

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for Illegal Leakage of Technological Information

技術流出の防止に向けて

本年第6号では、情報漏えいを防ぐための「5つの漏えい対策」のうち「秘密情報の『持ち出しを困難にする』ための対策」（持ち出し困難化）についてご紹介しましたが、今回は、

「漏えいが『見つけやすい』環境作りのための対策」（視認性の確保）についてご紹介します。

自社の実情に照らして対策を検討するなど、参考にしてください。



「視認性の確保」に資する対策

情報漏えい行為が「目につきやすい状況を作り出す対策」、「事後的に検知されやすい状況を作り出す対策」を講ずることにより、秘密情報の漏えいを行ったとしても見つかってしまう可能性が高い状態であると認識するような状況を作り出すことを目的としています。

- ✓ 視認性を確保することは、従業員等の行為の正当性（身の潔白）を証明する手段としても有効です。対策の目的が従業員の保護であることを、就業規則等に明記して周知徹底するとともに、従業員の理解を得た上で、適切な運用を行うことが必要と言えます。
- ✓ 現実に監視するというだけでなく、情報管理に関心の高い職場であると認識させ、心理的に漏えいしにくい状況を作り出すことも大切です。



具体的な対策

- 職場のレイアウトの工夫
互いの業務態度が目に入ったり、上司の目につきやすくするような座席配置
 - 入退室の記録
入退室を記録化することによって、氏名等が特定される状況を確認
 - 資料・ファイルの通し番号管理
書類等の必要性を適切に判断し、不要なものは廃棄するとともに、書棚の整理や職場の整理整頓を実施
 - パソコンのログ確認
秘密情報・重要情報へのアクセス履歴、操作履歴（Webへのアクセスログやメールに伴う送受信履歴など）等のログ・認証を記録し、一定期間保存
 - 録画機能付き防犯カメラの設置
情報漏えい行為を行おうとする者に「見られている」という認識の布石
- ※ ここにあるのは一例です。詳細は、経済産業省「秘密情報の保護ハンドブック」をご参照ください。