情報セキュリティ規程

ISO/IEC27001:2013

Ver.1.1

2019/12/04

株式会社アンサー

社外秘

承認	作成
五十嵐　一郎	小沼　慶征

目　次

1 アクセス権限管理手続

1.目的

本手続は、社内業務用途の情報システムに保持されている電子データの保護の為に必要な論理的アクセス権に関する事項を定めることを目的とする。ここでいう論理的アクセスとは、電子データに対して作成、閲覧、変更または削除を行うことをいう。システムの利用者は、オペレーティングシステムまたはアプリケーションプログラムを利用して電子データに論理的にアクセスする。この権利を論理的アクセス権という。オペレーティングシステムへのアクセスは，本アクセス権限管理に基づいたログオン手順によって制御すること。業務委託を受けて開発する情報システム、社外に向けた情報サービスのための情報システムなど社内利用目的以外で開発するシステムについては、原則として別途同等の手続方法を規定することとし、本手続は適用しない。

2.論理的アクセス権限管理体制の整備

（１）　ISMS 管理責任者ならびに開発部の情報管理者への特権付与

ISMS 管理責任者または開発部の情報管理者は、オペレーティングシステム、ユーティリティソフト及びアクセス管理ソフトの全機能を利用または管理する権限を付与された管理者ユーザ（以下、特権ユーザという）の権限を取得することが出来る。

（２）　ISMS 管理責任者への権限付与

開発部の情報管理者は、ISMS 管理責任者に対して、ISMS 管理責任者が開発部の情報管理者による論理的アクセス権限の設定等の管理業務のモニタリングを行うことが出来る権限を付与する。

3.アクセス権限の設定管理

（１）　アクセス権限の設定方針の作成

情報管理者は、自らが管理する電子データに対する論理的アクセス権限の設定基準書を作成しなければならない。

＜関連文書＞ 「**アクセス権限設定基準書**」

（２）　最小権限の付与

論理的アクセス権限は、業務上必要最小限の範囲で付与しなければならない。

（３）　アクセス権限の付与

情報管理者は、自らが管理する電子データに対する論理的アクセス権限の設定方針に基づき、ISMS 管理責任者または開発部の情報管理者に、利用ユーザの論理的アクセス権限の付与を申請するものとする。
ISMS 管理責任者または開発部の情報管理者は、情報管理者からの申請に基づいて論理的アクセス権限の設定作業を行わなければならない。

（４）　アクセス権限の変更・削除

情報管理者は、自らが管理する電子データ及びその電子データを扱うアプリケーションプログラムのユーザ（以下、ユーザという）から申請を受けた場合、または、自らが必要と認めた場合には、ISMS 管理責任者または開発部の情報管理者に対し、論理的アクセス権限の変更または削除の申請を行うものとする。
ISMS 管理責任者または開発部の情報管理者は、情報管理者からの申請に基づいて論理的アクセス権限の変更または削除作業を行わなければならない。

（５）　プログラムのインストールの制限

アプリケーションプログラムは、ISMS 管理責任者または開発部の情報管理者が許可を与えたプログラム以外はインストールしてはならない。業務上の必要性から、その他のプログラムをインストールする場合には、ISMS 管理責任者または開発部の情報管理者の承認を得た上でインストールしなければならない。

（６）　ユーティリティソフト等の利用制限

ユーティリティソフト（システム開発の補助やオペレーティングシステムの管理に利用される汎用ソフトウェア）及びシステム監査ツール（システム監査やモニタリングに利用されるソフトウェア）は、業務上必要な者のみが利用出来るように論理的アクセス権限を設定しなければならない。
アクセス管理ソフト（論理的アクセス権限を設定する専用ソフトウェア）は、ISMS 管理責任者または開発部の情報管理者に限り利用することが出来る。

（７）　アクセス権限設定状況の査問

情報管理者は、電子データに対するユーザの論理的アクセス権限の設定状況を定期的（**6**ヶ月）に確認しなければならない。

（８）　特権ユーザ設定状況の査問

内部監査責任者は、特権ユーザとその権限の設定状況を定期的（**6**ヶ月）に確認しなければならない。

4.ユーザ認証

開発部の情報管理者は、ユーザ ID、パスワードなどの「秘密認証情報」をユーザごとに発行し、それによってユーザ認証を行う。

ユーザ認証システムは、「対話式」とし、自動ログオンや ID/パスワードをウェブブラウザに記憶させることは認めない。

5.ユーザ ID（秘密認証情報を含む）の管理

（１）　ユーザ ID の付与

ユーザ ID は、ユーザからの申請に基づき ISMS 管理責任者または開発部の情報管理者が付与する。

（２）　ユーザ ID の削除

ユーザ ID が不要になった場合は、ユーザは速やかに ISMS 管理責任者または開発部の情報管理者にその旨を申請し、ISMS 管理責任者または開発部の情報管理者は、ユーザ ID を削除する。

（３）　ユーザ ID の変更

ユーザ ID の変更の必要性が生じた場合は、ユーザからの申請に基づき、ISMS 管理責任者または開発部の情報管理者が変更を行う。

（４）　ユーザ ID の存在確認

ISMS 管理責任者または開発部の情報管理者は、定期的（６ヶ月） に登録されているユーザ ID の棚卸を実施し、不要なユーザ ID を確認した場合には、速やかに削除しなければならない。

6.パスワード管理

（１）　最小文字数

ユーザの使用するパスワードは、パスワード解読ソフトウェア等で容易に解読されないよう、適切な文字数（英数字の組み合わせ 6 文字以上）以上設定しなければならない。

システム管理者及びシステム運用担当者の使用する特権ユーザのパスワードについても、**8** 文字以上で設定しなければならない。

（２）　パスワードの複雑性

パスワードは少なくとも文字と数字を組み合わせたものとし、容易に推測されないよう、一般的な単語、氏名等、容易に推測出来るものをパスワードに設定してはならない。

特権ユーザのパスワードは、特殊文字の利用も考慮するものとする。

（３）　パスワードまたは鍵の有効期限

特権ユーザは、同一パスワードを**１２**ヶ月以上使用してはならない。

（４）　パスワードファイルのアクセス管理と暗号化

パスワードを保存するファイルに対するアクセス権限を適切に設定し、復元が事実上不可能な暗号化によってパスワードを保護しなければならない。

（５）　最高試行回数

短期間で複数回を超えるログインの失敗があった場合は、一定時間内の再ログインを禁止しなければならない。
開発部の情報管理者は、ログインの失敗理由を調査し、必要に応じて適切な措置を講じなければならない。具体的な最高試行回数及び再ログイン許可時間等に関しては別途、定めることとする。

