(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6181881号
(P6181881)

(45)発行日　平成29年8月16日(2017.8.16)　(24)登録日　平成29年7月28日(2017.7.28)

(51)Int.Cl.　F I

H04L 12/70	(2013.01)	H04L	12/70	100Z
H04L 12/66	(2006.01)	H04L	12/70	B
		H04L	12/66	B

請求項の数 10　(全 20 頁)

(21)出願番号　特願2016-546587(P2016-546587)
(86)(22)出願日　平成27年8月26日(2015.8.26)
(86)国際出願番号　PCT/JP2015/074072
(87)国際公開番号　WO2016/035644
(87)国際公開日　平成28年3月10日(2016.3.10)
審査請求日　平成28年9月9日(2016.9.9)
(31)優先権主張番号　特願2014-176946(P2014-176946)
(32)優先日　平成26年9月1日(2014.9.1)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　永渕　幸雄
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　寺本　泰大
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　岸　寿春
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】制御装置、制御システム、制御方法、および、制御プログラム

(57)【特許請求の範囲】
【請求項１】
仮想ネットワークにより相互に接続される複数の拠点に設置され、当該拠点内の機器と外部ネットワークとの通信を中継する境界ルータに対し、各種制御を行う制御装置であって、
いずれかの拠点内の機器へのパケットの集中を検知したとき、
前記パケットの集中が検知された機器である攻撃対象の機器の属する拠点以外の各拠点の境界ルータに前記攻撃対象の機器のＩＰアドレスのＮＡＴ（Network Address Translation）設定を行うＮＡＴ設定部と、
いずれかの拠点内に設置されるリダイレクト装置に対し、前記リダイレクト装置へのアクセスを、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストへリダイレクトさせるよう設定するリダイレクト設定部と、
前記リダイレクトの設定後、前記攻撃対象の機器の属する拠点の境界ルータのＮＡＴ設定における前記攻撃対象の機器のプライベートＩＰアドレスを、前記リダイレクト装置のプライベートＩＰアドレスに変更するＮＡＴ変更部と
を備えることを特徴とする制御装置。
【請求項２】
前記リダイレクト設定部は、
前記機器のホスト名および前記ホスト名に対応するＩＰアドレスと、当該機器の属する拠点以外の拠点の境界ルータ配下のホストのホスト名および前記ホスト名に対応するＩＰ

アドレスとが設定されたＤＮＳ（Domain Name System）情報を有するＤＮＳサーバから、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストのホスト名を取得し、前記リダイレクト装置に対し、前記リダイレクト装置へのアクセスを、当該ホスト名のホストへリダイレクトさせるよう設定することを特徴とする請求項１に記載の制御装置。

【請求項３】

前記制御装置は、さらに、

ＤＮＳ（Domain Name System）サーバに設定された、前記機器のホスト名および前記ホスト名に対応するＩＰアドレスと、当該機器の属する拠点以外の拠点の境界ルータ配下のホストのホスト名および前記ホスト名に対応するＩＰアドレスとを含むＤＮＳ情報を記憶する記憶部を備え、

前記リダイレクト設定部は、

前記ＤＮＳ情報から、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストのホスト名を取得し、前記リダイレクト装置に対し、前記リダイレクト装置へのアクセスを、当該ホスト名のホストへリダイレクトさせるよう設定することを特徴とする請求項１に記載の制御装置。

【請求項４】

前記リダイレクト設定部は、

前記リダイレクト装置がないとき、拠点内に前記リダイレクト装置を作成、または、拠点内の機器を前記リダイレクト装置として動作させるよう設定を行うことを特徴とする請求項１～３のいずれか１項に記載の制御装置。

【請求項５】

前記ＮＡＴ変更部により、前記攻撃対象の機器の属する拠点の境界ルータのＮＡＴ設定における前記攻撃対象の機器のプライベートＩＰアドレスを、前記リダイレクト装置のプライベートＩＰアドレスに変更した後、前記攻撃対象の機器を、他の拠点へマイグレーションさせるマイグレーション実行部をさらに備えることを特徴とする請求項１～３のいずれか１項に記載の制御装置。

【請求項６】

前記いずれかの拠点内の機器へのパケットの集中の検知は、前記拠点の境界ルータにおいて、前記機器へのＤＤｏＳ攻撃を検知した場合、予め設定された閾値を超えるパケットの受信を検知した場合、および、前記境界ルータの外部ネットワーク側のインタフェースに設定された帯域を超えるトラヒック量のパケットの受信を検知した場合、のいずれかであることを特徴とする請求項１～３のいずれか１項に記載の制御装置。

【請求項７】

仮想ネットワークにより相互に接続される複数の拠点に設置され、当該拠点内の機器と外部ネットワークとの通信を中継する境界ルータに対し、各種制御を行う制御装置を備える制御システムであって、

他の装置からのアクセスをリダイレクトするリダイレクト装置を含み、

前記制御装置は、

いずれか拠点内の機器へのパケットの集中を検知したとき、

前記パケットの集中が検知された機器である攻撃対象の機器の属する拠点以外の各拠点の境界ルータに前記攻撃対象の機器のＩＰアドレスのＮＡＴ（Network Address Translation）設定を行うＮＡＴ設定部と、

前記リダイレクト装置に対し、前記リダイレクト装置へのアクセスを、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストへリダイレクトさせるよう設定するリダイレクト設定部と、

前記リダイレクトの設定後、前記攻撃対象の機器の属する拠点の境界ルータのＮＡＴ設定における前記攻撃対象の機器のプライベートＩＰアドレスを、前記リダイレクト装置のプライベートＩＰアドレスに変更するＮＡＴ変更部と

を備えることを特徴とする制御システム。

【請求項８】
前記制御システムは、さらに、
前記機器のホスト名および前記ホスト名に対応するＩＰアドレスと、当該機器の属する拠点以外の拠点の境界ルータ配下のホストのホスト名および前記ホスト名に対応するＩＰアドレスとが設定されたＤＮＳ（Domain Name System）情報を有するＤＮＳサーバを備え、
前記リダイレクト設定部は、
前記ＤＮＳサーバから、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストのホスト名を取得し、前記リダイレクト装置に対し、前記リダイレクト装置へのアクセスを、当該ホスト名のホストへリダイレクトさせるよう設定することを特徴とする請求項７に記載の制御システム。
【請求項９】
仮想ネットワークにより相互に接続される複数の拠点に設置され、当該拠点内の機器と外部ネットワークとの通信を中継する境界ルータに対し、各種制御を行う制御方法であって、
いずれかの拠点内の機器へのパケットの集中を検知したとき、
前記パケットの集中が検知された機器である攻撃対象の機器の属する拠点以外の各拠点の境界ルータに前記攻撃対象の機器のＩＰアドレスのＮＡＴ（Network Address Translation）設定を行うステップと、
いずれかの拠点内に設置されるリダイレクト装置に対し、前記リダイレクト装置へのアクセスを、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストへリダクレイトさせるよう設定するステップと、
前記リダイレクトの設定後、前記攻撃対象の機器の属する拠点の境界ルータのＮＡＴ設定における前記攻撃対象の機器のプライベートＩＰアドレスを、前記リダイレクト装置のプライベートＩＰアドレスに変更するステップと
を含んだことを特徴とする制御方法。
【請求項１０】
仮想ネットワークにより相互に接続される複数の拠点に設置され、当該拠点内の機器と外部ネットワークとの通信を中継する境界ルータに対し、各種制御を行う制御プログラムであって、
いずれかの拠点内の機器へのパケットの集中を検知したとき、
前記パケットの集中が検知された機器である攻撃対象の機器の属する拠点以外の各拠点の境界ルータに前記攻撃対象の機器のＩＰアドレスのＮＡＴ（Network Address Translation）設定を行うステップと、
いずれかの拠点内に設置されるリダイレクト装置に対し、前記リダイレクト装置へのアクセスを、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストへリダイレクトさせるよう設定するステップと、
前記リダイレクトの設定後、前記攻撃対象の機器の属する拠点の境界ルータのＮＡＴ設定における前記攻撃対象の機器のプライベートＩＰアドレスを、前記リダイレクト装置のプライベートＩＰアドレスに変更するステップと
をコンピュータに実行させることを特徴とする制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、制御装置、制御システム、制御方法、および、制御プログラムに関する。
【背景技術】
【０００２】
仮想環境を構築する技術としてOpenStack（登録商標）と呼ばれる技術が普及している。また、このOpenStack（登録商標）を用い、複数のデータセンタ等、複数の拠点を仮想Ｌ２（レイヤ２）ネットワークで接続する技術も提案されている（非特許文献１～３）。

