セキュリティポリシ構築におけるデータベース支援に関する考察
A Study of Database Support for enacting the Security Policy

佐野　雅彦　　松浦　健二　　上田　哲史　　大恵　俊一郎

Masahiko Sano　Kenji Matsuura　Tetsuhi Ueta　and Shunichiro Oe

徳島大学　高度情報化基盤センター

Center for Advanced Information Technology, Tokushima University

〒770-8506　徳島市南常三島町 2-1

2-1 Minami jyosanjima, Tokushima, 770-8506 Japan

{sano, matsuura, tetsuhi, oe}@ait.tokushima-u.ac.jp

概要

個人情報漏洩やウイルス感染など，今日の情報社会を脅かす様々な脅威が存在している．このような脅威に対抗するための方策として，セキュリティポリシを策定する組織は増加している．徳島大学においても，平成 15 年よりセキュリティポリシ策定の活動を開始しているが，セキュリティポリシを策定する際の人的コスト（リスク分析，資産洗い出し，リスク評価）削減の方策として，資産登録及びリスク評価データベースを構築し，運用した結果，短期間で リスク分析を行うことができた．本論文では，本学のセキュリティポリシ構築及び運用におけるデータベース支援について，支援システムを構築した結果も含めて考察する．

キーワード　セキュリティポリシ，構築支援，データベース

Abstract

Various and many incidents, which like infections by the computer virus and leakage of personal information, threat our information society nowadays. The number of organization enacting the security policy for protecting themselves from those threats is rising. At the security policy planning, high cost and manpower are required for investigating their property and assessing their risk. Therefore, we have developed the security policy support database system to decreasing the cost of manpower. In this paper, we describe the requirements to construct a support database system and the results of out construction and operation.

Keywords　Security Policy, Construction support, Database

１. はじめに

近年、様々な情報セキュリティに関する事故（インシデント）の発生が頻発しており，とくに，個人情報漏洩に関する事故が社会的に問題視されている．このため，セキュリティポリシ（以下ポリシ）に対する社会の認識とポリシ整備の必要性も高まっており，経済産業省や文部科学省，情報処理推進機構，情報セキュリティ対策推進会議，学会等において啓蒙活動が活発に行われた結果[1][2][3]，ポリシを定める組織は増加の一途である．しかしながら，ポリシを制定してもポリシの不備や運用上の不備により，結果としてセキュリティ事故に至る例も少なくない．そこで，ポリシの策定と技術的な対策に加え，人的・物理的セキュリティを重視した総合的な対策という観点から ISMS（Information Security Management System）[4]に準拠したポリシの策定または ISMS 認定を取得する動きが拡大している．徳島大学（本学）でも，法人化後の教員の個性ある研究結果などの知的財産，所属教職員と学生の個人情報等について情報セキュリティの確保するため，ISMS に準拠したポリシの策定を行っている[5].

ISMS に準拠したポリシ策定における最初の課題は，既存の資産の洗い出しとリスクの評価・分析であり，組織規模が大規模であるほど，多大な人的労力を必要とする．加えて，大学等教育研究機関では教育と研究及び組織運営の異なる目的の活動が行われているため，リスクの評価基準や評価項目において合意を得ることが難しいこともあり，資産洗い出し等の一連の作業への協力を得られにくいという実情がある．本学では ISMS 認定機関のコンサルティングを受けて客観性のある基準や項目を選定することにより，学内の合意を得るものとし，資産洗い出

し，リスク評価，資産目録のデータベースを開発して，ポリシ構築の支援を行うものとした．

本稿では，本学のセキュリティポリシ構築過程において，ポリシ構築支援にデータベースを活用したその手法と運用結果及び今後のポリシ運用のための考察について述べる．

2.本学のセキュリティポリシ策定状況

2.1 策定状況

徳島大学（以下本学）では，平成 14 年に公開された「大学における情報セキュリティポリシの考え方」[2]を参考に，高度情報化基盤センター内で準備作業を開始した．平成 15 年 12 月には，準備作業段階で作成した素案を基に，より客観性と具体性を伴ったポリシ策定を目標として，ISMS 認定機関[1]によるコンサルティングを受けている．図１は本学で導入したポリシ策定手順を示すものである．フェーズ I，II は平成 16 年 3 月に終了しており，ポリシを構成する基本文書のうち，基本方針，対策基準は策定終了[2]している．なお，現在はフェーズ III の段階にあり実施手順の策定を行っている．なお，策定の背景・状況は[5]に詳しく述べられている．

