コンピュータセキュリティ　18－3
(2002.　7.　18)

# 適応型セキュリティポリシー作成支援ツールの開発

諸橋 政幸† 藤山 達也† 永井 康彦†

†(株)日立製作所 システム開発研究所 〒212-8567 神奈川県川崎市幸区鹿島田890

E-mail: moro@sdl.hitachi.co.jp

**あらまし** インターネット利用によるセキュリティ上の脅威に対して，ファイアウォール設置等の個別対策だけではバランスの取れた対策でないため，対策に過不足が生じる可能性がある。そこで，情報資産を保護するための方針であるセキュリティポリシーを策定し，それに基づいた体系的な対策を実施することが必要となってきている。このセキュリティポリシーの作成には多くの作業工数と高度な専門知識が必要なことから，ポリシー作成作業を支援するツールが求められている。しかし，従来の一般的支援ツールでは特定のリスク分析手法や参照基準／事例を利用しており，ニーズ／対象に応じてリスク分析手法や参照基準／事例を選択・利用することができない。そこで，本稿では，ニーズ／対象に応じて多様なリスク分析手法や参照基準／事例を選択・利用できるツールの実現方式と開発結果について報告する。

**キーワード** セキュリティポリシー，セキュリティポリシー作成支援ツール，リスク分析手法，セキュリティ基準

# Development of a Flexible Support Tool for Production of Security Policies

Masayuki Morohashi† Tatsuya Fujiyama† Yasuhiko Nagai†

†Systems Development Laboratory, Hitachi, Ltd.

890, Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa-ken, 212-8567 Japan

E-mail: moro@sdl.hitachi.co.jp

**Abstract** To counter the increasing threats in proportion to popularization of the Internet, conventional countermeasures, such as setting firewall, have been enforced. But in the case that conventional countermeasures are merely enforced, there is possibility of arising excess or lack of countermeasures toward threats. Recently, to solve such problem, it is needed to make security policies that are policy to protect the assets and then enforce countermeasures based on the security policies. But it is needed long term and high expertise to make security policies. Accordingly support tool for production of security policies is requested. Conventional tools can support to make security policies by using specific risk analysis methodology and specific standards. But conventional tools cannot support to make security policies by using appropriate risk analysis methodology and appropriate standards selected according to the needs and the object. Then, in this paper, we report the realization method and development result of the tool that can support to make security policies by using appropriate risk analysis methodology and appropriate standards selected according to the needs and the object.

**Keyword** Security Policy, Support Tool for Production of Security Policy, Risk Analysis Methodology, Security Standard

## 1. はじめに

インターネット利用などにより，企業や組織へのセキュリティ上の脅威が増大しており，顧客データなどの情報資産を保護するため，脅威に対する十分な対策を実施することが重要になってきている。これに対し，一般の組織や企業では，ファイアウォール導入などの個別対策を行なっているところが多い。しかし，これでは，バランスの取れた対策でないため，対策に過不足が生じる可能性がある。そこで，情報資産を保護するための方針であるセキュリティポリシーを策定し，これに基づいた体系的な対策を実施す

ることが必要となってきている。

しかし，このセキュリティポリシーの作成では，情報資産に対する脅威の洗い出しやリスク評価などの分析を必要とするため，多くの作業工数と高度な専門知識が必要である。そこで，この作業を支援する方法およびツールが求められている。

このような要求に対し，既にいくつかの支援ツールが存在する。これらの支援ツールは，特定のリスク分析手法や参照基準／事例を利用してポリシーを作成するものが一般的である。しかし，これでは，ニーズ／対象に応じてリスク分析手法や参照基準／事例を選択・利用することができない。

このような背景のもと，報告者らは，ニーズ／対象に応じて多様なリスク分析手法や参照基準／事例を選択・利用できることを特徴とする適応型セキュリティポリシー作成支援ツールを開発した。本稿では，開発する際に検討したセキュリティポリシー作成支援ツールの実現方式と，その実現方式を適用したツールの開発結果について報告する。

