# 審査登録申込書(兼　見積作成依頼書) – 別紙

# 情報セキュリティマネジメントシステム審査登録用

# JIS Q 27001 :2023 (ISO/IEC 27001:2022)

|  |
| --- |
| 貴組織名： |
| Main (本社) 住所：  **サイトの人数:　　名**  ***※リスクの低い人数：上記人数の内、下記①-④に該当する人数：　　　名***  *①職務を遂行するために情報へ読み取り専用でアクセスできる人*  *②ISMSの適用範囲における組織の情報処理施設・設備へアクセスできない人*  *③ISMSの適用範囲における会社の情報処理施設・設備への明らかに特定のアクセスが制限されている人*  *④情報の開示を制限するために厳格な制限が実施されている場所で活動を行う人（例：作業領域へ私物や機器の持ち込み禁止する対策）*  *（サイト人数―①-④に該当する人数の平方根（整数以下切り上げ）＝****工数基準人数　　名）***  サイトの交代勤務回数：  常設サイト  一時的サイト  活動及びプロセス: ：  前回の内部監査の実施日:  結果（ISO/IEC 27001の順守に関する内部監査の結果を簡単に説明してください）：  サイトで前回情報セキュリティインシデントが発生した日 ：  インシデントの簡単な説明： |
| サイト1 住所：  ***サイトの人数:　　名***  ***※リスクの低い人数：上記人数の内、下記①-④に該当する人数：　　　名***  *①職務を遂行するために情報へ読み取り専用でアクセスできる人*  *②ISMSの適用範囲における組織の情報処理施設・設備へアクセスできない人*  *③ISMSの適用範囲における会社の情報処理施設・設備への明らかに特定のアクセスが制限されている人*  *④情報の開示を制限するために厳格な制限が実施されている場所で活動を行う人（例：作業領域へ私物や機器の持ち込み禁止する対策）*  *（サイト人数―①-④に該当する人数の平方根（整数以下切り上げ）＝****工数基準人数　　名）***  （サイト人数―①-④に該当する人数の平方根（整数以下切り上げ）＝**工数基準人数　　名）**  サイトの交代勤務回数：  常設サイト  一時的サイト  活動及びプロセス ：  前回の内部監査の実施日 ：  結果（JIS Q 27001（ISO/IEC 27001）の順守に関する内部監査の結果を簡単に説明してください）：  サイトで前回情報セキュリティインシデントが発生した日：    インシデントの簡単な説明： |
| サイト2 住所：  **サイトの人数:　　名**  ***※リスクの低い人数：上記人数の内、下記①-④に該当する人数：　　　名***  *①職務を遂行するために情報へ読み取り専用でアクセスできる人*  *②ISMSの適用範囲における組織の情報処理施設・設備へアクセスできない人*  *③ISMSの適用範囲における会社の情報処理施設・設備への明らかに特定のアクセスが制限されている人*  *④情報の開示を制限するために厳格な制限が実施されている場所で活動を行う人（例：作業領域へ私物や機器の持ち込み禁止する対策）*  *（サイト人数―①-④に該当する人数の平方根（整数以下切り上げ）＝****工数基準人数　　名）***  サイトの交代勤務回数：  常設サイト  一時的サイト  活動及びプロセス ：  前回の内部監査の実施日 ：  結果（JIS Q 27001（ISO/IEC 27001）の順守に関する内部監査の結果を簡単に説明してください）：  サイトで前回情報セキュリティインシデントが発生した日：    インシデントの簡単な説明： |
| サイト3 住所：  **サイトの人数:　　名**  ***※リスクの低い人数：上記人数の内、下記①-④に該当する人数：　　　名***  *①職務を遂行するために情報へ読み取り専用でアクセスできる人*  *②ISMSの適用範囲における組織の情報処理施設・設備へアクセスできない人*  *③ISMSの適用範囲における会社の情報処理施設・設備への明らかに特定のアクセスが制限されている人*  *④情報の開示を制限するために厳格な制限が実施されている場所で活動を行う人（例：作業領域へ私物や機器の持ち込み禁止する対策）*  *（サイト人数―①-④に該当する人数の平方根（整数以下切り上げ）＝****工数基準人数　　名）***  サイトの交代勤務回数：  常設サイト  一時的サイト  活動及びプロセス ：  前回の内部監査の実施日 ：  結果（JIS Q 27001（ISO/IEC 27001）の順守に関する内部監査の結果を簡単に説明してください）：  サイトで前回情報セキュリティインシデントが発生した日：    インシデントの簡単な説明： |
| ご連絡担当者名： |
| ご連絡電話番号 |

