審査報告書

受審企業／組織体情報：

企業／組織体名	エアーズ株式会社
所在地	［浜松オフィス］静岡県浜松市中央区砂山町 323-16 ヴェルメゾン浜松 2F–5
トップマネジメント	加藤　匡邦　様
管理責任者	鈴木　謙吾　様

審査情報：

審査実施日	2025 年 11 月 27 日～2025 年 11 月 28 日
チームリーダー名	山本　史夫

登録番号	適用規格（審査基準）	審査種別
50301747ISMS22	ISO/IEC 27001:2022 ISO/IEC 27001:2022/Amd.1:2024	登録審査 Stage2

※ 「審査基準」には、適用規格に基づき受審企業／組織体が定めた手順が含まれます。
※ 審査報告書は、「DQS 審査・認証規則」に従い、機密保持されます。
尚、審査報告書の写しが受審企業／組織体より外部に配付される場合、全ての頁が含まれていなければなりません。

1.審査概要

1.1 目的
☒ : マネジメントシステムの継続的適合性、有効性、認証範囲の適切性を評価する。（更新審査/登録審査）
☐ : マネジメントシステムの継続的適合性を評価する。（継続審査）
☐ : 申告された変化点に関する事項を評価する。（特別審査）

1.2 審査の実施範囲: 審査計画書を参照

1.3 基本情報・変化点

BR No. / 登録証番号	**50301747ISMS22**	
Customer Name / 組織名称	☒:変更無	エアーズ株式会社
	☐:変更有	
Scope / 登録範囲	☒:変更無	エアーズ株式会社における情報セキュリティマネジメントシステム
	☐:変更有	
Business Description / 対象事業	☒:変更無	・ソフトウェア開発事業 ・ソフトウェア保守運用事業 ・ソフトウェア開発コンサルティング業
	☐:変更有	
SOA / 適用宣言書	☒:変更無	適用宣言書 Ver.2025.10.03.01 (日付: 2025.10.10)
	☐:変更有	適用管理策の拡大/縮小： ☐:有 / ☐:無
要員数 / Employee Count	3 名	
登録拠点 / Location	☒:変更無	浜松オフィス(新規登録)
	☐:変更有	

1.4 審査対象期間
☒ : 運用開始から登録審査 Stage2 審査までの活動期間
☐ : 前回の更新(登録)から今回の更新評価までの約３年間
☐ : 前回の審査から今回の継続審査までの約１年間
☐ : 変化点に関する活動期間

1.5 審査チーム
チームリーダー：山本　史夫（ISO/IEC 27001 主任審査員）

1.6 審査工数
合計：2.0 人日 [文書審査：0.5 人日、現地審査(リモート審査)：1.5 人日]

2．審査結果

2.1 審査の結論

☒：不適合の指摘はなく、登録証の発行/維持/更新を推薦します。
□：指摘事項に対する是正処置回答に問題ないことを前提に、登録証の発行/維持/更新を推薦します。
□：指摘事項に対する是正処置回答を提示頂いた後、フォローアップ審査を実施します。
□：マネジメントシステムの構築・運用が不充分である為、登録証の不発行/一時停止を推薦します。

※ 審査結果はサンプリング確認に基づいています。その為、不確実性が残ることをご了解下さい。
※ 本報告書の記載事項以外に不適合が存在しないことを保証するものではありません。

2.2 登録証記載事項に関する結論

登録証記載事項に対し判断した結論は以下の通りです。
☒：登録証の記載事項は適切と判断しました。
□：登録証の記載事項に実態との不一致が確認されました。記載事項の変更を推薦致します。

3．審査所見

3.0 総合所見

ソフトウェアの開発、ソフトウェア保守運用、ソフトウェア開発コンサルティングの事業活動において、2025年7月からISMS運用管理クラウドサービス(SecureNavi)を使用した準備を開始し、情報セキュリティマニュアル/適用宣言書/社内ルール/各種規程類の整備を完了され、2025年9月の浜松オフィス開設後から運用を始めております。

