科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　２１　日現在

機関番号：　１３９０３
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００８４

研究課題名（和文）時空間解析に基づくセキュアネットワーキング基盤の研究

研究課題名（英文）A Research on Secure Networking Platforms Based on Temporal and Spatial Analysis

研究代表者
高橋　直久（Takahashi, Naohisa）

名古屋工業大学・工学（系）研究科（研究院）・教授

研究者番号：８０３３５０８３

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：本研究では，ファイアウォールと侵入検知システムの診断に関する研究に取り組み，以下のような成果を得た．１）フィルタ間のトポロジー関係に基づきファイアウォールポリシーを解析･診断する方式を開発，２）時限付きフィルタを有するファイアウォールポリシーの解析手法を開発，３）ファイアウォールポリシーとセキュリティポリシーの整合性解析手法の開発，４）侵入検知システムのルール間の空間的解析手法の開発．

研究成果の概要（英文）：In this research, we have investigated configuration diagnosis systems for firewalls and intrusion detection systems. The followings are main research products: 1) An analysis method for firewall policies based on topological relations between the filters, 2) An analysis method for firewall policies with timed filters, 3) A verification method for consistency between a security policy and a firewall policy, 4) An analysis method for spatial relations between the rules in a configuration file of an intrusion detection system.

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　時空間解析

１．研究開始当初の背景

安全で安定したネットワークを実現するためには，ファイアウォール（FW），侵入検知システム（IDS）など，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 と呼ぶ）が不可欠である．ネットワーク管理者は，セキュリティの運用指針に従って，NAI を正しく設定し，意図した通りに動作させるように維持管理しなければならない．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配置され，それぞれ異なる管理者に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 を設定する必要がある．また，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管理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．

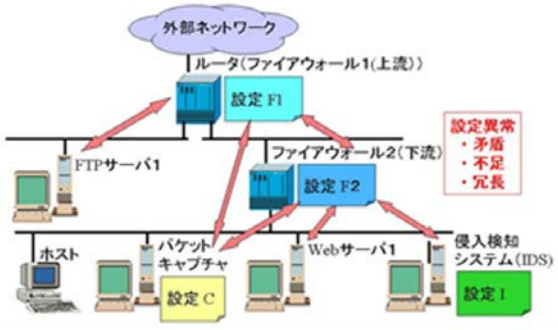


図１　ネットワークアクセス検査装置（NAI）の設定異常

上記問題に対して，ファイアウォールの設定検証手法が提案されている．しかし，セキュリティポリシー内の不整合を検出できない，実ネットワークとの対応を考慮していないため設定の冗長や不足を検出できないなどの問題がある．FW 内の設定誤り検出に関する研究には，フィルタ間の衝突の検出，冗長なフィルタの削除，会話型 FW 解析システムなど多数ある．しかし，いずれも，単一フィルタにより生じる設定誤りの検出に限られている，通信の状態によりフィルタの動作を変化させるステートフルファイアウォールや特定期間だけ特定ポートを開閉する時限付きフィルタなど時間に依存する設定への対応を考慮していない，計算途中で生成するデータ量が多く解析時間が長いなど，多くの問題が残されている．

２．研究の目的

本研究では，フィルタの空間的解釈に基づきファイアウォールを診断する技術を確立する．この技術は，フィルタを空間的に展開して解析することにより，複数フィルタの組み合わせにより生じる設定誤りなど各種誤りを網羅的に検出する．また，時限付きフィルタなどの時間変動を伴うファイアウォール，及び，パケットフィルタの動作が通信状態に依存する場合に対しても適用できるような時空間解析技術を開発し，従来よりも解析精度を向上させる．さらに，ネットワーク監視分析結果に対する記述形式及び変換結合系を開発して，上記解析技術と組み合わせることにより，ファイアウォール，侵入検知システム，侵入防御システムなどセキュリティ関連ツール群を有機的に結合するセキュアネットワーキング基盤を構築する．

