社外秘

情報セキュリティ管理策規程

制定／改訂日：　2025 年 12 月 3 日

版数：　2.7

文書番号：　AB-標準-250503

管理部門：　情報セキュリティ管理

承認	確認	作成
塩田	井上	岡

株式会社　アグ・ブレインズ・システム

目次

1　適用範囲

本規程は、ISMS マニュアルに記載されている職務担当者及び組織を対象とする。

2　引用規格

ISO/IEC27002:2022　情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策
ISO/IEC 27000:2019　情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語

3　用語及び定義

この文書で用いる主な用語及び定義は、JIS Q 27000: 2019 に準ずる。

4　構成

この手順書は、適用宣言書にて適用した ISO/IEC 27001:2022 の附属書 A（規定）情報セキュリティ管理策に規定された管理策を実施するための手順を示すためのもので、4 章で構成し、93 の管理策がある。
各管理策は、管理策、手順で構成される。尚、適用宣言書にて適用除外された管理策はその旨を明示する。

5　組織的管理策

管理策 5.1　　情報セキュリティのための方針群

情報セキュリティ方針及びトピック固有の方針は，これを定義し，管理層が承認し，発行し，関連する要員及び関連する利害関係者に伝達し，認識させ，あらかじめ定めた間隔で，及び重大な変化が発生した場合にレビューしなければならない。

■　手順

I.　情報セキュリティ基本方針

(1) 【情報セキュリティ基本方針】は、次のものから導き出される要求事項を考慮に入れる。
   a)　事業戦略及び要求事項
   b)　規制、法令及び契約
   c)　現在の及び予想される情報セキュリティのリスク及び脅威
(2) 【情報セキュリティ基本方針】には、次の事項に関する記載を含める。
   a)　情報セキュリティの定義
   b)　情報セキュリティの目的、又は情報セキュリティの目的を設定するための枠組み
   c)　情報セキュリティに関する全ての活動の指針となる原則
   d)　情報セキュリティに関連する適用可能な要求事項を満たすことのコミットメント
   e)　情報セキュリティマネジメントシステムの継続的な改善へのコミットメント
   f)　情報セキュリティマネジメントに関する責任の、定められた役割への割当て
   g)　逸脱及び例外を取り扱う手順
(3) 【情報セキュリティ基本方針】の変更は、トップマネジメントが承認する。

II.　情報セキュリティ個別方針

(1) 本規程に定める情報セキュリティ管理策の実施をさらに義務付けるために、必要に応じて、特定のグループの要求に対処する、又は特定のセキュリティ領域を対象とする、情報セキュリティ個別方針を定める。
(2) 情報セキュリティ個別方針の作成、レビュー及び承認に関する責任は、関連する要員に、彼らの適切なレベルの権限及び技術的力量に基づいて割り当てることができる。
(3) 本規程の以下の項目を、情報セキュリティ個別方針として定める。

運用ルール全般	【情報セキュリティ運用ルール】
アクセス制御方針	「管理策 5.15　　アクセス制御」
物理的・環境的セキュリティ方針	「管理策 7.5　　物理的及び環境的脅威からの保護」
資産管理方針	「**エラー! 参照元が見つかりません。**」
情報転送方針	「管理策 5.14　　情報の転送」
利用者エンドポイント機器管理・取扱方針	「管理策 8.1　　利用者エンドポイント機器」
ネットワークセキュリティ方針	「管理策 8.20　　ネットワークセキュリティ」

情報インシデント管理方針	「管理策 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」
バックアップ方針	「管理策 8.13　情報のバックアップ」
暗号・鍵管理方針	「管理策 8.24　暗号の利用」
情報分類・脆弱性方針	「管理策 5.12　情報の分類」
技術的脆弱性管理方針	「管理策 8.8　技術的ぜい弱性の管理」

III. 方針のレビュー・伝達

(1) 基本方針及び個別方針のレビューは、マネジメントレビューにて行う。
(2) 一貫性を維持するため、一つの方針を変更する場合は、他の関連する方針のレビュー及び更新を検討する。
(3) 基本方針及び個別方針は、関連する要員及び利害関係者に伝達する。
(4) 必要な場合、方針の受領者に、方針を理解したこと及びその遵守に同意することの確認を求める。

管理策 5.2　　情報セキュリティの役割及び責任

情報セキュリティの役割及び責任は，組織のニーズに従って定め，割り当てなければならない。

■ 手順

(1) 情報セキュリティマネジメントシステムにおける役割及び責任は、【組織の役割・責務一覧】において、明らかにする。
(2) 認証範囲に含まれる情報資産の管理責任は、【情報資産リスクアセスメント表】において明らかにする。

管理策 5.3　　職務の分離

相反する職務及び相反する責任範囲は，分離しなければならない。

■ 手順

(1) 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、分離する。

管理策 5.4　　管理層の責任

管理層は，組織の確立された情報セキュリティ方針，トピック固有の方針及び手順に従った情報セキュリティの適用を，全ての要員に要求しなければならない。

■ **手順**

(1) 経営責任者及び情報セキュリティ管理者は、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、全ての従業員に要求する。

(2) 経営責任者及び情報セキュリティ管理者の役割については、【組織の役割・責務一覧】において、明らかにする。

管理策 5.5　　関係当局との連絡

組織は，関係当局との連絡体制を確立し，維持しなければならない。

■ **手順**

(1) 関係当局の連絡先を【関係当局・専門組織との連絡先一覧】に維持する。

管理策 5.6　　専門組織との連絡

組織は，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・団体との連絡体制を確立し，維持しなければならない。

■ **手順**

(1) 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・団体の連絡先を【関係当局・専門組織との連絡先一覧】に維持する。

管理策 5.7　　脅威インテリジェンス

情報セキュリティの脅威に関連する情報を収集及び分析し，脅威インテリジェンスを構築しなければならない。

■ **手順**

(1) 情報セキュリティ管理者が、IPA サイトからセキュリティ脅威情報を情報メールで収集し、トップマネジメント(経営責任者)と情報セキュリティ管理者で問題の有無を協議し、必要に応じて対処する。

管理策 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

情報セキュリティをプロジェクトマネジメントに組み入れなければならない。

自社システム開発プロジェクトは無いが、社内業務におけるプロジェクトマネジメントに情報セキュリティを組み込む。

■ **手順**

(1) 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む。

管理策 5.9　　情報及びその他の関連資産の目録

情報及びその他の関連資産の目録を，それぞれの管理責任者を含めて作成し，維持しなければならない。

■ **手順**

(1) 当社の情報資産は、【情報資産リスクアセスメント表】に記録、随時または 1 回/年見直しを実施する。
(2) 全ての情報資産は、【情報資産リスクアセスメント表】にて、リスク所有者を明確にする。

管理策 5.10　　情報及びその他の関連資産の許容される利用

情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は，明確にし，文書化し，実施しなければならない。

■ **手順**

(1) 全ての情報資産は、その利用が許容される範囲を、【情報資産リスクアセスメント表】に明確にする。

管理策 5.11　　資産の返却

要員及び必要に応じてその他の利害関係者は，雇用，契約又は合意の変更又は終了時に，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。

■ **手順**

(1) 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、会社が貸与した自らが所持する組織の資産の全てを返却する。対象資産は【退職時及び契約終了時のチェックリスト】で明確にする。

管理策 5.12　　情報の分類

情報は，機密性，完全性，可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って，分類しなければならない。

■ 手順

(1) 全ての情報資産は、【情報セキュリティマニュアル】に規定する区分に従って分類する。
(2) 当社の情報資産それぞれの分類は、【情報資産リスクアセスメント表】で明確にする。

管理策 5.13　　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。

■ 手順

(1) 情報資産は、【情報セキュリティマニュアル】に規定された機密性の区分に基づいて、ラベルを付ける。
(2) 紙の場合は表紙やヘッダー、電子データの場合はファイル名等、容易に識別できる箇所にラベルを付ける。
(3) 機密性の区分に応じて、「社外秘」又は「極秘」の機密レベルの記載を加える。
(4) 作業負荷を減らすため、「社外秘」又は「極秘」でない情報のラベル付けは省略する。
(5) ただし、紙や電子データは、経営責任者のみアクセス可能な情報が多く、ラベル付けにより、却って秘密情報であることを公開することになりかねない為、「社外秘」については、経営責任者の承認の上、ラベル付けは省略可能とする。

