

II 情報セキュリティ対策について

教職員は、重要な情報を漏えいや不正アクセスなどから守り、情報システムをコンピュータウイルスなどの脅威から守るため、細心の注意を払わなければなりません。

知っておくべきこと

本県では、情報セキュリティを確保するため、「徳島県情報セキュリティポリシー」「徳島県教育委員会情報セキュリティポリシー」等を策定しています。

教職員一人ひとりが、情報セキュリティ対策の重要性を理解しなければなりません。

【USBメモリ等外部記録媒体を適切に管理】

USBメモリ等は、外部記録媒体取扱要領により、適切に管理してください。

- ① 登録していないUSBメモリ等は、使用してはいけません。
- ② 分類1（セキュリティ侵害が個人並びに団体及び組織の生命、財産へ重大な影響をおよぼすおそれのある情報を有する）の情報が入ったUSBメモリ等は持ち出し禁止です。
- ③ 分類2や分類3の情報が入ったUSBメモリ等を持ち出すときは、暗号化した上で持出許可簿により所属長の許可を得てください。
- ④ 外部からUSBを持ち込み利用する場合（講演講師など）はウイルスチェックソフトによりウイルスチェックを行ってください。

【ウィニーなどファイル交換ソフトに注意】

情報セキュリティポリシーに基づいて管理されている職場のパソコンで業務を行ってください。やむを得ず職場のパソコン以外で作業をする必要がある場合はウィニー等ファイル交換ソフトがインストールされていないか確認し、インストールされている場合は作業を行わないでください。

【無許可でのネットワークへの接続の禁止等】

職場のパソコンに無断でソフトウェアを導入してはいけません。

私物のパソコンを職場のネットワークに接続してはいけません。

【業務以外での利用の禁止】

業務以外の目的でインターネットや電子メールを利用してはいけません。

業務以外の目的で情報資産を利用してはいけません。

【クリアデスク・クリアスクリーンの推進】

机の上を片付けるクリアデスク、画面を盗み見られないようにするクリアスクリーンは、情報セキュリティの基本です。各自でクリアデスク・クリアスクリーンを徹底しましょう。

私たちに求められていること

教職員一人ひとりは、この「徳島県情報セキュリティポリシー」「徳島県教育委員会情報セキュリティポリシー」等を熟知し、遵守しながら業務を遂行しなければなりません。

関係法令等

- ・徳島県情報セキュリティポリシー
- ・徳島県教育委員会情報セキュリティポリシー
- ・徳島県教育委員会公文書管理規則
- ・徳島県教育委員会文書規程 等