Business Continuity Management
業務継続態勢

野村グループでは、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、社内の啓発活動も含めてさまざまな準備・対策に取り組んでいます。
これらの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、平時より危機管理態勢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。

業務継続に係る主な取り組み

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

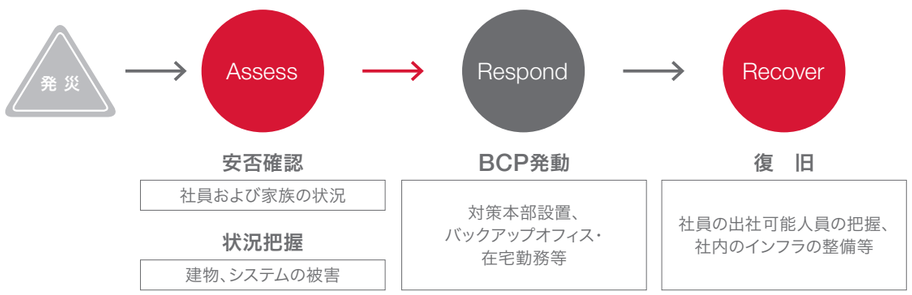
2
訓練・研修の継続的な実施
社員の安否確認訓練／
業務継続計画（Business Continuity Plan, BCP）に沿った業務訓練／
首都直下地震等の大規模地震発生時を想定した初動対応研修・訓練／南海トラフ地震研修

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

平時における業務継続のPDCAサイクル

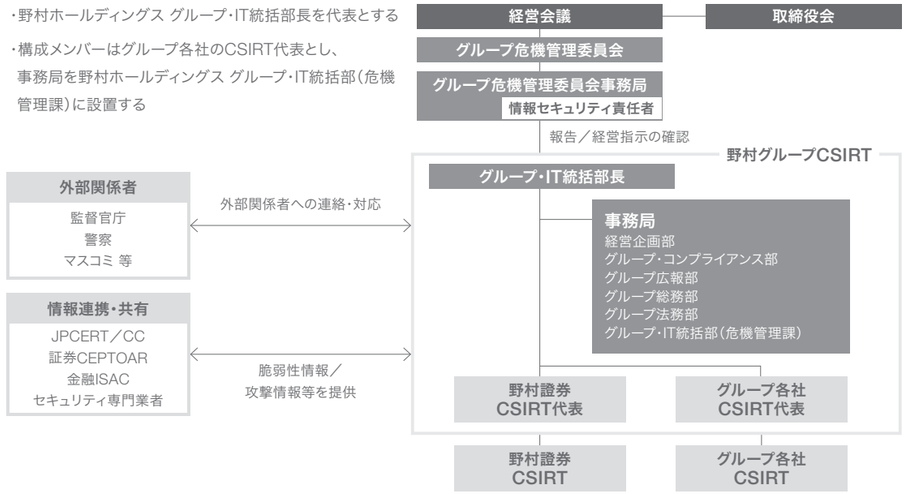
有事における対応の流れ



Cybersecurity
サイバーセキュリティ

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IT担当役員のリーダーシップの下、サイバーセキュリティ対策の継続的な強化を行っています。
対策にあたっては、金融庁が制定している金融商品取引業者等向けの総合的な監督指針や、米国国立標準技術研究所（NIST）の「Cybersecurity Framework」その他海外のフレームワークを参考にし、グループ・グローバルワイドでの包括的な取組みを進めています。
サイバーセキュリティ体制として、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います。

野村グループCSIRT体制について



サイバー対策

NIST Cybersecurity Frameworkの定める5つの機能分類ごとに次のようなサイバー対策を推進しています。

識別 Identify
- 経営ビジョンやリスクアペタイトを踏まえ、守るべき情報資産を明らかにし、グループ全体のガバナンス体制を整備しています。
- 脅威ベースペネトレーションテスト、第三者リスク評価などにより態勢の継続的な強化に努めています。
- 外部の委託先を含めたサイバーリスクの評価および対策を行っています。

防御 Protect
- 不正アクセスやコンピューターウイルスなどから防御するシステム的な対策を複数導入しています。
- 役職員の知見向上のための研修・訓練・注意喚起を定常的に実施しています。
- 金融ISAC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。

検知 Detect
- 異常をタイムリーに検知するため、24時間365日の監視体制を整備しています。
- システムのログを収集・分析し、内部不正を含めた異常を検知する態勢を構築しています。

対応 Respond
- サイバーのインシデント発生に備え、お客様や関係機関、経営層に迅速に連絡する体制を整備しています。
- インシデント対応マニュアルを整備し、CSIRTを中心に原因分析、被害の最小化などの対応を実施しています。

復旧 Recover
- 業務継続計画やバックアップデータセンターを整備しています。
- システムの切り替え訓練、サイバー演習を通じて、業務・システムの速やかな復旧に備えています。