

明 細 書

発明の名称：通信システム

技術分野

[0001] 本発明の実施形態は、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、通信システムは、複数の第1の通信制御装置と第2の通信制御装置とを備える。第1の通信制御装置は、無線通信部とコントローラとを有する。無線通信部は、無線通信を行う。コントローラは、無線通信部により第1の装置から第2の装置へ送信するデータを受信する場合、データを受信する第1の通信制御装置からネットワーク通信網へデータを送出するためのメッシュネットワーク内の通信経路を決定し、通信経路およびネットワーク通信網を介して通信する第2の通信制御装置と相互認証した後にデータを暗号化したデータを第2の通信制御装置へ送信する。

図面の簡単な説明

[0006] [図1]図1は、実施形態に係る通信システムの構成例を示す図である。

[図2]図2は、実施形態に係るクライアント装置およびサーバ装置の構成例を示すブロック図である。

[図3]図3は、実施形態に係る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の構成例を示すブロック図である。

[図4]図4は、実施形態に係る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、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カードにおける機能構成例を示すブロック図である。

[図6]図6は、実施形態に係る通信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、実施形態に係る通信システムにおけるクライアント装置からサーバ装置へのデータ送信処理の処理例を示すシーケンスである。

[図8]図8は、実施形態に係る通信システムにおけるサーバ装置からクライアント装置へのデータ送信処理の処理例を示すシーケンスである。

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（第1の装置の一例）10（10-1～10-N）と、サーバ装置（第2の装置の一例）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2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NWと、を備える。

- [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] クライアント装置10は、クライアント側の通信制御装置30と無線通信する。無線通信は、たとえば、Wi-Fi（登録商標）網、ブルートゥース（登録商標）などを利用した通信が含まれる。また、複数のクライアント側の通信制御装置30は、互いに無線通信を行う。複数のクライアント側の通信制御装置30は、無線通信で相互に接続することによりメッシュネットワーク8を構成する。メッシュネットワーク8は、単に広い空間でのネットワークに限らず、例えば、複数のクライアント装置が建屋内の複数の階が配置されていたり、遮蔽物が多い環境に設置されていたりするケースにおいて、各クライアント装置からのデータを確実に伝送するためのネットワークとして構成される。
- [0010] メッシュネットワーク8は、各クライアント側の通信制御装置30の無線通信エリア8-1、8-2、8-3でカバーされる通信エリアである。例えば、各クライアント側の通信制御装置30は、IEEE 802.11sなどに準拠するメッシュネットワークを実現する。メッシュネットワーク8は、制御対象とする全てのクライアント装置10と無線通信が可能となるように構築される。クライアント側の通信制御装置30は、メッシュネットワーク8内の他の通信制御装置30との無線通信においてメッシュIEEE 802.11sなどのプロトコルが採用されることにより、可用性と秘匿性が向上した無線セキュリティネットワークを実現できる。
- [0011] また、クライアント側の通信制御装置30は、ゲートウェイ／アクセスポイント（GW／AP）として動作する機能を有する。クライアント側の通信制御装置30は、メッシュネットワーク内のクライアント装置10に対応する鍵および証明書を保持する。これにより、各通信制御装置30は、クライアント装置10に対する認証を行う。また、各クライアント装置10は、メ

ッシュネットワークを構成する各通信制御装置30と無線通信を行うための設定を保持する。例えば、各クライアント装置10は、自身の識別情報としてのSSID、および、WPA等の認証に用いるパスワードなどが設定される。

[0012] 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との間に接続されるメッシュネットワーク8によって、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。すなわち、メッシュネットワーク8を構成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。

[0013] また、メッシュネットワーク8を構成する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。

[0014] なお、通信システム1において、複数のクライアント側の通信制御装置30のうち1つは、有線通信でネットワークNWに接続される。図1に示す構成例では、通信制御装置30-1が、ネットワークNWに接続され、ネットワークNWを介してサーバ側の通信制御装置31と通信する。メッシュネットワーク8において、通信制御装置30-1以外の通信制御装置30-2、…、30Nは、ネットワークNWに接続されるための通信部を持たなくても良く、他の通信制御装置30とクライアント装置10とに無線通信で接続す

