



1日5万通の電子メールを ウイルスの脅威から守る

金融機関にとってウイルス感染などは、単に業務運営上の支障にとどまらず、金融機関としての信認を損なう風評や、リーガルリスクを招くなど、影響は計り知れない。そのため、ウイルス対策ソフトウェアには必然的に、実装するセキュリティ機能に高い信頼性が要求されることになる。そうした要求を満たすものとして東京三菱銀行は、1日5万通に達する電子メールのウイルス対策ソリューションとして「Symantec Mail Security for SMTP」を選択した。

情報資産を統括的に管理する情報セキュリティ管理室



東京三菱銀行
情報セキュリティ管理室
主任調査役
齋藤雅則氏

金融システムは日本にとって重要なインフラであり、そのセキュリティ対策については一企業の問題だけでなく、社会インフラ全体の問題として各金融機関が対策に取り組んでいる。金融機関のコンピュータシステムは基幹系、勘定系にかかわらず個人情報を伴う重要な情報を有するシステムとなっている。そのため、従来のようにネットワークを含むコンピュータシステムとそれを運用する人とを分離して管理することは難しくなっており、さらにはコンピュータシステムそのものだけでなくその中で取り扱われる情報やそれを取り扱う内部外部の人についても十分なリスク評価と対策を実施していく必要が生じている。

「以前は、システムリスクについてはシステム部門が、それ以外のリスク管理全般は経営企画部門などで評価や対策を実施してきましたが、情報セキュリティの統括的なリスク管理の必要性を認識し、1999年7月に『情報セキュリティ管理室』が設置されました」(東京三菱銀行情報セキュリティ管理室主任調査役 齋藤雅則氏)。

情報セキュリティ管理室の当初のミッションは、情報セキュリティポリシーの策定と、組織としてそれを運用していくための組織体制の検討だった。運用していく中で齋藤氏は、「企業文化にあったポリシーでないと遵守されません。厳しすぎても甘すぎても機能しないし、用語にしてもわかりやすい表現で最終的に個人のリスク認識を高める施策が重要です。それを共有して全行的にリスクに対する感覚を磨いてリスク回避に向かう必要があります」と述べ、システムに対するセキュリティ関連の投資と実効性に関する課題とともに、扱う人に対する情報セキュリティ教育など、基本的な施策の重要性を強調する。

その例として、同行では各部署にセキュリティ管理者を配置して、全行員に情報セキュリティに関する教育がいきわたるような体制を構築している。

「例えば電子メールによるウイルス感染は、エンドユーザーにおける最も身近な脅威になるもので、ユーザー教育が非常に大切だと考えています。最新のウイルス対策の傾向などを取り上げ、陳腐化しない形で実効性のあるセキュリティ教育を展開しています」(東京三菱銀行情報セキュリティ管理室調査役 齋藤由美子氏)。



東京三菱銀行
情報セキュリティ管理室
調査役
齋藤由美子氏

ゲートウェイレベルでウイルス対策を実施

一方、セキュリティインフラの整備に関する対策も情報セキュリティ管理室発足時から重要なテーマだったという。銀行のシステムはホストコンピュータを中心に開発され、閉域ネットワークで運用されてきた期間が長いだけに、情報系を中心としたオープン系システムの浸透とともにセキュリティインフラ整備の重要性は急速に高まった。加えて同管理室を設置してすぐにインターネット・バンキング・サービスの開始などもあり、セキュリティインフラの強化は最重要課題として取り組んできた。現在、東京三菱銀行の電子メールを利用するクライアントPCは国内の営業店で約1万6,000台あり、1日に約4万～5万通のメールがゲートウェイを通じて送受信されている。これらはセンターにあるゲートウェイ型アンチウイルスシステムでチェックされる仕組みになっている。6年前に全行を集約したメールシステムを構築し、ゲートウェイで電子メールに対するウイルス対策を実施した。

「旧三菱銀行と旧東京銀行の合併を機に両行で使用してきた製品を検討し、大手セキュリティベンダーのアンチウイルスソフトを使用してきました。しかしそのソフトウェアには運用上の課題がありました。

