

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-147575

(P2017-147575A)

(43) 公開日 平成29年8月24日(2017.8.24)

(51) Int.Cl.		F I		テーマコード (参考)
H04L 12/717 (2013.01)		H04L 12/717		5B089
G06F 13/00 (2006.01)		G06F 13/00	351Z	5K030

審査請求 未請求 請求項の数 7 O L (全 35 頁)

(21) 出願番号 特願2016-27369 (P2016-27369)
 (22) 出願日 平成28年2月16日 (2016.2.16)

(71) 出願人 000005223
 富士通株式会社
 神奈川県川崎市中原区上小田中4丁目1番1号
 (74) 代理人 100074099
 弁理士 大菅 義之
 (74) 代理人 100133570
 弁理士 ▲徳▼永 民雄
 (72) 発明者 大崎 裕康
 神奈川県横浜市西区高島一丁目1番2号
 富士通ネットワークソリューションズ株式会社内

最終頁に続く

(54) 【発明の名称】 制御プログラム、制御装置、および、制御方法

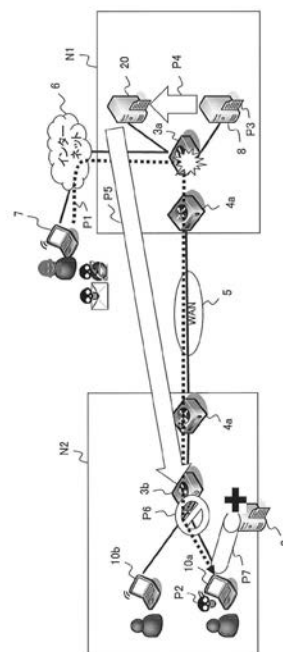
(57) 【要約】

【課題】 不正な通信の検出後に動的にネットワークを制御する。

【解決手段】 通信端末と、通信端末で送受信されるパケットを転送する1つ以上の転送装置とを含むネットワーク中の転送装置を制御する制御装置は、通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信する。制御装置は、検知情報から対象の通信端末と不正な通信の種類とを解析し、解析した対象の通信端末に対応付けられた転送装置を記憶する第1の記憶情報を参照して制御対象の転送装置を決定する。制御装置は、解析された不正な通信の種類に対応づけられた制御内容を記憶する第2の記憶情報を参照して、制御対象に決定した転送装置に対する制御を決定する。制御装置は、制御対象に決定された転送装置の種類ごとに、制御内容に対応する制御コマンドを記憶する第3の記憶情報から読み出した制御コマンドを含む制御パケットを転送装置に送信する。

【選択図】 図1

実施形態にかかる通信方法の例を説明する図



【特許請求の範囲】**【請求項 1】**

通信端末と、前記通信端末で送受信されるパケットを転送する 1 つ以上の転送装置とを含むネットワーク中の前記転送装置を制御する制御装置に、

前記パケットを用いて通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信し、

前記検知情報から対象の通信端末と前記不正な通信の種類とを解析し、

解析した対象の通信端末に対応付けられた転送装置を記憶する第 1 の記憶情報を参照して制御対象の転送装置を決定し、

解析された前記不正な通信の種類に対応づけられた制御内容を記憶する第 2 の記憶情報を参照して制御対象に決定した転送装置に対する制御を決定し、

前記制御対象に決定された転送装置の種類ごとに、前記制御内容に対応する制御コマンドを記憶する第 3 の記憶情報から制御コマンドを読み出して、当該転送装置に対して制御コマンドを含む制御パケットを送信する

処理を行わせることを特徴とする制御プログラム。

【請求項 2】

前記対象の通信端末に対する前記制御内容の解除を要求する解除要求を受信すると、前記第 3 の記憶情報を参照して、前記制御内容の解除に際して前記制御対象の転送装置の各々に適用する制御コマンドを生成すると共に、当該転送装置に、生成した制御コマンドを含む制御パケットを送信する

処理を前記制御装置に実行させることを特徴とする請求項 1 に記載の制御プログラム。

【請求項 3】

前記検知情報は、前記対象の通信端末と前記不正な通信の種類とを通知する通知メール、前記対象の通信端末で行われた通信履歴を表す履歴情報、または前記対象の通信端末と前記不正な通信の種類とを通知する制御情報のいずれかの形式から選択される

ことを特徴とする請求項 1 または 2 に記載の制御プログラム。

【請求項 4】

前記通知メールに含まれる文字列のうちで前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第 1 のテンプレート、前記履歴情報から前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第 2 のテンプレート、および、前記制御情報から前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第 3 のテンプレートを含み、

前記制御装置に、

前記通知メールを受信すると、前記第 1 のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出し、

前記履歴情報を受信すると、前記第 2 のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出し、

前記制御情報を受信すると、前記第 3 のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出する

処理を行わせることを特徴とする請求項 3 に記載の制御プログラム。

【請求項 5】

前記制御プログラムは、前記第 1 の記憶情報と前記第 2 の記憶情報とを、前記制御プログラムにより実行される情報を特定する実行テーブルとして備え、

前記実行テーブルは、前記複数の通信端末中の通信端末と前記不正な通信の種類との組み合わせに対応付けて、当該組み合わせが前記検知サーバから通知された場合に制御対象とする転送装置と、前記制御対象に決定された転送装置に対する制御を記憶する

ことを特徴とする請求項 1 ～ 4 のいずれか 1 項に記載の制御プログラム。

【請求項 6】

通信端末と、前記通信端末で送受信されるパケットを転送する 1 つ以上の転送装置とを含むネットワーク中の前記転送装置を制御する制御装置であって、

前記パケットを用いて通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信する受信部と、

前記検知情報から対象の通信端末と前記不正な通信の種類とを解析する解析部と、

解析した対象の通信端末に対応付けられた転送装置を記憶する第1の記憶情報を参照して制御対象の転送装置を決定すると共に、解析された前記不正な通信の種類に対応づけられた制御内容を記憶する第2の記憶情報を参照して制御対象に決定した転送装置に対する制御を決定する決定部と、

前記制御対象に決定された転送装置の種類ごとに、前記制御内容に対応する制御コマンドを記憶する第3の記憶情報から制御コマンドを読み出して生成された制御パケットを、当該転送装置に送信する送信部

10

を備えることを特徴とする制御装置。

【請求項7】

通信端末と、前記通信端末で送受信されるパケットを転送する1つ以上の転送装置とを含むネットワーク中の前記転送装置を制御する制御装置が、

前記パケットを用いて通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信し、

前記検知情報から対象の通信端末と前記不正な通信の種類とを解析し、

解析した対象の通信端末に対応付けられた転送装置を記憶する第1の記憶情報を参照して制御対象の転送装置を決定し、

解析された前記不正な通信の種類に対応づけられた制御内容を記憶する第2の記憶情報を参照して制御対象に決定した転送装置に対する制御を決定し、

20

前記制御対象に決定された転送装置の種類ごとに、前記制御内容に対応する制御コマンドを記憶する第3の記憶情報から制御コマンドを読み出して、当該転送装置に対して制御コマンドを含む制御パケットを送信する

処理を行うことを特徴とする制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、制御プログラム、制御装置、および、制御方法に関する。

【背景技術】

30

【0002】

近年、悪意のあるソフトウェア（マルウェア）を用いた標的型攻撃が増えてきている。そこで、マルウェア感染の見落としや誤検知を防ぐために、端末による通信と、予め保持しているパターンとの比較結果に従って、端末が不正な活動をしていると推測される程度を示す評価値を用いる判定方法が提案されている（例えば、特許文献1など）。この方法では、情報処理装置が、評価値をフェーズごとに求め、フェーズごとの評価値の最大値を用いて、端末が不正な活動を行っているかを判定する。また、安全性や悪意のソフトウェアでないことが確実ではないデータを検疫し、検疫の前後での安全性や悪意のソフトウェアであるかの判定結果を比較することにより、データがマルウェアに関連するかを推定する方法も提案されている（例えば、特許文献2など）。この方法では、マルウェアではないと推定されたデータは、検疫から開放される。

40

【0003】

また、近年、ソフトウェアを用いた仮想的なネットワークや、仮想的なネットワークの形成に用いられる技術であるSoftware Defined Networking（SDN）も注目されてきている。SDNでは、ネットワークのトポロジなどがソフトウェアで設定される。ここで、ネットワーク中のコントローラと呼ばれる制御装置がネットワーク中の装置の通信状況を監視し、各装置の状況に応じた制御を行う。

【先行技術文献】

【特許文献】

【0004】

50

【特許文献1】国際公開第2015/107861号

【特許文献2】特表2015-530678号

【発明の概要】

【発明が解決しようとする課題】

【0005】

多種多様のマルウェアが存在する上に、新たなマルウェアやマルウェアの亜種が次々に現れてきており、マルウェアの種類は爆発的に増えてきている。システム中でマルウェアに感染した装置が検出された場合、感染の拡大を防ぐための措置を取るようになるが、マルウェアの挙動は種類によって異なることが多いため、マルウェアへの感染を検出した後の措置も難しくなっている。さらに、システム中に含まれる装置数が多いなど、システムが複雑化すると、マルウェア感染を検出した後の措置はさらに煩雑になり、適切な処理を迅速に行うことは難しくなる。さらに、マルウェアを検出する定義パターンが配布される前に感染し、感染を検出できない場合が発生しており、マルウェアに起因する不正な通信を検出する重要性が増している。さらにマルウェアの動作内容や、感染した装置に応じて対処する処置が異なり、不正な通信を検出した場合の措置には高度な専門知識を必要とする。

10

【0006】

本発明は、ネットワークを制御する制御装置で対処可能な制御内容を蓄積しておくことにより、不正な通信の検出後に動的にネットワークを制御することを目的とする。

【課題を解決するための手段】

20

【0007】

ある1つの態様にかかる制御プログラムは、通信端末と、前記通信端末で送受信されるパケットを転送する1つ以上の転送装置とを含むネットワーク中の前記転送装置を制御する制御装置で実行される。制御装置は、前記パケットを用いて通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信する。制御装置は、前記検知情報から対象の通信端末と前記不正な通信の種類とを解析する。制御装置は、解析した対象の通信端末に対応付けられた転送装置を記憶する第1の記憶情報を参照して制御対象の転送装置を決定する。制御装置は、解析された前記不正な通信の種類に対応付けられた制御内容を記憶する第2の記憶情報を参照して制御対象に決定した転送装置に対する制御を決定する。制御装置は、前記制御対象に決定された転送装置の種類ごとに、前記制御内容に対応する制御コマンドを記憶する第3の記憶情報から制御コマンドを読み出して、当該転送装置に対して制御コマンドを含む制御パケットを送信する。

30

【発明の効果】

【0008】

ネットワークに接続された個々の装置では対処が困難なマルウェアに対しても、ネットワーク制御を動的に行うことで、対処が可能になる。

【図面の簡単な説明】

【0009】

【図1】実施形態にかかる通信方法の例を説明する図である。

【図2】制御装置の構成の例を説明する図である。

40

【図3】制御装置のハードウェア構成の例を説明する図である。

【図4】システムの例を説明する図である。

【図5】メールによる通知を受信したときの解析処理の例を説明する図である。

【図6】実行テーブルの例を説明する図である。

【図7】装置テーブルとコマンド情報の例を説明する図である。

【図8】コマンドの生成処理の例を説明する図である。

【図9】メールによる通知処理の例を説明する図である。

【図10】Syslogを受信したときの解析処理の例を説明する図である。

【図11】Trapを受信したときの解析処理の例を説明する図である。

【図12】装置の隔離の際に行われる処理の例を説明するフローチャートである。

50

【図 1 3】 隔離状況テーブルと実行テーブルの例を説明する図である。

【図 1 4】 コマンド情報の例を説明する図である。

【図 1 5】 隔離の解除の際に行われる処理の例を説明する図である。

【図 1 6】 メールによる通知処理の例を説明する図である。

【図 1 7】 隔離の解除の際に行われる処理の例を説明するフローチャートである。

【図 1 8】 第 3 の実施形態にかかる制御装置の構成の例を示す図である。

【図 1 9】 条件テーブルとポリシーマスタの例を説明する図である。

【図 2 0】 実行テーブルと装置テーブルの例を説明する図である。

【図 2 1】 コマンド情報の例を説明する図である。

【図 2 2】 通知先テーブルと隔離状況テーブルの例を説明する図である。

10

【図 2 3】 第 3 の実施形態で行われる処理の例を説明するフローチャートである。

【図 2 4】 制御装置が記憶する情報の変形例を説明する図である。

【発明を実施するための形態】

【0010】

図 1 は、実施形態にかかる通信方法の例を説明する図である。図 1 に示すシステムでは、ネットワーク N 1 とネットワーク N 2 が W A N（Wide Area Network）5 を介して接続されており、ネットワーク N 1 はインターネット 6 に接続されている。C & C サーバ（command and control server）7 は、インターネット 6 を介して、ネットワーク N 1 やネットワーク N 2 にアクセスを試みるものとする。ネットワーク N 1 には、制御装置 2 0、検知サーバ 8、スイッチ 3 a、ルータ 4 a が含まれている。一方、ネットワーク N 2 には、通信端末 1 0 a、通信端末 1 0 b、検疫サーバ 2、スイッチ 3 b、ルータ 4 b が含まれている。なお、図 1 はシステムの一例であり、ネットワーク N 1、N 2 中の装置は実装に応じて変更され得る。例えば、ネットワーク N 1 には、制御装置 2 0 や検知サーバ 8 以外の通信端末 1 0 が含まれていても良い。また、検疫サーバ 2 は、ネットワーク N 2 中に含まれていなくても良い。ネットワーク N 1、N 2 の形成に S D N が使用される場合、制御装置 2 0 は、S D N コントローラとして動作できるものとする。また、以下の説明では、スイッチ 3 やルータ 4 のように、通信端末 1 0 から送信されたパケットを転送する装置を「転送装置」と記載することがある。ネットワーク N 1、N 2 の形成に S D N が使用される場合、各転送装置は、S D N スイッチとして動作する。

20

【0011】

30

手順 P 1 において、C & C サーバ 7 から通信端末 1 0 a を標的とした標的型攻撃が行われたとする。図 1 の例では、標的型攻撃の種類は任意である。例えば、標的型メールの送信が行われても良く、特定のウェブサイトを開覧するように通信端末 1 0 a のユーザを誘導するための情報が通信端末 1 0 a に送信されても良い。標的型攻撃のために使用される情報は、インターネット 6、スイッチ 3 a、ルータ 4 a、ルータ 4 b、スイッチ 3 b を介して、通信端末 1 0 a に転送される。その後、C & C サーバ 7 から送信された情報を用いた処理が通信端末 1 0 a で行われたために、通信端末 1 0 a がマルウェアに感染したとする（手順 P 2）。

【0012】

40

検知サーバ 8 は、システム中の装置の挙動を監視しており、システム内での不正な通信や不正な通信の原因となるマルウェアへの感染などを検出すると、不正な通信等が確認された通信端末 1 0 と、検出された事象の種類を特定する。なお、「不正な通信」には、マルウェアを含むファイルの送受信やマルウェアの実行に起因する通信などが含まれるとする。例えば、ウイルスなどのマルウェアへの感染、バックドアによる C & C サーバへの通信、ネットワーク内の情報収集を試みる通信や、他の装置への感染の拡大を試みる通信などは、検知サーバ 8 によって、不正な通信の一種として特定されうる。図 1 の例では、検知サーバ 8 は、システム中で送受信されるパケットを用いて、通信端末 1 0 a での不正な通信を検知したことなどにより、通信端末 1 0 a がマルウェアに感染したと判定する（手順 P 3）。検知サーバ 8 は、不正な通信等が確認された通信端末 1 0 と、検出された事象の種類を制御装置 2 0 に通知する（手順 P 4）。なお、手順 P 4 での通知は、メール、S

