# 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 10 月 24 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<br>ISO/IEC 27001:2022/Amd.1:2024 | Stage1 審査 |

※ 「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.Stage1 審査概要

1.1 目的
☒ : 対象となるマネジメントシステムの Stage2 審査に対する準備状況を評価・判定する。
☒ : Stage2 審査に先立って、不適合となり得る懸念事項を抽出する。

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.<br>/ 登録証番号 | **50301747ISMS22** | |
| Customer Name<br>/ 組織名称 | ☒:変更無 | エアーズ株式会社 |
| | □:変更有 | |
| Scope<br>/ 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<br>/ 対象事業 | ☒:変更無 | ・ソフトウェア開発事業<br>・ソフトウェア保守運用事業<br>・ソフトウェア開発コンサルティング業 |
| | □:変更有 | |
| SOA<br>/ 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<br>/ Employee Count | 3 名 | |
| 登録拠点<br>/ Location | ☒:変更無 | 浜松オフィス(新規登録) |
| | □:変更有 | |

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

1.5 審査工数
合計：1.5 人日 [文書審査：0.5 人日、現地審査：1.0 人日]

1.6 審査の実施方法, 有効性に関する記述
□ : Stage1 は Document Review 形式のみで実施しています。
☒ : Stage1 は Onsite で実施されました。
□ : 物理的拠点を持たない組織の為、Stage1 には遠隔審査技法を適用しました。
□ : リスク評価に基づき、Stage1 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。

| |
|---|
| |

## 2．審査結果

2.1 審査の結論

☒：Ready for Stage2 / Stage2 審査の準備が出来ている。
☐：Not Ready for Stage2 / Stage2 審査の準備が出来ていない。

審査中は多大なご協力を賜りまして有難う御座いました。審査チームは貴社の ISMS 登録審査 Stage2 に対する準備状況を評価しました。Stage1 審査の結論は、登録証の発行を保証するものではありませんが、Stage2 審査に耐え得る状況であることを示しています。

※ Stage1 審査で特定された懸念事項に対する解決策を DQS Japan Inc.に報告する必要は御座いませんが、Stage2 審査において重点事項となることをご承知置き下さい。
※ Stage1 審査はサンプリング方式に基づいて行われたことをご了承下さい。本報告書で提示した懸念事項を全て是正したとしても、登録範囲全体の規格適合性を保証するものではございません。

2.2 総合所見

2025 年 7 月から 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/各種規定類の整備が完了しています。ISMS 運用に関しては、2025 年 9 月の浜松オフィス開設後、2025 年 10 月から運用を始めております。各種規程類は、以前から運用されていた規定を浜松オフィスに適用することで、無理のない運用の開始にされていました。

リスク対応計画に則り、セキュリティや監視の強化に取り組んでいました。

現在、内部監査を実施中であり、マネジメントレビューも未実施でしたが、Stage2 審査までに内部監査とマネジメントレビューの実施が計画されていますので、Stage2 審査の準備は一通り完了していると評価します。

1 件の懸念事項が検出されましたが、Stage2 審査までに改善可能な事象であり、準備は出来ていると判断します。

2.3 Stage1 審査で観察された懸念事項

| No. | サイト/部門 | 条項番号 (Rating) | 内容 |
|---|---|---|---|
| 1 | ISMS 責任者 | 9.1 (NC) | 監視及び測定が必要と決定された全ての対象に対して、規格が要求している決定事項（評価方法、実施時期、実施者、評価時期、評価実施者等）の記載がありませんでした。監視状況も含めて決定された事項については Stage2 審査で確認させて頂きます。 |

※上表の条項番号下に記載した括弧書きは、観察した事象に対する重付けとなります。
OFI: Stage2 審査では「改善の機会」に相当する事象
nc ：Stage2 審査では「軽微な不適合」となり得る事象
NC：Stage2 審査では「重大な不適合」となり得る事象

