情報セキュリティマネジメントシステム(ISMS)構築と運用実践による効用

グローバルフォーカス 株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

福　原　幸太郎

1978 年　（株）オリエント・ファイナンス入社
現：(株)オリエント・コーポレーション
システム開発業務担当
1999 年　グローバル・フォーカス（株）分社
2004 年　現在 監査統制部所属
ＩＳＭＳ推進担当

■ 論文要旨 ■

企業のグローバル化，情報通信ネットワークの高度化により，企業経営活動が社会に与える影響範囲が急激に増加している．この状況は今後も加速度的に広がり，スピードを増していくと考えられる．

ビジネス環境の変化に伴い情報資産(情報/データ等)のすべてに対して確実に情報資産の価値に見合った安全保護対策を打っていくためには，情報システム部門現場だけが，情報セキュリティの技術対策(ファイアウォール，ウイルス対策等)だけを必死に対応しても限界があり十分ではない．

情報資産の価値に見合った安全保護及び有効活用には，経営者の強力なリーダーシップと明確なセキュリティポリシー及び徹底したリスクマネジメントによる企業活動の適切かつ継続的な対策を打てるマネジメントシステム(プロセス)が必要不可欠であると考えるとともに，『情報セキュリティマネジメントシステム(以下ＩＳＭＳ)構築／運用』が情報セキュリティの継続的維持向上の第一歩であることを経営課題として認識してＩＳＭＳの構築に着手した．

当社はこの『ＩＳＭＳ構築作業』とその後の『ＩＳＭＳ運用実践』の中での失敗，苦労からＩＳＭＳ構築実践でリスクマネジメントを継続的に実施する仕組みと意識が重要であるということを得た．またそれらの活動は，組織マネジメント各層(経営者層／ミドルマネジメント層／業務担当層)ごとに情報セキュリティに対する意識変革と自信をもたらした．今後は，『脆弱性発見態勢の強化』と『全部署へのＩＳＭＳ拡大展開』によりセキュリティ強化を実現すると共にセキュリティ文化の醸成に努める．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社概要

当社は，株式会社オリエントコーポレーションと富士通株式会社が提携し，クレジットシステムを中心としたシステムの開発から運用までの業務受託サービス等のアウトソーシングサービスを提供する目的で１９９９年９月に設立された．

主たる業務は，株式会社オリエントコーポレーションのクレジットシステム全般のシステム開発・運用受託を中心にし，これまでに蓄積した，開発技術ならびに運用技術を活用したシステム全般のアウトソーシンググ事業やコンサルティング事業を行っている．

１．２　当社のＩＳＭＳ範囲内システム概要

当社は，国際規格である「ＢＳ７７９９」を英国の審査機関であるＬＲＱＡの審査を受けて２００３年２月に認証取得した．２００３年７月には定期審査ならびに最新バージョンの「ＢＳ7799－２：２００２」への移行を終え，２００４年７月の４回目の定期審査に向けて，継続的改善活動中である．

当社のＩＳＭＳの適用範囲は，クレジットカードオーソリシステム(以下 A－ONE)の開発保守運用を範囲とし**図１**に示す．また，システム規模については**表１**に示す．

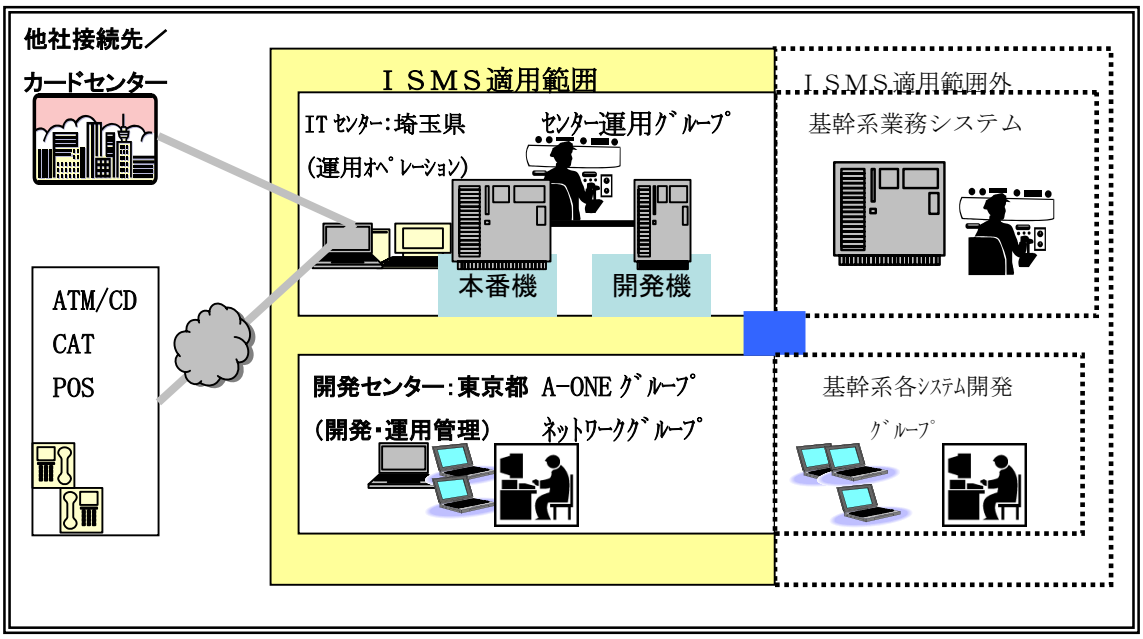

図１　当社のＩＳＭＳ適用範囲

表１　システム規模

本番機／ＯＳ	Himalaya　K2006／*NonStop Kernel D39.01*
開発機／ＯＳ	Himalaya　K1004／*NonStop Kernel D39.01*
ＰＧＭ	約１６００本(約１．２M Steps)
業務マスタ容量	約９０Ｇ
月間トランザクション	約５５０万件
月間バッチ処理	約４０００ＪＯＢ
ＣＲＴ端末数	約２５０台　（ＩＳＭＳ関係者数：約１６０名）

２．当社を取り巻く環境変化の認識

２．１　顧客情報の多様化と情報価値の高騰

顧客要求が多様化しより個性的になり，多品種，少量生産の商品サービスを提供するために，個々の顧客情報を細かく活用して顧客の要求事項に応えることがが企業活動を継続するうえで，一層重要になってきた．顧客情報を売買する業者がいてそれを買う業者がいると言うことは現実にあることであり，このことは逆に個々の顧客情報の経済的価値が高まっている証拠でもある．

２．２　グローバル化と情報通信システムのブロードバンド化

情報システムは個々の企業内に止まらずグローバル化による，企業相互間(Ｂ２Ｂ)，企業と顧客間（Ｂ２Ｃ）へと拡がり，情報通信ネットワークのブロードバンド化により情報資産が高速(短時間)に大量に広範囲に伝達交換できる時代に突入し続けている．