50

NMP (Simple Network Management Protocol) の Trap 通知、Syslog 通知などを含む任意の形式で行われ得る。

【0013】

制御装置 20 は、検知サーバ 8 から通知された情報を用いて、通信端末 10 a がマルウェアに感染していることを特定する。さらに、制御装置 20 は、マルウェアの種類などに応じて、攻撃の種類を特定する。

【0014】

制御装置 20 は、ネットワーク N1 とネットワーク N2 に含まれている通信端末 10 の各々に対して、その通信端末 10 での不正な通信が確認されたときに制御対象とする転送装置を記憶している。ここで、各通信端末 10 について、その通信端末 10 が他の通信端末 10 などとの通信を行う際の通信経路に含まれるスイッチ 3 やルータ 4 が、その通信端末 10 が不正な通信をしている場合の制御対象として対応付けられる。制御装置 20 は、検出される可能性のある不正な通信の種類ごとに実行する制御も記憶している。そこで、制御装置 20 は、検知サーバ 8 から通知された情報の解析結果と、制御装置 20 が記憶している情報を用いて、制御対象となる転送装置と各転送装置への制御の内容を決定する。例えば、通信端末 10 a に対してウイルスなどを用いた攻撃が行われたとする。そこで、制御装置 20 は、記憶している情報を用いて、スイッチ 3 b を制御対象の転送装置に決定し、通信端末 10 a が送信元か宛先に設定されているパケットを検疫サーバ 2 に転送する処理をスイッチ 3 b に行わせることを制御内容に決定したとする。

【0015】

手順 P5 において、制御装置 20 は、制御対象に決定した転送装置の各々に対して、その転送装置に対する制御の命令を含む制御パケットを送信する。図 1 の例では、制御装置 20 は、スイッチ 3 b に対して、通信端末 10 a が送信元か宛先に設定されているパケットを検疫サーバ 2 に転送することを要求する制御パケットを送信する。

【0016】

手順 P6 において、スイッチ 3 b は、制御装置 20 からの要求に応じて、パケットの転送処理を変更する。このため、手順 P7 に示すように、通信端末 10 a の通信に使用されるパケットが、強制的に検疫サーバ 2 に転送される。このため、攻撃された通信端末 10 a からのパケットがシステム中の他の通信端末 10 に到達することを防ぐことができる。

【0017】

なお、図 1 を参照しながら述べた説明は通信処理の一例にすぎない。例えば、制御装置 20 は、検出された不正な通信の種類に応じて、不正な通信が検出された通信端末 10 が送受信に使用する通信速度を小さくするように転送装置を制御してもよい。さらに、制御装置 20 は、制御対象とする転送装置に、不正な通信が検出された通信端末 10 が送信元か宛先となっているパケット中のデータに応じてパケットを削除させてもよい。例えば、制御装置 20 は、制御対象となる転送装置に対して、不正な通信が検出された通信端末 10 との通信に使用されるパケットのうち、特定の文字列が含まれているパケットを廃棄させてもよい。この場合、個人情報の記載に使用されると予測される文字列が削除対象のパケットを選択する際に使用される特定の文字列に設定されていれば、不正な通信が検出された通信端末 10 と他の通信端末 10 との間での個人情報の送受信を中断させることができる。

【0018】

このように、実施形態にかかる方法によると、ネットワーク中の転送装置に対して、攻撃の種類等に応じた制御を簡便に行うことができる。攻撃に使用されるマルウェアによっては、感染した装置を物理的に隔離すると解析等が困難になる場合もあるなど、マルウェアへの感染を検出した後の措置も難しくなっている。実施形態にかかる方法を用いると、攻撃によりマルウェアに感染した通信端末 10 を隔離しつつ、検疫サーバ 2 での検疫処理を開始させるなど、不正な通信の種類に応じた適正な処理が制御装置 20 によって自律的に行われる。このため、システムの運用や管理が簡便になる。さらに、マルウェアに感染した通信端末 10 に対する措置は、制御装置 20 に対する設定に応じて変更されるの

で、マルウェアによる攻撃の種類に応じた対応が簡便に行われる。

【0019】

<装置構成>

図2は、制御装置20の構成の例を説明する図である。制御装置20は、通信部21、制御部30、記憶部50を備える。通信部21は、受信部22と送信部23を有する。制御部30は、解析部31、処理決定部32、コマンド生成部40を有し、オプションとして通知処理部33を有する。記憶部50は、条件テーブル51、テンプレート情報52、装置テーブル53、コマンド情報55、隔離状況テーブル56、実行情報データベース60を格納する。制御装置20が通知処理部33を備える場合、記憶部50は、さらに、通知先テーブル54を格納する。

10

【0020】

送信部23は、スイッチ3やルータ4などの他の装置にパケットを送信する。受信部22は、検知サーバ8などの他の装置からパケットを受信する。受信部22は受信パケットを解析部31に出力する。

【0021】

解析部31は、入力されたパケットを、テンプレート情報52を用いて解析する。テンプレート情報52には、検知サーバ8から送信される通知の種類別に、不正な通信の対象となった通信端末10と、不正な通信の種類を特定するための情報が含まれている。テンプレート情報52の例は後で述べる。解析部31は、解析により得られた情報と条件テーブル51を用いて、処理の決定に使用する実行テーブルを決定する。実行情報データベース60は複数の実行テーブルを備えている。解析部31は、決定した実行テーブルの情報と、不正な通信の対象となった通信端末10の情報を処理決定部32に通知する。処理決定部32は、通知された実行テーブルを実行情報データベース60から選択し、選択した実行テーブルを用いて、制御対象となる転送装置と制御の内容を決定する。処理決定部32は、マルウェアに感染した通信端末10を隔離する場合には、決定した内容を、隔離状況テーブル56に記録する。コマンド生成部40は、処理決定部32で決定された情報を用い、適宜、コマンド情報55や装置テーブル53を用いて、制御対象の転送装置の各々に対して送信する制御パケットを生成する。装置テーブル53には、システム中の各装置の制御に使用される情報が記録されている。コマンド情報55は、装置の制御に使用される命令を記録している。コマンド生成部40は、生成した制御パケットを、送信部23を介して、制御対象の転送装置に送信する。

20

30

【0022】

通知処理部33は、制御装置20が行った処理によりネットワーク中の通信端末10の通信状況が変化する場合、通知先テーブル54に記録されているアドレスが割り当てられた装置に、通信状況が変化する場合、通信端末10と変化後の通信状況を通知する。例えば、通信端末10aがウイルスに感染したために通信端末10aをネットワーク中の他の装置から隔離する場合、通知処理部33は、通知先テーブル54に記録されている宛先に、通信端末10aを隔離することを通知する。通知先テーブル54には、例えば、システムのオペレータなどが使用する装置の情報が記録されている。

【0023】

図3は、制御装置20のハードウェア構成の例を示す。制御装置20は、プロセッサ101、メモリ102、入力装置103、出力装置104、バス105、ネットワークインタフェース109を備える。制御装置20は、さらに、記憶装置106、可搬記憶媒体駆動装置107の1つ以上を有していても良い。プロセッサ101は、Central Processing Unit(CPU)を含む任意の処理回路であり、メモリ102や記憶装置106に記憶されたプログラムを実行することができる。プロセッサ101は制御部30を実現する。メモリ102や記憶装置106は、記憶部50として動作する。また、ネットワークインタフェース109は、通信部21として動作する。バス105は、プロセッサ101、メモリ102、入力装置103、出力装置104、記憶装置106、可搬記憶媒体駆動装置107、ネットワークインタフェース109を、相互にデータの送受信が可能になるように

40

50

接続する。

【0024】

入力装置103は、キーボードやマウスなど、情報の入力に使用される任意の装置であり、出力装置104は、ディスプレイを含む表示デバイスなど、データの出力に使用される任意の装置である。可搬記憶媒体駆動装置107は、メモリ102や記憶装置106のデータを可搬記憶媒体108に出力することができ、また、可搬記憶媒体108からプログラムやデータ等を読み出すことができる。ここで、可搬記憶媒体108は、Compact Disc Recordable (CD-R) やDigital Versatile Disk Recordable (DVD-R) を含む、持ち運びが可能な任意の記憶媒体とすることができる。

【0025】

<第1の実施形態>

図4は、システムの例を説明する図である。図4に示すシステムでは、ネットワークN11とネットワークN12がWAN5を介して接続されており、ネットワークN11はインターネット6に接続されている。C&Cサーバ7は、インターネット6を介して、ネットワークN11やネットワークN12にアクセスを試みるものとする。ネットワークN11には、制御装置20、検知サーバ8、スイッチ3c、ルータ4cが含まれている。一方、ネットワークN12には、通信端末10c、通信端末10d、スイッチ3d、スイッチ3e、ルータ4d、検知サーバ2が含まれている。なお、図4はシステムの一例であり、ネットワークN11、N12中の装置は実装に応じて変更され得る。以下、図4にかかるシステムにおいて実施形態にかかる通信制御が行われる場合を例として、制御装置20で行われる処理の詳細を説明する。なお、以下の説明では、スイッチ3dとスイッチ3eは、いずれもL3スイッチであり、スイッチ3dとスイッチ3eのいずれにもIP (Internet Protocol) アドレスが割り当てられるものとする。

【0026】

図5は、メールによる通知を受信したときの制御装置20での解析処理の例を説明する図である。検知サーバ8は、ネットワークN11およびN12中の装置の挙動を監視することにより、通信端末10cがウイルスに感染したことを検出したとする。また、通信端末10cのアドレスは、172.16.1.1であるとする。図5では、検知サーバ8が不正な通信の検出の通知に使用するメールアドレスはserver@example.comであり、制御装置20で通知の受信に使用されるメールアドレスはclient@example.comであるとする。検知サーバ8は、図5中のメールM1を、制御装置20に送信する。

【0027】

解析部31は、入力されたパケットを処理することにより受信メールを取得すると、受信メールを条件テーブル51中の各条件と比較する。条件テーブル51には、制御装置20が受信する可能性のある通知の形式に対応付けて、処理に使用する実行テーブルを選択するための情報が記録されている。図5は、図を見やすくするために、条件テーブル51のうちでメールによる通知に適用可能な1つの条件の例を抽出して示しているが、条件テーブル51中の条件の数は任意である。図5の例では、条件テーブル51には、メールの送信元、subject中の文字列、context中の文字列、通知対象の組み合わせが含まれる。解析部31は、メールの送信元、subject中の文字列、context中の文字列の組み合わせを用いて、不正な通信の種類を特定する。通知対象は、検知サーバ8からの通知で、不正な通信の検出が伝えられる通信端末10のアドレスの範囲である。通知対象には、そのエントリ中の条件を適用する場合に、不正な通信が検出されている通信端末10に割り当てられたアドレスが対応付けられている。

【0028】

例えば、受信メールの送信元アドレスがserver@example.comであり、subjectに「virus detect」という文字列を含み、かつ、contextに「ウイルス検知」という文字列を含むとする。この場合、解析部31は、いずれかの通信端末10がウイルスに感染したと判定する。

10

20

30

40

50

【0029】

次に、解析部31は、ウイルスの感染が通知されたので、ウイルスの感染を通知するメールの解析に使用するテンプレートをテンプレート情報52から選択する。図5の例では、解析部31は、メールテンプレートMT1を選択したとする。解析部31は、受信メールをメールテンプレートMT1と比較する。メールテンプレートMT1は、contextの記載を「%1にてウイルス検知」という文字列とした場合、受信メールのcontext中の「%1」に該当する文字列が、ウイルスに感染した通信端末10に割り当てられたアドレスであることを示している。図5の例では、解析部31は、メールテンプレートMT1とメールM1を比較することにより、172.16.1.1のアドレスが割り当てられた通信端末10（通信端末10c）がウイルスに感染したと判定する。

10

【0030】

解析部31は、条件テーブル51中でウイルスへの感染が通知された場合に使用可能な条件の中から、IPアドレス=172.16.1.1の通信端末10が感染した場合に適用可能な条件を検索する。このとき、解析部31は、ウイルスへの感染が検出されたときに使用可能な条件の各々に対応付けられている通知対象の値と、ウイルスへの感染が検出された通信端末10のアドレスを比較する。図5に示す条件テーブル51中のエントリでは、通知対象が172.16.1.0/24である。すなわち、条件テーブル51には、172.16.1.0と第3オクテットまでが同じアドレスが割り当てられた装置でのウイルスへの感染が検出された場合に、実行テーブル61aが使用可能であることが示されている。ウイルスに感染した通信端末10cのIPアドレスは172.16.1.1であるので、解析部31は、条件テーブル51に基づいて、実行テーブル61aを使用可能であると判定する。解析部31は、実行テーブル61aを使用可能であることと、ウイルスに感染した通信端末10cに割り当てられているアドレスである172.16.1.1を、処理決定部32に出力する。

20

【0031】

図6は、実行テーブル61の例を説明する図である。図6は、IPアドレス=172.16.1.0/24のアドレスが割り当てられた通信端末10の隔離に使用される情報を含む実行テーブル61を示している。実行テーブル61は、その実行テーブル61を使用して行われる処理の内容と、制御対象となる装置を記録している。例えば、実行テーブル61aでは、感染が検出された通信端末10の隔離と、隔離処理を行ったことをオペレータへ通知するためのメール通知処理とが、処理内容として記録されている。実行テーブル61aには、通信端末10の隔離を行うための制御対象となる装置と、各制御対象の装置の制御のために実施されるコマンドのグループが各装置の情報に対応付けられている。なお、コマンドのグループは、コマンド情報55に含まれている。ここで、隔離の対象となった通信端末10が冗長経路を使用した通信を行うことが可能である場合、隔離対象の通信端末10が使用可能な全ての経路で隔離処理を行うための装置の情報が実行テーブル61に記録される。

30

【0032】

例えば、図4に示すネットワークでは、隔離対象となっている通信端末10cは、スイッチ3dとスイッチ3eのいずれを使用しても、他の装置と通信が可能である。そこで、実行テーブル61aの例では、通信端末10cの隔離を行うための制御対象として、ネットワークN2中のスイッチ3dとスイッチ3eが記録されている。スイッチ3dは、A社の製品であるとする。また、スイッチ3dの制御には、コマンドグループCG1の命令が使用されたとする。同様に、スイッチ3eはB社の製品であり、スイッチ3eに適用される命令はコマンドグループCG2の命令である。さらに、通知先テーブル54に含まれている通知先の各々に対して、メールテンプレートMT2を用いて生成した通知メールを送信することも、実行テーブル61aに記録されている。

40

【0033】

なお、実行テーブル61中の制御情報は実装に応じて変更され得る。例えば、実行テーブル61には、不正な通信が検知された通信端末10を、VPN（Virtual Private Netw

50

ork) を介して、検疫サーバ 2 に接続する処理でも良い。また、実行テーブル 6 1 には、スイッチ 3 だけでなく、ルータ 4 など、任意の種類の転送装置の情報が含まれ得る。