2.2 策定上の課題と本学の対応

ポリシ策定における最初の課題である資産洗い出しは，既存の資産管理が整備されていれば，比較的低い負荷で実施できると考えられる．しかし本学の場合，他大学と同様に事務定員削減に伴う業務効率化等が実施されおり，その結果，物品管理業務が簡素化された経緯がある．このため，リスクアセスメントのために必要な情報が物品管理簿等から得られず，資産洗い出しを再実施する必要があった．なお，本来であれば全てを調査範囲とするべきであったが，スケジュール上の制約[3]のため，調査範囲を表１に示すものに限定し，調査範囲外の資産に関するリスク評価はベースラインアプローチ[4]を採用した．このため，ポリシ運用サイクルにおいて，ベースラインアプローチを適用した資産を別途洗い出す必要がある．

表１　資産洗い出し調査範囲

調査項目	概要
重要度の高い情報	重要度２以上の情報[5]
サーバ機器	サーバ機能を有する機器
ネットワーク機器	基幹，支線ネットワーク機器
クライアント機器	調査範囲外とする

1 STNet 社による．
2 各種委員会での承認待ち段階である．
3 予算執行期限の関係で３ヶ月間以内にポリシ基本文書策定とリスクアセスメントを行わなければならなかった．
4 調査を簡略化又は省略してリスク分析を行う手法．
5 本学のポリシでは情報の重要度を３段階に分類する．

3.支援データベースの必要性

3.1 ISMS における要求要件

ISMS に即したセキュリティ対策実施手順[4]では，ポリシ策定段階においてリスクの調査・分析を実施（リスクアセスメント）することで適用範囲となる組織の現状を把握し，ポリシ運用サイクルにおいて対象となる情報資産，ポリシ運用記録を管理することが重要であるとされている． ISMS ではこれらの情報管理の管理手法は規定されておらず運用組織側で規定する．また，情報の操作（登録，削除，更新）及び各種の報告・記録についても必要な場合は履歴等の追跡が出来なければならないとされている．

3.2 リスク分析における DB の必要性

ポリシの対象範囲に依存するが，対象とする資産には，情報資産（データベースやファイル，個人情報，部外秘情報，資料，設定情報等）や物理的資産（パソコンやサーバ等の情報機器，記録媒体，空調・電気設備，什器，および収容設備等），ソフトウエア資産，サービス等を含むのが一般的である．情報機器や什器類の目録管理は既に何らかの方法で実施されていることが多いが，情報資産の管理は，体系的に管理するための様々な副次的情報（情報の管理者，複製，情報の存在期間，破棄，メディアの管理等）を管理する必要性があることから，実施が難しく，本学の場合，実現されていなかった[6]．

物理的資産だけでなく情報資産も DB で管理することにより，情報資産と物理的資産の関連（主たる保管場所等），情報伝達（複製や送受信等）の流れ，不明な業務プロセス等が明らかになり，潜在的なリスクの発見が期待できる． また，資産に対して重要度，管理状況によるリスク度，リスク係数（頻度）をパラメタとするリスク算定式[7]，を設定することにより，各資産のリスク値の算出や集約が簡単となる．但し，対象とする資産を出来るだけ詳細に洗い出して資産目録を作成する必要がある．

3.3運用サイクルにおける必要性

ポリシ運用サイクルでは，目録の内容は時間と共に変化するため，関連する資産や情報の流れも変化する．このような項目間の関係を管理するには DB を適用することが望ましい．さらに，リスクアセスメント段階において資産目録が DB で管理されていれば，その情報を効果的に再利用できる．DB の活用により，資産目録管理，リスク値算出，目録情報

6 紙媒体の文書に関しては既に文書管理規定がある
7 リスク算定式には各種の方法が考えられるが本学では上記パラメタの積をリスク値として採用している．

の変更や一覧の取得が容易に行えるので，ポリシ運用において各種手続きや確認の省力化等が期待できる．また，事故が発生したときの対応や，防止・是正措置において，効果が期待できる．

3.4 データベース

これまでの述べたことを踏まえて，以下では，DB で管理すべき項目について述べる．なお，４章以降で紹介する本学の経験も反映している．

（1）情報の管理

情報を管理対象とする場合，複製，保存，伝達，破棄に関する手順を定めることが推奨[4][6][7]されており，これらを考慮すると，少なくとも表 2 に示す取り扱い項目が必要である．これらの項目には，当該情報資産の存在とその情報資産の管理者に加えて，伝達先（複製や再利用，電子的な連携を含む）とその手段を含めている．これは，業務プロセスにおける潜在的リスクの発見と，部局間を越えた横断的な情報資産の再利用を管理するために有効である．重要性は，機密性及び完全性に重点を置いている．また，外部提供の項目は，組織外（例えば大学外）に提供される場合の方法と許可者を明確にするためのものである．

