４．　お客様にご準備いただきたい事項と審査の詳細

審査までにご準備いただきたい事項と、各段階の審査の詳細をご紹介します。

４．１　各審査共通のご準備をお願いする事項

項目	準備期限	準備事項
変更事項の通知	変更時即時	次の適用範囲に関わる事項に変更があった場合、変更時にその概要を ISA へご通知下さい。できる限り電子データでご送付下さい。変更審査の必要性を判断します。 (変更通知様式を巻末に提示します。) ● 対象事業/業務内容 ● 対象組織の代表者/所有権 ● 連絡先窓口 ● 認証対象事業所の所在地 ● 対象施設/情報システム等プロセス上の大きな変化
審査予定のご確認	「審査日程と審査員のお知らせ」返信まで	予定されている審査時期が近づいてまいりましたら ISA より「審査日程と審査員のご提案」(その時点で把握させていただいている貴組織の基本情報と、次回審査日程及び担当する審査員を通知する文書)を FAX 又はメールにより送付させていただきます。 通知内容に問題が無い場合（基本情報に間違い/変更がない事をご確認下さい。また審査日程及び担当審査員にご了解いただけるかを確認下さい。）本書にご担当者様のご署名をいただき、FAX 又はメールにてご返送をお願いします。本書返信受領にて、審査予定を確定させていただきますが、通知内容に変更がある場合(審査対象拠点の所在地、要員規模、対象業務内容等)、審査計画(審査工数、日程、担当審査員)を変更する必要が出てくる場合があります。
審査員宿泊先の手配	「審査日程と審査員のご提案」返信まで	ISA から御社に提示する「審査日程と審査員のご提案」に宿泊手配の依頼が提示されている場合、次の要件を満たす宿泊先をご手配下さい。また「審査日程と審査員のご提案」への返信時に、手配した宿泊先の情報を追記いただき ISA へご通知下さい。 ● 1 泊 1 万円以内（消費税別・朝食付　禁煙） ● 夕食不要　チェックイン 21 時
最新文書の準備	審査日前日まで	次の事項を含め、ISMS 文書記録一式を審査場所で審査員が確認できるように準備してください。紙でも、見読できるデータ資料でも結構です。 事前にご提出いただく必要はありません。 ● 情報セキュリティ方針/マニュアル/規定/手順書 ● 適用宣言書 ● リスクアセスメントの記録、リスク対応計画文書 ● 情報セキュリティ目的達成の為の計画文書 ● その他計画文書および記録

審査員用部屋の準備	審査日まで	オープニングミーティング、クロージングミーティングおよび、審査員が昼食を頂いたり各種作業を行ったりする部屋をご用意ください。 審査員は審査報告資料作成の為、モバイル PC の持ち込みをさせて頂きますので電源の確保もお願いします。
昼食の準備	審査日まで	簡単なもので結構ですので、審査日程に昼食時間を挟む場合、担当審査員人数分の昼食をお客様ご負担でご用意ください。
御社対応要員の確保	審査日まで	オープニングミーティング、クロージングミーティングおよび経営者インタビューの時間には、経営陣のご参加をお願いします。(通常オープニングは審査開始後の 30 分間、クロージングは審査終了前の 30 分間で行います）特にクロージングミーティング時には、経営者様もしくはその代理の方の署名が必要です。 その他審査対象者/部署については、審査日程表にて連絡申し上げます。
審査場所のご案内者	審査日まで	ご案内者（審査場所のご案内をいただける方）をご手配下さい。

４．２　初回認証審査　目的と方法

４．２．１　第１段階審査について

目　　的　： ● 御社の組織及び組織を取り巻く状況を理解すること。 ● 御社の ISMS とその準備状況理解すること。 ● 初回第２段階審査に移行できるかを判断し、その審査計画の焦点を定めること。
実施方法と対象： 主に ISMS 文書や計画文書を中心に評価を進めます。管理責任者・事務局を主たる対象者としますが、各部門の資産およびリスクの状況及びＩＴ管理所管者や人事総務所管者のセキュリティ管理手続きの整備状況などについては、各所管者に確認します。
留 意 事 項　： ● ISMS 運用のため計画が策定されていることを前提に審査を進めます。内部監査・マネジメントレビューについては実施計画が確実に整備されている状況が望ましいです。 ● 第１段階審査の結果は、審査員がクロージングミーティングの終了時に報告します。 ● 懸念事項は、第２段階審査までに修正を完了する必要があります。 ● 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。

