テーマ2
【ISMS要求事項の解釈と運用の実態】
（箇条4について）

JNSA標準化部会
日本ISMSユーザグループ
インプリメンテーション研究会

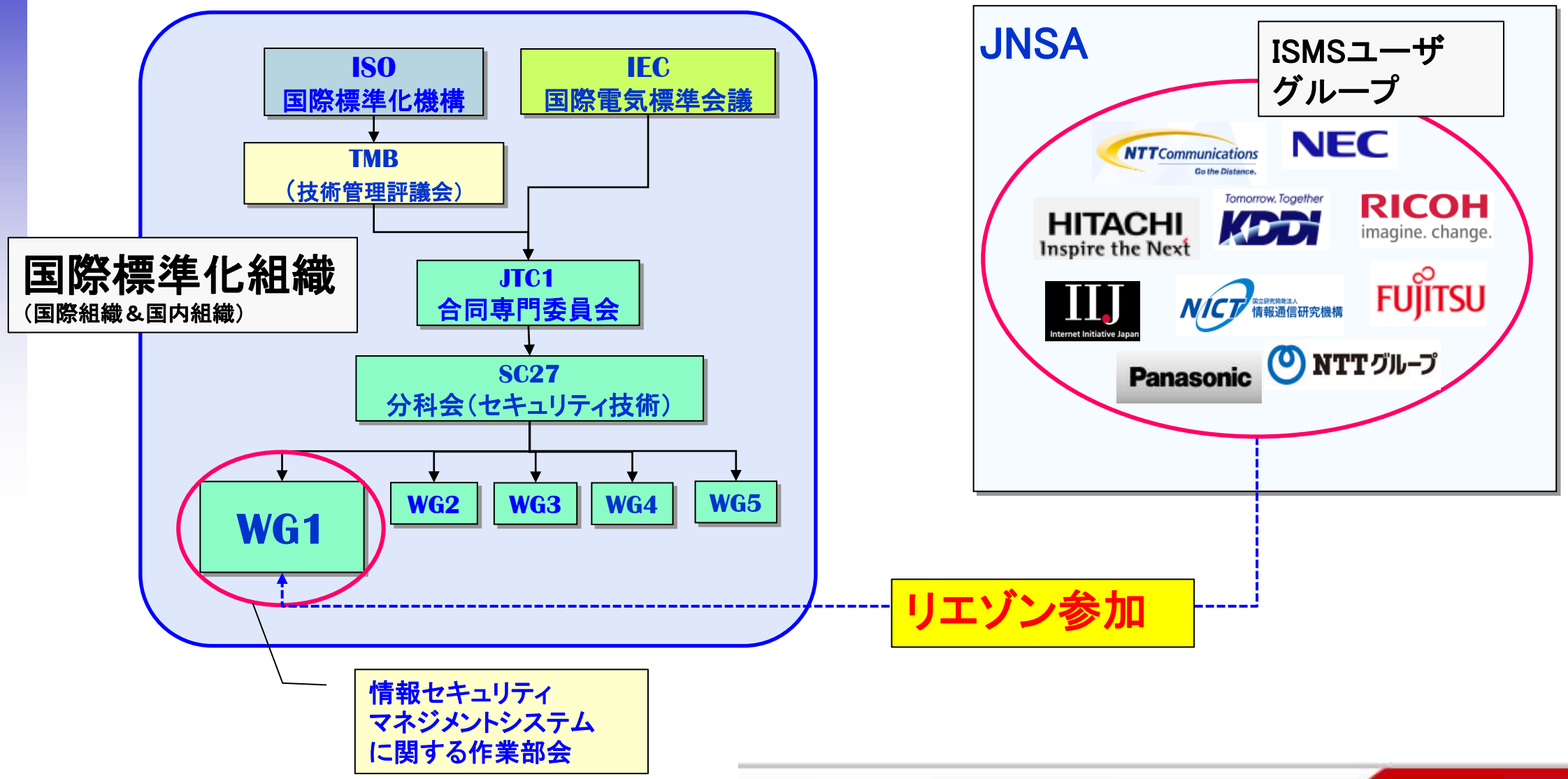
2021年12月17日

羽田　卓郎

リコージャパン（株）

（羽田情報セキュリティ研究所）

日本ISMSユーザGと国際標準化組織



日本ISMSユーザグループの立ち位置

- ISO/IECのWG1の国別代表は必ずしもISMSユーザーの代表ではない（政府機関やコンサルティング会社に所属する国別代表メンバーもいる）

- ISMSユーザの声を情報セキュリティマネジメント規格に反映するために、各国の中にISMSユーザGを作ることになり日本でも「日本ISMSユーザG」が発足した（現在はJNSAの傘下で活動）。

- この趣旨を活かすために、国内の標準化小委員会であるISO/IEC SC27 WG1（情報処理学会 情報規格調査会の中で活動）にISMSユーザGから1名がリエゾンとして参加し、ISMSユーザGと国際標準化組織とのコミュニケーションを行っている。

研究テーマ2の狙い

テーマ2　研究テーマの狙い

ISO/IEC 27001:2013（JIS Q 27001:2014）改定発行において、ISO規格を制定する際に従うルールである「ISO/IEC 専門業務用指針 補足指針Annex SL」に基づき、全てのマネジメントシステムに共通する標準テキストが適用された。

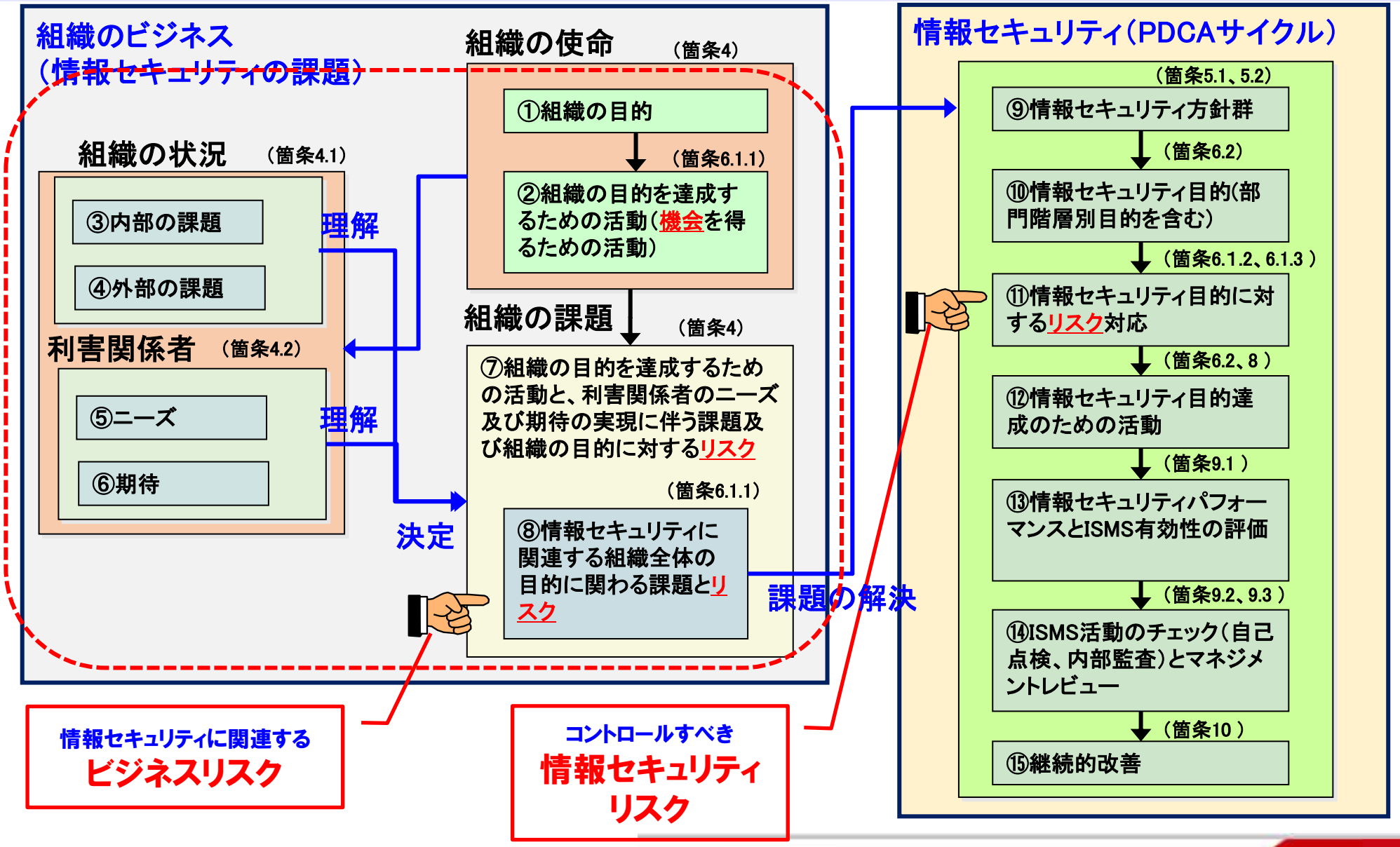
その中で採用された新しい要求事項について、実際のISMS構築・運用において適切な対応が行われていないのではないかという仮定のもとに、日本ISMSユーザグループメンバーの対応状況を確認し、課題点と解決方法を検討する。

