

サーベイランス仕様書

2020年9月29日

特定非営利活動法人日本セキュリティ監査協会
情報セキュリティサービス基準審査登録委員会

1. 件名

情報セキュリティサービス基準適合サービスリスト掲載サービスのサーベイランス業務

2. 目的

2020年6月末時点で情報セキュリティサービス基準適合サービスリスト（以下、「リスト」と言います。）に掲載されているサービス及びその提供事業者を対象とするサーベイランスに関して、利害関係を有しない監査業務経験者の立場である専門評価員が、関連文書の審査、調査対象事業者への訪問調査等のサーベイランス業務を実施する。

3. 作業内容及び実施方法

（1）サーベイランス項目の作成

特定非営利活動法人日本セキュリティ監査協会（以下、「JASA」という。）が契約時に指定するサービスについて、当該サービスの提供事業者（以下、「調査対象事業者」という。）による申請書類、及び JASA が提供するチェックリスト雛形（本仕様書巻末の別紙1～4参照）をもとに、申請書類に記載された内容が信じるに足り、虚偽がないことを確認するために必要と考えられるサーベイランス項目を作成し、JASA の承認を得ること。なお、チェックリスト雛形は契約時に Microsoft Excel ワークシート形式の電子ファイルにて提供する。雛形の変更の必要がなければそのままサーベイランスに使用して差し支えない。

（2）サーベイランスの実施

（1）で作成したサーベイランス項目について、次の2種類の調査を通じて確認すること。

① 文書調査

調査対象事業者が提供する、次に例示するような文書をもとにサーベイランス項目の確認を行う。

- ・要員リスト
- ・要員の有する資格や活動、教育・研修受講等に関するエビデンスに相当する文書
- ・品質管理マニュアルに相当する文書
- ・各種手続に関する文書

なお、サーベイランスに必要な文書は、（1）の結果をもとに JASA から調査対象事業者
に提供ないし開示を求めることとし、本業務の受託者から調査対象事業者に依頼する必要

はない。ただし、調査対象事業者が文書の開示場所を調査対象事業者の事業所に指定した場合は、②の調査を実施する際に確認するようにすること。

また、文書調査を通じて申請書類と文書調査で確認した文書との内容の不整合等が認められた場合は、②の訪問調査の際にその理由等について確認すること。

② 訪問調査

調査対象事業者を訪問することにより、以下の確認を行う。

- ・調査対象事業者の事業所での開示と指定された文書の確認
- ・①で実施する文書調査では把握困難ないし把握不十分な項目についての、調査対象事業者の担当者へのヒアリング調査による確認（このとき、品質管理責任者へのヒアリング調査は必ず行うこと）
- ・申請書類と文書調査で確認した文書との内容の不整合等についての確認

実施に際しては、最小限の訪問調査で必要な情報を得られるよう、ヒアリング対応者等に関して調査対象事業者と適宜調整を行った上で実施すること。

(3) サーベイランス報告書の作成

(2)の結果をサーベイランス報告書としてとりまとめる。サーベイランス報告書には、次の内容を含めること。

- ・サーベイランス項目の選定意図
- ・サーベイランス項目毎の確認内容（参照した文書等、確認結果）
- ・申請書類との不整合が存在した場合、その発生経緯
- ・上記2点を踏まえた申請書類の記載内容の妥当性についての判断

4. 納入物

作業報告書 一式（電子媒体 1部）

5. 納入条件

納入期日： 2020年12月31日

納入場所： 特定非営利活動法人日本セキュリティ監査協会

6. その他

業務遂行に際して本仕様で判断不能な事項が発生した場合は、双方協議の上決定する。

別紙1) チェックリスト案 - 情報セキュリティ監査サービス(1/3)

