

明 細 書

発明の名称： 通信システム及びコンピュータ可読記憶媒体

技術分野

[0001] 本発明の実施形態は、通信システム及びコンピュータ可読記憶媒体に関する。

背景技術

[0002] IoT (Internet of Things) 技術の発展により、家電や自動車、工場など世界中の様々なモノがインターネットへつながるようになってきた。このようなIoT技術を活用して、工場内や発電所、鉄道などで運転や点検時の様々な稼働データを収集し、AI (人工知能) にて分析することにより、事前に故障の兆候を検知する予防保全や設備の効率運用へと結びつける動きが高まっている。いずれも、センサー情報をネットワーク経由で収集し、そのデータを活用するために、かつてクローズドな独自ネットワークのみで運用していたものをオープンなネットワークにつなげる必要性が出てきている。独自ネットワークで守られていたシステムが、オープンなネットワークにつながると、オープンなネットワーク経由により不正アクセスされることがある。

先行技術文献

特許文献

[0003] 特許文献1：日本国特表2012-533231号公報

発明の概要

発明が解決しようとする課題

[0004] 上記した不正アクセスを検出するため、セキュリティの仕組みをIoTデバイス自体に組み込むことが考えられる。しかし、既に稼働している既存のIoTデバイスにセキュリティの仕組みを加えることは、既存のIoTデバイスに変更を加えることになるため、コストや可用性の点で難しく、既存のデバイスへの変更を必要としない不正アクセスを検出する仕組み要望されている。

[0005] 本発明が解決しようとする課題は、既存のデバイスを変更せずに不正アク

セスの検出に優れた通信システム及びコンピュータ可読記憶媒体を提供することにある。

課題を解決するための手段

[0006] 実施形態に係る通信システムは、ネットワーク接続装置と第1のクライアント装置の間に接続される第1の通信制御装置、前記ネットワーク接続装置と第2のクライアント装置の間に接続される第2の通信制御装置、及び前記ネットワーク接続装置に接続され、前記第1の通信制御装置と第2の通信制御装置による通信を管理する通信制御管理装置を備える。前記通信制御管理装置は、前記第1のクライアント装置と前記第2のクライアント装置の間の正規通信を第1の仮想タグを含む第1のパケットによる通信と定め、前記通信制御管理装置と前記第1の通信制御装置又は第2の通信制御装置の間の正規通信を第2の仮想タグを含む第2のパケットによる通信と定めた管理情報に基づき、通信を監視する。

図面の簡単な説明

[0007] [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による通信監視の一例を示すフローチャートである。

[図10]図10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11]図11は、第2の実施形態に係る通信システムによる通信監視の一例を示すフローチャートである。

実施形態

[0008] 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）（N：自然数）と、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）（N：自然数）（「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50（「プライベート認証局」の一例）と、ネットワーク6と、ネットワーク接続装置7（ゲートウェイなど）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等とを接続するネットワーク接続装置7と、をまとめて「ネットワークNW」とも称する。

[0009] クライアント装置10は、クライアント側の通信制御装置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。

[0010] 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。

[0011] 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。

[0012] 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。

[0013] 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。

[0014] 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。

[0015] 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。

[0016] 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。

[0017] 通信制御管理装置50は、ネットワーク接続装置7に接続、又はネットワーク6を介してネットワーク接続装置7に接続し、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50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50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 50 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。

[0018] また、通信制御管理装置 50 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 50 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 50 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。

[0019] 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。

[0020] 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。

[0021] 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。

[0022] 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。

[0023] 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N

W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。

[0024] 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。

[0025] 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。

[0026] 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。

[0027] 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

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。

[0028] 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。

[0029] 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。

[0030] 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、記憶部３６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。

[0031] 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。

[0032] 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。

[0033] 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。

[0034] 記憶部 36 は、非一時的なコンピュータ可読記憶媒体としてのメモリであ

り、制御部33の動作プログラム等を記憶する。制御部33は、動作プログラムに基づき動作し、各機能を実現する。例えば、制御部33は、動作プログラムに基づき動作し、通信状況を通信制御管理装置50へ報告し、また、通信制御管理装置50からの制御コマンドに基づく動作を制御する。

[0035] また、記憶部36は、送信先リスト（通信許可リスト）を記憶する。送信先リストは、通信が許可された通信相手を特定するための情報を含む。例えば、通信相手を特定するための情報は、URL（Uniform Resource Locator）である。本実施形態では、記憶部36に記憶される送信先リストは、クライアント装置10（10-1～10-N）を特定するための識別情報を含む。

[0036] 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。

[0037] 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。

[0038] 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。

- [0039] 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。
- [0040] 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。
- [0041] 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り、非一時的なコンピュータ可読記憶媒体である。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。
- [0042] 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400と、制御部401と、記憶部404とを備える。こ

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。

[0043] 通信部400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400は、所定の処理を要求するコマンド(処理要求)を通信制御装置30(31)から受信するとともに、コマンドに対するレスポンス(処理応答)を通信制御装置30(31)に送信する。通信部400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400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。

[0044] 制御部401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401は、コマンド処理部402と暗号化復号部403とを備える。

ここで、コマンド処理部402が行う処理は、「認証処理」の一例である。また、暗号化復号部403が行う処理は、「暗号化復号処理」の一例である。

[0045] コマンド処理部402は、各種コマンド処理を実行する。コマンド処理部402は、例えば、後述するHTTPSリクエストを要求するコマンド処理として、SSL/TLSハンドシェイクを行う。SSL/TLSハンドシェイクでは、暗号化された通信に必要な鍵情報等の交換、および通信先の装置との相互認証を行う。ここで、相互認証とは、クライアント側の通信制御装置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。

[0046] 暗号化復号部403は、データを暗号化する処理、および暗号化されたデータを復号する処理を実行する。暗号化復号部403は、通信部400を介して取得した装置(クライアント装置10、またはサーバ装置20)により

