

情報技術 (IT) シリーズ

情報セキュリティマネジメントシステム構築と運用

Construction and Operation of Information Security Management System

山野 浩
Yamano Hiroshi

インターネットの急速な普及に伴い不正アクセスや情報漏洩事件も急増している。また2005年4月1日よりの個人情報保護法施行等を背景に、情報セキュリティに対する関心がますます高まっている。それに伴い、企業等の組織では適切な情報セキュリティマネジメントシステムの構築と運用が必須となってきている。以下に、このシステムの構築と運用方法について解説する。

With the rapid spread of Internet, illegal computer access and leak of information have been increasing. In the meantime, the information security has taken a growing interest with the enforcement of the Act on the Protection of Personal Information on April 1, 2005. It has become necessary for organizations such as enterprises to construct and to operate suitable information security system. This article presents the explanation of the method to construct and operate the system.

キーワード：情報セキュリティ、情報マネジメントシステム、ISMS、リスクアセスメント、内部統制

1 はじめに

1.1 情報マネジメントの必要性

情報セキュリティに関する事件・事故は多発しており、それらが企業等の組織に与える影響は非常に大きい。このような状況の中で、企業は情報セキュリティを確保する組織や仕組みを構築して対応してきているが、それでも事件・事故は増えている。この原因としては、①情報セキュリティ対策を部署ごとに実施するので効果が得られない。②企業の情報セキュリティ対策への体制が不十分である。③外部からの脅威を想定した仕組みが多い。④セキュリティに対する投資目的が不明確なケースが多いと考えられる。更に、⑤ITの進歩が我々の想定をはるかに超えたスピードで進んでおり、これまでの組織や仕組みだとうまく対応できなくなっている。

企業の情報セキュリティ管理体制を適切に確保する方法として、経営層が定めた「情報セキュリティ基本方針」にしたがって適切に運用していくことが必要である。情報セキュリティの構築・運用に対しては、情報マネジメントシステム (ISMS) を活用することが必須である。

1.2 情報マネジメントとは

経営は、組織の4つの経営資源（人・物・金・情報）を調達して運用することによって存続し、発展している。したがって組織では、人・物・金・情報をうまくマネジメントしていく必要がある。情報社会の現代においては、情報資産が組織活動に大きな影響を及ぼすため、情報マネジメントシステムの構築と運用は組織にとって重要な課題である。

2 情報セキュリティとは

情報が適切に保護されていないと、漏洩することがある、内容が不正確である、必要なときに使えない等、業務に支障をきたすリスクがある。情報セキュリティに関しては重要な情報をこうしたリスクから守り、図1に示すように、主たる3要素を維持することが重要である。

(1) 機密性

機密性とはアクセスを認可された者だけが、情報にアクセスすることを確実にすることである。

盗聴やデータの流出、情報の漏洩などの防止を図るが、最近では特に個人情報の漏洩時の対応が重要であり、それを間違えると大きな金銭的なダメージや、企業ブランドの低下などに繋がる。

(2) 完全性

完全性とは情報および処理方法が、正確であることおよび完全であることを保護することである。

データの改ざんや詐欺・詐称などにより情報の信憑性が失われてしまうと、情報そのものの価値が失われる。

(3) 可用性

可用性とは認可された利用者が、必要な時に、情報および関連する資産にアクセスできることを確実にすることである。

データの破壊や紛失などで必要な時、タイムリーに情報にアクセスできないと、機会損失やサービス低下による売上の減少など様々な問題が発生する。



図1 情報セキュリティの3要素

3 情報セキュリティ管理

3.1 情報セキュリティ管理とは

情報セキュリティ管理では、組織体でリスクを認識し、実施することが求められる。組織の中で一人でも規則を守らない者がいると、社会的な信頼を失いかねない事件に発展する可能性がある。そのため、情報セキュリティ管理は事業活動を継続する上で内部統制と統合して実施すべきであるといえる。情報セキュリティ管理と関連する要件を以下に示す。

(1) 事業的要件

事業の目標や基準など事業継続する上で最低限必要な要件を明確化する。

(2) 技術的要件

セキュリティを維持するための具体的な手法や構成など技術的な要件を明確化する。

(3) 業界の最適な実践

各種業界（金融・公共など）毎にセキュリティの要件は異なってくる。組織が属する業界における最適な実践（ベストプラクティス）で要求される要件を明確化する。

(4) 法的要件

組織において法令，社会規範，企業倫理を順守し，社会を構成する一部として維持するための行動規範に必要な要件を明確化する。

(5) 管理的要件

組織や体制などに対する人的な管理に対する制約を明確化する。

3.2 実施内容

組織は情報セキュリティのリスクに対応し，そのリスクが事業を進めていくうえで受容できる内容であることを確認し，事業継続をはかることが求められている。内部統制の監査報告書を作成する企業は，IT内部統制において情報セキュリティ管理を導入することにより効率的な対応ができる。内部統制において，表1に示す情報セキュリティ管理を実施すべき内容を示す。

