機密管理と情報セキュリティ

機密漏えいの防止、情報の外部からの攻撃に対する防御が事業活動には不可欠と考えています。
当社のみならず取引先の情報は適切な管理・取り扱いをすべき資産であるとの認識に基づき、機密管理と情報セキュリティ活動を推進しています。

基本的な考え方

当社では、「社員行動指針」に「機密情報は、規則に従って厳重に管理し、漏えいの防止に努めます。」と定め、各部に機密管理責任者、機密情報取扱者を置き、職場でのミーティングや自主点検を実施することで機密管理意識の向上に努めています。

また、会社を守り、ひいては社員を守るために、「情報漏えい5つの対策」として、アクセス権の制限、施錠管理などの物理的・技術的な防御、パソコンの操作履歴の記録、機密区分の明示などの心理的な抑止、漏えい事例の周知などによる働きやすい環境の整備に取り組んでおり、その内容は国内外のガイドラインに準拠しています。

■5つの対策

物理的・技術的な防御

接近の制御

1

機密情報に近寄りにくくする対策

- アクセス権の制限
- 施錠管理
- ペーパーレス化

持ち出し困難化

2

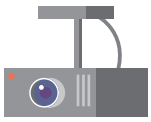
機密情報の持ち出しを困難にする対策

- 私用USBメモリの利用・持込み禁止
- 電子データの暗号化
- 外部へのアップロード制限

心理的な抑止

視認性の確保

3



漏えいが見つかりやすい環境をつくる

- 関係者以外立入禁止看板
- 職場の整理整頓
- パソコンの操作履歴の記録

機密情報に関する認識向上

4

機密情報であることを明示する

- マル秘表示
- 機密保持契約の締結
- 研修の実施

働きやすい環境の整備

信頼関係の維持・向上

5

社員に気づきを与える

- コミュニケーションの促進
- 漏えい事例の周知

※2016年6月 経済産業省「営業秘密の保護・活用について」を元に作成

物理的・技術的な防御の事例

2017年11月より、ICカード認証の複合機導入により情報漏えいリスクの低減を図りました。

また、半年に一度、抜き打ちでの持ち物検査を実施し、社員へ機密管理に対する自覚を促しています。

ICカード認証の複合機導入

持ち物検査の様子

心理的な抑止の事例

2018年10月に一般社員向けeラーニングを実施し、約4,000人が受講しました。

日常業務の様々なシチュエーションで想定される対処と、それにより発生しうるリスクについて知識を深めました。

また、2017年12月には機密管理のてびきを改訂し、機密の定義からインシデント発生時の対応方法までをイラスト付きで分かりやすく解説しています。

eラーニング画面

機密管理のてびき(抜粋)

実施
約4,000名