

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3802004号
(P3802004)

(45) 発行日 平成18年7月26日(2006.7.26)

(24) 登録日 平成18年5月12日(2006.5.12)

(51) Int. Cl.

F I

H O 4 L 12/66 (2006.01)

H O 4 L 12/66 B

G O 6 F 13/00 (2006.01)

G O 6 F 13/00 3 5 1 N

H O 4 L 12/56 (2006.01)

G O 6 F 13/00 3 5 1 Z

H O 4 L 12/56 4 O O Z

請求項の数 8 (全 18 頁)

(21) 出願番号 特願2003-114714 (P2003-114714)
 (22) 出願日 平成15年4月18日(2003.4.18)
 (65) 公開番号 特開2004-320644 (P2004-320644A)
 (43) 公開日 平成16年11月11日(2004.11.11)
 審査請求日 平成16年6月8日(2004.6.8)

(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二丁目3番1号
 (74) 代理人 100083806
 弁理士 三好 秀和
 (72) 発明者 佐藤 亮介
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内
 (72) 発明者 種茂 文之
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

審査官 菊地 陽一

最終頁に続く

(54) 【発明の名称】 ファイアウォール検査システム、ファイアウォール検査方法、ファイアウォール検査用プログラム、及びファイアウォール検査用記録媒体

(57) 【特許請求の範囲】

【請求項1】

外部からの不正アクセスなどから内部ネットワークを守るファイアウォール装置の検査を行うためのファイアウォール検査システムにおいて、
 前記ネットワーク内で前記ファイアウォール装置を挟んで接続可能な第1の検査端末及び第2の検査端末と、当該第1及び第2の検査端末の動作を管理する管理装置とを有し、更に、

前記管理装置は、

前記第1及び第2の検査端末に対して、前記第1及び第2の検査端末が所定のアルゴリズムで動作するための検査シーケンスデータを送信するデータ送信手段を有し、

前記第1の検査端末は、

前記検査シーケンスデータを受信する第1のデータ受信手段と、

前記第1のデータ受信手段で受信した検査シーケンスデータを記憶する第1のデータ記憶手段とを有し、

前記第2の検査端末は、

前記検査シーケンスデータを受信する第2のデータ受信手段と、

前記第2のデータ受信手段で受信した検査シーケンスデータを記憶する第2のデータ記憶手段とを有し、

前記第1の検査端末は、

前記第1のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイア

ウォール装置を介して前記第2の検査端末に検査パケットを送信する検査パケット送信手段を有し、

前記第2の検査端末は、

前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記第1の検査端末から送信されてきた検査開始信号を受信したことを契機とした所定時間内に、前記検査パケットを受信するか否かを判断する検査パケット受信判断手段と、

前記検査パケット受信判断手段によって判断した受信結果を記録する第2の受信結果記録手段と、

前記第2の受信結果記録手段に記録した受信結果を第2の検査結果データとして前記管理装置に送信する第2の検査結果送信手段と、

10

前記検査パケット受信判断手段によって前記検査パケットを受信したと判断した場合には、前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイアウォール装置を介して前記第1の検査端末に対し、前記検査パケットを受信したことを前記第1の検査端末に通知するための応答パケットを送信する応答パケット送信手段とを有し、

前記第1の検査端末は、

前記検査パケット送信手段によって検査パケットを送信したことを契機とした所定時間内に、前記応答パケットを受信するか否かを判断する応答パケット受信判断手段と、

前記応答パケット受信判断手段によって判断した受信結果を記録する第1の受信結果記録手段と、

20

前記第1の受信結果記録手段に記録した受信結果を第1の検査結果データとして前記管理装置に送信する第1の検査結果送信手段と、前記管理装置は、

前記第1及び第2の検査端末から送られてきた第1及び第2の検査結果データに基づいて、検査結果の解析を行う解析手段を有する

ことを特徴とするファイアウォール検査システム。

【請求項2】

前記管理装置の解析手段は、

前記第1の検査結果データが前記第1の検査端末によって所定時間内に応答パケットを受信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記応答パケットの通過が阻まれたと解析し、

30

前記第2の検査結果データが前記第2の検査端末によって所定時間内に検査パケットを受信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記検査パケットの通過が阻まれたと解析する

ことを特徴とする請求項1に記載のファイアウォール検査システム。

【請求項3】

前記検査シーケンスデータは、第1の検査端末に送信させる検査パケットの種類と数を第2の検査端末に通知するためのデータであり、更に、

前記第1の検査端末の検査パケット送信手段は、全てのIPアドレスを送信元とすると共に全てのIPアドレスを送信先として組み合わせた検査パケットを送信し、

前記第2の検査端末の検査パケット受信手段は、全ての検査パケットを受信可能とする

40

ことを特徴とする請求項1又は2に記載のファイアウォール検査システム。

【請求項4】

外部からの不正アクセスなどから内部ネットワークを守るファイアウォール装置の検査を行うためのファイアウォール検査方法において、

前記ネットワーク内で前記ファイアウォール装置を挟んで接続可能な第1の検査端末及び第2の検査端末と、当該第1及び第2の検査端末の動作を管理する管理装置とを利用し、更に、

前記第1の検査端末は、前記管理装置から送られてくる検査シーケンスデータを記憶する第1のデータ記憶手段と、前記第2の検査端末から送られたパケットの受信結果を記録する第1の受信結果記録手段とを有し、

50

前記第2の検査端末は、前記管理装置から送られてくる検査シーケンスデータを記憶する第2のデータ記憶手段と、前記第1の検査端末から送られたパケットの受信結果を記録する第2の受信結果記録手段とを有した状態で、

前記管理装置は、

前記第1及び第2の検査端末に対して、前記第1及び第2の検査端末が所定のアルゴリズムで動作するための検査シーケンスデータを送信するデータ送信ステップを実行し、

前記第1の検査端末は、

前記検査シーケンスデータを受信する第1のデータ受信ステップと、

前記第1のデータ受信ステップで受信した検査シーケンスデータを前記第1のデータ記憶手段に記憶するステップと実行し、

10

前記第2の検査端末は、

前記検査シーケンスデータを受信する第2のデータ受信ステップと、

前記第2のデータ受信ステップで受信した検査シーケンスデータを前記第2のデータ記憶手段に記憶するステップとを実行し、前記第1の検査端末は、

前記第1のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイアウォール装置を介して前記第2の検査端末に検査パケットを送信する検査パケット送信ステップを実行し、

