# 情報セキュリティ
# マネジメントシステム
# 管理規程

株式会社ＳＤホールディングス

| | |
|---|---|
| 制定日 | 2023/2/28 |
| 改定日 | 2023/9/27 |

# ～　改訂歴表　～

| 版番号 | 発行年月日 | 改　訂　内　容 |
|---|---|---|
| 01 | 23/02/28 | 初版発行 |

| | | |
|---|---|---|
| 02 | 23/09/25 | A.8.1.1 情報資産リスクアセスメント表管理項目へ保管期間を追加<br>A.8.1.3 情報資産リスクアセスメント表・補票を参照する旨を追加<br>A.8.2.1 情報資産リスクアセスメント表・補票を参照する旨を追加<br>A.8.2.3 情報資産リスクアセスメント表・補票を参照する旨を追加<br>A.9.1.1 情報資産リスクアセスメント表・補票を見直す旨を追加<br>A.9.2.1 情報資産リスクアセスメント表・補票を見直す旨を追加<br>A.11.1.2 以下の通り変更<br>「①応接共用区画の入口は、施設入口内側より解錠し、就業時間中は常時開放とする。」<br>↓<br>「①応接共用区画の入口は、施設入口内側より解錠し、就業時間中は常時開放とする。」<br>A.11.1.5 以下を削除<br>「机上にて配置する情報機器は、ワイヤーロック結着による固定もしくは、退社時に指定のキャビネットに収納し、施錠保管する。」<br>A.14.1.2 以下を追加<br>「当社は、公衆ネットワークを経由するアプリケーションサービスを利用しない。」<br>A.14.2.8 以下の通り変更<br>「セキュリティ機能の試験は、開発期間中に実施する。」<br>↓<br>「当社はシステム開発を行わない。システム開発する場合は、セキュリティ機能の試験は、開発期間中に実施する。」<br>A.14.3.1 以下の通り変更<br>「試験データは、管理責任者が選定し、適切に保護および管理するものとする。」<br>↓<br>「当社はシステム開発を行わない。<br>システム開発する場合は、試験データは、管理責任者が選定し、適切に保護および管理するものとする。」<br>A.18.1.1 以下を追加<br>「特に「法規制一覧表」に特定する法令等に改正等により要求事項に変更があり、本規程での既存の内容では要求事項を満たさず違反することが無いように見直し、本規程を改定した場合は直ちに社内に周知徹底する。」 |

| | | |
|---|---|---|
| 02 | 23/09/25 | A.18.1.5 以下を追加<br>「当社は、暗号化機能を要する利用はない。行う場合は、以下の原則とする。」<br>全文を通しあいまいな表現の修正 |

構成

| | |
|---|---|
| | |
| １．目的 | |
| ２．適用範囲 | |
| ３．責任と権限 | |
| ４．管理策 | |
| 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<br>A.5.1.1　情報セキュリティのための方針群<br>A.5.1.2　情報セキュリティのための方針群のレビュー |
| A.6. 情報セキュリティのための組織 | |
| | A.6.1　内部組織<br>A.6.1.1　情報セキュリティの役割及び責任<br>A.6.1.2　職務の分離<br>A.6.1.3　関係当局との連絡<br>A.6.1.4　専門組織との連絡<br>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管理規程<br>A.6.2　モバイル機器及びテレワーキング<br>A.6.2.1　モバイル機器の方針<br>A.6.2.2　テレワーキング |
| A.7.　人的資源のセキュリティ | |
| | A.7.1　雇用前<br>A.7.1.1　選考<br>A.7.1.2　雇用条件<br>A.7.2　雇用期間中<br>A.7.2.1　経営陣の責任<br>A.7.2.2　情報セキュリティの意識向上、教育及び訓練<br>A.7.2.3　懲戒手続<br>A.7.3　雇用の終了又は変更<br>A.7.3.1　雇用の終了又は変更に関する責任 |
| A.8 資産の管理 | |
| | A.8.1.1　資産目録<br>A.8.1.2　資産の管理責任者<br>A.8.1.3　資産利用の許容範囲<br>A.8.1.4　資産の返却<br>A.8.2　情報分類<br>A.8.2.1　情報分類の指針<br>A.8.2.2　情報セキュリティ資産のラベル付け及び取り扱い<br>A.8.2.3　情報の取り扱い手順 |

| | |
|---|---|
| | A.8.3　媒体の取り扱い<br>A.8.3.1　取り外し可能な媒体の管理<br>A.8.3.2　媒体の処分<br>A.8.3.3　物理的媒体の輸送 |
| 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<br>A.9.1.1　アクセス制御方針<br>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<br>A.9.2　利用者アクセスの管理<br>A.9.2.1　利用者登録及び登録削除<br>A.9.2.2　利用者アクセスの提供<br>A.9.2.3　特権的アクセス権の管理<br>A.9.2.4　利用者の秘密認証情報の管理<br>A.9.2.5　利用者アクセス権のレビュー<br>A.9.2.6　アクセス権の削除又は修正<br>A.9.3　利用者の責任<br>A.9.3.1　秘密認証情報の使用<br>A.9.4.1　情報へのアクセス制限<br>A.9.4.2　セキュリティに配慮したログオン手順<br>A.9.4.3　パスワード管理システム<br>A.9.4.4　特権的なユーティリティプログラムの使用<br>A.9.4.5　プログラムソースコードへのアクセス制御 |
| A.10　暗号 | |
| | A.10.1.2　鍵管理<br>A.10.1.1　暗号による管理策<br>A.10.1.1　暗号による管理策の利用方針 |
| 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<br>A.11.1.1　物理的セキュリティ境界<br>A.11.1.2　物理的入退管理策<br>A.11.1.3　オフィス、部屋及び施設のセキュリティ<br>A.11.1.4　外部及び環境の脅威からの保護<br>A.11.1.5　セキュリティを保つべき領域での作業<br>A.11.1.6　受渡場所<br>A.11.2　装置<br>A.11.2.1　装置の設置及び保護<br>A.11.2.2　サポートユーティリティ<br>A.11.2.3　ケーブル配線のセキュリティ<br>A.11.2.4　装置の保守 |

| | |
|---|---|
| | A.11.2.5　資産の移動 |
| | A.11.2.6　構外にある装置及び資産のセキュリティ |
| | A.11.2.7　装置のセキュリティを保った処分又は再利用 |
| | A.11.2.8　無人状態にある利用者装置 |
| | A.11.2.9　クリアデスク・クリアスクリーン方針 |
| A.12　運用のセキュリティ | |
| | A.12.1　　運用の手順及び責任 |
| | A.12.1.1　操作手順 |
| | A.12.1.2　変更管理 |
| | A.12.1.3　容量、能力の計画作成 |
| | A.12.1.4　開発環境、試験環境及び運用環境の分離 |
| | A.12.2　　マルウェアからの保護 |
| | A.12.2.1　マルウェアに対する管理策 |
| | A.12.3　　バックアップ |
| | A.12.3.1　情報のバックアップ |
| | A.12.4　　ログ取得及び監視 |
| | A.12.4.1　イベントログ取得 |
| | A.12.4.2　ログ情報の保護 |
| | A.12.4.3　実務管理者及び運用担当者の作業ログ |
| | A.12.4.4　クロックの同期 |
| | A.12.5　　運用ソフトウェアの管理 |
| | A.12.5.1　運用システムに関わるソフトウェアの導入 |
| | A.12.6　　技術的ぜい弱性管理 |
| | A.12.6.1　技術的ぜい弱性の管理 |
| | A.12.6.2　ソフトウェアのインストールの制限 |
| | A.12.7　　情報システムの監査に対する考慮事項 |
| | A.12.7.1　情報システムの監査に対する管理策 |
| 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 |
| | A.13.1.1　ネットワーク管理策 |
| | A.13.1.2　ネットワークサービスのセキュリティ |
| | A.13.1.3　ネットワークの分離 |
| | A.13.2　　情報の交換 |
| | A.13.2.1　情報交換の方針及び手順 |
| | A.13.2.2　情報交換に関する合意 |
| | A.13.2.3　電子的メッセージ通信 |
| | A.13.2.4　秘密保持契約又は守秘義務契約（当社内業務、外部委託） |
| A.14　情報システムの取得、開発及び保守 | |
| | A.14.1　　情報システムのセキュリティ要求事項 |

