適用宣言書

バージョン: 1.0

改訂日: 2024年4月1日

出力日: 2026年3月5日

目次

22. A.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

23. A.5.23 クラウドサービス利用における情報セキュリティ

24. A.5.24 情報セキュリティインシデント管理の計画及び準備

25. A.5.25 情報セキュリティ事象の評価及び決定

26. A.5.26 情報セキュリティインシデントへの対応

27. A.5.27 情報セキュリティインシデントからの学習

28. A.5.28 証拠の収集

29. A.5.29 事業の中断・阻害時の情報セキュリティ

30. A.5.30 事業継続のためのICTの備え

31. A.5.31 法令、規制及び契約上の要求事項

32. A.5.32 知的財産権

33. A.5.33 記録の保護

34. A.5.34 プライバシー及びPIIの保護

35. A.5.35 情報セキュリティの独立したレビュー

36. A.5.36 情報セキュリティのための方針群、規則及び標準の遵守

37. A.5.37 操作手順書

38. A.6.1 選考

39. A.6.2 雇用条件

40. A.6.3 情報セキュリティの意識向上、教育及び訓練

41. A.6.4 懲戒手続

42. A.6.5 雇用の終了又は変更後の責任

43. A.6.6 機密保持契約又は守秘義務契約

44. A.6.7 リモートワーク

45. A.6.8 情報セキュリティ事象の報告

46. A.7.1 物理的セキュリティ境界

47. A.7.2 物理的入退

48. A.7.3 オフィス、部屋及び施設のセキュリティ

49. A.7.4 物理的セキュリティの監視

50. A.7.5 物理的及び環境的脅威からの保護

51. A.7.6 セキュリティを保つべき領域での作業

52. A.7.7 クリアデスク・クリアスクリーン

53. A.7.8 装置の設置及び保護

54. A.7.9 構外にある資産のセキュリティ

55. A.7.10 記憶媒体

56. A.7.11 サポートユーティリティ

57. A.7.12 ケーブル配線のセキュリティ

58. A.7.13 装置の保守

59. A.7.14 装置のセキュリティを保った処分又は再利用

60. A.8.1 利用者エンドポイント機器

61. A.8.2 特権的アクセス権

62. A.8.3 情報へのアクセス制限

63. A.8.4 ソースコードへのアクセス

64. A.8.5 セキュリティを保った認証

65. A.8.6 容量・能力の管理

66. A.8.7 マルウェアに対する保護

67. A.8.8 技術的脆弱性の管理

68. A.8.9 構成管理

69. A.8.10 情報の削除

70. A.8.11 データマスキング

71. A.8.12 データ漏洩の防止

72. A.8.13 情報のバックアップ

73. A.8.14 情報処理施設の冗長性

74. A.8.15 ログ取得

75. A.8.16 監視活動

76. A.8.17 クロックの同期

77. A.8.18 特権的なユーティリティプログラムの使用

78. A.8.19 運用システムに関わるソフトウェアの導入

79. A.8.20 ネットワークのセキュリティ

80. A.8.21 ネットワークサービスのセキュリティ

81. A.8.22 ネットワークの分離

82. A.8.23 ウェブ・フィルタリング

83. A.8.24 暗号の使用

84. A.8.25 セキュリティに配慮した開発のライフサイクル

85. A.8.26 アプリケーションのセキュリティ要求事項

86. A.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

87. A.8.28 セキュリティに配慮したコーディング

88. A.8.29 開発及び受入れにおけるセキュリティ試験

89. A.8.30 外部委託による開発

90. A.8.31 開発環境、試験環境及び運用環境の分離

91. A.8.32 変更管理

92. A.8.33 試験情報

93. A.8.34 監査試験中の情報システムの保護

A.5.1 情報セキュリティのための方針群

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.1
分類	組織的管理策

管理策

情報セキュリティ方針及びトピック固有の方針は、定義し、経営陣が承認し、発行し、関連する要員及び関係する利害関係者に伝達し、認識させ、計画し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。

目的

経営陣の方向性及び情報セキュリティに対する支持を、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規定するため。

実施の手引き

組織は、最上位レベルで「情報セキュリティ方針」を定義し、経営陣の承認を得る必要がある。この方針には以下を含めることが推奨される。

- 情報セキュリティの定義、目的及び原則
- 情報セキュリティに関する役割及び責任の割当て
- 例外及び免除を扱うプロセス
- 情報セキュリティ方針の不遵守の結果

トピック固有の方針は、組織のニーズに基づいて策定し、以下のような分野を対象とすることができる。

- アクセス制御
- 物理的及び環境的セキュリティ
- 資産管理
- 情報転送
- エンドポイントデバイスのセキュリティ設定
- ネットワークセキュリティ
- 情報セキュリティインシデント管理
- バックアップ
- 暗号及び鍵管理
- 情報の分類及び取扱い
- 技術的ぜい弱性の管理
- セキュアな開発

当社における実施状況

当社では、情報セキュリティ責任者（代表取締役）の承認のもと、情報セキュリティ方針を策定し、全従業員に周知している。方針は年1回および重大な変化が発生した場合にレビューを行う。

関連文書

- 情報セキュリティ基本方針
- 1. 組織的対策
- 2. 人的対策
- 3. 情報資産管理
- 4. アクセス制御及び認証
- 5. 物理的対策
- 6. IT機器利用
- 7. IT基盤運用管理
- 8. システム開発及び保守
- 9. 委託管理

- 10. 情報セキュリティインシデント対応及び事業継続管理
- 11. テレワークにおける対策

A.5.2 情報セキュリティの役割及び責任

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.2
分類	組織的管理策

管理策

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義し、割り当てなければならない。

目的

組織内で情報セキュリティの実施、運用及び管理のための明確な構造を確立するため。

実施の手引き

情報セキュリティの役割及び責任の割当ては、情報セキュリティ方針に従って行う必要がある。以下の責任を定義し、割り当てることが推奨される。

- 情報及びその他の関連資産の保護
- 特定の情報セキュリティプロセスの実行
- 情報セキュリティリスクマネジメント活動、特にリスクの受容
- 情報及びその他の関連資産を使用するすべての活動

これらの責任は、必要に応じて、特定のサイト及び情報処理施設に対する追加の責任で補完する必要がある。

当社における役割分担

役職名	役割・責任	担当
情報セキュリティ責任者	情報セキュリティに関する方針の決定および全体の最終責任を負う	代表取締役
情報セキュリティ部門責任者	各業務における情報セキュリティ対策の運用管理および実施責任を負う	CTO
システム管理者	情報システムに対する技術的セキュリティ対策の設計・導入・運用	CTO（兼務）
インシデント対応責任者	インシデント発生時の影響評価、対応方針の決定および対応の指揮	CTO
個人情報保護管理者	個人情報保護法および関連法令の遵守責任	代表取締役
教育責任者	情報セキュリティ教育の企画・実施・記録管理	管理部責任者（または代表取締役）
監査・点検責任者	情報セキュリティ関連規程および運用状況の点検・評価	管理部責任者（または代表取締役）

当社における実施状況

当社では、情報セキュリティに関する役割及び責任を上記の通り定義し、各担当者に割り当てている。少人数体制のため、一部の役割は兼務としているが、責任の所在は明確にしている。役割分担は、組織変更や人事異動が発生した場合に見直しを行う。

関連文書

- 1. 組織的対策

A.5.3 職務の分離

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.3
分類	組織的管理策

管理策

相反する職務及び責任範囲は、分離しなければならない。

目的

組織の資産に対する不正若しくは意図しない変更又は誤用のリスクを低減するため。

実施の手引き

職務の分離は、一人の者が単独で資産にアクセスし、変更し、又は使用することができないようにすることで、エラー及び不正行為のリスクを低減する。

活動の開始、承認及び実行は、分離する必要がある。一人の者が相反する職務を遂行することが不可能又は実際的でない場合は、以下のような他の管理策を検討する必要がある。

- 活動の監視
- 監査証跡
- 経営陣による監督

職務の分離を設計する際には、以下を考慮する必要がある。

- 資産の取得、受領、支払いの承認を分離する

- システム開発と本番運用を分離する
- セキュリティ管理機能と一般的なIT機能を分離する

分離が必要な職務の例

職務1	職務2
システム開発	システム運用
アクセス権申請	アクセス権承認
変更要求	変更承認
監査実施	監査対象業務

当社における実施状況

組織構成と職務分離の課題

当社は少人数組織であり、一人の者が複数の職務を兼務することが避けられない。特にシステム開発・運用においては、開発メンバーが設計・実装・本番反映を一貫して担当する体制となっている。このため、従来型の「人員による職務分離」を完全に実施することは実際的でない。

代替統制：重要な変更に対する経営層確認

上記の制約を踏まえ、当社では以下の代替統制を実施している。

役割分担

役割	担当者	責任範囲
技術的実装・運用	開発メンバー	システムの設計、実装、テスト、本番反映
経営判断・承認	CEO（代表取締役）	重要な変更に対する事業影響確認、承認

CEO確認対象となる変更

全ての変更ではなく、以下に該当する重要な変更についてCEOが確認・承認を行う。

- 顧客に影響を与える機能変更・追加

- セキュリティ・権限・データに関わる変更
- 外部公開される変更（新機能リリース等）
- 事業リスクを伴う変更

軽微な変更（バグ修正、内部改善、ドキュメント更新等）については、開発メンバーの判断で実施し、必要に応じて事後報告とする。

統制プロセス

重要な変更については、開発メンバーがリリースノートを作成し、CEOがその内容を確認・承認する。これにより「活動の開始」と「承認」が分離され、重要な変更が一人で完結しない体制を確保している。

CEOによる確認は、技術的な実装詳細（コミット単位）ではなく、リリース単位で以下の観点から行う。

- 事業としてその変更を承認できるか
- リスクを理解した上でリリースしたか
- 顧客・外部への影響を把握しているか

リリースノートの記載事項

項目	内容
リリース日	変更を本番反映した日付
概要	何が変わったかの説明
影響範囲	顧客影響の有無、内部のみか外部公開か
セキュリティ影響	セキュリティ・権限・データへの影響の有無
ロールバック可否	必要に応じて記載

代替統制の妥当性

この代替統制は、ISO 27001の実施の手引きに記載された「一人の者が相反する職務を遂行することが不可能又は実際的でない場合」の対応として、以下を満たしている。

- **経営陣による監督**: CEOがリリース内容と影響を確認
- **監査証跡**: リリースノートが変更履歴と承認の証跡となる
- **活動の監視**: リリース単位での変更管理により、変更内容を追跡可能

関連文書

- 1. 組織的対策

A.5.4 経営陣の責任

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.4
分類	組織的管理策

管理策

経営陣は、組織の確立された方針、トピック固有の方針及び手順に従って情報セキュリティを適用することを、すべての要員に要求しなければならない。

目的

経営陣が情報セキュリティにおける自らの役割を理解し、すべての要員が情報セキュリティの責任を認識し、果たすことを確実にするための措置を講じることを確実にするため。

実施の手引き

経営陣は、以下を実証する必要がある。

- 情報セキュリティの役割及び責任を認識していること
- 情報セキュリティ方針を支持していること
- 情報セキュリティ目的の達成を支援していること
- 情報セキュリティ文化を促進していること

経営陣は、要員が以下を行うことを確実にする必要がある。

- 情報セキュリティに関する適切な意識向上、教育及び訓練を受ける
- 方針及び手順を遵守する

- 情報セキュリティの責任を果たす

経営陣の具体的な責任

責任	内容
方針の承認と支持	情報セキュリティ方針の承認と積極的な支持
リソースの割当て	適切な人員・予算・設備の確保
目的の設定と監視	情報セキュリティ目的の設定と達成の監視
パフォーマンスのレビュー	情報セキュリティパフォーマンスの定期的なレビュー
継続的改善の推進	ISMSの継続的改善の推進

当社における実施状況

当社では、情報セキュリティ責任者（代表取締役）が情報セキュリティに関する最終責任を負い、情報セキュリティ部門責任者（CTO）が運用管理責任を負う。経営陣は情報セキュリティ方針の承認、リソースの提供、定期的なレビューを通じて責任を果たしている。

関連文書

- 1. 組織的対策

A.5.5 関係当局との連絡

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.5
分類	組織的管理策

管理策

組織は、関係当局との連絡を確立し、維持しなければならない。

目的

情報セキュリティインシデントが発生した場合に、適切な当局との適切な情報の流れを確保するため。また、現在及び将来の法的又は規制上の要求事項及び義務を理解するため。

実施の手引き

組織は、以下の当局との連絡を維持する手順を持つ必要がある。

- 法執行機関
- 規制当局
- 監督官庁
- 消防署
- データ保護当局

連絡先情報は、最新の状態に維持し、関係者が利用できるようにする必要がある。

連絡先リスト

当局	連絡先	連絡する状況
警察	110	サイバー犯罪、不正アクセス
消防署	119	火災、災害
個人情報保護委員会	-	個人データ漏洩
IPA（情報処理推進機構）	-	セキュリティインシデント報告
JPCERT/CC	-	インシデント対応支援

当社における実施状況

当社では、情報セキュリティ共有者（管理部担当者）がIPA、JVN、JPCERT/CC、個人情報保護委員会等の外部機関から脅威インテリジェンス情報を収集し、適時全従業員に共有している。情報セキュリティ部門責任者（CTO）は、追加で対応が必要な脅威情報を認識した場合、情報セキュリティ共有者に伝達し、全従業員への共有を依頼する。

関連文書

- 1. 組織的対策
- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.6 専門組織との連絡

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.6
分類	組織的管理策

管理策

組織は、専門組織又はその他のセキュリティフォーラム及び専門家団体との連絡を確立し、維持しなければならない。

目的

情報セキュリティに関する知識を最新の状態に維持するため。

実施の手引き

専門組織又はフォーラムへの参加は、以下の目的で検討する必要がある。

- セキュリティのベストプラクティスに関する知識の向上
- 関連するセキュリティ情報の最新状態の維持
- 新たな脅威及びぜい弱性に関する早期警告の受信
- セキュリティインシデント対応時の専門家へのアクセス
- セキュリティに関する助言の入手

当社における実施状況

当社では、IPA、JVN、JPCERT/CC、個人情報保護委員会等の外部機関との連絡体制を確立している。インシデント発生時には、必要に応じてこれらの機関への報告を行う。

関連文書

- 1. 組織的対策
- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.7 脅威インテリジェンス

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.7
分類	組織的管理策

管理策

情報セキュリティの脅威に関する情報を収集し、分析して、脅威インテリジェンスを作成しなければならない。

目的

組織が脅威環境を認識し、適切な緩和措置を講じることができるようにするため。

実施の手引き

脅威インテリジェンスは、以下の3つの層に分類できる。

戦略的脅威インテリジェンス

変化する脅威の状況に関する高レベルの情報であり、経営陣の意思決定を支援する。

戦術的脅威インテリジェンス

攻撃者の戦術、技術及び手順（TTP）に関する情報であり、セキュリティ対策の計画を支援する。

運用的脅威インテリジェンス

特定の攻撃に関する技術的詳細であり、インシデント対応を支援する。

脅威インテリジェンスの情報源

情報源	内容
JPCERT/CC	脆弱性情報、注意喚起
IPA	セキュリティ情報、脅威レポート
警察庁	サイバー犯罪動向
セキュリティベンダー	脅威レポート、分析
ISAC	業界固有の脅威情報

脅威インテリジェンスの活用

- リスクアセスメントへの反映
- セキュリティ対策の優先順位付け
- インシデント対応の改善
- 従業員教育への活用

当社における実施状況

当社では、情報セキュリティ共有者（管理部担当者）がIPA、JVN、JPCERT/CC等のセキュリティ関連機関から脅威情報を収集し、適時全従業員に共有している。情報セキュリティ部門責任者（CTO）は、追加で対応が必要な脅威情報を認識した場合、情報セキュリティ共有者に伝達し、全従業員への共有を依頼する。

