情報セキュリティマネジメント

要　旨

企業や行政機関などの組織において、情報セキュリティの確立、実施、維持、継続的改善によって、その組織の目的を達成するための、一連の必要な要素（組織、役割及び責任、計画、運用など）が、情報セキュリティマネジメントシステム（Information Security Management System: ISMS）である。すなわち、ISMSは情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的な対策を総合的に含む、経営者を頂点とした組織的な取組である。

I　サイバーセキュリティ確立にむけた組織としての取組

企業や官公庁などの組織が現在直面しているサイバーセキュリティ上のリスクの多くは、ファイアウォールやウイルス対策ソフトなどの技術的対策を導入したとしても、発生を完全に防止することは困難なものである。これは、最近のサイバーセキュリティリスクが、組織の管理体制の問題点(1)などに起因するためである。どんなに優れた技術的対策も適切に運用されなければその効果は限定的であり、また組織の従業者が意図的あるいは非意図的に秘密情報を漏えいする可能性もある。そもそも、組織においてどのようなリスクがあるかを十分に把握することなしには、適切な対策をとることも不可能である。組織におけるサイバーセキュリティ確立に向けた一連の取組のことを情報セキュリティマネジメントという。本論では、情報セキュリティマネジメント及びその基礎となるリスクマネジメントについて説明する。また情報セキュリティマネジメントに関する第三者評価の仕組みとして、情報セキュリティマネジメントシステム認証制度や情報セキュリティ監査制度などを紹介する。さらにサイバーセキュリティに関連する組織上のリスクマネジメントの取組として、事業継続管理と内部統制について解説を加える。

II　情報セキュリティマネジメントとは

情報セキュリティマネジメントの基本は、組織運営全般の目的と情報セキュリティ目的の両面から、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）（以上の三要素をCIAと呼ぶ）を維持し、結果として、リスクを適切に管理しているという信頼を組織の利害関係者（ステークホルダ）に与えることである。しかし、対策を講じれば講じるほどコストはかかるものであり、現実には、実施するべき対策の効果と必要なコストのバランスを取ることが重要になっている。

企業や行政機関などの組織において、情報セキュリティを管理する（マネジメントする）ため

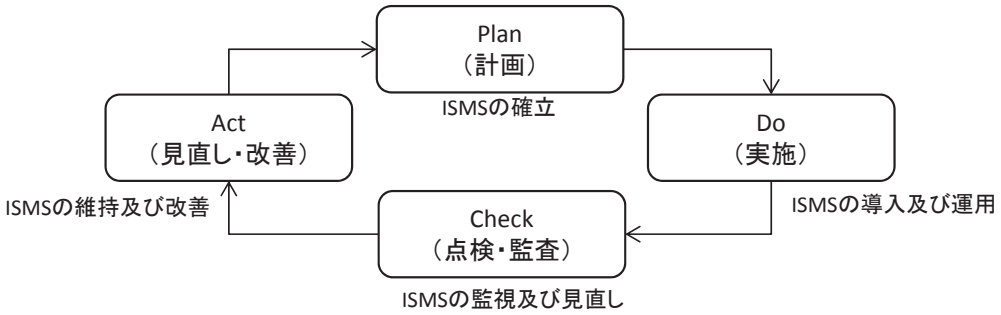
＊本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。

(1)　管理体制の問題点とは、例えば、Webサーバのオペレーティングシステムの既知の脆弱性を放置しておくことで攻撃者に不正アクセスされ、あるいは従業員教育を十分にしないことで秘密情報の漏えいを許す、などが典型的な問題である。

の枠組みとして、情報セキュリティを体系的に捉えたのが情報セキュリティマネジメントシステム（Information Security Management System: ISMS）である。ISMSとは、情報セキュリティの確立、実施、維持、継続的改善によって、その組織の目的を達成するための、一連の要素（組織の構造(2)、役割及び責任、計画、運用など）のことであり、組織的、人的、物理的、運用的、技術的な対策を含む、経営者を頂点とした組織的な取組である。(3)

情報セキュリティマネジメントの改善プロセスの考え方の一つに、PDCAサイクルがある。これはPlan（計画）・Do（実施）・Check（点検・監査）・Act（見直し・改善）のPDCAサイクルを繰り返すことで、絶えず見直しと改善を行うという考え方である（図1参照）。これは、情報技術の進展や脅威の変化などに伴い、適用する対策も適宜見直していくことが必要なためである。

図1　ISMSの構築、維持及び改善のサイクル



（出典）「情報セキュリティマネジメントとPDCAサイクル」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/manager/protect/pdca/index.html>を基に三菱総合研究所作成。