出力されたデータを暗号化する。また、暗号化復号部403は、通信部400を介して取得したネットワークNWからの暗号化されたデータを復号する。

[0047] 記憶部404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405と、秘密情報記憶部406とを備える。証明書情報記憶部405は、通信制御管理装置50が発行した装置（クライアント装置10、またはサーバ装置20）に対する証明書を記憶する。具体的には、クライアント側の通信制御装置30に装着されるICカード40の証明書情報記憶部405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405には、サーバ証明書を示す情報が記憶される。

[0048] 秘密情報記憶部406は、通信制御管理装置50が発行した装置（クライアント装置10、またはサーバ装置20）に対する秘密鍵を記憶する。具体的には、クライアント側の通信制御装置30に装着されるICカード40の秘密情報記憶部406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405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。

[0049] ここでは、通信制御管理装置50の構成について、図6を用いて説明する。図6は、図1に示す通信制御管理装置50の構成例を示すブロック図である。通信制御管理装置50は、例えば、NW（ネットワーク）通信部500と、制御部510と、記憶部520と、表示部530とを備える。

NW通信部500は、ネットワークNWに接続され、ネットワークNWを介して、通信制御装置30（31）と通信を行う。

[0050] 制御部510は、例えば、CPUなどのプロセッサを含む。制御部510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510は、通信制御管理装置50を統括的に制御する。また、制御部510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510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511、証明書発行部512、証明書更新部513、証明書管理部514、管理部515、および監視部516としての機能を実現するための処理を実行する。

[0051] 鍵生成部511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。

[0052] 証明書発行部512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。

[0053] 証明書更新部513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513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。

[0054] 証明書管理部514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514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514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514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514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。

[0055] 管理部515は、通信制御装置30(31)を管理する。例えば、管理部515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。監視部516は、クライアント装置10(10-1~10-N)の間の正規通信を、VLANタグTG1を含むパケットPA1による通信と定めた管理情報に基づき、クライアント装置10の間の通信を監視する。また、監視部516は、通信制御管理装置50と通信制御装置30(30-1~30-N)の間の正規通信を、VLANタグTG2を含むパケットPA2による通信と定めた管理情報に基づき、通信制御管理装置50と通信制御装置30の間の通信を監視する。或いは、監視部516は、通信制御管理装置50と通信制御装置30-1の間の正規通信を、VLANタグTG2を含むパケットPA2による通信と定めた管理情報に基づき、通信制御管理装置50と通信制御装置30-1の通信を監視し、通信制御管理装置50と通信制御装置30-2の間の正規通信を、VLANタグTG3を含むパケットPA3による通信と定めた管理情報に基づき、通信制御管理装置50と通信制御装置30-2の通信を監視する。

[0056] 記憶部520は、非一時的なコンピュータ可読記憶媒体としてのメモリであり、制御部510の動作プログラム等を記憶する。制御部510は、動作プログラムに基づき動作し、各機能を実現する。例えば、制御部510は、動作プログラムに基づき動作し、通信制御装置30に対して制御コマンドを送信することにより通信制御装置30を制御する。また、制御部510は、動作プログラムに基づき動作し、通信制御装置30に対してアラート情報を送信する。

また、記憶部520は、送信先リスト(通信許可リスト)を記憶する。送信先リストは、通信が許可された通信相手を特定するための情報を含む。例えば、通信相手を特定するための情報は、URL(Uniform Resource Locator)である。本実施形態では、記憶部520に記憶される送信先リストは、クライアント装置10(10-1~10-N)を特定するための識別情報を含

む。

[0057] また、記憶部520は、例えば、鍵情報記憶部521と、証明書情報記憶部522とを備える。鍵情報記憶部521は、例えば既に発行済みの公開鍵や、秘密鍵を示す情報を記憶する。証明書情報記憶部522は、例えば既に発行済みの証明書を示す情報を記憶する。鍵情報記憶部521と、証明書情報記憶部522とは、例えば、鍵生成部511が秘密鍵を発行する際、証明書発行部512が証明書を発行する際などに参照される。また、鍵情報記憶部521には、鍵生成部511が発行した秘密鍵を示す情報が記憶される。また、証明書情報記憶部522には、証明書発行部512が発行した証明書を示す情報が記憶される。

[0058] 表示部530は、攻撃された通信経路に関する情報を表示する。例えば、通信経路VP1が攻撃されていることが特定された場合には、表示部530は、通信経路VP1が攻撃されていること、通信経路VP1に異常が発生していること、通信経路VP1の通信が遮断されたことを表示する。

[0059] 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。

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。

[0060] クライアント装置10は、撮像データをサーバ装置20に送信する場合、まずサーバ装置20に対するHTTPリクエストを送信する（ステップS1）。クライアント装置10が送信したHTTPリクエストは、クライアント側の通信制御装置30により取得される（ステップS2）。

[0061] 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31に対して、HTTPSのリクエスト（ClientHello）を送信する（ステップS3）。これにより、クライアント側の通信制御装置30とサーバ側の通信制御装置31との間のハンドシェイクが開始される（ステップS4）。

[0062] 具体的には、クライアント側の通信制御装置30が送信するClientHelloに

は、例えば、T L S 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、ClientHello に対する応答として、クライアント側の通信制御装置 3 0 に対し H T T P S のレスポンス (ServerHello) を送信する。サーバ側の通信制御装置 3 1 が送信する ServerHello には、例えば ClientHello で提示された選択肢の中でサーバ装置 2 0 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 3 0 からの提示に対し、サーバ側の通信制御装置 3 1 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。

[0063] そして、サーバ側の通信制御装置 3 1 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 2 0 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 1 0 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 3 0 は、サーバ側の通信制御装置 3 1 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。