（2）機器の管理

物理的資産である情報機器は何らかの方法で目録管理されている場合が殆どである．本学では，管理番号，機器名，管理者，設置場所，日付，金額等が，主要な管理項目であるが，セキュリティマネジメントの観点では更に多くの管理項目が必要である．表３に機器の管理に必要な項目を示す．ここで示す重要度は，主として可用性，完全性に関しての重要度であり，機器が正常に動作することに重点を置いている．機器特性の項は，後述の環境の管理において，電力容量や，耐震措置などの管理策に影響する．当該機器がクライアント機器等である場合も同様に扱うことができる．

（3）環境の管理

物理的資産には，前述の機器管理の他，設置場所等（部屋や収納棚，電源設備，空調設備等を含む）も管理対象とされている[8]が，ISMS の管理策区分やその資産特性の違いを考慮して，機器と分けて管理するものとした．こうすることにより，設置場所としての環境と，設置される機器の関係が明確化され，組織全体で見た場合の設置環境の状況や対応状況の把握が容易になる利点がある．表４に環境の管理に必要な項目を示す．ここで示す重要度は，機密性，可用性である．つまり，権限を有する人のみアクセスを許可することが目的とする．アクセス管理は，この重要度を実現するための物理的・環境的手段を示しており，入退出管理や鍵管理およびその記録などが関係する．空調及び電源の項目は，その環境に設置又は保管された資産の可用性，完全性を維持するための必要設備であり，その機能や能力等が対象である．

（4）技術等の管理

通常，機器には各種ソフトウエアや，アクセス制御や管理等の技術的な方策や施策が行われている．ソフトウエアのライセンス管理やセキュリティホールの管理ということを主体とするのであれば，ソフ

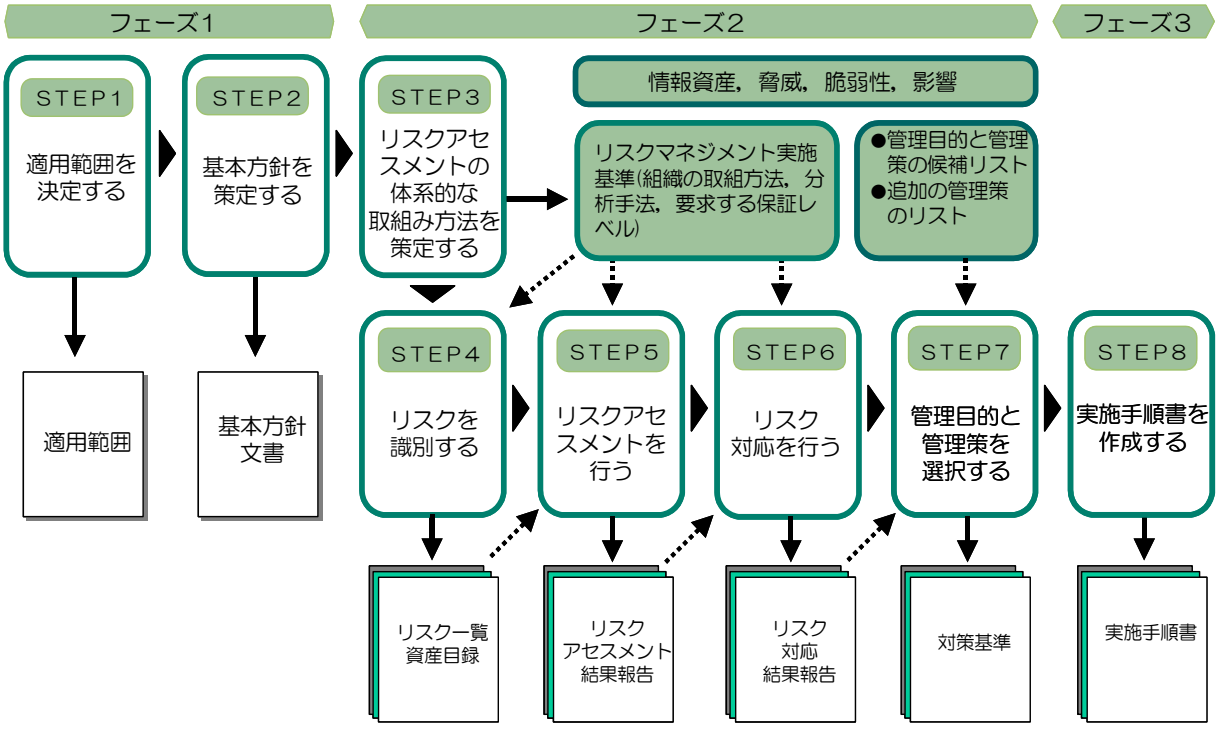

図１　本学で導入したセキュリティポリシ策定手順

8 管理区域の設定と管理をするために必要.