（６）ファイルサーバ上の共有フォルダ の設定

ファイルサーバ上に共有フォルダを設ける場合、当該フォルダへのアクセス権を確実に設定する。

7.アクセスログの管理

（１）　アクセスログの設定

機密情報を取り扱うまたは保管してあるサーバについては、アクセスログ（情報またはそれを取り扱うプログラム等の利用状況を監視する目的で記録されるログ）を取得しなければならない。
情報管理者は、ログ取得が必要な場合、情報システム管理者と協議の上、あらかじめアクセスログを取得する条件及び項目を決定しなければならない。

（２）　アクセスログの査閲

情報管理者は、記録したアクセスログを定期的に査閲しなければならない。情報管理者は、開発部の情報管理者にその業務を委託し、結果の報告を受けることも出来る。

（３）　アクセスログの保護

開発部の情報管理者は、アクセスログ機能及びアクセスログ情報を改ざん及び許可されていないアクセスから保護するために、許可された者のみがアクセスログにアクセス出来るようにシステムを設定しなければならない。

2 ネットワーク管理手続

1.目的

本手続は、ネットワークの安全・信頼性を確立し、通信の安定的な提供、通信の疎通の確保、通信の秘密の保護などを主な目的とすることで、ネットワークを取り巻くさまざまな脅威に対する耐障害性を強化し、その安定的な維持を図ることを目的とする。

2.ネットワーク運用手順

（１）ネットワーク運用手順の策定

開発部の情報管理者は、異常時の復旧手順を含めたネットワークの運用体制及び運用手順を策定し、ISMS 管理責任者の承認を得なければならない。

（２）運用手順の見直し

開発部の情報管理者は、最新のセキュリティに関する技術や業界動向に関する情報を入手すると共に、入手情報に基づいて適宜運用手順の見直しを行わなければならない。

3.ネットワークシステム計画

（１）適切なネットワークシステム計画の立案

開発部の情報管理者は、ISMS 管理責任者の指示の下、ネットワークシステムの計画を立案し、ISMS 管理責任者の承認を得なければならない。

（２）ネットワーク接続業者との契約

ネットワーク接続業者の回線、又は設備を利用して情報の通信を行う場合は、その情報の機密性、可用性、完全性を維持する性能に優れた回線又は回線契約形態を選択しなければならない。

開発部の情報管理者は、必要事項をネットワーク接続業者との契約内容に織り込むと共に、必要に応じてネットワーク接続業者が契約内容を遵守していることを確認するものとする。

（３）ネットワーク運用継続計画

開発部の情報管理者は、ネットワークを継続的に運用できるよう、機器構成、人員を考慮した計画を立案しなければならない。

4.ネットワークの設定

（１）文書化されたネットワーク設定記録とその保護

開発部の情報管理者は、ネットワークの概略を文書化又は図式化しなければならない。ネットワークの構成等に関する情報は、特定の者のみがアクセスできるよう適切に管理をしなければならない。

＜関連文書＞ 「**ネットワーク構成図**」

（２）ネットワークアクセス制御

当社のネットワーク及びサーバに接続する場合は、正当な権限を有する者のみがアクセスできなければならない。

認証手段については、アクセスする情報及び情報システムに求められるセキュリティに応じて適切な手段を選択しなければならない。又、適切な経路制御を行い、ネットワーク上の経路は管理されなければならない。

また、無線 LAN を設置する場合は、適用範囲外（廊下など）からの第三者による接続を予防するための措置（ステルス化、WEP2 以上の設定など）をとらなければならない。

（３）サーバルームのサーバ及びネットワーク機器のセキュリティ

サーバルームのサーバ及びネットワーク機器は、必要最小限の者のみがアクセスできるよう設置又は設定を行わなければならない。又、重要なサーバ上で稼動するネットワークサービスについては、必要最小限の機能を動作させることとし、業務上必要の無い機能は停止又は閉鎖しておかなければならない。

（４） 設定のための情報収集

開発部の情報管理者は、ネットワーク機器やサーバのセキュリティの弱点や不正アクセス等に関する情報を平素から収集かつ共有し、適切な対策を講じなければならない。

収集した情報については、必要に応じて ISMS 管理責任者に報告するものとする。

（５） ネットワーク設定更新手続

ネットワーク構成の設定変更に際して、更新内容が情報システムに重要な影響を及ぼす可能性があると判断される場合には、開発部の情報管理者は事前に ISMS 管理責任者の承認を得ると共に、更新前の状態にいつでも復帰可能な状態にしたうえで作業を進めなければならない。

5.ネットワークの分離

「**情報取扱管理手続**」で規定されている「極秘」以上に分類される電子データを保管している部門のネットワークは、物理的に分離するか又は論理的に分離して必要な者のみが必要なサービスのみ利用できるよう制御しなければならない。

6.ネットワークの監視

（１） ネットワークの利用状況の監視

開発部の情報管理者は、必要に応じて、ネットワークについてその利用状況を監視する機能を設け、アクセスした者及びそのアクセス内容についてログを取得し、一定期間保存しなければならない。取得したログは、業務上必要な者のみが必要に応じて閲覧できるよう適切に管理をしなければならない。

（２） 通信状況の監視

開発部の情報管理者は、回線の負荷状況等を含む通信状況を監視すると共に、故障や通信の途絶等を速やかに検知し、対処しなければならない。

（３）監視ログの取扱

開発部の情報管理者は、ネットワークの利用状況及び通信状況の監視ログを定期的に分析し、分析結果を監視ログと共に一定期間保存しなければならない。分析結果に応じて調査を行い、必要に応じてシステム変更の手続を講じるものとする。

7.不正アクセス行為の検知

（１）不正アクセス行為の禁止

従業者等による情報システム、ネットワーク資源の使用は、業務上必要な場合に限定することとする。従業者等は、業務上必要な場合を除き、ネットワーク上の情報を盗聴するような監視ソフトウェアやネットワークの設定や状況を探索するセキュリティソフトウェア及びネットワークに不正に侵入するために用いられるプログラム等は使用してはならない。

（２）不正アクセス行為の検知

権限の無いユーザによるログイン試行行為などの不正アクセスが行われた場合に、これを検出し、各情報管理者又は情報システム管理者に知らせる機能を必要に応じて設けなければならない。

（３）不正アクセス行為の報告

不正アクセス行為を発見した場合には、各情報管理者は、「**事故・障害対応手続**」に従って遅滞無く報告しなければならない。

（４）不正アクセス行為の対策

開発部の情報管理者は、不正アクセス等への対処を含めた具体的な危機管理対策を文書化し、ISMS 管理責任者の承認を得ると共に、必要に応じて適宜見直さなければならない。

（５）不正アクセス行為発生時の措置

異常が検知された場合に、ネットワーク及びサーバ等の機能を停止又は切り離し、関係機関等と協力して被害の状況を把握し、被害の拡大を防止するための措置を講じなければならない。

