ISMSマニュアル

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. 9.1 監視、測定、分析及び評価

23. 9.2 内部監査

24. 9.3 マネジメントレビュー

25. 10.1 継続的改善

26. 10.2 不適合及び是正処置

1. 適用範囲

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2026.03.04
適用範囲	全社
箇条番号	1
分類	適用範囲

要求事項

この規格は，組織の状況の下で，ISMSを確立し，実施し，維持し，継続的に改善するための要求事項について規定する。また，この規格は，組織のニーズに応じて調整した情報セキュリティのリスクアセスメント及びリスク対応を行うための要求事項についても規定する。この規格が規定する要求事項は，汎用的であり，形態，規模又は性質を問わず，全ての組織に適用できることを意図している。組織がこの規格への適合を宣言する場合には，**箇条4～箇条10** に規定するいかなる要求事項の除外も認められない。

ⓘノート

この規格の対応国際規格及びその対応の程度を表す記号を，次に示す。

ISO/IEC 27001:2022，Information security, cybersecurity and privacy protection－Information security management systems－Requirements（IDT）

なお，対応の程度を表す記号”IDT”は，ISO/IEC Guide 21-1 に基づき，“一致している”ことを示す。

目的

この規格の適用範囲を明確にし、ISMSを確立・実施・維持・継続的改善するための要求事項の対象を定めるため。

当社における適用

当社は、JIS Q 27001:2025（ISO/IEC 27001:2022 + Amd 1:2024）の要求事項に基づき、語学教育事業部を適用範囲としてISMSを構築・運用している。詳細な適用範囲については「4.3 ISMSの適用範囲の決定」を参照。

関連文書

- 情報セキュリティ基本方針
- 4.3 ISMSの適用範囲の決定

2. 引用規格

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2026.03.04
適用範囲	全社
箇条番号	2
分類	引用規格

要求事項

次に掲げる引用規格は，この規格に引用されることによって，その一部又は全部がこの規格の要求事項を構成している。この引用規格は，その最新版（追補を含む。）を適用する。

JIS Q 27000 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

ⓘノート

対応国際規格における引用規格：ISO/IEC 27000，Information technology－Security techniques－Information security management systems－Overview and vocabulary

目的

この規格が参照する引用規格を明確にし、用語及び定義の基準を示すため。

当社における参照

当社では、ISMSの構築・運用において、以下の規格を参照している。

- **JIS Q 27000:2019** - 用語及び定義
- **JIS Q 27001:2025（ISO/IEC 27001:2022 + Amd 1:2024）** - 要求事項（本規格。気候変動に関する追補を含む）

- **JIS Q 27002:2024** - 管理策の指針

ⓘノート

当社では、ISO/IEC 27001:2022/Amd 1:2024（気候変動に関する追補）を含むJIS Q 27001:2025を適用規格としている。

関連文書

- 3 用語及び定義
- ISO/IEC 27001:2022 参考資料

3. 用語及び定義

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
箇条番号	3
分類	用語及び定義

要求事項

この規格で用いる主な用語及び定義は，JIS Q 27000による。

なお，ISO及びIECでは，標準化に使用するための用語のデータベースが次に公開されている。

- ISO Online browsing platform: https://www.iso.org/obp/ui
- IEC Electropedia: https://www.electropedia.org/

目的

この規格で使用する用語の定義を明確にし、規格の解釈における一貫性を確保するため。

主要な用語（JIS Q 27000:2019より）

以下は、ISMSにおいて特に重要な用語の定義である。

情報セキュリティ（information security）

情報の機密性、完全性及び可用性を維持すること。

情報セキュリティマネジメントシステム（ISMS）

マネジメントシステムの一部であって、情報セキュリティリスクに対処するために、情報セキュリティ方針及び目的、並びにそれらの目的を達成するためのプロセスを含むもの。

リスク（risk）

目的に対する不確かさの影響。

リスクアセスメント（risk assessment）

リスク特定、リスク分析及びリスク評価のプロセス全体。

リスク対応（risk treatment）

リスクを修正するプロセス。

管理策（control）

リスクを修正する対策。

機密性（confidentiality）

認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。

完全性（integrity）

正確さ及び完全さの特性。

可用性（availability）

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

関連文書

- JIS Q 27000:2019 情報セキュリティマネジメントシステムー用語
- 2 引用規格

4.1 組織及びその状況の理解

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2026.03.04
適用範囲	全社
箇条番号	4.1
分類	組織の状況

要求事項

組織は、組織の目的に関連し、かつ、そのISMSの意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を決定しなければならない。

ⓘノート

これらの課題の決定とは、ISO 31000:2018の箇条5.4.1で考慮される組織の外部状況及び内部状況の確定のことをいう。

目的

組織が置かれている状況を理解し、ISMSの適用範囲及びリスクアセスメントの基礎となる情報を特定するため。

当社の事業計画

当社は以下の2つの事業を展開している。

語学教育事業

官公庁・地方教育委員会・一般のお客様向けに、オンライン英会話サービス及び教育支援サービスを提供する主力事業。システム開発、コーチング、学校派遣支援等を含む。

atomico（学童）事業

学童保育サービスを提供する新規事業。語学教育事業とは独立した事業運営を行っている。

実施の手引き

外部の課題

外部の課題には、以下のようなものが含まれる。

- 法的、規制的、及び契約上の要求事項
- 社会的、文化的、政治的、経済的環境
- 技術的な傾向及び発展
- 競争環境及び市場の状況
- 外部の利害関係者との関係

内部の課題

内部の課題には、以下のようなものが含まれる。

- 組織の文化
- 組織の構造、役割及び責任
- 方針、目的及びそれらを達成するための戦略
- 資源及び知識（資本、人、プロセス、システム及び技術など）
- 情報システム、情報の流れ及び意思決定プロセス
- 導入された規格、指針及びモデル
- 契約関係の形態及び範囲

当社における実施状況

当社では、以下の方法により外部及び内部の課題を特定し、定期的にレビューしている。

外部課題の特定

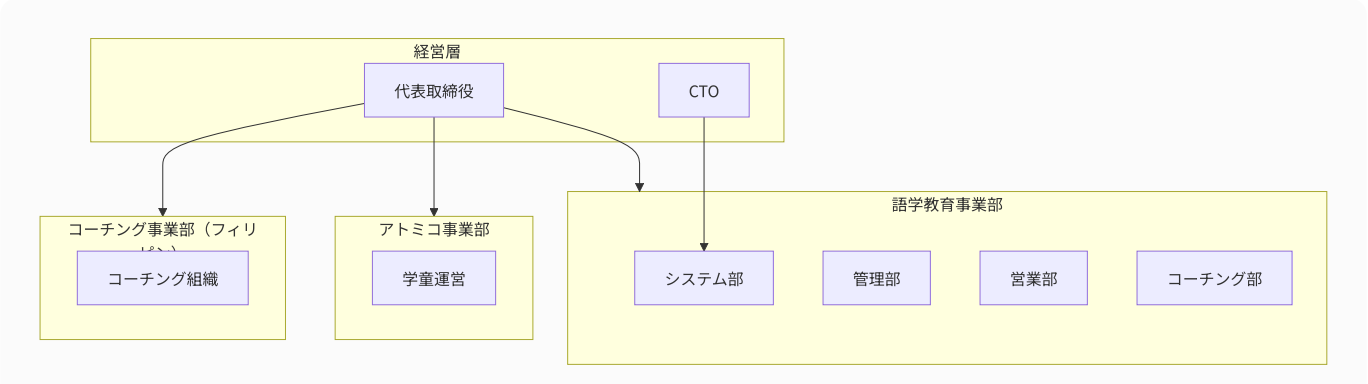
- 法令・規制の動向監視（個人情報保護法、サイバーセキュリティ基本法等）
- 業界動向及び技術トレンドの把握

- 顧客・取引先からの要求事項の収集
- セキュリティ脅威情報の収集・分析
- **生成AI時代における競争力の維持**: 生成AI技術の急速な発展に伴い、EdTech市場における競争環境が変化しており、技術革新への迅速な対応が求められる
- **お客様ニーズの変化への速やかな対応**: 官公庁・教育委員会・一般顧客のニーズが多様化・高度化しており、セキュリティを確保しながら柔軟なサービス提供が必要
- **気候変動への配慮**: 気候変動への配慮（温暖化対策等）について、関係者ニーズが高くなく、すでにWeb会議やペーパーレス化が進んでいるため、当社では考慮を含めない

内部課題の特定

- 組織体制及び役割分担の明確化
- 情報資産の棚卸し及び管理
- 従業員のセキュリティ意識・力量の評価
- 既存のセキュリティ対策の有効性評価
- **生成AI時代の新たな情報セキュリティ事故防止**: 生成AIツールの業務利用に伴う情報漏洩リスク（機密情報の意図しない入力等）への対策が必要
- **情報セキュリティリテラシーの向上**: 生成AI等の新技術に関する従業員のセキュリティ意識・知識の継続的な向上が必要
- **新規脆弱性への対応**: 生成AIを活用した新たな攻撃手法や、AI関連サービスの脆弱性に対する迅速な対応体制の整備が必要

組織体制



詳細な役割・責任については「1. 組織的対策」を参照。

レビュー

外部及び内部の課題は、年1回のマネジメントレビュー及び重大な変化が発生した場合に見直しを行う。

関連文書

- 情報セキュリティ基本方針
- 1. 組織的対策
- 14. リスクアセスメント

4.2 利害関係者のニーズ及び期待の理解

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
箇条番号	4.2
分類	組織の状況

要求事項

組織は、次の事項を決定しなければならない。

a) ISMSに関連する利害関係者 b) それらの利害関係者の、情報セキュリティに関連する要求事項 c) これらの要求事項のうち、ISMSを通じて取り組むもの

ⓘノート

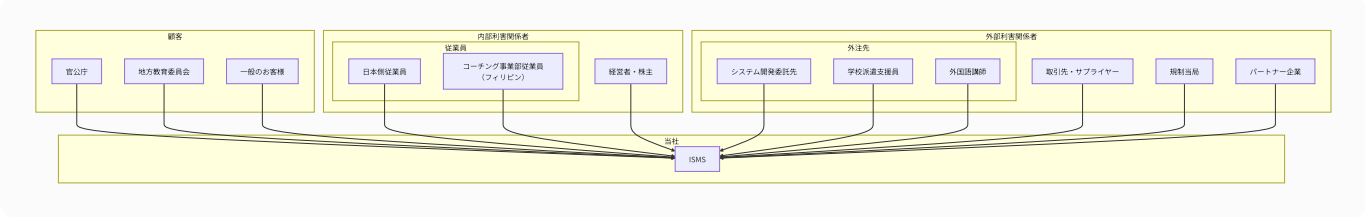
利害関係者の要求事項には、法的及び規制的要求事項並びに契約上の義務が含まれ得る。

目的

ISMSの適用範囲を決定し、利害関係者の期待に応えるための基礎情報を特定するため。

当社における利害関係者

利害関係者マップ



利害関係者と要求事項

利害関係者	情報セキュリティに関連する要求事項	ISMSでの対応
官公庁	政府統一基準への準拠、機密性の確保、インシデント報告体制	セキュリティポリシーの整備、アクセス制御、インシデント対応手順
地方教育委員会	教育情報セキュリティポリシーへの準拠、児童生徒情報の保護	個人情報保護対策、アクセス権限管理、データ暗号化
一般のお客様	個人情報の適切な取扱い、サービスの可用性	プライバシーポリシー、サービス継続性管理
従業員	安全な労働環境、情報セキュリティ教育	セキュリティ教育・訓練、インシデント報告体制
経営者・株主	事業継続性、コンプライアンス、リスク管理	BCP/BCM、内部監査、マネジメントレビュー
システム開発委託先	開発環境のセキュリティ、ソースコード管理、脆弱性対策	委託先管理、NDA締結、セキュリティ要件の明確化
学校派遣支援員	児童生徒情報の取扱いルール、現場でのセキュリティ遵守	セキュリティ教育、情報取扱いガイドライン
外国語講師	個人情報の取扱い、業務上知り得た情報の守秘義務	NDA締結、セキュリティ教育
取引先・サプライヤー	契約上のセキュリティ要件、情報共有ルール	委託先管理、NDA締結、セキュリティ要件の明確化
規制当局	法令遵守（個人情報保護法、サイバーセキュリティ基本法等）	法令対応、監査対応、報告体制
パートナー企業	協業におけるセキュリティ基準の統一	セキュリティ基準の共有、定期的な情報交換

レビュー

利害関係者及びその要求事項は、年1回のマネジメントレビュー及び重大な変化が発生した場合に見直しを行う。

関連文書

- 4.1 組織及びその状況の理解
- 情報セキュリティ基本方針
- 1. 組織的対策

4.3 ISMSの適用範囲の決定

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2026.03.04
適用範囲	全社
箇条番号	4.3
分類	組織の状況

要求事項

組織は、ISMSの適用範囲を定めるために、その境界及び適用可能性を決定しなければならない。

この適用範囲を決定するとき、組織は、次の事項を考慮しなければならない。

a) 4.1に規定する外部及び内部の課題 b) 4.2に規定する要求事項 c) 組織が実施する活動と他の組織が実施する活動との間のインターフェース及び依存関係

適用範囲は、文書化した情報として利用可能な状態にしておかなければならない。

目的

ISMSが適用される組織の範囲を明確にし、情報セキュリティ管理の対象を特定するため。

当社のISMS適用範囲

適用範囲に含まれる事業・組織

当社のISMSは、スパトレ株式会社 語学教育事業部を適用範囲とする。語学教育事業部は、以下の部門で構成される。

- システム部（日本）
- 管理部（日本）
- 営業部（日本）

語学教育事業部は当社の主力事業であり、官公庁・地方教育委員会・一般のお客様の機密情報及び個人情報を取り扱うため、ISMSの適用範囲に含める。

物理的な適用範囲

物理オフィスの範囲については、以下の文書を参照すること。

- ネットワーク構成図
- オフィスレイアウト図

適用範囲から除外する事業・組織

以下の事業及び組織は、リスクベースアプローチに基づく評価の結果、ISMSの適用範囲から除外する。

atomico（学童）事業

atomico事業は以下の理由により、ISMSの適用範囲から除外する。

1. **新規事業としての位置づけ**: atomico事業は立ち上げ段階の新規事業であり、事業規模が限定的である。事業の成熟度に応じて、将来的にISMS適用範囲への組み入れを検討する。

2. **事業影響度の限定性**: atomico事業で取り扱う情報資産の規模は小さく、万一のインシデント発生時においても、当社全体の事業継続性への影響は極めて限定的である。

3. **既存事業との独立性**: atomico事業は語学教育事業とは独立した事業運営を行っており、情報システム・情報資産の共有が限定的である。両事業間のインターフェース及び依存関係が低いため、語学教育事業のセキュリティリスクへの波及は想定されない。

