【抜粋】ISO27001/ISO27017内部監査チェックリスト（規格本文）

記入者	確認（承認）

－は非該当もしくは今回の監査では確認しなかった事項　　評価結果は適合、不適合、観察事項とします。 ●は被監査対象

規格項目		チェック内容		確認する文書・記録 *※記載はサンプル文面です。自社で該当する文書、記録の記入が必要です。*	IS管理責任者	営業部門	技術部門	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。*	評価結果	備考
4 組織の状況	4.1 組織及びその状況の理解	確認事項	クラウドサービスに関わる外部及び内部の課題を決定し、明確化しているか	「リスク一覧表」	●				「リスク一覧表」で明確にしていた。	適合	
	4.2 利害関係者のニーズ及び期待の理解	確認事項	クラウドサービスに関わる以下の事項を決定し、明確化しているか 1) ISMSに関連する利害関係者 2) 利害関係者の、情報セキュリティに関連する要求事項	「リスク一覧表」 顧客との契約書等	●				顧客より、CSPとしてのISO27017取得の要請があった。	適合	
	4.3 情報セキュリティマネジメントシステム（ISMS）の適用範囲の決定	確認事項	クラウドサービスに関わる以下の事項を考慮して適用範囲を決めているか 1) 4.1に規定する外部及び内部の課題 2) 4.2に規定する要求事項 3) 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	「ISMSマニュアル」（2021.00.00改訂版）	●				クラウドカスタマとしての適用として、具体的なクラウドサービス名を特定していた。	適合	
	4.4 情報セキュリティマネジメントシステム	確認事項	ISO27001:2013及びISO27017:2015の要求事項に従って、情報セキュリティマネジメントシステム（ISMS）を確立し、実施し、維持し、かつ継続的に改善を行う仕組みになっているか	「ISMSマニュアル」（2021.00.00改訂版）	●				ISO27017:2015のCSP要求事項は特定し、それに基づきルール化されていた。	適合	
5 リーダーシップ	5.1 リーダーシップ及びコミットメント	確認事項	経営層は以下の事項を実施しているか 1) 情報セキュリティ方針及び情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする。 2) 組織の事業プロセスへの情報セキュリティマネジメントシステム（ISMS）要求事項への統合を確実にする。 3) 情報セキュリティマネジメントシステム（ISMS）に必要な経営資源が利用可能であることを確実にする。 4) 有効な情報セキュリティマネジメント及び情報セキュリティマネジメントシステム（ISMS）要求事項への適合の重要性を伝達する。 5) 情報セキュリティマネジメントシステム（ISMS）がその意図した成果を達成することを確実にする。 6) 情報セキュリティマネジメントシステム（ISMS）の有効性に寄与するよう社員を指揮し、支援する。 7) 継続的な改善を促進する。 8) その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、その管理層の役割を支援する。	「ISMSマニュアル」（2021.00.00改訂版） 「マネジメントレビュー議事録」	●				経営理念に基づき、それを展開していた。	適合	
	5.2 方針	確認事項	情報セキュリティ方針は以下の事項を満たしているか 1) 組織の目的に対して適切である。 2) 情報セキュリティ目的を含むか又は情報セキュリティ目的の設定のための枠組みを示す。 3) 情報セキュリティに関連して適用される要求事項を満たすことへのコミットメントを含む。 4) 情報セキュリティマネジメントシステム（ISMS）の継続的改善へのコミットメントを含む。 5) 文書化した情報として利用可能である。 6) 組織内に伝達する。 7) 必要に応じて、利害関係者が入手可能である。	「情報セキュリティ方針」	●				変更はなかった。	適合	
	5.3 組織の役割、責任及び権限	確認事項	経営層は以下の事項を実施しているか 1) 構築した仕組みが、ISOの規格要求を満たすことを確実にする。 2) ISMSのパフォーマンスの状況が経営層に報告されることを確実にする。	「ISMSマニュアル」（2021.00.00改訂版） 「マネジメントレビュー議事録」	●				年度方針の発表の中で明確化されていた	適合	
6 計画	6.1 リスク及び機会に対処する活動 6.1.1 一般	確認事項	クラウドサービスに関わるISMSの計画を策定するとき、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、次の事項について対処する必要があるリスク及び機会を決定しているか 1)ISMSが、その意図した成果を達成できることを確実にする。 2)望ましくない影響を防止、又は低減する。 3)継続的改善を達成する。 4)決定したリスク及び機会に対処する活動を計画する。 5)計画された活動は、ISMSプロセスへの統合及び実施を行う。 6)計画された活動の有効性評価を行う。	「ISMSマニュアル」（2020.06.01改訂版） 「リスク一覧表」	●				年度方針の発表の中で明確化されていた	適合	
	6.1.2 情報セキュリティリスクアセスメント	a）確認事項	以下を含む基準を確立しているか 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	「ISMSマニュアル」（2020.06.01改訂版） 「リスクアセスメント結果表」	●				適切に策定されていた。	適合	
		b）確認事項	リスクアセスメントは、一貫性や妥当性があり、比較可能な結果を生み出すことを確実にしているか	「ISMSマニュアル」（2021.00.00改訂版） 「リスクアセスメント結果表」	●				適切に策定されていた。	適合	