情報セキュリティサービス基準の定める要件		チェック項目 (情報セキュリティ監査)	専門評価員が行うこと	
			確認するエビデンス	文書調査/往査での確認
(前提)	調査対象サービスが実在すること	申請書に記載された名称のサービスが実在するか	顧客向けパンフレット、ホームページ	サービス名称の一致、または通称や別名が存在する場合は対応関係を確認
① 技術要件	ア 専門性を有する者が申請のとおりに在籍しているか	明示された技術責任者が業務に従事しているか	サービスの技術責任者が誰かわかるもの・辞令またはサービスの要員名簿、体制図等	明示されたリストに記載の技術責任者が、当該サービスの要員として割り当てられていることを確認
		技術責任者は基準に定められた技術要件を満たしているか	合格証ほか、附則記載の資格が有効であることのエビデンス	リストに明示されたすべての技術責任者の資格が、申請時に有効であることを確認
	イ サービス仕様申請のとおりに明示されているか	附則に定められた基準に従ってサービスが行われていることが明示されているか	サービスの仕様を定義した文書・申請書に記載したホームページ、契約・約款等	附則に定める内容相当の基準をサービスで用いる旨が記載されていることを確認

別紙1) チェックリスト案- 情報セキュリティ監査サービス(2/3)

情報セキュリティサービス基準の定める要件		チェック項目 (情報セキュリティ監査)	専門評価員が行うこと	
			確認するエビデンス	文書調査/往査での確認
② 品質管理要件 (1/2)	ア 品質管理者が申請のとおりに割り当てられているか	品質管理者が申請の通りに割り当てられているか	品質管理者が割り当てられていることがわかるもの・辞令または体制図、組織図等	品質管理者が申請内容に一致することを確認し、当事者へのヒアリングでも確認
		品質管理マニュアルが申請のとおりに整備されているか	「品質管理マニュアル」相当文書	品質管理者に対し、品質管理マニュアルの運用方法・手順を確認
		(ア) サービス提供プロセスの管理 品質管理マニュアルにはサービス提供プロセスの管理に関する内容が記載されているか	「品質管理マニュアル」相当文書	「品質管理マニュアル作成の手引き（情報セキュリティ監査サービス）」の2.（「サービス提供プロセスの管理」について）に記載の内容相当が記載されていることを確認
(イ) アウトプットの管理 品質管理マニュアルにはアウトプットの管理に関する内容が記載されているか	「品質管理マニュアル」相当文書	「品質管理マニュアル作成の手引き（情報セキュリティ監査サービス）」の3.（「アウトプットの管理」について）に記載の内容相当が記載されていることを確認		

別紙1) チェックリスト案- 情報セキュリティ監査サービス(3/3)

情報セキュリティサービス基準の定める要件		チェック項目 (情報セキュリティ監査)	専門評価員が行うこと		
			確認するエビデンス	文書調査/ 往査での確認	
② 品質管理要件 (2/2)	品質の維持・向上に関する手続きが申請とあり行われているか	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のレビューを行うことが手続として定められているか	情報セキュリティ監査の作業マニュアル、手順書等の文書	監査計画及び監査報告書のレビューを行うことが定められていることを確認	
		当該案件に従事した者以外の者による監査計画及び監査報告書のレビューが手続に従って行われているか	レビューコメント、確認印等、レビューを行ったことのエビデンス	手続に定められた通りのレビューが行われていることを確認	
	品質の維持・向上に関する手続きが申請とあり導入されているか	(イ) 情報セキュリティサービスに従事する者に対して、情報セキュリティサービス基準の附則に定める教育又は研修等のいずれかを申請のとおり実施又は受講させているか	サービスに従事する者に対して、附則に定める教育及び研修のいずれかを実施又は受講させることが手続として定められているか	要員に対する教育・研修に関する手続を定めている文書・情報セキュリティ監査の担当部署における人材育成計画、研修計画、品質管理計画等、	附則に定める教育及び研修のいずれかを実施又は受講させることが手続として定められていることを確認
		サービスに従事する者は、附則に定める教育及び研修のいずれかを手続に従って実施又は受講しているか	社外実施分については受講報告書、終了証明書等、社内実施分については研修開催記録、出席者名簿等の教育・研修実績のわかるもの	附則に定める教育及び研修のいずれかを手続に従って実施又は受講していることを確認	
	(ウ) 申請のとおり、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か	顧客の情報を保護するための手続が定められているか	顧客の情報の保護を定めた社内規定や手続等の文書	顧客の情報を保護するための手続が定められていることを確認	
		顧客の情報は、手続に従って保護されているか	情報の管理状況に関する監査結果	顧客の情報に対して保護のための適切な対策が講じられていることを確認	
	当該案件の担当者以外による監査（内部監査又は外部監査）の実施により、手続の実効性が確保されているか	監査実施報告書相当の文書	当該案件の担当者以外により、適切に監査が実施されていることを確認		