企業活動を支えるためには，情報システム抜きにして語ることは出来ない状況(企業活動の情報システムへの依存度は高くなる一方)である．

今までの情報システムの有効性，効率性に加えて，より安全で信頼できる情報システムの開発及び運営が求められてきている．

２．３　情報セキュリティマネジメントの重要性認識

２．３．１　情報資産とコンピュータの遍在化

情報資産と一口に言ってもＰＣ等のコンピュータに格納された電子化された情報が何処でも，誰でも，何時でも手に入れることができる，未知なる環境(ユビキタス)が整いつつある．

また，それらの電子情報だけでなく，紙に印刷された情報，その他大容量メディアに記録された情報，従業員一人一人の頭の中にある記憶情報もある．どのような場所に，どれほどの価値をもった情報が存在するかを把握することが必要である．

２．３．２　情報セキュリティマネジメントの必要性

このように多様な形(未知なる形，処理形態)で存在する情報資産をその資産価値に応じた保護をしていくためには，情報システム部門だけが情報技術の導入対策に奔走しても実現できる次元のものではないことは既に自明の理である．

２．３．３　企業経営の領域

ビジネス環境の変化に伴い，企業の社会的責任がたかまり，一つの不祥事で企業が潰れるところまで追い込まれるような事例が現実のこととなってきている．

情報資産は情報システムの中にだけ完全に隠蔽されて，情報主体もしくは契約関係の利害関係者以外に露出されること無く処理されることは現実には有り得ない．情報セキュリティマネジメントは単に情報システム部門だけの問題課題ではなく，企業経営の領域の問題であると認識する．

したがって，当社は情報セキュリティマネジメントを継続的に運用改善していく，マネジメントシステムを重要と認識するに至り，経営者からの支持のもとに，ＩＳＭＳの構築

に着手することなった.

なお，上記の内容を整理する意味から，環境変化から情報マネジメントが重要であると認識するまでの関連を**図２**に示す.

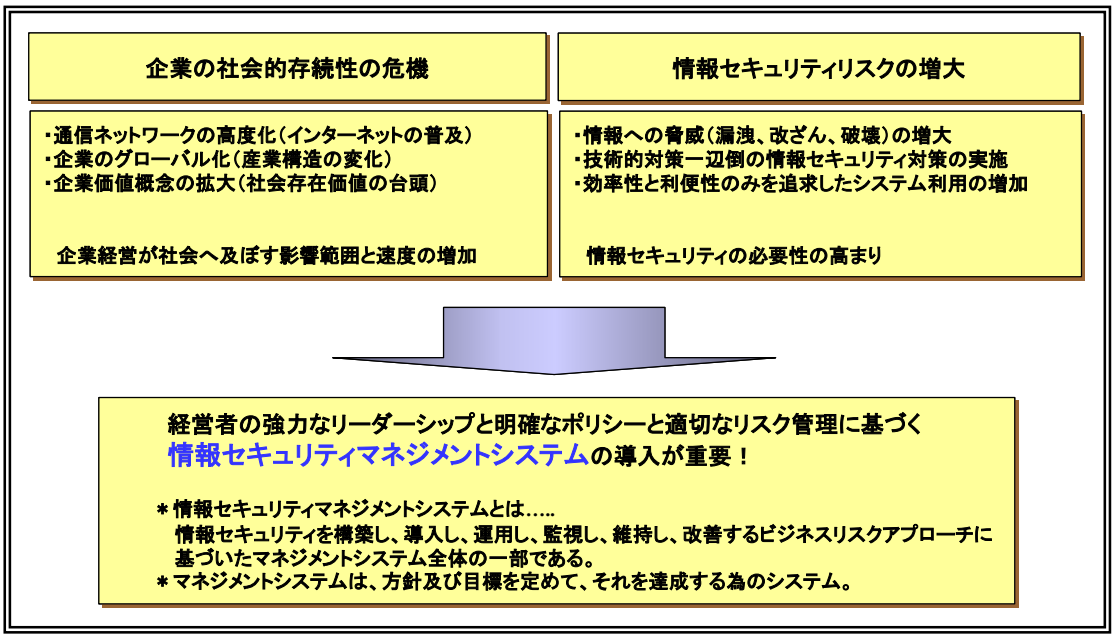

図２　情報セキュリティマネジメントシステムの重要性認識

３．ＩＳＭＳ導入前の状況（課題）

３．１　組織全体としての課題

情報処理システムの開発・運用を成熟した技術により専門化，分業化することにより，効率性，高生産性を追求した結果，縦割り構造組織運営を生まざるを得なくなってきた.

この組織構造は，部分最適になりがちな構造であり，全体バランスを必要とする情報セキュリティの側面から見るとリスクコントロールが適切に実施することが難しい体制及び態勢となっている.

また，その縦割型組織は，顧客の多様なニーズに応えるために必要な「サービス重視の観点」からもかけ離れた構造といえる.

組織全体の課題は生産性の向上／効率化から発生した縦割り組織運営を統括的（横串を通す）に連携をとる組織横断的活動の仕組みが欠けていると認識した.

３．２　各マネジメント層（経営層から現場担当まで）の課題

３．２．１　経営者層の悩み（未知との遭遇）

環境の急激な変化，特に消費者の企業に対する厳しい眼（要求）に対して，生産性とか効率性についての活動は熱心に行っているが，情報セキュリティリスクを総合的に把握できているのか？と言う疑問に対してハッキリと確信をもてない状況であった.

３．２．２　ミドルマネジメントの悩み

(1) 情報資産に対する責任範囲

自部門の管理保有する情報資産は何があり，どの程度の管理を実施すればよいのかの基準や明確な指示が無いことによる，不安があった．どこまでやればいいんだ？！

(2) 自己判断による担当者への指示

組織決定されていないセキュリティ判断基準による指示を業務担当者に出さざるを得ない状況か，または，生産性・効率性に相反するとして眼をつむる．もしくは，部分的な技術的対策を講じるに止まっていた．

３．２．３　業務担当者のセキュリティ意識

情報システムの開発・運用において，セキュリティを前面に押し出して設計・開発・運用を行う意識は少なかった．なぜならば，セキュリティ技術適用の教育は受けるけれども，それはシステムに組み込まれた機能としてとらえていた．

したがって，情報セキュリティに対する意識は一部危機にさらされた担当者が個人的に感じているものだった．

４．ＩＳＭＳ構築と運用

４．１　ＩＳＭＳ構築

(財)日本情報処理開発協会(JIPDEC)のＩＳＭＳ適合性評価制度で示されている構築ステップに準じて**図３**に示す構築ステップでＩＳＭＳを構築した．本論文では，**図３**に示すリスクアセスメント部分につてのみ記述する．その他の構築プロセスについての考慮事項は省略するが，『ＢＳ７７９９-２：２００２』及び『ＩＳＭＳ適合性評価制度』に準じ構築した．

