様式 C-19

# 科学研究費補助金研究成果報告書

平成２１年　６月　４日現在

研究種目：基盤研究（C）
研究期間：2006～2008
課題番号：18500050
研究課題名（和文）ネットワークアクセス検査装置の設定診断システムの研究

研究課題名（英文）　A Configuration Diagnosis System for Network Access Inspectors

研究代表者
高橋　直久（TAKAHASHI NAOHISA）
名古屋工業大学・大学院工学研究科・教授
研究者番号：80335083

研究成果の概要：本研究では，安全で安定したネットワークの実現を目指して，ファイアウォールポリシーの診断に関する研究に取り組み，以下の成果を得た．１）空間的関係を用いたファイアウォールポリシーの解析と診断のための新たな方法論を提案，２）上記方法論により従来手法では扱えなかった設定誤りを検出する手法を開発，３）上記手法を用いたファイアウォール診断システムのプロトタイプを実現，４）上記方法論を効率的に実現する手法を開発，５）ポリシーベースの協調による適応型ポリシー制御方式を開発．

交付額

（金額単位：円）

| | 直接経費 | 間接経費 | 合　計 |
|---|---|---|---|
| 2006 年度 | 1,200,000 | 0 | 1,200,000 |
| 2007 年度 | 1,200,000 | 360,000 | 1,560,000 |
| 2008 年度 | 1,100,000 | 330,000 | 1,430,000 |
| 年度 | | | |
| 年度 | | | |
| 総　計 | 3,600,000 | 690,000 | 4,190,000 |

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ネットワークセキュリティ，ファイアウォール，パケットフィルタリング

## １．研究開始当初の背景

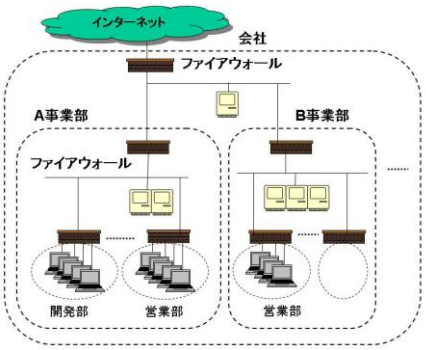


図１　分散型ファイアウォール

安全で安定したネットワークを実現するためには，ネットワークアクセスに対する制御，監視，診断の機能（ネットワークアクセス検査装置，略して NAI(Network Access Inspectors)と呼ぶ）が不可欠である．NAI には，ファイアウォール，パケットキャプチャ，侵入検知システム（IDS）などがある．

ネットワークの規模が大きくなると，図１のように NAI はネットワーク内に多数分散して存在し，それぞれ異なる管理者により設定されるようになる．このような場合には，相互の影響も考慮して注意深く各 NAI の設定ファイルを作成する必要がある．また，実際のネットワークの構成は刻々と変動するので，

管理者はそれに応じて設定を更新しなければならない．このため，NAI の設定を正しく維持する作業は困難であり，豊富な経験を有するネットワーク管理者が多大な時間を費やしても，NAI 設定に矛盾，不足，冗長などの異常が発生し，いわゆるセキュリティホールが発生する場合がある．実際，企業等で実運用されているファイアウォールの設定を調べた結果として，ファイアウォールの設定誤りにより，通過すべき通信を通過させていないなどの状況が数多く発生していることが報告されている．

本研究では，このような問題に対処するため，NAI の設定異常の究明を助ける基盤技術の開発に取り組む．

## ２．研究の目的

従来，ネットワークの制御，監視，診断の機能(NAI)を用いるためには，NAIの動作を一連のルール（ポリシーと呼ぶ）として設定する．ポリシーは，一般に計算機プログラムと同様に逐次的に解釈実行されるため，ネットワーク管理者は，NAIの動作手順を詳細に追いかけて，その妥当性を検証しなければならない．ネットワークの規模が大きくなり複雑化するに従い，これらの作業も複雑になる．また，多数の管理者の共同作業となるため，複数の装置での設定の矛盾や設定のもれが生じる場合がある．

本研究では，ネットワークのアクセス制御方針（セキュリティポリシー）や実ネットワークの構成などネットワークアクセス検査装置（NAI）の設定に係わる情報を有機的に結合させてファイアウォールポリシーを診断して設定異常を検出するシステムの実現技術を開発することを目的とする．