テーマ2　研究テーマの狙い

ISMSの要求事項には適合しなければならないが、審査で合格したらその組織のISMSは万全であるという事ではない。審査は、組織のISMSが規格要求事項を満たすことができるという事を検証しているのであり、組織の目的であるビジネス活動の課題を解決できているかは組織の責任なのである。

※ テーマ1における「ゼロトラストセキュリティの考察」でも、箇条4.1 組織を取り巻く環境の変化によって、境界防御の限界というリスクの変化を認識する重要性を主張しているが、リスク認識が適切に行われなければ必要なリスク対応も検討されない。

ISMS構築モデル：ビジネスリスク対策としての情報セキュリティ



テーマ2　研究テーマにおける仮説

【仮説（テーマリーダーの主張）】

1. ISO/IEC 27001：2013（JIS Q 27001:2014）移行において「箇条4 組織の状況」の趣旨を充分に理解していないか誤解があることにより、ISMS構築・運用の重要な部分が対応不十分である。
2. ISMS認証審査では、「箇条4.1と4.2は、経営陣が口頭で説明ができれば文書がなくても審査指摘にはしていない」。
3. 「箇条4　組織の状況」は、マネジメントシステム（ISMS、QMS、EMS他）が組織のビジネス目的や利害関係者の期待から逸脱することががないように、「何の為のXXXマネジメントシステムか」を明確にするために追加された要求であることを考えれば、組織の中で明文化した情報であることが望ましいが、文書化せずあいまいな形で運用している組織がある。

テーマ2　研究テーマの仮説の背景-1

【背景】

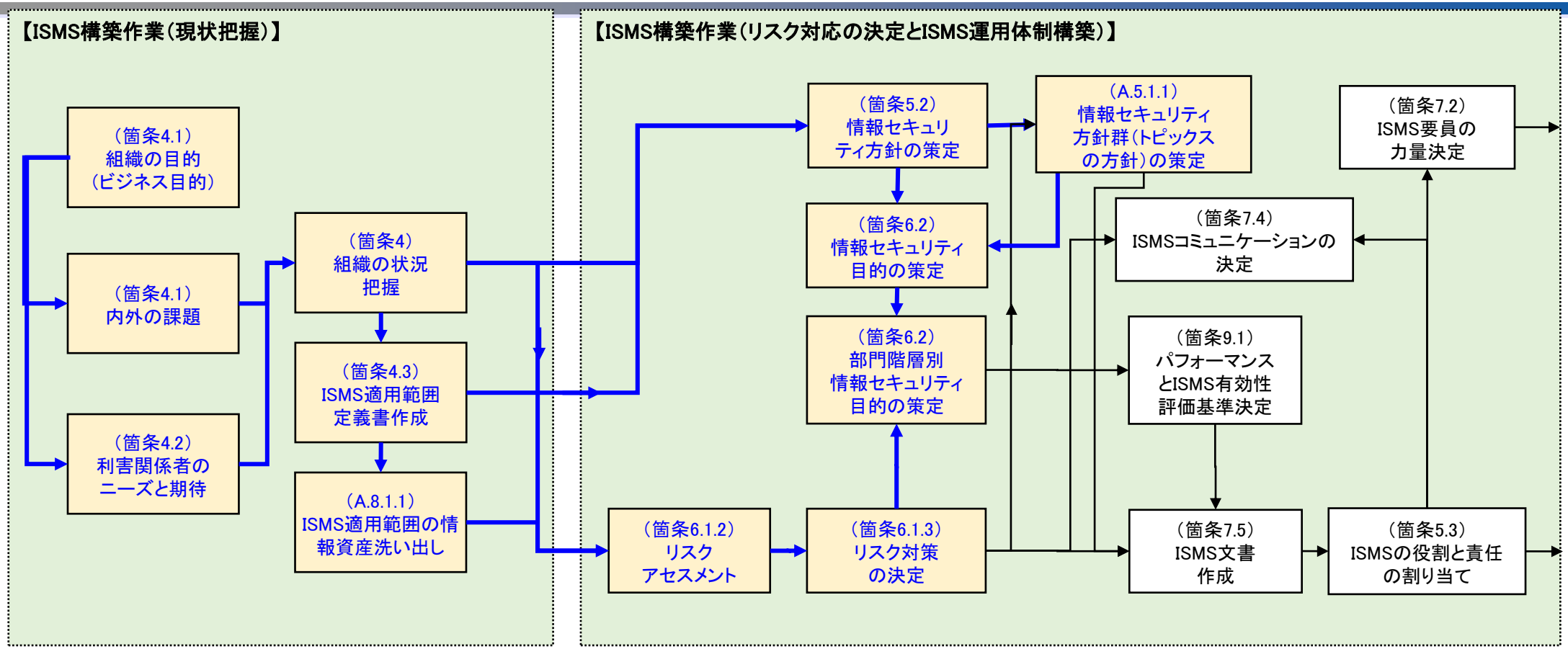
- テーマリーダーの立場から：
  2013年に改定されたISO/IEC 27001について、当時Annex SLの策定に関わっていたIRCA英国本部の方がIRCA-Japanの年次セミナーで、箇条4.1の組織及びその状況の理解（内部及び外部の課題の決定）と箇条4.2の利害関係者のニーズ及び期待という要求事項を組み込むことによって「組織の課題解決のためのMS」という方向性を明確にすることでMS認証の目的である「信頼を与える」ことを確実にしたと説明があった。

