

情報資産を守る I S M S 導入支援

独自の雛形とテンプレートを使って、的確・迅速にシステムを構築する

(有)シグマアイ・コンサルティング 太島 将義

E-mail : oshima@cityfujisawa.ne.jp

URL : <http://cityfujisawa.ne.jp/~oshima/>

昨今の個人情報の漏洩問題は、企業のリスクマネジメントに重大な影響を与えている。企業は個人情報のみならず、自社および関係各社の「営業機密情報」を保有している。もし「個人情報」や「営業機密情報」が漏洩することになれば、取引停止や損害賠償、風評被害などの事態に陥る可能性がある。これらの情報のセキュリティ管理は企業の責務であり、すなわち経営者の責務である。

シグマアイの「I S M S 導入支援プログラム」は無駄な文書作成を極力排除し、I S M S の情報セキュリティの精神を実現すべく、実践的なプログラムを提供する。

1 . 頻発する情報流出事故

(1) 情報セキュリティなど関係ないとお考えではないですか？

情報システムの活用の範囲はどんどん広がっている。また社会の変化につれて、情報システムに求められるものの質も変化する。こういったなかで新たな問題が生まれるのである。重要なことは、情報の漏洩や流出が、企業経営に大きな影響を与え始めたことである。高速化、ボーダレス

表1 最近の主な顧客情報紛失・流出事件

企 業 名	発覚時期	流出規模	顧客への主な対応
ローソン	03年6月	約56万人	会員に500円の商品券と謝罪文送付
アプラス	03年8月	約8万人	千円の商品券と謝罪文送付
日本信販	03年8月	約2400人	謝罪文を送付
JCB、UFJカード	03年8月	約7千人	カード再発行と千円の商品券送付
ファミリーマート	03年11月	約18万人	千円のプリペイドカードと謝罪文送付
NTTデータ	03年12月	約4300人	謝罪文を送付
三洋信販	04年1月	約32万人	24時間の相談受け付け
ソフトバンクBB	04年2月	約451万人	会員に500円相当の金券配布
ジャパネットたかた	04年3月	約30万人	販売自粛
アッカ・ネットワークス	04年3月	30万人以上	電話相談受け付け

化、高度情報化など、経営環境が複雑化する中で、経営情報のセキュリティに関するトラブルが急増している。

トラブルの様態や程度はさまざまであるが、時には経営者の引責辞任や個人賠償、あるいは、経営崩壊や経営権譲渡などにつながる大きな社会問題になっている。このように高度情報化社会に付随するさまざまな混乱要素に対して、社会性の高い企業には、情報セキュリティについてもより高度で普遍性の高い経営システムが求められている。

中小企業の場合は新聞沙汰になる事はないが、得意先の情報が流出したら即取引停止の危険がある。

(2) 2003年度の顧客名簿流出による被害額

NPO日本ネットワークセキュリティ協会の調べによると調査対象57件の被害推定総額は280億円を超える。1件当たりでは5億5千万円にもなる。1件当たりの被害者数は平均3万482人になっている。

表2 2003年の情報漏洩による推定損害額

件数	57件
損害賠償総額	280億6936万円
一件当たりの平均損害賠償額	5億5038万円
被害者数(合計)	155万4592人
(平均)	3万482人

一般に4つの基本情報(氏名、住所、生年月日、性別)だけでも一人当たり1万円といった損害賠償額になるといわれている(宇治市の例)。

情報の種類が多様になり、過去の取引履歴や個人の趣味・嗜好、さらには資産状況、信用情報などといった重要情報が含まれた場合には大幅に高騰すると考えられる。加えて、個人身体的特徴(下着メーカー、エステなどからの情報漏えい事件)、病歴、投薬の内容など(医薬品メーカーや病院、レセプト処理サービス事業者など)の場合を想定すると、想像を超える金額になると思われる。

