

# LogStare

## 導入事例

### VOL.05

LogStare  
CASE STUDY  
VOL.05  
BOOKS  
KINOKUNIYA

## 多種多様なシステムが混在する 環境で、サーバ管理者(特権IDユーザ) の操作ログを集中管理

～さらに強固な個人情報保護を実現～

### BOOKS KINOKUNIYA 紀伊國屋書店



後藤 一郎氏

株式会社紀伊國屋書店  
情報システム部  
情報基盤グループ リーダー  
課長

株式会社紀伊國屋書店は昭和2年創業の老舗書店で、日本各地や世界主要都市に店舗を持つほか、大学のブックセンターも多く経営している。近年ではネット販売サイト「BookWeb」も展開している。多くのITシステムを利用している同社では、個人情報保護の目的で特権IDを持つユーザのログ管理が検討されていた。そのために導入されたのが統合ログ管理システム「LogStare」だった。

紀伊國屋書店の業務ではさまざまなシステムが利用される。ネット販売で用いるEコマース、店舗でのPOS管理、クレジットカードの決済、人事や経理、電子メール、グループウェア、ERPパッケージなど多種多様なシステムが稼働し、70～80台のサーバで運用されている。そしてそれを管理しているのは、情報システム部のシステム担当者と、外部委託されているMSP事業者である。

彼らはサーバを管理するための特別なアカウント「特権ID」を持っている。もし特権IDが悪用されればサーバ上のシステムを自由に改変し、侵入の痕跡を消去することさえ可能だ。そのため特権IDを適切に管理することは、トラブルを未然に防ぎ、システムを健全に維持、運用するために不可欠なのである。特にサーバには顧客や社員の個人情報も含まれている。同社情報システム部 情報基盤グループ リーダー 課長 後藤 一郎氏は、ログ管理を含む厳重な対策が必要と考えていた。

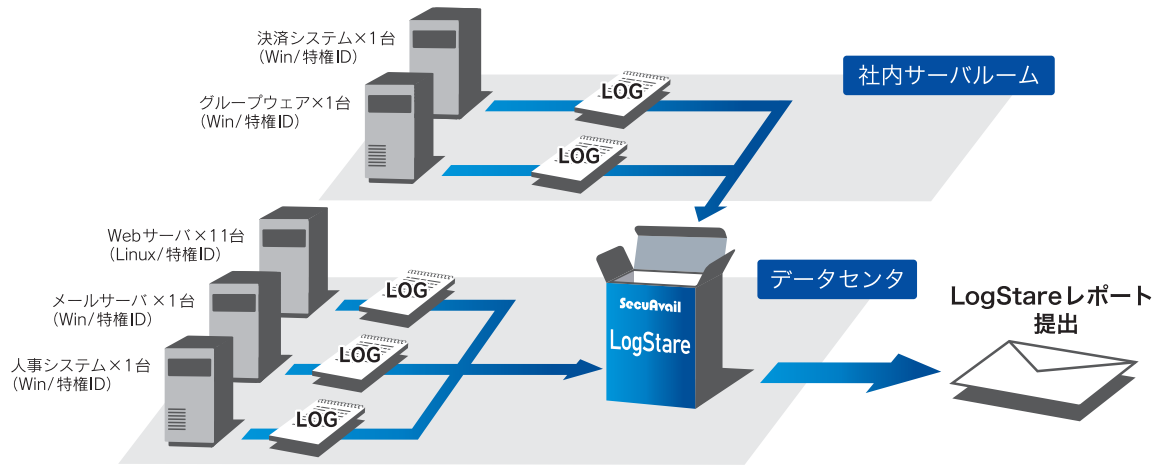
#### 特権IDと個人情報の管理は

企業にとって死活問題。

それにはログ管理が必須

「当社のサーバにはお客様や社員の個人情報も保管されています。個人情報の管理は非常に重要なことで、仮に間違いが起こったときには死活問題につながります。そこでかねてから特権IDのログ管理の強化を検討してきました。内部統制においても特権IDと個人情報の管理は重要視されています。」

以前からサーバに関するログはすべて保管していたが、保管したログはシステムごとに分散されており、それを効率よく収集し分析する機能が弱かった。その問題を、MSP事業者に相談したところ、紹介されたのがLogStareだった。



