

情報セキュリティマネジメント・セミナー2025

なぜ話が通じない？

～ ISMS審査・運用の現場で起こる認識のズレ ～

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

2025年12月5日

北村 俊樹（LINEヤフー株式会社）

1. ISO/IEC 27001における関係者の認識のズレ
2. 研究会メンバーからの事例集め
3. 事例紹介
4. まとめ

ISO/IEC 27001における関係者の認識のズレ

研究テーマを選定するためにISMSの審査や運用の課題をあげていきました。

その中で、審査員、事務局、コンサルタント、社内外の利害関係者の間で認識のズレがあって困っているケースがみられました。

「なぜ、こんな指摘が？」「こちらの意図が伝わらない...」と頭を抱えた経験を持ち寄って整理してみることが役に立つのではということ。

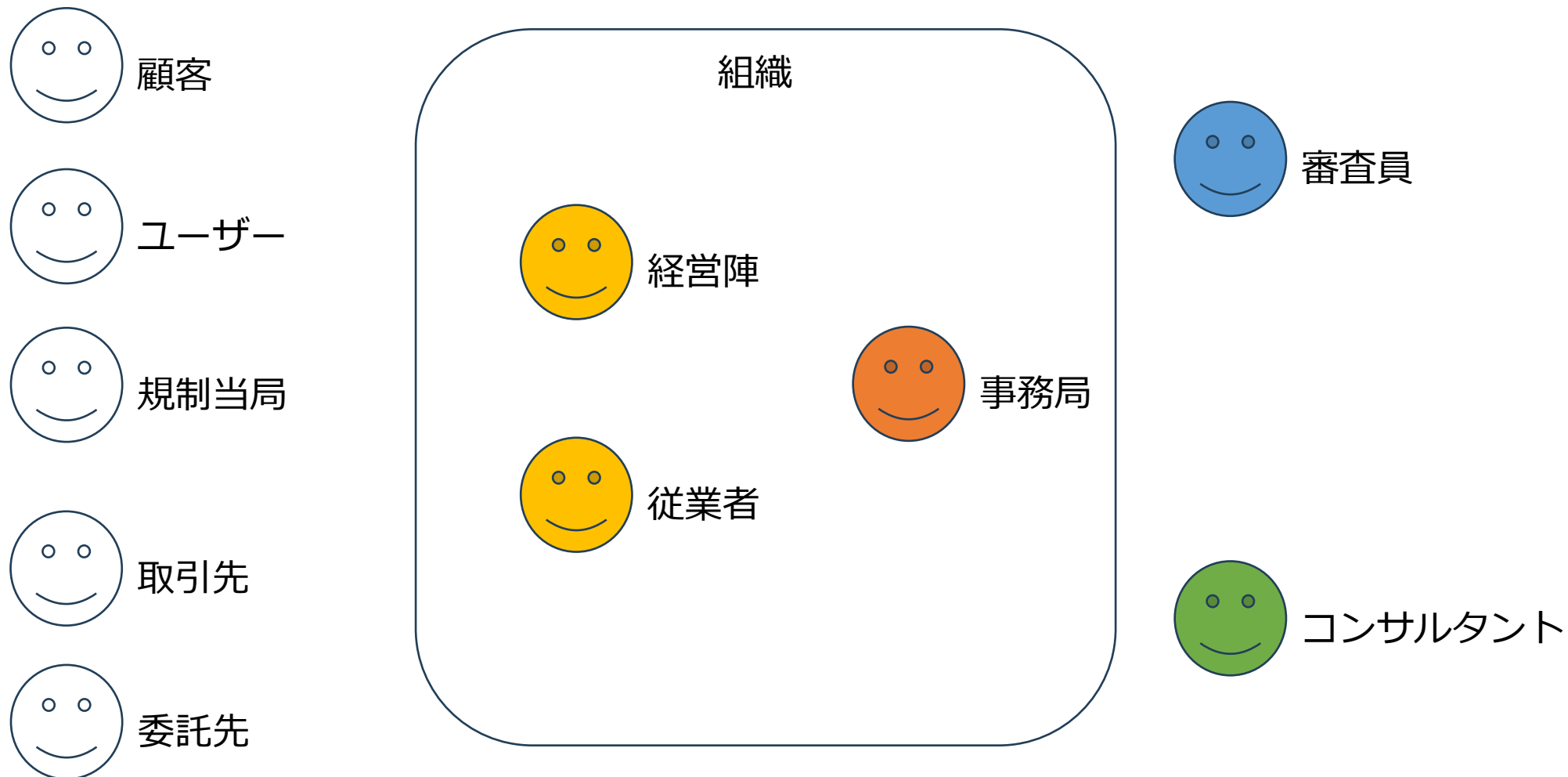
スタート！

課題：関係者の認識違いなどによる発生するISMS関連の無駄稼働の削減効率化事例を例示することで認証組織に対する悩み相談にも繋がる。

範囲：関係者（経営層、事務局、コンサルタント、審査員など）
規格の解釈だけではなく、規格を解釈した上での具体的な管理策の実装方法含めたシームレスな認識の合意形成を試行する。

事例：ISMSの運用や審査対応で悩んでいる課題から代表例を選択して
深掘り&整理する

ISMSの関係者



- 議論する中で、認識のズレの対象別に次の3つに分類することができました。

a)規格の認識のズレ

- 発生するのは、事務局、審査員、コンサルタント
- 対象は、認証規格JIS Q 27001(JIS Q 27002)