PDCAサイクルの考え方は国際標準ISO/IEC 27001:2013では削除されたが、ISO/IEC 27001:2013の基礎となっている「ISO/IEC Directives Part 1 and Consolidated ISO Supplement」のAnnex SLでは拡張されたPDCAの考え方（PDCAとは呼んでいない）が採用されており(4)、PDCAサイクルに基づくことは、一定の意味があると解釈できる。

Plan（JIS Q 27001:2014における「計画」に相当）とはISMSを確立するための計画であり、Do（JIS Q 27001:2014における「運用」に相当）とはISMSの導入と運用、Check（JIS Q 27001:2014における「パフォーマンス評価」に相当）とはISMSの監視と見直し、Act（JIS Q 27001:2014における「改善」に相当）とはISMSの維持と改善となる。より具体的に表現すれば、ISMSでは、「情報セキュリティマネジメントのための計画（準備）活動（リスクの特定や分析、評価、対策の選定等）」を行い、「計画に従ったセキュリティ対策の実施・運用」を推進する。さらに、「実施情報セキュリティ対策の日常的な監視及び定期的な情報セキュリティ監査」を行い、それらの「見直しと改善」を実施するというPDCAサイクルを繰り返すことになる。

(2)　組織の構造とは、組織のマネジメント構造などを指す。
(3)　日本工業標準調査会『JIS Q 27001:2014 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項』日本規格協会, 2014.
(4)　International Organization for Standardization and International Electrotechnical Commission, “ISO/IEC Directives Part 1 and Consolidated ISO Supplement: Procedures specific to ISO,” 2014. <http://www.iso.org/sites/directives/directives.html>

1　計画（Planに相当）

ISMSを確立するための計画段階であり、組織の状況を理解し、課題及び利害関係者の要求事項を考慮し、リスク及び機会[(5)]を決定する。情報セキュリティのリスク基準を確立し、情報セキュリティリスクアセスメントを実施する。実施したリスクアセスメントの結果を考慮して、適切な情報セキュリティリスク対策等を選定し、管理策を決定、適用宣言書（採用した管理策及び採用しなかった管理策と、採用・不採用の理由を記載した文書）及び情報セキュリティリスク対応計画を策定する。

2　実施（Doに相当）

上記で決定した対応計画にしたがい、その計画を実施することが求められる。また、情報セキュリティリスク基準と、情報セキュリティリスクアセスメントを実施するための基準を考慮して、定期的又は何らかの変更（規則の変更やICT環境の変更等）が行われた際に情報セキュリティリスクアセスメントを実施する。リスクアセスメントの結果を踏まえ、適切な情報セキュリティリスク対応の選択肢を決めて、実施する。

3　評価（Checkに相当）

組織は情報セキュリティパフォーマンス及びISMSの有効性を評価することが求められている。ISMSが規定した要求事項について適合しているかどうか、あらかじめ定めた間隔で内部監査を実施する。評価プロセスの最後に、トップマネジメント（企業であれば経営層）は、組織のISMSが適切、妥当かつ有効であることを確実にするために、あらかじめ定めた間隔でISMSの見直し（レビュー）を実施する。

4　改善（Actに相当）

JIS Q 27001:2014の要求事項や組織の規定を満たしていないなどの不適合が発生した場合には、組織はその不適合を改善するための対処を実施する。また、その不適合が再発又はほかのところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。

