

令和8年度情報システム監査業務 評価基準書（案）

項番	評価項目	評価基準	主な評価のポイントなど (例示)	配点	基準点
1	業務理解	本業務の目的、総合機構のサイバーセキュリティ対策の現状把握・自律的改善活動の支援、標的型メール訓練による知見向上の目的を理解しているか。 また、総合機構の業務特性、情報セキュリティ・個人情報保護上の留意点、監査対象となる重要情報資産・情報システムの性質を踏まえた提案となっているか。	以下を十分に理解し、これらを踏まえた提案となっているか。 ・総合機構の社会的役割及び業務特性 ・サイバーセキュリティ対策の現状把握と継続的改善の必要性 ・重要情報資産を扱う情報システム及び統合基盤の特性 ・資料閲覧で把握した過去の監査結果、監査対象システム及びサイバーセキュリティポリシー 本業務により仕様書に掲げる目的を達成できることが、具体的かつ論理的に示されているか。	120	60
2	実施計画・監査実施方法	監査全体のスケジュール、実施工程、使用ツール・機器、対象システム別の進め方、関係者へのインタビュー・資料閲覧・必要に応じた視察等の監査手続が、実効性及び具体性をもって示されているか。 特に、重要情報資産を扱う情報システム2システム（うち1システムは統合基盤を含む。）の監査を、マネジメント・情報システム・外部委託先の観点から適切に実施できる計画となっているか。	・契約締結後から令和9年3月末までの各工程、成果物、会議及びレビュー時期が明確か。 ・対象2システムの監査を、マネジメント、情報システム、外部委託先の各観点から漏れなく実施できるか。 ・インタビュー、規程・証跡の閲覧、必要に応じた現地視察等について、対象、手順、担当、想定工数が具体的か。 ・監査、標的型メール訓練、教育資料作成を並行しても、特定要員への過度な集中や工程遅延が生じない計画か。 ・企画提案書には工数だけでなく、その配分根拠及び重点項目が明記され、内容が妥当か。	220	110
3	情報セキュリティ監査の専門性及び実行能力	政府機関等のサイバーセキュリティ対策のための統一基準等、総合機構の規程類及び関連ガイドラインを踏まえ、整備状況・運用状況・準拠性を適切に確認できる監査手法が示されているか。 検出事項について、問題点、改善項目、対応優先度、推奨する運用管理方法を、根拠に基づき整理できる能力があるか。	・仕様書に掲げる基準、規程及び参考ガイドラインを、監査項目や監査手続に具体的に落とし込んでいるか。 ・整備状況、運用状況及び準拠性について、確認資料、質問、証跡、判定方法が具体的に示されているか。 ・過去の監査結果及び自己点検結果を踏まえ、再発・未改善・新規リスクを確認する方法が示されているか。 ・検出事項の事実確認、原因分析、リスク評価、対応優先度の判定及び改善提案の考え方が妥当か。 ・提案内容を円滑に実施できる知識、ノウハウ及び類似業務実績が示されているか。	260	130
4	標的型メール訓練及び教育支援	最大1,900人を対象とした標的型メール訓練を2回実施するための環境、訓練設計、送信管理、アクセス状況の集計、結果分析の方法が具体的か。 また、訓練結果を踏まえた教育用資料及び周知メール文案について、近時の標的型メールのトレンドや確認ポイントを踏まえ、総合機構職員の意識向上に資する内容を提案しているか。	・訓練メールのテーマ、難易度、2回の訓練の関係、送信管理及び不測事態への対応方法が具体的か。 ・最大1,900人への送信、Webサイトへのアクセス状況等の集計を安全かつ確実に行える環境か。 ・開封率、開封者、所属部署別の傾向等を適切に分析し、結果を視覚的に示す方法が提案されているか。 ・2回目の訓練後、訓練結果を踏まえて教育資料及び周知メール文案を作成し、総合機構の確認・修正指示を反映する工程が示されているか。 ・教育資料が新入職員等への再利用・加筆修正を考慮した内容及び形式となっているか。	160	80
5	監査報告書・成果物の品質	監査報告書に、監査目的、基準、実施内容、範囲、基準日・実施期間、監査人、監査所見等を体系的に記載できるか。 改善推奨事項について、一般的な対応方法に加え、総合機構のIT環境を踏まえた対応方法及び優先度を明確に示せるか。成果物を加工可能な形式・PDF形式等で適切に納品できるか。	・監査対象及び読者に応じ、事実、基準、原因、リスク、評価及び改善推奨事項が明確に区分された構成か。 ・改善推奨事項には、一般的な対応だけでなく、総合機構のIT環境を踏まえた実行可能な対応方法と優先度が示されるか。 ・聴取結果、改善事項、標的型メール訓練結果等を、比較・判断しやすい表や図で示す工夫があるか。 ・総合機構によるレビュー、認識合わせ、修正指示及び最終版確定の工程が明確か。 ・加工可能なファイル、PDF、図表の元データ及び監査証跡を整理して納入できるか。	160	80
6	実施体制・要員資格・品質管理体制	統括責任者、監査人、監査補助者、アドバイザーからなる監査チームが編成され、必要な資格・経験を有する専門家が適切に配置されているか。 また、情報セキュリティ対策の管理体制、品質保証体制、インシデント時の連絡体制、資料の不正変更等への対応体制が具体的に示されているか。	・統括責任者、監査人、監査補助者及びアドバイザーの役割、責任、指揮命令系統及び稼働が明確か。 ・仕様書で必須とする資格・実績を満たした上で、本業務に有用な追加の資格、経験又は専門性を有しているか。 ・監査業務と標的型メール訓練・教育支援の双方に必要な要員が配置され、欠員時の代替体制があるか。 ・成果物の品質レビュー、進捗・課題管理、インシデント時の連絡及び資料の不正変更を防止・検知する体制が具体的か。 ・再委託を行う場合、対象業務、役割分担、責任及び情報セキュリティ管理方法が明確か。	200	100
7	ワーク・ライフ・バランス等の推進に関する指標	女性活躍推進法、次世代法、若者雇用促進法に基づく認定状況を評価する。企画提案書には含めず、認定状況を証する書類により確認する。			
	女性活躍推進法に基づく認定（えるばし認定企業・プラチナえるばし認定企業）	プラチナえるばし認定：40点 3段階目（全認定基準5つ〇）：30点 2段階目（認定基準の3～4つ〇）：20点 1段階目（認定基準の1～2つ〇）：10点 行動計画策定段階：5点		40	—
	次世代法に基づく認定（くるみん認定企業・トライくるみん認定企業・プラチナくるみん認定企業）	プラチナくるみん認定：20点 くるみん/トライくるみん認定：10点		20	—
	若者雇用促進法に基づく認定（ユースエール認定企業）	ユースエール認定：20点		20	—
合計				1200	560