(3) 最近の主な情報漏洩事件例

① 京都宇治市の例

98年ころ京都宇治市が「あるシステムの構築」を民間事業者が発注したが、民間事業者は順次下請けに出し、末端の学生アルバイトが情報22万件を漏洩したもの。2001年12月25日大阪高裁は、京都地裁に引き続き個人情報漏洩の責任が宇治市にあると判断し、宇治市に対し住民に損害賠償をするよう命じた。その損害額は、1名あたり1万5000円と認定され、その内訳は慰謝料1万円、弁護士手数料5000円というものであった。

この訴訟の申し立て人は3人であり宇治市の実際の支払い賠償額は4万5千円であった。1人あたりの賠償金が1万5000円としても、すべての住民が訴えたら28億5000万円という途方もない金額になる。もちろん、賠償金以外にも、被害者への個別連絡や問い合わせ対応にかかる費用、

被害実態の調査にかかる費用なども必要となる。

② ソフトバンク BB の例

ソフトバンク BB は情報漏洩対策に総額で 40 億円を投じる。40 億円といえば相当大規模なシステムの新規開発に相当する金額である。またソフトバンク BB の情報漏洩が明らかになってから、ソフトバンク BB の Yahoo!BB を解約して他社のサービスに乗り換えるユーザーが激増しているという話がある。情報漏洩の影響がどこまであるかは不明だが、Yahoo!BB の利用者の伸びも鈍化している

③ ジャパネットたかたの例

ジャパネットたかたは、漏洩発覚時点で全業務を停止、原因究明に努めた。情報漏洩後、3月9日より4月25日まで、47日間（1.5ヶ月）のインターネットによる営業の停止を行った。この間の業務停止による被害金額は、年間売上高 700 億円で考えると、87.5 億円であった。

（4）新法公布と社会的関心

情報セキュリティに世間が注目し始めたのは「個人情報保護法」の成立・実施（平成 15 年 5 月 30 日公布・1 部施行、平成 17 年 4 月 1 日全面施行）が発端となっている。それまでも「不正アクセス禁止法」や「不正競争防止法」で情報の不正入手を禁止する法律はあったが、その存在は広く世間の注目にさらされる事はなかった。

① 個人情報保護法

この法律は高度情報通信社会の進展に伴い個人情報の利用が著しく拡大するなか、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的に成立した。その基本理念として「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであり、その適正な取扱いが図られなければならない」としている。

表 3 個人情報保護法の規定事項

- | |
|---|
| <ul style="list-style-type: none">・利用目的の特定、利用目的による制限・適正な取得、取得に際しての利用目的の通知等・データ内容の正確性の確保・安全管理措置、従業者・委託先の監督・第三者への提供の制限・公表等、開示、訂正等、利用停止等・苦情の処理 |
|---|

本人の意図しない個人情報の不正な流用や、個人情報を扱う事業者がずさんなデータ管理をしないように、一定数以上の個人情報を取り扱う事業者を対象に義務を課す法律である。社員情報を含め 5000 名を超える個人情報を保持する「個人情報取扱い事業者」に対して罰則を規定しており、表 3 の 7 項目が定められている。

② 不正アクセス禁止法

不正アクセス禁止法は、「ID・パスワードの不正な使用」や「そのほかの攻撃手法」によってアクセス権限のないコンピュータ資源へのアクセスを行うことを犯罪として定義するものである。

不正アクセス禁止法の目的は以下のようになる。

この条文の骨子は「ネットワークを利用してほかの端末に不正行為が行われることを防止したり、アクセス制御を越えて権限のないコンピュータ資源へアクセスするなどのハッキングに代表される行為を犯罪として定義し、罰することを規定することで秩序を守り、それがネットワーク社会の正常な発展につながる」ということである。罰則は1年以下の懲役または50万円以下の罰金である。

