

配付番号： _____

| |
|---------|
| 管 理 区 分 |
| 管 理 文 書 |

| | |
|-------|------------|
| 文書番号 | ISMS-A-03 |
| 制 定 日 | 2023.10.01 |
| 改 訂 日 | |
| 改訂番号 | 1 |

※購入希望の場合は、<https://www.iso-mi.com/>

ISMS の取得及び更新に必須となる基本文書（上位文書）のサンプルです。

JISQ27001:2023 にも対応しています。

ページ最後の購入方法をご確認ください。修正可能なワードファイルで提供しています。

【編集可能！】 ISMS マニュアル：2022 対応版

J I S Q 2 7 0 0 1 : 2 0 2 3 適 用

(I S O / I E C 2 7 0 0 1 : 2 0 2 2)

| | |
|-----|-----|
| 承 認 | 作 成 |
| | |

株式会社 サンプル

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

目 次

| | |
|--------------------------------|-----|
| 1. 適用範囲 | P5 |
| 2. 引用規格 | P6 |
| 3. 用語及び定義 | P6 |
| 4. 組織の状況 | P7 |
| 4.1 組織及びその状況の理解 | P7 |
| 4.2 利害関係者のニーズ及び期待の理解 | P7 |
| 4.3 情報セキュリティマネジメントシステムの適用範囲の決定 | P7 |
| 4.4 情報セキュリティマネジメントシステム | P7 |
| 5. リーダーシップ | P8 |
| 5.1 リーダーシップ及びコミットメント | P8 |
| 5.2 方針 | P8 |
| 5.3 組織の役割、責任及び権限 | P10 |
| 5.3.1 推進組織 | P10 |
| 5.3.2 権限と役割 | P11 |
| 6. 計画策定 | P12 |
| 6.1 リスク及び機会に対処する活動 | P12 |
| 6.1.1 一般 | P12 |
| 6.1.2 情報セキュリティリスクアセスメント | P12 |
| 6.1.3 情報資産の洗い出し | P14 |
| 6.1.4 情報資産台帳の作成 | P14 |
| 6.1.5 リスクの特定 | P15 |
| 6.1.6 リスクの分析及び評価 | P15 |
| 6.1.7 リスク対応の選択 | P17 |
| 6.1.8 管理策の選択 | P17 |
| 6.1.9 適用宣言書の作成 | P17 |
| 6.1.10 リスク対応計画の作成 | P17 |
| 6.1.11 リスク対応計画及び残留リスクの承認 | P18 |
| 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 | P19 |
| 6.3 変更の計画策定 | P19 |

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

| | |
|-------------------------|-----|
| 7. 支援 | P20 |
| 7.1 資源 | P20 |
| 7.2 力量（教育訓練） | P20 |
| 7.2.1 要求される力量 | P20 |
| 7.2.2 教育訓練計画 | P20 |
| 7.2.3 実施した教育訓練の評価 | P21 |
| 7.2.4 教育訓練記録の保持 | P21 |
| 7.3 認識 | P21 |
| 7.4 コミュニケーション | P21 |
| 7.4.1 内部コミュニケーション | P21 |
| 7.4.2 外部コミュニケーション | P22 |
| 7.5 文書化した情報 | P23 |
| 7.5.1 一般 | P23 |
| 7.5.2 作成及び更新（改訂） | P23 |
| 7.5.3 文書化した情報の管理 | P24 |
| 8. 運用 | P25 |
| 8.1 運用の計画策定及び管理 | P25 |
| 8.2 情報セキュリティリスクアセスメント | P25 |
| 8.3 情報セキュリティリスク対応 | P25 |
| 9. パフォーマンス評価 | P26 |
| 9.1 監視、測定、分析及び評価 | P26 |
| 9.1.1 社員による点検 | P26 |
| 9.1.2 管理策の有効性測定 | P27 |
| 9.1.3 ISMS の有効性測定 | P27 |
| 9.2 内部監査 | P27 |
| 9.2.1 内部監査の目的 | P27 |
| 9.2.2 内部監査プログラム | P27 |
| 9.2.3 内部監査員の選定 | P27 |
| 9.2.4 内部監査の手順 | P28 |
| 9.3 マネジメントレビュー | P29 |
| 9.3.1 マネジメントレビューの実施 | P29 |
| 9.3.2 マネジメントレビューのインプット | P29 |
| 9.3.3 マネジメントレビューのアウトプット | P29 |
| 9.3.4 マネジメントレビューの記録 | P29 |