トウエア管理で達成可能と考えられるが，アクセス制御やソフトウエア上に設定される間接的な設定情報等の管理を想定する場合，更に詳細な情報を保有する必要がある．なお，この点は検討課題としており，本稿では述べない．

4.本学のデータベース構築例

4.1　開発方針と目標

本学のポリシ構築において，その最初の課題である資産洗い出しとリスク評価の入力を効率化することにより，学内の資産調査委員の負担を低減することを主目標とし，ポリシ運用開始後は資産目録として活用することを二次目標としている．平成15年末から16年始めは主目標の達成を主眼として開発を行った．また二次目標の達成のための改良は，ポリシ運用と同期して行う予定である．

構築したシステムの開発方針は次の4点である．

（1）資産洗い出しの初期段階で提出された紙（実際はExcelのファイル）媒体の資料を効率よく管理し，今後の洗い出し内容を調査委員が直接入力及び変更を可能とすること．また，類似する内容の資産を入力する際の手間を省く仕組みを組み込むこと．

（2）調査委員が直接リスク評価を行うことにより，ヒアリング等の手間を最小限にすること．このため，リスク評価項目は単純な選択式とすること．（1）と同様に類似資産のリスク評価の手間を省く仕組みを組み込むこと．

（3）洗い出し内容から資産目録を自動生成することにより，リスクアセスメント及びポリシ運用段階における基礎データとすること．

（4）短期間で開発する必要性から，DB言語には開発者らが取り扱いに慣れたSQLを使用し，入力にはWWWサーバ上でPHP言語を使用すること．共にオープンソースを活用し，構築のためのコストを低く押さえること．

以上の目標と方針で，高度情報化基盤センターで平成15年末から平成16年始めの短期間で開発・実装を行った．開発期間はおよそ0.5人／月である．次節では，構築したシステムの詳細について説明する．

4.2　テーブル構造

SQLベースのDB（PostgreSQL）を使用しており，そのテーブル構成（主要部分のみ）を図2に示す．なお，平成16年始めの構築時点において，3章で述べたDBに必要な項目全てが含まれておらず，リスク評価に必要な最低限の項目のみで構築されている[9]．

9 ポリシ運用に従って，残りの項目も整備予定．

表2　情報の管理に必要な項目

項目	内容
情報名，区分	管理対象の情報名，資産区分
情報管理者	管理する部門・担当者・人等
重要度	情報の重要度（機密性，完全性）
入手先／方法	入手先（情報機器等含む）や方法
保管場所	情報機器，記録媒体，保管庫等
伝達先／方法	利用先，利用方法等（電子的含む）
廃棄／方法	情報の廃棄とその方法
外部提供	組織外への提供とその許可者等

表3　機器の管理に必要な項目

項目	内容
機器名，区分	管理対象の機器名，資産区分
機器管理者	管理する部門・担当者・人等
重要度	機器の重要度（可用性，完全性）
設置環境等	設置されている環境，設置方法等
アドレス等	IPアドレスやDNS名等
機器特性	寸法，形状，重量，消費電力等
提供サービス	機器が提供するサービス
情報資産	保有する情報資産等（ソフト含む）

表4　環境の管理に必要な項目

項目	内容
環境名	管理区域や設置場所等
管理者	管理する部門・担当者・人等
重要度	環境の重要度（機密性，可用性）
所在	棟，部屋，棚等の環境の所在
アクセス管理	入退出管理や施錠管理の有無等
空調	空調機能，能力等
電源	電源機能，能力等
収容資産等	収容されている機器や情報資産等

（1）資産目録テーブル

資産目録テーブルは，本システムが構築される直前に表5に示す調査項目で資産洗い出しが実施されており，これを活用するために，表5に準じた構成となっている．また，本学で区別する資産区分及び分類区分を表6に示す．資産区分は，ポリシ策定時点における本学の情報システムの運用形態を考慮して決定しているが，今後の運用形態により変更されることも予想される．

（2）リスク情報テーブル

入力された資産目録に対してリスク評価を行うために，ISMSの管理項目を基にしたリスク評価項目を，通信及び運用管理，アクセス制御，システムの開発及び保守，物理的・環境的リスク（機器対象）及び物理的・環境的リスク（設置場所）に5分類している．これらは，表6-2の資産分類に応じて表7に示すように適用している．また，資産のリスク値の集計においても，表6-2の分類を適用する．

４.３　入力支援

入力者の目録入力支援及びリスク評価入力支援のための機能として，既存の入力項目選択の機能（図3）や一覧画面から既入力結果を複製して新規入力とするテンプレート機能（図4）を有する．これら機能により，新規入力の場合と比較して半分以下の時間で入力できる．下記にこれらの特徴を示す．

