内部統制のための情報セキュリティ
―「SecureCube」ソリューション―

新会社法の施行（2006年5月）、証券取引法の改正（2008年に導入の見込み）など、企業の内部統制の強化を促す動きが強まっている。内部統制とは、いかに情報セキュリティを高めシステムの安全性を確保するかの問題でもある。本稿では、内部統制の強化に必要なポイントを整理するとともに、NRIセキュアテクノロジーズのソリューションについて紹介する。

内部統制の基礎となる証跡の管理

内部統制の目的は、業務の有効性・効率性、財務諸表の信頼性、関連法規の順守を確保することにあるとされるが、そもそも内部統制とは具体的に何ができていることなのだろうか。そこには以下の３つのポイントがあると考えられる。

①適切な文書規定があること
②文書規定が実際に運用されていること
③実際にどのように運用されているかについて内部からも外部からも監査・証明できること

何らかの文書規定を策定し、それに基づいた運用を行うことは、すでに多くの企業で実施されているであろうが、監査人や経営者にとっても理解できる文書や記録を、必要とされるタイミングで速やかに準備できることがますます重要となっている。その上で、業務の実態が適正かどうかを自己管理できる仕組みが求められているわけである。

実際にどのように運用されているかを証明するには、何らかの情報システムの利用が当然となっている今日では、相当する個々のシステムから出力される証跡情報（ログ）を使用することが現実的と考えられる。このとき、まず企業内で実際にどのようなログが存在し、どのように蓄積され利用されているかを調査して、実態を確認しておく必要がある。

①社内のどこにどのようなシステムがいくつあるのか。それらは誰がどのように利用しているのか。
②各システムのログは、目的とする監査や分析の観点に沿って、証跡として足るだけの項目をもっているか。また十分な期間保存蓄積されているか。
③セキュリティポリシーを含む利用統制規定に沿って、ログの参照・検索や分析、報告が適切に運用されているか。

このような視点で確認してみると、とくに多様な業務機能やシステム群をもつ組織であれば、ばらつきや不整合を発見することも決して少なくないであろう。

重要ポイントとなるアクセス管理

内部統制で重視される財務諸表が、結局は会計システムやそれにつながる個別業務システムから生成され、また情報システム自体が不正アクセスや情報漏洩などのリスクにさらされていることから、内部統制の重要な要素

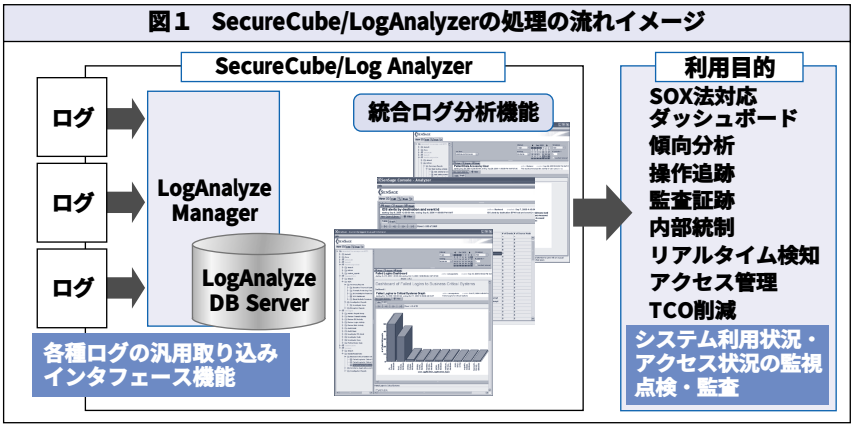
NRIセキュアテクノロジーズ
事業開発部
マネージャー、CISA
芦田　剛（あしだつよし）

専門はITセキュリティコンサルティング、
セキュリティ分野の各種サービス企画開発

がIT統制であることは間違いない。このとき、入力誤りなどのシステムオペレーションリスク、システムへの入出力を行う担当者のチェックもれや承認までの過程のミスや遅れといった業務オペレーションリスク、それに加えて、不正アクセスによる破壊や業務妨害、データの改ざんや削除などのセキュリティリスクは、財務報告の信頼性を損なう大きな要因となる。

すなわち、情報セキュリティ管理、なかでも情報資産に対する適切なアクセス管理は、財務報告の信頼性確保のためにも内部統制における重要なポイントとなる。

図1　SecureCube/LogAnalyzerの処理の流れイメージ



総合セキュリティ管理ソリューション

以上の観点から、NRIセキュアテクノロジーズでは、ログ管理とアクセス管理を基本に、電子メールの監査やPCのセキュリティ診断などを含む、社内システムの情報セキュリテ総合ソリューションとして「SecureCube」シリーズを提供している（http://www.nri.co.jp/products/secure/index.html）。

