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

特許第4341517号
(P4341517)

(45)発行日　平成21年10月7日(2009.10.7)　(24)登録日　平成21年7月17日(2009.7.17)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560B
G06Q 10/00	(2006.01)	G06F	12/14	520A
H04L 12/24	(2006.01)	G06F	17/60	174
		G06F	17/60	512
		H04L	12/24	

請求項の数 25　(全 87 頁)

(21)出願番号　特願2004-283160 (P2004-283160)
(22)出願日　平成16年9月29日 (2004.9.29)
(65)公開番号　特開2006-40247 (P2006-40247A)
(43)公開日　平成18年2月9日 (2006.2.9)
審査請求日　平成16年9月29日 (2004.9.29)
(31)優先権主張番号　特願2004-182214 (P2004-182214)
(32)優先日　平成16年6月21日 (2004.6.21)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103090
弁理士　岩壁　冬樹
(74)代理人　100124501
弁理士　塩川　誠人
(72)発明者　岡城　純孝
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　松田　勝志
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】セキュリティポリシー管理システム、セキュリティポリシー管理方法およびプログラム

(57)【特許請求の範囲】

【請求項１】

管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を記憶する設定情報記憶手段と、

前記設定情報記憶手段に記憶された設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する汎用セキュリティポリシー生成手段とを備え、

前記汎用セキュリティポリシー生成手段は、

セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報記憶手段に記憶された設定情報の記述仕様に関する知識を用いて、前記設定情報記憶手段に記憶された設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、

設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述する

ことを特徴とするセキュリティポリシー管理システム。

【請求項２】

管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力し、前記設定情報を設定情報記憶手段に記憶させる設定情報入力手段を備えた

請求項１に記載のセキュリティポリシー管理システム。
【請求項３】
管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力する設定情報入力手段と、
前記設定情報入力手段が入力した設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する汎用セキュリティポリシー生成手段とを備え、
前記汎用セキュリティポリシー生成手段は、
セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報入力手段が入力した設定情報の記述仕様に関する知識を用いて、前記設定情報入力手段が入力した設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、
設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述する
ことを特徴とするセキュリティポリシー管理システム。
【請求項４】
設定情報を入力するための設定情報入力サブルーチンを機器毎に記憶する設定情報入力サブルーチン記憶手段を備え、
設定情報入力手段は、設定情報の収集対象となる機器毎に設定情報入力サブルーチンを読み込み、前記設定情報入力サブルーチンに従って、前記設定情報を入力する
請求項２または請求項３に記載のセキュリティポリシー管理システム。
【請求項５】
設定情報の収集対象となる機器を備え、
前記機器は、当該機器の設定情報を抽出し、設定情報入力手段に送信する設定情報送信手段を含む
請求項２または請求項３に記載のセキュリティポリシー管理システム。
【請求項６】
特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成するためのセキュリティポリシー生成サブルーチンを機器毎に記憶するセキュリティポリシー生成サブルーチン記憶手段を備え、
汎用セキュリティポリシー生成手段は、設定情報入力手段が入力した設定情報に基づいて、前記設定情報を保持する機器に対応するセキュリティポリシー生成サブルーチンを前記セキュリティポリシー生成サブルーチン記憶手段から読み込み、前記セキュリティポリシー生成サブルーチンに従って前記セキュリティポリシーを生成する
請求項２から請求項５のうちのいずれか１項に記載のセキュリティポリシー管理システム。
【請求項７】
汎用セキュリティポリシー生成手段によって生成されるセキュリティポリシーの内容を分析する際に用いられる情報を記憶する分析知識データベースと、
前記分析知識データベースが記憶する情報を用いて、設定情報に基づいて生成されたセキュリティポリシーの内容を分析するセキュリティポリシー分析手段とを備えた
請求項１から請求項６のうちのいずれか１項に記載のセキュリティポリシー管理システム。
【請求項８】
汎用セキュリティポリシー生成手段によって生成されるセキュリティポリシーの内容を分析するためのセキュリティポリシー分析サブルーチンをセキュリティ機能毎に記憶するセキュリティポリシー分析サブルーチン記憶手段を備え、
セキュリティポリシー分析手段は、セキュリティ機能毎にセキュリティポリシー分析サブルーチンを前記セキュリティポリシー分析サブルーチン記憶手段から読み込み、前記セ

キュリティポリシー分析サブルーチンに従って、汎用セキュリティポリシー生成手段によって生成されたセキュリティポリシーの内容を分析する
請求項７に記載のセキュリティポリシー管理システム。
【請求項９】
セキュリティポリシー分析手段が同一のセキュリティ機能に関するセキュリティポリシーの分析結果を複数生成した場合に、前記分析結果を比較することにより、セキュリティポリシー分析手段によって分析された機器毎のセキュリティポリシーの相違点を特定するセキュリティポリシー比較手段を備えた
請求項７または請求項８に記載のセキュリティポリシー管理システム。
【請求項１０】
セキュリティポリシー分析手段による分析結果を比較するための比較サブルーチンをセキュリティ機能毎に記憶する比較サブルーチン記憶手段を備え、
セキュリティポリシー比較手段は、セキュリティ機能毎に比較サブルーチンを前記比較サブルーチン記憶手段から読み込み、前記比較サブルーチンに従って、分析結果を比較し、セキュリティポリシー分析手段によって分析された機器毎のセキュリティポリシーの相違点を特定する
請求項９に記載のセキュリティポリシー管理システム。
【請求項１１】
セキュリティ機能に関するセキュリティポリシーの分析結果を予め記憶する分析結果記憶手段と、
セキュリティポリシー分析手段がセキュリティポリシーの分析結果を少なくとも一つ生成した場合に、分析結果記憶手段が記憶する分析結果と、前記セキュリティポリシー分析手段によって生成された分析結果とを比較するセキュリティポリシー比較手段とを備えた
請求項７または請求項８に記載のセキュリティポリシー管理システム。
【請求項１２】
セキュリティポリシー分析サブルーチン記憶手段は、セキュリティポリシーに記述されているパケットの送信元の情報、パケットの宛先の情報、プロトコル情報、およびパケットを通過させるか否かを示す情報とに基づいて、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を特定するためのセキュリティポリシー分析サブルーチンを、パケットフィルタリング機能に対応するセキュリティポリシー分析サブルーチンとして記憶し、
セキュリティポリシー分析手段は、前記セキュリティポリシー分析サブルーチンに従って、セキュリティポリシー内のパケットフィルタリング機能のルールの優先度が低い方から順に、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を特定していき、優先度が高い方の特定結果を優先させる
請求項８から請求項１１のうちのいずれか１項に記載のセキュリティポリシー管理システム。
【請求項１３】
セキュリティポリシー分析手段による分析結果を出力する出力手段を備え、
セキュリティポリシー分析手段は、前記出力手段に、パケットの送信元の情報がとり得る値およびパケットの宛先の情報がとり得る値のいずれか一方を横軸として表し、他方を縦軸として表す二次元領域上に、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を表した図を表示させる
請求項１２に記載のセキュリティポリシー管理システム。
【請求項１４】
セキュリティポリシー分析手段による分析結果を出力する出力手段を備え、
セキュリティポリシー分析手段は、前記出力手段に、パケットの送信元の情報がとり得る値を表す軸を第一の軸とし、パケットの宛先の情報がとり得る値を表す軸を第二の軸とし、パケットを通過可能とするパケットの送信元の情報を第一の軸上に表し、パケットを通過可能とするパケットの宛先の情報を第二の軸上に表した図を表示させる

請求項１２に記載のセキュリティポリシー管理システム。
【請求項１５】
セキュリティポリシー分析手段が同種のセキュリティ機能に関するセキュリティポリシーの分析結果を複数生成した場合に、前記複数の分析結果に対する分析をさらに行って、複数のセキュリティポリシー全体としての分析結果を導出するセキュリティポリシー統合手段を備えた
請求項７または請求項８に記載のセキュリティポリシー管理システム。
【請求項１６】
セキュリティ機能に関するセキュリティポリシーの分析結果を予め記憶する分析結果記憶手段と、
セキュリティポリシー分析手段がセキュリティポリシーの分析結果を少なくとも一つ生成した場合に、前記分析結果記憶手段が記憶する分析結果および前記セキュリティポリシー分析手段によって生成された分析結果に対する分析を行い、これらのセキュリティポリシー全体としての分析結果を導出するセキュリティポリシー統合手段を備えた
請求項７または請求項８に記載のセキュリティポリシー管理システム。
【請求項１７】
複数の分析結果に対する分析をさらに行うための統合サブルーチンをセキュリティ機能毎に記憶する統合サブルーチン記憶手段を備え、
セキュリティポリシー統合手段は、セキュリティ機能毎に統合サブルーチンを前記統合サブルーチン記憶手段から読み込み、前記統合サブルーチンに従って、複数の分析結果に対する分析をさらに行い、複数のセキュリティポリシー全体としての分析結果を導出する
請求項１５または請求項１６に記載のセキュリティポリシー管理システム。
【請求項１８】
セキュリティポリシー統合手段は、パケットフィルタリングを行う複数の機器の設定情報に基づいて生成された各セキュリティポリシーの分析結果に対する分析をさらに行い、前記複数の機器を全て通過可能なパケットを特定する
請求項１５から請求項１７のうちのいずれか１項に記載のセキュリティポリシー管理システム。
【請求項１９】
異なるセキュリティ機能を有する複数の機器の設定情報に基づいて生成された各セキュリティポリシーまたは前記セキュリティポリシーの分析結果を参照して、前記複数の機器の設定情報に基づいて生成された各セキュリティポリシーを関連付けるセキュリティポリシー連携手段を備えた
請求項７または請求項８に記載のセキュリティポリシー管理システム。
【請求項２０】
異なるセキュリティ機能を有する複数の機器の設定情報に基づいて生成された各セキュリティポリシーを関連付けるための連携サブルーチンを、前記異なるセキュリティ機能の組み合わせ毎に記憶する連携サブルーチン記憶手段を備え、
セキュリティポリシー連携手段は、セキュリティ機能の組み合わせに対応する連携サブルーチンを前記連携サブルーチン記憶手段から読み込み、前記連携サブルーチンに従って、前記各セキュリティポリシーを関連付ける
請求項１９に記載のセキュリティポリシー管理システム。
【請求項２１】
セキュリティポリシー連携手段は、異なるセキュリティ機能を有する複数の機器の設定情報に基づいて生成された各セキュリティポリシーの不整合箇所を特定する
請求項１９または請求項２０に記載のセキュリティポリシー管理システム。
【請求項２２】
設定情報記憶手段が、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を記憶し、
汎用セキュリティポリシー生成手段が、前記設定情報記憶手段に記憶された設定情報に

基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成し、
前記セキュリティポリシーを生成する際に、前記汎用セキュリティポリシー生成手段が、セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報記憶手段に記憶された設定情報の記述仕様に関する知識を用いて、前記設定情報記憶手段に記憶された設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述する
ことを特徴とするセキュリティポリシー管理方法。
【請求項２３】
設定情報入力手段が、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力し、
汎用セキュリティポリシー生成手段が、前記設定情報入力手段が入力した設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成し、
前記セキュリティポリシーを生成する際に、前記汎用セキュリティポリシー生成手段が、セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報入力手段が入力した設定情報の記述仕様に関する知識を用いて、前記設定情報入力手段が入力した設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述する
ことを特徴とするセキュリティポリシー管理方法。
【請求項２４】
管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を記憶する設定情報記憶手段を備えたコンピュータに、
前記設定情報記憶手段に記憶された設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する処理を実行させ、
前記セキュリティポリシーを生成する処理で、
セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報記憶手段に記憶された設定情報の記述仕様に関する知識を用いて、前記設定情報記憶手段に記憶された設定情報に含まれる表記から導出させ、前記内容を記述することにより前記セキュリティポリシーを生成させ、
設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述させる
ためのセキュリティポリシー管理プログラム。
【請求項２５】
コンピュータに、
管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力する処理、および
入力された設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する処理を実行させ、
前記セキュリティポリシーを生成する処理で、
セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、入力された前

記設定情報の記述仕様に関する知識を用いて、入力された前記設定情報に含まれる表記から導出させ、前記内容を記述することにより前記セキュリティポリシーを生成させ、
設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述させる
ためのセキュリティポリシー管理プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は情報システムの構成要素であるセキュリティ機器の設定内容からセキュリティポリシーを導くセキュリティポリシー管理システム、セキュリティポリシー管理方法、およびセキュリティポリシー管理プログラムに関する。

【背景技術】

【０００２】

情報技術の発達とともに情報セキュリティの重要性が増大している。そこで現在、組織のネットワークシステムにおけるセキュリティに関する設定状況からセキュリティポリシーを構築し、管理者がセキュリティポリシーを把握できるようにすることが求められている。セキュリティポリシーを把握できるようにする技術として、特許文献１に記載された状況把握方法がある。特許文献１に記載された状況把握方法は、団体のメンバーに対して質問を行い、その質問の回答に基づき情報システムのセキュリティ状況を把握するステップと、調査ツールによる調査結果に基づき情報システムのセキュリティ状況を把握するステップと、この２つのステップでそれぞれ得られた情報を統合してセキュリティポリシーを構築するステップとを含んでいる。

【０００３】

また、特許文献１に記載された状況把握方法に用いられる統合装置は、質問の回答による情報システムの状況（第１状況）と、調査ツールによる情報システムの状況（第２状況）とを比較し、整合していない不整合部分を整合している整合部分から分離して取り出し、不整合部分を表示する。そして、利用者に対してこの不整合に対する利用者の選択入力を促し、利用者が選択した結果を表示し、整合部分と利用者が選択した結果とを合成する。このように特許文献１に記載の方法や装置では、質問だけでなく調査ツールを用いているため、調査ツールを用いて調べることができる事項に関しては、質問を行う必要がなくなる。また、不整合部分を表示し利用者に選択を促すことができるので、表示された内容から妥当な選択をすることができ、より適切なセキュリティポリシーを構築することが可能となる。

【０００４】

【特許文献１】特開２００３－２０３１４０号公報　（第５－７頁、図１）

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかし、従来の方法や装置では、セキュリティ管理者の経験や知識、組織の構成員に対する質問の回答結果に基づいてセキュリティポリシーが構築されている。そのため、従来のセキュリティポリシーの構築には、人手を介することによる課題が存在している。

【０００６】

第１に、セキュリティポリシーの構築や把握に多大な労力と時間が必要であるという問題がある。セキュリティポリシーは個々の組織ごとに構築する必要があり、また、セキュリティ管理者が経験や知識に基づいて一から作成したり、組織の構成員に対する質問の回答を集計しなければならない。また、既存のセキュリティ機器の設定情報は、個々のセキュリティ機器に固有の書式で記述されている。さらに、セキュリティ機器毎に暗黙の了解として一部の情報の記述が省略されている場合がある。そのような設定情報から導かれたセキュリティポリシーには、統一性ががなく、人手による修正や整理を行わなければ、セキュリティポリシーを把握しづらい。この結果、セキュリティポリシーの構築や把握に多

くの労力や時間が必要になってしまう。

【０００７】

第２に、セキュリティポリシーの構築やセキュリティ状況の把握において、誤りや漏れが生じる可能性が高いという問題がある。この理由は、セキュリティポリシーの構築の過程で、人手が介在することによって、セキュリティ管理者や質問の回答者の思い込みや勘違いに起因する誤りや漏れが生じる可能性があるためである。

【０００８】

また、特許文献１に記載の方法では、情報システムのセキュリティ状況を調査する調査ツールとして、スキャナが挙げられている。しかし、このような調査ツールでは調査対象のセキュリティ機器に実際に設定されている内容とは異なる誤った情報が収集される可能性がある。

【０００９】

また、セキュリティポリシーを構築した場合、そのセキュリティポリシーの内容を分かり易く管理者に提示できることが好ましい。さらに、異なる複数のシステムのセキュリティポリシーを比較できることが好ましい。また、異なる複数のシステムのセキュリティポリシーに限らず、セキュリティポリシー同士を比較できることが好ましい。例えば、一つのシステムのセキュリティポリシーと、予め定められた基準となるセキュリティポリシーとの比較も行えることが好ましい。

【００１０】

また、同じ種類の複数のセキュリティポリシーを統合的に分析できることが好ましい。例えば、パケットフィルタリングを行う機器が複数存在する場合、各機器からそれぞれ把握されるセキュリティポリシーを分析して、パケットフィルタリングを行う各機器を全て通過可能なパケットを特定できるようにすることが好ましい。

【００１１】

また、相異なる機能についての設定を定めたセキュリティポリシー等を連携させて、その関連性を把握できることが好ましい。例えば、パケットフィルタリング機能についての設定を定めたセキュリティポリシーと、侵入検知機能についての設定の分析結果とを連携させて、各設定の不整合の有無を判定する等の処理を行えることが好ましい。

【００１２】

そこで、本発明は、できるだけ管理者等の人間による作業を減らして、管理者に把握しやすいセキュリティポリシーを生成することができるセキュリティポリシー管理装置、セキュリティポリシー管理方法、セキュリティポリシー管理プログラムを提供することを目的とする。また、生成したセキュリティポリシーを分かり易く提示することができるセキュリティポリシー管理装置、セキュリティポリシー管理方法、セキュリティポリシー管理プログラムを提供することを目的とする。また、異なる複数のシステムのセキュリティポリシーを比較したり、セキュリティポリシー同士を比較したりすることができるセキュリティポリシー管理装置、セキュリティポリシー管理方法、セキュリティポリシー管理プログラムを提供することを目的とする。また、同じ種類の複数のセキュリティポリシーを統合的に分析できるセキュリティポリシー管理装置、セキュリティポリシー管理方法、セキュリティポリシー管理プログラムを提供することを目的とする。また、相異なる機能についての設定を定めたセキュリティポリシー等を連携させて、その関連性を把握できるセキュリティポリシー管理装置、セキュリティポリシー管理方法、セキュリティポリシー管理プログラムを提供することを目的とする。

【課題を解決するための手段】

【００１３】

本発明によるセキュリティポリシー管理システムは、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を記憶する設定情報記憶手段と、前記設定情報記憶手段に記憶された設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する汎用セキュリティポリシー生成手段とを備え、前記汎用セキュリティポリシー生成手段が、

セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報記憶手段に記憶された設定情報の記述仕様に関する知識を用いて、前記設定情報記憶手段に記憶された設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述することを特徴とする。そのような構成によれば、生成されたセキュリティポリシーは、特定の機器に依存する記述とは独立した書式で表現された記述を含むので、そのセキュリティポリシーの内容の把握が容易になる。また、汎用セキュリティポリシー生成手段が、設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成するので、設定情報に基づくセキュリティポリシーの生成を、人手を介さずに自動的に行うことができる。その結果、システム管理者等の作業者による思いこみや勘違いを排除し、セキュリティポリシーの記述の誤りや漏れを極めて低減させることができる。また、短時間で正確にセキュリティポリシーを生成することができる。

【００１４】

管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力し、前記設定情報を設定情報記憶手段に記憶させる設定情報入力手段を備えた構成であってもよい。

【００１５】

また、本発明によるセキュリティポリシー管理システムは、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力する設定情報入力手段と、前記設定情報入力手段が入力した設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する汎用セキュリティポリシー生成手段とを備え、前記汎用セキュリティポリシー生成手段が、セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報入力手段が入力した設定情報の記述仕様に関する知識を用いて、前記設定情報入力手段が入力した設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述することを特徴とする。そのような構成によれば、生成されたセキュリティポリシーは、特定の機器に依存する記述とは独立した書式で表現された記述を含むので、そのセキュリティポリシーの内容の把握が容易になる。また、汎用セキュリティポリシー生成手段が、設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成するので、設定情報に基づくセキュリティポリシーの生成を、人手を介さずに自動的に行うことができる。その結果、システム管理者等の作業者による思いこみや勘違いを排除し、セキュリティポリシーの記述の誤りや漏れを極めて低減させることができる。また、短時間で正確にセキュリティポリシーを生成することができる。

【００１６】

設定情報を入力するための設定情報入力サブルーチンを機器毎に記憶する設定情報入力サブルーチン記憶手段を備え、設定情報入力手段は、設定情報の収集対象となる機器毎に設定情報入力サブルーチンを読み込み、前記設定情報入力サブルーチンに従って、前記設定情報を入力する構成であってもよい。そのような構成によれば、設定情報入力サブルーチン記憶手段が、設定情報入力サブルーチンを機器毎に記憶するので、設定情報入力サブルーチン記憶手段に新たな設定情報入力サブルーチンを追加記憶させることで、新たに追加された機器からも設定情報を入力することができる。

【００１７】

設定情報の収集対象となる機器を備え、前記機器は、当該機器の設定情報を抽出し、設

定情報入力手段に送信する設定情報送信手段を含むように構成されていてもよい。

【００１８】

特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成するためのセキュリティポリシー生成サブルーチンを機器毎に記憶するセキュリティポリシー生成サブルーチン記憶手段を備え、汎用セキュリティポリシー生成手段は、設定情報入力手段が入力した設定情報に基づいて、前記設定情報を保持する機器に対応するセキュリティポリシー生成サブルーチンを前記セキュリティポリシー生成サブルーチン記憶手段から読み込み、前記セキュリティポリシー生成サブルーチンに従って前記セキュリティポリシーを生成する構成であってもよい。そのような構成によれば、セキュリティポリシー生成サブルーチン記憶手段が、セキュリティポリシー生成サブルーチンを機器毎に記憶するので、セキュリティポリシー生成サブルーチン記憶手段に新たなセキュリティポリシー生成サブルーチンを追加記憶させることで、新たに追加された機器に応じたセキュリティポリシーを生成することができる。

【００１９】

汎用セキュリティポリシー生成手段によって生成されるセキュリティポリシーの内容を分析する際に用いられる情報を記憶する分析知識データベースと、前記分析知識データベースが記憶する情報を用いて、設定情報に基づいて生成されたセキュリティポリシーの内容を分析するセキュリティポリシー分析手段とを備えた構成であってもよい。そのような構成によれば、セキュリティポリシー分析手段がセキュリティポリシーの内容を分析するので、管理者は、セキュリティポリシーの内容ををより把握しやすくなる。

【００２０】

汎用セキュリティポリシー生成手段によって生成されるセキュリティポリシーの内容を分析するためのセキュリティポリシー分析サブルーチンをセキュリティ機能毎に記憶するセキュリティポリシー分析サブルーチン記憶手段を備え、セキュリティポリシー分析手段は、セキュリティ機能毎にセキュリティポリシー分析サブルーチンを前記セキュリティポリシー分析サブルーチン記憶手段から読み込み、前記セキュリティポリシー分析サブルーチンに従って、汎用セキュリティポリシー生成手段によって生成されたセキュリティポリシーの内容を分析する構成であってもよい。そのような構成によれば、セキュリティポリシー分析サブルーチン記憶手段が、セキュリティポリシー分析サブルーチンをセキュリティ機能毎に記憶するので、セキュリティ機能単位で、セキュリティポリシーの内容を分析することができる。また、セキュリティポリシー分析サブルーチン記憶手段に新たなセキュリティポリシー分析サブルーチンを追加記憶させることで、新たなセキュリティ機能に応じた分析を行うことができる。

【００２１】

セキュリティポリシー分析手段が同一のセキュリティ機能に関するセキュリティポリシーの分析結果を複数生成した場合に、前記分析結果を比較することにより、セキュリティポリシー分析手段によって分析された機器毎のセキュリティポリシーの相違点を特定するセキュリティポリシー比較手段を備えた構成であってもよい。そのような構成によれば、セキュリティポリシー比較手段が、機器毎のセキュリティポリシーの相違点を特定するので、同一のセキュリティ機能を持つ異機種のセキュリティ機器間、あるいは複数の同機種のセキュリティ機器間で、設定情報から導出されたセキュリティポリシーの内容が異なっているか否かを判断できる。

【００２２】

セキュリティポリシー分析手段による分析結果を比較するための比較サブルーチンをセキュリティ機能毎に記憶する比較サブルーチン記憶手段を備え、セキュリティポリシー比較手段は、セキュリティ機能毎に比較サブルーチンを前記比較サブルーチン記憶手段から読み込み、前記比較サブルーチンに従って、分析結果を比較し、セキュリティポリシー分析手段によって分析された機器毎のセキュリティポリシーの相違点を特定する構成であってもよい。そのような構成によれば、比較サブルーチン記憶手段が、比較サブルーチンをセキュリティ機能毎に記憶するので、比較サブルーチン記憶手段に新たな比較サブルーチ

ンを追加記憶させることで、新たなセキュリティ機能に応じた分析結果の比較を行うことができる。

【００２３】

セキュリティ機能に関するセキュリティポリシーの分析結果を予め記憶する分析結果記憶手段と、セキュリティポリシー分析手段がセキュリティポリシーの分析結果を少なくとも一つ生成した場合に、分析結果記憶手段が記憶する分析結果と、前記セキュリティポリシー分析手段によって生成された分析結果とを比較するセキュリティポリシー比較手段とを備えた構成であってもよい。

【００２４】

セキュリティポリシー分析サブルーチン記憶手段は、セキュリティポリシーに記述されているパケットの送信元の情報、パケットの宛先の情報、プロトコル情報、およびパケットを通過させるか否かを示す情報とに基づいて、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を特定するためのセキュリティポリシー分析サブルーチンを、パケットフィルタリング機能に対応するセキュリティポリシー分析サブルーチンとして記憶し、セキュリティポリシー分析手段は、前記セキュリティポリシー分析サブルーチンに従って、セキュリティポリシー内のパケットフィルタリング機能のルールの優先度が低い方から順に、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を特定していき、優先度が高い方の特定結果を優先させる構成であってもよい。そのような構成によれば、分析結果として、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を得ることができる。

【００２５】

セキュリティポリシー分析手段による分析結果を出力する出力手段を備え、セキュリティポリシー分析手段は、前記出力手段に、パケットの送信元の情報がとり得る値およびパケットの宛先の情報がとり得る値のいずれか一方を横軸として表し、他方を縦軸として表す二次元領域上に、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を表した図を表示させる構成であってもよい。そのような構成によれば、セキュリティポリシー分析手段が、パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報を表した図を表示させるので、分析結果（パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報）を分かり易く提示することができる。

【００２６】

セキュリティポリシー分析手段による分析結果を出力する出力手段を備え、セキュリティポリシー分析手段は、前記出力手段に、パケットの送信元の情報がとり得る値を表す軸を第一の軸とし、パケットの宛先の情報がとり得る値を表す軸を第二の軸とし、パケットを通過可能とするパケットの送信元の情報を第一の軸上に表し、パケットを通過可能とするパケットの宛先の情報を第二の軸上に表した図を表示させる構成であってもよい。そのような構成によれば、セキュリティポリシー分析手段が、パケットを通過可能とするパケットの送信元の情報を第一の軸上に表し、パケットを通過可能とするパケットの宛先の情報を第二の軸上に表した図を表示させるので、分析結果（パケットを通過可能とするパケットの送信元の情報およびパケットの宛先の情報）を分かり易く提示することができる。

【００２７】

セキュリティポリシー分析手段が同種のセキュリティ機能に関するセキュリティポリシーの分析結果を複数生成した場合に、前記複数の分析結果に対する分析をさらに行って、複数のセキュリティポリシー全体としての分析結果を導出するセキュリティポリシー統合手段を備えた構成であってもよい。そのような構成によれば、複数のセキュリティポリシー全体としての分析結果を管理者に提供することができる。

【００２８】

セキュリティ機能に関するセキュリティポリシーの分析結果を予め記憶する分析結果記憶手段と、セキュリティポリシー分析手段がセキュリティポリシーの分析結果を少なくとも一つ生成した場合に、前記分析結果記憶手段が記憶する分析結果および前記セキュリテ

ィポリシー分析手段によって生成された分析結果に対する分析を行い、これらのセキュリティポリシー全体としての分析結果を導出するセキュリティポリシー統合手段を備えた構成であってもよい。

【００２９】

複数の分析結果に対する分析をさらに行うための統合サブルーチンをセキュリティ機能毎に記憶する統合サブルーチン記憶手段を備え、セキュリティポリシー統合手段は、セキュリティ機能毎に統合サブルーチンを前記統合サブルーチン記憶手段から読み込み、前記統合サブルーチンに従って、複数の分析結果に対する分析をさらに行い、複数のセキュリティポリシー全体としての分析結果を導出する構成であってもよい。そのような構成によれば、統合サブルーチン記憶手段が、統合サブルーチンをセキュリティ機能毎に記憶するので、統合サブルーチン記憶手段に新たな統合サブルーチンを追加記憶させることで、新たなセキュリティ機能に応じた統合的な分析を行うことができる。

【００３０】

セキュリティポリシー統合手段は、パケットフィルタリングを行う複数の機器の設定情報に基づいて生成された各セキュリティポリシーの分析結果に対する分析をさらに行い、前記複数の機器を全て通過可能なパケットを特定する構成であってもよい。

【００３１】

異なるセキュリティ機能を有する複数の機器の設定情報に基づいて生成された各セキュリティポリシーまたは前記セキュリティポリシーの分析結果を参照して、前記複数の機器の設定情報に基づいて生成された各セキュリティポリシーを関連付けるセキュリティポリシー連携手段を備えた構成であってもよい。そのような構成によれば、各セキュリティポリシーを関連付けた結果を管理者に提供することができる。

【００３２】

異なるセキュリティ機能を有する複数の機器の設定情報に基づいて生成された各セキュリティポリシーを関連付けるための連携サブルーチンを、前記異なるセキュリティ機能の組み合わせ毎に記憶する連携サブルーチン記憶手段を備え、セキュリティポリシー連携手段が、セキュリティ機能の組み合わせに対応する連携サブルーチンを前記連携サブルーチン記憶手段から読み込み、前記連携サブルーチンに従って、前記各セキュリティポリシーを関連付ける構成であってもよい。そのような構成によれば、連携サブルーチン記憶手段が、異なるセキュリティ機能の組み合わせ毎に連携サブルーチンを記憶するので、連携サブルーチン記憶手段に新たな連携サブルーチンを追加記憶させることで、新たなセキュリティ機能の組み合わせに応じたセキュリティポリシーの関連付けを行うことができる。

【００３３】

セキュリティポリシー連携手段は、異なるセキュリティ機能を有する複数の機器の設定情報に基づいて生成された各セキュリティポリシーの不整合箇所を特定する構成であってもよい。

【００３４】

また、本発明によるセキュリティポリシー管理方法は、設定情報記憶手段が、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を記憶し、汎用セキュリティポリシー生成手段が、前記設定情報記憶手段に記憶された設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成し、前記セキュリティポリシーを生成する際に、前記汎用セキュリティポリシー生成手段が、セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報記憶手段に記憶された設定情報の記述仕様に関する知識を用いて、前記設定情報記憶手段に記憶された設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述することを特徴とする。

【００３５】

また、本発明によるセキュリティポリシー管理方法は、設定情報入力手段が、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力し、汎用セキュリティポリシー生成手段が、前記設定情報入力手段が入力した設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成し、前記セキュリティポリシーを生成する際に、前記汎用セキュリティポリシー生成手段が、セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報入力手段が入力した設定情報の記述仕様に関する知識を用いて、前記設定情報入力手段が入力した設定情報に含まれる表記から導出し、前記内容を記述することにより前記セキュリティポリシーを生成し、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述することを特徴とする。

【００３６】

また、本発明によるセキュリティポリシー管理プログラムは、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を記憶する設定情報記憶手段を備えたコンピュータに、前記設定情報記憶手段に記憶された設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する処理を実行させ、前記セキュリティポリシーを生成する処理で、セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、前記設定情報記憶手段に記憶された設定情報の記述仕様に関する知識を用いて、前記設定情報記憶手段に記憶された設定情報に含まれる表記から導出させ、前記内容を記述することにより前記セキュリティポリシーを生成させ、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述させることを特徴とする。

【００３７】

また、本発明によるセキュリティポリシー管理プログラムは、コンピュータに、管理対象となるネットワークシステムに含まれる機器のセキュリティ機能に関する設定を定めた設定情報を入力する処理、および入力された設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する処理を実行させ、前記セキュリティポリシーを生成する処理で、セキュリティ機能を有する機器の動作としてモデル化され、前記セキュリティポリシーで記述される項目の集合として表現されたモデルにおける各項目の内容を、入力された前記設定情報の記述仕様に関する知識を用いて、入力された前記設定情報に含まれる表記から導出させ、前記内容を記述することにより前記セキュリティポリシーを生成させ、設定情報で省略されている場合にはデフォルト値を記述すると定められた項目については、設定情報で省略されている場合に前記デフォルト値を記述させることを特徴とする。

【発明の効果】

【００３８】

本発明によれば、設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する汎用セキュリティポリシー生成手段を備えた構成である。従って、生成されたセキュリティポリシーは、特定の機器に依存する記述とは独立した書式で表現された記述を含むので、そのセキュリティポリシーの内容の把握が容易になる。また、汎用セキュリティポリシー生成手段が、設定情報に基づいて、特定の機器に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成するので、設定情報に基づくセキュリティポリシーの生成を、人手を介さずに自動的に行うことができる。その結果、システム管理者等の作業者による思いこみや勘違いを排除し、セキュリティポリシーの記述の誤りや漏れを極めて低減させることができる。また、短時間で正確にセキュリティポリシーを生成することができる。

【発明を実施するための最良の形態】

【００３９】
次に、本発明を実施するための最良の形態について図面を参照して詳細に説明する。
【００４０】
実施の形態１.
図１は、本発明によるセキュリティポリシー管理システムの第１の実施の形態を示すブロック図である。図１に示すセキュリティポリシー管理システムは、プログラムに従って動作するコンピュータであるデータ処理装置１００と、情報の入出力を行う入出力手段１１０とを備えている。入出力手段１１０は、例えば、キーボードやマウス等の入力装置およびディスプレイ装置等の出力装置を含んでいる。
【００４１】
また、セキュリティ機器１３０は、例えば、ある組織が利用するネットワークシステム（図示せず。）の構成要素となる機器のうち、セキュリティ機能を有する機器である。このネットワークシステムは、システム管理者の管理対象となる。ネットワークシステムの構成要素となる各機器は、通信ネットワーク１２０を介して接続されている。ネットワークシステムは少なくとも一つのセキュリティ機器１３０を含み、通信ネットワーク１２０には少なくとも一つのセキュリティ機器１３０が接続されている。データ処理装置１００は、通信ネットワーク１２０を介してセキュリティ機器１３０と接続される。各セキュリティ機器１３０は、その機器が有するセキュリティ機能に関する設定を定めた設定情報を保持している。設定情報は、例えば、ハードウェアによって実現されるセキュリティ機能に関する設定を定めたものであってもよい。また、セキュリティ機器１３０に搭載されたソフトウェアによって実現されるセキュリティ機能に関する設定を定めた設定情報も、セキュリティ機器１３０の設定情報である。設定情報は、個々のセキュリティ機器１３０毎に固有の書式で定められている。
【００４２】
データ処理装置１００は、設定情報抽出手段１０１と、汎用セキュリティポリシー生成手段１０３とを含む。設定情報抽出手段１０１および汎用セキュリティポリシー生成手段１０３は、例えば、プログラムに従って動作するＣＰＵによって実現される。また、プログラムには、サブルーチンとして、少なくとも１つの設定情報抽出サブルーチン１０２および少なくとも１つのセキュリティポリシー生成サブルーチン１０４が含まれる。個々の設定情報抽出サブルーチン１０２は、それぞれが個々のセキュリティ機器１３０と一対一に対応する。また、個々のセキュリティポリシー生成サブルーチン１０４は、それぞれが個々のセキュリティ機器１３０と一対一に対応する。
【００４３】
設定情報抽出手段１０１は、通信ネットワーク１２０に接続されているセキュリティ機器１３０のうち少なくとも１つのセキュリティ機器１３０から設定情報を抽出、収集する。このとき、設定情報抽出手段１０１は、設定情報を抽出しようとするセキュリティ機器に対応する設定情報抽出サブルーチン１０２を呼び出し、その設定情報抽出サブルーチン１０２に従ってセキュリティ機器から設定情報を抽出、収集する。この設定情報は、設定情報の収集対象となったセキュリティ機器に固有のものである。
【００４４】
汎用セキュリティポリシー生成手段１０３は、設定情報抽出手段１０１により収集された設定情報から、設定情報の収集対象としたセキュリティ機器の動作に応じて定められるセキュリティポリシーを生成する。汎用セキュリティポリシー生成手段１０３は、このセキュリティポリシーを生成するときに、特定のセキュリティ機器１３０に依存する記述とは独立した書式で表現された記述を含むセキュリティポリシーを生成する。「特定のセキュリティ機器１３０に依存する記述とは独立した書式」とは、換言すれば、特定のセキュリティ機器１３０に依存しない書式である。汎用セキュリティポリシー生成手段１０３によって生成されるセキュリティポリシーは、セキュリティ機器１３０に依存する記述とは独立した書式で表現された記述を含んでいるので、以下の説明では、このセキュリティポリシーを汎用セキュリティポリシーと記す。

【００４５】
なお、汎用セキュリティポリシーは、セキュリティ機器１３０に依存する記述とは独立した書式で表現された記述のみを含んでいてもよい。また、汎用セキュリティポリシーは、特定のセキュリティ機器１３０に依存する記述を部分的に含んでいてもよい。
【００４６】
また、汎用セキュリティポリシー生成手段１０３は、設定情報の収集対象としたセキュリティ機器に対応するセキュリティポリシー生成サブルーチン１０４を呼び出し、そのセキュリティポリシー生成サブルーチン１０４に従って汎用セキュリティポリシーを生成する。このように、汎用セキュリティポリシー生成手段１０３は、セキュリティ機器単位に汎用セキュリティポリシーを生成する。
【００４７】
なお、各セキュリティ機器１３０に対応する設定情報抽出サブルーチン１０２およびセキュリティポリシー生成サブルーチン１０４は、データ処理装置１００が備える記憶装置（図１において図示せず。）に予め記憶させておく。記憶装置（図１において図示せず。）に記憶されている各サブルーチンを読み込むことを、「呼び出す」と記す。
【００４８】
また、セキュリティ機器１３０に設定情報が存在するということは、既にセキュリティポリシーが作成され、そのセキュリティポリシーに従って設定がなされていることになる。本発明では、セキュリティ機器１３０に依存しない書式で記述された汎用セキュリティポリシーを、既に存在するセキュリティポリシーとは別に新たに生成する。
【００４９】
次に、セキュリティ機器およびその機能について説明する。セキュリティ機器１３０の例として、例えば、ファイアウォール、ＷＷＷサーバ、ＦＴＰ（File Transfer Protocol）サーバ、スーパーサーバ、ロギングソフトウェアを搭載した機器等がある。また、これらのセキュリティ機器１３０が有するセキュリティ機能の例として、例えば、パケットフィルタリング機能、アドレス変換機能、ＵＲＬフィルタリング機能（有害Ｗｅｂページの閲覧を禁止する等の機能）、ウィルスチェック機能（ＦＴＰを使ってダウンロードするファイルに対してウィルスチェックを行う等の機能）、コンテンツスクリーニング機能（Ｗｅｂページのうち Ｊａｖａスクリプト（登録商標）やＡｃｔｉｖｅＸによる表示部分を表示しないようにする等の機能）、認証機能、ログ出力機能、アクセス制御機能等がある。ここに例示したセキュリティ機器１３０やセキュリティ機能は、例示であり、セキュリティ機器１３０やセキュリティ機能はここに挙げたものに限定されない。
【００５０】
セキュリティ機器１３０が保持する設定情報には、セキュリティに関するルールが含まれている。一つのルールは、一つのセキュリティ機能に関する記述のみで表される場合もあれば、複数のセキュリティ機能に関する記述で表される場合もある。例えば、「アドレスＡからアドレスＢに送信されるパケットは破棄する。」というルールは、一つのセキュリティ機能（本例ではパケットフィルタリング機能）に関する記述のみで表される。また、例えば、「アドレスＡからアドレスＢに送信されるパケットは通過させるが、Ｊａｖａスクリプトによる表示部分は表示させない。」というルールは、二つのセキュリティ機能（本例ではパケットフィルタリング機能およびコンテンツスクリーニング機能）に関する記述によって表される。設定情報では、個々のルールは各セキュリティ機器に固有の書式で表される。
【００５１】
次に、動作について説明する。
図２は、本実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者から汎用セキュリティポリシーの生成要求を入力される（ステップＡ１）。すると、設定情報抽出手段１０１は、ネットワークシステムに含まれる少なくとも一つのセキュリティ機器１３０について、そのセキュリティ機器１３０に対応する設定情報抽出サブルー