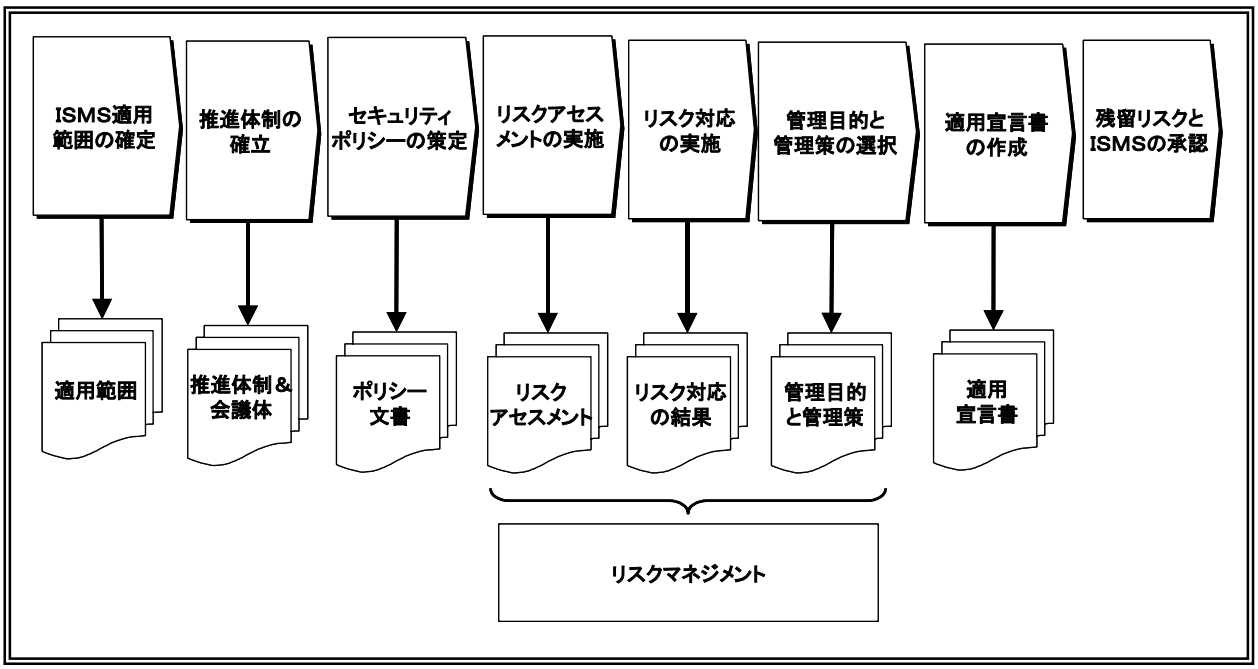

図３　構築ステップ

４．１．１　リスクアセスメントのポイント

ＩＳＭＳ構築プロセスで少しめんどくさい(時間がかかる)傾向にある，リスクアセスメントを行う上で特に留意した事項について説明する．

当社での基本的なリスクアセスメントの進め方は，**図４**に示すとおり情報セキュリティ管理基準（ＢＳ７７９９：Part１）との差分分析であるベースラインアプローチを最初に行い，重要と判断された部分について詳細リスク分析を行った．このアプローチにより，まずリスクアセスメント作業の全体像が把握でき重要資産の勘所がつかめた．

以下に説明する留意事項はこの詳細リスク分析についてのものである．

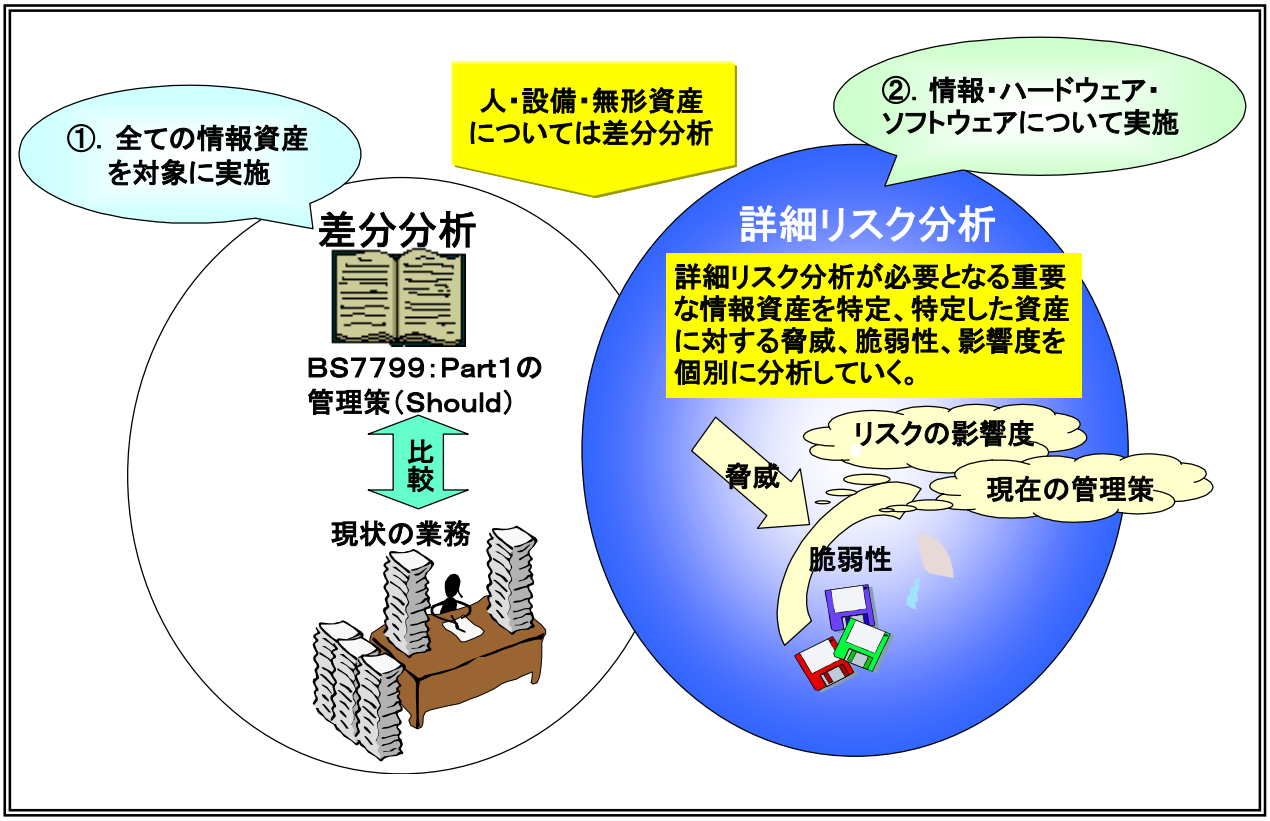

図４　当社のリスクアセスメント手順

（１）保護資産の抽出(資産の集約がポイント)