| | |
|---|---|
| | A.14.1.1　セキュリティ要求事項の分析及び仕様化<br>A.14.1.2　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<br>A.14.1.3　アプリケーションサービスのトランザクションの保護<br>A.14.2　　開発及び支援プロセスにおけるセキュリティ<br>A.14.2.1　セキュリティに配慮した開発のための方針<br>A.14.2.2　変更管理手順<br>A.14.2.3　オペレーティングシステムの変更後の業務用ソフトウェアの技術的レビュー<br>A.14.2.4　パッケージソフトウェアの変更に対する制限<br>A.14.2.5　セキュリティに配慮したシステム構築の原則<br>A.14.2.6　セキュリティに配慮した開発環境<br>A.14.2.7　外部委託によるソフトウェア開発<br>A.14.2.8　システムセキュリティの試験<br>A.14.2.9　システムの受入れ試験<br>A.14.3　　試験データ<br>A.14.3.1　試験データの保護 |
| A.15.　供給者関係 | |
| | A.15.1　　供給者関係における情報セキュリティ<br>A.15.1.1　供給者関係のための情報セキュリティの方針<br>A.15.1.2　供給者との合意におけるセキュリティの取扱い<br>A.15.1.3　ICT サプライチェーン<br>A.15.2　　供給者のサービス提供の管理<br>A.15.2.1　供給者のサービス提供の監視及びレビュー<br>A.15.2.2　供給者のサービス提供の変更に対する管理 |
| 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<br>A.16.1.１　責任及び手順<br>A.16.1.2　情報セキュリティ事象の報告<br>A.16.1.3　情報セキュリティの弱点の報告<br>A.16.1.4　情報セキュリティ事象の評価及び決定<br>A.16.1.5　情報セキュリティインシデントへの対応<br>A.16.1.6　情報セキュリティインシデントからの学習<br>A.16.1.7　証拠の収集 |
| A.17　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　　情報セキュリティ継続<br>A.17.1.1　情報セキュリティ継続の管理<br>A.17.1.2　情報セキュリティ継続の実施<br>A.17.1.3　情報セキュリティ継続の検証、レビュー及び評価 |

| | |
|---|---|
| | A.17.2　冗長性<br>A.17.2.1　情報処理施設の可用性 |
| A.18　順守 | |
| | A.18.1　法的及び契約上の要求事項の順守<br>A.18.1.1　適用法令及び契約上の要求事項の特定<br>A.18.1.2　知的所有権<br>A.18.1.3　記録の保護<br>A.18.1.4　プライバシー及び個人を特定できる情報の保護<br>A.18.1.5　暗号化機能に対する規制<br>A.18.2　情報セキュリティの独立したレビュー<br>A.18.2.1　情報セキュリティの独立したレビュー<br>A.18.2.2　情報セキュリティのための方針及び標準の遵守<br>A.18.2.3　技術的遵守のレビュー |

１．目的

本規程は、当社の情報セキュリティマネジメントシステムの情報管理を明確にする。

２．適用範囲

本規程は、当社の情報セキュリティマネジメントシステムの情報管理について適用する。

３．責任と権限

各個別の項目に責任と権限を明確にする。

４．管理策

情報セキュリティマネジメントシステムマニュアル（以下、ISMS マニュアルという）及び JIS Q 27001：2014（ISO/IEC 27001：2013）附属書 A（以下、附属書 A という）での管理策について、A.5 以降、具体的な情報管理手順を記す。

A.5.

内部監査でレビューする

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，事業上の要求事項並びに関連する法令及び規制に従って提示するため。

A.5.1.1 情報セキュリティのための方針群

| |
|---|
| 情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知しなければならない。 |

「情報セキュリティに関する方針」にて明示し、従業員に周知するとともに、関連する外部関係者に公表する。

A.5.1.2 情報セキュリティのための方針群のレビュー

| |
|---|
| 情報セキュリティのための方針群は，あらかじめ定めた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当かつ有効であることを確実にするためにレビューしなければならない。 |

「情報セキュリティに関する方針」にて示した目標及び目的を実施するための個別の方針を本管理規程の A.6.以降に記す。

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

| |
|---|
| 全ての情報セキュリティの責任を定め，割り当てなければならない。 |

ISMS マニュアル 5.3 及び「情報セキュリティマネジメントシステム体制図」にて明示する。

A.6.1.2　職務の分離

| |
|---|
| 相反する職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離しなければならない。 |

相反する作成者および承認者を明確にするため、「情報セキュリティマネジメントシステム体制図」にて職務分掌及び職務権限を明示する。

A.6.1.3　関係当局との連絡

| |
|---|
| 関係当局との適切な連絡体制を維持しなければならない。 |

管理責任者は、ISMS 運用のため、関係当局との連絡体制を整備し、具体的な連絡手段方法は、A.16.1.1 責任及び手順に従って、文書化する。

関係機関として、以下の機関を含む。

・顧客（委託元）、協力会社
・ISMS 認証機関
・通信事業会社、電気設備（電気設備工事、ネットワーク工事）
・ビル管理会社、警察、消防

A.6.1.4　専門組織との連絡

| |
|---|
| 情報セキュリティに関する研究会又は会議，および情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。 |

管理責任者は、ISMS 運用のため、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・団体との適切な連絡体制を維持し、適切な情報取得を行う。

専門組織として、以下の組織を含む。

・情報セキュリティの脆弱性
　IPA（独立行政法人情報処理推進機構）
　https://www.ipa.go.jp/security/index.html
・コンピュータセキュリティの脆弱性
　JPCERT（一般社団法人 JPCERT コーディネーションセンター）
　https://www.jpcert.or.jp/
・個人情報の保護
　JIPDEC（一般財団法人日本情報経済社会推進協会）
　https://www.jipdec.or.jp/project/purpose/study.html

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管理規程

| |
|---|
| プロジェクトの種類にかかわらず，プロジェクトマネジメントにおいては，情報セキュリティに取り組まなければならない。 |

プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティの保護に取り組む。

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

| |
|---|
| モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用しなければならない。 |

モバイル機器を携行して利用する際には、以下の手順とする。

①使用するモバイル機器は会社が貸与したモバイル機器を使用する。

②使用するソフトウェアは、貸与時に設定したのみとする。ウィルスソフトウェア及びOSの脆弱性ソフトは最新の状態に更新維持する。

③使用モバイル機器は貸与を受けた本人のみが使用をし、家族等の第三者に貸与できないよう、パスワードなどアクセス制限する。

④使用モバイル機器にデータをダウンロードして活用する場合は、③に加えデータファイルにも、パスワードなどアクセス制限または暗号化する。

⑤②にて特別にソフトウェアを追加して設定したい場合は、理由を明示した書面を添えて所属長の確認を経て管理責任者の承認を受けた場合のみ許可する。

⑥貸与時に上記を明示した確認書にて本人に貸与する。確認書には、期間を明示し、期間が満了した際に、速やかに返却し、継続する場合は、使用モバイル機器を持参した上で申請し、更新の許可を受ける。

A.6.2.2　テレワーキング

| |
|---|
| テレワーキングの場所でアクセス，処理及び保存される情報を保護するために，方針及びその方針を支援するセキュリティ対策を実施しなければならない。 |

A.6.2.1にて貸与を受けて社外にて、テレワーキングの場所で利活用する場合は、以下の手順を追加する。

①社内サーバへのアクセスを行う場合は、許可された通信経路端末の追加貸与を受けた場合のみとし、公衆Wi-Fiなどを経由しての接続は禁止する。

②指定されたストレージ（社外サーバ）にアクセスする場合は、指定されたIDとパスワードにて接続する場合のみ許可する。

③指定されたストレージ（社外サーバ）にアクセスし、データを使用モバイル機器にダウンロードして活用する場合は、データファイルにも、パスワードなどアクセス制限または暗号化する。

