ISMS マニュアル

株式会社 ●●●●

目次

1 適用範囲 1
1.1 目的 1
1.2 適用 1
2 引用規格 1
3 用語の定義 2
4 組織の状況 2
4.1 組織及びその状況の理解 2
4.2 利害関係者のニーズ及び期待の理解 3
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 3
4.4 情報セキュリティマネジメントシステム 3
5 リーダーシップ 4
5.1 リーダーシップ及びコミットメント 4
5.2 方針 4
5.3 組織の役割，責任及び権限 5
6 計画策定 5
6.1 リスク及び機会に対処する活動 5
6.1.1 一般 5
6.1.2 情報セキュリティリスクアセスメント 6
6.1.3 情報セキュリティリスク対応 6
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 7
6.3 変更の計画策定 8
7 支援 8
7.1 資源 8
7.2 力量 8
7.3 認識 9
7.4 コミュニケーション 9
7.5 文書化した情報 9
7.5.1 一般 9
7.5.2 作成及び更新 10
7.5.3 文書化した情報の管理 10
8 運用 11
8.1 運用の計画及び管理 11
8.2 情報セキュリティリスクアセスメント 11
8.3 情報セキュリティリスク対応 11
9 パフォーマンス評価 12
9.1 監視，測定，分析及び評価 12
9.2 内部監査 12

9.2.1 一般 12
9.2.2 内部監査プログラム 13
9.3 マネジメントレビュー 13
9.3.1 一般 13
9.3.2 マネジメントレビューへのインプット 13
9.3.3 マネジメントレビューの結果 14
10 改善 15
10.1 継続的改善 15
10.2 不適合及び是正処置 15
11 改訂履歴表 16

1 適用範囲

1.1 目的

お客様から信頼される情報流通企業として、お客様情報のセキュリティに関するインシデントの防止を図ることにより、お客様の信頼確保及び事業損失を最小限に留めることを目的とする。

（情報セキュリティ基本方針書の目的を挿入する。）

1.2 適用

(1) 適用範囲

組織	：	※※※株式会社
施設	：	本社　〒111-1111　東京都千代田区千代田 1-1-1
		※※支店　〒222-2222　東京都中央区中央 2-2-2
対象者	：	社長、役員、下記、“業務”に携わる全社員
業務	：	※※の開発および※※の管理業務
資産	：	上記業務、サービスにかかわる書類、データ、●●情報システム
ネットワーク	：	全社ネットワーク

(2) 適用除外項目

除外項目	：	なし（除外項目がある場合はその項目を記述する。）
除外理由	：	なし（除外した理由を記述する。）

2 引用規格

(1) 国際規格

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－要求事項
JIS Q 27001:2023（ISO/IEC 27001:2022）
情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項（追補１）
JIS Q 27001:2023/AMENDMENT 1:2025

(2) 引用規格

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
JIS Q 27000：2019

3 用語の定義

情報セキュリティマネジメントシステム（以下、「ISMS」という）に関する用語は JIS Q 27000：2019 の定義を引用する。

その他の用語については「ISMS 用語集」に示す。

4 組織の状況

4.1 組織及びその状況の理解

当組織は、情報セキュリティ委員会において、組織の目的に関連し、かつ 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、気候変動が関連する課題かどうかを踏まえて決定し、「**ISMS 組織状況管理表**」にまとめ、関係者へ周知する。（4.3 及び 6.1.1 参照）

なお、影響を与える外部及び内部の状況が変化した場合は、逐次、見直しを行う。

課題の決定において、以下の事項を考慮に入れる。

（外部の課題）

a) 国際、国内、地方又は近隣地域を問わず、社会、文化、政治、法律、規制、金融、技術、経済及び環境に関する要因
b) 組織の目的に影響を与える、鍵となる原動力及び傾向
c) 外部ステークホルダ（利害関係者）との関係、並びに外部ステークホルダの認知及び価値観、必要性及び期待
d) 契約上の関係及びコミットメント
（利害関係者との契約や約束事、及び法規制や業界標準への準拠に関するコミットメント）
e) ネットワークの複雑さ、及び依存関係
（サプライチェーン、パートナーシップなどとの関係性および依存度）

（内部の課題）

f) ビジョン、使命及び価値観
g) 組織統治、組織体制、役割及びアカウンタビリティ（説明の義務・責任）
h) 戦略、目的及び方針
i) 組織の文化
j) 組織が採用する規格、指針及びモデル
k) 資源及び知識として理解されている能力（例えば、資本、時間、人員、プロセス、システム、技術）
l) データ、情報システム及び情報の流れ

m) 内部ステークホルダの認知及び価値観を考慮に入れた、内部ステークホルダとの関係
n) 契約上の関係及びコミットメント
（雇用契約や部門間の合意事項や責任分担、及び方針や手順へのコミットメント）
o) 相互依存及び相互関連
（部門間における相互依存の程度及び関連性）

4.2 利害関係者のニーズ及び期待の理解

当組織は、情報セキュリティ委員会において、気候変動に関する要求事項をもつ可能性を踏まえ、以下の事項を決定し、「**ISMS 組織状況管理表**」にまとめ、関係者へ周知する。（4.3 及び 6.1.1 参照）

