エンジニアリング業界として初の ISO27001 認証取得

認証取得プロジェクトの成果と課題

日揮（株）

■ 執筆者Ｐｒｏｆｉｌｅ ■

田中　修司

1982 年　日揮（株）入社
　　プラント計装設計担当
1992 年　応用システム部～BS 事業部
　　システム開発，ネットワーク設計担当
2006 年　現在 情報技術部 企画グループ所属
　　情報セキュリティ関連担当
　　ISMS 審査員補

鈴木　茂明

1981 年　日揮（株）入社
　　プラント土木設計担当
1984 年　構造解析部
　　プラント構造物の安全性設計解析担当
1999 年　情報技術部　設計支援担当
2006 年　現在 情報技術部 企画グループ
　　グループリーダ

■ 論文要旨 ■

日揮株式会社は，エンジニアリングコントラクタとして，顧客から提供される設計情報など重要な情報を常に取り扱う立場にあり，情報セキュリティの確保は業務遂行上必須条件である．

情報セキュリティに関し，当社では 1999 年に情報セキュリティポリシーを社則として制定して以降，社内整備を進めてきた．

当社のセキュリティレベルを第三者の立場で検証することは，当社の顧客に対する信用度を高め，また競争力強化においても重要な意義があると判断し，ISMS の国際規格(ISO27001)の認証取得を目指して，2005 年 11 月より日揮情報システム株式会社と共同でプロジェクトチームを発足し，富士通 SSL 殿の支援を受けながら，2006 年 9 月に ISO/IEC 27001:2005(JISQ 27001:2006）を，エンジニアリング業界として初めて認証取得した．

認証取得作業においては，専任のプロジェクトメンバを置かず，また，他の業務と兼務しながら約 10 カ月間という短期間で効率よく認証取得に漕ぎ着けた．その間に直面した課題とその解決策，工夫点および得られた知見について，今後の予定を含めて述べる．

■ 論文目次 ■

■ 図表一覧 ■

1. はじめに

日揮株式会社(以下，JGC という)は，1928 年(昭和 3 年)に創業した日本初のエンジニアリング会社である．当社は，日本国内はもとより，アジア，中近東，アフリカ，南米，東欧など世界各地で石油・ガス・石油化学といったハイドロカーボン分野の国家プロジェクトに参画し，これまで世界 70 カ国，約 2 万件にも及ぶプロジェクトの遂行実績を誇る．

また，JGC はハイドロカーボン分野だけでなく，医薬品工場・研究所，食品工場，医療・福祉施設，インターネットデータセンターなど一般産業社会分野においても多種多様のプロジェクト実績があり，当社の提供するビジネス分野は多岐に亘る．

当社の従業員は，海外拠点を含め約7,000名を有し、横浜みなとみらいに在る横浜本社を中核拠点とし，設計や調達拠点，建設現場は世界各国に点在しており，「エンジニアリング業をコアとするグローバルな企業グループとして永続的発展を目指し，世界経済と社会の繁栄ならびに地球環境の保全に貢献する」という企業理念の下，企業価値の向上に努めている．

2. ISO27001 認証取得の経緯

本章では，当社が ISO27001 認証取得に至った経緯や背景について，エンジニアリング会社を取り巻く情報セキュリティに関わる外部環境等をまじえながら説明する．

2.1 エンジニアリング会社の特徴

基本的にエンジニアリング会社では，プロジェクトの基本計画から設計，資材・機器の調達，建設まで一貫した体制で遂行する．これらの業務を，エンジニアリング(E)・プロキュアメント(P)・コンストラクション(C)のそれぞれの頭文字をとって，EPC 業務と呼んでいる．EPC 業務だけでなく，EPC 業務の上流工程のフィージビリティスタディや建設後の試運転なども実施している．

現在のプロジェクトの大部分は，海外プロジェクトであり、調達も含めてワールドワイドな事業をタイムリーかつ効率的に遂行するため，グローバルなネットワークを構築し，海外のエンジニアリング拠点(GEC)やベンダー・サブコンも積極的に活用している．

2.2 JGC における IT 環境

現在 IT は企業が事業を推進する上で，必要不可欠なものとなっている．JGC も同様であり，日々の業務において，ERP，電子メールシステム，ドキュメント管理システム，グループウェア，CAD，ネットワーク･サーバなどを積極的に活用しており，IT は JGC において重要なライフラインとなっている．(図 1 参照)

また，JGC は情報システム基盤の構築と運用を，JGC の 100%子会社である日揮情報システム株式会社(以下，JSYS という)にフルアウトソーシングしており，JSYS はその安定運用を支える重要なビジネス･パートナーとなっている．