④貸与時に上記を明示した確認書（A.6.2.1に追記）にて本人に貸与する。

## 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

| |
|---|
| 全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従 |

って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。

採用募集に対して応募者に提出を求めた個人情報等は、個人情報保護委員会の指定するガイドラインなどにと基づき、以下の手順で行う。

①利用目的を明示した上で、同意を得て取得する。紙媒体での提出の際には、提出に先立って、明示した書面様式を送付し、同意を得た書面の添付を求める。また、応募書類の提出手段をウェブサイトに指定した場合は、提出手段（フォームなど）の脆弱性対策を講じるとともに、画面に明示した書面様式の内容を表示した上で、同意を得て画面遷移して取得することで同意を得る。

②選考課程において一時保管する個人情報等は、上記の同意を得た利用目的の範囲とし、提出された資料（紙媒体）はキャビネットに収納し施錠保管する。

③採否判定結果は、本人の指定する手段で回答する。なお、本人が指定する手段での回答ができない場合は、その理由を説明した上で回答する。

④不採用となった方の個人情報等は、①または面接時に同意を得た期間を満了したものを社内でシュレッダーにて細断廃棄する。

⑤④で完了した期日を同意書又は面接時の社内資料にその旨を明記し記録する。

A.7.1.2　雇用条件

従業員及び契約相手との雇用契約書には，情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。

業務に従事する者と情報セキュリティに関する各自の責任及び組織の責任を明記した以下の書面を手交する。

①直接雇用する者とは、「就業規則」または「雇入れ通知書」に従って、「誓約書」を取り交す。

②出向者とは、「出向契約書」に従って、「誓約書」を取り交す。

③役員とは、「就任承諾書」に従って、「誓約書」を取り交す。

④上記の「誓約書」には、情報の非開示条項を設け、退職後一定期間有効である旨を明記する。

⑤派遣社員とは、派遣会社との秘密保持契約書での情報の非開示条項を適用する。（ＳＥＳ契約での勤務者も同様とする。）

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

経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求しなければならない。

代表者は、従事する者に対し、情報セキュリティ基本方針及びその他の手順に従って業務上、情報セキュリティを遵守するよう、従事に先立って説明し、推進する責任者及び社内体制を周知する。

A.7.2.2　情報セキュリティの意識向上、教育及び訓練

| |
|---|
| 組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受けなければならず，また，定めに従ってその更新を受けなければならない。 |

教育責任者は、「情報セキュリティマネジメントシステムマニュアル」7.3 の規定に従い、当社の情報セキュリティ基本方針及び手順について、従事する者に対し、その業務分掌及び職務権限に応じて、適切な情報セキュリティ意識向上のため、以下の項目を含む事項の教育及び訓練を、年 1 回以上実施する。

なお、新規入社する者には、入社時のオリエンテーションにて、以下の項目を含む事項を臨時教育として実施する。

・情報セキュリティ方針
・情報セキュリティパフォーマンスの向上によって得られる便益を含む、ISMS の有効性に対する自らの貢献
・ISMS 要求事項に適合しないことの意味

A.7.2.3　懲戒手続

| |
|---|
| 情報セキュリティ違反を犯した従業員に対して処置をとるための，正式かつ周知された懲戒手続を備えなければならない。 |

ISMS に関する定めに違反した者は、A.7.1.2 にて手交した「誓約書」に従って「就業規則」を適用し懲戒処分とする。

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

| |
|---|
| 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，その従業員又は契約相手に伝達し，かつ，遂行させなければならない。 |

雇用および契約終了時は、A.7.1.2 にて手交した「誓約書」に従って、情報の非開示条項が、退職後一定期間有効であることを確認する。

重要な情報セキュリティの取扱い部署からの異動者については、上記に準じた情報の非開示条項を盛り込んだ「誓約書」に手交することで確認する場合もある。

## 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

| |
|---|
| 情報，情報に関連するその他の資産及び情報処理施設を特定しなければならない。また，これらの資産の目録を，作成し，維持しなければならない。 |

当社の情報資産は、業務上の必要性に基づいて保有していることから、業務の流れ及び情報の所在を参照しながら情報資産を「情報資産リスクアセスメント表」に特定し、維持する。

【情報資産リスクアセスメント表管理項目】

情報資産名

情報資産評価および資産分類

保管期間

情報の区分

情報資産内容

資産の管理責任者

委託先(あれば)

A.8.1.2　資産の管理責任者

| |
|---|
| 目録の中で維持される資産は，管理されなければならない。 |

「情報資産リスクアセスメント表」に資産の保有者を明確にする。

「情報資産リスクアセスメント表」での資産の管理責任者は、情報セキュリティのリスクを運用管理することについて，責任及び権限をもつ者とし、リスク所有者とする。

リスク所有者は、情報セキュリティのリスクを運用管理する実務を行わせるため、情報資産への制限されたアクセス権が付与する。

A.8.1.3　資産利用の許容範囲

| |
|---|
| 情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施しなければならない。 |

管理責任者は、「情報資産リスクアセスメント表」で特定された業務並びに取扱い場所などを勘案し、「情報資産リスクアセスメント表・補票」に情報セキュリティ目的とリスク基準及びリスク受容基準を定め、資産の管理責任者を指名する。

当社では、資産の管理責任者は、原則として部門責任者とする。特別のプロジェクト等、社内施設での横断的な業務執行の責任者がある場合は、業務分掌及び職務権限に基づき、管理責任者が、その任にあるものを任命する。

A.8.1.4　資産の返却

| |
|---|
| 全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，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。 |

A.7.3.1 に従って、雇用の終了又は変更に該当した者は、離任した組織の情報資産の全てを返却する。

返却を受けた管理責任者は、全ての組織の情報資産であることを確認する。

上記外の契約にて、組織の情報資産を利用してきた者がある場合は、契約満了又は終了の合意時に利用してきた組織の情報資産の全てを返却する。

返却を受けた管理責任者は、全ての組織の情報資産であることを確認する。

A.8.2　　情報分類

目的:組織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

| |
|---|
| 情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類しなければならない。 |

「情報資産リスクアセスメント表」での情報資産評価および資産分類の基準は、「情報資産リスクアセスメント表・補票」にて見直し、法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から決定し、「情報資産リスクアセスメント表」に反映する。

A.8.2.2　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。 |

A.8.2.1 にて「情報資産リスクアセスメント表」に反映された組織が採用した情報分類体系に従って、情報のラベル付けなど容易に認識できる表示とする。

A.8.2.3　資産の取扱い

| |
|---|
| 資産の取扱いに関する手順は，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。 |

当社は、「情報資産リスクアセスメント表・補票」にて定められた基準及び、A.8.1.3 に従い、資産の運用責任者が所管管理する。

A.8.3　　媒体の取り扱い

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　取り外し可能な媒体の管理

| |
|---|
| 組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施しなければならない。 |

当社では、以下を携行可能な記憶媒体とする。

①CD-R,CD-RW,DVD-R,DVD-RW 等

②USB メモリ等

③外付け HDD 等

携行可能な記憶媒体の使用は、当社の指定する利用目的のもと、指定された場所及び区域、指定された条件下での利用以外は禁止とする。

顧客より情報の授受のために指定された場合は、その旨を管理責任者に申告し、承認を得た条件でのみ利用を許可する。

A.8.3.2　媒体の処分

| |
|---|
| 媒体が不要になった場合は，正式な手順を用いて，セキュリティを保って処分しなければならない。 |

社内で使用された記憶媒体（ハードディスクも含む）が、更新などの理由にて不要となったものは、記録されている情報を消去削除した上で、初期化または指定された上書き消去を行った後、物理的に破砕し再使用不能な状態にして処分する。