（１）目録入力・編集支援

目録入力フォームでは，図3に示すように，新規入力だけでなく過去に入力した項目を選択入力可能としている．これにより，入力内容に関する判断支援を過去の事例により行うことができる（過去の入力履歴は当該部局で入力された内容に限定[10]されている）．目録中の機器名称，設置場所の項目については，同じ名称の物は同一のものとして扱う．これらの入力及び入力支援は，テンプレート機能の整備により，より効率が向上すると推測される（現在，目録入力画面では未使用）．

（２）リスク評価入力支援

入力された資産毎に，表7に示す分類でリスク評価を行う．実際の入力では管理項目5分類を資産分類3分類に適用してリスク評価の入力分類としている．リスク評価は項目数が非常に多いため（合計86項目），テンプレート機能による入力支援が効果的であり，積極的に実装した（図 4）．以下では，３分類されたリスク評価についてその詳細を述べる．

・リスク情報（一般）

表7に示すリスク分類のうち，通信及び運用管理（22項目），アクセス制御（33項目），システムの開発及び保守（18項目）の３分類（73項目）を入力対象としている．資産分類により，適用する項目数が変化するため，実際の入力画面では，入力不要項目には「該当無し」と表示する．これにより，誤入力や，入力の必要性について混乱することを防止できる．

・リスク情報（機器）

表7示すリスク分類のうち，物理的・環境的リスク（機器対象）（8項目）を入力対象としている．資産目録入力時の機器名と対応しており，目録が入力された時点で自動的に入力可能となる． 同一名称の機器については，一回のリスク評価入力でよい．

・リスク情報（設置場所）

表7示すリスク分類のうち，物理的・環境的リスク（設置場所）（5項目）を入力対象としている．資産目録入力時の設置場所に対応しており，目録が入力された時点で自動的に入力可能となる． 同一名称の場合，リスク情報（機器）場合と同様である．

10 他部局の内容を参照可能とすることにより，より効率的な入力支援となるが，現状では，セキュリティ的な配慮から，現在の範囲に限定している．

表５　資産洗い出し項目

項目名	内容
システム区分	本学で定めた７区分のいずれか
管理番号	識別番号
機器名称	機器の名称
設置場所	機器の設置場所
情報名	情報名，システム名
可用性	機器の重要度（可用性）
重要度	情報の重要度（機密性）
作成／修正	入手先，方法，担当者
保管	保管場所，保管方法
出力先	出力先・連携先／方法／対象
廃棄	廃棄方法
情報操作許可	作成／修正／利用／廃棄の許可者
外部提供	出力先／目的／方法
外部提供許可	上記外部提供の許可者
備考	その他の情報

表６-1　資産区分一覧

資産区分名	内容
基幹・情報系システム	共用利用されるシステム
研究系システム	研究利用されるシステム
教育系システム	教育利用されるシステム
病院系システム	病院系システム
外部情報システム	本学外のシステム
基幹・支線 NW	基幹ネットワーク等

表６-2　資産分類一覧

分類名	内容
機器・システム	機器名やシステム名
情報	情報そのもの
環境	保管場所，設置場所等

表７　資産分類に応じたリスク評価分類の適用

	資産分類		
リスク評価の分類	機器等	情報	環境
通信及び運用管理	△	△	－
アクセス制御	○	－	－
システムの開発及び保守	△	△	－
物理的・環境的リスク（機器対象）	○	－	－
物理的・環境的リスク（設置場所）	－	－	○

○：全て適用，△：部分的に適用：－：適用無し

表８　リスク度の段階

項目	値	内容
該当せず	－	項目が該当しない
十分に対策済み	0	リスクはない
現状で問題なし	1	リスクは低い
対策強化が必要	2	リスクは中程度
未対策	3	リスクは高い

・リスク度の段階

本システムにおけるリスク評価では，表 8 に示すリスク度の段階を用いている．「未対策」を最高数値 3 とし，「十分に対策済み」を最低数値 0 としている．この値はリスク値計算のためのパラメタとして使用される． また，リスク評価入力の取り扱い上，「該当無し」の選択肢も設けてあり，そのリスク評価が当該資産に該当しない場合に選択する．これは，項目が未入力となっている場合，見落として「未入力」なのか，該当しないために「未入力」なのかを判別できなくなることを防止するための方策である．これにより，「未入力」となっている場合には，見落としたか，意図的に入力を避けたかの何れかの場合と考えられ，入力の催促を機械的に行うことが可能となる．なお，実際のリスク評価入力は，ラジオボタンによる選択方式としている．