## 2. 従来のセキュリティポリシー作成支援ツールの概要と課題

代表的なポリシー策定ガイドに記載されているように，一般的に，ポリシー作成は以下のような手順に従って行なわれる。

(1) ステップ１：情報資産の定義
　対象範囲内に存在する情報資産を定義する。

(2) ステップ２：脅威の洗い出し
　ステップ１で定義した情報資産について，想定される脅威をすべて洗い出す。

(3) ステップ３：リスク評価
　ステップ２で洗い出した脅威毎に，脅威の発生可能性と脅威発生時の損失の大きさを評価し，リスクの大きさを評価する。

(4) ステップ４：ポリシーの立案
　ステップ３の評価結果を考慮して，各脅威に対抗するためのポリシーを立案する。

上記の各作業で多くの作業工数を要するため，ポリシー作成支援ツールでは，これらの各ステップを支援する機能を備えるものが一般的である（図 2-1）。

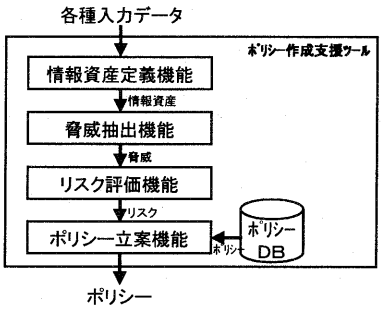


図 2-1：一般的ポリシー作成支援ツールの機能構成

例えば，以下のような支援ツール[1][2]が存在する。

・ BS7799 認証取得支援を目的としたツール
　- BS7799[3][4]に記載のリスク分析手法に準拠，および，BS7799 に記載の施策を利用したポリシー作成を支援する。
・ 複数の基準への準拠を特徴としたツール
　- BS7799 に記載のリスク分析手法に準拠，および，複数の基準を選択・利用したポリシー作成を支援する（ただし，利用可能な基準は固定）。

上記のように，従来の一般的ポリシー作成支援ツールでは，特定のリスク分析手法に準拠してリスク分析を実施し，特定の基準や事例 DB を利用してポリシー作成を支援するという特徴を持つ。

しかし，このような従来の一般的支援ツールでは，以下のような問題がある。

・ リスク分析手法には，GMITS[5]，BS7799，官公推奨のガイド[6]，FISC 推奨のガイド[7]，に記載された手法などが存在する。これらの手法は各々が特徴を持つため，現状では，ニーズ／対象に応じて適した手法を選択・利用するのが現実解となっている。しかし，従来ツールでは準拠可能な手法が固定であるため，特定のニーズ／対象にしか対応できない。
・ ポリシー作成では，特定の基準に準拠したい，過去の事例を利用したい，などの要望があることから，ニーズ／対象に柔軟に対応することが必要である。しかし，従来ツールでは利用可能な基準／事例が固定であるため，特定のニーズ／対象にしか対応できない。

そこで，上記の問題を解決する方法として，ニーズ／対象に応じて多様なリスク分析手法や参照基準／事例を選択・利用できることを特徴とする適応型セキュリティポリ

シー作成支援ツールが有効と考え，本ツールの開発を行なうこととした。

## 3. 適応型ポリシー作成支援ツールの実現方式

本章では，2章の課題を解決するために開発した機能の開発方針および実現方式について述べる。

### 3.1 リスク分析機能の実現方式

#### 3.1.1 開発方針

リスク分析手法は大別して，リスクを算出せずに基本的なポリシーを立案する基本アプローチ，対象毎に分析してリスクを算出する詳細アプローチ，これら2つを組合せた融合アプローチがある。これらの中で詳細アプローチは，数値やオーダーに基づいたグレード値を入力とする定量的手法と，ランク値を入力とする定性的手法に分けられる。さらに，具体的な手法はポリシー策定ガイド毎に異なるものが提案されており，多様なリスク分析手法が存在する。

これらの手法は，ポリシー作成に投入可能なコストや時間，対象の規模，対象の分野，準拠したいガイドの指定，などに応じて選択・利用する必要がある。このような多様なニーズ／対象に応じてリスク分析手法を選択・利用可能とするためには，代表的な手法をすべて網羅することが必要である。そこで，個別のリスク分析手法をすべてサポートすることを1つめの要件とした。

また，すべての手法をサポートしても，多様な手法からどれを選んだら良いか分からないという問題や，複数のガイド記載の手法を両方満足したい場合がある。これに対し，国際基準であるGMITSやBS7799においても詳細アプローチによる定性的手法であれば十分（BS7799の認証取得のためにも）と言われていることや，一般に情報セキュリティに関する脅威の発生確率等の定量データは入手困難なことから，国内外の代表的なポリシー策定ガイド等に記載された定性的手法をすべて満足する手法が有効と考え，これをサポートすることを2つめの要件とした。

