情報セキュリティ対策
ベンチマーク活用集

3章 情報セキュリティ対策ベンチマークからISMS認証取得へ

1 情報セキュリティマネジメントシステムの構築

1 J社の情報セキュリティ対策上の課題

J社では、各種のセンターサービス業務を行っており、アウトソーシングサービス、特にＡＳＰサービスなどが伸びている。これらのサービスは、顧客の基幹業務に大きな影響を与えるため、サービス業務の信頼性、安全性などを確実なものとしなければならなかった。しかしながら、外部委託先の情報セキュリティ対策状況の把握が不十分であり、顧客からの要求事項に対応できるかどうか不安があった。また、他社のデータセンターが顧客情報の漏えい事故を起こすなど、社会的信用にも大きな問題となっていた。J社では、2005年より情報セキュリティ対策ベンチマークを利用して、全社的に情報セキュリティ対策の実態を時系列で把握することとしていたが、このようなセキュリティ事故発生を契機に社内の情報セキュリティ対策を見直すこととなった（**図3.1**参照）。

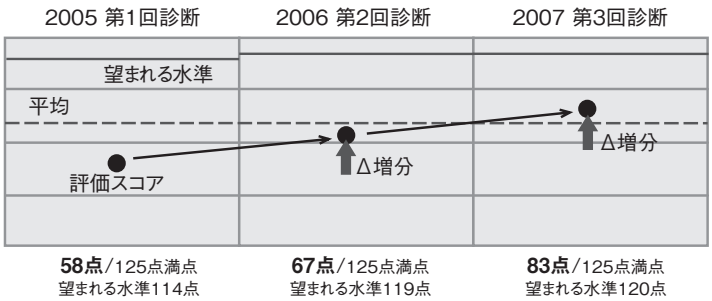

図3.1　情報セキュリティ対策ベンチマークによる時系列比較

その結果、情報セキュリティ対策は技術だけではなくそれをどう運用・管理するか、社内の制度・ルールなどが重要であると認識させられた。特に、情報セキュリティに対する危機意識が低いために起因する人的なミスを無くすためには、現場レベルにおける個人それぞれの情報セキュリティに対する認識を向上させることが重要であり、繰り返して教育・訓練活動を実施する必要があった。

このような状況から、情報セキュリティを確保するための企業の経営基盤として情報セキュリティマネジメントシステム（ISMS）の導入を検討することとなった。さらに、ISMS適合性評価制度の認証基準であるJIS Q 27001の要求事項に適合させることによって、顧客に対して組織の情報セキュリティ対策への取り組み姿勢をアピールすることにつながるとともに、情報セキュリティを維持・向上させる仕組みとしてISMS認証取得は有効と判断したからである。

2 ISMS導入の準備

▶情報セキュリティ対策推進会議の設置

J社では、情報セキュリティ管理活動や関連する規程は存在するが、情報セキュリティに関する統一的な活動が不足しているとの認識から、データセンター事業部部長を中心として、「情報セキュリティ対策推進会議」を設置し、全社的な情報セキュリティ対策について検討することとした。その際、JIS Q 27001の要求事項のほか、ISMSの実践規範であるJIS Q 27002、及びJIPDEC発行のISMSユー

ザーズガイド（平成18年12月発行）を参考にした。

その結果、データセンター事業部部長は、情報セキュリティマネジメントの仕組みを確立することの重要性を認識した。データセンター事業部部長が、検討成果を社長に報告した結果、「会社として情報セキュリティマネジメントの仕組みを確立するように」との指示が下った。検討成果の報告の際に、データセンター事業部部長は、社長に対して、情報セキュリティマネジメントの仕組みを確立するためには、各部との連携が不可欠である旨を説明し、各部門からの支援とコンセンサスを得る必要性から、「情報セキュリティ対策推進会議」を設置した。関係する各部門のメンバーを集めて検討することについては、取締役会の承認を得た。「情報セキュリティ対策推進会議」は、運用部門担当の役員（常務取締役）が責任者となり委員（関連部署の部長クラス）を任命し、通常の組織運営に組み込んだ。

「情報セキュリティ対策推進会議」のメンバー（部門）を**表3.1**に示す。

表3.1　情報セキュリティ対策推進会議のメンバー（部門）一覧

部門名	役　割	参加メンバー	選定理由
総務部	ルールを決める側として参加	総務課長 人事課長	・全社規程類の発行の管理責任部門である。 ・人の採用の責任部門である（外注を含む）。 ・社内のトラブル案件の相談窓口であり、情報セキュリティに関する対応も今後必要となる。 ・施設面に責任を負う部門である。 ・プライバシーを守るべき部門である。 ・懲罰等に関する部門である。 ・教育に関する部門である。
内部監査室	ルールを決める側として参加	監査室長	・内部監査を行う部門である。 ・情報セキュリティ監査の主管部門となる。
法務部	ルールを決める側として参加	法務部長	・契約関連及び法務面に関連する事項を担当する部門である。
データセンター事業部	ルールを決める側として参加	事業部長 A課長 B課長 C課長	・事業所の運用管理に責任をもつ部署である。 ・システムの企画・開発・運用の管理責任部門であり、情報システムのセキュリティ対策を実施している。 ・事業所内のLANに責任を負っている。

▶検討すべき課題と実施方針

「情報セキュリティ対策推進会議」における検討の結果、JIS Q 27001の要求事項に対して、下記の検討すべき課題について、その対策を実施する方針案が取締役会に報告され、承認された。

(1) ISMS基本方針の策定及びISMS適用範囲と境界の定義
(2) 情報セキュリティに関する管理組織の整備
(3) 情報セキュリティ基本方針に関する規程類の整備
(4) リスクアセスメント方針と手順の策定及びリスクアセスメントの実施
(5) 情報セキュリティインシデント管理
(6) 事業継続計画の作成
(7) 法的要求事項の順守
(8) 情報セキュリティに関する教育・訓練規程の策定とその実施
(9) 情報セキュリティ対策の運用及び記録
(10) 内部監査または情報セキュリティ監査に関する規程の策定とその実施
(11) マネジメントレビュー

(1)～(11)の課題に対する対策の実施については、3 ～ 13を参照のこと。

3 ISMS基本方針の策定及びISMS適用範囲と境界の定義

ISMS基本方針は、事業上の要求及び法的要求事項やリスクアセスメントなどから導かれる情報セキュリティへの要求事項を考慮し、リスクマネジメント環境、ISMSを確立し維持する組織環境、情報セキュリティの全般的な方向性及び行動指針を確立するためのものであり、情報セキュリティ基本方針のさらに上位の方針を示すものである。

