情報セキュリティ運営管理規程

株式会社 ●●●●

目次

1　総則

1.1　規程の位置付け

本規程は、情報セキュリティマネジメントシステムの基本規程である「**ISMS マニュアル**」に基づき、当組織における情報セキュリティマネジメントシステム（以下、ISMS と言う）の運用について定めた規程である。

1.2　目的

本規程は、当組織における ISMS の体制及び責任を定め、ISMS の運用形態を明確にする事を目的とする。

1.3　適用範囲

「ISMS マニュアル－1.2　適用」で行われる ISMS の運用管理に適用される。

1.4　対象者

「ISMS マニュアル－1.2　適用」で定める当組織のすべての社員等とする。

1.5　用語の定義

本規程内で用いる用語の定義は「**ISMS 用語集**」に従う。

2　組織

ISMS 管理体制及び指示系統を以下に示す。

2.1 管理体制と指示系統

ISMS に関する管理体制及び指示系統を明確にするために、相互関係を「**ISMS 推進体制図**」に示す。

2.2 役割及び責任（A.5.2）

(1) 情報セキュリティ委員長

- 当組織の ISMS 推進における最高責任と権限を有する。
- 情報セキュリティ委員会における、最終決定権を有する。
- マネジメントレビューを実施する。
- 情報セキュリティ推進責任者を任命する。
- 情報セキュリティ管理者を任命する。
- 情報セキュリティアドバイザを任命する。
- その他、情報セキュリティに関する、緊急時の判断を行う。

(2) 情報セキュリティ推進責任者

- ISMS を実施、維持運用するための責任と権限を有する。
- 情報セキュリティ委員長にかわり、関連担当者への指示及び協力を要請する。
- ISMS の実施状況を、情報セキュリティ委員長に報告する。
- 特例措置の承認を行う。
- ISMS の年間計画を記載した「**年間情報セキュリティ計画書**」の作成。
- ISMS が JIS Q 27001:2023（ISO/IEC 27001:2022）及び JIS Q 27001:2023/AMENDMENT 1:2025（ISO/IEC 27001:2022/Amd 1:2024）の規格要求事項に適合していることを確実にする。
- ISMS のパフォーマンスを情報セキュリティ委員長に報告する。

(3) 情報セキュリティアドバイザ

- 情報セキュリティ委員長より任命を受け、ISMS のネットワーク運用（社内 LAN）に関して、専門的な観点から、アドバイスを行う。
- 情報セキュリティの事件・事故に早急に対応するために関係各所と連携を図る。

(4) 情報セキュリティ内部監査員

- 情報セキュリティ委員長から任命を受け、ISMS の運用状況の内部監査を実施する。

(5) 情報セキュリティ推進事務局

- ISMS に関する推進や調整を行う。
- ISMS の運用・監査・是正に関する事務を実施する。
- マネジメントレビューの対応を行う。
- 情報セキュリティ委員会の事務を行う。

・ 情報セキュリティに関する連絡窓口業務を行う。
・ 情報セキュリティに関する教育訓練の実施。

(6) 情報セキュリティ管理者
・ ISMS 運用に関する当組織内の社員等への支援及び、各グループの総括管理を行う。（部門及び階層の長）
・ 情報セキュリティ委員会に参加する。
・ 組織の外部及び内部、利害関係者のニーズ及び期待が定められた「**ISMS 組織状況管理表**」を、社員等へ周知する。（4.1 及び 4.2 参照）

(7) 社員等
・ 情報資産のセキュリティ対策を実施する。
・ 情報セキュリティ事件・事故を報告する。
・ ISMS マニュアル及び各種規程を遵守する。
・ 「**情報セキュリティ基本方針書**」を遵守する。

2.3 職務の分離（A.5.3）

不注意又は故意によるシステムの誤用のリスクを軽減するため、責任領域の管理もしくは、実行の分離を行う。職務の分離については、次に示す内容を考慮する。

(1) 確認者と実施者は別々の人とする。
(2) 組織上困難と考えられる場合でも、職務の分離に努める。
(3) 困難な場合は、行動の監視、監査ログの採取、管理行為に対する監視を行う。
(4) 監査業務は完全に独立性を保障する。