別紙2) チェックリスト案- 脆弱性診断サービス(1/3)

情報セキュリティサービス基準の定める要件		チェック項目 (脆弱性診断)	専門評価員が行うこと		
			確認するエビデンス	文書調査/ 往査での確認	
(前提)	調査対象サービスが実在すること	申請書に記載された名称のサービスが実在するか	顧客向けパンフレット、ホームページ	サービス名称の一致、または通称や別名が存在する場合は対応関係を確認	
① 技術要件	技術責任者が要件の通りに割り当てられているか	技術責任者が要件の通りに割り当てられているか	サービスの技術責任者が誰かわかるもの・辞令またはサービスの要員名簿、体制図等	技術責任者が要件の通りに割り当てられていることを確認	
		技術責任者は基準に定められた技術要件を満たしているか	右のいずれか	(ア) 合格証ほか、附則記載の資格が有効であることのエビデンス (イ) 専門家コミュニティにおけるワーキンググループ等の活動計画、活動報告書、講演予稿、議事録等もしくは高等教育機関におけるシラバス等 (ウ) 診断実施計画書、報告書等、技術責任者が過去3年間に5件以上の脆弱性診断に従事していることを示すもの (エ) 研修の履修証明書または相当するエビデンス	申請時から継続して資格が有効であることを確認 申請時の対象者が専門家コミュニティにおいて講師又はリーダーとして活動した経験を有することを確認 申請時の実績数が要件を満たすことを確認 申請時の所定の研修を修了済みであることを確認
	基準2.(1)アの(ア)～(エ)の各項目を満たす要員数は申請書の通りか（申請後の異動は差し支えない）	右の要件に対応するそれぞれの人数	右の要件に対応するそれぞれの人数	(ア) 合格証ほか、附則記載の資格が有効であることのエビデンス (イ) 専門家コミュニティにおけるワーキンググループ等の活動計画、活動報告書、講演予稿、議事録等もしくは高等教育機関におけるシラバス等 (ウ) 診断実施計画書、報告書等、技術責任者が過去3年間に5件以上の脆弱性診断に従事していることを示すもの (エ) 研修の履修証明書または相当するエビデンス	申請時から継続して資格が有効であることを確認 申請時の対象者が専門家コミュニティにおいて講師又はリーダーとして活動した経験を有することを確認 申請時の実績数が継続して要件を満たすことを確認 申請時の所定の研修を修了済みであることを確認
		申請書の記載と一致するかどうか	(ア)～(エ)の各条件を満たす要員数が申請内容と一致することを確認		
サービス仕様	サービス仕様が申請とあり明示されているか	附則に定められた基準に従ってサービスが行われていることが明示されているか 附則に定められた診断結果の取扱いは明瞭に明示されているか	サービスの仕様を定義した文書（申請書に記載したホームページ、契約・約款等） サービスの仕様を定義した文書（申請書に記載したホームページ、契約・約款等）	附則に定める内容相当の診断サービスが明示され、運用されていることを確認 附則に定める結果の取扱方法に相当する診断結果の取り扱いが明示され、運用されていることを確認	

