IT戦略

基本的な考え方

SMBCグループでは、7つの戦略事業領域を支えるデジタライゼーションの取組を、攻めのデジタル化と守りのデジタル化の両面から推進しています。

攻めのデジタル化・守りのデジタル化

攻めのデジタル化は「新規ビジネス・事業の創造」と「既存のビジネスモデルの変革を通じた顧客価値・事業価値の創出」、守りのデジタル化は「旧来型の既存業務・プロセスのIT化」と「中長期ビジネス変革を支えるITインフラ」、合計4つの領域において、それぞれデジタル化を推進しています。

足許では、攻めのデジタル化として人工知能の活用や、キャッシュレス戦略等を推進する一方、守りのデジタル化においても、既存システムの維持や安定運行という観点だけではなく、グループベースでの共通基盤化やクラウドの活用による効率的な運営、先端のITインフラや開発技術等を活用し、最新のアーキテクチャに変革していくITトランスフォーメーションへの取組を推進しています。

IT投資戦略

前中期経営計画期間に三井住友銀行における勘定系システムの基盤更改や東西相互バックアップ体制の構築等、大型のシステム更改を終えており、現在の中期経営計画期間では、デジタライゼーションによる新規ビジネス創出や業務革新といった戦略分野に対しての資源配分を一層強化しています。

IT投資においては、システム化案件の厳選はもとより、その効果を極大化するため、システム開発プロジェクトの前後で効果の評価・検証を行っています。プロジェクトごとにROIやKPIを設定し、プロジェクト完了後もその達成度合いを5年にわたって検証の上、効果の低いものについては対策を講じます。また、効果達成後もシステムごとの有効性をユーザー満足度、効率性、安定性、活用度という4つの指標で検証し、有効性が悪化しているシステムについては対策を講じています。こうしたPDCAサイクルにより、IT投資効果の極大化を図っています。

デジタルガバナンス・人材の高度化

グループCIOの下、海外拠点も含めてグループ各社とのレポーティングラインを明確化し、グループ・グローバル一体のガバナンス態勢を構築するとともに、従来の品質を重視したITガバナンスに加え、リスクベースやスピード重視の考え方も取り入れた「デジタルガバナンス」に発展させ、デジタライゼーションを加速しています。

また、SMBCグループ各社のIT関連部署間における人材交流を計画的に実施するとともに、グループの中核IT会社である日本総合研究所にITやデジタル化推進に関する研修組織「デジタルユニバーシティ」を設置しています。ここでは、グループ各社の業務をベースとした研修や、プロジェクトの実例から得られるノウハウを活用したカリキュラム、最新技術に関するワークショップ等、独自の研修を行っています。

サイバーセキュリティ

深刻化・巧妙化の一途を辿るサイバー攻撃のリスクに対応するため、SMBCグループでは、トップリスクのひとつにサイバーリスクを掲げ、「サイバーセキュリティ経営宣言」を策定し、セキュリティ対策を強化しています。

経営主導の態勢強化のため、グループCIO・CROの下に、システムリスク統括室長を「CISO」という専門的な責任者として配置する体制としました。CISOの役割・責任を明確化するとともに、「CSIRT」「SOC」を設置、グループ内外から集まる脅威情報や観測事象を分析し、推進中のセキュリティ対策の状況と合わせて定期的に取締役会および経営会議の場で議論することで、継続的なレベルアップに努めています。

CSIRTは、サイバーセキュリティ専担組織を有するシステムリスク統括室が中心となって構成する組織で、サイバーインシデントの発生に備え、国やFS-ISAC*1、金融ISAC*2等の外部機関とも連携し、攻撃者の手口や脆弱性情報等を共有しています。

SOCは、日本総合研究所を中心に組織しており、グループ各社の監視体制の一元化推進、グローバルベースでの24時間365日監視体制構築等、高まるサイバー攻撃へのリスクに備えるべく、引き続きセキュリティ監視の強化に努めています。

*1 Financial Services Information Sharing and Analysis Center（米国における金融業界のセキュリティ連携を担う組織）の略
*2 日本版FS-ISAC

SMBCグループのサイバーセキュリティ経営体制