

	カテゴリ	新稿/変更/削	旧稿番	旧設問	旧選択肢	旧分岐先	新稿番	新設問	新選択肢	新分岐先
1	SM	変更	SM-1	調査対象の業務実行に当たり、外部委託先や外部サービスを利用する場合、その企業名やサービス名を回答してください。 ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 調査対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託	○ 外部委託先(企業名) ○ 外部サービス(サービス名) ○ 該当なし ○ 非公開		SM-1	調査対象業務の実行に当たり、 回答事業者が外部委託先や外部サービスを利用する場合 、その企業名・サービス名を回答してください。 ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 調査対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託	○ 外部委託先(企業名) ○ 外部サービス(サービス名) ○ 該当なし ○ 非公開	・ 「外部委託先」または「外部サービス」が選択: SM-2 SM-3 SM-4
2	SM	変更	SM-2	外部委託先や外部サービスに業務情報を提供する場合、業務情報に企業名、サービス名を回答してください。 ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 調査対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託 ※ 業務情報… 調査対象の業務において、個人情報を含む取引元から提供または預託された情報や当該業務において作成する情報	○ 業務情報を提供する外部委託先 ・ 該当するものすべてを選択してください ■ 業務情報 (個人情報除く) を提供する(企業名) ■ 特定個人情報 (マイナンバー) を提供する(企業名) ■ 要配慮個人情報 (人種、信条、社会的身分、両性等の配慮を要する個人情報) を提供する(企業名) ■ 個人データ (個人情報データベース等を構成する個人情報) を提供する(企業名) ○ 業務情報を提供する外部サービス ・ 該当するものすべてを選択してください ■ 業務情報 (個人情報除く) を提供する(サービス名) ■ 特定個人情報 (マイナンバー) を提供する(サービス名) ■ 要配慮個人情報 (人種、信条、社会的身分、両性等の配慮を要する個人情報) を提供する(サービス名) ■ 個人データ (個人情報データベース等を構成する個人情報) を提供する(サービス名) ■ 上記以外の個人情報提供する(サービス名) ○ 該当なし ○ 非公開		SM-2	調査対象業務の実行に当たり 回答事業者が利用する外部委託先や外部サービスのうち、業務情報を提供するものについて、その企業名・サービス名を回答してください。 [説明補足] 説明SM-1にて回答いただいた 外部委託先や外部サービスを利用します ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 調査対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託 ※ 業務情報… 調査対象の業務において、個人情報を含む取引元から提供または預託された情報や当該業務において作成する情報	○ 業務情報を提供する外部委託先 ・ 該当するものすべてを選択してください ■ 業務情報 (個人情報除く) を提供する(企業名) ■ 特定個人情報 (マイナンバー) を提供する(企業名) ■ 要配慮個人情報 (人種、信条、社会的身分、両性等の配慮を要する個人情報) を提供する(企業名) ■ 個人データ (個人情報データベース等を構成する個人情報) を提供する(企業名) ○ 業務情報を提供する外部サービス ・ 該当するものすべてを選択してください ■ 業務情報 (個人情報除く) を提供する(サービス名) ■ 特定個人情報 (マイナンバー) を提供する(サービス名) ■ 要配慮個人情報 (人種、信条、社会的身分、両性等の配慮を要する個人情報) を提供する(サービス名) ■ 個人データ (個人情報データベース等を構成する個人情報) を提供する(サービス名) ■ 上記以外の個人情報提供する(サービス名) ○ 該当なし ○ 非公開	
3	SM	変更	SM-3	セキュリティインシデントやサービス停止により、調査対象の業務に影響を与える外部委託先・外部サービスがあれば、その企業名・サービス名を回答ください。 ※ セキュリティインシデント… セキュリティに関する事故や故障 (情報漏えいおよび内部不正、外部侵害、ボット・感染、システム障害、作業ミス等を含む) ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 調査対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託	○ 業務やサービスレベルへの影響度が大きい重要な外部委託先(企業名を記載してください) ○ 業務やサービスレベルへの影響度が大きい重要な外部サービス (サービス名を記載してください) ○ 該当なし ○ 非公開		SM-3	調査対象業務の実行に当たり 回答事業者が利用する外部委託先や外部サービスのうち、セキュリティインシデントやサービス停止により業務に影響を与えるものについて、その企業名・サービス名を回答してください。 [説明補足] 説明SM-1にて回答いただいた 外部委託先や外部サービスを利用します ※ セキュリティインシデント… セキュリティに関する事故や故障 (情報漏えいおよび内部不正、外部侵害、ボット・感染、システム障害、作業ミス等を含む) ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 調査対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託	○ 業務やサービスレベルへの影響度が大きい重要な外部委託先(企業名を記載してください) ○ 業務やサービスレベルへの影響度が大きい重要な外部サービス (サービス名を記載してください) ○ 該当なし ○ 非公開	
4	SM	変更	SM-4	再委託に関する取り扱いについて、該当する選択肢をすべて選択してください。 [補足] 再委託とは、調査対象の業務からみた再委託を指します。すなわち、調査対象業務の外部委託先や外部サービスから行われる業務委託を指します	○ 再委託を禁止している ○ 再委託は可能としているが、再々委託以降は禁止している ○ 再委託先以降の追加・変更時に通知することを契約等で定めている ○ 該当なし ○ 非公開		SM-4	調査対象業務に 対して回答事業者の再委託に関する取り扱いについて、該当する選択肢をすべて選択してください。 [補足] 再委託とは、調査対象の業務からみた再委託を指します。すなわち、調査対象業務の外部委託先や外部サービスから行われる業務委託を指します	○ 再委託を禁止している ○ 再委託は可能としているが、再々委託以降は禁止している ○ 再委託先以降の追加・変更時に通知することを契約等で定めている ○ 該当なし ○ 非公開	
5	SM	変更	SM-5	取引元がセキュリティにおける責任を負う観点のみで業務を行う ○ 回答事業者がセキュリティにおける責任を負う観点のみで業務を行う [補足] リモートワークや外部委託先の拠点を含みます ○ 取引元と回答事業者の双方の拠点を利用して業務を行う	・ 「回答事業者がセキュリティにおける責任を負う観点のみで業務を行う」が選択: OA-5 OA-9 OA-10 PH-1 ・ 「取引元と回答事業者の双方の拠点を利用して業務を行う」が選択: OA-5 OA-9 OA-10 PH-1		SM-5	調査対象業務に 対して回答事業者が行う場当たりとして、該当するものを選択してください。 ○ 取引元がセキュリティにおける責任を負う観点のみで業務を行う ○ 回答事業者がセキュリティにおける責任を負う観点のみで業務を行う [補足] リモートワークや外部委託先の拠点を含みます ○ 取引元と回答事業者の双方の拠点を利用して業務を行う	・ 「回答事業者がセキュリティにおける責任を負う観点のみで業務を行う」が選択: OA-6 OA-9 OA-10 OA-11 PH-1 ・ 「取引元と回答事業者の双方の拠点を利用して業務を行う」が選択: OA-6 OA-9 OA-10 OA-11 PH-1	・ 「回答事業者がセキュリティにおける責任を負う観点のみで業務を行う」が選択: OA-6 OA-9 OA-10 OA-11 PH-1
6	SM	変更	SM-6	調査対象業務で利用する端末 (PC、スマートフォン等) について、該当するものを選択してください。 ○ 取引元がセキュリティにおける責任を負う端末のみで業務を行う ○ 回答事業者がセキュリティにおける責任を負う端末のみで業務を行う [補足] 利用端末 (BYOD) や外部委託先部署の端末を含みます ○ 取引元と回答事業者の双方の端末を利用して業務を行う	・ 「回答事業者がセキュリティにおける責任を負う端末のみで業務を行う」が選択: OA-1 OA-2 OA-3 OA-4 OA-6 OA-7 OA-8 ・ 「取引元と回答事業者の双方の端末を利用して業務を行う」が選択: OA-1 OA-2 OA-3 OA-4 OA-6 OA-7 OA-8		SM-6	回答事業者が 調査対象業務で利用する端末(PC、スマートフォン等)について、該当するものを選択してください。 ○ 取引元がセキュリティにおける責任を負う端末のみで業務を行う ○ 回答事業者がセキュリティにおける責任を負う端末のみで業務を行う [補足] 利用端末 (BYOD) や外部委託先部署の端末を含みます ○ 取引元と回答事業者の双方の端末を利用して業務を行う ○ 端末を利用せず業務を行う [回答補足] PC・スマートフォン等の端末を一切利用しない場合に選択してください。また、備考欄には具体的な業務の実行方法を記載してください。(例: 紙の帳票に手書きで記入し、原本を取引元へ郵送している等) ・ 備考(業務の実行方法)	・ 「回答事業者がセキュリティにおける責任を負う端末のみで業務を行う」が選択: OA-1 OA-2 OA-3 OA-4 OA-6 OA-7 OA-8 ・ 「取引元と回答事業者の双方の端末を利用して業務を行う」が選択: OA-1 OA-2 OA-3 OA-4 OA-6 OA-7 OA-8	・ 「回答事業者がセキュリティにおける責任を負う端末のみで業務を行う」が選択: OA-1 OA-2 OA-3 OA-4 OA-6 OA-7 OA-8

No.	カテゴリ	新稿/変更/削除	旧項目	旧説明	旧選択肢	旧分岐先	新項目	新説明	新選択肢	新分岐先
