【抜粋】ISO27001/ISO27017内部監査チェックリスト（附属書A管理策）

記入者	確認（承認）

https://www.iso-mi.com/

※有償にて、カスタマイズ可能なエクセルファイルで提供しています。上記のHPにてお問い合わせください。

総合評価結果は適合、不適合、観察事項とします。－は非該当もしくは今回の監査では確認しなかった事項
有効性評価については、管理策の目的を満たしているか、結果は出ているかを評価し、○、△、×で評価します。

規格項目	チェック内容	IS管理責任者	営業部門	技術部門	（システム管理責任者）管理部門	確認事項 *※記載はサンプル文面です。後で確認できる記載が好ましいです。*	有効性評価	総合評価結果	備考
A.5 情報セキュリティのための方針群 A.5.1 情報セキュリティのための経営陣の方向性 目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項、関連する法令及び規制に従って、規定するため。									
A.5.1.1 情報セキュリティのための方針群	「情報セキュリティ基本方針」を始めとする方針群を社長の承認を得て、発行し、全従業員及び関連する外部関係者に公表し、通知しているか	●				情報セキュリティ基本方針確認	―	適合	
	【CSC】 クラウドサービスの利用において、リスクを考慮して、クラウドサービス利用方針を作成し、社員に公開しているか	●				クラウドサービス利用方針確認	―	適合	
	【CSP】 クラウドサービス提供における方針を作成し、クラウドサービスカスタマに公開しているか	●				クラウドサービス情報セキュリティ方針を確認	―	適合	
A.5.1.2 情報セキュリティのための方針群のレビュー	レビュー実施のための手順は確立されているか	●				マネジメントレビューで見直す仕組みとしていた。	○	適合	
A.6 情報セキュリティのための組織 A.6.1 内部組織 目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。									
A.6.1.1 情報セキュリティの役割及び責任	情報セキュリティの責任を文書化して、具体的に明確にしてるか	●				「ISMSマニュアル」に明記	○	適合	
	【CSC】 クラウドサービスプロバイダと情報セキュリティの役割及び責任の適切な割当てについて合意し、それらの役割及び責任が遂行できることを確認し、その結果については、合意書（契約書や利用規約等）を取り交わしているか			●	●	Google Cloud利用規約確認	―	適合	
	【CSP】 クラウドサービスカスタマと情報セキュリティの役割及び責任の適切な割当てについて合意し、合意書（契約書や利用規約等）を取り交わしているか			●	●	利用規約（申込書）、○○クラウドセキュリティホワイトペーパー	―	適合	
A.6.1.2 職務の分離	不正使用の危険性を低減するために、職務を分離させるか、一つの職務権限に一人ではなく、複数の者を割り当てているか	●			●	対応確認	○	適合	
A.6.1.3 関係当局との連絡	具体的な連絡体制を確立しているか	●				WEBでのリンク等で明確化	○	適合	
	【CSC】 どのようにして、クラウドサービスに関連する省庁や団体、クラウドサービスの事業者団体を特定し、連絡体制を確立しているか			●	●	経済産業省、総務省、IPA等との連絡体制確認	―	適合	
	【CSP】 クラウドサービスカスタマに、自社の組織の所在地、カスタマデータを保存する可能性のある国を契約書や利用規約、自社WEB等を通じて、通知しているか			●	●	利用規約確認	―	適合	
A.6.1.4 専門組織との連絡	具体的な連絡体制を確立しているか	●				事例確認	○	適合	
A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ	プロジェクトマネジメントにおいても情報セキュリティの取り組みを行っているか	●				事例確認	○	適合	
A.6.2 モバイル機器及びテレワーキング 目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。									
A.6.2.1 モバイル機器の方針	モバイル機器の利用を行う場合の方針は定めているか	●			●	「ISMSマニュアル」に明記	○	適合	
A.6.2.2 テレワーキング	テレワーキングを行う場合のセキュリティ対策は定めているか	●			●	「ISMSマニュアル」に明記	○	適合	
A.6.3.1 クラウドコンピューティング環境における役割及び責任の共有及び分担	【CSC】 どのようにして、クラウドサービスの利用者にクラウドサービスの利用における自らの役割及び責任を意識させているか	●		●		「ISMSマニュアル」「ISMS管理策運用規定」の活用およびミーティングでの意識付け実施を確認	―	適合	
	【CSP】 クラウドサービスカスタマに、自らの情報セキュリティの能力、役割及び責任を契約書や利用規約等に文書化し、伝達しているか。また、クラウドサービスの利用の一部としてクラウドサービスカスタマが実施及び管理することが必要となる情報セキュリティの役割及び責任も伝達しているか		●	●		○○クラウドセキュリティホワイトペーパー等に明示。さらに「ISMSマニュアル」「ISMS管理策運用規定」の活用およびミーティングでの意識付け実施を確認	―	適合	
A.7 人的資源のセキュリティ A.7.1 雇用前 目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。									
A.7.1.1 選考	採用予定者が、情報セキュリティに関する必要な力量を備えていることの確認を行っているか				●	入社前面接にて確認	○	適合	

