NTT DATA
変える力を、ともに生み出す。

2012
情報セキュリティ報告書

株式会社NTTデータ

Corporate Philosophy

企業理念

（NTTデータグループの使命）

NTTデータグループは、情報技術で、
新しい「しくみ」や「価値」を創造し、
より豊かで調和のとれた
社会の実現に貢献する。

報告対象情報・期間

・本報告書は、NTTデータグループ会社が扱うすべての情報を対象としています。
・本報告書は、特に記載がない限り、2011年12月末までの情報セキュリティに関する取り組みを対象としています。

報告対象範囲

NTTデータグループ会社（223社、株式会社NTTデータを含む）
※2011年12月31日現在

責任部署

株式会社NTTデータ
品質保証部 情報セキュリティ推進室

お問い合わせ先

株式会社NTTデータ
品質保証部 情報セキュリティ推進室
〒135-6033 東京都江東区豊洲3-3-3
豊洲センタービル
TEL:050-5546-2545
URL:http://www.nttdata.co.jp/

CONTENTS

Message from the CISO 豊かで、持続可能な社会のために …… 3
NTTデータグループの情報セキュリティ取組方針 …… 4
NTTデータの情報セキュリティマネジメント体制 …… 6
情報セキュリティ報告書2010で報告した内容の振り返り …… 8
NTTデータの情報セキュリティ戦略 …… 9
情報セキュリティ推進施策の実践 …… 10
監査・モニタリング …… 11
情報セキュリティ施策の展開事例：1 …… 12
情報セキュリティ施策の展開事例：2 …… 14
情報セキュリティ施策の展開事例：3 …… 16
社会状況に応じたセキュリティ …… 18
情報セキュリティへの理解と意識向上のために …… 20
委託業務における取り組み …… 22
第三者評価・認証 …… 23
情報セキュリティ活動年表 …… 24
会社概要 …… 26
企業グループにおける情報セキュリティの実践 …… 27

Message from the CISO

豊かで、持続可能な社会のために

社会の変革を支えるための ITと情報セキュリティ

2011年は、大きな変化がもたらされた年となりました。

3月の東日本大震災では事業継続計画（BCP）の実運用を余儀なくされ、その後の電力総量規制に伴い節電対策を実施しました。また、他企業でのハッカー集団からの攻撃による大規模な顧客情報の流出や、主要省庁・重要企業への標的型攻撃による情報流出も続々と発覚し、情報セキュリティ対策がより注目された年になりました。

また、スマートフォンやタブレット端末といったデバイスや、クラウドサービスの利用が急速に進み、ビジネスシーンでも活用されています。TwitterやFacebookといったソーシャルネットワーキングサービス（SNS）による情報発信も企業活動に活用されています。

このようにITサービス業界だけでなく世の中全体が大きな環境の変化や技術の進歩にさらされており、各企業では様々な対策が必要となっています。

NTTデータグループは、社会インフラを担う大規模システムやお客様の戦略上の重要なシステムを数多く手掛けておりますが、これはお客様が当社を信頼してくださっているからこそできることと強く認識しております。この信頼を失うことの無い様、NTTデータグループ全体で、情報セキュリティ事故の発生を未然に防ぐための様々な対策に着実に取り組んでおります。

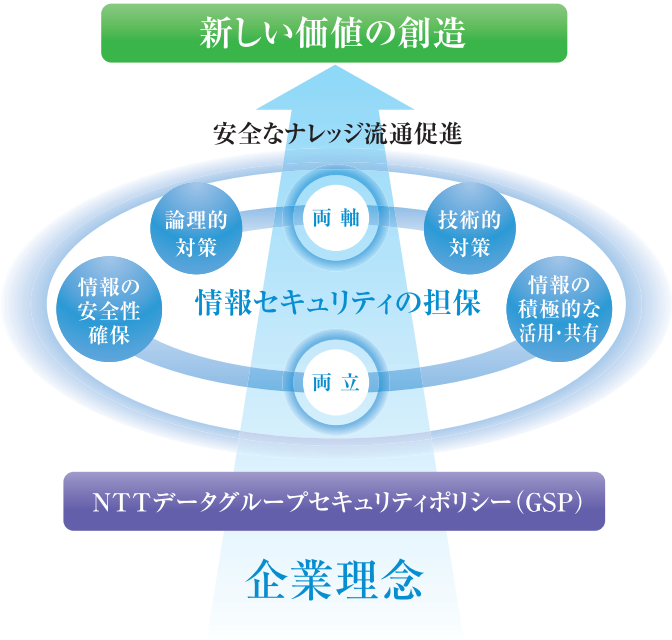
私たちNTTデータグループは、NTTデータグループ全体で共通の「グループセキュリティポリシー」を制定し、情報セキュリティのあるべき姿として「情報を安全に守る」ことと「情報を活用する」ことの両立を掲げ、技術的・論理的対策の両輪を持って実践してきました。そして、2008年、システムインテグレータとして初めて情報セキュリティ報告書を作成・公開しました。

第3号となる本書では、変化し続ける情報社会に対応した情報セキュリティ推進活動について、具体的に紹介いたします。本書を手に取られたすべてのステークホルダーの皆さまに、何かひとつでもお役に立てば幸いと存じます。

株式会社NTTデータ
代表取締役副社長執行役員 CISO
岩本 敏男

NTTデータグループの情報セキュリティ取組方針

NTTデータグループは、「情報の安全性確保」と「情報の積極的な活用・共有」を適正なバランスで両立させることにより、グループ全体で安全なナレッジ流通を促進し、お客様に新たな「価値」を提供します。
「情報の安全性確保」と「情報の積極的な活用・共有」を両立させるためには、ルールの策定や情報セキュリティ教育・啓発活動などの「論理的対策」と、情報漏えい対策ソリューションやシンクライアントPCの導入といった「技術的対策」の両軸が必要と考えています。

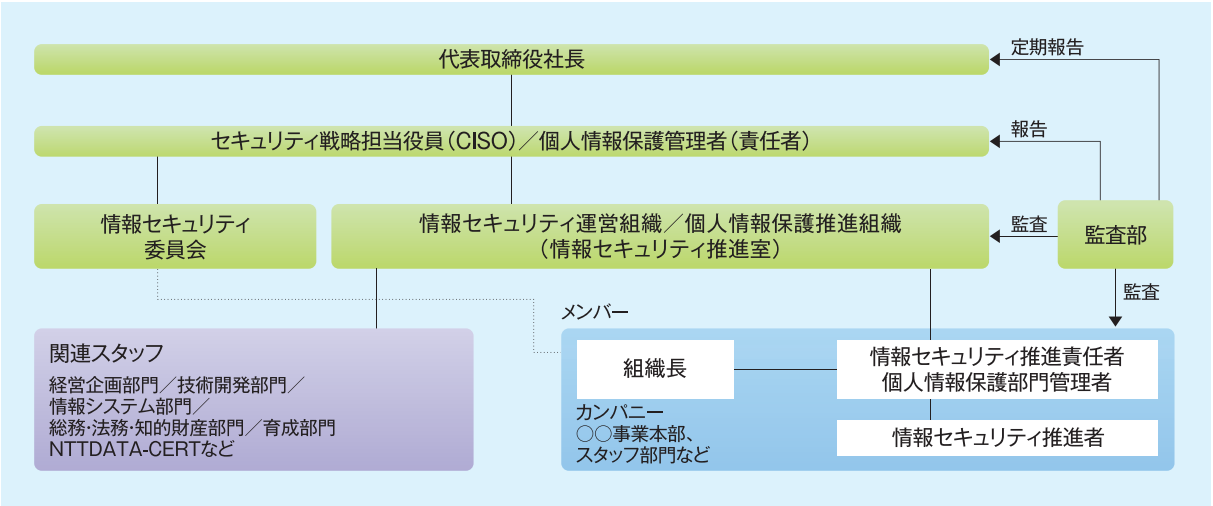


情報セキュリティポリシー、個人情報保護方針の策定

NTTデータでは、セキュリティ侵害などによる情報漏えいや情報の不正利用が、深刻な信用問題につながることをふまえ、早期から情報セキュリティマネジメントに対する取り組みに着手してきました。具体的には、情報資産を適切に取り扱い、情報セキュリティを確保することを目的とした「情報セキュリティポリシー」を1998年12月に制定しました。

また、個人情報保護の重要性を認識し、個人情報保護活動を企業における基盤的活動として位置付けています。
「個人情報保護方針」を2001年7月に制定するとともに、個人情報を適切に取り扱うための遵守事項を定めた社内規則を制定しています。個人情報保護方針や社内規則は、情報技術の進歩や社会の変化に応じて、見直しや改善を実施しています。

