情報セキュリティマネジメントのためのリスク分析ツールの試作

2005MT062 丸山 美希　　2005MT109 田口 佳美
指導教員　後藤 邦夫

1　はじめに

近年，不正アクセスやコンピュータウイルス，情報漏洩に関する事件が多発しており，組織の情報管理に対する関心が高まっている．そこで，多くの企業が情報セキュリティマネジメントシステム (以下，ISMS)[3] の認証を取得している．しかし，何百から何千の情報資産を分類し，評価するのは相当な手間がかかる．また，評価基準を定めないと正しい評価はできない．

本研究では，これから ISMS の導入する企業の少しでも助けとすることを目的とし，セキュリティマニュアル作成の基本となるリスクマネジメントの部分を自動化するシステムを試作する．本システムでは，データベースとして PostgreSQL[1] を，Web アプリケーションを実現するためのスクリプト言語として PHP[2] を使用する．

このようなシステムは，市販ソフトウェア [5] として実在している．しかし，実際に管理策にどのくらい手間がかかるか，どのくらいコストがかかるかなどは知ることができないため，本システムではその部分を取り入れる．

なお，システムの考案，構築は共同で行い，その中でも特に，丸山はリスクアセスメント部分，新規ユーザ・資産・脅威・脆弱性の登録部分のプログラミングを担当した．田口はリスク算出，管理策追加部分のプログラミングを担当した．

2　ISMS について

この節では，ISMS 及び，本研究で提案するシステムの自動化する部分が ISMS でどのように定義されているかを説明する．

2.1　ISMS とは

ISMS とは，個別の問題毎の技術対策の他に，組織のマネジメントとして，自らのリスクアセスメントにより必要なセキュリティレベルを決め，プランを持ち，資源配分して，システムを運用することである．組織が保護すべき情報資産について，機密性，完全性，可用性をバランス良く維持し改善することが ISMS の基本コンセプトである．

2.2　ISMS におけるリスク特定から管理策の選定まで

ISMS で採用されているモデルは，「Plan-Do-Check-Act(PDCA) モデル」である．本システムで自動化するのは，その中でも Plan(ISMS の確立) の事項 4 から 7 のリスクマネジメントの部分である．その部分を順に説明する．

まず，リスクを特定することから始める．リスクの特定では，「資産の洗い出し」と「脅威・脆弱性の明確化」の 2 つの作業が実施される．「資産の洗い出し」では，資産のグループ化が行われる．「脅威・脆弱性の明確化」では，まずどのような性質のセキュリティ対策を実施すればよいか整理しやすくするために，脅威を分類する．

次に，リスク評価を行う．本システムでのそれぞれの評価区分は，全て 5 区分でレベル 1 から 5 とする．資産の価値を評価するさいは，機密性，完全性，可用性に分け，それぞれが損なわれた時の事業上の影響 (損害) を評価する．脅威の評価は，脅威の識別と同様に自身の業務と関連する他部門と協力して整理する．脆弱性の評価は，その資産の持つ弱点がどの程度であるかを現在実施されている対策を考慮して評価する．

以上の評価基準の例として，意図的脅威に対する脆弱性の評価基準を表 1 に示す．

表 1　脆弱性の評価基準

レベル	意図的脅威に対する脆弱性
1	最高程度の対策を実施済み
2	高度な専門知識や設備を持つ者によって可能
3	専門能力を持つ者によって可能
4	一般者が調査を実施すれば可能
5	一般者が普通に実施可能

リスク値は，以上の「資産の価値」,「脅威の大きさ」,「脆弱性の度合い」の 3 つの評価を用いて，次の (1) 式で算出する．

$$\text{リスク値} = \text{資産の価値} \times \text{脅威} \times \text{脆弱性} \qquad (1)$$

資産の価値，脅威の大きさ，脆弱性の度合いの最大値が 5 であるので，リスク値の最大値は 125 である．リスクが算定されたら，リスク評価基準と比較することでリスク評価を行う．リスク評価基準は，経営陣が受容可能なリスクの水準として決定した値である．受容可能な範囲であったとしても，資産価値や脅威，脆弱性等の環境に変化が生じた場合は，適宜リスク値を見直さなければならない．次に，リスク対応を行う．本システムでは管理策を追加してリスク値を軽減することを目的とするため「適切な管理策を採用する」を選択したとして進める．

