

>>> Sarbanes-Oxley 法の遵守

LANDeskの管理ソリューションが、IT資産管理とIT全般のコントロールをいかにサポートするか。

要約

2002年に米国で成立した企業改革法であるSarbane-Oxley法(以下、SOX法)は、株式上場企業に対して、財務に関する厳格な説明責任を要求しています。この新しい標準において、組織は、内部プロセスが管理されていることを証明し、内部および外部監査の文書を証拠資料として残すことを求められます。

このようなプロセスを支えるサービス インフラストラクチャを維持するという仕事は、そのままIT部門の責任になります。サポート作業には、全社的に標準化されたソフトウェア ベースのプロセス管理および財務管理ツールの導入と運用、データの保管とバックアップとアクセス制御、プロセスの検証と報告書作成とデータ抽出、監査サポートなどが含まれます。そのほかにIT部門は、独自の財務および報告書作成プロセスをコントロールすることも求められています。

LANDesk® Management SuiteやLANDesk® Asset Managerといった自動システム管理ソリューションがあれば、ビジネス プロセスとIT資産管理および報告書作成との両方をサポートするITインフラストラクチャをよりよく管理できるようになり、SOX法などの規制による要求事項を遵守するための負荷が大幅に軽減されます。

本資料に記載されている情報はLANDesk Software 製品に関連して提供しているものです。本資料は、明示されているか否かに関わらず、また禁半言によるとよらずに関わらず、いかなる知的財産権のライセンスも許諾いたしません。これら製品の使用条件に記載されている場合を除き、LANDesk Software は、特定の目的への適合、市場性、あるいは何らかの商標、著作権およびその他知的財産権の違反に関する法的責任や保証を含む、LANDesk Software 製品の販売および/または使用に関する、いかなる責任も負わず、またいかなる保証もいたしません。LANDesk Software 製品は、医療、救命、または生命維持のアプリケーションとして使用することを意図していません。本資料およびここで述べられている技術に関連する知的財産権は第三者が所有している場合があります。またLANDesk Software の義務なしに、有能な弁護士の助言を求めてください。

LANDesk Software は、本資料または製品に関する仕様や記述をいつでも予告なく変更することがあります。LANDesk Software は本資料の使用に関していかなる保証もいたしません、また本資料のいかなる誤りにも責任を持たず、ここに記載されている情報の更新を約束するものではありません。

Copyright© 2005, LANDesk Software, Ltd. All rights reserved.

LANDesk, Targeted Multicast (ターゲットマルチキャスト)、およびPeer Download(ピアダウンロード)はLANDesk Software, Ltd. またはその子会社の米国およびその他国における登録商標または商標です。

*その他の製品名またはブランドは、それぞれ各社が所有している場合があります。

目次

要約	1
要旨	4
SOX法の概要	5
主要要素: 第302条および第404条	6
内部統制 = ビジネスのベスト プラクティス	7
ITIL、COBIT、およびITによる内部統制のサポート	7
IT統制目標の遂行:	
人、プロセス、ツール	8
セキュアな基盤	9
IT資産の知識とコントロール.....	10
システム全体のプロセス制御	10
結論	11

要旨

2002年に米国で成立したSarbanes-Oxley法(以下、SOX法)では、株式上場企業に対して、上級管理者自らが財務報告の正確さを証明するよう要求し、厳格な財務統制と文書化と監査を義務化しています。このようなプロセスや統制は監査を通じて検証し、監査結果をSEC提出書類やその他の財務開示情報として報告しなければなりません。SOX法の要求を遵守しなかった会社の最高責任者には、民事および刑事上の重大な罰則が定められています。

CEOやCFOに厳格な説明責任を求めることで、SOX法は基本的に組織に対して、一貫し、信頼性が高く、安全な、かつそのプロセスが十分に文書化された情報サービス インフラストラクチャを構築することを強めています。このインフラストラクチャを使って、財務情報開示および監査のための正確な情報を提供し、ビジネス プロセスが新しく作成されたり改定されたりした場合にはそれをすばやく実装することができます。

