F-4-1 チェックリスト

サービス種別	情報セキュリティ監査サービス

No	確　認　事　項		必要な添付資料等	確認☑
(前提)情報セキュリティ監査サービスが実在するか				
1	サービス名称は記載されているか	・サービス名称が記載されたホームページ(URL)と記載されている箇所は明確か	◎URL名、またはホームページの写し	
2		・サービス名称が総称名、通称や別名等の場合、その一部サービスとして情報セキュリティ監査が実施されていることが明確か	◎情報セキュリティ監査サービスとの対応関係が確認できるページの写し	
3		・サービス名称が記載された顧客への提出資料等(添付)が添付されているか	◎サービス名称が記載された顧客への提出資料等	
4	委託先の項目	情報セキュリティサービス基準を満たすために、外部委託している場合、委託先の項目はすべて記入されているか(複数の委託先がある場合、それぞれの委託先の項目は記入されているか)	◎外部委託先リスト	
(1)技術要件				
ア　専門性を有する者の在籍状況				
1	資格を有する技術責任者(監査人)が業務に従事しているか	・資格を有する技術責任者(監査人)が明確か	◎監査人リスト ・通し番号、氏名、保有資格名称、資格登録番号、有効期限、初度登録年	
2		・監査人の資格は附則1-1に例示された資格か		
3		・附則1-1に例示された資格を含め、監査人の資格が例示相当であることを説明した資料が添付されているか	◎保有資格の証書等	
4	資格を有する技術責任者(監査人)のリストの明示方法 ・資格番号の表示のみでもよい	a. HPに明示している場合、記述されたURLで監査人リストが確認できるか	◎URL名、またはページの写し	
5		b. 明示方法がその他の場合、監査人のリストが明示された顧客提出資料が添付されているか	◎監査人が明示された資料等	
イ　サービス仕様の明示				
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基準	・情報セキュリティ監査サービスの提供において用いる、具体的な基準と発行主体が明確か(附則1-2の基準)	(具体的な基準と発行主体について、申請システムに入力)	
2		・例示(附則1-2)以外の基準の場合、例示相当であることが明確か	◎基準の例示相当の説明資料	
3	サービス仕様(基準)の明示の方法	a. URLで基準が確認できるか	◎基準が明示されたHPの写し	
4		b. 契約・約款で基準が確認できるか	◎基準が確認できる契約・約款等	
5		c. その他の場合、添付資料に具体的内容が記載されているか	◎基準が確認できる他の資料	

(2)品質管理要件				
ア．品質管理者(サービス品質の管理に関する担当者)の割り当て状況				
1	品質管理者	・氏名、部署名/役職名、企業名(委託先の場合)、電話、e-mailが明確か	◎品質管理者のリスト	
イ．品質マニュアルの整備状況				
1	品質マニュアル	（ア）サービス提供プロセスの管理について、記述されている箇所が明確か	◎品質マニュアルの表紙と目次等 ・(ア)(イ)の記述個所が確認できるもの(該当部分のコピー等)	
2		（イ）アウトプットの管理について、記述されている箇所が明確か		
ウ．品質の維持・向上に関する手続等の導入状況				
1	（ア）品質の維持・向上に関する手続	a. のレビューを行っているか	(実施の有無を申請システムに入力)	
2		b. の査読を行っているか		
3	（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か	□監査人(技術責任者) 年間20時間以上の教育研修を受けているか （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。）	◎監査人(技術責任者)の教育・研修等の受講リスト ・通し番号、氏名、役責、教育又は研修名称、種別、受講時間又はCPE、教官名(OJTの場合)等	
4		□その他の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時間以上の教育研修を受けているか （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。）	◎技術責任者以外の従事者の教育・研修等の受講リスト ・通し番号、氏名、役責、教育又は研修名称、種別、受講時間又はCPE、教官名(OJTの場合)等	

