情報処理学会論文誌 Vol. 51 No. 9 1726–1735 (Sep. 2010)

安全なネットワークシステム設計のための マルチレイヤネットワークモデルの提案と応用

金岡 晃[†1] 原田敏樹[†1] 加藤雅彦[†2]
勝野恭治[†3] 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た現在において必要不可欠の基盤システムである．しかし現状の安全性に関す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と同様に経験に大きく依存して行われていて定性的である．そのため，方法論や理論を用いた再現性を持った定量的な評価をほとんど行っていない．本論文では，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，仮想環境も論理的に表現可能なマルチレイヤネットワークモデルを提案した．また提案モデルを利用し，安全なネットワークシステムの設計方法論を構築するための定量尺度として，脆弱性影響度の定量尺度を提案し，既存尺度であるシステム稼働率のマルチレイヤへの拡大も行った．本論文で提案したモデルとモデル評価尺度を用いることで，ネットワークシステムにおける最適な安全性を実現する設計手法を定量的に検証することが可能になった．

Multi-Layered Network Description Model for Secure Networked System Design

Akira Kanaoka,[†1] Toshiki Harada,[†1]
Masahiko Katoh,[†2] Yasuharu Katsuno[†3]
and Eiji Okamoto[†1]

Networked systems composed of multiple network equipments are foundation for the widespread Internet. Unfortunately, secure networked system designs still depend on expert knowledge, similar early days of the Internet. There is few quantitative evaluation using methodology or theory for networked system design, because qualitative design is mainly used now. In this paper, we propose a multi-layerd network model which enables to express logically structure without loss of characteristics for each network equipment and express virtual environment. We also propose two scoring methods using the network model: vulnerability impact scoring method for secure networked system design methodology and availability scoring method by extending existing availability scoring method for single-layerd network model. Our proposed model and scoring methods enable quantitative discussion for optimization of secure networked system design.

1. はじめに

データセンタ事業者やシステムインテグレータ事業者など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を適切に設定する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）の安全性に関する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持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曖昧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．

ネットワークの安全性に関する研究は多くされてきた[1)–3)]．またネットワークの最適設計に関する研究も多くされている[4)–10)]．しかしこれらの研究は，バックボーンネットワークといった Wide Area Network（WAN）に対する研究である．本論文の対象はデータセンター内のローカルエリアのネットワークシステムであり，バックボーンと比較してクローズドなネットワークとなっている．さらに多くの既存研究は単一種類の機器によるネットワークや単一レイヤでのネットワーク構成を前提としているため，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セキュリティ機能を提供しその結合により 1 つのサービスを提供するネットワークシステムとは大きく前提条件が異なり，従来研究の成果を用いてネットワークシステムにおける安全性の最適設計を行う

†1 筑波大学
University of Tsukuba
†2 株式会社アイアイジェイ
Internet Initiative Japan Inc.
†3 日本アイ・ビー・エム株式会社東京基礎研究所
IBM Research, Tokyo Research Laboratory

ことは困難が生じる．

ネットワークシステムの安全性に関する最適設定を検討する場合には，まず安全性の定義と，何が安全かを示す定量尺度が必要である．定量尺度の存在により，最適な安全性設計の議論が可能になる．そしてその尺度も，評価者によって測定値が異なることのないよう，同一のシステムと同一の条件下では同一の測定値が得られる必要がある．

システム測定値の同一条件下での一意性を保証するためには，測定に用いられるシステムは，曖昧さを排除した表現をされる必要がある．特にネットワークシステムの場合，複数の異なる機能を持つ機器群によりシステムが構成されるため，曖昧さを排除するためにはそれら複数機器の種類が特性を失うことなく表されることが必要になる．また，TCP/UDP のポート番号に従ってパケットのフィルタリングを行うファイアウォールや IP アドレスに従ってルーティングを行うルータなど，システムにおける各機器の機能が異なるレイヤで実現されていることから，各機能を表現するには複数のレイヤ情報を包含した表現が求められる．また上位レイヤの機能を実現するには関連する下位レイヤの機能も必要となり，各レイヤにまたがる機能の依存も不足なく表現される必要がある．

そこで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，それらの機器の機能特徴を失うことなく論理的に表現可能なマルチレイヤネットワークモデルを提案する．提案モデルはこれまでのグラフ理論によるグラフ表現にレイヤ構造を取り入れて拡張したモデルであるが，各ノード間にはレイヤ構造による依存関係があるほか，ノードを結ぶリンクは通信路を意味するだけでなくシステム内の中継機能や依存関係など複数の意味を持つ．レイヤ構造の適用と依存関係の反映により，提案モデルはこれまでのネットワークモデルでは表現が困難であった複数機器・複数機能の柔軟な表現を可能にした．またモデルは論理ネットワークだけではなく物理ネットワークを含むことで，物理的な構成によるリソース制限の論理的な構成への影響を検討可能にした．さらに，提案モデルはサーバなどの仮想化と実体の依存関係も表現可能であり，仮想化環境にも対応している．