チン１０２を呼び出す。そして、設定情報抽出手段１０１は、その設定情報抽出サブルーチン１０２に従って、セキュリティ機器１３０から設定情報を抽出、収集する（ステップＡ２）。複数のセキュリティ機器１３０から設定情報を収集する場合には、セキュリティ機器毎に設定情報を収集する。

【００５２】

ステップＡ２の次に、汎用セキュリティポリシー生成手段１０３は、ステップＡ２で設定情報の収集対象としたセキュリティ機器に対応するセキュリティポリシー生成サブルーチン１０４を呼び出す。そして、汎用セキュリティポリシー生成手段１０３は、そのセキュリティポリシー生成サブルーチン１０４に従って、ステップＡ２で収集した設定情報から汎用セキュリティポリシーを生成する（ステップＡ３）。ステップＡ２で複数のセキュリティ機器１３０から設定情報を収集した場合には、汎用セキュリティポリシー生成手段１０３は、セキュリティ機器毎に汎用セキュリティポリシーを生成する。続いて、汎用セキュリティポリシー生成手段１０３は、ステップＡ３で生成した汎用セキュリティポリシーを入出力手段１１０から出力しシステム管理者に提示する（ステップＡ４）。例えば、汎用セキュリティポリシーをディスプレイ装置に表示させる。

【００５３】

次に、ステップＡ２の設定情報抽出収集処理について説明する。図３は、ステップＡ２の設定情報抽出収集処理の例を示すフローチャートである。ステップＡ１において汎用セキュリティポリシー生成要求が入力されると、設定情報抽出手段１０１は、設定情報の抽出、収集の対象となるセキュリティ機器を決定する（ステップＡ２０１）。設定情報抽出手段１０１は、例えば、セキュリティ機器の指定をシステム管理者に促す画面を表示し、入出力手段１１０を介して指定されたセキュリティ機器を、設定情報の抽出、収集の対象となるセキュリティ機器として決定する。あるいは、セキュリティ機器１３０を含むネットワークシステムのトポロジー情報（各機器同士の接続関係を示す情報）を予め記憶しておき、そのトポロジー情報に記述された各セキュリティ機器を選択候補として表示してシステム管理者に選択を促し、入出力手段１１０を介して指定されたセキュリティ機器を、設定情報の抽出、収集の対象となるセキュリティ機器として決定してもよい。また、設定情報抽出手段１０１は、通信ネットワーク１２０に接続されているセキュリティ機器１３０を検索し、検索されたセキュリティ機器を、設定情報の抽出、収集の対象となるセキュリティ機器として決定してもよい。セキュリティ機器１３０を検索するときには、ＳＮＭＰ（Simple Network Management Protocol）を利用すればよい。また、セキュリティ機能を実現するためのソフトウェアを搭載したセキュリティ機器を検索する場合には、セキュリティ機器に搭載されているＯＳのコマンドを利用して検索を行ってもよい。

【００５４】

次に、設定情報抽出手段１０１はステップＡ２０１で決定したセキュリティ機器に対応する設定情報抽出サブルーチン１０２を呼び出す（ステップＡ２０２）。そして、その設定情報抽出サブルーチン１０２に従って、セキュリティ機器に設定されている設定情報を抽出、取得する（ステップＡ２０３）。セキュリティ機器１３０からどのような情報を抽出すればよいのかは、各セキュリティ機器１３０に対応する設定情報抽出サブルーチンに定められている。設定情報抽出手段１０１は、ＳＮＭＰを利用したり、設定情報の収集対象として決定されたセキュリティ機器に備わっている設定情報取得コマンドを実行するなどして設定情報の抽出、収集を行う。

【００５５】

ステップＡ２０３の後、設定情報抽出手段１０１は、ステップＡ２０１で決定された全てのセキュリティ機器から設定情報を抽出、収集したか否かを判定する（ステップＡ２０４）。全てのセキュリティ機器から設定情報を抽出、収集済みであるならば、設定情報抽出収集処理（ステップＡ２）を終了する。設定情報を抽出、収集していないセキュリティ機器がまだ残っている場合には、ステップＡ２０２以降の処理を繰り返す。

【００５６】

次に、ステップＡ３の汎用セキュリティポリシー生成処理について説明する。図４は、

ステップＡ３の汎用セキュリティポリシー生成処理の例を示すフローチャートである。ステップＡ２の終了後、汎用セキュリティポリシー生成手段１０３は、ステップＡ２で収集した設定情報から、その設定情報が元々保持されていたセキュリティ機器１３０を特定するセキュリティ機器情報を取得する（ステップＡ３０１）。セキュリティ機器情報としては、セキュリティ機器の名称やバージョン情報等があり、これらの情報は設定情報の中に記述されている。汎用セキュリティポリシー生成手段１０３は、例えば、収集した設定情報に記述されているセキュリティ機器の名称やバージョン情報等のセキュリティ機器情報を取得すればよい。

【００５７】

続いて、汎用セキュリティポリシー生成手段１０３は、セキュリティ機器情報によって、どのセキュリティ機器から設定情報を収集したのかを判定し、そのセキュリティ機器に対応するセキュリティポリシー生成サブルーチン１０４を呼び出す（ステップＡ３０２）。

【００５８】

次に、汎用セキュリティポリシー生成手段１０３は、呼び出したセキュリティポリシー生成サブルーチンに従って、セキュリティ機器に固有の形式で記述された設定情報の内容を解釈し、セキュリティ機器１３０に依存しない書式で記述される汎用セキュリティポリシーを生成する（ステップＡ３０３）。セキュリティポリシー生成サブルーチン１０４は、セキュリティ機器１３０と一対一に対応するので、ステップＡ３０３では、一つのセキュリティ機器１３０の設定情報から、そのセキュリティ機器に対応する汎用セキュリティポリシーを生成する。セキュリティポリシー生成サブルーチン１０４は、対応するセキュリティ機器の設定情報の記述仕様に関する知識と、生成する汎用セキュリティポリシーのフォーマット情報（セキュリティ機器１３０に依存しない書式の情報）を含んでいる。従って、汎用セキュリティポリシー生成手段１０３は、セキュリティ機器に固有の記述仕様で記述された設定情報から汎用セキュリティポリシーを生成することができる。なお、既に説明したように、セキュリティポリシー生成サブルーチン１０４は、データ処理装置１００が備える記憶装置（図１において図示せず。）に予め記憶されている。

【００５９】

次に、ステップＡ２で収集した全ての設定情報から汎用セキュリティポリシーを生成済みか否かを判定する（ステップＡ３０４）。収集した全ての設定情報から汎用セキュリティポリシーを生成したならば、汎用セキュリティポリシー生成処理（ステップＡ３）を終了する。まだ、汎用セキュリティポリシーが生成されていない設定情報が残っている場合には、ステップＡ３０２以降の処理を繰り返す。図４に示す汎用セキュリティポリシー生成処理によって、セキュリティ機器毎に汎用セキュリティポリシーが生成される。

【００６０】

次に、ステップＡ３において生成される汎用セキュリティポリシーの記述形式について説明する。汎用セキュリティポリシーは、セキュリティ機器固有の記述形式ではなく同類のセキュリティ機器が共通して持つセキュリティ機能に基づいて抽象化された、セキュリティ機器に非依存な形式で表現される。このような記述は、セキュリティ機能を有するセキュリティ機器の動作をモデル化し、そのモデルにおけるオブジェクトやアクションを定義した上で、セキュリティ機器の設定情報（具体的には設定情報に含まれる各ルール）をオブジェクトやアクションの属性として記述することで実現することができる。セキュリティ機能の動作のモデル化を行うことで、同一のセキュリティ機能を持つような同カテゴリに属するセキュリティ機器の設定情報を、セキュリティ機器に依存しない形式で汎用的に記述可能となる。

【００６１】

図５は、セキュリティ機能の動作のモデルの例を示す説明図である。図５では、主にパケットフィルタリング等のアクセス制御を行うセキュリティ機器の動作モデルを示す。このモデルで表されるセキュリティ機器の動作は、以下の二通りの動作に集約される。第一の動作は、「InputObject で表されるオブジェクトの入力を受けて、そのオブジェクトの

通過を許可あるいは拒否する」動作である。第二の動作は、InputObject で表されるオブジェクトの入力を受けて、OutputObjectで表されるオブジェクトを出力する」動作である。また、一つのセキュリティ機器が複数のセキュリティ機能を有することがある。例えばセキュリティ機器であるファイアウォールには、パケットフィルタリング機能、認証機能、アドレス変換機能など複数の機能を有するものがある。このようなセキュリティ機器は複数のセキュリティ機能(Function)を組み合わせて動作する。

【００６２】

図５に示す動作モデルによってその動作を表現可能なセキュリティ機器として、既に例示したファイアウォール、ＷＷＷサーバ、ＦＴＰサーバ、スーパーサーバ、ロギングソフトウェアを搭載した機器等がある。そして、これらのセキュリティ機器が有するセキュリティ機能として、パケットフィルタリング機能、アドレス変換機能、ＵＲＬフィルタリング機能、ウィルスチェック機能、コンテンツスクリーニング機能、認証機能、ログ出力機能、アクセス制御機能等がある。異なるセキュリティ機器であっても動作モデルが共通であれば、共通の書式の汎用セキュリティポリシーで表される。上記の各セキュリティ機器は共通の動作モデルを持つので、共通の動作モデルを持つセキュリティ機器には依存しない汎用セキュリティポリシーで表すことができる。動作モデルが異なれば、別の書式の汎用セキュリティポリシーで表される。従って、汎用セキュリティポリシーは、共通の動作モデルを持つセキュリティ機器の集合ごとに分類される。

【００６３】

図５に示す動作モデルを持つセキュリティ機器の汎用セキュリティポリシーで記述される項目について説明する。セキュリティ機能による動作は、Function（アクセス制御を行うセキュリティ機能）、InputObject （Functionへ入力されるオブジェクト）、OutputObject （Functionから出力されるオブジェクト）、Action（Functionの動作）の組によって表現する。

【００６４】

さらに、１つのセキュリティ機能による動作を表現するFunction、InputObject、OutputObject、Actionに加え、その動作を許可するか否かを表現するeffect（とりうる値はpermitあるいはdeny）の組み合わせによって表現する。既に説明したように、各セキュリティ機器１３０に固有の書式で表された設定情報には、一つのセキュリティ機能に関する記述のみで表されるルールもあれば、複数のセキュリティ機能に関する記述で表されるルールもある。いずれのルールであっても、汎用セキュリティポリシーとして記述した場合には、各セキュリティ機能に関する記述は、Function, InputObject ,OutputObject, Action, effectの組み合わせとして表される。以下、ルールを表現するためのセキュリティ機能に関する記述を、セキュリティ機器に依存しない書式で表したものをPolicyRuleと記す。PolicyRuleは、Function, InputObject ,OutputObject, Action, effectの組み合わせとなる。

【００６５】

一般的にはアクセス制御ルールを表現するためには、subject（誰が）、resource（何に）、action（何を）、effect（許可するか否か）で表現されることが多い。しかし、セキュリティ機能の動作はこの４項目の組み合わせだけでは表現できないものも存在する。その一つの例として、アドレス変換機能による動作をあげることができる。アドレス変換機能は、ルータやゲートウェイに入ってくる特定のパケットに対して、そのパケットの送信元ＩＰアドレス（およびポート番号）や宛先ＩＰアドレス（およびポート番号）を変換し出力する機能である。このとき書き換えたアドレスの対応関係を変換テーブルに記録しておくことにより、返信されてくるパケットを変換前の正しい送信元に転送できるようにしている。アドレス変換は一般的なアクセス制御ルールでは表現することができない。しかし、各セキュリティ機能に関する記述を、Function, InputObject ,OutputObject, Action, effectの組み合わせとして表すことにより、アドレス変換機能に関する記述もPolicyRuleとして表すことができる。すなわち、汎用セキュリティポリシー内で表されるPoicyRuleにおいて、InputObject にアドレス変換前の送信元ＩＰアドレス（およびポート番号

）や宛先ＩＰアドレス（およびポート番号）を含むパケット情報を記述し、OutputObjectにアドレス変換後の送信元ＩＰアドレス（およびポート番号）や宛先ＩＰアドレス（およびポート番号）を含むパケット情報を記述し、さらにFunctionにセキュリティ機能として送信元アドレスを変更する"SNAT"や宛先アドレスを変更する"DNAT"を記述すれば、アドレス変換機能に関する記述もPolicyRuleとして記述可能である。

【００６６】

また、セキュリティ機器に依存しない書式でルールを表したものをPolicyと記す。一つのルールから一つのPolicyが生成される。一つのセキュリティ機能に関する記述のみで表されるルールを、汎用セキュリティポリシーに含まれるPolicyとして表した場合、そのPolicy内には一つのPolicyRuleが含まれる。また、複数のセキュリティ機能に関する記述で表されるルールをPolicyとして表した場合、そのPolicy内には複数のPolicyRuleが含まれる。一つのPolicyに含まれる複数のPolicyRuleの結合方法をPolicyRule結合アルゴリズムで表現する。PolicyRule結合アルゴリズムには、"ordered-deny-overrides"や"ordered-permit-overrides"がある。"ordered-deny-overrides"は、複数のPolicyRuleのうちのいずれかのeffectが"deny"と評価された場合に、その複数のPolicyRuleを含むPolicyの評価を"deny"とするPolicyRule結合アルゴリズムである。"ordered-permit-overrides"は、複数のPolicyRuleのうちのいずれかのeffectが"permit"と評価された場合に、その複数のPolicyRuleを含むPolicyの評価を"permit"とするPolicyRule結合アルゴリズムである。このPolicyRule結合アルゴリズムによって、複数のセキュリティ機能に関する記述で表されるルールも一つのPolicyとして表現できる。

【００６７】

さらに、Policyには必要に応じてCondition （Policyを適用するための条件）とObligation（Policy適用時の責務）を付加することができる。従って、汎用セキュリティポリシーでは、一つのPolicyは一つまたは複数のPolicyRuleと、Conditionと、Obligationとの組み合わせで表現されることがある。通常、一つのルールにはそのルールが有効となるための条件が付随することが多い。汎用セキュリティポリシーではこのような条件を表現できるようにPolicyにConditionを付加することができる。また、一つのルールにはそのルールを適用する際に、そのルールで記述されるセキュリティ機能による処理以外に実行しなければならない処理が責務として付随することがある。汎用セキュリティポリシーではこのような責務を表現できるようにPolicyにObligationを付加することができる。

【００６８】

一つのセキュリティ機器で設定されているルールの集合を、セキュリティ機器に依存しない書式で表したものをPolicyGroup と記す。一つのセキュリティ機器から抽出された設定情報に基づいて生成された汎用セキュリティポリシーは一つのPolicyGroup として表される。従って、各セキュリティ機器と各PolicyGroup とは一対一に対応する。一つのセキュリティ機器から抽出された設定情報の中に複数のルールが記述されていれば、PolicyGroup の中には複数のPolicyが含まれることになる。一つのPolicyGroup に含まれる複数のPolicyの結合方法をPolicy結合アルゴリズムで表現する。Policy結合アルゴリズムには、"first-applicable"や"independent "がある。"first-applicable"は、Policyの順序に重要な意味がありPolicyの適用に際してはその記述順に適用しなければならないことを表している。"independent "は、Policyの適用順序は問わないことを表している。なお、各セキュリティポリシー生成サブルーチン１０４には、対応するセキュリティ機器１３０で設定されている各ルールがPolicyとして表された場合におけるPolicy結合アルゴリズムを示すパラメータが含まれている。

【００６９】

図６および図７は、セキュリティ機器に固有の設定情報から生成される汎用セキュリティポリシーにおけるPolicyGroup , Policy, PolicyRuleの包含関係を示す説明図である。図６に示す設定情報は、アクセス制御ソフトウェアであるiptables（ソフトウェアの製品名）が搭載されたセキュリティ機器の設定情報の例である。この設定情報に、図６に示すルール１，２が記述されているとする。ルール１は、特定のＩＰアドレスから特定のＩＰ

アドレスに送信されたパケットは破棄することを規定している。このルール１は、パケットフィルタリング機能のみに関する記述を含んでいる。ルール１におけるパケットフィルタリング機能に関する記述から一つのPolicyRuleが生成される。また、一つのルールから一つのPolicyが生成される。そのため、ルール１から生成されるPolicyの中には、パケットフィルタリング機能に関する記述に対応する一つのPolicyRuleが含まれる。また、ルール２は、アドレス変換機能のみに関する記述を含んでいる。従って、ルール２から生成されるPolicyの中には、アドレス変換機能に関する記述に対応する一つのPolicyRuleが含まれる。また、iptablesが搭載された一つのセキュリティ機器の設定情報全体から、一つのPolicyGroup が生成される。このPolicyGroup は、ルール１、ルール２に対応する各Policyを含んでいる。

【００７０】

図７に示す設定情報は、別のセキュリティ機器の設定情報である。この設定情報に、図７に示すルール３～５が記述されているとする。ルール３，４は、コンテンツフィルタリングに関するルールである。ルール５は、アドレス変換に関するルールである。ルール３は、パケットフィルタリング機能のみに関する記述を含んでいる。従って、ルール３から生成されるPolicyの中には、パケットフィルタリング機能に関する記述に対応する一つのPolicyRuleが含まれる。

【００７１】

また、ルール４は、パケットフィルタリング機能に関する記述と、コンテンツスクリーニング機能に関する記述を含んでいる。このようなルールとして、例えば、「アドレスＡからアドレスＢに送信されるパケットは通過させるが、Ｊａｖａスクリプトによる表示部分は表示させない。」等が挙げられる。このルールには、「アドレスＡからアドレスＢに送信されるパケットは通過させる。」というパケットフィルタリング機能に関する記述と、「Ｊａｖａスクリプトによる表示部分は表示させない。」というコンテンツスクリーニング機能に関する記述とが含まれている。ルール４から生成されるPolicyの中には、パケットフィルタリング機能に関する記述に対応する一つのPolicyRuleと、コンテンツスクリーニング機能に関する記述に対応する一つのPolicyRuleが含まれる。

【００７２】

また、ルール５は、アドレス変換機能のみに関する記述を含んでいる。従って、ルール５から生成されるPolicyの中には、アドレス変換機能に関する記述に対応する一つのPolicyRuleが含まれる。また、この設定情報全体から、一つのセキュリティ機器に対応する一つのPolicyGroup が生成される。このPolicyGroup は、ルール３～５に対応する各Policyを含んでいる。

【００７３】

図８および図９は、汎用セキュリティポリシーをＸＭＬ文書で表した場合の書式の例を示す説明図である。図９に示す記述は、図８に示す記述の続きである。図８および図９に示す書式は例であり、汎用セキュリティポリシーの書式は図８および図９に示す書式に限定されるわけではない。

【００７４】

PolicySet タグに囲まれた範囲は、図５に示したようなある一つの共通の動作モデルを持つ各セキュリティ機器に対応するPolicyGroup の集合を示す。policySetType 属性は、共通の動作モデルを持つセキュリティ機器のセキュリティポリシーのタイプを表す名前である。汎用セキュリティポリシー生成手段１０３がpolicySetType 属性を付加する。

【００７５】

PolicyGroupタグに囲まれた範囲は、設定情報を取得したセキュリティ機器単位のルールの集合を示す。policyGroupID 属性は他のPolicyGroup と区別するための識別子であり、汎用セキュリティポリシー生成手段１０３がPolicyGroup 生成時に付加する。policyGroupID 属性値の決定に際して、セキュリティ機器の名称やセキュリティ機器に対してシステム管理者が一意に決めた名前などを用いてシステム管理者にとって分かりやすい値を決定してもよい。また、target属性はセキュリティ機器の種別を表し、汎用セキュリティポリ

シー生成手段１０３がPolicyGroup 生成時に付加する。

【００７６】

policyCombiningAlg属性は、Policyを評価する際のPolicy結合アルゴリズムを表し、汎用セキュリティポリシー生成手段１０３がPolicyGroup 生成時に付加する。policyCombiningAlg属性が"first-applicable"であるならば、PolicyGroup に含まれる各Policyを先頭から順に評価することを示している。policyCombiningAlg属性が"independent"であるならば、PolicyGroup に含まれる各Policyを評価する際にその順序を問わないことを示している。

【００７７】

Policyタグに囲まれた範囲は、セキュリティ機器の設定情報に含まれていた一つ一つのルールを表す。一組のPolicyタグに囲まれた範囲は、例えば「送信元Ａから宛先Ｂへ向かうパケットの通過を許可する。」等の一つのルールを表す。policyID属性は他のPolicyと区別するための識別子であり、汎用セキュリティポリシー生成手段１０３がPolicy生成時に付加する。policyID属性値の決定に際しても、policyGroupID 属性値の決定時と同様に、システム管理者にとって分かりやすい値を決定してもよい。

【００７８】

policyRuleCombiningAlg属性は、Policyの子要素として記述されるPolicyRuleを評価する際のPolicyRule結合アルゴリズムを表す。汎用セキュリティポリシー生成手段１０３は、設定情報に応じてpolicyRuleCombiningAlg属性の値を決定する。policyRuleCombiningAlg属性が"ordered-deny-overrides"であるということは、PolicyRuleを順に評価していき、いずれかのPolicyRuleの評価がdenyとなったならば、これらPolicyRuleの集合であるPolicyの評価がdenyになることを意味する。この場合、すべてのPolicyRuleの評価がpermitとなったときにはPolicyの評価はPermitとなる。policyRuleCombiningAlg属性が"ordered-permit-overrides"であるということは、PolicyRuleを順に評価していき、いずれかのPolicyRuleの評価がpermitとなったならば、これらPolicyRuleの集合であるPolicyの評価がpermitになることを意味する。この場合、すべてのPolicyRuleの評価がdenyになるとPolicyの評価はdenyとなる。

【００７９】

PolicyRuleは、ルールを表現するためのセキュリティ機能に関する記述を表す。policyRuleID属性は他のPolicyRuleと区別するための識別子であり、汎用セキュリティポリシー生成手段１０３がPolicyRule生成時に付加する。policyRuleID属性値の決定に際しては、セキュリティ機器が有するセキュリティ機能（Function）の名前を用いてシステム管理者にとって分かりやすい値を決定してもよい。effect属性は、評価対象のオブジェクトとPolicyRuleに記述される後述のInputObject とが一致し、このPolicyRuleが有効と評価された場合におけるPolicyRuleの適用の可否を表す。effect属性がpermitであるならば適用許可を表し、denyであるならば適用拒否を表す。effect属性をpermitとするかdenyとするかは、汎用セキュリティポリシー生成手段１０３が設定情報に応じて決定する。

【００８０】

Targetタグに囲まれた範囲は、PolicyRuleとなるFunction（セキュリティ機能）、InputObject （セキュリティ機器への入力）、Action（セキュリティ機器の動作）、およびOutputObject（セキュリティ機器からの出力）の組み合わせを表す。

【００８１】

InputObject はオブジェクトの型をその子要素に持ち、さらにそのオブジェクトの属性を孫要素に持つ。子要素の例として、パケットを表すPacketがある。また 、孫要素の例として、パケットの送信元ＩＰアドレスを表すSrcIP 、送信元ポートを表すSrcPort 、プロトコルを表すProtocol 、宛先ＩＰアドレスを表すDestIP、宛先ポートを表すDestPort 等がある。

【００８２】

Functionタグに囲まれた範囲は、セキュリティ機能を表す。Actionタグに囲まれた範囲には、Functionで指定されたセキュリティ機能に対応する動作を表す。例えば、Function

タグに囲まれた範囲でパケットフィルタリング機能が指定されている場合には、Actionタグに囲まれた範囲に"accept"、"deny"、"reject"等が記述される。なお、"deny"は、単にパケットを破棄することを意味する。"reject"は、パケットを破棄し、破棄したことを送信元に伝えることを意味する。なお、これらの記述は、"accept"、"deny"、"reject"等の記述に限定されるわけではない。例えば、"deny"を用いずに、"drop"という記述を用いてもよい。

【００８３】

OutputObjectは、InputObject と同様にオブジェクトの型とその属性を持つ。

【００８４】

Condition タグに囲まれた範囲は、個々のルールを適用するための条件を表す。例えば、「午前８時３０分から午後５時まで」等のようにルールを適用可能な時間に関する条件等が記述される。Obligationタグに囲まれた範囲は、ルールを適用する際に実行しなければならない責務を表す。例えば、「ルール適用時には同時にログを記録する」等の責務が記述される。Condition やObligationの内容は、汎用セキュリティポリシー生成手段１０３が設定情報に応じて決定する。

【００８５】

次に、一つのセキュリティ機器１３０に対応する汎用セキュリティポリシー生成処理（ステップＡ３０３）について説明する。図１０は、このステップＡ３０３の処理の例を示すフローチャートである。

【００８６】

既に説明したように、各セキュリティポリシー生成サブルーチン１０４には、対応するセキュリティ機器１３０で設定されている各ルールがPolicyとして表された場合におけるPolicy結合アルゴリズムを示すパラメータが含まれている。汎用セキュリティポリシー生成手段１０３は、ステップＡ３０１で取得したセキュリティ機器情報（例えば、セキュリティ機器の名称やバージョン情報等）に基づいて呼び出したセキュリティポリシー生成サブルーチン１０４において定められているパラメータからPolicy結合アルゴリズムを判定する（ステップＡ３０３２）。また、パラメータによらずに、設定情報の記述内容に応じて、Policy結合アルゴリズムを判定してもよい。

【００８７】

また、各セキュリティポリシー生成サブルーチン１０４には、対応するセキュリティ機器の設定情報の記述仕様に関する知識が含まれている。汎用セキュリティポリシー生成手段１０３は、呼び出したセキュリティポリシー生成サブルーチン１０４に含まれている設定情報の記述仕様に関する知識に基づいて、そのセキュリティポリシー生成サブルーチン１０４に対応するセキュリティ機器１３０から抽出した設定情報をルール単位（Policy単位）に分割する（ステップＡ３０３３）

【００８８】

次に、汎用セキュリティポリシー生成手段１０３は、設定情報の記述仕様に関する知識を用いて、ステップＡ３０３３で分割された個々の設定情報からFunction、InputObject、OutputObject、Action、effect、Condition 、Obligation、PolicyRule結合アルゴリズムをそれぞれ判定する（ステップＡ３０３４）。このとき、ステップＡ３０３３でルール単位に分割された情報の中に、複数のセキュリティ機能に関する記述がある場合、各セキュリティ機能に関する記述毎に、Function, InputObject ,OutputObject, Action, effectの組み合わせを導出する。

【００８９】

次に、汎用セキュリティポリシー生成手段１０３は、ステップＡ３０３４においてセキュリティ機器に固有の設定情報から導出した各項目（Function、InputObject 、OutputObject、Action、effect、Condition 、Obligation、PolicyRule結合アルゴリズム）を用いて、セキュリティ機器に非依存な記述形式である汎用セキュリティポリシーのPolicy部分を一つ生成する（ステップＡ３０３５）。このとき、Function, InputObject ,OutputObject, Action, effectの組み合わせをPolicyRuleとし、生成するPolicy内にそのPolicyRul

eを記述する。また、Function, InputObject ,OutputObject, Action, effectの組み合わせが複数導出された場合には、生成するPolicy内に複数のPolicyRuleを記述する。汎用セキュリティポリシー生成手段１０３は、PolicyRuleと、PolicyRule結合アルゴリズムと、導出されている場合にはCondition とObligationとを組み合わせて一つのPolicyとする。

【００９０】

次に、汎用セキュリティポリシー生成手段１０３は、ステップＡ３０３３でルール毎に分割した各情報からそれぞれPolicyを生成したか否かを判定する（ステップＡ３０３６）。また、ルール毎に分割した情報の中にPolicyを生成していないものがあれば（ステップＡ３０３６のＮ）、その情報についてステップＡ３０３４以降の処理を行う。ルール毎に分割したそれぞれの情報からPolicyを生成したのであれば（ステップＡ３０３６のＹ）、生成された全てのPolicyと、ステップＡ３０３２で判定したPolicy結合アルゴリズムとを組み合わせてPolicyGroup を生成する（ステップＡ３０３７）。このPolicyGroup は、一つのセキュリティ機器１３０の設定情報を、セキュリティ機器に依存しない書式で表したものである。

【００９１】

再び、ステップＡ３０２に移行して別のセキュリティポリシー生成サブルーチン１０４を呼び出した場合には、そのセキュリティポリシー生成サブルーチン１０４に従って、別のセキュリティ機器に対応するPolicyGroup が生成される。新たに生成されたPolicyGroup は、図８および図９に示すようにPoilcySet タグに囲まれた範囲内に追加される。

【００９２】

このように汎用セキュリティポリシーでは、図５に示されるような共通の動作モデルを持つセキュリティ機器の動作を、機能ごとにFunction（機能）、InputObject（セキュリティ機器への入力）、OutputObject（セキュリティ機器からの出力）、Action（セキュリティ機能における動作）の組み合わせからなるPolicyRuleで表現する。さらにFunctionごとに有効となるInputObject、OutputObject、Actionの種類を定義することにより、同一のFunctionを持つセキュリティ機器について共通のフォーマットで汎用的に表現することが可能である。

【００９３】

また複数のPolicyRuleをPolicyRule結合アルゴリズムで束ねたものをPolciyとして表現することで、複数のセキュリティ機能を組み合わせて表現される設定情報内のルールも、汎用的に表現可能である。さらに、一つのPolicyGroup 内にPolicyが複数存在する場合にその順序関係の有無もPolicy結合アルゴリズムを用いて表現可能である。

【００９４】

また、汎用セキュリティポリシー生成手段１０３は、セキュリティ機器ごとにセキュリティポリシー生成サブルーチン１０４に従い、各セキュリティ機器の設定記述の仕様に基づいて汎用セキュリティポリシー内で記述する項目（Function、InputObject 、OutputObject、Action、effect、Condition 、Obligation、PolicyRule結合アルゴリズム等）の内容を判定する。そして、それらの項目を用いて汎用セキュリティポリシーを生成する。従って、個々のセキュリティ機器に固有な記述形式で表現された設定情報から汎用的な表現を持つ汎用セキュリティポリシーを生成することが可能である。

【００９５】

次に、PolicyGroup を生成する具体例について説明する。図１１は、セキュリティ機器１３０としてファイアウォールを設置する場合の設置例を示す。ネットワークシステムを構成する通信ネットワーク192.168.1.0/24と、インターネットとの境界にiptablesが搭載されたファイアウォールを設置したとする。iptablesはLinux（ＯＳの名称）上で動作するパケットフィルタリング型ファイアウォールソフトウェアであり、主な機能としてパケットフィルタリング機能を持つ。パケットフィルタリングは保護したい通信ネットワークを不正アクセスから守るための有効な方法であり、データパケットを中継するマシン上で動作し、受信データパケットを全て検査しフィルタリングのルールに基づいてデータパケットが通過することを許可あるいは拒否するものである。各ルールにはデータパケットに

関する幾つかの要素を定義し、これらの要素に応じてデータパケットが処理される。要素としては、データパケットの送信元や宛先のＩＰアドレスやポートなどがある。複数のルールの設定によって、ある送信元から送られるデータパケットの通過を許可したり、別の送信元から送られるデータパケットの通過を拒否したりすることが可能である。またパケットフィルタリングはこれらルールの順序に基づいて動作する。つまり、データパケットが到着した際、ルールは先頭から順に評価され、そのパケットに該当する最初のルールが適用され、そのパケットはそのルールに示されるように処理される。

【００９６】

図１２は、図１１に示したファイアウォールに搭載されているiptablesの設定を表す設定情報である。ファイアウォールから抽出した設定情報が、図１２に例示した設定情報である場合に、このファイアウォールに対応するPolicyGroup を生成する処理経過（図１０に示す処理）の具体例を示す。

【００９７】

図４に示すステップＡ３０２では、設定情報に含まれるiptablesのバージョン情報（図１２において図示せず。）に基づいて、図１１に示すファイアウォールに対応するセキュリティポリシー生成サブルーチンが呼び出されたものとする。このセキュリティポリシー生成サブルーチンには、図１１に示すファイアウォールの設定情報の記述仕様に関する知識として、例えば、図１３に示す知識が含まれているとする。図１３に示す知識では、設定情報内のルールに含まれる表記、その表記の意味、およびルールにその表記が含まれている場合に汎用セキュリティポリシーにどう記述すべきかという情報を含んでいる。なお、図１３に示す「表記」では同一の意味を持つ表記を「, 」で区切って並べている。例えば、ルール内に「-P」という表記があっても、ルール内に「--policy」という表記があっても、両者の表記は同一の意味を表している。

【００９８】

図１３に示す記述仕様に関する知識について説明する。図１３の表記「-t」に対応する意味の説明において「-t」の表記が省略されているときにはデフォルトであるパケットフィルタリングルールを示す旨が示されている。この場合、汎用セキュリティポリシー内では、パケットフィルタリング機能に対応するPolicyRule内のFunctionの項目では"packet_filtering"と記述することが示されている。

【００９９】

また、図１３に示す知識では、"-P"の表記があるルールは、デフォルトルール（他の各ルールが適用されなかった場合に適用されるルール）であることが示されている。そしてこのルールに対応するPolicyは、パケットフィルタリングのPolicyのうち、最後尾に記述されることが示されている。また、"-A"の表記があるルールは、パケットフィルタリング機能に関する一つルールであり、パケットフィルタリングのPolicyとして記述されることが示されている。

【０１００】

また、ルールに"-p"の表記がある場合、その後に続く記述はプロトコルを表していることを示している。そして、"-p"に続くプロトコルの記述に応じてPacketオブジェクトのProtocol属性を記述することが示されている。

【０１０１】

また、ルールに"-s"の表記がある場合、その後に続く記述が送信元ＩＰアドレスであり、PacketオブジェクトのSrcIP 属性として、その送信元ＩＰアドレスを記述することが示されている。同様に、"-d"の表記がある場合、その後に続く記述が宛先ＩＰアドレスであり、PacketオブジェクトのDestIP属性として、その宛先ＩＰアドレスを記述することが示されている。

【０１０２】

また、ルールに"-j ACCEPT "という記述があれば、パケット通過の許可を意味し、PolicyRuleのActionを"accept "と記述することが示されている。ルールに"-j DROP"という記述があれば、パケット通過の禁止を意味し、PolicyRuleのActionを"Deny"と記述すること

が示されている。

【０１０３】

図１３に示した記述仕様に関する知識は、例示であり、他の知識を含んでいてもよい。また、記述仕様に関する知識は、セキュリティポリシー生成サブルーチン毎に異なる。

【０１０４】

図１１に示すファイアウォールに対応するセキュリティポリシー生成サブルーチンを呼び出した汎用セキュリティポリシー生成手段１０３は、ファイアウォールに対応するPolicyGroup を生成するときに、まず、Policy結合アルゴリズムを判定する（ステップＡ３０３２）。本例では、汎用セキュリティポリシー生成手段１０３は、図１２に示す設定情報に含まれる各ルールがiptablesのルールであると判定する（各ルールにiptablesという記述があるため）。また、各ルールに"-t"の記述がないので、各ルールがパケットフィルタリングルールであると判定する。本例では、このような場合にPolicy結合アルゴリズムを"first-applicable"とすると、セキュリティポリシー生成サブルーチンに規定されていて、汎用セキュリティポリシー生成手段１０３は、その規定に従い、にPolicy結合アルゴリズムが"first-applicable"であると判定する。"first-applicable"は、Policy適用時にはPolicyの記述順に適用しなければならないことを意味する。

【０１０５】

次に、汎用セキュリティポリシー生成手段１０３は、記述仕様に関する知識を用いて、ファイアウォールから抽出した設定情報が３つのパケットフィルタリングルールから成ることを判断し、その設定情報を３つのルールに分割する（ステップＡ３０３３）。ただし、図１３には示していないが、「"iptables"を先頭とする１行で表現されるルールは、iptablesにおける一つのパケットフィルタリングルールを示す。」という記述仕様に関する知識が存在しているものとする。本例では、この知識に従って、図１２に示す設定情報を３つのルールに分割する。

【０１０６】

次に、汎用セキュリティポリシー生成手段１０３は、ルール単位に分割された設定情報から、図１３に例示する記述仕様に関する知識に基づいて、PolicyRuleに含まれる各項目、Condition 、Obligation、PolicyRule結合アルゴリズムをそれぞれ判定する（ステップＡ３０３４）。

【０１０７】

１行目のルールは"-P"オプションがあることからデフォルトルールであることが判断でき、最も優先度が低いルールとしてPolicyGroupの最後尾のPolicyとするので保留する。

【０１０８】

続いて、ステップＡ３０３６において、汎用セキュリティポリシー生成手段１０３は、まだPolicyを生成していないルールがあると判定して、ステップＡ３０３４に移行し、２行目のルールに対する処理を行う。

【０１０９】

このとき図１１に示すファイアウォールに対応するセキュリティポリシー生成サブルーチンに従う汎用セキュリティポリシー生成手段は、パケットフィルタリングの汎用セキュリティポリシーを生成することから、PolicyRuleのInputObject をPacket型とし、Actionをルールの記述に応じて"accept", "deny", "reject"のいずれかとする。また、iptablesではパケットの通過が許可された場合には出力となるOutputObjectの内容は入力であるInputObject と全く同一のものとなることからOutputObjectを省略する。また、パケットフィルタリングについては、InputObject で示されるPacketに対するActionは常に実行されるのでeffectは"permit"とする。また図１２に示された各ルールは、パケットフィルタリング機能に関する記述のみで表され、複数のセキュリティ機能に関する記述を含んでいない。従ってPolicyに含まれるPolicyRuleはそれぞれただ一つである。ただし、本例では、セキュリティポリシー生成サブルーチンに従って、PolicyRule結合アルゴリズムを"ordered-deny-overrides"と定める。iptables稼動時にInputObject で表されるパケットに一致するパケットが検知された場合にはPolicyRuleのeffectは常に"permit"となり、そのInpu

tObjectを含むPolicyRuleを持つPolicyの評価は"permit"と判断され、PolicyRuleのActionが実行されることになる。

【０１１０】

２行目のルールに対するステップＡ３０３４の処理では、汎用セキュリティポリシー生成手段１０３は、iptablesへの入力であるInputObjectとなるパケットの属性として、プロトコルは、tcp（"-p"オプションで表される）、送信元ＩＰアドレスは、0.0.0.0/0（"-s"オプションで表される）、宛先ＩＰアドレスは、192.168.1.248/29（"-d"オプションで表される）、アクションは、DROP（"-j"オプションで表される。汎用セキュリティポリシーでは"deny"として表現する。）と、それぞれ判定する。次のステップＡ３０３５の処理では、汎用セキュリティポリシー生成手段１０３は、これらの項目を図８および図９に示す書式に従って記述することにより、２行目のルールに対応するPolicyの部分を生成する。なお、２行目のルールでは、ルール適用条件や責務の記述はないので、ステップＡ３０３４ではCondition やObligationの項目については判定せず、ステップＡ３０３５ではPolicyの中にCondition やObligationを含めない。この点は、他の各行についても同様である。

