文書番号　　K-S101

# 適用宣言書

## 目的

当社の情報ｾｷｭﾘﾃｨﾏﾈｲｼﾞﾒﾝﾄｼｽﾃﾑ（以下，ISMS）を構築及び運用にあたり，一般財団法人日本規格協会殿（以下，JSA)が発行する「対訳 ISO/IEC 27001:2013（JIS Q 27001:2014）情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑの国際規格」で記載された附属書A(規定）管理目的及び管理策の各規定項目に対して宣言したものである．なお適用範囲と適用宣言書内容で不一致な項については2021年末までの進むべき方向性を視野に入れ適用宣言を行った。

## 採否理由

管理目的及び管理策の選択理由，又は，適用除外とした場合の理由は，次の通りである．

選択理由　：　当社の事業に必要とする管理目的及び管理策であることから選択した．

除外理由　：　選択された管理目的及び管理策が，当社の事業で扱っていない，もしくは，ﾘｽｸｱｾｽﾒﾝﾄした結果，その管理目的及び管理策のﾘｽｸに対して，ﾘｽｸ回避，ﾘｽｸ移転，残留ﾘｽｸとして受容し，保有することで，適用除外とした．

| | | | | | |
|---|---|---|---|---|---|
| 除外項目 ： | A6.2.2 | A8.1.3 | A9.2.4 | A9.2.5 | A9.2.6 |
| | A9.4.5 | A10.1.2 | A12.1.1 | A12.1.2 | A12.4.1 |
| | A12.4.2 | A12.4.3 | | | |

## 適用対象者

本附属書A(規定)は，事務所内で業務履行する役員及び従業員（協力会社・契約社員・ﾊﾟｰﾄ･ｱﾙﾊﾞｲﾄ含む）に適用される．

版　数　：　第1版

発行元　：　規格管理室

| 規定・管理目的・管理策<br>1・1・2 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| 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 | 1 | 情報セキュリティのための方針群 | 採 | 情報セキュリティにおける経営陣の方向性及びその支持を得た証として，情報セキュリティ基本方針を定め，社内外へ公表した．情報セキュリティ基本方針及びその他方針を役員及び従業員（正社員のみ）へグループウェアによる閲覧で，周知を図る．また，正社員以外の新入社員及び従業員（協力会社，契約社員，パート，アルバイト）へは，採用時に情報セキュリティ教育で周知させる．<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 情報セキュリティのための方針群のレビュー | 採 | 情報セキュリティ基本方針及び各個別方針への見直し及び変更事項については，定期的に実施するマネジメントレビューで諮る．<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策 1・2・7 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.6 情報セキュリティのための組織 | A.6.1 内部組織 | 1 | 情報セキュリティの役割と責任 | 採 | ISMSの運用に必要とする体制及びその役割から情報セキュリティの責任について定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 2 | 職務の分離 | 採 | 業務遂行における牽制機能としての不正や，誤謬の発生を防ぐため職務の分離を定める.<br>[関連文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 3 | 関係当局との連絡 | 採 | 情報セキュリティにおける事件及び事故のインシデント発生時に，適切な処置が迅速にとられ，助言を得られることを確実にするために，必要な行政機関，規制機関，情報サービス提供者及び通信業者の連絡先を明確にする.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ<br>・情報ｾｷｭﾘﾃｨﾙｰﾙﾌﾞｯｸ |
| | | 4 | 専門組織との連絡 | 採 | 情報処理設備における情報セキュリティに対して，最新情報の入手又はシステムのぜい弱性の助言等を得ることを目的として，内部及び外部との連絡先を明確にする.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 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 | 採 | 各種プロジェクトにおける情報セキュリティへの取り組みとして，次に示すリスクを考慮し，プロジェクト計画を策定する.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | A.6.2 モバイル機器及びテレワーキング | 1 | モバイル機器の方針 | 採 | 業務で利用するモバイル機器の定義からその取扱いにおける方針を定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 2 | テレワーキング | 否 | ﾃﾚﾜｰｷﾝｸﾞの管理策を定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ<br><br>※当社では，現行の業務においてテレワーキングは実施していない。今後において実施した場合を想定してその管理策を定めた. |

