

FIP IT BOX

Vol.26

Contents

2004年 7月23日 発行

■ 企業を脅かすITリスクへの処方箋

組織が直面するリスク
 拡大するITリスクの脅威
 求められるITリスクマネジメント
 FIPが提供するITリスクマネジメントソリューション

富士通エフ・アイ・ビー株式会社

東京都港区芝浦1-2-1 (シーパンスN館)
 パブリシティ推進部
 連絡先 03-5730-0707 info@fip.fujitsu.com
 URL http://www.fip.fujitsu.com/

ISMS

企業を脅かすITリスクへの処方箋

「リスク^{*1}」という言葉から何を想像しますか？
 「リスク」や「リスク管理」という言葉はすっかり
 社会に浸透しましたが、具体的にはどのようなもの
 なのでしょう。

企業や自治体・政府・学校などの組織は、急激な
 技術進歩・事業の国際化といった外的要因や、環境
 問題などに対応する社会的規制により、現在、多種
 多様なリスクにさらされています。(図1)

万一リスクへの対応を怠った場合、組織はそのス
 テークホルダー^{*2}に広範な損失を与えるだけでなく、
 市場での信頼喪失などの厳しいペナルティを受ける
 ことになります。このような状況の中で、リスクに
 対する意識も、次に示すように変化してきました。

【図1: 多様化するリスク】

X 企業が直面する様々なリスク(企業のリスクマネジメント対象例)	
保険リスク	大災害による財産損害/事業中断/雇用者賠償 など
業務リスク	ビジネス戦略の誤り/地域経済の諸問題 など
財務リスク	経理システムの故障/ハッカーによる攻撃 など
コンプライアンス	独禁法/会社法に対する違反/罰則税制 など
オペレーショナル・リスク等	新製品またはサービスの失敗/原材料の欠乏/機密漏洩 など

出典：(株)MSK 基礎研究所「リスクマネジメントの効能とそれを支えるスキル」

- (1) リスクは「避ける」から「受け止める」へ
 - (2) 「損失の回避・軽減」から
「価値の維持向上」へ
 - (3) 「組織の利益」から
「ステークホルダー、社会の利益」へ
 - (4) 「個別のリスク対応」から「全リスク対応」へ
- そして、組織の価値を維持・増大していくために、
 組織が経営・運営を行なっていく上で、事業に関連
 する内外の多様なリスクを適切に積極的に管理する
 活動が、リスクマネジメントです。

今や組織は、自らの判断でリスクを引き受け、管理
 し、収益を上げていくことを求められているのです。

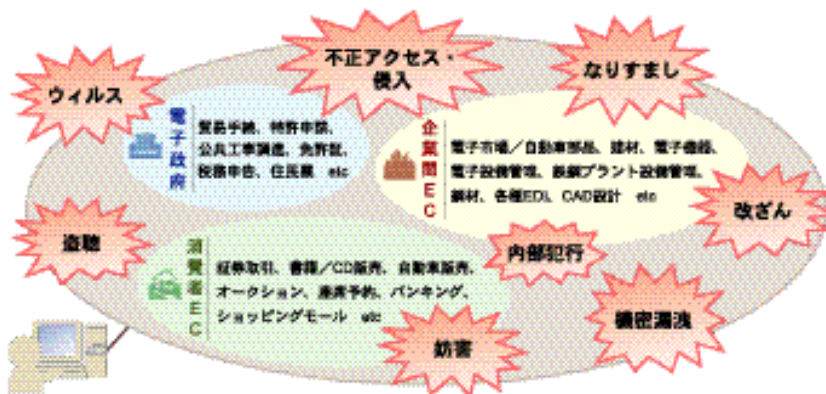
*1: ある脅威が、資産または資産グループの脆弱性を利用し、資産へ
 の損失、または損害を与える可能性

*2: stakeholder (企業に対して利害関係を持つ人。社
 員や顧客・消費者や株主だけでなく、地域社会までも
 も含めて言う場合が多い)

ITリスクとは

情報システムはネットワークで外部
 に接続されると同時に、不正アクセス
 やウィルス感染・情報改ざんといった
 外部的な危険や、情報資産の私的利用・

【図2: 組織を脅かすITリスク】



参考：セコムトラストネット（株）ホームページ

情報漏洩といった内部的な危険にさらされます。ひとたび情報システムの危険を軽視し、放置してしまうと、被害の出所として社会的責任^{*3}を問われ、名誉や信頼性を損ねるだけでなく、最悪の場合、組織の安定性や存続が危ぶまれてしまいます。（図2）

現在、情報システムには、信頼性や安全性が強く求められています。

^{*3}: イギリスやフランスでの上場企業に対する環境・社会的活動に関する情報開示の義務づけなど、企業の社会的責任(CSR: Corporate Social Responsibility)がクローズアップされ、日本国内でもCSRへの関心が高まっている。また、2003年には国際標準化機構(ISO)によるCSRに関する標準化検討も始まっている。