凡例：太枠内は、選択事項です。

サービス種別	脆弱性診断サービス

No	確　認　事　項		必要な添付資料等	確認☑
(前提)脆弱性診断サービスが実在するか				
1	サービス名称は記載されているか	・サービス名称が記載されたホームページ(URL)と記載されている箇所は明確か	◎URL名、またはホームページの写し	
2		・サービス名称が総称名、通称や別名等の場合、その一部サービスとして脆弱性診断が実施されていることが明確か	◎脆弱性診断サービスとの対応関係が確認できるページの写し	
3		・サービス名称が記載された顧客への提出資料等(添付)が添付されているか	◎サービス名称が記載された顧客への提出資料等	
4	委託先の項目	情報セキュリティサービス基準を満たすために、外部委託している場合、委託先の項目はすべて記入されているか(複数の委託先がある場合、それぞれの委託先の項目は記入されているか)	◎外部委託先リスト	
(1)技術要件				
ア　専門性を有する者の在籍状況				
1	要件を満たす技術責任者が業務に従事しているか ※(ア)～(エ)のいずれかの要件を満たす技術責任者	(ア)　附則２－１に定める資格を有する者 ・有資格者の人数が明確か ・附則2-1に例示された資格を含め、例示相当であることを説明した資料が添付されているか	◎有資格者リスト ・通し番号、氏名、保有資格名称、資格登録番号、有効期限、初度登録年 ◎保有資格の証書等	
2		(イ)-① 附則２－２に定める専門家コミュニティの講師・リーダの経験者 ・講師・リーダ経験者の人数が明確か ・専門家コミュニティが附則2-2例示以外の場合、例示相当であることを説明した資料が添付されているか	◎講師・リーダ経験者リスト ・通し番号、氏名、講師を行った団体名、講演名称の日時又はリーダーしたWG等の名称及び活動期間、所属部署における専門家としての業務開始年月等 ◎専門家コミュニティの例示相当の説明資料	
3		(イ)-②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 ・講師経験者の人数が明確か ・高等教育機関における教育内容が例示相当の専門性を満たすことを説明した資料が添付されているか	◎講師経験者リスト ・通し番号、氏名、講師を行った高等教育機関、講演名称の日時又は活動期間、所属部署における専門家としての業務開始年月等 ◎高等教育機関における教育内容が例示相当の専門性を満たすことを説明した資料	
4		(ウ)以下の実績を有する者 ・実績を有する者の人数は明確か ・各人の実績(業務内容(a～c)・期間(過去3年間)・件数(5件以上)は適切か　※診断方法は問わない 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	◎実績を有する者のリスト ・通し番号、氏名、事業脆弱性、業務開始年月日、業務終了年月日、基準となる年月日、基準日の3年前の年月日	
5		(エ)附則２－3に定める研修を修了した者 ・研修を修了した者の人数は明確か ・研修が附則2-3例示以外の場合、例示相当であることを説明した資料が添付されているか	◎研修修了者リスト ・通し番号、氏名、研修機関名、研修名、研修終了年月日等 ◎研修の例示相当の説明資料	

イ　サービス仕様の明示				
1	附則2－4のサービス品質の確保に資する基準に従い、附則2－5の内容相当の方法で脆弱性診断の結果を取扱っているか	・サービス仕様に、附則2－4のサービス品質の確保に資する基準が明記されているか ・例示(附則2-4)以外の基準の場合、例示相当であることを説明した資料が添付されているか	(下記のサービス仕様が確認できる資料にサービス品質の確保に資する基準明記されていること) ◎基準の例示相当の説明資料	
2		・サービス仕様に、附則2－5の脆弱性診断の結果の取り扱い方法が明記されているか	(下記のサービス仕様が確認できる資料に脆弱性診断の結果の取り扱い方法明記されていること)	
3	サービス仕様の明示の方法	a. URLでサービス仕様が確認できるか	◎サービス仕様が明示されたHPの写し	
4		b. 契約・約款でサービス仕様が確認できるか	◎サービス仕様が確認できる契約・約款等	
5		c. その他の場合、添付資料に具体的内容が記載されているか	◎サービス仕様が確認できる他の資料	
(2)品質管理要件				
ア．品質管理者(サービス品質の管理に関する担当者)の割り当て状況				
1	品質管理者	・氏名、部署名/役職名、企業名(委託先の場合)、電話、e-mailが明確か	◎品質管理者のリスト	
イ．品質マニュアルの整備状況				
1	品質マニュアル	（ア）サービス提供プロセスの管理について、記述されている箇所が明確か	◎品質マニュアルの表紙と目次等 ・(ア)(イ)の記述個所が確認できるもの(該当部分のコピー等)	
2		（イ）アウトプットの管理について、記述されている箇所が明確か		
ウ．品質の維持・向上に関する手続等の導入状況				
1	（ア）第三者による検査実施報告書のレビューを行っているか	・レビューを行っているか	(実施の有無を申請システムに入力)	
2	（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か	□脆弱性診断サービスに従事する者 ・次に掲げる教育及び研修等のいずれかを実施又は受講しているか ➢ 年間20時間以上の教育研修を受けているか （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。） ➢ 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 ➢ 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。 ➢ 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（CPE）による年間20ポイント以上の取得	◎従事する者の教育・研修等の実施または受講状況 ・通し番号、氏名、教育又は研修・講演等名称、実施機関名、種別、受講等の時間又はCPEポイント、期間(開始)、期間(終了)	

