経営者に情報セキュリティ対策の必要性を訴求する手法について

西日本支部　経営者向け情報セキュリティ対策実践手引き WG
西日本支部長　嶋倉　文裕

1. はじめに

企業における、情報セキュリティに関連する事故や事件による影響範囲は甚大であり、ひとたび発生させると、いままでの人材や技術など、社会に投資・貢献してきた努力が、一瞬にして「無に帰す」ことになる。情報セキュリティ事故は情報漏洩といった機密性の侵害に注目されがちであるが、マルウェアの侵入による工場ラインの停止や、不安定な動作による製品品質の劣化、低下、製品の出荷の遅れ・停止を招くこともあり、これらの経営への影響は計り知れない。

また、今後さらにIoT化により業務とITが密接に関係していくことを考慮すると、情報セキュリティ対策は、全ての組織にとって喫緊の課題である。

そのため、常日頃から、自組織がどのような環境でオペレーションを行っているのか、情報セキュリティ対策がどの程度実施されているのか、どのようなリスクにさらされており、どの程度の対策をしておくべきなのかを把握し、対応を決断することが経営者や経営層には問われているが、経営層にとって情報セキュリティリスクは、理解しにくいものである、というのが実態である。

それでは、情報セキュリティに起因する影響をできる限り最小限にし、情報セキュリティ対策が事業継続への投資として必要不可欠であることを経営者に理解していただくにはどうすれば良いか?

西日本支部の「経営者向け情報セキュリティ対策実践手引きWG」（以下、Risk WG）では、その解として経営者に情報セキュリティ対策の必要性を訴求し、対策に投資をしてもらうために、必要性の見える化として、ISO31000（リスクマネジメント）のリスクマネジメントを参考にして、自組織そのものを評価するための手段の検討を行った。

本稿では、Risk WGの成果物である「経営者のための情報セキュリティ対策　―ISO31000から組織状況の確定の事例―」に記載する、ISO31000の「組織の状況の確定」というステップを中心に、情報セキュリティの目的を明確にし、自組織の情報セキュリティに係るリスクの把握、リスクの評価、リスク対応を決断し、必要な対策の見える化について紹介する。

2. リスクアセスメントとマネジメントの考え方

「組織の状況の確定」は、ISO31000のリスクアセスメントの一ステップで、図1の位置づけとなる。

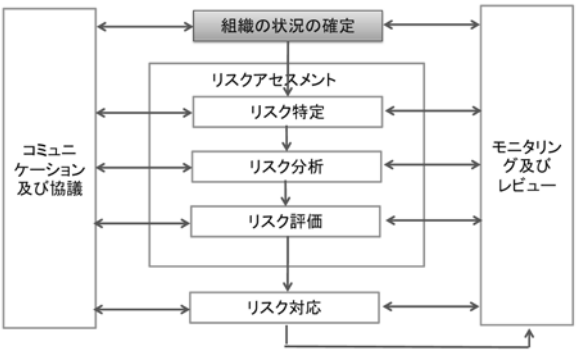

図1　ISO31000のリスクマネジメントプロセス

なお、ISO31000のリスクマネジメントプロセスの各ステップにおいて「コミュニケーション及び協議」が関連づけられているが、Risk WGでは、「コミュニケーション及び協議」を誰と行うのか、経営視点でのリスクとして捉えて行うために必要なことは何かを考え、それを図2に整理した。

組織には様々なリスクが存在し、情報セキュリティリスクはそのうちの一つではあるが、情報セキュリティリスクによる経営や業務への影響を情報システム部門のみで把握するには困難であり、経営者、業務部門でしかわからないことがある。

そのため、情報セキュリティリスクには、経営者、業務部門と情報システム部門が一体に対応することが必要であり、その要となる経営者、業務部門と情報システム部門間の「コミュニケーション及び協議」を効率的に進めるには、組織全体で共通の言葉と意味でリスクの認識を持つことが求められる。