7	SM	変更	SM-7	調査対象業務で利用するシステム環境（アプリケーション、サーバ、ネットワーク等）について、該当するものを選択してください。 [補足] 注意：システム開発や保守、運用案件において、調査対象業務の結果として納品される製品またはシステム自体は対象外です	「取引元がセキュリティにおける責任を負うシステム環境のみで業務を行う」が選択： AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 「調査事業者がセキュリティにおける責任を負うシステム環境のみで業務を行う」が選択： AC-1 AC-2 AC-3 AC-4 AC-5 AC-6 AC-7 AC-8 AC-9 CR-1 PH-2 PH-3 PH-4 PH-5 OP-1 OP-2 OP-3 OP-4 OP-5 OP-6 OP-7 MN-1 NW-1 NW-2 NW-3 NW-4 NW-5 NW-6 SV-1 SV-2 BC-1 BC-2 「取引元と調査事業者の双方のシステム環境を利用して業務を行う」が選択： AC-1 AC-2 AC-3 AC-4 AC-5 AC-6 AC-7 AC-8 AC-9 AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 CR-1 PH-2 PH-3 PH-4 PH-5 OP-1 OP-2 OP-3 OP-4 OP-5 OP-6 OP-7 MN-1 NW-1 NW-2 NW-3 NW-4 NW-5 NW-6 SV-1 SV-2 BC-1 BC-2	SM-7	「調査事業者が調査対象業務で利用するシステム環境（アプリケーション、サーバ、ネットワーク等）について、該当するものを選択してください。」 [補足] 注意：システム開発や保守、運用案件において、調査対象業務の結果として納品される製品またはシステム自体は対象外です	「取引元がセキュリティにおける責任を負うシステム環境（ 取引元のシステム ）のみで業務を行う」が選択： AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 「調査事業者がセキュリティにおける責任を負うシステム環境（ 調査事業者のシステム ）のみで業務を行う」が選択： AC-1 AC-2 AC-3 AC-4 AC-5 AC-6 AC-7 AC-8 AC-9 CR-1 PH-2 PH-3 PH-4 PH-5 OP-1 OP-2 OP-3 OP-4 OP-5 OP-6 OP-7 MN-1 NW-1 NW-2 NW-3 NW-4 NW-5 NW-6 SV-1 SV-2 BC-1 BC-2 「取引元と調査事業者の双方のシステム環境を利用して業務を行う」が選択： AC-1 AC-2 AC-3 AC-4 AC-5 AC-6 AC-7 AC-8 AC-9 AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 CR-1 PH-2 PH-3 PH-4 PH-5 OP-1 OP-2 OP-3 OP-4 OP-5 OP-6 OP-7 MN-1 NW-1 NW-2 NW-3 NW-4 NW-5 NW-6 SV-1 SV-2 BC-1 BC-2		
8	CT	変更	CT-1	情報セキュリティまたは個人情報保護について取得している第三者による認証や評価をすべて選択してください。 ※ SOC2 ... System and Organization Controls 2	□ISO/IEC 27001(登録番号・有効期限・範囲) □ISO/IEC 27011(登録番号・有効期限・範囲) □JISQ 15001(登録番号・有効期限・範囲) □プライバシーマーク(登録番号・有効期限) □SOC2(Type1)(取得年月・評価日・取得範囲) □SOC2(Type2)(取得年月・対象範囲・取得範囲) □ISMAP(登録番号・有効期限) □ISMAP-LIU(登録番号・有効期限) □データセンター-Tier(Tiers 1-4) □その他(詳細) □該当なし □非公開	CT-1	情報セキュリティまたは個人情報保護について、 調査事業者が取得している第三者による認証や評価をすべて選択してください。 ※ SOC2 ... System and Organization Controls 2	□ISO/IEC 27001(登録番号・有効期限・範囲) □ISO/IEC 27011(登録番号・有効期限・範囲) □JISQ 15001(登録番号・有効期限・範囲) □プライバシーマーク(登録番号・有効期限) [補足] 登録番号は枝番を含まない8桁の半角数字で入力してください □SOC2(Type1)(取得年月・評価日・取得範囲) □SOC2(Type2)(取得年月・対象範囲・取得範囲) □ISMAP(登録番号・有効期限) □ISMAP-LIU(登録番号・有効期限) □データセンター-Tier(Tiers 1-4) □その他(詳細) □未取得 □非公開	□ISO/IEC 27001(登録番号・有効期限・範囲) □ISO/IEC 27011(登録番号・有効期限・範囲) □JISQ 15001(登録番号・有効期限・範囲) □プライバシーマーク(登録番号・有効期限) □SOC2(Type1)(取得年月・評価日・取得範囲) □SOC2(Type2)(取得年月・対象範囲・取得範囲) □ISMAP(登録番号・有効期限) □ISMAP-LIU(登録番号・有効期限) □データセンター-Tier(Tiers 1-4) □その他(詳細) □未取得 □非公開	
9	HS	変更	HS-1	過去2年間にホームページ等で公表、または監督官庁や認証機関等へ報告するレベルのセキュリティインシデントが及びました。 ※ セキュリティインシデント…セキュリティに関する事故や故障（情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む）	□はい(詳細) □いいえ □非公開	HS-1	調査事業者において、過去2年間にホームページ等で公表、または監督官庁や認証機関等へ報告するレベルのセキュリティインシデントが及びました。 ※ セキュリティインシデント…セキュリティに関する事故や故障（情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む）	□はい(詳細) □いいえ □非公開	□はい(詳細) □いいえ □非公開	
10	LG	変更	LG-1	個人情報保護に関して対応しているものをすべて選択してください。	□個人情報保護法 □カリフォルニア州法（CCPA/CPRA） □EU一般データ保護規則（GDPR） □その他(詳細) □該当なし □非公開	LG-1	個人情報保護に関して、 調査事業者が対応しているものをすべて選択してください。	□個人情報保護法 □カリフォルニア州法（CCPA/CPRA） □EU一般データ保護規則（GDPR） □その他(詳細) □未取得 □非公開	□個人情報保護法 □カリフォルニア州法（CCPA/CPRA） □EU一般データ保護規則（GDPR） □その他(詳細) □未取得 □非公開	

	カテゴリ	新報/変更/廃止	旧項目	旧説明	旧分岐先	新項目	新説明	新分岐先
11	OR	変更	OR-1	情報セキュリティについて企業としての基本方針や規程類を定めていますか。	☐情報セキュリティに関する基本方針（情報セキュリティポリシー等）を策定している ☐情報セキュリティに関する規程類（対策基準やガイドライン等）を策定している ☐情報セキュリティに関する基本方針や規程類について、定期的な見直しを実施している ☐該当なし ☐非公開	OR-1	情報セキュリティに関する基本方針や規程類を定めていますか。 ☐情報セキュリティに関する基本方針（情報セキュリティポリシー等）を策定している ☐情報セキュリティに関する規程類（対策基準やガイドライン等）を策定している ☐情報セキュリティに関する基本方針や規程類について、定期的な見直しを実施している ☐対応 ☒月に1回以上 ☒半年に1回以上 ☒年に1回以上 ☒1年に1回より少ない（数年に1回など） ☒不定期 ☒非公開 ☐情報セキュリティに関する基本方針や規程類の策定時や見直し時、役員及び従業員へ周知している ☐情報セキュリティに関する基本方針や規程類について、役員及び従業員が定期的に最新情報を参照できる状態としている ☐未実施 ☐非公開	
12	OR	変更	OR-2	情報セキュリティを管理・推進するための責任者や組織体制が定められていますか。該当する選択様をすべて選択してください。	☐情報セキュリティ管理の責任者を定め、職務範囲や権限、責任について定めている ☐情報セキュリティ管理に関する関係部署や業務、機能を用いている ☐該当するものすべてを選択してください ☒セキュリティリスク管理、対策推進を行う体制の整備 ☒情報漏洩や情報収集を実施する脅威インテリジェンス体制の整備 ☒サイバー攻撃に対する監視体制の整備（SOC等 ※MSSなど外部のリソース活用を含む） ☒セキュリティインシデントが発生した場合の対応体制の整備（CSIRT等） ☐その他（詳細欄） ☐情報セキュリティ体制について、連携時だけでなく有事を想定した役割や責任を定めている ☐セキュリティ人材の育成・確保のための計画を策定している ☐自社の責任範囲と外部委託先や外部サービスとの責任範囲を明確にしている ☐該当なし ☐非公開 ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 調査対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SIS等の業務委託 ※ 情報セキュリティ管理の責任者… 役員やCISO等 ※ 有事… セキュリティインシデント発生時等	OR-2	情報セキュリティを管理・推進するための責任者や組織体制が定められていますか。該当する選択様をすべて選択してください。 ☐情報セキュリティ管理の責任者を定め、職務範囲や権限、責任、および連絡体制について定めている ☐情報セキュリティ管理に関する関係部署や業務、機能を用いている ☐該当するものすべてを選択してください ☒セキュリティリスク管理、対策推進を行う体制の整備 ☒情報漏洩や情報収集を実施する脅威インテリジェンス体制の整備 ☒サイバー攻撃に対する監視体制の整備（SOC等 ※MSSなど外部のリソース活用を含む） ☒セキュリティインシデントが発生した場合の対応体制の整備（CSIRT等） ☐その他（詳細欄） ☐情報セキュリティ管理の責任者および関係部署や業務、機能および連絡体制について、定期的に見直しを実施している ☐対応 ☒月に1回以上 ☒半年に1回以上 ☒年に1回以上 ☒1年に1回より少ない（数年に1回など） ☒不定期 ☒非公開 ☐情報セキュリティ体制について、連携時だけでなく有事を想定した役割や責任および連絡体制を定めている ☐セキュリティ人材の育成・確保のための計画を策定している ☐自社の責任範囲と外部委託先や外部サービスとの責任範囲を明確にしている ☐未実施 ☐非公開	
13	OR	変更	OR-3	セキュリティリスク管理として実施していることをすべて選択してください。	☐セキュリティリスクの管理プロセスを策定している ☐該当するものすべてを選択してください ☒セキュリティリスクの特定と評価に関する手続 ☒リスク対応における標準的な対応手続と例外的な対応手続 ☐その他（詳細欄） ☐セキュリティリスクへの対応計画を策定している ☐経営層にリスク評価・結果などが報告されている ☐定期的なセキュリティリスク評価を行っている ☐該当なし ☐非公開	OR-3	セキュリティリスク管理として実施していることをすべて選択してください。 ☐セキュリティリスクの管理プロセスを策定している ☐該当するものすべてを選択してください ☒セキュリティリスクの特定と評価に関する手続 ☒リスク対応における標準的な対応手続と例外的な対応手続 ☐その他（詳細欄） ☐セキュリティリスクへの対応計画を策定している ☐セキュリティリスクへの対応について、経営層が参加して経営判断を行う体制（情報セキュリティ委員会等）を設置している ☐経営層にリスク評価・結果などが報告されている ☐定期的なセキュリティリスク評価を行っている ☐対応 ☒月に1回以上 ☒半年に1回以上 ☒年に1回以上 ☒1年に1回より少ない（数年に1回など） ☒不定期 ☒非公開 ☐未実施	
