情報セキュリティ活動の見える化に関する検討

2013年3月

情報セキュリティガバナンス協議会

目次

1. 調査方針

1.1. 背景と目的

一般に情報セキュリティ活動に関する明確な尺度がないため、組織の情報セキュリティ担当部門では、以下の点で悩むケースが多いと考えられる。

・情報セキュリティ活動の状況や課題等をどのように把握するか

・情報セキュリティ活動の状況や課題等を経営陣にどのように報告するか

前者については、現在、各社が状況把握のために行っている情報収集・分析の方法を比較・整理する方向と、情報セキュリティ上の様々な脅威に対し、どのような対策をどこまでとるのが妥当か、各社の取組みやリスクの許容範囲等を比較し、妥当な水準の考え方を明らかにする方向がある。

後者については、必ずしもITや情報セキュリティの詳細に関して知見が十分でない経営陣が適切に理解し正しい評価を行えるように、情報セキュリティ活動の状況や課題等の報告において各社が行っている工夫（評価項目の設定、可視化等）を整理し、効果的な方法を明らかにする方向がある。

そこで、事例分析等を通じて、上記の方向で情報セキュリティ活動の見える化（情報セキュリティガバナンス活動における「モニタリング」）に関する問題の改善案を提示した。

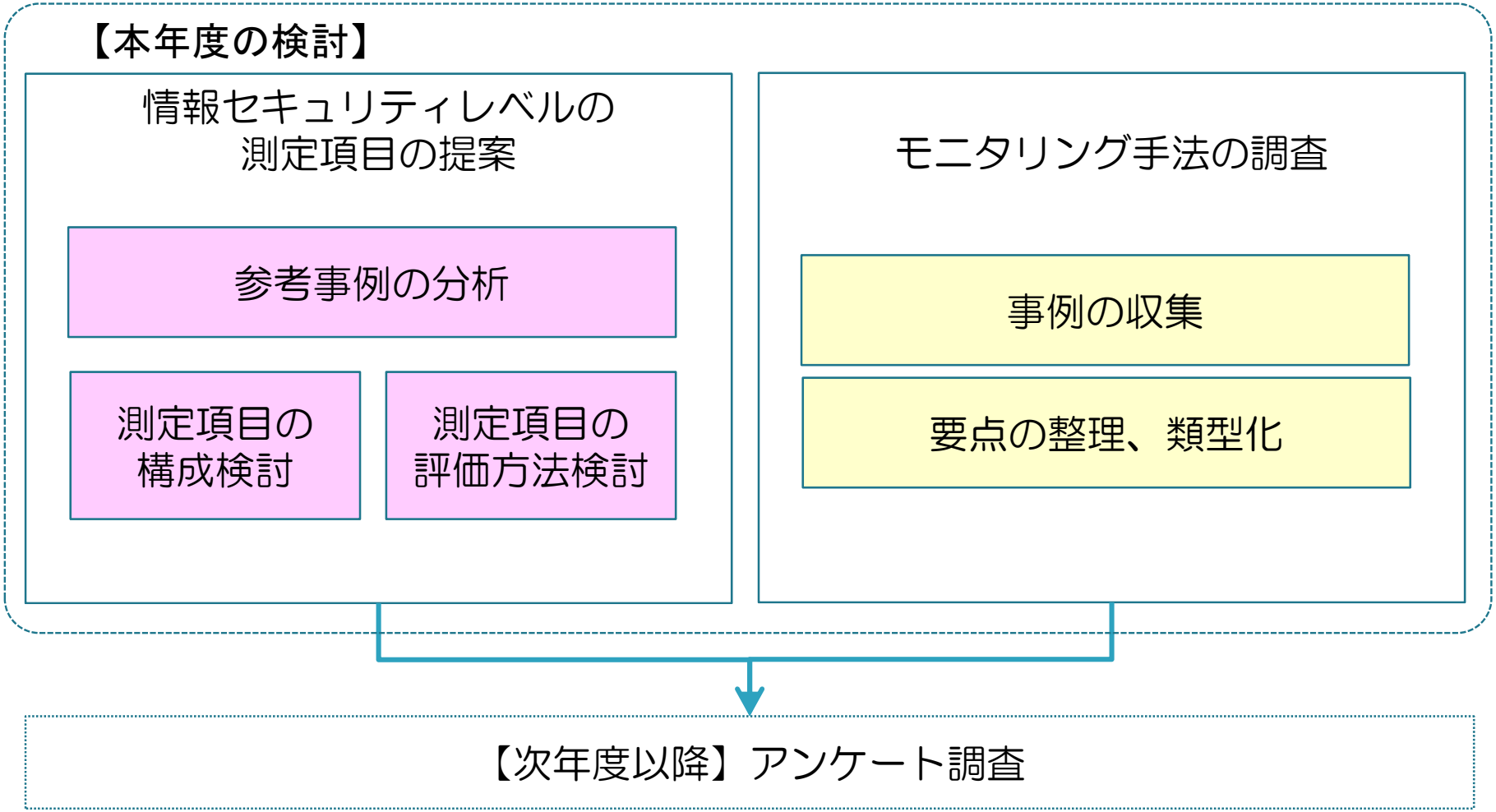
■問題認識

- 一般に情報セキュリティ活動に関する明確な尺度がない
- 情報セキュリティ活動の状況や課題等をどのように把握するか
- 情報セキュリティ活動の状況や課題等を経営陣にどのように報告するか

■目的

- 企業が自社の情報セキュリティの取り組み状況を客観的に評価するための尺度となる測定項目を定める
- 他社（業界等）の状況と自社の状況を比較できるようにする
- 役員への説明（取り組みの必要性の根拠として）に活用できるようにする

1.2. 調査方法


【本年度の検討】
情報セキュリティレベルの
測定項目の提案
参考事例の分析
測定項目の
構成検討
測定項目の
評価方法検討
モニタリング手法の調査
事例の収集
要点の整理、類型化
【次年度以降】アンケート調査

1.3. 検討メンバー

■　メンバー

EMCジャパン株式会社	宮園　充 / 矢野　薫
株式会社 インフォセック	田中　洋
新日本監査法人	佐々木　秀仁
積水化学工業株式会社	竹内　守
富士通株式会社	西見　俊彦
三菱電機インフォメーションテクノロジー株式会社	高原　照明
株式会社三菱総合研究所	川口　修司
持田製薬株式会社	簗取　興史

（事務局）

株式会社三菱総合研究所	江連　三香
株式会社三菱総合研究所	井上　信吾
株式会社neoAge	松岡　照夫

1.4. 検討経緯

第1回WG	6/13(木)	三菱総合研究所	自己紹介、目的・アウトプット等の検討、スケジュール
第2回WG	7/27(金)	インフォセック	事例紹介、文献調査、調査方針検討
第3回WG	9/12(火)	新日本監査法人	事例紹介、調査方針検討、報告書目次イメージ
第4回WG	10/23(火)	積水化学	事例紹介、測定項目・評価方法の検討
臨時WG	10/30(火)	三菱総合研究所	測定項目・評価方法の検討
臨時WG	11/20(火)	三菱総合研究所	測定項目・評価方法の検討
第5回WG	12/13(木)	三菱総合研究所	測定項目・評価方法の検討
第6回WG	1/15(火)	三菱電機インフォメーションテクノロジー	測定項目・評価方法の検討、とりまとめ方針の検討
第7回WG	2/26(火)	三菱総合研究所	測定項目・評価方法の検討、最終報告準備
第8回WG	3/06(水)	三菱総合研究所	事例紹介、最終報告準備
第9回WG	3/19(火)	三菱総合研究所	最終報告準備

2. 情報セキュリティレベルの測定項目の提案

2.1. 参考事例の分析

■ 対象

- 情報セキュリティ対策ベンチマーク（IPA）
- ISO/IEC 27001:2005, ISO/IEC 27004:2009
- SP800-55（NIST）
- 情報処理実態調査（経済産業省）

