

情報セキュリティ基本方針

株式会社研創（以下、当社）は、「常に学び 研究し 創造する」精神のもと、当社の情報資産を事故・災害・犯罪などの脅威から守り、当社のお客さま・取引先・株主・社員等のステークホルダー（利害関係者）、ならびに社会の信頼に応えるべく、以下の方針に基づき、全社で情報セキュリティの向上に継続的に取り組みます。

なお、当社はサインの受注から製造・販売において稼働するオリジナルシステムの可用性および安定性が、事業継続における最優先事項であることを認識しています。そのため、一般的な情報セキュリティの基準を一律に適用するのではなく、環境の特性に応じた最適な対策を講じるものとします。

1. 経営者の責任

当社は、サイバーセキュリティリスクを経営上の重要リスクの一つと認識し、組織のミッションや各資産の技術的制約を踏まえ、リスク許容度に基づいた戦略的な意思決定を行います。また、必要な資源（予算・人材・技術）を適切に配分し、実行責任と説明責任を明確にします。

2. 社内体制の整備と独自基準の運用

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。規則の策定にあたっては、最新のセキュリティ技術の適用が困難な環境等について、代替策による当社独自の管理基準を適用し、実効性の高いリスク管理を行います。

3. 従業員の取組み

当社の従業者は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

4. 法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

また従業員に対し、最新の脅威動向を踏まえた定期的かつ実践的な教育・訓練を実施します。又、専門的な職務を担う者には、その役割に応じた高度なスキルを習得させることで、組織全体の防御力を維持・向上させます。

5. 検知・対応及び復旧体制の整備

当社は、サイバー攻撃の予兆や侵害を早期に検知するための監視体制を整備します。万一、事案が発生した場合には、CSIRT（Computer Security Incident Response Team）を中心とした迅速な応急対応を行うとともに、あらかじめ策定した事業継続計画（BCP）に基づき、資産の完全性を検証した上で速やかに復旧し、ステークホルダーへの説明責任を果たします。

6. サプライチェーンの安全確保

当社は、委託先やクラウドサービス事業者等のパートナーを含めたサプライチェーン全体のセキュリティ向上を図ります。委託先の選定に際しては厳格な基準を設け、契約においてセキュリティ責任を明確にするとともに、継続的な監督・評価を実施します。

制定日；2026年10月1日

株式会社 研 創
代表取締役 社長 林 大一郎