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

- 10. 改善 P30
 - 10.1 継続的改善 P30
 - 10.2 不適合及び是正処置 P30

改訂歴表

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

1 適用範囲

当社は、「情報セキュリティ、サイバーセキュリティ及びプライバシー保護-情報セキュリティマネジメントシステム-要求事項」(以下 ISO27001) に準拠した情報セキュリティを構築する。

本マニュアルは、当社の ISMS の確立、導入、運用、監視、見直し、維持及び改善の枠組みを規定する。

(1) 適用事業

- ・ソフトウェア受託開発
- ・パッケージソフトウェア開発・販売・保守・導入支援
- ・ハードウェア受託開発

(2) 適用組織

別紙、組織図で示す組織

(3) 適用事業所

- 【事業所名】 ○○ 【事業所住所】 ○○
 【事業所名】 ○○ 【事業所住所】 ○○

(4) 適用範囲から除外される業務

適用範囲内でありながらその一部を適用除外する場合、その内容と除外する正当な理由を明示する。

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

2 引用規格

JISQ27000:2019/ISO27000:2018 「情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-用語」

3 用語及び定義

本マニュアルに関する用語の定義は、JISQ27000:2019 に従うが、定義が必要なものについては、下記に定義する。

- (1) 従業員：当法人の役員、社員、契約社員、嘱託、パート、アルバイトを含む ISMS 適用範囲内の全社員
- (2) 経営陣：社長及び役員
- (3) ISMS 推進委員会：情報セキュリティの施策を審議し、決定する委員会

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

4 組織の状況

4.1 組織及びその状況の理解

ISMS 推進委員会は、毎年 4 月に、組織の目的に関連し、かつ情報セキュリティマネジメントシステム (ISMS) の意図した成果を達成する能力に影響を与える、外部及び内部の課題を決定し、「リスク一覧表」に示す。また、これらの課題は、必要に応じて、適宜見直しを行う。

4.2 利害関係者のニーズ及び期待の理解

ISMS 推進委員会は、顧客等をはじめとする利害関係者を特定し、それらの要求事項および法的及び規制要求事項を以下に示し、決定する。また、それらの要求事項のうち、ISMS を通して取り組むもの (情報セキュリティ教育等) も決定する。

| 利害関係者 | 情報セキュリティに関する要求事項 |
|-------|---|
| 顧客 | 契約上の義務 (契約書) 情報の機密性・完全性・可用性の確保 |
| 従業員 | 業務情報の機密性・完全性・可用性の確保 情報セキュリティに関する教育の機会 個人情報の保護 |
| 政府・行政 | 情報セキュリティに関する法令 (法的要求事項登録簿) |

4.3 情報セキュリティマネジメントシステム (ISMS) の適用範囲の決定

当社は、適用範囲を決定する場合、以下の事項を考慮して、適用範囲を決定し、決定した適用範囲は、文書化した情報として利用可能な状態にしておく。

- (1) 4.1 に規定する外部及び内部の課題
- (2) 4.2 に規定する要求事項
- (3) 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

4.4 情報セキュリティマネジメントシステム (ISMS)

当社は、ISO27001:2022 (JISQ27001:2023) 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 (ISMS) を確立し、実施し、維持し、かつ継続的に改善を行う。詳細については、以下の章に基づき規定する。

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

5 リーダーシップ

5.1 リーダーシップ及びコミットメント

社長は、以下の事項によって、情報セキュリティマネジメントシステム (ISMS) に関するリーダーシップ及びコミットメントを実証する。

- (1) 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。
- (2) 組織の事業プロセスへの情報セキュリティマネジメントシステム (ISMS) 要求事項への統合を確実にする。
- (3) 情報セキュリティマネジメントシステム (ISMS) に必要な経営資源が利用可能であることを確実にする。
- (4) 有効な情報セキュリティマネジメント及び情報セキュリティマネジメントシステム (ISMS) 要求事項への適合の重要性を伝達する。
- (5) 情報セキュリティマネジメントシステム (ISMS) がその意図した成果を達成することを確実にする。
- (6) 情報セキュリティマネジメントシステム (ISMS) の有効性に寄与するよう社員を指揮し、支援する。
- (7) 継続的な改善を促進する。
- (8) その他の関連する管理者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、その管理者の役割を支援する。

