Vol.2009-CSEC-47 No.3
2009/12/18

向きを持つマルチレイヤネットワークモデルの提案とセキュリティへの応用

金岡 晃[†1] 原田敏樹[†1]
加藤雅彦[†2] 岡本栄司[†1]

複数機器・複数機能の相互接続により構成されるネットワークシステムは, インターネットが社会に幅広く普及し, さらにクラウドコンピューティングが本格化した現在において必要不可欠の基盤システムである. ネットワークシステムの設計はインターネット黎明期は単純であったが, 利用者の爆発的な増加, 利用形態やユーザニーズの変化, 処理量の増加により年々複雑になっている.

設計に向けた定量的評価を行うために, 著者らはネットワークシステムに対して機器の機能特徴を失うことなく論理的に表現することができるマルチレイヤネットワークモデルを提案した. しかし, 各リンクに向きを考慮していないモデルだったため, 稼働率計算や脆弱性の影響度などを考慮することが難しかった. そこで本論文では, 新たに向きの概念を入れ, さらにノード種別やリンク種別を詳細にしたモデルを提案し, そのセキュリティへの応用を検討する.

Directed Multi-Layer Network Model and its Application for Security

Akira Kanaoka,[†1] Toshiki Harada,[†1]
Masahiko Katoh[†2] and Eiji Okamoto[†1]

Networked systems formed by multiple network equipments are fundation system for widespreading of the Internet, particulary cloud computing environment. Thouhgh designing networked systems was simple in early days of the Internet, it is growing complex by user population explosion, changes of the user demands and platform, and increasing data to process. However, networked system is still designed based on expert knowledge similar in early days of the Internet.

To obtain measurement method of system characteristic for optimum designing, We have proposed a multi-layerd network model which enables to express logically without loss of characteristics for each network equipments.

However, this model is undirected network model, so that it is hard to measure availability and impact of vulnerabilities on a system.

In this paper, we propose new model including directed link, variaty of node and link. Then we discuss about application for security.

1. はじめに

近年のデータセンター事業者やサービスインテグレータ事業者等により提供されるシステムはインターネット黎明期と現在とでは構成が大きく異なり, 一般利用者の爆発的な増加, 利用形態やユーザニーズの変化により処理の複雑化, 処理量の増加が顕著となっている. サービスは機能の異なる複数の機器をネットワークで接続し, 相当な複雑さをもって連動させなければ十分な機能を提供できなくなっている. さらに近年では, クラウドコンピューティングと呼ばれるような, 顧客側がシステム構成を意識することなく, クラウド側が顧客サービスに必要なリソースは適切に設定するというサービスが本格化しつつある.

現状のネットワーク化されたシステム（ネットワークシステム）の設計は経験に大きく依存して行われており定性的であるため, 方法論や理論などの再現性をもった定量的な評価はほとんど行われていない. 定性的な評価によるあいまいさは技術の発展やシステムの安全性を阻害しているといっても過言ではない.

インターネット上の安全に関しては, 大規模ネットワークの安全性に関する研究は多くされてきたが[1)–3)], 大規模ネットワークに接続され実際のサービス提供を行うシステムや組織ネットワークの安全性はそれら研究では担保されず, また大規模ネットワーク研究の結果を小規模ネットワークに直接応用することは難しい. 一方でネットワーク設計の分野でも最適設計に関する研究は盛んであるが[4)–10)], 本研究で対象とするネットワークシステムは, サーバやルータ, スイッチ, ファイアウォール, ロードバランサなど構成機器がそれぞれ異なる機能を提供し, その結合によりひとつのサービスを提供するものであり, 単一機能の機器によるネットワークの設計が主眼である従来研究の成果を用いてネットワークシステムの最適設計を行うことは困難であった. 2008 年に, 金岡らによって提案されたモデル（Networked-system Security Quantification Model, NSQ モデル）は, 従来とは異なり構

†1 筑波大学
University of Tsukuba
†2 株式会社アイアイジェイテクノロジー
IIJ Technology Inc.