機器内部に設置され、社内で物理的に破壊ができない場合は、管理責任者の指定する委託

廃棄事業者に依頼し、処分記録を残す。

A.8.3.3　物理的媒体の輸送

| |
|---|
| 情報を格納した媒体は，輸送の途中における，認可されていないアクセス，不正使用又は破損から保護しなければならない。 |

社外でモバイル機器を取り扱うものは、A.6.2.1で許可されたものに限定し、貸与されているモバイル機器に重要情報を保存してはならない。

また携行時は、紛失防止に注意し、移動は直行直帰とし、許可されていない社外での保管は禁止とする。

顧客などの指定により、携行可能な記憶媒体を使用することをA.8.3.1で許可されたものは、許可を得た手順で移送送付を行わなければならない。

＜持参の場合＞

重要な資料であることを識別できる荷姿として、携行する鞄等に収納し、他の資料と混同しないように注意する。

経路は使用時に申告した経路（社用車、公共交通）とし、経路中においても、車中に放置せず、絶えず携行する。

引き渡し時には、授受記録にて記録する。引き受け時も同様とする。

＜郵送または宅配便などの配送の場合＞

送付中に破損しないよう、クッション材等で梱包し、配達記録の残る手段で配送する。

## 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

目的：情報及び情報処理施設へのアクセスを制限するため。

A.9.1.1　アクセス制御方針

| |
|---|
| アクセス制御方針は，業務及び情報セキュリティの要求事項に基づいて確立し，文書化し，レビューしなければならない。 |

当社のアクセス制御方針は、A.8.1.2「情報資産リスクアセスメント表」に従って、資産の管理責任者であるリスク所有者がISMSの管理責任者として設定付与する。

アクセス制御方針としては、付与する権限として以下を考慮する。

①閲覧参照権限、②更新変更権限、③ダウンロード権限

アクセス制御方針は、「情報資産リスクアセスメント表」の定期的（更新など）に、「情報資産リスクアセスメント表・補票」の見直しとして、管理責任者がレビューする。

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

| |
|---|
| 利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供しなければならない。 |

A.9.1.1に従って設定された当社のアクセス制御方針に従って、ネットワークおよびネットワークサービスへのアクセス権を付与する際には、予めA.8.1.2「情報資産リスクアセスメント表」に従って、資産の管理責任者であるリスク所有者がISMSの管理責任者として設定付与するものとする。

顧客を含む社外の利用者を含む場合は、利用者との利用約款等に応じた範囲のアクセス権を設定し付与する。

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

| |
|---|
| アクセス権の割当てを可能にするために,利用者の登録及び登録削除についての正式なプロセスを実施しなければならない。 |

A.9.1.1 アクセス制御方針による、A.8.1.2「情報資産リスクアセスメント表」に従って、資産の管理責任者であるリスク所有者が ISMS の管理責任者として設定付与する。

部門責任者は管理責任者に報告した 「情報資産リスクアセスメント表」に従って、運用管理する者へのアクセス権付与を申請する。

アクセス制御方針は、「情報資産リスクアセスメント表」の定期的（更新など）に、「情報資産リスクアセスメント表・補票」の見直しとして、管理責任者がレビューする。

A.9.2.2　利用者アクセスの提供

| |
|---|
| 全ての種類の利用者について,全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために,利用者アクセスの提供についての正式なプロセスを実施しなければならない。 |

A.9.2.1 の手順に従って、管理責任者として設定付与されていないアクセス権は無効とする。

A.9.2.3　特権的アクセス権の管理

| |
|---|
| 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。 |

当社は日常的な運用に特権的なアクセス権の利活用は禁止する。

機器の更新や修繕など、緊急かつ包括的な割り当てを要する場合は、管理責任者が特権的アクセス権を一時的に付与することができる。

付与する場合は、付与する者が法人であっても運用責任者を特定し、始期と終期を明示した上で、承認した場合に限る。

付与された者は、完了を報告し、報告を受け、管理責任者は速やかに利活用を停止する。

A.9.2.4　利用者の秘密認証情報の管理

| |
|---|
| 秘密認証情報の割当ては，正式な管理プロセスによって管理しなければならない。 |

A.9.2.1 の手順に従って、管理責任者として、秘密認証情報のアクセス権を付与する場合は、以下の手順とする。

①社内でアクセス権を発行する場合は、初回仮パスワードを発行し、付与者に通知する。
　付与者がシステム要件に準じた運用パスワードを登録し設定する。

②社外から指定されたアクセス権である場合は、付与者に口頭等で伝達する。

A.9.2.5　利用者アクセス権のレビュー

| |
|---|
| 資産の管理責任者は,利用者のアクセス権を定められた間隔でレビューしなければならない。 |

A.9.1.1「情報資産リスクアセスメント表」の定期的（更新など）に、A.12.4.1 にて取得したイベントログとともに、管理責任者がレビューする。

A.9.2.6　アクセス権の削除又は修正

| |
|---|
| 全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除しなければならず，また，変更に合わせて修正しなければならない。 |

A.7.1.2 での雇い入れ時、A.7.3.1 での離職時など、追加更新及び移動削除が確定したことを確認した場合は、管理責任者として追加更新及び移動削除する。

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　秘密認証情報の使用

| |
|---|
| 秘密認証情報の利用時に,組織の慣行に従うことを,利用者に要求しなければならない。 |

A.9.2.4 の手順に従って、利用者に付与されたアクセス権に伴う秘密認証情報（パスワード等）の利用時には、以下の事項を利用者は遵守する。

①秘密認証情報（パスワード等）は利用者以外の目に触れないようにする。

②パスワード等をシステム内に記憶させないこと（オートコンプリートの使用禁止)。

③パスワード等は、定期的にまたは随時、変更すること。

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

| |
|---|
| 情報及びアプリケーションシステム機能へのアクセスは，アクセス制御方針に従って，制限しなければならない。 |

A.9.1.1 にて設定されたアクセス権によってのみ、情報及びアプリケーションシステム機能へのアクセスが出来るものとして制限する。

A.9.4.2　セキュリティに配慮したログオン手順

| |
|---|
| アクセス制御方針で求められている場合には,システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御しなければならない。 |

システム及びアプリケーションにアクセスする際には、付与されたアクセス権に従った秘密認証情報でログオンする。

秘密認証情報は、付与されたものを特定する ID と、付与された本人を識別するパスワードを設定し管理する。

A.9.4.3　パスワード管理システム

| |
|---|
| パスワード管理システムは，対話式でなければならず，また，良質なパスワードを確実とするものでなければならない。 |

A.9.3.1 に従い、運用するパスワードは、8 文字以上（英数混合）にて設定し、秘密認証情報は他人に教えたりしないこととする。

A.9.4.4　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。 |

A.9.2.3 に準じ、特権的なユーティリティプログラムの使用は、以下に限定する。

機器の更新や修繕など、緊急かつ包括的な割り当てを要する場合は、管理責任者が特権的なユーティリティプログラムの使用を一時的に許可することができる。

許可する場合は、許可する者が法人であっても運用責任者を特定し、始期と終期を明示した上で、承認した場合に限る。

許可された者は、完了を報告し、報告を受け、管理責任者は速やかに利活用を停止する。

A.9.4.5　プログラムソースコードへのアクセス制御

| |
|---|
| プログラムソースコードへのアクセスは，制限しなければならない。 |

当社は、プログラムソースコードへのアクセスは禁止とする。

A.9.2.3 に準じ、プログラムソースコードへのアクセスは、以下に限定する。

機器の更新や修繕など、緊急かつ包括的な割り当てを要する場合は、管理責任者がプログラムソースコードへのアクセスを一時的に許可することができる。

許可する場合は、許可する者が法人であっても運用責任者を特定し、始期と終期を明示した上で、承認した場合に限る。

許可された者は、完了を報告し、報告を受け、管理責任者は速やかに利活用を停止する。

## A.10　　暗号

A.10.1.　暗号による管理策

目的：情報の機密性，真正性及び／又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

| |
|---|
| 情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施しなければならない。 |

情報を保護するための暗号化の措置として、以下の手順を講じる。

①メール添付ファイルにて、重要情報を送信する際には、ファイルにパスワードを設定する。パスワードは、受信者との約定での指定されたもの、または、添付送信メール以外の手段にて通知する。

②インターネット等の通信経路を活用して送受信する際には、通信経路として SSL などの

秘匿化された経路とする。

③社内通信網に無線 LAN を接続し運用する際には、WPA2 以上の暗号化の設定とし、アクセスポイントなどの秘匿化の設定とする。

A.10.1.2　鍵管理

| |
|---|
| 暗号鍵の利用，保護及び有効期間（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施しなければならない。 |

