パイオニアサービスネットワーク株式会社

Pioneer
sound. vision. soul

company profile ✳

- 設立:2000年
- 資本金:1億円
- http://pioneer.jp/psn/
- 本社:東京都目黒区
- 従業員:500名

高度なデータ保全を実現するツールとしてSecurity+++を導入

アフターサービス満足度調査で3年連続No.1

パイオニア製品のカスタマーサポートや修理、補修部品の販売を手がけるパイオニアサービスネットワーク(PSN)は、日経ビジネス誌が毎年行っている「アフターサービス満足度調査」の「薄型テレビ部門」で、3年連続で総合1位を受賞した(受賞対象商品は、パイオニアのプラズマテレビ)。また、このほかにも、メディア各誌が実施する顧客満足度調査において、各種商品がさまざまな賞の対象となっている。

これは、「お客様満足度No.1企業」を目指して全社を挙げて取り組んでいる同社の1つの大きな成果といえるものだが、その取り組みを支えるものとして、国内および全世界に張り巡らされたサービスのネットワークと情報システムがある。

PSNにおいて基幹システムの構築・運用を担当する櫻井孝司氏(経営統括室情報システムグループ 課長)は、「PSNにおけるCS(顧客満足度)向上に関しては、修理や問い合わせへの応答にどれだけの時間や期間がかかったのか、具体的な数値目標を設定し、その期間内に完了するよう取り組んでいます」と説明する。

顧客からの問い合わせや修理、部品購入の依頼は、電話、FAX、Webサイト(メール)などを通して入ってくる。

櫻井孝司 氏
経営統括室
情報システムグループ
課長

問い合わせについては、コールセンターで受け付けると、センターの担当員が顧客との間でQ&Aを行い、そこで解決しない場合は2次対応へ回す。修理については、電話やWebサイト経由のほかに全国のサービス・ステーションやサービス認定店に直接製品が持ち込まれるケースもあるが、受付を終えると修理システムに登録し、データを回していく。この修理システムには、見積もりや進捗状況を確認するためのサブシステムもあり、進捗状況確認システムでは、Webサイト上で受付番号を入力すると、顧客はいつでも修理に出した製品の進捗状況が分かるという仕組みだ。また、部品・付属品の販売では、電話やFAXによる受け付け時に、在庫確認から倉庫への出庫指示、発送までを一貫して行えるシステムが構築されている。この受付から出庫指示までは「即日処理が基本」(櫻井氏)という。このほか、部品調達システムなどがワールドワイドで稼働している。

データ保全の2つのアプローチ

これらのシステムは、いずれも構築から数年以上が経過し安定して稼働しているが、現在、同社が取り組んでいるのが「データの保全をどうするか。それをどのように高めるか」(櫻井氏)というテーマである。

「Webサイトで受付をする際の認証など基本的なセキュリティは実施していますが、内部統制の動きもあり、顧客情報を厖大に扱う当社としてデータの保全をどう確保していくのか、2005年から本格的に取り組んでいます」

Security+++

販売元 三和コムテック

セキュリティ／全般

導入のポイントと評価

- データ保全のための解決策
- System i対応のセキュリティツール
- ファイアウォールや監査ログ取得機能を持つ

同社の選択したアプローチは、「外部からの侵入を防ぐ」と「内部での保全性を高める」という2つである。そして、外部からの侵入を防ぐことから着手したが、そのためのツールとして採用したのが三和コムテックの「Security+++」だった。

同社は今、Security+++のファイアウォール機能(Firewall+++)を使って、日次で不正アクセスのチェックを行っている。

「Security+++から吐き出されるログをPC上のExcelに落とし、アクセスを開放しているリストや前日分のアクセスなどと対比させてチェックしています。見覚えのないIPアドレスからのアクセスに対しては、それを基に追跡し、場合によってはアクセスを遮断するといった処置を講じています」と櫻井氏は言う。

「ややアナログ的な管理になっているので、これを効率化することが今後の課題です。また、IPアドレスを中心にチェックしているので、関係会社や関係部署でPCやシステムの移動・変更があった時は速やかにファイアウォールに反映できるよう連絡を密にしていくことも課題です」

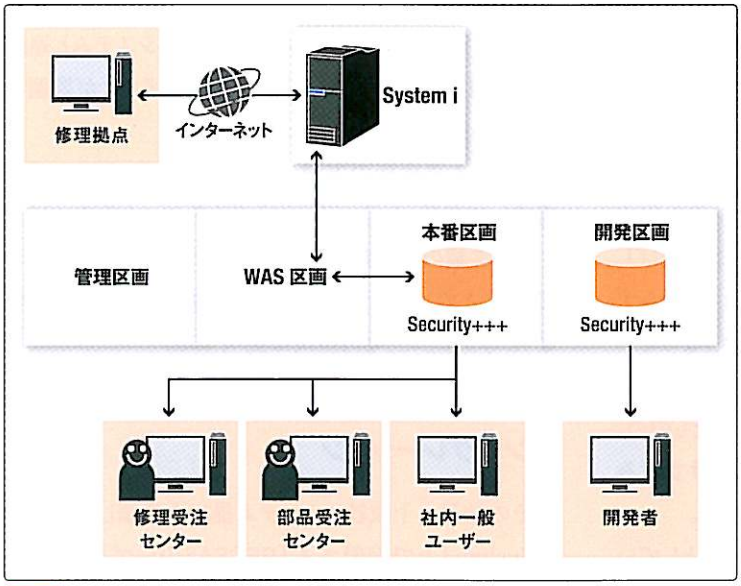
Audit+++を使い監査ログを分析・活用

一方、「内部での保全性を高める」取り組みも進めている。これは、Security+++の監査機能(Audit+++)を使い、その監査ログを分析・活用することにより対応を進めている。「これは、誰が、いつ、どのDBの何のファイルにアクセスしたかを把握することで、問題が発生した時に追跡できるようにするものです。特に、顧客情報がむやみにダウンロードされていないか、入念にチェックしています」(櫻井氏)。そして、監査ログデータは膨大なデータ量となるため、週2回監査ログをテープにバックアップし保存する体制としている。

基本的にはSystem iの権限設定とSecurity+++の設定で、むやみにデータダウンロードができない仕組みにしてあるものの、この監査ログの取得と分析を含め内部保全性向上をどこまでやるか、「常に悩んでいて、試行錯誤の連続です」と櫻井氏は語る。

「オペレーションへの負担を大きくせず、セキュリティ向上を実現するバランスに常に悩みます。また、詳細な情報を得ようとして細かくログを設定すれば、多くのデータを得ることができます。しかし、その分析だけに時間を当てることができないので、その他の業務とのバランスに常に悩みます。」

目下検討しているのは、「内部で顧客情報などがダウンロードされる前やダウンロードされた際に、どのようなアクションを取るか、監査ログをもっと効率的に有効に活用する手段が必要であるとともに組織全体としてセキュリティの考えをもっと浸透させ、少しずつ活動して行く必要がある」と櫻井氏は言う。



図表 バイオニアサービスネットワークのシステム概要