

(43) 国際公開日
2006年6月1日 (01.06.2006)

PCT

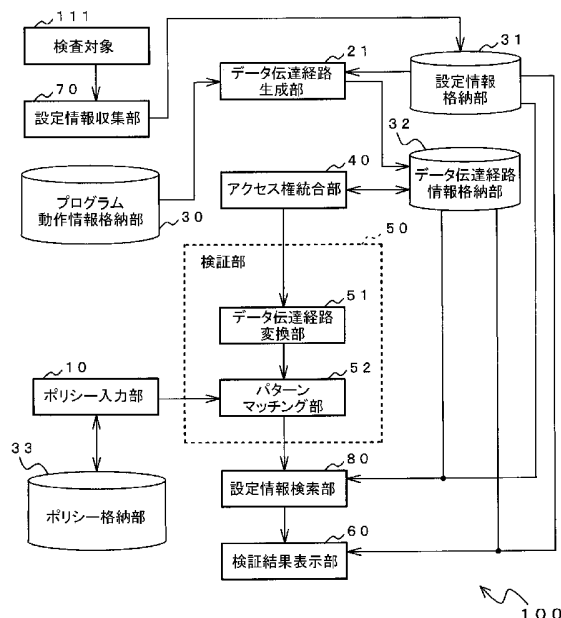
(10) 国際公開番号
WO 2006/057337 A1

- (51) 国際特許分類:
G06F 21/20 (2006.01) G06F 21/24 (2006.01)
- (21) 国際出願番号: PCT/JP2005/021674
- (22) 国際出願日: 2005年11月25日 (25.11.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2004-340898
2004年11月25日 (25.11.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 榊 啓 (SAKAKI, Hiroshi) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 宮崎 昭夫, 外 (MIYAZAKI, Teruo et al.); 〒1070052 東京都港区赤坂1丁目9番20号 第16興和ビル8階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR),

/ 続葉有 /

(54) Title: METHOD AND SYSTEM FOR GENERATING SECURITY VERIFICATION DATA

(54) 発明の名称: セキュリティ検証用のデータを生成する方法及びシステム



(57) Abstract: There is provided a system for generating input data for a security verification system includes: a system configuration information collection unit for collecting system configuration information from a computer system to be verified; an attribute information input unit for receiving attribute information to be added to the system configuration information; an access policy generation unit for generating an access policy by using the attribute information; and a verification policy generation unit for generating a verification policy expressing an inappropriate data movement route according to the access policy, the system configuration information, and the attribute information.

(57) 要約: セキュリティ検証システムに対する入力データを作成するシステムは、検証対象コンピュータシステムからシステム構成情報を収集するシステム構成情報集主部と、システム構成情報に付加される属性情報を受け取る属性情報入力部と、属性情報を用いてアクセスポリシーを生成するアクセスポリシー生成部と、アクセスポリシーと、システム構成情報及び属性情報とに基づいて、不適切なデータ移動経路を表す検証ポリシーを生成する検証ポリシー生成部と、を備える。

111. OBJECT TO BE INSPECTED
70. SETTING INFORMATION COLLECTION UNIT
30. PROGRAM OPERATION INFORMATION STORAGE UNIT
21. DATA TRANSMISSION ROUTE GENERATION UNIT
31. SETTING INFORMATION STORAGE UNIT
40. ACCESS RIGHT UNIFICATION UNIT
32. DATA TRANSMISSION ROUTE INFORMATION STORAGE UNIT
10. POLICY INPUT UNIT
33. POLICY STORAGE UNIT
50. VERIFICATION UNIT
51. DATA TRANSMISSION ROUTE CONVERSION UNIT
52. PATTERN MATCHING UNIT
80. SETTING INFORMATION SEARCH UNIT
60. VERIFICATION RESULT DISPLAY UNIT



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

明 細 書

セキュリティ検証用のデータを生成する方法及びシステム

技術分野

- [0001] 本発明は、ソフトウェアにおけるセキュリティ設定を検証するための方法及びシステムに関し、特に、セキュリティホールとなるソフトウェアのセキュリティ設定の複合的な誤りがあるか否かを検出して指摘することができるセキュリティ検証システムに対する入力データを生成するセキュリティ検証用データ生成方法及びシステムに関する。

背景技術

- [0002] 近年のインターネットの普及に伴い、インターネットは電話網などと並ぶ重要な社会インフラストラクチャとなりつつある。インターネットでは、ユーザは様々なサービスを受けることができる。インターネット上で提供されるサービスは、一般に、ユーザからの一連のリクエストを受け付け、受け付けたリクエストに応じた処理を実行し、その処理結果をユーザに送信することで実現されている。具体的には、WWW (World Wide Web) によるサービスが広く普及しており、現在では電子商取引などの様々なサービスの基盤となっている。
- [0003] インターネット上で提供される様々なサービスは、インターネットに接続されたサーバと呼ばれるシステムによって実現されている。特に、インターネットに公開されたサーバは、匿名性の高い不特定多数のユーザからのリクエストを受け付けるため、いわゆるサイバー攻撃、すなわちサイバースペースへの攻撃の対象となりやすく、セキュリティ上の大きな問題となっている。
- [0004] このような、公開サーバに対するサイバー攻撃には、サーバに内在する脆弱点やサーバにおける不適切な設定などのセキュリティホールを悪用し、サーバに悪意のあるリクエストを送りつけて不正動作させ、機密ファイルを盗むなどの悪意のある動作をさせるものがある。以下において、サーバにおける不適切な設定のことを不適設定と呼ぶ。サーバにおける脆弱点としては、例えば、サーバソフトウェアの障害を引き起こすプログラムのミスが挙げられる。不適設定としては、サーバソフトウェアの障害を引き起こすセキュリティ設定時の設定ミスなどが挙げられる。

- [0005] このようなサイバー攻撃は、理想的には、サーバのセキュリティホールをなくすことによって、未然に防止することができる。しかし、ソフトウェアのセキュリティホールを完全になくすことは非常に困難であり、現実的には不可能である。また、ソフトウェアの作成者とサーバ運用者は一般には同一でないため、サーバ運用者がソフトウェアの仕様を誤解して、セキュリティ上問題のある設定をしてしまう可能性は排除することができない。
- [0006] 従来、セキュリティを検証するための装置として、例えば、特開2002-229946号公報、あるいはhttp://www.isskk.co.jp/product/Internet_Scanner.htmlから入手できるインターネット文書“Internet Scanner”には、サーバ等の脆弱点の有無を検査し、コンピュータシステムのセキュリティの強さを判断するセキュリティ検証装置が提案されている。このセキュリティ検証装置は、具体的には、図1に示すように、擬似攻撃部520と、反応検査部530と、脆弱点データベース510から構成されている。
- [0007] 図1に示すセキュリティ検証装置では、擬似攻撃部520が、検査対象となるコンピュータシステムの構成に従い、脆弱点データベース510から、検査対象を擬似攻撃するための予め用意された攻撃手順を取り出す。擬似攻撃部520は、取り出した攻撃手順を使用して、検査対象を擬似攻撃する。反応検査部530は、攻撃された検査対象を調べ、検査対象の反応を、攻撃手順に応じて予め定義されている反応と比較し、検査対象の脆弱点の有無を確認する。図1に示すセキュリティ検証装置は、上記のようにして、すべての検査対象に擬似攻撃を実行し、脆弱点の有無から検査対象のセキュリティを検証するシステムである。
- [0008] また、http://www.isskk.co.jp/product/System_Scanner.htmから入手できるインターネット文書“System Scanner”には、予め用意されている推奨設定との比較により、対象となるコンピュータシステムのセキュリティを検証するシステムが開示されている。このシステムでは、推奨設定がデータベースに登録されており、その推奨設定と検査対象のコンピュータにおける実際の設定とを比較することによってセキュリティが検証される。
- [0009] さらに、Ronald W. Ritchey and Paul Ammannは、2000 IEEE Symp

osium on Security and Privacy, pp. 156–165, March 2000において、複数の脆弱点の相互関係をグラフに表現することにより、脆弱点の組み合わせがより大きな脅威となっている場合を検証することができるセキュリティ検証方式を提案している。この方式では、複数の脆弱点をあらかじめ検出し、それらの脆弱点の相互関係をグラフに表現する。

- [0010] 例えば、検証対象のシステムに2つの脆弱点があるとする。1つ目がインターネットを経由してユーザ権限を奪取できる脆弱点であり、2つ目が任意のユーザが管理者の権限を奪取できる脆弱点ある。このとき2つ目の脆弱点である「任意のユーザが管理者の権限を奪取できる」脆弱点は、直接、外部の者が利用することはできないため、脆弱点としては深刻ではない。このため、1つの脆弱点を検査するシステムでは、2つ目の脆弱点があったとしてもシステム全体としては、問題なしと判断することが多い。しかし、1つ目の脆弱点を利用したあとであれば、2つ目の脆弱点を利用することができる。つまり、この2つの脆弱点を組み合わせではじめて深刻な脆弱点と判断できるのである。このような脆弱点の組み合わせを検証するために、ある脆弱点を利用した後で利用できる脆弱点を網羅的に有向グラフで連結していく。Ritcheyらのシステムは、このようにして、複数の脆弱点の組み合わせを検証するシステムである。

特許文献1:特開2002-229946号公報

非特許文献1:“Internet Scanner”、[online]、[2003年10月27日検索]、インターネット<URL:http://www.isskk.co.jp/product/Internet_Scanner.html>

非特許文献2:“System Scanner”、[online]、[2003年10月27日検索]、インターネット<URL:http://www.isskk.co.jp/product/System_Scanner.html>

非特許文献3:ロナルド・W・リッチー(Ronald W. Ritchey)、ポール・アンマン(Paul Ammann)著、「2000 IEEE Symposium on Security and Privacy」,(米国), IEEE, 2000年3月, p. 156–165

発明の開示

発明が解決しようとする課題

- [0011] 上記の各従来技術では、セキュリティ設定の内容を検証対象とすることができないため、セキュリティ設定が不適設定であるか否かを検証することができないという問題点がある。すなわち、上記の各従来技術では、セキュリティ設定を検証するための擬似攻撃を行うことはできない。具体的には、例えば、図1に示したセキュリティ検証システムや、複数の脆弱点の相互関係をグラフに表現するセキュリティ検証システムでは、擬似攻撃方式と呼ばれる検査方式が採用されている。この検査方式では、脆弱点にあわせた攻撃手順をあらかじめ用意し、実際に攻撃することによって検査を行うことになる。このため、攻撃手順をあらかじめ作成できる脆弱点だけが検査の対象となり、擬似攻撃を作成することができないセキュリティ設定については、検証することができない。
- [0012] 推奨設定との比較による方法では、セキュリティ設定における設定ミスの有無を検証するようにしているが、セキュリティ設定における明らかな設定ミスの検証しか行うことができない。すなわちこの方法では、パスワードが空であった場合などの各設定単独で検証が可能であるような、明らかな設定ミスについてしか検証対象とすることができず、各設定のそれぞれによっては設定ミスか否かの判断が困難であるような、複合的な設定ミスに基づく不適設定の有無を検証することはできない。一方、不正アクセスの多くは設定ミスが原因で起こっているため、障害となる設定ミスがあるか否かについては、厳格に検証できるようにすることが望ましい。
- [0013] 上記の各従来技術では、複数のセキュリティ設定の組み合わせにより不適設定となっているかどうかを判断することができないという問題点もある。すなわち上記の各従来技術では、複合的な設定ミスに基づく不適設定の有無を検証することはできない。具体的には、図1に示した検証システムや推奨設定との比較に基づく検証システムは、単一の脆弱点もしくは単一の設定だけでコンピュータシステムが脆弱となるようなセキュリティホールの有無を検査対象としており、複数のセキュリティ設定の組み合わせを検証の対象にすることはできない。個々の設定自体で見ればミスとは言えず、セキュリティホールではないと判断されるようなものであっても、そのようなセキュリティ設定が複数合わさることによってコンピュータシステムのセキュリティホールとなることがあるが、これらの従来技術では、そのようなセキュリティホールを検出することができな

い。

[0014] Ritcheyらのシステムでは、セキュリティホールとなるような、複数の脆弱点の組合せの有無を検証するようにしているが、セキュリティ設定の設定ミス自体は検証対象とされていない。

[0015] さらに、上述した従来の各システムでは、検査対象システムに対する負荷が高いという問題点もある。具体的には、図1に示した検証システムは、擬似攻撃方式と呼ばれる検査方式を用いるものであって、この方式では、脆弱点を利用する攻撃を実際に行うため、検査対象のシステムは、実際に攻撃されるのと同じ負荷を受けることになり、場合によっては、検査対象のシステムのダウンを引き起こすおそれがある。したがって、図1に示した検証システムは、検証対象のシステムの状況によっては適用できなくなる場合がある。しかしながら、セキュリティ検証システムとしては、検証対象のシステムあるいはコンピュータがいかなる状態にあっても、それらの検証対象のシステムあるいはコンピュータのセキュリティを検証できるものであることが望ましい。

[0016] また、セキュリティの検証を行う場合には、セキュリティ検証システムに対する入力データが必要であるが、そのような入力データを容易に生成できるようにすることも好ましい。

[0017] そこで、本発明の目的は、セキュリティの検証を行うシステムに対する入力データを容易に生成できるデータ生成方法及びシステムを提供することにある。

[0018] 本発明の別の目的は、上述した問題を解消し、セキュリティ設定の厳格な検証ができる検証方法及びシステムを提供することにある。

[0019] 本発明のさらに別の目的は、複数のセキュリティ設定が複合的に作用することで発生する障害の有無を検証することができる方法及びシステムを提供することにある。

[0020] 本発明のさらに別の目的は、検証時における検査対象のシステムの負荷を低減させることができる方法及びシステムを提供することにある。

課題を解決するための手段

[0021] 本発明の目的は、検証対象システムにおけるセキュリティ設定の複合的な誤りを示す不適設定の有無を検証するセキュリティ検証システムへの入力データである検証ポリシーを生成するセキュリティ検証用データ生成方法であって、検証対象システム

におけるネットワーク、アプリケーション、ファイル、サービス及びユーザのうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むシステム構成情報を収集する段階と、システム構成情報に付加される属性情報であって、ネットワーク、アプリケーション、ファイル、サービス及びユーザの属性のいずれか一つまたはそれらの組み合わせた内容を示す属性情報を受け取る段階と、不適切なデータ移動経路におけるデータの移動元、移動先、及び移動経路のうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むアクセスポリシーを、属性情報を用いて生成する段階と、アクセスポリシーと、システム構成情報及び属性情報とに基づいて、不適切なデータ移動経路を表わす検証ポリシーを生成する段階と、を有する方法によって達成される。

[0022] このような本発明のセキュリティ検証用データ生成方法において、システム構成情報を収集する段階は例えばシステム構成情報収集手段によって実行され、属性情報を受け取る段階は例えば属性情報入力手段によって実行され、アクセスポリシーを生成する段階は例えばアクセスポリシー生成手段によって実行され、検証ポリシーを生成する段階は例えば検証ポリシー生成手段によって実行される。さらに、このセキュリティ検証用データ生成方法においては、検証対象システムにおけるデータ移動を表わすデータ移動経路と検証ポリシーとを用いて、検証対象システムにおけるデータ移動経路が適切であるか否かを検証する段階を設けてもよい。このような検証する段階は、例えば、検証手段によって実行される。検証する段階を設けることにより、検証用データの生成から検査対象システムのセキュリティ設定の検証までを一連の処理として実行することが可能になる。

[0023] 本発明の目的は、検証対象システムにおけるセキュリティ設定の複合的な誤りを示す不適設定の有無を検証するセキュリティ検証システムへの入力データである検証ポリシーを生成するセキュリティ検証用データ生成システムであって、検証対象システムにおけるネットワーク、アプリケーション、ファイル、サービス及びユーザのうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むシステム構成情報を収集するシステム構成情報収集手段と、システム構成情報に付加される属性情報であって、ネットワーク、アプリケーション、ファイル、サービス及びユーザの属性

のいずれか一つまたはそれらの組み合わせた内容を示す属性情報が入力される属性情報入力手段と、不適切なデータ移動経路におけるデータの移動元、移動先、及び移動経路のうちの少なくともいずれか一つまたはその組み合わせからなる情報を含むアクセスポリシーを、属性情報を用いて生成するアクセスポリシー生成手段と、アクセスポリシー生成手段によって生成されたアクセスポリシーと、システム構成情報及び属性情報とに基づいて、不適切なデータ移動経路を表わす検証ポリシーを生成する検証ポリシー生成手段と、を有するシステムによっても達成される。

[0024] 本発明のシステムにおいて、属性情報入力手段は、システム構成情報収集手段が収集したシステム構成情報を表示して、属性情報の入力をオペレータに促す構成であってもよい。そのような構成によれば、システム構成情報をオペレータに提示することで、検証対象システムのシステム構成に則った検証ポリシーを容易に作成することができるようになる。

[0025] 本発明のシステムにおいて、アクセスポリシー生成手段は、属性情報を選択肢として表示してオペレータに属性情報の選択を促し、選択された属性情報によって移動元、移動先、または移動経路を指定する構成のものであってもよい。そのような構成によれば、オペレータは、検証対象システムの個々の要素を直接指定する必要がなく、属性情報を選択することで検証ポリシーを作成することができる。したがって、オペレータは、検証対象システムのシステム構成の詳細を知らなくても、検証ポリシーを作成することができる。

[0026] 本発明のシステムにおいて、検証ポリシー生成手段は、属性情報を用いて指定されたアクセスポリシー内の移動元、移動先、または移動経路の情報を、システム構成情報または属性情報に含まれる情報に置き換えることにより検証ポリシーを生成する構成のものであってもよい。

[0027] さらに本発明のシステムは、検証対象システムにおけるデータ移動を表わすデータ移動経路と検証ポリシーとを用いて検証対象システムにおけるデータ移動経路が適切であるか否かを検証する検証手段をさらに備えていてもよい。そのような構成を採用することにより、検証用データの生成から検査対象システムのセキュリティ設定の検証までを一貫して行うことが可能になる。

[0028] 本発明の目的は、検証対象システムにおけるセキュリティ設定の複合的な誤りを示す不適設定の有無を検証するセキュリティ検証システムへの入力データである検証ポリシーを生成するコンピュータに搭載されるセキュリティ検証用データ生成プログラムであって、コンピュータに、検証対象システムにおけるネットワーク、アプリケーション、ファイル、サービス及びユーザのうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むシステム構成情報を収集する処理、システム構成情報に付加される属性情報であって、ネットワーク、アプリケーション、ファイル、サービス及びユーザの属性のいずれか一つまたはそれらの組み合わせた内容を示す属性情報を受け取る処理、不適切なデータ移動経路におけるデータの移動元、移動先、及び移動経路のうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むアクセスポリシーを、属性情報を用いて生成する処理、及び、アクセスポリシーと、システム構成情報及び属性情報とに基づいて、不適切なデータ移動経路を表わす検証ポリシーを生成する処理、を実行させるプログラムによっても達成される。

[0029] 本発明のプログラムは、コンピュータに、さらに、検証対象システムにおけるデータ移動を表わすデータ移動経路と検証ポリシーとを用いて、検証対象システムにおけるデータ移動経路が適切であるか否かを検証する処理を実行させるように構成されていてもよい。

[0030] 本発明によれば、属性情報を入力することにより、容易に検証ポリシーを作成することができるようになる。また、1つの属性情報で複数のシステム構成要素を同時に指定することができるので、少ないアクセスポリシー数で、必要十分な検証ポリシーを作成することができるようになる。

図面の簡単な説明

[0031] [図1]図1は、従来のセキュリティ検証システムの構成を示すブロック図である。

[図2]図2は、本発明のデータ生成方法によって作成されたデータを用いるセキュリティ検証システムの第1の構成を示すブロック図である。

[図3]図3は、設定情報格納部に格納されるデータの構造の例を示す図である。

[図4]図4は、プログラム動作情報格納部に格納されるデータの構造の例を示す図である。

[図5]図5は、データ伝達経路情報格納部に格納されるデータの構造の例を示す図である。

[図6]図6は、図2に示すセキュリティ検証システムが実行するセキュリティ検証処理を示すフローチャートである。

[図7]図7は、セキュリティ検証システムの第2の構成を示すブロック図である。

[図8]図8は、図7に示すセキュリティ検証システムが実行するセキュリティ検証処理を示すフローチャートである。

[図9]図9は、セキュリティ検証システムの第3の構成を示すブロック図である。

[図10]図10は、セキュリティ検証システムの第4の構成を示すブロック図である。

[図11]図11は、セキュリティ検証システムの第5の構成を示すブロック図である。

[図12]図12は、ポリシー格納部に格納されるポリシーの構造の例を示す図である。

[図13]図13は、図12に示すセキュリティ検証システムが実行するセキュリティ検証処理を示すフローチャートである。

[図14]図14は、図11に示したセキュリティ検証システムにおける検証部が実行する処理を示すフローチャートである。

[図15]図15は、ポリシーを変換する規則の例を示す図である。

[図16]図16は、本発明の第1の実施の形態のセキュリティ検証用データ生成システムの構成を示すブロック図である。

[図17]図17は、ネットワーク構成情報の例を示す図である。

[図18]図18は、アプリケーション情報の例を示す図である。

[図19]図19は、ファイル情報の例を示す図である。

[図20]図20は、サービス情報の例を示す図である。

[図21]図21は、ユーザ情報の例を示す図である。

[図22]図22は、図16に示すセキュリティ検証用データ生成システムの動作を示すフローチャートである。

[図23]図23は、本発明の第2の実施の形態のセキュリティ検証用データ生成システムの構成を示すブロック図である。

[図24]図24は、図23に示したセキュリティ検証用データ生成システムの動作を示す

フローチャートである。

[図25]図25は、図23に示したセキュリティ検証用データ生成システムの動作を示すフローチャートである。

[図26]図26は、セキュリティ検証システムの構成を示すブロック図である。

[図27A]図27Aは、検査対象コンピュータにおけるOSのユーザアカウントの設定の例を示す図である。

[図27B]図27Bは、検査対象コンピュータにおけるOSのグループの設定の例を示す図である。

[図28]図28は、検査対象コンピュータにおけるファイルのアクセス権の設定の例を示す図である。

[図29A]図29Aは、検査対象コンピュータにおけるウェブサーバの設定の例を示す図である。

[図29B]図29Bは、検査対象コンピュータにおけるウェブサーバの設定の例を示す図である。

[図30]図30は、検査対象コンピュータにおける、OSのセキュリティ設定情報に基づいて生成されたデータ伝達経路を表わすグラフを示す図である。

[図31]図31は、検査対象コンピュータにおける、OSが管理するディレクトリ構造から作られるアークとオブジェクトとが加えられたデータ伝達経路を表わすグラフを示す図である。

[図32]図32は、検査対象コンピュータにおける、ウェブサーバのセキュリティ設定情報に基づいて生成されたデータ伝達経路を表わすグラフを示す図である。

[図33]図33は、データ伝達経路生成部によって生成されるデータ伝達経路を表わすグラフを示す図である。

[図34]図34は、アクセス権統合処理の例を示すフローチャートである。

[図35]図35は、データ伝達経路生成部によって生成されるデータ伝達経路を表わすグラフを示す図である。

[図36]図36は、アクセス権統合部によって1つのアクセス権が統合された状態のデータ伝達経路を表わすグラフを示す図である。

[図37]図37は、アクセス権統合部によってすべてのアクセス権が統合された状態のデータ伝達経路を表わすグラフを示す図である。

[図38]図38は、データ伝達経路変換部に入力されるデータ伝達経路の例を表わすグラフを示す図である。

[図39]図39は、データ伝達経路変換部から出力される変換後のデータ伝達経路の例を表わすツリー構造を示す図である。

[図40]図40は、データ伝達経路変換処理を示すフローチャートである。

[図41]図41は、ポリシー入力部により入力されるセキュリティ検証用ポリシーの例を示す図である。

[図42]図42は、パターンマッチング処理によって探索された不適経路を表わすグラフを示す図である。

[図43]図43は、不適経路検索処理を示すフローチャートである。

[図44]図44は、探索された不適経路を取り出して示す図である。

[図45]図45は、設定情報検索処理を示すフローチャートである。

[図46]図46は、アクセス権の統合後のデータ伝達経路から不適経路に含まれるノードが検索された状態の例を示す図である。

[図47]図47は、アクセス権の統合前のデータ伝達経路における不適経路が検索された状態の例を示す図である。

[図48]図48は、権限委譲のアークと別名定義のアークとそれらのアークに接続されているノードが検索された状態の例を示す図である。

[図49]図49は、不適経路を作成する原因となった全てのノードとアークが検索された状態の例を示す図である。

[図50]図50は、データ伝達経路情報における不適設定箇所を表わした状態の例を示す図である。

[図51]図51は、設定情報格納部から取り出されたセキュリティ設定情報の例を示す図である。

[図52]図52は、パターンマッチング処理によって探索された不適経路の表示画面の例を示す図である。

[図53]図53は、セキュリティ検証システムにおけるユーザインターフェ이스の全体像を示す基本画面の例を示す図である。

[図54]図54は、トポロジー画面の例を示す図である。

[図55]図55は、トポロジー画面の例を示す図である。

[図56]図56は、ポリシー画面の例を示す図である。

[図57]図57は、アラート画面の例を示す図である。

[図58]図58は、リザルト画面の例を示す図である。

[図59]図59は、ディテール画面の例を示す図である。

[図60]図60は、セキュリティ検証システムの他の構成を示すブロック図である。

[図61A]図61Aは、データ伝達経路変換部から出力される変換後のデータ伝達経路の例を表わすツリー構造を示す図である。

[図61B]図61Bは、データ伝達経路変換部から出力される変換後のデータ伝達経路の例を表わすツリー構造を示す図である。

[図62]図62は、データ伝達経路変換処理の他の例を示すフローチャートである。

[図63]図63は、検証対象のホスト構成を示す図である。

[図64]図64は、設定モデル格納部に格納されたホスト構成を示す図である。

[図65]図65は、検証対象システムのIPアドレス構成とホストとの関係を示す図である。

[図66]図66は、検証対象システムを構成するホストにおけるIPアドレスの設定を示す図である。

[図67]図67は、設定モデル格納部に格納されたIPアドレスを示す図である。

[図68]図68は、検証対象システムのネットワーク接続を示す図である。

[図69]図69は、設定モデル格納部に格納された設定モデルの要素を示す図である。

[図70]図70は、検証対象システムのシステム構成を示す図である。

[図71]図71は、検証対象システムのユーザ設定を示す図である。

[図72]図72は、検証対象システムのグループ設定を示す図である。

[図73]図73は、設定モデル格納部に格納されたユーザを示す図である。

[図74]図74は、検証対象システムのファイルアクセス権の設定を示す図である。

[図75]図75は、設定モデル格納部に格納されたファイルを示す図である。

[図76]図76は、検証対象システムの検証結果の表示状態を示す図である。

[図77]図77は、検証対象となるコンピュータシステムの構成を示す図である。

[図78]図78は、ネットワーク構成情報属性が付加されたネットワーク構成情報の例を示す図である。

[図79]図79は、サービス情報属性が付加されたサービス情報の例を示す図である。

[図80]図80は、ユーザ情報属性が付加されたユーザ情報の例を示す図である。

[図81]図81は、ファイル情報属性が付加されたファイル情報の例を示す図である。

[図82]図82は、作成されたアクセスポリシーの例を示す図である。

[図83]図83は、アクセスポリシー作成時に提示する初期画面の例を示す図である。

[図84]図84は、アクセスポリシー新規作成画面の例を示す図である。

[図85]図85は、移動元入力画面の例を示す図である。

[図86]図86は、移動先入力画面の例を示す図である。

[図87]図87は、移動経路入力画面の例を示す図である。

[図88]図88は、属性情報を用いて移動元や移動先としてユーザが指定されているときに、そのユーザから変換されるユーザアカウントを検索する動作を示すフローチャートである。

[図89]図89は、属性情報を用いて移動元や移動先としてファイルが指定されているときに、そのファイルから変換されるファイル名を検索する動作を示すフローチャートである。

[図90]図90は、属性を用いて移動経路としてサービスが指定されているときに、そのサービスから変換されるIPアドレスやポート番号を検索する動作を示すフローチャートである。

符号の説明

- [0032] 1401 コンピュータシステム
- 1402 システム構成情報収集部
- 1403 属性情報入力部

- 1404 属性情報格納部
- 1405 アクセスポリシー生成部
- 1406 アクセスポリシー格納部
- 1407 検証ポリシー生成部
- 1408 検証ポリシー格納部
- 1509 データ伝達経路入力部
- 1510 検証部
- 1511 検証結果表示部

発明を実施するための最良の形態

[0033] 本発明は、セキュリティ検証システムに与える入力データを生成するための方法及びシステムに関するものなので、まず、本発明にしたがって生成される入力データが与えられることとなるセキュリティ検証システムについて説明する。本発明によって作成された入力データを使用できるセキュリティ検証システムとしては各種のものが考えられるが、以下では、そのようなセキュリティ検証システムについて、5通りの構成例を説明する。なお、以下の説明において、セキュリティ検証システムのユーザあるいはオペレータであって、検査対象のシステムのセキュリティ設定の検証を行なおうとするユーザのことを検証者と呼ぶことにする。これに対し、検査対象のシステム自体のユーザについては、そのままユーザと呼ぶことにする。

[0034] 第1のセキュリティ検証システム：

図2は、第1のセキュリティ検証システム100の構成を示している。図2に示すように、セキュリティ検証システム100は、検査対象111のセキュリティ設定を検証するものであって、ポリシー入力部10と、データ伝達経路生成部21と、プログラム動作情報格納部30と、設定情報格納部31と、データ伝達経路情報格納部32と、ポリシー格納部33と、アクセス権統合部40と、検証部50と、検証結果表示部60と、設定情報収集部70と、設定情報検索部80と、を備えている。

[0035] 検査対象111は、セキュリティ検証システム100による、セキュリティ設定上の誤りの検証対象となるコンピュータを意味する。具体的には、検証対象111としては、例えば、OS（オペレーティングシステム）、ウェブ(web)サーバ、ウェブ(web)クライアント

などが該当する。

- [0036] 設定情報収集部70は、検証対象のシステム111から、検証対象システム111内のセキュリティ設定を示すセキュリティ設定情報を収集し、設定情報格納部31に格納する処理を実行する機能を有する。言い換えれば、設定情報収集部70は、検査対象111のコンピュータシステムから、セキュリティに関連する設定情報を収集する。ここで、「セキュリティに関連する設定情報」すなわちセキュリティ設定情報とは、対象アプリケーションと、セキュリティ単位情報と、設定情報ファイル名とを含む情報を意味する。なお、セキュリティ単位情報のことを「セキュリティ設定情報」と言う場合もある。
- [0037] 設定情報格納部31は、例えばデータベース装置によって構成され、設定情報収集部70により収集されたセキュリティ設定情報を、設定情報IDとともに格納する。図3は、設定情報格納部31でのデータの格納態様の例を示している。図示されるように、設定情報格納部31には、例えば、設定情報IDと、セキュリティ設定情報とが格納される。
- [0038] 「設定情報ID」とは、各セキュリティ単位情報に対応して付与され、セキュリティ単位情報を識別するために一意に決められる識別符号である。「設定情報ID」には、セキュリティ単位情報の他、設定情報ファイル名と対象アプリケーションとが対応付けされている。
- [0039] 「対象アプリケーション」とは、セキュリティ検証の対象となるアプリケーションプログラムを意味する。具体的には、例えば、OS、ウェブサーバ、ウェブクライアントのうち、対応するセキュリティ単位情報が示すセキュリティ設定がなされているアプリケーションが、「対象アプリケーション」に該当する。
- [0040] 「セキュリティ単位情報」とは、アーク(arc)やノード(node)を生成する原因となるセキュリティ設定情報の最小単位を示す情報である。具体的には、設定情報格納部31に格納されるセキュリティ単位情報には、例えば、対象アプリケーションに設定されている設定情報ファイルの内容、対象アプリケーションのユーザ管理ファイルの内容、ファイルやディレクトリに対するアクセス権などが該当する。
- [0041] 「設定情報ファイル名」とは、各セキュリティ単位情報の名称を示すものであって、具体的には、セキュリティ単位情報を含むファイルの名前、もしくは、セキュリティ単位情

報のコンピュータシステム内における格納場所を示す情報である。

- [0042] セキュリティ設定情報には、例えば、セキュリティ設定検証の対象となるアプリケーションプログラムの名称、ファイル名などの設定情報の格納場所の名称、ファイルまたはディレクトリの構造を示すファイル情報、対象アプリケーションによって管理されるユーザの情報を表わすユーザ情報、ユーザとファイルまたはディレクトリとの間のアクセス権を表わすアクセス権情報、プログラムの種別、バージョン情報、ネットワーク構成情報、ネットワークへのアクセス権の設定情報、脆弱点修正プログラム適用情報、ネットワークフィルタリングの設定情報、IP (Internet Protocol) アドレス、ホスト名などの情報のうちの少なくとも1つが含まれる。
- [0043] プログラム動作情報格納部30は、セキュリティ設定収集部70が収集したセキュリティ設定情報から、検証対象システム111で用いられるプログラムの動作仕様を記述したプログラム動作情報を記憶保持する。「プログラム動作情報」は、ノードまたはアークを生成するために必要な情報であって、セキュリティ設定情報と、モデル上に作成するノードまたはアークの種類とを含む情報である。プログラム動作情報格納部30には、検証対象システム111で用いられるプログラムの種別やバージョンごとに、プログラム動作情報が格納される。ここで、「モデル上に作成するノードまたはアークの種類」は、プログラムの種類、バージョン情報、及び、そのバージョン情報に基づいてモデル上に作成されるノードまたはアークの種類を意味する。
- [0044] なお、「プログラム動作情報」には、脆弱点情報が含まれていてもよい。脆弱点情報をプログラム動作情報に含まれることにより、プログラムの不備などといった脆弱点も、プログラム動作情報としてモデルに反映させることができるようになる。
- [0045] 図4は、プログラム動作情報格納部30でのデータの格納態様を例示している。プログラム動作情報格納部30には、図示されるように、セキュリティ設定情報とモデル上に作成するノードまたはアークの種類を示す情報とが対応付けされているプログラム動作情報が格納されている。
- [0046] プログラム動作情報に含まれるセキュリティ設定情報は、検査対象111を示す対象アプリケーションと、セキュリティ単位情報と、設定情報ファイル名とを含む。図4に示すように、「セキュリティ単位情報」には、ファイル情報、ユーザ情報、グループ情報な

どがある。「モデル上に作成するノードまたはアークの種類を示す情報」は、後述するホストレイヤ、ファイルノード、ユーザノード、グループノード、別名定義を表わすアークなど、モデル上に作成するホストレイヤ、ノード、あるいはアークを示す情報となっている。

[0047] データ伝達経路生成部21は、検証対象システム111のセキュリティ設定情報(図3参照)と、プログラム動作情報(図4参照)とに基づいて、データ伝達経路を生成する機能を有する。ここで説明している例では、検査対象システム111内でのデータが伝達する経路をモデル化したデータ伝達経路が生成される。

[0048] 「データ伝達経路」は、検査対象システム111のセキュリティ設定情報やプログラムの動作情報から決定される検査対象システム111内のデータの移動経路(伝達経路)をモデル化し、有向グラフで表現したものである。データ伝達経路の詳細については、図33などを用いて後述するが、データ伝達経路は、1つのコンピュータを表わすホストレイヤと、1つのプログラムを表わすプログラムレイヤとによって表現される。

[0049] データ伝達経路において、プログラムレイヤは、ホストレイヤ上に表現される。プログラムレイヤは、ホストレイヤ上に複数あってもよい。プログラムレイヤは、対象となるプログラムによって管理されるアーク及びノードで表現される。プログラムレイヤが複数あるときは、複数のプログラムによって管理されるアークを含むプログラム間レイヤがあってもよい。また、複数のホストレイヤがあるときは、複数のホストレイヤによって管理されるアークを含むホスト間レイヤがあってもよい。なお、すべてのノードが一意に表現される場合には、レイヤ構造を持たなくともよい。

[0050] ホストレイヤは、コンピュータやルータなどのネットワーク機器ごとに作られ、それらの機器に含まれるプログラムを表わすプログラムレイヤや、プログラム間レイヤを含む。

[0051] プログラムレイヤは、コンピュータやルータなどのネットワーク機器に含まれるプログラムごとに作られる。プログラムレイヤには、それぞれのプログラムで管理されるノードや、ノードの関係を表わすアークが含まれる。

[0052] 結局、「データ伝達経路」は、ノードと、ノードの関係を表わすアークと、それらの構造を表わすレイヤとで表現される。ノードの関係を表わすアークすなわち有向グラフ

のアーキには、データの移動を表わすデータ移動関係と、ユーザ、グループ間の所属を表わす所属関係と、ファイルまたはディレクトリやユーザまたはグループの別名定義を表わす別名定義関係と、他のユーザに権限を譲渡する権限委譲関係とのうちの少なくとも1つが含まれる。データの移動としては、データの書き込みや読み込みなどが例示される。

[0053] 「データ移動関係」は、ユーザまたはグループがファイルまたはディレクトリに対するアクセス権があることと、ユーザまたはグループがネットワークストリームに対してデータを送受信可能なことを表わす。具体的には、例えば、ユーザノードまたはグループノードから、ファイルノードに向かうデータ移動関係のアーキは、ユーザまたはグループがデータをそのファイルまたはディレクトリに対して書き込むことが可能なことを表わす。ファイルノードまたはグループノードからユーザノードに向かうデータ移動関係のアーキは、ファイルまたはディレクトリのデータを、そのユーザまたはグループが読み込み可能なことを表わす。ユーザノードまたはグループノードからネットワークノードに向かうデータ移動関係のアーキは、そのユーザまたはグループがネットワークストリームに対してデータを送信できることを表わす。また、ネットワークノードからユーザノードまたはグループノードに向かうデータ移動関係のアーキは、そのユーザまたはグループがネットワークストリームからデータを受信可能なことを表わす。そして、ネットワークノード間のデータ移動関係のアーキは、ネットワークストリームの間でデータを送受信可能であることを表わす。

[0054] 「所属関係」は、ユーザがグループに所属していることを表わす。具体的には、例えば、ユーザノードからグループノードに向かう所属関係のアーキは、ユーザがアーキでつながれたグループに所属していることを表わす。

[0055] 「別名定義関係」は、複数のファイルが同一のファイルであることを表わす。具体的には、例えば、ファイルノードからファイルノードへ向かう別名定義関係のアーキは、両端のノードを管理するプログラムやファイルの名前は異なるが、実体は同一のものであることを表わす。

[0056] 「権限委譲関係」は、複数のユーザまたはグループが、同一のユーザまたはグループであることを表わす。また「権限委譲関係」は、あるユーザまたはグループが行う操

作が、他のユーザまたはグループの権限によって行われることを表わす。具体的には、例えば、第1のユーザまたはグループから、第2のユーザまたはグループに対する権限委譲関係のアーキは、第1のユーザまたはグループが、第2のユーザまたはグループと同一であること、または、第1のユーザまたはグループが、第2のユーザまたはグループの権限で操作を行うことを表わしている。

- [0057] グラフのノードには、データを表わすファイルノード、ネットワークサービスが利用するネットワークストリームを表わすネットワークノード、ユーザアカウントを表わすユーザノード、ユーザアカウントのグループを表わすグループノードのうちの少なくとも1つが含まれる。
- [0058] 図2に示したセキュリティ検証システム100において、データ伝達経路生成部21は、設定情報収集部70が収集したセキュリティ設定情報にしたがって、検査対象システム111で用いられるプログラムの動作仕様をプログラム動作情報格納部30に問い合わせ、検査対象システム111で実行され得る動作を示すプログラム動作情報と、セキュリティ設定情報とに基づいて、プログラム内でのデータ伝達経路を生成する。
- [0059] データ伝達経路情報格納部32は、例えばデータベース装置によって構成され、データ伝達経路生成部21が生成したデータ伝達経路と、そのデータ伝達経路に含まれるアーキ及びノードを作成する原因となったセキュリティ設定情報もしくはそのセキュリティ設定情報の保存場所を示す情報(設定情報ID)とを含むデータ伝達経路情報を格納する。ここで格納されるデータ伝達経路情報は、ノードとアーキの接続関係が分かり、モデル化されたデータ伝達経路が生成できる情報とされる。なお、データ伝達経路情報格納部32に保存するデータ伝達経路情報は、アクセス権統合部40によってアクセス権が統合されたあとのデータ伝達経路情報であってもよい。
- [0060] 図5は、データ伝達経路情報格納部32でのデータの格納態様の一例を示している。データ伝達経路情報格納部32には、データ伝達経路をモデル化して表現するためのプログラムが格納される。
- [0061] データ伝達経路情報格納部32に格納されるプログラムのデータ構造は、図5に示すように、1つのコンピュータに関する情報を格納する領域(図5での領域「I」)と、プログラムに関する情報を格納する領域(図5での領域「G」)と、複数のプログラムに関

わる情報を格納する領域(図5での領域「H」)と、アークに関する情報を格納する領域(図5での領域「F」)と、ノードに関する情報を格納する領域(図5における領域「C」)と、ノードまたはアークを生成する原因となったセキュリティ設定情報の識別符号(設定情報ID)を格納する領域(図5での領域「B」、「E」)と、ノードまたはアークに接続するアークまたはノードの識別符号を格納する領域(図5での領域「A」、「D」)とを含む。これらの領域のそれぞれは、複数あってもよく、コンピュータに関する情報を格納する領域が複数ある場合には、複数のコンピュータが関係する情報を格納する領域(図5での領域「J」)があってもよい。

- [0062] また、図5に示した各領域において、name属性には名前が、ID属性に識別符号が、type属性にアークまたはノードの種類が格納される。具体的には、type属性は、例えば、データ移動関係の場合には“transfer”、権限委譲関係の場合には“commission”、別名定義関係の場合には“alias”、所属関係の場合には“attach”、ユーザーノードの場合には“user”、グループノードの場合には“group”、ファイルノードの場合には“file”、ネットワークノードの場合には“network”となる。
- [0063] アクセス権統合部40は、複数のプログラムの動作をプログラム動作情報格納部30に問い合わせ、プログラム動作情報に基づいて、複数のプログラムのアクセス権のうち、統合可能な複数のアクセス権を1つのアクセス権に統合する処理を実行する機能を有する。具体的には、アクセス権統合部40は、ノードの関係を表わす最大で4種類(データ移動関係、所属関係、別名定義関係、権限委譲関係)となるアークを、2種類(データ移動関係、所属関係)のアークに統合する処理を行う。なお、アクセス権統合部40は、アクセス権を統合することで、データ伝達経路情報を、セキュリティ検証用ポリシーと容易に比較できるデータに変換する。
- [0064] ポリシー入力部10は、ポリシー格納部33に格納されているセキュリティ検証用ポリシーを読み出して、検証部50に入力する機能を有する。
- [0065] 「ポリシー」は、アクセスをデータの移動経路で表わしたものであり、データの移動経路の少なくとも始点と、終点とを指定する。ポリシーのうち、セキュリティ検証のために、不適切なアクセスをデータの移動経路で表わしたポリシーを、図41を用いて後述するように、特に「セキュリティ検証用ポリシー」と呼ぶ。すなわち、「セキュリティ検証

用ポリシー」とは、検査対象システム111上の不適切なデータ伝達経路が指定されたポリシーを意味する。不適切なデータ伝達経路には、例えば、あってはならないデータ伝達経路や、不正なデータ伝達経路が含まれる。「セキュリティ検証用ポリシー」は、例えばシステム管理者などによって、あらかじめ設定されてポリシー格納部33に格納されている。あるいは、「セキュリティ検証用ポリシー」は、後述するように、本発明に基づくセキュリティ検証用データ生成システムによって作成され、ポリシー格納部33に格納されていてもよい。

- [0066] 「ポリシー」は、データの始点、終点だけでなく、途中経路を指定するようにしてもよい。途中経路を指定するようにすれば、情報漏洩などのリスクを考慮し、特定の経路を経由するデータ伝達経路を指定することができる。
- [0067] ポリシーにおいて、始点、終点、途中経路には、コンピュータシステムを構成するノードを指定する。ノードには、ファイルノード、ネットワークノード、ユーザノード、グループノードの少なくとも1つが含まれる。
- [0068] 検証部50は、アクセス権統合部40によってアクセス権が統合されたデータ伝達経路から、セキュリティ検証用ポリシーに記述された経路を探索する処理を実行する機能を有する。検証部50は、データ伝達経路変換部51と、パターンマッチング部52とを含む。
- [0069] データ伝達経路変換部51は、アクセス権統合部40によって複数のアクセス権が統合されたデータ伝達経路を、ポリシー入力部10によって入力されたセキュリティ検証用ポリシーとの比較ができるようなデータに変換する機能を有する。すなわち、データ伝達経路変換部51は、データ伝達経路生成部21によって生成されたデータ伝達経路の表現形式を変換する。複数のアクセス権が統合されたデータ伝達経路については、図37を用いて後述し、セキュリティ検証用ポリシーとの比較ができるようなデータについては、図39を用いて後述する。
- [0070] パターンマッチング部52は、データ伝達経路変換部51によって変換されたデータ伝達経路から、ポリシー入力部10によって入力されたセキュリティ検証用ポリシーに一致するデータ伝達経路を探索する機能を有する。セキュリティ検証用ポリシーに一致するデータ伝達経路のことを不適経路と呼ぶ。

- [0071] 設定情報検索部80は、パターンマッチング部52によって探索されて出力された不適経路を示す情報と、データ伝達経路情報格納部32に格納されたデータ伝達経路情報とを用いて、不適経路が生成される原因となったセキュリティ設定情報(すなわち不適設定情報)を、設定情報格納部31に格納されたセキュリティ設定情報から検索する機能を有する。
- [0072] なお、ここで示すセキュリティ検証システムでは、設定情報検索部80が、設定情報格納部31に格納されたセキュリティ設定情報から不適設定情報を検索する構成とされているが、データ伝達経路情報(図5参照)に、設定情報IDの代わりにセキュリティ設定情報が格納されている場合には、設定情報格納部31を検索することなく、不適設定情報を検索することができる。その場合、設定情報検索部80は、パターンマッチング部52によって探索されて出力された不適経路情報と、データ伝達経路情報格納部32に格納されたデータ伝達経路情報とを用いて、不適経路を生成する原因となったすべてのノードとアークを検索し(後述のステップS291～ステップS294を参照)、上記のデータ伝達経路情報を用いて検索したノード及びアークとともに格納されているセキュリティ設定情報を検索することで、不適設定情報を検索する機能を有する。
- [0073] 検証結果表示部60は、例えば液晶表示装置などの表示装置によって構成され、設定情報検索部80によって検索された不適設定情報が示す不適設定を画面表示する機能を有する。よって、このセキュリティ検証システム100は、設定ミスを犯した場所、すなわちセキュリティ設定情報の設定場所を、検査対象システムの管理者に対して指摘することができる。なお、不適経路情報が示す不適経路も表示するようにしてもよい。
- [0074] 次に、第1の構成例のセキュリティ検証システム100の動作について、詳細に説明する。図6は、図2に示したセキュリティ検証システム100が実行するセキュリティ検証処理を示すフローチャートである。
- [0075] セキュリティ検証処理では、まず、ステップS201において、設定情報収集部70は、検証対象111のセキュリティ設定情報を収集し、収集したセキュリティ設定情報を設定情報格納部31に格納する。ステップS202において、データ伝達経路生成部21は、設定情報収集部70によって収集されて設定情報格納部31に格納されたセキュ

リティ設定情報を参照し、プログラム動作情報格納部30に対して検証対象111に関わるプログラム動作情報の問い合わせを行う。すなわち、データ伝達経路生成部21は、設定情報収集部70が収集した、対象アプリケーションのプログラム名、設定情報ファイル名、その設定情報ファイル名が示す設定ファイルに対応付けされているセキュリティ単位情報に基づいて、プログラム動作情報格納部30に対して、モデル上に生成するノードまたはアークの種類を問い合わせる。

- [0076] その後、データ伝達経路生成部21は、設定情報収集部70によって収集されて設定情報格納部31に格納されたセキュリティ設定情報と、ステップS202の問い合わせによって読み出したプログラム動作情報とを用いて、ステップS203において、データ伝達経路情報を生成する。データ伝達経路生成部21は、データ伝達経路情報を生成したあと、生成したデータ伝達経路情報をデータ伝達経路情報格納部32に格納する。
- [0077] データ伝達経路生成部21は、ステップS203において、データ伝達経路情報の作成に際し、各種のノードやアークを作成するので、以下、これらのノードやアークの作成について説明する。
- [0078] データ伝達経路生成部21は、セキュリティ設定情報に含まれるユーザを表わす情報を用いて、作成するノードをプログラム動作情報格納部30に問い合わせ、ユーザ情報に含まれるユーザを表わすユーザノードを作成する。例えば、あるプログラムが管理するユーザIDが含まれていた場合には、ユーザノードを作成する。
- [0079] データ伝達経路生成部21は、セキュリティ設定情報に含まれるグループを表わす情報を用いて、作成するノードをプログラム動作情報格納部30に問い合わせ、グループ情報に含まれるグループを表わすグループノードを作成する。例えば、あるプログラムが管理するグループIDが含まれていた場合には、グループノードを作成する。
- [0080] データ伝達経路生成部21は、セキュリティ設定情報に含まれるサーバが利用するネットワークストリームの情報を用いて、作成するノードをプログラム動作情報格納部30に問い合わせ、ネットワークストリームを表わすネットワークノードを作成する。例えば、あるプログラムが利用するネットワークストリームが書かれていた場合には、ネットワークノードを作成する。

