年　月　日

岐阜県知事　様

所在地

名称

代表者職氏名

情報セキュリティ体制報告書

　情報セキュリティに関する特記事項に基づき、次のとおり、情報セキュリティ体制を確保していることを確認しましたので報告します。

|  |  |  |  |
| --- | --- | --- | --- |
| **情報セキュリティ責任者名** | | ○○　○○ | |
| **個人情報取扱い責任者名** | | ××　×× | |
| **個人情報取扱い事務従事者名** | | ▲▲　▲▲ | |
| **対策項目** | | | **確認欄** |
| **１．メール誤送信システムの導入の有無について** | | | |
| メール送信時に宛先を秘匿する（Bcc強制変換機能）等といったメール誤送信を防止するためのシステムを導入している。 【導入しているシステムの概要を記載（又は概要資料を添付）】 | | | □ |
| **２．情報セキュリティマネジメントシステムについて** | | | |
| ISMS(Information Security Management System)適合性評価制度による認証を取得している。  【ISMS認証を取得していることが分かる資料を添付】 | | | □ |
| **※ISMS認証を取得している場合は以下３及び４の確認は不要** | | | |
| **３．システム的対策** | | | |
| (１)　リスク低減のための措置 | | | |
|  | ①パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化している。 | | □ |
| ② IoT 機器を含む情報資産の保有状況を把握している。 | | □ |
| ③ セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用している。 | | □ |
| (２)　インシデントの早期検知のための取り組み  ※委託業務内容にシステム構築等の業務が含まれない場合は回答しなくともよい | | | |
|  | ① サーバ等における各種ログを確認している。 | | □ |
| ② 通信の監視・分析やアクセスコントロールを点検している。 | | □ |
| (３)　インシデント発生時の適切な対処・回復 | | | |
|  | データ消失等に備えて、データのバックアップの実施及び復旧手順を確認している。 【バックアップ内容や復旧手順等について概要を記載（又は概要資料を添付）】 | | □ |
| **４．人的対策** | | | |
| (１)　組織における対策 | | | |
|  | ① セキュリティ事故発生時に備えて、対外応答や社内連絡体制等を準備し、事故を認知した際の対処手順を確認している。 【事故発生時の報告体制及び対処手順等の概要を記載（又は概要資料を添付）】 | | □ |
|  | ②定期的に情報セキュリティに関する研修を行っている。 【研修計画について概要を記載（又は概要資料を添付）】 | | □ |
| ③不審なメールを受信した際には、情報セキュリティ担当者等に迅速に連絡・相談する体制としている。  【連絡・相談体制について概要を記載（又は概要資料を添付）】 | | □ |
| (２)　各個人における対策 | | | |
|  | 文書・メールの送受信時に注意すべき事項について、パソコン・作業場所の近くに貼付する又は定期的に周知する等により注意喚起している。  【実際の注意喚起内容の概要を記載（又は通知、掲示資料等を添付）】 | | □ |

※未実施の項目がある場合は、その代替手段及び今後の対応方針について報告すること

※本報告書は委託事業者の情報セキュリティ対策状況を確認するものであり、本報告書の対策項目について未実施のものがあることだけを以て契約違反となるものではない