前記第2の検査端末は、

前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記第1の検査端末から送信されてきた検査開始信号を受信したことを契機とした所定時間内に、前記検査パケットを受信するか否かを判断する検査パケット受信判断ステップと、

20

前記検査パケット受信判断ステップによって判断した受信結果を第2の受信結果記録手段に記録するステップと、

前記第2の受信結果記録手段に記録した受信結果を第2の検査結果データとして前記管理装置に送信する第2の検査結果送信ステップと、

前記検査パケット受信判断ステップによって前記検査パケットを受信したと判断した場合には、前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイアウォール装置を介して前記第1の検査端末に対し、前記検査パケットを受信したことを前記第1の検査端末に通知するための応答パケットを送信する応答パケット送信ステップとを実行し、

30

前記第1の検査端末は、

前記検査パケット送信ステップによって検査パケットを送信したことを契機とした所定時間内に、前記応答パケットを受信するか否かを判断する応答パケット受信判断ステップと

、前記応答パケット受信判断ステップによって判断した受信結果を前記第1の受信結果記録手段に記録するステップと、

前記第1の受信結果記録手段に記録した受信結果を第1の検査結果データとして前記管理装置に送信する第1の検査結果送信ステップとを実行し、

前記管理装置は、

前記第1及び第2の検査端末から送られてきた第1及び第2の検査結果データに基づいて、検査結果の解析を行う解析ステップを実行することを特徴とするファイアウォール検査方法。

40

【請求項5】

前記管理装置の解析ステップは、

前記第1の検査結果データが前記第1の検査端末によって所定時間内に応答パケットを受信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記応答パケットの通過が阻まれたと解析し、

前記第2の検査結果データが前記第2の検査端末によって所定時間内に検査パケットを受信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記検査パケットの通過が阻まれたと解析する

50

ことを特徴とする請求項4に記載のファイアウォール検査方法。

【請求項6】

前記検査シーケンスデータは、第1の検査端末に送信させる検査パケットの種類と数を第2の検査端末に通知するためのデータであり、更に、

前記第1の検査端末の検査パケット送信ステップは、全てのIPアドレスを送信元とすると共に全てのIPアドレスを送信先として組み合わせた検査パケットを送信し、

前記第2の検査端末の検査パケット受信ステップは、全ての検査パケットを受信可能とする

ことを特徴とする請求項4又は5に記載のファイアウォール検査方法。

【請求項7】

前記ファイアウォール検査方法で利用する装置及び検査端末に、請求項4乃至6のいずれかに記載の各ステップを実行させるためのファイアウォール検査用プログラム。

【請求項8】

請求項7に記載のファイアウォール検査用プログラムを記録した、コンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、外部からの不正アクセスなどから内部ネットワークを守るファイアウォール装置におけるフィルタリングルールの検査を行う発明に関する。

【0002】

【従来の技術】

近年、インターネット接続時のセキュリティを確保するにあたっては、外部ネットワークからのアクセスをフィルタリングするファイアウォール装置が正しく設定されていることが重要であり、これを検査する必要性が生じている。従来のファイアウォール検査方法の一例が、下記文献に記載されている（非特許文献1参照）。

【0003】

ファイアウォール装置におけるパケットの通過・非通過を制御しているフィルタリングルールに係る従来のフィルタリングルール検査方法は、図12に示すようにファイアウォール装置302に検査端末301のIPアドレス、特定ポートとホスト（コンピュータ）303のIPアドレス、特定ポートに対してどのようなフィルタリングルールが設定されているかを確認する為に検査端末301が検査パケット304をホスト303のIPアドレスと特定のポートに向けて送出する。すると、ファイアウォール装置302で検査パケット304の通過を許可されていれば、検査パケット304はホスト303に到達する。そして、ホスト303が検査パケット304の宛先ポートでサービスを提供していれば、ホスト303が検査パケット304に対して応答パケット305を返すので、応答パケット305を受信した検査端末301は、応答パケット305の受信をもって、ファイアウォール装置302の検査端末301のIPアドレス、特定ポートとホスト303のIPアドレス、特定ポートに対してパケットを通過させるようなフィルタリングルールが設定されていると判断する。

【0004】

【非特許文献1】

クラッキング防衛大全（翔泳社，2000，ISBN4-88135-881-2）の287頁～290頁「ファイアウォールを通過するスキャン」

【0005】

【発明が解決しようとする課題】

しかしながら、ファイアウォール装置302のフィルタリングルール検査において、検査パケットに対する応答パケットが得られなかった場合には、上記従来技術では、検査パケット304がファイアウォール装置302を通過しなかったのか、或いは、相手ホスト303が従来方法の想定しているような応答パケットを返す設定になっていなかったのかを

10

20

30

40

50

判断することが出来ない。即ち、ファイアウォール装置 302 の反対側に接続されているホスト 303 が、必ずしも従来技術の方法が望ような応答パケットを返していないのか、ファイアウォール装置 302 のフィルタリングルールで通過が許可されていなかったのかを正確に判断できない。このため、ファイアウォール装置 302 のフィルタリングルールのうち、パケットを通過させない設定になっている部分の検査が正確に行えないという問題が生じていた。

【0006】

本発明は上述した事情に鑑みてなされたもので、ファイアウォール装置のフィルタリングルールのうちパケットを通過させない設定になっている部分の検査を正確に行うことの出来る発明を公開することを目的とする。

