品質管理マニュアル作成の手引き
（セキュリティ監視・運用サービス）

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、セキュリティ監視・運用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

セキュリティ監視・運用サービスの場合、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
サービス仕様の調整（例：対象範囲、検知方法、通知の条件と方法、駆けつけ対応の有無、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 ・定期的な仕様の見直し・改善
サービスに関する事前説明、見直し時の説明（例：検知漏れと誤検知が不可避なこと）	・顧客への説明 ・顧客による同意の徴求
サービス提供できていることの運用監視	・サービス提供状況の運用監視・体制の整備
インシデント発生時の対応（異常時の検知、障害の切り分け、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

3.「アウトプットの管理」について

セキュリティ監視・運用サービスの場合、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手段の提供（例：定期報告会の開催、レポートの作成）	・品質管理者による報告内容のレビュー

以上