【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】OpenStack、[online]、[平成26年6月16日検索]、インターネット<URL：http://www.openstack.org/>
【非特許文献２】石井久治他、「オープンソースlaaS　クラウド基盤OpenStack」、ＮＴＴ技術ジャーナルVol.23、No.8、2011.
【非特許文献３】北爪秀雄他、「クラウドサービスを支えるネットワーク仮想化技術」、ＮＴＴ技術ジャーナルVol.23、No.10、2011.
【非特許文献４】永渕幸雄他、「データセンタ間ライブマイグレーションにおける冗長経路回避に向けた経路制御方式の提案」、信学技報、IN2013-48、pp.71-76、Jul.2013.
【非特許文献５】DDoS攻撃の軽減対策、[online]、[平成26年6月16日検索]、インターネット<URL：http://www.cisco.com/web/JP/product/hs/security/tad/tech/pdf/dda_wp.pdf>
【非特許文献６】ウィキペディア、HTTPリダイレクト、[online]、[平成26年6月16日検索]、インターネット<URL：http://ja.wikipedia.org/wiki/%E3%83%AA%E3%83%80%E3%82%A4%E3%83%AC%E3%82%AF%E3%83%88_(HTTP)>
【非特許文献７】永渕幸雄他、「仮想データセンタ環境におけるDDoS攻撃トラヒック分散方式の提案」、信学技報、IN2014-48、pp.107-112、Jul.2014.
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ここでデータセンタ内の特定のＩＰ（Internet Protocol）機器が、大量のパケットによるＤＤｏＳ（Distributed Denial of Service）攻撃を受けた場合、当該データセンタの入り口に設置されたＦＷ（FireWall）に攻撃パケットが集中する。その結果、当該データセンタ内のＩＰ機器が正規ユーザ（攻撃者以外のユーザ）に対し、継続してサービスを提供できないおそれがあった。そこで、本発明は前記した問題を解決し、ＤＤｏＳ攻撃等の攻撃を受けた場合でも継続してサービスを提供することを課題とする。
【課題を解決するための手段】
【０００５】
前記した課題を解決するため、本発明は、仮想ネットワークにより相互に接続される複数の拠点に設置され、当該拠点内の機器と外部ネットワークとの通信を中継する境界ルータに対し、各種制御を行う制御装置であって、いずれかの拠点内の機器へのパケットの集中を検知したとき、前記パケットの集中が検知された機器である攻撃対象の機器の属する拠点以外の各拠点の境界ルータに前記攻撃対象の機器のＩＰアドレスのＮＡＴ（Network Address Translation）設定を行うＮＡＴ設定部と、いずれかの拠点内に設置されるリダイレクト装置に対し、前記リダイレクト装置へのアクセスを、前記攻撃対象の機器の属する拠点以外のいずれかの拠点の境界ルータ配下のホストへリダイレクトさせるよう設定するリダイレクト設定部と、前記リダイレクトの設定後、前記攻撃対象の機器の属する拠点の境界ルータのＮＡＴ設定における前記攻撃対象の機器のプライベートＩＰアドレスを、前記リダイレクト装置のプライベートＩＰアドレスに変更するＮＡＴ変更部とを備えることを特徴とする。
【発明の効果】
【０００６】
本発明によれば、ＤＤｏＳ攻撃等の攻撃を受けた場合でも継続してサービスを提供することができる。
【図面の簡単な説明】
【０００７】
【図１】図１は、システムの全体構成の一例を示す図である。
【図２】図２は、システムの効果を説明する図である。

【図３】図３は、境界ルータの構成を示す図である。
【図４】図４は、境界ルータのＮＡＴテーブルの一例を示す図である。
【図５】図５は、境界ルータのＮＡＴテーブルの設定変更の一例を示す図である。
【図６】図６は、ＤＮＳサーバの構成を示す図である。
【図７】図７は、クラウドコントローラの構成を示す図である。
【図８】図８は、グローバルＩＰアドレス帯情報の一例を示す図である。
【図９】図９は、リダイレクト装置の構成を示す図である。
【図１０】図１０は、クラウドコントローラの処理手順を示すフローチャートである。
【図１１】図１１は、リダイレクト装置の処理手順を示すフローチャートである。
【図１２】図１２は、ＶＭのマイグレーションを説明する図である。
【図１３】図１３は、制御プログラムを実行するコンピュータを示す図である。
【発明を実施するための形態】
【０００８】
以下、図面を参照しながら、本発明を実施するための形態（実施形態）について説明する。なお、本発明は本実施形態に限定されない。
【０００９】
（全体構成）
まず、図１を用いて本実施形態の制御システム（システム）の全体構成を説明する。システムは、データセンタ（データセンタ１，２，３）と、ユーザ端末１０（１０Ａ～１０Ｅ）と、ＤＮＳ（Domain Name System）サーバ４０と、クラウドコントローラ（制御装置）５０とを備える。これらは、インターネット等のネットワーク６０で接続される。
【００１０】
データセンタはそれぞれ、境界ルータ３０を備え、１以上のＶＭを設置することができる。ここでは、データセンタ１は境界ルータ３０Ａを備え、データセンタ２は境界ルータ３０Ｂを備え、データセンタ３は境界ルータ３０Ｃを備える場合を例に説明する。なお、本実施形態では、データセンタ内に設置される機器がＶＭ（Virtual Machine）である場合を例に説明するが、ＶＭ以外の機器であってもよい。
【００１１】
境界ルータ３０（３０Ａ，３０Ｂ，３０Ｃ）は、ネットワーク６０に接続され、ユーザ端末１０と各データセンタの各ＶＭとの通信を中継する。なお、各境界ルータ３０は、仮想Ｌ２（レイヤ２）ネットワーク２１で構成されるデータセンタ１，２，３を同じ共通のネットワークセグメント２２とネットワーク６０に分割する。
【００１２】
例えば、境界ルータ３０Ａのインタフェース３１には、データセンタ１に割り当てられたＩＰアドレス帯「aaa.bbb.ccc.0/24」から選択されたＩＰアドレス（グローバルＩＰアドレス）「aaa.bbb.ccc.101」が設定される。同様に、境界ルータ３０Ｂにも、当該境界ルータ３０Ｂの属するデータセンタ２に割り当てられたＩＰアドレス帯から選択されたＩＰアドレスが設定され、境界ルータ３０Ｃにも、当該境界ルータ３０Ｃの属するデータセンタ３に割り当てられたＩＰアドレス帯から選択されたＩＰアドレスが設定される。
【００１３】
境界ルータ３０は、ＮＡＴ（Network Address Translation）機能を備え、ＮＡＴテーブル（図４参照）により、各ＶＭのグローバルＩＰアドレス－プライベートＩＰアドレス間の相互変換を行う。例えば、データセンタ１の内部のプライベートＩＰアドレス空間として「xxx.yyy.zzz.0/24」が割り当てられ、ＶＭ（Ａ）のプライベートＩＰアドレスが「xxx.yyy.zzz.101」である場合を考える。この場合、境界ルータ３０Ａは、ＶＭ（Ａ）宛のパケットを受信すると、パケットの宛先のグローバルＩＰアドレス（例えば、「aaa.bbb.ccc.101」）を、当該ＶＭ（Ａ）のプライベートＩＰアドレス（「xxx.yyy.zzz.101」）に変換して、データセンタ１の内部のＶＭ（Ａ）へ転送する。なお、各データセンタ間は仮想Ｌ２（レイヤ２）ネットワーク２１で接続されており、いずれの境界ルータ３０もＮＡＴテーブルを用いることで、パケットを受信した場合に、当該パケットを宛先のＶＭ

へ転送できる。

【００１４】

また、境界ルータ３０は、いわゆるＦＷ（FireWall）としての機能も備え、ＤＤｏＳ攻撃等の攻撃を検知した場合、攻撃パケットのフィルタリングを行う。また、境界ルータ３０は、攻撃を検知した旨を、クラウドコントローラ５０へ通知する。この境界ルータ３０は、物理マシンにより実現されてもよいし、仮想マシンにより実現されてもよい。

【００１５】

ＶＭは、仮想Ｌ２ネットワーク２１および境界ルータ３０を介してユーザ端末１０との通信を実行する。このＶＭは、例えば、ＷｅｂサーバやＤＢ（データベース）サーバ等を実行する仮想マシンである。このＶＭは、データセンタ内に設置される物理リソースにより実現される。なお、物理リソースは、通信インタフェース、プロセッサ、メモリ、ハードディスク等である。以下では、データセンタ１のＶＭ（Ａ）に対する攻撃が発生し、このＶＭ（Ａ）のホスト名は「hoge.example.co.jp」である場合を例に説明する。