暗号鍵の使用は、管理責任者の承認を得た場合のみとする。

## 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

| |
|---|
| 取扱いに慎重を要する又は重要な情報及び情報処理施設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。 |

社内区画を以下の物理的セキュリティ境界を以下の基準で設定し、入退出を制限する。

①応接共用区画

（来訪者応対や荷受け等の区画）

②執務運用区画

（通常業務の作業区画）

③保護管理区画

（制限された情報の管理区画）

④隔離保全区画

（管理責任者の許可を要する区画）

A.11.1.2　物理的入退管理策

| |
|---|
| セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護しなければならない。 |

訪問者の入室・退室手続及び識別方法を以下の基準で設定し、入退出を制限する。

・訪問者が入退できるのは①応接共用区画に限定する。

・②執務運用区画への入室は、従業者が同行し退室まで確認する場合のみ許可する。

・③保護管理区画、④隔離保全区画は、いずれも管理責任者の許可を得て、管理責任者または管理責任者の指名した者の同行し退室まで確認する場合のみ許可する場合がある。

出入口の解錠及び施方法を以下の基準で設定し、入退出を制限する。

・施設入口のシリンダー錠と機械警備のセキュリティキーの解施錠によって入退室制限する。貸与者は、管理責任者が許可した者とする。

・①応接共用区画の入口は、施設入口内側より解錠し、応接時以外は施錠する。

・②執務運用区画の入口は、出退勤時に認証システムにて管理。就業時間中は常時開放とする。

・③保護管理区画及び④隔離保全区画は、管理責任者が保管する鍵で解錠する。入室する際には、管理責任者の許可を得る。

A.11.1.3　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，適用しなければならない。 |

A.11.1.1 で設定した物理的セキュリティ境界としての区画は、独立した区画として、A.11.1.2 物理的入退管理策を適用した解施錠された区画とする。

A.11.1.4　外部及び環境の脅威からの保護

| |
|---|
| 自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計し，適用しなければならない。 |

施設は、火災、洪水、地震、その他の自然又は人為的災害による損害に対する物理的な保護を以下の基準で考慮する。

①防火：区画は適法な防火区画で構成され、防火設備が配置されていること。

②風水害：区画内にある窓などの開口部からの漏水の可能性の有無の確認がされていること。

③地震：機器の固定及び耐震や免振装置の要否の確認がされていること。

④電源：非常電源や停電時の復旧設備の要否の確認がされていること。

⑤盗難：区画の施錠、電子警備等の設備の要否の確認がされていること。

A.11.1.5　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手順を設計し，適用しなければならない。 |

②執務運用区画③保護管理区画④隔離保全区画では、区画内に保管されている情報（情報機器を含む）をキャビネット又は袖机などでの施錠保管とし、鍵は、管理責任者が保管管理し、当該情報の管理者に１本貸与する。

サーバ等の社内共用情報機器は、サーバラックなどに収納し、施錠管理する。サーバラックは、規模に適合した耐震又は免振機能を施し、固定補強する。

A.11.1.6　受渡場所

| |
|---|
| 荷物の受渡場所などの立寄り場所，及び認可されていない者が施設に立ち入ることもあるその他の場所は，管理しなければならない。また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離さなければならない。 |

①応接共用区画での来訪者応対や荷受け等に際しては、以下の手順とする。

・応接共用区画には、重要情報を放置してはならない。打合せなどで持ち出す場合でも、常時携行し、残置してはならない。

・荷受け時は、呼び出された従業者が受け付け、②執務運用区画に搬入する。

・発送時は、荷受け事業者の引き取りまで、②執務運用区画内に保管する。

A.11.2　　装置

目的：資産の損失，損傷，盗難又は劣化，及び組織の業務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

| |
|---|
| 装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し，保護しなければならない。 |

情報関連機器の設置方法はA.11.1.4 にて考慮された基準で設定し、保護する。

A.11.2.2　サポートユーティリティ

| |
|---|
| 装置は，サポートユーティリティの不具合による，停電，その他の故障から保護しなければならない。 |

情報関連機器の設置方法はA.11.1.4 にて考慮された基準で設定し、保護する。

A.11.2.3　ケーブル配線のセキュリティ

| |
|---|
| データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護しなければならない。 |

データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線を含む設備は、④隔離保全区画に準じたものとする。

また、社内に配線されている箇所は、重要な結線等を頻繁な通行導線のある場所とせず、配線に負荷がかからないよう考慮し配線網を構築する。

A.11.2.4　装置の保守

| |
|---|
| 装置は，可用性及び完全性を継続的に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。 |

情報関連機器の保守は、導入時に確認された設置事業者の提示する保守内容を精査した上で、継続的な可用性及び完全性の維持を可能とするため、保守するものとする。

必要に応じて保守契約を委託し、定期的に確認する。

A.11.2.5　資産の移動

| |
|---|
| 装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出してはならない。 |

A.6.2.1 モバイル機器の方針に従って許可されたモバイル機器以外を社外に持ち出すことを禁止する。

A.11.2.6　構外にある装置及び資産のセキュリティ

| |
|---|
| 構外にある資産に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用しなければならない。 |

A.6.2.1 モバイル機器の方針に従って許可されたモバイル機器の社外での利用に際しては、A.6.2.2 テレワーキングでの取扱いに加え、以下の取り扱い手順に従うこととする。

①会社貸与の携帯電話の取扱

・盗難・紛失等を考慮し、パスワード設定等の機器個別のセキュリティを必ず設定すること。
・当社内での携帯電話のカメラ機能使用は禁止する。
・不特定多数の人間がいる場所（例：駅、公共の場所、レストラン等）での機密情報等の情報レベルが高い通話は禁止する。
・搭載されているメモリに業務情報の保存は行わないこと。
・業務上やむを得ない場合を除き、携帯電話で業務用のメールを送受信しないこと。
・緊急時を除き私用での通話は禁止する。

②個人所有の携帯電話の取扱
・業務での使用を許可された際に、会社貸与の携帯電話の取扱に準じた取扱いとする。
・USB でスマートフォンを会社のネットワークに接続しないこと。

A.11.2.7　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全ての装置は，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って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。 |

記憶媒体を内蔵した全ての装置は，処分又は再利用する際には、A.8.3.2 媒体の処分に従って、処分又は再利用を行う。

なお、処分又は再利用を行う前に、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を「情報資産リスクアセスメント表」に従って確認し、管理責任者の確認を得ることとする。

A.11.2.8　無人状態にある利用者装置

| |
|---|
| 利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にしなければならない。 |

当社の無人状態にある装置として、社内サーバ等の夜間定時バックアップ等の装置運用に際して、装置の状況を遠隔監視で確認し、異常の有無を確認するとともに、バックアップ媒体等の設定と無停電装置等の保護措置の状況も確認する。

A.11.2.9　クリアデスク・クリアスクリーン方針

| |
|---|
| 書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用しなければならない。 |

当社のクリアデスク方針及びクリアスクリーン方針を以下の手順とする。

①クリアデスク方針
・業務又は作業でキャビネットから出庫した書類及び取外し可能な記憶媒体は、作業完了後、速やかに出庫した場所に戻し、机上に放置してはならない。
・作業にて作成し出力した確認帳票などは、確認作業完了後、確定し保存するものはファイルし、廃棄するものは、シュレッダー等で細断処分すること。

②クリアスクリーン方針
・業務や作業で情報機器にてファイルを開いたまま、離席してはならない。

・離席する場合は、必ずログオフを行うものとするか、予めスクリーンセーバー5 分以内でパスワードロックがかかるの設定をすること。

## 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

| |
|---|
| 操作手順は，文書化し，必要とする全ての利用者に対して利用可能にしなければならない。 |

管理責任者は、個別情報システムの事業上の重要性を考慮し、当社が定めるリスク許容レベルを満たすために必要な場合、操作手順として文書化する。

#### A.12.1.2　変更管理

| |
|---|
| 情報セキュリティに影響を与える，組織，業務プロセス，情報処理設備及びシステムの変更は，管理しなければならない。 |

管理責任者は、情報処理設備及び情報システムを変更する際は、これを明確にし、全ての関係者に周知させる。

#### A.12.1.3　容量・能力の計画作成

| |
|---|
| 要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。 |

個別の情報システムの主な実務管理者（部門責任者）は、業務上の要求事項に基づく必要なシステム性能を確保するために、情報システムを監視し、将来必要とされる容量・能力を予測した計画を作成し、管理責任者に報告する。

