企業グループの情報セキュリティ対策

－グループセキュリティ対策の実践－

アブストラクト

１．背景

インターネットの普及により、情報漏洩、ホームページ改竄、コンピュータウィルス被害などは、一般的なニュースとして取り扱われ、情報セキュリティ対策への関心が高まっている。

企業においても、企業間電子商取引、電子メールなどの利用拡大により、情報セキュリティ対策が重要になっている。一度セキュリティ障害が発生すれば、業務の停止や復旧コストなどの直接的なダメージ以外に、企業イメージのダウンや株価下落など信用の失墜による２次的ダメージが発生する。

また最近、システムダウンや個人情報漏洩などの不祥事が多発している。グループ本社名やグループ名で報道され､原因や責任の所在に関わらず､グループ全体の信用失墜につながっているケースが多い。

２．情報セキュリティに関する現状

２．１　情報セキュリティへの取り組み（%）（2002 年調査データ N+I Network Guide 誌）

会社規模	経営課題として認識	システム部門が対応	ポリシー導入
30 人未満	9.8	7.2	11.1
100 人未満	11.9	15.0	15.0
300 人未満	16.2	28.1	22.7
1000 人未満	20.8	38.1	29.2
1000 人以上	43.0	34.5	51.5
計	20.3	24.6	24.8

２．２　セキュリティマネジメントの認知度（%）（2002 年調査データ N+I Network Guide 誌）

会社規模	熟知し導入済み	導入検討中	知らない
30 人未満	3.7	4.9	42.4
100 人未満	7.9	9.9	34.4
300 人未満	7.6	13.0	28.6
1000 人未満	11.9	17.9	26.8
1000 人以上	27.3	16.4	23.9
計	11.4	11.0	36.1

２．３　セキュリティポリシーの内容（%）（2002 年調査データ N+I Network Guide 誌）

	環境・物理	教育・訓練	通信・運用	資産管理	法的準拠
導入済	32.9	24.5	34.3	19.5	18.1
導入予定	16.9	19.4	18.0	14.5	17.8
検討中	9.9	13.2	9.6	15.3	13.2
導入予定無し	7.4	9.5	6.4	9.1	8.7
わからない	32.9	33.4	31.7	41.6	42.2

３．本分科会の問題意識と研究方針

上記調査データから、以下のことが読み取ることができる。

・ポリシー導入率と認識率には相関があるが、システム部門主導でポリシーを策定しているケースがまだまだ多い。

・セキュリティ対策は継続的な改善サイクルが必要であるにも関わらず、セキュリティマネジメント手法の認知度が極めて低い。

・ポリシーを導入しているにも関わらず、「わからない」という回答が極めて多い。

本分科会は、システム部門またはシステム子会社などに属するメンバーで構成されている。我々の果たすべき役割は、既存のシステム技術分野のみならず、システムの活用や定着およびより上位の経営課題や戦略への参画が求められている。本分科会では、以下の研究方針に基づき研究を実施することとした。

・「ソリューション」や「システム」の適用を研究の主眼から外す
・「仮想企業グループ」での実践シミュレーションを実施する
・国際標準・国際基準を適用する

４．研究内容と成果

我々は、分科会を通じて、以下の概念を明確にし、グループ経営におけるセキュリティ対策の実践シミュレーションを実施した。

(1) ポリシーの重要性について

ポリシーとは、共通ルールの集まりである。ポリシーが明確に定義され認知されていれば、個人の勝手な判断によるリスクを低減することができる。ポリシーを継続的に改定することで、リスクは企業レベルで低減されることになる。

(2) 情報セキュリティポリシーの重要性について

企業における資産は、「人」「もの」「金」に加え、「情報」「信用」が重要視されている。ＩＴにより情報は活用度を増し、資産価値を増大させるが、ＩＴによって信用も失うこともある。ＩＴでのセキュリティ対策は必須であるが、それを支えるのは、ポリシーであることは言うまでもない。どのような管理をするべきかを決めるのはポリシーであり、それに準じたセキュリティ製品を選択しなくてはならない。

(3) 情報セキュリティ対策を推進するには

ＩＴの発達により、リスクは確実に分散し、管理が困難かつ複雑になっている。セキュリティ対策を実施する際、脅威の分析が必須であるが、情報の持ち出し、改ざんなどの方法は、従業員であれば簡単に行える。結果としての脅威は、イメージダウンや信用の失墜による取引停止、社会的制裁（株価下落）など企業の存亡を揺るがしかねない。これは明らかに経営課題であり、経営の脅威である。もはや、情報セキュリティ対策に経営層の参画は不可欠なのである。

(4) グループ経営時代に対応するには

経営層への動機付け、グループセキュリティポリシー策定プロジェクトの実践シミュレーションを実施した。労務、法務、人事、システムなど各部門の連携と関係会社との調整、統合など、我々では簡単に解決できない多くの複雑な課題があることを再認識させられることとなったが、以下のヒントを得ることができた。

a. グループ経営における情報セキュリティ対策のあり方
b. グループ統制として本社の果たすべき役割

５．結論

グループ経営における究極の課題は、経営資源として「人」「もの」「金」「情報」「信用」を正しく捉え、シナジー効果を増大させることと考える。ダイナミックなグループ内連携、共同事業、新規事業創出を実施できるグループを形成できるかが課題ではないだろうか？グループとしての競争力を維持・増大させるために、グループ共通のコンプライアンスの確立、情報取り扱いの標準化（グループセキュリティポリシーの策定)、グループ全体の信用の維持・増大（グループでの PDCA 確立)、ＩＴ武装による情報の高度活用と競争力強化とを前向きに本テーマと捉え、立ち向かって欲しい。

本報告書を参照いただき、

・コンサルティングの事前シミュレーション
・情報セキュリティ対策、体制の見直し、グループポリシー策定の手引き
・経営課題としての認識
・経営層への提言

などに活用頂き、経営層、システム部門の各ポジションの方が、前向きに情報セキュリティ対策を捉えていただければ幸いである。