(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-500830
(P2018-500830A)
(43)公表日　平成30年1月11日(2018.1.11)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	***(2006.01)***	H04L	12/66	B	5K030
H04L 12/717	***(2013.01)***	H04L	12/717		
H04L 12/813	***(2013.01)***	H04L	12/813		

審査請求 有　予備審査請求 未請求　（全 47 頁）

(21)出願番号　特願2017-533598 (P2017-533598)
(86)(22)出願日　平成27年12月6日 (2015.12.6)
(85)翻訳文提出日　平成29年7月14日 (2017.7.14)
(86)国際出願番号　PCT/CN2015/096509
(87)国際公開番号　WO2016/101783
(87)国際公開日　平成28年6月30日 (2016.6.30)
(31)優先権主張番号　201410810857.X
(32)優先日　平成26年12月22日 (2014.12.22)
(33)優先権主張国　中国 (CN)

(71)出願人　504161984
ホアウェイ・テクノロジーズ・カンパニー・リミテッド
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション・ビルディング
(74)代理人　110000877
龍華国際特許業務法人

最終頁に続く

(54)【発明の名称】攻撃データパケット処理のための方法、装置、及びシステム

(57)【要約】
本発明の実施形態は、通信技術分野に関する攻撃データパケット処理のための方法、装置、及びシステムを提供し、攻撃データパケットがネットワークにおいて伝送された場合、攻撃データパケットが占有するネットワーク帯域幅を制限でき、これにより、正常なデータパケットの伝送を確保する。当該方法は、認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードによって受信する段階と、攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する段階と、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行するように、ＳＤＮコントローラを使用することによって、当該記述情報及び処理ポリシをスイッチに送信する段階であって、当該処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階とを備える。当該方法は、ネットワークセキュリティ維持技術に適用される。

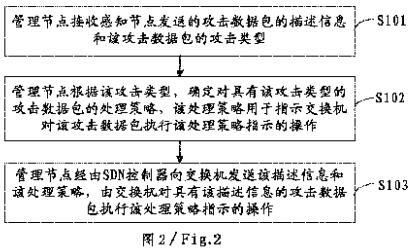


图2/Fig.2

S101 A management node receives description information and an attack type of the attack packet sent by a sensing node
S102 According to the attack type, the management node determines a processing policy with respect to the attack packet having the attack type, the processing policy being used to instruct an exchanger to conduct an operation instructed by the processing policy with respect to the attack packet
S103 The management node sends to the exchanger via a software defined network (SDN) controller the description information and the processing policy, and the exchanger conducts the operation instructed by the processing policy on the attack packet having the description information

【特許請求の範囲】
【請求項１】
攻撃データパケット処理方法であって、
認識ノードによって送信された、攻撃データパケットの記述情報及び前記攻撃データパケットの攻撃タイプを管理ノードによって受信する段階と、
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する段階であって、前記処理ポリシは、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階と、
前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示される前記オペレーションを前記スイッチが実行するように、ソフトウェアデファインドネットワーキングＳＤＮコントローラを使用することによって前記記述情報及び前記処理ポリシを前記管理ノードによって前記スイッチに送信する段階とを備える方法。
【請求項２】
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する前記段階は、
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する予め設定された処理ポリシを前記管理ノードによって取得する段階を含む、請求項１に記載の方法。
【請求項３】
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する前記段階は、
前記攻撃タイプ及び予め設定されたアルゴリズムに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって生成する段階を含む、請求項１に記載の方法。
【請求項４】
前記処理ポリシによって示される前記オペレーションは、
前記記述情報を有する前記攻撃データパケットに対する処理アクション、又は、前記記述情報を有する前記攻撃データパケットに対する処理アクション及び前記処理アクションを実行する時間を含む、
請求項１から３のいずれか一項に記載の方法。
【請求項５】
複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び前記複数の攻撃データパケットの攻撃タイプを前記管理ノードが受信した場合、
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する前記段階は、
少なくとも２つの同じ攻撃タイプを前記複数の攻撃データパケットの前記攻撃タイプに応じて前記管理ノードによって決定する段階と、
前記少なくとも２つの攻撃タイプのうちの１つに応じて、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する段階とを含む、請求項１から４のいずれか一項に記載の方法。
【請求項６】
ＳＤＮコントローラを使用することによって前記記述情報及び前記処理ポリシを前記管理ノードによって前記スイッチに送信する前記段階は、
前記ＳＤＮコントローラが、前記記述情報及び前記処理ポリシを前記スイッチに転送するように、予め設定された通信インタフェースを使用することによって前記記述情報及び前記処理ポリシを前記管理ノードによって前記ＳＤＮコントローラに送信する段階を含む、請求項１から５のいずれか一項に記載の方法。
【請求項７】
前記記述情報は、前記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、前記攻撃データパケットの送信元ポート番号、前記攻撃データパケットの宛先ＩＰ

アドレス、前記攻撃データパケットの宛先ポート番号、及び前記攻撃データパケットのプロトコル番号を含む、
請求項１から６のいずれか一項に記載の方法。
【請求項８】
攻撃データパケット処理方法であって、
管理ノードによって送信された、攻撃データパケットの記述情報と前記記述情報を有する前記攻撃データパケットに対する処理ポリシとをソフトウェアデファインドネットワーキングＳＤＮコントローラによって受信する段階と、
第１のスイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するように、前記記述情報及び前記処理ポリシを前記ＳＤＮコントローラによって前記第１のスイッチに送信する段階とを備える方法。
【請求項９】
管理ノードによって送信された、攻撃データパケットの記述情報と前記記述情報を有する前記攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する前記段階は、
前記管理ノードによって送信された前記記述情報及び前記処理ポリシを、予め設定された通信インタフェースを使用することによって前記ＳＤＮコントローラによって受信する段階を含む、請求項８に記載の方法。
【請求項１０】
管理ノードによって送信された、攻撃データパケットの記述情報と前記記述情報を有する前記攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する前記段階の後、前記方法は更に、
マスタＳＤＮコントローラが、前記記述情報及び前記処理ポリシを第２のスイッチに転送し、前記第２のスイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示される前記オペレーションを実行するように、前記記述情報及び前記処理ポリシを前記ＳＤＮコントローラによって、前記ＳＤＮコントローラに接続された前記マスタＳＤＮコントローラに送信する段階を含む、請求項８又は９に記載の方法。
【請求項１１】
攻撃データパケット処理方法であって、
認識ノードによって受信されたデータパケットを攻撃データパケットであると前記認識ノードによって識別する段階と、
前記攻撃データパケットの記述情報及び前記攻撃データパケットの攻撃タイプを前記認識ノードによって決定する段階と、
前記記述情報及び前記攻撃タイプを前記認識ノードによって管理ノードに送信する段階であって、前記攻撃タイプは、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを決定すべく前記管理ノードによって使用され、前記処理ポリシは、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される、段階とを備える方法。
【請求項１２】
前記記述情報は、前記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、前記攻撃データパケットの送信元ポート番号、前記攻撃データパケットの宛先ＩＰアドレス、前記攻撃データパケットの宛先ポート番号、及び前記攻撃データパケットのプロトコル番号を含む、
請求項１１に記載の方法。
【請求項１３】
認識ノードによって送信された、攻撃データパケットの記述情報及び前記攻撃データパケットの攻撃タイプを受信するよう構成される受信ユニットと、

前記受信ユニットによって受信された前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを決定するよう構成される決定ユニットであって、前記処理ポリシは、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、決定ユニットと、

前記スイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示される前記オペレーションを実行するように、前記受信ユニットによって受信された前記記述情報と、前記決定ユニットによって決定された前記処理ポリシとを、ソフトウェアデファインドネットワーキングＳＤＮコントローラを使用することによって前記スイッチに送信するよう構成される送信ユニットと、

を備える管理ノード。

【請求項１４】

前記決定ユニットは具体的に、前記受信ユニットによって受信された前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する予め設定された処理ポリシを取得するよう構成されている、

請求項１３に記載の管理ノード。

【請求項１５】

前記決定ユニットは具体的に、前記受信ユニットによって受信された前記攻撃タイプと予め設定されたアルゴリズムとに応じて、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを生成するよう構成されている、

請求項１３に記載の管理ノード。

【請求項１６】

前記決定ユニットによって決定された前記処理ポリシによって示される前記オペレーションは、

前記記述情報を有する前記攻撃データパケットに対する処理アクション、又は、前記記述情報を有する前記攻撃データパケットに対する処理アクション及び前記処理アクションを実行する時間を含む、

請求項１３から１５のいずれか一項に記載の管理ノード。

【請求項１７】

前記決定ユニットは具体的に、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び前記複数の攻撃データパケットの攻撃タイプを前記受信ユニットが受信した場合、少なくとも２つの同じ攻撃タイプを前記複数の攻撃データパケットの前記攻撃タイプに応じて決定し、前記少なくとも２つの攻撃タイプのうちの１つに応じて、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを決定するよう構成されている、

請求項１３から１６のいずれか一項に記載の管理ノード。

【請求項１８】

前記送信ユニットは具体的に、前記ＳＤＮコントローラが、前記記述情報及び前記処理ポリシを前記スイッチに転送するように、前記受信ユニットによって受信された前記記述情報と、前記決定ユニットによって決定された前記処理ポリシとを予め設定された通信インタフェースを使用することによって前記ＳＤＮコントローラに送信するよう構成されている、

請求項１３から１７のいずれか一項に記載の管理ノード。

【請求項１９】

前記受信ユニットによって受信された前記記述情報は、前記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、前記攻撃データパケットの送信元ポート番号、前記攻撃データパケットの宛先ＩＰアドレス、前記攻撃データパケットの宛先ポート番号、及び前記攻撃データパケットのプロトコル番号を含む、

請求項１３から１８のいずれか一項に記載の管理ノード。

【請求項２０】

管理ノードによって送信された、攻撃データパケットの記述情報と前記記述情報を有する前記攻撃データパケットに対する処理ポリシとを受信するよう構成される受信ユニットと、
第１のスイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するように、前記受信ユニットによって受信された前記記述情報及び前記処理ポリシを前記第１のスイッチに送信するよう構成される送信ユニットと
を備えるソフトウェアデファインドネットワーキングＳＤＮコントローラ。
【請求項２１】
前記受信ユニットは具体的に、前記管理ノードによって送信された前記記述情報及び前記処理ポリシを、予め設定された通信インタフェースを使用することによって受信するよう構成されている、
請求項２０に記載のＳＤＮコントローラ。
【請求項２２】
マスタＳＤＮコントローラが、前記記述情報及び前記処理ポリシを第２のスイッチに転送し、前記第２のスイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示される前記オペレーションを実行するように、前記送信ユニットは更に、前記受信ユニットによって受信された前記記述情報及び前記処理ポリシを前記マスタＳＤＮコントローラに送信するよう構成されている、
請求項２０又は２１に記載のＳＤＮコントローラ。
【請求項２３】
受信されたデータパケットを攻撃データパケットであると識別するよう構成される識別ユニットと、
前記識別ユニットによって識別された前記攻撃データパケットの記述情報と、前記攻撃データパケットの攻撃タイプとを決定するよう構成される決定ユニットと、
前記決定ユニットによって決定された前記記述情報及び前記攻撃タイプを管理ノードに送信するよう構成される送信ユニットであって、前記攻撃タイプは、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを決定すべく前記管理ノードによって使用され、前記処理ポリシは、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される、送信ユニットと、
を備える認識ノード。
【請求項２４】
前記決定ユニットによって決定された前記記述情報は、
前記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、前記攻撃データパケットの送信元ポート番号、前記攻撃データパケットの宛先ＩＰアドレス、前記攻撃データパケットの宛先ポート番号、及び前記攻撃データパケットのプロトコル番号を含む、
請求項２３に記載の認識ノード。
【請求項２５】
請求項１３から１９のいずれか一項に記載の管理ノード、請求項２０から２２のいずれか一項に記載のソフトウェアデファインドネットワーキングＳＤＮコントローラ、請求項２３又は２４に記載の認識ノード、及びスイッチ
を備える通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信技術分野に関し、特に、攻撃データパケット処理のための方法、装置、及びシステムに関する。
【背景技術】

【０００２】
クラウド技術の急速な発展とともに、クラウド技術の適用において、ますます問題が発生している。例えば、インターネットプロトコル（ＩＰ）通信中の様々な攻撃データパケットによって、例えば、分散型サービス拒否（ＤＤｏＳ）攻撃及び詐欺メッセージ攻撃によって、クラウドデータセンタのサーバ（略して、クラウドサーバ）が攻撃されることがある。従って、クラウドサーバのセキュアな通信を確保すべく攻撃データパケットを処理することが、クラウド技術の中核技術の１つになる。
【０００３】
現在、一般的な攻撃データパケット処理方式は次のようなものである。クラウドデータセンタのエントランスクラウドサーバ上に物理ファイアウォールを配置する、又は、クラウドデータセンタの各クラウドサーバにおいて動作するハイパーバイザ上に仮想ファイアウォールを配置することによって、クラウドサーバに入ろうと待機している全てのデータパケットが、確実に物理／仮想ファイアウォールによるフィルタリング及び転送を受けるようにする。従って、攻撃データパケットはフィルタリングにより除去され、攻撃データパケットのクラウドサーバへの侵入が阻止され、これにより、確実にクラウドサーバがセキュアな通信を実行できるようにする。具体的には、物理／仮想ファイアウォール用に従業員によって設定されたセキュリティポリシに従って、物理／仮想ファイアウォールは、ＩＰ層に入ろうと待機しているデータパケットによって搬送されるＩＰ層シグナリングを識別する。ＩＰ層シグナリングがセキュリティポリシに適合しない場合、物理／仮想ファイアウォールは、データパケットをフィルタリングして除去し、これにより、攻撃データパケットがクラウドサーバを攻撃するのを阻止し、更に、確実にクラウドサーバがセキュアな通信を実行できるようにする。
【０００４】
しかしながら、攻撃データパケットがクラウドサーバに侵入することをファイアウォールを使用することによって阻止するための上述の方法においては、攻撃データパケットがクラウドサーバに侵入することを阻止するのにファイアウォールしか使用され得ず、データパケットのファイアウォールへの転送を担うスイッチは、依然として、攻撃データパケットをファイアウォールに転送することがある、すなわち、攻撃データパケットはネットワークにおいて依然として伝送される。従って、異常なデータパケットが、大量のネットワーク帯域幅を占有し、正常なデータパケットの伝送に影響を及ぼす。
【発明の概要】
【０００５】
本発明は、攻撃データパケット処理のための方法、装置、及びシステムを提供する。当該方法は、攻撃データパケットがネットワークにおいて伝送された場合に、攻撃データパケットが占有するネットワーク帯域幅を制限でき、正常なデータパケットの伝送を確保する。
【０００６】
上述の目的を実現すべく、本発明においては以下の技術的解決手段が使用される。
【０００７】
第１態様において、本発明は攻撃データパケット処理方法を提供する。当該方法は、
認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードによって受信する段階と、
攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを管理ノードによって決定する段階であって、当該処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階と、
スイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、ソフトウェアデファインドネットワーキングＳＤＮコントローラを使用することによって、記述情報及び処理ポリシを管理ノードによってスイッチに送信する段階とを備える。

