



チェック・ポイントのソリューションで実現する SOX法第404条の遵守

Contents

本書の内容

概要	3
目的	4
背景	4
実効性のある内部統制に必要な構成要素	5
統制環境	5
リスク評価	5
統制活動	5
情報と伝達	5
監視活動	5
分析	6
COBITの統制目標とチェック・ポイントのソリューションとの対応	6
まとめ	12

概要

近年、大きな注目を集めている法令遵守は、ほとんどの組織にとって、多くの犠牲を伴う課題です。なぜならこれは、企業全体のみならず経営幹部にも影響を与える可能性があるからです。現在では、ますます多くの法令によってプライバシーの保護、消費者および事業に関する情報リソースへのアクセスの安全性確保、およびそれらの情報リソースの完全性確保が正しくなされていることを証明できるようにしておくことが企業に求められています。その中で特に注目を集めているのが、Sarbanes-Oxley Act of 2002 (サーベンス・オクスリー法：米国企業改革法、略称SOX法)です。SOX法は、著名な企業による会計スキャンダルが次々と明るみに出る中で、株主と一般市民を保護するために制定されました。この法律では、企業の責任の範囲を拡大し、開示される財務情報の妥当性を高め、企業による不正行為や粉飾決算を防ぐための、さまざまな改善策が定められています。

すでに多くの企業が認識しているように、SOX法の遵守は、財務処理に関するプロセス管理や文書化の問題に留まりません。SOX法で定められたこれらの新しい規定を満たすうえでは、ITセキュリティが重要な役割を担うようになっています。そしてその結果として、SOX法を遵守するために、膨大な時間と予算がセキュリティ技術、ツール、および情報資源に費やされています。チェック・ポイントのセキュリティ・ソリューションは、情報リソースの保護とSOX法の遵守を実現するための、最も実績のある統一されたセキュリティ・アーキテクチャを提供します。

目的

この技術白書では、Sarbanes-Oxley Act of 2002（サーベンス・オクスリー法：米国企業改革法、略称SOX法）の第404条の背景について概説し、チェック・ポイントのソリューションとCOBIT（ITセキュリティと統制のベスト・プラクティスとして広く利用されているガイドライン）のプロセス統制目標を用いてSOX法の規定を満たす方法について説明します。注意する必要があるのは、手っ取り早くSOX法第404条を遵守する方法はないということです。企業は、財務報告の妥当性を保証するために必要な相当の注意義務を果たしたことを経営上層部と外部監査人が相互に承認することによって、法令の遵守を証明する必要があります。

背景

SOX法は、企業の財務報告の質および妥当性を改善することを目的とした複数の条項から構成されています。ITの役割に直接的に影響するのは、第404条の「Management Assessment of Internal Controls（経営陣による内部統制の評価）」です。第404条では企業に対し、毎年次の事項を報告するように義務付けています。

- 財務報告に対する適切な内部統制を確立および維持するための経営陣の責任
- 財務報告に対する内部統制の有効性を評価する基準として用いるフレームワーク
- 財務報告および重大な欠陥の開示に対する内部統制の有効性についての経営陣の評価

第404条はまた、これらの報告書（その企業のCEOおよびCFOによる署名がなされたもの）の正確性を、外部監査人が証明することも義務付けています。

SOX法のための内部統制は、財務報告、および外部向けの決算報告書の準備が、一般会計原則（GAAP）に従ったものであることを合理的に保証するためのプロセスです。統制の対象となるのは、取引の記録、取引記録の保持、報告に「不可欠」と考えられる資産の取得、使用または譲渡などです。一部の統制は、これらの行為に直接影響します。一般的な（「広範囲にわたる」）統制は、すべての行為に適用される汎用規則となります。広範囲にわたる統制には、ITセキュリティに対する統制（財務報告に固有のものではないが、情報の妥当性を保証する統制としての役割を担う汎用的な機能および統制）が含まれます。

米証券取引委員会（SEC）では、内部統制の評価には、公開の適正手続を通じて確立された、適切かつ一般に認められたフレームワークを用いる必要があるとしています。SECは、この条件に合致するフレームワークの1つとして、COSOの「Internal Control-Integrated Framework（内部統制の統合的フレームワーク）」を挙げています。

今日では、財務および業務管理システムでのIT利用が広範囲に広がっており、IT統制でいかにしてCOSOフレームワークをサポートするかが重要となります。組織は、COSOフレームワークのすべての構成要素においてIT統制能力を備えていなければならないのです。

