日本化学キューエイ株式会社 行

e-mail： otoiawase\_mitsumori@jcqa.co.jp

依頼日　　　　　年　　　月　　　日

**ＩＳＭＳクラウドセキュリティ【ISO/IEC27017】**

**認証審査費用見積依頼書(1/3)**

|  |
| --- |
| **・ISO27001を取得済（もしくは同時取得予定）のお客様が対象となります**  ・**人数つき組織図**を添付してください  **ISMSｸﾗｳﾄﾞｾｷｭﾘﾃｨに関わっている部署名および人数を明記してください** |

＊ご記入いただきましたお客様の個人情報は、法令に基づいて見積もりに係る連絡・調整並びに弊社審査　　　　　　及び関連業務に利用させていただきます。

**１．**担当者（連絡窓口＝受信サイト（複数）の全貌が分かる方で、本受審の推進責任者）

事業所名

所属・職位

氏名

　　　　　　　　　　　電話　　　　　　　　　　　　　　　　 　　　ＦＡＸ

　　　　　　　　　　　Ｅ-mail

住所　〒

**２．**見積りご希望提出期限 　　　　　　月 　　　　　　日

※お見積もりに1週間程お時間をいただく場合がございます。

提出方法　　　郵送　　  Ｅ-mail

**３．**認証希望時期　　 　　　　　年 　　　　月頃　（  受審日 　 認証書取得）

**４．**適用範囲となる業務内容（ＩＳＯ27001の範囲内でご記入ください）

**５．**主な情報資産（ＩＳＯ27001と同一であれば、同じものをご記入ください）

（例）組織にとって価値のあるもの（情報ソフト、情報設備、ＰＣ、設備サーバ）

**６．**取り扱う情報資産　セキュリティの特徴（機密性・完全性・可用性）　　　　　　　　　　　　　　　　　　　　　　（ＩＳＯ27001と同一であれば、同じものをご記入ください）

**ＩＳＭＳｸﾗｳﾄﾞｾｷｭﾘﾃｨ認証審査費用見積依頼書(2/3)**

**７．**クラウドサーバが置いてある場所（次ページ3/3の※にご記入ください）

**８．**クラウドシステムの名称 （例：自社システム、MSAzure※1、ＡＷＳ※2、RCS※3等）

※1：マイクロソフトのクラウド(CLS) ※２：AmazonのCLS 　※３：ラクスのCLS

**９．**取得済み規格（最新版）

ISO27001　　　　　ISO9001　　　 　　ISO14001

ISO45001　　　　　ISO22000　　　　　その他（ 　　 　）

**１０．**コンサルタントと契約されていますか？

いいえ

はい　会社名：

契約期間：　　　年　　　月　　　日～　　　年　　　月　　　日

（**１１．**移管のお客様のみご記入ください）

現在の審査登録機関名

　　初回登録：　　　　　　年 　　　　　　月 　　　　　　日

　　有効期限：　　　　　　年 　　　　　　月 　　　　　　日

　　次回の審査：　維持審査（ｻｰﾍﾞｲﾗﾝｽ）/第　　　回目〔 　　　　年 　　　月　実施予定〕

更新審査/〔 　　　　年 　　　月　実施予定〕

**１２．**プロバイダーの場合（カスタマーの数をご記入ください）

**１３．**そ　の　他　（補足事項、ご質問等があればご記入ください）

**１４．**受審サイト（次ページ3/3にご記入ください）

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

