2009-IOT-4 (37)
2009 / 3 / 6

# 内的セキュリティ問題に対する自動管理システムのための知識の定式化

森下壮一郎† 橋口 博樹†† 三島 健稔††

† 東京大学人工物工学研究センター
〒 277–8568 千葉県柏市柏の葉 5–1–5
†† 埼玉大学大学院 理工学研究科
〒 338–8570 埼玉県さいたま市下大久保 255
E-mail: †mori@race.u-tokyo.ac.jp

**あらまし** 内的セキュリティ問題とは，外部からの侵入などではなく内部の利用者によって引き起こされるセキュリティに関する問題を指す．特に計算機システムの管理者によるものは深刻な結果をもたらしかねない．我々は今までにこれに対処するための自動管理システムを提案している．自動管理システムは認識機構，判断機構，応答機構の三機構からなるものであるが，本論文ではこのうち判断機構の構築方法について詳細を述べ定式化を行う．そしてその検証のためにネットワーク機能の一部についての知識を構築し，それに基づく動作の実例を示す．

**キーワード** 内的セキュリティ問題，Fault Tree Analysis，知識表現，システム管理．

# Formalization of Knowledge for Automatic Administration System to the Internal Security Problem

Soichiro MORISHITA†, Hidetsune KOBAYASHI††, and Taketoshi MISHIMA††

† RACE, The University of Tokyo
5–1–5 Kashiwanoha, Kashiwa, Chiba, 277–8568, Japan
†† Graduate School of Science and Engineering, Saitama University
255 Shimo-Okubo, Saitama, 338–8570, Japan
E-mail: †mori@race.u-tokyo.ac.jp

**Abstract** An internal security problem means the problem about security matters caused by users on the inside rather than outside intruders. In particular, the one caused by system administrators would bring grave consequences. We have proposed an automatic administration system to solve the problem. This system consists of recognition function, decision function and response function. In particular, this paper focuses on the decision function and formalizes it. Knowledge on computer network is established by administrator and the process of improvement is shown in order to indicate the validity of the formulation of the knowledge.

**Key words** Internal Security Problem, Fault Tree Analysis, Knowledge Representation, System Administration.

## 1. はじめに

現在，計算機システムの利用は社会のあらゆる分野へと拡がり，その重要性はますます高まっている．これに伴って計算機システムのセキュリティ問題が社会活動の根幹にまで影響を与える大きな課題となっている．

計算機システムのセキュリティ問題は大別して外的なものと内的なものとに分けられる．前者は利用権限を持たない外部の人間が計算機リソースを消費しようとするものであり，認証や暗号化などの対策が有効である．しかし後者は利用権限を持つ人間がリソースを毀損してしまうものであり，本質的に有効な対策はない．

内的セキュリティ問題はさらに過失と背信行為とに分けられる．これらはいずれも人的要因であり，人間が計算機が利用するとき常に生じる危険がある．正規の者による計算機の利用は制限できないのでこれらを完全に排除することはできない．

システム管理者による内的セキュリティ問題は障害に直結するので一般の利用者によるものに比べてより深刻である．一方で，システム管理からは作業の自動化により人的要因を排除することができる．完全に自動化されないまでも，人間が作業を

する機会が減ればそれだけ内的セキュリティの危険も減少する．

我々は既に内的セキュリティ問題を解決するための計算機の自動管理システムを提案している[1]．これは，人間の管理者に変わって計算機システムの管理作業を行うシステムであり，一種のエキスパートシステムである．その知識獲得のために障害分析手法の一つである FTA(Fault Tree Analysys)[5] を用いる．これにより系統的な知識獲得が可能であり，また AND-OR tree で知識が表現されるので推論機構の構築が容易になる．さらに，管理対象についての知識と運営方針に基づく知識とを分離することで，汎用性のある自動管理システムが実現でき，計算機システムの柔軟な運用が可能になる．