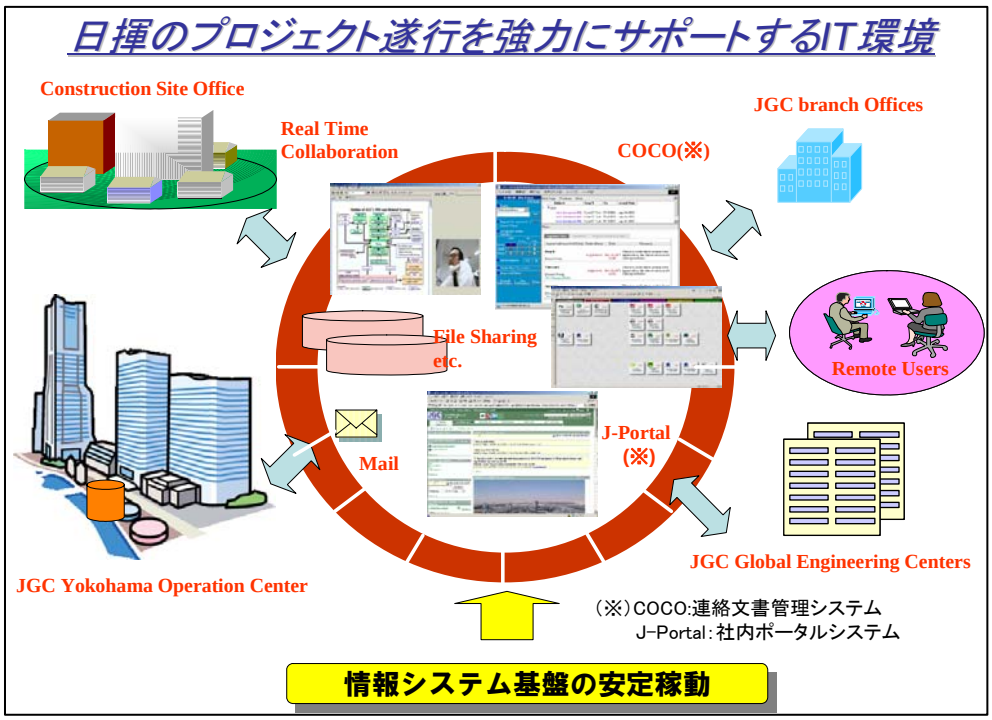


図 1　日揮の情報システム基盤

2.3　JGC における情報セキュリティの課題

社内固有の情報，ハイドロカーボン系の顧客から預かる情報，原子力・医薬品研究所・医療関連などの顧客から預かる情報と，JGC の取り扱う情報は，広範囲でかつ非常に重要度が高く，機密レベルも異なる．

このような状況の中，全社的な情報管理を組織的に推進するために，1999 年に、BS7799 をベースに「情報セキュリティ基本規程」を制定した．しかし，規程及びその下位文書に当たるガイドラインやマニュアル類は，時代の流れとともに陳腐化し一貫性に欠ける部分も見受けられるようになっていた．

この間、個人情報に関して、JSYS は個人情報管理のコンプライアンス･プログラムを導入し，プライバシーマークを取得した。2005 年 4 月に個人情報保護法が施行され，JGC は個人情報取扱事業者(5000 人以上の個人情報を保有する事業者)であるため，日揮グループの個人情報保護方針および個人情報保護規程を制定し対応してきた．

情報システム基盤の観点からは，ネットワークやサーバの冗長化，ファイアウォールやアンチウィルス・システムの安定運用により，JGC の EPC 業務は大きな障害もなく遂行している．しかし，JSYS に運用業務を移管してすでに 15 年以上になり、それらの運用業務は，属人的になっている部分も多く，マニュアル化の整備が遅れていることも分かった．このため，対応が場当たり的になっている部分もあり，セキュリティの確保が難しくなっていた．

このような問題を背景に，情報セキュリティの課題を根本的に解決するためには，情報セキュリティ･マネジメント･システム(以下，ISMS という)の構築が急務となっていた．

3. ISO27001 とは

3.1 国際動向

情報セキュリティマネジメントシステムの国際規格 ISO/IEC27001:2005(以下，ISO27001 という)は，2005 年 10 月 15 日に正式に発行された．ISO27001 は，情報資産の漏洩，流出，破壊や不正アクセスなどの脅威から企業を守るために，情報の機密性(C：Confidentiality)，完全性(I：Integrity)，可用性(A：Availability)を社内で継続的に確保・維持するシステムを確立するために定められた．ISO9001 や ISO14001 と同様に PDCA モデルが適用されている．

3.2 国内の動向

日本国内では，1970 年代に情報セキュリティの必要性の高まりを受けて，1979 年に当時の通産省が「情報セキュリティ安全対策基準」を制定し，これに続き「情報処理サービス業情報システム安全対策実施事業所認定制度」(以下，安対制度という)が発足した．現在の ISMS 適合性評価制度(以下，ISMS 制度という)はこの安対制度の後継であり，BS7799 を手本として ISMS 認証基準が制定された．その後，2006 年 5 月 20 日に JIS Q 27001:2006 が制定されたが，それまでは ISMS 認証基準 Ver.2.0 が使われていた．ISMS 制度の運用においては，日本情報処理開発協会(以下，JIPDEC という)が認定機関と審査員評価登録機関となっている．

なお，2006 年 10 月 13 日現在の ISMS 認証取得登録事業者数の累計は 1775 社で，この数字は他国の取得数と比べると圧倒的に多い．しかし，今後日本企業は日本版 SOX 法(以下，JSOX という)などの内部統制への対応を迫られ，情報セキュリティ対策はそれらの基盤（IT 全般統制）となる．このような状況の中，JGC は海外企業に対するアピール性を最重要視し，ISMS 制度の認証は取得せずに，ISO27001 の発行のタイミングを注視してプロジェクトを準備していた．

4. ISO27001 認証取得プロジェクトの概要

本章では，JGC が遂行した ISO27001 認証取得プロジェクトの概要について説明する．まず，実際のプロジェクトをスタートさせる前の準備段階に実施した内容から説明する．

4.1 準備段階

4.1.1 プロジェクト遂行体制

今回のプロジェクトは，JGC と JSYS の共同での認証取得という形態をとった．JIPDEC が公開している“ISMS 認証取得事業者検索”を調べてみたが，ほとんどの会社が 1 社で取得しており，共同で取得している例は見当たらない．JGC は，JSYS と別々に認証を取得するよりも効果的かつ効率良く認証取得が可能になると考え，JSYS との共同取得の体制とした．実際のプロジェクトの体制表を下図 2 に示す．