## ３．研究の方法

本研究では，ネットワーク全体のアクセス制御方針を抽象度の高いセキュリティポリシーとして宣言的に記述して,図２のように，①セキュリティポリシーとファイアウォールの設定の間の整合性検査，②ファイアウォールの設定間での整合性検査，③ファイアウォール内のフィルタ間の関係の検査を中心にファイアウォールポリシーの診断及びポリシーベースの協調方式に関する研究を進める．

具体的には，以下ように研究を進める．

（１）ファイアウォールポリシーの解析と診断のための新たな方法論の探求

（２）上記方法論により従来手法では扱えなかった設定誤りを求める手法の開発

（３）上記方法論を用いたファイアウォール診断システムの実現

（４）上記方法論を効率化する手法の開発

（５）ポリシーベースの協調方式の開発

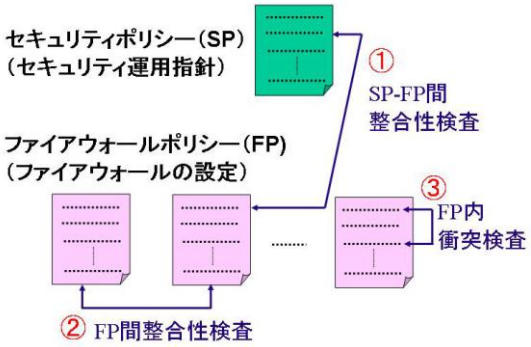


図２　ファイアウォールポリシーの診断

## ４．研究成果

### ４．１　空間的解釈に基づくファイアウォールポリシーの診断方式の提案

設定誤りを自動的に検出してファイアウォールポリシーを正しく維持管理するための新たな方法論 SPREAD (SPatial-RElation-based Analysis and Diagnosis for firewall policies)を提案した．SPREAD では，ファイアウォール設定の基本となる IP パケットフィルタを取り上げ，図３のように全てのフィルタの意味を空間的に表現し，図４のようなフィルタ間の空間的関係を求めて，ファイアウォールポリシーを分析診断する．

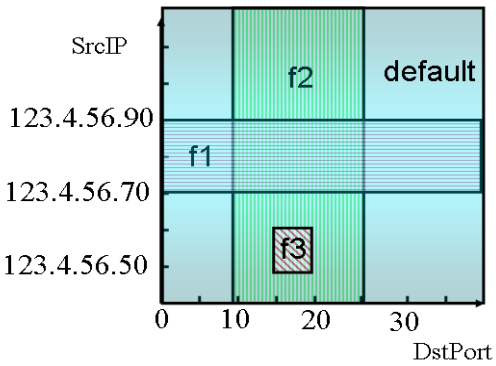


図３　パケットフィルタの空間的解釈

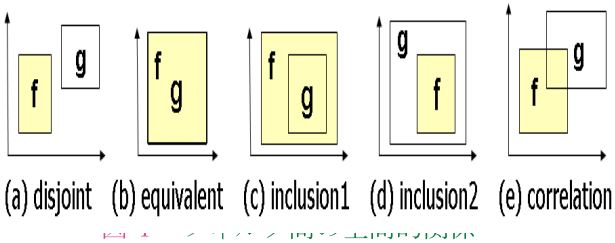


図４　フィルタ間の空間的関係

図３をみると，f1，f2 のフィルタ空間の一部に重なりがあることがわかる．また，f3 のフィルタ空間が f2 のフィルタ空間に完全に包含されていることがわかる．このようにフィルタ空間に重なりがある場合には，これら

のフィルタにより共通して指定されるパケットが存在する．このようなパケットに対しては，先に評価されるフィルタ（先行フィルタと呼ぶ）のアクションが施され，後から評価されるフィルタ（後続フィルタと呼ぶ）のアクションは施されることはない．このような場合に，後続フィルタに対して先行フィルタによるコンフリクトが生じたという．f3 に対して f2 により生じるコンフリクトでは，どのようなパケットに対しても f3 のアクションは決して施されることはない．このようなコンフリクトは設定誤りの結果生じたものである．一方，f2 に対して f1 により生じるコンフリクトでは，f2 が指定するパケットの一部は f2 のアクションが施される．f2 をこのようなパケットだけを指定するように変更すれば，コンフリクトは生じない．しかし，f2 の記述が複雑になる，あるいは，複数のフィルタに分割しなければならないという事態が生じる．ネットワーク管理者が，このような問題を回避するために敢えてコンフリクトを生じるように f2 を記述することもあるので，このようなコンフリクトは設定誤りとはいえない場合もある．しかし，この場合でも，意図的にコンフリクトを生じさせたのか，設定誤りか確認するため，ネットワーク管理者にコンフリクトが生じていることを通知する必要がある．