成機器がそれぞれの特徴を失うことなく表現されることを可能にしたものであり, これにより最適設計の議論を行う土台が整ったと言える.

本論文では, 複数機器・複数機能の相互接続により構成されるネットワークシステムに対し, これまでに提案された金岡らの NSQ モデルを改良したモデル提案する.

これまでの NSQ モデルでは通信の向きの欠如から稼働率計算や脆弱性の影響度範囲測定などで問題を生じていたが, 提案モデルにより精度の高い稼働率計算や脆弱性の影響度範囲測定を実現可能にした. さらに, モデル上のレイヤ 4 中継器（L4R）からのファイアウォールルール抽出が, 提案モデルにより通信の始点と終点が明確になったことで, 実現可能となった.

本稿の構成は以下の通りである. 第 2 章では関連研究について解説し, その中でも特に本稿の基となる NSQ モデルについては 3 章で解説する. 4 章において NSQ モデルの改良を提案し, 5 章でその利点を論ずる. 最後に 6 章でまとめる.

2. 関 連 研 究

ネットワークの最適設計は古くから行われている研究分野であり, 近年においても, Belotti らが複雑なノードコストを持つネットワークの設計問題についての解法を提案し[4], Chekuri らはフローギャップが単一であるケースでの頑健なネットワーク設計を行い[5], また El-Alfy が MPLS ネットワークにおける最小コストトポロジーを遺伝的アルゴリズムを利用して求めるなど[6], 多くの研究が行われている. しかしこれらの研究が対象としているネットワークはノードの種類が単一であり, 多数の機能を持った機器が相互作用するネットワークの設計を対象にしているものではない. また, 単一のノード種類ではないものであってもレイヤ構造を持つものではないものが多い[7),8].

一方, レイヤ構造を持ったモデルを検討している研究もある. Belotti らは MPLS ネットワークの設計において, 論理的なノードによるネットワークと物理的なノードによるネットワークの 2 階層を考慮した設計手法を提案している[9]. また Dijkstra らは ITU-T G.805 をもとにした多層構造を持つネットワークのモデルを提案している[10] が, 同じく MPLS のモデル化であり, MPLS 機器同士のネットワークはレイヤ構造は持つが単一のノードで構成されているものであることから複数機器の違いを包含可能なモデルとは言えない. 一方, Salvador らは様々な通信が行われるローカルエリアネットワークのモデル化を行っているが, ネットワークトポロジはモデルに含まれずネットワーク全体の機能を抽象化したものとなっている[11].

また, 従来のノード費用やフロー費用を尺度としたネットワーク設計だけでなく, 他の尺度を用いた最適設計の研究も行われている. Habib はネットワーク再設計でのコスト最適化手法を提案し[12], そこでは機器を複数扱うことやポート数やスループット性能, 価格等の属性を適用するなど, 複数尺度での最適化を提案している.

従来はレイヤ構造を持ったモデル化や, ノード種別を複数持つネットワークのモデル化, あるいはフロー費用やノード費用以外の尺度を用いたネットワーク設計手法など, 個々の関連研究は本研究が対象とするネットワークシステムの安全設計に関連するが, すべてを満たすモデルではなかった.

金岡らは, 提案したネットワークシステムのモデルは, これらを満たすべく提案されたマルチレイヤ型のネットワークモデルを提案し, アクセス制御状態の解析や稼働率計算, 脆弱性の影響度などが研究されてきた[13)–21)]. 次章では金岡らのモデルを解説する.

3. NSQ モデル

ネットワークシステム（Networked System）はハブ，スイッチ，ルータやサーバなど複数機能を有する多様な機器で構成される．その設計構築にはコスト，冗長性，セキュリティなど多くの性質が求められるが，これらを満たすためには小規模なシステムでさえその構成は複雑なものとなる．しかしその構築や運用は技術者への経験に依存しており，信頼性の高い自動設計・構築・運用方法に関する学術的な議論はほとんどされていない．そこで，ネットワークシステムの信頼性定量評価のため，複数機能を有するネットワークシステムの新たな表現モデルとして，NSQ モデルが金岡ら[13),21)] によって提案された.

