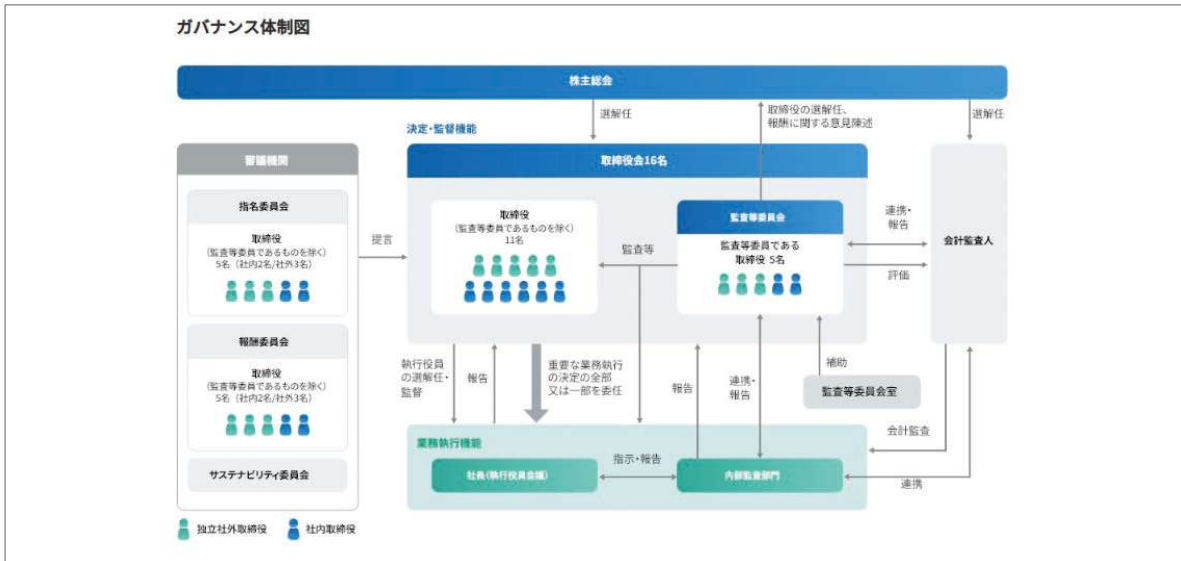


図表4-7-2 ▶ ガバナンス体制図



出所：NTT「コーポレート・ガバナンス」

図表4-7-3 ▶ パーソナルデータダッシュボード



出所：NTTドコモ「パーソナルデータダッシュボード」

憲章」を2018年に制定し、2019年に公表した。同憲章の目的は、最適なプライバシー保護を実現し、顧客が安心してドコモのサービスを利用できるようにすることである。これと同時に、顧客自身がパーソナルデータの取り扱いについて同意した内容を確認したり、設定・変更したりできる「パーソナルデータダッシュボード」(図表4-7-3)や、憲章の内容を分かりやすくまとめた資料の提供も開始している。

このように規制強化への対応を行ってきたものの、NTTグループでは近年大規模な違反や漏洩事故が相次いだ。

2022年には、GDPR違反でNTT Data Spainがスパイ

ンの情報保護当局から6万4千ユーロの制裁金を課された。直接には顧客の保険会社が個人データを漏洩した事案だが、情報管理システムを提供していたNTT Data Spainも過失を認定された。

2023年には、NTT西日本グループで大規模な情報漏洩が発覚した。これは、NTT西日本がテレマーケティング業務を委託していた株式会社NTTマーケティングアクトProCXにコンタクトセンターシステムを提供していたNTTビジネスソリューションズ株式会社において、同システムの運用保守業務従事者(元派遣社員)が、顧客情報を不正に持ち出していた事案である。2013～2023年までの間に持ち出された情報は計928万件に上った。同事案により、NTT西日本は総務省から行政指導を受けた。また、株式会社NTTマーケティングアクトProCXとNTTビジネスソリューションズ株式会社は個人情報保護委員会から勧告・指導を受けた。

このインシデントは、NTTグループ全体にとって深刻な問題となり、全社的なセキュリティ強化の必要性が改めて浮き彫りとなった。これを受け、NTTは緊急対応を実施し、内部統制の見直しを加速させることになった。横浜信一NTTグループCISOは当時の記者会見で、「今後は性善説ではなく、性悪説/性弱説に立って、内部不正に対するリスク管理を強化していく」と説明。具体的な対策として、アカウントや権限管理の厳格化、USBメモリの使用制限、特権アカウントの監視強化など、従業員による不正行為のリスクを最小化する施策を強化するとともに、経営層のリスクマネジメント力、インシデントマネジメント力の強化を目的に国内全社長へのセキュリティ研修を実施した。

また、NTT西日本では、サイバーセキュリティの強化を目的に、直ちに外部専門家と連携し、原因分析と再発防止