【００１６】

また、データセンタ内にはリダイレクト装置７０が設置される。このリダイレクト装置７０は、ユーザ端末１０からのアクセスを受け付けると、所定のリダイレクト先へのリダイレクトを行う。図１において、リダイレクト装置７０はデーセタンタ１に設置されるものとして表現しているが、データセンタ２，３にも設置されてよい。なお、このリダイレクト装置７０は、ＶＭにより実現されてもよいし、物理的なマシンにより実現されてもよい。さらに、境界ルータ３０にリダイレクト装置７０の機能を実装することで実現してもよい。

【００１７】

なお、各データセンタ内の境界ルータ３０、ＶＭおよびリダイレクト装置７０は、仮想スイッチ(図示省略)により仮想Ｌ２ネットワーク２１に接続される。この仮想Ｌ２ネットワーク２１は、各データセンタ間を接続する論理的なＬ２ネットワークである。この仮想Ｌ２ネットワーク２１はいわゆる仮想化技術により実現してもよいし、それ以外の技術により実現してもよい。

【００１８】

ユーザ端末１０は、ネットワーク６０経由で各データセンタ内の機器（例えば、ＶＭ）にアクセスし、ＶＭから各種サービスの提供を受ける。このユーザ端末１０は、例えば、パーソナルコンピュータやスマートフォン等である。

【００１９】

ＤＮＳサーバ４０は、ホスト名の名前解決を行う。例えば、ＤＮＳサーバ４０は、ユーザ端末１０からアクセス先のＶＭのホスト名の名前解決の要求を受け付けると、このホスト名に対応するＩＰアドレスを返す。例えば、ＤＮＳサーバ４０は自身が保有するＤＮＳ情報（符号１０２参照）を参照して、「hoge.example.co.jp」に対するＩＰアドレス「aaa.bbb.ccc.101」を返す。そして、ユーザ端末１０は、当該ＩＰアドレスを用いてＶＭ（例えば、ＶＭ（Ａ））へアクセスする。

【００２０】

なお、このＤＮＳ情報には、各ＶＭ（例えば、ＶＭ（Ａ））のホスト名に対するＩＰアドレス（グローバルＩＰアドレス）の他に、各ＶＭ（例えば、ＶＭ（Ａ））が攻撃を受けた場合のリダイレクト先のホスト名に対するＩＰアドレスが設定される。

【００２１】

例えば、図１の符号１０２に示すＤＮＳ情報には、ＶＭ（Ａ）のホスト名「hoge.example.co.jp」に対するＩＰアドレス「aaa.bbb.ccc.101」の他に、ＶＭ（Ａ）が攻撃されたときのリダイレクト先のホスト名とそのホスト名に対するＩＰアドレスが設定される。具体例を挙げて説明すると、ＶＭ（Ａ）が攻撃されたときのリダイレクト先が、データセンタ２の境界ルータ３０Ｂまたはデータセンタ３の境界ルータ３０Ｃである場合を考える。この場合、図１の符号１０２に示すＤＮＳ情報には、ホスト名「hoge.anti_ddos1.example.co.jp」に対するＩＰアドレスは「ddd.eee.fff.101（境界ルータ３０Ｂに設定されたＶ

Ｍ（Ａ）のグローバルＩＰアドレス）」であり、ホスト名「hoge.anti_ddos2.example.co.jp」に対するＩＰアドレスは「ggg.hhh.iii.101（境界ルータ３０Ｃに設定されたＶＭ（Ａ）のグローバルＩＰアドレス）」であるという情報が設定される。これにより、リダイレクト装置７０（詳細は後記）からのリダイレクトを受けたユーザ端末１０は、リダイレクト先のホスト名の名前解決を行うことができる。

【００２２】

クラウドコントローラ５０は、データセンタ内の各機器（例えば、境界ルータ３０やＶＭ、リダイレクト装置７０）の制御を行う。例えば、クラウドコントローラ５０は、他の境界ルータ３０に対するＮＡＴ用のＩＰアドレスの設定およびＮＡＴテーブルの設定の変更を行う。また、クラウドコントローラ５０は、リダイレクト装置７０に対しリダイレクトの設定を行う。

【００２３】

（動作概要）

次に、引き続き図１を用いて、上記のシステムにおける動作概要を説明する。ここでは、データセンタ１の境界ルータ３０Ａが、ＶＭ（Ａ）に対するＤＤｏＳ攻撃を検知した場合を例に説明する。例えば、データセンタ１の境界ルータ３０ＡがＤＤｏＳ攻撃を検知すると（Ｓ１）、クラウドコントローラ５０へＤＤｏＳ攻撃の検知を通知する（Ｓ２）。この通知を受けたクラウドコントローラ５０は、データセンタ２，３それぞれに割り当てられたグローバルＩＰアドレス帯から、ＮＡＴ用のＩＰアドレスを選択する（Ｓ３）。そして、クラウドコントローラ５０は、各境界ルータ３０にＮＡＴの設定を行う（Ｓ４）。つまり、クラウドコントローラ５０は、境界ルータ３０Ｂ，３０Ｃそれぞれのテーブルに Ｓ３で選択したＶＭ（Ａ）のグローバルＩＰアドレスとプライベートＩＰアドレスとを設定する。

【００２４】

例えば、クラウドコントローラ５０は、境界ルータ３０ＢのＮＡＴテーブルにＳ３で選択したＶＭ（Ａ）のグローバルＩＰアドレス「ddd.eee.fff.101」とＶＭ（Ａ）のプライベートＩＰアドレスとを設定する。また、クラウドコントローラ５０は、境界ルータ３０ＣのＮＡＴテーブルにＳ３で選択したＶＭ（Ａ）のグローバルＩＰアドレス「ggg.hhh.iii.101」とＶＭ（Ａ）のプライベートＩＰアドレスとを設定する。

【００２５】

次に、クラウドコントローラ５０は、リダイレクト装置７０にリダイレクトの設定を行う（Ｓ５）。例えば、クラウドコントローラ５０は、リダイレクト装置７０に対し、当該リダイレクト装置７０がユーザ端末１０からアクセスを受け付けたとき、ＵＲＬ２（hoge.anti_ddos1.example.co.jp）およびＵＲＬ３（hoge.anti_ddos2.example.co.jp）のいずれかにリダイレクトするようリダイレクトの設定を行う。このＵＲＬ２およびＵＲＬ３は、ＤＮＳサーバ４０のＤＮＳ情報に記載されたＶＭ（Ａ）が攻撃されたときのリダイレクト先のホスト名である。クラウドコントローラ５０は、このリダイレクト先のホスト名を、例えば、ＤＮＳサーバ４０のＤＮＳ情報から取得する。なお、データセンタ１内にリダイレクト装置７０がなければ、クラウドコントローラ５０は、データセンタ内のリソースを用いてリダイレクト装置７０を作成（用意）し、上記のリダイレクトの設定を行う。なお、リダイレクト装置７０のプライベートＩＰアドレスは、所定のプライベートＩＰアドレス空間（例えば、「xxx.yyy.zzz.0/24」）から空いているプライベートＩＰアドレス（例えば、「xxx.yyy.zzz.102」）を選択し割り当てる。

【００２６】

その後、クラウドコントローラ５０は、境界ルータ３０ＡのＮＡＴ設定の変更を行う（Ｓ６）。つまり、境界ルータ３０ＡのＮＡＴテーブルにおけるＶＭ（Ａ）のグローバルＩＰアドレスに対するプライベートＩＰアドレスを、ＶＭ（Ａ）のプライベートＩＰアドレスから、リダイレクト装置７０のプライベートＩＰアドレス（例えば、「xxx.yyy.zzz.102」）に変更する。

【００２７】

これにより、例えば、図２に示すように正規ユーザのユーザ端末１０（例えば、ユーザ端末１０Ｄ，１０Ｅ）は、はじめにリダイレクト装置７０へアクセスするが、リダイレクトされ、ＤＮＳサーバ４０によりリダイレクト先のホスト名の名前解決を行い、境界ルータ３０Ｂまたは境界ルータ３０Ｃ経由でＶＭ（Ａ）へアクセスする。つまり、正規ユーザのユーザ端末１０（例えば、ユーザ端末１０Ｄ，１０Ｅ）は、リダイレクト装置７０によりＵＲＬ２（hoge.anti_ddos1.example.co.jp）またはＵＲＬ３（hoge.anti_ddos2.example.co.jp）のいずれかにリダイレクトされる。ここで、正規ユーザのユーザ端末１０（例えば、ユーザ端末１０Ｄ，１０Ｅ）は、ＤＮＳサーバ４０によりＵＲＬ２（hoge.anti_ddos1.example.co.jp）またはＵＲＬ３（hoge.anti_ddos2.example.co.jp）に対するＩＰアドレス（「ddd.eee.fff.101」、「ggg.hhh.iii.101」）を知ると、このＩＰアドレスに基づき境界ルータ３０Ｂまたは境界ルータ３０Ｃ経由でＶＭ（Ａ）にアクセスする。