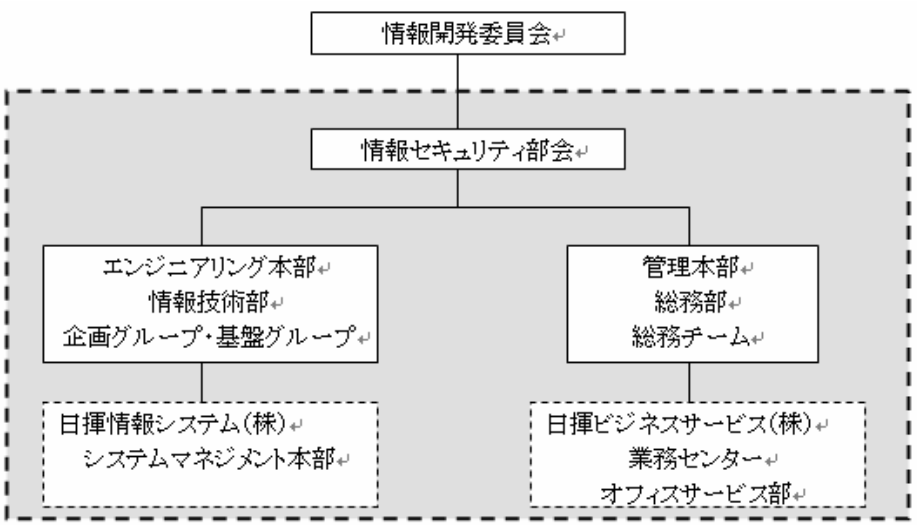


図 2　ISMS 推進プロジェクト体制（コアメンバ部門）

破線部分が，本プロジェクトのコアメンバ部門である．

(1)　情報開発委員会は，社内の情報システム開発や情報システム基盤の整備方針，予算化を審議する機関である．

(2)　情報セキュリティ部会は，情報開発委員会の下部組織で，社内の情報セキュリティの検討・審議機関である．また，当部会は，今回の ISO27001 認証取得における承認機関で，当部会の主査が経営陣(Management)にあたる．

(3)　コアメンバは，今回の ISO27001 認証取得プロジェクトの中心メンバー，全員本業と兼務である．また，情報技術部　企画グループが，当プロジェクトの事務局となった．なお，本プロジェクトがスタートした後，若干の組織変更はあったが，コアメンバ内での異動だけで，大きな影響がなかったのは幸いであった．

また，当プロジェクトは，2005 年 11 月からスタートし，約 11 ヵ月の期間の後，認証を取得することができた．スケジュールの概要は，下図 3 を参照いただきたい．

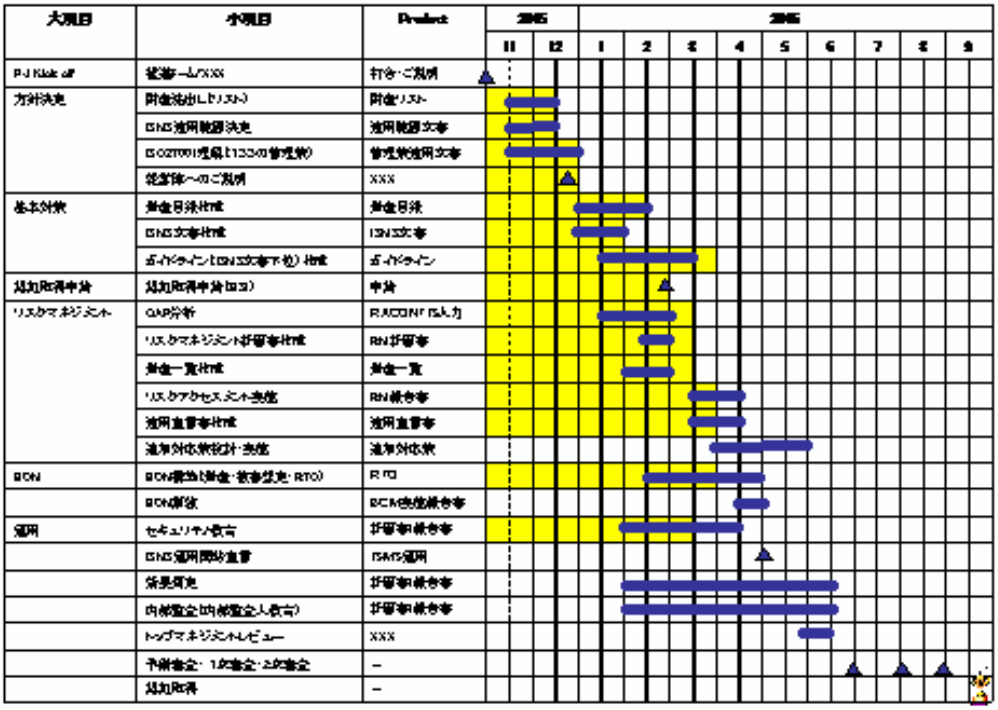


図 3　ISMS 認証取得スケジュールの概要

4.1.2　外部コンサルタントの活用

短期間で効率的に認証を取得するためには，以下のポイントからコンサルタントの支援は必要不可欠と考えた．

(1)　必要最低限の書類だけを文書化し(無駄な資料を作らない)，無駄な作業をしないなど業務の効率化を図る．

(2)　最も作業時間を要すると予想されたリスク・アセスメントに必要以上の時間をかけず、情報資産の洗い出し，リスク評価を短期間に効率的に行う．

(3)　規格発行から間もないため，審査機関による解釈のばらつきによる影響が懸念されたため，多くの情報を入手するための情報リソースとして活用する．

いくつかのコンサルタントの情報をインターネットからの情報やヒアリングを行い，最終段階で 3 社に絞り込んだ．審査機関を親会社に持つ A 社，専業のコンサルタントの B 社，残りの 1 社は，富士通ソーシャルサイエンスラボラトリ(以下，FSL という)である．

