

明 細 書

発明の名称：通信制御装置

技術分野

[0001] 本発明の実施形態は、通信制御装置に関する。

背景技術

[0002] 通信制御装置には、IoT機器などのクライアント装置とインターネットなどのネットワークとの間の通信を中継するものがある。そのような通信制御装置には、クライアント装置がウイルス感染などの攻撃を受けたことを検知した場合、ネットワークとの通信を遮断する。

[0003] 従来、通信制御装置は、攻撃に関する情報をクライアント装置から取得することができないという課題がある。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開2014-103503号公報

発明の概要

[0005] 上記の課題を解決するため、攻撃に関する情報をクライアント装置から取得することができる通信制御装置を提供する。

[0006] 実施形態によれば、装置とネットワークとの間に接続される通信制御装置であって、第1の通信部と、第2の通信部と、制御部と、を備える。第1の通信部は、前記装置とデータを送受信する。第2の通信部は、前記ネットワークとデータを送受信する。制御部は、前記第1の通信部を通じて前記装置からデータを受信し、前記データに基づいて、前記装置が攻撃されているかを判定し、前記装置が攻撃されていると判定すると、前記ネットワークとの通信を遮断し、前記第1の通信部を通じて前記装置から前記装置への攻撃に関する攻撃情報を取得する。

図面の簡単な説明

[0007] [図1]図1は、実施形態に係る通信制御システムの構成例を示すブロック図で

ある。

[図2]図2は、実施形態に係るサーバ装置及びクライアント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の動作例を示すフローチャートである。

発明を実施するための形態

[0008] 以下、実施形態に係る通信制御システムについて図面を参照して説明する。

[0009] 図1は、実施形態の通信制御システム1の構成例を示す図である。通信制御システム1は、クライアント装置10（10-1～10-N）と、サーバ装置20と、クライアント側通信制御装置30（30-1～30-N）と、サーバ側通信制御装置40と、通信制御管理装置50と、ネットワーク60と、ゲートウェイ70と、を備える。

[0010] なお、通信制御システム1は、図1が示すような構成の他に必要に応じた構成を具備したり、通信制御システム1から特定の構成が除外されたりしてもよい。

[0011] 以下の説明においては、ネットワーク60と、ネットワーク60とクライアント装置10等とを接続するゲートウェイ70と、をまとめて「ネットワークNW」とも称する。

[0012] クライアント装置10は、クライアント側通信制御装置30を介してネットワークNWと接続する。クライアント装置10は、ネットワークNWを介してサーバ装置20などとデータを送受信する。クライアント装置10については後述する。

[0013] サーバ装置20は、サーバ側通信制御装置40を介してネットワークNWと接続する。

サーバ装置20は、クライアント装置10を管理する。たとえば、サーバ装

置 2 0 は、クライアント装置 1 0 へ種々のコマンドを送信する。また、サーバ装置 2 0 は、クライアント装置 1 0 から種々のデータを受信する。サーバ装置 2 0 については後述する。

[0014] クライアント側通信制御装置 3 0 は、クライアント装置 1 0 とネットワーク NW との間に接続され、クライアント装置 1 0 とサーバ装置 2 0 との間の通信を仲介する。クライアント側通信制御装置 3 0 は、クライアント装置 1 0 によりサーバ装置 2 0 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 2 0 に対して出力する。なお、クライアント側通信制御装置 3 0 は、サーバ装置 2 0 に対してデータを送信する際に、クライアント装置 1 0 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 2 0 に対して送信してもよい。

[0015] また、クライアント側通信制御装置 3 0 は、サーバ装置 2 0 によりクライアント装置 1 0 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 1 0 に対して出力する。たとえば、クライアント側通信制御装置 3 0 が取得するデータは、暗号化されたデータであってもよい。この場合、クライアント側通信制御装置 3 0 は、クライアント装置 1 0 にデータを出力する際に、サーバ装置 2 0 からサーバ側通信制御装置 4 0 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 1 0 に出力する。

[0016] サーバ側通信制御装置 4 0 は、サーバ装置 2 0 とネットワーク NW との間に接続され、クライアント装置 1 0 とサーバ装置 2 0 との間の通信を仲介する。サーバ側通信制御装置 4 0 は、サーバ装置 2 0 によりクライアント装置 1 0 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 1 0 に対して送信する。なお、サーバ側通信制御装置 4 0 は、クライアント装置 1 0 に対してデータを送信する際に、サーバ装置 2 0 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 1 0 に対して送信してもよい。

