情報セキュリティポリシー作成支援システムの開発

林克明[*]　大江好充[**]　水上大樹[**]　上田芳弘[*]

近年の企業活動において情報システムは欠かせない業務環境となっている。そのため，様々な脅威から情報システムや情報資産を守ることの重要性が増大しており，情報セキュリティ対策の一層の強化が求められる。そこで，企業内での総合的な情報セキュリティ対策の指針となる情報セキュリティポリシー(以下，ポリシーという)の作成が重要となっている。しかし，ポリシーの作成には一般的に多くの時間と費用を要する。本研究では，従来の作成プロセスを見直すことで作成時間の短縮を図り，さらに中小企業での利用を考慮したポリシー作成支援システムを開発し，企業で評価実験を実施した。本報告は，システムの特徴と評価実験から得られた，作成時間とカバー率の結果から本システムの有効性を示したことについて述べる。

キーワード：情報システム，情報資産，情報セキュリティ，情報セキュリティポリシー

Development of Support System for Establishing Information Security Policy

Katsuaki HAYASHI, Yoshimitsu OOE, Daiki MIZUKAMI and Yoshihiro UEDA

Information systems have come to play a vital role in recent company activities. Therefore it is necessary to protect information systems and information assets from various risks. Information security policies, which outline comprehensive rules for security inside a company, have been receiving an increasing amount of attention. However, the establishment of a policy requires a lot of times and expense. We have developed a support system to assist small- and medium-sized businesses in establishing a policy. The time required is shorter than that required by other systems, because it involves reviewing conventional building process. The system was tested at companies for two kinds of performance evaluations. The results demonstrated the effectiveness of the system.

Keywords：Information system, Information asset, Information security, Information security policy

１．緒　　言

近年の企業活動には，情報システムが欠かせない業務環境となっており，今後もさらなる情報システム化が見込まれている。しかし，企業が情報システムに対する依存度を高めるということは，情報システムに対する脅威がそのまま企業の脅威に繋がることを意味する。最近では個人情報の漏洩，ウイルスの侵入，ハッカーによる情報の破壊・改ざんなどの情報セキュリティ事件，事故が多発し，企業活動に悪影響を与えている。従って，様々な脅威から情報資産(企業が所有するコンピュータやシステム，顧客データ，売り上げ情報，ドキュメントなど)を守るため，情報セキュリティ対策の一層の強化が重要となっている。そのためには，総合的な情報セキュリティ対策の指針となる情報セキュリティポリシーの導入が効果的であり，作成，導入する企業が近年増加している。ポリシーを導入することにより，1)顧客からの信頼を獲得，2)現状の情報資産の把握による効果的な対策の仕組みが構築可能，3)管理基準が一定化することによる対策費の節減効果，4)組織的な見直しにより最新リスクへ対応可能，などの効果が期待できる。

しかし，その作成に必要な時間や費用は企業にとって負担となる。そのため，ポリシーを作成，導入している企業は，情報セキュリティ事故などに敏感な，社会的信頼性を重視している金融機関や，大企業，情報サービス業などの一部に限られている。一方，一般的な中小企業ではポリシーの普及以前にポリシーの必要性が認識されていないように思われる。

[*]電子情報部　[**]金沢大学工学部

情報セキュリティ対策が不十分な企業に対しては，まずポリシーの導入を図ることが情報セキュリティ対策の第一歩であると考える。そこで，主なユーザを中小企業，特にポリシーが未導入の企業の情報システム担当者を対象ユーザとして，短時間で作成するためのポリシー作成支援システムを開発し，その評価を行った。本システムの目的は，中小企業におけるポリシーの普及であり，これら企業の情報セキュリティ対策底上げと充実にある。

２．情報セキュリティポリシー

２．１　ポリシーの構成

ポリシーとは，「情報システムの安全を確保するための基本的な考え方」[1)]とされ，情報資産を守るために行う対策や規約をまとめて文書化したものである。情報資産には，情報システムや記憶媒体だけでなく，書類などの紙も含まれる。そのため，ウイルスや不正アクセス対策だけでなく，文書類の管理や物理的な入退室管理もポリシーの対策に含まれる。

ポリシーは一般的に 3 階層構造をなしており，最上位に位置する基本方針から，対策基準，実施手順の順で構成される。なお，それぞれの概要は次のとおりである。

1)基本方針　ポリシーの最上位階層に位置し，情報セキュリティ対策に対する目的，および目的を達成するための行動指針を示した宣言文である。企業においては経営者が果たすべき役割を述べることが多い。

2)対策基準　基本方針に定められた情報セキュリティを確保するために遵守すべき行為および判断の基準である。すなわち，基本方針を実現するために何を実行しなければならないかをより詳細にまとめた文書である。

3)実施手順　対策基準に定められた内容を，具体的な情報システム又は業務において，どのような手順に従って実行していくのかを社内の各部署レベルで規定した文書である。すなわち，対策基準を実施するための詳細なマニュアルである。