ＩＳＭＳは，情報資産に対してのセキュリティ対策を施すためのマネジメントシステムである．その出発点は保護資産(情報資産の中で保護すべき資産)をすべて洗い出すことだ．

保護資産の洗い出しに漏れがあれば，これ以降の分析の対象外になり，このこと自体が脅威にさらされた状態になることから，ここは十分時間をかけて組織の保護資産をすべて抽出する必要がある．

しかし，そんなにも十分な時間など無いのが一般的な組織の常である．

そこで当社では，保護資産の洗い出し漏れを防ぐためと，以降のリスク分析において同一種保護資産の重複分析避けるために，保護資産を分類(集約化)する基準を予め設けて各業務担当の眼で洗い出す方法をとった．資産分類はＯＳＩ参照モデル(７階層)

の考え方にあやかり，情報伝達が物理層からアプリケーション層にどのような形態を取りながら実行され処理されるかを分類のベースにし，①情報，②ソフトウェア，③ハードウェア，④文書類という四つの大分類に集約した．さらに各大分類ごとに小分類を４分類ぐらいに分割することにより業務担当者が資産をイメージし易いようにした．集約された保護資産の集約表を**表２**に示す．

表２　保護資産分類と集約件数

大分類	大分類の中でさらに取り扱いが同じものを集約した資産種類数	小分類の中で取り扱いが同じものを集約した資産数種類数	資産数
①情報	１２種類	１５０種類	２７６
②ソフトウェア	１１種類	５１種類	１４２ ＊1
③ハードウェア	１４種類	７３種類	５２４
④文書	７種類	６７種類	約５００
合計	４４種類	３４１種類	約１４００

＊　1：ＰＧＭ分割され複数本のＰＧＭは一つして集計している．

大まかな分類があることにより，情報資産を洗い出す過程で，この塊はというような集約する思考ができ全体像をイメージしながら作業が進み，洗い出し漏れ防止に役立った．

（２）保護資産への脅威は予め用意する(脅威データベース策定がポイント)

保護資産への脅威分析とは，上記で抽出識別された保護資産に対してどのような脅威(想定脅威)があるのかを明確にすることである．

脅威については，保護資産(媒体ごと／保存場所ごと／処理工程)の取り扱い方(ライフサイクル)に対して起こりうる不都合な状況を想定しながら予め当社の検討グループ内において別途討議を重ねて蓄積してきたものを脅威データベースとした．その脅威データベースへの格納数は２００３年６月現在で２１７ケースとなっている．脅威データベースの内訳を**表３**に示す．

表３　脅威データベース内訳(概要)

	脅威分類数	脅威数
情報	１０(格納場所による分類)	６１
機能	６(ｾｷｭﾘﾃｨ機能による分類)	７２
システム	６ (ｼｽﾃﾑ開発運用工程による分類)	８４
合計	２２	２１７

この洗い出した脅威数自体については，ハインリッヒの法則(*2)から言っても十分活用できるのではないかと考えている．

(*2:一件の重大災害の裏には，２９件のかすり傷程度の軽災害があり，さらにその裏には３００件ものひやりとした経験が存在している．潜在的な災害と顕在化する確率を経験則から導き出した法則，出展：失敗学の進め 著者　畑村洋太郎　P72)

脅威データベースは脅威内容及びその対策と言う構成になっておりリスク分析者は保護資産とこれを付き合わせることにより，個別保護資産の脅威ならびにその対策が選択可能な準備ができた．

４．１．２　脅威に対する脆弱性がリスクとなる

上記の保護資産に対する脅威の抽出結果に対して，既存のセキュティ対策の脆弱性(弱い部分)と脅威の発生度を明確にすることにより，保護資産に対しての当社が抱えるリスクの程度を明らかにした．リスクの程度をリスク値としてモデル１で求めた．

モデル１　　**リスク値＝保護資産価値×脅威の度合い×脆弱性**

（１）リスク値

リスク値モデル１の各変数の値は以下の方法で確定した．

a. 保護資産価値

経営者の経営的視点からの定性的な価値評価．

(定性的評価：対象保護資産における情報システム稼動への影響度とビジネスへの影響度を０～４の５段階で評価)

b. 脅威の度合い

予め用意した脅威データベースと保護資産の処理方法を比較して発生しうる脅威の度合いを**表４**(脅威の発生度)と対比し決定した．

表４　脅威の度合い(発生度)

レベル	内容
低	ほとんど発生しない。(１０年に１回)
中	発生の可能性は低い(数年に１回)
高	発生の可能性は高い(数ヶ月に１回)

c. 脆弱性

現状対策で脅威が現実のものとなる程度を**表５**(脆弱性の発生度)と運用状況を対比し決定した．

表５　脆弱性の程度

レベル	内容
低	ほとんど発生しない。(１００回に数回)
中	発生の可能性は低い(１０回に１回)
高	ほぼ発生する(数回に１回)

（2）残留リスク

許容できないリスク範囲値を事前に経営者との合意の上**表６**を定めた.

表６　リスク値マトリックス

	脅威の度合	低			中			高		
資産の価値	脆弱性の程度	低	中	高	低	中	高	低	中	高
	0	0	1	2	1	2	3	2	3	4
	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
	4	4	5	6	5	6	7	6	7	8

許容リスク
（リスク値＜４）

対策が必要
残留リスク
（リスク値≧４）

（3）残留リスクの経営者承認

ＩＳＭＳ推進グループ事務局サイドは，モデル１により保護資産ごとにリスク値を算出し，リスク値マトリックスとの突合せにより残留リスク(リスク値≧４)の存在する保護資産を選別した．この選別結果を再度，全体的に再レビューした後，経営者との協議のうえ経営者承認を得た．その結果，組織として許容できないリスク数を**表７**に示す．なお，一つの保護資産に対して複数の脅威と脆弱性が認識されたものもある.