[0017] また、サーバ側通信制御装置 4 0 は、クライアント装置 1 0 によりサーバ装置 2 0 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。たとえば、サーバ側通信制御装置40が取得するデータは、暗号化されたデータであってもよい。この場合、サーバ側通信制御装置40は、サーバ装置20にデータを出力する際に、クライアント装置10からクライアント側通信制御装置30を介して取得したデータを復号し、復号したデータをサーバ装置20に出力する。

[0018] 実施形態において、たとえば、クライアント側通信制御装置30及びサーバ側通信制御装置40は、SSL (Secure Socket Layer) / TLS (Transport Layer Security) のプロトコルによってデータを暗号化する。たとえば、クライアント側通信制御装置30及びサーバ側通信制御装置40は、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) として送信する。

[0019] なお、クライアント側通信制御装置30及びサーバ側通信制御装置40が行うデータの暗号化は、HTTPをHTTPSとすることに限定されない。クライアント側通信制御装置30及びサーバ側通信制御装置40は、SSL / TLS プロトコルを種々の通信プロトコルと組み合わせることにより、安全性を向上させたセキュアな通信プロトコルに置き換えてもよい。例えば、クライアント側通信制御装置30及びサーバ側通信制御装置40は、FTP (File Transfer Protocol) をFTPS (FTP Secure) に置き換えてもよい。

[0020] 通信制御管理装置50は、クライアント側通信制御装置30及びサーバ側通信制御装置40などを管理する。たとえば、通信制御管理装置50は、クライアント側通信制御装置30に対し、クライアント証明書及び秘密鍵などを発行する。また、通信制御管理装置50は、サーバ側通信制御装置40に対し、サーバ証明書及び秘密鍵などを発行する。

[0021] 次に、クライアント装置10及びサーバ装置20の構成について説明する。たとえば、クライアント装置10とサーバ装置20とは、社会インフラシステムを構築する構成要素（コンポーネント）である。社会インフラとは、

例えば、道路交通網、発電設備、配送電設備、水処理設備、又はガス配給設備等、社会基盤を整えるために必要な設備である。社会インフラシステムとは、例えば、社会インフラを監視し、状況の変化を把握し、その変化に対応することにより、社会インフラを安定的に動作させる仕組みである。以下においては、クライアント装置１０とサーバ装置２０とは、道路や公共設備などを監視する監視システムのコンポーネントである場合を例に説明する。この場合、クライアント装置１０は、道路の状況等が撮像された撮像データを、ネットワークNWを介して送信する装置（ネットワーク監視カメラ）である。サーバ装置２０は、クライアント装置１０により送信された撮像データを、ネットワークNWを介して受信する装置である。

[0022] 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２０とは、発電設備又は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。また、クライアント装置１０とサーバ装置２０とは、物流センタにおける配送状況を取得するシステム、又は、工場若しくは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。

[0023] クライアント装置１０とサーバ装置２０とが用いられるシステム又はクライアント装置１０とサーバ装置２０との機能は、特定の構成に限定されるものではない。

[0024] 次に、クライアント装置１０及びサーバ装置２０について説明する。

図２は、クライアント装置１０及びサーバ装置２０の構成例を示すブロック図である。

[0025] 図２が示すように、クライアント装置１０は、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。クライアント制御部１２と、ネットワーク通信部１１及び撮像部１３とは、互いに通信可能に接続する。なお、クライアント装置１０は、図２が示すような構成の他に必要に応じた構成を具備したり、クライアント装置１０から特定の構成が除外さ

