

【公報種別】特許法第 17 条の 2 の規定による補正の掲載
 【部門区分】第 7 部門第 3 区分
 【発行日】平成29年7月6日 (2017.7.6)

【公開番号】特開2015-231131(P2015-231131A)
 【公開日】平成27年12月21日 (2015.12.21)
 【年通号数】公開・登録公報2015-080
 【出願番号】特願2014-116303(P2014-116303)
 【国際特許分類】

H 0 4 L 12/851 (2013.01)
 H 0 4 L 12/70 (2013.01)
 H 0 4 L 12/803 (2013.01)
 G 0 6 F 13/00 (2006.01)
 H 0 4 L 12/66 (2006.01)

【F I】

H 0 4 L 12/851
 H 0 4 L 12/70 1 0 0 Z
 H 0 4 L 12/803
 G 0 6 F 13/00 3 5 1 Z
 H 0 4 L 12/66 B

【手続補正書】

【提出日】平成29年5月10日 (2017.5.10)

【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】

ネットワークを介して通信するネットワーク機器間に設置され、前記ネットワーク機器間で送受信されるデータを中継するネットワーク中継装置であって、

パケットに関する検出条件と検出条件ごとの識別コードを格納する運用側と待機側とを相補的に切替可能な検出条件格納手段と、

前記検出条件格納手段の運用側と待機側とを切り替える切替手段と、

外部から前記検出条件を入力し待機側の前記検出条件格納手段に登録するパケット条件登録手段と、

一のネットワーク機器から他のネットワーク機器宛のパケットを受信するパケット受信手段と、

前記パケット受信手段によって受信されたパケットを運用側の前記検出条件格納手段のパケット条件に該当するか否かを判定する照合手段と、

前記照合手段による判定の結果、パケット条件に該当する場合は、該パケット条件に対応する処理内容を実行するパケット処理手段と、

外部からの前記検出条件の入力周期、処理負荷あるいはパケットのトラフィックによって異常を検知する監視手段と、を備え、

前記切替手段は、外部からの切替指令又は前記監視手段による異常検知により前記検出条件格納手段の運用側と待機側とを切り替えることを特徴とするネットワーク中継装置。

【請求項 2】

外部ネットワークを介して繋がるデータベースから I P アドレスコードごとの注意情報を入力し、前記検出条件のリストを生成するパケット条件設定手段を備え、

前記パケット条件登録手段は、前記パケット条件設定手段から前記検出条件を入力し、前記監視手段は、一定時間以上前記パケット条件設定手段からのデータの受信が無いことによって異常を検知することを特徴とする請求項 1 に記載のネットワーク中継装置。

【請求項 3】

前記パケット処理手段は O S I 参照モデルの I P 層(ネットワーク層)及び／又は T C P / U D P 層(トランスポート層)で前記処理内容を実行し、

予め設定された I P アドレス宛へ前記パケットを送信する処理を実行することを特徴とする請求項 1 または 2 に記載のネットワーク中継装置。

【請求項 4】

物理ポートの通信帯域を制限する帯域制限手段を備え、

前記パケット処理手段は、送信元 I P アドレスに基づいて、パケットを出力する物理ポートを選択し、

前記帯域制限手段は、前記照合手段による判定の結果、パケット条件に該当する場合は、該パケット条件に基づいて前記物理ポートの帯域を制限することを特徴とする請求項 1 乃至 3 のいずれか一項に記載のネットワーク中継装置。

【請求項 5】

請求項 1 乃至 4 のいずれか一項に記載のネットワーク中継装置を用いてネットワーク機器を D D o S 攻撃から防御する方法であって、前記ネットワーク中継装置の上位側の物理ポートは上位ネットワークと接続し、前記ネットワーク中継装置の下位側の一または二以上の物理ポートはネットワーク機器と接続し、前記検出条件格納手段はパケット条件として D D o S 攻撃の I P アドレス情報を保存し、前記パケット処理手段は上位側の物理ポートからの受信パケットの送信元 I P アドレスが D D o S 攻撃の I P アドレス情報に該当する場合は、当該受信パケットを廃棄することを特徴とする D D o S 防御方法。

【請求項 6】

請求項 4 に記載のネットワーク中継装置を用いて、ネットワークに接続されるサーバの負荷を分散する方法であって、前記ネットワーク中継装置の上位側ポートはルータを介して上位ネットワークと接続し、前記ネットワーク中継装置の下位側複数の物理ポートは、それぞれサーバと接続し、前記パケット処理手段は送信元 I P アドレスに基づいて、前記物理ポートを選択することを特徴とする負荷分散方法。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0 0 1 5

【補正方法】変更

【補正の内容】

【0 0 1 5】

また、このパケット処理手段は、一のネットワーク機器から他のネットワーク機器宛にパケット群を転送する際の送信元 I P アドレスを本ネットワーク中継装置が前記パケット群を受信した際の送信元 I P アドレス情報などに付け替える I P アドレス情報付け替え処理を実行するようにしても良い。前記処理内容のうちパケットの廃棄と通過の 2 項目のみを利用する場合には、本ネットワーク中継装置自身に I P アドレスを付与せずにデータを透過的に中継でき、本ネットワーク中継装置は外部から感知不能となるため、本ネットワーク中継装置は外部からのサイバー攻撃を受けず、高いセキュリティ性を保つことができる。加えて、本ネットワーク中継装置が透過的にデータを中継できることから、既存のネットワーク環境下でかつ I P v 4 と I P v 6 という異なるプロトコルが混在する利用環境下でも他のネットワーク中継装置の I P アドレス情報やルーティング情報の設定を変更することなく本ネットワーク中継装置を利用することができる。