(1) 統合ログ分析ソリューション
（SecureCube/LogAnalyzer（仮称））

ログの監査は、内部統制の観点だけでなく、事故の予防や早期の対処にいかに活かすかという、業務運用の視点からも重要である。「LogAnalyzer」（図1参照）は、企業内の各業務領域や、個別のネットワーク・部署において使用されている多様なシステム群から出力されるログデータを収集・蓄積し、適切な分析を行うことにより、業務事故の早期発見や予防、IT利用が全般に適切になされているかどうかの管理を可能にする。

(2) アクセス制御・監査ソリューション
（SecureCube/AccessCheck）

内部統制における職務分離の原則に基づき、システムの開発および本番運用を行う場面や、そのほかに利用者が制限されるシステム環境へのアクセスにおいて、ネットワークレベルでアクセス制御および操作内容の監査を行う（次ページ図2参照）。

たとえばシステム開発環境であれば、本番サーバー群の運用環境との分離、および本番運用環境への事前アクセス申請の受付と管理

者による承認、利用中の操作ログ取得に基づく監査などの機能を提供し、システムの運用における機密性を高めている。

(3)電子メール監査ソリューション（SecureCube/MailCheck）

社内ユーザー同士のメールや、社外からの受信メール、社内から社外へ発信されるメールに関し、メール内容を長期間保存蓄積するアーカイブ機能、および全文検索による利用状況監査やフィルター条件設定による定常チェックなどの監査支援機能を提供する（図3参照）。階層的な構造で監査者を設定することが可能であり、かつ監査する側とされる側のグルーピングによる関連付けも柔軟に設定できる。メール内容の監査は、本

