情報セキュリティサービス基準

第 4 版

経済産業省

令和 6 年 4 月 4 日

目次

第１章　総則

１　目的

本基準は、情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするための基準を設けることで、情報セキュリティサービス業の普及を促進し、国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的とする。

２　定義

本基準における用語の定義は、次に定めるところによる。

（１）情報セキュリティサービス

情報セキュリティ監査サービス、脆弱性診断サービス、ペネトレーションテスト（侵入試験）サービス、デジタルフォレンジックサービス、セキュリティ監視・運用サービス及び機器検証サービスのいずれか又は全てを行うサービス業をいう。

（２）情報セキュリティ監査サービス

情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与え又は助言を行うサービス業をいう。

（３）脆弱性診断サービス

システムやソフトウェア等の脆弱性に関する一定の知見を有する者が、システムやソフトウェア等に対して行う次に掲げるいずれか又は全てのサービスをいう。

ア　Web アプリケーション脆弱性診断

イ　プラットフォーム脆弱性診断

ウ　スマートフォン／タブレット端末アプリケーション脆弱性診断

（４）ペネトレーションテスト（侵入試験）サービス

脆弱性診断のサービスの定義を満たすサービスのうち、攻撃者が実際に侵入等を行うために用いる手法と同様の手法により、アプリケーション、システム、又はネットワークのセキュリティ機能を回避して攻撃の目的を達成できるかの観点から試験を行い、その結果をもとに助言を行うサービスをいう。

（５）デジタルフォレンジックサービス

システムやソフトウェア等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等や法的紛争・訴訟に際し、電磁的記録の証拠保全、調査及び分析を行うとともに、電磁的記録の改ざん及び毀損等についての分析及び情報収集等を行う一連の科学的調査手法及び技術（以下「デジタルフォレンジック」という。）についての次に掲げるいずれか又は全てのサービスをいう。

ア　機器や記録デバイスを対象とするデジタルフォレンジックによる調査

イ　デジタルフォレンジックによる調査に付帯する訴訟支援及び電子証拠開示対応（ｅディスカバリ）等のサービス

（６）セキュリティ監視・運用サービス

システムやソフトウェア等についての情報セキュリティを確保するための監視サービス及びシステムやソフトウェア等の適切な運用についての次に掲げるいずれか又は全てのサービスをいう。

ア　マネージドセキュリティサービス（セキュリティインシデント又はその予兆の検知、防御を目的とするものをいう。）

イ　セキュリティ監視サービス（セキュリティ製品が出力するログの分析、通知、レポート提供を継続的に提供するものをいう。）

ウ　マネージドセキュリティサービスやセキュリティ監視サービスを包含する複合的なサービス

（７）機器検証サービス

IoT 機器をはじめとするネットワーク通信機能を持つ機器及びその機器に対してネットワークを通じて操作・管理・データ処理等を行うアプリケーションから構成されるシステム（IoT システム）に対して行う次に掲げるいずれか又は全てのサービスをいう。

ア　機器検証

イ　機器検証及び Web アプリケーション脆弱性診断

ウ　機器検証及びプラットフォーム脆弱性診断

（８）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（以下「例示」という。）

本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文書をいう。

ア　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

イ　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

ウ　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

エ　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

オ　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

カ　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

キ　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

第２章　情報セキュリティサービスの基準に関する事項

１　情報セキュリティ監査サービスに係る審査基準

（１）技術要件

情報セキュリティ監査サービスを提供しようとする者は、次に掲げる技術要件に該当するものであること。

ア　専門性を有する者の在籍状況

サービス品質の確保のため、情報セキュリティ監査サービスに従事する要員のうち、例示１－１に定める資格又は同等のものを有する者を技術責任者として業務に従事させるとともに、技術責任者のリスト（資格番号の表示のみでもよい。）を明示すること。