つまり、SOX法は経営幹部レベルのビジネス プロセスや手続きに関するものではありませんが、SOX法のプロセスや統制を確立するには効果的なITインフラストラクチャが成功への鍵となり、遵守を証明する大きな機動力となります。たいていの会社では、IT部門が、その中心的情報サービス インフラストラクチャの構築と運用を行い、内部および外部監査のためのデータ抽出や報告書作成を自動化します。それと同じくらい重要なことに、財務データやプロセス統制の品質や整合性を守るために、情報セキュリティやアクセス制御が必要となります。

LANDesk Softwareソリューションを使うことで、IT管理者は、SOX法を遵守するために必要なハードウェアおよびソフトウェア ツールをすばやく実装、運用し、しかも現行のシステムやプロセスに対する影響やコストを最低限に抑えることができます。

LANDesk®ソリューションは、SOX法の遵守に固有の懸案事項3分野に対応しています。

- 内部プロセスコントロールと財務データの維持を行うための安全な基盤の開発と運用。データ インフラストラクチャを積極的に管理することで、IT部門は、企業規模のプロセスを可能にし、データやプロセスのコントロールが正確かつ安全で利用可能であることを保証することができます。
- 一元管理されたフォーム ベースの追跡ツールを使った、高いレベルのプロセス タスク フローを企業規模で実装するためのサポート。
- 組織全体でプロセスの一貫性を保つために、標準化されたプロセスを迅速に定義し、ログや追跡を実施するツール。
- 資産報告書作成プロセスの一部として、コンピュータのハードウェアおよびソフトウェアに関する正確かつリアルタイムのインベントリ情報収集と報告書作成。これまで、IT資産に関する正確なデータを維持するのは困難でした。強力なコンピュータ検出、インベントリ、ライセンス監視のツールと、優先的状态管理および拡張資産追跡ツールを使って、IT部門は、IT資産に関する正確かつ検証済みの情報を財務担当者に提供することができます。

LANDesk Softwareの提供する柔軟で適応性の高いインフラストラクチャ管理ソリューションによって、規制による要求事項の変化にすばやく対応でき、また、組織は安全で信頼性の高い情報インフラストラクチャを作成する情報サービスをよりよく管理できるようになります。さらにこの柔軟性があることで、全体的な規制の遵守のために監査チームが勧告した新しい方針や手続きを、簡単に実装することができます。

SOX法の概要

SOX法は、企業の会計報告に関する不祥事をきっかけに施行されたもので、「証券取引法に従った企業の情報開示に関する正確性と信頼性を改善することにより投資家を保護する等の目的」を持っています。