【0034】

処理決定部 3 2 は、解析部 3 1 から通知された実行テーブル 6 1 で通信端末 1 0 の隔離が制御内容として設定されていることから、隔離対象の通信端末 1 0 c の情報を、隔離状況テーブル 5 6 に記録する。例えば、処理決定部 3 2 は、隔離状況テーブル 5 6 に、隔離対象の装置のアドレスを記録する。なお、隔離状況テーブル 5 6 には、隔離対象の装置のアドレスとともに、隔離処理に使用する実行テーブル 6 1 中の情報を特定するエントリ番号などの識別情報が記録されても良い。例えば、図 6 の実行テーブル 6 1 a が使用される場合、隔離状況テーブル 5 6 には以下の情報が記録される。

10

隔離対象の装置のアドレス：172.16.1.1（通信端末 1 0 c）

隔離処理に使用する情報：実行テーブル 6 1 a

なお、隔離状況テーブル 5 6 には、実装に応じてその他の情報が含まれてもよい。

【0035】

処理決定部 3 2 は、解析部 3 1 から通知された実行テーブル 6 1 を用いて、制御対象となる装置と、制御対象の各装置に使用されるコマンドグループを特定すると、特定した情報をコマンド生成部 4 0 に出力する。このとき、処理決定部 3 2 は、不正な通信が検出された通信端末 1 0 の IP アドレスも、コマンド生成部 4 0 に通知するものとする。例えば、実行テーブル 6 1 a が使用される場合、コマンド生成部 4 0 には以下の情報が通知される。

20

不正な通信が検出された装置のアドレス：172.16.1.1（通信端末 1 0 c）

制御対象 1：スイッチ 3 d

制御対象 1 に適用するコマンド：コマンドグループ C G 1

制御対象 2：スイッチ 3 e

制御対象 2 に適用するコマンド：コマンドグループ C G 2

コマンド生成部 4 0 は、処理決定部 3 2 から取得した情報、装置テーブル 5 3、コマンド情報 5 5 を用いて処理を行う。

【0036】

図 7 は、装置テーブル 5 3 とコマンド情報 5 5 の例を説明する図である。図 7 には、コマンド情報 5 5 のうち、コマンドグループ C G 1 とコマンドグループ C G 2 に含まれるコマンドの情報を示している。なお、以下の説明では、IP ACL（Access Control List）を用いた処理が行われる場合を例としているが、実装に応じて、コマンド情報 5 5 には IP ACL 以外の任意の設定処理のコマンドが使用されうる。なお、以下の説明では、制御によって実現される処理ごとに、ACL の番号として異なる値が設定されているとする。以下、攻撃が検出される前の状態では、システム中のスイッチ 3 やルータ 4 でのフィルタリングは ACL 番号 = 1 0 1 の条件で行われており、攻撃の検出により通信端末 1 0 の隔離を行う場合は ACL 番号 = 1 0 2 の条件でフィルタリングされる場合を例とする。

30

【0037】

装置テーブル 5 3 には、システム中の装置を制御する場合に使用される情報が、装置の識別情報に対応付けて記録されている。図 7 の例では、装置の識別情報に対して、その装置に割り当てられた IP アドレス、その装置を制御する際に使用されるプロトコル、制御用の ID とパスワードが記録されている。スイッチ 3 d には、10.0.0.1 という IP アドレスが割り当てられており、サブネットマスクは 24 ビットである。さらに、スイッチ 3 d に対しては t e l n e t（Teletype network）を用いた制御が行われる。スイッチ 3 e に対しても、10.0.0.2 という IP アドレスが割り当てられており、サブネットマスクは 24 ビットであることや、スイッチ 3 e の制御に t e l n e t が用いられることが装置テーブル 5 3 に記録されている。

40

【0038】

コマンドグループ C G 1 には、アクセス制御のための 4 つの条件文が含まれている。コ

50

マンドグループCG1では、通信端末10cの隔離のための処理が記載されるので、拡張ACL番号=120が使用されている。1つ目の条件文では、制御対象のパケットの送信元のIPアドレスとして\$1が設定されている。ここで、\$1は、不正な通信が検出された通信端末10のIPアドレスに置換される情報である。\$1の後にワイルドカードマスクが指定されている。以下の説明では、ワイルドカードマスクの各ビットと\$1で示されている各ビットの間でのAND演算によって得られた値を用いて、処理対象のパケットに設定されたアドレス情報が特定されるものとする。制御対象のパケットの宛先のIPアドレスとして10.0.10.15が設定されている。なお、以下の説明では、検疫サーバ2には、10.0.10.15というIPアドレスが割り当てられているとする。また、1つ目の条件文のコマンド引数は、パケットの許可を表わすpermitである。従って、1つ目の条件文では、不正な通信が検出された通信端末10を送信元とするIPパケットのうち、検疫サーバ2を宛先とするパケットを許可することが記載されている。一方、2つ目の条件文のコマンド引数は、パケットの拒否を表わすdenyに設定されている。このため、2つ目の条件文では、不正な通信が検出された通信端末10を送信元とするIPパケット全てを拒否することが記載されている。なお、1つ目の条件文が適用される場合、2つ目以降の条件文は処理対象とならないので、不正な通信が検出された通信端末10を送信元とするIPパケットのうち検疫サーバ2以外を宛先としたパケットが、2つ目の条件文によって拒否されることになる。3つ目の条件文では、送信元と宛先がいずれであっても、パケットを許可することが記載されており、4つ目の条件文には、送信元と宛先がいずれであっても、パケットを拒否することが記載されている。さらに、コマンドグループCG1には、これらの条件文をインタフェースFa0/1に着信してくるパケットに対するフィルタリングに適用することが記載されている。

【0039】

コマンドグループCG2にもアクセス制御のための4つの条件文が含まれており、不正な通信が検出された通信端末10のIPアドレスに置換される情報として、\$1が含まれている。従って、コマンドグループCG2の1つ目の条件文は、不正な通信が検出された通信端末10を送信元とするIPパケットのうち、10.0.10.15（検疫サーバ2のIPアドレス）が宛先アドレスに設定されたパケットを許可することを記載している。一方、2つ目の条件文では、不正な通信が検出された通信端末10を送信元とするIPパケット全てを拒否することが記載されているので、不正な通信が検出された通信端末10から検疫サーバ2以外を宛先としたパケットは、2つ目の条件文によって拒否される。3つ目の条件文では、送信元と宛先がいずれであっても、パケットを許可することが記載されており、4つ目の条件文には、送信元と宛先がいずれであっても、パケットを拒否することが記載されている。さらに、コマンドグループCG2には、これらの条件文をインタフェースFa0/1に着信してくるパケットに対するフィルタリングに適用することが記載されている。

【0040】

なお、図7の例では、コマンドグループCG1とCG2に含まれるコマンドが共通している場合を示しているが、1つの通信端末10の隔離の際に実行される複数のコマンドグループ中のコマンドは実装に応じて異なっても同じであっても良い。さらに、各コマンドグループに含まれる条件文の数も任意である。

【0041】

図8は、コマンドの生成処理の例を説明する図である。図8を参照しながら、コマンドを設定する設定ブロックが設定対象の装置を製造した会社ごとに異なる場合の処理の例を説明する。図8では、コマンド生成部40中に、設定ブロック41a、設定ブロック41b、プロトコル処理部42が含まれている。設定ブロック41aはA社の製品の制御処理のためのコマンドを設定し、設定ブロック41bはB社の製品の制御処理のためのコマンドを設定するものとする。さらに、制御装置20に備えられている装置テーブル53とコマンド情報55には、図7に示す情報が含まれているものとする。

【0042】

10

20

30

40

50

処理決定部 3 2 は、図 6 に示す実行テーブル 6 1 a を用いて得られた情報のうち、以下の情報を設定ブロック 4 1 a に出力する（手順 P 2 1）。

不正な通信が検出された装置のアドレス：1 7 2 . 1 6 . 1 . 1（通信端末 1 0 c）

制御対象 1：スイッチ 3 d

制御対象 1 に適用するコマンド：コマンドグループ C G 1

【0 0 4 3】

設定ブロック 4 1 a は、これらの情報を取得すると、コマンドグループ C G 1（図 7 の C G 1）のコマンド中の \$ 1 という文字列を、不正な通信が検出された装置のアドレスに置き換えることにより、制御処理に使用されるコマンドを生成する。図 8 中の G は、コマンドグループ C G 1 中の条件文から、設定ブロック 4 1 a でスイッチ 3 d に送信する条件文が生成される場合の処理の例を示す。いずれの条件文においても、設定ブロック 4 1 a は、コマンドグループ C G 1 中の条件文の \$ 1 を、不正な通信が検出された通信端末 1 0 c のアドレスで置き換える。このため、図 8 の G に示すように、1 7 2 . 1 6 . 1 . 1（通信端末 1 0 c）から送信されたパケットは、1 0 . 0 . 1 0 . 1 5（検疫サーバ 2）以外には転送しないことを設定するためのコマンドが生成される。

【0 0 4 4】

同様に、処理決定部 3 2 は、実行テーブル 6 1 a（図 6）を用いて得られた情報のうち、以下の情報を設定ブロック 4 1 b に出力する（手順 P 2 2）。

不正な通信が検出された装置のアドレス：1 7 2 . 1 6 . 1 . 1（通信端末 1 0 c）

制御対象 2：スイッチ 3 e

制御対象 2 に適用するコマンド：コマンドグループ C G 2

設定ブロック 4 1 b においても、コマンドグループ C G 2 に含まれている条件文中の \$ 1 を、不正な通信が検出された通信端末 1 0 c のアドレスに置き換える処理が行われる。このため、通信端末 1 0 c から送信されたパケットを検疫サーバ 2 以外には転送しないことをスイッチ 3 e に設定するためのコマンドが生成される。

【0 0 4 5】

設定ブロック 4 1 a および設定ブロック 4 1 b は、生成したコマンドをプロトコル処理部 4 2 に出力する（手順 P 2 3、P 2 4）。このとき、設定ブロック 4 1 a および設定ブロック 4 1 b は、コマンドの送信に使用される情報を、生成したコマンドに対応付けてプロトコル処理部 4 2 に出力する。例えば、設定ブロック 4 1 a は、装置テーブル 5 3（図 7）中のスイッチ 3 d の IP アドレス、制御に際して使用される ID、パスワードの組み合わせを、生成したコマンドと共に、プロトコル処理部 4 2 に出力する。設定ブロック 4 1 b も同様に、装置テーブル 5 3 中のスイッチ 3 e の情報と、スイッチ 3 e 向けに生成したコマンドを、プロトコル処理部 4 2 に出力する。プロトコル処理部 4 2 は、入力されたコマンドを、そのコマンドの宛先との間の通信に使用するプロトコルに応じた形式の制御パケットに含める。図 8 の例では、制御装置 2 0 は、スイッチ 3 d とスイッチ 3 e のいずれとも t e l n e t で制御情報を送受信するので、プロトコル処理部 4 2 は、入力されたコマンドから t e l n e t に合わせた形式の制御パケットを生成する。プロトコル処理部 4 2 は、生成した制御パケットを、送信部 2 3 を介して、宛先の装置に送信する（手順 P 2 5、P 2 6）。

【0 0 4 6】

なお、以上の説明では、制御装置 2 0 と転送装置の間の通信に t e l n e t が用いられる場合を例として説明したが、制御装置 2 0 と転送装置の間の通信には、任意のプロトコルが使用されうる。例えば、制御装置 2 0 は、S S H（Secure Shell）、H T T P（Hypertext Transfer Protocol）などのプロトコルを用いて、ルータ 4 やスイッチ 3 での転送処理を制御しても良い。

【0 0 4 7】

さらに、コマンド生成部 4 0 は、設定ブロック 4 1 とプロトコル処理部 4 2 に分けられていなくても良い。この場合、コマンド生成部 4 0 が設定ブロック 4 1 とプロトコル処理部 4 2 の両方として動作する。

【0048】

図9は、メールによる通知処理の例を説明する図である。処理決定部32は、不正な通信が検出された通信端末10のアドレスと、通知処理に使用するメールテンプレートを、通知処理部33に通知する。図9の例では、通知処理部33に対して、不正な通信が検出された装置のアドレスが172.16.1.1（通信端末10c）であることと、メールテンプレートMT2を使用することが通知されたとする。

【0049】

通知処理部33は、メールテンプレートMT2のうち、不正な通信が検出された通信端末10のIPアドレスと置換する対象の文字列を、処理決定部32から通知されたIPアドレスに置き換える。図9中のMT2のうち、「%1」に該当する文字列は、不正な通信が検出された通信端末10のIPアドレスと置換する対象の文字列である。そこで、通知処理部33は、メールテンプレートMT2中の「%1」という文字列を、172.16.1.1というIPアドレスに置き換えることにより、メールM2を生成する。

【0050】

次に、通知処理部33は、通知メールの宛先を特定するために通知先テーブル54を参照し、通知先テーブル54中のアドレスの各々に対して生成したメールを送信するための処理を行う。図9の例では、通知先テーブル54には、test1@example.comなどの3つのメールアドレスが記録されている。そこで、通知処理部33は、通知先テーブル54中の3つのアドレスの各々に対してメールM2に示す文面の通知メールを生成する。その後、通知処理部33は、生成したメールの情報を含むパケットを生成すると、生成したパケットを、送信部23を介して、宛先に送信する。例えば、オペレータが、通信端末10xにおいて、test1@example.comというアドレスを使用しているとすると、図8を参照しながら説明した隔離処理の実行に伴って、メールM2に示す文面の通知メールが通信端末10xに送信される。従って、オペレータは、172.16.1.1というIPアドレスが割り当てられた通信端末10（通信端末10c）でウイルスが検知されたことにより、通信端末10cが隔離されたことを認識できる。

【0051】

図4～図9を参照しながら、不正な通信の検出が検知サーバ8から制御装置20に対してメールで通知される場合の例を説明したが、検知サーバ8からの通知は、SyslogやSNMP Trapで行われても良い。以下、検知サーバ8からの通知がSyslogやSNMP Trapで行われる場合の処理の例を説明する。

【0052】

図10は、制御装置20が検知サーバ8からSyslogを受信したときの解析処理の例を説明する図である。検知サーバ8は、IPアドレス=172.16.1.1（通信端末10c）がウイルスに感染したことを検出したとする。すると、検知サーバ8は、ウイルスを検出した時刻やウイルスが検出された通信端末10の情報を含むSyslogを制御装置20に送信する。図10のSYは、検知サーバ8から制御装置20に送信されるSyslogの例である。

【0053】

制御装置20の解析部31は、受信部22を介してSyslogを取得すると、Syslogを条件テーブル51中の各条件と比較する。図10は、図を見やすくするために、条件テーブル51のうちでSyslogによる通知に適用可能な条件の1つの例を抽出して示している。図10の例では、条件テーブル51には、Syslog中のprotocol中の文字列と、通知対象の組み合わせが含まれる。解析部31は、protocol中の文字列を用いて、不正な通信の種類を特定する。例えば、Syslog中のprotocol中に「protocol: the unidentified terminal was detected」という文字列を含むとする。この場合、条件テーブル51は、いずれかの通信端末10がウイルスに感染したと判定する。なお、メールでの通知の際と同様に、Syslogの処理に使用される条件についても、通知対象として、その条件が使用されるときに不正な通信が検出された通信端末10のアドレスが対応付けられている。

【0054】

次に、解析部31は、ウイルスの感染が通知されたので、ウイルスの感染を通知する Syslog の解析に使用するテンプレートをテンプレート情報52から選択する。図10の例では、解析部31は、Syslog テンプレートST1を選択したとする。解析部31は、Syslog を Syslog テンプレートST1と比較する。Syslog テンプレートST1は、protocol の記載を「protocol: the unidentified terminal was detected:IP=\$含む」という文字列としたときの「\$」に該当する文字列を、ウイルスに感染した通信端末10のアドレスとして指定している。図10の例では、解析部31は、Syslog テンプレートST1と Syslog の文字列を比較することにより、172.16.1.1のアドレスが割り当てられた通信端末10（通信端末10c）がウイルスに感染したと判定する。 10

