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―

JNSA　日本ネットワークセキュリティ協会
西日本支部
経営者のための情報セキュリティ対策実践手引き WG

目次

第１部

１ はじめに.....1
２ 背景.....1
３ 目的.....1
４ これまでの成果物と今回の成果物の位置づけ.....2
５ リスクアセスメントとマネジメントの考え方.....3
６ 組織の状況の確定方法.....5
　６．１ 外部状況と内部状況.....5
　６．２ 組織の状況の確定方法.....6
　６．３ 経営環境の分析.....7
　６．４ 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.....8
　６．５ 目指す姿への推進.....11
　６．６ 他のISOとの関係.....11
７ モデル企業での必要な対策を導くプロセス.....12
８ 最後に.....13

第２部

仮想のモデル企業.....14

第１部

１　はじめに

この冊子は、多々あるリスクのうち、情報セキュリティに絞ったものとし、経営者、または、経営者に情報セキュリティ対策を提言する方々を対象としています。

２　背景

現在の社会において、情報システムは経営を支える最重要基盤であり、また様々な分野や方法で我々の生活の中に溶け込んでいます。

この経営を支える情報システムの安定稼働に対する不安材料として、電気や通信の故障などのインフラの問題に加えて、近年では情報システムへのサイバー攻撃や従業者による内部不正など、情報セキュリティに対する問題が浮上しています。

ひとたび情報セキュリティに関連する事故や事件が発生すると、影響を受ける範囲は甚大であり、いままでに、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」ことになります。これまでにも、情報セキュリティ対策に力を入れてきた企業が情報漏洩事故を起こすことで社会から厳しく糾弾された例が多くあります。

また、情報漏洩以外でも、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・停止などによる、経営への影響は計り知れません。

このため、常日頃から、自社の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、それらを把握し、対応を決断することが経営者や経営層の方々に問われています。

３　目的

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、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、必要性の見える化施策を検討することを活動目的としました。背景で記述したような、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戴く方法として、ISO31000（リスクマネジメント）のリスクマネジメントを例にして、自社の組織そのものを評価するための一手段として提示いたします。

リスクマネジメントは、事業継続を目的とする経営者にとって、必須の事案です。

国際標準規格 ISO31000 ではリスクマネジメントに関する原則および指針を規格として提供しています。この規格では、リスクマネジメントの中で、現状に於ける自組織が引き起こすであろうリスクに対し、どのように、また、どの程度対応できるかを検討するうえでの「組織の状況の確定」プロセスが追加されています。

本冊子では、ISO31000 の「組織の状況の確定」と言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、自組織に必要な対策を導くプロセスを、いくつかの業種・業態の仮想のモデル企業例を参考に紹介しています。

４　これまでの成果物と今回の成果物の位置づけ

西日本支部では、これまでに図1に示す成果物を作成した活動を行ってきました。

西日本支部の各活動とその成果物は、日常業務に潜むリスクを認識する「気づき」、認識したリスクを評価し受容レベルの決断、導入する対策の決定、その対策の日々の実施を文書化する「運用」、その対策状況を確認する「チェック」の一連のプロセスを支援するものです。