b)社内規定の認識のズレ

- 発生するのは、組織内の事務局、経営陣、従業員
- 対象は、組織内のルール（情報セキュリティ規程）

c)外部の利害関係者との認識のズレ

- 発生するのは、組織と組織外（顧客、ユーザー、規制当局など）
- 対象は、組織内のルールと組織外のニーズ、期待

a)規格の認識のズレ

ケース

一部の部署が分社化したので、その会社として新規にISMS認証取得が必要になるな。

別会社だから、新会社との間に境界を設けないといけないから、パーティションとドアも用意しないと。

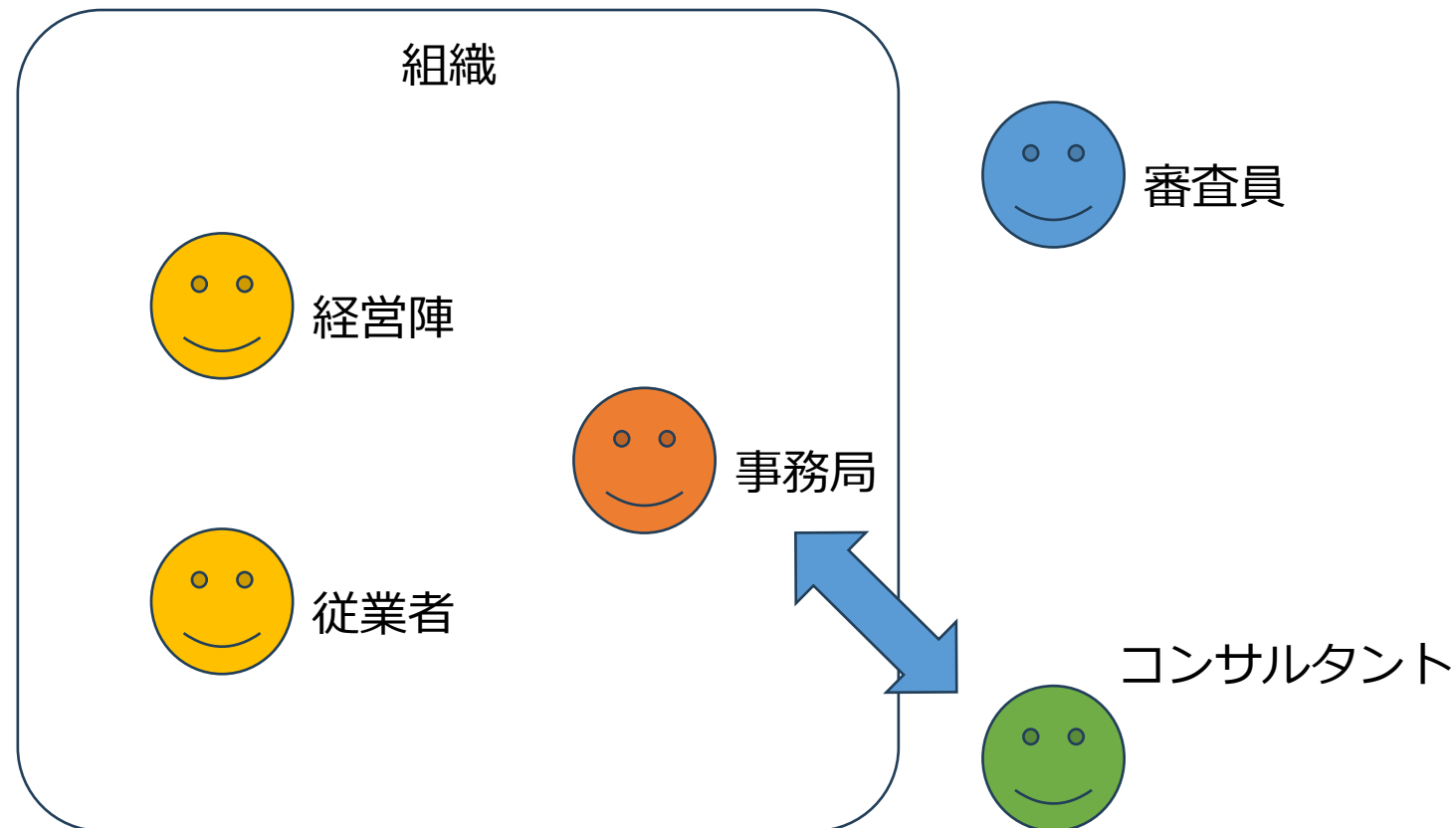


事務局

そんなことないですよ。

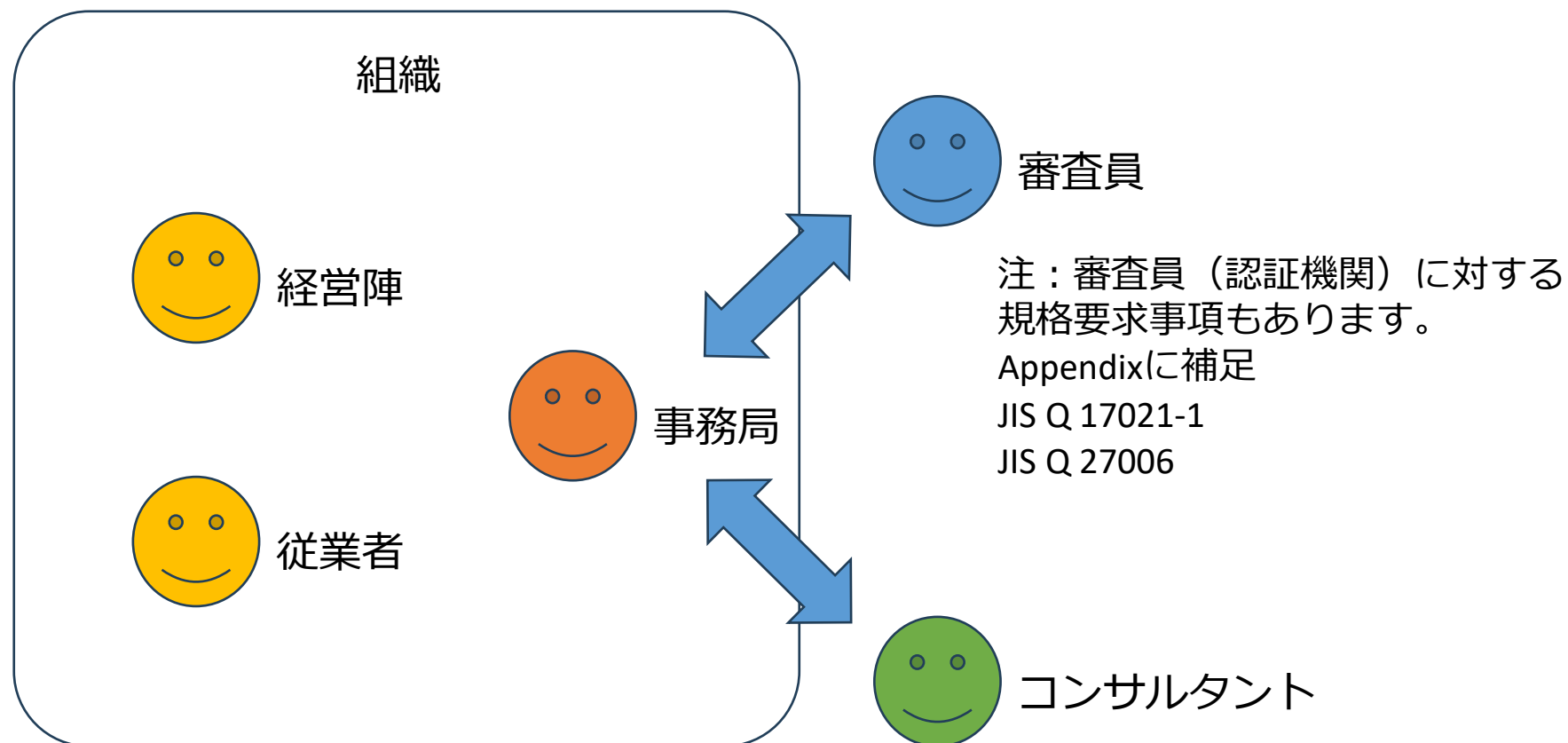


コンサルタント



a)規格の認識のズレ

- 発生するのは、事務局、審査員、コンサルタント
- 対象は、認証規格JIS Q 27001(JIS Q 27002)



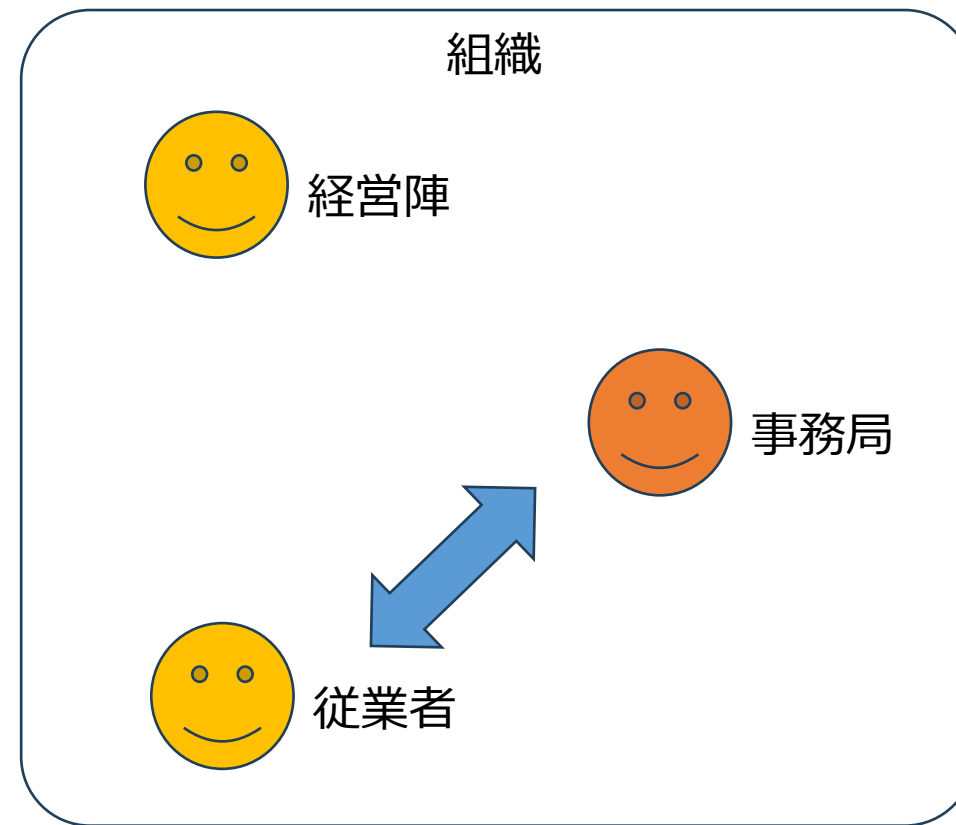
b)社内規定の認識のズレ

ケース

- クラウド (SaaS) 利用におけるセキュリティ審査を社内
内で実施している。
- 現場サイド (申請者) においてリスクについての認識
が少なくとりあえず審査を通過するために必要なこと
だけを教えて欲しいなど自分で考えることをしていな
いことが目につく。
- 社内規定の目的や重要性の認識が不足していることが
課題