定式化による集合の操作により各レイヤのネットワークを部分的に抽出することで，安全性に関する設計だけでなく，単一レイヤ・単一種類ノードで実現される既存のネットワーク設計理論における種々の手法を適用することも可能である．しかし適用可能なのはレイヤごとに抽出されたネットワークのみであり，マルチレイヤ全体への適用は難しい．その理由に，最適を示す尺度がマルチレイヤのモデルに適していないことがある．たとえば，これまでのネットワーク設計理論で研究されてきたフロー問題では尺度としてフロー流量が用いられ，システム全体の尺度としてはフローの総量が利用される．しかし，マルチレイヤ特性を持つ提案モデルでは各レイヤのフロー流量は他のレイヤと強い依存関係を持つことからレイヤ種類を考慮しないフロー総量は依存による重複が起こり，システムのフロー流量を判断するには不適切である．これら尺度についてもレイヤ構造や依存関係などマルチレイヤの特徴を考慮したものにならなければ，その尺度を用いた最適設計手法を検討することはできない．また，ネットワークシステムの安全性尺度に関しては，まだ開拓が進んでいるとはいえない．

本論文では，モデルの提案に加え提案モデルを利用した安全性の定量尺度もあわせて提案する．定量尺度は安全なネットワークシステムの設計方法論を構築するための尺度として，脆弱性影響度との提案と，既存尺度であるシステム稼働率のマルチレイヤへの拡大を行った．

本論文で提案したモデルとモデル評価尺度を用いることで，マルチレイヤネットワークモデルでの最適設計手法を検証することが可能になった．

2 章ではネットワーク設計についてこれまで行われてきた従来研究を紹介し，3 章で従来研究では実現されていなかったマルチレイヤネットワークモデルを提案する．4 章では提案モデルを利用した評価尺度の検討と，実際の機器との対応について述べ提案モデルの有効性を示し，最後に 5 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別が単一であり，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，単一のノード種別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)]．しかし，Dijkstra らの提案は Belotti らと同様に MPLS のモデル化であり，MPLS 機器どうし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いえない．これらのモデルは ISP などのネットワーク事業者が

持つバックボーンネットワークを対象にした大規模なネットワークモデルであり，電子商取引サービスなどのサービス側のネットワークシステム（小規模ネットワーク）にあるような，サーバを含む複数の機器を表現し，設計へ応用可能にしているものではない．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，価格など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，レイヤ構造を持ちノード種別が複数存在するネットワークのモデルや設計手法は存在していない．さらに個々の機器が持つ脆弱性に対するネットワークシステムの安全設計へのアプローチはなされていない．そこで本論文では次章以降でこれらを可能にするモデルを提案し，尺度を提案する．

3. マルチレイヤネットワークモデル

ネットワークシステムとは複数の機器がローカルエリアネットワーク（LAN）技術によって接続されネットワークを構成し，ネットワーク全体で 1 つ以上のサービスをネットワーク外部に提供しているシステムをいう．

本章では，ネットワークシステムを構成する各機器の特徴を失わない新たなネットワークモデルを提案する．提案モデルは，これまでのマルチレイヤモデルでは表現が難しかった依存関係の明確化や，複数種類の機器を同一モデル内に表現可能とするものである．

提案モデルはグラフ理論でのグラフ $G = (V, E)$ を拡張したものであり，ノードとリンクの集合と 4 つの写像で表現される．しかし，既存モデルとは異なり，1 つの機器は 1 つのノードでは表されず，機能の要素としてノードが各レイヤに存在し，それらノードとリンクの集合（部分グラフ）により 1 つの機器（モジュール）を表現する（**図 1**）．

モデルの定義は以下の点で行われる

- レイヤ定義
- ノード定義（属性定義）

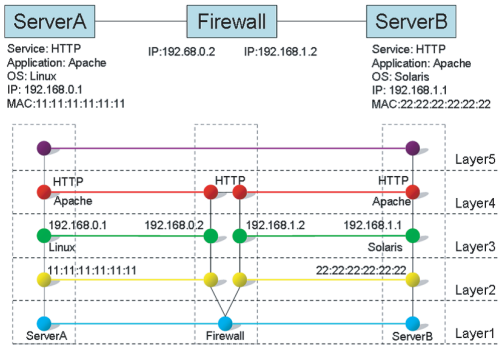

図 1　提案モデルによる表現例
Fig. 1　Networked system example of proposed model.

- リンク定義（属性定義）
- モジュール定義
- ネットワーク定義

3.1 モデルの定義

定義 3.1（レイヤ）　レイヤは 5 つからなる．レイヤ 1（L1）は物理的接続の層であり，レイヤ 2（L2）は Ethernet ネットワークの層，レイヤ 3（L3）は IP ネットワーク層，レイヤ 4（L4）は TCP/UDP ネットワーク層，そしてレイヤ 5（L5）は抽象化したサービスの層である（**表 1**）．

通信におけるレイヤの定義は ISO 7498 で定義されている OSI 参照モデルによる 7 階層や，RFC 1122 で定義されている TCP/IP による 4 階層が代表的であるが，本論文で定義するレイヤは TCP/IP をもとに，ネットワークシステムの設計で必要になる物理的な接続のレイヤを加え，5 階層としたものである（**図 2**）．

定義 3.2（ノード）　通信の終端あるいは中継点となる要素をノードと呼ぶ．ノードは終端ノードと中継ノードの 2 種類が存在する．

終端ノードは通信の始点また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，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

表 1　レイヤ定義
Table 1　Definition of layers.

