

## USBメモリなどポータブルデバイスによる情報漏えいを防止する秘策 「McAfee Device Control」

### 導入事例 株式会社 京樽

京樽

●株式会社 京樽について  
1932年、京都の河原町の割烹料理店として創業した京樽は、テイクアウト専門の鮭チェーン「京樽」や、でかネタ回転寿司「海鮮三崎港」、すし全皿105円の「うおえもん」、にぎり鮭2コ240円均一の江戸前専門店「すし三崎丸」などを運営する外食企業です。業界でいち早くメニューにカロリー表示を導入するなど、健康や食の安全性に力を入れ、業務の効率化を図るためのITシステムによる情報管理など、IT化にも積極的に取り組んでいます。

本社所在地  
〒103-0013 東京都中央区日本橋人形町3-8-1 TT-2ビルディング内  
電話: 03-5847-2311 (代)  
www.kyotaru.co.jp/

●業種  
フードサービス業

●導入製品  
McAfee Device Control、  
McAfee ePolicy Orchestrator

データの利用形態が可視化されたことで、次にどの対策をすべきかが具体的に見えてきました。

ITを基盤に業務展開する今日の企業にとって、情報セキュリティ管理は大きなテーマです。特に昨今は顧客情報などがUSBメモリなどのポータブルデバイスから漏えいする事件が多発しており、早急な対策が求められています。こうした問題に早くから注目し、数あるデバイス保護ソリューションを検討していた京樽は、McAfee Device Controlを選択しました。導入の決め手や効果について、同社管理本部、情報システム部の方々に伺います。



#### 懸念材料はUSBメモリによるデータ持ち出し管理と情報漏えい

「茶きん鮭」でお馴染みの株式会社京樽は、テイクアウト専門の鮭チェーン「京樽」や回転寿司「海鮮三崎港」などを展開する老舗の外食企業です。同社は、「おいしさ健康」、「食の安全、安心」をモットーに、早くから品質管理室を設置し、業界で初めてメニューのカロリー表示を実施、製造工程で発生しうる危害を分析して管理する「HACCP」(危害要因分析に基づく必須管理点)で認証を受けるなど、食の安全性に対して積極的な取り組みを行っています。

こうした経営理念を裏で支えるのが、同社の情報システム部です。「カロリーや原材料表示などをラベルに記載するシステムは情報システム部で開発しています。」と語る同社管理本部情報システム部担当の新田加奈子氏は、情報システム部が品質管理業務と消費者をITで橋渡しする重要な役割を果たしていると説明します。また、最近では食品に含まれるアレルギー物質についても表示が義務化されました。追加で管理する情報は日々増加しており、データベースの管理業務だけでも大変と、同部課長の後藤博氏は漏らします。

しかも、これに加えて企業データの保護を含むセキュリティ対策も推進しなければなりません。同社は2004年4月、個人情報保護法への対応に向けた情報セキュリティ管理部会を発足しています。同部会は現在コンプライアンス対策部会へ名前を変えており、情報システム部はその下でポリシーに基づくシステム運用を実施しています。

業界固有の法規制やコンプライアンスへの遵守、それに伴う情報セキュリティ対策の強化など、業務は増加する一方ででした。プライオリティの高い情報漏えい対策についても、一気に実現するのは困難であることから、「すでにファイルサーバーの重要なファイルへのアクセス管理については完了していた上、ノートパソコンについてもハードウェア暗号化が実施済みでした。次のステップとしてUSBメモリなどポータブルデバイスによる持ち出しの管理に着手するといった、段階的な導入を検討していました。」(同部部長、佐山和彦氏)

ポータブルデバイス経由での情報漏えいは、取引先企業から予約注文客まで、多種多様な個人情報を扱う京樽としては徹底的に回避したいリスクです。すでに市場には多数のデバイス制御製品が登場している中、早急な導入策が求められました。

#### McAfee Device Controlで安心を実感

製品の選定を開始してから、約4ヶ月。しかし、操作性の問題や既存システムへの対応といったさまざまな問題が噴出し、なかなか決定に至りません。そんなある日、偶然マカフィーの営業担当からMcAfee Device Controlの紹介を受けます。

