CYBER SECURITY

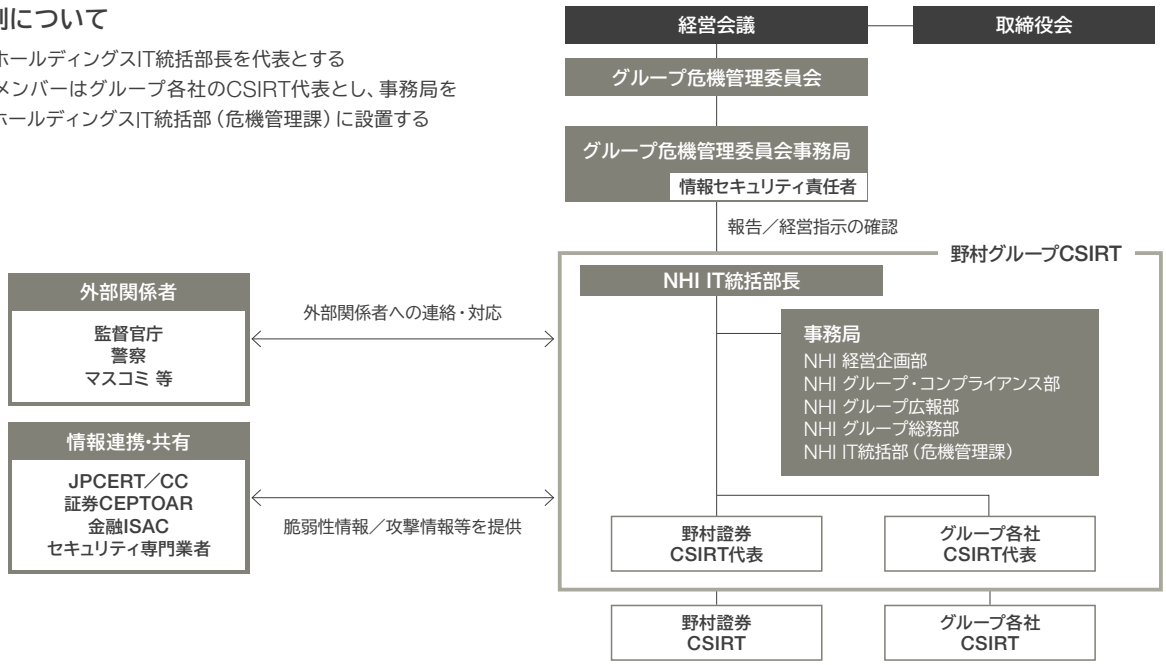
野村グループはサイバー攻撃に対してこれまでも一定の対策を講じていますが、サイバー上の脅威は日々深刻化しており、現在の対策が不十分となる可能性があります。また、金融分野のデジタライゼーションの動きが加速度的に進展しており、金融に関わるあらゆるシステムがネットワークにつながることで、サイバーセキュリティに関わるリスクがより一層高まっていくおそれがあります。当グループでは、これら深刻化するサイバーセキュリティに対する脅威からお客様の情報、お客様の資産を守り、安心してお取引を行っていただくため、金融庁が制定している金融商品取引業者向けの監督指針や、ISO27001および27002を参照している経済産業省のサイバーセキュリティ経営ガイドラインを参考に、包括的なサイバーセキュリティ対策の強化に努めています。

サイバーセキュリティ体制

野村グループ全体で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。野村ホールディングスに設置した野村グループCSIRT（Computer Security Incident Response Team）を中心に、野村證券および野村グループ各社にもCSIRTを設置。野村グループCSIRTは野村グループ各社のCSIRT等のガバナンスを行い、各社のCSIRTは各社の業務・情報資産・システムを守る機能を果たしており、組織運営、システム対応、人的対応、外部連携の4つの軸でサイバーセキュリティ対策を推進しています。

■体制について

・野村ホールディングス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、海外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」にもと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	野村グループでは金融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。