先進のユーザー事例⑮ **顧客情報漏えい対策**

株式会社日本オプティカル

約400万件ある顧客情報の漏えい対策を アクセス制御とログ取得・分析で実施

POINT
- 約400万件ある顧客情報の漏えい対策が改めて課題に
- アクセス制御とログ取得がツール選択の要件
- Firewall+++とLog Analyzer+++をセットで導入

COMPANY PROFILE
創業:1989年
設立:1993年
本社:愛知県名古屋市
資本金:9億7133万円(2008年12月)
従業員数:約950名
http://www.nopt.co.jp/

400万件の顧客情報と 950人の「アクセス可能」ユーザー

「ハートアップ」のチェーン店で知られる日本オプティカルは、コンタクトレンズの売上高で業界2位にランクされる小売販売会社である。2001年からはメガネ分野にも進出し、こちらでもすでに有数の地位を築くまでになっている。

同社の本格的なシステム化は1998年から。この時に基幹ネットワークを構築し、AS/400を導入している。その後、メガネ事業とネット販売への事業領域の拡大に伴ってシステムを拡張し、2007年5月からはシステム再構築プロジェクトをスタートさせ、2009年3月の「総合販売管理システム」の完成をもって、プロジェクトを完了させた。総合販売管理システムは、POSレジ・発注管理・在庫管理・物流管理などを内容とする基幹システムである。

そして、システムが安定して稼働し始めた矢先、マスコミでも大きく取り上げられた大手保険会社の個人情報流出事件が明るみに出て、同社でも改めて個人情報の漏えい対策が問題となった。「弊社では約400万件の顧客情報を保有していますが、それを保管しているのがIBM iという一般社員にとっては特殊なシステムであったため、これまではユーザーIDとパスワードだけでセキュリティ管理を行っていました。しかし、IT知識を持つ者が悪意を持って不正取得しようと思えば可能な仕組みだったので、それが問題となりました。顧客情報の中にはお客さま個人の目に関するデータが含まれていることから、万が一、顧客情報が流出した時の社会的責任は甚大なものになるとの経営判断が下り、万全のセキュリティ対策を講じることにしました」と総務部 情報システム担当の伊藤享臣課長は説明する。

ここでID・パスワードといっているのは、約300店あるショップと本社のスタッフ約950名がホルダーである。コンタクトレンズ販売の業法では、個人の処方箋に基づいて販売されているので、同社のスタッフなら誰でも顧客情報を蓄積しているシステムにアクセスし、閲覧できていた。それゆえ、Microsoft ACCESSなどを使えばODBC経由でIBM iにアクセスでき、簡単に個人情報のファイルをダウンロードされてしまう恐れがあった。FTPやIBM iのクライアント・アクセスなどによるアクセスについても同様である。

伊藤 享臣氏
総務部
情報システム担当
課長

アクセス制御と ログの取得が要件

そこで、セキュリティ・システムは、IBM i (System i5) 上で対策を講じることができ、「きめ細かいアクセスコントロールやログの取得が可能なこと」(伊藤氏) を要件とした。

「まず、IBM iに入る手前でアクセスをブロックできることと、弊社の場合、正規ユーザーなら顧客情報へのアクセス自体は制限できないので、その振る舞いをトレースできるログの取得を必須条件としました」(伊藤氏)

相談したシステムトラスト (「総合販売管理システム」を開発したSI会社) が提案してきたのは、三和コムテックのFirewall+++ (iSecurityシリーズの1アプリケーション) とLog Analyzer+++である。

Firewall+++は、IBM i上で稼働し、ファイル転送、FTP、エミュレータ接

続などの外部アクセスを、ユーザーID、IPアドレス、ファイルレベルごとにコントロールできるツール。Log Analyzer+++は、IBM iのアクセスログをPCサーバーへ取り込んで可視化する分析ツールである。

アクセスコントロールは、個々の店舗で使用しているプログラムを洗い出し、ユーザーIDと、店舗や本社で使用しているPCのIPアドレスを把握しておくことによって、ユーザーIDごと、IPアドレスごと、外部アクセスの形態ごとにきめ細かく設定することが可能である。

またログ分析では、例えば、店舗からのアクセスでODBCが使われていれば、Microsoft ACCESSなどのアプリケーションからのアクセスであると推定できる。TELNETであればエミュレータの起動、FTPならばファイル転送といった具合だ。

「Log Analyzer+++を使うことによって、どの店のどのPCからどういうユーザーがいつアクセスし、どのようなアクションを起こしたのかが明確に分かるようになりました。以前は、データを不正取得されても痕跡すら残りませんでしたが、今はログさえあれば過去に遡って特定することができます」と伊藤氏は評価する。