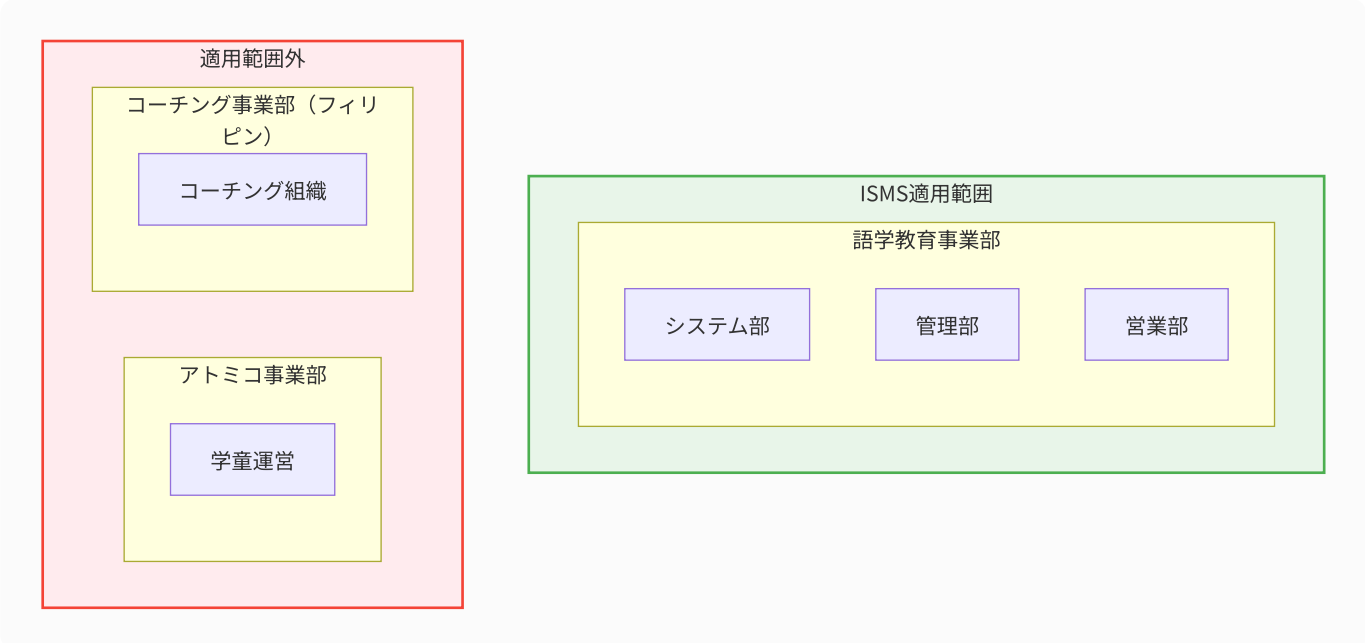
4. **リソースの最適配分**: 限られた情報セキュリティ管理リソースを、より高いリスクを有する語学教育事業部に集中させることで、ISMS全体の有効性を高める。

コーチング事業部（フィリピン）

コーチング事業部（フィリピン）は以下の理由により、ISMSの適用範囲から除外する。

1. **人員の流動性**: コーチング事業部は人員の入れ替わりが激しく、継続的なISMS運用体制の維持が困難である。
2. **事業影響度の限定性**: コーチング事業部でインシデントが発生した場合においても、当社の事業継続性への影響は極めて低い。コーチング業務は代替可能性が高く、サービス提供の継続に重大な支障を来すことは想定されない。
3. **機密情報へのアクセス制限**: コーチング事業部がアクセスできる情報は、レッスン実施に必要な最小限の情報に限定されており、機密性の高い情報資産へのアクセス権限は付与されていない。
4. **技術的分離**: コーチング事業部が利用するシステムは、日本側の基幹システムとは利用するアプリケーション、アクセスが分離されている。

適用範囲の図示



適用範囲除外の妥当性確認

適用範囲から除外した事業・組織については、以下の観点から妥当性を確認している。

除外対象	リスク評価	事業影響度	情報資産の独立性	除外の妥当性
アトミコ事業部	低	限定的	高（独立運営）	妥当
コーチング事業部（フィリピン）	低	極めて低	高（技術的分離）	妥当

適用範囲の見直し

適用範囲は、以下の場合に見直しを行う。

- 年1回のマネジメントレビュー時
- 事業構造に重大な変化が発生した場合
- 除外対象の事業規模が拡大した場合
- 除外対象と適用範囲内の事業との依存関係が増加した場合

特にatomico事業については、事業の成長に伴い、取り扱う情報資産の規模や機密性が増加した場合には、ISMS適用範囲への組み入れを検討する。

関連文書

- 4.1 組織及びその状況の理解
- 4.2 利害関係者のニーズ及び期待の理解
- 情報セキュリティ基本方針
- 14. リスクアセスメント

4.4 情報セキュリティマネジメントシステム

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
箇条番号	4.4
分類	組織の状況

要求事項

組織は、この規格の要求事項に従って、必要なプロセス及びそれらの相互作用を含む、情報セキュリティマネジメントシステムを確立し、実施し、維持し、かつ、継続的に改善しなければならない。

目的

組織が情報セキュリティを体系的に管理するための仕組み（ISMS）を構築し、継続的に運用・改善することで、情報セキュリティリスクを適切に管理するため。

当社における実施状況

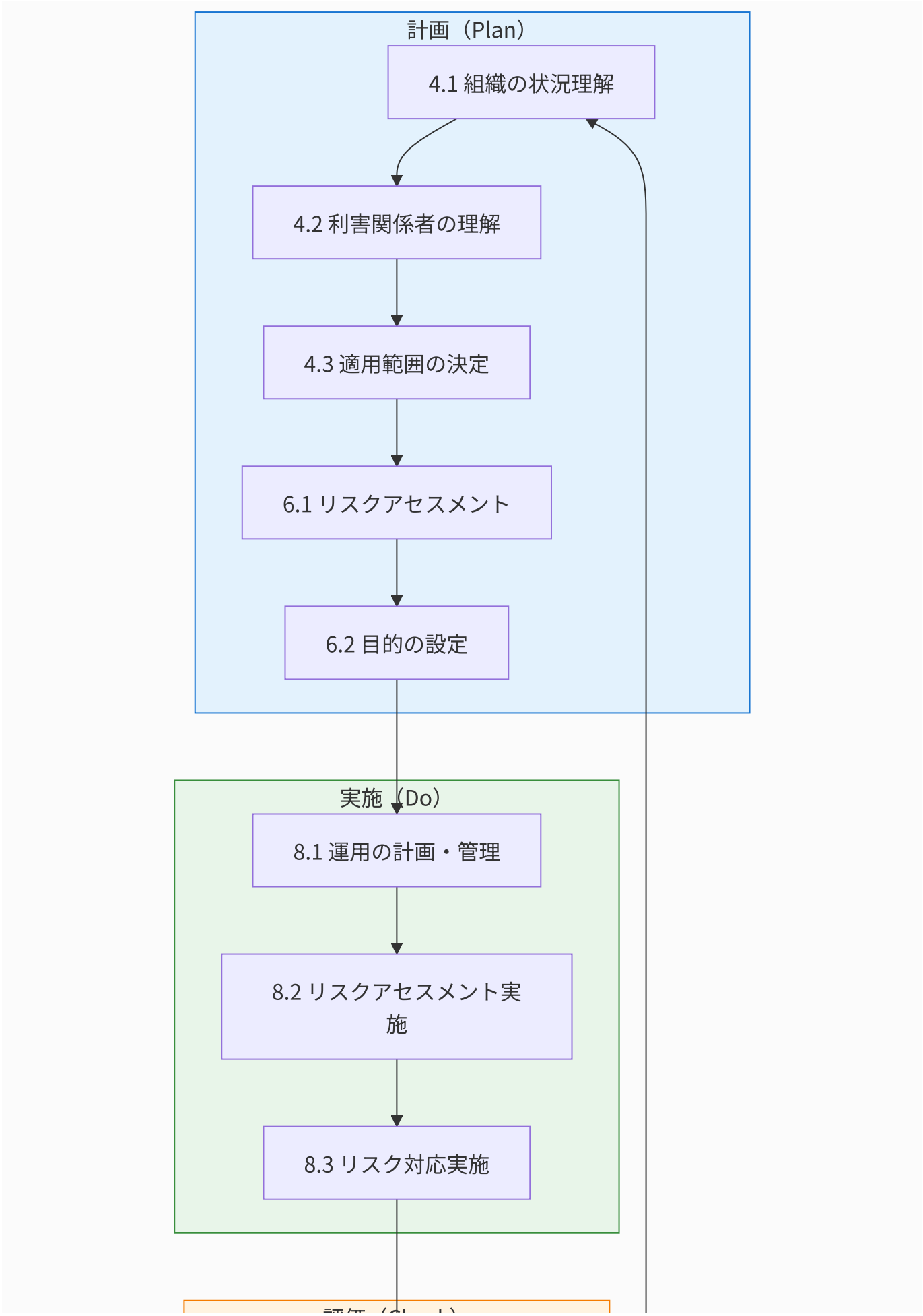
当社では、JIS Q 27001:2023の要求事項に従い、以下のプロセス及びその相互作用を含むISMSを確立し、運用している。

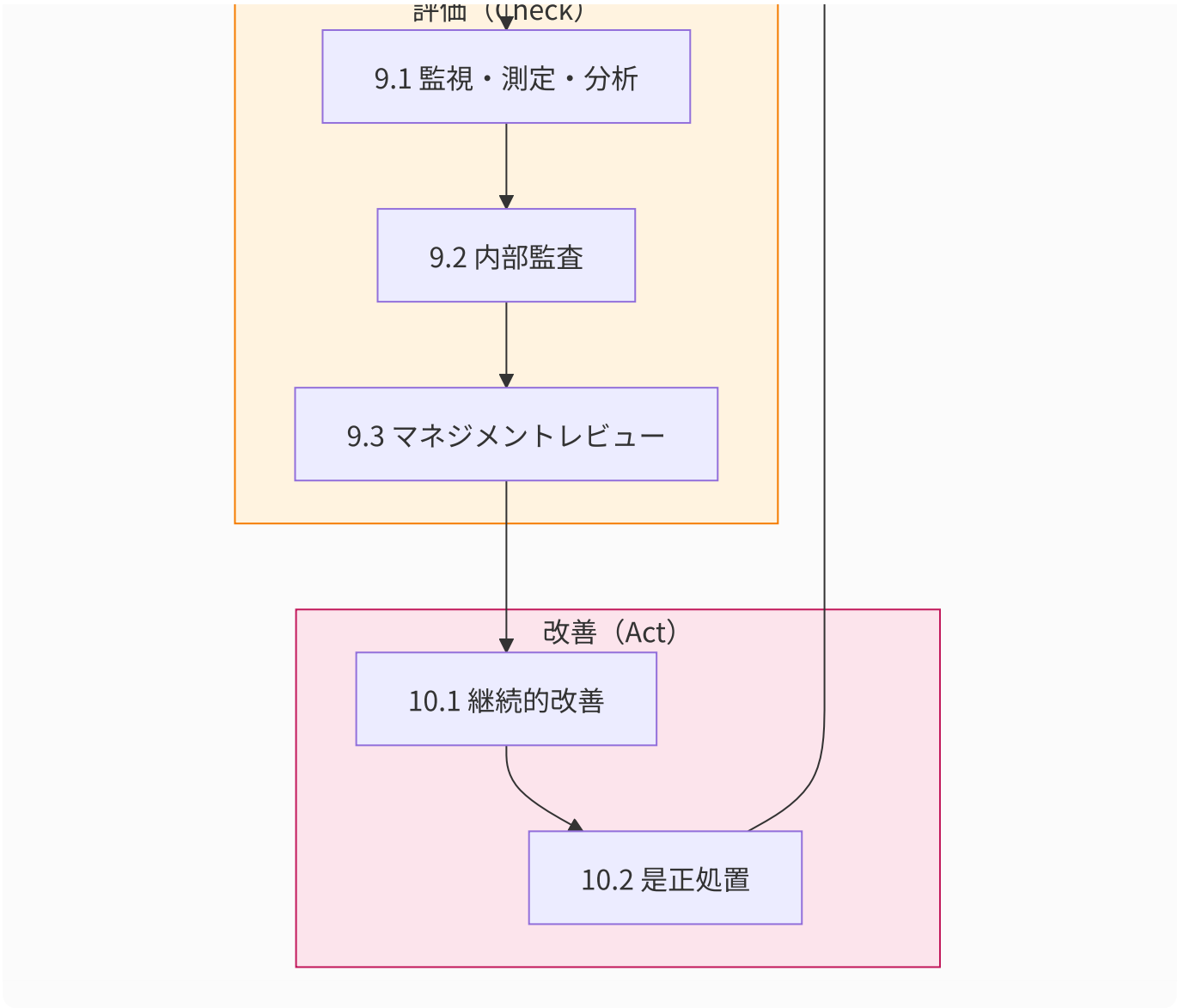
ISMSの主要プロセス

プロセス	概要	関連文書
リスクアセスメント	情報資産に対するリスクの特定・分析・評価	14. リスクアセスメント
リスク対応	特定されたリスクへの対応策の決定・実施	14. リスクアセスメント

プロセス	概要	関連文書
内部監査	ISMSの適合性・有効性の検証	9.2 内部監査
マネジメントレビュー	経営層によるISMSの見直し	9.3 マネジメントレビュー
是正処置	不適合の原因除去と再発防止	10.2 不適合及び是正処置
文書管理	ISMS文書の作成・承認・配布・改訂	7.5 文書化した情報

プロセスの相互作用


計画（Plan）
4.1 組織の状況理解
4.2 利害関係者の理解
4.3 適用範囲の決定
6.1 リスクアセスメント
6.2 目的の設定
実施（Do）
8.1 運用の計画・管理
8.2 リスクアセスメント実施
8.3 リスク対応実施



継続的改善

当社のISMSは、PDCAサイクルに基づき継続的に改善を行っている。

- **年次マネジメントレビュー**: 毎年8月に実施し、ISMSの有効性を評価
- **内部監査**: 年1回実施し、適合性を検証
- **是正処置**: 不適合発見時に原因分析と対策を実施

関連文書

- 4.1 組織及びその状況の理解
- 4.2 利害関係者のニーズ及び期待の理解
- 4.3 ISMSの適用範囲の決定

- 情報セキュリティ基本方針

5.1 リーダーシップ及びコミットメント

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
箇条番号	5.1
分類	リーダーシップ

要求事項

トップマネジメントは、次に示す事項によって、ISMSに関するリーダーシップ及びコミットメントを実証しなければならない。

- a) 情報セキュリティ方針及び情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする。
- b) 組織のプロセスへのISMS要求事項の統合を確実にする。
- c) ISMSに必要な資源が利用可能であることを確実にする。
- d) 有効な情報セキュリティマネジメント及びISMS要求事項への適合の重要性を伝達する。
- e) ISMSがその意図した成果を達成することを確実にする。
- f) ISMSの有効性に寄与するよう人々を指揮し、支援する。
- g) 継続的改善を促進する。
- h) その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する。