【0009】

【課題を解決するための手段】

上記目的を達成するため、本発明は、外部からの不正アクセスなどから内部ネットワークを守るファイアウォール装置の検査を行うためのファイアウォール検査システムにおいて、前記ネットワーク内で前記ファイアウォール装置を挟んで接続可能な第1の検査端末及び第2の検査端末と、当該第1及び第2の検査端末の動作を管理する管理装置とを有し、更に、前記管理装置は、前記第1及び第2の検査端末に対して、前記第1及び第2の検査端末が所定のアルゴリズムで動作するための検査シーケンスデータを送信するデータ送信手段を有し、前記第1の検査端末は、前記検査シーケンスデータを受信する第1のデータ受信手段と、前記第1のデータ受信手段で受信した検査シーケンスデータを記憶する第1のデータ記憶手段とを有し、前記第2の検査端末は、前記検査シーケンスデータを受信する第2のデータ受信手段と、前記第2のデータ受信手段で受信した検査シーケンスデータを記憶する第2のデータ記憶手段とを有し、前記第1の検査端末は、前記第1のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイアウォール装置を介して前記第2の検査端末に検査パケットを送信する検査パケット送信手段を有し、前記第2の検査端末は、前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記第1の検査端末から送信されてきた検査開始信号を受信したことを契機とした所定時間内に、前記検査パケットを受信するか否かを判断する検査パケット受信判断手段と、前記検査パケット受信判断手段によって判断した受信結果を記録する第2の受信結果記録手段と、前記第2の受信結果記録手段に記録した受信結果を第2の検査結果データとして前記管理装置に送信する第2の検査結果送信手段と、前記検査パケット受信判断手段によって前記検査パケットを受信したと判断した場合には、前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイアウォール装置を介して前記第1の検査端末に対し、前記検査パケットを受信したことを前記第1の検査端末に通知するための応答パケットを送信する応答パケット送信手段とを有し、前記第1の検査端末は、前記検査パケット送信手段によって検査パケットを送信したことを契機とした所定時間内に、前記応答パケットを受信するか否かを判断する応答パケット受信判断手段と、前記応答パケット受信判断手段によって判断した受信結果を記録する第1の受信結果記録手段と、前記第1の受信結果記録手段に記録した受信結果を第1の検査結果データとして前記管理装置に送信する第1の検査結果送信手段と、前記管理装置は、前記第1及び第2の検査端末から送られてきた第1及び第2の検査結果データに基づいて、検査結果の解析を行う解析手段を有することを特徴とするファイアウォール検査システムである。

【0010】

また、本発明は、前記管理装置の解析手段は、前記第1の検査結果データが前記第1の検査端末によって所定時間内に応答パケットを受信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記応答パケットの通過が阻まれたと解析し、前記第2の検査結果データが前記第2の検査端末によって所定時間内に検査パケットを受信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記検査パケットの通過が阻まれたと解析することを特徴とする請求項1に記載のファイアウォール検査システムである。

10

20

30

40

50

【0011】

また、本発明は、前記検査シーケンスデータは、第1の検査端末に送信させる検査パケットの種類と数を第2の検査端末に通知するためのデータであり、更に、前記第1の検査端末の検査パケット送信手段は、全てのIPアドレスを送信元とすると共に全てのIPアドレスを送信先として組み合わせた検査パケットを送信し、前記第2の検査端末の検査パケット受信手段は、全ての検査パケットを受信可能とすることを特徴とする請求項1又は2に記載のファイアウォール検査システムである。

【0014】

また、本発明は、外部からの不正アクセスなどから内部ネットワークを守るファイアウォール装置の検査を行うためのファイアウォール検査方法において、前記ネットワーク内で
10 前記ファイアウォール装置を挟んで接続可能な第1の検査端末及び第2の検査端末と、当該第1及び第2の検査端末の動作を管理する管理装置とを利用し、更に、前記第1の検査端末は、前記管理装置から送られてくる検査シーケンスデータを記憶する第1のデータ記憶手段と、前記第2の検査端末から送られたパケットの受信結果を記録する第1の受信結果記録手段とを有し、前記第2の検査端末は、前記管理装置から送られてくる検査シーケンスデータを記憶する第2のデータ記憶手段と、前記第1の検査端末から送られたパケットの受信結果を記録する第2の受信結果記録手段とを有した状態で、前記管理装置は、前記第1及び第2の検査端末に対して、前記第1及び第2の検査端末が所定のアルゴリズムで動作するための検査シーケンスデータを送信するデータ送信ステップを実行し、前記第1の検査端末は、前記検査シーケンスデータを受信する第1のデータ受信ステップと、前記第1のデータ受信ステップで受信した検査シーケンスデータを前記第1のデータ記憶手段に記憶するステップと実行し、前記第2の検査端末は、前記検査シーケンスデータを受信する第2のデータ受信ステップと、前記第2のデータ受信ステップで受信した検査シーケンスデータを前記第2のデータ記憶手段に記憶するステップとを実行し、前記第1の検査端末は、前記第1のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイアウォール装置を介して前記第2の検査端末に検査パケットを送信する検査パケット送信ステップを実行し、前記第2の検査端末は、前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記第1の検査端末から送信されてきた検査開始信号を受信したことを契機とした所定時間内に、前記検査パケットを受信するか否かを判断する検査パケット受信判断ステップと、前記検査パケット受信判断ステップによって判断した受信結果を第2の受信結果記録手段に記録するステップと、前記第2の受信結果記録手段に記録した受信結果を第2の検査結果データとして前記管理装置に送信する第2の検査結果送信ステップと、前記検査パケット受信判断ステップによって前記検査パケットを受信したと判断した場合には、前記第2のデータ記憶手段に記憶した検査シーケンスデータの内容に従い、前記ファイアウォール装置を介して前記第1の検査端末に対し、前記検査パケットを受信したことを前記第1の検査端末に通知するための応答パケットを送信する応答パケット送信ステップとを実行し、前記第1の検査端末は、前記検査パケット送信ステップによって検査パケットを送信したことを契機とした所定時間内に、前記応答パケットを受信するか否かを判断する応答パケット受信判断ステップと、前記応答パケット受信判断ステップによって判断した受信結果を前記第1の受信結果記録手段に記録するステップと、前記第1の受信結果記録手段に記録した受信結果を第1の検査結果データとして前記管理装置に送信する第1の検査結果送信ステップとを実行し、前記管理装置は、前記第1及び第2の検査端末から送られてきた第1及び第2の検査結果データに基づいて、検査結果の解析を行う解析ステップを実行することを特徴とするファイアウォール検査方法。
20
30
40

【0015】

また、本発明は、前記管理装置の解析ステップは、前記第1の検査結果データが前記第1の検査端末によって所定時間内に応答パケットを受信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記応答パケットの通過が阻まれたと解析し、前記第2の検査結果データが前記第2の検査端末によって所定時間内に検査パケットを受
50