③ 不正競争防止法

この法律の中では、不正競争となる15種類の行為が定められており、これらの行為によって、営業上の利益が侵害された場合、行為の停止や予防の請求（差止請求）および損害賠償を請求することができる。情報セキュリティに関連する「不正競争」とは「窃取、詐欺、脅迫その他の不正の手段により営業秘密を取得する行為、又は不正取得行為により取得した営業秘密を使用し、若しくは開示する行為」とされている。

この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいい、「不正競争」によって生じた損害を賠償する責任がある。

2. 企業の持続的発展のために

(1) 企業のリスクマネジメント

企業は、さまざまなリスクを抱えながら事業の運営を行っている。むしろリスクの上に経営が成り立っているといっても過言ではない。このリスクの発生をできるだけ少なくし、もしもリスクが発生した場合、その影響を最小限にとどめるようにすることが、リスクマネジメントである。情報セキュリティも企業のリスクマネジメントの一環としてとりあげなければならない。

表4 情報セキュリティで守るべきもの

1	関連設備	建物、電源、空調設備、監視設備等
2	ハードウェア	コンピュータ機器、ネットワーク機器等
3	ソフトウェア	基本ソフト、アプリケーションソフト等
4	情報	IT情報、印刷物等
5	人	関連要員

発生が予想されるリスクには、地震、豪雨・豪雪、風水害など避けることの難しい自然災害と、製造過程での異物の混入や不良品の発生、情報の漏洩や粉飾決算など、管理体制の不備や意図的な不正行為といった、避けようと思えば避けられる人為的なリスクがある。

自然災害の場合、発生を想定し、中長期的な視点に立った対応策、防衛策が必要になる。

しかし、人為的なリスクの場合、どんなリスクが発生するのかを事前に予測することが難しく、発生したリスクの内容にもよるが、企業のモラルが問われるような場合には、いったんその事実

がマスコミなどに取り上げられて公になると、企業の存続すら危うくなるケースが増えている。

発生したリスクによる損失は、補償や賠償などに要する直接的な金銭もあるが、それ以上に、信用の失墜がその後の企業経営に大きな影響を及ぼす。

人為的なリスクのセキュリティ対策として、不正侵入、盗聴・漏洩、ウイルスなどすべての脅威に対応しようとする、多大な人手とコストがかかる。また、予想される被害の発生頻度と金額によってとるべき対策の優先度は変わる。

リスクマネジメントにより、危険の局所化と最小化を行い、何を守るのか、何から守るのか、どのように守るのかなど、企業／組織としてのセキュリティポリシーを明確にした上で、経営資源の効率的な活用を考え、そのポリシーにもとづいたセキュリティ対策を行うことが重要である。

(2) 情報セキュリティの確立は経営者の責務

現代の企業のリスクマネジメントは、自社のリスクに対する姿勢を明確な基準として全社員で認識、共有するとともに、これを実現する体制を整え、さらにリスクマネジメントに情報システムをどう組み込み、活用するかが大きな鍵を握るようになってきた。

① 情報セキュリティ経営システムの必要性

経営者は情報の資産価値と直面しているリスクについて次の特性を認識しなければならない。

- 情報は、会社の重要な資産であり、事業継続性のカナメである。

得意先関係では顧客名簿、図面類などの顧客財産、自社関係では設計・技術資料、作業手順書のような情報など

- 情報は、脅威に曝されている。

システム利用者による情報漏洩、ハードウェア障害、ウイルス、ハッキング（クラッキング）、使用不能攻撃(DOS)など

- 従業員、パート、下請け会社従業員が最大の脅威となりうる。

不注意によるデータの削除、内部犯行による顧客情報の盗難・流出、違法な情報の隠蔽・改ざん操作、内部告発など

- 情報に必要な「機密性」、「完全性」及び「利用の可能性」のバランス管理の必要性

これらの特性は中小企業においても該当し、得意先などの情報がパソコンから容易に大容量記憶媒体に書き出され・持ち出しができることを考えると、中小企業の方が危険は大きい。