【００２８】

一方、攻撃者のユーザ端末１０（例えば、ユーザ端末１０Ａ，１０Ｂ，１０Ｃ）は、ブラウザの機能を持たない攻撃プログラム（攻撃ツール）で攻撃を行った場合、ブラウザの機能を必要とするリダイレクトに対応できないため、境界ルータ３０Ａ経由で元のＩＰアドレス（「aaa.bbb.ccc.101」）宛にリダイレクト装置７０を攻撃し続ける。

【００２９】

これにより、正規ユーザのユーザ端末１０（例えば、ユーザ端末１０Ｄ，１０Ｅ）は、アクセスが集中している境界ルータ３０Ａを避けてＶＭ（Ａ）へアクセスすることになるので、攻撃が発生したときもＶＭ（Ａ）へアクセスしやすくなる。また、境界ルータ３０Ａへのアクセスの集中が緩和されるので境界ルータ３０Ａの帯域圧迫を軽減できる。その結果、システムは、ＤＤｏＳ攻撃等の攻撃を受けた場合でもユーザ端末１０に対し継続してサービスを提供することができる。

【００３０】

（境界ルータ）

次に、システムの各構成要素を詳細に説明する。まず、図３を用いて境界ルータ３０を説明する。

【００３１】

前記したとおり、境界ルータ３０は、ネットワーク６０に接続され、ユーザ端末１０と各データセンタの各ＶＭとの通信を中継する。この境界ルータ３０は、インタフェース３１，３４と、記憶部３２と、制御部３３とを備える。

【００３２】

インタフェース３１は、境界ルータ３０とネットワーク６０とを接続するインタフェースである。このインタフェース３１には、この境界ルータ３０の属するデータセンタのＩＰアドレス帯から選択されたグローバルＩＰアドレスが設定される。インタフェース３４は、境界ルータ３０と仮想Ｌ２ネットワーク２１、ＶＭを接続するインタフェースである。

【００３３】

記憶部３２は、ＮＡＴテーブルを記憶する。ＮＡＴテーブルは、データセンタ内の機器（例えば、ＶＭ）のグローバルＩＰアドレスとプライベートＩＰアドレスとを対応付けた情報である。例えば、図４に示すＮＡＴテーブルは、境界ルータ３０ＡにおけるＮＡＴテーブルであり、このＮＡＴテーブルにおいて、グローバルＩＰアドレス「aaa.bbb.ccc.101」に対するプライベートＩＰアドレスは「xxx.yyy.zzz.101」であることを示す。このＮＡＴテーブルは、経路制御部３３２（後記）がＮＡＴを行うときに参照される。また、このＮＡＴテーブルは、クラウドコントローラ５０からの指示に基づき変更される。

【００３４】

図３の制御部３３は、ＮＡＴテーブル管理部３３１と、経路制御部３３２と、攻撃通知部３３３と、フィルタリング部３３４とを備える。

【００３５】

ＮＡＴテーブル管理部３３１は、外部装置からの指示に基づきＮＡＴテーブル（図４参

照）を更新する。例えば、クラウドコントローラ５０から、ＮＡＴテーブルに、ＶＭ（Ａ）のグローバルＩＰアドレスに対するプライベートＩＰアドレスの設定変更指示があった場合、これに応じてＮＡＴテーブルの設定変更を行う。

【００３６】

例えば、クラウドコントローラ５０から、ＮＡＴテーブルに、ＶＭ（Ａ）のグローバルＩＰアドレス「aaa.bbb.ccc.101」に対するプライベートＩＰアドレスを「xxx.yyy.zzz.101（ＶＭ（Ａ）のプライベートＩＰアドレス）」から「xxx.yyy.zzz.102（リダイレクト装置７０のプライベートＩＰアドレス）」への設定変更指示があった場合、ＮＡＴテーブル管理部３３１は、これに応じて、図５の符号３０１→符号３０２に示すようにＮＡＴテーブルの設定変更を行う。

【００３７】

図３の経路制御部３３２は、インタフェース３１，３４経由で入力されたパケットの経路制御を行う。例えば、インタフェース３１経由でユーザ端末１０からＶＭへのパケットを受信すると、このパケットを当該ＶＭへ転送する。このとき経路制御部３３２は、ＮＡＴテーブル（図４参照）を参照して、パケットに付されたグローバルＩＰアドレスとプライベートＩＰアドレスとのＮＡＴ変換を行う。

【００３８】

攻撃通知部３３３は、自身の境界ルータ３０を経由するＶＭへのＤＤｏＳ攻撃等の攻撃を検知した場合、攻撃を検知した旨を、クラウドコントローラ５０へ通知する。

【００３９】

フィルタリング部３３４は、攻撃パケットのフィルタリングを行う。例えば、フィルタリング部３３４は受信したパケットのヘッダ情報を参照し、攻撃パケットと推定されるパケットを廃棄する。

【００４０】

なお、この境界ルータ３０は、いわゆるＦＷ機能を備えるルータにより実現されるものとして説明したが、ルータとＦＷとの２つの装置により実現してももちろんよい。

【００４１】

（ＤＮＳサーバ）

次に、図６を用いてＤＮＳサーバ４０を説明する。ＤＮＳサーバ４０は、前記したとおり、アクセス先のホスト名の名前解決を行う。このＤＮＳサーバ４０は、通信制御部４１と、記憶部４２と、制御部４３とを備える。

【００４２】

通信制御部４１は、他の装置との通信を制御する。例えば、通信制御部４１は、ユーザ端末１０等との間で行われる通信を制御する。

【００４３】

記憶部４２は、ＤＮＳ情報を記憶する。このＤＮＳ情報は、ホスト名に対応するＩＰアドレス（グローバルＩＰアドレス）の情報を含む。このＤＮＳ情報は、ホスト名解決部４３２（後記）がホスト名の名前解決を行う際に参照される。このＤＮＳ情報は、例えば、図１の符号１０２に示す情報等である。

【００４４】

制御部４３は、ＤＮＳ情報管理部４３１と、ホスト名解決部４３２とを備える。

【００４５】

ＤＮＳ情報管理部４３１は、外部装置（例えば、クラウドコントローラ５０）からの指示に基づき、ＤＮＳ情報を設定する。例えば、ＤＮＳ情報は、図１の符号１０２に示すように、ＶＭ（Ａ）のホスト名「hoge.example.co.jp」に対するＩＰアドレスとして「aaa.bbb.ccc.101」が設定され、ホスト名「hoge.anti_ddos1.example.co.jp」に対するＩＰアドレス「ddd.eee.fff.101」が設定され、ホスト名「hoge.anti_ddos2.example.co.jp」に対するＩＰアドレスとして「ggg.hhh.iii.101」が設定される。つまり、このＤＮＳ情報には、ＶＭのホスト名とＩＰアドレスとのペアの他に、このＶＭに対する攻撃を検知したときに用いるＶＭのホスト名とＩＰアドレスとのペアが設定される。このＶＭに対する攻

撃を検知したときに用いるＶＭのホスト名に対応するＩＰアドレスは、攻撃対象のＶＭの属する拠点以外の拠点の境界ルータ３０配下のＩＰアドレスを用いる。なお、ＶＭに対する攻撃を検知したときに用いるＶＭのホスト名は、リダイレクト設定部５３３（後記）がリダイレクト装置７０に対しリダイレクトの設定をするときに参照される。また、上記のホスト名に含まれる「anti_ddos1」や「anti_ddos2」は、説明を簡単にするために用いた文字列であり、実際には、攻撃者にＤＤｏＳ対策であることが分かるような文字列は用いない。

【００４６】

ホスト名解決部４３２は、ＤＮＳ情報を参照して、ホスト名の名前解決を行う。例えば、ホスト名解決部４３２は、ユーザ端末１０からＶＭ（Ａ）のホスト名の名前解決の要求を受け付けると、ＤＮＳ情報を参照して、当該ホスト名に対応するＩＰアドレスを返す。

【００４７】

（クラウドコントローラ）

次に、図７を用いてクラウドコントローラ５０を説明する。クラウドコントローラ５０は、前記したとおりデータセンタ内の各機器（例えば、境界ルータ３０、ＶＭ、リダイレクト装置７０等）の制御を行う。

【００４８】

クラウドコントローラ５０は、通信制御部５１と、記憶部５２と、制御部５３とを備える。通信制御部５１は、他の装置との通信を制御する。例えば、通信制御部５１は、境界ルータ３０やＤＮＳサーバ４０との間で行われる通信を制御する。

