管 理 区 分
管 理 文 書

配付番号:

文書番号	IS-A-02
制定日	2014.04.01
改訂日	
改訂番号	1-0

適用宣言書

JIS Q 27001:2014 適用
（ ISO/IEC 27001:2013 ）

承 認	審 査

株式会社 サンプル

所 在 地:○○○○
電　　話:××－××××－××××
ＦＡＸ:××－××××－××××

IS-B-02

適用宣言書

制定:2014年04月01日

採否-○採用×採用せず　採用/除外理由-リ：リスクアセスメントの結果　法：法令規制要求　契：契約上の義務　事：事業上の要求

ISO27001附属書A　管理目的及び管理策	採否	採否の根拠	選択及び適用除外の理由	実行の有無
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	○	事	一連の情報セキュリティ方針を従業員並びに関係者へ確実に伝えるため	有
A.5.1.2 情報セキュリティのための方針群のレビュー	○	リ	方針に沿ったセキュリティ体制が正しく実施されていることを経営者に保証するため	有
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	○	リ、事	管理上の枠組みを確立し、セキュリティに関する役割及び責任を明確にするため	有
A.6.1.2 職務の分離	○	リ	業務上、故意の不正やオペレーションミスを防ぐため	有
A.6.1.3 関係当局との連絡	○	リ	セキュリティ上の事件・事故へ迅速な対応を行い、適切な連絡体制を維持するため	有
A.6.1.4 専門組織との連絡	○	リ	組織内で対応できないことを組織外の情報セキュリティ専門家より助言を受けるため	有
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	○	リ	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うため	有
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	○	リ	社外で利用するノートＰＣ等に保管された情報の漏洩や盗難を防止するため	有
A.6.2.2 テレワーキング	×	リ	対象となるリスクがないため（在宅勤務等の遠隔作業がないため）	無
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	○	リ	社員としての適正を採用時に判断することで、不正行為やリスクを軽減するため	有
A.7.1.2 雇用条件	○	事	雇用の際に情報セキュリティに対する責任事項を明確にし認識させるため	有
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	○	事	組織内の情報セキュリティを維持・管理して行くため	有
A.7.2.2 情報セキュリティの意識向上、教育及び訓練	○	事	従業員等に情報セキュリティ要求事項を遵守・維持させ、セキュリティの重要性を理解させるため	有
A.7.2.3 懲戒手続	○	事	従業員がセキュリティに関するルール違反を犯した際に、就業規則に従い適切に処分を行うため	有
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	○	事	組織からの離脱又は雇用の変更後も情報セキュリティに関する責任を負うことを明確にするため	有
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	○	事	資産の明確な識別を行い、適切に保護するため	有
A.8.1.2 資産の管理責任	○	事	組織の資産の適切な保護を維持・継続するため	有
A.8.1.3 資産利用の許容範囲	○	事	全ての資産利用者に対して、その利用範囲を明確にするため	有
A.8.1.4 資産の返却	○	事、契	資産の返却を確実に行うため	有
A.8.2 情報分類 目的：情報に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。				
A.8.2.1 情報の分類	○	事	情報資産の重要度を認識・分類し、適切な管理策を実施するため	有
A.8.2.2 情報のラベル付け	○	事	情報資産を分類し、適切なラベル表示を行い、そのラベル区分に応じた取り扱いを行うため	有
A.8.2.3 資産の取扱い	○	事	ラベル区分に応じた取り扱いを適切に行うため	有
A.8.3 媒体の取扱い 目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。				
A.8.3.1 取外し可能な媒体の管理	○	リ	適切な取り扱いを行い、紛失を防ぐため	有
A.8.3.2 媒体の処分	○	リ	廃棄時の情報漏洩を防止するため	有
A.8.3.3 物理的媒体の輸送	○	リ	配送中の不正アクセスや改ざん、破損から保護するため	有
A.9　アクセス制御				
A.9.1 アクセス制御に対する業務上の要求事項 目的：情報及び情報処理施設へのアクセスを制御するため。				
A.9.1.1 アクセス制御方針	○	リ	アクセスの必要のある者にだけアクセス権限を与えるため	有
A.9.1.2 ネットワーク及びネットワークサービスへのアクセス	○	リ	アクセスの必要のある者だけがアクセスできるようにするため	有
A.9.2 利用者アクセスの管理 目的：　システム及びサービスへの認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。				
A.9.2.1 利用者登録及び登録削除	○	リ	正規の利用者だけに利用を許可し、不要な利用者登録を残さないため	有