【０１１１】

続いて、ステップＡ３０３６において、汎用セキュリティポリシー生成手段１０３は、まだPolicyを生成していないルールがあると判定して、ステップＡ３０３４に移行し、３行目のルールに対する処理を行う。３行目のルールに対するステップＡ３０３４，Ａ３０３５の処理は、２行目に対する処理と同様に行えばよい。

【０１１２】

続くステップＡ３０３６において、汎用セキュリティポリシー生成手段１０３は、保留していた１行目のルールがあると判定し、ステップＡ３０３４に移行し、１行目のルールに対する処理を行う。１行目のデフォルトルールではパケットの属性であるプロトコル、送信元アドレス、宛先アドレスなどが省略されているので、設定情報の記述仕様に関する知識に基づいて、省略されている項目を予め定められているデフォルト値で補う。なお、図１３に示す記述仕様に関する知識では、ルール内で各項目が省略されているときに、省略された項目のをどのようなデフォルト値で補うかについて記載されていないが、省略された項目に適用されるデフォルト値も記述仕様に関する知識で規定されている。１行目のルールから各項目を判定したならば、汎用セキュリティポリシー生成手段１０３は、１行目に対応するPolicy部分を生成する（ステップあ３０３５）。"-P"の表記を含む１行目のルールは、保留され最後にPolicyが生成されるので、１行目のルールに対応するPolicyは各Policyの最後尾に記述されることになる。

【０１１３】

続くステップＡ３０３６では、汎用セキュリティポリシー生成手段１０３は、ルール毎に分割した各情報からそれぞれPolicyを生成したと判定し、ステップＡ３０３７に移行する。汎用セキュリティポリシー生成手段１０３は、ルール毎に作成した各Policyとステップ３０３２で判定したPolicy結合アルゴリズム"first-applicable"とを組み合わせてPolicyGroupを生成する（ステップＡ３０３７）。このとき汎用セキュリティポリシー生成手段１０３は、図８および図９に例示する書式にあわせてPolicyGroup を生成する。

【０１１４】

以上の手順を経て、図１２に示した設定情報を図８および図９に示したフォーマットで汎用セキュリティポリシーとして表現することができる。この汎用セキュリティポリシーを図１４に示す。図１４におけるPolicyGroup タグに囲まれた部分が、図１２に示す設定情報から生成された汎用セキュリティポリシーである。

【０１１５】

図１４に示すPolicyGroup では、Policy（パケットフィルタリングルール）は先頭から順に評価されるのでPolicyGroup のpolicyCombiningAlg属性に"first-applicable"が指定されている。この指定は、ステップＡ３０３７において汎用セキュリティポリシー生成手段１０３が行う。

【０１１６】
また、図１４に示すPolicyGroup では、図１２に示す各ルールに対応するPolicyが３個含まれている。各Policyはパケットフィルタリング機能を記述したPolicyRuleを１つずつ含む。各PolicyRuleの子要素"Function"にはパケットフィルタリング機能を表す"packet_filtering"が指定されており、"InputObject "にはパケットを表す"Packet"が指定されている。"Packet"の子要素にはそれぞれのルールに対応する送信元ＩＰアドレス、プロトコル、宛先ＩＰアドレスが記述されている。このように汎用セキュリティポリシーでは、パケットフィルタリングルールを記述するために最低限必要な情報を統一的な方法で記述することにより、パケットフィルタリングを行うセキュリティ機器それぞれに固有な設定記述形式によらず汎用的に表現することができる。

【０１１７】
次に、本実施の形態の効果について説明する。本実施の形態では、ネットワークシステムの構成要素であるセキュリティ機器の実際の設定内容（設定情報）から汎用セキュリティポリシーの構築 を行うように構成されているため、汎用セキュリティポリシーの構築およびネットワークシステムのセキュリティ状況把握が、短時間で正確に行うことが可能となる。また、設定情報の中に省略されている項目がある場合であっても、その項目をデフォルト値で補って、汎用セキュリティポリシーでは、省略されていた項目も記述されるので、システム管理者の負担が軽減される。

【０１１８】
また、汎用セキュリティポリシーの構築の際、システム管理者の操作は、セキュリティ機器の指定（ステップＡ２０１参照。）だけで済むので、ほとんど人手が介在することなく汎用セキュリティポリシーを生成することができる。また、セキュリティ機器の指定の後には、自動的に汎用セキュリティポリシーを生成することができる。さらに、設定情報抽出手段１０１がシステム管理者からの指定を受けずにセキュリティ機器１３０を検索する構成の場合には、人手を介することなく汎用セキュリティポリシーを生成することができる。

【０１１９】
また本実施の形態では、実際の設定情報に基づいてセキュリティポリシーの構築を行うように構成されているため、作業者（システム管理者等）の勘違いや思いこみに起因する誤りや漏れが極めて少ない汎用セキュリティポリシーの構築が可能となる。

【０１２０】
実施の形態２.
図１５は、本発明によるセキュリティポリシー管理システムの第２の実施の形態を示すブロック図である。第１の実施の形態と同様の構成部については、図１と同一の符号を付して説明を省略する。また、第１の実施の形態と同様の構成部の動作は、第１の実施の形態と同様である。

【０１２１】
第２の実施の形態において、セキュリティポリシー管理システムは、分析知識データベース１４０を備える。また、データ処理装置１００は、第１の実施の形態で示した設定情報抽出手段１０１、汎用セキュリティポリシー生成手段１０３に加え、セキュリティポリシー分析手段１０５を含んでいる。セキュリティポリシー分析手段１０５は、例えば、プログラムに従って動作するＣＰＵによって実現される。プログラムには、サブルーチンとして少なくとも１つのセキュリティポリシー分析サブルーチン１０６が含まれる。個々のセキュリティポリシー分析サブルーチン１０６は、各セキュリティ機器１３０によって実現される個々のセキュリティ機能と対応する。例えば、あるセキュリティポリシー分析サブルーチン１０６は、パケットフィルタリング機能と対応する。別のセキュリティポリシー分析サブルーチン１０６は、他のセキュリティ機能と対応する。各セキュリティポリシー分析サブルーチン１０６は、データ処理装置１００が備える記憶装置（図１５において図示せず。）に予め記憶させておく。

【０１２２】

セキュリティポリシー分析手段１０５は、分析知識データベース１４０を参照しながら、汎用セキュリティポリシー生成手段１０３により生成された汎用セキュリティポリシーを分析する。分析の態様は、セキュリティ機能によって異なる。分析の一態様として、要約がある。要約は、複数のルール（汎用セキュリティポリシー内ではPolicyとして記述される。）から導かれる内容をまとめることを意味する。後述するように、パケットフィルタリング機能の分析としては、要約を行う。セキュリティポリシー分析手段１０５は、分析処理を実行するときに、セキュリティ機能毎に、対応するセキュリティポリシー分析サブルーチン１０６を呼び出し、そのセキュリティポリシー分析サブルーチン１０６に従って分析を実行する。

【０１２３】

分析知識データベース１４０は、分析に用いられる情報を記憶する。この情報は、セキュリティポリシー分析手段１０５が分析を行う際に参照される。

【０１２４】

次に、動作について説明する。

図１６は、本実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者からセキュリティに関する分析要求を入力される（ステップＢ１）。次に、設定情報抽出手段１０１は通信ネットワーク１２０に接続されている少なくとも１つのセキュリティ機器１３０について、そのセキュリティ機器１３０に対応する設定情報抽出サブルーチン１０２を呼び出す。そして、そのセキュリティ機器１３０から設定情報を抽出、収集する（ステップＢ２）。続いて、汎用セキュリティポリシー生成手段１０３は、ステップＢ２で抽出、収集された設定情報から、セキュリティ機器１３０に対応するセキュリティポリシー生成サブルーチン１０４を呼び出し、セキュリティ機器１３０ごとに汎用セキュリティポリシーを生成する（ステップＢ３）。このステップＢ１～Ｂ３の処理は、第１の実施の形態におけるステップＡ１～Ａ３の処理と同様である。

【０１２５】

次に、セキュリティポリシー分析手段１０５は、分析知識データベース１４０を参照しながら、汎用セキュリティポリシー生成手段１０３により生成された汎用セキュリティポリシーの内容をセキュリティ機能毎に分析する（ステップＢ４）。セキュリティポリシー分析手段１０５は、分析後、分析結果を入出力手段１１０から出力しシステム管理者に提示する（ステップＢ５）。例えば、分析結果をディスプレイ装置に表示させる。

【０１２６】

図１７から図１９は、分析知識データベース１４０が記憶する情報の例を示す。分析知識データベース１４０は、各セキュリティ機能がどのようなオブジェクトを処理し、そのようなアクションを起こすことができるのかを示す情報を記憶する。図１７は、この情報の例を示す。図１７では、セキュリティ機能（Function）毎に、そのFunctionが取り扱うオブジェクトの型（例えば、Packet型等）や属性（例えば、SrcIP, DestIP, Protocol等）、およびアクションの種類（例えば、accept ,drop, reject等）を対応付けた情報を示している。

【０１２７】

また、分析知識データベース１４０は、オブジェクトに付随する属性がどのような値をとり得るかを示す情報を記憶する。図１８は、この情報の例を示す。例えば、図１８に示す情報は、オブジェクトの属性となる"PortNumber（ポート番号）"のとり得る値は、１から６５５３５までの整数であることを示している。他の属性についても、属性値となり得る範囲を示している。

【０１２８】

また、分析知識データベース１４０は、各オブジェクト間、各属性間の関係を示す情報を記憶する。図１９は、各属性間の関係を示す情報の例を示す。図１９に示す例では、IP Address （ＩＰアドレス）とPortNumber（ポート番号）との関係として、「一つのＩＰアドレスは、１～６５５３５番までのポート番号を持つ。」という情報を示している。また

、NetworkAddress とIPAddress との関係として、「NetworkAddress はNetMask のビット数分だけ最上位からのビットを固定し、残りのビットを０としたＩＰアドレスから、残りのビットを全て１としたＩＰアドレスまでの範囲のＩＰアドレスの集合を表す。」という情報を示している。

【０１２９】

図１７から図１９に示した情報は、分析知識データベース１４０が記憶する情報の例示であり、分析知識データベース１４０が記憶する情報は、図１７から図１９に示す情報に限定されない。また、分析の際には、分析知識データベース１４０が記憶する全ての情報が参照されるとは限らず、一部の情報のみが参照されてもよい。どの情報が参照されるかは、分析の種類（セキュリティ機能の種類）によって異なる。なお、新たなセキュリティ機能についての分析を行う場合には、その新たなセキュリティ機能の分析において参照される情報を分析知識データベース１４０に追加して記憶させればよい。

【０１３０】

次に、ステップＢ４の分析処理について説明する。図２０は、ステップＢ４の分析処理の例を示すフローチャートである。ステップＢ３において設定情報から汎用セキュリティポリシーが生成されると、セキュリティポリシー分析手段１０５はまず汎用セキュリティポリシーからセキュリティ機能の名前などのセキュリティ機能を特定する情報（セキュリティ機能情報）を取得する（ステップＢ４０１）。汎用セキュリティポリシーでは、セキュリティ機能情報は、Functionタグに囲まれた部分に記述されている。従って、Functionタグに囲まれた部分に記述された情報を取得すればよい。図１４に示す汎用セキュリティポリシーを例に説明すると、Functionタグに囲まれた部分に記述されている"packet_filtering"を取得する。この情報によりパケットフィルタリング機能というセキュリティ機能を特定することができる。

【０１３１】

次に、セキュリティポリシー分析手段１０５は、ステップＢ４０１で取得したセキュリティ機能情報に応じて、分析知識データベース１４０において所定の情報を検索する（ステップＢ４０２）。検索対象となる情報は、ステップＢ４０１で取得された情報によって異なる。本例では、ステップＢ４０１で"packet_filtering"という情報が取得された場合、図１９に示すNetworkAddress とIPAddress との関係を示す情報を検索するものとする。

【０１３２】

続いて、セキュリティポリシー分析手段１０５は、ステップＢ４０２で検索された情報を分析知識データベース１４０から取得する（ステップＢ４０３）。ステップＢ４０１で"packet_filtering"という情報が取得された場合、ステップＢ４０３では、「NetworkAddress はNetMask のビット数分だけ最上位からのビットを固定し、残りのビットを０としたＩＰアドレスから、残りのビットを全て１としたＩＰアドレスまでの範囲のＩＰアドレスの集合を表す。」という情報を分析知識データベース１４０から取得する。検索対象となる情報は、ステップＢ４０１で取得されたセキュリティ機能情報によって異なるので、ステップＢ４０３で取得される情報も、セキュリティ機能情報によって異なる。セキュリティ機能情報の種類によっては、セキュリティ機能の動作モデルや動作モデルがどのようなオブジェクトを扱うことが可能か等の情報を取得してもよい。

【０１３３】

次にセキュリティポリシー分析手段１０５は、セキュリティ機能情報から特定されるセキュリティ機能に対応するセキュリティポリシー分析サブルーチン１０６を呼び出す。セキュリティポリシー分析手段１０５は、そのセキュリティポリシー分析サブルーチン１０６に従って、ステップＢ４０３で取得した情報を用いて、既に生成されている汎用セキュリティポリシーを分析する（ステップＢ４０４）。

【０１３４】

続いて、セキュリティポリシー分析手段１０５は、ステップＢ４０１で取得した各セキュリティ機能情報について、ステップＢ４０２～Ｂ４０４の処理を行ったか否かを判定す

る（ステップＢ４０５）。まだ、各セキュリティ機能情報から特定されるセキュリティ機能のうち、まだ、ステップＢ４０２～Ｂ４０４の処理を行っていないものがあれば、ステップＢ４０２以降の動作を繰り返す。各セキュリティ機能に対してステップＢ４０２～Ｂ４０５の処理を行ったならばステップＢ４の分析処理を終了する。

【０１３５】

ステップＢ４０４の分析処理は、セキュリティ機能毎に異なる。ここでは、ポリシー分析の一例としてパケットフィルタリング機能に関する分析（要約）を例に説明する。例えば、図１４に例示する汎用セキュリティポリシーは、パケットフィルタリングに関する３つのPolicyを含んでいる。この３つのPolicyを参照することによって、どのようなパケットが通過を許可され、どのようなパケットが通過を禁止されるのかを把握することができる。Policyの順序、送信元領域あるいは宛先領域の包含関係、アクション（通過させる、通過させない）などを総合的に判断して、汎用セキュリティポリシーの内容を判断することになる。しかし、この３つのPolicyをまとめて、どのようなパケットが通過を許可され、どのようなパケットが通過を禁止されるのかを、直感的に把握できるようにすれば、より汎用セキュリティポリシーの内容を把握しやすくなる。第２の実施の形態では、分析を行うことによって、より汎用セキュリティポリシーの内容を把握しやすくしている。

【０１３６】

図２１は、パケットフィルタリング機能に応じた分析処理の例を示すフローチャートである。セキュリティポリシー分析手段１０５は、汎用セキュリティポリシーを参照して、パケットフィルタリング機能が処理対象としているプロトコルを判定する（ステップＢ４０４１）。プロトコルの判定は、PolicyRule内のInputObject に記述されたProtocol属性によって判定すればよい。Protocol属性がｔｃｐであるならば、ｔｃｐに応じた分析処理を実行する（ステップＢ４０４２）。Protocol属性がｕｄｐであるならば、ｕｄｐに応じた分析処理を実行する（ステップＢ４０４３）。Protocol属性がｉｃｍｐであるならば、ｉｃｍｐに応じた分析処理を実行する（ステップＢ４０４４）。

【０１３７】

図２２は、ｔｃｐに応じた分析処理の例を示すフローチャートである。セキュリティポリシー分析手段１０５は、汎用セキュリティポリシーに含まれる一つのPolicyGroup について、パケットフィルタリングルールに対応するPolicyをを優先度の低いものから並ぶようにソートする（ステップｂ１）。

【０１３８】

通常、パケットフィルタリングポリシーは、先頭のポリシーが最も優先度が高く最後尾のポリシーが最も優先度が低くなるようにしている。例えば、同じ内容のパケットについて通過を許可するポリシーの後に通過を拒否するを並べたとしても、前のポリシーが先に評価され、そのパケットは通過を許可される。また、パケットフィルタリングポリシーには、どのポリシーにもマッチしなかったパケットについてのアクションを指定するデフォルトポリシーを通常設ける。つまりデフォルトポリシーが最も優先度が低いポリシーとなる。ステップＢ３においてパケットフィルタリング機能のルールに対応する複数のPolicyを生成する場合にも、第１の実施の形態で説明したようにデフォルトのルールに対応するPolicyが最後尾に記述されるようにしている。他のPolicyは設定情報内に記述されたルールの順番に従って、PolicyGroup 内での順番が定められている。

【０１３９】

本実施の形態では、セキュリティポリシー分析手段１０５は、汎用セキュリティポリシーの一つのPolicyGroup 内で最後尾に記述されたデフォルトルールに対応するPolicyが先頭になり、一番最初に記述されたPolicy（最も優先度が高いPolicyが最後になるようにソートすればよい。

【０１４０】

ソート後、セキュリティポリシー分析手段１０５は、先頭のPolicy（デフォルトルールに対応するPolicy）を取得する（ステップｂ２）。次に、横軸を送信元のＩＰアドレスとし、縦軸を宛先のＩＰアドレスとする２次元平面を示すデータ（以下、２次元平面データ

と記す。）を作成する。ＩＰアドレスのとり得る範囲は有限であるので、２次元平面データによって表される領域は矩形となる。２次元平面データをディスプレイ装置上に表示した場合の画面の例については、後述の図２４や図２５で示す。セキュリティポリシー分析手段１０５は、２次元平面データにおいて、ステップｂ２で取得した先頭のPolicyの送信元ＩＰアドレスおよび宛先ＩＰアドレスによって特定される範囲に、そのPolicyのActionの内容を割り当てる（ステップｂ３）。具体的には、先頭のPolicyが、送信元アドレスとしてＩＰアドレスのとり得る全範囲を指定し、宛先アドレスとしてＩＰアドレスのとり得る全範囲を指定しているとする。そして、Actionとして"deny"が指定されているとする。この場合、セキュリティポリシー分析手段１０５は、２次元平面データによって表される領域に"deny"を割り当てる。

【０１４１】

次に、セキュリティポリシー分析手段１０５は、ソートされた順番に従って、次のPolicyを取得する（ステップｂ４）。セキュリティポリシー分析手段１０５は、２次元平面データにおいて、ステップｂ４で取得したPolicyの送信元ＩＰアドレスおよび宛先ＩＰアドレスによって特定される範囲に、そのPolicyのActionの内容を割り当てる（ステップｂ５）。この範囲には、既に前のPolicyのActionの内容が割り当てられているが、ステップｂ５では、その範囲については、ステップｂ４で取得したPolicyのActionの内容を割り当てる。すなわち、上書きすることになる。

【０１４２】

セキュリティポリシー分析手段１０５は、ソート後の最後のPolicyまでステップｂ４，ｂ５の処理を行ったか否かを判定し（ステップｂ６）、最後のPolicyまでステップｂ４，ｂ５の処理を行ったならば処理を終了する。まだ、ステップｂ４，ｂ５の処理を行っていないPolicyがある場合には、ステップｂ４以降の処理を繰り返す。

【０１４３】

なお、本例では、ステップｂ４において、Policyの送信元ＩＰアドレスおよび宛先ＩＰアドレスによって特定される範囲を決定するときに、分析知識データベース１４０から取得した情報を参照する。既に述べたように、パケットフィルタリング機能に関する分析を行う場合には、「NetworkAddress はNetMask のビット数分だけ最上位からのビットを固定し、残りのビットを０としたＩＰアドレスから、残りのビットを全て１としたＩＰアドレスまでの範囲のＩＰアドレスの集合を表す。」という情報を分析知識データベース１４０から取得する。また、図１４に例示するように、送信元ＩＰアドレスおよび宛先ＩＰアドレスは、"192.168.1.248/29"のようにNetMask を用いて記述される。"/ "の次の数値が、NetMask のビット数を表している。従って、"192.168.1.248/29"のように記述されたＩＰアドレスの範囲は、分析知識データベース１４０から取得した情報に基づいて、"192.168.1.248 "～"192.168.1.255 "の範囲を表しているということを導出できる。送信元ＩＰアドレスおよび宛先ＩＰアドレスそれぞれについて、このような範囲を導出することで、２次元平面データによって表される領域のうちの一部の領域を特定することができる。

【０１４４】

図２３は、パケットフィルタリング機能を有するセキュリティ機器の設定情報の例である。このような設定情報から汎用セキュリティポリシーを生成したとする。この汎用セキュリティポリシーに含まれる複数のPolicyを２次元平面データとしてまとめる（要約する）分析例について説明する。図２４は、本例の分析結果（要約結果）として表示される２次元平面データの例を示す。

【０１４５】

図２３に示す１行目のルールはデフォルトルールであるので、１行目のルールの優先度が最も低くなる。また、２行目のルールが最も優先度が高いルールであり、３行目のルールが２番目に優先度が高いルールである。従って、各ルールからPolicyを生成した場合、汎用セキュリティポリシー内では、２行目に対応するPolicy、３行目に対応するPolicy、１行目に対応するPolicyの順に記述される。ステップｂ１では、優先度の低い順にソートされるので、ソート後には各Policyの順番は逆になる。

【０１４６】
ソート後の先頭のPolicyはデフォルトルールのポリシーであり、デフォルトルールでは送信元ＩＰアドレス、宛先ＩＰアドレスに関わらずパケットを破棄（DROP）することを定めている。従って、ステップｂ３の処理では、セキュリティポリシー分析手段１０５は、図２４に示す領域全体に"deny"を割り当てる。
【０１４７】
次に、セキュリティポリシー分析手段１０５は、図２３に示す３行目に対応するPolicyを取得し（ステップｂ４）、ステップｂ５の処理を行う。このPolicyでは、送信元ＩＰアドレスは、"172.16.1.0/24"と記述されており、送信元ＩＰアドレスの範囲は、"172.16.1.0～172.16.1.255"であると判定される。同様に、宛先ＩＰアドレスの範囲は、"192.168.1.224～192.168.1.255"であると判定される。また、このPolicyのAtionは"accept"である。この結果、セキュリティポリシー分析手段１０５は、図２４に示す領域Ａ，Ｂに対して"accept"を割り当てる。
【０１４８】
次に、セキュリティポリシー分析手段１０５は、図２３に示す２行目に対応するPolicyを取得し（ステップｂ４）、ステップｂ５の処理を行う。このPolicyでは、送信元ＩＰアドレスは、"172.16.1.0/24"と記述されており、送信元ＩＰアドレスの範囲は、"172.16.1.0～172.16.1.255"であると判定される。同様に、宛先ＩＰアドレスの範囲は、"192.168.1.248～192.168.1.255"であると判定される。また、このPolicyのAtionは"deny"である。この結果、セキュリティポリシー分析手段１０５は、図２４に示す領域Ｂに対して"deny"を割り当てる。従って、領域Ｂは、"deny"が割り当てられた後、"accept"で上書きされ、さらに"deny"で上書きされることになる。
【０１４９】
ステップＢ５の分析結果出力処理では、セキュリティポリシー分析手段１０５は、分析結果として、図２４に示す画面を表示する。この結果から３つのパケットフィルタリングに関するPolicyを要約すると送信元ＩＰアドレス172.16.1.0～172.16.1.255から宛先ＩＰアドレス192.168.1.224～192.168.1.247に向かうパケットが通過を許可されることがわかる。この分析結果では、送信元ＩＰアドレスと宛先ＩＰアドレスによって定められる領域を"accept"や"deny"に応じて区別して表示することで、どのパケットが通過を許可され、どのパケットが通過を禁止されるのかを示している。このように、複数のPolicyが１つの２次元領域としてまとめられているので、どのようなパケットを通過させることになるのかを、汎用セキュリティポリシーの記述よりも、よりわかりやすく提示できるようになる。
【０１５０】
また、パケットフィルタリング機能に関するPolicyを含むPolicyGroup が複数存在する場合には、PolicyGroup の指定を受け付け、指定されたPolicyGroup の要約結果を表示してもよい。この場合のユーザインタフェースの例を図２５に示す。セキュリティポリシー分析手段１０５は、PolicyGroup 指定欄７１と、分析結果表示領域７２とを含む画面を表示する。PolicyGroup 指定欄７１は、プルダウンメニューによりPolicyGroupID 属性の値を表示し、システム管理者にPolicyGroup の選択を促す。セキュリティポリシー分析手段１０５は、PolicyGroupID の指定を受け付けると、そのPolicyGroupID によって特定されるPolicyGroup について分析を行い、図２５に示すように、分析結果表示領域７２に分析結果を表示する。
【０１５１】
以上の説明では、ステップＢ４０４１において、プロトコルがｔｃｐであると判定された場合について説明した。ステップＢ４０４１でプロトコルがｕｄｐであると判定された場合には、ステップＢ４０４３の処理を行うことになる。なお、ステップＢ４０４３の処理は、ステップＢ４０４２と同様の処理である。従って、プロトコルがｕｄｐであると判定された場合も、図２２に示すフローチャートと同様の処理を行えばよい。
【０１５２】

また、ステップＢ４０４１でプロトコルがｉｃｍｐであると判定された場合には、ステップＢ４０４４の処理を行うことになる。ステップＢ４０４４の処理も、ステップＢ４０４２と同様の処理である。従って、プロトコルがｉｃｍｐであると判定された場合も、図２２に示すフローチャートと同様の処理を行えばよい。ただし、プロトコルがｉｃｍｐである場合には、ステップｂ５において、送信元ＩＰアドレスおよび宛先ＩＰアドレスによって特定される範囲に対して、"deny"または"accept"だけでなく、ｉｃｍｐに応じたパケットフィルタリングルールで指定されたtypeも割り当てる。

【０１５３】

以下、プロトコルがｉｃｍｐであると判定された場合の処理の例について説明する。図２６は、ｉｃｍｐによるパケットフィルタリング機能を有するセキュリティ機器の設定情報の例である。図２７は、本例の分析結果（要約結果）として表示される２次元平面データの例を示す。図２６に示す１行目のルールはデフォルトルールであるので、１行目のルールの優先度が最も低くなる。また、２行目のルールが最も優先度が高いルールであり、３行目のルールが２番目に優先度が高いルールである。従って、各ルールからPolicyを生成した場合、汎用セキュリティポリシー内では、２行目に対応するPolicy、３行目に対応するPolicy、１行目に対応するPolicyの順に記述される。ステップｂ１では、優先度の低い順にソートされるので、ソート後には各Policyの順番は逆になる。

【０１５４】

ソート後の先頭のPolicyはデフォルトルールのPolicyであり、デフォルトルールでは送信元ＩＰアドレス、宛先ＩＰアドレスに関わらずパケットを破棄（DROP）することを定めている。従って、ステップｂ３の処理では、セキュリティポリシー分析手段１０５は、図２７に示す領域全体に"deny"を割り当てる。

【０１５５】

次に、セキュリティポリシー分析手段１０５は、図２６に示す３行目に対応するPolicyを取得し（ステップｂ４）、ステップｂ５の処理を行う。このPolicyでは、送信元ＩＰアドレスは、"192.168.1.250 "である。また、宛先ＩＰアドレスは、"172.16.1.100"である。また、このPolicyのAtionは"accept"である。この結果、セキュリティポリシー分析手段１０５は、図２７に示す領域Ａに対して、"accept"を割り当てる。また、このPolicyではtypeとして０が記述されている。従って、図２７に示す領域Ａに対して、type0 という情報も割り当てる。

【０１５６】

次に、セキュリティポリシー分析手段１０５は、図２６に示す２行目に対応するPolicyを取得し（ステップｂ４）、ステップｂ５の処理を行う。このPolicyでは、送信元ＩＰアドレスは、"172.16.1.100"である。また、宛先ＩＰアドレスは、"192.168.1.250 "である。また、このPolicyのAtionは"accept"である。この結果、セキュリティポリシー分析手段１０５は、図２７に示す領域Ｂに対して、"accept"を割り当てる。また、このPolicyではtypeとして８が記述されている。従って、図２７に示す領域Ｂに対して、type8 という情報も割り当てる。

【０１５７】

この結果、ステップＢ５の分析結果出力処理では、セキュリティポリシー分析手段１０５は、分析結果として、図２７に示す画面を表示する。

【０１５８】

また、図２４、図２５および図２７では、二次元平面により、パケットを通過させる場合と、通過させない場合とを示しているが、他の表示態様で、パケットを通過させる場合を表示してもよい。図２８は、分析結果出力処理（ステップＢ５）における他の出力態様を示す説明図である。この出力態様では、送信元ＩＰアドレスを表す軸（第一の軸）と、宛先ＩＰアドレスを表す軸（第二の軸）とをそれぞれ別々に表示する。図２８では、２本の軸を縦に表示し、また平行に並べた場合の例を示している。

【０１５９】

図２２に示す処理が完了することにより、パケットの通過を許可される送信元ＩＰアド

レスの範囲が決定される。同様に、パケットの通過を許可される宛先ＩＰアドレスの範囲も決定される。セキュリティポリシー分析手段１０５は、パケットの通過を許可される送信元ＩＰアドレスの範囲を、送信元ＩＰアドレスを表す軸上に表示するとともに、パケットの通過を許可される宛先ＩＰアドレスの範囲を、宛先ＩＰアドレスを表す軸上に表示すればよい。また、図２８に示すように、パケットの通過を許可される送信元ＩＰアドレスの範囲から、パケットの通過を許可される宛先ＩＰアドレスの範囲に対して、矢印を表示してもよい。なお、図２８の表示例は、パケットの通過許可領域のみを表示する例である。なお、図２８に示すPolicyGroup 指定欄７１は、図２５に示すPolicyGroup 指定欄７１と同様である。

【０１６０】

次に、本実施の形態の効果について説明する。本実施の形態では、分析知識データベース１４０が、各セキュリティ機能の動作モデルや動作モデルが扱うオブジェクトや属性の情報等を記憶し、セキュリティポリシー分析手段１０５が、分析知識データベース１４０に記憶される情報を参照して、セキュリティ機能を分析するように構成されているため、システム管理者等に、生成した汎用セキュリティポリシーの内容を分かり易く提示することができる。特に、図２４や図２８に例示する図によって分析結果を表示することにより、汎用セキュリティポリシーの内容をさらに分かり易く提示することができる。

【０１６１】

実施の形態３.

次に、本発明によるセキュリティポリシー管理システムの第３の実施の形態について説明する。本実施の形態は、汎用セキュリティポリシーの分析結果同士の同一性の検証を可能にすることを目的とする。図２９は、本発明によるセキュリティポリシー管理システムの第３の実施の形態を示すブロック図である。第２の実施の形態と同様の構成部については、図１５と同一の符号を付して説明を省略する。また、第２の実施の形態と同様の構成部の動作は、第２の実施の形態と同様である。

【０１６２】

第３の実施の形態において、データ処理装置１００は、第２の実施の形態における設定情報抽出手段１０１、汎用セキュリティポリシー生成手段１０３およびセキュリティポリシー分析手段１０５に加え、セキュリティポリシー比較手段１０７を含んでいる。セキュリティポリシー比較手段は、例えば、プログラムに従って動作するＣＰＵによって実現される。プログラムには、サブルーチンとして少なくとも１つの比較サブルーチン１０８が含まれる。個々の比較サブルーチンは、セキュリティポリシー分析サブルーチンと同様に、各セキュリティ機器１３０によって実現される個々のセキュリティ機能と対応する。例えば、ある比較サブルーチン１０８は、パケットフィルタリング機能と対応する。別の比較サブルーチン１０８は、他のセキュリティ機能と対応する。また、個々の比較サブルーチン１０８は、個々のセキュリティポリシー分析サブルーチン１０６と対応することになる。各比較サブルーチン１０８は、データ処理装置１００が備える記憶装置（図２９において図示せず。）に予め記憶させておく。

【０１６３】

セキュリティポリシー比較手段１０７は、セキュリティポリシー分析手段１０５から汎用セキュリティポリシーおよびその分析結果を受け取り、複数のセキュリティ機器の汎用セキュリティポリシーおよびその分析結果を比較検証する。　セキュリティポリシー比較手段１０７は、比較処理を実行するときに、分析が行われたセキュリティ機能に対応する比較サブルーチン１０８を呼び出し、その比較サブルーチンに従って分析結果の比較処理を行う。

【０１６４】

次に、動作について説明する。

図３０は、本実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者からセキュリティ機能の分析結果の比較要求を入力される（ステップＣ１）。また

、データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者からセキュリティに関する分析要求も入力される（ステップＣ２）。ステップＣ２の処理は、ステップＢ１（図１６参照。）の処理と同様である。ステップＣ１，Ｃ２において各要求が入力されると、設定情報抽出手段１０１は通信ネットワーク１２０に接続されている少なくとも１つのセキュリティ機器１３０について、そのセキュリティ機器１３０に対応する設定情報抽出サブルーチン１０２を呼び出す。そして、そのセキュリティ機器１３０から設定情報を抽出、収集する（ステップＣ３）。続いて、汎用セキュリティポリシー生成手段１０３は、ステップＢ２で抽出、収集された設定情報から、セキュリティ機器１３０に対応するセキュリティポリシー生成サブルーチン１０４を呼び出し、セキュリティ機器１３０ごとに汎用セキュリティポリシーを生成する（ステップＣ４）。さらに、セキュリティポリシー分析手段１０５は、生成された汎用セキュリティポリシーの内容を分析し（ステップＣ５）、分析結果を入出力手段１１０から出力しシステム管理者に提示する（ステップＣ６）。ステップＣ３～Ｃ６の各処理は、第２の実施の形態におけるステップＢ２～Ｂ５の各処理と同様の処理である。

【０１６５】

次に、セキュリティポリシー比較手段１０７は、ステップＣ５で分析が行われたセキュリティ機能毎に、分析結果を比較して比較した結果を入出力手段１１０から出力する（ステップＣ７）。比較態様の一例として、分析結果として出力される複数の出力画面を重ねて表示してもよい。例えば、パケットフィルタリング機能に関する分析を行った場合、あるセキュリティ機器Ｔ１のパケットフィルタリング機能の分析結果画面と、別のセキュリティ機器Ｔ２のパケットフィルタリング機能の分析結果画面とを重ねて表示してもよい。すなわち、分析結果として、図２４に例示するような出力画面の情報を複数作成したならば、それらの画面を重ねるようにして複数の分析結果画面を出力してもよい。分析結果の出力画面の態様が、図２５、図２７、図２８のような場合であっても同様である。

【０１６６】

なお、上記の例において、セキュリティ機器Ｔ１とセキュリティ機器Ｔ２は、異なる機種であっても、同一の機種であってもよい。

【０１６７】

また、セキュリティポリシー比較手段１０７は、分析結果の画面を重ねて表示する場合、分析結果が一致していない箇所を特定の表示態様で表示してもよい。例えば、分析結果が一致していない箇所を特定の色で表示したり、その箇所を点滅させて表示してもよい。例えば、あるセキュリティ機器Ｔ１のパケットフィルタリング機能の分析結果では、図２４に示す領域Ｂに"deny"が割り当てられ、別のセキュリティ機器Ｔ２のパケットフィルタリング機能の分析結果では、図２４に示す領域Ｂに"accept"が割り当てられていたとする。この場合、二つの分析結果の出力画面を重ねて表示するときに、領域Ｂの部分を特定の色で表示したり、あるいは、点滅させて表示してもよい。このように表示することによって、分析結果の相違点をシステム管理者に分かり易く提示することができる。さらに、セキュリティポリシー比較手段１０７は、図２４等の画面を重ねた画面だけでなく、汎用セキュリティポリシーのうち、分析結果が一致していない箇所に対応する部分（例えば、PolicyGroup に含まれるPolicyやPolicyRule）も表示してもよい。上記の例の場合、セキュリティ機器Ｔ１の汎用セキュリティポリシーのうち、領域Ｂに関する記述部分（PolicyあるいはPoilcyRule）と、セキュリティ機器Ｔ２の汎用セキュリティポリシーのうち、領域Ｂに関する記述部分（PolicyあるいはPoilcyRule）とをそれぞれ表示してもよい。一致していない箇所に対応するPolicyやPoilcyRuleを表示することによって、汎用セキュリティポリシーのどの部分が一致していないのかをシステム管理者に提示することができる。

【０１６８】

また、セキュリティポリシー比較手段１０７は、分析結果を並べて表示して、システム管理者自身に比較を促す構成であってもよい。例えば、あるセキュリティ機器Ｔ１のパケットフィルタリング機能の分析結果および別のセキュリティ機器Ｔ２のパケットフィルタリング機能の分析結果として、図２４等に例示する出力画面を並べるようにして表示し、

システム管理者に両者の一致点や相違点の判断を促してもよい。

【０１６９】

なお、分析結果の比較は、二つのセキュリティ機器のセキュリティ機能の分析結果の比較のみに限定されない。三つ以上のセキュリティ機器のセキュリティ機能の分析結果を比較してもよい。

【０１７０】

次に、パケットフィルタリング機能の分析結果の具体例について説明する。ネットワークシステム内にセキュリティ機器Ｔ１，Ｔ２が含まれていて、セキュリティ機器Ｔ１にはパケットフィルタリングソフトウェアＰ１が搭載されているとする。また、セキュリティ機器Ｔ２にはパケットフィルタリングソフトウェアＰ２が搭載されているとする。そして、パケットフィルタリングソフトウェアＰ１，Ｐ２には、同一のルールが設定されていなければならないとする。図３１は、セキュリティ機器Ｔ１（パケットフィルタリングソフトウェアＰ１を搭載）から抽出した設定情報に基づいて生成された汎用セキュリティポリシーの例を示す。図３２は、セキュリティ機器Ｔ２（パケットフィルタリングソフトウェアＰ２を搭載）から抽出した設定情報に基づいて生成された汎用セキュリティポリシーの例を示す。

【０１７１】

図３１に示す汎用セキュリティポリシーでは、一つのPolicyGroup 内に３つのPolicyが記述される。最後尾に記述されたPolicyは、送信元ＩＰアドレスが"172.16.1.0"から"172.16.1.255"までの範囲であり、宛先ＩＰアドレスが"192.168.1.10"であるパケットは"deny"とすることを示している。最初のPolicyは、送信元ＩＰアドレスが"172.16.1.0"から"172.16.1.255"までの範囲であり、宛先ＩＰアドレスが"192.168.1.10"であり、宛先ポート番号が１～１０２３であるパケットは、"accept"とすることを示している。２番目のPolicyは、送信元ＩＰアドレスが"172.16.1.0"から"172.16.1.255"までの範囲であり、宛先ＩＰアドレスが"192.168.1.10"であり、宛先ポート番号が１０２４であるパケットは、"accept"とすることを示している。この分析結果の出力画面は、例えば、図３３に示すような画面となる。