確認項目	主たる確認内容	主たる確認対象
組織の状況	組織及び組織を取り巻く状況の確認	● 組織の事業内容、利害関係者等からの要求事項等 ● 組織内部、外部の課題
事業上必要な規制事項の確認	適用規制の概要及び当局との協定/通信内容、責任範囲の確認。	● 法規制リストや許可証 ● 顧客との契約書 ● 外部事業者との契約書
適用範囲	適用範囲の業務/組織/物理的区画/論理的区画の確認。	● 各プロセスの責任の所在に関する情報 ● オフィス等の図面や組織図、ネットワーク構成図など審査対象範囲を特定するための資料 ● 外部委託事業者との契約書面 ● オフィスやＩＴインフラの状況
情報セキュリティ方針、情報セキュリティ目的	設定の仕組み、内容。	● 情報セキュリティ方針及び情報セキュリティ目的の記述文書
リスクアセスメントの方法、リスクアセスメント結果	リスクアセスメントの方法と関連様式等の確認。(比較可能性、再現可能性の担保)	● リスクアセスメントの方法や基準を定めた文書 ● リスクアセスメント結果記録
管理目的、管理策の導出状況	管理目的管理策の採用非採用理由の確認。	● 適用宣言書
リスク対応計画の策定状況 文書化の状況	計画の対象と計画内容の確認。(文書化された要求事項が実現できるか)	● リスク対応計画 ● 各種ＩＳＭＳ運用のための文書 ● 詳細管理策をもとに計画したＩＳＭＳ文書
情報セキュリティ目的及びその達成の為の計画	部門及び階層において確立された情報セキュリティ目的とその達成計画の確認。	● 情報セキュリティ目的と目的達成計画の管理文書

組織的/人的セキュリティ、教育訓練の計画	各種計画の確認。	● ＩＳＭＳ上の役割と責任、必要とする力量 ● 外部組織との関係や契約の状況 ● 入退職時の手続き、教育訓練手順、教育訓練計画など
事業継続マネジメントにおける情報セキュリティ継続の考慮	事業継続計画の立案状況と検証計画状況の確認	● 事業継続のプロセス及び手順に関する文書 ● 事業継続の検証の記録等
情報セキュリティパフォーマンス評価の対象と測定方法	ＩＳＭＳのパフォーマンス及び有効性をどのように測定するか確認。	● パフォーマンス評価の対象と方法
内部監査システム	計画状況確認。 (計画及び実施記録確認)	● 内部監査の実施計画と実施記録
マネジメントレビュー	計画状況確認。 (計画及び実施記録確認)	● マネジメントレビューの実施計画と実施記録
インシデント対応、セキュリティ違反対応	インシデント、セキュリティ違反発生時の対応方法確認。	● インシデント対応の手順など ● 就業規則など
不適合及び是正処置	計画状況確認。	● 是正処置の手順を文書化したものなど