ⓘノート

この規格で「事業」という場合、それは、組織の存在の目的の中核となる活動という広義の意味で解釈され得る。

目的

トップマネジメントがISMSに対する明確なリーダーシップとコミットメントを示すことで、組織全体の情報セキュリティ意識を高め、ISMSの有効な運用を確保するため。

当社における実施状況

当社では、代表取締役（情報セキュリティ責任者）がトップマネジメントとして、以下の方法によりISMSへのリーダーシップ及びコミットメントを実証している。

a) 情報セキュリティ方針及び目的の確立

代表取締役は、情報セキュリティ基本方針を承認し、組織の戦略的方向性と整合した情報セキュリティ目的を設定している。方針は年1回見直しを行い、必要に応じて改訂する。

b) 組織プロセスへのISMS要求事項の統合

情報セキュリティ要求事項は、以下の業務プロセスに統合されている。

- システム開発プロセス：8. システム開発・保守
- 委託先管理プロセス：9. 委託先管理
- 人事プロセス：2. 人的対策
- SaaS導入プロセス：13. SaaS・シャドーIT管理

c) 資源の確保

代表取締役は、ISMSの確立・実施・維持・継続的改善に必要な以下の資源を確保している。

- 人的資源：情報セキュリティ委員会の設置、各役割への担当者の任命
- 技術的資源：セキュリティツール、クラウドサービスの導入・維持
- 財務的資源：情報セキュリティ関連の予算確保

d) 重要性の伝達

情報セキュリティの重要性は、以下の方法で組織内に伝達されている。

- 入社時の情報セキュリティ教育：2. 人的対策

- 年1回の情報セキュリティ研修
- Slack等を通じた適時の情報共有：1. 組織的対策

e) 意図した成果の達成

ISMSの意図した成果（情報資産の機密性・完全性・可用性の維持）の達成状況は、以下により確認している。

- 年1回の内部監査
- マネジメントレビュー（8月実施）
- インシデント発生状況のモニタリング

f) 人々の指揮・支援

代表取締役は、1. 組織的対策に定める組織体制を通じて、従業員がISMSの有効性に寄与できるよう指揮・支援している。

g) 継続的改善の促進

継続的改善は、以下のプロセスを通じて促進されている。

- 内部監査結果に基づく改善
- インシデント対応後の再発防止策
- マネジメントレビューでの改善指示

h) 管理層の役割支援

代表取締役は、CTOをはじめとする管理層が各責任領域においてリーダーシップを発揮できるよう、権限委譲と支援を行っている。詳細は1. 組織的対策を参照。

証跡

証跡	内容	保管場所
情報セキュリティ基本方針	代表取締役承認済みの方針文書	ISMS文書管理システム
マネジメントレビュー議事録	年1回のレビュー記録	Google Drive
内部監査報告書	監査結果と改善指示	Google Drive

証跡	内容	保管場所
教育実施記録	研修参加記録、Slackリアクション	カレンダー、Slack

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
- 14. リスクアセスメント

5.2 方針

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2026.03.04
適用範囲	全社
箇条番号	5.2
分類	リーダーシップ

要求事項

トップマネジメントは、次の事項を満たす情報セキュリティ方針を確立しなければならない。

- a) 組織の目的に対して適切である。
- b) 情報セキュリティ目的（6.2 参照）を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。
- c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。
- d) ISMSの継続的改善へのコミットメントを含む。

情報セキュリティ方針は、次に示す事項を満たさなければならない。

- e) 文書化した情報として利用可能である。
- f) 組織内に伝達する。
- g) 必要に応じて、利害関係者が入手可能である。

目的

組織の情報セキュリティに対する基本的な方向性と経営層のコミットメントを明確にし、全従業員及び関係者に周知するため。

当社における実施状況

当社では、代表取締役（情報セキュリティ責任者）が情報セキュリティ基本方針を確立し、以下のとおり要求事項を満たしている。

a) 組織の目的に対する適切性

情報セキュリティ基本方針は、当社の語学教育事業部における情報資産（顧客情報、学習データ等）の保護を目的として策定されており、組織の事業目的と整合している。

当社の事業内容については4.1 組織及びその状況の理解を参照。

b) 情報セキュリティ目的の枠組み

情報セキュリティ基本方針には、以下の目的設定の枠組みが含まれている。

- 情報資産の機密性、完全性、可用性の維持
- 法令遵守（個人情報保護法、不正アクセス禁止法等）
- 継続的改善

具体的な情報セキュリティ目的は、14. リスクアセスメントに基づき設定される。

c) 適用される要求事項を満たすことへのコミットメント

情報セキュリティ基本方針には、以下の要求事項を満たすことへのコミットメントが含まれている。

- 個人情報保護法
- 不正アクセス禁止法
- 電子署名法
- サイバーセキュリティ基本法
- 顧客との契約上の義務

利害関係者の要求事項については4.2 利害関係者のニーズ及び期待の理解を参照。

d) 継続的改善へのコミットメント

情報セキュリティ基本方針には、ISMSの継続的改善へのコミットメントが明記されている。改善活動は以下のプロセスを通じて実施される。

- 年1回の内部監査
- マネジメントレビュー
- インシデント対応後の是正処置

e) 文書化した情報としての利用可能性

情報セキュリティ基本方針は、以下の形式で文書化され、利用可能な状態にある。

文書名	保管場所	形式
情報セキュリティ基本方針	ISMS文書管理システム	Markdown
情報セキュリティ基本方針（PDF）	Google Drive	PDF

f) 組織内への伝達

情報セキュリティ方針は、以下の方法で組織内に伝達されている。

- 入社時の情報セキュリティ教育での説明
- ISMS文書管理システムでの常時閲覧可能
- 年1回の情報セキュリティ研修での再確認
- 方針改訂時のSlack通知

教育・伝達の詳細は2. 人的対策を参照。

g) 利害関係者への入手可能性

必要に応じて、以下の利害関係者に情報セキュリティ方針を提供している。

- 顧客（官公庁・教育委員会）：セキュリティチェックシート等の回答時
- 委託先：契約締結時
- 監査機関：ISO 27001認証審査時

方針の見直し

情報セキュリティ基本方針は、以下の契機で見直しを行う。

- 年1回の定期見直し（マネジメントレビュー時）
- 重大なセキュリティインシデント発生時

- 法令・規制の重大な変更時
- 事業環境の大幅な変化時

証跡

証跡	内容	保管場所
情報セキュリティ基本方針	承認済み方針文書	ISMS文書管理システム
方針改訂履歴	改訂日、改訂内容	Git履歴
教育実施記録	方針説明の実施記録	カレンダー、Slack
マネジメントレビュー議事録	方針見直しの記録	Google Drive

関連文書

- 情報セキュリティ基本方針
- 4.1 組織及びその状況の理解
- 4.2 利害関係者のニーズ及び期待の理解
- 2. 人的対策
- 14. リスクアセスメント

5.3 組織の役割、責任及び権限

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
箇条番号	5.3
分類	リーダーシップ

要求事項

トップマネジメントは、情報セキュリティに関連する役割に対して、責任及び権限が割り当てられ、組織内に伝達されることを確実にしなければならない。

トップマネジメントは、次の事項に対して、責任及び権限を割り当てなければならない。

- a) ISMSが、この規格の要求事項に適合することを確実にする。
- b) ISMSのパフォーマンスをトップマネジメントに報告する。

ⓘノート

トップマネジメントは、ISMSのパフォーマンスを組織内に報告する責任及び権限を割り当てることも可能である。

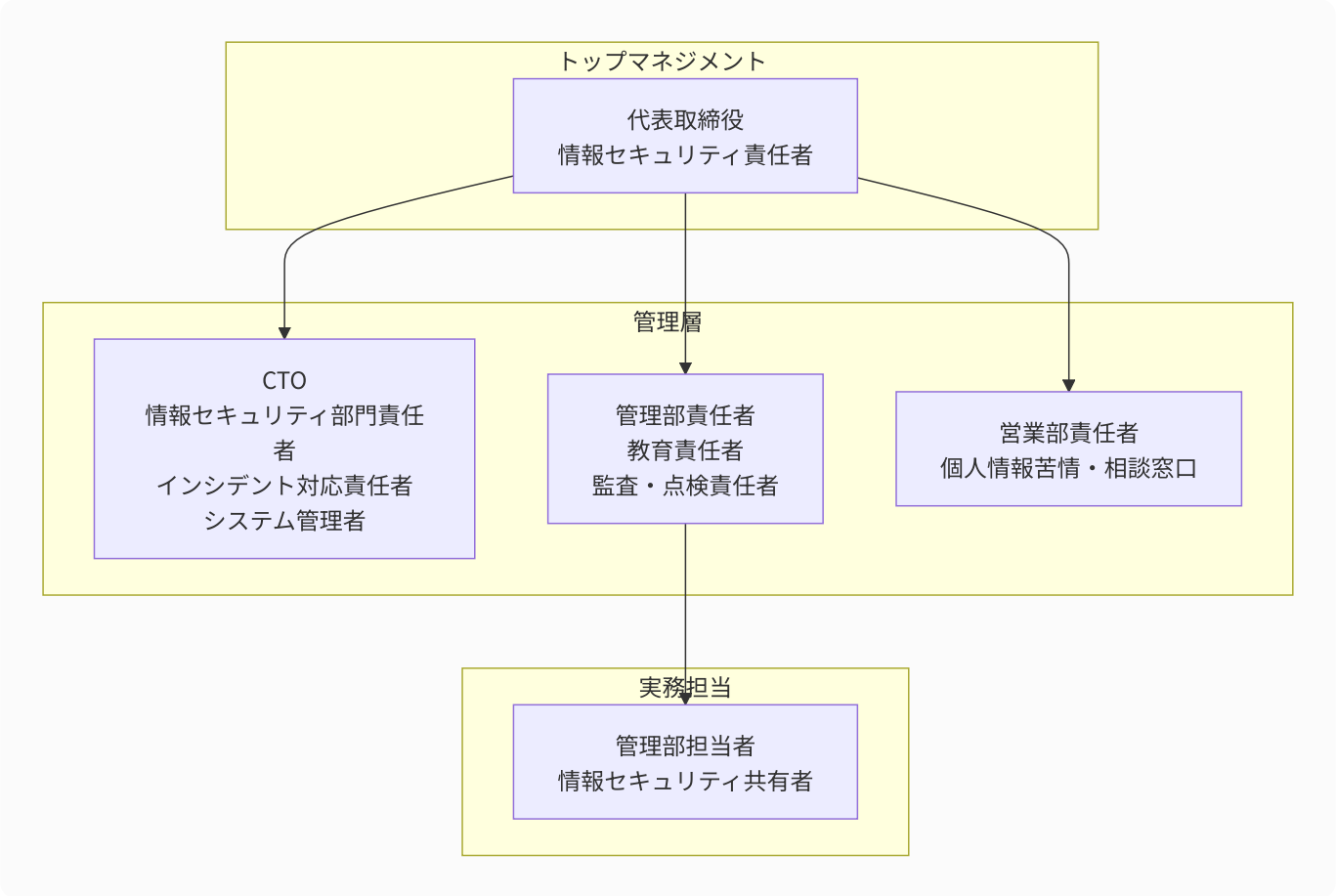
目的

情報セキュリティに関する役割、責任及び権限を明確にし、組織全体でISMSを効果的に運用するため。

当社における実施状況

当社では、1. 組織的対策において、情報セキュリティに関連する役割、責任及び権限を定義し、組織内に伝達している。

情報セキュリティ組織体制



役割と責任の定義

役職名	役割・責任	担当者
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

役職名	役割・責任	担当者
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
個人情報苦情・相談窓口	個人情報に関する苦情・相談の一次対応および社内連携	営業部責任者
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）
情報セキュリティ共有者	情報セキュリティに関する適時の情報共有	管理部担当者
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）

詳細は1. 組織的対策を参照。

a) ISMSの規格適合の確保

ISMSがJIS Q 27001:2023の要求事項に適合することを確実にする責任は、以下のとおり割り当てられている。

責任	担当者	具体的な活動
全体統括	情報セキュリティ責任者（代表取締役）	方針承認、資源配分、最終意思決定
運用管理	情報セキュリティ部門責任者（CTO）	技術的対策の実施、日常運用の監督
監査・点検	監査・点検責任者（管理部責任者）	年1回の内部監査、規程遵守状況の確認

b) ISMSパフォーマンスの報告

ISMSのパフォーマンスをトップマネジメントに報告する責任は、以下のとおり割り当てられている。

報告内容	報告者	報告先	頻度
内部監査結果	監査・点検責任者	情報セキュリティ責任者	年1回（8月）
インシデント対応状況	インシデント対応責任者	情報セキュリティ責任者	発生時、および年1回

報告内容	報告者	報告先	頻度
リスクアセスメント結果	情報セキュリティ委員会	情報セキュリティ責任者	年1回
教育実施状況	教育責任者	情報セキュリティ責任者	年1回

マネジメントレビューは年1回（8月）に実施し、内部監査と同日に行う。詳細は1. 組織的対策を参照。

組織内への伝達

役割、責任及び権限は、以下の方法で組織内に伝達されている。

- 1. 組織的対策での文書化
- ISMS文書管理システムでの公開
- 入社時の情報セキュリティ教育での説明
- 役割変更時の個別通知

少人数体制における運用

当社は少人数体制のため、一部の役割は兼務となっている。兼務による利益相反を防ぐため、以下の点に留意している。

- 内部監査は、運用当事者以外の者が担当（独立性の確保）
- 重大な意思決定は代表取締役が最終判断
- インシデント対応は迅速性を重視しCTOが担当、経営判断を要する場合は代表取締役が判断

証跡

証跡	内容	保管場所
組織的対策規程	役割・責任の定義	ISMS文書管理システム
組織図	組織体制の図示	ISMS文書管理システム
任命記録	各役割への任命	人事記録
マネジメントレビュー議事録	パフォーマンス報告の記録	Google Drive

関連文書

- 1. 組織的対策
- 4.1 組織及びその状況の理解
- 10. インシデント対応・事業継続
- 14. リスクアセスメント

6.1 リスク及び機会に対処する活動

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
箇条番号	6.1
分類	計画策定

要求事項

6.1.1 一般

ISMSの計画を策定するとき、組織は、4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し、次の事項のために対処する必要があるリスク及び機会を決定しなければならない。

- a) ISMSが、その意図した成果を達成できることを確実にする。
- b) 望ましくない影響を防止又は低減する。
- c) 継続的改善を達成する。

組織は、次の事項を計画しなければならない。

- d) 上記によって決定したリスク及び機会に対処する活動
- e) 次を行う方法
    - 1. その活動のISMSプロセスへの統合及び実施
    - 2. その活動の有効性の評価

6.1.2 情報セキュリティリスクアセスメント

組織は、次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め、適用しなければならない。

- a) 次を含む情報セキュリティのリスク基準を確立し、維持する。

    - 1. リスク受容基準
    - 2. 情報セキュリティリスクアセスメントを実施するための基準
- b) 繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にする。
- c) 次によって情報セキュリティリスクを特定する。
    - 1. ISMSの適用範囲内における情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために、情報セキュリティリスクアセスメントのプロセスを適用する。
    - 2. これらのリスク所有者を特定する。
- d) 次によって情報セキュリティリスクを分析する。
    - 1. 6.1.2 c) 1) で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。
    - 2. 6.1.2 c) 1) で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。
    - 3. リスクレベルを決定する。
- e) 次によって情報セキュリティリスクを評価する。
    - 1. リスク分析の結果と 6.1.2 a) で確立したリスク基準とを比較する。
    - 2. リスク対応のために、分析したリスクの優先順位付けを行う。