（６）不正アクセス行為の再発防止

開発部の情報管理者は、攻撃の分析及び原因の究明を行い、関係機関等と協力して再発防止のための措置を講じなければならない。

3 物理アクセス管理手続

1.目的

本手続は、物理的な不正アクセスから情報資産を保護するため、情報機器の取扱い及び施設へのアクセス全般に関する事項を定める。

2.セキュリティエリアの明確化

本手続で対象とする物理的なセキュリティエリアは、下記の通りとする。

本社	〒101-0021 東京都千代田区外神田 6-16-9 外神田千代田ビル 7F	レベル０：エレベーターホール レベル１：応接室 レベル２：執務室 レベル３：サーバラック

レベル１：退社時施錠
レベル２：カードキーまたは立会による入室管理
レベル３：常時施錠

＜関連文書＞「**セキュリティエリアレイアウト図**」

3.情報の設置

情報管理者は、機密情報（「情報取扱管理手続」参照）が保持されている機器をレベル 2 以上の立入り制限が実施されている部屋に設置しなければならない。

4.施錠管理

（１）退出時施錠箇所の施錠確認

従業者は、全ての人員がエリアを退出する際には、各エリアの退出時施錠箇所について施錠を確認しなければならない。

（２）常時施錠箇所の施錠

従業者は、各エリアの常時施錠箇所について、開錠後はできるだけ速やかに施錠するものとし、正当な理由なく開錠したままにしてはならない。

従業者は、全ての人員がエリアを退出する際には、各エリアの常時施錠箇所について施錠を確認しなければならない。

5.入退室管理

（１）セキュリティエリアへの入室

情報処理施設の主管部署の長（以下、施設管理者という）は、レベル２以上のセキュリティエリアへの入室の際、個人を識別して入室を制限しなければならない。識別方法としては、従業者証の着用、カードキー等を用いた入室制限、見知らぬ第三者の立ち入りに対する声かけ等がある。

（２）従業者の各エリアへの入室の承認と権限付与

各エリアへの従業者の入室権限は、ISMS 管理責任者承認の下で施設管理者が付与しなければならない。

（３）従業者以外の第三者の入室

レベル２以上のセキュリティエリアへ従業者以外の第三者が入室する場合（物品の配達、機器等の受渡し等を含む）には、そのエリアへ入室権限のある従業者が付き添わなければならない。

（４）入退室リスト

レベル２以上のセキュリティエリアへの入退室者は、従業者・訪問者を問わず氏名、会社、訪問目的、時間等を所定の「**入退室記録**」に記録しなければならない。

（５）入退室記録の保存

施設管理者は、入退室記録を１年以上保存しなければならない。

（６）入退室記録の調査

施設管理者は、適宜、入退室記録を調査し、その妥当性を確認しなければならない。

（７）入退室ログの取得

施設管理者は、カードキー等による入退室管理を行っている場合には、その入退室ログ（カードキー管理システムが記録するログ。以下、同様）を取得しなければならない。

（８）入退室ログの取扱い

施設管理者は、入退室ログを適切に保管管理しなければならない。

（９）入退室ログの保護

施設管理者は、入退室ログの改竄防止策を取らなければならない。

（10）入退室ログの分析

施設管理者は、セキュリティ事故が発生した場合、必要に応じて入退室ログの内容を分析し ISMS 管理責任者へ報告しなければならない。

（11）入退室ログの保存

施設管理者は、入退室ログを 1 年以上保存しなければならない。

6.その他

（１）装置の保護

レベル 2 未満のセキュリティエリア外（当法人の敷地内含む）、またはレベル 2 以上のセキュリティエリア内の無人エリアに設置されている装置は、誤用等のリスクを考慮した対策を施さなければならない。

また、レベル 2 未満のセキュリティエリア外（当法人の敷地内含む）に装置を設置する場合には、ISMS 管理責任者の許可を得なければならない。

また、レベル 2 以上のセキュリティエリア内に設置されている装置は、自然災害や悪意のある攻撃からの保護を考慮した対策を施さなければならない。

（２）機密情報機器の設置基準

従業者は、機密情報が保持されている機器を「耐火、耐震、耐水」、「電圧、静電気、電磁波、気温、湿度」等を考慮した環境に設置しなければならない。

（３）機密情報機器保管施設の明示の禁止

情報管理者は、機密情報機器が保管される施設の出入り口等にその所在を明示してはならない。

（４）機密情報機器の直接操作

機密情報機器への直接操作は、情報管理者が操作を許可した者に限定しなければならない。

また、情報管理者が許可した目的による直接操作に限定しなければならない。

（５）クリアデスク

従業者は、特に退出時に、書類あるいはメディアをその重要性に応じて引き出しまたは施錠可能なキャビネットに保管しなければならない。

（６）クリアスクリーン

従業者は、席を離れる場合、コンピュータのスクリーンロックまたはログオフ、または電源の切断を行わなければならない。

従業者は、長時間席を離れる場合、コンピュータのログオフ、または電源の切断を行わなければならない。

4 情報取扱管理手続

1.目的

本手続は、当法人における情報資産に対して、機密の重要度合いに応じた取扱いについて定めることを目的とする。

2.機密情報管理

（１）　情報の機密区分・情報のラベル付け

情報の機密区分及び取扱い基準を以下のとおり定義する。

- 極 秘：情報の漏洩により回復が容易ではない信用損失が発生する情報
- 機密：NDA 対象文書等、当事者または特定の関係者以外に漏洩してはならない情報
- 社外秘：社外に漏洩してはならない情報
- その他：「極秘」、「機密」「社外秘」以外の情報

「極秘」「機密」「社外秘」の情報を「機密情報」という。尚、個人情報の機密区分は「極秘」とする。

（２）　機密区分・情報のラベル付けの見直し

ISMS 管理責任者は、情報の機密区分及び取扱い基準の妥当性については、ISMS のマネジメントレビュー時に必要に応じて見直さなければならない。

（３）　機密情報の取扱い

各部署の情報管理者は、以下のような場合、ISMS 管理責任者に申請をおこなわなければならない。
NDA(秘密保持契約)により、その取り扱いが規定されている場合はそれにしたがう。

・　新規に機密情報を取得する場合

・　機密情報を破棄する場合

・　機密情報を開示する場合

- 機密情報を複製する場合
- 機密情報を社外へ持ち出す場合
- 社外秘情報を翌日に渡り社外に持ち出す場合
- ISMS 記録を破棄する場合

（４） 機密情報の破棄

各部署の情報管理者は、情報の形態に応じ以下の方法で破棄しなければならない。

- 機密情報を含んだ文書情報は、シュレッダーもしくは溶解処分
- 機密情報を含んだ記憶媒体は、ツールによる再読不可能処理もしくは破砕処理

（５） 機密情報の保管

各部署の情報管理者は、機密情報を含んだ可搬媒体及び文書を施錠可能な場所へ保管し、また電子情報の機密情報は「**アクセス権限管理手続**」にしたがい、適切なアクセス制限を設定しなければならない。