そこで、「情報セキュリティ対策推進会議」では、その最初の作業として、ISMS基本方針を策定し、取締役会の承認を得た。

ISMSの適用範囲とは、合理的なマネジメントシステムの構築が可能で、外部とのインターフェースが明確にできる範囲のことであり、そのため、事業、組織、所在地、資産、技術の特徴の見地から、ISMS適用範囲及び境界を定義する必要がある。

適用範囲については、情報セキュリティマネジメントの構築を行う際に、業務手順の変更が必要となる場面も想定されるため、第一ステップとして機動的に業務手順の変更等が行える特定の部門を対象とした。将来的には、情報セキュリティマネジメントの実践を行った結果をもとに全社的な体制へと拡張することとした。具体的には、「情報セキュリティ対策推進会議」が以下の2点を考慮してISMSの適用範囲の原案を作成し、取締役会にて承認された。

(1)会社にとって情報セキュリティが特に重要な資産を含むデータセンター事業部内の業務を適用範囲とする。また、データセンター事業部の情報セキュリティについて重要な関わりを持つ部署、データセンター事業部の業務に関連する部分についても適用範囲とする。

(2)組織の活動と情報セキュリティの関係から、守るべき資産についてどのように関係するかを考慮し、適用範囲内の情報セキュリティマネジメントを構築することで一定の効果をあげられるところを適用範囲とする。

今回定めたISMS適用範囲を次頁 **表3.2**に示す。

4 情報セキュリティに関する管理組織の整備

情報セキュリティに関する管理組織及び管理責任者として情報セキュリティ対策室及び情報セキュリティ責任者を設置、任命することとした。また、情報セキュリティ対策室の上位組織として、組織全体のリスクを管理する危機管理室を新たに設置した。ドキュメントとしては「情報セキュリティに関する組織規程」に詳細を記述することとした。J社の社内組織図は、**図3.2** (P41)に示す通りである。

▶ 情報セキュリティ対策室

情報セキュリティ対策室は、情報セキュリティに関する検討・承認及び重要事項について危機管理室に事案を発議する組織としての機能及び情報セキュリティに関する各部門の調整を行う機能を持つ。

(1)情報セキュリティ対策室の責務

①情報セキュリティ基本方針のレビュー・改定案作成

②情報セキュリティ関連各種ガイドラインの策定

③情報セキュリティリスク評価の承認

④情報セキュリティリスク管理の実施

⑤情報セキュリティ事故の統括管理
⑥事業継続に関する課題の監視及び報告
⑦情報セキュリティに関する各部の指導
⑧情報セキュリティに関する社外組織との連携
⑨その他、必要に応じ、情報セキュリティに関する重大な意思決定及び危機管理室への起案を行う

(2)情報セキュリティ対策室長

情報セキュリティ担当役員（CISO:Chief Information Security Officer相当）を情報セキュリティ対策室長とした。情報セキュリティ対策室のメンバーは、適用範囲内の各部門の部門長が兼任し、さらに事務・運営要員として専任スタッフを置くこととした。

表3.2　適用範囲

No.	カテゴリ	対　象	内　容	関連する文書
1	事　業	データセンター事業部の行う事業全体に関する情報セキュリティマネジメント	・データセンター事業 ・運用監視事業 ・運用委託事業	ISMSの文書
2	組　織	データセンター事業部	業務を行う部門	組織図 職務分掌
		情報セキュリティ対策室	情報セキュリティ協議会及びクロスファンクショナル協議会の機能を持つ組織	
		総務部	以下の業務を範囲とする。 ・人事採用（外注含む） ・施設管理 ・従業員教育 ・その他データセンター事業部（大手町）の情報セキュリティマネジメントに関わる業務	
		法務部	以下の業務を範囲とする。 ・法律に関連する業務 ・データセンター事業部の契約に関する業務 ・その他データセンター事業部の情報セキュリティマネジメントに関わる業務	
		内部監査室	以下の業務を範囲とする。 ・データセンター事業部のセキュリティ監査に関する業務 ・その他データセンター事業部の情報セキュリティ管理に関わる業務	
3	所在地	大手町事業所	データセンター事業部	フロアレイアウト（空調ダクト等の設備の構成も含む） 電源・電話の配線図
		本社（右部分）	情報セキュリティ対策室 総務部 法務部 内部監査室	
4	情報技術	ハードウェア・ソフトウェア	大手町事業所内で管理されるハード・ソフトウェアを適用範囲とする。	機器構成図 ネットワーク構成図
		ネットワーク	大手町事業所からの対顧客・対インターネット接続のルータを含む。	
5	資　産	上記1～4に所属するすべての情報資産を適用範囲とする。 各部の作成する資産管理目録にて詳細が定義される。		資産管理台帳

▶情報セキュリティ責任者及び情報セキュリティ管理者

適用範囲内の各部門に情報セキュリティ責任者を任命することとし、各部門の部門長を情報セキュリティ責任者に任命した。また、情報セキュリティ責任者を補佐する情報セキュリティ管理者（課長職相当）を各部門から2名任命した。

