**【様式CS－7】**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20yy年mm月dd日  **監査報告書**  クラウド事業管掌役員殿    監査責任者  （氏名（署名または記名押印））  監査基本計画及び実施計画に基づき、表記監査を実施しましたので、以下のとおり報告します。  １．監査の概要  当監査は、貴事業部のクラウドコンピューティングサービスにおいて、下記記載の言明が信頼できることの確認を目的として、クラウドセキュリティ管理基準のガバナンス基準、マネジメント基準及び管理策基準の基本的事項とリスクに対応する項目への適合状況について検証を行っています。  (1) 言明　　　　　　　　20yy年mm月dd日付記載　CS言明書  (2) 監査基準日　　　　　20yy年mm月dd日を基準日とした時点  (3) 監査手続実施期間　　20yy年mm月dd日(○)～dd日(○)  (4) 監査手続実施担当者　○○　○○　(公認情報セキュリティ主任監査人、チームリーダ)  ○○　○○　(公認情報セキュリティ監査人、サブリーダ)  ○○　○○　(公認情報セキュリティ監査人)  ○○　○○　(情報セキュリティ監査人補)  　　　　　　　　　　 監査担当者はいずれもクラウド事業から独立した立場にいます。  (5)監査対象  ① クラウドコンピューティングサービス名称   |  | | --- | |  |   ②対象範囲   |  | | --- | |  |   ③対象リスク  H01　リソース・インフラの高集約によるインシデントの影響の拡大（例示）   |  | | --- | |  |   ２．監査結果  貴事業部のクラウドコンピューティングサービスの上記のCS言明書に記載のシステムの運用管理サービスに対する情報セキュリティのマネジメント及び管理策はクラウドキュリティ管理基準に適合して適正に整備・実装・運用されており、言明書に違反する指摘事項はありません。  ３．監査手続と判定結果  （１）　マネジメント基準   |  |  |  |  | | --- | --- | --- | --- | | マネジメント基準 | 個別基準 | 監査手続 | 判定 | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |   （２）　管理策基準   |  |  |  |  | | --- | --- | --- | --- | | 管理策  （小分類） | 個別管理基準 | 監査手続 | 判定 | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |   注１　個別管理基準における判定が有効でない場合はその理由及び影響度を記載してください。  さらに管理策レベルで判定が有効とした場合の理由も合わせて記載してください。  注2　3.監査手順と判定結果は別紙で添付することもできます。  　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　以上 |

記入例

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| マネジメント基準 | 個別基準 | | 監査手続 | 判定 |
| 4.9.1 リスクコミュニケーションの計画 | | |  |  |
|  | 通常運用時の計画と緊急時の計画に分かれているか | | 顧客対応規則、マニュアルを閲覧し、基準どおりであるかを確認する。  コミュニケーション記録を閲覧し、基準どおりに行われているかを確認する。  ヘルプデスク担当者に質問し、実際の緊急時の対応状況を聞き取る。  マネジメントレビューにおけるレビュー内容を確認し、基準どおりの運用がなされていたを確認する。  なお、以下の点が定義されていること。   1. 通常運用時と緊急時 2. 適切な利害関係者 3. 効果的な情報交換／共有 4. 対象法令（法律・規則） 5. 信頼を醸成するためのコミュニケーション 6. 危機又は不測の事態 |  |
|  | 通常運用時の計画では、以下の内容が行われているか | |  |
|  |  | 適切な利害関係者の参画による、効果的な情報交換／共有 |  |
|  |  | 法律、規制及びガバナンスの要求事項の順守 |  |
|  |  | コミュニケーション及び協議に関するフィードバック及び報告の提供 |  |
|  |  | 組織に対する信頼を醸成するためのコミュニケーションの活用 |  |
|  |  | 危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施 |  |
|  | 緊急時の計画では、以下の内容が行われているか | |  |
|  |  | 適切な利害関係者の参画による、効果的な情報交換／共有 |  |
|  |  | 法律、規制及びガバナンスの要求事項の順守 |  |
|  |  | コミュニケーション及び協議に関するフィードバック及び報告の提供 |  |
|  |  | 組織に対する信頼を醸成するためのコミュニケーションの活用 |  |
|  |  | 危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施 |  |