組織は、情報セキュリティリスクアセスメントのプロセスについての文書化した情報を保持しなければならない。

6.1.3 情報セキュリティリスク対応

組織は、次の事項を行うために、情報セキュリティリスク対応のプロセスを定め、適用しなければならない。

- a) リスクアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。
- b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。
- c) 6.1.3 b) で決定した管理策を附属書Aに示す管理策と比較し、必要な管理策が見落とされていないことを検証する。
- d) 次を含む適用宣言書を作成する。
    - 必要な管理策（6.1.3 の b) 及び c) 参照）

    - それらの管理策を含めた理由
    - それらの必要な管理策を実施しているか否か
    - 附属書Aに規定する管理策を除外した理由
- e) 情報セキュリティリスク対応計画を策定する。
- f) 情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について、リスク所有者の承認を得る。

組織は、情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。

ⓘノート

この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは、JIS Q 31000 に規定する原則及び一般的な指針と整合している。

目的

組織の状況（4.1）及び利害関係者の要求事項（4.2）を踏まえ、ISMSの意図した成果を達成するために対処すべきリスク及び機会を特定し、適切なリスクアセスメント及びリスク対応を実施するため。

当社における実施状況

6.1.1 一般：リスク及び機会の決定

当社では、4.1 組織及びその状況の理解 で特定した外部・内部の課題、及び 4.2 利害関係者のニーズ及び期待の理解 で特定した要求事項を踏まえ、以下のリスク及び機会を決定している。

主なリスク：

- クラウドサービスの設定不備による情報漏えい
- 不正アクセスによる顧客情報・個人情報の流出
- 従業員の誤操作・内部不正による情報漏えい
- サービス停止による事業継続への影響
- 法令・規制要件への不適合

主な機会：

- クラウドサービスの活用による柔軟なセキュリティ対策の実現
- 少人数体制に適した効率的なISMS運用
- 継続的改善による顧客信頼の獲得

これらのリスク及び機会に対処する活動は、年1回のマネジメントレビュー（8月）において有効性を評価し、必要に応じて改善を行う。

6.1.2 情報セキュリティリスクアセスメント

当社のリスクアセスメントプロセスは、「14. 情報セキュリティリスクアセスメント」に定めている。

リスク基準：

項目	基準
リスク受容基準	リスク値2以下（低）は受容可能
影響度	3段階（1:限定的、2:事業支障、3:重大影響）
発生可能性	3段階（1:低、2:中、3:高）
リスクレベル	影響度 × 発生可能性（高:6-9、中:3-4、低:1-2）

リスク所有者：

各情報資産のリスク所有者は、情報資産台帳において明確化している。重要な情報資産については、情報セキュリティ責任者（代表取締役）が最終的なリスク所有者となる。

実施頻度：

- 定期実施：年1回（8月のマネジメントレビュー前）
- 臨時実施：新たな重要情報資産の追加、大規模なシステム構成変更、インシデント発生時等

6.1.3 情報セキュリティリスク対応

リスク対応の選択肢：

対応方針	説明
低減	管理策を適用してリスクを許容可能なレベルまで低減
受容	リスクが許容範囲内であり、追加対策を行わない
回避	リスク源となる活動を中止または変更
移転	保険加入や外部委託によりリスクを移転

リスク対応計画：

「高」と判定されたリスクについては、リスク対応計画をYouTrackのチケットとして管理し、実施期限・担当者を明確化している。

リスク所有者の承認：

リスクアセスメント結果及びリスク対応計画は、情報セキュリティ責任者（代表取締役）が承認する。

関連文書

- 4.1 組織及びその状況の理解
- 4.2 利害関係者のニーズ及び期待の理解
- 14. 情報セキュリティリスクアセスメント
- 1. 組織的対策
- 10. インシデント対応及び事業継続管理

6.2 情報セキュリティ目的及びそれを達成するための計画策定

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
箇条番号	6.2
分類	計画策定

要求事項

組織は、関連する機能及び階層において、情報セキュリティ目的を確立しなければならない。

情報セキュリティ目的は、次の事項を満たさなければならない。

- a) 情報セキュリティ方針と整合している。
- b) （実行可能な場合）測定可能である。
- c) 適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。
- d) これを監視する。
- e) これを伝達する。
- f) 必要に応じて、更新する。
- g) 文書化した情報として利用可能な状態にする。

組織は、情報セキュリティ目的に関する文書化した情報を保持しなければならない。

組織は、情報セキュリティ目的をどのように達成するかについて計画するとき、次の事項を決定しなければならない。

- h) 実施事項
- i) 必要な資源

- j) 責任者
- k) 達成期限
- l) 結果の評価方法

目的

情報セキュリティ方針と整合した具体的な目的を設定し、その達成に向けた計画を策定することで、ISMSの有効性を確保し、継続的改善を推進するため。

当社における実施状況

情報セキュリティ目的

当社は、「情報セキュリティ基本方針」と整合した以下の情報セキュリティ目的を設定している。

目的	測定指標	目標値	責任者
情報セキュリティインシデントの防止	重大インシデント（レベル2以上）の発生件数	0件/年	CTO
情報セキュリティ教育の徹底	教育受講率	100%	管理部責任者
アクセス権限の適正管理	退職者アカウントの即時無効化率	100%	CTO
リスクアセスメントの実施	年次リスクアセスメント実施	1回/年	情報セキュリティ責任者
法令・規制要件の遵守	法令違反・指摘事項	0件/年	情報セキュリティ責任者

達成計画

各情報セキュリティ目的について、以下の計画を策定している。

情報セキュリティインシデントの防止

項目	内容
実施事項	技術的管理策の維持・改善、脅威情報の収集・共有、インシデント対応訓練
必要な資源	クラウドサービスのセキュリティ機能、監視ツール
責任者	CTO
達成期限	通年（年度末に評価）
評価方法	インシデント記録の集計、マネジメントレビューでの報告

情報セキュリティ教育の徹底

項目	内容
実施事項	入社時教育、年次教育、随時の注意喚起
必要な資源	教育資料、Slack等のコミュニケーションツール
責任者	管理部責任者（または代表取締役）
達成期限	入社時：入社後1週間以内、年次：8月
評価方法	教育実施記録（Slack反応等）の確認

アクセス権限の適正管理

項目	内容
実施事項	入退社時のアカウント管理、イベント駆動型の権限見直し
必要な資源	Microsoft Entra ID、Google Workspace管理コンソール
責任者	CTO
達成期限	退職時：退職日当日、権限変更：役割変更時
評価方法	アカウント管理記録の確認

リスクアセスメントの実施

項目	内容
実施事項	年次リスクアセスメント、臨時アセスメント（必要時）
必要な資源	情報資産台帳、リスクアセスメント手順書
責任者	情報セキュリティ責任者（代表取締役）

項目	内容
達成期限	8月（マネジメントレビュー前）
評価方法	リスクアセスメント報告書の作成・承認

法令・規制要件の遵守

項目	内容
実施事項	法令動向の監視、契約要件の確認、内部監査
必要な資源	法令情報源、契約管理システム
責任者	情報セキュリティ責任者（代表取締役）
達成期限	通年
評価方法	内部監査結果、外部からの指摘有無

監視・伝達・更新

監視： 情報セキュリティ目的の達成状況は、年1回のマネジメントレビュー（8月）において確認する。

伝達： 情報セキュリティ目的は、本文書及び情報セキュリティ基本方針を通じて全従業員に伝達する。

更新： 情報セキュリティ目的は、マネジメントレビューの結果、事業環境の変化、リスクアセスメント結果等を踏まえ、必要に応じて更新する。

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
- 4. アクセス制御及び認証
- 14. 情報セキュリティリスクアセスメント
- 10. インシデント対応及び事業継続管理

6.3 変更の計画策定

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
箇条番号	6.3
分類	計画策定

要求事項

組織がISMSの変更の必要があると決定したとき、その変更は、計画的な方法で行わなければならない。

目的

ISMSの変更が必要な場合に、その変更を計画的かつ体系的に実施することで、ISMSの完全性を維持し、意図しない悪影響を防止するため。

実施の手引き

ISMSの変更には、以下のようなものが含まれる。

- 情報セキュリティ方針の改訂
- 情報セキュリティ目的の変更
- 組織構造の変更
- 情報セキュリティ関連規程の改訂
- 管理策の追加・変更・削除
- リスクアセスメント手法の変更
- 適用範囲の変更

変更を計画する際には、以下の事項を考慮する。

- 変更の目的及び潜在的な結果
- ISMSの完全性への影響
- 資源の利用可能性
- 責任及び権限の割当て又は再割当て

当社における実施状況

変更管理の原則

当社では、ISMSの変更を以下の原則に基づき計画的に実施する。

原則	内容
計画性	変更の目的、内容、影響範囲を事前に明確化する
承認	変更は情報セキュリティ責任者の承認を得て実施する
文書化	変更内容及び理由を文書化し、履歴を管理する
伝達	変更内容を関係者に適切に伝達する

変更の契機

ISMSの変更は、以下の契機で検討・実施する。

- マネジメントレビューの結果
- 内部監査の指摘事項
- 情報セキュリティインシデントからの教訓
- 法令・規制要件の変更
- 事業環境・組織構造の変化
- リスクアセスメント結果の変化
- 利害関係者からの要求事項の変化

変更管理プロセス

軽微な変更

規程の軽微な修正（誤字脱字、参照先の更新等）については、情報セキュリティ責任者の確認のもと、随時実施する。

重要な変更

以下の重要な変更については、計画的なプロセスに従って実施する。

ステップ	内容	責任者
1. 変更の提案	変更の必要性、目的、内容を明確化	提案者
2. 影響評価	ISMSへの影響、リスク、必要な資源を評価	情報セキュリティ委員会
3. 承認	変更計画の承認	情報セキュリティ責任者
4. 実施	変更の実施、文書の更新	担当者
5. 伝達	関係者への変更内容の伝達	情報セキュリティ委員会
6. 有効性確認	変更後の有効性を確認	情報セキュリティ責任者

文書管理

ISMSに関する文書の変更は、以下の方法で管理する。

- **版管理：** 文書のバージョン番号及び改訂日を明記
- **変更履歴：** 主要な変更内容を記録
- **承認記録：** 承認者及び承認日を記録
- **保管：** ISMS文書管理システム（本サイト）にて一元管理

変更の記録

重要な変更については、以下の情報を記録する。

- 変更日
- 変更内容
- 変更理由
- 承認者
- 影響を受ける文書・プロセス

定期的な見直し

ISMSの変更管理プロセス自体も、年1回のマネジメントレビュー（8月）において有効性を確認し、必要に応じて改善する。

関連文書

- 1. 組織的対策
- 情報セキュリティ基本方針
- 14. 情報セキュリティリスクアセスメント
- 8. システム開発及び保守

7.1 資源

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
箇条番号	7.1
分類	支援

要求事項

組織は、ISMSの確立、実施、維持及び継続的改善に必要な資源を決定し、提供しなければならない。

目的

ISMSを効果的に運用するために必要な人的資源、技術的資源、財務的資源を適切に確保し、情報セキュリティ目的の達成を支援するため。

当社における実施状況

当社では、代表取締役（情報セキュリティ責任者）の承認のもと、ISMSの運用に必要な資源を以下のとおり決定し、提供している。

人的資源

ISMSの運用に必要な役割と責任を明確にし、適切な人員を配置している。

役割	担当者	主な責務
情報セキュリティ責任者	代表取締役	ISMS全体の最終責任、方針承認
情報セキュリティ部門責任者	CTO	技術的対策の運用管理

役割	担当者	主な責務
システム管理者	CTO（兼務）	情報システムのセキュリティ対策
インシデント対応責任者	CTO	インシデント発生時の対応指揮
教育責任者	管理部責任者	セキュリティ教育の企画・実施
監査・点検責任者	管理部責任者	内部監査の実施

詳細は1. 組織的対策を参照。

技術的資源

情報セキュリティ対策に必要な技術的資源を確保している。

- **認証基盤**: Microsoft Entra ID、Google Workspace
- **クラウドインフラ**: AWS、Google Cloud Platform
- **セキュリティツール**: ウイルス対策ソフト、ファイアウォール、ログ管理
- **コミュニケーション**: Slack（情報共有・インシデント報告）
- **文書管理**: ISMS文書管理システム、Google Drive

技術的インフラの詳細はネットワーク構成図を参照。

財務的資源

代表取締役は、以下の情報セキュリティ関連費用について予算を確保している。

- クラウドサービス利用料（AWS、GCP、Google Workspace等）
- セキュリティツール・ソフトウェアライセンス
- 外部セミナー・研修費用
- 外部監査・認証維持費用

資源の見直し

資源の充足状況は、以下の機会に見直しを行う。

- 年1回のマネジメントレビュー（8月実施）
- 重大なインシデント発生時
- 組織体制の変更時

- 新規事業・サービス開始時

証跡

証跡	内容	保管場所
組織図	情報セキュリティ体制図	ISMS文書管理システム
マネジメントレビュー議事録	資源の充足状況確認記録	Google Drive
予算計画書	情報セキュリティ関連予算	社内管理システム

関連文書

- 1. 組織的対策
- 5.1 リーダーシップ及びコミットメント
- ネットワーク構成図

7.2 力量

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
箇条番号	7.2
分類	支援

要求事項

組織は、次の事項を行わなければならない。

- a) 組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。
- b) 適切な教育、訓練又は経験に基づいて、それらの人々が力量を備えていることを確実にする。
- c) 該当する場合には、必ず、必要な力量を身に付けるための処置を講じ、講じた処置の有効性を評価する。
- d) 力量の証拠として、適切な文書化した情報を保持する。

ⓘノート

適用される処置には、例えば、現在雇用している人々に対する、教育訓練の提供、指導の実施、配置転換の実施などがあり、また、力量を備えた人々の雇用、そうした人々との契約締結なども含まれ得る。

目的

ISMSの運用に関わる人々が必要な力量を備えていることを確実にし、情報セキュリティパフォーマンスの維持・向上を図るため。

当社における実施状況

a) 必要な力量の決定

当社では、情報セキュリティパフォーマンスに影響を与える役割ごとに、必要な力量を以下のとおり定めている。

役割	必要な力量
情報セキュリティ責任者	経営判断能力、情報セキュリティマネジメントの理解、法令・規制の知識
システム管理者	システム設計・運用スキル、セキュリティ技術の知識、インシデント対応能力
インシデント対応責任者	技術的判断能力、リスク評価能力、コミュニケーション能力
教育責任者	教育企画・実施能力、情報セキュリティの基礎知識
一般従業員	情報セキュリティの基礎知識、社内規程の理解、インシデント報告の理解

b) 力量の確保

従業員の力量は、以下の方法により確保している。

採用時の確認

- 職務経歴書・履歴書による経験・スキルの確認
- 面接による適性評価
- 必要に応じた技術試験の実施

継続的な教育・訓練

教育責任者は、2. 人的対策に基づき、以下の教育を実施している。

- **入社時教育**: 情報セキュリティ関連規程の説明、基本的なセキュリティ意識の醸成
- **年次教育**: 年1回の情報セキュリティ研修（全従業員対象）
- **適時教育**: 新たな脅威や注意喚起が必要な事項の共有（Slack等で実施）

c) 力量向上のための処置

必要な力量が不足している場合、以下の処置を講じる。

処置	内容	有効性評価
社内研修	情報セキュリティ教育の実施	理解度確認、Slackリアクション
外部セミナー	専門知識の習得	受講報告、業務への適用状況
OJT	実務を通じた指導	業務遂行状況の確認