## 3．今後の予定

**登録審査 Stage2**

2025 年 11 月 27 日～2025 年 11 月 28 日を予定。
文書レビュー：0,5 人日、現地審査(リモート審査)：1.5 人日

**審査チーム**

チームリーダー：山本　史夫（ISO/IEC 27001 主任審査員）

## 4．ISMS 要求事項の評価（ISO/IEC27001:2022 規格箇条）

| 条項 | 要求事項 | 証拠 | 評価 | 必要なアクション |
|---|---|---|---|---|
| 4.1 | 組織及びその状況の理解<br>(気候変動リスクに対する考慮) | SecureNavi-組織の状況と適用範囲 | (+) | |
| 4.2 | 利害関係者のニーズ及び期待の理解<br>(気候変動リスクに対する考慮) | SecureNavi-組織の状況と適用範囲 | (+) | |
| 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 | SecureNavi-組織の状況と適用範囲 | (+) | |
| 4.4 | 情報セキュリティマネジメントシステム | SecureNavi-組織の状況と適用範囲 | (+) | |
| 5.1 | リーダーシップ及びコミットメント | SecureNavi-役割・責任・権限リスト | (+) | |
| 5.2 | 方針 | SecureNavi-情報セキュリティ方針と目標<br>ホームページ | (+) | |
| 5.3 | 組織の役割，責任及び権限 | SecureNavi-役割・責任・権限リスト | (+) | |
| 6.1 | リスク及び機会に対処する活動 | SecureNavi-リスクアセスメント・対応マニュアル<br>SecureNavi-情報資産リスト<br>SecureNavi-適用宣言書 | (+) | |
| 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 | SecureNavi-リスクリスト<br>SecureNavi-タスクリスト | (+) | |
| 6.3 | 変更の計画策定 | SecureNavi-タスクリスト | (+) | |
| 7.1 | 資源 | SecureNavi-役割・責任・権限リスト | (+) | |
| 7.2 | 力量 | SecureNavi-力量<br>社内規程読み合せ記録<br>ISMS 規程理解度確認テスト<br>情報セキュリティ技術テスト | (+) | |
| 7.3 | 認識 | SecureNavi-教材の受講 | (+) | |
| 7.4 | コミュニケーション | SecureNavi-役割・責任・権限リスト | (+) | |
| 7.5 | 文書化した情報 | SecureNavi による管理 | (+) | |
| 8.1 | 運用の計画策定及び管理 | SecureNavi-タスク | (+) | |
| 8.2 | 情報セキュリティリスクアセスメント | SecureNavi-リスク対応 | (+) | |
| 8.3 | 情報セキュリティリスク対応 | SecureNavi-リスク対応 | (+) | |
| 9.1 | 監視，測定，分析及び評価 | SecureNavi-監視・測定 | (-) | 監視及び測定が必要と決定された全ての対象に対して、規格が要求している決定事項（評価方法、実施時期、実施者、評価時期、評価実施者等）の記載がありませんでした。監視状況も含めて決定された事項については Stage2 審査で確認させて頂きます。 |
| 9.2 | 内部監査 | SecureNavi-内部監査 | (+) | |
| 9.3 | マネジメントレビュー | SecureNavi-マネジメントレビュー | (+) | |
| 10.1 | 継続的改善 | SecureNavi-内部監査<br>SecureNavi-マネジメントレビュー<br>SecureNavi-インシデント管理 | (+) | |
| 10.2 | 不適合及び是正処置 | SecureNavi-改善<br>SecureNavi-インシデント管理 | (+) | |