以上のような事柄への対策を含めたセキュリティを確保するために情報セキュリティシステムの確立が不可欠である。

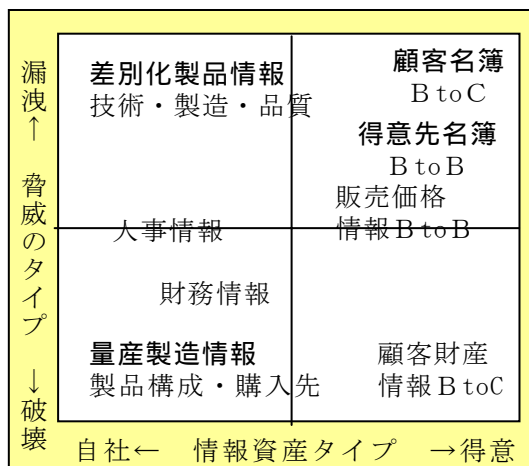


図1 情報資産のタイプ

② 経営トップのリーダーシップが欠かせない

こういった問題に取り組むには、システム関係者だけでなく、営業部門や工場部門の協力が必要である。また複数の部門をまとめて進めていくには経営トップのリーダーシップが欠かせない。

しかし事故が起こってからあわてて対策を練ったりソフトを導入したりしても遅いわけで、まず「事故を前提とする社会」「セキュリティ対策に完全はない」という認識に立って、事前に対策を立てておくことが重要なのである。

そのような仕組み作るのが「情報セキュリティ管理システム（ISMS）」である。

3 . I S M S （情報セキュリティマネジメントシステム）とは？

(1) I S M S の仕組み

経営は今や情報なくして成り立たない。組織活動のインフラとして情報セキュリティ確保は不可欠な要素となっている。ISMSを導入して得意先、取引先に属する情報資産と自社の存立基盤に係わる情報資産の「漏洩、破壊」を防御することが、会社としての責任と万一のリスク回避のために必要である。

ISMSは英国の規格 BS7799-2 をもとに作成されており、情報に必要な「機密性」、「完全性」および「利用の可能性」のバランス管理に必要なマネジメントシステムを規定したものである。

ISMSは「情報セキュリティに関して、企業の方針・目標を定め、情報資産を評価し、リスク対応計画を作成し目標が達成できるようにPDCAを回していく仕組み」である。

この仕組みは ISO14001 環境規格と酷似しており、環境規格が「環境負荷の影響度」を評価してその改善計画を立てるのに対し、ISMSは「情報資産を評価」してリスク対応計画を立てるというように、対象が異なるだけである。

ISMSでは127項目の管理策（情報を守るための対応策の例）が規定されていて、管理策は企業の実情に合わせて、取捨選択できることになっている。

ISMSは企業の方針・目標で示した情報セキュリティ対策が適切に実行されているか、不十分な点はないかを監視し、PDCAのサイクルを回して継続的に改善する。しかもそれが確実に行われているかを第三者の専門機関から認証を得る制度であるため、内部での活動の励みになり、外部に対しては基本方針の公約の実行が証明される。これが「ISMS適合性評価制度」である。