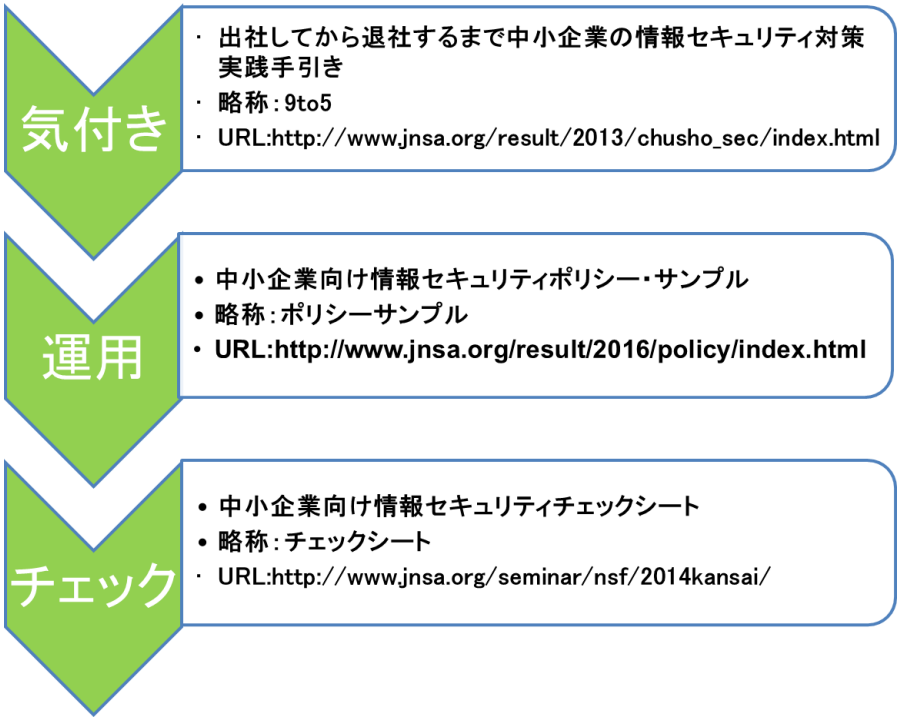
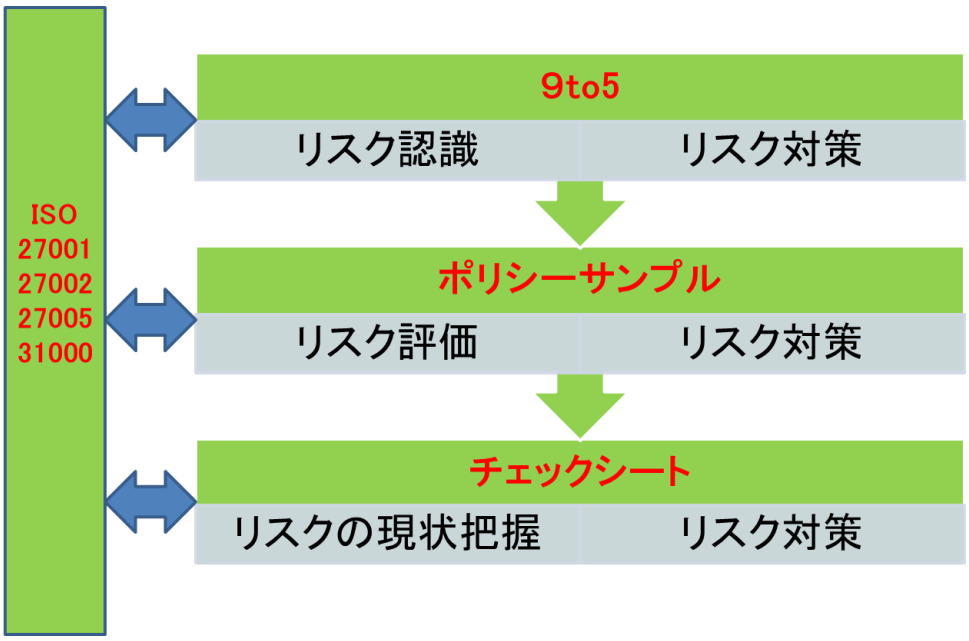


図１　JNSA 西日本支部のこれまでの活動

また、西日本支部の各成果物は、ISO の規格も考慮し検討、作成しており、ISO 規格との関係を図 2 に示します。

図 2 は、各活動での成果物を用いることで、リスク認識、リスク評価、リスクの現状把握を行い、必要な対策の明確化、決定の支援が可能なことを示しています。



ISO27001:情報セキュリティマネジメントシステム(要求事項)

ISO27002:情報セキュリティマネジメントの実践のための規範

ISO27005:情報セキュリティのリスクマネジメントに関するガイドライン規格

図 2　ISO 規格と成果物の関係

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した。そのため、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には不十分です。

西日本支部では、自組織の社会における位置づけ、社会や顧客からの期待を理解し、情報セキュリティ対策の必要性を経営的観点で組織として認識することが、情報セキュリティ対策への投資を経営者の決断につながると考えました。

「自組織の社会における位置づけ、社会や顧客からの期待を理解」とは、「ポリシーサンプル」で公開した「情報セキュリティポリシーサンプル改版(1.0 版) 概要」の「4．2 組織の状況の確定」に示すことであることから、西日本支部では「組織の状況の確定」の見える化施策を検討し、それを本冊子に整理しました。

５　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 3 の位置づけとなります。Risk WG における「組織の状況の確定」の見える化施策の検討では、「ポリシーサンプル」に引き続き ISO31000 を考慮して活動しています。