5.2 方針

社長は、以下の事項を満たす「**情報セキュリティ基本方針**」を制定し、文書化して利用可能とし、組織内に伝達する。また、必要に応じて、利害関係者が入手可能であるようにする。

- (1) 組織の目的に対して適切である。
- (2) 情報セキュリティ目的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。
- (3) 情報セキュリティに関連して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。
- (4) 情報セキュリティマネジメントシステム (ISMS) の継続的改善へのコミットメントを含む。

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

IS-A-01

情報セキュリティ基本方針

制定：2023年10月01日
最終改訂日：2023年〇月〇日

【基本理念】

株式会社●●は、コスト削減や業務効率向上を図るには IT は欠かせないツールであり、その IT の活用において、情報セキュリティの確保が重要課題の一つであると考えます。本方針は、当社の情報セキュリティマネジメントシステム (ISMS) を適切に構築し、継続的で有効性のある運用を確保するために、以下に情報セキュリティ基本方針を制定します。

【基本方針】

1. 情報資産の機密性、完全性、可用性を確実に保持するため、予防並びに是正に努め、組織的、技術的に適切な管理策を策定し、実施します。
2. 情報セキュリティ基本方針を具体的に実行するため、情報セキュリティ目標を設定し、その達成のための活動を行い、情報セキュリティ委員会で検証を行います。
3. 関連する法規制要求事項および契約上のセキュリティ事項を順守します。
4. 経営陣および従業員は情報セキュリティの重要性を認識するように、教育・訓練を受講し、高いモラル意識を持って作業に従事します。
5. 本「情報セキュリティ基本方針」および関連する諸規則、管理体制の評価、見直しを定期的に行うことで、情報セキュリティを運営管理する仕組みの継続的な改善を図ります。

以 上

株式会社 ●●
代表取締役社長 ●●

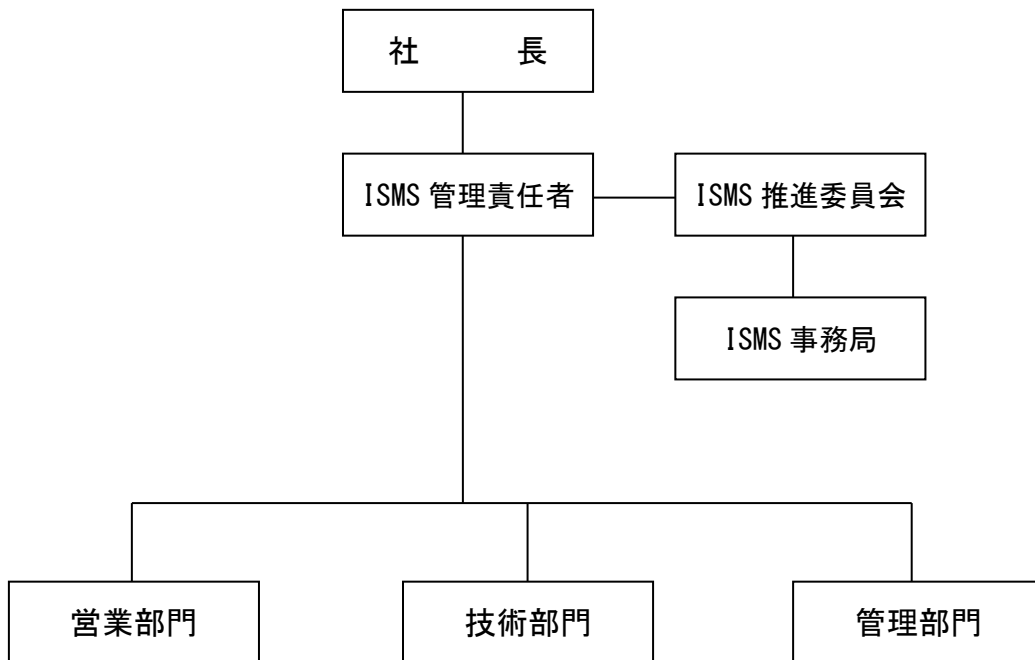
| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