SPREAD は，副作用分析，等価性判定，合成分析の３つの機能を有する．副作用分析機能は，ファイアウォールポリシーに，あるフィルタを追加したときに，その影響により決して実行されないフィルタが発生するなどの設定異常を検出する．等価性判定機能は，ファイアウォール機器を入れ替える場合に，新旧機器のファイアウォール設定の内容をまとめて解析し，相違点がある場合に明示する．合成分析機能は，複数のファイアウォールが階層的に存在する場合に，上流と下流のファイアウォール設定の間の矛盾や冗長などの設定異常を求める．

### ４．２　先行フィルタの組み合わせにより生じるコンフリクト検出手法の開発

従来手法では対象とすることができなかった，複数のフィルタの組み合わせによる影響により決して実行されないようなフィルタが発生するなどの設定異常に対して，SPREAD を適用する手法を開発した．これにより，ファイアウォールの設定誤り検出技術の適用領域を拡大した．

図５のような空間的な関係をもち，フィルタ *f1* と *f2* が，フィルタ *g* の前に評価されるようなフィルタ系列を考える．*f1*，*f2* は，それぞれ g と一部に重なりがあるが，これだけでは，*g* が決して実行されないとはいえないので，設定エラーと断定できない．しかし，図５より，フィルタ *g* のフィルタ空間が，フィルタ *f1* と *f2* のフィルタ空間の和に包含されることが分り，設定エラーであると断定できる．

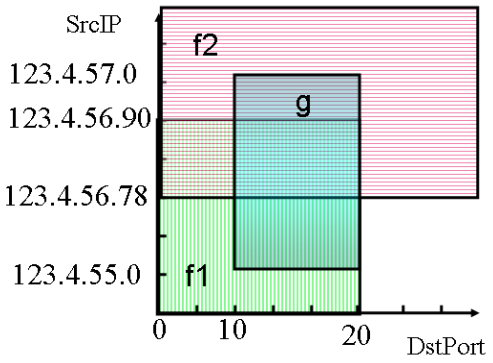


図５　フィルタの組み合わせによりコンフリクトが生じる例

### ４．３　フィルタ逆引きシステムの開発

パケットフィルタリングシステムでは，フィルタが，そのフィルタのアクションを施す対象となるパケットを定めている．このため，フィルタ系列からフィルタを読み出すと，そのフィルタが対象としているパケットを知ることができる．このような作業をフィルタの意味を調べる操作とみなすと，辞書で単語を調べる操作と同様となるので，フィルタ正引きと呼ぶ．一方，次のように，ある特定のパケットから，それらのパケットを対象とするフィルタを求める操作は，辞書の逆引きのように捉えられるので，フィルタ逆引きと呼ぶ．フィルタ逆引きは，たとえば，自分のホストから特定の外部サーバにパケットを送ることができない，あるいは，自分のホストが受信するはずのパケットが来ないといったトラブルが生じた場合に，その原因を調べる作業を助ける．すなわち，フィルタ逆引き機能は，注目するパケットから，そのパケットを棄却するように記述されたフィルタ，あるいは，通過させるように記述されたフィルタを求める．

本研究では，SPREAD を用いてフィルタ逆引きシステムを実現した．これにより，ファイアウォール診断のための実用的なシステムの実現法が提示された．

### ４．４　トポロジー方式による効率化

SPREAD は，空間分割型高速パケット分類器の原理をもとに開発したため，フィルタ間の空間的関係のうち，幾何的関係(ジオメトリー)を用いている．すなわち，パケット空間上でのフィルタの位置と図４のような空間的位相関係（トポロジー）を用いている．フィルタ間のコンフリクトの検出では，フィルタの位置は本質的ではないということに着目して，フィルタ間の空間的な関係のうち，ト