るための通信部を具備するものであれば良い。

- [0015] また、クライアント側の通信制御装置30のうちの1つは、1つのクライアント装置10との間をイーサケーブルなどの有線通信用のケーブルで接続するようにしても良い。1つのクライアント装置にクライアント側の通信制御装置30のうちの1つを有線で繋ぐことによって、クライアント装置10側の設定の変更を少なくでき、クライアント側の通信制御装置30側の変更も少なくすることができる。
- [0016] 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からクライアント装置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。
- [0017] 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からメッシュネットワーク8を構成する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。
- [0018] 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 Secu

re) に置き換える。

[0019] 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。

[0020] 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。

[0021] 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およびサーバ側の通信制御装置31を管理するためのデバイス管理サーバである。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。

[0022] 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 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、クライアント側の通信制御装置 3 0 とサーバ側の通信制御装置 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。

[0023] 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、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 1 0 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 1 0 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 2 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、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 1 0 とサーバ装置 2 0 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 1 0 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] 図 2 は、図 1 に示すクライアント装置 1 0、およびサーバ装置 2 0 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、無線通信部１１と、クライアント制御部１２と、撮像部１３とを備える。無線通信部１１は、メッシュネットワーク８を構成するクライアント側の通信制御装置３０と無線通信するための通信インターフェースである。無線通信部１１は、例えば、W i e r F iあるいはブルートゥースなどの無線通信を実行するポートである。無線通信部１１は、クライアント側の通信制御装置３０と無線通信によって接続され、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。

[0026] クライアント制御部１２は、例えば、C P U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。

[0027] サーバ装置２０は、N W（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。N W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。N W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。

[0028] サーバ制御部２２は、例えば、C P U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。

[0029] クライアント装置１０とサーバ装置２０とが、互いのN W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。

[0030] この場合、クライアント装置10、またはサーバ装置20は、暗号化されていない情報（いわゆる、平文）が出力される。ネットワークに平文を伝送させると、外部から悪意をもつ第三者が平文のデータを取得することで、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。

[0031] しかしながら、現在既に社会インフラに用いられている監視カメラなどのクライアント装置は、暗号化のための処理を行うだけの資源（リソース）を備えていないことが多い。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。このため、本実施形態に係る通信システム1は、クライアント装置10とネットワークNWとの間に配置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。

[0032] 次に、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のハードウェア構成について説明する。

図3は、図1に示す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のハードウェア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がクライアント装置10と無線通信するための無線通信部を有し、サーバ側の通信制御装置31がサーバ装置20と通信するための通信部を有する。これらの点以外は、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とは同様なハードウェア構成を具備するもので良い。また、サーバ側の通信制御装置31が無線通信部を具備していても良いし、クライアント側の通信制御装置30が有線による通信部を具備していても良いため、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とは同一のハードウェアで構成するようにしても良い。このため、以下では、クライアント側の通信制御装置30のハードウェア構成について説明し、サーバ側の通信制御装置31のハードウェア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。

[0033] 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、コントローラ(制御部)33、無線通信部34、リーダライタ35、ICカード40、電源36、メモリI/F37などを備える。

コントローラ33は、通信制御装置30(31)を制御するものである。図3に示す構成例において、コントローラ33は、MPU101、RAM102、SAM103およびデータメモリ104などを有する。

[0034] MPU101は、コントローラ33の制御を司るプロセッサの一例である。MPU101は、データメモリ104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33は、MPU101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。

[0035] また、コントローラ33は、MPU101がプログラムを実行することにより、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33は、リーダライタ105を介して接続するICカード40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。

[0036] RAM 102は、ランダムアクセスメモリである。RAM 102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 103は、シリアルアクセスメモリである。データメモリ 104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 104は、プログラムおよび設定情報などを記憶する。また、データメモリ 104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 104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へ送信されたり、自己診断処理に用いられったりする。

[0037] また、データメモリ 104は、正当なシステムコンポーネントであることを示すホワイトリストを記憶する。ホワイトリストは、通信を許可するクライアント装置 10などを示す情報をリストとして保存するものである。例えば、クライアント側の通信制御装置 30がMACアドレスなどの機器固有情報によってクライアント装置 10を認証する運用とする場合、通信を許可するクライアント装置 10の機器固有情報をホワイトリストとしてデータメモリ 104に保存する。例えば、コントローラ 33は、無線通信部 34により通信する装置が正当なシステムコンポーネント（クライアント装置）であることをホワイトリストを参照して認証する。なお、コントローラ 33は、データメモリ 104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。

[0038] また、データメモリ 104は、メッシュネットワーク 8内に存在するすべてのシステムコンポーネント（例えば、各クライアント装置 10）に対応する鍵と証明書とを記憶する。例えば、データメモリ 104に記憶するクライアント装置 10に対応する鍵と証明書とは、SSL/TLS通信における認証に用いられる。