信しなかった旨の受信結果である場合には、前記ファイアウォール装置によって前記検査パケットの通過が阻まれたと解析することを特徴とする請求項4に記載のファイアウォール検査方法である。

【0016】

また、本発明は、前記検査シーケンスデータは、第1の検査端末に送信させる検査パケットの種類と数を第2の検査端末に通知するためのデータであり、更に、前記第1の検査端末の検査パケット送信ステップは、全てのIPアドレスを送信元とすると共に全てのIPアドレスを送信先として組み合わせた検査パケットを送信し、前記第2の検査端末の検査パケット受信ステップは、全ての検査パケットを受信可能とすることを特徴とする請求項4又は5に記載のファイアウォール検査方法である。

10

【0017】

また、本発明は、前記ファイアウォール検査方法で利用する装置及び検査端末に、請求項4乃至6のいずれかに記載の各ステップを実行させるためのファイアウォール検査用プログラムである。

【0018】

ここで、本発明における「プログラム」とは、コンピュータによる処理に適した命令の順番付けられた列からなるものをいい、コンピュータのHD(Hard Disk)、CD-RW等にインストールされているものや、CD-ROM、DVD、FD、半導体メモリ、コンピュータのHDD等の各種記録媒体に記録されているものや、インターネット等の外部ネットワークを介して配信されるものも含まれる。

20

【0019】

また、本発明は、請求項7に記載のファイアウォール検査用プログラムを記録した、コンピュータ読み取り可能な記録媒体である。

【0020】

ここで、本発明における「記録媒体」とは、上記コンピュータで上記ステップを実行させるためのプログラムの読み取りに使用することができればよく、情報を媒体の物理的特性を利用してどのように記録するか等の物理的な記録方法には依存しない。例えば、FD(Flexible Disk)、CD-ROM(R, RW)(Compact Disc Read Only Memory(CD Recordable, CD Rewritable))、DVD-ROM(RAM, R, RW)(Digital Versatile Disk Read Only Memory(DVD Random Access Memory, DVD Recordable, DVD Rewritable))、半導体メモリ、MO(Magneto Optical Disk)、MD(Mini Disk)、磁気テープ等が該当する。

30

【0021】

【発明の実施の形態】

以下、図面を用いて、本発明の第1の実施形態について説明する。

【0022】

図1は、本実施形態に係るファイアウォール検査システム1の全体構成図である。図1に示すように、各内部ネットワーク100a, b, c(以下、これらの総称を示す場合は「内部ネットワーク100」という)には、それぞれファイアウォール装置43a, b, c(以下、これらの総称を示す場合は「ファイアウォール装置43」という)を挟んで各内部ネットワーク100内で、それぞれ検査端末A41a, b, c(以下、これらの総称を示す場合は「検査端末A41」という)と検査端末B42a, b, c(以下、これらの総称を示す場合は「検査端末B42」という)が接続されている。また、検査端末A41及び検査端末B42に、本方法専用の管理用ネットワーク200で接続された管理装置40と、管理装置40のユーザインタフェースを介して本方法の利用者がそれぞれ使用する管理端末44a, b, c(以下、これらの総称を示す場合には「管理端末44」という)によって構成されている。これらの管理端末44a, b, cは、それぞれファイアウォール装置43a, b, cの検査に使用される。尚、管理端末44aは、ファイアウォール装置43b, cの検査に使用される等、どの管理端末44から、どのファイアウォール装置43を管理してもよい。

40

【0023】

50

図2は、図1に示すファイアウォール検査システム1におけるデータ等の流れを示した概略構成図である。また、図3は、図2中のファイアウォール装置43のフィルタリングルールを示した図である。このようなルールをファイアウォール装置43に設定している場合、発信元IPアドレスが192.168.0.1、発信元ポートが任意(any)のポート、送信先IPアドレスが10.0.0.1、送信先ポート番号が80のパケットはファイアウォール装置43を通過することができ、発信元のIPアドレス、ポート番号、及び送信先IPアドレスが全て任意(any)で、送信先ポート番号が110のパケットはファイアウォール装置43を通過することができない。

【0024】

この場合、検査端末A41は、192.168.0.0/24のネットワークに接続され、検査端末B42は、10.0.0.0/8のネットワークに接続されている。このことは、検査端末A41、B42が持つIPアドレスを制限するものではない。

【0025】

また、管理端末44は、利用者が管理装置40に、図3に示すようなフィルタリングルール45の入力を行うためのコンピュータである。管理装置44は、管理装置44から入力を受け付けたフィルタリングルール45に基づいて、ファイアウォール装置の検査に必要な検査パケットの内容、検査パケットの数、検査パケットの送受信タイミング、及び、想定される検査パケットの通過・非通過の状態を分析し、図4に示すような検査シーケンスデータ46を作成し、管理用ネットワーク200を介して検査端末A41と検査端末B42に渡すためのコンピュータである。本実施形態では、図4に示すように、検査シーケンスデータ46として、送信元IPアドレスが192.168.0.1、発信元ポート番号が任意、送信先IPアドレスが10.0.0.1、送信先ポート番号が1~65535を作成する。

【0026】

また、検査シーケンスデータ46を受け取った検査端末A41は、検査シーケンスデータ46に従い、検査端末B42に対して、検査パケット47（発信元IPアドレス：192.168.0.1、発信元ポート番号：仮にxxxとする、送信先IPアドレス：10.0.0.1、送信先ポート番号：80）を送信する一方、検査シーケンスデータ46を受け取った検査端末B42では、検査シーケンスデータ46に従い、検査端末A41から送られて来るはずの検査パケット47を、予め決められた所定時間待ち受ける。そして、図3に示すフィルタリングルール45により、検査パケット47はファイアウォール装置43を通過し、所定時間内に検査端末B42が検査パケット47を受信出来れば、検査端末B42では、受信した旨の受信結果を記録しておく。この受信結果は、第2の検査結果データ50として管理端末40に送信される。これにより、管理端末40では、検査パケット47が持っていたパラメータを持つパケットは、ファイアウォール装置43の通過が許可されたと解析する。