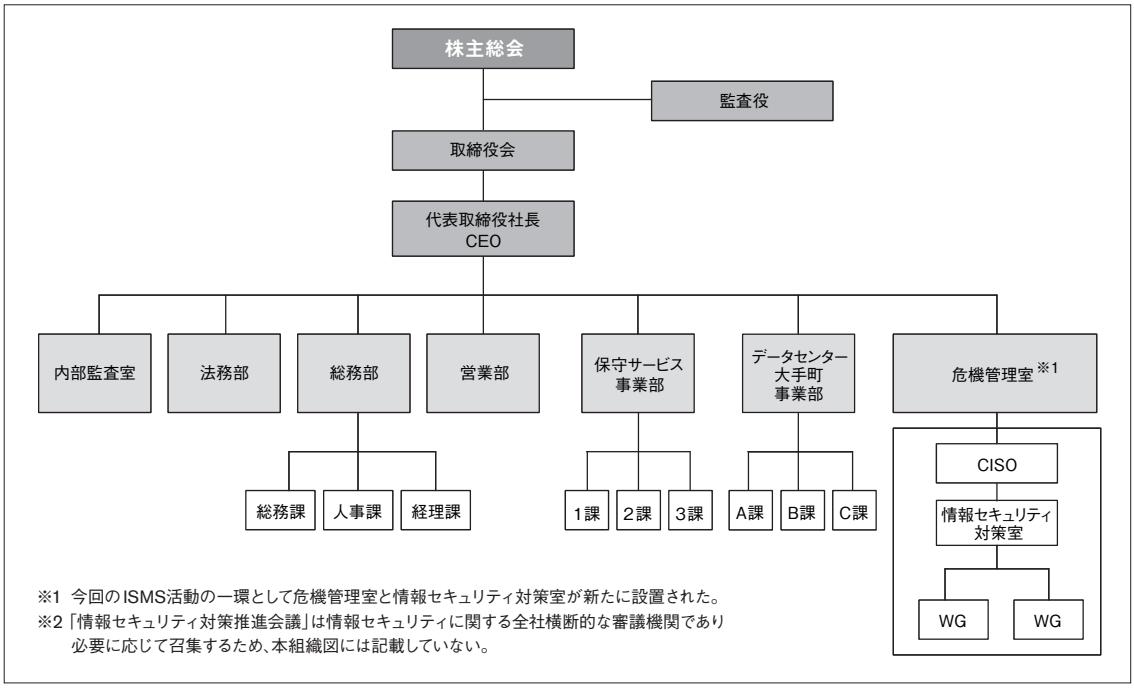

図3.2　J社の社内組織図

5 情報セキュリティに関する規程類の整備

情報セキュリティに関する規定類の整備に関しては、現在の情報セキュリティ基本方針及び既存の情報セキュリティに関連する各種の文書を活用した。さらに必要なドキュメントとして、適用範囲内向けの各種情報セキュリティガイドラインを作成し、それに従ってルール・手順書等を作成した。情報セキュリティ基本方針については、J社として考えるべき情報セキュリティ上のポイントを、現場に理解しやすい表現とすることで、現場への浸透を図ることを重視した。

▶情報セキュリティ関連のドキュメント類

情報セキュリティ基本方針に基づくドキュメント類は次の通りである。

(1)情報セキュリティ基本方針

情報セキュリティの目的とその考え方等について定義した文書である。当社の情報セキュリティに関する全社的な規程として存在する。

(2)情報セキュリティ関連全社規程

全社規程は、情報セキュリティに関連するか否かにかかわらず、その適用や周知について全社員が対象となっている規程の総称である。情報セキュリティ関連全社規程は、適用範囲内の資産に関連して情報セキュリティを守る管理・対策として適用可能なものを、情報セキュリティ対策室が選択したもので、情報セキュリティ基本方針から引用される規程である。なお、今回のISMS活動の一環として新たに危機管理室や情報セキュリティ対策室が設置されたが、これらの組織に関しては、「情報セキュリティに関する組織規程」に詳細を記述した。

(3)情報セキュリティガイドライン

情報セキュリティマネジメントを行うために必要であり、かつ上記(1)、(2)に含まれないものについて、対策の指針を示すものとして新たに適用範囲内のみの情報セキュリティガイドラインとして作成する。

(4)ルール・手順書等

(1)～(3)に基づいて作成され、部門内のルール及び手順書として作成する。

情報セキュリティ基本方針に基づくドキュメント体系を**図3.3**に示す。

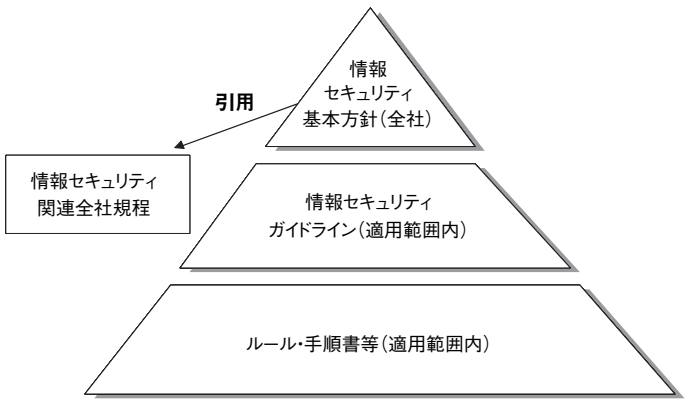

図3.3　ドキュメント体系

ドキュメント体系に対応するドキュメントの例示を**表3.3**～**表3.7**に示す。情報セキュリティ関連全社規程とは、J社に既に存在する情報セキュリティ関連規程である。

表3.3　情報セキュリティ基本方針(全社)

No.	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティ基本方針	全社の情報セキュリティ 基本方針	取締役会	役員・従業員等

表3.4　情報セキュリティ関連全社規程（全社）

No.	ドキュメント名	内容	承認者	実施責任者
1	文書管理規程	文書管理に関する規程	取締役会	従業員等
2	危機管理室規程	危機管理室の役割、メンバ及び責務に関する規程		危機管理室
3	営業秘密管理規程	不正競争防止法に対応し、企業における営業秘密を管理するための規程		役員・従業員等
4	内部監査規程	内部監査に関する規程		内部監査室
5	就業規則	社員の就業に関する規則		従業員等
6	システム開発規程	システム開発に関する規程		関連部門
7	契約締結に関する規程	ユーザと契約を締結する際の規程		
8	データセンター内ネットワーク管理規程	データセンターの有線、無線LANの構成管理等		
9	データセンターの環境整備に関する規程	耐震設備、耐火設備、電力供給、電話回線の維持等に関する規程		
10	顧客情報保護規程	顧客情報保護に関する規程		役員・従業員等
11	携帯電話の使用に関する規程	携帯電話の使用に関する規程		

表3.5　情報セキュリティ関連規程（適用範囲内）

No.	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティに関する組織規程	情報セキュリティ管理体制及び責任に関するガイドライン	取締役会	役員・従業員等
2	リスクマネジメント規程	リスクアセスメント及びリスク対応実施に関するガイドライン	危機管理室	情報セキュリティ対策室及び関連部門

新たに作成する必要がある情報セキュリティガイドライン（適用範囲内）及びルール・手順書等（適用範囲内）の例示を**表3.6**～**表3.7**に示す。

表3.6　情報セキュリティガイドライン（適用範囲内）（抜粋）

No.	ドキュメント名	内容	承認者	実施責任者
1	情報セキュリティ教育・訓練ガイドライン	情報セキュリティ教育に関するガイドライン	情報セキュリティ対策室長	総務部及びデータセンター事業部の情報セキュリティ責任者
2	情報セキュリティ監査ガイドライン	情報セキュリティ監査の計画実施及び報告に関するガイドライン		内部監査室の情報セキュリティ責任者
3	情報セキュリティ事故管理ガイドライン	情報セキュリティ事故管理に関するガイドライン		各部の情報セキュリティ責任者
4	コンプライアンスガイドライン	法律等への準拠に関するガイドライン		
5	事業継続計画作成ガイドライン	事業継続計画作成に関するガイドライン		データセンター事業部の情報セキュリティ責任者
6	物理的アクセス管理ガイドライン	入退室に関するガイドライン		総務部及びデータセンター事業部の情報セキュリティ責任者
7	論理的アクセス管理ガイドライン	オペレーションシステム、アプリケーションシステム、データベース等の論理的アクセスを設定する際のガイドライン		