東京三菱銀行

株式会社東京三菱銀行

設立：大正8年(明治13年創業)
資本金：8,719億円
店舗網：国内267、海外73
総資産：87兆6,866億円
業務純益(単体)：4,668億円
自己資本率：11.97%(2004年3月末)



Symantec Mail Security for SMTP

>ゲートウェイでSMTPトラフィックを監視します。ウイルス対策、コンテンツフィルタリング、スパムメール対策を統合し、ウイルスやワームの検出、スパムメールのブロックを行います。HTMLベースのコンソールを採用し、ローカル/リモート問わず容易に管理が出来ます。



東京三菱銀行
システム部
調査役
金原一郎氏

それはウイルス定義ファイルの更新タイミングでした。サーバ側でウイルス定義ファイルをダウンロードして更新するタイミングだけでなく、新種ウイルスの発生から定義ファイルの作成や提供までの迅速性を含めたセキュリティ企業としての体制が重要でした」(東京三菱銀行システム部調査役 金原一郎氏)。

当初使用していた製品に替わって東京三菱銀行のネットワークシステムの運用を行っている三菱電機情報ネットワークにより2年前に導入されたのが、「Symantec Mail Security for SMTP」(導入当時の名称はSymantec AntiVirus for SMTP Gateways)である。

セキュリティ企業としての信頼性

365日24時間体制でインターネット上の脅威を監視し、その対策を研究・開発する「Symantec Security Response」を高く評価している。

「最近のウイルス感染拡大の傾向として、新種のウイルスが発見されてから短時間に急速に蔓延していくとともに、亜種が短いサイクルで次々と生み出されるということがあげられる。したがって、新種・亜種のウイルス発見からウイルス定義ファイルの作成・配布までのタイミングが非常に重要な要素になっている。『Symantec Security Response』によるサポートは、そうした問題に迅速に対応してくれる」(金原氏)と強調する。

機能的優位性で「Symantec Mail Security for SMTP」を選定

「Symantec Mail Security for SMTP」は、ウイルススキャン、コンテンツフィルタリング、スパムメールへの対処など、SMTPゲートウェイにおける包括的なセキュリティを提供する。サービスを停止することなくスキャンエンジンをアップデートするNAVEX、新種ウイルスに対応するためのLiveUpdate機能、未知のウイルスを検出するBloodhound技術などを実装し、的確かつ高いパフォーマンスでウイルススキャンを実行する。

「アンチウイルス製品は、セキュリティレベルを高く設定すると誤認識が増加し、低く設定するとウイルスを通過させてしまう可能性があるが、『Symantec Mail Security for SMTP』はそうした問題にも悩まされることなく的確なウイルススキャンを実行する。また、大量のメールを処理できるパフォーマンスの高さ、ローカル/リモートを問わずに容易かつ充実した管理機能など、エンタープライズ製品としての優位性があると総合的に判断して選定しました」(金原氏)とSymantec Mail Security for SMTPを選択した動機を述べる。

「コンピュータウイルスからシステムを保護することは、お客様を相手にしている行員の仕事を守ることでもあり確実な対策が必要です。しかし、金融機関としてそこには適切な対価を常に考慮する必要があります。費用対効果の妥当性も満足させるものでした」(東京三菱銀行システム部調査役 徳永瑞彦氏)。

さまざまなリスクを抱える銀行にとって、リスクに見合った適切なリターンを確保・維持することは重要な課題となっている。コンピュータウイルスというシステムリスクを回避するために、金融機関としての厳しい見極めで選ばれたのが「Symantec Mail Security for SMTP」である。



東京三菱銀行
システム部
調査役
徳永瑞彦氏

株式会社シマンテック

〒150-0031 東京都渋谷区桜丘町20-1 渋谷インフォスター17F

お問い合わせ先

コーポレートカスタマーサービスセンター

電話受付時間：月～金 10:00～12:00、13:00～17:00(土・日・祝日・年末年始を除く)

電話：03-3476-1426

FAX：03-3476-1159

www.symantec.co.jp