【０００８】
第１態様の第１の可能な実施方式において、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを管理ノードによって決定する段階は、
攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する予め設定された処理ポリシを管理ノードによって取得する段階を含む。
【０００９】
上述の第１態様に関して、第１態様の第２の可能な実施方式において、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを管理ノードによって決定する段階は、
攻撃タイプ及び予め設定されたアルゴリズムに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを管理ノードによって生成する段階を含む。
【００１０】
上述の第１態様、又は、第１態様の第１の可能な実施方式及び第１態様の第２の可能な実施方式のいずれか１つに関して、第３の可能な実施方式において、
処理ポリシによって示されるオペレーションは、
当該記述情報を有する攻撃データパケットに対する処理アクション、又は、当該記述情報を有する攻撃データパケットに対する処理アクション及び処理アクションを実行する時間を含む。
【００１１】
上述の第１態様、又は、第１態様の第１の可能な実施方式から第１態様の第３の可能な実施方式のいずれか１つに関して、第４の可能な実施方式において、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び複数の攻撃データパケットの攻撃タイプを管理ノードが受信した場合、
攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを管理ノードによって決定する段階は、
複数の攻撃データパケットの攻撃タイプに応じて、少なくとも２つの同じ攻撃タイプを管理ノードによって決定する段階と、
少なくとも２つの攻撃タイプのうちの１つに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを、管理ノードによって決定する段階とを含む。
【００１２】
上述の第１態様、又は、第１態様の第１の可能な実施方式から第１態様の第４の可能な実施方式のいずれか１つに関して、第５の可能な実施方式において、ＳＤＮコントローラを使用することによって、記述情報及び処理ポリシを管理ノードによってスイッチに送信する段階は、
ＳＤＮコントローラが、記述情報及び処理ポリシをスイッチに転送するように、予め設定された通信インタフェースを使用することによって、記述情報及び処理ポリシを管理ノードによってＳＤＮコントローラに送信する段階を含む。
【００１３】
上述の第１態様、又は、第１態様の第１の可能な実施方式から第１態様の第５の可能な実施方式のいずれか１つに関して、第６の可能な実施方式において、
記述情報は、攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び、攻撃データパケットのプロトコル番号を含む。
【００１４】
第２態様において、本発明は攻撃データパケット処理方法を提供する。当該方法は、
管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとをソフトウェアデファインドネットワーキングＳＤＮコントローラによって受信する段階と、
第１のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、記述情報及び処理ポリシをＳＤＮコン

トローラによって第１のスイッチに送信する段階とを備える。
【００１５】
第２態様の第１の可能な実施方式において、管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する段階は、
管理ノードによって送信された記述情報及び処理ポリシを、予め設定された通信インタフェースを使用することによってＳＤＮコントローラによって受信する段階を含む。
【００１６】
上述の第２態様、又は、第２態様の第１の可能な実施方式に関して、第２の可能な実施方式において、管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する段階の後、当該方法は更に、
マスタＳＤＮコントローラが、記述情報及び処理ポリシを第２のスイッチに転送し、第２のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、記述情報及び処理ポリシをＳＤＮコントローラによって、ＳＤＮコントローラに接続されたマスタＳＤＮコントローラに送信する段階を備える。
【００１７】
第３態様において、本発明は攻撃データパケット処理方法を提供する。当該方法は、
認識ノードによって受信されたデータパケットを攻撃データパケットであると認識ノードによって識別する段階と、
攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを認識ノードによって決定する段階と、
記述情報及び攻撃タイプを認識ノードによって管理ノードに送信する段階であって、攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される、段階と備える。
【００１８】
第３態様の第１の可能な実施方式において、
記述情報は、攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号を含む。
【００１９】
第４態様において、本発明は管理ノードを提供する。当該管理ノードは、
認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを受信するよう構成される受信ユニットと、
受信ユニットによって受信された攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定するよう構成される決定ユニットであって、当該処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、決定ユニットと、
スイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、ソフトウェアデファインドネットワーキングＳＤＮコントローラを使用することによって、受信ユニットによって受信された記述情報と、決定ユニットによって決定された処理ポリシとをスイッチに送信するよう構成される送信ユニットとを備える。
【００２０】
第４態様の第１の可能な実施方式において、
決定ユニットは具体的に、受信ユニットによって受信された攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する予め設定された処理ポリシを取得するよう構成

されている。
【００２１】
上述の第４態様に関して、第２の可能な実施方式において、
決定ユニットは具体的に、受信ユニットによって受信された攻撃タイプと予め設定されたアルゴリズムとに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを生成するよう構成されている。
【００２２】
上述の第４態様、又は、第４態様の第１の可能な実施方式及び第４態様の第２の可能な実施方式のいずれか１つに関して、第３の可能な実施方式において、
決定ユニットによって決定された処理ポリシによって示されるオペレーションは、
当該記述情報を有する攻撃データパケットに対する処理アクション、又は、当該記述情報を有する攻撃データパケットに対する処理アクション及び処理アクションを実行する時間を含む。
【００２３】
上述の第４態様、又は、第４態様の第１の可能な実施方式から第４態様の第３の可能な実施方式のいずれか１つに関して、第４の可能な実施方式において、
決定ユニットは具体的に、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報と、複数の攻撃データパケットの攻撃タイプとを受信ユニットが受信した場合、複数の攻撃データパケットの攻撃タイプに応じて、少なくとも２つの同じ攻撃タイプを決定し、少なくとも２つの攻撃タイプのうちの１つに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定するよう構成されている。
【００２４】
上述の第４態様、又は、第４態様の第１の可能な実施方式から第４態様の第４の可能な実施方式のいずれか１つに関して、第５の可能な実施方式において、
送信ユニットは具体的に、当該記述情報及び処理ポリシをＳＤＮコントローラがスイッチに転送するように、受信ユニットによって受信された記述情報と、決定ユニットによって決定された処理ポリシとを予め設定された通信インタフェースを使用することによってＳＤＮコントローラに送信するよう構成されている。
【００２５】
上述の第４態様、又は、第４態様の第１の可能な実施方式から第４態様の第５の可能な実施方式のいずれか１つに関して、第６の可能な実施方式において、
受信ユニットによって受信された記述情報は、攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号を含む。
【００２６】
第５態様において、本発明はソフトウェアデファインドネットワーキングＳＤＮコントローラを提供する。当該ＳＤＮコントローラは、
管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとを受信するよう構成される受信ユニットと、
第１のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、受信ユニットによって受信された記述情報及び処理ポリシを第１のスイッチに送信するよう構成される送信ユニットとを備える。
【００２７】
第５態様の第１の可能な実施方式において、
受信ユニットは具体的に、管理ノードによって送信された記述情報及び処理ポリシを、予め設定された通信インタフェースを使用することによって受信するよう構成されている。
【００２８】

上述の第５態様、又は、第５態様の第１の可能な実施方式に関して、第２の可能な実施方式において、
送信ユニットは更に、マスタＳＤＮコントローラが、記述情報及び処理ポリシを第２のスイッチに転送し、第２のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、受信ユニットによって受信された記述情報及び処理ポリシをマスタＳＤＮコントローラに送信するよう構成されている。
【００２９】
第６態様において、本発明は認識ノードを提供する。当該認識ノードは、
受信されたデータパケットを攻撃データパケットであると識別するよう構成される識別ユニットと、
識別ユニットによって識別された攻撃データパケットの記述情報と、攻撃データパケットの攻撃タイプとを決定するよう構成される決定ユニットと、
決定ユニットによって決定された記述情報及び攻撃タイプを管理ノードに送信するよう構成される送信ユニットであって、当該攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、当該処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される、送信ユニットとを備える。
【００３０】
第６態様の第１の可能な実施方式において、
決定ユニットによって決定された記述情報は、
攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号を含む。
【００３１】
第７態様において、本発明は通信システムを提供する。当該通信システムは、
上述の第４態様、又は、第４態様のいずれかの可能な実施方式に係る管理ノードと、上述の第５態様、又は、第５態様のいずれかの可能な実施方式に係るソフトウェアデファインドネットワーキングＳＤＮコントローラと、上述の第６態様、又は、第６態様の第１の可能な実施方式に係る認識ノードと、スイッチとを備える。
【００３２】
本発明は、攻撃データパケット処理のための方法、装置、及びシステムを提供する。当該方法は具体的に、認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードによって受信する段階、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する段階、及び、スイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、ＳＤＮコントローラを使用することによって、記述情報及び処理ポリシをスイッチに送信する段階であって、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階である。本発明において提供される攻撃データパケット処理のための方法、装置、及びシステムによれば、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信でき、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパ

ケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

【図面の簡単な説明】

【００３３】

本発明の実施形態における技術的解決手段をより明確に説明すべく、実施形態又は従来技術を説明するために必要な添付図面を以下で簡潔に紹介する。以下の説明における添付図面は、本発明の実施形態の添付図面の一部に過ぎず、全てではないことは明らかである。

【００３４】

【図１】本発明の実施形態に係る通信システムのブロック図１である。

【００３５】

【図２】本発明の実施形態に係る攻撃データパケット処理方法のフローチャート１である。

【００３６】

【図３】本発明の実施形態に係る攻撃データパケット処理方法のフローチャート２である。

【００３７】

【図４】本発明の実施形態に係る第１のスイッチのフローテーブルの概略図である。

【００３８】

【図５】本発明の実施形態に係る攻撃データパケット処理方法のフローチャート３である。

【００３９】

【図６】本発明の実施形態に係る攻撃データパケット処理方法の相互作用図１である。

【００４０】

【図７】本発明の実施形態に係る攻撃データパケット処理方法の相互作用図２である。

【００４１】

【図８Ａ】本発明の実施形態に係る攻撃データパケット処理方法の相互作用図３である。

【図８Ｂ】本発明の実施形態に係る攻撃データパケット処理方法の相互作用図３である。

【００４２】

【図９】本発明の実施形態に係る通信システムのブロック図２である。

【００４３】

【図１０】本発明の実施形態に係る通信システムのブロック図３である。

【００４４】

【図１１】本発明の実施形態に係る管理ノードの概略構造図である。

【００４５】

【図１２】本発明の実施形態に係るＳＤＮコントローラの概略構造図である。

【００４６】

【図１３】本発明の実施形態に係る認識ノードの概略構造図である。

【００４７】

【図１４】本発明の実施形態に係る管理ノードの概略ハードウェア構造図である。

【００４８】

【図１５】本発明の実施形態に係るＳＤＮコントローラの概略ハードウェア構造図である。

【００４９】

【図１６】本発明の実施形態に係る認識ノードの概略ハードウェア構造図である。

【００５０】

【図１７】本発明の実施形態に係る通信システムのブロック図４である。

【００５１】

【図１８】本発明の実施形態に係る通信システムのブロック図５である。

【発明を実施するための形態】
【００５２】
本発明の実施形態の添付図面を参照して本発明の実施形態における技術的解決手段を以下で明確に説明する。説明される実施形態が、本発明の実施形態の一部に過ぎず、全てではないことは明らかである。
【００５３】
本発明の実施形態において、認識ノードは、クラウドデータセンタにあり、攻撃データパケットを識別し得る任意のクラウドサーバ、例えば、様々なサービス処理仮想マシン（ＶＭ）、ハイパーバイザ、ファイアウォール、負荷分散装置、又はゲートウェイであってよい。管理ノードは、クラウドデータセンタの任意のサービス管理ノード又はポリシ管理ノード、例えば、ＶＭマネージャ、仮想化インフラストラクチャマネージャ（ＶＩＭ）、又は、ポリシ及び課金ルール機能（ＰＣＲＦ）ユニットであってよい。
【００５４】
本発明の実施形態において提供される攻撃データパケット処理方法は、ソフトウェアデファインドネットワーキング（ＳＤＮ）技術に基づいているネットワークアーキテクチャに適用されてよい。ＳＤＮ技術に基づいているネットワークアーキテクチャは、制御を転送から切り離す、直接プログラム可能なネットワークアーキテクチャである。ＳＤＮ技術に基づいているネットワークアーキテクチャにおいて、ネットワークにおける各データパケットの特定の転送経路及び転送ポリシは共にＳＤＮコントローラによって制御され、ＳＤＮコントローラは、データパケットの転送経路及び転送ポリシをＯｐｅｎＦｌｏｗプロトコルを使用することによってＳＤＮアーキテクチャのスイッチクラスタに送信し、スイッチクラスタのスイッチは、データパケットをクラウドデータセンタのクラウドサーバに転送する。ＳＤＮ技術に基づいているネットワークアーキテクチャのスイッチは、データパケットの転送ポリシ及び転送経路に応じてデータパケットを転送することしか担っていない。
【００５５】
例示的に、図１は、本発明の実施形態に係る通信システムのブロック図を示す。図１に示されるように、データセンタは３つのＶＭ及び１つのＶＭマネージャを有する。ＳＤＮ技術に基づいているネットワークアーキテクチャにおいて、データセンタの３つのＶＭとデータセンタ外のサーバとの間で実行されるデータパケット伝送と、３つのＶＭの間で実行されるデータパケット伝送との両方について、データパケットの転送経路及び転送ポリシは、ＳＤＮコントローラによって制御され、スイッチはデータパケットの転送を実施する。
【００５６】
本発明の実施形態は、攻撃データパケット処理方法を提供する。攻撃データパケットを処理するようスイッチを制御することによって、スイッチによる攻撃データパケットの転送が制限され得る。従って、ネットワークにおいて攻撃データパケットが伝送された場合の、攻撃データパケットが占有するネットワーク帯域幅が制限され、これにより、正常なデータパケットの伝送を確保し、更に、確実にクラウドデータセンタのクラウドサーバがセキュアな通信を実行できるようにする。
［実施形態１］
【００５７】
本発明の実施形態は、攻撃データパケット処理方法を提供する。図２に示されるように、当該方法は、以下の段階を含んでよい。
【００５８】
Ｓ１０１．管理ノードが、認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを受信する。
【００５９】
攻撃データパケットは、認識ノードに脅威を及ぼすデータパケット、例えば、不正な形式のパケットを有するデータパケット、パケット断片化例外を有するデータパケット、無