※上表の評価欄に記載した記号は、以下の状態を示しています。

(+)　：該当する要求事項に対して適合する可能性が高いと評価されます。

0　：Stage2 審査で運用状況を確認した上で、適合/不適合を判断すべき事項となります。

(-)　：該当する要求事項に対して不適合となる可能性が高いと評価されます。

## 5．ISMS 管理策の評価（ISO/IEC27001:2022 附属書 A）

| No. | 管理策名 | 管理策 | 採否 | 評価 | 証拠/必要なアクション |
|---|---|---|---|---|---|
| 5.1 | 情報セキュリティのための方針群 | 情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で及び重大な変化が発生した場合にレビューしなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティ方針と目標 |
| 5.2 | 情報セキュリティの役割及び責任 | 情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てなければならない。 | 採択 | (+) | SecureNavi-役割・責任・権限リスト |
| 5.3 | 職務の分離 | 相反する職務及び相反する責任範囲は、分離しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.4 | 経営陣の責任 | 経営陣は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.5 | 関係当局との連絡 | 組織は、関係当局との連絡体制を確立し、維持しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>情報セキュリティ管理規程 |
| 5.6 | 専門組織との連絡 | 組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.7 | 脅威インテリジェンス | 情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | 情報セキュリティをプロジェクトマネジメントに組み入れなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.9 | 情報及びその他の関連資産の目録 | 情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持しなければならない。 | 採択 | (+) | SecureNavi-情報資産リスト<br>従業員向け基本規程<br>個人別資産台帳 |
| 5.10 | 情報及びその他の関連資産の許容される利用 | 情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施しなければならない。 | 採択 | (+) | SecureNavi-情報資産リスト |
| 5.11 | 資産の返却 | 要員及び必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>個人別資産台帳 |
| 5.12 | 情報の分類 | 情報は、機密性、完全性、可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って、分類しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.13 | 情報のラベル付け | 情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.14 | 情報の転送 | 情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備えなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.15 | アクセス制御 | 情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.16 | 識別情報の管理 | 識別情報のライフサイクル全体を管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |

| | | | | | |
|---|---|---|---|---|---|
| 5.17 | 認証情報 | 認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.18 | アクセス権 | 情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>SaaS 管理台帳 |
| 5.19 | 供給者関係における情報セキュリティ | 供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | 供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | ICT 製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | 組織は、供給者の情報セキュリティの活動及びサービス提供の変更を定常的に監視し、レビューし、評価し、管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | 組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>セキュリティインシデント対応マニュアル |
| 5.25 | 情報セキュリティ事象の評価及び決定 | 組織は、情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>インシデント管理規程<br>セキュリティインシデント対応マニュアル（セキュリティチーム用） |
| 5.26 | 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は、文書化した手順に従って対応しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>インシデント管理規程<br>セキュリティインシデント対応マニュアル（セキュリティチーム用） |
| 5.27 | 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知識は、情報セキュリティ管理策を強化し、改善するために用いなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>インシデント管理規程<br>セキュリティインシデント対応マニュアル（セキュリティチーム用） |
| 5.28 | 証拠の収集 | 組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>インシデント管理規程<br>セキュリティインシデント対応マニュアル（セキュリティチーム用） |
| 5.29 | 事業の中断・阻害時の情報セキュリティ | 組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>事業継続管理規程<br>安否確認・業務継続マニュアル |
| 5.30 | 事業継続のための ICT の備え | 事業継続の目的及び ICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持及び試験しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.31 | 法令、規制及び契約上の要求事項 | 情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを特定し、文書化し、また、最新に保たなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>SecureNavi-法規制 |

| | | | | | |
|---|---|---|---|---|---|
| 5.32 | 知的財産権 | 組織は、知的財産権を保護するための適切な手順を実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.33 | 記録の保護 | 記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.34 | プライバシー及び個人を特定できる情報（PII）の保護 | 組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシーの保護（preservation）及びPII の保護（protection）に関する要求事項を特定し、満たさなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.35 | 情報セキュリティの独立したレビュー | 人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | 組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを定期的にレビューしなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 5.37 | 操作手順書 | 情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にしなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 6.1 | 選考 | 要員になる全ての候補者についての経歴などの確認は、適用される法令、規制及び倫理を考慮に入れて、組織に加わる前に、及びその後継続的に行わなければならない。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 6.3 | 情報セキュリティの意識向上、教育及び訓練 | 組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の方針及び手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受けなければならず、また、定常的な更新を受けなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 6.4 | 懲戒手続 | 情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置を講じるために、懲戒手続きを正式に定め、伝達しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 6.5 | 雇用の終了又は変更後の責任 | 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 6.6 | 秘密保持契約又は守秘義務契約 | 情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定常的にレビューし、要員及びその他の関連する利害関係者が署名しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 6.7 | リモートワーク | 組織の構外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>従業員向け基本規程 |
| 6.8 | 情報セキュリティ事象の報告 | 組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設けなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>インシデント管理規程 |