Layer 5	抽象化サービス（WWW，DNS，etc.）
Layer 4	TCP/UDP ネットワーク（80，53，etc）
Layer 3	IP ネットワーク
Layer 2	Ethernet ネットワーク
Layer 1	物理的接続

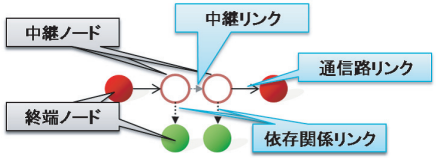

図 2　ノードとリンクの種類
Fig. 2　Types of node and link.

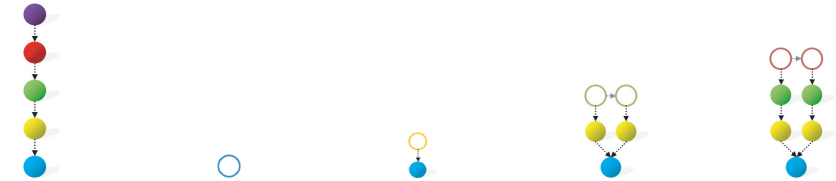

図 3　モジュール例
Fig. 3　Module examples.

識別されるための情報で，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．依存関係リンクに関しては後述する．

ネットワーク上の各ノードは v_i，その集合は V で表される．また 2 つの属性情報を持つため，レイヤ情報を示す写像 $l_V : V \to L_V$，ノード種別を示す写像 $s_V : E \to S_V$ が存在する．ここで $L_V = \{1, 2, 3, 4, 5\}$，$S_V = \{T, R\}$ である．L_V の各要素はレイヤ情報を示すものである．また S_V の要素 T は終端ノード（Terminal）であることを示す情報であり，R は中継ノード（Relay）であることを示す情報である．

定義 3.3（リンク）　ノード間を結ぶ要素をリンクと呼ぶ．リンクは通信路リンクと依存関係リンク，中継リンクの 3 種類よりなる（図 2）．

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．モジュールに関しては後述する．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．

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．

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．

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．

ネットワーク上の各リンクは $e_i = (v_a, v_b)$ で表される．ここでは e_i はノード v_a から v_b へのリンクであることを示している．リンクの集合は E で表される．また 2 つの属性情報を持つため，それぞれに写像 $l_E : E \to L_E$，$s_E : E \to S_E$ が存在する．ここで $L_E = \{0, 1, 2, 3, 4, 5\}$，$S_E = \{C, D, R\}$ である．L_E の各要素はレイヤ情報を示すものであり，0 はレイヤ情報を持たないことを示すものであり依存関係リンクの属性値として用いられる．S_E の要素 C は通信路（Communication）リンクを示し，D は依存関係（Dependancy）リンク，R は中継（Relay）リンクを示すものである．

定義 3.4（モジュール）　ネットワーク機器の機能を提供するものをモジュールと呼ぶ．モジュールは依存関係リンクと中継リンク，ノードにより構成される．

モジュールはその機能によりサービスモジュール，インターネットモジュール，中継モジュール 3 つに大別される．中継モジュールはレイヤごとに細分化して表される（**図 3**）．

- サービスモジュール（S）
- インターネットモジュール（I）
- 中継モジュール（R）
  - レイヤ n 中継モジュール（LnR）

サービスモジュール（S）はサービスを提供するモジュールである．また他のサービスモジュールに対するクライアントになることも可能である．各レイヤのノードはアイデンティティ情報を持つ．

インターネットモジュール（I）はシステムの外部全体（インターネット）を代表するモジュールであり，サービスモジュールに対するクライアントになる．各レイヤのノードは複数のアイデンティティ情報を持つことが可能である．

中継モジュール（R）はあるレイヤでの通信の中継を行うモジュールである．レイヤにより 5 つに細分化される．レイヤ 2 以上のノードはアイデンティティ情報を持たないことがあり，またモジュール内の最上位レイヤに存在するノードはすべて中継ノードとなる．

表 2　各モジュールが持つノード数
Table 2　Number of nodes in each modules.

	S	I	R				
			L1R	L2R	L3R	L4R	L5R
L4	$\geq n_3$	1	0	0	0	$\geq n_3$	$\geq n_3$
L3	$\geq n_2$	1	0	0	n_2	n_2	n_2
L2	≥ 1	1	0	≥ 1	≥ 1	≥ 1	≥ 1
L1	1	1	1	1	1	1	1

各モジュールが持つノード数は**表 2** のようになる．ここで n_i はそのモジュールのレイヤ i でのノード数を示す．また抽象化されたサービスを示すレイヤ 5 のノードは，複数のモジュールより構成されるものであるため，その個数は各モジュールごとには定まらない．よって表には記載されていない．

定義 3.5（ネットワークとシステム） ネットワークは，ノードとリンクの集合であり，システムは各レイヤのネットワークを結合したものである．
ネットワーク G は，以下で定式化される．

$$G = (V, E, l_V, s_V, l_E, s_E) \tag{1}$$

3.2　定式化によるネットワーク操作

定義とともに示した定式化により，ネットワーク G に対して部分グラフとして特定レイヤのネットワークを抽出することや，ノード部分集合の抽出といった操作が可能になる．