テーマ2　研究テーマの仮説の検証方法

【検証方法】

- Annex SLが策定された背景と目的を考慮した上で、インプリメンテーション研究会メンバー組織の対応を確認し、仮説のような状況があるのか、あるとすればどのように対応するのが望ましいかを討議することとした。
- 討議のたたき台として、テーマリーダーがISMS構築・運用コンサルタントとして使用しているコンセプトと実際の作業に使用するひな形を開示し、研究会メンバーの意見を求める。

ISMS規格要求事項実践のための関連モデル（抜粋）



上記モデルは、規格要求事項に適合したISMS構築プロセスの一部を表している。箇条4.1、4.2、4.3を考慮した上で情報セキュリティ方針を策定し、その情報は箇条6.1.1で機会とリスクを決定し、6.12以降のリスクアセスメントプロセスを実施するためのインプットにもなる。このように、重要な情報であることから箇条4.1、4.2、4.3の結果は文書化しISMS構築・推進関係者で共有すべきものと考える。

参考：付属書SLにおける4.1、4.2、4.3、6.1の関係

【JTCG N359：付属書SL策定に関するFAQ】 2014 年 10 月 8 日

Q:4.1、4.2、6.1及び8.1は、どのように繋がっているのか？

4.1で決定した外部及び内部の課題は、4.2で決定した関連する利害関係者の関連する要求事項と共に、4.3において組織の要求事項を決定するための、6.1において組織のマネジメントシステムを計画するための、さらには8.1において、これらの要求事項を達成するのに必要な管理活動を決定するための知識基盤となる。

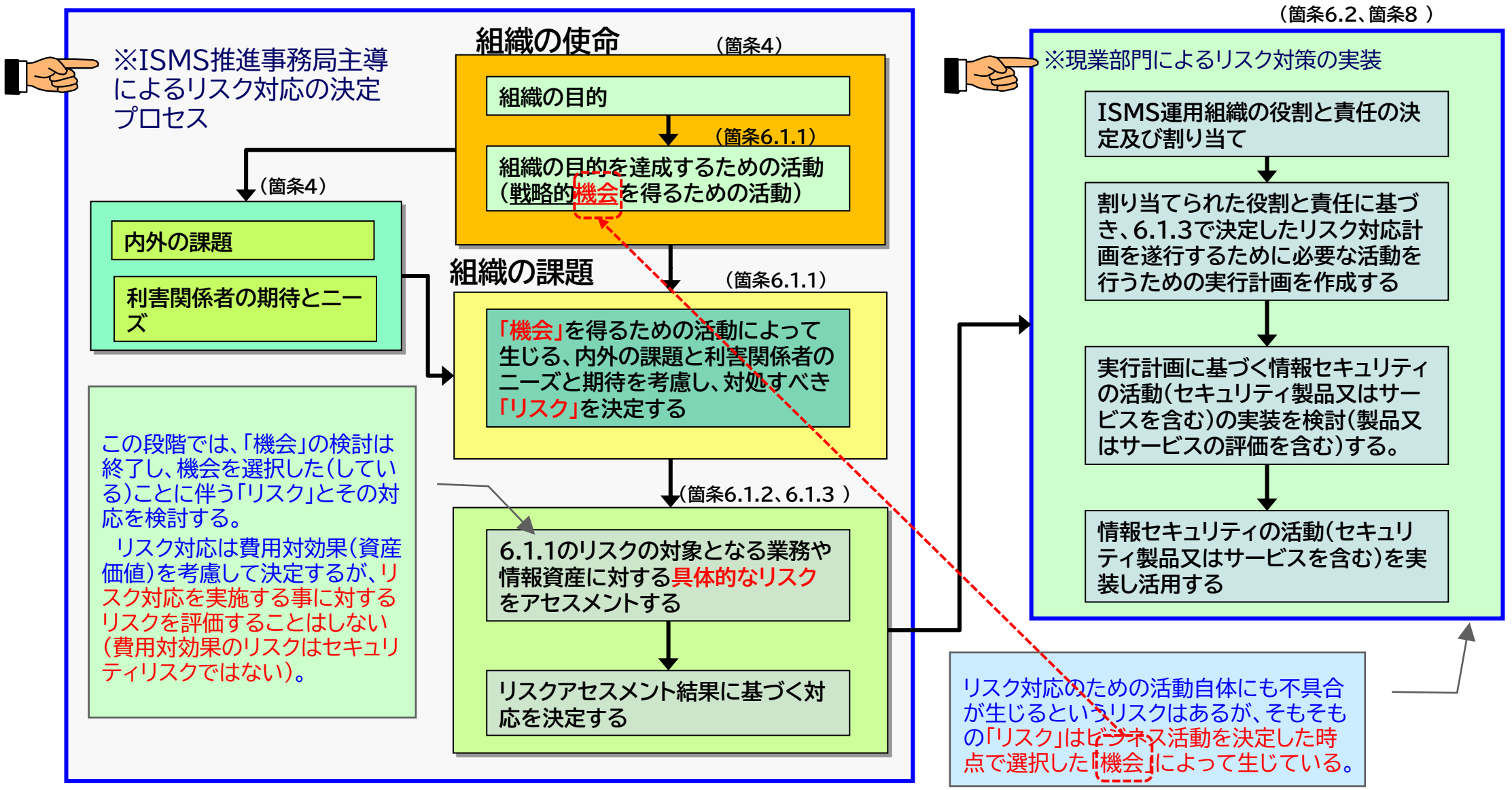
※出展日本規格協会グループ（JSA GROUP） ：https://webdesk.jsa.or.jp/pdf/dev/md_4618.pdf

箇条6.1：ISO/IEC専門業務用指針第1部統合ISO補足指針の附属書SL　コンセプト文書　2014年12月11日

リスク及び機会への取組みに関するこの箇条の意図は、マネジメントシステムを確立するための前提条件として必要とされる計画に関する要求事項を規定することである。ここでは、何を考慮する必要があるか、及び、何について取り組む必要があるかについて規定している。ここでの計画が戦略レベルで行われるものであるのに対して、実施計画（tactical planning）は、**運用の計画及び管理**（8.1）において行われる。

※出展：日本規格協会グループ（JSA GROUP） ：https://webdesk.jsa.or.jp/pdf/dev/md_4619.pdf

テーマ2　モデルで確認する「リスクと機会（opportunity）」



ISMS構築モデルの考え方-1

1. 箇条4.1『組織の目的（ビジネス目的）に関連しISMSの達成に影響を与える組織の内部・外部の課題（解決すべき課題）を決定する』と、箇条6.1.1の、『箇条4.1に規定する課題及び4.2に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定しなければならない 』に関する考察。

①（Opportunity）」は、組織の事業目的を達成するために採用した活動を行うために選択した機会であり、「リスク」は、機会を得るための活動に伴って生じる可能性のある事象（結果）が、目的達成に及ぼす不確実性である。

② 箇条4.1と4.2を考慮して決定する「リスクと機会」は、組織の目的を達成するための事業活動に伴うものである。情報セキュリティは、すでに選択した組織の事業活動に伴うリスクに対応するために行われる活動である。