関連文書

- 1. 組織的対策

A.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

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.8
分類	組織的管理策

管理策

情報セキュリティは、プロジェクトマネジメントに統合しなければならない。

目的

プロジェクトの実施中に情報セキュリティリスクが効果的に対処されることを確実にするため。

実施の手引き

情報セキュリティは、プロジェクトの種類に関係なく、すべてのプロジェクトに統合する必要がある。これには以下が含まれる。

- 情報システムプロジェクト
- ビジネスプロセスプロジェクト
- 施設プロジェクト
- 組織変更プロジェクト

プロジェクトにおけるセキュリティ活動

フェーズ	セキュリティ活動
企画	セキュリティ要件の特定、リスクアセスメント
設計	セキュリティアーキテクチャの設計、管理策の選定
開発	セキュアコーディング、コードレビュー
テスト	セキュリティテスト、脆弱性診断
導入	セキュリティ設定の確認、承認
運用	監視、インシデント対応
終了	データの安全な廃棄、アクセス権の削除

プロジェクトマネジメントへの統合ポイント

- プロジェクト計画にセキュリティ活動を含める
- セキュリティレビューをマイルストーンに設定
- セキュリティ担当者をプロジェクトチームに含める
- セキュリティリスクをプロジェクトリスクとして管理

当社における実施状況

当社では、新規プロジェクトや業務プロセスの企画段階から情報セキュリティ要件を検討し、情報セキュリティ部門責任者（CTO）がレビューを行っている。

関連文書

- 1. 組織的対策
- 8. システム開発及び保守

A.5.9 情報及びその他の関連資産の目録

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.9
分類	組織的管理策

管理策

情報及びその他の関連資産（関連する管理責任者を含む。）の目録を作成し、維持しなければならない。

目的

組織の情報及びその他の関連資産を特定し、適切な保護を確実にするため。

実施の手引き

目録には、情報セキュリティに関連するすべての資産を含める必要がある。資産は以下のように分類できる。

情報資産

電子データ、紙文書、知的財産

物理的資産

コンピュータ機器、通信機器、記憶媒体

ソフトウェア資産

アプリケーションソフトウェア、システムソフトウェア、開発ツール

サービス

クラウドサービス、通信サービス、ユーティリティサービス

目録に含める情報

項目	説明
資産ID	一意の識別子
資産名	資産の名称
資産の種類	情報、物理、ソフトウェア等
管理責任者	資産の管理責任者
所在地	資産の保管場所
分類	機密性、完全性、可用性のレベル
取得日	資産の取得日

当社における実施状況

当社では、「12. 情報資産の定義と管理ルール」に基づき、情報資産を識別・分類している。資産の分類は機密性3（極秘）、機密性2（社外秘）、機密性1（公開）の3段階で行い、各クラウドサービスの権限設定やフォルダ構成により管理している。

関連文書

- 3. 情報資産管理

A.5.10 情報及びその他の関連資産の許容される利用

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.10
分類	組織的管理策

管理策

情報及びその他の関連資産の許容される利用並びに取扱いの手順に関する規則は、特定し、文書化し、実施しなければならない。

目的

情報及びその他の関連資産が適切に保護され、使用され、取り扱われることを確実にするため。

実施の手引き

情報及びその他の関連資産を使用するすべての要員は、情報処理施設及び情報の取扱いに関するセキュリティ要求事項を認識する必要がある。

許容される利用の規則

一般原則

- 業務目的のみに使用する
- 法令及び規制を遵守する
- 組織の方針及び手順に従う

- 他者の権利を尊重する

禁止事項

- 私的利用（許可されている場合を除く）
- 不正なソフトウェアのインストール
- 機密情報の不正な開示
- セキュリティ管理策の回避

資産種類別の利用規則

資産種類	許容される利用	禁止事項
電子メール	業務連絡、情報共有	スパム送信、私的利用
インターネット	業務調査、情報収集	不適切なサイトへのアクセス
可搬媒体	承認されたデータ転送	未承認のデータ持ち出し
モバイルデバイス	業務アプリの使用	未承認アプリのインストール

当社における実施状況

当社では、「12. 情報資産の定義と管理ルール」に基づき、各情報資産の利用許容範囲を定めている。業務目的以外での利用は禁止され、SNSへの業務情報の投稿も禁止している。

関連文書

- 3. 情報資産管理
- 6. IT機器利用

A.5.11 資産の返却

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.11
分類	組織的管理策

管理策

要員及び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すべてを返却しなければならない。

目的

雇用、契約又は合意の変更又は終了プロセスの一部として、組織の資産を保護するため。

実施の手引き

返却プロセスは、以下の資産を含むすべての物理的及び電子的資産を対象とする必要がある。

- コンピュータ機器（ノートPC、デスクトップ等）
- モバイルデバイス（スマートフォン、タブレット等）
- 記憶媒体（USBメモリ、外付けHDD等）
- アクセスカード、鍵
- 文書、マニュアル
- ソフトウェアライセンス

返却プロセス

ステップ	内容	担当
1	返却対象資産の特定	管理部
2	返却期限の通知	管理部
3	資産の回収	管理部
4	資産の状態確認	管理部
5	データの消去	管理部
6	返却完了の記録	管理部

BYODに関する取扱い

個人所有デバイスの位置づけ

- 個人所有デバイスは物理的な返却対象とはしない。
- BYOD利用時の業務データ管理は、別途定めるBYOD運用ルールに従う。

業務データの消去

- 業務データは原則として会社指定のクラウド環境上で管理する。
- やむを得ず個人所有デバイス内に保存された業務データについては、退職または業務終了時に管理部の指示のもと削除を行う。
- 業務アカウントの停止をもって、業務データ利用の終了とする。

リモートワーク利用者の対応

- リモートワーク利用者の会社資産は、配送等の手段により回収を行う。
- 配送による回収が困難な場合は、管理部によるデータ消去およびアクセス停止の確認をもって返却に代えることができる。

返却困難時の代替対応（例外処理）

災害、急病、その他やむを得ない事情により物理的返却が困難な場合は、管理部の確認のもと、以下を実施する。

- 業務アカウントの停止
- 業務データの消去確認

上記対応をもって、資産返却完了とみなす。

記録管理

- 資産返却およびデータ消去の結果は、既存の管理ツール（チケット、チェックリスト等）で確認・記録する。
- 管理部は返却完了を確認する。

当社における実施状況

当社では、退職時に全ての情報資産（貸与機器、アクセス権限、データ等）を返却することを義務付けている。退職者のアカウントは速やかに無効化される。

関連文書

- 2. 人的対策
- 4. アクセス制御及び認証

A.5.12 情報の分類

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.12
分類	組織的管理策

管理策

情報は、機密性、完全性、可用性に関する組織の情報セキュリティニーズ及び法的要求事項に従って分類しなければならない。

目的

情報の重要性に応じた適切な保護レベルを確保するため。

方針

情報資産は、その重要性に応じて適切に管理する。当社における情報の分類は、個々の情報へのラベル付与によらず、保存先および利用するシステムに基づいて行う。

分類方法

情報資産は、以下の管理方法により分類する。

機密情報

以下に該当する情報は、機密情報として取り扱う。

- 会社指定のクラウド環境に保存された業務データ

- 業務用アカウントを通じてアクセス可能な情報

社内利用情報

- 社内での共有を目的とし、機密性が比較的低い情報
- 一般的な業務連絡、手続き情報等

公開情報

- 会社Webサイト等で一般に公開している情報
- プレスリリース、採用情報 等

BYOD利用時の取扱い

BYOD利用時においては、業務データを個人所有デバイス内に保存しないことを原則とする。

- 業務データは、会社指定のクラウド環境上で管理する。
- やむを得ず個人所有デバイス内に保存された業務データについては、管理部の指示のもと適切に削除を行う。

管理上の原則

- 情報の分類は、保存先およびアクセス制御により担保する。
- 個々のファイルや情報に対する分類ラベルの付与は行わない。
- 情報へのアクセス権限は、業務上必要な者に限定する。

例外対応

本方針に基づく管理が困難な場合は、管理部の承認を得たうえで代替管理策を講じる。

当社における実施状況

当社では、情報資産を機密情報・社内利用情報・公開情報の3段階に分類し、保存先およびアクセス制御により情報の重要性を担保している。個々のファイルへのラベル付与は行わず、会社指定のクラウド環境での一元管理を原則としている。

関連文書

- 3. 情報資産管理

A.5.13 情報のラベル付け

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.13
分類	組織的管理策

管理策

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。

目的

情報の分類を伝達し、適切な取扱いを促進するため。

方針

当社では、BYODを含む多様な利用環境を考慮し、情報資産に対する個別のラベル付与は原則として実施しない。

代替管理策

情報の重要性は、以下の管理策により担保する。

- 情報の保存先および利用するシステムによる分類（A.5.12）
- アクセス制御および権限管理（A.5.15）
- 業務データのクラウド集中管理および端末保存の制限

例外

法令・契約等によりラベル付与が必要な場合は、管理部の承認のもと、限定的に実施する。

当社における実施状況

当社では、BYODを含む多様な利用環境を考慮し、情報資産に対する個別のラベル付与は原則として実施していない。情報の重要性は、保存先システムによる分類、アクセス制御および権限管理、業務データのクラウド集中管理により担保している。

関連文書

- 3. 情報資産管理

A.5.14 情報転送

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.14
分類	組織的管理策

管理策

情報転送の規則、手順又は合意は、組織内及び組織と他の関係者との間のあらゆる種類の転送設備について整備しなければならない。

目的

転送中の情報のセキュリティを維持するため。

当社における方針

当社は、情報の機密性および完全性を維持するため、情報転送にあたっては、転送手段、保存先および情報の性質を考慮し、適切な保護措置を講じる。

用語の整理

用語	定義
業務データ	業務遂行に用いられる情報であり、原則としてすべて機密情報として取り扱う
機密性を要しない情報	業務データに該当せず、一般に公開されている、または機密性を要しない情報

本規程における取扱いは、上記定義に基づく。

情報転送の原則

業務データは、原則としてメール添付により転送しない。

情報転送は、会社指定のクラウドサービス等、暗号化された通信およびアクセス制御が確保された手段を用いて行う。

電子的手段による情報転送

クラウドサービスの利用

業務データは、HTTPS等により通信が暗号化された会社指定のクラウド環境を用いて共有する。

情報へのアクセスは、業務上必要な者に限定し、権限管理および必要に応じた共有期限の設定を行う。

メールの利用

業務データを含む情報は、原則としてメール添付で送信しない。

やむを得ずメール添付で情報転送を行う場合は、情報の重要性に応じて、暗号化等の適切な保護措置を講じる。

BYOD利用時の取扱い

BYOD利用時においては、業務データを個人所有デバイス内に保存しないことを原則とする。

情報転送は、会社指定のクラウドサービスを介して行い、個人所有デバイスへの直接保存を伴う転送は行わない。

郵便・宅配による情報転送

郵便または宅配による情報転送は、原則として業務データに該当しない、機密性を要しない情報に限定して行う。

機密性を要しない情報については、普通郵便や安価な配送手段を用いることができる。

例外的に業務データを郵送する必要がある場合は、追跡可能な配送手段を用い、内容物が第三者に容易に確認できないよう封緘を行う。

例外対応

本方針に基づく対応が困難な場合は、管理部門の承認を得たうえで、代替手段を講じる。

当社における実施状況

当社では、業務データの転送は会社指定のクラウドサービスを用いて行い、メール添付による転送は原則禁止としている。BYOD利用時も業務データは端末に保存せず、クラウド環境を介した転送を徹底している。

関連管理策

- A.5.12 情報の分類
- A.5.13 情報のラベル付け
- A.5.15 アクセス制御
- A.8.24 暗号化の利用（該当する場合）

A.5.15 アクセス制御

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.15
分類	組織的管理策

管理策

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、実施しなければならない。

目的

情報及びその他の関連資産への認可されたアクセスを確保し、認可されていないアクセスを防止するため。

方針

当社は、情報資産への不正アクセスを防止するため、業務上必要な範囲に限定したアクセス制御を実施する。アクセス権限は、最小権限の原則に基づき付与・管理する。

アクセス制御の原則

情報資産へのアクセスは、原則として個人ごとに付与されたアカウントにより行う。

アクセス権限の付与・変更・削除は、業務上の必要性に基づき、承認を得たうえで実施する。

不要となったアクセス権限は、速やかに削除する。

共有アカウントの取扱い

共有アカウントの使用は原則として禁止する。

ただし、業務上の必要性がある場合に限り、情報セキュリティ責任者の承認を得たうえで、限定的に共有アカウントの利用を認めることがある。

共有アカウントを利用する場合は、利用目的および利用可能者を明確にし、必要最小限の権限を付与する。

権限および利用状況の見直し

アクセス権限および共有アカウントの利用状況については、イベント駆動型（入退社、業務内容変更、委託開始・終了等）で見直しを行う。

見直しの結果、不要または過剰と判断された権限は、変更または削除を行う。

認証情報の管理

アカウントの認証情報は、適切に管理する。

共有アカウントについては、定期的にパスワードの変更を行う。

当社における実施状況

当社では、少人数体制での運用を前提としており、形式的な定期的アクセス権レビュー（一覧点検）は実施していない。その代替として、入退社、業務内容変更、委託開始・終了時にアクセス権を即時見直す運用を行っている。

Microsoft Entra IDを中心としたID管理により、変更履歴を記録・追跡可能としており、不要または過剰なアクセス権が残存しない運用を行っている。

原則として、各従業員に一意のアカウントを付与し、共有アカウントの使用は原則禁止としている。ただし、業務上の必要性がある場合に限り、情報セキュリティ責任者の承認を得たうえで、限定的に共有アカウントの利用を認めている。

アカウントの作成・変更・削除は、情報セキュリティ責任者の承認を得て実施している。

共有アカウントについては、利用状況の見直しを行い、パスワードの変更および利用可能者を必要最小限の範囲に制限するなど、適切な管理を行っている。

関連管理策

- A.5.12 情報の分類
- A.5.13 情報のラベル付け
- A.5.14 情報転送
- A.5.17 認証情報

A.5.16 識別情報の管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.16
分類	組織的管理策

管理策

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。

目的

組織の情報及びその他の関連資産にアクセスする個人及びシステムの一意の識別を可能にするため。

実施の手引き

識別情報の管理には、以下のライフサイクル全体を含める必要がある。

ライフサイクル管理

フェーズ	活動
作成	一意のIDの発行、本人確認
有効化	アカウントの有効化、初期パスワード設定
変更	属性変更、権限変更
無効化	一時的な停止
削除	アカウントの完全削除

識別情報の種類

- ユーザーID
- システムアカウント
- サービスアカウント
- 特権アカウント
- 共有アカウント（原則禁止）

管理要件

- 一意性：各識別情報は一意でなければならない
- 追跡可能性：行動を個人に追跡できること
- 共有禁止：識別情報の共有は原則禁止
- 定期レビュー：不要なアカウントの特定と削除

特権アカウントの管理

- 特権アカウントの使用は最小限に制限
- 特権アカウントの使用を監視・記録
- 特権アカウントには強力な認証を適用

当社における実施状況

当社では、Microsoft Entra IDを中心としたID管理を行っている。各従業員に一意のアカウントを付与し、共有アカウントの使用は禁止している。アカウントの作成・変更・削除は情報セキュリティ責任者の承認を得て実施する。

関連文書

- 4. アクセス制御及び認証

A.5.17 認証情報

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.17
分類	組織的管理策

方針

当社は、情報資産への不正アクセスを防止するため、認証情報を適切に管理し、漏えい・不正使用を防止する。

認証情報の管理原則

認証情報（ID、パスワード等）は、原則として個人ごとに管理する。

認証情報は、第三者に開示、共有または貸与してはならない。

認証情報は、適切な強度および管理方法により保護する。

共有アカウントに関する認証情報

共有アカウントの利用は原則として禁止する。

業務上の必要性により共有アカウントを利用する場合は、情報セキュリティ責任者の承認を得たうえで、利用目的および利用可能者を明確にする。

共有アカウントの認証情報については、定期的にパスワードの変更を行う。

BYOD利用時の取扱い

BYOD利用時においては、認証情報を個人所有デバイス内に保存しないことを原則とする。

業務システムへのアクセスは、会社指定の認証基盤を用いて行う。

認証情報の変更および無効化

認証情報は、必要に応じて変更する。

退職、契約終了、異動等により不要となった認証情報は、速やかに無効化する。

当社における実施状況

当社では、Microsoft Entra IDを中心とした認証基盤を用いて、アカウントおよび認証情報の管理を行っている。

原則として、各従業員に一意のアカウントを付与し、個人ごとの認証情報によりシステムへのアクセスを行っている。

共有アカウントについては、業務上の必要性がある場合に限り、承認制のもとで利用しており、定期的なパスワード変更および利用状況の見直しを行っている。

関連管理策

- A.5.15 アクセス制御
- A.5.12 情報の分類
- A.5.14 情報転送

A.5.18 アクセス権

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.18
分類	組織的管理策

管理策

アクセス権は、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。

目的

情報及びその他の関連資産へのアクセスが認可され、認可されていないアクセスが防止されることを確実にするため。

方針

当社は、情報資産への不正アクセスを防止するため、業務上必要な範囲に限定したアクセス権管理を行う。アクセス権は、最小権限の原則に基づき付与・管理する。

アクセス権の付与および変更

アクセス権の付与、変更および削除は、業務上の必要性に基づき、情報セキュリティ責任者の承認を得たうえで実施する。入退社、異動等により不要となったアクセス権は、速やかに変更または削除する。