【0055】

解析部31がウイルスに感染した通信端末10を特定した後に行う処理は、検知サーバ8からの通知がメールで行われた場合と同様である。すなわち、条件テーブル51を用いて処理に適用する実行テーブル61を決定すると共に、適用する実行テーブル61の情報と、ウイルスに感染した通信端末10のアドレスを処理決定部32に通知する。また、処理決定部32、通知処理部33、コマンド生成部40の処理も、検知サーバ8からの通知がメールで行われた場合と同様である。

【0056】

図11は、制御装置20が検知サーバ8からTrapを受信したときの解析処理の例を説明する図である。検知サーバ8は、IPアドレス=172.16.1.1（通信端末10c）がウイルスに感染したことを検出したとする。すると、検知サーバ8は、ウイルスを検出したことを通知するTrapを制御装置20に送信する。図11のTR1は、検知サーバ8から制御装置20に送信されるTrapの例である。TR1では、OID (Object Identifier) = 1.3.6.1.2.3.4.5.6について、ウイルス検知の情報が通知されている。また、ウイルスが検知された通信端末10のアドレスが172.16.1.1であることもTR1に含められている。 20

【0057】

制御装置20の解析部31は、受信部22を介してTrapを取得すると、Trapを条件テーブル51中の各条件と比較する。図11は、図を見やすくするために、条件テーブル51のうちでTrapによる通知に適用可能な条件の例を抽出して示している。図11の例では、条件テーブル51には、Trap中に「event:VIRUS Detect.ip-address」という文字列が含まれている場合、いずれかの通信端末10がウイルスに感染したと判定することが記載されている。なお、メールでの通知の際と同様に、Trapの処理に使用される条件についても、通知対象として、その条件が使用されるときに不正な通信が検出された通信端末10のアドレスが対応付けられている。 30

【0058】

次に、解析部31は、ウイルスの感染が通知されたので、ウイルスの感染を通知する Trap の解析に使用するテンプレートをテンプレート情報52から選択する。図11の例では、条件テーブル51は、Trap テンプレートTT1を選択したとする。解析部31は、Trap を Trap テンプレートTT1と比較する。Trap テンプレートTT1は、Trap 中の event の記載を「event:VIRUS Detect.ip-address \$1」という文字列としたときの「\$1」に該当する文字列を、ウイルスに感染した通信端末10のアドレスとして指定している。図11の例では、解析部31は、Trap テンプレートTT1と Trap の文字列を比較することにより、172.16.1.1のアドレスが割り当てられた通信端末10（通信端末10c）がウイルスに感染したと判定する。 40

【0059】

解析部31がウイルスに感染した通信端末10を特定した後に行う処理は、検知サーバ8からの通知がメールや Syslog で行われた場合と同様である。また、処理決定部32、通知処理部33、コマンド生成部40の処理も、検知サーバ8からの通知がメールで 50

行われた場合と同様である。

【0060】

図12は、装置の隔離の際に行われる処理の例を説明するフローチャートである。図12では、定数Nと変数nが使用される。定数Nは、攻撃の対象となった通信端末10を隔離するための制御の対象となる装置の総数であり、変数nは制御を行った装置の数を計数するために使用する変数である。

【0061】

制御装置20中の受信部22は、検知サーバ8で検出された攻撃の情報を受信する（ステップS1）。なお、攻撃として受信される情報は、ウイルスに対する感染に限られず、任意の種類不正な通信の検出が含まれる。解析部31は、検知サーバ8から受信した受信情報がメール形式であるかを判定する（ステップS2）。受信情報がメール形式である場合、解析部31は、メールテンプレートを用いて、ターゲットとなった通信端末10を特定する（ステップS2でYes、ステップS3）。なお、「ターゲット」は、不正な通信が検出された通信端末10であり、ウイルスなどのマルウェアによる攻撃のターゲットを含むものとする。検知サーバ8から受信した受信情報がメール形式ではない場合、解析部31は、検知サーバ8から受信した受信情報がSyslogであるかを判定する（ステップS2でNo、ステップS4）。受信情報がSyslogである場合、解析部31は、Syslogテンプレートを用いて、ターゲットとなった通信端末10を特定する（ステップS4でYes、ステップS5）。受信情報がSyslogではない場合、解析部31は、Trapテンプレートを用いて、ターゲットとなった通信端末10を特定する（ステップS4でNo、ステップS6）。

【0062】

ステップS3、S5、S6のいずれかの処理が終わると、解析部31は、条件テーブル51を用いて、適用する実行テーブル61を選択する（ステップS7）。解析部31は、実行テーブル61の選択結果とターゲットとなった通信端末10を、処理決定部32に通知する。処理決定部32は、選択された実行テーブル61から、制御対象の装置の総数（N）と制御対象の装置の情報を取得する（ステップS8）。コマンド生成部40は、変数nを1に設定する（ステップS9）。コマンド生成部40は、n番目の制御対象に送信するコマンドを生成し、送信部23を介してコマンドを含む制御パケットをn番目の制御対象に送信する（ステップS10）。その後、コマンド生成部40は、変数nが定数N以上であるかを判定する（ステップS11）。変数nが定数N未満の場合、コマンド生成部40は、変数nを1つインクリメントして、ステップS10に戻る（ステップS11でNo、ステップS12）。一方、変数nが定数N以上の場合、コマンド生成部40は、制御対象の全ての装置にコマンドを送信したと判定して、処理を終了する（ステップS11でYes）。

【0063】

このように、第1の実施形態にかかる方法によると、ネットワーク中の転送装置に対して、検出された不正通信の種類等に応じた制御を簡便に行うことができる。さらに、マルウェアの種類に応じて、適用されるテンプレートや実行テーブル61を変更することにより、マルウェアの種類等に応じて、ネットワークの制御内容を変更することもできる。従って、制御装置20を備えるシステムでは、簡便な処理で、様々な不正な通信に対して異なる対応を取ることができる。

【0064】

ところで、検知サーバ8から受信した情報の処理は解析部31で行われ、各装置への制御処理はコマンド生成部40と送信部23の処理により行われる。このため、検知サーバ8やシステム中の転送装置の仕様が変更されても、制御装置20の変更は限定的になるので、制御装置20の開発が容易である。また、第1の実施形態にかかる制御装置20では、検知サーバ8からの通知に基づいて、攻撃が確認されたときの処理を自律的に実行することができるため、感染確認後の処理が迅速に行われる。

【0065】

さらに、制御装置 20 には、制御装置 20 中に格納されている条件テーブル 51 や実行情報データベース 60 などの情報を変更することにより、制御の内容も柔軟に変更できるという利点もある。近年、マルウェアの種類も急増している上、例えば、ターゲットとなっている通信端末 10 のケーブルの接続を変更した場合や電源を切った場合に解析が困難になるマルウェアが開発されるなど、マルウェアの挙動も様々である。このため、制御内容を柔軟に変更可能な制御装置 20 を用いたシステムでは、オペレータの管理が簡便になる。

【0066】

＜第 2 の実施形態＞

第 2 の実施形態では、ターゲットとなった通信端末 10 からマルウェアを駆除できた場合などに、制御装置 20 が、隔離した通信端末 10 が隔離前と同様に通信できるように、転送装置を制御する場合について説明する。まず、隔離の解除の際に使用される情報の例を説明する。なお、装置テーブル 53 は、通信端末 10 の隔離の解除の際と通信端末 10 の隔離の際で同じものが使用される。

【0067】

図 13 は、隔離状況テーブル 56 と実行テーブル 61 の例を説明する図である。図 13 は、通信端末 10 c が隔離されている場合の隔離状況テーブル 56 の例を示している。図 13 の例では、隔離状況テーブル 56 には、隔離 ID、IP アドレス、検知日時、実行テーブルが記録されている。ここで、隔離 ID は、隔離処理ごとに対応付けられた識別情報であり、隔離の対象となった通信端末 10 ごとに異なる ID が割り当てられる。IP アドレスは、隔離の対象となっている通信端末 10 に割り当てられている IP アドレスである。図 13 の例では、IP アドレスの欄に、通信端末 10 c のアドレス（172.16.1.1）が記録されている。検知日時は、通信端末 10 c が隔離される原因となった不正な通信が検知された時刻の情報である。実行テーブルは、そのエントリ中の通信端末 10 の隔離に使用された実行テーブル 61 の情報を特定する際に使用される任意の情報である。図 13 の例では、実行テーブルとして実行テーブル 61 a が 172.16.1.1 のアドレスが割り当てられている装置（通信端末 10 c）の隔離に使用されたことが記録されている。

【0068】

第 2 の実施形態では、処理決定部 32 は、隔離に使用される可能性のある実行テーブル 61 の各々について、その実行テーブル 61 で行った隔離処理を解除するために使用する処理を特定する情報を予め記憶しているとする。例えば、実行テーブル 61 a によって行われた隔離処理の解除には実行テーブル 61 b が使用可能であることを、処理決定部 32 が予め記憶しているとする。すると、図 13 の例では、通信端末 10 c の隔離処理に実行テーブル 61 a が使用されているので、処理決定部 32 は、通信端末 10 c の隔離の解除の際に実行テーブル 61 b を使用することを決定できる。

【0069】

図 13 は、実行テーブル 61 b として、IP アドレス＝172.16.1.1 のアドレスが割り当てられた通信端末 10 c の隔離を解除する際に使用される情報を含む実行テーブル 61 を示している。実行テーブル 61 b では、感染が検出された通信端末 10 の隔離の解除と、隔離を解除したことをオペレータへ通知するためのメール通知処理とが、処理内容として記録されている。さらに、通信端末 10 の隔離を解除する際に制御対象となる装置と、各制御対象の装置の制御のために実施されるコマンドのグループが各装置の情報に対応付けられている。

【0070】

例えば、図 4 に示すネットワークにおいて、通信端末 10 c に対する隔離を解除する際には、通信端末 10 c の隔離の際に制御対象となった、スイッチ 3 d とスイッチ 3 e に対して、通信端末 10 c を隔離する前の通信を再開させることになる。そこで、実行テーブル 61 b の例では、通信端末 10 c の隔離を解除するための制御対象として、ネットワーク N2 中のスイッチ 3 d とスイッチ 3 e が記録されている。実行テーブル 61 b でも、実

10

20

30

40

50

行テーブル 6 1 a (図 6) と同様に、スイッチ 3 d は A 社の製品であることと、スイッチ 3 d の制御に使用されるコマンドグループの情報 (C G 1 1) が記録されている。同様に、スイッチ 3 e についても、B 社の製品であることと、スイッチ 3 e の制御にはコマンドグループ C G 1 2 が使用されることが登録されている。さらに、実行テーブル 6 1 b には、通知先テーブル 5 4 に含まれている通知先の各々に対して、メールテンプレート M T 1 1 を用いて生成した通知メールを送信することが登録されている。

【0071】

図 1 4 は、コマンド情報 5 5 の例を説明する図である。コマンドグループ C G 1 1 は、スイッチ 3 d において、コマンドグループ C G 1 (図 7) による制御を解除するためのコマンドのグループである。コマンドグループ C G 1 1 には、インタフェース F a 0 / 1 に着信してくるパケットに対するフィルタリングに、A C L 番号 = 1 0 1 の条件を適用することが記載されている。ここで、A C L 番号 = 1 0 1 の条件は、コマンドグループ C G 1 による処理が行われる前に適用されていた条件である。すなわち、フィルタリングに A C L 番号 = 1 0 1 の条件を適用する処理は、通信端末 1 0 の隔離を行う前のフィルタリングの条件を使用することを表わしている。さらに、コマンドグループ C G 1 1 には、アクセス制御のための条件文を削除するためのコマンドが含まれている。コマンドグループ C G 1 1 には、隔離の解除対象の通信端末 1 0 の I P アドレスに置換される情報として、\$ 1 が含まれている。コマンドグループ C G 1 1 のうち条件文の削除用の 1 つ目のコマンドは、隔離の解除対象の通信端末 1 0 を送信元とする I P パケットのうち、1 0 . 0 . 1 0 . 1 5 (検疫サーバ 2 の I P アドレス) 宛のパケットを許可する設定の削除を表わしている。条件文の削除用の 2 つ目のコマンドでは、隔離の解除対象の通信端末 1 0 を送信元とする I P パケット全てを拒否する設定を削除することが記載されている。条件文の削除用の 3 つ目のコマンドでは、A C L 番号 = 1 0 2 の条件において送信元と宛先がいずれであっても、パケットを許可する設定の削除が記載されている。条件文の削除用の 4 つ目のコマンドでは、A C L 番号 = 1 0 2 の条件において、送信元と宛先がいずれであっても、パケットを拒否する設定を削除することが記載されている。

【0072】

設定ブロック 4 1 a は、コマンドグループ C G 1 1 のコマンド中の \$ 1 という文字列を、隔離の解除対象として指定された装置のアドレスに置き換えることにより、制御処理に使用されるコマンドを生成する。図 1 4 中の C 1 1 は、コマンドグループ C G 1 1 中の条件文中の \$ 1 という文字列が通信端末 1 0 c (I P アドレス = 1 7 2 . 1 6 . 1 . 1) に置き換えられた場合のコマンドの例である。

【0073】

図 1 5 は、隔離の解除の際に行われる処理の例を説明する図である。以下、図 1 3 と図 1 4 を参照しながら説明した情報が使用される場合について、通信端末 1 0 c の隔離が解除される場合の処理の例を説明する。なお、第 2 の実施形態においても、不正な通信の検出に伴う隔離のための制御は、第 1 の実施形態と同様に行われているものとする。

【0074】

オペレータは、ターゲットとなった通信端末 1 0 からマルウェアを駆除できた場合などに、隔離の解除を制御装置 2 0 に要求するための処理を行う。オペレータは、例えば、制御装置 2 0 の入力装置 1 0 3 から、隔離の解除を要求する通信端末 1 0 に割り当てられた I P アドレスを入力しても良い。また、オペレータは、システムの管理に使用する管理端末 8 0 から制御装置 2 0 に対して、解除を要求する通信端末 1 0 に割り当てられた I P アドレスを含む要求パケットを送信しても良い。

【0075】

手順 P 3 1 において、解析部 3 1 は、管理装置 8 0 からの通知や入力装置 1 0 3 から入力された情報を取得すると、得られた情報から、隔離を解除する通信端末 1 0 の I P アドレスを特定する。解析部 3 1 は、特定した I P アドレスと、隔離の解除処理が要求されていることを、処理決定部 3 2 に通知する。

【0076】

処理決定部 3 2 は、図 1 3 に示す隔離状況テーブル 5 6 と実行テーブル 6 1 b を用いて得られた情報のうち、以下の情報を設定ブロック 4 1 a に出力する（手順 P 3 2）。

隔離が解除される装置のアドレス：1 7 2 . 1 6 . 1 . 1（通信端末 1 0 c）

制御対象 1：スイッチ 3 d

制御対象 1 に適用するコマンド：コマンドグループ C G 1 1

設定ブロック 4 1 a は、これらの情報を取得すると、コマンドグループ C G 1 1（図 1 4）のコマンド中の \$ 1 という文字列を、隔離の解除対象の装置のアドレスに置き換えることにより、制御処理に使用されるコマンド（図 1 4 の C 1 1）を生成する。