III　リスクマネジメント

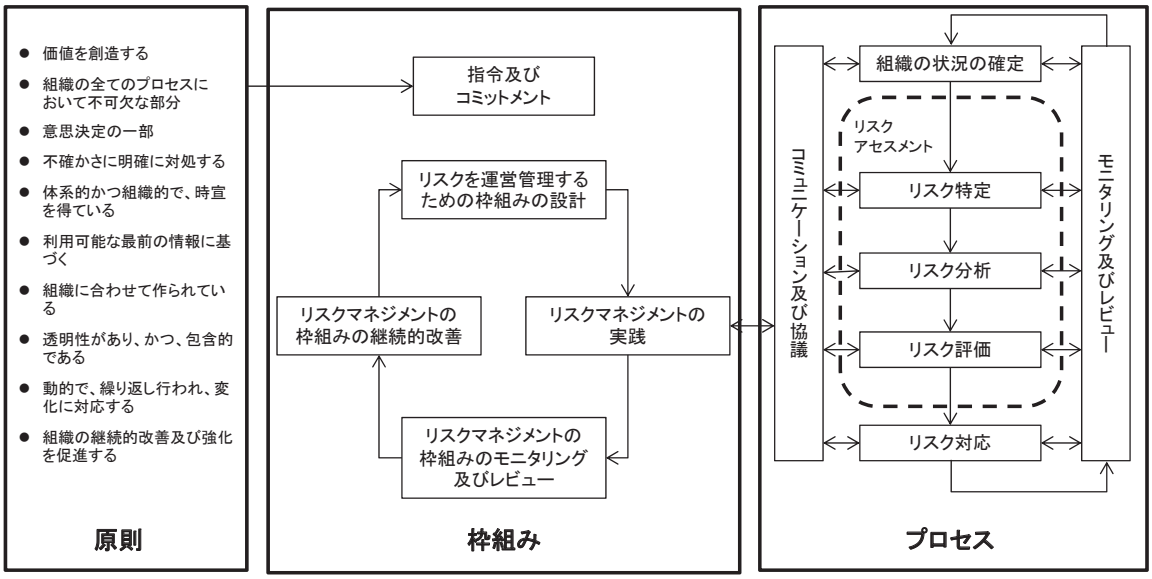
ISMSにおいては、情報セキュリティに関するリスクマネジメントを行うことが求められている。ここでリスクとは、ISO Guide 73:2009（JIS Q 0073:2010）によれば、「目的に対する不確かさの影響」のことである。ISMSにおける情報セキュリティリスクマネジメントは、リスク

(5)　リスクマネジメントでは、悪影響を与えるリスクだけではなく、好影響を与えるリスク（つまり機会）についても考慮する。

マネジメントに関する一般的なフレームを定めた国際標準であるISO 31000:2009（JIS Q 31000:2010「リスクマネジメント―原則及び指針」）に基づいて実施する（図2参照）。

情報セキュリティマネジメントとリスクマネジメントは密接な関係にある。つまりリスクマネジメントの枠組みは、企業を取り巻く様々なリスクに統一的に取り組むマネジメントシステムを指向しているが、そのうちの情報セキュリティにかかわるリスクに対する管理を取り出して、その分野に特化したマネジメントシステムが情報セキュリティマネジメントシステムである。

図2　JIS Q 31000:2010におけるリスクマネジメントの原則、枠組み、プロセス



（出典）JIS Q 31000:2010「リスクマネジメント―原則及び指針」を基に三菱総合研究所作成。

ISO/IEC 31000:2009におけるリスクマネジメントは、「リスクアセスメント」及び「リスク対応」によって構成されている。特定されたリスクを分析し評価して対応策を検討するという、リスクマネジメントの中核的な考え方はISMSにおいても、「情報セキュリティリスクアセスメント」及び「情報セキュリティリスク対応」として採用されている。

1　情報セキュリティリスクアセスメント

組織がどの程度のリスクをとるか（リスク受容基準）などを定めた上で、リスクアセスメントの一連のプロセス（リスクの特定、分析、評価）を実施する。

(1)　リスクの特定

リスクを発見、認識及び記述するプロセスである。リスク特定には、リスク源（「存在（ウイルスの存在等）」と「起こりやすさ（ウイルス対策ソフトの定義ファイルの未更新等）」）、事象（盗難、置き忘れ等）、それらの原因及び起こりうる結果（情報漏えい等）の特定が含まれる。

(2)　リスクの分析

リスクの特定で洗い出された各種リスクについて、その「発生時の影響の大きさ」と「発生確率」の両面からそのレベルを決定する。一般的にリスクの大きさは、両者の積で表されるため、それぞれを算定することによりリスクの大きさを計算することが可能になる。

(3)　リスクの評価

リスクの大きさが受容可能か又は許容可能かを決定するためにリスク分析の結果をリスク基準と比較する。この評価により、対応をとるべきリスクが決まる。

2　情報セキュリティリスク対応

リスクを修正するプロセスを「リスク対応」、その対策を「管理策」と呼んでいる。管理策としては、①リスクの回避、②リスクをとる又は増加させること（いわゆるリスクテイク）、③リスク源の除去、④起こりやすさの変更、⑤結果の変更、⑥リスクの共有、⑦リスクの保有の7つの手法が例示されている(6)。

3　リスクコミュニケーション及び協議

リスクの運用管理の過程では、利害関係者にリスクを開示（リスク開示）し、利害関係者間でのリスクコミュニケーション（対話）を通じて共通認識を確立することが重要である。