規格項目	チェック内容	ＩＳ管理責任者	営業部門	技術部門	（システム管理責任者）管理部門	確認事項 *※記載はサンプル文面です。後で確認できる記載が好ましいです。*	有効性評価	総合評価結果	備考
A.7.1.2 雇用条件	採用予定者に対して、「機密保持誓約書」に署名、提出させているか				●	誓約書確認	○	適合	
A.7.2 雇用期間中 目的：従業員及び契約相手が情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。									
A.7.2.1 経営陣の責任	すべての従業員及び契約相手に、当社の方針及び手順に従ったセキュリティの適用を要求しているか	●				誓約書にて明確化	○	適合	
A.7.2.2 情報セキュリティの意識向上、教育及び訓練	すべての従業員及に、自覚教育を実施しているか	●				「教育実施報告書」確認	○	適合	
	【CSC】 どのようにして、クラウドサービス利用における自覚教育、手順書教育を実施しているか			●	●	「教育実施報告書」確認	―	適合	
	【CSP】 クラウドサービスカスタマデータ及びクラウドサービス派生データを適切に取り扱うために、従業員に、意識向上、教育及び訓練を提供し、契約相手に同様のことを実施するよう要求しているか		●	●		「教育実施報告書」確認	―	適合	
A.7.2.3 懲戒手続	情報セキュリティ違反を犯した従業員に対して、懲戒規定に則り処罰しているか				●	規定はあるが、事例はなかっ	○	適合	
A.7.3 雇用の終了又は変更 目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。									
A.7.3.1 雇用の終了又は変更に関する責任	すべての従業員に対して、雇用の終了又は変更の実施に対する責任及び義務をを明確に定め、その対応を確実に行っているか				●	誓約書確認	○	適合	
A.8 資産の管理 A.8.1 資産に対する責任 目的：組織の資産を特定し、適切な保護の責任を定めるため。									
A.8.1.1 資産目録	適用範囲内における情報資産は、「情報資産台帳」において特定しているか	●	●	●	●	「情報資産台帳」確認	○	適合	
	【CSC】 「情報資産台帳」には、クラウドコンピューティング環境に保存される情報資産も記載しているか。また、クラウドサービスの特定など、情報資産を保持している場所も明確にしているか	●		●		「情報資産台帳」確認	―	適合	
	【CSP】 「情報資産台帳」には、クラウドサービスカスタマデータ（契約情報等）及びクラウドサービス派生データ（ログデータ、設定情報等）を明確に識別しているか	●		●		「情報資産台帳」には、クラウドサービスにおける派生データが明確でなかった	―	観察	
A.8.1.2 資産の管理責任	資産の管理責任者は、「情報資産台帳」にて明示している	●	●	●	●	「情報資産台帳」確認	○	適合	
A.8.1.3 資産利用の許容範囲	資産利用の許容範囲は、「情報資産台帳」にて明示しているか	●	●	●	●	「情報資産台帳」確認	○	適合	
A.8.1.4 資産の返却	雇用、契約の終了時に、該当する従業員又は外部利用者から、社員証、社用名刺、施設入退室カード、貸与PC、携帯電話をはじめ、貸与した情報資産の返却を確実に行っているか				●	事例確認	○	適合	
