先進のユーザー事例2　事業継続／J-SOX法

株式会社魚力

監査の網羅性とリソース負荷軽減を両立し J-SOX法対応のセキュリティ管理を実現

POINT
- iSecurityで4システム／41ライブラリーを対象にログ管理
- 物理ファイルを対象から外しディスク問題を解決
- 今後は放置端末の管理、アクセス制御、障害判別にも利用

COMPANY PROFILE
設立：1930年
本社：東京都八王子市
資本金：15億6362万円
売上高：234億5000万円（2008年3月期）
従業員数：438名（2008年3月末）
http://www.uoriki.co.jp/

セキュリティ強化に向け アクセスログ管理を実施

魚力の事業の柱は、鮮魚および寿司の小売事業、鮮魚など水産品の卸売事業、そして飲食事業の3つである。

スーパーマーケットや駅ビルなどに出店する同社の小売店舗は現在、首都圏を中心に35店舗、飲食店は10店舗。「安心・安全・満足」を経営理念に掲げ、独自の仕入れルートの開拓や新しい流通の仕組みの構築、販売システムの見直し、業界最大級の事業センターの開設など、常にポジティブな事業展開で、創業以来の成長を支えてきた。

山口豪將氏
情報システム室
係長

現在同社が、2006年に導入したSystem i（9406-520）で運用するのは、小売店舗からの受注・仕入れ・在庫・売掛金・買掛金・債権などを管理する「商品管理システム」である。それに小売店での週・月単位の利益率を管理する「営業情報システム」、テナントの家賃や水道光熱費などの諸経費を精算して売上を入金管理するための「売上返還金システム」、そして人事・給与システムと会計システムを加えた合計5システムである。

小売店舗のほとんどは百貨店、スーパーマーケット、駅ビルなどに出店しており、集中レジ方式を採用する。そのためPOSデータを使った単品単位による売上管理・分析はできないので、緻密な売上データ管理をシステムで支援する工夫が必要であったようだ。。

上記5システムは、パッケージ製品を利用する会計システムを除いて、全て自社開発型で構築されている。また3年前には、バックアップ機としてもう1台の520を導入し、HAソリューションを利用して全ファイルを同期する2重化体制を実現した。

同社の情報システム室は現在、2009年3月期に向けたJ-SOX法への対応で慌しい日々を送っている。既に2年近く前に、J-SOX法プロジェクトが発足。IT内部統制フレームワークとして注目されるCOBIT（Control Objectives for Information and related Technology）に準拠して、業務分析や規定づくりを進めてきた。またRADIUS認証に基づくネットワークの全面再構築を実施し、サーバールームの入退室管理といった物理的セキュリティの強化にも取り組んでいる。

そしてシステム内部のセキュリティ強化策として、「iSecurity」（三和コムテック）を導入し、アクセスログ管理を実施し始めたのは今年3月末。同社では2007年6月からセキュリティ製品の検討を開始し、自社の要件を満たす製品として同年末にiSecurityの採用を決定した。約3カ月の導入準備期間を経て本稼働を迎えている。

論理ファイルを対象外にして ディスク問題を解決

「セキュリティ製品の導入については、最初から全てのセキュリティ機能を厳密に実行するのではなく、運用状況を見ながら、段階的にセキュリティのレベルを上げていくこととしました」と、同社のセキュリティ方針を語るのは、情報システム室の山口豪將（ひでゆき）係長である。

iSecurityの導入に関して、同社が重

視したポイントは2つある。1つは開発権限と運用権限を分離し、開発ユーザーが業務システムを利用したり、運用ユーザーがシステムを変更することがないよう監視すること。そしてもう1つは、監査の網羅性とディスクリソース負荷のバランスを図ることである。

アクセスログ管理の対象としているのは、商品管理、売上返還金、人事・給与、会計の4システム。これらのシステムのライブラリーでは、基本的に全ファイルについて読み取り・更新・作成・削除・復元などのログを取得する（ライブラリー数は合計41）。これらに加えて、ディスク上で世代管理していた過去のファイル群についても管理対象にしたので、監査の対象は相当広範囲に及ぶことになった。

当初は物理ファイルと論理ファイルを含めて読み取りと更新のログを収集していたが、HAソリューションにより本番機からバックアップ機へデータを同期させていた関係で、監査ログが1日でディスクの1%、1カ月で30%を占有し、リソースへの負荷が非常に高いことが判明した。

何らかの対処が必要になったが、「iSecurityではログを取得したいファイルだけのグループを作成する機能を備えていたので、これを利用して、論理ファイルの読み取りをログの対象から外し、更新のログのみとすることで、ディスク容量の問題を解決しました」と、山口氏は指摘する。