■NTTデータの情報セキュリティ・個人情報保護活動体制



グループトータルでの情報セキュリティ

グループ･グローバル経営を推進するためには、基盤となる経営方針やルールを海外も含めて統一することが重要です。これは、情報セキュリティについても同様です。

NTTデータグループでは、グループ統一の情報セキュリティ･ルール「NTTデータグループセキュリティポリシー（GSP）」を2008年4月に制定しました。グループ各社は、各社の企業規模やビジネスの内容を踏まえて、GSPに準拠した情報セキュリティポリシーを制定しています。GSPでは、情報の取り扱いに関するルールも規定しています。これにより、NTTデータグループ全体で、安全に情報を流通することが可能となっています。

また、電子情報を安全かつ効率的にグループ内で共有するための情報流通インフラとして、グループワイドネットワーク（GWNet）、ファイル転送システム（ETRANPOT）、文書管理システム(Docφ)といった各種システムを構築･運用しています。これらに加え、グループ全社員のナレッジの共有を目的とした技術情報格納サイト（ソリューションウェアハウス®、TeSS）により、安全な情報の活用･共有を推進し、グループ全体の競争力強化につなげています。

■情報流通インフラの例

GWNet

NTTデータグループ各社をつなぐネットワークインフラで、
情報共有サービスは全てGWNet上で展開される。

Group EGG

NTTデータグループのイントラネットポータルサイト。グループ社員への周知事項、ニュースリリースなどを掲示している。

ETRANPOT

NTTデータ・NTTデータグループ会社と関連するお客様の間で、セキュアにファイルを転送するシステム。
一定期日以上の保管はできない。

Docφ

NTTデータ・NTTデータグループ会社及びNTTデータの業務委託会社間における、ファイル共有システム。アクセス権の設定やバージョン管理が可能。

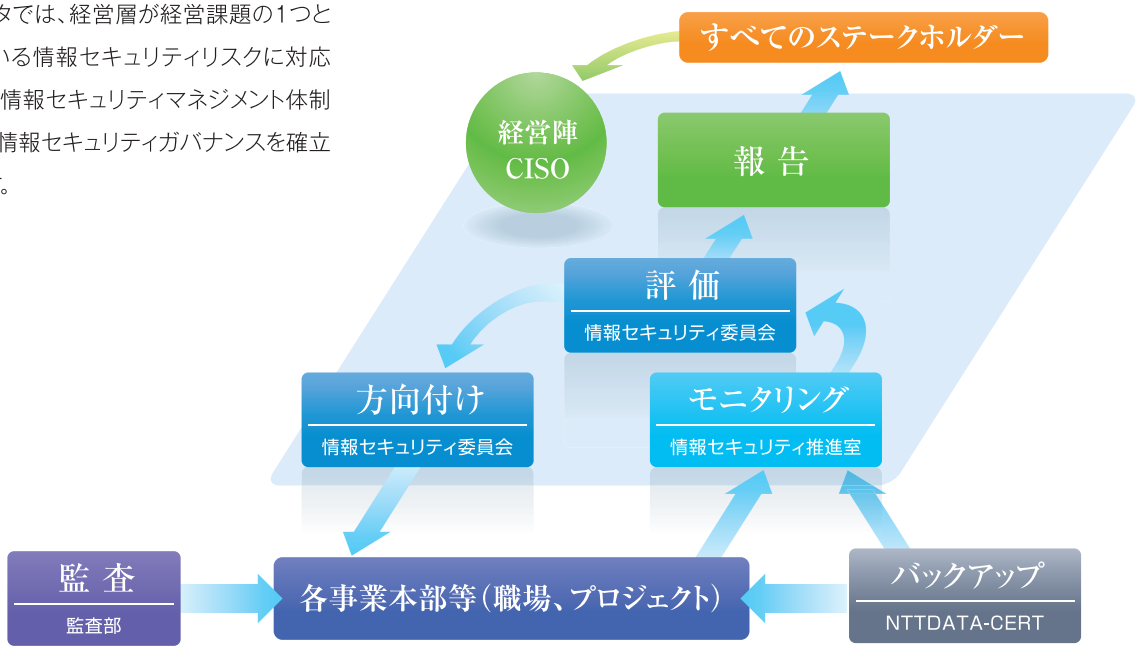
ソリューションウェアハウス® ／TeSS

ソリューションウェアハウス®：NTTデータグループ内の技術情報DB。
TeSS ： 技術問合せ窓口及びそのDB。
グループ内でノウハウを共有し、活用している。

NTTデータの情報セキュリティマネジメント体制

情報セキュリティガバナンスの確立

NTTデータでは、経営層が経営課題の1つと認識している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。



方向付け　情報セキュリティ委員会

代表取締役副社長・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（2011年12月まで累計54回開催）。

情報セキュリティ委員会では、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。

モニタリング　情報セキュリティ推進室

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されています。
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、各情報セキュリティ施策の実施状況をモニタリングしています。

評価 情報セキュリティ委員会

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、各個別施策を見直すとともに次の情報セキュリティ戦略の立案につなげています。

監査 監査部

NTTデータでは、情報セキュリティに関する内部監査を監査部が実施しています。
業務執行から独立した立場で各事業本部等に対し、情報セキュリティ監査を実施しています。

監査結果は、情報セキュリティ推進室にも報告され、必要に応じて制度や施策の改善・見直しにつなげています。

報告

NTTデータグループは、お客様、株主・投資家の皆様、お取引先の皆様、社員・家族の方々などさまざまな人々をステークホルダーとして認識しており、よき企業市民としての社会的責任を果たすため適時・適切な情報の開示に努めています。
株主・投資家の皆様にはIR部門、マスコミュニケーションを通じた一般の方々や社員・家族の方々には広報部門、お客様には営業部門を中心とした社員が、誠意を持って対応しています。
また、NTTデータグループは、率先して「情報セキュリティの確立」に取り組むことが社会的責任の1つだと考えており、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し、すべてのステークホルダーの方々に対して公開しています。

バックアップ NTTDATA-CERT

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：注）として、研究開発部門に設置されています。

セキュリティ事故防止のための情報収集・分析、対策実施を行っており、万が一セキュリティ事故が発生した際は緊急対応を行います。

注: 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、脆弱性等の情報を収集・分析し、有効な対策や訓練の実施等の活動を行います。

情報セキュリティ報告書2010で報告した内容の振り返り

ステークホルダーの皆様に対するご報告

NTTデータは、2008年にシステムインテグレーターとして国内初となる情報セキュリティ報告書を発行しました。本報告書が3回目の発行となります。

情報セキュリティ報告書2010にてステークホルダーの皆様にNTTデータがご提示した情報セキュリティ戦略に対する取り組みについての実施結果を報告します。

情報セキュリティ報告書で約束した取り組み

前回の情報セキュリティ報告書にて記載した情報セキュリティ戦略に対する取り組みについては、すべて達成しました。

■3つの情報セキュリティ戦略と実施結果

情報セキュリティ戦略	実施結果
1つ目 グローバル化・グループ拡大に対応した情報セキュリティ推進活動の実践	グループ全体に対するモニタリング体制や教育体系、内部監査体制を確立しました。 グループ共通のセキュリティ教育をマルチリンガル対応(日・英・中)のWebインタフェースで実施し、海外を含む83社・20,536名が受講しました。 また、内部監査体制を強化するために、従来座学研修のみで実施していたGSP内部監査人研修を自席オフライン研修・マルチリンガル対応(日・英・中)による受講も可能とし、新たに海外を含む66社・219名の内部監査人を育成しました。 さらに、海外のグループ個社に対しては、中国語、タイ語、ベトナム語による集合研修などを実施しました。
2つ目 事故を未然に防ぐ基本行動の徹底と、迅速な事故対応に向けた手順の確立	「セキュリティ基本行動の心得7ヶ条」を制定し、行動チェックポイントをまとめて社内展開しました。 また、万が一情報セキュリティ事故が発生した場合に現場組織が迅速に対応し、お客様および当社への事故による影響を最小限にすることを目的として、「情報セキュリティ事故発生時の初動対応ガイドライン」 を整備しました。 さらに、情報セキュリティ事故発生から状況把握までをストーリー化したNTTグループの事故対応演習に参加しました。
3つ目 情報を扱うプロフェッショナルにふさわしい情報セキュリティマインドの育成	年1回の「情報セキュリティ強化月間」および毎週金曜日の「セキュアフライデー」を実施しました。 強化月間では、情報セキュリティポスターの配布をしました。 また、セキュアフライデーでは、本社ビルを対象に「あいさつ運動」と館内放送を用いて、情報セキュリティを意識した行動を呼びかけました。 さらに、個人情報については、全社員を対象とした個人情報保護IBT(e-ラーニング)や、プロジェクトにおいて個人情報を取得する際の実施事項を理解するための個人情報権利保護研修(座学教育)を実施しました。