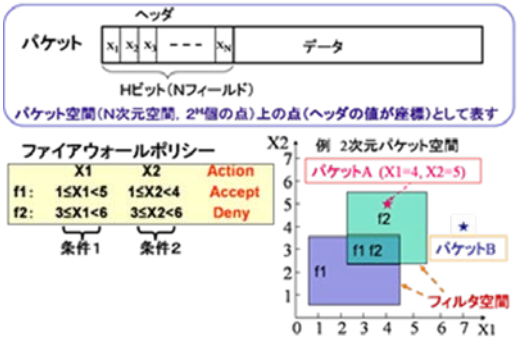


図２　パケット空間とフィルタ空間

３．研究の方法

本研究では，パケットフィルタにおけるキーフィールド数を N としたとき，各キーフィールドの値を座標とする N 次元空間上の点としてパケットを表すような空間（パケット空間と呼ぶ）を考える．このとき，フィルタの条件を，その条件を満たすパケットに対応するパケット空間上の総ての点の集合からなる部分空間（フィルタ空間と呼ぶ）として表すことができる．**図２**は，２つのヘッダフィールドを用いてフィルタの条件部を記述したファイアウォールポリシーから２次元パケット空間を構成した例である．

パケット空間上に２つのフィルタ空間を表すと，フィルタ間の空間的関係が得られる．**図３**の（ｂ）から（e）のように，２つのフィルタ空間に交わりがある場合，衝突があるといい，フィルタを誤って設定した可能性がある．たとえば，**図３**の（ｂ）の場合には，フィルタｆとｇのフィルタ空間は同じであり，フィルタ系列で下方に記述されているフィルタのアクションは決して実行されない．本研究では，これら空間的関係を用いてフィルタの衝突や設定異常の検出機能を実現する．

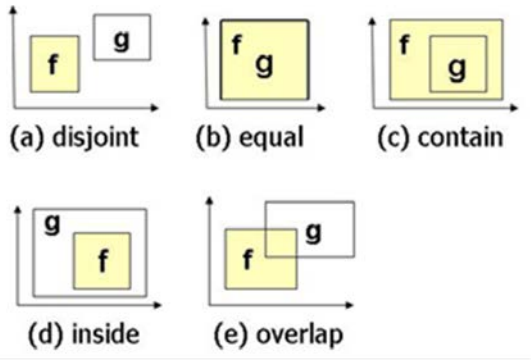


図３　フィルタ間の空間的関係

本研究では，上記のような空間的関係の解析を基礎に，次のように研究を進めて，ファイアウォール，侵入検知システムなどのネットワークアクセス検査装置（NAI）を有機的に結合するセキュアネットワーキング基盤を構築する．

（１）トポロジーに基づくフィルタ間の空間的関係解析手法の開発

（２）時限付きフィルタのための空間的関係解析手法の実現

（３）セキュリティポリシーとファイアウォールポリシーの整合性解析手法の開発

（４）侵入検知システム（IDS）のルール間の空間的関係解析手法の開発

４．研究成果

４．１　トポロジーに基づくフィルタ間の空間的関係解析手法の開発

報告者らは，これまでに，パケットのヘッダの値を座標とするパケット空間上にフィルタの意味を表現し，パケットを空間的に解釈して高速に分類する手法を提案した．また，これを，フィルタ系列の空間的解釈によりファイアウォールの設定誤りを検出する手法に発展させた（．この手法では，フィルタ間の空間的関係により，不足や冗長なフィルタと，他のフィルタと矛盾のあるフィルタを検出する．

本研究では，上記手法を，トポロジーに着目して，改良することにより，メモリ量と計算量を削減する方式を開発した．この方式では，**図４**のように，パケット空間において，フィルタ空間の重なりを調べて，空間を分割する．次に，各部分空間に対して，その空間を覆うフィルタ空間を表すビットベクターVを求める．ある，部分空間をフィルタ f_iが覆っているとき，その空間に対するVの第iビットを１とし，そうでないときは０にする．たとえば，図において，3≦SrcIP＜5，3 ≦DesIP＜４の部分空間は，フィルタ f_0と f_1の空間に覆われているので，V=[1100]となる．

