

NTT西日本

内部統制強化に向け「安心・安全・信頼」のセキュリティソリューションを提供

急務となった内部統制への対応を支援するソリューションを提供

米巨大企業が起こした不正会計事件を契機に2002年成立した米国SOX法成立を受け、日本では2005年6月に大会社に対して内部統制システムの構築を義務化した「会社法」が、また2006年6月に上場企業に対して内部統制報告書提出の義務化を明記した「金融商品取引法」（日本版SOX法）が成立した。日本版SOX法の適用は、2008年4月以降に開始する事業年度からとなっており、内部統制の仕組みを早急に確立することが求められている。

しかし、内部統制への対応には多大なコストと時間がかかるうえ、外部コンサルタント数が不足していることもあり、一部の企業で対応が進んでいるものの、全体的には企業の対応は十分でないというのが実情である。このような状況を踏まえ、NTT西日本では、各種ソリューションサービスを提供してきたこれまでの経験・実績と、米国SOX法への対応で蓄積したノウハウを活かし、内部統制プロジェクトの立上げから、統制の文書化、テスト・評価といった内部統制対応作業に対する支援、及びNTT西日本が有する豊富なソリューションメニューを軸

に、様々な経営課題を解決できる情報システムの構築までを体系化した「内部統制支援ソリューション」を2006年12月より提供している。以下では、本ソリューションのうち、内部統制強化の重要な要素である情報セキュリティに対応したソリューションについて紹介する。

内部統制を下支えする情報セキュリティ

内部統制は、業務が不正やミスなく適正に遂行されるように、企業自らが組織を健全かつ有効・効率的に運営する体制を構築し、管理・監視していくことである。内部統制を実現するためには、適正かつ効率的な業務フローを定め、それがルール通りに遂行されているかをチェックしていく必要があり、その手段として有効なのがITの活用である。

ITによる情報システムの活用は、不正やミスの削減、業務の記録の保全、業務

の効率化など、内部統制の強化に有効である。しかし、情報システムは常にセキュリティリスクにさらされている。例えば、・セキュリティに関する基本方針がなく、社員の意識・行動に格差がある、・PCへ誰でも簡単にログインできる、・重要な電子ファイルに誰でもアクセスできる、・ログが採取されておらず、情報セキュリティ事故への対応ができない、・オフィスやサーバールームへ誰でも入室できる、といった様々なリスクが存在し、財務報告の信頼性を保証するために、情報セキュリティ対策が必須要件となっている。まさに情報セキュリティは、内部統制を下支えする重要な要素といえる（図1）。



図1 内部統制強化に必須となる情報セキュリティ

内部統制強化のための セキュリティソリューションを提供

NTT西日本では、企業経営を支援するために、セキュリティコンサルティングやセキュリティ教育といった「組織的・人的対策」から、サーバ、クライアント、ネットワーク等の「技術的対策」、ビルセキュリティ、データセンタ等の「物理的対策」、そして「監査・診断」まで、トータルにラインナップ。NTT西日本の総合力（コンサルティング力、技術力、サポート力）を活かした、企業活動に潜む様々なセキュリティリスクに対応する「安心・安全・信頼」のトータルセキュリティサービスを提供している（図2）。以下、内部統制強化に有効なソリューションのうち、いくつかを紹介する。

内部統制強化に向けた情報セキュリティ対策の最初のステップがセキュリティポリシー（基本方針）の策定である。会社（組織）として統一したルール・方針を定め、情報セキュリティの推進組織や対策基準、教育活動などの基本方針を明確にすることは、効果的で継続性のあるセキュリティ対策を実現する第一歩といえる。NTT西日本では、国際基準に準拠する「セキュリティポリシー策定サービス」に加え、ISO27001（ISMS）の「認証取得コンサルティングサービス」を提供している。

次のステップとして、内部統制の観点から、不正アクセス防止、データ改ざんの防止、情報漏えい防止などのセキュリティ対策が必要となる。

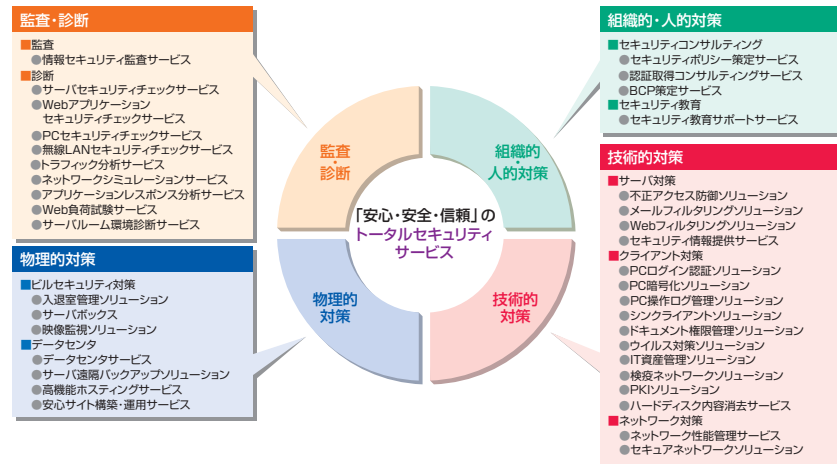


図2 「安心・安全・信頼」を提供するNTT西日本のトータルセキュリティサービス

財務データなどの重要データが格納されたサーバなどは、不正操作を防止する対策が必要不可欠である。その一つが、情報システムが置かれているサーバールームへの入退室を物理的に制限することである。NTT西日本では、顧客の環境に応じ、最適なアクセスコントロールを実現する「入退室管理ソリューション」を提供している。また、より高度なセキュリティ対策が施されたNTT西日本の「データセンタ」を活用することで、入退室の強化に加え自然災害からも重要情報を守ることができる。

物理的に制限する対策とは別に、PCへのログイン認証やPC操作のログ管理、特定ファイルへのアクセス制限も有効な対策である。NTT西日本では、PCへのログインを権限ある者のみに制限するため、ID・パスワードからICカード、生体認証まで、様々な認証方式による「PCログイン認証ソリューション」に加え、サーバやアプリケーションのアクセスログや操作履歴を記録する「PC操作ロ

グ管理ソリューション」を提供している。これは、セキュリティ事故の予防や原因究明に有効である。また、電子ドキュメントへのきめ細かなアクセス制限を実現する「ドキュメント権限管理ソリューション」を提供している。さらに、情報漏えいを未然に防止するソリューションとして、キーワードによるメール検査を行う「メールフィルタリングソリューション」を提供している。

以上、NTT西日本が提供するトータルセキュリティサービスの中から特に内部統制強化に有効と思われるものを紹介した。各サービスの詳細については、以下に問い合わせをお願いしたい。

お問い合わせ先

西日本電信電話株式会社

法人営業本部

ソリューションビジネス部

TEL：06-4803-3690

E-mail：sec-info@bch.west.ntt.co.jp

URL：http://www.ntt-west.co.jp/
solution/security/