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

本書が対応する情報セキュリティサービス基準：第 4 版（令和 6 年 4 月 4 日公表）

経済産業省

令和 6 年 4 月 4 日

本文書について

- 本文書は、情報セキュリティサービス基準において用いる次の内容について、それぞれの要件を満たすものを例示することを目的として経済産業省が公表するものである。
  1. 維持していることをもって、必要な専門性を満たすことができる資格要件
  2. 講師又はリーダーの経験をもって、必要な専門性を満たすことができる専門家コミュニティ
  3. 修了又は受講をもって、必要な専門性を満たすことができる研修修了又は受講実績
  4. 情報セキュリティサービスの提供において参照する基準等
  5. 情報セキュリティサービスにおける結果に関する取扱方法及びその明示方法
  6. 情報セキュリティサービスの提供において準拠する内容及びその明示方法
  7. 情報セキュリティサービスの品質確保に資する継続教育
- 本文書は、記載される例示をもって対象を限定するものではなく、記載される例示と同等のものについても、情報セキュリティサービス基準に基づく審査を通じて同等の効果を有するものとして扱われる。
- 本文書に記載する例示の内容は、経済産業省が設置する有識者会議において、下表の要件に対する適合性に関する審議の結果をもって決定される。

1. 維持していることをもって、必要な専門性を満たすことができる資格要件	● 現在受験可能な資格であること ● 例示の趣旨に照らして、以下の特徴を適切に満たすものであること ➢ 公的機関が実施又は監修している ➢ 当該サービスの提供に従事する国内の人材が自らの専門能力を証明する手段としての利用実績を有する ➢ 当該サービスの提供に求められる知識及び能力と、資格で求められる知識及び能力内容との関連性が高い
2. 講師又はリーダーの経験をもって、必要な専門性を満たすことができる専門家コミュニティ	● 現在参加可能なコミュニティであること ● 例示の趣旨に照らして、以下の特徴を適切に満たすものであること ➢ 公的機関が実施又は監修している ➢ 当該サービスの提供に従事する国内の人材が自らの専門能

	力をもって教育や普及啓発活動を行う場としての利用実績を有する ➢ 当該サービスの提供に求められる知識及び能力と、コミュニティで扱う内容との関連性が高い
3. 修了又は受講をもって、必要な専門性を満たすことができる研修修了又は受講実績	● 現在受講可能な研修等であること ● 例示の趣旨に照らして、以下の特徴を適切に満たすものであること ➢ 公的機関が実施又は監修している ➢ 当該サービスの提供に従事する国内の人材が自らの専門能力を高めるための手段としての利用実績を有する ➢ 当該サービスの提供に求められる知識及び能力と、研修内容との関連性が高い
4. 情報セキュリティサービスの提供において参照する基準等	● 品質が担保された当該サービスの提供において、現在広く用いられている基準等及び例示方法であること
5. 情報セキュリティサービスにおける結果に関する取扱方法及びその明示方法	● 品質が担保された当該サービスの提供において、現在広く用いられている取扱方法及びその明示方法であること
6. 情報セキュリティサービスの提供において準拠する内容及びその明示方法	● 品質が担保された当該サービスの提供において、現在広く用いられている準拠する内容及びその明示方法であること
7. 情報セキュリティサービスの品質確保に資する継続教育	● 品質が担保された当該サービスを提供している実務者が、現在実施している継続教育の実態を反映したものであること