選定評価において重視したポイントは，実績の豊富さや金額面だけではなく，各種のサポート等についても評価の対象とした．提案の内容やこれまでの実績に関しては 3 社ともに優劣が付けがたく，最後の決め手となったのは，リスクアセスメントを効率的に行なうことができるツール(リスク分析ツールを有していた FSL 殿の RACONTIS)である．このツールの特徴については，後述する．

情報セキュリティレベルを維持し向上を図るためには，下図 4 に示すような“PDCA サイクル”を継続的に繰り返していくことが求められる．

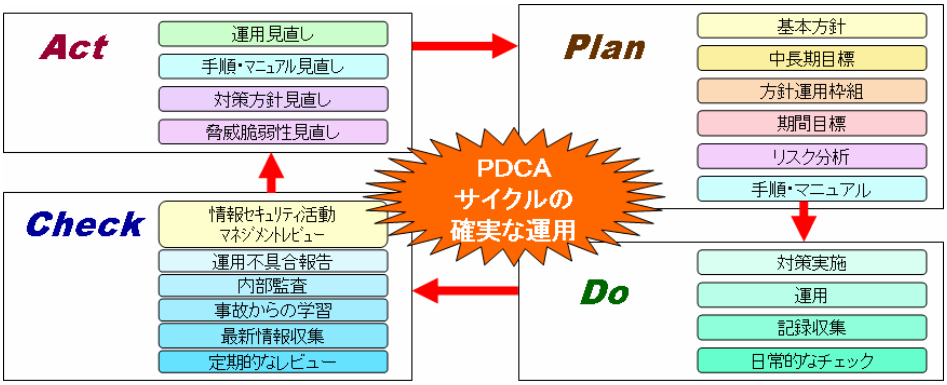


図 4　PDCA サイクル

●Plan　：情報セキュリティ対策の具体的計画・目標を策定する.
●Do　　：計画に基づいて対策の導入・運用を行う.
●Check ：実施した結果の監視・見直しを行う.
●Act　　：経営陣による改善・処置を行う.

次節からは，情報セキュリティマネジメントの PDCA サイクルにしたがって，各段階でのトピックスについて振り返ることにする.

4.2　Plan 段階

ISO27001 のファイナルドラフトをいち早く入手し，当初 2 カ月間毎週 1 回午後を使い，規格の内容を理解するために，コアメンバを中心とした勉強会を開催し，プロジェクトはスタートした．本節では，Plan 段階のトピックスについて説明する.

4.2.1　適用範囲の検討

ISO27001 認証取得の適用範囲の設定には，かなりの時間をかけて議論した．初回審査ということもあり、今回の認証取得を ISMS の第一ステップとし段階を踏んで適用範囲を広げていく，“Start Small to Big”の方針がまず決まった．(図 5 参照)

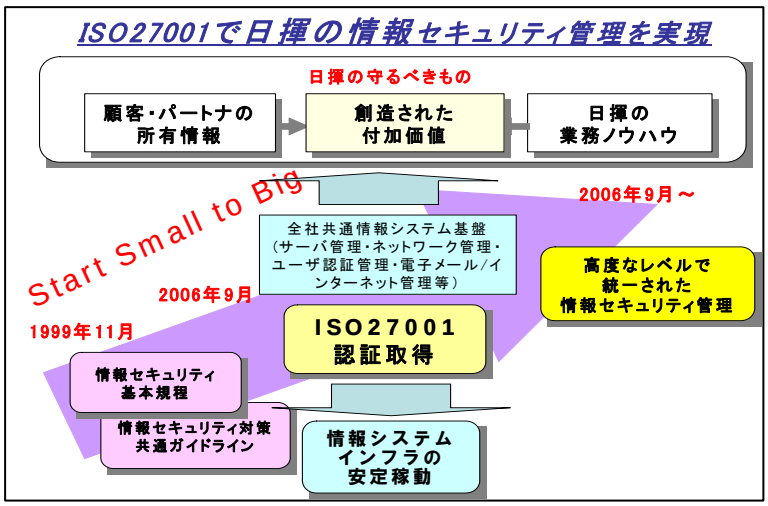
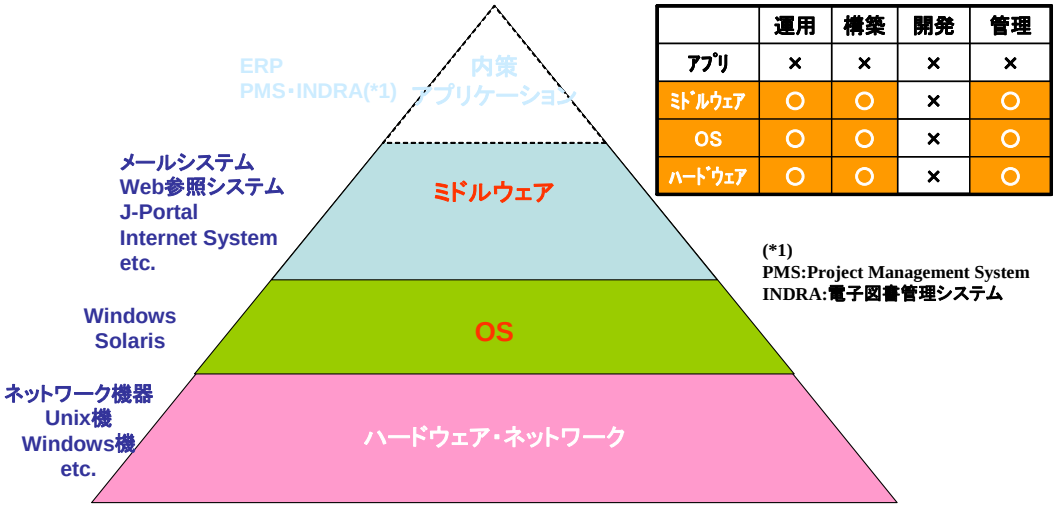


