情報セキュリティポリシー作成支援システムの開発

電子情報部　○林　克明　上田芳弘

１．目　的

近年，企業や自治体の業務処理に多くの情報システムが使用され，今後もますます利用が広がると予想される。しかし，そのことは情報システムに対する脅威がそのまま社会の脅威につながるということを意味する。そのため，情報セキュリティ対策が必要であり，この指針となる情報セキュリティポリシー(以下，ポリシー)が注目されている。ここで，ポリシーとは組織における情報システムの維持，運用に関してソフトウェア及びハードウェア両面に対する対策および，利用者の教育に関する規定なども含めて成文化したものである。しかし，その作成には多くの時間と費用を要し，そのことが企業の負担になっている。そこで，本研究では，企業のポリシーの原案となるものを容易に短時間かつ廉価で作成するためのシステムを開発することを目的とした。

２．内　容

2.1 情報セキュリティポリシーの作成とシステムの特徴

ポリシーは3階層に分けられる。階層の最上位には行動指針の宣言文である基本方針が位置し，次が基本方針を具体化した対策基準があり，最下層に行動マニュアルである実施手順が位置する。本システムでは上記3階層の作成を可能としていることが特徴の一つである。

本システムの開発目的は，作成時間の短縮である。従来のポリシーの作成方法は，専門担当者がその知識と技能，経験を参考にして，組織の情報資産などに基づいて作成するため2週間から2ヶ月程度かかる。その作成プロセスの流れは，図1左図に示すように，1)情報資産の特定，2)情報資産毎のリスクの列挙，分析，3)リスク分析結果に応じた対策を検討し体系化してまとめる，という流れになる。ここで，情報資産とは企業が所有するコンピュータや顧客データ，売り上げ情報，ドキュメントなどといった情報関連の資産である。また，リスクとは情報資産に危害を与える原因となる事象を指す。また，ポリシーの作成を社外のコンサルタント会社に依頼する場合，数百万円程度の費用がかかるとされている。

それに対して本システムの作成プロセスの特徴は，図1右図に示すように，1)情報資産にかかわらず汎用の対策をユーザに順次すべて提示し，その要否を判断させる，2)対策とは独立させてリスク毎の危険度(事件事故が発生した場合の損失)と頻度(発生する度合い)を入力，3)危険度と頻度から1)の対策の重要度を算出してポリシーを決定する，という流れになる。上記のように，本システムでのポリシー作成方法は従来方法とは逆の流れである。これは，近年の企業間における情報資産に大きな相違はないと考え，情報資産毎に対策を策定しなくても対策基準において大きな差異は無いと仮定したからである。この結果については，次節で述べる。また，本システムではリスク分析を対策とは独立して行うが，リスクと対策

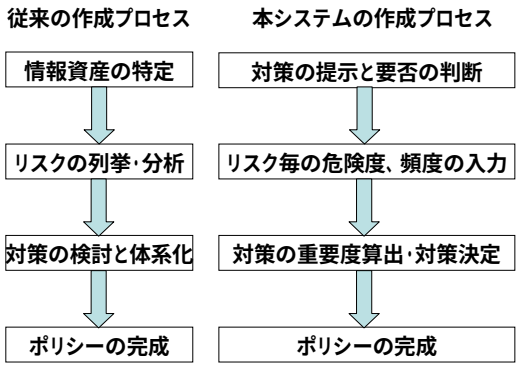

図１　セキュリティポリシーの作成プロセス

は相互に関連付けを行っており，情報資産や対策を考慮しなくてもリスク分析を行うことで自動的に対策の重要度が算出される。

2.2 システムの評価結果

作成したシステムを8企業の情報システム担当者が使用して評価結果を得た。システムは，第1版とそれを改良した図2に示す第2版があり，それぞれ4社ずつで評価した。第2版における改良点はユーザインターフェースとデータ量である。第1版はExcelのマクロ機能を利用していたが，第2版はWebアプリケーションへ移行し，Webブラウザ上での操作となる。さらに，この第2版でWebアプリケーション化したことによって，インターネットを利用して広く公開することが可能になる。また，対策基準データは62から132に，リスクデータは43から54に，実施手順データは375から500に増加させ再構築した。とくに対策基準のデータは第2版を作成するにあたりJISのセキュリティ規格のX5080の項目をカバーできるようにした。

ポリシー作成にかかる時間は平均98分であった。すなわち1日でポリシーを作成するという当初の目的は達せられた。また，本システムで作成されるポリシーの質を既存ポリシーとの一致率(カバー率)という指標で評価した。しかし，ポリシーをすでに保有している企業は無かったため，石川県庁のポリシーを対象として工業試験場職員による評価実験を実施した。その結果，第1版ではデータのカバー率が55%であったが，第2版では96%をカバーすることができた。すなわち，前節での仮定が確認されたといえる。さらに3社にはアンケートによる定性評価を実施した。そして，1)項目内容に難しい点がある，2)最初の対策基準の選定で作業ストレスを感じやすい，3)操作方法はわかりやすい，4)本システムは有用である，5)本システムを使用することによりポリシーを作成するための基礎知識及び手順を修得できた，との回答を得た。ここで，1)，2)に対しては，本システムにはヘルプ機能などがなく，使用に当たっては筆者が操作アシストを行う必要があった。そこで，広く使用してもらうためには，ユーザインターフェースをより使いやすいものとし，ヘルプ機能及びFAQ(Q&A事例集)の機能が必要だと考えられる。

3．結　果

ポリシー作成の時間を短縮することを目的にポリシー作成支援システムの第1版を開発し4社からの評価結果を基に，第2版を作成することができた。さらに，第2版を別の4企業が使用した実証実験の結果を以下にまとめる。

(1) ポリシー作成時間の短縮に効果があった。

(2) カバー率の高いポリシー作成に本システムは有用であった。

(3) より利用者が使用しやすいように，ヘルプ機能やFAQ機能が必要である。

最後に，実験にご協力頂いた8企業に感謝します。

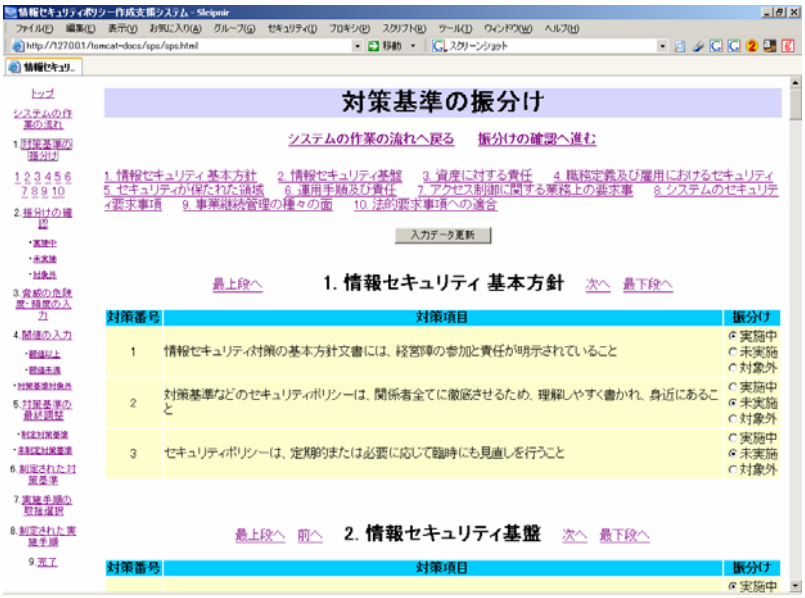

図２　作成支援システムの画面例