14	OR	変更	OR-4	セキュリティ対策が正しく実施され意図したとおり運用されているか、関連法令や規制、契約上の要求事項を満たしているかを確立した評価部門により定期的に評価していますか。実施していることをすべて選択してください。	☐内部調査もしくは内部評価 ☐実施頻度 ☐最終実施年月 ☐外部調査もしくは外部評価 ☐実施頻度 ☐最終実施年月 ☐該当なし ☐非公開	OR-4	セキュリティ対策が正しく実施され意図したとおり運用されているかを確立した評価部門により定期的に評価していますか。実施していることをすべて選択してください。 ☐内部調査もしくは内部評価 ☐実施頻度 ☒月に1回以上 ☒半年に1回以上 ☒年に1回以上 ☒1年に1回より少ない（数年に1回など） ☒不定期 ☒非公開 ☐最終実施年月 ☐外部調査もしくは外部評価 ☐実施頻度 ☒月に1回以上 ☒半年に1回以上 ☒年に1回以上 ☒1年に1回より少ない（数年に1回など） ☒不定期 ☒非公開 ☐最終実施年月 ☐未実施 ☐非公開	
15	IM	変更	IM-1	セキュリティインシデントやシステム障害へ対応するための役割や連絡体制について、定めているものを選択してください。	☐セキュリティインシデントやシステム障害が発生した場合の役割および責任を文書化している ☐セキュリティインシデントやシステム障害が発生した場合の連絡先や連絡体制、エスカレーションフローを文書化している ☐該当するものすべてを選択してください ☒自社内の連絡体制、エスカレーションフロー ☒取引先への連絡体制、エスカレーションフロー ☐その他（詳細欄） ☐文書化した内容を定期的に見直ししている ☐該当なし ☐非公開 ※ セキュリティインシデント… セキュリティに関する事故や攻撃（情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む）	IM-1	セキュリティインシデントやシステム障害へ対応するための役割や連絡体制について、定めているものを選択してください。 ☐セキュリティインシデントやシステム障害が発生した場合の役割および責任を文書化している ☐セキュリティインシデントやシステム障害が発生した場合の連絡先や連絡体制、エスカレーションフローを文書化している ☐該当するものすべてを選択してください ☒自社内の連絡体制、エスカレーションフロー ☒取引先への連絡体制、エスカレーションフロー ☐その他（詳細欄） ☐文書化した内容を定期的に見直ししている ☐対応 ☒月に1回以上 ☒半年に1回以上 ☒年に1回以上 ☒1年に1回より少ない（数年に1回など） ☒不定期 ☒非公開 ☐最終実施年月 ☐未実施 ☐非公開	
16	IM	変更	IM-2	セキュリティインシデントやシステム障害に備えて、平時から対応していることをすべて選択してください。	☐脅威情報（インシデント事例等）を収集し、自社の事業・情報資産に与える影響を評価している ☐（取引先からの要請があった場合）収集した脅威情報について、取引先へ提供可能である ☐セキュリティインシデントやシステム障害に対応するためのインシデント対応マニュアルを策定している ☐マニュアルに定められている事項として、該当するものすべてを選択してください ☒インシデントによる業務影響・対応優先度・原因に関する分析 ☒証拠・ログの保全 ☒インシデント対応の記録（インシデントの内容、その対応において取られた行動内容や調査における収集ログの一覧等） ☒サイバー攻撃に対する対応・検知 ☒攻撃者の動向・被害の状況・復旧後の正常稼働確認 ☒インシデント対応計画の作成や見直しにおける外部委託先との連携 ☐その他（詳細欄） ☐セキュリティインシデントやシステム障害へ対応するためのインシデント対応マニュアルを定期的に見直ししている ☐インシデント対応や訓練から学んだ教訓をインシデント対応マニュアルや手順に反映している ☐該当なし ☐非公開 ※ セキュリティインシデント… セキュリティに関する事故や攻撃（情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む） ※ 情報資産… 調査対象の業務において利用するシステムに関連するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等	IM-2	セキュリティインシデントやシステム障害に備えて、平時から対応していることをすべて選択してください。 ☐脅威情報（インシデント事例等）を収集する情報源や検出等を定め、収集した情報が自社の事業・情報資産に与える影響を評価している ☐（取引先からの要請があった場合）収集した脅威情報について、取引先へ提供可能である ☐セキュリティインシデントやシステム障害に対応するためのインシデント対応マニュアルを策定している ☐マニュアルに定められている事項として、該当するものすべてを選択してください ☒インシデントによる業務影響・対応優先度・原因に関する分析 ☒証拠・ログの保全 ☒インシデント対応の記録（インシデントの内容、その対応において取られた行動内容や調査における収集ログの一覧等） ☒サイバー攻撃に対する対応・検知 ☒攻撃者の動向・被害の状況・復旧後の正常稼働確認 ☒インシデント対応計画の作成や見直しにおける外部委託先との連携 ☐その他（詳細欄） ☐セキュリティインシデントやシステム障害へ対応するためのインシデント対応マニュアルを、役員及び従業員へ周知している ☐セキュリティインシデントやシステム障害へ対応するためのインシデント対応マニュアルを定期的に見直ししている ☐インシデント対応や訓練から学んだ教訓を社内共有し、インシデント対応マニュアルや手順に反映している ☐未実施 ☐非公開	

	カテゴリ	新稿/変更/削除	旧項目	旧設例	旧選択例	旧分岐先	新項目	新設例	新選択例	新分岐先
22	AS	変更	AS-4	クリアデスク・クリアスクリーンについて、実施している対策をすべて選択してください。	クリアデスク・クリアスクリーンに関するルールを定めている クリアデスク・クリアスクリーンに関するルールを定期的に見直している クリアデスクを実施している ・該当するものをすべて選択してください ■業務に関わる資料等について、利用時以外の書庫等への保管 ■業務に関わる機密性の高い資料等について、施設可能な書庫・金庫等への保管 ■その他(詳細) クリアスクリーンを実施している ・該当するものをすべて選択してください ■機密性の高いスクリーンロックまたはログオフ ■端末の無操作時間が続いた場合の、端末の自動的なスクリーンロックまたはログオフ ■その他(詳細) 該当なし 非公開		AS-4	クリアデスク/クリアスクリーンについて、 回答事業者が実施している対策をすべて選択してください。 クリアデスク・クリアスクリーンに関するルールを定めている クリアデスク・クリアスクリーンに関するルールを定期的に見直している クリアデスクを実施している ・該当するものをすべて選択してください ■業務に関わる資料等について、利用時以外の書庫等への保管 ■業務に関わる機密性の高い資料等について、施設可能な書庫・金庫等への保管 ■その他(詳細) クリアスクリーンを実施している ・該当するものをすべて選択してください ■機密性の高いスクリーンロックまたはログオフ ■端末の無操作時間が続いた場合の、端末の自動的なスクリーンロックまたはログオフ ■その他(詳細) 該当なし 非公開	クリアデスク・クリアスクリーンに関するルールを定めている クリアデスク・クリアスクリーンに関するルールを定期的に見直している クリアデスクを実施している ・該当するものをすべて選択してください ■業務に関わる資料等について、利用時以外の書庫等への保管 ■業務に関わる機密性の高い資料等について、施設可能な書庫・金庫等への保管 ■その他(詳細) クリアスクリーンを実施している ・該当するものをすべて選択してください ■機密性の高いスクリーンロックまたはログオフ ■端末の無操作時間が続いた場合の、端末の自動的なスクリーンロックまたはログオフ ■その他(詳細) 該当なし 非公開	
23	AS	変更	AS-5	情報資産を保護する方法について、該当する選択例をすべて選択してください。 ※外部サービス…調査対象業務を実施するうえで利用するクラウドサービス ※情報資産…調査対象の業務において利用するシステムに関連するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等 [補足] データや媒体の複製、契約終了後のデータの取り扱いに関するルールがあるかご回答ください。	情報資産（端末、システム、外部サービス、顧客情報、機密情報等）の保護に関するルールを定めている 情報資産の複製・契約終了に関するルールを定期的に見直している 重要度の高い情報資産については安全な方法で複製している ・該当するものをすべて選択してください ■端末（同等化済否や制限） ■破壊（自社での物理的な破壊、盗難、シェレディング） ■複製（複製業者の複製証明書（マニフェスト）があること） ■その他(詳細) 該当なし 非公開		AS-5	情報資産の保護について、 回答事業者が実施している対策をすべて選択してください。 ※ 外部サービス… 調査対象業務を実施するうえで利用するクラウドサービス ※ 情報資産… 調査対象の業務において利用するシステムに関連するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等 [補足] データや媒体の複製、契約終了後のデータの取り扱いに関するルールがあるかご回答ください。 情報資産（端末、システム、外部サービス、顧客情報、機密情報等）の複製・契約終了に関するルールを定めている 情報資産の複製・契約終了に関するルールを定期的に見直している 重要度の高い情報資産については安全な方法で複製している ・該当するものをすべて選択してください ■端末（同等化済否や制限） ■破壊（自社での物理的な破壊、盗難、シェレディング） ■複製（複製業者の複製証明書（マニフェスト）があること） ■複製（複製業者の複製証明書（マニフェスト）があること） ■情報資産の複製・抹消処理を行った記録を保管している ■未実施 非公開	情報資産（端末、システム、外部サービス、顧客情報、機密情報等）の複製・契約終了に関するルールを定めている 情報資産の複製・契約終了に関するルールを定期的に見直している 重要度の高い情報資産については安全な方法で複製している ・該当するものをすべて選択してください ■端末（同等化済否や制限） ■破壊（自社での物理的な破壊、盗難、シェレディング） ■複製（複製業者の複製証明書（マニフェスト）があること） ■複製（複製業者の複製証明書（マニフェスト）があること） ■情報資産の複製・抹消処理を行った記録を保管している ■未実施 非公開	
24	OA	変更	OA-1	端末におけるマルウェア対策について、実施している対策をすべて選択してください。	端末においてマルウェア対策を実施している ・該当するものをすべて選択してください ■既知のマルウェア対策として、アンチウイルスソフトを導入し、リアルタイムスキャン、定期的なウイルススキャンやパターンファイルの更新化を行っている ■未知のマルウェア対策として、EDR製品や振る舞い検知を行う製品を導入している ■その他(詳細) メール経由でのマルウェア感染への対策を実施している ・該当するものをすべて選択してください ■メールフィルタリング機能（不正サイトへのリンクの検出、隔離、ブロック等） ■添付ファイルに対するスキャン機能 ■その他(詳細) 該当なし 非公開		OA-1	回答事業者の端末に対して、実施しているマルウェア対策をすべて選択してください。 端末においてマルウェア対策を実施している ・該当するものをすべて選択してください ■既知のマルウェア対策として、アンチウイルスソフトを導入し、リアルタイムスキャン、定期的なウイルススキャンやパターンファイルの更新化を行っている ■未知のマルウェア対策として、EDR製品や振る舞い検知を行う製品を導入している ■その他(詳細) メール経由でのマルウェア感染への対策を実施している ・該当するものをすべて選択してください ■メールフィルタリング機能（不正サイトへのリンクの検出、隔離、ブロック等） ■添付ファイルに対するスキャン機能 ■その他(詳細) 該当なし 非公開	端末においてマルウェア対策を実施している ・該当するものをすべて選択してください ■既知のマルウェア対策として、アンチウイルスソフトを導入し、リアルタイムスキャン、定期的なウイルススキャンやパターンファイルの更新化を行っている ■未知のマルウェア対策として、EDR製品や振る舞い検知を行う製品を導入している ■その他(詳細) メール経由でのマルウェア感染への対策を実施している ・該当するものをすべて選択してください ■メールフィルタリング機能（不正サイトへのリンクの検出、隔離、ブロック等） ■添付ファイルに対するスキャン機能 ■その他(詳細) 該当なし 非公開	