3.1 定　　義

ネットワークシステムを構成する機器が持つ種々の機能は，それぞれ異なる通信層（レイヤ）におけるデータ通信によって実現される．そこで NSQ モデルはこの「レイヤ」の概念を取り入れ，レイヤを 5 つに分類した（図 1）.

各レイヤにはネットワーク機能の単位として「ノード」が存在し，各ノードは「リンク」によって接続される．異なるレイヤ間でノードが接続されたものを「モジュール」と定義し，モジュールは何らかのサービスを提供する S（Service）モジュールとそれらの中継を行う R（Relay）モジュールに大別される．S モジュールは例えば Web サーバやデータベースサーバなどがあり，R モジュールは L2 で中継を行う L2R（L2 スイッチ）や L3 で中継を行う L3R（ルータ）などがそれにあたる．またリンクも，レイヤ間リンクと，レイヤ内リンクが存在する．前者はノードの依存関係を表すものであり，通信は行われないがこのリンクを媒介して情報を届けることが可能である．後者は物理的あるいは論理的な接続を表

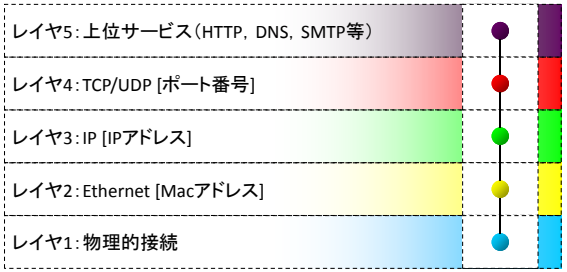

図 1 レイヤ定義

し，通信がなされる．

NSQ モデルを用いることで，ネットワークシステムを構成する各機器はモジュールとして表現され，それぞれの機能特性を失うことなくモデル上に表現可能となった．さらに NSQ モデルを用いて，金岡らはネットワークシステムのデータセットを構築した．そして不必要な通信路の存在による各ノードの次数分布の差を解析し，不必要な通信路を持たないネットワークシステムは，モジュールの構成やノード数に関わらず一定の次数分布を持つことが示された[21]．

一方で，NSQ モデルでは応用が難しいケースもあった．藤堂らによる NSQ モデルを用いた稼働率計算では，NSQ モデルが無向グラフにより実現されていることから正確な稼働率計算法が得られず，別途向きの情報を得る必要があった．また原田らによる脆弱性の影響度測定手法においても，可用性判定においてデータの流れる方向を知る必要があったが，同様に NSQ モデルからは得られなかったため，別途向きの情報を得る必要があった．さらに，モデル表現されたネットワークシステムを現実の機器やサーバに対応させる場合，NSQ モデル上ではノード種別やリンク種別に明確な差異がなかったために，設定情報が正確に生成されないことがあり，NSQ モデルは一定の成果を上げつつも，さらに改良を求められるものとなっていた．

4. モデルの改良

本章では，これまでの NSQ モデルを改良し，これまでモデルでは直接実現が難しかった手法を実現可能にする．なお，本文中ではこれまでに提案された NSQ モデルを「旧モデル」，本稿で提案する改良モデルを「提案モデル」と呼ぶ．

モデルの改良は主に 3 点に分類される

- リンクの有向化
- リンク種別の細分化
- ノード種別の細分化

4.1 各リンクの有向化

旧モデルではリンクは向きを持たなかったが新たに向きの概念を導入する．向きの定義は，リンク種別により異なるため，次節でそれぞれ解説する．

4.2 リンク種別の細分化

旧モデルではリンク種別は「レイヤ内リンク」と「レイヤ間リンク」の 2 種類であった．それを以下の 3 種に分類する．

- 通信路リンク
- 中継リンク
- 依存関係リンク

通信路リンクは同一レイヤでの異なるモジュールに属するノード間を結ぶリンクであり，当該レイヤでの通信路を示すものである．通信路リンクは向きを持ち，通信の方向を示す．レイヤ 2 以上に属する通信路リンクは，当該リンクの始点・終点となるノードの各下位ノード間で到達可能になっていなければ存在できない．