ISMS構築モデルの考え方-1（続き）

③　①の「機会」について、6.1.2で行うリスクアセスメントにおいても、リスクに対応した機会を明示すべきか？。

　　業務で扱う資産の運用手続きや運用環境のリスク対策を選択（例えばEDRの導入など）することはあくまでも手段であり組織の戦略的決定ではない。それを「機会」と位置付けるのは、リスクアセスメントの工数を増大させるだけである。

④　「内部の課題」では、ISMS適用範囲を内部組織として、情報セキュリティに関わるビジネス活動（=機会）を特定し、その活動において解決すべき情報セキュリティに関わる課題を特定する。

⑤　「外部の課題」では、③の組織内の外部（ISMS適用範囲外）を含め、組織のビジネスに関連する外部関係者に関連する課題を特定する。

2.『「利害関係者」とその「情報セキュリティに関する要求事項」』の考察

箇条4.2の利害関係者は、組織のビジネスに関連する取引先（仕入先、委託先等）、顧客、関連会社（親会社含む）などであり、組織の情報を開示又は利害関係者の情報を受領する相手先である。

① 利害関係者は、ISMS適用組織の情報セキュリティに関連して、直接的な影響を受ける関係者と考えるのが適切である。
株式会社であれば、ビジネス上の利害関係者に株主等や製品やサービスの納品先などがあるが、情報漏洩等で売り上げが減少したり、損害賠償等で財務的な損害を受けた場合に不利益を被ることになるが、情報セキュリティの具体的なニーズ及び期待を有する利害関係者とは言えない。

② 利害関係者が組織に対する情報セキュリティのニーズと期待について、必ずしも直接要求してくるとは限らないため、やり取りしている情報の種類（個人情報等）、取り扱い手順、重要性等を考慮し、情報資産の取り扱いに対する要求とその要求に応えてくれるだろうという期待を推定するとよい。

ISMS構築モデルの考え方-3

3. 箇条4.3 の『組織が実施する活動と他の組織が実施する活動との間の「インターフェース及び依存関係」』の考察

① 「他の組織」とは、1. ⑤のISMSの外部組織（部分認証の場合、ISMS適用範囲外とする予定の自組織を含む）である。

② 「インターフェース及び依存関係」とは、ISMS適用範囲（予定）の組織と外部組織について、

- 外部組織と内部組織（部門等）のビジネス関係
- インターフェースにおける情報のやり取り方法
- 各インターフェースのビジネス上の依存度

※ 規格要求事項としては、箇条4.1、4.2の課題を検討する上で「インターフェース及び依存関係」は重要な情報であるため別々に検討するのではなく、合わせて検討するのがよい。また、このインターフェースの情報は、機密情報のやり取りを意味するものであることから、箇条6.1.2のリスクアセスメントへのインプット情報でもある。

参考：ISMS構築　機会リスク関連表（ひな形の例）

No.	経営戦略に伴う活動（機会）	付随する課題	情報セキュリティリスク （組織に損害を与える可能性）	情報セキュリティ活動方針 （リスク対応方針）
3	法人向けネットワーク構築と保守管理サービス	A.顧客のネットワーク構成情報の安全な管理 B.顧客ネットワーク通信設備のセキュリティ設定の技術的標準及び脆弱性管理 C.技術者の力量不足によるネットワーク構築のミス及び保守管理のミスの防止	・顧客のネットワーク構築に関する情報の漏洩又は盗難(A) ・顧客ネットワーク通信設備の技術標準の不備による脆弱性を利用した不正アクセスの発生(B) ・顧客ネットワークの障害対応不備による業務停止の損害賠償請求(C) ・顧客ネットワーク構築又は保守管理のミスによる情報漏洩又は破壊事故の発生(C)	・顧客のネットワーク構築関連情報の安全な保管方法とアクセス管理の確立 ・顧客のネットワークの特性に合わせたハブ、ルータ、スイッチ、F/Wなどのセキュリティ標準の確立と実装 ・保守サービスにおける即応体制と障害対応手順の整備 ・ネットワーク構築/保守技術者の力量評価と教育・訓練の充実

事業内容に変化がなければ経営陣が交代したからといって変化するものではないが、文書化していなければ新しい経営陣によって説明が変化する可能性は高い。

関連部門と活動方針の関連					
営業部	システム部	法務部	総務部	技術部	○○部
・法務部と相談し、顧客との契約に受託業務に合わせたセキュリティ条項を記載し締結 ・顧客の情報セキュリティに関するニーズと期待の確認		・顧客との契約におけるセキュリティ条項に関する適切さの確認		・顧客情報の盗難及び不正利用対策の確立 ・通信機器のセキュリティ標準の整備 ・保守サービス体制の整備 ・ネットワーク管理技術者の力量評価と育成	

機会リスク関連表は、組織の経営戦略に基づく活動（機会）を確認し、その活動に付随する課題とその課題に関連する情報セキュリティリスク及びその対応方針を検討する。それらの活動やリスクと組織の関連部門の活動との結びつきを検討し、部門別情報セキュリティ目的策定のインプットとする。・・・P11参照

参考：ISMS構築　内部・外部・利害関係者関連表

外部組織（利害関係者を含む）							
名称	インターフェイス（コミュニケーション）					想定されるリスク	対策案
	内容	実施時期	対象者（外部側）	実施者（自組織側）	実施プロセス		
顧客（法人）	契約書・仕様書等の手渡し	契約締結時 仕様決定・変更時	購買窓口部門	営業部	面談を伴う手渡し（紙媒体）	・運搬時の紛失・盗難（顧客の事業機会損失の結果として自社の信頼喪失） ・保管時の紛失、契約内容の漏洩	・運搬時の紛失盗難対策（書類カバンに格納を義務付け等） ・保管時の施錠管理と物理的アクセス管理
	ネットワーク敷設仕様書・設計図面（紙＋電子情報）手渡し	仕様決定・変更時	購買窓口部門	開発部	面談を伴う手渡し（紙媒体又は/及び電子媒体）	・運搬時の紛失・盗難（顧客の事業機会損失の結果として自社の信頼喪失） ・電子媒体経由でのウイルス感染 ・受領後の業務関係者からの情報漏えい ・業務関係者以外の無許可アクセスによる流出/漏えい	・運搬時の紛失盗難対策 ・媒体の紛失盗難時の漏えい対策（暗号化等） ・媒体のウイルス使用前チェック（自社媒体の場合）／受領後の使用前チェック（自社媒体か相手先媒体かを問わない） ・社員教育の徹底と契約内容（特に守秘義務）の周知徹底 ・アクセス制御の徹底

内部組織との依存関係（含む依存度：高＝A～低：C）						利害関係者のニーズと期待	外部組織に関連する課題
営業部	IT運用部	ITシステム部	開発部	法務部	購買部		
[A] 契約取り交わし：契約書作成と保管			[B] 契約取り交わし時に契約書添付の要求仕様書内容の実現性・採算性確認	[B] 契約取り交わし時に契約書内容の適切性確認		【ニーズ】 ・契約書及び仕様書の取り交わし及びネットワーク敷設仕様書・設計図面のやり取りに伴う輸送の安全確保 ・契約書及び仕様書の保管・管理の安全確保（紛失漏洩の防止） ・業務関係者からのネットワーク敷設仕様書・設計図面の漏洩防止 ・業務関係者以外の者の不正アクセス防止 【期待】 ・提供又は貸与した情報の安全な管理	・顧客情報の漏洩や紛失・盗難等による信頼の喪失でビジネスに影響が出ることを防がなくてはならない ・万全な情報セキュリティ対策を行っている会社という評価を得てビジネスを拡大できるようにしなければならない
			[B] 要求仕様書に基づいて設計を行い結果の確認を受けて製造する 設計確認：仕様書、設計図 製品引き渡し：製品試験データ				

