定する。ここで、通信制御管理装置5へ送信する問合せは、ネットワークの混雑を

推定するためのデータであるため、それ自体がネットワークの負荷とならないような小さいサイズのデータとする。

[0215] ネットワークの混雑度が所定の閾値以上であれば（ステップS444、NO）、コントローラ320は、ログ情報の送信を中止する。ログ情報の送信を中止する場合、コントローラ320は、通信量の分析情報から再度ログ情報を送信する送出予定時刻を選定するようにする。

[0216] ネットワークの混雑度が所定の閾値未満であれば（ステップS444、YES）、コントローラ320は、ログ情報の送信が可能な状態であると判断し、データメモリ324に蓄積しているログ情報を通信制御管理装置5へ送信する（ステップS445）。

[0217] 通信制御装置301から送信されるログ情報は、ネットワークNWを経由して通信制御管理装置5へ伝送され、通信制御管理装置5に受信される（ステップS446）。通信制御管理装置5の制御部61は、通信制御装置301から受信したログ情報を記憶部66に保存する（ステップ457）。

[0218] 以上のように、第4の実施形態に係る第3の動作例は、通信制御装置が自身の通信量の分析情報に基づいてログ情報の送出予定時刻を設定する。通信制御装置は、時間が設定した送出予定時刻になると、ネットワークの混雑度を推定し、ネットワークの混雑度が閾値未満であれば、ログ情報を通信制御管理装置へ送信するものとする。

[0219] これにより、通信制御管理装置は、個々の通信制御装置に対してログ情報の送出時刻を決定する必要がなくなる。また、個々の通信制御装置は、自身が設定した送出予定時刻において、実際のネットワークの混雑度を確認してから、ログ情報を通信制御管理装置へ送信できる。この結果として、例えば、通信制御装置の数が大量となるような通信システムにおいても、通信制御管理装置5にかかる処理が大きくなることなく、多数の通信制御装置からネットワークに負荷をかけずにログ情報を収集できる。

[0220] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これ

ら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

## 請求の範囲

- [請求項1]       第1の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の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の装置と前記ネットワーク通信網との間に並列に接続される複数の通信系統と、
- 前記第1の装置または前記ネットワーク通信網と前記複数の通信系統との間に設け、前記第1の装置または前記ネットワーク通信網からのデータに対する処理の負荷に応じた数の通信系統で分散して通信処理を実行させる分散制御器と、を具備し、
- 前記複数の通信系統は、
- 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た前記第2の通信制御装置との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の装置から前記第2の装置へ送信される情報を暗号化した情報を前記第2の通信制御装置へ送信し、前記第2の装置から前記第1の装置へ送信される情報を復号した情報を前記第1の装置に送信する通信処理を実行する第1のコントローラをそれぞれ有し、
- 前記第2の通信制御装置は、
- 前記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た前記第1の通信制御装置との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の装置から前記第1の装置へ送信される情報を暗号化した情報を前記第1の通信制御装置に送信し、前記第1の装置から前記第2の装置へ送信された情報を復号した情報を前記第2の装置に送信する通信処理を実行する第2のコントローラを有する通信システム。

- [請求項2] 前記分散制御器は、前記複数の通信系統に含まれる第1の通信系統で通信処理を実行中に前記第1の装置または前記ネットワーク通信網からのデータ量が閾値以上となる場合、前記複数の通信系統に含まれる第1の通信系統とは異なる第2の通信系統を起動させて前記第1の通信系統と前記第2の通信系統とで分散して通信処理を実行させる、請求項1に記載の通信システム。
- [請求項3] 前記分散制御器は、前記複数の通信系統に含まれる2つの通信系統で通信処理を実行中に前記第1の装置または前記ネットワーク通信網からのデータ量が閾値未満となる場合、何れか一方の通信系統を未通信状態し、他方の通信系統での通信処理を継続して実行させる、請求項1に記載の通信システム。
- [請求項4] 前記第1の通信制御装置は、  
前記閾値を記憶するメモリと、  
前記メモリに記憶する閾値を入力するインターフェースと、を有する、  
請求項2または3の何れか1項に記載の通信システム。
- [請求項5] 第1の装置とネットワーク通信網との間に並列に接続される複数の通信系統と、  
前記第1の装置または前記ネットワーク通信網と前記複数の通信系統との間に設け、前記第1の装置または前記ネットワーク通信網からのデータに対する処理の負荷に応じた数の通信系統で分散して通信処理を実行させる分散制御器と、を備え、  
前記複数の通信系統は、  
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た第2の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の装置から前記第2の装置へ送信される情報を暗号化した情報を前記第2の通信制御装置へ送信し、前記第2の装置から前記第

1 の装置へ送信される情報を復号した情報を前記第 1 の装置に送信する通信処理を実行するコントローラをそれぞれ有する、  
通信制御装置。

[請求項6] 前記分散制御器は、前記複数の通信系統に含まれる第 1 の通信系統で通信処理を実行中に前記第 1 の装置または前記ネットワーク通信網からのデータ量が閾値以上となる場合、前記複数の通信系統に含まれる第 1 の通信系統とは異なる第 2 の通信系統を起動させて前記第 1 の通信系統と前記第 2 の通信系統とで分散して通信処理を実行させる、  
請求項 5 に記載の通信制御装置。

[請求項7] 前記分散制御器は、前記複数の通信系統に含まれる 2 つの通信系統で通信処理を実行中に前記第 1 の装置または前記ネットワーク通信網からのデータ量が閾値未満となる場合、何れか一方の通信系統を未通信状態し、他方の通信系統での通信処理を継続して実行させる、  
請求項 5 に記載の通信制御装置。

[請求項8] 前記閾値を記憶するメモリと、  
前記メモリに記憶する閾値を入力するインターフェースと、を有する、  
請求項 6 または 7 の何れか 1 項に記載の通信制御装置。