[0064] 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 3 0 は、今までに受信した ServerHello 等から署名を生成し、サーバ側の通信制御装置 3 1 に送信する。サーバ側の通信制御装置 3 1 は、クライアント側の通信制御装置 3 0 から受信した署名を、クライアント側の通信制御装置 3 0 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 3 1 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 3 0 のものであると判定する。また、サーバ側の通信制御装置 3 1 は、今までに受信した ClientHello 等から署名を生成し、クライアント側の通信制御装置 3 0 に送信する。クライアント側の通信制御装置 3 0 は、サーバ側の通信制御装置 3 1 から受信した署名を、サーバ側の通信制御装置 3 1 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 3 0 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 3 1 のも

のであると判定する。

- [0065] 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。
- [0066] 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。
- [0067] 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。
- [0068] 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)。
- [0069] 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S12）。クライアント装置10は、復号されたHTTPレスポンスを受信する（ステップS13）。このとき、クライアント装置10は、サーバ装置20からHTTPレスポンスが応答されたと認識する。このため、クライアント装置10は、サーバ装置20に対し、撮像データを送信する（ステップS14）。

[0070] クライアント装置10が送信した撮像データは、クライアント側の通信制御装置30により取得される（ステップS15）。クライアント側の通信制御装置30は、クライアント装置10により送信された撮像データを、共通鍵を用いて暗号化する（ステップS16）。クライアント側の通信制御装置30により暗号化された撮像データは、ネットワークNWを介してサーバ側の通信制御装置31に受信される（ステップS17）。

[0071] サーバ側の通信制御装置31は、受信した撮像データを、共通鍵を用いて復号する（ステップS18）。サーバ側の通信制御装置31により復号された撮像データは、サーバ装置20にとり取得される（ステップS19）。サーバ装置20は、復号された撮像データを受信する（ステップS20）。このとき、サーバ装置20は、クライアント装置10からの撮像データを受信したと認識する。

[0072] なお、上記フローチャートのステップS4において、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なかった場合、クライアント側の通信制御装置30は、通信先との通信を許可しない。具体的には、クライアント側の通信制御装置30は、通信先から送信された情報をクライアント装置10に出力しない。相互認証が正しく行われなかった場合、通信先がサーバ側の通信制御装置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は、例えば、相互認証が正しく行われなかった場合の通信記録を通信制御管理装置50に送信するようにしてもよい。これより、通信制御管理装置50は相互認証が正しく行われなかった場合の通信記録を取

得することができ、管理下にあるクライアント側の通信制御装置 30 に対する不正な通信のパターンや頻度を把握することで、ネットワークの異常を監視することができる。

[0073] 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 S 4 において行われるハンドシェイクにおいて相互認証の代わりにクライアント装置 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。

[0074] 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 50 に送信するようにしてもよい。この場合、例えば、通信制御管理装置 50 は、クライアント側の通信制御装置 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 50 により送信先リストが更新されることで、通信制御管理装置 50 が管理下にあるクライアント側の通信制御装置 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。

[0075] また、クライアント側の通信制御装置 30 は、ステップ S 4 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 30 の制御部 33 は、ネットワーク NW を介してクライアント装置 10 のファームウェアの更新プログラムが送信された場合、検証用の鍵（検証鍵）を用いて検証する。この場合、通信制御管理装置 50 は、例えば、クライアント側の通信制御装置 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。

[0076] 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。

[0077] 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。

[0078] これにより、クライアント装置 10 は、検証済みである正しい内容であることが検証された情報のみを受け取ることができる。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。

[0079] 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。

[0080] 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 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。

[0081] 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、いずれか一方の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

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。

[0082] 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たと、管理が面倒になってしまい、パスワードをメモに残したり、ウェブブラウザに記録させたりするなど、かえってパスワードが漏洩してしまう場合があった。

[0083] これに対し、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。

[0084] 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。

る。

[0085] 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。

[0086] 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。

[0087] 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５０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。

[0088] 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。

[0089] 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。

[0090] 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。

[0091] また、通信システム１は、通信制御管理装置５０を更に備え、通信制御管理装置５０は、クライアント側の通信制御装置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５０により発行された正当な秘密鍵、証明書を用いて、ハンドシェイクを行い、共通鍵を決定することができ、上述した効果を奏する他、社会インフラシステムの安全性を更に向上させることができる。

- [0092] 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。
- [0093] 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。
- [0094] 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。
- [0095] 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５０に不正なアクセスの記録が送信されるようにしてもよい。通信制御管理装置５０は、不正なアクセスの有無を認識することができ、システム全体に対する大規模攻撃が開始される前の予兆の段階を検出して対策することが可能となる。
- [0096] 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５０に接続状態を示す情報が送信されるようにしてもよい。通信制御管理装置５０は、通信制御装置３０（３１）から接続状態を示す情報が受信できない場合などには、通信制御装置３０（３１）がクライアント装置１０またはサーバ装置２０から切り離された判断し、当該切り離された通信制御装置３０（３１）を無効とする。こうすることで通信制御管理装置５０は、切り離された通信制御装置３０（３１）が不正な装置に接続されてなりすましに悪用されることを抑制する。

[0097] 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。

[0098] 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５０等から、通信制御装置３０（３１）を介して、クライアント装置１０のプログラムを更新させるようにしてもよい。通信制御装置３０（３１）を介してプログラムの更新（ファームウェアのアップデート）が行われることにより、安全にクライアント装置１０の機能を更新させることができる。このようにサーバ装置２０からクライアント装置１０に対してファームウェアが送信される場合、サーバ装置２０から送信されるファームウェアには、例えばサーバ側の通信制御装置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。

[0099] また、このように通信制御装置30(31)を介して通信が行われることにより、サーバ装置20や通信制御管理装置50等からクライアント装置10にファームウェアを安全に更新することができるため、作業員が複数のクライアント装置10に対して物理的に各々のクライアント装置10が設置されている場所まで移動してファームウェアのアップデート作業を行う場合と比較して、作業コストを低減させることも可能である。