レイヤ x に属するノード集合 V_x とリンク集合 E_x はそれぞれ以下のように表すことができる．

$$V_x = \{v_i | l_V(v_i) = x\} \tag{2}$$

$$E_x = \{e_i | l_E(e_i) = x\} \tag{3}$$

またこれらから，システム全体のネットワーク G からレイヤ x のネットワーク G_x を抽出することが可能である．

$$G_x = (V_x, E_x, l_V, s_V, l_E, s_E) \tag{4}$$

さらに，リンク種別ごとの集合 E_C，E_D，E_R を以下のように抽出することも可能である．

$$E_C = \{e_i | s_E(e_i) = C\} \tag{5}$$

$$E_D = \{e_i | s_E(e_i) = D\} \tag{6}$$

$$E_R = \{e_i | s_E(e_i) = R\} \tag{7}$$

上記の各集合により，ネットワーク G が各レイヤの論理ネットワーク G_i と各ノードの依存関係のみを表現したネットワーク $(V, E_D, l_V, s_V, l_E, s_E)$ で構成されることが分かる．

$$G = (V, E_D, l_V, s_V, l_E, s_E) \cup \bigcup_i G_i \tag{8}$$

3.3　モデルによる利点

既存研究においてもマルチレイヤネットワークのモデルは存在するが，ネットワークシステムへの適用には向いていない．たとえば，マルチレイヤモデルで表現されたシステムから，システム内に存在するファイアウォールのルールを抽出することを考える場合，通信路の始点と終点が明確にされていなければルール抽出は不可能である．既存モデルではノード種別がされていないため，ファイアウォールもサーバも同一レイヤで同一ノードとして表現されるため始点と終点を明確に表現できないが，提案モデルでは正確にファイアウォールのルールを抽出可能である．このように，提案モデルは現実機器・設定への適用などの運用に対応可能である．

近年のクラウドコンピューティング環境で主流になりつつある仮想化にも提案モデルは対応している．依存関係リンクを利用することにより，依存ノードにゲスト PC の L1 ノード，被依存ノードにホスト PC の L1 ノードを用意し，両者を依存関係リンクを結び，さらに仮想ブリッジとして L1 ノードを設け，仮想ブリッジノードからホスト PC の L1 ノードに依存関係リンクを結ぶことで，ホスト・ゲストの依存関係の表現が可能である．そして上位レイヤではそれらの依存関係を考慮することなくサービス構成を行うことが可能になる．

さらに，冗長化の面においても仮想 IP アドレスを用いるロードバランサや，仮想ルータにも対応可能である．仮想 IP アドレスを L3 ノードとして設け，それらと実際の提供サービスホストとを依存関係リンクで結ぶことで冗長化されたシステムの表現が可能になる．

提案モデルによる柔軟な表現の対応は，一方でモデルの複雑さを招き，利用者にとって可読性の低いものとなる可能性がある．しかし利用者は本質的にモデル自体を閲覧する必要はなく，モデルを用いた各アプリケーションが，その用途に応じて必要な情報のみを提示することで可読性が高められるべきである．

3.4　モデルによる表現の例

図 4 のネットワーク図で表されるシステムを，提案モデルで表現した例を**図 5** に示す．図 4 のネットワーク図は機器の物理的つながりを示したネットワークでしかなく，IP ネットワークなどの論理的な接続やセグメント表現はできていない．一方，提案モデルを用いた図 5 では，物理的つながりはレイヤ 1 で表され，上位の論理的なネットワークも表現されており，さらにそれらの依存関係も表現されていることが分かる．なお，図 5 では，各レイヤは色分けして表現してあるが，外観の煩雑さを除くために各リンク種別とノード種別の

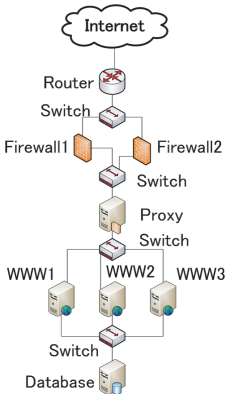

図 4　ネットワークシステムのネットワーク図
Fig. 4　Existing expression for networked system.

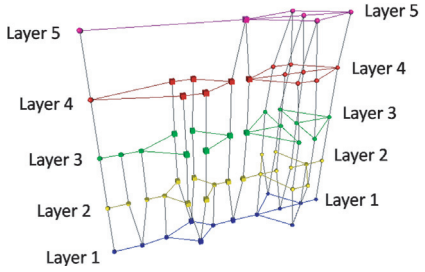

図 5　ネットワークシステムの提案モデルによる表現
Fig. 5　Proposed model expression for networked system.

差，またリンクの向きは表現していない．

4. 提案モデルの応用

4.1 最適性と評価尺度

ネットワーク設計の最適性を論じるには，最適を示す尺度が必要である．そしてその尺度を用いて，ネットワークの最適性を求める問題を解くことがネットワーク設計問題である．

これまでのネットワーク設計理論では，フロー費用を尺度とした最小費用フロー問題や，利用者均衡フロー問題，システム最適化フロー問題などがあり，予算を尺度とした予算制約を持つネットワーク設計問題（Budget Network Design problem）や固定費用を持つネットワーク設計問題（Fixed charge Network Design problem）などがある[13]．これらはレイヤ構造を持たない既存のネットワークモデルでの問題であり，提案モデルを用いた最適設計を論じるには，これら尺度をマルチレイヤに拡張する必要がある．

さらに安全性の視点では，システムの最適性はアクセス制御の状態，各機器の脆弱性がシステムの安全性にどこまで影響を及ぼすか，各機器の障害がシステムにどのように影響するか，といったフロー費用や予算などとは異なる様々な視点で検討される必要がある．