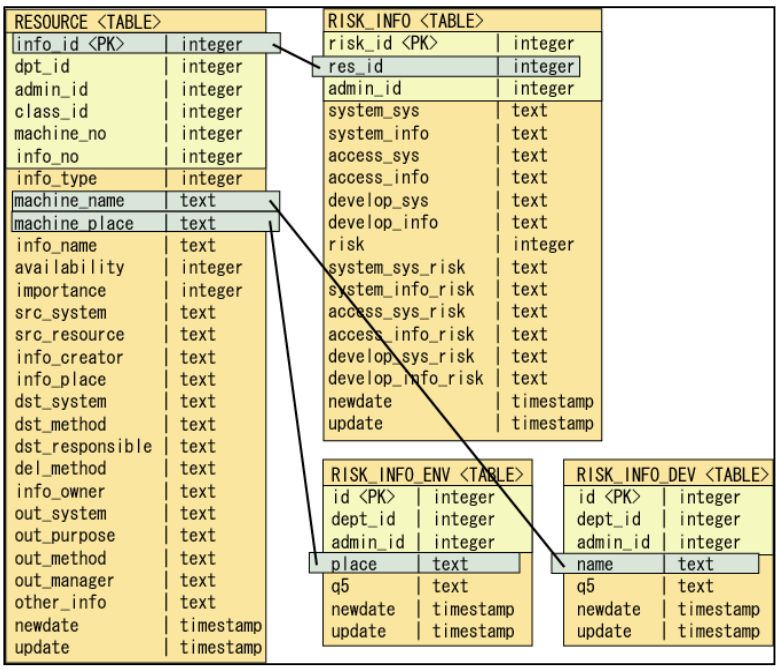

図 2　テーブルの構成（主要部分のみ）

図 3　入力選択による入力支援

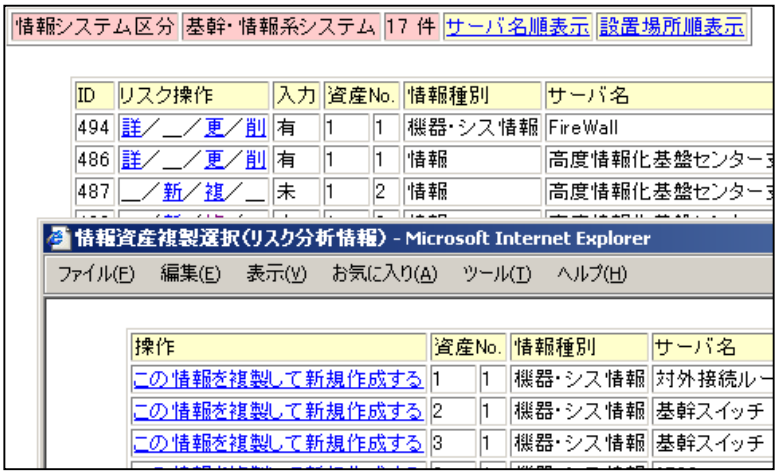

図 4　テンプレート機能による入力支援
（上段：作成元情報，下段：テンプレート選択）

4.4　リスク値計算と分析支援

入力されたリスク度から，下記式によりリスク評価に対するリスク値を算出する．重要度は 1 から 3 範囲としている．リスク度は表 8 に示す通りである．リスク係数は資産区分毎にリスク評価項目に対して設定した係数（0 から 3 の範囲）であり，リスク評価項目に対応した管理項目を脅かす頻度を基準にしている．よってリスク評価項目毎の最大リスク値は 27 となる．リスク評価項目毎に異なる最大リスク値を定めたリスク値計算及び分析方法も議論されたが，最終的には人手でリスク判断を行うため，同一最大値によるリスク値管理方法を採用した．なお，資産のリスク値はリスク評価項目毎に算出されたリスク値を表 7 に示す資産分類単位で集計することにより得られる．

リスク値＝重要度×リスク度×リスク係数

図 1 の STEP6，7 において，組織における管理策選択の基本情報とするため，個々に算出されているリスク値を集約（リスクアセスメントの要約）しなければならない．本学では，各資産のリスク評価項目毎に算出されたリスク値の最大値で集約する手法を用いた．具体的には，各資産区分に含まれる資産に対してリスク評価項目毎の最大リスク値を調べ，この最大リスク値を当該資産区分における当該リスク評価項目のリスク値とする方法である． この場合，リスク値の分布と無関係に値が決定されるため，リスクを過大に評価する傾向があると推測される．しかし本学のポリシ策定における議論では，そのようなリスク値を持つリスク評価項目の存在を，集約した結果に反映すべきであるとの意見から，この方法を採用している．

なお，資産のリスク値の最大値による集約方法も検討されたが，資産のリスク値が最大であっても，リスク評価項目のリスク値が最大である保証は無いため，この方法は採用しなかった．

