川崎医療福祉学会誌　Vol. 14　No. 2　2005　403–407

短　報

ビジュアライゼーション技法による パケットフィルタリングの設計 —保健医療分野におけるネットワークセキュリティの考察—

三上史哲[*1]　田中昌昭[*2]　太田　茂[*2]

はじめに

近年，医療機関において，患者情報など非常に秘匿性の高い個人情報がネットワークを前提とした病院情報システムで取り扱われている．そのため，これらの情報を保護するためのネットワークセキュリティ対策は重要な課題となっている．ネットワークセキュリティ対策には，ファイアウォール技術，暗号技術，ユーザ認証技術，ウィルス対策技術など様々な技術が必要となるが，いずれも高度な専門的知識が要求されるため，専任の管理者の配備が望まれる．しかしながら，医療費抑制の施策が進行するなか，多くの医療機関において，不採算部門であるネットワーク管理部門に人的・経済的な投資を行う余裕がないのが現状で，ネットワークの専門家ではない職員が本来の業務のかたわらでネットワークの管理を行っているケースが多く見受けられる．今後，電子化が進むにつれて，情報漏洩等の事故が起きると大きな社会問題になる可能性があり，医療不信を増長しかねない．

このように，扱う情報が極度に秘匿性が高いにもかかわらず専任のスタッフを配備する余裕がないという医療分野の特殊性を鑑み，筆者らは経験の浅い管理者でも必要最低限のネットワークセキュリティ対策を講じることができるような支援策を検討してきた．その際，要求分析におけるデータ・フロー・ダイアグラム（DFD）やデータベース設計におけるE–R図など，図式表現を用いて対象を可視化することにより関係者の間で概念を共有し，問題点の顕在化を容易にするビジュアライゼーション技法が有効であると考え，これをネットワークセキュリティ対策の土台となるファイアウォール技術の中でもとりわけ基本的な技術であるパケットフィルタリングへの適用を試みた．

本稿では，筆者らが考案した，ビジュアライゼーション技法によるパケットフィルタリングの設計支援手法であるパケット・フィルタリング・ダイアグラム（PFD）についてその概要を述べるとともに，オブジェクト指向技法を用いて実装を行い，その有効性について検討を行ったので報告する．

背　景

1．ビジュアライゼーション技法

システム開発時におけるデータベース設計やプログラミングなどの抽象的な概念，大量の数値データや文章からの情報など，一目では理解できない複雑なデータや概念を図式化して可視化することにより，第三者への情報伝達が効果的になるが，これをビジュアライゼーション技法と呼ぶ．我々が日常でよく見かけるものでは，数値データのグラフ化や表作成もビジュアライゼーション技法の一つである．システム開発においては，データの流れに注目してシステムを記述するDFDやシステムが扱うデータのグループ化やデータ間の関係を記述するE–R図があるが，これらのビジュアライゼーション技法もシステム開発者と業務担当者の間のコミュニケーションを促進するツールとして利用されている．また，図式化することにより，システムの全体像が把握できるため，システム完成後に不具合があった場合などの検証時にも有効である．

ビジュアライゼーション技法を利用した研究として，ビジュアライゼーション技法とテキストマイニングを用いてネットワークのログ情報を調査・解析するシステムの開発研究[1)]や論文理解のためのチャートを考案した研究[2)]などがあり，様々な領域でビジュアライゼーション技法が注目されている．

2．パケットフィルタリング

パケットフィルタリングは，外部ネットワークからの不正アクセスやハッキング行為を防ぐとともに，内

*1 川崎医療福祉大学大学院　医療技術学研究科　医療情報学専攻　*2 川崎医療福祉大学　医療技術学部　医療情報学科
（連絡先）三上史哲　〒701-0193　倉敷市松島288　川崎医療福祉大学

部ネットワークから外部ネットワークへの同様の行為も防ぐことができるファイアウォール技術の一つである.この他のファイアウォール技術にはアプリケーションゲートウェイがある．パケットフィルタリングはトランスポート層以下の下位層でのファイアウォールの実現方法であり，パケットの送受信 IP アドレス，ポート番号，プロトコル等を調べて，通信の許可・不許可を決定する．一方，アプリケーションゲートウェイはアプリケーション層でのファイアウォールの実現方法であり，個々のアプリケーションのプロトコルに依存するが，プロトコル内部の解釈を行い，通信の許可・不許可，書き換え，転送などを行う．したがって，アプリケーションゲートウェイの方が，細かい制御が行えるという利点があるが，個別対応になるので対応していないプロトコルはファイアウォールを通過できないという問題がある．一般的に，最低でもパケットフィルタリングは必ず行い，必要に応じてアプリケーションゲートウェイを設けるという方法が採られており，本研究は，必須となるパケットフィルタリングを対象とした．