- [0081] データ伝達経路生成部21は、セキュリティ設定情報に含まれるファイル構造を表わす情報を用いて、作成するノードをプログラム動作情報格納部30に問い合わせ、ファイルやディレクトリを表わすファイルノードを作成する。例えば、あるプログラムが管理するファイルやディレクトリ構造が含まれていた場合には、それぞれのファイルやディレクトリに当たるファイルノードを作成する。
- [0082] さらにデータ伝達経路生成部21は、セキュリティ設定情報に含まれるファイル構造や、アクセス権を表わす情報や、プログラムがインストールされているという情報を用いて、作成するアークをプログラム動作情報格納部30に問い合わせ、データ移動関係を表わすアークを作成する。例えば、ユーザがファイルを読み込み可能である場合には、ファイルノードからユーザノードに向かうデータ移動関係を表わすアークを作成する。
- [0083] 同様に、データ伝達経路生成部21は、ファイルにユーザが書き込み可能な場合には、ユーザノードからファイルノードに向かうデータ移動関係を表わすアークを作成する。ユーザがネットワークストリームにデータを送出可能である場合には、データ伝達経路生成部21は、ユーザノードからネットワークノードに向かうデータ移動関係を表わすアークを作成する。ユーザがネットワークストリームからデータを受信可能な場合には、データ伝達経路生成部21は、ネットワークノードからユーザノードに向かうデータ移動関係を作成する。グループがファイルを読み込み可能である場合には、データ伝達経路生成部21は、ファイルノードからグループノードに向かうデータ移動関係を表わすアークを作成する。
- [0084] また同様に、ファイルにグループが書き込み可能な場合には、データ伝達経路生成部21は、グループノードからファイルノードに向かうデータ移動関係を表わすアークを作成する。グループがネットワークストリームにデータを送出可能である場合には、データ伝達経路生成部21は、グループノードからネットワークノードに向かうデータ移動関係を表わすアークを作成する。グループがネットワークストリームからデータを受信可能な場合には、データ伝達経路生成部21は、ネットワークノードからグループノードに向かうデータ移動関係を作成する。ネットワークストリーム間でデータの送受信が可能な場合には、データ伝達経路生成部21は、ネットワークストリーム間でデー

タの移動する方向にあわせてデータ移動関係のアークを作成する。

- [0085] データ伝達経路生成部21は、セキュリティ設定情報に含まれるグループに所属するユーザを特定する情報を用いて、作成するアークをプログラム動作情報格納部30に問い合わせ、所属関係を表わすアークを作成する。例えば、ユーザがグループに所属する場合、ユーザからグループに向かう所属関係のアークを作成する。
- [0086] データ伝達経路生成部21は、セキュリティ設定情報に含まれるプログラムの実行ユーザを表わす情報を用いて、作成するアークをプログラム動作情報格納部30に問い合わせ、権限委譲関係を表わすアークを作成する。例えば、あるプログラムで管理されているユーザが、プログラムの実行ユーザの設定により他のプログラムで管理されている他のユーザとして実行される場合には、あるユーザノードから、他のユーザノードに向かう権限委譲関係のアークを作成する。
- [0087] そして、データ伝達経路生成部21は、セキュリティ設定情報に含まれるサーバのファイル情報やファイル構造情報を用いて、作成するアークをプログラム動作情報格納部30に問い合わせ、権限委譲関係を表わすアークを作成する。例えば、あるプログラムで管理されているファイルが他のプログラムで別の名前で管理されている場合には、あるプログラムで管理されているファイルノードから他のプログラムで管理されているファイルノードに向かう別名定義関係のアークを作成する。
- [0088] アクセス権統合部40は、ステップS204において、データ伝達経路情報格納部32から、データ伝達経路生成部21によって生成されたデータ伝達経路情報を読み出して、読み出したデータ伝達経路情報が示すデータ伝達経路に別名定義関係を示すアークと権限委譲関係を示すアークが含まれていれば、これらのアークの両端にある4つのノードについて同じレイヤに所属するノード間のアクセス権を、レイヤを超えたデータ移動関係に統合する処理を行う。つまり、別名定義関係を表わすアークの起点にあるノードと権限委譲関係を表わすアークの起点にあるノード間のデータの移動と、各々のアークの終点にあるノード間のデータの移動が同じ方向のときに、それらを統合したデータ移動関係のアークを新たに作成し、該当する別名定義関係と権限委譲関係のアークを削除する。ここでデータの移動の方向は、ユーザ(グループ)ノードからファイルノードへのデータの移動の方向、または、ファイルノードからユーザ(グル

ープ)ノードへのデータ移動の方向である。

- [0089] データ伝達経路変換部51は、ステップS205において、複数のプログラムにかかわるアクセス権が統合されたデータ伝達経路情報をアクセス権統合部40から受け取り、受け取ったデータ伝達経路情報を、セキュリティ検証用ポリシーに一致するデータ伝達経路が探索できるようなデータ伝達経路を示すデータ伝達経路情報に変換する処理を行う。そのようなデータ伝達経路の例は、後述するように図39に示されている。
- [0090] 次にステップS206において、ポリシー入力部10は、例えばオペレータからの指示に従い、望ましくないデータの移動経路を示すセキュリティ検証用ポリシーをポリシー格納部33から読み出して、パターンマッチング部52に入力する。
- [0091] パターンマッチング部52は、ステップS207において、データ伝達経路変換部51によって変換されたデータ伝達経路情報と、ポリシー入力部10によって入力されたセキュリティ検証用ポリシーとを比較し、データ伝達経路情報が示すデータ伝達経路にセキュリティ検証用ポリシーに一致するデータ伝達経路があるか否かを探索する。
- [0092] ステップS207での探索処理は、ステップS208に示すように、ポリシー入力部10によって入力されたセキュリティ検証用ポリシーそれぞれについて繰り返し実行され、ポリシー入力部10によって入力された全てのセキュリティ検証用ポリシーについて実行される。ステップS208において、全てのセキュリティ検証用ポリシーについての探索処理を終えたと判断されると、パターンマッチング部52は、探索処理の結果を設定情報検索部80に出力する。
- [0093] 探索処理の結果を受けると、設定情報検索部80は、ステップS209において、不適経路が探索されているかを確認する。不適経路がなかった場合には、そのまま処理を終了してもよいし、不適設定が発見されなかったことを表示してから処理を終了してもよい。
- [0094] ステップS209において不適経路があった場合には、設定情報検索部80は、ステップS210において、設定情報格納部31に格納されているセキュリティ設定情報の中から、探索された不適経路を生成する原因となった不適設定を検索する処理を実行する。そして、検証結果表示部60は、検索結果を受けると、ステップS211において、

検索された不適設定を示す不適設定情報を表示する処理を行い、その後、一連の処理を終了させる。

[0095] 以上説明したように、図2に示したセキュリティ検証システムは、検査対象システム111で用いられているプログラムのセキュリティ設定情報に基づくデータ伝達経路と、望ましくないデータの移動経路を示すセキュリティ検証用ポリシーとを比較して、不適設定に基づく不適経路を含むデータ伝達経路を探索する構成としている。したがってこのセキュリティ検証システムを用いることにより、検証対象システムの個々の設定を検証しただけでは不適設定であるか否かを判定することができないような場合であっても、不適設定であることを特定し、管理者に対して指摘することができるようになる。言い換えれば、このセキュリティ検証システムによれば、それぞれの設定ミス単独では障害は生じないが、それらの設定ミスが複数あることによって支障が出る可能性のある複合的な設定ミスを探索することができるようになり、複合的な設定ミスの有無を検証することができ、セキュリティ設定の検証を厳格に行うことができるようになる。

[0096] 図2に示したセキュリティ検証システムは、検査対象システム111からセキュリティ設定情報を収集し、データ伝達経路をモデル化し、セキュリティ検証用ポリシーを指定することで不適設定の有無を検証する構成としたので、検査対象システム111の実際の稼働状況にあわせて不適設定を特定することができる。したがって、セキュリティ検証システム100を用いることにより、実際に検査対象システム111を安全に運用することができるようになる。すなわち、検証対象システム111の運用前に検証することで、その検証結果を、セキュリティ設定を施す指針とすることができる。また、このセキュリティ検証システム100は、擬似攻撃のような検査対象システム111の負荷が大きくなってしまような方式を採用することなく、複合的な設定ミスの有無を検証するようにしているので、検証時における検査対象システム111の負荷を軽減させることができる。

[0097] 第2のセキュリティ検証システム：

図7は、第2のセキュリティ検証システム100aの構成の一例を示している。以下の説明において、上述の図2に示したセキュリティ検証システム100と同一の構成及び処理を行う部分については、同一の符号を付与してその詳細な説明を省略する。

- [0098] 図7に示すように、セキュリティ検証システム100aは、検査対象111のセキュリティ設定を検証するものであって、設定情報収集部70と、設定情報格納部31と、プログラム動作情報格納部30と、データ伝達経路生成部21と、データ伝達経路情報格納部32と、アクセス権統合部40と、データ伝達経路表示部90とを含む。
- [0099] データ伝達経路表示部90は、例えば液晶表示装置などの表示装置によって構成され、データ伝達経路情報格納部32に格納されているデータ伝達経路情報が示すデータ伝達経路と、設定情報格納部31に格納されているセキュリティ設定情報とを関連付けて画面表示する機能を有する。具体的には、データ伝達経路生成部21によって生成されたデータ伝達経路や、アクセス権統合部40によって生成されたデータ伝達経路を画面表示する。
- [0100] 次に、このセキュリティ検証システム100aの動作について説明する。図8は、セキュリティ検証システム100aが実行するセキュリティ検証処理の一例を示している。
- [0101] セキュリティ検証処理においては、まず、上述したステップS201～ステップS204の処理を実行する。その後、データ伝達経路表示部90は、ステップS401において、データ伝達経路情報格納部32に格納されているアクセス権統合部40が生成したデータ伝達経路情報が示すデータ伝達経路を、設定情報格納部31に格納されているセキュリティ設定情報に関連付けて画面表示する。すなわち、アクセス権統合部40が生成したデータ伝達経路情報が示すデータ伝達経路情報と、そのデータ伝達経路情報に含まれている設定情報IDに対応するセキュリティ単位情報を含むセキュリティ設定情報とを関連付けて表示する。
- [0102] ここで述べた例では、データ伝達経路表示部90が、アクセス権統合部40が生成したデータ伝達経路情報に含まれている設定情報IDに対応するセキュリティ設定情報を、設定情報格納部31を検索して読み出す構成とされている。しかしながら、アクセス権統合部40によって生成されたデータ伝達経路情報に、設定情報IDの代わりにセキュリティ設定情報が格納されている場合には、設定情報格納部31を検索することなくセキュリティ設定情報を特定することができる。この場合、データ伝達経路表示部90は、アクセス権統合部40が生成したデータ伝達経路情報が示すデータ伝達経路を、そのデータ伝達経路情報に含まれているセキュリティ設定情報を認識可能な

表示態様、例えば強調表示で表示するようにすればよい。

- [0103] 以上説明したように、セキュリティ検証システム100aによれば、検証対象システム111からセキュリティ設定情報を収集し、データ伝達経路をモデル化し、データの伝達経路を画面表示する構成としたので、個々の設定だけでは分からない、複数のプログラムがかかわるデータの流れを確認することができる。そのため、システムの検証者は、実際の設定を施した後、データの流れを確認することで、その設定の正しさを検証することができる。また、このセキュリティ検証システム100aでは、データの流れとその流れのつくる原因となっているセキュリティ設定が関連付けて表示されるため、検証者にとっては、複合的な設定ミスの発見が容易となる。

- [0104] 第3のセキュリティ検証システム:

図9は、第3のセキュリティ検証システム100bの構成の一例を示している。以下の説明において、上述の図7に示したセキュリティ検証システム100aと同一の構成及び処理を行う部分については、同一の符号を付与してその詳細な説明を省略する。

- [0105] 図9に示したセキュリティ検証システム100bは、図7に示したセキュリティ検証システム100aと同様のものであるが、アクセス権統合部40が備えられていない点で相違する。

- [0106] ここでは、データ伝達経路表示部90は、データ伝達経路生成部21によって生成されたデータ伝達経路情報が示すデータ伝達経路をそのまま画面表示する。

- [0107] このように、セキュリティ検証システム100bでは、検査対象111のコンピュータシステムのセキュリティ設定情報を収集し、プログラム動作情報にしたがってデータ伝達経路を生成し、生成したデータ伝達経路を表示する構成としている。したがってこのセキュリティ検証システム100bを用いることにより、表示されたデータ伝送経路を確認することによって、個々のセキュリティ設定情報を確認することができ、システム検証者などの者は、特定のプログラムの複合的な設定が間違っているということを、容易に認識することができる。

- [0108] 第4のセキュリティ検証システム:

図10は、第4のセキュリティ検証システム100cの構成の一例を示している。以下の説明において、上述の図2に示したセキュリティ検証システム100と同一の構成及び

処理を行う部分については、同一の符号を付与してその詳細な説明を省略する。

- [0109] 図10に示したセキュリティ検証システム100cは、上述した図2に示したセキュリティ検証システム100と同様のものであるが、データ伝達経路生成部21に代えてデータ伝達経路入力部20が設けられ、設定情報収集部70に代えて設定情報入力部71が設けられている点で相違する。すなわち、このセキュリティ検証システム100cは、データ伝達経路入力部20により、検証者などによって指定されたデータ伝達経路が入力され、設定情報入力部71により、検証者などによって指定されたセキュリティ設定情報が入力される構成とされている。
- [0110] データ伝達経路入力部20は、例えばシステム検証者などのユーザの操作によって指定(選択、入力)されたデータ伝達経路情報を、データ伝達経路情報格納部32に向けて出力し、データ伝達経路情報格納部32に格納させる機能を有する。
- [0111] 設定情報入力部71は、例えばシステム検証者などのユーザの操作によって指定(選択、入力)されたセキュリティ設定情報(図3参照)を、設定情報格納部31に向けて出力し、設定情報格納部31に格納させる機能を有する。また、設定情報入力部71は、検証者などの操作にしたがって、データ伝達経路入力部20によって入力されたデータ伝達経路の各アーク及びノードについて、それらが入力される原因となるセキュリティ設定を示すセキュリティ設定情報をアークやノードに関連付けて入力する機能も有する。検証者などがノードまたはアークを指定するとともに、そのノードまたはアークを作成する原因となるセキュリティ設定情報をあわせて指定したことに応じて、設定情報入力部71は、アークやノードに関連付けされたセキュリティ設定情報を設定情報格納部31に格納する。
- [0112] 上述の機能に加え設定情報入力部71は、例えばシステム検証者などのユーザの操作によって指定されたセキュリティ設定情報を、設定情報格納部31に向けて出力し、設定情報格納部31に格納させる機能と、検証者などの操作にしたがって、データ伝達経路入力部20によって入力されたデータ伝達経路の各アーク及びノードについて、それらが入力される原因となるセキュリティ設定を示すセキュリティ設定情報をアークやノードに関連付けて入力する機能とを有する。
- [0113] このセキュリティ検証システム100cは、システム検証者やシステム管理者などのユ

ユーザが、検査対象111におけるプログラムのセキュリティ設定情報や動作情報を確認し、検証対象システム111内のデータの移動経路を示すデータ伝達経路情報を生成する技能を有している場合に有効である。すなわち、セキュリティ検証システム100cは、検証者あるいは管理者などによって生成されたデータ伝達経路情報に、不適設定に基づく不適経路が含まれているか否かを検証することができる。

[0114] ここで示す例では、セキュリティ検証処理において、設定情報入力部71が、検証者などの操作に応じて、検証者などによって設定されたセキュリティ設定情報を設定情報格納部31に入力する。次いで、データ伝達経路入力部20が、検証者などの操作に応じて、検証者などによって設定されたデータ伝達経路情報をデータ伝達経路情報格納部32に入力する。その後、上述したステップS204～ステップS211の処理が実行される。

[0115] このように、セキュリティ検証システム100cは、システム検証者などのユーザが指定したセキュリティ設定情報及びデータ伝達経路情報を用いてセキュリティ検証処理を実行する構成としたので、システム検証者やシステム管理者によって生成されたデータ伝達経路情報に不適設定に基づく不適経路が含まれているか否かを検証することができる。なお、セキュリティ設定情報またはデータ伝達経路情報のいずれか一方を検証者などが指定するようにしてもよい。

[0116] なお上述の説明において、セキュリティ検証システム100cは、システム検証者などのユーザが指定したセキュリティ設定情報及びデータ伝達経路情報を用いるものとした。しかしながら、セキュリティ検証システム100c以外の他のシステムによって生成されたデータ伝達経路情報や、他のシステムによって収集されたセキュリティ設定情報を用いる構成としてもよい。このように構成すれば、他のシステムによって生成されたデータ伝達経路情報に不適設定に基づく不適経路が含まれているか否かを検証することができる。具体的には、例えばセキュリティ設定や機器の設定を行うシステム、すなわちネットワークやその機器を設定するシステムについて、そのシステムの出力をセキュリティ検証システム100cへの入力とすることで、これから施そうとする設定がセキュリティ検証用ポリシーと一致しているか否かを検証することができ、不適設定の指摘などを行うことができるようになる。それにより、より安全なセキュリティ設定やシス

テム設計を行うための対応を容易にとることができるようになる。また、例えばソフトウェア及びハードウェアなどの資産管理ソフトウェアや、ソフトウェアのバージョンを管理するバージョン管理ソフトウェアと連携し、そのソフトウェアに基づく出力をセキュリティ検証システム100cへの入力とすることで、現在運用中のシステムの設定の不備を指摘することができる。

[0117] 第5のセキュリティ検証システム:

図11は、第5のセキュリティ検証システム100dの構成の一例を示している。以下の説明において、上述の図2に示したセキュリティ検証システム100と同一の構成及び処理を行う部分については、同一の符号を付与してその詳細な説明を省略する。

[0118] 図11に示すように、セキュリティ検証システム100dは、設定モデル入力部11と、設定モデル格納部34と、ポリシー入力部10と、ポリシー格納部33と、検証部50aと、検証結果格納部35と、検証結果表示部60とを含む。

[0119] ポリシー入力部10は、例えばシステム検証者などのユーザによって操作され、セキュリティ検証用ポリシーを記述してポリシー格納部33に格納する機能を有する。

[0120] 設定モデル入力部11は、例えばシステム検証者などのユーザによって操作され、システム構成にしたがった設定モデルが入力される。なお、「設定モデル」については、後で詳しく説明する。ここでは、設定モデル入力部11には、検査対象システムを構成する機器のセキュリティに関連する設定情報であるセキュリティ設定情報を反映した設定モデルが入力される。

[0121] 設定モデル格納部34は、例えばデータベース装置によって構成され、設定モデル入力部11に入力された設定モデルを格納する。

[0122] 検証部50aは、ポリシー格納部33に格納されたポリシーを取り出し、設定モデル格納部34に格納された設定モデルと比較し、セキュリティ検証用ポリシーにマッチする設定モデルが存在するか否かや、セキュリティ検証用ポリシーにマッチしない設定モデルが存在するか否かを検証する。

[0123] このセキュリティ検証システム100dを用いる例においては、検査対象システムで満たされるべきでない条件を記述したポリシーだけでなく、検査対象システムで満たされるべき条件が記述されたポリシーについても「セキュリティ検証用ポリシー」と呼ぶこ

とにする。また、両者を区別するため、前者を「禁止ポリシー」と呼び、後者を「許可ポリシー」と呼ぶことにする。「セキュリティ検証用ポリシー」は、例えば、詳細は後述するが、`b()`、`acc()`、`cas()`、`auth()`、`flow()`などの記号を用いて記述される。

- [0124] 検証結果格納部35は、例えばデータベース装置によって構成され、検証部50aによる検証結果を格納する。具体的には、検証結果格納部35は、検証結果として、セキュリティ検証用ポリシーにマッチする結果が出た場合には、該当するセキュリティ検証用ポリシーと、マッチした設定モデルを格納する。また、セキュリティ検証用ポリシーにマッチしない結果が出た場合には、該当するセキュリティ検証用ポリシーを格納する。このとき、マッチしなかったことを示す記号をあわせて格納してもよい。
- [0125] 検証結果表示部60は、検証結果格納部35に格納されている検証部50aによる検証結果を検証者などに提示するために、セキュリティ検証用ポリシーと、そのセキュリティ検証用ポリシーにマッチした設定モデルまたはマッチしなかったことを示す記号とをあわせて表示する処理を実行する機能を有する。
- [0126] ここで、「設定モデル」について説明する。
- [0127] 「設定モデル」とは、検査対象システムのセキュリティ設定情報と、プログラム動作情報とに基づいて、検査対象システムの構成をモデル化したものである。設定モデルは、例えば、検証者や設計者により、検査対象システムの全体の構成と動作とが、モデル記述言語によって記述されたものである。「モデル記述言語」とは、例えばシステム構成やセキュリティ設定を表現することができる記述言語である。
- [0128] このような「設定モデル」は、プログラム動作情報(例えば図4参照)によって特定される複数の要素によって構成される。具体的には、設定モデルを構成する要素として、例えば、検査対象システムを構成するホストを表わすホストの集合、検査対象システムのネットワーク構成を表わすネットワーク接続表現、ユーザやグループを表わすユーザの集合、データの格納場所を表わすファイルの集合、ユーザからファイルに対する操作やネットワークサービスを表わすサービス名の集合、ファイルに対するユーザの権限を表わすアクセス制御行列表現、ネットワークのフィルタリングを現すネットワークアクセス表現、ネットワークを利用したユーザ間の権限獲得関係を表わしたネットワークサービスの権限獲得関係、ユーザがネットワークサービスや、ユーザとグルー

プの所属関係を利用して他のユーザの権限を獲得したときに、権限を獲得したユーザの権限で利用できるサービスを表わしたカスケード関係などが該当する。

[0129] 以下、設定モデルを構成する要素について詳しく詳説する。

[0130] 「ホスト」は、コンピュータやルータなどのネットワーク機器を表わし、1つまたは複数のIPアドレスを有する。

[0131] 「ネットワーク接続表現」とは、検証対象システムのインターネット層レベルでのネットワーク構成を表わし、IPアドレスをノードとする無向グラフとして表わされる。具体的には、例えば、「192. 168. 1. 1」、「192. 168. 1. 2」、「192. 168. 2. 3」、「192. 168. 2. 4」及び「192. 168. 2. 5」の5つのIPアドレスをノードとし、向きを持たない接続関係が示されたグラフによって各ノードの接続構成が表現されたものが、その5つのIPアドレスからなるネットワーク接続表現である。そのようなネットワーク接続表現は、後述する図68に例示されている。

[0132] 「ネットワークアクセス表現」とは、ネットワーク上をパケットが通るときに、そのパケットのIPアドレスまたはポート番号によってパケットの通過を拒否したり、許可したりするネットワークフィルタリング装置の動作をモデルで表現したものである。このような「ネットワークアクセス表現」は、ネットワークフィルタリングが行われているホストのIPアドレスと、制御対象のパケットの送信元IPアドレスと、送信先IPアドレスと、送信先ポート番号との4つの組の集合で表わされる。具体的には、ネットワークアクセス表現は、例えば「n(ip1, s-ip, d-ip, d-port)」のような、上記の4つの組の内容を意味する記号によって表わされる。なお、この「n(ip1, s-ip, d-ip, d-port)」は、IPアドレス「ip1」を有するホストで、送信元IPアドレスが「s-ip」、送信先IPアドレスが「d-ip」、送信先ポート番号が「d-port」であるTCP (Transmission Control Protocol) コネクションを許可していることを意味する。

[0133] なお、「ネットワークアクセス表現」には、送信元ポート番号を含めてもよい。このように構成すると、送信元ポート番号によるパケットフィルタリングも表現することができる。「ネットワークアクセス表現」にプロトコル種別を含めてもよい。このように構成すると、TCPパケットのフィルタリングだけでなく、UDP (User Datagram Protocol) パケットのフィルタリングも表現することができる。

- [0134] また、「ネットワークアクセス表現」は、許可されたものを表現せずに、禁止されているものをモデルとして表現してもよい。このように構成すると、原則許可と設定されたシステムにおいては、ネットワークアクセス表現を短く簡便に記述することができる。この場合には、後述するパケットの通過の可否の判断を反転する必要がある。具体的には、許可されたネットワークアクセス表現の場合には、設定モデルにネットワークアクセス表現が含まれていれば、通信が許可されていると判断でき、禁止されたネットワークアクセス表現の場合には、設定モデルにネットワークアクセス表現が含まれていなければ、通信が許可されていると判断できる。
- [0135] 「ユーザ」は、オペレーティングシステム(OS)や、アプリケーションソフトウェアの有するファイルアクセス制御機構におけるアクセス制御の主体を意味する。具体的には、Linux(リナックス)オペレーティングシステムでは、ファイル「/etc/passwd」によって「ユーザ」が定義され、ファイル「/etc/group」によってグループが定義されるが、これらで定義されるユーザ及びグループが、設定モデルにおける「ユーザ」となる。また、Apache(アパッチ)サーバでは、ファイル「htpasswd」によって、サーバの持つファイルアクセス制御機構の主体を定義することができるが、これらも「ユーザ」に対応する。
- [0136] 「ユーザ」は、いずれかのホストに所属している。このユーザの所属関係は、例えば、「b(u1)=h1」で表現される。「b(u1)=h1」は、ユーザ「u1」が、ホスト「h1」に所属することを意味する。
- [0137] 「ファイル」は、OSやアプリケーションソフトウェアの持つファイルアクセス制御機構におけるアクセス制御の対象を意味する。「ファイル」は、データの中身そのものではなく、パス名などによって識別されるデータの置き場を表わす。「ファイル」は、いずれかのホストに所属している。このファイルの所属関係は、例えば、「b(f1)=h1」で表現される。「b(f1)=h1」は、ファイル「f1」が、ホスト「h1」に所属することを意味する。
- [0138] 「サービス名」は、ユーザがファイルに対して実行できる操作の名前や、ネットワークを経由してユーザが受けられるサービスの名前を意味する。ユーザがファイルに対して実行できる操作としては、例えば、読み込み「read」、書き込み「write」があり、ネットワークを経由してユーザが受けられるサービスとしては、例えば、「http」、「ssh」が

ある。また、空のサービスを表わすサービス名「null」も定義される。サービス「null」によって、後述するとおり、一般のOSにおけるユーザとグループの関係を記述することができる。

- [0139] 「アクセス制御行列表現」は、ユーザが、ファイルに対して、読み込みまたは書き込みを許可されているか否かを表わし、ユーザ「u」と、ファイル「f」と、読み込み、書き込みを表わすサービス「s」とで表現される。アクセス制御行列表現「acc(u, s, f)」は、ユーザ「u」がファイル「f」にサービス「s」が可能であることを表わしている。具体的には、ユーザ「tutor」がファイル「answer. txt」を読み込み可能な場合には、アクセス制御行列表現は、acc (tutor, read, answer. txt)となる。
- [0140] 「権限獲得関係」とは、あるホストのユーザが、サービスを利用して、他のユーザの権限を獲得できることを表わしている。権限獲得関係「auth(u1, s, u2)」は、ユーザ「u1」がサービス「s」を利用してユーザ「u2」の権限を獲得できることを表わしている。具体的には、auth(student, telnet, guest)は、ユーザ「student」がサービス「telnet」を利用して、ユーザ「guest」としてログインすることができることを表わす。この場合、ユーザ「student」はユーザ「guest」の権限で、ユーザ「guest」の属するホスト上のファイルにアクセスすることができる。また、auth(taro, null, student)は、ユーザ「taro」とグループ「student」が同一のホストに属する場合、ユーザ「taro」がグループ「student」に属することを表わす。この場合、ユーザ「taro」が、無条件に、ユーザ「student」の権限で、グループ「student」の属するホスト上のファイルにアクセスすることができる。
- [0141] 「カスケード関係」とは、ユーザがサービスを利用して他のユーザの権限を獲得したときに、獲得したユーザの権限で利用できるサービスがある、という関係を意味する。この「カスケード関係」は、権限獲得後のユーザと、権限を獲得するために利用したサービスの種類とによって決まり、サービス「s1」を利用して、ユーザ「u」の権限を獲得したときに、サービス「s2」が利用できるときに、記号cas(s1, u, s2)で表現される。具体的には、サービス「telnet」を利用してユーザ「u」の権限を獲得したときに、サービス「ftp」が利用できるときには、cas(telnet, u, ftp)となる。
- [0142] 次に、セキュリティ検証用ポリシーを構成する各記号について説明する。

- [0143] セキュリティ検証用ポリシーを構成する各記号 $b()$ 、 $acc()$ 、 $auth()$ 、 $cas()$ は、それぞれ、所属関係、アクセス制御行列表現、権限獲得関係、カスケード関係を表現するために用いられる。また、セキュリティ検証用ポリシーを構成する $flow()$ は、2つのファイルの間のデータフロー関係を表現するために用いられる。例えば、セキュリティ検証用ポリシー「 $flow(file-a, file-b)$ 」とは、ファイル「 $file-a$ 」からファイル「 $file-b$ 」に対してデータが流れることを示している。つまり、ファイル「 $file-a$ 」の内容が、任意のユーザやサービスを経由して「 $file-b$ 」に書き込まれることを表わしている。
- [0144] これらの各述語(記号)を連結することによって、システム内のデータの流れを表現することができる。なお、この連結はAND結合(「 $\wedge$ 」で表わす)、つまり、全ての述語が成り立つ場合に限り、全体が成り立つことを意味する。また、各述語には論理変数を用いることができるものとする。
- [0145] 例えば、 $(b(U)=h) \wedge (b(F1)=h1) \wedge acc(U, read, f) \wedge auth(u1, ftp, U) \wedge acc(u1, write, F1)$ は、あるユーザ「 U 」がホスト「 h 」に所属し、あるファイル「 $F1$ 」がホスト「 $h1$ 」に所属し、ユーザ「 U 」がファイル「 f 」を読み出し(read)し、ユーザ「 $u1$ 」がサービス「 ftp 」を利用してユーザ「 U 」の権限を獲得し、ユーザ「 $u1$ 」がファイル「 $F1$ 」に書き込み(write)することができることを表わしている。すなわち、ユーザ「 $u1$ 」が、サービス「 ftp 」を用いてホスト「 h 」上のファイル「 f 」を読み込んだ後、ホスト「 $h1$ 」上のあるファイルに書き込めることを表わしている。なお、述語において大文字アルファベットを用いた場合には、論理変数すなわち、任意のユーザ、ファイル、ホストまたは、サービスを表わすものとする。
- [0146] ポリシー格納部33は、ポリシー入力部10において入力されたセキュリティ検証用ポリシーを記憶保持する。具体的には、ポリシー格納部33は、例えば図12に示すような形式でセキュリティ検証用ポリシーを格納する。セキュリティ検証用ポリシーを格納するファイルやデータベースには、複数のセキュリティ検証用ポリシーを格納することができ、セキュリティ検証用ポリシーだけでなく、セキュリティ検証用ポリシーに付随する情報を格納してもよい。
- [0147] セキュリティ検証用ポリシーに付随する情報とは、ポリシーの分類や、人間に分かりやすいようにポリシーの意味を記載した説明などである。さらに、ポリシー格納部33

は、セキュリティ検証用ポリシーが許可ポリシーを表わすものか禁止ポリシーを表わすものかを格納する。例えば、図12に示すように、Policy要素のtype属性がallowのときは、該当する設定モデルがポリシーになくてはならないことを示す許可ポリシーを表わし、type属性がdenyのときは、該当するモデルがポリシーにあってはならない禁止ポリシーを表わす。

[0148] 次に、セキュリティ検証システム100dの動作について詳細に説明する。

[0149] 図13は、セキュリティ検証システム100dが実行するセキュリティ検証処理を示している。

[0150] まず、セキュリティ検証者やシステム構築者などのユーザが、設定モデル入力部11を操作して、検証対象となるシステムやこれから構築しようとするシステムのシステム構成にしたがって設定モデルを入力すると、設定モデル入力部11は、ステップS301において、入力された設定モデルを設定モデル格納部34に格納する。検証者などがポリシー入力部10を操作して、システムが満たすべき条件または満たされるべきでない条件を示したセキュリティ設定用ポリシーを入力すると、ポリシー入力部10は、ステップS302において、入力されたセキュリティ設定用ポリシーをポリシー格納部33に格納する。次いで、検証者の指示にしたがって、検証部50aは、ポリシー格納部33から1つ以上のセキュリティ設定用ポリシーを取り出す。

[0151] 入力されたポリシーが許可ポリシーであれば、検証部50aは、ステップS303において、その許可ポリシーにマッチする設定モデルが存在するか否かを検索する。検索の結果、一致する設定モデルが存在したときは、検証部50aは、ステップS304において許可ポリシーを表示し、ステップS305において、その許可ポリシーにマッチした設定モデルを表示する。その後、ステップS306に移行する。ステップS306において、許可ポリシーにマッチしない設定モデルが存在しない場合もステップS306に移行する。

[0152] ステップS306において、検証部50aは、入力されたポリシーが禁止ポリシーであれば、検証部50aは、その禁止ポリシーにマッチする設定モデルが存在するか否かを検索する。禁止ポリシーが設定モデルにマッチした場合にはそのまま処理が終了し、禁止ポリシーが設定モデルにマッチなかった場合には、検証結果表示部60は、ステ

ップS307において、その禁止ポリシーを、マッチしなかったことを示す記号とともに表示する。

[0153] 図14は、図13に示したセキュリティ検証処理のステップS303での処理の具体例を示すフローチャートである。図15は、この処理において用いる書き換え規則を例示している。

[0154] 検証部50aは、検証対象のポリシーにデータフロー関係が含まれる場合には、ステップS311において、あらかじめ定められている図15に示す書き換え規則によって、データフロー関係を権限獲得関係などによる表現に変形する。ここで述べている例では、変形後の許可ポリシーを示す各関係が、それぞれ、設定モデルを満たしているか否かを検証する。ポリシーが権限獲得関係を含む場合には、検証部50aは、ステップS312において、権限獲得関係に含まれる2つのユーザが所属しているホストのIPアドレスを利用して、2つのユーザをつなぐネットワークの構造をネットワーク接続表現から求める。これにより、2つのユーザをつなぐネットワークを構成するIPアドレスの集合が求められる。

[0155] 次いで、検証部50aは、ステップS313において、求めたネットワーク構造のIPアドレスと2つのユーザの所属するIPアドレス、権限獲得関係に含まれるサービスが利用するポート番号を利用して、ネットワークアクセス権表現を検索する。ネットワークアクセス権表現を検索すると、検証部50aは、ステップS314において、検索したネットワークアクセス権表現から該当するネットワークアクセスが許可されているか否かを確認する。具体的には、権限獲得関係のユーザのIPアドレスが送信元IPアドレス「10. 56. 1. 2」及び送信先IPアドレス「10. 56. 1. 3」で、サービスが利用するポート番号が「80」で、2つのユーザを接続するIPアドレスの集合がIPアドレス「10. 56. 3. 1」とIPアドレス「10. 56. 3. 2」とである場合には、検証部50aは、検索されたネットワークアクセス権表現に、 $n(10. 56. 3. 1, 10. 56. 1. 2, 10. 56. 1. 3, 80)$ と、 $n(10. 56. 3. 2, 10. 56. 1. 2, 10. 56. 1. 3, 80)$ とが含まれているか否かを探索する。上記の各記号のいずれか一方がネットワークアクセス権表現に含まれていなければ、セキュリティ検証用ポリシーに含まれる権限獲得関係は、設定モデルにマッチしないと判定され、処理はステップS306に移行する。

- [0156] ステップS314においてネットワークアクセス権表現で通信が許可されていれば、検証部50aは、ステップS315において、セキュリティ検証用ポリシーに含まれる関係のうちのネットワーク接続関係以外の各関係が、設定モデルで定義されているか否かを検索する。ネットワーク接続関係以外の各関係に、設定モデルで定義されていない関係があれば、検証部50aは、ポリシーが設定モデルにマッチしないと判定し、ステップS306に移行する。
- [0157] ステップ315においてセキュリティ検証用ポリシーに含まれる各関係のすべてが設定モデルで定義されていれば、検証部50aは、ポリシーが設定モデルにマッチしていると判定し、ステップS316において、ポリシーを検索結果とともに検索結果格納部に格納する。
- [0158] 以上に説明したように、セキュリティ検証システム100dは、システム全体の設定を表わす設定モデルに対して、検証対象システム内のデータの移動を表現したポリシーを用いて検索する構成である。したがって、セキュリティ検証システム100dを用いることにより、複数のコンピュータに関わる、設計者または検証者が意図した動作とは異なる設定あるいは設定ミスを発見することができる。
- [0159] なお、セキュリティ検証システム100, 100a, 100b, 100c, 100dの各部は、自己が内部または外部に備えるコンピュータプログラムすなわちセキュリティ検証プログラムにしたがって上述した各種の処理を実行する。すなわち、セキュリティ検証システム100は、セキュリティ検証プログラムにしたがって、上述した図6に示す処理を実行する。具体的には、例えば、セキュリティ検証プログラムは、検査対象システム111におけるセキュリティ設定の複合的な誤りを示す不適設定の有無を検証させるためのセキュリティ検証用プログラムであって、例えばセキュリティ検証システム100に、検査対象システムで用いられるプログラムの動作を記述したプログラム動作情報に基づいて生成された当該検査対象システムにおけるデータ移動を表わすデータ伝達経路を格納したデータ伝達経路格納部から当該データ伝達経路を読み出すステップと、読み出したデータ伝達経路のアクセス権を統合するステップと、セキュリティ上不適切なデータ移動の経路である不適経路があらかじめ設定されたセキュリティ検証用ポリシーに基づいて、アクセス権が統合されたデータ伝達経路から不適経路を探索するス

テップとを実行させるプログラムである。さらに、セキュリティ検証プログラムは、例えばセキュリティ検証システム100に、プログラム動作情報に基づいて、探索された不適経路のデータ移動を許容している複合的なセキュリティ設定を検索するステップとを実行させるプログラムであつてもよい。

[0160] 上述した各セキュリティ検証システムによれば、検査対象のコンピュータにおけるデータ移動を表わすデータ伝達経路と、セキュリティ上不適切なデータ移動の経路が設定されたセキュリティ検証用ポリシーとを比較する構成としたので、検証対象のコンピュータにセキュリティ設定の複合的なミスである不適設定があるか否かを容易に検証することができる。複合的なミスである不適設定を探索する構成を含むようにすれば、不適設定の原因となっているセキュリティ設定を指摘することができ、設定の修正を促すことができる。また、擬似攻撃のような負荷の高い手法を用いることなく、検証対象のコンピュータからセキュリティ設定情報を収集するだけの構成としたので、検証対象のコンピュータに対して低負荷で検証することができる。

[0161] 第1の実施形態：

次に、以上説明した各セキュリティ検証システム100, 100a, 100b, 100c, 100dを踏まえ、これらのセキュリティ検証システムに対して与えられる検証用のデータを作成する、本発明に基づくセキュリティ検証用データ生成システムを説明する。図16は、本発明の第1の実施形態のセキュリティ検証用データ生成システムの構成を示している。このセキュリティ検証用データ生成システムは、図2あるいは図10に示したセキュリティ検証システムに対して入力されるデータ、具体的にはポリシーを生成するものである。なお、以下の説明において、セキュリティ検証用データ生成システム自体のユーザのことをオペレータと呼ぶことにする。

[0162] 図16に示すセキュリティ検証用データ生成システムは、セキュリティの検証対象となるコンピュータシステム1401に対応して、ポリシーを作成するものであり、システム構成情報収集部1402と、属性情報入力部1403と、属性情報格納部1404と、アクセスポリシー生成部1405と、アクセスポリシー格納部1406と、検証ポリシー生成部1407と、検証ポリシー格納部1408と、を備えている。

[0163] セキュリティの検証対象となるコンピュータシステム1401は、図16に示す例では、2

台のコンピュータ1401a, 1401cと、2台のコンテンツDB(データベース)1401b, 1401dとを備えている。コンテンツDB 1401b, 1401dは、コンテンツとして、例えばファイル等を格納する。なお、コンピュータシステム1401の構成は、図16に例示する構成に限定されないことは言うまでもない。

[0164] このセキュリティ検証用データ生成システムにおいて、システム構成情報収集部1402は、検証対象となるコンピュータシステム1401からシステム構成情報を収集する。システム構成情報については後述する。属性情報入力部1403には属性情報が入力される。属性情報については後述する。また、属性情報入力部1403は、システム構成情報収集部1402が収集したシステム構成情報に対し、入力された属性情報を付加して、属性情報格納部1404に格納する。なお、属性情報入力部1403は、属性情報が付加されたシステム構成情報を入力として、そのシステム構成情報を属性情報格納部1404に格納してもよい。属性情報格納部1404は、システム構成情報と属性情報とを対応付けた情報を記憶する。具体的には、属性情報が付加されたシステム構成情報を記憶する。

[0165] アクセスポリシー生成部1405は、属性情報格納部1404に格納あるいは記憶されたシステム構成情報や属性情報を利用して、アクセスポリシーを作成する。アクセスポリシーについては後述する。例えば、アクセスポリシー生成部1405は、ディスプレイ装置(不図示)に属性情報を表示して、オペレータに属性情報の選択を促す。そして、選択された属性情報に基づいて、アクセスポリシーを作成する。また、後述するようにアクセスポリシーには、「移動元」、「移動先」、「移動経路」の情報の少なくとも一つが含まれる。アクセスポリシー生成部1405は、ディスプレイ装置に「移動元」、「移動先」、「移動経路」の入力欄を表示して、その入力欄を介して「移動元」、「移動先」、「移動経路」の情報を受け取るようにしてもよい。このとき、「移動元」、「移動先」、「移動経路」の入力欄から、属性情報ではなく、「移動元」、「移動先」、「移動経路」を示す情報が直接入力されるようにしてもよい。アクセスポリシー生成部1405は、属性情報ではなく、「移動元」、「移動先」、「移動経路」そのものを直接示す情報からアクセスポリシーを作成してもよい。

[0166] アクセスポリシー格納部1406は、アクセスポリシー生成部1405が作成したアクセス

ポリシーを記憶する。検証ポリシー生成部1407は、アクセスポリシーを検証ポリシーに変換する処理を行う。なお、検証ポリシーについては後述する。検証ポリシー格納部1408は、検証ポリシー生成部1407によって生成された検証ポリシーを記憶する。

[0167] システム構成情報収集部1402は、例えば、プログラムにしたがって動作するCPUと、コンピュータシステム1401に対するインタフェースによって実現される。属性情報入力部1403は、例えば、プログラムに従って動作するCPUと、キーボード等の入力装置によって実現される。アクセスポリシー生成部1405は、例えば、プログラムにしたがって動作するCPUと、ディスプレイ装置と、キーボード等の入力装置とによって実現される。検証ポリシー生成部1407は、例えば、プログラムにしたがって動作するCPUによって実現される。これらのプログラムは、予め記憶装置(不図示)に記憶される。また、属性情報格納部1404、アクセスポリシー格納部1406、及び検証ポリシー格納部1408は、例えば、記憶装置によって実現される。当然のことながら、システム構成情報収集部1402、属性情報入力部1403、アクセスポリシー生成部1405及び検証ポリシー生成部1407を単一のCPUを用いて実現し、属性情報格納部1404、アクセスポリシー格納部1406及び検証ポリシー格納部1408を単一の記憶装置によって実現することができる。

[0168] 次に、システム構成情報について説明する。システム構成情報は、検証対象となるコンピュータシステムにおけるネットワーク、アプリケーション、ファイル、サービス及びユーザのうちの少なくともいずれか一つに関する情報を含むものである。したがってシステム構成情報は、検証対象となるコンピュータシステム1401におけるネットワーク構成情報、アプリケーション情報、ファイル情報、サービス情報、ユーザ情報のうちの少なくとも一つを含む情報である。

[0169] ネットワーク構成情報は、コンピュータシステム1401におけるネットワークシステムの情報を表わす。ネットワーク構成情報には、例えば、ホストや、ネットワーク機器の接続構成や、セグメント構成や、セグメント名等に関する情報が含まれる。ただし、これらの情報を全て含んでいなくてもよい。図17は、ネットワーク構成情報の一例を示しており、この例では、ネットワーク構成情報が、XML (eXtensible Markup Language) 形式のフォーマットで記述されている。

[0170] 図17に例示するネットワーク構成情報では、networksystemタグに囲まれた範囲に、複数のセグメントの情報が記述されている。個々のセグメントの情報は、segmentタグに囲まれた範囲に記述される。例えば、segmentタグに囲まれた記述851は、1つのセグメントの情報を表わしている。また、セグメントの情報の中には、セグメントの名称や、そのセグメントに属するホストの情報が含まれる。例えば、記述851には、“kansaiken-dmz”というセグメントの名称が含まれる。また、記述851には、3つのホストの情報が含まれている。個々のホストの情報は、hostタグによって表わされる。例えば、hostタグに囲まれた記述852は、1つのホストの情報を表わしている。ホストの情報の中には、ホストの名称や、そのホストのIPアドレスの情報が含まれる。このような記述により、ネットワーク構成情報は、どのセグメントにどのホストが属するのかわかっている。なお、記述853に示すように、ホストの名称としてIPアドレスが記述されていてもよい。また、図17に示す例では、segmentタグに囲まれた範囲の記述の中に、name属性等の属性情報も含まれている。

[0171] ネットワーク構成情報の中に含まれている個々のホストの情報をホスト構成情報と呼ぶことにする。ホスト構成情報は、ホストの名称やIPアドレス等を表わす。例えば、記述852はホスト構成情報であり、このホスト構成情報では、ホスト名が“fw-1”であり、IPアドレスが“10. 56. 191. 1”であることを示している。

[0172] アプリケーション情報は、コンピュータシステム1401の各ホストに導入されているOS (Operating System)やアプリケーションソフトウェアに関する情報を表わす。アプリケーション情報には、例えば、導入されたアプリケーションの種類や名前、アプリケーションの起動順等に関する情報が含まれる。ただし、これらの情報を全て含んでいなくてもよい。図18は、アプリケーション情報の一例を示しており、この例では、アプリケーション情報がXML形式のフォーマットで記述されている。

[0173] 図18に示す例では、applicationListタグに囲まれた範囲がアプリケーション情報である。また、hostタグで囲まれた範囲すなわち記述861に、各アプリケーションの情報が記述862として記載されている。この例では、hostタグとともにそのホストのIPアドレスが示されており、hostタグで囲まれた範囲(記述861)には、そのホストに導入された各アプリケーションの名称(“Fedora”, “xinetd”, “vsftpd”等)が記述されてい

る。

- [0174] また、図18に示す例では、applicationタグとともに各アプリケーションの種類を示すtype属性863が記述されている。このtype属性863は、システム構成情報収集部1402がコンピュータシステム1401から収集したアプリケーション情報には含まれていない。図18に例示したtype属性863は、属性情報入力部1403に入力し、システム構成情報収集部1402が収集したアプリケーション情報に付加されたものである。
- [0175] ファイル情報は、ファイルの名称や構成、ファイルシステムの構成等を示す情報である。図19にファイル情報の一例を示しており、この例のファイル情報は、ファイルの名称として、“paper. txt”を示している。
- [0176] サービス情報は、アプリケーションが用いるプロトコルやサービスに関する情報であり、例えば、サービス名やサービスが利用するプロトコル名等を示している。図20は、サービス情報の一例を示しており、この例では、Serviceタグとともに、“http”，“https”，“samba”，“ftp”等のサービス名が示されている。なお、図20に示す例では、暗号化を行うか否かを示すencryption属性871及びポート番号(port number)に関する属性872の記述を含んでいる。
- [0177] ユーザ情報は、ユーザアカウントの構成や認証機構の構成等を示す情報である。図21はユーザ情報の一例を示している。この例示されるユーザ情報では、“tanaka”，“w-tanaka”，“s-tanaka”等のユーザアカウントが示されている。
- [0178] 属性情報とは、システム構成情報に付加される情報であり、システム構成情報が示す内容の属性、例えば役割などの属性を表わす情報である。属性情報には、ネットワーク構成情報属性、ホスト構成情報属性、アプリケーション構成情報属性、ユーザ情報属性、ファイル情報属性等がある。
- [0179] ネットワーク構成情報属性は、ネットワーク構成情報に与えられる属性である。ネットワーク構成情報属性には、セグメント名や、ネットワークセグメント役割情報等がある。ネットワークセグメント役割情報は、例えば、セグメントが公開用セグメント、社内LAN（ローカルエリアネットワーク）セグメント、あるいは部内LANセグメント等としての役割を担っていることを示す。
- [0180] ホスト構成情報属性は、ホストや、ホストの構成に対する属性である。ホスト構成情

報属性には、例えば、ホスト名や使用者、所有者などの属性や、ウェブ公開用サーバ等の役割を表わす役割情報等がある。

- [0181] アプリケーション構成情報属性は、OSやアプリケーションソフトウェアの属性である。アプリケーション属性には、例えば、サーバアプリケーションや、クライアントアプリケーションといったアプリケーションの役割や、ウェブクライアント、FTP (file transfer protocol) サーバなどのアプリケーションの種類等がある。
- [0182] ユーザ情報属性は、個々のユーザや、ユーザアカウントの属性である。ユーザ情報属性には、例えば、ユーザアカウントを利用する人の名前、システム管理者やコンテンツ管理者、ウェブ管理者等の役割や、役職名がある。
- [0183] ファイル情報属性は、ファイルやディレクトリ、及び、そのようなファイルやディレクトリに格納されているコンテンツの属性である。また、ファイル情報属性には、公開情報、機密情報、関係者外秘などの公開属性、管理レベル、個人情報、技術情報などのカテゴリー属性、作成日時や、作成者などの編集属性、暗号化の有無、圧縮の有無、デジタル権限管理機構の有無などの機密属性がある。
- [0184] サービス情報属性は、サービスを利用しているホスト名や、アプリケーション名、ポート番号、暗号化の有無等の属性である。
- [0185] 属性情報入力部1403は、例えば、ディスプレイ装置(不図示)にシステム構成情報を表示させることにより、システム構成情報をオペレータに提示する。そして、オペレータに対し、そのシステム構成情報に付加する属性情報の入力を促す。そして、属性情報入力部1403には、そのオペレータから属性情報が入力する。また、カテゴリー属性のうち、コンテンツの公開属性や機密度等を、コンテンツを解析する手段を用いて抽出し、それをファイル情報属性としてもよい。ユーザ属性については、アカウント管理システムと連携し、アカウント管理システムに登録されたユーザに関する属性をユーザ属性としてもよい。
- [0186] アクセスポリシーは、属性情報を用いてアクセス権限をポリシーとして記述した情報であり、不適切なデータ移動経路における移動元、移動先、移動経路の情報を少なくとも一つ含む。したがって、アクセスポリシーは、移動元の情報のみを含んでいてもよい。移動元の情報のみを含む場合は、全ての移動先及び移動経路を指定している