管理策 5.14　　情報の転送

情報の転送の規則，手順又は合意を，組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備えなければならない。

■ 手順

(1) 組織の内部及び外部における情報の転送及び交換について、その方針を次に定める。
　① インターネット経由にて情報を転送する場合は、セキュアな通信方式にて行う。
　② 機密情報を電子メールの添付ファイルで送信する場合は、パスワードによる暗号化を行う。
　　電子メールでの運用ついては、【情報セキュリティ運用ルール】No.15 を順守する。
(2) 外部組織との間で情報転送する場合には、経営責任者の承認を得て実施する。

管理策 5.15　　アクセス制御

情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を，事業上及び情報セキュリティの要求事項に基づいて確立し，実施しなければならない。

■ 手順

(1) 情報システムへの無許可アクセスを防止するため、パスワードまたはフォルダに対するアクセス設定によるアクセス管理を実施することを方針とし、利用者や利用者グループごとにアクセス権を設定する。
(2) 経営責任者が認可したネットワークのみを使うこととし、個人が勝手にネットワークを構築してはならない。
(3) 第三者が提供するネットワークサービスに情報を格納する場合には、経営責任者が認可したものだけを使う。
(4) 【情報セキュリティ運用ルール】No.11 を順守する。

管理策 5.16　　識別情報の管理

識別情報のライフサイクル全体を管理しなければならない。

原則、社員には、データの保管場所となっている Microsoft Business を使用する ID を与えない。経営責任者が必要と判断した場合は付与する。

■　手順

(1) メールアドレス
　① 新規の利用者 ID が必要になった場合には、経営責任者が必要な権限と必要性を検討し、妥当と判断した場合には、情報セキュリティ管理者に依頼し、情報セキュリティ管理者が新規メールアドレスを取得し、対象者に渡す。
　② パスワードは情報セキュリティ管理者が発行し、利用者が初期ログイン時、及び定期的に(1 回/1 年)変更する。
　③ 退職などで不要となった利用者 ID は、経営責任者からの指示により情報セキュリティ管理者が速やかに削除・停止する。

(2) Microsoft Business の ID
　④ 新規の利用者 ID が必要になった場合には、経営責任者が必要な権限と必要性を検討し、妥当と判断した場合には、新規利用者 ID を取得し、対象者に渡す。
　⑤ パスワードは経営責任者が発行し、利用者が初期ログイン時、及び定期的に(1 回/1 年)変更する。
　⑥ 退職などで不要となった利用者 ID は、経営責任者が速やかに削除・停止する。

(3) 一時的に必要なフォルダのみを更新する権限
　① 一時的にゲストとして必要なフォルダのみへのアクセスが必要となった場合には、経営責任者が必要な権限と必要性を検討し、妥当と判断した場合には、フォルダへのアクセス権を取得し、対象者に渡す。
　② パスワードは経営責任者が発行し、定期的に(1 回/1 年)変更する。

③　退職などで不要となったアクセス権は、経営責任者が速やかに削除・停止する。

詳細な手順は、【操作手順集】及び、さくら Internet、MicroSoft のマニュアルに従う。

管理策 5.17　　認証情報

認証情報の割当て及び管理は，認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。

メールアドレス及び Microsoft Business に対する認証情報の管理プロセスは以下の通りとする。

■　手順

利用者 ID の発行手順を次に定める。
【情報セキュリティ運用ルール】No.20 を順守しなければならない。

(1)　メールアドレス

利用者が最初に使用するメールアドレスの初期設定のパスワードは、経営責任者が発行し、口頭で該当者に通知する。利用者はパスワードが発行された後、速やかに自らログインしパスワードを変更する。

①　パスワードは英数字を含め 8 文字以上に設定する。
②　個人のパスワードは秘密に保ち、他人による自身の ID の使用を防がなければならない。
③　パスワードを忘れたり、間違えたりした場合、再度新しいパスワードの発行を行う。
④　パスワードの他人による流用が発覚した場合、パスワードが漏えいしたと疑われる場合、直ちにパスワードを変更する。
⑤　ID とパスワードは同じものを使用してはならない。
⑥　ユーザーは自身の ID に関するあらゆる活動の責任を負う。
⑦　パスワードは、定期的(1 回/1 年)変更する。

(2)　Microsoft Business

経営責任者がパスワードを発行し、口頭で該当者に通知する。利用者はパスワードが発行された後、速やかに自らログインしパスワードを変更する。

①　パスワードは英数字を含め 8 文字以上に設定する。
②　パスワードは秘密に保つ。
③　パスワードを忘れたり、間違えたりした場合、再度新しいパスワードの発行を行う。
④　パスワードの他人による流用が発覚した場合、パスワードが漏えいしたと疑われる場合、直ちにパスワードを変更する。
⑤　ID とパスワードは同じものを使用してはならない。

⑥　ユーザーは自身の ID に関するあらゆる活動の責任を負う。
⑦　パスワードは、定期的(1 回/1 年)変更する。

管理策 5.18　　アクセス権

情報及びその他の関連資産へのアクセス権は，組織のアクセス制御に関するトピック固有の方針及び規則に従って，提供，レビュー，変更及び削除しなければならない。

情報資産は Microsoft Business に保管されている。Microsoft Business へのアクセス管理は経営責任者のみ実施する。

■　**手順**

(1) 必要最低限のアクセス権を付与する。アクセス権の設定は、経営責任者によりなされるものとする。
(2) 経営責任者が必要と判断した場合のみ、付与する。
(3) アクセス権一覧は「Microsoft 365 管理センター」「OneDrive 経営責任者ホーム」で確認する。
(4) 経営責任者は、対象者のアクセスが不要になった場合、直ちにアクセス権を削除する。
(5) 経営責任者は、1 年に 1 回以上、Microsoft Business に対するアクセス権を見直し、必要に応じて変更・修正するものとする。アクセス権の参照方法は【操作手順集】を参照する。

管理策 5.19　　供給者関係における情報セキュリティ

供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め，実施しなければならない。

■　**手順**

(1) 契約関連書類や供給者のホームページ等で、供給者の活動において、当社のセキュリティが確保されていることを確認する。
(2) リモート保守や機器保守など、第三者によるシステムのアクセスを許可する場合、経営責任者がセキュリティが確保されることを判断し、アクセスを許可する。
(3) パートナー企業がパソコン等の機器を持ち込み、当社 LAN への接続により業務することは許可しない。

管理策 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

供給者関係の種類に応じて，関連する情報セキュリティ要求事項を確立し，各供給者と合意しなければならない。

■ **手順**

(1) 供給者のホームページを確認することにより当社の情報セキュリティ要求事項が満たされることを確認する。または、契約関連書類や秘密保持契約書により当社の情報セキュリティ要求事項が満たされることを確認する。

管理策 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管理

ICT 製品及びサービス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を管理するためのプロセス及び手順を定め，実施しなければならない。

■ **手順**

(1) サービスの供給者との間で契約内容やサービスレベルに変更があった場合、e メールまたは HP 閲覧によるアナウンスにより、変更点の連絡を受け、社内で受入れることができるか否かを検証し、必要に応じて契約内容の見直しを実施する。

管理策 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

組織は，供給者の情報セキュリティの活動及びサービス提供を定常的に監視し，レビューし，評価し，変更を管理しなければならない。

■ **手順**

(1) セキュリティ管理者または経営責任者は、供給者のサービス提供を、供給者のホームページから 1 度/月の頻度で監視し、弊社の活用範囲で支障がないかレビューし、監査する。状況の確認方法は【操作手順集】を参照する。
(2) 経営責任者は、サービスの実際の実施状況について、実際に業務使用の中で監視する。
(3) 経営責任者は、サービスの実施状況において、応答遅延や品質劣化等の問題が発生した場合、供給者へ報告し、適切に対処する。
(4) 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。）はサービス提供業者から連絡を受け取ることで管理する。業務システム及び業務プロセスの重要性、リスクの再評価を考慮して、対処する。変更情報は、供給者のホームページから 1 度/月の頻度で監視し、弊社の活用範囲で支障がないかレビューし、監査する。状況の確認方法は【操作手順集】を参照する。
(5) サービス内容における要求事項の変更については、業務システム及び業務プロセスの重要性、リスクの再評価を考慮して、必要に応じて、供給者へ通知し、合意する。