パケットフィルタリングの問題点として

1） 設定方法が機種毎に異なり，しかも低水準コマンドの羅列で記述され，またルールの適応順にも考慮しなければならないなど，設定方法が複雑で，適切な設定をするのが難しい．

2） ルール設定後の検証が難しい．

などが指摘されている[3]．

本研究ではビジュアライゼーション技法を応用してこれらの問題点を解決し，容易に適切なパケットフィルタリングの設定が可能になることを目的としている．類似研究として，論理記号及び論理演算を使用してパケットフィルタリングの設計・検証を行う手法が提案されている[4]．しかし，この手法では，ルールを論理演算の集合として記述しているため，ルールの適応順が考慮されていない．本研究では，パケットの流れに着目してパケットフィルタリングを図式化することにより，設計の過程で自然にルールの適応順を考慮できるようにした．

設計の要点

本研究における設計の要点は以下の 2 点である．

1） ネットワーク構築の対象である実世界（医療機関におけるセキュリティ方針）の特徴を的確に捉えた構造的な表現であり，容易に実装技術ベースの設計へと転換可能なもの．

2） 業務専門家 (ネットワークの非専門家) でも，わずかな努力で理解可能なもの．

この 2 点を満たすものとして PFD（パケットフィルタリング・ダイアグラム）を考案した．PFD は，パケットフィルタリングの個々のルールを図式表現したものである．ついで，オブジェクト指向技法を用いて PFD によって記述されたセキュリティ要件をモデル化した．

システムの詳細

1．PFD

PFD は，システムやプログラムの機能を概要から詳細へと段階的に記述する技法である HIPO（Hierarchy plus Input Process Output）を参考にし，PFSC（Packet Filtering Specification Contents），総括 PFD，詳細 PFD から構成される構造化ドキュメントとした．PFD の構成を図 1 に示す．

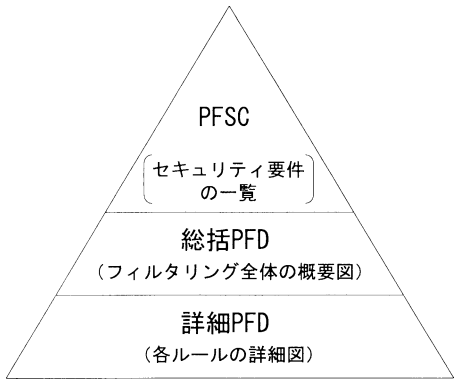


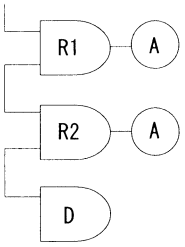
図 1　PFD 構成図

PFSC は HIPO における図式目次に相当するもので，パケットフィルタリングの仕様の目次となる．以下の例が示すように，セキュリティ要件の一覧となる．

- 基本的には全てのパケットを拒否する．
  ただし，
- 内部 LAN から Web は利用できる．
- 内部 LAN からメールは利用できる．
- SSH の通信はできる．

総括 PFD は HIPO における総括ダイアグラムに相当するもので，パケットフィルタリングの仕様の概要を図示したものである．パケットの流れを表す図とフィルタリング条件の一覧を表す表のセットでフィルタリングの全体像を記述する．PFSC が「Web のみ利用可能」である場合の総括 PFD は図 2 のようになる．

図の実線はパケット，「R1」,「R2」はフィルタリングの条件，「A」は条件が一致した場合に行う処理 (例では ACCEPT) を意味している．この例の場



ルール

ルール	プロトコル	Dポート	Sポート	Iインタフェース	Oインタフェース	Dアドレス	Sアドレス	ターゲット
R1	tcp	80	any	eth1	any	any	any	ACCEPT
R2	tcp	any	80	eth0	any	any	any	ACCEPT

