テクノロジー・リーダーのためのコンピューティング情報誌

IDG JAPAN

COMPUTERWORLD

月刊［コンピュータワールド］

Get Technology Right

7

2007 July

ITマネジャーのための
内部統制/日本版SOX法
講座

内部統制における「ログ管理」の重要性

脚光を浴びる「ログ管理」

ログとは、一般的にはコンピュータの利用状況などが記録されたデータを指す。具体的にはコンピュータにおける操作やデータの送受信が行われた日時、だれがどんな操作を行ったのか、どのデータが送受信されたのか、といった情報が記録されている。

企業におけるネットワーク機器や業務アプリケーション・サーバ、ファイル・サーバなどのシステムは大抵ログを出力している。むしろログをはき出さないシステムは皆無に等しいとも言える。

今でこそ、各PCの操作ログを取得／管理するためのシステムがいくつか登場し、セキュリティ対策としてそれらを導入する企業も増えつつあるが、これまでのログは、単にシステムが正常に稼働しているかどうかを確認するためのものでしかなかった。

ところが、個人情報保護法が施行され、また、Winnyなどのファイル共有ソフトが原因の情報漏洩事件が多発するようになって以来、ログ管理がにわかに注目されるようになった。さらには、日本版SOX法（金融商品取引法）やe文書法などの法令順守においても、ログ管理が重要な役割を果たすようになってきているのである。

なかでも日本版SOX法は、財務情報の不正や誤りを防ぐ監視システムを上場企業に整備させることを

内部統制における「ログ管理」の重要性

ファイル・サーバや入退室管理システムなど、企業におけるさまざまなシステムがはき出す「ログ」を包括的に管理することが、内部統制にも役立つとして、にわかに注目を集めている。内部統制の推進／日本版SOX法（金融商品取引法）への対応を進めるにあたって、ログ管理はどんな役割を果たすのだろうか。本稿では、その意義と重要性を明らかにするとともに、ログ管理システムを用いた作業ポイントなどについて解説する。

川原一郎
リエンクリプション・テクノロジーズ

ねらいとしているが、企業の財務業務のほとんどがITシステムで管理されている今日、業務プロセスの正当性を証明するためには、業務システムのログを管理する必要がある。

また、2007年2月15日には、金融庁より「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について(意見書)」が公開された。これは日本版SOX法におけるITの内部統制に関する正式なガイドラインである。内容としてはこれまでの公開草案から大きく変更されていないが、正式にまとめられ公表されたという意味では、今後の企業における内部統制整備を加速させるものとなるだろう。

同意見書の中では、ITにかかわる全般統制の具体例として、次のような項目が挙げられている。

- システムの開発、保守に係る管理
- システムの運用・管理
- 内外からのアクセス管理などのシステムの安全性の確保
- 外部委託に関する契約の管理

こうした内部統制の有効性の評価において、ログが重要な役割を果たしていくことはまちがいない。実際に、経済産業省が2007年3月30日に公表した「システム管理基準 追補版(財務報告に係るIT統制ガイダンス)」の中でも、ITを活用したログ管理の重要性が指摘されている。具体的には、経営者が、実施部門および内部の監査部門からの報告を通して計画や統制の有効性を確認・評価する際、あるいは、統制の実施状況のモニタリングの効率性と有効性を高めるのにITを活用すること、といった内容が記されている。このように、今後は社内にあるすべてのログを集計したリポートを作成したり、各種ログから問題を検知したりできるシステムを構築することが重要になってくると思われる。

ログ管理の問題点

以下では、ログ管理を行ううえで考えられる問題点をいくつか挙げてみたい。

■分散状態

前節で述べたとおり、今日ではあらゆるシステムがログを出力している。例えば、ファイアウォールやルータなどのネットワーク機器、メール・サーバやファイル・サーバなどの基幹サーバ、各種業務システムなど、システムごとにログはたまっていく。これらのログは各サーバに点在し、その閲覧方法も専用アプリを用いたり、CUIベースでコマンドを使ったりとさまざまだ。だが、このようにログが点在したままでは、いざ「重要な情報にいつだれがどのくらいアクセスしたか」を調べようとしても、そのログの所在や閲覧方法などがわからないといった事態に陥りかねない。