アクセス権の見直し

アクセス権の見直しは、年次等の定期イベントではなく、実運用におけるイベント駆動型（入退社、役割変更等）で実施する。当該運用は、権限変更の即時性および実効性を重視したものである。

特権アカウントの取扱い

特権アカウントについては、利用目的および利用者を明確にしたうえで、必要最小限の権限を付与する。特権アカウントの利用状況についても、イベント駆動型で見直しを行い、権限の付与・変更・削除は都度承認を得て実施する。

共有アカウントの取扱い

共有アカウントの使用は原則として禁止する。ただし、業務上の必要性がある場合に限り、承認を得たうえで、限定的に利用を認める。共有アカウントについては、利用状況の見直しおよびパスワードの変更を適宜行い、利用可能者を必要最小限の範囲に制限する。

当社における実施状況

当社では、少人数体制での運用を前提としており、形式的な定期的アクセス権レビュー（一覧点検）は実施していない。その代替として、入退社、業務内容変更、委託開始・終了時にアクセス権を即時見直す運用を行っている。

Microsoft Entra IDを中心としたID管理により、変更履歴を記録・追跡可能としており、クラウドサービス上の監査ログにより事後確認が可能である。

原則として、各従業員に一意のアカウントを付与し、個人アカウントによるアクセス制御を実施している。共有アカウントについては、業務上の必要性がある場合に限り承認制で利用しており、適宜見直しおよびパスワード変更を行っている。

関連文書

- 4. アクセス制御及び認証

A.5.19 供給者関係における情報セキュリティ

作成者: 情報セキュリティ委員会

方針

当社は、供給者との関係において、 当社の情報資産に影響を与える情報セキュリティ上のリスクを考慮し、 適切な管理を行う。

供給者の取扱い

供給者は、業務内容および当社の情報資産の取扱有無に応じて管理する。 当社の情報資産を直接取り扱わない供給者については、 一般的なサービス提供者として取り扱う。

業務委託先に対する管理

業務委託等により、当社の情報資産を直接取り扱う供給者については、 契約または合意文書において、 情報セキュリティに関する事項を定める。

一般的なサービス提供者に対する管理

クラウドサービス、通信事業者、配送業者等、 一般的なサービス提供を行う供給者については、 利用規約、公開されているセキュリティ情報、 第三者認証等の確認により、 情報セキュリティ上の管理を行う。

供給者関係の見直し

供給者との関係については、 業務内容や利用状況の変化に応じて、 必要に応じた見直しを行う。

当社における実施状況

当社では、情報資産を直接取り扱う委託先については、契約または合意文書により守秘義務および情報セキュリティ上の要件を定めている。一般的なSaaS等のサービス提供者については、利用規約、公開されているセキュリティ情報および第三者認証の確認により管理している。

個別のセキュリティ対策確認チェックリストは作成していないが、公開情報（ISO/SOC2認証、プライバシーポリシー、DPA等）および契約条項により、情報セキュリティ上の管理を行っている。

A.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

作成者: 情報セキュリティ委員会

方針

当社は、供給者との合意内容において、 当社の情報資産の取扱いに関する情報セキュリティ上の要件が、 業務内容および情報の重要性に応じて適切に定められるよう管理を行う。

合意内容の取扱い

供給者との合意は、契約書、利用規約その他の合意文書に基づき管理する。 当社の情報資産を取り扱う場合は、 合意内容に応じて、 機密情報の取扱いに関する事項を定める。

業務委託先との合意

業務委託等により、当社の情報資産を直接取り扱う供給者との合意においては、 契約内容に応じて、 情報の取扱い、利用範囲、契約終了時の対応等について定める。

一般的なサービス提供者との合意

SaaS 等の一般的なサービス提供者については、 利用規約や公開されている条件を合意内容として取り扱い、 当該内容を確認したうえで利用する。

合意内容の見直し

供給者との合意内容については、 業務内容や利用状況の変更があった場合に、 必要に応じて見直しを行う。

当社における実施状況

当社では、情報資産を直接取り扱う委託先については、契約または合意文書により守秘義務および情報セキュリティ上の要件を定めている。一般的なSaaS等のサービス提供者については、利用規約、公開されているセキュリティ情報および第三者認証の確認により管理している。

契約管理はクラウド契約管理サービス（Money Forward クラウド契約）を用いて一元管理しており、契約終了時の対応も追跡可能な状態としている。

A.5.21 ICTサプライチェーンにおける情報セキュリティの管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.21
分類	組織的管理策

管理策

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義し、実施しなければならない。

目的

ICTサプライチェーン全体を通じて、合意されたレベルの情報セキュリティを維持するため。

実施の手引き

ICTサプライチェーンのセキュリティ管理には、以下を含める必要がある。

- ICT製品及びサービスに適用するセキュリティ要件の定義
- 供給者がセキュリティ要件を下流の供給者に伝達することの要求
- ICT製品及びサービスの完全性の検証
- 供給者のセキュリティ慣行の監視

サプライチェーンリスク

リスク	対策
悪意のあるコードの混入	コードレビュー、完全性検証
偽造部品	信頼できる供給者からの調達
脆弱性の伝播	脆弱性管理、パッチ適用
情報漏洩	機密保持契約、アクセス制御

管理策の実施

- 供給者のセキュリティ評価基準の策定
- 契約におけるセキュリティ要件の明記
- 定期的なセキュリティ監査の実施
- インシデント報告体制の確立

当社における実施状況

ICTサプライチェーンに関するリスクについては、委託先およびクラウドサービス選定時に、公開されているセキュリティ情報および実績を確認することで評価している。下流供給者に対する個別の監査は実施していないが、利用する範囲を限定することでリスク低減を図っている。

当社では、主要なクラウドサービス（AWS、GCP、Google Workspace等）を利用しており、これらのサービス提供者が公開しているセキュリティ認証（ISO 27001、SOC 2等）および責任共有モデルに基づいて管理を行っている。

関連文書

- 9. 委託管理

A.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

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.22
分類	組織的管理策

管理策

組織は、供給者の情報セキュリティの実践及びサービス提供を定常的に監視し、レビューし、監査し、変更を管理しなければならない。

目的

供給者との合意に従って、情報セキュリティ及びサービス提供の合意されたレベルを維持するため。

実施の手引き

供給者のサービス提供の監視には、以下を含める必要がある。

- サービスレベルのパフォーマンス監視
- 供給者が作成したサービスレポートのレビュー
- 情報セキュリティインシデントの管理
- 監査証跡及び情報セキュリティイベントの記録のレビュー

変更管理

供給者サービスの変更には、以下を考慮する必要がある。

- 現在の情報セキュリティ方針への影響
- ビジネスプロセスへの影響
- リスクの再評価の必要性
- 変更の承認プロセス

当社における実施状況

供給者のサービス提供および情報セキュリティ状況については、利用継続の可否、重大な仕様変更、インシデント発生の有無等を通じて継続的に把握している。形式的な定期レビューは実施していないが、必要に応じて見直しを行う運用としている。

当社では、クラウドサービス（AWS、GCP、Google Workspace等）の利用状況を監視し、サービス提供者からの重要な通知やセキュリティアップデートを確認している。問題がなければ利用を継続し、重大な変更やインシデントがあった場合に再評価を行う。

関連文書

- 7. IT基盤運用管理
- 9. 委託管理

A.5.23 クラウドサービス利用における情報セキュリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2025.01.15
適用範囲	全社・全従業員
管理策番号	A.5.23
分類	組織的管理策

管理策

クラウドサービスの取得、利用、管理及び終了のプロセスは、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。

目的

クラウド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。

実施の手引き

クラウドサービスの利用に際しては、以下を考慮する必要がある。

- クラウドサービスの種類（IaaS、PaaS、SaaS）
- 責任分界点の明確化
- データの所在地と法的管轄
- セキュリティ管理策の実装状況

クラウドサービス選定基準

評価項目	確認内容
セキュリティ認証	ISO 27001、SOC 2等の取得状況
データ保護	暗号化、アクセス制御
可用性	SLA、冗長構成
コンプライアンス	法令遵守、データ所在地
終了時対応	データ返却・削除手順
AIサービスの場合	入力データの学習利用に関する利用規約、オプトアウト方法の有無

責任分界

管理項目	IaaS	PaaS	SaaS
データ	顧客	顧客	顧客
アプリケーション	顧客	顧客	提供者
ミドルウェア	顧客	提供者	提供者
OS	顧客	提供者	提供者
インフラ	提供者	提供者	提供者

当社における実施状況

当社では、承認されたクラウドサービスのみを利用し、新規導入時には情報セキュリティ上の観点から確認を行っている。シャドーITは禁止しており、業務で利用するSaaSは情報セキュリティ責任者の承認を得たうえで導入している。

クラウドサービスの選定にあたっては、公開されているセキュリティ情報、第三者認証（ISO 27001、SOC 2等）、利用規約を確認したうえで採用している。個別のチェックリストは作成していないが、利用範囲を限定し、問題があれば見直す運用としている。

関連文書

- 7. IT基盤運用管理
- 11. テレワークにおける対策
- 13. SaaS導入・シャドーIT管理

A.5.24 情報セキュリティインシデント管理の計画及び準備

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.24
分類	組織的管理策

管理策

組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定義し、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。

目的

情報セキュリティインシデントに対する迅速、効果的、一貫した対応を確実にするため。

実施の手引き

インシデント管理の計画には、以下を含める必要がある。

- インシデント管理の手順
- インシデント対応チームの編成
- 役割と責任の定義
- 連絡体制の確立
- 訓練と演習の計画

インシデント対応体制

役割	責任
インシデント対応責任者	対応の指揮、意思決定
技術担当	技術的な調査、対応
連絡担当	関係者への連絡、報告
記録担当	対応状況の記録（チケット等）

当社における実施状況

当社では、インシデント対応責任者（CTO）がインシデント対応の計画・準備を行っている。インシデントレベル（0〜3）に応じた対応手順を定め、定期的に見直しを行っている。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.25 情報セキュリティ事象の評価及び決定

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.25
分類	組織的管理策

管理策

組織は、情報セキュリティ事象を評価し、それを情報セキュリティインシデントに分類するかどうかを決定しなければならない。

目的

情報セキュリティ事象を適切に分類し、優先順位を付けて対応するため。

実施の手引き

情報セキュリティ事象の評価には、以下を考慮する必要がある。

- 事象の性質と範囲
- 影響を受ける資産
- 潜在的な影響
- 緊急性

事象とインシデントの区別

用語	定義
情報セキュリティ事象	情報セキュリティ方針への違反又はセキュリティ管理策の失敗の可能性を示す、システム、サービス又はネットワークの状態の発生
情報セキュリティインシデント	事業運営を危うくする可能性が高い、又は情報セキュリティを脅かす可能性が高い、望まない又は予期しない情報セキュリティ事象

評価基準

評価項目	確認内容
影響範囲	影響を受けるシステム、データ、ユーザーの範囲
機密性への影響	情報漏洩の有無、範囲
完全性への影響	データ改ざんの有無、範囲
可用性への影響	サービス停止の有無、期間

当社における実施状況

当社では、インシデント発生時の影響評価基準を定めている。レベル3（顧客・社会への影響）、レベル2（事業継続への影響）、レベル1（社内のみの影響）、レベル0（将来的なリスク）の4段階で評価する。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.26 情報セキュリティインシデントへの対応

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.26
分類	組織的管理策

管理策

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。

目的

情報セキュリティインシデントに対する効率的かつ効果的な対応を確実にするため。

実施の手引き

インシデント対応手順には、以下を含める必要がある。

- インシデントの封じ込め
- 証拠の収集と保全
- インシデントの根絶
- 復旧
- 関係者への通知

インシデント対応フロー

フェーズ	活動
検知	インシデントの発見、報告

フェーズ	活動
初動対応	被害拡大防止、証拠保全
分析	原因調査、影響範囲特定
封じ込め	被害の局所化
根絶	原因の除去
復旧	システム・サービスの復旧
事後対応	報告書作成、再発防止策

通知先

状況	通知先
個人情報漏洩	個人情報保護委員会、本人
サイバー犯罪	警察
重大インシデント	経営陣、関係当局

当社における実施状況

当社では、インシデント発見者は速やかにインシデント対応責任者（CTO）に報告することを義務付けている。報告内容には発見日時、状況、影響範囲等を含める。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.27 情報セキュリティインシデントからの学習

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.27
分類	組織的管理策

管理策

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、改善するために利用しなければならない。

目的

将来のインシデントの発生可能性又は影響を低減するため。

実施の手引き

インシデントからの学習には、以下を含める必要がある。

- インシデントの根本原因分析
- 再発防止策の策定
- 管理策の有効性評価
- 手順の改善
- 教育・訓練への反映

学習プロセス

ステップ	活動
分析	インシデントの詳細分析、根本原因の特定
評価	既存管理策の有効性評価
改善	再発防止策の策定、管理策の強化
共有	教訓の組織内共有
反映	方針・手順への反映、教育への組み込み

分析項目

項目	内容
発生原因	技術的原因、人的原因、プロセス上の原因
検知の遅れ	検知までの時間、検知方法の有効性
対応の課題	対応手順の問題点、リソースの不足
影響	実際の被害、潜在的な被害

当社における実施状況

当社では、インシデント対応後に原因分析と再発防止策の検討を行い、得られた教訓を情報セキュリティ対策の改善に活用している。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.28 証拠の収集

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.28
分類	組織的管理策

管理策

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。

目的

懲戒処分及び法的措置のために、証拠として認められる方法で情報セキュリティ事象に関連する証拠を管理するため。

実施の手引き

証拠の収集には、以下を考慮する必要がある。

- 証拠の完全性の維持
- 証拠の連鎖（Chain of Custody）の確立
- 法的要件への適合
- 証拠の安全な保管

証拠の種類

種類	例
デジタル証拠	ログファイル、メモリダンプ、ディスクイメージ
物理的証拠	ハードウェア、記憶媒体、文書
証言	目撃者の証言、インタビュー記録

証拠収集手順

ステップ	活動
特定	関連する証拠の特定
収集	証拠の安全な収集
保全	証拠の完全性維持
記録	収集過程の文書化
保管	安全な保管場所での管理

Chain of Custody

証拠の連鎖を維持するために、以下を記録する。

- 証拠の発見者、発見日時、発見場所
- 証拠の取扱者、取扱日時
- 証拠の保管場所、保管方法
- 証拠へのアクセス記録

当社における実施状況

当社では、インシデント対応時に必要に応じて証拠を収集・保全している。証拠の取扱いは情報セキュリティ部門責任者（CTO）の指示に従う。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.29 事業の中断・阻害時の情報セキュリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.29
分類	組織的管理策

管理策

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。

目的

事業の中断・阻害時においても、情報及びその他の関連資産を保護するため。

実施の手引き

事業の中断・阻害時の情報セキュリティ計画には、以下を含める必要がある。

- 中断・阻害時に維持すべきセキュリティ要件の特定
- 代替手段のセキュリティ確保
- 復旧時のセキュリティ検証
- 緊急時のアクセス制御

考慮すべき事項

項目	内容
アクセス制御	緊急時のアクセス権限、代替認証手段

項目	内容
データ保護	バックアップからの復旧時のセキュリティ
通信セキュリティ	代替通信手段のセキュリティ
物理的セキュリティ	代替施設のセキュリティ

事業継続計画との連携

フェーズ	セキュリティ活動
準備	セキュリティ要件の定義、代替手段の準備
対応	セキュリティ管理策の維持、監視の継続
復旧	セキュリティ設定の検証、アクセス権の確認
回復	通常運用への移行、セキュリティレビュー