表７　識別された脅威と脆弱性

保護資産分類	情報	ネットワーク	ソフトウェア	ハードウェア	文書	合計
リスク数	１０２	２１	４４	１９	２５	２１１

４．２　認証後のＩＳＭＳ運用状況

ＩＳＭＳ構築完了後運用を**図５**に示す．この大きなＰ(Plan)－Ｄ(Do)－Ｃ(Check)－Ａ(Act)のマネジメントサイクルでＩＳＭＳ適用範囲の情報資産のセキュリティ向上活動を開始した．

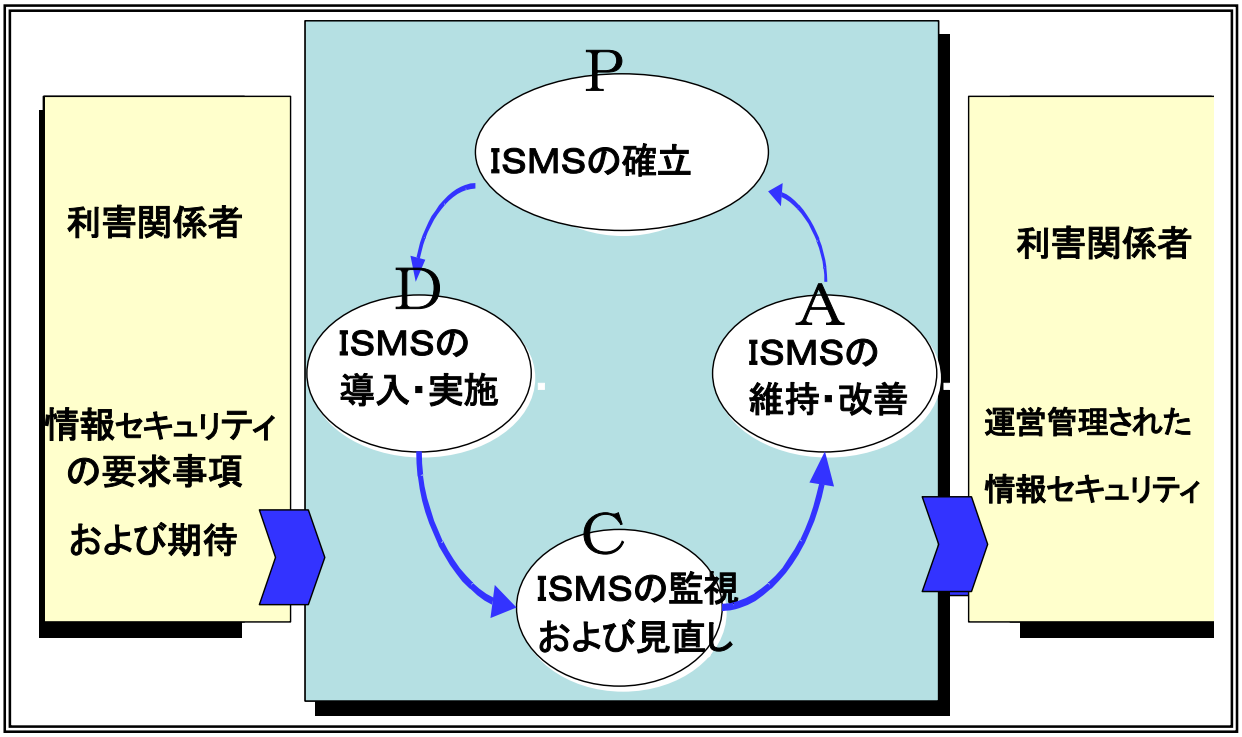

図５　ＩＳＭＳのプロセス

ＩＳＭＳのＰＤＣＡプロセスイメージを**図５**に示す．この中のＰ(ＩＳＭＳの確立)が４．１　ＩＳＭＳ構築で説明してきた部分になる．以降の説明では，**図５**のＤ以降について説明する．

４．２．１　業務に組み込まれたＩＳＭＳ

実践の場での業務は，具体的なシステムの企画設計・開発･保守運用のサイクルにあわせた活動が必要になってくる．上記の**図５**に対応した，より具体的なＩＳＭＳ活動プロセスを**図６**に示す．

業務上の活動にＩＳＭＳプロセスが埋め込まれた状態で業務を遂行している．

特にＩＳＭＳ実践で重要なことは，**図６**の中のＤＯプロセスにおける審査(システム変更等による新たなる脅威発生を認識し，その対応が取れているかを確認する組織内小活動)と**図６**の中のＣｈｅｃｋプロセスにおける内部監査(業務担当部署とは独立し，経営者から任命された監査責任者と監査人による，ＩＳＭＳが確実に実施運用されていることを確認する，組織内小活動)が挙げられる．

また，日々の業務運用の中での業務担当者の意識維持と事故の予兆を未然に発見する態勢支援が重要となる．

これらの活動全体状況が定期に実施している経営者の大きな判断を仰ぐマネジメントレ

ビューの重要なインプット情報として活用され次の改善活動につながっている.

