1. 適用範囲

1.1　一般

(1)　ISO27001 マニュアルの目的

このISO27001マニュアルは、ISO27001認証基準に対する当社の情報セキュリティマネジメントシステム（ISMS）の主要な骨格を定めたもので、企業経営における情報セキュリティマネジメントシステムの、継続的かつ効果的運用を図ることを目的とする。

ａ）当システムは、利害関係者（顧客）のニーズとそれに適用する順守すべき法令・規則の明確化から始まり、すべてのシステムの過程を通じて、当社が要求事項を達成する能力を実証し、情報セキュリティを向上するために当社の事業活動に適用される。

ｂ）システムの継続的改善及び不適合防止の活動を効果的に実施し、情報セキュリティ向上へ取り組むことを目的とする。

ｃ）当ISO27001マニュアルは、経営責任者が定める方針に沿って、当社の製品･サービスに対する情報セキュリティを満足させ得るように定めたすべての業務に関する手順を規定する。

ｄ）方針を具現化するにあたって従業員が遵守すべき業務は、当マニュアル、手順書類で示され、業務は正しい業務指示に基づいて行われ、これらの業務を行うにあたって必要とする教育訓練を従業員は受けることになる。

(2)　関連事項

ａ）経営責任者

当社の情報セキュリティ方針を定め、規定された要求事項に適合した情報セキュリティマネジメントシステムを効果的に運用していく執行上の最高責任を有する経営責任者は、代表取締役所長とする。

ｂ）ISO27001マニュアルの作成･承認

このISO27001マニュアルの作成は、システム管理者とし､承認はISMS管理責任者とする。

ｃ）配付管理

このISO27001マニュアルの配付管理手順は、FlexCRM登録により行う。

尚、外部関係者に配布する場合は、ISMS管理責任者の承認を必要とする。

ｄ）見直し

ISO27001マニュアルの見直しは、定期的(1回/年、経営年度の最後の内部監査後)に行う。また活動の手順の変更時にレビューすると共に、経営責任者によって随時見直しを指示される。次のような場合には、ISO27001マニュアルを改訂する。

①ISO27001認証基準に関する規格が変更された場合

②情報セキュリティ方針が変更された場合

③社内文書の見直し実施による改訂内容がISO27001マニュアルの改訂に及ぶ場合

④内部監査の結果、又はその他の不適合による是正処置、予防処置が、ISO27001マニュアルの改訂に及ぶ場合

⑤第三者機関の審査により改訂を要する場合

⑥経営責任者が必要と認めた場合

1.2　適用

(1)　適用事業

ビル・マンション等建物管理に係わる業務

ただし、客先マンションに派遣する管理員業務を除く

(2)　適用組織

別紙、組織図で示す組織

(3)　適用事業所

別紙、事業所一覧で示す事業所

(4)　適用範囲から除外される業務

適用範囲から除外される業務はない

2. 引用規格

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

この引用規格は、その最新版（追補を含む）を適用する。

3. 用語及び定義

この規格で用いる主な用語及び定義は、JIS Q 27000 による。

ただし、当社独自の用語を代わって使用することもできる。

4. 組織の状況

4.1 当社及びその状況の理解

当社は、当社の目的に関連し、かつ、ISMS の意図した成果を達成する当社の能力に影響を与える、外部及び内部の課題を決定する。

4.2 利害関係者のニーズ及び期待の理解

組織は、次の事項を決定する。

a) 情報セキュリティマネジメントシステムに関連する利害関係者

b) それらの利害関係者の関連する要求事項

c) それらの要求事項のうち、情報セキュリティマネジメントシステム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

適用範囲を決定する場合、以下の事項を考慮する。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。

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) 当社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

当社は、この規格の要求する事項に従って、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、継続的に改善を行う。

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

トップマネジメントは、次に示す事項によって、情報セキュリティマネジメントシステムに関するリーダーシップ及びコミットメント（積極的な関与）を実証する。

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、それらが当社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情報セキュリティマネジメントシステム要求事項の統合を確実にする。

c) 情報セキュリティマネジメントシステム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情報セキュリティマネジメントシステム要求事項への適合の重要性を伝達する。

e) 情報セキュリティマネジメントシステムがその意図した成果を達成することを確実にする。

f) 情報セキュリティマネジメントシステム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。

5.2 方針

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）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に積極的にかかわる。

d) 情報セキュリティマネジメントシステムの継続的改善へ積極的にかかわる。

情報セキュリティ方針は、次に示す事項を満たすこと。

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。

5.3 組織の役割、責任及び権限

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、責任及び権限を割り当て、組織内に伝達することを確実にする。

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ること。

a) ISMS が、ISO/IEC 27001:2022 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。

6. 計画

6.1 リスク及び機会に対処する活動

6.1.1 一般

情報セキュリティマネジメントシステム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すること。

a）情報セキュリティマネジメントシステムが、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、次の事項を計画すること。
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）次の事項を行う方法
1）その活動の情報セキュリティマネジメントシステム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、適用すること。
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行う。
c）次によって情報セキュリティリスクを特定する。
1） 情報セキュリティマネジメントシステム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すること。

6.1.3 情報セキュリティリスク対応

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、適用すること。
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すること。
注記 4 ISO/IEC 27001:2022 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、ISO 31000 に規定する原則及び一般的な指針と整合している。