高まるITリスクマネジメントへの需要

このような風潮の中で、情報システムに関するリスクへの関心も高まり、情報セキュリティマネジメントシステムにおけるリスクマネジメント（以下、ITリスクマネジメント）という考え方が生まれました。

ITリスクマネジメントが重要視され始めた中、すべての事業者を対象とした情報システムのセキュリティ管理に関する第三者認証制度^{*4}として、通商産業省(現 経済産業省)が認定する安全対策事業所認定制度に代わり、新たにISMS適合性評価制度^{*5}が制定されました。(BS7799^{*6}に準拠)

^{*4}: ISMS は(財)日本情報処理開発協会(JIPDEC)が認証

^{*5}: Information Security Management System

^{*6}: British Standard (英国規格協会: British Standards Institution)が規定する情報セキュリティに関する管理システム規格。英国は最も早くからISMSの規格化に取り組んでおり、1995年にISMSの国家規格としてBS7799を規定した。その後BS7799-1、-2と枝分かれしたうちのBS7799-1情報セキュリティ管理実施基準が国際基準となり、各国でも英国をモデルに認証制度の作成・運用が行なわれるようになった)

ISMSは、情報資産に対するリスクアセスメント^{*7}を行ない、それに基づき、管理すべきリスクに対して管理策を選択し、計画・実施・監視・見直しを行ない、継続的にセキュリティを向上させます。

従来の安全対策事業所認定制度では、設備等の物理的な対策に比較的審査基準の重点が置かれていたが、本制度では設備・運用面をバ

ランスよく盛り込むとともに、情報セキュリティマネジメントの観点からの管理策を審査基準に付加しています。また、審査基準は時代に沿って見直し・改訂が図られています。

^{*7}: ISMS適用範囲内において、情報資産を洗い出し、各々の情報資産に対する脅威・脆弱性分析を行い、リスク値を算出するプロセス

ITリスクマネジメントは以下の手順で実施されます。

- (1)組織が守るべき情報資産の洗い出し
- (2) CIA^{*8}に影響を及ぼす脅威・脆弱性の明確化
- (3)リスク度合いの算定
- (4)算定したリスクに対するリスク対応計画の策定・実施
- (5)結果の評価

^{*8}: Confidentiality(機密性)、Integrity(完全性)、Availability(可用性)

ISMSについて

ISMSの取得メリット

ISMS認証を取得することは、情報および情報システムが安全かつ適正に運営・運用されていることの客観的な証明になり、顧客からの信頼獲得や競争力向上につながっています。

取得メリットの実際の具体例としては、以下のようものが挙げられます。

- (1)情報資産の整理

組織の情報資産を重要度に応じて体系的に管理できるようになります。

- (2)情報セキュリティレベルの底上げ

投資効果を考慮したトップダウンで、物理面・管

理面・技術面と総合的なセキュリティレベルの向上を図ることができます。

(3)従事者のセキュリティ意識改革

従業員の教育・啓もう活動によるモラル向上およびセキュリティ意識の高揚が図れます。

(4)アカウントビリティ(説明責任)

第三者による認証を取得することで、ステークホルダーに対して組織の活動や経営の内容を説明すると同時に、内部管理の透明性をアピールできます。

(5)イメージ(価値)の向上

信頼性・安全性について、組織のイメージアップが図れます。

(6)同業他社との差別化(優位性)

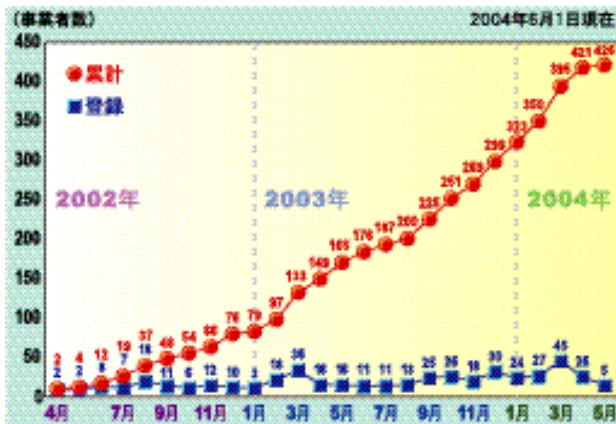
自治体では現在、セキュリティに関する認証取得を受注/入札/取引条件として掲げる場合も多くなり^{*9}、認証を取得することで、商談の機会が広がります。

このようなことから、ISMS 認証を取得する組織は年々増加しております。(図3)

このように、ISMSの必要性は高まる一方ですが、認証取得までのプロセスは多く、煩雑で、組織の要

*9: 「公共ITにおけるアウトソーシングに関するガイドライン」(総務省、2003年3月)

【図3: ISMS 認証取得事業者数推移】



出典: (財)日本情報処理開発協会 (JIPDEC)