管理策 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

クラウドサービスの調達，利用，管理及び利用終了のプロセスを，組織の情報セキュリティ要求事項に従って確立しなければならない。

■　手順

(1) クラウドサービスの導入については、事業運営上の必要性から経営責任者が判断し、クラウドサービスのセキュリティ対策を確認し、導入する。経営責任者が不要となったと判断した場合、利用を終了し、存在するデータを処分し契約を終了する。
(2) クラウドサービスの利用に伴う情報セキュリティリスクの回避策として、管理策 5.18　アクセス権を管理する。

管理策 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

組織は，情報セキュリティインシデント管理のプロセス，役割及び責任を定め，確立し，伝達することによって，情報セキュリティインシデント管理を計画し，準備しなければならない。

■　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する。

I.　事件、事故、セキュリティ弱点の対応手順

顧客先業務で発生した事故の場合

(1) 発見者は、即座にリードプロフェッショナル、連絡がつかない場合は経営責任者へ報告し、被害拡大防止の為の応急処置を実施する。リードプロフェッショナルは顧客先ルールに従い、即座に顧客先管理者に対して必要なエスカレーションを行い、かつ経営責任者へ報告する。
(2) 防止策が不明な場合は、経営責任者の指示に従う。

社内で発生した事故の場合

(1) 情報セキュリティ管理者は事件、事故の証拠の保全に努める。
(2) 経営責任者及び情報セキュリティ管理者は、事件、事故の対象となった情報資産に対するリスクアセスメントを実施し、恒久処置を決定、実施しなければならない。
(3) 情報セキュリティ管理者は、処置による管理策の変更が伴う場合、規程、手順類の改訂を実施する。
(4) 情報セキュリティ管理者は、適当な時期に、処置の有効性を検証しなければならない。

II.　懲戒手続き

(1) セキュリティ規程違反が認められた場合、経営責任者は懲戒を決定する。
(2) 具体的な懲戒手続きは就業規則による。

III.　事故の公表

(1) 経営責任者は、事故の公表について検討し、公表を実施する。このときは必ず、弁護士等法的なアドバイスを受ける。

IV. 関係者等への連絡

(1) 経営責任者は、事故の警察(関係当局)等への連絡について検討する。

(2) 情報セキュリティ管理者または経営責任者は経営責任者の指示に従い、警察等への連絡を実施する。このときは必ず、弁護士等法的なアドバイスを受ける。

管理策 5.25　　情報セキュリティ事象の評価及び決定

組織は，情報セキュリティ事象を評価し，それらを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。

■　手順

(1) 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する。
(2) 経営責任者は報告されるセキュリティ事象に関して、それにより外部の組織や顧客に影響を及ぼす場合は、セキュリティインシデントとして対応すべきかを判断する。

管理策 5.26　　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。

■　手順

(1) 情報セキュリティインシデントは、5.24　1.事件、事故セキュリティ弱点の対応手順にしたがって対処する。
(2) セキュリティ事象と判断されたインシデントは、管理策 5.24 に規定される手順に基づいて対応する。
(3) 対応策には、次の事項を含める。
    ① 知る必要性を認められている内部・外部の他の要員又は組織に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達する。
    ② インシデントの原因又はインシデントの一因であることが判明した情報セキュリティ弱点に対処する。
    ③ インシデントへの対応が滞りなく済んだ後、正式にそれを終了し、記録する。

管理策 5.27　　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から得られた知識は，情報セキュリティ管理策を強化し，改善するために用いなければならない。

■　手順

(1) 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る。
(2) 年に 1 回、マネジメントレビューにおいて、情報セキュリティで発生した問題を分析する機会をもつ。

管理策 5.28　　証拠の収集

組織は，情報セキュリティ事象に関連する証拠の特定，収集，取得及び保存のための手順を確立し，実施しなければならない。

■　**手順**

(1) 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、適用する。
(2) 経営責任者及び情報セキュリティ管理者は、Microsoft Business の監査ログ等を裁判の証拠となるように収集を計る。
(3) 従業員は法的な強制による情報の開示に、経営責任者の決定のもと、同意する。
(4) 従業員は裁判における証拠の提供にあたって、経営責任者の許可を得て行う。
(5) 関係当局から事件の証拠としてデータの提出を要求された場合、経営責任者の指示に従い協力体制を整備する。
(6) 情報セキュリティ犯罪調査の途中経過報告は、経営責任者と情報セキュリティ管理者のみに成される。
(7) コンピュータ犯罪における証拠、仮説、手口及び同期等の資料は、経営責任者管理下にて制限情報として保管され、アクセス制限をする。

管理策 5.29　　事業の中断・阻害時の情報セキュリティ

組織は，事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画しなければならない。

弊社のデジタル情報資産は主にストレージ（Microsoft Business）に存在する。
1 回/月の頻度で経営責任者が USB にバックアップしており、データは USB から復旧する。

■　**手順**

I.　事業継続マネジメントの基本方針

経営責任者並びに情報セキュリティ管理者の承認のもと、以下の方針に基づいて、情報セキュリティ要求事項が織り込まれた事業継続マネジメントプロセスを実施する。

(1) 事業継続計画は、身体・生命の安全確保に加え、優先的に継続・復旧すべき重要業務の継続または早期復旧を目的とする。
(2) 事業継続計画は、特定の発生事象による被害想定を前提にするものの、「どのような危機的事象が発生しても重要業務を継続する」という目的意識を持って実施されることも認識し、被害の様相が異なっても可能な限り柔軟さも持つように策定する。
(3) 事業継続計画は、故障などのリスクを考慮し、可能な範囲の ICT 設備の備えを用意する。また、定期的に稼働するかどうか試験を行う。

II. リスクの特定

事業継続計画を策定するために、当社の事業活動の中断・阻害を引き起こしうる事象及びそのリスクを以下に特定する。

	緊急事態（原因事象）	リスク（結果事象）
1	災害（自身、火災等天災）	・オフィス、社屋の使用不可 ・社員及び関係者の影響の恐れ ・情報システムの使用不可
2	感染症の広域感染	・オフィス、社屋の使用不可 ・社員及び関係者の影響の恐れ
3	供給サービスの障害	・情報システムの使用不可

