情報処理学会論文誌　Vol. 50　No. 9　2243–2256 (Sep. 2009)

事象連鎖の把握と原因推測が可能なリスク・利便性・対策表示モデルの提案

加藤弘一[†1]　勅使河原可海[†1]

ネットワークのリスクや対策は，リスク連鎖の関係や，複数リスクに効果を発揮する対策の存在など，複雑な関係がある．同様に，対策はネットワークサービスの利便性へ影響を与えうる．そのため，リスク，利便性の正確な把握と導入すべき対策の選定は容易ではない．また，対策変更時には，不適切なリスク増大や利便性低下を避けなければならない．さらに，多くの機器が存在する環境では，インシデントの検出や対応のための管理・監視箇所の決定も困難である．そこで本論文では，リスク連鎖や対策効果の表現，および事象の原因推測が可能なモデルを提案し，実験を通して本モデルが対策選定へ活用できることを示す．本モデルは，リスクが顕在化する流れやサービス利用の流れを状態遷移図で表現し，対策とあわせてネットワークモデル上へ配置することで，リスク，利便性，対策の関係を視覚的に把握することができる．さらに，状態遷移確率を用いることで，本モデルをベイジアンネットワークとして扱い，リスク顕在化の原因の推測が可能となる．

A Proposal of a Risks, Usability and Countermeasures Representation Model for Event Chain Clarification and Causal Inference

Koichi Kato[†1] and Yoshimi Teshigawara[†1]

Network risks and their countermeasures have complex relationships, for example, risk chains and existence of countermeasures effecting to several risks. Similarly, countermeasures can affect to usability of network service. Therefore, proper understanding of risks and usability as well as selecting countermeasures to install are difficult. In addition, inappropriate risk increase and usability decrease must be avoided when changing countermeasures. Moreover, to decide checking or monitoring points for incident detection and response is also difficult in an environment locating with many devices. This paper proposes a model for representing risk chains and countermeasure effects, and estimating causes of events. Under the experiment of a network example, it is confirmed that the model can be utilized for selecting countermeasures. This model expresses phases of tangible risks and services in state transition diagram (STD) and deploys them together with countermeasures on an object network model so that the model can confirm relationship among risks, usability and countermeasures visually. Furthermore, by using probability of state transition, the model can be converted to a Bayesian network and thereby can infer causes of incidents.

1. はじめに

近年，企業などの組織において，情報セキュリティマネジメントシステム（ISMS）の構築が重要視されている．国内では，ISMS 適合性評価制度における認証取得事業者数も年々増加している[1)]．ISMS の構築においては，リスクを分析・評価し，組織が保有する情報資産を保護できる堅牢なセキュリティと，組織の目的達成に必要な利便性を両立できるような対策を選択することが重要である[2)]．同時に，セキュリティ上の問題が起きていないかどうかを把握するために，リスクに関連する箇所の管理・監視も重要なセキュリティ対策の 1 つとして位置づけられている[3)]．

一般的なリスク分析では，資産を洗い出し，資産ごとに脅威や脆弱性を分析してリスクを特定する[4)]．ところが，リスク間には，あるリスクの顕在化が他のリスクの顕在化を誘発するリスク連鎖の関係が存在する．さらに，リスク連鎖は，リスク顕在化に至るまでの中間的な事象から他のリスクへと分岐する場合もある．リスクが連鎖的に顕在化した場合，組織は非常に大きな損害を被ることになりかねない．そのため，リスクを適切に抑制するためには，リスク連鎖の関係を分析することが必要である．しかし，複雑なリスク連鎖の関係を体系的に分析する仕組みは確立されていない．

一方，セキュリティ対策の導入・変更に関する対策選定手法は様々研究されている[5)–8)]．しかし，これらはリスク連鎖を考慮していない．同時に，1 つの利便性の低下が他の利便性低下を引き起こすという利便性の連鎖関係も考慮していない．さらに，必要な対策の理論的な導出を主としており，実際のネットワーク構成を考慮したリスク分析や対策選定について言及していない．

また，セキュリティ状況の監視箇所は経験則により決定される場合が多く，その妥当性を

†1 創価大学大学院工学研究科
Graduate School of Engineering, Soka University

評価できない．加えて，リスクが顕在化した場合には，原因を予測するための客観的な指標がなく，分析範囲が不必要に拡大する場合がある．

本研究の目的は，ネットワーク環境に基づいて，連鎖関係を考慮したリスクと利便性の分析，対策の決定，および監視箇所の選択や事故発生の原因解明が可能な仕組みを構築することである．そこで本論文では，リスク・利便性・対策の関係を視覚的に把握することができ，リスク顕在化の原因を確率的に推測可能な，リスク・利便性・対策表示モデルを提案する．まず 2 章で，既存手法とその問題点を述べる．次に，3 章で本モデルに必要な要件を明確にし，4 章ではネットワーク環境に基づいてリスク，利便性，対策の関係をモデル化する方法を述べる．そして，5 章で本モデルの利用実験を行い，6 章で評価・考察する．最後に，7 章で今後の課題を述べ，8 章でまとめる．

2. 既存手法とその問題点

2.1 FTA を用いたリスクと利便性の分析

文献 7) では，リスクが顕在化するまでの流れやサービス利用の手順をフェーズとしてとらえ，フォルトツリー解析（FTA: Fault Tree Analysis）を用いてリスクや利便性を分析している．この手法では，対象のリスクやサービスを頂上事象におき，フェーズ単位でフォルトツリー（FT: Fault Tree）を展開する．これにより，各フェーズの成立する確率をもとに，対策が必要なフェーズが明確となる．

しかし，リスクや利便性の連鎖関係を FT で表現する場合には，ある FT の一部が別の FT に含まれることになる．FTA では，分析の対象や観点により FT が肥大化することがあり，FT の重複の増加は，分析の労力や対策選定のための計算量の点で問題となる．そのため，リスクや利便性の連鎖や分岐の関係を体系的に把握することが難しい．

2.2 状態遷移リスクモデル

大谷らは，リスクの顕在化における一連の脅威の流れを分析し，状態遷移リスクモデルを作成している[9]．この手法では，状態遷移の有無からリスク連鎖の関係を分析することができる．また，資産価値，脅威の発生確率，対策コストなどを割り当てることで，適切な対策の決定が可能であることを示唆している．

しかし，具体的な脅威の発生箇所や，対策実施箇所など，ネットワーク環境との対応関係については扱っていない．そのため，ネットワーク環境に基づき，リスクと対策の位置づけを把握して対策や監視箇所を決定することは難しい．

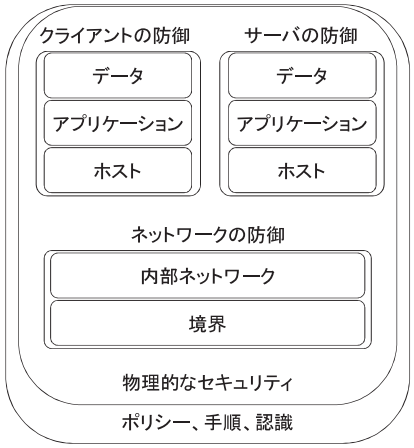

図 1　Microsoft の多層防御セキュリティモデル
Fig. 1　Security model of defense in depth by Microsoft.