【０１７２】

図３２に示す汎用セキュリティポリシーでは、一つのPolicyGroup 内に２つのPolicyが記述される。最後尾に記述されたPolicyは、送信元ＩＰアドレスが"172.16.1.0"から"172.16.1.255"までの範囲であり、宛先ＩＰアドレスが"192.168.1.10"であるパケットは"deny"とすることを示している。最初のPolicyは、送信元ＩＰアドレスが"172.16.1.0"から"172.16.1.255"までの範囲であり、宛先ＩＰアドレスが"192.168.1.10"であり、宛先ポート番号が１～１０２４であるパケットは、"accept"とすることを示している。この分析結果の出力画面は、図３３に示す画面と同様の画面となる。ただし、宛先ポート番号に関しては、１～１０２４までで一つのPolicyにまとめられているので、宛先ポート番号１０２３での区切りは表示されない。

【０１７３】

セキュリティポリシー比較手段１０７は、この二つの分析結果の出力画面を重ねて表示する。このときの出力画面は、図３３に示す画面と同様の画面である。図３１と図３２のそれぞれのセキュリティポリシーの分析結果では、"deny"が割り当てられた領域と、"accept"が割り当てられた領域とがそれぞれ一致する。従って、特定の表示態様（特定の色、あるいは点滅状態等）で表示される箇所はない。この結果、図３１が示す汎用セキュリティポリシーの内容と、図３２が示す汎用セキュリティポリシーの内容とが同一内容であることを簡単に把握することができる。

【０１７４】

次に、本実施の形態の効果について説明する。本実施の形態では、セキュリティ機器に固有の表現を持つ設定情報からセキュリティ機器の種類によらない汎用セキュリティポリシーを生成した後、汎用セキュリティポリシーの比較検証を行うように構成されている。そのため、同じセキュリティ機能を持つセキュリティ機器であれば異なる機器間でも機器

固有の設定記述の形式を意識することなく設定内容の比較検証を行うことができる。また、汎用セキュリティポリシーの内容が同一であっても、図３１および図３２に例示したように記述が異なる場合がある。本実施の形態では、ポリシー分析の結果を用いて比較検証を行うように構成されているため、幾通りもの記述方法で記述される汎用セキュリティポリシーについてそれぞれの記述の違いを意識することなくその内容の同一性を検証することができる。

【０１７５】

なお、複数のセキュリティ機器の設定情報から導出される汎用セキュリティポリシーの分析結果を比較検証する場合、設定情報抽出手段１０１は、ステップＣ３（図３０参照。）において複数のセキュリティ機器から設定情報を収集すればよい。例えば、ある会社の各事業所や各研究所のファイアウォールの設定情報から導出される汎用セキュリティポリシーの分析結果を比較検証する場合には、ステップＣ３において、各ファイアウォールから設定情報を収集すればよい。また、少なくとも一台のセキュリティ機器の設定情報から導出される汎用セキュリティポリシーの分析結果と、予め生成された基準となる汎用セキュリティポリシーの分析結果とを比較検証してもよい。この場合、設定情報抽出手段１０１は、ステップＣ３において、少なくとも一台のセキュリティ機器から設定情報を抽出すればよい。また、予め生成された基準となる汎用セキュリティポリシーの分析結果は、記憶装置（図２９において図示せず。）に記憶させておけばよい。そして、少なくとも一台のセキュリティ機器の設定情報から汎用セキュリティポリシーおよびその汎用セキュリティポリシーの分析結果を生成し、ステップＣ７で予め生成された分析結果を読み込み、ステップＣ７の処理を行えばよい。この結果、一つのセキュリティ機器の汎用セキュリティポリシーの分析結果と、予め生成された基準となる汎用セキュリティポリシーの分析結果とを比較検証することができる。この場合、予め分析結果を記憶する記憶装置が、分析結果記憶手段に相当する。

【０１７６】

実施の形態４．

次に、本発明によるセキュリティポリシー管理システムの第４の実施の形態について説明する。本実施の形態は、同種のセキュリティ機能の設定について定めた複数の汎用セキュリティポリシーを統合的に分析することを目的とする。本実施の形態では、第２の実施の形態と同様に、個々の汎用セキュリティポリシーの分析を行う。そして、各分析結果を統合して、統合的な分析結果を得る。

【０１７７】

図３４は、本発明によるセキュリティポリシー管理システムの第４の実施の形態を示すブロック図である。第２の実施の形態と同様の構成部については、図１５と同一の符号を付して説明を省略する。また、第２の実施の形態と同様の構成部の動作は、第２の実施の形態と同様である。

【０１７８】

第４の実施の形態において、データ処理装置１００は、第２の実施の形態で示した設定情報抽出手段１０１、汎用セキュリティポリシー生成手段１０３およびセキュリティポリシー分析手段１０５に加え、セキュリティポリシー統合手段１１１を含んでいる。セキュリティポリシー統合手段１１１は、例えば、プログラムに従って動作するＣＰＵによって実現される。プログラムには、サブルーチンとして少なくとも一つの統合サブルーチン１１２が含まれる。個々の統合サブルーチンは、セキュリティポリシー分析サブルーチンと同様に、各セキュリティ機器１３０によって実現される個々のセキュリティ機能と対応する。例えば、ある統合サブルーチン１１２は、パケットフィルタリング機能と対応する。別の統合サブルーチン１１２は、他のセキュリティ機能と対応する。また、個々の統合サブルーチン１１２は、個々のセキュリティポリシー分析サブルーチン１０６と対応することになる。各統合サブルーチン１１２は、データ処理装置１００が備える記憶装置（図３４において図示せず。）に予め記憶させておく。

【０１７９】

本発明において、「セキュリティポリシーの統合」とは、同種のセキュリティ機能の設定について定めた複数の汎用セキュリティポリシーの分析結果をさらにまとめて分析し、複数の汎用セキュリティポリシー全体としての分析結果を導出することをいう。すなわち、本発明における「統合」とは、汎用セキュリティポリシーの分析結果をさらにまとめて分析することを意味する。例えば、同一のセキュリティ機能を持つ複数のセキュリティ機器からそれぞれ導出された汎用セキュリティポリシーの分析結果をさらにまとめて分析し、それら複数のセキュリティ機器から導出された各汎用セキュリティポリシー全体としての分析結果を導出することが、「セキュリティポリシーの統合」に該当する。

【０１８０】

汎用セキュリティポリシーの分析として、パケットフィルタリング機能について定めた汎用セキュリティポリシーの要約を行う場合を例に説明する。パケットフィルタリングを行う複数のセキュリティ機器があり、各セキュリティ機器の設定情報から汎用セキュリティポリシーを導出したとする。個々の汎用セキュリティポリシーは、それぞれ１台のセキュリティ機器の設定情報から導出されたものであるので、個々の汎用セキュリティポリシーの分析結果（要約結果）は、１台のセキュリティ機器において通過を許可されるパケットおよび通過を禁止されるパケットを示すことになる。この場合に、各汎用セキュリティポリシーの分析結果（要約結果）をさらにまとめ、複数のセキュリティ機器を全て通過できるパケットやあるセキュリティ機器で通過を禁止されるパケットを把握できるように分析することが、「セキュリティポリシーの統合」の一例である。

【０１８１】

以上のように、「セキュリティポリシーの統合」は汎用セキュリティポリシーの分析結果をさらにまとめて分析することである。従って、複数の汎用セキュリティポリシーの記述自体を統合するわけではない。

【０１８２】

セキュリティポリシー統合手段１１１は、セキュリティポリシー分析手段１０５から複数のセキュリティ機器の汎用セキュリティポリシーの分析結果を受け取り、その複数の分析結果を用いて統合処理を行う。セキュリティポリシー統合手段１１１は、統合処理を実行するときに、分析が行われたセキュリティ機能に対応する統合サブルーチン１１２を呼び出し、その統合サブルーチンに従って分析結果の統合処理を行う。

【０１８３】

次に動作について説明する。

図３５は、本実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者からセキュリティ機能の分析結果の統合要求を入力される（ステップＤ１）。また、データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者からセキュリティに関する分析要求も入力される（ステップＤ２）。ステップＤ２の処理は、ステップＢ１（図１６参照。）の処理と同様である。ステップＤ１、Ｄ２において各要求が入力されると、設定情報抽出手段１０１は通信ネットワーク１２０に接続されている少なくとも二つのセキュリティ機器１３０について、そのセキュリティ機器１３０に対応する設定情報抽出サブルーチン１０２を呼び出す。そして、その複数のセキュリティ機器１３０から設定情報を抽出、収集する（ステップＤ３）。続いて、汎用セキュリティポリシー生成手段１０３は、ステップＤ３で抽出、収集された設定情報に基づいて、セキュリティ機器１３０に対応するセキュリティポリシー生成サブルーチン１０４を呼び出し、セキュリティ機器１３０ごとに汎用セキュリティポリシーを生成する（ステップＤ４）。さらに、セキュリティポリシー分析手段１０５は、生成された汎用セキュリティポリシーの内容を分析し（ステップＤ５）、分析結果を入出力手段１１０から出力しシステム管理者に提示する（ステップＤ６）。ステップＤ３～Ｄ６の各処理は、第２の実施の形態におけるステップＢ２～Ｂ５の各処理と同様の処理である。

【０１８４】

次に、セキュリティポリシー統合手段１１１は、ステップＤ５で分析が行われたセキュ

リティ機能ごとに、分析結果を用いて統合を行い、分析結果を統合した結果を入出力手段１１０から出力する（ステップＤ７）。統合を実行するときの具体的動作については後述する。統合結果を出力する場合、例えば、入出力手段１１０に含まれるディスプレイ装置に統合結果を表示出力すればよい。

【０１８５】

次に、統合結果の表示について説明する。また、ここでは、汎用セキュリティポリシーの分析としてパケットフィルタリング機能について定めた汎用セキュリティポリシーの要約を行い、その要約結果の統合結果を表示する場合を例に説明する。セキュリティポリシー統合手段１１１は、複数の分析結果を統合した統合結果のみをディスプレイ装置に表示してもよい。例えば、セキュリティポリシー分析手段１０５がパケットフィルタリング機能に関する要約（分析）を行った場合、セキュリティポリシー統合手段１１１は、あるセキュリティ機器Ｔ１のパケットフィルタリング機能の分析結果（要約結果）と、別のセキュリティ機器Ｔ２のパケットフィルタリング機能の分析結果（要約結果）の統合結果をディスプレイ装置に表示してもよい。なお、本例における統合結果は、例えば、図２４等に例示する２次元平面データとしてディスプレイ装置に表示される。

【０１８６】

また、セキュリティポリシー統合手段１１１は、個々の分析結果とそれらの分析結果を統合した統合結果とを並べて表示してもよい。例えば、あるセキュリティ機器Ｔ１のパケットフィルタリング機能の分析結果と、別のセキュリティ機器Ｔ２のパケットフィルタリング機能の分析結果と、その二つの分析結果の統合結果とを並べてディスプレイ装置に表示してもよい。

【０１８７】

なお、セキュリティポリシー分析手段１０４による各セキュリティ機器のセキュリティ機能の分析結果を並べて表示して、システム管理者に分析結果の統合結果の判断を促すようにしてもよい。例えば、あるセキュリティ機器Ｔ１のパケットフィルタリング機能の分析結果および別のセキュリティ機器Ｔ２のパケットフィルタリング機能の分析結果をディスプレイ装置に表示して、二つの分析結果を統合した場合の統合結果の導出をシステム管理者に促してもよい。ただし、この場合、データ処理装置１００自身が分析結果の統合を行うわけではないので、データ処理装置１００は、セキュリティポリシー統合手段１１１を備えていなくてもよい。すなわち、分析結果を並べて表示して、システム管理者に分析結果の統合結果の判断を促す実施形態は、第２の実施の形態（図１５に示す構成）により実現可能である。

【０１８８】

また、セキュリティポリシー統合手段１１１は、統合の過程を段階的に表示してもよい。例えば、複数のセキュリティ機器Ｔ１～Ｔ３を全て通過できるパケットやセキュリティ機器Ｔ１～Ｔ３のいずれかで通過禁止とされるパケットを把握できるようにするために、あるセキュリティ機器Ｔ１のパケットフィルタリング機能の分析結果と、別のセキュリティ機器Ｔ２、Ｔ３それぞれのパケットフィルタリング機能の分析結果との統合結果を表示するものとする。この場合、セキュリティポリシー統合手段１１１は、まずセキュリティ機器Ｔ１の分析結果を表示し、次に、セキュリティ機器Ｔ１の分析結果とセキュリティ機器Ｔ２の分析結果との統合結果を表示し、続いて、各セキュリティ機器Ｔ１～Ｔ３の各分析結果の統合結果を表示してもよい。

【０１８９】

このように段階的に表示を行う場合、セキュリティポリシー統合手段１１１は、既に表示した分析結果（または分析結果の統合結果）とは異なる内容となる箇所が生じたときには、その箇所を特定の表示態様で表示してもよい。例えば、その箇所を特定の色で表示したり、その箇所を点滅させて表示してもよい。例えば、最初にセキュリティ機器Ｔ１の分析結果を、図２４に例示する場合と同様に２次元平面データとして表示したとする。そして、セキュリティ機器Ｔ１の分析結果である２次元平面データにおいて、ある領域Ｃに”accept”が割り当てられているとする。そして、セキュリティ機器Ｔ２の分析結果である

２次元平面データでは、領域Ｃに”deny”が割り当てられているとする。このとき、セキュリティ機器Ｔ１，Ｔ２の各分析結果の統合結果では、領域Ｃに”deny”が割り当てられる。この場合、セキュリティポリシー統合手段１１１は、セキュリティ機器Ｔ１の分析結果とセキュリティ機器Ｔ１，Ｔ２の分析結果の統合結果のいずれか片方あるいは両方における領域Ｃの部分を特定の色で表示したり、点滅させて表示してもよい。また、セキュリティ機器Ｔ１，Ｔ２の各分析結果の統合結果として表示した２次元平面データでは、領域Ｄに”accept”が割り当てられているとする。そして、セキュリティ機器Ｔ３の分析結果である２次元平面データでは、領域Ｄに”deny”が割り当てられているとする。このとき、セキュリティ機器Ｔ１～Ｔ３の各分析結果の統合結果では、領域Ｄに”deny”が割り当てられる。この場合、セキュリティポリシー統合手段１１１は、セキュリティ機器Ｔ１，Ｔ２の分析結果の統合結果とセキュリティ機器Ｔ１～Ｔ３の分析結果の統合結果のいずれか片方あるいは両方における領域Ｄの部分を特定の色で表示したり、点滅させて表示してもよい。このように表示することによって、統合過程において、既に表示した分析結果（または分析結果の統合結果）とは異なる内容となる箇所をシステム管理者に分かり易く提示することができる。

【０１９０】

さらに、セキュリティポリシー統合手段１１１は、図２４等に例示する２次元平面データを並べて表示するだけでなく、汎用セキュリティポリシーのうち、統合の過程で一致していない箇所に対応する部分（例えばPolicyGroupに含まれるPolicyやPolicyRule）も表示してよい。上記の例の場合、セキュリティ機器Ｔ１の汎用セキュリティポリシーのうち、領域Ｃおよび領域Ｄに関する記述部分（PolicyあるいはPolicyRule）と、セキュリティ機器Ｔ２の汎用セキュリティポリシーのうち、領域Ｃと領域Ｄに関する記述部分（PolicyあるいはPolicyRule）と、セキュリティ機器Ｔ３の汎用セキュリティポリシーのうち、領域Ｃと領域Ｄに関する記述部分（PolicyあるいはPolicyRule）とをそれぞれ表示してもよい。このような表示によって、個々の分析結果と各分析結果の統合結果との相異箇所に対応するPolicyやPolicyRuleをシステム管理者に提示することができる。

【０１９１】

なお、上記の各例において、セキュリティ機器Ｔ１～Ｔ３は、異なる機種であっても、同一の機種であってもよい。また、統合処理は、二つないし三つのセキュリティ機器のセキュリティ機能の分析結果の統合のみに限定されない。四つ以上のセキュリティ機器のセキュリティ機能の分析結果を統合してもよい。

【０１９２】

次に、統合処理における具体的動作を説明する。以下の説明においても、汎用セキュリティポリシーの分析としてパケットフィルタリング機能について定めた汎用セキュリティポリシーの要約を行い、その分析結果（要約結果）の統合を行う場合を例にして説明する。

【０１９３】

図３６は、パケットフィルタリングを行うセキュリティ機器Ｔ１，Ｔ２を含むネットワークシステムの例を示す。ネットワークＡには、”10.56.100.0 ”から”10.56.100.255 ”までのＩＰアドレスが割り当てられている。ネットワークＢには、”172.16.10.0 ”から”172.16.10.255 ”までのＩＰアドレスが割り当てられている。ネットワークＣは、ネットワークＢに包含され、”172.16.10.224 ”から”172.16.10.255 ”までのＩＰアドレスが割り当てられている。また、ネットワークＡとネットワークＢとの境界にはセキュリティ機器Ｔ１が設けられている。同様に、ネットワークＢのうちのネットワークＣ以外の部分と、ネットワークＣとの境界にはセキュリティ機器Ｔ２が設けられている。セキュリティ機器Ｔ１は、パケットフィルタリングソフトウェアＰ１を搭載し、セキュリティ機器Ｔ２は、パケットフィルタリングソフトウェアＰ２を搭載している。

【０１９４】

図３７は、セキュリティ機器Ｔ１から抽出した設定情報に基づいて生成された汎用セキュリティポリシーの例を示す。図３８は、セキュリティ機器Ｔ２から抽出した設定情報に

基づいて生成された汎用セキュリティポリシーの例を示す。

【０１９５】

図３７では、一つの PolicyGroup内に二つのPolicyが記述された汎用セキュリティポリシーを例示している。最初に記述されたPolicyは、送信元ＩＰアドレスが”172.16.10.192 ”から”172.16.10.255 ”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲であるパケットは”deny”とすることを示している。最後尾のPolicyは、送信元ＩＰアドレスが”172.16.10.0 ”から”172.16.10.255 ”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲であるパケットは”accept”とすることを示している。また、Policy結合アルゴリズムは"first-applicable"となっている。従って、ネットワークＣを含むネットワークＢと、ネットワークＡとのパケットの通過を禁止している。図３９は、図３７に示す汎用セキュリティポリシーの分析結果の出力画面を示す。

【０１９６】

図３８では、一つの PolicyGroup内に一つのPolicyが記述された汎用セキュリティポリシーを例示している。ここに記述されたPolicyは、送信元ＩＰアドレスが”172.16.10.224 ”から”172.16.10.255 ”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲であるパケットは”accept”とすることを示している。すなわち、ネットワークＡ，Ｃ間のパケットの通過を許可している。図４０は、図３８に示す汎用セキュリティポリシーの分析結果の出力画面を示す。

【０１９７】

ステップＤ１，Ｄ２における各要求の入力後、設定情報抽出手段１０１がセキュリティ機器Ｔ１，Ｔ２から設定情報を抽出し（ステップＤ３）、汎用セキュリティポリシー生成手段１０３が、図３７および図３８に示す汎用セキュリティポリシーを生成したとする（ステップＤ４）。さらに、セキュリティポリシー分析手段１０５が、各セキュリティ機器毎に（すなわち、図３７および図３８に示す各汎用セキュリティポリシー毎に）パケットフィルタリング機能に関する分析（要約）を行い、各分析結果（図３９および図４０参照。）を表示したとする（ステップＤ５，Ｄ６）。このとき、セキュリティポリシー分析手段１０５は、各分析結果をセキュリティポリシー統合手段１１１に出力する。分析結果は、例えば、汎用セキュリティポリシーの記述形式で記述される。ただし、分析結果の記述形式は特に限定されず、他の記述形式で記述されていてもよい。汎用セキュリティポリシーの記述形式等で記述された分析結果に基づいてディスプレイ装置上に２次元平面データを表示すると、図３９や図４０に例示する２次元平面データが表示される。

【０１９８】

図４１は、パケットフィルタリング機能について定めた汎用セキュリティポリシーの分析結果の統合処理（図３５に示すステップＤ７）の例を示すフローチャートである。図４１に示す統合処理は、パケットフィルタリング機能を持つ複数のセキュリティ機器が連結されている場合に、両端に位置するセキュリティ機器の外側の二つのネットワーク間でどのようなパケットが通過を許可され、どのようなパケットが通過を禁止されるのかを、連結されたパケットフィルタリング機能を持つ複数のセキュリティ機器の分析結果を統合して判定する処理である。例えば、図３６に示すネットワークシステムにおいて、パケットフィルタリング機能を有するセキュリティ機器Ｔ１，Ｔ２の外側の二つのネットワークＡ，Ｃ間で、どのようなパケットが通過を許可され、どのようなパケットが通過を禁止されるのかを判定する。パケットフィルタリング機能を持つセキュリティ機器が複数連結している場合には、このように個々のセキュリティ機器の分析結果を統合しなければ、両端の二つのネットワーク間でどのようなパケットが通過を許可され、どのようなパケットが通過を禁止されるのか判定することはできない。図４１に示すフローチャートに従って、複数の分析結果を統合する例を、図３９および図４０の分析結果例を用いて説明する。

【０１９９】

まず、セキュリティポリシー統合手段１１１は、複数の分析結果（パケットフィルタリング機能の設定について定めた複数の汎用セキュリティポリシーの分析結果）をセキュリ

ティ機器の連結順にソートする（ステップｄ１）。ソートする際、セキュリティ機器の連結方向は問わない。例えば、図３６に示す例では、２台のセキュリティ機器Ｔ１，Ｔ２が連結されている。この場合、各セキュリティ機器Ｔ１，Ｔ２それぞれから得られた汎用セキュリティポリシーの分析結果を、Ｔ１，Ｔ２の順にソートしてもよいし、Ｔ２，Ｔ１の順にソートしてもよい。また、仮に、図３６に示す例において、セキュリティ機器Ｔ１の次にセキュリティ機器Ｔ３が連結され、その次にセキュリティ機器Ｔ２が連結されているとする。この場合、各セキュリティ機器Ｔ１～Ｔ３それぞれから得られた汎用セキュリティポリシーの分析結果を、Ｔ１，Ｔ３，Ｔ２の順にソートしてもよいし、Ｔ２，Ｔ３，Ｔ１の順にソートしてもよい。ただし、Ｔ３，Ｔ１，Ｔ２等の順は、連結順に該当しないので、このような順にソートすることはない。

【０２００】

また、図３６に示すように、連結されるセキュリティ機器が２台の場合、ソート順は問わないので、セキュリティポリシー統合手段１１１がソート順を決定してよい。連結されるセキュリティ機器が３台以上存在する場合には、例えば、セキュリティポリシー統合手段１１１がディスプレイ装置（入出力手段１１０に含まれる。）に、ソート順の指定を促す画面を表示し、セキュリティ管理者から入出力手段１１０を介してソート順を指定されてもよい。このとき、セキュリティポリシー統合手段１１１は、指示された順に分析結果をソートする。

【０２０１】

ステップｄ１の後、セキュリティポリシー統合手段１１１は、ステップｄ１でソートされた分析結果から最初の分析結果と２番目の分析結果を取得する（ステップｄ２）。本例では統合対象となる分析結果は二つ（図３９に示す２次元平面データを表示するためのデータおよび図４０に示す２次元平面データを表示するためのデータ）であるので、この二つの分析結果を取得する。

【０２０２】

次に、セキュリティポリシー統合手段１１１は、二つの分析結果によって表される２次元平面データの領域について、”accept”を真、”deny”を偽としてＡＮＤ計算（論理積計算）を行う（ステップｄ３）。ＡＮＤ計算では、計算対象となる二つの値がともに真のときのみ計算結果も真となり、計算対象となる二つの値の少なくとも一方が偽であれば計算結果は偽となる。つまり、統合処理する二つの分析結果の領域について、ともに”accept”である領域のみ統合結果の領域も”accept”となり、少なくとも一方が”deny”である領域は統合によって”deny”となる。図３９および図４０に示すように表示される分析結果について統合処理を行った結果を図４２に示す。

【０２０３】

図４２はすべてのパケットの通過が禁止されていることを示している。つまり、連結しているセキュリティ機器Ｔ１とセキュリティ機器Ｔ２の外側の領域であるネットワークＡとネットワークＣの間ではいかなるパケットも通過できないことを意味する。

【０２０４】

この結果、ネットワークＣに接続されているセキュリティ機器Ｔ２に搭載されたパケットフィルタリングソフトウェアＰ２において、ネットワークＡとネットワークＣの通信を許可するように設定されているにもかかわらず、セキュリティ機器Ｔ１に搭載されたパケットフィルタリングソフトウェアＰ１において、ネットワークＡと（ネットワークＣを含む）ネットワークＢとの通信を禁止する設定がされているために、結局、ネットワークＡとネットワークＣとの通信は実現できないことを把握することができる。すなわち、セキュリティ管理者は、パケットフィルタリングソフトウェアＰ１の設定を、ネットワークＡとネットワークＣとの間のパケットの通過を許可するように変更すれば正しく通信できるようになることを容易に把握することができる。

【０２０５】

次に、セキュリティポリシー統合手段１１１は、まだ統合すべき分析結果があるか否かを判定する（ステップｄ４）。まだ統合すべき分析結果があればステップｄ５に移行し、

なければ統合処理を終了する。この結果、各分析結果の統合結果が得られる。本例では統合する分析結果が二つであるので、ここで統合処理が終了する。

【０２０６】

統合する分析結果が三つ以上ある場合には、セキュリティポリシー統合手段１１１は、ステップｄ４の後、次の分析結果を取得する。（ステップｄ５）。そして、既に導出している統合結果と新たに取得した分析結果についてステップｄ３と同様の領域計算を行う（ステップｄ６）。ステップｄ６の後、セキュリティポリシー統合手段１１１は、全ての分析結果について統合（具体的にはＡＮＤ計算）が終了したかを判定する（ステップｄ７）。全ての分析結果について統合が終了しているならば、処理を終了する。この結果、各分析結果の統合結果が得られる。全ての分析結果について統合が終了しておらず、まだ統合すべき分析結果があるならば、ステップｄ５に移行し、ステップｄ５以降の動作を繰り返す。

【０２０７】

次に、第４の実施の形態の変形例について説明する。複数のパケットフィルタリング機能を持つセキュリティ機器が連結されている場合に、そこに含まれる一部のセキュリティ機器においてパケットフィルタリング機能と同時にアドレス変換機能によってアドレス変換を行う場合がある。この場合には、図４１に示すフローチャートを拡張し、ステップｄ２およびステップｄ５で分析結果を取得した後、すなわちステップｄ３およびステップｄ６で統合処理を行う前に、パケットフィルタリング分析結果に対してアドレス変換機能について定めたポリシー（ルール）を適用すればよい。以下、このポリシー（ルール）をアドレス変換ポリシーと記す。アドレス変換ポリシーを適用することによって、２次元平面データ上の領域が変換されることになる。さらに、全ての分析結果についての統合処理が終了した後（ステップｄ４においてＮＯ、またはステップｄ７においてＹＥＳと判定された後）、アドレス変換ポリシーを逆に適用し、変換された領域を元に戻せばよい。この場合のフローチャートを図４３に示す。図４３では、図４１に示すフローチャートのステップｄ２，ｄ３の間に、パケットフィルタフィルタリング機能に関する分析結果に対してアドレス変換ポリシーを適用するステップｄ２－１が追加されている。同様に、図４１に示すフローチャートのステップｄ５，ｄ６の間に、パケットフィルタフィルタリング機能に関する分析結果に対してアドレス変換ポリシーを適用するステップｄ５－１が追加されている。さらに、ステップｄ４においてＮＯ、またはステップｄ７においてＹＥＳと判定された後に、統合結果に対してアドレス変換ポリシーを逆適用するステップｄ８が追加されている。

【０２０８】

次に、図４３のフローチャートに従って、パケットフィルタリングとアドレス変換を同時に行うネットワークシステムにおいて、パケットフィルタリング機能に関する分析結果を統合する例について説明する。

【０２０９】

まず、パケットフィルタリングとアドレス変換を同時に行うネットワークシステムの例について説明する。図４４は、このようなネットワークシステムの例を示す。ネットワークＡには、”10.56.100.0 ”から”10.56.100.255 ”までのＩＰアドレスが割り当てられている。ネットワークＢには、”172.16.10.0 ”から”172.16.10.255 ”までのＩＰアドレスが割り当てられている。ネットワークＤには、”192.168.1.0 ”から”192.168.1.255 ”までのＩＰアドレスが割り当てられている。また、ネットワークＡとネットワークＢとの境界にはセキュリティ機器Ｔ１が設けられ、ネットワークＢとネットワークＤとの境界にはセキュリティ機器Ｔ２が設けられている。セキュリティ機器Ｔ１は、パケットフィルタリングソフトウェアＰ１を搭載している。また、セキュリティ機器Ｔ２は、アドレス変換機能を含むパケットフィルタリングソフトウェアＰ２を搭載している。本例では、セキュリティ機器Ｔ２は、ソフトウェアＰ２に従い、以下のようにアドレス変換を実行する。すなわち、送信元ＩＰアドレスが”192.168.1.0 ”から”192.168.1.255 ”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲である

パケットの送信元ＩＰアドレスを”172.16.10.10”に変換する。

【０２１０】

図４５は、セキュリティ機器Ｔ１から抽出した設定情報に基づいて生成された汎用セキュリティポリシーの例を示す。図４６は、セキュリティ機器Ｔ２から抽出した設定情報に基づいて生成された汎用セキュリティポリシーの例を示す。

【０２１１】

図４５では、一つの PolicyGroup内に一つのPolicyが記述された汎用セキュリティポリシーを例示している。ここに記述されたPolicyは、送信元ＩＰアドレスが”172.16.10.0”から”172.16.10.255”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0”から”10.56.100.255”までの範囲であるパケットは”accept”とすることを示している。図４７は、図４５に示す汎用セキュリティポリシーの分析結果の出力画面を示す。

【０２１２】

図４６では、一つの PolicyGroup内に二つのPolicyが記述された汎用セキュリティポリシーを例示している。最初に記述されたPolicyは、送信元ＩＰアドレスが”192.168.1.0”から”192.168.1.255”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0”から”10.56.100.255”までの範囲であるパケットは”accept”とすることを示している。最後尾に記述されたPolicyはアドレス変換に関するPolicyである。このPolicyは、送信元ＩＰアドレスが”192.168.1.0”から”192.168.1.255”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0”から”10.56.100.255”までの範囲であるパケットの送信元ＩＰアドレスを”172.16.10.10”に変換することを示している。

【０２１３】

図４６に示す汎用セキュリティポリシーにおいて、アドレス変換機能に関するPolicyを考慮せずに、パケットフィルタリング機能に関するPolicyのみを分析すると、その分析結果は、図４８に示す２次元平面データとして表すことができる。仮に、図４８に示すように表される分析結果と、図４７に示すように表される分析結果とを統合する場合について検討する。この場合、図４８に示す２次元平面データで”accept”とされている領域Ｓ（具体的には、送信元ＩＰアドレスが”192.168.1.0”から”192.168.1.255”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0”から”10.56.100.255”までの範囲である領域）が、図４７に示す２次元平面データでは”deny”とされている。従って、統合により図４８に示す領域Ｓは、”deny”となってしまう。しかし、実際には、アドレス変換が行われ、送信元ＩＰアドレスが”192.168.1.0”から”192.168.1.255”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0”から”10.56.100.255”までの範囲であるパケットの送信元ＩＰアドレスは、”172.16.10.10”に変換される。すなわち、実際には、図４８に示す領域Ｓの送信元ＩＰアドレスは”172.16.10.10”に変換され、このアドレス変換を行った場合における統合結果では、領域Ｓの変換後の領域は、”accept”のまま維持される。

【０２１４】

このようなアドレス変換を行う場合の動作を、図４３に示すフローチャートに従って説明する。まず、セキュリティポリシー統合手段１１１は、各分析結果をセキュリティ機器の連結順にソートし、最初と二番目の分析結果を取得する（ステップｄ１，ｄ２）。この処理は、図４１に示したステップｄ１，ｄ２の処理と同様である。続いて、セキュリティポリシー統合手段１１１は、汎用セキュリティポリシーにアドレス変換機能に関するPolicyが記述されている場合には、その汎用セキュリティポリシーの分析結果に対して、アドレス変換機能に関するPolicyを適用し、２次元平面データ上の領域を変換する（ステップｄ２－１）。例えば、上記の例では、図４６に示すアドレス変換ポリシー（最後尾に記述されたPolicy）を、図４８に示す２次元平面データ上の領域Ｓに適用し、領域Ｓのアドレス（本例では送信元ＩＰアドレス）を変換する。図４６に示す最後尾のPolicyでは、送信元ＩＰアドレスが”192.168.1.0”から”192.168.1.255”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0”から”10.56.100.255”までの範囲であるパケットの送信元ＩＰアドレスを”172.16.10.10”に変換することを定めている。図４８に例示する領域

Ｓは、送信元ＩＰアドレスが ”192.168.1.0 ”から”192.168.1.255 ”までの範囲であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲を示している。従って、領域Ｓは、送信元ＩＰアドレスが”172.16.10.10”であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲に変換される。この変換後の２次元平面データを図４９に示す。

【０２１５】

なお、Policy内のActionタグに”snat”または”dnat”が記載されているならば、そのPolicyは、アドレス変換機能に関するPolicyであると判定することができる。

【０２１６】

セキュリティポリシー統合手段１１１は、汎用セキュリティポリシーの分析結果に対してステップｄ２－１の処理を行った場合には、ステップｄ２－１の処理後の分析結果を用いて、ステップｄ３の統合処理（ＡＮＤ計算）を行う。本例では、図４８および図４９のように表示される分析結果についてＡＮＤ計算を行う。本例では、このＡＮＤ計算を行った結果得られる統合結果は、図４９と同一の２次元平面データとして表示できる。

【０２１７】

ステップｄ３の後、セキュリティポリシー統合手段１１１は、まだ統合すべき分析結果があるか否かを判定する（ステップｄ４）。まだ統合すべき分析結果があればステップｄ５に移行し、なければステップｄ８に移行する。本例では、統合する分析結果が二つであるので、ステップｄ８に移行する。

【０２１８】

ステップｄ８では、ステップｄ２－１（または、後述するステップｄ５－１）で適用したアドレス変換ポリシーを逆に適用して、アドレス変換された領域を元の領域に戻す。この結果、最終的な統合結果が得られる。本例では、ステップｄ３の統合結果として得られた２次元平面データ（図４９と同一の２次元平面データ）において、送信元ＩＰアドレスが”172.16.10.10”であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲である領域は、アドレス変換ポリシーで指定された変換後の領域に一致する。従って、送信元ＩＰアドレスが”172.16.10.10”であり、宛先ＩＰアドレスが”10.56.100.0 ”から”10.56.100.255 ”までの範囲である領域に対して、ステップｄ２－１で適用したアドレス変換ポリシーを逆に適用する。この結果、図４８に示す２次元平面データが得られる。この２次元平面データを表す統合結果が、最終的な統合結果である。

【０２１９】

また、ステップｄ５では、図４１に示すステップｄ５と同様に、次の分析結果を取得する。セキュリティポリシー統合手段１１１は、ステップｄ５で取得した分析結果に対応する汎用セキュリティポリシーにアドレス変換機能に関するPolicyが記述されている場合には、ステップｄ５で取得した分析結果に対して、アドレス変換機能に関するPolicyを適用し、２次元平面データ上の領域を変換する（ステップｄ５－１）。この処理は、ステップｄ２－１と同様の処理である。そして、セキュリティポリシー統合手段１１１は、既に導出している統合結果と、新たに取得した分析結果（ステップｄ５－１の処理を行った場合には、ステップｄ５－１の処理後の分析結果）について、ステップｄ３と同様の領域計算を行う（ステップｄ６）。ステップｄ６の後、セキュリティポリシー統合手段１１１は、全ての分析結果について統合（具体的にはＡＮＤ計算）が終了したかを判定する（ステップｄ７）。全ての分析結果について統合が終了しているならば、ステップｄ８に移行する。ステップｄ８の処理により、最終的な統合結果が得られる。全ての分析結果について統合が終了しておらず、まだ統合すべき分析結果があるならば、ステップｄ５に移行し、ステップｄ５以降の動作を繰り返す。

【０２２０】

次に、本実施の形態の効果について説明する。本実施の形態では、セキュリティ機器に固有の表現を持つ設定情報からセキュリティ機器の種類によらない汎用セキュリティポリシーを生成し、その分析を行った後、分析結果の統合を行うように構成されている。そのため、同じセキュリティ機能を持つセキュリティ機器であれば異なる機器間でも機器固有

の設定記述の形式を意識することなく設定内容の統合結果をシステム管理者に提示することができる。例えば、パケットフィルタリングを行う複数のセキュリティ機器が存在する場合に、各セキュリティ機器の分析結果（要約結果）を統合することにより、複数のセキュリティ機器を全て通過できるパケットやあるセキュリティ機器で通過を禁止されるパケットをシステム管理者に提示することができる。また、統合処理を行わず個別に分析しただけでは検出できない設定不備（例えば、複数のセキュリティ機器を全て通過できるパケットが存在しない等の不備）などを容易に検出することができる。

【０２２１】

なお、ステップＤ３（図３５参照。）では、複数のセキュリティ機器１３０から設定情報を抽出、収集する場合を示した。予め生成された汎用セキュリティポリシーの分析結果が存在する場合には、ステップＤ３において、少なくとも一つのセキュリティ機器１３０から設定情報を抽出、収集すればよい。そして、ステップＤ４で少なくとも一つの汎用セキュリティポリシーを生成し、ステップＤ５で少なくとも一つの分析結果を生成すればよい。なお、予め生成された分析結果は、例えば、記憶装置（図３４において図示せず。）に記憶させておけばよい。そして、ステップＤ７で、その記憶装置から予め生成された分析結果を読み込み、ステップＤ５で得られた分析結果と統合してもよい。この場合、予め分析結果を記憶する記憶装置が、分析結果記憶手段に相当する。

【０２２２】

実施の形態５．

次に、本発明によるセキュリティポリシー管理システムの第５の実施の形態について説明する。図５０は、本発明によるセキュリティポリシー管理システムの第５の実施の形態を示すブロック図である。第２の実施の形態と同様の構成部については、図１５と同一の符号を付して説明を省略する。また、第２の実施の形態と同様の構成部の動作は、第２の実施の形態と同様である。