III. 事業継続計画

上記で特定したリスクに対して、事業継続のための対応計画を以下に策定する。

(1) 緊急時の体制

① 対策本部構成と役割

経営責任者を対策本部長とし、情報セキュリティ管理者で構成する対策本部を設置する。

対策本部は、事業継続計画の指揮、意思決定、行動の指示、実行状況の監督等の役割を担う。

② 設置基準

II. で特定した緊急事態に該当するまたはそれに類する事象が発生した場合に、対策本部を設置する。

③ 対策本部の設置場所

対策本部は、原則として本社に設置するが、本社が倒壊した際には、経営責任者が設置場所を決定する。対策本部設置場所は、緊急連絡網で通知する。

④ 対策本部の役割

機能区分	機能
対外機能	顧客対応、業務継続（対顧客）
対内機能	安否確認、連絡、要員配置、 施設・システムの復旧・保全、物資調達

(2) 緊急時の対応手順

A) 初動対応	**① 対策本部の参集** － 安全が確認できたら、対策本部メンバーは対策本部に集結する。 － （※安全確保の観点等から必要に応じて参集対象者の出社を抑制） － 参集場所が利用できない場合は、代替拠点を決定し参集する。 **② 顧客・従業員の安全確保・安否確認** － 対策本部は、避難が必要な場合、顧客・従業員の避難誘導を行う。 － 各従業員は、勤務先、出先、自宅問わず、自身及び周囲の安全を確保する。周囲の状況に応じて、必要な場合には避難を行う。 － 各従業者は、緊急連絡網に従い、安否を報告する（勤務先、出先、自宅で共通）。通常の通信手段を使用できない場合は、NTT 災害伝言ダイヤル、災害用伝言板を利用し、報告する。 － 対策本部は、状況に応じて、安全な帰宅方法の指示や、かえって帰宅することが危険な場合の待機を指示する。 **③ 建物、設備等経営資源の被害状況の確認** － 建物、構築物、設備、作業現場等の被害を確認する。 **④ 二次災害の防止** － 落下防止、火災の防止（ガス栓の遮断・確認等、必要なら一部電源の遮断を含む）、薬液漏洩防止、危険区域の立入禁止など、安全対策を実施する。 － 危険が周辺に及ぶ可能性のある場合、住民への危険周知や避難要請、行政当局への連絡を行う。 **⑤ 自社の状況についての情報発信** － 対策本部は、社内の被害状況等の情報集約し、社内外の必要な相手先に対し、自社の状況についての情報発信を行う（連絡先一覧による）。 **⑥ 事業継続計画の発動** － 初動が落ち着いた後、対策本部は、事業継続計画発動の要否を判断し、発動となった場合、事業継続体制へ移行する（本項 B) を参照）。 **⑦ 対応の記録** － 実施した対応や、発生した問題点等の記録を行う。
B) 事業継続対応	**① 自社の事業継続に対して、求められている事項の確認、調整** － 対策本部は、受託先や関係当局との連絡、WEB サイトによる通達や告示の閲覧等により情報収集を行う。 － 対策本部は、自社の事業継続に対して、求められている事項の確認、必要に応じて相手方と調整を行う。 **② 現拠点、代替拠点での事業継続の能力・可能性の確認** － 対策本部は、自社の経営資源の被災状況、調達先の状況等、必要資源の

	確保可能性の確認を行う。 － 対策本部は、情報のバックアップ、バックアップシステムの保存・稼働、ならびに事業継続に必要な ICT 設備の稼働の状況の確認を行う。 － 故障など稼働が困難なものがあれば、備蓄していた代替物を確認する。 － 対策本部は、復旧資材の必要性・入手可能性を把握する。 － 対策本部は、現拠点での復旧可能性や復旧可能時間の見積もりを実施する。 － 必要であれば、代替拠点での業務立ち上げ時間等の見積もりを実施する。 **③ 実施する戦略や対策の決定** － 対策本部は、実施する復旧、代替等の戦略を決定する（現地復旧、代替拠点活用等）。 － 対策本部は、基本方針、目標、対策の優先順位を決定する。 － 対策本部は、戦略に基づき実施する主要な対策を決定する。 **④ 業務の継続・再開** － 対策本部は、業務の継続・再開に向けた各対策を実施する（本項 C) を参照）。 － 必要に応じて従業員・顧客の安全確保が前提であることの認識を徹底する。 － 重要業務に関係する主体との連絡調整を行う。 － 対策実施状況の進捗管理及び追加指示を行う。 － 臨時予算を確保する。 － 業務の継続・再開・復旧の状況を把握する。 **⑤ 自社の状況についての情報発信** － 対外的に発信すべき情報の集約・判断を行う。 － 取引先、従業員、株主、**地方公共団体**などに対して、自社の事業継続の状況について情報発信を行う。
C) システム復旧手順	**① システムの被害状況を確認** － ネットワーク機器等のシステムまわりの被害状況を確認する。 － バックアップデータの状態を確認する。 － PC は、破損に応じた状況を確認する。 **② インフラまわりの状況確認** － 電源の供給、通信設備（電話回線・インターネット回線）等のインフラまわりの状況を確認する。尚、電源については、安定した供給が得られること。 **③ システムの復旧** － 経営責任者は、被害における状況をまとめる。 － 復旧作業を開始する。尚、データの復元が必要な場合は、復元までの所

	要時間を利用者へ伝え、その間の使用を厳禁とする。 ④ **復旧終了後の被害額及び損失額の算出** － 復旧終了後、経営責任者は被害額及び損失額を算出する。

IV. 情報セキュリティ継続の実施

II. にて特定されたリスクに当たる状況下に陥った時、III. の事業継続経過に沿って対応する。
事業継続計画を実施した結果は、【事業継続計画実施記録】に記録する。

V. 教育・訓練の実施

(1) 事業継続計画を実効性のあるものとするために、教育及び訓練の実施計画を策定する。
(2) 教育及び訓練の実施計画は【教育・訓練計画表】に、予定時期・実施時期を記録する。
(3) 経営責任者及び情報セキュリティ管理者は、実施した教育・訓練の結果を【教育・訓練計画表】に記録する。
(4) また、事業継続のための執務室ルーターの代替の機器(デザリング)の稼働を試験する。
(5) 事業継続計画を実行性のあるものにするために、教育・訓練計画は以下の事項を考慮して策定する。各項目にその実施方法も併せて記載する。

教育	基礎知識の提供	・ 事業継続の概念や必要性、想定する発生事象（インシデント）の概要など ・ 講義、e ラーニング等による
	自社の事業継続マネジメントの周知	・ 講義、Web を使った広報　等による
	最新動向の把握	・ 専門文献や記事の購読
訓練	BCP、手順の内容の理解促進	・ 本管理策Ⅰ.事業継続計画 に基づき、役割分担、手順、代替先への移動、確保資源の確認等を机上訓練などにより行う
	手順の習熟	・ 安否報告・緊急連絡訓練などがある
	ICT 設備及び手段の備えの試験	・ 事業継続計画の実行に基づき、代替 NW の可用性を維持すべく、それら設備及び手段の稼働状況をテストする

VI. 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、1 回/年でこれらの管理策を検証する。

VII. 見直し・改善の実施計画

V. で定められた訓練により検証・評価し、是正すべき点は、【是正処置報告書】にて改善する。
また、その内容はマネジメントレビューにて報告する。

管理策 5.30　　事業継続のための ICT の備え

事業継続の目的及び ICT 継続の要求事項に基づいて，ICT の備えを計画し，実施し，維持し，試験しなければならない。

■　手順

「管理策 5.29　　事業の中断・阻害時の情報セキュリティ」の手順に基づき、事業継続のための ICT に関連する情報セキュリティ継続の計画をして試験を行う。

管理策 5.31　　法令，規制及び契約上の要求事項

情報セキュリティに関連する法令，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を特定し，文書化し，また，最新に保たなければならない。

■　手順

(1) 情報セキュリティ管理者は、認証範囲の業務における情報セキュリティに関して各法規（ガイドラインを含む）の要求事項を明確にし、社員等に周知徹底する。
(2) これら法令、規制は【適用法令一覧】として文書化し、1 回/年見直しを実施する。

管理策 5.32　　知的財産権

組織は，知的財産権を保護するための適切な手順を実施しなければならない。

■　手順

(1) 全ての従業員は、知的所有権の侵害等、違法行為となる恐れがあるファイル等を送受信してはならない。また、ダウンロードデータの扱いについても該当する規則を遵守し、その行為が違法行為とならないよう配慮して取扱う。
(2) 全ての従業員は、他社の保有する特許権を侵害してはならない。また、他社の保有する特許権に関わる取扱いについては管理者に確認する。
(3) 全ての従業者が利用する市販パッケージソフトのライセンスの維持管理を行い、市販パッケージソフト及び無償ソフトウェア製品はその使用許諾契約を守って使用する。

管理策 5.33　　記録の保護

記録は，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。

■　**手順**

(1)　重要な記録は、情報の分類に従って取扱い、管理する。
(2)　管理方法は、【文書管理・採番ルール】に従う。

管理策 5.34　　プライバシー及び個人識別可能情報（PII）の保護

組織は，適用される法令，規制及び契約上の要求事項に従って，プライバシー及び PII の保護に関する要求事項を特定し，満たさなければならない。

■　**手順**

(1)　個人情報保護法及び番号法に準じた管理等を以下の手順に基づき実施する。
　①　保有する個人情報の利用目的はプライバシーポリシーとして定め(HP に提示)、定めた利用目的の範囲内で利用する。
　②　個人番号を含む個人情報は、アクセス制限を実施した保管場所で管理する