ポロジーのみを用いて設定誤りを求める方式を考案した．この方式では，解析の初期の段階で位置情報を排除して，従来方式では異なるデータとして扱っていた解析結果をまとめることにより，解析に必要なメモリ量と計算時間を軽減することが可能になる．この方式によるコンフリクト検出システムを開発し，ジオメトリーを用いた従来方式と比較して有効性を確認した．図６にフィルタ数を変化させたときの計算時間の比較結果を示す．

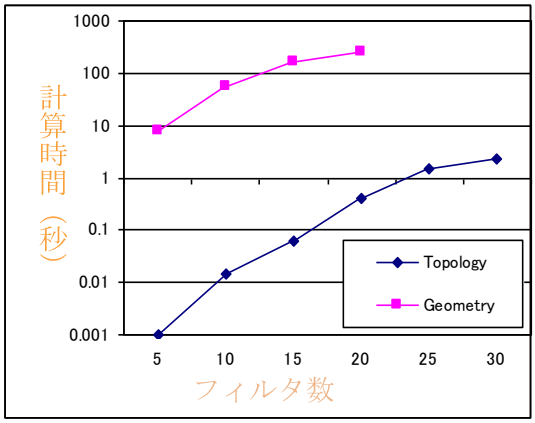


図６　トポロジー方式とジオメトリー方式の比較実験結果

また，本研究では，前記トポロジーを用いて，時限指定のあるフィルタを含むIPパケットフィルタリングの設定異常を診断するシステムを考案し，実現方式を設計した．

４．５　ポリシーベースの協調方式の開発

分散システムでは，ファイアウォール等のセキュリティ管理の他に，トラフィック監視，資源割り付け，データ複製，経路制御など様々な機能モジュールが，互いに関係を持ちながら運用されている．本研究では，各機能モジュールの動作規範をポリシーとして記述して，ポリシーに基づき協調動作を決定し，その妥当性を検証する機構について検討した．

また，ネットワークモニタリングの結果を用いて，モバイルアドホックネットワーク（MANET）のルーティングポリシーを適応的に制御する方式，及び，パケットキャプチャのためのフィルタリングポリシーを適応的に制御する方式を開発し，評価実験により各方式の有効性を明らかにした．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計４件）


① Yi Yin, Yoshiaki Katayama and Naohisa Takahashi, ”Detection of Conflicts Caused by a Combination of Filters Based on Spatial Relationships," IPSJ Journal, Vol. 49, No.9, pp. 3121-3235 (2008).

② Yi Yin, Kazuaki Hida, Yoshiaki Katayama, Naohisa Takahashi, "Implementation of Filter Reverse Search System based on Spatial Relationships of Filters, " Journal of Convergence Information Technology, Vol. 3, No. 2, pp.6-12 (2008).

③ Fang Jing, R.S.Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, “Adaptive Route Selection Policy Based on Back Propagation Neural Networks.” *JOURNAL OF NETWORKS (JNW)*, Vol. 3, No. 3, pp. 34-41 (2008).

④ R. S. Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, "A Framework for an Integrated Co-allocator for Data Grid in Multi-sender Environment," IEICE Transactions on Communications, Vol. E-90-B, No. 4, pp.742-749 (2007).


〔学会発表〕（計１７件）


① Subana Thanasegaran, Yi Yin, Yuichiro Tateiwa, Yoshiaki Katayama and Naohisa Takahashi, "BISCAL: Bit Vector Based Spatial Calculus for Analyzing the Mis-configurations in Firewall Policies," IEICE Technical Report, IA2008-65, pp.101-106 (2009).

② Subana Thanasegaran, Yi Yin, Yuichiro Tateiwa, Yoshiaki Katayama and Naohisa Takahashi, "Topological Approach to Detect Conflicts in Firewall Policies," International Workshop on Security in Systems and Networks, Proc. of 23rd IEEE International Parallel and Distributed Processing Symposium, SSN-1569173665-paper-3.pdf (2009).

③ 殷奕・片山喜章・高橋直久，“セキュリティポリシーとファイアウォールポリシーの不整合検査手法について，”電子情報通信学会 2009 年総合大会講演論文集，A-7-12　（2009）.

④ Subana Thanasegaran・立岩佑一郎・片山喜章・高橋直久，“Detection of Conflicts in Time-Dependent Firewall Policies，”電子情報通信学会 2009 年総合大会講演論文集，A-7-13　（2009）.