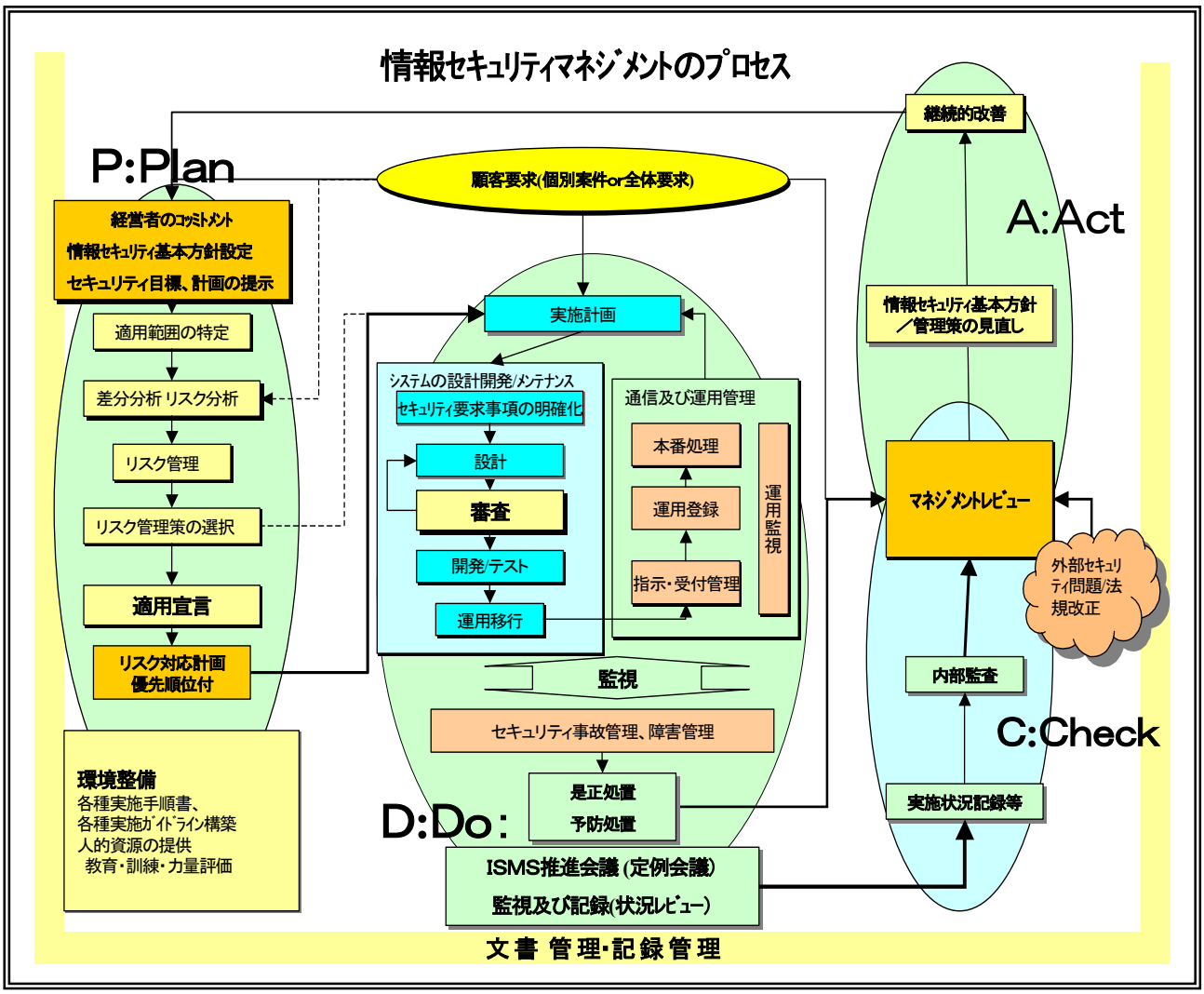

図６　当社のシステム開発運用プロセス

４．２．２　ＩＳＭＳ運用ポイント

ＩＳＭＳプロセスとして重要機能を説明したが，以下に，組織内において，実践で経験したＩＳＭＳ運営上重要なポイントをＩＳＭＳ運用ポイントとして説明する.

組織内におけるＩＳＭＳ推進上の必要なものとして以下の三つのポイントが掲げられる.

（１）ポイント１：情報セキュリティに対する強い意識の維持に向けた刺激策の設定

定期審査をクリアすることのためだけの小さな意識ではなく，自分たちの責任を果たすためのマネジメント活動を継続し，適切でセキュアなシステムを維持していくと言う強い意識を長期間もち続けることは実際には困難である.

それを克服するために，当社では具体的な刺激策を設定した.

刺激項目例：①社外で発生するセキュリティ事故の分析会開催

②内部監査の実施

また，当社では，①の活動として「法令に関する情報」，「セキュリティ事故に関する情報」，「使用製品に依存するセキュリティ関連情報」)を社内への情報として毎月１回発信している．その分析内容の件数傾向を**表８**に示す.

表８　セキュリティ分析傾向(2003 年 2 月～2004 年 3 月)

分析の種類	分析対象件数
法律・法令関連	６件（個人情報保護法関連が主)
セキュリティ事故	16 件(情報漏洩，システム停止関連)
セキュリティ全般(注意すべき情報)	5 件（ウィルス，不審ソフト･･･)
使用製品に対するセキュリティ関連情報	3 件

さらに，②の活動として社内の業務とは独立した部署で年一回の内部監査を実施することにより，ＩＳＭＳ活動の形骸化マンネリ化防止の一つの刺激策としている.

（２）ポイント２：技術革新/環境変化/組織変更などの新たな脅威への迅速な対応

一度構築したセキュリティ対策が永遠に有効に働くとは誰も思わないであろう.

社内システムのみならず，社外で起こる事故，環境の変化等をウォッチする仕組みを強化することで，新たなる脅威に対する業務システムの脆弱性とリスクの度合いを適時再認識することが必要である.

当社での具体的な強化活動としては，保護資産に対する新たな脅威が発生する要因，つまり，システム環境変更(ユーザー要件変更・追加，機器老朽化による機種変更，新規接続先発生　等)，組織変更(人事異動，組織統廃合　等)などが発生した都度，そのグループのセキュリティ責任者は変更に伴う審査依頼(**図６**の審査)をＩＳＭＳ推進グループ(**図７**　機密情報管理責任者)に申請し，新たなるリスク分析を実施する．これにより，システム環境変化，組織内変化に対応したタイムリーなリスク対策が計画される.

（３）ポイント３：管理するだけでなく支援する環境づくり

ＩＳＭＳプロセス(**図６**のＩＳＭＳプロセスの中のＤＯ)に具体的に組み込まれているＩＳＭＳ推進会議の推進役であるＩＳＭＳセキュリティ推進グループ(次章５．１の**図７**　ＩＳＭＳ推進体制)のメンバーがいつも心がけていることは，ＩＳＭＳを管理する道具ではなく，組織(各事業部，従業員)を支援する仕組みづくりに向けて常に改善していくことである.

人は誰しも，怒られるよりは褒められるほうが心地よい．情報セキュリティは社会・技術・制度・環境の変化により今までわれわれが経験したことのない未知の環境での出来事にどのように対処していくかという位置に立たされている.

未知の領域での失敗や障害を隠すのではなく，積極的に伝達，共有することができるポジティブ態勢を持つことは，組織にとって重大な事故を未然に防ぎ，不幸にも起きた事故に対しての有効に作用する．われわれは，そのことをを外部発生の事故とその対処を通じて学んだ.

５．ＩＳＭＳ導入後の変化・効用

５．１　組織構造上の変化と効用

５．１．１　組織横断的な体制

ＩＳＭＳセキュリティ推進グループの設立により３．１で述べた縦割り構造に横串しを通して全体バランスとれた組織横断的セキュリティ対策が経営者参画の上で立案が容易になった.

この組織要員は人事発令によりセキュリティ責任を明確にすると共に，このＩＳＭＳセキュリティ推進グループ責任者は経営者が担当することとした.

また，経営トップからの支持がＩＳＭＳセキュリティ推進グループを通して明確に伝達され，指示事項に対する実施報告が経営トップへ確実に伝達されることが周知され実行されている.

横串しを通す組織横断的かつ経営者直列体制であるＩＳＭＳ推進体制を**図７**に示す.