最後に，管理目的と管理策を選択する．管理策を選択した後，資産が保有する脅威や脆弱性に対してどう効果的なのか，どの程度リスク値が軽減され，残留リスクはどの程度なのかを算出する．特に管理策を選択した後も残留リスクが高い場合は，追加の管理策を検討し，その繰り返しでリスク値を受容可能な範囲に落し込む．

3　システムの概要

この節では，2 節で述べた部分をどのように自動化するか及び，使いやすさを考慮したユーザの画面を説明

する．

3.1 リスクアセスメントの自動化

リスク特定の部分では，資産名，脅威名，脆弱性名の一般的なものを分類毎に用意しておく．しかし，組織によって所有する内容は異なるため，リストから選択する形式とする．また，リストにないものは，各組織毎で追加登録する．

リスク評価，算出の部分では，評価者によるバラツキを防ぐため，用意されたレベル 1 から 5 までの評価基準に沿って評価を入力する．管理策の追加部分では，JIS Q 27002:2006 の箇条 5 から 15 までにかかげられているもの用意しておき，リスク特定同様にリストから選択する．

管理策追加後の再評価では，ユーザ入力にした．再評価を自動化するためには，組織毎にその管理策追加後に脅威，脆弱性に与える影響度をあらかじめ定めておく必要がある．しかし，管理策の影響度は組織毎に異なるため，あらかじめ定めておくことは不適切であると判断し，入力形式とした．

手間，コストの算出部分では，追加する管理策を決定した後，その管理策を取り入れた際の手間とコストを入力し，それぞれの合計をその資産管理に対する手間とコストとして表示する．

また，システムの基本機能部分の流れの説明として，機能のモデル化に用いられるアクティビティ図 [4] を図 1 に示す．

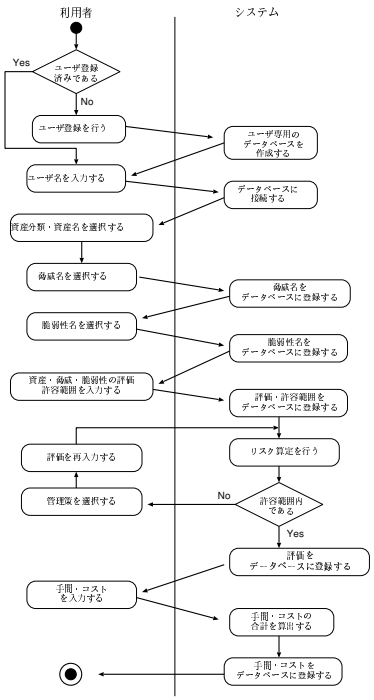

図 1　基本機能のアクティビティ図

3.2 使いやすさを考慮したユーザの画面

本システムを初めて利用する人が分かりやすいようにマニュアルページを作成した．マニュアルページには，本システムの説明，使い方を記載した．また，操作の流れと行っている操作が分かるように，画面上部に常に表示される図を追加した．その画面を図 2 に示す．

図 2　システムの流れ

4 システムの実現

この節では，システム構築について説明する．本システムでは，データベースとして PostgreSQL[1] を Web アプリケーションを実現するためのスクリプト言語として PHP[2] を使用する．

4.1 データベース

本システムのデータベースの要求分析結果の例として，「ある情報資産に対して必要な管理策を知りたい」，「リスク値が基準以下だった場合のみ，管理策を追加したい」や「管理策を追加するとどれくらいの手間がかかるかコストがかかるかを評価したい」などが挙げられる．

データの構造を ER 図で現したものが図 3 である．ER 図では，分析する対象が実体，2 つの実体関係が関連，実体や関連が持つ属性が属性として表現される．

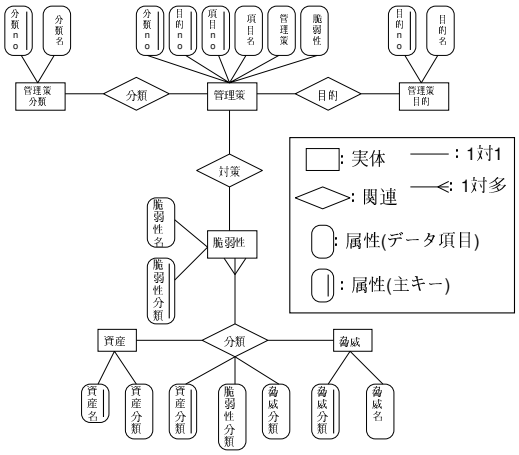

図 3　データ構造の ER 図

関係データベースを表 2 に示す．

表 2　本システムのテーブル一覧

テーブル名	項目名					
資産リスト	*資産名			資産分類		
分類リスト	*{ 資産分類 }		{ 脆弱性分類 }	{ 脅威分類 }		
脆弱性リスト	*{ 脆弱性分類 }			{ 脆弱性名 }		
脅威リスト	*{ 脅威分類 }			{ 脅威名 }		
管理策リスト	*分類 no	*目的 no	*項目 no	項目	管理策	脆弱性
管理策目的リスト	*目的 no		目的分類	目的名		
管理策分類リスト	*分類 no			分類名		