デフォルト

DROP

図2　総括PFD

合，まず「R1」にパケットを入力し，パケットと条件を比較して，条件に一致した場合は「A」にパケットが送られる．条件に一致しなかった場合は「R2」にパケットが送られ，「R2」の条件との比較を行う．最終的にどの条件にも一致しなかった場合は「D」（Default）で指定された処理を行うことになる．なお，表には各条件の詳細と条件に一致した場合の処理を記述する．

詳細PFDはHIPOにおける詳細ダイアグラムに相当するもので，パケットフィルタリングの個々のルールを詳細に図示したものである．図2に示した総括PFDに対応する詳細PFDは図3のようになる．

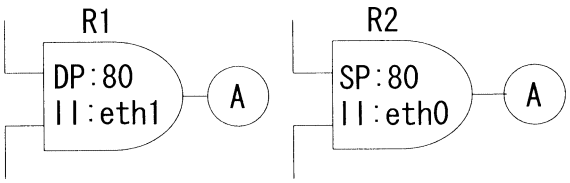


図3　詳細PFD

2．PFDのモデル化

PFDで記述されたセキュリティ要件を，オブジェクト指向技法を用いてモデル化した．図4に考案したモデルのクラス図を示す．

詳細PFD(図3)で示される個々のルールをRuleクラス，総括PFD(図2)で記されるパケットフィルタリング全体の要件をFilterクラス(Ruleクラスの集合)としてモデル化した．LinuxのNetfilterやFreeBSDのIP Firewallなど，機種に依存するパケットフィルタリングの実装コマンドの出力は，動作環境に左右されないようにするため，Filterクラスを継承したサブクラスによって定義した．Packetクラスはネットワーク中を流れるパケットをモデル化したもので，より現実的なデータで検証を行えるようにするため，UNIX系のOSで多用されるパケットキャプチャツールであるtcpdumpのログからパケットのインスタンスを生成できるようにした．また，Filterクラスに，作成したモデルの実装コマンドを出力するメソッド(CmdPrintメソッド)とフィルタリングの検証が行えるメソッド(Simulateメソッド)を用意した．CmdPrintメソッドの使用例として，図3に示した詳細PFDに対応するNetfilter及びIP Firewallのコマンドを生成した結果をそれぞれ図5 a, bに示す．

期待される効果と今後の課題

PFDの考案により，具体的な実現方法にとらわれることなく，パケットフィルタの抽象的な概念の記述が可能となった．これにより，経験の浅いネットワーク管理者でもその全体像を把握することができ，より適切な設定及び検証が行えるようになることが期待される．

また，オブジェクト指向技法を用いてパケットフィルタの抽象的概念をモデル化したことにより以下の利点が得られた．

1） オブジェクト指向技術の継承によって，個々のフィルタリングの実装を動作環境に依存することなく実現できるようになった．
2） 設計したパケットフィルタリングを作成したモデル上で容易に検証できるようになった．

しかしながら，本研究はまだ完成されたものではなく，現状では以下の問題点が残されている．

1） 実際のパケットフィルタリングではアドレス変換(NAT)を併用することが多いが，今回のモデルにはアドレス変換が考慮されていない．
2） ファイアウォールマシン上にネームサーバなどのサーバプロセスを稼働させる運用を行うことがあるが，本モデルでは入力パケットをサーバプロセスで処理する場合が考慮されていない．

また，PFDはビジュアライゼーション技法であり，CASEツールのように，GUIによるマン・マシン・インターフェースを使った設計を可能にしてこそ初めてその真価が発揮できる．今後は，上記の問題点を解決するとともに，実際に利用可能な開発支援ツールとして完成させ，その有効性を実証していきたい．