ことを意味する。アクセスポリシーは、移動先の情報のみを含んでいたり、移動経路の情報のみを含んでいたりしてもよい。

[0187] アクセスポリシーにおいて、移動元とは、アクセス権の妥当性の検証対象となるファイルまたはユーザである。移動元がファイルの場合、その移動元は、ファイル名、ディレクトリ名、ホスト名、セグメント名等の移動元となる情報の格納場所の名前、または、それらを特定できる属性情報を用いて指定される。移動元がユーザの場合、その移動元は、ユーザアカウント名、ホスト名、セグメント名などのユーザの登録場所の名前、または、それらを特定できる属性情報を用いて指定される。移動先とは、移動元のファイルまたはユーザの情報の伝達先である。移動先は、移動元と同様に指定される。移動元及び移動先がともにファイルである場合は、そのアクセスポリシーは、移動元のファイルの全部または一部が移動先のファイルにコピー可能であることを表わす。移動元がファイルであり、移動先がユーザである場合は、そのアクセスポリシーは、ユーザがファイルを読めることを表わす。移動元及び移動先がともにユーザである場合は、移動元のユーザが自身の持つ情報をファイルに書き込み、そのファイルを移動先のユーザが読み込む等して、移動元のユーザから移動先のユーザまで情報が伝達することが可能であることを表わす。移動元がユーザであり、移動先がファイルである場合は、移動元のユーザが移動先のファイルに情報を書き込むことが可能であることを表わす。

[0188] 移動経路とは、移動元の情報が通過するネットワークインタフェースのIPアドレスやホスト名などの途中経路、移動元の情報を公開しているアプリケーションの利用ポートやサービス名などのサービス情報等である。移動経路の指定は、これらの移動経路を表わす情報を直接指定することによって行われたり、あるいは、これらの情報を特定可能な属性情報を指定することによって行われたりする。

[0189] 検証ポリシーとは、コンピュータシステムが意図したように設定されているか、または、意図したように動作するかを検証するための判定基準である。図2に示すセキュリティ検証システム100や図10に示すセキュリティ検証システム100cにおいてポリシー入力部10に入力するポリシーが検証ポリシーに該当する。検証ポリシーは、不適切なデータ移動経路を表わしている。

[0190] 次に、図16に示したセキュリティ検証用データ生成システムの動作について説明する。図22は、セキュリティ検証用データ生成システムの動作を示すフローチャートである。

[0191] まず、ステップS601において、システム構成情報収集部1401は、検証対象であるコンピュータシステム1401のシステム構成情報を収集する。ここでは、コンピュータシステム1401に予めインストールされたエージェントと通信を行うことによって、システム構成情報を収集すればよい。すなわち、システム構成情報収集部1401は、エージェントにしたがって動作するコンピュータからシステム構成情報を受信することによって、システム構成情報を収集すればよい。なお、コンピュータシステム1401に予めインストールされたエージェントは、そのコンピュータシステム1401に導入されたアプリケーションごとに用意され、OSを担当するエージェントが、各アプリケーションのインストール構成と、ファイル構成、ユーザ／グループ構成を収集する。OSを担当するエージェントは、アプリケーション構成等を直接収集してもよいし、あるいは予め用意された設定ファイルを解析することによってアプリケーション構成等を収集してもよい。

[0192] 続いて、OSを担当するエージェントは、収集した構成にしたがって、それぞれのアプリケーションに対応するエージェントを起動する。各エージェントは、システム構成情報をコンピュータに収集する処理や、そのシステム構成情報をシステム構成情報収集部1402に送信する処理を行う。また、一つのアプリケーションが他のアプリケーションを起動あるいは実行する構成となっている場合には、当該一つのアプリケーションに応じたエージェントが他のアプリケーションのエージェントを起動する。

[0193] 次に、属性情報入力部1403に、属性情報が入力される。例えば、ステップS601で収集されたシステム構成情報をディスプレイ装置(不図示)に表示するものとして、オペレータは、そのシステム構成情報に対応する属性情報を属性情報入力部1403に入力する。属性情報入力部1403は、ステップS602において、入力された属性情報をシステム構成情報に付加して属性情報格納部1404に格納する。次に、アクセスポリシー生成部1405は、ステップS603において、システム構成情報または属性情報に基づいてアクセスポリシーを作成し、アクセスポリシー格納部1406に格納する。

[0194] 続いて、検証ポリシー生成部1407は、アクセスポリシー格納部1406からアクセス

ポリシーを読み込み、アクセスポリシーから検証ポリシーを作成する。そして、検証ポリシー生成部1407は、検証ポリシーを検証ポリシー格納部1408に格納する。検証ポリシー生成部1407は、以下のようにして検証ポリシーを作成する。

- [0195] まずステップS604において、検証ポリシー生成部1407は、属性情報を用いてアクセスポリシーにおける移動元を作成したか否かを判定する。すなわち、アクセスポリシーにおける移動元が、ユーザ属性やファイル情報属性を用いて作成されたか否かを判定する。属性情報を利用してアクセスポリシーにおける移動元を作成している場合には、ステップS605において、検証ポリシー生成部1407は、その属性情報を用いてシステム構成情報の中から移動元となる情報を検索し、ステップS606に移行する。一方、属性情報を用いずにアクセスポリシーにおける移動元が作成されているとステップS604において判断した場合には、例えば、アクセスポリシーにおける移動元がオペレータから直接入力されている場合には、ステップS605を実行せずに、ステップS606に移行する。
- [0196] ステップS606では、検証ポリシー生成部1407は、属性情報を用いてアクセスポリシーにおける移動先を作成したか否かを判定する。属性情報を利用してアクセスポリシーにおける移動先を作成している場合には、検証ポリシー生成部1407は、ステップS607において、その属性情報を用いて、システム構成情報の中から移動先となる情報を検索し、ステップS608に移行する。一方、属性情報を用いずにアクセスポリシーにおける移動先が作成されているとステップS606において判断した場合には、例えば、アクセスポリシーにおける移動先がオペレータから直接入力されている場合には、ステップS607を実行せずに、ステップS608に移行する。
- [0197] ステップS608では、検証ポリシー生成部1407は、アクセスポリシーが移動経路を含み、かつ、その移動経路は属性情報を用いて作成されたか否かを判定する。アクセスポリシーが移動経路を含み、かつ、その移動経路は属性情報を用いて作成された場合には、検証ポリシー生成部1407は、ステップS609において、その属性情報を用いてシステム構成情報の中から移動経路となる情報を検索し、ステップS610に移行する。一方、アクセスポリシーが移動経路を含んでいない場合や、属性情報を用いずに移動経路が作成されている場合には、例えば、アクセスポリシーにおける移動

経路がオペレータから直接入力されている場合には、ステップS609を実行せずに、ステップS610に移行する。

[0198] ステップS610では、検証ポリシー生成部1407は、ステップS605で検索された移動元の情報がある場合、アクセスポリシーに含まれる移動元、すなわち属性情報を用いて作成した移動元を、検索した移動元の情報に置換する。同様に、検証ポリシー生成部1407は、ステップS607で検索された移動先の情報がある場合、アクセスポリシーに含まれる移動先、すなわち属性情報を用いて作成した移動先を、検索した移動先の情報に置換する。また、同様に、検証ポリシー生成部1407は、ステップS609で検索された移動経路の情報がある場合、アクセスポリシーに含まれる移動経路、すなわち属性情報を用いて作成した移動経路を、検索した移動経路の情報に置換する。この結果、検証ポリシーが得られる。

[0199] 検証ポリシー生成部1407は、ステップS604～S610までの処理によって作成した検証ポリシーを検証ポリシー格納部1408に格納する。この検証ポリシー格納部1408に記憶された検証ポリシーは、図2に示すセキュリティ検証システム100のポリシー入力部10や、図10に示すセキュリティ検証システム100cのポリシー入力部10への入力データ、すなわちポリシーとして使用される。

[0200] 本実施の形態によれば、セキュリティ検証用データ生成システムは、システム構成情報を用いてアクセスポリシーを作成し、検証ポリシーに変換する構成である。したがってこのセキュリティ検証用データ生成システムは、検証対象のシステム構成に沿った検証ポリシーを容易に作成することができる。また、システム構成情報に属性情報を付加し、その属性情報を用いてアクセスポリシーを作成し、検証ポリシーに変換する構成であるので、オペレータは、検証対象のシステムの構成の詳細を知らなくても、アクセスポリシーを作成できる。その結果、オペレータは、検証対象のシステム構成の詳細を知らなくても容易に検証ポリシーを作成することができる。また、システム構成情報に属性情報を付加して、その属性情報を用いてアクセスポリシーを作成し、検証ポリシーに変換する構成としたため、オペレータは、検証ポリシー固有の複雑な文法を知らなくても簡単に検証ポリシーを作成することができる。また、ひとつの属性情報で複数のシステム構成要素を同時に指定することができるので、少ないアクセスポ

リシー数で、必要十分な検証ポリシーを作成することができる。

[0201] 第2の実施形態：

図23は、本発明の第2の実施の形態のセキュリティ検証用データ生成システムの構成を示している。以下の説明において、図16に示した第1の実施の形態のセキュリティ検証用データ生成システムと同一の構成及び処理を行う部分については、同一の符号を付与してその詳細な説明を省略する。図23に示すように、本実施の形態におけるセキュリティ検証用データ生成システムは、セキュリティの検証の対象となるコンピュータシステム1401に対応したポリシーを作成するものであって、システム構成情報収集部1402と、属性情報入力部1403と、属性情報格納部1404と、アクセスポリシー生成部1405と、アクセスポリシー格納部1406と、検証ポリシー生成部1407と、検証ポリシー格納部1408と、データ伝達経路入力部1509と、検証部1510と、検証結果表示部1511と、を備えている。

[0202] データ伝達経路入力部1509は、検証部1510にデータ伝達経路情報を渡す。このデータ伝達経路情報は、例えば、図2に示すセキュリティ検証システム100あるいは図10に示すセキュリティ検証システム100cにおけるアクセス権統合部40が出力する、アクセス権が統合された後のデータ伝達経路情報と同様のデータ伝達経路情報である。なお、アクセス権が統合された後のデータ伝達経路情報は、図2に示すセキュリティ検証システム100あるいは図10に示すセキュリティ検証システム100cに関連して上述したものと同様の処理によって作成すればよい。

[0203] 検証部1510は、図2に示すセキュリティ検証システム100あるいは図10に示すセキュリティ検証システム100cにおける検証部50と同様の構成であって、この検証部50と同様の動作を行う。検証部1510は、検証ポリシー生成部1407が生成した検証ポリシーを用いて、検証対象システムであるコンピュータシステム1401におけるデータ伝達経路が不適切か否かを検証する。

[0204] 検証結果表示部1511は、例えば、ディスプレイ装置であり、検証部1510による検証結果、例えば、不適切と判定したデータ伝達経路を表示する。

[0205] 次に、第2の実施形態のセキュリティ検証用データ生成システムの動作について説明する。図24及び図25は、本実施の形態のセキュリティ検証用データ生成システム

の動作を示すフローチャートである。図24に示すステップS601～S610の処理は、上述の第1の実施の形態において図22を用いて説明したステップS601～S610の処理と同様の処理である。

[0206] ステップS610の後、データ伝達経路入力部1509は、ステップS611において、データ伝達経路情報を検証部1510に入力する。続いて、検証部1510は、ステップS610において検証ポリシー生成部1407が生成した検証ポリシーを用いて、ステップS612において、データ伝達経路情報が示すデータ伝達経路が不適切か否かを検証する。この検証処理は、検証ポリシーと一致するデータ伝達経路があるか否かを判定することによって行えばよい。そして、検証ポリシーと一致するデータ伝達経路を不適切なデータ伝達経路と判定すればよい。なお、検証部1510は、検証ポリシー格納部1408から検証ポリシーを読み込んでもよい。

[0207] ステップS612における検証処理の後、ステップS613において、検証部1510は、まだ検証に用いていない検証ポリシーがあるか否かを判定する。まだ検証に用いていない検証ポリシーがある場合には、ステップS612に移行し、その検証ポリシーを用いて検証処理を行う。検証に用いていない検証ポリシーがなくなった場合、すなわちステップS613において検証ポリシーがないと判定した場合には、ステップS614において、検証部1510は、検証ポリシーと一致するデータ伝達経路があったか否かを判定する。ここで検証ポリシーと一致するデータ伝達経路がなければ処理を終了する。ステップS614において検証ポリシーと一致するデータ伝達経路があれば、ステップS616において、検証部1510は、そのデータ伝達経路を不適切なデータ伝達経路として検証結果表示部1511に表示する。このとき、検証部1510は、不適切なデータ伝達経路とともに、そのデータ伝達経路を作成する原因となった設定やシステム構成情報を表示してもよい。

[0208] 図23に示したセキュリティ検証用データ生成システムは、属性情報を利用して作成したアクセスポリシーを用いて、検証部の入力データ(検証ポリシー)を生成し、検証ポリシーと一致したデータ伝達経路を表示する構成となっている。したがってオペレータは、このセキュリティ検証用データ生成システムを用いることにより、複雑な検証ポリシーの文法を知らなくてもポリシーに違反したファイルや、システム構成を見つけ

ることができる。また、オペレータは、検証対象システムのシステム構成情報や、保存されているファイルなどの情報の詳細を知らなくても、不適切なファイルやシステム構成を見つけることができる。

[0209] 以上説明した本発明の各実施形態のセキュリティ検証用データ生成システムは、上述した各セキュリティ検証システムと組み合わせて使用することができる。例えば、図16に示したセキュリティ検証用データ生成システムと、図2または図10に示したセキュリティ検証システムとを組み合わせた構成としてもよい。そのような構成とすることによって、図2または図10に示したセキュリティ検証システムと同様の効果を得ることができる。

[0210] 例えば、図16に示すセキュリティ検証用データ生成システムに対し、図2に示すセキュリティ検証システム100における設定情報収集部70とプログラム動作情報格納部30とデータ伝達経路生成部21と設定情報格納部31とデータ伝達経路情報格納部32とアクセス権統合部40と検証部50と設定情報検索部80と、検証結果表示部60(図2参照)とを付加し、検証ポリシー生成部1407が、検証部50に検証ポリシーを入力する構成としてもよい。

[0211] あるいは、図16に示すセキュリティ検証用データ生成システムに対し、図10に示すセキュリティ検証システム100cにおける設定情報入力部71と設定情報格納部31とデータ伝達経路入力部20とデータ伝達経路情報格納部32とアクセス権統合部40と検証部50と設定情報検索部80と検証結果表示部60とを付加し、検証ポリシー生成部1407が、検証部50に検証ポリシーを入力する構成としてもよい。

実施例

[0212] 次に、本発明について、具体的実施例を用いてさらに説明する。

[0213] 例1:

図26は、図2に示したセキュリティ検証システム100の具体的構成を示している。なお、図26は、図2に示した構成のうち、ポリシー格納部33を省略して描いている。

[0214] 図26に示すように、セキュリティ検証システム100は、検査対象コンピュータ110と、検査コンピュータ120とを備えている。検査対象コンピュータ110と、検査コンピュータ120とは、それぞれ、インターネットや専用回線などの通信ネットワーク130に接続

されている。なお、検査対象コンピュータ110は、複数台備えられていてもよい。

[0215] 検査対象コンピュータ110は、検査対象111と、設定情報収集部70と、データ伝達経路生成部21と、アクセス権統合部40と、設定情報格納部31と、プログラム動作情報格納部30と、データ伝達経路情報格納部32とを含む。検査コンピュータ120は、ポリシー入力部10と、データ伝達経路変換部51と、パターンマッチング部52と、設定情報検索部80と、検証結果表示部60とを含む。

[0216] ここで、設定情報収集部70と、データ伝達経路生成部21と、アクセス権統合部40と、設定情報格納部31と、プログラム動作情報格納部30と、データ伝達経路情報格納部32とのうち一部または全部が、検査コンピュータ120に含まれていてもよい。また、検査コンピュータ120は、検査対象コンピュータ110に含まれていてもよい。

[0217] 検査対象111は、OS 111aと、ウェブサーバ111bと、ウェブクライアント111cとで構成されている。本例では、OS 111aにLinux 2.4系を、ウェブサーバ111bにApache 1.3を、ウェブクライアント111cにMozilla 1.5を利用している。

[0218] 次に、このセキュリティ検証システムにおけるセキュリティ検証処理を、上述した図6を参照しつつ説明する。

[0219] 図27A及び図27Bは、それぞれ、OS 111aのユーザアカウントとグループの設定の一例を示し、図28は、ファイルのアクセス権の設定の一例を示し、図29A及び図29Bは、ウェブサーバ111bの設定の例を示している。これらの図では、上述した図5に示す設定と同様に、Linuxと呼ばれる広く利用されているOSソフトウェアによって各部の設定がなされた例が示されている。なお、他のソフトウェアによって設定するようにしてもよい。

[0220] 図27Aは、OS 111aにおけるユーザ設定ファイル「/etc/passwd」の内容の例を示す図であって、ここには、ユーザ設定ファイル「/etc/passwd」の内容の抜粋が示されている。ユーザ設定ファイル「/etc/passwd」には、図27Aに示すように、OS 111a上で管理されているユーザを示す情報と、その所属グループを示す情報とが記されている。

[0221] 図27Bは、OS 111aにおけるグループ設定ファイル「/etc/group」の内容の例を示す図であって、ここには、グループ設定ファイル「/etc/group」の内容の抜粋

が示されている。グループ設定ファイル「/etc/group」には、図27Bに示すように、OS 111a上で管理されているグループを示す情報と、そのグループに所属するユーザを示す情報とが記されている。

[0222] 図28は、OS 111aにおけるファイルまたはディレクトリの構造とそのアクセス権の設定の一例を示している。図28には、コマンド「ls -lar」を実行することによって得られるものの抜粋が示されている。

[0223] 図29Aは、ウェブサーバ111bの設定ファイル「httpd.conf」の内容の一例を示す図であって、ここには、apacheの設定ファイル「httpd.conf」の内容の抜粋が示されている。設定ファイル「httpd.conf」には、図29Aに示すように、ウェブサーバ111bが利用するファイルまたはディレクトリの指定を示す情報と、ファイルまたはディレクトリのアクセス権を示す情報と、ネットワークポートの設定を示す情報と、認証に利用するユーザ設定ファイルを示す情報などが記されている。

[0224] 図29Bは、ウェブサーバ111bの設定ファイルの内容の例を示す図であり、ここには、認証に利用するユーザ設定ファイルとして、図29Aに示す設定ファイルに記されているファイル「/var/www/.htpasswd」の内容が示されている。ファイル「/var/www/.htpasswd」には、図29Bに示すように、ウェブサーバ111bが利用する認証のユーザを示す情報が記されている。

[0225] セキュリティ検証処理において、まず、設定情報収集部70は、ステップS201において、図27A、図27B、図28、図29A及び図29Bに示すセキュリティ設定を、検査対象111から収集する。その後、設定情報収集部70は、収集したセキュリティ設定情報を設定情報格納部31に格納する。

[0226] データ伝達経路生成部21は、設定情報収集部70が収集して設定情報格納部31に格納したセキュリティ設定情報にしたがって、プログラムごとにプログラム動作情報格納部30にプログラムの仕様を問い合わせる。具体的には、プログラム動作情報(図4参照)を参照し、図27A、図27B、図28、図29A及び図29Bに示すセキュリティ設定情報内の各プログラムごとに、モデル上に作成するノードまたはアークの種類を問い合わせ、各プログラムに対応するプログラムの仕様を含むプログラム動作情報を読み出す。そして、データ伝達経路生成部21は、ステップS203において、設定情報

収集部70が収集して設定情報格納部31に格納したセキュリティ設定情報とプログラム動作情報格納部30から読み出されたプログラム動作情報とに基づいて、ノードやアークを作成して行き、データ伝達経路情報を生成する。

[0227] この例では、例えば、OS 111aのセキュリティ設定情報(図27A及び図27B参照)から、ユーザには、「a」と、「b」と、「apache」とがあることが分かる。また、グループには、「a」と「apache」とがあることが分かる。さらに、ユーザ「a」とユーザ「b」とがグループ「a」に属しており、「apache」がグループ「apache」に所属していることが分かる。図30は、OS 111aのセキュリティ設定情報に基づいて生成されたデータ伝達経路を示している。

[0228] ステップS203では、上記のセキュリティ設定情報に基づいて、データ伝達経路生成部21が、以下の手順でデータ伝達経路を作成する。

[0229] まず、データ伝達経路生成部21は、ユーザ「a」があることより、ノードU<a> 501を作成し、グループ「a」が存在することより、ノードG<a> 503を作成する。また、ユーザ「a」がグループ「a」に所属していることより、所属関係を表わすアーク502を作成する。上記の手順で全てのユーザと、全てのグループと、その所属関係とを反映させると、図30に示したデータ伝達経路が生成される。ここで、U<>はユーザノードを表わし、G<>はグループノードを表わし、F<>はファイルノードを表わし、N<>はネットワークノードを表わすものとする。図30及び以下の各グラフにおいて、特に言及する場合を除き、実線黒矢印はデータ移動関係を表わし、点線黒矢印は所属関係を表わし、実線矢印は別名定義を表わし、点線矢印は権限委譲を表わすものとする。

[0230] 図31は、OS 111aが管理するディレクトリ構造(図28参照)から作られるアークとオブジェクトとが加えられたデータ伝達経路を示している。データ伝達経路生成部21は、ディレクトリ構造にファイル「/home/a/」が存在することより、ノードF</home/a/> 603を作成する。また、データ伝達経路生成部21は、このファイル「/home/a/」のアクセス権の設定より、ユーザ「a」がファイルに書き込み権限があることから、データ移動関係のアーク601を作成し、読み込み権限があることから、データ移動関係のアーク602を作成する。上記のようにして、図31に示すデータ伝達経路

が生成される。図32は、ウェブサーバ111bのセキュリティ設定情報(図29参照)に基づいて生成されたデータ伝達経路を示している。ウェブサーバ111bのセキュリティ設定情報によると、「User apache」と記載されているため、ウェブサーバ111bの実行ユーザがU<apache>であることが分かる。したがって、データ伝達経路生成部21は、ユーザノードU<apache> 702を作成する。

[0231] また、データ伝達経路生成部21は、ディレクトリ「/home/b/public/s/」にBasic(ベーシック)認証が設定され、「.htpasswd」ファイルにユーザ「g」が設定されていることより、ユーザノードU<g> 701を作成する。さらに、ウェブサーバ111bの動作情報により、U<apache>は、Basic認証が必要なファイルノード以外のファイルノードに対して読み書きが可能である。このため、データ伝達経路生成部21は、Basic認証のディレクトリ以外に対しては、データ移動関係のアークを作成し、U<g>がBasic認証のユーザであるため、Basic認証のファイルノード及びその他のファイルノードとデータ移動関係のアークを作成する。

[0232] 次に、データ伝達経路生成部21は、ウェブクライアント111c及びこれらのプログラム間の動作情報をプログラム動作情報格納部30に問い合わせる。ウェブクライアント111cがhttp(hypertext transfer protocol)を利用してデータを移動させることから、データ伝達経路生成部21は、httpに関するネットワークノードを作成する。以上のようにして、各レイヤ内のノードとアークが生成される。

[0233] 次に、プログラム間レイヤの生成と、それに含まれるアークの生成について説明する。まず、ウェブサーバ111bとOS 111aがインストールされていることより、ウェブサーバ111bのレイヤとOS 111aのレイヤに関係づけられたプログラム間レイヤを作成する。次に、ウェブサーバ111bの動作情報より、ウェブサーバ111bのファイルノードに、OS 111aのファイルノードの別名定義があることが分かる。このため、データ伝達経路生成部21は、プログラム間レイヤを作成し、図33に示すように、ウェブサーバ111bの該当するファイルノードから、OS 111aの該当するファイルノードに対して、別名定義関係のアークを作成する。なお、図33には、プログラム間レイヤは明記されていない。

[0234] 同様に、ウェブサーバ111bの動作情報より、ウェブサーバ111bのユーザに、OS

111a上のユーザからの権限委譲であるものがあることが分かる。このため、データ伝達経路生成部21は、図33に示すように、ウェブサーバ111bの該当するユーザから、OS 111aの該当するユーザに対して権限委譲関係を表わすアークを作成する。

[0235] また、ウェブクライアント111cは、ウェブサーバ111bの80番ポートを利用してデータを移動させ、OS 111aのダイナミック(Dynamic)ポートに対してもデータを移動させることが分かる。このため、データ伝達経路生成部21は、OS 111aとウェブクライアント111cに関連付けられたプログラム間レイヤと、ウェブサーバ111bとウェブクライアント111cに関連付けられたプログラム間レイヤとを作成し、図33に示すように、上記の各ポートに対してデータ移動関係を表わすアークを作成する。

[0236] また、ウェブクライアント111cは、ウェブサーバ111bの80番ポートを利用してデータを移動させ、OS 111aのダイナミックポートに対してもデータを移動させることが分かる。このため、データ伝達経路生成部21は、図33に示すように、上記の各ポートに対してデータ移動関係を表わすアークを作成する。

[0237] 上記のようにして、データ伝達経路生成部21により、データ伝達経路情報が生成される。図33は、ステップS203において生成されるデータ伝達経路情報が示すデータ伝達経路を示している。

[0238] 次に、ステップS204で実行される、アクセス権統合部40によるアクセス権統合処理の具体例について説明する。図34は、アクセス権統合処理を示すフローチャートである。アクセス権統合処理は、複数のプログラムにかかわるアクセス権を統合する処理である。図35は、ステップS203において生成されたデータ伝達経路情報が示すデータ伝達経路に対し、以下の説明を行うための符号を付与した図である。

[0239] 図35に示すように、ウェブサーバ111b上のユーザU<apache> 806は、OS 111a上のどのファイルにどのようなアクセスが可能であるかは、一見しただけでは分からない。そこで、ウェブサーバ111bとOS 111aとの間のアクセス権を統合する必要がある。

[0240] アクセス権統合処理において、アクセス権統合部40は、ステップS181において、統合すべきアークがあるかどうかを調べ、統合すべきアークが存在する場合にステップS182において権限委譲関係あるいは別名定義関係のアークを選択することにより

、ウェブサーバ111bとOS 111aとの間のアークのうち、任意の権限委譲関係を表わすアーク、または、別名定義関係を表わすアークに着目する。ここでは、権限委譲を表わすアーク805に着目するものとする。次いで、アクセス権統合部40は、ステップS183において、権限委譲関係のアークの始点にあるノード806にデータ移動関係のアークがあるか確認する。データ移動関係のアークがなければステップS181に戻り、データ移動関係のアーク807があれば、ステップS184において、それを選択する。アクセス権統合部40は、ステップS185において、選択したデータ移動関係を表わすアーク807をたどり、移動元のノード809を選択する。

[0241] 次いで、アクセス権統合部40は、ステップS186において、選択したノード809に別名定義関係のアーク808があることを確認する。別名定義関係のアークがなければステップS186に戻り、別名定義関係のアーク808があれば、ステップS187において、そのアーク808をたどり別名定義されているノード801を選択する。そして、アクセス権統合部40は、ステップS188において、別名定義されたノード801から、権限委譲されたノード803に向けてデータ移動があることを特定する。このとき、アークは記述しないものとする。そして、アクセス権統合部40は、ステップS189において、ステップS188において特定したデータ移動の方向と、ステップS184のデータ移動の方向が同じかどうかを判断する。方向が同じでない場合には処理はステップS183に戻り、方向が同じである場合には、アクセス権統合部40は、ステップS190において、図36に示すように、別名定義されたノード801から、権限委譲関係のアークの始点にあるノード806に向けて新たなデータ移動関係のアーク901を作成する。ステップS190の後、処理は、ステップS181に戻る。

[0242] アクセス権統合部40は、統合すべきアーク、すなわち権限委譲関係を表わすアーク及び別名定義関係のアークがなくなるまで上記の処理を繰り返し実行し、新たなデータ移動関係のアークを作成するとともに、権限委譲関係を表わすアーク及び別名定義関係のアークを消去して、図37に示すような2種類のアーク、すなわち所属関係を表わすアーク及びデータ移動関係を表わすアークに統合されたグラフを作成する。

[0243] 次に、ステップS205における、データ伝達経路変換部51によるデータ伝達経路変

換処理の具体例について説明する。データ伝達経路変換処理は、セキュリティ検証用ポリシーに一致するデータ伝達経路を探索することができるように、所属関係を表わすアーク及びデータ移動関係を表わすアークの2種類のアークからなるグラフを、データ移動関係のアークだけからなるツリー構造に変換する処理である。言い換えれば、データ伝達経路変換部51は、2種類のアークからなるグラフを、1種類のアークからなるツリー構造(木構造)に変換する。以下、ツリー構造のことを単にツリー(木)と呼ぶことがある。

- [0244] ここでは、例えば、図38に示すデータ伝達経路が与えられたときのデータ伝達経路変換処理について説明する。図39は、図38に示すデータ伝達経路を、データ伝達経路変換処理によって変換した後のデータ伝達経路を示している。図40は、データ伝達経路変換処理を示すフローチャートである。
- [0245] データ伝達経路変換処理において、データ伝達経路変換部51は、まず、ステップS215において、任意の利用していないノードを選択する。「利用していないノード」とは、今回のデータ経路変換処理において未だ利用していないノードのことを意味する。ステップS215では、データ伝達経路の各ノードのうち、アークを示す矢印が入り込んでいない任意のノードが選択される。この例では、ステップS215において、図38に示すノード1001またはノード1005が選択される。
- [0246] ステップS215においてノード1001を選択すると、データ伝達経路変換部51は、ステップS216において、選択したノード1001をノード1101とし、ツリー構造のルートとして加える。ノード1001をツリーに加えると、データ伝達経路変換部51は、ステップS217において、ツリーに加えたノード1001に利用していないアークがあるかどうかを確認する。ここで、「利用していないアーク」とは、今回のデータ経路変換処理において未だ利用していないアークのことを意味する。
- [0247] 利用していないアークがあった場合には、データ伝達経路変換部51は、ステップS218において、そのアークがデータ移動関係であるかどうかを判断し、そのアークがデータ移動関係である場合には、ステップS219において、そのアークの行先にあるノード1002を、ノード1102としてツリーに加え、ステップS217に戻る。
- [0248] また、利用していないアークがデータ移動関係でない場合には、ステップS220に

において、そのアークが所属関係かどうかを判断し、所属関係でなければステップS217に戻り、所属関係であれば、データ伝達経路変換部51は、ステップS221において、そのアークの行先にあるノードをツリーに加える。具体的には、図38に示すように、ツリーに加えたノード1002に利用していない所属関係のアークがあるため、そのアークの行先にあるノード1004をノード1103として、図39に示すようにツリーに加える。

[0249] 所属関係のアークの行先にあるノードをツリーに加えると、データ伝達経路変換部51は、ステップS222において、利用していないデータ移動関係のアークがあるか確認し、そのようなアークがあれば、ステップS223において、そのアークの行先にあるノードをツリーに加え、ステップS217に戻る。すなわち、所属関係のアークを利用してノードを訪問したあとは、データ伝達経路変換部51は、データ移動関係のアークを利用して訪問できるノードがあるかだけを確認する。

[0250] ステップS217において利用していないアークがないと判定したとき、またはステップS222において利用していないデータ移動関係のアークがないと判定したときには、データ伝達経路変換部51は、ステップS224において、戻るノードがあるか否かを確認する。戻るノードがあれば、データ伝達経路変換部51は、ステップS226において、ノードを1つ戻し、ステップS217に移行する。一方、ステップS224において戻るノードがなければ、データ伝達経路変換部51は、ステップS225において、利用していないアークとノードとの組合せがあるか否か確認し、あればステップS215に移行し、なければ処理を終了する。

[0251] 上記の手順で、すべてのアークを利用して、図38に示すグラフ構造を変換すると、図39に示すような、ノード1001をノード1101としたルートと、ノード1005をノード1109としたルートとを有するツリー構造が作成される。すなわち、図39に示すツリー構造のデータ伝達経路に変換される。

[0252] 次に、ステップS206における、ポリシー入力部10によるセキュリティ検証用ポリシー入力処理の具体例について説明する。セキュリティ検証用ポリシー入力処理は、ユーザからのセキュリティ検証用ポリシーの指定を受け付け、検証部50に入力する処理である。

- [0253] セキュリティ検証用ポリシーは、あってはならないデータ移動経路を表わすものであり、ノードの正規表現で記述される。なお、ノードの他に、ノードの集合を表わす記号を定義して利用するようにしてもよい。ここでは、例えば、[NET]は任意のネットワークノードを表わし、[USER]は任意のユーザを表わすものとする。また、「.」は任意のノードを表わし、「*」は直前のノードもしくは記号の0回以上の繰り返しを表わし、「|」は「OR」を表わし、「^」は直後のノード以外のノードを表わすものとする。この他、周知の正規表現を用いて表現することができる他の記号を用いるようにしてもよい。
- [0254] 図41は、ポリシー入力部10がユーザから受け付けるセキュリティ検証用ポリシーの表現例を示している。図41には、「ポリシー1」から「ポリシー5」までのセキュリティ検証用ポリシーの5つの例が記載されている。
- [0255] 「ポリシー1」は、ユーザノードU<a>の情報が任意のノードを経由してファイルノードF</d/>に移動してはならないことを意味する。言い換えると、「ポリシー1」は、ユーザ「a」がファイル「/d/」に任意の経路で書き込んではならないことを表わす。
- [0256] 「ポリシー2」は、ファイルノードF</c/>の情報が、任意のノードを経由し、任意のネットワークを経由し、ユーザノードU<a>に移動してはならないことを意味する。言い換えると、「ポリシー2」は、ファイル「/c/」を、ネットワークを経由してユーザ「a」が読んではならないことを表わす。
- [0257] 「ポリシー3」は、ファイルノードF</c/>の情報が、任意のノードを経由してネットワークノードN<p443>以外を通り、さらに任意のノードを経由してユーザノードUに移動してはならないことを意味する。言い換えると、「ポリシー3」は、ファイル「/c/」を443ポート以外のネットワークを利用してユーザ「b」が読んではいけないことを表わす。
- [0258] 「ポリシー4」は、ユーザノードU以外の情報が、任意のノードを経由してファイルノードF</b/public/>に移動してはならないことを意味する。言い換えると、「ポリシー4」は、ユーザ「b」以外のユーザがファイル「/b/public/」に書き込んではならないことを表わす。
- [0259] 「ポリシー5」は、ユーザノードUまたはユーザノードU<g>以外の情報が、任意のノードを経由してファイルノードF</b/public/s/>に移動してはならないことを表わす。

いことを意味する。言い換えると、「ポリシー5」は、ユーザ「b」またはユーザ「g」以外が、ファイル「/b/public/s/」に書き込んで서는ならないことを表わす。

[0260] 次に、ステップS207における、パターンマッチング部52が実行するパターンマッチング処理の具体例について説明する。

[0261] パターンマッチング処理において、パターンマッチング部52は、データ伝達経路変換部51からデータ伝達経路を受け取るとともに、ポリシー入力部10からセキュリティ検証用ポリシーを受け取る。そして、パターンマッチング部52は、データ伝達経路変換部51から受け取ったデータ伝達経路の中から、ポリシー入力部10から受け取ったセキュリティ検証用ポリシーに一致する経路を探索する。具体的には、セキュリティ検証用ポリシーに一致する経路に含まれているアークとノードとを探索して抽出する。図41に示したセキュリティ検証用ポリシーは、正規表現に準じている。このため、パターンマッチング部52によるパターンマッチング処理は、周知の正規表現の探索アルゴリズムを用いて実現できる。

[0262] 次に、パターンマッチング部52が、ステップS210の前に実行される処理として実行する違反経路検索処理について説明する。

[0263] 図42は、パターンマッチング部52によるパターンマッチング処理によって探索された不適経路を表わすグラフを示しており、この図では、実線矢印部分が不適経路を示している。図42において実線で囲まれているノードは、不適経路の始点、終点または通過点となっているノードである。図43は、違反経路検索処理を示すフローチャートである。図44は、図42に表れている不適経路を取り出して示す図である。以下、図42に表れている不適経路を検索し、図44に示す不適経路を生成する処理について説明する。

[0264] 違反経路検索処理において、パターンマッチング部52は、まず、ステップS241において、不適経路の先頭ノード1201を取り出す。ステップS242において、先頭ノードに接続されたアークがあるかどうかを調べ、そのようなアークがあれば、パターンマッチング部52は、ステップS243において、アーク1202とノード1203を取り出す。次いで、パターンマッチング部52は、ステップS244において、ノード1203を先頭ノードとし、ステップS242に移行し、上述の処理を繰り返す。これにより、図44に示す不

適経路を生成することができる。そして、パターンマッチング部52は、生成した不適経路を示すデータを設定情報検索部80に向けて出力する。

[0265] 次に、ステップS210における、設定情報検索部80が実行する設定情報検索処理について説明する。図45は、設定情報検索処理を示すフローチャートである。ここでは、図44に示した不適経路が許容されている原因となっている不適設定を、設定情報検索部80が検索する処理について説明する。

[0266] 設定情報検索処理において、設定情報検索部80は、まず、ステップS291において、パターンマッチング部52から受け取った不適経路に含まれるノードを、データ伝達経路情報格納部32に格納されている、アクセス権統合部40によるアクセス権の統合後のデータ伝達経路から検索する。図46は、アクセス権の統合後のデータ伝達経路から不適経路に含まれるノードが検索された状態の例を示している。図46に示すように、アクセス権の統合後のデータ伝達経路から、不適経路に含まれるノード、すなわち太字で囲まれているノードが検索される。また、ステップS291では、パターンマッチング部52から受け取った不適経路に基づいて、図46に示すように、アクセス権の統合後のデータ伝達経路に対応するアークがあれば、不適経路に含まれる各ノードについてのデータ移動関係を示すアーク、すなわち太字黒矢印で示されたアークが検索される。

[0267] 次いで、設定情報検索部80は、ステップS292において、検索されたノードに対応するノードをアクセス権の統合前のデータ伝達経路から検索する。図47は、アクセス権の統合前のデータ伝達経路における不適経路が検索された状態の例を示している。図47に示すように、ステップS291において検索されたノードに対応するノードがアクセス権の統合前のデータ伝達経路から検索され、アクセス権の統合前のデータ伝達経路から不適経路に含まれるノード、すなわち太字で囲まれているノードが検索される。また、ステップS292では、パターンマッチング部52から受け取った不適経路に基づいて、図46に示すように、ステップS291において検索されたアークに対応するアークがアクセス権の統合前のデータ伝達経路にあれば、そのアーク(太字黒矢印のアーク)が検索される。

[0268] 設定情報検索部80は、ステップS293において、アクセス権の統合前のデータ伝

達経路から検索されたノードに含まれる権限委譲のアーキと別名定義のアーキとを検索し、それらのアーキに接続されているノードを検索する。ステップS293では、アクセス権の統合前のデータ伝達経路から検索されたノードに関する権限委譲及び別名定義のアーキが検索される、権限委譲及び別名定義のアーキは、権限委譲元、権限委譲先、別名定義元、別名定義先のいずれかを示すアーキである。さらに、ステップS293では、そのように検索されたアーキに関する全てのノード、すなわち権限委譲元、権限委譲先、別名定義元、別名定義先のいずれかとなっているノードが検索される。図48は、権限委譲のアーキと別名定義のアーキとそれらのアーキに接続されているノードが検索された状態の例を示している。この例では、図48に示すように、ステップS293において、図47に示すアクセス権の統合前のデータ伝達経路で検索された各ノードに基づいて、権限委譲のアーキと別名定義のアーキがそれぞれ1つ検索され、それらのアーキに関する4つのノードが検索される。

[0269] 次に、設定情報検索部80は、ステップS294において、ステップS293において新たに検索されたアーキとノードに対してデータ統合で行った処理を逆の手順で適用し、不適経路を作成する原因となった全てのノードとアーキを検索する。図49は、不適経路を作成する原因となった全てのノードとアーキが検索された状態の例を示している。この例では、図49に示すように、ステップS294において、ステップS293において新たに検索されたアーキとノードとに基づいて、別名定義関係にある2つのノードについて移動方向が同じとなる2つのデータ移動関係のアーキと、データ移動先が権限委譲関係にあることを示す2つの権限委譲のアーキのうちの1つとが検索されるとともに、新たに検索されたアーキに関するノードが検索され、さらに、図47に示されている検索済みの不適経路が付加される。

[0270] そして、設定情報検索部80は、ステップS295において、検索された全てのノードとアーキに対してそれらが作成される原因となったセキュリティ設定情報を、データ伝達経路情報に含まれるセキュリティ設定情報のIDを利用して設定情報格納部31から取り出す。図50は、データ伝達経路情報における不適設定箇所を表わした状態の例を示し、図51は、設定情報格納部31から取り出されたセキュリティ設定情報の例を示している。図50に示すように、設定情報検索部80は、データ伝達経路情報格納部32

からデータ伝達経路情報(図5参照)を読み出し、図49に示した不適経路に基づいて、データ伝達経路情報内の不適設定がなされている部分、例えば4角形で囲まれている部分を検索する。そして、図51に示すように、設定情報検索部80は、不適設定となっているセキュリティ設定の設定情報IDに基づいて、設定情報格納部31から、不適設定となっているセキュリティ単位情報を含むセキュリティ設定情報を読み出す。

[0271] 上記の処理により、不適経路を生成する原因となった設定ミスを含むセキュリティ設定情報を取り出すことができる。

[0272] 次に、ステップS211における、検証結果表示部60による不適設定表示処理について説明する。

[0273] 検証結果表示部60は、設定情報検索部80によって検索された不適設定を示す情報、例えば、図50に示す不適設定箇所を示す情報や図51に示す不適設定の内容を示す情報を表示画面に表示して、システム検証者などのユーザに報知する処理を実行する。このような具体的処理を実行することで、検証対象システム111における不適経路を探索して不適設定を報知することができる。

[0274] なお、上記の例では言及していないが、不適設定に基づく経路を表示するようにしてもよい。この場合、例えば、図52に示すようなグラフを表示画面に表示することで、不適当である移動経路を強調して報知するようにすればよい。図52には、不適経路のみが実線黒矢印によって表わされている。なお、不適経路が強調されていれば、どのような表示形式であってもよい。なお、図49に示したような、不適経路を作成する原因となった全てのノードとアークが検索された状態のグラフを表示するようにしてもよい。

[0275] この例では、アクセス権統合部40は、アクセス権を統合する際に、例えば、図35に示す権限委譲を表わすアーク805などから、図36に示すデータ移動関係を表わすアーク901を生成する処理を行う。上記の例では言及していないが、データ移動関係を表わすアーク901を生成するときに、アーク901の生成に利用した全てのアーク及びノード、すなわちデータ移動関係を特定するために利用された全てのアーク及びノードに付随する設定情報IDを、新たに作成したアーク901の設定情報IDとして

複写するようにしてもよい。これにより、アクセス権の統合の際に生成されたデータ移動関係のアーキには、そのアーキの生成に利用された全てのアーキ及びノードの設定情報IDが対応付けされることになる。なお、設定情報IDでなくセキュリティ設定情報がアーキ及びノードに対応付けされていた場合には、そのセキュリティ設定情報を新たに生成されたデータ移動関係のアーキに複写するようにすればよい。このように、アクセス権の統合の際に新たに生成されたデータ移動関係のアーキに設定情報IDを対応付けさせる機能を有するアクセス権統合部40を備えたセキュリティ検証システム100においては、設定情報検索部80は、以下のような処理を行うようにすればよい。すなわち、この場合、設定情報検索部80は、パターンマッチング部52によって出力された不適経路のノード列から、不適経路を構成する全てのノードとアーキを検索したあと、それらのノードとアーキに対応付けされている設定情報IDに基づいて、設定情報格納部31からセキュリティ設定情報を検索し、検索によって抽出されたセキュリティ設定情報を検証結果表示部60に出力する処理を行う。設定情報IDでなくセキュリティ設定情報がアーキ及びノードに対応付けされていた場合には、設定情報検索部80は、設定情報格納部31を検索することなく、不適経路を構成する全てのノードとアーキに対応付けされているセキュリティ設定情報を検証結果表示部60に出力するようにすればよい。

[0276] 例2:

次に、上述したセキュリティ検証システム100の具体例を、ユーザインタフェースの観点から説明する。ここでは、図26に示したセキュリティ検証システム100において、検査コンピュータ120が備える表示装置に表示される画面を中心に説明する。

[0277] 図53は、セキュリティ検証システム100におけるユーザインターフェイスの全体像を示す基本画面の例を示している。基本画面には、複数のタブ101, 102, 103, 104, 105を表示する表示領域が設けられている。システム検証者などのユーザの操作によって、タブ101, 102, 103, 104, 105のいずれかが選択されると、選択されたタブに対応する画面が表示される。すなわち、基本画面では、検証者などによるタブの選択操作に応じて、画面の表示内容を切り替えることができ、複数の情報を表示することができる。なお、図53には、アラートタブ103が選択されたときに表示されるアラ

ート画面が示されている。

- [0278] 次に、セキュリティ検証システム100にセキュリティ認証処理を実行させる場合における、検証者などによるユーザインタフェースの操作について説明する。
- [0279] セキュリティ検証システム100にセキュリティ認証処理を実行させるときには、システム検証者などのユーザは、先ず、検査コンピュータ120が備える操作部(不図示)を操作して、表示装置に基本画面(図53参照)を表示させる。操作部としては、例えば、キーボードやマウスなどの情報入力装置が用いられる。
- [0280] 次に、システム検証者などのユーザは、操作部の操作によってトポロジータブ101を選択し、トポロジー画面を表示させる。図54及び図55は、トポロジータブ101が選択されているときに表示装置に表示されるトポロジー画面の例を示している。基本画面においてトポロジータブ101が選択されると、検査コンピュータ120は、表示装置に図54に示すトポロジー画面を表示させる。図53は、設定情報収集部70によって情報が収集されていないときのトポロジー画面の例を示している。
- [0281] 図54に示すトポロジー画面には、設定情報表示窓201と、設定情報収集ボタン203と、設定情報収集対象設定ボタン204とが設けられている。ここでは、設定情報表示窓201には、情報が未収集であることを意味する「設定情報未収集表示」202がなされている。設定情報収集ボタン203は、設定情報収集部70に対してセキュリティ設定情報の収集指示するためのボタンである。設定情報収集対象設定ボタン204は、セキュリティ設定の検証対象となるホストを選択するためのボタンである。なお、設定情報収集対象設定ボタン204を押すことで、セキュリティ設定の検証対象となるコンピュータまたは、プログラムの候補の一覧が表示され、その中からセキュリティ設定の検証対象を選択することもできる。
- [0282] 図54に示すトポロジー画面が表示されると、検証者などは、操作部の操作によって設定情報収集ボタン203を押下またはクリックし、セキュリティ設定情報の収集指示、あるいはデータ伝達経路の生成指示を行う。
- [0283] 設定情報収集ボタン203の押下またはクリックによる収集指示に応じてセキュリティ設定情報が収集されると、例えば図55に示すように、設定情報表示窓201に、収集されたセキュリティ設定情報に基づいて作成されたデータ伝達経路が表示される。こ

ここでは、図55に示すように、データ伝達経路生成部21によって生成されたデータ伝達経路(図33参照)が表示される。

- [0284] 図55に示すトポロジー画面には、データ伝達経路が表示される表示領域301と、設定情報再収集ボタン302と、検証開始ボタン303と、設定情報収集対象設定ボタン204とが設けられている。すなわち、設定情報収集ボタン203は、セキュリティ設定情報の収集等が実行された後に、設定情報再収集ボタン302に変化する。また、図55に示すトポロジー画面には、設定情報収集ボタン203が押下またはクリックされたことに応じて収集されたセキュリティ設定情報に基づいて生成されたデータ伝達経路が、設定情報表示窓201内の表示領域301に表示された状態が示されている。
- [0285] 設定情報再収集ボタン302は、設定情報収集部70に対して改めてセキュリティ設定情報の収集指示を行い、設定情報表示窓201にデータ伝達経路を再描画させるための指示を行うためのボタンである。検証開始ボタン303は、データ伝達経路生成部21によって生成されたデータ伝達経路情報格納部32に格納されたデータ伝達経路のアクセス権を統合する処理をアクセス権統合部40に実行させ、アクセス権が統合された後のデータ伝達経路を検証部50に送信させ、さらに、検証部50でのセキュリティ検証の開始を指示するためのボタンである。
- [0286] 図55に示すトポロジー画面が表示されると、検証者などは、操作部の操作によって検証開始ボタン303を押下またはクリックし、検証部50での検証の開始指示を行う。この例では、検証の開始指示に応じて、アクセス権統合部40によってアクセス権が統合され、さらにデータ伝達経路変換部51によって変換されたデータ伝達経路が生成され、パターンマッチング部52に送信される。そして、検証部50は、セキュリティ検証用ポリシーの入力待ち状態となる。
- [0287] 次いで、検証者などは、操作部の操作によって検証に用いるセキュリティ検証用ポリシーの指定するための操作を行う。すなわち、検証者などは、操作部の操作によってポリシータブ102を選択し、ポリシー画面を表示させ、ポリシー画面においてセキュリティ検証用ポリシーを指定する。
- [0288] 図56は、ポリシータブ102が選択されたときに表示装置に表示されるポリシー画面の例を示している。図56に示すように、ポリシー画面には、セキュリティ検証用ポリシ

の一覧表示がなされるポリシー一覧窓401が設けられる。ポリシー一覧窓401のチェックボックス402は、対象ポリシーを実際に用いて検証を行うかどうかを示すものである。すなわち、チェックボックス402がONになっているポリシーだけが、ポリシー入力部10によってパターンマッチング部52に送信され、検証対象のセキュリティ検証用ポリシーとされる。なお、図56においては、チェックボックス内が塗り潰し表示された状態が、そのチェックボックスがONになっていることを示している。

[0289] ポリシー画面には、ポリシーの名前、書式、意味、分類などの付属情報のうちの少なくとも1つが表示されるポリシー詳細情報表示窓408が設けられている。書式とは、ポリシーの記述形式にしたがった表記のことである。ここでは、システム検証者などのユーザによる操作部の操作によって、ポリシー一覧窓401においてポリシーの名前403が選択されると、選択されたポリシーに関する詳細情報がポリシー詳細情報表示窓408に表示されるとともに、詳細情報を表示しているポリシーの名前が、図56において破線囲み部分として表わされているように、強調表示される。

[0290] さらに、ポリシー画面には、検証開始ボタン406と、読込ボタン407と、ポリシー追加ボタン408と、保存ボタン410とが設けられている。読込ボタン407は、ポリシー格納部33に保存されているポリシーの読込指示を行うためのボタンである。保存ボタン410は、ポリシー格納部33へのポリシーの保存指示を行うためのボタンである。