【０２２３】

第５の実施の形態において、データ処理装置１００は、第２の実施の形態で示した設定情報抽出手段１０１、汎用セキュリティポリシー生成手段１０３およびセキュリティポリシー分析手段１０５に加え、セキュリティポリシー連携手段１１３を含んでいる。セキュリティポリシー連携手段１１３は、例えば、プログラムに従って動作するＣＰＵによって実現される。プログラムには、サブルーチンとして少なくとも一つの連携サブルーチン１１４が含まれる。個々の連携サブルーチンは、各セキュリティ機器１３０によって実現される個々のセキュリティ機能の組み合わせと対応する。例えば、ある連携サブルーチン１１４は、パケットフィルタリング機能とＮＩＤＳ（Network Intrusion Detection System：ネットワーク型侵入検知システム）による侵入検知機能（パケットモニタリング機能）との組み合わせと対応する。別の連携サブルーチン１１４は、他のセキュリティ機能の組み合わせと対応する。また、連携サブルーチン１１４は、複数のセキュリティ機能の組み合わせと対応するので、個々の連携サブルーチンは、複数のセキュリティポリシー分析サブルーチン１０６と対応することになる。各連携サブルーチン１１４は、データ処理装置１００が備える記憶装置（図５０において図示せず。）に予め記憶させておく。

【０２２４】

セキュリティポリシー連携手段１１３は、セキュリティポリシー分析手段１０５から汎用セキュリティポリシーと汎用セキュリティポリシーの分析結果とを受け取り、その汎用セキュリティポリシーや分析結果を用いて連携処理を実行する。連携処理では、あるセキュリティ機器の設定情報から導出された汎用セキュリティポリシー（またはその分析結果）と、別のセキュリティ機能を有する他のセキュリティ機器の設定情報から導出された汎用セキュリティポリシー（またはその分析結果）とを用いて連携処理を行う。すなわち、連携処理の態様には、複数の分析結果により連携処理を行う態様や、ある汎用セキュリティポリシーと、他の汎用セキュリティポリシーの分析結果とにより連携処理を行う態様がある。また、複数の汎用セキュリティポリシーにより連携処理を行ってもよい。

【０２２５】

セキュリティポリシー連携手段１１３がセキュリティポリシー分析手段１０５から汎用セキュリティポリシーや汎用セキュリティポリシーの分析結果を受け取る場合、互いに異なるセキュリティ機能に関する汎用セキュリティポリシー（またはその分析結果）を受け取る。例えば、セキュリティポリシー連携手段１１３は、パケットフィルタリング機能について定めた汎用セキュリティポリシーと、パケットモニタリング機能について定めた汎用セキュリティポリシーの分析結果とを受け取る。なお、セキュリティポリシー分析手段１０５は、分析結果をセキュリティポリシー連携手段１１３に出力する場合、分析対象となった汎用セキュリティポリシーも併せてセキュリティポリシー連携手段１１３に出力する。従って、セキュリティポリシー連携手段１１３は、分析結果を受け取る場合、分析対象となった汎用セキュリティポリシーも受け取る。上記の例では、パケットモニタリング機能について定めた汎用セキュリティポリシーの分析結果を受け取る場合、その分析結果と併せて、パケットモニタリング機能について定めた汎用セキュリティポリシーも受け取る。

【０２２６】

既に説明したように、セキュリティポリシー連携手段１１３は、セキュリティポリシー分析手段１０５から汎用セキュリティポリシーや汎用セキュリティポリシーの分析結果を受け取る場合、互いに異なるセキュリティ機能に関する汎用セキュリティポリシー（またはその分析結果）を受け取る。セキュリティポリシー連携手段１１３は、そのセキュリティ機能の組み合わせに対応する連携サブルーチン１１４を呼び出し、その連携サブルーチンに従って連携処理を行う。例えば、上記の様に、パケットフィルタリング機能について定めた汎用セキュリティポリシーと、パケットモニタリング機能について定めた汎用セキュリティポリシーの分析結果とを受け取った場合、パケットフィルタリング機能とパケットモニタリング機能の組み合わせに対応する連携サブルーチン１１４を呼び出し、その連携サブルーチンに従って連携処理を行う。

【０２２７】

以下の説明では、分析結果が汎用セキュリティポリシーの記述形式で記述されているものとする。

【０２２８】

本発明において、「連携」とは、異なるセキュリティ機能を持つ複数のセキュリティ機器からそれぞれ導出された汎用セキュリティポリシーまたは汎用セキュリティポリシーの分析結果を参照し、それら複数のセキュリティ機器の関連性を見出すことにより、異なるセキュリティ機能を有するセキュリティ機器の汎用セキュリティポリシーを相互に関連付けることである。例えば、それぞれ異なるセキュリティ機能を持つ複数のセキュリティ機器について、それらセキュリティ機器の汎用セキュリティポリシーや汎用セキュリティポリシーの分析結果を参照することによって、それぞれの汎用セキュリティポリシーを個別に分析するだけでは検出不可能な、異なるセキュリティ機能を持つセキュリティ機器間の不整合検出などを行うことができる。

【０２２９】

具体的例を説明する。パケットフィルタリング機能についての記述を含む汎用セキュリティポリシーでパケットの通過許可が記述されている場合には、ＮＩＤＳによる監視を十分に行うことが好ましい。逆に、汎用セキュリティポリシーでパケットの通過禁止が記述されている場合には、ＮＩＤＳによる監視を行う必要がない。上記の「連携」を行うことにより、例えば、ＮＩＤＳによる監視が十分でない、あるいは、ＮＩＤＳによって過剰な（必要以上な）監視を行っている等の不整合検出を行うことができる。

【０２３０】

連携は、予め定められた連携方針に従って実行される。例えば、連携サブルーチン１１４は、ある連携方針に従って予め作成され、セキュリティポリシー連携手段１１３は、その連携サブルーチンに従って連携処理を行う。連携方針の例として、例えば、「セキュリティ機器Ａとセキュリティ機器Ｂに設定されたルール間に矛盾する内容があるかどうかを確認する。」等の連携方針が挙げられる。このような連携方針に基づいて作成された連携

サブルーチン１１４に従って、セキュリティポリシー連携手段１１３は、「パケットフィルタリング機能でパケットの通過を許可しているにもかかわらず、ＮＩＤＳによる監視が十分でない。」、「パケットフィルタリング機能でパケットの通過を禁止しているにもかかわらず、ＮＩＤＳにより不必要な監視を行っている。」等の不整合を検出する。

【０２３１】

次に動作について説明する。

図５１は、本実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者から汎用セキュリティポリシーや汎用セキュリティポリシーの分析結果の連携要求を入力される（ステップＥ１）。また、データ処理装置１００は、入出力手段１１０を介して、例えばシステム管理者からセキュリティに関する分析要求も入力される（ステップＥ２）。ステップＥ２の処理は、ステップＢ１（図１６参照。）の処理と同様である。ステップＥ１、Ｅ２において各要求が入力されると、設定情報抽出手段１０１は通信ネットワーク１２０に接続されている少なくとも二つのセキュリティ機器１３０について、そのセキュリティ機器１３０に対応する設定情報抽出サブルーチン１０２を呼び出す。そして、その複数のセキュリティ機器１３０から設定情報を抽出、収集する（ステップＥ３）。続いて、汎用セキュリティポリシー生成手段１０３は、ステップＥ３で抽出、収集された設定情報に基づいて、セキュリティ機器１３０に対応するセキュリティポリシー生成サブルーチン１０４を呼び出し、セキュリティ機器１３０ごとに汎用セキュリティポリシーを生成する（ステップＥ４）。さらに、セキュリティポリシー分析手段１０５は、生成された汎用セキュリティポリシーの内容を分析し（ステップＥ５）、分析結果を入出力手段１１０から出力しシステム管理者に提示する（ステップＥ６）。ステップＥ３～Ｅ６の各処理は、第２の実施の形態におけるステップＢ２～Ｂ５の各処理と同様の処理である。

【０２３２】

次に、セキュリティポリシー連携手段１１３は、ステップＥ４で生成された汎用セキュリティポリシーまたはステップＥ５で分析が行われたセキュリティ機能の分析結果を用いて連携処理を行い、連携処理の結果を入出力手段１１０から出力する（ステップＥ７）。連携処理における具体的動作については後述する。

【０２３３】

なお、連携処理は、セキュリティ機能の異なる二つのセキュリティ機器から導出された汎用セキュリティポリシーまたは分析結果を用いて行われる場合に限定されない。セキュリティ機能の異なる三つ以上のセキュリティ機器から導出された汎用セキュリティ機器または分析結果を用いて連携処理を実行してもよい。

【０２３４】

連携処理は、汎用セキュリティポリシーまたは汎用セキュリティポリシーの分析結果に記述されたオブジェクトおよび属性を関連付けることによって行う。既に説明したように、分析結果は、汎用セキュリティポリシーの記述形式で記述されているものとする。セキュリティポリシー連携の概念図を図５２に示す。図５２に示されたセキュリティ機器Ａとセキュリティ機器Ｂは異なるセキュリティ機能を持つセキュリティ機器であるとする。セキュリティ機器Ａおよびセキュリティ機器Ｂからそれぞれ汎用セキュリティポリシーが生成され、必要に応じてセキュリティポリシー分析も行われたとする。このセキュリティポリシー分析結果は、汎用セキュリティポリシーの記述形式で出力されている。このとき、それぞれの汎用セキュリティポリシーの分析結果の中に同一のオブジェクト Obj.Xについての記述があったとする。この場合、異なるセキュリティ機能を持つセキュリティ機器Ａおよびセキュリティ機器Ｂから生成された汎用セキュリティポリシーの分析結果の間に、Obj.Xを介した関連付けを行う。

【０２３５】

図５２に示す例では、分析結果同士で、Obj.Xを介した関連付けを行う場合を示している。汎用セキュリティポリシーそのものと、他の汎用セキュリティポリシーの分析結果との関連づけを行ってもよい。例えば、セキュリティ機器Ａから導出した汎用セキュリティ

ポリシーと、セキュリティ機器Ｂから導出した汎用セキュリティポリシーの分析結果とにそれぞれObj.Xについての記述があったとする。この場合、例えば、セキュリティ機器Ａから導出した汎用セキュリティポリシーと、セキュリティ機器Ｂから導出した汎用セキュリティポリシーの分析結果とを関連付けてもよい。また、同様に、汎用セキュリティポリシー同士で関連付けを行ってもよい。

【０２３６】

次に、セキュリティポリシー連携の具体例について説明する。ここでは、セキュリティポリシー連携の具体例として、パケットフィルタリングに関するポリシー（ルール）とＮＩＤＳに関するポリシー（ルール）との不整合検出について説明する。以下、パケットフィルタリングに関するポリシー（ルール）をパケットフィルタリングポリシーと記し、ＮＩＤＳに関するポリシー（ルール）をＮＩＤＳポリシーと記す。

【０２３７】

まず、連携の具体例の説明の前提として、ＮＩＤＳ、ＮＩＤＳを表す動作モデル、ＮＩＤＳの機能を表現する汎用セキュリティポリシー、およびその汎用セキュリティポリシーに対する分析処理についてそれぞれ説明する。

【０２３８】

ＮＩＤＳは、ネットワークセグメント上を流れるパケットを監視し、不正なアクセスや異常状態を検知するものである。ＮＩＤＳにおける検知手法としては大きく二つに分類される。それぞれ「シグネチャ方式」と「統計方式」と呼ぶ。シグネチャ方式とは、過去に認識された攻撃パターンをデータベース化したものであり、一般的に一つのパケットパターンは一つのシグネチャとして管理される。パケットをキャプチャし、シグネチャと比較することによって攻撃パケットを検出する。統計方式とは、ＮＩＤＳを一定期間運用して通常運用時のシステムのプロファイルを作成し、以降運用していく過程で明らかにプロファイルと異なるアクティビティがあった場合に、それを異常状態として検出する。ＮＩＤＳでは主にシグネチャ方式の検出が用いられる。以下の説明においてもシグネチャ方式の検知を行うＮＩＤＳの利用を想定するものとする。

【０２３９】

また、ＮＩＤＳは不正アクセスを検出した場合に、ＮＩＤＳを管理するコンソール端末にアラートを通知したり、電子メールによってシステム管理者に不正アクセスの発生を通知したりすることができる。

【０２４０】

また、ＮＩＤＳ製品によってはシグネチャがその種類によってグループ化され、カテゴリと呼ばれる単位に分類されているものもある。

【０２４１】

図５３は、図５とは異なるセキュリティ機能の動作のモデルの例を示す説明図である。図５３では、主にＮＩＤＳなどの監視を行うセキュリティ機器の動作モデルを示す。このモデルで表されるセキュリティ機器の動作は、「 MonitoredObjectで表されるオブジェクトを監視し、監視状況に応じてReponseを出力する」動作である。

【０２４２】

図５３に示す動作モデルによってその動作を表現可能なセキュリティ機器として、ＮＩＤＳ、ファイル改ざん監視ソフトウェアを搭載した機器、ログ監視ソフトウェアを搭載した機器等がある。そして、これらのセキュリティ機器が有するセキュリティ機能として、パケットモニタリング機能、ファイル改ざん監視機能、ログ監視機能などがある。

【０２４３】

図５３に示す動作モデルを持つセキュリティ機器の汎用セキュリティポリシーで記述される項目について説明する。セキュリティ機能による動作は、 Function（監視を行うセキュリティ機能）、 MonitoredObject（監視対象となるオブジェクト）、 Responses（監視により、あるシグネチャに合致するパケットパターンが検知されたときのアクション）の組によって表現する。

【０２４４】

図５４は、ＮＩＤＳの汎用セキュリティポリシーの例を示す説明図である。
Policyタグに囲まれた範囲は、監視を行うセキュリティ機器の設定情報に含まれていた一つ一つのルールを表す。一組のPolicyタグに囲まれた範囲は、例えば「特定のイベントを引き起こすパケットを監視し、そのパケットが検出された場合にアラートを送信する。」等の一つのルールを表す。

【０２４５】

Targetタグに囲まれた範囲は、セキュリティ機器による動作を表すFunction（セキュリティ機能）、MonitoredObject （監視対象となるオブジェクト）、Responses （アクションの組）の組み合わせを表す。

【０２４６】

Functionタグに囲まれた範囲は、セキュリティ機能を表す子要素を持ち、孫要素でセキュリティ機能についての属性を指定する。セキュリティ機能を表す子要素として”PacketMonitoring”等があり、”PacketMonitoring”はパケットモニタリング機能を表している。また、孫要素の例として、後述のMonitoredObjectで指定するオブジェクトに対する監視について有効とするか無効とするかを表す”Enabled”がある。例えば、”Enabled”がfalse である場合、オブジェクトに対する監視を無効にすることを意味し、”Enabled”がtrueである場合、オブジェクトに対する監視を有効にすることを意味する。また、図５４に示す例では、Functionタグに囲まれた範囲には、”Enabled”の他に孫要素として”Priority”も記述される。この”Priority”は、アラートを出力したことをログに記録する場合におけるアラートの重要度を表す。図５４では”Priority”が”Low“として記述されているので、図５４に示すPolicy（ルール）に従ってアラートを出力し、ログにアラート出力を記録するときには、アラートの重要度として”Low“、すなわち重要度が低い旨も記録される。このように、ログに”Priority”の内容を記録することにより、ログの内容をアラートの重要度に応じて分類できるようにしている。

【０２４７】

MonitoredObject タグに囲まれた範囲は、監視対象となるオブジェクトを表す子要素を持つ。子要素の例としてＮＩＤＳではシグネチャによって監視する”SecurityEvent“などがある。MonitoredObject タグに囲まれた範囲に子要素として”SecurityEvent“が記述されている場合、シグネチャによる監視を実行することを意味する。また、”SecurityEvent“はさらにその子要素として、シグネチャによって監視するイベント名を記述する”EventName ”を持つ。図５４に示す例では、”EventName ”として、”FTP_get ”が記述されている。

【０２４８】

Responses タグに囲まれた範囲は、特定のイベントが検出された場合のアクションを表す。このとき複数のアクションを同時に行うことが可能であることが多いので、Responses タグは子要素として複数のResponseタグを持つ。それぞれのResponseタグは、一つのアクションを表す子要素を持ち、孫要素でそのアクションの属性を指定する。アクションの例としてはイベントの検出を電子メールで管理者などに通知する”EMAIL“や、ＳＮＭＰトラップによってＳＮＭＰマネージャにアラートを発する”SNMP”等がある。”EMAIL“の属性として、メールサーバのＩＰアドレスやメールの送信先アドレスを指定する。また、”SNMP”の属性として、ＳＮＭＰマネージャのＩＰアドレス等を指定する。図５４に示す例では、Responses タグに囲まれた範囲における最初のResponseタグでは、”EMAIL“を子要素としている。また、孫要素である”Gateway ”でメールサーバのＩＰアドレス”10.10.10.5”を指定し、孫要素である”Account ”でメールの送信先アドレス”admin@abcde.com ”を指定している。また、Responses タグに囲まれた範囲における二番目のResponseタグでは、”SNMP“を子要素としている。また、孫要素である”Manager ”で、アラートの発信先であるＳＮＭＰマネージャのＩＰアドレスを指定している。

【０２４９】

その他の要素や属性については、図５に示す動作モデルで表現可能なセキュリティ機器についての汎用セキュリティポリシーをＸＭＬ文書で表した場合の書式の例（図８および

図９参照。）と同一であるので、ここでは説明を省略する。
【０２５０】
本実施の形態では、パケットフィルタリングポリシーとＮＩＤＳポリシーの連携を行う場合を例にして説明する。本例では、第１の実施の形態ないし第４の実施の形態と同様に、セキュリティ機器であるＮＩＤＳについても、まずステップＥ３（図５１参照。）で設定情報を抽出し、ステップＥ４（図５１参照。）で上述の書式の汎用セキュリティポリシーを生成する。
【０２５１】
次に、本実施の形態では、第２の実施の形態ないし第４の実施の形態と同様、ＮＩＤＳについてセキュリティポリシー分析を行う（ステップＥ５、図５１参照。）。なお、パケットフィルタリングポリシーとＮＩＤＳポリシーの連携を行う場合、パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーに対する分析は行わなくてよい。
【０２５２】
以下、シグネチャをサービス（関係するプロトコルとポート番号）によって分類して、ＮＩＤＳの汎用セキュリティポリシー（ＮＩＤＳの設定情報から導出された汎用セキュリティポリシー）を分析する例を説明する。
【０２５３】
通常、一つのイベントは、それを監視するシグネチャと１対１に対応している。つまり、ＮＩＤＳでは、一つのシグネチャを有効化することによってそのシグネチャに対応する一つのイベントを監視する。製品によってその数は異なるが、一つのＮＩＤＳ製品には数百を超える数のシグネチャが用意されている。このため先に述べたように製品によってはシグネチャをカテゴリと呼ばれる単位でグループ化しているものもある。しかし、このシグネチャをカテゴリに分類するための指針があいまいであり、意味のある分類とは言えない。これに対し本実施の形態では、各シグネチャをサービス（関係するプロトコルとポート番号）という指針で分類する。このような分類方法により、ＮＩＤＳによってどのサービスについて監視が行き届いているか、あるいはあまり監視されていないかを把握しやすくなる。
【０２５４】
図５５は、ＮＩＤＳの汎用セキュリティポリシーの分析に必要な情報の例を示す。この情報は、分析知識データベース１４０に予め記憶され、ＮＩＤＳの汎用セキュリティポリシーの分析が行われる際に、セキュリティポリシー分析手段１０５によって読み込まれる。
【０２５５】
図５５に示す情報では、”EventName ”と、”CategoryName”と、”VulnerabilityProtocol ”とが対応付けられている。”VulnerabilityProtocol ”には、”Protocol”、”SrcPort ”および”DestPort”が含まれる。”EventName ”は、シグネチャによって監視するイベントのイベント名を表す。”CategoryName”は、そのシグネチャが属するカテゴリのカテゴリ名を表す。”VulnerabilityProtocol ”は、シグネチャによって監視するプロトコル、送信ポート番号および宛先ポート番号を表す。具体的には、”VulnerabilityProtocol ”に含まれる”Protocol”が、シグネチャによって監視するプロトコルを表し、同様に、”SrcPort ”および”DestPort”が、それぞれシグネチャによって監視する送信ポート番号、宛先ポート番号を表している。
【０２５６】
セキュリティポリシー分析手段１０５は、ＮＩＤＳの汎用セキュリティポリシーに記述された”EventName ”と、分析知識データベース１４０が記憶する”CategoryName”および”VulnerabilityProtocol ”とを対応付ける分析を行い、その分析結果を得る。この分析結果は、汎用セキュリティポリシーの記述形式で記述される。
【０２５７】
図５６は、ＮＩＤＳの汎用セキュリティポリシーの分析処理の例を示すフローチャート

である。セキュリティポリシー分析手段１０５は、ステップＥ４（図５１参照。）により生成されたＮＩＤＳの汎用セキュリティポリシーから先頭のPolicyを選択し、そのPolicy中のEventName の内容を取得する（ステップＥ５０１）。次に、セキュリティポリシー分析手段１０５は、分析知識データベース１４０が記憶している図５５に示す情報の中から、ステップＥ５０１で取得したEventName に対応するCategoryNameとVulneralibityProtocol の情報を検索する（ステップＥ５０２）。次に、セキュリティポリシー分析手段１０５は、ステップえ５０３で検索したCategoryNameとVulneralibityProtocol の情報（EventName に対応するCategoryNameとVulneralibityProtocol の情報）を分析知識データベース１４０から取得する（ステップＥ５０３）。続いて、セキュリティポリシー分析手段１０５は、ステップＥ５０３で取得した情報を汎用セキュリティポリシーに追加する（ステップＥ５０４）。具体的には、選択したPolicyにおける”SecurityEvent “の子要素として、CategoryNameとVulneralibityProtocol を追加する。図５７は、CategoryNameとVulneralibityProtocol の情報が追加された汎用セキュリティポリシーの例を示す。図５７に示すように、セキュリティポリシー分析手段１０５は、CategoryNameの情報を、CategoryNameタグの間に記述する。同様に、VulneralibityProtocol の情報（Protocol、SrcPortおよびDestPort)を、VulneralibityProtocol タグの間に記述する。さらに、Protocol、SrcPort およびDestPortの情報もそれぞれProtocolタグ、SrcPort タグおよびDestPortタグの間に記述する。

【０２５８】

セキュリティポリシー分析手段１０５は、汎用セキュリティポリシー内の最後のPolicyまで”EventName ”と”CategoryName”との対応付けが完了したか否かを判定する（ステップＥ５０５）。完了したならば処理を終了する。完了していなければ、汎用セキュリティポリシー内の次のPolicyを選択し、そのPolicy中のEventName の内容を取得する（ステップＥ５０６）。ステップＥ５０６の後、ステップＥ５０２に移行し、ステップＥ５０２以降の動作を繰り返す。この結果、図５７に例示する記述形式の分析結果が得られる。

【０２５９】

ここで、パケットフィルタリングについて定めた汎用セキュリティポリシーと、ＮＩＤＳポリシー分析結果の連携を行う前に、ＮＩＤＳポリシーの分析結果を表示してもよい。

【０２６０】

図５８はＮＩＤＳポリシーのセキュリティポリシー分析結果の表示例を示している。図５８に示す例では、シグネチャをプロトコルおよびポート番号に基づいて分類したカテゴリのカテゴリ名（ＤＮＳ等）と、そのカテゴリに属するシグネチャ（イベント）の総数と、そのカテゴリに属するシグネチャのうち有効化されているシグネチャの数（有効数）、およびシグネチャの有効率を表示している。

【０２６１】

各カテゴリに属するシグネチャ（イベント）の総数として表示される値は、図５７に例示する記述形式の分析結果において、同一のCategoryNameを子要素として持つSecurityEvent の総数である。なお、ＮＩＤＳにおいてシグネチャは日々追加されていく。従って、ＮＩＤＳの設定情報から生成した汎用セキュリティポリシーの分析結果におけるシグネチャ（イベント）の総数は、一定であるとは限らない。図５８に示す画面を表示する場合に、セキュリティポリシー分析手段１０５は、設定情報の抽出から、図５７に例示する記述形式の分析結果の導出までを行った後に、その分析結果を用いて、同一のCategoryNameを子要素として持つSecurityEvent の総数をカウントし、その値を「総数」として表示すればよい。

【０２６２】

また、カテゴリ毎の有効数は、同一のCategoryNameを子要素として持つSecurityEventのうち、対応付けられているFunctionタグで囲まれた範囲に記述されたEnabled の記述がtrue（有効）となっているSecurityEvent の数である。セキュリティポリシー分析手段１０５は、この数をカウントして有効数として表示すればよい。

【０２６３】

また、有効率は、各カテゴリ毎に、（[有効数]／［シグネチャ総数］）×１００として計算される。セキュリティポリシー分析手段１０５は、この計算によって得られる有効率を表示すればよい。また、図５８に示すように有効率を数値として表示するだけでなく、グラフとして表示してもよい。有効率を表示することにより、図５８に例示する「ＤＮＳ」、「ＦＴＰ」、「ＨＴＴＰ」等の各種サービス毎に、監視が行き届いているか、あるいはあまり監視されていないかを把握しやすくなる。

【０２６４】

また、プロトコルとポート番号によってカテゴリを分類する場合、カテゴリによっては、一般的なサービス名が付けられていない場合もある。そのような場合には、図５８に例示する「ＤＮＳ」等のような一般的なサービス名の代わりに、プロトコルとポート番号の組み合わせをカテゴリ名として表示してもよい。

【０２６５】

以下、セキュリティポリシー連携の具体例について説明する。

連携処理としてパケットフィルタリングに関するポリシー（ルール）とＮＩＤＳに関するポリシー（ルール）との不整合検出を行う場合、パケットフィルタリング機能について定めた汎用セキュリティポリシーと、ＮＩＤＳの汎用セキュリティポリシーの分析結果とを用いる。セキュリティポリシー分析手段１０５は、パケットフィルタリング機能について定めた汎用セキュリティポリシーについては、分析を行う必要はなく、その汎用セキュリティポリシーをそのままセキュリティポリシー連携手段１１３に出力すればよい。また、セキュリティポリシー分析手段１０５は、ＮＩＤＳから導出された汎用セキュリティポリシーについては図５６に示す分析を行い、汎用セキュリティポリシーおよびその分析結果をセキュリティポリシー連携手段１１３に出力する。従って、セキュリティポリシー連携手段１１３は、ＮＩＤＳから導出された汎用セキュリティポリシーおよびその分析結果と、パケットフィルタリング機能について定めた汎用セキュリティポリシーとを受け取る。そして、パケットフィルタリング機能について定めた汎用セキュリティポリシーと、ＮＩＤＳの汎用セキュリティポリシーの分析結果との不整合を検出して、その結果を出力する。

【０２６６】

セキュリティポリシー分析手段１０５が、セキュリティポリシー連携手段１１３に対して、パケットフィルタリング機能について定めた汎用セキュリティポリシーとして、図５９に示す汎用セキュリティポリシーを出力したとする。図５９に示す汎用セキュリティポリシーでは、DestIPとして”200.100.100.10”が記述され、DestPortとして21が記述されている。また、Actionとしてacceptが記述されている。従って、図５９に示す汎用セキュリティポリシーは、”200.100.100.10”のＩＰアドレスを持つサーバ上のＦＴＰサービス（ポート番号２１）へのアクセスを許可していることを示している。

【０２６７】

セキュリティポリシー分析手段１０５が、セキュリティポリシー連携手段１１３に対して、ＮＩＤＳから導出された汎用セキュリティポリシーの分析結果として、図５７に示す分析結果を出力したとする。図５７に示す分析結果では、EventName としてFTP_Get が記述され、DestPortとして21が記述されている。また、Enabled としてfalse が記述されている。従って、図５７に示す分析結果は、シグネチャ名（イベント名）がFTP_Get で表されるＦＴＰサービス（ポート番号２１）に関するイベントを監視するシグネチャが無効化されていることを示している。

【０２６８】

図６０は、パケットフィルタリングポリシーとＮＩＤＳポリシーの連携処理（図５１に示すステップＥ７に相当する処理）の例を示すフローチャートである。図６０に示す連携処理では、パケットフィルタリングポリシーとＮＩＤＳポリシーとの不整合を検出する。

【０２６９】

セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー分析結果のカテゴリから一つを選択する（ステップｅ１）。すなわち、ＮＩＤＳから導出された汎用セキュリティポ

リシーの分析結果（本例では図５７に示す分析結果）から、一つのカテゴリを選択する。ここで、シグネチャは、プロトコルとポート番号の組み合わせによって各カテゴリに分類されている。従って、ステップｅ１では、カテゴリとして、プロトコルとポート番号の組み合わせを一つ選択すればよい。プロトコルとポート番号の組み合わせは、分析結果においてVulnerabilityProtocol として記述されている。具体的にはVulnerabilityProtocolの子要素であるProtocol（プロトコル）、SrcPort （送信元ポート番号）、DestPort（宛先ポート番号）として記述されている。従って、セキュリティポリシー連携手段１１３は、Protocol、SrcPort およびDestPortの内容を分析結果から取得すればよい。図５７に例示する分析結果では、Protocol、SrcPort およびDestPortの内容はそれぞれtcp ,any ,21であるので、セキュリティポリシー連携手段１１３は、「tcp ,any ,21」という組み合わせを取得する。また、セキュリティポリシー連携手段１１３は、ステップｅ１で、プロトコルとポート番号の組み合わせとともに、その組み合わせに対応するCategoryNameを取得してもよい。本例では、プロトコルとポート番号の組み合わせとともに、そのCategoryNameも取得する場合を例にして説明する。従って、セキュリティポリシー連携手段１１３は、この組み合わせと、この組み合わせに対応するCategoryNmae（FTP ）を取得する。

【０２７０】

さらに、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー分析結果から取得したProtocol、SrcPort およびDestPortに対応するパケットが、パケットフィルタリング機能について定めた汎用セキュリティポリシー（本例では図５９に示す汎用セキュリティポリシー）において、通過を許可されているか否かを判定する（ステップｅ２）。通過を許可されている場合にはステップｅ３に移行し、通過を禁止されている場合にはステップｅ４に移行する。

【０２７１】

例えば、ステップｅ１で、セキュリティポリシー連携手段１１３がProtocol、SrcPort およびDestPortの内容として「tcp ,any ,21」という組み合わせを取得済みであるとする。この取得内容と同一内容の記述を、パケットフィルタリング機能について定めた汎用セキュリティポリシー内で検索すると、Protocol、SrcPort およびDestPortの内容がそれぞれtcp ,any ,21と記述されていることが分かる（図５９参照。）。さらに、その記述に対応するActionの内容が、acceptと記述されている（図５９参照。）。従って、本例では、セキュリティポリシー連携手段１１３は、取得したProtocol、SrcPort およびDestPortに対応するパケットが通過を許可されていると判定し、ステップｅ３に移行する。

【０２７２】

ステップｅ３において、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー分析結果において、ステップｅ１で選択したカテゴリに属する全てのシグネチャが有効化されているか否かを判定する。具体的には、ステップｅ１で選択したカテゴリ（Protocol,SrcPort ,およびDestPortの組み合わせ）の内容と同一内容であるカテゴリを検索し、そのカテゴリに対応するEnabled の記述が全てtrue（有効）となっているか否かを判定すればよい（ステップｅ３）。選択したカテゴリに対応するEnabled の記述が全てtrueとなっているならば（すなわち、ステップｅ１で選択したカテゴリに属する全てのシグネチャが有効化されているならば）、ステップｅ７に移行する。選択したカテゴリに対応するEnabled の記述にfalse となっているものが一つでもあれば（すなわち、ステップｅ１で選択したカテゴリに属するシグネチャのうち無効化されているものが一つでもあれば）、ステップｅ５に移行する。

【０２７３】

本例では、図５７に示すように、選択したカテゴリ（tcp ,any ,21の組み合わせ）に対応するEnabled の記述の中にfalse となるものがある。従って、ステップｅ１で選択したカテゴリに属するシグネチャのうち無効化されているものが存在するので、ステップｅ５に移行する。

【０２７４】

ステップｅ５において、セキュリティポリシー連携手段１１３は、ステップｅ１で選択

したカテゴリのCategoryName、Protocol、SrcPort 、DestPortの情報と、パケットフィルタリングポリシーおよびＮＩＤＳポリシーにおいて不整合を起こしているPolicyのpolicyID属性値を「監視漏れまたはフィルタ漏れ不整合リスト」に格納する。図６１は、「監視漏れまたはフィルタ漏れ不整合リスト」の例を示す。図６１に示すように、「監視漏れまたはフィルタ漏れ不整合リスト」には、「CategoryNmae」、「Protocol」、「SrcPort 」、「DestPort」、「ＮＩＤＳポリシーのpolicyID属性値ＩＤリスト」および「パケットフィルタリングポリシーのpolicyID属性値リスト」が格納される。セキュリティポリシー連携手段１１３は、ステップｅ１で選択したカテゴリのCategoryName、Protocol、SrcPort 、DestPortの情報を、それぞれ図６１に示すように「監視漏れまたはフィルタ漏れ不整合リスト」に格納する。

【０２７５】

また、セキュリティポリシー連携手段１１３は、パケットフィルタリングポリシーにおいて不整合を起こしているPolicyのpolicyID属性値を、「監視漏れまたはフィルタ漏れ不整合リスト」の「パケットフィルタリングポリシーのpolicyID属性値リスト（図６１参照。）」に格納する。このとき、セキュリティポリシー連携手段１１３は、パケットフィルタリングポリシーにおいて不整合を起こしているPolicyを、以下のようにして特定すればよい。すなわち、ステップｅ１で取得したProtocol、SrcPort 、およびDestPortと一致する値がそれぞれProtocolタグ、SrcPort タグ、およびDestPortタグに記述されたPolicyのうち、最も優先度が高く、Actionタグにacceptが記述されているPolicyを特定すればよい。セキュリティポリシー連携手段１１３は、このような条件を満たすPolicyのpolicyID属性値を「パケットフィルタリングポリシーのpolicyID属性値リスト」に格納する。

【０２７６】

また、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシーにおいて不整合を起こしているPolicyのpolicyID属性値を、「監視漏れまたはフィルタ漏れ不整合リスト」の「ＮＩＤＳポリシーのpolicyID属性値リスト（図６１参照。）」に格納する。このとき、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシーにおいて不整合を起こしているPolicyを、以下のようにして特定すればよい。すなわち、ステップｅ１で選択したカテゴリ（Protocol,SrcPort ,およびDestPortの組み合わせ）の内容と同一内容であるカテゴリを有し、そのカテゴリに対応するEnabled の記述がfalse となっているPolicyを特定すればよい。セキュリティポリシー連携手段１１３は、このような条件を満たすPolicyのpolicyID属性値を「ＮＩＤＳポリシーのpolicyID属性値リスト」に格納する。

【０２７７】

図６１に示す例では、Protocol、SrcPort およびDestPortの組み合わせが「tcp ,any ,21」という組み合わせになるＦＴＰカテゴリの各情報を「監視漏れまたはフィルタ漏れ不整合リスト」に格納した状態を示している。

【０２７８】

セキュリティポリシー連携手段１１３は、ステップｅ５の処理終了後、ステップｅ７に移行する。

【０２７９】

ＮＩＤＳポリシー分析結果から取得したProtocol、SrcPort およびDestPortに対応するパケットが、パケットフィルタリング機能について定めた汎用セキュリティポリシーで通過禁止とされていると判定した場合（ステップｅ２におけるＮＯの場合）、ステップｅ４に移行する。ステップｅ４では、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー分析結果において、ステップｅ１で選択したカテゴリに属する全てのシグネチャが無効化されているか否かを判定する。具体的には、ステップｅ１で選択したカテゴリ（Protocol,SrcPort ,およびDestPortの組み合わせ）の内容と同一内容であるカテゴリを検索し、そのカテゴリに対応するEnabled の記述が全てfalse （無効）となっているか否かを判定すればよい（ステップｅ４）。選択したカテゴリに対応するEnabled の記述が全てfalse となっているならば（すなわち、ステップｅ１で選択したカテゴリに属する全てのシグネチャが無効化されているならば）、ステップｅ７に移行する。選択したカテゴリに対応

するEnabled の記述にtrueとなっているものが一つでもあれば（すなわち、ステップｅ１で選択したカテゴリに属するシグネチャのうち有効化されているものが一つでもあれば）、ステップｅ６に移行する。

【０２８０】

ステップｅ６において、セキュリティポリシー連携手段１１３は、ステップｅ１で選択したカテゴリのCategoryName、Protocol、SrcPort 、DestPortの情報と、パケットフィルタリングポリシーおよびＮＩＤＳポリシーにおいて不整合を起こしているPolicyのpolicyID属性値を「監視過剰またはフィルタ過剰不整合リスト」に格納する。「監視過剰またはフィルタ過剰不整合リスト」のデータ構造は、「監視漏れまたはフィルタ漏れ不整合リスト」のデータ構造と同様でよい。従って、図６１に示す場合と同様に、「監視過剰またはフィルタ過剰不整合リスト」には、「CategoryNmae」、「Protocol」、「SrcPort 」、「DestPort」、「ＮＩＤＳポリシーのpolicyID属性値ＩＤリスト」および「パケットフィルタリングポリシーのpolicyID属性値リスト」が格納される。セキュリティポリシー連携手段１１３は、ステップｅ１で選択したカテゴリのCategoryName、Protocol、SrcPort 、DestPortの情報を、それぞれ「監視過剰またはフィルタ過剰不整合リスト」に格納する。

【０２８１】

また、セキュリティポリシー連携手段１１３は、パケットフィルタリングポリシーにおいて不整合を起こしているPolicyのpolicyID属性値を、「監視過剰またはフィルタ過剰不整合リスト」の「パケットフィルタリングポリシーのpolicyID属性値リスト」に格納する。このとき、セキュリティポリシー連携手段１１３は、パケットフィルタリングポリシーにおいて不整合を起こしているPolicyを、以下のようにして特定すればよい。すなわち、ステップｅ１で取得したProtocol、SrcPort 、およびDestPortと一致する値がそれぞれProtocolタグ、SrcPort タグ、およびDestPortタグに記述されたPolicyのうち、最も優先度が高く、Actionタグにdenyが記述されているPolicyを特定すればよい。セキュリティポリシー連携手段１１３は、このような条件を満たすPolicyのpolicyID属性値を「パケットフィルタリングポリシーのpolicyID属性値リスト」に格納する。

【０２８２】

また、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシーにおいて不整合を起こしているPolicyのpolicyID属性値を、「監視過剰またはフィルタ過剰不整合リスト」の「ＮＩＤＳポリシーのpolicyID属性値リスト」に格納する。このとき、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシーにおいて不整合を起こしているPolicyを、以下のようにして特定すればよい。すなわち、ステップｅ１で選択したカテゴリ（Protocol,SrcPort ,およびDestPortの組み合わせ）の内容と同一内容であるカテゴリを有し、そのカテゴリに対応するEnabled の記述がtrueとなっているPolicyを特定すればよい。セキュリティポリシー連携手段１１３は、このような条件を満たすPolicyのpolicyID属性値を「ＮＩＤＳポリシーのpolicyID属性値リスト」に格納する。

【０２８３】

セキュリティポリシー連携手段１１３は、ステップｅ６の処理終了後、ステップｅ７に移行する。

【０２８４】

ステップｅ７では、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー分析結果にまだ選択されていないカテゴリがあるか否かを判定する。ＮＩＤＳポリシー分析結果にまだ選択されていないカテゴリがある場合には（ステップｅ７におけるＹＥＳの場合）、ステップｅ１に移行し、ステップｅ１以降の動作を繰り返す。ＮＩＤＳポリシー分析結果にまだ選択されていないカテゴリがない場合には、ステップｅ８に移行する。