管理策 5.35　　情報セキュリティの独立したレビュー

人，プロセス及び技術を含む，情報セキュリティ及びその実施の管理に対する組織の取組について，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。

■　**手順**

情報セキュリティ及びその実施の管理に対する組織の取組について、1 回/年、内部監査にてレビューする。

管理策 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

組織の情報セキュリティ方針，トピック固有の方針，規則及び標準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。

■　**手順**

組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを 1 回/年、内部監査にてレビューする。

管理策 5.37　　操作手順書

情報処理設備の操作手順は，文書化し，必要とする要員に対して利用可能にしなければならない。

■　手順

(1)　操作手順書は原則、メーカー提供のマニュアルを使用する。

(2)　必要に応じて、マニュアルを作成する。発行、改訂を行う場合は、情報セキュリティ管理者の承認を得る。マニュアルは、【操作手順集】に記載する。

6　人的管理策

管理策 6.1　　選考

要員になる全ての候補者についての経歴などの確認は，適用される法令，規制及び倫理を考慮に入れて，組織に加わる前に，及びその後継続的に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。

■　手順

(1) 全ての従業員候補者についての経歴などの確認は、個人情報保護法、規制及び倫理に従って行う。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う。

(2) 社員の採用選考にあたっては、情報セキュリティ管理を含む当社の業務遂行に対する被採用者の適正性と能力を評価し、採用を決定する。

(3) 採用選考において扱う応募者の情報は、個人情報保護法に基づき、適切な処置が行われることを確実にする。

管理策 6.2　　雇用条件

雇用契約書には，情報セキュリティに関する要員及び組織の責任を記載しなければならない。

■　手順

(1) 人事担当者は、従業者の入社時に【秘密保持契約書】を説明し、署名の上、提出させる。

(2) 【秘密保持契約書】は、情報へのアクセス権を与える前に提出させることを確実にする。

(3) 【秘密保持契約書】には、以下の事項を定める。

a) 情報セキュリティに関する従業者の責任

b) 従業者の法的な責任及び権利（例えば、著作権法、個人情報保護法）

c) 従業者によって扱われる情報システム及びサービスに関連する、情報の分類及び当社の資産の管理に関する責任

d) 他社又は外部組織から受け取った情報の扱いに関する従業者の責任

e) 雇用の結果として、又は雇用の過程で作成された個人情報を含む、個人情報の扱いに関する当社の責任

f) 社外及び通常の勤務時間外に及ぶ責任（例えば、在宅勤務における責任。）

g) 従業者が当社のセキュリティ要求事項に従わない場合の懲戒手続

h) 業務上知り得た機密情報に関する異動後及び退職後の守秘義務

i) 退職時に当社の資産をすべて返却

j) 個人所有の設備を使用する場合は、退職時に機密情報をすべて消去

管理策 6.3　　情報セキュリティの意識向上、教育及び訓練

組織の要員及び関連する利害関係者は，職務に関連する組織の情報セキュリティ方針，トピック固有の方針及び手順についての，適切な，情報セキュリティに関する意識向上プログラム，教育及び訓練を受けなければならず，また，定常的な更新を受けなければならない。

■　手順

(1) 組織の全ての従業員については、【情報セキュリティマニュアル】に従い、情報セキュリティに関する教育・訓練を実施する。

(2) 契約相手が、当社の情報セキュリティパフォーマンスに影響のある業務に従事する場合には、【情報セキュリティマニュアル】に従い、情報セキュリティに関する教育・訓練を実施する。

管理策 6.4　　懲戒手続

情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために，懲戒手続を正式に定め，伝達しなければならない。

■　手順

(1) 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る。

管理策 6.5　　雇用の終了又は変更後の責任

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，施行し，関連する要員及びその他の利害関係者に伝達しなければならない。

■　手順

(1) 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、遂行させる。

(2) 従業員の退職時または契約終了時には、【退職時及び契約終了時のチェックリスト】の内容を確認する。

(3) 従業員の退職時または契約終了時には、【退職時の秘密保持誓約書】を説明し、署名、捺印の上、提出させる。

管理策 6.6　　秘密保持契約又は守秘義務契約

情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は，特定し，文書化し，定常的にレビューし，要員及びその他の関連する利害関係者が署名しなければならない。

■ **手順**

(1) 秘密保持契約又は守秘義務契約の締結に際しては、【秘密保持誓約書〔対従業員〕】を使用する。

管理策 6.7　　リモートワーク

組織の構外でアクセス，処理又は保存される情報を保護するために，要員が遠隔で作業をする場合のセキュリティ対策を実施しなければならない。

■ **手順**

(1) リモートワークを行う場所でアクセス、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する。
   ① 使用する PC は、家族等の同居人と共有してはならない。
   ② 使用する PC は、アンチウィルスソフトを導入する。
   ③ 使用する PC にファイル交換ソフト等の不正なソフトウェアをインストールしてはならない。
   ④ 【情報セキュリティ運用ルール】No.5、No.14 を順守しなければならない。

管理策 6.8　　情報セキュリティ事象の報告

組織は，要員が発見した又は疑いをもった情報セキュリティ事象を，適切な連絡経路を通して時機を失せずに報告するための仕組みを設けなければならない。

■ **手順**

(1) 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、できる限り速やかに報告する。
(2) 情報セキュリティ事象を発見した従業員は、組織図上の上位管理者(チーフリードプロフェッショナル及びリードプロフェッショナル)に対しできる限り速やかに報告する。
(3) 上位管理者(チーフリードプロフェッショナル及びリードプロフェッショナル)は、委託元(お客様)管理者にできる限り速やかに報告し、併せて経営責任者にできる限り速やかに報告する。
(4) 事象がインシデントにあたる場合、情報セキュリティ事象を発見した従業員は、その内容・原因・対処結果等を【是正処置報告書】に記録し、上位管理者、情報セキュリティ責任者、及び経営責任者に対し、速やかに報告する。

(5) 情報セキュリティ事象の報告を考慮する状況には、次の事項が含まれる。

① 情報の完全性、機密性又は可用性に関する期待に対する違反
② 人による誤り
③ 個別方針又は指針の不順守
④ 物理的セキュリティの取決めに対する違反
⑤ 管理されていないシステム変更
⑥ ソフトウェア又はハードウェアの誤動作
⑦ アクセス違反

(6) 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する。

(7) セキュリティ上の弱点を発見した者は、これらの事象に対処するとともに、その内容・原因・対処結果等を経営責任者へ報告する。

7　物理的管理策

管理策 7.1　　物理的セキュリティ境界

情報及びその他の関連資産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。

■　手順

(1) 社内の情報処理設備や秘密情報を保護するため、定められたセキュリティエリアを設定するものとする。

(2) セキュリティエリアは、以下の定義とする。

事務所の執務エリア

管理策 7.2　　物理的入退

セキュリティを保つべき領域は，適切な入退管理策及びアクセス場所（受付など）によって保護しなければならない。

■　手順

(1) 従業員の事務所への入退場については、特に制限しない。

(2) 外来者は原則、事務所の執務エリアへの入場を禁止し、1F フリースペースにて応対する。

(3) 外来者との打合せの場合は、1F フリースペースにて応対する。この場合、【入館簿】に記載し、履歴を残すこと。

(4) 物品の受け渡しは、原則として、物理的セキュリティ境界エリア外で行う。但し、物理的セキュリティ境界エリア外での受け渡しが難しい場合は、従業員の監督のもと、オフィスエリアへの立ち入りを許可する。

管理策 7.3　　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，実装しなければならない。

■　手順

(1) 事務所は当社従業員の執務時のみ開錠し、それ以外は施錠する。

(2) メディア保管場所へのアクセス：重要な磁気メディア、書類の保管場所は、施錠により一般従業員のアクセスを制限する。

(3) 物理的アクセス権限は、１回/年、内部監査時に見直しを行い、必要に応じて更新する。

管理策 7.4　　物理的セキュリティの監視

施設は，認可していない物理的アクセスについて継続的に監視しなければならない。

■　手順

(1)　物理的な施設は、ALSOK が侵入者警報により監視する。

管理策 7.5　　物理的及び環境的脅威からの保護

自然災害及びその他の意図的又は意図的でない，インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し，実装しなければならない。