[0291] この例では、ポリシー画面において、検証者などによる操作部の操作によって新規のポリシー405が選択されると、ポリシー詳細情報表示窓408のすべての情報がいったん空になる。そして、検証者などによる操作部の操作によって、ポリシー詳細情報表示窓408に新しいポリシーが書き込まれたあと、ポリシー追加ボタン409が押下またはクリックされると、新たなポリシーが、ポリシー一覧窓401に追加される。

[0292] セキュリティ検証システム100では、検証者などは、ポリシー画面において、操作部の操作によって、検証に用いるポリシーを指定したあと、検証開始ボタン406を押下またはクリックする。すると、指定したセキュリティ検証用ポリシーがパターンマッチング部52に送信されるとともに、指定したセキュリティ検証用ポリシーと既に入力されているデータ伝達経路とを用いたパターンマッチング処理が実行される。その後、さらに、設定情報検索部80による設定情報検索処理が実行され、検索結果が検証結果

表示部60に送信される。

[0293] 検証者などは、操作部の操作によって、アラートタブ103を押下またはクリックする。図57は、アラートタブ103が選択されたときに表示装置に表示されるアラート画面の例を示している。図57に示すように、アラート画面には、設定情報検索部80による検索結果の一覧が表示される。アラート一覧表示窓421には、検証結果表示部60によって、設定情報検索部80によって検索された検索結果の全ての不適設定が表示される。不適設定として表示される項目は、例えば、セキュリティ検証用ポリシーの分類、名前、書式、そのセキュリティポリシーが示す禁止経路と一致していたデータ伝送経路のうち、少なくとも1つを含む。なお、アラート一覧表示窓421に、上述した図50や図51に示した不適設定の詳細内容が表示されるようにしてもよい。

[0294] 検証者などは、操作部の操作によって、リザルトタブ104を押下またはクリックする。図58は、リザルトタブ104が選択されたときに表示装置に表示されるリザルト画面の例を示している。図58に示すように、リザルト画面には、設定情報検索部80が探索した全ての不適経路を表わすグラフ(図49参照)が表示される。リザルト画面には、検出結果表示窓431に、データ伝達経路のうち不適経路が強調表示されたグラフが表示される。また、ポリシー情報表示窓432には、検出結果表示窓431に表示されている違反経路(不適経路)に関する各種の情報を表示する。

[0295] この例では、検証者などによる操作部の操作によって表示経路変更ボタン433が選択されると、違反経路一覧が表示される。そして、検証者などによる操作部の操作によって、違反経路一覧の中から1つの違反経路が選択されると、検出結果表示窓431に表示される違反経路が変更される。なお、違反経路一覧は、例えば、図42に示すような表示形式とされる。

[0296] そして、検証者などは、操作部の操作によって、ディテールタブ105を押下またはクリックする。図59は、ディテールタブ105が選択されたときに表示装置に表示されるディテール画面の例を示している。図59に示すように、ディテール画面には、検証結果表示部60によって、不適経路の詳細が表示される。ここでは、設定情報検索部80で不適設定として検索されたセキュリティ単位情報に対応する設定情報ファイルの一覧を、設定ミスの可能性のある設定情報ファイルの内容すなわちセキュリティ単位情

報が表示される不適設定表示窓451に表示する。

[0297] ディテール画面には、不適設定表示窓451において検証者などによって選択された設定情報ファイルの内容が、設定ファイル内容表示窓452に表示される。さらに、現在表示している不適経路に関する情報が表示違反経路表示窓453に表示される。

[0298] 上記のようにして、ユーザインターフェイスのための各種の画面表示がなされ、システム検証者などのユーザによる画面上の操作に基づいて各種の処理が実行され、実行結果が表示される。

[0299] 例3:

図60は、図2に示したセキュリティ検証システム100の他の具体的構成を示している。なお、図60に示すセキュリティ検証システム100は、図26と比較すると、データ伝達経路変換部51にポリシー入力部からの情報入力がなされる構成となっている部分が異なり、他の構成は同一である。

[0300] この例では、ポリシー入力部10は、入力されたセキュリティ検証用ポリシーの先頭ノードをデータ伝達経路変換部51に出力する。データ伝達経路変換部51は、アクセス権統合部40から受けたデータ伝達経路情報を、ポリシー入力部10からのセキュリティ検証用ポリシーの先頭ノードをルートとするツリー構造に変換し、変換したツリー構造のデータをパターンマッチング部52に出力する。パターンマッチング部52は、ポリシー入力部10からのセキュリティ検証用ポリシーを、データ伝達経路変換部51によって変換されたツリー構造から検索し、検索結果を設定情報検索部80に出力する。

[0301] 次に、ステップS205に示した、この例におけるデータ伝達経路変換部51によるデータ伝達経路変換処理の具体例について説明する。ここでは、例えば、図38に示すデータ伝達経路が与えられたときのデータ伝達経路変換処理について説明する。

[0302] 図61A及び図61Bは、ポリシー入力部10からセキュリティ検証用ポリシー「(U<a> | U). *F<e>」の先頭ノードとして「(U<a> | U)」が与えられたときに、図38に示すデータ伝達経路をこの例におけるデータ伝達経路変換処理によって変換した後のデータ伝達経路を示している。図62は、この例におけるデータ伝

達経路変換処理を示すフローチャートである。

- [0303] データ伝達経路変換処理において、データ伝達経路変換部51は、まず、ステップS461において、ポリシー入力部10からセキュリティ検証用ポリシーの先頭ノードとして「(U<a> | U)」を受信する。データ伝達経路変換部51は、ステップS462において、受信したセキュリティ検証用ポリシーの先頭ノードが、グループ、すなわち、グループノードまたはORで結ばれた複数のノードをグループにしたものであるかどうかを判断する。ステップS462において、先頭ノードがグループであった場合には、データ伝達経路変換部51は、ステップS463において、そのグループに所属するノードの1つを先頭ノードとして選択する。この例では、先頭ノード「(U<a> | U)」がグループであるから、ステップS463において、グループに当てはまる任意のノード(例えば(U<a>))が選択される。ステップS462において、セキュリティ検証用ポリシーの先頭ノードがグループでない場合、すなわち単独のノードであれば、データ伝達経路変換部51は、ステップS464において、そのノードを先頭ノードとして選択する。
- [0304] 先頭ノードを選択すると、データ伝達経路変換部51は、ステップS465において、選択したノードをルートとするツリー構造を作成する。ステップS465では、上述したステップS216～ステップS223と同様の処理が実行される。その結果、この例では、図61Aに示すようなノード(例えば(U<a>))をルートとするツリー構造が生成される。
- [0305] その後、ステップS466において、受信したセキュリティ検証用ポリシーの先頭ノードがグループであり、そのグループに所属するノードに未だ先頭ノードとして選択されていないノードがあるかどうかを判断し、そのようなノードがある場合には、データ伝達経路変換部51は、ステップS462に戻り、その後、ステップS463において、そのノードを先頭ノードとして選択する。この例では、先頭ノード「(U<a> | U)」がグループであり、ノード(例えば(U<a>))が既に先頭ノードとして選択されているから、このステップS463において、グループに当てはまるノード(例えば(U))が選択される。そして、ステップS465において、選択したノードをルートとするツリー構造を作成する。その結果、この例では、図61Bに示すようなノード(例えば(U))をルートとするツリー構造が生成される。

- [0306] 上記のステップS463～ステップS466の処理は、グループに当てはまる全てのノードをルートするツリー構造のデータ伝達経路情報が作成されるまで繰り返される。
- [0307] この例では、以上のようにして、データ伝達経路変換部51が、ポリシー入力部10から入力されたセキュリティ検証用ポリシーの先頭ノードを利用して、ツリー構造のデータ伝達経路情報に変換する処理を実行する。
- [0308] 例4:
次に、図11に示したセキュリティ検証システム100dの具体的例について説明する。ここでは、セキュリティ検証システム100dにおけるセキュリティ検証処理(図13参照)の具体的動作について説明する。
- [0309] この例では、図63に示すような4つのホストSERVER1, SERVER2, FIREWALL及びCLIENTから構成されるコンピュータシステムの設定検証を行う場合について説明する。なお、すべてのホストのOSは、Linuxで構成されてるものとし、ホストSERVER1, SERVER2は、後述するサービスがインストールされたサーバとして動作するものとする。また、ホストFIREWALLは、「ipchains」と呼ばれているファイアウォール用ソフトウェアが導入され、パケットフィルタリングを行う。ホストCLIENTには、ユーザがログインして他のサーバの機能を利用するためなどに用いられるクライアントソフトが導入されている。
- [0310] 始めに、設定モデル入力部11により、コンピュータシステムの構成及びセキュリティ設定情報を表わした設定モデルをこのシステムに入力する(ステップS301参照)。設定モデルは、以下の手順で、システム検証者などのユーザによって入力された各種情報を、設定モデル入力部11が設定モデル格納部34に格納することで入力される。
- [0311] まず、設定モデル入力部11は、検証者などのユーザの操作によって入力された検証対象となるホストを、設定モデル格納部34に格納する。この処理は、検証者が検証対象となるホストを特定したことに基づいて行う。
- [0312] ここでは、図63に示すSERVER1, SERVER2, FIREWALL、及びCLIENTの4つのホストが存在するため、設定モデル入力部11によってこれら4つのホストを入力する。4つのホストが入力されると、例えば図64のように、検証対象となるホストが設

定モデル格納部34に格納される。

- [0313] 次に、検証者などは、設定モデル入力部11を操作して、ホストのIPアドレスを入力する。この例では、図65に示すようにIPアドレスがホストにそれぞれ割り当てられているものとする。この場合、検証者などは、IPアドレスがどのホストに所属しているかを表わす関数「b」を用いて、

$b(192.168.2.5) = \text{SERVER2},$

$b(192.168.2.4) = \text{SERVER1},$

$b(192.168.2.3) = b(192.168.1.1) = \text{FIREWALL},$

$b(192.168.1.2) = \text{CLIENT}$

と入力する。

- [0314] IPアドレスの所属情報は、OSがLinuxの場合には、各ホストのディレクトリ「/etc /sysconfig/network-script/」に格納された「ifcfg-eth0, ifcfg-eth1」などの設定ファイルに書かれている。具体的には、ホストSERVER2には、図66に示すファイル「ifcfg-eth1」が格納されており、このファイル中の文字列「IPADDR=」以降に続く数字がSERVER2に関連付けられたIPアドレスである。他のIPアドレスも同様である。

- [0315] ホストのIPアドレスは、前述の4つのホストとあわせて、例えば図67に示すように、設定モデル格納部34に格納される。

- [0316] 次に、ネットワーク接続を表現したグラフGを入力する。グラフGは、各IPアドレスを頂点とするグラフである。なお、この例では、検証対象のネットワークシステムが、図68に示す構成であるとする。このグラフGは、検証者がネットワーク機器の接続状況を確認し、設定モデル入力部11に対するユーザ操作を行うことによって入力される。各IPアドレスが図67に示すように定義され、検証対象のネットワークシステムが図68に示すような関係にあるため、検証対象のネットワーク接続を示すグラフGは、例えば図69の範囲aに示すように記述され、設定モデル格納部34に格納される。

- [0317] 次に、ユーザを入力する。図70は、ホストとユーザの関係を示している。図70では、角丸四角によって囲まれたノードがユーザを表わし、楕円で囲まれたノードがホストを表わし、その間の矢印はユーザのホストへの所属関係を表わしている。

- [0318] 図70に示す関係は、ユーザが所属するホストを表わす関数「b」を用いて、
b(ftp) = SERVER2,
b(student) = SERVER1,
b(hanako) = SERVER1,
b(taro) = CLIENT
と記述することができる。
- [0319] 各ホストのユーザは、OSのユーザ設定及びグループ設定により作成する。具体的には、Linuxの場合、ユーザ設定は、ディレクトリ「/etc/passwd」に格納され、グループ設定は、ディレクトリ「/etc/group」に格納されている。
- [0320] 図71は、ホストSERVER1のユーザ設定を示している。この設定により、ホストSERVER1には、ユーザ「hanako」があることが把握できる。よって、b(hanako) = SERVER1となる。
- [0321] 図72は、ホストSERVER1のグループ設定を示している。この設定により、ホストSERVER1には、グループ「student」があることが分かる。ユーザとグループは、設定モデルにおいて、共にユーザとして扱うためグループ「student」もユーザとして扱い、b(student) = SERVER1となることが把握できる。他のホストの設定についても同様である。
- [0322] 上記のようにして入力されたユーザは、前述の4つのホストやホストのIPアドレスとあわせて、例えば図73のように設定モデル格納部34に格納される。
- [0323] 次に、ファイルを入力する。各ホストのファイルは、OSのファイルシステムを参照することによって作成する。具体的には、Linuxの場合、コマンド「ls -alr」を実行することによって、ファイルの一覧を取得することができる。例えば、ホストSERVER2上で取得できるファイルの一覧は、図74に示すようになる。ファイルの一覧により、ホストSERVER2には、ファイル「paper.txt」があることが把握できる。よって、b(paper.txt) = SERVER2となる。他のホストについても同様である。上記のようにして入力されたファイルは、前述の4つのホスト、ホストのIPアドレス、及びユーザとあわせて、例えば図75に示すように設定モデル格納部34に格納される。
- [0324] 次に、ネットワークアクセス表現を入力する。検証対象システムでは、ホストFIREW

ALLでパケットフィルタリングが行われている。例えば、送信元IPアドレス「192. 168 . 1. 2」の任意のポート番号から、送信先IPアドレス192. 198. 2. 4のポート番号80への通信が許可されているとする。この情報と、フィルタリングが行われているIPアドレスにより、ネットワークアクセス表現の設定n(192. 168. 2. 3, 192. 168. 1. 2, 192. 168. 2. 4, 80)が作成できる。このようにして入力されたネットワークアクセス表現は、例えば、図69の範囲bに示すように記述され、設定モデル格納部34に格納される。

[0325] 次に、ファイルのアクセス制御行列表現を入力する。「アクセス制御行列表現」とは、ファイルに対するユーザのアクセス権限の有無を表わしたものであり、アクセス権限にはファイルの読み取り権限を表わす「read」と、ファイルの書き出し権限を表わす「write」の2種類がある。例えば、コマンド「ls ? alr」の出力結果より、図74に示すように、各ファイルに対してそのファイルの所有者と権限とを把握することができる。図74に示す一覧では、ユーザ「ftp」は、ファイル「paper. txt」に対して、「read」権限と「write」権限とを与えられている。この情報により、アクセス制御行列表現「acc(ftp, read, paper. txt)、acc(ftp, write, paper. txt)」と記述できる。このように入力されたファイルのアクセス制御行列表現は、図69の範囲eに示すように記述され、設定モデル格納部34に格納される。

[0326] 次に、サービス利用によりどのような権限獲得が引き起こされるか、すなわち権限獲得関係を入力する。「権限獲得」とは、あるユーザがサービスを利用して他のユーザの権限を獲得できることを表わしており、あるユーザが、他のユーザのID、パスワードなどの認証に必要な情報を保持しているとき、または、特別な認証を経ずに権限獲得できる場合には無条件に作成する。具体的には、ホスト上で実行されているネットワークサービスと、その設定を調べることによって作成できる。

[0327] この例では、ホストSERVER1上でサービス「telnet」が提供されており、かつ、ホストCLIENTのユーザ「taro」は、ホストSERVER1のユーザ「hanako」にサービス「telnet」でアクセスするときのパスワードを知っているものとする。また、本例では、ホストSERVER2では匿名ftp(anonymous FTP)サービスが提供されており、ホストSERVER1上のグループ「student」に属するユーザは無条件にこのサービス「ftp」を

利用できるものとする。その場合、ホストCLIENTのユーザ「taro」は、ホストSERVER1のユーザ「hanako」の権限をサービス「telnet」によって獲得できる。このため、権限獲得関係は、auth(taro, telnet, hanako)となる。また、ホストSERVER1のユーザ「student」は、無条件でホストSERVER2のユーザ「ftp」の権限をサービス「ftp」で獲得できる。このため、権限獲得関係は、auth(student, ftp, ftp)となる。

[0328] サービス「null」は、ユーザがグループに所属していることを表わす。Linuxの場合、図71に示すユーザ設定ファイルと、図72に示すグループ設定ファイルとから、サービス「null」を用いた権限獲得関係を作成することができる。具体的には、図71に示すユーザ設定ファイルより、ユーザ「hanako」のグループIDが「501」であり、図72に示すグループ設定ファイルのグループIDが「501」であるグループが「student」であることから、ユーザ「hanako」は、グループ「student」に所属していることが把握できる。よって、権限獲得関係として、auth(hanako, null, student)を作成することができる。

[0329] このように入力された権限獲得関係は、図69の範囲cに示すように記述され、設定モデル格納部34に格納される。

[0330] 次に、カスケード関係を入力する。「カスケード関係」とは、あるサービスを利用して権限獲得したときに、引き続き利用できるサービスの種類を表わしたものである。これは、サービスの種類により決まっている。具体的には、サービス「telnet」で権限を獲得したあとにサービス「ftp」を利用することはできるが、サービス「ftp」で権限を獲得したあとにサービス「telnet」を利用することはできないなどのように、サービスの種類によってあらかじめ定められている。また、利用できる権限の種類は、該当するサービスがホストにインストールされているか否かや、権限を獲得したユーザがサービスの実行権限を持っているか否かで決まる。本例では、サービス「telnet」でホストSERVER1のユーザ「hanako」の権限を獲得したときに、サービス「null」を利用することができる。よって、カスケード関係は、cas(telnet, hanako, null)となる。また、サービス「null」を利用してホストSERVER1のユーザ「student」の権限を獲得したときに、サービス「ftp」を利用することができる。よって、カスケード関係は、cas(null, student, ftp)となる。

- [0331] このように入力されたカスケード関係は、図69の範囲dに示すように記述され、設定モデル格納部34に格納される。
- [0332] さらに、サービスが利用するネットワークのポート番号を、図69の範囲fに示すように入力する。なお、Linuxでは、ファイル「/etc/services」を参照することによってサービス名とポート番号の対応を調べることができる。
- [0333] 以上のようにして、設定モデルを構成する各種の情報が入力され、設定モデル格納部34に順次格納されることで、設定モデル格納部34内に、検証対象システムのシステム構成(図75等参照)を含む設定モデル(図69参照)が構築される。すなわち、設定モデル格納部34に設定モデルが入力される。
- [0334] 次に、ステップS302において、ポリシー入力部10によりセキュリティ検証用ポリシーを入力する。この例で与えるセキュリティ検証用ポリシーは、ポリシー「flow(secret.txt, paper.txt)」であるものとする。このポリシー「flow(secret.txt, paper.txt)」は、secret.txtから、paper.txtへのデータの移動があってはいけないことを表わしており、secret.txtの内容をpaper.txtに書き込んで서는ならないという禁止ポリシーである。
- [0335] 上記のようにして入力された設定モデルとポリシーとを用いて、検証部50aは、ステップS303において、ポリシーにマッチするモデルがあるか否かを検証する処理を行う。
- [0336] 検証部50aは、公知の言語処理系であるPrologインタプリタを用いて実現することができる。ここで、ポリシー記述中の各述語のうち、「acc」、「auth」、及び「cas」は、組み込み述語として実装する。
- [0337] なお、それぞれの組み込み述語の実装の内容は、
acc(U, S, F):「設定モデル格納部中のアクセス制御行列表現に、(U, S, F)が含まれる場合にtrue(真)」
cas(S1, U, S2):「設定モデル格納部中のカスケード関係に、(S1, U, S2)が含まれる場合にtrue」
auth(U1, S, U2):「設定モデル格納部中の権限獲得関係に、(U1, S, U2)が含まれ、かつ、U1が属するホストから、U2が属するホストに対して、U2上でサ

ービスSを実現するポートへのコネクションが確立できる場合にtrue」であるものとする。

[0338] ここで、ユーザ「U1」が属するホストから、ユーザ「U2」が属するホストに対して、ユーザ「U2」上でサービス「S」を実現するポートへのコネクションが確立できるか否かの判定は、設定モデル格納部34に設定モデルとして格納されているネットワーク接続表現に、ユーザ「U1」が属するホストから、ユーザ「U2」が属するホストを結ぶ経路があり、かつ、その経路中で、当該ポートが、設定モデル格納部34に設定モデルとして格納されているネットワークアクセス表現で許可されているか否かを検査することによって実現することができる。

[0339] また、データフロー関係を表わす述語flowは、

flow (F, F) :- true.

flow (F1, F2) :- flow2(F1, F3), flow(F3, F2).

flow2 (F1, F2) :- acc (U1, read, F1), auth2 (U3, S1, U1),
auth2 (U3, S2, U2), acc (U2, write, F2).

auth2 (U, S, U) :- true.

auth2 (U3, S1, U1) :- auth (U3, S1, U2), cas (S1, U2, S2),
auth2 (U2, S2, U1).

のようなPrologプログラムによって記述できる。

[0340] したがって、ポリシー入力部10によって記述されたポリシーが設定モデルとマッチするか否かは、上記の組み込み述語を備えたProlog処理系上の上記のPrologプログラムによって判定することができる。

[0341] 以上説明した機能を有する検証部50aを用いる構成とすることで、ポリシー「flow(secret.txt, paper.txt)」が、設定モデル格納部34に格納された設定モデルにマッチするか否かを判定できる。

[0342] この例で示した設定モデルの場合、ポリシー「flow(secret.txt, paper.txt)」にマッチするという結果が得られる。

[0343] この例では、マッチした許可ポリシーを検証結果表示部60によって表示するものとする。具体的は、図76に示すように、検証したポリシーを表示して、検証者に提示す

る。また、図76に示すように、ポリシーがあってはならない経路を示したものか、なくてはならない経路を示したものを、ポリシーの種類として提示する。すなわち、ポリシーの種類が禁止ポリシーであるか許可ポリシーであるかを報知する。また、図76に示すように、マッチした禁止ポリシーを表示するときに、その禁止ポリシーが示すあってはならない経路にマッチした設定モデルを合わせて表示してもよい。

[0344] さらに、ポリシー格納部33にポリシーの説明などの付随情報が格納されているときは、説明文などの付随情報をあわせて表示するようにしてもよい。

[0345] 以上のように、システム構成及び設定を、設定モデルとして入力し、あってはならないフローや、なくてはならないフローを示したポリシーを用いてモデルを検索し、ポリシーとモデルを表示する構成としたので、検証者は、表示されたポリシーやモデルを頼りに、設定を見直すことができ、複数のホストやプログラムの設定が複合的に関係した設定ミスを発見し修正することができる。

[0346] 例5:

次に、図16に示した第1の実施形態のセキュリティ検証用データ生成システムについての具体的な例について説明する。

[0347] 図77は、検証対象となるコンピュータシステムの構成例を示している。図77に示す破線の四角はセグメント(ネットワークセグメント)を表わしていて、ここでは、インターネット(Internet)セグメント951、DMZ(DeMilitarized Zone;非武装地帯)セグメント952、及びLANセグメント953の3つのセグメントがある。また、図77では、ホストを実線の四角で表わしている。各セグメントにはホストが存在し、Internetセグメント951には、IPアドレスが12. 34. 56. 7であるOutside-Client(外部クライアント)ホスト954がある。DMZセグメント952には、IPアドレスが10. 56. 1. 1であるFire Wall(ファイアウォール)ホスト955と、IPアドレスが10. 56. 1. 10であるWWWホスト956と、IPアドレスが10. 56. 1. 20であるData(データ)ホスト957とがある。LANセグメント953には、IPアドレスが10. 56. 2. 10であるInside-Client(内部クライアント)ホスト958がある。

[0348] Outside-Clientホスト954では、ウェブ(web)、ftp、sambaの各クライアント(client)アプリケーションが稼動しており、outsider(外部)ユーザがある。Fire Wallホス

ト955には、root(ルート)ユーザがある。WWWホスト956では、ウェブサーバが稼働しており、w-tanakaユーザと、w-suzukiユーザと、customerユーザと、webmasterユーザがあり、“/passwd/顧客ID管理情報.xml”ファイルと、“/home/w-suzuki/index.html”ファイルがある。Dataホスト957では、sambaサーバが稼働しており、guestユーザと、s-tanakaユーザと、s-suzukiユーザがあり、“/secret/4月顧客情報.xml”ファイルと、“/secret/アンケート.xml”ファイルと、“/secret/集計結果.xml”ファイルと、“/回路図.svg”ファイルがある。Inside-Clientホスト958では、ウェブクライアントとsambaクライアントとが稼働しており、tanakaユーザと、suzukiユーザと、miyamotoユーザと、wwwユーザがあり、“/secret/4月顧客情報.xml”ファイルがある。

[0349] 図16に示したセキュリティ検証用データ生成システムのシステム構成情報収集部1402は、図77に例示したコンピュータシステムからシステム構成情報を収集する。属性情報入力部1403は、属性情報が入力され、その属性情報をシステム構成情報に付加して属性情報格納部1404に格納する。属性情報の入力を受け付ける際には、例えば、ディスプレイ装置(不図示)によりシステム構成情報を管理者あるいはオペレータに対して提示し、その管理者あるいはオペレータが入力した属性情報を受け付けられればよい。

[0350] 図78は、ネットワーク構成情報属性が付加されたシステム構成情報すなわちネットワーク構成情報の一例を示している。この例では、「networksystem」エレメント内に、複数(ここでは3つ)の「segment」エレメントが記述されている。記述1601は、「segment」エレメントのうちの一つ、具体的にはDMZセグメントのエレメントを示している。この記述1601を例に説明すると、「segment」エレメントには、セグメントの名称(この例では“DMZ”)が、ネットワーク構成情報属性のname属性として記述されている。また、「segment」エレメント内には、そのセグメントに所属するホストの情報が格納されている。各ホストの情報は、hostタグに囲まれた「host」エレメントとして記述される。記述1602は、3つの「host」エレメントを示している。各「host」エレメントには、name属性として、各ホストの名称(この例では、“Fire Wall”, “WWW”, 及び“Data”)が記述されている。各「host」エレメント内には、記述1603に示すように、そのホ

ストが持つIPアドレスが「ip」エレメントにおけるaddress属性として記述されている。

記述1603は、ホストFire Wallに関するものなので、このホストが保持する3つのIPアドレスを含んでいる。

[0351] 図78において、categoryタグで囲まれた記述すなわち「category」エレメントは、セグメントのネットワークセグメント役割情報や、ホストの役割情報を表わす属性情報を表わしている。図示する例における「<category>DMZ</category>」は、セグメントの役割がDMZであることを示す属性情報である。また、「<category>public__www</category>」は、ホストの役割が“public__www”であることを示す属性情報(ホスト構成情報属性)である。

[0352] 図79は、サービス情報属性が付加されたシステム構成情報すなわちサービス情報の一例を示している。この例では、サービス情報属性は、「Service」エレメント内で、サービス名単位で管理されている。ここで、httpサービスの「Service」エレメントの記述である記述1701を用いて、「Service」エレメントを説明する。「Service」エレメント内には、暗号化の有無がencryption属性として記述される。記述1701では、encryption属性が“OFF”として記述されている。なお、encryption属性が“OFF”の場合、暗号化しないことを示し、“ON”の場合、暗号化することを示す。また、各「Service」エレメントは、属性情報として「port」エレメントを含む。「port」エレメント内には、対象サービスが利用するポート番号が記述される。例えば、記述1701に含まれる「port」エレメントの記述1702では、「80」というポート番号が記述されている。これは、httpサービスがTCPにおける80番ポートを使用することを意味する。また、特定のホストでのみ特定のポートでサービスが行われる場合には、記述1703に示すように、「port」エレメントにポート番号ではなく、IPアドレスが記述されることもある。

[0353] 図80は、ユーザ情報属性が付加されたシステム構成情報すなわちユーザ情報の一例を示している。この例では、「UserList」エレメント内に、ユーザの役割ごとに「UserCategory」エレメントが記述されている。記述1801は、「UserCategory」エレメントのうちの一つを示している。「UserCategory」エレメントのname属性には、ユーザの役割が記述される。例えば、記述1801の「UserCategory」エレメントのname属性では、ユーザの役割として「営業」が記述されている。また、「UserCategory」エ

メント内には、その「UserCategory」エレメントのname属性が示す役割に該当するユーザが、それぞれ「User」エレメントとして記述される。例えば、記述1801の「UserCategory」エレメント内の記述1802では、「営業」という役割を担うユーザの「User」エレメントが2つ記述されている。「User」エレメントのname属性には、ユーザの名前が記述される。記述1802に含まれる二つの「User」エレメントでは、それぞれname属性として“suzuki”, “miyamoto”が記述されている。また、「User」エレメント内には、記述1803に示すように、ユーザが持っているユーザアカウントが「ID」エレメントとして記述される。図80に例示する「ID」エレメントでは、ユーザアカウントの名前が「ID」エレメントのname属性に記述され、ユーザアカウントが登録されているホストが「ID」エレメントのhost属性に記述され、ユーザアカウントを管理しているアプリケーションがapplication属性に記述されている。例えば、記述1803における最初の「ID」エレメントでは、name属性、host属性、application属性は、それぞれ“suzuki”, “10.56.2.10”, “OS”と記述されている。また、図21に示したシステム構成情報(ユーザ情報)は、この「ID」エレメントの記述部分に相当する。したがって、図80において、「ID」エレメントの記述部分は、システム構成情報(ユーザ情報)に該当し、図80におけるそれ以外の記述部分、例えば、「営業」等の役割を示す役割情報や、「User」エレメントにおけるname属性等は、ユーザ情報に付加されるユーザ情報属性に該当する。

- [0354] 図81は、ファイル情報属性が付加されたシステム構成情報すなわちファイル情報の一例を示している。この例では、「contents」エレメント内において、ファイルが格納されているホストごとに、具体的には「host」エレメントごとに、ファイル情報属性が記述されている。例えば、記述1901には、一つのホストに格納されているファイルのファイル情報属性が記述されている。「host」エレメント内では、記述1902に示すように、ファイルごとに「file」エレメントが記述される。「file」エレメントのname属性には、ファイルの格納場所及びファイル名が記述される。このファイル格納場所及びファイル名の記述はファイル情報に該当し、他の記述がファイル情報属性に該当する。例えば、記述1902では、“／passwd／顧客ID管理情報.xml”という記述がファイル情報(システム構成情報)に該当し、他の記述部分がファイル情報属性に該当する。

また、「file」エレメントには、そのファイルの内容、役割、あるいは種別を表わすファイル情報属性が、「category」エレメントとして記述される。例えば、記述1903に含まれる2つの「category」エレメントでは、“個人情報”、“顧客情報”というファイルの種別や役割が示されている。

[0355] 本例のセキュリティ検証用データ生成システムは、構成としては図16に示したセキュリティ検証用データ生成システムと同様のものであるから、アクセスポリシー生成部1405を備えている。このアクセスポリシー生成部1405は、システム構成情報に付加された属性情報を用いて、アクセスポリシーを作成する。アクセスポリシー生成部1405は、属性情報ではなく、「移動元」、「移動先」、「移動経路」そのものを直接示す情報を入力し、その情報を用いてアクセスポリシーを作成してもよい。

[0356] 図82は、アクセスポリシー生成部1405によって作成されたアクセスポリシーの一例を示している。この例では、アクセスポリシーは、ファイルとして作成され、ファイルとして管理される。図82に示すように、アクセスポリシーは、InputPolicyListタグに囲まれた範囲に記述される。そして、InputPolicyListタグに囲まれた範囲内で、個々のアクセスポリシーは、「InputPolicy」エレメントとして記述される。図示するように、「InputPolicy」エレメント、すなわちInputPolicyタグに囲まれた記述は、複数存在してもよい。一つの「InputPolicy」エレメントにおいて、移動元は「Src」エレメントとして記述され、移動先は「Dst」エレメントとして記述され、移動経路は「Service」エレメントとして記述される。図示する例では、「InputPolicy」エレメント2001の中に、移動元を示す「Src」エレメント2002と、移動先を示す「Dst」エレメント2003と、移動経路を示す「Service」エレメント2004とが含まれている。

[0357] 「Src」エレメント及び「Dst」エレメントには、「NodeString」エレメントと「Domain」エレメントが記述される。図82に示す例では、「Src」エレメント2002には、「NodeString」エレメント2005と「Domain」エレメント2006とが含まれている。「NodeString」エレメントには、アクセスポリシー作成時に、オペレータが直接指定した情報が記述される。オペレータが直接指定した情報とは、候補となる情報を提示してその中から選択されたものではなく、候補を提示しない状態でオペレータが指定した情報を意味する。例えば、「NodeString」エレメント2005では、オペレータが直接指定した移動元

として、「/mnt/apache/htdocs/index.html」というファイルの格納場所及びファイル名が記述されている。また、「Domain」エレメントには、ドメインが記述される。アクセスポリシー作成時に、オペレータに属性情報の選択候補を提示して、その候補の中から属性情報がオペレータによって選択された場合には、「Src」エレメントや「Dst」エレメントは、「NodeString」エレメントの代わりに、「Category」エレメントを含む。例えば、図82での2番目の「InputPolicy」エレメントは、「Category」エレメント2007を含んでいる。この「Category」エレメント2007は、送信元の属性情報の中から選択された「顧客情報」という属性情報を示している。

[0358] 次に、アクセスポリシー作成時すなわち図22に示すステップS603において、アクセスポリシー生成部1405がオペレータに提示するユーザインタフェースについて説明する。図83は、アクセスポリシー作成時にオペレータに提示される初期画面の一例を示している。

[0359] アクセスポリシー生成部1405は、アクセスポリシー作成時において、まず図83に例示する初期画面をディスプレイ装置(不図示)表示する。アクセスポリシー生成部1405は、初期画面内のアクセスポリシー表示欄2101に、既に作成済みのアクセスポリシーを表示する。あるいは、推奨するアクセスポリシーとして、デフォルトとして設定されたアクセスポリシーをアクセスポリシー表示欄2101に表示してもよい。アクセスポリシー生成部1405は、アクセスポリシー表示欄2101に表示する各アクセスポリシーと対応させて、ラジオボックス2102と、編集ボタン2103と、削除ボタン2104とを表示する。ラジオボックス2102は、ラジオボックスに対応するアクセスポリシーを有効にするか無効にするかを指定するために用いられる。例えばマウスクリック等によって編集ボタン2103が操作された場合、アクセスポリシー生成部1405は、操作された編集ボタンに対応するアクセスポリシーの編集画面をディスプレイ装置に表示する。また、削除ボタン2104が操作された場合、アクセスポリシー生成部1405は、操作された削除ボタンに対応するアクセスポリシーを削除する。また、アクセスポリシー生成部1405は、初期画面内に新規作成ボタン2105を表示する。新規作成ボタン2105が操作された場合、アクセスポリシー生成部1405は、アクセスポリシー新規作成画面をディスプレイ装置に表示する。なお、編集画面は、アクセスポリシー新規作成画面と同様のユー

ザインタフェースを有し、オペレータに対して編集を促すものであればよい。

[0360] 図84は、アクセスポリシー新規作成画面の一例を示している。アクセスポリシー生成部1405は、アクセスポリシー新規作成画面内に、画面選択肢2201と決定ボタン2202と移動元入力欄2203と移動先入力欄2204と移動経路入力欄2205と適用ボタン2206とを表示する。画面選択肢2201は、移動元入力画面、移動先入力画面、及び移動経路入力画面のいずれかの選択をオペレータに促す選択肢の表示である。画面選択肢2201においてオペレータによる選択が行われ、決定ボタン2202が操作されると、アクセスポリシー生成部1405は、オペレータによる選択結果に応じて、移動元入力画面、移動先入力画面、または移動経路入力画面を表示する。すなわち、「移動元を作成する」が選択された場合には移動元入力画面を表示し、「移動先を作成する」が選択された場合には移動先入力画面を表示し、「移動経路を作成する」が選択された場合には移動経路入力画面を表示する。移動元入力画面、移動先入力画面、または移動経路入力画面では、それぞれ移動元、移動先、移動経路の情報を指定されるが、これらの各画面については、図85～図87を用いて後述する。

[0361] また、移動先、移動元、移動経路の各項目の入力値をオペレータが予め把握している場合には、オペレータは、キーボード等の入力装置を用いて、移動元入力欄2203、移動先入力欄2204、及び移動経路入力欄2205にそれらの入力値を直接入力してもよい。移動元入力欄2203、移動先入力欄2204、及び移動経路入力欄2205に入力される値は、選択候補を提示しない状態でオペレータが指定する入力値、すなわちオペレータが直接指定する入力値である。

[0362] アクセスポリシー生成部1405は、適用ボタン2206が操作されると、移動元入力画面、移動先入力画面、及び移動経路入力画面において指定された移動元、移動先、移動経路の情報や、移動元入力欄2203、移動先入力欄2204、及び移動経路入力欄2205に入力された情報に基づいて、図82に例示するアクセスポリシーを作成する。そして、アクセスポリシー生成部1405は、図83に示す初期画面(図83参照)を再び表示する。

[0363] 図85は、移動元入力画面の一例を示している。アクセスポリシー生成部1405は、移動元入力画面内に、移動元タイプ選択欄2301と移動元選択欄2302とドメイン選

択欄2303と決定ボタン2308とを表示する。

- [0364] 移動元タイプ選択欄2301は、情報の移動元としてのファイルまたはユーザのいずれかの選択を、オペレータに対して促すものである。図85に示す例では、プルダウンメニューにより、移動元としてファイルが選択されている。
- [0365] ここでは、アクセスポリシー生成部1405は、移動元選択欄2302内に、移動元指定方法選択欄2304と選択肢表示欄2305とを表示する。移動元指定方法選択欄2304は、属性情報を用いずにファイル名やユーザ名等を指定するのか、あるいは属性情報を指定するのかの決定をオペレータに促すものである。この例では、移動元指定方法選択欄2304をプルダウンメニューにより実現している。移動元指定方法選択欄2304は、移動元タイプ選択欄2301で「ファイル」が指定されている場合に、例えば「ファイルカテゴリーで選択する」、「ディレクトリで指定する」、「ファイルで指定する」の指定方法のうちのいずれかの選択をオペレータに促すものである。また移動元タイプ選択欄2301で「ユーザ」が指定されている場合には、移動元指定方法選択欄2304は、「ユーザカテゴリーで選択する」、「ユーザ名で指定する」の指定方法のうちのいずれかの選択をオペレータに促す。
- [0366] また、アクセスポリシー生成部1405は、移動元指定方法選択欄2304で選択された指定方法に応じた選択肢を選択肢表示欄2305に表示し、その選択肢の中から一つの項目を選択するようにオペレータに促す。図85に示す例では、「ファイルカテゴリーで選択する」という指定方法が選択されたので、アクセスポリシー生成部1405は、「顧客情報」、「個人情報」、「一般情報」、「秘密情報」及び「機密情報」というファイル情報属性を選択肢として選択肢表示欄2305に表示しており、この例では、選択肢表示欄2305において「個人情報」が選択されている。アクセスポリシー生成部1405は、「ディレクトリで指定する」または「ファイルで指定する」という指定方法が移動元指定方法選択欄2304で選択された場合には、選択肢表示欄2305にディレクトリ名やファイル名を表示して、ディレクトリ名やファイル名の選択をオペレータに促す。なお、ディレクトリ名やファイル名は、属性情報に該当しない。アクセスポリシー生成部1405は、「ユーザカテゴリーで選択する」という指定方法が移動元指定方法選択欄2304で選択された場合には、例えば、「部長」、「課長」、「一般社員」、「ウェブ管理者」、「

営業」等のユーザ情報属性を選択肢として選択肢表示欄2305に表示し、ユーザ情報属性の選択をオペレータに促す。「ユーザ名で指定する」という指定方法が移動元指定方法選択欄2304で選択された場合には、アクセスポリシー生成部1405は、選択肢表示欄2305にユーザ名を表示して、ユーザ名の選択をオペレータに促す。なお、ユーザ名も、属性情報に該当しない。

[0367] また、アクセスポリシー生成部1405は、ドメイン選択欄2303内に、ドメイン指定方法選択欄2306とドメイン選択肢表示欄2307とを表示する。ドメイン指定方法選択欄2306は、ドメインとして例えばセグメントを指定するのか、あるいはホストを指定するのかの選択をオペレータに促すものである。図示した例では、ドメイン指定方法選択欄2306は、プルダウンメニューにより実現されている。ドメイン指定方法選択欄2306は、例えば、「セグメントで指定する」、「ホストで指定する」、「ドメインを指定しない」という指定方法のうちのいずれかの選択をオペレータに促すものである。

[0368] アクセスポリシー生成部1405は、ドメイン指定方法選択欄2306で選択された指定方法に応じた選択肢をドメイン選択肢表示欄2307に表示し、その選択肢の中から一つの項目を選択するようにオペレータに促す。図85に示す例では、「セグメントで指定する」という指定方法が選択されているので、アクセスポリシー生成部1405は、ネットワーク構成情報属性に含まれる「LAN」、「DMZ」及び「Internet」というセグメント名を選択肢としてドメイン選択肢表示欄2307に表示しており、これらの中で「DMZ」が選択されている。アクセスポリシー生成部1405は、「LAN」、「DMZ」及び「Internet」等の選択肢として、ネットワーク構成情報に付加された属性情報である「segment」エレメントのname属性(図78参照)を表示すればよい。アクセスポリシー生成部1405は、「ホストで指定する」という指定方法がドメイン指定方法選択欄2306で選択された場合、ドメイン選択肢表示欄2307にホストを表示して、ホストの選択をオペレータに促す。なお、この場合に選択されるホストは、属性情報に該当しない。また、アクセスポリシー生成部1405は、ドメイン指定方法選択欄2306において「ドメインを指定しない」という項目が選択された場合には、ドメイン選択肢表示欄2307を表示しなくてよい。

[0369] アクセスポリシー生成部1405は、決定ボタン2308を操作されると、移動元タイプ選

択欄2301、移動元選択欄2302及びドメイン選択欄2303における、オペレータが指定した内容を確認し、アクセスポリシー新規作成画面(図84参照)を表示する。図85に示す例では、アクセスポリシー生成部1405は、移動元として「DMZ」セグメント内の「個人情報」ファイルが指定されたことを確定する。

[0370] 図86は、移動先入力画面の一例を示している。アクセスポリシー生成部1405は、移動先入力画面内に、移動先タイプ選択欄2401と移動先選択欄2402とドメイン選択欄2403と決定ボタン2408とを表示する。移動先入力画面の画面構成は、移動元入力画面の画面構成と同様である。移動先選択欄2402は、図85に示す移動元選択欄2302と同様に、移動先指定方法選択欄2404と選択肢表示欄2405とを含む。ドメイン選択欄2403は、図85に示すドメイン選択欄2303と同様に、ドメイン指定方法選択欄2406とドメイン選択肢表示欄2407とを含む。移動先入力画面における移動先のタイプの選択、移動先の選択、及びドメインの指定の態様は、移動元入力画面における移動元のタイプの選択、移動元の選択、及びドメインの指定の態様と同様である。

[0371] アクセスポリシー生成部1405は、決定ボタン2408が操作されると、移動先タイプ選択欄2401、移動先選択欄2402及びドメイン選択欄2403における指定内容を確認し、アクセスポリシー新規作成画面(図84参照)を表示する。図86に示す例では、アクセスポリシー生成部1405は、移動先として「LAN」セグメント内の「営業」ユーザが指定されたことを確定する。

[0372] 図87は、移動経路入力画面の一例を示している。アクセスポリシー生成部1405は、移動経路入力画面内に、移動経路指定方法選択欄2501と移動経路指定欄2502と決定ボタン2503とを表示する。

[0373] 移動経路指定方法選択欄2501は、サービス属性により移動経路を指定するのか、他の方法、例えば、サービス名やポート番号により移動経路を指定するのかの決定をオペレータに促すためのものである。ここでは、移動経路指定方法選択欄2501をプルダウンメニューにより実現している。移動経路指定方法選択欄2501は、選択候補として、例えば、「サービス属性」、「サービス名」、「ポート番号」を表示する。図86には、「サービス属性」が選択された場合が示されている。

- [0374] アクセスポリシー生成部1405は、移動元指定方法選択欄2501で選択された指定方法に応じた移動経路指定欄2502を表示する。図86に示した例では、「サービス属性」が選択された結果、アクセスポリシー生成部1405は、「暗号化の有無」や「認証の有無」というサービス属性によって移動経路を指定する欄を表示しており、ここでは、暗号化を行わない移動経路が指定されている。アクセスポリシー生成部1405は、移動経路指定方法選択欄2501において「サービス名」や「ポート番号」が選択された場合、移動経路指定欄2502にサービス名やポート番号を表示して、サービス名やポート番号による移動経路の指定を促す。なお、この場合に指定されるサービス名やポート番号は、属性情報に該当しない。
- [0375] アクセスポリシー生成部1405は、決定ボタン2503が操作されると、移動経路指定方法選択欄2501及び移動経路指定欄2502における指定内容を確定し、アクセスポリシー新規作成画面(図84参照)を表示する。
- [0376] 移動元入力画面(図85参照)、移動先入力画面(図86参照)及び移動経路入力画面(図87参照)における指定内容が確定した後、図84に示したアクセスポリシー新規作成画面内の適用ボタン2206が操作されると、アクセスポリシー生成部1405は、指定内容に応じたアクセスポリシーを作成する。なお、移動元入力画面内のドメイン指定方法選択欄2306において「ドメインを指定しない」と指定された場合には、アクセスポリシー生成部1405は、「Src」エレメント(図82参照)内に「Domain」エレメントを作成しない。同様に、移動先入力画面内のドメイン指定方法選択欄2406において「ドメインを指定しない」と指定された場合には、アクセスポリシー生成部1405は、「Dst」エレメント(図82参照)内に「Domain」エレメントを作成しない。
- [0377] このように図85～図87に例示した指定内容が確定され、図84に示すアクセスポリシー新規作成画面が表示され、その後、適用ボタン2206(図84参照)が操作されたとする。その場合、アクセスポリシー生成部1405は、『「DMZ」セグメント内の「個人情報」ファイルから「LAN」セグメント内の「営業」部員に対して暗号で保護されていない経路を用いて情報が移動してはならない。』というアクセスポリシーを作成することになる。
- [0378] 次に、このようにしてアクセスポリシー生成部1405が作成したアクセスポリシーを、

検証ポリシー生成部1407(図16参照)が検証ポリシーに変換する動作を説明する。アクセスポリシーから検証ポリシーへの変換は、アクセスポリシーの移動元、移動先及び移動経路が属性を用いて指定されたときに、それらの属性に基づいて、実際のファイル名やユーザアカウントなどのシステム構成要素を検索して、検索結果を用いて移動元、移動先及び移動経路を表わすことにより実現する。検証ポリシーへの変換は、移動元や移動先として属性情報を用いて指定されたユーザについて、そのユーザをユーザアカウントに変換する動作と、移動元や移動先として属性情報を用いて指定されたファイルについて、そのファイルをファイル名に変換する動作と、移動経路として属性を用いて指定されたサービスについて、そのサービスをIPアドレスやポート番号に変換する動作と、に分けられる。以下、これらの3つの動作について説明する。

[0379] 図88に示すフローチャートは、移動元や移動先としてユーザが属性情報を用いて指定されているときに、そのユーザから変換されるユーザアカウントを検索する動作を示している。この動作は、上述した図22でのステップS605やステップS607で行われる。

[0380] まず、検証ポリシー生成部1407は、ステップS701において、アクセスポリシーのユーザ指定にドメイン指定があるか否かを判定する。すなわち、検証ポリシー生成部1407は、ユーザを表わすアクセスポリシー内の「Src」エレメントまたは「Dst」エレメントが「Domain」エレメントを含んでいるか否かを判定する。なお、「Src」エレメントまたは「Dst」エレメント内の「Domain」エレメントは、ドメイン選択欄2303(図85参照)やドメイン選択欄2403(図86参照)においてドメインが指定された場合に、アクセスポリシー生成部によって生成されている。

[0381] ユーザを表わすアクセスポリシー内の「Src」エレメントまたは「Dst」エレメントが「Domain」エレメントを含んでいるとステップS701において判定した場合、検証ポリシー生成部1407は、ステップS702において、そのドメインの指定が、ネットワーク構成情報に付加された属性情報である「segment」エレメントのname属性(図78参照)を利用して行われたか否かを判定する。「segment」エレメントのname属性を利用してドメイン指定が行われた場合というのは、アクセスポリシー生成部1405が、ネットワーク

構成情報に付加された属性情報である「segment」エレメントのname属性を選択肢としてドメイン選択肢表示欄2307(図85参照)やドメイン選択肢表示欄2407(図86参照)に表示し、その選択肢の中からドメインが指定された場合のことである。

- [0382] 「segment」エレメントのname属性を利用してドメイン指定が行われたとステップS702で判定した場合には、検証ポリシー生成部1407は、ステップS703において、ネットワーク構成情報属性が付加されたシステム構成情報、すなわち図78に示すネットワーク構成情報から、アクセスポリシー作成時にドメインとして指定されたセグメントに含まれる全てのホストのIPアドレスを検索する。一方、「segment」エレメントのname属性を利用せずにドメイン指定が行われたと判定した場合には、検証ポリシー生成部1407は、ステップS704において、アクセスポリシー作成時にドメインとして指定されたホストのIPアドレスを、ネットワーク構成情報属性が付加されたシステム構成情報すなわちネットワーク構成情報から検索する。ステップS703, S704の後、ステップS705に移行する。
- [0383] ステップS705において、検証ポリシー生成部1407は、以下のようにしてユーザアカウントを取り出す。検証ポリシー生成部1407は、アクセスポリシー作成時に移動元選択欄2302(図85参照)または移動先選択欄2402(図86参照)で指定された属性情報を有するユーザを、ユーザ情報属性が付加されたユーザ情報(図80参照)の中から特定する。そして、そのユーザのユーザアカウントのうち、ステップS703またはステップS704で検索したIPアドレスに対応するユーザアカウントを取り出す。
- [0384] ステップS701において、ユーザを表わすアクセスポリシー内の「Src」エレメントまたは「Dst」エレメントが「Domain」エレメントを含んでいないと判定した場合、検証ポリシー生成部1407は、ステップS706において、アクセスポリシー作成時に移動元選択欄2302または移動先選択欄2402で指定された属性情報を有するユーザのユーザアカウントを、ユーザ情報属性が付加されたユーザ情報の中から取り出す。
- [0385] このように、検証ポリシー生成部1407は、移動元や移動先として属性情報を用いて指定されたユーザを、ステップS705またはステップS706で取り出したユーザアカウントに置き換えることにより、アクセスポリシーを変換する。この処理は、図22に示すステップS605やステップS607で行われる。