表1 情報セキュリティ管理実施内容

分類	管理の内容
全般的な統制	・ 経営者の宣言と関与
	・ 方針の作成
	・ 推進体制，役割などの組織の取り組み
リスク管理	・ 情報資産の特定
	・ リスクの評価
管理施策	・ 安全管理の基準
	・ 組織的安全管理の基準，ガイドラインの作成
	・ 技術的安全管理の基準，ガイドラインの作成
管理実施	・ 管理施策の実施
	・ 安全管理のモニタリング，分析
対応，事業継続	・ インシデント管理
	・ 災害対策
	・ 事業継続

3.3 情報セキュリティマネジメントシステム

組織は情報セキュリティを管理し，機密を守るための包括的な枠組みとして情報マネジメント

システム (ISMS) を活用している。ISMSはコンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針 (セキュリティポリシー) や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた統合的なリスクマネジメント体系である。ISMSの要求事項は、組織の自らの事業の活動全般及び直面するリスクを考慮して、文書化されたISMSを確立、導入、運用、監視、見直し、維持し、かつこれを継続的に改善することである。

ISMSにより組織が享受できる主なメリットは以下の2点である。

(1) 情報セキュリティ体制の強化

情報セキュリティの体制整備、あるいはそれによる責任・権限の明確化、リスクマネジメントなどの定着により社内組織の体質強化につながる。

(2) 認証取得による信頼性強化

認証を取得することで、対外的に情報セキュリティに対する信頼性が高まる。最近では、顧客からの要求事項 (RFP: request for proposal) に認証取得が条件となっているケースが多く、ビジネスに必須である。

4 情報セキュリティマネジメントシステムの構築と運用

4.1 ISMSの構築

ISMSの確立には、図2に示すように3つのフェーズが存在する。最初のフェーズ1では、ISMSの適用範囲を決定し、情報セキュリティの全般的な方向性及び行動指針を定義する。次のフェーズ2では、リスクに関して、詳細に分析し、障害が生じた場合の事業上の損害及び発生頻度から、リスクの度合いを評価し、対応策や管理策を決定する。最後のフェーズ3では、ISMS適用宣言書を作成すると共に、経営陣は残存リスクを承認し、ISMSを実施する許可を与える。

これら3つのフェーズのなかで、特に重要なものは、フェーズ2で行うリスク対応策の決定である。リスク対応策には、「リスク回避」「リスク移転」「リスク分散」「リスク保有」という4つの方法論がある。これらの対応策はリスクの度合いに応じて選択される。軽度のリスクはそのまま保有し、管理策だけを講じることも考えられるが、組織にとって重大な損害が発生することが想定される場合は、そのリスクを含む業務を中止し、物理的・技術的な対策を実施することで抜本的な予防処理を講じることが望ましい場合もある。

