# 情報セキュリティサービス基準

経済産業省

平成 30 年 2 月 28 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、デジタルフォレンジックサービス及びセキュリティ監視・運用サービスのいずれか又は全てのサービスをいう。

（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　スマートフォンアプリケーション脆弱性診断

（４）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

（５）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

## 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、附則１－１に定める資格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、附則１－２に定める基準に従って、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）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附則１－３に定める教育及び研修等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）附則２－１に定める資格を有する者

（イ）附則２－２に定める専門家コミュニティ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　スマートフォンアプリケーション脆弱性診断

（エ）附則２－３に定めるサービス品質確保に資する研修を修了している者

イ　サービス仕様の明示

サービス品質の確保のため、附則２－４に定める基準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、附則２－５に定める脆弱性診断の結果の取扱い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）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附則２－６に定める教育及び研修等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。

## 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）附則３－１に定める資格を有する者

（イ）附則３－２に定める専門家コミュニティ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）附則３－３に定めるサービス品質確保に資する研修を修了している者

イ　サービス仕様の明示

サービス品質の確保のため、附則３－４に定める基準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附則３－５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の受講並びに教育及び研修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）附則４－１に定める資格を有する者

（イ）附則４－２に定める専門家コミュニティ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）附則４－３に定めるサービス品質確保に資する研修を修了している者

イ　サービス仕様の明示

サービス品質の確保のため、附則４－４に定める内容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み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附則４－５に定める継続的な教育及び研修等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。

## 附則

第２章各項における要件の詳細は次のとおりとする。なお、本附則の内容は、情報セキュリティ技術の進歩の速度と情報セキュリティサービスへの要求の変化に鑑み、第１章第１項に示す目的の継続的な達成のため、基準等については常に最新のものを参照しつつ、適宜見直しを行うこととする。

### １．　情報セキュリティ監査サービスに関する附則

| | |
|---|---|
| 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以下に例示する内容相当の資格 | |
| | ・ 公認情報セキュリティ監査人<br>・ 公認システム監査人<br>・ CISA（Certified Information System Auditor）<br>・ システム監査技術者 |
| ２　情報セキュリティ監査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<br>・ 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 |
| ３　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<br>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。）<br>・ 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）<br>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。） |

### ２．　脆弱性診断サービスに関する附則

| | |
|---|---|
| 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以下に例示する内容相当の資格 | |
| | ・ 情報処理安全確保支援士<br>・ CEH（Certified Ethical Hacker）<br>・ CISSP（Certified Information Systems Security Professional）<br>・ CISA |

| | |
|---|---|
| | ・ CISM（Certified Information Security Manager）<br>・ GIAC（Global Information Assurance Certification） |
| ２　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以下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）<br>・ 日本セキュリティオペレーション事業者協議会（ISOG-J）<br>・ OWASP（The Open Web Application Security Project） |
| ３　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以下に例示する内容相当の研修 | |
| | ・ SANS Security Courses（504, 542, 560） |
| ４　脆弱性診断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】<br>・ OWASP の定める ASVS（Application Security Verification Standard）レベル１以上<br>・ 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<br>・ OWASP が定める「Security Testing Guideline」<br>・ 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」<br><br>【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】<br>・ Vulnerability Explorer（VEX）<br>・ IBM Security AppScan<br><br>【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】<br>・ QualysGuard<br>・ Tripwire IP360/PureCloud<br>・ Nessus<br>・ Metasploit<br>・ OpenVAS |
| ５　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 | |

| | |
|---|---|
| | 示方法の例示 |
| | ・ ツール出力についての分析を含んだ診断を実施する。<br>・ 診断結果報告書としてとりまとめる。<br>・ 診断結果に関する報告会を開催する。 |
| ６ | 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<br>➢ 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。）<br>➢ 附則２－２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<br>➢ 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。<br>➢ 附則２－１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 |

## ３．　デジタルフォレンジックサービスに関する附則

| | |
|---|---|
| １ | 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以下に例示する内容相当の資格 |
| | ・ 情報処理安全確保支援士<br>・ CISSP |
| 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以下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） |
| ３ | 当該研修の修了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以下に例示する内容相当の研修 |
| | ・ SANS Forensic Courses (500, 508, 558, 572, 578, 610)<br>・ Guidance (DF120, DF210)<br>・ AccessData (FTK BootCamp)<br>・ 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 |
| ４ | 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以下に例示する内容相当の基準及びその明示方法の例示 |
| | ・ 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 |

| | |
|---|---|
| | ジック研究会作成の「証拠保全ガイドライン」に準拠)。<br>・ 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。<br>・ 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。 |
| ５　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 | |
| | ・ 附則３－１に定める資格を満たす者<br>各資格に定められた教育及び研修<br>・ 附則３－１に定める資格を満たさない者<br>年間３５時間以上の次に掲げる活動のいずれか<br>➢ 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、附則３－１、３－２、３－３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。）<br>➢ 附則３－２に定める専門家コミュニティにおける活動 |

## ４．　セキュリティ監視・運用サービスに関する附則

| | |
|---|---|
| １　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以下に例示する内容相当の資格 | |
| | ・ 情報処理安全確保支援士<br>・ CISA<br>・ CISM<br>・ CISSP<br>・ GIAC |
| ２　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以下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<br>・ 日本セキュリティオペレーション事業者協議会<br>・ 日本コンピュータインシデント対応チーム協議会（NCA）<br>・ $(ISC)^2$（International Information Systems Security Certification Consortium）<br>・ ISACA<br>・ SANS |

| | |
|---|---|
| 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以下に例示する内容相当の研修 | |
| | ・ SANS Security Courses (501, 503, 511) |
| ４　セキュリティ監視・運用サービスの提供において用いる以下に例示する内容及びその明示方法の例示 | |
| | ・ 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。<br>・ SLA/SLO/約款において、可用性に関する指標を示す。<br>・ 次に例示すような具体的なサービス内容を示す。<br>➢ 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。<br>➢ 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。<br>・ 次に例示すような具体的なサービス提供体制を示す<br>➢ 組織的な運用体制が存在し、属人的な運用に依存しない。<br>➢ 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。<br>➢ 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。 |
| ５　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<br>➢ 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。）<br>➢ 附則４－２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<br>➢ 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。<br>➢ 附則４－１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 |