実効性のある内部統制に必要な構成要素

COSOフレームワークでは、実効性のある内部統制に必要な構成要素として、次の5つを挙げています。

- 統制環境 (Control environment)
- リスク評価 (Risk assessment)
- 統制活動 (Control activities)
- 情報と伝達 (Information and communication)
- 監視活動 (Monitoring)

統制環境は、実効性のある内部統制を行うための基盤となり、「tone at the top (経営者の理念)」を確立し、企業のガバナンス構造の最上位層を表すものです。この構成要素から生じる問題は、組織全体に影響します。

リスク評価では、(統制活動を決定する際の基盤となる) 事前に設定した目標を達成するうえでのリスクを経営陣が識別および分析します。

統制活動は、企業の目標を達成し、リスク軽減計画を実施するためのポリシー、手続き、およびプラクティスです。統制活動は、各統制目標を達成して識別されたリスクを軽減することを目的として策定します。

情報と伝達は、事業を運営し、その統制目標を達成するために、組織内のすべてのレベルで必要になります。統制目標を達成するために必要な情報は何かを判断し、人々が自らの責務を全うできるような形式および時間枠でその情報を伝達することが、COSOフレームワークにおける他の4つの構成要素をサポートするために重要です。

監視活動では、内部統制の効果を長期的にわたって評価します。継続的な評価、およびある時点における評価を通じて、経営陣による内部統制の不備を補います。

SOX法の規定を満たす内部統制を確立するうえでは、IT全般、特にITセキュリティが重要な役割を果たします。しかしながら、SOX法とCOSOフレームワークのどちらも、企業がITセキュリティを活用して内部統制を確立するための具体的な方法には言及していません。そのため、COSOフレームワークと併せて用いるもう一つのフレームワークが必要になります。その例としては、「Control Objectives for Information and related Technology (COBIT) 4.1 Edition」と「ISO 17799: Code of Practice for Information Security Management (情報セキュリティ管理実施基準)」が挙げられます。

COBITは、企業レベルおよび活動レベルの目標と、それに付随する統制についての基準を提供するITガバナンス・モデルです。COBITにより、SOX法第404条を遵守するためのIT統制の仕組みを設計することが可能になります。

分析

この技術白書では、その目的に照らして、COBITで説明されている統制目標 (Control Objectives) のみを扱います。統制目標は、ほとんどのIT組織に適した事実上の標準と見なされているためです。

注意する必要があるのは、上述のフレームワークやドキュメントは、「確実にSOX法の遵守につながる」という方法論を提供しているわけではないということです。実際のところ、ほとんどの企業は、(外部監査人の同意の下で) 自社固有の財務報告プロセスに合わせてカスタマイズしたフレームワークを使用することになります。

次の項では、COBITのいくつかの統制目標と、これらの統制目標の達成に貢献するチェック・ポイントのセキュリティ・ソリューションについて説明します。

COBITの統制目標とチェック・ポイントのソリューションとの対応

下記の表は、COBITの統制目標のうち、「サービス提供とサポート：システムのセキュリティの保証 (Delivery and Support: Ensures Systems Security: DS5)」および「監視活動 (Monitoring: M)」と、それに対応するチェック・ポイントのソリューションをまとめたものです。ただし、企業の実環境はそれぞれ異なるため、各企業は、自社のリスクおよび統制を評価して、SOX法を遵守するための自社固有の要件を判断する必要があることに注意してください。

COBITの統制目標	チェック・ポイントのソリューション
<p>DS5.3: ID管理 (Identity Management)</p> <ul style="list-style-type: none"> ● すべてのユーザを一意に識別できるようにする。認証メカニズムによりユーザの識別を可能にする。 ● ユーザIDおよびアクセス権を中央リポジトリで管理する。 ● ユーザの識別、認証の実施、およびアクセス権の運用管理を行うための費用対効果に優れた技術的・手続的な方策を導入し、これらを常に最新の状態に保つ。 	<p>アクセス制御の機能は、チェック・ポイントのすべてのセキュリティ・ソリューションが基本機能として備えています。チェック・ポイントの境界、内部、Web、およびエンドポイント向けのソリューションでは、きめ細かなアクセス・ルールと権限付与ルールを作成することができます。VPN-1®とInterSpect™は、境界と内部ネットワーク上でアクセス・ポリシーを実施します。Connectra™とVPN-1は、境界の外にいるユーザにリモート・アクセスを許可する際にアクセス・ポリシーを実施します。Check Point Endpoint Securityは、デスクトップ・ファイアウォール・ルールとネットワーク・ゾーンを使用して、ネットワーク・リソースおよびネットワーク・セグメントへのPCアクセスを制限します。これらのアクセス・ポリシーでは、個人、グループ、または部門に対してどのリソースへのアクセスを許可するかを定義します。</p> <p>チェック・ポイントのVAR、SI、およびビジネス・パートナーは、チェック・ポイントのソリューションを用いて、DS5.3に規定されているアクセス制限に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>

