Business Continuity Management 業務継続

当グループでは、地震・台風等の自然災害や火災・テロ等の人的災害、新型コロナウイルスも含めた感染症、システム障害および情報資産の漏洩を主な危機として捉え、発災時における業務継続態勢をグローバルに構築し、社内の啓蒙活動も含めてさまざまな準備・対策に取り組んでいます。

業務継続態勢

当グループでは危機発災時に備えて「グループ危機管理委員会」を設置し、国内・海外における業務継続をはじめ、平時より危機管理体制の整備を進めています。危機管理委員会は、グループCEOが指名した役員を委員長としグループ各社役員等の委員で構成され、同委員会の決議内容は経営会議に対して報告されます。また、同委員長は大きな災害発生の際には、対策本部を設置し、社員や家族の安否確認、安全確保、被害拡大の防止、および業務継続態勢の維持等のため適切な措置を講じます。

具体的な業務継続態勢としては、地震、台風、または気候変動を要因とした自然災害等で主要拠点が被災し使用不能となった場合、バックアップオフィスでの業務継続に加えリモートで対応できる態勢を整えています。また、データセンターで障害が発生した場合もバックアップのデータセンターを遠隔地に設けることにより、重要なデータやアプリケーションの維持に努めております。さらに自家発電装置等インフラ面でも強化を図っており、局所的な災害のみならず首都直下地震等の広域災害が発生した場合においても、システミックリスクの回避やお客様の生活基盤保護等の観点から重要な業務を継続できるよう準備しています。海外の主要拠点においても同様のインフラを整備しています。

今般の新型コロナウイルスへの対応では、当グループのガイドラインおよび政府や自治体の要請に沿い、在宅勤務やローテーション勤務によるオフィス出社の抑制、出張等の移動の制限、セミナーや会議の開催など感染の一因となるおそれがある活動の自粛等を実施し、感染拡大防止と業務継続態勢の確保に努めております。海外の主要拠点においても在宅勤務を中心とした勤務体制により業務継続を図っています。

これらの地震・感染症等の有事発生時に迅速に対応できるよう、平時から、危機管理委員会事務局（海外ではBusiness Continuity Managementチーム）は安否確認訓練・防災訓練・業務継続訓練などを実施し、練度の向上と危機管理態勢の強化に努めています。

業務継続にかかる主な取り組み

1 業務継続態勢の強化

バックアップオフィスの整備／非常時対応要員の確保／通信機器の整備/テレワーク環境の整備

2 訓練・研修の継続的な実施

社員の安否確認訓練／業務継続計画（Business Continuity Plan, BCP）に沿った業務訓練／首都直下地震等の大規模地震発生時を想定した初動対応研修・訓練／南海トラフ地震研修

3 国内外グループ各社との連携強化

国内グループ会社との情報連携の充実／海外グループ会社との情報連携体制の強化

4 BCP

首都直下地震等の大規模災害、大規模システム障害等を想定した業務継続計画の更新

CyberSecurity サイバーセキュリティ

サイバーセキュリティ対策

野村グループでは、深刻化するサイバーセキュリティに対する脅威からお客様の情報、お客様の資産を守り、安心してお取引を行っていただくため、グループ危機管理委員会およびグループ情報セキュリティ担当役員のリーダーシップのもと、金融庁が制定している金融商品取引業者向けの監督指針や、米国国立標準研究所（NIST）の「Cybersecurity Framework」その他海外のフレームワークを参考に、グループ・グローバルワイドでの包括的なサイバーセキュリティ対策の強化に努めております。

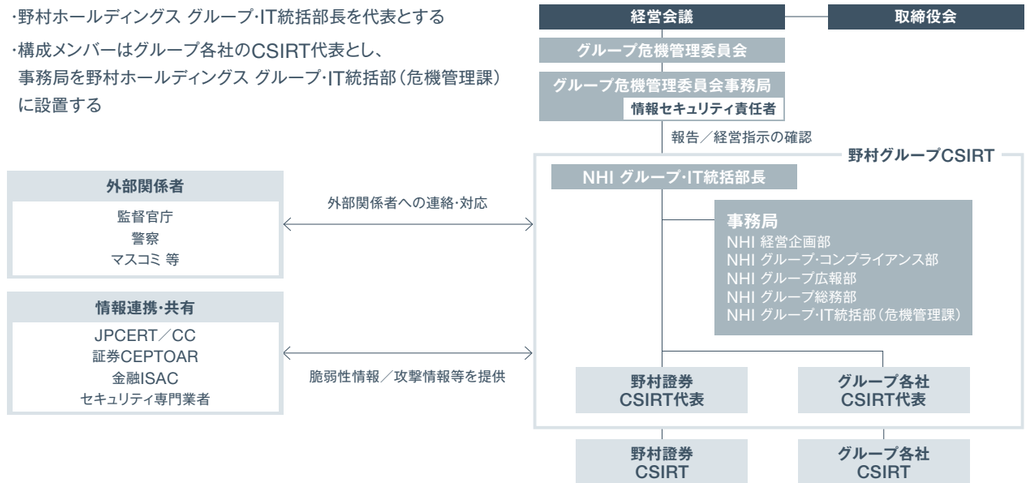
直近では、クラウドサービス利用の進展を踏まえたガバナンス態勢の見直しを重点強化ポイントの一つとして推進していますが、今後も、他金融機関やセキュリティ専門業者、官公庁などと緊密に連携しつつ、情勢の変化に迅速に対応してまいります。

サイバーセキュリティ体制

野村グループでは、グループ危機管理委員会の事務局のもとに野村グループCSIRT（Computer Security Incident Response Team）を設置し、サイバー攻撃により発生した事象への対応、および被害を軽減させるためのグローバルな体制を構築しています。
このほか、野村證券および野村グループ各社にもCSIRTを設置し、各社の業務・情報資産・システムを守る体制を構築しております。

野村グループCSIRT体制について

・野村ホールディングス グループ・IT統括部長を代表とする
・構成メンバーはグループ各社のCSIRT代表とし、事務局を野村ホールディングス グループ・IT統括部（危機管理課）に設置する



組織運営	「平時」は、サイバー演習への参加、「脅威ベースペネトレーションテスト」の実施、リスク評価、子会社や外部委託先の対策状況の把握などにより態勢の継続的な強化に努めています。また、危険な脆弱性情報の入手や、サイバー攻撃の検知といった「有事」には、CSIRTを中心に原因分析、被害の最小化、早期復旧のための対応を実施します。
システム対応	不正アクセスや、コンピューターウイルスなどの不正プログラムに対する検知・防御の仕組みを複数導入するなど、多段階の対策（多層防御）を行っています。また、新しい脅威の発生に対して適時これらの対策の見直しを行っています。
人的対応	役職員のサイバーセキュリティの知見向上のため「野村グループ情報セキュリティ基本方針」に基づき全役職員に対して研修・訓練・注意喚起を定常的に実施しています。
外部連携	金融ISACやFS-ISAC等の情報共有機関やサイバーセキュリティ専業ベンダーとのコミュニケーションを通じて、攻撃者や攻撃方法に関する情報の収集・共有体制を構築しています。