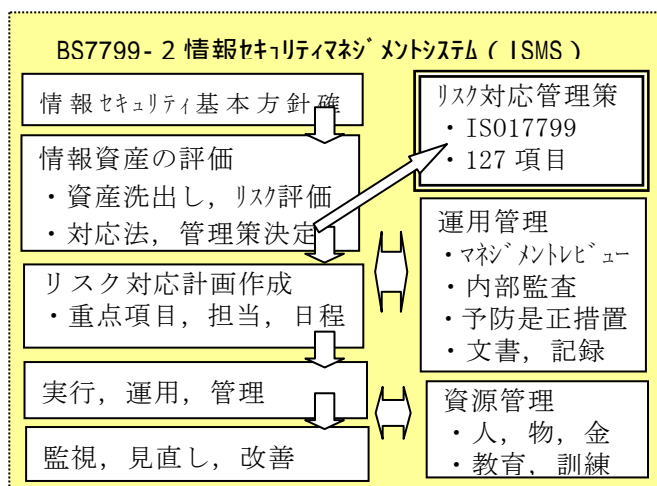


図2 ISMSの体系図

(2) ISMSの期待効果

ISMS構築の目的は情報セキュリティの確立にあるが、基本的には、「顧客信頼」と事業継続に係わる「リスクを回避」して、企業の「社会的責任」を果たすものであり、次の効果が期待される。

- ① 得意先の信頼の確保：お客から「この会社なら安心（企業イメージ向上）」と考えて貰え、重要ユニットや部品の「発注や情報提供」を頂ける可能性が増す。
- ② 社内のITレベルの向上：情報には「機密性」の高低や「事故発生時の影響」の大小があることが社内に浸透し、社内の「情報資産」を守ると共に、社内のIT関連の業務規範が形成できる。
- ③ 事業継続性・安定性の確保：事故による「取引停止・損害賠償」や業界での「風評被害の拡大」など会社存続に係わるリスクを軽減できる。

4. シグマアイのISMS導入支援

シグマアイは顧客の企業実態に合わせたISMS導入のため、図の支援ツールを用意している。

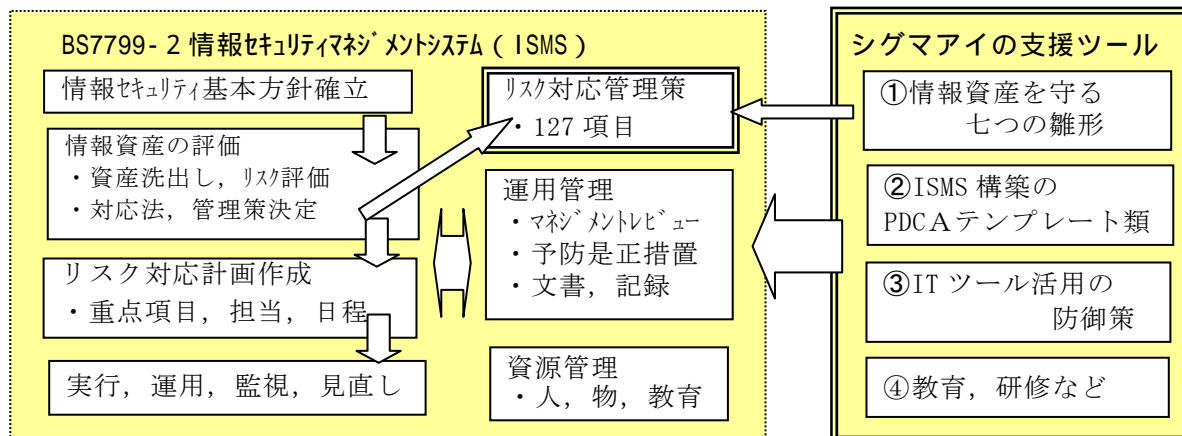


図3 シグマアイが構築支援するISMSの体系図

これらは情報資産を守るノウハウやISMSのPDCAの回し方などを組み込んだ「雛形とテンプレート類」であり、専門家が少ない中小企業のISMS導入支援を狙いとするものである。