（６） 守秘義務契約の締結

各部署の情報管理者は、機密情報を第三者へ「開示」、「授受複製」、「提供」及び「破棄処理を委託」する場合は、守秘義務契約を締結しなければならない。

（７） 機密情報に関する会話

機密情報を扱う者は、第三者との会話の中で当該情報を漏洩してはならない。また、機密情報を扱う者同士が、公然で機密情報に関する会話をしてはならない。

（８）　携帯端末等の取扱い（ノート PC、スマートフォン、携帯電話、タブレット等のモバイル機器）

機密情報を扱う者は、機密情報を保存した携帯端末等を不特定多数の人物が公然と機密情報を閲覧できるような状態で放置してはならない。例えば、情報を画面に表示したまま放置してはならない。

機密情報を扱う者は、機密情報を保存した携帯端末等を放置してはならない。

携帯端末等の持込または持ち出しは、その旨を各部署の情報管理者に申請し、承認を得なければならない。「**端末持込・持出申請書**」

携帯端末には次の事項を考慮しなければならない。

- パスワード、PIN ナンバー等によるロックの設定
- 業務に使用しないアプリケーションのインストールの制限
- ウィルス、マルウェア等からの保護
- 私用の携帯端末は業務で使用せず、業務用 PC に接続しない

（９）　機密文書の再利用

機密文書（紙媒体）を扱う者は、機密文書を再利用（メモ帳や裏紙として利用など）してはならない。

（１０）　情報機器及び磁気媒体の再利用

情報管理者は、機密情報を保存してある情報機器及び磁気媒体を再利用する場合、初期化して再読不可能な状態にしなければならない。

（１１）　音声・映像の通信設備及びファクシミリによる機密情報の通信

機密情報を音声・映像の通信設備で通信する際には、第三者に漏洩の危険が無いことを確認し通信しなければならない。

機密情報をファクシミリで通信する際には、通信開始時に第三者に漏洩の危険が無いことを確認するとともに、通信先と通信開始の連絡を取り合ったうえで通信をおこなわなければならない。通信後の機密文書は**(5) 機密情報の保管**にしたがい、適切に管理しなければならない。

（１２）　電子メールによる機密情報の送信

機密情報を扱う者は、機密情報を電子メールによって送信する際に暗号化をおこなわなければならない。

また、機密情報を電子メールによって送信する際には、誤送信を防ぐために、ダブルチェック等により必ず宛先を確認しなければならない。

（１３）　暗号方式

ISMS 管理責任者は、暗号方式について社内標準を明確にしなければならない。（パスワードつき ZIP ファイル）。また、暗号に鍵を利用する場合には、その鍵の管理を適切におこなわなければならない。

（１４）　社内標準の暗号方式

機密情報を扱う者は、情報を暗号化する場合、社内標準の暗号方式を使用しなければならない。

（１５）　機密情報の郵送、輸送

機密情報を郵送する者は、二重化など通常の包装より厳重に包装しなければならない。また、通達確認のできる方法で郵送をおこなわなければならない。また、当該機密情報の情報管理者が必要と認めた場合には、暗号化をおこなわなければならない。また、機密情報を輸送する者は、機密情報を格納した鞄を体から離してはならない。

（１６）　機密情報の守秘扱い

役員及び従業員は、業務上知りえた機密情報を部外者及び社外の第三者との会話・電話・ファクシミリ等を通じて漏洩してはならない。

（１７）　印刷機、複写機ならびにファクシミリにおける機密情報の取扱い

各部署の情報管理者は、印刷機、複写機ならびにファクシミリを設置する際には、「**物理アクセス管理手続**」に規定されるレベル２以上の情報セキュリティエリアに設置しなければならない。

従業者は、自身が印刷した機密情報を含む文書を速やかに受け取ることとし、印刷機上に文書を放置してはならない。

従業者は、複写機ならびにファクシミリにセットした機密情報を含む原稿について、読み取り完了後速やかに回収することとし、複写機ならびにファクシミリ上に原稿を放置してはならない。また、ファクシミリが印刷した文書については、手近の者が速やかに宛先の者に届けることとし、ファクシミリ上に文書を放置してはならない。

（１８）　可搬性を持つ記憶媒体における機密情報の取扱い

USB 端子等により一時的に端末に接続して情報を保管することのできる記憶媒体（USB メディア）、バックアップメディア、端末から取り外した記憶媒体の取扱いについては、機密情報を含む場合、**(8)携帯端末**と同等に取扱うものとする。

3.情報処理設備の管理

（１）　情報処理設備の認可

従業者は、機密情報を格納または処理するための情報処理機器を導入するにあたり、ISMS 管理責任者または開発部の情報管理者の事前の許可を得なければならない。

（２）　情報処理設備の記録

従業者は、機密情報を格納または処理するための情報処理機器を導入した際、管理部門の情報管理者に報告し、情報・情報資産台帳への追記を依頼しなければならない。

4.データ保全

（１）　記憶媒体の交換

各部署の情報管理者は、記憶媒体の劣化状況を定期的に確認し、必要に応じて媒体を交換しなければならない。

（２）　情報の恣意的な変更

従業者は、情報を恣意的に変更してはならない。

5.知的所有権

（１）　知的所有権の管理責任

ISMS 管理責任者は、知的所有権に対する管理責任の所在を明確にしなければならない。

（２）　知的財産の取扱い

特許出願前の知的財産等は、極秘の機密区分に分類し、管理しなければならない。

（３）　第三者の知的所有権

従業者は、第三者の知的所有権を尊重し、侵害してはならない。

5 個人情報保護管理手続

1.目的

本手続は、事業運営上必要な個人情報の取扱いに関して、その取得、利用、提供、開示、廃棄を適切に行う手順を確立し、維持するための責任及び行動を定めることを目的とする。

2.適用範囲

本手続が対象とする個人情報の範囲は、当社の管理下にある全ての個人情報とする。

3.個人情報の取得

（１）個人情報の取得担当者は、個人情報の取得時（取得後も含む）には、その利用目的を情報主体に通知（文書または口頭）もしくは公表（ホームページ上など）する。

但し、個人情報の取得、利用又は提供の目的が一般的に明らかである場合（たとえば、契約書等の表題等で本人が目的を理解していると判断される場合、市場調査又は統計処理等に利用する場合）で、本人が取得に応じている場合は、本人の同意を得ているとみなすこととする。

4.個人情報の利用

（１）取得した個人情報の利用に関しては、管理責任者が適切に管理する。管理方法は、当社の「**個人情報保護規程運用マニュアル**」及び「**個人情報保護規程**」その下位手続類に従うものとする。

（２）取得目的の範囲を超えて個人情報の利用を行う場合、又は本人以外から間接的に個人情報を取得した場合において、個人情報の提供・預託を行うことが予定されている場合は、その旨を本人に通知し、同意を得る。