【０２８５】

ステップｅ８では、セキュリティポリシー連携手段１１３は、「監視漏れまたはフィルタ漏れ不整合リスト」および「監視過剰またはフィルタ過剰不整合リスト」を、パケットフィルタリングポリシーとＮＩＤＳポリシーの不整合検出結果として出力する。

【０２８６】

図６２は、セキュリティポリシー連携手段１１３による、パケットフィルタリングポリシーとＮＩＤＳポリシーの不整合検出結果の出力画面例である。図６２に例示する出力画面では、画面上部に「監視漏れまたはフィルタ漏れ不整合リスト」を表示している。具体的には、「監視漏れまたはフィルタ漏れ不整合リスト」に格納されたProtocol、SrcPort、およびDestPortの組み合わせから特定される各カテゴリについて、図５８と同様に有効数、総数、有効率を算出して表示している。また、図６２に例示する出力画面では、画面下部に「監視過剰またはフィルタ過剰不整合リスト」を表示している。具体的には、「監視過剰またはフィルタ過剰不整合リスト」に格納されたProtocol、SrcPort 、およびDest Portの組み合わせから特定される各カテゴリについて、図５８と同様に有効数、総数、有効率を算出して表示している。

【０２８７】

図６２に例示するような「監視漏れまたはフィルタ漏れ不整合リスト」の表示によって、パケットフィルタリングポリシーでパケットの通過が許可されているにもかかわらず、ＮＩＤＳポリシーでそのパケットの監視が十分に行われていないことをセキュリティ管理者に提示することができる。すなわち、パケットフィルタリングポリシーが正しいと仮定すると、ＮＩＤＳにおける監視が不十分であり監視漏れが起こっておりＮＩＤＳの設定不備の可能性があることをセキュリティ管理者に提示することができる。また、カテゴリに属するすべてのシグネチャが無効化されている場合には、ＮＩＤＳポリシーが正しいと仮定すると、パケットフィルタリングで通過を禁止すべきであるパケットが通過を許可されていることになること（パケットフィルタリングにおける漏れが起こっている可能性があること）をセキュリティ管理者に提示することができる。

【０２８８】

この結果を受けて、セキュリティ管理者はパケットフィルタリングポリシーを確認し、パケットフィルタリングポリシーが正しいと判断した場合には、ＮＩＤＳで監視が十分に行われるようにＮＩＤＳポリシーを修正すればよい（具体的には、Enabled の記述をfalse からtrueに変更すればよい。）。また、例えば、図６２に示すTelnetカテゴリのように、カテゴリに属するすべてのシグネチャが無効化されている場合には、セキュリティ管理者はそのカテゴリに関するサービスが行われているかを確認し、そのサービスが行われていない場合にはそのサービスのパケットが通過できないようにパケットフィルタリングポリシーを修正すればよい。

【０２８９】

また、図６２に例示するような「監視過剰またはフィルタ過剰不整合リスト」の表示によって、パケットフィルタリングポリシーでパケットの通過が禁止されているにもかかわらず、ＮＩＤＳポリシーでそのパケットの監視を無駄に行っていることをセキュリティ管理者に提示することができる。すなわち、パケットフィルタリングポリシーが正しいと仮定すると、ＮＩＤＳにおける監視が過剰でありＮＩＤＳの設定不備の可能性があることをセキュリティ管理者に提示することができる。また、カテゴリに属するすべてのシグネチャが有効化されている場合には、ＮＩＤＳポリシーが正しいと仮定すると、パケットフィルタリングで通過を許可すべきであるパケットが通過を禁止されていることになること（パケットフィルタリングにおいて過剰にフィルタリングを行っている可能性があること）をセキュリティ管理者に提示することができる。

【０２９０】

この結果を受けて、セキュリティ管理者はパケットフィルタリングポリシーを確認し、パケットフィルタリングポリシーが正しいと判断した場合には、ＮＩＤＳで無駄な監視を行わないようにＮＩＤＳポリシーを修正すればよい（具体的には、Enabled の記述をtrue からfalse に変更すればよい。）。また、例えば、図６２に示すＨＴＴＰカテゴリのように、カテゴリに属するすべてのシグネチャが有効化されている場合には、セキュリティ管理者はそのカテゴリに関するサービスが行われているかを確認し、そのサービスが行われている場合にはそのサービスのパケットが通過できるようにパケットフィルタリングポリシーを修正すればよい。

【０２９１】
図６３は、パケットフィルタリングポリシーとＮＩＤＳポリシーの不整合検出結果の出力画面の他の例を示す。図６３に示す出力画面例では、表示されている不整合リストから一つの不整合が選択されると、該当するパケットフィルタリングポリシーの不整合部分とＮＩＤＳポリシーの不整合部分が表示される。図６３例示する出力画面は、不整合カテゴリ表示領域９１と、不整合ＮＩＤＳポリシーＩＤ表示領域９２と、不整合パケットフィルタリングＩＤ表示領域９３と、ＮＩＤＳポリシー表示領域９４と、パケットフィルタリングポリシー表示領域９５とを含む。
【０２９２】
セキュリティポリシー連携手段１１３は、「監視漏れまたはフィルタ漏れ」の不整合や、「監視過剰またはフィルタ過剰」の不整合を起こしているカテゴリを不整合カテゴリ表示領域９１に表示する。図６３に示す不整合カテゴリ表示領域９１では、Protocol、SrcPort 、およびDestPortの内容もそれぞれ表示している。なお、図６３に示す「TransportLayer」はProtocolを意味する。セキュリティポリシー連携手段１１３は、例えばマウス（入出力手段１１０に含まれる。）によって、不整合カテゴリ表示領域９１に表示されているカテゴリを選択される。図６２では、「ＨＴＴＰ」が選択された場合を示している。
【０２９３】
セキュリティポリシー連携手段１１３は、不整合カテゴリ表示領域９１において選択されたカテゴリに対応する「ＮＩＤＳポリシーのpolicyID属性値リスト（図６１参照。）」を「監視漏れまたはフィルタ漏れ不整合リスト」あるいは「監視過剰またはフィルタ過剰不整合リスト」から抽出し、不整合ＮＩＤＳポリシーＩＤ表示領域９２に表示する。同様に、セキュリティポリシー連携手段１１３は、不整合カテゴリ表示領域９１において選択されたカテゴリに対応する「パケットフィルタリングポリシーのpolicyID属性値リスト（図６１参照。）」を「監視漏れまたはフィルタ漏れ不整合リスト」あるいは「監視過剰またはフィルタ過剰不整合リスト」から抽出し、不整合パケットフィルタリングＩＤ表示領域９３に表示する。従って、不整合ＮＩＤＳポリシーＩＤ表示領域９２および不整合パケットフィルタリングＩＤ表示領域９３にはpolicyID属性値が表示される。図６３に示す例では、選択されたカテゴリ（ＨＴＴＰ）は「監視漏れまたはフィルタ漏れ」に該当するので、ＨＴＴＰに対応する「ＮＩＤＳポリシーのpolicyID属性値リスト」および「パケットフィルタリングポリシーのpolicyID属性値リスト」を「監視漏れまたはフィルタ漏れ不整合リスト」から抽出し、それぞれ不整合ＮＩＤＳポリシーＩＤ表示領域９２と不整合パケットフィルタリングＩＤ表示領域９３に表示している。セキュリティポリシー連携手段１１３は、例えばマウスによって、不整合ＮＩＤＳポリシーＩＤ表示領域９２と不整合パケットフィルタリングＩＤ表示領域９３に表示されているpolicyID属性値を選択される。
【０２９４】
セキュリティポリシー連携手段１１３は、ＮＩＤＳから導出された汎用セキュリティポリシーに記述されたPolicyのうち、不整合ＮＩＤＳポリシーＩＤ表示領域９２で選択されたpolicyID属性値によって特定されるPolicyをＮＩＤＳポリシー表示領域９４に表示する。なお、セキュリティポリシー連携手段１１３は、図５７に例示するような分析結果だけでなく、汎用セキュリティポリシーそのものもセキュリティポリシー分析手段１０５から受け取っている。従って、汎用セキュリティポリシーに記述されたPolicyをＮＩＤＳポリシー表示領域９４に表示することができる。
【０２９５】
同様に、セキュリティポリシー連携手段１１３は、パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーに記述されたPolicyのうち、不整合パケットフィルタリングＩＤ表示領域９３で選択されたpolicyID属性値によって特定されるPolicyをパケットフィルタリングポリシー表示領域９５に表示する。
【０２９６】
セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー表示領域９４やパケットフィルタリングポリシー表示領域９５にPolicyを表示するだけでなく、各領域９４，９５に

おいて表示したPolicyに対する修正操作を入力されてもよい。すなわち、ＮＩＤＳポリシー表示領域９４やパケットフィルタリングポリシー表示領域９５においてセキュリティ管理者によってPolicyに対する編集が行われた場合に、その編集内容に従って汎用セキュリティポリシーを修正してもよい。例えば、ＮＩＤＳポリシー表示領域９４においてPolicyの編集が行われた場合、その編集内容に従って、ＮＩＤＳから導出された汎用セキュリティポリシーを修正してもよい。同様に、パケットフィルタリングポリシー表示領域９５においてPolicyの編集が行われた場合、その編集内容に従って、パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーを修正してもよい。このような構成の場合、セキュリティ管理者が、図６３に例示する画面上において手動で不整合を解消することができる。

【０２９７】

また、不整合が検出された場合に、セキュリティポリシー連携手段１１３が自動的にその不整合を修正し（例えば汎用セキュリティポリシーを修正し）、セキュリティ機器に対して修正されたセキュリティポリシーを再設定するようにしてもよい。例えば、パケットフィルタリングポリシーに応じてＮＩＤＳポリシーを一括して修正してもよい。この場合、パケットフィルタリングポリシーで通過が許可されているパケットに対応するＮＩＤＳのカテゴリに属するシグネチャはすべて有効化し、パケットフィルタリングポリシーで通過が禁止されているパケットに対応するＮＩＤＳのカテゴリに属するシグネチャはすべて無効化すればよい。そして、シグネチャを修正した後の汎用セキュリティポリシーに基づいて、ＮＩＤＳの設定を変更してもよい。

【０２９８】

図６４および図６５は、パケットフィルタリングポリシーに応じてＮＩＤＳポリシーを一括して修正する処理を示すフローチャートである。図６４は、「監視漏れまたはフィルタ漏れ不整合リスト」に格納されたカテゴリの不整合を修正する処理のフローチャートである。「監視漏れまたはフィルタ漏れ不整合リスト」に格納されたカテゴリの不整合を修正する場合、まず、セキュリティポリシー連携手段１１３は、「監視漏れまたはフィルタ漏れ不整合リスト」に格納されたカテゴリの中から一つのカテゴリを選択する（ステップｅ９）。続いて、セキュリティポリシー連携手段１１３は、選択されたカテゴリに含まれるシグネチャを全て有効化する（ステップｅ１０）。ステップｅ１０では、ＮＩＤＳから導出された汎用セキュリティポリシーに記述されているPolicyのうち、ステップｅ９で選択したカテゴリに該当するPolicyを検索する。この検索処理では、例えば、ステップｅ９でProtocol、SrcPort 、およびDestPortの組み合わせを選択し、その組み合わせと同一内容が記述されたPolicyを検索すればよい。セキュリティポリシー連携手段１１３は、検索した全てのPolicy内におけるEnabled の記述をtrueに修正すればよい。続いて、セキュリティポリシー連携手段１１３は、「監視漏れまたはフィルタ漏れ不整合リスト」に格納された全てのカテゴリを選択したか否かを判定する（ステップｅ１１）。全てのカテゴリを選択していれば、修正処理を終了する。また、まだ選択されていないカテゴリが存在するならばステップｅ９に移行して、ステップｅ９以降の処理を繰り返す。

【０２９９】

図６５は、「監視過剰またはフィルタ過剰不整合リスト」に格納されたカテゴリの不整合を修正する処理のフローチャートである。「監視過剰またはフィルタ過剰不整合リスト」に格納されたカテゴリの不整合を修正する場合、まず、セキュリティポリシー連携手段１１３は、「監視過剰またはフィルタ過剰不整合リスト」に格納されたカテゴリの中から一つのカテゴリを選択する（ステップｅ１２）。続いて、セキュリティポリシー連携手段１１３は、選択されたカテゴリに含まれるシグネチャを全て無効化する（ステップｅ１３）。ステップｅ１３では、ＮＩＤＳから導出された汎用セキュリティポリシーに記述されているPolicyのうち、ステップｅ１２で選択したカテゴリに該当するPolicyを検索する。この検索処理では、例えば、ステップｅ１２でProtocol、SrcPort 、およびDestPortの組み合わせを選択し、その組み合わせと同一内容が記述されたPolicyを検索すればよい。セキュリティポリシー連携手段１１３は、検索した全てのPolicy内におけるEnabled の記述

をfalse に修正すればよい。続いて、セキュリティポリシー連携手段１１３は、「監視過剰またはフィルタ過剰不整合リスト」に格納された全てのカテゴリを選択したか否かを判定する（ステップｅ１４）。全てのカテゴリを選択していれば、修正処理を終了する。また、まだ選択されていないカテゴリが存在するならばステップｅ１２に移行して、ステップｅ１２以降の処理を繰り返す。

【０３００】

また、図６４および図６５に示すPolicyの自動修正処理は、例えば、ステップｅ８の後に行ってもよい。例えば、ステップｅ８の後に、ステップｅ９～ｅ１１の処理を行い、ステップｅ１１でＹＥＳと判定された場合に、ステップｅ１２以降の処理を行ってもよい。

【０３０１】

また、これまで、ＮＩＤＳポリシーの MonitoredObjectで記述したオブジェクトとパケットフィルタリングポリシーにおける通過許可設定または通過禁止設定との不整合検出について述べた。ＮＩＤＳポリシーとパケットフィルタリングポリシーとの不整合検出を行う場合、ＮＩＤＳポリシーのResponseで記述したアクションとパケットフィルタリングポリシーにおけるパケットの通過設定との不整合検出を行ってもよい。

【０３０２】

以下、ＮＩＤＳポリシーのResponseで記述したアクションとパケットフィルタリングポリシーにおけるパケットの通過設定との不整合検出について説明する。ＮＩＤＳにおいて、シグネチャに合致するパケットが検出された場合にＮＩＤＳが起こすアクションには様々な種類があり、ＮＩＤＳ製品によっても異なる。このアクションの代表的な例としてＥメール（電子メール）送信とＳＮＭＰトラップがある。Ｅメール送信は、シグネチャに合致するパケットが検出されると、指定されたメールアカウントにＥメールを送信することによってアラートを発するアクションである。ＳＮＭＰはネットワーク機器の管理のための標準的なプロトコルであり、個々のネットワーク機器に常駐し、そのネットワーク機器の情報を収集するＳＮＭＰエージェントと、ＳＮＭＰエージェントを操作しエージェントが収集した情報を収集・管理するＳＮＭＰマネージャとを含んでいる。ＳＮＭＰトラップとは、ＳＮＭＰエージェントが自主的にＳＮＭＰマネージャに情報を送信することを指す。ここでは、ＮＩＤＳがＳＮＭＰエージェントとなり、シグネチャに合致するパケットが検出されると、ＮＩＤＳがＳＮＭＰマネージャにＳＮＭＰトラップによってアラートを発する。

【０３０３】

なお、既に説明したように、シグネチャに合致するパケットが検出されたときにＮＩＤＳが起こすアクションは、汎用セキュリティポリシーにおいて、Responses タグに囲まれた範囲に記述される。そして、Responses タグは、個々のアクションをそれぞれ表すResponseタグを子要素として持つ。

【０３０４】

図６６および図６７は、連携処理として、ＮＩＤＳポリシーによるアクション（本例では、Ｅメール送信およびＳＮＭＰトラップとする。）と、パケットフィルタリングポリシーにおけるパケットの通過設定との不整合検出を行う処理のフローチャートである。以下の説明において、本実施の形態によるセキュリティ管理システムは、ＮＩＤＳ自身のＩＰアドレスを予め記憶しているものとする。例えば、セキュリティ管理システムは、セキュリティ管理者によって、入出力手段１１０からＮＩＤＳのＩＰアドレスを入力され、そのＩＰアドレスを記憶装置（図５０において図示せず。）に記憶させているものとする。

【０３０５】

セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー分析結果から、有効化されており、かつシグネチャに合致するパケット検出時のアクションとしてEMAIL またはSNMPが指定されているPolicyを検索する（ステップｆ１）。すなわち、ＮＩＤＳポリシーの分析結果に記述されている各Policyのうち、Enabled の記述がtrueとなっていて、かつ、Responses タグに囲まれた範囲に”EMAIL “ を子要素とするResponseタグまたは”SNMP ”を子要素とするResponseタグとを含むPolicyを検索する。

【０３０６】
ステップｆ１の後、セキュリティポリシー連携手段１１３は、検索したPolicy内に、”EMAIL“を子要素とするResponseタグの記述が含まれている場合には、その孫要素である”Gateway”の記述からメールサーバのＩＰアドレスを読み取る。そして、”EMAIL“を子要素とするResponseタグの記述を含むPolicyから読み取ったメールサーバのＩＰアドレスのリストを作成する。なお、メールサーバには、シグネチャに合致するパケット検出時にＥメールが送信される。また、検索したPolicy内に、”SNMP”を子要素とするResponseタグの記述が含まれている場合には、その孫要素である”Manager“の記述からＳＮＭＰマネージャのＩＰアドレスを読み取る。そして、”SNMP”を子要素とするResponseタグの記述を含むPolicyから読み取ったＳＮＭＰマネージャのＩＰアドレスのリストを作成する。

【０３０７】
次に、セキュリティポリシー連携手段１１３は、ステップｆ２で作成したメールサーバのＩＰアドレスリストからＩＰアドレスを一つ選択する（ステップｆ３）。次に、セキュリティポリシー連携手段１１３は、ＮＩＤＳのＩＰアドレスが送信元ＩＰアドレスであり、選択したメールサーバのＩＰアドレスが宛先ＩＰアドレスであり、宛先ポート番号が２５番（Ｅメール送信に使用されるポート番号）となっているパケットの通過が許可されているか否かを、パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーに基づいて判定する（ステップｆ４）。パケットの通過が禁止されている場合には、セキュリティポリシー連携手段１１３は、ステップｆ４において、ＮＩＤＳのＩＰアドレスが送信元ＩＰアドレスであり、選択したメールサーバのＩＰアドレスが宛先ＩＰアドレスであり、宛先ポート番号が２５番となっているパケットの通過の禁止を示すPolicyのPolicyID属性値を取得する。ステップｆ４でパケットの通過が許可されていると判定した場合、ステップｆ６に移行し、パケットの通過が禁止されていると判定した場合、ステップｆ５に移行する。

【０３０８】
ステップｆ５では、セキュリティポリシー連携手段１１３は、ステップｆ３で選択したメールサーバのＩＰアドレスを記述したPolicyのPolicyID属性値を不整合リストに加える。このとき、セキュリティポリシー連携手段１１３は、メールサーバのＩＰアドレスを記述したPolicyのPolicyID属性値と対応させて、ステップｆ４で取得したPolicyID属性値も不整合リストに加える。ステップｆ５の後、ステップｆ６に移行する。

【０３０９】
ステップｆ６では、ステップｆ２で作成したメールサーバのＩＰアドレスリストに含まれるＩＰアドレスを全て選択したかどうかを判定する（ステップｆ６）。まだ選択していないＩＰアドレスがあるならばステップｆ３に移行し、ステップｆ３以降の動作を繰り返す。メールサーバのＩＰアドレスリストに含まれるＩＰアドレスを全て選択済みならば、ステップｆ７（図６７参照。）に移行する。

【０３１０】
次に、セキュリティポリシー連携手段１１３は、ステップｆ２で作成したＳＮＭＰマネージャのＩＰアドレスリストからＩＰアドレスを一つ選択する（ステップｆ７）。次に、セキュリティポリシー連携手段１１３は、ＮＩＤＳのＩＰアドレスが送信元ＩＰアドレスであり、選択したＳＮＭＰマネージャのＩＰアドレスが宛先ＩＰアドレスであり、宛先ポート番号が１６２番（ＳＮＭＰトラップで使用されるポート番号）となっているパケットの通過が許可されているか否かを、パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーに基づいて判定する（ステップｆ８）。パケットの通過が禁止されている場合には、セキュリティポリシー連携手段１１３は、ステップｆ８において、ＮＩＤＳのＩＰアドレスが送信元ＩＰアドレスであり、選択したＳＮＭＰマネージャのＩＰアドレスが宛先ＩＰアドレスであり、宛先ポート番号が１６２番となっているパケットの通過の禁止を示すPolicyのPolicyID属性値を取得する。ステップｆ８でパケットの通過が許可されていると判定した場合、ステップｆ１０に移行し、パケットの通過

が禁止されていると判定した場合、ステップｆ９に移行する。

【０３１１】

ステップｆ９では、セキュリティポリシー連携手段１１３は、ステップｆ７で選択したＳＮＭＰマネージャのＩＰアドレスを記述したPolicyのPolicyID属性値を不整合リストに加える。このとき、セキュリティポリシー連携手段１１３は、ＳＮＭＰマネージャのＩＰアドレスを記述したPolicyのPolicyID属性値と対応させて、ステップｆ８で取得したPolicyID属性値も不整合リストに加える。ステップｆ９の後、ステップｆ１０に移行する。

【０３１２】

ステップｆ１０では、ステップｆ２で作成したＳＮＭＰマネージャのＩＰアドレスリストに含まれるＩＰアドレスを全て選択したかどうかを判定する（ステップｆ１０）。まだ選択していないＩＰアドレスがあるならばステップｆ７に移行し、ステップｆ７以降の動作を繰り返す。メールサーバのＩＰアドレスリストに含まれるＩＰアドレスを全て選択済みならば、セキュリティポリシー連携手段１１３は、ステップｆ５およびｆ９で作成した不整合リストを利用して不整合検出結果を出力する（ステップｆ１１）。

【０３１３】

ＮＩＤＳポリシーによるアクションと、パケットフィルタリングポリシーにおけるパケットの通過設定との不整合検出の具体例を示す。図６８は、パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーの例を示す。図６８に示す例では、二つ目のPolicyで、送信元ＩＰアドレスが200.100.100.0から200.100.100.255の範囲であり、宛先ＩＰアドレスが200.100.200.100であり、宛先ポート番号が25のパケットの通過が禁止されている。

【０３１４】

また、図６９は、ＮＩＤＳポリシー分析結果の例を示す。図６９に示す例では、Enabled の記述がtrueとなっていて、イベントに対する監視が有効とされている。また”EMAIL“を子要素とするResponseタグが記述され、その孫要素である”Gateway ”の内容は” 200.100.200.100 ”となっている。すなわち、シグネチャに合致するパケット検出時に、ＩＰアドレス” 200.100.200.100 ”を持つメールサーバに対してＥメール送信を行うと定められている。

【０３１５】

また、予めセキュリティポリシー管理システムが記憶しているＮＩＤＳのＩＰアドレスが 200.100.100.0から200.100.100.255の範囲に含まれるものであったとする。このとき、ＮＩＤＳポリシーにおいてＮＩＤＳからメールサーバにＥメール送信を行うと指定されているにもかかわらず、パケットフィルタリングによりそのパケットの通過が禁止されていることになる。つまり、ＮＩＤＳから発せられるＥメールによるアラートがパケットフィルタリングにより通過不可能となり、実際にはアラートが発せられないときと同じ結果となる。このような場合、セキュリティポリシー連携手段１１３は、このＮＩＤＳポリシーのPolicyのPolicyID属性値（図６９に示す例では” packetMonitoring0188 ”）およびパケットの通過禁止を示すPolicyのPolicyID属性値（図６８に示す例では、” packet_filtering501 ”）を不整合リストに追加し、不整合検出結果を出力する。

【０３１６】

図７０は、ＮＩＤＳポリシーのResponseで記述したアクションとパケットフィルタリングポリシーにおけるパケットの通過設定との不整合検出結果の出力画面の例を示す。図７０に示す出力画面は、不整合ＮＩＤＳポリシーＩＤ表示領域９６と、不整合パケットフィルタリングＩＤ表示領域９７と、ＮＩＤＳポリシー表示領域９８と、パケットフィルタリングポリシー表示領域９９とを含む。

【０３１７】

セキュリティポリシー連携手段１１３は、ステップｆ５またはステップｆ９で不整合リストに追加したPolicyID属性値のうち、ＮＩＤＳポリシー分析結果から取得したPolicyID属性値（ステップｆ３またはステップｆ７で選択したＩＰアドレスを記述したPolicyのPolicyID属性値）を不整合ＮＩＤＳポリシーＩＤ表示領域９６に表示する。セキュリティポ

リシー連携手段１１３は、例えばマウスによって、不整合ＮＩＤＳポリシーＩＤ表示領域９６に表示されているpolicyID属性値を選択される。図７０では、不整合ＮＩＤＳポリシーＩＤ表示領域９６において、”packetMonitoring0209”が選択された場合を示している。

【０３１８】

セキュリティポリシー連携手段１１３は、ＮＩＤＳから導出された汎用セキュリティポリシーに記述されたPolicyのうち、不整合ＮＩＤＳポリシーＩＤ表示領域９６で選択されたpolicyID属性値によって特定されるPolicyをＮＩＤＳポリシー表示領域９８に表示する。既に説明したように、セキュリティポリシー連携手段１１３は、分析結果だけでなく、汎用セキュリティポリシーそのものもセキュリティポリシー分析手段１０５から受け取っている。従って、汎用セキュリティポリシーに記述されたPolicyをＮＩＤＳポリシー表示領域９８に表示することができる。

【０３１９】

また、セキュリティポリシー連携手段１１３は、不整合ＮＩＤＳポリシーＩＤ表示領域９６でpolicyID属性値を選択されると、選択されたpolicyID属性値と対応するpolicyID属性値を不整合パケットフィルタリングＩＤ表示領域９７に表示する。また、セキュリティポリシー連携手段１１３は、例えばマウスによって、不整合パケットフィルタリングＩＤ表示領域９７に表示されているpolicyID属性値を選択される。図７０では、不整合パケットフィルタリングＩＤ表示領域９７において、”packetFiltering0152 ”が選択された場合を示している。

【０３２０】

セキュリティポリシー連携手段１１３は、パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーに記述されたPolicyのうち、不整合パケットフィルタリングＩＤ表示領域９７で選択されたpolicyID属性値によって特定されるPolicyをパケットフィルタリングポリシー表示領域９９に表示する。

【０３２１】

図７０に例示する不整合検出結果の出力画面によって、管理者はパケットフィルタリングポリシーとＮＩＤＳポリシーの不整合部分を容易に把握することができる。

【０３２２】

また、図６３に示す画面の場合と同様に、セキュリティポリシー連携手段１１３は、ＮＩＤＳポリシー表示領域９８やパケットフィルタリングポリシー表示領域９９にPolicyを表示するだけでなく、各領域９８，９９において表示したPolicyに対する修正操作を入力されてもよい。すなわち、ＮＩＤＳポリシー表示領域９８やパケットフィルタリングポリシー表示領域９９においてセキュリティ管理者によってPolicyに対する編集が行われた場合に、その編集内容に従って汎用セキュリティポリシーを修正してもよい。このような構成の場合、セキュリティ管理者が、図７０に例示する画面上において手動で不整合を解消することができる。

【０３２３】

また、不整合が検出された場合に、セキュリティポリシー連携手段１１３が自動的にその不整合を修正し（例えば汎用セキュリティポリシーを修正し）、セキュリティ機器に対して修正されたセキュリティポリシーを再設定するようにしてもよい。

【０３２４】

次に、本実施の形態の効果について説明する。本実施の形態では、セキュリティ機器に固有の表現を持つ設定情報からセキュリティ機器の種類によらない汎用セキュリティポリシーを生成した後、連携処理を行うように構成されている。セキュリティポリシーの連携においては、汎用セキュリティポリシー（またはその分析結果）に記述されるオブジェクトやその属性の関連性を利用してセキュリティポリシー間の関連付けを行っている。そのため、異なるセキュリティ機能を持つセキュリティ機器であっても、セキュリティ機能の違いを意識することなく、また異なる機器間でも機器固有の設定記述の形式を意識することなく設定内容の連携処理を行うことができる。また、連携処理を行わず個別に汎用セキ

ュリティポリシーを分析しただけでは検出できない設定不備などを容易に検出することができる。

【０３２５】

なお、連携の態様は、不整合検出に限定されない。不整合検出以外の連携の例として、関連ポリシー検出がある。関連ポリシー検出とは、ある一つのPolicyを指定したときに、その指定したPolicy内で記述されているオブジェクトについて記述されている別のPolicyを検出することである。これは不整合検出処理の過程で、同一オブジェクトの記述を持つPolicyを列挙することで実現できる。関連ポリシー検出によって、あるPolicyの内容を変更する場合に影響を受けるPolicyを、セキュリティ機能の違いやセキュリティ機器ごとの固有の設定記述の形式を意識することなく把握することができる。

【０３２６】

また、図６４や図６５に例示したような不整合検出時に自動的に汎用セキュリティポリシーを修正する処理も連携の一態様である。また、連携の例として、動的ポリシー変更も挙げられる。動的ポリシー変更とは、あるルールが適用されたときに自動的に他のルールを変更し、変更後のルールを適用することである。動的ポリシー変更の具体例には、ＮＩＤＳとファイアウォールを含むネットワークシステム運用中に、ＮＩＤＳポリシーによって不正なパケットが検知された場合には、そのパケットの通過を許可しているパケットフィルタリングポリシーを、パケット通過を禁止するようにその内容を変更させる処理等がある。このような処理によって、不正パケット検知後の被害を最小に抑えることができる。

【０３２７】

なお、ステップＥ３（図５１参照。）では、複数のセキュリティ機器１３０から設定情報を抽出、収集する場合を示した。予め生成された汎用セキュリティポリシーまたは汎用セキュリティポリシーの分析結果が存在する場合には、ステップＥ３において、少なくとも一つのセキュリティ機器１３０から設定情報を抽出、収集すればよい。予め生成された汎用セキュリティポリシーまたは分析結果は、例えば、記憶装置（図５０において図示せず。）に記憶させておけばよい。そして、ステップＥ７で、その記憶装置から予め生成された汎用セキュリティポリシーまたは分析結果を読み込み、連携処理を行ってもよい。

【０３２８】

上記の各実施の形態において、設定情報抽出手段１０１は、設定情報入力手段に相当する。設定情報抽出サブルーチン１０２は、設定情報入力サブルーチンに相当する。入出力手段１０１に含まれる出力装置は、出力手段に相当する。また、データ処理装置１００が備える記憶装置（図１、図１５、図２９、図３４、図５０において図示せず。後述の図７３参照。）は、設定情報入力サブルーチン記憶手段、セキュリティポリシー生成サブルーチン記憶手段、セキュリティポリシー分析サブルーチン記憶手段、比較サブルーチン記憶手段、統合サブルーチン記憶手段および連携サブルーチン記憶手段に相当する。

【０３２９】

また、上記の各実施の形態では、セキュリティ機器に対応させて設定情報抽出サブルーチンやセキュリティポリシー生成サブルーチンを記憶させておく。そして、設定情報抽出手段１０１および汎用セキュリティポリシー生成手段１０３は、セキュリティ機器毎に、対応するサブルーチンを読み込んで動作する。従って、新たにセキュリティ機器を追加した場合には、そのセキュリティ機器に対応する設定情報抽出サブルーチンやセキュリティポリシー生成サブルーチンを追加記憶させることにより、新たなセキュリティ機器から設定情報を抽出したり、新たなセキュリティ機器の設定情報に応じた汎用セキュリティポリシーを生成することができる。

【０３３０】

また、上記の各実施の形態では、セキュリティ機能に対応させてセキュリティポリシー分析サブルーチン、比較サブルーチン、統合サブルーチンを記憶させておく。そして、セキュリティポリシー分析手段１０５、セキュリティポリシー比較手段１０７およびセキュリティポリシー統合手段１１１は、セキュリティ機能毎に、対応するサブルーチンを読み

込んで動作する。従って、新たなセキュリティ機能が追加された場合には、そのセキュリティ機能に対応するセキュリティポリシー分析サブルーチン、比較サブルーチン、統合サブルーチンを追加記憶させることにより、新たなセキュリティ機能に応じた分析、分析結果の比較、分析結果の統合を行うことができる。

【０３３１】

同様に、第５の実施の形態では、セキュリティ機能の組み合わせに対応させて連携サブルーチンを記憶させておく。そして、セキュリティポリシー連携手段１１３は、セキュリティ機能の組み合わせ毎に、対応するサブルーチンを読み込んで動作する。従って、新たなセキュリティ機器が追加された場合には、新たに生じるセキュリティ機能の組み合わせに対応する連携サブルーチンを追加記憶させることにより、新たなセキュリティ機能の組み合わせに応じた連携を行うことができる。

【０３３２】

また、第１の実施の形態から第５の実施の形態では、データ処理装置１００が設定情報抽出手段１０１を備え、設定情報抽出手段１０１がセキュリティ機器１３０から設定情報を抽出、収集する場合について説明した。セキュリティ機器１３０が設定情報抽出手段１０１を備え、セキュリティ機器１３０に備えられる設定情報抽出手段１０１が、セキュリティ機器１３０自身から設定情報を抽出し、その設定情報をデータ処理装置１００に送信する構成であってもよい。図７１は、この場合の構成例を示すブロック図である。セキュリティ機器１３０は、設定情報抽出サブルーチン１０２に従って動作する設定情報抽出手段１０１を備える。設定情報抽出サブルーチン１０２は、例えば、セキュリティ機器１３０が備える記憶装置（図示せず。）にエージェントとして記憶される。設定情報抽出手段１０１は、設定情報抽出サブルーチン１０２を呼び出し、設定情報抽出サブルーチン１０２に従って動作する。設定情報抽出手段１０１は、セキュリティ機器１３０に設けられるＣＰＵによって実現される。

【０３３３】

また、データ処理装置１００は、セキュリティ機器１３０と通信を行うためのソフトウェア（マネージャと記す。）３０２を予め記憶装置（図示せず。）に記憶する。また、データ処理装置１００は、マネージャ３０２に従って動作する設定情報受信手段３０１を備える。設定情報受信手段３０１は、例えばＣＰＵによって実現される。設定情報受信手段は、セキュリティ機器１３０に設定情報を要求する。この要求を受けると、設定情報抽出手段１０１は、設定情報抽出サブルーチン１０２を呼び出し、設定情報抽出サブルーチン１０２に従って設定情報を抽出する。続いて、設定情報抽出手段１０１は、抽出した設定情報をデータ処理装置１００に送信する。設定情報受信手段３０１は、この設定情報を受信する。汎用セキュリティポリシー生成手段は、この設定情報を用いて、ステップＡ３以降（あるいは、ステップＢ３以降、ステップＣ４以降、ステップＤ４以降、ステップＥ４以降）の動作を行えばよい。なお、図７１では、セキュリティポリシー分析手段１０５、セキュリティポリシー比較手段１０７、セキュリティポリシー統合手段１１１、セキュリティポリシー連携手段１１３を示していないが、図７１に示すデータ処理装置１００は、セキュリティポリシー分析手段１０５、セキュリティポリシー比較手段１０７、セキュリティポリシー統合手段１１１、セキュリティポリシー連携手段１１３を備えていてもよい。

【０３３４】

この場合、セキュリティ機器１３０が備える設定情報抽出手段１０１が、設定情報送信手段に相当し、設定情報受信手段３０１が、設定情報入力手段に相当する。

【０３３５】

また、第１の実施の形態から第５の実施の形態において、入出力手段１１０を介して設定情報を入力される構成であってもよい。この場合、システム管理者が、カットアンドペースト作業等により、セキュリティ機器が保持する設定情報と同一内容を有するファイルを作成すればよい。そして、データ処理装置１００は、入出力手段１１０を介してそのファイル（すなわち設定情報）を入力されればよい。汎用セキュリティポリシー生成手段は

、入出力手段１１０を介して入力された設定情報を用いて、ステップＡ３以降（あるいは、ステップＢ３以降、ステップＣ４以降、ステップＤ４以降、ステップＥ４以降）の動作を行えばよい。この場合、入出力手段１１０が、設定情報入力手段に相当する。

【０３３６】

また、第１の実施の形態から第５の実施の形態において、データ処理装置１００が予め外部のセキュリティ機器１３０の設定情報を記憶し、データ処理装置１００が予め記憶している設定情報に基づいて汎用セキュリティポリシーを生成してもよい。図７２は、データ処理装置１００が予め設定情報を記憶する場合の構成例を示すブロック図である。設定情報記憶手段３１０は、外部のセキュリティ機器１３０の設定情報を予め記憶する。汎用セキュリティポリシー生成手段１０３の動作は、第１の実施の形態から第５の実施の形態における動作と同様である。ただし、本例における汎用セキュリティポリシー生成手段１０３は、設定情報記憶手段３１０が予め記憶している設定情報を用いて汎用セキュリティポリシーを生成する。なお、図７２では、セキュリティポリシー分析手段１０５、セキュリティポリシー比較手段１０７、セキュリティポリシー統合手段１１１、セキュリティポリシー連携手段１１３を示していないが、図７２に示すデータ処理装置１００は、セキュリティポリシー分析手段１０５、セキュリティポリシー比較手段１０７、セキュリティポリシー統合手段１１１、セキュリティポリシー連携手段１１３を備えていてもよい。

【０３３７】

図７２に示す構成の場合、設定情報記憶手段３１０が予め設定情報を記憶しているので、設定情報抽出手段１０１（図１参照。）や設定情報受信手段３０１（図７１参照。）を備えていなくてもよい。また、図７２に示す構成において、設定情報抽出手段１０１または設定情報受信手段３０１を設け、設定情報抽出手段１０１が抽出した設定情報（または設定情報受信手段３０１が受信した設定情報、あるいは入出力手段１１０から入力された設定情報）を設定情報記憶手段３１０に記憶させる構成であってもよい。そして、汎用セキュリティポリシー生成手段１０３は、設定情報記憶手段３１０に記憶された設定情報を用いて汎用セキュリティポリシーを生成してもよい。

【０３３８】

図７３は、本発明によるセキュリティ管理システムの具体的な構成例を示すブロック図である。データ処理装置１００には、入出力手段として、キーボードやマウス等の入力装置１１０ａや、ディスプレイ装置等の出力装置１１０ｂが接続される。また、データ処理装置１００は、ＣＰＵ４０１と、記憶装置４０２と、ネットワークインタフェース部４０３とを備える。記憶装置４０２は、設定情報抽出サブルーチン１０２やセキュリティポリシー生成サブルーチン１０４を記憶する。第二の実施の形態の場合、記憶装置４０２は、さらにセキュリティポリシー分析サブルーチン１０６も記憶する。第三の実施の形態の場合、記憶装置４０２は、さらに比較サブルーチン１０８も記憶する。第四の実施の形態の場合、記憶装置４０２は、第三の実施の形態における比較サブルーチン１０８の代わりに統合サブルーチン１１２を記憶する。第五の実施の形態の場合、第三の実施の形態における比較サブルーチン１０８の代わりに連携サブルーチン１１４を記憶する。ＣＰＵ４０１は、記憶装置４０２から各種サブルーチンを読み込み、そのサブルーチンに従って動作する。この結果、ＣＰＵ４０１は、設定情報抽出手段１０１、汎用セキュリティポリシー生成手段１０３としての動作を行う。なお、第二の実施の形態の場合には、ＣＰＵ４０１はセキュリティポリシー分析手段１０５としての動作も行い、第三の実施の形態の場合には、セキュリティポリシー比較手段１０７としての動作も行う。また、第四の実施の形態の場合には、ＣＰＵ４０１は、セキュリティポリシー統合手段１１１としての動作も行い、第五の実施の形態の場合には、セキュリティポリシー連携手段１１３としての動作も行う。ネットワークインタフェース部４０３は、通信ネットワーク１２０とのインタフェースである。ＣＰＵ４０１は、ネットワークインタフェース部４０３を介して、セキュリティ機器から設定情報を抽出する。

