

# サイバーセキュリティ管理に関する基本方針

制定 2026年4月1日

網走信用金庫は、サイバー攻撃による脅威が高まる状況を踏まえ、サービスを安定的かつ適切に提供するため、サイバーセキュリティへの取組みを重要な経営課題と位置づけ、以下の方針に基づきサイバーセキュリティ管理を継続的に実施します。

## 1. 経営陣の責務

経営陣は、自らがリーダーシップを発揮し、サイバーセキュリティリスクを把握するとともに、必要となる経営資源を配分し、サイバーセキュリティに関する管理態勢の整備及び対策の実施等に努めます。

## 2. 管理態勢の整備

サイバーセキュリティリスクへの対応に関する役割と責任範囲を明確にし、サイバーセキュリティ管理態勢を構築します。具体的には、サイバー攻撃の検知、特定、防衛体制を整備するとともに、インシデント発生時の業務継続計画や緊急対応態勢の整備およびサイバー攻撃に備えた業務継続・復旧体制を整備します。

## 3. 対策の実施

サイバーセキュリティリスクを把握したうえで、必要な対策を事業計画等に反映し、実施します。

## 4. 継続的な改善

事業環境やリスクの変化に対応するため、サイバーセキュリティ管理態勢の見直しを継続的に実施します。

## 5. 委託先の管理

委託先（サードパーティを含む。）におけるサイバーセキュリティ対策について、適切な管理に努めます。

## 6. 法令遵守

サイバーセキュリティに関する法律等及び契約上の義務を遵守します。

## 7. 人事育成

役職員のサイバーセキュリティに係る意識向上に必要な教育・訓練等の啓発活動に努めます。

## 8. 情報連携

平時及びインシデント発生時において、関係省庁、委託先、業界関連組織等と密接に連携のうえ、ステークホルダーに対する適切な情報開示に努めます。

以上