別紙2) チェックリスト案- 脆弱性診断サービス(2/3)

情報セキュリティサービス基準の定める要件		チェック項目 (脆弱性診断)	専門評価員が行うこと	
			確認するエビデンス	文書調査/往査での確認
② 品質管理要件 (1/2)	品質管理者が申請のとおり割り当てられているか	品質管理者が申請の通りに割り当てられているか	品質管理者が割り当てられていることがわかるもの ・辞令または体制図、組織図等	品質管理者が申請内容に一致することを確認し、当事者へのヒアリングでも確認
	品質管理マニュアルが申請のとおり整備されているか。特に、右の内容が申請のとおりであるか	品質管理マニュアルが申請のとおり整備されているか	「品質管理マニュアル」相当文書	品質管理者に対し、品質管理マニュアルの活用方法を確認
		(ア) サービス提供プロセスの管理 品質管理マニュアルにはサービス提供プロセスの管理に関する内容が記載されているか	「品質管理マニュアル」相当文書	「品質管理マニュアル作成の手引き（脆弱性診断サービス）」の2.（「サービス提供プロセスの管理」について）に記載の内容相当が記載されていることを確認 左記に加えて事例をベースに品質管理マニュアルがどのように使われているかを確認
(イ) アウトプットの管理 品質管理マニュアルにはアウトプットの管理に関する内容が記載されているか	「品質管理マニュアル」相当文書	「品質管理マニュアル作成の手引き（脆弱性診断サービス）」の3.（「アウトプットの管理」について）に記載の内容相当が記載されていることを確認		

別紙2) チェックリスト案- 脆弱性診断サービス(3/3)

情報セキュリティサービス基準の定める要件		チェック項目 (脆弱性診断)	専門評価員が行うこと	
			確認するエビデンス	文書調査/往査での確認
② 品質管理要件 (2/2)	品質の維持・向上に関する手続きが申請のとおり行われているか	当該案件に従事した者以外の者が検査実施報告書のレビューを行うことが手続として定められているか	脆弱性診断の作業マニュアル、手順書等の文書	検査実施報告書のレビューを行うことが定められていることを確認
		当該案件に従事した者以外の者による検査実施報告書のレビューが手続に従って行われているか	レビューコメント、確認印等、レビューを行ったことのエビデンス	手続に定められた通りのレビューが行われていることを確認
	品質の維持・向上に関する手続きが申請のとおり導入されているか	サービスに従事する者に対して、附則に定める教育及び研修のいずれかを実施又は受講させることが手続として定められているか	脆弱性診断の担当部署における人材育成計画、研修計画、品質管理計画等、要員に対する教育・研修に関する手続を定めている文書	附則に定める教育及び研修のいずれかを実施又は受講させることが手続として定められていることを確認
		サービスに従事する者は、附則に定める教育及び研修のいずれかを申請のとおり実施又は受講させているか	社外実施分については受講報告書、終了証明書等、社内実施分については研修開催記録、出席者名簿等の教育・研修実績のわかるもの	附則に定める教育及び研修のいずれかを手続に従って実施又は受講していることを確認
申請のとおり、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か	顧客の情報を保護するための手続が定められているか	顧客の情報の保護を定めた社内規定や手続等の文書	顧客の情報を保護するための手続が定められていることを確認	
	顧客の情報は、手続に従って保護されているか	情報の管理状況に関する監査結果	顧客の情報に対して保護のための適切な対策が講じられていることを確認	
	当該案件の担当者以外による監査（内部監査又は外部監査）の実施により、手続の実効性が確保されているか	監査実施報告書相当の文書	当該案件の担当者以外により、適切に監査が実施されていることを確認	

別紙3) チェックリスト案-デジタルフォレンジックサービス(1/3)