効な伝送制御プロトコル（ＴＣＰ）接続を使用したデータパケット、及び、特大のデータ量を有するデータパケットとして理解されてよい。

【００６０】

任意で、攻撃データパケットの記述情報は、攻撃データパケットのパケットヘッダから認識ノードによって取得された情報であってよく、具体的に、攻撃データパケットの送信元ＩＰアドレス、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号であってよい。攻撃データパケットの送信元ポート番号は具体的に、ユーザデータグラムプロトコル（ＵＤＰ）送信元ポート番号であってよく、攻撃データパケットの宛先ポート番号は具体的に、ＵＤＰ宛先ポート番号であってよい、又は、攻撃データパケットの送信元ポート番号は具体的に、ＴＣＰ送信元ポート番号であってよく、攻撃データパケットの宛先ポート番号は具体的に、ＴＣＰ宛先ポート番号であってよい。記述情報を使用することによって、スイッチは、当該記述情報を有する攻撃データパケットを処理できる。

【００６１】

攻撃データパケットの攻撃タイプは、限定はされないが、ＤＤｏＳ攻撃、セッション確立プロトコル（ＳＩＰ）ベースの攻撃、無効なＴＣＰ接続、特大のデータ量、詐欺メッセージ攻撃、及び同様のものを含んでよい。

【００６２】

Ｓ１０２．管理ノードが、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する。ここで、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される。

【００６３】

処理ポリシは、攻撃データパケットに対する処理アクション、例えば、ドロップ、専用アクセスレート（ＣＡＲ）、又はリダイレクトを含んでよい。或いは、処理ポリシは、攻撃データパケットに対する処理アクションと、処理アクションを実行する時間とを含んでよい。処理アクションを実行する時間は具体的に、直ちに処理アクションを実行する、遅延後に処理アクションを実行する、持続的に処理アクションを実行する、又は同様のことであってよい。

【００６４】

更に、本発明のこの実施形態において、管理ノードが攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する方式が複数存在する。管理ノードが攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定することは、以下の２つの可能な実施方式（方式１及び方式２）を使用することによって例示的に説明される。管理ノードが攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する他の全ての方式は、本発明の保護範囲に含まれるものとし、本発明において限定されない。

【００６５】

方式１：本発明のこの実施形態において、管理ノードは、攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する予め設定された処理ポリシを取得してよい。具体的には、攻撃タイプと処理ポリシとの間のマッピング関係は、管理ノードにおいて予め設定されてよい。攻撃タイプを受信した場合、管理ノードは、攻撃タイプに応じて、予め設定されたマッピング関係から、当該攻撃タイプに対応する処理ポリシを決定してよい、すなわち、当該攻撃タイプの攻撃データパケットに対する処理ポリシが決定される。

【００６６】

例えば、攻撃タイプと処理ポリシとの間の、管理ノードにおいて予め設定されたマッピング関係は、表１に示されるであろうと仮定する。表１の処理ポリシは、攻撃データパケットに対する処理アクションを含む。「Ｃａｒ＋１Ｍｂｐｓ」とは、特大のデータ量を有する攻撃データパケットに対して専用アクセスレートオペレーションを実行し、これによ

り、専用アクセスレートオペレーション後のデータパケットによって使用される最大帯域幅が１Ｍｂｐｓであることを示す。「Ｒｅｄｉｒｅｃｔ＋ｎｕｌｌ０」とは、ＳＩＰベースの攻撃のタイプの攻撃データパケットに対してリダイレクトオペレーションを実行し、これにより、攻撃データパケットが、ルーティングブラックホールインタフェースを示すｎｕｌｌ０インタフェースに転送され、ｎｕｌｌ０インタフェースに転送された全てのデータパケットがドロップされ、攻撃データパケットをｎｕｌｌ０インタフェースに転送することは、ネットワーク負荷に対してほとんど影響を及ぼさないことを示す。具体的には、例えば、管理ノードによって受信された攻撃タイプがＤＤｏＳ攻撃である場合、ＤＤｏＳ攻撃タイプの攻撃データパケットに対する処理ポリシは、表１に従って「ｄｒｏｐ」と決定されてよい。

【表１】

攻撃タイプ	処理ポリシ
ＤＤｏＳ攻撃	ｄｒｏｐ
特大のデータ量	Ｃａｒ＋1Ｍｂｐｓ
ＳＩＰベースの攻撃	Ｒｅｄｉｒｅｃｔ＋ｎｕｌｌ０

【００６７】

任意で、上記の表１における処理ポリシは、処理アクションと、処理アクションを実行する時間とを含んでよい。例えば、ＤＤｏＳ攻撃に対応する処理ポリシは、「Ｄｒｏｐ＋ｉｍｍｅｄｉａｔｅｌｙ」に予め設定されてよく、「Ｄｒｏｐ＋ｉｍｍｅｄｉａｔｅｌｙ」とは、ＤＤｏＳ攻撃タイプの攻撃データパケットに対してドロップオペレーションを直ちに実行することを示しており、ＳＩＰベースの攻撃に対応する処理ポリシは、「Ｒｅｄｉｒｅｃｔ＋ｎｕｌｌ０＋ｉｍｍｅｄｉａｔｅｌｙ＋ｄｕｒａｔｉｏｎ１８０」であってよく、「Ｒｅｄｉｒｅｃｔ＋ｎｕｌｌ０＋ｉｍｍｅｄｉａｔｅｌｙ＋ｄｕｒａｔｉｏｎ１８０」とは、ＳＩＰベースの攻撃のタイプの攻撃データパケットに対してリダイレクトオペレーションを直ちに実行し、これにより、当該攻撃データパケットは、ｎｕｌｌ０インタフェースに直ちに転送され、転送は１８０分にわたって連続的に実行されることを示している。

【００６８】

具体的な実施プロセスでは、実際のエンジニアリング要件に従って、攻撃タイプと処理ポリシとの間の適切なマッピング関係が管理ノードにおいて設定されてよく、このことは本発明において限定されないことに留意すべきである。

【００６９】

方式２：管理ノードが、攻撃タイプ及び予め設定されたアルゴリズムに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを生成する。具体的には、管理ノードにおいてアルゴリズムが予め設定されてよい。攻撃タイプを受信した場合、管理ノードは、当該攻撃タイプ用の予め設定されたアルゴリズム手順を実行することによって、当該攻撃タイプの攻撃データパケットに対する処理ポリシを生成する。

【００７０】

例示的に、管理ノードによって受信された攻撃タイプがＤＤｏＳ攻撃である場合、管理ノードは、予め設定されたアルゴリズムを使用することによって当該攻撃タイプのコードを計算し、当該攻撃タイプの攻撃データパケットに対する処理ポリシ「ｄｒｏｐ」を生成する、又は、管理ノードによって受信された攻撃タイプがＳＩＰベースの攻撃である場合、管理ノードは、予め設定されたアルゴリズムを使用することによって当該攻撃タイプのコードを計算し、当該攻撃タイプの攻撃データパケットに対する処理ポリシ「Ｒｅｄｉｒｅｃｔ＋ｎｕｌｌ０」を生成する。

【００７１】

具体的な実施プロセスでは、実際のエンジニアリング要件に従って、適切なアルゴリズ

ムが管理ノードにおいて設定されてよく、このことは本発明において限定されないことに留意すべきである。

【００７２】

Ｓ１０３：管理ノードが、ＳＤＮコントローラを使用することによって、記述情報及び処理ポリシをスイッチに送信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。

【００７３】

例示的に、攻撃データパケットの、管理ノードによって受信された記述情報は具体的に、「［１０．１１．１００．１００，１０．２２．２００．２００，６，１２３４，４３２１］」であり、ここで、１０．１１．１００．１００は、攻撃データパケットの送信元ＩＰアドレスを示し、１０．２２．２００．２００は、攻撃データパケットの宛先ＩＰアドレスを示し、１２３４は、攻撃データパケットの送信元ポート番号を示し、４３２１は、攻撃データパケットの宛先ポート番号を示し、攻撃データパケットのプロトコル番号は６であると仮定する。攻撃データパケットの、管理ノードによって受信された攻撃タイプは、ＤＤｏＳ攻撃であり、攻撃データパケットに対するものであり、攻撃タイプに応じて決定される処理ポリシは、「Ｄｒｏｐ＋ｉｍｍｅｄｉａｔｅｌｙ」である。管理ノードは、記述情報及び処理ポリシを「［１０．１１．１００．１００，１０．２２．２００．２００，６，１２３４，４３２１］＋Ｄｒｏｐ＋ｉｍｍｅｄｉａｔｅｌｙ」のフォーマットでＳＤＮコントローラに送信してよい。ＳＤＮコントローラは、受信した「［１０．１１．１００．１００，１０．２２．２００．２００，６，１２３４，４３２１］＋Ｄｒｏｐ＋ｉｍｍｅｄｉａｔｅｌｙ」を、Ｏｐｅｎ　Ｆｌｏｗプロトコルによって規定されるフォーマットでスイッチに転送する。

【００７４】

記述情報及び処理ポリシの受信後、スイッチは、処理ポリシに従って、記述情報を有する攻撃データを直ちにドロップする。このように、スイッチはもはや攻撃データパケットを転送せず、これにより、攻撃データパケットはネットワークにおいて伝送されない、すなわち、当該記述情報を有する攻撃データパケットはネットワーク帯域幅を占有せず、これにより、正常なデータパケットの伝送を確保する。

【００７５】

攻撃データパケットに対するものであり、攻撃タイプに応じて管理ノードによって決定された処理ポリシが「Ｃａｒ＋１Ｍｂｐｓ」である場合、管理ノードが記述情報及び処理ポリシをＳＤＮコントローラを使用することによってスイッチに送信した後、スイッチは、当該記述情報を有する攻撃データパケットに対して、専用アクセスレートオペレーションを実行し、これにより、ネットワークにおいて伝送された場合、当該記述情報を有する攻撃データパケットは、最大１Ｍｂｐｓの帯域幅を占有することが理解されるであろう。すなわち、スイッチが依然として攻撃データパケットを転送するにもかかわらず、攻撃データパケットは、ネットワークにおいて伝送された場合、最大１Ｍｂｐｓの帯域幅を占有する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保される。

【００７６】

更に、スイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するプロセスが、以下の実施形態において詳細に説明され、詳細は本明細書において更には説明されない。

【００７７】

本発明のこの実施形態は、攻撃データパケット処理方法を提供する。当該方法は、具体的に、認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードによって受信する段階、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する段階、及び、スイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレー

ションを実行するように、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信する段階であって、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階である。当該方法によれば、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信でき、これにより、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

【００７８】

本発明の実施形態は、攻撃データパケット処理方法を提供する。図３に示されるように、当該方法は、以下の段階を備えてよい。

【００７９】

Ｓ２０１．ＳＤＮコントローラが、管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとを受信する。

【００８０】

攻撃データパケットの記述情報、及び、当該記述情報を有する攻撃データパケットに対する処理ポリシについては、特に、図２に示される実施形態における関連する記載を参照してよく、詳細は本明細書において更には説明されない。

【００８１】

Ｓ２０２．ＳＤＮコントローラが、記述情報及び処理ポリシを第１のスイッチに送信し、これにより、第１のスイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。

【００８２】

第１のスイッチは、ＳＤＮコントローラによって制御されるスイッチクラスタの任意のスイッチである。

【００８３】

具体的には、ＳＤＮコントローラは、記述情報及び処理ポリシをコントローラ‐スイッチメッセージに変換し、コントローラ‐スイッチメッセージを第１のスイッチに送信してよい。コントローラ‐スイッチメッセージは、Ｏｐｅｎ　Ｆｌｏｗプロトコルによって規定されるメッセージタイプであり、ＳＤＮコントローラによってスイッチに送信されて、スイッチのフローテーブルに記録された情報を変更又はドロップするようスイッチに命令する。

【００８４】

ＳＤＮコントローラが記述情報及び処理ポリシをコントローラ‐スイッチメッセージへと変換し、コントローラ‐スイッチメッセージを第１のスイッチに送信した後、第１のスイッチは、コントローラ‐スイッチメッセージに含まれた記述情報に従って、記述情報に適合する攻撃データフローがないか第１のスイッチのフローテーブルを検索し、次に、コントローラ‐スイッチメッセージに含まれた処理ポリシに従って、攻撃データフローの攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する、すなわち、ＳＤＮコントローラは、処理ポリシに従って、当該記述情報を有する攻撃データパケットに対して処理ポリシによって示されるオペレーションを実行する。

【００８５】

図４は、本発明の実施形態に係る第１のスイッチのフローテーブルの概略図である。図４では、第１のスイッチのフローテーブルは、パケットヘッダフィールド、カウンタ、及びデータパケットに対して実行されるアクションを備える。パケットヘッダフィールドは具体的に、第１のスイッチによって受信されたデータフローの、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元媒体アクセス制御（ＭＡＣ）アドレス、宛先ＭＡＣアドレス、プロトコル番号、送信元ポート番号、宛先ポート番号、及び同様のものを含んでよい。カウンタは、第１のスイッチによって受信されたデータフローの、データパケット数、バイト数、伝送期間、及び同様のものに関する統計を収集するよう設定されている。データパケットに対して実行されるアクションは、データパケットの転送、データパケットのドロップ、フローテーブルにおけるデータパケットのパケットヘッダの情報の変更、及び同様のものを含んでよい。

【００８６】

例示的に、ＳＤＮコントローラによって受信された記述情報及び処理ポリシが、「［１０．１１．１００．１００，１０．２２．２００．２００，６，１２３４，４３２１］＋Ｄｒｏｐ＋ｉｍｍｅｄｉａｔｅｌｙ」であると仮定すると、ＳＤＮコントローラが「［１０．１１．１００．１００，１０．２２．２００．２００，６，１２３４，４３２１］＋Ｄｒｏｐ＋ｉｍｍｅｄｉａｔｅｌｙ」をＯｐｅｎ　Ｆｌｏｗプロトコルによって規定されるフォーマットで第１のスイッチに送信した後、第１のスイッチは、その送信元ＩＰアドレスが１０．１１．１００．１００であり、宛先ＩＰアドレスが１０．２２．２００．２００であり、送信元ポート番号が１２３４であり、宛先ポート番号が４３２１であり、プロトコル番号が６である攻撃データフローがないか第１のスイッチのフローテーブルを検索する。第１のスイッチが攻撃データフローを見つけた後、処理ポリシによれば、攻撃データフローの攻撃データパケットに対して実行されたアクションは具体的に、直ちにドロップする、である。すなわち、第１のスイッチは、記述情報「［１０．１１．１００．１００，１０．２２．２００．２００，６，１２３４，４３２１］」を有する攻撃データパケットに対して、直ちにドロップするというオペレーションを実行する。