このように最適性を論じるにはその視点が重要になるが，本提案モデルにおける最適性の検討では下記の 2 点が考慮されなければならない．

- 安全性視点でのネットワーク設計問題の設定
- 既存設計問題のマルチレイヤモデルへの拡張

本論文では，上記 2 点のうち「安全性視点でのネットワーク設計問題の設定」に注目し，各ノードが持つ脆弱性がネットワークシステム全体にどれほどの影響度を及ぼすかの定量尺度の検討と，各ノードやリンクの障害がシステムのサービス提供に及ぼす影響を測定可能な稼働率の検討を行うことを目的とする．

既存の設計問題では各問題についてその解法に先立つ計算困難性についてが論じられており，提案モデルをはじめとしたマルチレイヤモデルへの拡張にあたっては計算困難性から再検討しその解法を議論する必要があるため，今後の課題とする．

4.1.1 脆弱性の影響度

脆弱性の影響度に関しては，CVSS（Common Vulnearbility Scoring System）による測定が知られている[14),15)]．CVSS は脆弱性単体の危険度を示す基本値（Base Score）や，脆弱性を利用するワームや脆弱性を無効化するパッチの存在など時間経過により異なる脆弱性の危険度を示す現状値（Temporal Score），そしてシステムやネットワークといった環境全体への脆弱性の危険度を示す環境値（Environmental Score）の 3 つの尺度からなる．

CVSS の基本値が米国標準技術局（NIST）が持つデータベース NVD（National Vulnerability Database）に含まれるすべての脆弱性情報に付与されていることや，日本でも情報処理推進機構（IPA）による脆弱性対策情報データベース JVN iPedia でも採用されるなど広範に利用されている一方で，現状値や環境値はほとんど利用されていない．さらに，環境値は自分の環境情報として「影響を受ける対象システムの範囲（TD: Target Distribution）」を入力しなければその値が出力されないが，その入力すべき情報が「なし」「小規模（利用環境の 1–25%）」「中規模（利用環境の 26–75%）」「大規模（利用環境の 76–100%）」と非常に粗い尺度でしか設定ができない．それらの範囲測定についても明確な基準がなく，再現性が高いとは決していえない．そこで，本モデルを利用することで曖昧さを排除可能な環境値への TD 入力手法を提案する．提案にあたりデータセンタ内で管理されているネットワークシステムを仮定する．ネットワークシステムは物理的に保護されており，ネットワークシステム内の脆弱性を利用した攻撃は外部からのネットワーク経由による攻撃のみを考慮することとした．そのため，CVSS の基本評価基準内の「AV：攻撃元区分」において物理的なアクセス可能状態からの攻撃を必要とする「ローカル」は考慮しない．

まず脆弱性とモデルのマッピングを行う．脆弱性はモデル上のノードがそれぞれ保持することとし，脆弱性が持つ属性情報と各レイヤのノードを**表 3** のように対応付けた．

表 3　属性のマッピング
Table 3　Mapping between layer and attribute.

レイヤ	属性
5	アプリケーションデータ
4	アプリケーション名，バージョン
3	OS 名，バージョン
2	—
1	製品名，ベンダ名

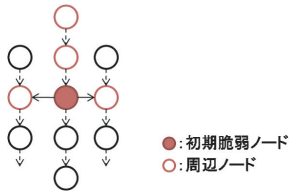

図 6　初期脆弱ノードと周辺ノード
Fig. 6　Initial vulnerable node and peripheral nodes.

ネットワークシステムがファイアウォールなどによりアクセス制御が行われている場合，脆弱性が存在したとしても攻撃が該当機器まで到達せず，脆弱性の影響を受けない可能性がある．そのため，単純に脆弱性のあるアプリケーションがネットワークシステム内部に存在するというだけでは影響は判断せず，システム外部（インターネットモジュール）から到達可能であるノードかつ脆弱性を持つノードを脆弱なノードとした．

そして脆弱なノードのシステム内での位置と，脆弱性の性質により影響範囲を決定する．脆弱性の性質は CVSS の基本評価基準（Base Metric）に沿って機密性への影響（C: Confidentiality Impact），完全性への影響（I: Integrity Impact），可用性への影響（A: Availability Impact）を考慮する．

機密性は，サービスがかかえる情報の機密性と，サービスを構成している各機器が持つ設定情報やユーザ情報などの機密性とに大別できる．本モデルはサービス上のデータ自体ではなく，サービスを構成する機器とネットワーク構成を示すことから，ここでは後者を考える．完全性も同様にサービス自体の完全性と，サービス提供を行う機器が持つ情報の完全性とに大別でき，ここでは後者を考える．一方，可用性は構成する機器やソフトウェアの可用性が保たれることでサービスの可用性が実現されるため，分離して考えることはしない．

CVSS において各脆弱性の C，I，A 評価はそれぞれ「なし」「部分的」「全面的」の 3 段階で評価される．提案手法では各ノードの依存関係を考慮し，「部分的」である場合は脆弱性が存在するノードの上位に存在するノード（依存関係リンクで結ばれた上位ノード）も影響を受ける．「全面的」である場合は脆弱性が存在するノードが所属するモジュール全体（当該ノードから依存関係リンクのみで到達可能なすべてのノード）を影響を受けるとし，それらのノード集合を「初期脆弱ノード群」と呼び，$V_{\mathrm{init}C}$，$V_{\mathrm{init}I}$，$V_{\mathrm{init}A}$ で表す．さらに，脆弱性のシステムの影響は初期脆弱ノード群だけにとどまらず周辺にも影響を及ぼすことから，初期脆弱ノード群からリンクでつながっているノード群（以後，周辺ノードと呼ぶ）を「脆弱性影響ノード群」とし，V_C，V_I，V_A と表す．機密性（C）と完全性（I）は「通信リンクを通じて隣接しているノードが影響を受ける」を周辺ノードとし，可用性（A）については「通信リンクを通じて到達可能なノードすべてが影響を受ける」を周辺ノードとした．**図 6** は C と I に「部分的」な脆弱性を持つ場合の初期脆弱ノードと周辺ノード群を示したものである．