詳細は2. 人的対策 5. 人材育成を参照。

d) 力量の証拠

力量の証拠として、以下の文書化した情報を保持している。

証跡	内容	保管場所
採用記録	職務経歴書、面接記録	人事管理システム
教育実施記録	研修参加記録、カレンダー招待	カレンダー、Slack
理解確認記録	Slackでの「理解しました」リアクション	Slack

証跡

証跡	内容	保管場所
役割・力量定義書	各役割に必要な力量の定義	ISMS文書管理システム
教育計画	年間教育計画	Google Drive
教育実施記録	研修参加記録	カレンダー、Slack
人事記録	採用・異動・退職記録	人事管理システム

関連文書

- 2. 人的対策
- 1. 組織的対策
- 7.3 認識

7.3 認識

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
箇条番号	7.3
分類	支援

要求事項

組織の管理下で働く人々は、次の事項に関して認識をもたなければならない。

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

目的

組織の管理下で働くすべての人々が、情報セキュリティの重要性を理解し、自らの役割と責任を認識することで、ISMSの有効な運用を支援するため。

当社における実施状況

当社では、全従業員が情報セキュリティに関する認識を持つよう、以下の取り組みを実施している。

a) 情報セキュリティ方針の認識

従業員は、情報セキュリティ基本方針について、以下の機会に認識を深めている。

機会	内容	頻度
入社時教育	情報セキュリティ基本方針の説明と理解確認	入社時
年次研修	方針の再確認と最新情報の共有	年1回
方針改訂時	改訂内容の周知と理解確認	改訂時

情報セキュリティ基本方針は、ISMS文書管理システムにて常時閲覧可能な状態としている。

b) ISMSの有効性に対する自らの貢献

従業員は、以下の点について認識を持つよう教育を受けている。

情報セキュリティパフォーマンス向上の便益

- 顧客・取引先からの信頼獲得
- 情報漏えい・インシデントによる損害の防止
- 法令遵守による罰則・制裁の回避
- 業務の継続性確保

自らの貢献

- 日常業務における情報セキュリティ規程の遵守
- 不審な事象の早期発見と報告
- セキュリティ意識の維持・向上
- 同僚への注意喚起と相互支援

詳細は2. 人的対策 2. 従業員の責務を参照。

c) ISMS要求事項に適合しないことの意味

従業員は、ISMS要求事項に適合しない場合の影響について、以下のとおり認識している。

影響範囲	具体的な影響
組織への影響	情報漏えい、システム障害、顧客・取引先からの信頼喪失、法的責任
個人への影響	就業規則に基づく懲戒処分の対象となる可能性
社会への影響	個人情報の漏えいによる被害者の発生、社会的信用の失墜

違反時の懲戒については、就業規則に準じる。詳細は2. 人的対策を参照。

認識向上のための取り組み

教育責任者は、従業員の認識向上のため、以下の取り組みを実施している。

取り組み	内容	実施方法
定期教育	情報セキュリティ研修	年1回の集合研修またはオンライン研修
適時共有	新たな脅威・注意喚起	Slack等での情報共有
インシデント共有	発生事例と教訓の共有	社内ミーティング、Slack
外部情報活用	IPA、JPCERT/CC等からの情報	1. 組織的対策に基づく共有

認識の確認

従業員の認識状況は、以下の方法で確認している。

- 教育実施後のSlackリアクション（「理解しました」等）
- 年次研修での理解度確認
- 日常業務における規程遵守状況の観察

証跡

証跡	内容	保管場所
教育実施記録	研修参加記録、カレンダー招待	カレンダー、Slack
理解確認記録	Slackでの「理解しました」リアクション	Slack
情報共有記録	脅威情報等の共有記録	Slack
秘密保持契約	入社時の契約書	人事管理システム

関連文書

- 情報セキュリティ基本方針
- 2. 人的対策
- 1. 組織的対策
- 7.2 力量

7.4 コミュニケーション

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
箇条番号	7.4
分類	支援

要求事項

組織は、次の事項を含む、ISMSに関連する内部及び外部のコミュニケーションを実施する必要性を決定しなければならない。

- a) コミュニケーションの内容
- b) コミュニケーションの実施時期
- c) コミュニケーションの対象者
- d) コミュニケーションの方法

目的

ISMSに関連する情報を、適切な内容・時期・対象者・方法で伝達することにより、組織内外の関係者との効果的なコミュニケーションを確保するため。

当社における実施状況

当社では、ISMSに関連するコミュニケーションを以下のとおり実施している。

内部コミュニケーション

定常的なコミュニケーション

内容	時期	対象者	方法
情報セキュリティ方針	入社時、年1回、改訂時	全従業員	研修、ISMS文書管理システム
情報セキュリティ関連規程	入社時、改訂時	全従業員	研修、ISMS文書管理システム
セキュリティ教育	入社時、年1回	全従業員	集合研修、オンライン研修
脅威・脆弱性情報	適時	全従業員	Slack
マネジメントレビュー結果	年1回（8月）	経営層、関係者	会議、議事録
内部監査結果	年1回（8月）	経営層、関係者	監査報告書

インシデント発生時のコミュニケーション

内容	時期	対象者	方法
インシデント発生報告	発見時即時	インシデント対応責任者	Slack、電話
対応状況の共有	対応中随時	関係者	Slack、会議
再発防止策の周知	対応完了後	全従業員	Slack、研修

詳細は10. インシデント対応・事業継続管理を参照。

外部コミュニケーション

利害関係者とのコミュニケーション

内容	時期	対象者	方法
情報セキュリティ方針	要求時	顧客、取引先	文書提供、Webサイト
セキュリティ対策状況	契約時、要求時	顧客、取引先	セキュリティチェックシート
インシデント報告	発生時	影響を受ける顧客、監督官庁	書面、電話
個人情報に関する問い合わせ	随時	本人、監督官庁	問い合わせ窓口

利害関係者の詳細は4.2 利害関係者のニーズ及び期待の理解を参照。

専門機関からの情報収集

情報セキュリティ共有者は、以下の専門機関から脅威・脆弱性情報を収集し、社内に共有している。

- IPA（独立行政法人情報処理推進機構）
- JPCERT/CC
- JVN（Japan Vulnerability Notes）
- 個人情報保護委員会

詳細は1. 組織的対策 3. 情報セキュリティに関する情報共有を参照。

コミュニケーション手段

当社では、以下のコミュニケーション手段を用途に応じて使い分けている。

手段	用途	特徴
Slack	日常的な情報共有、インシデント報告、脅威情報共有	即時性、記録性
メール	外部との正式なコミュニケーション	正式性、証跡性
会議	重要事項の協議、マネジメントレビュー	双方向性、意思決定
ISMS文書管理システム	規程・方針の公開	常時閲覧可能、版管理
Google Drive	文書の共有・保管	アクセス制御、共同編集

コミュニケーションの記録

コミュニケーションの証跡は、以下のとおり保管している。

コミュニケーション	証跡	保管場所
教育・研修	カレンダー招待、Slackリアクション	カレンダー、Slack
脅威情報共有	Slack投稿記録	Slack

コミュニケーション	証跡	保管場所
マネジメントレビュー	議事録	Google Drive
インシデント対応	YouTrackチケット、Slack記録	YouTrack、Slack
外部報告	報告書、メール	Google Drive、メール

証跡

証跡	内容	保管場所
コミュニケーション計画	年間の教育・情報共有計画	Google Drive
情報共有記録	Slack投稿記録	Slack
会議議事録	マネジメントレビュー等の記録	Google Drive
外部コミュニケーション記録	顧客・取引先との連絡記録	Google Drive、メール

関連文書

- 1. 組織的対策
- 2. 人的対策
- 10. インシデント対応・事業継続管理
- 4.2 利害関係者のニーズ及び期待の理解

7.5 文書化した情報

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2026.03.04
適用範囲	全社
箇条番号	7.5
分類	支援

7.5.1 一般

要求事項

組織のISMSは、次の事項を含まなければならない。

- a) この規格が要求する文書化した情報
- b) ISMSの有効性のために必要であると組織が決定した、文書化した情報

ⓘノート

ISMSのための文書化した情報の程度は、次のような理由によって、それぞれの組織で異なる場合がある。

1. 組織の規模、並びに活動、プロセス、製品及びサービスの種類
2. プロセス及びその相互作用の複雑さ
3. 人々の力量

当社における実施状況

当社のISMSは、以下の文書化した情報を含んでいる。

文書体系

当社のISMS文書は、以下の3つの主要文書で構成される。

文書名	内容	対応ディレクトリ
ISMSマニュアル	JIS Q 27001:2025の箇条4〜10に対応する要求事項への対応方針を記述	clauses/
運用規定	ISMSマニュアルの方針に基づく具体的な運用ルール・手順を記述	policies/
適用宣言書	ISO/IEC 27001:2022 附属書Aの93管理策の適用・非適用と実施状況を記述	annexa/

※ 運用規定は、組織内で「情報セキュリティマネジメントシステム（ISMS）文書集」とも称される場合がある。

a) JIS Q 27001:2023が要求する文書化した情報

箇条	文書化した情報	当社の対応文書	文書体系
4.3	ISMSの適用範囲	4.3 ISMSの適用範囲の決定	ISMSマニュアル
5.2	情報セキュリティ方針	情報セキュリティ基本方針	ISMSマニュアル
6.1.2	情報セキュリティリスクアセスメントプロセス	14. 情報セキュリティリスクアセスメント	運用規定
6.1.3	情報セキュリティリスク対応プロセス	14. 情報セキュリティリスクアセスメント	運用規定
6.1.3 d)	適用宣言書	適用宣言書	適用宣言書
6.2	情報セキュリティ目的	6.2 情報セキュリティ目的及びそれを達成するための計画策定	ISMSマニュアル
7.2	力量の証拠	教育実施記録	記録・帳票
8.1	運用計画及び管理の証拠	運用規定（各種規程）	運用規定
8.2	リスクアセスメント結果	14. 情報セキュリティリスクアセスメント	運用規定
8.3	リスク対応計画	14. 情報セキュリティリスクアセスメント	運用規定

箇条	文書化した情報	当社の対応文書	文書体系
9.1	監視及び測定の結果	内部監査報告書、マネジメントレビュー議事録	記録・帳票
9.2	内部監査プログラム及び結果	内部監査報告書	記録・帳票
9.3	マネジメントレビューの結果	マネジメントレビュー議事録	記録・帳票
10.2	不適合及び是正処置の証拠	是正処置記録	記録・帳票

b) 当社が必要と決定した文書化した情報

文書体系	文書
ISMSマニュアル	箇条4〜10（JIS Q 27001:2023要求事項への対応）
運用規定	1. 組織的対策〜14. 情報セキュリティリスクアセスメント
適用宣言書	附属書A管理策（93管理策の適用状況）
記録・帳票	ネットワーク構成図、オフィスレイアウト
参考資料	JIS Q 27001:2023 参考資料

7.5.2 作成及び更新

要求事項

文書化した情報を作成及び更新する際、組織は、次の事項を確実にしなければならない。

- a) 適切な識別及び記述（例えば、タイトル、日付、作成者、参照番号）
- b) 適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）
- c) 適切性及び妥当性に関する、適切なレビュー及び承認

当社における実施状況

a) 識別及び記述

当社の文書化した情報は、以下の識別情報を含んでいる。

識別項目	内容
タイトル	文書の内容を示す明確なタイトル
版（バージョン）	文書のバージョン番号
作成者	文書の作成責任者（情報セキュリティ委員会等）
発行日	文書の発行日または改訂日
適用範囲	文書が適用される範囲

b) 形式及び媒体

項目 当社の対応

言語 日本語

形式 Markdown形式（ISMS文書管理システム）、PDF（印刷用）

媒体 電子媒体（ISMS文書管理システム、Google Drive）

c) レビュー及び承認

文書化した情報のレビュー及び承認は、以下のプロセスで実施している。

文書種別	レビュー者	承認者
ISMSマニュアル	情報セキュリティ委員会	代表取締役
運用規定	情報セキュリティ委員会	情報セキュリティ責任者
適用宣言書	情報セキュリティ委員会	情報セキュリティ責任者
記録・帳票	作成者	管理責任者

7.5.3 文書化した情報の管理

要求事項

ISMS及びこの規格で要求されている文書化した情報は、次の事項を確実にするために、管理しなければならない。

- a) 文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態である。

- b) 文書化した情報が十分に保護されている（例えば、機密性の喪失、不適切な使用又は完全性の喪失からの保護）。

文書化した情報の管理に当たって、組織は、該当する場合には、必ず、次の行動に取り組まなければならない。

- c) 配付、アクセス、検索及び利用
- d) 読みやすさが保たれることを含む、保管及び保存
- e) 変更の管理（例えば、版の管理）
- f) 保持及び廃棄

ISMSの計画策定及び運用のために組織が必要と決定した外部からの文書化した情報は、必要に応じて識別し、管理しなければならない。

当社における実施状況

3つの主要文書の位置づけと相互関係

当社のISMS文書は、以下の相互関係に基づき管理されている。

文書	役割	他文書との関係
ISMSマニュアル	規格要求事項（箇条4〜10）への対応方針を記述	運用規定・適用宣言書の上位文書
運用規定	ISMSマニュアルの方針に基づく具体的な運用ルール・手順を記述	ISMSマニュアルの方針を具体化
適用宣言書	附属書A管理策の適用・非適用と実施状況を記述	各管理策の実施手順は運用規定を参照

a) 入手可能性及び利用適合性

文書種別	保管場所	アクセス方法
ISMSマニュアル	ISMS文書管理システム	Webブラウザ（社内ネットワーク）
運用規定	ISMS文書管理システム	Webブラウザ（社内ネットワーク）
適用宣言書	ISMS文書管理システム	Webブラウザ（社内ネットワーク）
記録・帳票	Google Drive	Google Workspace認証

文書種別	保管場所	アクセス方法
外部文書（ISO規格等）	ISMS文書管理システム（参照）	Webブラウザ

b) 文書の保護

保護対策	実施内容
機密性	アクセス制御（Google Workspace認証、IAP）
完全性	Git版管理、変更履歴の記録
可用性	クラウドサービスの冗長性、バックアップ

c) 配付、アクセス、検索及び利用

項目	実施内容
配付	ISMS文書管理システムでの公開、Slackでの周知
アクセス	従業員はGoogle Workspace認証でアクセス可能
検索	ISMS文書管理システムの検索機能
利用	Webブラウザでの閲覧、PDF出力

d) 保管及び保存

項目	実施内容
保管場所	ISMS文書管理システム（Cloud Run）、Google Drive
保存期間	規程類：永年、記録類：5年以上
読みやすさ	Markdown形式、PDF形式で可読性を確保

e) 変更の管理

項目	実施内容
版管理	Git（GitHub）による版管理
変更履歴	コミット履歴、文書内のバージョン情報
変更承認	プルリクエストによるレビュー・承認

f) 保持及び廃棄

項目	実施内容
保持	最新版をISMS文書管理システムで公開、旧版はGit履歴で保持
廃棄	不要となった文書は適切な手順で削除（Git履歴は保持）

外部文書の管理

外部からの文書化した情報（ISO規格、法令等）は、以下のとおり管理している。

外部文書	管理方法
ISO/IEC 27001:2022	参考資料としてISMS文書管理システムに概要を掲載
関連法令	法改正時に情報セキュリティ委員会で確認、規程への反映
顧客要求事項	契約書・仕様書として保管