【００４９】

記憶部５２は、境界ルータ情報と、グローバルＩＰアドレス帯情報とを記憶する。

【００５０】

境界ルータ情報は、境界ルータ３０ごとに当該境界ルータ３０の属するデータセンタと、当該境界ルータ３０のＩＰアドレスとを示した情報である。

【００５１】

グローバルＩＰアドレス帯情報は、各データセンタに割り当てられたグローバルＩＰアドレス帯を示した情報である。例えば、図８に示すグローバルＩＰアドレス帯情報において、データセンタ１に割り当てられたグローバルＩＰアドレス帯は「aaa.bbb.ccc.0/24」であり、データセンタ２に割り当てられたグローバルＩＰアドレス帯は「ddd.eee.fff.0/24」であることを示す。このグローバルＩＰアドレス帯情報は、ＮＡＴ設定部５３２（後記）が、各境界ルータ３０にＮＡＴの設定を行うときに参照される。

【００５２】

制御部５３は、攻撃通知受信部５３１と、ＮＡＴ設定部５３２と、リダイレクト設定部５３３と、ＮＡＴ変更部５３４とを備える。破線で示すマイグレーション実行部５３５、ＤＮＳ情報設定部５３６は装備される場合と装備されない場合とがあり、装備される場合については、後記する。

【００５３】

攻撃通知受信部５３１は、境界ルータ３０からの攻撃通知を受信する。

【００５４】

ＮＡＴ設定部５３２は、攻撃通知受信部５３１により攻撃通知を受信したとき、各データセンタの境界ルータ３０に対し、攻撃対象のＶＭのＮＡＴの設定を行う。

【００５５】

例えば、攻撃対象のＶＭがデータセンタ１のＶＭ（Ａ）である場合を考える。この場合、ＮＡＴ設定部５３２は、データセンタ２，３の各境界ルータ３０に対し、グローバルＩＰアドレス帯情報（図８参照）を参照して、ＶＭ（Ａ）のＮＡＴ用のＩＰアドレスを選択する。例えば、ＮＡＴ設定部５３２は、グローバルＩＰアドレス帯情報（図８参照）を参照して、データセンタ２に割り当てられたグローバルＩＰアドレス帯「ddd.eee.fff.0/24」から、「ddd.eee.fff.101」を選択し、データセンタ３に割り当てられたグローバルＩＰアドレス帯「ggg.hhh.iii.0/24」から、「ggg.hhh.iii.101」を選択する。そして、Ｎ

ＡＴ設定部５３２は、ＶＭのプライベートＩＰアドレス（例えば、「xxx.yyy.zzz.101」）に対し、「ddd.eee.fff.101」を対応付けたＮＡＴの設定を、データセンタ２の境界ルータ３０Ｂに行う。また、ＮＡＴ設定部５３２は、ＶＭのプライベートＩＰアドレス（例えば、「xxx.yyy.zzz.101」）に対し、「ggg.hhh.iii.101」を対応付けたＮＡＴの設定を、データセンタ３の境界ルータ３０Ｃに対し行う。なお、ＮＡＴ設定部５３２は、ＮＡＴに設定済みの各ＶＭのＩＰアドレスを記憶部５２に記憶しておき、ＮＡＴの設定において各ＶＭ間でＩＰアドレスの重複がないようにする。

【００５６】

リダイレクト設定部５３３は、攻撃通知受信部５３１により攻撃通知を受信したとき、リダイレクト装置７０に対し、リダイレクトの設定を行う。

【００５７】

例えば、攻撃対象のＶＭがデータセンタ１のＶＭ（Ａ）である場合、リダイレクト設定部５３３は、ＤＮＳサーバ４０のＤＮＳ情報（図１の符号１０２参照）から、このＶＭ（Ａ）に対する攻撃を検知したときに用いるＶＭのホスト名（「hoge.anti_ddos1.example.co.jp」と「hoge.anti_ddos2.example.co.jp」）を取得し、リダイレクト装置７０に対し、この取得したいずれかのホスト名のホストへのリダイレクトの設定を行う。これにより、ユーザ端末１０（正規ユーザのユーザ端末１０）からリダイレクト装置７０へのアクセスは、「hoge.anti_ddos1.example.co.jp」または「hoge.anti_ddos2.example.co.jp」のいずれかへリダイレクトされる。その結果、ユーザ端末１０（正規ユーザのユーザ端末１０）は、境界ルータ３０Ｂまたは境界ルータ３０Ｃ経由でＶＭ（Ａ）へアクセスすることになる。なお、リダイレクト設定部５３３は、リダイレクト装置７０に複数のリダイレクト先を設定する場合、リダイレクト装置７０におけるリダイレクト先の選択方法（例えば、ラウンドロビン等）についても設定するようにしてもよい。

【００５８】

なお、リダイレクト装置７０が攻撃対象のＶＭの属するデータセンタ内にないとき、リダイレクト設定部５３３は、リダイレクト装置７０（例えば、リダイレクト用ＶＭ）を、例えば、攻撃対象のＶＭの属するデータセンタ内に作成し、この作成したリダイレクト装置７０に対し、上記のリダイレクトの設定を行う。なお、各データセンタ間は仮想Ｌ２ネットワーク２１により接続されているため、リダイレクト設定部５３３は、攻撃対象のＶＭの属するデータセンタ以外にリダイレクト装置７０を作成してもよいが、攻撃対象のＶＭの属するデータセンタ内にリダイレクト装置７０を作成することで、攻撃パケットがデータセンタ間をまたがって疎通すること避けることができる。

【００５９】

ＮＡＴ変更部５３４は、リダイレクト設定部５３３によるリダイレクトの設定後、攻撃対象のＶＭの属するデータセンタの境界ルータ３０のＮＡＴテーブルにおける当該ＶＭのプライベートＩＰアドレスを、リダイレクト装置７０のプライベートＩＰアドレスに変更する。

【００６０】

例えば、攻撃対象のＶＭがデータセンタ１のＶＭ（Ａ）である場合、ＮＡＴ変更部５３４は、ＶＭ（Ａ）の属するデータセンタ１の境界ルータ３０ＡのＮＡＴテーブルにおけるＶＭ（Ａ）のプライベートＩＰアドレスを、リダイレクト装置７０のプライベートＩＰアドレスに変更する（図１のＳ６参照）。これにより、境界ルータ３０Ａ経由でのＶＭ（Ａ）宛のトラヒックはリダイレクト装置７０に到達することになる。

【００６１】

（リダイレクト装置）

次に、図９を用いて、リダイレクト装置７０を説明する。前記したとおりリダイレクト装置７０は、ユーザ端末１０からのアクセスをリダイレクトする。このリダイレクト装置７０は、通信制御部７１と、記憶部７２と、制御部７３とを備える。

【００６２】

通信制御部７１は、他の装置との通信を制御する。例えば、通信制御部７１は、クラウ

ドコントローラ５０やユーザ端末１０との間で行われる通信を制御する。

【００６３】

記憶部７２は、リダイレクト先情報を記憶する。このリダイレクト先情報は、リダイレクト装置７０のリダイレクト先のホスト名を示す情報であり、例えば、「hoge.anti_ddos1.example.co.jp」および「hoge.anti_ddos2.example.co.jp」等が記載される。

【００６４】

制御部７３は、リダイレクト設定受付部７３１と、リダイレクト部７３２とを備える。

【００６５】

リダイレクト設定受付部７３１は、通信制御部７１経由でクラウドコントローラ５０からリダイレクト設定を受け付けると、リダイレクト設定に含まれるリダイレクト先情報（リダイレクト先のホスト名）を記憶部７２へ出力する。

【００６６】

リダイレクト部７３２は、ユーザ端末１０からのアクセスのＨＴＴＰリダイレクト（リダイレクト）を行う。例えば、リダイレクト部７３２は、通信制御部７１経由でユーザ端末１０からのアクセスを受け付けると、リダイレクト先情報に示されるホスト名（例えば、「hoge.anti_ddos1.example.co.jp」および「hoge.anti_ddos2.example.co.jp」）からラウンドロビンにより決定したホスト名へのリダイレクトを行う。なお、リダイレクト部７３２は上記のようにラウンドロビンによりリダイレクト先を決定することで、正規ユーザのユーザ端末１０から攻撃対象のＶＭ（例えば、ＶＭ（Ａ））へのトラヒックが各データセンタの境界ルータ３０に分散される。