SOX法は全11章からなり、財務報告に関する具体的な命令および要求が記述されています。

- 第I章 上場会社会計監視審議会(Public Company Accounting Oversight Board: PCAOB)
外部監査の独立した監視を定着させる。会計事務所の監査人登録、法に則った監査を行うための具体的なプロセスと手続きの定義、これら会計事務所の行いおよび品質管理の検査と取り締まり、SOX法の具体的な命令の遵守の強制、といった仕事を課せられた中央監視審議会を設置し、定義する。
- 第II章 監査人の独立
監査人が独立性を保てるようにするためのプラクティスを規定し、利害の衝突を制限する。SOX法で義務付けられた監査を行う事務所に対する要求と制限について記述する。事前承認の要求、監査人の交替方針、利害の衝突の問題、および監査人報告書の要求について記述する。
- 第III章 企業責任
上級管理者が会社の財務報告の正確性および完全性に個人的に責任を持つよう義務付ける。外部監査人と社内監査委員会とのやりとりを定義し、会社の財務報告の正確性および有効性に対する役員の実行責任を明記する。役員の実行について具体的な制限を列挙し、遵守しない場合の収益の没収および民事罰について記述する。
- 第IV章 財務情報開示の強化
財務取引(オフ バランス シート取引、会社役員の実行上のデータや証券取引など)の報告要求の強化について記述する。財務情報開示の正確性を保つための内部統制を要求し、その統制についての監査および報告を義務付ける。財務状況の重要な変化をタイムリーに報告することを要求し、SECまたはその代理人による企業報告の検査の強化を明記する。
- 第V章 アナリストの利害の衝突
証券アナリストに対する投資家の信頼を回復し、報復からアナリストを守るための要求を規定する。証券アナリストの実行規範を定義し、知り得た利害の衝突の情報開示を要求する。
- 第VI章 委員会の財源および権限
証券アドバイザーに対する投資家の信頼を回復するためのプラクティスを規定する。証券の専門家を譴責し、プラクティスから除外するというSECの権限を定義し、SEC標準違反で見つかった人々による安値株の売却を拒む権限を規定し、ブローカーやアドバイザーやディーラーの業務を停止する条件を定義する。
- 第VII章 研究および報告
SOX法が可決される原因となった企業の不祥事を誘発し放置した規制の状況を分析するために諸官庁が公表する、一連の研究および報告を定義する。この研究および報告には、会計事務所の合併の効果、証券市場の運用における格付け機関の役割、証券違反と施行のための措置、エンロン(Enron)やグローバル クロッシング(Global Crossing)などが収益を不正操作し正確な財務状況をごまかすのに投資銀行が加担したかどうか、などが含まれる。
- 第VIII章 企業と不正犯罪行為の説明責任
「2002年の企業および不正犯罪行為説明責任法(Corporate and Criminal Fraud Act of

2002)」とも呼ばれる。財務記録の操作、破棄、改竄による不正行為、あるいはその他の捜査妨害に対する具体的な刑事罰について記述する。内部告発者の確実な保護を規定する。

- 第IX章 ホワイトカラー犯罪に対する罰則強化
「2002年のホワイトカラー犯罪罰則強化法(White Collar Crime Penalty Enhancement Act of 2002)」とも呼ばれる。ホワイトカラー犯罪および陰謀に関する刑事罰を強化する。より厳しい判決指針を推奨し、特に企業の財務報告の証明不履行を刑事犯罪として追加する。
- 第X章 法人税の還付
CEOが法人税の還付に署名しなければならないことを明記する。
- 第XI章 企業の不正と説明責任
「2002年の企業不正行為説明責任法(Corporate Fraud Accountability Act of 2002)」とも呼ばれる。特に企業の不正および記録の改竄を刑事犯罪であるとし、これらの犯罪に具体的な罰則を設ける。判決指針を改定し、罰則を強化する。多額または異例の支払いを一時的に凍結する権限をSECに与える。

企業のIT部門にもっとも大きな影響を直接及ぼすのは第302条と第404条です。

主要要素: 第302条および第404条

第302条および第404条は、事実上、正確な財務データが投資家、監査人、およびSECに定期的な報告書として提供されること、そこで提供されるデータと内部統制プロセスの両方が外部監査によって検証されていることを保証するよう、最高責任者に要求しています。

第302条は、四半期または一年ごとの財務報告のもととなる内部統制について、個人的に責任を取るようCEOおよびCFOに要求しています。役員はこれらの報告書に署名することで、はっきりと以下のことを証明することになります。

- 報告書が最新、正確、完全であり、財務状況について事実と異なる記述をしたり曲げて述べたりしていないこと。
- 情報が正確になるよう、企業の内部統制が策定、実施、保守されていること。
- 最新の財務状況を企業役員にはっきりと知らせるよう、内部統制が策定されていること。
- 報告書の作成前90日以内に内部統制の効果が評価されており、その評価の結果が報告書に反映されていること。
- 最新の財務データの正確性や可用性を損なう可能性のある内部統制の欠陥や弱点が、報告書準備中の監査人および監査委員会に報告されていること。
- それらの欠陥を修正するために内部統制を最近変更した場合は、それが報告書自体に文書化されていること。