【0 0 7 7】

同様に、処理決定部 3 2 は、実行テーブル 6 1 b（図 1 3）を用いて得られた情報のうち、以下の情報を設定ブロック 4 1 b に出力する（手順 P 3 3）。

隔離が解除される装置のアドレス：1 7 2 . 1 6 . 1 . 1（通信端末 1 0 c）

制御対象 2：スイッチ 3 e

制御対象 2 に適用するコマンド：コマンドグループ C G 1 2

設定ブロック 4 1 b は、これらの情報を取得すると、コマンドグループ C G 1 2 のコマンド中の \$ 1 という文字列を、隔離の解除対象の装置のアドレスに置き換えることにより、制御処理に使用されるコマンドを生成する。

【0 0 7 8】

設定ブロック 4 1 a および設定ブロック 4 1 b は、生成したコマンドをプロトコル処理部 4 2 に出力する（手順 P 3 4、P 3 5）。このとき、設定ブロック 4 1 a と設定ブロック 4 1 b は、コマンドの送信に使用される情報を、装置テーブル 5 3（図 7）から取得すると共に、取得した情報をコマンドに対応付けてプロトコル処理部 4 2 に出力する。なお、装置テーブル 5 3 から設定ブロック 4 1 が取得する情報等は、図 8 を参照しながら説明した手順 P 2 3、P 2 4 と同様である。プロトコル処理部 4 2 は、入力されたコマンドを、そのコマンドの宛先との間の通信に使用するプロトコルに応じた形式の制御パケットに含める。プロトコル処理部 4 2 は、生成した制御パケットを、送信部 2 3 を介して、宛先の装置に送信する（手順 P 3 6、P 3 7）。

【0 0 7 9】

手順 P 3 8 において、処理決定部 3 2 は、隔離が解除される装置のアドレスと、通知処理に使用するメールテンプレートを、通知処理部 3 3 に通知する。通知処理部 3 3 は、通知されたテンプレートとアドレス情報を用いて、通知先テーブル 5 4 中に記録されている装置への通知メールを送信する（手順 P 3 9）。手順 P 3 8 と手順 P 3 9 で行われる処理の詳細は、図 1 6 を参照しながら説明する。

【0 0 8 0】

図 1 6 は、メールによる通知処理の例を説明する図である。図 1 6 の例では、通知処理部 3 3 に対して、隔離が解除される通信端末 1 0 のアドレスが 1 7 2 . 1 6 . 1 . 1（通信端末 1 0 c）であることと、メールテンプレート M T 1 1 を使用することが通知されたとする。通知処理部 3 3 は、メールテンプレート M T 1 1 のうち、隔離が解除される通信端末 1 0 の I P アドレスと置換する対象の文字列を、処理決定部 3 2 から通知された I P アドレスに置き換える。図 1 6 中の M T 1 1 のうち、「% 1」に該当する文字列は、隔離が解除される通信端末 1 0 の I P アドレスと置換する対象の文字列である。そこで、通知処理部 3 3 は、メールテンプレート M T 1 1 中の「% 1」という文字列を、1 7 2 . 1 6 . 1 . 1 という I P アドレスに置き換えることにより、メール M 1 1 を生成する。

【0 0 8 1】

図 1 7 は、隔離の解除の際に行われる処理の例を説明するフローチャートである。図 1 7 において、定数 N は通信端末 1 0 の隔離状態を解除するための制御の対象となる装置の総数であり、変数 n は制御を行った装置の数を計数するために使用する変数である。

【0 0 8 2】

制御装置 2 0 中の受信部 2 2 は、管理装置 8 0 から隔離の解除の要求（隔離解除要求）を受信する（ステップ S 2 1）。処理決定部 3 2 は、隔離状況テーブル 5 6 を用いて、適

10

20

30

40

50

用する実行テーブル 61 を選択する（ステップ S 22）。処理決定部 32 は、選択した実行テーブル 61 から、制御対象の装置の総数（N）と制御対象の装置の情報を取得する（ステップ S 23）。コマンド生成部 40 は、変数 n を 1 に設定する（ステップ S 24）。コマンド生成部 40 は、n 番目の制御対象に送信するコマンドを生成し、送信部 23 を介して、n 番目の制御対象にコマンドを含む制御パケットを送信する（ステップ S 25）。その後、コマンド生成部 40 は、変数 n が定数 N 以上であるかを判定する（ステップ S 26）。変数 n が定数 N 未満の場合、コマンド生成部 40 は、変数 n を 1 つインクリメントして、ステップ S 25 に戻る（ステップ S 26 で No、ステップ S 27）。一方、変数 n が定数 N 以上の場合、コマンド生成部 40 は、制御対象の全ての装置にコマンドを送信したと判定して、処理を終了する（ステップ S 26 で Yes）。

10

【0083】

なお、図 13～図 17 にかかる説明では、隔離された通信端末 10 に対して、隔離の解除を行う場合を例として説明したが、管理装置 80 などからの解除処理に応答して行われる処理は、隔離の解除に限られない。例えば、通信端末 10 が使用可能な経路が制限されていた場合や、通信端末 10 が使用可能な転送速度が制限されていた場合には、第 2 の実施形態で説明した処理と同様の処理により、これらの制限が解除され得る。なお、その場合には、制限が行われている通信端末 10 と現在行われている制限を解除するために使用する実行テーブル 61 を一意に特定できる情報が、隔離状況テーブル 56 と同様の形式で保持されているものとする。

【0084】

20

このように、第 2 の実施形態にかかる方法によると、隔離された通信端末 10 などに對する処理の解除の際にも、ネットワーク中の転送装置に対して攻撃の種類等に応じた制御を簡便に行うことができる。従って、マルウェアの感染や不正な通信の検出後に行う処理だけでなく、不正な通信の検出に伴って行われた処理の解除も迅速に行われる。さらに、マルウェアの感染に対して行われる対処が多岐にわたっている場合、第 2 の実施形態で説明したように、マルウェアの感染に対する対処の解除に使用される実行テーブル 61 があらかじめ決定されていることにより、オペレータの負担は軽減される。従って、第 2 の実施形態を用いたシステムでは、オペレータの管理が簡便になる。

【0085】

< 第 3 の実施形態 >

30

システム中に含まれる装置が多い場合や、転送装置の入れ替えが発生する可能性が高い場合などには、第 1 および第 2 の実施形態よりも、さらに柔軟にシステムの設定を行うことができることが望ましい。このため、制御装置が記憶している情報は、システム設定を行いやすいように、適宜、複数のテーブルが統一されてもよく、1 つのテーブルやデータベースが複数に分割されてもよい。第 3 の実施形態では、このようなデータの変形の一例を、具体例を挙げて説明する。

【0086】

図 18 は、第 3 の実施形態にかかる制御装置 70 の構成の例を示す図である。制御装置 70 は、通信部 21、制御部 30、記憶部 45 を備える。記憶部 45 は、条件テーブル 73、実行情報データベース 77、装置テーブル 53、通知先テーブル 54、コマンド情報 55、隔離状況テーブル 56、テンプレート情報 78 を備える。通信部 21 と制御部 30 は、第 1 の実施形態と同様である。

40

【0087】

条件テーブル 73 は、テンプレート 71 と処理条件情報 72 を含む。テンプレート 71 は、第 1 の実施形態で説明したテンプレート情報 52 のうちで、検知サーバ 8 から送信された通知の解析に使用されるテンプレートに相当する。処理条件情報 72 は、第 1 の実施形態で説明した条件テーブル 51 の情報を含む。すなわち、第 3 の実施形態では、条件テーブル 73 は、条件テーブル 51 と通知の解析に使用するテンプレートを統合したテーブルとして、処理を適用する対象ごとに設定されている。なお、通知の解析に使用するテンプレート 71 として、通知メールの解析に使用されるメールテンプレート（MT1）、S

50

yslogテンプレート(ST1)、Trapテンプレート(TT1)などが、条件テーブル73に含められる。一方、テンプレート情報78は、制御装置70が通知先テーブル54中の通知先に送信するメールの生成に使用するテンプレートである。

【0088】

実行情報データベース77は、ポリシーマスタ75と実行テーブル76を含む。図18では図を見やすくするために、実行テーブル76を1つだけ図示しているが、実行情報データベース77には複数の実行テーブル76が含まれてもよい。ポリシーマスタ75は、実行情報データベース77に含まれている各実行テーブル76のいずれを適用するかを決定する際に使用される。装置テーブル53には、システム中の各転送装置の情報が、転送装置ごとに記録されている。制御装置70は、システム中の転送装置の数と同数の装置テーブル53を備えているものとする。

10

【0089】

制御装置70も、制御装置20と同様のハードウェアを備えているものとする。プロセッサ101は制御部30を実現し、メモリ102と記憶装置106は、記憶部45として動作する。また、ネットワークインタフェース109は、通信部21として動作する。

【0090】

図19は、条件テーブル73とポリシーマスタ75の例を説明する図である。条件テーブル73は、条件ID、情報ソースID、メールサーバID、メール差出人、メール件名、メールキーワード、IPアドレス、ポリシーID、条件有効フラグが含まれる。

【0091】

20

条件IDは、条件ごとに設定される識別情報である。情報ソースIDは、不正な通信の検出の通知に使用される情報源の種類の特定に使用される。図19の例では、情報ソースIDの値は、テーブルT1に示すように、1～3のいずれかの値に設定される。情報ソースID=1は、不正な通信の検出に関する情報がメールで制御装置70に通知されることを表す。同様に、情報ソースID=2は、不正な通信の検出に関する情報がSyslogで制御装置70に通知されることを表し、情報ソースID=3は、不正な通信の検出に関する情報がTrapで制御装置70に通知されることを表す。メールサーバIDは、不正な通信の検出に関する情報がメールで制御装置70に通知される場合の通知元となるメールサーバを識別する識別情報である。テーブルT2には、メールサーバIDに対応付けて、各メールサーバに関する詳細情報が記録されている。テーブルT2には、メールサーバIDに対応付けて、受信メールサーバのサーバ名、受信プロトコル、受信ポート、受信アカウント、ID、パスワードが記録されている。受信メールサーバのサーバ名はsample.comであり、受信プロトコルはPOP3 (Post Office Protocol Version 3)、受信ポート番号は110である。さらに、受信アカウントはtest@example.comであり、メール受信の際に使用されるIDはtest、メール受信の際に使用されるパスワードはtestである。メール差出人は、不正な通信の検出に関する情報がメールで制御装置70に通知される場合の通知元となるメールサーバが使用するメールアドレスであり、図19の例ではsend@example.comである。

30

【0092】

40

メール件名は、検知サーバ8から不正な通信の検出を制御装置70に通知するメールの件名に含まれる情報である。メールキーワードは、検知サーバ8が制御装置70に通知するメールの本文に含まれる情報であり、検知サーバ8がマルウェアを含むファイルや不正な通信に使用されているファイル等に対して行った処理の内容の通知に使用される定型文である。図19の例では、メール件名は「情報：ファイルの隔離」である。メールキーワードは、「ドメイン「FNETS」のコンピューター「%target_host」で次のイベントが発生しました：\nファイルの隔離\n結果：隔離しました」という文字列である。なお、メールキーワード中で、「¥n」は改行を表すものとする。メールキーワード中の「%target_host」は可変パラメータであり、不正な通信が検出された通信端末10に割り当てられたIPアドレスが設定される。すなわち、メール件名とメールキーワードの組み合わせは、第1の実施形態等のメールテンプレートMT1などに含まれる情報に相当する。

50

【0093】

図19に示す条件テーブル73には、その条件を適用するIPアドレスの範囲が設定されている。従って、制御装置70が記憶している条件テーブル73中のエントリのうち、IPアドレスの範囲を含む全ての条件が合致したエントリの情報が、以後の処理に使用される。条件テーブル73の例では、メール件名、メールキーワードが合致した上、隔離される対象の通信端末10に割り当てられたIPアドレスが、192.168.0.1から192.168.0.99の範囲に含まれる場合に、条件ID=1の条件が適用される。ポリシーIDは、ポリシーマスタ75での実行テーブル76の分類に使用される値であり、実行テーブル76を一意に識別する値である。図19の例では、ポリシーID=1である。条件有効フラグは、設定された条件を有効にするかを示すフラグである。条件有効フラグ=enableの場合、設定された条件が使用可能な状態にシステムが設定されていることを表す。一方、条件有効フラグ=disableの場合、設定された条件が使用可能な状態にシステムが設定されていないことを表す。従って、条件有効フラグ=disableに設定された条件は、制御装置70での処理に使用されない。

10

【0094】

解析部31は、検知サーバ8からの通知メールを取得すると、条件テーブル73中のメール件名とメールキーワードを用いて通知メールを解析することにより、ターゲットとなった通信端末10を特定する。さらに、解析部31は、通知メールの送信元などの情報をキーとして、条件テーブル73のうちで通知メールの処理に適用される可能性のある条件を絞り込む。さらに、解析部31は、絞り込んだ条件の中から、IPアドレスの適用範囲にターゲットとなった通信端末10のIPアドレスを含む条件を抽出する。抽出した条件の条件有効フラグがenableに設定されている場合、解析部31は、抽出した条件の中のポリシーIDをキーとして、ポリシーマスタ75を検索する。ここでは、解析部31がポリシーID=1の条件を適用することを決定したとする。

20

【0095】

ポリシーマスタ75は、ポリシーID、ポリシー名、ポリシーファイル名を含む。ポリシーマスタ75は、個々の実行テーブル76を1つのポリシーとして、各ポリシーのメタデータを格納する。ポリシー名は、ポリシーIDで特定されるポリシーの名称であり、ポリシーファイル名は、ポリシーIDで特定されるポリシーに相当する実行テーブル76の識別情報である。図19の例では、ポリシーID=1のポリシーのポリシー名はP01であり、ポリシーファイル名は実行テーブル76aである。

30

【0096】

解析部31は、ポリシーID=1をキーとして、図19中の条件テーブル73を検索したとする。すると、解析部31は、ポリシーID=1を適用するために実行テーブル76aが使用できると認識する。解析部31は、処理決定部32に対して、実行テーブル76aを使用することを要求する。

【0097】

図20は、実行テーブル76aと装置テーブル53aの例を説明する図である。実行テーブル76aには、実行テーブル76aに設定されているポリシーを実行する際の制御対象となる転送装置と各転送装置に対する処理が、処理対象リストとして含まれている。処理対象リストには、処理対象機器、設定コンフィグ、実行順などの情報が含まれる。実行テーブル76a中の設定処理機器の欄には、処理対象となる装置の情報を格納した装置テーブル53の識別情報が指定されている。以下の説明では、装置テーブル53aに情報が記録されている装置が、制御対象に選択されているとする。設定コンフィグは、処理対象の機器の設定に使用されるコマンド情報55を特定する情報である。図20の例では、設定コンフィグはコマンド情報55aである。実行順は、処理対象リストに複数の装置の情報が登録された場合の実行順序を表す。図20の例では、装置テーブル53aで特定される装置にコマンド情報55aを用いたコマンドによる設定を最初（実行順=1）に行うことが登録されている。

40

【0098】

50

処理決定部 32 は、実行テーブル 76 a から得られた情報を、コマンド生成部 40 に出力する。すると、コマンド生成部 40 は、処理決定部 32 から通知された装置テーブル 53 a のファイル名と、コマンド情報 55 a を用いて、コマンドの生成を開始する。