図2　SecureCube/AccessCheckによる処理の流れ

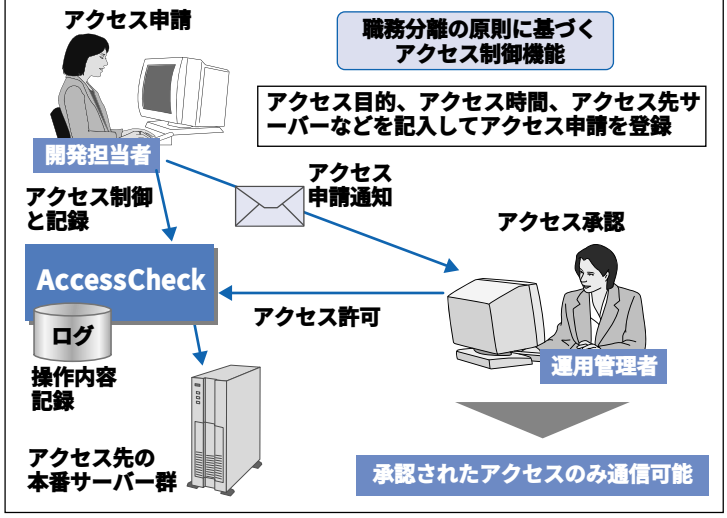


図3　SecureCube/MailCheckの利用イメージ

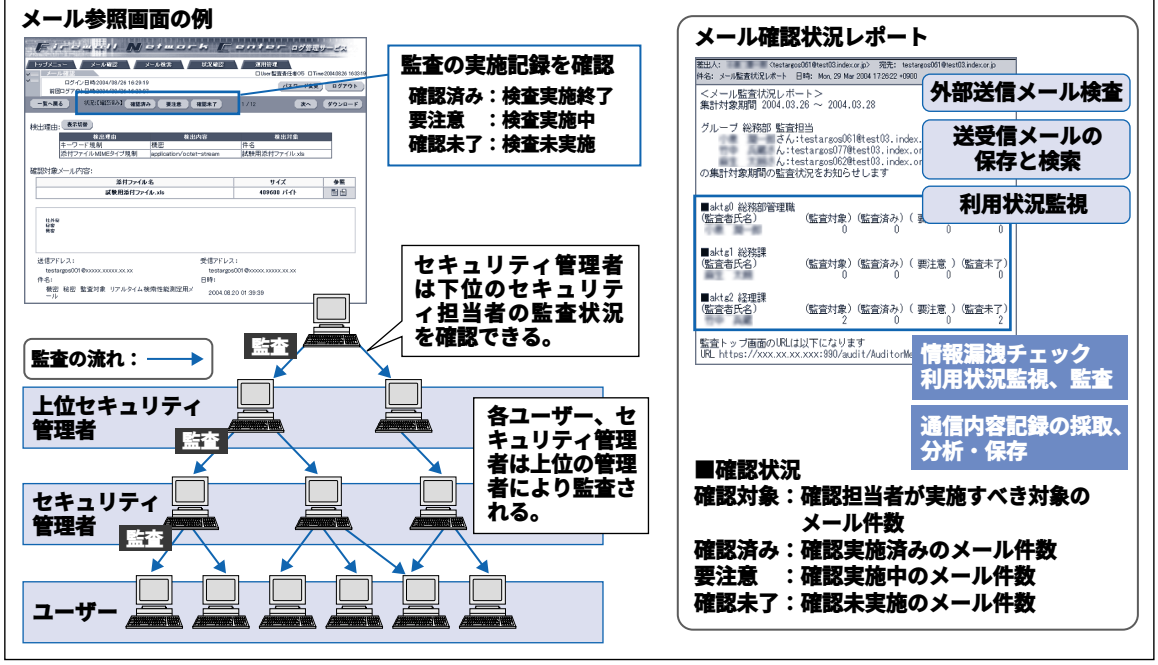
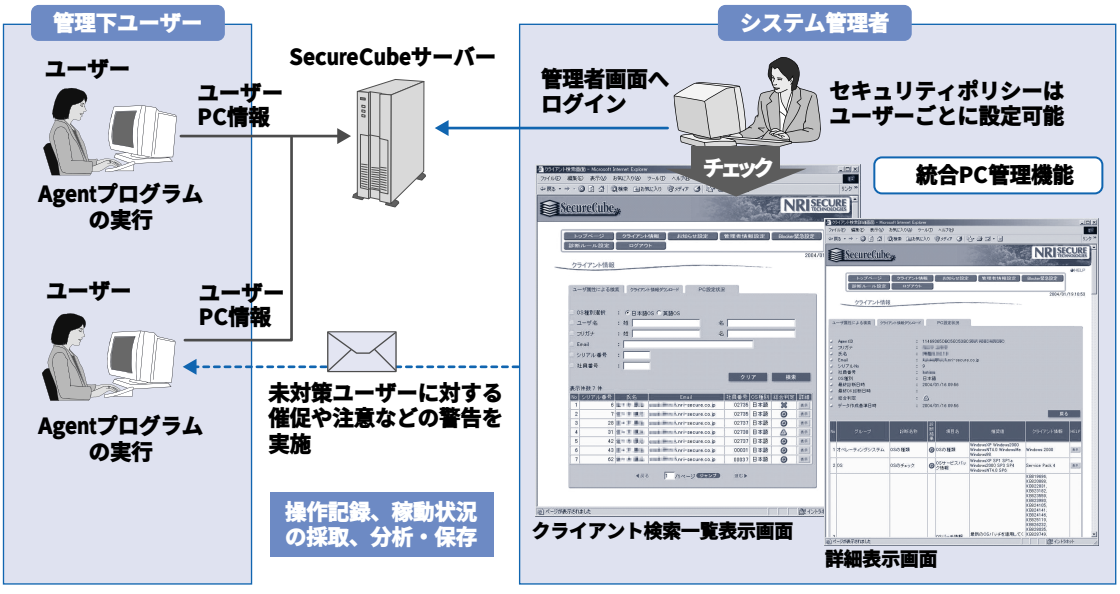


図4　SecureCube/PCCheckポリシーに沿った設定チェックと管理



文および添付ファイルについても可能である。特定のキーワードや添付ファイルの拡張子・サイズ、発信者および受信者に関する条件検出設定や、要注意メール抽出を行うことができ、監査者が確認したかどうかも記録する。条件設定は全社単位、また組織単位や任意のグループ単位に行うことができるので、実際の業務実態に合わせた運用が容易である。

(4) PCセキュリティ診断・監査支援ソリューション（SecureCube/PCCheck）

企業のセキュリティポリシーに従って、社員が日常的に使用するPC端末について、システム設定が適切か、また利用状況が適切かどうかを自動的に診断してレポートする（図4参照）。PC操作ログ記録や、USBメモリーなど外部メディア機器への書き出し制御機能、資産管理機能をもとに、情報漏洩や不正利用の予防・チェックに活用でき、社員のPCのセキュリティ状態について自動的かつ網羅的に可視化できる。サーバー機器へはSecureCube/SiteSecurityCheckが対応する。

情報セキュリティ総合ソリューションとして

NRIセキュアテクノロジーズでは、これらさまざまなソリューションをもとに企業の適切なIT利用環境づくりを支援していく。

また、企業組織全体としてのセキュリティ状態をわかりやすく可視化するソリューションとして「SecureCube/Navi」（仮称）の提供も予定している。 ■