25	OA	変更	OA-2	端末におけるソフトウェアの制御・モニタリングについて、実施している対策をすべて選択してください。	端末における導入ソフトウェアの技術的な制御を実施している ・該当するものをすべて選択してください ■ソフトウェアのインストール制御 ■セキュリティ関連設定の変更制御 ■その他(詳細) 端末における導入ソフトウェアのモニタリングを実施している ■その他(詳細) 該当なし 非公開		OA-2	回答事業者の端末におけるOS/ソフトウェアの複製、制御・モニタリングについて、実施している対策をすべて選択してください。 端末のOS及びソフトウェアについて、利用許可ソフトウェアや安全な標準構成・設定ルールを定め、構成・設定している（ソフトウェアインストールは強制） ■端末のOS及び導入ソフトウェアの技術的な制御を実施している ・該当するものをすべて選択してください ■ソフトウェアのインストール制御 ■セキュリティ関連設定の変更制御 ■その他(詳細) ■端末のソフトウェアのモニタリングを実施している ・頻度 ●月に1回以上 ●半年に1回以上 ●1年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 ■その他(詳細) ■未実施 非公開	端末のOS及びソフトウェアについて、利用許可ソフトウェアや安全な標準構成・設定ルールを定め、構成・設定している（ソフトウェアインストールは強制） ■端末のOS及び導入ソフトウェアの技術的な制御を実施している ・該当するものをすべて選択してください ■ソフトウェアのインストール制御 ■セキュリティ関連設定の変更制御 ■その他(詳細) ■端末のソフトウェアのモニタリングを実施している ・頻度 ●月に1回以上 ●半年に1回以上 ●1年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 ■その他(詳細) ■未実施 非公開	
26	OA	変更	OA-3	端末における脆弱性管理について、実施している対策をすべて選択してください。	■端末の脆弱性管理およびセキュリティパッチ適用に関するルールを定めている ■端末におけるセキュリティパッチ適用の状況を把握している ■端末に対するセキュリティパッチは自動的に適用されている(適用タイミング) ■その他(詳細) 該当なし 非公開		OA-3	回答事業者の端末における脆弱性管理について、実施している対策をすべて選択してください。 ■端末の脆弱性管理およびセキュリティパッチ適用に関するルールを定めている ■端末におけるセキュリティパッチ適用の状況を定期的に把握している ・頻度 ●月に1回以上 ●半年に1回以上 ●1年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 ■端末に対するセキュリティパッチは自動的に適用されている(適用タイミング) ■その他(詳細) ■未実施 非公開	■端末の脆弱性管理およびセキュリティパッチ適用に関するルールを定めている ■端末におけるセキュリティパッチ適用の状況を定期的に把握している ・頻度 ●月に1回以上 ●半年に1回以上 ●1年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 ■端末に対するセキュリティパッチは自動的に適用されている(適用タイミング) ■その他(詳細) ■未実施 非公開	
27	OA	変更	OA-4	端末における紛失・盗難時の対策について、該当する選択例をすべて選択してください。	■端末の紛失・盗難対策を実施している ・該当するものをすべて選択してください ■端末の記憶装置（HDDやSSD等）の暗号化 ■リモートロック ■リモートワイプ ■その他(詳細) ■端末にデータが保存されない方式（シンククライアントPC、データレスPC等）としている(詳細) 該当なし 非公開		OA-4	回答事業者の端末における紛失・盗難時の対策について、該当する選択例をすべて選択してください。 ■端末の紛失・盗難対策を実施している ・該当するものをすべて選択してください ■端末の記憶装置（HDDやSSD等）の暗号化 ■リモートロック ■リモートワイプ ■その他(詳細) ■端末にデータが保存されない方式（シンククライアントPC、データレスPC等）としている(詳細) ■未実施 非公開	■端末の紛失・盗難対策を実施している ・該当するものをすべて選択してください ■端末の記憶装置（HDDやSSD等）の暗号化 ■リモートロック ■リモートワイプ ■その他(詳細) ■端末にデータが保存されない方式（シンククライアントPC、データレスPC等）としている(詳細) ■未実施 非公開	
28	OA	新規	-	-	-		OA-5	回答事業者の端末へのログイン認証について、回答事業者が実施している対策をすべて選択してください。 ・最小の文字数 ・（使用している認証手段）該当するものをすべて選択してください ■生体認証技術、顔認証等を利用している ■セキュリティキーやスマートカード等の物理デバイスを採用している ●追加の認証手段は使用していない ■端末のログイン認証に、アカウントロック制(試行回数の制限、一定回数失敗時のロック等)を設定している ■未実施 非公開	・最小の文字数 ・（使用している認証手段）該当するものをすべて選択してください ■生体認証技術、顔認証等を利用している ■セキュリティキーやスマートカード等の物理デバイスを採用している ●追加の認証手段は使用していない ■端末のログイン認証に、アカウントロック制(試行回数の制限、一定回数失敗時のロック等)を設定している ■未実施 非公開	
29	OA	変更	OA-5	社内LAN（有線・無線）への接続制限について、実施している対策をすべて選択してください。	社内LAN（有線・無線）へ接続可能な端末を技術的に制限している ・該当するものをすべて選択してください ■MACアドレスフィルタリング ■IPアドレス認証 ■証明書認証 ■その他(詳細) ■安全な暗号方式により無線LANを暗号化している [補足] 安全でない暗号方式としてはWPAやWEPが挙げられます ■その他(詳細) 該当なし 非公開		OA-6	回答事業者のオフィス等に設置された社内LAN（有線・無線）への接続制限について、実施している対策をすべて選択してください。 社内LAN（有線・無線）へ接続可能な端末を技術的に制限している ・該当するものをすべて選択してください ■MACアドレスフィルタリング ■IPアドレス認証 ■証明書認証 ■その他(詳細) ■安全な暗号方式により無線LANを暗号化している [補足] 安全でない暗号方式としてはWPAやWEPが挙げられます ■その他(詳細) ■対応となる社内LANがない(詳細) [回答補足]フルリモートで業務を行う場合等、自社オフィスで作業を実施しない場合等に選択してください ■未実施 非公開	社内LAN（有線・無線）へ接続可能な端末を技術的に制限している ・該当するものをすべて選択してください ■MACアドレスフィルタリング ■IPアドレス認証 ■証明書認証 ■その他(詳細) ■安全な暗号方式により無線LANを暗号化している [補足] 安全でない暗号方式としてはWPAやWEPが挙げられます ■その他(詳細) ■対応となる社内LANがない(詳細) [回答補足]フルリモートで業務を行う場合等、自社オフィスで作業を実施しない場合等に選択してください ■未実施 非公開	
30	OA	変更	OA-6	私用端末（PC、スマートフォン等）を業務利用していますか。	はい いいえ 非公開	・ [はい] が選択： OA-7	OA-7	回答事業者の従業員等が所有する私用端末（PC、スマートフォン等）を業務利用していますか。 はい いいえ 非公開	・ [はい] が選択： OA-8	
31	OA	変更	OA-7	私用端末（PC、スマートフォン等）のセキュリティ対策について、実施している対策をすべて選択してください。 ※業務情報…調査対象の業務において、個人情報を含む取引元から提供された情報や当該業務において作成する情報	私用端末上に企業領域を設定し、企業領域外への業務情報の持ち出しを制限している 私用端末上に業務情報を保存していない ■その他(詳細) 該当なし 非公開		OA-8	回答事業者の従業員等が所有する私用端末（PC、スマートフォン等）に対して、実施しているセキュリティ対策をすべて選択してください。 ※ 業務情報… 調査対象の業務において、個人情報を含む取引元から提供または提供された情報や当該業務において作成する情報 私用端末上に企業領域を設定し、企業領域外への業務情報の持ち出しを制限している 私用端末上に業務情報を保存していない ■その他(詳細) ■未実施 非公開		

	カテゴリ	新設/変更/廃止	旧項目	旧設内容	旧分岐先	旧分岐先	新項目	新設内容	新選択肢	新分岐先
32	OA	変更	OA-8	端末経由の情報漏えい対策について、実施している対策をすべて選択してください。	☐ インターネット経由での情報漏えい対策を実施している ・該当するものをすべて選択してください ■意思のあるWebサイトへの接続制御 ■ファイルアップロードの制御 ■その他(詳細) ☐ メール経由での情報漏えい対策を実施している ・該当するものをすべて選択してください ■外部への添付ファイル付きメールの上長承認 ■外部への添付ファイル付きメールのモニタリング ■その他(詳細) ☐ プリンター経由での情報漏えい対策を実施している ・該当するものをすべて選択してください ■許可されたプリンターのみ印刷を制御 ■プリンター側でのユーザー認証 ■その他(詳細) ☐ 該当なし ☐ 非公開		OA-9	回答事業者の端末経由の情報漏えい対策について、実施している対策をすべて選択してください。 □インターネット経由での情報漏えい対策を実施している ・該当するものをすべて選択してください ■意思のあるWebサイトへの接続制御 ■ファイルアップロードの制御 ■その他(詳細) □メール経由での情報漏えい対策を実施している ・該当するものをすべて選択してください ■外部への添付ファイル付きメールの上長承認 ■外部への添付ファイル付きメールのモニタリング ■その他(詳細) □プリンター経由での情報漏えい対策を実施している ・該当するものをすべて選択してください ■許可されたプリンターのみ印刷を制御 ■プリンター側でのユーザー認証 ■その他(詳細) □外部との情報共有・情報送迎に関するルールを定め、役員及び従業員へ周知している ☐ 未実施 ☐ 非公開		