- [0386] 図89に示すフローチャートは、移動元や移動先としてファイルが属性情報を用いて指定されているときに、そのファイルから変換されるファイル名を検索する動作を示している。この動作は、上述した図22でのステップS607の処理に相当する。
- [0387] まず、検証ポリシー生成部1407は、ステップS711において、アクセスポリシーのファイル指定にドメイン指定があるか否かを判定する。すなわち、検証ポリシー生成部1407は、ファイルを表わすアクセスポリシー内の「Src」エレメントまたは「Dst」エレメントが「Domain」エレメントを含んでいるか否かを判定する。なお、「Src」エレメントまたは「Dst」エレメント内の「Domain」エレメントは、上述したようにドメイン選択欄2303やドメイン選択欄2403においてドメインが指定された場合に、アクセスポリシー生成部によって生成されている。
- [0388] ファイルを表わすアクセスポリシー内の「Src」エレメントまたは「Dst」エレメントが「Domain」エレメントを含んでいると判定した場合、検証ポリシー生成部1407は、ステップS711において、ドメインの指定がネットワーク構成情報に付加された属性情報である「segment」エレメントのname属性(図78参照)を利用して行われたか否かを判定する。「segment」エレメントのname属性を利用してドメイン指定が行われた場合というのは、アクセスポリシー生成部1405が、ネットワーク構成情報に付加された属性情報である「segment」エレメントのname属性を選択肢としてドメイン選択肢表示欄2307(図85参照)やドメイン選択肢表示欄2407(図86参照)を表示し、その選択肢の中からドメインが指定された場合のことである。
- [0389] 「segment」エレメントのname属性を利用してドメイン指定が行われたとステップS712では、検証ポリシー生成部1407は、ステップS713において、ネットワーク構成情報属性が付加されたシステム構成情報すなわちネットワーク構成情報(図78参照)から、アクセスポリシー作成時にドメインとして指定されたセグメントに含まれる全てのホストのIPアドレスを検索する。これに対し、「segment」エレメントのname属性を利用せずにドメイン指定が行われたと判定した場合には、検証ポリシー生成部1407は、ステップS714において、アクセスポリシー作成時にドメインとして指定されたホストのIPアドレスを、ネットワーク構成情報属性が付加されたシステム構成情報すなわちネットワーク構成情報から検索する。ステップS713, S714の後、ステップS715に移

行する。

- [0390] ステップS715において、検証ポリシー生成部1407は、以下のようにしてファイル名を取り出す。検証ポリシー生成部1407は、ステップS713またはステップS714で検索したIPアドレスを属性として有するホストを、ファイル情報属性が付加されたファイル情報(図81参照)の中から特定する。そして、そのホストに含まれるファイルのファイル名のうち、アクセスポリシー作成時に移動元選択欄2302(図85参照)または移動先選択欄2402(図86参照)で指定された属性情報を有するファイルのファイル名を取り出す。
- [0391] ステップS711において、ファイルを表わすアクセスポリシー内の「Src」元素または「Dst」元素が「Domain」元素を含んでいないと判定した場合、検証ポリシー生成部1407は、ステップS716において、アクセスポリシー作成時に移動元選択欄2302または移動先選択欄2402で指定された属性情報を有するファイルのファイル名を、ファイル情報属性が付加されたファイル情報に含まれる全ファイルのファイル名の中から取り出す。
- [0392] このように、検証ポリシー生成部1407は、移動元や移動先として属性情報を用いて指定されたファイルを、ステップS715またはステップS716で取り出したファイル名に置き換えることにより、アクセスポリシーを変換する。この処理は、図22に示すステップS610で行われる。
- [0393] 図90に示すフローチャートは、移動経路としてサービスが属性を用いて指定されているときに、そのサービスから変換されるIPアドレスやポート番号を検索する動作を示している。この動作は、上述した図22でのステップS609の処理に相当する。
- [0394] まず、検証ポリシー生成部1407は、ステップS721において、移動経路の指定が属性情報を用いて行われたか否かを判定する。例えば、図86に例示するように、アクセスポリシー生成部1405が「暗号化の有無」や「認証の有無」というサービス属性によって移動経路を指定する指定欄2502を表示し、その指定欄2502において移動経路が指定されたか否かを判定する。移動経路の指定が属性情報を用いて行われていなければ処理を終了する。移動経路の指定が属性情報を用いて行われている場合には、検証ポリシー生成部1407は、ステップS722において、移動経路の指定

に用いられた属性情報をもつIPアドレスまたはポート番号を、サービス情報属性が付加されたシステム構成情報すなわちサービス情報(図79参照)から取り出す。

[0395] その後、検証ポリシー生成部1407は、移動経路として属性を用いて指定されたサービスを、ステップS722で取り出したIPアドレスまたはポート番号に置き換えることによって、アクセスポリシーを変換する。この処理は、上述の図22に示すステップS610で行なわれる。

[0396] 次に、具体例を用いて、図85、図86及び図87に例示する指定内容に基づいて作成されたアクセスポリシーを検証ポリシーに変換する手順を説明する。図85に示される指定内容では、移動元として、「DMZ」セグメントの「個人情報」ファイルが選択されている。そこで、検証ポリシー生成部1407は、属性情報格納部に格納されたネットワーク構成情報属性(図78参照)から、name属性が“DMZ”となっている「segment」エレメントを取り出す。取り出した「segment」エレメントに含まれる情報が「DMZ」セグメントに関わる情報である。続いて、検証ポリシー生成部1407は、取り出した「segment」エレメントに含まれるIPアドレス一覧を取り出す。本例では、「12. 34. 56. 1」、「10. 56. 1. 1」、「10. 56. 2. 1」、「10. 56. 1. 10」、「10. 56. 1. 20」というIPアドレスが取り出される。

[0397] 次に、検証ポリシー生成部1407は、取り出したIPアドレスを持つホストに含まれる「個人情報」ファイルを、ファイル情報属性(図81参照)から取り出す。つまり、取り出したIPアドレスをaddress属性として有する「host」エレメントに含まれるファイルであって、categoryタグとともに「個人情報(図85で指定された属性情報)」が記述されているファイルを取り出す。本例では、IPアドレスが「10. 56. 1. 10」のホストに含まれる「/passwd/顧客ID管理情報. xml」と、IPアドレスが「10. 56. 1. 20」のホストに含まれる「/secret/4月顧客情報. xml」及び「/secret/アンケート. xml」というファイル名の情報を取り出す。

[0398] 検証ポリシー生成部1407は、図87に示す画面における移動経路の入力から途中経路を検索する。図87に例示する画面では、暗号で保護されていない経路が指定されている。そこで、検証ポリシー生成部1407は、サービス情報属性から、暗号化のないサービスのポート番号を検索する。図79に例示するサービス情報属性では、暗

号化のない経路、すなわち「encryption=OFF」となっているサービスは、「http」、「samba」及び「ftp」であり、これらのサービスのポート番号は、それぞれ「80番ポート」、「139番ポート」、「21番ポート」である。

[0399] 検証ポリシー生成部1407は、移動先を検索する。図86に例示する画面では、「LAN」セグメント内の「営業」ユーザが移動先として指定されている。移動元検索と同様に、検証ポリシー生成部1407は、まずネットワーク構成情報属性から「LAN」セグメントに所属するホストのIPアドレスを検索する。すなわち、name属性が“LAN”となっている「segment」エレメントに含まれるIPアドレスを検索する。この結果、「10. 56. 2. 10」というIPアドレスが検索される。そして、検証ポリシー生成部1407は、IPアドレス「10. 56. 2. 10」に対応する「営業」ユーザのIDをユーザ情報属性が付加されたユーザ情報(図80参照)から検索する。この結果、「suzuki」というIDが検索される。

[0400] 次に、検証ポリシー生成部1407は、これまでに検索した移動元、移動経路、移動先をまとめて検証ポリシーとする。この結果、ファイル「／／10. 56. 1. 10/passwd／顧客ID管理情報. xml」と「／／10. 56. 1. 20/secret／4月顧客情報. xml」と「／／10. 56. 1. 20/secret／アンケート. xml」とが、暗号化されていない経路であるポート番号「80」とポート番号「139」を通過して、「10. 56. 2. 10」のユーザ「suzuki」に到達してはいけないという経路が得られる。これを例1に示した正規表現を用いる検証ポリシーで表現すると、「[F(“／passwd／顧客ID管理情報. xml”@10. 56. 1. 10)F(“／secret／4月顧客情報. xml”@10. 56. 1. 20)F(“／secret／アンケート. xml”@10. 56. 1. 20)]. *[N(0. 0. 0. 0ー, 21, 0. 0. 0. 0ー, 0ー)N(0. 0. 0. 0ー, 80, 0. 0. 0. 0ー, 0ー) N(0. 0. 0. 0ー, 139, 0. 0. 0. 0ー, 0ー)]. *U(suzuki@10. 56. 2. 10)」となる。

[0401] 以上のように、システム構成情報に付加した属性情報を利用することで、たとえ複雑なシステム構成の検証でも、複雑な検証ポリシーを手で書くことなく、平易なアクセスポリシーの入力から、検証ポリシーを生成することができる。これにより、検証対象システムに対する特別な知識を持たないコンテンツの管理者や一般ユーザであっても、自らのコンテンツが適切に保護されているか、適切なアクセス権が与えられている

かを検証するためのアクセスポリシーを作成し、検証ポリシーを生成し、検証部1510 (図23参照)の入力とすることで、不適切な設定を見つけることができるようになる。

[0402] 上述したように、セキュリティ検証用データ作成システム及びセキュリティ検証システムは、いずれも、それらのシステムの各機能を発現するためのソフトウェアプログラムをコンピュータに読み込ませ、そのプログラムを実行させることによっても実現できるものである。したがって、本発明の範疇には、そのようなプログラム、そのようなプログラムを有するプログラムプロダクト、及びそのようなプログラムを格納した記録媒体も含まれるものである。

請求の範囲

- [1] 検証対象システムにおけるセキュリティ設定の複合的な誤りを示す不適設定の有無を検証するセキュリティ検証システムへの入力データである検証ポリシーを生成するセキュリティ検証用データ生成方法であって、
- 前記検証対象システムにおけるネットワーク、アプリケーション、ファイル、サービス及びユーザのうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むシステム構成情報を収集する段階と、
- 前記システム構成情報に付加される属性情報であって、ネットワーク、アプリケーション、ファイル、サービス及びユーザの属性のいずれか一つまたはそれらの組み合わせた内容を示す属性情報を受け取る段階と、
- 不適切なデータ移動経路におけるデータの移動元、移動先、及び移動経路のうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むアクセスポリシーを、前記属性情報を用いて生成する段階と、
- 前記アクセスポリシーと、前記システム構成情報及び属性情報とに基づいて、不適切なデータ移動経路を表わす検証ポリシーを生成する段階と、
- を有する方法。
- [2] 前記検証対象システムにおけるデータ移動を表わすデータ移動経路と前記検証ポリシーとを用いて、前記検証対象システムにおけるデータ移動経路が適切であるか否かを検証する段階をさらに有する、請求項1に記載の方法。
- [3] 検証対象システムにおけるセキュリティ設定の複合的な誤りを示す不適設定の有無を検証するセキュリティ検証システムへの入力データである検証ポリシーを生成するセキュリティ検証用データ生成システムであって、
- 前記検証対象システムにおけるネットワーク、アプリケーション、ファイル、サービス及びユーザのうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むシステム構成情報を収集するシステム構成情報収集手段と、
- 前記システム構成情報に付加される属性情報であって、ネットワーク、アプリケーション、ファイル、サービス及びユーザの属性のいずれか一つまたはそれらの組み合わせた内容を示す属性情報が入力される属性情報入力手段と、

不適切なデータ移動経路におけるデータの移動元、移動先、及び移動経路のうちの少なくともいずれか一つまたはその組み合わせからなる情報を含むアクセスポリシーを、前記属性情報を用いて生成するアクセスポリシー生成手段と、

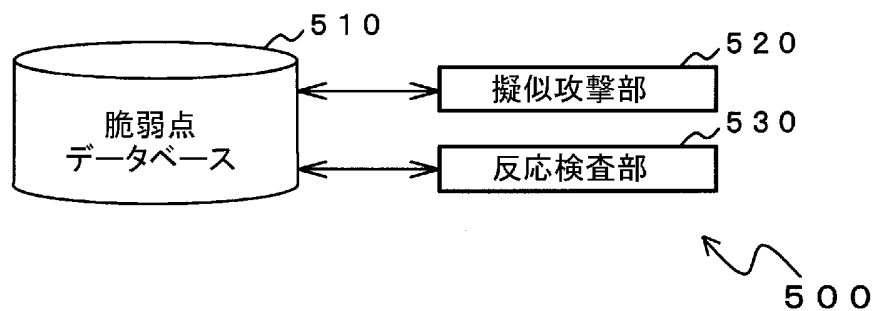
前記アクセスポリシー生成手段によって生成されたアクセスポリシーと、前記システム構成情報及び属性情報とに基づいて、不適切なデータ移動経路を表わす検証ポリシーを生成する検証ポリシー生成手段と、

を有するシステム。

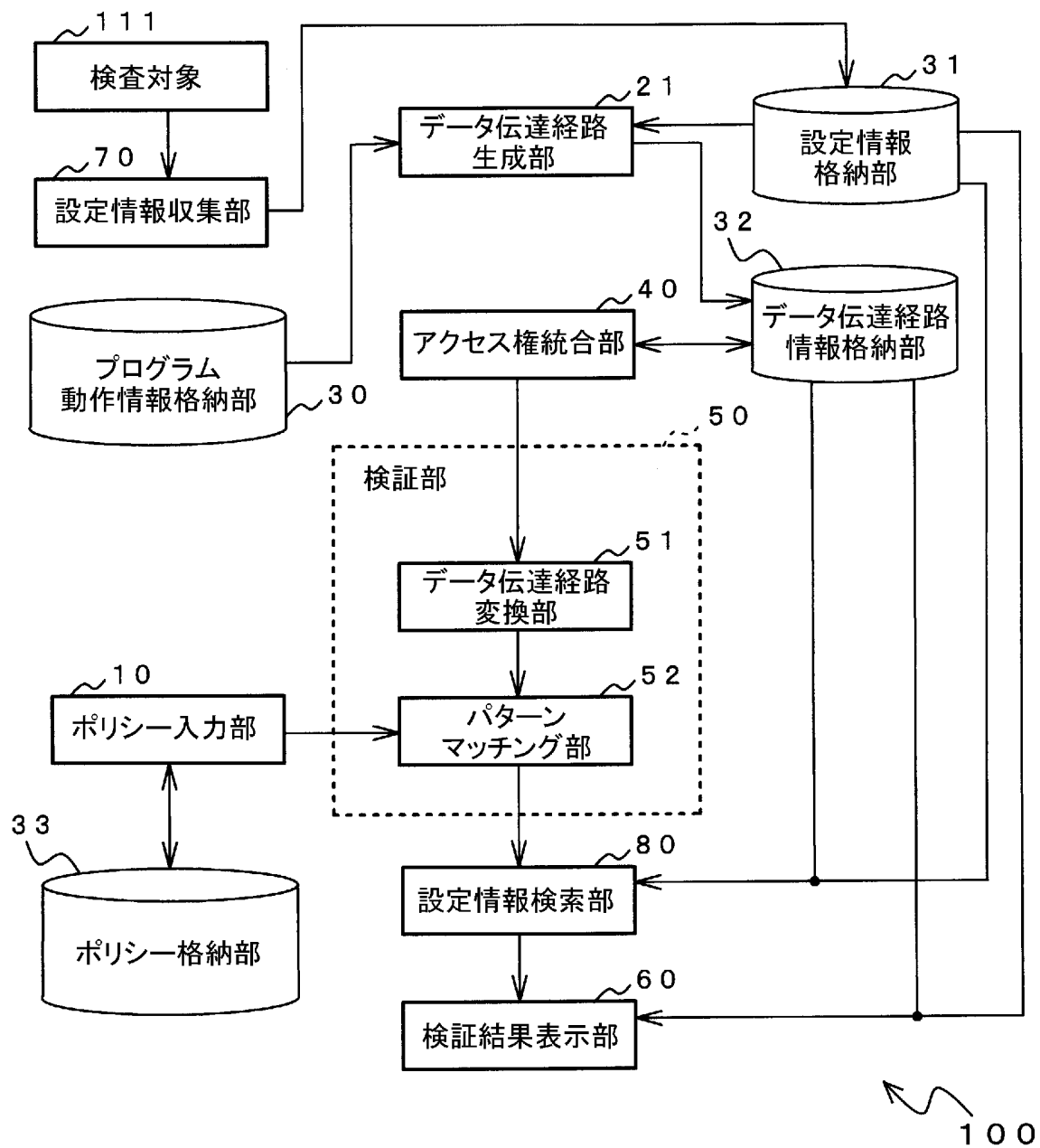
- [4] 前記属性情報入力手段は、前記システム構成情報収集手段が収集したシステム構成情報を表示して、前記属性情報の入力をオペレータに促す、請求項3に記載のシステム。
- [5] 前記アクセスポリシー生成手段は、前記属性情報を選択肢として表示してオペレータに前記属性情報の選択を促し、選択された属性情報によって前記移動元、前記移動先、または前記移動経路を指定する、請求項3に記載のシステム。
- [6] 前記アクセスポリシー生成手段は、前記属性情報を選択肢として表示してオペレータに前記属性情報の選択を促し、選択された属性情報によって前記移動元、前記移動先、または前記移動経路を指定する、請求項4に記載のシステム。
- [7] 前記検証ポリシー生成手段は、前記属性情報を用いて指定されたアクセスポリシー内の移動元、移動先、または移動経路の情報を、前記システム構成情報または前記属性情報に含まれる情報に置き換えることにより検証ポリシーを生成する、請求項3に記載のシステム。
- [8] 前記検証ポリシー生成手段は、前記属性情報を用いて指定されたアクセスポリシー内の移動元、移動先、または移動経路の情報を、前記システム構成情報または前記属性情報に含まれる情報に置き換えることにより検証ポリシーを生成する、請求項4に記載のシステム。
- [9] 前記検証ポリシー生成手段は、前記属性情報を用いて指定されたアクセスポリシー内の移動元、移動先、または移動経路の情報を、前記システム構成情報または前記属性情報に含まれる情報に置き換えることにより検証ポリシーを生成する、請求項5に記載のシステム。

- [10] 前記検証ポリシー生成手段は、前記属性情報を用いて指定されたアクセスポリシー内の移動元、移動先、または移動経路の情報を、前記システム構成情報または前記属性情報に含まれる情報に置き換えることにより検証ポリシーを生成する、請求項6に記載のシステム。
- [11] 前記検証対象システムにおけるデータ移動を表わすデータ移動経路と前記検証ポリシーとを用いて前記検証対象システムにおけるデータ移動経路が適切であるか否かを検証する検証手段をさらに備える、請求項3乃至10のいずれか1項に記載のシステム。
- [12] 検証対象システムにおけるセキュリティ設定の複合的な誤りを示す不適設定の有無を検証するセキュリティ検証システムへの入力データである検証ポリシーを生成するコンピュータに搭載されるセキュリティ検証用データ生成プログラムであって、
前記コンピュータに、
前記検証対象システムにおけるネットワーク、アプリケーション、ファイル、サービス及びユーザのうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むシステム構成情報を収集する処理、
前記システム構成情報に付加される属性情報であって、ネットワーク、アプリケーション、ファイル、サービス及びユーザの属性のいずれか一つまたはそれらの組み合わせた内容を示す属性情報を受け取る処理、
不適切なデータ移動経路におけるデータの移動元、移動先、及び移動経路のうちの少なくともいずれか一つまたはそれらの組み合わせからなる情報を含むアクセスポリシーを、前記属性情報を用いて生成する処理、及び、
前記アクセスポリシーと、前記システム構成情報及び属性情報とに基づいて、不適切なデータ移動経路を表わす検証ポリシーを生成する処理
を実行させるプログラム。
- [13] 前記コンピュータに、さらに、前記検証対象システムにおけるデータ移動を表わすデータ移動経路と前記検証ポリシーとを用いて、前記検証対象システムにおけるデータ移動経路が適切であるか否かを検証する処理を実行させる、請求項12に記載のプログラム。

[図1]



[図2]



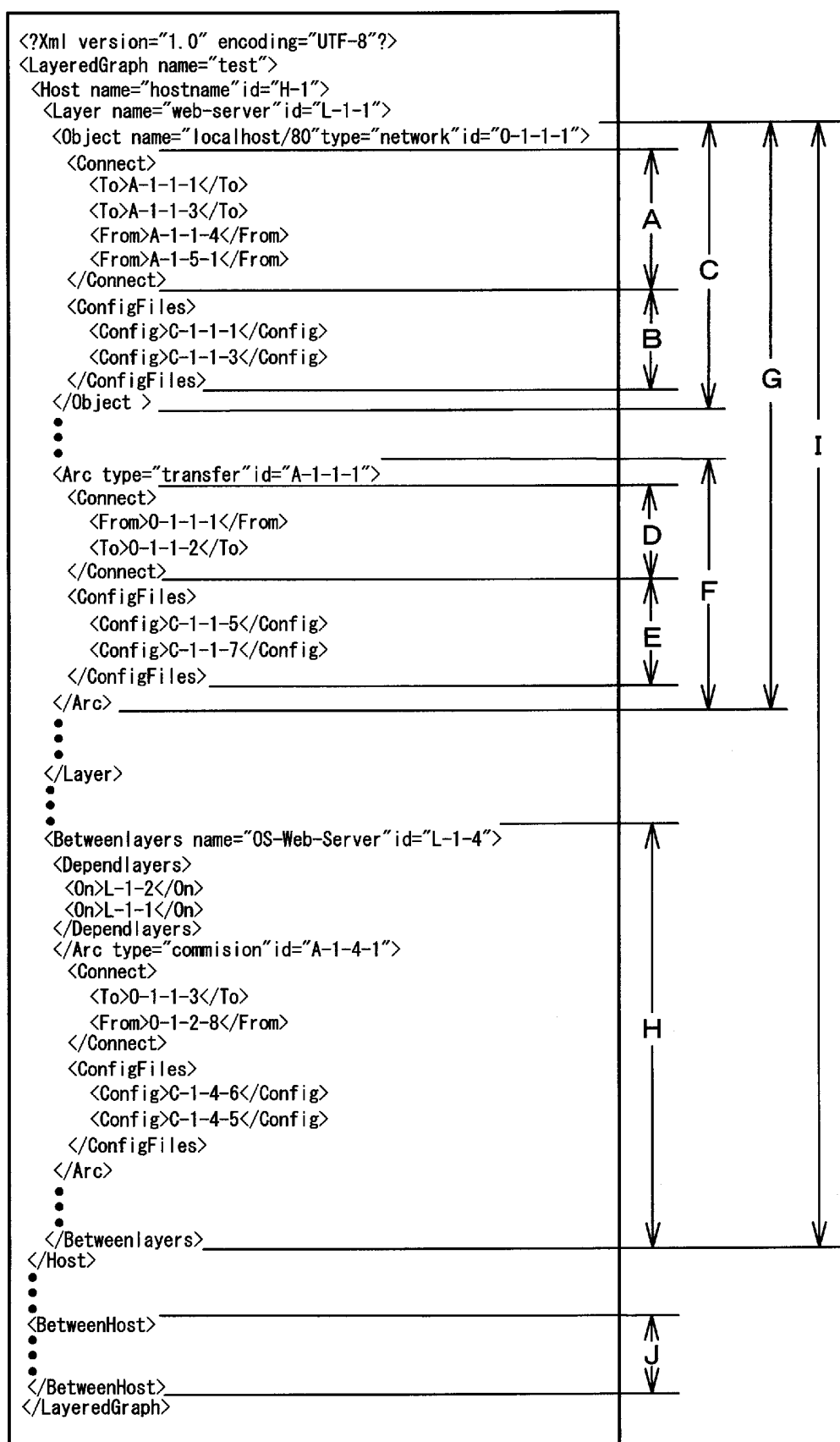
[図3]

設定情報ID	セキュリティ設定情報		
	対象アプリケーション	設定情報ファイル名	セキュリティ単位情報
C-1-1-1	ウェブサーバ	サーバ設定ファイル	ネットワーク構成情報
C-1-1-2	OS	ユーザ設定ファイル	ユーザ情報
-----	-----	-----	-----

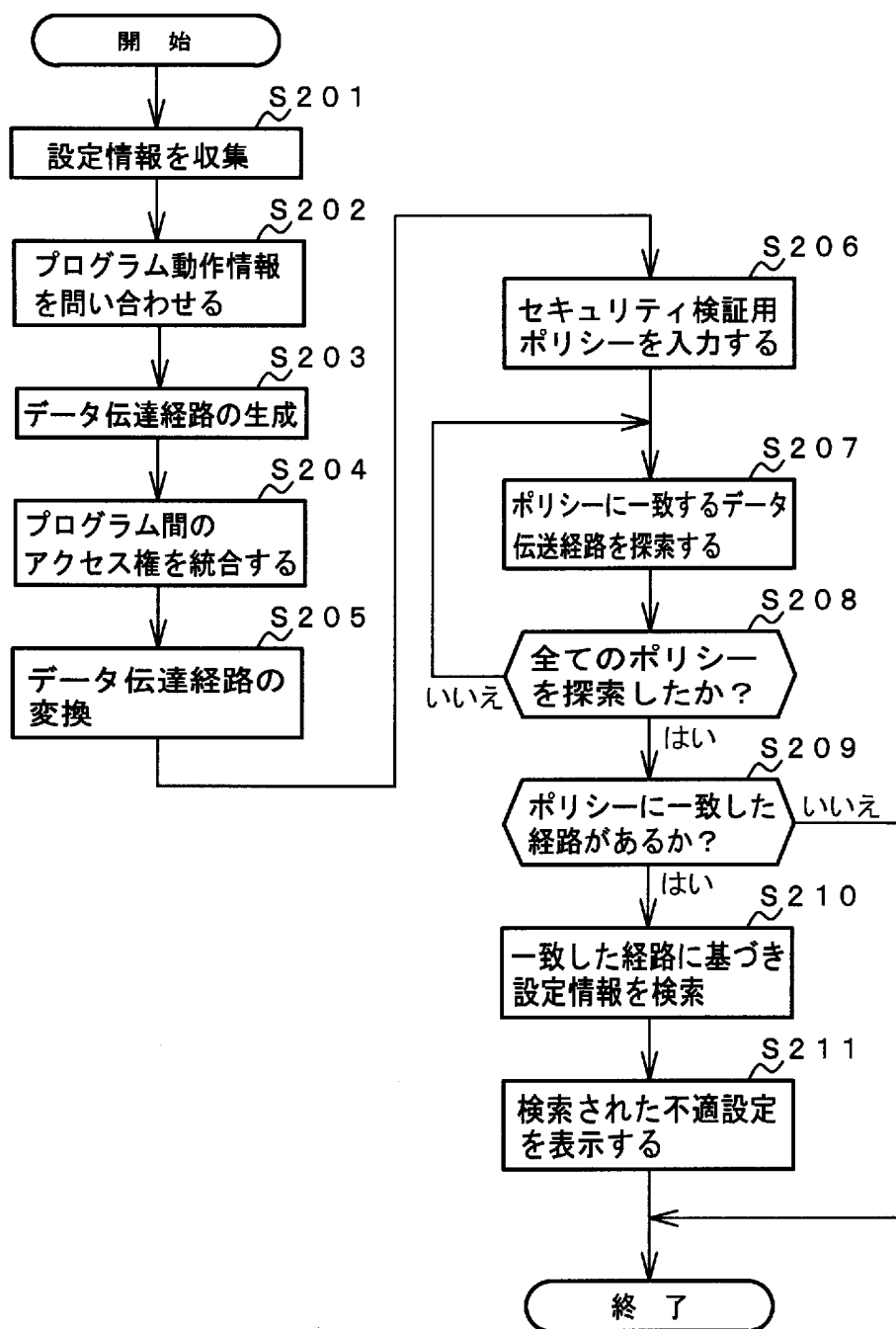
[図4]

セキュリティ設定情報			モデル上に作成するノード またはアークの種類
対象アプリケーション	設定情報ファイル名	セキュリティ単位情報	
OS	OSの内部情報	OSがインストールされているという情報	OSに関するレイヤを作成する
OS	ファイル設定ファイル	ファイル構造を表す情報	ファイルノードを作成する。 別名定義を表すアークを作成する。
OS	ユーザ設定ファイル	ユーザを表す情報	ユーザノードを作成する
OS	グループ設定ファイル	グループを表す情報	グループノード
OS	グループ設定ファイル	グループに所属するユーザを特定する情報	グループノードとそのグループに所属するユーザノードとの間に所属関係を表すアークを作成する
OS	ファイル設定ファイル	ファイルアクセス権の情報	ファイルノードとユーザ(グループ)ノードの間にデータ移動を表すアークを作成する
-----	-----	-----	-----
ウェブサーバ	OSの内部情報	ウェブサーバがインストールされているという情報	ウェブサーバに関するレイヤを作成する
ウェブサーバ	サーバ設定ファイル	ユーザ情報	ユーザノード
ウェブサーバ	サーバ設定ファイル	ウェブサーバが利用するネットワークの情報	ネットワークノードを作成する
ウェブサーバ	サーバ設定ファイル	サーバの実行ユーザ情報	ユーザノード、権限委譲関係を表すアーク
ウェブサーバ	サーバ設定ファイル	ファイル情報	ファイルノード、別名定義を表すアーク
-----	-----	-----	-----
ウェブクライアント	クライアント設定ファイル	ウェブクライアントがインストールされているという情報	ネットワークノードを作成する
ウェブクライアント	OSの内部情報	ウェブサーバがインストールされているという情報	ウェブサーバのネットワークノードとウェブクライアントのネットワークノードとの間にデータ移動関係を表すアークを作成する
-----	-----	-----	-----

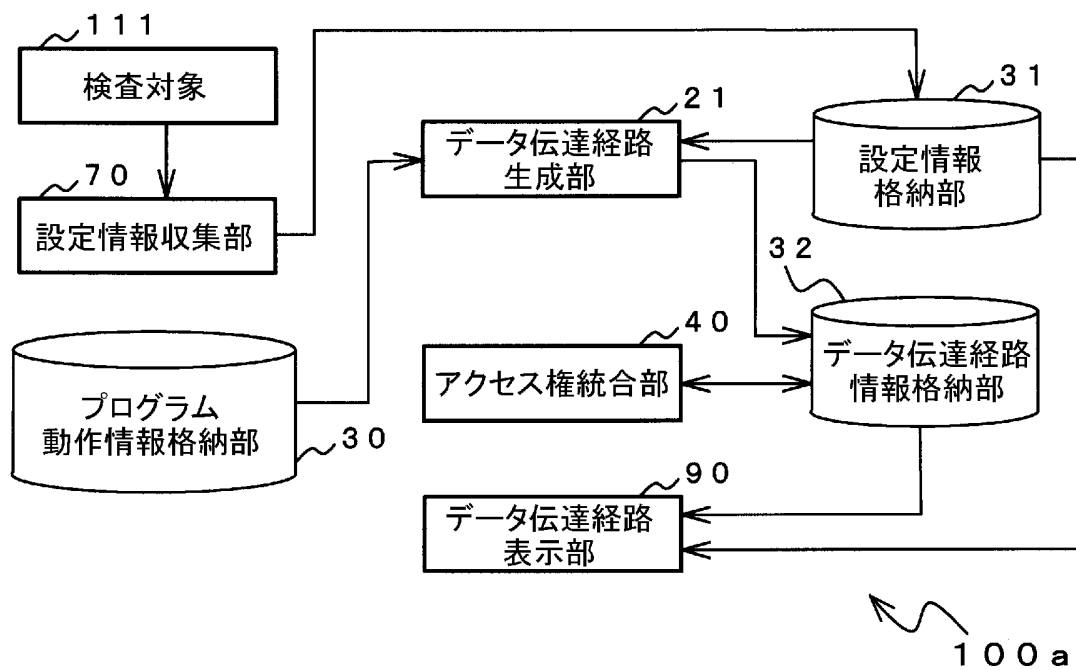
[図5]



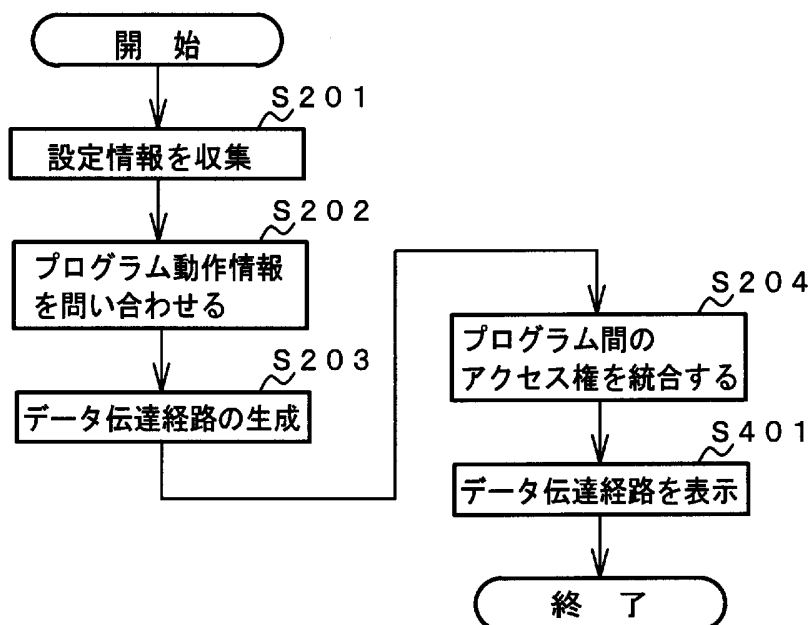
[図6]



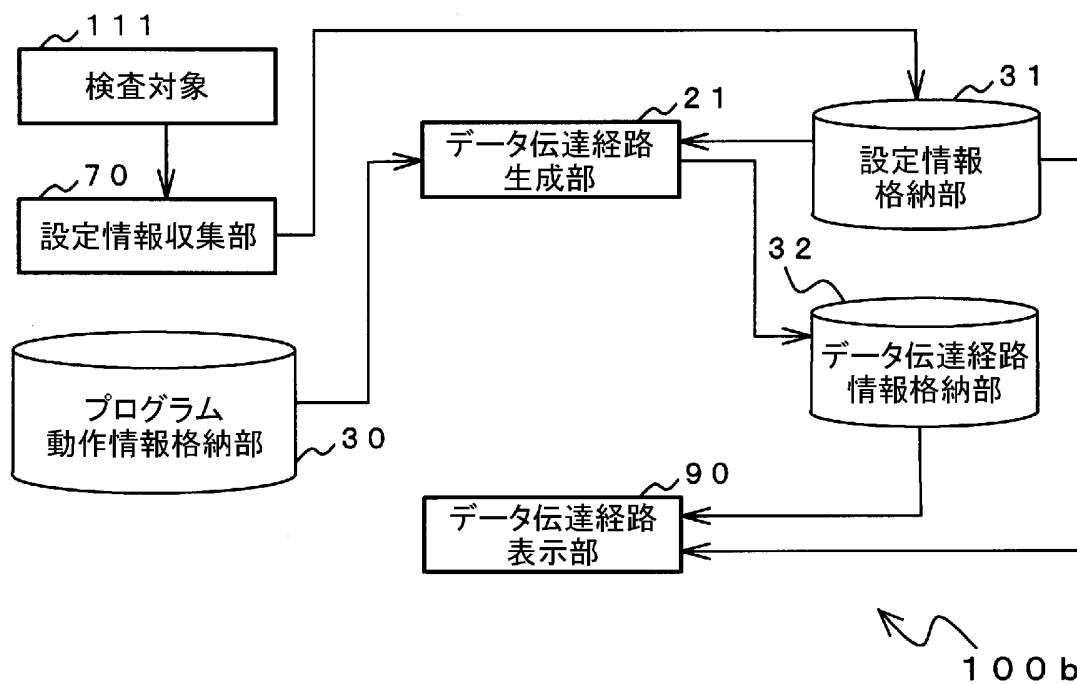
[図7]



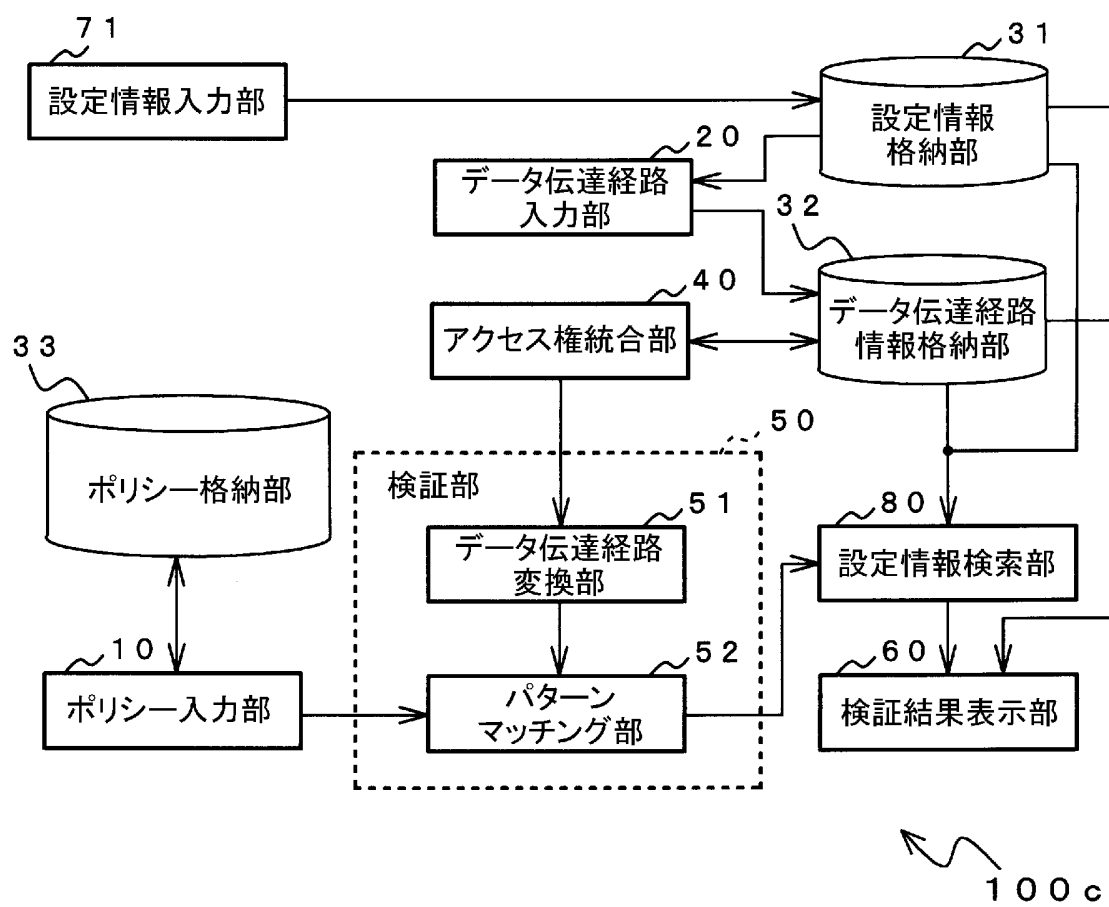
[図8]



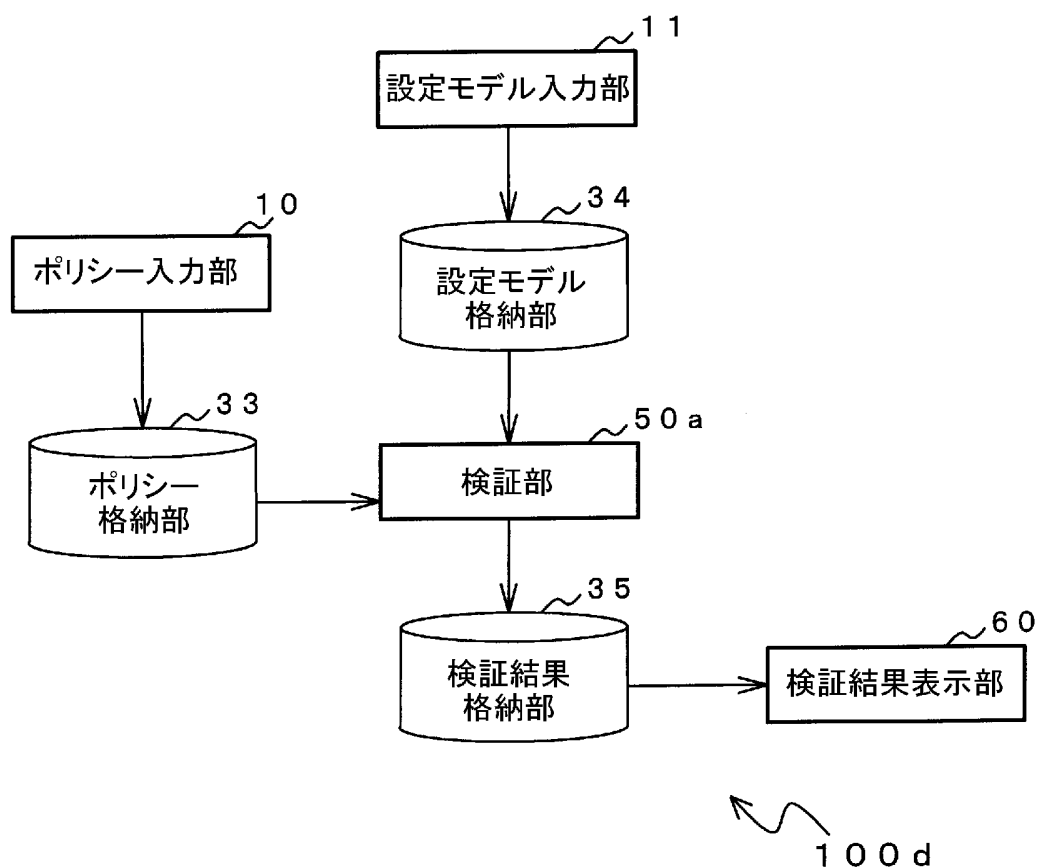
[図9]



[図10]



[図11]

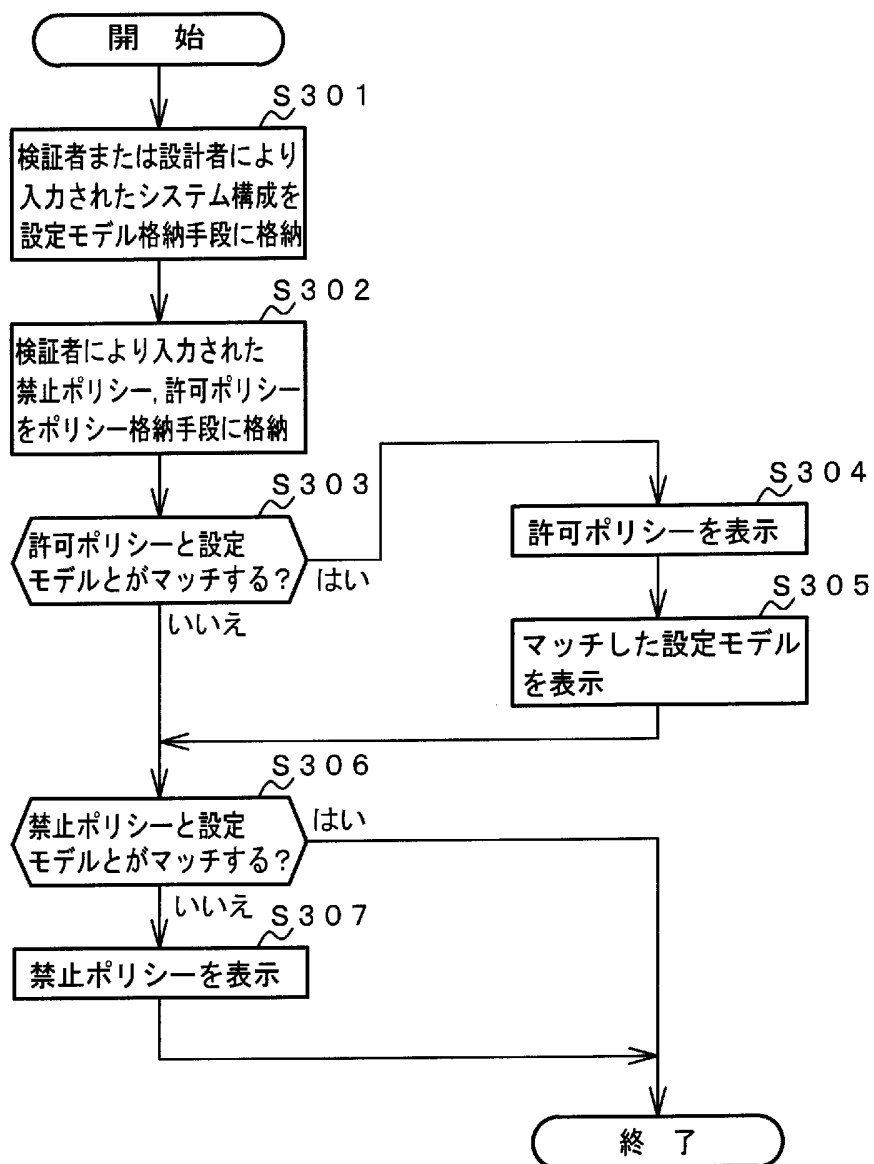


[図12]

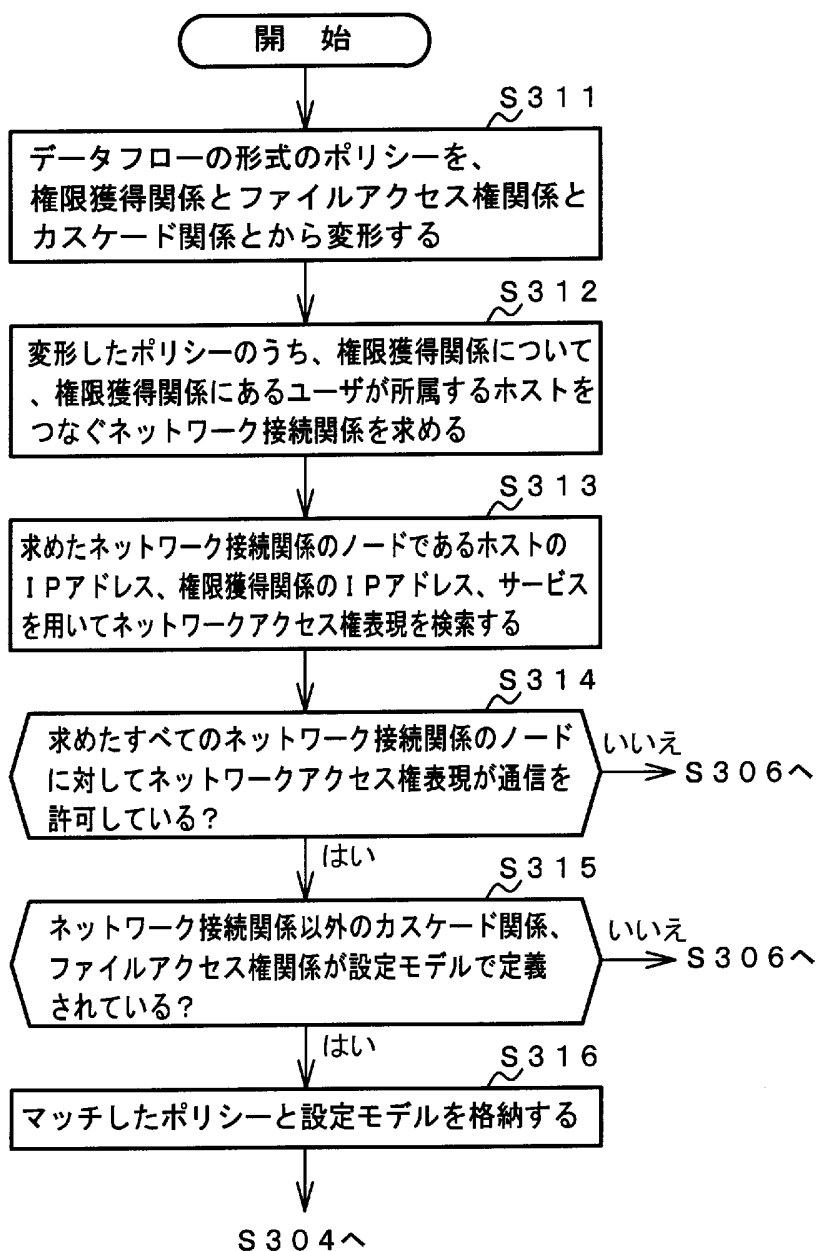
```

<PolicySet>
  <Policy type="deny">
    <Rule>flow(fileA, fileB)</Rule>
    <Description>ファイル「fileA」の内容は、ファイル「fileB」に移動してはならない
  </Description>
</Policy>
</Policy type="allow">
  <Rule>(b(U1)=h1) ∧ acc(u, read, f) ∧ auth(U1, ssh, u) ∧ acc(U1, write, f1)</Rule>
  <Description>ホスト「h」上のユーザ「u」は、ファイル「f」の内容をサービス「ssh」を用いて、ホスト「h1」上の任意のユーザの権限を獲得し、ファイル「f1」に書き込むことができる。
</Description>
</Policy>
</PolicySet>
  
```

[図13]



[図14]

