ISMS
ISO/IEC 27001:2013

PLAN
DO
CHECK
ACT

4 組織の状況

4.1 組織及びその状況の理解
4.2 利害関係者のニーズ及び期待の理解
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
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) 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
適用範囲は，文書化した情報として利用可能な状態に
4.4 情報セキュリティマネジメントシステム

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
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
b) 組織のプロセスへの ISMS 要求事項の統合
c) 必要な資源
d) 要求事項への適合の重要性を伝達
e) 意図した成果を達成
f) 寄与するよう人々を指揮し，支援
g) 継続的改善を促進
h) 管理層がリーダーシップを実証するよう役割を支援

5.2 方針
a) 組織の目的に対して適切
b) 情報セキュリティ目的（6.2 参照）を含むか又は設定のための枠組み
c) 要求事項を満たすことへのコミットメント
d) 継続的改善へのコミットメント
e) 文書化した情報として利用可能
f) 組織内に伝達
g) 利害関係者が入手可能

5.3 組織の役割，責任及び権限
責任及び権限を割り当て，伝達する
a) この規格の要求事項に適合すること
b) ISMS のパフォーマンスをトップマネジメントに報告

7 支援

7.1 資源
ISMS 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

7.2 力量
a) 必要な力量を決定
b) 教育，訓練又は経験にて，力量を備えていること
c) 必要な力量を身につけるためのとった処置の有効性を評価
d) 力量の証拠として，適切な文書化した情報を保持

7.3 認識
次の事項に関して認識をもたなければならない。
a) 情報セキュリティ方針
b) パフォーマンスの向上によって得られる便益を含む自らの貢献
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
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
a) 内容（何を伝達するか。）
b) 実施時期
c) 対象者
d) 実施者
e) 実施プロセス

6 計画

6.1 リスク及び機会に対処する活動
6.1.1 一般
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
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。
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 ISMS 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
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
a) リスク基準を確立
b) リスクアセスメント
c) リスクを特定
d) リスクを分析
e) リスクを評価
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
6.1.3 情報セキュリティリスク対応
情報セキュリティリスク対応のプロセスを定め適用
a) 適切な情報セキュリティリスク対応の選択肢を選定
b) 選定した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
c) 決定した管理策を附属書 A に示す管理策と比較し検証
d) 適用宣言書を作成
e) リスク対応計画を策定
f) リスク対応計画及び残留しているリスクの受容について承認
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

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
部門及び階層において，情報セキュリティ目的を確立
a) 情報セキュリティ方針と整合
b)（実行可能な場合）測定可能である。
c) 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
d) 伝達
e) 必要に応じて，更新
情報セキュリティ目的に関する文書化した情報を保持

8 運用

8.1 運用の計画及び管理
情報セキュリティ要求事項を満たすため，6.1 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，かつ管理しなければならない。
6.2 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しなければならない。
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，文書化した情報を保持

8.2 情報セキュリティリスクアセスメント
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しなければならない
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

8.3 情報セキュリティリスク対応
情報セキュリティリスク対応計画を実施
情報セキュリティリスク対応結果の文書化した情報を保持

9 パフォーマンス評価

9.1 監視，測定，分析及び評価
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
a) 必要とされる監視及び測定の対象
b) 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
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

9.2 内部監査
あらかじめ定めた間隔で内部監査を実施
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

9.3 マネジメントレビュー
トップマネジメントは，組織の ISMS 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，ISMS をレビューしなければならない。
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) 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
d) 利害関係者からのフィードバック
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
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なければならない。
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

10 改善

10.1 不適合及び是正処置
a) その不適合に対処し，該当する場合には，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
2) その不適合によって起こった結果に対処
b) 再発又は他のところで発生しないため，原因を除去するための処置をとる必要性を評価
1) その不適合をレビュー
2) その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
d) とった全ての是正処置の有効性をレビュー
e) 必要な場合には，ISMS の変更を行う
次に示す事項の証拠として，文書化した情報を保持
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
ISMS の適切性，妥当性及び有効性を継続的に改善

7.5 文書化した情報
7.5.1 一般
a) この規格が要求する文書化した情報
b) 必要であると組織が決定した文書化した情報
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，次の事項を確実にする
a) 適切な識別及び記述
b) 適切な形式及び媒体
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
a) 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
b) 文書化した情報が十分に保護されている
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