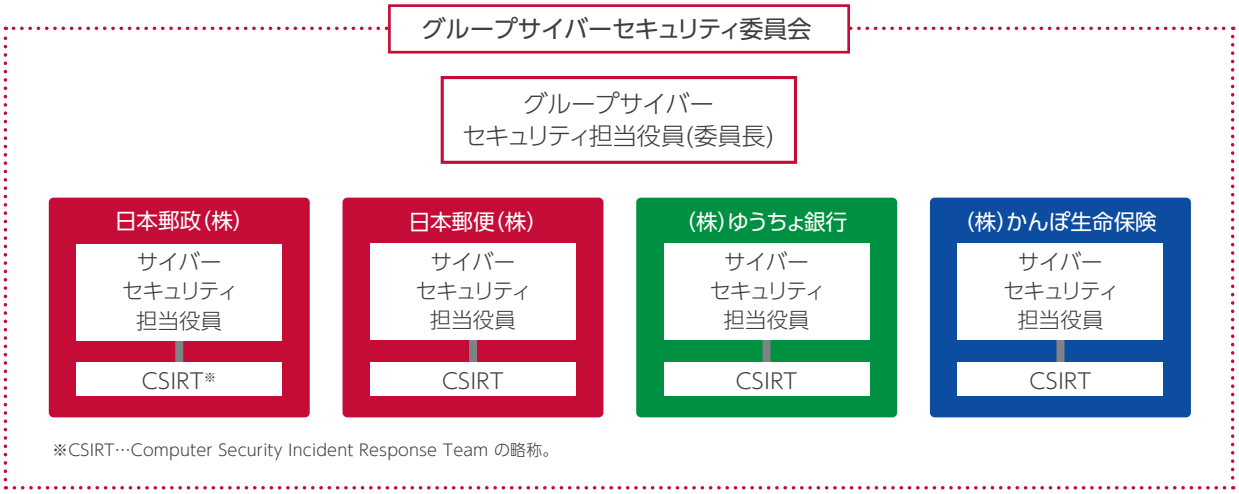
日本郵政グループのサイバーセキュリティ対策

サイバー攻撃が日々高度化・巧妙化していることに鑑み、日本郵政グループではサイバー攻撃の脅威を重大なリスクとして捉え、リスクに対応できる態勢を整備しています。
サイバー攻撃等に起因する情報の流出・紛失などの被害から、重要な情報を守り、安全に管理することに取り組んでいます。

グループサイバーセキュリティ体制

持株会社である日本郵政(株)のガバナンスの下で、グループのサイバーセキュリティ管理態勢の整備を行っています。
日本郵政グループ主要4社のサイバーセキュリティ担当役員から構成されるグループサイバーセキュリティ委員会を設置し、グループのサイバーセキュリティ戦略策定のほか、グループ各社のサイバーセキュリティ対策の取り組み状況の把握・高度化を行っています。
日本郵政(株)のサイバーセキュリティ担当役員が、グループのサイバーセキュリティに関し、グループガバナンスを統括する体制としています。
サイバーセキュリティの取り組み状況について、定期的に経営に報告しています。



※CSIRT…Computer Security Incident Response Team の略称。

日本郵政のサイバーセキュリティ対策の取り組み

多層防御	社外からのマルウェア攻撃や内部からの不正な情報持ち出しのリスクを低減するため、不正アクセスや不正プログラムに対する検知・防御の仕組みを複数導入し、多段階の対策(多層防御)を行っています。 防御の有効性について、第三者による評価を定期的に行っています。
インシデント対応体制	CSIRTを中心とした対応体制を整備しており、サイバー攻撃などが発生した時に原因の把握を迅速に行い、被害を最小化すると同時に、経営に対し迅速に報告します。 平時よりセキュリティ・インシデントを想定した対応訓練を実施しており、インシデント対応体制が有効に機能するか点検するとともに、CSIRT要員ほか社員のインシデント対応能力向上に努めています。
教育・訓練	役員・社員を対象にサイバーセキュリティに関する教育・訓練を行っており、役員・社員のセキュリティ意識向上に努めています。
外部連携	JPCERT/CC、日本CSIRT協議会、警視庁等の外部組織と連携して攻撃情報や対策動向の共有等を行っており、日々高度化するサイバー攻撃に迅速に対応できるよう努めています。