【0027】

次に、管理装置40から検査シーケンスデータ46を受け取った検査端末A41が、検査シーケンスデータ46に従い、検査パケット47（発信元アドレス：192.168.0.1 発信元ポート番号：xxx 送信先アドレス：10.0.0.1 送信先ポート番号：110）を送出する。一方で検査端末B42は、検査シーケンスデータ46に従って、検査端末A41から送られてくるはずの検査パケット47を決められた時間待ち受ける。図5のフィルタリングルールにより、検査パケット47はファイアウォールを通過できない。その後、時間内に検査端末B42が検査パケット47を受信出来なかった場合には、検査端末B42はファイアウォール装置43によって検査パケット47が通過を許可されずに遮断された（非通過）と判断し、その判断を記録する。

【0028】

以上のようにして、検査端末A41が、図4に示されている検査シーケンスデータ46のパケットを全て送出し終わると、管理装置40は、管理端末44に、発信元IPアドレス：192.168.0.1、発信元ポート番号：xxx、送信先アドレス：10.0.0

10

20

30

40

50

． 1、送信先ポート番号：80のパケットは、ファイアウォール装置43を通過し、発信元IPアドレス：192.168.0.1、発信元ポート番号：xxx、送信先IPアドレス：10.0.0.1、送信先ポート番号：110のパケットは、ファイアウォール装置を通過しなかったという報告を管理端末44に送信して、管理端末44で、結果表示が行われる。また、管理装置40は、利用者が入力したフィルタリングルール45と実際に検査した結果が異なっている場合には、その点についても結果報告に含めて利用者に通知する。

【0029】

尚、ファイアウォール装置43における検査パケットの通過・非通過の解析は、検査端末B42で行って、解析結果を管理装置に送信してもよい。

10

【0030】

続いて、図5及び図6を用いて、本実施形態の動作について説明する。図5は、本実施形態に係るファイアウォール検査方法を示したシーケンス図である。また、図6は、本実施形態に係る装置及び端末での処理を示した処理フロー図である。

【0031】

尚、下記ステップは、管理装置40に記録されたプログラム(p0)、検査端末Aに記録されたプログラム(p1)、検査端末Bに記録されたプログラム(p2)を実行することで、行うことができる。

【0032】

まず、図6に示すように、利用者が管理端末44の画面に表示されたGUI(Graphical User Interface)を使って、検査対象となるファイアウォール装置43のフィルタリングルール45(図3)を入力する(ステップS1)。これにより、図5に示すように、入力データが管理装置40に送られる。

20

【0033】

次に、管理装置40は、フィルタリングルール45に基づいて、検査シーケンスデータ46(図4)を作成する。ここで作成される検査シーケンスデータ45は、複数のシーケンスを含むものであるが、それぞれの検査パターンは1組のパケットに関するやり取りしか示されておらず、正常なTCP, ICMP, UDPのプロトコルシーケンスに沿ったものとなっている。

【0034】

次に、図5及び図6に示すように、管理装置40は、検査端末A41、検査端末B42に、上記作成された検査シーケンスデータ45を送信して、配布する(ステップS3)。

30

【0035】

次に、図6に示すように、検査端末A41は、上記受信した検査シーケンスデータ46を検査シーケンスデータ記憶部161に記憶すると共に、検査端末B42と検査開始の同期を取るための検査開始信号を検査端末B42に送信する(ステップS4)。この検査シーケンスデータ記憶部161は、検査端末A41内の不図示のHD(Hard Disk)の一部領域に構築されている。同様に、検査端末B42は、上記受信した検査シーケンスデータ46を検査シーケンスデータ記憶部162に記憶する(ステップS5)。この検査シーケンスデータ記憶部162は、検査端末B42内の不図示のHDの一部領域に構築されている。

40

【0036】

次に、検査端末A41では、検査シーケンスデータ記憶部161に記憶した検査シーケンスデータ46の内容(検査シーケンスデータ46で示されている送信元IPアドレス及び送信先IPアドレスの指定)に従い、ファイアウォール装置43を介して検査端末B42に検査パケット47を送信する(ステップS6)。

【0037】

次に、検査端末B42では、図5に示すように、検査シーケンスデータ記憶部162に記憶した検査シーケンスデータ46の内容に従い、検査端末A41から送信されてきた検査開始信号を受信したことを契機とした所定時間内に、検査パケット47を受信するか否かを判断する(ステップS7)。そして、検査パケット47を所定時間内に受信したと判断

50

した場合には（ＹＥＳ）、検査シーケンスデータで示されているＩＰアドレスを使って、検査パケット４７を受信したことを検査端末Ａ４１に通知するための応答パケットを、ファイアウォール装置４３を介して検査端末Ａ４１に送信する（ステップＳ８）。

【００３８】

一方、検査端末Ａ４１では、上記ステップＳ６によって検査パケット４７を送信したことを契機とした所定時間内に、上記応答パケット４８を受信するか否かを判断する（ステップＳ９）。そして、所定時間内に応答パケット４８を受信したと判断した場合には（ＹＥＳ）、その旨を示す受信結果を受信結果記録部１５１に記録し、その後、この受信結果を検査結果データ４９として管理装置４０に送信することで、受信結果を管理装置４０に通知する（ステップＳ１０）。また、上記ステップＳ９において、所定時間内に応答パケット４８を受信しなかったと判断した場合には（ＮＯ）、その旨を示す受信結果を受信結果記録部１５１に記録し、その後、この受信結果を検査結果データ４９として管理装置４０に送信することで、受信結果を管理装置４０に通知する（ステップＳ１１）。尚、受信結果記録部１５１は、検査端末Ａ４１内の不図示のＨＤの一部領域に構築されている。

10

【００３９】

一方、検査端末Ｂ４２では、上記ステップＳ８により、検査パケット４７を受信した場合には、その旨を示す受信結果を受信結果記録部１５２に記録し、その後、この受信結果を検査結果データ５０として管理装置４０に送信することで、受信結果を管理装置４０に通知する（ステップＳ１２）。また、上記ステップＳ７において、所定時間内に検査パケット４７を受信しなかったと判断した場合には（ＮＯ）、その旨を示す受信結果を受信結果記録部１５２に記録し、その後、この受信結果を検査結果データ５０として管理装置４０に送信することで、受信結果を管理装置４０に通知する（ステップＳ１３）。尚、受信結果記録部１５２は、検査端末Ｂ４２内の不図示のＨＤの一部領域に構築されている。