(1) シグマアイのISMS導入支援の特徴

シグマアイがグループの力を結集して開発した「雛形・テンプレート類」を使って、的確・迅速にシステム構築を行う。大量の「文章形式の文書」は作らない。

① 経営方針と整合をとる

IT技術に精通した経営コンサルタントの立場から、経営方針と社内情報化の現状の双方を踏

まえて的確なシステム構築を行う。

② 現場運用と雛形・テンプレートを適合理化させる

情報資産の「質と量」の実態にもとづき、シグマアイが用意した「雛形・テンプレート」を現場の運用に適合理化して迅速にシステム構築を行う。

③ ITツールの組み込み

より高い安全性が求められる場合は、必要に応じ、ITツールの情報漏えい防御・抑止機能をパートナーと協働してシステムに組み込む。

(2) シグマアイのISMS導入支援サービスメニュー

シグマアイは情報セキュリティ基本方針確立から始まって、情報資産の評価、リスク対応計画、実行、運用さらに監視、見直し、改善までのISMSプロセスの全般にわたって支援するため、次のサービスメニューを用意している。

表5 シグマアイのサービスメニュー

1	ISMS研修：経営層、導入責任者向け
2	情報資産およびリスクの評価
3	リスク対応管理策の構築
4	ISMSの構築
5	社内教育
6	内部監査員教育
7	ITを活用した防御策

① ISMS研修

経営層、導入責任者向けにISMSの重要性、考え方から計画、実施、改善にいたる責任や体制の確立についての研修を行う。

② 情報資産およびリスクの評価

情報資産の洗い出し、情報資産の価値評価、リスク分析、リスクの評価を情報資産評価フォームを使用して行う。最終的には適用宣言書を作成する。この作業は一般的に多くの作業量を要し、また初めて導入する時には資産価値の評価、想定リスク等困惑する点が多いが、テンプレートを使用して作業の円滑化を図る。

③ リスク対応管理策構築：七つの雛形

情報資産を守るリスク対応の管理策として表6に示す雛形を用意した。

表6 リスクに対応する管理策の「七つの雛形」

項	雛形など	目的、内容
1	基本方針	情報セキュリティ取り組みの社長方針
2	組織運用規定	ISMS委員会、担当、助言者など
3	情報資産及びリスク評価運用規定	資産一覧、資産価値、想定リスク、対応水準（テンプレート）
4	個人遵守事項管理規定	ウィルス対策、電子媒体扱い、メール処理、罰則規定
5	社内情報システム運用管理規定	サーバ保全、入退室、利用者アクセス、バックアップ、監視記録
6	事故対応管理規定	事業継続計画、予防、回復など
7	適合性管理規定	法的・社内要求、点検、監査

これらの文書はISMSの運用において守るべき事項を規定した文書の雛形である。これら「七つの雛形」はお客様の企業の実情にあわせて修正し、実施可能な管理策として定める。

元々の規格では127項目の管理策が推奨

されているが、小規模の中小企業向けに必要な項目だけを取り出し、同時に「対象者別、用途別」で括って、使い易い規定書としてある。

なお雛形とテンプレートの違いは、

- 雛形は具体的なサンプル文書であり、それを使用時に企業の実態に合わせて修正して使う。
- テンプレートは計画書、報告書などの「空の書式（フォーム）」であり、該当する管理段階でそれらに記入して使用する形式であり、そこに I SMS 構築のノウハウ・要点を組み込んで、中小企業における便宜をはかるものである。

④ I SMS の構築：テンプレート類

I SMS は継続的に P D C A を回し、情報セキュリティの不断の改善活動を行わなければならない。シグマアイはこの P D C A を回すことが容易に出来るように 8 種類のテンプレートを用意した。

P D C A の各アクティビティごとに適切なテンプレートに書き込むだけで、漏れや無駄のない P D C A を回す仕組みを作ることが出来る。

例えば、まずテンプレートの資産評価フォームを使って守るべき情報資産を決定し、そのセキュリティを確保する「雛形」を選定・実情に合わせて修正して規定書として制定する。それらをまとめたものが「適用宣言書」である。