以上の考えに基づき，本研究ではまず内的セキュリティ問題について詳細を述べ，次に認知心理学におけるモデルを参考に運営方針等まで含めた広義の管理作業を分析する．さらにその結果をふまえて内的セキュリティシステムをデザインする．内的セキュリティシステムの中核は自動管理システムであり，その実現のために管理者および運営方針の知識表現を定式化する．知識表現の定式化のために障害分析手法の一つである FTA (Fault Tree Analysys)[5] 用いて，これが持つ AND-OR tree で知識が表現される利点を活かして推論機構の構築を目指す．さらに汎用性のある自動管理システムを実現するために管理対象についての知識と運営方針に基づく知識とを分離するデザインにする．これにより計算機システムの柔軟な運用が可能になる．そして定式化の検証をネットワークの透過性の問題を通じて行う．

## 2. 内的セキュリティ問題

### 2.1 計算機リソース

計算機システムを利用する人間を利用者と呼ぶ．計算機の利用とは，計算機を操作し，リソースを消費することを指す．

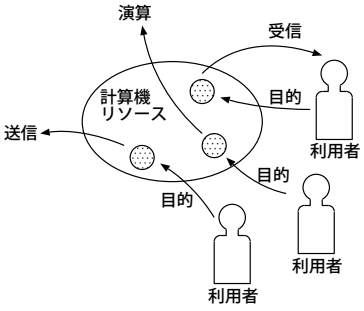


図 1　計算機システムの利用

ここで計算機リソースとは，CPU 時間やメモリ空間，外部記憶装置の容量，記録されている情報，ネットワーク帯域などを指す．ハードウエアが消費する電力やプリンタ用紙なども広義の計算機リソースである．計算機リソースは，利用者に与えられた目的に応じて形を変え，利用者の目的を達成する．与えられた目的によっては何も生み出すことなく無駄に消費される．

### 2.2 計算機システムの利用者権限

計算機システムのリソースには限りがあるため，利用者が無制限にリソースを消費できてはならない．また，計算機システムの運用上で必須のリソースが利用者によって消費されてしまうことがあってもならない．そのため利用者が利用できるリソースには制限が設けられている．利用者は，その制限の範囲内で割り当てられたリソースのみ利用できる．割り当てられたリソースを利用する権限を利用者権限と呼ぶ．

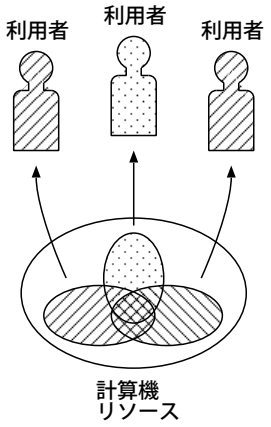


図 2　利用者権限

### 2.3 外的セキュリティ問題

計算機システムの安全な運用のためには，利用者権限を持たない外部の者によって計算機リソースが消費されてはならない．このような計算機システムの不正利用によって引き起こされる問題を本稿では外的セキュリティ問題と呼ぶ．

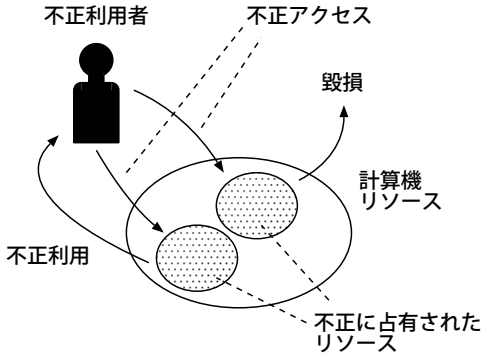


図 3　計算機システムの不正利用

計算機システムを不正利用しようとする者は，正規の利用者を装って利用者権限を得ようとする．もしくはシステムの脆弱性を利用することで利用者権限の奪取を試みる．これらの不正アクセスで利用者権限を得た不正利用者は，悪意のある目的でリソースを利用する．もしくは共有リソースを棄損する．