【００８７】

第１のスイッチのフローテーブルに格納された各データフローは、ただ１つの記述情報と、各データフローのデータパケットに対して実行されるアクションとを有することに留意すべきである。データフローの全てデータパケットの伝送が完了した後、フローテーブルは、当該データフローの記録を削除する。従って、本発明のこの実施形態において提供される攻撃データパケット処理方法では、第１のスイッチは、ＳＤＮコントローラによって送信された記述情報及び処理ポリシに従って、当該記述情報を有する攻撃データフローがないかフローテーブルを検索し、攻撃データフローの攻撃データパケットに対して実行されるアクションを、処理ポリシによって示されるオペレーションに変更し、これにより、攻撃データフローの攻撃データパケットにおいて伝送されない攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行できる。更に、クラウドデータセンタの認識ノードが、攻撃データフローの攻撃データパケットによって連続的に攻撃されることを回避する。

【００８８】

本発明のこの実施形態は攻撃データパケット処理方法を提供する。当該方法は具体的に、管理ノードによって送信される、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する段階と、第１のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、記述情報及び処理ポリシを第１のスイッチに送信する段階とを備える。当該方法によれば、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送

信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタのクラウドサーバがセキュアな通信を実行できるようにする。

【００８９】

本発明の実施形態は、攻撃データパケット処理方法を提供する。図５に示されるように、当該方法は、以下の段階を備えてよい。

【００９０】

Ｓ３０１．認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別する。

【００９１】

認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別する方式は複数あり、攻撃データパケットを認識ノードによって識別するための方法は、以下の３つの例を使用することによって例示的に説明される。

【００９２】

例１：データパケットの受信後、認識ノードは、認識ノードによって受信されたデータパケットのパケットを識別し、データパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスが同一であると認識ノードが決定した場合、認識ノードは、データパケットのパケットは不正な形式のパケットであると決定し、データパケットは攻撃データパケットであると決定する。

【００９３】

例２：認識ノードがデータパケットを受信した後、認識ノードによって受信されたデータパケットのパケットトラフィック量が予め設定された閾値を超えていると、認識ノードが予め設定された時間内に決定した場合、認識ノードは、データパケットは攻撃データパケットであると決定する。

【００９４】

例３：データパケットの受信後、認識ノードは、データパケットのＳＩＰシグナリングを識別し、データパケットのＳＩＰセッションプロセスが、既知の規格のＳＩＰセッションプロセスと同一であるかどうかを判断する。データパケットのＳＩＰセッションプロセスが、既知の規格のＳＩＰセッションプロセスと異なると認識ノードが決定した場合、認識ノードは、データパケットは攻撃データパケットであると決定する。

【００９５】

更に、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別する他の方式は、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別する従来技術の方式と同一であり、本明細書においては１つ１つ列挙されない。

【００９６】

本発明のこの実施形態において、認識ノードは、クラウドデータセンタにあり、攻撃データパケットを識別できる任意のサービスノード、例えば、ＶＭ、ハイパーバイザ、ファイアウォール、負荷分散装置、又はゲートウェイであってよいことに留意すべきである。従って、攻撃データパケットが、ファイアウォールを使用することによって、ＩＰ層シグナリングを識別することによって識別される従来技術と比較して、本発明のこの実施形態は、認識ノードが、ＩＰ層シグナリングを識別することによって攻撃データパケットを識別する（例えば、不正な形式のパケットを識別することによって攻撃データパケットを識別する）のみならず、サービス層シグナリングを識別することによって攻撃データパケットを識別もできる（例えば、ＳＩＰシグナリングを識別することによってＳＩＰベースの攻撃のタイプの攻撃データパケットを識別する）攻撃データパケット処理方法を提供する

。このように、攻撃データパケットの識別精度が向上され、更に、認識ノードへの攻撃データパケットの攻撃がより包括的に阻止される。

【００９７】

Ｓ３０２．認識ノードが、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定する。

【００９８】

例示的に、認識ノードによって受信されたデータパケットのパケットが不正な形式のパケットであると認識ノードが識別した場合、不正な形式のパケットによる攻撃はＤＤｏＳ攻撃タイプに属するので、認識ノードは、攻撃データパケットの攻撃タイプはＤＤｏＳ攻撃であると決定してよい、又は、認識ノードによって受信されたデータパケットを攻撃データパケットであると、ＳＩＰ情報を識別することによって認識ノードが識別した場合、認識ノードは、データパケットの攻撃タイプはＳＩＰベースの攻撃であると決定してよい、又は、認識ノードによって受信されたデータパケットのパケットトラフィック量が予め設定された閾値を超えたと認識ノードが決定した場合、認識ノードは、データパケットを攻撃データパケットであると識別し、これにより、認識ノードは、データパケットの攻撃タイプは大量データ攻撃であると決定してよい。

【００９９】

更に、認識ノードによって受信されたデータパケットが攻撃データパケットであると認識ノードが決定した後、認識ノードは、攻撃データパケットから攻撃データパケットの記述情報を取得する。任意で、攻撃データパケットの記述情報は具体的に、攻撃データパケットの送信元ＩＰアドレス、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号であってよい。

【０１００】

Ｓ３０３．認識ノードが、記述情報及び攻撃タイプを管理ノードに送信する。ここで、攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される。

【０１０１】

管理ノードが当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定するプロセスについては、特に、図２に示される実施形態における関連する記載を参照してよく、スイッチが、処理ポリシに従って、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するプロセスについては、特に、図３に示される実施形態における関連する記載を参照してよく、詳細は、本明細書において更には説明されない。

【０１０２】

本発明のこの実施形態は、攻撃データパケット処理方法を提供する。当該方法は具体的に、認識ノードによって受信されたデータパケットを攻撃データパケットであると認識ノードによって識別する段階、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定する段階、及び、記述情報及び攻撃タイプを管理ノードに送信する段階であって、攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される、段階である。当該方法によれば、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットの攻撃タイプとを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信し、これにより、スイッチは、当

該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、攻撃データパケットが大量のネットワーク帯域幅を占有し、正常なデータパケットの伝送に影響を及ぼすという従来技術における問題が解決され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

［実施形態２］

【０１０３】

本発明の実施形態は、攻撃データパケット処理方法を提供する。図６に示されるように、当該方法は、以下の段階を備えてよい。

【０１０４】

Ｓ４０１．認識ノードが、データパケットを受信する。

【０１０５】

Ｓ４０２．認識ノードが、データパケットを攻撃データパケットであると識別する。

【０１０６】

Ｓ４０３．認識ノードが、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定する。

【０１０７】

Ｓ４０４．認識ノードが、記述情報及び攻撃タイプを管理ノードに送信する。

【０１０８】

具体的には、上述の段階Ｓ４０１からＳ４０４の具体的な実施方式について、図５に示される実施形態における関連する記載を参照してよく、詳細は本明細書において更には説明されない。

【０１０９】

Ｓ４０５．認識ノードによって送信された記述情報及び攻撃タイプの受信後、管理ノードが、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する。

【０１１０】

Ｓ４０６．管理ノードが、記述情報及び処理ポリシをＳＤＮコントローラに送信する。

【０１１１】

本発明のこの実施形態において、管理ノードにおいて通信インタフェースが予め設定され、当該通信インタフェースは、記述情報及び攻撃タイプをＳＤＮコントローラに送信すべく管理ノードによって使用されることに留意すべきである。加えて、ＳＤＮコントローラにおいて通信インタフェースが予め設定され、当該通信インタフェースは、管理ノードによって送信された記述情報及び攻撃タイプを受信すべくＳＤＮコントローラによって使用される。

【０１１２】

具体的には、管理ノード及びＳＤＮコントローラがＵＤＰプロトコルを使用することによって情報のやり取りを実行した場合、管理ノード及びＳＤＮコントローラに別々にある通信インタフェースは、ＵＤＰプロトコルに基づいて設定されてよい。記述情報及び攻撃タイプをＳＤＮコントローラに送信した場合、管理ノードは、ＳＤＮコントローラと通信リンクを確立する必要はなく、管理ノードにおいて予め設定された通信インタフェースのアドレスと、ＳＤＮコントローラにおいて予め設定された通信インタフェースのアドレスとを使用することによって、記述情報及び攻撃タイプをＳＤＮコントローラに直接送信してよい。

【０１１３】

管理ノード及びＳＤＮコントローラがＴＣＰプロトコルを使用することによって情報の

やり取りを実行した場合、管理ノード及びＳＤＮコントローラに別々にある通信インタフェースは、ＴＣＰプロトコルに基づいて設定されてよい。管理ノードが記述情報及び攻撃タイプをＳＤＮコントローラに送信した場合、２つの予め設定された通信インタフェースの間で通信リンクを確立すべく、管理ノードとＳＤＮコントローラとの間にＴＣＰ接続が確立される必要があり、管理ノードは、当該通信リンクを使用することによって記述情報及び攻撃タイプをＳＤＮコントローラに送信する。

【０１１４】

Ｓ４０７．ＳＤＮコントローラが、記述情報及び処理ポリシを第１のスイッチに送信する。

【０１１５】

Ｓ４０８．第１のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。

【０１１６】

具体的には、上述の段階Ｓ４０７からＳ４０８の具体的な実施方式について、図３に示される実施形態における関連する記載を参照してよく、詳細は本明細書において更には説明されない。

【０１１７】

任意で、上述の段階Ｓ４０５において、管理ノードが、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び複数の攻撃データパケットの攻撃タイプを受信した場合、図６を参照して、図７に示されるように、上述の段階Ｓ４０５は具体的に、以下の段階を備えてよい。

【０１１８】

Ｓ４０５ａ．管理ノードが、複数の攻撃データパケットの攻撃タイプに応じて、少なくとも２つの同じ攻撃タイプを決定する。

【０１１９】

Ｓ４０５ｂ．管理ノードが、少なくとも２つの攻撃タイプのうちの１つに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する。

【０１２０】

具体的に、管理ノードが、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び複数の攻撃データパケットの攻撃タイプを受信した場合、管理ノードは、少なくとも２つの同じ攻撃タイプが複数の攻撃データパケットの攻撃タイプの中に存在するかどうかを、複数の攻撃データパケットの攻撃タイプに応じて判断する。管理ノードが、少なくとも２つの同じ攻撃タイプが複数の攻撃データパケットの攻撃タイプの中に存在すると決定した場合、管理ノードは、少なくとも２つの攻撃タイプのうちの１つに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する。すなわち、少なくとも２つの攻撃タイプは同一なので、管理ノードは、少なくとも２つの攻撃タイプのいずれか１つに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定する。

【０１２１】

更に、管理ノードは、少なくとも２つの攻撃データパケットの各攻撃データパケットの記述情報と共に処理ポリシをＳＤＮコントローラに送信する、すなわち、同一の攻撃タイプの少なくとも２つの攻撃データパケットの各攻撃データパケットの記述情報に対応する処理ポリシが、当該処理ポリシである。

【０１２２】

更に、上述の段階Ｓ４０６の後、図６を参照して、図８Ａ及び図８Ｂに示されるように、当該方法は、更に以下の段階を含む。

【０１２３】

Ｓ４０９．ＳＤＮコントローラが、記述情報及び処理ポリシを、ＳＤＮコントローラに接続されたマスタＳＤＮコントローラに送信する。

【０１２４】

Ｓ４１０．マスタＳＤＮコントローラが、記述情報及び処理ポリシを第２のスイッチに送信する。

【０１２５】

Ｓ４１１．第２のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。

【０１２６】

上述の段階Ｓ４０７及びＳ４０９の順序は、本発明のこの実施形態において限定されないことに留意すべきである。

【０１２７】

具体的には、データセンタの内部ネットワーク及び外部ネットワークが共に、ＳＤＮ技術に基づいているネットワークアーキテクチャを使用した場合、データセンタ内のＳＤＮコントローラが、管理ノードによって送信された記述情報及び処理ポリシを受信した後、ＳＤＮコントローラは、記述情報及び処理ポリシをマスタＳＤＮコントローラに直接転送する。マスタＳＤＮコントローラは、データセンタ外にあり、ＳＤＮコントローラに接続されているＳＤＮコントローラである、すなわち、マスタＳＤＮコントローラは、バックボーンネットワーク内にあり、データセンタに接続されているＳＤＮコントローラである。マスタＳＤＮコントローラは、記述情報及び処理ポリシを、Ｏｐｅｎ　Ｆｌｏｗプロトコルによって規定されるフォーマットで第２のスイッチに送信する。第２のスイッチは、マスタＳＤＮコントローラによって制御されるスイッチクラスタの任意のスイッチである。記述情報及び処理ポリシの受信後、第２のスイッチは、当該記述情報を有するデータパケットに対して、処理ポリシによって示されるオペレーションを実行し、これにより、攻撃データパケットが伝送された場合の、攻撃データパケットが占有するネットワーク帯域幅がネットワーク全体において制限され、正常なデータパケットの伝送が確保される。

【０１２８】

第２のスイッチが、処理ポリシによって示されるオペレーションを攻撃データパケットに対して実行する具体的なプロセスについては、第１のスイッチが、処理ポリシによって示されるオペレーションを攻撃データパケットに対して実行する図３に示される実施形態における具体的なプロセスを参照してよく、詳細は、本明細書において更には説明されない。

【０１２９】

更に、以下では２つの可能な適用シナリオを挙げて、本発明のこの実施形態において提供される攻撃データパケット処理方法を例示的に説明する。図９は、本発明の実施形態に係る通信システムのブロック図を示す。認識ノードが具体的に、クラウドデータセンタにおけるゲストオペレーティングシステム層のＶＭ、例えば、仮想スイッチ（ｖＳｗｉｔｃｈ）のＶＭである場合、認識ノードは、ＶＭスイッチ２のＶＭ２であってよく、管理ノードが具体的に、クラウドデータセンタにおけるＶＭマネージャである場合、ＶＭ２はデータパケットのＩＰ層シグナリングを識別できるので、ＶＭ２が（不正な形式のパケットによる攻撃などの）ＩＰ層のＤＤｏＳ攻撃タイプの攻撃データパケットを受信した場合、ＶＭ２は、当該攻撃データパケットを識別できる。従って、図９に示される通信システム内のＶＭ２、ＶＭマネージャ、ＳＤＮコントローラ、及びスイッチは、図６又は図７に示された上述の方法を実行することによって、攻撃データパケットを処理できる。

