# 情報セキュリティガバナンス

## 監査・モニタリング体制

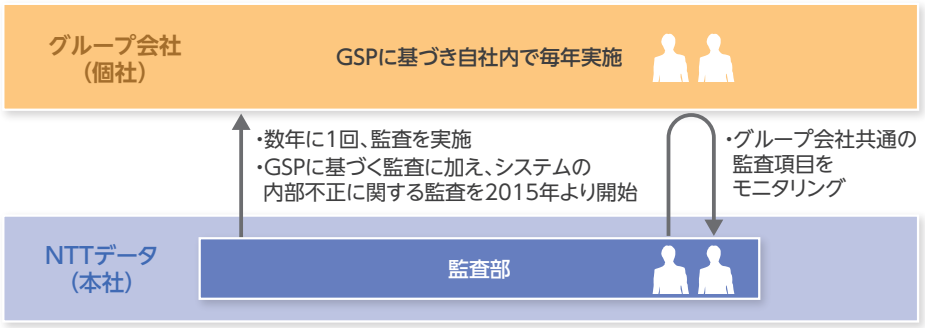
NTTデータグループでは、2006年度からNTTデータグループセキュリティポリシー(GSP)に基づく情報セキュリティを徹底しています。これに対応すべく、国内外のグループ会社を含めた監査・モニタリングの体制を確立しています。

セキュリティ監査については、「基本動作の徹底」「外部からの不正への対応」「内部の不正への対応」という3つの視点で、取り組みを進めてきました。

今後は、基本動作の徹底を図りつつ、より不正行為への対応に注力していきます。

| | |
|---|---|
| 1　基本動作の徹底 | GSPに基づく組織の安全管理状況および個人情報を扱うシステムの安全管理状況を確認しています。 |
| 2　外部からの不正への対応 | 高度化・複雑化するサイバー攻撃に対応するため、グループ会社のシステム的な対策状況を確認しています。 |
| 3　内部の不正への対応 | 内部不正の防止に取り組んでおり、システムの対策状況を確認しています。 |

内部監査体制



# グローバル・ガバナンス

NTTデータグループの海外拠点では、北米、EMEA(欧州・中東・アフリカ)、APAC(アジア・太平洋地域)、中国とソリューションを軸とした事業運営を2012年度から行っています。それに伴い、情報セキュリティについても運用体制の再構築を進めました。

## グローバルセキュリティを支える連携

情報セキュリティのグローバル・ガバナンスを徹底するために、本社、地域統括会社等、個社に配置される情報セキュリティ運営組織の3層からなる情報セキュリティガバナンス体制を整えています。

それぞれの層に置かれる情報セキュリティ運営組織は緊密に連携し、情報セキュリティポリシーの維持・整備、情報セキュリティ施策のモニタリング、緊急時の対応、インシデント防止のための予防措置活動の役割を担っています。

## インシデント対応ワークショップの実施

グローバル・ガバナンス強化に向けて、2015年度、特に注力しているのが、インシデント発生時の初動対応を現場で適切に行えるようにすることです。その実現のためワークショップを行っています。

国内グループ会社と海外グループ会社を対象に、世界各地で初動対応ガイドラインをベースにした訓練を実施。インシデント対応における初動対応の目的と、各スタッフそれぞれがやらなければならないことを理解するとともに、NTTデータグループで発生しているインシデント事例を通して、昨今のサイバー攻撃者の狙いと手口への知識を深めることに貢献しています。

情報セキュリティガバナンス体制