れたりしてもよい。

- [0026] ネットワーク通信部 11 は、クライアント側通信制御装置 30 とデータを送受信するためのインターフェースである。ネットワーク通信部 11 は、クライアント側通信制御装置 30 に接続される。ネットワーク通信部 11 は、クライアント制御部 12 からサーバ装置 20 に対して送信されるデータをクライアント側通信制御装置 30 に出力する。また、ネットワーク通信部 11 は、クライアント側通信制御装置 30 からのデータをクライアント制御部 12 へ出力する。たとえば、ネットワーク通信部 11 は、LAN 接続をサポートする。
- [0027] クライアント制御部 12 は、クライアント装置 10 を統括的に制御する。たとえば、クライアント制御部 12 は、サーバ装置 20 からの制御に従い、撮像部 13 に撮像を開始又は停止させたり、撮像部 13 に対し撮像するカメラの方向又は撮像する際の倍率等の撮像条件を設定したりする。
- [0028] クライアント制御部 12 は、プロセッサなどから構成される。たとえば、クライアント制御部 12 は、プロセッサ及びメモリなどから構成されてもよい。また、クライアント制御部 12 は、ASIC (application specific integrated circuit) 又は FPGA (field-programmable gate array) などから構成されてもよい。
- [0029] 撮像部 13 は、クライアント制御部 12 の指示に従い、所定箇所を撮像する。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。たとえば、撮像部 13 は、CCD (Charge Coupled Device) などから構成されるカメラを備える。
- [0030] なお、クライアント装置 10 は、撮像部 13 以外の機器を備えるものであってもよい。
- たとえば、クライアント装置 10 は、種々のセンサ、照明、空調、スピーカ又はマイクなどを備えるものであってもよい。
- [0031] また、クライアント装置 10 は、デスクトップ PC、ノート PC、タブレット PC、スマートフォン又はウェアラブル端末などであってもよい。

クライアント装置１０の構成は、特定の構成に限定されるものではない。

[0032] 図２が示すように、サーバ装置２０は、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。サーバ制御部２２と、ネットワーク通信部２１及び撮像データ記憶部２３とは、互いに通信可能に接続する。なお、サーバ装置２０は、図２が示すような構成の他に必要に応じた構成を具備したり、サーバ装置２０から特定の構成が除外されたりしてもよい。

[0033] ネットワーク通信部２１は、サーバ側通信制御装置４０とデータを送受信するためのインターフェースである。ネットワーク通信部２１は、サーバ側通信制御装置４０に接続される。ネットワーク通信部２１は、サーバ装置２０からクライアント装置１０に対して送信されるデータをサーバ側通信制御装置４０に出力する。また、ネットワーク通信部２１は、サーバ側通信制御装置４０からのデータをサーバ制御部２２へ出力する。たとえば、ネットワーク通信部２１は、ＬＡＮ接続をサポートする。

[0034] サーバ制御部２２は、サーバ装置２０を統括的に制御する。たとえば、サーバ制御部２２は、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。サーバ制御部２２は、プロセッサなどから構成される。たとえば、サーバ制御部２２は、プロセッサ及びメモリなどから構成されてもよい。

[0035] 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。撮像データ記憶部２３は、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、又はフラッシュメモリなどから構成される。

[0036] 次に、クライアント側通信制御装置３０について説明する。

図３は、クライアント側通信制御装置３０の構成例を示すブロック図である。

[0037] 図３に示すように、クライアント側通信制御装置３０は、ネットワーク通信部３１（第２の通信部）と、プロセッサ３２と、装置通信部３３（第１の通信部）と、メモリ３４とを備える。プロセッサ３２と、ネットワーク通信

部 3 1 及び装置通信部 3 3 とは、互いに通信可能に接続する。なお、クライアント側通信制御装置 3 0 は、図 3 が示すような構成の他に必要に応じた構成を具備したり、クライアント側通信制御装置 3 0 から特定の構成が除外されたりしてもよい。

[0038] ネットワーク通信部 3 1 は、ネットワーク NW とデータを送受信するためのインターフェースである。ネットワーク通信部 3 1 は、ネットワーク NW に接続される。ネットワーク通信部 3 1 は、ネットワーク NW を介して、他のクライアント側通信制御装置 3 0 及びサーバ側通信制御装置 4 0 と通信を行う。即ち、ネットワーク通信部 3 1 は、プロセッサ 3 2 からサーバ装置 2 0 に対して送信されるデータをネットワーク NW に出力する。また、ネットワーク通信部 3 1 は、ネットワーク NW からのデータをプロセッサ 3 2 へ出力する。たとえば、ネットワーク通信部 3 1 は、LAN 接続をサポートする。