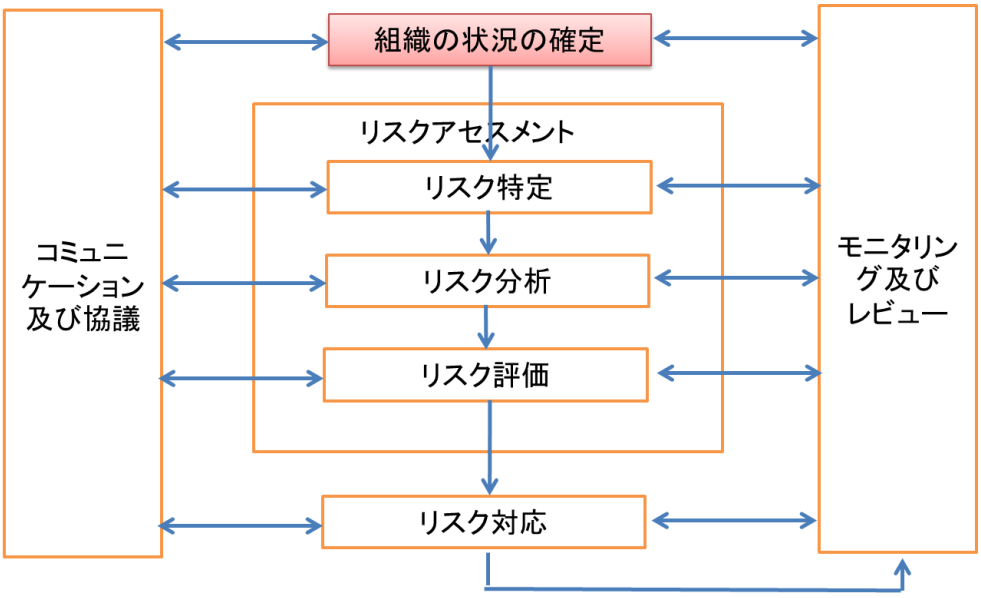


図 3　ISO31000 のリスクマネジメントプロセス

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ます。

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に必要なことは何かを考え、それを図 4 に整理しました。

組織には様々なリスクが存在しますが、情報セキュリティリスクはそのうちの一つです。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ります。

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となって対応することが必要です。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ます。

組織全体で共通の言葉と意味でリスクの認識を持つために、図 4 では情報セキュリティリスクを、システムリスクや品質リスクに分解しています。

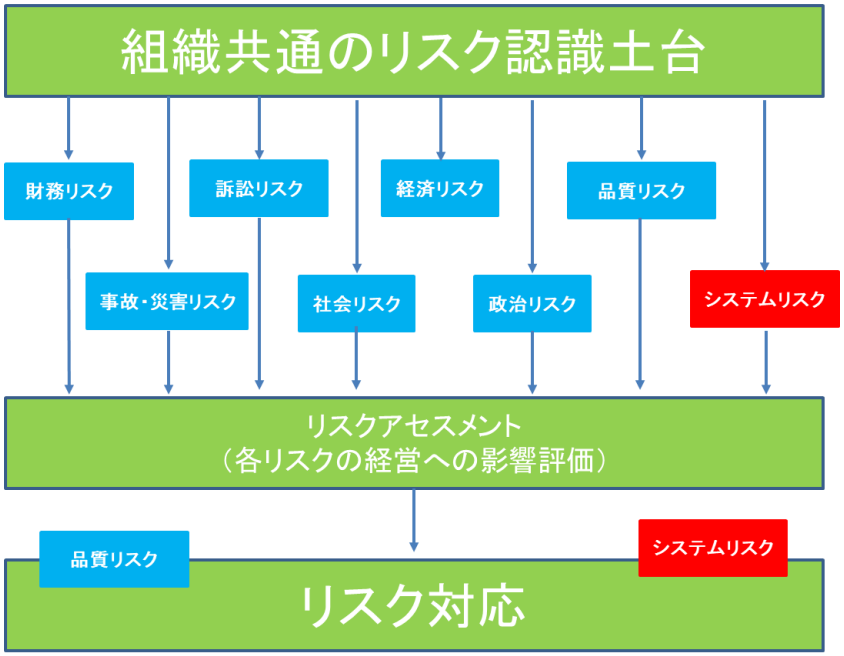


図 4　リスクの共通土台

６　組織の状況の確定方法

６．１　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ます。

以下に ISO31000 に記載されている外部状況、内部状況の例を示します。

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

６．２　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 5 に示す以下の事項が明確にできると考えました。

