

品質管理マニュアルについて (情報セキュリティ監査サービス)

本文書は、経済産業省より公表されている「情報セキュリティサービス基準」(平成 30 年3 月 28 日付)において、情報セキュリティ監査サービスの品質管理要件として示されている事項のうち、「品質管理マニュアル」に関して審査の観点から期待される内容について、申請を行う際の参考として説明するものです。なお、下記に示されている内容はあくまで典型的なサービスを前提とした参考であり、本文書の内容に準拠しなければ基準を満たさないと判断されるわけではないことにご留意ください。

記

1. 「品質管理マニュアル」の整備と取扱について

「品質管理マニュアル」とは、申請対象サービスに関する品質の維持・向上を目的とした品質管理についての手続や手順を定めた文書のことを指します。この文書に期待される内容を次に示します。

- (1) 「品質管理マニュアル」は文書化されている必要があります。「品質管理マニュアル」の原本が電子データであっても差し支えありませんが、審査は印刷された紙文書を対象に行われますので、電子データでなければ発現しない内容は審査対象とはなりません。
- (2) 文書名に「品質管理マニュアル」という名称を含む必要はなく、独立した文書である必要もありません。例えば、JIS Q 9001 規格の認定を取得している企業の場合、同規格に準拠した運用を行うための組織内の手続や手順のうち、申請対象サービスの提供に関連する部分をもって、「品質管理マニュアル」とみなすことが可能です。
- (3) 申請時に提出いただく「品質管理マニュアル」は、申請時点で当該サービスの品質管理に実際に用いられているものである必要があります。ただし、「品質管理マニュアル」の策定以降に顧客を対象としたサービスの提供実績がなくても差し支えありません。
- (4) 「品質管理マニュアル」の対象はあくまで品質管理に関する内容のみであって、要員サービスの提供時に参照するような、サービスの具体的な提供方法や実施手順を定めたマニュアルの提供は必要ありません。

2. 「サービス提供プロセスの管理」について

情報セキュリティ監査サービスの場合、サービス提供プロセスの管理に相当する内容として、「品質管理マニュアル」に次表の項目について必要な品質を保つために実施する事項が定められていることが期待されます。

| サービス提供プロセスの管理に関する項目 | 必要な品質を確保するために「品質管理マニュアル」で定める内容の例 |
|--|---|
| 品質管理者のレビュー事項 | ・ 監査リスクに応じた、品質管理者の承認事項 |
| 受注基準 | ・ 独立性の観点等から受注をお断りする基準 |
| 顧客へのサービス内容の説明 | ・ 実施する監査の種別（保証型、助言型等）、進め方、報告書のイメージ及び取扱の制限等の説明 ・ 監査の中断が発生する場合の説明 ・ フォローアップ監査の実施是非の説明 |
| 顧客のニーズの把握 | ・ 顧客の目的、期待、スコープの理解 |
| 監査チームの編成 | ・ 監査品質の低下を招かない実施体制の確保 ・ 監査人の資格の基準 |
| 監査人の行動指針 | ・ 行動規範・ポリシーの規定 ・ 監査人による遵守 |
| サービスの実施方法を個別に定める文書の作成（例：監査基本計画書、監査実施計画書、監査手続書） | ・ 品質管理者による内容のレビュー ・ 顧客への説明と同意の取得 ・ 顧客側の準備作業についての説明 |
| サービスの進捗管理 | ・ 品質管理者による進捗状況の確認 |
| 顧客から提供された情報の管理 | ・ 情報管理規程・手順等の整備 ・ 情報管理体制の整備 |
| 顧客からの要求、意見、クレーム等への対応 | ・ 受付窓口の設置 ・ 品質管理者による受付内容の確認 |

3. 「アウトプットの管理」について

情報セキュリティ監査サービスの場合、アウトプットの管理に相当する内容として、「品質管理マニュアル」に次表の項目について必要な品質を保つために実施する事項が定められていることが期待されます。

| アウトプットの管理に関する項目 | 必要な品質を確保するために「品質管理マニュアル」で定める内容の例 |
|---------------------------------|----------------------------------|
| サービスの実施結果を報告するための文書の作成（例：監査報告書） | ・ 品質管理者による内容のレビュー |

以上