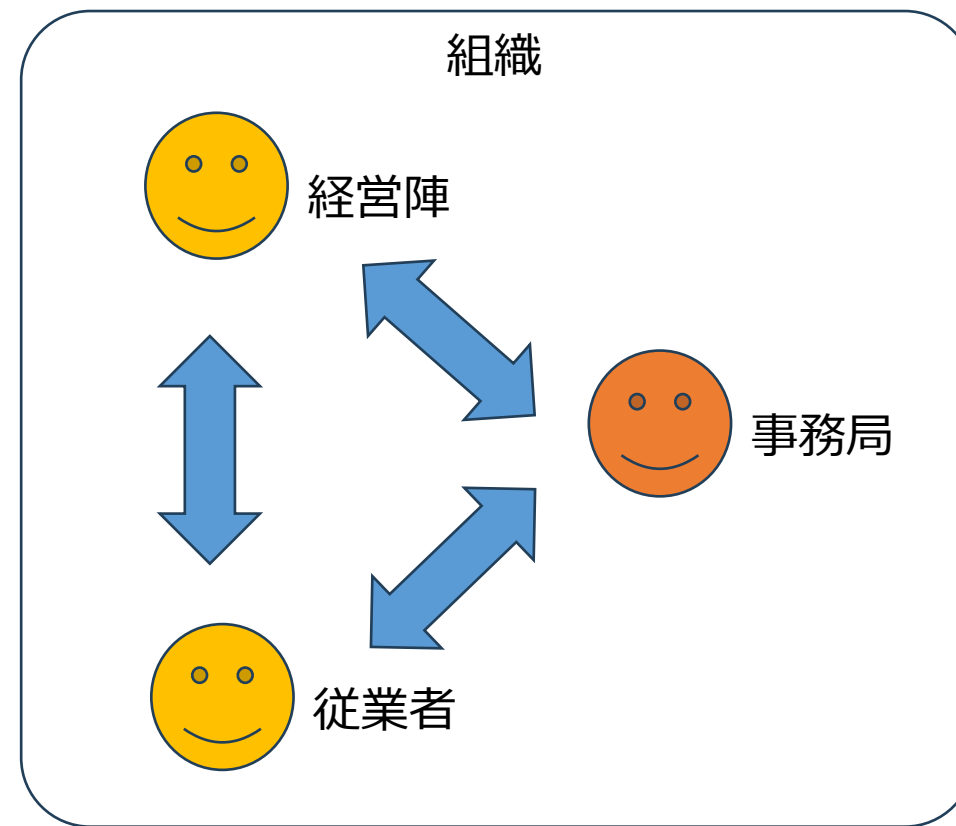


事務局



b)社内規定の認識のズレ

- 発生するのは、組織内の事務局、経営陣、従業者
- 対象は、組織内のルール（情報セキュリティ規程）
- 関連する認証規格JIS Q 27001
 - 経営陣
 - 箇条5 リーダーシップ
 - 従業者
 - 箇条 6.3 意識向上、教育及び訓練
 - 箇条 7.3 認識



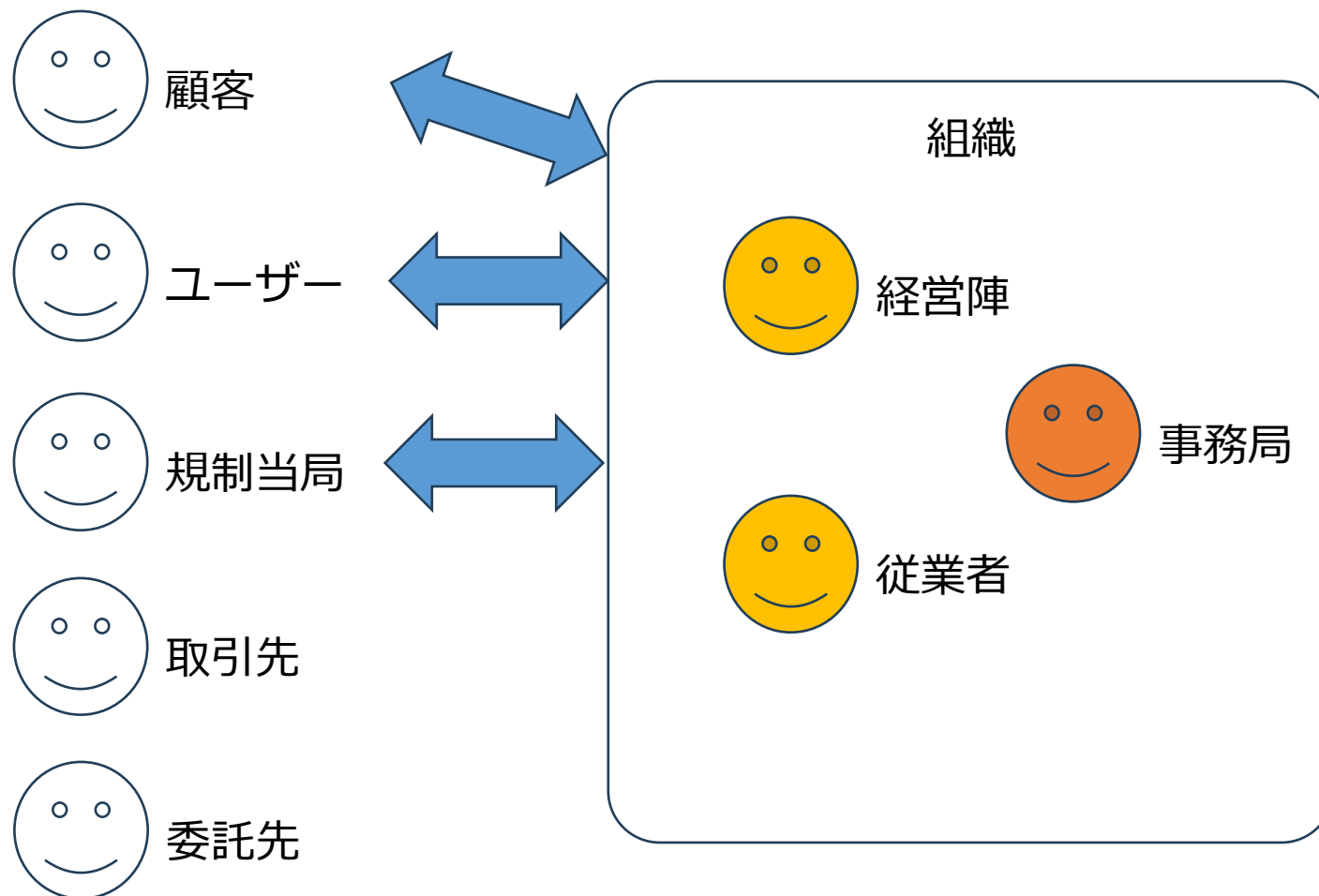
c)外部の利害関係者との認識のズレ

ケース

- ISMSはどこまで対策するかを決めて対応していくが、ユーザーの信頼をどこまでやれば勝ち取れるのかが大きな課題
- セキュリティ事故が発生したら、その規模の会社なら多要素認証を導入していて当然ではと指摘された。
- どこまでやればOKなのか（経営層が決めることなのかもしれないが）認識合わせがむずかしい。



