No	**分類**	**説明**	**例**	**対応策**
1	情報管理の徹底	重要な機密情報や知的財産の取扱いに関して、厳重な管理体制を敷くことが求められます。	機密データへのアクセス制限、データの暗号化	アクセス権限の見直し、情報の使用履歴の定期的な監査
2	従業員のモニタリング	不審な行動や不正な情報の持ち出しを防ぐための監視体制を強化します。	不審なデータ転送、異常なログイン履歴	ネットワークの監視システム導入、セキュリティアラートの設定
3	従業員教育	従業員に対して、機密情報の取り扱いに関する教育を行い、スパイ行為への警戒心を高めます。	情報漏洩防止の研修、スパイ行為への警戒心の強化	定期的なセキュリティ教育、倫理研修の実施
4	内部告発制度の整備	従業員が不正行為を匿名で報告できる仕組みを整備し、内部からのスパイ行為を早期に発見します。	匿名通報システム、ホットラインの設置	内部告発の保護、透明な報告プロセスの構築
5	セキュリティソフトウェアの導入	情報の不正な持ち出しや外部との不正な通信を防ぐため、最新のセキュリティ技術を導入します。	ファイアウォール、侵入検知システム	最新のセキュリティソフトの導入、定期的なアップデート
6	採用・退職時の管理	新規採用時や退職時に、不正行為を防止するための手続きや管理を徹底します。	採用時の信用調査、退職時のデータ持ち出し防止	厳格な採用プロセス、退職者のITアクセス権限の即時停止