■ 結果

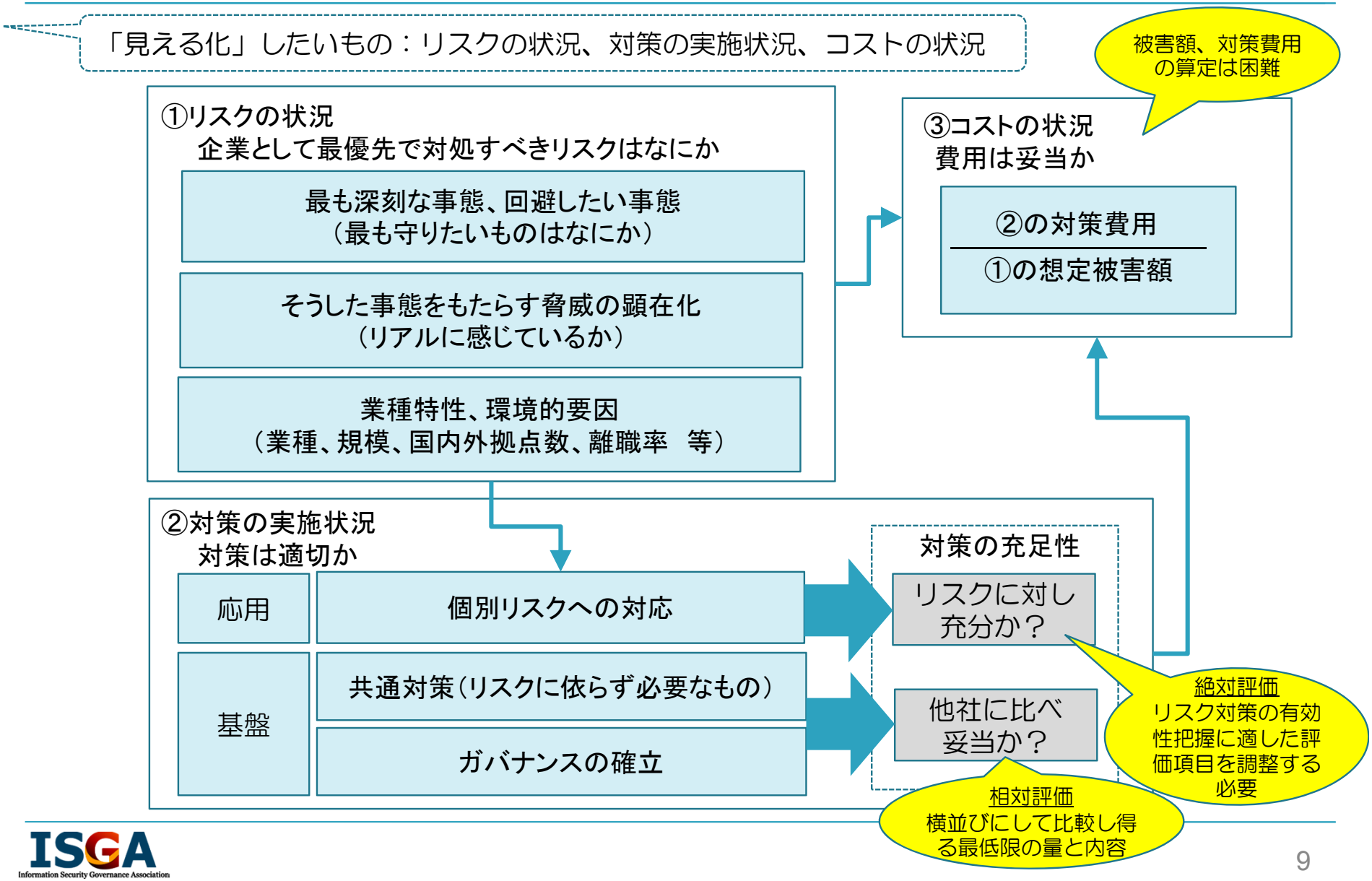
①現在の測定方法に足りない要素

- 情報セキュリティ対策の有効性の測定・評価に関する研究は数多く行なわれてきた。ただし、今のところ、ユーザのニーズを満たす情報セキュリティ対策の評価に関する測定方法は確立されていない。
- 成熟度評価とは別に、対策の強度という観点で、自社の取組が適切なのかを測る方法も必要。
- 必要とされる対策の強度　＝　リスクに対する対策の必要十分性
- 対策の過不足の判定には、対象とすべきリスクの把握が必要。
- リスクの捉え方は、業界属性（どの情報資産が重要で、何をリスクと考えるか）によっても異なる。
  参考事例の中には、それに応えた取組みは見られなかった。

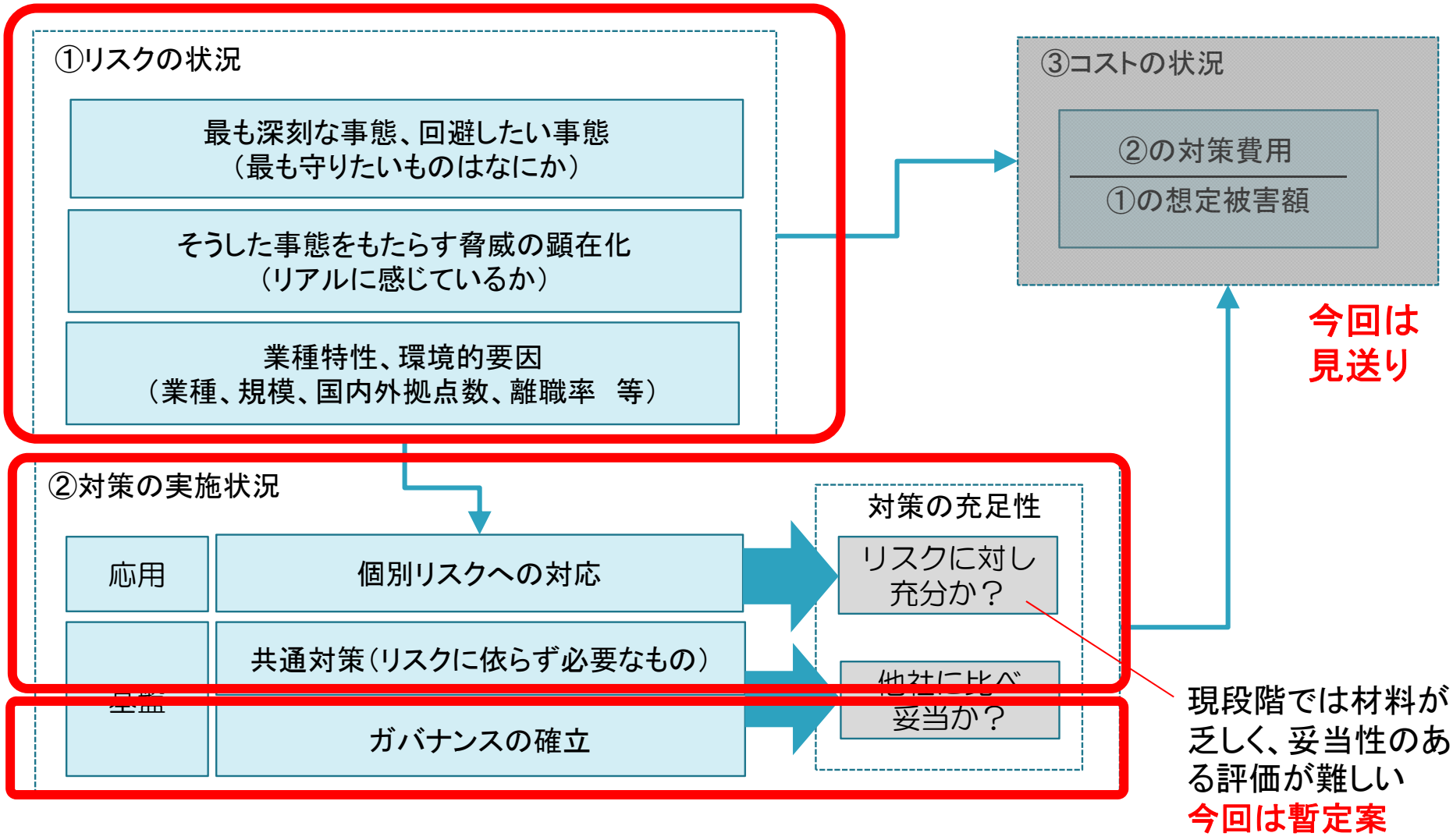
②測定方法のイメージ

- 測定は、ツールによる自動計測やログの解析の他、回答者の自己評価によって実施されている。
  対策の成熟度やルール・制度の状況、技術的対策の状況等
- したがって、測定方法を検討する上で、自己評価の選択肢を工夫することが重要。

2.2. 測定項目の構成（1）全体構造①



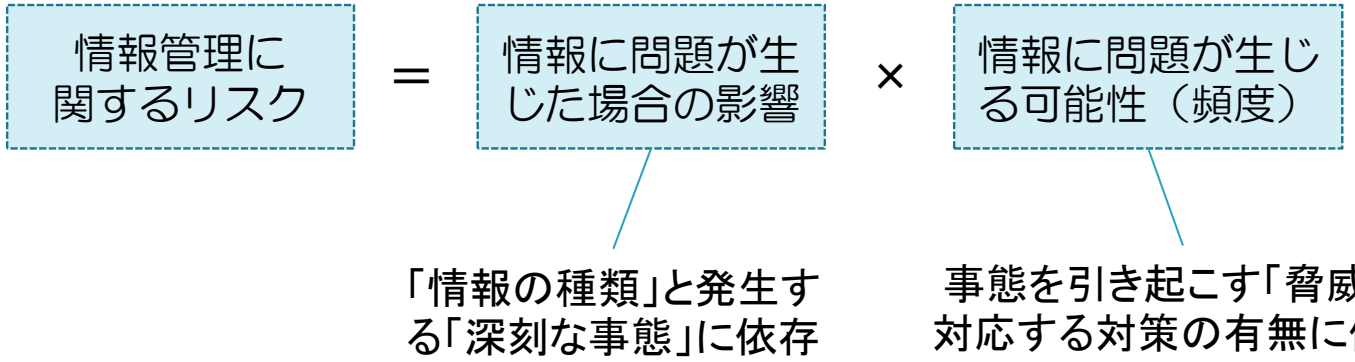
2.2. 測定項目の構成（1）全体構造②



2.2. 測定項目の構成（2）リスクの状況　①考え方

■リスクの考え方

- 情報資産に関するリスク　＝　情報管理に関するリスク　＋　サービス維持に関するリスク
- 情報管理に関するリスクは、情報に問題が生じた場合の影響と、そうした事態が生じる可能性（頻度）によって算定される。
- 情報に問題が生じた場合の影響は、情報の種類と発生する**深刻な事態**に依存する。
- 情報に問題が生じる可能性（頻度）は、その**事態を引き起こす脅威**に依存する。