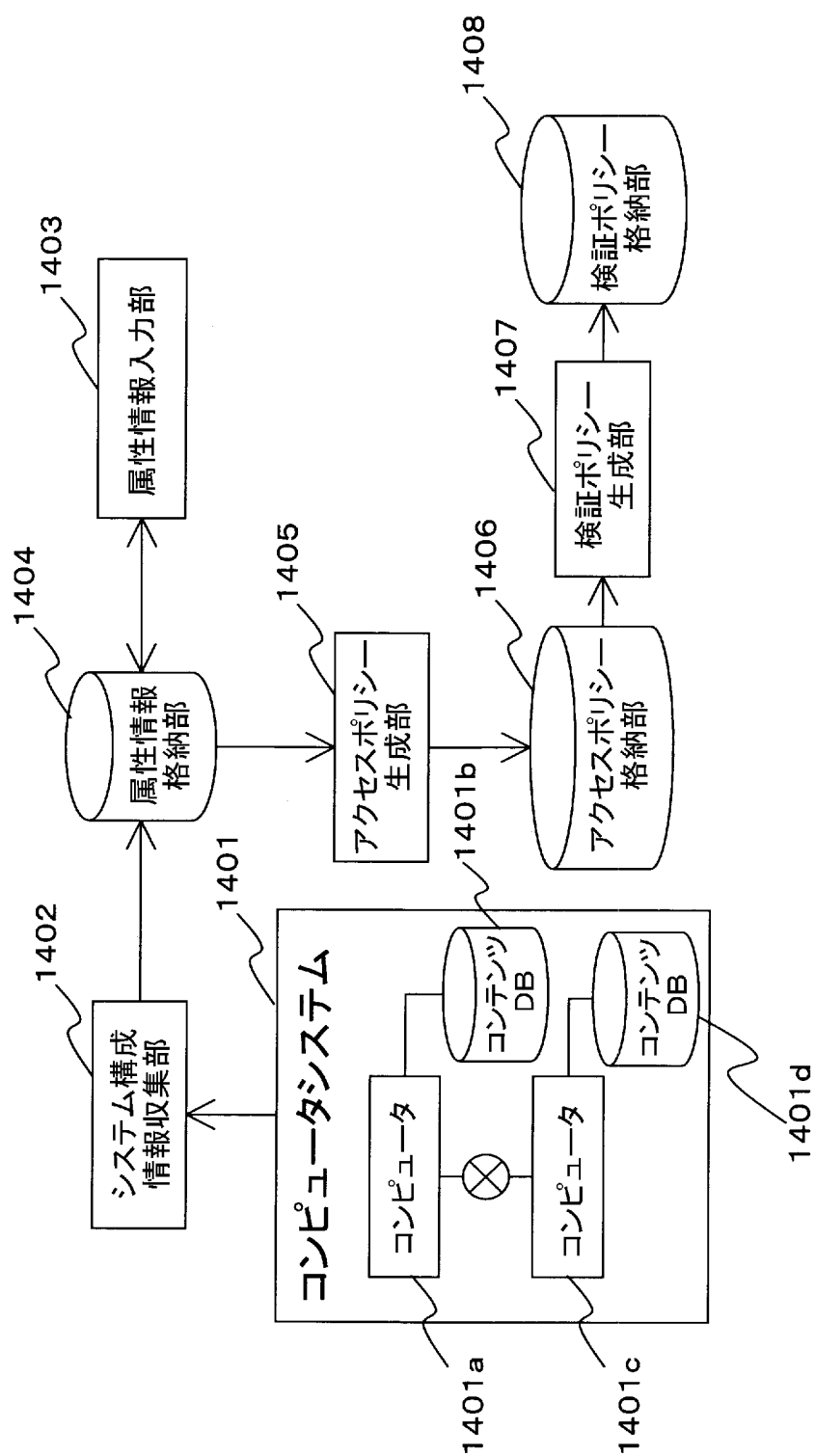


[図15]

$$\text{flow}(F1, F2) \rightarrow \text{flow}(F1, F3) \wedge \text{flow}(F3, F2)$$

$$\text{flow}(F1, F2) \rightarrow \text{acc}(U, \text{read}, F1) \wedge \text{auth}(U3, S1, U) \wedge \text{auth}(U3, S2, U2) \wedge \text{acc}(U2, \text{write}, F2)$$

[図16]



[図17]

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<networksystem>
```

```
<segment name="kansaiken-dmz">
```

```
<host name="fw-1">
```

```
<ip addresss="10.56.191.1" />
```

```
</host>
```

```
<host name="www">
```

```
<ip addresss="10.56.191.10"/>
```

```
</host>
```

```
<host name="file">
```

```
<ip addresss="10.56.191.20"/>
```

```
</host>
```

```
</segment>
```

```
<segment name="kansai-lan">
```

```
<host name="fw-1">
```

```
<ip addresss="10.56.192.1" />
```

```
</host>
```

```
<host name="10.56.192.2"/>
```

```
<host name="10.56.192.3"/>
```

```
<host name="10.56.192.4"/>
```

```
<host name="10.56.192.5"/>
```

```
</segment>
```

```
<segment name="Internet">
```

```
<host name="Internet" />
```

```
<host name="fw-1">
```

```
<ip addresss="1.1.1.1" />
```

```
</host>
```

```
</segment>
```

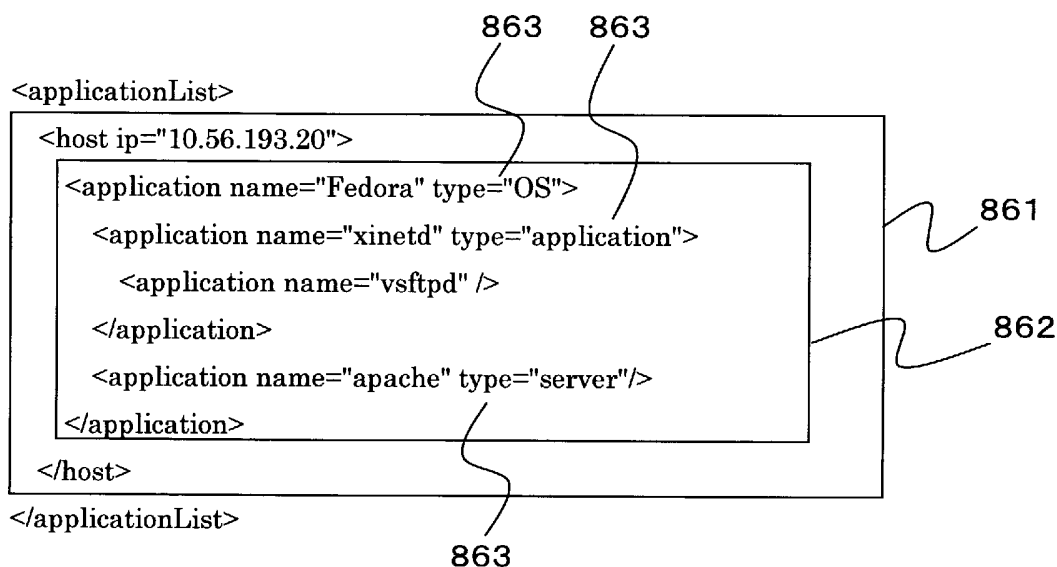
```
</networksystem>
```

852

851

853

[図18]



[図19]

```

-rw-rw-r-- 1 ftp ftp Mar 5 2003 .
-rw-rw-r-- 1 ftp ftp Nov 3 2003 ..
-rw-rw-r-- 1 ftp ftp Mar 2 17:17 paper.txt

```

[図20]

```

<Services>
  <Service name="http" encryption="OFF">
    <port number="80" />
  </Service>
  <Service name="https" encryption="ON">
    <port number="443" />
  </Service>
  <Service name="samba" encryption="OFF">
    <port number="139" />
  </Service>
  <Service name="ftp" encryption="OFF">
    <port number="21">
      <ip address="10.56.1.10" />
    </port>
  </Service>
</Services>

```

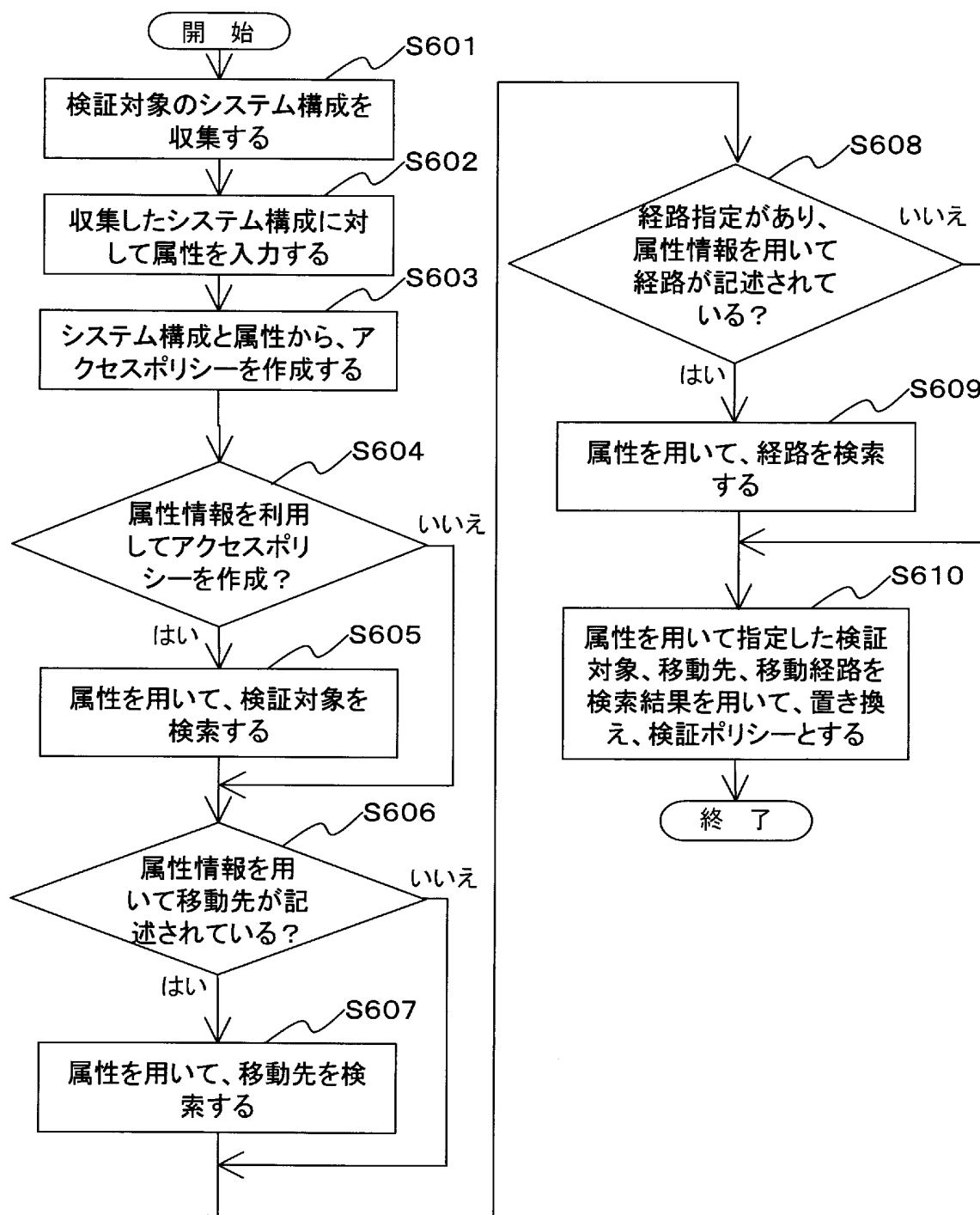
[図21]

```

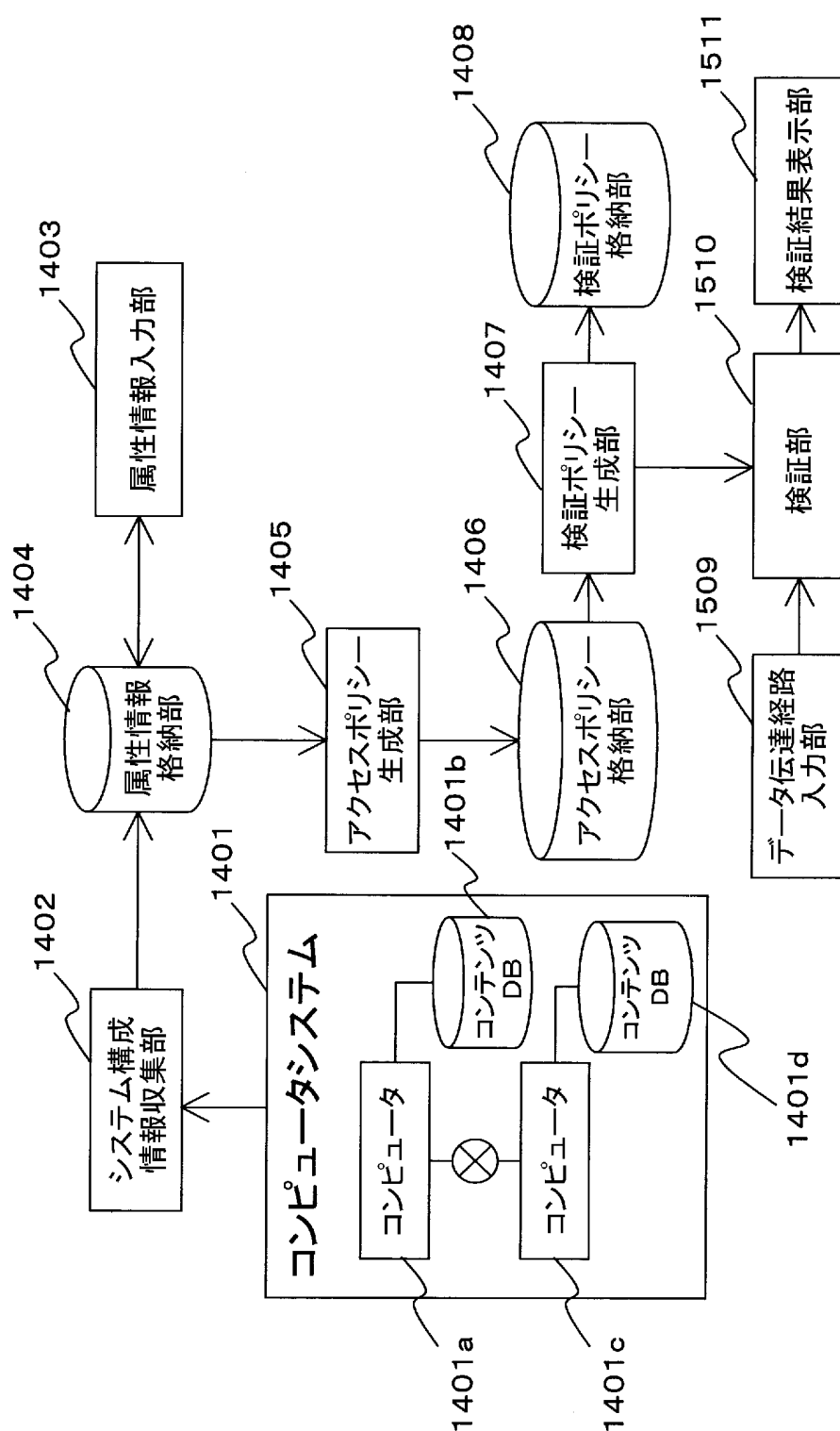
<ID name="tanaka" host="10.56.2.10" application="OS"/>
<ID name="w-tanaka" host="10.56.1.10" application="OS" />
<ID name="s-tanaka" host="10.56.1.20" application="OS" />

```

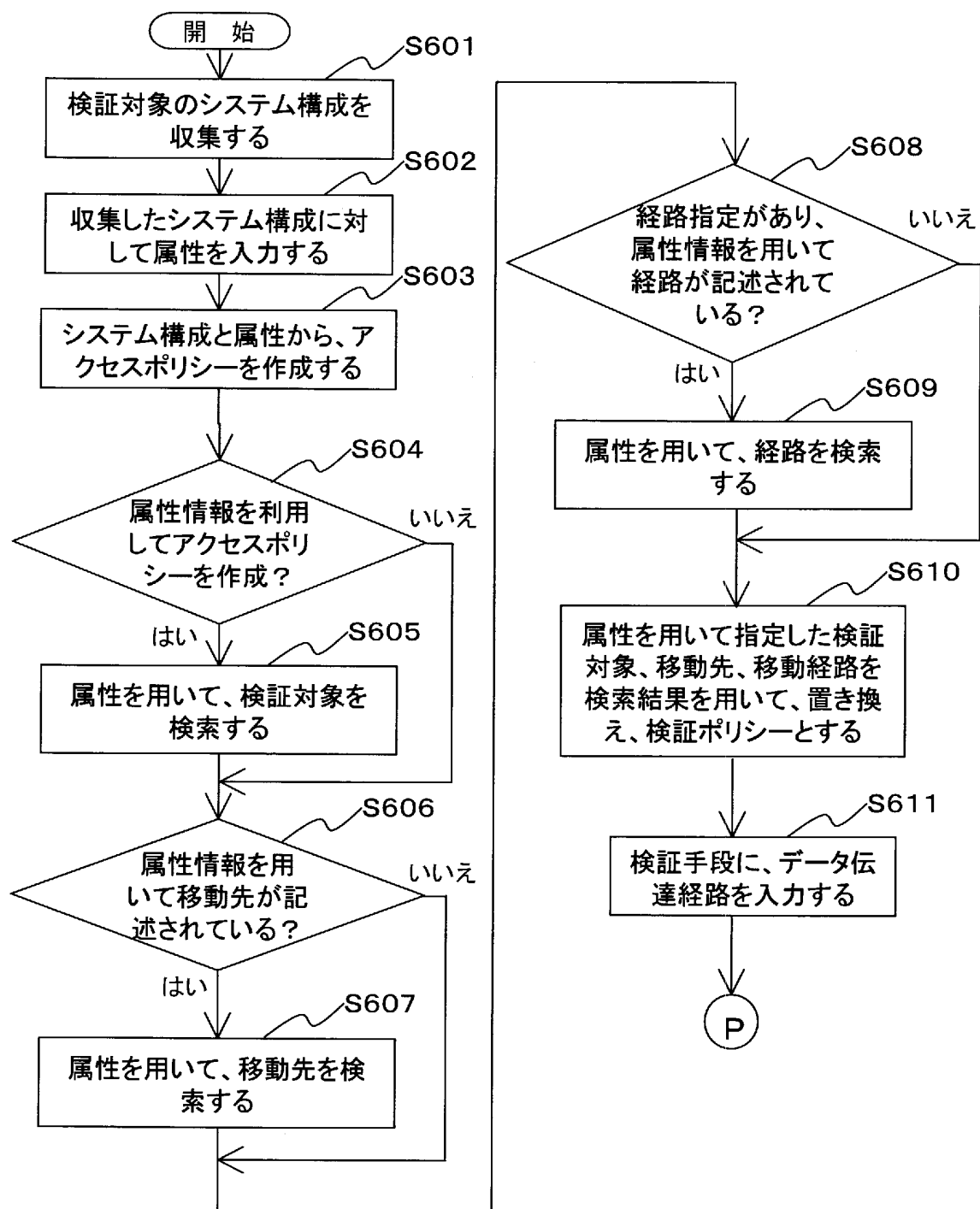
[図22]



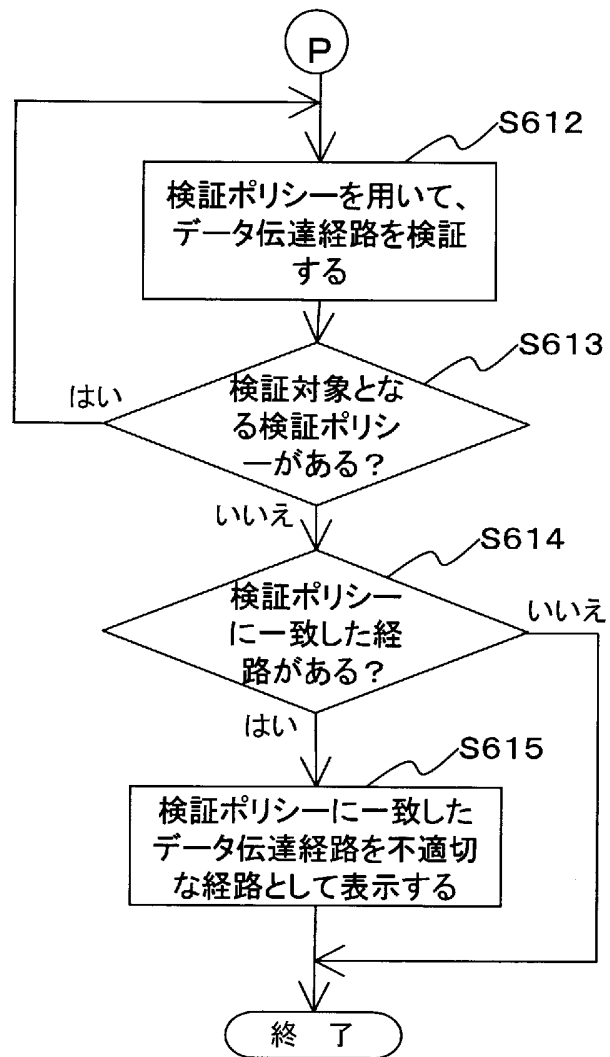
[図23]



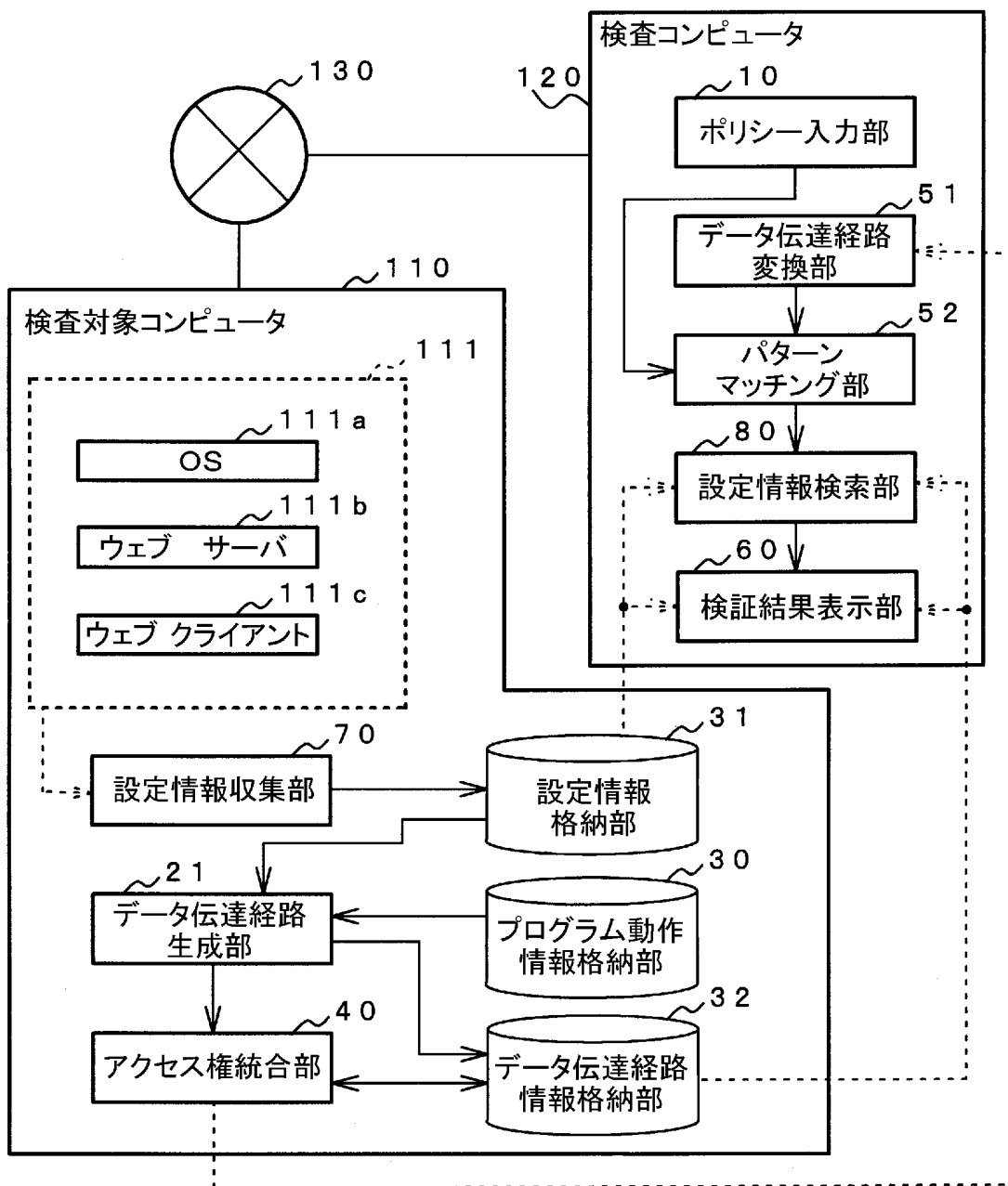
[図24]



[図25]



[図26]



[図27A]

```

apache:x:48:48:Apache:/var/www:/bin/false
a:x:501:501::/home/a:/bin/bash
b:x:502:501::/home/b:/bin/bash
  
```

[図27B]

```

apache:x:48:
a:x:501:
  
```

[図28]

```

drwxr-x--x b a /home/b/
drwxrwxr-x b a /home/b/public/
-rw---xr-- b a /home/b/public/index.html
drwx--xrw b a /home/b/public/s/
drwx--x--x a a /home/a/
-rw----- a a /home/a/notpublic.html
drwx--xrw a a /home/a/public/

```

[図29A]

```

Port 80
User apache
Group apache
UserDir public_html

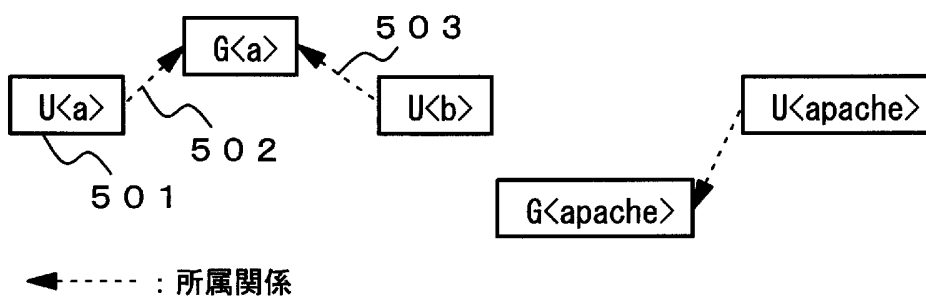
<Directory "/var/www/html/secret/">
    AuthUserFile /var/www/.htpasswd
    AuthGroupFile /dev/null
    AuthName "Test For Basic Auth"
    AuthType Basic
    require valid-user
</Directory>
...

```

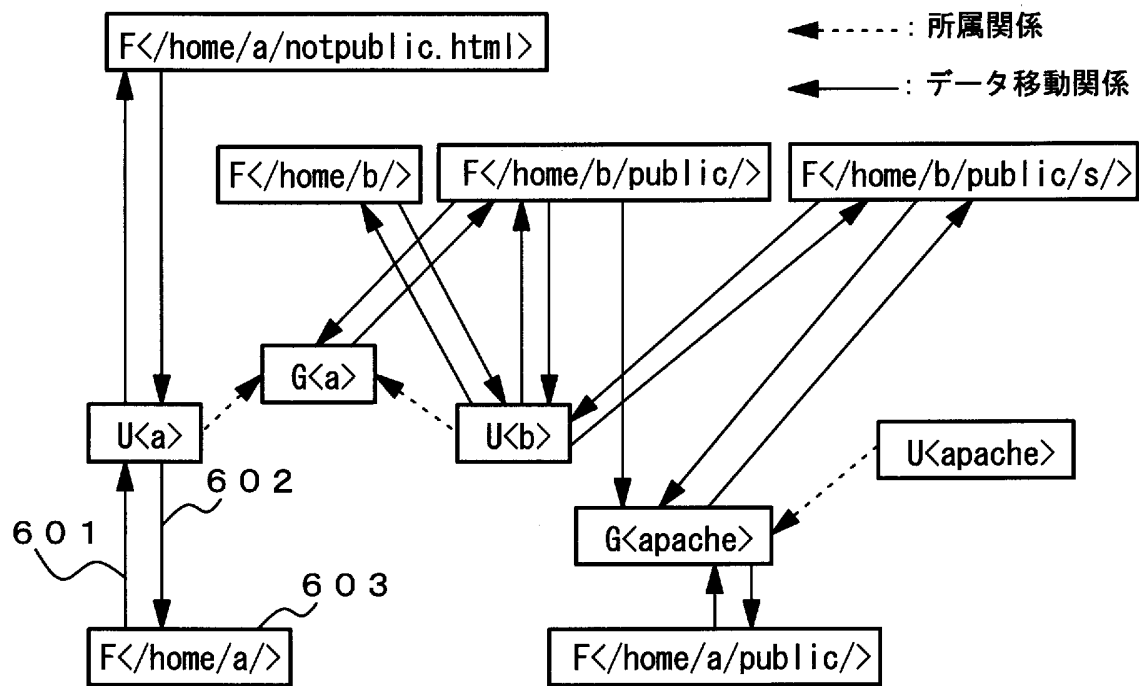
[図29B]

