品質管理マニュアル作成の手引き
（ペネトレーションテスト（侵入試験）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」（令和 6 年 4 月 4 日付）において、ペネトレーションテスト（侵入試験）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

ペネトレーションテスト（侵入試験）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
サービス利用者（顧客）との侵入試験仕様調整（例：試験計画、試験対象範囲、実施内容、情報の取り扱い）	・手順書等の整備 ・顧客への説明 ・顧客による同意の徴求 ・情報管理体制の整備
ペネトレーションテスト（侵入試験）サービスに関する事前説明、見直し時の説明（例：試験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
侵入試験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

3.「対象システム等に関する調査」について

ペネトレーションテスト（侵入試験）サービスの場合、対象システム等に関する調査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。

対象システム等に関する調査に関する項目	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
ネットワーク構成、システム構成、重要情報等の調査	・ネットワーク構成図、システム構成図 ・侵入試験を実施するためのシステムの動作の確認方法（ルールセット、システム設定、ログ管理）
テストする必要があるシステムとデータの特定	・テストする必要があるシステムとデータを特定し、テストの目標と目的を明確にする

4. ペネトレーションテスト（侵入試験）方法の選定・実施

ペネトレーションテスト（侵入試験）方法の選定・実施する内容として、「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。

ペネトレーションテスト（侵入試験）方法の選定・実施に関する項目	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
想定されている脅威	想定されている脅威は、例示 4-2-1、4-2-2 に例示する基準等に基づくものとする
サービス実施方法に関する内容	・テスト方法の選定は、契約内容や事前に把握した事項又は各種の事前調査結果からの脅威のモデリング等に基づいて行う ・ペネトレーションテスト（侵入試験）サービスで提供する検査のプロセスは、例示 4-2-2 に定める基準又は同等のものとする ・実施するテスト方法には、情報セキュリティサービス基準 2-2(1)ア(イ)の a から e までに相当するテストを 1 つ以上含む ・品質管理者によるレビュー

5.「アウトプットの管理」について

ペネトレーションテスト（侵入試験）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：試験結果報告書、報告会等）	・試験結果を PTES（Penetration Testing Execution Standard）の基準または同等以上の報告書作成基準に基づき、「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示 第 3 版」別表の内容を満たす試験実施報告書としてとりまとめる ・当該案件に従事した者以外の者が行う実施結果文書の内容レビュー ・試験結果に関する報告会の開催
顧客の情報を保護するための手続	・ペネトレーションテスト（侵入試験）サービスで使用した顧客の情報を保護するための手続の内容、手続きの実効性を確認する監査実施方法など

以上