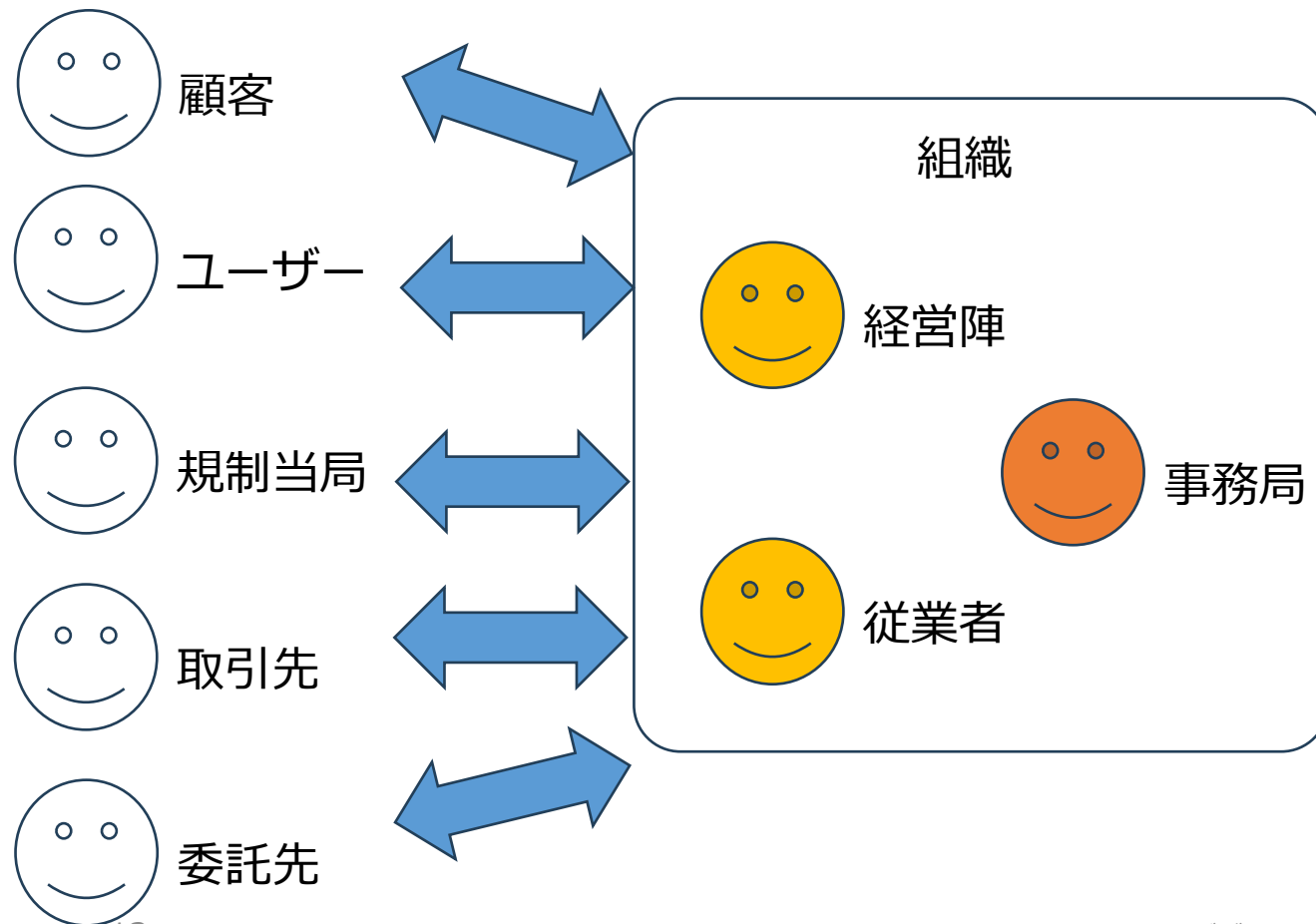
事務局



c)外部の利害関係者との認識のズレ

- 発生するのは、組織と組織外（顧客、ユーザー、規制当局など）
- 対象は、組織内のルールと組織外のニーズ、期待

- 関連する認証規格JIS Q 27001
 - 4.1 組織及びその状況の理解
 - 4.2 利害関係者のニーズ及び期待の理解



研究会メンバーからの事例集め

研究会メンバーからの事例集め



• アンケートフォーム

テーマA 認識合わせ

6月13日（金）までに、アンケートへの回答をお願いいたします。

「認識合わせ」をテーマに、これまで関係者間の認識が合わず苦労した事例をインプリ研のメンバーの皆さまから集めるためにアンケートです。
皆さまの組織やコンサルしているお客様の事例について差し支えない範囲でお答えいただければ幸いです。

tokitamu@lycorp.co.jp [アカウントを切り替える](#)

* 必須の質問です

メールアドレス*

メールアドレス

事例名*

回答を入力

事例の分類*

認識合わせを要する関係者によって、a)~c)のいずれかを選択してください。

- a)規格の解釈（審査員、コンサルと事務局の認識合わせ）
- b)正しい規格解釈の後の実装（内部の利害関係者と事務局の認識合わせ）
- c)外部の利害関係者（審査員、コンサル以外の外部の利害関係者と事務局の認識合わせ）
- その他: _____

認識合わせを要する関係者*

認識合わせを要する関係者を選択してください。

- 審査員
- 事務局
- コンサルタント
- 経営陣
- 従業者
- 顧客・ユーザー
- 規制当局
- 取引先
- 委託先
- その他: _____

事例が見られたフェーズ*

事例が見られたフェーズを選択してください。

- ISMS構築フェーズ（初回認証までの審査以外の場）
- ISMS構築フェーズ（初回認証までの審査の場）
- ISMS運用フェーズ（初回認証後の審査以外の場）
- ISMS運用フェーズ（初回認証後の審査の場）
- その他: _____