(1) セキュリティ対策の目的は

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の大きな要因であり、セキュリティ対策の目的となります。

(2) 対策の範囲は

内部状況を見て、目的を達成するために、把握した外部状況、内部状況から対策すべき範囲が明確になります。

(3) どの程度リスクを低減するのか、どの程度のリスクであれば対策を行うのか

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します。

(4) どの程度の予算を充てるのか

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、予算計画を立案します。

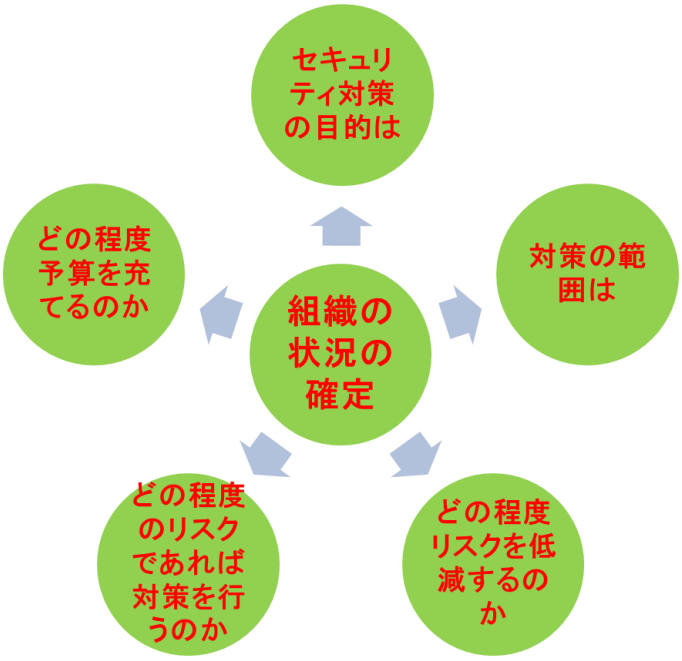


図 5　組織の状況の確定を行う視点とは

共通土台のリスク認識を踏まえたうえで、情報セキュリティ対策に必要な項目が抽出できれば、多様な視点を考慮した組織の状況の確定が行えます。

６．３　経営環境の分析

Risk WG では、経営に訴求する方法として、図6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、検討を行いました。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ます。

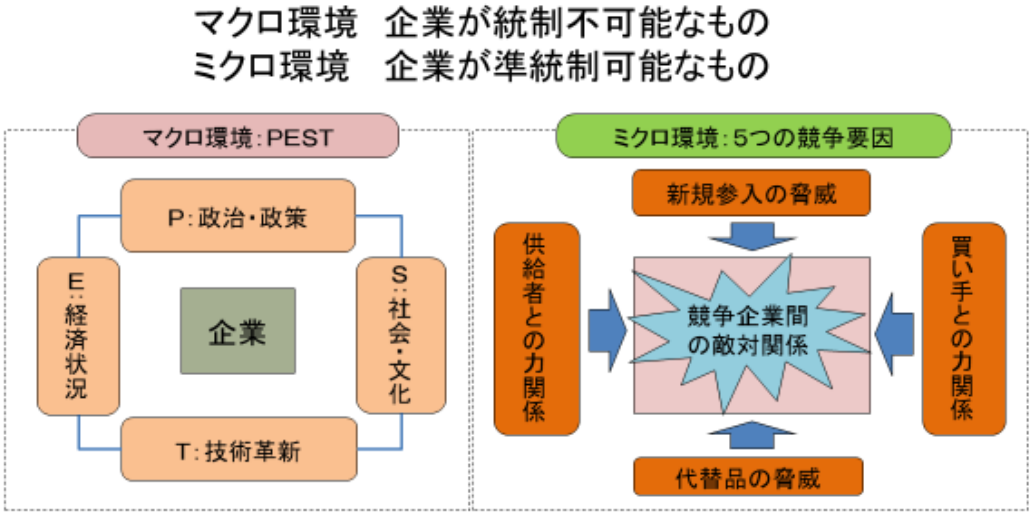


図6　マクロ環境とミクロ環境

ミクロ環境は，ハーバード大学の教授であるマイケル・ポーター氏が提唱したフレームワークで、長期的な投資の収益率を決める際に用いられるものです。

下記の5つの業界の競争要因をもとに、自社が現在どのような状況であるかを分析・判断するための考え方です。

新規参入の脅威
競争企業間の敵対関係
代替品の脅威
買手の脅威
供給業者の脅威

マクロ環境では、企業を取り巻く環境のうち、マクロ的な視点で、現在の、あるいは将来の事業活動に影響を及ぼす可能性のある要素を下記の5つの視点から分析を行います。マクロ環境は、企業が統制不可能なもとのとして、捉えています。