【００６７】

（処理手順）

次に、図１０を用いてクラウドコントローラ５０の処理手順を説明する。クラウドコントローラ５０の攻撃通知受信部５３１は、境界ルータ３０からＶＭへの攻撃通知を受信すると（Ｓ１１）、ＮＡＴ設定部５３２は、グローバルＩＰアドレス帯情報（図７参照）を参照して、当該ＶＭのＮＡＴ用のＩＰアドレスを選択する（Ｓ１２）。そして、ＮＡＴ設定部５３２は、Ｓ１２で選択したＩＰアドレスを、各境界ルータ３０（攻撃対象のＶＭの属するデータセンタ以外の各データセンタの境界ルータ３０）のＮＡＴテーブルに設定する（Ｓ１３）。その後、リダイレクト設定部５３３は攻撃対象のＶＭの属するデータセンタにリダイレクト装置７０があるか否かを確認し（Ｓ１４）、リダイレクト装置７０がなければ（Ｓ１４でＮｏ）、リダイレクト設定部５３３はリダイレクト装置７０を作成する（Ｓ１５）。そして、Ｓ１６へ進む。一方、リダイレクト設定部５３３は攻撃対象のＶＭの属するデータセンタにリダイレクト装置７０があれば（Ｓ１４でＹｅｓ）、Ｓ１５をスキップして、Ｓ１６へ進む。

【００６８】

Ｓ１６において、リダイレクト設定部５３３は、リダイレクト装置７０に対し、リダイレクトの設定を行う。リダイレクト設定部５３３は、ＤＮＳサーバ４０のＤＮＳ情報（図１の符号１０２参照）から、攻撃対象のＶＭ（例えば、ＶＭ（Ａ））に対する攻撃を検知したときに用いるＶＭのホスト名（「hoge.anti_ddos1.example.co.jp」と「hoge.anti_ddos2.example.co.jp」）を取得し、リダイレクト装置７０に対し、この取得したいずれかのホスト名のホストへのリダイレクトの設定を行う。

【００６９】

そして、Ｓ１６の後、ＮＡＴ変更部５３４は、攻撃対象のＶＭの属するデータセンタの境界ルータ３０のＮＡＴ設定における攻撃対象のＶＭのプライベートＩＰアドレスを、リダイレクト装置７０のプライベートＩＰアドレスに変更する（Ｓ１７）。

【００７０】

次に、図１１を用いて、リダイレクト装置７０の処理手順を説明する。リダイレクト装置７０のリダイレクト部７３２は、ユーザ端末１０からのアクセスを受け付けると（Ｓ２１でＹｅｓ）、リダイレクト先情報に示されるホストからリダイレクト先ホストをラウンドロビンで決定し（Ｓ２２）、ユーザ端末１０からのアクセスを、Ｓ２２で決定したホス

トへリダイレクトする（Ｓ２３）。一方、リダイレクト部７３２がユーザ端末１０からのアクセスを受け付ける前は（Ｓ２１でＮｏ）、Ｓ２１へ戻る。

【００７１】

（効果）

システムが上記の処理を行うことで、正規ユーザのユーザ端末１０から、攻撃対象のＶＭへのアクセスはリダイレクト装置７０によりリダイレクトされる。そして、正規ユーザのユーザ端末１０は、ＤＮＳサーバ４０によりリダイレクト先のホスト名の名前解決を行うと、攻撃対象のＶＭの属するデータセンタ以外のデータセンタの境界ルータ３０を経由して攻撃対象のＶＭにアクセスすることになる。一方、攻撃者のユーザ端末１０は、リダイレクト装置７０にアクセスしてもリダイレクトに対応できないため、リダイレクト装置７０にアクセスしたままの状態となる。

【００７２】

つまり、正規ユーザのユーザ端末１０は、攻撃によりアクセスが集中している境界ルータ３０を避けて攻撃対象のＶＭへアクセスするので、攻撃対象のＶＭへアクセスしやすくなる。また、リダイレクトにより攻撃対象のＶＭの属するデータセンタの境界ルータ３０へのアクセスの集中が緩和されるので当該境界ルータ３０の帯域圧迫を軽減できる。その結果、システムは、ＤＤｏＳ攻撃等の攻撃を受けた場合でもユーザ端末１０に対し継続してサービスを提供することができる。

【００７３】

図１２を参照しながら、本実施形態の効果を、具体例を用いながら詳細に説明する。ここでは、各データセンタとネットワーク６０とを接続するアクセス回線の帯域が１０Ｇｂｐｓ、攻撃者のユーザ端末１０（１０Ａ，１０Ｂ，１０Ｃ）からの攻撃トラヒックの合計が８Ｇｂｐｓ、正規ユーザのユーザ端末１０（１０Ｄ，１０Ｅ）からのトラヒックの合計が４Ｇｂｐｓ、ＶＭは１つの要求に対し、２Ｍバイトのデータを応答する場合を例に考える。

【００７４】

この場合、データセンタ１のアクセス回線の負荷は、８Ｇｂｐｓ＋４Ｇｂｐｓ＝１２Ｇｂｐｓである。一方、データセンタ１とネットワーク６０とを接続するアクセス回線の帯域は１０Ｇｂｐｓであるので、このままでは、正規ユーザのユーザ端末１０からのトラヒックを含め２Ｇｂｐｓ分のトラヒックが廃棄されることになる。

【００７５】

ここで、システムがリダイレクト装置７０によるリダイレクトを実施することで、以下の効果が期待できる。

【００７６】

すなわち、正規ユーザのユーザ端末１０（１０Ｄ，１０Ｅ）からのトラヒックは２つのデータセンタ（データセンタ２，３）の境界ルータ３０に分散される。その結果、データセンタ１の境界ルータ３０Ａへのトラヒックは８Ｇｂｐｓ、データセンタ２の境界ルータ３０Ｂへのトラヒックは２Ｇｂｐｓ、データセンタ３の境界ルータ３０Ｃへのトラヒックは２Ｇｂｐｓとなる。つまり、１０Ｇｂｐｓ以下となるので、トラヒックは廃棄されず、正規ユーザのユーザ端末１０からのトラヒックを守ることができる。

【００７７】

さらに、リダイレクト装置７０はユーザ端末１０に対しリダイレクト情報を送信するので、ＶＭ等によりユーザ端末１０にデータ（上記の例では２Ｍバイト）を応答する場合に比べて、ユーザ端末１０へのトラヒック量を低減することができる。また、リダイレクト装置７０は、リダイレクト処理を主な処理とするため、ユーザ端末１０等からのアクセスに対して、通常のウェブサーバよりもＣＰＵ（Central Processing Unit）、メモリ等のリソースが少なくて済む。その結果、リダイレクト装置７０は多数のユーザ端末１０からのアクセスにも対応できる。また、ＶＭのリソースに対して行われるＤＤｏＳ攻撃に対しても効果的である。

【００７８】

さらに、境界ルータ３０におけるＮＡＴ設定の変更およびリダイレクト装置７０によるリダイレクトにより、攻撃者のユーザ端末１０からのアクセスは攻撃対象のＶＭに到達しない。したがって、攻撃対象のＶＭは、正規ユーザのユーザ端末１０からのアクセスに対応すればよいため、前記したようなＶＭのリソースに対して行われるＤＤｏＳ攻撃に対処できる。

【００７９】

また、システムは、攻撃検知前にＤＮＳサーバ４０へのＤＮＳ情報の設定を行っておく。したがって、システムは、例えば、非特許文献７の記載の技術のように、攻撃検知後にＤＮＳサーバのＤＮＳ情報を変更して対処する場合に比べて、攻撃に対する対処を迅速に行うことができる。

【００８０】

（その他の実施形態）

なお、クラウドコントローラ５０が上記のようにリダイレクト装置７０によるリダイレクトの設定を行った後、攻撃対象のＶＭを、他のデータセンタ（例えば、データセンタ２）にマイグレーションさせてもよい。この場合、クラウドコントローラ５０は、図７に示すマイグレーション実行部５３５を備え、このマイグレーション実行部５３５により当該ＶＭのマイグレーションを実行する。

【００８１】

例えば、クラウドコントローラ５０のマイグレーション実行部５３５は、図１２に示すように、攻撃対象のＶＭ（Ａ）をデータセンタ１からデータセンタ２にマイグレーションさせる。このようなマイグレーションを実行することで、境界ルータ３０Ｂまたは境界ルータ３０Ｃ経由でＶＭ（Ａ）へアクセスしてきた正規ユーザのユーザ端末１０は、データセンタ１まで通信を行う必要がなくなるので、ＶＭ（Ａ）との通信時間を短縮することができる。

【００８２】

また、各データセンタには境界ルータ３０が１台設置される場合を例に説明したが、各データセンタに境界ルータ３０が複数台設置されていてももちろんよい。この場合、クラウドコントローラ５０は上記と同様の処理手順により、各境界ルータ３０にＮＡＴの設定を行い、攻撃対象のＶＭの属するデータセンタの境界ルータ３０のＮＡＴの変更を行う、リダイレクト装置７０によるリダイレクトを実行させる。