【0099】

装置テーブル 53 a には、機器種別、通信種別、接続先 IP アドレス、接続先 URL (Uniform Resource Locator) の他、装置テーブル 53 a に情報が登録されている装置に接続する際の実行権限ごとに使用可能な情報が含まれている。装置テーブル 53 a のうち、ユーザ名待ち受け、ユーザ名、パスワード待ち受け、パスワードは、設定変更を行わない一般のユーザ (User) としての権限でのアクセスに使用される。装置テーブル 53 a の例では、User の権限でのアクセスの際に、処理対象の装置から「Login:」という情報が制御装置 70 に送信されると、制御装置 70 中のコマンド生成部 40 は、「admin」というユーザ名を出力する。同様に、User の権限でのアクセスの際に、処理対象の装置から「Password:」という情報が制御装置 70 に送信されると、制御装置 70 中のコマンド生成部 40 は、「fnet s」というデータを出力する。

【0100】

管理モードコマンド、管理ユーザ名待ち受け、管理ユーザ名、管理パスワード待ち受け、管理パスワード、管理モード終了コマンドは、User よりもアクセス権限の大きなユーザ (Enable) としての権限でのアクセスに使用される。制御装置 70 は、処理対象の装置から管理ユーザ名待ち受けが通知されると、その装置にアクセスするために管理ユーザ名を出力する。同様に、制御装置 70 は、処理対象の装置から管理パスワード待ち受けが通知されると、その装置にアクセスするために、管理パスワードを出力する。管理モードコマンドは、Enable としての権限でのアクセス時に使用され、管理モード終了コマンドは Enable としての権限でのアクセスの終了時に使用される。

【0101】

コンフィグモードコマンド、コンフィグユーザ名待ち受け、コンフィグユーザ名、コンフィグパスワード待ち受け、コンフィグパスワード、コンフィグモード終了コマンド、設定保存コマンドは、Config としての権限でのアクセスに使用される。ここで、「Config」は、設定変更の可能なユーザである。制御装置 70 は、処理対象の装置からコンフィグユーザ名待ち受けが通知されると、その装置にアクセスするためにコンフィグユーザ名を出力する。同様に、制御装置 70 は、処理対象の装置からコンフィグパスワード待ち受けが通知されると、その装置にアクセスするために、コンフィグパスワードを出力する。コンフィグモードコマンドは、Config としての権限でのアクセス時に使用され、設定保存コマンドは設定した内容の保存の際に使用される。コンフィグモード終了コマンドは Config としての権限でのアクセスの終了時に使用される。

【0102】

なお、装置テーブル 53 中の項目のうち、装置テーブル 53 に情報が格納されている装置に対して制御装置 70 のアクセスに使用される情報に対応付けられた項目についてはデータが登録されるが、全てのデータが登録されなくても良い。例えば、Enable としての権限では制御装置 70 がアクセスしない転送装置については、Enable の権限でアクセスする際に使用される情報が装置テーブル 53 に登録されていなくても良い。

【0103】

図 21 は、コマンド情報 55 a の例を説明する図である。コマンド情報 55 a は、コマンドリストを含む。コマンドリストには、コマンドの適用先の機器の情報に対応付けて、コマンドの実行順、実行権限、実行コマンド、種別が記録される。図 21 の例では、コマンドの実行順の 1 番目に、Config としての実行権限でコマンド C01 が実行される。Config としての実行権限でのアクセスの際には、適宜、装置テーブル 53 a (図 20) において Config に対応付けられている情報が使用される。コマンド C01 の種類は BASE である。コマンドの種別には、BASE と ACTION があるものとする。コマンドの種別 = BASE に設定されているコマンドは、不正な通信が検出されていないときに使用されるコマンドである。一方、コマンドの種別 = ACTION に設定されて

いるコマンドは、不正な通信が通知されたことにより制御の際に使用されるコマンドである。

【0104】

図21中のコマンド情報55aには紙面の関係で1つのコマンドの登録例を示したが、コマンドの実行順に羅列すると、例えば、リストL1やリストL2に示すようなコマンドのリストが得られる。

【0105】

コマンド生成部40は、得られたコマンドのリストを通知するための制御パケットを生成し、送信部23を介して、処理対象の装置に送信する。このため、処理対象の転送装置は、制御パケットで指定されたコマンドを実行することにより、第1の実施形態と同様に、処理対象の通信端末10を隔離できる。

【0106】

図22は、通知先テーブル54と隔離状況テーブル56の例を説明する図である。処理決定部32は、実行テーブル76を用いて、ターゲットとなった通信端末10に対する隔離が行われるかを判定し、隔離が行われる場合には、ターゲットの通信端末10の情報を隔離状況テーブル56に記録する。なお、第1の実施形態や図19などを参照した説明では、ターゲットとなった通信端末10のIPアドレスだけが解析部31で検出されていたが、実装に応じて、ターゲットとなった通信端末10のホスト名も制御装置70などに通知されてもよい。この場合、解析部31は、メールテンプレート等の設定によっては、ターゲットとなった通信端末10のIPアドレスとともに、ホスト名も抽出できる。

【0107】

隔離状況テーブル56は、隔離ID、ホスト名、IPアドレス、検知日時、ポリシーIDなどが含まれる。隔離IDは、隔離された通信端末10の情報に対するエン트리番号である。ホスト名は、隔離された通信端末10に設定されたホスト名である。IPアドレスは、隔離された通信端末10に設定されたIPアドレスである。検知日時は、隔離された通信端末10で不正な通信が検知された時刻を表す。

【0108】

図22の例では、隔離ID=1として、okamura-pcというホスト名で、192.168.0.1というアドレスが割り当てられている通信端末10が隔離されたことが記録されている。さらに、okamura-pcというホスト名の通信端末10は2016年1月29日の11時29分に検出された攻撃により、ポリシーID=1で識別されるポリシー（実行テーブル76a）を用いて隔離されている。

【0109】

通知処理部33は、処理決定部32から隔離状況テーブル56が更新されたことを通知されたとする。すると、通知処理部33は、隔離状況テーブル56を参照することにより、ターゲットとなった通信端末10の情報を特定する。すると、通知先テーブル54の情報を用いて、通知先に処理内容を通知するメールを送信する。

【0110】

通知先テーブル54には、通知先ID、通知先名、通知先メールアドレスが含まれる。通知先IDは、通知先ごとのエン트리番号である。通知先名は、制御装置70での処理結果を送信する通知先のホスト名である。通知先メールアドレスは、制御装置70での処理結果を送信する通知先のメールアドレスである。図22の例では、通知先ID=1の情報として、検疫検知通知先というホスト名の装置に通知が送られる。なお、検疫検知通知先というホスト名の装置では、info@example.comというメールアドレスが使用されている。

【0111】

このため、図22の例では、info@example.comに宛てて、okamura-pcというホスト名で、192.168.0.1というアドレスが割り当てられている通信端末10が隔離されたことを通知するメールが送信される。このため、検疫検知通知先というホスト名の装置では、制御装置70によって行われた処理の内容が特定さ

れる。

【0112】

図23は、第3の実施形態で行われる処理の例を説明するフローチャートである。図23において、定数Nは通信端末10を隔離するための制御の対象となる装置の総数であり、変数nは制御を行った装置の数を計数するために使用する変数である。

【0113】

制御装置70中の解析部31は、条件テーブル73を用いて、検知サーバ8から通知された不正な通信が検出された通信端末10であるターゲットと、適用するポリシーのポリシーIDを特定する(ステップS31)。さらに、解析部31は、ポリシーIDに対応付けられた実行テーブル76を、ポリシーマスタ75を用いて特定する(ステップS32)。処理決定部32は、適用対象となる実行テーブル76中の制御対象の装置の総数Nを取得する(ステップS33)。コマンド生成部40は、変数nを1に設定する(ステップS34)。コマンド生成部40は、n番目の制御対象に対応付けられた実行コマンドを読み込んで制御パケットを生成し、送信部23は、生成された制御パケットを宛先に送信する(ステップS35)。その後、コマンド生成部40は、変数nが定数N以上であるかを判定する(ステップS36)。変数nが定数N未満の場合、コマンド生成部40は、変数nを1つインクリメントして、ステップS35に戻る(ステップS36でNo、ステップS37)。一方、変数nが定数N以上の場合、コマンド生成部40は、制御対象の全ての装置にコマンドを送信したと判定して、処理を終了する(ステップS36でYes)。

【0114】

なお、図18～図23にかかる説明では、通信端末10に対して隔離が行われる場合を例として説明したが、第1の実施形態等と同様に、攻撃の対象となった通信端末10に対して行われる処理は、実装に応じて任意に変更され得る。

【0115】

<その他>

第3の実施形態においても、第2の実施形態と同様の手順により、隔離などの解除を制御装置70が行っても良い。また、ワイルドカードマスクを用いた演算方法などの設定も、実装に応じて変更され得る。

【0116】

第3の実施形態では、設定用に使用されるテーブル等の情報の設定方法の変更例の一例を示したが、これらの情報の設定方法は、実装に応じて任意に変更され得る。例えば、図6などに示した実行テーブル61には、制御対象の装置と、各装置に対する実施コマンドが対応付けて登録されているが、実行テーブル61を複数のテーブルに分割しても良い。

【0117】

図24は、制御装置20や制御装置70が記憶する情報の変形例を説明する図である。図24は、実行テーブル61中の情報と条件テーブル51中の不正な通信の種別に関する情報とを、テーブルT11～T13に分けて保持する場合の例を示している。

【0118】

テーブルT11は、システム中の通信端末10の各々について、その通信端末10をターゲットとした不正な通信が検出された場合に、制御対象となる転送装置のリストを記録している。なお、テーブルT1の例では、検知サーバ8からの通知内容に基づいて転送装置を特定しやすくするために通信端末10のIPアドレスに対応付けて転送装置のリストを記憶する場合を示している。例えば、192.168.1.1(通信端末10c)をターゲットとする不正な通信が検出された場合、IPアドレス=10.0.0.1の装置(スイッチ3d)とIPアドレス=10.0.0.2の装置(スイッチ3e)が制御対象となる。

【0119】

テーブルT12は、不正な通信の種別に対応付けて、行われる制御の種類に対応付けている。例えば、テーブルT12によると、ウイルス感染検知が通知された場合、ターゲットとなっている通信端末10を隔離する制御が行われる。一方、バックドア通信の検知が

通知された場合、ターゲットとなっている通信端末10のIPアドレスを含むパケットの転送速度を閾値以下に制限するための制御が行われる。なお、テーブルT12の例では、不正な通信の種類に応じて制御が一意に特定できる場合を例として示しているが、同じ種類の不正な通信が通知されても、制御の内容をターゲットのアドレス等に応じて変更するように設定されていても良い。

【0120】

テーブルT13は、制御対象の転送装置と制御の種類に応じて使用される制御コマンド（コマンドグループ）を対応付けている。例えば、IPアドレス＝10.0.0.1の装置（スイッチ3d）がターゲットの隔離のために制御される場合、コマンドグループCG1（図7）が使用され、ターゲットの隔離の解除のために制御される場合、コマンドグループCG11（図14）が使用される。同様に、IPアドレス＝10.0.0.2の装置（スイッチ3e）がターゲットの隔離のために制御される場合、コマンドグループCG2（図7）が使用される。また、ターゲットとなっている通信端末10のIPアドレスを含むパケットの転送速度を閾値以下に制限するためにIPアドレス＝10.0.0.1の装置（スイッチ3d）が制御される場合、コマンドグループCG15が使用される。なお、テーブルT13の例では、ターゲットの隔離だけでなく、隔離等の解除の処理も制御の種類として含めているが、隔離等の解除の処理はテーブルT13とは異なるテーブルに格納されていても良い。

【0121】

図24に示すようにテーブルが生成されている場合、解析部31は、検知サーバ8からの通知を用いて、ターゲットとなっている通信端末10と、不正な通信の種類を特定すると、特定した情報を処理決定部32に通知する。処理決定部32は、テーブルT11を参照して、制御対象とする転送装置を決定するとともに、不正な通信の種類をキーとしてテーブルT12を検索することにより、制御内容を特定する。処理決定部32は、制御対象とする転送装置と、制御内容の組み合わせをコマンド生成部40に通知する。すると、コマンド生成部40は、テーブルT13とコマンド情報55を用いて、制御対象となっている転送装置の各々について、処理決定部32で決定された制御内容に対応する制御コマンドを生成する。コマンド生成部40は、生成した制御コマンドを含む制御パケットを生成すると、送信部23を介して、制御対象の転送装置に制御パケットを送信する。

【0122】

一方、隔離等の解除要求を制御装置20が受信した場合には、処理決定部32は、解除の対象となる通信端末10のアドレスをキーとしてテーブルT11を検索することにより、制御対象の転送装置を特定できる。すると、処理決定部32は、隔離の解除が要求されていることと、制御対象の転送装置の情報を、コマンド生成部40に出力する。コマンド生成部40は、処理決定部32から取得した情報を用いてテーブルT13を検索することにより、ターゲットとなっている通信端末10の隔離の解除に使用するコマンドグループを特定できる。このため、コマンド生成部40は、特定したコマンドを用いた制御パケットを生成し、送信部23を介して、制御対象の転送装置に制御パケットを送信できる。

【0123】

図24に示すように変形されたデータが用いられている制御装置20や制御装置70を用いたシステムでも、第1～第3の実施形態と同様に、不正な通信の検出後の処理が簡便になる。

【0124】

上述の第1～第3の実施形態を含む実施形態に関し、さらに以下の付記を開示する。
（付記1）

通信端末と、前記通信端末で送受信されるパケットを転送する1つ以上の転送装置とを含むネットワーク中の前記転送装置を制御する制御装置に、

前記パケットを用いて通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信し、

前記検知情報から対象の通信端末と前記不正な通信の種類とを解析し、

10

20

30

40

50

解析した対象の通信端末に対応付けられた転送装置を記憶する第 1 の記憶情報を参照して制御対象の転送装置を決定し、

解析された前記不正な通信の種類に対応付けられた制御内容を記憶する第 2 の記憶情報を参照して制御対象に決定した転送装置に対する制御を決定し、

前記制御対象に決定された転送装置の種類ごとに、前記制御内容に対応する制御コマンドを記憶する第 3 の記憶情報から制御コマンドを読み出して、当該転送装置に対して制御コマンドを含む制御パケットを送信する

処理を実行させることを特徴とする制御プログラム。

(付記 2)

前記対象の通信端末に対する前記制御内容の解除を要求する解除要求を受信すると、前記第 3 の記憶情報を参照して、前記制御内容の解除に際して前記制御対象の転送装置の各々に適用する制御コマンドを生成すると共に、当該転送装置に、生成した制御コマンドを含む制御パケットを送信する

処理を前記制御装置に実行させることを特徴とする付記 1 に記載の制御プログラム。

(付記 3)

前記検知情報は、前記対象の通信端末と前記不正な通信の種類とを通知する通知メール、前記対象の通信端末で行われた通信履歴を表す履歴情報、または前記対象の通信端末と前記不正な通信の種類とを通知する制御情報のいずれかの形式から選択される

ことを特徴とする付記 1 または 2 に記載の制御プログラム。

(付記 4)

前記通知メールに含まれる文字列のうちで前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第 1 のテンプレート、前記履歴情報から前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第 2 のテンプレート、および、前記制御情報から前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第 3 のテンプレートを含み、

前記制御装置に、

前記通知メールを受信すると、前記第 1 のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出し、

前記履歴情報を受信すると、前記第 2 のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出し、

前記制御情報を受信すると、前記第 3 のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出する

処理を行わせることを特徴とする付記 3 に記載の制御プログラム。

(付記 5)