*注：従業員数とは、認証範囲内における組織の管理下で働く全ての勤務シフトの合計の人数です。（パートタイムの人は、常勤勤務者と比較した勤務時間数に比例した時間数で加算してください。）*

\*サイトが4ヶ所以上の場合はコピーしてご記入下さい。

|  |  |
| --- | --- |
| ＊上記の情報をもとに、弊社にてISMSを適切に審査できるかをレビューし、決定します。ISMSの審査を適切に行えないという結論に達した場合、貴社が適切なアクセスの手配をお取り頂くまで審査の開始ができません。（実施不可の基準：規格要求事項及び管理策の客観的証明が審査で確認できないと弊社にて判断した場合） | |
| **その他の事業所(サイト)が該当するものにチェックをして下さい：**  全てのサイトが同一のISMSに基づいて稼動している。ISMSは一元管理され審査を受け、中央(本社)のマネジメントレビューの対象である。  全てのサイトが貴組織のISMS内部監査プログラムに含まれている。  全てのサイトが貴組織のISMSマネジメントレビュープログラムに含まれている。 | |
| 該当する場合は、サイト間の差異についてご記入ください (例: ISMSの範囲内の事業プロセスの差異) |  |

|  |  |
| --- | --- |
| 該当する場合は、一時的サイトの期間、認証範囲の活動が実施される場所、活動、人数を記載してください。  また、不適合のリスクはありますか？ |  |

※訪問の基準：一時的サイトに起因する不適合によって情報セキュリティ目的を満たせなくなることのリスク評価を実施します。

|  |  |
| --- | --- |
| いくつかのサイトでは、複数の言語を使用する、又は、複数の言語での文書が提供されますか？  はい  いいえ  「はい」の場合、具体的にご記入ください | 適用される言語：  通訳の可否 |
| **貴社の事業と組織に関連する要因(情報テクノロジー以外)を特定するため、該当するものにチェックをして下さい。**  **事業の種類と規制要求事項：**  **注**: 重要な事業セクター とは、健康、安全、経済、イメージのリスクを生じる重要な公共サービスに影響を及ぼす分野、及び国家に多大な悪影響をもたらす可能性のある、政府が機能する能力を指します。  1. 当組織は非重要な事業セクターかつ非規制対象セクターにて業務を行っている。  .  2. 当組織には、重要な事業セクターの顧客が存在する。  3. 当組織は重要な事業セクターで業務を行っている。  **プロセスとタスク(事業及び組織の複雑さ【IT以外】に関連する要因の決定）:**  1. 標準的な反復タスクを行う標準プロセス。多数のスタッフが組織の管理下で、同じタスク、少数の製品またはサービスに関する作業を行う。  2. 標準的だが非反復的なプロセス。多数の製品またはサービス。  3. 複雑なプロセス。多数の製品及びサービス。多くの事業部門が審査登録範囲に含まれる。  **ISMS確立のレベル::**  1. ISMS がすでに確立されている、及び/または他のマネジメントシステムが整っている。  2. 他のマネジメントシステムの一部の要素は実施されているが、他は未実施である。  3. 他のマネジメントシステムは何も実施されておらず、ISMSも新規でまだ確立されていない。  **情報テクノロジー環境に関連する要因にチェックください(ITの複雑さに関する要因の決定):**  **IT 基盤と複雑さ:**  1. 少数または高度に標準化されたITプラットフォーム、サーバ、オペレーティングシステム、データベース、ネットワーク。  2. いくつかの異なるITプラットフォーム、サーバ、オペレーティングシステム、データベース、ネットワーク。  3. 多くの異なるITプラットフォーム、サーバ、オペレーティングシステム、データベース、ネットワーク。  **外注及び供給者への依存性。クラウドサービスを含む:**  1. 外注または供給者への依存はほとんどまたはまったくない。  .  2. 外注または供給者への依存は少しある。重要な事業活動の一部に関連するがすべてに関連はしていない。  3. 外注または供給者への依存が高い。重要な事業活動に大いに影響がある。  **情報システム開発:**  1. 社内システム/アプリケーション開発は未実施か、ごく一部。  2. 一部の重要な事業プロセスに対して、一部の社内または外注システム/アプリケーション開発。  3. 重要な事業プロセスに対して、広範囲に及ぶ社内または外注システム/アプリケーション開発。 | |