NTTデータの情報セキュリティ戦略

NTTデータは、経営方針の達成と情報セキュリティリスクの低減のため、情報セキュリティ戦略を定めます。

情報セキュリティ戦略を元に、具体的な情報セキュリティ施策（アクションプラン）を立案し、実行します。

経営方針と企業経営に関わるリスク

NTTデータは、「変革の先進企業」として「お客様満足度No.1」を追求することを経営方針としています。
具体的には、2009年度に設定した中期経営方針として、次の3つを重点施策としています。

- **サービス提供能力の強化**
- **グループ事業の拡大・強化**
- **環境志向経営の推進**

中期経営方針の下、企業経営に影響を与える重点リスクの1つとして、「情報セキュリティ」に関するリスクを定めています。
特に「情報の流出・漏えいといった情報セキュリティ事故によるさまざまな影響」をリスクと捉えており、情報システムを提供する企業として、情報セキュリティの確保、個人情報保護に注力しています。

NTTデータの情報セキュリティ戦略

お客様のグローバル化に対応するためには、NTTデータグループ自体もグローバル経営を推進するとともに、グループ会社に所属する社員一人ひとりのナレッジを流通させ、グループ全体の英知を活用できる環境が必要です。
お客様の変革パートナーとなるためには、NTTデータグループセキュリティポリシー（GSP）の目的である「情報の安全性確保」と「情報の積極的活用・共有」の両立を実践することが重要です。具体的には、グローバルな規模での安全なナレッジ流通の促進はもちろんのこと、お客様の大切な情報を漏えい・流出することのないよう、情報セキュリティ事故の防止に取り組むことが必須だと考えています。
そのためには、私たちNTTデータグループを構成する一人ひとりが「情報を扱うプロフェッショナル」としての自覚を持ち、常に情報セキュリティを意識した行動をとる必要があります。
NTTデータでは、2011年度は、次の3つを情報セキュリティ戦略として掲げ、具体的な施策として展開しています。

■ 情報セキュリティ戦略（目的）

1. 海外グループ会社の情報セキュリティ推進強化
2. セキュリティ基本行動の徹底
3. 経営に寄与するセキュリティ

情報セキュリティ推進施策の実践

情報セキュリティ戦略に基づいたアクションプラン

NTTデータの情報セキュリティ施策は、情報セキュリティ戦略に基づき立案・実行されています。ここでは、情報セキュリティ戦略の重点テーマ毎に、具体的なアクションプランを紹介します。

海外グループ会社の情報セキュリティ推進強化

経営方針「お客様満足度No.1」を実現するためには、NTTデータグループ全体で安全に情報共有することが必須です。
そのために、国内・海外の全グループ会社はGSPに準拠したセキュリティポリシーを制定し、各種情報セキュリティ施策を実行しています。NTTデータでは、グループ各社に対して、各種施策の支援を実施しています。

■ **情報セキュリティ目標**：2010年度は、新規グループ会社へのポリシー制定・教育・運用支援を目標としました。2011年度は、ルール策定・運用に課題が残る海外グループ会社への支援強化と海外グループ会社に対するモニタリング実施を目標としています。

■ **アクションプラン**：運用支援、教育（リテラシー・GSP・監査人）支援、キャラバンによる課題解決支援など

セキュリティ基本行動の徹底

情報セキュリティ事故を防ぐためには、ハードウェア・ソフトウェアといった技術による解決もありますが、最終的にはそのシステムを使用する「人」が適切に行動する必要があります。
社員一人ひとりが日常から適切な行動をとれるよう、従来の教育・啓発施策を見直し、継続的に実施しています。さらに、基本行動の徹底強化を目的として、組織トップへの積極的な働きかけを実施しています。

■ **情報セキュリティ目標**：2010年度は、「セキュリティ基本行動の心得7ヶ条」の制定と、個人情報保護に関する社員全員へのIBT研修や、PJ向けの座学教育の実施を目標としました。2011年度は、セキュリティレベルを見える化し経営層への基本行動の徹底の働きかけを目標とします。

■ **アクションプラン**：「セキュリティ基本行動の心得7ヶ条」の制定とその啓発、情報セキュリティ強化月間・セキュアフライデーを契機とした啓発、経営層向けアドバイザリーレポートの作成およびキャラバンなど

経営に寄与するセキュリティ

新技術や新規ビジネスツールの普及は、情報セキュリティの観点では新たなリスクを抱えることにもなります。NTTデータでは、こうしたリスクを最小限にするために、新技術・新規ビジネスツールについて利便性を考慮しタイムリーに対応しています。
情報セキュリティ事故の発生は企業にとって大きな経営リスクとなることから、「事故を発生しない仕組み」と「万が一事故が発生した際に被害を最小限に抑える仕組み」の構築をします。

■ **情報セキュリティ目標**：2010年度は、スマートフォン・タブレット端末利用のルール化と、インシデント対応チームの設立を目標としました。2011年度は、ソーシャルネットワーキングサービス（SNS）利用のルール化と、インシデント対応力の強化を目標とします。

■ **アクションプラン**：SNSやスマートフォン・タブレット端末の利用ルール策定、NTTDATA-CERTの設立及びFIRST（注）加盟など

注：FIRST(Forum of Incident Response and Security Teams) とは、50カ国以上の約250の政府機関、教育機関、企業等組織のセキュリティ専門家がベストプラクティスを共有するコミュニティです。(http://www.first.org/)

監査・モニタリング

NTTデータの監査・モニタリング体制

監査部

監査内容	事業本部等やグループ会社に対する情報セキュリティ監査を実施しています。

情報セキュリティ推進室

モニタリング内容	技術的対策の運用状況、情報管理体制の構築状況、個人情報保護の運用状況など個別の情報セキュリティ施策に対する管理目標を定め、実施状況などをモニタリングし、CISOに報告しています。 2011年からグループ会社へのモニタリングを海外会社まで拡大しました。 CISOは、情報セキュリティ戦略が経営方針の達成や情報セキュリティリスクの低減に寄与しているかを判断する材料として、各種モニタリング結果を使用しています。

監査結果をもとにした施策の改善

NTTデータの情報セキュリティ監査では、情報セキュリティポリシーなどの遵守状況を確認しています。また監査結果をもとに施策の改善につながる提言も行っています。

NTTデータ社内

■ 監査結果

- 情報セキュリティポリシーやその下位規定に定められた管理が徹底されていないことが確認された。

■ 提言

- 規定に定められた管理の更なる徹底が望まれる。

■ 施策の改善

- 情報セキュリティに対する意識の底上げのために、「セキュリティ基本行動の徹底」を重点施策に盛り込むことを情報セキュリティ委員会で決定。
- 今までの各種モニタリング結果を基に、各組織の情報セキュリティの成熟度を評価した「アドバイザリーレポート」を作成し、成熟度の低い組織の経営層に説明。従来のボトムアップによる意識付けの他、トップダウンによる情報セキュリティの意識付けを要請。

グループ会社

■ 監査結果

- 海外グループ会社では、グループセキュリティポリシー（GSP）に準拠した自社の情報セキュリティポリシーが未策定の企業が確認された。
- 情報セキュリティポリシー等で定められた管理が徹底されていないことが確認された。海外グループ会社では国内グループ会社よりも多くの不備が確認された。

■ 提言

- 海外グループ会社に対する積極的な改善対応が求められる。

■ 施策の改善

- 従来海外グループ会社に展開していなかった「情報セキュリティ運用状況のモニタリング」（四半期に1度実施）を海外グループ会社にも展開。情報セキュリティ運用状況を把握し、改善を指導。
- 上記モニタリングを実施する人材を育成するための「GSP内部監査人研修」を日・英・中の3カ国語対応に拡大し、海外グループ会社におけるGSP内部監査人を育成。
- GSP教育を日・英の2カ国語から日・英・中の3カ国語対応に拡大。

情報セキュリティ施策の展開事例：1

海外グループ会社の情報セキュリティ推進強化

NTTデータグループは、「Global IT Innovator」をグループビジョンとして掲げています。
ここでは、グループの拡大やグローバル化に対応するために、NTTデータで実施している情報セキュリティ施策を紹介します。2011年度は、特に海外グループ会社に対して情報セキュリティ推進を強化しています。