COBITの統制目標	チェック・ポイントのソリューション
<p>DS5.4: ユーザ・アカウント管理 (User Account Management)</p> <ul style="list-style-type: none"> ● ユーザ・アカウントおよびそれに付随するユーザ権限の申請、作成、発行、一時停止、変更、抹消は、ユーザ・アカウント管理のための一連の手続きに基づいて行う。 ● すべてのアカウントおよびそれに付随する権限について、経営陣による検証を定期的に行う。 	<p>チェック・ポイントの管理ツールでは、ユーザやエンドポイントで構成されるグループのリソースへのマッピングおよび割り当てなどを行うためのポリシーを作成することができます。すべてのチェック・ポイント製品では、複数のゲートウェイにまたがるユーザ・アクセスや、管理者がシステムに対して行った変更をログに記録し、レポートを作成することができます。この情報は、SmartViewTracker™またはEventia™ Reporter™で確認できます。</p> <p>VPN-1などのVPNソリューションを始めとするチェック・ポイントのソリューションは、いずれも認証機能を備えています。VPN-1は、認証用に複数のデータベース(内部データベース、Microsoft Active Directory、OPSEC認定LDAP/RADIUSデータベースなど)をサポートしています。</p> <p>チェック・ポイントのIPS-1™は、インラインでリアルタイムのパスワード・ポリシー検証(パスワードの長さや英数字の組み合わせに関する要件を満たしているかどうかなど)を行うように設定できます。</p> <p>チェック・ポイントのVAR、SI、およびビジネス・パートナーは、各ユーザに一意のIDを割り当てるIDプログラムをチェック・ポイントのソリューションと連携させるためのコンサルティング・サービスを提供しています。</p>

COBITの統制目標	チェック・ポイントのソリューション
<p>DS5.5: セキュリティの検査、監督、監視 (Security Testing, Surveillance and Monitoring)</p> <ul style="list-style-type: none"> ● 予防的措置として、ITセキュリティ機能の検査および監視を行う。 ● ログイングおよび監視の機能を使用することにより、何らかの対応が必要となる例外的・異常な活動を抑制、あるいは早期に発見し、適宜報告を可能とする。 	<p>チェック・ポイントのSmartCenter™とEventia Suite (Eventia ReporterとEventia Analyzer™)は、システム・イベントおよびアクティビティのログイング、アップデート、監視、レポートを一元化することにより、セキュリティ・アクティビティおよびネットワーク・アクティビティの全体的な傾向を把握できるようにします。組織全体のデータが統一形式で表示されるため、より効率的なデータの収集、分析、および対応が可能になります。</p> <p>Eventia Suiteは、すべてのチェック・ポイント製品および多種多様なサードパーティ製品で記録されたログとイベント・アクティビティについて、収集、監査、相関分析、およびレポート作成を行います。Eventia Reporterは、各種の情報を収集し、複数の製品にまたがる攻撃、ブロックしたトラフィック、ログイン・アクティビティ、およびネットワーク・アクティビティについてレポートします。</p> <p>Eventia Reporterのエンドポイント・セキュリティ・レポートでは、Check Point Endpoint Securityのデータ (ポリシー違反、ファイアウォール・イベント、ブロックしたプログラム、Check Point Endpoint Security MailSafe™ イベント、スパイウェア、Malicious Code Protector™の結果、およびクライアント・エラーなど) についての統一レポートが提供されます。Eventia Reporterは、アンチウイルス・アクティビティ、Connectra、InterSpect、およびVPN-1 Power VSX™ログ・レポートについてのレポートも提供します。</p> <p>IPS-1 Dashboardは、オペレーティング・システム (OS)、アプリケーション・サーバ、およびネットワーク・デバイスのあらゆる脆弱性をまとめた現在のランキングを、バージョン/パッチ・レベルで管理するVulnerability Browserを備えています。この脆弱性リストは、SmartDefense™およびIPS-1のパッシブOSフィンガープリンティングにより、継続的に更新されます。</p> <p>Eventia Suiteでは、データへのユーザ・アクセス、管理者が行った操作、無効な論理的アクセスの試みなどについての監査証跡を記録することができます。Eventia Analyzerは、監査ログの初期化と監査情報への安全なアクセスをサポートし、システム・レベル・オブジェクトの作成と削除にも対応しています。また、監査ログが初期化されたときや、システム・オブジェクトが作成または削除されたときにアラートを生成することもできます。</p>