| | | | | | |
|---|---|---|---|---|---|
| 7.1 | 物理的セキュリティ境界 | 情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>フロア図 |
| 7.2 | 物理的入退 | セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所によって保護しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.3 | オフィス、部屋及び施設のセキュリティ | オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.4 | 物理的セキュリティの監視 | 施設は、認可していない物理的アクセスについて継続的に監視しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.5 | 物理的及び環境的脅威からの保護 | 自然災害及びその他の意図的又は意図的でない、インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.6 | セキュリティを保つべき領域での作業 | セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.7 | クリアデスク・クリアスクリーン | 書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施させなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>従業員向け基本規程 |
| 7.8 | 装置の設置及び保護 | 装置は、セキュリティを保って設置し、保護しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.9 | 構外にある資産のセキュリティ | 構外にある資産を保護しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.10 | 記憶媒体 | 記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.11 | サポートユーティリティ | 情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護しなければならない。 | 不採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.12 | ケーブル配線のセキュリティ | 電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護しなければならない。 | 不採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.13 | 装置の保守 | 装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 7.14 | 装置のセキュリティを保った処分又は再利用 | 記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.1 | 利用者エンドポイント機器 | 利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.2 | 特権的アクセス権 | 特権的アクセス権の割当て及び利用は、制限し、管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>Admina |
| 8.3 | 情報へのアクセス制限 | 情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.4 | ソースコードへのアクセス | ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |

| | | | | | |
|---|---|---|---|---|---|
| 8.5 | セキュリティを保った認証 | セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備えなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.6 | 容量・能力の管理 | 現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.7 | マルウェアに対する保護 | マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.8 | 技術的ぜい弱性の管理 | 利用中の情報システムの技術的ぜい弱性に関する情報を獲得しなければならない。また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.9 | 構成管理 | ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューしなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>Admina |
| 8.10 | 情報の削除 | 情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.11 | データマスキング | データマスキングは、適用される法律を考慮して、組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.12 | データ漏えい防止 | データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.13 | 情報のバックアップ | 合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.14 | 情報処理施設・設備の冗長性 | 情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.15 | ログ取得 | 活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.16 | 監視活動 | 情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.17 | クロックの同期 | 組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.18 | 特権的なユーティリティプログラムの使用 | システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.19 | 運用システムへのソフトウェアの導入 | 運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |

| | | | | | |
|---|---|---|---|---|---|
| 8.20 | ネットワークセキュリティ | システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.21 | ネットワークサービスのセキュリティ | ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.22 | ネットワークの分離 | 情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.23 | ウェブフィルタリング | 悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.24 | 暗号の利用 | 暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.25 | セキュリティに配慮した開発のライフサイクル | ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>システム開発セキュリティ規程 |
| 8.26 | アプリケーションセキュリティの要求事項 | アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 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 | セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.28 | セキュリティに配慮したコーディング | セキュリティに配慮したコーディングの原則をソフトウェア開発に適用しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.29 | 開発及び受入れにおけるセキュリティテスト | セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.30 | 外部委託による開発 | 組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューしなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール<br>サプライヤー管理規程 |
| 8.31 | 開発環境、テスト環境及び本番環境の分離 | 開発環境、テスト環境及び本番環境は、分離してセキュリティを保たなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.32 | 変更管理 | 情報処理設備及び情報システムの変更は、変更管理手順に従わなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.33 | テスト用情報 | テスト用情報は、適切に選定し、保護し、管理しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |
| 8.34 | 監査におけるテスト中の情報システムの保護 | 運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。 | 採択 | (+) | SecureNavi-情報セキュリティマニュアル<br>SecureNavi-社内ルール |

※上表の評価欄に記載した記号は、以下の状態を示しています。

(+)　：該当する要求事項に対して適合する可能性が高いと評価されます。

0　：Stage2 審査で運用状況を確認した上で、適合/不適合を判断すべき事項となります。

(-)　：該当する要求事項に対して不適合となる可能性が高いと評価されます。