内部・外部・利害関係者関連表は、適用範囲組織の外部と情報資産のやり取りがある場合そのインターフェースの内容とそのやり取りに関するリスク及び対策案を検討する。また、組織の関連部門との依存関係を確認し、その結果を6.1.2のリスクアセスメントのインプットとする。

テーマ2　仮説に関する討議結果

テーマ2　研究テーマの仮説に対する研究会意見

【主な意見】

- 事務局の立場から：テーマリーダーの文書化提案とサンプル様式は、そこまですれば良いのは分るがなかなかそこまでできないのが現実ではないか。
- 審査機関の立場から：規格が文書化された情報を要求していない場合、「文書化していない」ことを一律的に問題提起することはできない。

テーマ2　研究テーマの仮説の検証：合意した解釈

- 「機会（opportunity＝好機、選択するチャンス）」を選択するのは、「ビジネス目的に寄与するための手段」と考えるのが自然。ビジネスを維持・発展させるための様々な戦略・戦術の決定に伴うリスク（解決すべき課題によって決定したことが実現できない可能性）が生じる。⇒箇条4と箇条6.1.1の世界
- 情報セキュリティは、そのリスクの中で、情報資産のCIA喪失に関連するリスクを防止又は低減するために行うものである。
- ISMS構築組織では、リスク対策の実施を「機会」としてリスクアセスメントを実施しているケースがある。この場合、リスク対策（機会）を選択する事にリスクが生じるという考えに立つため、リスクアセスメントの結果の対策に対するリスクアセスメントを要求することになる。

テーマ2　アンケート実施

仮説の討議結果を受けて、箇条4.1、4.2、4.3（インターフェース部分）の文書化についてアンケート調査を実施した。

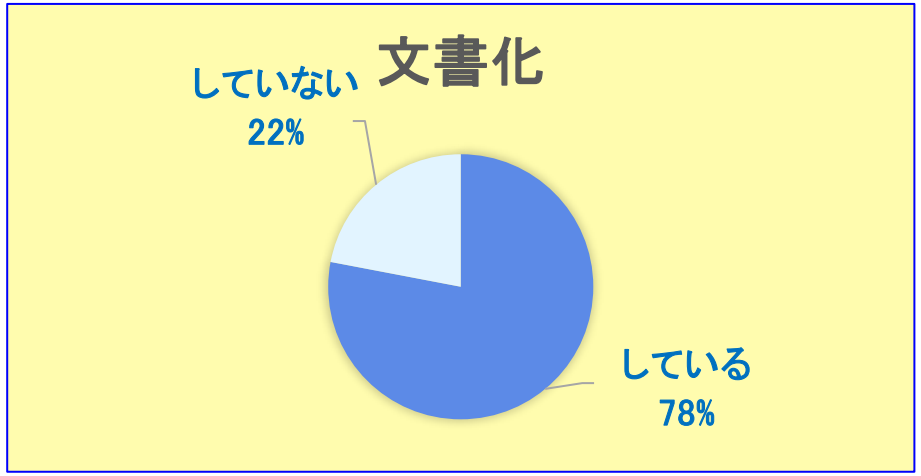
テーマ2　アンケート

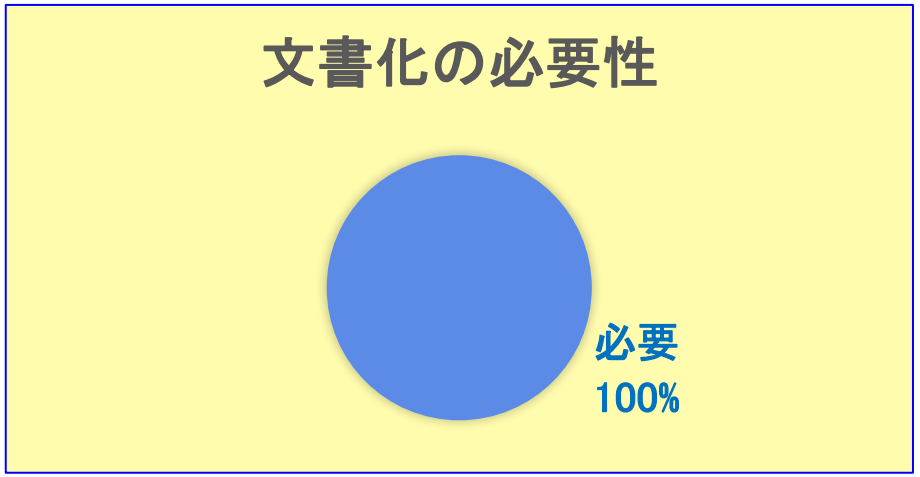
6月のテーマ2に関する討議の結果、ISMS規格（ISO/IEC 27001）本文の箇条4.1~4.3の要求事項の対応について、参加組織の実情を確認するためのアンケートを実施し、9社からの回答を得た。