規定書でただちに実行できるものは実行に移すが、情報保護の I T ツールの導入など時間と経営資源を要するものは「リスク対応計画」を立てて実行し、進捗を管理する。

それら全体の活動を内部監査、マネジメントレビューなどのテンプレートを使って管理する。

⑤ 社内教育

I SMS では全従業員を対象とした情報セキュリティの教育を定期的（年 1 回程度）に行う事が義務付けられている。これについて、情報セキュリティの一般的知識を教育するとともに、情報資産に対する意識の向上をはかる。

表 7 I SMS の P D C A を回すテンプレート

項	テンプレート	目的、内容
1	情報セキュリティマニュアル	情報セキュリティ取組みの憲法、活動の枠組み・基本事項を明示
2	情報資産評価フォーム	資産一覧、資産価値、想定リスク、対応水準等（雛形の 3 項と同じ）
3	リスク対応計画書	テーマ毎の年度「実行計画書」
4	マネジメントレビュー計画書兼記録	インプット情報、レビュー項目、レビュー結果
5	内部監査計画書兼報告書	対象範囲・部門・項目・時期、前回の問題点、実施結果・要改善点
6	教育計画書兼記録	対象職務・スキル・対象者、実施内容・時期、実施結果・評価
7	諸措置報告書	事故及び是正・予防等措置報告書
8	文書及び記録管理	承認・識別・配付・廃却等の管理 対象文書一覧+管理規定

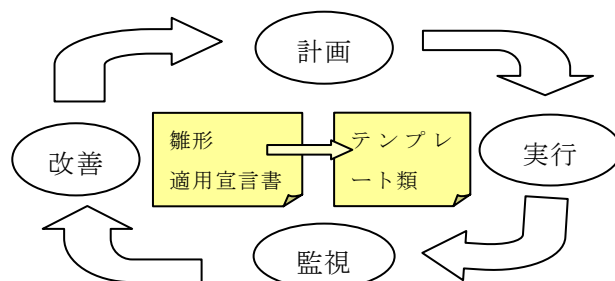


図 4 I SMS の P D C A

⑥ 内部監査員教育

内部監査員向けに、内部監査として情報セキュリティの立場からどのような観点から監査すべきかを教育する。

I S M S が日常の業務活動の中に定着するかどうかは、定期的に行う内部監査の「有効性」如何にかかっているため、特別にこの教育メニューを用意してある。

⑦ I T を活用した防御策

情報漏えいなどの情報セキュリティの確立のため、ハードウェア、ソフトウェアを活用してより確実に、情報漏えいの防止や監視を行うことが必要な場合がある。

具体的には、「データの大容量媒体への書き出しの禁止」「データごとの閲覧、編集、印刷などの監視・記録」や「電子メールのやりとりの監視・記録」、「システムへのアクセスやログオンの管理」等がある。これらの場合、シグマアイのパートナーと連携してそれらをシステムに組み込む。

(3) 導入スケジュール

代表的な I S M S 構築・認証取得支援のスケジュール例を図 5 に示す。ただし実際は企業規模、対象部門、現在の管理レベルなどで異なるので、プロジェクトごとに日程決定を行う。

作業項目	月数	1	2	3	4	5	6	7	8	9	10	11	12
基本方針、情報資産の評価、管理策		→											
リスク対応計画作成				→									
ISMS 管理システム構築				→									
実行、運用、監視、見直し、改善							→						
教育・訓練		▲						▲		▲			
予備審査、文書審査、実地審査									▲			▲	▲

図 5 ISMS 導入支援スケジュール

5 . (株) シグマアイ・コンサルティングのプロフィール

当社は 2000 年に統合生産管理システム T P i C S を導入するグループ (T P i C S 研究所の登録 S I) としてスタートし 2003 年 9 月に法人化した。現メンバーは、情報系製造業出身の中小企業診断士を主体に 7 名である。E R P は「電子台帳化・全社即時情報共有」をベースに業務改革を進める強力なツールであるが、同時に情報面でのリスクがある。従って E R P と I S M S を「コインの裏表」として対応する必要があるとの考えから、I S M S 構築支援も開始した。