中継リンクはモジュール内で同一レイヤの中継ノード間を結ぶリンクである．中継リンクは向きを持ち，中継の方向を示す．

通信路リンクと中継リンクは，旧モデルで「レイヤ内リンク」として扱われていたものである．

依存関係リンクは、依存関係があるノードを結ぶリンクである。レイヤ間を結ぶことも可能であるがノード間のレイヤ属性値の差は 1 に限る．また依存関係リンクは、依存ノードから被依存ノードへの向きを持つ。

リンクは 2 つの属性を持つ．1 つはレイヤ情報であり，もう 1 つは通信路リンク，依存関係リンク，中継リンクのリンク種別を示す種別情報である．

4.3 ノード種別の細分化

旧モデルではノード種別を持たず単にノードとしていたが，以下のように分類する．

- 終端ノード
- 中継ノード

終端ノードは通信の始点あるいは終点となるノードであり，中継ノードは，通信の始点あ

るいは終点ではないが, 通信を行うにあたりそれら始点のアイデンティティ情報と終点のアイデンティティ情報からデータ配送可否の判断や配送する通信路の決定を行うノードである.

ノードは 3 つの属性を持つ. 1 つはレイヤ情報であり, もう 1 つは終端ノードか中継ノードの種別情報, 最後にアイデンティティ情報である. アイデンティティ情報はシステム内で一意に識別されるための情報であり, IP アドレスや MAC アドレス, ポート番号などが適用される.

レイヤ 2 以上に属するノードは, 必ず 1 階層下のノードと依存関係リンクにより接続されていなければならない.

4.4 モデルによる表現の例

図 2 にシステムの例と旧モデルでの表現を示す. また図 3 に同じシステムの提案モデルでの表現を示す.

図 3 では, 各リンクがそれぞれ向きを持つことが矢印で示されており, また L4R（ファイアウォール）の最上位レイヤノードが中継ノードを示す白抜きのものに変わっている. これにより, 中継ノードが明確化され通信の始点と終点も把握できることとなる.

5. 提案モデルの利点

本章では, 旧モデルを改良して得られた提案モデルの利点について述べる.

5.1 稼働率計算の精度向上

旧モデルを使ったネットワークシステムの稼働率計算では, リンクに向きを持たないことで, 特にレイヤ 3 と 4 において, 通信の依存関係を正確に抽出する際に, 本来システム上では存在しないループを検出してしまい, 正確に稼働率を計算することが困難であった[17].

提案モデルにより通信の方向が明確になり, ループ検出を回避することができ, 稼働率計算を正確に行うことが可能となった.

5.2 脆弱性影響範囲測定の精度向上

旧モデルを使ったネットワークシステムにおける脆弱性の影響度範囲測定では, 特に可用性の影響範囲を特定するにあたり, 通信の向きが考慮されていないことは大きな問題であった[20].

提案モデルによる通信方向の明確化により, 可用性の影響範囲が正確に測定することができ, それにより脆弱性のシステムへの危険性を定量化することが実現可能となった.

