



産業スパイはあなたの身近に・・・。
 「情報漏洩はうちの会社には関係ない」。いいえ、それは間違いです。
 外部からの不正アクセスや人為的なミスによる漏洩ばかりではなく、
 過去には現職従業員や退職者による漏洩も発生しているのです。
 漏洩を防ぐためには、各事業者による対策が重要となります。



物理的・技術的な防御

接近の制御

秘密情報等に近寄りにくくするための対策をしていきましょう。

- 社内規程に基づく適切なアクセス権の付与・管理
- 分離保管による秘密情報へのアクセス制限 等



持出し困難化

秘密情報等の持ち出しを困難にするための対策をしていきましょう。

- 秘密情報の社外持ち出しを物理的に阻止
- 私物のUSBメモリ等の情報機器の業務利用、持込みを制限 等

心理的な抑止

視認性の確保

漏えいが見つかりやすい環境づくりのための対策をしていきましょう。

- 防犯カメラの設置
- PCやネットワークにおける操作ログの記録、保存とその周知徹底 等



秘密情報に対する認識向上

秘密情報だと思わなかった！という事態を招かないための対策をしていきましょう。

- 秘密情報の取扱い方法等に関する社内規程の作成・周知
- 秘密保持契約等の締結
- 秘密情報であることの表示 等

働きやすい環境の整備

信頼関係の維持・向上等

秘密情報を持ち出そうという考えを起こさせないための対策をしていきましょう。

- 企業への帰属意識の醸成、従業員等の仕事へのモチベーション向上
- 退職者に向けた対策 等



▼ SEAGULL事務局(外事課内) ▼

〒231-8403 横浜市中区海岸通2丁目4番 神奈川県警察本部

相談窓口

Email : seagull@police.pref.kanagawa.jp

