サイバーセキュリティ管理の基本方針

株式会社日本政策金融公庫（以下「公庫」といいます。）は、サイバー攻撃の脅威が日々深刻化・巧妙化する状況においても、政策金融機関としてお客さまの信頼に応え続けるため、サイバーセキュリティの確保を経営上の重要課題と位置づけ、その取組みの基礎となる「サイバーセキュリティ管理の基本方針」を定めています。本方針のもと、経営主導によるサイバーセキュリティ管理態勢の強化を推進してまいります。

◆ サイバーセキュリティ対策と管理態勢

公庫は、お客さまに安心して政策融資をご利用いただくために、サイバーセキュリティ管理態勢を構築し、その高度化に取り組みます。

具体的には、IT 部門が、人的・技術的・物理的なサイバーセキュリティ対策を推進し、訓練や過去のインシデントから得た教訓、最新の技術・脅威動向を踏まえたリスク評価を定期的に行います。同時に、サイバーセキュリティに関する監査結果や、外部の専門機関の知見を取り入れながら、サイバーセキュリティ対策の継続的な改善を行います。加えて、外部委託先によるセキュリティ対策の実施状況についても、継続的に確認を行います。

サイバーセキュリティの統括管理責任者である企画管理本部長は、IT 部門から定期的に報告を受け、サイバーセキュリティ管理態勢の整備に取り組むとともに、これらの報告内容を、定期的かつ必要に応じて取締役会で報告します。

◆ セキュリティインシデント対応チーム（CSIRT）の設置

サイバー攻撃事案が発生した際の初動対応を迅速に行うための内部横断的組織として、日本公庫 CSIRT（Computer Security Incident Response Team）を設置し、早期に事態収束を図り事業を継続する体制を整えています。また、平時には関係者が広く参加する各種演習・訓練を実施することで、CSIRT のスキル向上やサイバー攻撃への対応力強化に取り組みます。この演習・訓練には、経営陣及び業務部門の責任者も参加し、結果や課題の共有と改善策の検討に直接的に関与します。

◆ サイバーセキュリティに関する社内教育

経営陣を含む全職員に対し、サイバーセキュリティの意識向上を目的とする教育及び研修を定期的に実施します（標的型メール訓練、情報セキュリティに関するｅラーニング等）。また、全職員を対象とする自己啓発支援制度により、セキュリティ関連の資格取得に向けた支援を行います。加えて、情報セキュリティ業務に従事する職員は、外部機関が実施するサイバーセキュリティ訓練等に参加し、知識・技量の継続的な向上に取り組みます。

◆ 情報の共有

関係省庁・組織・団体等と連携し、積極的な情報共有を図ります。具体的には、主務省、捜査機関等に適時適切に報告するとともに、外部機関との情報交換を行います。