[0100] 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50等から、通信制御装置30(31)を介して、クライアント装置10の起動や停止を行ってもよい。通信制御装置30(31)を介して起動や停止(リモートアクティベーション)が行われることにより、安全にクライアント装置10の機能を更新させることができ、セキュアな遠隔制御を実現させることができる。

[0101] 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(Local Area Network)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。

[0102] 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。

[0103] (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 1 の構成例を示す図である。図 8 に示す通信システム 1 の各ハードウェア構成等は、既に説明した通りである。

[0104] 図 8 に示すように、通信制御装置 30-1 (第 1 の通信制御装置) は、ネットワーク接続装置 7 (スイッチ等) とクライアント装置 10-1 (第 1 のクライアント装置) との間に接続される。通信制御装置 30-2 (第 2 の通信制御装置) は、ネットワーク接続装置 7 とクライアント装置 10-2 (第 2 のクライアント装置) との間に接続される。同様に、通信制御装置 30-N (第 N の通信制御装置) は、ネットワーク接続装置 7 とクライアント装置 10-N (第 N のクライアント装置) との間に接続される。例えば、クライアント装置 10 は、IoT デバイスである。また、通信制御管理装置 50 は、ネットワーク接続装置 7 に接続され、通信制御装置 30-1 と通信制御装置 30-2 による通信を管理する。即ち、通信制御装置 30-N 及び通信制御管理装置 50 が、ネットワーク接続装置 7 を挟み込むように配置される。

[0105] 例えば、通信制御管理装置 50 は、通信制御装置 30-N に対して制御コマンドを送信し、所定の VLAN タグを含むパケットを生成させる。VLAN タグは、ID 等の識別情報を含む。また、通信制御管理装置 50 は、通信

制御装置 30-N から報告される通信内容に基づき通信異常を検出する。例えば、通信異常は、第三者によるネットワークへの攻撃であり、データの改ざん等を含む。

[0106] 通信制御装置 30-1 の NW 通信部 32 は、通信制御管理装置 50 から制御コマンドを受信する。通信制御装置 30-1 の制御部 33（第 1 のプロセッサ）は、通信制御管理装置 50 からの制御コマンド等に従い、VLAN タグ TG1（第 1 の仮想タグ）を含むパケット PA1（第 1 のパケット）を生成する。通信制御装置 30-1 の装置通信部 34（第 1 のインタフェース）は、VLAN タグ TG1 を含むパケット PA1 の送受信により、クライアント装置 10-1 と他のクライアント装置（例えばクライアント装置 10-2）の間の通信を仲介する。

[0107] 例えば、制御部 33 は、記憶部 36 に記憶された送信先リスト（通信許可リスト）に、クライアント装置 10-1 とクライアント装置 10-2 が登録されている場合に、クライアント装置 10-1 とクライアント装置 10-2 の通信を許可する。装置通信部 34 は、クライアント装置 10-1 から送信されるデータを受信し、制御部 33 は、受信したデータに基づき VLAN タグ TG1 を含むパケット PA1 を生成し、装置通信部 34 は、生成されたパケット PA1 をクライアント装置 10-2 へ送信する。なお、通信制御装置 30-1 が、クライアント装置 10-1 を制御し、クライアント装置 10-1 から送信されるデータを、VLAN タグ TG1 を含むパケット PA1 にしてもよい。

[0108] 通信制御装置 30-2 の NW 通信部 32 は、通信制御管理装置 50 から制御コマンドを受信する。通信制御装置 30-2 の制御部 33（第 2 のプロセッサ）は、通信制御管理装置 50 からの制御コマンド等に従い、VLAN タグ TG1（第 1 の仮想タグ）を含むパケット PA1（第 1 のパケット）を生成する。通信制御装置 30-2 の装置通信部 34（第 2 のインタフェース）は、VLAN タグ TG1 を含むパケット PA1 の送受信により、クライアント装置 10-2 と他のクライアント装置（例えばクライアント装置 10-1

)の間の通信を仲介する。

- [0109] 例えば、制御部33は、記憶部36に記憶された送信先リスト（通信許可リスト）に、クライアント装置10-1とクライアント装置10-2が登録されている場合に、クライアント装置10-1とクライアント装置10-2の通信を許可する。装置通信部34は、クライアント装置10-2から送信されるデータを受信し、制御部33は、受信したデータに基づきVLANタグTG1を含むパケットPA1を生成し、装置通信部34は、生成されたパケットPA1をクライアント装置10-1へ送信する。なお、通信制御装置30-2が、クライアント装置10-2を制御し、クライアント装置10-2から送信されるデータを、VLANタグTG1を含むパケットPA1にしてもよい。
- [0110] 通信制御管理装置50の制御部510は、各通信制御装置30-Nと通信するためのVLANタグTG2（第2の仮想タグ）を含むパケットPA2（第2のパケット）を生成する。通信制御管理装置50のNW通信部500は、VLANタグTG2を含むパケットPA2により各通信制御装置30-Nと通信する。例えば、NW通信部500は、VLANタグTG2を含むパケットPA2により通信制御装置30-1又は通信制御装置30-2と通信する。
- [0111] さらに、制御部510は、クライアント装置10（10-1～10-N）の間の正規通信を、VLANタグTG1を含むパケットPA1による通信と定めた管理情報に基づき、クライアント装置10の間の通信を監視する。また、制御部510は、通信制御管理装置50と通信制御装置30（30-1～30-N）の間の正規通信を、VLANタグTG2を含むパケットPA2による通信と定めた管理情報に基づき、通信制御管理装置50と通信制御装置30の間の通信を監視する。管理情報は、記憶部520等に記憶される。
- [0112] このように、通信システム1では、通信制御装置30及び通信制御管理装置50が、VLANタグを含むパケットにより通信することにより、論理的に通信経路を分けてセキュリティの向上を図る。第1の実施形態では、各ク