なお、影響を与える利害関係者のニーズ及び期待が変化した場合は、逐次、見直しを行う。

a) ISMS に関連する利害関係者
b) a)の関連する要求事項
c) それらの要求事項のうち、ISMS を通して取り組むもの

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

当組織は、以下の事項を考慮し、その境界及び適用可能性を 1.2 適用に定義する。

なお、情報セキュリティに関連する業務などの詳細については、「**適用範囲関連資料**」に示す。

a) 4.1 で決定した外部及び内部の課題
b) 4.2 で決定した利害関係者の要求事項
c) 当組織が行う業務と委託業者など他の組織が行う業務の分担や責任範囲、および業務間での情報のやりとり。

4.4 情報セキュリティマネジメントシステム

当組織は、JIS Q 27001:2023（ISO/IEC 27001:2022）及び JIS Q 27001:2023/AMENDMENT 1:2025（ISO/IEC 27001:2022/Amd 1:2024）の規格要求事項に従って、必要なプロセス及びそれらの相互作用を含む、ISMS を確立し、実施し、維持し、かつ継続的に改善するために、以下の事項を実施する。

a) 情報セキュリティ方針や目的、リスク対応計画、規程を作成し、ISMS を確立する。（6 参照）
b) a)で定めた事項を確実に実施するために、必要な資源及び教育訓練等を実施する。（7 参照）
c) 必要に応じて、方針や目的、計画を見直し、修正する。（9 参照）
d) 情報セキュリティに関する取り組みの継続的な改善に取り組む。（10 参照）

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

代表取締役社長（情報セキュリティ委員長）は、次に示す事項により、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。

a) 情報セキュリティ方針（5.2 参照）及び情報セキュリティ目的（6.2 参照）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) JIS Q 27001:2023（ISO/IEC 27001:2022）及び JIS Q 27001:2023/AMENDMENT 1:2025（ISO/IEC 27001:2022/Amd 1:2024）の規格や顧客の要求事項へ対応するための取り組みは、仕事や業務の手順の中に取り込むことを確実にする。

c) ISMS に必要な資源が利用可能であることを確実にする。（7.1 参照）

d) 全社ミーティング（1 回／3 ヶ月）や朝礼などを通して、有効な ISMS 及び JIS Q 27001:2023（ISO/IEC 27001:2022）及び JIS Q 27001:2023/AMENDMENT 1:2025（ISO/IEC 27001:2022/Amd 1:2024）の規格要求事項への適合の重要性を、周知する。

e) ISMS がその意図した成果を達成することを確実にするため、「**情報セキュリティ基本方針書**」から「**年間情報セキュリティ目標**」、「**年間情報セキュリティ計画**」を策定し、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 参照）

f) ISMS が有効に機能するため、ISMS の体制及び責任、運用形態に関して「**情報セキュリティ運営管理規程**」を定め、それに従い、従業員を指揮し支援する。

g) ISMS の定期的なレビューを「9.3 マネジメントレビュー」（9.3 参照）に定め、継続的な改善を促進する。

h) 管理者が自分の管理する部門に対して、情報セキュリティに関する取り組みを推進できるように、管理者の役割や権限を「**情報セキュリティ運営管理規程**」を定め、支援する。

5.2 方針

代表取締役社長（情報セキュリティ委員長）は、次の事項を満たす「**情報セキュリティ基本方針書**」を策定する。

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）の設定のための枠組みを示す。
c) 法律の遵守及び 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、

顧客の要求事項を満たすことのコミットメント

d) ISMS の継続的な改善に関するコミットメント

策定された「**情報セキュリティ基本方針書**」は、次の状態を維持する。

e) 文書化し、関係者がいつでも見られるように、本マニュアル（1.1 参照）に掲載する。
f) 一般研修または新入社員研修（「**人的セキュリティ管理規程**」参照）で、組織内に伝達する。
g) 必要な場合、顧客や委託先などの利害関係者が見られるよう、当組織ホームページに掲載する。

5.3 組織の役割，責任及び権限

代表取締役社長（情報セキュリティ委員長）は、情報セキュリティに関連する役割に対する責任及び権限を「**情報セキュリティ運営管理規程**」に定め、一般研修または新入社員研修（「**人的セキュリティ管理規程**」参照）を通して組織内に伝達する。

代表取締役社長（情報セキュリティ委員長）は、当組織の情報セキュリティ推進責任者を任命し、次の責任及び権限を割り当てる。

a) 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。
b) ISMS のパフォーマンスを代表取締役社長（情報セキュリティ委員長）に報告する。

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

当組織は、ISMS の計画を策定するに当たり、4.1 項（組織及びその状況の理解）及び 4.2 項（利害関係者のニーズ及び期待の理解）で決定した事項を考慮し、次の事項に対処する必要があるリスク及び機会を決定する手順を、「**リスクマネジメント管理規程**」にて定める。

a) ISMS が、定めた情報セキュリティ目的（目標）を達成することを確実にする。
b) 望ましくない影響を防止または低減する管理策の設定。
c) 継続的な改善を行う。

当組織は、次の事項に関するリスク対応計画を策定し、実施する。（6.1.3 参照）