[0039] また、データメモリ 104は、メッシュネットワーク 8を構築する各通信制御装置 30が正当であることを示すための鍵と証明書を記憶する。例えば

、データメモリ 104 に記憶する各通信制御装置 30 が正当であることを示すための鍵と証明書とは、メッシュネットワーク 8 内に設定される通信経路における各通信制御装置 30 同士の相互認証に用いられる。

[0040] NW通信部 32 は、通信制御装置 30 (31) におけるネットワーク NW 側の通信を実行する。ただし、クライアント側の通信制御装置 30 のうちネットワーク NW と直接通信しない通信制御装置 (例えば、図 1 に示す通信制御装置 30-2、30-3) は、NW通信部 32 の構成を省略しても良い。NW通信部 32 は、通信回線を介してネットワーク NW に接続するためのインターフェースを想定して説明するが、NW通信部 32 についても、ネットワーク NW と無線で通信するものであっても良い。

[0041] 無線通信部 34 は、クライアント装置 10 および他の通信制御装置 30 と無線通信する通信インターフェースである。ただし、サーバ側の通信制御装置 31 は、サーバ装置 20 と無線で通信するものでなければ、無線通信部 34 に換えてサーバ装置 20 と通信するサーバ通信部を有する。

[0042] 電源 36 は、外部電源に接続され、外部電源からの電力を通信制御装置 30 (31) 内の各部へ供給する。メモリ I/F 37 は、メモリカードなどのメモリデバイス 38 をセットするインターフェースである。例えば、メモリ I/F 37 には、初期設定情報などの当該通信制御装置 30 (31) に適用する情報を記憶したメモリデバイス 38 がセットされる。メモリ I/F 37 にセットするメモリデバイス 38 には、ログデータなどのデータを記憶するようにしても良い。

[0043] なお、ネットワーク NW に接続するクライアント側の通信制御装置 30-1 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。このような通信制御装置 30-1 は、一方の通信デバイスで通信処理を実行する運用とし、通信処理を実行中の通信デバイスで故障や通信障害が発生した場合に、他方の通信デバイスで通信処理を継続して実行する。これにより、ネットワーク NW に接続する 1 つの通信制御装置 30-1 が冗長化され、故障や障害が発生しても通信処理

がと切れることがない可用性を向上できる。

- [0044] また、ネットワークNWに接続するクライアント側の通信制御装置30-1は、通信処理を実行するデバイスに故障や障害などが発生した場合あるいは電源36に供給される電力が停止（停電）した場合に、データをそのまま通過させせるパススルーモードで動作するようにしても良い。さらに、通信制御装置30-1がパススルーモードとなった場合、他のクライアント側の通信制御装置30（30-2又は30-3）がネットワークNWに接続するクライアント側の通信制御装置として機能するようにしても良い。このような動作制御は、通信制御管理装置（デバイス管理サーバ）5が各通信制御装置30の動作状態を監視し、各通信制御装置30に対して動作モードなどを指示することで実現できる。
- [0045] リーダライタ35は、コンタクト部35a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。ここで、ICカード40は、後述する処理を実行する「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。
- [0046] ICカード40は、例えば、プラスチックのカード基材に、コンタクト部40aを有する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35aを介して通信制御装置30（31）と通信可能である。
- [0047] 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35aおよびコンタクト部40a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）のコンタクト部35aにコンタクト部40aを介して送信する。

[0048] ICモジュール41は、コンタクト部40aとICチップ42とを備える。コンタクト部40a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)のコンタクト部35a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。

[0049] 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40a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。

[0050] 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。

[0051] 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40a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。

[0052] 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。

[0053] 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。

[0054] 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40a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。

[0055] 制御部51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 5 1 は、コマンド処理部 5 2 と暗号化復号部 5 3 とを備える。

ここで、コマンド処理部 5 2 が行う処理は、「認証処理」の一例である。

また、暗号化復号部 5 3 が行う処理は、「暗号化復号処理」の一例である。

[0056] コマンド処理部 5 2 は、各種コマンド処理を実行する。コマンド処理部 5 2 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 3 0 とサーバ側の通信制御装置 3 1 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。

[0057] 暗号化復号部 5 3 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 5 3 は、通信部 5 0 を介して取得した装置（クライアント装置 1 0、またはサーバ装置 2 0）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 5 3 は、通信部 5 0 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。