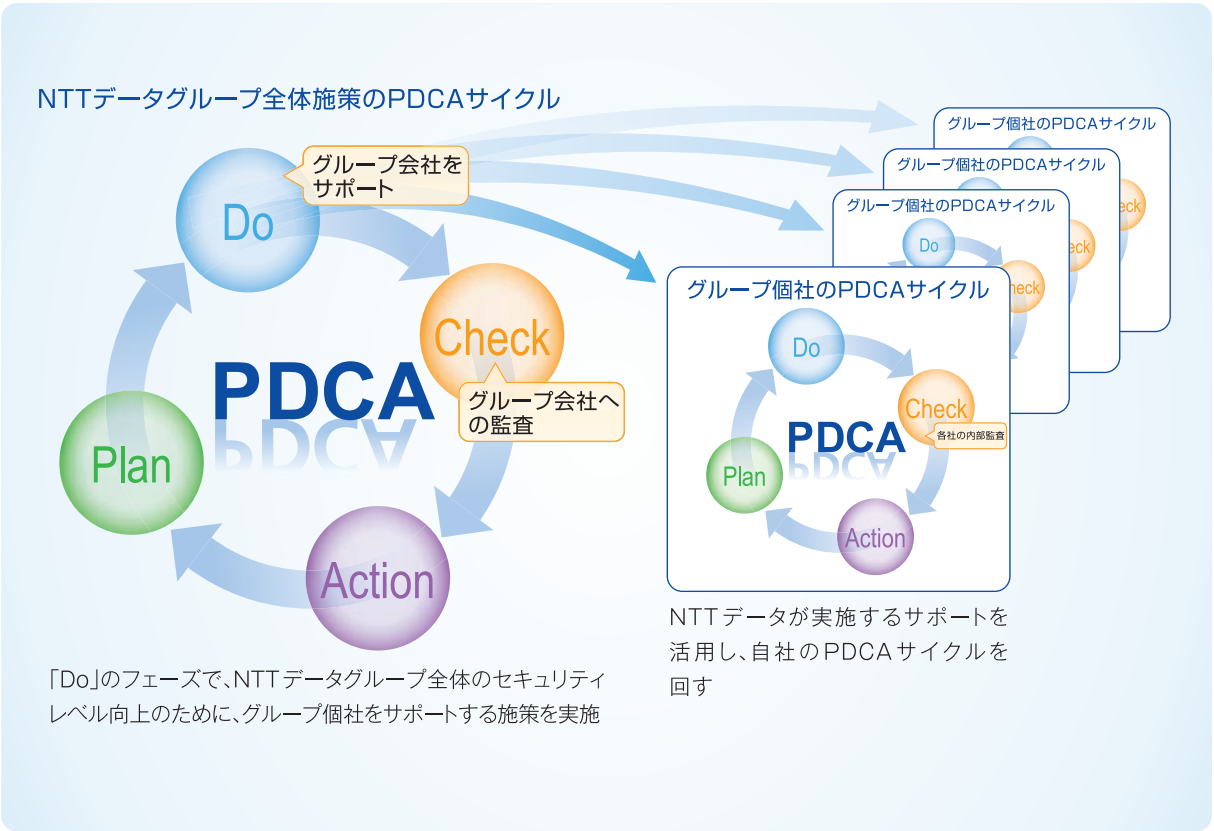
PDCAダブルループ

NTTデータグループでは、情報セキュリティ推進活動のマネジメントサイクルとして、

①企業グループ全体のマネジメント
②グループ各社における個別のマネジメント

の2つがあり、この2つが相互に良い影響を与えながら回転している状態が理想と考えています。NTTデータでは、これを「PDCAダブルループ」と呼んでいます。
2010年度までは「PDCAダブルループの定着」、2011年度からの3カ年は「PDCAダブルループの成熟」を目標とし、アクションプランを実施しています。
特に、海外グループ会社に対しては、自社のPDCAループの形成を早期に実現できるよう個別に支援をしています。

■個社のPDCAが回りながらグループ全体のPDCAが回っている例



「Do」のフェーズで、NTTデータグループ全体のセキュリティレベル向上のために、グループ個社をサポートする施策を実施

NTTデータが実施するサポートを活用し、自社のPDCAサイクルを回す

グループ全体を統制するPDCAサイクル構築のための具体的施策

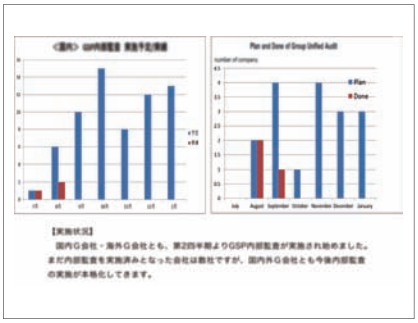
■ グループ全体の情報セキュリティ推進状況の見える化（グループ会社モニタリング）

NTTデータでは、グループ各社の情報セキュリティレベルを把握し、向上するため、情報セキュリティ推進体制の構築状況や教育実施状況、内部監査実施状況などをモニタリングしています。2011年からは海外グループ会社も対象としました。

モニタリング結果は分析され、各社にフィードバックされています。これにより、グループ各社は、グループ全体の状況と自社のレベルを客観的に把握し、自社の取り組みに反映することができます。

また、モニタリング結果は、NTTデータグループ全体の情報セキュリティ施策の有効性を評価する材料としても使用しています。

■GSP内部監査計画・実績



グループ各社内の情報セキュリティ推進PDCAサイクル構築・運用支援策

国内グループ会社に展開している施策を海外グループ会社にも拡大することで、全グループ会社における情報セキュリティ推進のPDCAサイクルを形成・強化しています。

■ グループ会社キャラバン

- NTTデータの情報セキュリティ推進室が各グループ会社に実際に足を運び、グループ各社の抱えている問題点や課題についてヒアリングし、その場でアドバイスや対策の検討などを実施しています。
- 2010年度は国内4社・海外5社、2011年度は国内5社・海外8社に対して実施しました。

■ グループ会社向け情報セキュリティ教育

- グループ統一ルールであるGSPに関するWebインターフェースの教育システムを、グループ全体で活用しています。
- グローバル化に対応し、日本語・英語・中国語の3カ国語での受講が可能です。
- 2011年度からはグループ各社の協働者も受講可能としています。
- 2010年度は国内60社・海外7社、2011年度は国内61社・海外22社が本システムを社員教育に、34社が協働者教育に活用しました。

■ GSP内部監査人研修

- 実際にグループ各社で内部監査を担当する社員を対象に研修を実施しています。
- グループ統一ルールであるGSPへの準拠性に焦点を合わせ、模擬監査演習を組み込むなど、自社内での内部監査実施への展開が容易です。
- 2011年からはグローバル化に対応し、日本語・英語・中国語での受講も可能としました。
- 2010年度は国内57社・169人、2011年度は海外を含め66社・268人が受講し、内部監査人となりました。

■ セキュリティ推進者育成（グループ会社情報セキュリティ推進者フォーラム）

- グループ会社の情報セキュリティ推進者が集合し（国内のみ）、各グループ会社個別の優良事例やNTTデータの取り組みと施策の説明、情報セキュリティ推進に関するポイントなどの情報を共有するための会合を、定期的に開催しています。
- グループ内のノウハウ共有とともに、情報セキュリティ推進者のスキルアップにつなげています。
- 2010年度、2011年度共、2回開催しました。

情報セキュリティ施策の展開事例：2

セキュリティ基本行動の徹底

情報漏えいや流出を防ぐためには、大切な情報を扱う「人」の意識を高めることが重要です。
取り扱う情報に責任を持つ、ITのプロフェッショナルとしての自覚を持ち、常に適切な行動を社員一人ひとりが当たり前のこととして実践し続けるため、NTTデータでは社員の情報セキュリティ基本行動の徹底の向上を目的とした、情報セキュリティ教育・啓発活動に力を入れています。
2010年度からは、特に重要な基本行動を「セキュリティ基本行動の心得７ヶ条」として定め、これを浸透させることに注力しました。
ここでは、2010年度、2011年度で企画・実行した情報セキュリティ教育・啓発施策のうち主なものを紹介します。

セキュリティ基本行動の心得7ヶ条の制定とセキュアフライデーの展開

2009年度より、NTTデータでは毎週金曜日を「セキュアフライデー」と定め、情報セキュリティ確保に必要な行動の実践について啓発活動を実施しています。
2010年7月に、「必要な行動」をわかりやすく浸透させるため「セキュリティ基本行動の心得7ヶ条」を制定し、期間を定めて1条ずつ重点的に展開してきました。展開の際には、教材やチェックリスト、ケーススタディ等の資料の提供や、社内での実践事例の紹介など、職場ですぐに取り組める形をとりました。
2011年9月まで、NTTデータ本社ビルでは毎週金曜日の朝、出勤する社員一人ひとりに「セキュリティ基本行動の心得7ヶ条」を語りかける「あいさつ運動」を実施しました。
2011年10月からは、社内の「ヒヤリハット」事例に基づき、四半期単位でケーススタディの展開を進めています。また、後述する「情報セキュリティ・ワークショップ」をメニュー化し、情報セキュリティの啓発を進めています。

情報セキュリティ強化月間

2008年度より、11月を「情報セキュリティ強化月間」と定め、NTTデータの現場の情報セキュリティレベルの向上を目的としてさまざまなツールや活動を通じて、社員・協働者に情報セキュリティに触れる機会を提供し、自発的な行動を促しています。
2010年度は、「セキュリティ基本行動の心得7ヶ条の実施徹底」をテーマとして情報セキュリティ啓発ポスターを作成し、各職場に配布するとともに、情報セキュリティ啓発ツールを希望者に配布しました。
2011年度は、内閣官房情報セキュリティセンター（NISC）の「情報セキュリティ月間」に合わせて2月開催とし、「機密情報はあなたが守る!」をテーマに、標的型攻撃対策訓練の実施や新たな啓発ツールの配布等を予定しています。