| 規定・管理目的・管理策<br>1・3・6 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.7<br>人的資源のセキュリティ | A.7.1<br>雇用前 | 1 | 選考 | 採 | 正社員における新卒及び中途社員への採用手順を定める. なお, 正社員以外のパート及びアルバイト又は外注技術者については, その依頼業務に応じて, 経歴及びその他, 必要書類の確認から面談を経た後, 担当者が採用判断する.<br>[関係文書]<br>・情報セキュリティマニュアル<br>・情報セキュリティルールブック |
| | | 2 | 雇用条件 | 採 | 本採用した正社員についての雇用条件を定める. なお, 正社員以外のパート及びアルバイト又は外注技術者に対しても, 同様の雇用条件とする.<br>[関係文書]<br>・情報セキュリティマニュア<br>・情報セキュリティルールブック |
| | A.7.2<br>雇用期間中 | 1 | 経営陣の責任 | 採 | 社長の責任として, 当社のISMSで定めた情報セキュリティ基本方針及びルールを, 従業員が遵守することを確実にする. なお, これらの実施責任者は, 社長より任命されたセキュリティ管理責任者が担う.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 情報セキュリティの意識向上, 教育及び訓練 | 採 | セキュリティ管理責任者は, 役員及び従業員に対して, 情報セキュリティへの適切な意識向上を図るための教育又は訓練を実施する.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 懲戒手続 | 採 | ISMSで定めた規定及びルールに対して, その違反又は意図的な行ためにより, 当社が保有する情報資産を脅かした場合の罰則を定義する.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.7.3<br>雇用の終了及び変更 | 1 | 雇用の終了又は変更に関する責任 | 採 | 従業員の退職(契約終了含む)から職位及び業務の変更による役割について, その職務に応じた機密レベルに従ったアクセス権限の見直しをを定める.<br>[関係文書]<br>・情報セキュリティマニュアル<br>・情報セキュリティルールブック |

| 規定・管理目的・管理策 1・3・10 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.8 資産の管理 | A.8.1 資産に対する責任 | 1 | 資産目録 | 採 | 情報資産の評価規定に従い，情報資産管理台帳にて，維持管理する.<br>[関係文書]<br>・情報資産管理台帳 ： 顧客情報のみ<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 2 | 資産の管理責任者 | 採 | 情報資産管理台帳に登録された個々の情報資産に対して，その管理責任者を定める.<br>[関係文書]<br>・情報資産管理台帳 ： 顧客情報のみ<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 3 | 資産利用の許容範囲 | 否 | 組織で取扱う業務情報の利用にあたって，その許容範囲を定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 4 | 資産の返却 | 採 | 従業員の雇用終了に伴う，情報資産の返却から削除及び廃棄について定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ<br>・情報ｾｷｭﾘﾃｨﾙｰﾙﾌﾞｯｸ ： 別紙3-11の雇用の終了ﾙｰﾙ |
| | A.8.2 情報分類 | 1 | 情報の分類 | 採 | 情報の取扱いにおける，その重要度合いに応じた機密レベルを定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ<br>・情報ｾｷｭﾘﾃｨﾙｰﾙﾌﾞｯｸ ： 別紙3-9の情報取扱ﾙｰﾙ |
| | | 2 | 情報のラベル付け | 採 | 情報の機密レベルに応じた取扱いを確実にするためのラベル付けについて定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | | 3 | 資産の取扱い | 採 | 資産の機密レベルに応じた取扱いについて定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |

