

情報セキュリティ基本方針

1. 基本方針

川西航空機器工業株式会社（以下当社という）は、航空機、宇宙関連機材等の設計・開発・製造及びサービス提供（引取り修理）を行う事業所として、お客様およびお取引先様から貸与された情報資産ならびに当社の情報資産を守ることが責務と考え、以下の方針に基づき情報セキュリティ管理を行う。

(1) 情報セキュリティの組織目的と維持

顧客から委託され取り扱う資産の消失、盗難、不正使用、漏えいを防止することを組織の目的とする。情報セキュリティとして、顧客から委託され取り扱う資産及び当社が取得した個人情報及び当社が保有する資産について、機密性、完全性、可用性を確保し、維持する。

(2) 適用範囲

本社工場・那須工場

「航空・宇宙関連機材の設計・開発・製造及びサービス提供（引取り修理）」

(3) 経営者の責任

ISMSの基本方針及び目的を定め、情報セキュリティ管理責任者を任命する。また、ISMSの活動に必要な経営資源を提供する。経営者は、リスクアセスメントの枠組み、リスク受容水準及びリスクの受容可能レベルを決め、リスクアセスメントの結果、残留リスク、管理策の採否結果及び構築されたISMS、推進するセキュリティ計画の承認、決定を行う。また、定期的な内部監査、マネジメントレビューを実施し、採用した管理策の有効性評価、実施した改善の有効性の評価、リスクアセスメントの結果及びマネジメントシステム並びにこの基本方針を見直し、ISMSの継続的な改善を図る。

(4) 情報セキュリティ管理責任者の義務

ISMSの活動を推進し、情報セキュリティ責任者とともにISMSを確立し、導入、運用、監視、見直し、維持及び改善を図る。

(5) 資産の特定とリスクアセスメント及び管理策の選択

情報セキュリティ委員会は、資産の管理者を特定する。特定した資産について、リスクアセスメント法を定め、資産の保護の為に適切な管理策を選択する。

(6) 法令の順守

業務上関連する法令を明確にし、順守する。

(7) 要員の義務

組織は「ISMS基本方針」及び「ISMSに関する社内規定」を順守して行動する。違反した場合には当社の就業規則に則り懲戒処分する。

(8) 教育・訓練

組織は教育訓練計画書及び情報セキュリティ管理責任者の指示に基づき実施する。

2. 目標

No	項目	チェック
1	ISO/IEC27001:2013 (JISQ27001:2014) のマネジメントシステムの継続的改善（管理策有効性測定評価管理表→目標達成可否評価→P-D-C-A 継続改善）	PDCA 内容の評価と改善 1回/年
2	リスク対応計画書におけるリスク受容水準の維持	受容水準のチェックと内容改善 2回/年
3	携帯電話等、進歩の著しい情報システムに関するセキュリティ計画の立案ならびに推進	セキュリティ計画立案回数 1回/年
4	那須工場の ISMS 認定の維持と向上	特別監査実施 1回/年
5	情報セキュリティスキルの維持と理解度確認テストによる教育訓練の継続的实施及びフォローアップ	テスト実施 1回/年
6	事業の継続を図るため、発生する災害、故障、事故への迅速かつ的確な対応により被害の最小化と再発防止策の対応による事業を早期回復できる体制の構築。	迅速対応の状況確認と改善 1回/年