　【ＪＣＱＡ使用欄】

担当欄

年　　月　　日

承認欄

年　　月　　日

・分類：

　・シフト　　　　　：  有　　 無

・一時的サイト ：  有　　 無

・人数つき組織図の入手 ：  済　 　 未了　（未了の場合は第1段階までに入手のこと）

→　 追加入手済み　（　　　　年　　月　　日）

　・適用範囲への商品名記載　：　 無

**ＩＳＭＳｸﾗｳﾄﾞｾｷｭﾘﾃｨ認証審査費用見積依頼書(3/3)**

**１４．**受審サイト

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **工場・事業所・支店・営業所など** | | | **人数（従事者）** | | |
| **従業員** | | **その他**（派遣・パート含） |
| 1 | 名称：    所在地：〒      最寄りの駅：　　　　　　　　　　　　　　　　　シフト勤務： あり 　 なし | |  | |  |
| 2 | 名称：    所在地：〒    最寄りの駅：　　　　　　　　　　　　　　　　　シフト勤務： あり 　 なし | |  | |  |
| 3 | 名称：    所在地：〒    最寄りの駅：　　　　　　　　　　　　　　　　　　シフト勤務： あり 　 なし | |  | |  |
| 4 | 名称：    所在地：〒    最寄りの駅：　　　　　　　　　　　　　　　　　　シフト勤務： あり 　 なし | |  | |  |
| 合計人数（人） | |  | |

※**７．**クラウドサーバの場所

|  |  |
| --- | --- |
|  | 名称：    所在地：〒    最寄りの駅： |

※欄が足りない場合はコピーしてお使いください。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 資産の機密性  の喪失時の影  響度合い | | | 低：顧客に対する影響が小 | |  | 5,000人未満の個人情報しか取り扱わず、不正競争防止法で言う営業機密に相当  する企業機密を保有していない組織。 |
| 中：顧客に対する影響が大 | |  | 個人情報取扱い事業者（5,000人以上の個人情報の取り扱い）、または不正競争  防止法で言う営業機密に相当する企業機密などを保有している組織。 |
| 高：社会に対する重大な影響 | |  | 国家機密,社会インフラ(電力,広域通信,金融など),医療に係る個人情報など情報漏洩の影響が社会的広がりを持つ資産,サービスを取り扱っている組織。 |
| 2 | 資産の完全  性、可用性の  喪失時の影響  度合い | | | 低：顧客に対する影響が小 | |  | サービスの停止が数日許容される。またサービスにより提供される情報が改竄されていても許容される。 |
| 中：顧客に対する影響が大 | |  | サービスの停止は１日以下が許容限度である。また、サービスにより提供される情報が不正確であると、利用者に金銭的不利益をもたらす。 |
| 高：社会に対する重大な影響 | |  | サービス停止は短時間でも許容されない。また サービスにより提供される情報が不正確であると生命への影響など金銭を超えた危険をもたらす。 |
| 3 | 業界特有の法  規制、情報セ  キュリティ要  求･標準の順  守の必要性 | | | 低：法令規制違反を犯すリスクは小 | | -- | 該当無し |