20

【００４０】

一方、検査端末Ａ４１では、上記ステップＳ１０，１１後に、検査シーケンスデータ記憶部１６１内をチェックして、まだ検査シーケンスデータが残っているか否かを判断する（ステップＳ１４）。そして、まだ残っていると判断した場合には（ＹＥＳ）、上記ステップＳ６へ進んで同じ処理を繰り返し、もう残っていないと判断した場合には（ＮＯ）、受信結果記録部１５１内にこれまで記録された受信結果を検査結果データ４９として、管理装置４０に送信する（ステップＳ１６）。

30

【００４１】

一方、検査端末Ｂ４２では、上記ステップＳ１２，１３後に、検査シーケンスデータ記憶部１６２内をチェックして、まだ検査シーケンスデータが残っているか否かを判断する（ステップＳ１５）。そして、まだ残っていると判断した場合には（ＹＥＳ）、上記ステップＳ７へ進んで同じ処理を繰り返し、もう残っていないと判断した場合には（ＮＯ）、受信結果記録部１５２内にこれまで記録された受信結果を検査結果データ５０として、管理装置４０に送信する（ステップＳ１７）。尚、上記ステップＳ６，Ｓ７へ進んで同じ処理を繰り返す場合には、図５に示すように、検査パケット４７'及び応答パケット４８'の送受信を再び行う。

【００４２】

次に、管理装置４０は、検査端末Ａ６１と検査端末Ｂ６３から受け取った、検査結果データ（ＩＰアドレス、ポート番号の組に対するパケットの通過状況等）４９，５０を精査し、特定のＩＰアドレス、ポート番号の組に対するファイアウォール装置４３のフィルタリングルールの設定が、利用者が入力したポリシ通りか否かを解析し、この結果報告データ５１を管理端末４４に送信して、管理端末４４で解析結果を表示する（ステップＳ１８）。これにより、例えば、検査結果データ５０が所定時間内に検査パケット４７を受信しなかった旨の受信結果である場合には、ファイアウォール装置４３によって検査パケット４７の通過が阻まれたと解析することができる。

40

【００４３】

以上説明したように本実施形態によれば、内部ネットワーク内で検査端末Ａ４１，Ｂ４２

50

によってファイアウォール装置 4 3 を挟むと共に、管理装置 4 0 から、内部ネットワーク 1 0 0 とは別の管理用ネットワーク 2 0 0 を介して、検査端末 A 4 1, B 4 2 に対して検査シーケンスデータ 4 6 と検査結果データ 4 9, 5 0 の送受信を行い、しかも、検査端末 B 4 2 で所定時間だけ検査パケット 4 7 の到着を待っているため、ファイアウォール装置 4 3 で検査パケット 4 7 が阻止されたのか、或いは、検査端末 B 4 2 で検査パケット 4 7 が阻止されたのかを認識することができる。これにより、ファイアウォール装置 4 3 のフィルタリングルールのうちパケットを通過させない設定になっている部分の検査を正確に行うことができるという効果を奏する。

【0044】

尚、本実施形態において、検査端末 A 4 1 で、送信元 IP アドレスを任意のアドレスに設定し、送信元 IP アドレスを任意に設定して、任意の送信元 IP アドレスと任意の送信先 IP アドレスを組み合わせた検査パケットを送出することによって、全ての IP アドレスの組に対するファイアウォール装置 4 3 のフィルタリングルールの検査を実施することができる。相手先の IP アドレスを実際に利用しているホストが、内部ネットワーク上に存在していない場合には、IP の仕様により arp (Address Resolution Protocol) アドレスの解決が出来ないためにパケットが送出されないという問題があるが、この方法を採用すれば、検査対象となっている IP アドレスが内部ネットワーク上で利用されているか否かを検査端末 B 4 2 が認識しており、利用されていない IP アドレスに関するファイアウォール装置 4 3 のフィルタリングルールの検査を行う場合には、検査端末 B 4 2 の IP アドレスを検査対象の利用されていない IP アドレスに自動的に変更して検査を実施することにより、内部ネットワーク上で利用されていないアドレスに関するファイアウォール装置 4 3 のフィルタリングルールの検査を行うことが可能である。

【0045】

即ち、検査端末 A 4 1 からファイアウォール装置 4 3 を挟んで反対側に、特定の IP アドレスを使っているホストコンピュータが実在しない場合でも、全てのパケットを取得することができ、しかも、検査端末 A 4 1, B 4 2 が検査シーケンスデータ 4 6 を共有しているため、検査端末 B 4 2 では、検査端末 A 4 1 から送られてくる検査パケットの種類と数を正確に知ることができる。このため、全ての IP アドレスの組の検査パケットによりファイアウォール装置 4 3 で通過許可、非許可の検査を行うことができるという効果を奏する。

〔第 2 の実施形態〕

以下、図 7 乃至図 1 1 を用いて、本発明の第 2 の実施形態について説明する。

【0046】

尚、上記第 1 の実施形態と同一構成、同一処理、同一機能等については、同一の符号を付して、その説明を省略する。

【0047】

本実施形態は、ステートフルファイアウォール装置にも使用することができる例を示したものである。そのため、まず、図 7 及び図 8 を用い、ステートフルファイアウォール装置について説明する。

【0048】

図 7 に示すように、特定のパケット 2 0 3 が検査端末 A から検査端末 B 宛に送信されたときに、ステートフルファイアウォール装置でパケット 2 0 3 の通過が拒否される場合であっても、図 8 に示すように、まず通過可能な特定のパケット 2 0 1 を送信し、その応答パケット 2 0 2 がステートフルファイアウォール装置を通過すると、ステートフルファイアウォール装置内部で自動的にパケット 2 0 3 を通過させるようにフィルタリングルールが変更される。ステートフルファイアウォール装置は、このような高度なフィルタリングルールを記述することが可能なファイアウォール装置である。

【0049】

次に、図 9 乃至図 1 1 を用いて、本実施形態の内容について説明する。

【0050】

図9は、ファイアウォール検査システム1'におけるデータ等の流れを示した概略構成図である。

【0051】

本実施形態は、検査シーケンスデータ46'に、検査端末A41、B42の計算機資源の許す限りのパケットのやり取りに関するデータを記述することによって、ステートフルファイアウォール装置43'の検査も実施できるものである。