情報セキュリティサービス基準の定める要件		チェック項目 (デジタルフォレンジック)	専門評価員が行うこと	
			確認するエビデンス	文書調査/往査での確認
(前提)	調査対象サービスが実在すること	申請書に記載された名称のサービスが実在するか	顧客向けパンフレット、ホームページ	サービス名称の一致、または通称や別名が存在する場合は対応関係を確認
① 技術要件	ア 専門性を有する者が申請のとおり在籍しているか	技術責任者が要件の通りに割り当てられているか	サービスの技術責任者が誰かわかるもの・辞令またはサービスの要員名簿、体制図等	技術責任者が要件の通りに割り当てられていることを確認
		技術責任者は基準に定められた技術要件を満たしているか	右のいずれか (ア) 合格証ほか、附則記載の資格が有効であることのエビデンス (イ) 専門家コミュニティにおけるワーキンググループ等の活動計画、活動報告書、講演予稿、議事録等もしくは高等教育機関におけるシラバス等 (ウ) 研修の履修証明書または相当するエビデンス	申請時から継続して資格が有効であることを確認 申請時に対象者が専門家コミュニティの講師又はリーダーとして活動した経験もしくは高等教育機関における講師経験を有することを確認 申請時の所定の研修を修了済みであることを確認
		基準3.(1)アの(ア)～(ウ)の各項目を満たす要員数は申請書の通りか(申請後の異動は差し支えない)	右の要件に対応するそれぞれの人数	(ア) 合格証ほか、附則記載の資格が有効であることのエビデンス (イ) 専門家コミュニティにおけるワーキンググループ等の活動計画、活動報告書、講演予稿、議事録等もしくは高等教育機関におけるシラバス等 (ウ) 研修の履修証明書または相当するエビデンス
	イ サービス仕様申請のとおり明示されているか	附則に定められた基準に従ってサービスが行われていることが明示されているか	サービスの仕様を定義した文書(申請書に記載したホームページ、契約・約款等)	申請書に記載した内容を文書調査/往査で確認 附則に定める内容相当の基準をサービスで用いる旨が記載されており、運用されていることを確認

別紙3) チェックリスト案-デジタルフォレンジックサービス(2/3)

情報セキュリティサービス基準の定める要件		チェック項目 (デジタルフォレンジック)	専門評価員が行うこと	
			確認するエビデンス	文書調査/往査での確認
② 品質管理要件 (1/2)	ア 品質管理者が申請のとおり割り当てられているか	品質管理者が申請の通りに割り当てられているか	品質管理者が割り当てられていることがわかるもの・辞令または体制図、組織図等	品質管理者が申請内容に一致することを確認し、当事者へのヒアリングでも確認
	イ 品質管理マニュアルが申請のとおり整備されているか。特に、右の内容が申請のとおりであるか	(ア) サービス品質の管理のためのマニュアルが申請のとおり整備されているか (イ) 報告品質に関する約款及び基準	「サービス品質の管理のためのマニュアル」相当文書 報告品質に関する約款及び基準が申請のとおり整備されているか	「サービス品質の管理のためのマニュアル」相当文書 品質管理者に対し、当該マニュアルが品質の維持・向上に用いられていることを確認 品質管理者に対し、当該約款及び基準が品質の維持・向上に用いられていることを確認

別紙3) チェックリスト案-デジタルフォレンジックサービス(3/3)