■統計が困難

ログの形式がテキスト・ファイルで、しかもシステムごとにばらばらに保存されているとすれば、それらを検索したり、集計したりすることは容易ではない。例えば、システムの利用状況やアクセス状況などを元に統計を取る場合、異なる形式のログを組み合わせた集計データが必要となるが、社内にログが点在している状況では、必要なデータを探し出すだけで一苦労となる。

■保全・保管

最近よく「フォレンジック」という言葉を耳にするかと思う。コンピュータ関連でフォレンジックという言葉を用いる場合は、不正アクセスや情報漏洩といった犯罪行為の痕跡を調査し、将来の訴訟に備えて法廷で立証できる“証拠”を集めることを意味する。なかでもログは、事故や事件が起きた際の法的証拠として重視されるようになっている。このように、ログが問題の原因究明だけでなく、法的証拠としても重要な意味を持つようになると、証拠保全に向けて、ログをいかに適切に保管するかといった運用面も考慮しなければならない。

■改竄

ログが重要な意味を持ってくると、それが正当なログであるのかということも重要になってくる。証拠隠滅のためにログを改竄されてしまっては、証拠として

使えなくなるからだ。

例えば、不正アクセスの痕跡はサーバのアクセス・ログなどから調べることができるが、攻撃者はそうした痕跡を残さぬようログを改竄する傾向にあるため、法的証拠としてログを提出するにあたっては、改竄されていない正当なログであることを証明できなくてはならない。

統合ログ管理の必要性

実際に、内部統制を目的としたログ監査を実施するには、社内の機密情報にいつ、だれが、どのくらいの頻度でアクセスしたかを“可視化”できる仕組みを構築することが重要となる。そこで注目を集めているのが、統合ログ管理システムである。

統合ログ管理システムが持つべき機能

では、統合ログ管理システムには具体的にどのような機能が求められるのだろうか。以下、統合ログ管理に必要なポイントをまとめる。

■生ログ(注1)の保存

各システムが出力するログは、そのままでは単なる文字の羅列でしかないため、閲覧するにあたってフィルタリングをかけられることが多い。だが、フォレンジックやコンプライアンスの観点では、証跡として原本性が求められるので、ログは加工した状態で保存するのではなく、生ログの状態で保存すべきである。

■改竄防止

内部統制における証跡としてログを活用するためには、それが改竄されていないという正当性を保障できなくてはならない。

■一元管理

各システムが出力するログは、多種多様なフォーマットであることが考えられる。ログの統合管理を実現するには、フォーマットを問わず、あらゆるログを一元的に管理できる仕組みが必要となる。

■高速検索

生ログの状態で各システムのログを保存していくと、当然、データ量も増大していくが、データの取り出しに時間がかかってしまっては意味がない。したがって、大量のログを高速に検索できる機能が求められる。

■横串検索・集計

ログの統合管理では、システムごとに管理されているログを横断的に検索し、集計データを作成できる機能が求められる。例えば、重要なデータが持ち出されたことが発覚した場合には、クライアントPCの操作ログや、ファイル・サーバおよびメール・サーバのログなどを横串検索して、事故・事件に迅速に対応しなければならないからだ。