凡例：太枠内は、選択事項です。

サービス種別	デジタルフォレンジックサービス

No	確　認　事　項		必要な添付資料等	確認☑
(前提)デジタルフォレンジックサービスが実在するか				
1	サービス名称は記載されているか	・サービス名称が記載されたホームページ(URL)と記載されている箇所は明確か	◎URL名、またはホームページの写し	
2		・サービス名称が総称名、通称や別名等の場合、その一部サービスとしてデジタルフォレンジックが実施されていることが明確か	◎デジタルフォレンジックサービスとの対応関係が確認できるページの写し	
3		・サービス名称が記載された顧客への提出資料等(添付)が添付されているか	◎サービス名称が記載された顧客への提出資料等	
4	委託先の項目	情報セキュリティサービス基準を満たすために、外部委託している場合、委託先の項目はすべて記入されているか(複数の委託先がある場合、それぞれの委託先の項目は記入されているか)	◎外部委託先リスト	
(1)技術要件				
ア　専門性を有する者の在籍状況				
1	要件を満たす技術責任者が業務に従事しているか ※(ア)～(ウ)のいずれかの要件を満たす技術責任者	(ア)　附則3-1に定める資格を有する者 ・有資格者の人数が明確か ・附則3-1に例示された資格を含め、例示相当であることを説明した資料が添付されているか	◎有資格者リスト ・通し番号、氏名、保有資格名称、資格登録番号、有効期限、初度登録年 ◎保有資格の証書等	
2		(イ)-① 附則3-2に定める専門家コミュニティの講師・リーダの経験者 ・講師・リーダ経験者の人数が明確か ・専門家コミュニティが附則3-2例示以外の場合、例示相当であることを説明した資料が添付されているか	◎講師・リーダ経験者リスト ・通し番号、氏名、講師を行った団体名、講演名称の日時又はリーダーしたWG等の名称及び活動期間、所属部署における専門家としての業務開始年月等 ◎専門家コミュニティの例示相当の説明資料	
3		(イ)-②高等教育機関におけるデジタルフォレンジックサービスの技術を対象とする講師経験を有する者 ・講師経験者の人数が明確か ・高等教育機関における教育内容が例示相当の専門性を満たすことを説明した資料が添付されているか	◎講師経験者リスト ・通し番号、氏名、講師を行った高等教育機関、講演名称の日時又は活動期間、所属部署における専門家としての業務開始年月等 ◎高等教育機関における教育内容が例示相当の専門性を満たすことを説明した資料	
4		(ウ)附則3－3に定める研修を修了した者 ・研修を修了した者の人数は明確か ・研修が附則3-3例示以外の場合、例示相当であることを説明した資料が添付されているか	◎研修修了者リスト ・通し番号、氏名、研修機関名、研修名、研修終了年月日等 ◎研修の例示相当の説明資料	

