リスクマネジメントの強化

情報通信サービスを支える企業として、事業を取り巻くリスクを特定し、
ビジネスリスクに対する危機管理体制の充実を図っていきます。

ビジネスリスクを特定し、影響の最小化を図る

自然災害や通信テロ、企業情報漏えいなど、事業活動に重大な影響を及ぼすリスクへの対応をはじめ、法令の遵守、社内の情報セキュリティ等、NTT西日本グループを取り巻くさまざまなビジネスリスクについて発生を予防する施策を講じています。また、万一問題が発生した場合は、迅速かつ的確に対処する体制を整えることにより、リスクに対する影響の最小化を図るなど再発防止に努めています。

リスクマネジメント体制を強化

事業運営に影響を及ぼすビジネスリスクを適切に管理する必要から、NTT西日本本社総務部長を委員長とし、関係会社および各部の部長クラスをメンバー、総務部渉外担当を事務局とする「ビジネスリスクマネジメント連絡会」を設置しました。

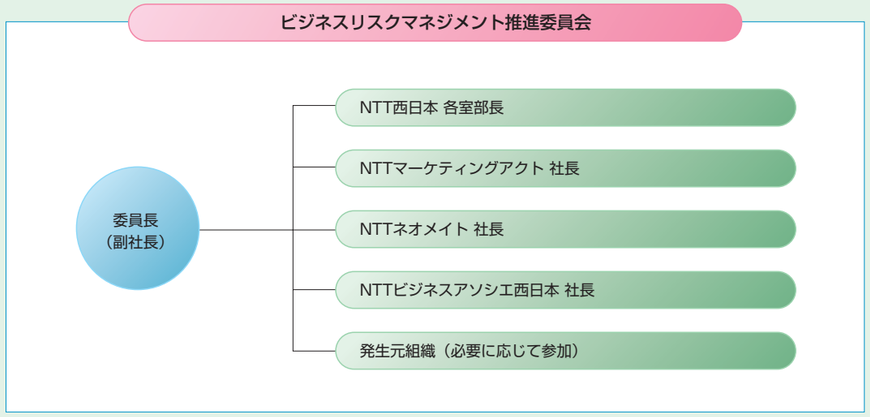
そして、2006年7月からは、同連絡会を「ビジネスリスクマネジメント推進委員会」と改め、代表取締役副社長を委員長とする組織に体制を強化しました。

予期せぬ障害や自然災害に備え、さまざまな対策を実施

予期せぬ障害や自然災害が発生した場合に通信ネットワークを確保することは、情報通信サービスを提供する企業として最も重要な役割であると認識し、さまざまな対策を実施しています。
自然災害等が発生した場合に備えて、ネットワーク機能の冗長化や設備の耐震性向上、監視・制御体制を強化するなど、ネットワークの信頼性向上に取り組んでいます。

また、自然災害等により通信ネットワークが被災した場合には、被災状況の把握、復旧体制の構築を迅速に行い、重要通信の確保、通信サービスの早期復旧に努めています。

● ビジネスリスクマネジメント推進委員会



情報セキュリティの推進体制を構築

NTT西日本グループでは、情報通信サービスという公共性の高い事業に携わる企業として、すべてのお客様に安心していただけるように、情報セキュリティ体制を構築し、各種取り組みを推進しています。

これまでは、経営会議のもとに「情報セキュリティ推進委員会」を設置し、情報セキュリティ対策の立案・策定を推進してきました。しかし、グループ横断的にお客様情報の保護とネットワークセキュリティの向上を実現するため、これまで各社・業務ごとの縦割り組織であった情報セキュリティにかかわるすべての組織を一つにまとめた「情報セキュリティ推進本部」を設置し、グループ全体の情報セキュリティレベルの向上に向けた取り組みを推進しています。

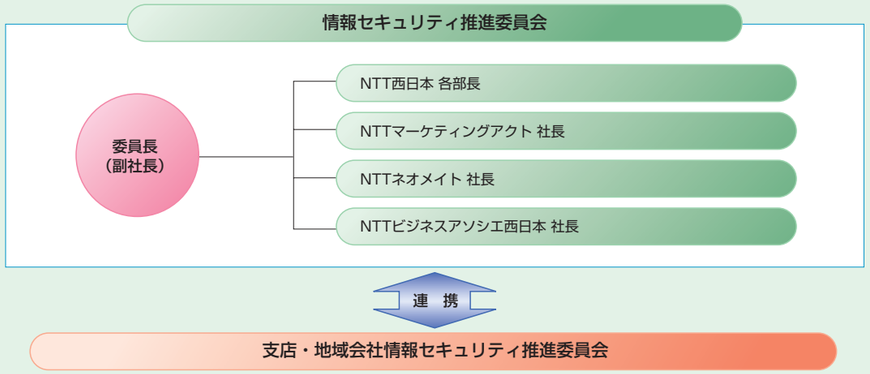
また、お客様情報管理体制を強化するため、本社、各支店、各関係会社において「情報管理責任者」、「お客様情報適正利用監督者」、「お客様情報適正利用推進者」を定め、管理責任範囲と役割を明確化しました。