| 中：法令規制違反の影響は平均的 | |  | 個人情報保護法、不正競争防止法、知的財産権関連法規、刑法、民法等の法律、地方自治体の条例等がコンプライアンスの基準。罰金刑。世評の低下を招く。 |
| 高：法令規制違反の影響が大 | |  | 業界特有のコンプライアンスへの強い要求、違反した場合の制裁（法的、社会的）の影響が事業にとって致命的、訴訟になりえる。 |
| 4 | 情報セキュリティに対する内部統制の有効性 | | | 低：高度な内部統制を実施 | |  | レベルMの内容に加え、認証登録範囲で ISO9001 などのマネジメントシステムが運営されている。（リスク小） |
| 中：内部統制のレベルは平均的 | |  | 会社規則が整備されており、監査部など内部統制を実施する組織が明確になっている。（リスク中） |
| 高：内部統制が弱い | |  | 会社規則などが未整備であり、内部統制機能を担う組織も不明確である。（リスク大） |
| 5 | ＩＴ環境の業務  に対する影響  度合い（規模、  広域性） | | | 低：ＩＴ環境は小規模でリスクが小 | |  | 下記a、b、c、d、eがすべて「低」の場合。 |
| 中：IT環境は平均的 | |  | 下記a、b、c、d、eが「高」がなく、一つでも「中」がある場合。 |
| 高：IT環境が大規模、広域でリスクが大 | |  | 下記a、b、c、d、eで、一つでも「高」がある場合。 |
| a | ネットワークの規模 | | | 低 |  | 国内ネットワーク、少数拠点接続を組織で運営している。（小規模イントラネット） |
| 中 |  | 国内ネットワーク、多数拠点接続を組織で運営している。（平均的イントラネット） |
| 高 |  | 国内・海外含む大規模ネットワークを組織で運営している。（大規模イントラネット） |
| b | ＰＣ（ＷＳ）台数 | | | 低 |  | 半分程度の従業員しか利用していない。 |
| 中 |  | 一人1台利用している。 |
| 高 |  | 一人1台以上利用している。（OA用１台、開発用１台など） |
| c | モバイルＰＣ台数 | | | 低 |  | 利用していない。 |
| 中 |  | 従業員一人０．５台程度利用している。 |
|  | 従業員が１人１台のPCを利用している（リモートワークが中心で、そのセキュリティが整っている） |
| 高 |  | ほとんどの従業員が利用している。（リモートワークが中心であるが、そのセキュリティが整っていない） |
| d | サーバ台数  　　（クラウドサーバ含む） | | | 低 |  | サーバを利用していない。 |
| 中 |  | 従業員２０人に１台程度のサーバを運用している。 |
| 高 |  | 従業員一人当たり１台以上のサーバを運用している。例：データセンターなど。 |
| e | ＯＳの種類数 | | | 低 |  | 単一OSに統一している。 |
| 中 |  | 複数のOSを標準と定めて管理している。 |
| 高 |  | OSは必要に応じて決めており、どれだけの種類のOSがあるかは直ぐには分からない。 |
| ｆ |  | クラウドサービスプロバイダ | | |  | 他社に提供している　（何ユーザー位） |
|  | 社内にもユーザーがいる　（何ユーザー位） |
|  | クラウドサービスカスタマﾞ | | | | 外部のプロバイダを使用している |