情報セキュリティ啓発ツールの一例

■情報の種類追記用はんこ

紙の資料に後から情報の種類（情報種別）を追記する際の作業を簡略化するため、はんこにして配布しています。

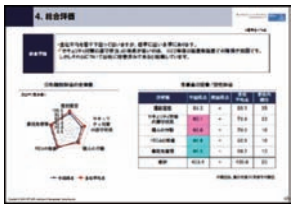
■情報セキュリティ腕章

情報セキュリティ推進活動時に着用してもらうために配布しています。あいさつ運動においても、着用しました。

アドバイザリーレポートの展開

2011年度から、経営層に自分が管轄する組織がどのようなセキュリティレベルにあるのかを知ってもらい、効果的な対応策が打てるよう、社内の組織単位およびグループ会社単位に「アドバイザリーレポート」を作成しています。
特に対応が必要な項目が抽出された組織やグループ会社に対しては、経営層と情報セキュリティ推進者に対してキャラバンを行い、アドバイザリーレポートを通じて評価結果をフィードバックしました。
キャラバンでは残存するセキュリティリスクやその改善策について意見交換を行い、後述する「情報セキュリティ・ワークショップ」の実施を提案するなど、具体的なセキュリティ対策について検討しました。

■アドバイザリーレポートの例



■キャラバンの模様

情報セキュリティ・ワークショップ

2011年度から新たに「情報セキュリティ・ワークショップ」という形で、実際の「ヒヤリハット」事例や「セキュリティ基本行動の心得７ヶ条」に基づくケーススタディを通じて自らの行動を考えてもらう場を提供しています。
ワークショップでは、問題が起こった場合の対応を参加者同士が議論し、ルールや基本行動を互いに確認し合うことで、それらを知識として確実に定着させることを狙いとしています。
また、実施の申し込みがあった組織で実際にあったヒヤリハット事例をケーススタディの題材にし、参加者に現実感を持ちながら議論をしてもらうことで、実施の効果を高めています。

■情報セキュリティ・ワークショップの模様

情報セキュリティ施策の展開事例：3

経営に寄与するセキュリティ

情報セキュリティは、日々進化する技術や製品に早急に対応していく必要があります。新しい技術や製品は、より便利な社会作りに貢献しますが、その反面、使い方を誤れば新しい脅威となる可能性があります。
NTTデータでは、新しい技術・製品が生み出す大きなビジネスチャンスを活かせるよう、それらが迅速かつ安全に使用できる環境を整備しています。また、情報セキュリティ事故の発生は大きな経営リスクとなることから、「事故を発生させない仕組み」と「被害を最小限に抑える仕組み」の構築に取り組んでいます。
ここでは、新しい技術・製品への対応及びセキュリティ・インシデント・レスポンス・チーム(CSIRT)の取り組みを紹介します。

スマートフォン、タブレット端末への対応

スマートフォンやタブレット端末等の新しい製品の普及により、従来の携帯電話やノートPCに比べユーザの利便性は向上しましたが、自由度が高い分、情報漏えいのリスクも高まっています。
NTTデータでは、スマートフォンとタブレット端末に対して、次のような対応により情報漏えいリスクを低減しています。

スマートフォンへの対応

スマートフォンは、従来の携帯電話とは違った性質を持っています。

- 取り扱う情報は様々なアプリケーション上で利用ができる（クラウドサービス上に情報が保管される可能性が高い）
- OSが全世界共通のプラットフォームの場合が多く、コンピュータウイルスへの感染リスクが高い

そのため、NTTデータでは、2011年5月より、スマートフォンから社内サーバにアクセスする際に専用サービスによって端末や一般のクラウドサービス上に情報が残らない仕組みを導入しました。これにより、安全に社外からも社内メールなどの社内システムを利用することができます。
また、セキュリティ機能の設定についてガイドライン上で詳細に手順を説明し、必要となるセキュリティ対策を確実に実施できるよう工夫しています。

タブレット端末への対応

タブレット端末は、ノートPCよりも操作性や携行性に優れているため、ビジネスの現場での利用希望が早々にありました。しかし、タブレット端末では、当社のシンクライアントの仕組みを利用できないため、スマートフォンやノートPCと同じレベルでの安全性の担保が難しい状況にあります。
そこで、端末設定や利用手順等をルール化し、ルールを遵守できる機種については2010年11月から申請制でシンクライアントの利用と同等に扱うことができるようにしました。
今後は、社内サービスや製品自体の機能拡充を踏まえて、社内のルールの見直しや対象機種の拡大を行っていく予定です。

ソーシャルメディアへの対応

従来、ソーシャルメディアは個人対個人での利用が基本でしたが、企業がアカウントを取得できるようになる等、ビジネス面での利用も可能となっています。
NTTデータでは、2011年6月に、公式に運営するソーシャルメディアを対象として「ソーシャルメディアポリシー」を公開し、ソーシャルメディアでの当社の具体的な対応を明らかにしています。社内での運用ルールも同時期に策定し、会社名で運営するアカウントについては、公開されたソーシャルメディアポリシーを遵守しています。さらに全社でアカウント管理をする体制を取り、「ソーシャルメディア公式アカウント一覧」として公開しています。

NTTデータソーシャルメディアポリシー ：http://www.nttdata.co.jp/info/privacy-sm.html
NTTデータソーシャルメディア公式アカウント：http://www.nttdata.co.jp/info/accountlist.html

NTTDATA-CERTによる事故対応

ITサービスやその構成要素は次々と進歩し、さらにサイバー攻撃と呼ばれる攻撃手法も専門的かつ多岐にわたっているため、企業はより早く必要な情報を取得して対応することが求められます。これを怠り、一旦、個人情報漏えいなど情報セキュリティ事故を起こしてしまうと、ブランド力低下による顧客離れなど企業は多大な経営リスクを負ってしまうことになります。
NTTデータでは、こうした情報セキュリティに関わる経営リスクに対応し、システムやサービスを安全かつ安心してお客様に提供するため、セキュリティ事故の防止や事故発生時の緊急対応を迅速かつ正確に行うためのセキュリティインシデント対応の専門チーム(CSIRT)として、2010年7月、「NTTDATA-CERT」を設立しました。
NTTDATA-CERTはインシデント対応力の強化を目的に、他のCSIRT組織とのグローバルなコミュニケーションパスの確立を進めています。
NTTデータおよびNTTデータグループ各社における情報セキュリティ事故発生の際には、NTTDATA-CERTや関連するスタッフ部門などが一体となって速やかに適切な対応を行う体制を整えています。
また、万が一の情報セキュリティ事故発生時に適切な対応を行うため、NTTDATA-CERTは、NTTグループで行われた、情報セキュリティ事故発生から状況把握までをストーリー化した事故対応演習に参加しました。

■ NTTグループで行われた事故対応演習の様子

社会状況に応じたセキュリティ

東日本大震災にかかわる事業継続・夏季電力利用抑制への取り組みについて

NTTデータグループでは、東日本大震災においては、事業継続が不可能となるレベルの被害はありませんでした。
東日本大震災が起きた3月11日中に災害対策本部を設置し、社員・家族の安否確認および入居ビルの損傷確認を行うとともに、被災地域のお客様システムの復旧作業やサービスの維持などに取り組んできました。

また、NTTデータでは、2011年夏の東京電力管内での電力不足や政府の要請などを踏まえ、2011年7月1日～2011年9月22日を実施期間として節電に取り組みました。
ここでは、節電に関する取り組みのうち、情報セキュリティに関わるものを紹介します。

1.オフィスフロアの輪番不使用

本社（豊洲センタービル、豊洲センタービルアネックス）をはじめ、オフィスフロアごとに空調、照明、コンセント電力を不使用とする日を設け、消費電力の削減を行いました。
不使用フロアのオフィスに所属する一部の社員が出社して業務を行うために、本社ビルに「共通オフィス」を設置しました。共通オフィスでは、シンクライアント端末のみを利用可能として、セキュリティを保ちつつ複数部署の社員が作業できるようにしました。

2.働き方の変革

NTTデータでは、テレワーク、休日取得促進、週休日変更等を推奨し、働き方の変革を推進しました。
テレワークにおいては、通常勤務と同様に情報セキュリティポリシーを遵守するほか、主に以下のルールを定め、技術面・運用面の両輪でセキュリティを担保しました。

■技術面

- 原則として、会社から貸与されたシンクライアントPCを利用
- リモートアクセスの認証には、ワンタイムパスワードを利用
- 自宅で無線LANを使用する場合は、通信経路の暗号化が必須

