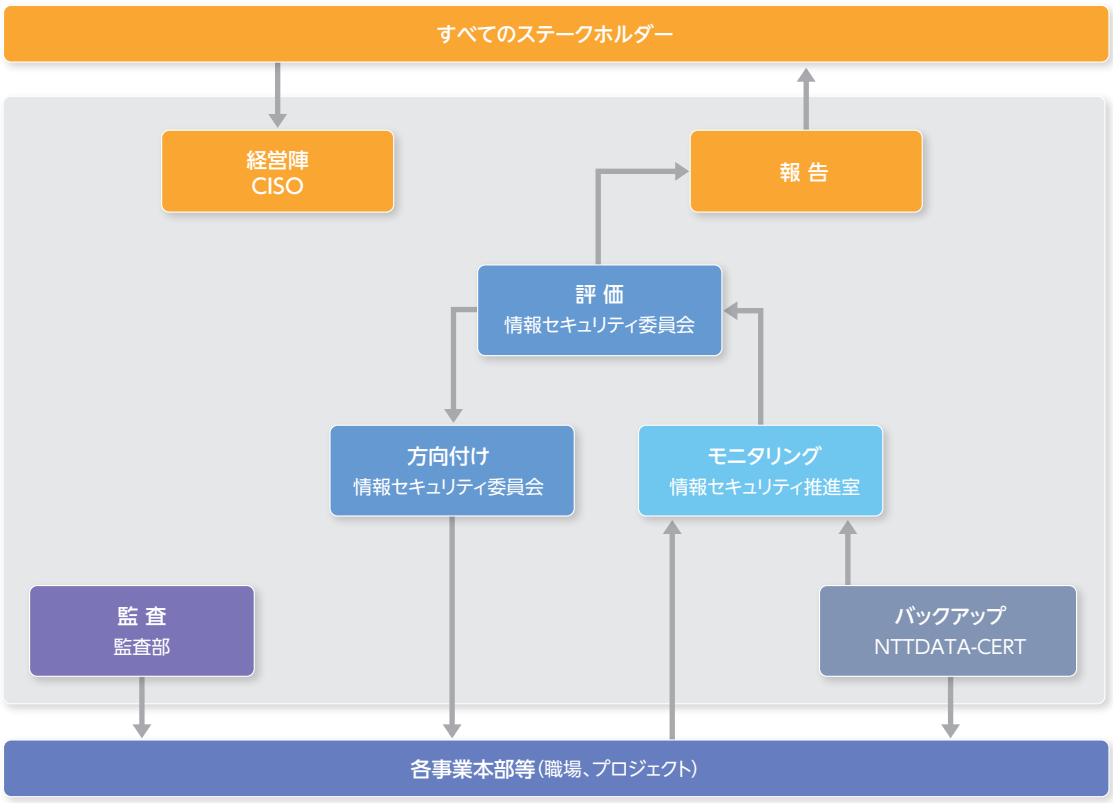
情報セキュリティマネジメント体制

NTTデータグループは情報セキュリティリスクに対応するため、情報セキュリティマネジメント体制を構築し、情報セキュリティガバナンスを確立しています。

各組織が情報セキュリティに対しそれぞれ役割を担っており、職場やプロジェクトを運営する各事業部に対して方向付け・実施状況をモニタリングし、さらにその結果を評価します。監査や緊急対応といったバックアップも実施しています。

また、各組織が実施した結果や状況については適時・適切な情報開示に努めています。お客様、株主・投資家の皆様、お取引先の皆様、社員・家族の方といった様々な人々をステークホルダーとして認識しており、株主・投資家の皆様にはIR部門が、お客様には営業部門を中心とした社員が対応し、よき企業市民としての社会的責任を果たしています。なお、情報セキュリティの確立への取り組みが社会的責任の1つと考え、2008年にシステムインテグレーターとして初となる情報セキュリティ報告書を作成・公開しています。



1 情報セキュリティ委員会［評価］［方向付け］

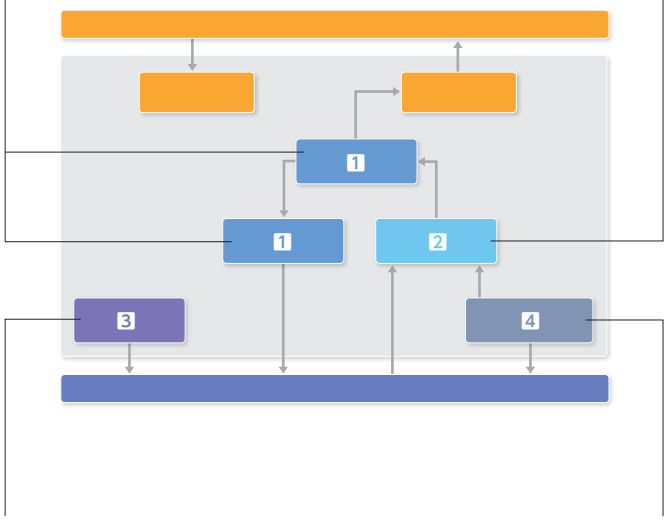
情報セキュリティリスクの低減、安全な情報活用・共有の推進を目的として、NTTデータグループの情報セキュリティ戦略を定めています。

また、情報セキュリティ戦略に基づいた当該年度の情報セキュリティ推進活動を、個別施策のモニタリング情報、内部監査の結果などから総合的に評価します。評価結果をもとに各個別施策を見直し、次の情報セキュリティ戦略の立案につなげています。

代表取締役副社長執行役員・CISO（セキュリティ戦略担当役員）を委員長とし、各事業部門のトップをメンバーとした「情報セキュリティ委員会」を定期的に開催しています（2015年12月まで累計65回開催）。

2 情報セキュリティ推進室［モニタリング］

NTTデータグループの情報セキュリティ推進活動を担う専門組織として設置。情報セキュリティ戦略に基づく個別の情報セキュリティ施策を実行するとともに、実施状況をモニタリングしています。



3 監査部［監査］

NTTデータでは、監査部において情報セキュリティに関する内部監査を実施しています。業務執行から独立した立場で各事業本部などに対し行います。監査結果は、情報セキュリティ推進室と共有し、必要に応じて制度や施策の改善・見直しにつなげます。

4 NTTDATA-CERT［バックアップ］

NTTデータグループのセキュリティインシデント対応専門チーム「CSIRT」※を、情報セキュリティ推進室に設置しています。セキュリティ事故防止のための情報収集・分析、対策実施を行い、万が一のセキュリティ事故発生時に緊急対応します。

※ CSIRT（Computer Security Incident Response Team）とは、セキュリティ専門家から構成されるインシデント対応を行うための組織です。セキュリティインシデント、セキュリティ関連技術、脆弱性などの情報を収集・分析し、有効な対策や訓練の実施などの活動を行います