機密保持契約を交わしても審査中に審査員が調査できない記録、文書等がありますか？

情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ/ＩＳＭＳｸﾗｳﾄﾞｾｷｭﾘﾃｨ認証の特性

別紙-1

（ はい、　いいえ）

グラフィカル ユーザー インターフェイス, アプリケーション

自動的に生成された説明

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 資産の機密性  の喪失時の影  響度合い | | | 低：顧客に対する影響が小 | | **〇** | 5,000人未満の個人情報しか取り扱わず、不正競争防止法で言う営業機密に相当  する企業機密を保有していない組織。 |
| 中：顧客に対する影響が大 | |  | 個人情報取扱い事業者（5,000人以上の個人情報の取り扱い）、または不正競争  防止法で言う営業機密に相当する企業機密などを保有している組織。 |
| 高：社会に対する重大な影響 | |  | 国家機密,社会インフラ(電力,広域通信,金融など),医療に係る個人情報など情報漏洩の影響が社会的広がりを持つ資産,サービスを取り扱っている組織。 |
| 2 | 資産の完全  性、可用性の  喪失時の影響  度合い | | | 低：顧客に対する影響が小 | | **〇** | サービスの停止が数日許容される。またサービスにより提供される情報が改竄されていても許容される。 |
| 中：顧客に対する影響が大 | |  | サービスの停止は１日以下が許容限度である。また、サービスにより提供される情報が不正確であると、利用者に金銭的不利益をもたらす。 |
| 高：社会に対する重大な影響 | |  | サービス停止は短時間でも許容されない。また サービスにより提供される情報が不正確であると生命への影響など金銭を超えた危険をもたらす。 |
| 3 | 業界特有の法  規制、情報セ  キュリティ要  求･標準の順  守の必要性 | | | 低：法令規制違反を犯すリスクは小 | | **--** | 該当無し |
| 中：法令規制違反の影響は平均的 | | **〇** | 個人情報保護法、不正競争防止法、知的財産権関連法規、刑法、民法等の法律、地方自治体の条例等がコンプライアンスの基準。罰金刑。世評の低下を招く。 |
| 高：法令規制違反の影響が大 | |  | 業界特有のコンプライアンスへの強い要求、違反した場合の制裁（法的、社会的）の影響が事業にとって致命的、訴訟になりえる。 |
| 4 | 情報セキュリティに対する内部統制の有効性 | | | 低：高度な内部統制を実施 | | **〇** | レベルMの内容に加え、認証登録範囲で ISO9001 などのマネジメントシステムが運営されている。（リスク小） |
| 中：内部統制のレベルは平均的 | |  | 会社規則が整備されており、監査部など内部統制を実施する組織が明確になっている。（リスク中） |
| 高：内部統制が弱い | |  | 会社規則などが未整備であり、内部統制機能を担う組織も不明確である。（リスク大） |
| 5 | ＩＴ環境の業務  に対する影響  度合い（規模、  広域性） | | | 低：ＩＴ環境は小規模でリスクが小 | |  | 下記a、b、c、d、eがすべて「低」の場合。 |
| 中：IT環境は平均的 | | **〇** | 下記a、b、c、d、eが「高」がなく、一つでも「中」がある場合。 |
| 高：IT環境が大規模、広域でリスクが大 | |  | 下記a、b、c、d、eで、一つでも「高」がある場合。 |
| a | ネットワークの規模 | | | 低 |  | 国内ネットワーク、少数拠点接続を組織で運営している。（小規模イントラネット） |
| 中 | **〇** | 国内ネットワーク、多数拠点接続を組織で運営している。（平均的イントラネット） |
| 高 |  | 国内・海外含む大規模ネットワークを組織で運営している。（大規模イントラネット） |
| b | ＰＣ（ＷＳ）台数 | | | 低 |  | 半分程度の従業員しか利用していない。 |
| 中 | **〇** | 一人1台利用している。 |
| 高 |  | 一人1台以上利用している。（OA用１台、開発用１台など） |
| c | モバイルＰＣ台数 | | | 低 |  | 利用していない。 |
| 中 |  | 従業員一人０．５台程度利用している。 |
| **〇** | 従業員が１人１台のPCを利用している（リモートワークが中心で、そのセキュリティが整っている） |
| 高 |  | ほとんどの従業員が利用している。（リモートワークが中心であるが、そのセキュリティが整っていない） |
| d | サーバ台数  　　（クラウドサーバ含む） | | | 低 |  | サーバを利用していない。 |
| 中 | **〇** | 従業員２０人に１台程度のサーバを運用している。 |
| 高 |  | 従業員一人当たり１台以上のサーバを運用している。例：データセンターなど。 |
| e | ＯＳの種類数 | | | 低 |  | 単一OSに統一している。 |
| 中 | **〇** | 複数のOSを標準と定めて管理している。 |
| 高 |  | OSは必要に応じて決めており、どれだけの種類のOSがあるかは直ぐには分からない。 |
| ｆ | **〇** | クラウドサービスプロバイダ | | | **10** | 他社に提供している　（何ユーザー位） |
| **10** | 社内にもユーザーがいる　（何ユーザー位） |
|  | クラウドサービスカスタマﾞ | | | | 外部のプロバイダを使用している |

機密保持契約を交わしても審査中に審査員が調査できない記録、文書等がありますか？

**記入例**

情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ/ＩＳＭＳｸﾗｳﾄﾞｾｷｭﾘﾃｨ認証の特性

情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ/ＩＳＭＳｸﾗｳﾄﾞｾｷｭﾘﾃｨ認証の特性

別紙-1

（ はい、　いいえ）