株式会社エコーステーション 様

万全な対策で外部への情報漏えいを防止
セキュリティ対策の強化と業務の効率化を短期に実現

導入商品

クライアントセキュリティ管理「FUJITSU Software Systemwalker Desktop Keeper」
クライアント資産管理「FUJITSU Software Systemwalker Desktop Patrol」

課　題	効　果
■ お客様情報を不正操作から守りたい	→ ■ データの持ち出し状況を把握して不正操作を抑止
■ USBメモリ紛失による情報漏えいを防止したい	→ ■ セキュリティポリシーの統制と暗号化で情報漏えいを防止
■ ICT資産の管理にかかる煩わしさを解消したい	→ ■ ICT資産を一元管理して全社のセキュリティリスク把握と効率化を実現

エコーステーションでは、情報漏えい対策に「FUJITSU Software Systemwalker Desktop Keeper」と「FUJITSU Software Systemwalker Desktop Patrol」を導入。従業員の業務特性を考慮し、セキュリティ対策の見直しを図った。お客様情報の保護を強化するとともに、ICT資産の一元管理と全社のセキュリティポリシーの統制も実現した。同社は今後、自社の導入実績をモデル化し、お客様に向けて情報漏えい対策ソリューションの提案を進めていく。

導入の背景

万全なセキュリティ対策を目指し システムによるセキュリティ管理を見直し

エコーステーションは、主に首都圏でICT機器の販売と保守メンテナンスのビジネスを展開する。同社は各種契約情報などに記載されるお客様情報を守るため、セキュリティ対策を講じている。「個人情報を預かる企業として、情報管理体制の整備はもちろんですが、セキュリティ事故を防止するための社員教育が重要です。万全を期するためには、さらにシステムによる対策強化も必要となります」と代表取締役兼CEOの岩崎拓二氏は語る。

同業他社で発生した転売目的の顧客名簿持ち出し事件が、同社のシステムによるセキュリティ管理のあり方を見直すきっかけとなった。当時導入していたセキュリティ対策ソフトウェアでは、パソコンの操作ログは取れるようになっていたが、ファイルを持ち出したことで情報漏えいが起こった場合、どのファイルが持ち出されたかを確認できる機能はなかった。

岩崎氏はセキュリティ対策ソフトウェアの見直しを決意した。とは言え、業務の進め方などを変更すると社員への負担が大きくなる。「社員に負担をかけずに、お客様情報を守る仕組みが必要でした」と岩崎氏は振り返る。

導入のポイント

情報漏えい対策とICT資産管理の 機能の豊富さが導入の決め手

同社は2014年10月、情報セキュリティ対策の強化を目的にSystemwalker Desktop Keeper（以下、DTK）とSystemwalker Desktop Patrol（以下、DTP）の導入を決めた。セキュリティ対策ソフトウェアの選定と導入を担当

株式会社エコーステーション
代表取締役兼CEO
岩崎 拓二氏

株式会社エコーステーション
OA事業本部
ビジネスソリューション事業部技術部
エリアサービス&サポート課リーダー
佐川 正吉氏

お客様プロフィール

株式会社エコーステーション

OA Network Planner Eco Station

本社所在地	埼玉県川越市新宿町6-3-5
設立	1998年10月
資本金	3,000万円（単体）
代表取締役兼CEO	岩崎 拓二
従業員数	25名（単体）
ホームページ	http://www.eco-station.co.jp/
事業内容	IT機器コンサルティング並びに IT機器保守メンテナンス業務

したOA事業本部ビジネスソリューション事業部技術部エリアサービス&サポート課リーダーの佐川正吉氏は、「以前よりお客様からもセキュリティ管理システムの相談をいただいていたこともあり、各社のセキュリティ製品の情報を集めて比較していました。DTKとDTPの導入がベストな解決策でした」と語る。

DTKは、パソコンの操作ログ管理、ファイルの持ち出し禁止、許可されていないUSBメモリの使用禁止、PrintScreenキーの無効化などの基本機能に加えて、持ち出しファイルの強制暗号化、ファイル操作の追跡、スマートデバイスを含めたログ収集や検索といった幅広い情報漏えい対策機能を有する。「注目したのは、ログの記録とともに、持ち出したファイルが原本として自動的に保管される点です。万一、USBメモリを紛失しても、ファイルの中身がわかれば迅速に対応できます」と、佐川氏は導入の決め手を語る。

DTPにより、パソコンやスマートデバイス、周辺機器（プリンタやファックスなど）のICT資産全体をセキュリティと資産の両面で一元管理することで、全社でセキュリティポリシーを統制できる。セキュリティ管理面では、セキュリティパッチやウイルスパターンファイルなどの適用状況を一目で把握し、セキュリティパッチをクライアントへ強制適用できる。DTPがパッチ適用機能を有するため、WSUSサーバのようなパッチ専用サーバは必要ない。資産管理面では、管理対象機器の契約情報や導入したソフトウェアのライセンス状況を管理できるため、リース切れやライセンスの過不足を把握し、コスト削減につなげることも可能だ。佐川氏は、「富士通は業務の中でDTKとDTPがどのように使えるかを分析して、効果的な利用方法を提案してくれました。富士通の手厚いサポートに大きな信頼を置いています」と続ける。