IV　情報セキュリティマネジメントに関する第三者評価の仕組み

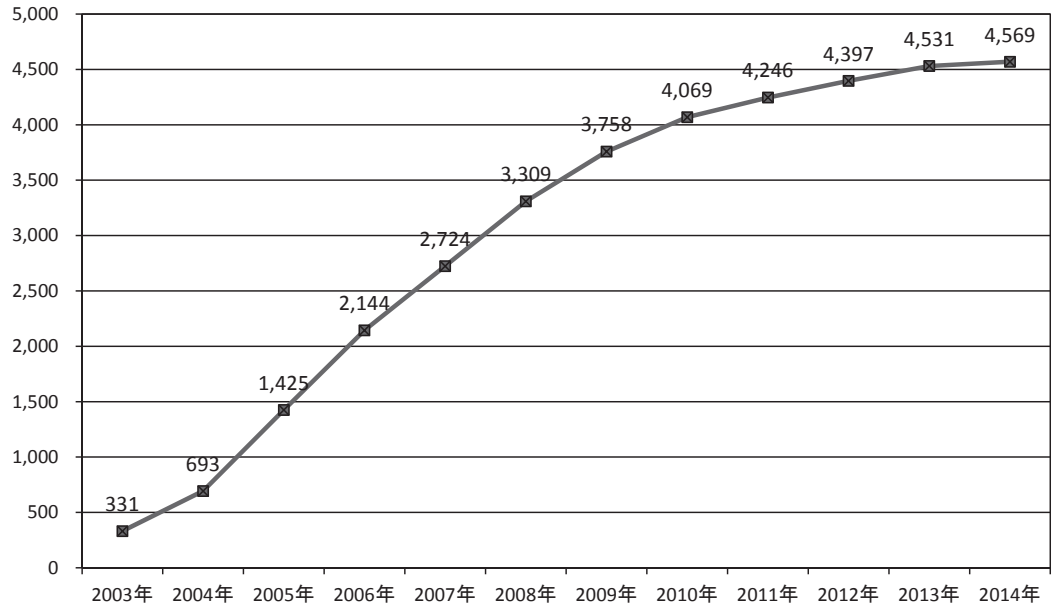
1　情報セキュリティマネジメントシステム認証制度

組織のISMSが適切なものであるかを第三者評価するための基盤として、ISMSを構築する上の要求事項をまとめた国際規格「ISO/IEC 27001:2013 Information technology－Security techniques－Information security management systems－Requirements」がある。日本ではその日本語版である「JIS Q 27001:2014 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」に関する適合性評価制度として「ISMS適合性評価制度」が運用されている。同制度の本格運用の開始は2002年4月で、我が国では日本情報経済社会推進協会（JIPDEC）の情報マネジメントシステム推進センターが認定機関となっている。なお、同制度は国が決めて運用している制度ではないため、厳密には公的な制度ではなく民間の評価制度であるが、世界的に運用されていることもあり、組織にとっては重要な制度と位置付けられている。

図3に示すように、日本国内のISMS取得数は2014年12月現在約4,500社である。また、全世界の取得数の多くを日本が占めている(7)。

(6)　日本工業標準調査会　前掲注(3)
(7)　“ISO Survey 2013.”International Organization for Standardization Website <http://www.iso.org/iso/iso-survey>

図3　ISMS認証取得機関数の推移



（出典）「認証取得組織数推移、認証機関別・県別認証取得組織数」2014.12.25. 日本情報経済社会推進協会ウェブサイト <http://www.isms.jipdec.or.jp/lst/ind/suii.html>を基に三菱総合研究所作成。

2　情報セキュリティ監査制度

情報セキュリティ監査とは、経済産業省が定めた「情報セキュリティ管理基準（平成20年経済産業省告示第246号）」「情報セキュリティ監査基準（平成15年経済産業省告示第114号）」等に基づき実施されている監査制度である。情報セキュリティマネジメント認証制度がJIS Q 27001に対する適合性を評価することを目的としているのに対し、監査制度では、監査の内容は監査を受ける組織が自由に選択することができ、選択された内容に対して監査人は情報セキュリティマネジメントが確かに実施されているかを確認し保証する。したがって監査制度はJIS Q 27001に対する適合性を評価するものではない。

情報セキュリティ管理基準は、JIS Q 27001及び27002に基づき策定され、監査を受ける主体の行動規範として、また、監査人の判断の尺度として用いられる。情報セキュリティ監査基準は、高い品質で有効かつ効果的に監査を実施するための監査人の行動規範を定めたものである。情報セキュリティ監査制度の確立と普及を目的として、特定非営利活動法人日本セキュリティ監査協会（JASA）が設立されている。