5.個人情報の提供・預託

（１）個人情報の提供

以下の a) から e) の条件に該当し、個人情報を第三者に提供する場合、当該個人情報の管理責任者は、その内容の妥当性を確認する。

a) 法令に基づく場合

b) 人の生命、身体又は財産の保護のために必要であるが、本人の同意を得ることが困難である場合

c) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要があるが、本人の同意を得ることが困難である場合

d) 国の機関もしくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要があるが、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがある場合

e) 既に通知してある利用目的に第三者への提供が含まれており、その内容として、提供する個人情報の内容、提供方法、及び本人の求めに応じた第三者への提供の停止が含まれている場合

（２）個人情報の預託

① 取引先から個人情報の預託を受ける場合は、その内容の妥当性を確認の上で承認し、担当者に作業を指示する。
② 預託を受ける取引先とは、契約等により責任の所在を明確にする。

6.個人情報の開示・訂正

（１）情報主体から個人情報の開示・訂正・削除及び第三者への提供拒否の要請があった場合、受付担当者は本人確認を行い、本人である事を確認する。

（２）当該個人情報の管理責任者は、その内容の合理性を確認の上で承認し、担当者に作業を指示する。情報主体からの要請は合理的な範囲内で応じるものとする。但し、合理的な範囲を超えている場合であっても、要請の理由や状況から本人の権利保護の必要性が高いと判断した場合は、要請に応じることとする。

（３）個人情報の開示方法は、郵送による書面で開示を行う。

（４）個人情報の訂正および利用停止は、結果を情報主体に照会し、その適切性を確保する。

（５）個人情報の廃棄は、“7 個人情報の廃棄”に従う。また、廃棄後、情報主体にその旨を連絡する。

（６）個人情報の第三者への提供拒否は、それに伴う情報主体への影響（サービスの制限等）を通知し、合意を得る。

7.個人情報の廃棄

（１）個人情報を廃棄する場合は、当該個人情報の管理責任者の承認の上で廃棄を行う。

6 業務委託管理手続

1.目的

本手続は、当法人が第三者と締結するすべての業務委任契約あるいは業務請負契約（以下、委託契約という）に関して必要な秘密保護に関する事項を手続する。

ここでいう委託契約とは、第三者に当法人の業務を委任あるいは第三者が当法人の業務を請け負うにあたり、第三者と交わす契約をいう。また、その契約により、当法人の業務を委任する業者及び当法人の業務を請け負う業者を委託業者という。

2.委託先の信用調査と選定

当法人が第三者との間に委託契約を締結する場合は、費用面のみならず委託先の経営状態、実績、情報セキュリティレベル等を考慮して慎重に選定を行わなければならない。

3.守秘義務契約

（１）　守秘義務契約の締結

「情報取扱管理手続」で定義された「機密情報」を取扱う可能性のある委託業者と委託契約を締結する場合は、守秘義務契約を締結しなければならない。

（２）　委託業者が重要情報を扱う場合

委託業者が、業務委託契約の業務を遂行するにあたって、「機密情報」の中でも特に重要な情報を扱うと情報管理者が認めた場合は、当該委託業者のみならず当法人と当該業務に携わる個人との間に秘密保持誓約書を別途入手しなければならない。

4.委託業者の再委託

委託業者が当該業務の遂行に関して第三者との間に委託契約を締結すること（以下、再委託という）は原則として禁止し、その旨を契約書に記載する。但し、当初の委託業者（以下、一次委託業者という）との間で、次の内容を記載した誓約書等を事前に取り交わす場合はこの限りではない。

- 一次委託業者と二次委託業者（再委託事業者）との間に当法人と一次委託業者との間と同等以上の秘密保持契約を結ぶ旨
- 二次委託業者が、当該秘密保持契約に違反し、当法人に損害を与えた場合にも一次委託業者が当法人に対する損害賠償責任等を免れない旨
- 二次委託業者が再委託を行わない旨
- 二次委託業者が当該誓約書等に違反したことが明らかである場合は、当法人は一次委託業者との間の委託契約を破棄できる旨

5.進捗管理

業務委託に関する管理者は、委託先から、業務の進捗、品質管理について定期的に報告を受け、進捗状況を把握しなければならない。

6.その他の契約時の考慮事項

業務委託契約を締結する際には、上記の事項以外にも必要に応じて次の事項を考慮しなければならない。

- 資産保護に関する事項
- 達成されるサービスレベルに関する事項
- 契約当事者それぞれの義務に関する事項
- 知的所有権及び著作権の取扱いに関する事項
- 委託した業務に対する監視に関する事項
- 関係者への情報セキュリティに係る訓練に関する事項
- 当 ISMS で取り決められた管理策への遵守に関する事項
- その他、ISMS 管理責任者、又は業務委託に関する管理者が必要と判断した事項

7 情報システム開発管理手続

1.目的

本手続は、当社が開発する情報システム及びソフトウェアへのセキュリティの組み込みを確実にするとともに、その維持を目的とする。

2.定義

（１）情報システム：当社が開発するシステムの総称（社内業務用途に開発するものならびに社外向け情報サービスのために開発するもの。業務委託を受けて開発するものは含めない。）

（２）ソフトウェア：当社が外部から購入する OS 及びパッケージソフトウェアの総称

（３）開発担当者：開発を行う者で、アウトソーシング先の担当者を含む

（４）試験データ：開発において使用するデータ等

3.情報システム及びソフトウェアのセキュリティ仕様の承認

既存の関連セキュリティ管理策及びリスク評価に基づくセキュリティ要件を明確にし、仕様に盛込まなければならない。また、情報管理者は、必要なセキュリティ仕様が盛込まれていることを確認し、承認しなければならない。

内容	変更実施者・報告者	承認者	記録
開発着手時	開発担当者	情報管理者	仕様書又は議事録
開発中及びリリース後の仕様	開発担当者	情報管理者	仕様変更書又は議事録

4.情報システム及びソフトウェアの技術的レビューと試験

以下の観点に基づき、技術的レビューを実施しなければならない。

① 入出力データの妥当性
② 定められたセキュリティ要件の実装

③　内部処理情報の破壊を検出するための妥当性確認
④　メッセージの完全性
⑤　出力データの妥当性確認
⑥　その他、情報管理者が必要と判断した事項

内容	試験実施者・報告者	承認者	記録
開発中の試験	開発担当者	情報管理者/情報システム管理者	テスト計画書または報告書
リリース後の変更に伴う試験	開発担当者	情報管理者/情報システム管理者	テスト計画書または報告書

5.開発環境と本番環境の分離

開発環境と本番環境は、原則として分離し、移行作業は定められた手順に従って実施しなければならない。

6.システム試験データの管理

開発部の情報管理者は開発着手時に試験データ管理責任者を定め、保護及び管理を確実にする。また、本番データを試験データとしてはならない。

7.プログラム・ライブラリへのアクセス管理

開発担当者への ID・パスワードの付与は、「アクセス権限管理手続」に従って実施し、プログラムソースライブラリ及びデータファイルへのアクセス権を明確にしなければならない。