■運用面

- 在宅勤務の申請時に、セキュリティルールをチェックリストで確認
- 個人情報および極秘資料を使用する業務の禁止
- 自宅での紙媒体の使用を禁止
- 自宅でのFAXの使用を禁止
- 在宅勤務の作業場所に、家族が近寄らないように工夫

3.パソコンの置き換えによる節電

NTTデータでは、オフィスで使用しているデスクトップPC約1万台を、電力消費量の低いノート型PCや、シンクライアント端末に置き換えました。

新規ノートPCについては、設定に関する個別の対策マニュアルとチェックリストを作成し、情報セキュリティ対策の実施漏れを防止しました。

置き換えにより不要となったデスクトップPCについては、情報を確実に消去してからリサイクルしました。また、被災地にPCを寄付する場合は、PCを安全に再利用できるようにするためのルールを作り、情報漏えい防止を徹底しました。

サイバー攻撃への対応

2011年は、米国の日系企業におけるハッカー集団からのサイバー攻撃による個人情報漏えい事件や国内企業等への標的型攻撃の発覚などがマスメディアを賑わせました。

システムをセキュアに保つことは、サイバー攻撃への対抗策の一つとなります。NTTデータでは、1998年からNTTデータにおいてシステム開発やシステム運用上利用が想定されるハードウェア・ソフトウェアにおけるセキュリティの脆弱性発見やセキュリティパッチの提供などについて、多岐にわたる情報を取りまとめ、これらの情報が公開された日にメールマガジン形式およびWebサイト上で情報提供を行っています。これにより、システム開発や運用の担当者はタイムリーかつ一元的にセキュリティの脆弱性の把握やセキュリティパッチ情報を取得することができます。本メールマガジンの発行とWebサイトの更新は、NTTDATA-CERTが独自の情報網を用いて行っています。

また、NTTデータグループでは、2011年5月に、個人情報を取り扱うWebシステムについて総点検を実施しました。

■ セキュリティ情報メールマガジンのイメージ

情報セキュリティへの理解と意識向上のために

継続的な情報セキュリティ教育・啓発

情報セキュリティの継続的な実践のためには、役員・社員・協働者一人ひとりが情報を扱うプロフェッショナルであることを自覚し、日常の行動の中で常に情報セキュリティポリシーに従った適切な行動をとることが必要です。

NTTデータでは、継続的な情報セキュリティ教育・啓発運動を通じ、ルールや行動の理解と、実践に必要な情報セキュリティマインドの醸成に取り組んでいます。

情報セキュリティ教育

NTTデータグループでは、個人情報保護やグループセキュリティポリシーに記載されたルールの理解、および情報セキュリティを意識した行動の理解を中心に、継続的な情報セキュリティ教育を実施しています。

■ NTTデータにおける2010・2011年度の情報セキュリティ教育実績

対象者	実施形態	内容・狙い
全社員（必須）	個人情報保護IBT （Webインターフェース）	個人情報に関する考え方／個人情報の取り扱い方法／社内規程の内容理解／個人情報に対する意識向上 ※2010年度、2011年度の実績：社員100%
	情報セキュリティポリシー・アセスメント （Webインターフェース）	情報セキュリティポリシーの理解度向上／情報セキュリティ事故発生時の基本動作の理解／携帯電話や小型可搬媒体の適切な取り扱いなど、正しい知識の習得 ※2010年度、2011年度の実績：役員、社員100%
特定プロジェクト	個人情報権利保護研修 （座学教育）	プロジェクトにおいて個人情報を取得する際の実施事項を理解するための教育 ※2010年度実績：5回・140名、2011年度実績：4回・83名
全社員（任意）	情報セキュリティ・ワークショップ	情報セキュリティ・個人情報保護などに関する問い合わせが多い項目をテーマとして取り上げたワークショップ ※2011年度実績：5回（年度末までの予定を含む）
全社員 （ワークグループ単位、任意）	「セキュリティ基本行動の心得7ヶ条」のケーススタディ	グループディスカッションで、情報セキュリティ対策のより深い理解や浸透などの「自らの行動を考える」場 2カ月毎に展開をした「セキュリティ基本行動の心得7ヶ条」のテーマにそって、各職場にて実施
各階層	情報セキュリティ講話 （座学教育）	新入社員、中途採用社員、課長、部長などの各階層別に必要な知識や役割、責任の違い、心構え、必須事項などについて説明 情報セキュリティ理解の向上と実践のための知識習得
協働者（必須）	個人情報保護導入教育 情報セキュリティ教育 （Webインターフェース、教材提供）	個人情報保護に関する考え方、NTTデータにおける情報セキュリティルールについて、NTTデータで働くパートナーとして知っておくべき内容を教育 社内システム利用時は受講が必須で、かつ定期的な受講が必要 ※マルチリンガル対応（英語・中国語・日本語）
協働者（新規）	情報セキュリティ教育ハンドブック	新規のNTTデータグループの協働者に対して、NTTデータと働く上で知っておいて欲しい情報セキュリティや個人情報の取り扱いについて説明したハンドブックをNTTデータグループと契約を締結する際に配布 ※マルチリンガル対応（英語・中国語・日本語）

グループ会社の教育活動サポート

グローバル化・グループ拡大に対応した「PDCAダブルループ」形成のため、グループ全体の情報セキュリティレベル向上の観点から、NTTデータはグループ各社が自社内で情報セキュリティ教育を実施する際に必要なツールを提供し、サポートを行っています。

グループ会社教育サポートツール

対象者	実施形態	内容・狙い
グループ会社社員	GSPセキュリティ教育 (Webインターフェース)	NTTデータグループセキュリティポリシーの理解向上／個人情報の取り扱い方法／ NTTデータグループセキュリティポリシーの解説 ※マルチリンガル対応(英語・中国語・日本語) ※2010年度実績:60社・14,197名、2011年度実績:83社・20,536名
グループ会社協働者	協働者用GSPセキュリティ教育 (Webインターフェース)	NTTデータグループで働くパートナーとして知っておくべき、個人情報保護に関する考え方、情報セキュリティルールについて教育 ※2011年度開始:34社・4,752名
内部監査人	GSP内部監査人研修 (集合座学研修、2011年度より自席オフライン研修での実施も追加)	情報セキュリティ監査を行うための教育 模擬監査演習も実施 ※自席オフライン研修はマルチリンガル対応(英語・中国語・日本語) ※2010年度実績:57社・169名、2011年度実績:66社・268名(海外を含む)

情報セキュリティ啓発ツールの一例

NTTデータでは、情報セキュリティ戦略の重点テーマとして注力しているセキュリティ基本行動の徹底以外にも、情報セキュリティレベルの維持・向上を目的とした継続的な情報セキュリティ啓発活動を実施しています。

情報セキュリティ啓発ポスター

世の中や社会の動き、情報セキュリティ戦略の重点テーマなど、タイムリーなテーマを用いて、各職場における情報セキュリティの「気づき」の機会を提供する。2008年度よりマルチリンガル版の発行を開始し、マルチリンガル版はグループ会社にも展開。

2010年度のテーマ
セキュリティは君の命綱
Incident Zero
(マルチリンガル)

2011年度のテーマ
シンクライアント利用促進／ PC設定再チェック
誤送信防止／ SNS利用時の注意
(マルチリンガル)

月間ニュースレター「Security Today」

NTTデータグループ内の情報セキュリティへの取り組みや施策の説明、セキュリティにかかわる社会情勢や最新技術、事故情報などメールマガジン形式で月1回発行。
一部はグループ会社・協働者にも展開し、情報を共有。

CISOメッセージ

2011年度より四半期に一回、CISOから直接社員に対してメッセージを発信。最新動向を見据えて、CISOが考えていること、社員にお願いしたいことなど、CISOと社員の目線合わせの場として活用。

委託業務における取り組み

NTTデータでは、ソフトウェア開発業務を委託したパートナー企業からの情報漏えい・情報流出を未然に防ぐため、さまざまな基準を定めています。機密情報や個人情報を取り扱う業務を委託する場合は、誓約書の受領やセキュリティ対策実施状況の確認などを実施しています。

パートナー企業の選定

体制・対策状況の確認	一定水準を満たす取引先を選定するために、別途定めた基準に従い、ヒアリングなどにより取引先のセキュリティ対策状況を確認する。
ルールの提示・対策レベルの合意	プロジェクトなどにおけるセキュリティ管理や個人情報保護に関するルールを提示し、パートナー企業に求める対策レベルについて合意を得る。