- サービス維持に関するリスク
  情報システムやネットワークによるサービスの中断　→　事業が中断する事態が発生

2.2. 測定項目の構成（2）リスクの状況　①考え方

■ 類型化の考え方

- 想定しうる**深刻な事態**を検討するため、流出や喪失によって大きな影響を及ぼす重要情報を抽出する。
- ここで重要情報とは、企業の**コアビジネス**（主活動）を支える、価値ある情報をさす。具体的には、**コアビジネス**の事業における業務プロセス（営業、顧客管理、調達、事業企画、設計開発、製造、保守、品質管理）別に重要情報の有無について検討する。

※経営や総務、人事等、業種に依らず共通に存在する業務については、コアビジネスに直結しないため、ここでは検討対象から除く。

コアビジネスの分類	概要	対象事業の例
規制分野	・ 所管省庁の許認可や規制が厳しい分野 ・ 申請や記録等に係る完全性が重視される	金融、医薬品、防衛、エネルギー、通信
企画競争分野	・ 設計や製造方法、デザイン等秘密が多い分野 ・ 委託先も含めた機密性が重視される	ゲーム、広告、デザイン家電、
量産・汎用分野	・ 製品やサービスの差別化が難しい分野 ・ 継続・安定的な製造・サービス供給が重要	日用品、定型サービス

2.2. 測定項目の構成（2）リスクの状況　②重要情報・重要サービスの種類

■ コアビジネスにおける重要情報や重要サービスの例

業務プロセス / コアビジネス	営業	顧客管理	流通	企画設計	製造	運用保守	品質管理
規制型 ・法令遵守 ・申請・報告		△顧客のセンシティブ情報		○実験・試験データ		○トラブル対応情報 □制御システム	
企画競争型 ・競争優位				△アイディア △デザイン △実験・試験データ △技術情報	△設計図面 △製造工法 △レシピ △ノウハウ		△苦情情報
価格競争型 ・低価格化 ・事業継続	△営業先リスト △販売価格		□仕入先リスト △仕入価格		□生産システム △製造工法 △生産ライン △レシピ △ノウハウ	□サービスインフラ	△苦情情報

完全性重視○、 機密性重視△、 可用性重視□

■重要情報の管理場所

1: サーバ　3: ネットワーク　5: モバイル機器
2: 端末　4: メディア　6: 書類

対策の選択に必要

2.2. 測定項目の構成（2）リスクの状況　③「深刻な事態」のイメージ

■ 深刻な事態のイメージ例

事業分類	生じうる問題	「深刻な事態」のイメージ例
規制分野	情報漏えい	・顧客のセンシティブ情報が漏えいし、謝罪、賠償等の対応が必要となる
	情報改ざん	●申請・報告したデータに誤謬が生じ、事業の許認可が取り消しになる
	情報喪失	・保存が義務付けられているデータを喪失し、管理義務違反とされる
	サービス中断	●常時運用が義務付けられている社会サービスを中断し、社会問題となる
企画競争分野	情報漏えい	●重要なアイディアやデザイン、試験データ、レシピ、ノウハウ等が漏えい、競合他社に知られてしまい、競争優位を失う
	情報改ざん	・試験データの改ざん、喪失が発生した場合、試験のやり直しが必要となり、時間とコストが無駄になる
	情報喪失	
量産・汎用分野	情報漏えい	・仕入価格や販売価格が漏えいすると、仕入先や販売先に迷惑をかけることがある ・生産ラインや製造ノウハウの情報が漏えい、競合他社に知られてしまい、低コスト・高歩留まりの優位性を失う
	情報改ざん	・仕入額や販売額に誤謬が発生すると、結果的に取引先に迷惑をかける
	情報喪失	
	サービス中断	●制御システムにマルウェアが混入し、生産システムやサービスインフラに障害が発生する ・仕入先や仕入額のデータを喪失し、支払が遅れると、仕入先が倒産することもある

●：特に深刻な影響を及ぼすと考えられる事態

■ 評価

1: ほとんど影響なし
2: 一部に影響がある
3: 大きな影響がある
4: 深刻な影響がある

ホームページ上で評価対象者がコアビジネスを選択すると、想定される「深刻な事態」が提示され、それらが自社のコアビジネスに及ぼす影響を評価する

2.2. 測定項目の構成（2）リスクの状況　④脅威と発生可能性

■主な脅威の項目

ISO/IEC 27005:2011「情報セキュリティリスクマネジメント」附属書C（典型的な脅威の例）を参考に、現在の企業において一般的に採り上げられることの多い脅威をリストアップ

■評価

1：ほとんどない
2：可能性はある
3：他社では発生した
4：自社で発生した

脅威の分類				主な脅威
物理的脅威	偶発			災害等（地震、洪水、落雷、火災、テロなど）
				設備の事故（停電、断水、空調故障、ケーブル損傷など）
	人為	アクセス権限なし		不正な立ち入りによる持ち出し・盗難
				盗み見
				（立ち入れる場所での）端末、媒体の盗難
		アクセス権限あり	故意・過失	端末、媒体の不正な持ち出し
				端末、媒体の移送時の漏えい、紛失、盗難、破損
				端末、媒体の持出し時の漏えい、紛失、盗難、破損
				端末、媒体の廃棄時の漏えい
情報システム的脅威	偶発			トラフィック／処理の過負荷、容量オーバー
				HW障害、SW障害、NW障害
	人為	アクセス権限なし		コンピュータウィルス等の悪意あるソフトウェア
				DDoS攻撃
				不正アクセスによる改ざん・破壊
				不正アクセスによる漏えい
				ユーザIDのなりすまし
				通信の盗聴・改ざん
				通信経路の不正変更（フィッシング等）
		アクセス権限あり	故意・過失	情報の改ざん・破壊
				無許可の利用者・不正な方法でのリソース使用
				ソフトウェアや外部サービスの違法な使用
				電子メール等通信経由の情報漏えい
				システム利用時のミス
				システム運用時のミス
				システム変更時のミス

2.2. 測定項目の構成（3）対策の実施状況　①対策項目と評価方法

■評価シートのイメージ

（オフィスの入退管理）
大問10．オフィス（建物・フロア・部屋）への防犯対策を実施していますか。
※対応するリスク
【サーバ、ネットワーク】
・なし
【PC、モバイル機器、電子媒体、紙媒体】
・第三者の不正な立ち入りによる持ち出し・盗難
・第三者の盗み見
・第三者が立ち入れる場所での端末、媒体の盗難
・端末、媒体の不正な持ち出し

選択肢）

ほぼ実施済み	（80～100点のイメージ）
大部分は実施済み	（50～79点のイメージ）
大部分は未実施	（30～49点のイメージ）
ほぼ未実施	（　0～29点のイメージ）

他社実施率

小問1－1．扉や窓は、開放時以外は施錠している	（はい／いいえ）XX%
小問1－2．入退出の記録をとっている	（はい／いいえ）XX%
小問1－3．部外者が入る際はバッジ等を着用させる	（はい／いいえ）XX%
小問1－4．接客等の区画ははっきり区別している	（はい／いいえ）XX%

大問を30～50項目程度とする。情報セキュリティ対策として大まかな分類をし、自社での実施の程度を評価してもらう。

大問1つにつき小問を5～10項目程度とする。全体で150～200項目程度とする。具体的かつ細かい対策項目に対して、自社での実施有無を「はい」「いいえ」の二択で評価してもらう。

回答者は、自社における対策の実施有無を回答する。主観を交えず客観的に回答できるよう、項目内容は具体的なものとする。
小問への回答は、大問に回答する際の参考にする目的でのみ必要である（総合評価自体は大問への回答から算出され、小問の回答は影響しない）。

回答者は、自社における対策の実施程度を自己判断して回答する。大問への回答を集計したものが、総合評価となる。
回答の判断には回答者の主観が含まれるが、以下の情報を参考にすることで、根拠ある判断ができるようにする。
・この対策が対象とするリスク項目、および自社にとってのリスク状況
　⇒自社の事業特性を鑑みて、高度な対策まで行って初めて満点であるのか、それとも世間並みの対策を行っていれば満点とみなせるかの判断根拠
・この対策に含まれる小問対策の他社実施率、および自社の実施有無
　⇒自社での対策の実施状況が、世間並みなのか、世間並みより高度な対策をしているのか、世間並みより対策不足なのか、の判断根拠

2.2. 測定項目の構成（3）対策の実施状況　①対策項目と評価方法

■評価結果の算出方法

【全体的な評価結果】

評価シートに回答した結果、大問1問につき1～4点のスコアがつく。
これを対策分野別に集計した平均得点(※1)を、レーダーチャート形式で図示する。この図は「自社の対策状況において、対策がすでに整備されている分野／対策漏れの多い分野を把握すること」を目的とする。
また、他社での平均得点を同様のレーダーチャートで図示し、これと自社の図とを比較すれば「世間一般の対策状況とくらべて、対策が十分なのか／対策が不足しているのか／対策を実施しすぎなのかを評価すること」ができる(※2)。
また今後、評価事例が多数集まれば、業種別・企業規模別などにより、自社のリスクと似通った他社の対策状況と比較を行うことも可能である。