5.3 組織の役割、責任及び権限

社長は、関連する役割に対して、以下のような責任及び権限を割り当て、組織内に伝達することを確実にする。

5.3.1 推進組織

情報セキュリティマネジメントシステム（ISMS）を推進するための組織を以下に定める。



| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

5.3.2 権限と役割

情報セキュリティマネジメントシステム (ISMS) を推進するための権限と役割を以下に定める。

| ISMS 上の名称 | 権限と役割 | 備考 |
|-------------------------------|---|--------------------------------------|
| 社長 | (1)ISMS における最高責任者。 (2)ISMS 管理責任者、内部監査責任者を任命する。 (3)ISMS 基本方針を確立し、維持する。 (4)ISMS の確立、導入、運用、監視、見直し、維持、及び改善に十分な経営資源を提供する。 (5)リスクを受容するための基準、及び受容可能なリスクの水準を決める。 (6)ISMS のマネジメントレビューを実施する。 | — |
| ISMS 管理責任者 (情報セキュリティ管理責任者) | (1)本マニュアルに従った情報セキュリティマネジメントシステムの推進に責任を持つ。 (2)社長による見直しのための参考資料及び情報セキュリティマネジメントシステムの改善の基礎として、社長に情報セキュリティマネジメントシステムの実績を報告する。 (3)ISMS 推進委員と ISMS 事務局員を任命する。 (4)ISMS 推進委員会を主宰する。 (5)ISMS の目的が設定され、計画が策定されることを確実にする。 (6)情報セキュリティに対する役割及び責任を定める。 (7)情報セキュリティ目的を達成することの重要性及び情報セキュリティ基本方針に適合することの重要性、当社の法的責任、ならびに継続的改善の必要性を組織内に周知する。 (8)ISMS の内部監査が実施されることを確実にする。 (9)ISMS が ISO27001 の規格要求事項に適合することを確実にする。 | 社長により任命される。 |
| ISMS 推進委員会 (情報セキュリティ推進委員会) | 当社の情報セキュリティマネジメントシステム推進のための連絡及び各部門間の調整を行う。 | ISMS 推進委員会のメンバーは ISMS 管理責任者により任命される。 |
| ISMS 事務局 (管理部門) | ISMS 管理責任者の指示に従い、情報セキュリティマネジメントシステムの推進のための実務を行う。 | — |
| 内部監査責任者 | 内部監査プログラムを立案し、内部監査チームリーダー及びメンバーを選定する。監査結果を社長に報告する。 | 社長により任命される。 |
| システム管理責任者 | 社内システム及びネットワークの構築、運用、保守に責任を持つ。 | ISMS 管理責任者により任命される。 |
| 各部門長 | (1)部門員に対して、本 ISMS マニュアルをはじめ、情報セキュリティ手順を順守させること。 (2)部門の情報セキュリティの実施状況を日常的に点検し、改善に努めること。 | — |

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

6 計画策定

6.1 リスク及び機会に対処する活動

6.1.1 一般

ISMS の計画を策定するとき、前項 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、以下の事項について対処する必要があるリスク及び機会を決定し、「リスク一覧表」に記入する。

- (1) ISMS が、その意図した成果を達成できることを確実にする。
- (2) 望ましくない影響を防止、又は低減する。
- (3) 継続的改善を達成する。
- (4) 決定したリスク及び機会に対処する活動を計画する。
- (5) 計画された活動は、ISMS プロセスへの統合及び実施を行う。
- (6) 計画された活動の有効性評価を行う。

6.1.2 情報セキュリティリスクアセスメント

- (1) リスクアセスメント手法

6.1.2 以下に示す方法でリスクアセスメントを実施する。

- (2) リスク受容の基準

当社は下記の考え方で、リスクを受容する。

- ① 6.1.5 で計算したリスク値が「6」以下のリスクは受容（保有）する。
- ② リスク値が「8」「9」の場合は、該当する情報資産、脅威を考慮して状況に応じて、受容するか否かを決定する。
- ③ リスク値が「10」以上の場合、6.1.5 に記すように、「管理策を採用し、リスクを低減する」「リスクを移転する」、あるいは「リスクを回避する」対応をとり、リスク値を「6」以下に低減する。
- ④ リスク値が「10」以上で、リスク値を受容水準以下に低減させることが、事業上の理由により不可能である場合は、ISMS 推進委員会でその受容の可否を審議し、組織としてそのリスクを受容する。

