活用事例

金融業（ネットバンク）
Symantec Data Loss Prevention
楽天銀行株式会社 様

Symantec Data Loss Preventionで情報の保護と安全な運用を実践

楽天銀行株式会社　システム運用本部長　早川　一 氏
システム運用本部 システム管理部 兼 リスク管理本部
総合リスク管理部 情報セキュリティオフィサー　藤島 真人 氏
システム運用本部 システム基盤部　星野 修平 氏

世界一のインターネット専業銀行を目指し、機密情報の管理と保護を強化

2001年にイーバンク銀行として開業し、2009年の楽天グループ入り後、楽天銀行に社名を変更。現在410万口座を超える顧客数を誇る国内最大のネットバンクに成長。楽天グループの一員として、更なる拡大を目指し、数多くのサービスを提供している。同社では、社内のサーバーに蓄積されている機密情報を安全かつ的確に保護するために、Symantec Data Loss Prevention（以下DLP）を導入した。

- Windows ベースのファイルサーバーと大型ファイルサーバーを監視
- 当該データに対するアクセスの定期監査レポートを作成
- サーバー内にあるファイルのアクセス状況を的確に把握

会社概要

楽天銀行株式会社

- 従業員数：単体261人、連結299人
  （2010年3月31日時点）
- 業　　種：金融業
- 事業概要：
  電子メディアによる銀行業、おもに決済業務
  http://www.rakuten-bank.co.jp/

導入概要

- 製品名
  - Symantec Data Loss Prevention
- 概要
  - 保存場所や使用場所に関わらず、機密データを検出、監視、保護する、総合的なコンテンツ重視のソフトウェア
- 主な機能
  - 機密データ所有者の特定・保護
  - データ所有者の推察・特定

課題　個人情報や機密情報の安全性を守るための監視ソリューションの必要性

Symantec DLPを導入する以前の背景や取り組みについて、システム運用本部の早川一本部長は、次のように振り返る。

「当行では、設立当初からオープンシステムによる自社開発のシステムでサービスを提供してきました。そのおかげで、数あるネットバンクの中でも、先進的な取り組みやサービスをいち早く開発してきました。一方で、ネットバンクという特長から、常に外部からの攻撃という脅威とも戦ってきました。また金融機関であることから、社内のサーバーに保管されているデータの保護に関しては、積極的に取り組んできました。しかし、以前から試験的に導入していた他社製のログ管理ソリューションでは、効果的な監視や監査ができませんでした。そこで、より効果的で実用性の高い情報漏えい防止ソリューションを求めていました」

以前のログ管理システムの問題について、システム基盤部の星野修平氏が補足する。

「以前使用していたログ管理ソリューションでは、アクセスログをCSV形式でファイルに保存するだけなので、その後で自分たちでExcelなどを使って読み込んで整形して解析しなければなりませんでした。リアルタイムではないので、実際に不正なアクセスなどがあっても、即座に検知できないという問題がありました。また、実際の監視では、アクセスの失敗ログだけを監視してもあまり意味がなく、成功ログが適切なものかどうかを判断できなければなりません。旧システムでは、こうした判断が困難でした」

選定理由　高性能な保護機能と使いやすさでSymantec Data Loss Preventionを選定

「アクセス検知の不十分さに加えて、以前のソリューションでは、あらかじめ監視対象となるファイルサーバーなどの情報を正確に登録しなければなりませんでした。もしも、対象から外れているサーバーや共有フォルダなどで、不正なアクセスがあっても、発見が遅れる可能性があったのです。これでは、監視の意味がありませんでした」と星野氏は問題を振り返る。

楽天銀行のシステム基盤部では、試験的に導入していたログ管理ソリューションが、銀行本体のネットワーク環境に不向きだと判断し、より安全で運用効率の高い監視ソリューションを探すことにした。情報セキュリティ・オフィサーの藤島真人氏は、Symantec DLPを選定した経緯について、以下のように説明する。