2.3 多層防御セキュリティモデル

多層防御とは，データ，アプリケーション，マシン，内部ネットワーク，外部ネットワークとの境界といった様々な箇所で対策をとることで，資産に対する脅威の発生を防ぐという概念である．1 つの脅威に対して複数の対策を実施することで，もし対策の 1 つが損なわれても，他の対策によりリスクの顕在化を抑制することができる．

この多層防御について，Microsoft 社は対策の位置づけを明確に把握するための多層防御セキュリティモデルを示している[10]．さらに，このモデルを扱う際には，**図 1** のようにネットワーク環境に応じてクライアントやサーバなど対象を分類し，複数の層に分けてモデル化することで，ネットワーク環境を考慮した効果的な対策選定が可能となる[11]．しかし，このモデルの対象は，分析された特定のリスクにおける対策選定に限定されており，リスク連鎖には対応していない．

3. モデルに必要な要件

1 章で述べた目的を達成するためには，本モデルにおいて，リスク，利便性，対策の関係，およびネットワーク環境との対応を明確にできる必要がある．また，リスクに対する監視や，事故の原因特定に利用できる必要がある．そこで，本モデルに必要な要件を次のように定め

る．なお，この要件が目的達成に十分であるかどうかは，後述の実験・評価により確認する．

（要件 a）　ネットワーク環境と対応してリスクを表現可能

リスクを正確に分析するために，個々のリスク，およびリスク間の連鎖や分岐の関係を表現できる必要がある．また，ネットワーク環境に即した対策選定を行うために，リスクが顕在化する流れを実際のネットワーク環境と対応して表現できる必要がある．

（要件 b）　ネットワーク環境と対応して利便性を表現可能

業務に支障をきたさないような対策を選択するためには，サービス利用の利便性も考慮すべきである．そこで，個々のサービス利用の利便性，および複数の利便性の連鎖関係を，ネットワーク環境と対応して，リスクとともに表現できる必要がある．

（要件 c）　対策の実施箇所やリスク・利便性との関係を表現可能

ネットワーク環境に即した対策を選択するためには，とりうる対策とその実施箇所，また対策の導入・変更により影響を受けるリスクと利便性を把握できる表現である必要がある．

（要件 d）　監視箇所の選択や事故の原因解明のための指標を提示可能

ネットワークの監視や，インシデント発生時の対応を適切に行うためには，リスクの顕在化につながりやすい，またはリスク顕在化の原因となった箇所や事象を特定するための指標を提示できる必要がある．

4. リスク，利便性，対策のモデル化

本章では，3 章の要件を満たすモデルを構築する手法を述べる．また，4.3 節では本モデルを用いたリスクと利便性の算出方法について述べる．

4.1 ネットワーク環境のモデル化

まず，3 章の全要件で，本モデルがネットワーク環境の表現を必要とするため，ネットワーク環境をモデル化する．一般に，組織のネットワークは DMZ，イントラネットなどの領域に分けられ，さらにイントラネットも部署単位など適当な領域に分割されている．そこで，図 1 のモデルの概念を用いて，分割された領域ごとにネットワークを区切り，各領域にある端末や機器をさらに複数の層に展開したネットワークモデルを作成する．たとえば，簡単なネットワーク構成例として**図 2** のネットワークに対し，DMZ，イントラネットに区切り，各領域にある端末をホスト層，アプリケーション層，データ層に展開すると，このネットワーク環境は**図 3** のようにモデル化される．なお，ここでは FW（Firewall）は対策の 1 つと見なして除外し，ルータは脅威の対象外として省略した．

ここで，ネットワークモデルは，必ずしも図 3 と同じ構成である必要はない．たとえば，同じセキュリティレベルとして扱われる複数の領域を 1 つとして扱う場合や，記憶装置（ハードディスクなど）や I/O デバイス（LAN カードなど）のようなハードウェア関係の層を追加する場合もありうる．モデルの詳細化の程度は，組織の求めるリスク分析の対象や粒度・精度に応じて決定する．

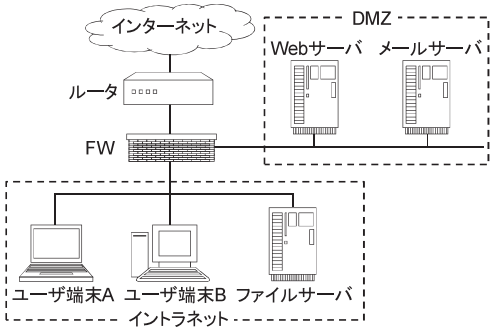

図 2　ネットワーク構成例
Fig. 2　Example of a network configuration.

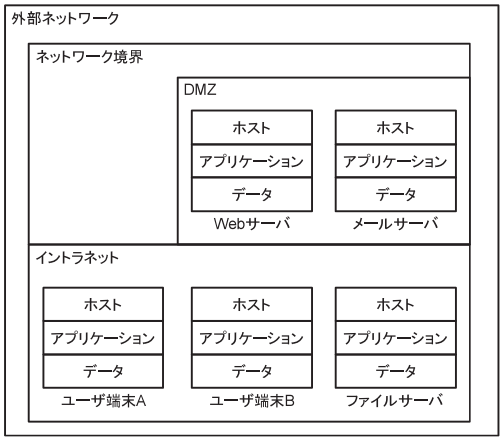

図 3　図 2 のネットワークモデル
Fig. 3　Model of the network in Fig. 2.

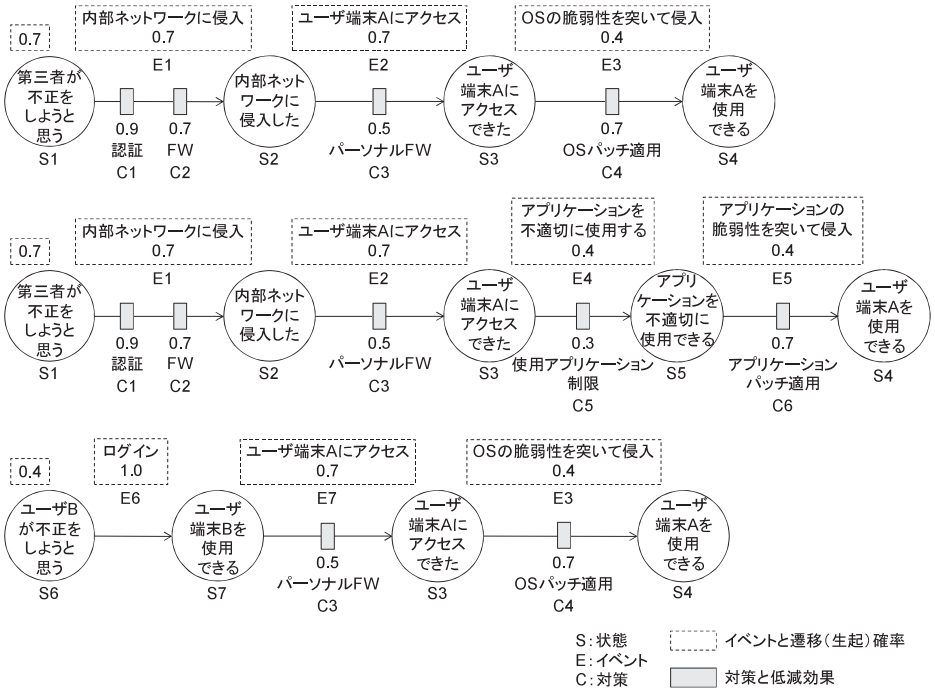

図 4　状態遷移図によるリスク表記
Fig. 4　Risk description using state transition diagram.