「*」は主キー，「{}」は配列を表わしている．

次に，必要な脅威，脆弱性，管理策を選択可能とするが，基本は変更されないようにするために，テーブルを 2 つ追加してそこに挿入していくことにした (表 3)．

表 3　追加テーブル

テーブル名	項目名				
my_select	*資産名	{ 脅威名 }	{ 脆弱性名 }		
select_manage	*資産名	{ 管理策 }	機密性	完全性	可用性
	脅威評価	脆弱性評価	手間	コスト	

最後に，ユーザ登録での新規ユーザのデータベースの作成方法を説明する．まず，テンプレートのデータベースを用意しておき，それをコピーして各ユーザ名のデータベースを作成する．

4.2　Web アプリケーション

本システムで必要なページをページ間の関係を明確にして遷移図として図 4 に示す．

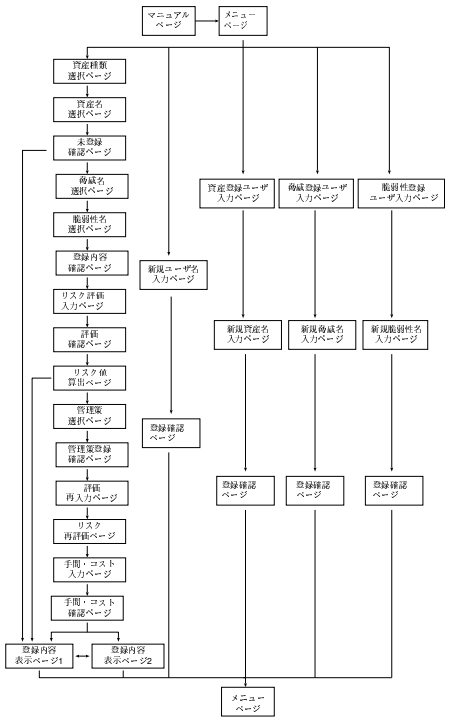

図 4　Web ページの遷移図

本システムの Web アプリケーションの要求分析結果の例として，資産名選択ページを挙げる．

- 資産名選択ページ
  - 資産名を選択し，「検索」ボタンを押すと，未登録確認ページが表示される
  - 資産名未選択の場合，資産名が未選択であることと資産名選択ページへのリンクが表示される

この要求分析の実現を説明する．資産の種類と資産名は複数から 1 つ選択するのでセレクトボックスを使用する．脅威，脆弱性，管理策は複数から複数選択するのでチェックボックスを使用する．また，資産名の上書き確認は 2 つから 1 つ選択なので，ラジオボタンを使用する．

5　評価の方法とその結果

この節では，本システムの評価方法について説明する．本システムの評価は，作成者と利用者の視点から評価する．

5.1　作成者の評価

本システムを作成者の視点から評価する方法を説明する．

5.1.1　評価方法

作成者の評価では，システムが必要な用件を満たしているかシステムテストとして，機能テスト [4] と例外処理テストを行う．

機能テストでは，画面の遷移，画面表示，データベースの更新を確認する．まず，画面の遷移，画面表示のテストでは，すべてのページの遷移を網羅するように，以下の 3 件のテストケースで行う．有効範囲外の値であった場合は，例外処理テストで確認するので，機能テストで入力する値は，有効範囲内であることを前提として行う．

- ケース 1
  - 未登録確認ページで'YES' を選択
  - リスク値算出ページで' 許容範囲内でない' と判定
- ケース 2
  - 未登録確認ページで'YES' を選択
  - リスク値算出ページで' 許容範囲内である' と判定
- ケース 3
  - 未登録確認ページで'NO' を選択