クライアント装置 10 の間の定常的な通信を VLAN タグ TG1 で特定される仮想の通信経路 VP1 で実行し、通信制御管理装置 50 と通信制御装置 30 の間の制御コマンド及びアラート情報の通信を VLAN タグ TG2 で特定される仮想の通信経路 VP2 で実行する。このように、論理的に通信経路 VP1 と VP2 を分けることにより、中間者攻撃を受けている経路と受けていない経路とで矛盾が生じた場合にその矛盾を検知することができ、どの通信経路で中間者攻撃を受けているかを容易に特定できる。また、攻撃された通信経路を遮断することにより、他の通信経路を守ることができる。

[0113] 図 9 は、第 1 の実施形態に係る通信システム 1 による通信監視の一例を示すフローチャートである。

[0114] 通信制御管理装置 50 の制御部 510 は、通信経路の通信異常を監視する。例えば、通信異常は、第三者によるネットワークへの攻撃であり、データの改ざん等を含む。制御部 510 は、記憶部 520 に記憶される送信先リスト（通信許可リスト）に基づき、通信が許可されたクライアント装置 10 による通信であることを確認し、通信経路のパケットに含まれる VLAN タグに基づき、パケットの矛盾を監視する（ST101）。例えば、制御部 510 は、パケットの矛盾を検知しなければ（ST102、NO）、通信経路への異常が無いものと判定し、監視を継続する（ST101）。制御部 510 は、通信経路のパケットの矛盾を検知すると（ST102、YES）、矛盾検知に応じた処理へ移行する。なお、制御部 510 は、通信が許可されたクライアント装置 10 による通信であることを確認できなければ、不正な通信と判定し、通信を遮断する。

例えば、制御部 510 は、クライアント装置 10（10-1～10-N）の間の通信経路 VP1 の正規通信を、VLAN タグ TG1 を含むパケット PA1 による通信と定めた管理情報に基づき、通信経路 VP1 を監視する。また、制御部 510 は、通信制御管理装置 50 と通信制御装置 30（30-1～30-N）の間の正規通信を、VLAN タグ TG2 を含むパケット PA2 による通信と定めた管理情報に基づき、通信経路 VP2 を監視する。

[0115] 制御部510は、通信経路VP1のパケットから検出されたVLANタグがVLANタグTG1と異なる場合に、通信経路VP1のパケットの矛盾を検知し(ST103、YES)、通信経路VP1で攻撃を受けていることを特定する(ST104)。制御部510は、通信経路VP1が攻撃されていることを示す警告情報の出力を指示し、表示部530は、通信経路VP1が攻撃されていることを示す警告情報を表示する(ST106)。また、制御部510は、ネットワークを攻撃から守るため、通信経路VP1の通信を遮断するようにしてもよい。

[0116] また、制御部510は、通信経路VP2のパケットから検出されたVLANタグがVLANタグTG2と異なる場合に、通信経路VP2のパケットの矛盾を検知し(ST103、NO)、通信経路VP2で攻撃を受けていることを特定する(ST105)。制御部510は、通信経路VP2が攻撃されていることを示す警告情報の出力を指示し、表示部530は、通信経路VP2が攻撃されていることを示す警告情報を表示する(ST105)。制御部510は、ネットワークを攻撃から守るため、通信経路VP2の通信を遮断するようにしてもよい。

[0117] (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。

第1の実施形態に係る通信システム1は、通信制御管理装置50が、2台のクライアント装置10の間の通信経路と、通信制御管理装置50とクライアント装置10の間の通信経路とを異なる通信経路にして、攻撃された通信経路を特定する。ここで説明する第2の実施形態に係る通信システム1は、通信制御管理装置50が、2台のクライアント装置10の間の通信経路と、通信制御管理装置50とクライアント装置10の間の通信経路VP2とを異なる通信経路にした上で、さらに、通信制御管理装置50と各クライアント装置10の間の通信経路を異なる通信経路にして、攻撃された通信経路を特定する。第2の実施形態の説明では、第1の実施形態との相違部分を中心に説明し、共通部分については適宜省略する。

図10は、第2の実施形態に係る通信システム1の構成例を示す図である。図10に示す通信システム1の各ハードウェア構成等は、既に説明した通りである。

[0118] 通信制御管理装置50の制御部510は、各通信制御装置30-Nと通信するための異なるVLANタグを含む異なるパケットを生成する。つまり、制御部510は、通信制御装置30-1と通信するためのVLANタグTG2（第2の仮想タグ）を含むパケットPA2（第2のパケット）を生成し、通信制御装置30-2と通信するためのVLANタグTG3（第3の仮想タグ）を含むパケットPA3（第3のパケット）を生成する。通信制御管理装置50のNW通信部500は、異なるVLANタグを含む異なるパケットにより各通信制御装置30-Nと通信する。つまり、NW通信部500は、VLANタグTG2を含むパケットPA2により通信制御装置30-1と通信し、また、VLANタグTG3を含むパケットPA3により通信制御装置30-2と通信する。

[0119] さらに、制御部510は、クライアント装置10（10-1～10-N）の間の正規通信を、VLANタグTG1を含むパケットPA1による通信と定めた管理情報に基づき、クライアント装置10の間の通信を監視する。また、制御部510は、通信制御管理装置50と通信制御装置30-1の間の正規通信を、VLANタグTG2を含むパケットPA2による通信と定め、通信制御管理装置50と通信制御装置30-2の間の正規通信を、VLANタグTG3を含むパケットPA3による通信と定めた管理情報に基づき、通信制御管理装置50と通信制御装置30-1の間の通信を監視し、通信制御管理装置50と通信制御装置30-2の間の通信を監視する。

[0120] このように、通信システム1では、通信制御装置30及び通信制御管理装置50が、VLANタグを含むパケットにより通信することにより、論理的に通信経路を分けてセキュリティの向上を図る。第2の実施形態では、各クライアント装置10の間の定常的な通信をVLANタグTG1で特定される通信経路VP1で実行し、通信制御管理装置50と通信制御装置30-1の