リスク受容基準

| 脅威のレベル ぜい弱性のレベル | | 1 | | | 2 | | | 3 | | |
|--------------------|---|---|---|----|---|----|----|----|----|----|
| | | 1 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 3 |
| 事業に与える損害 | 1 | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| | 2 | 4 | 6 | 8 | 6 | 8 | 10 | 8 | 10 | 12 |
| | 3 | 6 | 9 | 12 | 9 | 12 | 15 | 12 | 15 | 18 |

原則受容

受容可能

リスク対応

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

6.1.7 リスク対応の選択

ISMS 事務局又は ISMS 推進委員会のメンバーは、リスク値が「10」以上のリスク、及びリスク値が「8」「9」であっても受容できないと判断したリスクについては、以下の3つの対応策の中から一つを選択し、「**リスクアセスメント結果表**」に記入する。

- (1) 管理策を採用し、リスクを低減する。
- (2) リスクを共有する。十分な対策がとれない場合は、保険をかけるか、その業務を適用範囲外の組織に業務委託する。
- (3) リスクを回避する。当該業務を廃止するか、あるいはその資産（装置）の使用を止める。

6.1.8 管理策の選択

- (1) 必要な管理策の選択

ISMS 事務局又は ISMS 推進委員会のメンバーは、以下の事項に当てはまる適切な管理策を ISO27001:2022 の附属書 A 情報セキュリティ管理策の中から採用し、ISMS 管理責任者の承認を得る。適切な管理策がない場合は、新たに管理策を立案し、追加を行う。必要な管理策が見落とされていないかどうかは、ISMS 推進委員会で検証を行う。

- ① リスクアセスメントの結果から採用する管理策
- ② 情報セキュリティ対応の選択肢の実施に必要な全ての管理策

- (2) 残留リスクの明確化とリスク低減ができない場合の対応

ISMS 事務局又は ISMS 推進委員会のメンバーは、リスクごとに管理策を採用した後のリスク値を計算し、「**リスクアセスメント結果表**」に残留リスクとして記入する。リスクが受容水準以下に低減しない場合には、管理策を追加してリスク値を受容水準以下に低減する。管理策を適用してもリスクが受容水準以下への低減が期待できない場合は下記により対応を決定する。

- ① そのリスクが顕在化した場合に、組織が対外的に責任を果たせないと判断した場合は当該業務を移転するか、廃止する。
- ② そのリスクが顕在化した場合に、その被害が自組織内に限定される場合、リスク所有者の明確な承認のもとに、当該リスクを保有することができる。

6.1.9 適用宣言書の作成

ISMS 事務局は、採用した管理策を示した「**適用宣言書**」を作成する。なお、採用した管理策の採用理由及び除外した管理策の除外理由、管理策の実施の有無も明確にする。

6.1.10 リスク対応計画の作成

ISMS 事務局は、リスクアセスメントの結果受け、以下の項目を考慮し、「**リスク対応計画書**」を作成する。

- (1) 具体的な対策
- (2) 実施責任者
- (3) 計画に必要な要員とコスト

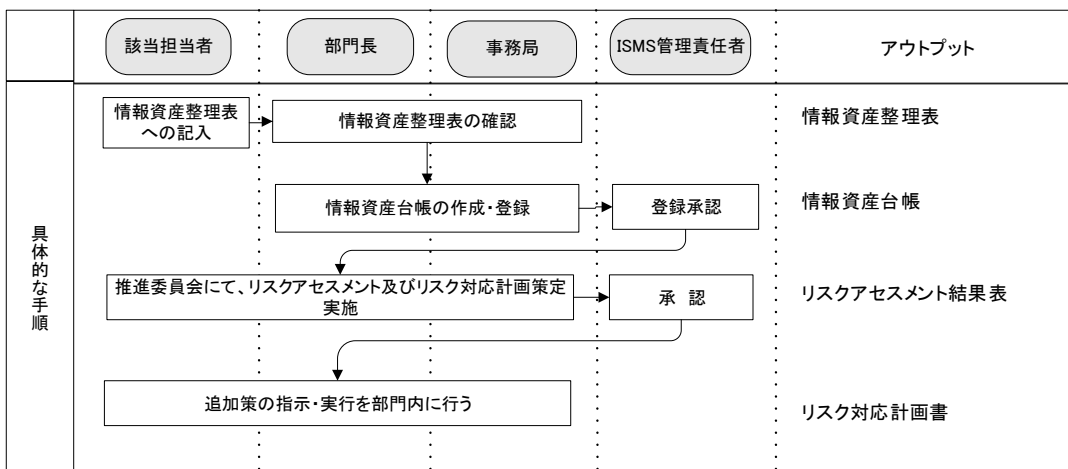
| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