V_C，V_I，V_A は以下のように表される．

$$\begin{aligned} V_C &= V_{\mathrm{init}C} \bigcup \{v_i | (v_i, v_x) \in E_C\} \\ V_I &= V_{\mathrm{init}I} \bigcup \{v_i | (v_i, v_x) \in E_C\} \\ V_A &= V_{\mathrm{init}A} \bigcup V_{\mathrm{reachable}A} \end{aligned} \tag{9}$$

ここで $V_{\mathrm{reachable}A}$ は $V_{\mathrm{init}A}$ から通信リンクのみを利用して到達可能なノードの集合である．そして，対象範囲（TD-Rate）の計算を以下の式で行う．

$$\text{TD-Rate} = \frac{N(V_C \bigcup V_I \bigcup V_A)}{N_G - N_I} \tag{10}$$

ここで N_G はシステム全体のノード数，$N(V)$ はノード集合 V のノード数，N_I はインターネットモジュールのノード数を示す．TD-Rate により脆弱性のネットワークシステムへの影響度が一意に決定できることになり，細かい影響度の利用が可能である．TD-Rate の算出は従来の CVSS 利用にも利点がある．TD-Rate の値を TD の「利用環境の範囲」と照合することで既存 CVSS が利用可能であることに加え，利用者ごとの入力曖昧さを排除することが可能となり，環境値評価の一意性や再現性を提供することが可能になる．

4.1.2　稼　働　率

システム工学や信頼性工学の分野では，稼働率を用いてシステムの可用性を評価する．本項ではそれらを応用し，レイヤ構造による依存関係を考慮した稼働率計算手法を示す．

ネットワークシステムの稼働は，システムを構成するリンクの稼働とノードの稼働により実現されることから，システム稼働率をリンク稼働率とノード稼働率を用いて求める．

提案モデルの特徴としてレイヤ間の依存関係があるが，稼働率においても依存関係は継承される．下位通信路リンクの稼働は，上位通信路リンクの稼働に欠かせないためである．一方で，上位通信路リンクに障害が起きることが必ずしも下位通信路リンクの障害を示すことではない．よって，それぞれの通信路リンクは上位と下位で共通の稼働率ではなく，それぞれが独自の稼働率を持つこととなる．ノード稼働率も同様であり，依存関係リンクを持つノード群の稼働は下位ノードの稼働の影響を受ける．

まず下位レイヤ影響を排除した，リンクやノードそのものの稼働率の写像 f_E，f_V を以下のように定義する．

$$\begin{aligned} &f_E : E \to [0,1] \\ &f_V : V \to [0,1] \end{aligned} \tag{11}$$

レイヤ影響を考慮したリンクやノードの稼働率の写像 p_E，p_V を以下のように定義する．

$$\begin{aligned} &p_E : E \to [0,1] \\ &p_V : V \to [0,1] \end{aligned} \tag{12}$$

ここで $e_i = (v_a, v_b)$，$V_a = \{v_i | (v_a, v_i) \in E_D\}$，$V_b = \{v_i | (v_b, v_i) \in E_D\}$ とすると，p_E と f_E，p_V と f_V は以下の関係を持つ．

$$\begin{aligned} p_E(e_i) &= f_E(e_i)\left(1 - \prod_{v_\alpha \in V_a, v_\beta \in V_b}\left(1 - \frac{A_R(v_\alpha, v_\beta)}{p_V(v_\alpha)p_V(v_\beta)}\right)\right) \\ p_V(v_a) &= f_V(v_a)\left(1 - \prod_{v_\alpha \in V_a}(1 - p_V(v_\alpha))\right) \end{aligned} \tag{13}$$

ここで $A_R(v_a, v_b)$ はある同一レイヤの 2 点 v_a，v_b 間の稼働率とする．またレイヤ 1 のリンクやノードは下位に依存しないことから，$p_E(e_i) = f_E(e_i)$，$p_V(v_i) = f_V(v_i)$ となる．

システム全体の稼働率は，レイヤ 5 における通信がすべて稼働している状態であるとし，システム全体の稼働率 $A_S(G)$ は以下のように定義する．

$$A_S(G) = \prod_{v \in V_5} p_V(v) \prod_{e \in E_5} p_E(e) \tag{14}$$

$A_R(v_a, v_b)$ は 2 点 v_a，v_b 間のパス数で決定される．そのパス i を，リンク集合だけでなくノード集合も含んだ部分グラフ $P^i_{a,b} = (V_{P^i_{a,b}}, E_{P^i_{a,b}})$ で表すと，それぞれの稼働率 $A_P(P^i_{a,b})$ は以下の式で表される．以降，本論文では $P^i_{a,b}$ をパス部分グラフと呼び，$A_P(P^i_{a,b})$ をパス稼働率と呼ぶこととする．

$$A_P(P^i_{a,b}) = \prod_{v_i \in V_{P^i_{a,b}}} p_V(v_i) \prod_{e_i \in E_{P^i_{a,b}}} p_E(e_i) \tag{15}$$