間の制御コマンド及びアラート情報の通信をVLANタグTG2で特定される通信経路VP2で実行し、通信制御管理装置50と通信制御装置30-2の間の制御コマンド及びアラート情報の通信をVLANタグTG3で特定される通信経路VP3で実行する。このように、論理的に通信経路VP1とVP2とVP3を分けることにより、中間者攻撃を受けている経路と受けていない経路とで矛盾が生じた場合にその矛盾を検知することができ、どの通信経路で中間者攻撃を受けているかを容易に特定できる。また、攻撃された通信経路を遮断することにより、他の通信経路を守ることができる。

[0121] 図11は、第2の実施形態に係る通信システム1による通信監視の一例を示すフローチャートである。

[0122] 通信制御管理装置50の制御部510は、通信経路の通信異常を監視する。例えば、通信異常は、第三者によるネットワークへの攻撃であり、データの改ざん等を含む。制御部510は、記憶部520に記憶される送信先リスト（通信許可リスト）に基づき、通信が許可されたクライアント装置10による通信であることを確認し、通信経路のパケットに含まれるVLANタグに基づき、パケットの矛盾を監視する（ST201）。例えば、制御部510は、パケットの矛盾を検知しなければ（ST202、NO）、通信経路への異常が無いものと判定し、監視を継続する（ST201）。制御部510は、通信経路のパケットの矛盾を検知すると（ST202、YES）、矛盾検知に応じた処理へ移行する。なお、制御部510は、通信が許可されたクライアント装置10による通信であることを確認できなければ、不正な通信と判定し、通信を遮断する。

例えば、制御部510は、クライアント装置10（10-1～10-N）の間の通信経路VP1の正規通信を、VLANタグTG1を含むパケットPA1による通信と定めた管理情報に基づき、通信経路VP1を監視する。また、制御部510は、通信制御管理装置50と通信制御装置30-1の間の正規通信を、VLANタグTG2を含むパケットPA2による通信と定めた管理情報に基づき、通信経路VP2を監視する。また、制御部510は、通

信制御管理装置 50 と通信制御装置 30-2 の間の正規通信を、VLAN タグ TG3 を含むパケット PA3 による通信と定めた管理情報に基づき、通信経路 VP3 を監視する。

- [0123] 制御部 510 は、通信経路 VP1 のパケットから検出された VLAN タグが VLAN タグ TG1 と異なる場合に、通信経路 VP1 のパケットの矛盾を検知し (ST203、YES)、通信経路 VP1 で攻撃を受けていることを特定する (ST205)。制御部 510 は、通信経路 VP1 が攻撃されていることを示す警告情報の出力を指示し、表示部 530 は、通信経路 VP1 が攻撃されていることを示す警告情報を表示する (ST208)。また、制御部 510 は、ネットワークを攻撃から守るため、通信経路 VP1 の通信を遮断するようにしてもよい。
- [0124] また、制御部 510 は、通信経路 VP2 のパケットから検出された VLAN タグが VLAN タグ TG2 と異なる場合に、通信経路 VP2 のパケットの矛盾を検知し (ST204、YES)、通信経路 VP2 で攻撃を受けていることを特定する (ST206)。制御部 510 は、通信経路 VP2 が攻撃されていることを示す警告情報の出力を指示し、表示部 530 は、通信経路 VP2 が攻撃されていることを示す警告情報を表示する (ST208)。制御部 510 は、ネットワークを攻撃から守るため、通信経路 VP2 の通信を遮断するようにしてもよい。
- [0125] また、制御部 510 は、通信経路 VP3 のパケットから検出された VLAN タグが VLAN タグ TG3 と異なる場合に、通信経路 VP3 のパケットの矛盾を検知し (ST204、NO)、通信経路 VP3 で攻撃を受けていることを特定する (ST207)。制御部 510 は、通信経路 VP3 が攻撃されていることを示す警告情報の出力を指示し、表示部 530 は、通信経路 VP3 が攻撃されていることを示す警告情報を表示する (ST208)。制御部 510 は、ネットワークを攻撃から守るため、通信経路 VP3 の通信を遮断するようにしてもよい。
- [0126] (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。

第3の実施形態は、第1及び第2の実施形態と組み合わせて実施する。第3の実施形態では、通信システム1は、1以上の複数のダミーの通信経路を生成する。

[0127] 例えば、通信システム1は、通信制御管理装置50と各クライアント装置10の間にダミーの通信経路を生成する。つまり、正規の通信経路VP2に並行してダミーの通信経路を生成する。例えば、通信制御管理装置50の制御部510は、VLANタグTG4（第4の仮想タグ）を含むパケットPA4（第4のパケット）を生成する。通信制御管理装置50のNW通信部500は、VLANタグTG4を含むパケットPA4により各通信制御装置30-Nとダミーの通信経路で通信する。攻撃者は、正規の通信経路VP1及びVP2と、ダミーの通信経路とを区別することができない。よって、ダミーの通信経路を生成することにより、正規の通信経路VP1及びVP2が攻撃されるリスクを低減できる。

[0128] また、通信システム1は、通信制御管理装置50と各クライアント装置10の間に異なるダミーの通信経路を生成してもよい。つまり、正規の通信経路VP2及びVP3のそれぞれに並行してダミーの通信経路を生成する。通信制御管理装置50の制御部510は、VLANタグTG4（第4の仮想タグ）を含むパケットPA4（第4のパケット）を生成する。通信制御管理装置50のNW通信部500は、VLANタグTG4を含むパケットPA4により各通信制御装置30-1とダミーの通信経路で通信する。同様に、制御部510は、VLANタグTG5（第5の仮想タグ）を含むパケットPA5（第5のパケット）を生成する。通信制御管理装置50のNW通信部500は、VLANタグTG5を含むパケットPA5により各通信制御装置30-2とダミーの通信経路で通信する。攻撃者は、正規の通信経路VP1、VP2、及びVP3と、ダミーの通信経路とを区別することができない。よって、ダミーの通信経路を生成することにより、正規の通信経路VP1及びVP2が攻撃されるリスクを低減することができる。