```
user-g: passwd
```

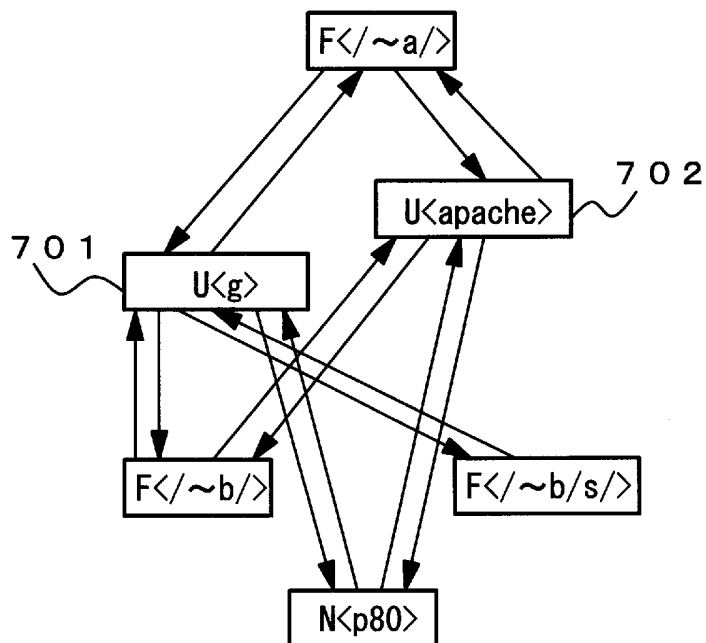
[図30]



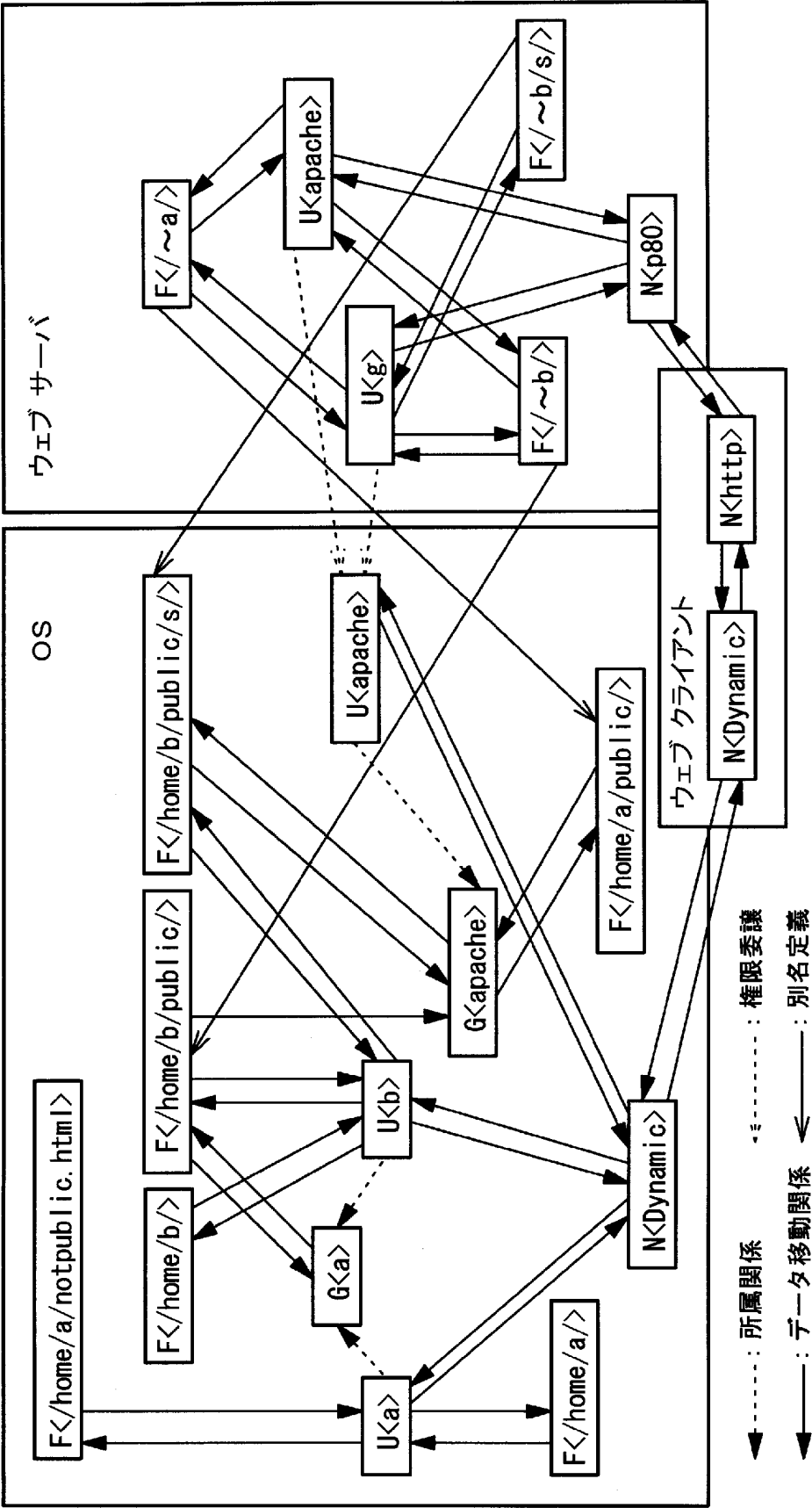
[図31]



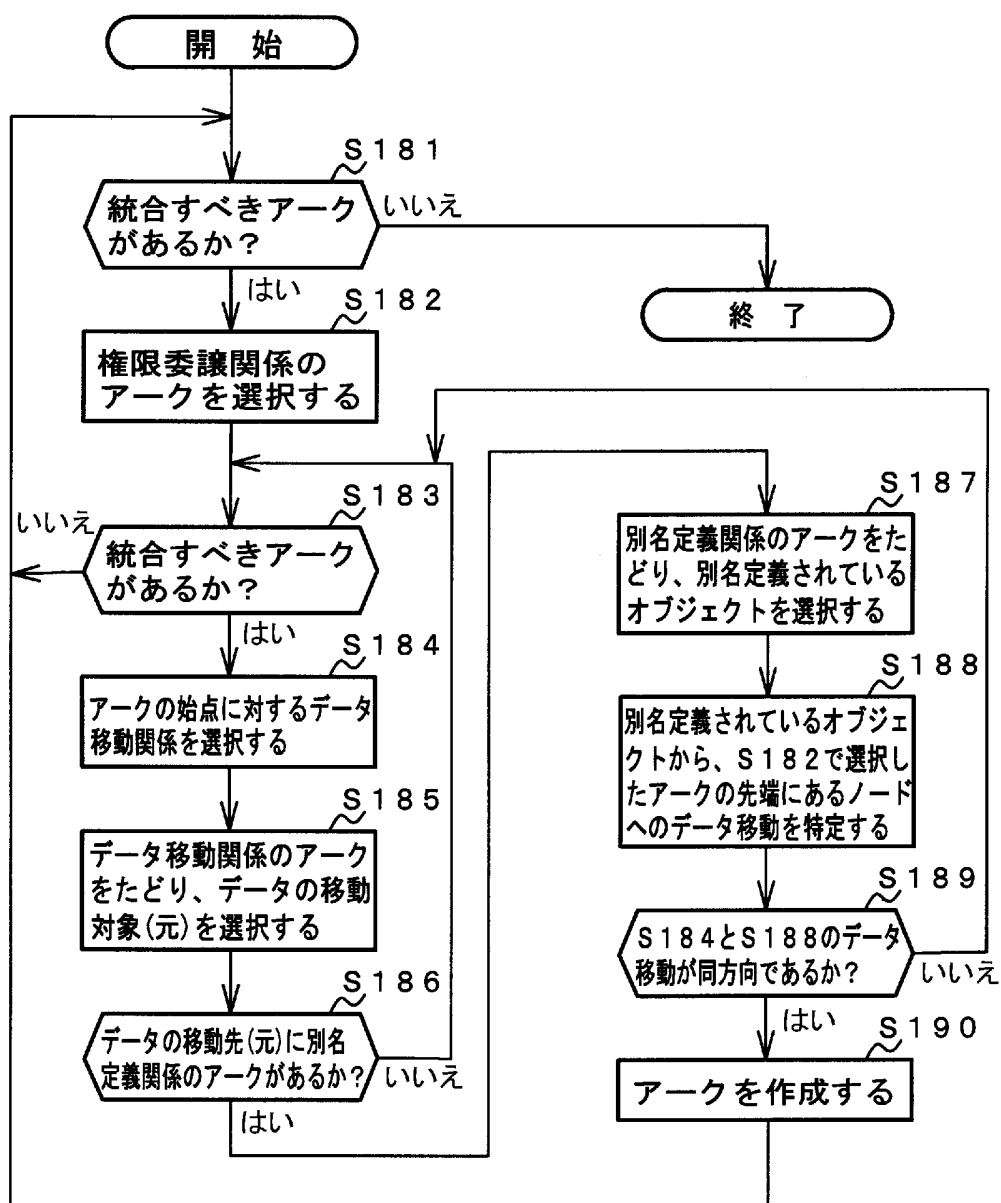
[図32]



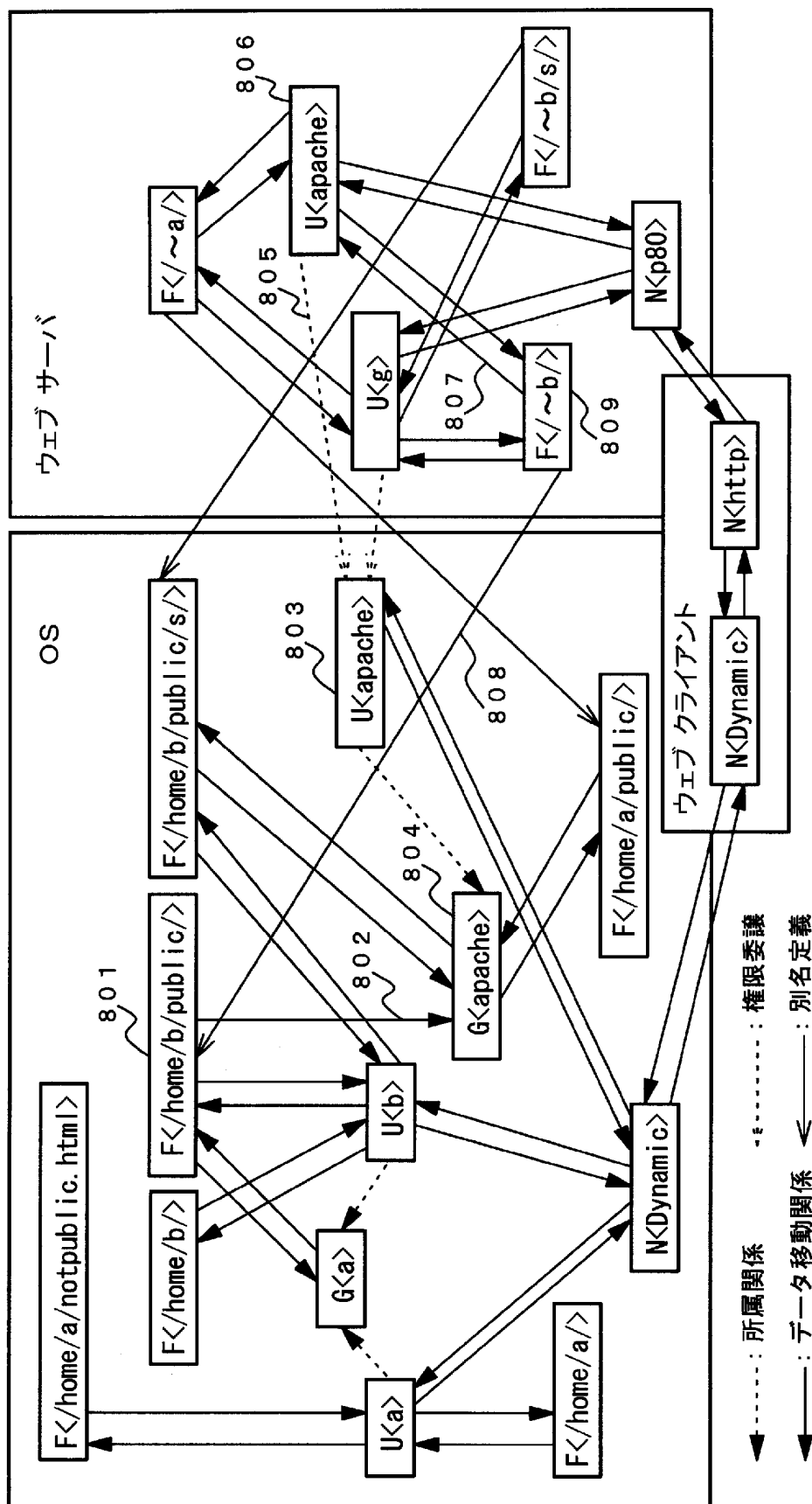
[図33]



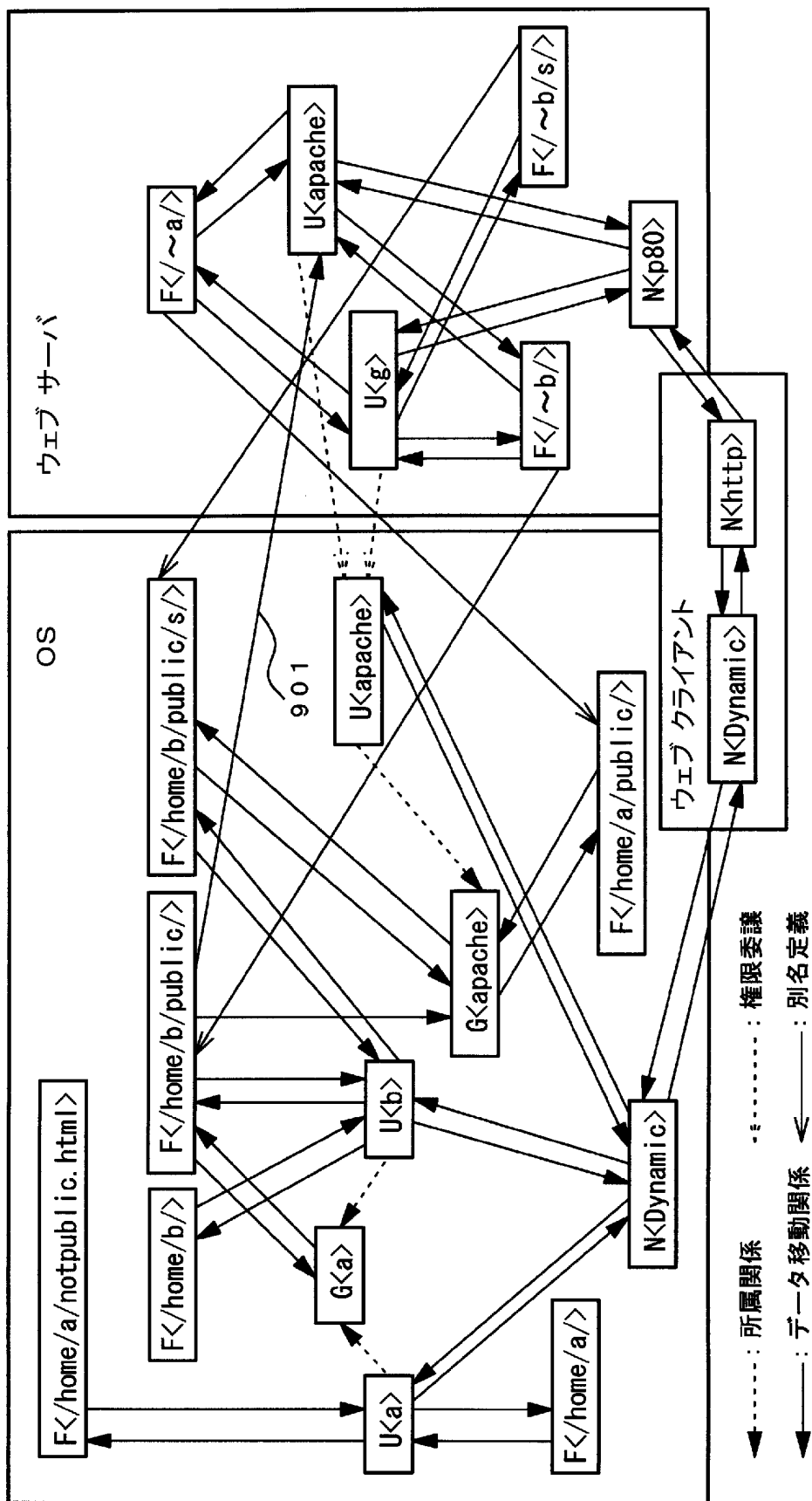
[図34]



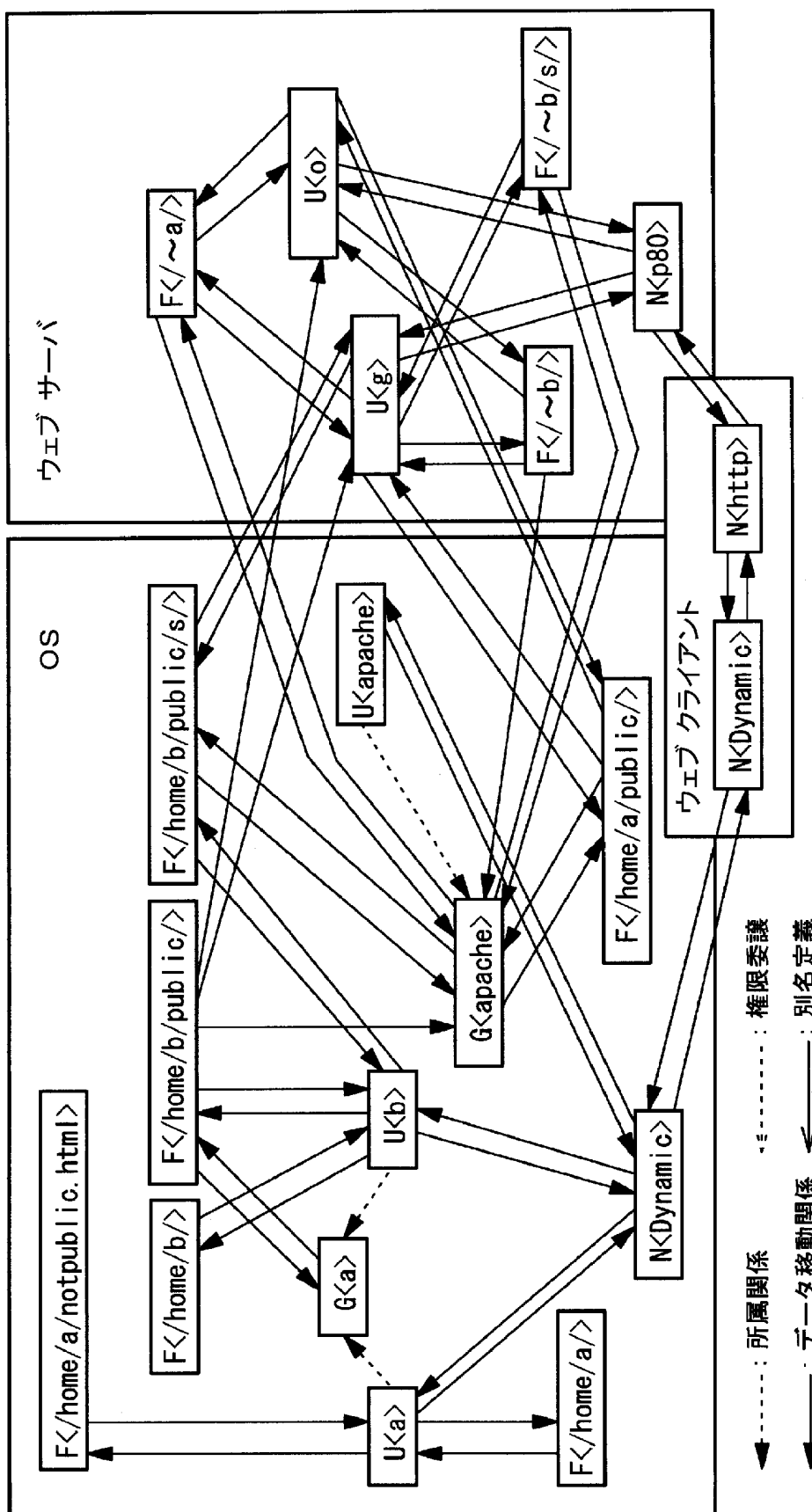
[図35]



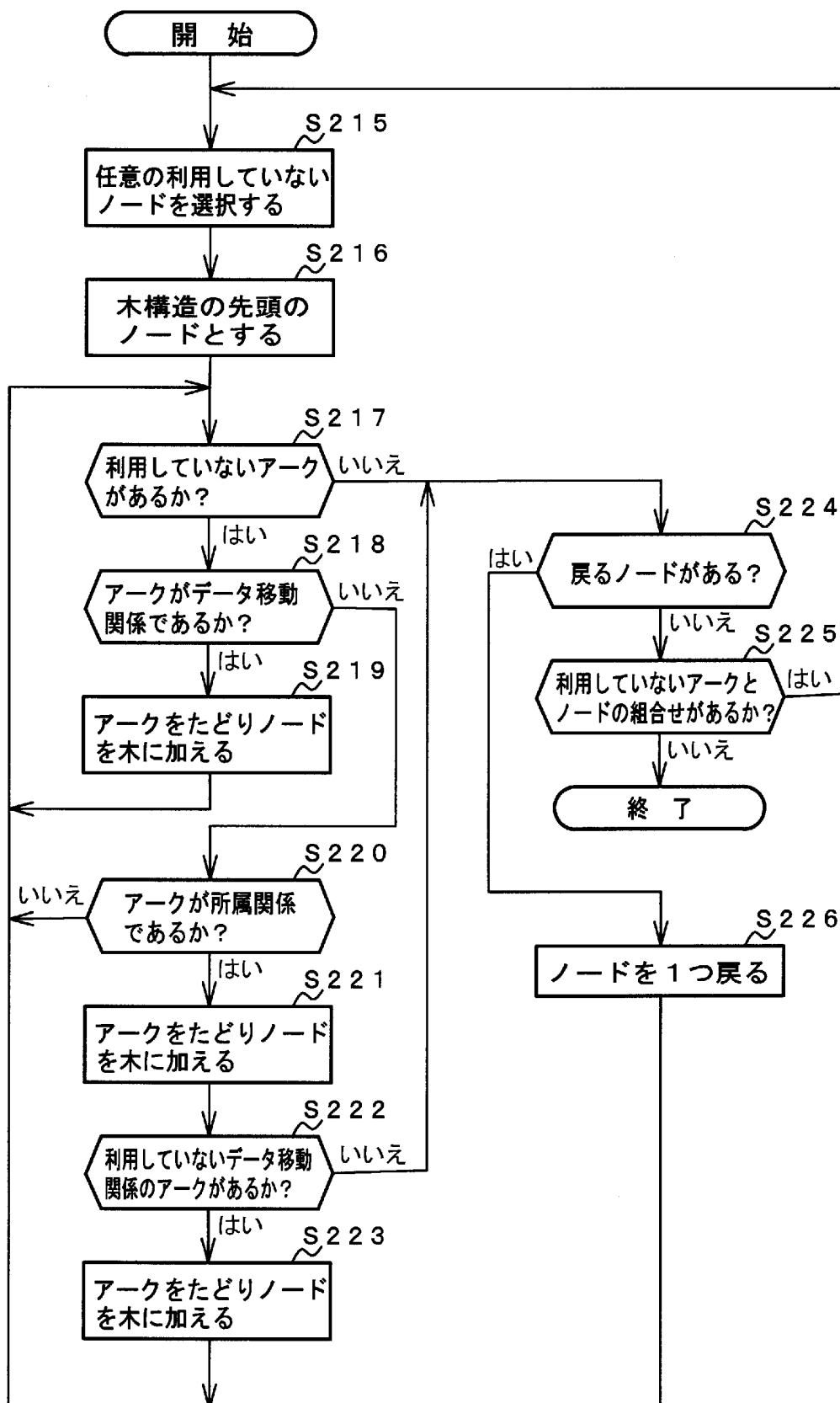
[図36]



[図37]



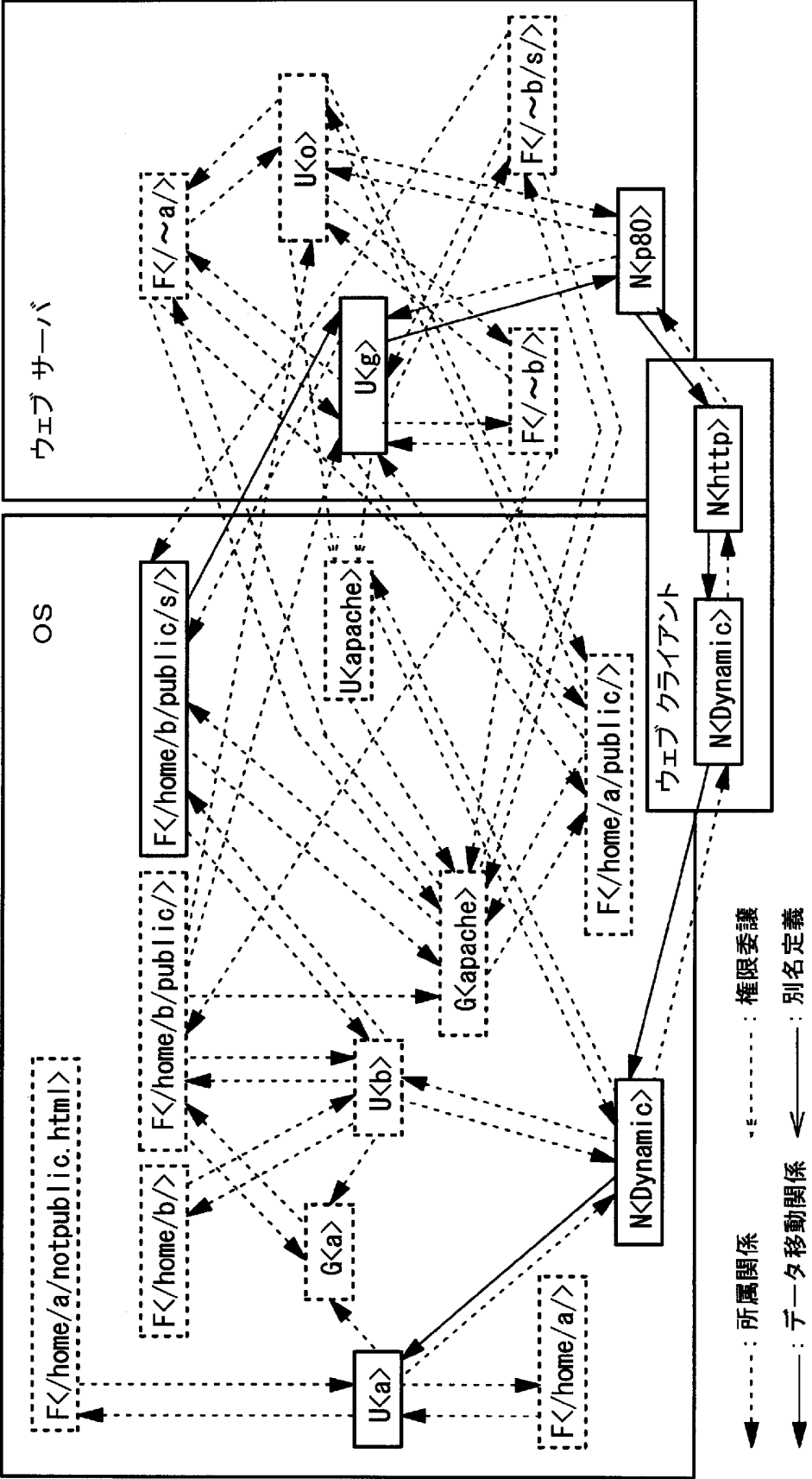
[図40]



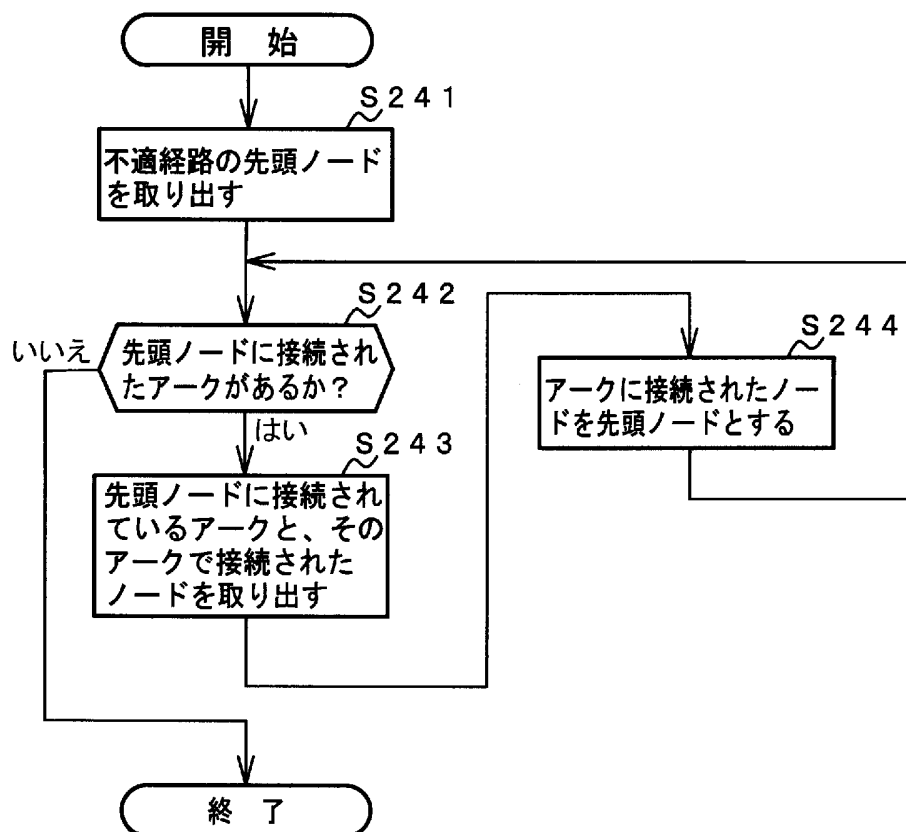
[図41]

ポリシー1	U<a>. * F</d/>
ポリシー2	F</c/>. * [NET] . * U<a>
ポリシー3	F</c/>. * ^ N<p 4 4 3>. * U
ポリシー4	^ U. * F</b/p u b l i c/>
ポリシー5	^ (U U<g>) . * F</b/p u b l i c/s/>

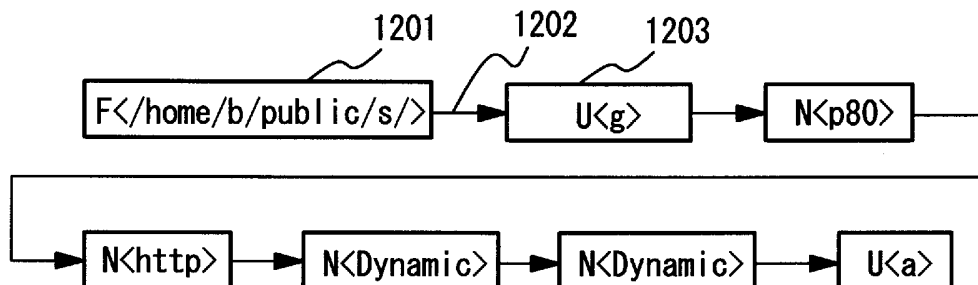
[図42]



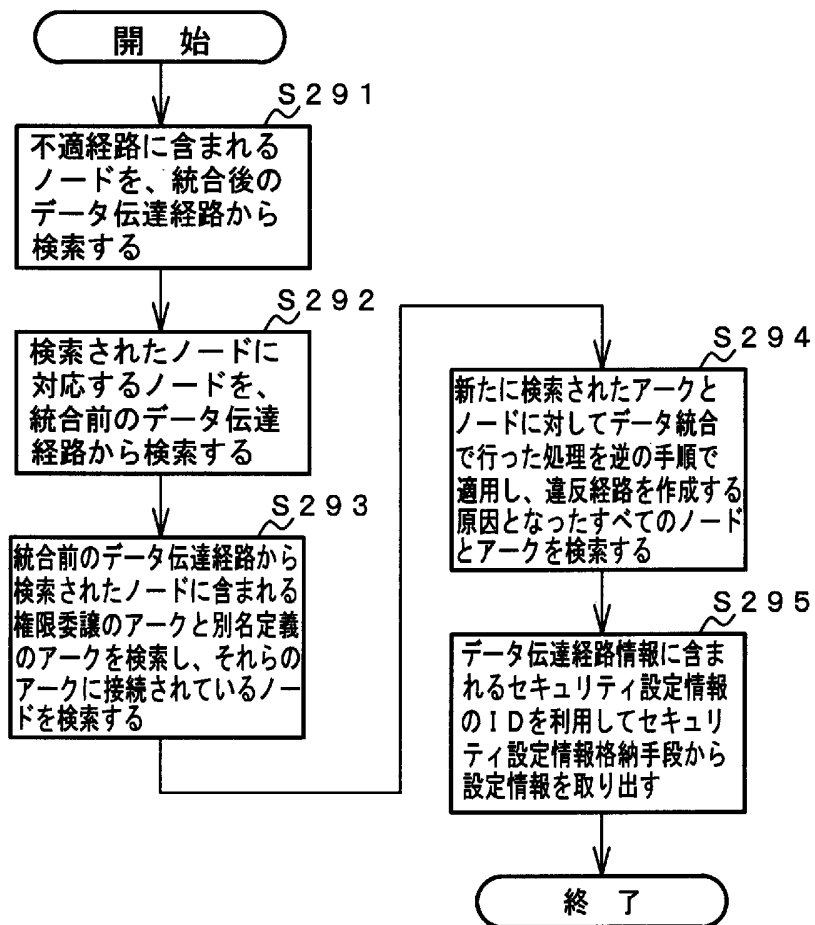
[図43]



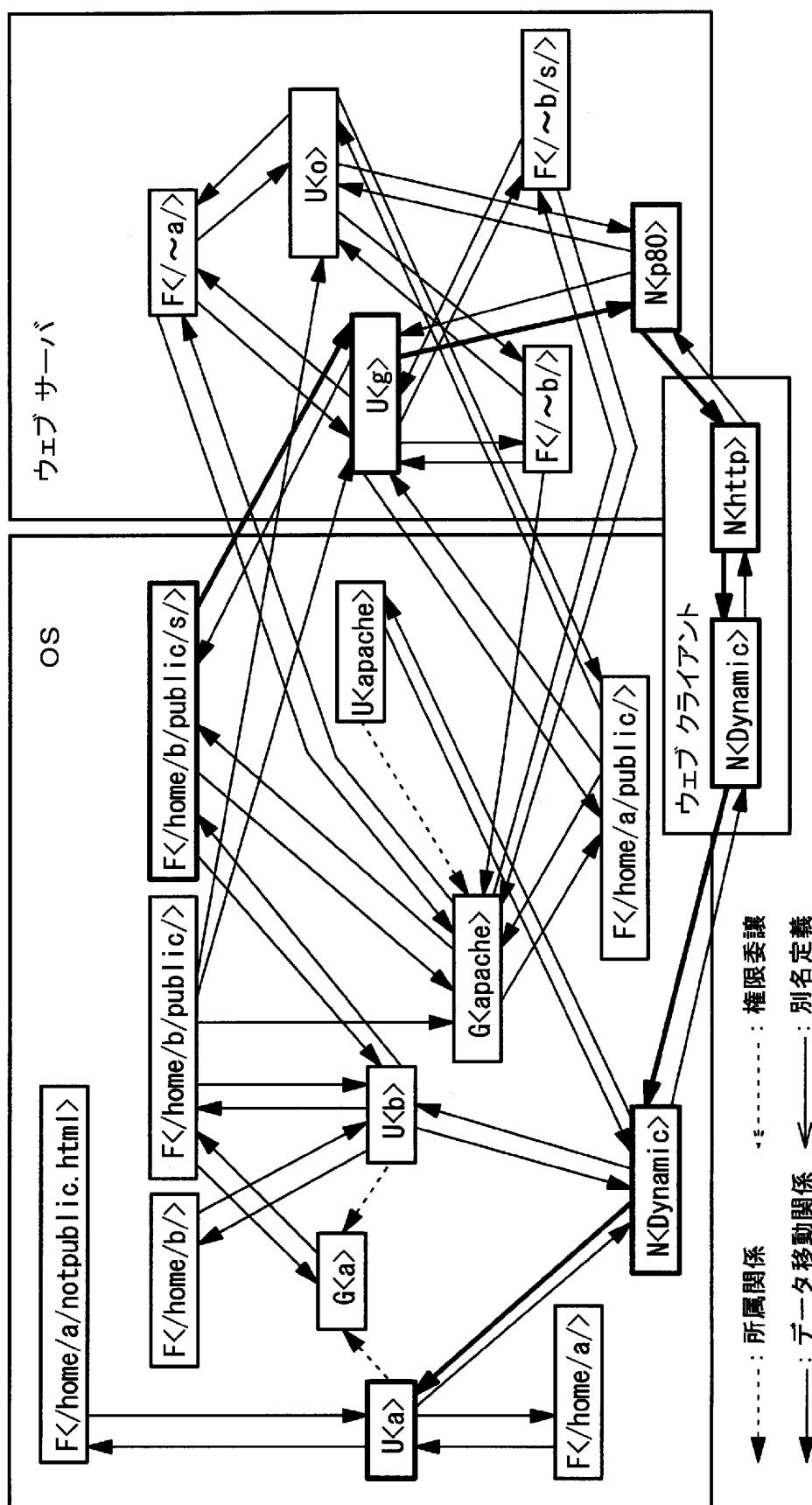
[図44]



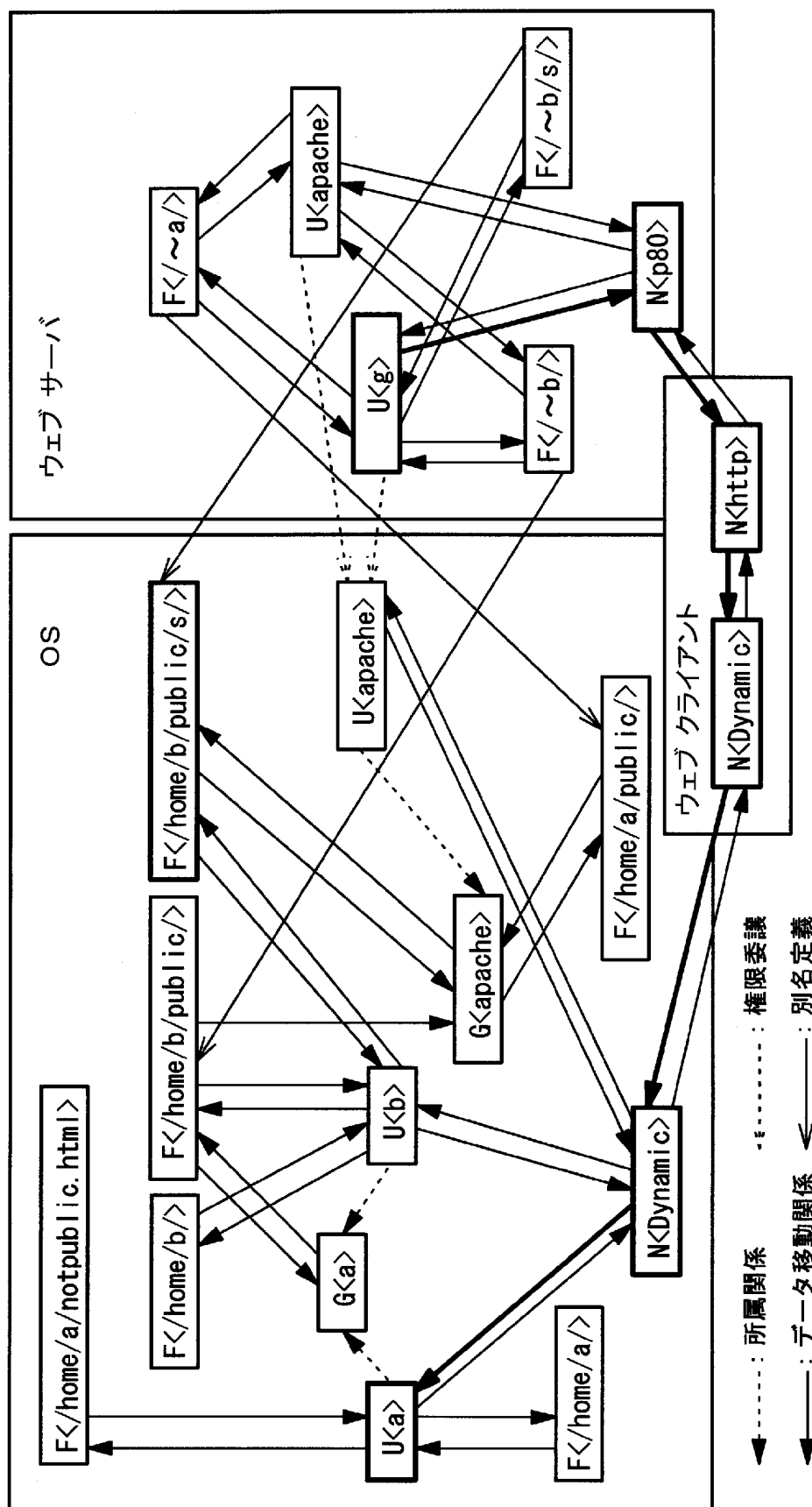
[図45]



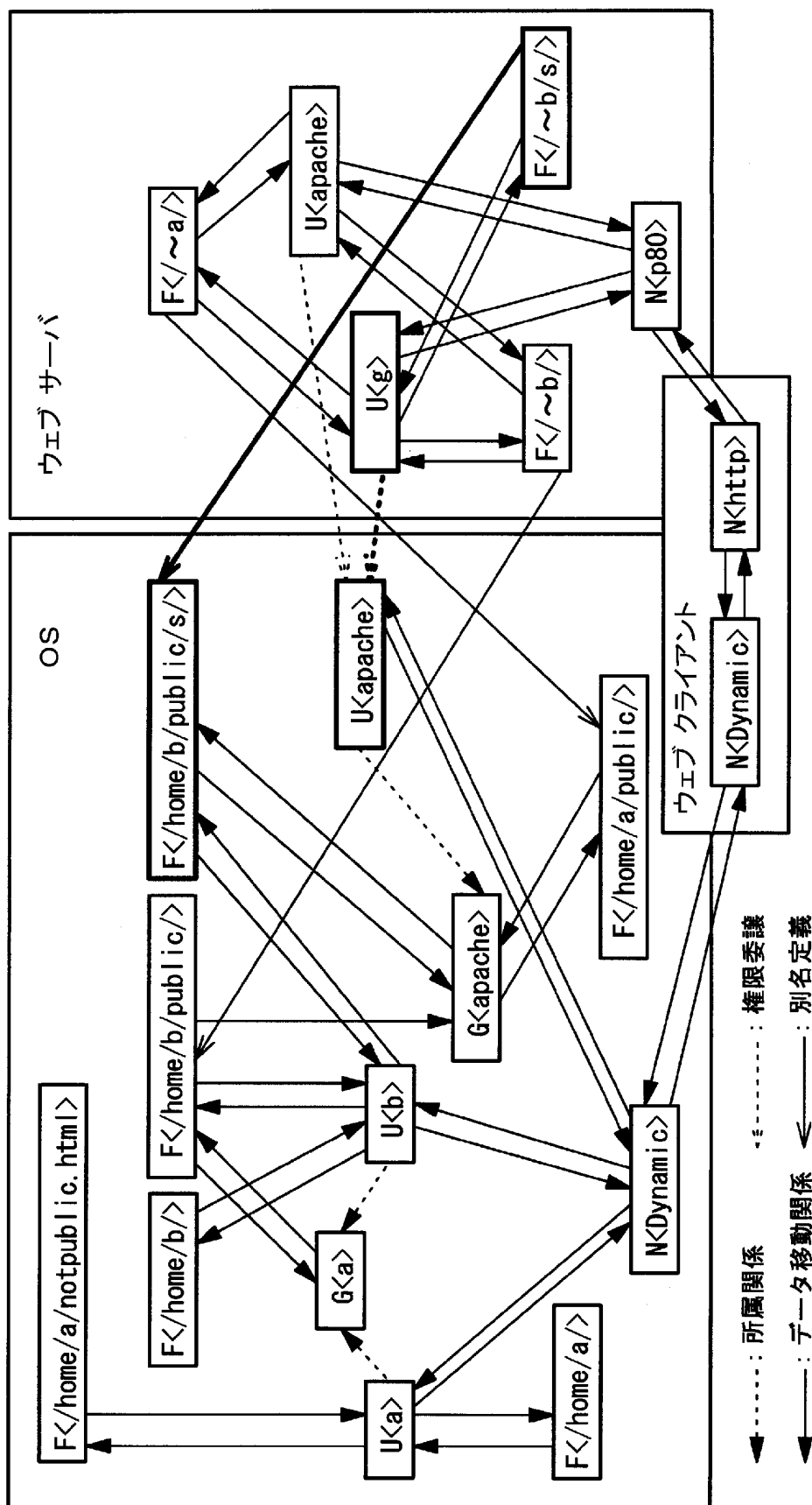
[図46]



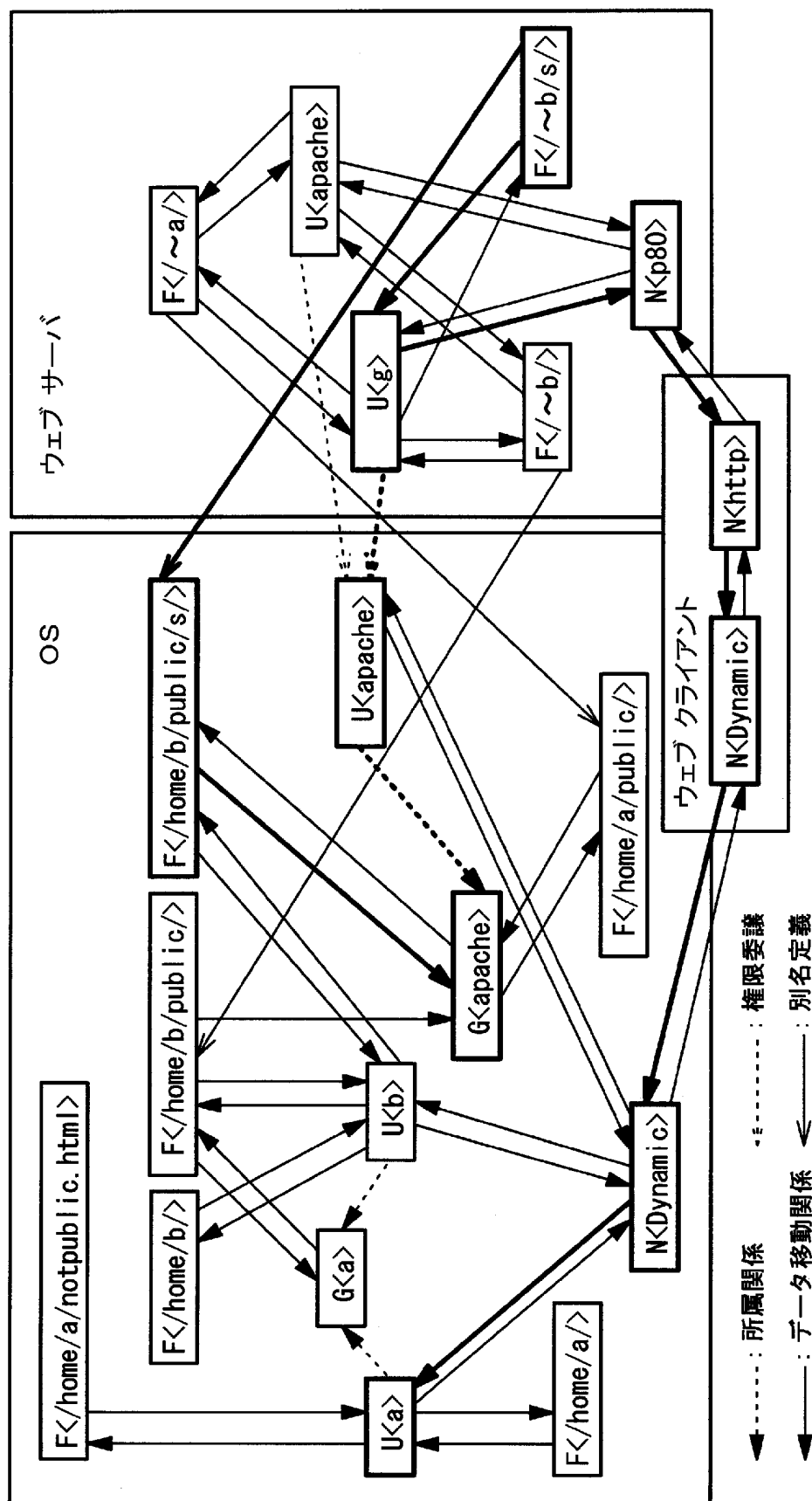
[図47]



[図48]



[図49]



[図50]

```

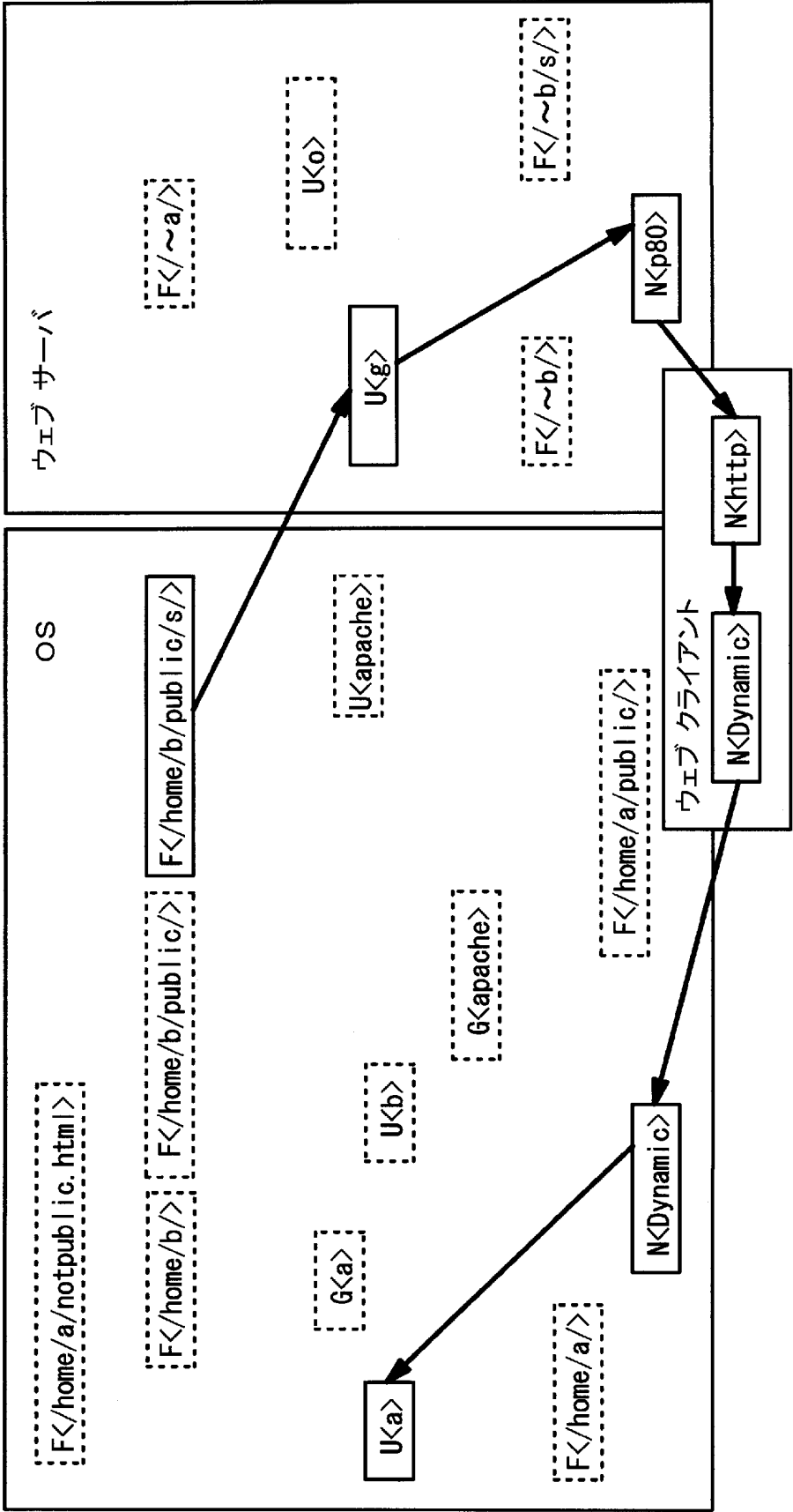
<?Xml version="1.0" encoding="UTF-8"?>
<LayeredGraph name="test">
  <Host name="hostname" id="H-1">
    <Layer name="web-server" id="L-1-1">
      <Object name="localhost/80" type="network" id="0-1-1-1">
        <Connect>
          <To>A-1-1-1</To>
          <To>A-1-1-3</To>
          <From>A-1-1-4</From>
          <From>A-1-5-1</From>
        </Connect>
        <ConfigFiles>
          <Config>C-1-1-1</Config>
          <Config>C-1-1-3</Config>
        </ConfigFiles>
      </Object >
      .
      .
    </Layer>
    .
    .
    <Betweenlayers name="OS-Web-Server" id="L-1-4">
      <Dependlayers>
        <On>L-1-2</On>
        <On>L-1-1</On>
      </Dependlayers>
      </Arc type="commision" id="A-1-4-1">
        <Connect>
          <To>0-1-1-3</To>
          <From>0-1-2-8</From>
        </Connect>
        <ConfigFiles>
          <Config>C-1-4-6</Config>
          <Config>C-1-4-5</Config>
        </ConfigFiles>
      </Arc>
      .
      .

```

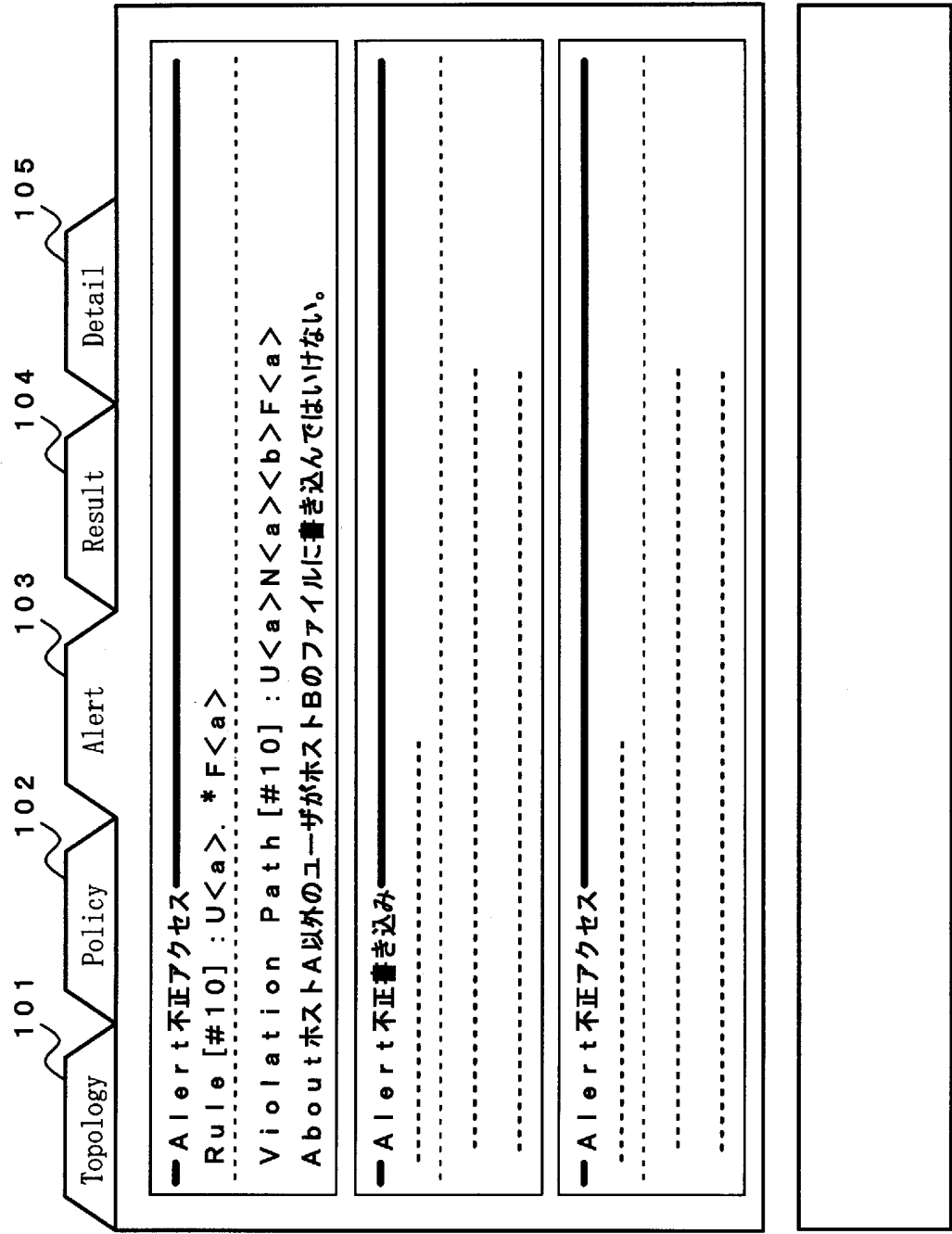
[図51]

設定情報 I D	セキュリティ単位情報	設定情報ファイル名
C-1-1-1	<Directory"/home/b/public/s/"> AuthUserFile/ver/www/.htpasswd AuthGroupFile/dev/null AuthName"Test For Basic Auth" AuthType Basic Require valid-user </Directory>	httpd.conf
C-1-1-6	User-g:passwd	.htpasswd
-----	-----	-----
C-1-4-5	a:x:501:501::/home/b:/bin/bash	/etc/passwd
C-1-4-6	apache:x:48:48:Apache:/ver/www:bin/false	/etc/passwd
C-1-4-7	apache:x:48	/etc/group
C-1-4-8	drwx--rwx b a/home/b/public/s/	Directory
-----	-----	-----

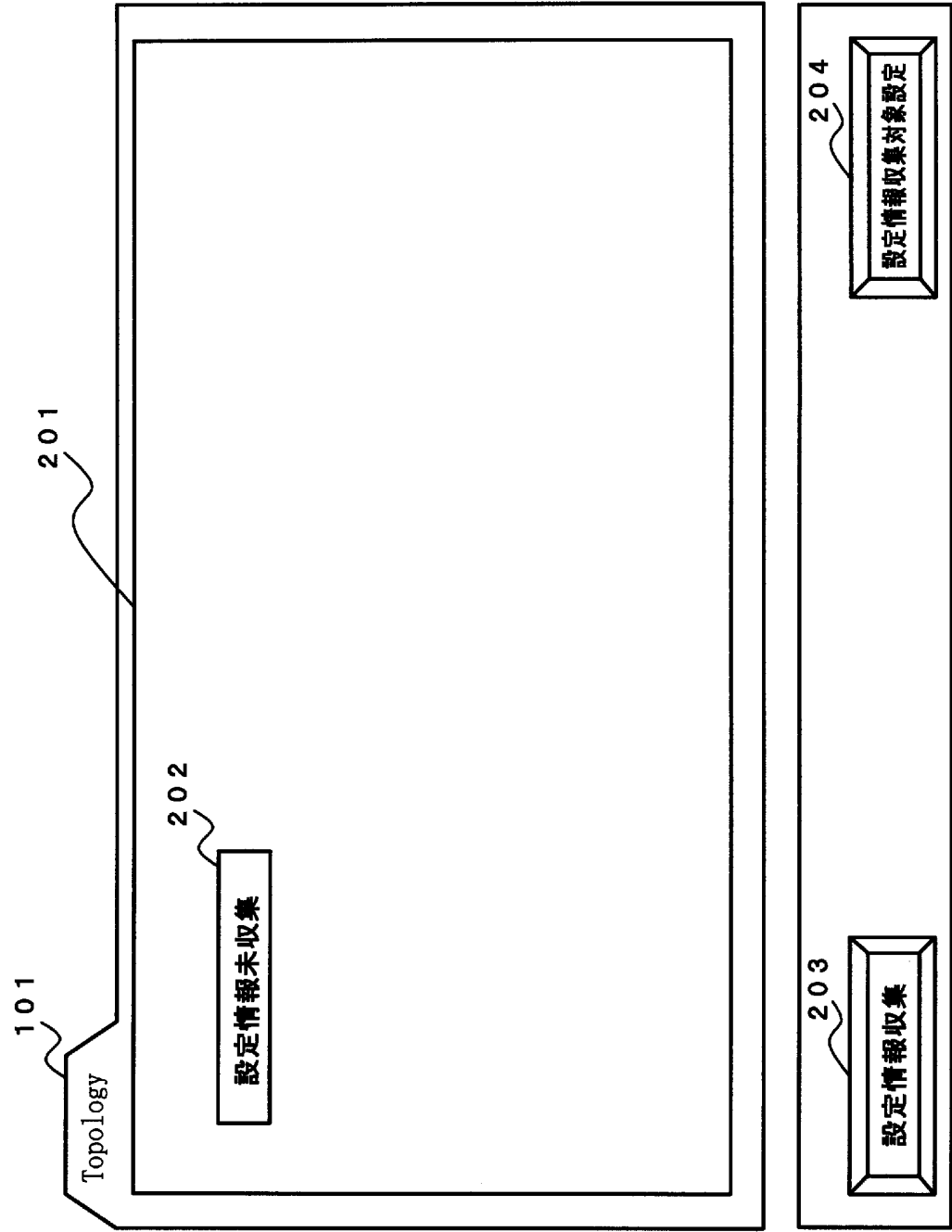
[図52]



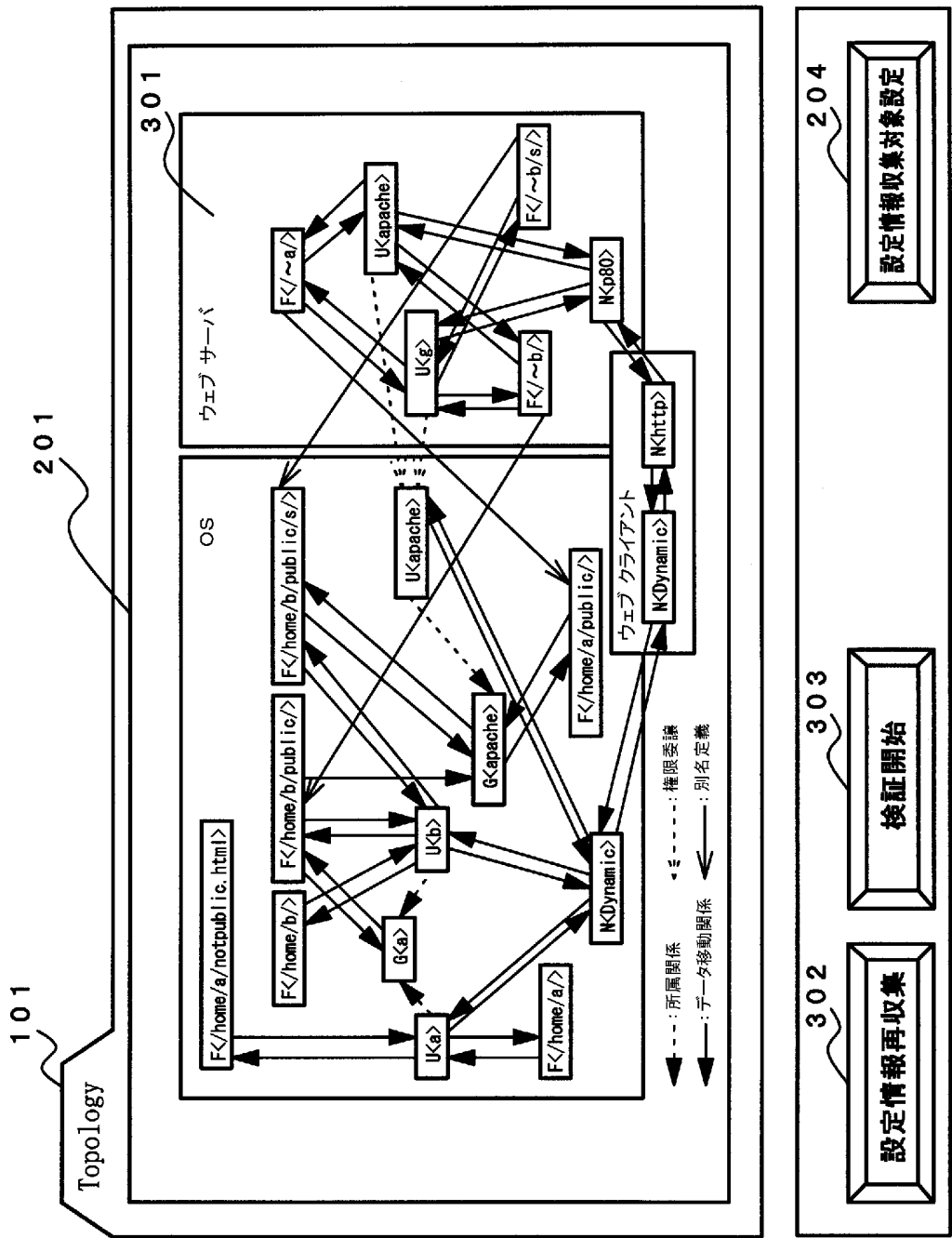
[図53]



[図54]



[図55]



[図56]

401

Policy

ON/OFF

名前

意味

403

404

☒ ポリシー1 : ホストA以外のユーザがホストBのファイルに書き込んではいけない。

☐ ポリシー2 : ホストAで公開されているファイルは認証ユーザのみが書き込んでよい。

☒ ポリシー3 : ファイル「/home/b/public/s/」はネットワークを経由して読んではいけない。

☐ 新規のポリシー

402

405

削除

削除

削除

406

407

408

409

410

検証開始

読み込み

名前

書式

意味

ポリシー1

$U < a > | U < c > | U < d > . * F < a > F < c >$

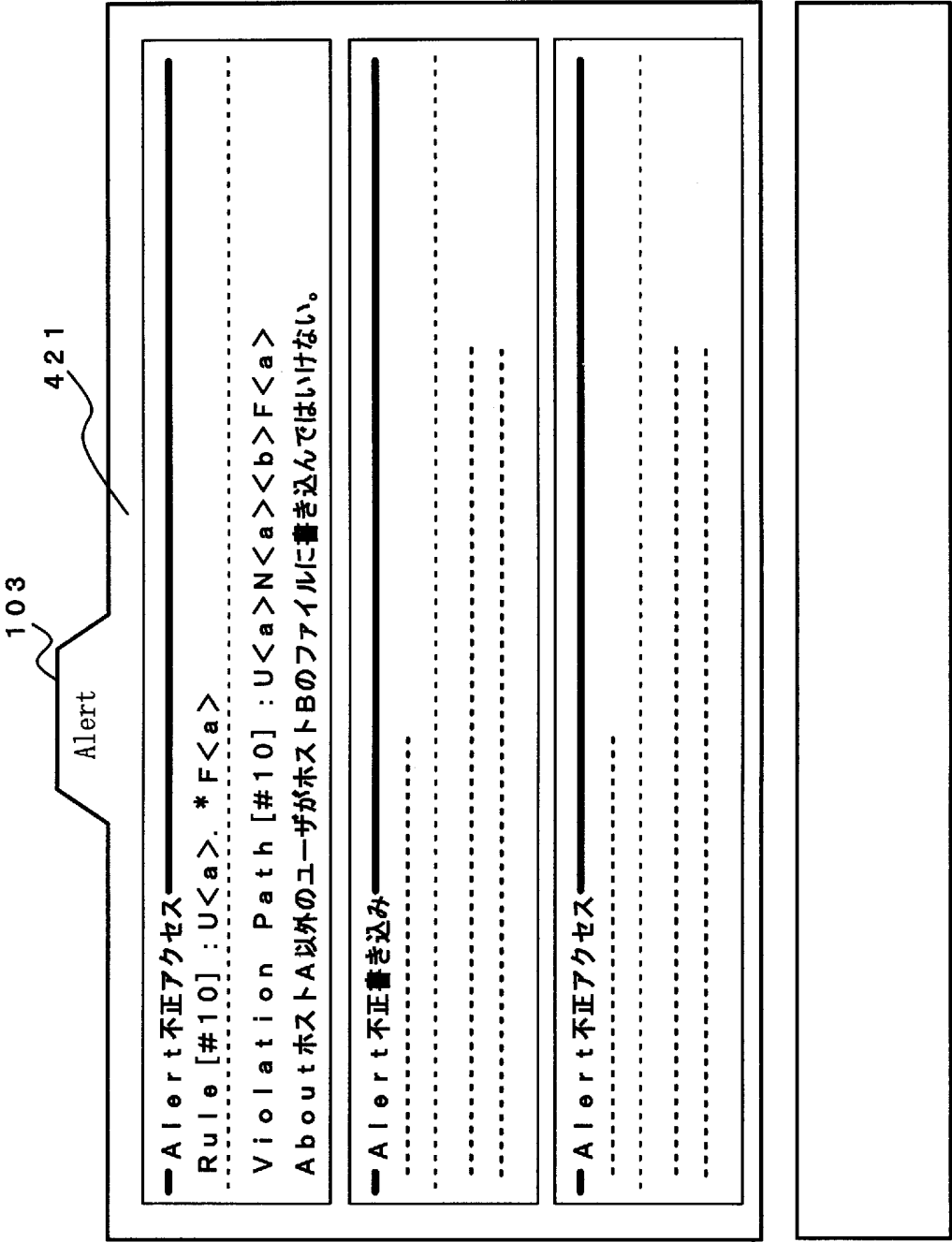
ホストA以外のユーザがホストBのファイルに書き込んではいけない。

不正書き込み

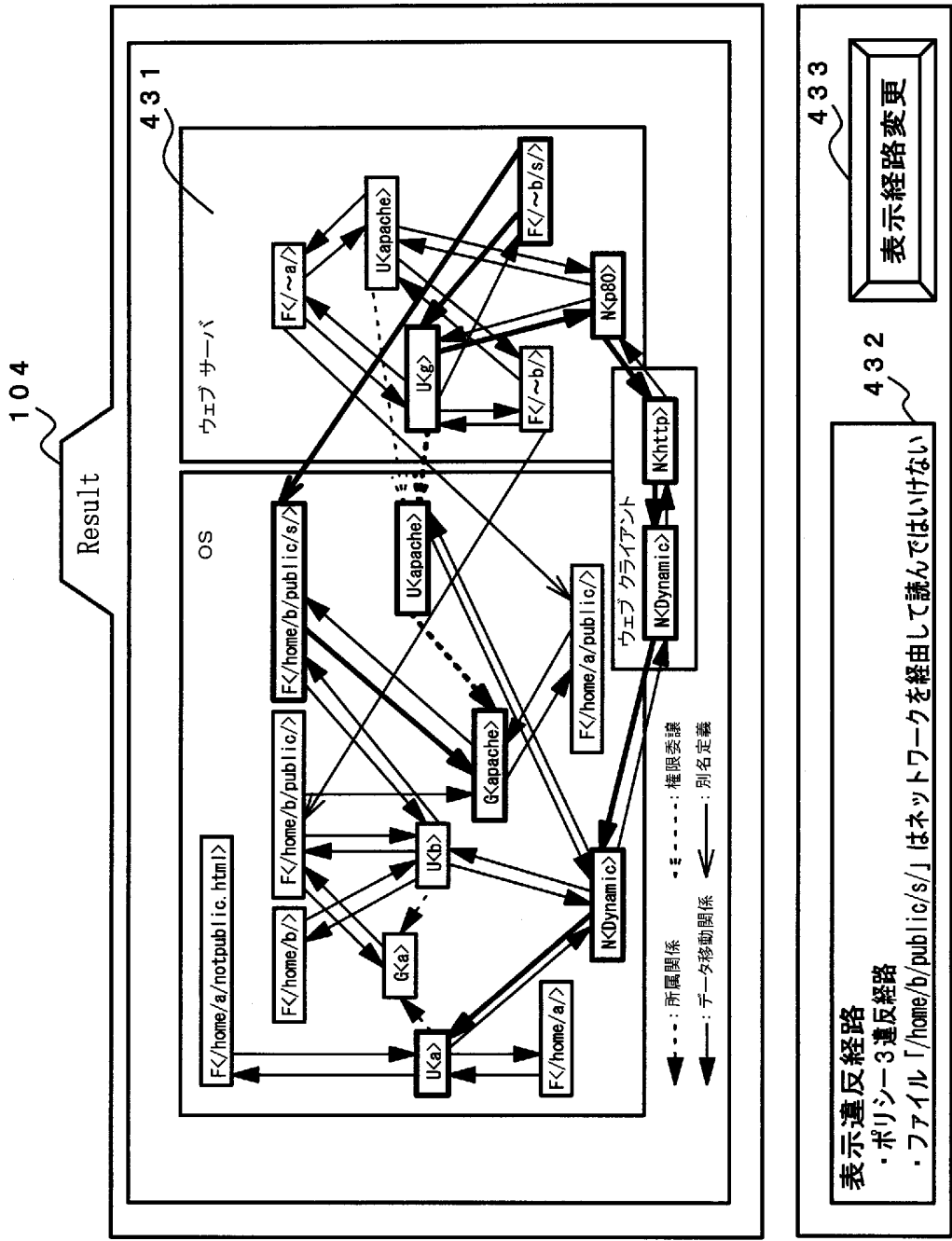
ポリシー追加

保存

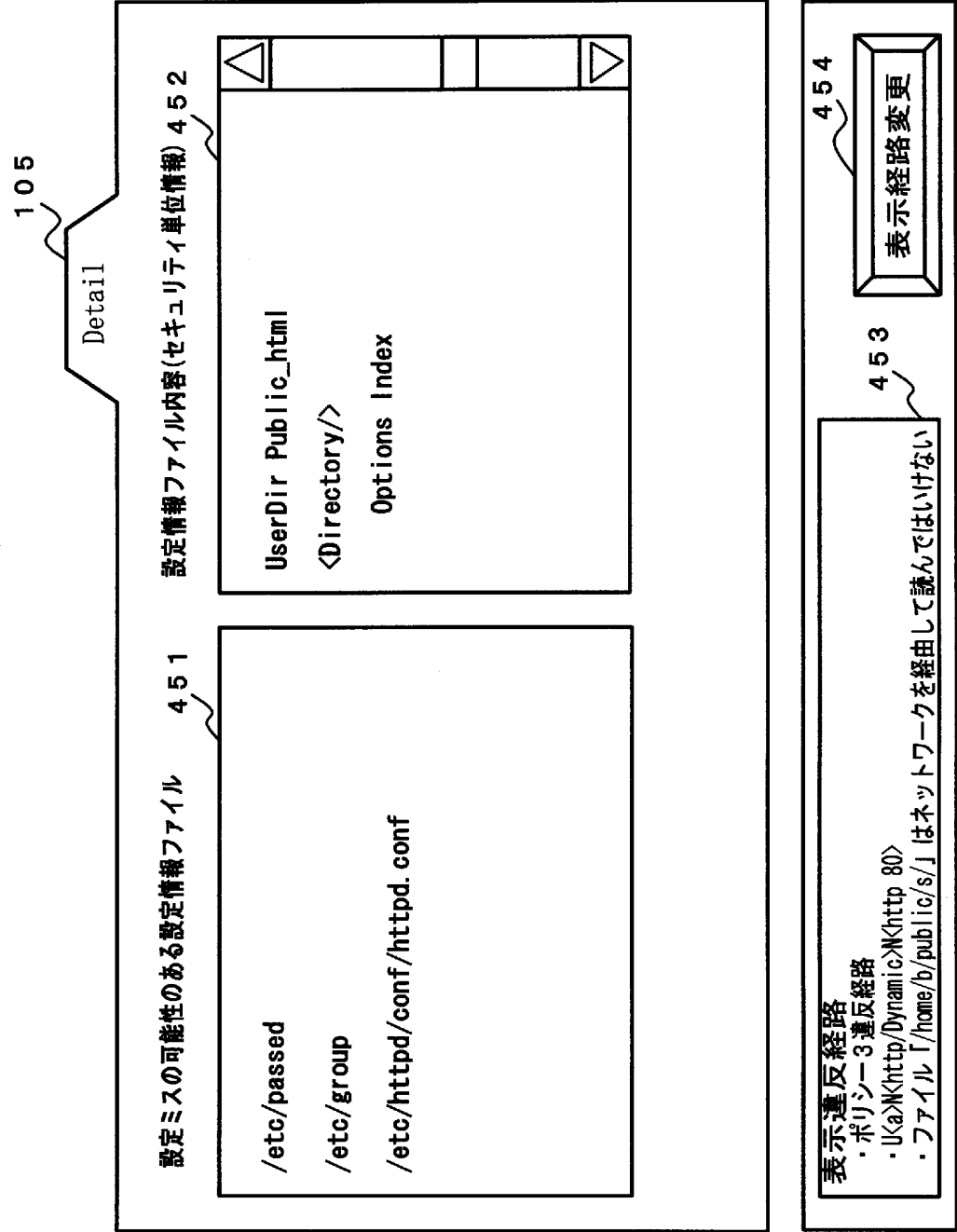
[図57]



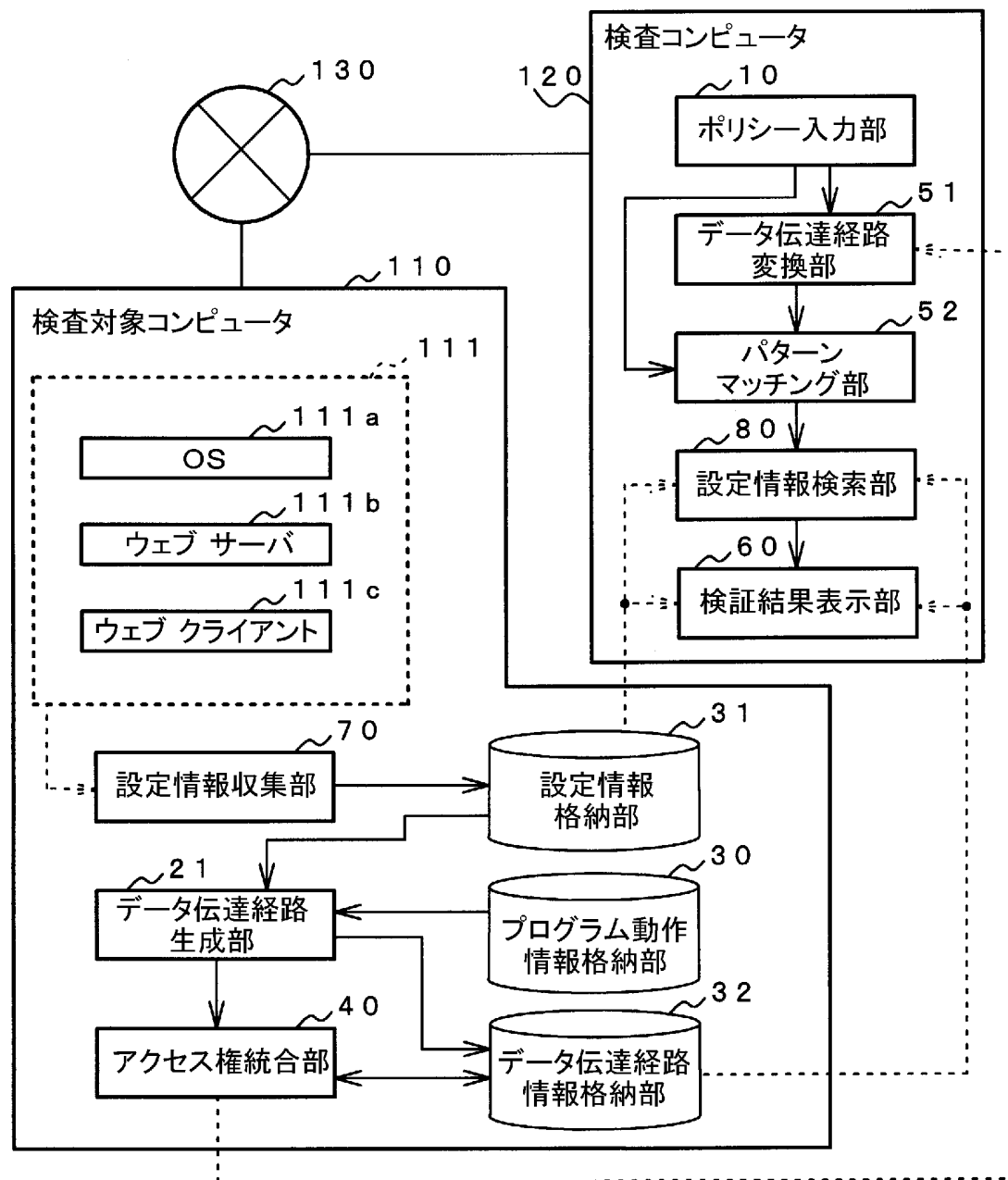
[図58]



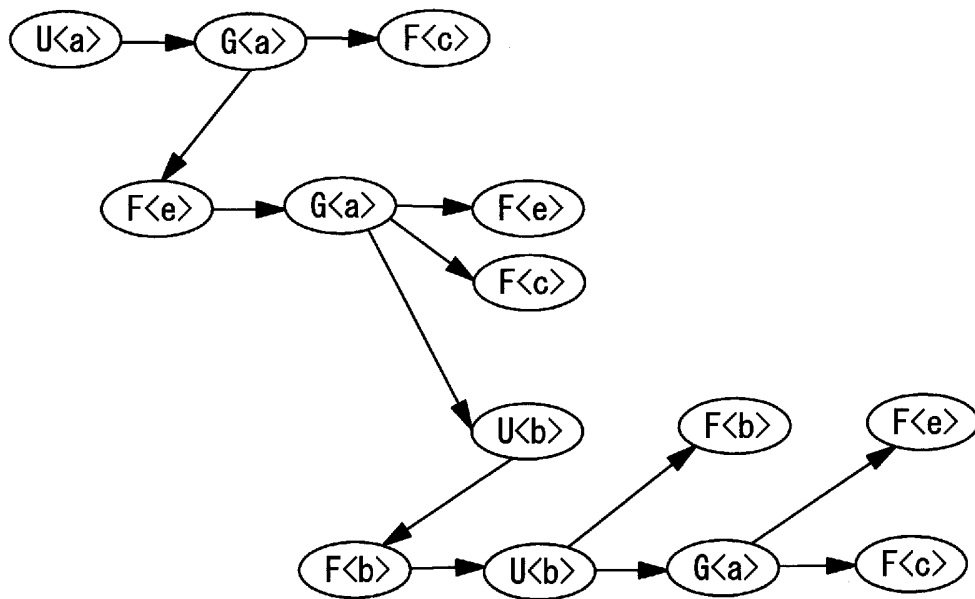
[図59]



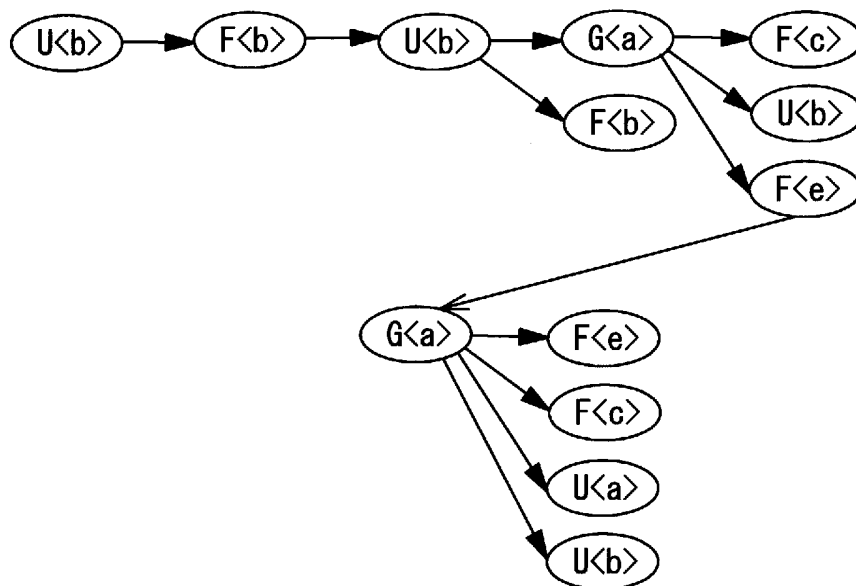
[図60]



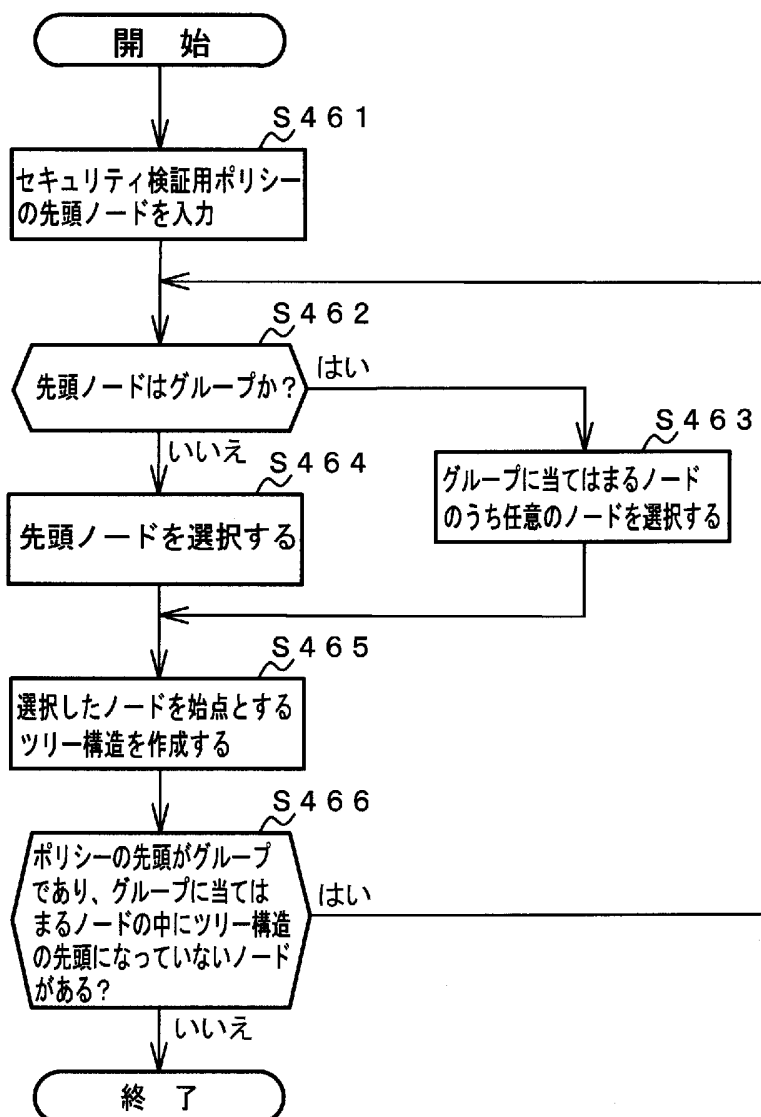
[図61A]



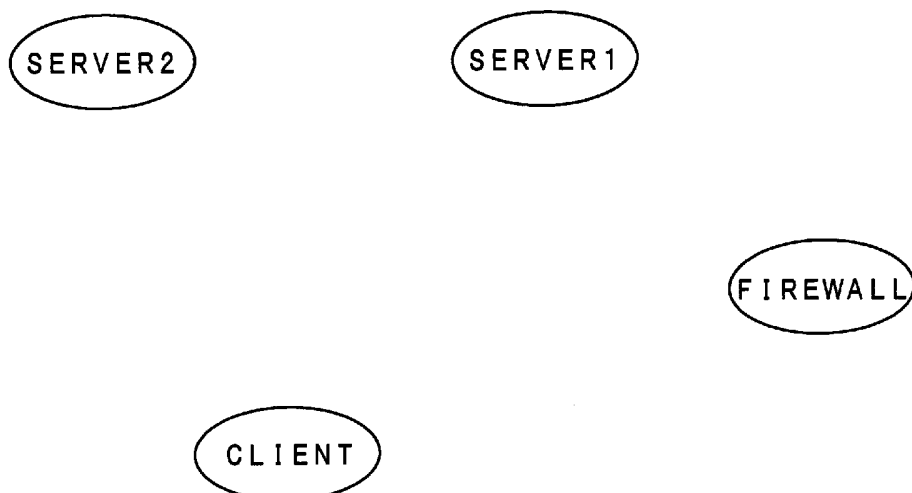
[図61B]



[図62]



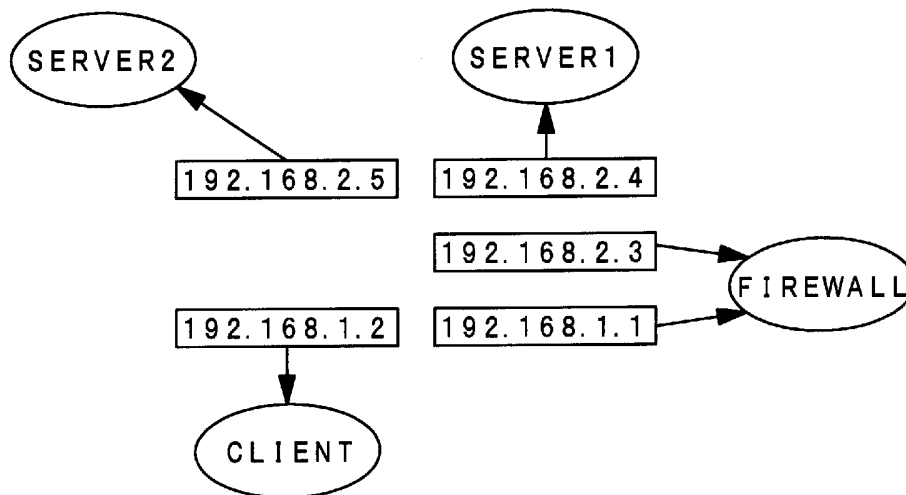
[図63]



[図64]