COBITの統制目標	チェック・ポイントのソリューション
<p>DS5.6: セキュリティ・インシデントの定義 (Security Incident Definition)</p> <ul style="list-style-type: none"> インシデント/問題管理プロセスにおいて適切な分類と対応を行えるように、起こり得るセキュリティ・インシデントの特性を明確に定義し、関係者に周知する。 	<p>SmartDefenseとWeb Intelligence™技術は、Connectra、Check Point Endpoint Security、およびVPN-1の一部として侵入防御機能を提供します。SmartDefenseサービスにより、侵入防御エンジンを常に最新の状態で維持することができます。</p> <p>Eventia Analyzerは、セキュリティ・インシデントの識別、対応、およびレポートを包括的にサポートするための機能を提供します。Eventia Analyzerは、チェック・ポイントのソリューションおよび広く使用されているセキュリティ・デバイスが生成するログ・データをほぼリアルタイムで分析し、ネットワーク上に存在する深刻な脅威を識別します。セキュリティ・イベントの検出時には、事前設定された内容に応じて、アラートを生成する、レポートを作成する、または検出された脅威の影響を軽減するために適切なアクションを実行するといった処理を行うことができます。Eventia Reporterでは、セキュリティ・イベントのリアルタイム・レポート、履歴レポート、傾向分析レポートを作成する機能が提供されます。</p> <p>ミッション・クリティカルな環境に対応する侵入防御専用のIPSソリューションであるIPS-1は、きめ細かなフォレンジック分析機能を備え、さまざまな導入形態に柔軟に対応します。IPS-1の中核機能である脅威記述言語、N-Code™は、複合ロジックを用いてプロトコル要素とアプリケーション要素を検査および相関分析する独自の機能を提供します。これにより、複雑な検査ルールが簡潔で効率的なルールに置き換えられると共に、高い拡張性と柔軟性が実現されます。</p> <p>高機能なブラウザ・ベースの管理ツールまたはSmartCenterのタブ・コンポーネントとして機能するIPS-1 Dashboardは、内蔵の脆弱性評価ツールによって重み付けされた侵入関連のあらゆるイベントを網羅的に把握するためのビューを提供します。IPS-1 Dashboardでは、ネットワークで発生したイベントを時系列で高レベルから把握できます。そして、これらのイベントをドリルダウンすることにより、パターンや不審なアクティビティをバケット・レベルまたはルール・レベルで調べることができます。</p>
<p>DS5.7: セキュリティ技術の保護 (Protection of Security Technology)</p> <ul style="list-style-type: none"> セキュリティ関連の技術が改ざんされることのないように対策を講じる。 	<p>アクセス制御の機能は、チェック・ポイントのすべてのセキュリティ・ソリューションが基本機能として備えています。チェック・ポイントの境界、内部、Web、およびエンドポイント向けのソリューションでは、きめ細かなアクセス・ルールと権限付与ルールを作成することができます。VPN-1とInterSpectは、境界と内部ネットワーク上でアクセス・ポリシーを実施します。ConnectraとVPN-1は、境界の外にいるユーザにリモート・アクセスを許可する際にアクセス・ポリシーを実施します。Check Point Endpoint Securityは、デスクトップ・ファイアウォール・ルールとネットワーク・ゾーンを使用して、ネットワーク・リソースおよびネットワーク・セグメントへのPCアクセスを制限します。これらのアクセス・ポリシーでは、個人、グループ、または部門に対してどのリソースへのアクセスを許可するかを定義します。</p> <p>チェック・ポイントのVAR、SI、およびビジネス・パートナーは、チェック・ポイントのソリューションを用いて、DS5.7に規定されているセキュリティ関連技術の改ざん防止に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>

