ISMSリスクマネジメントの流れ　ISO/IEC 27001:2022（JIS Q 27001:2023）要求事項にみる関連図

4 組織の状況

4.1 組織及びその状況の理解

ここで決定する組織内外の課題は、「6.1 リスク及び機会に対処する活動」における ISMS の計画を策定する際のインプットにもなり、この計画の中で組織が対処する必要があるリスク及び機会を決定することになります。

注記　これらの課題の決定とは，JISQ 31000:2019 の 5.4.1 に記載されている組織の外部状況及び内部状況の確定のことをいう。

ISO/IEC 31000:2018（JIS Q 31000:2019）
5.4.1 組織及び組織の状況の理解

リスクのマネジメントを行うための枠組みを設計するに当たって，組織は，外部及び内部の状況を検証し，理解することが望ましい。

組織の**外部状況の検証**には，次の事項が含まれる場合がある。ただし，これらに限らない。

- 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
- 組織の目的に影響を与える，鍵となる原動力及び傾向
- 外部ステークホルダとの関係，並びに外部ステークホルダの認知，価値観，必要性及び期待
- 契約上の関係及びコミットメント
- ネットワークの複雑さ，及び依存関係

組織の**内部状況の検証**には，次の事項が含まれる場合がある。ただし，これらに限らない。

- ビジョン，使命及び価値観
- 組織統治，組織体制，役割及びアカウンタビリティ
- 戦略，目的及び方針
- 組織の文化
- 組織が採用する規格，指針及びモデル
- 資源及び知識として理解される能力（例えば，資本，時間，人員，知的財産，プロセス，システム，技術）
- データ，情報システム及び情報の流れ
- 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
- 契約上の関係及びコミットメント
- 相互依存及び相互関連

法規制の改定やステークホルダとの関係、組織方針や体制の変更など

4.2 利害関係者のニーズ及び期待の理解

取引先、顧客、従業員などの利害関係者からの要求や期待

ここでは、顧客、供給者、従業員、親会社など、組織の情報セキュリティの取組みに期待している者または影響を受ける者などの「利害関係者」を決定するとともに、そのニーズなどを考慮し、情報セキュリティに関連する要求事項を決定します。
この 4.2 も、「4.1 組織及びその状況の理解」と同様に、「6.1 リスク及び機会に対処する活動」における ISMS 計画策定へのインプットとなります。

JIS Q 27000:2019
3.37
利害関係者（interested party）（推奨用語）
ステークホルダー（stakeholder）（許容用語）
ある決定事項若しくは活動に影響を与え得るか，その影響を受け得るか，又はその影響を受けると認識している，個人又は組織（3.50）

6 計画策定

状況の変化により、発生リスクも変わるため、計画も更新される。

6.1 リスク及び機会に対処する活動

組織の状況の確認

6.1.1 一般

4.1 及び 4.2 を考慮に入れて対処する必要があるリスク及び機会を決定するプロセス。リスク及び機会に対処する活動を計画し、必要なプロセス及び手順を整備し、ISMS に取組み、「8.1 運用の計画策定及び管理」に基づく運用に備えます。

リスクアセスメントの実施規定を作成する。

6.1.2 情報セキュリティリスクアセスメント

基準の確立

a) リスク規準の確立及び維持
決定するリスク基準は、リスク受容規準と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規準を含みます。
「リスク受容基準」は、e) のリスクを評価する際の比較対象であり、また 6.1.3 の情報セキュリティリスク対応において達成目標とする基準です。
「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」には、リスクの種類、測定方法、算定方法及びレベルの記述方法などがあります。

b) リスク基準の一貫性、妥当性及び比較可能性
繰り返し行われるリスクアセメントが、一貫性及び妥当性をもち、かつ比較可能な結果を生み出すように、一貫したリスク基準を適用します。

リスクの特定

c) リスクの特定
リスクが情報の機密性、完全性及び可用性の喪失に由来するものであることを確認し、リスクアセスメントプロセスを適用してリスクを特定することを規定。
「リスク特定」では、リスク源、情報セキュリティ事象及び起こり得る結果を特定して、包括的なリスク一覧を作成。なお、リスク源には、「脅威」及び「脆弱性」が含まれます。
また、6.1.3 f) での役割を考慮してリスク所有者を特定します。