情報セキュリティサービス基準の定める要件		チェック項目 (デジタルフォレンジック)	専門評価員が行うこと	
			確認するエビデンス	文書調査/往査での確認
② 品質管理要件 (2/2)	品質の維持・向上に関する手続きが申請のとおりで導入されているか	(ア) 品質の維持・向上に関する手続きが申請のとおりで行われているか	デジタルフォレンジックの作業マニュアル、手順書等の文書	調査報告書のレビューを行うことが定められていることを確認
		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技術責任者の要件を満たす者による調査報告書のレビューが申請のとおりで実施されているか	レビューコメント、確認印等、レビューを行ったことのエビデンス	手続に定められた通りのレビューが行われていることを確認
		(イ) 情報セキュリティサービスに従事する者に対して、情報セキュリティサービス基準の附則に定める教育又は研修等のいずれかを申請のとおりで実施又は受講させているか	デジタルフォレンジックの担当部署における人材育成計画、研修計画、品質管理計画等、要員に対する教育・研修に関する手続を定めている文書	附則に定めるコース並びに教育及び研修を実施又は受講させることが手続として定められていることを確認
		サービスに従事する者は、附則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手続きに従って実施又は受講しているか	社外実施分については受講報告書、終了証明書等、社内実施分については研修開催記録、出席者名簿等の教育・研修実績のわかるもの	附則に定めるコース並びに教育及び研修を手続きに従って実施又は受講していることを確認
(ウ) 申請のとおりに、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か	顧客の情報を保護するための手続が定められているか 顧客の情報は、手続に従って保護されているか 当該案件の担当者以外による監査（内部監査又は外部監査）の実施により、手続の実効性が確保されているか	顧客の情報の保護を定めた社内規定や手続等の文書 情報の管理状況に関する監査結果 監査実施報告書相当の文書	顧客の情報を保護するための手続が定められていることを確認 顧客の情報に対して保護のための適切な対策が講じられていることを確認 当該案件の担当者以外により、適切に監査が実施されていることを確認	

別紙4) チェックリスト案-セキュリティ監視・運用サービス(1/3)

情報セキュリティサービス基準の定める要件		チェック項目 (セキュリティ監視・運用)	専門評価員が行うこと		
			文書による事実関係の調査 (確認するエビデンス)	往査での確認	
(前提)	調査対象サービスが存在すること	申請書に記載された名称のサービスが実在するか	顧客向けパンフレット、ホームページ	サービス名称の一致、または通称や別名が存在する場合は対応関係を確認	
① 技術要件	専門性を有する者が申請のとおりで在籍しているか	技術責任者が要件の通りに割り当てられているか	サービスの技術責任者が誰かわかるもの ・辞令またはサービスの要員名簿、体制図等 (ア) 合格証ほか、附則記載の資格が有効であることのエビデンス	技術責任者が要件の通りに割り当てられていることを確認 申請時から継続して資格が有効であることを確認	
		技術責任者は基準に定められた技術要件を満たしているか	右のいずれか (イ) 専門家コミュニティにおけるワーキンググループ等の活動計画、活動報告書、講演予稿、議事録等もしくは高等教育機関におけるシラバス等 (ウ) 契約書、作業報告書等、技術責任者が過去3年間に5件以上の運用業務に従事していることを示すもの (エ) 研修の履修証明書または相当するエビデンス	申請時に対象者が専門家コミュニティにおいて講師又はリーダーとして活動した経験を有することを確認 申請時の実績数が要件を満たすことを確認 申請時の所定の研修を修了済みであることを確認	
		基準2.(1)アの(ア)～(エ)の各項目を満たす要員数は申請書の通りか（申請後の異動は差し支えない）	右の要件に対応するそれぞれの人数	(ア) 合格証ほか、附則記載の資格が有効であることのエビデンス (イ) 専門家コミュニティにおけるワーキンググループ等の活動計画、活動報告書、講演予稿、議事録等もしくは高等教育機関におけるシラバス等 (ウ) 契約書、作業報告書等、技術責任者が過去3年間に5件以上の運用業務に従事していることを示すもの (エ) 研修の履修証明書または相当するエビデンス	申請時から継続して資格が有効であることを確認 申請時の対象者が専門家コミュニティにおいて講師又はリーダーとして活動した経験を有することを確認 申請時の実績数が要件を満たすことを確認 申請時に所定の研修を修了済みであることを確認
		サービス仕様が申請のとおりで明示されているか	附則に定められた基準に従ってサービスが行われていることが明示されているか	サービスの仕様を定義した文書（申請書に記載したホームページ、契約・約款等）	附則に定める内容相当のセキュリティ監視・運用を行う旨が記載され、記載のとおりで運用されていることを確認