4.2　リスク，利便性のモデル化と対策の割当て

本節では，要件 a，b，c へのアプローチを述べる．

(1)　個々のリスクと対策のモデル化

リスクが顕在化するまでには，いくつかのフェーズが存在する．そのため，リスクの顕在化は，各フェーズの成立に応じて状態が遷移し，全フェーズが成立することで最終的に望まない状態へ遷移した結果ととらえることができる．そこで，状態遷移図を用いてリスクが顕在化する流れを表現する．

図 4 は「ネットワーク経由での内部端末 A への不正アクセス」というリスクが顕在化する 3 パターンの流れと，関連する対策を表現している．各状態を結ぶ矢印は，状態が遷移するイベントであり，攻撃の成功確率といった状態遷移確率を保持する．また，フェーズの達成を抑制する対策を，矢印上に重ねて配置する．このとき，同一矢印上に複数の対策が存在してもよい．各対策は，そのフェーズに対する低減効果として，遷移確率を抑制する割合を保持する．また,「〜しようと思う」といった動機など，独立に生起する状態には，その状態が生起する確率（以下，生起確率と呼ぶ）を割り当てる．

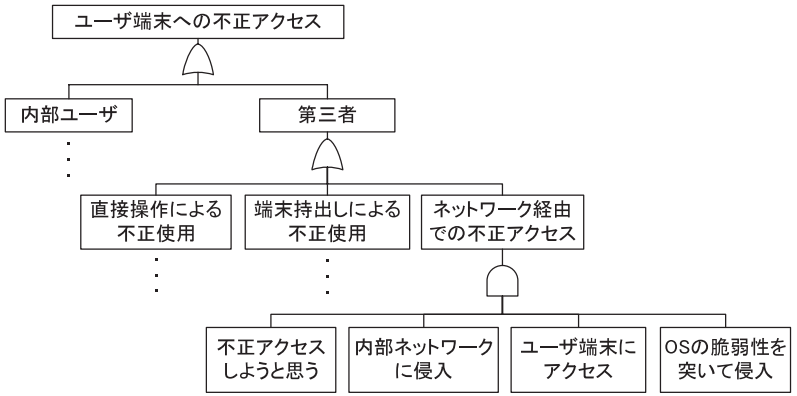

図 5　ユーザ端末への不正アクセスのフォルトツリー
Fig. 5　Fault tree for unauthorized access to a user's PC.

表 1　リスクと対策の分析
Table 1　Analysis of risks and countermeasures.

資産	脅威	基本事象	発生確率	対策	低減効果	実施
ユーザ端末	第三者の経由でのネットワーク不正アクセス	不正アクセスしようと思う	0.7	—	—	—
		内部ネットワークに侵入	0.7	外部からのアクセス認証	0.9	0
				FWによるアクセス制御	0.7	1
		ユーザ端末にアクセス	0.7	ユーザ端末　パーソナルFWによるアクセス制御	0.5	1
		OSの脆弱性を突いて侵入	0.4	ユーザ端末　OSパッチ適用	0.7	1

ここで，**図 5** および**表 1** は，2.1 節の手法に基づく FT と，リスクと対策の分析の例である．図 4 の上部の状態遷移図はこの FT や分析結果と対応しており，FT の基本事象をイベントととらえ，相互に変換可能である．

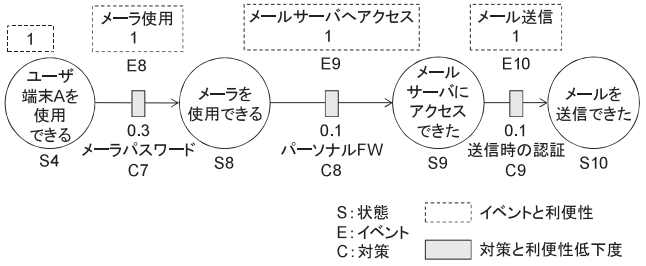

図 6　状態遷移による利便性表記
Fig. 6　Usability description using state transition diagram.

(2)　利便性のモデル化

利便性についても，リスクと同様にモデル化する．サービス利用の流れをフェーズとして分解し，(1) と同様に状態遷移図で表す．**図 6** は「ユーザが利用端末 A からメールを送信する」際の流れを表現している．ここで，各イベント（矢印）は，対策による影響を受けずに利用できる度合いを基準値 1 として保持し，遷移確率とする．各矢印上にはそのフェーズの達成を妨げる対策を配置し，各対策は利便性低下度を保持する．また，初期状態の生起確率は，利用上の制約がない正規ユーザの場合にはその状態をつねに生起できると見なして，基準値 1 を割り当てる．

なお，利便性に関しても (1) と同様に，図 6 は 2.1 節の手法に基づく利便性の FT および分析結果と対応させることができる．

(3)　状態遷移図の結合

図 4，図 6 のように複数のリスクや利便性の状態遷移図が存在するとき，**図 7** のように同一の状態を重ね合わせて結合する．なお，図 7 の状態，イベント，対策の各ラベルは，図 4 と図 6 に対応している．

状態遷移図の結合方法として，(1)，(2) より状態遷移モデルと FT は対応関係があるため，状態とイベントをリスクの構成要素として扱い，べき等律，分配律などにより結合する[12]．ただし，状態遷移は向きがあるため，交換律は適用されない．

ここで，リスクと利便性の結合について，たとえば図 4 と図 6 の “ユーザ端末 A を使用できる” という状態のように，リスクと利便性のモデルに共通して含まれる状態が結合される．これにより，たとえば端末 A からメールを使用して情報漏洩などの不正を行う場合，図 6 の利便性の基準値 1 をそのまま攻撃の成功確率として扱うことができ，利便性モデル

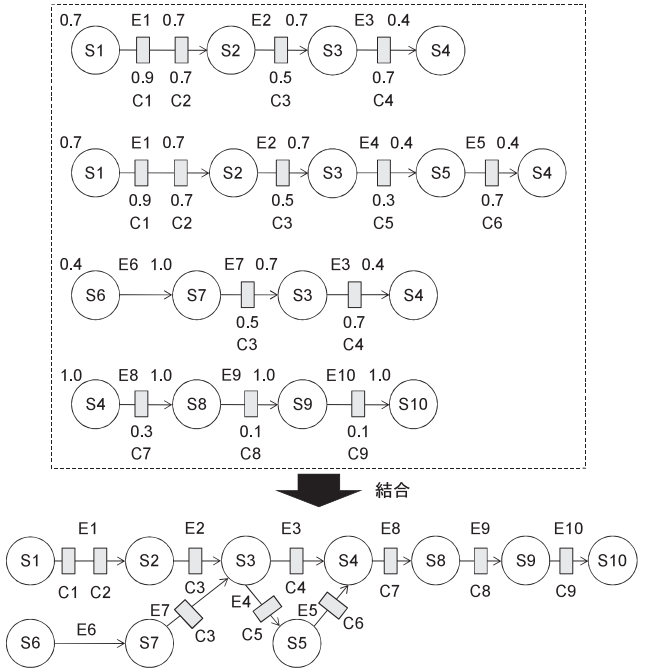

図 7　状態遷移図の結合
Fig. 7　Merging of each state transition diagram.

がそのままリスクモデルへ変化する．

(4)　状態遷移の独立性

本モデルを最大限に活用するために，状態遷移図の作成と結合時において，注意すべき点がある．それは，個々の状態遷移が前後のフェーズと無関係，つまりその状態に遷移した原因やその後に続く遷移を考慮せずにフェーズの遷移確率を割り当てられるように，状態を詳細化して定義することが望ましいということである．

たとえば，図 7 では，第三者（S1）または内部ユーザ（S6）のいずれであるかにかかわらず，端末にアクセスできた（S3）後，端末に侵入するための行為（E3，または E4 かつ E5）に関する遷移確率は，状態 S3 以前の状態遷移に依存しない．このような場合には，結合後のモデルに遷移確率や対策の低減効果の値も表記することができる．

しかし，遷移確率や対策効果が前後の状態遷移に依存する場合がある．たとえば，端末を利用できる状態（S4）にあるときに，メールによる情報漏洩などのリスクが考えられる．メーラ使用時のパスワード（C7）や，メール送信時の認証パスワード（C9）について，正規ユーザはパスワードを知っているため，図 6 のように対策効果が非常に小さい．一方，不正アクセスを行った攻撃者がパスワードを知らない場合，正規ユーザよりも対策効果が大きくなる．ところが，外部の第三者よりも内部ユーザの方がパスワードを推測しやすい可能性がある．つまり，C7 や C9 の対策効果は攻撃者によって異なる場合があり，S4 以前の状態遷移に依存することになる．