COBITの統制目標	チェック・ポイントのソリューション
<p>DS5.9: 悪意あるソフトウェアの抑止、検出、是正 (Malicious Software Prevention, Detection and Correction)</p> <ul style="list-style-type: none"> ● ウイルス、ワーム、スパイウェア、スパムなどのマルウェアから情報システムや技術を保護するため、組織全体にわたり、それらを抑止、検出、是正するための対策を講じる (最新のセキュリティ・パッチやウイルス・シグネチャを適用するなど)。 	<p>UTM-1ファミリ (UTM-1, UTM-1 Edge™) およびVPN-1ファミリ (VPN-1 UTM™, VPN-1 UTM Power™) には、ゲートウェイ・ベースのアンチウイルス機能が統合されています。ゲートウェイ・ベースのアンチウイルス機能は、個々のPCやサーバに導入されているアンチウイルス・ソリューションを補完し、より広範な脅威に対処できるようにします。</p> <p>Check Point Endpoint Securityには、ウイルスなどのマルウェアを検出してエンドポイントPCから駆除する高性能なアンチウイルス技術が統合されています。ウイルス検出は、シグネチャ、振る舞いブロック機能、およびヒューリスティック分析機能を組み合わせて行われるため、業界最高レベルの検出率が実現されています。また、世界規模で活動するマルウェア専門の研究者チームが、1時間おきに新しいシグネチャを公開するなど、24時間365日の積極的な対応を行います。</p> <p>チェック・ポイントのVAR、SI、およびビジネス・パートナーは、チェック・ポイントのソリューションを用いてこの条項の要件に対処したり、導入済みのアンチウイルス・ソリューションとチェック・ポイントのソリューションを連携させたりするためのコンサルティング・サービスを提供しています。</p>
<p>DS5.10: ネットワーク・セキュリティ (Network Security)</p> <ul style="list-style-type: none"> ● セキュリティ技術およびそれに付随する管理手続き (ファイアウォール、セキュリティ・アプライアンス、ネットワークのセグメント化、侵入検出など) を用いて、ネットワークへのアクセス許可とネットワークの情報フローを制御する。 	<p>業界最高レベルの実績を誇るステートフル・ファイアウォール・ソリューション、VPN-1 (FireWall-1®を統合) は、セキュリティ対策の最前線であるファイアウォールのまきに標準と言える製品です。VPN-1は、適切な設定規準を確立する機能を搭載するなど、ファイアウォールに関するさまざまな要件をサポートしています。例えば、ネットワーク・コンポーネントのきめ細かな論理的管理、内部ネットワーク・ゾーンのセグメント化によるネットワーク各部の切り分けと保護、ポートの割り当ておよび文書化、ファイアウォール設定のポリシー策定、監査およびレポート、ネットワーク接続の図示といった機能を備えています。</p> <p>チェック・ポイントのセキュリティ管理アーキテクチャ SMART™により、管理者は、ネットワーク・トポロジを集中的に管理、承認、および表示し、すべての外部ネットワーク接続やファイアウォール設定の変更を検証することができます。ファイアウォールのセキュリティ・ポリシー、プロトコル、およびルール・セットを一覧表示したり、ファイアウォールのポリシーを集中管理して複数のVPN-1ゲートウェイに一括適用したりすることも可能です。</p> <p>SmartDefense、Web Intelligence技術、Eventia Suite、およびIPS-1は、侵入防御機能を提供します。これらの技術と製品は、単独で、または他の製品と連携して動作し、ネットワーク・トラフィックを監視して不審なアクティビティやセキュリティ侵害の可能性が見つかった場合に担当者に通知します。</p>