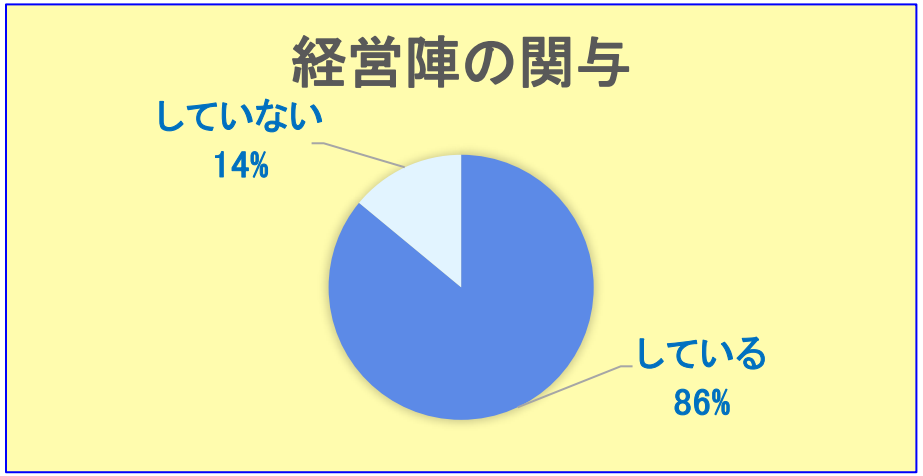
⇒他に2社からISMS事務局ではない旨の回答を受領

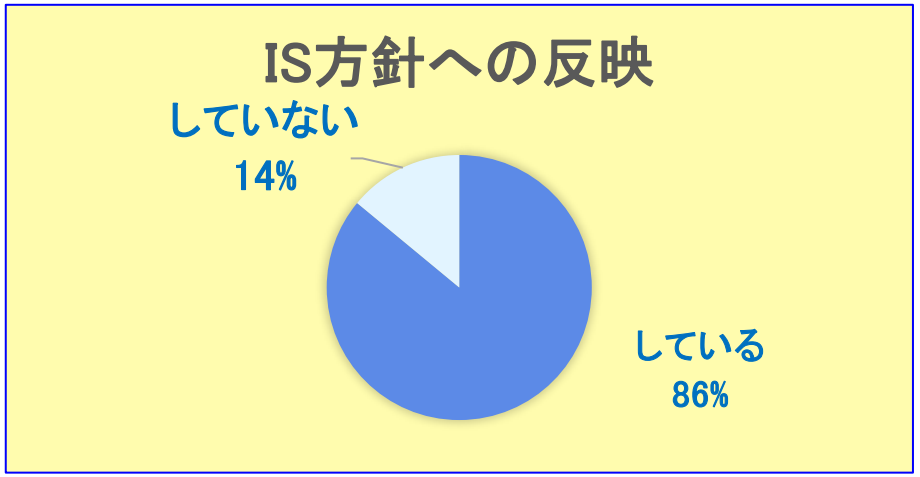
テーマ2　アンケート実施結果

箇条4.1、4.2、4.3（インターフェース部分）の検討結果に関する文書化について



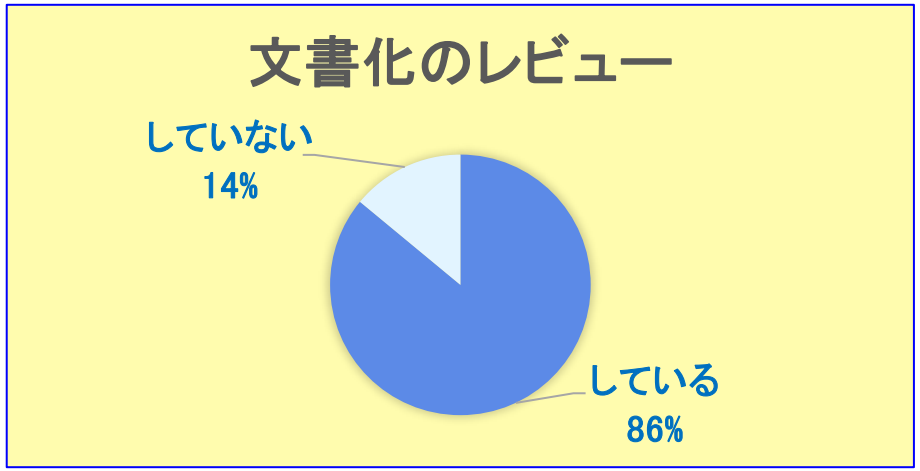


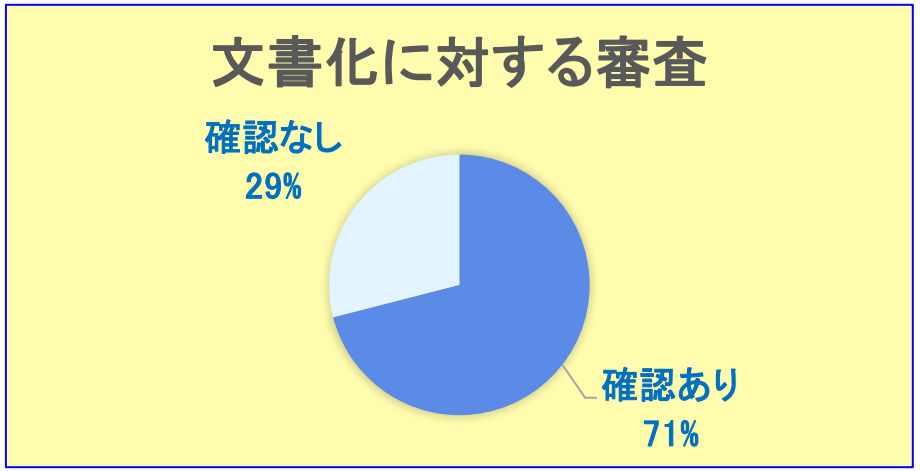




テーマ2　アンケート実施結果：続き

箇条4.1、4.2、4.3（インターフェース部分）の検討結果に関する文書化について





箇条4.1、4.2、4.3（インターフェース部分）の文書化に関する各組織の意見としては、「必要性は認めるが、大きな組織ではISMS推進事務局の負担が大きく、実務的に難しい部分がある。」という意見が多かった。現在文書化していない組織でも、「できれば文書化したい」「文書化したいが負担が大きいため実務的には困難」というものであった。

テーマ2　研究テーマにおける仮説の検証

【仮説（テーマリーダーの主張）】

1. **ISO/IEC 27001：2013（JIS Q 27001:2014）移行において「箇条4 組織の状況」の趣旨を充分に理解していないか誤解によって、ISMS構築・運用の重要な部分が対応不十分である。**

⇒回答のあったISMSユーザグループ内の組織では、規格要求事項の解釈に理解不足や誤解はなかったが、組織の大きさなどで対応については意見が分かれた。

※参考意見：

- **コミュニケーション媒体としての文書化は必須**
- **大規模組織の場合、多数の従業員と連携する必要があるため、文書化が望ましいが、小規模組織の場合、少数の従業員が把握できれば良いため、文書化は必須ではないと思う**

テーマ2　研究テーマにおける仮説の検証

【仮説（テーマリーダーの主張）】

2. ISMS認証審査では、「箇条4.1と4.2は、経営陣が口頭で説明ができれば文書がなくても審査指摘にはしていない」。

⇒文書化していることを要求事項として審査した審査機関は無いようであったが、文書を作成している組織の審査では文書を確認しながら審査を実施しているケースが多い。

※参考意見：

- **トップインタビューにおいて文書化が要求されたことはない**
- **審査会社から明示的に文書化したものは求められていないが説明の時に提示すると審査がスムーズ**
- **審査機関では必ず文書確認が実施されており対応**

テーマ2　研究テーマにおける仮説の検証

【仮説（テーマリーダーの主張）】

3. 「箇条4　組織の状況」は、マネジメントシステム（ISMS、QMS、EMS他）が組織のビジネス目的や利害関係者の期待から逸脱することががないように、「何の為のXXXマネジメントシステムか」を明確にするために追加された要求であることを考えれば、組織の中で明文化した情報であることが望ましいが、文書化せずあいまいな形で運用している組織がある。