このように，状態遷移が前後のフェーズに依存する場合，リスク顕在化の流れや対策の位置づけを把握するために，図 7 のように状態やイベントを結合することはできるが，遷移確率や対策効果の値の結合は，リスクが顕在化する確率（以下，事故発生確率と呼ぶ）の誤った算出につながる．そのため，結合後の状態遷移図にはこれらの値を表記できない．

なお，依存関係が生じる原因は，性質の異なる状態，イベント，対策が同一のものとして分析されているためである．上記の例では，C7 と C9 の対策効果の違いを考慮せず，S4 から S10 に至る状態遷移を攻撃者によらず一律に扱ってしまっている．

しかし，初めからすべての状態遷移が独立となるような分析を行うことは非常に難しく，個々のリスクの分析と，結合による不整合の確認を繰り返す中で，妥当な分析結果を得なければならない可能性がある．

(5)　ネットワークモデルへの配置

4.1 節で作成したネットワークモデルに対し，モデル化されたリスク，利便性，対策を**図 8** のように配置する．状態は成立する適切な箇所に，矢印は経由する層を通るように，対策は実施される層に配置する．ここで，同一領域内の複数の端末が同一のリスク下にある場合，1 つの端末上に配置した結果を他の端末上に複製することも可能であり，必要に応じて対策実施状況の違いなどを端末ごとに調整すればよい．

4.3　事故発生確率，リスク値，利便性の算出

図 8 のように作成されたモデルから，事故発生確率，資産価値を考慮したリスク値，利便性の値を算出する．まず，事故発生確率を算出する対象リスクとして，始点と終点の 2 つの状態を選択する．このとき，複数の始点を選択してもよい．次に，始点から終点へとたどり着くパスを抽出する．そして，式 (1) を用いて，パス n の事故発生確率 P_n を算出する．ここで，パス n に含まれるイベント（始点の生起を含む）e とその集合 E_n，イベント e の遷移確率や生起確率 P_e，対策 i の実施の有無 $X_i \in \{0,1\}$，対策 i を実施したときのイベント e に対するリスク低減効果 $\Delta P_{e,i}$ とする．

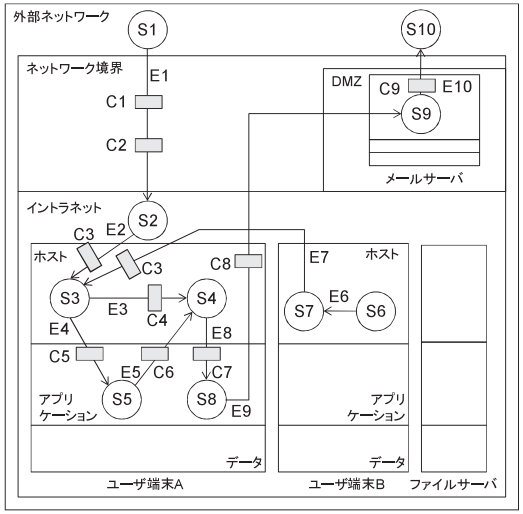

図 8　ネットワークモデルへのリスク，利便性，対策の配置
Fig. 8　Deployment of risks, usability and countermeasures on the network model.

$$P_n = \prod_{e \in E_n} P_e \prod_i (1 - \Delta P_{e,i} X_i) \tag{1}$$

そして，始点から終点へたどり着く総合的な事故発生確率 P_{total} は，すべてのパス（集合 N とする）のうち少なくとも 1 つのパスが成立する確率として，式 (2) により求まる．

$$P_{total} = 1 - \prod_{n \in N} (1 - P_n) \tag{2}$$

なお，4.2 節で述べたように，本モデルは FT との対応関係があるため，式 (1)，式 (2) は FTA における頂上事象の発生確率の算出式と一致する．そのため，複数のパスに共通のイベントが含まれる場合には，遷移確率や低減効果の累乗計算をしてはならず，

$$\left\{ P_e \prod_i (1 - \Delta P_{e,i} X_i) \right\}^2 \rightarrow \left\{ P_e \prod_i (1 - \Delta P_{e,i} X_i) \right\}$$

と置き換えなければならないことに注意が必要である[12]．

さらに，資産価値を考慮した場合を考える．本論文ではリスク値を

表 2　状態遷移確率の条件付き確率への変換
Table 2　Transforming state transition probability to conditional probability.

P(S1)
P_{S1}

P(S6)
P_{S6}

S1	P(S2)
T	P_{E1}
F	0

S6	P(S7)
T	P_{E6}
F	0

S2	S7	P(S3)
T	T	1-(1-P_{E2}) (1-P_{E7})
T	F	P_{E2}
F	T	P_{E7}
F	F	0

S3	P(S5)
T	P_{E4}
F	0

S3	S5	P(S4)
T	T	1-(1-P_{E3}) (1-P_{E5})
T	F	P_{E3}
F	T	P_{E5}
F	F	0

※ P(S2), P(S3), P(S4), P(S5), P(S7) は条件付き確率である．
※ T はその状態に遷移するとき，F は遷移しないときを表す．

リスク値 = 資産価値 × 発生確率

と定義する．たとえば，データ層に位置づけられている状態が終点として選択されたとき，その状態にたどり着く状態遷移はデータに対するリスクである．そこで，式 (1)，式 (2) を用いて事故発生確率を求め，データの資産価値をあわせてリスク値を算出する．ここで，すべてのデータが同一の資産価値とは限らないため，複数のデータについてリスク値を求めたい場合には，対象データごとにリスク値を求める．さらに，データごとにアクセス権が違うなど，対策の実施の有無や対策の低減効果の大きさが異なる場合には，資産ごとにリスクの状態遷移図を複製・展開して個別に事故発生確率を算出し，リスク値を求める．

また，利便性の値は事故発生確率と同様に，始点と終点を決め，たどり着くパスについて式 (1)，式 (2) を用いて算出できる．なお，$\Delta P_{e,i}$ は利便性低下度となる．

4.4　事故発生原因の確率的推測

本節では，要件 d に対するアプローチを述べる．図 8 のような状態遷移図は，確率的に状態間の因果関係を表現しているととらえることができる．そのため，4.2 節 (4) で述べたように各フェーズの遷移確率を前後のフェーズと無関係に割り当てられる場合，各確率を条件付き確率へと変換し，ベイジアンネットワークとして扱うことができる．これにより，リスクが顕在化した場合の原因を確率的に推測することが可能となる．

図 8 において，状態 S4 が発生したとする．このとき，対策をすべて実施していないとすると，S4 に至るパスに含まれる状態がそれぞれ発生する条件付き確率は，**表 2** のようになる．このとき，たとえば S1 が発生していた確率は，

$$P(\mathrm{S1}|\mathrm{S4}) = P(\mathrm{S1} \cap \mathrm{S4})/P(\mathrm{S4})$$

として求めることができる．また，たとえば状態の集合 {S2，S3，S4，S5} に閉じて考えるような場合，生起確率が存在しない．そこで，式 (1)，式 (2) を用いて S2 の発生確率を求め，生起確率とする．

以上より，ある状態から逆向きにたどる経路上に存在する任意の状態について，原因となった可能性を推測することができる．

5.　本モデルの利用実験

本章では，簡単なネットワークを想定し，対策導入時と対策変更時におけるモデルの作成および利用に関する実験を行う．なお，本実験では，本モデルを用いることで，連鎖関係を考慮してリスクや利便性の流れを分析し，この流れに対して実施箇所を考慮した対策選定が可能であるかどうかを確認する．そのため，資産価値を含むリスク値ではなく，事故発生確率や利便性に基づく分析を行う．