■　手順

(1)　オフィスに火災に対する煙探知機、消火器を設置する。
(2)　重要な情報資産が格納された施設、部屋はそれと判る表示をしない事。

管理策 7.6　　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セキュリティ対策を設計し，実施しなければならない。

■　手順

(1)　執務エリアでカメラ、録音機、ビデオの使用は経営責任者の許可を必要とする。

管理策 7.7　　クリアデスク・クリアスクリーン

書類及び取外し可能な記憶媒体に対するクリアデスクの規則，並びに情報処理設備に対するクリアスクリーンの規則を定め，適切に実施させなければならない。

■　手順

(1)　作業場所及びディスプレイについて、クリアデスク及びクリアスクリーン方針を次に定める。
　①　帰宅時や長時間離席する時は、書類や可搬媒体をキャビネットに保管する。
　②　重要な書類や可搬媒体は、セキュリティが確保された場所に保管する。
　③　スクリーンロックは 5 分以内で設定し、パスワードロックをかける。

管理策 7.8　　装置の設置及び保護

装置は，セキュリティを保って設置し，保護しなければならない。

■ **手順**

(1) 喫煙は全面禁止とする。
(2) 業務用システム機器の配置：組織の業務システム用のネットワーク機器等は、事務所内に設置する。
(3) コンピュータの持ち込み：事前に経営責任者の認可無しに、会社所有以外のコンピュータ、周辺機器、ソフトウェアを事務所内に持ち込んではならない。
(4) 物理的セキュリティ境界エリアを含む事務所内は、火災に対する自動警報装置を備えなければならない。

管理策 7.9　　構外にある資産のセキュリティ

構外にある資産を保護しなければならない。

■ **手順**

(1) 構外にノート PC を持ち出す場合は、必ずログオンパスワードを設定する。
(2) 重要な情報の持ち出しは原則禁止する。重要情報を持ち出す場合は以下のような管理手順によって厳格に管理する。
　① 持ち出す情報が適切であることを経営責任者が確認の上、承認を得ること。
　② 持ち出す情報量が必要最小限であることを経営責任者が確認の上、承認を得ること
　③ 万一紛失した際持ち出し情報を特定できるよう、【秘密事項扱いの紙文書の持ち出し状況】【秘密関連機器管理台帳】に記録すること

管理策 7.10　　記憶媒体

記憶媒体は，組織における分類体系及び取扱いの要求事項に従って，その取得，使用，移送及び廃棄のライフサイクルを通して管理しなければならない。

■ **手順**

(1) 認証範囲における個々媒体は、【情報資産リスクアセスメント表】で、保管・廃棄方法、資産価値、想定リスクなどについて管理する。
(2) 会社資産の媒体には資産管理番号を付して、【設備・媒体管理台帳】で、使用・廃棄について管理する。
(3) 個人所有の USB 等の媒体は原則使用禁止とする。
(4) 装置、情報又はソフトウェアを構外に持ち出す場合、【秘密事項扱いの紙文書の持ち出し状況】または【秘密関連機器管理台帳】に記録し、情報セキュリティ管理責任者が承認する。
(5) 従業員は、機器等を社外持ち出しする際は、【情報セキュリティ運用ルール】No. 9 を順守しなければならない。
(6) 情報を格納して社外に持ち出す場合は、「管理策 8.1　　利用者エンドポイント機器」の内容を順守する。

(7) 媒体を廃棄する場合は、【情報資産リスクアセスメント表】に記されている廃棄方法で行う。
(8) 廃棄した場合は、【設備・媒体管理台帳】にその結果を記録し、【情報資産リスクアセスメント表】を更新する。

管理策 7.11　　サポートユーティリティ

情報処理施設・設備は，サポートユーティリティの不具合による，停電，その他の中断から保護しなければならない。

■　手順

(1) 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することが望ましい。
(2) ネットワーク装置等は、事務所に設置しなければならない。
(3) 事務所には、消火器または消火設備を設置し、火災発生時に消火活動ができるようにしなければならない。

管理策 7.12　　ケーブル配線のセキュリティ

電源ケーブル，データ伝送ケーブル又は情報サービスを支援するケーブルの配線は，傍受，妨害又は損傷から保護しなければならない。

■　手順

(1) 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、妨害又は損傷をさけて配線する。(現在ノート PC の電源等のケーブルのみ)

管理策 7.13　　装置の保守

装置は、情報の可用性、完全性及び機密性を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。

■　手順

(1) 保守が必要な装置は、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、正しく保守する。
(2) 定期的に保守すべき装置は無い。

管理策 7.14　　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てるよう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。

■　手順

(1) 不要になった PC、サーバー及びハードディスク等の記憶装置を廃棄する場合は、経営責任者に承認されたうえで、情報セキュリティ管理者に申請しなければならない。

(2) 不要になった PC、サーバー及びハードディスク等の記憶装置を廃棄する場合は、廃棄業者に委託し、データ消去証明を入手しなければならない。

(3) 異動等で PC の利用者が変更になる場合、不要なデータを削除しなければならない。

8　技術的管理策

管理策 8.1　　利用者エンドポイント機器

利用者エンドポイント機器に保存されている情報，処理される情報，又は利用者エンドポイント機器を介してアクセス可能な情報を保護しなければならない。

■　手順

(1) 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する。

(2) 当社の業務上でのモバイル機器の利用について、その利用方針を次に定める。

① ノート PC 等の構外での使用については、持ち出し申請を行うこと。

② ノート PC 等は、ユーザー名とパスワード入力を必須とする。

③ 持ち出し者はノート PC 等を所定の場所に返却するまで、常に安全な状態を保つこと。

④ 会社貸与の携帯電話を紛失した場合は、遠隔ロックサービスを利用し、情報の漏えいを防止する。

(3) 情報セキュリティ管理者は、アクセス権限のない者の不正アクセスから保護する為、重要な PC 等にパスワードロック対策（スクリーンセーバーやログオフ・電源オフ等）を施し、アクセス権限のない者が容易に操作できないように指示する。

管理策 8.2　　特権的アクセス権

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。

■　手順

(1) 特権の割当て及び使用は、制限し、管理する。

(2) 一般従業員には特権 ID を与えてはならない。

(3) 特権 ID は、情報セキュリティ管理者、保守会社及び、データセンターの定められた人以外には与えてはならない。特権 ID の登録は情報セキュリティ管理者が申請し、経営責任者の許可を得る。

(4) 不要となった特権 ID は直ちに抹消する。

(5) 特権 ID はそれを必要としない業務に使用してはならない。

(6) 特権 ID の初期パスワードは変更する。

(7) 特権 ID の利用者について、1 回/年以上、レビューする。

管理策 8.3　　情報へのアクセス制限

情報及びその他の関連資産へのアクセスは，確立されたアクセス制御に関するトピック固有の方針に従って，制限しなければならない。

■ **手順**

(1) 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、制限する。
(2) 経営責任者は、ログイン ID を個人別に発行し、管理する。
(3) 従業員は、担当する職務に応じて利用できるメニューが制限される。

管理策 8.4　　ソースコードへのアクセス

ソースコード，開発ツール，及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理しなければならない。

■ **手順**

(1) プログラムソースコードは社内に保持しない。

管理策 8.5　　セキュリティを保った認証

セキュリティを保った認証技術及び手順を，情報へのアクセス制限，及びアクセス制御に関するトピック固有の方針に基づいて備えなければならない。

■ **手順**

(1) 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する。
(2) 3 回のパスワード入力の失敗の後、システム管理者がリセットするまで ID、パスワードを使用停止にする。

管理策 8.6　　容量・能力の管理

現在の及び予測される容量・能力の要求事項に合わせて，資源の利用を監視し，調整しなければならない。

■ **手順**

(1) Microsoft Bisuness One Drive について、情報セキュリティ管理者がハードディスクの容量を 1 回/半年確認する。
(2) Microsoft Bisuness One Drive の応答時間など、経営責任者がその負荷状況について業務を通じて、問題がないかどうかについて能力を 1 回/半年毎に確認する。