● 本文書に記載する例示の内容について、年１回以上上表の要件に対する該当性が維持されているかどうかの確認を行い、必要に応じて内容の見直しを行うこととする。

１．　資格要件の例示

１－１	情報セキュリティ監査サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	専門資格（注）	・ 公認情報セキュリティ監査人 ・ 公認システム監査人 ・ CISA（Certified Information System Auditor） ・ システム監査技術者
１－２－１	脆弱性診断サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	汎用資格（注）	・ 情報処理安全確保支援士 ・ CISSP（Certified Information Systems Security Professional） ・ CISA（Certified Information System Auditor） ・ CISM（Certified Information Security Manager） ・ GIAC（Global Information Assurance Certification）
		専門資格	・ CEH（Certified Ethical Hacker） ・ OSCP（OffSec Certified Professional） ・ OSEP（OffSec Experienced Pentester） ・ OSWA（OffSec Web Assessor） ・ OSWE（OffSec Web Expert）
１－２－２	ペネトレーションテスト（侵入試験）サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	専門資格	・ OSCP（OffSec Certified Professional） ・ OSEP（OffSec Experienced Pentester） ・ CRTO（Certified Red Team Operator） ・ CRTP（Certified Red Team Professional） ・ CRTE（Certified Red Team Expert） ・ CRTM（Certified Red Team Master） ・ GPEN（GIAC Penetration Tester） ・ GWAPT（GIAC Web Application Penetration Tester） ・ GCPN（GIAC Cloud Penetration Tester）

			・ GXPN（GIAC Exploit Researcher and Advanced Penetration Tester）
１－３	デジタルフォレンジックサービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	汎用資格	・ 情報処理安全確保支援士 ・ CISSP（Certified Information Systems Security Professional）
		専門資格	・ デジタル・フォレンジック資格（CDFP-B、CDFP-P、CDFP-M）
１－４	セキュリティ監視･運用サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の資格	汎用資格	・ 情報処理安全確保支援士 ・ CISA（Certified Information System Auditor） ・ CISM（Certified Information Security Manager） ・ CISSP（Certified Information Systems Security Professional） ・ GIAC（Global Information Assurance Certification）
		専門資格	・ CND（Certified Network Defender）
１－５	機器検証サービスの提供に必要な専門性を満たすことができる右に例示する内容相当の資格	汎用資格	・ 情報処理安全確保支援士 ・ CISM（Certified Information Security Manager） ・ CISSP（Certified Information Systems Security Professional） ・ GIAC（Global Information Assurance Certification）
		専門資格	・ エンベデッドシステムスペシャリスト ・ CEH（Certified Ethical Hacker） ・ CHFI（Computer Hacking Forensic Investigator） ・ OSCP（Offensive Security Certified Professional） ・ GICSP（Global Industrial Cyber Security Professional） ・ デジタル・フォレンジック資格（CDFP-B、CDFP-P、CDFP-M）

（注）汎用資格：情報セキュリティ分野の幅広い知識を有することを証する資格の例示

２．　専用資格：当該サービスの提供に関する専門的な知識を有することを証する資格の例示専門家コミュニティの例示

２－１	講師又はリーダーの経験をもって、脆弱性診断サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の専門家コミュニティ	・ 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA） ・ 日本セキュリティオペレーション事業者協議会（ISOG-J） ・ OWASP（The Open Web Application Security Project）
２－２	講師又はリーダーの経験をもって、デジタルフォレンジックサービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の専門家コミュニティ	・ 特定非営利活動法人デジタル・フォレンジック研究会（IDF）
２－３	講師又はリーダーの経験をもって、セキュリティ監視・運用サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の専門家コミュニティ	・ 特定非営利活動法人日本ネットワークセキュリティ協会 ・ 日本セキュリティオペレーション事業者協議会 ・ 日本コンピュータインシデント対応チーム協議会 ・ ISC2（International Information Systems Security Certification Consortium） ・ ISACA ・ SANS

３．　研修受講実績の例示

３－１	当該研修の修了をもって脆弱性診断サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の研修	・ SANS Security Courses (460, 504, 542, 560, 575, 660, 760)
３－２	当該研修の受講をもってデジタルフォレンジックサービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の研修	・ SANS Forensic Courses (500, 508, 572, 578, 585, 610) ・ Guidance (DF120, DF210) ・ AccessData (FTK BootCamp) ・ 特定非営利活動法人デジタル･フォレンジック研究会が実施する「IDF講習会」の受講、資格(CDFP)維持に関わる継続的教育の受講 ・ 特定非営利活動法人デジタル･フォレンジック研究会会員企業が設けている各種フォレンジックトレーニングコース
３－３	当該研修の修了をもってセキュリティ監視・運用サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の研修	・ SANS Security Courses (501, 503, 511)
３－４	当該研修の修了をもって機器検証サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の研修	・ SANS Penetration Courses (556, 560, 642, 660, 760)

