

青森県情報セキュリティ対策基準

本書は、青森県情報セキュリティ基本方針に則り、受注者が順守すべき情報セキュリティ要件を示したものである。

1. 情報資産の分類と管理

- ・ 受注者は、県の情報資産を業務以外の目的に利用してはならない。
- ・ 受注者は、県の情報資産を適切に保管しなければならない。
- ・ 電子メール等により県の情報を送信する場合、必要に応じ暗号化又はパスワード設定を行わなければならない。
- ・ 車両等により県の情報資産を運搬する場合、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等の措置を講じなければならない。
- ・ 本業務を実施するために県庁舎外へ持ち出しを行う必要のある情報資産については、受注者は、事前に県にその持出理由、場所、種類、形式、媒体、期間を記載した申請書（様式任意）を提出の上、持ち出しの許可を得ること。
- ・ 受注者は、委託業務終了時に情報資産の返還、廃棄等を確実に行うこと。

2. 物理的セキュリティ

- ・ 受注者は、県の情報資産を取り扱う場所、パソコン等について、盗難防止のため物理的措置を講じなければならない。
- ・ 受注者は、情報システム（パソコン等を含む）へのログインパスワードの入力を必要とするように設定しなければならない。

3. 人的セキュリティ

- ・ 受注者は、本業務に携わる者に情報セキュリティに関する研修を実施しなければならない。
- ・ 研修の内容は、本書を含む県の情報資産の取扱に関するものを含めなければならない。
- ・ 自己が利用しているIDは、他人に利用させてはならない。
- ・ パスワードは、他者に知られないように管理しなければならない。
- ・ パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

4. 技術的セキュリティ

- ・ 受注者は、アクセスする権限のない者がアクセスできないように、システム上制限しなければならない。
- ・ 受注者は、利用者の登録、変更、抹消等を行い、適切にアクセス権を管理しなければならない。
- ・ 受注者は、県の情報資産を取り扱うパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させ、常に最新の状態に保たなければならない。
- ・ 受注者は、県の情報資産を取り扱うソフトウェアにおいて、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

5. 運用

- ・ 受注者は、情報セキュリティに関するインシデントを認知した場合、速やかに県に報告しなければならない。（コンピュータウイルス等に感染、検知した場合も含む）

6. 情報セキュリティ監査および自己点検の実施

- ・ 受注者は、情報セキュリティ対策状況に問題がないか、定期的に確認しなければならない。
- ・ 受注者は、県から情報セキュリティ対策状況の報告を求められた場合に、確認結果を提出しなければならない。
- ・ 受注者は、県が要請する場合は情報セキュリティ監査を受け入れなければならない。