Beyond the Bank
あなたの明日へ

OKINAWA KAIHO 海邦銀行

株式会社沖縄海邦銀行

標的型攻撃やランサムウェアが急増するなか、
メールの安全性を
Eメール・セキュリティー管理サービスで担保

沖縄県に拠点を置くリテール・バンクである株式会社沖縄海邦銀行（以下、沖縄海邦銀行）は、標的型攻撃メールやランサムウェアなど、ますます悪質化・巧妙化していくサイバー攻撃に対して行内における人的・組織的対策の強化に加え、「IBM® Eメール・セキュリティー管理サービス」（以下、ESMS）を導入。ウイルスメールなどの脅威が入ってくる前に行外で歯止めをかけるという基本方針に沿ってウイルス感染のリスクを低減するとともに、不審メールの調査のために長時間を費やすことがなくなり、業務負荷を軽減することができました。

お客様情報

株式会社沖縄海邦銀行

●本社所在地
〒900-8686 沖縄県那覇市久茂地2-9-12
https://www.kaiho-bank.co.jp/

1949年に無尽会社として設立。その後、相互銀行、普通銀行への転換を経て2019年に創業70周年を迎える。中期経営計画では、業容の拡大や収益管理態勢の強化、経営管理態勢の強化、将来に向けてのシステム機能強化などを大きなテーマとし、県内における好調な観光産業や人口の状況を考慮しつつ、地域密着によるボリュームの拡大とシェアアップを図っていく。また、長期的な取組みの一環としてブランディングの強化に着手。「Beyond the Bank あなたの明日へ」をスローガンに掲げ、イメージキャラクターによるPRやSNS、モバイルアプリにも取り組み、「お役に立てる銀行」を目指している。

ウイルス感染が疑われるPCの調査に膨大な時間と手間を費やしていた

沖縄県に49店舗を展開する沖縄海邦銀行は、2015年4月から2018年3月までの第14次中期経営計画において「～New Stage!～地域とともに未来に向けて」というスローガンを掲げ、地域密着の金融サービスをさらに進化させようとしています。

ただ、そうした中での大きな脅威となっているのが、悪質化・巧妙化の一途をたどるサイバー攻撃です。

同行 事務統括部の部長を務める高宮城 毅氏は、「2015年後半頃から当行を狙った標的型攻撃メール（ウイルス添付メール）が急増しています。例えば大手金融機関に成りすました偽装メールが短期間のうちに十数件も発覚したほか、最近ではランサムウェアの感染を試みようとするメールも、延べ30件以上に増加しています」と話します。

また、こうした標的型攻撃やランサムウェアの対策は、これまでなかった多大な負担をシステム部門やさまざまな業務の所管部署に発生させます。

同行 事務統括部 システム担当企画グループ 調査役の山城 克也氏は、「行内のPCにウイルス感染が疑われた場合、システム担当者はその都度、調査にあたる必要があり、膨大な工数がとられています。また、当該PCは丸1日近く隔離されて使えなくなるため、部署自体の業務にも大きな影響をもたらしてしまいます」と話します。

この課題を解決するため、沖縄海邦銀行ではまず「人的・組織的対策」に重点をおいたセキュリティー対策に乗り出しました。

同行 事務統括部 システム担当企画グループの島村 祐介氏は、「役職者を含めたすべての行員にセキュリティー研修を実施しました」と話します。さらに同行 事務統括部 システム担当情報系開発グループの大城 裕紀氏も、「イント

事例概要

課題

- 標的型攻撃メールやランサムウェアなどのサイバー攻撃に対する行内における対策強化

ソリューション

- IBM Eメール・セキュリティー管理サービス（ESMS）

効果

- ESMSが標的型攻撃メールなどの脅威に対して、行外で歯止めをかけることで、ウイルス感染のリスクを低減し、導入後は行内でのウイルス感染と問い合わせが「0」になった
- 不審メールの調査のために長時間を費やすことがなくなり、本来の仕事であるシステム企画や開発に専念できるようになった
- ESMSが提供する充実したログによって、メールの運用管理担当者の業務負担も大幅に軽減された

ラネットのニュースリリースなどでも、あやしいメールを絶対に開かないように周知徹底を図りました」と強調します。

しかしながら、行員のセキュリティー意識をどんなに高めたとしても、万全を期すことは不可能です。人間であれば誰もが持っている“心の隙”を、巧妙に突いてくるのが標的型攻撃やランサムウェアだからです。

