

情報セキュリティ対策

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口を■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口を■にしてください。

- ☐ ISO/IEC 27001（JIS Q 27001）
- ☐ プライバシーマーク

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口を■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口を■にしてください。

- ISO/IEC 27001 (JIS Q 27001)
- プライバシーマーク