### 2.4 内的セキュリティ問題

利用者権限を持たない人間による悪意のある不正利用は，不正アクセスによる利用者権限の奪取を防ぐことで回避することができる．

しかし，正規の利用者が悪意のある目的で計算機リソースを利用することを防ぐことはできない．また，悪意はなくとも過失により計算機リソースを棄損してしまうことも防げない．これが内的セキュリティ問題である．

内的セキュリティ問題の原因は二つに分類できる．

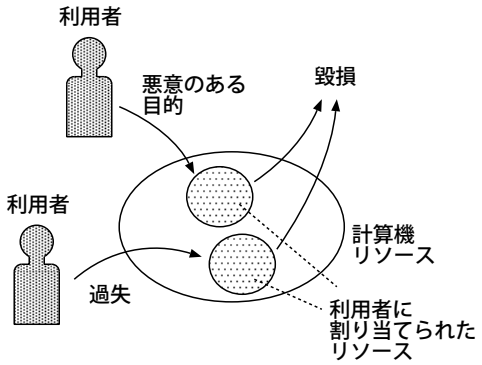


図 4　内的セキュリティ問題

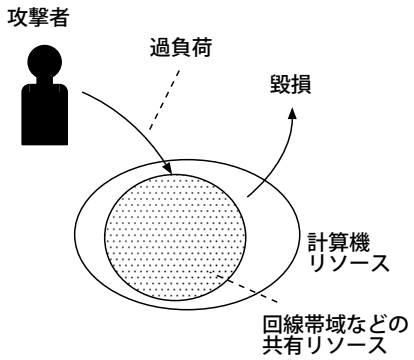


図 6　DoS 攻 撃

- 背信行為
- 過失

悪意のある目的を持って計算機リソースを消費することが背信行為である．利用者は確信的に利用者権限を悪用する．一方，悪意はなく，操作などの誤りによって計算機リソースを消費することが過失である．

### 2.5　管理者権限

管理者は計算機システムにおける最大の権限が与えられている．すなわち，一般の利用者に対しては設けられている制限がない．なぜなら，障害は計算機システムの全体において発生しうるため，管理者の業務の一つである障害分析および修正は制限された権限ではできないからである．

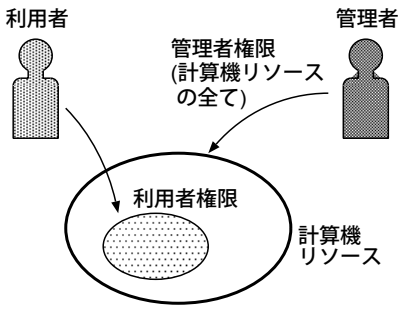


図 5　管理者権限

したがって，管理者による内的セキュリティ問題は利用者による者に比べて深刻である．

#### 2.5.1　補足： DoS 攻撃

内的セキュリティ問題の特殊な例として，Deny of Service (DoS) 攻撃が挙げられる．これは，計算機システムに過負荷をかけることでサービスを提供できない状態にしてしまうものである．

DoS 攻撃は外部の人間によるものであるから，不正アクセスと混同しがちである．しかし，これは外部にアクセスが許可された計算機リソースを毀損するものである．すなわち既に与えられている権限の範囲内で攻撃をするから，内的セキュリティ問題である．

しかし，狭義の内的セキュリティ問題としては，不特定多数の人間によるものではなく，内部の特定できる人間によるものを指すべきであろう．

## 3.　自動管理システム

前節で，管理者による内的セキュリティ問題は重大かつ深刻であることを述べた．内的セキュリティ問題は，計算機を人間が利用する以上不可避な問題である．したがって，この問題を根本的に解決するには，計算機の管理作業から人的要因を排除するのみ方法はない．本節ではそのために我々が提案した自動管理について述べる．

### 3.1　行為の 7 段階理論と自動管理システム

Norman の「行為の 7 段階理論」によると，人間の行為は図 7 に示す 7 つの段階を経て達成される [2], [3].