そもそもウイルスを社内に持ち込まずにクラウド上で検知・ブロックするサービス形態に魅力を感じた

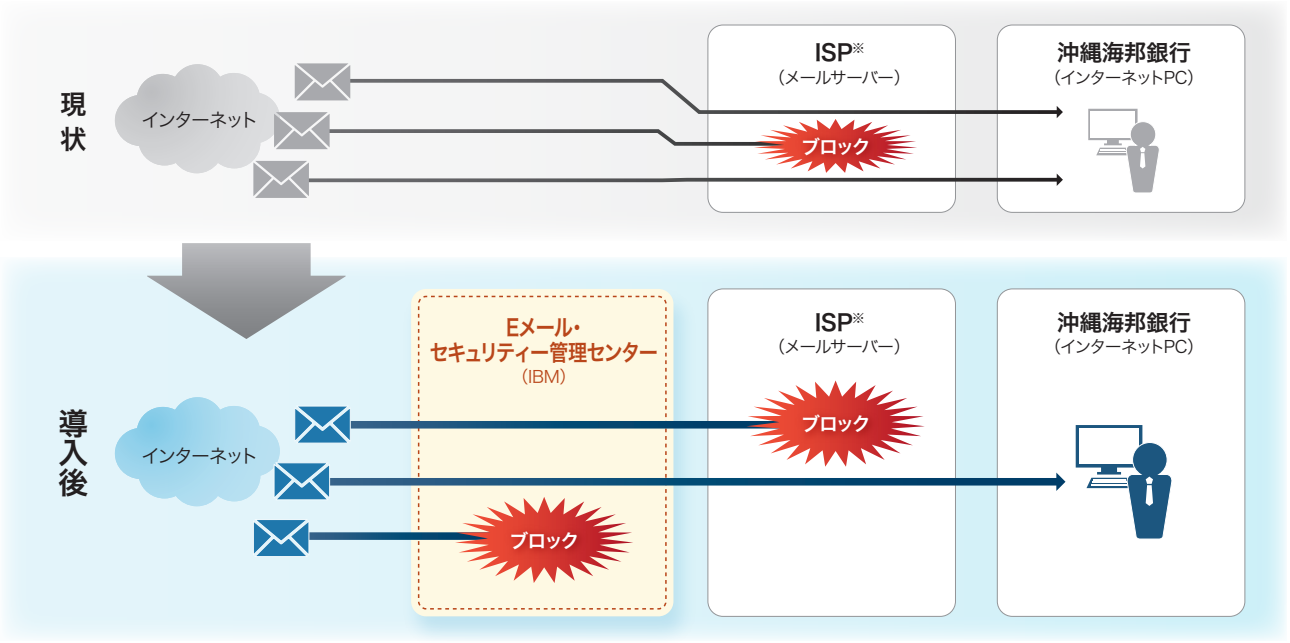
沖縄海邦銀行は、人的・組織的対策と両輪をなす「技術的対策」を求めました。そこにタイミングよくIBMから提案されたのが、ESMSです。

ESMSは、ユーザー企業が送受信するメールをいったんインターネット上で「Eメール・セキュリティー管理センター」が受け止め、セキュリティー対策を実施し、安全と判断されたEメールだけを届けるというクラウド型サービスです。主な機能として、メールに添付されたウイルスを検知してブロックする「アンチウイルス・サービス」、スパムメール（迷惑メール）を検知してブロックする「アンチスパム・サービス」、ユーザー企業が独自に決めたルールに従ってブロックする「コンテンツ・コントロール・サービス」などを提供しています。なお、Eメール・セキュリティー管理センターは全世界十数カ所に展開され、毎日、数十億のEメールのスキャンを行っています。また、グローバルレベルでの負荷分散によりシステムの可用性を確保しています。

2016年6月にESMSに関してIBMと正式契約を結んだ沖縄海邦銀行は、わずか

IBM Eメール・セキュリティー管理サービス（ESMS）導入イメージ

出典：株式会社沖縄海邦銀行



※ISP インターネット・サービス・プロバイダー

新規導入環境　既存環境

“標的型攻撃メールのようなウイルスを「そもそも社内に持ち込ませない」とするESMSの基本的なコンセプトは、まさに当行が描いていた理想像そのものでした”

事務統括部 部長
高宮城 毅氏

“ESMSで標的型攻撃メールの実態をより正確に可視化できるようになったことで、セキュリティー対策の安心感を大幅に高めることができました”