事例が関連する27001箇条番号（本文）*

事例が関連するISO/IEC27001箇条番号を選択してください（複数ある場合は、そのうちの1つを選択）。

選択

その他（付属書Aの箇条番号、自由記載）

前の質問で、「その他」を選択された場合、どちらかをご記載ください。

- ・付属書Aの5.1～8.34から該当するもの（記載例 6.8 情報セキュリティ事象の報告）
- ・関連しそうな規格要求事項について自由記載

回答を入力

事例の内容*

フリーフォーマットです。

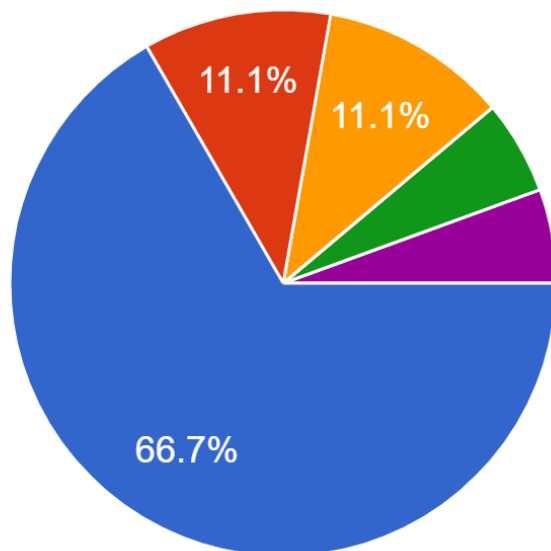
回答を入力

回答のコピーが指定したアドレスにメールで送信されます。

- ほとんどの事例は、a)規格の解釈に関するものでした

事例の分類

18件の回答



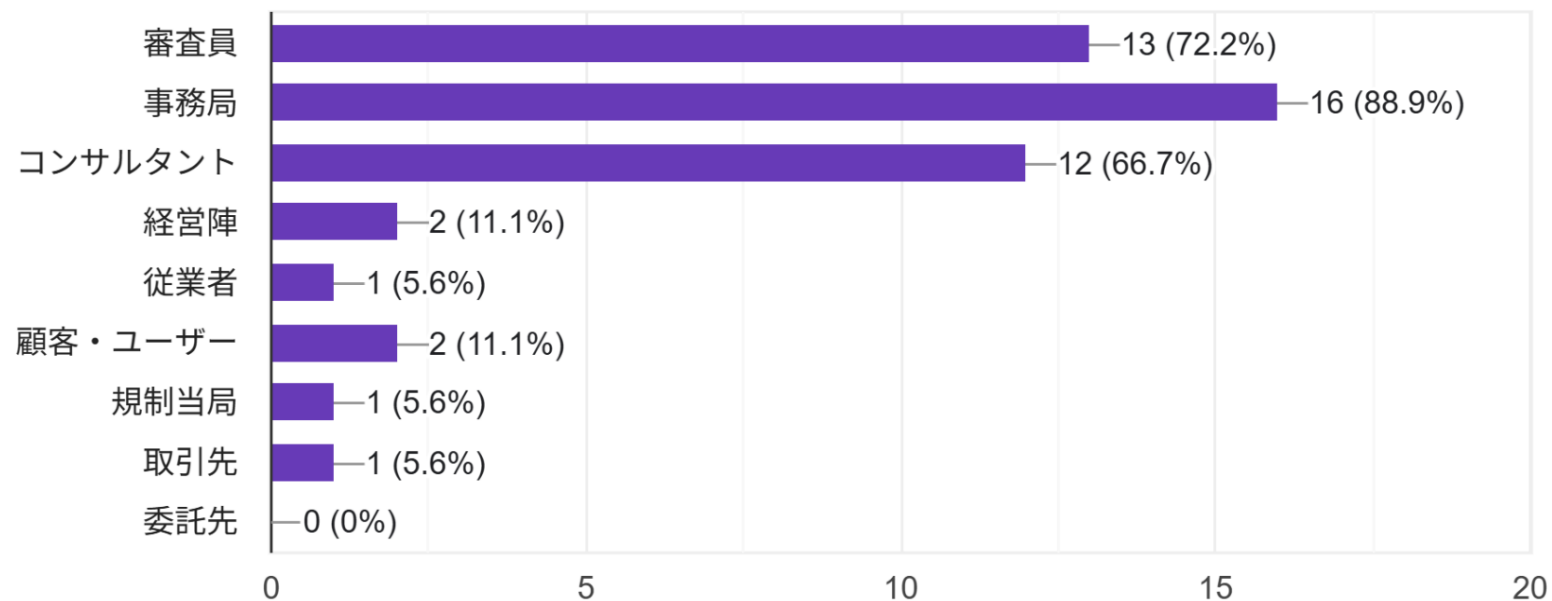
- a)規格の解釈 (審査員、コンサルと事務局の認識合わせ)
- b)正しい規格解釈の後の実装 (内部の利害関係者と事務局の認識合わせ)
- c)外部の利害関係者 (審査員、コンサル以外の外部の利害関係者と事務局の認...
- 監査法人 (審査員)、コンサル、事務局の事例を記載しました。
- 認証機関に対する国際的指針に従っていない審査員

認識合わせを要する関係者

- 関係者は、事務局、審査員、コンサルタントがほとんど

認識合わせを要する関係者

18件の回答

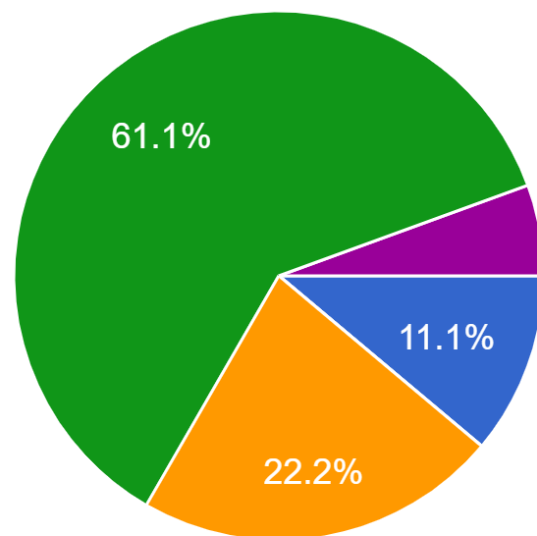


事例が見られたフェーズ

- 構築フェーズよりも運用フェーズにおける事例が多く集まりました。

事例が見られたフェーズ

18件の回答



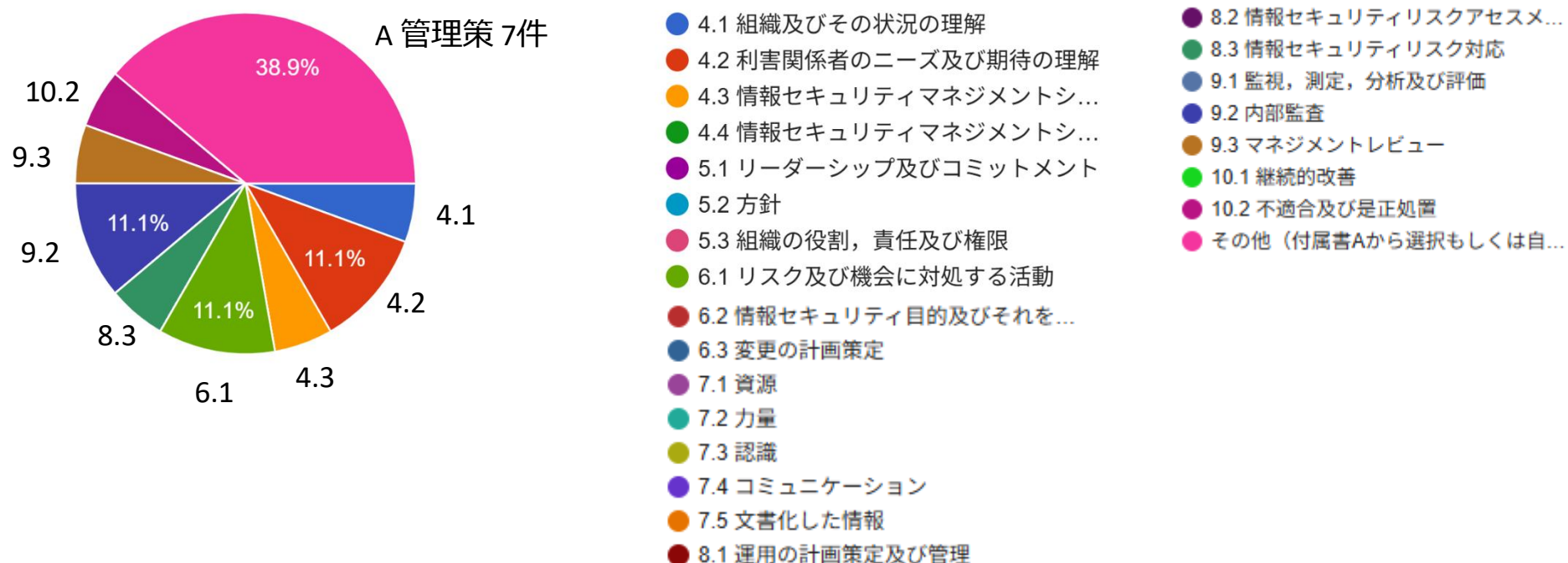
- ISMS構築フェーズ (初回認証までの審査以外の場)
- ISMS構築フェーズ (初回認証までの審査の場合)
- ISMS運用フェーズ (初回認証後の審査以外の場)
- ISMS運用フェーズ (初回認証後の審査の場合)
- NIST SP800の運用フェーズ

事例が関連するJIS Q 27001箇条番号（本文）

- 箇条4～10、付属書Aの管理策について、偏りなく集まりました。

事例が関連する27001箇条番号（本文）

18件の回答



事例紹介

a) 規格の解釈 で集まった事例を紹介します。

箇条4～10、付属書Aの管理策の順

事例 1 一部の部署が分社化したケースの認証範囲

箇条4.3 情報セキュリティマネジメントシステムの適用範囲の決定

事例 1 一部の部署が分社化したケースの認証範囲

ISMS運用フェーズ（初回認証後の審査以外の場）

分社化したので、その会社のISMS認証も必要になるな。大変だ。。



事務局

当社の一部の部署が分社化しました。分社化した会社として、ISMS認証取得する必要がありますよね。コストはどれくらいでしょうか。

今まで通りのISMS適用範囲で問題はないですよ。もともと同じ会社でISMSを運用していたので、1つのISMSとして変更申請（適用範囲の組織構成の変更）又は適用範囲拡大申請（分社化した組織の追加）をすればよいです。