第404条は、企業の年次報告書の一部として内部統制報告書を準備するよう要求しています。また、この内部統制報告書は、内部統制の正確性と効果を検証し、欠陥の修正を勧告する監査人に届けなければなりません。

財務情報の正確性に関する個人的責任を最高責任者と監査人の両方に集中させることで、SOX法は本質的に、組織に内部ビジネスプロセスと情報インフラストラクチャの両方を直接積極的に統制するよう強いており、行わなければ民事および刑事上の重大な罰則が課せられることとなります。

これはIT部門にとってどのような意味を持つのでしょうか。報告書はその元となったデータと同じだけの

価値しかありません。上級管理者が、企業報告に含めるデータを集める各部門にこれまで以上に厳しい説明責任を要求するため、IT部門はプレッシャーを感じるでしょう。ITシステムがほとんどすべての部署の作業を支えているため、ITはこれまで以上に関心を集め、詳しい調査を受けることになります。

内部統制 = ビジネスのベスト プラクティス

SOX法は基本的に組織に対して、一貫し、信頼性が高く、安全な、かつそのプロセスが十分に文書化された情報サービス インフラストラクチャを構築することを強めています。このインフラストラクチャを使って、財務情報開示および監査のための正確な情報を提供し、ビジネス プロセスが新しく作成されたり改定されたりした場合にはそれをすばやく実装することができます。

SOX法自体が内部財務統制を制定し評価するための特定の標準を義務化しているわけではありませんが、一般の人々に簡単に手に入る一般に認められた標準を満たすよう、会社に要求しています。トレッドウェイ委員会組織委員会(COSO*)が制定した指針は、SOX法に指定された内部統制の要求を満たす全般統制フレームワークの一例です。しかし、これらの統制に関する報告の責任は、まだ個々の会社に任されています。

COSOとSOX法の関係について詳しくは、Sarbanes-OxleyのWebサイトで以下の『Discussion of Amendments Implementing Section 404』を参照してください。

http://www.sarbanes-Oxley.com/displaysection.php?level=2&pub_id=SEC-Rules&chap_id=SEC14&message_id=269

これはIT部門にとってどのような意味を持つのでしょうか。現代の会社では統制フレームワークは技術ソリューションによって支えられており、そのソリューションの基盤となるインフラストラクチャを実装し保守する責任を担っているのはIT部門です。ITILやCOBITといった一般に認められたITサービス管理フレームワークおよび標準への動きは、IT部門から始まり、徐々に社内にも広まっていく、主体的な取り組みであるべきです。SOX法は、標準にもとづいたIT管理基盤の必要性を理解し、願わくは支援することを、上級管理者に強いています。

ITIL、COBIT、およびITによる内部統制のサポート

SOX法は上級管理者のビジネス プロセスや財務手続きに関するものではありませんが、SOX法統制を制定するには効果的なITインフラストラクチャが成功への鍵となり、遵守を証明する大きな機動力となります。

PCAOB発行、SEC承認の『監査基準第2号』では、統制全体の効果を判断する上でのITをコントロールする構造の重要性が、第50項で述べられています(強調を追加)。

コントロールの中には(第53項で述べる企業レベルの統制など)、統制基準の全体的目標の多くを達成するために幅広い効果を持つものがある。たとえば、プログラム開発、プログラム変更、コンピュータ運用、プログラムやデータへのアクセスに関する情報技術全般をコントロールすることによって、取引の処理に対する特定の統制を効果的かつ確実に実施することができる。

特定の監査機能にITコントロールが及ぼす可能性のある影響については、第105項で述べられています。

コントロールの本質。監査人は、自動化されたコントロールよりも手作業によるコントロールの方を、より広範囲にテストしなければならない。状況によって、情報技術全般に対するコントロールが効果的に働いているのであれば、自動化されたコントロールのうち1つの動作をテストするだけで、コントロールが効果的に働いていることを高いレベルで十分に保証できることがある。