当社における実施状況

当社では、クラウドサービスの冗長性を活用し、単一障害点を排除することで事業継続性を確保している。災害時には人命安全を最優先とし、復旧よりも安全を優先する方針としている。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.30 事業継続のためのICTの備え

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.30
分類	組織的管理策

管理策

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

目的

事業の中断・阻害時に、組織の情報及びその他の関連資産の可用性を確保するため。

実施の手引き

ICTの備えには、以下を含める必要がある。

- 事業影響分析に基づくICT要件の特定
- ICT継続戦略の策定
- ICT継続計画の策定と維持
- 定期的な試験と演習

ICT継続計画の要素

要素	内容
目標復旧時間（RTO）	サービス復旧までの目標時間

要素	内容
目標復旧時点（RPO）	許容されるデータ損失の時点
復旧手順	システム復旧の詳細手順
連絡体制	緊急時の連絡先、エスカレーション

備えの種類

種類	説明
バックアップ	データの定期的なバックアップ
冗長構成	システムの冗長化
代替サイト	災害時の代替拠点
クラウド活用	クラウドサービスによる可用性確保

試験と演習

- バックアップ復旧試験（必要に応じて実施）
- フェイルオーバー試験
- 災害復旧演習
- 試験結果に基づく計画の改善

当社における実施状況

当社では、クラウドサービス（AWS RDS、Cloud SQL等）の冗長性と自動バックアップ機能により事業継続性を確保している。データは基本的にMySQLに格納されており、標準的なmysqldump/復元手順で対応可能なため、定期的な復元テストは実施していない。クラウドサービスのマネージド機能により、データの可用性と復旧性を担保している。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.5.31 法令、規制及び契約上の要求事項

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.31
分類	組織的管理策

管理策

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みは、特定し、文書化し、最新に保たなければならない。

目的

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への適合を確実にするため。

実施の手引き

組織は、以下を特定し、文書化する必要がある。

- 適用される法令及び規制
- 契約上の義務
- 要求事項を満たすための取組み

主要な法令・規制

法令・規制	概要
個人情報保護法	個人情報の適正な取扱い
不正アクセス禁止法	不正アクセス行為の禁止

法令・規制	概要
不正競争防止法	営業秘密の保護
電子署名法	電子署名の法的効力
マイナンバー法	特定個人情報の適正な取扱い

契約上の要求事項

種類	内容
顧客との契約	セキュリティ要件、機密保持義務
供給者との契約	セキュリティ要件、監査権
業界基準	PCI DSS、FISC等

遵守状況の確認

- 定期的な法令・規制の変更確認
- コンプライアンス監査の実施
- 是正措置の実施

当社における実施状況

当社では、個人情報保護法、不正競争防止法等の関連法令を遵守している。法令要件は情報セキュリティ方針および各規程に反映している。

関連文書

- 1. 組織的対策

A.5.32 知的財産権

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.32
分類	組織的管理策

管理策

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。

目的

知的財産権に関連する法令、規制及び契約上の要求事項への適合を確実にするため。

実施の手引き

知的財産権の保護には、以下を含める必要がある。

- ソフトウェアライセンスの管理
- 著作権の遵守
- 特許権の尊重
- 商標の適切な使用

知的財産権の種類

種類	説明
著作権	著作物の創作者に与えられる権利
特許権	発明に対する独占的権利

種類	説明
商標権	商品・サービスを識別する標識の権利
営業秘密	秘密として管理される事業上の情報

ソフトウェアライセンス管理

活動	内容
台帳管理	ライセンス情報の記録、更新
使用状況監視	ライセンス数と使用数の照合
定期監査	ライセンス遵守状況の確認
違反対応	違反発見時の是正措置

注意事項

- 不正コピーソフトウェアの使用禁止
- オープンソースライセンスの遵守
- 第三者の知的財産権の尊重

当社における実施状況

当社では、知的財産権（著作権、特許権等）を尊重し、ライセンス条件を遵守したソフトウェアの使用を義務付けている。

関連文書

- 6. IT機器利用

A.5.33 記録の保護

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.33
分類	組織的管理策

管理策

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。

目的

法令、規制、契約及び事業上の要求事項に従って、記録を保護するため。

実施の手引き

記録の保護には、以下を考慮する必要がある。

- 記録の分類と保存期間の決定
- 適切な保管方法の選択
- アクセス制御の実施
- 廃棄手順の確立

記録の種類と保存期間

記録の種類	保存期間	根拠
会計記録	10年	会社法

記録の種類	保存期間	根拠
税務記録	7年	法人税法
雇用記録	退職後3年	労働基準法
契約書	契約終了後10年	民法
セキュリティログ	1年以上	社内規程

保護対策

対策	内容
完全性	改ざん防止、バージョン管理
機密性	アクセス制御、暗号化
可用性	バックアップ、冗長化
真正性	タイムスタンプ、電子署名

廃棄手順

- 保存期間終了の確認
- 廃棄承認の取得
- 安全な廃棄方法の選択
- 必要に応じて廃棄の記録を残す

当社における実施状況

当社では、情報セキュリティに関する記録（アクセスログ、インシデント記録等）を適切に保護・保管している。記録の保存期間は法令要件および業務要件に基づいて定めている。

セキュリティログの長期保存

セキュリティログ（1年以上保存）の要件を満たすため、デフォルトの保持期間が不足するサービスについては、以下の長期保存の仕組みを導入している。

サービス	デフォルト保持期間	長期保存方法
Microsoft Entra ID	7日	nightwatch によるエクスポート

サービス	デフォルト保持期間	長期保存方法
Google Workspace Admin	6ヶ月	nightwatch によるエクスポート
AWS CloudTrail	90日	S3への全ログ保存
GCP Cloud Audit Logs (Admin Activity)	400日	要件充足のため追加対応不要

関連文書

- 1. 組織的対策
- 7. IT基盤運用管理

A.5.34 プライバシー及びPIIの保護

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.34
分類	組織的管理策

管理策

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（個人識別情報）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。

目的

プライバシー及びPIIの保護に関連する法令、規制及び契約上の要求事項への適合を確実にするため。

実施の手引き

PIIの保護には、以下を含める必要がある。

- PIIの特定と分類
- 取扱いルールの策定
- 技術的・組織的対策の実施
- 本人の権利への対応

PIIの取扱い原則

原則	内容
利用目的の特定	利用目的を具体的に特定
利用目的の制限	目的外利用の禁止
適正な取得	適法かつ公正な手段での取得
正確性の確保	正確かつ最新の状態に維持
安全管理措置	漏洩等の防止
第三者提供の制限	本人同意なき提供の禁止

本人の権利

権利	内容
開示請求	保有個人データの開示
訂正請求	内容の訂正、追加、削除
利用停止請求	利用の停止、消去
第三者提供停止請求	第三者への提供の停止

当社における実施状況

当社では、個人情報保護管理者（代表取締役）が個人情報保護法および関連法令の遵守責任を負っている。個人情報の取扱いに関する規程を定め、全従業員に周知している。

関連文書

- 1. 組織的対策
- 3. 情報資産管理

A.5.35 情報セキュリティの独立したレビュー

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.35
分類	組織的管理策

方針

当社は、情報セキュリティに関する管理策が適切に設計され、 有効に運用されていることを確認するため、 独立したレビューを実施する。

独立したレビューの実施

独立したレビューは、 日常のISMS運用から独立した立場により実施する。 レビューにおいては、 情報セキュリティ方針、管理策の有効性、 法令および規制への適合状況等を確認する。

内部監査

内部監査は、年1回以上実施する。 内部監査は、監査対象業務から独立した立場の者が担当し、 ISMSの要求事項および当社が定めた規程への適合状況を確認する。

マネジメントレビュー

マネジメントレビューは、年1回以上実施する。 経営層は、内部監査の結果、 情報セキュリティに関する課題および改善の機会を踏まえ、 ISMSの継続的な改善について判断を行う。

当社における実施状況

当社では、情報セキュリティに関する独立したレビューとして、 内部監査およびマネジメントレビューを実施している。 これらのレビューを通じて、 情報セキュリティ管理策の有効性および改善の機会を確認している。

A.5.36 情報セキュリティのための方針群、規則及び標準の遵守

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.5.36
分類	組織的管理策

管理策

情報セキュリティ方針、トピック固有の方針、規則及び標準の遵守は、定期的にレビューしなければならない。

目的

情報セキュリティが組織の方針、トピック固有の方針、規則及び標準に従って実施され、運用されることを確実にするため。

実施の手引き

遵守状況のレビューには、以下を含める必要がある。

- 方針及び手順の遵守状況の確認
- 技術的管理策の有効性の検証
- 是正措置の実施状況の確認

レビュー方法

方法	内容
自己点検	部門による自己評価
内部監査	独立した内部監査員による監査
ログレビュー	アクセスログ、セキュリティログの分析

遵守状況の確認項目

項目	確認内容
アクセス制御	権限設定の適切性
パスワード管理	パスワードポリシーの遵守
情報分類	保存先・アクセス制御による分類の適切性
インシデント報告	報告手順の遵守
教育・訓練	受講状況

不遵守への対応

- 原因の分析
- 是正措置の実施
- 再発防止策の策定
- 必要に応じた懲戒処分

当社における実施状況

当社では、情報セキュリティ方針および各規程の遵守状況を定期的に確認している。不遵守が発見された場合は、是正措置を講じる。

関連文書

- 1. 組織的対策

A.5.37 操作手順書

作成者: 情報セキュリティ委員会

方針

当社は、情報セキュリティに影響を与える重要な操作について、 適切な運用を確保するため、必要最小限の操作手順を文書化する。

操作手順書の対象

操作手順書は、 情報セキュリティ上重要と判断される操作に限定して作成する。 すべての業務操作について手順書を作成するものではない。

操作手順書の内容

操作手順書には、 操作の目的、担当者、 誤操作時の影響および注意事項等、 運用上必要な事項を記載する。

操作手順書の管理

操作手順書は、 業務内容やシステム構成の変更に応じて、 必要に応じた見直しを行う。

当社における実施状況

当社では、 アカウント管理、アクセス権管理、 インシデント対応等、 情報セキュリティ上重要な操作について、 必要最小限の操作手順書を整備している。

A.6.1 選考

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.1
分類	人的管理策

管理策

すべての採用候補者の経歴確認は、関連する法令、規制及び倫理に従って実施しなければならない。また、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たものでなければならない。

目的

すべての採用候補者が、その役割にふさわしく、信頼でき、採用に適格であることを確実にするため。

実施の手引き

経歴確認には、以下を含めることができる。

- 身元の確認（パスポート、運転免許証等）
- 学歴・資格の確認
- 職歴の確認
- 犯罪歴の確認（法令で許可される場合）
- 信用調査（役割に応じて）

確認項目

確認項目	方法	対象
身元確認	本人確認書類の確認	全員
職歴確認	前職への照会	必要に応じて
資格確認	資格証明書の確認	該当者
犯罪歴確認	法令に基づく確認	特定職種

注意事項

- 個人情報保護法を遵守する
- 本人の同意を得て実施する
- 確認結果は適切に管理する
- 差別につながる確認は行わない

当社における実施状況

当社では、採用時に身元確認を実施し、秘密保持契約を締結している。従業員の適格性を確認した上で雇用を行っている。

関連文書

- 2. 人的対策

A.6.2 雇用条件

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.2
分類	人的管理策

管理策

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

目的

従業員が情報セキュリティに関する責任を理解し、受け入れることを確実にするため。

実施の手引き

雇用契約には、以下の情報セキュリティに関する事項を含める必要がある。

- 機密保持義務
- 情報セキュリティ方針の遵守義務
- 資産の適切な使用
- 違反時の措置
- 雇用終了後の義務

契約に含める事項

項目	内容
機密保持	業務上知り得た情報の秘密保持義務
方針遵守	情報セキュリティ方針・規程の遵守
資産利用	組織の資産の適切な利用
報告義務	セキュリティインシデントの報告義務
違反時措置	違反時の懲戒処分
終了後義務	退職後の機密保持義務

契約書類

書類	内容
雇用契約書	雇用条件、責任の明記
秘密保持契約書	機密保持義務の詳細
誓約書	方針遵守の誓約

当社における実施状況

当社では、雇用契約において情報セキュリティに関する責任と義務を明確に定めている。秘密保持契約を締結し、営業秘密の保護義務を課している。

関連文書

- 2. 人的対策

A.6.3 情報セキュリティの意識向上、教育及び訓練

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.3
分類	人的管理策

管理策

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、適切な、情報セキュリティに関する意識向上、教育及び訓練を受け、定期的にその更新を受けなければならない。

目的

要員及び関連する利害関係者が、情報セキュリティの責任を認識し、果たすことを確実にするため。

実施の手引き

情報セキュリティの意識向上、教育及び訓練プログラムには、以下を含める必要がある。

- 情報セキュリティ方針及び手順
- 情報セキュリティの役割と責任
- 脅威と脆弱性
- インシデント報告手順
- 法令・規制の要求事項

教育プログラム

種類	対象	頻度
入社時教育	新入社員	入社時
定期教育	全従業員	年1回以上
専門教育	IT担当者等	随時
臨時教育	全従業員	必要時

教育内容

内容	説明
方針・規程	情報セキュリティ方針、関連規程
脅威・リスク	最新の脅威動向、リスク
対策	具体的なセキュリティ対策
インシデント対応	報告手順、初動対応
法令遵守	関連法令、コンプライアンス

教育効果の測定

- 受講率の管理
- インシデント発生状況の分析
- フィードバックの収集

当社における実施状況

当社では、教育責任者（管理部責任者）が年1回以上の情報セキュリティ教育を実施している。教育内容には情報セキュリティ方針、個人情報の取扱い、脅威への対応等を含めている。

関連文書

- 2. 人的対策

A.6.4 懲戒手続

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.4
分類	人的管理策

管理策

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係者に対して措置をとるための懲戒手続を正式に定め、伝達しなければならない。

目的

要員及びその他の関係者が情報セキュリティ方針違反の結果を理解することを確実にするため。

実施の手引き

懲戒手続には、以下を含める必要がある。

- 違反の種類と重大度の定義
- 調査手順
- 懲戒処分の種類
- 不服申立て手順
- 記録の保管

違反の分類

分類	例	処分例
軽微	パスワードの不適切な管理	注意、指導
中程度	情報の不適切な取扱い	戒告、減給
重大	意図的な情報漏洩	出勤停止、解雇

懲戒手続のプロセス

ステップ	内容
報告	違反の報告、受付
調査	事実関係の調査
評価	違反の重大度評価
決定	懲戒処分の決定
通知	本人への通知
実施	処分の実施
記録	記録の保管

注意事項

- 公平かつ一貫した適用
- 適正手続の保障
- 労働法令の遵守
- プライバシーへの配慮

当社における実施状況

当社では、情報セキュリティ方針違反に対する懲戒手続きを就業規則に定めている。違反の程度に応じた措置を講じる。

関連文書

- 2. 人的対策

A.6.5 雇用の終了又は変更後の責任

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.5
分類	人的管理策

管理策

雇用の終了又は変更後も有効な情報セキュリティの責任及び義務を定め、要員に伝達し、遵守させなければならない。

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。

実施の手引き

雇用の終了又は変更後の責任には、以下を含める必要がある。

- 機密保持義務の継続
- 競業避止義務（該当する場合）
- 知的財産権の帰属
- 資産の返却

終了後の義務

義務	期間	内容
機密保持	無期限	業務上知り得た機密情報の秘密保持

義務	期間	内容
競業避止	契約による	競合他社への就職制限（合理的範囲）
知的財産	無期限	在職中に創作した知的財産の帰属

終了時の手続

手続	内容
資産返却	貸与機器、文書、データの返却
アクセス権削除	システムアクセス権の即時削除
引継ぎ	業務の適切な引継ぎ
退職面談	義務の確認、誓約書の取得

変更時の対応

- 新しい役割に応じたアクセス権の見直し
- 不要となったアクセス権の削除
- 新しい責任の伝達

当社における実施状況

当社では、退職時に貸与機器の返却、アクセス権限の削除、機密情報の返却を義務付けている。退職後も秘密保持義務が継続することを確認している。

関連文書

- 2. 人的対策

A.6.6 機密保持契約又は守秘義務契約

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.6
分類	人的管理策

管理策

情報保護に対する組織のニーズを反映した機密保持契約又は守秘義務契約は、特定し、文書化し、定期的にレビューし、要員及びその他の関係する利害関係者によって署名されなければならない。