## 多種多様なシステムが 混在する環境で効率的な ログ管理を実現

同社のシステムには異なる環境が混在していた。サーバのOSにはWindows ServerとUNIX系のSolarisが使われている。稼働しているアプリケーションの中には独自開発したものもある。そのため独自形式で出力されるログもあり、なかにはログを出力しないアプリケーションさえあったのである。

そのように複数の形式が混在するログを取り込むには、LogStareが適していたのである。

後藤氏にLogStareを勧めたのは紀伊國屋書店のEコマースサイトの運用を受託しているサイタスマネジメントである。同社は、MSP事業者として企業向けシステム監視・運用管理業務を数多く手がけている。

多数のログ管理製品の中からLogStareを選んだ1番の理由は、LogStareのULPというオプション機能にある。この機能はあらゆる形式のログの取り込みを実現するもので、同社のような多種多様なシステムが混在する環境でのログ管理に効果を発揮する。ログを出力しないアプリケーションの場合は、OS上に残されたログイン、ログアウトの記録を取得して対応することも可能だった。

MSP事業者からの説明を受け、後藤氏はLogStareの導入を決めた。

## ログ監視されている 緊張感が不正使用の 抑止力に

導入後に感じた効果として後藤氏は、抑止効果を挙げる。

「特権IDを持つユーザにはLogStareでログ管理されていることを告知しています。そのためシステム担当者は常に、自分のサーバへのアクセスが監視されていることを意識するようになります。私自身、サーバにアクセスするときは以前にも増して緊張感を持つようになりました」

## 外部委託業者が 正当性を証明できる という安心感

エキスパートであるMSP事業者自身も外部委託されている立場からログ管理のメリットを享受している。

「私たちは外部から紀伊國屋書店様のシステムにアクセスしていますが、作業した履歴が後藤様の目に触れるので、以前よりも慎重に、そして丁寧に作業するようになりました。また何か問題が起こったとしても、LogStareを見れば自分に責任がないということも明確になります。ログ管理されることは行動を監視されることでもあります。自分の正当性を証明できるという安心感もあるのです」

## 報告書作成の手間が 大幅に軽減

後藤氏は、月例のセキュリティ委員会でも提出する報告書もLogStareで作成している。

「LogStareはPDF形式でレポートを出力する機能を持っています。この手のツールは画面に映っているものをそのまま出力するだけのものも珍しくはないのですが、

LogStareはグラフを含んだ非常に見やすいレイアウトの報告書を出力できます。そのため加工の必要もなく、そのまま報告書として利用できます」

## システムの 安定稼動にも貢献

「ストレージの使用状況、ハードウェアの状況、突然起こった再起動などのイベントの記録もログを見ればわかります。それらを分析することで故障によるトラブルを未然に防ぐことができます。エラー情報も詳細に把握できるようになったので、古い設定が残されているパソコンが自動的にサーバにアクセスを繰り返しているようなケースも見つけられるようになりました」

LogStareは本来の目的である特権IDの管理強化のみならず、同社のシステムの見えない不安を浮き彫りにし安定稼働させることにも役立っていた。

# SecuAvail

株式会社セキュアヴェイル

本社 / 〒530-0044  
大阪府大阪市北区東天満 1-1-19 アーバンエース東天満ビル  
TEL 06-6136-0020

東京ランチ / 〒100-0011  
東京都千代田区幸町 1-1-1 帝国ホテルタワー 16F  
TEL 03-5511-8757  
E-Mail : sales@secuavail.com  
URL : http://www.secuavail.com

○このカタログの情報は2010年7月現在のものです。内容は事前の予告無しに変更する場合があります (CS201007-1)  
○本事例中に記載の冊書きや数値、固有名詞等は初掲載当時のものであり、閲覧される時点では、変更されている可能性があることをご了承ください。  
○製品、サービス等詳細については、弊営業担当員にご相談ください。

※SECUAVAIL、LOGSTAREは、株式会社セキュアヴェイルの商標です。  
※その他の会社名および製品名は、各社の商標または登録商標です。  
※Copyright ©2010 SECUAVAIL Inc. All Rights Reserved.