5.1　想 定 環 境

複雑なネットワーク構成は分析が煩雑になるため，簡単なネットワークとして図 2 のネットワークを想定する．ユーザはユーザ端末を使用して Web 閲覧やメール送受信，ファイル操作などの一般業務を行う．また，DMZ には外部に公開された Web サーバ，メールサーバが設置されている．

また，実組織のネットワークにおけるリスク分析結果は重要なセキュリティ情報であり入手困難なため，本論文では簡易的にリスクを分析する．扱うリスクは，ネットワーク経由でのユーザ端末への不正アクセス，ネットワーク経由での機密情報の外部への漏洩，ユーザ端末へのウィルス感染の 3 つとする．また，利便性として扱うサービスは，Web 閲覧，メー

ル送信，メール閲覧，ファイルサーバ内のファイル使用の 4 つとする．

遷移確率や対策効果については，ISMS ユーザーズガイド[13] を参考に，段階で分けることとした．本実験では，リスクの各フェーズの遷移確率は 4 段階（0.1，0.4，0.7，1.0），対策によるリスクの低減効果は 5 段階（0.1，0.3，0.5，0.7，0.9）とした．一方，利便性については各フェーズの遷移確率を基準値 1 とし，対策による利便性低下度は 5 段階（0.1，0.3，0.5，0.7，0.9）とした．そして，対策の未実施を 0，実施を 1 として表現した．

5.2　対策導入時

(1)　モデルの作成

まず，ネットワークをモデル化する．5.1 節で述べた対象のリスクと利便性を考える際，図 1 のようにデータ，アプリケーション，ホスト（OS）が主に関係すると考え，本実験ではネットワークモデルを図 3 のように定めた．

次に，本実験で扱うリスクについて，資産，脅威，脆弱性を列挙する．そして，図 5 のように，リスク顕在化またはサービス利用に結び付くフェーズを分析する．そして，表 1 のように，各フェーズの遷移確率を割り当て，各フェーズへの対策を列挙し，対策の低減効果（利便性低下度）と実施の有無を割り当てる．

これらの結果から，リスクと利便性を状態遷移図で表し，対策とともにネットワークモデル上に配置する．この結果，**図 9** のようなモデルが作成された．なお，図が煩雑になるため，状態名や対策名は簡易表記とし，イベント名，遷移確率，対策の低減効果や利便性低下度は省略している．また，ユーザ端末 B はユーザ端末 A における状態遷移図を複製したものであるため，ユーザ端末 B の対策や，ユーザ端末 B から生じる状態遷移は，図の簡素化のため省略した．

(2)　リスク分析と対策選定への活用

本実験では，モデル作成時に，リスク分析結果や対策実施の有無がいくらか見直された．まず，フェーズの粒度が粗く，対策が効果を発揮する箇所を適切に表現できない部分があったため，より詳細なフェーズに展開する修正が行われた．これは，本モデルにより，ネットワーク構成に対して，リスクの各フェーズや対策の位置づけが明確になったことによる．具体的には，リスク分析時には，“PC にアクセス” できた状態から “PC の使用” ができた状態への遷移に対し，OS のパッチ適用とアプリケーションのパッチ適用の 2 つの対策があげられていた．しかし，モデル作成時に，後者はアプリケーション層における対策と判断した．そこで，“アプリケーションの不適切な使用” ができる状態を追加し，この状態から “PC の使用” への遷移上に “アプリケーションのパッチ適用” の対策を記述した．また，不要なアプリケーションのインストールや使用ができないようにすることで，PC にアクセスされてもアプリケーションの不適切な使用が抑制できると考え，“PC にアクセス” から “アプリケーションの不適切な使用” への遷移上に “使用可能なアプリケーションの制限” を対策候補として追加した．なお，この対策は実施しないと判断したため，図 9 には記載されていない．また，この修正に合わせて，“ウィルス感染” へのイベントと，関連する対策が追加された．

また，複数のリスクに共通するフェーズについて，前後の状態遷移に関係なく確率を割り当てられる遷移でありながらリスクによって遷移確率が異なっていたため，遷移確率の修正があった．これは，状態遷移の結合によって複数のリスクの分析結果の不整合を発見できたためである．たとえば，不正アクセスと情報漏洩の両リスクの分析結果において，“PC にアクセス” できてから “PC を使用” できる状態への遷移確率が異なっていたが，情報漏洩へと遷移が続くかどうかにかかわらず，この確率は同じであるとして，同一の値に修正された．

同様に，複数のリスクに共通して含まれるフェーズについて，個々のリスクの分析時に同じ対策があげられたが，割り当てられた低減効果の値が異なっていた．そのため，低減効果の値の修正があった．これは，上記と同様に，状態遷移の結合時に不整合を発見できたためである．

また，あるリスクのフェーズに対して選択した対策が他のリスクのフェーズにも効果を発揮することを発見したため，分析漏れのあったフェーズに対して対策の低減効果と実施の有無を追加した．これは，リスクのフェーズや対策が位置づけられる層が明確になることで，同じ層を通過する他のイベントに対して対策効果があるかどうかを判断できたためである．具体的には，情報漏洩への対策としてあげられた “データのアクセス権の設定” を実施した場合には，ウィルス感染の抑制やメールでの添付ファイルの送受信に影響すると判断し，これらに関連するデータ層への状態遷移に対して，同一の対策が追加された．また，該当フェーズごとにこれらの対策の低減効果が割り当てられた．

さらに，複数のリスク（遷移）に共通して効果を発揮する対策として，“Web フィルタリング”，“パーソナル FW（PFW: Personal Firewall）による inbound アクセス制限”，“PWF による outbound アクセス制限”，“メールでの添付ファイル使用制限” が追加された．これは，本モデルを用いることで，同一の層を通過するイベントが明確となり，複数のイベントに対して効果を発揮する対策があるかどうかの判断が容易になったためである．たとえば，“Web フィルタリング” を実施すれば，3 つのフェーズに対して効果を発揮するため，効率良く対策が実施できると判断した．