４．　参照する基準の例示

４－１	情報セキュリティ監査サービスの提供において用いる右に例示する内容相当の基準及びその明示方法の例示	・ 情報セキュリティ監査基準を含む行政機関が定める情報セキュリティに係る監査基準 ・ 国際会計士連盟に加盟する団体又は Payment Card Industry Security Standards Council が定める基準
４－２－１	脆弱性診断サービスの提供において用いる右に例示する内容相当の基準等及びその明示方法の例示	【Web アプリケーション脆弱性診断において、次に示す内容相当の診断を行う旨の提示】 ・ OWASP の定める ASVS(Application Security Verification Standard) レベル１以上 ・ 独立行政法人情報処理推進機構による「ウェブ健康診断仕様」が定める診断内容 ・ OWASP が定める「Security Testing Guideline」 ・ 日本セキュリティオペレーション事業者協議会及び OWASP による脆弱性診断士スキルマッププロジェクトが定める「脆弱性診断ガイドライン」 【Web アプリケーション脆弱性診断において、次に示すツールを使用して診断を行う旨の提示】 ・ Burp Suite ・ HCL AppScan ・ InsishtAppsec/Appspider ・ OWASP ZAP ・ Vulnerability Explorer (VEX) 【プラットフォーム脆弱性診断において、次に示すツールを使用して診断を行う旨の提示】 ・ insightVM/Nexpose

		・ Nessus ・ OpenVAS ・ QualysGuard ・ Tripwire IP360
４－２－２	ペネトレーションテスト（侵入試験）サービスの提供において用いる以下に例示する内容相当の基準等及びその明示方法の例示	・ NIST SP800-115 (Technical Guide to Information Security Testing and Assessment - Recommendations of the National Institute of Standards and Technology) ・ Penetration Testing Execution Standard (PTES) ・ MITRE ATT&CK に示されている攻撃手法や技術
４－３	デジタルフォレンジックサービスの提供において用いる右に例示する内容相当の基準及びその明示方法に関する例示	・ 証拠保全、解析手順、報告書作成等の各段階での基準を作成する（使用するツールや一連の手順等は、特定非営利活動法人デジタル・フォレンジック研究会（IDF）作成の「証拠保全ガイドライン」に準拠)。 ・ 代表的ツール（Encase, Xways, FTK 等）及び特定非営利活動法人デジタル・フォレンジック研究会の「日本語処理解析性能評価」を受検した製品を使用する。 ・ 対象サービス内容は、特定非営利活動法人デジタル・フォレンジック研究会作成の「証拠保全ガイドライン」の付録「IDF 団体会員「製品・サービス区分リスト」」①～④までとする。
４－４	機器検証サービスの「機器検証」の提供において用いる右に例示する内容相当の基準及びその明示方法に関する例示	・ 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」（以下、「手引き」という）の「3.1　検証手順」において明記されている次の検証手順 準備　：契約締結に向けて、必要な情報の整理や検証目的の明確化を行う。 計画　：契約締結後、検証体制及び検証環境を構築する。また、

		検証の実施に向けた検証項目や検証手法の策定を行う。 検証実施：検証依頼者の要望を踏まえ、検証を実施する。 分析　　：検証結果に基づき、特定・検出された脆弱性や詳細検証によって明らかになった脅威に対して、想定される影響や対応策の案を分析する。 報告　　：検証報告書を作成する。