目的

情報へのアクセスを持つ要員及び外部関係者による情報の機密性の維持を確実にするため。

実施の手引き

機密保持契約には、以下を含める必要がある。

- 保護すべき情報の定義
- 情報の使用目的
- 情報の取扱い方法
- 契約期間と終了後の義務
- 違反時の措置

契約に含める事項

項目	内容
機密情報の定義	保護対象となる情報の範囲
使用目的	情報の使用が許可される目的
開示制限	第三者への開示の制限
保護措置	情報を保護するための措置
返却・廃棄	契約終了時の情報の取扱い
有効期間	契約の有効期間、終了後の義務
違反時措置	違反時の損害賠償、法的措置

契約の種類

種類	対象
従業員向けNDA	従業員
取引先向けNDA	供給者、パートナー
相互NDA	双方が情報を開示する場合

レビュー

- 定期的な契約内容の見直し
- 法令変更への対応
- 事業環境の変化への対応

当社における実施状況

当社では、秘密保持契約において退職後も秘密保持義務が継続することを定めている。競業避止義務についても必要に応じて契約に含めている。

関連文書

- 2. 人的対策

A.6.7 リモートワーク

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.7
分類	人的管理策

管理策

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

目的

リモートワーク時に情報のセキュリティを確保するため。

実施の手引き

リモートワークのセキュリティ対策には、以下を含める必要がある。

- 物理的セキュリティ
- 通信セキュリティ
- アクセス制御
- 機器のセキュリティ
- 情報の取扱い

セキュリティ対策

分野	対策
物理的セキュリティ	作業場所の選定、のぞき見防止
通信セキュリティ	VPN使用、暗号化通信
アクセス制御	多要素認証、セッション管理
機器セキュリティ	画面ロック、暗号化、ウイルス対策
情報取扱い	クラウドサービス利用、ローカル保存禁止

リモートワーク規則

項目	内容
作業場所	自宅、承認された場所のみ
使用機器	会社貸与機器、承認されたBYOD
ネットワーク	VPN必須、公衆Wi-Fi禁止
情報保存	クラウドサービスのみ、ローカル保存禁止
印刷	原則禁止、必要時は適切に廃棄

従業員の責任

- セキュリティ規則の遵守
- 機器の適切な管理
- インシデントの報告
- 作業環境の確保

当社における実施状況

当社では、テレワーク時のセキュリティ対策を定めている。承認されたクラウドサービスのみを使用し、データはクラウド上に保存する。自宅ネットワークのセキュリティ確保、公衆WiFi利用時の注意等を義務付けている。

関連文書

- 11. テレワークにおける対策

A.6.8 情報セキュリティ事象の報告

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.6.8
分類	人的管理策

管理策

組織は、要員が認識した情報セキュリティ事象を、適切な連絡経路を通じて、時機を失せずに報告するための仕組みを提供しなければならない。

目的

情報セキュリティ事象の適時の報告を支援するため。

実施の手引き

情報セキュリティ事象の報告の仕組みには、以下を含める必要がある。

- 報告すべき事象の定義
- 報告経路の明確化
- 報告手順の周知
- 報告者の保護

報告すべき事象

事象	例
セキュリティ侵害	不正アクセス、マルウェア感染

事象	例
情報漏洩	データの紛失、誤送信
物理的セキュリティ	機器の紛失、盗難
方針違反	規程違反の発見
脆弱性	セキュリティ上の弱点の発見

報告プロセス

ステップ	内容
発見	事象の発見、認識
報告	指定された連絡先への報告
受付	報告の受付、記録
初動対応	必要な初動対応の実施
エスカレーション	必要に応じた上位への報告

報告先

状況	報告先
通常	上長、システム管理者
緊急	インシデント対応責任者
匿名	内部通報窓口

報告者の保護

- 善意の報告者への不利益取扱いの禁止
- 匿名報告の受付
- 報告者情報の保護

当社における実施状況

当社では、情報セキュリティインシデントや脆弱性を発見した場合、速やかにインシデント対応責任者（CTO）に報告することを義務付けている。報告者が不利益を受けないよう配慮して

いる。

関連文書

- 10. 情報セキュリティインシデント対応及び事業継続管理

A.7.1 物理的セキュリティ境界

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.1
分類	物理的管理策

管理策

セキュリティ境界は、機密情報又は重要な情報を含む領域及び情報処理施設を保護するために定義し、使用しなければならない。

目的

組織の情報及びその他の関連資産への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。

実施の手引き

物理的セキュリティ境界には、以下を考慮する必要がある。

- 境界の明確な定義
- 壁、ドア、窓の物理的強度
- 侵入検知システム
- 受付又は入退室管理

セキュリティ境界の種類

境界	説明	対策例
建物境界	建物の外周	施錠、監視カメラ、警備員
フロア境界	フロアの入口	入退室管理、受付
セキュリティエリア	重要な情報処理施設	生体認証、二重ドア
サーバールーム	IT機器設置場所	厳格なアクセス制御

境界の保護対策

対策	内容
物理的障壁	壁、フェンス、施錠ドア
監視	監視カメラ、警備員
検知	侵入検知センサー、アラーム
照明	十分な照明の確保

当社における実施状況

当社では、セキュリティ領域をレベル1領域（来客対応エリア）とレベル2領域（執務エリア）に区分している。クラウドのみの運用のため、レベル3領域（サーバールーム）は設置していない。

関連文書

- 5. 物理的対策

A.7.2 物理的入退

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.2
分類	物理的管理策

管理策

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ポイントによって保護しなければならない。

目的

認可された者だけが組織の情報及びその他の関連資産への物理的アクセスを許可されることを確実にするため。

実施の手引き

物理的入退管理には、以下を含める必要がある。

- 入退の記録
- 認証手段の使用
- 訪問者の管理
- アクセス権の定期的なレビュー

入退管理方法

方法	説明	適用場所
ICカード	非接触カードによる認証	一般エリア
暗証番号	PIN入力による認証	制限エリア
生体認証	指紋、顔認証等	高セキュリティエリア
二要素認証	カード＋暗証番号等	サーバールーム

入退記録

- 入退日時
- 入退者の識別情報
- 入退場所
- 記録の保存期間

当社における実施状況

当社では、レベル2領域（執務エリア）への入退室を管理している。来訪者はレベル1領域（来客対応エリア）で対応し、レベル2領域への入室時は従業員が同行する。

関連文書

- 5. 物理的対策

A.7.3 オフィス、部屋及び施設のセキュリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.3
分類	物理的管理策

管理策

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、実施しなければならない。

目的

オフィス、部屋及び施設内の情報及びその他の関連資産への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。

実施の手引き

オフィス、部屋及び施設のセキュリティには、以下を考慮する必要がある。

- 重要な施設の所在地の非公開
- 建物の外観からの業務内容の非表示
- 適切な施錠と警報システム
- 機密情報を扱う場所の分離

セキュリティ設計

要素 考慮事項

配置 重要施設は建物の奥に配置

要素 考慮事項

表示 機密エリアの表示を最小限に

分離 一般エリアと機密エリアの分離

監視 監視カメラの設置

エリア別セキュリティ

エリア	セキュリティレベル	対策
受付・ロビー	低	受付対応、訪問者管理
一般オフィス	中	入退管理、施錠
会議室	中	予約管理、使用後の確認

当社における実施状況

当社では、オフィスの施錠管理を実施している。最終退出者は施錠を確認し、不審者の侵入を防止している。

関連文書

- 5. 物理的対策

A.7.4 物理的セキュリティの監視

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.4
分類	物理的管理策

管理策

施設は、認可され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。

目的

認可されていない物理的アクセスを検知し、抑止するため。

実施の手引き

物理的セキュリティの監視には、以下を含める必要がある。

- 監視カメラシステム
- 侵入検知システム
- 警備員による巡回
- 監視記録の保管

監視システム

システム	機能	設置場所
監視カメラ	映像記録、リアルタイム監視	入口、通路、重要エリア
侵入検知センサー	不正侵入の検知	窓、ドア、壁

システム	機能	設置場所
動体検知	動きの検知	夜間の無人エリア
アラーム	異常時の警報	全エリア

監視記録の管理

- 記録へのアクセス制限
- 記録の改ざん防止
- 法令に基づく保存期間の遵守
- プライバシーへの配慮

当社における実施状況

当社では、クラウドサービス（AWS、GCP等）を利用しており、物理的なセキュリティはサービス提供者が管理している。オフィスについては、ビル管理会社と連携してセキュリティを確保している。

関連文書

- 5. 物理的対策
- 7. IT基盤運用管理

A.7.5 物理的及び環境的脅威からの保護

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.5
分類	物理的管理策

管理策

自然災害及びその他の意図的又は意図的でない物理的脅威からの保護を設計し、実施しなければならない。

目的

自然災害及びその他の物理的脅威による情報及びその他の関連資産への損害を防止又は軽減するため。

実施の手引き

物理的及び環境的脅威からの保護には、以下を考慮する必要がある。

- 自然災害（地震、洪水、台風等）
- 火災
- 爆発
- 近隣の騒乱
- その他の人為的災害

脅威と対策

脅威	対策
火災	消火設備、防火壁、火災報知器
水害	排水設備、防水対策、高所設置
地震	耐震構造、固定、免震装置
落雷	避雷針、サージ保護
停電	UPS、非常用発電機

環境管理

項目	管理内容
温度	サーバールーム：18-27℃
湿度	40-60%
空調	冗長構成、監視
清掃	定期的な清掃、埃の除去

緊急時対応

- 避難経路の確保
- 緊急連絡先の掲示
- 定期的な避難訓練
- 事業継続計画との連携

当社における実施状況

当社では、クラウドサービスを利用しており、自然災害等の物理的脅威に対する保護はサービス提供者が実施している。オフィスについては、ビルの防災設備を活用している。

関連文書

- 5. 物理的対策
- 10. 情報セキュリティインシデント対応及び事業継続管理

A.7.6 セキュリティを保つべき領域での作業

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.6
分類	物理的管理策

管理策

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。

目的

セキュリティを保つべき領域での作業中に、情報及びその他の関連資産を保護するため。

実施の手引き

セキュリティを保つべき領域での作業には、以下の規則を適用する必要がある。

- 認可された者のみのアクセス
- 作業の監督
- 施錠と監視
- 記録機器の制限

作業規則

規則	内容
アクセス制限	業務上必要な者のみ入室可

規則	内容
同行	外部者は従業員が同行
記録禁止	写真撮影、録音の禁止
持込制限	私物の持込制限
退室確認	退室時の確認

セキュリティエリアの種類別規則

エリア	規則
開発エリア	情報持出し禁止、クリーンデスク
会議室（機密）	使用後の確認、資料の回収

外部作業者への対応

- 事前の身元確認
- 作業内容の確認
- 常時監督
- 作業完了後の確認

当社における実施状況

当社では、レベル1領域（来客対応エリア）での作業時は、機密情報を含む書類を放置しない、ホワイトボードの内容を消去する、無断での撮影・録音を禁止する等のルールを定めている。

関連文書

- 5. 物理的対策

A.7.7 クリアデスク・クリアスクリーン

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.7
分類	物理的管理策

管理策

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、並びに情報処理施設に対するクリアスクリーンの規則を定め、適切に実施しなければならない。

目的

認可されていないアクセス、情報の消失及び損傷のリスクを低減するため。

実施の手引き

クリアデスク・クリアスクリーン方針には、以下を含める必要がある。

- 離席時の対応
- 終業時の対応
- 機密情報の保管
- 画面ロックの設定

クリアデスク規則

状況	対応
離席時	機密書類を裏返す又は片付ける

状況	対応
終業時	書類を施錠保管、机上を整理
会議後	資料の回収、ホワイトボードの消去
外出時	機密情報を持ち出さない

クリアスクリーン規則

状況	対応
離席時	画面ロック（Windows: Win+L）
自動ロック	5分以内に自動ロック設定
終業時	ログオフ又はシャットダウン
機密作業	のぞき見防止フィルターの使用

実施のポイント

- 定期的な啓発活動
- 違反時の指導
- 施錠可能な収納の提供

当社における実施状況

当社では、クリアデスクポリシーを実施している。離席時や退社時には、機密情報を含む書類を施錠可能な場所に保管し、デスク上に放置しない。

関連文書

- 5. 物理的対策
- 6. IT機器利用

A.7.8 装置の設置及び保護

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.8
分類	物理的管理策

管理策

装置は、環境上の脅威及び災害による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。

目的

装置の消失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。

実施の手引き

装置の設置及び保護には、以下を考慮する必要がある。

- 環境条件（温度、湿度、埃等）
- 自然災害からの保護
- 認可されていないアクセスからの保護
- 飲食物からの保護

設置場所の選定

考慮事項	対策
環境条件	空調設備、除湿機

考慮事項	対策
自然災害	耐震固定、高所設置
アクセス	施錠エリア、監視
電源	安定した電源供給

装置別の保護対策

装置	保護対策
サーバー	ラック収納、施錠、空調管理
ネットワーク機器	施錠キャビネット、ケーブル保護
PC	盗難防止ワイヤー、施錠保管
可搬媒体	施錠保管、暗号化

環境管理

項目	基準
温度	18-27℃
湿度	40-60%
埃	定期清掃
振動	防振対策

当社における実施状況

当社では、IT機器は業務目的でのみ使用し、適切に保管・管理している。機器の持ち出し・持ち込みは必要に応じて管理している。

関連文書

- 5. 物理的対策
- 6. IT機器利用

A.7.9 構外にある資産のセキュリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.9
分類	物理的管理策

管理策

構外にある資産は、構外での作業に伴う様々なリスクを考慮して保護しなければならない。

目的

構外にある資産の消失、損傷、盗難又は侵害を防止するため。

実施の手引き

構外にある資産の保護には、以下を考慮する必要がある。

- 持出しの承認
- 物理的保護
- 暗号化
- 監視と追跡

保護対策

対策	内容
物理的保護	施錠ケース、目を離さない
暗号化	ディスク暗号化、ファイル暗号化

対策	内容
認証	強力なパスワード、生体認証
追跡	紛失時の追跡機能

利用者の責任

- 常に目の届く場所で管理
- 公共の場での使用に注意
- 車内への放置禁止
- 紛失・盗難時の即時報告

紛失・盗難時の対応

- 直ちに上長・管理部に報告
- リモートワイプの実行
- 必要に応じて警察に届出
- インシデント報告書の作成

当社における実施状況

当社では、BYODを許可しており、個人所有機器の使用条件を定めている。画面ロックの設定、クラウドのみでのデータ保存、脱獄・root化の禁止等を義務付けている。

関連文書

- 2. 人的対策
- 6. IT機器利用

A.7.10 記憶媒体

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.10
分類	物理的管理策

管理策

記憶媒体は、組織の分類体系及び取扱い要求事項に従って、その取得、使用、輸送及び廃棄を通じて管理しなければならない。

目的

記憶媒体上の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。

実施の手引き

記憶媒体の管理には、以下を含める必要がある。

- 媒体の登録と追跡
- 適切な保管
- 安全な輸送
- 安全な廃棄

記憶媒体の種類

種類	例
可搬媒体	USBメモリ、外付けHDD、SDカード

種類	例
光学媒体	CD、DVD、Blu-ray
磁気媒体	磁気テープ
内蔵媒体	HDD、SSD

廃棄方法

方法	説明
上書き消去	データを複数回上書き
消磁	磁気的にデータを消去
物理的破壊	シュレッダー、破砕

当社における実施状況

当社では、データはクラウドサービス上に保存することを原則とし、ローカルへの恒久的な保存は行わない。業務上やむを得ず一時的にローカルストレージに保存する場合は、「3. 情報資産管理」に定める条件（作業完了後の速やかな削除、ディスク暗号化の有効化等）に従う。USBメモリ等の外部記憶媒体の使用は原則禁止している。

関連文書

- 3. 情報資産管理
- 6. IT機器利用

A.7.11 サポートユーティリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.11
分類	物理的管理策