[0039] プロセッサ 3 2 は、クライアント側通信制御装置 3 0 を統括的に制御する。プロセッサ 3 2 は、ネットワーク通信部 3 1 及び装置通信部 3 3 を用いて、クライアント装置 1 0 とネットワーク NW との間の通信を仲介する。即ち、プロセッサ 3 2 は、装置通信部 3 3 を通じてクライアント装置 1 0 から受信したデータを、ネットワーク通信部 3 1 を通じてネットワーク NW へ送信する。また、プロセッサ 3 2 は、ネットワーク通信部 3 1 を通じて受信したデータを、装置通信部 3 3 を通じてクライアント装置 1 0 へ送信する。

[0040] たとえば、プロセッサ 3 2 は、メモリ 3 4 などに格納される制御プログラムを実行する。また、プロセッサ 3 2 は、ASIC (application specific integrated circuit) 又は FPGA (field-programmable gate array) などから構成されてもよい。

[0041] 装置通信部 3 3 は、クライアント装置 1 0 とデータを送受信するためのインターフェースである。装置通信部 3 3 は、クライアント装置 1 0 に接続され、クライアント装置 1 0 と通信を行う。即ち、装置通信部 3 3 は、プロセッサ 3 2 からのデータをクライアント装置 1 0 に出力する。また、装置通信

部33は、クライアント装置10からのデータをプロセッサ32へ出力する。たとえば、装置通信部33は、LAN接続をサポートする。

[0042] メモリ34は、種々のデータを格納する。たとえば、メモリ34は、ROM、RAM及びNVMとして機能する。

たとえば、メモリ34は、制御プログラム及び制御データなどを記憶する。制御プログラム及び制御データは、クライアント側通信制御装置30の仕様に依拠して予め組み込まれる。たとえば、制御プログラムは、クライアント側通信制御装置30で実現する機能をサポートするプログラムなどである。

[0043] また、メモリ34は、プロセッサ32の処理中のデータなどを一時的に格納する。また、メモリ34は、アプリケーションプログラムの実行に必要なデータ及びアプリケーションプログラムの実行結果などを格納してもよい。

[0044] メモリ34は、ネットワークNWへデータを転送することが許可される通信を示すホワイトリストを予め格納する。たとえば、ホワイトリストは、宛先、宛先のポート、送信元のポート、プロトコル又はそれらの組合せなどから構成される。また、ホワイトリストは、通信が許可される期間などを示すものであってもよい。

[0045] また、メモリ34は、攻撃を特定するための攻撃毎の辞書情報を含む攻撃リストを格納する。たとえば、通信制御管理装置50は、攻撃リストをクライアント側通信制御装置30へ送信する。ネットワーク通信部31は、通信制御管理装置50等から送信される攻撃リストを受信する。プロセッサ32は、通信制御管理装置50等から送信される攻撃リストをメモリ34に格納する。たとえば、攻撃リストに含まれる辞書情報は、攻撃（攻撃手法又はウイルスなど）の特徴などを示す情報である。また、辞書情報は、学習によって構築されたAIモデルなどであってもよい。

[0046] 次に、クライアント側通信制御装置30が実現する機能について説明する。クライアント側通信制御装置30が実現する機能は、プロセッサ32によって実現される。

[0047] まず、プロセッサ32は、クライアント装置10からのデータに基づいて

クライアント装置 10 が攻撃されているかを判定する機能を有する。

[0048] クライアント装置 10 は、攻撃者からの攻撃によって不正な動作を行うことがある。たとえば、クライアント装置 10 は、攻撃者の所持する装置（パソコン又はメモリなど）を接続され、装置から不正なコマンド又はウイルスなどを入力される。クライアント装置 10 は、不正なコマンド又はウイルス感染などによって不正な動作を行う。また、クライアント装置 10 は、ネットワーク NW からのデータによってウイルスなどに感染することもある。

[0049] プロセッサ 32 は、クライアント装置 10 からのデータをネットワーク NW に中継する際に、クライアント装置 10 からのデータに基づいてクライアント装置 10 が攻撃されているかを判定する。

[0050] プロセッサ 32 は、クライアント装置 10 からのデータを受信すると、メモリ 34 が格納するホワイトリストを参照してクライアント装置 10 が攻撃されているかを判定する。

即ち、プロセッサ 32 は、クライアント装置 10 からのデータが、ホワイトリストが示す通信以外の通信によって送信される場合、クライアント装置 10 が攻撃されていると判定する。