#### 3.1.2 実現方式

1つめの要件は個別の手法を実装するだけで実現できるので，本節では2つめの要件を満たす実現方式の検討内容および結果を示す。

各ポリシー策定ガイド等（GMITS，BS7799，FISC推奨のガイド，官公推奨のガイド）に記載の定性的手法では，発生可能性と損失の大きさの評価項目を評価者の主観からランク付けし，発生可能性と損失の大きさのランク値を掛け算してリスクを算出する点は共通している。しかし，各ポリシー策定ガイド毎に発生可能性と損失の大きさの評価項目が異なっており，評価する視点の異なる評価方法となっている。そこで，各手法の不足部分を明確にするため，表3-1に示すように，各手法の評価項目の比較を行なった。

表 3-1：各ポリシー策定ガイドの評価項目

| | 発生可能性の評価項目 | 損失の大きさの評価項目 |
|---|---|---|
| GMITS | 脅威の程度（発生頻度）<br>- 偶然：地理的条件、自然災害<br>- 故意：攻撃の動機、攻撃者の能力、使用できるリソース、資産の価値に対する認識、資産の脆弱性に対する認識<br>脆弱性の程度<br>- 評価する要因：物理的条件、管理、人、組織、ハード、ソフト、通信機器 | 資産価値<br>- 機密性侵害時の影響<br>- 完全性侵害時の影響<br>- 可用性侵害時の影響<br>- 資産の再作成に要する費用 |
| BS7799 | 発生可能性<br>- 脅威<br>- 脆弱性<br>- 既に実施している対策 | 脅威発生時の影響<br>- 機密性侵害時の影響<br>- 完全性侵害時の影響<br>- 可用性侵害時の影響 |
| 金融機関等におけるセキュリティポリシー策定のための手引書（FISC推奨のガイド） | 脆弱性の大きさ<br>- 機能的弱点の有無<br>- 物理的弱点の有無<br>- 対策の実施状況<br>- 運用規則の遵守状況 | 資産の重要性<br>(i) 情報資産が情報の場合<br>- 機密性侵害により大きな影響のある情報<br>- 厳格な取扱いを行う情報<br>- 社内外に公開している情報<br>(ii) 情報資産がシステムの場合<br>- 資金移動を伴う業務を扱うシステム<br>- 顧客に関する業務を扱うシステム<br>- 社内向け業務を扱うシステム |
| 情報セキュリティポリシーに関するガイドライン（官公推奨のガイド） | 脅威の発生頻度 | 資産の重要性<br>- 機密性侵害時の影響<br>- 完全性侵害時の影響<br>- 可用性侵害時の影響 |

その結果，GMITSの評価項目の構成は他の手法を含んでいることが判明したため，GMITSの評価項目をベースとし，GMITSに不足する他の手法の評価項目を追加することで，以下に示す評価項目を作成した。

(1) 定性的手法で用いる評価項目（表3-2）

脅威の発生可能性と損失の大きさに関する評価項目を以下に示す。

(a) 脅威の発生可能性

発生可能性は，脅威が発生する頻度と，脅威が発生したときの被害の受け易さを表す尺度である。そこで，以下の分類に分けて評価する。

(a-1) 脅威の発生頻度

脅威は攻撃の種類から偶然と故意に大別できるため，偶発的脅威と故意的脅威の発生頻度に分けて詳細項目に分類した。

(a-2) 脆弱性の程度

脆弱性の程度とは脅威に対する保護対策の不十分さの程度のことである。そこで，現状の対策実施状況から評価することとし，対策の分類毎に詳細項目に分

類した。

(b) 損失の大きさ

セキュリティの目的は情報資産の機密性･完全性･可用性を確保することである。そこで，損失の大きさをこれらの侵害による影響の大きさと考え，以下の分類に分けて評価する。