例えば、図2では情報セキュリティリスクが、システ

ムリスクや品質リスクに影響することを示しており、情報セキュリティリスクによるシステムリスク、品質リスクを把握し、それぞれにおける対策の明確化を「コミュニケーション及び協議」を通じ行うことを示す。

逆に言えば、情報セキュリティリスクがシステムリスクや品質リスクに何ら、影響を与えない組織であれば、対策は不要であり、リスクを正しく把握することは無駄な投資を防ぐことになる。

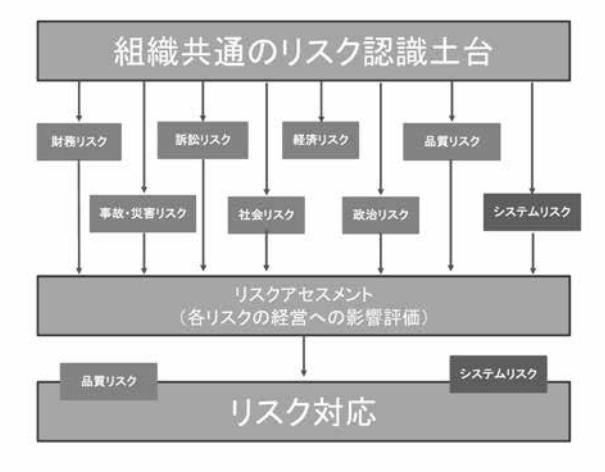

図2　リスクの共通土台

3. 組織の状況の確定方法

3.1　外部状況と内部状況

組織の目的を明確化するISO31000の「組織の状況の確定」では、リスク管理において考慮するのが望ましい外部及び内部の要因を定めている。

以下にISO31000に記載されている外部状況、内部状況の例を示す。

3.2　組織の状況の確定方法

Risk WGでは、経営の視点から自組織の状況の確定を行うことで、図3に示す以下の事項が明確にできると考えた。

(1) セキュリティ対策の目的、望まれる対策とレベル
自組織の社会における位置づけ、社会や顧客からの期待など、外部からの要請が自組織のセキュリティの動機付け、対策の範囲やレベルの要件となる。

(2) 対策の範囲
把握した外部状況、内部状況から対策すべき範囲が明確となる。

表1　外部状況と内部状況例

外部状況例	国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制、金融、技術、経済、自然並びに競争の環境
	組織の目的に影響を与える主要な原動力及び傾向
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観
内部状況例	統治、組織体制、役割及びアカウンタビリティ
	方針、目的及びこれらを達成するために策定された戦略
	資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）
	内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
	組織の文化
	情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
	組織が採択した規格、指針及びモデル
	契約関係の形態及び範囲

(3) リスクの低減
目的を達成するために、軽減すべきリスク、最低限受容可能なリスクを識別する。
(4) 予算
リスク軽減に向けて、運用も含めた必要な費用と、自組織で投資可能な費用から、予算計画を立案する。

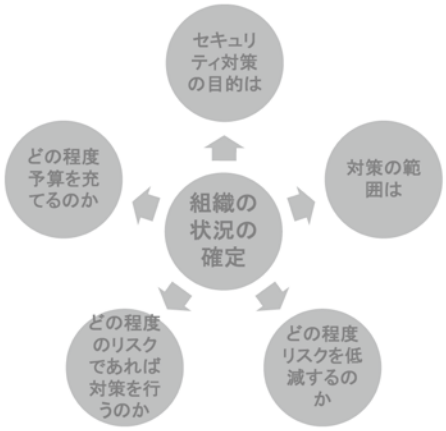

図3　組織の状況の確定を行う視点とは

3.3　経営環境の分析

Risk WGでは、経営に訴求する方法として、図4の一般に使われる以下のマクロ環境(PEST)とミクロ環境（Five Forces：5つの競争要因）を利用できないか、検討を行った。マクロ環境は、企業が統制不可能なこと、ミクロ環境は企業が準統制可能なこととして捉えている。