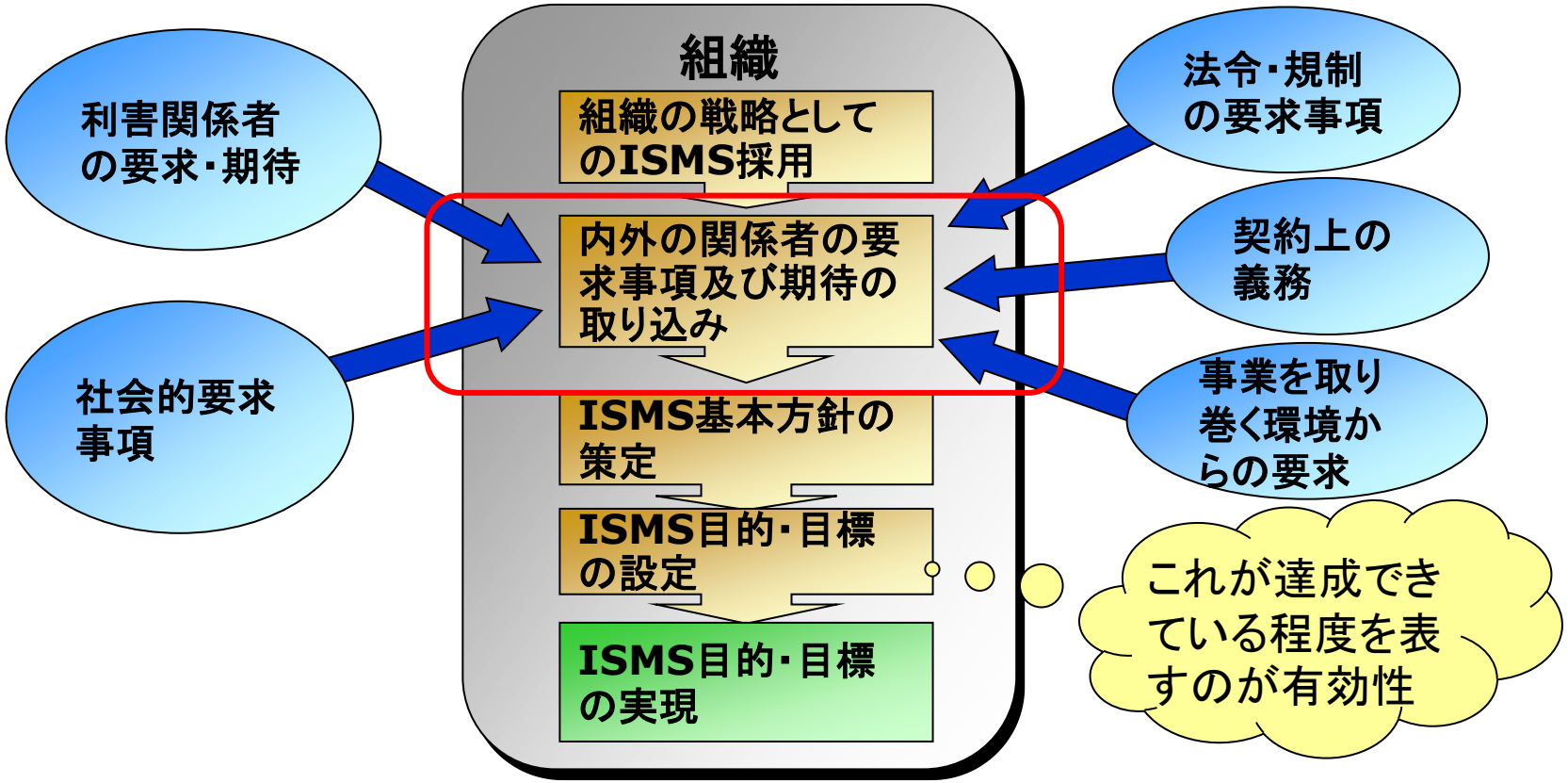
⇒アンケートに答えた全組織が文書化の必要性は認めていたが、ISMS推進事務局の負担が大きいことや審査で要求されないこともあり文書化まではしていない組織が見られた。

※参考意見：

・組織や業務が多岐で広範囲にわたる場合、正確に記述し、適切に情報を更新して維持していくには、相当な負担を要するため、実務的に困難を伴う

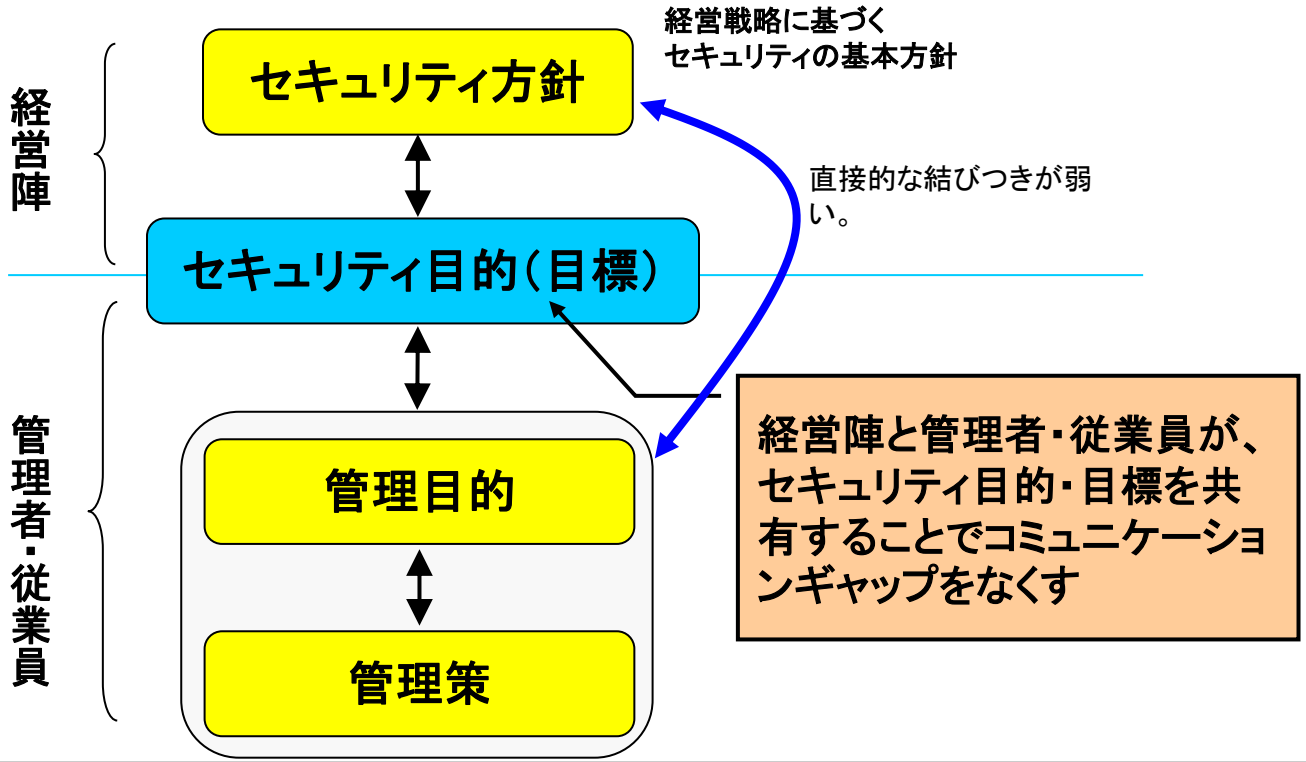
参考：ISMSの目的・目標設定の基本プロセス

ISMSの有効性を決定する要素



参考の図は、2009年のISMSユーザグループ研究発表資料の一部である。赤枠の部分が本年（2021年）の研究テーマで、この部分の文書化の是非が組織のISMSにとって重要かどうかを討議した。

テーマ2　参考：情報セキュリティ方針と目的の関係



参考の図は、P30の図と同様に、2009年のISMSユーザグループ研究発表資料の一部である。前図は、情報セキュリティ方針と目的（目標）を作成するための考え方である。本図は、経営陣と管理者・従業者とのコミュニケーションギャップの考察であるが、情報セキュリティ方針に4.1、4.2に関する経営陣の意思が反映されないと意味がない。

テーマ2　研究結果に対する結論

1. 箇条4.1、4.2、4.3（インターフェース部分）の規格要求事項 に対する対応では、対応状況にばらつきはあるが、不適切な対応が行われているという事はない。
2. ISMS構築ユーザとしての立場では、可能であればきちんと文書化した上でISMSの運用を行いたいという考えであった。しかし、審査機関の立場では、規格要求事項として（文書化が）明記されていない以上は一律的に文書化していないことに問題提起はできないという事であるため、組織の判断にゆだねることになる。
3. 規格要求事項の解釈については、テーマリーダーの解釈（考察）に同意するという事であり、今後の各組織の維持・改善の中で今回のアンケート結果を生かして行けるように実用的な対応方法を研究していきたい。