事務統括部
システム担当
企画グループ
調査役
山城 克也氏

2週間程度のリードタイムですぐさま本番運用を開始しました。
「ESMSで何より気に入ったのは、そのサービス形態です。多くの他社のEメール・セキュリティー対策製品は、すべてのEメールを受信してから切り分けを行わなければなりません。これに対して、標的型攻撃メールのようなウイルスを『そもそも社内に持ち込ませない』とするESMSの基本的なコンセプトは、まさに当行が描いていた理想像そのものでした。それでいながら、思っていた以上に安価に利用できることに驚きました」と、高宮城氏は話します。
さらに山城氏も、「インターネット上でEメールをチェックするというサービス形態だったからこそ、当行の社内業務はまったく影響を受けることなく、行員も今までと同じ方法でEメールをやり取りすることができます。クラウド・サービスであるため、新規のシステム導入・構築のような手間もまったくかかりません。契約を結んでからわずか2週間という短期間でESMSを本番業務に適用できた“訳”もそこにあります」と言葉を続けます。

問い合わせ対応および不審メールによるウイルス感染はゼロに

沖縄海邦銀行はESMSを導入する直前の2015年12月からの約4カ月間に担当部署から延べ55件を超える標的型攻撃メールや不審メールの連絡を受けましたが、水面下ではもっと多くの脅威にさらされていると考えられていました。
それがESMSを導入した同年7月以降、ウイルス感染はもちろん、さまざまな業務部門の行員から寄せられる連絡・問い合わせ件数も「0件」となりました。「おかげで不審メールの調査のために長時間を費やすことがなくなり、自分たちの本来の仕事であるシステム企画や開発に専念できるようになりました」と、島村氏は話します。
一方、ESMSが2016年7月にチェックした約4,000通に及ぶすべてのEメールのうち、アンチウイルス・サービスで67件、アンチスパム・サービスで60件、合計127件をブロックしました。
「Eメールの総受信件数は毎月変動するため単純な比較はできませんが、ESMS導入直前の約4カ月間で当行が標的型攻撃メールと特定できたのは、わずか22件にすぎませんでした。つまり、この22件以外は特定不可能であり、ESMSの導入以前はかなり多くの標的型攻撃メールの侵入を見過ごしていた可能性があります。ESMSで標的型攻撃メールの実態をより正確に可視化できるようになったことで、セキュリティー対策の安心感を大幅に高めることができました」と山城氏は話します。
なお、ESMSが効果を上げたのはセキュリティー対策だけではありません。「これまで以上に充実した内容のログが可視化されたことで、メールの運用管理担当者の業務負担も大幅に軽減されています」と強調するのは大城氏です。例えば「送信したはずのメールが相手に届かない」といったクレームを受けた場合、これまではその都度ISP（インターネット・サービス・プロバイダー）に問い合わせなければなりませんでした。それが現在では、「ESMSから提供されるログを見ることで、行内でかなりの部分まで原因を判断できるようになりました」と大城氏は話します。

“不審メールの調査のために長時間を費やすことがなくなり、自分たちの本来の仕事であるシステム企画や開発に専念できるようになりました”

事務統括部
システム担当
企画グループ
島村 祐介氏

“これまで以上に充実した内容のログが可視化されたことで、メールの運用管理担当者の業務負担も大幅に軽減されています”

事務統括部
システム担当
情報系開発グループ
大城 裕紀氏

左から島村氏、山城氏、高宮城氏、大城氏

ガードをすり抜けてくる脅威も想定した多層防御に注力していく

ただしセキュリティー対策には、もうこれで安心という終わりはありません。
「ここまでは主に、標的型攻撃メールなどの脅威が入ってくる前に行外で歯止めをかけるという基本方針に沿った対策に注力してきましたが、それでもガードをすり抜けてくる可能性は十分にありえます。また、添付ファイルをうっかり開いてしまうミスも避けられないだけに、さらなる対策が必須です」と島村氏。
これを受けて山城氏は、「今後はそうしたリスクもしっかり考慮し、内部におけるシステムおよび人的な体制も固めていく、いわゆる“多層防御”の考え方に基づいたセキュリティー対策をさらに強化していく考えです」と話します。
具体的にはセキュリティー・インシデントをいち早く察知し、被害の拡大を最小限に抑えられるように、ログ収集の強化およびその検知・分析能力の向上を図っていく計画です。また、行内のさまざまなシステムに潜在しているセキュリティーの脆弱性を顕在化し、早期に解消するため、「IBMインフラ・セキュリティー診断サービス」や「IBM Webアプリケーション・セキュリティー診断サービス」といったセキュリティー・サービスの導入も検討しています。
「IBMには引き続き、セキュリティーの専門家としての知見やノウハウ、グローバルの最新情報などを共有していただければと思います」と、山城氏はIBMに期待を寄せています。
沖縄海邦銀行はIBMとのパートナーシップをさらに深めながら、ますます悪質化・巧妙化していくセキュリティーの脅威に立ち向かっていく意向です。

日本アイ・ビー・エム株式会社
〒103-8510　東京都中央区日本橋箱崎町19番21号