[0058] 記憶部 5 4 は、例えば、EEPROM 4 7 により構成された記憶部であり、証明書情報記憶部 5 5 と、秘密情報記憶部 5 6 とを備える。証明書情報記憶部 5 5 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 1 0、またはサーバ装置 2 0）に対する証明書を記憶する。具体的には、クライアント側の通信制御装置 3 0 に装着される IC カード 4 0 の証明書情報記憶部 5 5 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 3 1 に装着される IC カード 4 0 の証明書情報記憶部 5 5 には、サーバ証明書を示す情報が記憶される。

[0059] 秘密情報記憶部 5 6 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 1 0、またはサーバ装置 2 0）に対する秘密鍵を記憶する。具体的には、クライアント側の通信制御装置 3 0 に装着される IC カード 4 0 の秘密情報記憶部 5 6 には、クライアント側の通信制御装置 3 0 に対して発行された秘密鍵を示す情報が記憶される。また、サーバ側の通信制御装置 3 1 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。

[0060] なお、ＩＣカード４０は、通信制御装置３０（３１）が実行すべき処理の一部を実施するための処理部（認証部）の一例である。上述したＩＣカード４０が実現する処理は、コントローラ３３または別途設ける処理回路などで実現するようにしても良い。すなわち、通信制御装置３０（３１）は、認証部として機能するＩＣカード４０を具備するものに限定されるものでなく、コントローラ３３や処理回路などが相互認証処理および暗号化復号化処理などの処理を実現するものであっても良い。

[0061] 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。

[0062] 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。

[0063] 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。

[0064] 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。

[0065] 証明書更新部 64 は、有効期限が渡過した証明書に対して新たな有効期限を設定することにより、証明書の更新を行う。証明書更新部 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。

[0066] 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を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。

[0067] 管理部 69 は、通信制御装置 30 (31) を管理する。例えば、管理部 69 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。

記憶部 66 は、例えば、鍵情報記憶エリア 67 と、証明書情報記憶エリア 68 とを備える。鍵情報記憶エリア 67 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 68 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 67 と、証明書情報記憶エリア 68 とは、例えば、鍵生成部 62 が秘密鍵を発行する際、証明書発行部 63 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 67 には、鍵生成部 62 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 68 には、証明書発行部 63 が発行した証明書を示す情報が記憶される。

[0068] 次に、実施形態に係る通信システム 1 においてクライアント装置 10 からサーバ装置 20 へデータを送信する場合の処理の流れについて説明する。

図 7 は、実施形態に係る通信システム 1 においてクライアント装置 10 からサーバ装置 20 へデータを送信する場合の処理の一例を示すシーケンスである。

クライアント装置 10 は、撮像データなどのデータをサーバ装置 20 に送信する場合、無線通信エリアにあるクライアント側の通信制御装置 30 に対して自身の機器固有情報を送信する（ステップ S11）。例えば、クライアント装置 10 は、WPA2 等のデータリンク層のプロトコルや MAC アドレスなどの機器固有情報を送信することによりクライアント側の通信制御装置 30 に認証を要求する。ここでは、図 7 に示すように、クライアント装置 10 が、メッシュネットワーク 8 を形成する複数の通信制御装置 30 のうち通信制御装置 30-3 に機器固有情報として SSID とパスワード（PW）とを送信するものとする。クライアント装置 10 が送信した機器固有情報は、クライアント側の通信制御装置 30-3 により取得される。

[0069] クライアント側の通信制御装置 30-3 のコントローラ 33 は、クライアント装置 10 からの機器固有情報を取得すると、受信した機器固有情報に基づいて正当な機器であるかを認証する（ステップ S12）。例えば、コントローラ 33 は、データメモリ 104 に保持するホワイトリストにより受信した機器固有情報のクライアント装置 10 が正当な機器であるかを認証する。

[0070] これにより、各クライアント側の通信制御装置 30 は、正しいシステムコンポーネント（ホワイトリストが示す機器）以外の通信を破棄できる。正しいシステムコンポーネント以外の通信を破棄することによって、多数の機器との無線通信可能な通信制御装置 30 であっても、不特定の機器からの多量通信による攻撃を防ぐことができる。また、メッシュネットワークを構成す

る各通信制御装置 30 がそれぞれ認証処理を行うため、特定の通信制御装置だけが認証を行うシステムに比べて、不正な機器からの攻撃を分散でき、認証処理の負荷も下げることができる。