#### A.12.1.4　開発環境、試験環境及び運用環境の分離

| |
|---|
| 開発環境，試験環境及び運用環境は，運用環境への認可されていないアクセス又は変更によるリスクを低減するために，分離しなければならない。 |

情報システムの試験環境は、稼働している運用環境から分離し、社内において顧客環境を再現し設定する場合であっても、稼働している社内のネットワークとは分離した環境で行う。

### 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

| |
|---|
| マルウェアから保護するために，利用者に適切に認識させることと併せて，検出，予防及び回復のための管理策を実施しなければならない。 |

情報システムが悪意のあるコードやコンピュータウイルスに感染する可能性がある場合としての脆弱性対策について、管理責任者はそれらを検出、防止する手段を導入する。

具体的には、稼働する OS のセキュリティパッチ等の自動更新設定を行い、かつウイルス対策ソフトを稼働させ、同様にセキュリティパッチ等の自動更新設定を行う。

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

| |
|---|
| 情報，ソフトウェア及びシステムイメージのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査しなければならない。 |

管理責任者は、情報資産としてのデータを保全するため、社内サーバに保存されているデータを定期的にバックアップとして保存する。

具体的には、サーバに接続する外付けストレージ（又はNAS（Network Attached Storage））に、毎日差分を夜間定時に取得し、毎週日曜にフルバックアップを取得する設定で自動バックアップを行う。

管理責任者は、保存されている状況を定期的に確認する。

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

| |
|---|
| 利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューしなければならない。 |

管理責任者は、社内の情報システムへの付与したアクセス権に従って、利用者の行動、例外事項、情報セキュリティ事象を記録した監査ログを取得し、将来の調査及びアクセス制御の監視を補うために、3ヶ月以上保存する。

また、監査ログについては定期的にレビューをする。

A.12.4.2　ログ情報の保護

| |
|---|
| ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護しなければならない。 |

管理責任者は、ログ機能及びログ情報を改ざん及び認可されていないアクセスから保護するため、管理責任者のみがアクセス可能な領域にログ機能及びログ情報を保存する。

A.12.4.3　実務管理者及び運用担当者の作業ログ

| |
|---|
| システムの実務管理者及び運用担当者の作業は，記録し，そのログを保護し，定期的にレビューしなければならない。 |

個別の情報システムの主な実務管理者（部門責任者）及び運用担当者は、作業内容について記録する。

また、作業ログについては定期的にレビューする。

A.12.4.4　クロックの同期

| |
|---|
| 組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは，単一の参照時刻源と同期させなければならない。 |

管理責任者は、当社のサーバ及び情報機器について、その時刻を外部のタイムサーバと同

期する。

なお各情報端末は、当社のサーバと時刻の同期する設定とする。

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

| |
|---|
| 運用システムに関わるソフトウェアの導入を管理するための手順を実施しなければならない。 |

業務用システムでのソフトウェアの導入（更新・変更など）は、個別の情報システムの主な実務管理者（部門責任者）の提案を受け、管理責任者が承認し、行う。

A.12.6　技術的ぜい弱性管理

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

| |
|---|
| 利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに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なければならない。さらに，それらと関連するリスクに対処するために，適切な手段をとらなければならない。 |

管理責任者は、利用中の業務用システムの技術的脆弱性に関する情報は、時期を失せずに獲得する。

また、脆弱性に当社がさらされていることまたは顕在化していることを認識した際には、A.16.1.4 情報セキュリティ事象の評価及び決定に従い、情報セキュリティ事象について評価し、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。

A.12.6.2　ソフトウェアのインストールの制限

| |
|---|
| 利用者によるソフトウェアのインストールを管理する規則を確立し，実施しなければならない。 |

利用者によるソフトウェアのインストールを含む情報機器の環境設定は、利用開始時の引き渡し時の設定を超えたソフトウェアのインストールは禁止する。

設定環境が維持されていることを定期的なシステム監査時に、ソフトウェアのインストール状況として確認する。

A.12.7　情報システムの監査に対する考慮事項

目的：運用システムに対する監査活動の影響を最小限にするため。

A.12.7.1　情報システムの監査に対する管理策

| |
|---|
| 運用システムの検証を伴う監査要求事項及び監査活動は，業務プロセスの中断を最小限に抑えるために，慎重に計画し，合意しなければならない。 |

情報システムの監査の実施は、次のとおりとする。

①ISMS の規程類等の修正等の実施に即して適時行うこと。

②運用状況の監査は、年次の監査実施計画に基づき行うこと。

③その他必要に応じて随時監査を行うこと。

## 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

目的：ネットワークにおける情報の保護，及びネットワークを支える情報処理施設の保護を確実にするため。

#### A.13.1.1　ネットワーク管理策

| |
|---|
| 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，ネットワークを管理し，制御しなければならない。 |

管理責任者は、当社が構築する社内ネットワークについて、リスク分析に基づき許可された利用者が許可されたシステム及びアプリケーションに対しアクセスできるようにし、一定の可用性を保証するとともに、外部からの不正なアクセスを防止する構成として構築する。

#### A.13.1.2　ネットワークサービスのセキュリティ

| |
|---|
| 組織が自ら提供するか外部委託しているかを問わず，全てのネットワークサービスについて，セキュリティ機能，サービスレベル及び管理上の要求事項を特定しなければならず，また，ネットワークサービス合意書にもこれらを盛り込まなければならない。 |

社外のネットワークサービスを利用する場合は、業務委託管理の定めに従い、ネットワークサービスを選定し、セキュリティ機能、サービスレベル及び管理上の要求事項を特定確認した上で、ネットワークサービス合意書にもこれらを盛り込まなければならない。

#### A.13.1.3　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，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。 |

情報サービス、利用者及び情報システムは、ネットワーク上で、付与したアクセス権に基づき、グループごとに分離する。

### A.13.2　　情報転送

目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。

#### A.13.2.1　情報転送の方針及び手順

| |
|---|
| あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えなければならない。 |

通信設備を利用した情報転送方針及び手順を、以下の基準とする。

①電子メールの場合

・メールアドレスを発行した者に情報転送の手段としての利用を認める。
・情報転送に際しては、A.10.1.1 暗号による管理策の利用方針に従って、転送する情報を記録したファイルにパスワードを設定する。
・パスワードは、受信者との約定での指定されたもの、または、添付送信メール以外の手段にて通知する。

②外部ストレージの場合

・当社が指定した外部ストレージを活用する場合のみ、情報転送の手段としての利用を認める。

・外部ストレージの指定する手順に従って、転送する情報を記録したファイルをアップロードし、転送先に通知する。

・通知した格納先は、外部ストレージとの約定に従って、一定期間後、消去される。

A.13.2.2　情報転送に関する合意

| |
|---|
| 合意では，組織と外部関係者との間の業務情報のセキュリティを保った転送について，取り扱わなければならない。 |

組織と外部関係者の間で、情報転送する場合には、合意を得て実施する。

具体的には、A.13.2.1 情報転送の方針及び手順に従って、組織と外部関係者の間で合意を得る。

A.13.2.3　電子的メッセージ通信

| |
|---|
| 電子的メッセージ通信に含まれた情報は，適切に保護しなければならない。 |

電子メール自体にて情報を転送する場合には、以下の基準とする。

①本文には、送信意図を明確に示し、機密情報を含む添付ファイル等で転送すべき内容を直接記述してはならない。

②タイトルは、電子メールの内容が類推できるものとし、受信者に電子メールの主旨が伝わるよう配慮する。

③電子メールの宛先誤送信による、事業への悪影響を防止するため、受信者（宛先）の電子メールアドレスは、宛先はメールの文書を打ち終わった後に正確に入力し、送信前に再度確認する。