図 5　“Start Small to Big”の方針

また、規格では，ISMS の適用範囲を定義する際に，境界を記述する必要があり，また除外理由についても明記する必要があった．今回の適用範囲は，ネットワーク機器・サーバ・PC などのハードウェア，その機器に搭載された OS，およびその上で稼動するミドルウェアの「情報システム基盤」を対象として，業務用アプリケーション部分は適用対象外とした．

これは，情報システム基盤は，情報システムの根幹を成し EPC 業務遂行に欠かせない存在となっている．そのため，強固な情報システム基盤を構築することにより，安全で安定したプロジェクトの遂行を保障することは，JGC における情報セキュリティを考える上で，最も重要性が高いと考えたからである．



	運用	構築	開発	管理
ｱﾌﾟﾘ	×	×	×	×
ﾐﾄﾞﾙｳｪｱ	○	○	×	○
OS	○	○	×	○
ﾊｰﾄﾞｳｪｱ	○	○	×	○

図 6　ISMS 認証取得の適用範囲

上図 6 にもあるとおり，今回の適用範囲には，開発業務は含まれていない．そのため，適用宣言書においても，開発に関わる一部の管理策「A12.2　業務用ソフトウェアでの正確な処理」などは適用外とした．

4.2.2　リスクアセスメントの概要

リスクアセスメントの内容を，図 7 リスクアセスメントフローの流れに沿って説明する．

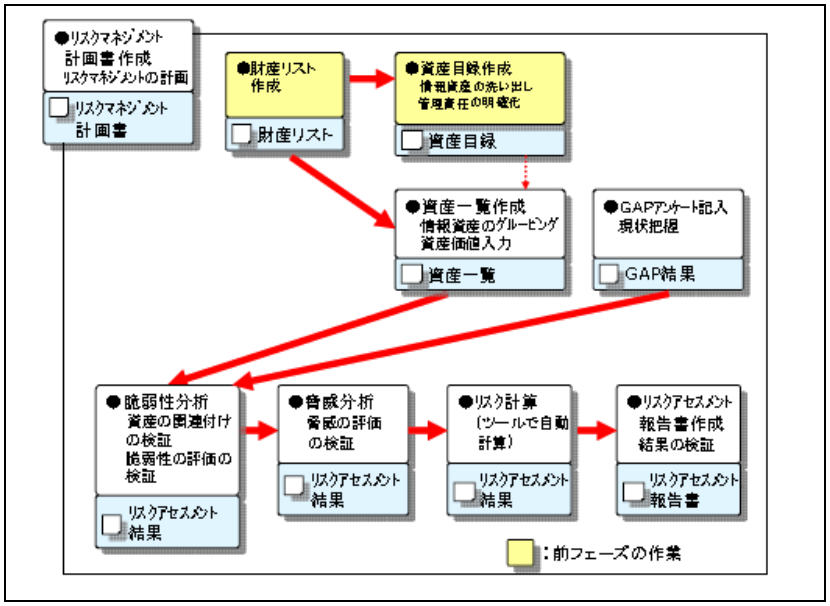


図 7　リスクアセスメントフロー

(1)　ギャップ分析の実施

各部署での情報資産の洗い出しを行い資産一覧が完了した後，ギャップ分析を実施した．ギャップ分析とは，IS027001 に規定されている 133 の詳細管理策に対して，どの程度対策が実施されているかを現状把握するためのものである．適用範囲に関連する 10 の部門に対して，下図 8 に示すような質問事項（サンプル）を用い現場へのヒアリングを実施した．

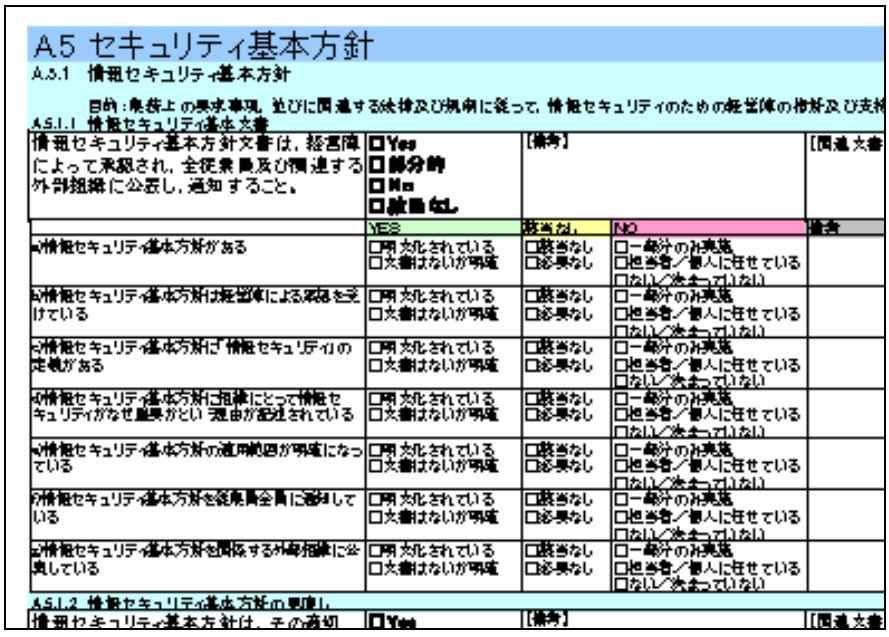


図 8　ギャップ分析質問表(サンプル)