表3.7　ルール・手順書等（適用範囲内）

No.	ドキュメント名	内容	承認者	実施責任者
1	ルール・手順書等（ここでは詳細は記述しない）	**表3.6**のドキュメントに従って各部門で作成する	情報セキュリティ対策室長	各部の情報セキュリティ責任者

6 リスクアセスメントの実施

▶リスクアセスメント方針と手順の策定及び実施部門

(1) リスクアセスメントの方針と手順の策定

リスクアセスメントの目的は、ISMSの適用範囲において特定した資産に対して、情報セキュリティに与える影響を考慮し、実際に情報セキュリティマネジメントの対策を講じる対象となるリスクを洗い出すことにある。リスクアセスメント方針及びその手順は、ISMS基本方針に従って、資産価値、脅威、ぜい弱性等を評価するための構造、仕組みとして定義し、文書化する必要がある。

リスクアセスメントは、リスク分析からリスク評価までの全てのプロセスと定義される。リスク分析においては、それぞれの資産に対する脅威とぜい弱性からリスクのレベルを算定し、リスク評価ではリスク受容基準及びリスク受容可能レベルを決定する。そして、リスク評価の結果に基づきリスク対応を実施することとなる。

J社では、ISMSユーザーズガイドを参照し、自社に適した方式を検討した。その結果、ベースラインアプローチと詳細リスク分析手法に基づき、資産とそれに関連する脅威をリストアップし、リスクアセスメントを実施する方法を採用することとした。

ベースラインアプローチは、大きく分けると「ベースラインの決定」と「ギャップ分析の実施」の2つの手順で実施される。ベースラインは、情報セキュリティ管理について、組織の定める独自の対策基準であるが、J社では、この基準にJIS Q 27001付属書Aの管理策を準用することとした。また、ギャップ分析の際は、情報セキュリティ対策ベンチマークの25項目の質問と対策状況を把握することにより、ギャップ分析結果として活用することとした。

(2) リスクアセスメントの実施項目及び実施部門

リスクアセスメント実施項目と実施部門を**表3.8**に示す。

表3.8　リスクアセスメント実施項目と実施部門

No.	実施項目	実施部門	承認
1	リスクアセスメント手法の決定	情報セキュリティ対策室	危機管理室
2	情報セキュリティリスクアセスメント手順書作成	情報セキュリティ対策室	危機管理室
3	リスクアセスメント実施	データセンター事業部	情報セキュリティ対策室
4	リスク評価結果を情報セキュリティ対策室へ報告	データセンター事業部	情報セキュリティ対策室
5	リスク対応の決定（管理策の決定）	情報セキュリティ対策室	危機管理室
6	ガイドライン等の作成	情報セキュリティ対策室	危機管理室
7	基本方針及び関連規程の見直し	情報セキュリティ対策室	危機管理室
8	リスク対応より対策の決定	データセンター事業部	情報セキュリティ対策室
9	対策の実施・運用	データセンター事業部	情報セキュリティ対策室

情報セキュリティリスクアセスメント手順書や関連するガイドラインは、リスクアセスメントを実際に行う部門が実施可能なように、平易な表現で記述することとした。方針、手順、実施部門が決まったところで、第一段階としてギャップ分析を、第2段階として詳細リスク分析を行うこととなった。

▶リスク分析の実施

(1)第1段階：ギャップ分析の実施

ギャップ分析の目的は、現状の管理策の適用状況の把握にある。ギャップ分析は、一般的に推奨される管理レベルと組織の現状の管理レベルを比較し、「大きな差が認められる箇所」、「明らかに管理策の適用を必要としている箇所」を発見し、より詳細なリスク分析の実施を検討することにある。

ISMSの適用範囲で定義した資産は、すべてギャップ分析の対象である。この段階では、資産を一つひとつ個別に比較するのではなく、対象となる資産をまとめたグループを一つのまとまりと見て分析を実施することが望ましい。

JIS Q 27001の管理策の適用状況を初期段階でチェックする際に、情報セキュリティ対策ベンチマークによる診断結果をもとに、組織における管理策の適用状況、問題の所在等を、25項目の情報セキュリティ対策状況を確認したり、146項目の対策のポイントを利用して確認した。

(2)第2段階：詳細リスク分析の実施

ギャップ分析により発見された問題箇所の重大なリスクの存在を明らかにした後に、詳細リスク分析を実施した。

詳細リスク分析の対象は、ギャップ分析の結果、「基準に適合していない」、「基準に一部適合していない」と判断された箇所のみとする。そこで、ISMSが対象とする資産のうち、すでに適切な管理策が適用されていると判断された項目については、詳細リスク分析の対象から除外し、基準への適合が疑わしい項目に関連するものについて、資産ごとに詳細リスク分析を実施した。

▶リスク対応

詳細リスク分析の評価結果から、リスク受容基準を超える場合のリスク対応として、情報セキュリティ対策（選択した管理策）を実施することとなる。

J社では、「情報セキュリティリスクアセスメント手順書」に従い、データセンター事業部にてリスクアセスメントを実施した。その結果、明らかとなったリスクについて、情報セキュリティ対策室がリスク対応策の検討を行った。

リスク評価およびそれに続くリスク対応の方針は下記の通りである。

(1) 情報セキュリティ対策チェックシートを作成し、チェックシートに現状を記述し、記入者がリスクを評価する。

(2) 実現できない対策については、情報セキュリティ対策室の検討メンバーが対策チームとなり、評価の上、リスクを受容する判断をくだす。

リスク評価シート　　No.