【0052】

上記第1の実施形態では、検査端末A41、B42間の1往復のパケットの通過した状態でのファイアウォールにおける検査パケットの通過、非通過だけでなく、図10に示すように複数のパケットのやり取りに関して記述されているシーケンスを複数持つ検査シーケンスデータ46'を用いることによって、単一若しくは多数のパケットが通過した後の状態でのステートフルファイアウォール装置43'における検査パケット47の通過、非通過に関する状態も正確に認識することができる。

10

【0053】

続いて、図11を用いて、本実施形態の動作について説明する。

【0054】

まず、本実施形態におけるステップS21～S33は、上記第1の実施形態におけるステップS1～S13とそれぞれ同じ処理を行う。但し、検査シーケンスデータ46'が、利用者により入力されたステートフルファイアウォール装置43'用のフィルタリングルール45'に従って、図10に示すような内容になっている。この検査シーケンスデータ46'は、検査シーケンスデータを構成する複数のシーケンスの中に、更に、様々な検査パケットを送信するためのパケット情報が含まれている。

20

【0055】

そして、検査端末A41では、ステップS30、S31の後に、検査シーケンスデータ記憶部161に記憶されている検査シーケンスデータ46'を参照して、検査パケットが残っているか否かを判断する(ステップS34)。この判断の結果、検査パケットが残っている場合には(N O)、ステップS26に戻って処理を繰り返す。また、検査パケットが残っておらず、シーケンス中のパケットが全て処理し終わった場合には(Y E S)、ステップS36に進む。

【0056】

一方、検査端末B42においても、ステップS32、S33の後に、検査シーケンスデータ記憶部162に記憶されている検査シーケンスデータ46'を参照して、検査パケットが残っているか否かを判断する(ステップS35)。この判断の結果、検査パケットが残っている場合には(N O)、ステップS27に戻って処理を繰り返す。また、検査パケットが残っておらず、シーケンス中のパケットが全て処理し終わった場合には(Y E S)、ステップS37に進む。

30

【0057】

そして、その後のステップS36～S40は、上記第1の実施形態におけるステップS14～S18とそれぞれ同じ処理を行う。

【0058】

以上説明したように本実施形態によれば、上記第1の実施形態の効果に加え、更に、図10に示すように、検査シーケンスデータ46'は、検査シーケンスデータを構成する複数のシーケンスの中に、更に、様々な検査パケットを送信するためのパケット情報が含まれているため、過去の通信状態を加味してパケットの通過の可否を決定するような高度なフィルタリングルールを持ったステートフルファイアウォール装置43'の検査も行うことができるという効果を奏する。

40

【0059】

尚、第1及び第2の実施形態では、図1に示すように、1つの管理装置40によって一組の検査端末A、Bを管理しているが、一組、二組、或いは、四組以上の検査端末A、Bを管理してもよい。

50

【0060】

また、第1及び第2の実施形態では、検査端末A、Bの2台を一組としてが、これに限るものではなく、3台、或いは4台以上の検査端末を一組として、同じ内部ネットワーク100内で、様々な検査を行うようにしてもよい。更に、第1及び第2の実施形態においては、TCP、UDP、ICMPパケットにおける各種パラメータを任意の値に設定した検査パケットを送信してもよい。これにより、通常のやり取りでは生成されないパラメータを有したTCP、UDP、ICMPを検査パケットとして生成して、異常なパラメータを有したTCP、UDP、ICMPパケットがファイアウォール装置43、43'の通過を許可されるか否かを検査することが出来る。異常なパラメータとして設定できる項目例を表1に示している。

10

【0061】

【表1】

プロトコル	パラメータ名
I P	バージョン
	ヘッダ長
	T O S
	データ長
	識別子
	フラグ
	オフセット
	T T L
	プロトコル
	I Pヘッダチェックサム
U D P	発信元ポート番号
	発信先ポート番号
	UDPデータ長
	UDPデータ長チェックサム
T C P	発信元ポート番号
	発信先ポート番号
	シーケンス番号
	確認応答番号
	ヘッダ長
	T C Pフラグ
	ウインドウサイズ
	T C Pチェックサム

20

30

40

また、上記プログラム(p0)、(p1)、(p2)が記録されたCD-ROM等の記録媒体を用いて、コンピュータ(管理装置、検査端末A41、B42)に、それぞれプログラム(p0)、(p1)、(p2)を記録して使用してもよい。

【0062】

【発明の効果】

以上説明したように本発明によれば、内部ネットワーク内で第1及び第2の検査端末によってファイアウォール装置を挟むと共に、管理装置から、内部ネットワークとは別の管理用ネットワークを介して、第1及び第2の検査端末に対して検査シーケンスデータと検査結果データの送受信を行い、しかも、第2の検査端末で所定時間だけ検査パケットの到着

50

を待っているため、ファイアウォール装置で検査パケットが阻止されたのか、或いは、第2の検査端末で検査パケットが阻止されたのかを認識することができる。これにより、ファイアウォール装置のフィルタリングルールのうちパケットを通過させない設定になっている部分の検査を正確に行うことができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明に係るファイアウォール検査システム1、1'の全体構成図。