シミュレーション・モードでテスト運用し、実情を把握

Firewall+++の本番利用に先立って、同社では「シミュレーション・モード」を使用して、ユーザーの利用状況の把握とアクセス制御の設定を行うための情報を収集した。Firewall+++のシミュレーション・モードとは、本番利用を想定した設定でFirewall+++を稼働させるが、「アクセス拒否」と設定したファイルにユーザーがアクセスしてもログに「拒否されました」というメッセージを表示するだけで、アクセス自体は可能にする機能である。

「このテスト運用を実施したことによって、業務の実情に即したアクセス設定が行えました。本番への移行後も、ユーザーからクレームや不具合の連絡はまったく寄せられていません。使える、非常にいい機能だと思います」(伊藤氏)

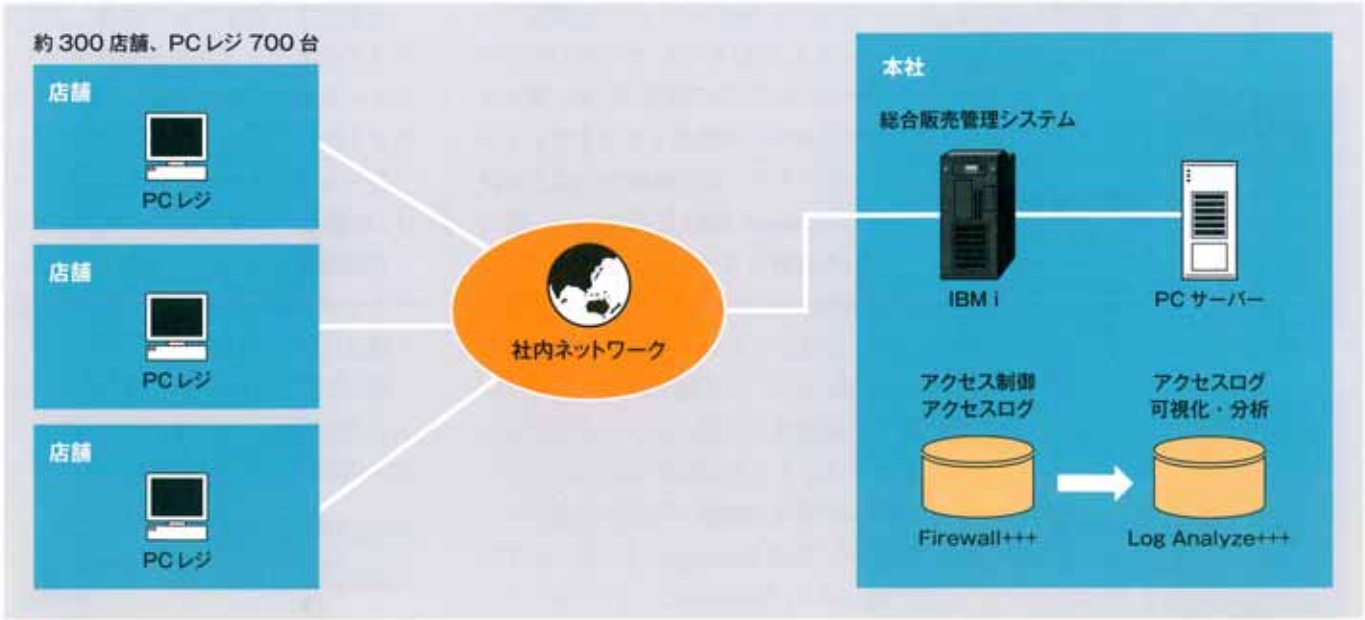
2009年9月10日にFirewall+++をインストールし、シミュレーションモードでのテスト運用を経て、同月25日にサービスインしている。非常にスピーディな導入である。

伊藤氏は、「これで顧客情報に関する漏えい対策は、問題のないレベルになったと考えています。後は、Log Analyzer+++を使い、日次・週次・月次で分析を行い、さらにブラッシュアップしていく予定です」と語る。

このほかセキュリティを含む事業継続関連の取り組みとして、遠隔地バックアップを検討中である。同社では今年6月までHAツールを用いた災害対策を実施してきたが、HAツールの利用を取りやめたため別の対策を講じる必要が出てきた。現在は、テープへのバックアップを毎日行っているが、これの保管・管理を効率化するために遠隔地バックアップを導入する計画という。

また、来年2月には本社移転も控えており、現在2カ所あるデータセンターの統合と、Windowsだけで40台以上あるサーバーの整理・統合も実施する予定だ。

「顧客情報の漏えい対策をスピーディに行えたので、余裕を持って移転・移設計画に取り組むことができています」と伊藤氏は言う。



図表 日本オプティカルの顧客情報漏えい対策時システム概要