４．２．２　第２段階審査について

目　　的　： ● 情報セキュリティ方針、情報セキュリティ目的、手順に従って構築された ISMS が実施されていることを確認する。 ● ISMS 規格のすべての要求事項に適合していること、御社 ISMS が情報セキュリティ方針及び情報セキュリティ目的を実現しつつあることを確認する。
実施方法と対象： ● ISMS 文書・運用記録閲覧、お客様の組織内の活動や機器の設定状況の観察、役職員への質問を通じて、計画されたマネジメントシステムの運用状況、遵守の状況を確認します。特に次の事項を重点的に確認します。 ➢ 情報セキュリティ方針及び情報セキュリティ目的の確立、ISMS 活動に対する積極的な関与によりトップマネジメントのリーダーシップ及びコミットメントが実証されていること ➢ 組織内外の課題・要求事項と、情報セキュリティ方針及び情報セキュリティ目的が、相互に論理的に矛盾なく結び付けられていること ➢ 情報セキュリティに関するリスクアセスメントが一貫性/妥当性があり、比較可能な結果を生み出していること ➢ リスクアセスメント及びリスク対応プロセスに基づく，管理目的及び管理策の選択が適切に行われていること ➢ ISMS の意図した成果を達成する為に選択した管理策が適切に運用され管理されていること ➢ 27001 規格の文書化に関する要求事項が全て満たされていること ➢ ISMS のパフォーマンス及び有効性の評価の仕組みが明確であること ➢ ISMS 内部監査及びマネジメントレビューが実施されていること ➢ ISMS の各プロセスのレビューを通じて、経営陣の決定が裏付けられており、情報セキュリティ方針及び情報セキュリティ目的の達成へ向けた取り組みが行われていること
留 意 事 項 ： ● 内部監査・マネジメントレビューが完了し、マネジメントシステムの運用が、少なくとも 1 度完了していることを前提に審査を進めます。 ● 第 2 段階審査の結論は、審査員がクロージングミーティング終了時に通知いたします。 ● 第 2 段階審査で提示するマイナーな不適合は、審査完了日から１カ月以内にその完了をＩＳＡへ通知しなければなりません。改善が望ましい観察事項については、次回審査時にその対応状況を確認します。 ● メジャーな不適合については、再審査となります。検出した時点で審査は停止する場合があります。その後の対応方法については、ＩＳＡからご案内します。 ● 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。

確認項目	主たる確認内容	主たる確認対象
組織の状況	内外の課題、要求事項 事業環境の変化点	● マネジメントレビュー/経営者インタビュー ● 法規制リストや許可証 ● 顧客及び外部供給者との契約書

情報セキュリティ方針、情報セキュリティ目的	達成の状況。今後の展開。	● マネジメントレビュー/経営者インタビュー ● 情報セキュリティ方針文書、情報セキュリティ目的に関する文書
適用範囲	現在の状況及び見直しの状況。	● 各プロセスの責任の所在に関する情報 ● オフィス等の図面や組織図など審査対象範囲を特定するための資料 ● 外部委託事業者との契約書面 ● オフィスやＩＴインフラの状況 ● ネットワーク構成を図示した資料
リスクアセスメントのプロセス及び結果	実施結果と見直しの状況	● リスクアセスメントの基準やリスクアセスメント結果記録
管理目的、管理策の導出状況	現在の状況及び見直しの状況	● 適用宣言書
リスク対応の状況	リスク対応計画とその進捗状況 採用管理策の運用状況	● リスク対応計画とその結果 ● 採用された詳細管理策の運用状況及びその管理記録(各種機器等の設定運用の状況含む)
組織的/人的セキュリティ	運用結果の確認。	● 組織要員及び関係する場合サービス提供を受ける外部供給者に対し実施される教育や契約、評価等の実施状況
事業継続マネジメントにおける情報セキュリティの側面	事業継続における要求事項の決定、手順の確立とその検証状況の確認。	● 事業継続の計画文書及びそのテスト結果
ISMS のパフォーマンス及び有効性評価	ISMS のパフォーマンス及び有効性評価の為に特定した監視測定の方法と結果を確認。	● 監視測定の対象とその評価方法 ● 監視測定の結果
内部監査	内部監査の計画と結果を確認。	● 内部監査の計画状況とその実施記録
マネジメントレビュー	マネジメントレビューへの報告事項と評価結果、決定/指示事項の確認。	● マネジメントレビュー記録 ● マネジメントレビューから出た決定/指示事項への対応状況
インシデント対応、ｾｷｭﾘﾃｨ違反対応 苦情への対応状況	インシデント発生状況と処置の実施状況の確認。	● インシデントの発生実績及び処置の記録
不適合及び是正処置	発生した不適合の実績と発生時の対応結果の確認。	● 不適合及び是正処置の記録

４．３　サーベイランス審査　目的と方法

目　　的　：

- 御社が経営環境の変化を踏まえ、ISMS の必要な見直しを実施している事を確認する。
- ISMS が引き続き適切に実施されていること、認証要求事項を満足していることを確認する。