内外の課題、利害関係者のニーズ及び期待の特定、リスクアセスメントが実施されています。内外の課題とリスクアセスメントの結果から、リスク対応と目標管理の計画が策定され、リスク対応、目標管理、要員教育が実施されています。内部監査・マネジメントレビューでそれらの有効性を監視・分析・評価されていることを確認できました。内部監査では、6件の不適合が検出されていましたが、是正処置プロセスに従い処置されています。

Stage1審査で観察された1件の懸念事項は、規格に適合していることを確認できました。

以上のことから組織のISMSは適切に構築・運用されていると評価します。

内部監査で検出された不適合とマネジメントレビューの結果に対処することで、より堅固なマネジメントシステムになると期待されます。

3.1 不適合(指摘事項)

☒：今回の審査においては発見されませんでした。
□：別紙(Action Plan)を参照下さい。[重大な不適合：0件、軽微な不適合：0件]

3.2 観察された事象

【良好な側面】

No.	サイト/部門	条項番号	内容
1	ISMS委員会	箇条7.2	社内ルールは、「情報セキュリティマニュアル」として文書化されていました。社内ルールの理解を深めるために、ISMS活動の役割毎に分類・詳細化した「情報セキュリティ管理規程」と「従業員向け基本規程」を作成し、追加教育としてこれらの規程の読み合せと確認テストが実施されていました。統一ルールへの認識をより確実にするための処置として評価できます。

3.3 運用状況の評価

3.3.1 気候変動リスクに関する取組みについて

利害関係者からの要求はなく、自社を取巻く状況から、現時点では取り組むべき気候変動リスクはないと評価されていました。

3.3.2 マネジメントシステムの目標への対応状況

☒：目標の確立、計画及び実施において、不適合は発見されませんでした。
☐：目標の確立、計画及び実施において、不適合が発見されました。詳細は 3.1 項を参照下さい。

3.3.3 苦情への対応状況

☒：苦情への対応に不適合は発見されませんでした。
☐：苦情への対応に不適合が発見されました。詳細は 3.1 項を参照下さい。

運用開始から登録審査 Stage2 審査までの活動期間で 1 件の情報セキュリティインシデントが報告されていました。これは事業継続計画の試験中に発見された準備物の不備に関するものです。是正処置プロセスによる処置が必要と判断され、インシデントとして報告されていました。そのため、利害関係者からの苦情やフィードバックを伴うものではありませんでした。
その他に利害関係者からの苦情やフィードバックの実績はありません。

3.3.4 法令・規制要求事項への対応状況

☒：法令・規制要求事項の順守プロセス及びその運用に不適合は発見されませんでした。
☐：法令・規制要求事項を順守プロセス及びその運用に不適合が発見されました。詳細は 3.1 項を参照下さい。

個人情報保護法、著作権法、 不正アクセス禁止法など

3.3.5 内部監査の状況

☒：組織の内部監査の以下事項において、不適合は発見されませんでした。
・組織の内部監査プログラムが計画されていました。
・組織の内部監査プログラムに従って実施されていました。
・不適合が発生していた場合、必要な処置が計画若しくは実施されていました。
☐：組織の内部監査において、不適合が発見されました。詳細は 3.1 項を参照下さい。

3.3.6 マネジメントレビューの状況

☒：組織のマネジメントレビューの以下事項において、不適合は発見されませんでした。
・予め定めた間隔でマネジメントレビューが実施されていました。
・必要な情報がインプット若しくは考慮がされていました。
・アウトプットに対して、必要な処置が計画若しくは実施されていました。
☐：組織のマネジメントレビューに、不適合が発見されました。詳細は 3.1 項を参照下さい。

3.3.7 登録の公表及び登録マークの使用について

公表／使用の有無　：　☐：有　　☒：無
公表／使用の適切性：　☒：適切　　☐：不適切
確認対象物： 初回登録審査のため、審査時点では登録マークは未使用です。

3.3.8 前回指摘事項のフォローアップ
☒ : 初回登録審査につき、該当はありません。
☐ : 前回の審査においては、不適合は発見されていません。
☐ : 前回指摘事項は効果的に是正されていることを確認しました。
☐ : 前回指摘事項の是正状況に、不適合が発見されました。詳細は 3.1 項を参照下さい。

