2026年4月1日

公式キャラクター
はまなか　あい

プレスリリース

福島銀行

「福島銀行サイバーセキュリティ管理の基本方針」の策定について

福島銀行（取締役社長 鈴木 岳伯（たけのり））は、近年高度化・巧妙化するサイバー攻撃への対応を強化し、お客さまの大切な情報資産および金融サービスの安全性・信頼性を一層確保するため、「福島銀行サイバーセキュリティ管理の基本方針」を策定しておりますので、お知らせいたします。

金融機関を取り巻くサイバーリスクは年々増大しており、システム障害や情報漏えいが社会・経済活動に与える影響は極めて大きなものとなっています。当行は、地域金融機関としての社会的責任を果たすべく、サイバーセキュリティを経営上の重要課題の一つと位置付け、組織的かつ継続的な対策を推進してまいります。

記

1．　福島銀行サイバーセキュリティ管理の基本方針

別紙の通り

2．　制定日

2025年7月1日（火）

3．　公表日

2026年4月1日（水）

以　上

本件に関するお問い合わせ先
事務・システム部 システム課 佐藤　TEL 024-525-3158

報道機関のお問合せ先
総合企画部 経営企画課 広報室 山内　TEL 024-525-2973

（最終改訂 2025 年 7 月 1 日）

福島銀行サイバーセキュリティ管理の基本方針

1. 経営の基本姿勢

当行は、サイバーセキュリティを事業の持続的成長と社会的責任の重要な要素と位置付ける。安全かつ信頼性の高いサービスを提供するため、サイバーセキュリティ対策を組織全体で推進し、必要な資源を確保しながら継続的な強化・改善を行う。

また、顧客、取引先、従業員、金融当局、地域社会などの関係者の信頼を維持し、法規制や業界ガイドラインに適切に対応する。

2. 体制と責任

・サイバーセキュリティに関する管理責任者はシステム担当役員とし、組織的なリスク管理を実施する。サイバーセキュリティの主管部署はシステム担当部署とする。
・サイバー攻撃への対応能力強化策として、CSIRT※を設置する。
・関連会社・外部委託先に対しても適切なセキュリティ対策を求め、定期的な確認を行う。

※CSIRT（Computer Security Incident Response Team：シーサート。サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための銀行全体の横断的な組織）

3. リスク管理と対策

・情報資産を特定、リスクの洗い出しと評価を実施し、必要な対策を計画・実行する。
・最新の脅威情報を収集・分析し、適切なセキュリティ対策を講じる。
・サイバー攻撃に備え緊急時の対応マニュアルを策定し、迅速な復旧体制を確立する。

4. 人材育成と意識向上

・サイバーセキュリティ専門人材の育成を推進し、研修や資格取得を支援する。
・全社員を対象としたセキュリティ教育や演習を定期的に実施し、意識向上を図る。

5. 継続的な改善

・サイバーセキュリティ対応の状況を定期的に経営陣へ報告し、リスク管理の透明性を確保する。
・最新の技術や脅威動向を踏まえ、対策を定期的に見直し、強化する。

以上