【０１３０】

図１０は、本発明の実施形態に係る別の通信システムのブロック図を示す。認識ノードが具体的に、ハイパーバイザ、例えば、クラウドデータセンタのハイパーバイザ２であり、管理ノードが具体的に、クラウドデータセンタのＰＣＲＦである場合、ハイパーバイザ２は、データパケットのサービス層シグナリングを識別することによって攻撃データパケットを識別できる、例えば、ＳＩＰシグナリングを識別することによってＳＩＰベースの攻撃のタイプの攻撃データパケットを識別できるので、ハイパーバイザ２がＳＩＰベースの攻撃のタイプの攻撃データパケットを受信した場合、ハイパーバイザ２は、攻撃データパケットを識別できる。従って、ハイパーバイザ２、ＰＣＲＦ、ＳＤＮコントローラ、及

びスイッチは、図６又は図７に示される上述の方法を実行することによって、攻撃データパケットを処理できる。

【０１３１】

本発明のこの実施形態は、攻撃データパケット処理方法を提供する。当該方法は具体的に、認識ノードによって受信されたデータパケットを攻撃データパケットであると認識ノードによって識別する段階と、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定する段階と、記述情報及び攻撃タイプを管理ノードに送信する段階と、当該攻撃タイプの攻撃データパケットに対する処理ポリシを攻撃タイプに応じて管理ノードによって決定する段階と、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行するように、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信する段階であって、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階とを備える。当該方法によれば、攻撃データパケットがネットワークにおいて伝送された場合の、攻撃データパケットが占有するネットワーク帯域幅が制限され得、正常なデータパケットの伝送が確保され、攻撃データパケットが大量のネットワーク帯域幅を占有し、正常なデータパケットの伝送に影響を及ぼすという従来技術における問題が解決され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタのクラウドサーバがセキュアな通信を実行できるようにする。

［実施形態３］

【０１３２】

図１１に示されるように、本発明のこの実施形態は、管理ノードを提供する。当該管理ノードは、

認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを受信するよう構成される受信ユニット１０と、

受信ユニット１０によって受信された攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定するよう構成される決定ユニット１１であって、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、決定ユニット１１と、

当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行するように、受信ユニット１０によって受信された記述情報と、決定ユニット１１によって決定された処理ポリシとを、ソフトウェアデファインドネットワーキングＳＤＮコントローラを使用することによってスイッチに送信するよう構成される送信ユニット１２とを備えてよい。

【０１３３】

任意で、決定ユニット１１は具体的に、受信ユニット１０によって受信された攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する予め設定された処理ポリシを取得するよう構成されている。

【０１３４】

任意で、決定ユニット１１は具体的に、受信ユニット１０によって受信された攻撃タイプと予め設定されたアルゴリズムとに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを生成するよう構成されている。

【０１３５】

任意で、決定ユニット１１によって決定された処理ポリシによって示されるオペレーションは、当該記述情報を有する攻撃データパケットに対する処理アクション、又は、当該記述情報を有する攻撃データパケットに対する処理アクション及び処理アクションを実行する時間を含む。

【０１３６】

任意で、決定ユニット１１は具体的に、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを受信ユニット１０が受信した場合、複数の攻撃データパケットの攻撃タイプに応じて少なくとも２つの同じ攻撃タイプを決定し、少なくとも２つの攻撃タイプのうちの１つに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定するよう構成されている。

【０１３７】

任意で、送信ユニット１２は具体的に、ＳＤＮコントローラが、記述情報及び処理ポリシをスイッチに転送するように、受信ユニット１０によって受信された記述情報と決定ユニット１１によって決定された処理ポリシとを予め設定された通信インタフェースを使用することによってＳＤＮコントローラに送信するよう構成されている。

【０１３８】

任意で、受信ユニット１０によって受信された記述情報は、攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号を含む。

【０１３９】

本発明のこの実施形態において提供される管理ノードは、クラウドデータセンタの任意のサービス管理ノード又はポリシ管理ノード、例えば、ＶＭマネージャ、ＶＩＭ、ＰＣＲＦ、又は同様のものであってよいことに留意すべきである。

【０１４０】

本発明のこの実施形態は、管理ノードを提供する。当該管理ノードは、認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを受信でき、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって、記述情報及び処理ポリシをスイッチに送信でき、これにより、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行する。ここで、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される。従って、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、本発明のこの実施形態において提供される管理ノードは、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信でき、これにより、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

【０１４１】

図１２に示されるように、本発明のこの実施形態はＳＤＮコントローラを提供する。当該ＳＤＮコントローラは、

管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとを受信するよう構成される受信ユニット２０と、

当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを第１のスイッチが実行するように、受信ユニット２０によって受信された当該記述情報及び処理ポリシを第１のスイッチに送信するよう構成される送信ユニット２１とを備えてよい。

【０１４２】
任意で、受信ユニット２０は具体的に、管理ノードによって送信された記述情報及び処理ポリシを、予め設定された通信インタフェースを使用することによって受信するよう構成されている。
【０１４３】
任意で、送信ユニット２１は更に、マスタＳＤＮコントローラが、当該記述情報及び処理ポリシを第２のスイッチに転送し、第２のスイッチが、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するように、受信ユニット２０によって受信された記述情報及び処理ポリシをマスタＳＤＮコントローラに送信するよう構成されている。
【０１４４】
本発明のこの実施形態はＳＤＮコントローラを提供する。当該ＳＤＮコントローラは、管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとを受信し、当該記述情報及び処理ポリシを第１のスイッチに送信でき、これにより、第１のスイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、本発明のこの実施形態において提供されるＳＤＮコントローラを使用することによって、記述情報及び処理ポリシをスイッチに送信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。
【０１４５】
図１３に示されるように、本発明のこの実施形態は認識ノードを提供する。当該認識ノードは、
認識ノードによって受信されたデータパケットを攻撃データパケットであると識別するよう構成される識別ユニット３０と、
識別ユニット３０によって識別された攻撃データパケットの記述情報と攻撃データパケットの攻撃タイプとを決定するよう構成される決定ユニット３１と、
決定ユニット３１によって決定された記述情報及び攻撃タイプを管理ノードに送信するよう構成される送信ユニット３２とを備えてよい。ここで、攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される。
【０１４６】
任意で、決定ユニット３１によって決定された記述情報は、攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号を含む。
【０１４７】
本発明のこの実施形態において提供される認識ノードは、クラウドデータセンタにあり、攻撃データパケットを識別できる任意のクラウドサーバ、例えば、様々なサービスの処理ＶＭ、ハイパーバイザ、ファイアウォール、負荷分散装置、又はゲートウェイであって

よいことに留意すべきである。

【０１４８】

本発明のこの実施形態は、認識ノードを提供する。当該認識ノードは、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定し、当該記述情報及び攻撃タイプを管理ノードに送信できる。ここで、攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される。従って、本発明のこの実施形態において提供される認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットの攻撃タイプとを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

［実施形態４］

【０１４９】

図１４に示されるように、本発明のこの実施形態は管理ノードを提供する。当該管理ノードは、プロセッサ４０、通信インタフェース４１、メモリ４２、及びシステムバス４３を備えてよい。プロセッサ４０、通信インタフェース４１、及びメモリ４２は接続されており、システムバス４３を使用することによって相互通信を完了する。

【０１５０】

プロセッサ４０は、本発明のこの実施形態を実施するよう構成される中央処理装置（ＣＰＵ）、又は特定用途向け集積回路（ＡＳＩＣ）、又は１又は複数の集積回路であってよい。

【０１５１】

通信インタフェース４１は、別のデバイスと情報をやり取りする、例えば、認識ノードと情報をやり取りする、又は、ＳＤＮコントローラと情報をやり取りするよう構成されている。

【０１５２】

メモリ４２は、揮発性メモリ、例えばランダムアクセスメモリ（ＲＡＭ）を含んでよい、又は、メモリ４２は、不揮発性メモリ、例えば、リードオンリメモリ（ＲＯＭ）、フラッシュメモリ、ハードディスクドライブ（ＨＤＤ）、又はソリッドステートドライブ（ＳＳＤ）を含んでよい、又は、メモリ４２は、上述のタイプのメモリの組み合わせを含んでよい。

【０１５３】

管理ノードが動作した場合、プロセッサ４０、通信インタフェース４１、及びメモリ４２は、図２、又は図６から図８Ａ及び図８Ｂのいずれか１つにおいて説明された方法手順を実行してよく、それは具体的に以下を含む。

【０１５４】

プロセッサ４０は、通信インタフェース４１を使用することによって、認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを受信し、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示さ

れるオペレーションをスイッチが実行するように、ＳＤＮコントローラを使用することによって当該記述情報及び処理ポリシをスイッチに送信するよう構成されている。ここで、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される。メモリ４２は、ソフトウェアプログラムを実行し、記述情報のコード、攻撃タイプのコード、及び処理ポリシのコードを呼び出すことによってプロセッサ４０が上述のプロセスを完了するように、記述情報のコードと、攻撃タイプのコードと、処理ポリシのコードと、上述のプロセスを完了するようプロセッサ４０を制御するソフトウェアプログラムとを格納するよう構成されている。

【０１５５】

任意で、プロセッサ４０は具体的に、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する予め設定された処理ポリシを取得するよう構成されている。

【０１５６】

任意で、プロセッサ４０は具体的に、攻撃タイプ及び予め設定されたアルゴリズムに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを生成するよう構成されている。

【０１５７】

任意で、プロセッサ４０によって決定された処理ポリシによって示されるオペレーションは、

当該記述情報を有する攻撃データパケットに対する処理アクション、又は、当該記述情報を有する攻撃データパケットに対する処理アクション及び処理アクションを実行する時間を含む。

【０１５８】

任意で、プロセッサ４０は具体的に、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び複数の攻撃データパケットの攻撃タイプを通信インタフェース４１が受信した場合、複数の攻撃データパケットの攻撃タイプに応じて少なくとも２つの同じ攻撃タイプを決定し、少なくとも２つの攻撃タイプのうちの１つに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定するよう構成されている。

【０１５９】

任意で、プロセッサ４０は具体的に、ＳＤＮコントローラが記述情報及び処理ポリシをスイッチに転送するように、予め設定された通信インタフェースを使用することによって記述情報及び処理ポリシをＳＤＮコントローラに送信するよう構成されている。

【０１６０】

任意で、通信インタフェース４１を使用することによって、プロセッサ４０によって受信された記述情報は、攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号を含む。

【０１６１】

本発明のこの実施形態は、管理ノードを提供する。当該管理ノードは、認識ノードによって送信された、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを受信でき、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって、記述情報及び処理ポリシをスイッチに送信でき、これにより、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行する。ここで、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される。従って、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、本発明のこの実施形態において提供される管理ノードは、攻撃タイプに応じて、当該

攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信でき、これにより、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションをスイッチが実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

【０１６２】

図１５に示されるように、本発明のこの実施形態はＳＤＮコントローラを提供する。当該ＳＤＮコントローラは、プロセッサ５０、通信インタフェース５１、メモリ５２、及びシステムバス５３を備えてよい。プロセッサ５０、通信インタフェース５１、及びメモリ５２は接続されており、システムバス５３を使用することによって相互通信を完了する。

【０１６３】

プロセッサ５０は、本発明のこの実施形態を実施するよう構成されるＣＰＵ、又はＡＳＩＣ、又は１又は複数の集積回路であってよい。

【０１６４】

通信インタフェース５１は、別のデバイスと情報をやり取りする、例えば、管理ノードと情報をやり取りする、又は、スイッチと情報をやり取りするよう構成されている。

【０１６５】

メモリ５２は、揮発性メモリ、例えばＲＡＭを含んでよい、又は、メモリ５２は、不揮発性メモリ、例えば、ＲＯＭ、フラッシュメモリ、ＨＤＤ、又はＳＳＤを含んでよい、又は、メモリ５２は、上述のタイプのメモリの組み合わせを含んでよい。

【０１６６】

ＳＤＮコントローラが動作した場合、プロセッサ５０、通信インタフェース５１、及びメモリ５２は、図３、又は図６から図８Ａ及び図８Ｂのいずれか１つにおいて説明された方法手順を実行してよく、それは具体的に以下を含む。

【０１６７】

プロセッサ５０は、通信インタフェース５１を使用することによって、管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとを受信し、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを第１のスイッチが実行するように、当該記述情報及び処理ポリシを第１のスイッチに送信するよう構成されている。メモリ５２は、ソフトウェアプログラムを実行し、記述情報のコード及び処理ポリシのコードを呼び出すことによって、プロセッサ５０が上述のプロセスを完了するように、記述情報のコードと、処理ポリシのコードと、上述のプロセスを完了するようプロセッサ５０を制御するソフトウェアプログラムとを格納するよう構成されている。

【０１６８】

任意で、プロセッサ５０は具体的に、管理ノードによって送信された記述情報及び処理ポリシを、予め設定された通信インタフェースを使用することによって受信するよう構成されている。

【０１６９】

任意で、プロセッサ５０は更に、マスタＳＤＮコントローラが、当該記述情報及び処理ポリシを第２のスイッチに転送し、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを第２のスイッチが実行するように、通信インタフェース５１を使用することによって当該記述情報及び処理ポリシをマスタＳＤＮコントローラに送信するよう構成されている。

【０１７０】

本発明のこの実施形態はＳＤＮコントローラを提供する。当該ＳＤＮコントローラは、

管理ノードによって送信された、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットに対する処理ポリシとを受信し、当該記述情報及び処理ポリシを第１のスイッチに送信でき、これにより、第１のスイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、本発明のこの実施形態において提供されるＳＤＮコントローラを使用することによって、記述情報及び処理ポリシをスイッチに送信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

【０１７１】

図１６に示されるように、本発明のこの実施形態は認識ノードを提供する。当該認識ノードは、プロセッサ６０、通信インタフェース６１、メモリ６２、及びシステムバス６３を備えてよい。プロセッサ６０、通信インタフェース６１、及びメモリ６２は接続されており、システムバス６３を使用することによって相互通信を完了する。

【０１７２】

プロセッサ６０は、本発明のこの実施形態を実施するよう構成されるＣＰＵ、又はＡＳＩＣ、又は１又は複数の集積回路であってよい。

【０１７３】

通信インタフェース６１は、別のデバイスと情報をやり取りする、例えば、別の認識ノードと情報をやり取りする、又は、管理ノードと情報をやり取りするよう構成されている。

【０１７４】

メモリ６２は、揮発性メモリ、例えばＲＡＭを含んでよい、又は、メモリ６２は、不揮発性メモリ、例えば、ＲＯＭ、フラッシュメモリ、ＨＤＤ、又はＳＳＤを含んでよい、又は、メモリ６２は、上述のタイプのメモリの組み合わせを含んでよい。