■検知

ログ管理はもちろん、統制活動を行ううえでも、システムをモニタリングし、事故やエラーなどの異常を即座に検知できる機能が求められる。

■リポート出力

システムの状況や、重要な情報へのアクセス状況などをモニタリングし、それらの状況を監査リポートとして定期的に提出できる機能も重要となる。

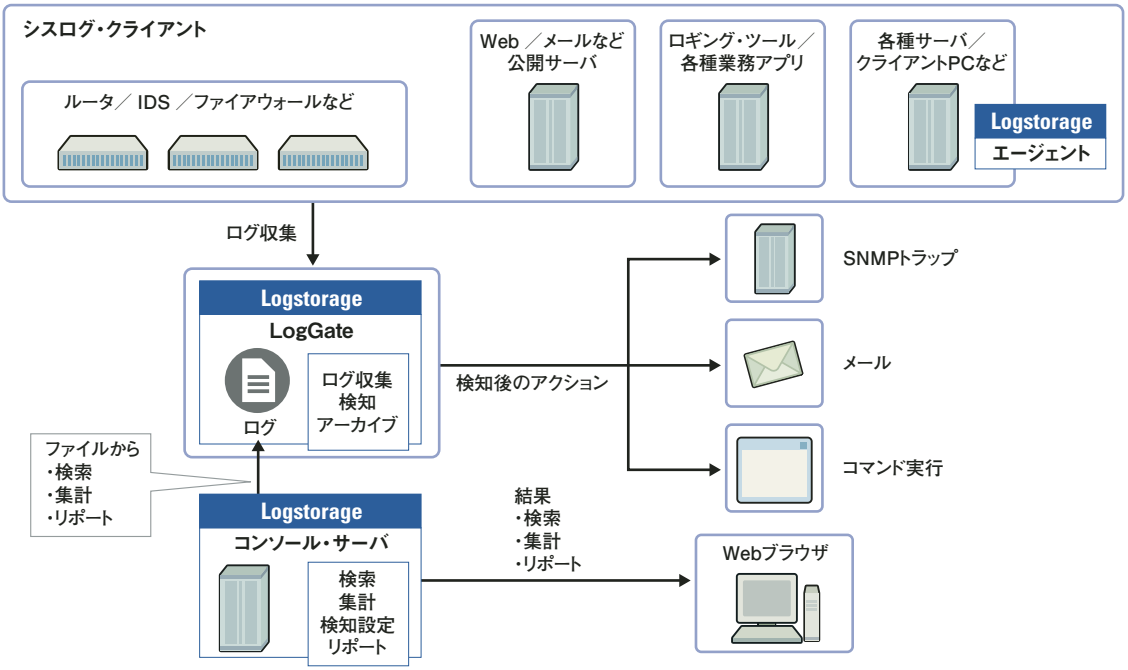
「ログ統制」の実現に向け統合ログ管理システムを活用

今後は、内部統制を進めるにあたって、ログ管理のPDCAサイクルを回していくことが重要となるだろう。ログ管理のPDCAサイクルでは、収集すべきログを定義し(Plan)、各種システムがはき出すログを統合的に管理する(Do)とともに、ログを用いてシステム状況のモニタリングや異常の検知を行い(Check)、日次あるいは月次リポートを作成してシステム監査を実施する(Act)、という作業を繰り返すことになる。

インフォサイエンスが開発した純国産の統合ログ管理システム「Logstorage」(**図1**)は、そうしたログ管理

注1：出力時のログで、内容を加工しない状態

図1：Logstorageの基本的なシステム構成



のPDCAサイクルを支援する各種機能を備えている。以下、Logstorageの主な機能を紹介しよう。

■ログ・フォーマット定義

Logstorageでは、ログを生ログの状態で保存できる。また、必要に応じてログのフォーマットを自由に定義することが可能で、ログにタグ付けすることでログにさまざまな意味を持たせることもできる。さらに、正規表現によるログの識別、タグ設定によるログの意味の解釈にも対応する。これにより、生ログの状態で保存されたログを、アプリケーションごとに管理することができる。

■ログの完全性証明

ログに電子署名を付加することでログの改竄を検出し、格納されたログの正当性を証明することができる。

■ブラウザで簡単にログを検索

統合ログ管理システムを使わずにログを検索する場合は、システムごとに異なる操作手順で検索を実行しなければならない。例えば、Windowsであれば標準で搭載される「イベントビューア」ツールを使ってログを閲覧する、あるいはUNIXであればCUIのコマンド・ベースでログを閲覧・検索することになる。Logstorageでは、使い慣れたWebブラウザから簡単にログを検索することが可能で、ファイル・インデックスによる高速検索にも対応している（110ページの**画面1**）。また、複雑な検索条件は保存して後から読み出したり、複数の検索条件を組み合わせたりすることもできる。