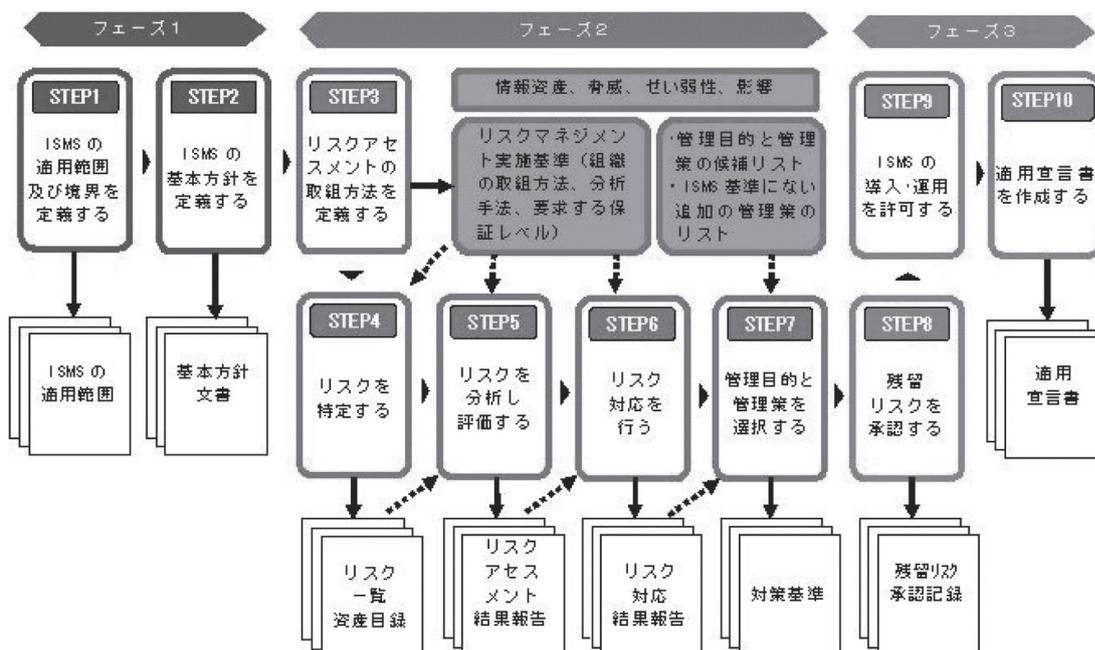


図2 ISMSの確立 (出典：日本情報処理開発協会)

ISMS 認証を取得することによって、情報セキュリティ事故の発生頻度は低減できるが、ゼロにはならない。多くの場合は重大なリスクの存在を認めながらも、「リスク回避」「リスク移転」の処置を行わずに、そのリスクを継続して保有することを経営陣が判断し、管理策を決定したものが多いのではないかと考える。これらは、後に述べる ISMS の運用の過程で見直すことで、リスクの低減を図ることが必要である。

4.2 ISMS の運用

ISMS の取り組みには、計画、導入・運用、監視・見直し、維持・改善の PDCA サイクルを回す取り組みが要求される。それによって情報セキュリティ管理が向上し、ISMS をより有効に作用させることができる。全体を通じて①経営陣によるトップダウン活動であること、②目的を明確にすること、③適用範囲を明確にすること、④対策・手順は実現可能で具体的に細かく決めることが必要である。特にリスクの大きいものから優先順位をつけ対策を行うことが重要である。

(1) Plan (ISMS の確立)

リスクマネジメント及び情報セキュリティの改善に関連した、情報セキュリティ基本方針、目的、目標、プロセス及び手順を確立する。それらは、組織の全体的な基本事項及び目標に沿ったものでなければならない。ポイントは、①組織の事業目的を反映したセキュリティポリシーを策定すること、②リスク評価に基づく適切なプランであること、③技術的な面と、運用管理面とバランスがとれていることである。

(2) Do (ISMS の導入・運用)

策定した情報セキュリティポリシー基本方針、管理策、プロセス及び手順を導入し運用する。ポイントは、手順に沿って ISMS を実行・運用することがあげられ、組織長を含む組織員全員にセキュリティポリシーが周知され、適切なセキュリティ教育が継続的に実施されることが重要である。

(3) Check (ISMS の監視・見直し)

情報セキュリティ基本方針、目的、目標、実施結果と照合し、評価し、測定（可能な場合）し、

その結果をシステムの見直しのために経営陣に報告する。ポイントは、①実施状況の評価結果に対して、改善のための提言をフィードバックする仕組みがあること、②情報セキュリティ監査制度などを活用することである。

(4) Act (ISMS の維持・改善)

ISMS の継続的な改善を行うために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。

5 まとめ

大企業等で既に ISMS の構築・運用を実施しているケースが多い。しかしながら、情報漏えいが多発している現状において、PDCA サイクルによる継続的な改善が不十分なケースもあり、運用における技術面や、体制面などに課題は多い。また、中小企業では未構築が多く、信頼性を高めるとともに、受注競争参加資格として早急に取り組む必要がある。技術士が今後、このような課題に対して ISMS の構築および監査などで活躍する場が増えてくるものと考えられる。

<引用文献>

- 1) (財) 日本情報処理開発協会 (JIPDEC) ホームページ <http://www.isms.jipdec.jp/isms/>

<参考文献>

- 1) (社) 日本技術士会プロジェクトチーム：技術図書刊行会編、技術士コンサルティングハンドブック、オーム社、2009
- 2) 羽生田和正 他：ISMS 構築・認証取得ハンドブック、日科技連出版社、2008
- 3) 福丸典芳 他：実践 ISMS 構築と運営法、日刊工業新聞社、2004
- 4) (社) 日本技術士会プロジェクトチーム：技術図書刊行会編、技術士ハンドブック、オーム社、2006
- 5) 山野浩 他：先端技術と個人情報保護、オーム社、2003

山野 浩 (やまの ひろし)

技術士 (情報工学部門)

(株) 日立情報システムズ
ネットワークサービス事業部 副技師長
APEC エンジニア (電気工学) EMF エンジニア
e-mail : h-yamano@hitachijoho.com