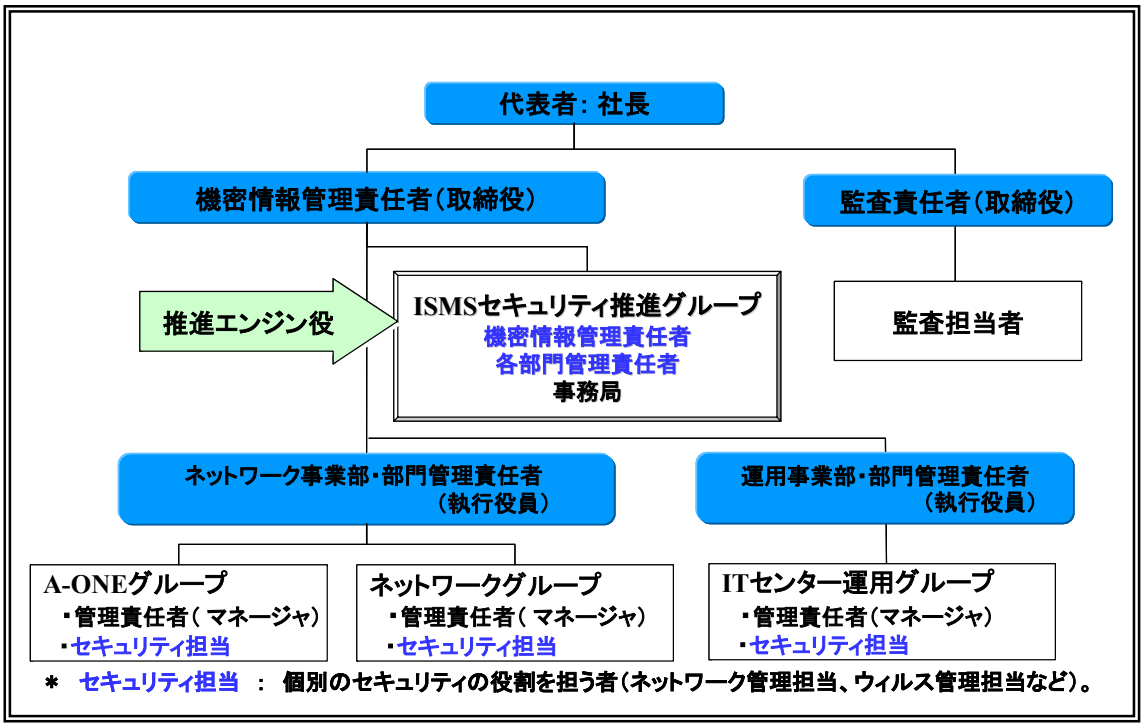

図７　ＩＳＭＳ推進体制

５．１．２　改善活動と効用

組織構造上の変化による効用は，ＩＳＭＳセキュリティ推進グループが主催するＩＳＭＳ推進会議（**図６**当社のシステム開発運用プロセス）での改善活動の中で現れてきている.

まず第一に改善事項の抽出が積極的に行われ，事前の対策が打てるようになってきた.

次に，組織的改善（役割の見直し等）が迅速に行われるようになった．ＩＳＭＳ推進会議は認証取得当初の６ヶ月間は一週間に１回のペースで開催した.

その後，落ち着き具合を見て隔週１回の開催で継続的改善事項を推進中である．これらについての現状を改善実績とその傾向分析を以下に述べる.

（1）改善実績

その改善管理状況を改善管理件数で**表９**に示す．また，その集計結果を分析する．

表９　改善管理分類と件数

改善分類	技術	組織	規則	調査	認証維持	ISMS運用	未計画	合計
設定件数	１７	１０	１２２	３４	2	３８	5	２２８
未解決件数	2	0	１９	0	0	4	5	３０

改善分類は，①技術，②組織，③規則，④調査，⑤認証維持，⑥ＩＳＭＳ運用，⑦未計画に分類して改善事項の推進状況を管理している．

各分類内容は**表１０**に示す．

表１０　改善分類

改善分類名称	内容
技術	システム的／技術的対応を要する改善事項
組織	組織体制及び組織に役割を追加して対応する改善事項
規則	ルール・手順の策定及び簡素化(身の丈化)をして対応する改善事項
調査	課題発生を起点に課題を単純化分解するための詳細調査を指す.
認証維持	ＢＳ７７９９認証取得・維持のために対応する改善事項(外部監査機関からの指摘事項対応)
ＩＳＭＳ運用	ＩＳＭＳのＰＤＣＡサイクルを確実に運用するための基準(機密区分)や運用スケジュール見直し
未計画	課題認識はできているが実施計画が立案されていない改善事項

（2）改善事項の分析

上記の**表９**が示すとおり，規則に関する改善と組織に関する改善を合わせると６０％近くあるということから分かるように，情報セキュリティの対策は技術的な対応ではなく，社内ルールや手順を確実に実施し，現場にあったやり方を見つけていくことが肝要である．

規則に関する未解決事項が未解決全体の６０％以上を占めているということは，これから各現場での改善に向けては身の丈にあった仕組みを策定していく活動を継続して実施する必要性を示している．（ＩＳＭＳ構築時にはオーバースペックの傾向があった．）

それに対して，組織に関する未解決件数が０件は，組織改善が経営者直列体制となったため問題が比較的早く解決ができるようになった結果である．

５．２　日常業務活動での変化

これまで述べてきた内容の総括的な位置付けとして，各マネジメント層(経営者層，ミド

ルマネジメント層，業務担当者)の意識がどのように変化したかを記述する．

まず，経営者層の意識の変化は，自社業務マネジメントに対する自信(信頼感)を持ち，顧客への説明性の確保，経営資源の最適な配分，ミドルマネジメントへの的確な指示と支持ができるようになった．(ＩＳＭＳは，何か利益を直接生むわけではなく，何も起こらないことが成果であるという点を経営者層と共有した．)

次に，ミドルマネジメント層の意識の変化は，自分の職務遂行(情報セキュリティ管理責任)における管理責任範囲内の情報資産が明確になり責任と権限が明確になったことにより，業務遂行の説明性が高まり，職務に対して自信が回復した．

最後に，業務担当者層の意識の変化は，日常の業務における情報セキュリティ意識の向上が挙げられる．「多少窮屈でめんどくさい．」という感覚，感情はどうしてもあるが，繰り返しの教育により，徐々に意識の向上が出てきて，教育方法，教材に対する要望が自発的に出てくるようになってきた．この要望に対しての第一弾としては，ＩＳＭＳハンドブック(五十音順の解説本)の作成と配布を実施した．