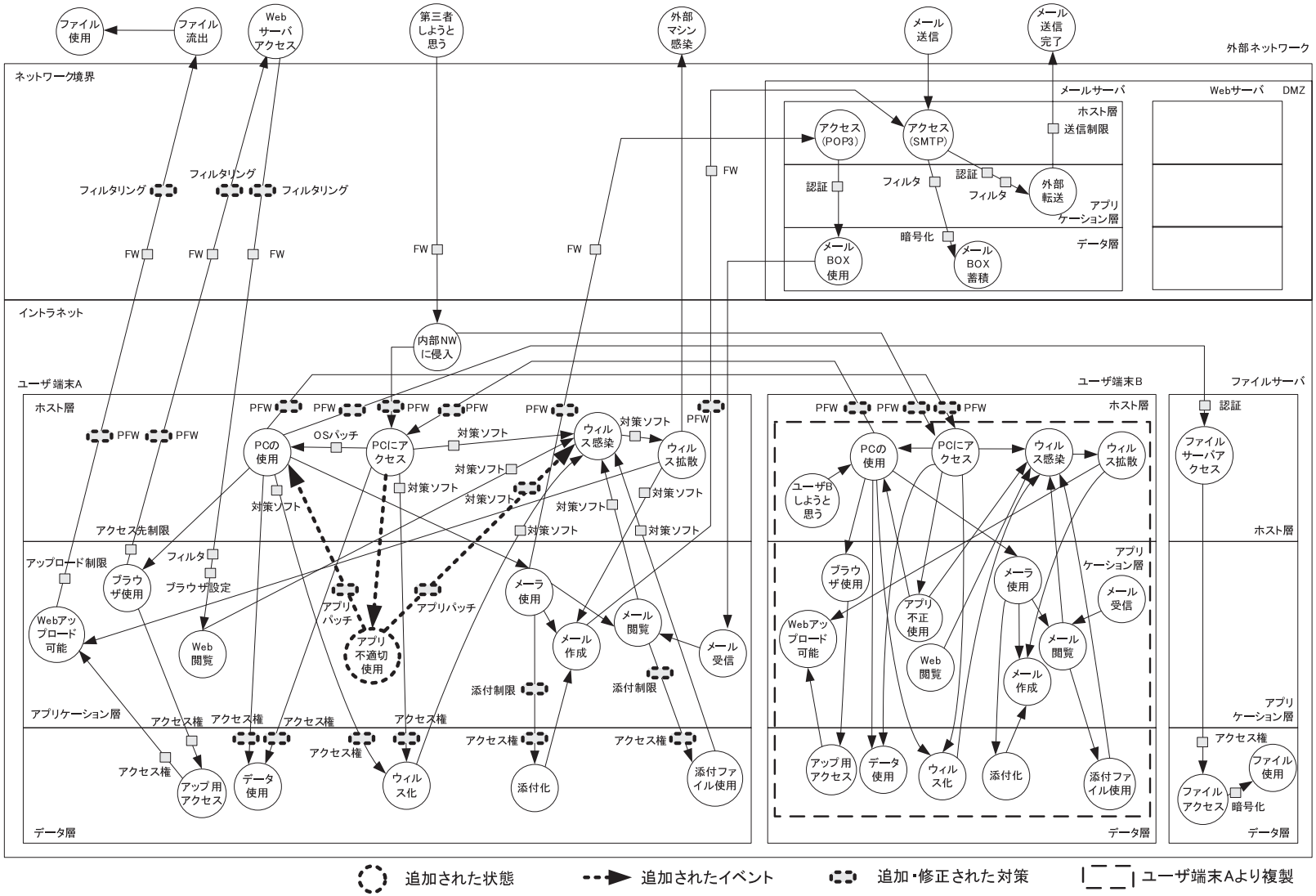

図 9　想定ネットワークにおけるリスク，利便性，対策のモデル化
Fig. 9　Modeling of risks, usability and countermeasures in the assumed network.

表 3　初期分析，およびモデルを利用した再分析後の事故発生確率と利便性
Table 3　Probability and usability by first analysis and reanalysis using the model.

リスク・利便性		初期分析	再分析後
リスク	不正アクセス	0.0285	0.0494
	情報漏洩	0.0430	0.0139
	ウィルス感染	0.0181	0.0158
利便性	Web アクセス	0.810	0.590
	メール送信	0.590	0.413
	メール閲覧	0.590	0.459
	ファイルサーバ利用	0.729	0.510

最初の分析時と，本モデルを用いて行われた上記の修正後における，事故発生確率と利便性の値を**表 3** に示す．なお，一部に事故発生確率の増大や利便性の低下が見られるが，リスクや利便性をより正確にとらえ，対策を選択したうえで許容された値であり，望まない事故発生確率の増大や利便性の低下となったわけではない．

このように，本モデルを用いることで，ネットワーク構成に対応してリスク顕在化の流れを分析できているかどうかを検証し，複数のリスクに共通するフェーズの遷移確率の不整合を解消して，リスク分析結果へ反映させることができた．また，対策が効果を発揮する順序や箇所が明確となるため，複数のリスクにおける対策の低減効果の不整合を解消しつつ，各フェーズに対して必要な対策を決定することができた．以上から，本モデルはリスクや対策の分析，さらに対策の選定に利用可能であることが確認できた．

5.3　対策変更時

(1)　リスク連鎖の関係の把握と抑制

対策を変更する場合にはセキュリティと利便性の変化を把握できることが重要であり，対策を追加するなどの処置が必要な場合もある．そこで，対策変更を行った場合に，どのような状態へ遷移しやすくなるのか，また，各対策の効果について，図 9 のモデルを用いて確認した．

たとえば，ユーザが一時的に FW の特定ポートを開放してほしいと要求した場合を考える．FW のポートを開放した場合，第三者が内部ネットワークへ侵入する確率が高くなる．同時に，この変化により “内部ネットワークへ侵入” 以降に続くすべての状態へ第三者がたどり着く確率が増加する．これに対し，考えられる効果的な対策は，FW と同一遷移上にある “ネットワークアクセス時の認証” の実施（通常時には未実施と判断されていたため，図 9 では非表示）であり，これによって内部ネットワークへの侵入を抑制できる．また，直後の遷移上にある “PFW” の対策強化も考えられ，PC へのアクセスを防ぐことで，以降の状態への遷移を抑制できる．

このように，対策変更を行った部分に該当する遷移の直後の状態を基点として，遷移と順方向へたどることで連鎖的に発生しうる状態を，逆方向へたどることでその状態となる原因を確認することができる．さらに，連鎖を食い止めるか，原因を排除するかという方針に応じて，選択すべき対策を絞り込むことができる．

なお，図 9 における FW の特定ポートの開放では他のフェーズへの影響がなかったが，たとえばウィルス対策ソフトのように複数フェーズに効果を発揮する対策を変更する場合もありうる．この際には，モデルを用いて対策変更の影響を視覚的に把握するとともに，影響するフェーズを含むそれぞれのリスクについて事故発生確率やリスク値の変動を算出することで，対策が必要なリスクや対策実施箇所を検討することができる．

(2)　利便性への影響の把握と対応

たとえば，あるリスクの抑制のために，メーラ使用時にパスワードを使用することになったとする．このとき，“PC の使用” から “メーラの使用” へ遷移する際の利便性が低下し，その先へ続くメールの送信や閲覧へ影響する．

このように，本モデルを用いることで，セキュリティ対策の変更にともなう利便性への影響を把握することができる．さらに，利便性の回復について，リスクや利便性に与える影響を確認しつつ，原因を解消するか，その先の利用行為を快適にできるようにするかを考慮して，対応を検討することができる．

5.4　事故発生原因の確率的推測

ここでは，例として “端末 A が不正に使用される” 状態を考える．まず，“端末 A を使用できる”（図 9 の端末 A における “PC の使用”）状態から逆方向の経路を抽出する．抽出結果は**図 10** のようになる．なお，図 10 では未実施の対策も記述し，ユーザ端末 B に関しては状態 S6，S7，およびこれらに関連するイベントと対策に限定した．また，図 9 では簡易表記であった状態名や対策名を，図 10 では具体的に記述している．

ここで，図 10 は図 8 と対応した表記になっているが，図 8 に存在しないイベント E11 と対策 C10 を含んでいる．これは，図 9 から，内部ネットワークに侵入後，端末 B へもアクセスされる可能性があることと，端末 B を踏み台にして端末 A へアクセスするリスクが考えられるためである．ただし，外部から端末 B を使用できる状態へたどり着くためには，端末 B へアクセスして侵入することが必要であり，本来はこれを考慮した分析が必要であ

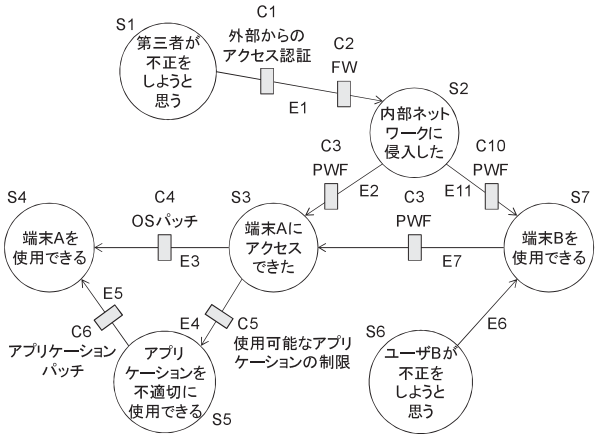

図 10　ユーザ端末の不正使用の原因候補
Fig. 10　Candidates of the causes in unauthorized use of a user's PC.