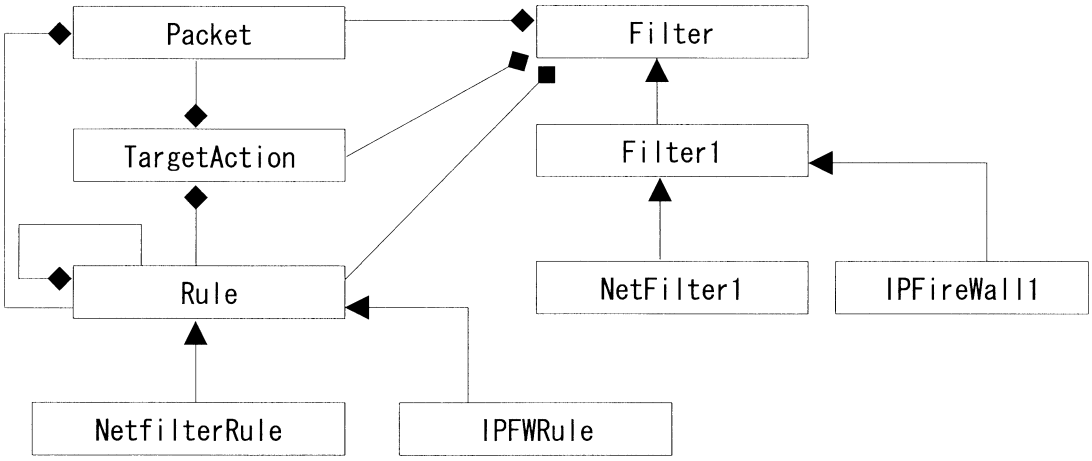


図4　クラス図

```
iptables -t filter -A FORWARD -i eth1 -p tcp --dport 80 ACCEPT
iptables -t filter -A FORWARD -i eth0 -p tcp --sport 80 ACCEPT
```

a) Netfilter の iptables コマンド

```
add allow tcp from any to any 80 recv eth1
add allow tcp from any 80 to any recv eth0
```

b) IP firewall の ipfw コマンド

図5　CmdPrint メゾットで生成したコマンド

考　　察

DFD やE−R図などの例が示すように，要求レベルの抽象的な概念を図式化して可視化することにより，当事者間で仕様を共有したり事前に問題点を発見したりすることが容易になる．一般に，こうしたビジュアライゼーション技法は要件と実装の間に大きな隔たりがあるほど有効な手法である．本研究は，このビジュアライゼーション技法をパケットフィルタリングの設計に適用したものである．

医療機関のセキュリティ要件を実際に実装するには多くの専門的な知識や豊富な経験を必要とするため，そういった技術者を置く余裕のない多くの医療機関にとっては，本研究の「要件と実装の隔たりを埋める」というアプローチは有効と考える．

今回は，パケットフィルタリングにのみ焦点をあてたが，ウィルス対策や侵入検知システムあるいは暗号技術など，その他のセキュリティ技術においても，要件と実装の隔たりを埋めるための技法を考案することは意義のあることである．ソフトウェア工学の領域には UML(Unified Modeling Language) やデザインパターンなどの技法があり，実際に活用されているが，表現の自由度が高すぎて，それらを利用するにはある程度の知識や訓練が必要となり，むしろ DFD やE−R図などのように問題領域に特化した技法の方が敷居が低く，したがって利用されやすい．ネットワークセキュリティの領域においてもこういった技法が体系的に構築されるべきであり，本研究をその出発点にしたい．

本研究は平成15年度川崎医療福祉大学プロジェクト研究費の助成を受けて行った．

文　　献

1）高田哲司，小池英樹：見えログ　情報視覚化とテキストマイニングを用いたログ情報ブラウザ．情報処理学会論文誌，**41**(12)，2000．※1
2）岡孝明，武田英明：論文理解のためのチャート理解支援システム．人工知能学会全国大会第14回論文集，502–505，2000．
3）Elizabeth D.Zwicky，Simon Cooper and D.Brent Chapman：ファイアウォール構築．第2版，O'REILLY，東京，120–121，2002．
4）鶴正人，黒田英夫：パケットフィルタリングの記述法について．情報処理学会研究報告 DSM[分散システム/インターネット運用技術]，**1999**(098)，37-41，1999．※1
5）開米瑞浩：SE のための図解技術．初版，翔泳社，東京，2003．
6）藤代一成：空間，可視化，思想の結晶．情報処理学会研究報告 IM[情報メディア]，**2000**(063)，31–36，2000．※1

※1 下記 URL(情報処理学会電子図書館) よりダウンロード
http://www.bookpark.ne.jp/ipsj/index.asp

（平成16年11月20日受理）

Packet-filtering Design using Visualization Techniques —Consideration of Network Security in a Healthcare Domain—

Fumiaki MIKAMI, Masaaki TANAKA and Shigeru OTA

(Accepted Nov. 20, 2004)

Key words : network security, visualization technique, packet-filtering diagram, sobject-oriented technique, firewall

Correspondence to : Fumiaki MIKAMI　Master's Program in Medical Informatics, Graduate School of Medical Professions, Kawasaki University of Medical Welfare Kurashiki, 701-0193, Japan
(Kawasaki Medical Welfare Journal Vol.14, No.2, 2005 403–407)