管理策

情報処理施設は、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。

目的

サポートユーティリティの不具合による情報処理施設の中断を防止するため。

実施の手引き

サポートユーティリティには、以下が含まれる。

- 電力供給
- 空調設備
- 給水設備
- 通信設備

電力供給の保護

対策	内容
UPS	無停電電源装置による瞬断対策

対策	内容
非常用発電機	長時間停電への対応
冗長化	電源系統の二重化
サージ保護	雷サージからの保護

空調設備の保護

対策	内容
冗長化	空調機の二重化
監視	温度・湿度の常時監視
アラート	異常時の自動通知
定期点検	予防保全の実施

監視と保守

項目	内容
監視	24時間監視、異常検知
点検	定期的な点検、テスト
保守	予防保全、部品交換
記録	点検・保守記録の保管

当社における実施状況

当社では、クラウドサービス（AWS、GCP等）を利用しており、電源やネットワーク等のユーティリティはサービス提供者が管理している。オフィスについては、ビルの設備を利用している。

関連文書

- 7. IT基盤運用管理

A.7.12 ケーブル配線のセキュリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.12
分類	物理的管理策

管理策

電力及び通信のためのケーブル配線は、傍受、妨害又は損傷から保護しなければならない。

目的

ケーブル配線を通じた情報の傍受、妨害又は損傷を防止するため。

実施の手引き

ケーブル配線のセキュリティには、以下を考慮する必要がある。

- 物理的保護
- 電力線と通信線の分離
- ケーブルの識別
- アクセス制限

保護対策

対策	内容
配管・ダクト	ケーブルを配管内に収容
床下配線	二重床による保護

対策	内容
施錠	配線盤の施錠
分離	電力線と通信線の分離

ケーブルの種類別対策

ケーブル種類	対策
電力ケーブル	過負荷保護、接地
ネットワークケーブル	シールド、暗号化
光ファイバー	物理的保護
外部接続	地下埋設、保護管

管理項目

項目	内容
文書化	配線図の作成、更新
ラベリング	ケーブルの識別表示
点検	定期的な点検
変更管理	配線変更の記録

当社における実施状況

当社では、クラウドサービスを利用しており、ケーブル配線のセキュリティはサービス提供者が管理している。オフィス内のネットワーク配線は適切に管理している。

関連文書

- 7. IT基盤運用管理

A.7.13 装置の保守

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.13
分類	物理的管理策

管理策

装置は、情報の可用性及び完全性を継続的に確保するために、正しく保守しなければならない。

目的

装置の不具合による情報の消失又は損傷を防止するため。

実施の手引き

装置の保守には、以下を含める必要がある。

- 製造者の推奨に従った保守
- 認可された保守要員のみによる実施
- 保守記録の保管
- 保守前後のセキュリティ確認

保守の種類

種類	内容	頻度
予防保守	定期点検、部品交換	計画的

種類	内容	頻度
是正保守	故障修理	随時
適応保守	環境変化への対応	必要時

保守プロセス

ステップ	内容
計画	保守計画の策定
準備	データバックアップ、機密情報の保護
実施	認可された要員による保守
確認	動作確認、セキュリティ確認
記録	必要に応じて保守の記録を残す

外部保守要員への対応

項目	内容
身元確認	保守要員の身元確認
監督	作業中の監督
アクセス制限	必要最小限のアクセス
機密保護	機密情報へのアクセス防止

当社における実施状況

当社では、IT機器の保守はシステム管理者（CTO）が管理している。クラウドサービスの保守はサービス提供者が実施している。

関連文書

- 7. IT基盤運用管理

A.7.14 装置のセキュリティを保った処分又は再利用

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.7.14
分類	物理的管理策

管理策

記憶媒体を内蔵した装置は、処分又は再利用する前に、機密データ及びライセンス供与されたソフトウェアが削除されている又はセキュリティを保って上書きされ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。

目的

装置の処分又は再利用による情報の漏洩を防止するため。

実施の手引き

装置の処分又は再利用には、以下を含める必要がある。

- データの完全消去
- ライセンスソフトウェアの削除
- 消去の検証
- 処分記録の保管

データ消去方法

方法	説明	適用
上書き消去	データを複数回上書き	再利用時
消磁	磁気的にデータを消去	HDD
物理的破壊	シュレッダー、破砕	処分時
暗号化消去	暗号鍵の破棄	SSD

処分プロセス

ステップ	内容
申請	処分申請書の提出
承認	資産管理者による承認
データ消去	適切な方法でのデータ消去
検証	消去の確認
処分	適切な方法での処分
記録	必要に応じて処分の記録を残す

再利用時の注意

- データの完全消去の確認
- OSの再インストール
- ライセンスの確認
- 資産台帳の更新

当社における実施状況

当社では、機器の廃棄時にデータの完全消去または物理破壊を実施している。紙媒体は細断または溶解処理により廃棄している。

関連文書

- 3. 情報資産管理

A.8.1 利用者エンドポイント機器

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.1
分類	技術的管理策

管理策

エンドポイント機器に保存されている情報、エンドポイント機器で処理される情報又はエンドポイント機器を介してアクセス可能な情報は、保護しなければならない。

目的

エンドポイント機器を介した情報への認可されていないアクセス、情報の消失又は盗難を防止するため。

実施の手引き

エンドポイント機器のセキュリティには、以下を含める必要がある。

- 機器の登録と管理
- セキュリティ設定の適用
- マルウェア対策
- 暗号化
- リモート管理

セキュリティ対策

対策	内容
認証	強力なパスワード、生体認証
暗号化	ディスク暗号化
マルウェア対策	ウイルス対策ソフトの導入
パッチ管理	OS・アプリケーションの更新
ファイアウォール	パーソナルファイアウォールの有効化

機器の種類別対策

機器	追加対策
ノートPC	盗難防止、リモートワイプ
スマートフォン	MDM、アプリ制限
タブレット	MDM、画面ロック
デスクトップPC	物理的セキュリティ

利用者の責任

- セキュリティ設定の維持
- 不審な動作の報告
- 紛失・盗難時の即時報告
- 私的利用の制限

当社における実施状況

当社では、BYODを含むエンドポイントデバイスのセキュリティ対策を定めている。画面ロックの設定、OSおよびソフトウェアの最新化、不審なソフトウェアのインストール禁止等を義務付けている。

関連文書

- 6. IT機器利用
- 11. テレワークにおける対策

A.8.2 特権的アクセス権

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.2
分類	技術的管理策

管理策

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。

目的

特権的アクセス権の認可されていない使用による損害を防止するため。

実施の手引き

特権的アクセス権の管理には、以下を含める必要がある。

- 特権アカウントの特定
- 最小権限の原則の適用
- 使用の監視と記録
- 定期的なレビュー

特権アカウントの種類

種類	例
システム管理者	root、Administrator
データベース管理者	DBA、sa

種類	例
ネットワーク管理者	ネットワーク機器の管理者
アプリケーション管理者	アプリの管理者権限

管理策

対策	内容
最小権限	必要最小限の権限のみ付与
分離	通常業務と特権業務の分離
認証強化	多要素認証の適用
監視	特権操作のログ記録
レビュー	定期的な権限レビュー

特権アクセスの利用規則

- 特権アカウントは必要な場合のみ使用
- 通常業務には一般アカウントを使用
- 特権操作は記録・監視される
- 特権アカウントの共有禁止

当社における実施状況

当社では、システムへのアクセスには情報セキュリティ責任者の承認を得た上で、最小権限の原則に基づいてアクセス権限を付与している。特権アクセスは必要最小限に制限している。

関連文書

- 4. アクセス制御及び認証

A.8.3 情報へのアクセス制限

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.3
分類	技術的管理策

管理策

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

目的

認可されたアクセスのみを確保し、情報及びその他の関連資産への認可されていないアクセスを防止するため。

実施の手引き

情報へのアクセス制限には、以下を含める必要がある。

- アクセス制御方針に基づく制限
- 役割に基づくアクセス制御
- 機密性レベルに基づく制限
- アクセスログの記録

アクセス制御モデル

モデル	説明
RBAC	役割に基づくアクセス制御
MAC	強制アクセス制御
DAC	任意アクセス制御
ABAC	属性に基づくアクセス制御

制限の実装

レベル	制限方法
ネットワーク	ファイアウォール、セグメンテーション
システム	OSのアクセス制御
アプリケーション	アプリ内の権限管理
データ	暗号化、アクセス制御リスト

アクセス制御の原則

- Need-to-know：知る必要がある者のみ
- 最小権限：必要最小限の権限
- 職務分離：相反する権限の分離
- デフォルト拒否：明示的に許可されない限り拒否

当社における実施状況

当社では、「12. 情報資産の定義と管理ルール」に基づき、情報へのアクセスを制限している。機密性に応じたアクセス制御を実施し、不正アクセスを防止している。

関連文書

- 4. アクセス制御及び認証
- 3. 情報資産管理

A.8.4 ソースコードへのアクセス

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.4
分類	技術的管理策

管理策

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は、適切に管理しなければならない。

目的

ソースコードへの認可されていない機能の導入及び意図しない変更を防止するため。

実施の手引き

ソースコードへのアクセス管理には、以下を含める必要がある。

- アクセス権の制限
- バージョン管理システムの使用
- 変更の追跡
- コードレビュー

アクセス制御

対象	制御方法
ソースコードリポジトリ	認証、認可、ログ記録

対象	制御方法
開発環境	アクセス制限、分離
ビルドシステム	認可された者のみ
本番環境	開発者のアクセス制限

バージョン管理

項目	内容
リポジトリ	Git等の使用
ブランチ管理	開発、テスト、本番の分離
コミット	変更内容の記録
マージ	レビュー後のマージ

セキュリティ対策

- ソースコードの暗号化保存
- アクセスログの記録
- 定期的なアクセス権レビュー
- 退職者のアクセス権即時削除

当社における実施状況

当社では、ソースコードはGitHubで管理し、アクセス権限を適切に設定している。本番環境へのデプロイ権限は限定された担当者のみに付与している。

関連文書

- 8. システム開発及び保守
- 4. アクセス制御及び認証

A.8.5 セキュリティを保った認証

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.5
分類	技術的管理策

管理策

セキュリティを保った認証技術及び手順は、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実施しなければならない。

目的

利用者、エンティティ又はデバイスが、アクセスを要求しているものであることを確実にするため。

実施の手引き

セキュリティを保った認証には、以下を含める必要がある。

- 適切な認証方式の選択
- 多要素認証の実装
- 認証情報の保護
- 認証失敗への対応

認証要素

要素	説明	例
知識要素	知っているもの	パスワード、PIN
所持要素	持っているもの	スマートカード、トークン
生体要素	本人固有のもの	指紋、顔認証

認証方式

方式	セキュリティレベル	適用場面
パスワード	低〜中	一般システム
多要素認証	高	重要システム
生体認証	高	高セキュリティ
証明書認証	高	システム間認証

認証の強化

対策	内容
パスワードポリシー	複雑性、有効期間
アカウントロック	連続失敗時のロック
セッション管理	タイムアウト、同時ログイン制限
監視	認証ログの監視

当社における実施状況

当社では、各サービスの認証機能を利用し、強固なパスワードの設定を義務付けている。Microsoft Entra IDを中心としたシングルサインオンを活用している。

関連文書

- 4. アクセス制御及び認証

A.8.6 容量・能力の管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.6
分類	技術的管理策

管理策

資源の利用を監視し、調整しなければならない。また、現在及び予想される容量・能力の要求事項に合わせて調整しなければならない。

目的

情報処理施設の必要な容量・能力を確保するため。

実施の手引き

容量・能力の管理には、以下を含める必要がある。

- 現在の使用状況の監視
- 将来の需要予測
- 容量計画の策定
- 閾値の設定とアラート

監視項目

リソース	監視項目
CPU	使用率、負荷

リソース	監視項目
メモリ	使用量、空き容量
ストレージ	使用量、空き容量、I/O
ネットワーク	帯域使用率、遅延
データベース	接続数、クエリ性能

容量計画

ステップ	内容
現状分析	現在の使用状況の把握
需要予測	将来の需要の予測
計画策定	増強計画の策定
実施	計画に基づく増強
評価	効果の評価

当社における実施状況

当社では、クラウドサービス（AWS、GCP等）のリソース使用状況を監視し、適切な容量管理を行っている。必要に応じてリソースを拡張している。

関連文書

- 7. IT基盤運用管理

A.8.7 マルウェアに対する保護

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.7
分類	技術的管理策

管理策

マルウェアに対する保護は、実施し、適切な利用者の意識向上によって支援しなければならない。

目的

情報及びその他の関連資産がマルウェアから保護されることを確実にするため。

実施の手引き

マルウェアに対する保護には、以下を含める必要がある。

- マルウェア対策ソフトウェアの導入
- 定義ファイルの更新
- 定期的なスキャン
- 利用者への教育

マルウェアの種類

種類	説明
ウイルス	他のプログラムに感染

種類	説明
ワーム	自己複製して拡散
トロイの木馬	正規ソフトを装う
ランサムウェア	データを暗号化し身代金要求
スパイウェア	情報を窃取

対策

対策	内容
検知	リアルタイムスキャン、定期スキャン
防御	不正プログラムの実行阻止
更新	定義ファイルの自動更新
監視	感染状況の監視
対応	感染時の隔離、駆除

利用者の責任

- 不審なメール・添付ファイルを開かない
- 不審なWebサイトにアクセスしない
- 許可されていないソフトウェアをインストールしない
- 感染の疑いがある場合は直ちに報告

当社における実施状況

当社では、OSおよびサービスの標準的なセキュリティ機能を活用してマルウェア対策を実施している。不審なソフトウェアのインストールを禁止し、OSおよびソフトウェアを最新の状態に保つことを義務付けている。

関連文書

- 6. IT機器利用
- 11. テレワークにおける対策

A.8.8 技術的脆弱性の管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.8
分類	技術的管理策

管理策

利用中の情報システムの技術的脆弱性に関する情報は、獲得しなければならない。また、そのような脆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。

目的

技術的脆弱性の悪用を防止するため。

実施の手引き

技術的脆弱性の管理には、以下を含める必要がある。

- 脆弱性情報の収集
- 脆弱性の評価
- パッチ適用
- 脆弱性診断

脆弱性管理プロセス

ステップ	内容
情報収集	脆弱性情報の収集、監視

ステップ	内容
評価	影響度、緊急度の評価
優先順位付け	対応の優先順位決定
対応	パッチ適用、回避策
検証	対応の有効性確認

脆弱性の評価基準

評価項目	内容
CVSS	共通脆弱性評価システム
影響範囲	影響を受けるシステム
悪用可能性	攻撃コードの有無
事業影響	事業への影響度

当社における実施状況

当社では、DependabotやRenovateを活用して依存関係の脆弱性を自動検出し、速やかにアップデートを実施している。IPA、JVN等から脆弱性情報を収集している。

関連文書

- 8. システム開発及び保守
- 1. 組織的対策

A.8.9 構成管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.9
分類	技術的管理策

管理策

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は、確立し、文書化し、実施し、監視し、レビューしなければならない。

目的

ハードウェア、ソフトウェア、サービス及びネットワークが、必要なセキュリティ設定で正しく機能することを確実にするため。

実施の手引き

構成管理には、以下を含める必要がある。

- 標準構成の定義
- 構成の文書化
- 変更管理
- 構成の監視

構成管理の対象

対象	管理項目
ハードウェア	機器情報、設置場所
ソフトウェア	バージョン、ライセンス
ネットワーク	構成図、設定
セキュリティ	セキュリティ設定

標準構成（ベースライン）

項目	内容
OS設定	セキュリティ設定、不要サービス無効化
アプリケーション	承認されたソフトウェアのみ
ネットワーク	ファイアウォール設定
認証	パスワードポリシー

構成管理プロセス

ステップ	内容
識別	管理対象の特定
記録	構成情報の記録
管理	変更の管理
監査	構成の確認

当社における実施状況

当社では、システム構成情報を適切に管理し、変更履歴を記録している。Infrastructure as Codeを活用し、構成の一貫性を確保している。

関連文書

- 7. IT基盤運用管理
- 8. システム開発及び保守

A.8.10 情報の削除

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.10
分類	技術的管理策

管理策

情報システム、機器又はその他の記憶媒体に保存した情報は、不要になった場合に削除しなければならない。

目的

機密情報の不必要な露出を防止し、プライバシー及びその他の要求事項への適合を確実にするため。

実施の手引き

情報の削除には、以下を考慮する必要がある。

- 削除の時期と方法
- 法的保存要件
- 削除の検証
- 削除の記録

削除方法

方法	説明	適用
論理削除	ファイルシステムからの削除	一般データ
上書き消去	データを複数回上書き	機密データ
暗号化消去	暗号鍵の破棄	暗号化データ
物理的破壊	媒体の物理的破壊	最高機密