- (4) 計画が複数ある場合はその優先順位
- (5) スケジュール

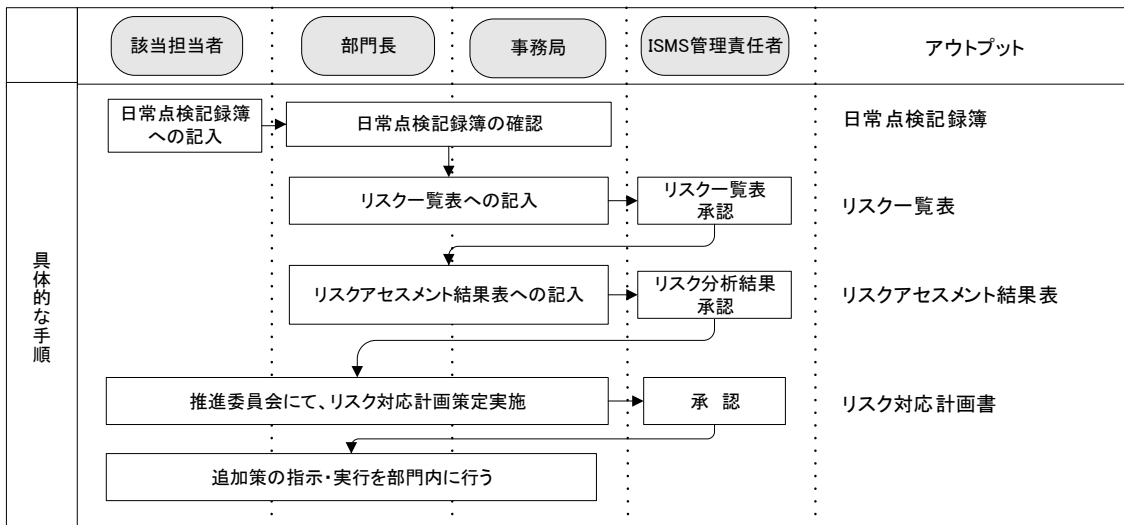
6.1.11 リスク対応計画及び残留リスクの承認

ISMS 事務局は、作成したリスク対応計画及び残留リスクに対してリスク所有者から承認を得る。

参考図 1：新たな情報資産の追加・変更時の対応



参考図 2：業務手順の見直し・変更等、リスク変化によるリスク見直し時の対応



| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

7.5 文書化した情報

7.5.1 一般

当社における情報セキュリティマネジメントシステム (ISMS) は、以下の事項を確実にする。

- (1) ISO27001:2022 (JISQ27001:2023) の規格が要求事項する文書化された情報
- (2) 情報セキュリティマネジメントシステム (ISMS) の有効性のために必要であると当社が決定した、文書化された情報

7.5.2 作成及び更新 (改訂)