NTTグループ情報セキュリティポリシー

NTTグループでは、グループ全体としての情報セキュリティ管理体制の強化を図る観点から、2005年4月に「NTTグループ情報セキュリティポリシー」を策定しました。

1. **ブロードバンド・ユビキタス社会における情報セキュリティの重要性を深く認識し、安心・安全で便利なコミュニケーションネットワーク環境の構築に努め、情報セキュリティの確保に取り組んでまいります。**
2. **情報を保護することは、NTTグループの事業活動の基本であり、企業としての重要な社会的責任であることをNTTグループ会社の役員・従業員が十分に認識し、通信の秘密の厳守はもとより個人情報保護法等の関連法令等を遵守してまいります。**
3. **情報セキュリティの管理体制を整備し、情報への不正なアクセス、情報の紛失・改ざん・漏洩の防止等に向けた物理面、システム面での厳格なセキュリティ対策の実施、社員教育の徹底、委託先への適切な監督等、情報の保護に向けた必要な取り組みを継続的に実施してまいります。**

● 情報セキュリティ推進委員会



情報セキュリティのマネジメントシステムを構築

社内のセキュリティレベル向上をめざし、情報セキュリティシステムの英国標準規格であるBS7799および国内標準規格ISMS適合性評価制度を情報セキュリティ管理担当部署（ソリューション営業本部、各支店、グループ会社）で認証取得しました。

なお、現在認証を取得しているBS7799とISMS適合性評価制度は、順次ISO27001へ移行しています。

システムセキュリティの強化

お客様情報保護に向けたシステム面でのセキュリティを高めるため、4つの対策を行いました。まず、2005年4月～5月に、お客様情報を保有するすべてのシステムについて、122項目の総点検を実施し、必要な場合にはシステムの改善を実施しました。また、お客様情報を保有するシステムへ指紋認証機能を導入したほか、社外へメールを送信する際は、管理者をCCに入れなければ送信できないようにしていく予定です。

さらに、NTT西日本独自の取り組みとして、「使用可能端末を限定できる指紋認証機能付きUSBフラッシュメモリ」を導入し、USBメモリからの個人情報漏えい等への対策を進めました。

お客様情報の管理体制を強化

お客様情報を管理するシステムにアクセスできる社員を最小限に限定し、さらに担当者ごとにアクセス可能な情報を制限しました。また、入退室管理や記録媒体管理について定めた「お客様情報保護運用マニュアル」と個人情報の取り扱いについて定めた「利用目的の公表および情報開示等運用マニュアル」を整備したほか、点検シートに基づいた自主点検を職場の管理者等が毎日実施しています。

さらに、日常の運用管理状況や社員へのアクセス権限の付与状況等について四半期ごとの点検を行うほか、毎年5月を「お客様情報保護強化月間」として、他部門の管理者によるクロス点検を実施しています。

個人情報保護に関する社員への研修

NTT西日本グループでは、経営トップから派遣社員までの全社員等を対象に個人情報保護に関する研修を実施しています。使用する教材には、個人情報保護法についてのビデオのほか、ケーススタディで学べる「ワンポイントアドバイスブック」やトラブル事例シート等があります。また、全社員を対象とした研修では社員一人ひとりが発生原因や再発防止策について考え、グループディスカッションを通して、知識や考え方の共有化を図ることにより、参加者全員の意識の向上を図っています。研修受講後には、Webを用いた自己診断テストによる理解度テストを行い、確実な理解度の向上をめざしています。2005年度は理解度チェックを2回実施しました。

業務委託会社における個人情報保護への取り組み

NTT西日本グループではこれまで独自の「情報セキュリティマネジメント規程」に基づき情報セキュリティを推進してきましたが、これに加えて、業務委託先でもNTT西日本グループと同様のお客様情報管理が徹底されるように、「委託会社におけるお客様情報保護に関するセキュリティガイドライン」を新たに制定し、遵守を義務付けました。

また、人材派遣会社における個人情報管理体制の強化をめざして、人材派遣の基本契約についてはNTT西日本本社で一括して行い、一定の基準を満たしている会社のみと契約することにしました。さらに、年1回、人材派遣会社の派遣元責任者を集めて個人情報保護に関する研修を行い、人材派遣会社の研修テキストにも内容を盛り込むように要請しています。

お客様情報流出に関して

2006年3月、NTT西日本の社員の自宅にある個人用パソコンがウィルスに感染し、パソコン内に保管されていたNTT西日本およびNTT東日本（以下、NTT東西）のお客様情報を含む業務関連ファイルが、ファイル交換ソフト「Winny」のネットワーク上に流出していたことが判明しました。

1. 流出した情報および件数

お客様情報　237ユーザ
- NTT西日本　124ユーザ（内訳、個人：106ユーザ、法人：18ユーザ）
- NTT東日本　113ユーザ（内訳、個人：58ユーザ、法人：55ユーザ）

2. お客様への対応

当該のお客様へは、早急にお詫び文をお送りするなど、個別にご説明させていただき、お詫びをさせていただきました。

3. 再発防止策

NTT東西では、従来より業務関連情報等の社外への持ち出しを禁止しているところですが、本件を厳粛に受け止め、全社員に対し、再度「業務関連情報の自宅等社外への持ち出し禁止」を周知徹底するとともに、自宅パソコン等に業務関連情報を保存していないか全社員への一斉点検を実施し、「自宅パソコンに業務関連情報が入っている場合は消去する」等、情報管理のさらなる強化を図り、お客様の信頼回復に全力をあげて努めてまいります。

4. その他

流出した業務関連ファイルには、お客様情報のほかに、NTTグループの社員情報等が含まれておりました。社員情報については、2,456名の個人情報（氏名、所属組織、電話番号、役職、メールアドレス等）が含まれていました。