以上の意識の変化をイメージとして**図８**に示す．

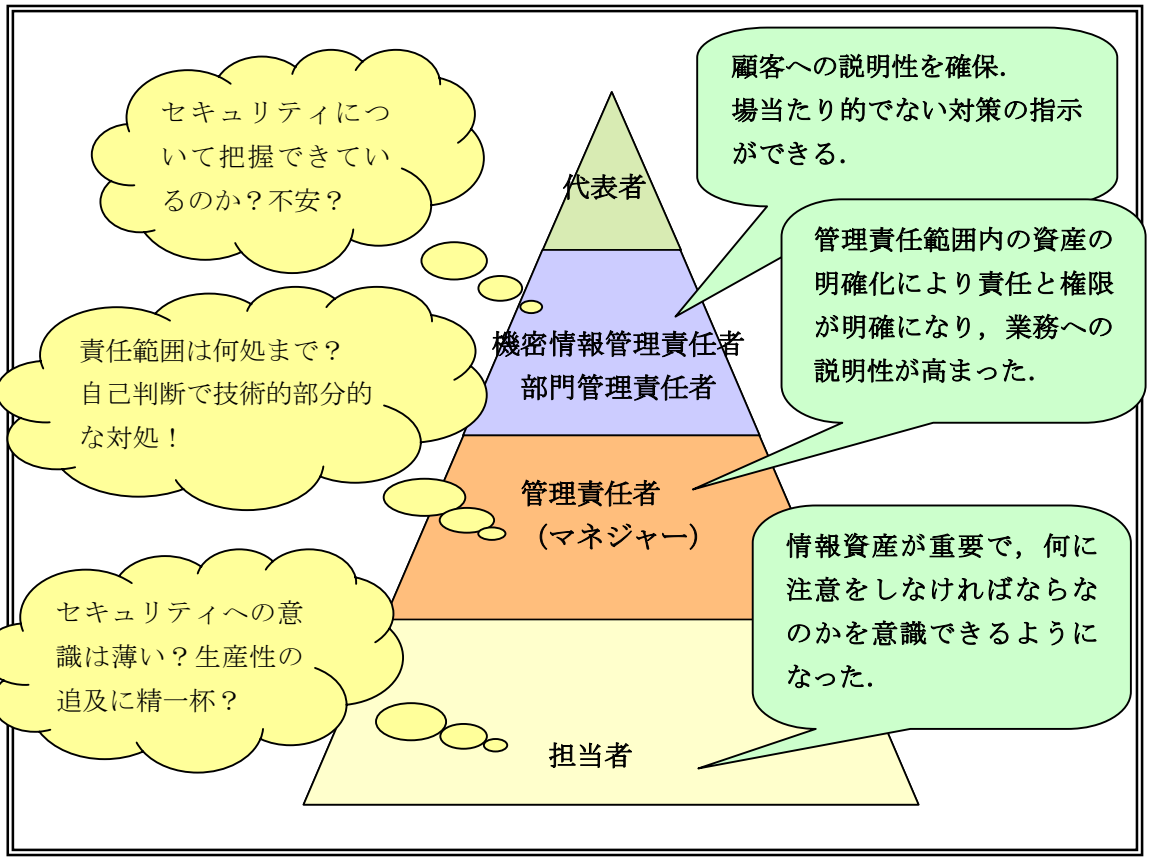

図８　意識の変化

６．今後の課題

６．１　ＩＳＭＳ導入後の現状認識

ＩＳＭＳを推進するという立場からは，やっと，ＩＳＭＳを有効に活用できるだろうスタートラインにつけたような認識です.

これからも，経営者が強い意識により組織全体を引っ張っていくことはいうまでもない.

それ以上に，セキュリティ障害・事故は１００％防げるものではないという前提で，ミドルマネジメントから担当者までが，障害・セキュリティ事故をポジティブにとらえ，隠すものではなく，セキュリティ障害・事故につながる日常感じた不安やドッキリ・ヒヤリを報告できる仕組みを組織文化として醸成することが最も必要である.

６．２　今後に残された課題

上記の認識を踏まえて，今後の課題の一つめは，**「脆弱性発見態勢の強化」**である．また，課題の二つめは，今始まったＩＳＭＳはほんの一部の部門サービス範囲である.

このＩＳＭＳ適用範囲をできるだけ早急に**「全部署へのＩＳＭＳ拡大展開」**をすることである.

６．３　課題に対するアプローチ方法

課題１『脆弱性発見態勢の強化』

脅威は専門的(化)してデータベースを整備すればよいかもしれない.

しかし，脆弱性については，自組織内のことであるから，外部(外部監査で一部指摘されることを除いて)から得られるものではない.

したがって，自らが深く注視しなくては見付けられない．では誰が，どのように見付けるかであるが，これはとても難しい.

６．１で述べたように，障害・事故・脆弱性は隠すものではなく，ポジティブに明らかにすることが重要であるということを浸透させ収集できる態勢を整える必要があると考える.

しかし，ポジティブに考えなさいということが中々浸透しない．その理由のひとつとしては，障害を起こした担当者，そのマネジャークラスは何らかのマイナス評価(業績評価)を受ける可能性があると感じており，これがなかなか浸透させるための弊害になっているようである.

したがって，事前に事故の予感したことを話し合える場所（コミュニティ）のようなものを設けて，各個人ではなく互助的な連携を作ることにより，言い易い環境，議論できる場所を整えることを思考中である.（まだ，答えが出ていない）

課題２『全部署へのＩＳＭＳ拡大展開』

速いスピードで拡大するということを実現することを最優先した方法をとる．具体的には，ＩＳＭＳプロセスのＣ(Check)プロセスの中の内部監査から拡大の切り口を見つけようとと考えている.（これについては，既にアプローチを開始した.）

７．おわりに

私個人としては，自社内の組織に埋没することなく，また，自己流のアプローチではなく，社会全体の流れの中で情報セキュリティに対する考え方，対応の仕方が社会に根付くためには，社会システムにセキュリティマネジメントシステムが組み込まれて，各階層(公助＞互助＞自助)で安全で安心にすごせる社会を目指して微力ながら尽くして生きたいと思っている．

理想論かもしれないが，個々の理想と理念をしっかり持って自助の努力，そして，そこで補えないものを互助の力で補っていかなければ，企業も個人も存続はありえない時代になってきたことをひしひしと感じながら筆を置くこととしたい．

最後に，私の口癖を述べたい．

≪セキュリティ文化の醸成≫

セキュリティは空気のようなもの，日ごろは何の気にもかけられないが，一旦なくなると，汚れると，苦しくなり大変困るもの．

あって当然なものがあるからこそ，いつまでもなくならないように，汚れないように，日ごろから環境にあわせて継続的に維持する活動をすることを再認識しています．

あたり前にあるものを，ある日，突然なくさないように！！

８．参考文献

［１］畑村洋太郎：“失敗学のすすめ”，講談社,
2004年3月4日　第19刷発行,P53，P59，P72-P73

［２］ISO/IEC 17799:2000 information technology - Code of practice for information security management
情報技術－情報セキュリティ管理実施基準　英和対訳版

［３］財団法人　日本規格協会　JIS x 5080
情報技術－情報セキュリティマネジメントの実践のための規範

［４］財団法人　日本情報処理開発協会，ＩＳＭＳ認証基準(Ver. 2.0)