業務委託後の取り組み

契約開始

教育・誓約書の確認	・契約時に合意した内容に従い、情報を取り扱うパートナー企業担当者へ教育を行う。 ・誓約書の写しを確認・受領する。
パートナー企業からの報告	情報管理体制・情報の取り扱い状況・セキュリティ対策の実施状況などについて、報告書の提出や会議の開催により、定期的に確認する。
パートナー企業の検査	必要に応じて、立ち入り検査などを実施して、セキュリティ対策状況を確認し、情報が適切に運用・管理されているかを判断する。判断結果に従って是正要求および改善確認を行う。
情報廃棄などの確認	利用目的が終了した情報や利用期間中に不要となった情報、およびそれらが保存された媒体は、プロジェクトであらかじめ定めた方法により適切に返還または廃棄を行う。

契約終了

情報セキュリティ事故の発生状況

初めて情報セキュリティ報告書を発行した2008年以降、本報告書発行に至るまでの間、NTTデータでは重大な情報セキュリティ事故は発生しておりません。

なお、重大な情報セキュリティ事故発生を未然に防ぐため、以下のような技術的対策を社内に導入しています。

- 情報漏えい対策ソリューション（Total Security Fort：TSF）の用PCへの導入
- 原則すべての社外持ち出しPCをシンクライアント化
- メールフィルタリングソリューションの導入
- Web（URL）フィルタリングソリューションの導入
- ウイルス対策ソフトウェアの全業務利用PCへの導入

第三者評価・認証

ISMS認証の取得状況

NTTデータおよびNTTデータグループ各社では、必要に応じて、機密情報や個人情報を扱う組織単位で情報セキュリティマネジメントシステムの国際規格ISMS（ISO/IEC 27001）の認証を取得しています。

ISMS認証を取得した組織を持つグループ会社は、以下のとおりです。
（NTTデータを含む40社、2011年12月末現在）

■ISMS認証取得組織を持つ会社

株式会社NTTデータ	株式会社NTTデータ経営研究所	株式会社クニエ
NTTデータ・システム技術株式会社	株式会社NTTデータSMS	株式会社NTTデータセキスイシステムズ
株式会社NTTデータアイ	NTTデータカスタマサービス株式会社	株式会社テクノパワー
NTTデータ先端技術株式会社	NTTデータフォース株式会社	株式会社エマーズ
株式会社NTTデータ・フィナンシャルコア	株式会社NTTデータフロンティア	株式会社NTTデータテラノス
株式会社NTTデータ北海道	日本カードプロセシング株式会社	株式会社NTTデータ NCB
株式会社NTTデータ東北	株式会社リアライズ	NTTデータ・ジェトロニクス株式会社
株式会社NTTデータ信越	株式会社NTTデータ3C	株式会社NTTデータCCS
株式会社NTTデータ東海	株式会社NTTデータウェーブ	株式会社NTTデータMSE
株式会社NTTデータ北陸	株式会社大阪エクセレント・アイ・ディ・シー	株式会社JSOL
株式会社NTTデータ関西	株式会社NTTデータ・チャイナ・アウトソーシング	株式会社NTTデータアイテックス
株式会社NTTデータ中国	株式会社NTTデータビジネスブレインズ	株式会社エヌジェーケー
株式会社NTTデータ四国	株式会社NTTデータソルフィス	株式会社NTTデータ・エム・シー・エス
株式会社NTTデータ九州		

プライバシーマークの付与状況

NTTデータおよびNTTデータグループにおける、プライバシーマーク付与事業者は、以下のとおりです。
（NTTデータを含む32社、2011年12月末現在）

■プライバシーマーク付与グループ会社

株式会社NTTデータ	株式会社NTTデータSMS	株式会社NTTデータ・エービック	株式会社NTTデータテラノス
NTTデータ先端技術株式会社	NTTデータカスタマサービス株式会社	株式会社NTTデータソルフィス	株式会社NTTデータCCS
株式会社NTTデータ北海道	NTTデータマネジメントサービス株式会社	株式会社NTTデータビジネスシステムズ	株式会社JSOL
株式会社NTTデータ東北	株式会社NTTデータフロンティア	株式会社NTTデータセキスイシステムズ	株式会社エックスネット
株式会社NTTデータ東海	日本カードプロセシング株式会社	株式会社NTTデータスミス	株式会社NTTデータアイテックス
株式会社NTTデータ関西	株式会社NTTデータユニバーシティ	株式会社NTTデータエンジニアリングシステムズ	東北情報システム株式会社
株式会社NTTデータ中国	株式会社NTTデータ3C	株式会社テクノパワー	メディアドライブ株式会社
株式会社NTTデータ経営研究所	株式会社NTTデータ・アール	株式会社コメット情報	株式会社エマーズ

■ 情報セキュリティ活動年表

社会の動き	技術動向		NTTデータの実績・動き
	1994 線形解読法により「DES」が解読	1994	1997 情報セキュリティ委員会　設置
1995 情報セキュリティマネジメントの英国規格BS7799 Part1が策定	Windows 95発売	1995	1998 12月 「情報セキュリティポリシー」制定
	1996 Yahoo！(日本語)サービス開始 6月 Microsoft Excelに感染するマクロウィルス「Laroux」発見	1996 1997	1999 CISO(セキュリティ戦略担当役員)設置 2月 IBT（Internet Based Testing）研修開始
1998 情報セキュリティマネジメントの仕様として英国規格BS7799 Part2が規定 4月 財団法人日本情報処理開発協会(JIPDEC)、プライバシーマークの運用を開始	1997 米国で「PKI」が提唱される Google設立	1998 1999	
1999 5月 BS7799 Part1、Part2改訂	NTTドコモ「iモード」サービス開始 「Napster」公開 3月 メール繁殖型ウイルス「Melissa」流行 4月 国内初の商用ADSLサービス開始	2000	2000 2月 ベンチャー制度活性化(NTTデータイントラマート設立) 3月 3月期より連結決算制度導入 6月 情報セキュリティポリシーアセスメント実施開始
2000 7月 情報セキュリティの国際標準規格ISO15408の国内版JIS X 5070制定 9月 BS7799 Part1が国際規格ISO／IEC17799となる	Google(日本語)提供開始 DoS攻撃が増加 10月 「WinMX」Beta版公開 12月 NTT東西「フレッツADSL」開始	2001	2001 2月 「標準セキュリティポリシー(SSP)」策定 6月 「個人情報保護規程」策定 7月 「個人情報保護方針」公表 9月 国内で初めてBS7799を取得
2001 e-Japan戦略策定	米国にてDES、トリプルDESに代わりAESが政府標準暗号化 「Code Red」「Sircam」が猛威をふるう 6月 NTT東西「Bフレッツ」開始 11月 「WinMX」で初の逮捕者	2002	2002 9月 協働者向け教育(CISP)開始 10月 NTTデータグループセキュリティ合意書(GSA)制定
2002 4月 財団法人日本情報処理開発協会(JIPDEC)、ISMS適合性評価制度の運用を開始	ボットネットの出現 5月 P2Pソフト「Winny」Beta版公開	2003	2003 6月 プライバシーマーク認証の取得 7月 地域子会社体制構築(地域子会社9社体制)
2003 10月 日本セキュリティ監査協会発足	Skype社設立 1月 ワーム「Slammer」発生 8月 Skypeパブリックbeta版公開	2004	
2004 Google株式公開	1月 「Share」公開 2月 ワーム「W32/Netsky」流行 5月 P2Pソフト「Winny」開発者逮捕		

2005

社会の動き
「ウェブ2.0」流行
4月 個人情報保護法完全施行

技術動向
12月 「YouTube」公式サービス開始

NTTデータの実績・動き
6月 リモート接続PCのP2Pソフトウエアチェック
11月 TSF導入開始

2006

社会の動き
ファイル交換ソフト「Winny」による情報漏えい事件が多発
2月 「情報セキュリティの日」制定

技術動向
「Facebook」一般に公開
7月 「Twitter」サービス開始
12月 「Amazon EC2」スタート、クラウドコンピューティング具現化
12月 家庭向け高速PLC製品発売

NTTデータの実績・動き
7月 テレワークトライアル開始
9月 NTTデータの全社員を対象に誓約書を取得（個人PCの業務関連情報の削除、個人PCでの業務遂行の禁止）
10月 誓約書の取得対象を全NTTデータグループ社員に展開
11月 誓約書の取得対象を委託先に展開

2007

社会の動き
1月 「情報セキュリティガバナンス研究会」開催

技術動向
10月 Skypeオンラインユーザ1000万人突破

NTTデータの実績・動き
4月 自社ビルにおいてISMS認証を取得
7月 シンクライアント開始
12月 メールフィルタリング開始

2008

社会の動き
1月 コンピュータウイルス作成で日本初の逮捕者
6月 内閣官房情報セキュリティセンター(NISC)が「セキュア・ジャパン2008」を公開

技術動向
2月 USBメモリ経由で感染するウイルスが出現
4月 GoogleとSalesforce.comがクラウドコンピューティングで提携

NTTデータの実績・動き
2月 テレワーク本格導入
3月 システムインテグレーターとして初めて「情報セキュリティ報告書 2008」を発行
4月 NTTデータグループセキュリティポリシー（GSP）施行
11月 「情報セキュリティ強化月間」制定