【０１７５】

認識ノードが動作する場合、プロセッサ６０、通信インタフェース６１、及びメモリ６２は、図５から図８Ａ及び図８Ｂのいずれか１つにおいて説明された方法手順を実行してよく、それは具体的に以下を含む。

【０１７６】

プロセッサ６０は、通信インタフェース６１によって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定し、当該記述情報及び攻撃タイプを管理ノードに送信するよう構成されている。ここで、攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される。メモリ６２は、ソフトウェアプログラムを実行し、攻撃データパケットのコード、記述情報、及び攻撃タイプを呼び出すことによってプロセッサ６０が上述のプロセスを完了するように、攻撃データパケットのコードと、記述情報と、攻撃タイプと、上述のプロセスを完了するようプロセッサ６０を制御するソフトウェアプログラムとを格納するよう構成されている。

【０１７７】

任意で、プロセッサ６０によって決定された記述情報は、攻撃データパケットの送信元

インターネットプロトコルＩＰアドレス、攻撃データパケットの送信元ポート番号、攻撃データパケットの宛先ＩＰアドレス、攻撃データパケットの宛先ポート番号、及び攻撃データパケットのプロトコル番号を含む。

【０１７８】

本発明のこの実施形態は、認識ノードを提供する。当該認識ノードは、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定し、当該記述情報及び攻撃タイプを管理ノードに送信できる。ここで、攻撃タイプは、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定すべく管理ノードによって使用され、処理ポリシは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される。従って、本発明のこの実施形態において提供される認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報と当該記述情報を有する攻撃データパケットの攻撃タイプとを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって記述情報及び処理ポリシをスイッチに送信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

［実施形態５］

【０１７９】

図１７に示されるように、本発明のこの実施形態は通信システムを提供する。当該通信システムは、図１１に示される管理ノード、図１２に示されるＳＤＮコントローラ、図１３に示される認識ノード、及びスイッチを備えてよい、又は、本発明のこの実施形態において提供される通信システムはまた、図１４に示される管理ノード、図１５に示されるＳＤＮコントローラ、図１６に示される認識ノード、及びスイッチを備えてよい。スイッチは、ＳＤＮ技術に基づくネットワークアーキテクチャにあり、ＳＤＮコントローラによって制御されるスイッチである。

【０１８０】

本発明のこの実施形態において提供される通信システムでは、認識ノードは、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを決定し、当該記述情報及び攻撃タイプを管理ノードに送信できる。記述情報及び攻撃タイプの受信後、管理ノードは、攻撃タイプに応じて、当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、当該記述情報及び処理ポリシをＳＤＮコントローラに送信できる。管理ノードによって送信された処理ポリシ及び記述情報の受信後、ＳＤＮコントローラは、当該記述情報及び処理ポリシをスイッチに送信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。

【０１８１】

任意で、図１８に示されるように、本発明のこの実施形態において提供される通信システムは更に、マスタＳＤＮコントローラと、マスタＳＤＮコントローラによって制御されるスイッチとを備えてよい。マスタＳＤＮコントローラは、データセンタ外にあり、ＳＤＮコントローラに接続されているＳＤＮコントローラである。

【０１８２】

本発明のこの実施形態において提供される通信システムでは、管理ノードによって送信された記述情報及び処理ポリシをＳＤＮコントローラが受信した後、ＳＤＮコントローラ

は、当該記述情報及び処理ポリシをマスタＳＤＮコントローラに転送し、マスタＳＤＮコントローラは、当該記述情報及び処理ポリシを、マスタＳＤＮコントローラによって制御されたスイッチに送信し、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。

【０１８３】

本発明のこの実施形態において提供される通信システムによれば、認識ノードが、認識ノードによって受信されたデータパケットを攻撃データパケットであると識別し、攻撃データパケットの記述情報及び攻撃データパケットの攻撃タイプを管理ノードに送信した後、管理ノードは、攻撃タイプに応じて当該攻撃タイプの攻撃データパケットに対する処理ポリシを決定し、ＳＤＮコントローラを使用することによって当該記述情報及び処理ポリシをスイッチに送信でき、これにより、スイッチは、当該記述情報を有する攻撃データパケットに対して、処理ポリシによって示されるオペレーションを実行する。従って、当該記述情報を有する攻撃データパケットがネットワークにおいて伝送された場合の、当該記述情報を有する攻撃データパケットが占有するネットワーク帯域幅が制限され、正常なデータパケットの伝送が確保され、更に、クラウドデータセンタの認識ノードが、当該記述情報を有する攻撃データパケットによって連続的に攻撃されることを回避し、これにより、確実にクラウドデータセンタの認識ノードがセキュアな通信を実行できるようにする。

【０１８４】

説明を簡便かつ簡単にする目的で、上述の機能モジュールの分割が、説明の一例であると見なされることを当業者は明確に理解するであろう。実際の適用では、上述の機能は、種々の機能モジュールに割り当てられ、要件に応じて実装され得る、すなわち、装置の内部構造が、種々の機能モジュールに分割されて、上述の機能の全部又は一部を実装する。上記のシステム、装置、及びユニットの具体的な動作プロセスについては、上述の方法の実施形態の対応するプロセスを参照してよく、詳細は本明細書において再びは説明されない。

【０１８５】

本願において提供されるいくつかの実施形態では、開示されたシステム、装置、及び方法は他の方式で実装されてよいことが理解されるべきである。例えば、説明された装置の実施形態は例示のものに過ぎない。例えば、モジュール又はユニットの分割は、論理的機能の分割に過ぎず、実際の実装においては他の分割であってよい。例えば、複数のユニット又はコンポーネントが組み合わせられてよい、又は、別のシステムに統合されてよい、又は、一部の特徴が無視されてよい、又は実行されなくてよい。加えて、表示又は論じられた相互連結、又は直接的な連結若しくは通信接続は、いくつかのインタフェースを使用することによって実装されてよい。装置間又はユニット間の間接的な連結又は通信接続は、電子的、機械的、又は他の形態で実装されてよい。

【０１８６】

別個の部分として説明されたユニットは、物理的に別個であってもなくてもよい。また、ユニットとして表示された部分は、物理的ユニットであってもなくてもよい、一か所に配置されてよい、又は、複数のネットワークユニット上に分散されてよい。実施形態の解決手段の目的を実現するよう、実際の必要性に応じてそれらのユニットの一部又は全部が選択されてよい。

【０１８７】

加えて、本発明の実施形態の機能ユニットが１つの処理ユニットに統合されてよい、又は、それらのユニットの各々が、物理的に単独で存在してよい、又は、２つ以上のユニットが１つのユニットに統合されてよい。統合されたユニットは、ハードウェアの形態で実装されてよい、又は、ソフトウェア機能ユニットの形態で実装されてよい。

【０１８８】

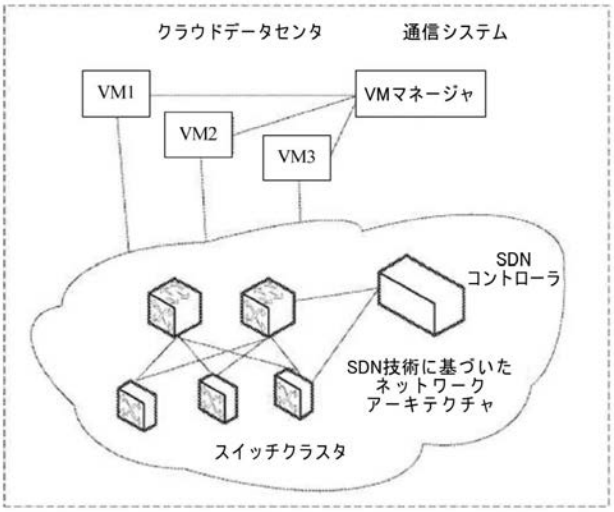
統合されたユニットがソフトウェア機能ユニットの形態で実装され、独立した製品として販売又は使用された場合、統合されたユニットは、コンピュータ可読記憶媒体に格納されてよい。そのような理解に基づいて、本発明の技術的解決手段は基本的に、又は従来技

術に寄与する部分は、又は技術的解決手段の全部又は一部は、ソフトウェア製品の形態で実装されてよい。コンピュータソフトウェア製品が記憶媒体に格納され、本発明の実施形態で説明された方法の段階の全部又は一部を実行するよう、（パーソナルコンピュータ、サーバ、若しくはネットワークデバイスであってよい）コンピュータデバイス又はプロセッサに命令するためのいくつかの命令を含む。上記記憶媒体は、プログラムコードを格納できる、ＵＳＢフラッシュドライブ、リムーバブルハードディスク、リードオンリメモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、磁気ディスク、又は光ディスクなどの任意の媒体を含む。

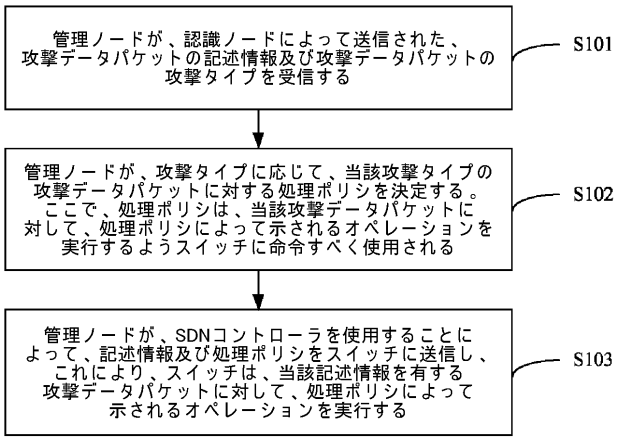
【０１８９】

上記の説明は、本発明の特定の実施方式に過ぎず、本発明の保護範囲を限定するよう意図されてはいない。本発明において開示された技術的範囲内で当業者が容易に考え出した変更又は置き換えはいずれも、本発明の保護範囲に含まれるものとする。従って、本発明の保護範囲は、特許請求の範囲の保護範囲に従うものとする。

