品質管理マニュアル作成の手引き
（脆弱性診断サービス）

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、脆弱性診断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

脆弱性診断サービスの場合、サービス提供プロセス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
脆弱性診断の仕様調整（例：実施内容、実施対象、診断方法、情報の取り扱い、仕様自体の見直し）	・手順書等の整備 ・品質管理者によるレビュー
脆弱性診断サービスに関する事前説明、見直し時の説明（例：診断実施により影響が生ずる可能性、すべての脆弱性検出が困難であること）	・顧客への説明 ・顧客による同意の徴求
脆弱性診断に関連するインシデント発生時の対応（異常時の検知、問題の切り分け、責任範囲の明確化、復旧レベル）	・インシデント対応手順の整備 ・インシデント対応体制の整備 ・顧客への説明と顧客による同意の徴求
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
脆弱性診断の仕様調整（例：実施内容、実施対象、診断方法、情報の取り扱い、仕様自体の見直し）	・手順書等の整備 ・品質管理者によるレビュー

3.「アウトプットの管理」について

脆弱性診断サービスの場合、アウトプット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：診断報告書）	・品質管理者による内容のレビュー

以上