【産業上の利用可能性】

【０３３９】

本発明は、同一のセキュリティ機能を持ちながら機器によってその設定方法が異なるような各セキュリティ機器の設定検証といった用途に適用できる。

【図面の簡単な説明】

【０３４０】

【図１】本発明によるセキュリティポリシー管理システムの第１の実施の形態を示すブロック図である。

【図２】第１の実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。

【図３】設定情報抽出収集処理の例を示すフローチャートである。

【図４】汎用セキュリティポリシー生成処理の例を示すフローチャートである。

【図５】セキュリティ機能の動作のモデルの例を示す説明図である。

【図６】PolicyGroup , Policy, PolicyRuleの包含関係を示す説明図である。

【図７】PolicyGroup , Policy, PolicyRuleの包含関係を示す説明図である。

【図８】汎用セキュリティポリシーをＸＭＬ文書で表した場合の書式の例を示す説明図である。

【図９】汎用セキュリティポリシーをＸＭＬ文書で表した場合の書式の例を示す説明図である。

【図１０】一つのセキュリティ機器に対応する汎用セキュリティポリシー生成処理の例を示す説明図である。

【図１１】セキュリティ機器としてファイアウォールを設置する場合の設置例を示す説明図である。

【図１２】iptablesの設定を表す設定情報の例を示す説明図である。

【図１３】設定情報の記述仕様に関する知識の例を示す説明図である。

【図１４】生成された汎用セキュリティポリシーの例を示す説明図である。

【図１５】本発明によるセキュリティポリシー管理システムの第２の実施の形態を示すブロック図である。

【図１６】第２の実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。

【図１７】分析知識データベースが記憶する情報の例を示す説明図である。

【図１８】分析知識データベースが記憶する情報の例を示す説明図である。

【図１９】分析知識データベースが記憶する情報の例を示す説明図である。

【図２０】分析処理の例を示すフローチャートである。

【図２１】パケットフィルタリング機能に応じた分析処理の例を示すフローチャートである。

【図２２】ｔｃｐに応じた分析処理の例を示すフローチャートである。

【図２３】パケットフィルタリング機能を有するセキュリティ機器の設定情報の例を示す説明図である。

【図２４】分析結果として表示される２次元平面データの例を示す説明図である。

【図２５】分析結果を表示するユーザインタフェースの例を示す説明図である。

【図２６】ｉｃｍｐによるパケットフィルタリング機能を有するセキュリティ機器の設定情報の例を示す説明図である。

【図２７】分析結果として表示される２次元平面データの例を示す説明図である。

【図２８】分析結果の他の出力態様を示す説明図である。

【図２９】本発明によるセキュリティポリシー管理システムの第３の実施の形態を示すブロック図である。

【図３０】第３の実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。

【図３１】汎用セキュリティポリシーの例を示す説明図である。

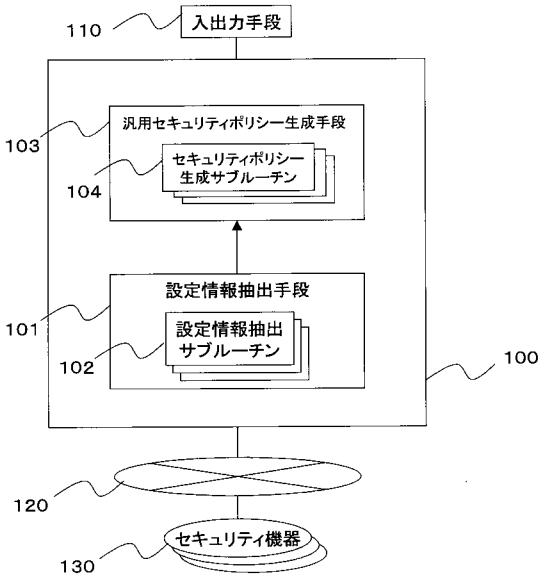
【図３２】汎用セキュリティポリシーの例を示す説明図である。

【図３３】比較結果の出力画面の例を示す説明図である。

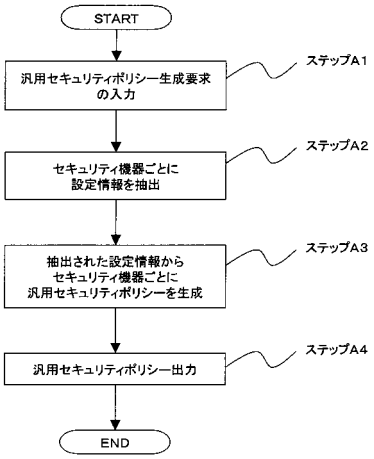
【図３４】本発明によるセキュリティポリシー管理システムの第４の実施の形態を示すブロック図である。
【図３５】第４の実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。
【図３６】パケットフィルタリングを行うセキュリティ機器を含むネットワークシステムの例を示す説明図である。
【図３７】汎用セキュリティポリシーの例を示す説明図である。
【図３８】汎用セキュリティポリシーの例を示す説明図である。
【図３９】汎用セキュリティポリシーの分析結果の出力画面の例を示す説明図である。
【図４０】汎用セキュリティポリシーの分析結果の出力画面の例を示す説明図である。
【図４１】統合処理の例を示すフローチャートである。
【図４２】統合処理結果の出力画面の例を示す説明図である。
【図４３】統合処理の変形例を示すフローチャートである。
【図４４】パケットフィルタリングとアドレス変換を同時に行うネットワークシステムの例を示す説明図である。
【図４５】汎用セキュリティポリシーの例を示す説明図である。
【図４６】汎用セキュリティポリシーの例を示す説明図である。
【図４７】汎用セキュリティポリシーの分析結果の出力画面の例を示す説明図である。
【図４８】アドレス変換ポリシーを適用しない場合における汎用セキュリティポリシーの分析結果の出力画面の例を示す説明図である。
【図４９】アドレス変換ポリシーを適用する場合における汎用セキュリティポリシーの分析結果の出力画面の例を示す説明図である。
【図５０】本発明によるセキュリティポリシー管理システムの第５の実施の形態を示すブロック図である。
【図５１】第５の実施の形態のセキュリティポリシー管理システムの動作の例を示すフローチャートである。
【図５２】セキュリティポリシー連携の概念図である。
【図５３】セキュリティ機能の動作のモデルの他の例を示す説明図である。
【図５４】ＮＩＤＳの汎用セキュリティポリシーの例を示す説明図である。
【図５５】ＮＩＤＳの汎用セキュリティポリシーの分析に必要な情報の例を示す説明図である。
【図５６】ＮＩＤＳの汎用セキュリティポリシーの分析処理の例を示すフローチャートである。
【図５７】カテゴリの情報が追加された汎用セキュリティポリシーの例を示す。
【図５８】ＮＩＤＳポリシーのセキュリティポリシー分析結果の表示例を示す説明図である。
【図５９】パケットフィルタリング機能について定めた汎用セキュリティポリシーの例を示す説明図である。
【図６０】パケットフィルタリングポリシーとＮＩＤＳポリシーの連携処理の例を示すフローチャートである。
【図６１】監視漏れまたはフィルタ漏れ不整合リストの例を示す説明図である。
【図６２】パケットフィルタリングポリシーとＮＩＤＳポリシーの不整合検出結果の出力画面例を示す説明図である。
【図６３】パケットフィルタリングポリシーとＮＩＤＳポリシーの不整合検出結果の出力画面の他の例を示す説明図である。
【図６４】パケットフィルタリングポリシーに応じてＮＩＤＳポリシーを一括して修正する処理を示すフローチャートである。
【図６５】パケットフィルタリングポリシーに応じてＮＩＤＳポリシーを一括して修正する処理を示すフローチャートである。
【図６６】ＮＩＤＳポリシーによるアクションと、パケットフィルタリングポリシーにお

けるパケットの通過設定との不整合検出を行う処理のフローチャートである。
【図６７】ＮＩＤＳポリシーによるアクションと、パケットフィルタリングポリシーにおけるパケットの通過設定との不整合検出を行う処理のフローチャートである。
【図６８】パケットフィルタリングを行うセキュリティ機器から導出された汎用セキュリティポリシーの例を示す説明図である。
【図６９】ＮＩＤＳポリシー分析結果の例を示す説明図である。
【図７０】ＮＩＤＳポリシーによるアクションと、パケットフィルタリングポリシーにおけるパケットの通過設定との不整合検出結果の出力画面の例を示す説明図である。
【図７１】セキュリティ機器が設定情報抽出手段を備える場合のブロック図である。
【図７２】データ処理装置１００が予め設定情報を記憶する場合の構成例を示すブロック図である。
【図７３】本発明によるセキュリティ管理システムの具体的な構成例を示すブロック図である。
【符号の説明】
【０３４１】
１００　データ処理装置
１０１　設定情報抽出手段
１０２　設定情報抽出サブルーチン
１０３　汎用セキュリティポリシー生成手段
１０４　セキュリティポリシー生成サブルーチン
１０５　セキュリティポリシー分析手段
１０６　セキュリティポリシー分析サブルーチン
１０７　セキュリティポリシー比較手段
１０８　比較サブルーチン
１１０　入出力手段
１２０　通信ネットワーク
１３０　セキュリティ機器
１４０　分析知識データベース

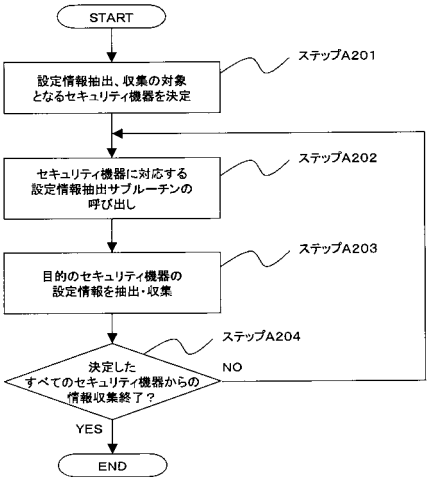
【図１】


110
入出力手段
103
汎用セキュリティポリシー生成手段
104
セキュリティポリシー
生成サブルーチン
101
設定情報抽出手段
102
設定情報抽出
サブルーチン
100
120
130
セキュリティ機器

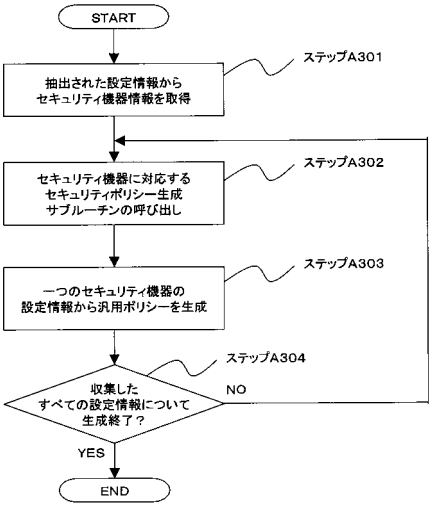
【図２】


START
汎用セキュリティポリシー生成要求
の入力
ステップA1
セキュリティ機器ごとに
設定情報を抽出
ステップA2
抽出された設定情報から
セキュリティ機器ごとに
汎用セキュリティポリシーを生成
ステップA3
汎用セキュリティポリシー出力
ステップA4
END

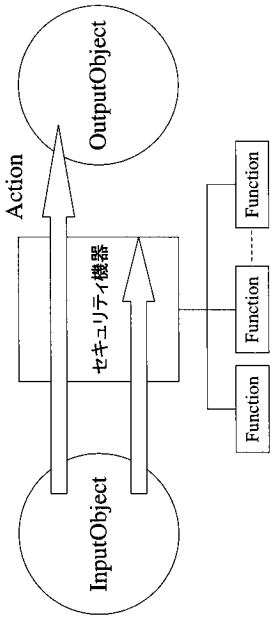
【図３】


START
設定情報抽出、収集の対象
となるセキュリティ機器を決定
ステップA201
セキュリティ機器に対応する
設定情報抽出サブルーチンの
呼び出し
ステップA202
目的のセキュリティ機器の
設定情報を抽出・収集
ステップA203
決定した
すべてのセキュリティ機器からの
情報収集終了？
ステップA204
NO
YES
END

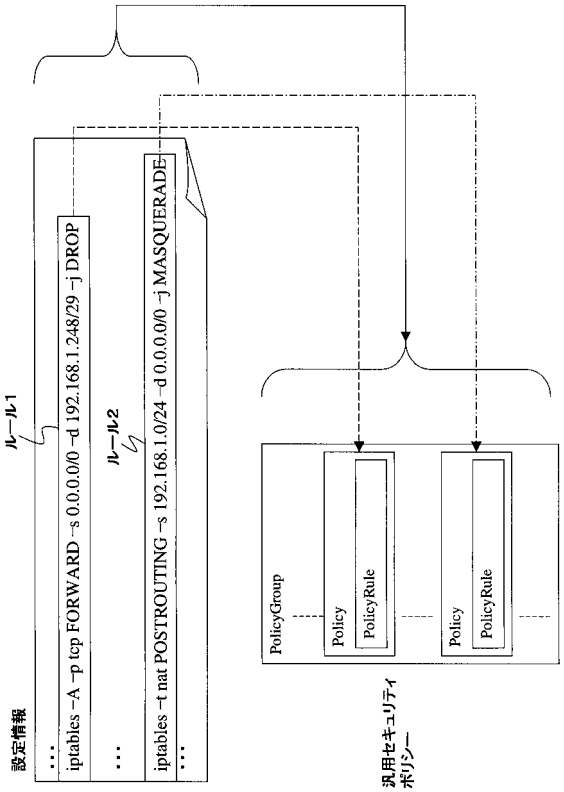
【図４】


START
抽出された設定情報から
セキュリティ機器情報を取得
ステップA301
セキュリティ機器に対応する
セキュリティポリシー生成
サブルーチンの呼び出し
ステップA302
一つのセキュリティ機器の
設定情報から汎用ポリシーを生成
ステップA303
収集した
すべての設定情報について
生成終了？
ステップA304
NO
YES
END

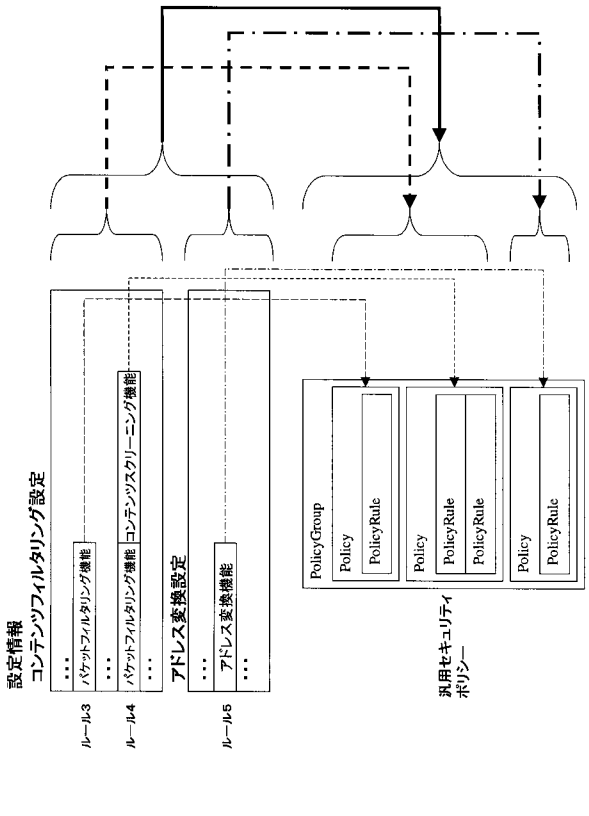
【図５】


OutputObject
Action
セキュリティ機器
InputObject
Function
Function
Function

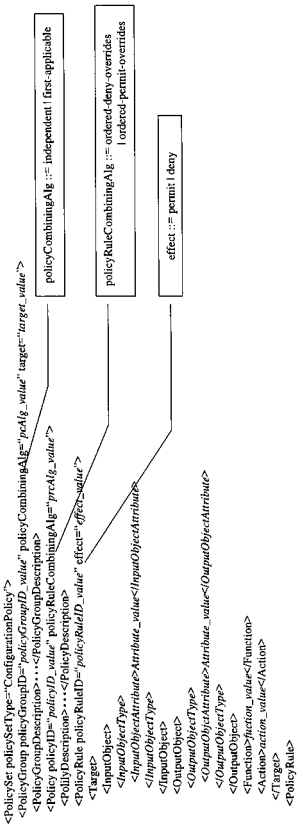
【図６】


ルール1
設定情報
...
iptables -A -p tcp FORWARD -s 0.0.0.0/0 -d 192.168.1.248/29 -j DROP
...
ルール2
iptables -t nat POSTROUTING -s 192.168.1.0/24 -d 0.0.0.0/0 -j MASQUERADE
...
PolicyGroup
Policy
PolicyRule
Policy
PolicyRule
汎用セキュリティポリシー

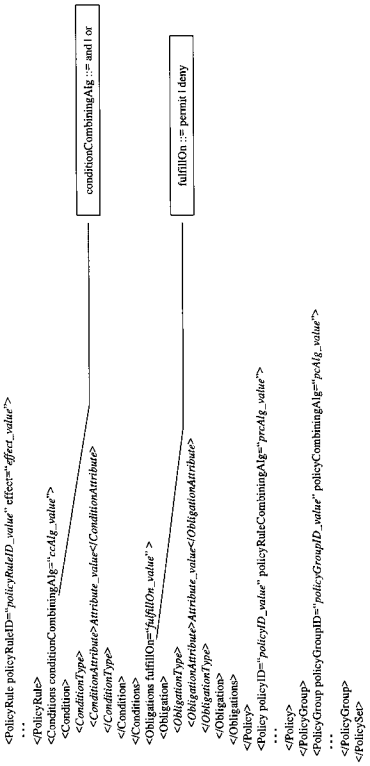
【図７】


設定情報
コンテンツフィルタリング設定
...
パケットフィルタリング機能
ルール3
...
パケットフィルタリング機能
コンテンツスクリーニング機能
ルール4
...
アドレス変換設定
...
アドレス変換機能
ルール5
...
PolicyGroup
Policy
PolicyRule
Policy
PolicyRule
PolicyRule
Policy
PolicyRule
汎用セキュリティポリシー

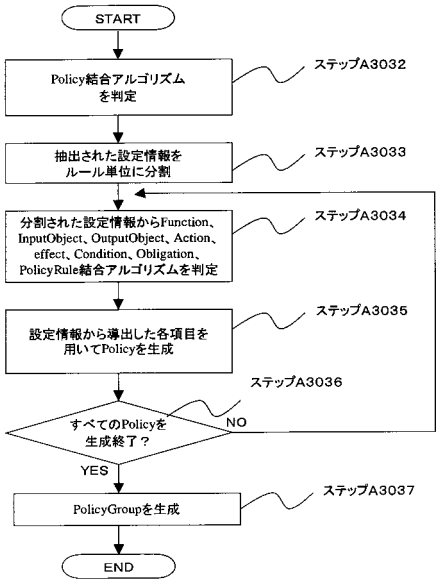
【図８】


<PolicySet policySetType="ConfiguarationPolicy">
<PolicyGroup policyGroupID="policyGroupID_value" policyCombiningAlg="prcAlg_value" target="target_value">
<PolicyGroupDescription>...</PolicyGroupDescription>
<Policy policyID="policyID_value" policyRuleCombiningAlg="prcAlg_value">
<PollyDescription>...</PolicyDescription>
<PolicyRule policyRuleID="policyRuleID_value" effect="effect_value">
<Target>
<InputObject>
<InputObjectType>
<InputObjectAttribute>Attribute_value</InputObjectAttribute>
</InputObjectType>
</InputObject>
<OutputObject>
<OutputObjectType>
<OutputObjAttribute>Attribute_value</OutputObjectAttribute>
</OutputObjectType>
</OutputObject>
<Function>fuction_value</Function>
<Action>action_value</Action>
</Target>
</PolicyRule>
policyCombiningAlg ::= independent | first-applicable
policyRuleCombiningAlg ::= ordered-deny-overrides
| ordered-permit-overrides
effect ::= permit | deny

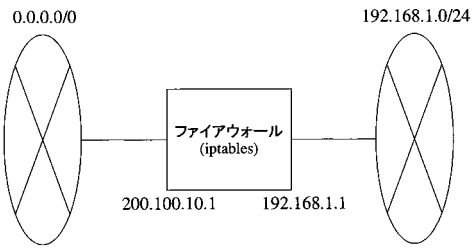
【図９】



【図１０】



【図１１】



【図１２】

```
iptables -P FORWARD DROP

iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.168.1.248/29 -j DROP
iptables -A FORWARD -p tcp -s 0.0.0.0/0 -d 192.168.1.224/27 -j ACCEPT
```

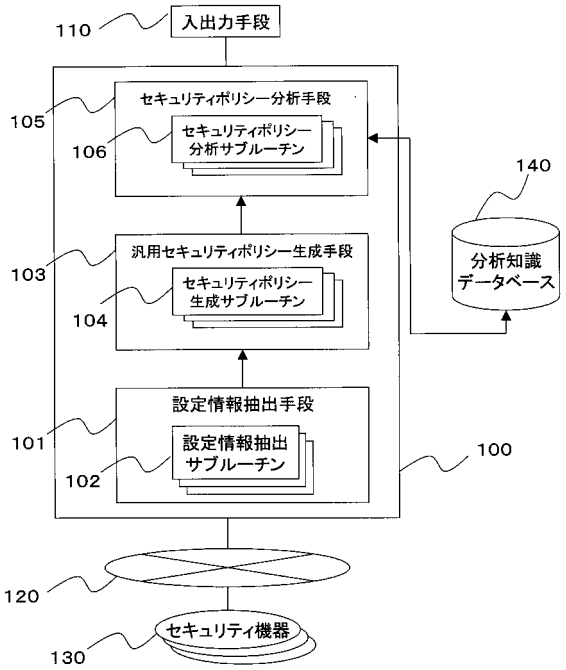
【図１３】

表記	意味	汎用セキュリティポリシーにおけるオブジェクト／属性
-t, --table *table*	table=filterのとき パケットフィルタリングルール（-tが省略時のデフォルト） table=natのとき アドレス変換ルール	Functionがpacket_filtering Functionがaddress_translation
-P, --policy	デフォルトルール	パケットフィルタリングポリシーの最後尾のPolicy
-A, --append	一つのパケットフィルタリングルール	パケットフィルタリングポリシーの一つのPolicy
-p, --protocol *protocol*	protocol=tcpのときtcpプロトコル	Packetオブジェクトの Protocol属性がtcp
	protocol=udpのときudpプロトコル	Packetオブジェクトの Protocol属性がudp
	----	----
-s, --source, --src	送信元IPアドレス	Packetオブジェクトの SrcIP属性
-d, --destination, --dst	宛先IPアドレス	Packetオブジェクトの DestIP属性
-j, --jump ACCEPT	パケット通過の許可	パケットフィルタリングポリシーのAction がaccept
-j, --jump DROP	パケット通過の禁止	パケットフィルタリングポリシーのAction がdeny
	----	----

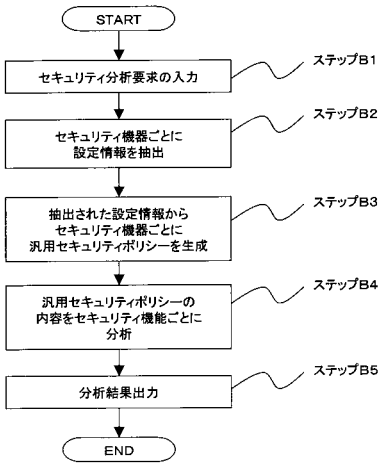
【図１４】

```
<PolicyGroup policyGroupID="firewallPolicy001" policyCombiningAlg="first-applicable"
             target="firewall">
  <Policy policyID="packet_filtering001" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering001-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>0.0.0.0/0</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>192.168.1.224/27</DestIP>
          </Packet>
        </InputObject>
        <Action>deny</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="packet_filtering002" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering002-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>0.0.0.0/0</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>192.168.1.248/29</DestIP>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="packet_filtering003" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering003-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>0.0.0.0/0</SrcIP>
            <Protocol>all</Protocol>
            <DestIP>0.0.0.0/0</DestIP>
          </Packet>
        </InputObject>
        <Action>deny</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

【図１５】



【図１６】



【図１７】

Function	InputObject	OutputObject	Action
packet_filtering	Type : Packet Attributes : SrcIP DestIP Protocol SrcPort(Protocol == tcpあるいはudpのとき) DestPort (Protocol == tcpあるいはudpのとき) TypeCode (Protocol == icmpのとき)	Type : Packet Attributes : SrcIP DestIP Protocol SrcPort(Protocol == tcpあるいはudpのとき) DestPort (Protocol == tcpあるいはudpのとき) TypeCode (Protocol == icmpのとき)	accept, drop, rejectの いずれか
snat	Type : OriginalPacket Attributes : OriginalSrcIP OrigmalSrcPort OriginalProtocol	Type : TranslatedPacket Attributes : TranslagedSrcIP TranslatedSrcPort TranslatedProtocol	translate
------	------	------	------

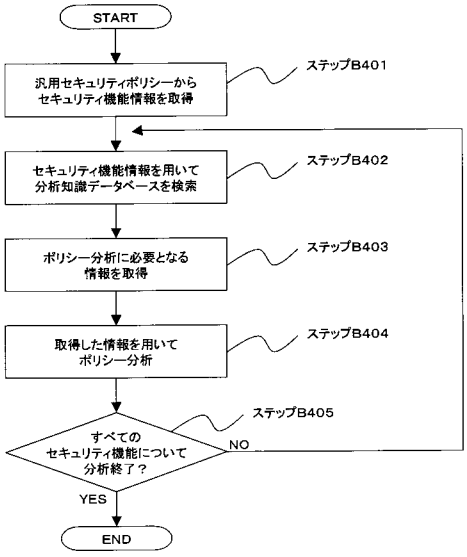
【図１８】

属性名	意味	値
SrcIP	送信元IPアドレス	NetworkAddressあるいはIPアドレス
DestIP	宛先IPアドレス	NetworkAddressあるいはIPアドレス
Protocol	プロトコル	tcp, udp, icmp, anyのいずれか
SrcPort	送信元ポート番号	PortNumberあるいはany
DestPort	宛先ポート番号	PortNumberあるいはany
TypeCode	icmpタイプコード	0, 3, 4, 5, 8, 11, 12, 13, 14, 17, 18, anyのいずれか
NetworkAddress	ネットワークアドレス	IPAddress/NetMask
IPAddress	IPアドレス	0.0.0.0～255.255.255.255
NetMask	ネットマスク	0～31の整数
PortNumber	ポート番号	1～65535の整数
------	------	------

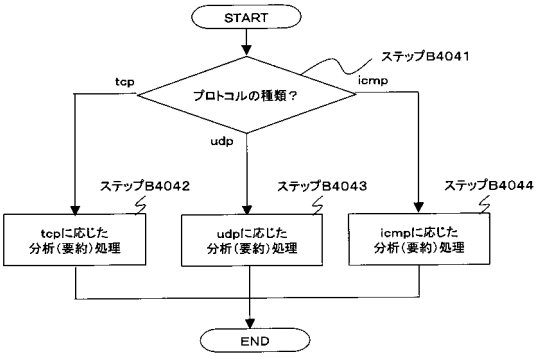
【図１９】

属性<->属性	属性間関係	
IPAddress<->PortNumber	・一つのIPアドレスは1～65535番までのポート番号を持つ	-----
NetworkAddress<->IPAddress	・NetworkAddressはNetMaskのビット数分だけ最上位からのビットを固定し、残りのビットをすべて0としたIPアドレスから、残りのビットをすべて1としたIPアドレスの範囲のIPアドレスの集合を表す	-----
-----	-----	-----

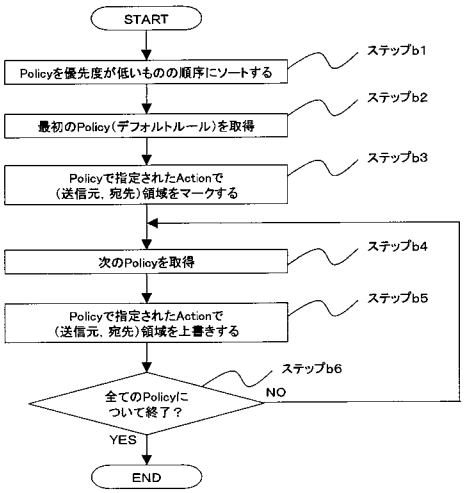
【図２０】



【図２１】



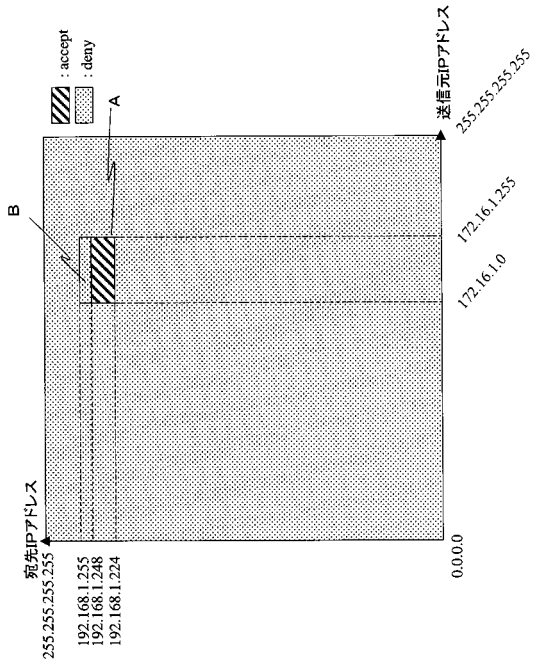
【図２２】



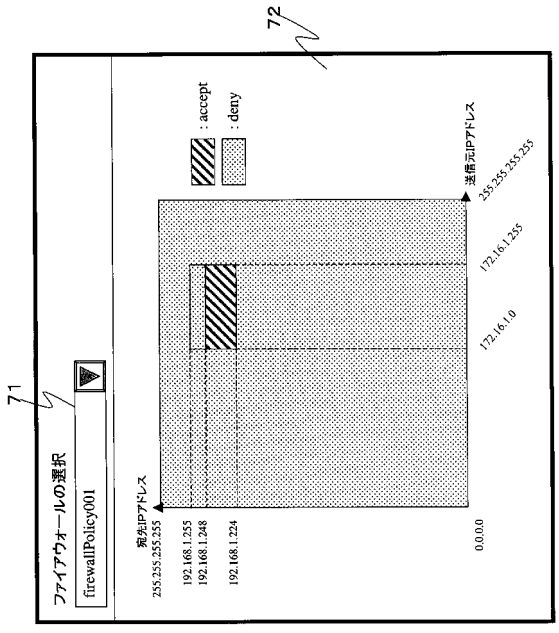
【図２３】

```
iptables -P FORWARD DROP
iptables -A FORWARD -p tcp -s 172.16.1.0/24 -d 192.168.1.248/29 -j DROP
iptables -A FORWARD -p tcp -s 172.16.1.0/24 -d 192.168.1.224/27 -j ACCEPT
```

【図２４】



【図２５】

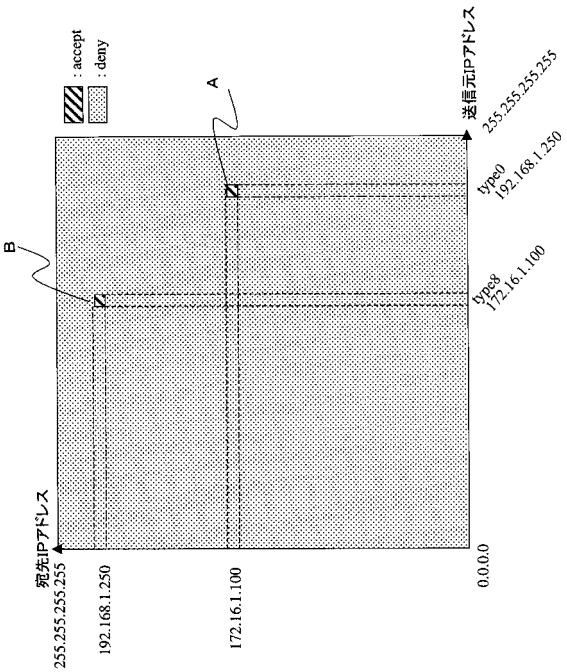


【図２６】

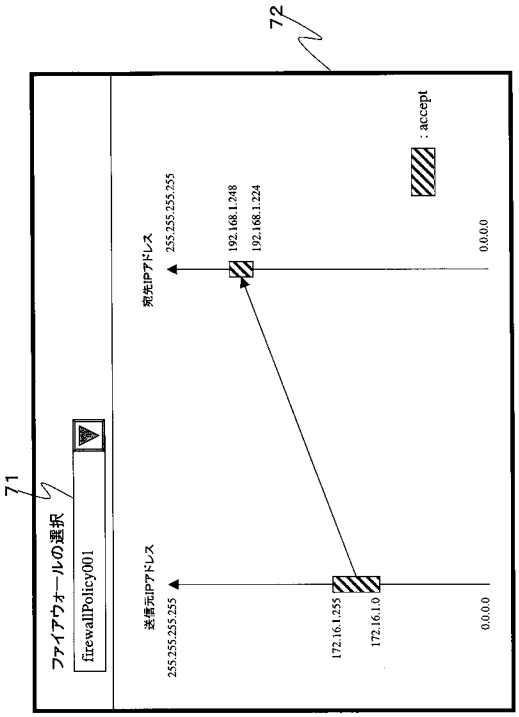
```
iptables -P FORWARD DROP

iptables -A FORWARD -p icmp --icmp-type 8 -s 172.16.1.100 -d 192.168.1.250 -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type 0 -s 192.168.1.250 -d 172.16.1.100 -j ACCEPT
```

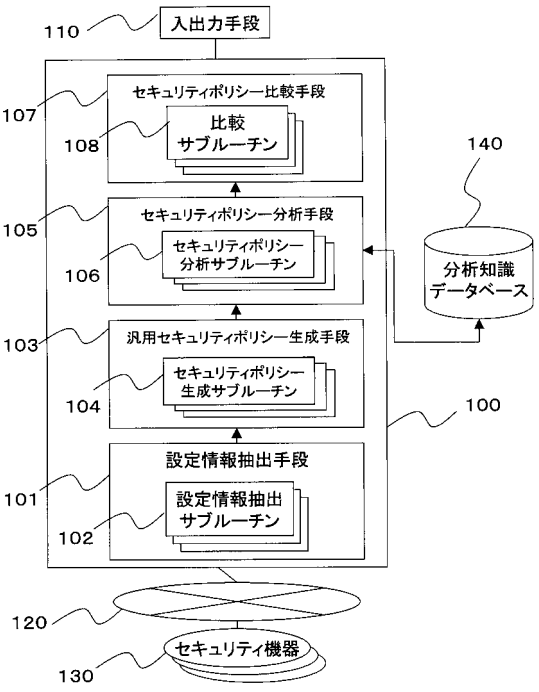
【図２７】



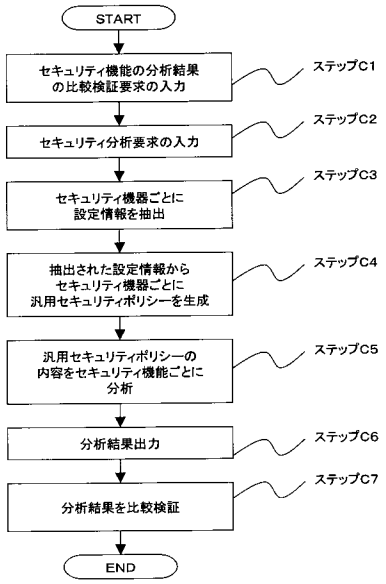
【図２８】



【図２９】



【図３０】



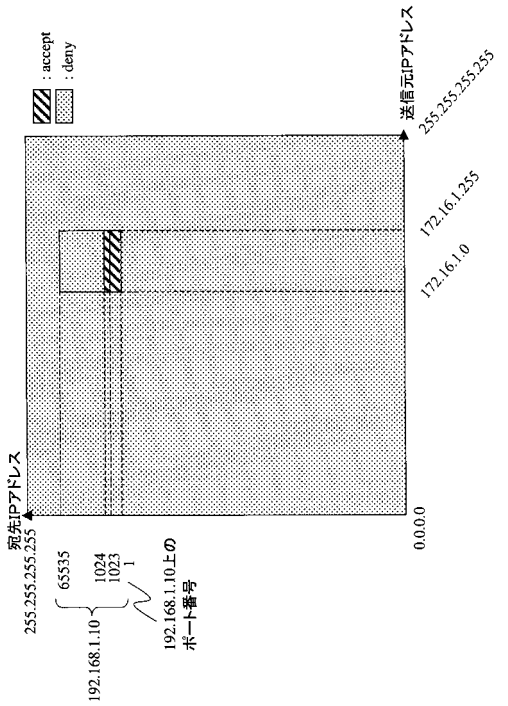
【図３１】

```
<PolicyGroup policyGroupID="firewallPolicy010" policyCombiningAlg="first-applicable"
              target="firewall">
  <Policy policyID="packet_filtering010" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering010-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.1.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>192.168.1.10</DestIP>
            <DestPort>1:1023</DestPort>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="packet_filtering011" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering011-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.1.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>192.168.1.10</DestIP>
            <DestPort>1024</DestPort>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="packet_filtering013" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering013-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.1.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>192.168.1.10</DestIP>
          </Packet>
        </InputObject>
        <Action>deny</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