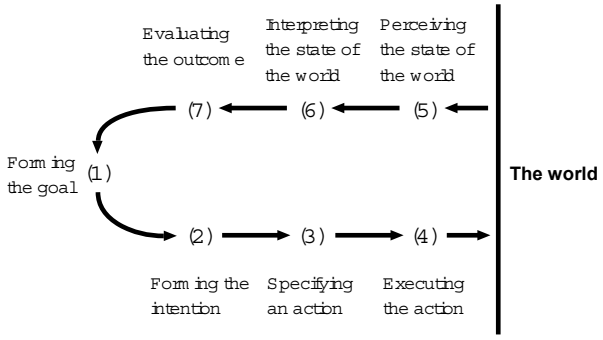


図 7　ノーマンの「行為の 7 段階理論」
Fig. 7　Norman's the seven stages of action model

管理作業では管理対象のシステムが外界にあたる．このいずれの段階でもヒューマンファクタによる揺らぎが生じうる．この揺らぎはゴールの形成の揺らぎとその他の段階の揺らぎとに分けられ，前者は背信行為，後者は過失の問題に相当する．

ゴールの形成の歪みには法整備や啓蒙，教育による対策が考えられる．またその他の段階の歪みにはフールプルーフ・フェイルセーフ機構や，行為系列の自動化によって対策されている．しかしいずれの対策もヒューマンファクタを完全に排除するものではなく，決定的な解決にはならない．したがって安全なシステム管理のためにはすべての段階の自動化によるヒューマンファクタの排除が必要になる．

行為の各段階は，図 8 に示すようにその役割から「認識」「判断」「応答」の 3 つに分けられる．自動管理システムは，それぞれを自動化する認識機構，判断機構，応答機構の三機構で構成される．管理の手続きは次の通りである．

（1） 認識機構は，管理対象の状態を観測し判断機構に通知する．

（2） 判断機構は，通知された状態と予め与えられた知識を基に行動を決定し応答機構に通知する．

（3） 応答機構は，通知された行動を実行する．

（4） 実行された行動により管理対象の状態が変化する．それをまた認識機構が観測し，判断機構に通知する．

以上の繰り返しで管理作業は行われる．

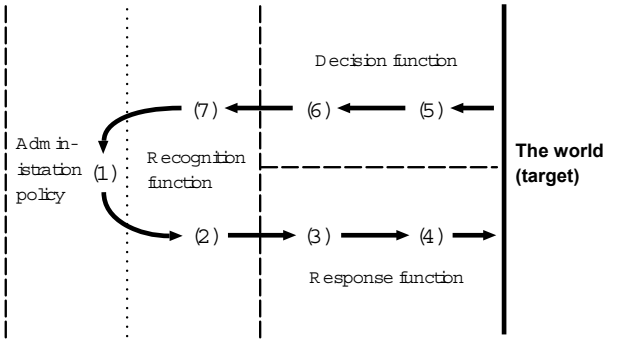


図 8 自動管理システムの概念モデル

Fig. 8 A conceptual model of Automatic Administration System

### 3.2 判 断 機 構

三機構のうち，判断機構がエキスパートシステムとしての役割を果たす．判断機構には**管理対象についての知識**と**運営方針についての知識**が予め与えられている．管理対象についての知識とは，認識機構によって観測しうる管理対象の状態と，応答機構によって実行しうる管理対象に対する行動とその効果についての知識である．運営方針についての知識とは，管理対象の状態の是非を定めたものである．これらを得るための手法の詳細は次節で述べる．

判断機構は，認識機構によって観測された状態の是非を，運営方針についての知識に基づいて判断し，修正すべきであれば管理対象についての知識に基づいて行動を決定する．

なお，知識を二つに分けるのは自動管理システムの汎用性のためである．エキスパートシステムの構築では知識獲得の自動化がもっとも困難であるため，知識を変更する機会は少ないほうが望ましい．知識が二つに分けられていれば，運営方針を改正したときは運営方針についての知識を置き換えるだけでよく，逆に管理対象のシステム構成を変更した場合は，管理対象についての知識を置き換えるだけでよい．これにより運営方針やシステム構成の変更への対応が容易になり，柔軟な運用ができる．