コンサルタント



事務局

よかった。

事例 1 一部の部署が分社化したケースの認証範囲



- 関連する27001箇条

- 4.3 情報セキュリティマネジメントシステムの適用範囲の決定

別会社であっても、適用範囲とすることができる。

- ISMS適用範囲は、1つの会社である必要はない。
 - ISO/IEC 27001で「組織」は、「自らの目的（3.49）を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり」とされており、「自らの目的（3.49）を達成する」という目的の定義は「達成する結果」で注記には「目的は、様々な領域に関連し得るものであり、様々な階層で適用できる。」とある。
資本関係の無い組織が1つのISMSとして認証を受けていることもあるが、同じ目的（ISMSの構築及び運用）を持った集まり（領域 = 1つのISMS）と考えれば、不思議ではない。
- ただし、別会社となるため、「1つのISMS」として運用できることを示す必要がある。
例えば、分社化した会社とのISMS運用に関する協定や親元の規定を分社化した組織が順守することなど。
- 1つのISMSとして運用可能であれば認証取得ができる可能性は高い。認証機関によってできる/できないの条件に対する考え方が違う場合があるので事前に相談する必要がある。

4.3 情報セキュリティマネジメントシステムの適用範囲の決定

組織は、ISMS の適用範囲を定めるために、その境界及び適用可能性を決定しなければならない。

この適用範囲を決定するとき、組織は、次の事項を考慮しなければならない。

- a) 4.1 に規定する外部及び内部の課題
 - b) 4.2 に規定する要求事項
 - c) 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フェース及び依存関係
- ISMS の適用範囲は、文書化した情報として利用可能な状態にしなければならない。

(ISO/IEC 27001:2022 JIS Q 27001:2023より引用)

事例 1 に関連するISO/IEC 27000の条文



3.50 組織 (organization)

自らの目的 (3.49) を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。

注記 組織という概念には、法人か否か、公的か私的かを問わず、自営業者、会社、法人、事務所、企業、当局、共同経営会社、非営利団体若しくは協会、又はこれらの一部若しくは組合せが含まれる。ただし、これらに限定されるものではない。

3.49 目的 (objective)

達成する結果。

注記1 目的は、戦略的、戦術的又は運用的であり得る。

注記2 目的は、様々な領域 [例えば、財務、安全衛生、環境の到達点 (goal)] に関連し得るものであり、様々な階層 [例えば、戦略的レベル、組織全体、プロジェクト単位、製品ごと、プロセス (3.54) ごと] で適用できる。

注記3 目的は、例えば、意図する成果、目的 (purpose) 、運用基準など、別の形で表現することもできる。また、情報セキュリティ目的という表現の仕方もあり、さらに、同じような意味をもつ別の言葉 [例えば、狙い (aim) 、到達点 (goal) 、目標 (target)] で表すこともできる。

注記4 ISMS の場合、組織は、特定の結果を達成するため、情報セキュリティ方針と整合のとれた情報セキュリティ目的を設定する。

(ISO/IEC 27000:2018 JIS Q 27000:2019より引用)

原因

ISMSの適用範囲に関する誤解が生じた可能性

対策

事務局は、ISMSの適用範囲についての規格の要求事項を正しく理解し適切な対応を行うように努め、コンサルタントはそれを支援する。

事例 2 部分認証：ISMS適用範囲外の部署の管理策（初回審査前）

箇条 6.1 リスク及び機会に対処する活動

6.1.1 一般

6.1.2 情報セキュリティリスクアセスメント

6.1.3 情報セキュリティリスク対応

事例 2 部分認証：ISMS適用範囲外の部署の管理策（初回審査前）

初回審査前

当社のISMSは、適用範囲を事業部だけにして
認証取得するから適用範囲で行ってるセキュ
リティ対策を確認すればいいな。



事務局

当社は事業部で認証を取得するので、事業部以外のICT部門
や人事及び総務部門などが実施しているリスク対策につい
ては、適用宣言書で適用除外としていいですよ？

適用範囲の資産を保護する上で、必要な対策であれば、
適用範囲外の部署が行っている対策であっても、適用
宣言書では「適用」としなければならないですよ。



コンサルタント



事務局

どうして??

- **関連するISO/IEC 27001箇条**

- 6.1 リスク及び機会に対処する活動
 - 6.1.1 一般
 - 6.1.2 情報セキュリティリスクアセスメント
 - 6.1.3 情報セキュリティリスク対応

規格では、情報資産の保護が要求されている。

- 箇条6.1.2 c) 1) で組織は、適用範囲のリスクを特定するためにリスクアセスメントを行うことが要求されている。箇条6.1.3 a)では、特定したリスクには対応が必要となる。これらについて、規格要求では「誰がそのリスク対策を実施しているか」に拘ってはいない。
- 適用範囲の資産（情報及び情報を取り扱うICT設備とソフトウェア等）に関連するリスクについて、適用範囲外の部署が行っているリスク対策であっても、適用宣言書では「適用」である。
- その上で、適用範囲外の部署が行っているリスク対策（管理策）が適用範囲の部署の要求を満たしているかを確認し、満たしていなければ改善を要求し、それができなければリスク受容を行う必要がある。

6.1 リスク及び機会に対処する活動

6.1.1 一般

ISMS の計画を策定するとき、組織は、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。

- a) ISMS が、その意図した成果を達成できることを確実にする。
- b) 望ましくない影響を防止又は低減する。
- c) 継続的改善を達成する。

組織は、次の事項を計画しなければならない。

- d) 上記によって決定したリスク及び機会に対処する活動
- e) 次を行う方法
 - 1) その活動の ISMS プロセスへの統合及び実施
 - 2) その活動の有効性の評価

(ISO/IEC 27001:2022 JIS Q 27001:2023より引用)

6.1.2 情報セキュリティリスクアセスメント

組織は、次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め、適用しなければならない。

- a) 次を含む情報セキュリティのリスク基準を確立し、維持する。
 - 1) リスク受容基準
 - 2) 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
- b) 繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にする。
- c) 次によって情報セキュリティリスクを特定する。
 - 1) ISMS の適用範囲内における情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために、情報セキュリティリスクアセスメントのプロセスを適用する。
 - 2) これらのリスク所有者を特定する。

(ISO/IEC 27001:2022 JIS Q 27001:2023より引用)

6.1.2 情報セキュリティリスクアセスメント

組織は、次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め、適用しなければならない。

d) 次によって情報セキュリティリスクを分析する。

1) 6.1.2 c) 1) で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。

2) 6.1.2 c) 1) で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。

3) リスクレベルを決定する。

e) 次によって情報セキュリティリスクを評価する。

1) リスク分析の結果と 6.1.2 a) で確立したリスク基準とを比較する。

2) リスク対応のために、分析したリスクの優先順位付けを行う。

組織は、情報セキュリティリスクアセスメントのプロセスについての文書化した情報を保持しなければならない。

(ISO/IEC 27001:2022 JIS Q 27001:2023より引用)

6.1.3 情報セキュリティリスク対応

組織は、次の事項を行うために、情報セキュリティリスク対応のプロセスを定め、適用しなければならない。

- a) 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応の選択肢を選定する。
- b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。

注記 1 組織は、必要な管理策を設計するか、又は任意の情報源の中から管理策を特定することが可能である。

- c) 6.1.3 b) で決定した管理策を附属書 A に示す管理策と比較し、必要な管理策が見落とされていないことを検証する。

注記 2 附属書 A は、考えられる情報セキュリティ管理策のリストである。この規格の利用者は、必要な情報セキュリティ管理策の見落としがないことを確実にするために、附属書 A を参照することが求められている。

注記 3 附属書 A に規定した情報セキュリティ管理策は、全てを網羅していない。必要な場合は、追加の情報セキュリティ管理策を含めることが可能である。

(ISO/IEC 27001:2022 JIS Q 27001:2023より引用)

