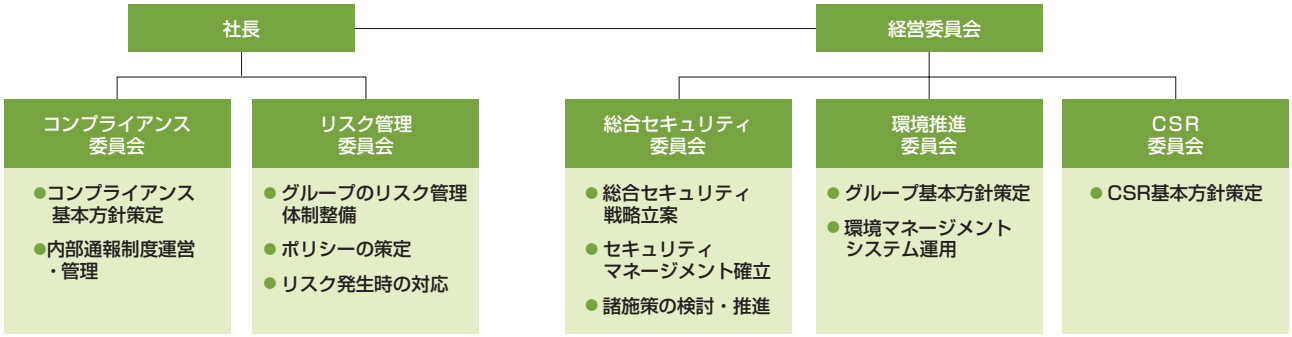
CSR推進体制とマネジメント

日本ユニシスグループでは、経営の透明性・倫理性を高めるべくコーポレート・ガバナンス体制の強化に努めています。そして、「コンプライアンス」、「リスク管理」、「情報セキュリティ」、「環境」、「社会貢献」など、それぞれの活動に対応した体制を整備するとともに、必要に応じて委員会や専任組織を設置し、基本方針の策定、社員に対する啓発活動の徹底を図るための諸施策を展開しています。

CSR推進体制

CSR推進という観点からは下記の五つの委員会を設置し、それぞれの委員会の連携により、コーポレート・ガバナンスの強化を図っています。

●CSR推進体制図



グループ社員へのCSR活動の浸透

コンプライアンス、情報セキュリティなどを社員個人個人の課題として認識し、その規定を厳守するためには繰り返しの教育による浸透活動が必要とされます。日本ユニシスグループではグループ全社員を対象としてeラーニングにより、常に最新の課題に対する教育を実施しています（右図参照）。

～2004年度	●インサイダー取引について ●セキュリティ自己監査 ●個人情報の取扱いについて
2005年度	●セキュリティ自己監査 ●日本ユニシスグループのCSR活動について ●秘密情報の取扱いについて

2005年度実施の「日本ユニシスグループのCSR活動について」では、CSRとは何か、CSRが重視されるようになってきた背景、日本ユニシスグループの取り組み、推進体制など、CSR活動の概要を学習しました。

日本ユニシスグループの情報セキュリティ対策

日本ユニシスグループでは1990年度より「情報セキュリティ委員会」のもと情報セキュリティ対策に取り組んできましたが、2004年度より総合的かつ広範囲な視野で中長期的な情報セキュリティ強化を「日本ユニシスグループ情報セキュリティ総合戦略」として策定し、推進中です。今年度は3ヵ年計画の最終年であり、グループ各社／主要部門のISMS認証取得、Pマーク認定取得などの制度対応を推進しています。また企業を取り巻く環境の変化をうけて、戦略およびアクションアイテムの見直しを進めています。

● 日本ユニシスグループの顧客情報漏洩対策

ビジネスを推進する上で、顧客情報の漏洩対策は最重要課題と認識しています。
物理的・技術的対応として顧客情報へのアクセス制限、アクセスログの管理、執務室への入退室管理の徹底などを実施しています。また、日本ユニシスグループ社員および協力会社のメンバーには「顧客秘密情報の取扱い要領」に基づく啓発活動を徹底し、定期的な情報セキュリティ教育、情報セキュリティ自己監査を実施しています。

● ISMS（情報セキュリティマネージメントシステム）認証取得状況

2001年にISMSのベースであるBS7799（英国規格）をフルアウトソーシング事業を展開する企業として世界で初めて取得しています。
2004年度からは本格的に組織単位の認証取得に着手し、日本ユニシス、国際システムにおいては本年度、ISO27001の統一認証※を取得する計画で対応中です。また、他のグループ会社においても、各社毎に拡大、または新規認証取得対応中です。
なお、2004年度より日本ユニシスグループ全体のセキュリティレベル向上のためにセキュリティ専任部門（40名）を編成し、情報セキュリティ強化をすすめています。

※統一認証：ISMSは通常組織単位で認証を取得しPDCAを回しますが、統一認証では会社全体が対象となります。

● 個人情報保護法対応状況

当社グループでは、「個人情報保護基本方針」、「個人情報取扱基本規定」を定めるとともに、「個人情報保護責任者（CPO：チーフ・プライバシー・オフィサ）」を任命し、社員への個人情報取扱・保護の周知・徹底を図っています。
また、保有する個人情報については適正な取扱方法と、種別・区分などに応じた安全管理措置を定め、紛失・漏洩・改ざん・不正アクセスなどの事故未然防止に努めています。
なお、プライバシー・マークについてはグループ主要3社（日本ユニシス、ユニアデックス、日本ユニシス・ソリューション）を含む5社にて認定取得済であり、2007年度には日本ユニシスグループ全社にて取得予定です。

BCP（事業継続計画）／BCM（事業継続管理）

日本ユニシスグループはお客さまの重要な経営資産である情報システムの構築、保守、運用を担当する企業として大規模災害などのリスクが発生した場合も、自らの事業を継続することの社会的責任を強く認識し、グループ全体の事業継続計画の策定とその遂行のために事業継続管理に取り組んでいます。

●日本ユニシスグループ事業継続計画の必要性

2005年度は、災害時に社員とその家族の安否を迅速に確認し、安全を確保し、事業の再開に必要な体制を早急に構築できるようにするために安否確認システムを導入しました。また、グループ全体として、事業継続のために早急に復旧すべき業務の洗い出し、優先度付け、要員の割り付けの計画を策定しています。
お客さまのシステムに障害が発生した場合の対応としては、障害情報の迅速な収集、復旧のための機器、要員手配の計画を策定しています。また、お客さまのシステムの安全な稼働を確保するためには、当社自身の基幹システムの稼働が必須ですが、これに対しては、遠隔地にバックアップセンターを設置し、対応しています。