削除のタイミング

状況	対応
保存期間終了	定期的な削除
契約終了	顧客データの削除
退職	個人データの削除
機器廃棄	全データの削除

削除の検証

- 削除完了の確認
- 復元不可能性の検証
- 必要に応じて削除の記録を残す
- 監査証跡の保持

当社における実施状況

当社では、不要なデータは速やかに削除し、データの保持期間を適切に管理している。退職者のデータ、不要なバックアップ等は定期的に削除している。

関連文書

- 3. 情報資産管理

A.8.11 データマスキング

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.11
分類	技術的管理策

管理策

データマスキングは、適用される法令を考慮して、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使用しなければならない。

目的

機密データ及びPIIの露出を制限し、法令要求事項への適合を確実にするため。

実施の手引き

データマスキングには、以下の技術を使用できる。

- 静的マスキング
- 動的マスキング
- トークン化
- 匿名化

マスキング技術

技術	説明	用途
静的マスキング	データを恒久的に変換	テスト環境
動的マスキング	表示時にマスク	本番環境
トークン化	代替値に置換	決済データ
匿名化	個人を特定不能に	分析用データ

マスキング対象

データ種類	マスキング例
氏名	山田 → ○○
電話番号	090-1234-5678 → 090--
メールアドレス	user@example.com → u***@example.com
クレジットカード	1234-5678-9012-3456 → --****-3456

適用場面

- テスト環境でのデータ使用
- 開発者へのデータ提供
- 外部委託先へのデータ提供
- レポート・分析

当社における実施状況

当社では、テスト環境や開発環境で本番データを使用する場合は、必要に応じてデータマスキングを実施している。

関連文書

- 8. システム開発及び保守

A.8.12 データ漏洩の防止

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.12
分類	技術的管理策

管理策

データ漏洩防止策は、機密情報を処理、保存又は送信するシステム、ネットワーク及びその他の機器に適用しなければならない。

目的

個人又はシステムによる情報の認可されていない開示及び抽出を検知し、防止するため。

実施の手引き

データ漏洩防止（DLP）には、以下を含める必要がある。

- 機密データの識別と分類
- データの移動の監視
- 不正な転送のブロック
- インシデントの記録と対応

DLPの適用範囲

範囲	対策
エンドポイント	USB制御、印刷制御

範囲	対策
ネットワーク	メール監視、Web監視
クラウド	クラウドアプリの監視
ストレージ	ファイルサーバーの監視

検知ルール

ルール種類	例
キーワード	「機密」「社外秘」
パターン	クレジットカード番号、マイナンバー
ファイル種類	特定の拡張子
宛先	外部ドメイン

対応アクション

アクション	説明
監視	ログ記録のみ
警告	利用者への警告表示
ブロック	転送の阻止
通知	管理者への通知

当社における実施状況

当社では、データはクラウドサービス上に保存することを原則とし、ローカルへの恒久的な保存を禁止している。業務上やむを得ず一時的にローカルストレージに保存する場合は、「3. 情報資産管理」に定める条件（作業完了後の速やかな削除、ディスク暗号化の有効化等）に従う。USBメモリ等の外部記憶媒体の使用は原則禁止し、データ漏洩を防止している。

関連文書

- 3. 情報資産管理
- 6. IT機器利用

A.8.13 情報のバックアップ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.13
分類	技術的管理策

管理策

情報、ソフトウェア及びシステムのバックアップは、合意されたトピック固有のバックアップ方針に従って、維持し、定期的に検査しなければならない。

目的

データの消失からの復旧を可能にするため。

実施の手引き

バックアップには、以下を含める必要がある。

- バックアップ方針の策定
- バックアップの実施
- バックアップの検証
- 復旧テスト

バックアップの種類

種類	説明	特徴
フルバックアップ	全データのバックアップ	復旧が容易

種類	説明	特徴
差分バックアップ	前回フルからの変更分	中程度の効率
増分バックアップ	前回からの変更分	効率的

バックアップ計画

項目	内容
対象	バックアップ対象データ
頻度	日次、週次、月次
保存期間	世代管理、保存期間
保管場所	オンサイト、オフサイト
暗号化	バックアップデータの暗号化

当社における実施状況

当社では、重要なデータはクラウドサービス（AWS RDS、Cloud SQL等）の自動バックアップ機能を利用して定期的にバックアップを取得している。データは基本的にMySQLに格納されており、標準的なmysqldump/復元手順で対応可能なため、特別な復元訓練は実施していない。クラウドサービスの冗長性とマネージドバックアップ機能により、データの可用性を確保している。

関連文書

- 3. 情報資産管理
- 7. IT基盤運用管理

A.8.14 情報処理施設の冗長性

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.14
分類	技術的管理策

管理策

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実施しなければならない。

目的

情報処理施設の継続的な運用を確実にするため。

実施の手引き

冗長性の確保には、以下を考慮する必要がある。

- 可用性要件の特定
- 冗長構成の設計
- フェイルオーバーの実装
- 定期的なテスト

冗長化の対象

対象	冗長化方法
サーバー	クラスタリング、負荷分散

対象	冗長化方法
ストレージ	RAID、レプリケーション
ネットワーク	冗長経路、冗長機器
データセンター	DR サイト
電源	UPS、非常用発電機

冗長構成の種類

構成	説明
アクティブ-スタンバイ	待機系への切替
アクティブ-アクティブ	両系で負荷分散
N+1	予備系を1台確保
地理的分散	複数拠点での運用

フェイルオーバー

項目	内容
自動切替	障害検知時の自動切替
手動切替	計画的な切替
切替時間	RTO（目標復旧時間）
テスト	定期的な切替テスト

当社における実施状況

当社では、クラウドサービスの冗長性を活用し、単一障害点を排除している。重要なシステムは複数のアベイラビリティゾーンに分散配置している。

関連文書

- 7. IT基盤運用管理
- 10. 情報セキュリティインシデント対応及び事業継続管理

A.8.15 ログ取得

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.15
分類	技術的管理策

管理策

活動、例外処理、障害及びその他の関連する事象を記録したログを作成し、保存し、保護し、分析しなければならない。

目的

事象の記録、証拠の生成、ログ情報の完全性の確保、及び認可されていないアクセスの防止のため。

実施の手引き

ログ取得には、以下を含める必要がある。

- ログ取得の対象と内容
- ログの保存と保護
- ログの分析
- ログの保存期間

ログの種類

種類	内容
認証ログ	ログイン、ログアウト、認証失敗
アクセスログ	リソースへのアクセス
操作ログ	システム操作、設定変更
セキュリティログ	セキュリティイベント
エラーログ	エラー、例外処理

ログに含める情報

項目	内容
日時	イベント発生日時
利用者	利用者ID
イベント	イベントの種類
結果	成功/失敗
送信元	IPアドレス、端末

ログの保護

対策	内容
アクセス制御	ログへのアクセス制限
改ざん防止	ログの完全性保護
暗号化	ログの暗号化
バックアップ	ログのバックアップ

当社における実施状況

当社では、クラウドサービスのログ機能を活用し、アクセスログ、操作ログ等を記録・保存している。ログは定期的にレビューし、不正アクセスの検知に活用している。

各サービスのログ保存期間と長期保存

社内規程（セキュリティログ1年以上保存）を満たすため、デフォルトの保持期間が不足するサービスについては長期保存の仕組みを導入している。

サービス	ログの種類	デフォルト保持期間	長期保存方法
Microsoft Entra ID	サインインログ・監査ログ	7日	nightwatch によるエクスポート
Google Workspace Admin	管理者監査ログ	6ヶ月	nightwatch によるエクスポート
AWS CloudTrail	API操作ログ	90日	S3への全ログ保存
GCP Cloud Audit Logs (Admin Activity)	管理アクティビティログ	400日	要件充足のため追加対応不要

関連文書

- 7. IT基盤運用管理

A.8.16 監視活動

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.16
分類	技術的管理策

管理策

ネットワーク、システム及びアプリケーションは、異常な挙動がないか監視し、潜在的な情報セキュリティインシデントを評価するための適切な処置をとらなければならない。

目的

異常な挙動及び潜在的な情報セキュリティインシデントを検知するため。

実施の手引き

監視活動には、以下を含める必要がある。

- 監視対象の特定
- 監視ツールの導入
- アラートの設定
- インシデント対応

監視対象

対象	監視項目
ネットワーク	トラフィック、接続、異常通信

対象	監視項目
サーバー	リソース使用率、プロセス
アプリケーション	エラー、応答時間
セキュリティ	不正アクセス、マルウェア
ユーザー活動	異常な操作パターン

監視ツール

ツール種類	機能
SIEM	ログ収集、相関分析
IDS/IPS	侵入検知、防止
EDR	エンドポイント監視
NTA	ネットワークトラフィック分析

当社における実施状況

当社では、クラウドサービスの監視機能を活用し、システムの稼働状況、セキュリティイベント等を監視している。異常を検知した場合は速やかに対応している。

関連文書

- 7. IT基盤運用管理

A.8.17 クロックの同期

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.17
分類	技術的管理策

管理策

組織が使用する情報処理システムのクロックは、承認された時刻源と同期しなければならない。

目的

イベントの相関分析及び証拠としての利用を支援するため、システム間で一貫した時刻を確保するため。

実施の手引き

クロックの同期には、以下を含める必要がある。

- 時刻源の選定
- 同期プロトコルの設定
- 同期状態の監視
- タイムゾーンの統一

時刻同期の構成

要素	内容
時刻源	NTPサーバー、GPS
プロトコル	NTP、SNTP
階層	Stratum構成
精度	許容誤差

NTP構成例

階層	役割
外部NTPサーバー	公開NTPサーバー
内部NTPサーバー	組織内の時刻配信
クライアント	各システム、機器

監視項目

項目	内容
同期状態	同期の成功/失敗
時刻差	時刻源との差異
到達性	NTPサーバーへの接続

注意事項

- 信頼できる時刻源の使用
- 冗長な時刻源の確保
- ファイアウォールでのNTP許可
- ログのタイムスタンプの一貫性

当社における実施状況

当社では、クラウドサービスの時刻同期機能を利用し、システム間の時刻を同期している。ログの整合性を確保するため、NTPを活用している。

関連文書

- 7. IT基盤運用管理

A.8.18 特権的なユーティリティプログラムの使用

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.18
分類	技術的管理策

管理策

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が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。

目的

システム及びアプリケーションの制御を迂回するユーティリティプログラムの認可されていない使用を防止するため。

実施の手引き

特権的なユーティリティプログラムの管理には、以下を含める必要がある。

- 使用の制限
- アクセス制御
- 使用の監視
- 不要なプログラムの削除

特権ユーティリティの例

カテゴリ	例
システム管理	レジストリエディタ、サービス管理
ネットワーク	パケットキャプチャ、ポートスキャナ
ディスク	パーティション管理、データ復旧
セキュリティ	パスワードリセット、暗号化解除

管理策

対策	内容
制限	使用を認可された者のみに制限
削除	不要なユーティリティの削除
監視	使用状況のログ記録
分離	本番環境からの分離

使用手順

ステップ	内容
申請	使用目的、期間の申請
承認	管理者による承認
使用	承認された範囲での使用
記録	使用内容の記録
報告	使用結果の報告

当社における実施状況

当社では、特権ユーティリティプログラムの使用を制限し、必要な場合のみシステム管理者（CTO）が使用している。使用履歴を記録している。

関連文書

- 7. IT基盤運用管理

- 4. アクセス制御及び認証

A.8.19 運用システムに関わるソフトウェアの導入

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.19
分類	技術的管理策

管理策

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。

目的

運用システムの完全性を確保し、技術的脆弱性の悪用を防止するため。

実施の手引き

ソフトウェアの導入管理には、以下を含める必要がある。

- 導入の承認プロセス
- テスト環境での検証
- 変更管理との連携
- ロールバック手順

導入プロセス

ステップ	内容
申請	ソフトウェア導入の申請

ステップ	内容
評価	セキュリティ評価、互換性確認
承認	管理者による承認
テスト	テスト環境での検証
導入	本番環境への導入
確認	動作確認、監視

承認基準

項目	確認内容
必要性	業務上の必要性
ライセンス	適切なライセンス
セキュリティ	脆弱性、マルウェア
互換性	既存システムとの互換性
サポート	ベンダーサポート

禁止事項

- 未承認ソフトウェアの導入
- 不正コピーソフトウェアの使用
- 個人所有ソフトウェアの導入
- P2Pソフトウェアの使用

当社における実施状況

当社では、承認されたソフトウェアのみを使用することを義務付けている。新規ソフトウェアの導入にはシステム管理者（CTO）の承認が必要である。

関連文書

- 6. IT機器利用

A.8.20 ネットワークのセキュリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.20
分類	技術的管理策

管理策

ネットワーク及びネットワーク機器は、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、セキュリティを保ち、管理しなければならない。

目的

ネットワーク及びそのサポートする情報処理施設内の情報を保護するため。

実施の手引き

ネットワークのセキュリティには、以下を含める必要がある。

- ネットワーク設計
- アクセス制御
- 監視
- 機器の管理

ネットワークセキュリティ対策

対策	内容
ファイアウォール	境界防御、アクセス制御

対策	内容
IDS/IPS	侵入検知、防止
VPN	暗号化通信
セグメンテーション	ネットワーク分離

ネットワーク設計

要素	考慮事項
境界	DMZ、内部/外部の分離
セグメント	業務別、セキュリティレベル別
冗長性	経路の冗長化
監視	トラフィック監視ポイント

機器管理

項目	内容
構成管理	設定の文書化、変更管理
パッチ管理	ファームウェア更新
アクセス制御	管理アクセスの制限
ログ	機器ログの収集

当社における実施状況

当社では、クラウドサービス提供者の標準的なネットワークセキュリティ機能を活用している。VPC、セキュリティグループ等を適切に設定し、不正アクセスを防止している。

関連文書

- 7. IT基盤運用管理

A.8.21 ネットワークサービスのセキュリティ

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.21
分類	技術的管理策

管理策

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要求事項は、特定し、実施し、監視しなければならない。

目的

ネットワークサービスの利用におけるセキュリティを確保するため。

実施の手引き

ネットワークサービスのセキュリティには、以下を含める必要がある。

- サービスの特定
- セキュリティ要件の定義
- サービスレベルの合意
- 監視と管理

ネットワークサービスの種類

サービス	セキュリティ要件
インターネット接続	ファイアウォール、フィルタリング

サービス	セキュリティ要件
VPN	暗号化、認証
クラウドサービス	アクセス制御、暗号化
専用線	物理的セキュリティ

サービスレベル要件

項目	内容
可用性	稼働率、復旧時間
性能	帯域、遅延
セキュリティ	暗号化、認証
サポート	対応時間、連絡先

提供者の管理

項目	内容
契約	SLA、セキュリティ要件
監視	サービスレベルの監視
レビュー	定期的なレビュー
監査	セキュリティ監査

当社における実施状況

当社では、クラウドサービス提供者のネットワークセキュリティ機能を活用し、ネットワークサービスを保護している。必要に応じてWAF等を導入している。

関連文書

- 7. IT基盤運用管理

A.8.22 ネットワークの分離

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.22
分類	技術的管理策

管理策

情報サービス、利用者及び情報システムのグループは、組織のネットワーク上で分離しなければならない。

目的

ネットワーク上の情報及び情報処理施設のセキュリティを管理するため。

実施の手引き

ネットワークの分離には、以下を考慮する必要がある。

- セキュリティ要件に基づく分離
- 物理的又は論理的な分離
- 境界でのアクセス制御
- 分離の監視

分離の方法

方法	説明
物理的分離	別々のネットワーク機器

方法	説明
VLAN	論理的なネットワーク分離
ファイアウォール	セグメント間のアクセス制御
SDN	ソフトウェア定義ネットワーク

分離の例

セグメント	内容
DMZ	公開サーバー
内部ネットワーク	業務システム
管理ネットワーク	管理用通信
ゲストネットワーク	来客用
開発ネットワーク	開発環境

分離のルール

項目	内容
通信制御	必要な通信のみ許可
デフォルト拒否	明示的に許可されない通信は拒否
監視	セグメント間通信の監視
文書化	分離ルールの文書化

当社における実施状況

当社では、VPC、セキュリティグループ等を活用してネットワークを分離している。本番環境と開発環境は分離し、相互のアクセスを制限している。

関連文書

- 7. IT基盤運用管理
- 8. システム開発及び保守

A.8.23 ウェブ・フィルタリング

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.23
分類	技術的管理策

管理策

外部のウェブサイトへのアクセスは、悪意のあるコンテンツへの露出を低減するために管理しなければならない。

目的

マルウェア感染及び認可されていないウェブリソースへのアクセスからシステムを保護するため。

実施の手引き

ウェブ・フィルタリングには、以下を含める必要がある。

- フィルタリングポリシーの策定
- カテゴリベースのフィルタリング
- URLフィルタリング
- コンテンツ検査

フィルタリング対象

カテゴリ	対応
マルウェア配布サイト	ブロック
フィッシングサイト	ブロック
アダルトサイト	ブロック
ギャンブルサイト	ブロック
SNS	業務に応じて制限
クラウドストレージ	業務に応じて制限