3.3.9 適用除外管理策/追加管理策およびその根拠
☒ : 情報セキュリティリスクアセスメント、リスク対応の結果に基づき適切でした。
☐ : 以下の管理策の適用除外の理由は正当でなく改善指摘事項に記述しました。
・除外管理策の項目： 適用宣言書 Ver.2025.10.03.01 (日付: 2025.10.10)による
・追加管理策の内容： --

3.3.10 訪問したテンポラリーサイトに関する情報

N/A

3.4 マネジメントシステムにおける変更の確認
☒ : マネジメントシステムの運用に大きな影響はなく、適切と判断しました。
☐ : 下記変化点の確認において、不適合は発見されませんでした。
☐ : 下記変化点の確認において、不適合が発見されました。詳細は 3.1 項を参照下さい。

特記事項なし

4.その他
4.1 次回の審査予定/工数
審査実施の約 3 ヶ月前に DQS 事務所より日程調整をご案内させて頂きます。

	継続審査 1 回目 (2026 年)	継続審査 2 回目 (2027 年)	更新審査 (2028 年)
現地審査工数	1.0 PD	1.0 PD	1.5 PD
文書審査工数	0.5 PD	0.5 PD	0.5 PD

※ 上表の審査工数は登録範囲・要員数が現行と同等とを前提としています。変更点が生じた場合は改めて工数を算出させて頂きます。

4.2 受領文書
☒ : 事前資料 (マニュアル、適用宣言書、組織図)
☒ : オープニング／クロージングミーティングの出席簿
☐ : その他（）
※ 受領した文書は、認証判定等のために使用させて頂きます。
※ 受領したもの以外のお借りした文書（許可を頂いてコピーしたものや電子ファイルを含む）は、審査最終日に返却若しくは作業終了後に責任を持って消却・消去致します。

4.3 苦情及び異議申し立て
重大な不適合事項を含む登録証一時停止/取消などの審査結論に対して、又は、審査チームの見解に同意できない場合には、弊社代表取締役宛に貴社の代表取締役名の文書にて異議申し立てを行う権利がございます。
[連絡先]：iso.jp@dqs.de

4.4 審査の実施方法，有効性に関する記述
☐：本審査は Onsite で実施されました。
☐：物理的拠点を持たない組織の為、本審査は遠隔審査技法を適用しました。
☒：リスク評価に基づき、本審査の一部(全て)に遠隔審査技法を適用しました。
[有効性]
☒：審査は有効に実施され、審査目的は達成されました。
☐：審査の実施に支障が生じた為、審査計画を下記の通り、修正しました。

4.5 その他，特記事項
☒：特にありません。
☐：その他：

5.審査概要

ISO/IEC 27001:2022 要求項目 / 各審査で発見された改善指摘事項の件数		審査サイクル			指摘事項識別番号 その他
		初回登録	継続 1	継続 2	
4.1	組織及びその状況の理解	0			
4.2	利害関係者のニーズ及び期待の理解	0			
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	0			
4.4	情報セキュリティマネジメントシステム	0			
5.1	リーダーシップ及びコミットメント	0			
5.2	方針	0			
5.3	組織の役割，責任及び権限	0			
6.1	リスク及び機会に対処する活動	0			
6.2	情報セキュリティ目的及びそれを達成するための計画策定	0			
6.3	変更の計画策定	0			
7.1	資源	0			
7.2	力量	0			
7.3	認識	0			
7.4	コミュニケーション	0			
7.5	文書化した情報	0			
8.1	運用の計画策定及び管理	0			
8.2	情報セキュリティリスクアセスメント	0			
8.3	情報セキュリティリスク対応	0			
9.1	監視，測定，分析及び評価	0			
9.2	内部監査	0			
9.3	マネジメントレビュー	0			
10.1	継続的改善	0			
10.2	不適合及び是正処置	0			
附属書 A 管理策					
5.1	情報セキュリティのための方針群	0			
5.2	情報セキュリティの役割及び責任	0			
5.3	職務の分離	0			
5.4	経営陣の責任	0			
5.5	関係当局との連絡	0			
5.6	専門組織との連絡	0			
5.7	脅威インテリジェンス	0			
5.8	プロジェクトマネジメントにおける情報セキュリティ	0			
5.9	情報及びその他の関連資産の目録	0			
5.10	情報及びその他の関連資産の許容される利用	0			
5.11	資産の返却	0			
5.12	情報の分類	0			
5.13	情報のラベル付け	0			
5.14	情報の転送	0			
5.15	アクセス制御	0			
5.16	識別情報の管理	0			
5.17	認証情報	0			
5.18	アクセス権	0			
5.19	供給者関係における情報セキュリティ	0			
5.20	供給者との合意における情報セキュリティの取扱い	0			
5.21	情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理	0			
5.22	供給者のサービス提供の監視、レビュー及び変更管理	0			
5.23	クラウドサービスの利用における情報セキュリティ	0			
5.24	情報セキュリティインシデント管理の計画策定及び準備	0			
5.25	情報セキュリティ事象の評価及び決定	0			
5.26	情報セキュリティインシデントへの対応	0			
5.27	情報セキュリティインシデントからの学習	0			
5.28	証拠の収集	0			
5.29	事業の中断・阻害時の情報セキュリティ	0			
5.30	事業継続のための ICT の備え	0			
5.31	法令、規制及び契約上の要求事項	0			
5.32	知的財産権	0			
5.33	記録の保護	0			
5.34	プライバシー及び個人を特定できる情報(PII)の保護	0			
5.35	情報セキュリティの独立したレビュー	0			
5.36	情報セキュリティのための方針群、規則及び標準の順守	0			
5.37	操作手順書	0			