別紙4) チェックリスト案-セキュリティ監視・運用サービス(2/3)

情報セキュリティサービス基準の定める要件		チェック項目 (セキュリティ監視・運用)	専門評価員が行うこと	
			文書による事実関係の調査 (確認するエビデンス)	往査での確認
② 品質管理要件 (1/2)	ア 品質管理者が申請のとおり割り当てられているか	品質管理者が申請の通りに割り当てられているか	品質管理者が割り当てられていることがわかるもの ・辞令または体制図、組織図等	品質管理者が申請内容に一致することを確認し、当事者へのヒアリングでも確認
	イ 品質管理マニュアルが申請のとおり整備されているか。特に、右の内容が申請のとおりであるか	(ア) サービス提供プロセスの管理 品質管理マニュアルが申請のとおり整備されているか	「品質管理マニュアル」相当文書	品質管理者に対し、品質管理マニュアルの活用方法を確認
		品質管理マニュアルにはサービス提供プロセスの管理に関する内容が記載されているか	「品質管理マニュアル」相当文書	「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)」の2.「(サービス提供プロセスの管理)」について記載の内容相当が記載されていることを確認
(イ) アウトプットの管理 品質管理マニュアルにはアウトプットの管理に関する内容が記載されているか	「品質管理マニュアル」相当文書	「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)」の3.「(アウトプットの管理)」について記載の内容相当が記載されていることを確認		

別紙4) チェックリスト案 -セキュリティ監視・運用サービス(3/3)

情報セキュリティサービス基準の定める要件		チェック項目 (セキュリティ監視・運用)	専門評価員が行うこと		
			文書による事実関係の調査 (確認するエビデンス)	往査での確認	
② 品質管理要件 (2/2)	ウ 品質の維持・向上に関する手続きが申請のとおり導入されているか	(ア) 品質の維持・向上に関する手続きが申請のとおり行われているか	従業員の確保及び作業の実施等についてのサービスの品質の維持・向上に関する管理が手続として定められているか	サービスの運用手続、マニュアル、手順書等の文書	従業員の確保及び作業の実施等についてのサービスの品質の維持・向上に関する管理が行われていることを確認
		従業員の確保及び作業の実施等についてのサービスの品質の維持・向上に関する管理が手続に従って行われているか	レビューコメント、確認印等、レビューを行ったことのエビデンス	従業員の確保及び作業の実施等についてのサービスの品質の維持・向上に関する管理が行われていることを確認	
	(イ) 情報セキュリティサービスにに従事する者に対して、情報セキュリティサービス基準の附則に定める教育又は研修等の実施又は受講させているか	サービスに従事する者に対して、附則に定める継続的な教育及び研修のいずれかを実施又は受講させることが手続として定められているか	サービスの担当部署における人材育成計画、研修計画、品質管理計画等、要員に対する教育・研修に関する手続を定めている文書	附則に定める継続的な教育及び研修のいずれかを実施又は受講させることが手続として定められていることを確認	
	サービスに従事する者は、附則に定める継続的な教育及び研修のいずれかを手続きに従って実施又は受講しているか	社外実施分については受講報告書、終了証明書等、社内実施分については研修開催記録、出席者名簿等の教育・研修実績のわかるもの	附則に定める継続的な教育及び研修のいずれかを手続きに従って実施又は受講していることを確認		
エ 申請のとおり、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か	顧客の情報を保護するための手続が定められているか	顧客の情報を保護するための社内規定や手続等の文書	顧客の情報を保護するための手続が定められていることを確認		
	顧客の情報は、手続に従って保護されているか	情報の管理状況に関する監査結果	顧客の情報に対して保護のための適切な対策が講じられていることを確認		
	当該案件の担当者以外による監査(内部監査又は外部監査)の実施により、手続の実効性が確保されているか	監査実施報告書相当の文書	当該案件の担当者以外により、適切に監査が実施されていることを確認		