イ　サービス仕様の明示

サービス品質の確保のため、例示４－１に定める基準又は同等のものに従って、情報セキュリティ監査サービスが行われていることを明らかにしていること。

（２）品質管理要件

情報セキュリティ監査サービスを提供しようとする者は、次に掲げる品質管理要件に該当するものであること。

ア　品質管理者の割当状況

品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。

イ　品質管理マニュアルの整備

品質の維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。

（ア）サービス提供プロセスの管理

（イ）アウトプットの管理

ウ　品質の維持・向上に関する手続等の導入状況

品質維持・向上のため、次に掲げる手続等を行っていること。

（ア）次のいずれかの品質の維持・向上に関する手続等を行っていること。

ａ　情報セキュリティ監査サービスを行った案件について、当該案件に従事した者以外の者が監査計画及び監査報告書についてのレビューを行っていること。

ｂ　情報セキュリティ監査サービスを行った案件についての査読を行っていること。

（イ）情報セキュリティ監査サービスに従事する者に対して例示７－１に定める教育及び研修等又は同等のもののいずれかを実施又は受講させていること。

（ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続について情報セキュリティ監査サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

２　脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービスに係る審査基準

２－１　脆弱性診断サービスに係る審査基準

（１）技術要件

脆弱性診断サービスを提供しようとする者は、次に掲げる技術要件に該当するものであること。

ア　専門性を有する者の在籍状況

サービス品質の確保のため、脆弱性診断サービスに従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。

（ア）例示１－２－１に定める資格又は同等のものを有する者

（イ）例示２－１に定める専門家コミュニティ又は同等のものにおける講師若しくはリーダーの経験又は高等教育機関における脆弱性診断サービスの技術を対象とする講師経験を有する者

（ウ）次のいずれかの事業において基準となる日から起算して過去３年間に合計で５件（契約件数。包括的な契約の場合は１年間分で１件とみなす。）以上の実績（診断方法は問わない。）を有する者

ａ　Web アプリケーション脆弱性診断

ｂ　プラットフォーム脆弱性診断
ｃ　スマートフォン／タブレット端末アプリケーション脆弱性診断
ｄ　その他ソフトウェアやシステムの脆弱性対策を目的とした診断又はテスト

（エ）例示３－１に定めるサービス品質確保に資する研修又は同等のものを修了している者

イ　サービス仕様の明示

サービス品質の確保のため、例示４－２－１に定める基準又は同等のものに従って脆弱性診断サービスが行われていることとともに、例示５－１－１に定める脆弱性診断の結果の取扱又は同等のものを明らかにしていること。

（２）品質管理要件

脆弱性診断サービスを提供しようとする者は、次に掲げる品質管理要件に該当するものであること。

ア　品質管理者の割当状況

品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。

イ　品質管理マニュアルの整備

品質維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。

（ア）サービス提供プロセスの管理

（イ）アウトプットの管理

ウ　品質の維持・向上に関する手続等の導入状況

品質の維持・向上のため、次に掲げる手続等を行っていること。

（ア）脆弱性診断サービスを行った案件について、当該案件に従事した者以外の者が検査実施報告書についてレビューを行っていること。

（イ）脆弱性診断サービスに従事する者に対して例示７－２に定める教育及び研修等又は同等のもののいずれかを実施し又は受講させていること。

（ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続について脆弱性診断サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

２－２　ペネトレーションテスト（侵入試験）サービスに係る審査基準

（１）技術要件

本基準で定めるペネトレーションテスト（侵入試験）サービスを提供しようとする者は、２－１（１）に掲げる技術要件かつ、次に掲げる技術要件に該当するものであること。

ア　専門性を有する者の在籍状況

サービス品質の確保のため、ペネトレーションテスト（侵入試験）サービスに従事する要員のうち、次のいずれかの要件を満たす者を１名以上業務に従事させること。

（ア）例示１－２－２に定める資格又は同等のものを有する者

（イ）次のいずれかのペネトレーションテスト（侵入試験）を含む事業に関して基準となる日から起算して過去３年間に合計で３件（契約件数。包括的な契約の場合は１年間分で１件とみなす。）以上の、顧客が管理しているシステムに対して以下のいずれかを実施した実績を有する者

