２０２５年9月２６日

各　　位

株式会社 大垣共立銀行

「サイバーセキュリティ管理に関する基本方針」の制定

大垣共立銀行（頭取　林 敬治）は本日、**「サイバーセキュリティ管理に関する基本方針」を下記の通り制定**しました。

ＯＫＢは、サイバーセキュリティ基本法に規定される重要社会基盤事業者としての責務を果たすため、有事の際における業務の早期復旧と事業継続性の確保を図るとともに、お客さまの大切な資産および情報資産をサイバー脅威から保護し、安心・安全な金融サービスを提供することを使命とします。金融という社会インフラの安定稼働と持続的発展に貢献するため、ＯＫＢグループが一体となって本方針に基づきサイバーセキュリティの確保に取り組んでいきます。

記

■「サイバーセキュリティ管理に関する基本方針」

項　　目	**１．経営課題としての認識とリーダーシップ** **２．セキュリティ対策の基本的な考えと体制整備** **３．サプライチェーンおよび先進技術への対応** **４．人材育成と組織文化の醸成** **５．法令順守と透明性の確保** **６．地域社会・業界との連携と貢献** **７．サービス開発におけるセキュリティ確保**
全　　文	別紙またはＯＫＢのホームページ（https://www.okb.co.jp/announcement/）をご参照ください

以　上

別　紙

サイバーセキュリティ管理に関する基本方針

株式会社大垣共立銀行（以下「当社」といいます）は、サイバーセキュリティ基本法にて規定される重要社会基盤事業者としての責務を果たすべく、インシデント発生時における業務の早期復旧と事業継続性の確保を図るとともに、お客さまの大切な資産および情報資産をサイバー脅威から保護し、安心・安全な金融サービスを提供することを使命とします。

また、金融という社会インフラの安定稼働と持続的発展に貢献するため、当社およびグループ各社が一体となって、以下の基本方針に基づき、サイバーセキュリティの確保に取り組みます。

１．経営課題としての認識とリーダーシップ

当社はサイバーセキュリティを経営の重要課題と位置づけ、必要な投資を行い、経営陣自らがリーダーシップを発揮して対策を推進します。

また、取締役会等においてリスク状況を定期的に検証し、経営レベルでの意思決定と対応を行います。

２．セキュリティ対策の基本的な考えと体制整備

サイバーセキュリティ戦略および対応計画に基づき、リスクの特定、防御、検知、対応、復旧までを一貫して実施する体制を整備するとともに、インシデント発生時の早期復旧を目的としたＢＣＰ（事業継続計画）との連携を強化します。

また、専担組織を設置し、必要な予算・人員を確保するとともに、定期的な演習・訓練等を通じて対応力の向上を図ります。

３．サプライチェーンおよび先進技術への対応

取引先や委託先、クラウドサービス事業者などを含むサプライチェーン全体のサイバーセキュリティリスクを適切に管理・監視します。

また、適切な先進技術を活用し、脅威への対応力を強化します。

４．人材育成と組織文化の醸成

全役職員を対象としたセキュリティ教育・訓練等を継続的に実施し、サイバーセキュリティに対する意識と知識の向上を図るとともに、経営層から現場まで一体となったセキュリティ文化の醸成に努めます。

５．法令遵守と透明性の確保

サイバーセキュリティ関連法令・ガイドライン等を遵守し、社内外のステークホルダーに対して、リスクと対応状況を適切に開示します。

６．地域社会・業界との連携と貢献

行政機関や業界団体等と連携し、情報共有や注意喚起を通じて、地域社会および業界全体のサイバーセキュリティ向上に貢献します。

７．サービス開発におけるセキュリティ確保

新たなシステムやサービスの開発・提供においては、セキュリティ・バイ・デザインの考え方を取り入れ、安全なセキュリティ対策を実施し、お客さまが使いやすく安心してご利用いただけるサービスの提供に努めます。