COBITの統制目標	チェック・ポイントのソリューション
<p>DS5.11: 機密データの受け渡し (Exchange of Sensitive Data)</p> <ul style="list-style-type: none"> 機密性の高い業務データのやり取りは、内容の完全性確保、受信証明 (受領証明)、送信証明 (発送証明)、および送り手側の否認防止が可能な、信頼できる経路またはメディアを使用して行う。 	<p>チェック・ポイントのCheck Point Endpoint Security Full Disk Encryption (Pointsec PC) は、デスクトップPCおよびノートPC向けの強力なフルディスク暗号化機能とアクセス制御機能を提供し、最高レベルのデータ・セキュリティを実現します。Check Point Endpoint Security Full Disk Encryption (Pointsec PC) により、データの完全性と信頼性を保証しながら安全に機密データの受け渡しを行うことが可能になります。</p> <p>チェック・ポイントの安全なリモート・アクセス・ソリューションであるVPN-1とConnectraは、公衆網経由でデータを送信する際、標準ベースの暗号化プロトコルを使用して強力な暗号化を行います。VPN-1は、SSLとIPSecによる暗号化通信をサポートしています。Connectraは、SSLとTLSによる暗号化通信をサポートしています。またどちらの製品も、機密情報の送受信を伴う通信の完全性を確保するため、MD5とSHA-1をサポートしています。</p> <p>IPS-1 Sensorは、暗証番号や医療情報、機密指定されたファイルなど、特定構造のデータをインラインで検出し、アラートを生成する機能を提供します。</p> <p>チェック・ポイントのVAR、SI、およびビジネス・パートナーは、チェック・ポイントのソリューションを用いて、安全にデータの受け渡しを行うためのコンサルティング・サービスを提供しています。</p>
<p>ME1.4: 成果の評価 (Performance Assessment)</p> <ul style="list-style-type: none"> 目標に対する達成度を定期的に検証し、目標未達があった場合はその原因を分析して、原因に対する是正措置を実施する。また、目標未達全般の根本原因分析を適宜行う。 <p>ME1.5: 取締役会および経営陣への報告 (Board and Executive Reporting)</p> <ul style="list-style-type: none"> ビジネスに対するITの貢献について、経営上層部向けのレポートを作成する。 経営上層部にレポートを提出し、レビュー後のフィードバックを求める。 <p>ME1.6: 是正措置 (Remedial Actions)</p> <ul style="list-style-type: none"> 成果を監視、評価、および報告した結果に基づいて是正措置を策定し、実施する。 	<p>チェック・ポイントのSmartCenterとEventia Suite (Eventia ReporterとEventia Analyzer) は、システム・イベントおよびアクティビティのロギング、アップデート、監視、レポートを一元化することにより、セキュリティ・アクティビティおよびネットワーク・アクティビティの全体的な傾向を把握できるようにします。組織全体のデータが統一形式で表示されるため、より効率的なデータの収集、分析、および対応が可能になります。</p> <p>Eventia Suiteは、すべてのチェック・ポイント製品および多種多様なサードパーティ製品で記録されたログとイベント・アクティビティについて、収集、監査、相関分析、およびレポート作成を行います。Eventia Reporterは、各種の情報を収集し、複数の製品にまたがる攻撃、ブロックしたトラフィック、ログイン・アクティビティ、およびネットワーク・アクティビティについてレポートします。</p> <p>Eventia Reporterのエンドポイント・セキュリティ・レポートでは、Check Point Endpoint Securityのデータ (ポリシー違反、ファイアウォール・イベント、ブロックしたプログラム、Check Point Endpoint Security MailSafe イベント、スパイウェア、Malicious Code Protectorの結果、およびクライアント・エラーなど) についての統一レポートが提供されます。Eventia Reporterは、アンチウイルス・アクティビティ、Connectra、InterSpect、およびVPN-1 Power VSXのログ・レポートについてのレポートも提供します。</p> <p>Eventia Suiteでは、データへのユーザ・アクセス、管理者が行った操作、無効な論理的アクセスの試みなどについての監査証跡を記録することができます。Eventia Analyzerは、監査ログの初期化と監査情報への安全なアクセスをサポートし、システム・レベル・オブジェクトの作成と削除にも対応しています。また、監査ログが初期化されたときや、システム・オブジェクトが作成または削除されたときにアラートを生成することもできます。</p>

まとめ

多くのIT組織にとって、SOX法第404条は、財務報告を行うために必要なITセキュリティの統制とプロセスを確立して文書化するうえで、重要な転換点となっています。情報の完全性を確保し、リソースへのアクセスを制御することは、企業を維持していくために不可欠な要素であると同時に、法令を遵守するために必要なことでもあります。チェック・ポイントのセキュリティ・ソリューションは、SOX法の第404条で規定されている要件を満たすうえでの基盤となる、COBITの多くの統制目標を達成するために活用することができます。境界からエンドポイントに至る堅牢なインフラストラクチャを提供する、最も実績のあるチェック・ポイントの統一セキュリティ・アーキテクチャは、大きな安心感を企業にもたらします。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022

東京都新宿区新宿5-5-3 建成新宿ビル6F

E-mail : info_jp@checkpoint.com

Tel : 03 (5367) 2500

<http://www.checkpoint.co.jp/>

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityのlogo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Achieving Sarbanes-Oxley Act Section 404 Compliance with Check Point Solutions

P/N:502779-J 2008.02

※記載された製品仕様は予告無く変更される場合があります。