管理策 8.7　　マルウェアに対する保護

マルウェアに対する保護を実施し，利用者の適切な認識によって支援しなければならない。

■　**手順**

(1) ウィルス対策ソフトの更新プログラムは常に最新版を使用するよう自動更新設定を施す。
(2) すべてのファイルをウィルス対策ソフトで定期的にスキャンし、マルウェアが存在しないか確かめる。
(3) 不明な相手先からの受信メールを安易に開封してはならない。
(4) 不審なメールに含まれる、Web リンクはむやみにクリックしてはならない。
(5) メールの添付ファイルを不用意に開かない。
(6) 業務外の Web サイトを閲覧しない。
(7) 禁止ソフトウェアおよびアプリは、業務で使用するＰＣ、スマートデバイスにインストールおよび業務資利用しない。

管理策 8.8　　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を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，適切な手段をとらなければならない。

■　**手順**

(1) 全ての管理者および従業員は、クライアント PC のソフトウェア更新を自動適用に設定する。
(2) 異常を発見した場合は、「管理策 5.26　情報セキュリティインシデントへの対応」に従って対処する。

管理策 8.9　　構成管理

ハードウェア，ソフトウェア，サービス及びネットワークのセキュリティ構成を含む構成を確立し，文書化し，実装し，監視し，レビューしなければならない。

■　**手順**

(1) 組織は、ハードウェア、ソフトウェア、サービス（例えば、クラウドサービス）及びネットワークに関して、新しく導入したシステムに関して、並びに運用システムに関して、それらの存続期間にわたって、定義した構成（セキュリティ構成を含む。）を維持するためのプロセス及びツールを定義し実装する。
(2) 社有 PC は、インストールされているソフトウェアが【ソフトウェア管理台帳】通りであることを 1 回/年監査する。
(3) クラウドサービスについては、1 回/年　業務機能、及びセキュリティ対策について大きな変化がな

いことを各サービスの HP で確認する。

管理策 8.10　　情報の削除

情報システム，装置又はその他の記憶媒体に保存している情報は，必要でなくなった時点で削除しなければならない。

■　**手順**

(1) 取扱いに慎重を要する情報は、望ましくない開示のリスクを減らすために、必要な期間より長く保持しない。

(2) 第三者が組織に代わってその情報を保存する場合、組織は、情報の削除に関する要求事項を第三者との合意に含め、サービスの実施中及び終了時に実行させることを検討する。

(3) データの保持に関する組織のトピック固有の個別方針に従い、また、関連する法律及び規制を考慮して、取扱いに慎重を要する情報は、必要がなくなったとき次の方法で削除する。

a)　古い版、複製及び一時ファイルは、それらがどこにあっても削除する。

管理策 8.11　　データマスキング

データマスキングは，適用される法令を考慮して，組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針，並びに事業上の要求事項に従って利用しなければならない。

■　**手順**

(1) 取扱いに慎重を要するデータ（例えば、PII（Personally Identifiable Information：個人識別用情報））はアクセス制御により経営責任者のみがアクセス可能。必要に応じてマスキングを行う。

管理策 8.12　　データ漏えい防止

データ漏えい防止対策を，取扱いに慎重を要する情報を処理，保存又は送信するシステム，ネットワーク及びその他の装置に適用しなければならない。

■　**手順**

(1) データ漏えいのリスクを減らすために次の事項を考慮する。

a)　漏えいから保護する情報（例えば、個人情報、価格設定モデル及び製品設計）の特定及び分類

b)　データ漏えいのチャネルの監視（例えば、電子メール、ファイル転送、モバイル装置及び携帯可能な記憶装置）

c)　情報漏えいを防止するための処置（例えば、取扱いに慎重を要する情報を含むメールの検疫）

(2) アクセス制御により経営責任者のみがアクセス可能である。監査ログでアクセス履歴を監査する。

管理策 8.13　　情報のバックアップ

合意されたバックアップに関するトピック固有の方針に従って，情報，ソフトウェア及びシステムのバックアップを維持し，定期的に検査しなければならない。

■　**手順**

(1) 重要なファイルおよびソフトウェアは経営責任者により 1 回/月にバックアップする。
1 回/月、存在することを検査する。

管理策 8.14　　情報処理施設・設備の冗長性

情報処理施設・設備は，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。

■　**手順**

(1) Microsoft　Business の One Drive は冗長化されている。
(2) 執務室内の NW 機器は、スマホによるデザリングにより障害発生時に代用する。

管理策 8.15　　ログ取得

活動，例外処理，過失及びその他の関連する事象を記録したログを取得し，保存し，保護し，分析しなければならない。

■　**手順**

(1) パスワードのアタック等インターネットからの不正アクセスは、ログ情報にて確認する。
(2) 従業員に対して、セキュリティ違反に関する活動は記録されることを、明確に知らせる。
(3) システム管理者の作業は、記録し、そのログを保護し、定期的にレビューする。
(4) 経営責任者は、オペレーションの運用記録を定期的にレビューし、【運用状況チェックリスト】に記録する。
(5) ログ情報は、特権 ID を与えられた者だけがアクセスできるように限定する。
(6) ログファイルが一定容量を超えると上書きされる方式である場合は、バックアップサイクル内で消失してしまわないよう容量設計する。
(7) Microsoft Bisuness の監査ログで監視する。手順は【操作手順集】を参照する。

管理策 8.16　　監視活動

情報セキュリティインシデントの可能性を評価するために，ネットワーク，システム及びアプリケーションについて異常な挙動がないか監視し，適切な処置を講じなければならない。

■　**手順**

(1) 監視記録は、５年間維持する。
(2) 組織は、正常な行動・動作の基準を確立し、この基準に照らして異常を監視する。
(3) 監視は、１回/月の間隔でログを取得する。
(4) Microsoft Bisuness の監査ログで監視する。手順は【操作手順集】を参照する。

管理策 8.17　　クロックの同期　対象外

組織が使用する情報処理システムのクロックは，組織が採用した時刻源と同期させなければならない。

■　**手順**

(1) PC は OS の設定により自動的に同期している。

管理策 8.18　　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。

■　**手順**

(1) 一般利用者はアクセス権により特権プログラムを使用できない。

管理策 8.19　　運用システムへのソフトウェアの導入

運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施しなければならない。

■　**手順**

(1) 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、実施する。
(2) パソコンへソフトウェアを追加インストールする場合は、情報セキュリティ管理者の許可を得る。
(3) 情報セキュリティ管理者は、【ソフトウェア管理台帳】で、ソフトウェアのインストールされたハードウェアを管理する。

管理策 8.20　　ネットワークセキュリティ

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，ネットワーク及びネットワーク装置のセキュリティを保ち，管理し，制御しなければならない。

■　**手順**

~~(1)~~ 社内 NW の IP アドレス付与は行わない。

(2) ルーターの設定情報は経営責任者の認可を得なければ設定変更してはならない。

管理策 8.21　　ネットワークサービスのセキュリティ

ネットワークサービスのセキュリティ機能，サービスレベル及びサービスの要求事項を特定し，実装し，監視しなければならない。

■　**手順**

(1) 外部データセンターのレンタルサーバや社内ネットワークへの接続は、ユーザー名、パスワード認証により接続を制限する。

(2) ネットワーク関連サービスを新たに契約する場合は、次の要求事項について確認し、HP でのアナウンスされていることを確認する、または契約書へ盛り込む。

① セキュリティの確保

② サービスの品質の確保

③ 保守体制とサービスレベル

管理策 8.22　　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，組織のネットワーク上で，グループごとに分離しなければならない。

■　**手順**

(1) ネットワーク環境は、以下に示す 1 環境とする。

① インターネット(クラウドサービス)と接続する環境

管理策 8.23　　ウェブフィルタリング

悪意のあるコンテンツにさらされることを減らすために，外部ウェブサイトへのアクセスを管理しなければならない。

■　**手順**

(1) 不要なサイトへのアクセスは行わない。制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合は、経営責任者の承認を必要とする。