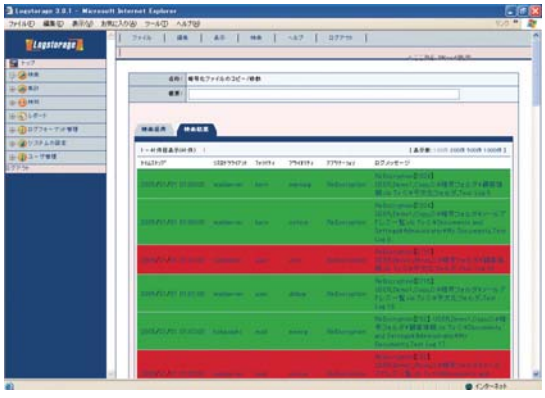
■ログの追跡・集計機能

ブラウザ上で検索結果のデータをクリックすることで、自動的に関連するログの再検索を行いながら追跡することできるトラッキング機能を搭載。また、異なる形式のログを組み合わせた集計を行い、その結果を各種形式の表／グラフで表示する集計機能を備える（110ページの**画面2**）。また、検索機能と同様、集計条件を保存して作業を定型化することも可能だ。

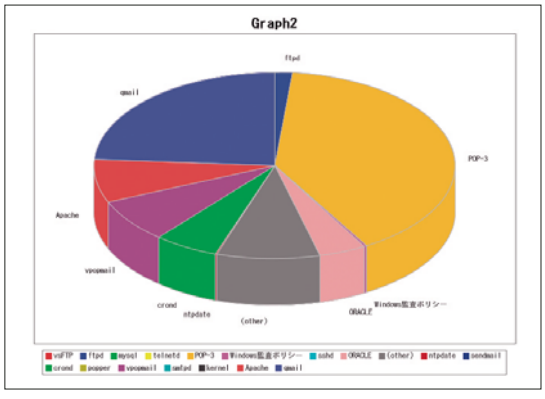
■検知・通知機能

検知ポリシーを定義してログを監視することによって、不正アクセスや障害などの検出・通知を行う。例えば、システム・エラーであれば管理者へメールで通知

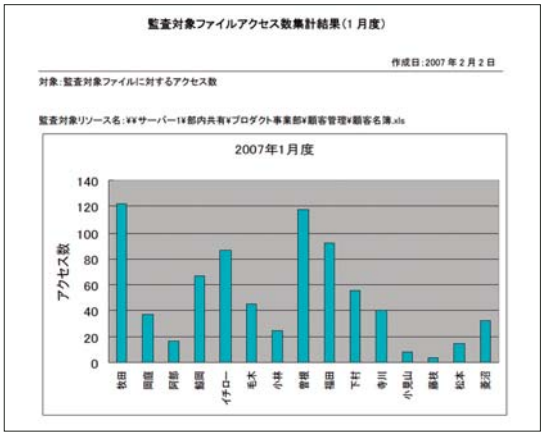
画面1：Logstorageの検索結果例。ブラウザ上で検索結果のデータをクリックすることで、自動的に関連するログの再検索を行いながら追跡するトラッキングが可能で、注意すべきログにハイライトを付けてわかりやすく表示させることもできる



画面2：Logstorageで得た集計結果は、表形式、折線グラフ、円グラフ、棒グラフによって表示することができる



画面3：Logstorageのリポート機能。リポート形式はテキスト、CSV、PDF、HTMLなどをサポート



画面4：Logstorageで作成した監査用リポート

したり、不正アクセスであればユーザー・コマンドを実行して必要なポートを閉じたりするなど、通知方法も選択することが可能。

●リポート機能

検索や集計の各条件に応じたログをリポートとして出力することが可能。リポートは日次や月次など定期的に作成することができる。リポート形式はテキスト、CSV、PDF、HTMLなどに対応し（**画面3**）、監査リポート作成の支援機能も備える（**画面4**）。

このようにLogstorageでは、テキスト形式であればどんなフォーマットのログも取り込めるため、異種混合のシステム環境においてもログの一元管理を実現することができる。また、高度なスキルを持つオペレーターでなくても検索や集計を容易に行えるなど、ログの積極活用を促す各種機能を備えているのも大きな特徴としている。

内部統制に向けた今後のログ管理

日本版SOX法への対応が急務とされるなか、企業においては今後、財務報告の正当性を証明するためのITインフラ構築、すなわち、重要なデータを守り、データが正しい状態にあることを保証できる環境を整備することが課題になる。統合ログ管理システムは内部統制を推進するうえで、社内の機密情報へのアクセス状況を全社的に可視化するための仕組みとして大きな役割を担うことはまちがいない。CW