基準目的	【基準目的の番号】
基準項目	【基準項目の内容】
当社状況	【当社にとっての該当内容】

関連する資産

番号	内容	ビジネスへの影響
A1	【該当する情報資産1】	【ABCで記入】

関連する脅威

番号	内容	備考
T1	【該当する脅威の内容】	

関連する対策

番号	内容	対策済	備考
P1	【当社における基準対策】	□ 済の場合（■）	対策状況、不備内容等

リスク

A	T	P	内容	リスク	備考
資産	脅威	未実施対策	【リスク内容】	ABCで記入	理由等

図3.4　リスク評価シート

リスクアセスメントとリスク対応は、以下の手順で実施された。

(1)情報セキュリティ対策室がリスク評価シート（**図3.4**参照）の「当社状況」、「関連する脅威」、「関連する対策」を記述する。

(2)リスクアセスメントを行う部門は、次の作業を実施する。

①「関連する資産」に、該当する資産を記述し、事業への影響を記入する。

②「関連する対策」の「対策済」欄を記入する。

③「リスク」を記入する。

④すべてのリスク評価シートに対して①～③を行った後、結果を情報セキュリティ対策室に提出する。

(3)情報セキュリティ対策室は、提出されたリスク評価シートをもとにリスク対応を行う。

▶規程類・ガイドライン及び適用宣言書の見直し

リスク対応の結果、規程・ガイドライン等の見直しが必要になる場合がある。これらの見直しについても順次行うこととした。

また、リスク対応の結果、選択した管理目的及び管理策、並びにそれらを選択した理由について見直しを行い、適用宣言書の改訂版を作成した。

リスク対応計画フォーマットを**表3.9**に示す。

表3.9　リスク対応計画フォーマット

				ISMS 管理責任者	実行責任者
管理No.	×××××××	優先順位	①		
資産		管理策		対策費用	
				想定損害額	
現状の問題点					
改善策と 予想改善効果				リスクのレベル （前）	リスクのレベル （後）

実施項目		担当者						
1								
2								
3								
4								
5								
6								
7								
8								
		確認						

7 情報セキュリティインシデント管理

情報セキュリティインシデントの発見・報告・対応及び再発防止策を速やかに行うためには、事前に情報セキュリティインシデント管理に関する手法や手順を定める必要がある。そこで「情報セキュリティインシデント管理ガイドライン」を策定し、手法と手順を詳細に記述した。また、事故が起こった際は、「情報セキュリティインシデント対策報告書」を記録として保存することとし、報告書の雛形も作成した。

通常の情報セキュリティインシデント管理の系統については、次頁 **図3.5**に示す。

▶情報セキュリティインシデントの定義と特例

(1)情報セキュリティインシデントの定義

次頁 **表3.10**のいずれかを情報セキュリティインシデントとして定義した。

(2)情報セキュリティインシデントの特例

情報セキュリティインシデントの特例となる重大な情報セキュリティインシデントについて定義し、特例については、別途「危機管理規程」にて定めることとした。

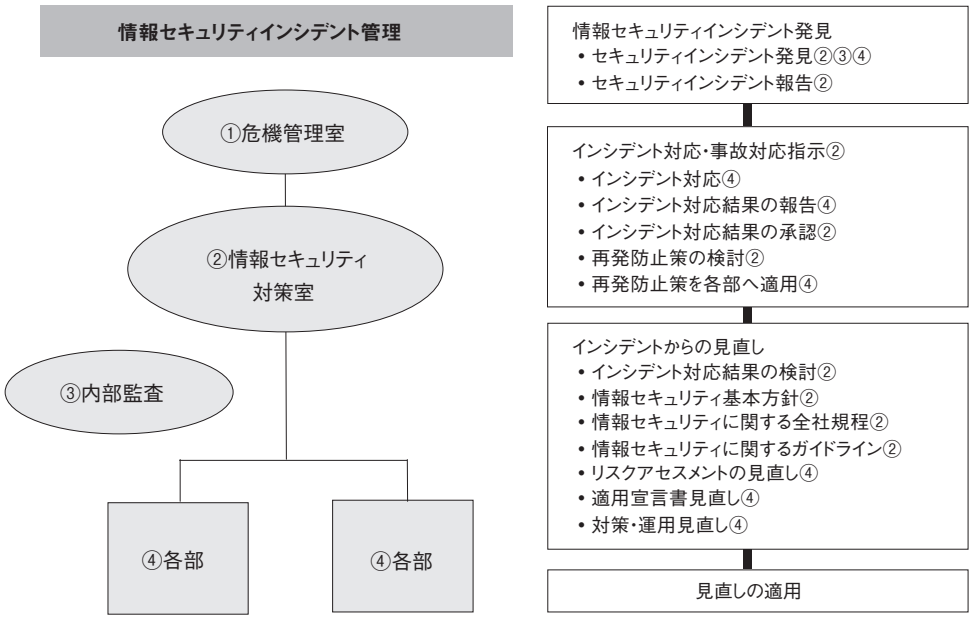

図3.5　通常の情報セキュリティインシデント管理の系統

表3.10　情報セキュリティインシデントの例示

No.	分類	内容	原因
1	業務障害	業務の継続が困難	天災、人災、公共インフラ停止、機器破壊等
2	サービス障害	正常なサービスの継続が困難	ハード・ソフト障害、スタッフの緊急入院等
3	情報障害	守るべき情報の不全	情報漏えい、情報改ざん、情報破壊等
4	セキュリティ侵害	（実害とは関係なく）情報セキュリティ対策が破られる	不正アクセス、ウィルス発生、パスワード漏洩等
5	セキュリティ障害	情報セキュリティ対策が実施されないまたは効果がない	ファイアウォール設定不備、鍵管理不備等
6	インシデントの疑い	上記1 ～ 5への重大な疑い	

表3.11　情報セキュリティインシデントの特例（例示）

No.	分類	内容	原因
1	重大事故	経営に関わる事故	大災害、事件、多くのスタッフの緊急入院、大量の顧客情報流出等

▶情報セキュリティインシデント対応

(1)情報セキュリティインシデント発生時の連絡体制

情報セキュリティインシデント発生時の連絡体制を定めておくことで、発見者は、情報セキュリティインシデントまたは情報セキュリティインシデントに関する重大な疑いがある場合に遭遇した場合に、速やかに報告することが可能になる。インシデント発生時の連絡体制は、**表3.12**のように定められた。

表3.12　インシデント発生時の連絡体制

No.	連絡元	連絡先	内容
1	発見者	所属部門の情報セキュリティ責任者	情報セキュリティインシデントの種類・状況 発見者氏名及び発見者への連絡方法等
2	所属部門の情報セキュリティ責任者	情報セキュリティ対策室長	情報セキュリティ責任者の判断で、必要時に連絡
3	情報セキュリティ対策室長		情報セキュリティ対策室長が重大事故と判断した場合、「危機管理規程」に従い連絡

(2)情報セキュリティインシデントの調査及び対応

情報セキュリティインシデントの調査及び対応は、情報セキュリティ責任者の指示により、各部門が行うものとした。ただし、緊急性のある場合はこの限りではない。

(3)情報セキュリティインシデントの記録

情報セキュリティインシデント対応後、情報セキュリティ責任者は、情報セキュリティインシデント報告書を作成し、情報セキュリティ対策室に提出することとした。

(4)情報セキュリティインシデントからの学習

情報セキュリティインシデント発生の際は、速やかな対応が必要であるが、再発防止のために、情報セキュリティインシデントより学ぶことは重要である。そこで、対策の見直しや再発防止策について以下の通り定めた。