33	OA	変更	OA-9	リモートワークを実施していますか。	☐ はい ☐ いいえ ☐ 非公開	・ [はい] が選択： OA-10	OA-10	回答事業者はリモートワークを実施していますか。 □リモートワークに関するセキュリティルールの策定 □リモートワークに関するセキュリティルールの定期的に見直し ☐ 未実施 ☐ 非公開	☐ はい ☐ いいえ ☐ 非公開	・ [はい] が選択： OA-11
34	OA	変更	OA-10	リモートワークに関するセキュリティルールや目的について、該当する選択肢をすべて選択してください。	☐ リモートワークに関するセキュリティルールの策定 ☐ リモートワークに関するセキュリティルールの定期的に見直し ☐ 不特定多数の人がいる公共の場所でのリモートワークを禁止している ☐ 他者（家族、友人等）からののぞき見等を防止する施策を実施している ☐ 該当なし ☐ 非公開		OA-11	リモートワークに関するセキュリティルールの策定時や見直し時に、役員及び従業員へ周知している ・頻度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●年に1回より少ない（数年に1回など） ●不定期 ●非公開 □リモートワークに関するセキュリティルールの定期的に見直し時に、役員及び従業員へ周知している ☐ 未実施 ☐ 非公開		
35	AC	変更	AC-1	情報資産に対するアクセス制御の方針やルールについて、該当する選択肢をすべて選択してください。 ※ 情報資産…調査対象の業務において利用するシステムに関連するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等	☐ 情報資産に対するアクセス制御の方針やルールが定められている ・該当するものをすべて選択してください ■情報資産へのアクセス権限を必要最小限のユーザーのみに限定している ■許可されたアプリケーション/機能（アカウント、サーバ、データベース等）を分離している ■その他(詳細) ☐ 情報資産に対するアクセス制御の方針やルールを定期的に見直ししている ☐ 該当なし ☐ 非公開		AC-1	情報資産に対するアクセス制御やファイアウォールの管理に関する方針やルールについて、回答事業者が実施している対策をすべて選択してください。 ※ 情報資産…調査対象の業務において利用するシステムに関連するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等 □情報資産に対するアクセス制御の方針やルールが定められている ・該当するものをすべて選択してください ■情報資産へのアクセス権限を必要最小限のユーザーのみに限定している ■許可されたアプリケーション/機能（アカウント、サーバ、データベース等）を分離している ■その他(詳細) □情報資産に対するアクセス制御の方針やルールを定期的に見直ししている □ファイアウォールの設定・運用に関する社内ルールを定めている ・頻度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●年に1回より少ない（数年に1回など） ●不定期 ●非公開 ■ファイアウォールバーストの検出 ■検出されたルールバーストの検出 ■十分な強度の確保 ■パスワードの使い回しの禁止 ■パスワードの安全な保管/暗号化/保管、パスワード管理アプリの利用等 ■パスワードの変更が必要な場合(漏洩の疑い、疑い等)に、速やかに変更する手順を定めている ■その他(詳細) □パスワードの設定・運用に関するルールを定期的に見直ししている □パスワードの設定・運用に関するルールを定期的に見直し時に、役員及び従業員へ周知している ☐ 未実施 ☐ 非公開		
36	AC	変更	AC-2	業務で利用するアプリケーションのユーザーアカウントについて業務上の必要性を確認していますか。	☐ ユーザーアカウントを発行・付与する場合は、業務上の必要性を確認している ☐ アプリケーションの利用者が退職・異動となった場合、速やかにユーザーアカウントのアクセス権限の更新や削除を実施している ☐ 定期的にユーザーアカウントの権限を実施している ☐ 定期的に見直し ☐ 該当なし ☐ 非公開		AC-2	回答事業者のシステムにおけるアプリケーションのユーザーアカウントについて業務上の必要性を確認していますか。 □ユーザーアカウントを発行・付与する場合は、業務上の必要性を確認している □アプリケーションの利用者が退職・異動となった場合、速やかにユーザーアカウントのアクセス権限の更新や削除を実施している □定期的にユーザーアカウントとアクセス権限の更新や削除を実施している ☐ 未実施 ☐ 非公開		
37	AC	変更	AC-3	業務で利用するアプリケーションのアカウントについて共有されているものがありますか。	☐ 共有アカウントが存在する(詳細を記載してください) ☐ 個別ユーザー毎にアカウントが設定されている ☐ 非公開	・ [共有アカウントが存在する] が選択： AC-4	AC-3	回答事業者のシステムにおけるアプリケーションのアカウントについて共有されているものがありますか。 □共有アカウントが存在する(詳細を記載してください) □個別ユーザー毎にアカウントが設定されている ☐ 未実施 ☐ 非公開		
38	AC	変更	AC-4	業務で利用するアプリケーションの共有アカウントについて実施している対策をすべて選択してください。	☐ 共有するアカウントと利用可能なユーザーを特定している(詳細を記載してください) ☐ 事前に承認を得た場合のみ利用可能としている ☐ 利用後に認証情報を変更している ☐ 監視ログや利用ログ等で適切な利用が確認している ☐ その他(詳細) ☐ 該当なし ☐ 非公開		AC-4	回答事業者のシステムにおけるアプリケーションの共有アカウントについて実施している対策をすべて選択してください。 □共有するアカウントと利用可能なユーザーを特定している(詳細を記載してください) □事前に承認を得た場合のみ利用可能としている □利用後に認証情報を変更している □監視ログや利用ログ等で適切な利用が確認している ・頻度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●年に1回より少ない（数年に1回など） ●不定期 ●非公開 ☐ 未実施 ☐ 非公開		

No.	カテゴリ	新稿/変更/削除	旧・新稿	旧設想	旧選取様	旧分岐先	新稿	新設想	新選取様	新分岐先
46	AC	変更	AC-12	取引元から委譲された権限を使用したアカウントおよびアクセス権限の管理について、該当するものをすべて選択してください。	- アカウントの発行やアクセス権限の付与を行う場合は、業務上の必要性を確認している - システムの利用者が退職・異動となった場合、速やかにアカウントの削除またはアクセス権限の剥奪を実施している - 定期的にアカウントの権限を実施し、不要なアカウントやアクセス権限が残存していないことを確認している - 該当なし - 非公開		AC-12	取引元から委譲された権限を使用したアカウントおよびアクセス権限の管理について、 回答事業者が実施している対策 をすべて選択してください。 [補記] AC-10で取引元から委譲された権限と委譲または個人所有のアカウントを利用しているに該当するものも取引元のシステムと同等に管理していること。	- アカウントの発行やアクセス権限の付与を行う場合は、業務上の必要性を確認している - システムの利用者が退職・異動となった場合、速やかにアカウントの削除またはアクセス権限の剥奪を実施している - 定期的にアカウントの権限を実施し、不要なアカウントやアクセス権限が残存していないことを確認している - 程度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 - 未実施 - 非公開	
47	AC	変更	AC-13	回答事業者のID基盤におけるアカウント管理、および取引元システムへのアクセス権限管理について、該当するものをすべて選択してください。	- システムの利用者が退職となった場合、回答事業者のID基盤において、速やかにアカウントの削除または無効化を実施している - システムの利用者が退職・異動となった場合、取引元に対して速やかにアクセス権限の剥奪を依頼している - 該当なし - 非公開		AC-13	回答事業者のID基盤におけるアカウント管理、および取引元のシステムへのアクセス権限管理について、該当するものをすべて選択してください。 [補記] AC-10で回答事業者のID基盤と連携または個人所有のアカウントを利用しているに該当するものも取引元のシステムと同等に管理していること。	- システムの利用者が退職となった場合、回答事業者のID基盤において、速やかにアカウントの削除または無効化を実施している - システムの利用者が退職・異動となった場合、取引元に対して速やかにアクセス権限の剥奪を依頼している - 未実施 - 非公開	
48	AC	変更	AC-14	取引元が管理するシステムを利用する際のアカウントを管理していますか。	- はい（共有アカウントが存在する） - いいえ（共有アカウントは存在しない） - 非公開	・「はい（共有アカウントが存在する）」が選択：AC-15	AC-14	取引元のシステムを利用する際のアカウントを 回答事業者内で共有 していますか。	- はい（共有アカウントが存在する） - いいえ（共有アカウントは存在しない） - 非公開	・「はい（共有アカウントが存在する）」が選択：AC-15
49	AC	変更	AC-15	共有アカウントについて実施している対策をすべて選択してください。	- 共有するアカウントと利用可能なユーザーを特定している - 業務上の承認を得た場合のみ利用可能としている - 共有アカウントを貸出専用とし、退却の前後、認証情報（パスワード等）を変更している - 管理権限や利用ログ等で適切な利用を確認している - その他(詳細) - 該当なし - 非公開		AC-15	共有アカウントについて 回答事業者が共有する共有アカウント について、実施している対策をすべて選択してください。	- 共有するアカウントと利用可能なユーザーを特定している - 業務上の承認を得た場合のみ利用可能としている - 共有アカウントを貸出専用とし、退却の前後、認証情報（パスワード等）を変更している - 管理権限や利用ログ等で適切な利用を確認している - その他(詳細) - 未実施 - 非公開	
50	CR	変更	CR-1	データに関する暗号化について、実施していることをすべて選択してください。 ※ 情報資産… 調査対象の業務において、個人情報を含む取引元から提供または預託された情報や当該業務において作成する情報 [補記] 安全性が認められたプロトコルやアルゴリズムとは、C、RC4、RC5などで暗号化された暗号化方式を指します	- 安全性が認められたプロトコルやアルゴリズムを使用している暗号化することを定めている - 安全な暗号化方式と十分な鍵長により、業務情報が格納されたデータベースやファイルが暗号化されている - 安全な暗号化方式と十分な鍵長により、バックアップデータを暗号化している - 該当なし - 非公開		CR-1	回答事業者のシステムにおける保管するデータに関する暗号化について、実施していることをすべて選択してください。 ※ 情報資産… 調査対象の業務において、個人情報を含む取引元から提供または預託された情報や当該業務において作成する情報 [補記] 安全な暗号化アルゴリズムとは、日本のCRYPTRECや米国のFIPS、NISTで推奨されたアルゴリズムを指します。	- 暗号化の方針に関するセキュリティルールの策定を定めている - 該当するものをすべて選択してください - 安全な暗号化アルゴリズムを使用している暗号化することを定めている - 安全な暗号化アルゴリズムと十分な鍵長により、業務情報が格納されたデータベースやファイルが暗号化されている - 安全な暗号化アルゴリズムと十分な鍵長により、バックアップデータを暗号化している - 未実施 - 非公開	