8.電子商取引

開発部の情報管理者は、電子商取引について、不正行為、認可されていない開示または改ざんから取引を保護するために、SSL 等適切な暗号化技術を導入しなければならない。また、取引の成立又は不成立に関する紛争の回避等のために、否認防止の手段（例えば、取引内容に関する最終確認の実施）を講じなければならない。

9.オンライントランザクション

開発部の情報管理者は、電子商取引などにおける取引データ及び個人情報データのオンライントランザクションについて、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、認可されていない複製又は再生から情報を保護するために、クライアントインターフェイスのセキュリティ実装（セッションハイジャック、クロスサイトリクエストフォージェリ等への対策）、システムのネットワーク構成ならびにデータベースサーバのセキュリティ実装について、システムの正式運用を開始する時点までに検証を行わなければならない。検証の結果問題が認められるときは、是正を確認するまでシステムの正式運用を開始してはならない。

8 情報システム運用管理手続

1.目的

本手続は、当社が運用する情報システム及びソフトウェアへのセキュリティの組み込みを確実にするとともに、その維持を目的とする。

2.定義

（１）情報システム：当社が開発するシステムの総称（社内業務用途に開発するものならびに社外向け情報サービスのために開発するもので、業務委託を受けて開発するものは含めない。）

（２）ソフトウェア：当社が外部から購入する OS 及びパッケージソフトウェアの総称

（３）開発担当者：開発を行う者で、アウトソーシング先の担当者を含む

（４）試験データ：開発において使用するデータ等

3.操作手順書

（１）操作手順書の作成

開発部の情報管理者は、必要に応じて以下の内容を含む操作手順書を作成し、維持管理しなければならない。

①システム運用

②障害対応（障害発生時の対処方法等）

③運用記録の保持及び運用変更の管理

④管理者による定期的な運用記録、運用変更の精査

（２）操作手順書の承認

内容	変更実施者・報告者	承認者	記録
運用開始前	運用管理担当者	開発部の情報管理者	操作手順書又は議事録
運用中	運用管理担当者	開発部の情報管理者	操作手順変更書又は議事録

4.運用変更管理手順書

（１）開発部の情報管理者は、以下の内容を例とする情報処理施設・設備及び運用システムの変更管理に関する手順書を作成し、維持管理しなければならない。

①重要な変更の識別及び記録

②そのような変更の潜在影響の評価

③提案される変更の正式な申請と承認手順

④変更の詳細について、全関係者への通知

⑤情報システムプログラムの変更作業は開発担当者が行うこと

⑥データの修正は運用管理担当者が行うこと

⑦ソフトウェアの変更は極力行わないこと

⑧ソフトウェアの購入は信頼のおける業者から行い、その使用等を管理すること

⑨新規、アップグレード及び新バージョンの情報システム及びソフトウェアは、受入れ試験を実施すること

（２）運用変更管理手順書の承認

内容	変更実施者・報告者	承認者	記録
運用中	運用管理担当者	開発部の情報管理者	運用変更管理手順書又は議事録

5.システム計画の作成及び受入れ

（１）処理能力及び記憶容量計画の作成

開発部の情報管理者は、新しい事業及びシステム要求事項並びに組織の情報処理における現在の傾向及び予想される傾向を考慮して、将来も十分な処理能力及び記憶容量が確実に得られるよう、容量需要を監視して将来の容量の要求を予測し、処理能力及び記憶容量計画の作成をしなければならない。

（２）処理能力及び記憶容量計画の承認

内容	試験実施者・報告者	承認者	記録
計画開始前	開発担当者	開発部の情報管理者	処理能力・記憶容量計画書又は議事録
運用中	開発担当者	開発部の情報管理者	処理能力・記憶容量計画変更書又は議事録

6.保守

（１）関連機器の保守実施

関連機器の保守は、製造元、又は購入先の作成したマニュアルに従い、実施すること。

（２）保守作業用ポートのアクセス管理

情報システムにおいてネットワーク経由の保守作業用ポートを利用している場合には、そのアクセスは適切に管理をすること。

（３）第三者が提供するサービスのセキュリティモニタリングと運用管理

第三者が提供するサービスを利用している場合、開発部の情報管理者は、第三者が提供するサービスについて契約時の内容が維持されていることを定期的に確認すること。また、提供サービス自体の変更（機能強化、新たなセキュリティ対策の導入等）や当社での利用形態等の変更が生じた場合には、情報セキュリティに関するリスクを再評価し、必要に応じて措置を講じること。

7.コンピュータウィルス、ワーム、スパイウェア、悪質なモバイルコードへの対策

開発部の情報管理者は、次の事項を実施しなければならない。

- ウィルス、ワーム、スパイウェア、悪質なモバイルコードに関する情報について定期的に情報収集を行い、役従業者等に対する注意喚起を行うこと
- サーバ等において、定期的にウィルス、ワーム、スパイウェア、悪質なモバイルコードおよびバックドア等サーバ設定の改ざんに関するチェックを行うこと
- サーバ等において、ウィルス、ワーム、スパイウェア、悪質なモバイルコードのチェック用パターンファイルは、定期的及び緊急時に最新のものに更新すること
- ウィルス、ワーム、スパイウェア、悪質なモバイルコードに感染した場合（ウィルス検知ソフトがウィルスを検知した場合も含む）、もしくは感染した恐れがある場合には、別途定める手順に従い、対応すること

情報システムの利用者は、次の事項を実施しなければならない。

- 利用 PC 等に対して、ウィルス、スパイウェア、悪質なモバイルコードの検知ソフトを常駐設定にし、常時ウィルス、スパイウェア、悪質なモバイルコードの検知ができるようにすること
- 利用 PC 等に対して、定期的にウィルス、スパイウェア、悪質なモバイルコードのチェックを行うこと
- 利用 PC 等に対して、ウィルス、スパイウェア、悪質なモバイルコードのチェック用パターンファイルは常に最新のものに保つこと
- 開発部の情報管理者が提供するウィルス、スパイウェア、悪質なモバイルコードに関する情報を常に確認すること
- PC 等がウィルス、スパイウェア、悪質なモバイルコードに感染した場合（ウィルス検知ソフトがウィルスを検知した場合も含む）、もしくは感染した恐れのある場合には、速やかに開発部の情報管理者に連絡して指示を受けること
- 導入許可されたアプリケーション以外のアプリケーションをインストールしないこと。（Microsoft Internet Explorer 上で動作する ActiveX コントロール等のモバイルコードについても同様であるため注意すること）

8.技術的脆弱性の管理

開発部の情報管理者は、利用中の情報システムに関する技術的脆弱性（セキュリティホール等）に関する情報を常に収集し、技術的脆弱性が発見された時は、速やかにリスク評価を行い、次の基準に基づいて適切な処置を施さなければならない。