5.3 仮想化環境への対応

＜＜ここは追加で行きましょう＞＞

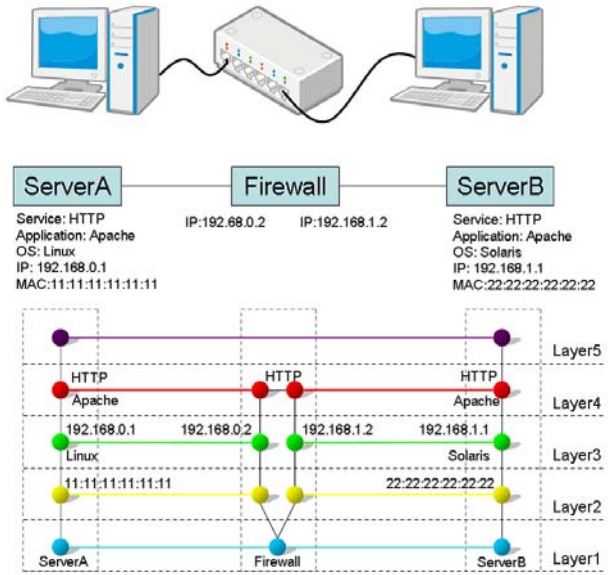

図 2 システム例と旧モデルでの表現

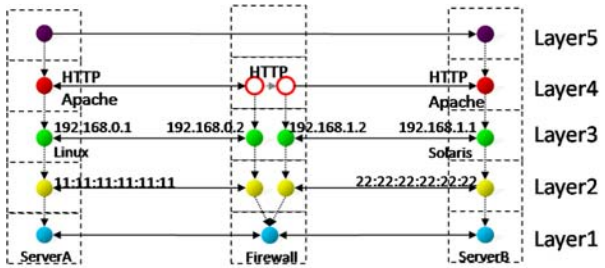

図 3 提案モデルでの表現

5.4 ファイアウォールルールの抽出

NSQ モデルによるモデル化は, モデル上でのさまざまな特徴解析や測定を基に, ネットワークシステムの設計や, 既存システムの拡張や補強時への補助として, 実際の機器へ設定情報を受け渡すことが大きな目的となっている. そのため, モデルから実際の機器への設定情報の変換は重要な要素であった. しかし旧モデルでは, 通信方向や依存関係が不明瞭であっ

たため, 特にルータやファイアウォールなどの中継モジュールにおける設定情報変換に困難を生じていた. 特にファイアウォールルールでは, 通信の向きが不明瞭なことに加え通信の始点と終点が不明確なことで, 通信を許可するルールを策定することは難しく, 別途始点と終点を指定することが必要であった.

提案モデルでは, 通信方向の表現を実現したことと, ノード種別を行ったことによる通信の始点・終点の明確化によりこれらの問題を解決し, ファイアウォールルールをモデルより抽出可能にした.

6. ま と め

本論文では, 複数機器・複数機能の相互接続により構成されるネットワークシステムに対し, これまでに提案されたマルチレイヤネットワークモデル（NSQ モデル）を改良したモデル提案した.

改良したモデルでは, 各リンクを有向化し, またリンク種別とノード種別をそれぞれ細分化した.

これまでの NSQ モデルでは各リンクが無向であったために通信の向きなどを指定することができず, 稼働率計算や脆弱性の影響度範囲測定などで問題を生じていたが, 提案モデルにより精度の高い稼働率計算や脆弱性の影響度範囲測定を実現可能にした.

さらに, これまでの NSQ モデルでは実現が困難であった, モデル上のレイヤ 4 中継器（L4R）からのファイアウォールルール抽出が, 提案モデルにより通信の始点と終点が明確になったことで, 実現可能となった.

今後の課題は, 既存ネットワーク設計理論を拡張し提案モデルへの適用を目指すとともに, 新たな計算困難性の存在も調査・研究する. また実際の機器・ネットワークへの適用や実環境からのモデル情報化など, 実際の環境との整合性の実証実験についても行う.