51	PH	変更	PH-1	オフィスの物理セキュリティ対策について、該当する選択肢をすべて選択してください。 ※ 情報資産… 調査対象の業務において利用するシステムに連携するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等	- オフィスへの入館および情報資産が保管されている区画への入館は承認にもとづき許可され、ICカード認証や生体認証等の認証により制限している - 入退館ログや入退館ログを定期的に確認し、不正アクセスがないか確認している - 該当するものをすべて選択してください - 防犯設備（監視カメラ、物理的な侵入検知システム等）の導入 - 立会人を同行 - 持ち込み品および持ち出し品の制限 - その他(詳細) - ネットワーク機器、サーバ等の設置エリア・ラックが監視されている - 該当なし - 非公開		PH-1	回答事業者のオフィスにおける物理セキュリティ対策について、該当する選択肢をすべて選択してください。 ※ 情報資産… 調査対象の業務において利用するシステムに連携するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等	- 情報資産の重要度に基づいて、物理的セキュリティ対策の位置や強度を定めている - オフィスへの入館および情報資産が保管されている区画への入館は承認にもとづき許可され、ICカード認証や生体認証等の認証により制限している - 入退館ログや入退館ログを定期的に確認し、不正アクセスがないか確認している - 入退館や入退館ログの保管期間 ●1年以上 ●1ヶ月以上～1年未満 ●3ヶ月以上～6ヶ月未満 ●1ヶ月以上～3ヶ月未満 ●1ヶ月未満 ●非公開 - オフィスへの入館および情報資産が保管されている区画への入館権限について、定期的に権限を実施している - 程度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 - オフィス内の情報資産の重要性に応じて、入室制限に加えて追加の物理セキュリティ対策を定めている - 該当するものをすべて選択してください - 防犯設備（監視カメラ、物理的な侵入検知システム等）の導入 - 立会人を同行 - 持ち込み品および持ち出し品の制限 - その他(詳細) - 対象となるオフィスが存在しない(詳細) - 回答事項[フルリモートで業務を行う場合等、自社オフィスを持たない場合に選択してください] - 未実施 - 非公開	
52	PH	変更	PH-2	データセンターの利用形態について、該当するものをすべて選択してください。	- 自社データセンターや自社内のサーバールーム - IaaS/PaaS等 - 他社データセンター（ハウジングやホスティング） - データセンターを利用していない - 非公開	・「自社データセンターや自社内のサーバールーム」が選択：PH-3、PH-4 ・「IaaS/PaaS等」または「他社データセンター（ハウジングやホスティング）」もしくはいずれもが選択：PH-5	PH-2	回答事業者のシステムにおけるデータセンター等の利用形態について、該当するものをすべて選択してください。	- 回答事業者のデータセンター - 回答事業者のオフィス（他社内部のラック、サーバールーム等） - IaaS/PaaS等 - 回答事項[AWS、Azure、Google Cloud等のクラウド基盤上でシステムを構築・運用している場合に選択してください] - 他社データセンター（ハウジングやホスティング） - 上記のいずれにも該当しない - 回答事項[SaaS等の利用のみで、システム基盤の管理を一任しない場合に選択してください] - 未実施 - 非公開	「回答事業者のデータセンター」または「回答事業者のオフィス（他社内部のラック、サーバールーム等）」もしくはいずれもが選択：PH-3、PH-4 「IaaS/PaaS等」または「他社データセンター（ハウジングやホスティング）」もしくはいずれもが選択：PH-5
53	PH	変更	PH-3	システムが稼働しているデータセンターの耐震・耐火対策について、該当する選択肢をすべて選択してください。	- 電力設備と電力ケーブルを耐震および耐火から保護している - 主電源が失われた場合に備え非常用電源や無停電電源装置（UPS）を導入している - 免震や耐震等の地震対策を導入している - 洪水および火災検知のための装置や仕組みを導入している - 消防対策を導入している - 温度と湿度を保つための装置や仕組みを導入している - 防水措置や漏水防止対策を導入している - 代替業務サービスを確認している - 代替拠点を用意している - 上記の対策・設備について定期的に点検している - 該当なし - 非公開		PH-3	回答事業者のシステムが稼働している、回答事業者のデータセンターやオフィスの耐震・耐火対策について、該当する選択肢をすべて選択してください。	- 電力設備と電力ケーブルを耐震および耐火から保護している - 主電源が失われた場合に備え非常用電源や無停電電源装置（UPS）を導入している - 免震や耐震等の地震対策を導入している - 洪水および火災検知のための装置や仕組みを導入している - 消防対策を導入している - 温度と湿度を保つための装置や仕組みを導入している - 防水措置や漏水防止対策を導入している - 代替業務サービスを確認している - 代替拠点を用意している - 上記の対策・設備について定期的に点検している - 未実施 - 非公開	
54	PH	変更	PH-4	システムが稼働しているデータセンターにおける物理セキュリティ対策について、該当する選択肢をすべて選択してください。 ※ 情報資産… 調査対象の業務において利用するシステムに連携するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等	- 情報資産の重要度に基づいて、物理的セキュリティ対策の位置や強度を定めている - オフィスへの入館および情報資産が保管されている区画への入館は承認にもとづき許可され、ICカード認証や生体認証等の認証により制限している - 入退館ログや入退館ログを定期的に確認し、不正アクセスがないか確認している - データセンター内の情報資産の重要性に応じて、入室制限に加えて追加の物理セキュリティ対策を定めている - 該当するものをすべて選択してください - 防犯設備（監視カメラ、物理的な侵入検知システム等）の導入 - 立会人を同行 - 持ち込み品および持ち出し品の制限 - その他(詳細) - 該当なし - 非公開		PH-4	回答事業者のシステムが稼働している、回答事業者のデータセンターやオフィスにおける物理セキュリティ対策について、該当する選択肢をすべて選択してください。 ※ 情報資産… 調査対象の業務において利用するシステムに連携するアプリケーションやOS、ミドルウェア、ハードウェア、ネットワーク、データ、外部サービス等	- 情報資産の重要度に基づいて、物理的セキュリティ対策の位置や強度を定めている - オフィスへの入館および情報資産が保管されている区画への入館は承認にもとづき許可され、ICカード認証や生体認証等の認証により制限している - 入退館ログや入退館ログを定期的に確認し、不正アクセスがないか確認している - 入退館や入退館ログの保管期間 ●1年以上 ●1ヶ月以上～1年未満 ●3ヶ月以上～6ヶ月未満 ●1ヶ月以上～3ヶ月未満 ●1ヶ月未満 ●非公開 - 建物への入館および情報資産が保管されている区画への入館権限について、定期的に権限を実施している - 程度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 - 情報資産の重要性に応じて、入室制限に加えて追加の物理セキュリティ対策を定めている - 該当するものをすべて選択してください - 防犯設備（監視カメラ、物理的な侵入検知システム等）の導入 - 立会人を同行 - 持ち込み品および持ち出し品の制限 - その他(詳細) - 建物への入館および情報資産が保管されている区画への入館権限について、定期的に権限を実施している - ネットワーク機器、サーバ等の設置エリア・ラックが監視されている - ネットワーク機器、サーバ等の設置エリア・ラックの点検について、管理者を定めたうえで安全に管理している - 未実施 - 非公開	
55	PH	変更	PH-5	利用しているIaaS/PaaS等、そのほか自社以外のデータセンターの選定にあたり、データセンターの入居室管理や自然災害への対策等の物理的なセキュリティ対策を確認していますか。	- はい - いいえ - 非公開		PH-5	回答事業者のシステムにおいて、IaaS/PaaSや他社データセンター等を利用するにあたり、データセンターの入居室管理や自然災害への対策等の物理的なセキュリティ対策を確認していますか。	- はい - いいえ - 非公開	

No.	カテゴリ	新稿/変更/削除	旧項目	旧設問	旧選択肢	旧分岐先	新項目	新設問	新選択肢	新分岐先
56	OP	変更	OP-1	システムの保守、運用において、実施している対策をすべて選択してください。	運用手続について、マニュアルや運用手順書のような形式で文書化している ☐マニュアルや運用手順書について定期的に見直ししている ☐保守、運用作業時の安全性を確保する対策を実施している ・該当するものをすべて選択してください ■複数人での作業体制 ■作業計画および作業結果のチェック・承認 ■その他(詳細) ☐その他(詳細) ☐該当なし ☐非公開		OP-1	旧稿:事業者のシステムの保守、運用において、実施している対策をすべて選択してください。 ☐運用手続について、マニュアルや運用手順書のような形式で文書化している ☐マニュアルや運用手順書について定期的に見直ししている ☐保守、運用作業時の安全性を確保する対策を実施している ・該当するものをすべて選択してください ■複数人での作業体制 ■作業計画および作業結果のチェック・承認 ■その他(詳細) ☐その他(詳細) ☐未実施 ☐非公開		
57	OP	変更	OP-2	バックアップやリストアテストについて、該当する選択肢をすべて選択してください。	☐バックアップを取得している ・世代 ●年度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない (数年に1回など) ●不定期 ●非公開 ☐バックアップデータの隔離と保護を実施している ・該当するものをすべて選択してください ■上書き禁止 ■遠隔地保管 ■その他(詳細) ☐リストアテストを定期的に実施している ・頻度 ●毎年実施年月 ☐該当なし ☐非公開		OP-2	旧稿:事業者のシステムにおけるバックアップやリストアテストについて、該当する選択肢をすべて選択してください。 ☐バックアップを取得している ・世代 ●年度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない (数年に1回など) ●不定期 ●非公開 ☐バックアップデータの隔離と保護を実施している ・該当するものをすべて選択してください ■上書き禁止 ■遠隔地保管 ■その他(詳細) ☐リストアテスト頻度を定期的に実施している ☐リストアテストを定期的に実施している ・頻度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない (数年に1回など) ●不定期 ●非公開 ●毎年実施年月 ☐未実施 ☐非公開		