```
<hosts>
  <host id="h1" name="CLIENT"/>
  <host id="h2" name="FIREWALL"/>
  <host id="h3" name="SERVER1"/>
  <host id="h1" name="SERVER2"/>
</hosts>
```

[図65]

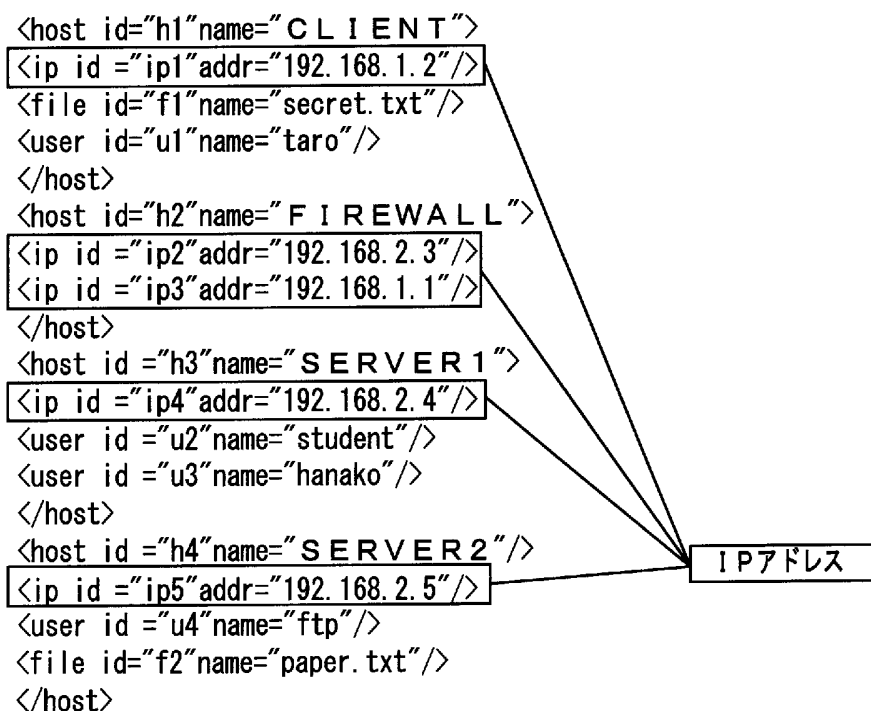


[図66]

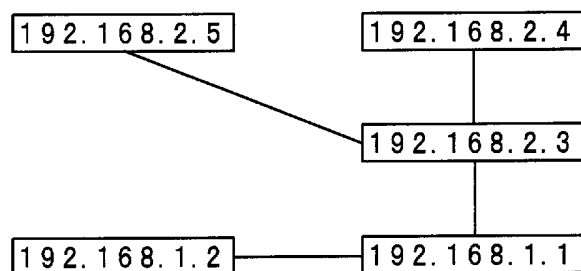
```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=192.168.2.255
IPADDR=192.168.2.5
NETMASK=255.255.255.0
NETWORK=192.168.2.0
ONBOOT=YES
```

IPアドレス

[図67]



[図68]



[図69]

<arcs>

<g end1="ip1" end2="ip3"/>	a
<g end1="ip2" end2="ip3"/>	
<g end1="ip2" end2="ip4"/>	
<g end1="ip2" end2="ip5"/>	
<g end1="ip4" end2="ip5"/>	
<n position="192.168.2.3" srcip="192.168.1.2" detip="192.168.2.4" detport="80"/>	b
<auth user="u1" service="telnet" targetuser="u3"/>	c
<auth user="u3" service="null" targetuser="u2"/>	
<auth user="u2" service="ftp" targetuser="u4"/>	
<cas service="telnet" user="u3" targetservice="null"/>	d
<cas service="null" user="u2" targetservice="ftp"/>	
<acc user="u4" service="read" file="f2"/>	e
<acc user="u4" service="write" file="f2"/>	
<acc user="u1" service="read" file="f1"/>	
<serviceport service="telnet" port="23"/>	f
<serviceport service="ftp" port="21"/>	

</arcs>

[図74]

```

-rw-rw-r-- 1 ftp ftp Mar 5 2003 .
-rw-rw-r-- 1 ftp ftp Nov 5 2003 ..
-rw-rw-r-- 1 ftp ftp Mar 2 17:17 paper.txt

```

アクセス権 所有者 ファイル

[図75]

```

<host id="h1" name="CLIENT">
<ip id="ip1" addr="192.168.1.2"/>
<file id="f1" name="secret.txt"/>
<user id="u1" name="taro"/>
</host>
<host id="h2" name="FIREWALL">
<ip id="ip2" addr="192.168.2.3"/>
<ip id="ip3" addr="192.168.1.1"/>
</host>
<host id="h3" name="SERVER1">
<ip id="ip4" addr="192.168.2.4"/>
<user id="u2" name="student"/>
<user id="u3" name="hanako"/>
</host>
<host id="h4" name="SERVER2">
<ip id="ip5" addr="192.168.2.5"/>
<user id="u4" name="ftp"/>
<file id="f2" name="paper.txt"/>
</host>

```

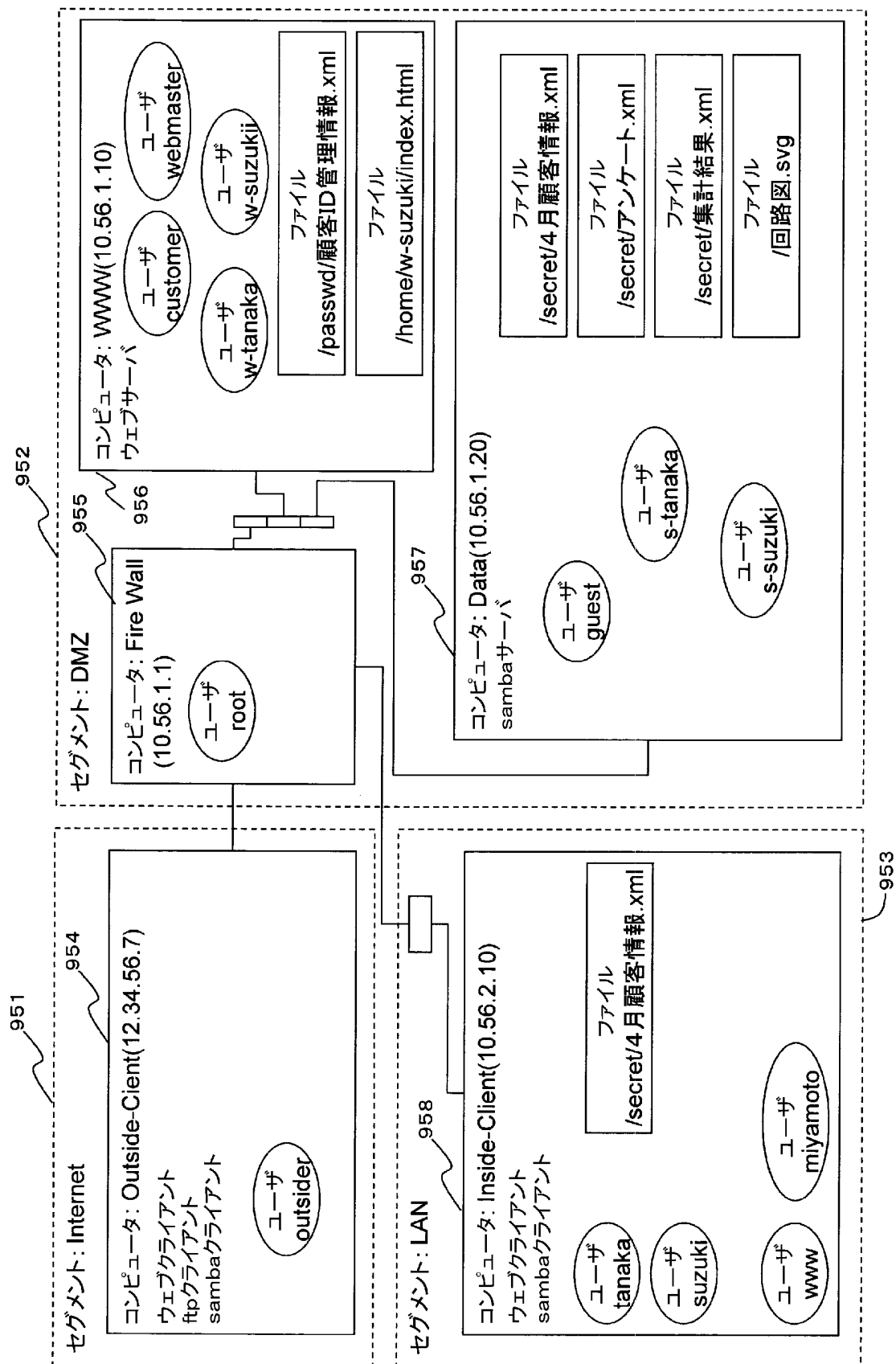
ファイル

[図76]

検証結果		ポリシーの種類 (禁止または許可)
ポリシー	検証したポリシー	
	flow(secret.txt, paper.txt)	禁止
設定モデル	acc(taro, read, secret.txt) ∧ auth(taro, telnet, hanako) ∧ cas(telnet, hanako, student) ∧ auth(hanako, null, student) ∧ cas(null, student, ftp) ∧ auth(student, ftp, ftp) ∧ acc(ftp, write, paper.txt)	

ポリシーにマッチした設定モデル

[図77]



[図78]

```
<networksystem>
  <segment name="Internet">
    <host name="Outside-Client">
      <ip address="12.34.56.7"/>
    </host>
  </segment>
  <segment name="DMZ">
    <category>DMZ</category>
    <host name="Fire Wall">
      <ip address="12.34.56.1"/>
      <ip address="10.56.1.1"/>
      <ip address="10.56.2.1"/>
    </host>
    <host name="WWW">
      <ip address="10.56.1.10"/>
      <category>public_www</category>
    </host>
    <host name="Data">
      <ip address="10.56.1.20"/>
      <category>public_www</category>
    </host>
  </segment>
  <segment name="LAN">
    <category>UBQi_LAN</category>
    <host name="Inside-Client">
      <ip address="10.56.2.10"/>
      <category>Inside-Client</category>
    </host>
  </segment>
</networksystem>
```

Diagram illustrating the XML structure for a network system configuration, with annotations 1601, 1602, and 1603 pointing to specific elements.

- 1601 points to the `<segment name="DMZ">` element.
- 1602 points to the `<host name="WWW">` element.
- 1603 points to the `<ip address="10.56.1.1"/>` element.

[図79]

```

<Services>
  <Service name="http" encryption="OFF">
    <port number="80" />
  </Service>
  <Service name="https" encryption="ON">
    <port number="443" />
  </Service>
  <Service name="samba" encryption="OFF">
    <port number="139" />
  </Service>
  <Service name="ftp" encryption="OFF">
    <port number="21">
      <ip address="10.56.1.10" />
    </port>
  </Service>
</Services>

```

Diagram 79 shows an XML structure for services. The root element is <Services>. It contains four <Service> elements. The first <Service> has name="http", encryption="OFF", and a <port number="80" /> child. The second <Service> has name="https", encryption="ON", and a <port number="443" /> child. The third <Service> has name="samba", encryption="OFF", and a <port number="139" /> child. The fourth <Service> has name="ftp", encryption="OFF", and a <port number="21"> child, which contains a <ip address="10.56.1.10" /> child. Reference numerals 1701, 1702, and 1703 point to the <Services> root, the first <Service> element, and the <ip address> element, respectively.

[図80]

```

<UserList>
  <UserCategory name="部長">
    <User name="Tanaka">
      <ID name="tanaka" host="10.56.2.10" application="OS"/>
      <ID name="w-tanaka" host="10.56.1.10" application="OS" />
      <ID name="s-tanaka" host="10.56.1.20" application="OS" />
    </User>
  </UserCategory>
  <UserCategory name="ウェブ管理者">
    <User name="webmaster">
      <ID name="webmaster" host="10.56.2110" application="OS"/>
      <ID name="www" host="10.56.2.10" application="OS"/>
    </User>
  </UserCategory>
  <UserCategory name="営業">
    <User name="suzuki">
      <ID name="suzuki" host="10.56.2.10" application="OS"/>
      <ID name="s-suzuki" host="10.56.1.20" application="OS"/>
      <ID name="w-suzuki" host="10.56.1.10" application="OS"/>
    </User>
    <User name="miyamoto">
      <ID name="miyamoto" host="10.56.2.10" application="OS"/>
    </User>
  </UserCategory>
  <UserCategory name="ゲスト">
    <User name="guest">
      <ID name="Outsider" host="12.34.56.7" application="OS" />
      <ID name="customer" host="10.56.1.10" application="OS" />
      <ID name="guest" host="10.56.1.20" application="OS" />
    </User>
  </UserCategory>
  <UserCategory>
    <User name="FW-Administrator">
      <ID name="root" host="10.56.1.10" application="OS" />
    </User>
  </UserCategory>
</UserList>

```

Diagram 80 shows an XML structure for a user list. The root element is <UserList>. It contains five <UserCategory> elements. The first <UserCategory> has name="部長" and contains one <User> element with name="Tanaka", which has three <ID> children: "tanaka" (host="10.56.2.10", application="OS"), "w-tanaka" (host="10.56.1.10", application="OS"), and "s-tanaka" (host="10.56.1.20", application="OS"). The second <UserCategory> has name="ウェブ管理者" and contains one <User> element with name="webmaster", which has two <ID> children: "webmaster" (host="10.56.2110", application="OS") and "www" (host="10.56.2.10", application="OS"). The third <UserCategory> has name="営業" and contains two <User> elements. The first <User> has name="suzuki" and has three <ID> children: "suzuki" (host="10.56.2.10", application="OS"), "s-suzuki" (host="10.56.1.20", application="OS"), and "w-suzuki" (host="10.56.1.10", application="OS"). The second <User> has name="miyamoto" and has one <ID> child: "miyamoto" (host="10.56.2.10", application="OS"). The fourth <UserCategory> has name="ゲスト" and contains one <User> element with name="guest", which has three <ID> children: "Outsider" (host="12.34.56.7", application="OS"), "customer" (host="10.56.1.10", application="OS"), and "guest" (host="10.56.1.20", application="OS"). The fifth <UserCategory> is empty. Reference numerals 1801, 1802, and 1803 point to the "営業" <UserCategory> element, the "suzuki" <User> element, and the "suzuki" <ID> element, respectively.

[図81]

```

<contents>
  <host address="10.56.1.10">
    <file name="/passwd/顧客ID管理情報.xml">
      <category>個人情報</category>
      <category>顧客情報</category>
    </file>
    <file name="/home/w-suzuki/index.html">
      <category>一般情報</category>
    </file>
  </host>
  <host address="10.56.1.20">
    <file name="/secret/4月顧客情報.xml">
      <category>個人情報</category>
      <category>顧客情報</category>
    </file>
    <file name="/secret/アンケート.xml">
      <category>個人情報</category>
      <category>顧客情報</category>
    </file>
    <file name="/secret/集計結果">
      <category>顧客情報</category>
    </file>
    <file name="/回路図.svg">
      <category>技術情報</category>
    </file>
  </host>
  <host address="10.56.2.10">
    <file name="/secret/4月顧客情報.xml">
      <category>顧客情報</category>
      <category>個人情報</category>
    </file>
  </host>
</contents>

```

[図82]

```

<InputPolicyList>
  <InputPolicy ID="P001">
    <Src type="free">
      <NodeString type="file">/mnt/apache/htdocs/index.html</NodeString>
      <Domain type="host">12.46.56.78</Domain>
    </Src>
    <Dst type="free">
      <NodeString type="user">uchida</NodeString>
      <Domain type="host">12.46.56.78</Domain>
    </Dst>
    <Service type="port">80</Service>
  </InputPolicy>
  <InputPolicy ID="P002">
    <Src type="choice">
      <Category type="file">顧客情報</Category>
      <Domain type="host">192.168.12.3</Domain>
    </Src>
    <Dst>
      <Category type="group">担当</Category>
      <Domain type="segment">LAN</Domain>
    </Dst>
    <Service type="name">http</Service>
  </InputPolicy>
  <InputPolicy ID="P003">
    <Src type="choice">
      <Category type="file">個人情報</Category>
      <Domain type="segment">DMZ</Domain>
    </Src>
    <Dst>
      <Category type="user">営業</Category>
      <Domain type="segment">LAN</Domain>
    </Dst>
  </InputPolicy>
</InputPolicyList>

```

2002
 2005
 2006
 2003
 2004
 2001
 2007

[図83]

アクセスポリシー一覧

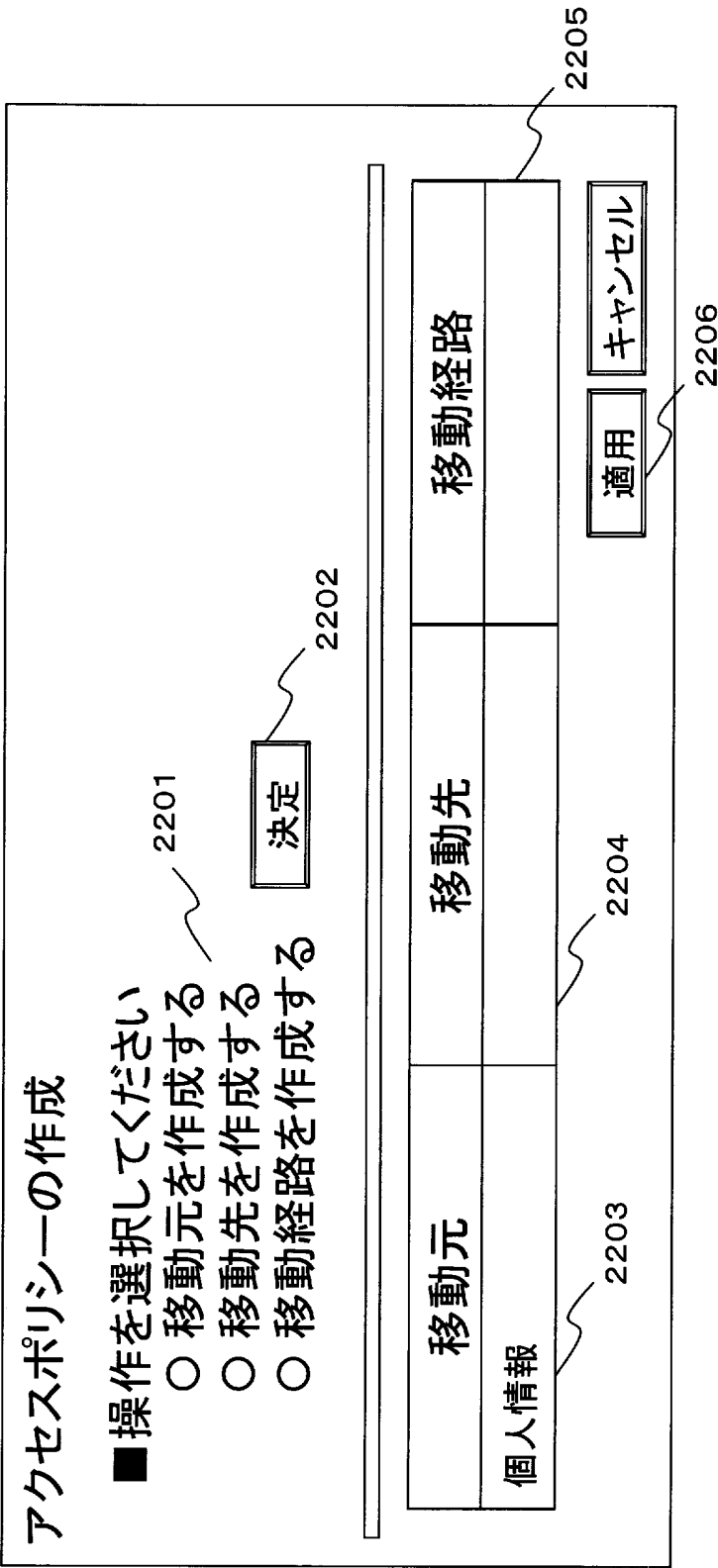
2101

No.	ON OFF	アクセスポリシー			移動経路	2103	2104
		移動元	移動先				
1	☐	/mnt/apache/htdocs/index.html@12.46.56.78	uchida@12.46.56.78	80	☐ 編集	☐ 削除	
2	☐	顧客情報@192.168.12.3	担当@LAN	http	☐ 編集	☐ 削除	
3	☐	個人情報@DMZ	営業@LAN	非暗号化経路	☐ 編集	☐ 削除	
					☐ 新規作成		

2102

2105

[図84]



[図85]

検証対象の移動元の入力

■移動元のタイプを選択してください 2301

ファイル 2302

■移動元を選択してください 2304

ファイルカテゴリで選択する

顧客情報 2305

個人情報

一般情報

秘密情報

機密情報

■ドメインを選択してください 2306

セグメントで指定する

LAN 2307

DMZ

Internet

決定 2308

キャンセル

[図86]

検証対象の移動先入力

■移動先のタイプを選択してください

ユーザ ▾

■移動先を選択してください

ユーザカテゴリで選択する ▾

部長
課長
一般社員
ウェブ管理者
営業

■ドメインを指定してください

セグメントで指定する ▾

LAN
DMZ
Internet

決定 キャンセル

2401

2402

2403

2404

2405

2406

2407

2408

[図87]

移動経路の入力

■移動経路の指定方法を選択してください

サービス属性

■移動経路の指定

サービス属性による指定

☐ 暗号の有無	☐ あり ☒ なし
☐ 認証の有無	☐ あり ☐ なし

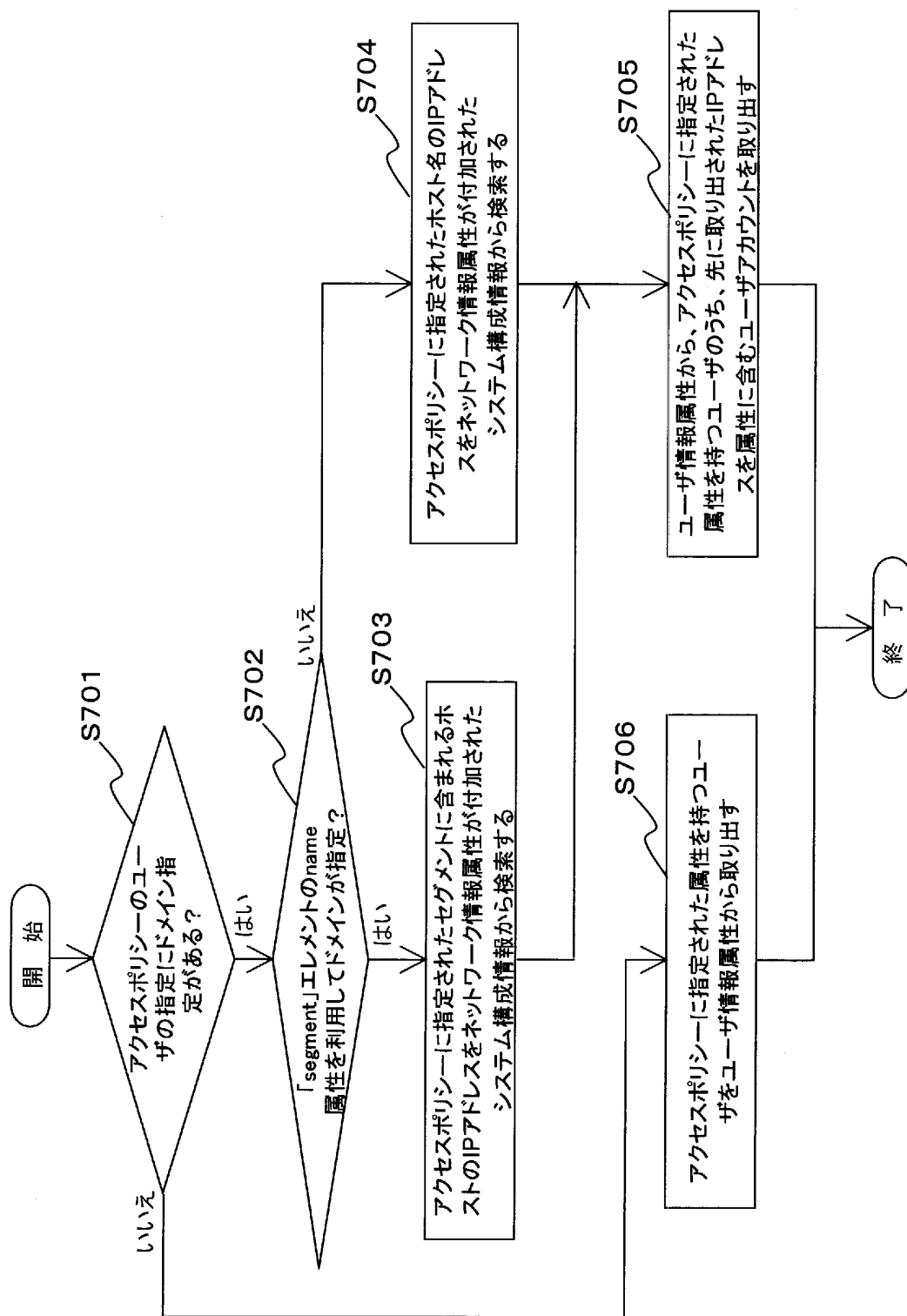
決定 キャンセル

2501

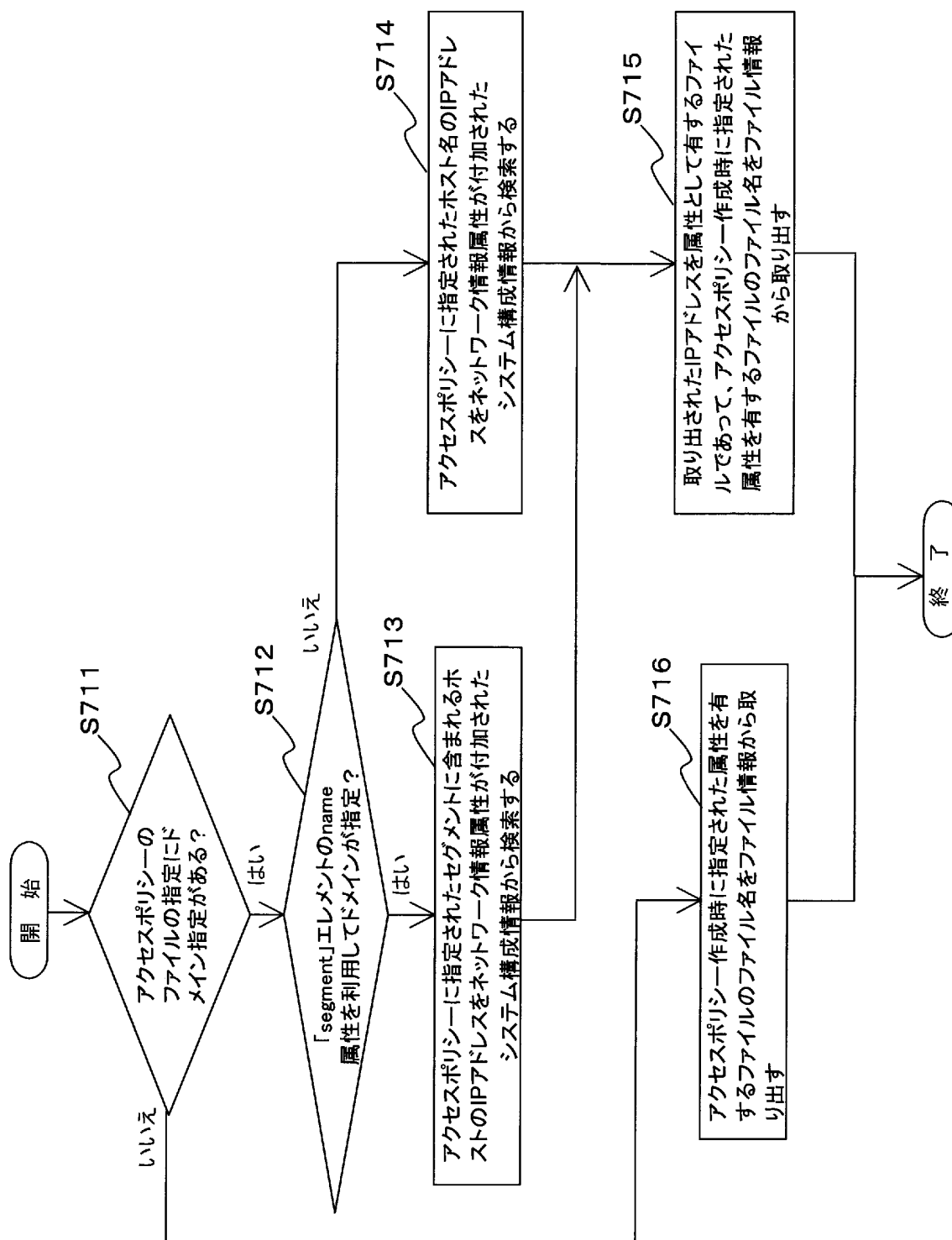
2502

2503

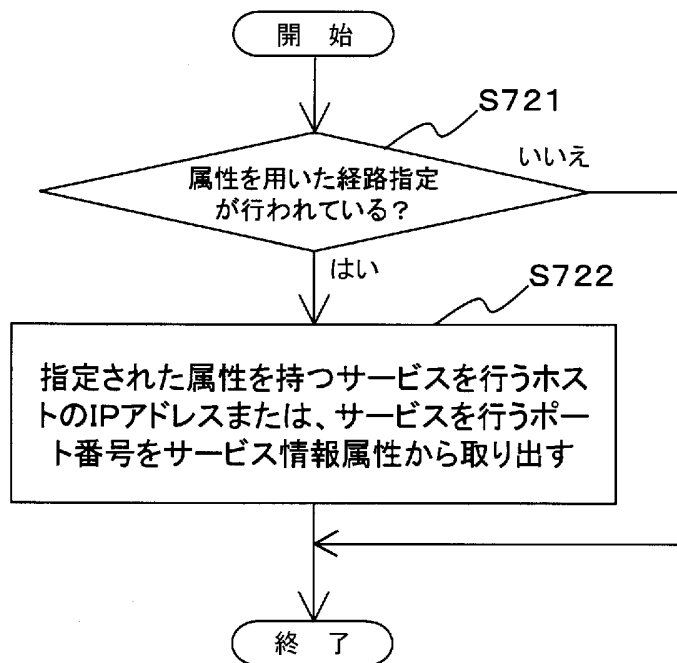
[図88]



[図89]



[図90]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/021674

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/20 (2006.01), **G06F21/24** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/20 (2006.01), **G06F21/24** (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-261788 A (Mitsubishi Electric Corp.), 13 September, 2002 (13.09.02), Full text; all drawings & US 2003/0115313 A1	1-13
Y	JP 2004-139292 A (Hitachi, Ltd.), 13 May, 2004 (13.05.04), Par. No. [0058] (Family: none)	1-13
A	JP 2000-253066 A (Lucent Technologies Inc.), 14 September, 2000 (14.09.00), Full text; all drawings & US 2003/0120955 A1 & EP 001024627 A2	1-13

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
05 January, 2006 (05.01.06)Date of mailing of the international search report
24 January, 2006 (24.01.06)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/021674

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-173301 A (Hitachi, Ltd.), 20 June, 2003 (20.06.03), Full text; all drawings (Family: none)	1-13

A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G06F21/20 (2006.01), G06F21/24 (2006.01)		
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. G06F21/20 (2006.01), G06F21/24 (2006.01)		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2006年 日本国実用新案登録公報 1996-2006年 日本国登録実用新案公報 1994-2006年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2002-261788 A (三菱電機株式会社) 2002.09.13, 全文全図 & US2003/0115313 A1	1-13
Y	JP 2004-139292 A (株式会社日立製作所) 2004.05.13, 第58段落 (ファミリー無し)	1-13
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願 の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 05.01.2006	国際調査報告の発送日 24.01.2006	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 永野 志保 電話番号 03-3581-1101 内線 3546	5S 3350

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2000-253066 A (ルーセント テクノロジーズ インコーポレーテッド) 2000. 09. 14, 全文全図 & US 2003/0120955 A1 & EP 001024627 A2	1-13
A	JP 2003-173301 A (株式会社日立製作所) 2003. 06. 20, 全文全図 (ファミリー無し)	1-13