### 3.3 認識機構と応答機構

認識機構と応答機構は自動管理システムと管理対象とのインタフェースであり，これらが具体的にどのようなものになるかは自動化をどの程度まで実現するかに依る．ソフトウェア的な障害への対応を自動化するのは比較的容易であるが，物理的な障害まで対応しようとすると著しく困難になる．実用としては，物理的操作が必要になるときには管理者に通知する仕組みを応答機構に設けることで対処するほかない．

### 3.4 自動管理システムに伴う内的セキュリティ問題

自動管理システムによって自動化されていない作業を管理者が行うときの内的セキュリティ問題は避けられない．また，運営方針についての知識を設定するときも内的セキュリティ問題が生じる危険がある．

これらの解決手段として，周らによる管理者支援システム [4] を併用することが考えられる．これは複数の管理者が一定数以上同意しなければシステムを変更できないような枠組みを設けるものである．これを介した管理作業の手続きは煩雑になるので日常の管理作業を行うには実用性に欠ける．しかし自動管理システムと併用するならば必要なときのみこの枠組みのもとで作業を行えばよい．

## 4. 管理者の知識表現の定式化

本節では，管理者が判断機構に与える知識の知識表現について述べる．判断機構には，管理対象の状態とその原因となる事象全体 $\mathcal{X} = (X_1, \cdots, X_n)$ についての知識 $K = (K_r, K_o, K_a, K_d)$ を与える．それぞれは次のような知識を表す．

- 管理対象についての知識
  - $K_r$: 事象の因果関係についての知識
  - $K_o$: 観測可能な事象についての知識
  - $K_a$: 実行可能な行動についての知識
- 運営方針についての知識
  - $K_d$: 望ましい状態についての知識

事象の因果関係についての知識 $K_r$ は，$\mathcal{X}$ 上の論理関係を決める管理者の知識である．例えば，システム状態 $X_1$ に対して，その原因となる事象 $X_2$, $X_3$ の論理関係 $X_2 \cap X_3 \rightarrow X_1$ のように記述される．知識 $K_r$ の要素は，論理関係をもった木構造で管理者の知識を表現したものであるので，これを特に知識表現木 (Knowlegde Representation Tree: KRT) と呼ぶ．

次に，観測可能な事象についての知識 $K_o$ では，各観測結果に対して事象 $X$ の真偽を記述する．ある観測が一つ得られた場合，$K_o$ と $\mathcal{F}(K_r)$ の基づいて $\mathbf{X} = (X_1, \ldots, X_n)$ の値

$$\mathbf{X} \mid (K_o, K_r) = (x_1, \ldots, x_n)$$

が決定される．ここで $x_i$ は，$X_i$ の状態を示す値

$$x_i = \begin{cases} 1 & \text{事象 } X_i \text{ が真の場合} \\ 0 & \text{事象 } X_i \text{ が偽の場合} \\ \phi & \text{事象 } X_i \text{ の真偽が不明の場合} \end{cases} \quad (1)$$

を取るとする．また，不明状態を含む論理演算は，表 1 に従う．

表 1 不明状態 $\phi$ の演算

Table 1 The operations of unknown state $\phi$

| 式 | 値 |
|---|---|
| $\phi \cup 1$ | 1 |
| $\phi \cup 0$ | $\phi$ |
| $\phi \cap 1$ | $\phi$ |
| $\phi \cap 0$ | 0 |
| $\neg\phi$ | $\phi$ |

望ましい状態についての知識 $K_d$ は，運営方針に基づいて次のように決められる．管理者は $\mathcal{X}$ の部分集合 $\mathcal{X}' \subset \mathcal{X}$ に対し