文書の作成、承認及び文書番号の付与は以下の表の通りとする。

なお、様式 (文書 B) の保管期限、保管場所については、「ISMS 様式集」に記す。

| 文書分類 | 文書名 | 文書番号 | 起案 (作成・改訂) | 承認 |
|--------------|--------------------|-----------|---------------|------------|
| 文書 A | 情報セキュリティ基本方針 | ISMS-A-01 | ISMS 管理責任者 | 社長 |
| | 適用宣言書 | ISMS-A-02 | ISMS 管理責任者 | 社長 |
| | ISMS マニュアル | ISMS-A-03 | ISMS 管理責任者 | 社長 |
| | ISMS 管理策運用規定 | ISMS-A-04 | ISMS 管理責任者 | 社長 |
| | ISMS 様式集 | ISMS-A-05 | ISMS 管理責任者 | 社長 |
| 文書 B (様式) | 情報資産台帳 | ISMS-B-01 | ISMS 事務局 | ISMS 管理責任者 |
| | リスクアセスメント結果表 | ISMS-B-02 | ISMS 事務局 | ISMS 管理責任者 |
| | リスク対応計画書 | ISMS-B-03 | ISMS 事務局 | 社長 |
| | 法的要求事項登録簿 | ISMS-B-04 | ISMS 事務局 | 社長 |
| | 事業継続リスクアセスメント | ISMS-B-05 | ISMS 事務局 | ISMS 管理責任者 |
| | 事業継続計画書 | ISMS-B-06 | ISMS 事務局 | 社長 |
| | 事業継続計画テスト結果記録 | ISMS-B-07 | ISMS 事務局 | 社長 |
| | 年間教育計画表 | ISMS-B-08 | ISMS 事務局 | ISMS 管理責任者 |
| | 教育訓練実施報告書 | ISMS-B-09 | ISMS 事務局 | ISMS 管理責任者 |
| | 管理策測定評価表 | ISMS-B-10 | ISMS 事務局 | ISMS 管理責任者 |
| | ISMS の有効性レビュー実施結果表 | ISMS-B-11 | ISMS 事務局 | ISMS 管理責任者 |
| | セキュリティインシデント報告書 | ISMS-B-12 | ISMS 事務局 | ISMS 管理責任者 |
| | 情報セキュリティ事象記録簿 | ISMS-B-13 | ISMS 事務局 | ISMS 管理責任者 |
| | 入退室管理票 (外部・従業員) | ISMS-B-14 | ISMS 事務局 | ISMS 管理責任者 |
| | 機密保持誓約書 | ISMS-B-15 | ISMS 事務局 | 社長 |
| | 個人情報取扱いに関する同意書 | ISMS-B-16 | ISMS 事務局 | 社長 |
| | 新規委託先評価表 | ISMS-B-17 | ISMS 事務局 | ISMS 管理責任者 |
| | 委託先継続評価表 | ISMS-B-18 | ISMS 事務局 | ISMS 管理責任者 |
| | 委託先管理台帳 | ISMS-B-19 | ISMS 事務局 | ISMS 管理責任者 |
| | 内部監査実施計画書 | ISMS-B-20 | ISMS 事務局 | ISMS 管理責任者 |
| | 内部監査員登録台帳 | ISMS-B-21 | ISMS 事務局 | ISMS 管理責任者 |
| | 内部監査チェックリスト | ISMS-B-22 | ISMS 事務局 | ISMS 管理責任者 |
| | 内部監査報告書 | ISMS-B-23 | ISMS 事務局 | ISMS 管理責任者 |
| | 是正処置に関する報告書 | ISMS-B-24 | ISMS 事務局 | ISMS 管理責任者 |
| | ISMS マネジメントレビュー議事録 | ISMS-B-25 | ISMS 事務局 | ISMS 管理責任者 |
| | 情報セキュリティ目標管理表 | ISMS-B-26 | ISMS 事務局 | ISMS 管理責任者 |
| | リスク一覧表 | ISMS-B-27 | ISMS 事務局 | ISMS 管理責任者 |

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

8 運用

8.1 運用の計画及び管理

当社は、以下に示す事項によって、情報セキュリティに関する要求事項を満たすため、及び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、管理を行う。

- ① プロセスに関する基準の設定
- ② その基準に従ったプロセスの管理の実施

また、プロセスが計画通りに実施されたという確信を持つために必要とされる、文書化した情報（規定した情報セキュリティ関連文書）を利用可能な状態（必要とする者が、必要な時に利用できること）にし、計画した変更は管理し、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ずる（これには外部に委託したプロセス、製品又はサービスも含む）。

8.2 情報セキュリティリスクアセスメント

ISMS 事務局又は ISMS 推進委員会のメンバーは、毎年、4月に、該当部門の協力を得て、リスクアセスメントの見直しを実施する。また、以下の事項が生じた場合も見直しを実施する。