システム概要

現行システムに影響なく稼働開始
セキュリティポリシーの統制も短期に実現

ファイルサーバにはDTKとDTPのサーバ用ソフトウェアを、全社のパソコンには、クライアント用ソフトウェアをインストールしたが、インストールに伴う業務システムの変更は必要なく、DTKとDTPの導入にあたっては社員の混乱も全くなかった。導入決定からわずか2カ月弱、2014年12月にシステムが稼働。運用が始まってから約1年、「従来品に比べ、セキュリティパッチの自動配付などによりシステム管理を担当するIT部門の負担はありません」（佐川氏）と運用もスムーズだ。

「全社のセキュリティポリシーを統制できたことと持ち出しファイルを強制暗号化できたことで、情報の流出を防止し、セキュリティリスクを低減できています」と岩崎氏は語る。

導入効果と今後の展望

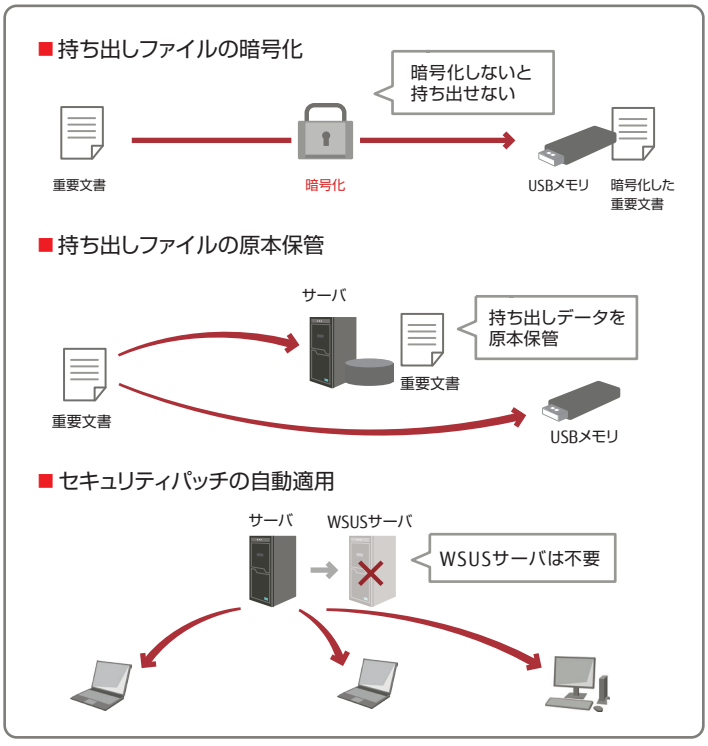
自社の導入実績をモデル化
お客様に最適な情報漏えい対策ソリューションを提供

エコーステーションは、DTK、DTPの導入によって、情報セキュリティ対策の強化を実現した。資産を一元管理することで、管理者の業務が効率化され、セキュリティ対策はより万全なものになった。従来はファイルをUSBメモリへコピーして持ち出す際、各社員が自ら暗号化していたが、今では「DTKにより、USBメモリにコピーするファイルは強制的に暗号化できるようになりました」（佐川氏）。

同社は複数の営業拠点を有しているが、今後拠点が拡大すれば、各拠点で保有するお客様情報には担当拠点からのみアクセスを認めるといった、よりきめ細かな管理が求められる。このような将来的な対策もDTKとDTPの導入により、「拠点に応じたセキュリティポリシーの設定を簡単に変更できます」（佐川氏）。

今後の展望として、自社の導入実績をモデル化することで、情報漏えい対策ソリューションの提供にも注力していく。同社は持ち出しファイルの強制暗号化などによるセキュリティ対策を講じているが、お客様によっては、より強固な禁止機能を用いるなど、必要とされる対策は企業によって異なる。お客様が必要とする多種多様なセキュリティ対策に応える提案ができるよう、自社でも継続的にセキュリティ対策を強化していく方針だ。セキュリティ管理のソフトウェア導入が実は容易であることや、お客様のシステム規模に関係なく最適な情報漏えい対策ソリューションを提供できることを強調していく考えである。

【導入の3つの決め手】



お問い合わせ先

富士通コンタクトライン（総合窓口） 0120-933-200

受付時間 9:00 ～ 17:30（土・日・祝日を除く）

富士通株式会社 〒105-7123 東京都港区東新橋 1-5-2 汐留シティセンター

http://www.fujitsu.com/jp/software/systemwalker/desktop-keeper/

http://www.fujitsu.com/jp/software/systemwalker/desktop-patrol/

●このカタログには、環境に配慮した用紙、植物油インキ、有害な廃液を出さない水なし印刷方式を採用しています。

CZ8532-2016 年 2 月