| 規定・管理目的・管理策<br>1・3・10 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.8<br>資産の管理 | A.8.3<br>媒体の取扱い | 1 | 取外し可能な媒体の管理 | 採 | 資産の機密レベルに応じた取外し可能な媒体について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 媒体の処分 | 採 | 情報が記録及び記憶された媒体の処分について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 物理的媒体の輸送 | 採 | 情報が記録及び記憶された物理的媒体における社外への持出しについて，その輸送方法に応じた保護対策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策 1・4・14 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| 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 | 1 | アクセス制御方針 | 採 | 情報や，それを扱う情報処理設備，及び業務上で利用する各種ソフトウェアへのアクセスについて，そのアクセス制御方針を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 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 | 採 | ネットワーク環境及びそのネットワークを利用したサービスについての方針を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.9.2 利用者アクセスの管理 | 1 | 利用者登録及び登録削除 | 採 | システム及びサービスへの利用にあったて，必要となる各種申請を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 利用者アクセスの提供 | 採 | 利用者登録された利用者のアクセスへの提供について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 特権的アクセス権の管理 | 採 | システムにおける特権管理について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | 利用者の秘密認証情報の管理 | 否 | 秘密認証情報における管理について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 5 | 利用者アクセス権のレビュー | 否 | システムのアクセス権における見直しについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 6 | アクセス権の削除又は修正 | 否 | 情報及び情報処理設備におけるアクセス権についての削除及びその登録情報の変更を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策 1・4・14 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.9 アクセス制御 | A.9.3 利用者の責任 | 1 | 秘密認証情報の利用 | 採 | 秘密認証情報としてのユーザIDとパスワードとなるが，特にパスワードの条件及びその管理方法について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.9.4 システム及びアプリケーションのアクセス制御 | 1 | 情報へのアクセス制限 | 採 | 情報へのアクセスについては，その利用者への制限及び取扱いに慎重を要する情報処理設備への利用制限も含めて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | セキュリティに配慮したログオン手順 | 採 | システム及びアプリケーションへのアクセスについて，セキュリティに配慮したログオン手順を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | パスワード管理システム | 採 | パスワードの条件及び管理方法について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | 特権的なユーティリティプログラムの使用 | 採 | 特権的なユーティリティプログラムの使用環境について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 5 | プログラムソースコードへのアクセス制御 | 否 | 社内システムへのプログラムソースコードのアクセス制御を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策<br>1・1・2 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.10<br>暗号 | A.10.1<br>暗号による管理策 | 1 | 暗号による管理策の利用方針 | 採 | 情報を保護するための暗号化による，その利用方針を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 鍵管理 | 否 | 暗号化で使用する鍵の管理について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策 1・2・15 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| 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 | 1 | 物理的セキュリティ境界 | 採 | 情報処理設備が設置された領域の物理的な保護を目的とした，セキュリティ対策について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 物理的入退管理策 | 採 | 施設への入退室について，そのセキュリティ対策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | オフィス，部屋及び施設のセキュリティ | 採 | 施設への物理的なセキュリティについて，その対策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | 外部及び環境の脅威からの保護 | 採 | 天災や事故等の災害におけるセキュリティ対策について定める.<br>[関係文書]<br>・情報セキュリティマニュアル<br>・事業継続計画 ： 適用なし |
| | | 5 | セキュリティを保つべき領域での作業 | 採 | セキュリティを保つべき領域での作業について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 6 | 受渡場所 | 採 | 荷物の搬入及び搬出のやり方を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.11.2 装置 | 1 | 装置の設置及び保護 | 採 | 装置の設置及びその保護により，性能が期待通り，安定的に使用できることを保証するための処置について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | サポートユーティリティ | 採 | 装置のサポートユーティリティとしては，部門サーバ以外の特に重要とする各種サーバの運用に必要とする付帯設備について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策 1・2・15 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.11 物理的及び環境的セキュリティ | A.11.2 装置 | 3 | ケーブル配線のセキュリティ | 採 | 各種ケーブル配線の保護策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | 装置の保守 | 採 | 装置が正しく動作することを確実にするための保守について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 5 | 資産の移動 | 採 | 保有する情報資産における社外への持出しについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 6 | 構外にある装置及び資産のセキュリティ | 採 | 