員をそこに投入すると本業への専念の妨げとなることもあり、自前で行なうのはなかなか容易ではありません。

【図4: FIP のIT リスクマネジメントソリューション】



FIP が提供するリスクマネジメントソリューション

FIPは、早くからITリスクマネジメントに積極的に取り組み、自社でISMS 認証取得(2001年)を行なうだけでなく、そのノウハウを活かしてお客様の「信頼・安心」という事業価値の強化をご支援する各種ソリューションをご提供しております。

ISMS認証取得を支援するサービスはもちろんのこと、運用・運営中のセキュリティ監査・診断を行なうサービスや、ツールを用いた技術的なチェック・構築サービスをご用意しています。

お客様の現状システムの評価・分析から、組織としてのセキュリティ方針策定、それに基づくセキュリティマネジメントシステム構築、そしてシステムの経常的な監視まで、お客様のセキュリティ管理サイクルの実践をトータルにご支援いたします。(図4)

ISMS コンサルティングサービス

ISMS コンサルティングサービスは、お客様のISMS(およびBS7799)認証取得をご支援するサービスです。

サービスの特長は以下の通りです。

- ・専門スタッフによるサービス

ISMS主任審査員の資格をもったスタッフが、自社を含む豊富な審査現場の立会い経験に基づいた知識・ノウハウを活かし、お客様に最適なサービスをご提供いたします。

・認証取得から取得後のシステム維持までを
トータルサポート

情報セキュリティ管理システムの構築や認証審査の準備だけでなく、認証を取得した後のシステムの維持運用・改善までのライフサイクルをトータルにご支援いたします。(図5)

このISMSコンサルティングサービスは、全国でお客様の業種を問わずご利用いただいております。(図6)

プライバシーマーク取得支援サービス

(財)日本情報処理開発協会で付与認定している「プライバシーマーク^{*10}」を取得するにあたり、レビュー、ノウハウの提供、アドバイス、運用改善による支援を行なうサービスです。

^{*10}: JIS Q15001 に基づく個人情報保護の仕組みができていない民間事業者を認定する制度

監査・診断サービス

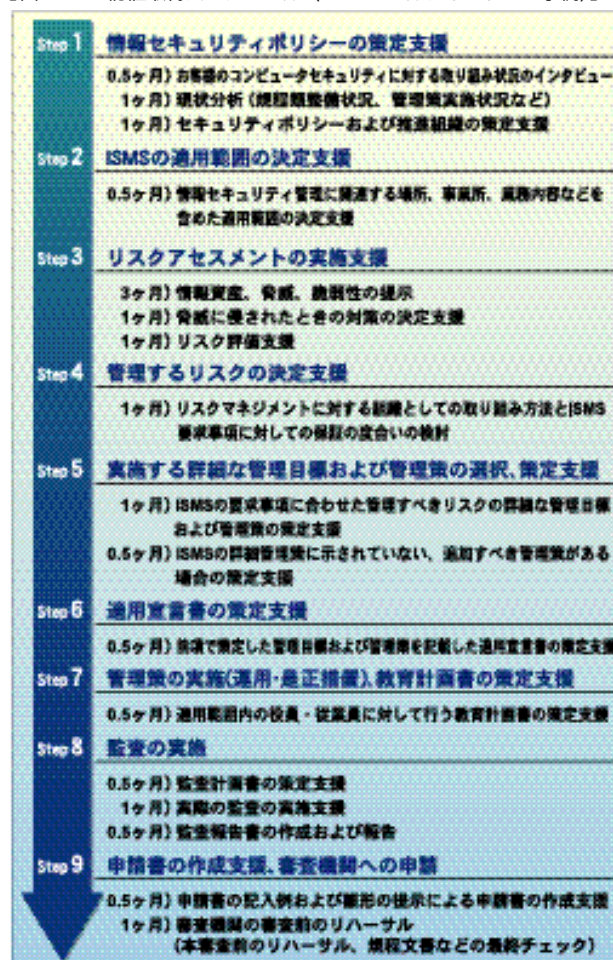
マネジメントシステム、運用管理、安全対策などの実施状況を、規格・規程・スタンダード、お客様のポリシーに基づき確認します。

この他にも、セキュリティを確保したサーバの構築サービスや、ツールを利用したシステム監査サービスも行なっております。

これらのサービスをお客様の状況に応じて選択・ご利用いただくほか、日々の運用におけるセキュリティ監視サービスもご利用いただけます。

FIPは、アウトソーシングやソフトウェアなどの各種サービス/ソリューションを通して、IT分野の発展のお手伝いをしてまいりました。今後とも、お客

【図5: ISMS 認証取得スケジュール (FIP コンサルティングでの事例)】



様をご支援しながら、セキュリティが確保された「情報と知識が付加価値の源泉となる社会^{*11}」の発展を担っていきたいと考えております。

^{*11}: 高度情報通信ネットワーク社会形成基本法第2条

【図6: FIPのISMSコンサルティングサービスご利用実績】