6.1.3 情報セキュリティリスク対応

組織は、次の事項を行うために、情報セキュリティリスク対応のプロセスを定め、適用しなければならない。

d) 次を含む適用宣言書を作成する。

- 必要な管理策 [6.1.3 の b) 及び c) 参照]
- それらの管理策を含めた理由 – それらの必要な管理策を実施しているか否か
- 附属書 A に規定する管理策を除外した理由

e) 情報セキュリティリスク対応計画を策定する。

f) 情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について、リスク所有者の承認を得る。

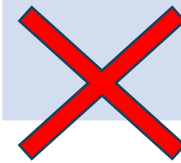
組織は、情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。

注記 4 この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは、JIS Q 31000に規定する原則及び一般的な指針と整合している。

(ISO/IEC 27001:2022 JIS Q 27001:2023より引用)

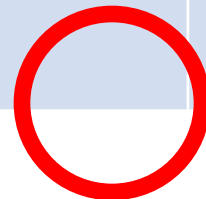
誤った適用宣言書 例：6.2雇用条件

項番	管理策	目的	選択	選択・除外理由	当社の対応
6.2 雇用条件	雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載しなければならない。	要員が、自らの役割における情報セキュリティの責任を理解していることを確実にするため。	適用しない	実施部門がISMS適用範囲外であるため	人事部門が主管となり、「正社員就業規則」「契約社員就業規則」「嘱託社員就業規則」にて定め、周知されている。また入社時、誓約書を記載してもらっている。



正しい適用宣言書

項番	管理策	目的	選択	選択・除外理由	当社の対応
6.2 雇用条件	雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載しなければならない。	要員が、自らの役割における情報セキュリティの責任を理解していることを確実にするため。	適用する	情報資産の保護に必要であるため	人事部門が主管となり、「正社員就業規則」「契約社員就業規則」「嘱託社員就業規則」にて定め、周知されている。また入社時、誓約書を記載してもらっている。



原因

ISMSの「部分認証」における適用範囲と管理策の責任範囲に関する誤った認識

対策

事務局は、規格の適用範囲と管理策の責任範囲についての要求事項を正しく理解し適切な対応を行うように努め、コンサルタントはそれを支援する。

事例 3 部分認証：ISMS適用範囲外の部署の管理策（初回審査）

箇条6.1 リスク及び機会に対処する活動

6.1.1 一般

6.1.2 情報セキュリティリスクアセスメント

6.1.3 情報セキュリティリスク対応

事例3 部分認証：ISMS適用範囲外の部署の管理策（初回審査）



初回審査

事業部以外のICT部門や人事及び総務部門がリスク対応策を実施していることは確認した。リスクアセスメントしてリスク対策を確認したことで、すべてリスク受容水準にあることも確認した。



事務局

適用範囲内の資産の保護について適用宣言書を作成しました。
A.X.XX・・・は適用範囲外の部門が担当している管理策になります。

A.X.XX・・・は認証範囲外の他部署の管轄なの
ですね。では、適用範囲の部門が担当している管
理策を確認していきましょう



審査員



コンサルタント

【事務局に対して】審査では他部門のリスク対策について確認
しませんでした。適用範囲の資産に影響のあるリスク対策に
ついては、定期的な見直しを継続してください。

• 関連するISO/IEC 27001箇条

- 6.1 リスク及び機会に対処する活動
 - 6.1.1 一般
 - 6.1.2 情報セキュリティリスクアセスメント
 - 6.1.3 情報セキュリティリスク対応

審査員（認証機関）に対する要求事項がある。

- 認証機関に対する要求事項のISO17021-1では、初回認証審査においてすべての要求事項を審査することを要求している。また、再認証審査では、内部及び外部の変更に対するマネジメントシステム全体としての有効性、並びに認証範囲に対するマネジメントシステムの継続的な関連性及び適用可能性を確認することが要求されている。
- 従って、「適用範囲外の部署の責任である」という言葉だけで、該当部分のリスクが受容水準まで低減されていることを適用範囲の組織が把握しているかの確認をしないのは、組織のマネジメントシステムの有効性や継続的な関連性及び適用可能性を評価できていないことになる。
- 他ケースでISMS構築の段階では他部署の活動の確認をしたが、翌年以降に継続的な実施確認をしていなかったとして、サーベイランス審査で改善の機会を指摘されていることもあった。

原因

審査時の解釈が規格要求の範囲と乖離していた可能性

対策

審査員としては、認証審査に対する要求事項を理解し実行すること。

事務局としては、次のとおり。適用範囲外の部門が担当しているリスク対策の状況を確認しなかったとしても、不当な審査所見を出したわけではないため認証機関への苦情は出しにくい。

しかし、本来の審査であれば、他部門が担当しているリスク対策の継続的实施状況について、適用範囲のリスクの見直しの対象となっているかの確認が行われる。そのため、組織は、今回の審査対象にならなかったとしても他部門のリスク対策の確認を中止することなく、他部門に依存しているリスク対策を一種の供給者関係とみなして継続的に確認する必要がある。

事例 4 リスクの対象が無いリスク対応計画

箇条 6.1 リスク及び機会に対処する活動

6.1.1 一般

6.1.2 情報セキュリティリスクアセスメント

6.1.3 情報セキュリティリスク対応

事例 4 リスクの対象が無いリスク対応計画

ISMS運用フェーズ（初回認証後の審査の場）



事務局

当社では、CDやUSBメモリなどの可搬媒体を廃止し全てネットワーク上のサーバに格納することにしました。

可搬媒体の廃止はリスク対策として実行するものであるなら、リスク対応計画があるべきです。リスク対応計画がないという指摘になります。



審査員



事務局

既に終わったことだがこれから計画を作成すればよいか。



コンサルタント

今後のこともあるので、既に完了した処理について計画するのは意味がないので対応不要と回答しなさいとアドバイスしよう

事例 4 リスクの対象が無いリスク対応計画



- **関連するISO/IEC 27001箇条**

- 6.1 リスク及び機会に対処する活動
 - 6.1.1 一般
 - 6.1.2 情報セキュリティリスクアセスメント
 - 6.1.3 情報セキュリティリスク対応

リスク対応計画は、計画したことを確実に実施するために作成するもの

- 本件は単純にリスクの対象となるものがなくなる（＝リスク源の除去）のであるため、それ以上の対策は存在しない。リスク対応計画は、計画したことを確実に実施するために作成するものであり、決定と同時に完了するような事項には必要ない。
- 審査員は、「リスク対策」という言葉に反応し、リスク対応計画を出すように要求したが組織が実際に行ったことをきちんと確認すれば指摘の必要はなかった可能性がある。
- コンサルタントは今後のこともあるので、事務局に規格の趣旨を説明した上で対応不要とするようにアドバイスした。
- 多少のやり取りはあったが、最終的には審査員もリスク対応計画は不要であることに同意した。

原因

審査員がISMSの要求事項を表面的に、かつ形式的に解釈したこと。
または（推測含む）、指摘の意図を伝えられなかったこと。

対策

審査員は、「リスク対策」には「リスク対応計画」が必要であると短絡的に指摘しないようにISMSの要求事項を理解する。

または（推測含む）、審査員の指摘が媒体の廃棄計画について、過去に遡って計画を作成するようということではなく、発見した事実として「計画がなかった」ということを指摘し、今後同じようなことが起きないようにしなさいという意味であった場合は、その意図を正しく事務局に伝えること。