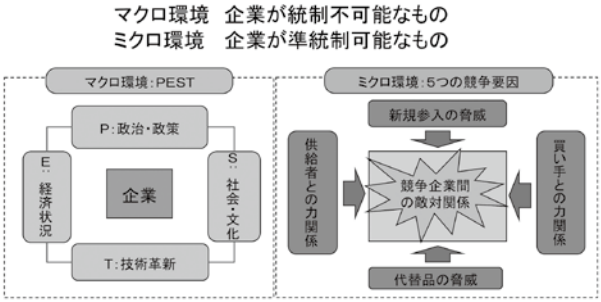

図4　マクロ環境とミクロ環境

3.4　外部状況、内部状況とマクロ環境、ミクロ環境の関係の再整理

Risk WGでは、ISO31000の外部状況、内部状況とマクロ環境（PEST）、ミクロ環境（Five Forces）の関係について検討を行い表2に再整理した。

マクロ環境、ミクロ環境とも外部要因であり、これらはISO31000の外部状況との関係で整理できる。

また、3.2項に示すとおり、自組織の社会における位置づけ、社会や顧客からの期待など、外部からの要請といった外部状況が、自組織のセキュリティの動機付けの大きな要因となり、セキュリティ対策の範囲、レベルの要件となる。

一方、内部状況は自組織の様々な要因と紐づけられ、セキュリティの視点では、表3に示す現状の対策状況となる。

以上を踏まえ、セキュリティにおける外部状況、内部状況の関係をまとめると、以下のように整理できる。

- 外部状況が自組織のセキュリティ対策の動機付けとなり、目指すセキュリティの姿が定まる
- 内部状況は、自組織の現状であり、内部要因により現状のセキュリティレベルとなっている
- 目指すセキュリティの姿と現状のセキュリティレベルの差異が改善すべき対策となる

図5にその関係を示す。

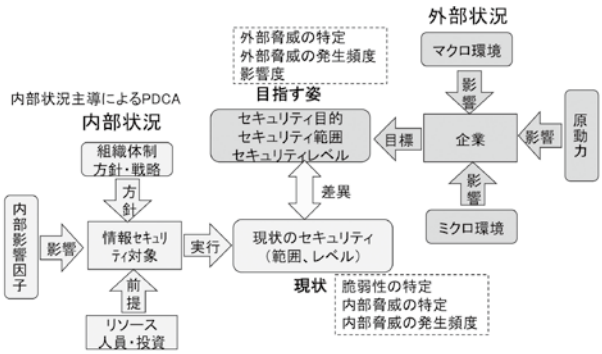

図5　セキュリティにおける外部状況と内部状況の関連

目指す姿との差異が確認されれば、図6のように、内部状況および外部状況を踏まえたPDCAを行い、組織体制や方針・戦略へのフィードバック、内部影響

表2　外部状況とマクロ環境、ミクロ環境

		分類	セキュリティとの関係	再分類	
外部状況	国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制金融、技術、経済、自然並びに競争の環境	政治	P:政策により、セキュリティ攻撃等セキュリティ脅威が増大	マクロ環境	要求要件
		経済	E:セキュリティ投資に影響		
		金融	セキュリティ投資に影響		
		社会及び文化	S:脅威、セキュリティ対策に影響（要リスク評価）		
		技術	T:脅威、セキュリティ対策に影響（要リスク評価）		
		法律/規制	脅威、セキュリティ対策に影響（要リスク評価）		
		自然	脅威、セキュリティ対策に影響（要リスク評価、事業継続）		
		競争環境	ミクロ環境:脅威、セキュリティ対策に影響（要リスク評価）	ミクロ環境	
	組織の目的に影響を与える主要な原動力及び傾向	N/A	組織の目的に影響を与えるセキュリティレベル（最低のセキュリティレベルより大） セキュリティ対策の目的、セキュリティ対策の範囲、セキュリティレベル	セキュリティ対策の目的 セキュリティ対策の範囲 セキュリティレベル	
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観	株主	業種により外部から要求されるセキュリティレベル（最低のセキュリティレベル） セキュリティレベル、範囲		
		顧客			
		取引先他			

