

情報管理体制チェックリストの参考例

1 基本的な対策のポイント

- (1) 漏えいして困る情報を取り扱うパソコンには、ファイル交換ソフト (Winny等) を導入しない。
- (2) 職場のパソコンに許可無くソフトウェアを導入しない、または、できないようにする。
- (3) 職場のパソコンを外部に持ち出さない。
- (4) 職場のネットワークに、私有パソコンを接続しない、または、できないようにする。
- (5) 自宅に仕事を持って帰らなくて済むよう作業量を適切に管理する。
- (6) 職場のパソコンからUSBメモリやCD等の媒体に情報をコピーしない、またはできないようにする。
- (7) 漏えいして困る情報を許可無くメールで送らない、または、送れないようにする。
- (8) ウイルス対策ソフトを導入し、最新のウイルス定義ファイルで常に監視する。
- (9) 不審なファイルは開かない。

2 管理対策上の点検項目例 (パソコン利用のルールができていますか?)

- (1) 学校、事務所、研究室等で使用するパソコンのセキュリティ対策状況 (ウイルス対策状況、修正プログラム適用状況) を把握しているか?
- (2) 個人情報や機密情報等の外部への持ち出しについてのルールを定めておく。
 - ① 個人情報や機密情報等を含む業務情報を記録媒体などにコピーして外部に持ち出すことについてルールはあるか?
 - ② 持ち出しが認められていない情報が含まれていないか?
 - ③ 記憶媒体などにコピーされて外部に持ち出された個人情報や機密情報等を管理できるか?
- (3) 私有パソコンの利用条件を定めておく。
 - ① 私有パソコンを職場に持ち込んで使用したり、職場のネットワークに接続することについてのルールを定めているか?
 - ② 私有パソコンを利用することを許可制にしているか?
 - ③ 私有パソコンを職場から持ち出す場合のチェックは十分か?

- (4) 教職員へウイルス対策の重要性を再認識させる。
- ①Winny等による情報漏えい事件の主な発生要因を十分理解させているか？
 - ②自分は大丈夫だ、自分には関係ないということは間違いであることの意識改革をさせているか？
 - ③セキュリティ対策製品やサービスも完全ではないことを理解させているか？
- (5) ファイル交換ソフトの使用条件を定めておく。
- ①研究用途など、限られた業務において必要ということでファイル交換ソフトを使用しているパソコンはないか？
 - ②ファイル交換ソフト及びファイルの管理は充分に行っているか？
(実際は、完全なウイルスへの対策は不可能であるといわれており、ファイル交換ソフトを安易に使用しない。)

3 技術対策上の点検項目例（技術上の対策はできていますか？）

- (1) 重要情報に対するアクセス制限を設けているか？
- (2) 重要な情報に対するコピー制限を設けているか？
- (3) 重要な情報を暗号化しておくための対策ができていますか？
- (4) USBメモリ、CD-R、FD、MOなどの記録媒体の利用制限を設けているか？
- (5) 私有パソコンの職場内ネットワーク接続に制限を設けているか？

*この情報管理体制チェックリストの参考例は、独立行政法人情報処理推進機構セキュリティーセンター（IPA）の資料をもとに作成しました。詳しくは、資料6「対策リンク集」のIPA「Winnyによる情報漏えいを防止するために」をご参照ください。

*この情報管理体制チェックリストの参考例は、機関ごとのルールに応じて利用してください。