５．　結果に関する取扱方法及びその明示方法の例示

５－１－１	脆弱性診断サービスの提供において示す結果に関する取扱方法及びその明示方法	・ ツール出力についての分析を含んだ診断を実施する。 ・ 診断結果報告書としてとりまとめる。 ・ 診断結果に関する報告会を開催する。
５－１－２	ペネトレーションテスト（侵入試験）サービスの提供において示す結果に関する取扱方法及びその明示方法	・ 試験結果を PTES（表外注参照）の基準または同等以上の報告書作成基準に基づき、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。
５－２	機器検証サービス提供において示す結果に関する取扱方法及びその明示方法	・ 下記①から③を含む内容を検証結果報告書としてとりまとめる。 ① 検証結果報告書において、検出された脆弱性に関する情報と、当該脆弱性が悪用された場合に想定される影響、攻撃の再現手順を記載する。 ② 検証結果報告書において、検証結果に対する分析や考察等の追加情報を記載する。 ③ 検証結果に基づき、検証対象機器に求められるセキュリティ管理策の提案を行う。 ・ 検証結果に関する報告会を開催する。

（注）PTES：Penetration Testing Execution Standard が規定する Reporting に関する基準

６．　準拠する内容及びその明示方法の例示

６－１	セキュリティ監視･運用サービスの提供において準拠する右に例示する内容及びその明示方法	・ SLA(サービスレベルアグリーメント)、SLO（サービスレベル目標）又は約款の設定により、役割や責任の所在を明確化する。 ・ SLA/SLO/約款において、可用性に関する指標を示す。 ・ 次に例示するような具体的なサービス内容を示す。 ➢ 監視のみなのか、保護するのか、検知精度をどうするか等の仕様。 ➢ サービスで利用するセキュリティ製品について､その提供ベンダーによるサポート期間内において､当該ベンダーと継続的な関係を持ち、システムのメンテナンスを行い、パッチ適用や検知パターン/シグネチャのアップデートや製品のバージョンアップに追従する。 ➢ 製品の調達を伴うサービスにおいては､その提供ベンダーからの正規の保守・運用サポートを合わせて取り扱う。 ・ 次に例示するような具体的なサービス提供体制を示す ➢ 組織的な運用体制が存在し、属人的な運用に依存しない。 ➢ サービス提供環境（マシンルーム・監視ルーム）に対する物理的又は論理的に監視運用基盤へのアクセス及び利用は制限されている。 ➢ サービス提供環境の管理は、自社の ISMS のもとで実施される。 ・ サービスに関する制限事項(定型のサービスから外れるカスタマイズの可否、サービスメンテナンス、回線断時の対応等）を示す。
６－２	機器検証サービスの「機器検証」の提供において準拠する右に例示する内容及びその明示方法	下記①から③を含む内容を明示する。 ① 免責条項は、以下の事項すべてを含むこと。 ・検証時点における既知の脆弱性に関する検証であり、検証時点以降に発見される脆弱性には対応していない。 ・検証環境と異なる環境における脆弱性は検知できない。 ・検証後、事業者が明示する期間を経た検証対象システムにおい

		て生じた事故等については、検証との関係の有無に関わらず免責とする。 ② 検証の際における既知の脆弱性のリスト又は判定の基準、検証環境を記述した資料について、第三者に説明できる記録を「事業者が明示する期間」保管すること。 ③ 手引きにおいて明記されているツール・手法のうち、どのツール・手法を使用して検証を行うかを示すこと。

７．　継続教育の例示

７－１	情報セキュリティ監査サービスの品質確保に資する教育又は研修	・ 技術責任者 年間２０時間以上の教育又は研修（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT（On the Job Training)、社内講習や自習を含む。） ・ 情報セキュリティ監査サービスに従事する者（技術責任者以外） 年間５時間以上の教育又は研修（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT、社内講習や自習を含む。）
７－２	脆弱性診断サービスの品質確保に資する教育又は研修	・ 脆弱性診断サービスに従事する者 ➢ 年間２０時間以上の教育又は研修（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT、社内講習や自習を含む。） ➢ 本例示２－１に定める専門家コミュニティにおける年間２０時間以上の活動 ➢ 上記、教育、研修及び専門家コミュニティにおける活動を合計で年間２０時間以上実施していること。 ➢ 本例示１－２に定める資格を有する者における継続専門教育（以下「CPE」という。）による年間２０ポイント以上の取得

