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、顧客要求事項及び規制要求事項の明確化から始まり、すべての情報セキュリティマネジメント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、サイボウズ登録により行う。

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　組織及びその状況の理解

当社は、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する。

4.2　利害関係者のニーズ及び期待の理解

当社は、顧客等をはじめとする利害関係者を特定し、その利害関係者の情報セキュリティに関連する要求事項を明らかにする。

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。

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

4.4　情報セキュリティマネジメントシステム（ISMS）

当社は、ISO27001:2013（JISQ27001:2014）の要求事項に従って、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。

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

経営責任者は、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（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。

c）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。

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（ISMS）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（ISMS）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（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。

5.2　方針

経営責任者は、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へのコミットメントを含む。

d）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。

情報セキュリティ方針は、ポスター及びホームページで文書化し、ポスターによって、組織内に伝達し、ホームページによって、利害関係者が入手可能とする。

5.3　組織の役割、責任及び権限

経営責任者は、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、伝達することを確実に行う。

経営責任者は、次の事項に対して、責任及び権限を割り当てる。

a）情報セキュリティマネジメントシステム（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）情報セキュリティマネジメントシステム（ISMS）のパフォーマンスを経営責任者に報告する。

6. 計画

6.1 リスク及び機会に対処する活動

6.1.1 一般

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、次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、「リスク評価表」に記入する。

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。

当社は、次の事項を計画する。

d）決定したリスク及び機会に対処する活動を計画する。

e）次の事項を行う方法

①その活動の ISMS プロセスへの統合及び実施

②その活動の有効性評価

6.1.2 情報セキュリティリスクアセスメント（客観的評価）

当社は、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。

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。

①ISMS 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。

①6.1.2 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。

②6.1.2 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。

当社は、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、リスクアセスメント手順に定める。

6.1.3　情報セキュリティリスク対応

当社は、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、適用する。

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すべての管理策を決定する。

c）6.1.3 b）で決定した管理策を JIS Q 27001:2014 付属書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。

・必要な管理策及び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

・付属書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。

当社は、情報セキュリティリスク対応のプロセスについて、リスクアセスメント手順に定める。

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

当社は、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。

情報セキュリティ目的は、次の事項を満たすものとする。

a）情報セキュリティ方針と整合している。

b）測定可能である。（実行可能な場合）

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）伝達する。

e）必要に応じて、更新する。

当社は、情報セキュリティ目的に関する文書化した情報を保持する。

当社は、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、次の事項を決定する。

f）実施事項

g）必要な資源

h）責任者

i）達成期限

j）結果の評価方法

7. 支援

7.1　資源

当社は、次の事項に必要な経営資源を決定し、提供する。

a）ISMS を確立、導入、運用、監視、レビュー、維持及び改善する。

b）事業上の要求事項を満たすことに情報セキュリティの手順が寄与することを確実にする。

c）法令上及び規制の要求事項並びに契約上のセキュリティ義務を明確にし、これを扱う。

d）導入したすべての管理策を正しく適用することによって十分なセキュリティを維持する。

e）必要に応じてレビューし、レビューの結果に対して適切に対応する。

f）必要な場合には、ISMS の有効性を改善する。

7.2　力量（教育訓練）

当社は、次の事項を行う。

a）当社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

当社の管理下で働く人々は、次の事項に関して認識をもつものとする。

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

7.4　コミュニケーション

当社は、次の事項を含め、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する。

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

e）コミュニケーションの実施者

f）コミュニケーションの実施プロセス

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、次の事項を確実にする。

a）ISO27001：2013（JISQ27001:2014）の規格が要求事項する文書化された情報

b）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）

文書化した情報を作成及び更新する際、当社は、次の事項を確実に行う。

a）適切な識別及び記述（タイトル、日付、作成者、版数など）

b）適切な形式（言語、ソフトウェアの版、図表など）及び媒体（紙、電子媒体など）

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

ISMS 及びこの規格で要求されている文書化された情報は､次の事項を確実にするために､管理する。

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。（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など）

文書化した情報の管理に当たって、当社は、該当する場合には、必ず、次の行動に取り組む。

c）配布、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（版数の管理）

f）保持及び廃棄

ISMS の計画及び運用のために当社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。

8. 運用

8.1　運用の計画及び管理

当社は、情報セキュリティ要求事項を満たすため、及び 6.1「リスク及び機会に対処する活動」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。また、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」で決定した情報セキュリティ目的を達成するための計画を実施する。

当社は、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文書化した情報を保持する。

当社は、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（見直し）し、必要に応じて、有害な影響を軽減する処置をとらなければならない。

当社は、外部委託したプロセスが決定され、かつ、管理されていることを確実にする。

8.2　情報セキュリティリスクアセスメント（客観的評価）

当社は、あらかじめ定めた間隔で、また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、その結果の文書化した情報を保持する。

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

当社は、情報セキュリティパフォーマンス及び ISMS の有効性を評価する。

当社は、次の事項を決定する。

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。

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

当社は、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保持する。

9.2　内部監査

当社は、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する。

a）次の事項に適合している。

①ISMS 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。

当社は、次に示す事項を行う。

c）頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持、監査プログラムは、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に入れる。

d）各監査について、監査基準及び監査範囲を明確にする。

e）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。

f）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。

g）監査プログラム及び監査結果の証拠として、文書化した情報を保持する。

9.3　マネジメントレビュー

経営責任者は、組織の ISMS が、引き続き適切であり、妥当であり、かつ、有効であることを確実にするために、あらかじめ定められた間隔（少なくとも年 1 回）で、ISMS をレビュー（見直し）する。

マネジメントレビューは、次の事項を考慮する。

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）ISMS に関連する外部及び内部の課題の変化

c）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（情報の伝達）

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

d）利害関係者からのフィードバック（情報の伝達）

e）リスクアセスメントの結果及びリスク対応計画の状況

f）継続的改善の機会

マネジメントレビューからのアウトプットには、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る。

当社は、マネジメントレビューの結果の証拠として、文書化した情報を保持する。

10. 改善

10.1　不適合及び是正処置

不適合が発生した場合、当社は、次の事項を行う。

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とる

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その不適合をレビュー（見直し）

②その不適合の原因を明確化

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

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（見直し）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（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とする。

当社は、次に示す事項の証拠として、文書化した情報を保持する。

f）不適合の性質及びとった処置

g）是正処置の結果

10.2　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、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）

以上