事例 5 内部監査の指摘事項ゼロ

箇条 9.2 内部監査

9.2.1 一般

9.2.2 内部監査プログラム

事例 5 内部監査の指摘事項ゼロ

ISMS運用フェーズ（初回認証後の審査の場）



事務局

内部監査の指摘事項はありませんでした。

指摘事項がゼロ件というのは内部監査プログラムの不備です。次回もゼロ件なら不適合とします。



コンサルタント

【事務局へ】そのような要求事項はないので、内部監査の実施内容を説明するとよいですよ。



審査員



事務局

内部監査プログラムの要求事項には、「指摘事項がゼロ件ではないこと」はありません。当社の内部監査プログラムと実際に行ったヒアリング結果を見てください。

内部監査プログラムに不備がないことがわかりました。



審査員

事例 5 内部監査の指摘事項ゼロ



- 関連するISO/IEC 27001箇条

- 9.2 内部監査
 - 9.2.1 一般
 - 9.2.2 内部監査プログラム

指摘事項がゼロ件ではないことは、内部監査プログラムの要求事項ではない。

- この組織の内部監査では、事前に監査チェックリストを配布し各部署から「できている証拠」を添付して回答することを要求し、その結果をもとに「できていること」を事務局が監査員としてインタビューで確認するという手法をとっている。
- 内部監査プログラムに不備がありそのために監査所見がないのであれば指摘するのは当然であるが、単に現象としての「内部監査の指摘事項ゼロ件」を証拠として指摘しようとするのは規格要求事項と不整合がある。
- 審査では、内部監査プログラムと実際に行ったヒアリングの結果を提示し、規格には指摘事項がなければ不適合という要求は書いていないはずという反論を行い結果的にその意見は取り下げとなった。

事例 5 内部監査の指摘事項ゼロ



原因

審査員のISMS規格に対する拡大解釈と、内部監査プログラムの確認不足

対策

審査員は拡大解釈をしないように努め、内部監査の審査においては内部監査プログラムを確認する。

事例 6 一部の部署が分社化したケースの物理セキュリティ

付属書A 7.1 物理的セキュリティ境界

事例 6 一部の部署が分社化したケースの物理セキュリティ

ISMS運用フェーズ（初回認証後の審査以外の場）

分社化したから、その会社も適用範囲にして、審査までに対応しないと。



事務局

当社の一部の部署が分社化しました。分社化した会社は同じ事務所フロアに同居するため、パーティションで囲いドアをつけて独立した区画にしようと考えています。

それはリスクアセスメントに基づいた対策ですか。審査で指摘されそうだからパーティションで仕切るということではなく、リスクアセスメントに基づいて決めることが大事です。



コンサルタント



事務局

なるほど。無駄なコストかけるところだった。

- **関連するISO/IEC 27001箇条**

- 付属書A 7.1 物理的セキュリティ境界

審査のためではなく、リスクアセスメントの結果に基づいて対策を行う。

- ISMSのリスク対応は、リスクアセスメントに基づいて対策するものであり、審査で指摘されないことを念頭に対応を考えているところが誤っている。
- 分社化した相手がどれほどのリスクある存在なのかをアセスメントした上で対応を決めればよく、審査で指摘されそうだからパーティションで仕切るというのはやや短絡的と思われる。
- リスクアセスメントにおいては、昨日まで一緒にISMSを推進してきた部門が分社化したとたんに危険な組織に変化するという考え方は論理的ではなく、お互いに同居する兄弟会社としてそれぞれの情報資産を保護するという意思があれば、会社間の協定や同居する部署同士の話し合いで解決できる部分は多々あると考えられる。同じ部屋で仕事ができる間柄であれば、業務時間中のリスクは受容できるレベルであろうし、不在時（業務時間外）の安全対策は施錠管理で十分かもしれない。

原因

ISMSの管理策の選択を審査のために行うという誤った認識

対策

事務局は、規格の要求事項を正しく理解し適切な対応を行うように努め、コンサルタントはそれを支援する。

まとめ

なぜ「話が通じない」のか？

・視点の違いがズレを生む

- ・ 審査員・コンサルタントは、職業柄「規格」や「形式」の適合性を重視する傾向があります。
- ・ 事務局（皆さん）は、日々の「現場」や「実態」を見ています。
- ・ この違いこそが、コミュニケーション不全の根本原因です。
- ・ 「どちらが間違っているか」ではなく、「視点が違う」ことを前提に対話する必要があります。



ズレを解消する「3つの原則」



1. リスクに立ち返る

指摘やアドバイスに迷ったら、自問してください。

「それは当社の情報セキュリティリスクを本当に下げるのか？」

形式的な対応ではなく、実質的なリスク低減を優先しましょう。

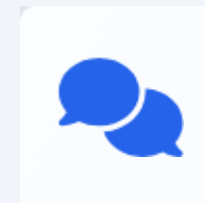


2. 目的を説明する

「規格にこうあるから」と言われたら、反論ではなく説明をします。

「当社のプロセスの目的は〇〇であり、現状でそれは達成できている」

手順の有無ではなく、目的の達成度で合意を図ります。



3. 対話を恐れない

審査員やコンサルタントの言葉を鵜呑みにする必要はありません。

「その指摘の根拠はJIS Q 27001のどこですか？」

納得がいかない場合は根拠を確認し、こちらの意図を伝えましょう。

事務局のみなさんへ



審査や運用で「どうして伝わらないんだろう？」と悩むこともあるかもしれません。

でも、これだけは覚えておいてください。

ISMSの主演は、審査員やコンサルタントでもなく、日々現場を守っている「事務局」のみなさんです。

アドバイスはうまく使いながら、最後は自分たちの会社が一番合ったやり方を決めてよいのです。

自信をもってISMSを構築し運用していきましょう！

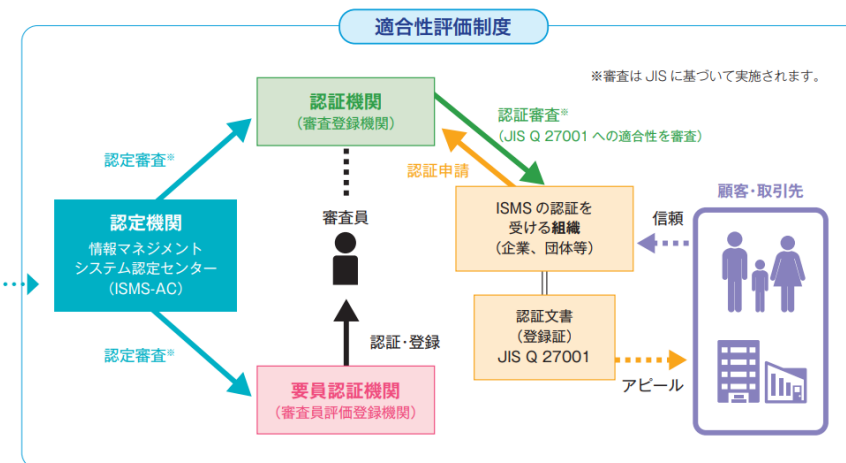


ご清聴ありがとうございました。

Appendix

ISO/IEC 27006 (JIS Q 27006)

- JIS Q 27006
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の審査及び認証を行う機関に対する要求事項
- JIS Q 17021-1
適合性評価－マネジメントシステムの審査及び認証を行う機関に対する要求事項－第1部：要求事項
- JIS Q 17021-1は、マネジメントシステム審査・認証を行う機関（認証機関）に求められる一般的な要求事項を定めた規格です。JIS Q 27006は、情報セキュリティマネジメントシステムを審査・認証する機関に対して、JIS Q 17021-1の要求に加えてさらにISMS審査・認証に特化した追加要求および手引きを定めた規格です。したがって、認証機関がISMS認証を実施する場合はまずJIS Q 17021-1に適合することが前提となり、さらにJIS Q 27006の要求も満たす必要があります。
- 日本産業標準調査会（JISC）のHPの「JIS検索」から、本文を閲覧できます。<https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html>



認定機関がISMS認証機関を認定する意義

認定機関である情報マネジメントシステム認定センター（ISMS-AC）は、認証機関が適切に審査を実施できる体制・能力を持っているかを、国際規格（ISO/IEC 27006）[※]に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けたISMS認証機関は、適切なISMS認証審査を実施することのできる、信頼のおける認証機関であることを意味します。要員認証機関についても同様です。

認定シンボル（右）と認証機関マーク（左）が並んだ表示例



認定シンボルと認証機関のマークが2つ並んでいることは、その認証機関が国際規格に従った適切な審査を実施していることを、認定機関であるISMS-ACが保証していることを示します。

※ISO/IEC 27006(JIS Q 27006)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の審査及び認証を行う機関に対する要求事項

ISMS適合性評価制度の概要（パンフレット）より
<https://isms.jp/doc/JIP-ISMS120-72.pdf>

JNSA