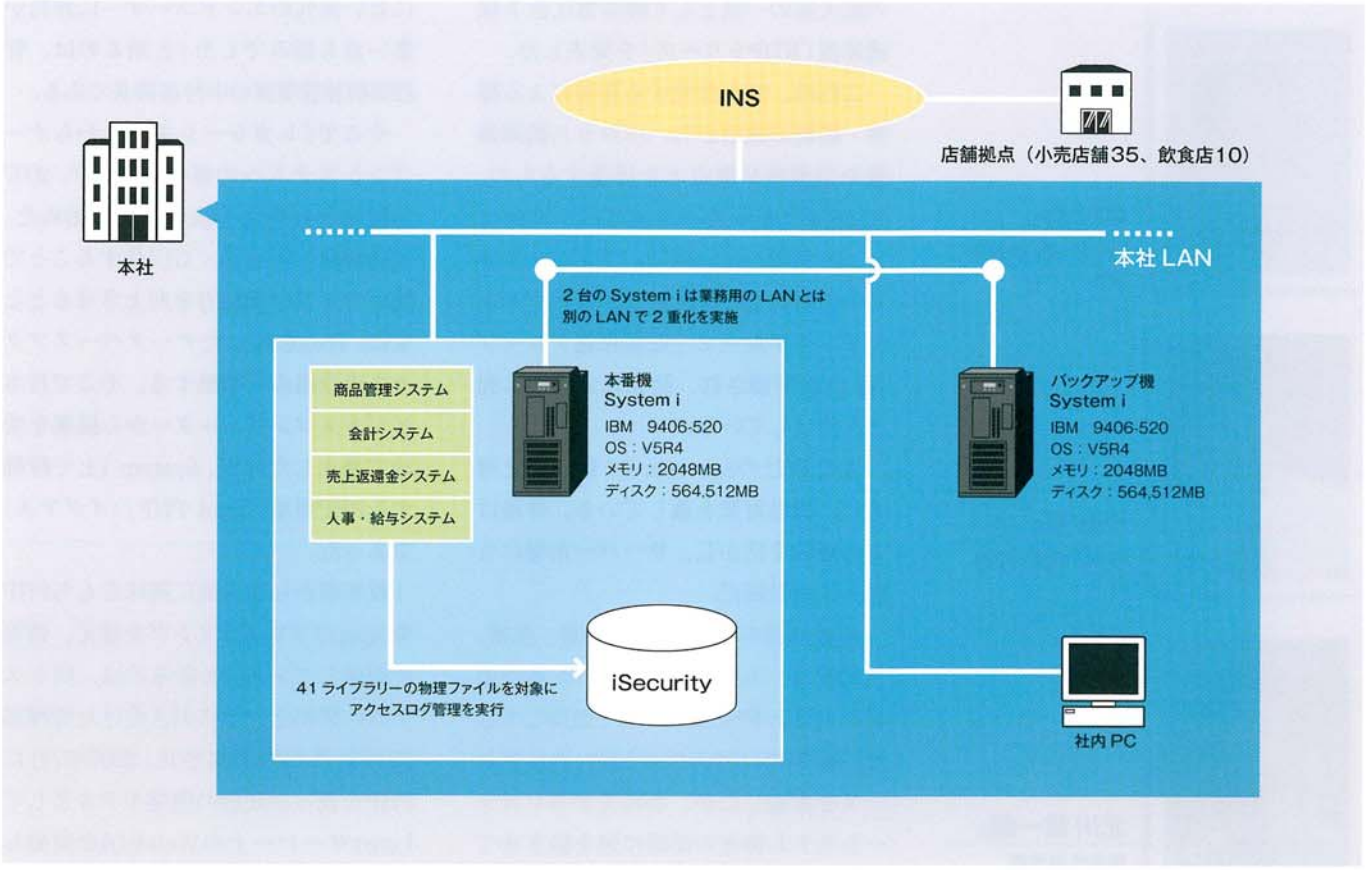
またオブジェクトの変更管理については、「誰がいつ、どのプログラムを変更したか」の管理にとどめ、「プログラムのどの行を変更したか」までの詳細な管理は行わないこととした。

iSecurityは機能に応じた8つのモジュールを提供しているが、同社ではフルモジュールを導入している。

「運用を始めたばかりなので、まだiSecurityの全ての機能を使いこなしてはいませんが、今後は監査だけでなくアクセス制御の機能も使っていきたいと考えています」（山口氏）

iSecurityではIPアドレスやアクセス経路ごとのログも取得できるので、ユーザーごとにアクセス経路を制限することが可能だ。また放置端末の管理や、画面遷移の記録機能を利用した障害対応にも利用していく方針である。何らかの不具合が発生した場合、画面遷移のキャプチャデータをトレースしていけば、障害判別や原因特定に利用できることになる。

今後2カ月で各部門への集中ヒアリングを実施し、業務処理統制を含めシステムに関する現状の不具合や不備に関する調査を進めていくことを計画している。その結果から、セキュリティ運用の方針に加え、今後の基幹業務システムの将来的な青写真についても明確な方向性が打ち出されることになるだろう。



図表 魚力のシステム概要