# カルビーグループ 情報セキュリティポリシー

## ・基本理念

カルビーグループにとって、デジタル・IT の活用は、「変革」を興す重要な手段です。一方で、デジタル・IT を安全に活用し続けるためには、情報セキュリティは不可欠です。そこで、情報資産を「ヒト・モノ・カネ」に次ぐ第 4 の資産と捉え、サイバー攻撃、不正アクセス、情報漏えい、改ざん、紛失、災害その他の脅威から適切に保護します。また、事業活動の継続と社会からの信頼確保のため、以下の方針に基づき、グループ全体で情報セキュリティに取り組みます。

## ・適用範囲

カルビー株式会社及びその国内、海外の子会社（以下、「当社グループ」といいます）を対象とします。

## ・情報セキュリティポリシー

### 1. 経営者の責任

当社グループの経営層は、情報セキュリティを経営課題として認識し、必要な体制・人材・予算を確保するとともに、全社的かつ継続的な情報セキュリティ活動を推進します。

### 2. 法令・規制および契約上の要求事項の遵守

当社グループは、各国・地域における情報セキュリティに関する法令、規制、ガイドラインならびにお客様・お取引先様との契約上の義務を遵守します。そのために、当社グループ各会社において、本方針に則した規程などを整備・運用します。

### 3. 推進体制の整備

当社グループは、情報セキュリティに関する責任と役割を明確にした推進体制を整備し、グループ全体のガバナンスの強化に取り組みます。体制整備においては、内部統制、プライバシー保護など他のリスク体制との整合を考慮します。

### 4. 情報資産の保護と安全なデジタル・IT 活用

当社グループは、事業推進に必要な情報およびシステムを情報資産として管理し、デジタル・IT を安全かつ適切に活用できる環境を整備します。その際には、守るべき資産とリスクを把握して、リスクへの対策を計画します。また、情報資産を扱うビジネス・IT パートナーにも適切な保護と安全な活用を求めます。

**5. 教育・啓発**

当社グループは、情報資産を扱う従業員に対して、雇用形態にかかわらず教育・訓練を実施し、情報セキュリティに関する知識、意識および対応能力の向上を図ります。

**6. インシデントの防止と対応**

当社グループは、インシデントを防止するための仕組みを構築し、事業環境や脅威に応じた見直しを行います。万が一、インシデントが発生した際には、迅速かつ適切に対応し、被害の最小化、原因究明および再発防止に努めます。

**7. 取組状況の点検・監査と継続的改善**

当社グループは、情報セキュリティ対策の有効性について定期的な点検、評価および監査を実施し、その結果を踏まえて継続的な改善に取り組みます。また、情報技術の発展にあわせた改善ができるように社外の情報収集を積極的に行います。

**8. 個人情報保護**

個人情報については、各国・地域の法令および当社グループのプライバシーポリシーに基づき適切に管理運用を行います。

2026 年 10 月 8 日制定