フィルタリング方式

方式	説明
URLフィルタリング	URLに基づくブロック
カテゴリフィルタリング	サイトカテゴリに基づく制御
コンテンツフィルタリング	コンテンツ内容の検査
SSL検査	暗号化通信の検査

運用

項目	内容
ポリシー更新	定期的なポリシー見直し
例外申請	業務上必要な場合の例外
ログ	アクセスログの記録
レポート	利用状況のレポート

当社における実施状況

当社では、インターネット接続はクラウドサービスのセキュリティ機能を活用して保護している。不審なサイトへのアクセスは禁止している。

関連文書

- 6. IT機器利用
- 7. IT基盤運用管理

A.8.24 暗号の使用

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.24
分類	技術的管理策

管理策

暗号の効果的な使用のための規則は、鍵管理を含めて、定め、実施しなければならない。

目的

情報の機密性、真正性及び完全性を保護するために、暗号を適切かつ効果的に使用することを確実にするため。

実施の手引き

暗号の使用には、以下を含める必要がある。

- 暗号方針の策定
- 適切な暗号アルゴリズムの選択
- 鍵管理
- 法令要件への対応

暗号の用途

用途	説明
機密性	データの暗号化

用途	説明
完全性	ハッシュ、MAC
認証	デジタル署名
否認防止	デジタル署名

暗号アルゴリズム

種類	推奨アルゴリズム
共通鍵暗号	AES-256
公開鍵暗号	RSA-2048以上、ECDSA
ハッシュ	SHA-256以上
TLS	TLS 1.2以上

鍵管理

項目	内容
生成	安全な乱数生成
配布	安全な鍵配布
保管	安全な保管、アクセス制御
更新	定期的な鍵更新
廃棄	安全な鍵廃棄

当社における実施状況

当社では、機密情報の転送時にはHTTPS等の暗号化通信を使用している。クラウドサービスの暗号化機能を活用し、保存データも暗号化している。

関連文書

- 3. 情報資産管理
- 7. IT基盤運用管理

A.8.25 セキュリティに配慮した開発のライフサイクル

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.25
分類	技術的管理策

管理策

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は、確立し、適用しなければならない。

目的

開発ライフサイクル全体を通じて、情報セキュリティが設計され、実装されることを確実にするため。

実施の手引き

セキュリティに配慮した開発には、以下を含める必要がある。

- セキュリティ要件の定義
- セキュアコーディング
- セキュリティテスト
- セキュリティレビュー

開発ライフサイクルの各フェーズ

フェーズ	セキュリティ活動
要件定義	セキュリティ要件の特定
設計	セキュリティ設計、脅威モデリング
実装	セキュアコーディング
テスト	セキュリティテスト
リリース	セキュリティレビュー
運用	脆弱性管理

セキュアコーディング

項目	内容
入力検証	すべての入力の検証
出力エンコーディング	XSS対策
認証・認可	適切な認証・認可
エラー処理	安全なエラー処理
暗号化	適切な暗号化の使用

セキュリティテスト

テスト種類	内容
静的解析	ソースコードの分析
動的解析	実行時の分析
ペネトレーションテスト	侵入テスト
コードレビュー	セキュリティ観点のレビュー

当社における実施状況

当社では、システム開発時にセキュリティ要件を考慮し、セキュアな開発ライフサイクルを実施している。コードレビュー、セキュリティテスト等を実施している。

関連文書

- 8. システム開発及び保守

A.8.26 アプリケーションのセキュリティ要求事項

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.26
分類	技術的管理策

管理策

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

目的

アプリケーションの開発又は取得において、必要なすべての情報セキュリティ要求事項が特定され、対処されることを確実にするため。

実施の手引き

アプリケーションのセキュリティ要求事項には、以下を含める必要がある。

- 認証・認可要件
- データ保護要件
- 監査・ログ要件
- 可用性要件

セキュリティ要求事項の分類

分類	要求事項例
認証	多要素認証、パスワードポリシー
認可	役割ベースアクセス制御
データ保護	暗号化、マスキング
監査	ログ記録、監査証跡
可用性	冗長性、バックアップ

要求事項の定義プロセス

ステップ	内容
特定	セキュリティ要求事項の特定
分析	リスク分析、影響評価
文書化	要求事項の文書化
承認	関係者による承認
検証	実装の検証

取得時の考慮事項

項目	内容
ベンダー評価	セキュリティ対応能力
契約	セキュリティ要件の明記
検証	受入テスト
サポート	脆弱性対応

当社における実施状況

当社では、アプリケーション開発時にセキュリティ要件を定義し、設計・実装に反映している。認証、認可、入力検証等のセキュリティ機能を実装している。

関連文書

- 8. システム開発及び保守

A.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

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.27
分類	技術的管理策

管理策

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は、確立し、文書化し、維持し、あらゆる情報システムの開発活動に適用しなければならない。

目的

情報システムがセキュリティに配慮して設計、実装、運用されることを確実にするため。

実施の手引き

セキュリティに配慮したシステム構築の原則には、以下を含める必要がある。

- 多層防御
- 最小権限
- フェイルセキュア
- 攻撃面の最小化

セキュリティ設計原則

原則	説明
多層防御	複数の防御層を設ける
最小権限	必要最小限の権限のみ付与
フェイルセキュア	障害時も安全な状態を維持
攻撃面の最小化	不要な機能・サービスの無効化
職務分離	重要な機能の分離

アーキテクチャの考慮事項

要素	考慮事項
ネットワーク	セグメンテーション、境界防御
アプリケーション	入力検証、セッション管理
データ	暗号化、アクセス制御
インフラ	ハードニング、パッチ管理

実装ガイドライン

項目	内容
標準化	セキュリティ標準の適用
レビュー	設計レビュー、コードレビュー
テスト	セキュリティテスト
文書化	セキュリティ設計の文書化

当社における実施状況

当社では、セキュアなシステムアーキテクチャを採用し、多層防御の原則に基づいて設計している。クラウドサービスのセキュリティ機能を活用している。

関連文書

- 8. システム開発及び保守

- 7. IT基盤運用管理

A.8.28 セキュリティに配慮したコーディング

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.28
分類	技術的管理策

管理策

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

目的

ソフトウェアがセキュリティの脆弱性なく開発されることを確実にするため。

実施の手引き

セキュリティに配慮したコーディングには、以下を含める必要がある。

- コーディング標準の策定
- 脆弱性の防止
- コードレビュー
- 静的解析

一般的な脆弱性と対策

脆弱性	対策
SQLインジェクション	パラメータ化クエリ

脆弱性	対策
XSS	出力エンコーディング
CSRF	トークン検証
バッファオーバーフロー	境界チェック
認証の欠陥	適切な認証実装

コーディング標準

項目	内容
入力検証	すべての入力を検証
出力エンコーディング	コンテキストに応じたエンコード
エラー処理	安全なエラー処理
暗号化	標準的な暗号ライブラリの使用
ログ	機密情報をログに含めない

コードレビュー

項目 内容

目的 セキュリティ脆弱性の検出

方法 ピアレビュー、ツール支援

頻度 コミット時、リリース前

記録 レビュー結果の記録

当社における実施状況

当社では、セキュアコーディングの原則に従って開発を行っている。OWASP等のガイドラインを参考に、脆弱性を作り込まない開発を実施している。

関連文書

- 8. システム開発及び保守

A.8.29 開発及び受入れにおけるセキュリティ試験

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.29
分類	技術的管理策

管理策

セキュリティ試験のプロセスは、開発ライフサイクルにおいて定め、実施しなければならない。

目的

新しい又は更新されたシステムが、セキュリティ要件を満たしていることを検証するため。

実施の手引き

セキュリティ試験には、以下を含める必要がある。

- 試験計画の策定
- 試験の実施
- 結果の評価
- 是正措置

セキュリティ試験の種類

種類	説明
静的解析	ソースコードの分析

種類	説明
動的解析	実行時の分析
脆弱性スキャン	既知の脆弱性の検出
ファジング	異常入力によるテスト

試験プロセス

フェーズ	活動
計画	試験計画、範囲、基準の定義
準備	環境構築、ツール準備
実施	試験の実行
報告	結果の分析、報告書作成
是正	発見事項への対応
再試験	是正後の確認

受入れ基準

項目	基準
重大な脆弱性	ゼロ
高リスク脆弱性	是正済み
中リスク脆弱性	是正計画あり
低リスク脆弱性	文書化

当社における実施状況

当社では、開発・受入れ時にセキュリティテストを実施している。脆弱性診断等を必要に応じて実施している。

関連文書

- 8. システム開発及び保守

A.8.30 外部委託による開発

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.30
分類	技術的管理策

管理策

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

目的

外部委託による開発において、組織が要求するセキュリティ対策が実施されることを確実にするため。

実施の手引き

外部委託による開発の管理には、以下を含める必要がある。

- 委託先の選定と評価
- 契約でのセキュリティ要件
- 開発の監視
- 成果物の検証

委託先の選定

評価項目	内容
セキュリティ体制	ISMS認証、セキュリティポリシー

評価項目	内容
実績	類似プロジェクトの経験
技術力	セキュア開発能力
財務状況	事業継続性

契約要件

項目	内容
セキュリティ要件	開発標準、セキュリティ基準
機密保持	NDA、情報の取扱い
知的財産	著作権、ソースコードの帰属
監査権	セキュリティ監査の実施権
責任	脆弱性発見時の対応責任

監視活動

活動	内容
進捗管理	定期的な進捗確認
品質管理	コードレビュー、テスト結果確認
セキュリティ確認	セキュリティ要件の遵守確認
成果物検証	受入テスト

当社における実施状況

当社では、開発を外部委託する場合、NDAを締結し、セキュリティ要件を契約に含めている。委託先には指定された環境での作業、最小限の権限付与、契約終了時のアカウント削除を義務付けている。

関連文書

- 8. システム開発及び保守
- 9. 委託管理

A.8.31 開発環境、試験環境及び運用環境の分離

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.31
分類	技術的管理策

管理策

開発環境、試験環境及び運用環境は、分離し、セキュリティを保たなければならない。

目的

開発及び試験活動から運用環境を保護するため。

実施の手引き

環境の分離には、以下を含める必要がある。

- 物理的又は論理的な分離
- アクセス制御
- データの分離
- 変更管理

環境の種類

環境	目的
開発環境	ソフトウェアの開発
試験環境	テストの実施

環境	目的
ステージング環境	本番前の検証
運用環境	本番サービスの提供

分離の方法

方法	内容
物理的分離	別々のサーバー、ネットワーク
論理的分離	仮想化、コンテナ
アクセス制御	環境ごとのアクセス権
ネットワーク分離	環境間の通信制限

環境別のルール

項目	開発	試験	運用
アクセス	開発者	テスター	運用者
データ	テストデータ	マスクデータ	本番データ
変更	自由	管理下	厳格な管理

注意事項

- 本番データを開発・試験環境で使用しない
- 開発者の本番環境へのアクセス制限
- 環境間の移行手順の確立

当社における実施状況

当社では、開発環境、テスト環境、本番環境を分離している。本番データを開発・テスト環境で使用する場合は、必要に応じてマスキングを実施している。

関連文書

- 8. システム開発及び保守

A.8.32 変更管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.32
分類	技術的管理策

管理策

情報処理施設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。

目的

変更の実施時に情報セキュリティを維持するため。

実施の手引き

変更管理には、以下を含める必要がある。

- 変更要求の記録
- 影響評価
- 承認プロセス
- テスト
- 実施とレビュー

変更管理プロセス

ステップ	内容
要求	変更要求の提出

ステップ	内容
評価	影響評価、リスク評価
承認	適切な承認
計画	実施計画、ロールバック計画
テスト	変更のテスト
実施	変更の実施
レビュー	実施後のレビュー

変更の分類

分類	説明	承認
標準変更	事前承認された変更	自動承認
通常変更	計画的な変更	適切な承認
緊急変更	緊急対応が必要な変更	緊急承認

変更記録

項目	内容
変更ID	一意の識別子
要求者	変更要求者
内容	変更の詳細
影響	影響範囲
承認者	承認者
実施日	実施日時
結果	実施結果

当社における実施状況

当社では、システム変更は適切な承認プロセスを経て実施している。変更履歴はGitHub Issue/PR等で管理し、問題発生時にはロールバックできるようにしている。

関連文書

- 8. システム開発及び保守
- 7. IT基盤運用管理

A.8.33 試験情報

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.33
分類	技術的管理策

管理策

試験情報は、適切に選定し、保護し、管理しなければならない。

目的

試験活動の妥当性及び試験情報の保護を確実にするため。

実施の手引き

試験情報の管理には、以下を含める必要がある。

- 試験データの選定
- 本番データの保護
- 試験データの管理
- 試験後のデータ処理

試験データの種類

種類	説明
合成データ	人工的に生成したデータ
マスクデータ	本番データをマスキング

種類	説明
サンプルデータ	本番データの一部
本番データ	実際の本番データ

本番データ使用時の対策

対策	内容
マスキング	個人情報等のマスキング
匿名化	個人を特定できないよう加工
アクセス制御	試験データへのアクセス制限
削除	試験後のデータ削除

試験データ管理

項目	内容
作成	試験データの作成、準備
保管	安全な保管
使用	承認された目的での使用
廃棄	試験後の適切な廃棄

注意事項

- 本番データの使用は最小限に
- 個人情報を含むデータは必ずマスキング
- 試験環境のセキュリティ確保
- 試験データの漏洩防止

当社における実施状況

当社では、テストデータは本番データと分離して管理している。本番データをテストに使用する場合は、必要に応じてマスキングを実施している。

関連文書

- 8. システム開発及び保守

A.8.34 監査試験中の情報システムの保護

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員
管理策番号	A.8.34
分類	技術的管理策

管理策

運用システムの検証を伴う監査試験及びその他の保証活動は、計画し、監査人と管理者との間で合意しなければならない。

目的

監査活動による運用プロセスへの影響を最小限に抑えるため。

実施の手引き

監査試験中の保護には、以下を含める必要がある。

- 監査の計画と合意
- アクセスの制限
- 活動の監視
- 結果の保護

監査計画

項目	内容
範囲	監査対象システム、データ

項目	内容
日程	実施日時、期間
方法	監査手法、ツール
担当	監査人、立会者
影響	想定される影響

アクセス制御

対策	内容
読取り専用	可能な限り読取り専用アクセス
監視	監査活動の監視
記録	アクセスログの記録
立会い	担当者の立会い

監査ツールの管理

項目	内容
承認	使用ツールの事前承認
検証	ツールの安全性確認
制限	使用範囲の制限
削除	監査後のツール削除

監査結果の保護

- 監査結果の機密保持
- 報告書のアクセス制限
- 発見事項の適切な取扱い
- 是正措置の追跡

当社における実施状況

当社では、監査テスト時に本番システムへの影響を最小限に抑えるよう計画している。監査ツールへのアクセスは制限し、使用後は適切に管理している。

関連文書

- 1. 組織的対策
- 7. IT基盤運用管理