

【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 21 年 3 月 12 日 (2009.3.12)

【公表番号】特表 2008-536418 (P2008-536418A)
 【公表日】平成 20 年 9 月 4 日 (2008.9.4)
 【年通号数】公開・登録公報 2008-035
 【出願番号】特願 2008-505873 (P2008-505873)
 【国際特許分類】

H 0 4 L 12/56 (2006.01)

H 0 4 L 12/66 (2006.01)

【F I】

H 0 4 L 12/56 B

H 0 4 L 12/66 B

【手続補正書】
 【提出日】平成 21 年 1 月 22 日 (2009.1.22)
 【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】

接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースの衝突を防止する方法であって、遠隔ソース・クライアントからの宛先ホストにおける接続上の受信パケットに応答して、前記接続を司るセキュリティ・アソシエーションに従うポート番号の範囲内でポート番号が利用可能であるかどうかを判断するステップと、利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するステップと、前記接続を司るポート番号の前記範囲内で利用可能なポート番号がない場合に、前記パケットを拒絶するステップを含む、方法。

【請求項 2】

遠隔ソース・クライアント毎に割り当て可能なポート番号のリストと、前記リスト内の各ポート番号の前記割り当ておよび非割り当て状態とを保持するステップをさらに含む、請求項 1 に記載の方法。

【請求項 3】

割り当て可能なポート番号の各リストは、ビット・ベクトルであって、ビット位置は、ポート番号を識別し、前記ビットの状態は、前記ポート番号の前記割り当ておよび非割り当て状態を表す、請求項 2 に記載の方法。

【請求項 4】

各クライアント側の接続を変換されたポート番号に関連付けるソース・ポート変換テーブルを保持するステップをさらに含む、請求項 1 に記載の方法。

【請求項 5】

前記ソース・ポート変換テーブルは、ソース・ポート・エントリと、変換されたソース・ポート・エントリとを含み、各ソース・ポート・エントリは、変換されたソース・ポート・エントリに固有に関連付けられ、各ソース・ポート・エントリは、インターネット・ソース・アドレスと、NAPTによって割り当てられたUDPソース・ポート番号と、クライアント・ソース・ポート番号と、クライアント・プロトコル識別子とを含み、各変換されたソース・ポート・エントリは、インターネット・ソース・アドレスと、変換された

クライアント・ソース・ポート番号と、クライアント・プロトコル識別子とを含み、ソース・ポート・エントリは、受信パケット上で検索されて、遠隔クライアント接続に以前に割り当てられたポート番号を識別し、変換されたソース・ポート・エントリは、送信パケット上で検索されて、以前に割り当てられた変換されたポート番号からクライアント・ポート番号を識別する、請求項 4 に記載の方法。

【請求項 6】

接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースを防止する方法であって、

- a) パケットをサーバにおいて受信するステップと、
- b) 前記パケットがネットワーク・アドレス・ポート変換器によって変換されており、カプセル化および暗号化されたパケットを含むかどうかを判断するステップと、
- c) 前記パケットが変換されており、カプセル化および暗号化されたパケットを含む場合には、前記カプセル化されたパケットを復号化して、元の接続情報を得るステップと、
- d) 前記接続を司るセキュリティ・アソシエーションに適合するポート番号の範囲内でポート番号が利用可能かどうかを判断するステップと、
- e) 利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するステップと、
- f) 前記接続を司るポート番号の前記範囲内でポート番号が利用可能でない場合に、前記パケットを拒絶するステップと

を含む、方法。

【請求項 7】

接続毎に割り当て可能なポート番号のリストと、前記リスト内の各ポート番号の割り当ておよび非割り当て状態とを保持するステップをさらに含む、請求項 6 に記載の方法。

【請求項 8】

割り当て可能なポート番号の各リストは、ビット・ベクトルであって、ビット位置は、ポート番号を識別し、前記ビットの状態は、前記ポート番号の前記割り当ておよび非割り当て状態を表す、請求項 7 に記載の方法。

【請求項 9】

接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースの衝突を防止するための装置であって、遠隔ソース・クライアントからの宛先ホストにおける接続上の受信パケットにตอบสนองして、前記接続を司るセキュリティ・アソシエーションに従うポート番号の範囲内でポート番号が利用可能であるかどうかを判断するための手段と、利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するための手段と、前記接続を司るポート番号の前記範囲内で利用可能なポート番号がない場合に、前記パケットを拒絶するための手段とを備える、装置。

【請求項 10】

接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースを防止するための装置であって、

- a) パケットをサーバにおいて受信するための手段と、
 - b) 前記パケットがネットワーク・アドレス・ポート変換器によって変換されており、カプセル化および暗号化されたパケットを含むかどうかを判断するための手段と、
 - c) カプセル化されたパケットを復号化して、元の接続情報を得るための手段と、
 - d) 前記接続を司るセキュリティ・アソシエーションに適合するポート番号の範囲内でポート番号が利用可能かどうかを判断するための手段と、
 - e) 利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するための手段と、
 - f) 前記接続を司るポート番号の前記範囲内でポート番号が利用可能でない場合に、前記パケットを拒絶するための手段と
- を含む、装置。

【請求項 1 1】

コンピュータにロードされると、前記コンピュータに対して、接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースの衝突を防止する方法を行わせるプログラム命令を記憶するための記憶媒体であって、前記命令は、遠隔ソース・クライアントからの宛先ホストにおける接続上の受信パケットに応答して、前記接続を司るセキュリティ・アソシエーションに従うポート番号の範囲内でポート番号が利用可能であるかどうかを判断するための命令と、利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するための命令と、前記接続を司るポート番号の前記範囲内で利用可能なポート番号がない場合に、前記パケットを拒絶するための命令とを備える、記憶媒体。

【請求項 1 2】

請求項 1 ～ 8 のいずれか 1 つに記載の方法の各ステップをコンピュータに実行させるプログラム。