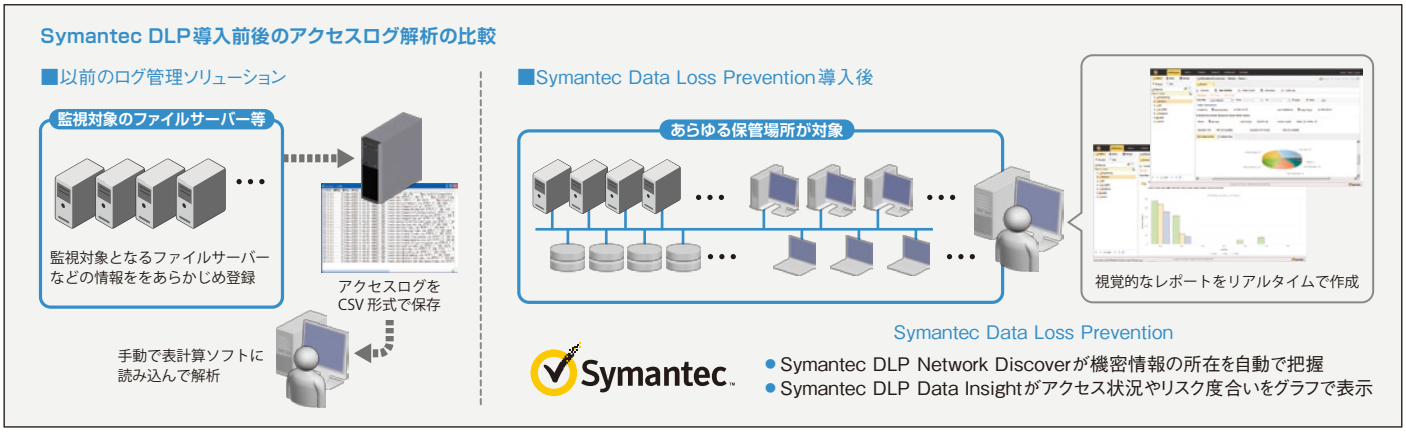
「われわれがログ管理ソリューションに代わる製品を探しているときに、シマンテック社からSymantec DLPの提案がありました。そこで、楽天銀行のシステムを開発していた子会社で、半年ほどかけてテスト運用を行いました」

Symantec Data Loss Preventionは、コンテンツベースの情報漏えい対策ソリューション。ネットワークやストレージ、エンドポイントなど、場所にかかわらず、機密データを検出し監視および保護を

活用事例

Symantec Data Loss Prevention

楽天銀行株式会社 様



行うことができる。同社のテスト運用では、サーバーに保管されている機密情報の所在をデータベース化して、機密ファイルへのアクセス状況などをウェブブラウザから視覚的にリアルタイムで把握できるようにした。

導入効果　これまで見落とされていたファイルの保管場所なども明確になる

楽天銀行では、いくつかあるSymantec DLPの機能の中から、機密情報の所在を明らかにするSymantec DLP Network Discoverと、情報の利用状況を分析し分かりやすく表示するSymantec DLP Data Insightを利用している。Symantec DLP Network Discoverの高度な検出機能によって、システム基盤部の作業も大幅に軽減した。機密データが保存されている場所を探し出して、機密データのインベントリを自動的に作成し、データの管理と整理を実行してくれるためだ。

「Symantec DLP Network Discoverの検出機能によって、これまでわれわれが認識していなかったファイルの保管場所も、的確に把握できるようになりました。またアクセスの状況がグラフなどで可視化されるので、これまでと比べて圧倒的に見やすくなりました」と星野氏は導入の効果について話す。

高性能な検知機能によって、管理者の手を煩わせることなく、サーバー内の機密情報が自動的に収集されるので、これまで見落とされていた共有フォルダや重要なファイルも、監視から漏れる心配がなくなった。それに加えて、アクセスの状況やリスクの度合いがグラフ化されるので、脅威の程度をリアルタイムに的確に把握できるようになった。

「以前のソリューションでは、アクセスログが膨大なテキスト情報でプリントアウトされていました。正直、見る気が起きないレポートなので、監視をしている意味が感じられませんでした。しかしSymantec DLP Data Insightが作成するグラフならば、安全にファイルがアクセスされているかどうかが、すぐにわかります。これならば、楽天銀行の本部システムで運用しても、十分に効果が上がると判断できました」と早川氏は試験運用から本採用に至った理由を説明する。

「運用している部門としても、監査レポートの作成が正確で容易になりました。正直、社内の情報の保管場所は、日々刻々と変わっているので、一ヶ月前の情報では役に立たないこともあります。それだけに、Symantec DLP Network Discoverによる保管場所の正確な検知は、とても重宝しています。これまで、管理部門では把握しづらかったファイルの保管場所なども発見できるようになりました」と藤島氏は導入の成果を評価する。

今後の展望　保護の強化とWindows以外のOS環境にも導入を計画

Symantec DLP Network Discover及びData Insightによって、サーバー内に散在する機密情報の正確な保管場所とアクセス状況を把握できるようになった楽天銀行のシステム基盤部では、さらなる保護の強化と安全性の確立に向けて、取り組みを推進していく考えだ。

「今後は、ネットワークやWindows以外のOS環境にも、導入を計画しています。また監視だけではなく、漏えい防止に向けたソリューションへの拡張も検討しています。これからもセキュリティに対する脅威は増えていくので、当行としてはシマンテック社に対して、さらなる積極的なソリューションの提案や情報の共有を期待しています」と早川氏は今後に向けた抱負を語った。

楽天銀行株式会社
システム運用本部長
早川 一 氏

楽天銀行株式会社
システム運用本部 システム管理部
兼 リスク管理本部 総合リスク管理部
情報セキュリティオフィサー
藤島 真人 氏

楽天銀行株式会社
システム運用本部
システム基盤部
星野 修平 氏

株式会社シマンテック
〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ
www.symantec.com/jp

お問い合わせ

E1303CR0-bb-DLPRKTN