社外におけるモバイル機器及びPCの取扱いについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 7 | 装置のセキュリティを保った処分又は再利用 | 採 | 装置，つまりサーバ，PC，モバイル機器及びNASを含めた外部記憶装置に対しての再利用及び廃棄について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 8 | 無人状態にある利用者装置 | 採 | 装置の無人状態，つまり，PC及びサーバの使用中における離席や，社外に設置されたPCについてのセキュリティ対策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 9 | クリアデスク・クリアスクリーン方針 | 採 | 作業場所のクリアデスク及びディスプレイのクリアスクリーンについての方針を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策<br>1・7・14 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.12 運用のセキュリティ | A.12.1 運用の手順及び責任 | 1 | 操作手順書 | 否 | 情報処理設備の運用における操作手順の作成について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 変更管理 | 否 | 情報処理設備への変更についての手順を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 容量・能力の管理 | 採 | 情報処理設備に対して，業務を遂行するうえで，ストレスなく快適に使用できる性能及び，余裕ある容量について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | 開発環境，試験環境及び運用環境の分離 | 採 | 業務システムの運用に影響を及ぼす運用環境，試験環境，開発環境は，分離し，その妨げとなるリスクを軽減するための処置を定める.<br>[関連文書]<br>・情報セキュリティマニュアル |
| | A.12.2 マルウェアからの保護 | 1 | マルウェアに対する管理策 | 採 | マルウェアからの攻撃による脅威に対抗するための処置を定める.<br>[関係文書]<br>・情報セキュリティマニュアル<br>・情報セキュリティルールブック |
| | A.12.3 バックアップ | 1 | 情報のバックアップ | 採 | 情報処理設備で取扱う重要なデータのバックアップについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.12.4 ログ取得及び監視 | 1 | イベントログ取得 | 否 | システムにおける各種のイベントログについて，主に採取する項目を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策<br>1・7・14 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.12<br>運用のセキュリティ | A.12.4<br>ログ取得及び監視 | 2 | ログ情報の保護 | 否 | 取得したログの保護について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 実務管理者及び運用担当者の作業ログ | 否 | 重要なシステムであるサーバラック内で運用する各種サーバの作業について，そのセキュリティ対策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | クロックの同期 | 採 | 当社のドメインに参加するサーバ及びPCへのクロック同期について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.12.5<br>運用ソフトウェアの管理 | 1 | 運用システムに関わるソフトウェアの導入 | 採 | 運用システムの変更からその利用について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.12.6<br>技術的ぜい弱性管理 | 1 | 技術的ぜい弱性の管理 | 採 | 情報システムにおける技術的なぜい弱性に関する情報の管理について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | ソフトウェアのインストールの制限 | 採 | PCへインストールするソフトウェアの制限について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.12.7<br>情報システムの監査に対する考慮事項 | 1 | 情報システムの監査に対する管理策 | 採 | 運用システムにおける監査の実施について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策 1・2・7 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.13 通信のセキュリティ | A.13.1 ネットワークセキュリティ管理 | 1 | ネットワーク管理策 | 採 | ネットワークへの脅威から保護するためのセキュリティについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | ネットワークサービスのセキュリティ | 採 | ネットワークサービスの利用におけるセキュリティについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | ネットワークの分離 | 採 | 社内LANに接続されたサーバや，PC，プリンタ装置及びネットワーク機器等におけるネットワークアドレスの管理について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.13.2 情報の転送 | 1 | 情報転送の方針及び手順 | 採 | 組織間又は外部との情報の転送や，交換についての方針及び手順を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 情報転送に関する合意 | 採 | 組織外との情報における転送や，交換について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 電子的メッセージ通信 | 採 | 電子メール及びお客様との商取引で利用する電子データ交換におけるセキュリティ対策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | 秘密保持契約又は守秘義務契約 | 採 | 秘密保持契約，守秘義務契約，機密保持契約又はCA，NDAといった契約の留意点について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策<br>1・3・13 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.14<br>システムの取得，開発及び保守 | A.14.1<br>情報システムのセキュリティ要求事項 | 1 | セキュリティ要求事項の分析及び仕様化 | 採 | 情報システムの開発及び購入にあたって，その利用状況に応じたセキュリティ要件を含めた導入検討について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮 | 採 | インターネット上で公開するウェブサイトへのセキュリティ対策について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | アプリケーションサービスのトランザクションの保護 | 採 | アプリケーションサービスのトランザクションにおけるセキュリティ対策を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.14.2<br>開発及びサポートプロセスにおけるセキュリティ | 1 | セキュリティに配慮した開発のための方針 | 採 | セキュリティに配慮した情報システムの開発について，その方針を定める. |
| | | 2 | システムの変更管理手順 | 採 | 情報システムの導入から変更及び廃棄における手順を定める. |
| | | 3 | オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー | 採 | 情報システムの動作環境におけるOSの変更について定める. |
| | | 4 | パッケージソフトウェアの変更に対する制限 | 採 | ベンダ又はメーカより購入したパッケージソフトの使用について定める. |