前記制御プログラムは、前記第 1 の記憶情報と前記第 2 の記憶情報とを、前記制御プログラムにより実行される情報を特定する実行テーブルとして備え、

前記実行テーブルは、前記複数の通信端末中の通信端末と前記不正な通信の種類との組み合わせに対応付けて、当該組み合わせが前記検知サーバから通知された場合に制御対象とする転送装置と、前記制御対象に決定された転送装置に対する制御を記憶する

ことを特徴とする付記 1 ～ 4 のいずれか 1 項に記載の制御プログラム。

(付記 6)

通信端末と、前記通信端末で送受信されるパケットを転送する 1 つ以上の転送装置とを含むネットワーク中の前記転送装置を制御する制御装置であって、

前記パケットを用いて通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信する受信部と、

前記検知情報から対象の通信端末と前記不正な通信の種類とを解析する解析部と、

解析した対象の通信端末に対応付けられた転送装置を記憶する第 1 の記憶情報を参照して制御対象の転送装置を決定すると共に、解析された前記不正な通信の種類に対応付けられた制御内容を記憶する第 2 の記憶情報を参照して制御対象に決定した転送装置に対する制御を決定する決定部と、

10

20

30

40

50

前記制御対象に決定された転送装置の種類ごとに、前記制御内容に対応する制御コマンドを記憶する第3の記憶情報から制御コマンドを読み出して生成された制御パケットを、当該転送装置に送信する送信部

を備えることを特徴とする制御装置。

(付記7)

前記対象の通信端末に対する前記制御内容の解除を要求する解除要求を前記受信部が受信すると、前記第3の記憶情報を参照して、前記制御内容の解除に際して前記制御対象の転送装置の各々に適用する制御コマンドを生成すると共に、生成した制御コマンドを含む当該転送装置宛の他の制御パケットを生成する生成部

をさらに備え、

前記送信部は、前記他の制御パケットを送信することを特徴とする付記6に記載の制御装置。

(付記8)

前記受信部は、前記対象の通信端末と前記不正な通信の種類とを通知する通知メール、前記対象の通信端末で行われた通信履歴を表す履歴情報、または前記対象の通信端末と前記不正な通信の種類とを通知する制御情報のいずれかの形式で前記検知情報を受信する

ことを特徴とする付記6または7に記載の制御装置。

(付記9)

前記通知メールに含まれる文字列のうちで前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第1のテンプレート、前記履歴情報から前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第2のテンプレート、および、前記制御情報から前記不正な通信の種類と前記対象の通信端末の通知に使用される領域を特定する第3のテンプレートを備え、

前記解析部は、

前記受信部が前記通知メールを受信すると、前記第1のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出し、

前記受信部が前記履歴情報を受信すると、前記第2のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出し、

前記受信部が前記制御情報を受信すると、前記第3のテンプレートを用いて前記不正な通信の種類と前記対象の通信端末を抽出する

ことを特徴とする付記8に記載の制御装置。

(付記10)

前記第1の記憶情報と前記第2の記憶情報とを、前記制御装置により実行される情報を特定する実行テーブルとして記憶する記憶部を備え、

前記実行テーブルは、前記複数の通信端末中の通信端末と前記不正な通信の種類との組み合わせに対応付けて、当該組み合わせが前記検知サーバから通知された場合に制御対象とする転送装置と、前記制御対象に決定された転送装置に対する制御を記憶する

ことを特徴とする付記6～9のいずれか1項に記載の制御装置。

(付記11)

通信端末と、前記通信端末で送受信されるパケットを転送する1つ以上の転送装置とを含むネットワーク中の前記転送装置を制御する制御装置が、

前記パケットを用いて通信端末の不正な通信を検知する検知サーバから通知される検知情報を受信し、

前記検知情報から対象の通信端末と前記不正な通信の種類とを解析し、

解析した対象の通信端末に対応付けられた転送装置を記憶する第1の記憶情報を参照して制御対象の転送装置を決定し、

解析された前記不正な通信の種類に対応づけられた制御内容を記憶する第2の記憶情報を参照して制御対象に決定した転送装置に対する制御を決定し、

前記制御対象に決定された転送装置の種類ごとに、前記制御内容に対応する制御コマンドを記憶する第3の記憶情報から制御コマンドを読み出して、当該転送装置に対して制御

10

20

30

40

50

コマンドを含む制御パケットを送信する
 処理を行うことを特徴とする制御方法。
 (付記 1 2)

前記対象の通信端末に対する前記制御内容の解除を要求する解除要求を受信すると、前記第 3 の記憶情報を参照して、前記制御内容の解除に際して前記制御対象の転送装置の各々に適用する制御コマンドを生成すると共に、当該転送装置に、生成した制御コマンドを含む制御パケットを送信する

処理を前記制御装置が行うことを特徴とする付記 1 1 に記載の制御方法。

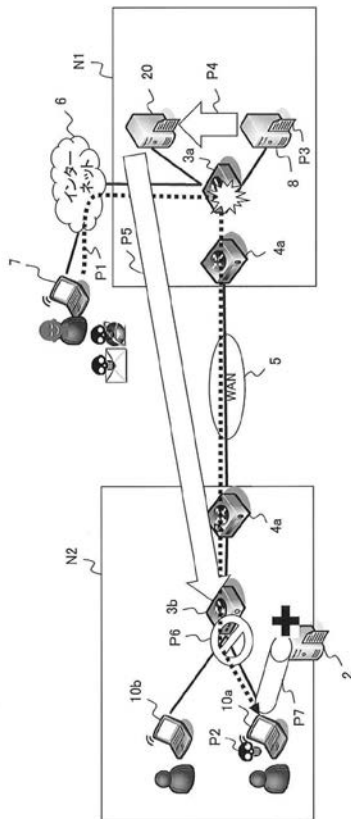
【符号の説明】

【0 1 2 5】

2	検疫サーバ	
3	スイッチ	
4	ルータ	
5	W A N	
6	インターネット	
7	C & Cサーバ	
8	検知サーバ	
10	通信端末	
20、70	制御装置	10
21	通信部	20
22	受信部	
23	送信部	
30	制御部	
31	解析部	
32	処理決定部	
33	通知処理部	
40	コマンド生成部	
41	設定ブロック	
42	プロトコル処理部	
45、50	記憶部	30
51、73	条件テーブル	
52、78	テンプレート情報	
53	装置テーブル	
54	通知先テーブル	
55	コマンド情報	
56	隔離状況テーブル	
60、77	実行情報データベース	
61、76	実行テーブル	
71	テンプレート	
72	処理条件情報	40
75	ポリシーマスタ	
101	プロセッサ	
102	メモリ	
103	入力装置	
104	出力装置	
105	バス	
106	記憶装置	
107	可搬記憶媒体駆動装置	
108	可搬記憶媒体	
109	ネットワークインタフェース	50