[0051] なお、プロセッサ 32 は、人工知能によって攻撃されているかを判定してもよい。たとえば、プロセッサ 32 は、判定用の AI モデルを予め格納し、クライアント装置 10 からのデータとモデルとをマッチングさせて攻撃されているかを判定してもよい。

[0052] クライアント装置 10 が攻撃されているかを判定する方法は、特定の方法に限定されるものではない。

[0053] また、プロセッサ 32 は、クライアント装置 10 が攻撃されていると判定すると、ネットワーク NW との通信を遮断する機能を有する。

[0054] 即ち、プロセッサ 32 は、クライアント装置 10 からのデータをネットワーク NW へ転送しない。また、プロセッサ 32 は、ネットワーク NW からのデータをクライアント装置 10 へ転送しない。

[0055] また、プロセッサ 32 は、クライアント装置 10 とデータを送受信するこ

とで、クライアント装置１０への攻撃に関する情報（攻撃情報）を取得する機能を有する。

攻撃情報は、攻撃に用いられる攻撃機器固有情報又は通信日時情報などを含む。

[0056] プロセッサ３２は、ネットワークNWへの通信を遮断した後も、クライアント装置１０との通信を維持する。プロセッサ３２は、クライアント装置１０との通信によって種々のデータをクライアント装置１０から取得する。

[0057] たとえば、プロセッサ３２は、所定の情報を取得するためのコマンド（情報取得コマンド）を送信する。情報取得コマンドは、クライアント装置１０の状態などを取得する。たとえば、情報取得コマンドは、クライアント装置１０の型番又はバージョンなど、クライアント装置１０自体に関する情報を取得する。また、情報取得コマンドは、クライアント装置１０で動作しているアプリケーション、プロセッサなどの使用率若しくは温度、又は、メモリの使用率など、クライアント装置１０の動作に関する情報を取得してもよい。また、情報取得コマンドは、クライアント装置１０に接続する機器を示す情報（攻撃機器固有情報）を取得するものであってもよい。たとえば、情報取得コマンドは、攻撃者がクライアント装置１０に接続した情報処理装置を示す情報を取得する。

なお、情報取得コマンドが取得する情報は、特定の構成に限定されるものではない。

[0058] プロセッサ３２は、情報取得コマンドによって得られた情報を攻撃情報として取得する。なお、プロセッサ３２は、複数の情報取得コマンドをクライアント装置１０に送信してもよい。

[0059] また、プロセッサ３２は、攻撃情報を取得するためのセキュリティ上のハニーポットを構築する。たとえば、プロセッサ３２は、ハニーポットとして、仮想のプラットフォーム上にシステムを構築する。つまり、ハニーポットは、脆弱性が判明しているOSやアプリケーションをそのまま使用したり、それらのOSをエミュレートした構成を具現化したプログラムを実行して構

築することができる。なお、これらのいわゆる高対話型、低対話型に限らず、製品化する時点で知られている様々なタイプのハニーポットを用いることができる。

[0060] プロセッサ32は、ハニーポットを通じてクライアント装置10に対してダミーデータを送信する。たとえば、プロセッサ32は、ネットワークNWとの通信が継続しているかのように偽装するダミーデータをクライアント装置10に送信する。

[0061] プロセッサ32は、予め設定されたダミーデータをクライアント装置10に送信してもよい。また、プロセッサ32は、人工知能を用いてダミーデータを送信してもよい。たとえば、プロセッサ32は、所定のAIモデルを用いてダミーデータ的内容及び順序などを決定してもよい。

[0062] プロセッサ32は、クライアント装置10にデータを送信した後に、クライアント装置10の挙動（たとえば、クライアント装置10から送信されるデータなど）を取得する。

プロセッサ32は、クライアント装置10の挙動を示す情報を攻撃情報として取得する。

たとえば、プロセッサ32は、クライアント装置10からのデータの内容又は通信日時などを攻撃情報として取得する。

[0063] なお、プロセッサ32は、クライアント装置10の挙動によってAIモデルを更新してもよい。

[0064] プロセッサ32は、情報取得コマンド及びハニーポットの両者を用いて攻撃情報を取得してもよいし、一方を用いて攻撃情報を取得してもよい。また、プロセッサ32は、他の手法を用いて攻撃情報を取得してもよい。プロセッサ32が攻撃情報を取得する方法は、特定の構成に限定されるものではない。

