Case Study

digicert®

横浜銀行、Eメールの受信ボックスにブランドマークを表示する認証マーク証明書（VMC）を導入

横浜銀行
Bank of Yokohama

概要

企業名: 株式会社横浜銀行
https://www.boy.co.jp

業種: 銀行
本社: 横浜市

主なビジネス要件:

- Eメールのセキュリティ強化
- 顧客保護
- 顧客との関係強化

ソリューション:

- DIGICERT® 認証マーク証明書（VMC）

主な特徴:

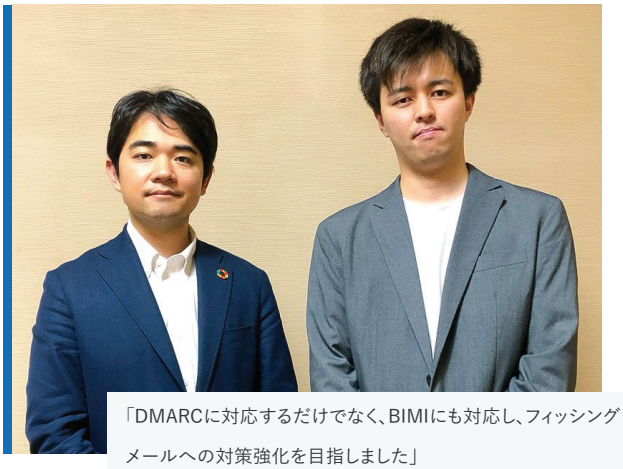
- 顧客の受信トレイに認証済みのロゴを表示し、メールが本物であることを視覚的に識別可能に
- 厳格なEメール認証規格の利用により、セキュリティ、可視性、配信性の向上
- 最も利用され、競争力のあるコミュニケーションツールであるEメールに、組織のブランドを表示、開封率の向上

要件

増加を続けるフィッシングメールから消費者を守る

日本最大の地方銀行であり、株式会社コンコルディア・フィナンシャルグループのリーダーである株式会社横浜銀行は、フィッシングメールの増加に直面しており、詐欺行為について顧客に注意を喚起している。実際、日本語の間違いが目立たなくなるなどフィッシングの脅威は生成AIツールの普及によってますます巧妙化している。また、フィッシング・ツールがサービスとして提供されるようになっており、マルウェア配布や詐欺サイトへ誘導するために利用できるようになりつつある。

金融機関は、そのビジネスの性質上、このような攻撃の最初の標的となりがちだ。フィッシング対策協議会の定期報告でも、犯罪者は金融資産を真っ先に標的にし、金融ブランドが狙われていることが指摘されている。同行は、EメールのドメインにDMARCを導入するとともに、顧客のEメールの受信ボックスにブランドのロゴを表示するBIMIを導入することを決定した。同行は当初から、DMARCとBIMIの両方を達成することを目標とし、プロジェクト開始時から上層部の承認を得ることを明確にしていた。



「DMARCに対応するだけでなく、BIMIにも対応し、フィッシングメールへの対策強化を目指しました」

株式会社横浜銀行　ICT推進部　セキュリテイ統括室
リーダー　伏見亮大氏（CISSP）、久世拓海氏（左より右）

ソリューション

DigiCert 認証マーク証明書がEメールの受信ボックスに視覚的なロゴを表示

株式会社横浜銀行は毎日約30万通のEメールを送信しているが、その80%は個人顧客向けだ。2023年、同行は行動を起こすことを決定し、1年以内にDMARCとBIMIへの対応を完了させ、ユーザーの受信トレイにブランドのロゴを表示した。この素早い対応は、彼らの決断力と組織に対する強いリーダーシップを表している。

「DMARCに対応するだけでなく、BIMIにも対応し、フィッシングメールへの対策強化を目指しました。」とICT推進部セキュリティ統括室の伏見亮大氏は語る。　「コンコルディア・フィナンシャルグループのセキュリティはすべて当部署が担っており、グループの他の銀行でもDMARCの設定を推進していますが、横浜銀行は個人のお客様にメールを送信することが多いため、BIMIまで行うことを決定しました。」

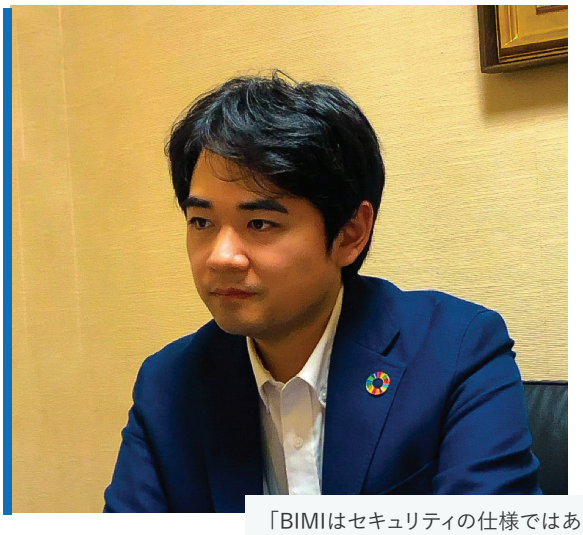
DMARCがフィッシングEメールに対する基本的なセキュリティを提供

DMARCは、Eメールの認証ポリシー、報告プロトコルである。これは、広く実装が進みつつあるSPFとDKIMプロトコルをベースに、送信者（“From:”）ドメイン名と送信組織の関係を、認証に失敗した場合の受信者の処理に関する公開ポリシー、受信者から送信者への報告などを追加し、不正メールからのドメイン保護を改善・監視するものである。つまり、偽装によって株式会社横浜銀行を装ったメールは顧客に届かなくし、それらの問題のメールは管理者に報告される仕組みだ。