58	OP	変更	OP-3	取得しているログについて、該当する選択肢をすべて選択してください。 ※セキュリティインシデント…セキュリティに関する事故や攻撃 (情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む)	※例外処理や誤操作によるエラー、システム障害、セキュリティインシデントに関するイベントログ ・該当するものをすべて選択してください ■アプリケーションのログ(保管期間) ■インフラ (ネットワークやIaaS環境等) のログ(保管期間) ■その他(詳細) ☐ユーザーアカウントの認証ログやアクセスログ、操作ログ(保管期間) ☐管理権アクセスログやアカウントの認証ログやアクセスログ、操作ログ(保管期間) ☐該当なし ☐非公開		OP-3	旧稿:事業者のシステムにおいて取得しているログについて、該当する選択肢をすべて選択してください。 ※例外処理や誤操作によるエラー、システム障害、セキュリティインシデントに関するイベントログ ・該当するものをすべて選択してください ■アプリケーションのログ ●1年以上 ●6ヶ月以上～1年未満 ●3ヶ月以上～6ヶ月未満 ●1ヶ月以上～3ヶ月未満 ●1ヶ月未満 ●非公開 ■インフラ (ネットワークやIaaS環境等) のログ ・保管期間 ●1年以上 ●6ヶ月以上～1年未満 ●3ヶ月以上～6ヶ月未満 ●1ヶ月以上～3ヶ月未満 ●1ヶ月未満 ●非公開 ■その他(詳細) ☐ユーザーアカウントの認証ログやアクセスログ、操作ログ ・保管期間 ●1年以上 ●6ヶ月以上～1年未満 ●3ヶ月以上～6ヶ月未満 ●1ヶ月以上～3ヶ月未満 ●1ヶ月未満 ●非公開 ☐管理権アクセスログやアカウントの認証ログやアクセスログ、操作ログ ・保管期間 ●1年以上 ●6ヶ月以上～1年未満 ●3ヶ月以上～6ヶ月未満 ●1ヶ月以上～3ヶ月未満 ●1ヶ月未満 ●非公開 ☐未実施 ☐非公開		
59	OP	変更	OP-4	脆弱性診断やペネトレーションテストについて、該当する選択肢をすべて選択してください。	☐プラットフォーム (OS、ミドルウェアやネットワーク) に対する脆弱性診断を実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ・最終実施年月 ☐設定診断 (セキュリティポスチャアセスメント) を実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ・最終実施年月 ☐アプリケーションに対して脆弱性診断を実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ・診断対象 ●Webアプリケーション全体 ●API、特定機能や画面等に限定 ☐システムに対して第三者によるペネトレーションテストを実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ・最終実施年月 ☐その他(詳細) ☐該当なし ☐非公開		OP-4	旧稿:事業者のシステムに対する脆弱性診断やペネトレーションテストについて、該当する選択肢をすべて選択してください。 ☐プラットフォーム (OS、ミドルウェアやネットワーク) に対する脆弱性診断を実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない (数年に1回など) ●不定期 ●非公開 ●毎年実施年月 ☐設定診断 (セキュリティポスチャアセスメント) を実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない (数年に1回など) ●不定期 ●非公開 ●毎年実施年月 ☐アプリケーションに対して脆弱性診断を実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない (数年に1回など) ●不定期 ●非公開 ●毎年実施年月 ・診断対象 ●Webアプリケーション全体 ●API、特定機能や画面等に限定 ☐システムに対して第三者によるペネトレーションテストを実施している ・実施状況 ●定期的に実施(頻度) ●不定期に実施 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない (数年に1回など) ●不定期 ●非公開 ●毎年実施年月 ☐その他(詳細) ☐未実施 ☐非公開		

No.	カテゴリ	新稿/変更/削除	旧稿番	旧設簡	旧設抜粋	旧設優先	新設簡	新設簡	新設抜粋	新設優先
71	SV	変更	SV1	システムの取得、開発および保守におけるルールやプロセスを定めているか。	□はい □いいえ □非公開		SV1	当該事業等のシステムの取得、開発および保守におけるルールやプロセスについて、実施していることをすべて選択してください。	□システムの取得、開発および保守におけるルールやプロセスを定めている □システムの取得、開発および保守におけるルールやプロセスを定期的に見直している □システムの取得、開発および保守におけるルールやプロセスの遵守状況について、定期的に確認を実施している ・程度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 ○未実施 ○非公開	
72	SV	変更	SV2	システムの取得、開発および保守において、実施していることをすべて選択してください。 ※ OSS… Open Source Software：オープンソースソフトウェア	□コーディング規約などを定め、セキュアコーディングを実施している □ソースコードのレビューをしている ・該当するものをすべて選択してください ■人による確認 ■SASTなどのツールを用いた自動検証 □システムで利用しているOSSを把握している □その他(詳細) □該当なし □非公開		SV2	当該事業等のシステムの取得、開発および保守において、実施していることをすべて選択してください。 ※ OSS… Open Source Software：オープンソースソフトウェア	□コーディング規約などを定め、セキュアコーディングを実施している □ソースコードのレビューをしている ・該当するものをすべて選択してください ■人による確認 ■SASTなどのツールを用いた自動検証 □システムで利用しているOSSを把握している □システムのOS及びソフトウェアについて、安全な標準構成・設定ルールを定め、構成・設定している（ソフトウェアフィアウォールの有効化等） □その他(詳細) □未実施 ○非公開	
73	BC	変更	BC-1	自然災害や大規模なシステム障害、セキュリティインシデントに備えてリバリ計画およびコンティンジェンシープランを策定しているか。	□リバリ計画およびコンティンジェンシープランを策定している □リバリ計画およびコンティンジェンシープランを定期的に見直し、更新している □リバリ計画およびコンティンジェンシープランの実現性を確認するための訓練を定期的に実施している ・該当するものをすべて選択してください ■実施訓練の実施 ■机上訓練の実施 ■情報セキュリティ管理の責任者の訓練への参加 □取引元からの要請があった場合、かつ、契約に該当する内容がある場合に）取引元の演習・訓練に参加している □該当なし □非公開		BC-1	当該事業等のシステムにおいて、自然災害や大規模なシステム障害、セキュリティインシデントに備えてリバリ計画およびコンティンジェンシープランを策定し、定期的な訓練または見直しで実施しているか。 ※ コンティンジェンシープラン… 緊急時対応計画 ※ セキュリティインシデント… セキュリティに関する事故や故障（情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む）	□リバリ計画およびコンティンジェンシープランを策定している □リバリ計画およびコンティンジェンシープランを定期的に見直し、更新している □リバリ計画およびコンティンジェンシープランの実現性を確認するための訓練を定期的に実施している ・該当するものをすべて選択してください ■実施訓練の実施 ■机上訓練の実施 ■情報セキュリティ管理の責任者の訓練への参加 □取引元からの要請があった場合、かつ、契約に該当する内容がある場合に）取引元の演習・訓練に参加している □未実施 ○非公開	
74	BC	変更	BC-2	自然災害や大規模なシステム障害、セキュリティインシデントに対応するため、冗長性を備えたシステム構成になっているか。	□同一地域に跨って冗長化されたシステム構成となっている（例：マルチリージョンや遠隔地のデータセンター利用） □同一地域内の複数拠点に跨って冗長化されたシステム構成となっている（例：マルチAZや近郊データセンターの利用） □同一拠点内で冗長化されたシステム構成となっている（例：シングルAZや同一データセンター内でのサーバ冗長化） □該当なし □非公開		BC-2	当該事業等のシステムは、自然災害や大規模なシステム障害、セキュリティインシデントに対応するため、冗長性を備えたシステム構成になっているか。 ※ セキュリティインシデント… セキュリティに関する事故や故障（情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む）	□同一地域に跨って冗長化されたシステム構成となっている（例：マルチリージョンや遠隔地のデータセンター利用） □同一地域内の複数拠点に跨って冗長化されたシステム構成となっている（例：マルチAZや近郊データセンターの利用） □同一拠点内で冗長化されたシステム構成となっている（例：シングルAZや同一データセンター内でのサーバ冗長化） □未実施 ○非公開	
75	OS	変更	OS-1	外部委託先や外部サービスの選定および管理について、方針や体制を整備しているか。	□外部委託先や外部サービスのセキュリティリスク管理に関する方針や規程を策定している □外部委託先や外部サービスを把握し、定期的に情報を更新する仕組みがある ・該当するものをすべて選択してください ■外部委託先や外部サービスのセキュリティリスク管理を行う体制が整備（管理部署の設置や、関係部署間の連携を含め各部署の役割及び責任の明確化）されている ■外部委託先や外部サービスを把握するための台帳等を作成し、管理対象を把握している ■その他(詳細) □外部委託先や外部サービスを把握するための台帳等や、定期的に棚卸している □外部委託先や外部サービスとセキュリティ対応に関する要求書を合意し、文書化している □該当なし □非公開		OS-1	当該事業等は外部委託先や外部サービスの選定および管理に、方針や体制を整備しているか。 ※ 外部委託… 顧客対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 顧客対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託	□外部委託先や外部サービスのセキュリティリスク管理に関する方針や規程を策定している ・該当するものをすべて選択してください ■外部委託先や外部サービスのセキュリティリスク管理を行う体制が整備（管理部署の設置や、関係部署間の連携を含め各部署の役割及び責任の明確化）されている ■外部委託先や外部サービスを把握するための台帳等を作成し、管理対象を把握している ■その他(詳細) □外部委託先や外部サービスを把握するための台帳等や、定期的に棚卸している ・程度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開	