【００８３】

なお、境界ルータ３０がＤＤｏＳ攻撃を検知したときに攻撃通知を送信することとしたが、これに限定されない。例えば、当該境界ルータ３０で中継するＶＭへのパケットが所定の閾値を超えて送信されたときに攻撃通知を送信するようにしてもよい。ここでの閾値は、例えば、境界ルータ３０からネットワーク６０へ接続するインタフェース３１に設定される帯域の値を用いる。

【００８４】

また、クラウドコントローラ５０のリダイレクト設定部５３３は、ＤＮＳサーバ４０のＤＮＳ情報から、リダイレクト装置７０に設定するリダイレクト先のホスト名を取得することとしたが、これに限定されない。例えば、ＤＮＳサーバ４０のＤＮＳ情報をクラウドコントローラ５０が設定する場合、クラウドコントローラ５０は、ＤＮＳサーバ４０に設定したＤＮＳ情報を記憶部５２に記憶しておく。そして、クラウドコントローラ５０は、記憶部５２のＤＮＳ情報からリダイレクト先のホスト名を取得し、リダイレクト装置７０に設定する。すなわち、クラウドコントローラ５０は、ＤＮＳサーバ４０のＤＮＳ情報を設定するＤＮＳ情報設定部５３６（図７参照）をさらに備え、ＤＮＳ情報設定部５３６はＤＮＳサーバ４０に設定したＤＮＳ情報を記憶部５２に記憶しておく。そして、リダイレクト設定部５３６は、記憶部５２のＤＮＳ情報から、攻撃対象のＶＭの属する拠点以外のいずれかの拠点の境界ルータ３０配下のホストのホスト名を取得し、当該ホスト名のホストをリダイレクト先のホストとしてリダイレクト装置７０に設定する。

【００８５】

なお、前記したシステムの各構成要素は機能概念的なものであり、必ずしも各図に示したように構成されている必要はなく、任意の単位で統合・分散して構成することが可能である。

【００８６】

（プログラム）

また、上記実施形態に係るクラウドコントローラ５０が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成し、実行することもできる。この場合、コンピュータがプログラムを実行することにより、上記実施形態と同様の効果を得ることができる。さらに、かかるプログラムをコンピュータに読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータに読み込ませて実行することにより上記実施形態と同様の処理を実現してもよい。以下に、クラウドコントローラ５０と同様の機能を実現する制御プログラムを実行するコンピュータの一例を説明する。

【００８７】

図１３は、制御プログラムを実行するコンピュータを示す図である。図１３に示すように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有する。これらの各部は、バス１０８０によって接続される。

【００８８】

メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１およびＲＡＭ（Random Access Memory）１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース１０３０は、ハードディスクドライブ１０９０に接続される。ディスクドライブインタフェース１０４０は、ディスクドライブ１１００に接続される。ディスクドライブ１１００には、例えば、磁気ディスクや光ディスク等の着脱可能な記憶媒体が挿入される。シリアルポートインタフェース１０５０には、例えば、マウス１１１０およびキーボード１１２０が接続される。ビデオアダプタ１０６０には、例えば、ディスプレイ１１３０が接続される。

【００８９】

ここで、図１３に示すように、ハードディスクドライブ１０９０は、例えば、ＯＳ１０９１、アプリケーションプログラム１０９２、プログラムモジュール１０９３およびプログラムデータ１０９４を記憶する。上記実施形態で説明した各テーブルは、例えばハードディスクドライブ１０９０やメモリ１０１０に記憶される。

【００９０】

また、制御プログラムは、例えば、コンピュータ１０００によって実行される指令が記述されたプログラムモジュールとして、ハードディスクドライブ１０９０に記憶される。具体的には、上記実施形態で説明したクラウドコントローラ５０が実行する各処理が記述されたプログラムモジュールが、ハードディスクドライブ１０９０に記憶される。

【００９１】

また、制御プログラムによる情報処理に用いられるデータは、プログラムデータとして、例えば、ハードディスクドライブ１０９０に記憶される。そして、ＣＰＵ１０２０が、ハードディスクドライブ１０９０に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出して、上述した各手順を実行する。

【００９２】

なお、制御プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０９０に記憶される場合に限られず、例えば、着脱可能な記憶媒体に記憶されて、ディスクドライブ１１００等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、制御プログラムに係るプログラムモジュール１０９３や

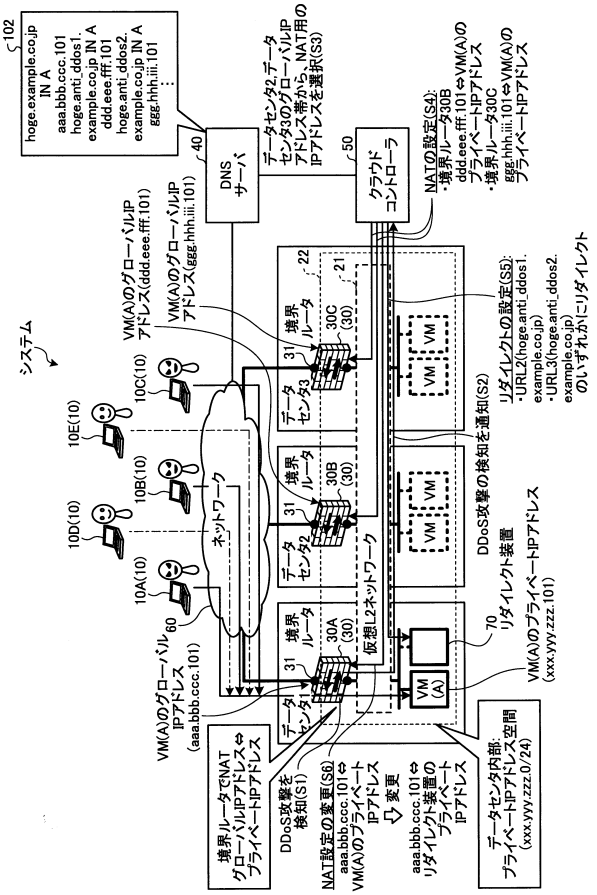
プログラムデータ１０９４は、ＬＡＮ（Local Area Network）やＷＡＮ（Wide Area Network）等のネットワークを介して接続された他のコンピュータに記憶され、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

【符号の説明】

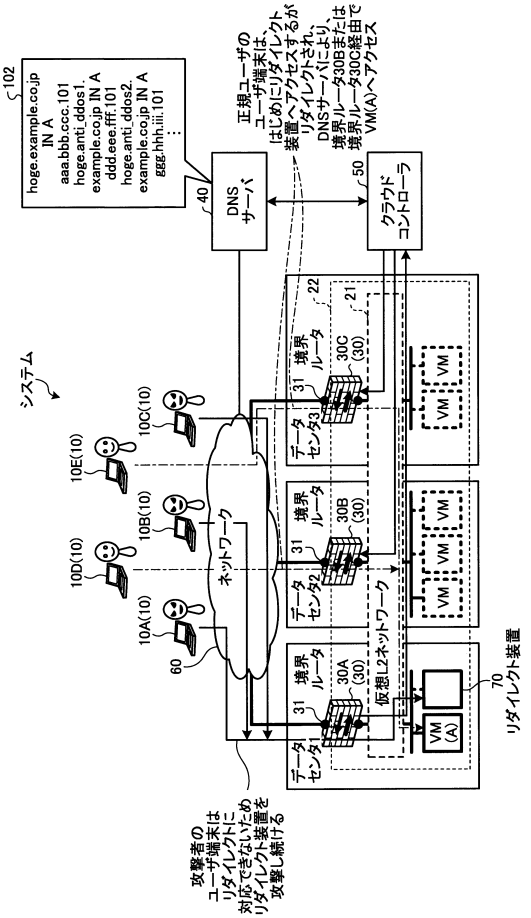
【００９３】

１，２，３　データセンタ
１０　ユーザ端末
２１　仮想Ｌ２ネットワーク
２２　ネットワークセグメント
３０　境界ルータ
３１，３４　インタフェース
３２，４２，５２，７２　記憶部
３３，４３，５３，７３　制御部
４０　ＤＮＳサーバ
４１，５１，７１　通信制御部
５０　クラウドコントローラ
６０　ネットワーク
３３１　ＮＡＴテーブル管理部
３３２　経路制御部
３３３　攻撃通知部
３３４　フィルタリング部
４３１　ＤＮＳ情報管理部
４３２　ホスト名解決部
５３１　攻撃通知受信部
５３２　ＮＡＴ設定部
５３３　リダイレクト設定部
５３４　ＮＡＴ変更部
５３５　マイグレーション実行部
５３６　ＤＮＳ情報設定部
７３１　リダイレクト設定受付部
７３２　リダイレクト部