表 4　状態遷移確率，対策の低減効果，対策実施状態の関係
Table 4　Relations among probability of each state transition, countermeasure effect and the state of implementation.

初期状態，イベント	遷移（生起）確率	対策	低減効果	実施
S1	0.7	—	—	—
S6	0.4	—	—	—
E1	0.7	C1	0.9	0
		C2	0.7	1
E2	0.7	C3	0.5	1
E3	0.4	C4	0.7	1
E4	0.4	C5	0.3	0
E5	0.4	C6	0.7	0
E6	1.0	なし	—	—
E7	0.7	C3	0.5	1
E11	0.7	C10	0.5	1

るが，ここでは簡単のため S2 から S7 へ直接イベントをつないだ．

次に，各遷移確率から条件付き確率へ変換し，原因の確率的推測を行う．5.2 節より，状態の生起確率，遷移確率，対策の低減効果と実施の有無が**表 4** のように分析，決定された．このときの，“端末 A が不正に使用される” 原因を推測する．FW（図 10 中 C2）開放前，

表 5　ユーザ端末不正使用の原因の推測
Table 5　Causal inference of unauthorized use of a user's PC.

	FW 開放前	FW 開放後	認証追加時
P(S1 | S4)	0.78	0.86	0.73
P(S2 | S4)	0.38	0.77	0.15
P(S3 | S4)	1.00	1.00	1.00
P(S5 | S4)	0.72	0.72	0.72
P(S6 | S4)	0.80	0.59	0.92
P(S7 | S4)	0.90	0.78	0.96

開放後，外部からのアクセスに対する認証（図 10 中 C1）を追加した場合において，S4 が発生した際に各状態がそれぞれ発生している確率は，**表 5** のようになる．

まず，FW 開放前は外部からのアクセスを防いでいるため，第三者が不正をしようと思っていても（S1），内部ネットワークに侵入できていた（S2）確率は抑制されている．一方で，端末 B を使用していた（S7）確率が高く，ユーザ B がしようと思っていた（S6）可能性も高い．このことから，内部ユーザによる不正が大きく疑われる．

次に，FW を開放すると外部からのアクセスが容易になる．そのため，第三者が内部ネットワークに侵入した（S2）可能性が急激に増加している．このことから，第三者による不正の疑いが大きくなる．

そして，外部からのアクセス時に認証を実施するようにした場合，第三者が内部ネットワークに侵入した（S2）可能性は大きく低下している．端末 B を使用していた（S7）確率が高く，ユーザ B がしようと思っていた（S6）可能性も高いため，内部ユーザによる不正がより強く疑われる結果となった．

なお，端末 A を不正使用できた（S4）場合，必ず端末にアクセスできている（S3）ことになる．また，端末 A にアクセスした（S3）後，OS とアプリケーションのどちらの脆弱性を突いて端末 A へ侵入するか，つまり S5 を経るか経ないかは，攻撃者や攻撃経路（それ以前の状態）に関係ないとしている．そのため，

$$P(\mathrm{S3}|\mathrm{S4}) = 1,\ P(\mathrm{S5}|\mathrm{S4}) = 0.72$$

で一定となっている．

このように，対策の変更に応じて，各状態が原因となりうる確率を推測することができる．そのため，この確率を，事前の監視箇所の決定や事故が起きた際の原因分析のための情報の 1 つとして利用できる．

なお，4.4 節で述べたように，この推測を行うためには，各フェーズの遷移確率が前後の

フェーズと無関係である必要がある．そのため，対策の効果も該当イベントで完結し，それ以降の遷移に影響してはならない．ただし，複数のフェーズに同一の対策が存在してはならないということではない．各状態遷移が独立であるという条件を満たさない場合には，遷移確率や対策の低減効果が他のフェーズに影響しないようにモデルを見直す必要がある．

6. 評価・考察

6.1 本モデルの要件達成に関する評価

5 章の結果から，本モデルが 3 章の 4 つの要件を満たしているかどうかを評価する．

(1) ネットワーク環境に対応したリスク表現

5.2 節において，リスク分析結果をもとに，個々のリスクが顕在化する流れを状態遷移図でモデル化し，複数の状態遷移を結合して，実際の構成に基づくネットワークモデル上に配置した．この結果，本モデルにより，リスクの各フェーズとネットワーク環境との対応関係を表現できた．また，5.3 節より，あるリスク顕在化によって連鎖的に顕在化しやすくなるリスクが明確となり，リスク連鎖の関係を表現できることが確認できた．

(2) ネットワーク環境に対応した利便性の表現

5.2 節でのモデル作成時に，利用サービスの流れも状態遷移図でモデル化し，リスクの状態遷移と結合して配置した．これにより，本モデルが，利便性の連鎖関係を表現でき，かつ利便性をリスクと同時に表現できることを確認した．また，5.3 節より，対策変更にともなう利便性への影響を把握することができることを確認した．

(3) 対策の実施箇所やリスク・利便性との関係の表現

5.2 節において，モデル作成時に対策を該当する層へと配置した結果，対策実施箇所を明確に把握することができた．さらに，5.3 節より，対策変更にともなうリスクや利便性への影響が明確となったことから，本モデルは対策とリスク・利便性の関係を表現できているといえる．

(4) 監視箇所の選択や事故の原因解明の指標提示

5.4 節において，各フェーズの遷移確率を条件付き確率へと変換し，ベイジアンネットワークとして扱った．この結果，監視箇所の決定や事故原因の解明のための指標として，リスクの原因を確率的に推測できることが確認できた．

6.2 本モデルの有効性と要件の十分性に関する評価・考察

3 章の 4 つの要件を満たす本モデルが，1 章で述べた目的を達成できるかどうかを評価・考察する．また，本モデルが備えるべき要件がこの 4 つで十分であるかどうかを確認する．

(1) 連鎖関係を考慮したリスクと利便性の分析

5.2 節より，個々のリスクの状態遷移を結合することで，リスクの連鎖関係が明確となった．また，複数のリスクにおける分析結果の不整合を発見・修正することができた．さらに，ネットワーク環境と対応させた分析により，リスク顕在化の流れをより詳細に分析することができた．利便性も同様に，個々の利便性の状態遷移を結合することで，利便性の連鎖関係が明確となった．

このことから，本モデルにより，ネットワーク環境に基づいて，連鎖関係を考慮したリスクと利便性の分析が可能である．

(2) 対策選定への活用

対策導入時において，フェーズに基づいて対策を検討することで，複数のリスクに共通して効果を発揮する対策を決定することができた．また，対策実施箇所が明確となることで，あるフェーズへの対策が他のフェーズにも効果を発揮することを発見し，分析時の見落としを解消することができた．加えて，複数のリスクに共通するフェーズへの対策について，対策効果の不整合を発見することができた．このことから，本モデルを用いることで，対策導入時において対策効果や対策実施箇所をより正確に分析し，対策選定に活用することができる．

また，対策変更時には，対策変更によるリスクや利便性への影響を視覚的に把握することができる．そして，対策変更箇所に対して，前のフェーズで対策を実施して原因を抑制するか，後のフェーズで対策を実施して連鎖を防ぐかという判断が可能となる．このことから，本モデルでは，対策変更時において，リスク増大や利便性低下を抑制する対策の選定にも活用することができる．

ただし，リスクや利便性を正しく評価するためには，状態の生起確率や遷移確率，対策のリスク低減効果や利便性低下度が正確でなければならない．しかし，これらの値や利便性の判断基準は，組織やユーザによって異なるため，妥当な値を決定することは難しい．この対応の 1 つとして，リスクの分析・評価と，運用を通した見直しを繰り返すことにより，妥当な値へと改善する方法がある．また，文献 5) のようにリスクや利便性の影響を受ける関与者が参加して値を決定することも，現実的な対応方法の 1 つであると考えられる．