イ　サービス仕様の明示				
1	附則3－4の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か	・サービス仕様に、附則3－4の 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基準が明記されているか ・例示(附則3-4)以外の基準の場合、例示相当であることを説明した資料が添付されているか	(下記のサービス仕様が確認できる資料にサービス品質の確保に資する基準明記されていること) ◎基準の例示相当の説明資料	
2		・サービス仕様に、附則3－4の代表的ツールや製品が が明記されているか ・例示(附則3-4)以外のツールや製品の場合、例示相当であることを説明した資料が添付されているか	(下記のサービス仕様が確認できる資料にサービス品質の確保に資する基準明記されていること) ◎ツールや製品の例示相当の説明資料	
3		・サービス仕様に、附則3－5の対象サービス内容が明記されているか ・例示(附則3-4)以外の対象サービス内容の場合、例示相当であることを説明した資料が添付されているか	(下記のサービス仕様が確認できる資料にサービス品質の確保に資する基準明記されていること) ◎対象サービス内容の例示相当の説明資料	
4	サービス仕様の明示の方法	a. URLでサービス仕様が確認できるか	◎サービス仕様が明示されたHPの写し	
5		b. 契約・約款でサービス仕様が確認できるか	◎サービス仕様が確認できる契約・約款等	
6		c. その他の場合、添付資料に具体的内容が記載されているか	◎サービス仕様が確認できる他の資料	
(2)品質管理要件				
ア．品質管理者(サービス品質の管理に関する担当者)の割り当て状況				
1	品質管理者	・氏名、部署名/役職名、企業名(委託先の場合)、電話、e-mail等が明確か	◎品質管理者のリスト	
イ．品質マニュアルの整備状況				
1	品質マニュアル	（ア）サービス品質の管理のためのマニュアル	◎品質マニュアルの表紙と目次等 ・サービス品質の管理が確認できるもの(該当部分のコピー等)	
2		（イ）報告品質に関する約款及び基準	◎約款及び基準 ・報告品質に関する事項が確認できるもの(該当部分のコピー等)	
ウ．品質の維持・向上に関する手続等の導入状況				
1	（ア）案 件に従事した者又は（１）アの要件を満たす者(技術責任者)が調査報告書につい てレビューを行っているか	・レビューを行っているか	(レビュー実施の有無を申請システムに入力)	
2	（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に定める教育及び研修等の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か	□ 附則３－１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を受けているか □ 附則３－１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を実施又は受講しているか ➢ 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、 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。） ➢ 附則３－２に定める専門家コミュニティにおける活動	◎従事する者の教育・研修等の実施または受講状況 ・通し番号、氏名、教育又は研修・講演等名称、実施機関名、種別、受講等の時間又はCPEポイント、期間(開始)、期間(終了)	