[0071] クライアント装置 10 の認証が成功すると、コントローラ 33 は、当該クライアント装置 10 からサーバ装置 20 へ送信するデータを受け付ける。クライアント装置 10 は、相互認証に基づく暗号化を施していないデータ（ここでは、平文のデータと称する）を無線通信先の通信制御装置 30-3 へ送信する。ただし、クライアント装置 10 から通信制御装置 30-3 へ送信されるデータは、WPA2 等のデータリンク層で保護される。

[0072] 通信制御装置 30-3 のコントローラ 33 は、メッシュネットワーク内においてクライアント装置 10 からサーバ装置 20 へのデータを送信するルートを検索するルーティング検索を実行する（ステップ S14）。ルーティング検索は、当該通信制御装置 30-3 からネットワーク NW へ繋がる通信制御装置 30-1 へデータを送信するための通信経路を検索する処理である。

[0073] ルーティングプロトコルとしては、RMAODV などの隣接するノード（通信制御装置）の無線伝送速度、トラフィック量、干渉量などから決定されるリアクティブなメトリクスを利用するプロトコルを採用する。ここで、無線伝送速度の中には、その時の処理負荷状況を含める。ルーティング検索は、通信が発生するごとに実施する。

データの送信要求を受けるごとにルーティング検索を実行することにより、同一のクライアント装置 10 であっても、常に予め設定した固定の通信経路ではなく、都度検索する最適な（例えば最も高速な）経路でメッシュネットワーク内をデータ転送できる。また、都度ルーティング検索を実行することにより、メッシュネットワークを構成する通信制御装置の 1 つが、不正な攻撃や故障によってダウンした場合でも、メッシュネットワーク内の別の利用可能な通信制御装置を利用した通信経路の中でより良い経路を選択することができ、冗長化を実現できる。なお、ルーティング検索では、MAC アドレスなどで正当性が確認できる装置であれば、通信制御装置以外の装置を含

む通信経路を検索するようにしても良い。

- [0074] ルーティング検索によってメッシュネットワーク 8 内の通信経路が決まると、通信制御装置 30-3 のコントローラ 33 は、メッシュネットワーク内の通信経路を形成する各通信制御装置 30 の認証を実行する（ステップ S 15）。コントローラ 33 は、各通信制御装置 30 が保持している鍵と証明書を用いて、メッシュネットワーク内の通信経路を形成する通信制御装置 30 間の相互認証を行う。これにより、メッシュネットワークにおいて正当性が確認できた通信制御装置群によって経路を作成することができ、メッシュネットワーク対応機器によるなりすましや中間者攻撃などによる乗っ取りを防ぐことができる。なお、メッシュネットワークにおける通信経路に通信制御装置以外の装置を含む場合、通信制御装置以外の装置については、MAC アドレスなどの別の認証方法を用いて認証するようにしても良い。
- [0075] メッシュネットワーク内の通信経路における通信制御装置 30 同士の相互認証が成功すると、通信制御装置 30-3 のコントローラ 33 は、SSL/TLS における認証として、クライアント装置 10 に対応する鍵と証明書とを利用してサーバ側の通信制御装置 31 との相互認証を実行する（ステップ S 16）。
- [0076] 例えば、クライアント側の通信制御装置 30-3 は、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を送信する。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 30-3 に対し、サーバ側の通信制御装置 31 が暗号化アルゴリズムを決定する。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 に対応する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 30-3 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。

- [0077] クライアント側の通信制御装置 30-3 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 30-3 は、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、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 30-3 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 30-3 は、検証が成功すると、その証明書がサーバ側の通信制御装置 31 のものであると判定する。
- [0078] クライアント側の通信制御装置 30-3 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 30-3 とサーバ側の通信制御装置 31 とは、それぞれ暗号化および復号に用いる共通鍵を交換する。
- [0079] 通信制御装置 30-3 とサーバ側の通信制御装置 31 との相互認証が成功した後、通信制御装置 30-3 のコントローラ 33 は、クライアント装置 10 からのデータをサーバ側の通信制御装置 31 との相互認証結果に基づいて暗号化する（ステップ S 17）。通信制御装置 30-3 のコントローラ 33 は、暗号化されたデータ（暗号文）をルーティング検索によって設定された通信経路に沿ってメッシュネットワーク 8 内を送信させる（ステップ S 18、S 19）。
- [0080] 例えば、通信制御装置 30 のコントローラ 33 は、暗号化したデータにメッシュネットワーク 8 内における通信経路を示す情報を付加して通信経路上の次の通信制御装置へ送信する。図 7 に示す例では、通信制御装置 30-3 のコントローラ 33 は、暗号化したデータを通信制御装置 30-2 へ送信し