(2)　リスク分析ツールの利用

規格では，“比較可能でかつ再現可能な結果を生み出す”内容が求められている．

RACONTIS は，分析結果をデータとして保存することができ，まさに比較が可能で再現性があり非常に有用なツールである．また，リスク分析に使用する Methodology は，我流ではなく，ある程度世間に一般的に認められた手法であることも必要である．その点でも，RACONTIS は，GMITS(ISO13355)という一般に知られたリスク分析手法を採用しており，我々の求める要件を十分に満足するものであった．RACONTIS の計算プロセスは，図 9 の通りである．

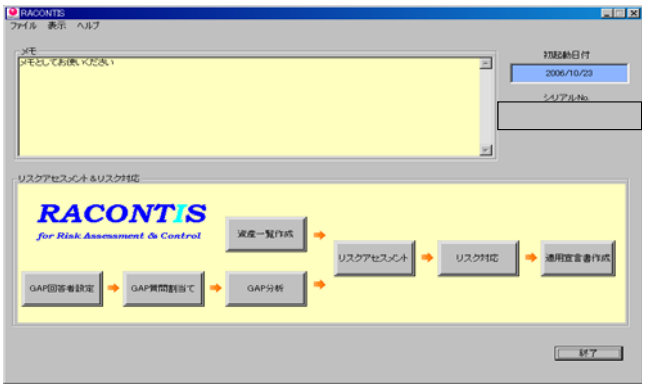


図 9　RACONTIS メニュー画面

(3)　定性的評価の概要とその結果

リスク値計算は，「リスク＝資産価値＋脆弱性値＋脅威値－２」という計算式を用いた．その結果，この方法で計算を行なうと，図 10 リスクマトリックス表のとおりとなる．

脅威値		1			2			3		
脆弱性値		1	2	3	1	2	3	1	2	3
資産価値	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7

図 10　リスクマトリックス表

リスク分析の結果，リスク値の分布は，図 11 のようになった．リスク値”4”の対策については，今回の ISMS 文書作成で対応が可能となる部分も多いこと，許容可能なリスクと考えられるものも多いこと，また全てのリスクに対応することは現実的に困難であることなどを理由に，プロジェクトメンバの協議の末，リスク許容値は”4”に設定し，リスク”5”と”6”を対象にリスク対策を実施することになり，本決定はマネジメントレビューにおいて承認された．なお，リスク値”7”は，今回のリスクアセスメントの結果では得られなかった．

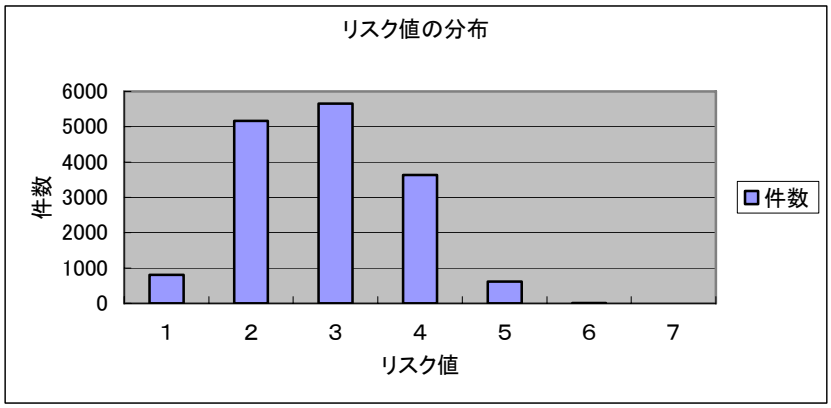


図 11　リスク値の分布

4.2.3　ISMS 文書の作成および管理

ISMS 文書の作成は，規格準拠のドキュメント作成という観点，リスク対応という観点，両者から必須の作業であった．基本方針，基本規程，各種ガイドラインなど約 50 種類のドキュメントのほぼ全てを新規に作成した．

数人のメンバーで文書作成作業を分担したが，着手してから約 2～3 ヶ月の期間を要した．FSL 殿にて用意していただいたガイドラインやマニュアル類の雛型に基づいて、当社の運用にあわせた言葉で書き下すことに専念した。この雛型には，規格で規定されている項目が各ドキュメントに漏れなく反映されており，非常に役に立った．この完成度の高さにより，ドキュメント作成の時間は大幅に短縮につながったと思う．これがなければ，おそらく倍以上の時間がかかっただろう．

また，ISMS 文書の文書管理は，当社で利用しているグループウェア Lotus Notes のデータベースを活用した．紙の文書では，版管理や配布管理が煩雑となる．Lotus Notes では，必要なときに最新の文書にアクセスでき，伝達や検索も容易にでき非常に便利である．なお，版数の表示では，最新版と旧版を明確に区別した．

4.2.4　事業継続管理（Business Continuity Management:BCP）の策定

当社の危機管理規程は，2001 年 9 月 11 日の同時多発テロを契機として策定された．災害を想定しているため，人命救済という意味合いが強い．安否確認システムなども導入されている．

しかし，事業継続という観点で考えた場合，事業の継続性に影響を与えるのは，災害やテロだけではない，今回 BCP に関しては，従来の防災対策の観点を踏襲しながら，リスク分析の結果に基づき身近な部分にも目を向け BCP の検討を行った．具体的には，インフルエンザなどによるキーマンの不在など従来の防災対策では考慮していなかった要素を盛り込んだ．

策定されたガイドラインやマニュアルに基づき，地震など 3 つのシナリオを事前に作成し，関係者を一堂に集め机上ながらも BCP 演習を実施した．あとで振り返り参考できるように，下図 12 に示すようなチェック・ポイントをあらかじめリストアップした．