P: Political	政治的環境要因
E: Economic	経済的環境要因
S: Social	社会的環境要因
T:Technologocal	技術的環境要因

自社にとってこれらの要因が、プラスインパクトなのかマイナスインパクトなのか、あるいは状況により影響度を双方に考える必要があるのかを整理していきます。

６．４ 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 に再整理しました。

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ます。

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ります。

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		
		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	現状のセキュリティレベル	
		取引先との契約			

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ます。

・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 7 にその関係を示します。

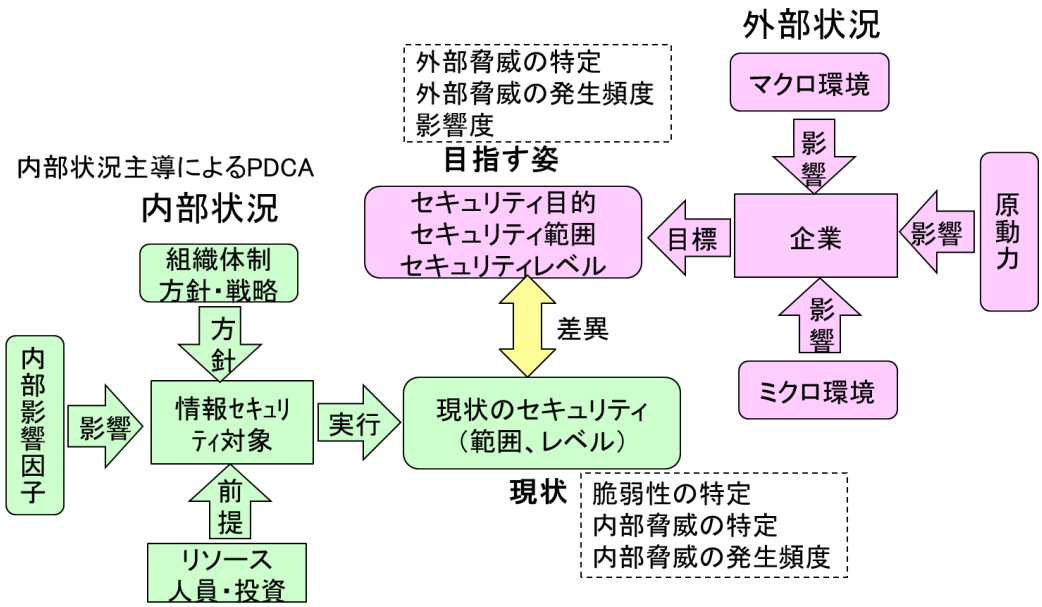


図 7　セキュリティにおける外部状況と内部状況の関連

目指す姿との差異が確認されれば、図8のように、内部状況による PDCA から、外部状況を踏まえて PDCA へと、組織体制や方針・戦略へのフィードバック、内部影響因子への説得、またリソース・人員・投資への再整備などを行います。