【図2】第1の実施形態に係るファイアウォール検査システム1におけるデータ等の流れを示した概略構成図。

【図3】図2中のファイアウォール装置43のフィルタリングルールを示した図。

【図4】第1の実施形態に係る検査シーケンスデータの内容を示した図。

10

【図5】第1の実施形態に係るファイアウォール検査方法を示したシーケンス図。

【図6】第1の実施形態に係る装置及び端末での処理を示した処理フロー図。

【図7】ステートフルファイアウォール装置の説明に使用する図。

【図8】ステートフルファイアウォール装置の説明に使用する図。

【図9】第2の実施形態に係るファイアウォール検査システム1におけるデータ等の流れを示した概略構成図。

【図10】第2の実施形態に係る検査シーケンスデータの内容を示した図。

【図11】第2の実施形態に係る装置及び端末での処理を示した処理フロー図。

【図12】従来のファイアウォール検査システムにおけるデータ等の流れを示した概略構成図。

20

【符号の説明】

40 管理装置

41 検査端末A

42 検査端末B

43 ファイアウォール装置

44 管理端末

45 フィルタリングルール

46 検査シーケンスデータ

47 検査パケット

48 応答パケット

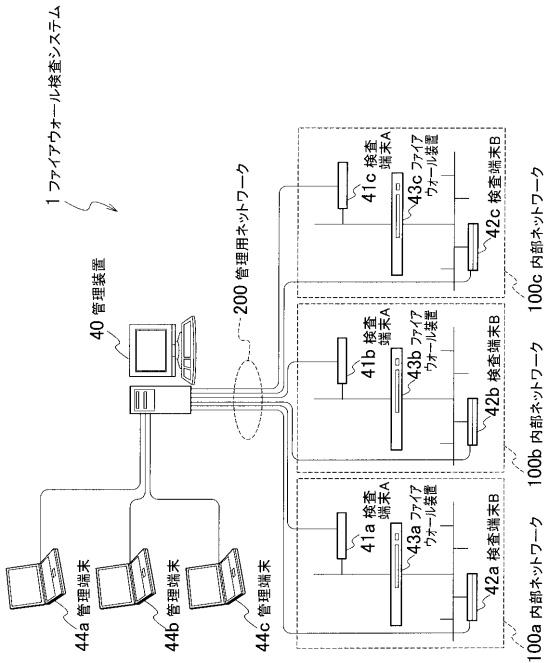
49 検査結果データ

50 検査結果データ

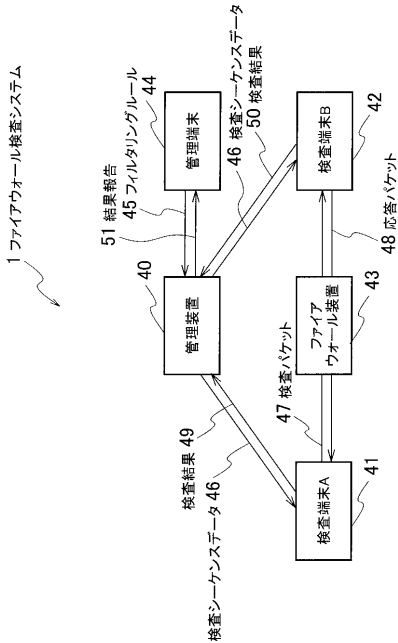
51 結果報告

30

【図 1】



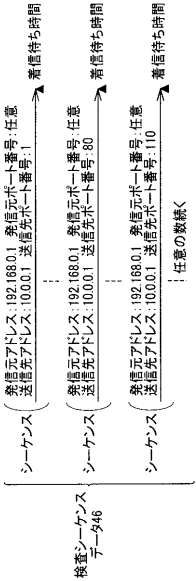
【図 2】



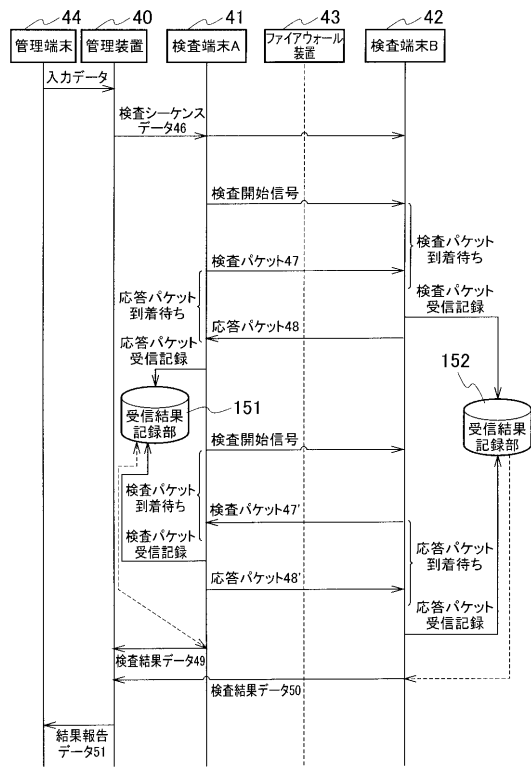
【図 3】

ルール番号	発信元 IP アドレス	宛信元ポート番号	送信先 IP アドレス	送信先ポート番号	ポリシー	コメント
1	192.168.0.1	any	100.0.1	80	通過許可	web 設定
2	any	any	any	110	通過非許可	POP 禁止

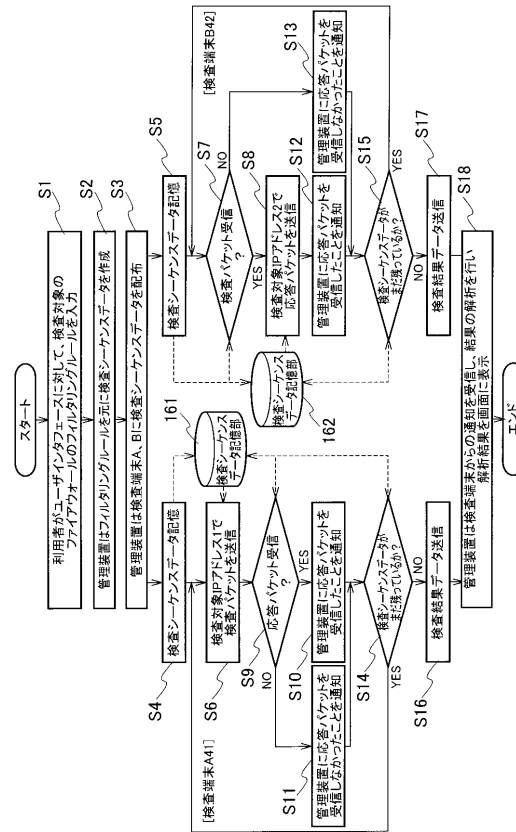
【図 4】



【図 5】



【図 6】



【図 7】



【図 8】



フロントページの続き

- (56)参考文献 特開平10-285165 (JP, A)
特開2000-151602 (JP, A)
特開2003-198624 (JP, A)
特開2001-237895 (JP, A)
特開2002-016644 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/66

G06F 13/00

H04L 12/56