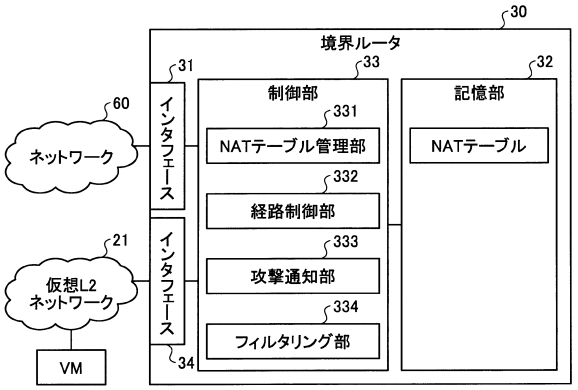
【図１】



【図２】



【図３】



【図５】

NATテーブル

グローバルIPアドレス	プライベートIPアドレス
aaa.bbb.ccc.101 (VM(A)のグローバルIPアドレス)	xxx.yyy.zzz.101 (VM(A)のプライベートIPアドレス)

⇩

NATテーブル

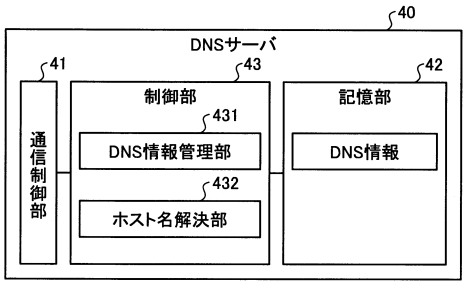
グローバルIPアドレス	プライベートIPアドレス
aaa.bbb.ccc.101 (VM(A)のグローバルIPアドレス)	xxx.yyy.zzz.102 (リダイレクト装置のプライベートIPアドレス)

【図４】

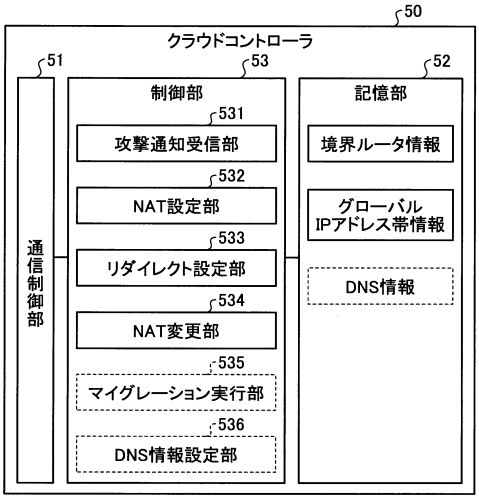
NATテーブル

グローバルIPアドレス	プライベートIPアドレス
aaa.bbb.ccc.101	xxx.yyy.zzz.101

【図６】



【図７】

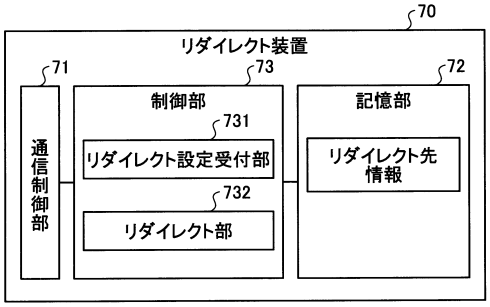


【図８】

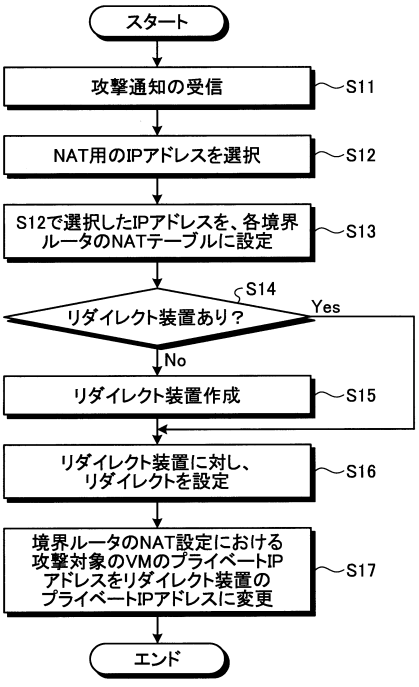
グローバルIPアドレス帯情報

データセンタ	グローバルIPアドレス
データセンタ1	aaa.bbb.ccc.0/24
データセンタ2	ddd.eee.fff.0/24
データセンタ3	ggg.hhh.iii.0/24

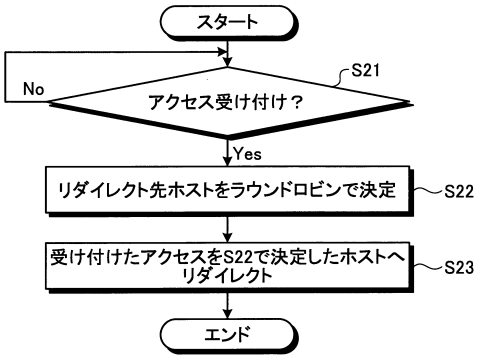
【図９】



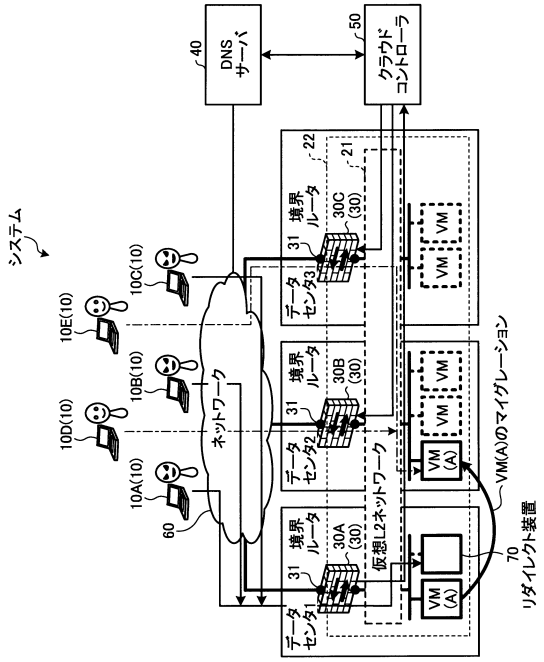
【図１０】



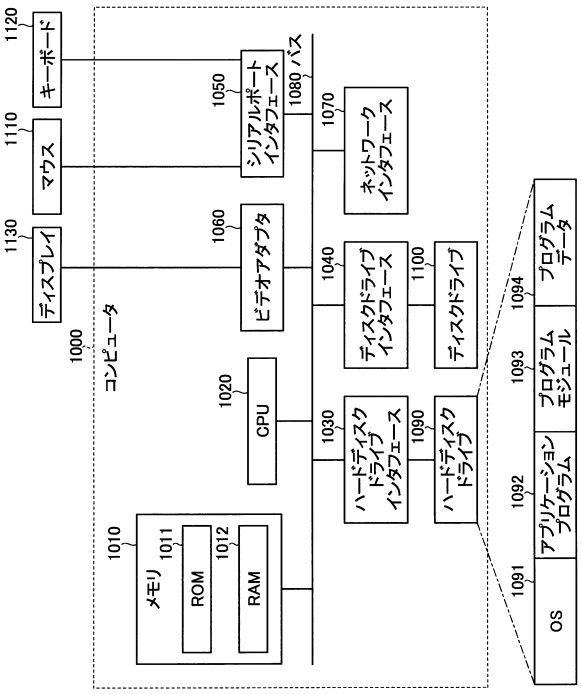
【図１１】


スタート
S21
No
アクセス受け付け？
Yes
リダイレクト先ホストをラウンドロビンで決定
S22
受け付けたアクセスをS22で決定したホストへリダイレクト
S23
エンド

【図１２】


システム
DNSサーバ
40
クラウドコントローラ
50
ネットワーク
60
境界ルータ
31
30A(30)
30B(30)
30C(30)
データセンタ1
データセンタ2
データセンタ3
22
21
仮想L2ネットワーク
VM
VM(A)
VM(A)のマイグレーション
リダイレクト装置
70
10A(10)
10B(10)
10C(10)
10D(10)
10E(10)

【図１３】


コンピュータ
1000
メモリ
1010
ROM
1011
RAM
1012
CPU
1020
ビデオアダプタ
1060
ディスプレイ
1130
シリアルポートインタフェース
1050
マウス
1110
キーボード
1120
ネットワークインタフェース
1070
バス
1080
ディスクドライブインタフェース
1040
ディスクドライブ
1100
ハードディスクドライブインタフェース
1030
ハードディスクドライブ
1090
OS
1091
アプリケーションプログラム
1092
プログラムモジュール
1093
プログラムデータ
1094

フロントページの続き

(72)発明者　小山　高明
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　北爪　秀雄
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

審査官　大石　博見

(56)参考文献　特開２０１１－２２１９９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／７０
Ｈ０４Ｌ　１２／６６