④必要に応じて、CC や BCC を利用し、関係者に情報を伝達するようにする場合も、誤送信とならないよう再度確認する。

⑤添付ファイルサイズは、受信者の電子メール受信環境を考慮し、送信する。

⑥電子メールの送信は、ウイルス対策ソフトウェアが導入されているパソコンから行う。

⑦ファイルを添付する場合は、必ずウイルスが感染していないことを確認する。

A.13.2.4　秘密保持契約又は守秘義務契約（当社内業務、外部委託）

| |
|---|
| 情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューし，文書化しなければならない。 |

管理責任者は、以下の秘密保持契約又は守秘義務契約を文書化し、関係者と手交し、保管し、レビューする。

①お客様：秘密保持契約書

②従業員：誓約書

③協力会社：秘密保持契約書

## A.14　　情報システムの取得、開発及び保守

### A.14.1　　情報システムのセキュリティ要求事項

目的：ライフサイクル全体にわたって，情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには，公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。

#### A.14.1.1　セキュリティ要求事項の分析及び仕様化

| |
|---|
| 情報セキュリティに関連する要求事項は，新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない。 |

当社の情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含め、考慮する。

#### A.14.1.2　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

| |
|---|
| 公衆ネットワークを経由するアプリケーションサービスに含まれる情報は，不正行為，契約紛争，並びに認可されていない開示及び変更から保護しなければならない。 |

当社は、公衆ネットワークを経由するアプリケーションサービスを利用しない。

利用する場合は、公衆ネットワークを経由するアプリケーションサービスに含まれる情報でのセキュリティは、不正行為，契約紛争，並びに認可されていない開示及び変更から保護するものとする。

#### A.14.1.3　アプリケーションサービスのトランザクションの保護

| |
|---|
| アプリケーションサービスのトランザクションに含まれる情報は，次の事項を未然に防止するために，保護しなければならない。<br>－ 不完全な通信<br>－ 誤った通信経路設定<br>－ 認可されていないメッセージの変更<br>－ 認可されていない開示<br>－ 認可されていないメッセージの複製又は再生 |

アプリケーションサービスのトランザクションに含まれる情報を、不完全な通信経路および認可のない開示等から保護するものとする。

未然に防止する事項としては、次の事項を考慮する。

－ 不完全な通信
－ 誤った通信経路設定
－ 認可されていないメッセージの変更
－ 認可されていない開示
－ 認可されていないメッセージの複製又は再生

### A.14.2　　開発及びサポートプロセスにおけるセキュリティ

目的：情報システムの開発サイクルの中で情報セキュリティを設計し，実施することを確実にするため。

#### A.14.2.1　セキュリティに配慮した開発のための方針

| |
|---|
| ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用しなければならない。 |

当社は、ソフトウェア及びシステムの開発は行わない。
ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。
当社は、「情報資産リスクアセスメント表」に従って、セキュリティに配慮した開発を行うこととする。

A.14.2.2　システムの変更管理手順

| |
|---|
| 開発のライフサイクルにおけるシステムの変更は，正式な変更管理手順を用いて管理しなければならない。 |

開発のライフサイクルにおけるシステムの変更は、部門責任者の提案を受け、管理責任者の承認を得た正式な変更管理手順を用いて管理する。

A.14.2.3　オペレーティングシステムの変更後の業務用ソフトウェアの技術的レビュー

| |
|---|
| オペレーティングプラットフォームを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要なアプリケーションをレビューし，試験しなければならない。 |

オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。

A.14.2.4　パッケージソフトウェアの変更に対する制限

| |
|---|
| パッケージソフトウェアの変更は，抑止しなければならず，必要な変更だけに限らなければならない。また，全ての変更は，厳重に管理しなければならない。 |

パッケージソフトウェアの変更は行わない。
変更を行うことが必要となる場合は、変更に伴うリスクを考慮し、変更計画を管理責任者が承認した範囲で行い、試験を行ったうえで、管理責任者の承認を得て、変更する。

A.14.2.5　セキュリティに配慮した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実装に対して適用しなければならない。 |

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として､A.14.2.1 セキュリティに配慮した開発のための方針を確立し、具体的な原則を文書化し維持し、全ての情報システムの実装に対して適用する。

A.14.2.6　セキュリティに配慮した開発環境

| |
|---|
| 組織は，全てのシステム開発ライフサイクルを含む，システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し，適切に保護しなければならない。 |

当社は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みの

ためのセキュリティに配慮した開発環境を確立し、適切に保護する。

A.14.2.7　外部委託による開発

| |
|---|
| 組織は，外部委託したシステム開発活動を監督し，監視しなければならない。 |

システム開発を外部委託する場合は､A.15.1.2 供給者との合意におけるセキュリティの取扱いに従い、業務委託を行うこと。

A.14.2.8　システムセキュリティの試験

| |
|---|
| セキュリティ機能（functionality）の試験は，開発期間中に実施しなければならない。 |

当社はシステム開発を行わない。

システム開発する場合は、セキュリティ機能の試験は、開発期間中に実施する。

A.14.2.9　システムの受入れ試験

| |
|---|
| 新しい情報システム，及びその改訂版・更新版のために，受入れ試験のプログラム及び関連する基準を確立しなければならない。 |

新しい情報システム、改訂版及び更新版を受け入れる際は、管理責任者の指示により、当該情報システムの部門責任者は、業務上の要求事項を明確にした受け入れ基準を確立し、その基準に基づき受け入れ前に適切な試験を実施する。

あるいは、新規または改訂版、更新版の情報システムが受け入れ基準を満たしていることを確認する。

A.14.3　　試験データ

目的：試験に用いるデータの保護を確実にするため。

A.14.3.1　試験データの保護

| |
|---|
| 試験データは，注意深く選定し，保護し，管理しなければならない。 |

当社はシステム開発を行わない。

システム開発する場合は、試験データは、管理責任者が選定し、適切に保護および管理するものとする。

## A.15.　　供給者関係

A.15.1　　供給者関係における情報セキュリティ

目的：供給者がアクセスできる組織の資産の保護を確実にするため。

A.15.1.1　供給者関係のための情報セキュリティの方針

| |
|---|
| 組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。 |

A.13.2.4 秘密保持契約又は守秘義務契約に従う。

A.15.1.2　供給者との合意におけるセキュリティの取扱い

| |
|---|
| 関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない。 |

A.13.2.4 秘密保持契約又は守秘義務契約に従う。

A.15.1.3　ICT サプライチェーン

| |
|---|
| 供給者との合意には，情報通信技術（ICT）サービス及び製品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に対処するための要求事項を含めなければならない。 |

組織の資産に対する供給者のアクセスに関連するリスクを軽減させるための情報セキュリティ要求事項について、供給者と合意し、契約書や機密保持誓約書へ文書化する。

A.15.2　　供給者のサービス提供の管理

目的：供給者との合意に沿って，情報セキュリティ及びサービス提供について合意したレベルを維持するため。

A.15.2.1　供給者のサービス提供の監視及びレビュー

| |
|---|
| 組織は，供給者のサービス提供を定常的に監視し，レビューし，監査しなければならない。 |

管理責任者は、供給者（委託先）が提供するサービスの取り決めに含まれるセキュリティ管理策、サービスの定義、及び提供のレベルを、委託先が確実に実施、運用、維持していることを監視する。

委託先が再委託をしている場合は、委託先にも再委託先に対し同等の監視をすることを義務付け、管理責任者は、委託先が確実に監視していることをチェックする。

①新規評価

・部門責任者が面接して当社のセキュリティ要件に適合しているか判断し、基本契約書、秘密保持契約書を締結した後「委託先一覧」に登録する。

②継続評価

・セキュリティ講習会に参加しているか？秘密保持誓約の取り交わしが行われているか？

・重大な不適合が起こった場合、

└他にも重大な不適合を発生させていないか

└当社のセキュリティ要件に適合しているか

を確認し、基本契約書、秘密保持契約書に則り再評価する。

A.15.2.2　供給者のサービス提供の変更に対する管理

| |
|---|
| 関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む。）を管理しなければならない。 |