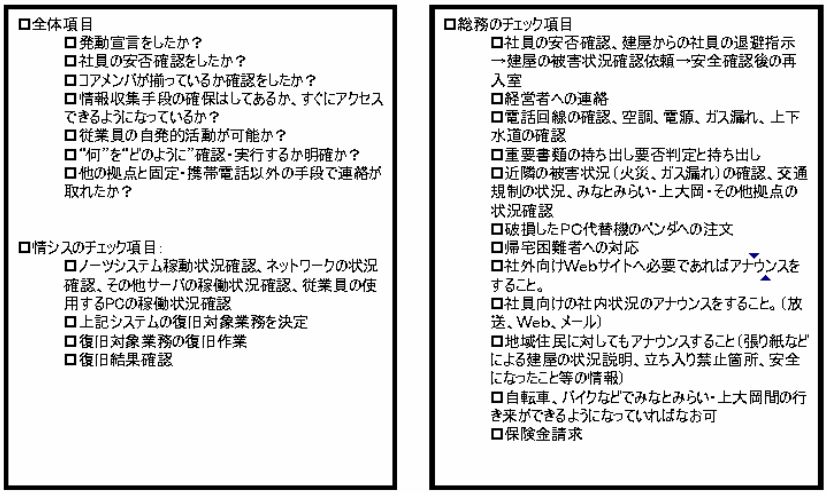


図 12　BCP 演習におけるチェック・ポイント

4.3　Do 段階

基本方針で示した目標は，以下のとおりである．

(1) 適切な情報セキュリティ管理を実施し，情報セキュリティ・インシデントを未然に防止し，情報セキュリティ・インシデントの発生ゼロを目指す．

(2) 万が一情報セキュリティ・インシデントが発生した場合も，その被害を最小限にとどめ，迅速な復旧を行い，またその再発を防止する．

(3) 情報資産の可用性を確保し，必要な情報が必要な時に利用できるようにする．

この目標を掲げ，本年 5 月より ISMS の運用がスタートした．

4.3.2　リスク対策の実施

リスクアセスメントの結果，対策として，ISMS 文書整備（契約書の見直しを含む）とシステム的な対応（モバイル PC への暗号化ソフト/パーソナルファイアウォールの導入，システム運用管理ツールの導入など）を行なうこととなった．

4.3.3　セキュリティ教育

コアメンバから実運用担当者への ISMS 技術伝承は重要である。ISO27001 の考え方、本 PJ の目的、作成文書の意味合いについての独自の教育資料を作成し、Face To Face の教育を対象者 91 名に対して実施した。特に、JSYS 部次長レベル者には数回繰り返し、ディスカッションを実施することで共通意識の醸成と実務に即した運用化が図れた。当社には，外国人スタッフも多く，彼らに対しても教育を行なった．また教育終了時には，理解度を確認するためのテスト(全 20 問)を実施し，70 点以上(14 問以上の正解)の得点を目標とした．

さらに，本教育だけでは，規格やガイドラインの内容を理解するのは困難であるとの声が現場から上がり，マネージャクラス以上の特別講習を休日を利用して行い，理解不足の点を補った．

4.4 Check 段階

4.4.1 内部監査

内部監査は，ISO27001 では章(第 6 章)に格上げされた．これは，内部監査が，「ISMS が計画通りに確実に行なわれていることを確認し有効性を判定する」という，重要な業務であるとの認識に他ならない．

まず，内部監査を実施するに当たって，監査員はだれが適切なのかを検討した．内部監査では，客観的な監査を行なうため原則として公正かつ独立した立場で実施する必要があり，その前提で考えると ISMS 適用範囲外の他の組織から監査員を選ぶことになる．当社では，既に品質マネジメントシステム(QMS)及び環境マネジメントシステム(EMS)の ISO(ISO9001/ISO14001)を取得しており，EMS だけでも主任監査員 22 名，監査員 30 名の合計 50 人強の内部監査員がいる．しかし，今回の ISMS の監査では，規格の適合性や有効性の確認にとどまらず，システム改善に効果的な不適合の抽出方法及び是正処置の要求方法等を提示することが必要であり，そのためには IT 業務や情報セキュリティに精通し，また規格に関する知識が必要であろうと判断した．このため，初回の内部監査に関しては，完全な独立性は求めず，互いの部門を相互監査するという方法をとった．内部監査人教育は，内部監査規程や FSL 殿作成の内部監査手順などを教科書として使用しながら実施し，演習等も行なった．

4.4.2 有効性の評価･測定

有効性の評価や測定は，ISO27001 の新しい要求事項であり，実際に採った対策が有効であったかどうかを評価するため，有効性の測定と評価を規格では求めている．事前に約 50 項目の効果測定基準を作成し，その中から今回は，初回審査ということもあり，情報セキュリティ教育の理解度確認テストの結果と情報セキュリティ･インシデントの発生件数の二点に絞った．

4.4.3 マネジメントレビュー

マネジメントレビューでは，これまで実施してきた，一連の作業に関して報告を行なった．そして，リスク分析の手順とその結果，またその結果に基づきリスクの許容レベルと残存リスクに対してどのような対策を実施するのかを説明し，承認を得た．

4.5 審査に関して

4.5.1 審査機関の検討

審査機関として,以下の理由からビーエスアイ･ジャパン(以下，BSIJ という)を選定した。③については，審査機関側での審査員の養成時期でもあり,また分野が全く異なることから今後も難しいと予想される．

① 審査実績
② 海外での評価
③ QMS/EMS の認証を取得済みで将来的な総合審査の可能性

4.5.2 予備審査

一次審査の 1 ヶ月前に予備審査を受審することとした．これは，一次審査への準備状況の不備を確認し，一次審査をスムーズに乗り越えたいと考えたからだ．予備審査では，いくつかの観察事項が指摘されたが，特に大きな問題はなかった．しかし，「テレワーキング」(Teleworking)の解釈については，BSIJ 殿の審査員と認識の違いが生じたため，かなり議論の時間を費やした．我々の解釈は，「テレワーキング」は在宅勤務であり，PC の社外利用などは，モバイルコンピューティングやリモートアクセスの管理策で対応しているとした．このような点は，審査機関の横のつながりも強くし，用語の解釈でばらつきがないよう改善して欲しいと感じた．