また、類似の第三者評価の仕組みとして情報セキュリティ格付が民間企業（アイ・エス・レーティング）により提供されている。

Ⅴ　サイバーセキュリティに関連するその他のリスクマネジメント

1　事業継続管理・事業継続計画

大規模災害や、サイバー攻撃などにより情報システムやサービスが停止するリスクは年々増大しており、組織や社会に大きな影響を及ぼすようになってきている。災害やシステム障害が発生した場合でも事業を継続し、企業や行政機関などの組織目標を達成することが重要であ

る。

リスクが発現した場合でも可能な限り事業を継続し、サービスを提供し続けるための管理方法として、事業継続管理（Business Continuity Management: BCM）が考えられている。また、BCMの一環として事業継続計画（Business Continuity Planning/Plan: BCP）の策定が必要とされている。情報セキュリティの観点からのBCM・BCPは、情報セキュリティ3要素の一つである可用性（Availability）を守るための取組と考えることができる。

BCMの国際標準として、「ISO 22301:2012 Societal security－Preparedness and continuity management system－Requirements」や、「ISO 22313:2012 Societal security－Business continuity management systems－Guidance」が定められている。JIPDECではISO 22301:2012に基づく適合性評価制度である「事業継続マネジメントシステム」（BCMS）を運用している。

2　内部統制

「内部統制」とは、コンプライアンス（法令遵守）の確保、財務報告の信頼性の確保及び業務の効率化を目的として、「企業がその業務を適正かつ効果的に遂行するために、社内に構築され、運用される体制及びプロセス」[(8)]である。

内部統制が注目されるようになったきっかけは、米国の「上場企業会計改革及び投資家保護法（Public Company Accounting Reform and Investor Protection Act of 2002, P.L.107-204）」の制定である。米国では、不正経理等による粉飾決算が明るみ出たことによりエンロン社が破綻した事件や同じく粉飾会計によりワールドコム社が破綻した事件など、監査する立場の会計事務所と企業との癒着から粉飾決算や連結外し（損失を連結対象外会社に付け替えること）、有価証券報告書の虚偽記載などが見逃されたり、会計事務所自体が積極的にそのような不正に関与したりするような悪質な不祥事が相次いだことを受け、2002年に同法が制定された。これは法案を提出したポール・サーベンス（Paul Sarbanes）上院議員とマイケル・G・オクスリー（Michael G. Oxley）下院議員の名をとって「サーベンス・オクスリー法（Sarbanes–Oxley Act of 2002）」と呼ばれ、その略称として「SOX法」とも呼ばれている。

日本においても、「金融商品取引法」（昭和23年法律第25号）の2006年改正「証券取引法等の一部を改正する法律」（平成18年法律第65号）の中で「財務報告に係る内部統制の強化等に関する制度整備」として、内部統制の評価、報告及び監査に関する制度が導入された。これを日本版SOX法（J-SOX法）と呼ぶ場合もある。

金融商品取引法は財務報告の信頼性の確保を目的としたものであるが、現在の企業において、財務処理は情報システムに依存していることから、財務報告の信頼性確保のためには情報システムの処理についても信頼性・正確性が求められている。

情報セキュリティマネジメントについて見てきたように、企業や官公庁などの組織にとって、サイバーセキュリティ対策という観点だけでも様々な体制の構築や管理が求められるようになってきている。情報セキュリティマネジメントの導入にはコストがかかる一方、必ずしも

(8)　経済産業省「リスク新時代の内部統制」2003.6, p.1. <http://www.meti.go.jp/report/downloadfiles/ 030627risk-hokokusyo.pdf>

生産性の向上や利益の拡大にはつながらないため、導入に消極的な組織も存在する。一方で、十分な対策をとらずにサイバーセキュリティ対策を講じない企業が増えると、公害問題のように社会全体に大きな損害を与える可能性がある。今後、組織におけるサイバーセキュリティ対策の問題は社会全体の問題として捉えていく必要がある。具体的には、負の外部性（外部不経済）による市場の失敗の観点から国などの関与（規制等）を求める方向に進めるのか、あるいは何らかの方策を導入することで市場メカニズムにより自律的な対策水準の向上につなげるのか、について検討が必要となると思われる。

執筆：株式会社三菱総合研究所　情報通信政策研究本部　主席研究員　村野（むらの）　正泰（まさやす）
監修：工学院大学　常務理事・情報学部　教授　大木（おおき）　榮二郎（えいじろう）
独立行政法人情報通信研究機構
ネットワークセキュリティ研究所　主管研究員
KDDI株式会社　情報セキュリティフェロー　中尾（なかお）　康二（こうじ）