表3　内部状況の再整理

		分類	セキュリティとの関係	再分類	
内部状況	統治、組織体制、役割及びアカウンタビリティ	統治	脆弱性:組織的対策	組織体制・方針・戦略	現状
		体制			
		役割			
	方針、目的及びこれらを達成するために策定された戦略	経営方針	脆弱性:組織的対策		
		情報セキュリティポリシー群			
	資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）	資本	セキュリティ投資	リソース（人、金、プロセス）	
		人員/時間	リスク評価分析、セキュリティ対策・管理を行う人材		
		プロセス/システム	リスク評価分析、セキュリティ対策・管理方法		
		技術	リスク評価分析、セキュリティ対策・管理を行う技術力		
	内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観	経営者	脆弱性:組織的対策 ※内部組織の関係、認知及び価値観に基づき組織を構成する	内部影響因子	
		セキュリティ管理部門			
		情報システム部門			
		従業者			
	組織の文化	組織の行動原理 ※ITリテラシー	脆弱性:人的対策、技術的対策 ※組織の文化を考慮して人的対策、技術的対策を検討する		
		組織の思考様式 ※ITリテラシー			
	情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む）	情報資産	脆弱性:組織的対策、人的対策、技術的対策、物理的対策	セキュリティ対策の対象=現状のセキュリティレベル	
		情報処理			
		情報資産を取り扱う物理的範囲			
		リスク評価・分析			
	組織が採択した規格、指針及びモデル	規格/指針	脆弱性:組織的対策	現状のセキュリティレベル	
		モデル			
	契約関係の形態、内容及び範囲	従業員との契約	脆弱性:人的対策		
		取引先との契約			

因子への説得、またリソース・人員・投資への再整備などを行うこととなる。

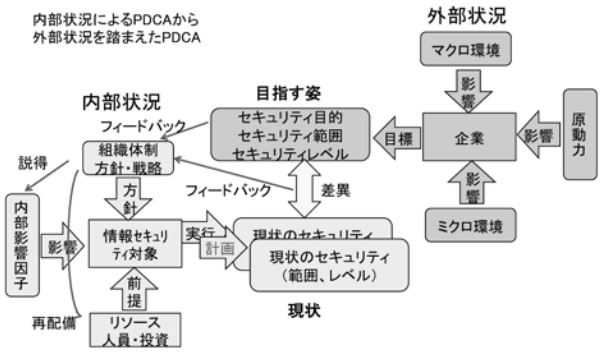

図6　目指す姿との差異が確認された場合

3.5　目指す姿への推進

現状から目指す姿に推進するとき、必ずしも順調にいくとは限らず、正しいと考えていたものが、時代の変化・技術の進歩等により必ずしも正しいとは言い切れなくなることや、失敗、挫折、訂正、変更や後戻りなど、目指す姿へ直線的に最短、最小コストでいけないことのほうが多いかもしれない。

また日常における情報セキュリティは「今そこにある危機」に対して、スピード感をもった対応が要求されるケースもある。

前述の「目指す姿」への推進は、PDCAサイクルのような長い周期（例えば、1年）での取り組みとなるが、日々の脅威や脆弱性の変化の対応や、不幸にも情報セキュリティの侵害を検知した時には、自社への影響、状況を把握し、その対応の意思決定、およびその対応の実行という措置を短期間で行う必要がある。この短期間でのプロセスはOODA（Observe（監視）、Orient（情勢判断）、Decide（意思決定）、Act（行動））と呼ばれ、目指す姿にフィードバックを行うことも考慮する必要がある。

4.　モデル企業での必要な対策を導くプロセス

これまでの検討結果を踏まえ、Risk WGでは様々な企業のケースが考えられるため、いくつかの仮想モデル企業を作成しモデルケースでの経営者への情報セキュリティ対策の必要性を訴求する方法を試案した。