6.1	選考	0			
6.2	雇用条件	0			
6.3	情報セキュリティの意識向上、教育及び訓練	0			
6.4	懲戒手続	0			
6.5	雇用の終了又は変更後の責任	0			
6.6	秘密保持契約又は守秘義務契約	0			
6.7	リモートワーク	0			
6.8	情報セキュリティ事象の報告	0			
7.1	物理的セキュリティ境界	0			
7.2	物理的入退	0			
7.3	オフィス、部屋及び施設のセキュリティ	0			
7.4	物理的セキュリティの監視	0			
7.5	物理的及び環境的脅威からの保護	0			
7.6	セキュリティを保つべき領域での作業	0			
7.7	クリアデスク・クリアスクリーン	0			
7.8	装置の設置及び保護	0			
7.9	構外にある資産のセキュリティ	0			
7.10	記憶媒体	0			
7.11	サポートユーティリティ	0			
7.12	ケーブル配線のセキュリティ	0			
7.13	装置の保守	0			
7.14	装置のセキュリティを保った処分又は再利用	0			
8.1	利用者エンドポイント機器	0			
8.2	特権的アクセス権	0			
8.3	情報へのアクセス制限	0			
8.4	ソースコードへのアクセス	0			
8.5	セキュリティを保った認証	0			
8.6	容量・能力の管理	0			
8.7	マルウェアに対する保護	0			
8.8	技術的ぜい弱性の管理	0			
8.9	構成管理	0			
8.10	情報の削除	0			
8.11	データマスキング	0			
8.12	データ漏えい防止	0			
8.13	情報のバックアップ	0			
8.14	情報処理施設・設備の冗長性	0			
8.15	ログ取得	0			
8.16	監視活動	0			
8.17	クロックの同期	0			
8.18	特権的なユーティリティプログラムの使用	0			
8.19	運用システムへのソフトウェアの導入	0			
8.20	ネットワークセキュリティ	0			
8.21	ネットワークサービスのセキュリティ	0			
8.22	ネットワークの分離	0			
8.23	ウェブ・フィルタリング	0			
8.24	暗号の利用	0			
8.25	セキュリティに配慮した開発のライフサイクル	0			
8.26	アプリケーションセキュリティの要求事項	0			
8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	0			
8.28	セキュリティに配慮したコーディング	0			
8.29	開発及び受入れにおけるセキュリティテスト	0			
8.30	外部委託による開発	0			
8.31	開発環境、テスト環境及び本番環境の分離	0			
8.32	変更管理	0			
8.33	テスト用情報	0			
8.34	監査におけるテスト中の情報システムの保護	0			
追加管理策					
	N/A				

※上表の数字は改善指摘事項の件数を示します。“0”は指摘事項が無かったことを示します。
“N/A”は除外管理目的を示します。