ａ　脆弱性または設定不備を利用することで、管理者権限（ドメイン管理者等）を持つアカウントによるオペレーティングシステムへのログインや任意のコマンド実行

ｂ　脆弱性または設定不備を利用することで、一般権限を持つアカウントによるオペレーティングシステムへのログインや任意のコマンド実行

ｃ　脆弱性または設定不備を利用することで、本来アクセス権のないアカウントによる機密情報の入手・外部持ち出し

ｄ　脆弱性または設定不備を利用することで、アカウントに対し本来許可していない権限での操作

ｅ　ａ～ｄに限らず、脆弱性、外部に漏えいした認証情報又は内部情報を利用することで、オペレーティングシステムやアプリケーション等に対して本来許可されていない操作を実施

イ　サービス仕様の明示

サービス品質の確保のため、例示４－２－２に定める基準又は同等のものに従って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、及び例示５－１－２に定めるペネトレーションテスト（侵入試験）の結果の取扱又は同等のものを具体的に明らかにすること。

（２）品質管理要件

ペネトレーションテスト（侵入試験）サービスを提供しようとする者は、

２－１（２）に掲げる品質管理要件かつ、次に掲げる品質管理要件に該当するものであること。

ア　品質管理マニュアルの整備

品質維持・向上のため、ペネトレーションテスト（侵入試験）サービスについて次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。

（ア）サービス提供プロセスの管理

（イ）対象システム等に関する調査

（ウ）ペネトレーションテスト（侵入試験）方法の選定・実施

（エ）アウトプットの管理

イ　品質の維持・向上に関する手続等の導入状況

品質の維持・向上のため、次に掲げる手続等を行っていること。

（ア）ペネトレーションテスト（侵入試験）サービスを行った案件について、当該案件に従事した者以外の者が試験実施報告書についてレビューを行っていること。

（イ）ペネトレーションテスト（侵入試験）サービスに従事する者に対して例示７－２に定める教育及び研修等又は同等のもののいずれかを実施し又は受講させていること。

（ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続についてペネトレーションテスト（侵入試験）サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

３　デジタルフォレンジックサービスに係る審査基準

（１）技術要件

デジタルフォレンジックサービスを提供しようとする者は、次に掲げる技術要件に該当するものであること。

ア　専門性を有する者の在籍状況

サービス品質の確保のため、デジタルフォレンジックサービスに従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。

（ア）例示１－３に定める資格又は同等のものを有する者

（イ）例示２－２に定める専門家コミュニティ又は同等のものにおける講師若しくはリーダーの経験又は高等教育機関におけるデジタルフォレンジックの技術を対象とする講師経験を有する者

（ウ）例示３－２に定めるサービス品質確保に資する研修又は同等のものを修了している者

イ　サービス仕様の明示

サービス品質の確保のため、例示４－３に定める基準又は同等のものに従ってデジタルフォレンジックサービスが行われていることを明らかにしていること。

（２）品質管理要件

デジタルフォレンジックサービスを提供しようとする者は、次に掲げる品質管理要件に該当するものであること。

ア　品質管理者の割当状況

品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。

イ　品質管理マニュアル等の整備

品質の維持・向上のため、次に掲げるものを整備していること。

（ア）サービス品質の管理のためのマニュアル

（イ）報告品質に関する約款及び基準

ウ　品質の維持・向上に関する手続等の導入状況

品質の維持・向上のため、次に掲げる手続等を行っていること。

（ア）デジタルフォレンジックサービスを行った案件について、当該案件に従事した者又は（１）アの要件を満たす者が調査報告書についてレビューを行っていること。

（イ）デジタルフォレンジックサービスに従事する者に対して例示７－３に定める継続的なデジタルフォレンジック技術資格維持コース又は同等のものを受講させ並びに教育及び研修を実施し又は受講させていること。

（ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続についてデジタルフォレンジックサービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

４　セキュリティ監視・運用サービスに係る審査基準

（１）技術要件

セキュリティ監視・運用サービスを提供しようとする者は、次に掲げる技術要件に該当するものであること。

ア　専門性を有する者の在籍状況

サービス品質の確保のため、セキュリティ監視・運用サービスに従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させているとともに、要件を満たす者ごとの人数を明らかにすること。

（ア）例示１－４に定める資格又は同等のものを有する者

（イ）例示２－３に定める専門家コミュニティ又は同等のものにおける講師若しくはリーダーの経験又は高等教育機関におけるセキュリティ監視・運用サービスの技術を対象とする講師経験を有する者