2009

社会の動き
2月 NISCが「第2次情報セキュリティ基本計画」を発表
6月 NISCが「セキュア・ジャパン2009」を公開
9月 消費者庁に個人情報保護法が移管

技術動向
4月 「Gumblar」出現

NTTデータの実績・動き
「セキュアフライデー」制定
12月 クラウドソリューションの総合サービスを発表

2010

社会の動き
7月 情報セキュリティ戦略会議が「情報セキュリティ 2010」を公開
7月 不正競争防止法改正
11月 中国漁船衝突事故の映像流出

技術動向
Twitterを狙った攻撃が横行
5月 iPad 日本で発売
12月 Android初のボット型ウイルス「Geinimi」出現

NTTデータの実績・動き
3月 「情報セキュリティ報告書2010」の発行
7月 「セキュリティ基本行動の心得7ヶ条」の制定
7月 NTTDATA-CERT設立

2011

社会の動き
3月 東日本大震災に便乗したフィッシング詐欺が横行
5月 サイバー攻撃による日本企業米国子会社からの個人情報漏えい事故が発覚
6月 刑法改正により「ウイルス作成罪」が成立
9月 国内防衛産業への標的型攻撃が発覚

技術動向
5月 アジア・太平洋地域のIPv4アドレスが枯渇

NTTデータの実績・動き
4月 NTTDATA-CERT FIRSTに加入
5月 スマートフォン向け社内接続サービス開始
6月 NTTデータソーシャルメディアポリシーを公開
7月 電力利用抑制のためオフィス利用のPCをノートPCに移行

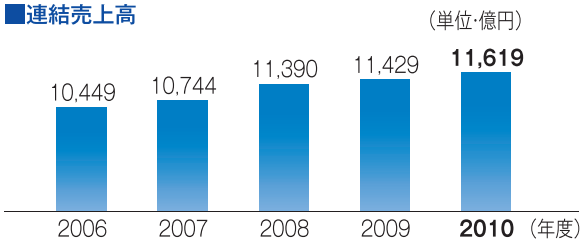
会社概要

NTTデータグループは、1988年に日本電信電話(株)から分社して以来、公共分野のシステム、金融、製造、流通、通信、医療・ヘルスケアなどの法人向けシステム、さらには業界横断的な社会インフラサービスまで、社会の要請・課題に応える情報システムやサービスを提供してきました。そして近年は、事業のグローバル化を推進しており、2011年9月30日現在、海外拠点は34カ国・143都市にまで拡大しています。

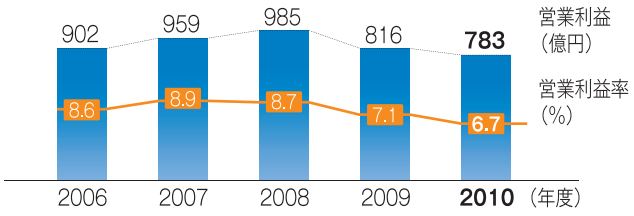
我が国のIT産業の"先導的役割"を果たす企業として、また世界各地で事業を展開するグローバル企業として、これからの社会を支え、変革していく新しい「しくみ」や「価値」を提供していきます。

会社名	株式会社エヌ・ティ・ティ・データ　(NTT DATA CORPORATION)
本社所在地	〒135-6033 東京都江東区豊洲3-3-3 豊洲センタービル
設立年月日	1988年 (昭和63年) 5月23日
代表者	代表取締役社長　山下　徹
資本金	1,425億2千万円 (2011年3月31日現在)
売上高(連結)	1兆1,619億円 (2010年4月1日~2011年3月31日)
経常利益(連結)	783億円 (2010年4月1日~2011年3月31日)
従業員数 (単独)	10,139名(2011年3月31日現在)
従業員数 (連結)	49,991名(2011年3月31日現在)
連結子会社および関連会社	連結子会社:215社(2011年3月31日現在) 関連会社:20社(2011年3月31日現在)

■連結売上高



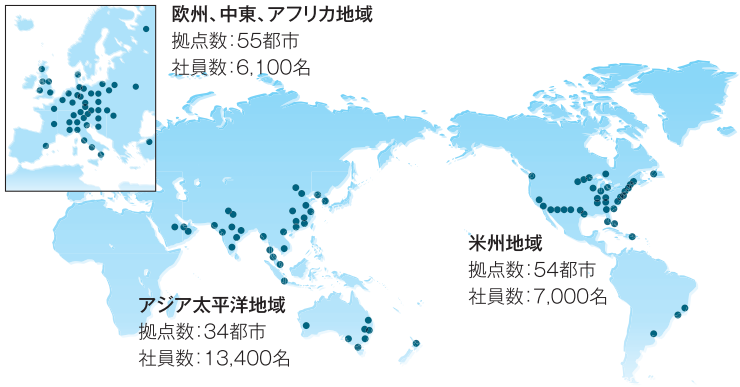
■連結営業利益／連結営業利益率



主な事業内容	システムインテグレーション事業／ネットワークシステムサービス事業 その他これらに関する一切の事業
海外拠点の状況	

欧州、中東、アフリカ地域　55都市　6,100名
アジア太平洋地域　34都市　13,400名
北米地域　54都市　7,000名

※要員数:2011年9月30日現在



企業グループにおける情報セキュリティの実践

～あとがきにかえて～

企業の情報セキュリティを取り巻く環境変化は著しく、その脅威は高度化、多様化し、被害は甚大さを増しています。特に、2011年に起きたアプリケーションサーバの脆弱性を突いた攻撃による延べ1億件を超える個人情報の流出事件や、標的型メール攻撃による機密情報の漏えい事件は社会的に大きな問題となり、企業は外部からの新たな攻撃に対する対策を迫られました。一方、スマートフォンやタブレット端末は、ソーシャルネットワーキングサービスやクラウドサービスと共に急速な普及を遂げ、社会は、本格的なポストPC時代に突入しました。

NTTデータグループでは、「情報の安全性確保」と「情報の積極的な活用・共有」を適正なバランスで両立させることにより、グループ全体で安全なナレッジ流通を促進し、お客様に新たな「価値」を提供することを情報セキュリティ取り組み方針としています。NTTデータではこれに基づき、昨年より3つの情報セキュリティ戦略に基づき推進しています。1点目は、海外グループ会社の情報セキュリティ推進強化です。積極的なグローバル展開による海外グループ会社の増加に対し、ポリシー制定支援や運用支援、教育支援に力を入れて取り組んでいます。2点目は、セキュリティ基本行動の徹底です。一人ひとりが事故を起こさないために、情報セキュリティを意識し適切な行動がとれるよう「セキュリティ基本行動の心得7ヶ条」を制定し、教育・ケーススタディを展開しています。3点目は、経営に寄与するセキュリティです。スマートフォンやタブレット端末、ソーシャルネットワーキングサービスなど、ビジネスに不可欠な新規ツールやサービスを安全に利用するため、ルールやガイドラインを策定し運用を開始しました。また、情報セキュリティ事故発生防止・緊急時対応の専門チーム「NTTDATA-CERT」を立ち上げ、インシデント対応力を強化しています。

また、社内やグループ会社から届く情報セキュリティに係わる様々な質問や提案に対し、情報セキュリティのプロフェッショナルとして地道ではありますが真摯に対応を進めました。これらの対応は目立たない日常業務かもしれませんが、一つひとつを確実に行うことにより、お客様への迅速な対応や社内・NTTデータグループのセキュリティリスク低減につながり、結果としてお客様満足度向上やNTTデータグループの情報セキュリティ向上を支えると考えています。

本報告書は、NTTデータグループが実践する情報セキュリティガバナンスから社会的関心が高いと思われる取り組みを紹介しました。興味を持ちご覧いただいた皆様にとって少しでもお役に立てれば幸いです。

私たちNTTデータグループは、一人ひとりが「情報を扱うプロフェッショナル」としての自覚を持ち、常に情報セキュリティを意識した行動をとり、安心と信頼を通してお客様に新たな価値を提供し続けるよう、情報セキュリティガバナンスを推進いたします。

株式会社NTTデータ
品質保証部 情報セキュリティ推進室長
高橋 成文

NTTデータグループ　情報セキュリティ報告書2012
発行者：株式会社NTTデータ　情報セキュリティ推進室
Copyright© 2012 NTT DATA CORPORATION
2012年3月　第1.0版　発行

注：本報告書に掲載されているサービス名および商品名などは、NTTデータあるいは各社の登録商標または商標です。

株式会社NTTデータ
〒135-6033 東京都江東区豊洲3-3-3 豊洲センタービル
Tel:03-5546-8202(代表)
www.nttdata.co.jp

FSC www.fsc.org
ミックス
責任ある木質資源を使用した紙
FSC® C010463

VEGETABLE OIL INK