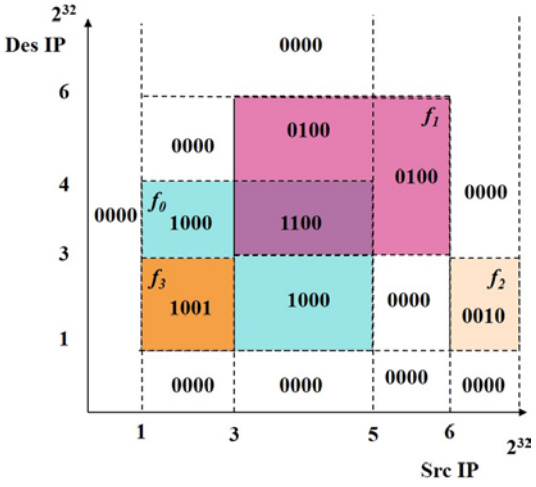


図４　BISCALを用いた部分空間の表現

本研究では，フィルタのトポロジー関係をVであらわし，Vを用いたビットベクター演算系 BISCAL(Bit-Vector Based Spatial Calculus)を設計した．また，BISCALを用いて，N次元空間でのフィルタ間のトポロジー関係を包括的に求める手法を開発した．また，従来のジオメトリーに基づき空間的関係を求める手法に比べて，本手法は，メモリ量と計算時間に関して優れていることを実験的に確認した．**図５**に，従来方式（ジオメトリー方式）と提案方式（トポロジー方式）で必要なメモリ量の比較実験の結果の例を示す．

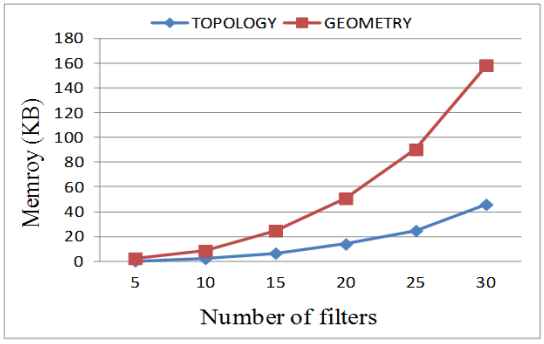


図５　メモリ量に関する比較実験

４．２　時限フィルタのための空間的関係解析手法の拡張

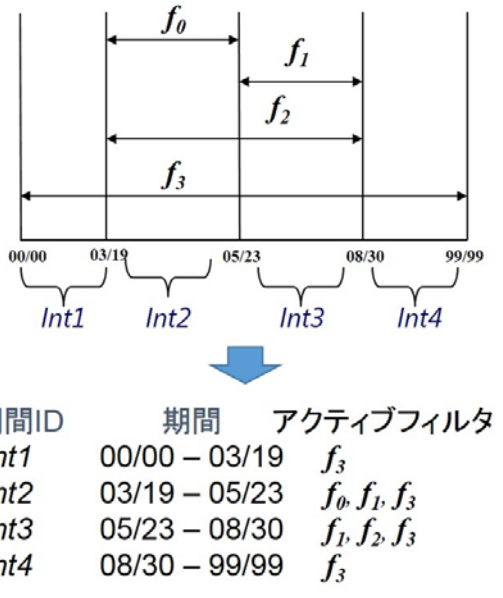
ある特定のイベントの開催期間中だけポートを開けて，外部から内部のサーバへのアクセスを許可したいという場合には，**図６**のStartとStopの値で定められるような有効期間が指定されたフィルタ（時限フィルタ）を用いる．たとえば，図の f_1は，2012年３月１９日の１０：００から，５月２３日の２０：００までの間は，129.6.48.*から123.4.5.*宛のパケットを通過させる．このような時限付きフィルタを有するファイアウォールにおいて，従来の空間的解析では，フィルタの