実施方法と対象：

- サーベイランス審査では、次の事項を含む運用状況を審査して、お客様のマネジメントシステムが認証要求事項を満足しているか否か評価します。
  - 内外の課題、要求事項(関連法令規制含む)の変化と変化への対応状況
  - 組織、文書、適用範囲の変更の必要性の検討結果と対応の状況
  - 前回までの「是正処置要求書」への対応状況
  - 前回までの「観察事項」への対応状況
  - その他 ISA からの照会事項への対応状況
  - ISMS の継続的な運用管理状況
  - インシデント（あった場合）への対応状況
  - 不適合、是正処置への対応状況
  - 内部監査実施状況
  - マネジメントレビュー実施状況
  - 登録証/認定・認証マークの使用状況、「電子清刷」の管理状況
  - 情報セキュリティ方針及び情報セキュリティ目的の達成状況
  - ISMS パフォーマンス及び有効性の評価結果

留 意 事 項 ：

- 審査の結論は、審査員がクロージングミーティング終了時に通知いたします。
- 審査で提示するマイナーな不適合は、審査完了日から１カ月以内にその完了をＩＳＡへ通知しなければなりません。改善が望ましい観察事項については、次回審査時にその対応状況を確認します。
- メジャーな不適合については、再審査となります。検出した時点で審査は停止します。その後の対応方法については、ＩＳＡからご案内します。
- 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。

確認項目	主たる確認内容	審査員が主に確認する物
組織の状況	内外の課題、要求事項 事業環境の変化	● マネジメントレビュー/経営者インタビュー ● 法規制リストや許可証 ● 顧客及び外部供給者との契約書
情報セキュリティ方針、目的	達成の状況。今後の展開。	● マネジメントレビュー/経営者インタビュー ● 情報セキュリティ方針文書、情報セキュリティ目的に関する文書
適用範囲	現在の状況及び見直しの状況。	● 各プロセスの責任の所在に関する情報 ● オフィス等の図面や組織図など審査対象範囲を特定するための資料 ● 外部委託事業者との契約書面 ● オフィスやＩＴインフラの状況 ● ネットワーク構成を図示した資料

リスクアセスメントのプロセス及び結果	実施結果と見直しの状況	● リスクアセスメントの基準やリスクアセスメント結果記録
管理目的、管理策の導出状況	現在の状況及び見直しの状況	● 適用宣言書
リスク対応の状況	リスク対応計画とその進捗状況 採用管理策の運用状況	● リスク対応計画の結果 ● 詳細管理策をもとに計画したＩＳＭＳ文書の運用記録及び各種機器等の設定運用の状況
組織的/人的セキュリティ	運用結果の確認	● 組織要員及び関係する場合サービス提供を受ける外部供給者に対し実施される教育や契約、評価等の実施状況
事業継続マネジメントにおける情報セキュリティの側面	事業継続における要求事項の決定、手順の確立とその検証状況の確認	● 事業継続の計画文書及びそのテスト結果
ISMS のパフォーマンス及び有効性評価	ISMS のパフォーマンス及び有効性評価の為に特定した監視測定の方法と結果を確認	● 監視測定の対象とその評価方法 ● 監視測定の結果
内部監査	内部監査の計画と結果を確認	● 内部監査の計画状況とその実施記録
マネジメントレビュー	マネジメントレビューへの報告事項と評価結果、決定/指示事項の確認	● マネジメントレビュー記録 ● マネジメントレビューから出た決定/指示事項への対応状況
インシデント対応、セキュリティ違反/苦情への対応状況	インシデント発生状況と処置の実施状況の確認	● インシデントの発生実績及び処置の記録
不適合及び是正処置	発生した不適合の実績の確認と発生時の対応結果	● 不適合及び是正処置の記録