- 情報セキュリティ対策室は、情報セキュリティインシデント報告書をもとに、情報セキュリティマネジメント及び対策に関する全社的見直しを行う。
- 情報セキュリティ対策室は、情報セキュリティインシデント報告書をもとに、再発防止策の全社への適用を検討する。

8 事業継続計画の作成

データセンター事業部が中心となり、事業継続計画を作成した。ドキュメントとしては、「業務継続計画作成ガイドライン」に事業継続の目的、枠組み、事業継続対応組織などの詳細を記述した。また、「事業所業務継続計画」には、対応手順等の詳細を記述した。

▶災害・事故の想定

事業継続計画策定にあたっては、想定される災害及び事故について、業務への影響を分析した。

- 天災　　：地震、水害、火災、落雷等
- 人的災害・障害　　：テロ、犯罪、誤用等による事故等
- 公共インフラの不全　：電力、水道、ガス、公衆回線等
- 情報セキュリティ侵害：情報の改ざん、破壊、漏えい、サービス 妨害等

▶リスクアセスメントと危機管理の実施

想定する災害・事故に対し、リスクアセスメント手順書に従ってリスクを評価し、危機管理によるエスカレーションモデルを確立することとした。

事業継続計画はJ社にとって重要度が非常に高いため、情報セキュリティ基本方針に明確に事業継続管理について記述することとなった。また、リスクアセスメントの結果明らかになった事業継続上の不備については、その改善点を検討した上で、情報セキュリティ規程へ反映させることとなった。

▶訓練及び試験の実施

実際に事業の継続を脅かすような事態が発生した場合に、現実の対応が滞りなく行われるよう、事業継続要員の訓練も必要である。そこで、「事業所業務継続訓練計画」を定め、危機管理によるエスカレーションモデルにもとづいて、訓練及び試験を実施する。訓練結果は、「事業継続訓練・試験結果」としてその記録を保存することとした。

9 法的要求事項の順守

法務部が中心となり、法的要求事項の順守プログラムを作成した。ドキュメントとして「コンプライアンスガイドライン」に枠組みや体制等の詳細を記述した。また、「法的要求事項の順守プログラム」には対応手順等の詳細を記述した。さらには、「法的要求事項の順守プログラム」に従い、各種記録を保存することとした。

▶法的要求事項の順守プログラム策定にかかわる作業

以下に、法的要求事項の順守プログラム策定にかかわる作業を列記する。

(1)関連する法規のリストアップ

法務部は、当社業務に関連する法律、条例、業界ガイドライン等（以下、法令等）の一覧を作成する。

(2)責任部門及び実施部門の明確化

情報セキュリティ対策室は、関連する法令等に対し、順守すべき責任部門を割り当て、責任部門の情報セキュリティ責任者をその責任者とする。

(3)法的要求事項の順守プログラムの作成

各法律等の責任者が法的要求事項の順守プログラムを作成する。この際、責任者は必要に応じ法務部の助言を受ける。

(4)社内規程及び契約のチェック

法務部は、社内規程及び契約について、関連法令等への準拠をチェックする。

10 情報セキュリティに関する教育・訓練規程の策定と実施

J社では、継続的な教育・啓蒙活動を重視し、すべての役員・従業員等に対し、初期及び定期的な情報セキュリティ教育を行うことを定めている。教育は、集合教育に加え、シフト勤務者、協力会社要員も多いことから、e-ラーニングを各部署単位で導入し、活用・実施することとした。ドキュメントとして「情報セキュリティ教育・訓練ガイドライン」に教育計画の策定方法、教育対象、実施に関する事項を記述した。また、「情報セキュリティ教育教材」及び「情報セキュリティ教育出席簿」を記録として保存することとした。

▶全社的な情報セキュリティ教育

全社的な情報セキュリティ教育については、総務部が担当部署となり、ISMS適用範囲内の全役員・従業員等に対する情報セキュリティ教育計画を策定し、教育の実施および実施記録の作成と保管を行うこととなった。教育は、毎年4月に定期的に行うこととし、これ以外の時期に新たに任命される役員、新たに就業する従業員等については、個別に教育を行うものとした。

教育実施時には教育受講者の記録を作成し、全役員・従業員等が教育を受講したことを確認することとした。

情報セキュリティ教育は、実施時期や実施方法により次の場合が考えられる。

(1) 初期情報セキュリティ教育

役員の新規任命時、従業員等の就業開始時に初期情報セキュリティ教育を実施する。また、ISMSの導入時に対象となる役員及び従業員等に対して情報セキュリティ教育を行う。

(2) 定期情報セキュリティ教育

役員・従業員等に対し、定期的な情報セキュリティ教育を実施する。

(3) 社内イントラによる随時の教育

情報セキュリティ教育のフォローアップとして、社内イントラにて教材を公開し、社員がいつでも参照可能な状態とする。

▶情報セキュリティ教育の内容及び教材

全社を対象とした教育内容を以下の通り定めた。

(1) 情報セキュリティに関する一般的な啓発

(2) 情報セキュリティ基本方針・全社的な情報セキュリティ関連規程及び情報セキュリティに関するガイドラインの内容の説明等

教材については、情報セキュリティ対策室が原案を作成し、総務部が教材として整理した。

▶部門による情報セキュリティ教育・訓練の方針と教育内容

部門内の情報セキュリティ教育については、各部門が担当部署となり、教育計画の策定、教材の作成、教育・訓練の実施・記録を行うこととした。

(1) 情報セキュリティ教育・訓練の対象及び実施時期

関連する各部門にて業務を行う全スタッフに対し、着任時及び定期的に情報セキュリティ教育・訓練を実施する。

(2)教育・訓練内容

教育・訓練内容を以下とする。教育マニュアルは各部門で作成する。

①業務及び情報取り扱い時のルールに関する教育・訓練

②事業継続計画実施に関する教育・訓練

③情報セキュリティ事故対応に関する教育・訓練

(3)情報セキュリティ教育・訓練の計画及び記録

部門内の全スタッフに対する情報セキュリティ教育計画を作成し、実施する。実施時には教育受講者の記録を作成し、部門内の全スタッフが教育を受講したことを確認する。

▶データセンター事業部での情報セキュリティ教育・訓練の実施

(1)情報セキュリティ教育・訓練計画

今回ISMS適用範囲と定めたデータセンター事業部では、部門内情報セキュリティ教育・訓練のための教育・訓練計画を策定した。

(2)情報セキュリティ教育・訓練の実施

データセンター事業部の部門内情報セキュリティ教育・訓練は、計画に従って順次実施した。教育・訓練の結果は「教育・訓練出席者名簿」に記録した。全社的教育及び部門情報セキュリティ教育の効果について、「教育アンケート」により出席者からアンケートを収集し、改善を行った。「教育アンケート」は記録として規定の期間保存することとした。