(PCAOB監査基準の全文はhttp://www.pcaobus.org/Rules_of_the_Board/rules_of_the_board.asp)

を参照してください。)

多くの会社では、IT部門が、財務コントロールの構造を支える中心的情報サービス インフラストラクチャの構築と維持を行い、内部および外部監査のためのデータ抽出や報告書作成を自動化します。それと同じくらい重要なことに、財務データやプロセスのコントロール品質や整合性を守るために、情報セキュリティやアクセス制御が必要となります。

その結果、多くの企業が、全社的にITをコントロールするフレームワークを使って、ビジネスや規制の状況の変化にすばやく対応できるよう特別に設計された、情報サービス インフラストラクチャを開発しようとしています。ITインフラストラクチャ ライブラリ(IT Infrastructure Library:ITIL)は、総合的なサービスの可用性を支える効果的な内部ITコントロールを開発するための、もっとも有名で広く受け入れられている標準です。

ITILは、情報技術統制目標(Control Objectives for Information and related Technology:COBIT*)ガイドラインなどのIT統制フレームワークの基礎となっています。COBITは特に、情報の依存の問題とその依存がビジネス プロセスにどう影響するかに取り組んでいます。さらに重要なのは、COBITが監査報告や要求を扱っていて、SOX法が要求する内部プロセス統制を遵守するためのITベースの基礎となる十分なフレームワークを提供していることです。

ITコントロール目標の遂行:人、プロセス、ツール

一般的な標準はどれもそうですが、ITILやCOBITも、人とプロセスとツールを組み合わせ、ITおよびビジネスのベスト プラクティスを可能にしています。テクノロジーという魔法の弾丸が使われているわけではありません。ビジネス目標全体をサポートできるITのコントロール プロセスを実装しているのです。そこでは、CEOやCFOやCIOが、協力して中心的技術システムを計画、評価、改善、最適化するだけでなく、データ抽出を自動化してデータの安全性と整合性を保証するには組織全体でこれらのシステムをどう使えばよいかを判断することが求められます。

LANDesk Softwareソリューションを使うことで、IT管理者は、SOX法を遵守するために必要なハードウェアおよびソフトウェア ツールをすばやく実装、維持し、しかも現行のシステムやプロセスに対する影響やコストを最低限に抑えることができます。

LANDeskソリューションは、SOX法の遵守に固有の次の3つのことがらに対処しています。

- 内部プロセスのコントロールと財務データの維持を行うための安全な基盤の開発と維持。データ インフラストラクチャを積極的に管理することで、IT部門は、企業規模のプロセスを可能にしたり、データやプロセスのコントロールが正確かつ安全で利用可能であることを保障したりすることができます。
- 中央に置かれたフォーム ベースの追跡ツールを使った、高いレベルのプロセス タスク フローを企業規模で実装するためのサポート。
- 組織全体でプロセスの一貫性を保つための、標準手続きのすばやい定義、ログおよび追跡ツール。
- 資産報告書作成プロセス全体の一部としての、コンピューティング ハードウェアおよびソフトウェアに関する正確かつリアルタイムのインベントリおよび報告書作成の実現。これまで、IT資産に関する正確なデータを保守するのは困難でした。強力なコンピュータ検出、インベントリ、ライセンス監視のツールと、優先的状态管理および拡張資産追跡ツールを使って、IT部門は、IT資産に関する正確かつ検証済みの情報を財務担当者に提供することができます。

LANDesk Softwareの提供する柔軟で適応性の高いインフラストラクチャ管理ソリューションによって、規制による要求事項の変化にすばやく対応でき、また、組織は安全で信頼性の高い情報インフラ

ラクチャを作成する情報サービスをよりよく管理できるようになります。さらにこの柔軟性があることで、全体的な規制の遵守のために監査チームが勧告した新しい方針や手続きを、簡単に実装することができます。