(b-1) 機密性の侵害による被害の大きさ

ランク付けする視点を提供するため，被害の種類の視点から詳細項目に分類した。

(b-2) 完全性の侵害による被害の大きさ

(b-3) 可用性の侵害による被害の大きさ

共に(b-1)と同様である。

表 3-2：定性的手法で用いる評価項目

| 大項目 | 中項目 | 小項目 | 詳細項目 |
|---|---|---|---|
| 発生可能性 | 脅威の発生頻度 | 偶発的脅威の発生頻度 | 自然災害による脅威の発生頻度 |
| | | | … |
| | | 故意的脅威の発生頻度 | 攻撃の動機 |
| | | | … |
| | 脆弱性の程度 | 物理的セキュリティ | 設備･建物に対する対策の実施状況 |
| | | | … |
| | | 論理的セキュリティ | ソフトウェアに対する対策の実施状況 |
| | | | … |
| | | 管理･運用セキュリティ | 組織に対する対策の実施状況 |
| | | | … |
| 損失の大きさ | 機密性の侵害による被害の大きさ | 直接的損失 | 被害を受けた資産自体の損失による影響 |
| | | | … |
| | | 間接的損失 | 経営や業務への影響 |
| | | | … |
| | | 事後対応の損失 | 再発防止に必要な費用 |
| | | | … |
| | 完全性の侵害による被害の大きさ | 直接的損失 | 被害を受けた資産自体の損失による影響 |
| | | | … |
| | | 間接的損失 | 経営や業務への影響 |
| | | | … |
| | | 事後対応の損失 | 再発防止に必要な費用 |
| | | | … |
| | 可用性の侵害による被害の大きさ | 直接的損失 | 被害を受けた資産自体の損失による影響 |
| | | | … |
| | | 間接的損失 | 経営や業務への影響 |
| | | | … |
| | | 事後対応の損失 | 再発防止に必要な費用 |
| | | | … |

(2) 各定性的手法への対応方法

(1)の評価項目を全体利用することで，全ての定性的手法に準拠できる。なお，評価項目間の関係から，詳細項目毎に付けたランクを平均および掛け算することでリスクを算出する。

また，評価項目を全体利用･部分利用することで，同じ方法で以下のように個別手法にも対応できる。

- GMITS/BS7799 の定性的手法：全体利用
- FISC 推奨の定性的手法：(a-2)(b)のみ利用
- 官公推奨の定性的手法：(a-1)(b)のみ利用

## 3.2 参照基準／事例 DB の実現方式

### 3.2.1 開発方針

ポリシー作成機能は，基本的に，基準や事例を DB 化しておき，ユーザが選択した基準や事例をマージすることでポリシー作成作業を効率化するものである。本機能において多様なニーズ／対象に応じて基準や事例を利用可能とするためには，既存の基準や事例だけでなく，今後作成される基準や事例も利用可能とすることが必要である。そこで，今後作成される基準や事例の追加に簡単に対応するため，ツールの機能変更なしで基準や事例を追加･削除できることを 1 つめの要件とした。

また，ユーザの使い勝手を良くするためには，追加した基準や事例をユーザが複雑な操作をしなくても利用できることを 2 つめの要件とした。

### 3.2.2 実現方式

まず 1 つめの要件は，基準や事例を共通の DB スキーマに手作業で入力し，その DB スキーマに対応したポリシー作成機能を開発することで満たすことができる。しかし，現状の基準や事例はポリシーの分類が異なる。そこで，統一した分類にするための DB スキーマを開発することとした。

また，2 つめの要件は，ユーザが簡単な操作でツールに DB を登録する方式，および，登録した DB をツールが自動的に識別する方式を開発することで満たすことができる。そこで，DB 登録･識別方式を開発することとした。

以下に，各々の検討結果を示す。

(1) 統一 DB スキーマ

統一 DB スキーマを開発するためには，各基準毎に表形式で格納される対策群の横軸と縦軸の分類を決める必要がある。ポリシー策定において，セキュリティ基準の参照とは，策定するポリシーの適用範囲（情報システム，組織，利用者）と，策定するポリシーのサポート内容･種別（物理，論理，管理･運用）により，該当する対策を選択することで行なわれる。そこで，以下のような横軸･縦軸となることを要件とした分類方法を検討し，表 3-3に示す統一 DB スキーマを作成した。

(a) 横軸の分類：ポリシーの策定範囲の分類

ポリシーは情報システム／管理／利用者の側面で構成されるため，これらの側面からポリシーの策定範囲を選択できることが必要である。そこで，これらの側面から「技術」「組織」「利用者」に分類した。また，各々を適用範囲の視点からさらに分類した。

(b) 縦軸の分類：ポリシーの種別の分類

ポリシーは一般に物理／論理／管理･管理という種別

の視点で分類されるため，策定されたポリシーはこの分類に従って出力されることが適当である。そこで，この視点から「物理セキュリティ」「論理セキュリティ」「管理･運用セキュリティ」と分類した。また，各々を種別の視点からさらに分類した。