A.8.1.5 クラウドサービスカスタマの資産の除去	【CSC】 クラウドサービスプロバイダに対して、その資産の返却及び除去、並びにこれらの資産の全ての複製のクラウドサービスプロバイダのシステムからの削除の記述を含む、サービスプロセスの終了に関する文書を入手しているか			●	●	規約確認。終了後の情報資産の取り扱いを確認	―	適合	
	【CSP】 クラウドサービスカスタマに対して、クラウドサービス利用のための合意の終了時における、全ての資産の返却及び除去の取決めについて、情報を提供しているか。また、資産の返却及び除去についての取決めは、合意文書の中に記載し、予定通りに実施し、その取決めでは返却及び除去する資産を特定しているか		●	●		利用規約、〇〇クラウドセキュリティホワイトペーパーに明示	―	適合	
A.16 情報セキュリティインシデント管理 A.16.1 情報セキュリティインシデントの管理及びその改善 目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取り組みを確実にするため。									
A.16.1.1 責任及び手順	情報セキュリティインシデントが発生した場合の手順と責任は明確か	●				「ISMS管理策運用規定」に明記	○	適合	
	【CSC】 クラウドサービスにおける情報セキュリティインシデントが発生した場合の手順と責任は明確か	●		●	●	「ISMS管理策運用規定」に明記	―	適合	
	【CSP】 クラウドサービスカスタマとの間で、情報セキュリティインシデント管理に関する責任の割当て及び手順をサービス仕様の一部として定めているか			●	●	「ISMS管理策運用規定」、〇〇クラウドセキュリティホワイトペーパーに明記	―	適合	
A.16.1.2 情報セキュリティ事象の報告	社員は、セキュリティの弱点や脅威に気づいた場合、ISMS事務局へ報告しているか	●			●	メール等で報告	○	適合	
	【CSC】 社員は、クラウドサービスにおけるセキュリティの弱点や脅威に気づいた場合、管理責任者へ報告しているか			●	●	メール等で報告	―	適合	
	【CSP】 クラウドサービスカスタマとの間で、情報セキュリティ事象を当社に報告するなどの仕組みを確立しているか			●	●	メール等で報告	―	適合	
A.16.1.3 情報セキュリティ弱点の報告	システム管理責任者は、情報セキュリティ弱点に関する、利用者への周知を、社内回覧またはメールで行っているか				●	メール確認	○	適合	
A.16.1.4 情報セキュリティ事象の評価及び決定	システム管理責任者は、情報セキュリティ事象の評価及び決定を行い、その結果および指示事項を社内に伝達しているか	●			●	メール確認	○	適合	
A.16.1.5 情報セキュリティインシデントへの対応	情報セキュリティインシデントへの対応手順は明確か	●			●	メール確認	○	適合	
A.16.1.6 情報セキュリティインシデントからの学習	情報セキュリティインシデントから得られた情報は、再発防止のための社員教育に役立てているか	●			●	メール確認	○	適合	
A.16.1.7 証拠の収集	セキュリティインシデントの結果、法的処置がとられる可能性があると判断した場合は、記録、証拠を保全する手順があるか				●	「ISMS管理策運用規定」に明記	○	適合	