**複数サイトの登録をお申込みの場合にご記入ください。**

|  |  |
| --- | --- |
| 前回のマネジメントレビュー実施日 | マネジメントレビューではサイト毎の違いを確認しましたか。（例：リスクの大小、情報資産の大小など）  はい 　  いいえ  「はい」の場合、具体的にご記入ください |
| サイトによって作業慣行に違いはありますか。  はい  いいえ  「はい」の場合、具体的にご記入ください | サイトによって、設計や運用の管理に違いはありますか。  はい  いいえ  「はい」の場合、具体的にご記入ください |
| サイト間で重要な情報システムや機密情報を処理する情報システムのやりとり（情報交換）がありますか。  はい  いいえ  「はい」の場合、具体的にご記入ください | 適用される法的要求事項はすべてのサイトで同一ですか。  はい  いいえ  「いいえ」の場合、具体的にご記入ください |
| いくつかのサイトは、DRサイト（ディザスタリカバリサイト）（災害復旧、災害対策）の拠点ですか？（仮想サイトも含む）  はい  いいえ  「はい」の場合、具体的にご記入ください  サイト名：  ホットスタンバイ：本拠点のデータ複製などを常時行う方式（本拠点のミラーのような位置づけにする）  コールドスタンバイ：施設やインフラのみを用意しておく方式  ウォームスタンバイ：ホットスタンバイとコールドスタンバイの中間に位置するもので、システム構成は本拠点とほぼ同じ、非常時に稼働を開始する方式  ＊必要に応じて右の枠をご使用ください。 |  |

|  |  |
| --- | --- |
| **ISMS マルチサイトランク** | |
|  |
| **ランク** | **ランク基準** |  |
| **3** | サイトの活動には、次のような機密性の高い情報の管理が含まれる。   * 価格設定、マージン、知的財産[ソースコード/デザイン]、サプライヤーの身元/サプライヤー価格/部品番号/部品仕様などの機密性の高い内部情報。 * セキュリティの脆弱性、クライアントサイトの概略図（IPアドレスを使用したネットワークトポロジ（ネットワーク図）などの物理的または技術的）、リモートアクセス管理（認証によってクライアントサイトにリモートアクセスされたなど）などの機密性の高いクライアント情報 * 特別なカテゴリデータ（健康/医療記録など）、有罪判決、財務データ（資産/富、銀行口座情報）など、従業員、請負業者、クライアント、クライアントのエンドユーザー向けの機密性の高い個人情報 * セキュリティ/プライバシーリスク評価には、サイトで実施される活動に対する高い残存情報セキュリティまたはプライバシーリスクが含まれる。 |  |
| **2** | 機密性、完全性、または可用性の喪失が、クライアントまたはクライアントの顧客/エンドユーザー、従業員、請負業者などの他の利害関係者に大きな影響を与えない情報。  このサイトとその活動に関連する高い残存情報セキュリティまたはプライバシーリスクはない。 |  |
| **1** | これらのサイトで管理される情報は、機密性、整合性、または可用性が失われた場合の影響は少ないか、わずか。  このサイトとその活動に関連するすべての情報セキュリティとプライバシーの残存リスクは低く評価されている。 |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 上記のランク基準の表を参考に、各サイトのランクを以下に示してください。サイト数が足りない場合はコピーをしてご記入ください。 | | | | | | | | | | | |
| サイト | Main  (本社) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| ランク |  |  |  |  |  |  |  |  |  |  |  |

注意：見積もり後及び認証後の組織の変化における通知依頼

審査工数に影響を与える変化（新規の重大なリスクやインシデントなど）がある場合、組織の以下の変更においては、御社より変更通知を送付ください。規格要求事項を満たすマネジメントシステムの能力に影響を与える可能性のある事項の量と程度を考慮しレビューの結果、審査工数の見直しを行います。

a）法的、商業的、組織上の地位又は所有権

b）組織及び経営層（例えば、重要な管理層、意思決定または専門業務携わる要員）

c）連絡先及び事業所

d）認証されたマネジメントシステムに基づく活動の範囲

e）マネジメントシステム及びプロセスの重大な変更