以上の 3 件のケースを図 4 で示されたすべてのページ遷移で実行して確認する．次に，データベース更新の確認は，データベースに直接接続し確認する．

例外処理テストでは，チェックボックスとラジオボタンが未選択の場合，入力フィールドが未入力，有効範囲外の値であった場合の処理を確認する．

5.1.2　テスト結果

機能テストの結果，いずれのテストケースでもきちんしたページの遷移と画面表示が確認できた．その後，3

件のテストケースで登録された内容がデータベースにきちんと更新されいることを確認した．

例外処理テストの結果，未選択，未入力である場合のエラー処理はきちんとできていることを確認した．また，有効範囲外である値として，アルファベット，全角文字，全角数字，記号が挙げられるが，数値入力場所への数値以外の入力は想定しておらず，有効範囲外の数値以外のエラー処理ができていないことが確認できた．

5.2 利用者の評価

利用者の視点からの本システムを評価する方法を説明する．

5.2.1 評価方法

利用者の評価では，情報分野を専攻している大学生と大学院生を対象にアンケートを行う．アンケートは，実際にシステムを使ってもらって，以下の項目を評価してもらう．

- システムの使いやすさ
  - 操作 (進んで行く中で操作に困るところがなかったか等)
  - 入力 (入力内容に困ることがなかったか，最低限の入力に抑えられているか等)
  - 誘導 (困ることなく進められたか，間違えた場合の誘導は適切だったか等)
- システムの性能
  - リスク分析の役に立ったか
  - このツールを使用することでリスク分析の手間は軽減されたか
  - 適切な管理策が作成されたか

評価は，奇数段階だと「どちらでもない」の評価が増えてしまうため，1(Bad)〜4(Good) の 4 段階で評価してもらう．

5.2.2 アンケート結果

まず，評価の結果は平均の値を表 4 に示す．

表 4　評価の平均値

評価項目	操作	入力	誘導	役に立ったか	軽減されたか	適切な管理策か
評価平均値	3.3	3.1	2.8	3.3	3.2	3.2

次に，コメントをまとめたものを以下に示す．

- 管理者やリスクマネジメントの講習を受けた人対象に作られていて，専門知識がないと分からない部分がある
- 戻るボタンがないため，ブラウザのボタンで戻ると，複数項目の入力があるページで未入力があって戻った時に，入力した値も消えてしまったり，不具合が発生する箇所が出てきてしまう部分がある
- 評価基準や入力の例が少なく，評価入力や何を入力したらよいかに困った

以上より，説明や入力例の不足で知識がない人には分かりにくく，途中からの変更が行えないシステムになってしまっていることが分かった．

しかし，使いやすさ，性能の評価は共に高かった．この原因として，使いやすさの評価では，情報分野を専攻している大学生対象に実施したため，使い慣れていて困ることはなかったが，初心者では困ってしまうという意見だと考える．性能の評価では，意見から情報分野を専攻していても，専門的な知識がないと，リスクマネジメントがどのくらい手間がかかるかなどの基準が分からずに評価が高くなってしまったと考える．

6 おわりに

本研究では，リスク分析とリスク算定と管理策選択の自動化を実現することができた．また，追加機能として，登録されていない資産，脅威，脆弱性の登録と資産管理に必要な手間とコストの一覧の確認を可能とした．さらに，ユーザ登録の際に，ユーザごとのデータベースを作成することで，複数のユーザの利用も可能となった．また，サーバを稼働して，システムを使ってもらえるようにすることもできた．

以下に今後の課題を挙げる．

- 用語の説明や評価基準，入力の例を増やすことで，専門的な知識のない人にも分かりやすくする
- 戻るボタンで戻って変更可能にする
- 管理策が脅威，脆弱性のどちらにどれだけ影響を与えるかを管理策 1 つ 1 つに設定し，再評価を自動化する
- データベースで項目名がユーザ名とパスワードのテーブルを作成してユーザ認証を行う

また，最終的な目標は，セキュリティマニュアルが自動作成できるシステムである．

参考文献

[1] Lockhart, T: PostgreSQL ユーザガイド (accessed Aug. 2008). (http://www.postgresql.jp/document/pg653doc/j/user/).

[2] The PHP Group: PHP マニュアル (accessed Aug. 2008). (http://www.php.net/manual/ja/index.php).

[3] 日本規格協会/編：対訳 ISO/IEC27001:2005(JIS Q 27001:2006) 情報セキュリティマネジメントシステム [ポケット版]，日本規格協会 (2006). (http://www.isms.jipdec.jp/index.html).

[4] 町田欣史：まるごと図解 最新 UML がわかる，技術評論社 (2002).

[5] 富士通ソーシアルサイエンスラボラトリ：リスク分析・対策立案ツール (accessed Aug. 2008). (http://www.ssl.fijitsu.com/products/network/bs7799/racontis-web/).