（ウ）次のいずれかの事業において基準となる日から起算して過去３年間に合計５件（契約件数。継続的な契約の場合は１年間分で１件とみなす。）以上かつ運用年数のべ１０年以上の実績を有する者

ａ　マネージドセキュリティサービス

ｂ　セキュリティアプライアンス製品の運用

（エ）例示３－３に定めるサービス品質確保に資する研修又は同等のものを修了している者

イ　サービス仕様の明示

サービス品質の確保のため、例示６－１に定める内容又は同等のものに従ってセキュリティ監視・運用サービスが行われていることを明らかにしていること。

（２）品質管理要件

セキュリティ監視・運用サービスを提供しようとする者は、次に掲げる品質管理要件に該当するものであること。

ア　品質管理者の割当状況

品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。

イ　品質管理マニュアルの整備

品質の維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。

（ア）サービス提供プロセスの管理

（イ）アウトプットの管理

ウ　品質の維持・向上に関する手続等の導入状況

品質の維持・向上のため、次に掲げる手続等を行っていること。

（ア）従事者の確保及び作業の実施等についてサービスの品質の維持・向上に関する管理の取組が行われていること。

（イ）セキュリティ監視・運用サービスに従事する者に対して例示７－４に定める継続的な教育及び研修等又は同等のもののいずれかを実施又は受講させていること。

（ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続についてセキュリティ監視・運用サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

５　機器検証サービスに係る審査基準

（１）技術要件

機器検証サービスを提供しようとする者は、次に掲げる技術要件に該当するものであること。

ア　専門性を有する者の在籍状況

（ア）サービス品質の確保のため、機器検証サービスの機器検証に従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。

①　例示１－５に定める資格又は同等のものを有する者

②　基準となる日から起算して過去３年間に合計で５件（契約件数。包括的な契約の場合は１年間分で１件とみなす。）以上の実績（診断方法は問わない。）を有する者

③　例示３－４に定めるサービス品質確保に資する研修又は同等のものを修了している者

（イ）サービス品質の確保のため、機器検証サービスの脆弱性診断に従事する者は脆弱性診断サービスの「ア　専門性を有する者の在籍状況」に示す要件を満たす者を業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。

なお、（ア）と（イ）の要件を同一人が満たす場合には、それぞれの要件の充足状況の確認のため、兼務者として人数を明らかにすること。

イ　サービス仕様の明示

（ア）サービス品質の確保のため、機器検証については例示４－４、Webアプリケーション脆弱性診断及びプラットフォーム脆弱性診断については例示４－２－１に定める基準又は同等のものに従って、サービスが行われていること。

（イ）機器検証においては、例示６－２に定める内容又は同等のものに従ってサービスが行われていることを明らかにするとともに、例

示５－２に定める検証の結果の取扱又は同等のものを明らかにしていること。脆弱性診断においては、脆弱性診断サービスの「イ サービス仕様の明示」に示す要件を満たすこと。

（ウ）検証の対象と範囲を明示し、その対象と範囲についてのみ検証に対する責任を有することを表明すること。

（２）品質管理要件

機器検証サービスを提供しようとする者は、次に掲げる品質管理要件に該当するものであること。

ア　品質管理者の割当状況

品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。

イ　品質管理マニュアルの整備

品質維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルや規則等を整備していること。

（ア）サービス提供プロセスの管理

・　サービス利用者（検証依頼者）との仕様調整（例：検証計画、検証対象範囲、実施内容、情報の取り扱い）に関する内容

・　サービス実施方法に関する内容

・　サービス利用者からの要求、意見、クレーム等への対応に関する内容

（イ）アウトプットの管理

ウ　品質の維持・向上に関する手続等の導入状況

品質の維持・向上のため、次に掲げる手続等を行っていること。

（ア）機器検証サービスを行った案件について、当該案件に従事した者以外の者が検査実施報告書についてレビューを行っていること。

（イ）機器検証サービスに従事する者に対して例示７－５に定める教育及び研修等または同等のもののいずれかを実施又は受講させていること。

（ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続について機器検証サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。