【大問ごとの評価結果】

全体評価を把握した上、さらに個々の分野についての詳細を見たい場合のために、大問単位での回答（1～4点）を表またはグラフで図示する。また大問ごとに他社の平均得点を掲載し、自社の回答と比較できるようにする。
自社のリスクの状況から見て、重点的に行うべき対策は強調して記載される（【別紙3】脅威・対策の対応付けによる）。これを参照すれば「自社にとってとくに重要な対策において他社平均に比べて対策が不足していないか？」、また逆に「自社にとって重要でない対策において他社平均よりも対策し過ぎていることはないか？」といった評価を行うことができる。
また今後、評価事例が多数集まれば、業種別・企業規模別などにより、自社のリスクと似通った他社の対策状況と比較を行うことも可能である。

【小問ごとの評価結果】

大問ごとの評価から、さらに具体的に対策単位での実施状況を見たい場合のために、小問単位での対策実施有無の回答（はい／いいえ）も掲載する。
小問ごとに他社での実施率（パーセント表示）を併記し、他社の多くで実施している対策と自社で実施済み対策とを比較できるようにする。

2.2. 測定項目の構成（3）対策の実施状況　②ガバナンス項目と評価方法

■ 情報セキュリティガバナンスのプロセスに関する評価項目案
ISO/IEC 27014の検討を踏まえ作成

大項目	対象	中項目	小項目	評価尺度
評価	経営陣	事業の推進役が情報セキュリティ問題を考慮することを保証する。	経営陣は、事業責任者に対し、情報セキュリティの問題が各々の事業に与える影響について検討するように、指示していますか。	1.大半の事業に対して実施している 2.一部の事業に対してのみ実施している 3.ほろんど実施していない
		情報セキュリティの実績結果に対応し、必要な措置の優先順位を決めて開始する。	経営陣は、自社の情報セキュリティの取組状況について定期的に報告を受けていますか。	1.定期的に評価可能な報告（達成率等）がなされている 2.不定期だが評価可能な報告（達成率）がなされている 3.報告はあるが、評価可能な形ではない 4.経営陣への報告は実施していない
			経営陣は、情報セキュリティの取組状況から、優先順位を踏まえて、次の行動（例：戦略の見直し）を指示していますか。	1.経営陣が報告を踏まえて指示を出している 2.経営陣が指示を出すが、報告を踏まえていない 3.経営陣からは指示を出していない
	CISO	情報セキュリティが事業目的を十分にサポートして支えることを保証する。	.CISOがコアビジネスの実施に必要な情報セキュリティの取組を実施していることを確認していますか。	1.CISOが定期的に確認している 2.CISOが確認することがある 3.CISOは確認していない
		有意な影響力を持つ新しい情報セキュリティプロジェクトを経営陣に提言する。	CISOは、経営陣に対し、新規の情報セキュリティプロジェクトを提案し、その必要性について説明していますか。	1.CISOが経営陣に提案し、その必要性を説明している 2.CISOは経営陣に提案するが、その必要性を十分に説明できていない 3.CISOからは経営陣への提案を行っていない

「指導（方向付け）」、「監視（モニタリング）」、「説明」、「保証」についても別途作成

2.3. 課題

- リスクに対する対策の必要十分性の評価については、現段階では材料が乏しく、妥当性のある評価項目の構成になっていない。しかし、この評価は、本来、本検討の動機にも当たる要素であり、改善が望まれる。そのためには、企業における対策の取組状況等について把握し、それに応じて評価項目を調整する必要がある。

- 想定している設問構成が、情報セキュリティ対策の実施状況に加え、トラブルがもたらす事業への影響、ガバナンスなど、多岐に渡っているため、すべての項目に回答できる人材があまりいない可能性がある。回答企業において、セキュリティ担当者が現場とどうやって情報共有するか検討すべきである。

- 対象者が的確にリスクを把握するためには、対象者にとってできるだけリアリティのある「深刻な事態」を提示することが有効である。したがって、「深刻な事態」のバリエーションを充実させることが望ましい。

- 対策項目については、全体で大問41件、小問236件とした。対策項目の項目数は多過ぎると回答者に負担となり、少な過ぎると適切な把握が難しくなるため、バランスが重要となる。その意味で、内容やバランスについてさらなるブラッシュアップを図ることが望まれる。

3.モニタリング手法の調査

3.1. 調査方針

■めざす方向
経営陣、CISOに報告する情報の集約・可視化について、具体的な事例を集める

■検討課題
・分析すべき評価項目
・収集すべきデータ
・提示方法

■検討方法
(1)事例の収集
(2)要点の整理
(3)課題の抽出

■モニタリング手法の参考
•参考5　情報セキュリティガバナンス導入ガイダンス（経済産業省）

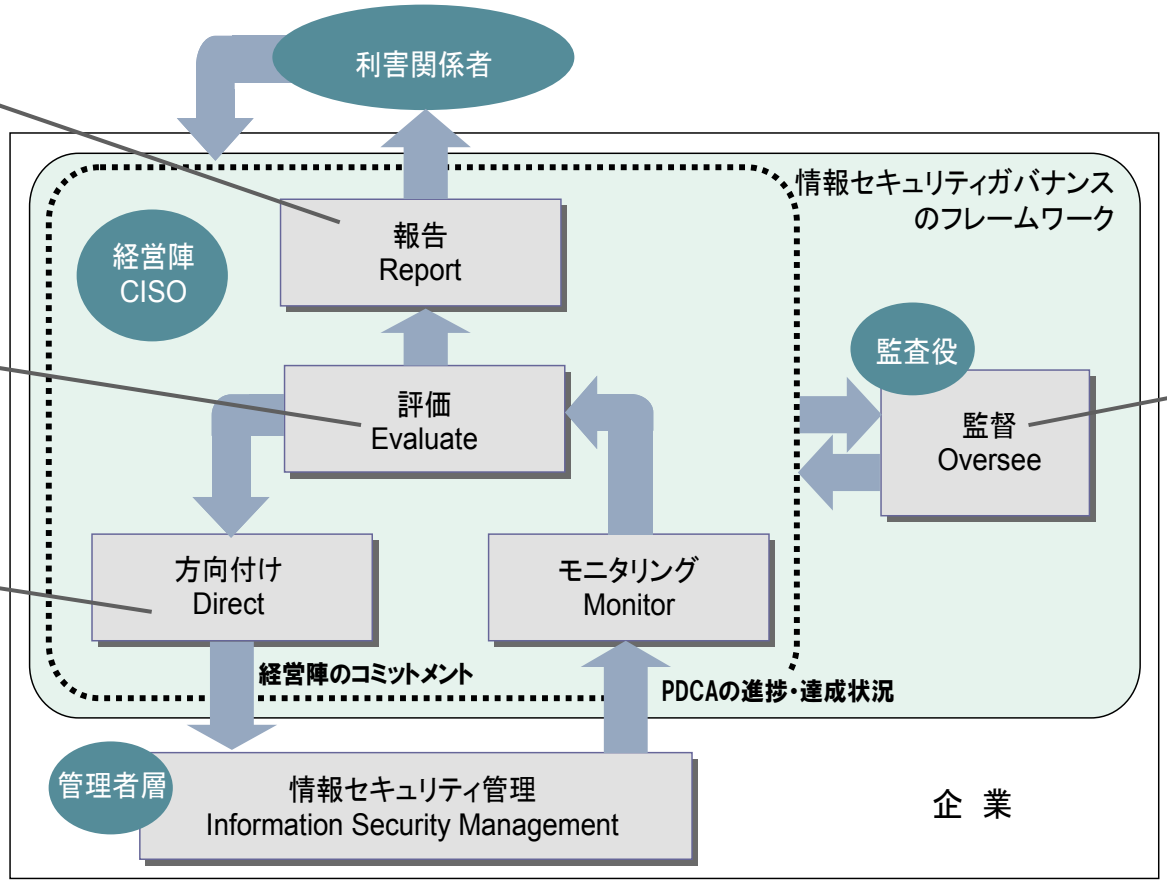
参考　情報セキュリティガバナンス導入ガイダンス（経済産業省）①

情報セキュリティガバナンスのフレームワークを提供し、企業内に導入する手順を解説。

情報リスクの管理状況について、経営陣が利害関係者に説明する

目標・目的が達成されているか、それが適切であったかを経営陣が評価する

経営陣が情報リスクの管理方針や目標・目的を示す



そうした仕組みが機能していることを監査役等が確認する

情報セキュリティガバナンスのフレームワーク

（出典：経済産業省「情報セキュリティガバナンス導入ガイダンス」, 2009/06を基に作成）

参考　情報セキュリティガバナンス導入ガイダンス（経済産業省）②

■モニタリング
経営陣、CISO、管理者それぞれの「方向付け」した内容が適切であるか、達成状況、適用状況の実情を適時に把握すること

■経営陣が行うモニタリング項目の例
・ 経営環境の変化
・ リスクの変動や新規リスクの発生が起きているか
・ 情報セキュリティ投資効果
・ リスク分析の結果に照らして期待されるリスク低減の効果が発揮できているか
・ 情報セキュリティ目的・目標の達成度評価
・ リスク管理方針が実装できたか