- [0129] さらに、通信システム 1 は、各クライアント装置 10 の間に異なるダミーの通信経路を生成してもよい。つまり、正規の通信経路 V P 1 に並行してダミーの通信経路を生成する。通信制御装置 30-1 の制御部 33 は、V L A N タグ T G 4（第 4 の仮想タグ）を含むパケット P A 4（第 4 のパケット）を生成する。装置通信部 34 は、V L A N タグ T G 4 を含むパケット P A 4 により各通信制御装置 30-2 とダミーの通信経路で通信する。また、通信制御装置 30-2 の制御部 33 は、V L A N タグ T G 4（第 4 の仮想タグ）を含むパケット P A 4（第 4 のパケット）を生成する。装置通信部 34 は、V L A N タグ T G 4 を含むパケット P A 4 により各通信制御装置 30-1 とダミーの通信経路で通信する。攻撃者は、正規の通信経路 V P 1 及び V P 2 と、ダミーの通信経路とを区別することができない。よって、ダミーの通信経路を生成することにより、正規の通信経路 V P 1 及び V P 2 が攻撃されるリスクを低減することができる。
- [0130] 上記説明した第 1 乃至第 3 の実施形態によれば、既存のデバイスを変更せずに不正アクセスの検出に優れた通信システム及びプログラムを提供することができる。各実施形態に係る通信システム 1 は、各装置間の通信経路を V L A N タグを用いて論理的に異なる通信経路にする。例えば、攻撃によって通信経路のパケットが偽装された場合であっても、パケットの矛盾から攻撃を受けている通信経路を特定することができ、さらに、攻撃を受けている通信経路を遮断することもできる。なお、論理的に異なる通信経路を構築するための手段として、V L A N タグのような識別情報を利用するケースについて説明したが、本実施形態はこれに限定されるものではなく、I P（Internet Protocol）アドレス等を用いて不正を検出するようにしてもよい。
- [0131] また、本実施形態に係るプログラムは、電子機器に記憶された状態で譲渡されてもよいし、電子機器に記憶されていない状態で譲渡されてもよい。後者の場合は、プログラムは、ネットワークを介して譲渡されてよいし、記憶媒体に記憶された状態で譲渡されてもよい。記憶媒体は、非一時的な有形の媒体である。記憶媒体は、コンピュータ可読媒体であり、通信システム 1 を

構成する各装置により読み取られ、実行される。記憶媒体は、ＣＤ－ＲＯＭ、メモリカード等のプログラムを記憶可能かつコンピュータで読取可能な媒体であればよく、その形態は問わない。

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] ネットワーク接続装置と第1のクライアント装置の間に接続される第1の通信制御装置、前記ネットワーク接続装置と第2のクライアント装置の間に接続される第2の通信制御装置、及び前記ネットワーク接続装置に接続され、前記第1の通信制御装置と第2の通信制御装置による通信を管理する通信制御管理装置を備える通信システムであって、
- 前記第1の通信制御装置は、
- 第1の仮想タグを含む第1のパケットを生成する第1のプロセッサと、
- 前記第1のパケットの送受信により前記第1のクライアント装置と前記第2のクライアント装置の間の通信を仲介する第1のインタフェースと、
- を備え、
- 前記第2の通信制御装置は、
- 前記第1の仮想タグを含む前記第1のパケットを生成する第2のプロセッサと、
- 前記第1のパケットの送受信により前記第1のクライアント装置と前記第2のクライアント装置の間の通信を仲介する第2のインタフェースと、
- を備え、
- 前記通信制御管理装置は、
- 第2の仮想タグを含む第2のパケットを生成する第3のプロセッサと、
- 前記第2のパケットにより前記第1の通信制御装置又は前記第2の通信制御装置と通信する第3のインタフェースと、
- を備え、
- 前記第3のプロセッサは、前記第1のクライアント装置と前記第2

のクライアント装置の間の正規通信を前記第1の仮想タグを含む前記第1のパケットによる通信と定め、前記通信制御管理装置と前記第1の通信制御装置又は第2の通信制御装置の間の正規通信を前記第2の仮想タグを含む前記第2のパケットによる通信と定めた管理情報に基づき、通信を監視する通信システム。

[請求項2] 前記第3のプロセッサは、前記第1のクライアント装置と前記第2のクライアント装置の間の第1の通信経路のパケットから検出される仮想タグが前記第1の仮想タグと矛盾する場合に、前記第1の通信経路の異常を検出する請求項1の通信システム。

[請求項3] 前記第3のプロセッサは、前記通信制御管理装置と前記第1の通信制御装置の間の第2の通信経路のパケット、又は前記通信制御管理装置と前記第2の通信制御装置の間の第2の通信経路のパケットから検出される仮想タグが前記第2の仮想タグと矛盾する場合に、前記第2の通信経路の異常を検出する請求項2の通信システム。

[請求項4] 前記通信制御管理装置は、
前記第1又は第2の通信経路の異常を表示する表示部を備える請求項3の通信システム。

[請求項5] 前記通信制御管理装置は、
前記第1のクライアント装置と前記第2のクライアント装置を特定する識別情報を含む通信許可リストを記憶するメモリを備え、
前記第3のプロセッサは、前記通信許可リストに基づき前記第1のクライアント装置と前記第2のクライアント装置の通信を許可する請求項1乃至4の何れか一つの通信システム。