表3.13にデータセンター事業部の教育・訓練計画を例示する。

表3.13　教育・訓練計画

No.	内容	ドキュメント	周期
1	情報システム運用技術教育・訓練	運用手順書	1回／年
2	情報セキュリティインシデント 発見時の訓練	情報セキュリティインシデント 管理ガイドライン	1回／年
3	障害・セキュリティ欠陥発見時の 教育・訓練	障害対応 手順書	1回／年
4	業務継続に関する教育・訓練 災害発生時の連絡 ハード・ソフト障害時の切り替え バックアップからのリストアップ	事業所業務 継続計画	各項目に関する周期は業務継続計画に従う

※新規スタッフへの教育は、着任時に行う

11 情報セキュリティ対策の運用及び記録

▶情報セキュリティ対策の実施

情報セキュリティのリスク評価結果により見直された情報セキュリティ基本方針、情報セキュリティに関する全社規程／情報セキュリティに関するガイドラインをもとに、データセンター事業部にて情報セキュリティ対策を実施した。

この段階における情報セキュリティ対策ベンチマークの診断結果は、日頃の情報セキュリティ対策の実施状況をチェックし、日々の改善に役立てる場合などに活用することができる。

▶情報セキュリティ対策に関する記録の収集とチェック

情報セキュリティ対策に関する記録について、定期的にチェックを行う。利用者アクセスの管理に関する記録の収集とチェックについて、**表3.14**に例示する。

表3.14　記録の収集とチェック

No.	記録	周期	管理者	記録チェックの観点	対応するドキュメント
1	施設の予約 及び訪問者の記録	1回／月	施設管理者	予約者と訪問者の一致 不必要と考えられる訪問	物理的アクセス管理ガイドライン 入退管理手順書
2	施設内のセキュリティドア等の利用記録	1回／月	施設管理者	入室と退室の整合性 過度に頻繁な入退室	物理的アクセス管理ガイドライン
3	IDカード配布台帳 IDカード貸出し記録	1回／月	施設管理者	貸出し期限を越えた貸出し	物理的アクセス管理ガイドライン
4	情報処理機器保守記録	1回／月	システム管理者	定期的な保守の実施 臨時保守の理由	運用手順書
5	保守時のID貸出し記録	1回／月	システム管理者	マシン保守記録との一致	運用手順書
6	情報処理関連設備保守・試験記録	1回／月	施設管理者	定期保守及び緊急保守	事業継続計画

▶情報セキュリティ対策の実施状況の把握

ISMS適用範囲内において適用している管理策の実施状況、要員に対する情報セキュリティ対策の周知度などを把握することとした。

たとえば、実際にはリスク対応計画（**表3.9**参照）により管理策を実施することになっていても、情報セキュリティ対策ベンチマークを用いた診断結果からは実施していないと読み取れる場合、その管理策について具体的に何が問題だったのかを判断し、改善に役立てることができる。

また、教育・訓練の実施の際に、適用しているはずの管理策を、個々のスタッフが実践していないことを発見できる場合がある。その場合、スタッフに対しては順守しなければいけない規定ルールはこれであると明示することで、情報セキュリティ対策の周知度を深めることができる。

12 内部監査または情報セキュリティ監査の実施

内部監査室の監査の一環として、内部監査または情報セキュリティ監査を実施する。監査は、最低でも年1回を原則として実施する。ドキュメントとして、「内部監査ガイドライン」または「情報セキュリティ監査ガイドライン」に詳細を記述する。「内部監査報告書」または「情報セキュリティ監査報告書」を記録として保存する。特に情報セキュリティに関する監査を重視している。

▶内部監査または情報セキュリティ監査

内部監査または情報セキュリティ監査は、内部監査室が監査計画を立案し、各部門の監査を行う。各部門が半年に1回以上の情報セキュリティ監査を受けるものとする。内部監査または情報セキュリティ監査は下記の内容とする。

(1)情報セキュリティ基本方針・情報セキュリティに関する全社規程及び情報セキュリティに関するガイドラインへの準拠に関する監査

(2)関連する法律、条例、業界ガイドライン、契約等への準拠に関する監査

(3)情報システムのセキュリティに関する技術的な監査（内部監査室の判断により、外部セキュリティ監査を実施している会社を利用できる。）

▶監査の報告とレビュー及び考察

(1)内部監査または情報セキュリティ監査結果の報告

監査報告書は、内部監査室長が作成し、社長、情報セキュリティ対策室長及び監査対象部門を統括する部長に報告する。

(2)監査結果によるレビュー

情報セキュリティ対策室は、情報セキュリティ対策室長の指示により、監査結果を参考にして現在の情報セキュリティ対策等をレビューする。

(3)監査結果の反映

情報セキュリティ対策室は、監査結果によるレビューを受け、情報セキュリティ対策についての指示を出す。実行については、各部門の責任者が実施する。

(4)監査の有効性に関する考察

内部監査というと一般的には被監査部門と独立した第三者による監査を意味する。したがって、内部監査室の要員がすべて他部門との兼務であれば、有効な内部監査が実施できる可能性は低いと思われる。

J社の現状では、内部監査室の要員のうち内部監査室長を含めすべてネットワーク運用管理部門、施設管理部門との兼務である。コスト削減のおり、内部監査室の専任者を要することは困難である。また、ネットワーク運用管理部門を監査するスキルを持っている要員が現在不足しており、やむを得ずネットワーク運用管理部門との兼務により実施している。要員不足は否めないが、監査の実施において有効性を確保するよう注意深く監視するとともに、独立した監査が可能な体制を早急に整えることとした。

▶監査員の教育訓練

情報セキュリティ教育・訓練ガイドラインでは、各部門で部門内の全スタッフに対する情報セキュリティ教育計画を作成し、実施することになっている。しかしながら、情報セキュリティ監査が始まったばかりであり、内部監査室では具体的な教育計画の作成がされていない。

また、実際の監査の教育も実施されていない。そこで、計画を作成し、早急に教育を実施し、効果の確認をすることとした。

13 マネジメントレビュー

経営陣は、組織の情報セキュリティマネジメントの導入および実施の最高責任者であり、その意味からも、組織の情報セキュリティマネジメントシステムが適切であり、有効に機能していることを確認する必要がある。また、確認の結果必要となった是正措置や改善を行わなければならない。