3 内部コミュニケーション

(1) 情報セキュリティ委員会

a) 内容	ISMS の有効性と適切性のレビュー、及び「ISMS マニュアル」に関する事項の審議が行われる場として開催する。 情報セキュリティ委員会で審議される事項に関する最終決定権及び最終責任は、情報セキュリティ委員長にある。
b) 実施時期	原則年●回（●●月、●●月）に開催する。但し、情報セキュリティ委員長が必要と判断した場合は、随時開催する。
c) 対象者	・情報セキュリティ推進責任者、各部門の情報セキュリティ管理者。 ・情報セキュリティ委員会の運営事務は、情報セキュリティ推進事

	務局が行う。 ・情報セキュリティ委員長の判断により、関連するメンバーの出席を可能とする。
d) 実施者（主催者）	情報セキュリティ委員長
e) 実施プロセス	会議形式

(2) プロジェクト会議

a) 内容	ISMS 運用全般に関する運用状況。
b) 実施時期	原則、1 回/月
c) 対象者	・プロジェクトの関係者
d) 実施者（主催者）	情報セキュリティ委員長
e) 実施プロセス	会議形式

4 情報処理設備の認可手続き

新規の情報処理設備または、既存設備の変更は、セキュリティ上の有効性、経済性、ポリシーとの整合性を考慮し、認可を行うため以下の内容を実施する。

(1) 社員等は ISMS に影響があると考えられる情報処理設備もしくはソフトウェアを購入する場合、「**稟議書**」を作成し情報セキュリティ管理者に ISMS への影響評価の依頼を行なければならない。

(2) 情報セキュリティ管理者は、「**リスクマネジメント管理規程**」に従いリスク評価を行う。

(3) リスク値が受容レベル以上になった場合は、再検討が必要として、依頼者に差し戻しを行う。

(4) 依頼者は、購入の再検討を行う。

(5) 依頼者は、再検討後、購入が必要と判断された場合は、情報セキュリティ管理者にリスク対応策の検討を依頼する。

(6) 情報セキュリティ管理者は、リスク対応策を検討した結果、ISMS への影響が大きい場合は、リスク対応策を情報セキュリティ推進責任者の承認を得なければならない。

(7) 情報セキュリティ推進責任者は、ISMS 全体の影響評価を行い、影響が大きいと判断した場合は、差し戻すか、もしくは情報セキュリティ委員長に報告を行い承認する。

5 組織間の協力

5.1 関係当局及び専門組織との連携（A.5.5 / A.5.6）

情報セキュリティ委員会はセキュリティ関連組織と密接な連携を行う。カテゴリー、対象先及び情報セキュリティ委員会窓口を以下に示す。

各情報セキュリティ委員会窓口は、ISMS を運営、維持するのに必要な情報を入手するため、対象先へ定期的に確認を行う。

カテゴリー	対象先	情報セキュリティ委員会窓口
法律、規制	●●部　（御社での担当部署）	情報セキュリティ推進事務局
契約によるセキュリティ要求事項	●●部　（御社での担当部署）	情報セキュリティ推進事務局
採用、懲戒	●●部　（御社での担当部署）	情報セキュリティ推進事務局
セキュリティ教育	●●部　（御社での担当部署）	情報セキュリティ推進事務局
コンピュータウィルス	アンチウィルスベンダー	情報セキュリティアドバイザ
セキュリティ情報	IPA/ISEC、JPCERT	情報セキュリティアドバイザ

5.2 プロジェクトマネジメントにおける情報セキュリティ（A.5.8）

5.2.1 一般

プロジェクトの種類にかかわらず、プロジェクト長は、情報セキュリティリスクがプロジェクトの中で特定及び対処されることを確実にするために，情報セキュリティを組織のプロジェクトマネジメント手法に組み入れること。

次の事項を含めること。

(1) 情報セキュリティ目的をプロジェクトの目的に含める。
(2) 必要ならば、プロジェクトに必要な管理策を特定するため、情報セキュリティリスクアセスメントを実施する。

5.2.2 セキュリティ要求事項の分析及び仕様化

新しいシステム又は既存のシステムの改善に関する業務上の要求事項を記述した文書のセキュリティ要求事項については、以下に示す内容を考慮し仕様化する。