証跡

証跡	内容	保管場所
文書一覧	ISMS文書の一覧	ISMS文書管理システム
変更履歴	文書の変更履歴	GitHub
承認記録	プルリクエストの承認記録	GitHub
アクセスログ	文書へのアクセス記録	Cloud Run、Google Workspace

関連文書

- ISMSマニュアル（箇条4〜10）
- 運用規定（情報セキュリティ関連規程）
- 適用宣言書（附属書A管理策）
- 情報セキュリティ基本方針
- 14. 情報セキュリティリスクアセスメント

8.1 運用の計画策定及び管理

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
箇条番号	8.1
分類	運用

要求事項

組織は、次に示す事項の実施によって、要求事項を満たすため、及び箇条6で決定した活動を実施するために必要なプロセスを計画し、実施し、かつ、管理しなければならない。

- プロセスに関する基準の設定
- その基準に従った、プロセスの管理の実施

組織は、プロセスが計画どおりに実施されたという確信をもつために必要とされる、文書化した情報を利用可能な状態にしなければならない。

組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置を講じなければならない。

組織は、ISMSに関連する、外部から提供されるプロセス、製品又はサービスが管理されていることを確実にしなければならない。

目的

箇条6で計画したリスク及び機会への対処活動、リスクアセスメント、リスク対応を確実に実施し、ISMSの意図した成果を達成するため。

当社における実施状況

プロセスの計画及び実施

当社では、ISMSの運用に必要なプロセスを以下のとおり計画し、実施している。

主要なISMSプロセス

プロセス	基準・手順	実施頻度	責任者
リスクアセスメント	14. 情報セキュリティリスクアセスメント	年1回（8月）及び臨時	情報セキュリティ責任者
内部監査	1. 組織的対策	年1回（8月）	監査・点検責任者
マネジメントレビュー	1. 組織的対策	年1回（8月）	情報セキュリティ責任者
インシデント対応	10. インシデント対応及び事業継続管理	随時（発生時）	インシデント対応責任者
教育・訓練	2. 人的対策	入社時及び年1回	教育責任者
アクセス権管理	4. アクセス制御及び認証	随時（イベント駆動）	システム管理者

プロセスの基準

各プロセスの基準は、対応する規程・手順書に定めており、以下の観点を含む。

- 実施の契機・頻度
- 役割と責任
- 入力情報と成果物
- 実施手順
- 記録の管理

変更管理

計画した変更及び意図しない変更については、6.3 変更の計画策定に基づき管理する。

計画した変更の管理

変更の種類	管理方法	承認者
規程・方針の改訂	変更管理プロセスに従い承認後実施	情報セキュリティ責任者
システム構成の変更	8. システム開発及び保守に従い実施	システム管理者
組織体制の変更	変更内容を文書化し、関係者に伝達	情報セキュリティ責任者

意図しない変更への対応

意図しない変更（インシデント、障害等）が発生した場合は、10. インシデント対応及び事業継続管理に従い、影響を評価し、必要な是正処置を講じる。

外部から提供されるプロセス、製品又はサービスの管理

当社はクラウドサービスを前提とした事業運営を行っており、外部から提供されるサービスの管理は以下のとおり実施している。

クラウドサービス（SaaS/PaaS/IaaS）

- **導入時の評価：** 13. SaaS導入・シャドーIT管理に基づき、情報セキュリティ責任者の承認を得て導入
- **継続的な管理：** 7. IT基盤運用管理に基づき、システム管理者が運用管理
- **見直し：** 重大なセキュリティインシデント発生時、仕様変更時等に再評価

委託先

- **評価・選定：** 9. 委託管理に基づき、情報セキュリティ対策を確認のうえ選定
- **契約：** 守秘義務、再委託、事故時の報告等を契約に明記
- **管理：** 連絡及び業務内容の確認を通じて、情報セキュリティ上の問題がないことを確認

文書化した情報

プロセスが計画どおりに実施されたことを示す文書化した情報として、以下を保持している。

文書・記録	内容	保管場所
リスクアセスメント報告書	リスク評価結果及び対応方針	ISMS文書管理システム
内部監査報告書	監査結果及び指摘事項	ISMS文書管理システム

文書・記録	内容	保管場所
マネジメントレビュー議事録	レビュー結果及び決定事項	ISMS文書管理システム
インシデント記録	インシデント対応履歴	YouTrack
教育実施記録	教育の実施状況	Slack記録、カレンダー
変更履歴	規程・システムの変更記録	Git、各システムの監査ログ

関連文書

- 6.1 リスク及び機会に対処する活動
- 6.3 変更の計画策定
- 1. 組織的対策
- 7. IT基盤運用管理
- 9. 委託管理
- 10. インシデント対応及び事業継続管理
- 13. SaaS導入・シャドーIT管理
- 14. 情報セキュリティリスクアセスメント

8.2 情報セキュリティリスクアセスメント

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
箇条番号	8.2
分類	運用

要求事項

組織は、あらかじめ定めた間隔で、又は重大な変更が提案されたか若しくは重大な変化が生じた場合に、6.1.2 a)で確立した基準を考慮して、情報セキュリティリスクアセスメントを実施しなければならない。

組織は、情報セキュリティリスクアセスメント結果の文書化した情報を保持しなければならない。

目的

6.1.2で定めた情報セキュリティリスクアセスメントのプロセスを、定期的に及び必要に応じて実施し、リスクの変化を把握して適切な対応を行うため。

当社における実施状況

リスクアセスメントの実施

当社では、14. 情報セキュリティリスクアセスメントに基づき、情報セキュリティリスクアセスメントを実施している。

実施の契機・頻度

契機	頻度	備考
定期実施	年1回（8月のマネジメントレビュー前）	内部監査と同時期に実施
臨時実施	随時	下記の事象発生時

臨時実施の契機：

- 新たな重要情報資産の追加
- 大規模なシステム構成変更（クラウドサービスの追加・変更、ネットワーク構成の変更等）
- 情報セキュリティインシデントの発生
- 法令・規制要件の重大な変更
- 事業環境の大幅な変化

リスク基準

6.1.2 a)で確立したリスク基準に基づき、リスクアセスメントを実施する。

影響度（Impact）

レベル	定義
3	法令違反、個人情報漏えい、取引先・顧客への重大な影響が発生する
2	事業運営に支障が生じる、信用低下が発生する
1	社内業務への限定的な影響にとどまる

発生可能性（Likelihood）

レベル	定義
3	過去事例や構成上、発生の可能性が高い
2	一定の条件下で発生する可能性がある
1	発生可能性は低い

リスクレベル判定

リスクレベル ＝ 影響度 × 発生可能性

リスク値	判定	対応方針
6〜9	高（要対応）	原則として低減または回避
3〜4	中（管理策により低減）	管理策の適用を検討
1〜2	低（受容）	受容可能

実施手順

リスクアセスメントは、14. 情報セキュリティリスクアセスメントに定める以下のステップで実施する。

1. **対象資産の選定：** 情報資産台帳から機密性レベル1以上の資産を抽出
2. **脅威・脆弱性の洗い出し：** 各資産に対する想定脅威と脆弱性を識別
3. **影響度・発生可能性の評価：** リスク基準に基づき評価
4. **リスク値算出と判定：** リスクレベルを判定
5. **リスク対応方針の決定：** 低減、受容、回避、移転のいずれかを決定
6. **結果の承認：** 情報セキュリティ責任者が承認

役割と責任

役割	担当者	責任
実施責任者	情報セキュリティ責任者（代表取締役）	アセスメント全体の統括、最終承認
実施担当者	情報セキュリティ委員会	アセスメントの実施、報告書作成
資産オーナー	各情報資産の管理責任者	資産情報の提供、脅威・脆弱性の確認

文書化した情報

リスクアセスメント結果は、以下の文書化した情報として保持する。

文書	内容	保管場所
リスクアセスメント報告書	対象資産、脅威・脆弱性、リスク評価結果、対応方針	ISMS文書管理システム
情報資産台帳	情報資産の一覧、機密性レベル、管理責任者	ISMS文書管理システム

最新のリスクアセスメント結果

最新のリスクアセスメント結果は、14. 情報セキュリティリスクアセスメントの「4. リスクアセスメント結果」に記載している。

現在、以下の情報資産について「高」と判定されたリスクがあり、既存の管理策により低減を図っている。

- IA-001：顧客基本情報（Cloud SQL / Amazon RDS）
- IA-001-2：顧客管理資料（Google Workspace 共有ドライブ）
- IA-004：ソースコード（GitHub）
- IA-009：カスタマーサポート情報（Zendesk）
- IA-010：分析データ（BigQuery）

関連文書

- 6.1 リスク及び機会に対処する活動
- 14. 情報セキュリティリスクアセスメント
- 12. 情報資産の定義と管理ルール

8.3 情報セキュリティリスク対応

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
箇条番号	8.3
分類	運用

要求事項

組織は、情報セキュリティリスク対応計画を実施しなければならない。

組織は、情報セキュリティリスク対応結果の文書化した情報を保持しなければならない。

目的

6.1.3で策定した情報セキュリティリスク対応計画を確実に実施し、リスクを許容可能なレベルまで低減するため。

当社における実施状況

リスク対応計画の実施

当社では、6.1.3で策定したリスク対応計画に基づき、以下のとおりリスク対応を実施している。

リスク対応の選択肢

対応方針	説明	適用例
低減	管理策を適用してリスクを許容可能なレベルまで低減	アクセス制御、暗号化、監査ログ
受容	リスクが許容範囲内であり、追加対策を行わない	リスク値2以下の低リスク
回避	リスク源となる活動を中止または変更	高リスクなサービスの利用中止
移転	保険加入や外部委託によりリスクを移転	サイバー保険、クラウドサービス利用

管理策の実施状況

ISO/IEC 27001:2022 附属書Aの93の管理策について適用・非適用を明確化し、適用する管理策を実施している。

主な管理策の実施状況

管理策カテゴリ	主な実施内容	関連規程
組織的管理策（A.5）	情報セキュリティ方針、役割・責任の明確化、インシデント対応体制	1. 組織的対策、10. インシデント対応
人的管理策（A.6）	採用時審査、教育・訓練、退職時手続き	2. 人的対策
物理的管理策（A.7）	オフィスセキュリティ、クリアデスク	5. 物理的対策
技術的管理策（A.8）	アクセス制御、認証、暗号化、ログ管理	4. アクセス制御及び認証、6. IT機器利用

高リスクへの対応状況

8.2 情報セキュリティリスクアセスメントにおいて「高」と判定されたリスクについては、以下の管理策により低減を図っている。

資産ID	情報資産	主な管理策	実施状況
IA-001	顧客基本情報（Cloud SQL / Amazon RDS）	DBはインターネット非公開、アプリ経由アクセス、権限管理、監査ログ	実施済
IA-001-2	顧客管理資料（Google Workspace 共有ドライブ）	共有ドライブ権限管理、管理者限定、定期的な権限確認	実施済
IA-004	ソースコード（GitHub）	組織管理、リポジトリ権限管理、SSO、監査ログ	実施済
IA-009	カスタマーサポート情報（Zendesk）	サポート部のみアクセス可能、ロール・権限管理、SSO連携、監査ログ	実施済
IA-010	分析データ（BigQuery）	IAMによる権限管理、データセット権限設定、監査ログ、VPC Service Controls	実施済

リスク対応計画の管理

追加の管理策が必要な場合は、リスク対応計画をYouTrackのチケットとして管理し、以下の情報を明確化している。

- 対応すべきリスク
- 実施する管理策
- 実施期限
- 担当者
- 進捗状況

リスク所有者の承認

リスク対応計画及び残留リスクの受容については、情報セキュリティ責任者（代表取締役）が承認する。

文書化した情報

リスク対応結果は、以下の文書化した情報として保持する。

文書	内容	保管場所
リスクアセスメント報告書	リスク対応方針、管理策の実施状況	ISMS文書管理システム

文書	内容	保管場所
適用宣言書	管理策の適用・非適用及び理由	ISMS文書管理システム
リスク対応計画	追加管理策の実施計画、進捗	YouTrack
各種規程・手順書	管理策の詳細な実施手順	ISMS文書管理システム

継続的な確認

リスク対応の有効性は、以下の機会において確認する。

- **年次リスクアセスメント：** 管理策の有効性を評価し、必要に応じて見直し
- **内部監査：** 管理策の実施状況を確認
- **マネジメントレビュー：** リスク対応計画の状況を報告、改善の必要性を検討
- **インシデント発生時：** 管理策の有効性を検証、必要に応じて追加対策を実施

関連文書

- 6.1 リスク及び機会に対処する活動
- 8.2 情報セキュリティリスクアセスメント
- 14. 情報セキュリティリスクアセスメント
- 1. 組織的対策
- 10. インシデント対応及び事業継続管理

9.1 監視、測定、分析及び評価

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
箇条番号	9.1
分類	パフォーマンス評価

要求事項

組織は、次の事項を決定しなければならない。

- a) 監視及び測定が必要な対象。これには、情報セキュリティプロセス及び管理策を含む。
- b) 該当する場合には、必ず、妥当な結果を確実にするための、監視、測定、分析及び評価の方法。選定した方法は、妥当と考えられる、比較可能で再現可能な結果を生み出すことが望ましい。
- c) 監視及び測定の実施時期
- d) 監視及び測定の実施者
- e) 監視及び測定の結果の、分析及び評価の時期
- f) 監視及び測定の結果の、分析及び評価の実施者

組織は、この結果の証拠として、文書化した情報を利用可能な状態にしなければならない。

組織は、情報セキュリティパフォーマンス及びISMSの有効性を評価しなければならない。

目的

ISMSが意図した成果を達成しているか、情報セキュリティプロセス及び管理策が有効に機能しているかを客観的に把握し、継続的改善につなげるため。

当社における実施状況

監視・測定の対象と方法

当社では、以下の項目について監視・測定を実施している。

監視・測定対象	測定方法	実施時期	実施者	分析・評価時期	分析・評価者
情報セキュリティインシデント	YouTrackでのインシデント記録の集計	随時（発生時）	インシデント対応責任者	年1回（8月）	情報セキュリティ責任者
情報セキュリティ教育の実施状況	Slack反応・カレンダー記録の確認	入社時・年1回	教育責任者	年1回（8月）	情報セキュリティ責任者
アクセス権限の管理状況	Microsoft Entra ID・Google Workspace監査ログ	随時（イベント駆動）	システム管理者	年1回（8月）	情報セキュリティ責任者
リスクアセスメントの実施	リスクアセスメント報告書	年1回（8月）	情報セキュリティ責任者	年1回（8月）	情報セキュリティ責任者
法令・規制要件の遵守状況	内部監査結果、外部指摘の有無	年1回（8月）	監査・点検責任者	年1回（8月）	情報セキュリティ責任者
クラウドサービスのセキュリティ状況	各サービスのセキュリティ設定確認	随時（変更時）	システム管理者	年1回（8月）	情報セキュリティ責任者