(ステップS 18)、通信制御装置30-2のコントローラ33は、通信制御装置30-3からの暗号化されたデータを通信制御装置30-1へ送信する(ステップS 19)。

[0081] メッシュネットワーク8における通信経路の終端となるネットワークNWに接続する通信制御装置30-1のコントローラ33は、メッシュネットワーク内の他の通信制御装置30-1、30-2をから転送されてくる暗号化されたデータをネットワークNWを介してサーバ側の通信制御装置31へ送信する(ステップS 20)。サーバ側の通信制御装置31のコントローラ33は、クライアント側の通信制御装置30から受信した暗号化されたデータをクライアント側の通信制御装置30-3との相互認証結果に基づいて復号する(ステップS 21)。例えば、サーバ側の通信制御装置31のコントローラ33は、クライアント装置10からの暗号化されたデータを相互認証で得られた公開鍵を用いて復号したデータをサーバ装置20へ送信する(ステップS 22)。これにより、クライアント装置10からサーバ装置20までのデータ送信処理が完了する。

[0082] 通信制御装置30-3とサーバ側の通信制御装置31とのメッシュネットワークおよびネットワークNWを介した相互認証が成功すると、相互認証に基づく暗号化を含む通信処理が実現できる。これにより、クライアント装置10から送信されるデータは、データの送信元のクライアント装置10の近傍(通信エリア内)にあるクライアント側の通信制御装置3-3まではWPA2等のデータリンク層による保護であるが、それ以降の通信経路(メッシュネットワーク内およびネットワークNW内)においては、SSL/TLSによる認証された秘匿通信となる。この結果、本実施形態に係る通信システムは、ネットワークNWにおけるセキュリティだけでなく、メッシュネットワークにおいて伝送されるデータのセキュリティも確保できる。

[0083] 次に、実施形態に係る通信システム1においてサーバ装置からクライアント装置へデータを送信する場合の処理の流れについて説明する。

図8は、実施形態に係る通信システム1においてサーバ装置20からクラ

クライアント装置 10 へデータを送信する場合の処理の一例を示すシーケンスである。

サーバ装置 20 は、クライアント装置 10 へコマンドあるいはソフトウェアの更新データなどを送信することがある。サーバ装置 20 は、クライアント装置 10 へデータを送信する場合、送信先のクライアント装置 10 を示す識別情報を付加して送信すべきデータをサーバ側の通信制御装置 31 へ送信する（ステップ S 31）。

[0084] サーバ側の通信制御装置 31 のコントローラ 33 は、サーバ装置 20 からクライアント装置宛のデータを受信すると、サーバ装置 20 に対応する鍵と証明書とに基づく SSL/TLS における認証の要求をクライアント側の通信制御装置 30-1 へ送信する（ステップ S 32）。

[0085] クライアント側の通信制御装置 30-1 のコントローラ 33 は、メッシュネットワーク内においてネットワーク NW から宛先のクライアント装置 10 へデータを送信するルートを検索するルーティング検索を実行する（ステップ S 34）。ここで、通信制御装置 30-1 がネットワーク NW に接続し、宛先のクライアント装置 10 と無線通信するのが通信制御装置 30-3 であれば、クライアント側の通信制御装置 30-1 のコントローラ 33 は、メッシュネットワーク 8 におけるルーティング検索として、通信制御装置 30-1 から通信制御装置 30-3 へデータを送信するための通信経路を検索する。

[0086] ルーティング検索は、上述したようなルーティングプロトコルによって実施され、データの送信要求を受けるときの処理の負荷状況を踏まえて決定する。データの送信要求を受けるとにルーティング検索を実行することにより、処理の負荷状況に応じた最適な（例えば最も高速な）通信経路を決定できる。また、都度ルーティング検索を実行することにより、1つの通信制御装置が不正な攻撃や故障によってダウンした場合でも、メッシュネットワーク内の別の利用可能な通信制御装置を利用した通信経路の中でより良い経路を選択することができ、冗長化を実現できる。なお、ルーティング検索では