４．４　再認証審査　目的と方法

目　　的　： ● ISA 登録後の全期間の ISMS の運用実績、審査結果を踏まえ、続く有効期限まで、御社へ認証を継続して付与しうるかを評価する。 ● 情報セキュリティ方針、情報セキュリティ目的、手順に従って構築された ISMS が実施されていることを確認する。 ● 御社 ISMS が有効に機能し、情報セキュリティ目的を実現しつつあることを確認する。
実施方法と対象： ● 再認証審査では、過年度のサーベイランス審査報告書の内容、ISA からお客様へ行った照会への対応状況を踏まえ、現地審査で次の事項を含めて評価を進めます。 ➢ 組織内外の課題・要求事項の変化に対応し、継続して情報セキュリティ方針及び情報セキュリティ目的が確立されていること、認証の適用範囲が妥当であること ➢ ISMS 活動に対する積極的な関与により引き続きトップマネジメントのリーダーシップ及びコミットメントが実証されていること ➢ 情報セキュリティに関するリスクアセスメント及びリスク対応のプロセスが引き続き一貫性/妥当性があり、環境の変化に対応して適切な結果が生み出されていること ➢ ISMS のパフォーマンス及び有効性の評価が行われ、必要に応じ改善の為の対策がとられていること ➢ 過去３年間の内部監査活動の信頼性 ➢ 過去３年間に発生したインシデントや顧客苦情、不適合事項への対応状況 ➢ ISA からの指摘事項の処理状況
留　意　事　項　： ● 審査の結論は、審査員がクロージングミーティング終了時に通知いたします。 ● 審査で提示するマイナーな不適合は、審査完了日から登録有効期限日前に到来するＩＳＡの判定日前までにその完了をＩＳＡへ通知しなければなりません。改善が望ましい観察事項については、次回審査時にその対応状況を確認します。 ● メジャーな不適合については、再審査となります。検出した時点で審査は停止します。その後の対応方法については、ＩＳＡからご案内します。 ● 審査の結果、審査範囲の再確認、審査工数・費用再見積が必要となる場合があります。

確認項目	主たる確認内容	審査員が主に確認する物
組織の状況	内外の課題、要求事項 事業環境の変化	● マネジメントレビュー/経営者インタビュー ● 法規制リストや許可証 ● 顧客及び外部供給者との契約書
情報セキュリティ方針、目的	達成の状況。今後の展開。	● マネジメントレビュー/経営者インタビュー ● 情報セキュリティ方針文書、情報セキュリティ目的に関する文書
適用範囲	現在の状況及び見直しの状況。	● 各プロセスの責任の所在に関する情報 ● オフィス等の図面や組織図など審査対象範囲を特定するための資料 ● 外部委託事業者との契約書面 ● オフィスやＩＴインフラの状況

		● ネットワーク構成を図示した資料
リスクアセスメントのプロセス及び結果	実施結果と見直しの状況	● リスクアセスメントの基準やリスクアセスメント結果記録
管理目的、管理策の導出状況	現在の状況及び見直しの状況	● 適用宣言書
リスク対応の状況	リスク対応計画とその進捗状況 採用管理策の運用状況	● リスク対応計画の結果 ● 詳細管理策をもとに計画したＩＳＭＳ文書の運用記録及び各種機器等の設定運用の状況
組織的/人的セキュリティ	運用結果の確認	● 組織要員及び関係する場合サービス提供を受ける外部供給者に対し実施される教育や契約、評価等の実施状況
事業継続マネジメントにおける情報セキュリティの側面	事業継続における要求事項の決定、手順の確立とその検証状況の確認	● 事業継続の計画文書及びそのテスト結果
ISMS のパフォーマンス及び有効性評価	ISMS のパフォーマンス及び有効性評価の為に特定した監視測定の方法と結果を確認	● 監視測定の対象とその評価方法 ● 監視測定の結果
内部監査	内部監査の計画と結果を確認	● 内部監査の計画状況とその実施記録
マネジメントレビュー	マネジメントレビューへの報告事項と評価結果、決定/指示事項の確認	● マネジメントレビュー記録 ● マネジメントレビューから出た決定/指示事項への対応状況
インシデント対応、セキュリティ違反/苦情への対応状況	インシデント発生状況と処置の実施状況の確認	● インシデントの発生実績及び処置の記録
不適合及び是正処置	発生した不適合の実績の確認と発生時の対応結果	● 不適合及び是正処置の記録