| 規定・管理目的・管理策<br>1・3・13 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.14<br>システムの取得，開発及び保守 | A.14.2<br>開発及びサポートプロセスにおけるセキュリティ | 5 | セキュリティに配慮したシステム構築の原則 | 採 | セキュリティに配慮したシステム構築を行うための原則について定める. |
| | | 6 | セキュリティに配慮した開発環境 | 採 | 情報システム及び自社パッケージソフト等の開発における環境について定める. |
| | | 7 | 外部委託による開発 | 採 | 外部委託によるｿﾌﾄｳｪｱ開発のセキュリティ対策について定める. |
| | | 8 | システムセキュリティの試験 | 採 | 情報システムの試験について定める. |
| | | 9 | システムの受入れ試験 | 採 | 情報システムの新たな導入及び更改について定める. |
| | A.14.3<br>試験データ | 1 | 試験データの保護 | 採 | 情報システムの処理結果に対して，その妥当性を確認するための試験データについて定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |

| 規定・管理目的・管理策<br>1・2・5 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.15<br>供給者関係 | A.15.1<br>供給者関係における情報セキュリティ | 1 | 供給者関係のための情報セキュリティの方針 | 採 | 供給者との新たな取引きにあたっての方針を定める.<br>[関連文書]<br>・情報セキュリティマニュアル |
| | | 2 | 供給者との合意におけるセキュリティの取扱い | 採 | 供給者との合意(契約)について定める.<br>[関連文書]<br>・情報セキュリティマニュアル |
| | | 3 | ICTサプライチェーン | 採 | 情報通信技術(ICT:Information and Communication Technology)サービス及び製品のサプライチェーン, つまり, ICTサプライチェーンによるクラウドサービスの利用にあたって, その提供企業の選定条件について定める.<br>[関連文書]<br>・情報セキュリティマニュアル |
| | A.15.2<br>供給者のサービス提供の管理 | 1 | 供給者のサービス提供の監視及びレビュー | 採 | 供給者からのサービス提供における取り決めた事項の合意, 及びその運用における監視について定める.<br>[関連文書]<br>・情報セキュリティマニュアル |
| | | 2 | 供給者のサービス提供の変更に対する管理 | 採 | 供給者からのサービス提供における見直しのきっかけ, 及び見直し後のサービス変更におけるセキュリティ対策について定める.<br>[関連文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策 1・1・7 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.16 情報セキュリティインシデントの管理 | A.16.1 情報セキュリティインシデントの管理及びその改善 | 1 | 責任及び手順 | 採 | セキュリティ全般における事象又は弱点の報告から，情報システムの警告や，ぜい弱性におけるインシデントの発生に対して，その責任体制及び必要とする管理手順について定める.<br>[関連文書]<br>・情報セキュリティマニュアル |
| | | 2 | 情報セキュリティ事象の報告 | 採 | 情報セキュリティ事象における報告の義務及びその経路について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 情報セキュリティ弱点の報告 | 採 | 情報システム及び各種サービスにおける情報セキュリティ上の弱点の報告義務について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | 情報セキュリティ事象の評価及び決定 | 採 | 情報セキュリティの事象における評価及びインシデントとしての判定基準を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 5 | 情報セキュリティインシデントへの対応 | 採 | 情報セキュリティインシデントにおける処置手順を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 6 | 情報セキュリティインシデントからの学習 | 採 | 情報セキュリティインシデントからの学習について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 7 | 証拠の収集 | 採 | 証拠の収集について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

| 規定・管理目的・管理策<br>1・2・4 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.17<br>事業継続マネジメントにおける情報セキュリティの側面 | A.17.1<br>情報セキュリティ継続 | 1 | 情報セキュリティ継続の計画 | 採 | 事業活動の継続が困難な状況下において，いち早く復旧させるための計画を定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ<br>・事業継続計画 |
| | | 2 | 情報セキュリティ継続の実施 | 採 | 業務の中断におけるﾘｽｸｱｾｽﾒﾝﾄを取り込んだ事業継続を定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ<br>・事業継続計画 |
| | | 3 | 情報セキュリティ継続の検証，レビュー及び評価 | 採 | 事業継続計画の試験及び維持における検証について定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |
| | A.17.2<br>冗長性 | 1 | 情報処理施設の可用性 | 採 | 情報処理施設及び情報処理設備への冗長化について定める.<br>[関係文書]<br>・情報ｾｷｭﾘﾃｨﾏﾆｭｱﾙ |

| 規定・管理目的・管理策 1・2・8 | | | | 採否 | 処置結果及び関係文書 |
|---|---|---|---|---|---|
| A.18 順守 | A.18.1 法的及び契約上の要求事項の順守 | 1 | 適用法令及び契約上の要求事項の特定 | 採 | 情報セキュリティに関連する法令，規制及び契約上の義務に対しての特定について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 知的財産権 | 採 | 知的財産権及び権利関係が存在するOS及びパッケージソフトの利用について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 記録の保護 | 採 | 記録の保護における手段を定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 4 | プライバシー及び個人を特定できる情報（PII）の保護 | 採 | プライバシー及び個人情報(PII:Personality Identifiable Information)に関連する情報の取扱いについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 5 | 暗号化機能に対する規則 | 採 | 暗号化機能を持つ機器及びソフトウェア製品の輸出又は輸入について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | A.18.2 情報セキュリティのレビュー | 1 | 情報セキュリティの独立したレビュー | 採 | ISMSが効果的，かつ，有効的に運用されているか，判断するためのレビューについて定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 2 | 情報セキュリティのための方針群及び標準の順守 | 採 | 適切に情報セキュリティ基本方針，規定，ルールが守られているか，そのための点検について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |
| | | 3 | 技術的順守のレビュー | 採 | 情報処理設備へのセキュリティ対策が，規定された通りに順守されているかの点検について定める.<br>[関係文書]<br>・情報セキュリティマニュアル |

## 改版履歴

| 版数 | 改版日 | ﾍﾟｰｼﾞ | 変更内容 | 担当者 |
|---|---|---|---|---|
| 1.0 | 2019年7月1日 | 全頁 | 初版 | 露無 |
| | | | | |
| | | | | |