[0065] また、プロセッサ32は、攻撃情報に基づいて攻撃を特定する機能を有する。即ち、プロセッサ32は、攻撃情報に基づいて、クライアント装置10に対する攻撃の攻撃手法又はクライアント装置10に感染しているウイルス

などを特定する。

[0066] プロセッサ32は、攻撃情報とメモリ34が格納する攻撃リストに含まれる各辞書情報とをマッチングさせる。プロセッサ32は、マッチングの結果に基づいて、攻撃を特定する。プロセッサ32は、特定された攻撃を示す情報を外部装置に送信してもよい。また、プロセッサ32は、特定された攻撃を示す情報をメモリ34などに格納してもよい。

[0067] なお、プロセッサ32は、攻撃を特定できなかった場合には、当該攻撃を特定するための新たな辞書情報を攻撃リストへ格納してもよい。即ち、プロセッサ32は、攻撃が特定されなかった攻撃情報に基づいて、クライアント装置10に対する攻撃の新たな辞書情報を生成し、新たな辞書情報を攻撃リストへ登録する。また、プロセッサ32は、攻撃を特定できた場合でも、攻撃が特定された攻撃情報に基づいて、新たな辞書情報を生成し、新たな辞書情報を攻撃リストへ登録するようにしてもよい。このようにして、プロセッサ32は、攻撃情報の取得に応じて、通信制御管理装置50から送信された攻撃リストへ辞書情報を追加登録し、攻撃リストを更新する。ネットワーク通信部31は、更新される攻撃リストを通信制御管理装置50へ送信する。通信制御管理装置50は、各クライアント側通信制御装置30へ新たな攻撃リストを配信することができる。

[0068] また、プロセッサ32は、攻撃を特定できなかった場合には、当該攻撃に関する攻撃情報を通信制御管理装置50に送信してもよい。通信制御管理装置50は、攻撃情報に含まれる攻撃機器固有情報及び通信日時情報等から攻撃の傾向等を分析することができる。

[0069] また、プロセッサ32は、攻撃を受けたクライアント装置10を停止させる機能を有する。

たとえば、プロセッサ32は、クライアント装置10に対してシャットダウンさせるコマンドを送信する。

[0070] また、プロセッサ32は、クライアント装置10に対する電力供給を停止させてもよい。たとえば、クライアント側通信制御装置30がP o E (Power

of Ethernet（登録商標））でクライアント装置１０へ電力を供給している場合、プロセッサ３２は、ＰｏＥでの電力供給を停止させる。

[0071] また、プロセッサ３２は、クライアント装置１０へ電力を供給している電源部などに対してクライアント装置１０への電力供給を停止させるコマンドを送信してもよい。

[0072] プロセッサ３２がクライアント装置１０を停止させる方法は、特定の方法に限定されるものではない。

[0073] 次に、クライアント側通信制御装置３０の動作例について説明する。図４は、クライアント側通信制御装置３０の動作例について説明するためのフローチャートである。

[0074] まず、クライアント側通信制御装置３０のプロセッサ３２は、クライアント装置１０からデータを受信する（Ｓ１１）。データを受信すると、プロセッサ３２は、データに基づいて、クライアント装置１０が攻撃されているかを判定する（Ｓ１２）。

[0075] クライアント装置１０が攻撃されていると判定すると（Ｓ１２、ＹＥＳ）、プロセッサ３２は、ネットワークＮＷとの通信を遮断する（Ｓ１３）。ネットワークＮＷとの通信を遮断すると、プロセッサ３２は、クライアント装置１０から攻撃情報を取得する（Ｓ１４）。

[0076] 攻撃情報の取得に成功すると（Ｓ１５、ＹＥＳ）、プロセッサ３２は、攻撃情報と攻撃リストに含まれる辞書情報とをマッチングする（Ｓ１６）。攻撃情報と辞書情報とをマッチングすると、プロセッサ３２は、攻撃を特定できたか判定する（Ｓ１７）。

[0077] 攻撃を特定できないと判定すると（Ｓ１７、ＮＯ）、プロセッサ３２は、攻撃情報に基づいて、新たに辞書情報を生成し、新たな辞書情報を攻撃リストへ登録する（Ｓ１８）。