テーマ2　アンケート結果詳細
（参考資料）

テーマ2　設問1：箇条4.1～箇条4.3の要求事項対応の文書化

(a) 文書化している

〇結果：9社中7社（78%）が文書化

〇主なコメント：

- コミュニケーション媒体としての文書化は必須
- 審査の際の手持ち資料として必要
- 可視化するという意味で必要
- ISMSのためということではなく、労務管理や品質管理を含めて組織の課題を洗い出している
- 組織の状況把握及び適用範囲を定義するために必要
- 組織を取り巻く状況の把握及び組織の改編やトップ交代においても基本方針の継続を可能にするために必要
- 大規模組織の場合、多数の従業員と連携する必要があるため、文書化が望ましいが、小規模組織の場合、少数の従業員が把握できれば良いため、文書化は必須ではないと思う

テーマ2　設問1：箇条4.1～箇条4.3の要求事項対応の文書化

（b）文書化してない

〇結果：9社中2社（22%）が文書化していない

〇「今は文書化していなくても必要だと感じていますか」に対する主なコメント：

- 『管理システム』である以上、その管理の適用範囲とその境界線を明らかにして定めることは当然
- 経営陣や利害関係者の要望を正しく把握する必要があるため、文書化は役に立つ手段になり得る

テーマ2　設問1：箇条4.1～箇条4.3の要求事項対応の文書化

(c) 文書化の提供

〇結果：7社中3社（43%）が提供

〇主なコメント：

＜A社＞

- 目的/目標設定におけるビジネスとセキュリティの関係（提示済）
- ステークホルダー一覧（ステークホルダーの活動状況については可視化しているが、ニーズとしてはまとめていない？）
- 適用範囲の決定

＜B社＞

- ISMS事務局の業務に「ＩＳＭＳ管理目標達成に影響を与える社内および社外の課題および変化」と「当社の利害関係者およびその利害関係者からの要求事項」を把握することが入っている

テーマ2　設問2：設問１.で文書化していると回答

(a) 文書化について経営陣が関与している場合

〇結果：7社中6社（86％）が関与

〇主なコメント：

- 経営陣からの事業計画案に対しその実現を脅かす情報セキュリティ上の内外の課題をISMS事務局がフィードバックする
- ISMS事務局が、インプット情報としてマネジメントレビューやセキュリティ方針文書の作成に対する指示事項等を参考に纏めている
- 小規模のＭＳ関連の月次報告会の中で状況変化の有無の確認⇒社長指示事項として改善を推進し実施⇒次年度の対応方針を一次検討し経営トップにて最終決定を行い文書化
- マネジメントレビュー及び各種会議体などの機会に確認しまとめる

テーマ2　設問2：設問１.で文書化していると回答

b.ビジネス環境の変化などで内外の課題や利害関係者のニーズ及び期待の変化について、文書化された情報のレビュー

〇結果： 7社中6社（86％）がレビュー実施

〇主なコメント：

- 事業計画策定時に見直し、契約条件や情報セキュリティに対する要求状況を確認し適用範囲の情報セキュリティ水準とのギャップ分析を行い対応計画を策定する。
- ISMS事務局内で内容の精査レビューを実施し、マネジメントレビューで確認＆対応指示を受ける
- 年初PDCAの計画時に見直しレビューを実施
- 顧客要求事項については、取引先ごとの要求事項及び顧客満足度調査のヒアリング結果を反映し法的要求と一緒にマネジメントレビューで討議
- マネジメントレビュー及び各種会議体などの機会にレビュー

テーマ2　設問2：設問１.で文書化していると回答

(ｃ)文書化した内容が自組織の情報セキュリティ方針に明確に反映されている

〇結果：7社中6社（86％）が反映している

〇主なコメント：

- 情報セキュリティ方針は、事業計画案が策定されてから、事業計画案に基づいて検討するため反映
- 基本方針としては反映されている。但し、基本方針にどこまで記載するかの粒度については各組織の特性に任せるべき
- 反映されている。ISMSの審査の際は、他部門のエビデンスやQMSで作成した資料で審査を受けている
- 経営理念・経営計画を踏まえ検討する

テーマ2　設問2：設問１.で文書化していると回答

(d) 箇条4.1、箇条4.2、箇条4.3（インターフェース）に係わる審査で、文書化された内容について審査機関からのコメント

〇結果：7社中5社（71%）が審査で文書を確認
　　7社中2社（29%）が審査で文書の確認なし

〇主なコメント：

- トップインタビューにおいて文書化が要求されたことはない
- 4.1、4.2の資料を見せると、文書化要求が無いのにその資料についてコメントが出る
- 審査会社から明示的に文書化したものは求められていないが説明の時に提示すると審査がスムーズ
- 文書の確認がされ、審査では特に問題なし
- 審査機関では必ず文書確認が実施されており対応
- 審査で文書を確認した。文書化は求められていないが、審査がスムーズに進行した。

テーマ2　設問3：設問１.で文書化していないと回答

(a) 文書化（箇条4.1、箇条4.2、箇条4.3（インターフェース））していないことについて

a. できれば文書化したいと感じている場合、その理由

〇結果：2社中2社（100％）が文書化したい

〇主なコメント：

- 規格の趣旨は理解しているため、本来であれば文書化したいと考えている。ただ、適用範囲が限定的であれば、文書化は容易であるが、組織や業務が多岐で広範囲にわたる場合、正確に記述し、適切に情報を更新して維持していくには、相当な負担を要するため、実務的にははかなりの困難を伴うと考えている。
- 出来れば文書化したい。理由は組織としてＩＳＭＳ目標などを立案する際、役に立つと考えている

テーマ2　設問4：本件に関するコメント/意見等

1. 特定の業務や組織に限定した認証であれば、本箇条の趣旨は適切に対応できると思うが、全社レベルでの認証となると相応の負担が必要で、実務的には困難を伴う。

2. 本質問の対象者の帰属組織が経営企画部のような全社の長期経営計画、中期経営計画の策定に関与し影響を及ぼす組織の場合は有効な質問ですが、多くのISMSユーザでは経営計画の策定プロセスではISMS事務局は蚊帳の外にあることが一般的だと想定される。 ISMS事務局が情報セキュリティやそのマネジメントには興味を持っても経営には興味を持っていないことが危惧される。ISMSの経営システムへの実装が課題だと認識している。

3. P.D.C.Aの順番で計画を組み立てようとするから、4.1、4.2が審査で説明が難しくなるのではないか。

テーマ2　設問4：本件に関するコメント/意見等

4. 全般的に文書化されていない要求事項に対するアンケートでしたが、箇条4.3（インターフェース）については、サービス境界、ネットワーク境界などの形で、ＩＳＭＳ認証適用範囲を定義するための文書の一部で作図などを行っておりました。

5. 会社が策定した経営理念・経営計画を踏まえ、各主管部門にて業務を行っている。ISMSもその一つだが、情報セキュリティインシデント未然防止・被害最小化等のため、経営層、CISO、CIO、各事業部門と連携している。