

JIS Q 27001 附属書 A に記載された管理策の中で、当社が社内ルールとして採用している管理策は以下のとおりです。

各管理策に基づいた具体的な実施事項については、別途「情報セキュリティマニュアル」に定めます。

事業目標、リスクアセスメントの観点から以下の管理策が策定されており、組織内での実施状況は以下のとおりです。

項番	管理策	採否	実施の状態
A.5.1	情報セキュリティのための方針群	Yes	実施中
A.5.2	情報セキュリティの役割及び責任	Yes	実施中
A.5.3	職務の分離	Yes	実施中
A.5.4	管理層の責任	Yes	実施中
A.5.5	関係当局との連絡	Yes	実施中
A.5.6	専門組織との連絡	Yes	実施中
A.5.7	脅威インテリジェンス	Yes	実施中
A.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	Yes	実施中
A.5.9	情報及びその他の関連資産の目録	Yes	実施中
A.5.10	情報及びその他の関連資産の許容される利用	Yes	実施中
A.5.11	資産の返却	Yes	実施中
A.5.12	情報の分類	Yes	実施中
A.5.13	情報のラベル付け	Yes	実施中
A.5.14	情報の転送	Yes	実施中
A.5.15	アクセス制御	Yes	実施中
A.5.16	識別情報の管理	Yes	実施中

- | A.5.17 | 認証情報 | Yes | 実施中 |
- | A.5.18 | アクセス権 | Yes | 実施中 |
- | A.5.19 | 供給者関係における情報セキュリティ | Yes | 実施中 |
- | A.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 | Yes | 実施中 |
- | A.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 | Yes | 実施中 |
- | A.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 | Yes | 実施中 |
- | A.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 | Yes | 実施中 |
- | A.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 | Yes | 実施中 |
- | A.5.25 | 情報セキュリティ事象の評価及び決定 | Yes | 実施中 |
- | A.5.26 | 情報セキュリティインシデントへの対応 | Yes | 実施中 |
- | A.5.27 | 情報セキュリティインシデントからの学習 | Yes | 実施中 |
- | A.5.28 | 証拠の収集 | Yes | 実施中 |
- | A.5.29 | 事業の中断・障害時の情報セキュリティ | Yes | 実施中 |
- | A.5.30 | 事業継続のための ICT の備え | Yes | 実施予定 |
- | A.5.31 | 法令、規制及び契約上の要求事項 | Yes | 実施中 |
- | A.5.32 | 知的財産権 | Yes | 実施中 |
- | A.5.33 | 記録の保護 | Yes | 実施中 |
- | A.5.34 | プライバシー及び個人識別可能情報 (PII) の保護 | Yes | 実施中 |
- | A.5.35 | 情報セキュリティの独立したレビュー | Yes | 実施中 |
- | A.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 | Yes | 実施中 |
- | A.5.37 | 操作手順書 | Yes | 実施中 |
- | A.6.1 | 選考 | Yes | 実施中 |
- | A.6.2 | 雇用条件 | Yes | 実施中 |

- | A.6.4 | 懲戒手続 | Yes | 実施中 |
- | A.6.5 | 雇用の終了又は変更後の責任 | Yes | 実施中 |
- | A.6.6 | 秘密保持契約又は守秘義務契約 | Yes | 実施中 |
- | A.6.7 | リモートワーク | Yes | 実施中 |
- | A.6.8 | 情報セキュリティ事象の報告 | Yes | 実施中 |
- | A.7.1 | 物理的セキュリティ境界 | Yes | 実施中 |
- | A.7.2 | 物理的入退 | Yes | 実施中 |
- | A.7.3 | オフィス、部屋及び施設のセキュリティ | Yes | 実施中 |
- | A.7.4 | 物理的セキュリティの監視 | Yes | 実施中 |
- | A.7.5 | 物理的及び環境的脅威からの保護 | Yes | 実施中 |
- | A.7.6 | セキュリティを保つべき領域での作業 | Yes | 実施中 |
- | A.7.7 | クリアデスク・クリアスクリーン | Yes | 実施中 |
- | A.7.8 | 機器の設置及び保護 | Yes | 実施中 |
- | A.7.9 | 構外にある資産のセキュリティ | Yes | 実施中 |
- | A.7.10 | 記録媒体 | Yes | 実施中 |
- | A.7.11 | サポートユーティリティ | Yes | 実施中 |
- | A.7.12 | ケーブル配線のセキュリティ | Yes | 実施中 |
- | A.7.13 | 装置の保守 | Yes | 実施中 |
- | A.7.14 | 装置のセキュリティを保った処分又は再利用 | Yes | 実施中 |
- | A.8.1 | 利用者エンドポイント機器 | Yes | 実施中 |
- | A.8.2 | 特権的アクセス権 | Yes | 実施中 |
- | A.8.3 | 情報へのアクセス制限 | Yes | 実施中 |
- | A.8.4 | ソースコードへのアクセス | Yes | 実施中 |
- | A.8.5 | セキュリティを保った認証 | Yes | 実施中 |

- | A.8.6 | 容量・能力の管理 | Yes | 実施中 |
- | A.8.7 | マルウェアに対する保護 | Yes | 実施中 |
- | A.8.8 | 技術的ぜい弱性の管理 | Yes | 実施中 |
- | A.8.9 | 構成管理 | Yes | 実施中 |
- | A.8.10 | 情報の削除 | Yes | 実施中 |
- | A.8.11 | データマスキング | Yes | 実施中 |
- | A.8.12 | データ漏えい防止 | Yes | 実施中 |
- | A.8.13 | 情報のバックアップ | Yes | 実施中 |
- | A.8.14 | 情報処理施設・設備の冗長性 | Yes | 実施中 |
- | A.8.15 | ログ取得 | Yes | 実施中 |
- | A.8.16 | 監視活動 | Yes | 実施中 |
- | A.8.17 | クロックの同期 | Yes | 実施中 |
- | A.8.18 | 特権的なユーティリティプログラムの使用 | Yes | 実施中 |
- | A.8.19 | 運用システムへのソフトウェアの導入 | Yes | 実施中 |
- | A.8.20 | ネットワークのセキュリティ | Yes | 実施中 |
- | A.8.21 | ネットワークサービスのセキュリティ | Yes | 実施中 |
- | A.8.22 | ネットワークの分離 | Yes | 実施中 |
- | A.8.23 | ウェブフィルタリング | Yes | 実施中 |
- | A.8.24 | 暗号の使用 | Yes | 実施中 |
- | A.8.25 | セキュリティに配慮した開発のライフサイクル | Yes | 実施中 |
- | A.8.26 | アプリケーションセキュリティの要求事項 | Yes | 実施中 |
- | A.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 | Yes | 実施中 |
- | A.8.28 | セキュリティに配慮したコーディング | Yes | 実施中 |

| A.8.29 | 開発及び受入れにおけるセキュリティテスト | Yes | 実施中 |

| A.8.30 | 外部委託による開発 | Yes | 実施中 |

| A.8.31 | 開発環境、テスト環境及び本番環境の分離 | Yes | 実施中 |

| A.8.32 | 変更管理 | Yes | 実施中 |

| A.8.33 | テスト用情報 | Yes | 実施中 |

| A.8.34 | 監査におけるテスト中の情報システムの保護 | Yes | 実施中 |