凡例：　太枠内は、選択事項です。

サービス種別	セキュリティ監視・運用サービス

No	確　認　事　項		必要な添付資料等	確認☑
(前提)セキュリティ監視・運用サービスが実在するか				
1	サービス名称は記載されているか	・サービス名称が記載されたホームページ(URL)と記載されている箇所は明確か	◎URL名、またはホームページの写し	
2		・サービス名称が総称名、通称や別名等の場合、その一部サービスとしてセキュリティ監視・運用が実施されていることが明確か	◎セキュリティ監視・運用サービスとの対応関係が確認できるページの写し	
3		・サービス名称が記載された顧客への提出資料等(添付)が添付されているか	◎サービス名称が記載された顧客への提出資料等	
4	委託先の項目	情報セキュリティサービス基準を満たすために、外部委託している場合、委託先の項目はすべて記入されているか(複数の委託先がある場合、それぞれの委託先の項目は記入されているか)	◎外部委託先リスト	
(1)技術要件				
ア　専門性を有する者の在籍状況				
1	要件を満たす技術責任者が業務に従事しているか ※(ア)～(エ)のいずれかの要件を満たす技術責任者	(ア)　附則4-1に定める資格を有する者 ・有資格者の人数が明確か ・附則4-1に例示された資格を含め、例示相当であることを説明した資料が添付されているか	◎有資格者リスト ・通し番号、氏名、保有資格名称、資格登録番号、有効期限、初度登録年 ◎保有資格の証書等	
2		(イ)-① 附則4-2に定める専門家コミュニティの講師・リーダの経験者 ・講師・リーダ経験者の人数が明確か ・専門家コミュニティが附則4-2例示以外の場合、例示相当であることを説明した資料が添付されているか	◎講師・リーダ経験者リスト ・通し番号、氏名、講師を行った団体名、講演名称の日時又はリーダーしたWG等の名称及び活動期間、所属部署における専門家としての業務開始年月等 ◎専門家コミュニティの例示相当の説明資料	
3		(イ)-②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 ・講師経験者の人数が明確か ・高等教育機関における教育内容が例示相当の専門性を満たすことを説明した資料が添付されているか	◎講師経験者リスト ・通し番号、氏名、講師を行った高等教育機関、講演名称の日時又は活動期間、所属部署における専門家としての業務開始年月等 ◎高等教育機関における教育内容が例示相当の専門性を満たすことを説明した資料	
4		(ウ)以下の実績を有する者 ・実績を有する者の人数は明確か ・各人の実績(事業内容(a or b)・期間(過去3年間)・件数(5件以上)・運用年数のべ10年以上)は適切か a マネージドセキュリティサービス	◎実績を有する者のリスト ・通し番号、氏名、事業、業務開始年月日、業務終了年月日、基準となる年月日、基準日の3年前の年月日、延べ運用日数	
5		(エ)附則4－3に定める研修を修了した者 ・研修を修了した者の人数は明確か ・研修が附則4-3例示以外の場合、例示相当であることを説明した資料が添付されているか	◎研修修了者リスト ・通し番号、氏名、研修機関名、研修名、研修終了年月日等 ◎研修の例示相当の説明資料	

イ　サービス仕様の明示				
1	附則4－4の基準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か	・サービス仕様に、附則4－4に例示する内容が明記されているか ➢ 役割や責任の所在(SLA/SLO/約款の設定等) ➢ SLA/SLO/約款における可用性の指標 ➢ 例示された具体的なサービス内容 ➢ 例示された具体的なサービス提供体制 ・例示(附則4-4)以外の基準の場合、例示相当であることを説明した資料が添付されているか	(下記のサービス仕様が確認できる資料にサービス品質の確保に資する基準明記されていること) ◎対象サービス内容の例示相当の説明資料	
2	サービス仕様の明示の方法	a. URLでサービス仕様が確認できるか	◎サービス仕様が明示されたHPの写し	
3		b. 契約・約款でサービス仕様が確認できるか	◎サービス仕様が確認できる契約・約款等	
4		c. その他の場合、添付資料に具体的内容が記載されているか	◎サービス仕様が確認できる他の資料	
(2)品質管理要件				
ア．品質管理者(サービス品質の管理に関する担当者)の割り当て状況				
1	品質管理者	・氏名、部署名/役職名、企業名(委託先の場合)、電話、e-mail等が明確か	◎品質管理者のリスト	
イ．品質マニュアルの整備状況				
1	品質マニュアル	（ア）サービス提供プロセスの管理について、記述されている箇所が明確か	◎品質マニュアルの表紙と目次等 ・(ア)(イ)の記述個所が確認できるもの(該当部分のコピー等)	
2		（イ）アウトプットの管理について、記述されている箇所が明確か		
ウ．品質の維持・向上に関する手続等の導入状況				
1	（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か	・管理の取組みが行われているか	(実施の有無を申請システムに入力)	
2	（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か	□ セキュリティ監視・運用サービスに従事する者 ・次に掲げる活動のいずれかを実施又は受講しているか ➢ 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。） ➢ 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 ➢ 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。 ➢ 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	◎従事する者の教育・研修等の実施または受講状況 ・通し番号、氏名、教育又は研修・講演等名称、実施機関名、種別、受講等の時間又はCPEポイント、期間(開始)、期間(終了)	
3	（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か	・顧客情報の保護の手続きを設けて運用し、実効性を確保しているか	(実施の有無を申請システムに入力)	

凡例：太枠内は、選択事項です。