表 3-3：統一 DB スキーマ

| 大分類 | 中分類 | ポリシー | 技術 | | | 組織 | | | | 利用者 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 情報システム | 管理運用 | 設置 | 一般 | サービス事業者 | ハードウェア供給事業者 | ソフトウェア供給事業者 | システムユーザ | システム管理者 |
| 物理セキュリティ | 建物の物理セキュリティ | | | | | | | | | | |
| | 部屋の物理セキュリティ | | | | | | | | | | |
| | 付帯設備の物理セキュリティ | | | | | | | | | | |
| | 情報システムの物理セキュリティ | | | | | | | | | | |
| 論理セキュリティ | アクセス権の設定・管理 | | | | | | | | | | |
| | 識別と認証 | | | | | | | | | | |
| | アクセス制御 | | | | | | | | | | |
| | ファイル・伝送データの暗号化 | | | | | | | | | | |
| | セキュリティ監視 | | | | | | | | | | |
| | セキュリティ機構の保護 | | | | | | | | | | |
| | セキュリティ監査 | | | | | | | | | | |
| 管理・運用セキュリティ | 組織・体制 | | | | | | | | | | |
| | 入退室管理 | | | | | | | | | | |
| | 要員管理 | | | | | | | | | | |
| | 運用管理 | | | | | | | | | | |
| | システム切替・変更 | | | | | | | | | | |
| | 各種設備の管理 | | | | | | | | | | |
| | 教育・訓練・啓蒙 | | | | | | | | | | |
| | 情報収集 | | | | | | | | | | |
| | 外部委託管理 | | | | | | | | | | |
| | システム監査 | | | | | | | | | | |
| | 不正・異常・障害の検出と回復 | | | | | | | | | | |

(2) DB 登録･識別方式

各基準や事例を統一 DB スキーマに入力し，各々を 1 枚のシートにする。さらに，ユーザがシートの挿入／削除を指定するだけで，それを可能にする機能を用意する。これにより，シートに入力した基準や事例を簡単にツールに登録できる。

また，登録するシートの名称を，組織共通ポリシー（組織全体に共通するポリシー）と部門特定ポリシー（組織内の特定の部門やシステムを対象とするポリシー）を区別する「ポリシー種別」と，基準や事例の名称を示す「基準･事例名」で構成する。さらに，登録したシートの名称から，登録した基準や事例のポリシー種別と名称を判別する機能を用意する。これにより，登録したシートをツールが自動的に識別できる。

本方式により，基準や事例をツールに容易に追加可能となるため，多様な基準／事例を DB に登録することで多様なニーズに対応可能となる。

## 4. ツールの開発結果

本章では，3章で示した実現方式を適用した (1)適応型リスク分析機能と，(2)基準／事例のカセッタブル･ローディング機能，を持つツールの開発結果について述べる。なお，本ツールの機能構成を図 4-1に示す。

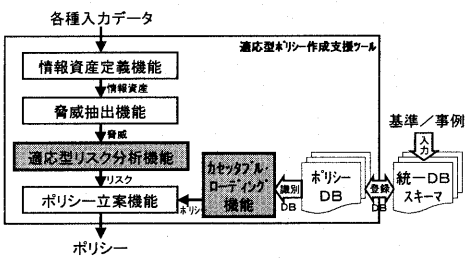


図 4-1：適応型ポリシー作成支援ツールの機能構成

### 4.1 適応型リスク分析機能

本機能は，ニーズ／対象に応じて選択したリスク分析手法に従ってリスク分析を実施することを特徴とする機能である。以下に，本機能の動作概要を説明する。

リスク分析手法の選択では，まず，基本／詳細／融合アプローチから利用するものを選択させる。詳細アプローチ選択時は，さらに 5 つの手法から選択させる（図 4-2）。このように多様なリスク分析手法から利用する手法を選択できる。

リスク分析手法選択後は，選択された手法に応じて必要なデータを入力させる。例えば，ガイド記載の全ての定性的手法を満足できる統合型のリスク分析手法が選択された場合は，脅威毎に各評価項目のランク値を入力させる（図 4-3）。最後に，入力データから各脅威のリスクを算出する。