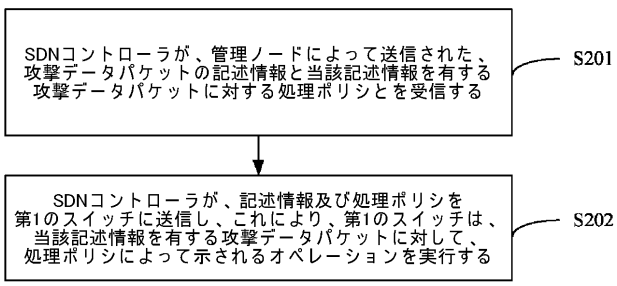
【図１】



【図２】

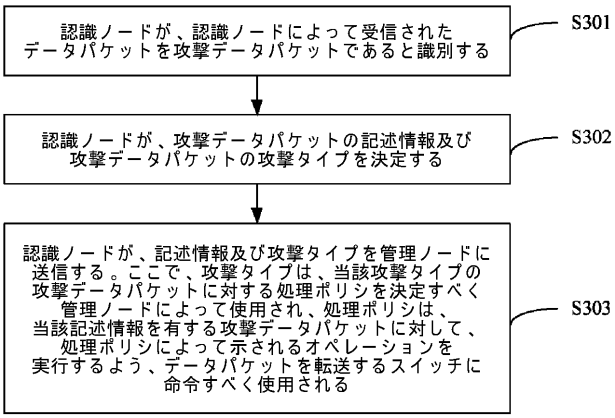


【図３】

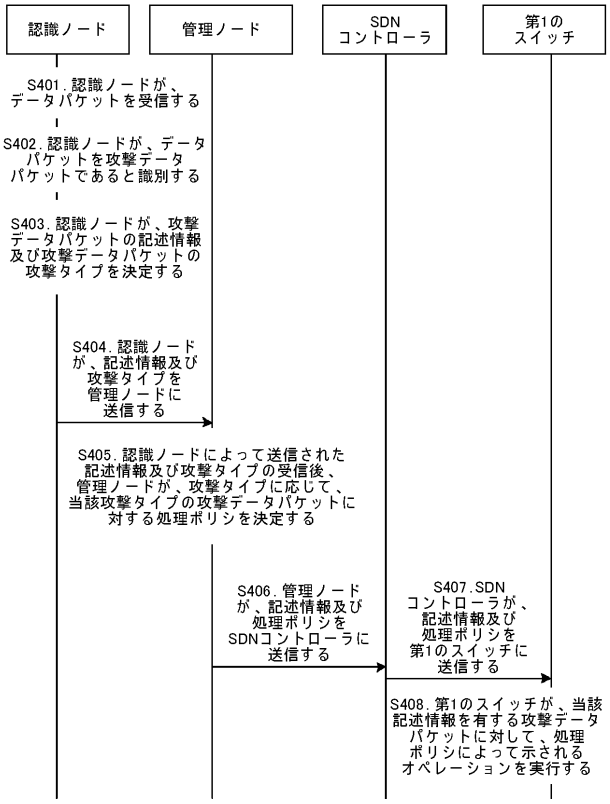


【図４】

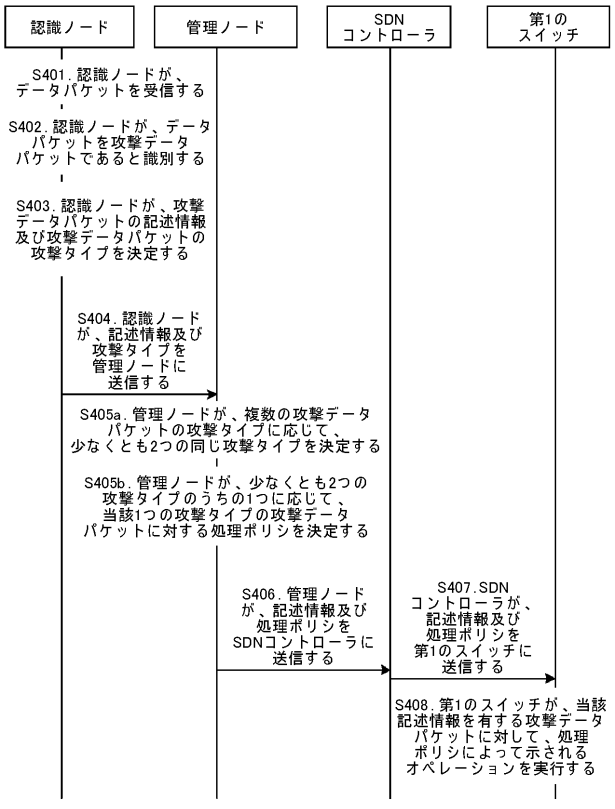
【図５】



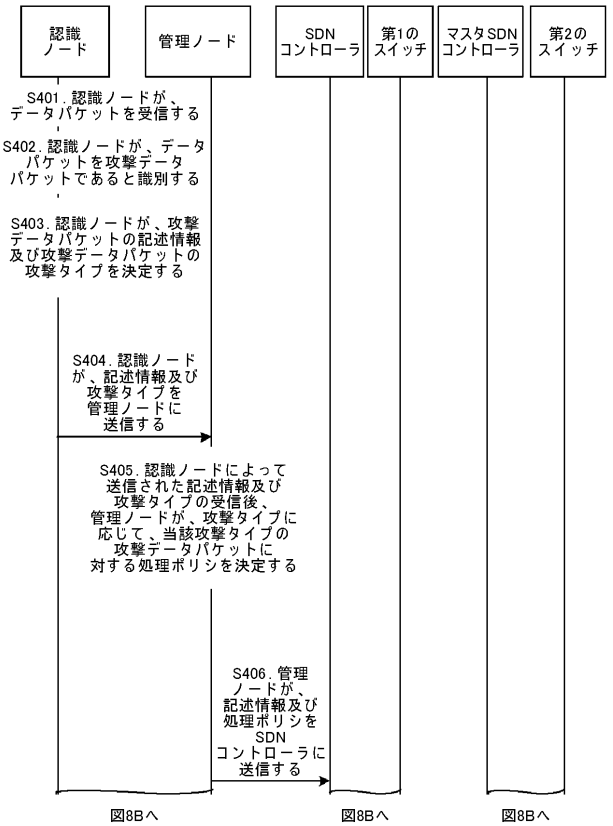
【図６】



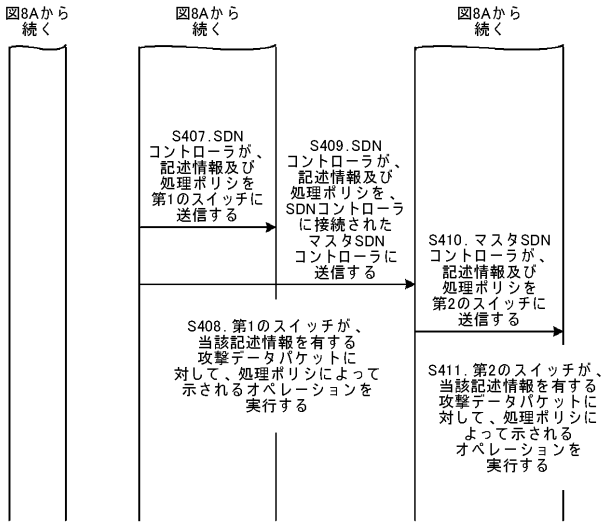
【図７】



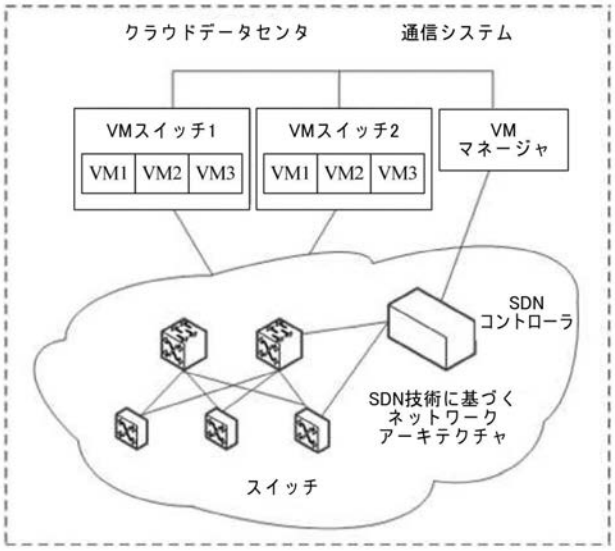
【図８Ａ】



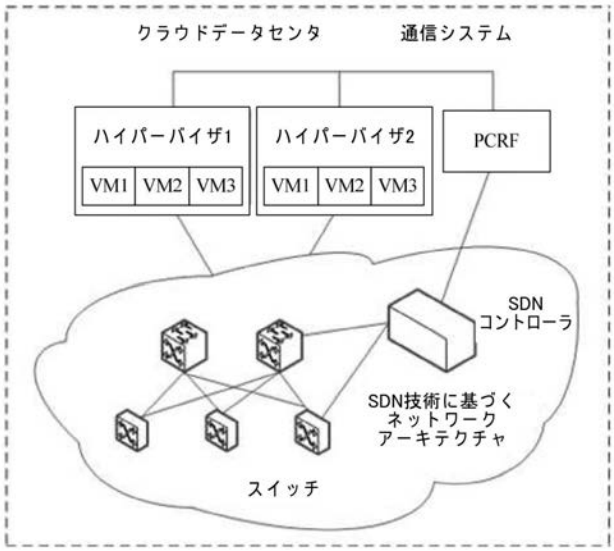
【図８Ｂ】



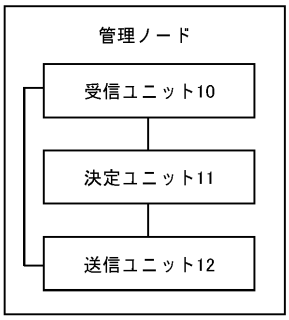
【図９】



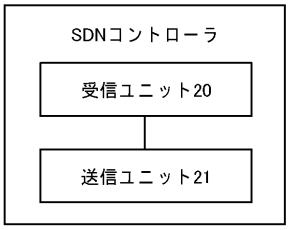
【図１０】



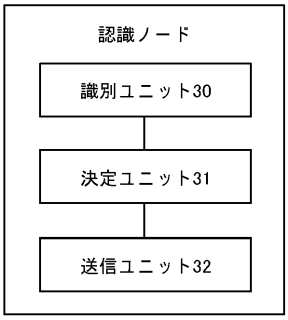
【図１１】



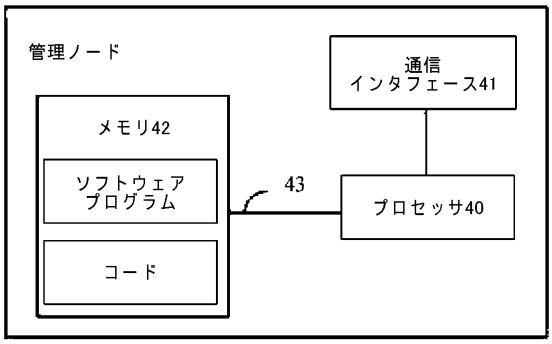
【図１２】



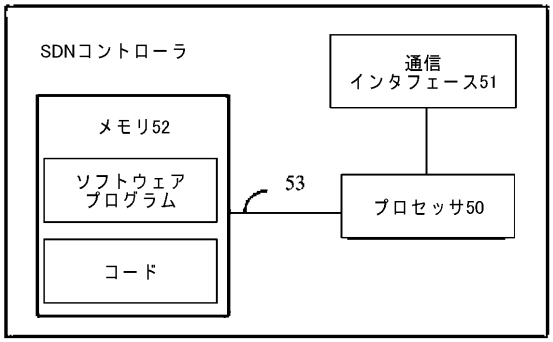
【図１３】



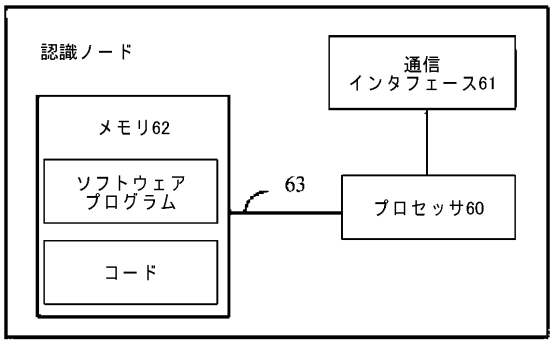
【図１４】



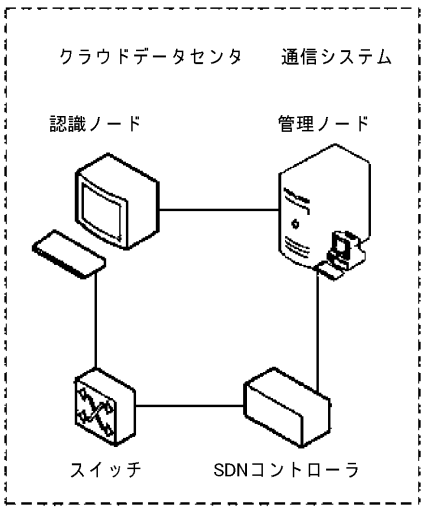
【図１５】



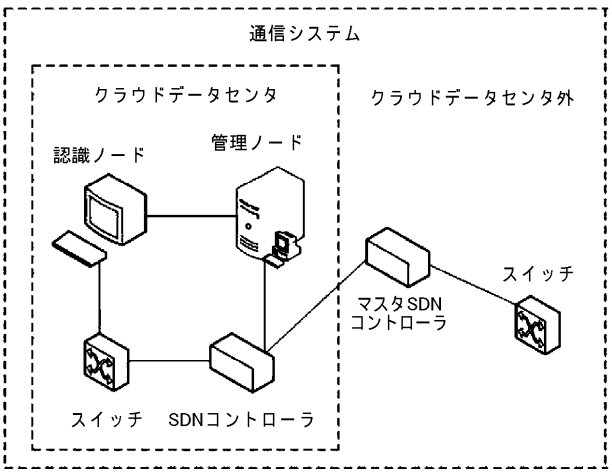
【図１６】



【図１７】



【図１８】



【手続補正書】
【提出日】平成29年7月14日(2017.7.14)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
攻撃データパケット処理方法であって、
認識ノードによって送信された、攻撃データパケットの記述情報及び前記攻撃データパケットの攻撃タイプを管理ノードによって受信する段階と、
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する段階であって、前記処理ポリシは、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階と、
前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示される前記オペレーションを前記スイッチが実行するように、ソフトウェアデファインドネットワーキング（ＳＤＮ）コントローラを使用することによって前記記述情報及び前記処理ポリシを前記管理ノードによって前記スイッチに送信する段階とを備える方法。
【請求項２】
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する前記段階は、
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する予め設定された処理ポリシを前記管理ノードによって取得する段階を含む、請求項１に記載の方法。
【請求項３】
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する前記段階は、
前記攻撃タイプ及び予め設定されたアルゴリズムに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって生成する段階を含む、請求項１又は２に記載の方法。
【請求項４】
前記処理ポリシによって示される前記オペレーションは、
前記記述情報を有する前記攻撃データパケットに対する処理アクション、又は、前記記述情報を有する前記攻撃データパケットに対する処理アクション及び前記処理アクションを実行する時間を含む、
請求項１から３のいずれか一項に記載の方法。
【請求項５】
複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び前記複数の攻撃データパケットの攻撃タイプを前記管理ノードが受信した場合、
前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する前記段階は、
少なくとも２つの同じ攻撃タイプを前記複数の攻撃データパケットの前記攻撃タイプに応じて前記管理ノードによって決定する段階と、
前記少なくとも２つの攻撃タイプのうちの１つに応じて、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを前記管理ノードによって決定する段階とを含む、請求項１から４のいずれか一項に記載の方法。
【請求項６】
ＳＤＮコントローラを使用することによって前記記述情報及び前記処理ポリシを前記管理ノードによって前記スイッチに送信する前記段階は、

前記ＳＤＮコントローラが、前記記述情報及び前記処理ポリシを前記スイッチに転送するように、予め設定された通信インタフェースを使用することによって前記記述情報及び前記処理ポリシを前記管理ノードによって前記ＳＤＮコントローラに送信する段階を含む、請求項１から５のいずれか一項に記載の方法。

【請求項７】

攻撃データパケット処理方法であって、

管理ノードによって送信された、攻撃データパケットの記述情報と前記記述情報を有する前記攻撃データパケットに対する処理ポリシとをソフトウェアデファインドネットワーキング（ＳＤＮ）コントローラによって受信する段階と、

第１のスイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するように、前記記述情報及び前記処理ポリシを前記ＳＤＮコントローラによって前記第１のスイッチに送信する段階とを備える方法。

【請求項８】

管理ノードによって送信された、攻撃データパケットの記述情報と前記記述情報を有する前記攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する前記段階は、

前記管理ノードによって送信された前記記述情報及び前記処理ポリシを予め設定された通信インタフェースを使用することによって前記ＳＤＮコントローラによって受信する段階を含む、請求項７に記載の方法。

【請求項９】

認識ノードによって送信された、攻撃データパケットの記述情報及び前記攻撃データパケットの攻撃タイプを受信する受信ユニットと、

前記受信ユニットによって受信された前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを決定する決定ユニットであって、前記処理ポリシは、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、決定ユニットと、

前記スイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示される前記オペレーションを実行するように、前記受信ユニットによって受信された前記記述情報と、前記決定ユニットによって決定された前記処理ポリシとを、ソフトウェアデファインドネットワーキング（ＳＤＮ）コントローラを使用することによって前記スイッチに送信する送信ユニットと、

を備える管理ノード。

【請求項１０】

前記決定ユニットは具体的に、前記受信ユニットによって受信された前記攻撃タイプに応じて前記攻撃タイプの前記攻撃データパケットに対する予め設定された処理ポリシを取得する、

請求項９に記載の管理ノード。

【請求項１１】

前記決定ユニットは具体的に、前記受信ユニットによって受信された前記攻撃タイプと予め設定されたアルゴリズムとに応じて、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを生成する、

請求項９に記載の管理ノード。

【請求項１２】

前記決定ユニットによって決定された前記処理ポリシによって示される前記オペレーションは、

前記記述情報を有する前記攻撃データパケットに対する処理アクション、又は、前記記述情報を有する前記攻撃データパケットに対する処理アクション及び前記処理アクションを実行する時間を含む、