J社の社長及び役員は、情報セキュリティ基本方針及び情報セキュリティ目標を含むISMSの導入状況や改善の必要性について、監査報告書によりマネジメントレビューを行った。

また、導入した管理策がどの程度有効に機能しているかについては、導入前の情報セキュリティ対策ベンチマークの診断結果と、導入後の診断結果を比較し、管理策の有効性測定の一助として活用した。

2 ISMS認証取得

1 認証登録までの流れ

▶審査準備

J社では、ISMS認証取得のために追加の情報セキュリティ関連の設備投資は実施していないが、毎年の設備投資計画にデータセンターのセキュリティの強化を組み込んでいる。

審査登録機関（認証機関）は、J社からの見積依頼書を受理し、対象範囲のビジネスの内容、組織の規模等を考慮し、審査の工数の算定に基づく費用を見積書として提示した。

審査登録機関は、J社へ見積書を提出し、双方が同意のもと、認証契約を行った。

▶審査実施

審査登録機関は、審査員を決定し、審査チームを編成し、審査日程の調整を行った。

J社の審査実施にあたって、審査チームには審査をマネジメントするチームリーダーが配員された。さらに、十分な審査をするために審査チームが確保すべき専門性としては、データセンターの経営・運営に関する事項、施設、設備に関する要求事項、利用しているサーバ、ネットワーク等の技術的事項、適用される法規制等があげられた。

申請が受理され、審査登録機関との認証契約等の締結後、審査チームの編成や審査の日程等が調整された後、審査が開始される。

審査登録機関は、審査チームにデータセンターでの業務経験及び関連する業務に携わった経験のある審査員をアサインした。審査チームは、審査業務計画を作成し、審査を実施した。

▶審査登録

審査は、文書審査（ステージ1ともいう）と実地審査（ステージ2ともいう）の2段階で行われた。文書審査の目的は、組織のセキュリティ基本方針及び目標に照らして、当該ISMSを理解し、また当該審査に対する組織の準備状況を理解することにより、実地審査の計画に焦点を定めることにある。実地審査の目的は、組織が自ら定めた基本方針、目標、及び手順を順守していること、当該ISMSが認証基準又は規準文書のすべての要求事項に適合していること、並びに当該ISMSが組織の基本方針及び目標を実現しつつあることを確認することにある。

審査日数や審査工数は、ISMSの適用範囲、受審組織の規模、事業所数、リスクの程度、プロセスの複雑さなどによって異なってくる。また、申請から登録までの期間は、審査日数のほか、審査の不適合（注：不適合とは、マネジメントシステムが基準に適合していないか、システムが実行されていない場合である）の状況によっても異なってくるが、規模があまり大きくなく、特に問題が無い場合には3〜4ヶ月程度と思われる。

J社では、審査の結果、2007年に無事に認証を取得することができた。認証登録の情報は、審査登録機関から認定機関に報告されるが、報告時期により1ヶ月程度ずれる場合がある（**図3.6**参照）。認証登録は、初回審査から3年間有効となる。認証登録後、通常1年を超えないサイクルで維持審査（サーベイランス）が実施される。

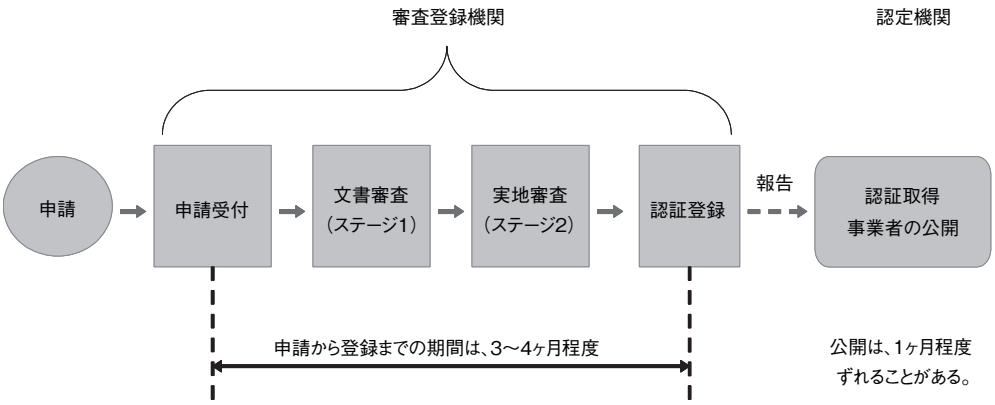

図3.6　審査登録の流れ

2 今後の課題

J社では、今回のISMS認証取得後に、情報セキュリティマネジメントの構築・導入・運用における今後の課題を、次の通り整理した。

(1) ISMS構築に際しての特別な設備投資は行っていない。ただし、情報セキュリティは日々変化していくため、将来に亘って現状のままで十分とは思っていない。リスク評価や事業継続管理といった面について、PDCAサイクルの中で順次向上させていく必要がある。

(2) トップダウンによる推進が重要である。ある程度作業が進んで、ISMS構築が自分達のためになることの理解が得られれば、その後は関係者が自ら進んで始めるようになる。こうしたステップをうまく進めるためには、具体的な推進組織体制が必要である。また、情報セキュリティは、経営の最重要事項であること、そのために経営資源を投入する必要があるとのメッセージを繰り返し発信する必要がある。

(3) ISMSの構築のポイントは、既存コンプライアンスの整理・活用、教育・啓発活動の推進、現場の仕事に合わせた手続き策定などである。教育については、社員・協力会社要員にはe-ラーニングを実行している。e-ラーニングはこれからも続けていくが、内容はISMSの重要なポイント（現場としてやるべきこと）のみに限定しており、ISMS基本方針全体を詳細に説明するための教育は、今後の課題として考えている。

(4) 従来は、データセンター業務の重要性をなかなか理解してもらえなかったが、ISMSを構築することで、情報セキュリティの重要性についての認識が広まり、その結果データセンター業務の重要性を理解してもらうことができた。データセンターのスタッフも業務自体に自信を持てるようになった。

(5) 規程・ルールを明確にすることで、個人の対策実施状況のバラツキを抑えることもできるようになった。今後は、ISMSの改善活動をどのように有効性の測定につなげていくかが課題である。

(6) 情報セキュリティマネジメントの運用においては、日常の活動に無理なく組み入れることで、現場の負担を少なくすることが肝要である。たとえば、現場の業務手順にISMSの手順を組込み、業務手順を参照することで自然にISMSが要求する手順を実施し、記録を残せるようにすることである。

(7) 今後は、ISO 9001等の既存のマネジメントシステムとの融合をいかに進めるかが課題である。