攻撃を特定できたと判定した場合（Ｓ１７、ＹＥＳ）、又は、新たな辞書情報を攻撃リストへ登録した場合（Ｓ１８）、プロセッサ３２は、クライアント装置１０を停止させる（Ｓ１９）。

- [0078] クライアント装置10が攻撃されていないと判定すると(S12、NO)、プロセッサ32は、通常の動作を行う(S20)。即ち、プロセッサ32は、クライアント装置10からのデータをネットワークNWへ転送する。
- [0079] クライアント装置10を停止させた場合(S19)、又は、通常の動作を行った場合(S20)、プロセッサ32は、動作を終了する。
- [0080] なお、プロセッサ32は、攻撃情報を取得した後にクライアント装置10を停止させてもよい。
- [0081] また、通信制御システム1は、各クライアント側通信制御装置30で更新された攻撃リストを共有することにより対攻撃性能の向上を図ることができる。上記したように、通信制御管理装置50は、各クライアント側通信制御装置30から送信される攻撃リストを分析して新たな攻撃リストを生成し、新たな攻撃リストを各クライアント側通信制御装置30へ配信する。クライアント側通信制御装置30は、他のクライアント側通信制御装置30が受けた攻撃の分析結果を利用して生成された新たな攻撃リストを参照し、攻撃を特定しクライアント装置10を停止させるなどの対応を取ることができる。
- [0082] また、サーバ側通信制御装置40は、クライアント側通信制御装置30の機能を有するものであってもよい。この場合、サーバ側通信制御装置40は、サーバ装置20に対してクライアント側通信制御装置30の動作と同様の動作を行う。
- [0083] また、クライアント側通信制御装置30は、複数のクライアント装置10とネットワークNWとの間の通信を仲介してもよい。この場合、クライアント側通信制御装置30は、各クライアント装置10に対して同様の動作を行う。
- [0084] 以上のように構成されたクライアント側通信制御装置は、クライアント装置が攻撃されていると判定すると、ネットワークとの通信を遮断する。その結果、クライアント側通信制御装置は、クライアント装置が不正にデータを外部に送信することを防止することができる。
- [0085] また、クライアント側通信制御装置は、ネットワークとの通信を遮断する

が、クライアント装置との通信を維持する。クライアント側通信制御装置は、維持している通信を用いてクライアント装置から種々のデータを取得する。その結果、クライアント側通信制御装置は、不正なデータ通信を遮断しつつ、攻撃に関する攻撃情報を取得することができる。

[0086] 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] 装置とネットワークとの間に接続される通信制御装置であって、
前記装置とデータを送受信する第1の通信部と、
前記ネットワークとデータを送受信する第2の通信部と、
前記第1の通信部を通じて前記装置からデータを受信し、
前記データに基づいて、前記装置が攻撃されているかを判定し、
前記装置が攻撃されていると判定すると、前記ネットワークとの
通信を遮断し、前記第1の通信部を通じて前記装置から前記装置への
攻撃に関する攻撃情報を取得する、
制御部と、
を備える通信制御装置。
- [請求項2] 前記制御部は、前記第1の通信部を通じて情報取得コマンドを送信
することで前記攻撃情報を取得する、
前記請求項1に記載の通信制御装置。
- [請求項3] 前記制御部は、前記情報取得コマンドを送信することで前記装置に
接続する機器を示す情報を含む前記攻撃情報を取得する、
前記請求項2に記載の通信制御装置。
- [請求項4] 前記制御部は、前記攻撃情報を取得するためのセキュリティ上のハ
ニーポットを構築する、
前記請求項1乃至3の何れか1項に記載の通信制御装置。
- [請求項5] 前記制御部は、ハニーポットを通じてダミーデータを前記装置に送
信する、
前記請求項4に記載の通信制御装置。
- [請求項6] 前記制御部は、前記攻撃情報及び攻撃リストに基づいて、前記装置
への攻撃を特定する、
前記請求項1乃至5の何れか1項に記載の通信制御装置。
- [請求項7] 前記制御部は、前記装置への攻撃を特定できない場合、前記攻撃情
報に基づく辞書情報を前記攻撃リストへ登録する、

前記請求項 6 に記載の通信制御装置。

[請求項 8] 前記制御部は、前記攻撃情報を取得した後に前記装置を停止させる
、
前記請求項 1 乃至 7 の何れか 1 項に記載の通信制御装置。