セキュアな基盤

スプレッドシートを使って財務データを手作業で集計している場合でも、ERPシステムを使っていたりSOX法向けに最適化された財務統制および報告書作成システムを実装していたりする場合でも、現代のワークフローやデータ処理の基盤を構成しているのは技術です。

COBITは、SOX法が要求するデータの可用性および正確性を保証するための、ITシステムに関する一連のコントロール目標を指摘しています。LANDesk管理ソリューションは、以下のような調達と導入、提供と支援の目標のための基盤コントロールの目標遂行を、直接的にサポートしています。

- AI2 アプリケーション ソフトウェアの調達とメンテナンス
- AI3 技術インフラストラクチャの調達と保守
- AI5 システムの導入と受入信任

LANDesk® Management Suiteを使うことで、セキュアで対象の絞られたアプリケーション配布、アプリケーション自動修復およびリモート問題解決が可能になります。自動パッチ管理とポリシー ベースのアプリケーションのメンテナンスを、高度なアプリケーション可用性技術と組み合わせて、会社全体の利害関係者用のソフトウェアの導入とメンテナンスを自動化します。

- AI6 変更管理

LANDesk® Management Suiteは、詳細なハードウェアおよびソフトウェア インベントリと変更管理アラートを組み合わせることで、IT部門に各管理対象コンピュータの運用環境の変化を知らせます。ポリシー ベースの管理とアプリケーション自動修復によって、各コンピュータ上の好みの設定を保持することができ、アプリケーション起動拒否によって、望まない変更がシステムに影響するのを防ぐことができます。

- 拡張インベントリ クエリおよびレポート作成を使うと、廃止、アップグレードやリプレースをスムーズに計画することができます。アプリケーションおよび個人設定の移行が可能なOSの自動配布を使うと、生産性の損失やダウンタイムを最低限に抑えながらのリプレースが容易になります。ポリシー ベースのアプリケーション管理を使うと、ソフトウェア設定を自動化でき、IT環境を制御しながら拡張することができます。
- DS3 性能と容量の管理
- DS4 継続的サービスの保証
- DS5 システム セキュリティの保証

LANDesk® System Manager(英語版のみ)を使うと、障害の予測分析用のリアルタイムのパフォーマンス監視が可能になり、問題アラート機能により、IT部門は迅速な対応をして継続的サービスを保証することができます。また、パフォーマンス履歴の傾向を見ることで、パフォーマンスが落ちた場合に容量を拡張する必要があると気づくことができます。

構成管理とソフトウェア配布は、ソフトウェアベースのシステム セキュリティ基準の展開と維持を自動化します。また、モデムおよびUSBポートの監視によって権限のないデータ転送が行われないう保護します。役割ベースの管理とイベント ログによって、IT部門が特定のシステムにアクセスできないようにし、どの管理ユーザがどのアクションを行ったかを監査します。

- DS9 構成管理

LANDesk® Management Suiteでは、詳細インベントリと、ソフトウェア ライセンス監視、ソ

ソフトウェア配布、OS配布、自動パッチ管理、および変更管理アラートが使われていて、IT部門はすべての管理対象コンピュータの設定をしっかりと制御することができます。アプリケーション修復とポリシーベースの構成管理を使えば、システム設定を自動的に保守することができます。

■ DS10 問題と事故の管理

広範なリモートコントロール、ファイル転送、チャット、リモート実行、リモート電源制御によって、システムのほとんどの問題や事故に直接かつ迅速に対処できます。RemedyやBMCといった一流のヘルプデスクベンダーと直接統合されているため、直接の構成管理および管理機能でタスク中心の問題解決を拡張し、効果的に問題を識別、追跡、解決、報告することができます。

(COBITとその目標および手法に関するより詳しい説明は、IT Governance Instituteの『COBIT Control Objectives』第3版を参照してください。)

LANDesk管理ソリューションを使うことで、IT部門は、インフラストラクチャ計画、インベントリ、構成管理、問題解決、およびキャパシティ管理を直接コントロールし、財務コントロールを構築、実装するためのセキュアな基盤を作成、運用することができます。