有効期間を考慮しないため，本来コンフリクトのないフィルタ対に対して，コンフリクしていると判定して，冗長であるなどの誤りを通知していた．

本研究では，このような時限フィルタを有するファイアウォールにおいて，有効期間を考慮して，フィルタ間のコンフリクトを検出する手法を開発した．この手法では，まず，**図７**のように，各フィルタの有効期間の重なりを調べて，時間帯を分割し，各期間と有効期間が重なるフィルタ（アクティブフィルタという）を求める．次に，各期間ごとに，アクテイィブフィルタの間の空間的関係を調べて，コンフリクトを検出する．フィルタの有効期間を考慮することにより，従来よりも誤ってコンフリクトがあると判定する割合を減らすことが可能になる．

	SrcIP	DesIP	Start	Stop	Action
f_0:	129.6.48.*	123.4.5.*	2012/03/19/10/00	2012/05/23/20/00	Accept
f_1:	129.6.48.5	123.4.5.9	2012/03/31/17/00	2012/08/30/17/00	Deny
f_2:	129.6.48.25	123.4.5.*	2012/04/03/20/00	2012/04/25/20/00	Accept
f_3:	*	*	0000/00/00/00/00	9999/99/99/99/99	Deny

図６　時限付きフィルタの例



期間ID	期間	アクティブフィルタ
Int1	00/00 – 03/19	f_3
Int2	03/19 – 05/23	f_0, f_1, f_3
Int3	05/23 – 08/30	f_1, f_2, f_3
Int4	08/30 – 99/99	f_3

図７　アクティブフィルタの導出

評価実験では，毎日定時に有効期間を設定するような場合には，**図８**のように，誤りや警告を発する割合が1/16から1/2に減らすことができるという結果が得られた．

また，本研究では，上記のように毎日定時の時間帯，毎週指定曜日の指定時間帯など，有効期間を周期的に繰り返すような時限フィルタを有するファイアウォールに対して，周期性を考慮して，フィルタ間の空間的関係を効率的に求める手法を開発した．

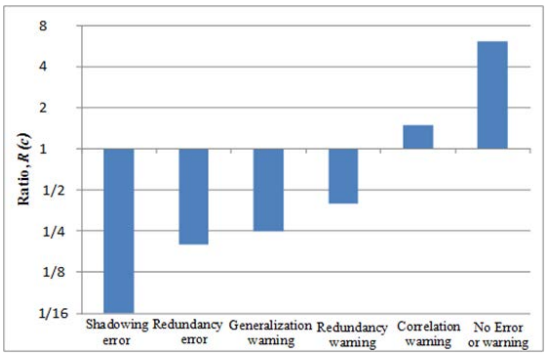


図８　時間の考慮による誤りと警告の削減

４．３　セキュリティポリシーとファイアウォールポリシーの整合性解析手法の開発

本研究では，セキュリティポリシーに記述されたルールの系列と，ファイアウォールのフィルタ系列との間の空間的関係を求める問題を制約充足問題（CSP）として定式化した．また，神戸大学で開発されたSAT型CSPソルバーSugarを用いて，２つの系列の空間的関係を求めて，整合性を解析するシステムを開発した．

４．４　侵入検知システム（IDS）のルール間の空間的関係解析手法の開発

IDSのルールは，ルールアクションとシグネチャからなる．ルールアクションでは，シグネチャにマッチした場合に，警告やログ記録など，どのような動作をとるべきかを指定する．シグネチャは，ヘッダ条件とペイロード条件からなる．ルール r_i のヘッダ条件とペイロード条件の両方を満たすパケットが到着すると，ルール r_i のルールアクションを行う．

本研究では，ファイアウォールのフィルタ間の空間的関係と同様に，ルール r_i と r_j のシグネチャにマッチするパケットの集合の包含関係を調べて，５つの空間的関係に分類する．このような空間的関係は，ヘッダ条件を満たすパケット集合の包含関係と，ペイロード条件を満たすパケット集合の 包含関係から求められる．前者は，ファイアウォールのフィルタ間の空間的関係と同じであり，すでに計算法が開発されている．このため，本研究では，主に後者を求める方式に取り組んだ．