、正当性が確認できる装置であれば、通信制御装置 30 以外の装置を含む通信経路を検索するようにしても良い。

[0087] ルーティング検索によってメッシュネットワーク 8 内の通信経路が決まると、通信制御装置 30-1 のコントローラ 33 は、メッシュネットワーク内の通信経路を形成する各通信制御装置 30 同時の認証を実行する（ステップ S35）。コントローラ 33 は、各通信制御装置 30 が保持している鍵と証明書を用いてメッシュネットワーク 8 内の通信経路を形成する通信制御装置 30 間の相互認証を行う。これにより、メッシュネットワークにおいて正当性が確認できた通信制御装置群によって通信経路を作成することができ、メッシュネットワーク対応機器によるなりすましや中間者攻撃などによる乗っ取りを防ぐことができる。なお、メッシュネットワークにおける通信経路に通信制御装置以外の装置を含む場合、通信制御装置以外の装置については、MAC アドレスなどの別の認証方法を用いて認証するようにしても良い。

[0088] メッシュネットワーク内の通信経路における通信制御装置 30 同士の相互認証が成功すると、通信経路の終端となる通信制御装置（宛先のクライアント装置 10 と無線通信する通信制御装置）30-3 のコントローラ 33 は、SSL/TLS における認証としてサーバ側の通信制御装置 31 との相互認証を実行する（ステップ S36）。クライアント側の通信制御装置 30-3 とサーバ側の通信制御装置 31 との間の相互認証は、上述したような手法で実施される。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 30-3 とサーバ側の通信制御装置 31 とは、それぞれ暗号化および復号に用いる共通鍵を交換する。

[0089] 通信制御装置 30-3 とサーバ側の通信制御装置 31 との相互認証が成功した後、サーバ側の通信制御装置 31 のコントローラ 33 は、サーバ装置 20 からクライアント装置 10 宛のデータを相互認証によって得られた共通鍵を用いて暗号化する（ステップ S37）。通信制御装置 31 のコントローラ 33 は、暗号化した暗号化データ（暗号文）をネットワーク NW を介してクライアント側の通信制御装置 30-1 へ送信する（ステップ S38）。

- [0090] クライアント側の通信制御装置30-1のコントローラ33は、ネットワークNWを介してサーバ側の通信制御装置31から取得する暗号化データにルーティング検索によって設定された通信経路に沿ってメッシュネットワーク8内を送信させる（ステップS39、S40）。ここで、クライアント側の通信制御装置30-1のコントローラ33は、通信経路の終端となる通信制御装置を明示するため、暗号化データにメッシュネットワーク8内における通信経路を示す情報（または通信経路の終端となる通信制御装置を示す情報）を付加して通信経路を伝送させる。
- [0091] 図8に示す例では、クライアント側の通信制御装置30-1のコントローラ33は、暗号化データ（暗号文）に通信経路を示す情報を付加したデータを通信制御装置30-2へ送信し（ステップS39）、通信制御装置30-2のコントローラ33は、通信制御装置30-1からのデータを通信制御装置30-3へ転送する（ステップS40）。
- [0092] メッシュネットワーク8における通信経路の終端となるクライアント装置10と直接無線通信する通信制御装置30-3のコントローラ33は、メッシュネットワーク8内の他の通信制御装置30-1、30-2から転送されてくる暗号化データに付加されたデータから自身が通信経路の終端であることを判断し、受信した暗号化データをサーバ側の通信制御装置31との相互認証で得られた共通鍵を用いて復号する（ステップS41）。通信制御装置30-3のコントローラ33は、復号したデータを無線通信部によりクライアント装置10へ送信する（ステップS42）。これにより、サーバ装置20からクライアント装置10までのデータ送信処理が完了する。
- [0093] 以上の処理によれば、サーバ装置20からクライアント装置10へ送信するデータについても、ネットワークNWおよびメッシュネットワーク内を通信制御装置30-3とサーバ側の通信制御装置31との相互認証結果を用いて暗号化した状態でセキュアに伝送できる。この結果、本実施形態に通信システムは、クライアント装置10とサーバ装置20との間を伝送されるデータについて、ネットワークNWにおけるセキュリティだけでなく、メッシュ

ネットワークにおいて伝送されるデータのセキュリティも確保できる。

[0094] なお、クライアント側の通信制御装置 30-3 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なかった場合、クライアント側の通信制御装置 30-3 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 30-3 は、通信先から送信された情報をクライアント装置 10 に出力しない。相互認証が正しく行われなかった場合、通信先がサーバ側の通信制御装置 31 に見せかけた不正な通信装置である可能性があるためである。この場合、クライアント側の通信制御装置 30-3 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。これにより、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 30-3 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。

[0095] また、クライアント側の通信制御装置 30-3 は、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 のコントローラ 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。