コントロールされたセキュアなIT基盤があれば、会社は、コンサルタントに勧められたことを迅速に実施し、規制の変更にも一貫した方法ですばやく対応することができます。

IT資産の知識とコントロール

構成管理と問題解決を効果的に行うには、システムハードウェア、ソフトウェア、構成、パフォーマンスといった、IT資産に関する広範な知識が重要になります。この資産情報は、パフォーマンス管理だけでなく、財務報告や資産管理に関係しているという点でも重要です。

LANDesk@マネジメントソリューションの特徴に詳細デバイス検出があり、IT部門はこれを使ってネットワーク上で動いているコンピュータ資産を探し出すことができます。拡張されたハードウェアおよびソフトウェアインベントリでは、資産を直接識別し、文書化することができます。詳細なソフトウェア利用状況の監視およびアラート機能では、ライセンス契約をより厳しく管理し、今後のソフトウェア購入計画を効果的に立てることができます。拡張インベントリクエリおよびレポート作成機能を使うと、すばやく正確な洗い出しとレポート作成によって内部および外部監査をサポートすることが可能です。

これらをプロセス管理ツールや統一されたIT資産リポジトリと組み合わせることで、IT部門は、財務コントロールに直接対応し、資産と減価償却の両方を文書化することができます。カスタムデータ収集、契約やリースの管理、およびサービス履歴の管理によってIT支出の詳細な財務会計がサポートされていて、これまで困難だった仕事を直接制御することができますようになります。

システム全体のプロセスコントロール

ITコントロールの構築は財務コントロール全体の開発および文書化の一部ではありませんが、多くのITツールを応用することで、ビジネスプロセス全体に付加価値を付けることができます。

たとえば、システムのアクセス制御とデータセキュリティを作成すると、IT設定だけではなく、財務コントロールも保護することができます。システムイベントログも、説明責任を強化し、情報インフラストラクチャ全体の統制を証拠付ける監査証跡となります。同様に、IT資産管理のための中央でのドキュメント格納や情報収集を拡張することで、部門や地域を横断する会社全体のプロセスをサポートすることができます。一貫した正確な記録管理やプロセス管理が可能になります。

LANDesk® Asset Managerは拡張可能なフォーム ベースのツールで、これをカスタマイズすればほとんどのようなビジネス プロセスもサポートすることができます。中央で行うタスクのチェックリストを作成し、主要な作業のログを記録します。IT資産管理がサポートしている中央の場所にプロセス情報を格納して、主要なプロセスやポリシーを皆が同じように理解できるようにし、セキュアで一元化された情報収集とプロセス レポートの作成を行います。システムはIT資産管理に合わせて最適化されていますが、全般プロセス コントロールや文書化を暫定的にサポートすることは可能です。

結論

SOX法によって、会社にビジネス プロセスの統制が義務付けられ、違反すれば厳しい罰則が課せられることになりました。ビジネス プロセスおよび内部財務コントロールの実現や文書化は複雑な仕事であり、CEO、CFO、CIOは連携して、特定のニーズに最適化された一貫したシステムを開発する必要があります。

1つの魔法の弾丸でSOX法を遵守できるわけではありませんが、強力でセキュアなIT基盤があれば、遵守のための作業のスピードが向上し、より高レベルのプロセス制御が可能になって、内部および外部監査をサポートすることができます。LANDesk®の管理製品群を使うことで、会社は、ITシステムをコントロールして、規制で義務付けられた特定の財務コントロールが可能になるようなコントロール全般を実装することができます。また、セキュアかつ柔軟で一貫したITインフラストラクチャを作成して、ビジネスや規制の状況の変化により早く順応することが可能になります。

LANDeskの管理ソリューションの詳しい情報については、LANDeskエキスパート ソリューション パートナまでお問い合わせください。また、当社Webサイト(www.landesk.co.jp)でも、一流のシステム管理ソリューションを紹介しています。