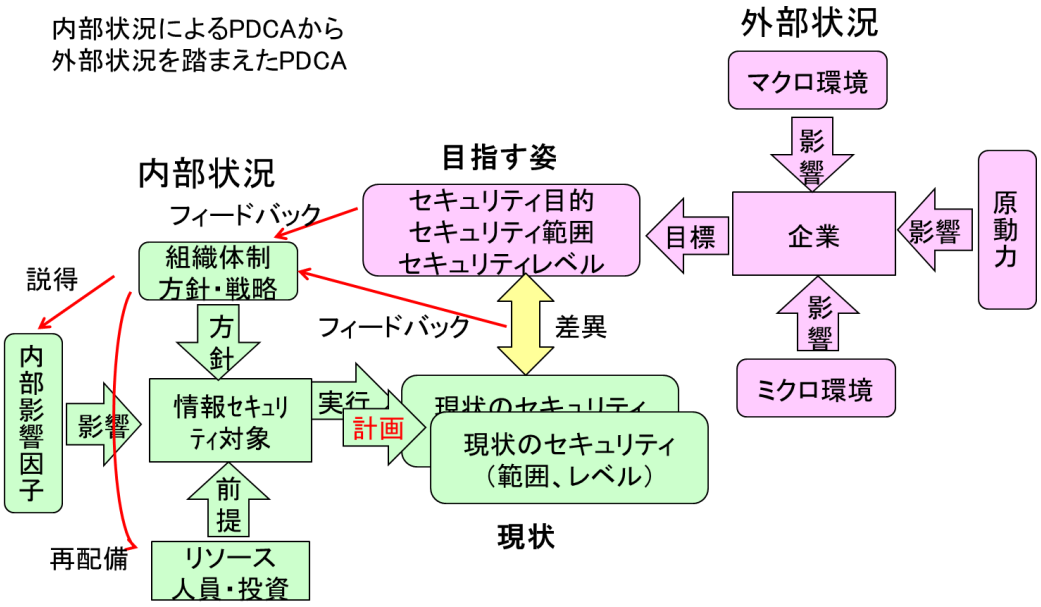


図 8　目指す姿との差異が確認された場合

６．５　目指す姿への推進

現状から目指す姿に推進するとき、図9のように必ずしも順調にいくとは限りません。

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ません（図中では曲線など）。

紆余曲折、前進や後退を繰り返したり、時には立ち止まったりして考え直すときがあるかもしれません。

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ます。

「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）での取り組みとなりますが、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います。

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、その4段階のプロセスから改善点を把握した場合は、目指す姿にフィードバックを行うことになります。

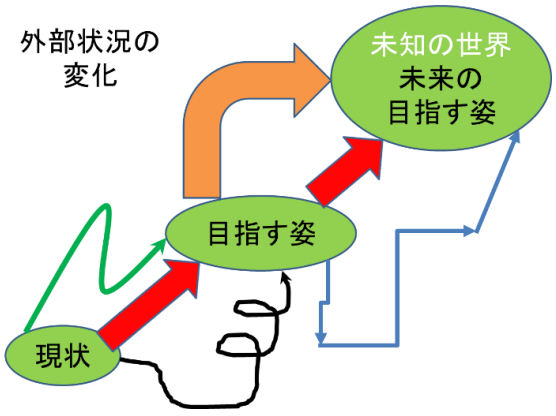


図9　あるべき姿への推進

６．６　他のＩＳＯとの関係

多くの企業では、国際標準である品質に関する ISO9001 や環境基準の ISO14000 をすでに取得されている事業体もあるかと思われます。

ISO31000 では、リスクマネジメントに特化して国際標準化されています。すでに品質や環境基準の取り組みをされている組織においては、この冊子で提案している手法や考え方は理解しやすいと思われます。

7　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、それらの企業毎に、経営者の視点による外部状況、内部状況を整理し、経営者に必要な対策を訴求するために、図 10 に示すプロセスの見える化を行いました。