$A_R(v_a, v_b)$ はパス稼働率 $A_P(P^i_{a,b})$ より求められるが，それぞれのパスを構成するノードやリンクの重複を考慮しなければならない．すべてのパスで共通する部分がある場合，その部分グラフ $G' = (V', E')$ を取り出し，G' の稼働率と積和をとることで $A_R(v_a, v_b)$ の稼働率が得られる．

$$A_R(v_a, v_b) = \prod_{v_i \in V'} p_V(v_i) \prod_{e_i \in E'} p_E(e_i)\left(1 - \prod_k \left(1 - A_P(P^k_{a,b} \setminus G')\right)\right) \tag{16}$$

なお，すべての i において v_a，$v_b \in V_{P^i_{a,b}}$ であるため，V' は空集合にはならない．

しかし，パス間でそれぞれ共通部分があり，重複が複雑多岐にわたる場合，上記 2 つの算出方法は利用できず，また $A_R(v_a, v_b)$ の厳密計算は難しい．一方，従来の信頼性工学において，複雑な重複を持つシステムの稼働率は，最小カットセットと最小パスセットを用いると，上限稼働率と下限稼働率を求められることが知られている．ここでは提案モデル上に拡張した上限稼働率と下限稼働率を示す．

上限・下限稼働率を求めるにあたり用いられる最小カットセットと最小パスセットは求めることが難しいことが知られているが，パス部分グラフ $P^i_{a,b}$ のすべてのノードとリンクが稼働していればノード v_a，v_b 間が稼働するため，パス部分グラフはパスセットであり，同時に，パス部分グラフのどの要素が欠けた部分グラフでもノード v_a，v_b 間の稼働は保証されないため，パス部分グラフは最小パスセットである．最小パスセット群の稼働率の余事象から上限稼働率が求められることから下のように示すことができる．

$$A_R(v_a, v_b) \le 1 - \prod_k \left(1 - A_P(P^k_{a,b})\right) \tag{17}$$

また，パス部分グラフ群の中から任意のリンクまたはノードを 1 つずつ選択した部分グラフ $\Theta^i_{a,b} = (V_{\Theta^i_{a,b}}, E_{\Theta^i_{a,b}})$ は，それらすべてが非稼働になると v_a，v_b 間が非稼働になるためカットセットであり，また Θ からどの要素が欠けた部分グラフでも v_a，v_b 間の非稼働が保証されないため，最小カットセットである．最小カットセット群の稼働率の積和から最小

稼働率が求められることから

$$A_R(v_a, v_b) \geq \prod_k A_\Theta(\Theta^k_{a,b}) \tag{18}$$

と示すことができる．ここで

$$A_\Theta(\Theta^i_{a,b}) = 1 - \prod_{v_i \in V_{\Theta^k_{a,b}}} (1 - p_V(v_i)) \prod_{e_i \in E_{\Theta^k_{a,b}}} (1 - p_E(e_i)) \tag{19}$$

である．よって，これら最小パスセット群と最小カットセット群より，下記のように上限稼働率と下限稼働率が定まる．

$$\prod_k A_\Theta(\Theta^k_{a,b}) \leq A_R(v_a, v_b) \leq 1 - \prod_k \left(1 - A_P(P^k_{a,b})\right) \tag{20}$$

上記を式 (14) に適用することで，システム稼働率の上限と下限を求めることが可能となる．

5. 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，機器の機能特徴を失うことなく表現可能なマルチレイヤネットワークモデルを提案した．また提案モデルを利用し，安全なネットワークシステムの設計方法論を構築するための定量尺度として，脆弱性影響度の定量尺度を提案し，既存尺度であるシステム稼働率のマルチレイヤへの拡大も行った．

提案モデルはこれまでのグラフ理論によるグラフ表現にレイヤ構造を取り入れ拡張したモデルであるが，ノード，リンクはそれぞれ単一種類ではなく複数の種類を持つ．そしてそれらの複数種類のノード，リンクの組合せによりこれまでのネットワークモデルでは表現が困難であったスイッチやルータ，ファイアウォールなどの各ネットワーク機器を機能特性を保ったまま表現可能にし，仮想化環境への対応も可能にした．

またリンクとノードの集合と，リンク種別やノード種別などの各属性を写像として表現することでモデルの定式化を行った．集合の操作を行うことで抽出される各レイヤのネットワークは，単一レイヤ・単一種類ノードで実現される既存のネットワーク設計理論における種々の手法を適用することも可能である．

一方，最適性を示す尺度がマルチレイヤのモデルに適していないために，既存ネットワーク設計理論は提案モデルには直接適用が困難である．そこで本論文では，提案モデルを用いた定量尺度として，脆弱性影響度の提案と，システム稼働率の提案を行った．なおシステム稼働率は既存の尺度であるが，本論文は既存尺度をマルチレイヤへと拡張したものである．