て，$X \in \mathcal{X}'$ が取るべき $y_i$ を決める．この $y_i$ は (1) 式同様，

$$y_i = \begin{cases} 1 & \text{事象 } X_i \text{ が真となるべき場合} \\ 0 & \text{事象 } X_i \text{ が偽となるべき場合} \\ \phi & \text{事象 } X_i \text{ の真偽どちらでも良い場合} \end{cases} \quad (2)$$

を取るとする．ここで，$\phi$ の論理演算も表 1 に従う．したがって，$K_d$ は次のように定式化される．

$$K_d = \{(X, y) \mid X \in \mathcal{X}', y \in \{0, 1, \phi\}\}$$

最後に，事象の状態を変更する行動についての知識 $K_a$ は，$x_i \neq y_i$ なる (1) の $X_i$ の値を $x_i$ から $y_i$ へ変更する行動を集めたものであり，スクリプト命令などを想定している．ただし，$y_i$ は 0 か 1 である．

$$K_a = \{a \mid a(X_i) = y_i,\ y_i \in \{0, 1\}\}$$

以上の知識を元に，判断機構は以下のような手続きで行動を決定する．

（1） 認識機構から通知された観測結果と $(K_o, K_r)$ に基づいて $\boldsymbol{x} = \mathbf{X} \mid (K_o, K_r)$ を得る

（2） $\boldsymbol{x}$ と $K_d = \{(X, y)\}$ に基づいて望ましくない状態にある事象を列挙し，$U$ へ格納する．

$$U = \{i \mid x_i \neq y_i, y_i \neq \phi\}$$

（3） $U$ と $K_a$ に基づいて行動を列挙し，応答機構に通知する．

応答機構は，判断機構により通知された行動 $a \in K_a$ を実行する処理を行う．

## 5. 定式化の検証

検証事例として，ネットワークの透過性を調べるコマンドである ping を実行したときの結果を 4. 節の定式化に沿って分析する．対象とする事象は $X_1, \ldots, X_8$ の 8 つとして，それぞれ次のような意味を持つ．

- $X_1$: `ping OWN_IPADDR` が成功する
- $X_2$: ホストに IP ネットワーク機能がインストールされている
- $X_3$: ネットワークインタフェースカードが機能している
- $X_4$: IP アドレスが正しく設定されている
- $X_5$: `ping OWN_HOSTNAME` が成功する
- $X_6$: ホスト名が正しく解決される
- $X_7$: `/etc/hosts` に `OWN_HOSTNAME` についての記述がある
- $X_8$: DNS の設定が適切である

ここで，管理する計算機のホスト名を `OWN_HOSTNAME`, IP アドレスを `OWN_IPADDR` とする．この $\mathcal{X} = \{X_1, \ldots, X_8\}$ に関する管理者の知識を論理関係で表現し，$K_r$ を次のように作る．

$$K_r = \{\ X_1 \leftrightarrow X_2 \cap X_3 \cap X_4,\ X_5 \leftrightarrow X_1 \cap X_6, X_6 \leftrightarrow X_7 \cup X_8\ \} \quad (3)$$