⑤ 肥田和明，片山喜章，高橋直久，“ステートフルファイアウォールを有するＬＡＮのためのフィルタ逆引きシステム

の実現，”電子情報通信学会情報ネットワーク研究会 IN2007-153， pp. 65-70 (2008).
⑥ タナセガラン・スバナ，殷奕，片山喜章，高橋直久，“フィルタの空間的関係解析のためのビットベクタ型空間計算法，”平成 20 年度電気関係学会東海支部連合大会，セキュリティ基盤技術 0079 (2008).
⑦ Yi Yin, R. S. Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, "Analysis Methods of Firewall Policies by using Spatial Relationships between Filters," Proc. of IEEE International Conference on Signal Processing Communications and Networking 2007 (ICSCN 2007), Chennai, India, 23-24 Feb. 2007, pp.348-354 (2007).
⑧ Fang Jing, R. S. Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, "Dynamic Route Selection Policy Protocol in MANET," Proc. of IEEE 21st International Conference on Advanced Information Networking and Applications, Niagara Falls, Ontario, Canada 21-23 May 2007, Vol. II, pp. 673-678 (2007).
⑨ Fang Jing, R. S. Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, "Multipath Routing Selection Strategies in Wireless Mobile Ad-Hoc Networks," Proc. of IEEE International Conference on Signal Processing Communications and Networking 2007 (ICSCN 2007), Chennai, India, 23-24 Feb. 2007, pp.117-121 (2007).
⑩ 中村陸，片山喜章，高橋直久，〃フィルタリングポリシをトラヒック特性に適応させる機能を有するパケットキャプチャシステム，〃電子情報通信学会第 18 回データ工学ワークショップ (DEWS2007) 論文集，B7-1 (2007).
⑪ **Yi Yin, R. S. Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, "Inferring the Impact of Firewall Policy Changes by Analyzing Spatial Relations between Packet Filters," Proc. of 2006 IEEE International Conference on Communication Technology, Guilin, China, 27-30 Nov 2006, IEEE Communications Society (2006).**
⑫ R. S. Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, "Coordinated Co-allocator Model for Data Grid in Multi-sender Environment," Proc. of 4th International Conference on Service Oriented Computing, Chicago, USA, 4-7 Dec. 2006, ACM SIGsoft and SIGweb (2006).
⑬ Fang Jing, R. S. Bhuvaneswaran, Yoshiaki Katayama and Naohisa Takahashi, "On-demand Multipath Routing Protocol with Preferential Path Selection Probabilities for MANET," Proc. of IEEE 20th International Conference on Advanced Information Networking and Application, Vol. 2, pp.759-762 (2006).
⑭ R.S.Bhuvaneswaran, Yoshiaki .Katayama and Naohisa Takahashi, “Redundant Parallel Data Transfer Schemes for the Grid Environment,” Proc. of 4th Australasian Symposium on Grid Computing and e-Research (AusGrid 2006) pp. 71-78, (2006).
⑮ 高橋直久，片山喜章，R.S. Bhuvaneswaran，“データグリッドのためのポリシーベースの協調モデル”第 23 回日本ソフトウエア科学会大会，「情報爆発」特別セッション，1A-3，9 月 13-14，東京大学 (2006).
⑯ 肥田和明，片山喜章，高橋直久，“複数ネットワークアクセス検査装置を有するＬＡＮのためのフィルタ逆引きシステムの実現，”マルチメディア，分散，協調とモバイルシンポジウム (DICOMO2006)， pp. 905-908 (2006).
⑰ 中村陸，片山喜章，高橋直久，〃トラヒック特性に基づく近似機能を有する空間分割型パケットキャプチャシステム，〃電子情報通信学会技術報告情報ネットワーク研究会， IN2006-48， pp. 79-86 (2006).

〔産業財産権〕
○出願状況（計２件）
① 高橋直久，片山喜章，高木麻未，ファイアウォールの制御方式及び設定解析方式，特願2008-31236，2008年２月13日.
② 高橋直久，片山喜章，肥田和明，ステートフルファイアウォール設定解析方式，特願2008-18839，2008年１月30日.

６．研究組織
(1)研究代表者
高橋　直久（TAKAHASHI NAOHISA）
名古屋工業大学・大学院工学研究科・教授
研究者番号：80335083
(2)研究分担者
片山　喜章（KATAYAMA YOSHIAKI）
名古屋工業大学・大学院工学研究科・准教授
研究者番号：10263435