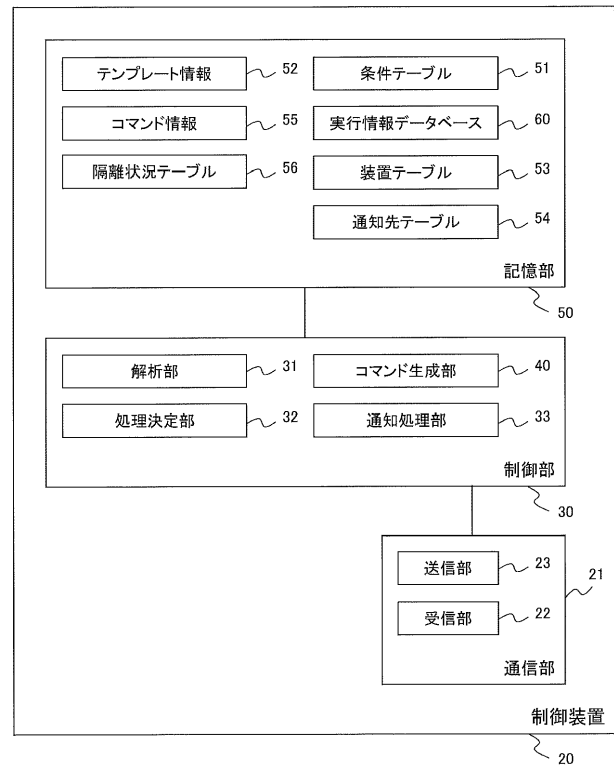
【図 1】

実施形態にかかる通信方法の例を説明する図



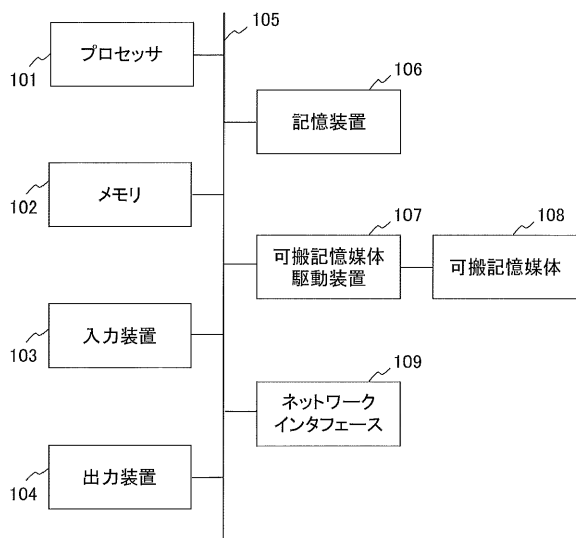
【図 2】

制御装置の構成の例を説明する図



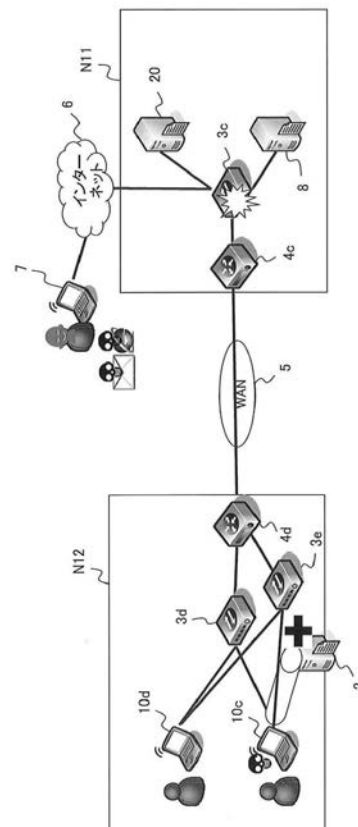
【図 3】

制御装置のハードウェア構成の例を説明する図



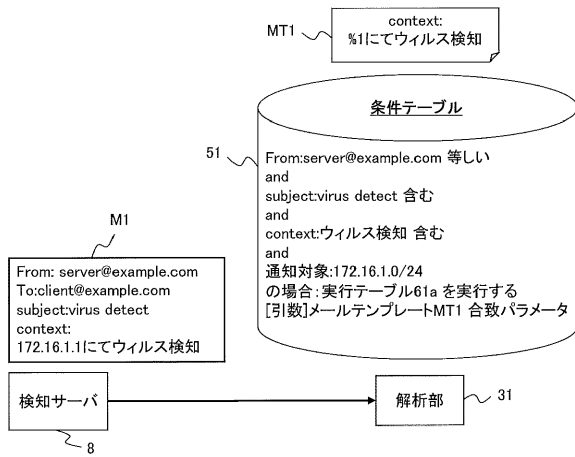
【図 4】

システムの例を説明する図



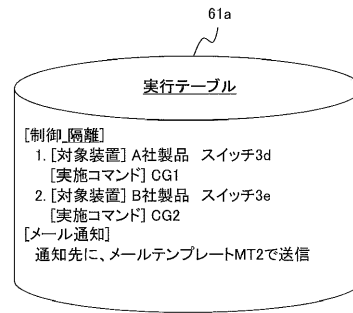
【図 5】

メールによる通知を受信したときの解析処理の例を説明する図



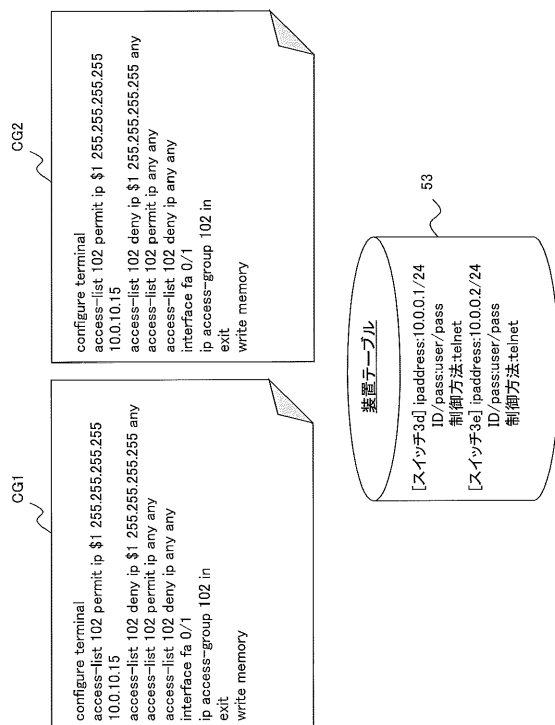
【図 6】

実行テーブルの例を説明する図



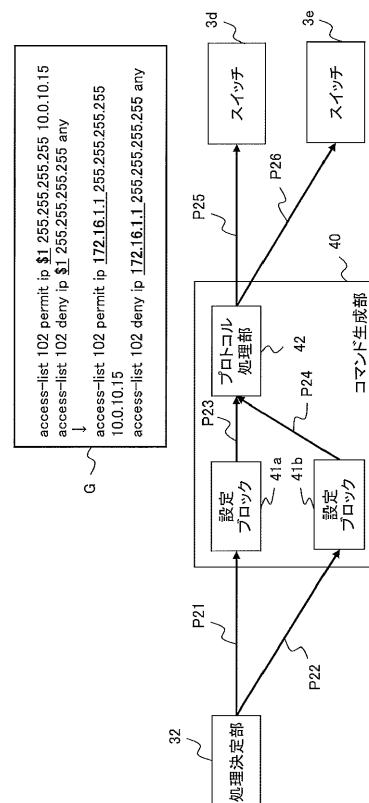
【図 7】

装置テーブルとコマンド情報の例を説明する図



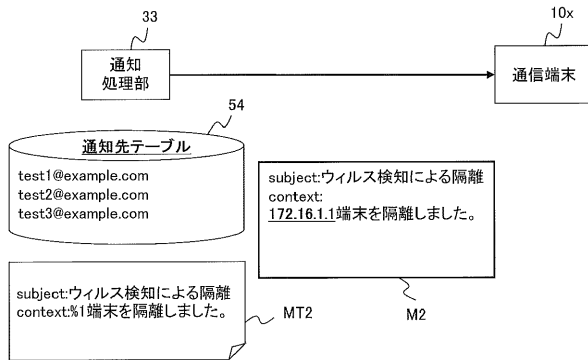
【図 8】

コマンドの生成処理の例を説明する図



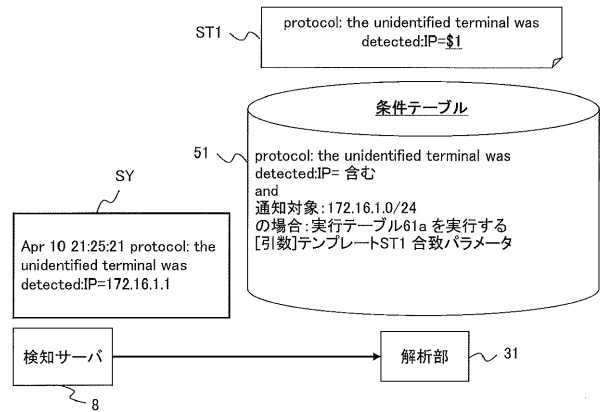
【図 9】

メールによる通知処理の例を説明する図



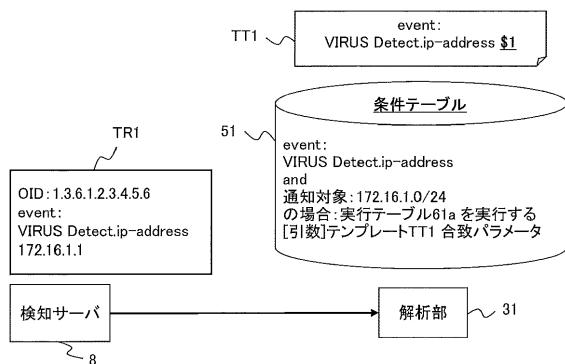
【図 10】

Syslogを受信したときの解析処理の例を説明する図



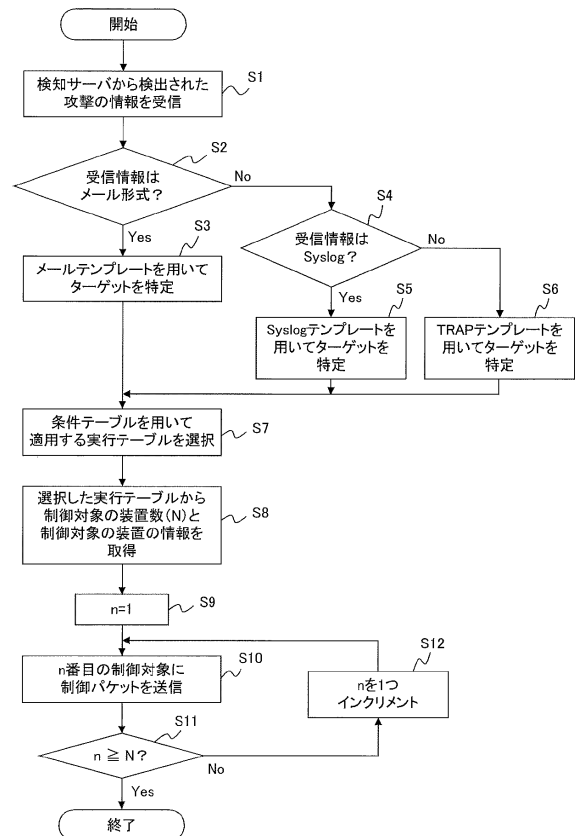
【図 11】

Trapを受信したときの解析処理の例を説明する図



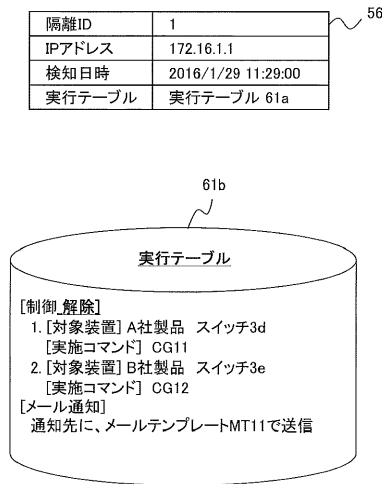
【図 12】

装置の隔離の際に行われる処理の例を説明するフローチャート



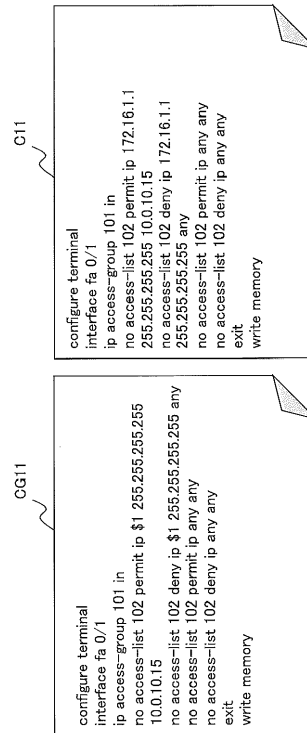
【図 1 3】

隔離状況テーブルと実行テーブルの例を説明する図



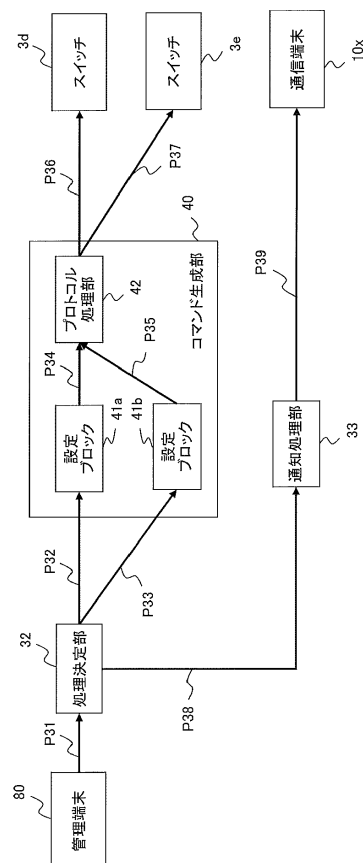
【図 1 4】

コマンド情報の例を説明する図



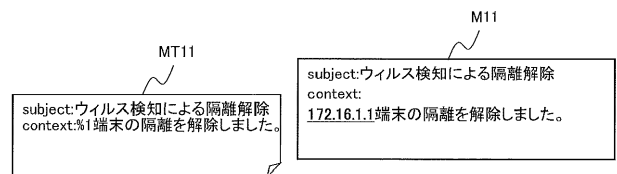
【図 1 5】

隔離の解除の際に行われる処理の例を説明する図



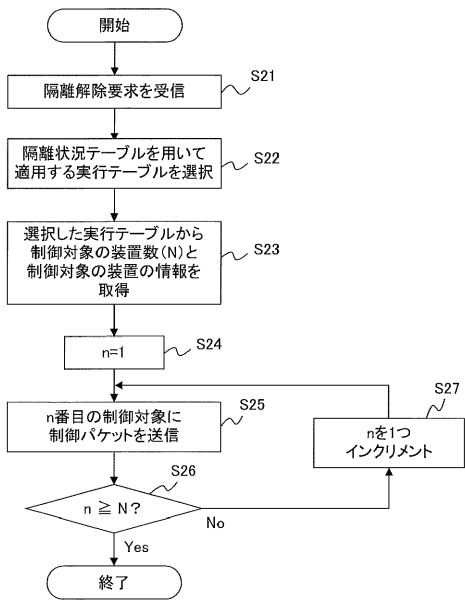
【図 1 6】

メールによる通知処理の例を説明する図



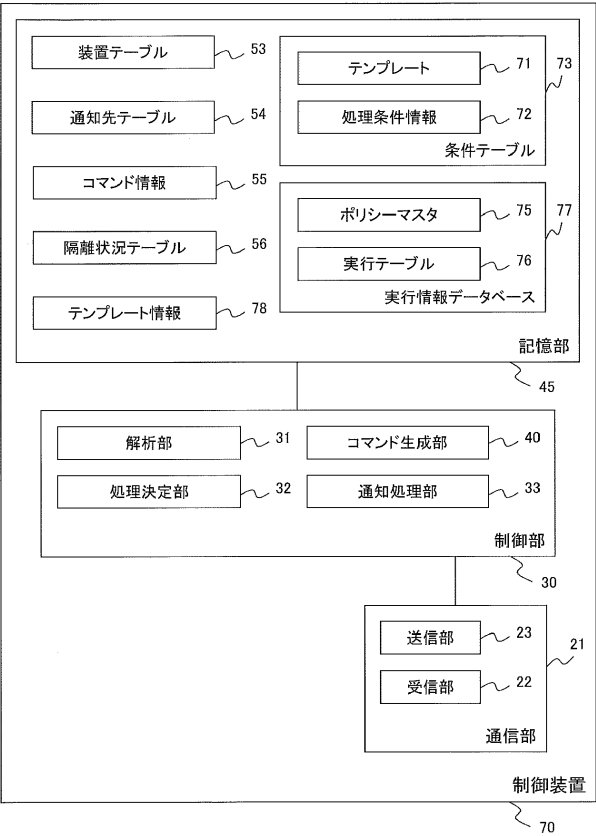
【図 1 7】

隔離の解除の際に行われる処理の例を説明するフローチャート



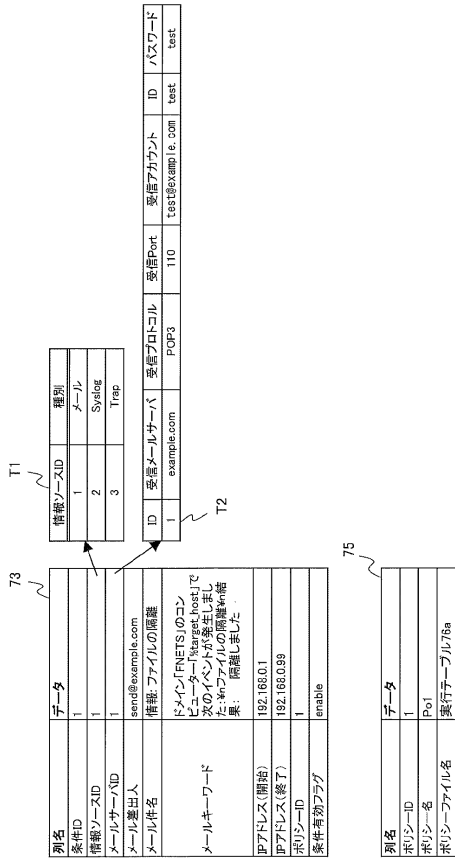
【図 1 8】

第3の実施形態にかかる制御装置の構成の例を示す図



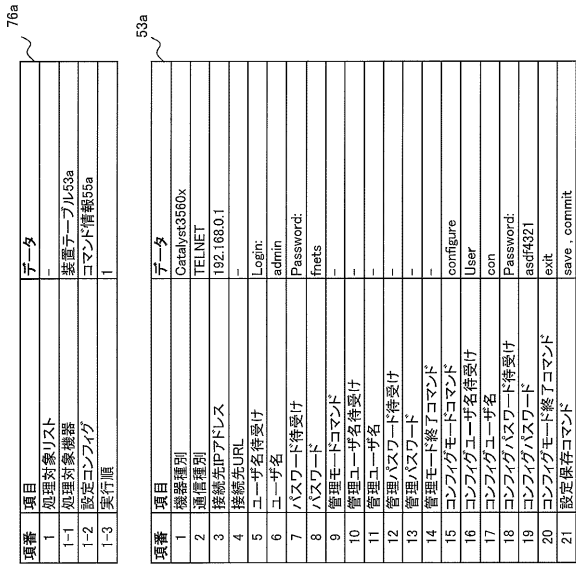
【図 1 9】

条件テーブルとポリシーマスタの例を説明する図



【図 2 0】

実行テーブルと装置テーブルの例を説明する図



【図 2 1】

コマンド情報の例を説明する図

項目	データ
1 コマンドリスト	Catalyst3560x
1-1 実行順	1
1-2 実行権限	CONFIG
1-3 実行コマンド	コマンド001
1-4 種別	BASE

55a

コマンドリスト	実行順	実行権限	実行コマンド	種別
Catalyst3560x	1	CONFIG	(config)# access-list 101 deny tftp 172.16.0.0 0.0.127 any echo	1BASE
Catalyst3560x	2	CONFIG	(config)# access-list 101 deny tcp 172.16.0.0 0.0.127 any eq ssh	1BASE
Catalyst3560x	3	CONFIG	(config)# access-list 101 permit ip any any	1BASE
Catalyst3560x	4	CONFIG	(config)# access-list 101 deny ip any any	1BASE
Catalyst3560x	5	CONFIG	(config)# interface fa 0/1	1BASE
Catalyst3560x	6	CONFIG	(config-if)# ip access-group 101 in	1BASE

L1

コマンドリスト	実行順	実行権限	実行コマンド	種別
Catalyst3560x	1	CONFIG	access-list 102 permit ip %target_host 255.255.255.255 192.168.0.100	2ACTION
Catalyst3560x	2	CONFIG	access-list 102 deny ip %target_host 255.255.255.255 any	2ACTION

L2

【図 2 2】

通知先テーブルと隔離状況テーブルの例を説明する図

列名	データ
通知先ID	1
通知先名	検疫検知通知先
通知先メールアドレス	info@example.com

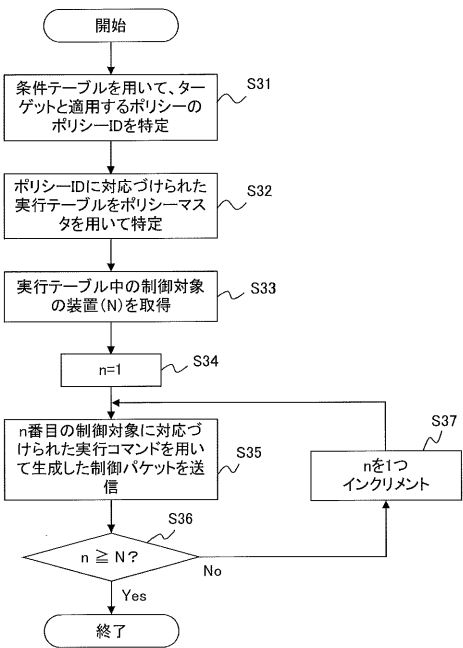
54

列名	データ
隔離ID	1
ホスト名	okamura-pc
IPアドレス	192.168.0.1
検知日時	2016/1/29 11:29:00
ポリシーID	1

56

【図 2 3】

第3の実施形態で行われる処理の例を説明するフローチャート



【図 2 4】

制御装置が記憶する情報の変形例を説明する図

通信端末	転送装置
192.168.1.1 (通信端末10c)	10.0.0.1 (スイッチ3d) 10.0.0.2 (スイッチ3e)
...	...

T11

不正な通信の種別	制御
ウイルス感染検知	ターゲットの隔離
バックドア通信検知	ターゲットのIPアドレスを含むパケットの転送速度を閾値以下に制限
...	...

T12

転送装置	制御	コマンド
10.0.0.1 (スイッチ3d)	ターゲットの隔離	コマンドグループCG1
	ターゲットに対する隔離の解除	コマンドグループCG11
	ターゲットのIPアドレスを含むパケットの転送速度を閾値以下に制限	コマンドグループCG15
	...	...
10.0.0.2 (スイッチ3e)	ターゲットの隔離	コマンドグループCG2
...	...	...

T13

フロントページの続き

- (72)発明者 島▲崎▼ 高広
神奈川県横浜市西区高島一丁目1番2号 富士通ネットワークソリューションズ株式会社内
- (72)発明者 真弓 英彦
神奈川県横浜市西区高島一丁目1番2号 富士通ネットワークソリューションズ株式会社内
- (72)発明者 松岡 周
神奈川県横浜市西区高島一丁目1番2号 富士通ネットワークソリューションズ株式会社内
- (72)発明者 岡村 敬
神奈川県横浜市西区高島一丁目1番2号 富士通ネットワークソリューションズ株式会社内
- (72)発明者 岡島 満
神奈川県横浜市西区高島一丁目1番2号 富士通ネットワークソリューションズ株式会社内
- Fターム(参考) 5B089 GA11 GA31 GB02 JB10 JB22 JB24 KA17 KC60 MC02
5K030 GA15 HA08 HB06 HC01 HC13 HD03 HD06 JA07 JA10 JA11
JT03 KA04 LA20 LB08 MA04 MC07 MC08