(3) 監視箇所の選択や事故原因の解明への活用

本モデルでは，リスクの原因を確率的に推測することができる．そのため，原因となる可能性の高い事象や，その事象を含む機器において監視を行うことで，リスク顕在化を検出することができる．また，それ以前のフェーズに対して監視を行うことで，リスクが顕在化す

る前に対応することも可能になる．

さらに，リスクが顕在化してしまった際には，原因であった可能性の高い事象を特定することができる．このような事象を対象として事後調査を行うことで，効率的に事故原因の解明が可能になると期待できる．

(4) 本モデルが備えるべき要件の十分性

本節 (1)，(2)，(3) より，本モデルは，ネットワーク環境に基づいて，連鎖関係を考慮したリスクと利便性の分析と，対策導入時および対策変更時における対策選定が可能である．また，監視箇所の選択や事故発生の原因解明のための指標を得ることができる．このことから，本モデルにより 1 章で述べた目的を達成することができ，本モデルが備えるべき要件が 3 章で述べた 4 つで十分であるといえる．

7. 今後の課題

7.1 物理的リスクへの対応

本モデルは，ネットワーク利用に関するリスクや利便性を対象としている．そのため，物理的なリスクや対策を考慮できていない．しかし，組織におけるリスクは，端末や印刷物の盗難，機器の直接破壊といった人的リスク，停電や災害など，様々なものがある．そのため，これらのリスクも表現できるようにすることで，より環境に適合したリスクの把握ができるようになる．今後は，現在のモデル上に物理的な空間モデルを重ね合わせるなどの検討を行う．

7.2 本モデルの拡張性の検証

5.2 節で作成したモデルは，簡単なネットワークにおける 3 つのリスクと 4 つのサービス利用だけでも，状態数が多くなってしまった．そのため，実際のネットワークにおいて，多くのリスクや利便性をモデル化しようとした際には，膨大な状態数となることが予想される．一方で，同一経路を経由するリスクや利便性は共通の状態遷移を含むことが多く，ある程度状態数が増えると，状態の増加数が小さくなる可能性もある．また，本実験では扱わなかった資産価値を考慮した場合，異なる価値を持つ複数の資産を考慮してリスク値を算出する必要があるため，分析がより複雑になる可能性がある．

そのため，より複雑なネットワーク環境における多数のリスクや利便性について本モデルを用いて分析し，本モデルの拡張性について検証する．さらに，資産価値を考慮した場合における分析への影響についても検証する．

7.3 各状態遷移の独立化

リスクの原因の確率的推測を行うためには，各状態遷移が前後の状態遷移と独立になるようにモデルを作成する必要がある．状態遷移を独立させる 1 つの方針として，いつ，誰により遷移するのかといった要素を状態やイベントに含ませる方法が考えられる．一方で，多くの要素を考慮してリスクを細分化すると，状態の結合ができず，7.2 節で述べた状態数の肥大化へとつながる可能性がある．そのため，リスク分析の詳細さの程度と状態遷移の独立性に関して検討する必要がある．

7.4 作成したモデルの妥当性の証明

本実験では，リスク分析の結果をもとにモデルを作成し，状態遷移とその確率，対策の効果と位置づけについて見直しを繰り返すことで，より正確な分析へとつなげた．そのため，分析を重ねて最終的に作成されたモデルを，妥当なモデルと見なした．しかし，実際には不適当な状態遷移を含む場合や，状態の分析漏れが生じる場合も考えられる．そのため，リスク分析者やモデル作成者による主観的な判断ではなく，モデルの妥当性を客観的に評価する仕組みについて検討が必要である．

さらに，6.2 節 (2) で述べたように，遷移確率や対策効果，利便性の判断基準について妥当な値を決定することは難しい．そのため，本モデルを実際の組織のネットワークに適用し，妥当な値を決定するための現実的な評価尺度を検討する．

8. ま と め

本論文では，リスクや利便性の連鎖関係を考慮した対策選定を実現するために，リスク，利便性，対策の関係を視覚的に把握でき，かつリスク顕在化の原因を確率的に推測可能なモデルを提案した．まず，モデルの作成方法として，状態遷移図を用いてリスクと利便性をモデル化し，対策とともにネットワークモデルへ配置する手法を述べた．また，本モデルをベイジアンネットワークとして扱い，リスク顕在化の原因を確率的に推測する方法を述べた．さらに，利用実験を通して，本モデルがリスクや利便性の連鎖関係を考慮した対策選定に活用できることを確認した．

今後は 7 章で述べた課題に取り組み，実際の組織のネットワークにおいて，物理的リスクなどを含む多くのリスクを対象として扱えるモデルの確立を目指していく．

参 考 文 献

1) JIPDEC：ISMS 適合性評価制度．http://www.isms.jipdec.jp/isms.html

2) 打川和男（著），ジェイエムシー（編）：市場の失敗事例で学ぶ情報セキュリティポリシーの実践的構築手法，オーム社 (2003).
3) ISO: ISO/IEC 27002. http://www.iso.org/iso/home.htm
4) ISO: ISO/IEC 13335. http://www.iso.org/iso/home.htm
5) 佐々木良一，日高　悠，守谷隆史，谷山充洋，矢島敬士，八重樫清美，川島泰正，吉浦裕：多重リスクコミュニケータの開発と適用，情報処理学会論文誌，Vol.49，No.9，pp.3180–3190 (2008).
6) 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝：セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌，Vol.45, No.8, pp.2022–2033 (2004).
7) 加藤弘一，勅使河原可海：ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案，情報処理学会論文誌，Vol.49, No.9, pp.3209–3222 (2008).
8) 榊　啓，矢野尾一男，小川隆一：多目的最適化によるセキュリティ対策立案方式の提案，コンピュータセキュリティシンポジウム 2007（CSS2007）論文集，Vol.2007, No.10, pp.193–198 (2007).
9) 大谷尚通，梅田伸明：不正アクセス行為の状態遷移モデルに基づくセキュリティ脅威と対策作成方法，コンピュータセキュリティシンポジウム 2007（CSS2007）論文集，Vol.2007, No.10, pp.283–288 (2007).
10) Microsoft：Windows 2000 Server セキュリティ運用ガイド，第 2 章—セキュリティリスクとは．http://www.microsoft.com/japan/technet/security/prodtech/windows2000/staysecure/secops02.mspx
11) Microsoft：第 3 章—クライアント，サーバー，およびネットワークのための対ウイルス防御．http://technet.microsoft.com/ja-jp/library/cc162798.aspx
12) 塩見　弘，島岡　淳，石山敬幸：日科技連信頼性工学シリーズ 7 FMEA，FTA の活用，日科技連 (1983).
13) JIPDEC：ISMS ユーザーズガイド—JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応—リスクマネジメント編．http://www.isms.jipdec.jp/doc/JIP-ISMS113-21.pdf

(平成 20 年 12 月 1 日受付)
(平成 21 年　6 月 4 日採録)

加藤　弘一（学生会員）

2005 年創価大学工学部情報システム学科卒業．2007 年同大学大学院工学研究科博士前期課程修了．現在，同大学院工学研究科博士後期課程在学中．情報セキュリティに関する研究に従事．

勅使河原可海（フェロー）

1970 年東京工業大学大学院理工学研究科制御工学専攻修了．工学博士．同年日本電気入社．コンピュータネットワーク，ネットワークアーキテクチャ，衛星データネットワーク等の開発に従事．1994〜1996 年ハワイ大学アロハシステム客員研究員，1995 年創価大学工学部教授，工学部長，工学研究科長を歴任．ユビキタスコンピューティング，グループウェア，e-learning，ネットワークセキュリティ等の研究に従事．情報処理学会，オペレーションズリサーチ学会各フェロー，電子情報通信学会，経営情報学会，IEEE，ACM 各会員．