（１）緊急度の高いリスクについては、直ちに修正プログラム等による動作検証を行い、可及的速やかにシステムの修正を行う。

（２）緊急度の低いリスク（システムの設定により脆弱性を回避できるもの及び利用者が役員、従業者ならびに業務委託先に限定され注意喚起により脆弱性を回避できるもの（但し、利用者が対策に応じないことでシステムが管理する情報の漏洩、改ざん、破壊を引き起こすもので、利用者に強制的に対策を採らせることができないものを除く）等）については、必要に応じて修正プログラムの動作検証ならびにシステムの修正を実施する。

（３）技術的脆弱性については、以下のウェブサイトを参照する

・IPA　http://www.ipa.go.jp/security/vuln/documents/

・JPCERT　https://www.jpcert.or.jp/vh/top.html

9.その他

（１）重要な業務を行うソフトウェア・端末は、必要に応じて作業時間（接続時間）の制限を設けること

（２）遠隔地から情報システムを利用する場合には、定められた接続方法に従い、行うこと

（３）情報システムにおけるソフトウェアの実施は「アクセス権限管理手続」に従い、管理をすること

9 事故・障害対応手続

1.目的

本手続は、当法人において情報セキュリティに係る障害が発生した場合の速やかな対策の実施を目的とする。

2.範囲

本手続の対象範囲は、当法人が管理する機密情報、サーバ及びネットワーク機器とする。

3.責任

本手続の実施責任者は、部門管理責任者またはプロジェクト管理者とする。

4.実施手順

（１）事故・障害箇所の特定

情報管理者は、事故・障害箇所の特定を行う。

（２）事故・障害中間報告

情報セキュリティ事故、または復旧に要する時間が当該サービス又は業務の可用性の限度を上回る場合、情報管理者は、「**事故・障害報告書**」を ISMS 管理責任者に提出する。又、必要に応じて利用者への事故・障害告知を行う。

（３）復旧

①ハードウェア障害の場合

代替機器に切り替える。又は、障害機器の修繕を迅速に実施する。

②ソフトウェア障害の場合

代替機器に切り替える。代替機器に切り替えられない場合は、バックアップにより障害前の状態に復旧する。

（４）障害報告

情報管理者は、「**事故・障害報告書**」を ISMS 管理責任者に提出する。又、必要に応じて利用者への障害復旧の告知を行う。

（５）是正措置

ISMS 管理責任者は、再現性のある障害の場合には、情報管理者に是正措置の実施を指示し、その結果の報告を受ける。その結果は、「**事故・障害報告書**」に記録する。

JIS Q 27001:2014(ISO/IEC 27001:2013)の規格要求事項又は当法人が定めた ISMS 手順の根本的欠陥に起因する障害については、「**情報セキュリティマニュアル** 」の「**10.1 不適合及び是正処置**」に従い対応する。

（６）障害記録の維持

ISMS 管理責任者は、発生した障害に関して、その記録を維持する。（**事故・障害報告書**）

また、記録には、種類、規模（影響範囲）、被害（想定）額を記載する。

10 事業継続計画手続

1.目的

本手続は、事業活動に対する障害に対処し、重大な障害または災害の影響から重要なビジネスプロセスを保護することを目的とする。また、当手続により組織全体にわたる事業継続を開発・維持するための管理されたプロセスを明確にする。

2.事業継続計画の立案

（１）　業務プロセスの識別

ISMS 管理責任者は、当法人の業務プロセスを分類し、各業務プロセスの継続性について責任を持つ者（以下、業務管理責任者）を定める。

（２）　業務中断の影響の評価

業務管理責任者は、ISMS 管理責任者と協力し、担当業務にどの程度の中断の発生で企業存続に重要な影響を与えるかを評価し、その原因となる事象を識別する。評価は以下の 5 区分による。

① 1 日以内

② 1 日以上

③ 1 週間以上

④ 1 ヶ月以上

⑤長期にわたり復旧が著しく困難な場合

（３）　重要な中断の原因となる脅威の識別

ISMS 管理責任者は、各業務に（２）で評価した以上の中断を与える可能性のある脅威を識別する。識別に際しては以下の脅威を想定し、「**情報セキュリティマニュアル 6.1.2.2 リスク評価**」に従って実施したリスクアセスメントの結果を参照する。

- 天災（地震、水害、火災、落雷等）
- 人災（故意（テロ、犯罪）、誤用等による事故等）
- 公共インフラの不全（電力、水道、ガス、公衆回線等）
- 障害（ハード障害、ソフト障害、ネットワーク障害等）
- 情報セキュリティ侵害（情報の改ざん、破壊、漏えい、サービス妨害等）

（４） 事業継続計画の立案

業務管理責任者は、重要な中断の原因となる脅威が識別された事象に対し、事業継続計画を立案、文書化し、ISMS 管理責任者に提出する。複数の業務に関連する事象については、ISMS 管理責任者が指名した担当者が作成する。

事業継続計画の策定に際しては以下の項目の必要性を考慮する。

- 組織体制と責任の割り当て
- 要員の確保と連絡手段
- 施設、備品、消耗品の確保
- リカバリー時間の決定
- バックアップ手続とリカバリテスト計画、それらの実行
- バックアップメディアの外部保管（物理的アクセスコントロール）
- 復旧用代替施設（ホットサイト・ウォームサイト・コールドサイト、相互施設利用契約、代替ハードウェア施設（ベンダー、サードパーティ））
- 連絡リストの作成（要員、サプライヤ、サービスプロバイダ、保険会社）
- ネットワークの冗長性（代替ルート、二重化、音声）
- 保険（装置と施設、ソフトウェアの再構築、臨時の支出、中断による損失、貴重な書類・記録の価値、損害賠償、等）
- 利用者の遵守事項（利用規約）

（５） 事業継続計画の承認

ISMS 管理責任者は事業継続計画を取りまとめ、「**事業継続計画書**」を作成し、情報セキュリティ委員会の審議を受け、トップマネジメントの承認を得る。

3.事業継続計画の訓練

（１）　訓練の実施

業務管理責任者は、ISMS 管理責任者の協力のもと、立案した事業継続計画が最新で効果的なものであることを確実にするために、定期的にテストし、そのテスト結果を評価しなければならない。

（２）　訓練の要件

定期的なテストは通常の業務の中断を最小限にすることを考慮したものとする。重要な業務であるとトップマネジメントが判断した業務については、計画に含まれるすべての要員が参加し、実際の手順に沿ったテストを実施する。

（３）　訓練の計画

業務管理責任者は、ISMS 管理責任者の協力のもと、すべての種類のテストの実施計画を立案しなければならない。ISMS 管理責任者は、必要に応じてそれぞれのテスト実施時期を調整し、その実施計画についてトップマネジメントの承認を得なければならない。