76	OS	変更	OS-2	外部委託先や外部サービスに対する要求事項として合意事項をすべて選定してください。	□実施すべきセキュリティ対策や脆弱性診断 □セキュリティインシデント発生時の報告や対応 □セキュリティ教育や研修の実施 □関係法令の遵守 □監査等 □ポリシー違反、システム障害、作業ミス等を含む ※ 外部サービス… 顧客対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 顧客対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託		OS-2	外部委託先や外部サービスに対して、当該事業等が要求および希望している事項を、すべて選択してください。 ※ セキュリティインシデント… セキュリティに関する事故や故障（情報漏えいおよび内部不正、外部侵害、ポリシー違反、システム障害、作業ミス等を含む） ※ 外部サービス… 顧客対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 顧客対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託 [補足] 外部委託先や外部サービスがない場合は、ルールとして定められている項目を選択ください	□実施すべきセキュリティ対策や脆弱性診断 □セキュリティインシデント発生時の報告や対応 □セキュリティ教育や研修の実施 □関係法令の遵守 □監査等 □サービスレベル □機密情報の保護（秘密保持契約の締結、利用制限・保管・廃棄等の取扱いの取り決め等） □その他(詳細) □未実施 ○非公開	
77	OS	変更	OS-3	外部委託先や外部サービスとの合意内容が履行されているか確認していますか。	・該当するものをすべて選択してください ■契約事項について履行状況の報告を受けている(頻度) ■契約事項について履行状況の確認や監査を実施している(頻度) ■契約事項やサービス仕様が変更された場合に、自社への影響を確認している ■その他(詳細) □該当なし □非公開		OS-3	外部委託先や外部サービスとの合意内容が履行されているかを定期的に確認していますか。 ※ 外部サービス… 顧客対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 顧客対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託 [補足] 外部委託先や外部サービスがない場合は、ルールとして定められている項目を選択ください	□契約事項について履行状況の報告を受けている ・程度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 □契約事項やサービス仕様が変更された場合に、自社への影響を確認している □その他(詳細) □未実施 ○非公開	
78	OS	変更	OS-4	外部委託先や外部サービスに対してセキュリティリスク評価を実施していますか。	□取引開始前にリスク評価を実施している ・該当するものをすべて選択してください ■外部認証（ISO27001やSOCなど）の有無 ■セキュリティ水準（組織的な体制や技術的対策状況） ■取得済データのデータの取扱い ■インシデント対応計画、コンティンジェンシープラン ■過去のインシデントの発生・対応状況 ■その他(詳細) □定期的なリスク評価を実施している ・評価頻度 ・該当するものをすべて選択してください ■外部認証（ISO27001やSOCなど）の有無 ■セキュリティ水準（組織的な体制や技術的対策状況） ■取得済データのデータの取扱い ■インシデント対応計画、コンティンジェンシープラン ■過去のインシデントの発生・対応状況 ■その他(詳細) □該当なし □非公開		OS-4	当該事業等は外部委託先や外部サービスに対してセキュリティリスク評価を実施していますか。 ※ 外部サービス… 顧客対象業務を実施するうえで利用するクラウドサービス ※ 外部委託… 顧客対象業務におけるシステム開発や運用保守、データ加工、保管、カスタマーサポート、SES等の業務委託 [補足] 外部委託先や外部サービスがない場合は、ルールとして定められている項目を選択ください	□取引開始前にリスク評価を実施している ・程度 ●月に1回以上 ●半年に1回以上 ●年に1回以上 ●1年に1回より少ない（数年に1回など） ●不定期 ●非公開 ・該当するものをすべて選択してください ■外部認証（ISO27001やSOCなど）の有無 ■セキュリティ水準（組織的な体制や技術的対策状況） ■取得済データのデータの取扱い ■インシデント対応計画、コンティンジェンシープラン ■過去のインシデントの発生・対応状況 ■その他(詳細) □未実施 ○非公開	

No.	カテゴリ	新規/変更/廃止	旧項目	旧設例	旧設例先	旧項目先	新項目	新設例先	新項目先	
79	AI	新規	-	-	-	-	AI-1	調査対象業務の遂行、または成果物(業務の実施結果)の作成に当たり、調査対象業務におけるものの関与程度として該当するものをすべて選択してください。	・「他社が提供するAIを、調査対象業務において利用している」 [回答補足]:業務効率化、調査、分析、プログラムコード生成の補助等、他社が提供するサービス(生成AIサービス等)を、調査対象業務の作業プロセス内で利用する形態。 ・「他社が提供するAIを組み込んだ自社システムを、調査対象業務に利用している」 [回答補足]:他社が提供するAIを、API連携やAPI連携等により自社のサービス・システムに組み込む形態。取引元に提供する場合など、自社で保持して業務遂行に用いる場合の取扱いを含む。組み込んだAIシステム・サービスの安全性やガバナンスに責任を負う。 ・「調査事業者が自ら開発・学習に責任を持つAIモデル・システムを、調査対象業務に利用している」 [回答補足]:調査事業者が開発・学習するAIモデルやAIシステムそのものを、調査対象業務に用いる形態。AIモデル・システムそのものの開発・学習に責任を負う。 ・「調査対象業務においてAIを一切利用していない」 ○非公開	・「他社が提供するAIを、調査対象業務において利用している」or「他社が提供するAIを組み込んだ自社サービス(SaaS等)を、取引元に提供して調査対象業務を遂行している」or「調査事業者が自ら開発・学習に責任を持つAIモデル・システムを、調査対象業務に利用している」もしくは複数、全てが該当: AI-1
80	AI	新規	-	-	-	-	AI-2	調査対象業務におけるAI利用において、以下の対策を実施していますか。	「入力データがモデルの学習に利用されない設定(オプトアウト等)を適用している」 ○プライバシー保護機能や監視プログラムの導入、AIを含むAIシステムの利用を、組織として管理(許可・制限等)している ○AIへの入力(データやプロンプト等)に確認情報・個人情報が入り込むことを防止する対策を実施している ・「該当するものをすべて選択してください」 ■取引元の確認情報・個人情報が入り込む運用ルールを廃止している ■入力フィルタリングやマスキング等の技術的な保護策を実施している ■その他(確認情報保護に関する具体的な対策) ○AI出力結果の品質、権利侵害やバイアスの発生を監視する工程を設けている ・「該当するものをすべて選択してください」 ■人間が出力結果の妥当性や事実確認(ファクトチェック)を行っている ■第三者の著作権侵害や不正な複製・模倣(バイパス)が含まれない点を確認している ■その他(品質・権利点検に関する具体的な対策) ○その他 ○記録 ○未実施 ○非公開	・「他社が提供するAIを組み込んだ自社サービス(SaaS等)を、取引元に提供して調査対象業務を遂行している」or「調査事業者が自ら開発・学習に責任を持つAIモデル・システムを、調査対象業務に利用している」もしくは複数、全てが該当: AI-2
81	AI	新規	-	-	-	-	AI-3	AIを安全に運用するための管理体制について、以下の項目を評価・実施していますか。	「AI利用に関する社内規定(禁止事項、承認プロセス等)を文書化し、徹底している」 「指定したAI利用規定を最新の技術動向やリスクに基づき、定期的に見直ししている」 「AI利用に関する責任体制(責任者の任命や主要部署の設置等)を明確に定めている」 ・「備考」 ○承認済みAIツールのリスト化等、社内での利用実態を継続的に把握している ・「備考」 ○AI特有のリスクや社内規定に関する教育を定期的に実施している ・「該当するものをすべて選択してください」 ■退出力(ハルシネーション)に伴うセキュリティおよび法的リスクを把握している ■自社で利用可能なツール、禁止事項、および利用時の承認フローを教育している ■その他(教育に関する具体的な独自対策) ○AIに関連するトラブル発生時の報告・対応体制を整備している ・「該当するものをすべて選択してください」 ■自社内の連絡体制や報告フローを確立している ■取引元への連絡体制や報告基準を確立している ■情報の取扱いやAI利用範囲を行うための手順を策定している ■その他(トラブル対応に関する具体的な独自対策) ○AI利用による差の発生防止や原因究明のための体制を整備している ・「該当するものをすべて選択してください」 ■インシデント発生時の原因究明のため、AIの入出力ログ等を必要期間保存している ■その他(再発防止・検証に関する具体的な独自対策) ○取引元に対し、AIの安全対策の実施状況や利用モデル等を説明できる体制を整えている ○その他 ○未実施 ○非公開	・「他社が提供するAIを組み込んだ自社サービス(SaaS等)を、取引元に提供して調査対象業務を遂行している」or「調査事業者が自ら開発・学習に責任を持つAIモデル・システムを、調査対象業務に利用している」もしくは複数、全てが該当: AI-3
82	AI	新規	-	-	-	-	AI-4	AIシステムは開発や検証の学習等を行うに当たり、信頼性と安全性を確保するため、以下の対策を実施していますか。	「開発または検証するAIモデルおよびそのデータについて、安全性と正当性を確認・確保している」 ・「該当するものをすべて選択してください」 ■AI開発元の信頼性およびデータ取り扱い方針(学習利用の有無等)を確認している ■利用または学習に用いるデータの入手経路や権利関係(著作権等)の正当性を確認している ■学習データやAPI等を通じてデータに対するデータ汚染(ポイズニング)対策を実施している ■入出力における差やバイアス(バイパス)を監視する対策を実施している ■その他(モデル開発・学習に関する具体的な独自対策) ○AIシステム機能において、データ保護やアクセス制御を実装している ・「該当するものをすべて選択してください」 ■ユーザーの権限に応じたデータアクセス制御(認可制御)を実装している ■データから個人情報や機密情報を除去する技術的対策(マスキング等)を講じている ■その他(データ保護・アクセス制御に関する具体的な独自対策) ○システムの開発性対策および安全性テストを実施している ・「該当するものをすべて選択してください」 ■稼働前および定期的に、AI特有の不正入力(プロンプトインジェクション等)を想定した脆弱性テストを実施している ■入出力のリソース制限(トークン数等)を実装し、AI特有のサービス拒否(DoS)対策を講じている ■AIがプログラムコード等を出力する場合、悪意あるAIの悪意ある脆弱性・脆弱性の有無を確認している ■その他(脆弱性対策・安全性テストに関する具体的な独自対策) ○その他 ○未実施 ○非公開	・「他社が提供するAIを組み込んだ自社サービス(SaaS等)を、取引元に提供して調査対象業務を遂行している」or「調査事業者が自ら開発・学習に責任を持つAIモデル・システムを、調査対象業務に利用している」もしくは複数、全てが該当: AI-4