[請求項6] 前記第1のクライアント装置と前記第2のクライアント装置の間の通信は、前記第1のクライアント装置又は前記第2のクライアント装置で生成された情報の送受信であり、
前記通信制御管理装置と前記第1のクライアント装置又は前記第2のクライアント装置の間の通信は、制御コマンド又は通信アラートの

送受信である請求項 1 乃至 5 の何れか一つの通信システム。

[請求項7] 前記第 1 の通信経路は、前記第 1 の仮想タグにより特定される仮想の通信経路であり、前記第 2 の通信経路は、前記第 2 の仮想タグにより特定される仮想の通信経路である請求項 3 又は 4 の通信システム。

[請求項8] ネットワーク接続装置と第 1 のクライアント装置の間に接続される第 1 の通信制御装置、前記ネットワーク接続装置と第 2 のクライアント装置の間に接続される第 2 の通信制御装置、及び前記ネットワーク接続装置に接続され、前記第 1 の通信制御装置と第 2 の通信制御装置の通信を管理する通信制御管理装置を備える通信システムであって、
前記第 1 の通信制御装置は、
第 1 の仮想タグを含む第 1 のパケットを生成する第 1 のプロセッサと、
前記第 1 のパケットの送受信により前記第 1 のクライアント装置と前記第 2 のクライアント装置の間の通信を仲介する第 1 のインタフェースと、
を備え、
前記第 2 の通信制御装置は、
前記第 1 の仮想タグを含む前記第 1 のパケットを生成する第 2 のプロセッサと、
前記第 1 のパケットの送受信により前記第 1 のクライアント装置と前記第 2 のクライアント装置の間の通信を仲介する第 2 のインタフェースと、
を備え、
前記通信制御管理装置は、
第 2 の仮想タグを含む第 2 のパケットを生成し、また、第 3 の仮想タグを含む第 3 のパケットを生成する第 3 のプロセッサと、
前記第 2 のパケットにより前記第 1 の通信制御装置と通信し、また

、前記第3の packets により前記第2の通信制御装置と通信する第3のインタフェースと、

を備え、

前記第3のプロセッサは、前記第1のクライアント装置と前記第2のクライアント装置の間の正規通信を前記第1の仮想タグを含む前記第1の packets による通信と定め、前記通信制御管理装置と前記第1の通信制御装置の間の正規通信を前記第2の仮想タグを含む前記第2の packets による通信と定め、前記通信制御管理装置と前記第2の通信制御装置の間の正規通信を前記第3の仮想タグを含む前記第3の packets による通信と定めた管理情報に基づき、通信を監視する通信システム。

[請求項9]

ネットワーク接続装置と第1のクライアント装置の間に接続される第1の通信制御装置、前記ネットワーク接続装置と第2のクライアント装置の間に接続される第2の通信制御装置、及び前記ネットワーク接続装置に接続され、前記第1の通信制御装置と第2の通信制御装置による通信を管理する通信制御管理装置に実行させるプログラムを記憶した非一時的コンピュータ可読記憶媒体であって、

前記第1の通信制御装置に、

第1の仮想タグを含む第1の packets を生成する手順と、

前記第1の packets の送受信により前記第1のクライアント装置と前記第2のクライアント装置の間の通信を仲介する手順とを実行させ、

前記第2の通信制御装置に、

前記第1の仮想タグを含む前記第1の packets を生成する手順と、

前記第1の packets の送受信により前記第1のクライアント装置と前記第2のクライアント装置の間の通信を仲介する手順とを実行させ、

前記通信制御管理装置に、

第2の仮想タグを含む第2のパケットを生成する手順と、

前記第2のパケットにより前記第1の通信制御装置又は前記第2の通信制御装置と通信する手順と、

前記第1のクライアント装置と前記第2のクライアント装置の間の正規通信を前記第1の仮想タグを含む前記第1のパケットによる通信と定め、前記通信制御管理装置と前記第1の通信制御装置又は第2の通信制御装置の間の正規通信を前記第2の仮想タグを含む前記第2のパケットによる通信と定めた管理情報に基づき、通信を監視する手順とを実行させるプログラムを記憶した非一時的コンピュータ可読記憶媒体。

[請求項10]

ネットワーク接続装置と第1のクライアント装置の間に接続される第1の通信制御装置、前記ネットワーク接続装置と第2のクライアント装置の間に接続される第2の通信制御装置、及び前記ネットワーク接続装置に接続され、前記第1の通信制御装置と第2の通信制御装置の通信を管理する通信制御管理装置に実行させるプログラムを記憶した非一時的コンピュータ可読記憶媒体であって、

前記第1の通信制御装置は、

第1の仮想タグを含む第1のパケットを生成する手順と、

前記第1のパケットの送受信により前記第1のクライアント装置と前記第2のクライアント装置の間の通信を仲介する手順とを実行し、

前記第2の通信制御装置は、

前記第1の仮想タグを含む前記第1のパケットを生成する手順と、

前記第1のパケットの送受信により前記第1のクライアント装置と前記第2のクライアント装置の間の通信を仲介する手順とを実行し、

前記通信制御管理装置は、

第2の仮想タグを含む第2のパケットを生成し、また、第3の仮想タグを含む第3のパケットを生成する手順と、

前記第2のパケットにより前記第1の通信制御装置と通信し、また

、前記第 3 のパケットにより前記第 2 の通信制御装置と通信する手順と、

前記第 1 のクライアント装置と前記第 2 のクライアント装置の間の正規通信を前記第 1 の仮想タグを含む前記第 1 のパケットによる通信と定め、前記通信制御管理装置と前記第 1 の通信制御装置の間の正規通信を前記第 2 の仮想タグを含む前記第 2 のパケットによる通信と定め、前記通信制御管理装置と前記第 2 の通信制御装置の間の正規通信を前記第 3 の仮想タグを含む前記第 3 のパケットによる通信と定めた管理情報に基づき、通信を監視する手順とを実行させるプログラムを記憶した非一時的コンピュータ可読記憶媒体。