経営基盤

業務継続体制

基本的な考え方

当行では、万一の大規模な自然災害、感染症の蔓延等の危機発生時において、早期に被害の復旧を図り、必要最低限の業務を継続するための業務継続計画(BCP)を策定する等、業務継続体制の構築を図っております。

また、近年、サイバーセキュリティ対策の重要性が高まっており、当行では、サイバー攻撃による危機を未然に防ぐとともに被害局限化に向けた取り組みを行っております。

業務継続の基本方針

自然災害・感染症の蔓延・事故災害・人為的災害等による大規模な被害発生により、当行の業務継続が脅かされる危機発生時において、速やかに業務の復旧を図るため、次の方針を定めております。

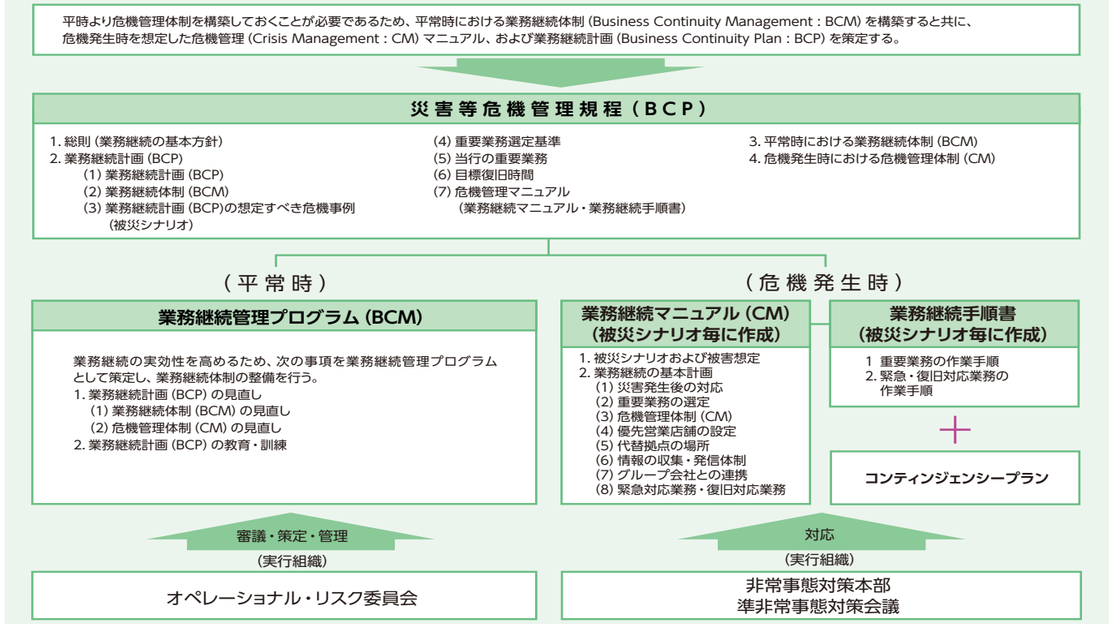
○被災地等の地域住民のみなさまの生活や経済活動の維持のため、金融サービスの継続に努めます。
○金融決済機能を維持し、経済活動の混乱を抑制することに努めます。
○役職員の安全を確保するとともに、業務の停止に伴うお客さまからの信認低下など、当行の経営面の影響を軽減します。

災害発生時の危機管理態勢

平常時には、BCPに基づく危機管理体制を見直し、改善するための年間計画として業務継続プログラムを策定し、体制整備を図っております。

また、自然災害・感染症の蔓延等の危機発生時には、「非常事態対策本部」により一元的に指揮・命令を行う体制としており、被災シナリオごとに作成した業務継続マニュアル、業務継続手順書およびコンティンジェンシープランに基づき、早期の業務復旧を目指します。

【当行の危機管理態勢】



【大規模災害発生に備えた自治体や他金融機関等との連携】

当行では、大規模災害時においても、地域における金融・決済業務を維持・継続するため、次のように、地元自治体や他の金融機関との相互支援に向けた連携を強化しております。

- NTTデータ地銀共同センター参加行とNTTデータによる「大規模災害発生時における相互支援協定」を締結
- 地域再生・活性化ネットワーク参加9行での「大規模災害発生時の広域相互支援協定」を締結
- 近畿地銀7行での「大規模災害時の相互支援に関する協定書」を締結
- 京都府および京都府に本店を置く3信用金庫と「大規模災害発生時における相互支援協定」を締結

サイバーセキュリティ

当行は内外の組織や専門家と協力し、コンピュータ・セキュリティ事案の検知、解決、被害局限化および発生の防止を図ることにより、サイバーセキュリティ向上に取り組んでおります。

具体的には、「情報セキュリティポリシー」に基づき、「システムリスク管理規程」ならびに「サイバーセキュリティ対応規程」を定め、サイバー攻撃に関するリスクを適切に管理し、サイバーセキュリティ対応を行うための態勢を整備しております。

当行では、日々高度化・巧妙化していくサイバー攻撃による脅威に対応するため、システム部内にサイバーセキュリティ対策室を設置し、サイバー攻撃の動向や脆弱性等の情報収集・把握、サイバー攻撃事案への対応(検知、解決、被害局限化、対策等)を一元的に実行できるようにしております。

また、定期的にサイバー攻撃事案を想定した訓練を実施し、実効性の向上に努めております。

お客さまに提供するインターネット上のサービスについては、不正アクセスやサービス停止攻撃等への対策を講じるほか、インターネットバンキングの不正使用防止を図るための対策を実施しております。

【事例】 外部評価を活用した取り組み

サイバーセキュリティへの取り組みにおいて、これまでの金融庁から還元される資料を基にした自己評価に加え、NRIセキュアテクノロジーズ株式会社が提供するSecure SketCHの自動診断機能(SecurityScorecard社のリスクレーティング連携)を採用し、客観的かつ俯瞰的な評価を活用した取り組みを行っております。

現時点では5段階評価の最上位評価かつ同業種平均を上回る評価を得ておりますが、発見された課題解決に取り組むとともに、リスク状況の変化に応じた将来的な情報セキュリティの高度化を図ってまいります。

【Secure SketCHによる評価結果(一部抜粋)】