情報セキュリティポリシー

株式会社エイ・シー・テイ(以下、ACT とします)は情報漏洩リスクに対して対策を講じることによりお客様の信頼を得る必要があります。このため、情報セキュリティを社の基本的理念とする目的でその方針を明文化した情報セキュリティポリシーを策定しました。
今後はこの情報セキュリティポリシー及び個人情報保護方針を遵守し、高度な情報セキュリティ管理体制を維持していくことに努めます。

1 情報セキュリティポリシーの対象
情報セキュリティポリシーが対象とする情報資産は ACT の企業活動において入手及び知り得た情報、ならびに ACT が業務上保有するすべての情報とし、この情報資産の取り扱い及び管理に携わる ACT の役員、社員および、ACT の情報資産を取り扱う業務委託先およびその社員が遵守することとします。

2 情報セキュリティ管理体制の構築
ACT が保有する全ての情報資産を保護するとともに、情報セキュリティに関する法令その他の規範を遵守し、セキュアな情報セキュリティ管理体制を構築します。

3 情報セキュリティ管理責任者の配置
情報セキュリティ管理責任者(※)を設置します。これにより全社レベルの情報セキュリティの状況を正確に把握し、必要な対策を迅速に実施できるようにします。

4 情報セキュリティに関する内部規程の整備
情報セキュリティポリシーに基づいた内部規程を整備し、個人情報だけではなく情報資産全般の取り扱いについて明確な方針を示します。情報漏洩等に対しては、厳格な態度で臨むことを周知徹底します。

5 徹底した情報セキュリティ対策システムの実現
情報資産に対する不正な侵入、漏洩、改ざん、紛失、破壊、利用妨害などが発生しないよう、徹底した対策を反映したシステムを実現していきます。対策として高セキュリティエリアでの作業(錠、訪問者確認などを施した作業場所)、DB アクセス権の制限(グラント、パスワード管理、ファイアウォール)などによりコンピュータ、DB へのアクセスをコントロールします。

6 情報セキュリティリテラシーの向上
役員・社員にセキュリティ教育や訓練を徹底し、ACT の情報資産に関わる全員が情報セキュリティを理解し業務を遂行します。また、刻々と変化する状況に対応できるよう、教育や訓練を継続します。

7 外部委託先の管理体制強化
外部委託の際は、外部委託先としての適格性を十分に審査し、ACT と同等以上のセキュリティレベルを維持するよう要請していきます。また、これらのセキュリティレベルが適切に維持されていることを継続して確認するため、外部委託先を継続的に見直し、契約の強化に務めます。

8 情報セキュリティポリシーの見直し
情報セキュリティポリシーは、随時見直しをしていきます。

※CISO:Chief Information Security Officer

2007 年 2 月 20 日制定