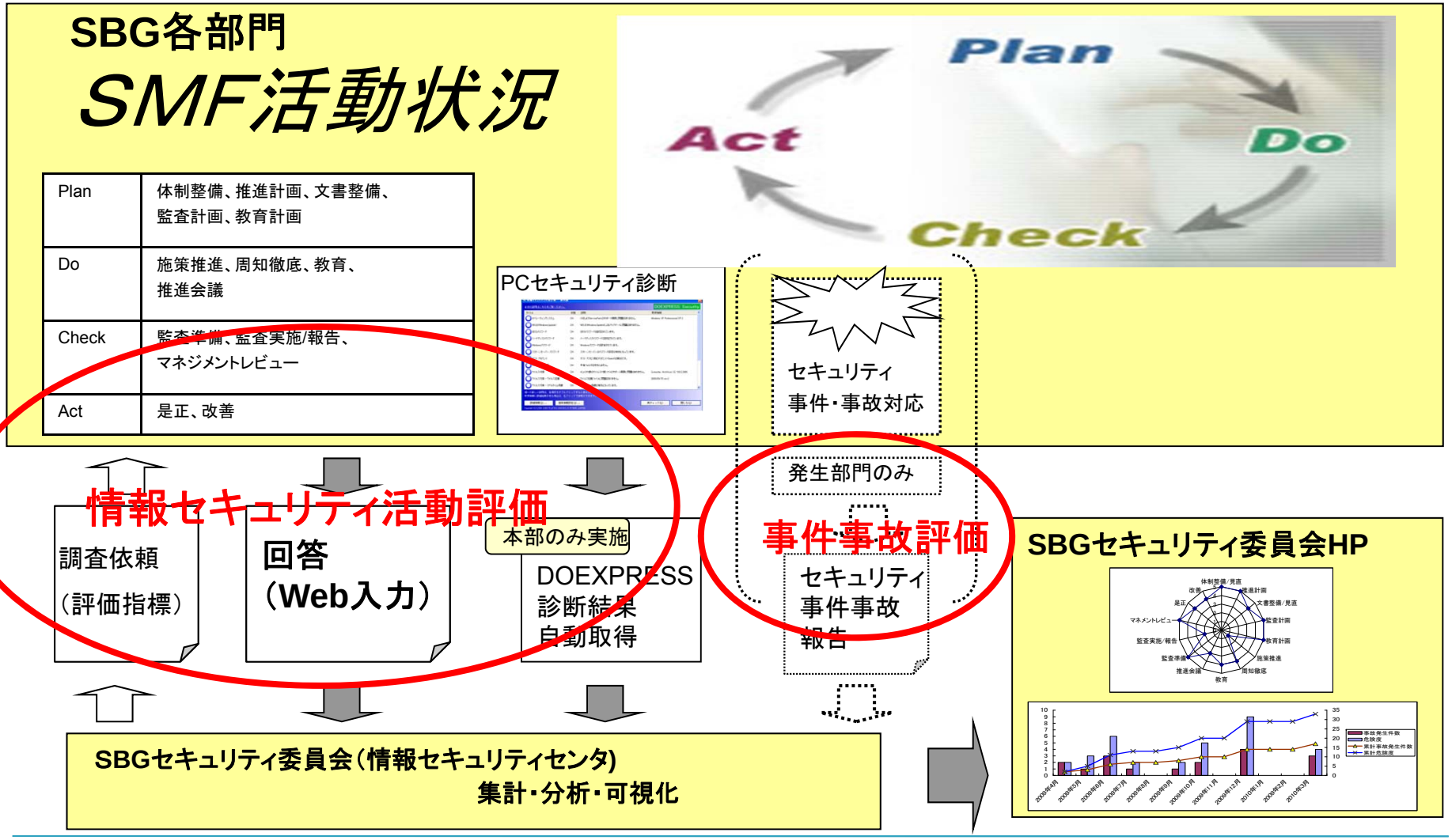
■CISOが行うモニタリング項目の例
・情報セキュリティ投資効果
・ リスク管理方針に照らして有効かつ効率的な投資であったか
・ 情報セキュリティ目標の達成状況
・ 情報セキュリティ目的が達成できたか
・ PDCA の進捗・達成状況
・ 情報セキュリティマネジメントが機能しているか

情報セキュリティ管理策に基づくモニタリング指標の例

分野	モニタリング指標の例
人的・組織的セキュリティ	情報セキュリティ委員会の開催数と参加率
	情報セキュリティ教育の受講者数と受講率
情報資産	情報資産リストの登録数と適用率
	リスクアセスメントの実施数と適用率
	PC 管理規程の見直し回数
システム開発	セキュリティ要件定義書の策定数と適用率
	Web アプリケーションセキュリティガイドラインの適用数と適用率
システム運用	ポリシーに準拠した ID 管理の適用数と適用率
セキュリティ監査	バッチ管理の適用数と適用率
	ぜい弱性診断の診断回数とぜい弱性の発見数
	監査回数と指摘事項数
セキュリティ事故	不正アクセス、ウイルス感染等の事故件数と復旧までの時間（RTO）
	個人情報流出事象の発生件数と影響規模