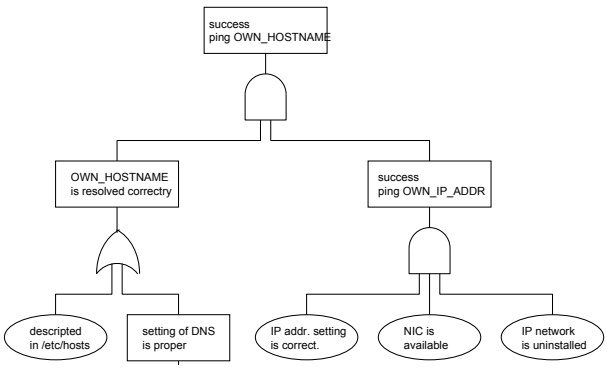


図 9 ネットワーク機能の一部の KRT

表 3 観測可能な事象についての知識 $K_o$
Table 3 Knowledge about observable events $K_r$

| command | message | value |
|---|---|---|
| `ping OWN_IPADDR` | `succeeded` | $X_1 = 1$ |
| | `no answer` | $X_1 = 0$ |
| `ping 127.0.0.1` | `succeeded` | $X_2 = 1$ |
| | `no answer` | $X_2 = 0$ |
| `ping OWN_HOSTNAME` | `succeeded` | $X_5 = 1$ |
| | `not resolved` | $X_6 = 0$ |
| | `no answer` | $(X_1 = 0) \cap (X_6 = 1)$ |
| `ping localhost` | `succeeded` | $(X_2 = 1) \cap (X_9 = 1)$ |
| | `not found` | $X_6 = 0$ |
| | `no answer` | $(X_2 = 0) \cap (X_9 = 1)$ |
| `grep OWN_HOSTNAME /etc/hosts` | `succeeded` | $X_7 = 1$ |
| | `not found` | $X_7 = 0$ |

図 9 に，表 2 にこれを一覧として示す．なお，(3) 式の論理関係は $X_1, \ldots, X_8$ の意味から自明である．例えば，$X_1$: `ping OWN_IPADDR` が成功することと，$X_3$: ネットワークインタフェースカードが機能し，$X_4$: IP アドレスが正しく設定され，$X_5$: `ping OWN_HOSTNAME` が成功することは，同値であることは明らかであるし，$X_5 \leftrightarrow X_1 \cap X_6$，$X_6 \leftrightarrow X_7 \cup X_8$ も同値であることは明らかである．

次に，観測可能な事象についての知識 $K_o$ は，表 3 のように観測結果とそれが示す状態の組として管理者から与えられる．

もし，観測結果「`ping OWN_HOSTNAME not resolved` 」が得られたとすれば，$X_6 = 0$ である．さらに，生起が不明な事象 $(X_1, \ldots, X_5, X_7)$ の値を (3) 式に基づいて推論すると，$X_i$ $(i = 1, 2, \ldots, 8)$ の値は

$$\mathbf{X} \mid (K_o, K_r) = (0, \phi, \phi, \phi, 0, 0, 0, 0, \phi) \quad (4)$$

となる．

一方，望ましい状態についての知識を $K_d = \{(X_5, 1)\}$ とすると，$K_r$ に基づく望ましい状態は

$$\mathbf{X} \mid (K_d, K_a) = (1, 1, 1, 1, 1, 1, \phi, \phi) \quad (5)$$

となる．したがって，望ましくない状態の集合 $U$ は，$U = \{1, 2, 3, 4, 5, 6\}$ となる．この $U$ を修正するための知識として，実行可能な行動についての知識 $K_a$ が，

表 2　事象の因果関係についての知識 $K_r$

Table 2　Knowledge about causal relation between events $K_r$

| event | name | child |
|---|---|---|
| $X_1$ | ping OWN_IPADDR is succeeded | $X_2 \cap X_3 \cap X_4$ |
| $X_2$ | IP network function is installed | – |
| $X_3$ | NIC is available | – |
| $X_4$ | setting of OWN_IPADDR is proper | – |
| $X_5$ | ping OWN_HOSTNAME is succeeded | $X_1 \cap X_6$ |
| $X_6$ | OWN_HOSTNAME is resolved properly | $X_7 \cup X_8$ |
| $X_7$ | OWN_HOSTNAME is descripted in /etc/hosts | – |
| $X_8$ | setting of DNS is proper | – |

$$K_a = \{a_1, a_2, a_3\},$$
$$a_1(X_2) = 1,\ a_2(X_4) = 1,\ a_3(X_7) = 1 \qquad (6)$$