集約により，部局毎に資産分類別のリスク情報がリスク評価項目毎に集約されるため，部局の傾向（又は管理実施状況）の把握に大いに役立つ．また同様の集約を全体に対して行うことにより，組織全体のリスク状況が把握できる．表 9 はある部局のリスク値を集約（一部）した例である．これは，資産区分，資産分類，重要度でリスク評価項目毎に集約したものである．各資産区分中，左側３項目と右側３項目は，それぞれ，機器・システム，情報に関して重要度順（重要度３，２，１）にリスク値を表している．空欄部分はその重要度に該当する資産が無いことを意味する．

次に，集約結果を検討してリスクを受容する閾値を設定する．なお，リスクの受容とはそのリスクを受容し，積極的な防止策（回避，転嫁，移転）は実施しないことを意味する．集約結果からリスク受容の閾値以下のリスク値を除去し，残ったリスク値を含むリスク評価項目に対してリスク対応を検討後，リスク受容の閾値以下とするための管理策の選択・決定が行われる．この選択・決定が行われた内容に基づいて，対策基準を策定することになる．本システムでは，リスク値の算出，集約結果の作成及びリスク受容の閾値処理を自動化しており，リスク分析支援を行っている．

４.５　システム構成

構築した資産登録-リスク分析システムは，パソコン（DOS/V マシン，P4 2GHz, Memory 1GB）の FreeBSD 上に構築されており，DB には Postgre-SQL，WWW サーバには Apache，WWW サーバ側の処理ロジック言語に PHP を用いて実装されている．利用者は，各自のパソコン等から Web ブラウザ（SSL で保護）を介し，利用者認証後に使用可能となる．セキュリティ等の配慮から各利用者は担当部局のみアクセス可能で，全体をアクセス可能な権限（閲覧を含む）を有する人は数人程度である．なお，図 5 程度のアクセス頻度（一日 300 件程度）であれば，上記機器性能で十分である．

５．運用

５.１　運用状況

平成 16 年 1 月下旬から，提出された洗い出し情報の入力（追加分を含む）とリスク評価入力が行われた．洗い出しにおいて，ポリシ策定組織作りを行うために支線管理者と資産調査委員を中心として開催されたキックオフミーティングの参加者が各部局の責任者となり，末端システム管理者までを含めた教職員により資産洗い出しとリスク評価入力の作業が行われた．洗い出された資産は約 770 項目に集約された．リスク評価入力期間は約 3 週間程度設けられ，登録された資産の 80%に相当する 610 件に関してリスク評価入力が行われた．図 5 は，日付毎のリスク評価入力件数を示したグラフである．

洗い出された資産が，大学構成員 8000 名，部局数 31 に対して 800 件程度と少ない理由は，本学の洗い出し作業では，詳細な洗い出し及びリスク評価は表 1 に示す範囲に留めたことと，システム単位での入力を許容したことによる影響が大きい．本学では，概算で 7700 台程度（平成 15 年 10 月時点）の機器を有しており，全体の 1～2 割程度が入力されたものと判断される．部局の平均登録数は 24 件で，システムに登録された入力者数は 65 名で，一人平均 10 件程度のリスク評価入力数である．

表 9　リスク評価項目のリスク値を集約した例

項目	基幹･情報系						基幹･支線NW					
	機器等			情報等			機器等			情報等		
	重要度			重要度			重要度			重要度		
	3	2	1	3	2	1	3	2	1	3	2	1
Q6_00	18	12	6				18	12				
Q6_01	18	12	6				18	12				
Q6_02	18	12	6				18	12				
Q6_03	18	12	6				18	12				
Q6_04	12	8	4				12	8				
Q6_05	12	8	4				12	8				
Q6_06	12	8	4				12	8				

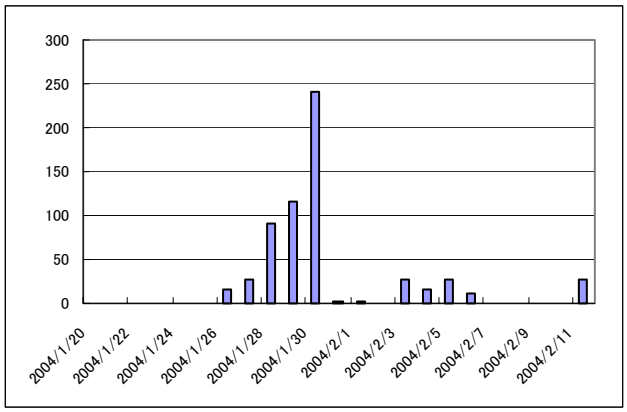

図 5　日付毎のリスク評価入力件数のグラフ

５.２　効果

約 3 週間程度の短期間でリスク評価入力が実施された．入力の大半は，図 5 が示すように，前半 5 日間に集中している．リスク評価項目が 86 項目と非常に多いにもかかわらず，短期間で入力されたことは，資産洗い出し調査委員諸氏の協力も大きいが，