[0096] また、コントローラ 33 は、送信先リストを更新するようにしてもよい。コントローラ 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、コントローラ 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。

[0097] また、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との相互認証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30のコントローラ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。

[0098] 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。

[0099] 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。

[0100] 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。

[0101] 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メッシュネットワークを構成する複数の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。クライアント装置 10 と直接無線通信するクライアント側の通信制御装置 30-3 は、メッシュネットワーク内の通信経路を決定し、クライアント装置 10 からの情報を暗号化してメッシュネットワークの通信経路およびネットワーク NW 経由でサーバ側の通信制御装置 31 へ送信する。また、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）は、ネットワーク NW に接続するクライアント側の通信制御装置 30-1 が検索する通信経路でメッシュネットワークで伝送し、メッシュネットワーク内の通信経路の終端となる通信制御装置 30-3（クライアント装置 10 と直接無線通信する通信制御装置 30-3）が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。

[0102] 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、クライアント装置10と直接無線通信する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。

[0103] 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。

[0104] 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。

[0105] 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しても良い。この場合、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。

[0106] 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。

[0107] 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。

[0108] 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。

[0109] 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。

[0110] また、通信システム１では、ＩＣカード４０の制御部５１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。

[0111] 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、上記のようにカードの形態に限定されるものではない。

[0112] 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。

[0113] 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。

[0114] 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。

[0115] 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。

[0116] 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。

[0117] 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。

[0118] 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。

[0119] 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。

[0120] 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。

[0121] 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。

[0122] 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。

[0123] 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。

[0124] 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。

[0125] 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メッシュネットワークを構成する複数の第1の通信制御装置と、
 第2の装置と前記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、
 無線通信を行う無線通信部と、
 前記無線通信部により前記第1の装置から前記第2の装置へ送信するデータを受信する場合、前記データを受信する当該第1の通信制御装置から前記ネットワーク通信網へ前記データを送出するための前記メッシュネットワーク内の通信経路を決定し、前記通信経路および前記ネットワーク通信網を介して通信する前記第2の通信制御装置と相互認証した後に前記データを暗号化したデータを前記第2の通信制御装置へ送信するコントローラと、を有する、
 通信システム。
- [請求項2] 前記第1の装置から前記データを取得した当該第1の通信制御装置のコントローラは、前記第1の装置から前記第2の装置へ送信するデータを前記第2の通信制御装置と相互認証によって決定された共通鍵を用いて暗号化する、
 請求項1に記載の通信システム。
- [請求項3] 前記コントローラは、前記無線通信部により前記第1の装置から機器固有情報を取得し、前記機器固有情報による認証が成功した後、前記第1の装置から前記第2の装置へ送信するデータを受け付ける、
 請求項1に記載の通信システム。
- [請求項4] 前記コントローラは、前記メッシュネットワーク内の通信経路を決定した場合に前記通信経路にある各第1の通信制御装置同士で相互認証し、前記通信経路にある各第1の通信制御装置同士の相互認証が成功した後、前記通信経路および前記ネットワーク通信網を介して前記

第2の通信制御装置と通信する、

請求項1乃至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接続されるメッシュネットワークを構成する複数の第1の通信制御装置と、

第2の装置と前記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、

無線通信を行う無線通信部と、

前記第2の装置から前記第1の装置へ送信するデータを暗号化した暗号化データを前記第2の通信制御装置から受信する場合、前記暗号化データを受信する当該第1の通信制御装置から前記第1の装置へ前記データを送出するための前記メッシュネットワーク内の通信経路を決定し、前記通信経路の終端となる第1の通信制御装置と前記第2の通信制御装置とが相互認証した後、前記ネットワーク通信網を介して前記第2の通信制御装置から取得する前記暗号化データを前記通信経路により前記通信経路の終端となる第1の通信制御装置へ送信するコントローラと、を有する、

通信システム。

[請求項6]

前記通信経路の終端となる第1の通信制御装置のコントローラは、前記第2の通信制御装置と相互認証によって決定された共通鍵を用いて前記暗号化データを復号し、復号したデータを前記第1の装置へ送信する、

請求項5に記載の通信システム。

[請求項7]

前記コントローラは、前記メッシュネットワーク内の通信経路を決定した場合に前記通信経路にある各第1の通信制御装置同士で相互認証し、前記通信経路にある各第1の通信制御装置同士の認証が成功した後、前記通信経路を介して通信する、

請求項5又は6の何れか1項に記載の通信システム。