		c)確認事項	以下を含んでクラウドサービスに関わる情報セキュリティリスクを特定しているか 1)機密性、完全性、可用性の喪失に伴うリスクを特定しているか 2)リスク所有者を特定しているか	「ISMSマニュアル」（2021.00.00改訂版） 「リスクアセスメント結果表」		●	●	●	「リスクアセスメント結果表」において、クラウドサービスの提供が明確化されていた	適合	
		d)確認事項	以下を含んでクラウドサービスに関わるリスク分析をしているか 1)実際に起こり得る結果についてアセスメントているか 2)リスクの現実的な起こりやすさについてアセスメントしているか 3)リスクレベルを決定しているか	「ISMSマニュアル」（2021.00.00改訂版） 「リスクアセスメント結果表」		●	●	●	クラウドサービスプロバイダとしてのリスクも分析されていた。	適合	
		e)確認事項	以下を含んでクラウドサービスに関わるリスク評価をしているか 1)リスク分析の結果、受容基準を評価しているか 2)リスクの優先順位付けを行っているか	「ISMSマニュアル」（2021.00.00改訂版） 「リスクアセスメント結果表」		●	●	●	「リスクアセスメント結果表」に受容基準、点数にての優先順位は明確化されていた。	適合	
8 運用	8.1 運用の計画及び管理	確認事項	クラウドサービスを含めた情報セキュリティ要求事項を満たすため、6.1で決定した活動及び6.2で決定した情報セキュリティ目的の達成を実施するために必要なプロセスを計画し、実施、管理を行っているか。また、プロセスが計画通りに実施されたという文書化した情報はあるか	「ISMSマニュアル」（2021.00.00改訂版） 「リスク対応計画書」 「情報セキュリティ目的目標管理表」	●		●		日頃のミーティング等で適切な運用が図られていた。メール等確認	適合	
		確認事項	計画した変更を管理しているか。有害な影響を軽減する措置及び外部に委託したプロセスの管理は適切に行っているか	「リスクアセスメント結果表」 「リスク対応計画書」 「ISMS管理策運用手順書」		●	●	●	日頃のミーティング等で適切な運用が図られていた。メール等確認	適合	
	8.2 情報セキュリティリスクアセスメント	確認事項	あらかじめ定めた間隔で、リスクアセスメントの見直しを実施しているか	「リスクアセスメント結果表」		●	●	●	見直しの仕組みは策定されていた。	適合	
	8.3 情報セキュリティリスク対応	確認事項	情報セキュリティリスク対応計画は、進捗状況をチェックして、記録し、計画に遅延または障害が生じた場合は、実施責任者と対応を協議しているか	「リスクアセスメント結果表」		●	●	●	日頃のミーティング等で適切な運用が図られていた。メール等確認	適合	
9 パフォーマンス評価	9.1 監視、測定、分析及び評価	確認事項	以下の事項を決定し、監視及び測定の結果の証拠として、文書化した情報を保持しているか 1) 必要とされる監視及び測定の対象。これには、情報セキュリティプロセス及び管理策を含む 2) 該当する場合には、必ず、妥当な結果を確実にするための、監視、測定、分析及び評価の方法 3) 監視及び測定の実施時期 4) 監視及び測定の実施者 5) 監視及び測定の結果の、分析及び評価の時期 6) 監視及び測定の結果の、分析及び評価の実施者	メール 「管理策測定評価表」	●	●	●	●	メールでの報告内容を確認。情報セキュリティにおける事件・事故はなかった。	適合	
	9.2 内部監査	a)確認事項	以下の事項に適合しているか 1) 組織自体が規定した要求事項 2) ISO27001:2013の要求事項 3) ISO27017:2015の要求事項	内部監査記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		b)確認事項	あらかじめ定められた間隔で、有効に実施され、維持されているか	内部監査記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		c)確認事項	以下が実施されているか 1) 監査計画があるか 2) 監査計画は適切で、漏れがないか 3) 前回までの監査結果を考慮しているか	内部監査記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		d)確認事項	監査基準及び監査範囲は明確か	内部監査記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		e)確認事項	1) 監査員の選定は適切か（資格、教育記録を確認） 2) 監査員は自分の仕事を監査していないか	内部監査記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		f)確認事項	監査結果は、確実に、経営層に報告されるか	内部監査記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		g)確認事項	監査結果を、文書化した情報として保持しているか	内部監査記録	●				昨年度のものを確認。適切に実施されていた。	適合	
	9.3 マネジメントレビュー	確認事項	マネジメントレビューが定められた間隔（少なくとも年1回）で実施されているか	マネジメントレビュー記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		a)確認事項	前回までのマネジメントレビューの結果とった処置は適切か	マネジメントレビュー記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		b)確認事項	外部及び内部の課題は、考慮しているか	マネジメントレビュー記録	●				昨年度のものを確認。適切に実施されていた。	適合	
		c)確認事項	以下の事項を考慮しているか 1)不適合及び是正処置 2)監視及び測定の結果 3)監査結果 4)情報セキュリティ目的の達成 5)利害関係者（顧客等）からのフィードバック 6)リスクアセスメントの結果及びリスク対応計画の状況 7)継続的改善の機会	マネジメントレビュー記録	●				昨年度のものを確認。適切に実施されていた。	適合	