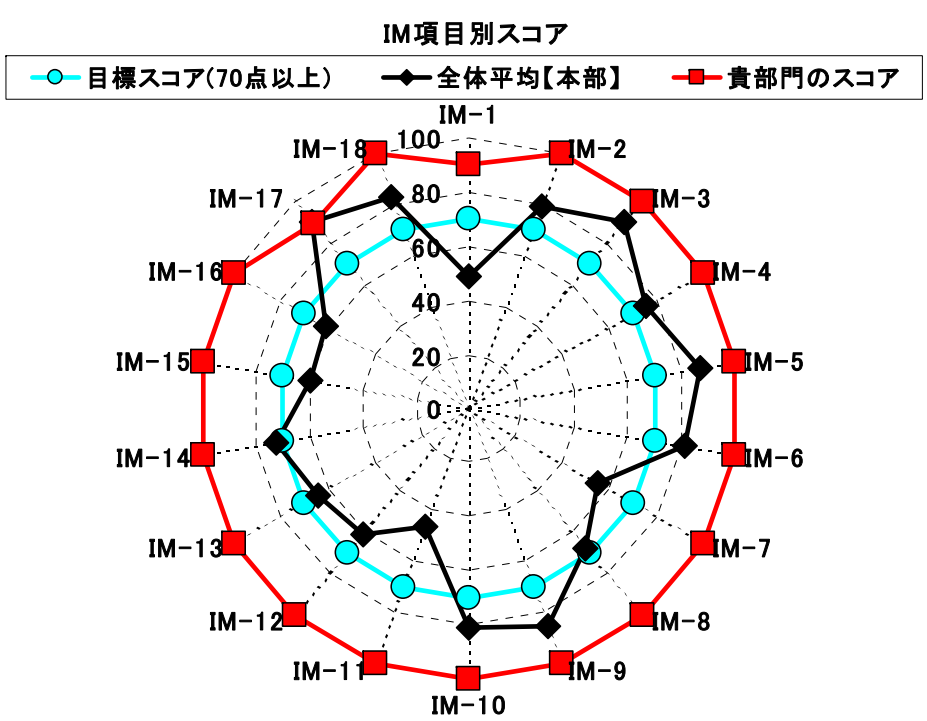
3.2. 事例A：①実施概要

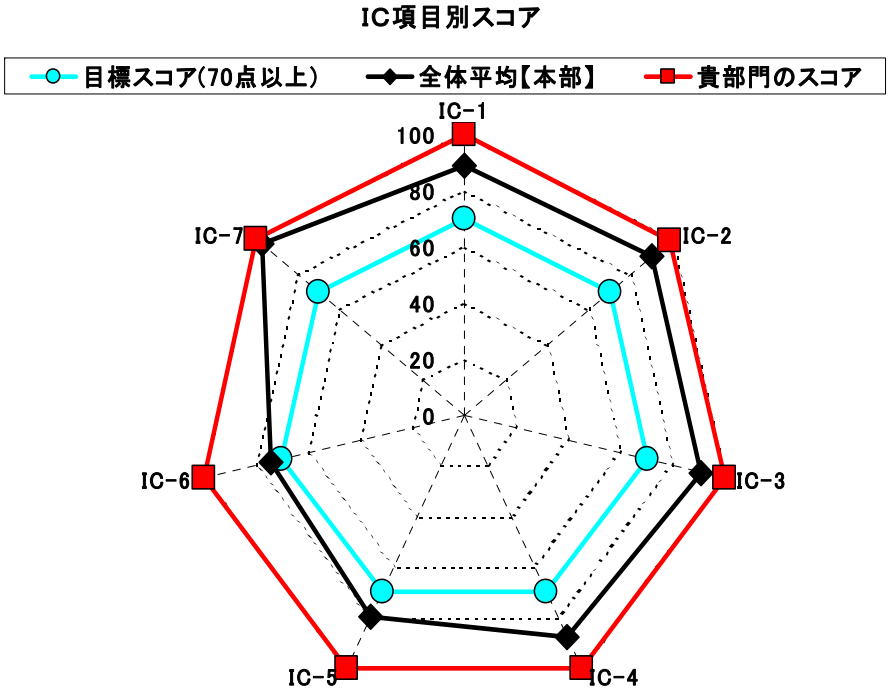
実施概要（イメージ）



3.2. 事例A：②活動の評価・可視化

情報セキュリティ活動の評価指標を策定
実施度・達成度を評価・可視化



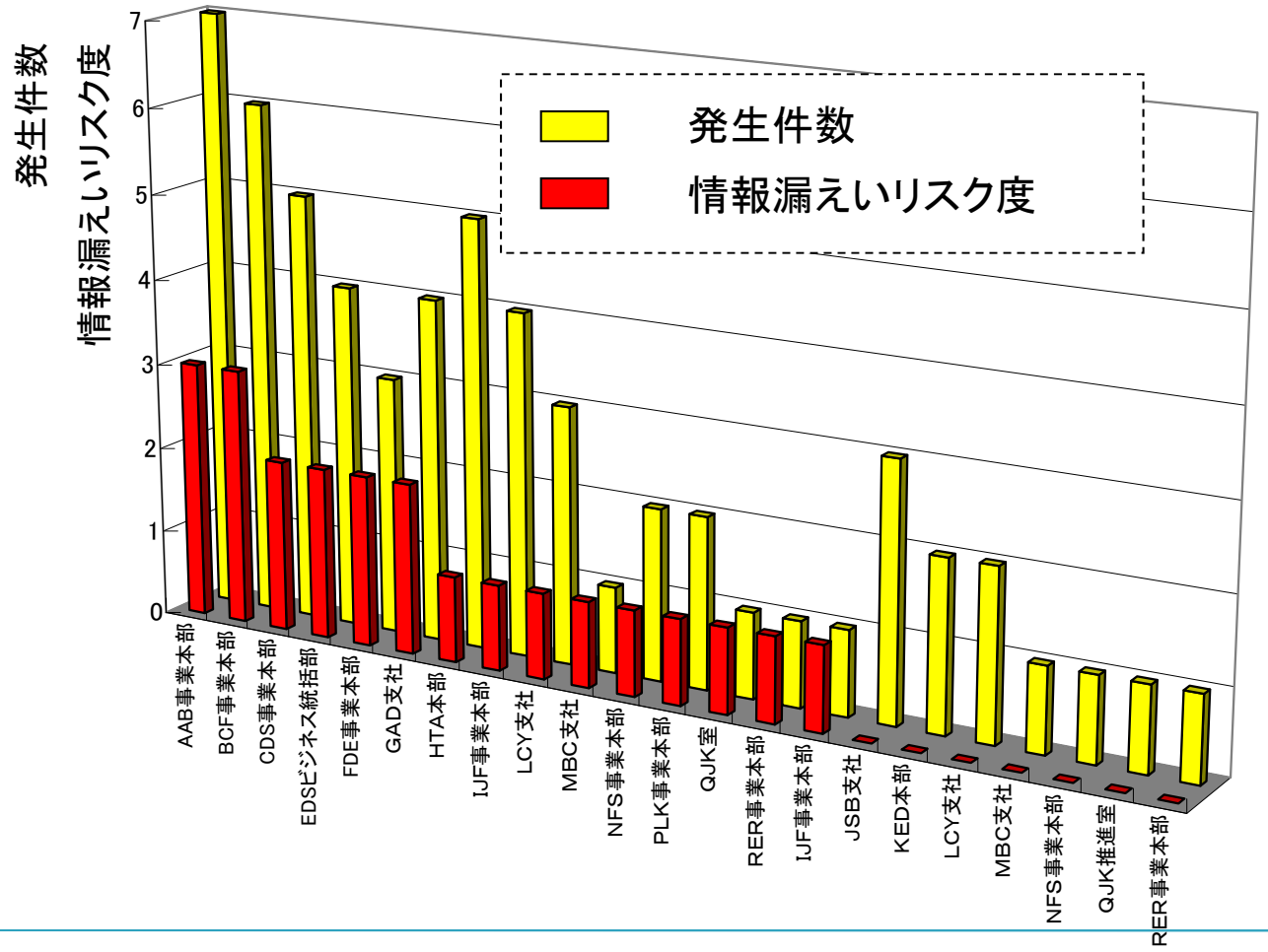


推進体制、教育計画、監査等の整備状況やＰＣや携帯電話等
セキュリティ対策状況を見える化し、各部門が活動実態を認識

ISGA
Information Security Governance Association

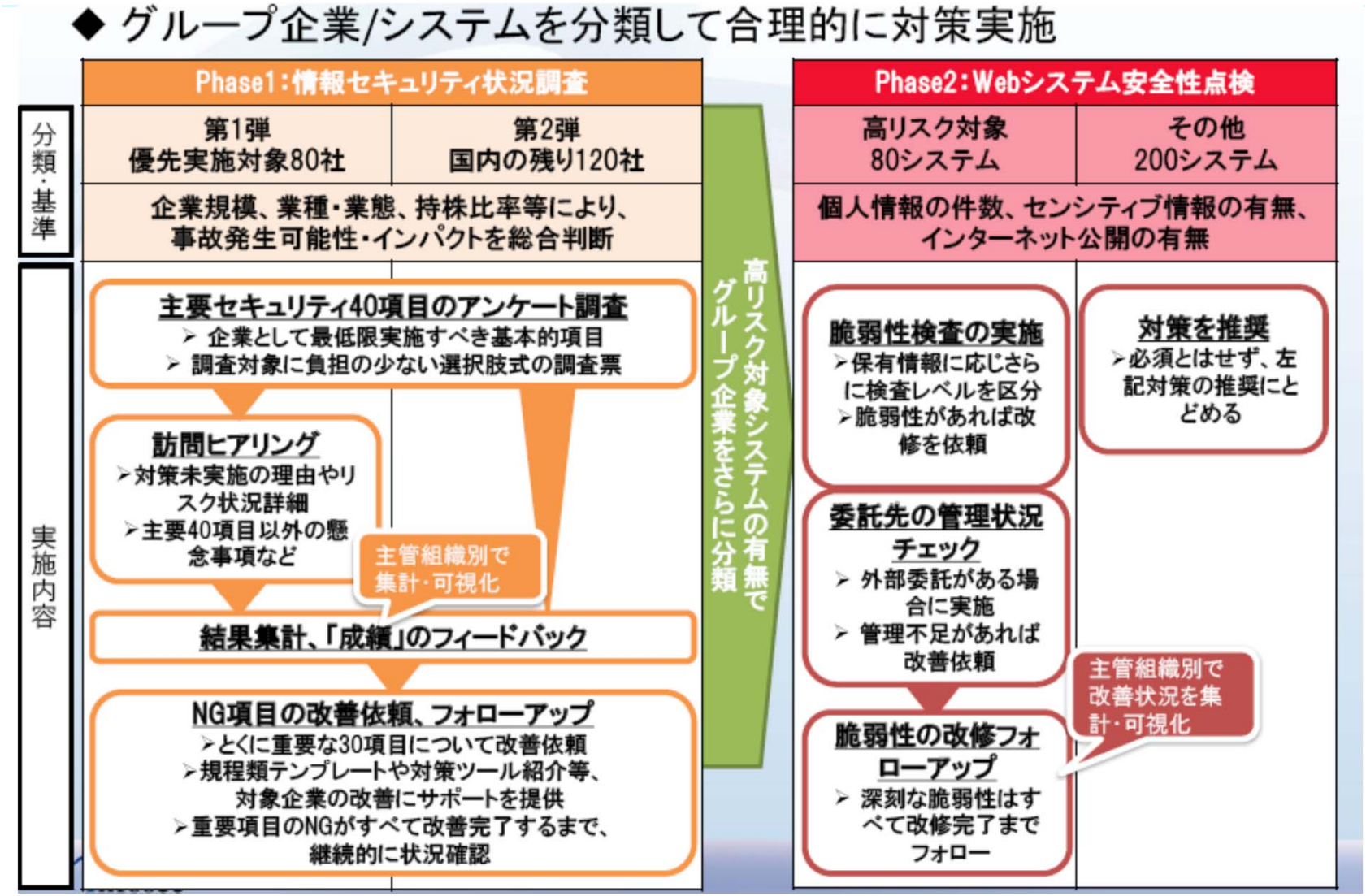
3.2. 事例A：③事件・事故の情報漏えいリスク度評価

情報漏えいリスク度を4段階にレベル付けし評価
発生件数では見えないリスクを可視化

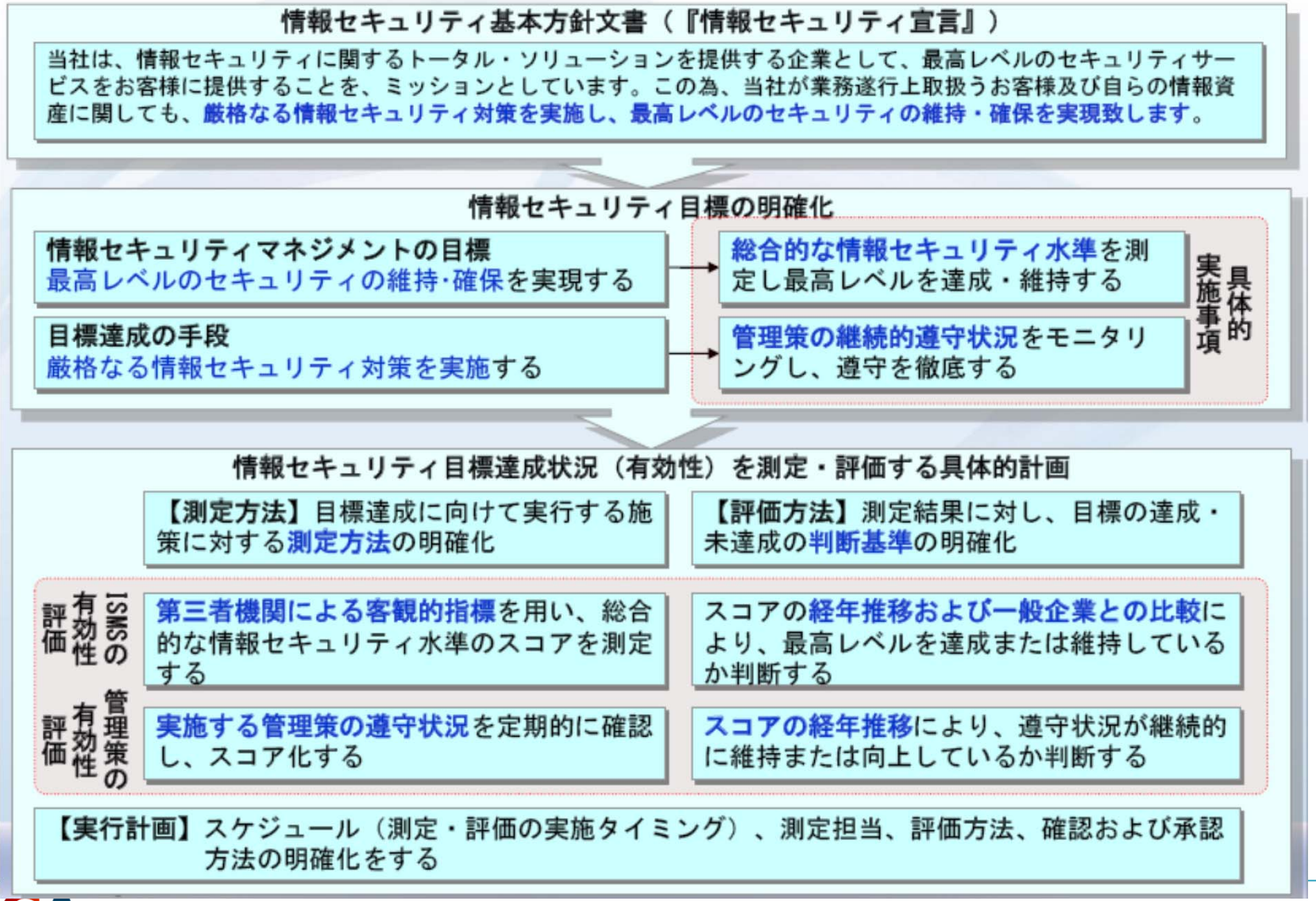


ISGA
Information Security Governance Association

3.2. 事例B：①大規模グループにおける評価の取り組み



3.2. 事例B：②中小企業における可視化の取組み：全体の構造



3.2. 事例 B：②中小企業における可視化の取組み：確認方法

◆ 確認方法は、対策ごとに適切なものを選ぶ

A） ウォークアラウンドによる測定 （四半期に1回程度）

日常業務のなかで実施される対策のうち、見回り点検や簡単なヒアリングでチェックできるもの。【例】クリアデスク、私物ソフトウェアの有無、キャビネット施錠など

B） セルフチェックによる測定 （定期教育時）