本システムで用いた入力支援による効果があったものと判断できる．また，リスク評価入力後の目録作成及びリスク分析のためのリスク集約作業は数時間で完了しており，本システムのリスク分析支援による効果が確認された．

５.３　問題点と考察

今回の構築したシステムの運用上，得られた問題点と今後の課題についての考察を下記に示す．

（１）クライアントの資産登録の必要性

今回の洗い出しに伴う入力では，クライアント機器のリスク分析にベースラインアプローチを用いたため，潜在的なリスクが残っている可能性は高い．大学のように，多様な使用法が存在する組織では，同じクライアント機器でも異なる使用が存在する（例えば，教員と事務職員等）．このため，明確なポリシ運用を実施するためには，クライアント機器の資産登録及びリスク評価の入力が不可欠である．

（２）資産登録率の問題

ポリシ策定時の資産洗い出し割合が低い場合，潜在的なリスクを抑えるために，少なくとも，特徴的な運用を行っている機器類は資産登録を行うように，教育及び指導する必要がある．その特徴を代表する機器が登録されれば，その機器に関するリスクの潜在化は避けられ，その後の同様機器の入力は入力支援機能により省力化を図ることができる．

（３）機器の分類区分の再検討

現時点では機器の分類を明確に想定していないが，今後の多様な機器の登場を見越して，何らかの機器分類区分を導入する必要がある．考慮すべき点は，情報家電や各種の新しい概念の機器が登場することを鑑みて，従来のサーバ機器，クライアント機器という分類は，今後，明確でなくなると推測されることである．このため，機器単位の分類だけでなく，機能単位での分類も必要になると考えられる（例えば機器に機能目録を設ける）．

（４）ポリシ運用のための機能追加

本学のポリシ運用では，新規設置される機器及び新規に作成される情報を資産として登録することになる．入力者が多数存在することが想定されているため，統合認証システムとの連携や，階層的な権限管理機能の導入も検討課題である．

（５）システムの改良

４.２節で述べたように，構築したDBには運用のための情報が不足しており，３章で示した項目を今後整備する必要がある．また，上記に列挙した問題点の解決及び課題の達成をするためのシステムの改良が必要である．

６.おわりに

セキュリティポリシ策定において課題となる，資産洗い出しやリスク評価は，ISMSに準拠したポリシを策定する上で必要なプロセスである．しかしながらその作業量は多く，結果として簡易手法（例えばベースラインアプローチ）等により，回避してしまうこともある．しかし，回避により表面化しないリスクの存在が，今後問題視されることは確実である．この表面化しないリスクを検出する意味でも，詳細な資産洗い出しとリスク分析は不可欠である．

本稿では，過去に構築したDBの経験から，この作業を支援するためのDBについて必要とされる項目について検討・提案した．示した各項目は，セキュリティポリシを構築及び運用するに際して，必要最小限と判断されるもので，実際の構築には，組織毎の実情を含めた検討が必要と考える．

本学のポリシ策定は，本稿執筆時点で，発行手順に移行している．今後，本研究はポリシ運用のためのDB支援を行う段階に達しており，本稿で提示した項目を含めて運用のための改良を行う．

謝辞　本学のセキュリティポリシ策定は平成15年度徳島大学学長裁量経費によるものである．また，コンサルタントであるSTNet寶田氏の多数の貴重なアドバイス及び本学セキュリティポリシ策定WG諸氏の意見と議論は，本施策の遂行に多いに貢献した．ここに謝意を表す．

参考文献

[1] 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のガイドライン"，2000. http://www.kantei.go.jp/jp/it/security/index.html

[2] 大学の情報セキュリティポリシに関する研究会，"大学における情報セキュリティポリシの考え方"，2002. http://www.kudpc.kyoto-u.ac.jp/Security/

[3] 電子情報通信学会，情報処理学会，電気学会，"高等教育機関におけるネットワーク運用ガイドライン"，2003, http://www.ieice.org/jpn/teigen/nwgl.html

[4] 打川和男，"情報セキュリティポリシの実践的構築手法"，オーム社，2003.

[5] 松浦健二 ほか，"大学における ISMS 準拠のセキュリティポリシ策定に関する一考察", 報処理学会研究報告, Vol.2004-DSM-33, (号), pp.59-64, 2004.

[6] 日本工業標準調査会，"情報技術－情報セキュリティマネジメントの実践のための規範"，JIS X 5080，2002.

[7] 日本工業標準調査会，英和対訳版 British Standards, Information Security Management Systems – Specification with Guidance for Use, BS7799-2:2002.