リスクの分析

d) リスクの分析
次の2つの面でアセスメントを行う。
- c) で特定したリスクについて、情報漏えい、情報の毀損や情報処理の停止などの事故に至った場合に起こり得る結果を想定します。
- リスクについて、事故の起こりやすさを想定します。

想定する結果は、期間あたりの頻度で表すことが考えられます。
これらの2つの面をあわせて、リスクについてその大きさの想定ができます。

リスクの評価

e) リスクの評価
リスク分析の結果として得られたリスクごとのリスクレベルは、例えば、情報及び情報処理施設に関連する資産別、機密性・完全性・可用性の別で区別し、把握されます。
リスク評価の結果、リスク対応のために、リスクの優先順位付けをしておくことになります。

リスク対応実施プロセスを確立する。

リスク対応

6.1.3 情報セキュリティリスク対応

a) リスク対応の選択肢の選定
6.1.2 を考慮して、リスク対応プロセスを定め、適用。選択肢は、JIS Q 27001の「3.72 リスク対応」の 注記1 及び 注記2 を参考。
b) 管理策の決定
a) で選定した選択肢の実施に必要な管理策を決定。
c) 附属書Aとの比較による管理策の検証
b) で決定した管理策を附属書A にある管理策と比較し、検証。
d) 適用宣言書の作成
必要な管理策及び理由、実施の可否及び除外理由を記載した適用宣言書。
e) リスク対応計画の策定
「リスク対応計画」を策定する。
f) 残留リスク受容の承認
リスク対応計画及び残留リスクの受容について、リスク所有者の承認を得る。

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

組織が、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し、その情報セキュリティ目的を達成するために、実施事項・必要な資源・責任者・達成期限及び結果の評価方法を踏まえた計画を策定します。

6.3 変更の計画策定

組織は、ISMSの変更の必要性を決定したとき、計画的な方法で変更を行わなければならない。

8 運用

「6 計画策定」の実施と管理

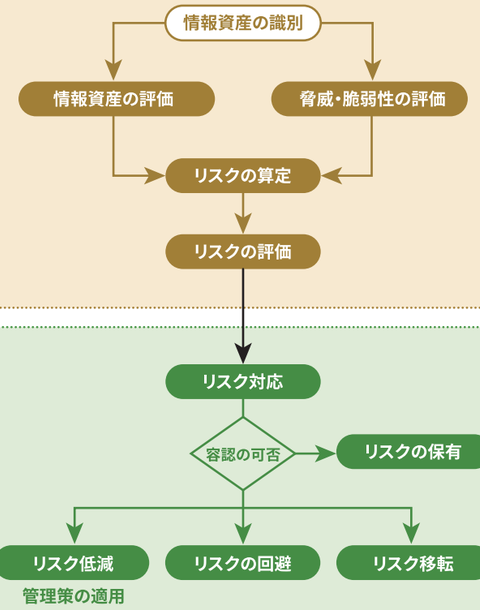
8.1 運用の計画策定及び管理

組織は、情報セキュリティ要求事項を満たすため、及び「6 計画策定」で決定した計画を実施するために、必要なプロセスを計画し、実施し、管理することが求められています。
これは、通常の計画の具体化（例：マイルストン設定）と実行管理が求められており、計画の変更の管理や結果をレビュー。必要に応じた処置を講じることにもなります。
また、ISMSに関連する外部から提供されるプロセスや製品又はサービスも管理する。

8.2 情報セキュリティリスクアセスメント

6.1.2 の規定に基づき実施理

6.1.2 a) で確立した基準に従って、あらかじめ定められて間隔、または必要な都度（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）に実施することが要求されています。
組織内外の環境は、常に変化しているため、リスクも変動していることを念頭に置き、情報セキュリティアクセスメントを適時に実施することが必要となります。



8.3 情報セキュリティリスク対応

6.1.3 の規定に基づき実施理

6.1.3 e) において、これを策定するプロセスを定め、適用することが求められている「情報セキュリティリスク対応計画」を、8.2に従って実施した情報セキュリティリスクアセスメントの結果を考慮して実施することになります。

2023.12.26