情報セキュリティ目的の達成状況

6.2 情報セキュリティ目的及びそれを達成するための計画策定で設定した目的について、以下の指標で監視・測定を行う。

目的	測定指標	目標値	測定方法
情報セキュリティインシデントの防止	重大インシデント（レベル2以上）の発生件数	0件/年	YouTrackインシデント記録の集計
情報セキュリティ教育の徹底	教育受講率	100%	Slack反応・カレンダー記録
アクセス権限の適正管理	退職者アカウントの即時無効化率	100%	アカウント管理記録
リスクアセスメントの実施	年次リスクアセスメント実施	1回/年	リスクアセスメント報告書
法令・規制要件の遵守	法令違反・指摘事項	0件/年	内部監査結果

パフォーマンス測定の方法

パフォーマンス測定では、以下の2つの観点から評価を行う。

観点	説明	用途
実施度	計画した管理策に対してどの程度実施されたかを測定	管理策の実装・運用の妥当性チェック、不足点の特定
達成度	計画した管理策を実施した結果、情報セキュリティ目的がどの程度達成されたかを測定	管理策が目的を達成する能力を果たしたかの評価

分析及び評価

監視・測定の結果は、年1回のマネジメントレビュー（8月）において分析・評価を行う。分析・評価では以下の観点を確認する。

- 情報セキュリティ目的の達成状況
- 管理策の有効性
- 傾向分析（前年度との比較）
- 改善が必要な領域の特定

パフォーマンス評価の基準

測定結果に基づき、管理策のパフォーマンスを以下の基準で評価する。

評価区分	基準	対応
能力あり	目標を達成し、有効に機能している	現状の運用を継続
経過監視	目標は達成しているが、傾向として悪化が見られる	監視頻度を上げて経過を観察
改善必要	目標未達成または有効に機能していない	原因分析、是正処置の実施

フィードバック

パフォーマンス評価結果は、以下にフィードバックする。

フィードバック先	内容
マネジメントレビュー	ISMSの有効性評価のインプットとして活用
リスクアセスメント	リスク対応の妥当性確認、再アセスメントの要否判断
監視プロセス	監視項目・頻度の見直し
インシデント管理	インシデント対応基準の見直し

文書化した情報

監視・測定の結果は、以下の形式で文書化し保持する。

文書・記録	内容	保管場所
インシデント記録	インシデント対応履歴、件数集計	YouTrack
教育実施記録	教育の実施状況、受講者記録	Slack記録、カレンダー
アカウント管理記録	アクセス権限の変更履歴	Microsoft Entra ID監査ログ、Google Workspace監査ログ（いずれもnightwatchで長期保存）
リスクアセスメント報告書	リスク評価結果	ISMS文書管理システム
内部監査報告書	監査結果、指摘事項	ISMS文書管理システム
マネジメントレビュー議事録	分析・評価結果、決定事項	ISMS文書管理システム

関連文書

- 6.2 情報セキュリティ目的及びそれを達成するための計画策定
- 1. 組織的対策
- 2. 人的対策
- 10. インシデント対応及び事業継続管理
- 14. 情報セキュリティリスクアセスメント
- 9.2 内部監査
- 9.3 マネジメントレビュー

9.2 内部監査

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2026.03.04
適用範囲	全社
箇条番号	9.2
分類	パフォーマンス評価

要求事項

9.2.1 一般

組織は、ISMSが次の状況にあるか否かに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施しなければならない。

- a) 次の事項に適合している。
    - 1. ISMSに関して、組織自体が規定した要求事項
    - 2. この規格の要求事項
- b) 有効に実施され、維持されている。

9.2.2 内部監査プログラム

組織は、監査プログラムを計画し、確立し、実施し、維持しなければならない。これには、その頻度、方法、責任、計画策定の要求事項及び報告を含める。

それ（ら）の内部監査プログラムを確立するとき、組織は、関連するプロセスの重要性及び前回までの監査の結果を考慮しなければならない。

組織は、次に示す事項を行わなければならない。

- a) 各監査について、監査基準及び監査範囲を明確にする。

- b) 監査プロセスの客観性及び公平性を確保するために、監査員を選定し、監査を実施する。
- c) 監査の結果を関連する管理層に報告することを確実にする。

組織は、監査プログラムの実施及び監査結果の証拠として、文書化した情報を利用可能な状態にしなければならない。

目的

ISMSが規格要求事項及び組織自体が規定した要求事項に適合し、有効に機能しているかを独立した立場から評価し、改善の機会を特定するため。

当社における実施状況

当社の内部監査は、マネジメントレビューと同日に実施し、**内部監査＋マネジメントレビュー議事録**（Google Docs）として1本の文書にまとめている。

内部監査に関する組織体制及び基本的な実施方針は、1. 組織的対策の「2. 情報セキュリティ取組みの監査・点検」に定めている。

本項では、内部監査の概要を示す。

内部監査の概要

項目	内容
実施頻度	年1回（8月）
監査責任者	監査・点検責任者（管理部責任者または代表取締役）
監査範囲	ISMSの適用範囲全体（語学教育事業部）
監査基準	JIS Q 27001:2023要求事項、当社情報セキュリティ関連規程

独立性の確保

当社は少人数体制であるため、内部監査の独立性確保について以下のとおり対応している。

- 内部監査部分については、運用当事者以外の者が担当する
- 監査・点検責任者は、自身が直接運用に関与していない領域を監査する

- 必要に応じて、外部の専門家の支援を受けることを検討する

監査プログラム

内部監査プログラムは以下の要素を含む。

要素	内容
頻度	年1回（8月、マネジメントレビューと同日実施）
方法	文書レビュー、記録確認、関係者へのヒアリング
責任	監査・点検責任者
計画策定	監査実施前に監査計画を策定
報告	監査結果を情報セキュリティ責任者に報告

監査の実施

各監査において、以下を明確にする。

監査基準：

- JIS Q 27001:2023の要求事項（箇条4〜10）
- 当社情報セキュリティ関連規程
- 適用宣言書に記載された管理策

監査範囲：

- ISMSの適用範囲（語学教育事業部）
- 情報セキュリティ関連規程の実施状況
- 管理策の運用状況

監査結果の報告

監査結果は、内部監査報告書として取りまとめ、情報セキュリティ責任者に報告する。報告内容には以下を含む。

- 監査の概要（日時、監査員、監査範囲）
- 適合状況の評価
- 指摘事項（不適合、観察事項、改善の機会）

- 是正処置の要否と推奨事項

文書化した情報

文書・記録	内容	保管場所
内部監査計画	監査の計画（範囲、基準、スケジュール）	ISMS文書管理システム
内部監査報告書	監査結果、指摘事項	ISMS文書管理システム
内部監査チェックリスト	監査項目と確認結果	ISMS文書管理システム

関連文書

- 1. 組織的対策
- 9.1 監視、測定、分析及び評価
- 9.3 マネジメントレビュー
- 10.2 不適合及び是正処置
- 内部監査＋マネジメントレビュー 議事録（Google Docs）

9.3 マネジメントレビュー

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
箇条番号	9.3
分類	パフォーマンス評価

要求事項

9.3.1 一般

トップマネジメントは、組織のISMSが、引き続き、適切、妥当かつ有効であることを確実にするために、あらかじめ定めた間隔で、ISMSをレビューしなければならない。

9.3.2 マネジメントレビューへのインプット

マネジメントレビューは、次の事項を考慮しなければならない。

- a) 前回までのマネジメントレビューの結果講じた処置の状況
- b) ISMSに関連する外部及び内部の課題の変化
- c) ISMSに関連する利害関係者のニーズ及び期待の変化
- d) 次に示す傾向を含めた、情報セキュリティパフォーマンスに関するフィードバック
    - 1. 不適合及び是正処置
    - 2. 監視及び測定の結果
    - 3. 監査結果
    - 4. 情報セキュリティ目的の達成
- e) 利害関係者からのフィードバック
- f) リスクアセスメントの結果及びリスク対応計画の状況
- g) 継続的改善の機会

9.3.3 マネジメントレビューの結果

マネジメントレビューの結果には、継続的改善の機会、及びISMSのあらゆる変更の必要性に関する決定を含めなければならない。

組織は、マネジメントレビューの結果の証拠として、文書化した情報を利用可能な状態にしなければならない。

目的

トップマネジメントがISMSの適切性、妥当性及び有効性を定期的に評価し、必要な改善や変更を決定することで、ISMSの継続的な有効性を確保するため。

当社における実施状況

当社のマネジメントレビューは、内部監査と同日に実施し、**内部監査＋マネジメントレビュー議事録**（Google Docs）として1本の文書にまとめている。

マネジメントレビューに関する組織体制及び基本的な実施方針は、1. 組織的対策の「2. 情報セキュリティ取組みの監査・点検」に定めている。

本項では、マネジメントレビューの概要を示す。

マネジメントレビューの概要

項目	内容
実施頻度	年1回（8月）
実施責任者	情報セキュリティ責任者（代表取締役）
参加者	トップマネジメント、情報セキュリティ部門責任者（CTO）
実施形式	内部監査と同日に実施し、議事録1本にまとめる

インプット情報

マネジメントレビューでは、以下の情報をインプットとして考慮する。

インプット項目	情報源	担当
前回マネジメントレビューの処置状況	前回議事録、是正処置記録	情報セキュリティ責任者
外部及び内部の課題の変化	4.1 組織及びその状況の理解の見直し	情報セキュリティ責任者
利害関係者のニーズ及び期待の変化	4.2 利害関係者のニーズ及び期待の理解の見直し	情報セキュリティ責任者
不適合及び是正処置	内部監査報告書、是正処置記録	監査・点検責任者
監視及び測定の結果	9.1 監視、測定、分析及び評価の結果	情報セキュリティ責任者
監査結果	9.2 内部監査報告書	監査・点検責任者
情報セキュリティ目的の達成	6.2 情報セキュリティ目的の達成状況	情報セキュリティ責任者
利害関係者からのフィードバック	顧客からの要望、監査指摘等	情報セキュリティ責任者
リスクアセスメント結果	14. 情報セキュリティリスクアセスメント	情報セキュリティ責任者
継続的改善の機会	各種レビュー結果、改善提案	全参加者

アウトプット（レビュー結果）

マネジメントレビューの結果として、以下の事項を決定する。

- ISMSの継続的改善の機会
- ISMSの変更の必要性（方針、目的、プロセス、管理策等）
- 資源の必要性
- 是正処置の指示
- 次回レビューまでの重点事項

文書化した情報

文書・記録	内容	保管場所
マネジメントレビュー議事録	レビュー結果、決定事項、処置指示	ISMS文書管理システム

文書・記録	内容	保管場所
是正処置記録	指摘事項への対応状況	YouTrack

関連文書

- 1. 組織的対策
- 4.1 組織及びその状況の理解
- 4.2 利害関係者のニーズ及び期待の理解
- 6.2 情報セキュリティ目的及びそれを達成するための計画策定
- 9.1 監視、測定、分析及び評価
- 9.2 内部監査
- 14. 情報セキュリティリスクアセスメント
- 10.1 継続的改善
- 内部監査＋マネジメントレビュー 議事録（Google Docs）

10.1 継続的改善

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
箇条番号	10.1
分類	改善

要求事項

組織は、ISMSの適切性、妥当性及び有効性を継続的に改善しなければならない。

目的

ISMSが組織の情報セキュリティニーズに対して常に適切であり、効果的に機能し続けることを確保するため、継続的な改善活動を実施する。

当社における実施状況

当社では、ISMSの継続的改善を以下のプロセスを通じて実施している。

継続的改善の情報源

ISMSの改善機会は、以下の活動から特定される。

情報源	内容	関連文書
マネジメントレビュー	ISMSの適切性・妥当性・有効性の評価、改善機会の特定	9.3 マネジメントレビュー
内部監査	規格要求事項・社内規程への適合状況の評価、改善の機会の特定	9.2 内部監査

情報源	内容	関連文書
監視・測定結果	情報セキュリティパフォーマンスの分析、傾向の把握	9.1 監視、測定、分析及び評価
是正処置	不適合の原因除去、再発防止策の実施	10.2 不適合及び是正処置
インシデント対応	インシデントからの教訓、再発防止策	10. インシデント対応及び事業継続管理
リスクアセスメント	リスク状況の変化、新たなリスクへの対応	14. 情報セキュリティリスクアセスメント
外部環境の変化	法令・規制の変更、脅威動向の変化	4.1 組織及びその状況の理解

継続的改善のサイクル

当社では、PDCAサイクルに基づき継続的改善を実施している。

フェーズ	活動内容	実施時期	責任者
Plan（計画）	リスクアセスメント、情報セキュリティ目的の設定、改善計画の策定	年1回（8月）および随時	情報セキュリティ責任者
Do（実施）	管理策の実施、教育・訓練、運用	通年	各担当者
Check（評価）	監視・測定、内部監査、マネジメントレビュー	年1回（8月）および随時	監査・点検責任者、情報セキュリティ責任者
Act（改善）	是正処置、予防処置、ISMS文書の改訂	随時	情報セキュリティ責任者

改善活動の実施

改善の機会が特定された場合、以下のプロセスで対応する。

1. **改善機会の評価**: 情報セキュリティ責任者が改善の必要性と優先度を評価
2. **改善計画の策定**: 具体的な改善内容、担当者、期限を決定
3. **改善の実施**: 計画に基づき改善を実施
4. **有効性の確認**: 改善が意図した効果を達成したかを確認

改善の対象

継続的改善の対象には以下が含まれる。

- 情報セキュリティ方針及び目的
- 情報セキュリティ関連規程
- リスクアセスメント及びリスク対応のプロセス
- 管理策の有効性
- 組織体制及び役割・責任
- 教育・訓練プログラム
- 監視・測定の方法

文書化した情報

継続的改善に関する記録は、以下の形式で文書化し保持する。

文書・記録	内容	保管場所
マネジメントレビュー議事録	改善機会の特定、改善の決定事項	ISMS文書管理システム
内部監査報告書	改善の機会、観察事項	ISMS文書管理システム
是正処置記録	是正処置の内容と結果	YouTrack
ISMS文書改訂履歴	規程・手順の改訂内容	ISMS文書管理システム（Git履歴）

関連文書

- 1. 組織的対策
- 9.1 監視、測定、分析及び評価
- 9.2 内部監査
- 9.3 マネジメントレビュー
- 10.2 不適合及び是正処置
- 14. 情報セキュリティリスクアセスメント
- 10. インシデント対応及び事業継続管理