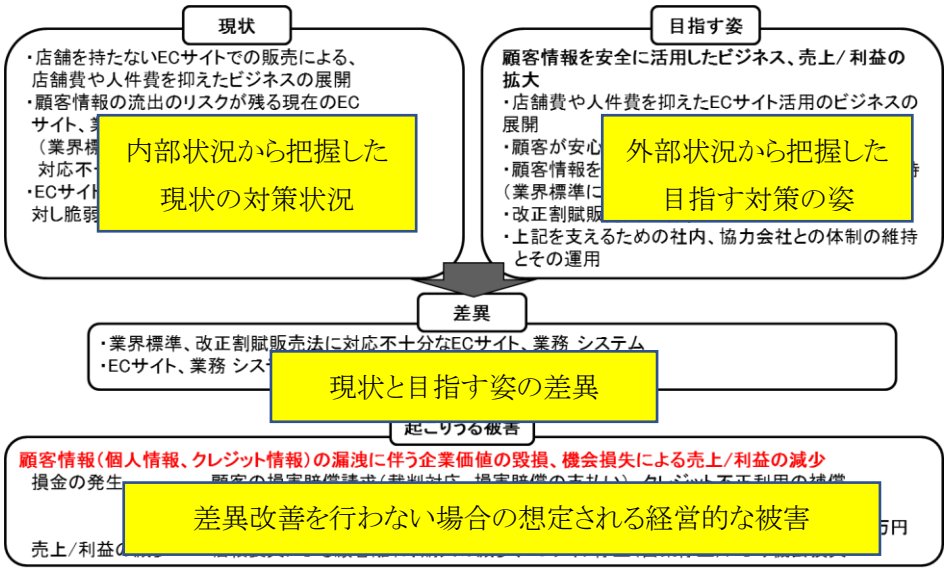


図 10　現状と目指す姿の例

対象が経営者であるため、現状と目指す姿の差異を改善するための施策を、図 11 に示す投資費用、回収計画という形で見える化を行いました。

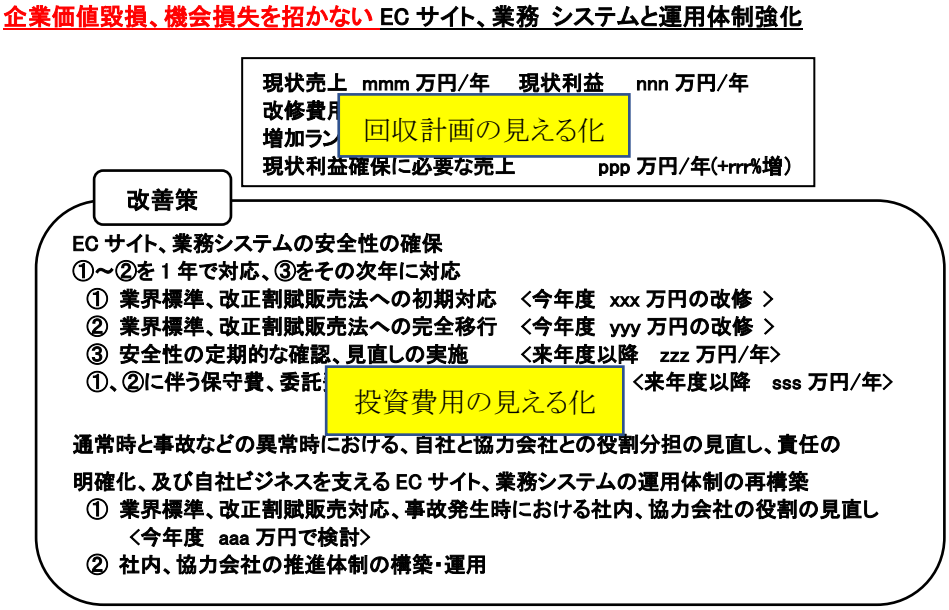


図 11　投資計画と回収計画例

８　最後に

Risk WG での検討結果を基に、「ポリシーサンプル」の「情報セキュリティ方針　7．体制」の体制図を元にリスク管理委員会の企業での位置づけ、体制を見直したものを図 12 に示します。

5ページの「5　リスクマネジメントの考え方」に記載したとおり、組織には様々なリスクがあり、情報セキュリティリスクはその一つです。

経営者、業務部門と情報システム部門が一体となって情報セキュリティリスクに対応していくためには、組織全体のリスク管理委員会において、他の様々なリスクと同じ位置づけで「コミュニケーション及び協議」を行うことが有効です。