このDMARC対応の準備は、まずどのようなメールがどこから送信されているかの調査を行なった。そして、次にDMARCレポートの分析だが、XMLのレポートをそのまま読むのは困難な為、同行はProofpoint社の「Email Fraud Defense」を使って分析し、各ケースの処理方法を決定した。同行は、顧客向けEメールを送信するために、十数種類のEメールシステム／サービスを利用している。DMARCで拒否されたメールのデータを検証することで、チームはメールが拒否された理由を確認できた。

なお、ドメイン所有者が送信システムを見落としたり、誤認したまま、DMARCポリシーを施行（「隔離」または「拒否」に設定）すると、「問題のない」メールもブロックしてしまうことになり、さらに時間のかかる問題を引き起こし、進捗が頓挫する可能性もある。しかし、同行では、メールを再送することが多い金融パートナー向けメールと個人顧客へのメールへの見極めを明確に行い、対策を決定していった。また、DMARCポリシーを設定する際に、一般的に提案されている数値以外の拒否率を独自の基準で判断、決定したという。

また、チームはFAQや対策プランを準備し、他のチームと緊密に連絡を取り合うことでDMARC対応をスムーズに実現したという。



「BIMIはセキュリティの仕様ではあるものの、メール開封率の向上も期待できる”楽しい”プロジェクトです」

Case Study

BIMIがメール受信者に安心を提供

ブランドロゴを表示することは、顧客にとって非常にわかりやすい目印になる。カズンドメイン（よく似たドメイン名だが、アルファベットのO（オー）と数字の0（ゼロ）を置き換えるような実体とは関係ないドメイン）のような意図的に騙そうとするドメイン名はエンドユーザーを簡単に欺くことができる。しかし、BIMIはこのようなケースを明確に見分けることができる（カズンドメインの場合、DMARCだけではSPFとDKIMを正しく設定してあればパスできる）。

BIMIによりロゴを表示するには、認証マーク証明書にエンコードされたロゴが必要で、メールクライアントが組織のBIMIレコードでDMARCの成功を確認する。発行認証局デジサートは、認証マーク証明書の発行にあたり組織のロゴを特許庁に照合し、所有者が合法的に実在していること、公的な登記情報と業務実態が一致する組織からの申請であることを確認し、ビデオ経由で申請者の身元を認証する。疑わしいドメインの運用者が認証マーク証明書を取得することは不可能である。

株式会社横浜銀行は、1年前のプロジェクト開始時にBIMIの仕様も把握し、ロゴが適切に商標登録されていることを確認していた。伏見氏は「BIMIはセキュリティの仕様ではあるものの、メール開封率の向上も期待できる”楽しい”プロジェクトです」と説明する。通常、セキュリティ・プロジェクトは実現して当然で、トラブルが発生すると対応に追われるものだが、BIMIはEメールのエンゲージメント／開封率の向上も期待される規格であるため実装に際して喜びがあったことを明かす。

「CertCentralからのVMCの購入はスムーズで、全く問題はなかった」

認証マーク証明書の購入と設定

認証マーク証明書の購入はSSL/TLSサーバ証明書など各種パブリック証明書の購入ができるウェブサイト、CertCentralから申請、決済を行うことができる。その申請に基づいてデジサートは組織の実在認証、申請の意思の確認、そして担当者の本人認証を行い証明書が発行されることになる。

「CertCentralからのVMCの購入はスムーズで、全く問題はなかった」とセキュリティ統括室の久世拓海氏は語る。同行のデザインチームと協力してロゴを準備、BIMIのSVG P/Sフォーマット用に修正を行なった。久世氏は、「利用可能なツールをいくつか試しましたが、それではうまく作成できなかったものの、デジサートのブログに詳細が説明されていた」と振り返る。

認証マーク証明書とロゴのホスティングについて、同行は他の組織がどのように行っているか調査し、CDN を利用した独自環境でのホスティングを決定した。ただ、デジサートの証明書に付随して提供されるロゴホスティングサービスとの比較は十分に行えていなかったという。デジサートホスティングの利点はホスティングコストだけでなく、証明書の更新に伴う作業ミスをなくすことになる。証明書は毎年更新が必要であり、ホスティング証明書やロゴの再アップロード、更新したファイルの指定ミスを防ぐためBIMIレコードを指定するリンクも同様に更新が必要である。更新時にそれらの何れかを忘れるのは簡単で、よく見られるミスだ。 同行は、次回更新時にデジサートホスティングの利用を検討する予定である。

同行は個人顧客に、正規のEメールがどのように見えるかをHPへの掲載やSNS等を通じて周知している。その効果が最大化されるため、より広範なメールプラットフォームでDMARCとBIMIが採用されることに期待している。