日常業務のなかで実施される対策だが、第三者の確認が困難であり、各人の意識に依存するもの。【例】メール送信時の宛先確認、PJT資料の取扱い順守など。

C） 記録の集計 （マネジメントレビュー時）

マネジメントレビューで報告している集計により測定が可能な対策。

【例】教育の効果測定、事故発生・対応件数

D） アクセス権の棚卸し、ぜい弱性検査、リスクアセスメント見直し （毎年実施）

年間計画に組み入れ、これらを計画通り実施したことで遵守確認できる対策。

【例】アクセス制御関連、ぜい弱性対策関連、資産目録関連など

E） 内部監査 （毎年実施。ただし全管理策を一巡するのは3年間）

文書での確認や、個別のインタビューなどでの確認が適切な管理策の場合。

【例】組織体制関連、コンプライアンス関連、システム構成関連など

F） 技術的方法

技術的に強制実施しているため測定不要な対策。

【例】ウイルス対策、推測困難なパスワード設定、HDD暗号化など

3.2. 事例C：①可視化の取り組み

■機械による情報収集・管理

- ネットワーク管理
- モニタリングシステム

■セキュリティ監査

- 国内事業所
- 海外事業所

国内・海外とも2005年度から実施

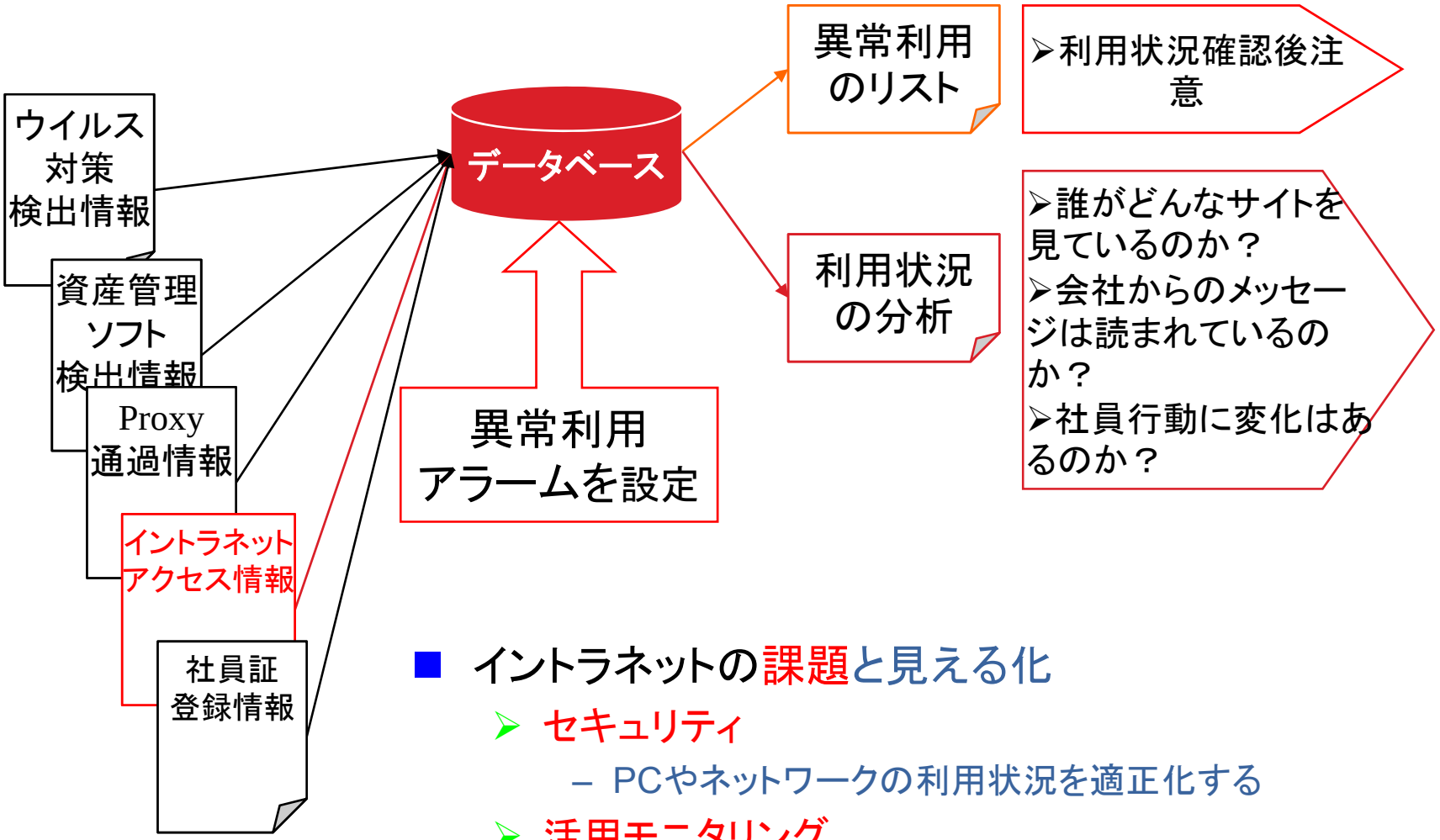
■啓蒙活動

- メールニュース
- インターネット閲覧試験

概ね2週間に一度発信

試験に合格しておかないと
WEBサイトの閲覧ができない

3.2. 事例C：②モニタリングシステム



- イントラネットの課題と見える化
  - セキュリティ
    - PCやネットワークの利用状況を適正化する
  - 活用モニタリング
    - イントラ視聴率のモニタリングでIT利活用をタイムリーに促進