本システムではこれら 3 階層のポリシー作成を支援する。ただし，本システムでの実施手順は，本来の実施手順ほど具体的な内容を提示せず，実施手順を作成する場合の注意事項という位置づけである。実施手順のレベルでは，汎用性が低いため，企業毎ではなく部署や事業部単位での作成が必要となる。

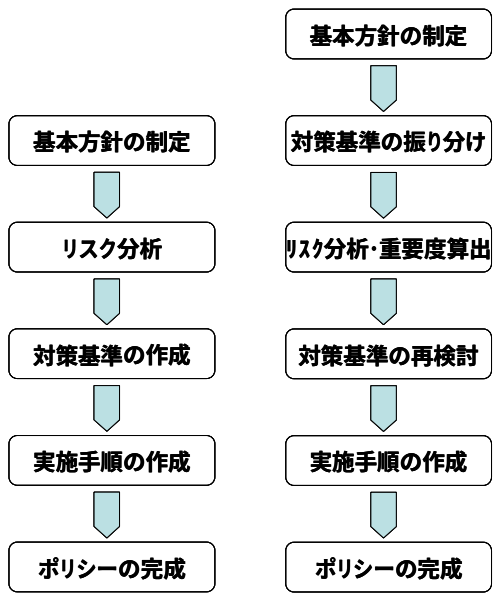

図１(a)一般的なポリシー作成のプロセスと
(b)本システムでのポリシー作成のプロセス

２．２　一般的なポリシーの作成方法

ポリシーを作成する一般的なプロセスを図 1(a)に示す。まず基本方針として，情報セキュリティ対策を実施する目的，対象となる範囲，組織の基本的な考え方を定める。次に，組織において保護すべき情報資産を明らかにし，それらに対するリスクを評価(リスク分析)し，その結果から得られた各情報資産に対する個々の対策について体系化し，対策基準を定める。そして，その対策基準を具体的な業務や情報システムにおいてどのような手順に従って実施していくかをまとめた実施手順を定める。

このうち，一般的な作成方法でのリスク分析は重要なプロセスであり，また時間を要する工程でもある。これに要する時間は，通常 2 週間から 2 ヶ月程度[2)]とされている。

リスク分析とは，前述のように情報資産の特定とリスクの評価である。一般的な作成方法では，ここで十分に情報資産を検討しておくことがポリシーの品質を左右することになる。リスクの評価とは，ある情報資産に損害を与える可能性が考えられる外的要因の危険(脅威)と内的要因の危険(脆弱性)にどのようなものがあるか，そしてその危険が生じた場合どの程度の損害が想定されるか，さらにその危険がどの程度の頻度で発生するかを想定する。これにより，損害が算出される。また，比較を容易にするた

めに損害を金額に換算する方法もある。

さらに，リスク分析は，組織における情報システムなどの現状把握に有効である。

３．システムの概要

３．１　システムの特徴

本システムの特徴は，従来の作成方法とは作成プロセスを変更することにより大幅な作成時間の短縮を目指したことである。

用いた対策基準は 132 個のデータから構成され，JIS X5080[3](以下 JIS という)を参考にし，それに準拠するようにした。なお，上記のデータは以下のように JIS に沿って分類してある。

1)情報セキュリティ基本方針
2)情報セキュリティ基盤
3)資産に対する責任
4)職務定義および雇用におけるセキュリティ
5)セキュリティが保たれた領域
6)運用手順および責任
7)アクセス制御に関する業務上の要求事項
8)システムのセキュリティ要求事項
9)事業継続管理の種々の面
10)法的要求事項への適合

リスク分析に用いる脅威のデータ数は 54 個であり，準拠する規格が無いため，複数の事例資料などから代表的なものを取り上げた。

３．２　本システムでのポリシー作成方法

本システムを使用してポリシーを作成するプロセスを図 1(b)に示す。本システムでは，情報資産の特定を行わず，最初に対策基準の振り分けを行い，次にリスク分析を行う。

３．２．１　対策基準の振り分け

対策基準の振り分けとは，上述した汎用の対策をユーザに順次全て提示し，その対策の要否を判断させることである。

例えば，「記憶媒体，特に重要情報が含まれている媒体の処分に関する手順を確立すること」という対策が提示されたときに，

1)現在同様の対策を実施中
2)必要性を認めるが現在未実施
3)対策に該当する情報資産が存在しないため不要

の中から一つに判断することである。

表１　危険度および頻度の入力値

レベル	危険度	頻度
0	無し	発生しない
1	経営にほとんど影響しない	数年に１度発生する
2	経営にやや影響する	年に1度発生する
3	経営に多少の影響がある	月に１度発生する
4	経営に大きな影響がある	週に１度発生する
5	経営に致命的影響がある	頻繁に発生する

このような処理プロセスを採用したのは，近年の企業間で情報資産に大きな相違は無いものと考えられるため，情報資産毎に対策を作成しなくても，対策基準について大きな差異が生じないと考えたためである。さらに，本システムの主な対象ユーザは中小企業の情報システム担当者であり，情報資産のほぼ全てを情報システム担当者が把握している，すなわち本システムを利用してポリシー作成を行う場合に必要な判断が可能と考えたためである。これにより，情報資産の特定に必要とされた時間を割愛でき，ポリシー作成に要する時間の大幅短縮が期待される。なお，3)の不要に分類された対策のデータは，この段階で削除され，以後の処理では扱われない。