それらのモデル企業毎に、経営者の視点による外部状況、内部状況を整理し、その差異とセキュリティ対策を放置することで招く恐れのある被害を金額で明示する、図7に示す見える化、および目指す姿の差異を改善するための施策を、図8に示す投資費用、回収計画という形で、経営者に向けた見える化の手法の検討を行った。

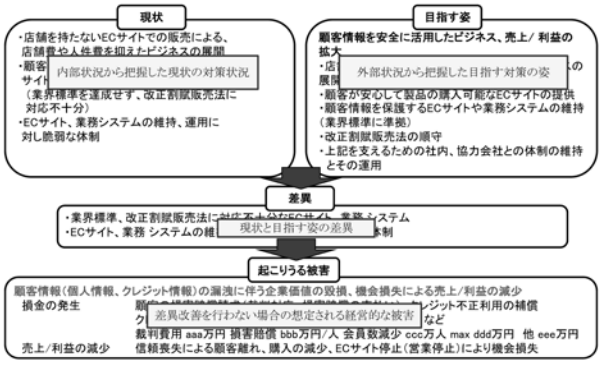

図7　現状と目指す姿の例

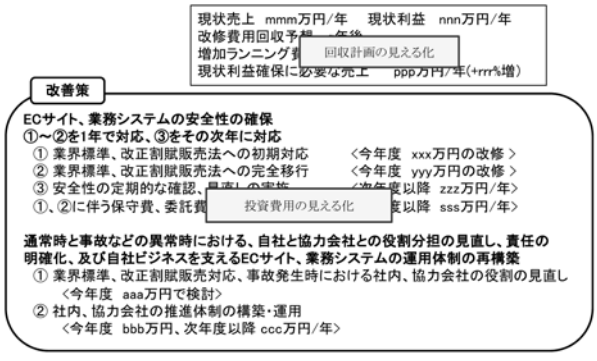

図8　投資計画と回収計画例

5. 最後に

Risk WGの成果物である「経営者のための情報セキュリティ対策　―ISO31000から組織状況の確定の事例―」の第2部には、WGで想定した仮想モデル企業について外部状況、内部状況を整理し、必要な対策を導くプロセスの見える化例を作成しており、経営者にセキュリティ対策の必要性を訴求したい読者の方の参考となれば幸いである。

また、組織がなぜ情報セキュリティ対策を行うのか、その動機付けや情報セキュリティ対策への投資を経営者に決断して頂くためのアプローチを本Risk WGで実施したが、これまでの西日本支部での活動は、情報セキュリティ対策を行うことが前提となっている組織にアプローチする活動であり、西日本支部は図9に示す関連性をもった成果物を作成してきた。

これらについてもご利用頂ければ幸いである。

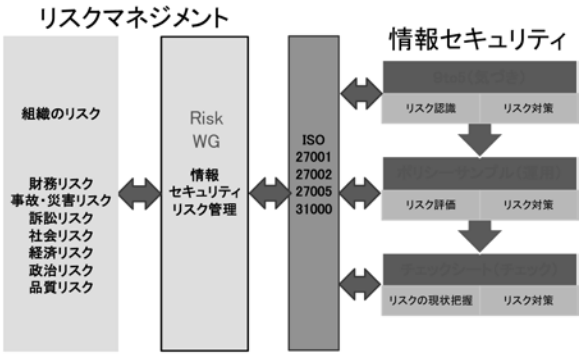

図9　西日本支部の成果物の関係

参考

西日本支部の成果物と参照先

＜気付き＞

「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」　略称：9to5

https://www.jnsa.org/result/2013/chusho_sec/

＜運用＞

「中小企業向け情報セキュリティポリシー・サンプル」　略称：ポリシーサンプル

https://www.jnsa.org/result/2016/policy/

＜チェック＞

「中小企業向け情報セキュリティチェックシート」　略称：チェックシート

https://www.jnsa.org/seminar/nsf/2014kansai/

＜リスクマネジメント＞

「経営者のための情報セキュリティ対策 ―ISO31000から組織状況の確定の事例―」

https://www.jnsa.org/result/2018/west_tebiki/