ISO27001附属書A 管理目的及び管理策	採否	採否の根拠	選択及び適用除外の理由	実行の有無
A.9.2.2 利用者アクセスの提供	○	リ	正規の利用者に対して適切なプロセスを提供するため	有
A.9.2.3 特権的アクセス権の管理	○	リ	権限のない者による特権の使用によって、不正アクセスが発生し、障害の発生することを防止するため	有
A.9.2.4 利用者の秘密認証情報の管理	○	リ	情報システムのパスワード発行、管理を確実にするため	有
A.9.2.5 利用者のアクセス権のレビュー	○	リ	許可された利用者だけがアクセス出来ることを確実にするため	有
A.9.2.6 アクセス権の削除又は修正	○	リ	不要な利用者登録を残さず、適切にアクセス権を保つため	有
A.9.3 利用者の責任 目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。				
A.9.3.1 秘密認証情報の利用	○	リ、事	正規利用者以外の情報機器へのアクセスを制限し、不正使用を防止するため	有
A.9.4 システム及びアプリケーションのアクセス制御 目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため。				
A.9.4.1 情報へのアクセス制限	○	リ	開示範囲の異なる情報に対して適切にアクセス権を制御するため	有
A.9.4.2 セキュリティに配慮したログオン手順	○	リ	セキュリティに配慮した手順によって不正なログインを防止するため	有
A.9.4.3 パスワード管理システム	○	リ、事	適切なパスワードを使用することで不正アクセスを防止するため	有
A.9.4.4 特権的なユーティリティプログラムの使用	○	リ	許可のない者がユーティリティを使用し、不正行為を行わないようにするた	有
A.9.4.5 プログラムソースコードへのアクセス制御	○	リ	業務のセキュリティ確保のため	有
A.10 暗号				
A.10.1 暗号による管理策 目的：情報の機密性、真正性または完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。				
A.10.1.1 暗号による管理策の利用方針	○	リ	暗号を適切に利用するため	有
A.10.1.2 鍵管理	○	リ	情報の機密性、真正性、完全性を確保するため	有
A.11 物理的及び環境的セキュリティ				
A.11.1 セキュリティを保つべき領域 目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため				
A.11.1.1 物理的セキュリティ境界	○	リ	社員以外の者が立ち入る事の出来る領域を明確にするため	有
A.11.1.2 物理的入退管理策	○	リ	セキュリティを保つべき領域において、適切な入退室管理を行うため	有
A.11.1.3 オフィス、部屋及び施設のセキュリティ	○	リ	無許可の者が無断で入室できないよう入退室を管理するため	有
A.11.1.4 外部及び環境の脅威からの保護	○	リ	自然災害又は人的災害による被害を物理的に保護するため	有
A.11.1.5 セキュリティを保つべき領域での作業	○	リ	セキュリティを保つべき領域内において、セキュリティに配慮した作業を確実に行うた	有
A.11.1.6 受渡場所	○	リ	セキュリティを保つべき領域内での外部業者の作業を制限するため	有
A.11.2 装置 目的：資産の損失、損傷、盗難又は劣化、及び組織の活動に対する妨害を防止するため。				
A.11.2.1 装置の設置及び保護	○	リ	環境上のリスクや無許可アクセスから装置を保護するため	有
A.11.2.2 サポートユーティリティ	○	リ	停電やその他の電気的異常から装置を防御するため	有
A.11.2.3 ケーブル配線のセキュリティ	○	リ	ネットワークケーブルを傍受又は損傷から保護するため	有
A.11.2.4 装置の保守	○	リ	業務で利用する装置について、装置の故障や不具合を防いで可用性及び完全性を維持するため	有
A.11.2.5 資産の移動	○	リ	可搬性の高い周辺機器やアプリケーション及び情報の移動を管理し、保護するため	有
A.11.2.6 構外にある装置及び資産のセキュリティ	○	リ	社外における情報機器無断設置によって引き起こされる脅威を防止するため	有
A.11.2.7 装置のセキュリティを保った処分又は再使用	○	リ	装置廃棄時の情報漏洩を防止するため	有
A.11.2.8 無人状態にある利用者装置	○	リ	無人運転の装置を不正使用、盗難や破損から保護するため	有
A.11.2.9 クリアデスク・クリアスクリーン方針	○	リ	情報資産の漏洩・損傷・紛失を防止するため	有
A.12 運用のセキュリティ				
A.12.1 運用の手順及び責任 目的：情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため。				
A.12.1.1 操作手順書	○	リ	情報セキュリティ維持に必要な装置の誤用を防ぐため	有
A.12.1.2 変更管理	○	リ	運用、設定変更の情報を管理、共有するため	有
A.12.1.3 容量・能力の管理	○	リ	情報機器の障害を未然に防ぐため	有
A.12.1.4 開発施設、試験施設及び運用施設の分離	○	リ	運用システムへの不正アクセス防止のため	有
A.12.2 マルウェアからの保護 目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。				
A.12.2.1 マルウェアに対する管理策	○	リ	社内外からのコンピュータウイルスや破壊的なプログラムの脅威から情報資産を保護するため	有
A.12.3 バックアップ 目的：データの消失から保護するため。				
A.12.3.1 情報のバックアップ	○	リ	重要な情報を消失という脅威から保護するため	有
A.12.4 ログ取得及び監視 目的：イベントを記録し、証拠を作成するため。				
A.12.4.1 イベントログ取得	○	リ	情報機器の利用状況を把握し、問題を検出するため	有
A.12.4.2 ログ情報の保護	○	リ	必要なログ情報を確実に取得出来るようにするため	有
A.12.4.3 実務管理者及び運用担当者の作業ログ	○	リ	伝達情報の誤用や間違いを防ぐため	有
A.12.4.4 クロックの同期	○	リ	データやログファイルの時刻を正確に記録し、事件･事故の際の調査及びログの監視に役立てるため	有
A.12.5 運用ソフトウェアの管理 目的：運用システムの完全性を確実にするため。				
A.12.5.1 運用システムに関わるソフトウェアの導入	○	リ	ソフトウエアの誤作動を防止するため	有
A.12.6 技術的ぜい弱性の管理 目的：技術的ぜい弱性の悪用を防止するため。				
A.12.6.1 技術的ぜい弱性の管理	○	リ	情報システム全般のリスクに対処し、そのリスクを低減するため	有

改 訂 歴 表

改訂番号	改訂日付	内　　容	作　成	承　認
1－0	2014.04.01	制定	○○	●●