３．２．２　本システムでのリスク分析

次にリスク分析を行うが，これは対策とは独立させて脅威毎の危険度(事件，事故が発生した場合の損害)と頻度(事件，事故が発生する頻度)を入力するプロセスである。そして，この危険度と頻度を用いて，対策個々の重要度を算出する。ここで，危険度および頻度ともに表 1 のように 6 段階のレベルで入力する。

例えば，「モバイルパソコン・記憶媒体等の社外持ち出しによるデータ紛失・盗難」という脅威に対して会社経営へ多少の損害があり，発生頻度が年に 1 度程度ならば，それぞれ 3 および 2 を入力する。

危険度および頻度の入力値はともにユーザの主観に左右されるため絶対値としては意味がないが，同一ユーザが一貫して判断，入力することにより，相対値として意味を有するものと考える。

脅威は対策とは独立しているが，システム内では関連づけられている。これは，ユーザが対策の順位付けを行うことは困難なため，個々の脅威に対するリスク分析を行うことによって，対策の順位付けを行うことが出来るようにするためである。そして，このようにして得られた対策の重要度によりすべて

の対策を再度見直し，最終的なポリシーが完成する。

また，このリスク分析には，上述した対策基準の振り分けの確認の意味も含まれる。すなわち，振り分けされた対策基準(3．2．1 で不要と判断した対策を除く)を客観的に評価することがリスク分析で可能となる。

4．システムの評価

本システムの評価は，8 企業の情報システム担当者の協力を得て実施した。評価項目は，作成終了までの所要時間，作成されたポリシーの質である。

4．1　所要時間の評価

ポリシー作成に要する総所要時間の平均値は，98 分であった。これは，一般的なポリシー作成時間に比較して十分低い数値であり，当初目的を達成できた。ただし，ここでいうポリシー作成時間とは，対策基準および実施手順の作成までの時間である。基本方針の作成は，対策基準および実施手順作成用のシステムとは別システムである。基本方針の作成に要する時間は，平均で 10 分以下と推定される。

4．2　ポリシーの質の評価

作成されたポリシーが企業に対してどの程度適合しているか，というポリシーの質の評価が必要である。評価には，作成した企業が現有するポリシーと比較する，または本システム使用後に実際に他の方法でポリシーを作成してもらいそれと比較することが最善である。しかし，実験参加企業でポリシーを保有しているところは無く，また数ヶ月かけてポリシーを作成してもらうことは困難であった。そのため，工業試験場の職員を被験者とし，工業試験場の現有ポリシーで比較実験を行った。なお，工業試験場のポリシーは，コンサルタント企業と石川県庁が 6 箇月以上の時間を要して作成されたポリシーを基に，工業試験場業務の特性などを加味して構築したものである。

ポリシーの比較には，JIS の項目による方法を用いた。システムで作成されたポリシーは，JIS の項目および表現に準拠している。そこで，既存のポリシーを JIS の項目で整理し双方を比較した。それにより，作成されたポリシーがどの程度現有ポリシーを含むか，というカバー率での評価を行った。その結果，　3 名での平均で 96.2%となった。

本システムの構築目的は，容易にポリシーを作成することであった。併せて，高いカバー率となった結果は，本システムの質的な実用性も十分に示したと考える。

5．結　　言

本研究で開発したポリシー作成支援システムは，ポリシーを短時間で作成することを可能にした。

作成したシステムについては，8 企業のシステム担当者の協力を得て評価実験を行った結果，2 時間以下で作成出来ることを確認した。さらに，作成されたポリシーのカバー率も十分高く，作成されたポリシーの質的実用度が高いことも確認できた。

また，本システムの評価実験において，全てのユーザがポリシーを作成できた。これにより対象ユーザである中小企業の情報システム担当者が本システムを使用することによりポリシーを作成できることを確認できた。

さらに，工業試験場の事業である企業参画型研究として㈱石川コンピュータ・センター(以下，ICC という)と共同研究を実施した。これにより本システムを用いたセキュリティポリシーの作成から，ICC 製のセキュリティ対策製品を用いた実際の対策実施までを総合的に支援出来る，セキュリティソリューションが実現できた。

今後の課題としては，ユーザビリティ向上のために，用語や操作に関するヘルプ機能を充実させ，FAQ(Frequently Asked Question)の機能を持たせることが考えられる。

謝　　辞

本研究を遂行するに当たり，終始適切なご助言を頂いた金沢大学工学部教授木村春彦氏に感謝します。また，システムの検証実験に御協力頂いた 8 社の担当者に感謝します。

参考文献

1) 中野明ほか著.秀和システム.よくわかる最新 ISMS Ver.2 の基本と仕組み

2) 白濱敏朗.2時間でわかる図解ISO17799/ISMS 早わかり情報セキュリティの国際規格.中経出版.

3) JISX5080：2002（ISO/IEC17799）情報セキュリティマネジメントの実践のための規範