		確認事項	アウトプットは以下の事項を考慮しているか 1)継続的な改善の機会 2)変更の必要性	マネジメントレビュー記録	●				昨年度のものを確認。適切に実施されていた。	適合	
10 改善	10.1 不適合及び是正処置	a)確認事項	不適合に該当する場合には、以下の事項を行っているか 1)その不適合を管理し、修正するための処置をとる 2)その不適合によって起こった結果に対処する	「是正処置計画」(審査機関様式) メール	●		●		外部審査機関が出した是正処置の対応確認	適合	
		b)確認事項	不適合に該当する場合には、以下の事項を行っているか 1)その不適合のレビュー 2)その不適合の原因の明確化 3)類似の不適合の有無又はそれが発生する可能性の明確化	「是正処置計画」(審査機関様式)メール	●		●		外部審査機関が出した是正処置の対応確認	適合	
		c)確認事項	必要な処置を実施しているか	「是正処置計画」(審査機関様式) メール	●		●		外部審査機関が出した是正処置の対応確認	適合	
		d)確認事項	是正処置の有効性をレビューしているか	「是正処置計画」(審査機関様式) メール	●		●		外部審査機関が出した是正処置の対応確認	適合	
		e)確認事項	必要な場合は、ISMSの変更を行っているか	「是正処置計画」(審査機関様式) メール	●		●		外部審査機関が出した是正処置の対応確認	適合	
		f)確認事項	不適合の性質及びとった処置は、記録しているか	「是正処置計画」(審査機関様式) メール	●		●		システム管理責任者が行う処置やその記録が一部確認できなかった。	観察	
		g)確認事項	是正処置の結果は、記録しているか	「是正処置計画」(審査機関様式) メール	●		●		外部審査機関が出した是正処置の対応確認	適合	
	10.2 継続的改善	確認事項	ISMSの適切性、妥当性及び有効性を継続的に改善しているか	「各種議事録」 メール	●		●		適切に実施されていた。	適合	