（４）　訓練結果の保管

ISMS 管理責任者は、テスト結果を「**教育訓練報告書**」に記録し、保管しなればならない。

4.事業継続計画の見直し

（１）　定期的な見直し

業務管理責任者と ISMS 管理責任者は、定期的に実施する訓練の結果、保守の優位性の評価に基づき事業継続計画を見直し、トップマネジメントに承認を得なければならない。

（２）　障害または事故発生時の見直し

事業継続計画を立案している重要な業務に、障害または事故等が発生し、事業継続計画の内容どおり処理できず、業務の中断が生じた場合、業務管理責任者は、ISMS 管理責任者の協力のもとに事業継続計画を見直し、トップマネジメントに承認を得なければならない。

5.事業継続計画書の保管

（１）　要員への配布

ISMS 管理責任者は、「**事業継続計画書**」を各要員に配布しておかなければならない。

（２）　コピーの保管

事業継続計画の実行において意思決定権を持つ重要な要員は、自宅に事業継続計画書のコピーを保管しなければならない。ISMS 管理責任者は、その実施状況について確認を行う。

11 従業者管理手続

1.目的

本手続は、適用範囲において従業者の情報セキュリティに関する職務責任と採用に関するポリシーを明らかにする為に必要な事項を定める。

2.職務と採用

（１） 職務責任

従業者は、当法人が定める手続類を遵守し、職務に関する情報資産の保護に責任を負わなければならない。職務に応じた情報セキュリティに関する教育が実施された場合、該当する教育を受けなければならない。

（２） 従業者採用審査及びポリシー

採用担当者は、従業者採用時には採用の可否を審査する場合、原則として以下の資料を参照しなければならない。

- 履歴書及び身上書
- 卒業証明書および学業成績証明書（新規学卒者の場合に限る）
- 滞在許可証明書（外国人の場合に限る）

（３） 誓約書締結

従業者は、採用時に契約の条件の一部として機密情報および個人情報取り扱い誓約書、個人情報取り扱いに関する同意書、個人情報・情報セキュリティ誓約書に署名しなければならない。なお、これらの誓約書・同意書の効力は、離職時・退職時にも適用される。

（４） 採用者に対する責任の明示

採用担当者は、採用する際に、採用者に対して情報セキュリティに関する責任が課せられることを明示、もしくは説明しなければならない。

（５）　資産の返却

従業者は、退任時・離職時・退職時に自らが所有する会社の資産すべてを返却しなければならない。

（６）　アクセス権の削除

ISMS 管理責任者または開発部の情報管理者は、退任・離職・退職した役員及び従業者に付与されたアクセス権を速やかに削除しなければならない。

（７）懲罰

従業者が情報資産の機密性、完全性、可用制を損失した場合、懲罰委員会を招集し懲罰を決定する。役員及び従業者に課する懲罰は就業規則第 18 条、第 19 条に準ずる。

12 情報処理施設設備管理手続

1.目的

本手続は、適用範囲における情報システムの安全な運用のために、適用範囲で取り扱われる情報処理施設及び設備の設置、運用に関して必要な事項を定める。

2.情報処理施設及び設備の設置

（１）防火対策

当法人の業務で使用する情報処理施設には、煙探知機、消火設備を完備しなければならない。又、喫煙は所定の場所に限定し、各エリア内は禁煙とする。

（２）防水対策

施設管理者は、台風等の暴風雨など水害の影響を受けないように設備の設置には十分配慮をしなければならない。

（３）落雷対策

サーバルーム及び開発部のサーバやその関連施設の内重要なものが使用する電源設備には、落雷に対する異常電流に対する措置を講じなければならない。

（４）地震対策

施設管理者は、サーバルーム内のコンピュータ及び周辺機器、キャビネット類の内重要なものについては地震による転倒防止措置を講じなければならない。

（５）停電対策

施設管理者は ISMS 管理責任者の指示の下で、サーバルームのサーバ及び周辺機器、並びに開発部のサーバの内、重要なものについては無停電電源装置をしなければならない。

（６）ケーブル保護対策

役員及び従業者は、電源及びネットワークケーブル等の設置に関して、通行帯以外への設置あるいはモール等の設置など物理的な保護に十分配慮しなければならない。

3.設定管理

（１）環境設定の文書化と承認

開発部の情報管理者は、サーバルームに設置してあるサーバ及びネットワーク機器の設定情報を文書化し、これを管理保管しなければならない。

（２）事故発生時の対応の文書化と承認

開発部の情報管理者は、サーバルームに設置してあるサーバ及びネットワーク機器にエラーが発生した場合には、「**事故・障害対応手続**」に従い、対応しなければならない。

4.リソース管理

開発部の情報管理者は、パフォーマンスやディスク容量等に異常が生じた場合は、速やかに対策を講じ、ISMS 管理責任者に報告をしなければならない。

5.監視

（１）障害監視

開発部の情報管理者は、情報システムの使用状況を常に監視し、各サーバの情報の重要性に応じた対応を実施しなければならない。開発部の情報管理者は、障害の重大性と情報資産への影響を考慮し、ISMS 管理責任者への報告を行うものとする。

（２）ログ

開発部の情報管理者は、各サーバの情報の重要性に応じ、各サーバのログ取得項目、保管期間を決定しなければならない。

ログはそれ自体改ざんされないようにし、開発部の情報管理者が **1** ヶ月に一度、査閲しなければならない。ログの査閲により重要な事項が発見された場合は、開発部の情報管理者は、その重大性と情報資産への影響を考慮し、必要に応じて ISMS 管理責任者への報告を行うものとする。又、ログの正確性を確保するために、各サーバは定期的に内部時計の同期を行わなければならない。

6.システムのバックアップ

（１）データのバックアップ

情報管理者は、その情報の可用性の観点での重要性に応じ、バックアップの頻度及び保管方法を決定しなければならない。

（２）バックアップ手順の文書化

開発部の情報管理者は、情報管理者の決定に基づいてバックアップ手順を明確にしなければならない。

（３）バックアップメディアの保管

バックアップメディアは、原則としてバックアップ元のデータの存在するエリアとは別のエリアに保管をしなければならない。また、保管に際しては、バックアップ元のデータと同等のセキュリティを確保しなければならない。

７.装置の処分（廃棄、再利用）

記憶媒体を内蔵した装置は、廃棄又は再利用する前に以下の作業を実施しなければならない。

① データの消去（再生不可能な状態にすること）
② ソフトウェアの消去（再生不可能な状態にすること）
③ データディスクの物理的破壊（廃棄時）
④ データ廃棄証明書の取得（リース物件、廃棄の外部委託の場合）

改定履歴

版	内容	日付
Ver.1.0	初版	2019 年 9 月 27 日
Ver.1.1	4.2.(8)へ以下の文章を追加 私用の携帯端末は業務で使用せず、業務用 PC に接続しない	2019 年 12 月 4 日