管理策 8.24　暗号の利用

暗号鍵の管理を含む，暗号の効果的な利用のための規則を定め，実施しなければならない。

■ **手順**

(1) 機密情報を電子メールで送信する場合は、パスワードで保護するか又は暗号化措置を施す。
(2) 機密情報を保護するために設定したパスワードを相手方へ伝達する場合は、機密情報を含む電子メールと別の電子メールまたは別の伝達方法を用いる。
(3) 公式 Web サイトの入力フォームから取得する情報は SSL/TLS により暗号化し、鍵の有効期限を管理し、期限が切れる前にサーバー証明書を更新する。
(4) 無線 LAN の通信は暗号化し、暗号化の規格はぜい弱性の報告されていない安全な方法とし、接続はパスワードを設定する。

管理策 8.25　セキュリティに配慮した開発のライフサイクル

ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し，適用しなければならない。

■ **手順**

(1) 自社内での開発作業は無い為対象外。
(2) 客先環境での開発は、クライアントから提示のあったセキュリティの方針・ルール等に従う。

管理策 8.26　アプリケーションセキュリティの要求事項

アプリケーションを開発又は取得する場合，情報セキュリティ要求事項を特定し，規定し，承認しなければならない。

■ **手順**

(1) 自社内での開発作業は無い為対象外。
(2) 客先環境での開発は、クライアントから提示のあったセキュリティの方針・ルール等に従う。

管理策 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

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

テムの開発活動に対して適用しなければならない。

■ **手順**

(1) 自社内での開発作業は無い為対象外。
(2) 客先環境での開発は、クライアントから提示のあったセキュリティの方針・ルール等に従う。

管理策 8.28　セキュリティに配慮したコーディング

セキュリティに配慮したコーディングの原則をソフトウェア開発に適用しなければならない。

■ **手順**

(1) 自社内での開発作業は無い為対象外。
(2) 客先環境での開発は、クライアントから提示のあったセキュリティの方針・ルール等に従う。

管理策 8.29　開発及び受入れにおけるセキュリティテスト

セキュリティテストのプロセスを開発のライフサイクルにおいて定め，実施しなければならない。

■ **手順**

(1) 自社内での開発作業は無い為対象外。
(2) 客先環境での開発は、クライアントから提示のあったセキュリティの方針・ルール等に従う。
(3) 外部委託先での開発においては、委託先に任せる。

管理策 8.30　外部委託による開発

組織は，外部委託したシステム開発に関する活動を指揮し，監視し，レビューしなければならない。

■ **手順**

(1) 開発したソフトウェアのコードの所有権及び知的所有権は、予め委託先（外部委託先）との間で明確にする。
(2) スケジュールに対する進捗状況は、定期的に委託先の責任者から報告させる。
(3) ソフトウェアの検収後の保証期間は、予め委託先と取決めをする。
(4) 当社の承認なしで委託先が再委託する事は、禁止する。
(5) 必要時は当社が委託先を監査することを、予め合意しておく。

管理策 8.31　開発環境、テスト環境及び本番環境の分離

開発環境，テスト環境及び本番環境は，分離してセキュリティを保たなければならない。

■ 手順

(1) 自社内での開発作業は無い為対象外。
(2) 客先環境での開発は、クライアントから提示のあったセキュリティの方針・ルール等に従う。

管理策 8.32　　変更管理

情報処理設備及び情報システムの変更は，変更管理手順に従わなければならない。

■ 手順

(1) 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、管理する。
(2) 以下に記載するシステム変更については、経営責任者の承認を得る。
　① クライアント PC の OS 変更
　② 外部ネットワークとの接続
　③ 委託先データセンターの変更
(3) 変更が発生する場合、【変更管理記録表】に変更要求・変更計画を記入し、システム管理責任者の承認を得る。
(4) 情報セキュリティ管理者は必要に応じて利用者へ変更の詳細について通知する。
(5) 承認者の不在時に緊急に変更する必要が生じた場合は、後日速やかに承認を得るものとする。
(6) 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する。
(7) 情報セキュリティ管理者は、社内からシステムの変更の依頼を受けた場合、変更によって関連システムに悪影響を及ぼさないか確認し、作業スケジュールを検討する。
(8) 情報セキュリティ管理者は、検討した変更内容とスケジュールについて【変更管理記録表】に記入し、システム管理責任者の承認を得る。
(9) 情報セキュリティ管理者は、システムの安定稼働を確実にするために、変更、追加部分を明確にし、想定される影響について妥当性の確認を行う。
(10) 社内システム・業務ソフトのオペレーティングシステム（OS）を変更する場合は、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【アプリケーションレビュー記録】に記録する。
(11) パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。

管理策 8.33　　テスト用情報

テスト用情報は，適切に選定し，保護し，管理しなければならない。

■ **手順**

(1) 自社内での開発作業は無い為対象外。

(2) 客先環境での開発は、クライアントから提示のあったセキュリティの方針・ルール等に従う。

管理策 8.34　　監査におけるテスト中の情報システムの保護

運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し，テスト実施者と適切な管理層との間で合意しなければならない。

■ **手順**

(1) 監査の範囲は経営責任者の合意を得た上で、業務に支障がないように配慮する。

〔制定・改訂履歴〕

版数	制定・改定日	制定または改訂主旨	作成	承認
1.0	2025/7/11	初版	岡	塩田
2.0	2025/8/30	手順の確認	岡	塩田
2.1	2025/9/8	5.7、5.19、5.20、5.21、8.11　手順を変更	岡	塩田
2.2	2025/10/14	7.2　入退室記録表→入館簿　名称変更	岡	塩田
		5.7　脅威の収集方法を修正	岡	塩田
		5.16　ID 発行手順を明確化	岡	塩田
		6.8　情報セキュリティ事象の報告　手順を明確化	岡	塩田
		8.29　外部委託先での開発について追加	岡	塩田
2.3	2025/10/27	5.18　誤字を修正	岡	塩田
		7.10　情報持出時に記録する帳票を修正。		
		全体　【手順集】→【操作手順集】へ変更		
2.4	2025/11/18	5.13 情報のラベル付け　紙や電子データは、経営責任者のみアクセス可能な情報が多い為、「社外秘」については経営責任者の承認の上、ラベル付けは省略可能の記載を追記。	岡	塩田
		6.2 雇用条件　(1)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する。 を削除。	岡	塩田
2.5	2025/11/30	管理策 8.23 ウェブフィルタリング　誤記修正	岡	塩田
2.6	2025/12/1	管理策 6.2　雇用条件 捺印は不要。修正。	岡	塩田
2.7	2025/12/3	管理策 5.4　　管理層の責任 契約相手は契約会社で教育する為、不要につき削除。	岡	塩田
		管理策 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管理　誤記修正　((2) →(1))	岡	塩田
		管理策 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　誤記修正(シニアプロフェッショナル→リードプロフェッショナル)	岡	塩田
		管理策 5.34　　プライバシー及び個人識別可能情報（PII）の保護　個人情報はもたない為、	岡	塩田

		(2)を削除		
		管理策 6.5　雇用の終了又は変更後の責任 契約相手は不要につき削除。		
		管理策 7.8　装置の設置及び保護　誤字修正(組織→事務所内)	岡	塩田
		管理策 7.9　構外にある資産のセキュリティ　帳票名を修正	岡	塩田
		管理策 7.10　記憶媒体　帳票名を修正	岡	塩田
		管理策 7.11　サポートユーティリティ　誤字修正(執務室→事務所)	岡	塩田
		管理策 7.12　ケーブル配線のセキュリティ 「上に伸ばす」必要はない為、削除	岡	塩田
		管理策 7.13　装置の保守　NW 機器は以後は本項目とは関係が無い為、削除。	岡	塩田
		管理策 8.8　技術的ぜい弱性の管理　技術的ぜい弱性に関するレビューは IPA メール授受にて実施する為、削除	岡	塩田
		管理策 8.23　ウェブフィルタリング 不要な記載を削除	岡	塩田