規格項目	チェック内容	ＩＳ管理責任者	営業部門	技術部門	（システム管理責任者）管理部門	確認事項 *※記載はサンプル文面です。後で確認できる記載が好ましいです。*	有効性評価	総合評価結果	備考
	【CSC】【CSP】共通 クラウドサービスにおけるセキュリティインシデントの結果、法的処置がとられる可能性があると判断した場合は、記録、証拠を保全する手順があるか	●		●		「ISMS管理策運用規定」に明記	―	適合	
A.17 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									
A.17.1 情報セキュリティ継続 目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。									
A.17.1.1 情報セキュリティ継続の計画	困難な状況（災害もしくは大事故時など）においても、情報セキュリティ及び情報セキュリティマネジメントを適切に維持管理できるように、組織で行うべきことは明確か	●			●	「ISMS管理策運用規定」に明記	○	適合	
A.17.1.2 情報セキュリティ継続の実施	「事業継続計画書」を作成し、社長の承認を得ているか	●			●	「事業継続計画書」確認	○	適合	
A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価	「事業継続計画書」を検証し、評価しているか	●			●	「事業継続計画書」確認	○	適合	
A.17.2 冗長性 目的：情報処理施設の可用性を確実にするため。									
A.17.2.1 情報処理施設の可用性	十分な冗長性を持って、情報処理施設の可用性を保つようにしているか				●	現場確認	○	適合	
A.18 順守 A.18.1 法的及び契約上の要求事項の順守 目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。									
A.18.1.1 適用法令及び契約上の要求事項の特定	「法的要求事項登録簿」の見直し及びその周知を図っているか	●				「法的要求事項登録簿」確認。	○	適合	
	【CSC】 クラウドサービスにおける「法的要求事項登録簿」の見直し及びその周知を図っているか	●				「法的要求事項登録簿」確認。	―	適合	
	【CSP】 クラウドサービスカスタマに対して、クラウドサービスに適用される法域を契約書や利用規約等において、特定し、情報提供しているか。また、適用法令及び契約上の要求事項については、自社の現在の順守の証拠をクラウドサービスカスタマに提供しているか	●		●		○○クラウドセキュリティホワイトペーパーに明記	―	適合	
A.18.1.2 知的財産権	著作権の侵害等、知的財産権の重要性について教育を行っているか		●	●	●	「教育実施報告書」確認	○	適合	
	【CSC】 該当する場合、クラウドサービスにおける著作権の侵害等、知的財産権の重要性について教育を行っているか		●	●	●	必要に応じて、メール等での周知実施	―	適合	
	【CSP】 クラウドサービスカスタマに対して、ライセンス条項等の知的財産権の侵害の苦情（相談）に対しては、問い合わせの窓口を示し、対応を図っているか。		●	●	●	メール・窓口の周知	―	適合	
A.18.1.3 記録の保護	ログや運用記録等、セキュリティに関係する重要な記録は消失、破壊、改ざんがないように管理しているか			●	●	ヒアリング確認	―	適合	
	【CSC】 クラウドサービスプロバイダが収集し、保存する記録の保護（保管）に関する情報をクラウドサービスプロバイダに要求できるか			●	●	規約確認	―	適合	
	【CSP】 クラウドサービスカスタマによるクラウドサービスの利用に関連して、自社が収集し、保存する記録の保護（保管）に関する情報をクラウドサービスカスタマに提供しているか			●	●	○○クラウドセキュリティホワイトペーパーに明記	―	適合	
A.18.1.4 プライバシー及び個人を特定できる情報の保護	個人情報保護法や関連する各種ガイドライン等を順守しているか				●	現場確認	○	適合	
A.18.1.5 暗号化機能に対する規制	暗号機能の関連する協定、法令及び規制を認識している			●	●	ヒアリング確認	○	適合	
	【CSC】 システム管理責任者は、クラウドサービスの利用に適用する暗号による管理策群が、外国為替及び外国貿易法等の法令及び規制を順守していること確認しているか			●	●	法が適用されず、問題ないことを確認	―	適合	
	【CSP】 外国為替及び外国貿易法等の法令及び規制の順守をクラウドサービスカスタマがレビューするために、実施している暗号による管理策の記載を自社WEB等にて、その情報を提供しているか			●	●	○○クラウドセキュリティホワイトペーパーに明記	―	適合	
A.18.2 情報セキュリティのレビュー 目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。									
A.18.2.1 情報セキュリティの独立したレビュー	情報セキュリティのための管理目的、管理策、方針、プロセス、手順について見直しを行っているか	●		●	●	ミーテイングで検証を行っていた	―	適合	
	【CSC】 クラウドサービスプロバイダが、クラウドサービスのための情報セキュリティ管理策及び指針の実施状況（サービス提供状況）がクラウドサービスプロバイダの提示どおりであることについて確認しているか	●		●	●	クラウドサービスプロバイダのISO27017認証を確認	―	適合	
	【CSP】 自社が約束する情報セキュリティ管理策の実施を立証するために、クラウドサービスカスタマに文書化した証拠（外部の審査機関による認証証等）を自社WEB等にて、提供しているか	●		●	●	○○クラウドセキュリティホワイトペーパーに明記	―	適合	
A.18.2.2 情報セキュリティのための方針群及び標準の順守	情報セキュリティ方針及び関連する手順書の順守を達成するために、すべてのセキュリティ手順が正しく実行されているか			●	●	現場確認	○	適合	
A.18.2.3 技術的順守のレビュー	情報システムが、当社の定めたセキュリティ基準に従って順守されているかどうか、定めに従って点検を行っているか			●	●	現場確認	○	適合	