ISMS 事務局は、当社の情報セキュリティ基本方針、ISMS マニュアル、規程、手順等の維持及び改善も含め、委託先によるサービスの提供に対する変更を管理する。

変更には関連する業務システム及びプロセスの重要性と、再度のリスクアセスメントを考

慮に入れなければならない。

## 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

目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む，情報セキュリティインシデントの管理のための，一貫性のある効果的な取組みを確実にするため。

#### A.16.1.1　責任及び手順

| |
|---|
| 情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立しなければならない。 |

ISMS 関連のインシデントの管理は、管理責任者がインシデント管理責任者として、発生したインシデントに対する対応策の検討及び実施と再発防止に関する責任を負う。

#### A.16.1.2　情報セキュリティ事象の報告

| |
|---|
| 情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告しなければならない。 |

情報セキュリティ事故やそれに準ずる（疑わしい場合も含む）インシデントを発見、あるいは質問の問い合わせを受けた役員または従業者は、定められた報告経路に基づき、速やかに報告を行い、対応するものとし、報告内容は、「インシデント報告書」に漏れなく記載しなければならない。

インシデントを発見した役員または従業者は、独自の判断で対応してはならない。

但し、きわめて緊急性を要する場合は、部門責任者、直属の上司、及び複数の従業者の助言を受けて、管理責任者の判断により対応するものとする。

#### A.16.1.3　情報セキュリティの弱点の報告

| |
|---|
| 組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は，どのようなものでも記録し，報告するように要求しなければならない。 |

情報セキュリティ事故やそれに準ずる（疑わしい場合も含む）インシデントを発見した役員または従業者は、即座に事故状況を把握し、口頭で直属の上司に報告しなければならない。発見者は、直属の上司に報告後、「インシデント報告書」に事故の内容を記載しなければならない。

#### A.16.1.4　情報セキュリティ事象の評価及び決定

| |
|---|
| 情報セキュリティ事象は，これを評価し，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。 |

情報セキュリティ事象については、管理責任者はこれを評価し、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する。

#### A.16.1.5　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。 |

情報セキュリティインシデントは、以下の手順に従う。

①原因追求・状況の把握

②対応策の検討

③クライアントおよび社内への伝達

④再発防止策の検討

⑤応急処置の実施

⑥是正処置報告書の報告

A.16.1.6　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の分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。 |

当社において発生したセキュリティ事故やソフトウェア誤動作の種別、及び大きさ等の影響度を、ISMS 事務局にて可能な限り定量化し記録する。

記録を収集した結果を、次回の教育から実施するものとする。

A.16.1.7　証拠の収集

| |
|---|
| 組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない。 |

情報セキュリティインシデント発見後の人又は組織に対するフォローアップ措置が（民事であれ刑事であれ）法的行為にかかわるものである場合、インシデント管理責任者によって、証拠は、該当する司法権のもとで定められた証拠に関する規定に適合するように、収集、保管、及び提示できるようにするため、保全すること。

盗難・不正アクセス等犯罪による可能性が高いインシデントが発生した場合の手順

①警察などへの連絡

②インシデント関連施設の証拠保全

③情報システムのログ管理

④インシデント関連施設利用の停止、あるいは証拠保全に影響のない利用

⑤現場の写真撮影

その他外部機関等の指示に従う。

## A.17　　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　　情報セキュリティ継続

目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込まなければならない。

A.17.1.1　情報セキュリティ継続の計画

| |
|---|
| 組織は，困難な状況（adverse situation）（例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。 |

管理責任者は、組織全体を通じて事業継続のための活動のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う管理された手続きを策定し維持する。

A.17.1.2　情報セキュリティ継続の実施

| |
|---|
| 組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プロセス，手順及び管理策を確立し，文書化し，実施し，維持しなければならない。 |

管理責任者は、重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し実施する。

実施した内容は「事業継続計画・結果」に記録する。

A.17.1.3　情報セキュリティ継続の検証、レビュー及び評価

| |
|---|
| 確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証しなければならない。 |

確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、１年に１度、「事業継続・結果」の管理策を検証する。
実施した内容は「事業継続・結果」に記録する。

A.17.2　　冗長性

目的：情報処理施設の可用性を確実にするため。

A.17.2.1　情報処理施設の可用性

| |
|---|
| 情報処理施設は，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。 |

情報処理施設は、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。

## A.18　　順守

A.18.1　　法的及び契約上の要求事項の順守

目的：情報セキュリティに関連する法的，規制又は契約上の義務に対する違反，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

A.18.1.1　適用法令及び契約上の要求事項の特定

| |
|---|
| 各情報システム及び組織について，全ての関連する法令，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，明確に特定し，文書化し，また，最新に保たなければならない。 |

管理責任者は「法規制一覧表」に記載されている法令等の新規・更新・修正・削除（廃止）があった場合には、直ちにその法令等の要求事項を確認した上で、本規程に反映させ、常に最新の状態で情報を維持するものとし、定期的および随時、更新等の有無について確認する。

また、更新などを確認し、「法規制一覧表」を更新した場合は、管理責任者は社内情報伝

達ツールを用いて、更新内容を役員及び従業者に速やかに通達する。通達文書を掲示し、従業員は確認の捺印をする。

特に「法規制一覧表」に特定する法令等に改正等により要求事項に変更があり、本規程での既存の内容では要求事項を満たさず違反することが無いように見直し、本規程を改定した場合は直ちに社内に周知徹底する。

A.18.1.2　知的財産権

| |
|---|
| 知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を実施しなければならない。 |

管理責任者は、知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，法令，規制及び契約上の要求事項の順守を確実にするため、社内で利用する権利関係のあるソフトウェア製品の契約関係及び許諾事項等を確認し、契約上の要求事項を特定する。

また、社内で利用する他に知的財産権の有する事例がある場合も同様とする。

A.18.1.3　記録の保護

| |
|---|
| 記録は，法令，規制，契約及び事業上の要求事項に従って，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。 |

当社の事業活動並びに日常業務に関わる重要な記録は、法令、規則、契約及び事業上の要求事項に従って、消失、破壊、改ざんから保護し、少なくとも法令等の定める期間、具備しなくてはならない。

A.18.1.4　プライバシー及び個人を特定できる情報（PII）の保護

| |
|---|
| プライバシー及び PII の保護は，関連する法令及び規制が適用される場合には，その要求に従って確実にしなければならない。<br>(PII :Personally Identifiable Information) |

個人情報保護法にしたがうものとし、具体的な要求は、個人情報保護委員会の定める事項を参照する。

A.18.1.5　暗号化機能に対する規制

| |
|---|
| 暗号化機能は，関連する全ての協定，法令及び規制を順守して用いなければならない。 |

当社は、暗号化機能を要する利用はない。行う場合は、以下の原則とする。

暗号の使用については、その使用を統制する国による協定、法律、規制、又はその他の手段に適合しなければならない。

A.18.2　　情報セキュリティのレビュー

目的：組織の方針及び手順に従って情報セキュリティが実施され，運用されることを確実にするため。

A.18.2.1　情報セキュリティの独立したレビュー

| |
|---|
| 情報セキュリティ及びその実施の管理（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）に対する組織の取組みについて，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。 |

情報セキュリティおよびその実施のマネジメントに対する組織の取組みについて、あらかじめ計画した間隔で、又はセキュリティの実施に重大な変化が生じた場合に、マネジメントレビューする。

A.18.2.2　情報セキュリティのための方針群及び標準の遵守

| |
|---|
| 管理者は，自分の責任の範囲内における情報処理及び手順が，適切な情報セキュリティのための方針群，標準類，及び他の全てのセキュリティ要求事項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。 |

情報セキュリティ及びその実施のマネジメントに対する組織の取組みは、マネジメントレビューで、又はセキュリティの実施に重大な変化が生じた場合に、独立したレビュー-を実施する。

A.18.2.3　技術的遵守のレビュー

| |
|---|
| 情報システムを，組織の情報セキュリティのための方針群及び標準の順守に関して，定めに従ってレビューしなければならない。 |

必要な場合には、適切なソフトウェアツールによる助けを得て、技術的順守の点検を実施する。