また、図 13 に組織のリスクと情報セキュリティリスク管理の位置づけ、および JNSA 西日本支部のこれまでの成果物との関連を示します。

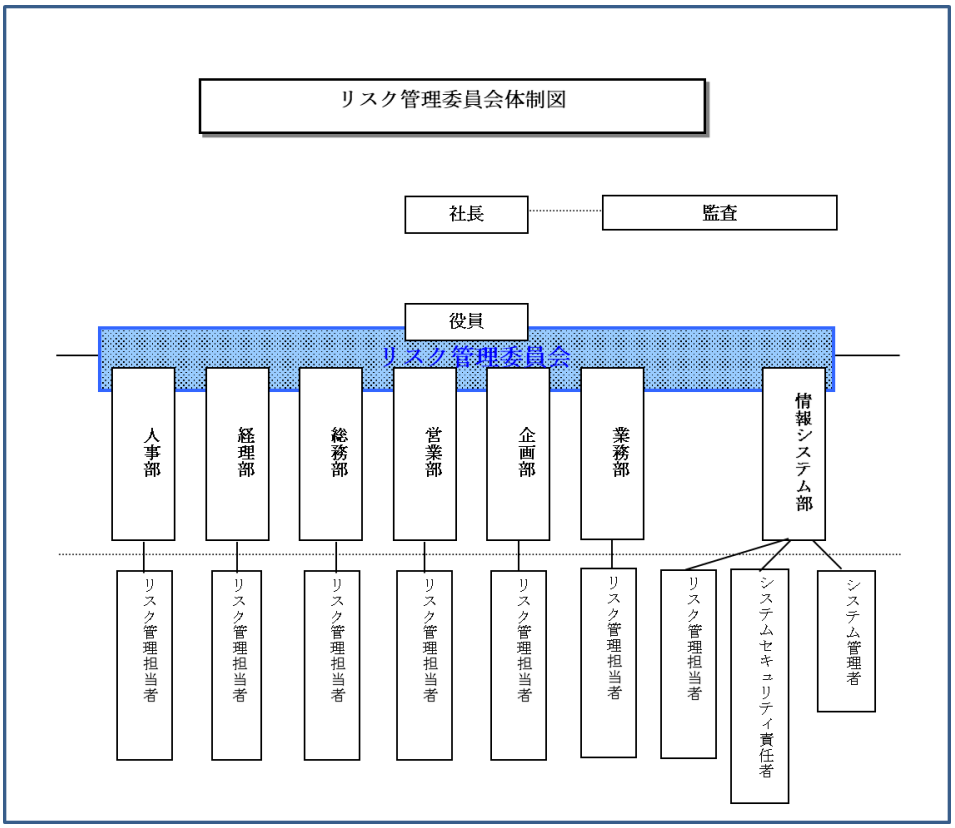


図 12　リスク管理委員会の位置づけ例

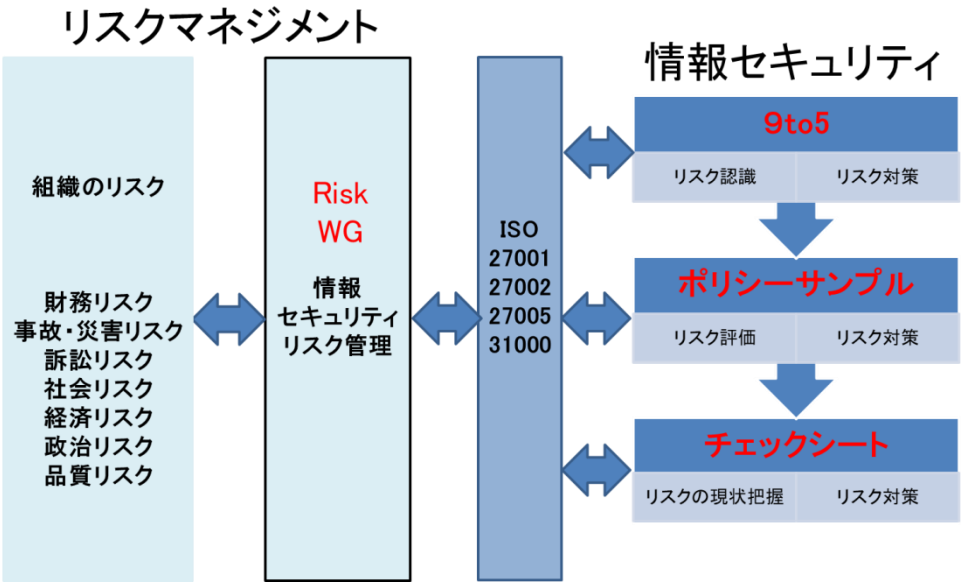


図 13　まとめ

第 2 部では、WGで想定したモデル企業について、組織の状況の確定例を示します。

第2部

仮想のモデル企業

第 2 部ではWGで想定した下記の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の作成を行いました。 なお、各モデル企業については、想像や想定を基に記述しているため、不完全なところなどがあります。その点を考慮いただき、ご利用ください。

それぞれ別紙に示します。

- ECサイト企業
- スーパーマーケット
- 医療機関
- 商社
- 製造業（装置系）
- 製造業（情報系）

経営者向け情報セキュリティ対策実践手引き WG メンバー

井上 陽一	JNSA 顧問
大室 光正	株式会社インターネットイニシアティブ
河野 愛	株式会社インターネットイニシアティブ
久保 智夫	株式会社サーバーワークス
小柴 宏記	ジーブレイン株式会社
嶋倉 文裕	富士通関西中部ネットテック株式会社
久井 隆晶	富士通関西中部ネットテック株式会社
元持 哲郎	アイネット・システムズ株式会社
吉崎 大輔	NECソリューションイノベータ株式会社
米澤 美奈	株式会社ソリトンシステムズ

WG にご協力を頂いた皆様

青木 茂
今井 実
塩田 廣美
西川 和予