また，予備審査の後，一次審査に向けて数回の内部リハーサル(模擬審査)も実施した．FSL 殿に審査員に扮していただき，本番さながらのピリピリとした状態を演出してもらった．どうしても，審査となると肩に力が入ってしまいがちだが，このような経験を経て自信が持て，比較的平常心で審査に臨めたと思う．一次審査直前には，ポスターも掲示し，審査が迫ってきていると従業員の意識の定着を図った．

4.5.3 一次審査

一次審査の結果，不適合事項はなく，8 件の観察事項の指摘がなされた．内一つは，グッドポイントであった．グッドポイントとして評価されたのは，BCP の演習に対する評価であった．作成したシナリオの中に，当日に初めて知らされる内容もあり変化への対応力についても検証した．また，事前にチェックすべきポイントをリストアップしてあとで振り返る際の参考とした．その点が評価された．

4.5.4 二次審査

二次審査では，観察事項が 3 件で，内 1 件はグッドポイントという結果であった．積極的な経営資源の投入（4.3.2 に示すシステム的な対応）に対しての評価であった．

BISJ 殿の審査全般を振り返ってみると，予備審査から始まり二次審査までのプロセスにおいて，指摘事項を含む適切なアドバイスを頂き，また互いの意見をぶつけ合うことで，より一層規格の要求している意図を理解することができた．審査される側，審査する側という立場に踏み止まらず，一種のビジネス･パートナーとしての関係を構築させていただいたと思う．

5. 当プロジェクトで得られたもの

今までの説明を振り返り，今回のプロジェクトで効果のあった点等をまとめてみると，以下のようになる．

(1) ISMS 認証取得範囲を事前に綿密に検討を行った．これが，プロジェクト期間およびコストに大きな影響もなく進めることができた大きな要因の一つとなっている．

(2) リスクアセスメント作業は，資産の棚卸，リスク評価，その対策案立案等，最も時間がかかる作業である．リスク分析ツール“RACONTIS”の導入により，リスクアセスメ

ント作業を大幅に短縮できた．また，“RACONTIS“は，資産・評価・対策後の評価など一連の作業において生成するデータをメンバ間で共有することが可能で，データの「見える化」にもつながる．最終的には，セキュリティの三要素である，C(Confidentiality)，I(Integrity)，A(Availability)のバランスの取れた対策を講じることができた．

(3) ISMS は，運用記録も含め，必要とされるドキュメントの量が非常に多い．作成に際しては，FSL 殿に用意していただいた雛形が大いに活用できた．さらに，「紙」ベースの管理を取りやめ，Lotus Notes データベース上に電子ファイルの最新版のみを提供することで，文書管理の手間を大幅に低減できた．

(4) コアメンバから実運用担当者への ISMS 技術伝承は重要である．ISO の考え方，本 PJ の目的，ポリシーや基準等の作成文書の意味合いを解説した独自の教育資料（ポスター作成やハンドブックも別途作成・配布）を作成し，共通意識醸成と実務に即した運用化が図れた．

(5) 審査機関とも熱心な議論ができたおかげで，良好なパートナーシップが得られた．

(6) 情報セキュリティ事故に対する対応を強化し，発生時対応と対応策監査およびその Lessons & Learned の共有を，月例報告会で行う仕組みを構築した．現在までに発生したいくつかのインシデントに対する改善を実施している．

6. 今後の予定

(1) リスク許容レベルの見直し

リスクは，時間の経過と共に常に変化している．今回のリスク分析の結果許容値は”4”に設定したが，外的･内的要因の変化に応じて許容レベルを”3”とハードルを上げることも考える必要がある．

(2) 内部監査員の拡充･強化

PDCA サイクルの中で大きな役割を果たすのが内部監査である．内部監査員は独立性が要求されるが，ISMS の内部監査員の力量としては，ISMS を構築し運用するための手順，実行結果，文書等を理解していなければ~~なければ~~ならない．組織の現状と問題点を把握し，被監査部門に適切なアドバイスを行うことも必要である．2007 年の維持審査に向けて，他部門と調整を図りながら，内部監査員の拡充･強化を図る計画である．

(3) 適用範囲の拡大

先にも述べたとおり，当社の適用範囲は，現時点では情報システム基盤に限定している．今後は，海外の設計拠点である GEC やグループ会社などへの展開も視野に入れているが，まず今回の適用範囲内での定着が先決と考えている．

7. 最後に

JGC/JSYS は ISO27001 の認証を無事取得できたが，これで 100%のセキュリティが保証された訳ではない．CMMI モデルでは企業の成熟モデルを 5 段階で定義しているが，この認証取得により，当社はようやくレベル 3 に達したと考える．今後，１年毎の維持審査，３年目には更新審査を迎えることとなる．したがって，このレベルを維持し，さらに 4 もしくは 5 のレベルに上げていくためには，PDCA サイクルをしっかりとまわしていくことが必要となる．

毎月の定例会では，セキュリティ・インシデントの対応のレビューを毎回行なうようになり，議論の内容にも活気が出て，セキュリティ意識が定着してきた．しかし，社会環境は変化し IT の進歩は日進月歩である．また，社内での組織変更の可能性もある．当社のビジネス･スタイルも変わっていく可能性もある．それらにも随時対応していく必要がある．

本書が，今後 ISO27001 認証取得を検討されている企業の担当者の方々に，少しでも参考になれば幸いである．

参考文献

[１] “ RACONTIS Ver.1.1 仕様手引書 ”, 富士通ソーシャルサイエンスラボラトリ,
2005年12月20日