参 考 文 献

1) David M. Nicol, Jason Liu, Michael Liljenstam, Guanhua Yan: Simulation of large scale networks I: simulation of large-scale networks using SSF, *Proceedings of the 35th conference on Winter simulation*, pp.650-657 (2003)
2) M. Bakhouya and J. Gaber and A. Koukam: Immune-Based Middleware for Large Scale Network, *Annual IEEE Conference on Local Computer Networks*, pp.230 (2002)
3) Fabian Fischer, Florian Mansmann, Daniel A. Keim, Stephan Pietzko and Marcel Waldvoge: Large-Scale Network Monitoring for Visual Analysis of Attacks, *Proceedings of the 5th international workshop on Visualization for Computer Security*, pp.111-118 (2008)
4) P. Belotti, F. Malucelli, and L. Brunetta: Multicommodity network design with discrete node costs, *Networks*, vol.49, issue 1, pp.90-99 (2007)
5) C. Chekuri, F. B. Shepherd, G. Oriolo, and M. G. Scutella: Hardness of robust network design. *Networks*, vol. 50, issue 1, pp.50-54 (2007)
6) El-Sayed M. El-Alfy: Applications of genetic algorithms to optimal multilevel design of MPLS-based networks, *Computer Communications*, vol. 30, issue 9, pp.2010-2020 (2007)
7) Hu-Gon Kim, Chun-Hyun Paik, and Yong-Joo Chung: Heuristics for the Access Network Design Problem in 3G Mobile Communication Networks *Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control* , (2008)
8) Eric Rosenberg: Hierarchical topological network design, *IEEE/ACM Transactions on Network*, vol.13, issue 6, pp.1402-1409(2005)
9) Pietro Belotti, Antonio Capone, Giuliana Carello, and Federico Malucelli: Multilayer MPLS network design: The impact of statistical multiplexing, *Computer Networks*, vol. 52, issue 6, pp.1291-1307(2008)
10) Freek Dijkstra, Bert Andree, Karst Koymans, Jeroen van der Ham, Paola Grosso, and Cees de Laat: A multi-layer network model based on ITU-T G.805 *Computer Networks*, vol.52, issue 10, pp.927-1937(2008)
11) Paulo Salvador, Antonio Nogueira, and Rui Valadas: Local Area Network Modeling for Performance Prediction ,*Proceedings of the 32nd IEEE Conference on Local Computer Networks*, pp.249-251, 2007.
12) Sami J. Habib: Redesigning network topology with technology considerations, *International Journal of Network Management*, vol.18, issue 1, pp.1-13 (2008)
13) 金岡 晃, 藤堂 伸勝, 加藤 雅彦, 岡本 栄司：ネットワークシステムの安全性定量化に向けた新たな表現モデルとアクセス制御解析, 2008 年暗号と情報セキュリティシンポジウム（SCIS2008）, 2008 年 1 月
14) 金岡 晃, 加藤 雅彦, 藤堂 伸勝, 岡本 栄司：アクセス制御の違いによる ネットワークシステムの特性変化に関する考察, 電子情報通信学会 情報通信システムセキュリティ研究会, 2008 年 9 月
15) 加藤 雅彦, 金岡 晃, 藤堂 伸勝, 岡本 栄司：ネットワークシステムにおける脆弱性影響度の定量化と可視化 , コンピュータセキュリティシンポジウム 2008 （CSS2008）, 2008 年 10 月
16) 金岡 晃, 藤堂 伸勝, 加藤 雅彦, 岡本 栄司：適切なアクセス制御状態にあるネットワークシステムの特徴抽出, コンピュータセキュリティシンポジウム 2008 （CSS2008）,

Vol.2009-CSEC-47 No.3
2009/12/18

2008 年 10 月
17) 藤堂 伸勝, 加藤 雅彦, 金岡 晃, 岡本 栄司：ネットワークシステムにおける可用性測定の考察, コンピュータセキュリティシンポジウム 2008 （CSS2008）, 2008 年 10 月
18) 原田 敏樹, 金岡 晃, 加藤 雅彦, 岡本 栄司：脆弱性情報提供 Web API ”AVIP”の開発, 2009 年暗号と情報セキュリティシンポジウム（SCIS2009）, 2009 年 1 月
19) 原田 敏樹, 金岡　晃, 岡本 栄司, 加藤 雅彦:CVSS を用いたネットワークシステムにおける危険度測定手法の検討, 信学技報, vol. 109, no. 115, ICSS2009-48, pp. 189-194, 2009 年 7 月
20) 原田 敏樹, 金岡　晃, 岡本 栄司, 加藤 雅彦:ネットワークシステムにおける CVSS を用いた脆弱性影響範囲特定手法の検討, 信学技報, vol. 109, no. 285, ICSS2009-54, pp. 1-6, 2009 年 11 月
21) A. Kanaoka, M. Katoh, N. Toudou, E. Okamoto, ”Extraction of Parameters from Well Managed Networked System in Access Control”, Proceedings of The Fourth International Conference on Internet Monitoring and Protection (ICIMP 2009), pp.56-61, May. 2009