McAfee Device Controlは、USBメモリやMP3プレーヤー、CD、DVDなど各メディアに対して、書き込みの制限や監視、フィルタリングなどを実施するソフトウェアです。エージェントをクライアント端末にインストールすることで、使用可能なデバイスの限定やファイル単位での書き込み制限、特定アプリケーションからのデータコピー禁止などを実現します。

「弊社では、すでにエンドポイントセキュリティのスイート製品であるMcAfee Total Protection for Endpointや、管理ツ-

ルのMcAfee ePolicy Orchestrator<sup>®</sup>などを使用しており、製品群の機能性や拡張性が高いことを知っていました。マカフィー社から提案頂いた購入価格もさることながら、McAfee Device Controlであれば新規に管理サーバを導入したり新たに操作を覚えたりせず、McAfee ePolicy Orchestratorで既に導入済みのセキュリティ製品と一括で管理でき、運用コストも抑えられるということから、すぐにでも検討しようということになったのです。」(後藤氏)

仕様確認は1週間、動作検証は2週間かかりました。その間、マカフィーのシステムエンジニアが導入のサポートをフルバックアップし、疑問や確認事項などを1つずつ潰していきました。こうして問題ないと確認を得た同部は、約300ライセンスを購入し、2008年12月初旬、USBメモリなどを業務で頻繁に使用する社員20名と情報システム部にてテスト導入を開始しました。全社員への展開は、McAfee ePolicy Orchestrator 4.0へのアップグレードとあわせて、12月末までに実施する運びとなりました。「デフォルトで動作するので、設定の難しさもなく、比較的少ない作業で導入へ漕ぎ着けたと思います。」(佐山氏)

テスト期間では、どのようなポータブルデバイスが使われており、どの頻度で使用されているのかを調査するため、ログ取りに専念しました。ログ取りを行った理由として、佐山氏は「業務上で利便性が下がることは避けたいので、まずは使われ方を知ることから始めたかった。」と説明します。現場での利便性を下げることは、往々にして業務効率に支障をきたします。円滑な業務を支えるのがITシステムであり、それを阻害するような対策はとらないという判断でした。「その上で、例えば読み取りは可能、書き出しは制限するといったポリシーを策定し、万が一のデバイス紛失時にもデータを保護できる仕組み作りをしたいと考えています。」

実際、「ログでデバイスの利用が可視化されたことで、今後どのような対策をとるべきか、具体的に見えてきました。」と後藤氏は言います。McAfee Device Controlの導入は、セキュリティ対策の推進において大きな足がかりとなったのです。

### 今後はメールセキュリティなどを含むMcAfee Data Loss Preventionへのアップグレードも検討

もう一つの導入メリットは、利用実体を把握しながら利用者へのある程度の牽制を実現できたという「安心感が得られたこと」(佐山氏)です。この安心感は、利用者側も感じてもらえるものだとして後藤氏は強調します。「本格稼働が始まれば、多少の制限が敷かれるため、現場からは不満の声が上がるかもしれませんが、利用を続けていけば、余計な心配や作業をしなくてもデータが保護されていることが分かってもらえるはずですよ。」何か特別なことをしなくても安心できる。McAfee Device Controlが管理側と利用者側にもたらす安心感というメリットに、同部は期待を寄せています。

このほか、レポートや資料作成に有用である点も評価しました。コンプライアンスでは、要請に応じて必要なデータを収集し、報告書にまとめることが求められます。「今後も規制が強化される可能性は高く、作成すべき報告書も増えると思われそうです。」(佐山氏)

ユーザやデバイスごとのログ情報を管理し、タイムスタンプやデータ証明などのイベントを詳細に収集できるMcAfee Device Controlであれば、監査に必要な情報を漏れなく提供できます。

同社はこれで、ノートブックPCのHDD暗号化、USBメモリなどリムーバブルメディアの不正使用防止を実現しました。次のステップでは、電子メールの添付ファイルによる漏えい防止を含めたメールセキュリティを考えているそうです。McAfee Device Controlは、ライセンスキーを追加するだけで電子メールへの添付やWebへの投稿、印刷など、保護対象データの操作の制御やログ収集が可能なMcAfee Host Data Loss Preventionへ拡張することができます。「より統合的なセキュリティ対策を実施すべく、前進していきたいと思えます。」(佐山氏)

取材日:2008年12月