10.2 不適合及び是正処置

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
箇条番号	10.2
分類	改善

要求事項

不適合が発生した場合、組織は、次の事項を行わなければならない。

- a) その不適合に対処し、該当する場合には、必ず、次の事項を行う。
    - 1. その不適合を管理し、修正するための処置を講じる。
    - 2. その不適合によって起こった結果に対処する。
- b) その不適合が再発又は他のところで発生しないようにするため、次の事項によって、その不適合の原因を除去するための処置を講じる必要性を評価する。
    - 1. その不適合をレビューする。
    - 2. その不適合の原因を明確にする。
    - 3. 類似の不適合の有無、又はそれが発生する可能性を明確にする。
- c) 必要な処置を実施する。
- d) 講じた全ての是正処置の有効性をレビューする。
- e) 必要な場合には、ISMSの変更を行う。

是正処置は、検出された不適合のもつ影響に応じたものでなければならない。

組織は、次に示す事項の証拠として、文書化した情報を利用可能な状態にしなければならない。

- f) 不適合の性質及びそれに対して講じたあらゆる処置
- g) 是正処置の結果

目的

不適合が発生した場合に適切に対処し、原因を特定して是正処置を講じることで、同様の不適合の再発を防止し、ISMSの有効性を維持・向上させるため。

当社における実施状況

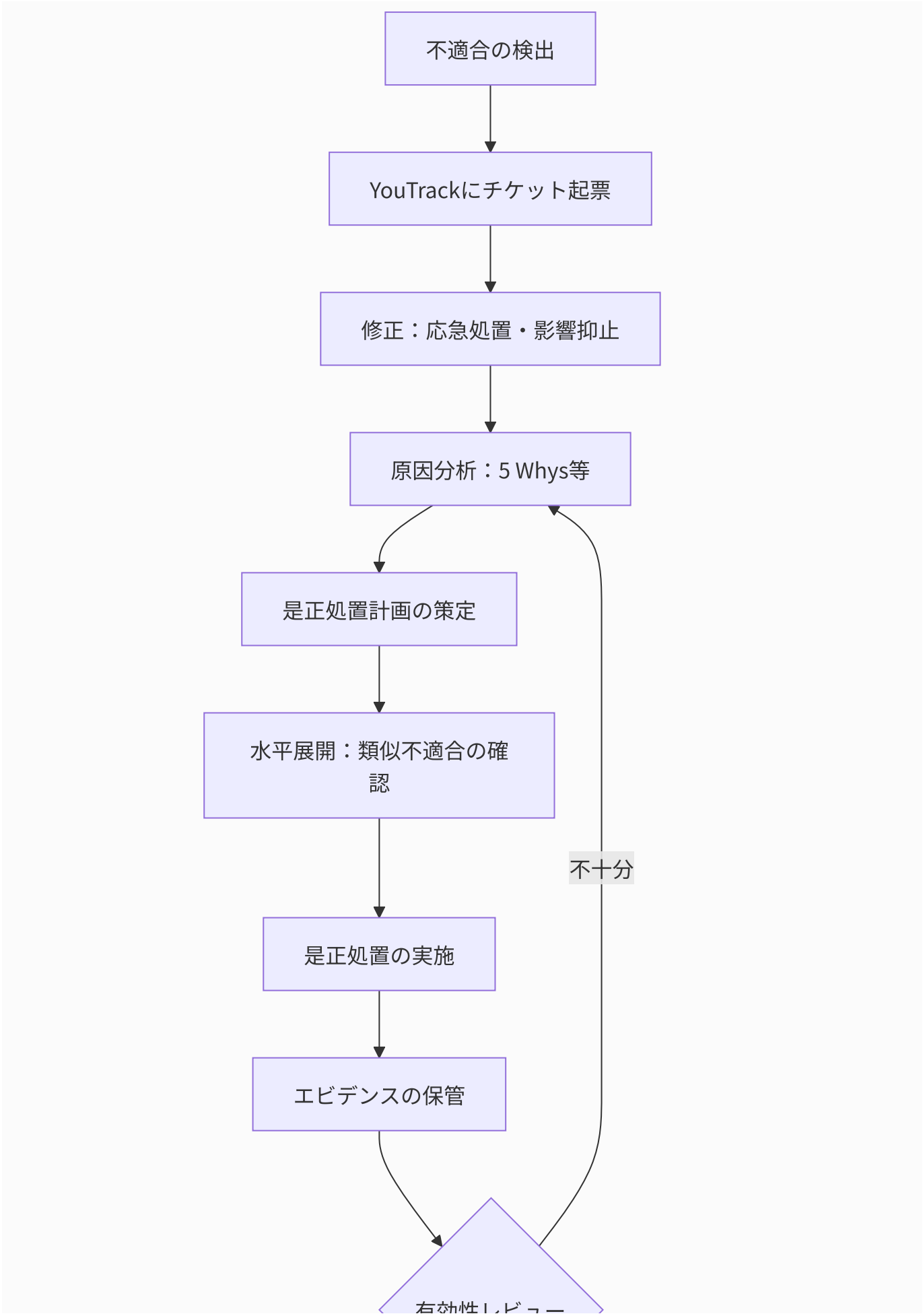
本セクションは、不適合及び是正処置に関する当社の手順を定める。内部監査指摘、情報セキュリティインシデント、顧客苦情、法令・契約逸脱、運用逸脱等、ISMS適用範囲内で発生するあらゆる不適合に対して適用する。

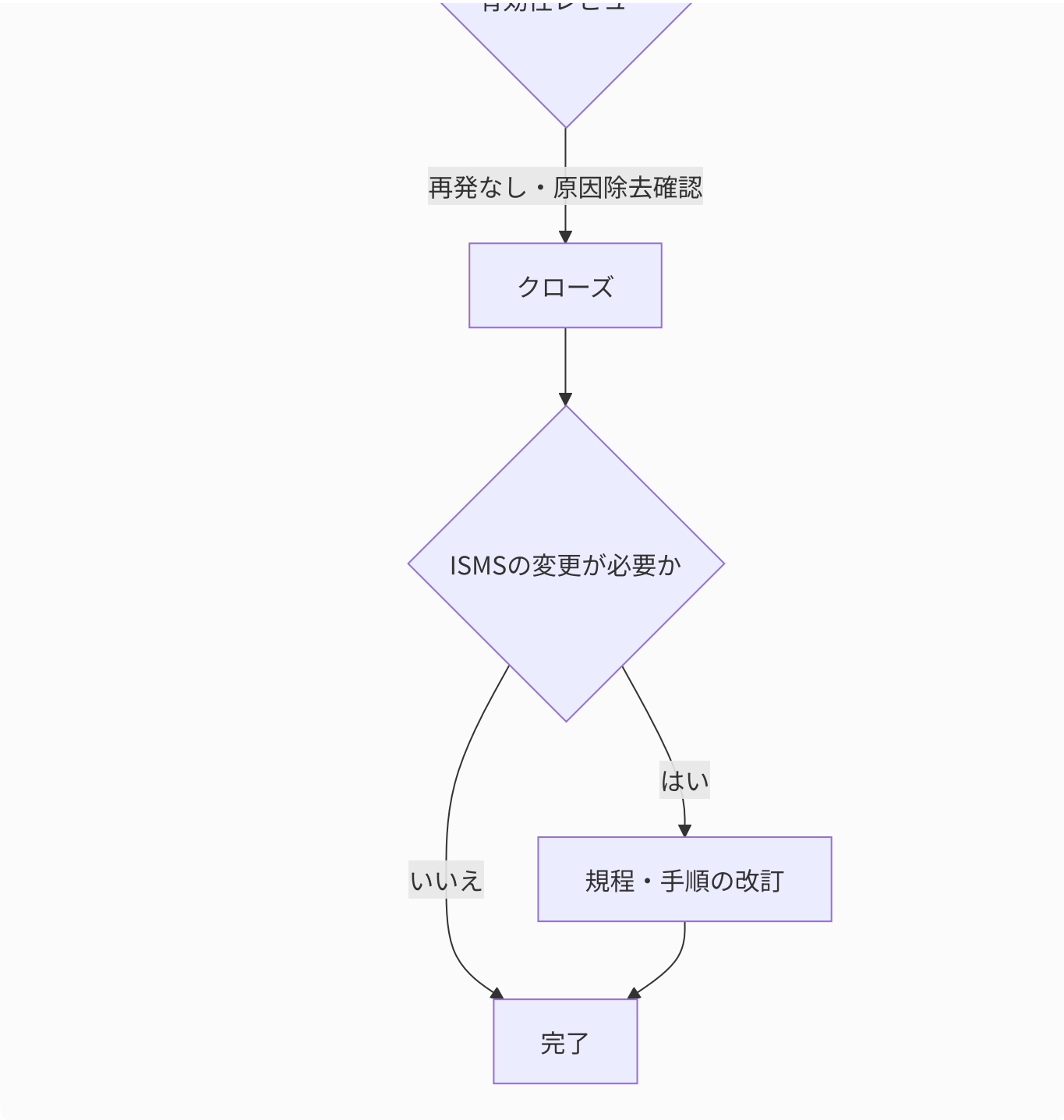
用語の定義

用語	定義
不適合	要求事項を満たしていないこと。規格要求事項、社内規程、法令・契約要件等への逸脱を含む。
修正（correction）	検出された不適合を除去するための処置。応急処置・暫定対処として、不適合状態を直ちに是正し、影響を抑止する。
是正処置（corrective action）	不適合の原因を除去し、再発を防止するための処置。根本原因の分析に基づき実施する。
水平展開	類似の不適合が他の領域で発生していないか、または発生する可能性がないかを確認し、予防的に対処すること。JIS Q 27001:2023における予防処置的な要素に相当する。

是正処置手順フロー

以下のフロー図は、不適合の検出から是正処置の完了までの全体プロセスを示す。


不適合の検出
YouTrackにチケット起票
修正：応急処置・影響抑止
原因分析：5 Whys等
是正処置計画の策定
水平展開：類似不適合の確認
是正処置の実施
エビデンスの保管
不十分



不適合の検出源

不適合は、以下の活動を通じて検出される。

検出源	内容	関連文書
内部監査	規格要求事項・社内規程への不適合	9.2 内部監査

検出源	内容	関連文書
マネジメントレビュー	ISMSの運用における問題点	9.3 マネジメントレビュー
監視・測定	目標未達、パフォーマンス低下	9.1 監視、測定、分析及び評価
インシデント対応	情報セキュリティインシデント	10. インシデント対応及び事業継続管理
日常業務	規程違反、手順の逸脱	各担当者からの報告
外部監査	認証審査での指摘事項	外部審査報告書

不適合への対処プロセス

ステップ1: 不適合の検出と記録

不適合が検出された場合、以下の情報をYouTrackに記録する。

- 不適合の内容（何が、いつ、どこで発生したか）
- 検出日と検出者
- 影響範囲
- 関連する規格要求事項・社内規程

ステップ2: 応急処置（修正）

不適合による影響を最小限に抑えるため、必要に応じて応急処置を実施する。

- 不適合状態の是正（修正）
- 不適合によって生じた結果への対処
- 影響を受けた関係者への連絡

ステップ3: 原因分析

不適合の再発防止のため、根本原因を分析する。

分析項目	内容
不適合のレビュー	不適合の内容、発生状況の詳細確認

分析項目	内容
原因の特定	なぜ不適合が発生したかの分析（5 Whys等）
類似不適合の確認	同様の不適合が他の領域で発生していないか、発生する可能性があるかの確認

ステップ4: 是正処置計画の策定

原因分析の結果に基づき、是正処置計画を策定する。

計画項目	内容
是正処置の内容	根本原因を除去するための具体的な処置
担当者	是正処置の実施責任者
完了期限	是正処置の完了予定日
必要な資源	是正処置に必要な人員、ツール、予算等

ステップ5: 水平展開（予防処置的対応）

是正処置の実施前または並行して、類似の不適合が他の領域で発生する可能性を確認し、予防的に対処する。これはJIS Q 27001:2023における予防処置的な要素に相当する。

確認項目	内容
類似プロセスの確認	同様の不適合が発生しうる他のプロセス・領域の特定
予防的対処	特定された領域への是正処置の適用検討
関係者への周知	不適合の内容と対策を関係者に共有し、再発防止を図る

ステップ6: 是正処置の実施とエビデンス保管

是正処置計画に基づき、処置を実施し、エビデンスを保管する。

実施項目	内容
是正処置の実施	計画に基づく処置の実行
エビデンスの保管	実施記録、変更差分、教育記録等をYouTrackチケットに添付
進捗の更新	YouTrackチケットのステータスを随時更新

ステップ7: 有効性レビュー

是正処置が完了した後、一定期間経過後にその有効性を確認する。

確認項目	判定基準
是正処置の実施状況	計画どおり実施されたか
原因の除去	不適合の根本原因が除去されたか
再発の有無	同様の不適合が再発していないか（一定期間の監視）

有効性が不十分と判断された場合は、ステップ3（原因分析）に戻り、再度分析と是正処置を実施する。

ステップ8: クローズ条件

以下の条件をすべて満たした場合、是正処置をクローズする。

- 是正処置が計画どおり完了している
- 有効性レビューで再発なし・原因除去が確認されている
- 必要なエビデンスがYouTrackに保管されている
- 情報セキュリティ責任者（または監査・点検責任者）の承認を得ている

ステップ9: ISMSの変更（必要な場合）

是正処置の結果、ISMSの変更が必要と判断された場合は、以下を検討する。

- 情報セキュリティ関連規程の改訂
- プロセス・手順の変更
- 管理策の追加・変更
- 教育・訓練内容の見直し

是正処置の管理（記録様式）

是正処置は、YouTrackでチケットとして管理し、以下の情報を記録する。これにより、箇条10.2 f)「不適合の性質及びそれに対して講じたあらゆる処置」およびg)「是正処置の結果」の文書化要求を満たす。

記録項目	内容	対応する規格要求
不適合の内容	不適合の詳細な説明（何が、いつ、どこで発生したか）	10.2 f)
検出日・検出源	いつ、どのように検出されたか	10.2 f)
修正（応急処置）の内容	不適合状態を除去するために講じた処置	10.2 a)
原因分析結果	根本原因の特定結果（5 Whys等の分析記録）	10.2 b)
水平展開の結果	類似不適合の確認結果と予防的対処	10.2 b)3)
是正処置の内容	実施する是正処置の詳細	10.2 c)
担当者・期限	是正処置の責任者と完了期限	-
実施状況	是正処置の進捗状況	-
エビデンス	実施記録、変更差分、教育記録等	10.2 f) g)
有効性確認結果	是正処置の有効性評価結果	10.2 d) g)
完了日・承認者	是正処置の完了日とクローズ承認者	10.2 g)

文書化した情報

文書・記録	内容	保管場所
是正処置記録	不適合の内容、原因分析、是正処置、有効性確認	YouTrack
内部監査報告書	監査で検出された不適合	ISMS文書管理システム
インシデント記録	インシデントに起因する不適合	YouTrack
ISMS文書改訂履歴	是正処置に伴う規程改訂	ISMS文書管理システム（Git履歴）

関連文書

- 1. 組織的対策
- 9.1 監視、測定、分析及び評価

- 9.2 内部監査
- 9.3 マネジメントレビュー
- 10.1 継続的改善
- 10. インシデント対応及び事業継続管理