本論文で提案したモデルとモデル評価尺度を用いることで，マルチレイヤネットワークモデルにおける安全性の最適設計手法を検討することが可能になった．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) Nicol, D.M., Liu, J., Liljenstam, M. and Yan, G.: Simulation of large scale networks I: simulation of large-scale networks using SSF, *Proc. 35th Conference on Winter Simulation*, pp.650–657 (2003).
2) Bakhouya, M., Gaber, J. and Koukam, A.: Immune-Based Middleware for Large Scale Network, *Annual IEEE Conference on Local Computer Networks*, p.230 (2002).
3) Fischer, F., Mansmann, F., Keim, D.A., Pietzko, S. and Waldvoge, M.: Large-Scale Network Monitoring for Visual Analysis of Attacks, *Proc. 5th International Workshop on Visualization for Computer Security*, pp.111–118 (2008).
4) Belotti, P., Malucelli, F. and Brunetta, L.: Multicommodity network design with discrete node costs, *Networks*, Vol.49, Issue 1, pp.90–99 (2007).
5) Chekuri, C., Shepherd, F.B., Oriolo, G. and Scutella, M.G.: Hardness of robust network design, *Networks*, Vol.50, Issue 1, pp.50–54 (2007).
6) El-Alfy, E.-S.M.: Applications of genetic algorithms to optimal multilevel design of MPLS-based networks, *Computer Communications*, Vol.30, Issue 9, pp.2010–2020 (2007).
7) Kim, H.-G., Paik, C.-H. and Chung, Y.-J.: Heuristics for the Access Network Design Problem in 3G Mobile Communication Networks, *Proc. 2008 3rd International Conference on Innovative Computing Information and Control* (2008).
8) Rosenberg, E.: Hierarchical topological network design, *IEEE/ACM Trans. on Network*, Vol.13, Issue 6, pp.1402–1409 (2005).
9) Belotti, P., Capone, A., Carello, G. and Malucelli, F.: Multi-layer MPLS network design: The impact of statistical multiplexing, *Computer Networks*, Vol.52, Issue 6, pp.1291–1307 (2008).
10) Dijkstra, F., Andree, B., Koymans, K., van der Ham, J., Grosso, P. and de Laat, C.: A multi-layer network model based on ITU-T G.805, *Computer Networks*, Vol.52, Issue 10, pp.927–1937 (2008).
11) Salvador, P., Nogueira, A. and Valadas, R.: Local Area Network Modeling for Per-

formance Prediction, *Proc. 32nd IEEE Conference on Local Computer Networks*, pp.249–251 (2007).
12) Habib, S.J.: Redesigning network topology with technology considerations, *International Journal of Network Management*, Vol.18, Issue 1, pp.1–13 (2008).
13) 片岡直登：ネットワーク設計問題，朝倉書店 (2008).
14) Mell, P., Scarfone, K. and Romanosky, S.: A Complete Guide to the Common Vulnerability Scoring System Version 2.0 (2007). http://www.first.org/cvss/cvss-guide.pdf
15) 情報処理推進機構セキュリティセンター：共通脆弱性評価システム CVSS v2 概説 (2007). http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html

(平成 21 年 11 月 30 日受付)
(平成 22 年 6 月 3 日採録)

金岡　晃（正会員）

2004 年年筑波大学大学院博士課程システム情報工学研究科修了．同年セコム株式会社入社．筑波大学大学院システム情報工学研究科研究員を経て 2008 年より筑波大学大学院システム情報工学研究科助教．ネットワークシステムの安全設計方式，電子認証に関する研究に従事．博士（工学）．IEEE，ACM，電子情報通信学会各会員．

原田　敏樹

2009 年筑波大学情報学類卒業．現在，筑波大学大学院システム情報工学研究科博士前期課程に所属．ネットワークシステムの脆弱性影響の研究に従事．

加藤　雅彦（正会員）

1995 年豊橋技術大学大学院知識情報工学専攻修士課程修了．修士（工学）．同年旭化成情報システム株式会社入社．1998 年同社を退職し株式会社インターネットイニシアティブ入社．関連企業のアイアイジェイテクノロジーでシステムインテグレーション，セキュリティ検査，インシデントレスポンス，ネットワークシステムにおける安全性定量評価に関する研究開発業務に従事し，2010 年 4 月より 2010 年 4 月よりインターネットイニシアティブセキュリティ情報統括室シニアエンジニア．日本ネットワークセキュリティ協会幹事，調査研究部会長，日本セキュリティオペレーション事業者協議会運営委員，2008 年度および 2009 年度内閣官房セキュリティセンター WG 委員．クラウドセキュリティアライアンス運営委員．情報処理学会，電子情報通信学会各会員．

勝野　恭治（正会員）

1998 年慶應義塾大学大学院理工学研究科計算機科学専攻修士課程修了．同年日本アイ・ビー・エム株式会社入社．東京基礎研究所主任研究員．2009 年筑波大学大学院システム情報工学研究科リスク工学専攻後期博士課程修了．2003 年ソフトウェア科学会高橋奨励賞受賞．情報セキュリティ，コンピュータ・ネットワーク，エージェント技術に関する研究開発に従事．博士（工学）．日本ソフトウェア科学会会員．

岡本　栄司（正会員）

1973 年東京工業大学工学部電子工学科卒業．1978 年同大学院博士課程修了．工学博士．同年日本電気中央研究所入社．その後，北陸先端科学技術大学院大学，東邦大学をへて 2002 年より筑波大教授．情報セキュリティの教育・研究に従事．1990 年電子情報通信学会論文賞，1993 年本会ベストオーサ賞受賞．著書『暗号理論入門』（共立出版），『電子マネー』（岩波書店）等．