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

組織は、関連する部門及び階層において、情報セキュリティ目的を確立すること。

情報セキュリティ目的は、次の事項を満たすこと。

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) 監視する。

e) 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

情報セキュリティ目的に関する文書化した情報を保持すること。

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、次の事項を決定すること。

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

6.3 変更の計画

当社が情報セキュリティマネジメントシステムの変更の必要性を決定したとき、その変更は、計画的な方法で行うこと。

7. 支援

7.1 資源

組織は、情報セキュリティマネジメントシステムの確立、実施、維持及び継続的改善に必要な資源を決定し、提供すること。

7.2 力量

組織は、次の事項を行うこと。

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、必要な力量を身につけるための処置をとり、とっ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。

7.3 認識

組織の管理下で働く人々は、次の事項に関して認識をもつこと。

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､情報セキュリティマネジメントシステムの有効性に対する自らの貢献

c) 情報セキュリティマネジメントシステム要求事項に適合しないことの意味

7.4 コミュニケーション

組織は、次の事項を含め、情報セキュリティマネジメントシステム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すること。

a) コミュニケーションの内容（何を伝達するか。）

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

7.5 文書化した情報

7.5.1 一般

当社の情報セキュリティマネジメントシステムは、次の事項を含むこと。

a) ISO/IEC 27001:2022 が要求する文書化した情報

b) 情報セキュリティマネジメントシステム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

注記 情報セキュリティマネジメントシステム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

7.5.2 作成及び更新

文書化した情報を作成及び更新する際、組織は、次の事項を確実にすること。

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

7.5.3 文書化した情報の管理

情報セキュリティマネジメントシステム及び ISO/IEC 27001:2022 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、管理すること。

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、不適切な使用及び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、次の行動に取り組むこと。

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

情報セキュリティマネジメントシステムの計画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、特定し、管理すること。

注記 アクセスとは、文書化した情報の閲覧だけの許可に関する決定、文書化した情報の閲覧及び変更の許可及び権限に関する決定、などを意味する。

8. 運用

8.1 運用の計画及び管理

当社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、かつ管理すること。

- 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

プロセスが計画通りに実施されたという確信をもつために必要な程度の、文書化した情報を利用可能とすること。

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とること。

情報セキュリティマネジメントシステムに関連する、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すること。

8.2 情報セキュリティリスクアセスメント

当社は、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すること。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すること。

8.3 情報セキュリティリスク対応

当社は、情報セキュリティリスク対応計画を実施し、その結果の文書化した情報を保持する。

9. パフォーマンス評価

9.1 監視、測定、分析及び評価

次の事項を決定すること。

a) 必要とされる監視及び測定の対象。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

注記 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

監視及び測定の結果の証拠として、適切な文書化した情報を利用可能な状態にすること。組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントシステムの有効性を評価すること。

9.2 内部監査

9.2.1 一般

組織は、情報セキュリティマネジメントシステム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すること。

a) 次の事項に適合している。

1) 情報セキュリティマネジメントシステムに関して、当社が規定した要求事項

2) ISO/IEC 27001:2022 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

監査プログラムを計画し、確立し、実施し維持すること。これには、その頻度、方法、責任及び計画に関する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すること。

次に示す事項を行うこと。

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。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すること。

9.3 マネジメントレビュー

9.3.1 一般

トップマネジメントは、組織の情報セキュリティマネジメントシステムが、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、情報セキュリティマネジメントシステムをレビューすること。

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、次の事項を考慮すること。

a) 前回までのマネジメントレビューの結果とった処置の状況
b) 情報セキュリティマネジメントシステムに関連する外部及び内部の課題の変化
c) 情報セキュリティマネジメントシステム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、及び情報セキュリティマネジメントシステムのあらゆる変更の必要性に関する決定を含めること。

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すること。

10. 改善

10.1 継続的改善

組織は、情報セキュリティマネジメントシステムの適切性、妥当性及び有効性を継続的に改善すること。

10.2 不適合及び是正処置

不適合が発生した場合、次の事項を行うこと。

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) 不適合を管理し、修正するための処置をとる。

2）不適合によって起こった結果に対処する。

b） 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とる必要性を評価する。

1）不適合をレビューする。

2）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）とっ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、情報セキュリティマネジメントシステムの変更を行う。

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あること。

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すること。

f）不適合の性質及びとった処置

g）是正処置の結果

以上

改訂履歴

版数	発行・改定・廃止日	制定・改定・廃止理由	改訂ページ
００	2005.03.10	情報保護に関して ISO27001 構築に伴い、新規制定	――――――
０１	2005.04.10	手順の見直しにより全面改訂	全頁改訂
０２	2005.08.01	各規程の様式変更に伴い改訂	全頁改訂
０３	2006.04.01	内部審査に伴い改訂	全頁改訂
０４	2006.07.01	１ｓｔ審査に伴い改訂	全頁改訂
０５	2006.09.21	適用範囲の改定	２ページ
０６	2007.09.18	ISO27001：2005 に適応する変更	全頁改訂
０７	2014.07.11	ISO27001：2013 に適応する変更	全頁改訂
０８	2024.07.23	ISO27001：2022 に適応する変更	全頁改訂
０９			
１０			
１１			
１２			
１３			
１４			
１５			
１６			