- ① 情報資産台帳に新たな情報資産が追加されたとき
- ② 組織の大幅な変更（組織の新設、統廃合、場所の移転）
- ③ 提供する製品、サービスの変更
- ④ 業務の進め方の変更
- ⑤ 新たな脅威、脆弱性を認識したとき
- ⑥ 外部環境、例えば新たな法律の制定
- ⑦ 外部及び内部の課題の変化
- ⑧ 顧客等利害関係者の要求事項の変化

なお、リスクアセスメントの結果、必要に応じ「リスクアセスメント結果表」「適用宣言書」「リスク対応計画書」を改訂し、ISMS 管理責任者の承認を得る。

8.3 情報セキュリティリスク対応

実施責任者は、「リスク対応計画書」に記載されている計画を実施する。

また、ISMS 事務局は、月1回、「リスク対応計画書」の進捗状況をチェックして、記録し、計画に遅延または障害が生じた場合は、実施責任者と対応を協議する。

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

10 改善

10.1 継続的改善

当社は、情報セキュリティマネジメントシステム（ISMS）の適切性、妥当性及び有効性を継続的に改善するために、以下の活動を行う。

- (1) ISMS の実施状況の監視、見直し結果（外部／内部監査結果、日常点検、セキュリティインシデントの反省、顧客要求など）に基づく是正処置の実施
- (2) 当社 ISMS の枠組みについての見直しによる改善（マネジメントレビュー、文書の見直し）
- (3) セキュリティ目標の達成と、さらなるセキュリティレベルの向上を目指した目標の設定
- (4) 外部及び内部の課題の変化に即応したリスク対応（リスクアセスメント、リスク対応計画の見直しなど）

10.2 不適合及び是正処置

各該当部門の該当者は、不適合が発生した場合、以下の事項を実施し、「**是正処置に関する報告書**」に、その結果を記録し、保持する。

- (1) その不適合を特定し、該当する場合には、必ず次の事項を実施する。
 - 1) その不適合を管理し、修正するための処置をとる
 - 2) その不適合によって起こった結果に対処する
- (2) その不適合の再発又は他のところで発生しないようにするため、次の事項を実施し、その不適合の原因を除去するための処置をとる必要性を評価する。
 - 1) その不適合のレビュー
 - 2) その不適合の原因の明確化
 - 3) 類似の不適合の有無又はそれが発生する可能性の明確化
- (3) 必要な処置を実施する。
- (4) とった全ての是正処置の有効性をレビューする。
- (5) 必要な場合には、情報セキュリティマネジメントシステム（ISMS）の変更を行う。

| | | |
|---------------------|------------------|----------------|
| (株) サンプル ISMS マニュアル | 制定日 2023. 10. 01 | 文書番号 ISMS-A-03 |
| | 改訂日 | 改訂番号 1 |

ISO/IEC27001:2022 に完全対応した ISMS マニュアルサンプルを有料にて、ワードファイルで提供中です。有料版には、掲載した目次のすべてが含まれています。

提供価格：16,500 円（税込）

購入方法：

1. 下記のホームページのお問い合わせにて、Eメールで購入のご連絡をお願い致します。
→ <https://www.iso-mi.com/>
ご要望欄に、「ISMS マニュアル 2022 購入希望」ご記入ください。
2. 当事務所にメールが届き、確認次第、請求書と共に入金口座をお知らせ致します。なお、振り込み手数料については、ご負担頂けますようお願い致します。
3. ご入金を確認でき次第、Eメールにて納品致します。領収書が必要な場合は、お申し出ください。※また、納品したファイルが開けない、破損している場合は、その旨をご連絡下さい。交換致します。その他ご質問等は下記のメールアドレスにてお願い致します。

注意事項：

1. 本商品（ISMS マニュアル 2022）を転売する等の商用利用※を禁止致します。 ※商用利用とは、顧客等へのコンサルツールの利用も含みます。
2. 本商品（ISMS マニュアル 2022）にあるサンプル文例は、あくまでもサンプルですので、実際の文面は、必ず自社の実態にあったものをお書きください。
3. 個人（顧問を含む）やコンサルタント事業者様、士業様には、ご購入は、ご遠慮頂いております。