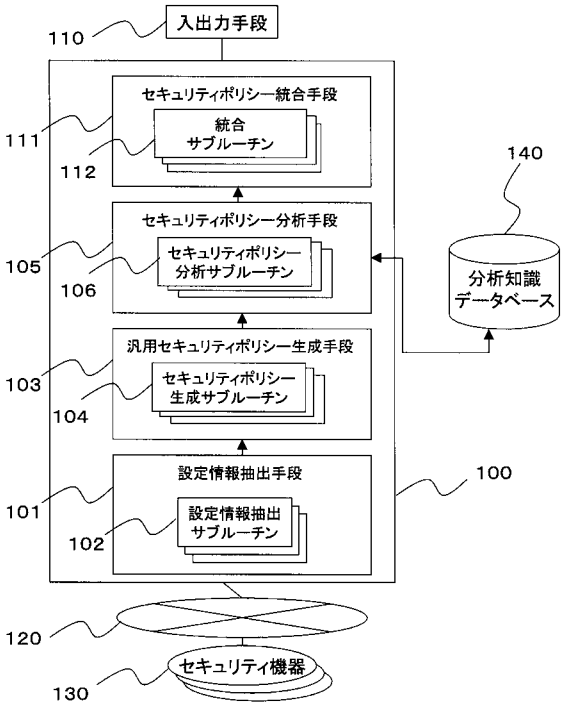
【図３２】

```
<PolicyGroup policyGroupID="firewallPolicy020" policyCombiningAlg="first-applicable"
              target="firewall">
  <Policy policyID="packet_filtering021" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering021-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.1.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>192.168.1.10</DestIP>
            <DestPort>1:1024</DestPort>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="packet_filtering022" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering022-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.161.1.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>192.168.1.10</DestIP>
          </Packet>
        </InputObject>
        <Action>deny</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

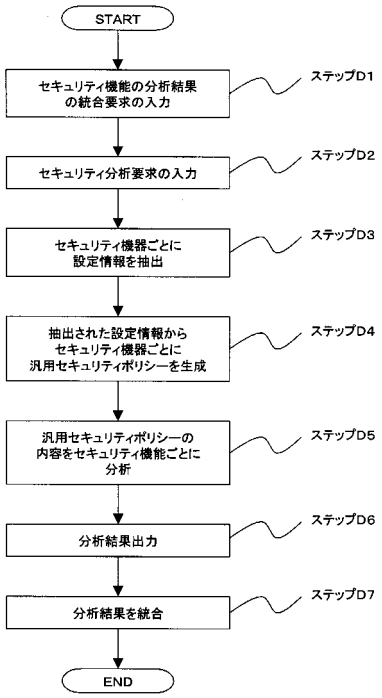
【図３３】



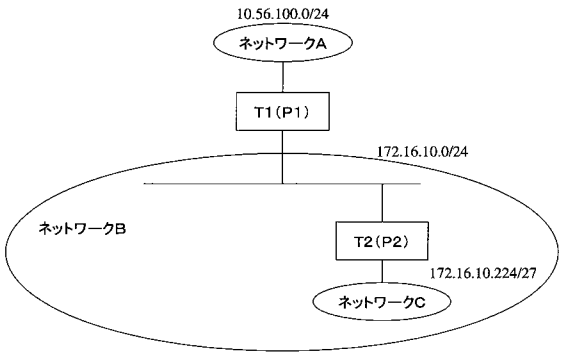
【図３４】



【図３５】



【図３６】



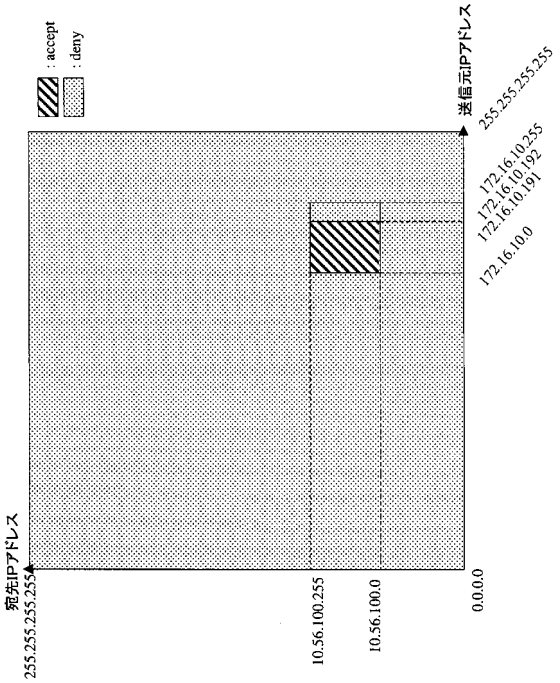
【図３７】

```
<PolicyGroup policyGroupID="firewallPolicy100" policyCombiningAlg="first-applicable"
             target="firewall">
  <Policy policyID="packet_filtering100" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering100-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.10.192/26</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>10.56.100.0/24</DestIP>
          </Packet>
        </InputObject>
        <Action>deny</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="packet_filtering101" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering101-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.10.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>10.56.100.0/24</DestIP>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

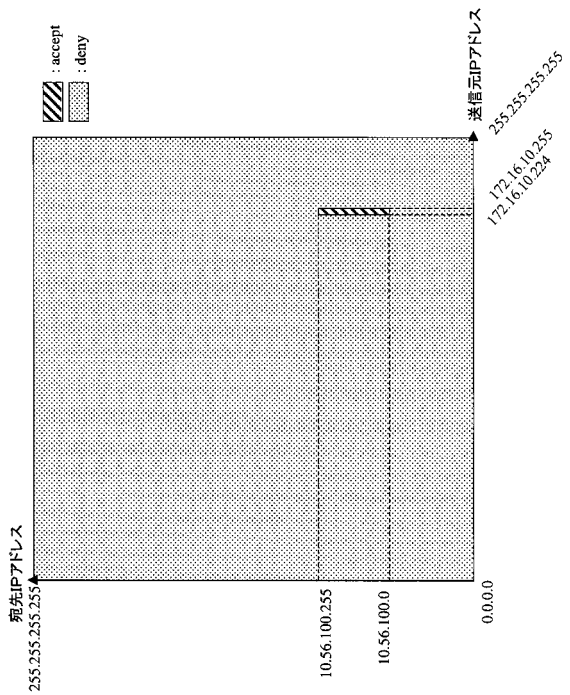
【図３８】

```
<PolicyGroup policyGroupID="firewallPolicy200" policyCombiningAlg="first-applicable"
             target="firewall">
  <Policy policyID="packet_filtering200" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering200-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.10.224/27</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>10.56.100.0/24</DestIP>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

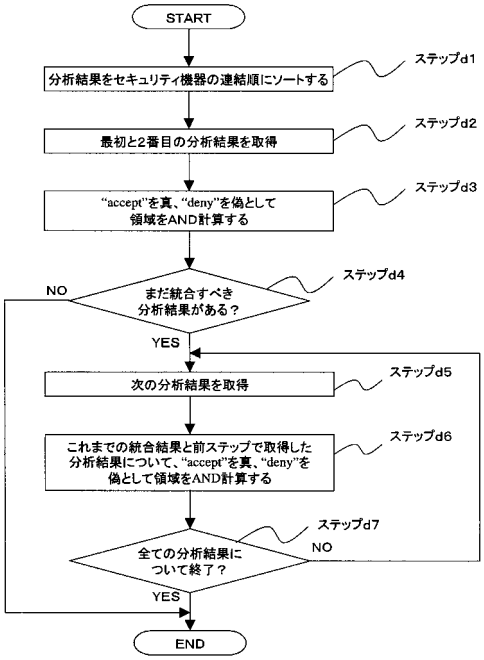
【図３９】



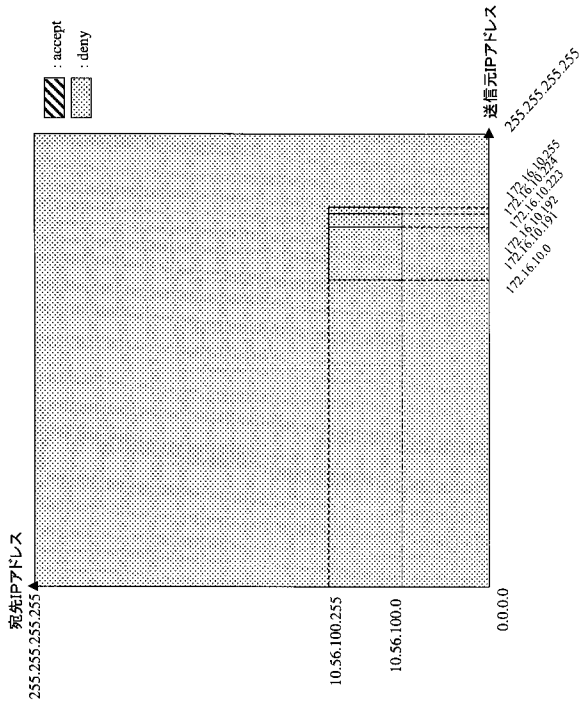
【図４０】



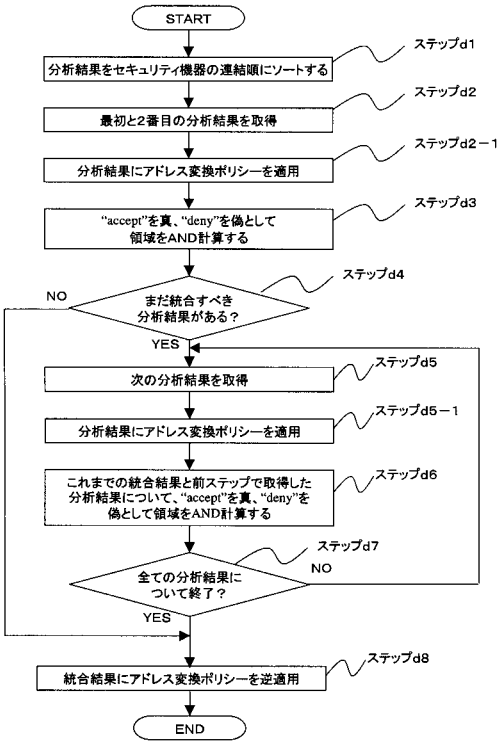
【図４１】



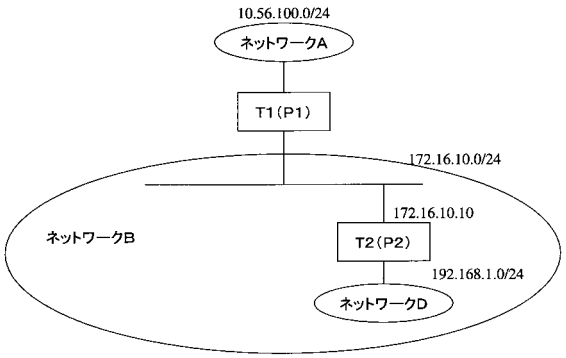
【図４２】



【図４３】



【図４４】



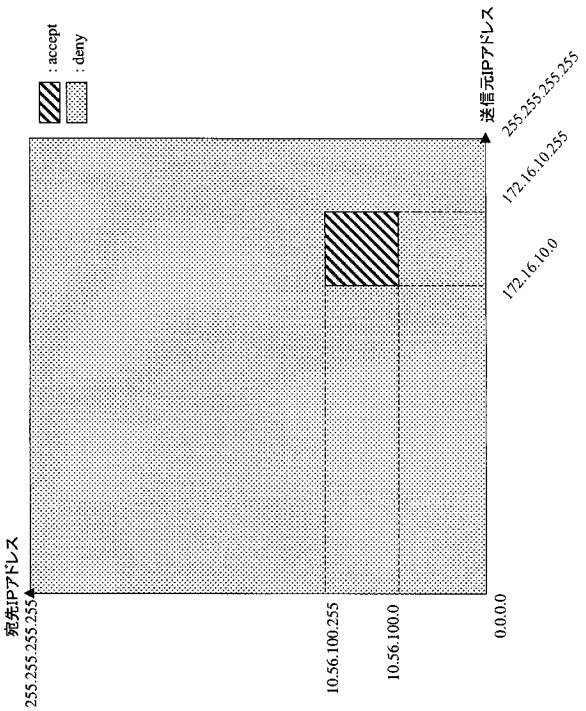
【図４５】

```
<PolicyGroup policyGroupID="firewallPolicy300" policyCombiningAlg="first-applicable"
             target="firewall">
  <Policy policyID="packet_filtering300" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering300-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>172.16.10.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>10.56.100.0/24</DestIP>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

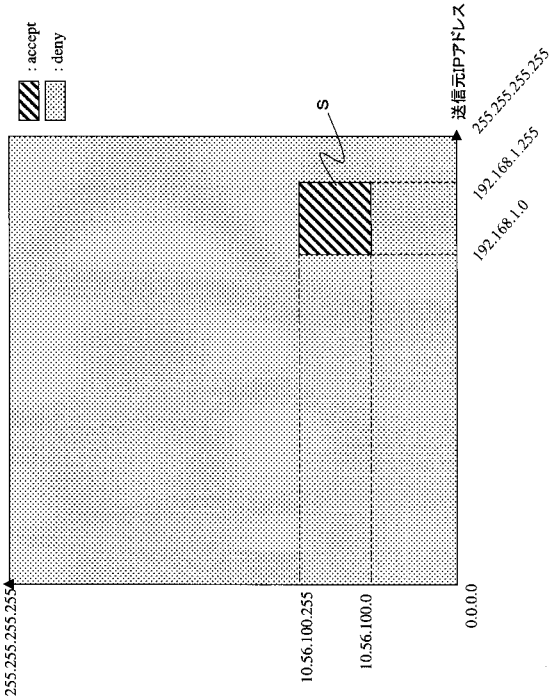
【図４６】

```
<PolicyGroup policyGroupID="firewallPolicy400" policyCombiningAlg="first-applicable"
             target="firewall">
  <Policy policyID="packet_filtering400" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering400-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>192.168.1.0/24</SrcIP>
            <Protocol>tcp</Protocol>
            <DestIP>10.56.100.0/24</DestIP>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="address_translation410" policyRuleCombiningAlg="ordered-permit-overrides">
    <PolicyRule policyRuleID="address_translation410-1" effect="permit">
      <Target>
        <Function>address_translation</Function>
        <InputObject>
          <Packet>
            <SrcIP>192.168.1.0/24</SrcIP>
            <DestIP>10.56.100.0/24</DestIP>
          </Packet>
        </InputObject>
        <Action>snat</Action>
        <OutputObject>
          <Packet>
            <SrcIP>172.16.10.10</SrcIP>
            <DestIP>10.56.100.0/24</DestIP>
          </Packet>
        </OutputObject>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

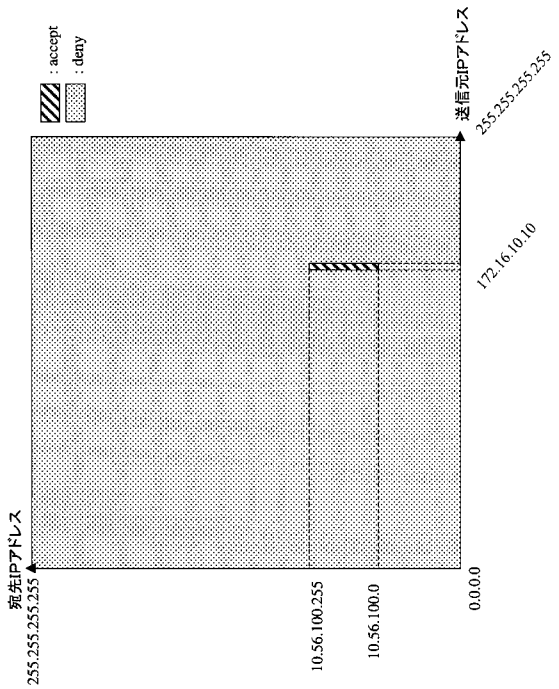
【図４７】



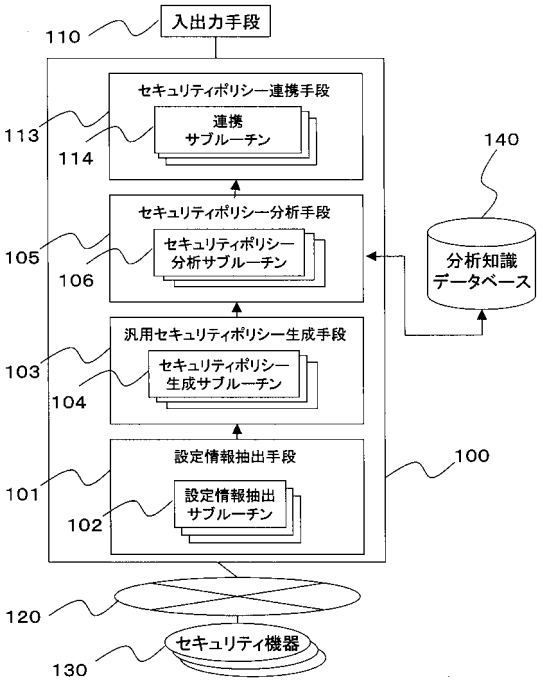
【図４８】



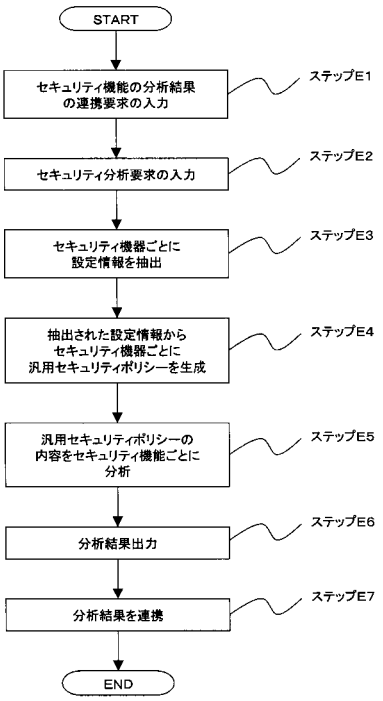
【図４９】



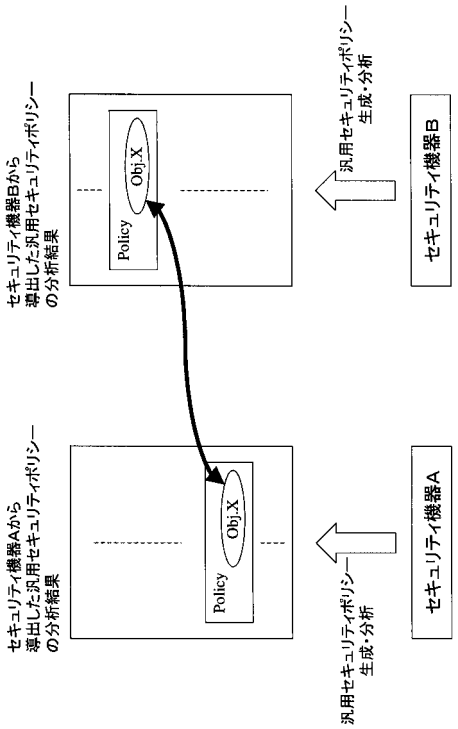
【図５０】



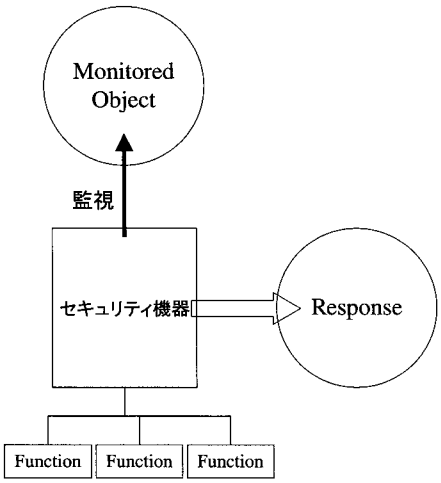
【図５１】



【図５２】



【図５３】



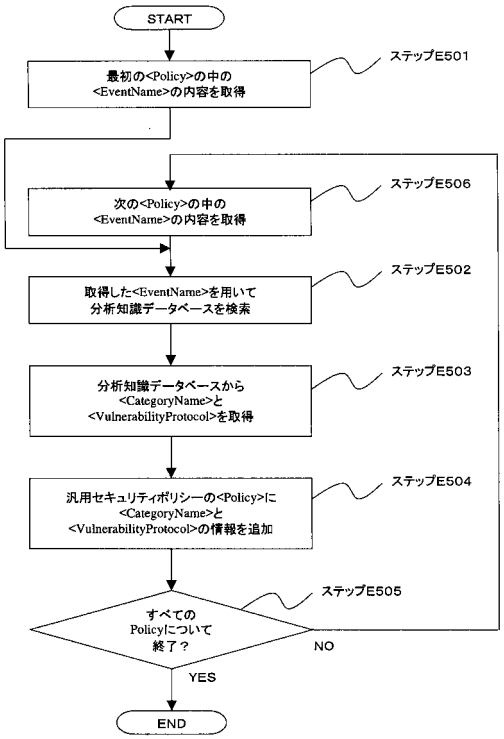
【図５４】

```
<PolicyGroup policyGroupid="127.0.0.1:network_sensor_1"
 policyCombiningType=independent
 target="nids">
  <PolicyGroupDescription>NIDSに関するポリシー</PolicyGroupDescription>
  <Policy policyID="packetMonitoring0188">
   <PolicyDescription>Decode FTP get file command</PolicyDescription>
   <Target>
    <MonitoredObject>
     <SecurityEvent>
      <EventName>FTP_Get</EventName>
     </SecurityEvent>
    </MonitoredObject>
    <Function>
     <PacketMonitoring>
      <Enabled>false</Enabled>
      <Priority>Low</Priority>
     </PacketMonitoring>
    </Function>
    <Responses>
     <Response>
      <EMAIL>
       <Gateway>10.10.10.5</Gateway>
       <Account>admin@abcde.com</Account>
      </EMAIL>
     </Response>
     <Response>
      <SNMP>
       <Manager>10.10.10.10</Manager>
       <Community>public</Community>
      </SNMP>
     </Response>
    </Responses>
   </Target>
  </Policy>
  <Policy>
   ・・・
  </Policy>
  ・・・
</PolicyGroup>
```

【図５５】

EventName	CategoryName	VulnerabilityProtocol			
		Protocol	SrcPort	DestPort	
FTP_Get	FTP	tcp	any	21	
FTP_Put	FTP	tcp	any	21	
-----	-----	-----	-----	-----	
HTTP_Head	HTTP	tcp	any	80	
-----	-----	-----	-----	-----	

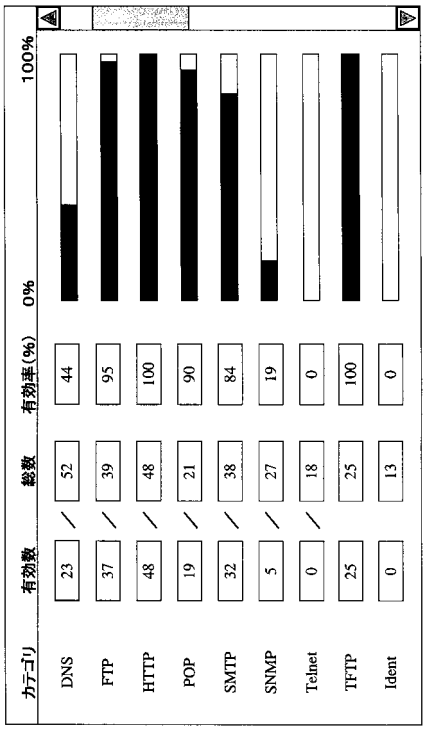
【図５６】



【図５７】

```
<PolicyGroup policyGroupid="127.0.0.1:network_sensor_1"
 policyCombiningType=independent
 target="nids">
  <PolicyGroupDescription>NIDSに関するポリシー</PolicyGroupDescription>
  <Policy policyID="packetMonitoring0188">
    <PolicyDescription>Decode FTP get file command</PolicyDescription>
    <Target>
      <MonitoredObject>
        <SecurityEvent>
          <EventName>FTP_Get</EventName>
          <CategoryName>FTP</CategoryName>
          <VulnerabilityProtocol>
            <Protocol>tcp</Protocol>
            <SrcPort>any</SrcPort>
            <DestPort>21</DestPort>
          </VulnerabilityProtocol>
        </SecurityEvent>
      </MonitoredObject>
      <Function>
        <PacketMonitoring>
          <Enabled>false</Enabled>
          <Priority>Low</Priority>
        </PacketMonitoring>
      </Function>
      <Responses>
        <Response>
          <EMAIL>
            <Gateway>10.10.10.5</Gateway>
            <Account>admin@abcde.com</Account>
          </EMAIL>
        </Response>
        <Response>
          <SNMP>
            <Manager>10.10.10.10</Manager>
            <Community>public</Community>
          </SNMP>
        </Response>
      </Responses>
    </Target>
  </Policy>
  <Policy>
    ...
  </Policy>
  ...
</PolicyGroup>
```

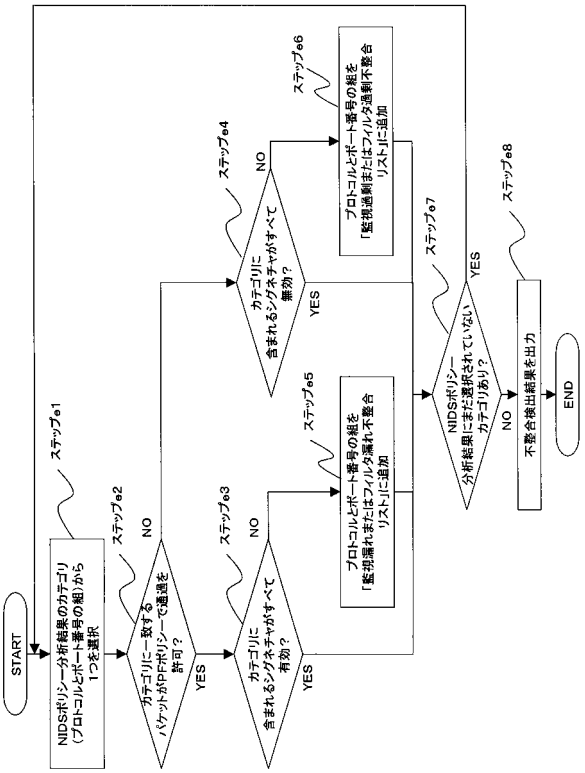
【図５８】



【図５９】

```
<PolicyGroup policyGroupID="firewallPolicy500" policyCombiningAlg="first-applicable"
             target="firewall">
  <Policy policyID="packet_filtering500" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering500-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>0.0.0.0/0</SrcIP>
            <SrcPort>any</SrcPort>
            <Protocol>tcp</Protocol>
            <DestIP>200.100.100.10</DestIP>
            <DestPort>21</DestPort>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

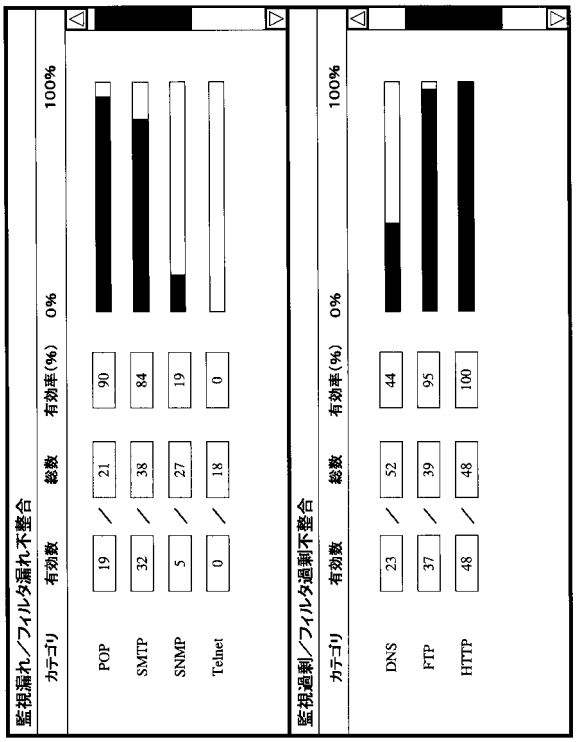
【図６０】



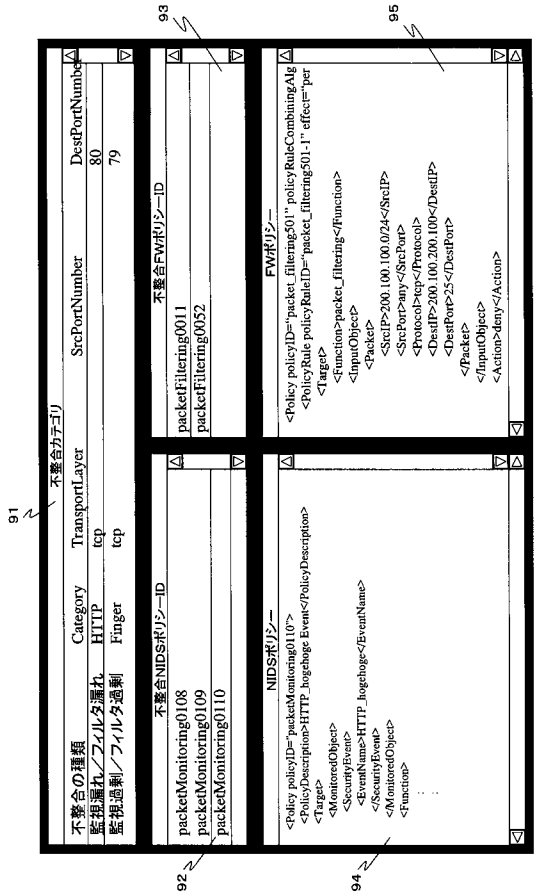
【図６１】

categoryName	Protocol	SrcPort	DestPort	NIDSポリシーの policyID属性値リスト	パケットフィルタリングポリシーのpolicyID属性値リスト
FTP	tcp	any	21	packetMonitoring060 packetMonitoring061 packetMonitoring065	packet_filtering011 packet_filtering022
				-----	-----
			-----	-----	

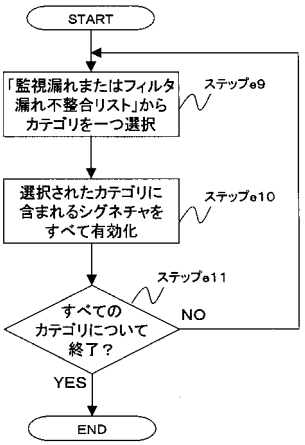
【図６２】



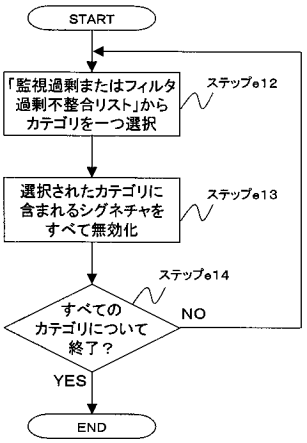
【図６３】



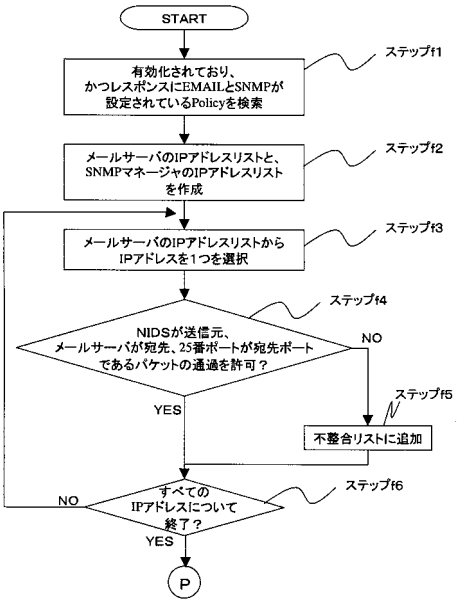
【図６４】



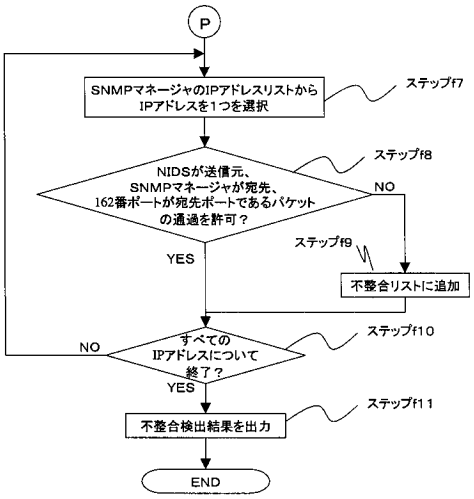
【図６５】



【図６６】



【図６７】



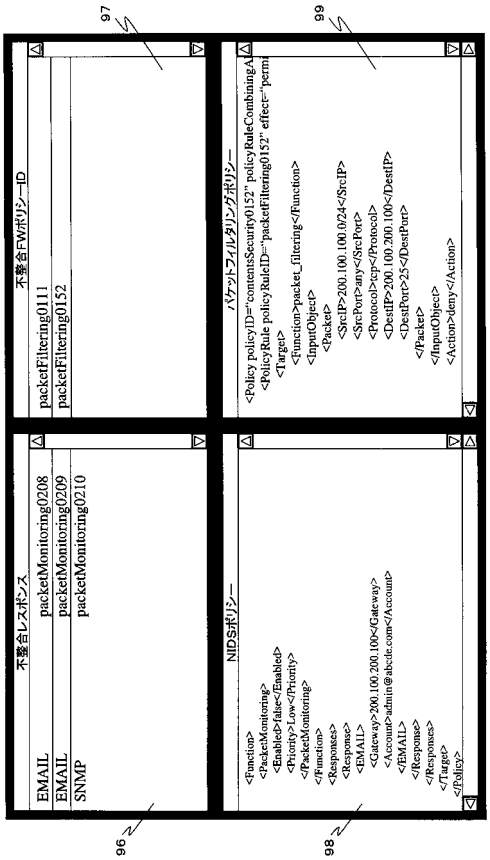
【図６８】

```
<PolicyGroup policyGroupID="firewallPolicy500" policyCombiningAlg="first-applicable"
             target="firewall">
  <Policy policyID="packet_filtering500" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering500-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>0.0.0.0/0</SrcIP>
            <SrcPort>any</SrcPort>
            <Protocol>tcp</Protocol>
            <DestIP>200.100.100.10</DestIP>
            <DestPort>21</DestPort>
          </Packet>
        </InputObject>
        <Action>accept</Action>
      </Target>
    </PolicyRule>
  </Policy>
  <Policy policyID="packet_filtering501" policyRuleCombiningAlg="ordered-deny-overrides">
    <PolicyRule policyRuleID="packet_filtering501-1" effect="permit">
      <Target>
        <Function>packet_filtering</Function>
        <InputObject>
          <Packet>
            <SrcIP>200.100.100.0/24</SrcIP>
            <SrcPort>any</SrcPort>
            <Protocol>tcp</Protocol>
            <DestIP>200.100.200.100</DestIP>
            <DestPort>25</DestPort>
          </Packet>
        </InputObject>
        <Action>deny</Action>
      </Target>
    </PolicyRule>
  </Policy>
</PolicyGroup>
```

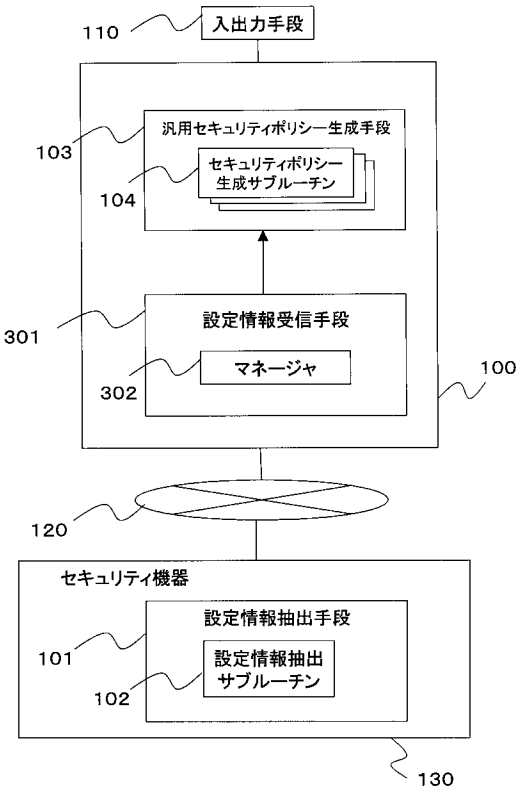
【図６９】

```
<PolicyGroup policyGroupid="127.0.0.1:network_sensor_1"
 policyCombiningType=independent
 target="nids">
  <PolicyGroupDescription>NIDSに関するポリシー</PolicyGroupDescription>
  <Policy policyID="packetMonitoring0188">
    <PolicyDescription>Decode FTP get file command</PolicyDescription>
    <Target>
      <MonitoredObject>
        <SecurityEvent>
          <EventName>FTP_Get</EventName>
          <CategoryName>FTP</CategoryName>
          <VulnerabilityProtocol>
            <Protocol>tcp</Protocol>
            <SrcPort>any</SrcPort>
            <DestPort>21</DestPort>
          </VulnerabilityProtocol>
        </SecurityEvent>
      </MonitoredObject>
      <Function>
        <PacketMonitoring>
          <Enabled>true</Enabled>
          <Priority>Low</Priority>
        </PacketMonitoring>
      </Function>
      <Responses>
        <Response>
          <EMAIL>
            <Gateway>200.100.200.100</Gateway>
            <Account>admin@abcde.com</Account>
          </EMAIL>
        </Response>
      </Responses>
    </Target>
  </Policy>
  <Policy>
    ...
  </Policy>
  ...
</PolicyGroup>
```

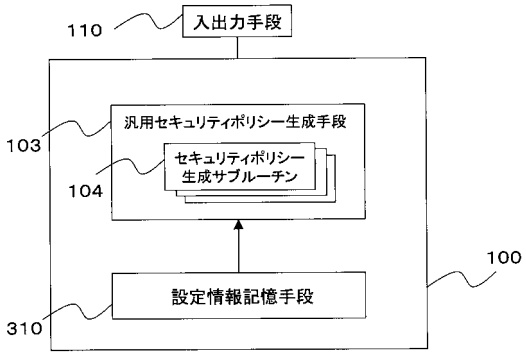
【図７０】



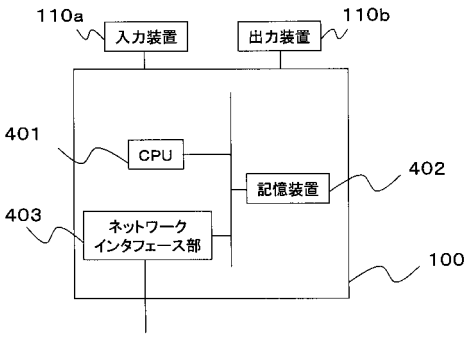
【図７１】


110
入出力手段
103
汎用セキュリティポリシー生成手段
104
セキュリティポリシー
生成サブルーチン
301
設定情報受信手段
302
マネージャ
100
120
セキュリティ機器
101
設定情報抽出手段
102
設定情報抽出
サブルーチン
130

【図７２】


110
入出力手段
103
汎用セキュリティポリシー生成手段
104
セキュリティポリシー
生成サブルーチン
100
310
設定情報記憶手段

【図７３】


110a
入力装置
110b
出力装置
401
CPU
402
記憶装置
403
ネットワーク
インタフェース部
100

フロントページの続き

(56)参考文献 特開２００２－２４７０３３（ＪＰ，Ａ）
特開２００３－０９９６０２（ＪＰ，Ａ）
国際公開第２００４／０５１４３７（WO，Ａ１）
特開２００２－２３７０３３（ＪＰ，Ａ）
特開２００１－０１６２０４（ＪＰ，Ａ）
特開２００４－０８６８８０（ＪＰ，Ａ）
特表２００６－５１６３３９（ＪＰ，Ａ）
杉本 隆洋 Takahiro Sugimoto, 安全な企業ネットワークを構築するためのセキュリティ大全, ＳｕｎＷｏｒｌｄ Ｖｏｌ．９ Ｎｏ．８, 日本, 株式会社アイ・ディ・ジーコミュニケーションズ, 第9巻, p.66-75

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２４