７－３	デジタルフォレンジックサービスの品質確保に資する教育又は研修	・ 本例示１－３に定める資格を満たす者 各資格に定められた教育及び研修 ・ 本例示１－３に定める資格を満たさない者 年間３５時間以上の次に掲げる活動のいずれか ➢ 教育又は研修(教育サービス事業者が提供する教育･研修のほか、本例示１－３、２－２、３－２の条件を満たし、デジタルフォレンジックの実務経験を有する者を教官とした OJT 又は社内講習を含む。) ➢ 本例示２－２に定める専門家コミュニティにおける活動
７－４	セキュリティ監視・運用サービスの品質確保に資する教育又は研修	・ セキュリティ監視・運用サービスに従事する者 ➢ 年間２０時間以上の教育又は研修（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT、社内講習や自習を含む。） ➢ 本例示２－３に定める専門家コミュニティにおける年間２０時間以上の活動 ➢ 上記、教育、研修及び専門家コミュニティにおける活動を合計で年間２０時間以上実施していること。 ➢ 本例示１－４に定める資格を有する者における CPE による年間２０ポイント以上の取得
７－５	機器検証サービスの品質確保に資する教育又は研修	・ 機器検証サービスに従事する者 ➢ 年間２０時間以上の教育又は研修（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT、社内講習や自習を含む。）

別表　ペネトレーションテスト（侵入試験）に関する試験実施報告書において満たすべき事項

分類	満たすべき事項
試験実施報告書全体	• 「エグゼクティブサマリ」と「テクニカルレポート」に分ける等、報告すべき対象者（読者）の違いに応じた複数のセクションで構成されている。 • 報告書に用いた用語や表現について、読者が平易に理解できることへの配慮がなされている（例：専門用語への脚注や用語集の付加等）。
エグゼクティブサマリ又は相当するセクション	• テストの目的が記載されている。 • テストを通じて重大な脆弱性や問題が検出された場合は、読者が緊急対応の必要性（対策しない場合に生じうる被害等）を理解できるよう、他の検出事項と区別して記載されている。 • テスト結果を示す際には、読者が対策の優先順位付け等を行いやすいよう、結果から想定されるリスクの影響度合いに関する説明やプロファイル等を用いた整理等の配慮が可能な範囲で行われている。 • テストを通じて検出されたリスクへの対応に関する推奨事項として、合理的かつ実現可能な内容が記載されている。
テクニカルレポート又は相当するセクション	• テストの実施体制（担当部署、責任者、資格保有者等）が明記されている。 • テストの目的を踏まえ、テストを通じて把握すべき内容が記載されている。 • 委任者との合意のもとで実施されたテストの対象範囲（環境、資産等）が記載されている。 • 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われている。 • 想定されている脅威は、例示４－２－１に例示する基準等に基づいている。 • 実施したテスト方法を選定した根拠として、テストの目的、想定する脅威の特徴及び例示４－２－２に例示する基準等に照らしてどのような判断をしたかが示されている。 • 実施したテスト方法には、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が１つ以上含まれる。

	• テストを実施した際の条件として、読者に伝える必要のある内容（実施にあたっての制約事項、検証環境での実施、システム、ネットワーク又は資産の管理部門との調整結果等）が記載されている。 • テストを実施した結果として、その根拠を説明可能な内容が記載されている。 • テスト結果から想定されるリスクについて、その影響の大きさや発生可能性がマトリクス等を用いる等により整理されて記載されている。 • テスト対象組織やそのシステム等の事情等を考慮した、テスト結果に基づく推奨事項が記載されている。