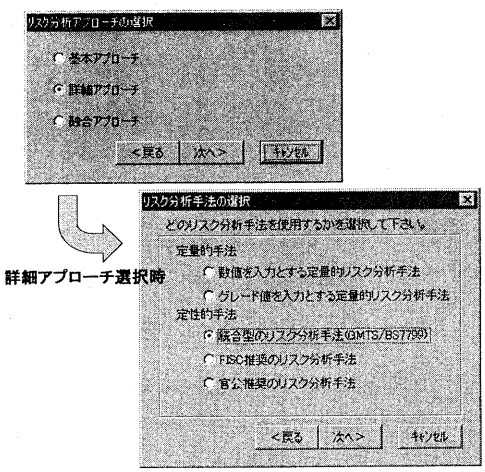


図 4-2：リスク分析手法の選択画面

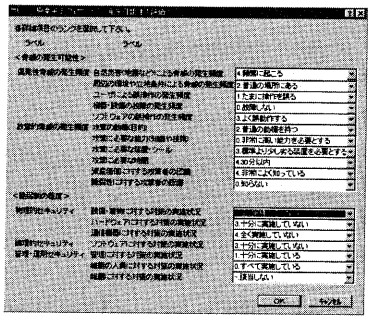

図 4-3：定性的手法選択時のランク値入力画面

## 4.2 カセッタブル･ローディング機能

本機能は，参照基準／事例 DB を容易に追加･削除および利用できることを特徴とする機能である。以下に，本機能の動作概要を説明する。

利用可能な基準として 2 つのシートが登録されていた場合，その 2 つを DB 選択画面に表示する（図 4-4の左上）。ここで，図 4-5に示すようにユーザが安全対策基準のシートを挿入するだけで，そのシートをツールが自動的に識別し，ポリシー作成で安全対策基準を選択･利用可能となる（図 4-4の右下）。

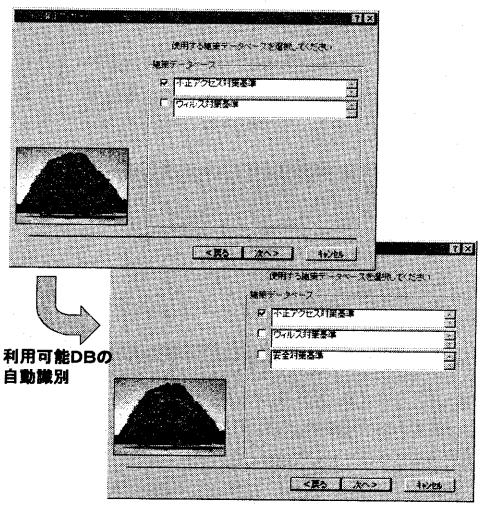


図 4-4：参照基準／事例 DB の選択画面

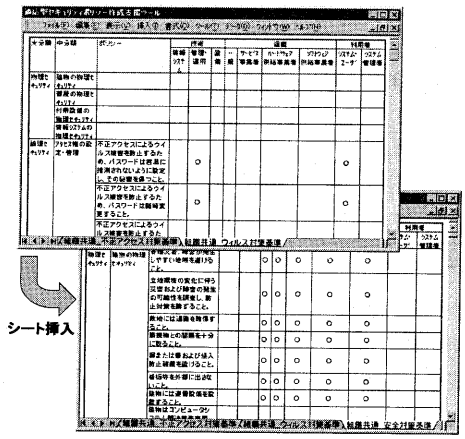


図 4-5：基準を格納したシートの挿入

## 5. まとめと今後の課題

本稿では，適応型ポリシー作成支援ツールの実現方式と，その方式を適用したツールの開発結果について報告した。

本方式は，ニーズ／対象に応じて，多様なリスク分析手法や参照基準／事例を利用できることを特徴としており，これにより，多様なユーザの要望に対応することを可能とした。

今後，本ツールを事例適用することにより，有効性の検証と改良を行なっていく予定である。

### 参考文献

[1] RA Software tool, http://www.aexis.de/RA%20ToolPage.htm

[2] M@gicPolicy, http://www.asgent.co.jp/

[3] BSI : BS7799 part1:Code of practice for information security management, 1999

[4] BSI : BS7799 part2:Specification for information security management systems, 1999

[5] ISO/IEC JTC1/SC27/WG1 : Information technology - Guidelines for the management of IT Security - Part3: Techniques for the management of IT Security, ISO/IEC TR13335-3, 1998.6.15

[6] FISC : 金融機関等におけるセキュリティポリシー策定のための手引書, 1999.1.29

[7] 情報セキュリティ対策推進会議 : 情報セキュリティポリシーに関するガイドライン, 2000.7.1