と与えられているとする．修正のための $K_a$ の適用順番はいくつか考えられ，$U$ の辞書順や，あるいは，複数候補がある場合は親となる事象の数が少ないものを優先する，などの方法が考えられる．判断機構では $U$ と $K_a$ からどの行動 $a \in K_a$ を選択すればよいかを判断する．例えば，判断機構が $a_3$ を選択したとすると，それを応答機構に通知する．応答機構で処理され，改めて観測機構で観測が行われる．この観測の結果，「ping OWN_HOSTNAME no answer」が報告されたとする．このとき $\mathbf{X} \mid (K_o, K_r)$, $U$ は次のようになる．

$$\mathbf{X} \mid (K_o, K_a) = (0, \phi, \phi, \phi, 0, 1, 1, 0, \phi),$$
$$U = \{1, 2, 3, 4, 5\} \qquad (7)$$

しかし，$K_a$ からは $U$ の値を修正する行動は挙げられないので，値が $\phi$ である事象を観測する行動を $K_o$ から選択する．選択肢は

「ping 127.0.0.1」，「ping localhost」，
「grep OWN_HOSTNAME」

となり，それを実行することでそれぞれ観測結果が，

「succeeded」$(X_2 = 1)$,「succeeded」$(X_2 = 1)$,
「not found」$(X_7 = 0)$

となったとする．このとき，$\mathbf{X} \mid (K_o, K_r)$ の値および $U$ は，

$$\mathbf{X} \mid (K_o, K_r) = (0, 1, \phi, 0, 0, 1, 1, 0, 1),$$
$$U = \{1, 3, 4, 5\} \qquad (8)$$

となり，今度は判断機構により $a_2$ が選択される．選択された行動の結果 $a_2(X_4) = 1$ により，認識機構から ping OWN_IPADDR is succeeded が報告され，

$$\mathbf{X} \mid (K_o, K_r) = (1, 1, 1, 1, 1, 1, 0, 1),$$
$$U = \emptyset \qquad (9)$$

となり，運営方針 $K_d$ を満たすように改善される．

## 6. おわりに

本稿では，計算機システムに人間が介在することで生じる内的セキュリティ問題を指摘し，これに対処するための自動管理システムを定式化した．

自動管理システムは認識機構，判断機構，応答機構の三機構からなり，本論文ではこのうち判断機構の構築方法について詳細を述べた．判断機構はエキスパートシステムの一種で，事象の因果関係を記述する知識表現木 (KRT) に基づいて観測結果から不具合の原因を推論し，それに応じた行動を選択するものである．必要な知識を，管理対象についての知識と運営方針についての知識とに分けることで，管理対象のシステム構成や運営方針の変更などに対し柔軟な運用を可能とした．定式化の検証として，ネットワーク機能の一部についての知識を構築し，それに基づく動作の実例を示した．

利用者による過失や背信行為の問題は，不正アクセスなどの外的なものと異なり，法的アプローチや倫理的アプローチを採るほか解決策はないとされてきた．本論文で提案したような技術的アプローチも同時にとることで，この問題を内的セキュリティ問題として定義し，工学的な枠組みでの議論も必要である．

**謝　辞**

本稿で述べた内的セキュリティ問題の元となる考え方は日本大学理工学部数学科の小林英恒教授から頂いた示唆によるものである．ここに感謝の意を表したい．

**文　献**

[1] 森下壮一郎, 小林英恒, 三島健稔. FTA による内的セキュリティシステムのための知識表現. 信学技報 SITE2002-23(2002-10), pp. 29–32, 埼玉, 2002. IEICE.
[2] D. A. Norman. *The Psychology of Everyday Things*. Basic Books New York, 1988.
[3] D. A. ノーマン. 誰のためのデザイン？ 新曜社, 1990. 野島久雄 訳.
[4] 周展飛, 森下壮一郎, 三上洋, 三島健稔. 管理者支援システムに関する考察. 信学技報 FACE2001-16(2001-11), pp. 5–8, 東京, 2001. IEICE.
[5] 牧野鐵治, 野中保雄. 信頼性工学. 日科技連出版社, 1983.