請求項９から１１のいずれか一項に記載の管理ノード。
【請求項１３】
前記決定ユニットは具体的に、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び前記複数の攻撃データパケットの攻撃タイプを前記受信ユニットが受信した場合、少なくとも２つの同じ攻撃タイプを前記複数の攻撃データパケットの前記攻撃タイプに応じて決定し、前記少なくとも２つの攻撃タイプのうちの１つに応じて、前記攻撃タイプの前記攻撃データパケットに対する処理ポリシを決定する、
請求項９から１２のいずれか一項に記載の管理ノード。
【請求項１４】
管理ノードによって送信された、攻撃データパケットの記述情報と前記記述情報を有する前記攻撃データパケットに対する処理ポリシとを受信する受信ユニットと、
第１のスイッチが、前記記述情報を有する前記攻撃データパケットに対して、前記処理ポリシによって示されるオペレーションを実行するように、前記受信ユニットによって受信された前記記述情報及び前記処理ポリシを前記第１のスイッチに送信する送信ユニットと
を備えるソフトウェアデファインドネットワーキング（ＳＤＮ）コントローラ。
【請求項１５】
前記受信ユニットは具体的に、前記管理ノードによって送信された前記記述情報及び前記処理ポリシを、予め設定された通信インタフェースを使用することによって受信する、
請求項１４に記載のＳＤＮコントローラ。
【請求項１６】
請求項１から８のいずれか一項に記載の方法をコンピュータに実行させるプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０１８９
【補正方法】変更
【補正の内容】
【０１８９】
上記の説明は、本発明の特定の実施方式に過ぎず、本発明の保護範囲を限定するよう意図されてはいない。本発明において開示された技術的範囲内で当業者が容易に考え出した変更又は置き換えはいずれも、本発明の保護範囲に含まれるものとする。従って、本発明の保護範囲は、特許請求の範囲の保護範囲に従うものとする。
［項目１］
攻撃データパケット処理方法であって、
認識ノードによって送信された、攻撃データパケットの記述情報及び上記攻撃データパケットの攻撃タイプを管理ノードによって受信する段階と、
上記攻撃タイプに応じて上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを上記管理ノードによって決定する段階であって、上記処理ポリシは、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、段階と、
上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示される上記オペレーションを上記スイッチが実行するように、ソフトウェアデファインドネットワーキングＳＤＮコントローラを使用することによって上記記述情報及び上記処理ポリシを上記管理ノードによって上記スイッチに送信する段階とを備える方法。
［項目２］
上記攻撃タイプに応じて上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを上記管理ノードによって決定する上記段階は、
上記攻撃タイプに応じて上記攻撃タイプの上記攻撃データパケットに対する予め設定された処理ポリシを上記管理ノードによって取得する段階を含む、項目１に記載の方法。
［項目３］

上記攻撃タイプに応じて上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを上記管理ノードによって決定する上記段階は、
上記攻撃タイプ及び予め設定されたアルゴリズムに応じて上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを上記管理ノードによって生成する段階を含む、項目１に記載の方法。
［項目４］
上記処理ポリシによって示される上記オペレーションは、
上記記述情報を有する上記攻撃データパケットに対する処理アクション、又は、上記記述情報を有する上記攻撃データパケットに対する処理アクション及び上記処理アクションを実行する時間を含む、
項目１から３のいずれか一項に記載の方法。
［項目５］
複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び上記複数の攻撃データパケットの攻撃タイプを上記管理ノードが受信した場合、
上記攻撃タイプに応じて上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを上記管理ノードによって決定する上記段階は、
少なくとも２つの同じ攻撃タイプを上記複数の攻撃データパケットの上記攻撃タイプに応じて上記管理ノードによって決定する段階と、
上記少なくとも２つの攻撃タイプのうちの１つに応じて、上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを上記管理ノードによって決定する段階とを含む、項目１から４のいずれか一項に記載の方法。
［項目６］
ＳＤＮコントローラを使用することによって上記記述情報及び上記処理ポリシを上記管理ノードによって上記スイッチに送信する上記段階は、
上記ＳＤＮコントローラが、上記記述情報及び上記処理ポリシを上記スイッチに転送するように、予め設定された通信インタフェースを使用することによって上記記述情報及び上記処理ポリシを上記管理ノードによって上記ＳＤＮコントローラに送信する段階を含む、項目１から５のいずれか一項に記載の方法。
［項目７］
上記記述情報は、上記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、上記攻撃データパケットの送信元ポート番号、上記攻撃データパケットの宛先ＩＰアドレス、上記攻撃データパケットの宛先ポート番号、及び上記攻撃データパケットのプロトコル番号を含む、
項目１から６のいずれか一項に記載の方法。
［項目８］
攻撃データパケット処理方法であって、
管理ノードによって送信された、攻撃データパケットの記述情報と上記記述情報を有する上記攻撃データパケットに対する処理ポリシとをソフトウェアデファインドネットワーキングＳＤＮコントローラによって受信する段階と、
第１のスイッチが、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示されるオペレーションを実行するように、上記記述情報及び上記処理ポリシを上記ＳＤＮコントローラによって上記第１のスイッチに送信する段階とを備える方法。
［項目９］
管理ノードによって送信された、攻撃データパケットの記述情報と上記記述情報を有する上記攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する上記段階は、
上記管理ノードによって送信された上記記述情報及び上記処理ポリシを、予め設定された通信インタフェースを使用することによって上記ＳＤＮコントローラによって受信する段階を含む、項目８に記載の方法。

［項目１０］
管理ノードによって送信された、攻撃データパケットの記述情報と上記記述情報を有する上記攻撃データパケットに対する処理ポリシとをＳＤＮコントローラによって受信する上記段階の後、上記方法は更に、
マスタＳＤＮコントローラが、上記記述情報及び上記処理ポリシを第２のスイッチに転送し、上記第２のスイッチが、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示される上記オペレーションを実行するように、上記記述情報及び上記処理ポリシを上記ＳＤＮコントローラによって、上記ＳＤＮコントローラに接続された上記マスタＳＤＮコントローラに送信する段階を含む、項目８又は９に記載の方法。
［項目１１］
攻撃データパケット処理方法であって、
認識ノードによって受信されたデータパケットを攻撃データパケットであると上記認識ノードによって識別する段階と、
上記攻撃データパケットの記述情報及び上記攻撃データパケットの攻撃タイプを上記認識ノードによって決定する段階と、
上記記述情報及び上記攻撃タイプを上記認識ノードによって管理ノードに送信する段階であって、上記攻撃タイプは、上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを決定すべく上記管理ノードによって使用され、上記処理ポリシは、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される、段階とを備える方法。
［項目１２］
上記記述情報は、上記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、上記攻撃データパケットの送信元ポート番号、上記攻撃データパケットの宛先ＩＰアドレス、上記攻撃データパケットの宛先ポート番号、及び上記攻撃データパケットのプロトコル番号を含む、
項目１１に記載の方法。
［項目１３］
認識ノードによって送信された、攻撃データパケットの記述情報及び上記攻撃データパケットの攻撃タイプを受信するよう構成される受信ユニットと、
上記受信ユニットによって受信された上記攻撃タイプに応じて上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを決定するよう構成される決定ユニットであって、上記処理ポリシは、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示されるオペレーションを実行するようスイッチに命令すべく使用される、決定ユニットと、
上記スイッチが、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示される上記オペレーションを実行するように、上記受信ユニットによって受信された上記記述情報と、上記決定ユニットによって決定された上記処理ポリシとを、ソフトウェアデファインドネットワーキングＳＤＮコントローラを使用することによって上記スイッチに送信するよう構成される送信ユニットと、
を備える管理ノード。
［項目１４］
上記決定ユニットは具体的に、上記受信ユニットによって受信された上記攻撃タイプに応じて上記攻撃タイプの上記攻撃データパケットに対する予め設定された処理ポリシを取得するよう構成されている、
項目１３に記載の管理ノード。
［項目１５］
上記決定ユニットは具体的に、上記受信ユニットによって受信された上記攻撃タイプと予め設定されたアルゴリズムとに応じて、上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを生成するよう構成されている、

項目１３に記載の管理ノード。
［項目１６］
上記決定ユニットによって決定された上記処理ポリシによって示される上記オペレーションは、
上記記述情報を有する上記攻撃データパケットに対する処理アクション、又は、上記記述情報を有する上記攻撃データパケットに対する処理アクション及び上記処理アクションを実行する時間を含む、
項目１３から１５のいずれか一項に記載の管理ノード。
［項目１７］
上記決定ユニットは具体的に、複数の認識ノードによって送信された、複数の攻撃データパケットの記述情報及び上記複数の攻撃データパケットの攻撃タイプを上記受信ユニットが受信した場合、少なくとも２つの同じ攻撃タイプを上記複数の攻撃データパケットの上記攻撃タイプに応じて決定し、上記少なくとも２つの攻撃タイプのうちの１つに応じて、上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを決定するよう構成されている、
項目１３から１６のいずれか一項に記載の管理ノード。
［項目１８］
上記送信ユニットは具体的に、上記ＳＤＮコントローラが、上記記述情報及び上記処理ポリシを上記スイッチに転送するように、上記受信ユニットによって受信された上記記述情報と、上記決定ユニットによって決定された上記処理ポリシとを予め設定された通信インタフェースを使用することによって上記ＳＤＮコントローラに送信するよう構成されている、
項目１３から１７のいずれか一項に記載の管理ノード。
［項目１９］
上記受信ユニットによって受信された上記記述情報は、上記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、上記攻撃データパケットの送信元ポート番号、上記攻撃データパケットの宛先ＩＰアドレス、上記攻撃データパケットの宛先ポート番号、及び上記攻撃データパケットのプロトコル番号を含む、
項目１３から１８のいずれか一項に記載の管理ノード。
［項目２０］
管理ノードによって送信された、攻撃データパケットの記述情報と上記記述情報を有する上記攻撃データパケットに対する処理ポリシとを受信するよう構成される受信ユニットと、
第１のスイッチが、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示されるオペレーションを実行するように、上記受信ユニットによって受信された上記記述情報及び上記処理ポリシを上記第１のスイッチに送信するよう構成される送信ユニットと
を備えるソフトウェアデファインドネットワーキングＳＤＮコントローラ。
［項目２１］
上記受信ユニットは具体的に、上記管理ノードによって送信された上記記述情報及び上記処理ポリシを、予め設定された通信インタフェースを使用することによって受信するよう構成されている、
項目２０に記載のＳＤＮコントローラ。
［項目２２］
マスタＳＤＮコントローラが、上記記述情報及び上記処理ポリシを第２のスイッチに転送し、上記第２のスイッチが、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示される上記オペレーションを実行するように、上記送信ユニットは更に、上記受信ユニットによって受信された上記記述情報及び上記処理ポリシを上記マスタＳＤＮコントローラに送信するよう構成されている、
項目２０又は２１に記載のＳＤＮコントローラ。

［項目２３］
受信されたデータパケットを攻撃データパケットであると識別するよう構成される識別ユニットと、
上記識別ユニットによって識別された上記攻撃データパケットの記述情報と、上記攻撃データパケットの攻撃タイプとを決定するよう構成される決定ユニットと、
上記決定ユニットによって決定された上記記述情報及び上記攻撃タイプを管理ノードに送信するよう構成される送信ユニットであって、上記攻撃タイプは、上記攻撃タイプの上記攻撃データパケットに対する処理ポリシを決定すべく上記管理ノードによって使用され、上記処理ポリシは、上記記述情報を有する上記攻撃データパケットに対して、上記処理ポリシによって示されるオペレーションを実行するよう、データパケットを転送するスイッチに命令すべく使用される、送信ユニットと、
を備える認識ノード。
［項目２４］
上記決定ユニットによって決定された上記記述情報は、
上記攻撃データパケットの送信元インターネットプロトコルＩＰアドレス、上記攻撃データパケットの送信元ポート番号、上記攻撃データパケットの宛先ＩＰアドレス、上記攻撃データパケットの宛先ポート番号、及び上記攻撃データパケットのプロトコル番号を含む、
項目２３に記載の認識ノード。
［項目２５］
項目１３から１９のいずれか一項に記載の管理ノード、項目２０から２２のいずれか一項に記載のソフトウェアデファインドネットワーキングＳＤＮコントローラ、項目２３又は２４に記載の認識ノード、及びスイッチ
を備える通信システム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/096509

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, IEEE, GOOGLE: attack, packet, processing, strategy, method, management node, perception node, description, information, attack, type, switch, SDN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104580168 A (HUAWEI TECHNOLOGIES CO., LTD.) 29 April 2015 (29.04.2015) claims	1-25
A	CN 103051605 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTER et al.) 17 April 2013 (17.04.2013) description, paragraphs [0098] to [0125]	1-25
A	CN 1588880 A (HUAZHONG UNIVERSITY OF SCIENCE & TECHNOLOGY) 02 March 2005 (02.03.2005) the whole document	1-25
A	US 2006075093 A1 (ENTERASYS NETWORKS, INC.) 06 April 2006 (06.04.2006) the whole document	1-25

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 February 2016	02 March 2016

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
XING, Yunfeng
Telephone No. (86-10) 62413374

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/096509

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104580168 A	29 April 2015	None	
CN 103051605 A	17 April 2013	None	
CN 1588880 A	02 March 2005	None	
US 2006075093 A1	06 April 2006	EP 1817684 A2	15 August 2007
		WO 2006041818 A2	20 April 2006

国际检索报告

国际申请号
PCT/CN2015/096509

A. 主题的分类
H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)
H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)
CNKI;CNPAT;WPI;EPODOC;IEEE;GOOGLE:攻击，数据包，处理，策略，方法，管理节点，感知节点，描述信息，攻击类型，类型，交换机，软件定义网络，attack, packet, strategy, method, management node, description, type, switch, SDN

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 104580168 A (华为技术有限公司) 2015年 4月 29日 (2015-04-29) 权利要求书	1-25
A	CN 103051605 A (国家计算机网络与信息安全管理中心等) 2013年 4月 17日 (2013-04-17) 说明书第[0098]-[0125]段	1-25
A	CN 1588880 A (华中科技大学) 2005年 3月 2日 (2005-03-02) 全文	1-25
A	US 2006075093 A1 (ENTERASYS NETWORKS, INC.) 2006年 4月 6日 (2006-04-06) 全文	1-25

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件
"E" 在国际申请日的当天或之后公布的在先申请或专利
"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
"O" 涉及口头公开、使用、展览或其他方式公开的文件
"P" 公布日先于国际申请日但迟于所要求的优先权日的文件
"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 2月 25日	2016年 3月 2日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 邢雲峰 电话号码 (86-10)62413374

表 PCT/ISA/210（第2页）(2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/096509

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	104580168	A	2015年 4月 29日	无			
CN	103051605	A	2013年 4月 17日	无			
CN	1588880	A	2005年 3月 2日	无			
US	2006075093	A1	2006年 4月 6日	EP	1817684	A2	2007年 8月 15日
				WO	2006041818	A2	2006年 4月 20日

表 PCT/ISA/210（同族专利附件）（2009年7月）

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 ユー、チアンフア
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション・ビルディング ホアウェイ・テクノロジーズ・カンパニー・リミテッド内
(72)発明者 ヤン、シンファ
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション・ビルディング ホアウェイ・テクノロジーズ・カンパニー・リミテッド内

Ｆターム(参考) 5K030 GA13 GA15 HD03 JA10 LB07 LC13