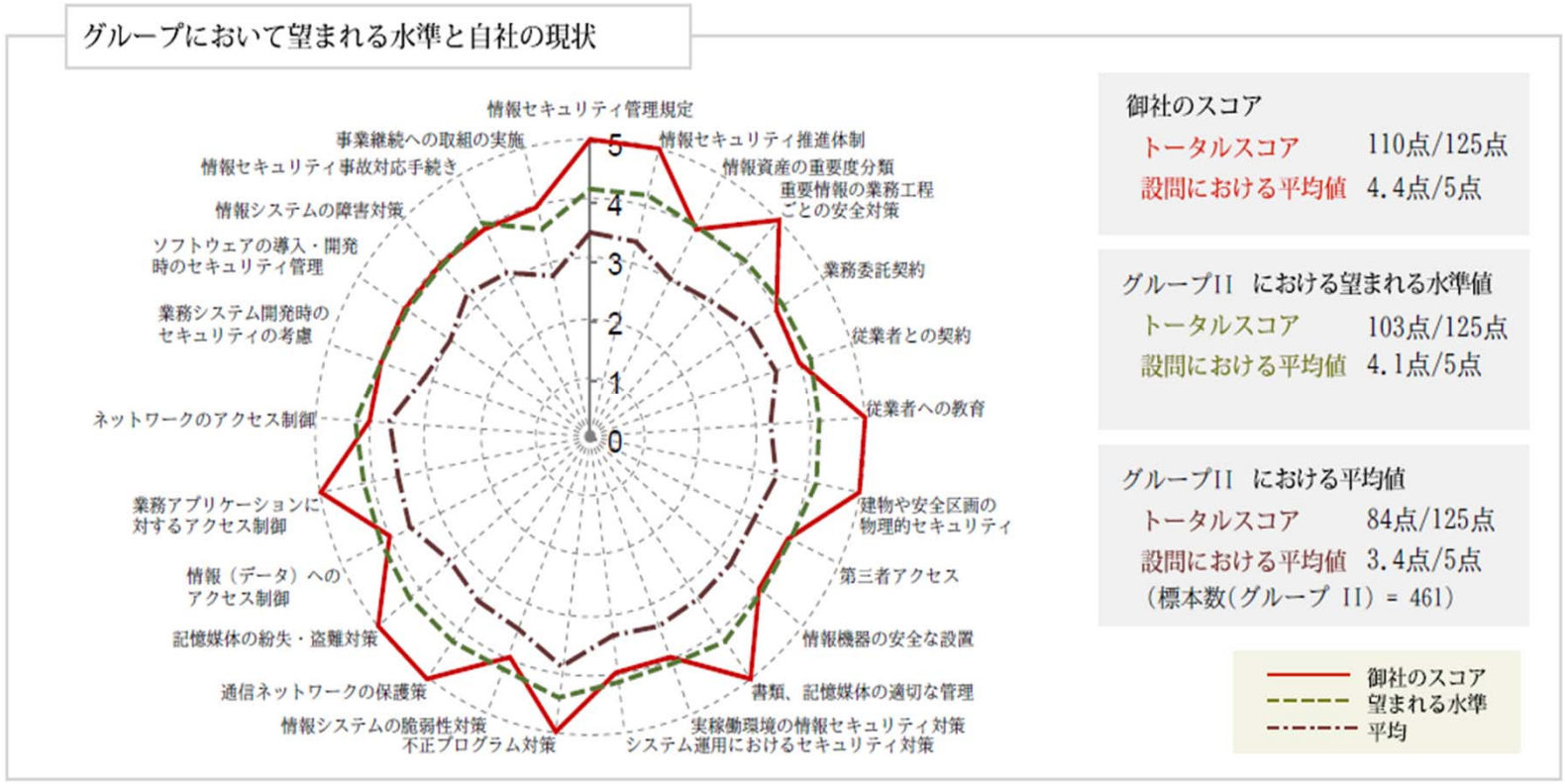
3.2. 事例D：①情報セキュリティ管理のポイント

■総合リスク管理の一部としての情報セキュリティリスク管理の実施
リスクマネジメントシステムを構築し、情報セキュリティリスクに関してもその下で一元管理とし、次のような効果を得る。
・俯瞰的、網羅的な情報セキュリティリスクの把握。
・総合的、計画的な対応を図り、効果的、効率的な管理の促進
各種リスクについてのモニタリングやレビューについては当社のリスクマネジメントシステムにおいて推進して効率化を図るとともにレビューについては内部監査結果をも踏まえPDCAサイクルを構築運用している。また、情報セキュリティインシデントが発生したときの危機対応についてはリスク管理規則に従って実施している。

■情報セキュリティリスクマトリクスの作成とリスク評価
リスクマネジメントシステムのリスク台帳の一部として、情報セキュリティ部分に特化したリスクマトリクスを作成しリスクの洗い出しを実施。
各種情報セキュリティリスクに対して、すでに実施済みの対策を踏まえた残余リスクについて、事例を踏まえて発生頻度・影響度について評価を行っている。
＜残余リスク＞＝＜固有リスク＞－＜コントロール＞
コントロールすなわち対策としては当社で既に対策を講じている対策とともに実施可能な対策についても想定される範囲で検討を行っている。

3.2. 事例D：②セキュリティリスクの可視化に向けた取り組み

1. 経済産業省/IPAの情報セキュリティベンチマークの活用



2. 情報セキュリティリスクマトリクスの作成とリスク評価（再掲）

3.2. 事例E：①セキュリティリスクの可視化に向けた取り組み

【事業と活動の概要】
- 情報システムの分析、開発から構築、展開、運用、保守、リサイクルまでをワンストップ化して、幅広く提供。
- 顧客や取引先から預かる情報は多岐にわたる。個人情報を含む情報に対して厳重な安全管理に努めている。
  - ISMS認証（全事業部門）
  - プライバシーマーク（全社）取得

【情報セキュリティへの取組】
- 安全管理は、リスクを評価して問題があればそれを除去することで実現。
- リスク評価は、全社共通のアプローチと各事業部門におけるアプローチの2種を実施。

全社共通部分	ベースライン・アプローチによって、標準に対し不足する部分を補う
各事業部門	詳細リスク分析により、追加対策の要否を評価しリスク対応を実施

【経営陣への報告】
- 経営陣に対しては、定常活動の実施状況よりも見直し・改善とその実効果の報告に力点をおくように努める
  - インシデント発生状況（対策、社内展開含む）
  - リスク対応の実施状況
  - 実施済み対策の有効性状況
  - 是正措置の実施状況（内部監査やパトロール結果）等

3.2. 事例E：②課題

【課題】
活動の基盤は整備できたものの、十分な結果が伴わないことの改善が最大の課題である。
■実効率の向上（認証取得の目的から身を取る活動へのシフト）
■運用負荷の削減（活動の負荷に比べ十分な結果がなかなか得られない）
ー　インシデントが減らない
ー　対策は適切であるか、的はずれでないか、過剰ではないか
・目的を理解し定着しているか（やらされ感はないか）
・管理部門と現場のギャップはないか（現場は冷めていないか）
・費用の妥当性
（認証維持による効果と活動の実効果に対してランニングコストは妥当か）

3.3. 要点・類型化、課題

■ モニタリングの基準
- 独自にセキュリティのマネジメント基準や指標を定めている企業とISMS管理策を活用している企業に分かれる。
- 独自基準とISMS管理策のギャップ分析を実施しているケースもある。

■ モニタリングの手法
- 各部門でのセキュリティ担当者によるアセスメントの実行、もしくは本社管轄部門によるヒアリングの実行が中心。
- ログによるアラート発報システムの活用によるインシデントの早期検知の実施に取り組むケースもある。

■ セキュリティ可視化
- IPAベンチマークを基準とし数値化を実施する企業、もしくは自社独自基準に対する達成度を表記する企業などがある。
- より洗練された可視化のための基準ならびに可視化の手法の確立が急務。

■ 情報セキュリティマネジメント
- リスク分析に主眼がおかれるようになってきたことが明らかとなった。
- グローバル・ガバナンスの実行、情報セキュリティマネジメントにおける網羅性の確保、複雑化する脅威への柔軟な対応に対し課題認識が高まっている。

■ その他
- セキュリティ施策を「経営課題」として捉え、優先度をもった取り組みを実施できる環境の構築が急務。

4. 総括

■本WGでは、以下の活動を実施した。

- 企業が自社の情報セキュリティの取り組み状況を客観的に評価するための尺度となる測定項目の提案
- 情報セキュリティ活動の見える化（情報セキュリティガバナンス活動における「モニタリング」）の事例分析

■この成果として、情報セキュリティレベルの測定項目の雛形を策定するとともに、経営者への情報セキュリティ活動の報告に係る現状と課題を整理することができた。

■今後は、策定した測定項目や情報セキュリティ活動の見える化の状況に基づき、調査票を策定し、情報セキュリティレベルの実態調査を行う。