|  |
| --- |
| **情報セキュリティ対策に関する書類** |
| **次の１～２について回答してください。**  **１　業務形態別に必須とする情報セキュリティ対策を、次のとおり定めました｡**  **次の（１）～（４）のうち該当する業務形態に応じ、実施する対策について□を■にしてください。**  （１）個人情報等の重要な情報を取り扱うパソコンをインターネットに接続して使用する形態  　□従事者に対して情報セキュリティ教育を実施する  　□情報セキュリティインシデントが発生した際の体制を整える  　□ＩＤ及びパスワードが第三者に流失しないよう管理する  　□アクセスする権限のない従事者がアクセスできないよう制限する  　□パソコンに不正プログラム対策ソフトを常駐させる  　□ネットワークを通した外部からの攻撃に備える対策を実施する  （２）個人情報等の重要な情報を取り扱うパソコンをインターネットに接続しないで使用する形態  　□従事者に対して情報セキュリティ教育を実施する  　□情報セキュリティインシデントが発生した際の体制を整える  　□ＩＤ及びパスワードが第三者に流失しないよう管理する  　□アクセスする権限のない従事者がアクセスできないよう制限する  　□パソコンに不正プログラム対策ソフトを常駐させる  （３）個人情報等の重要な情報を取り扱わずパソコンを使用する形態  　□従事者に対して情報セキュリティ教育を実施する  □情報セキュリティインシデントが発生した際の体制を整える  　□ＩＤ及びパスワードが第三者に流失しないよう管理する  　□アクセスする権限のない従事者がアクセスできないよう制限する  （４）個人情報等の重要な情報を取り扱うがパソコンを使用しない形態  　□従事者に対して情報セキュリティ教育を実施する  　□情報セキュリティインシデントが発生した際の体制を整える  ※重要な情報とは、当該情報が漏えいした際に、業務に影響を及ぼすおそれがあるものを指します。  **２　次の認証について、取得している場合は□を■にしてください。**  　□ISO/IEC 27001（JIS Q 27001）  　□プライバシーマーク |
| **情報セキュリティ**  記載例 |
| **次の１～２について回答してください。**  **１　業務形態別に必須とする情報セキュリティ対策を、次のとおり定めました｡**  **次の（１）～（４）のうち該当する業務形態に応じ、実施する対策について□を■にしてください。**  （１）個人情報等の重要情報を取り扱うパソコンをインターネットに接続する形態  　■従事者に対して情報セキュリティ教育を実施する  　■情報セキュリティインシデントが発生した際の体制を整える  　■ＩＤ及びパスワードが第三者に流失しないよう管理する  　■アクセスする権限のない従事者がアクセスできないよう制限する  　■パソコンに不正プログラム対策ソフトを常駐させる  　■ネットワークを通した外部からの攻撃に備える対策を実施する  （２）個人情報等の重要情報を取り扱うパソコンをインターネットに接続しないで使用する形態  　□従事者に対して情報セキュリティ教育を実施する  　□情報セキュリティインシデントが発生した際の体制を整える  　□ＩＤ及びパスワードが第三者に流失しないよう管理する  　□アクセスする権限のない従事者がアクセスできないよう制限する  　□パソコンに不正プログラム対策ソフトを常駐させる  （３）個人情報等の重要情報を取り扱わないでパソコンを使用する形態  　□従事者に対して情報セキュリティ教育を実施する  □情報セキュリティインシデントが発生した際の体制を整える  　□ＩＤ及びパスワードが第三者に流失しないよう管理する  　□アクセスする権限のない従事者がアクセスできないよう制限する  （４）パソコンを利用しない形態  　□従事者に対して情報セキュリティ教育を実施する  　□情報セキュリティインシデントが発生した際の体制を整える  ※重要な情報とは、当該情報が漏えいした際に、業務に影響を及ぼすおそれがあるものを指します。  **２　次の認証について、取得している場合は□を■にしてください。**  　■ISO/IEC 27001（JIS Q 27001）  　■プライバシーマーク |