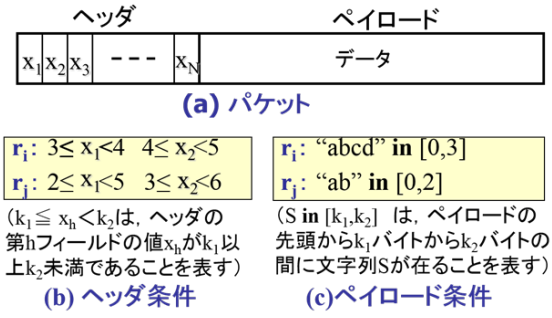


図９　対象とするルールの記述法

ここでは，最初の段階として問題を簡単化し，**図９**のような，ヘッダ条件とペイロード条件からなるルールを対象とした．すなわち，ペイロード条件が，ペイロードに含まれる一つの文字列とその位置の範囲だけである場合について検討した．このような場合について，ペイロード条件を満たすパケット集合の包含関係を求め，ルール間の空間的関係を求める手法を開発した．また，空間的関係に基いて，ルールを分類して，ルールセットの実行制御に用いる手法を開発した．

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３件）
①Subana Thanasegaran, Yuichiro Tateiwa, Yoshiaki Katayama, Naohisa Takahashi: A Mapping Mechanism for Periodic Filters in a Conflict Detection System for Time-Based Firewall Policies, International Journal of Computer Science and Network Security, Vol. 12, No. 4, pp.29-36 (2012/4).
②Thanasegaran Subana, Yuichiro Tateiwa, Yoshiaki Katayama, Naohisa Takahashi, : A Topology-Based Conflict Detection System for Firewall Policies using Bit-Vector-Based Spatial Calculus, IJCNS: International Journal of Communication Network and System Sciences, Vol.4, No.11,pp.683-695, 2011/11.
③Thanasegaran Subana, Yi Yin, Yuichiro Tateiwa, Yoshiaki Katayama, Naohisa Takahashi: Design and Implementation of Conflict Detection System for Time-based Firewall Policies, JNIT: International Journal of Next Generation Information Technology, Vol.2, No.4, pp.24-39, 2011/11.

〔学会発表〕（計７件）
①井上 和哉, 片山 喜章, 高橋 直久，複数のIDSを用いたログ解析によるネットワーク診断システムについて，マルチメディア，分散，協調とモバイル(DICOMO2014)シンポジウム，2014/7（発表予定）.
②立岩 佑一郎, 高橋 直久，仮想マシンを用いたネットワーク構築演習におけるトレースに基づく答案評価システムの提案，マルチメディア，分散，協調とモバイル(DICOMO2014)シンポジウム，2014/7（発表予定）.
③Dong Xinming，立岩佑一郎，片山喜章，高橋直久，ルールセットの構造化に基づく侵入検知システムの高速化，第５回データ工学と情報マネジメントに関するフォーラム（DEIM2013），2013/3.
④ Yi Yin, Jiangdong Xu and Naohisa Takahashi, Verifying Consistency between Security Policy and Firewall Policy by Using a Constraint Satisfaction Problem Solver, 2011 International Conference on Future Wireless Network and Information Systems, Lecture Notes in Electrical Engineering, LNEE 144, Vol2. pp.135-145, 2012.
⑤大見浩明，立岩佑一郎，片山喜章，高橋直久, "フロークラスター記述言語を有するネットワークトラヒック検査システムの提案", 情報処理学会第 74 回全国大会，4X-5，2012/3.
⑥青木滋, 立岩佑一郎, 片山喜章, 高橋直久, "侵入検知機能を用いたフロークラスター診断システム", 情報処理学会第 74 回全国大会，4X-6，2012/3.
⑦長谷川皓一，立岩佑一郎，片山喜章，高橋直久, "ＬＡＮ接続機器の配置図管理補助システムの実現について"，情報処理学会第 74 回全国大会，4X-8，2012/3.

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）連携研究者
片山喜章（KATAYAMA YOSHIAKI）
名古屋工業大学・大学院工学研究科・教授
研究者番号：10263435
立岩佑一郎(TATEIWA YUICHIRO)
名古屋工業大学・大学院工学研究科・助教
研究者番号：30534367