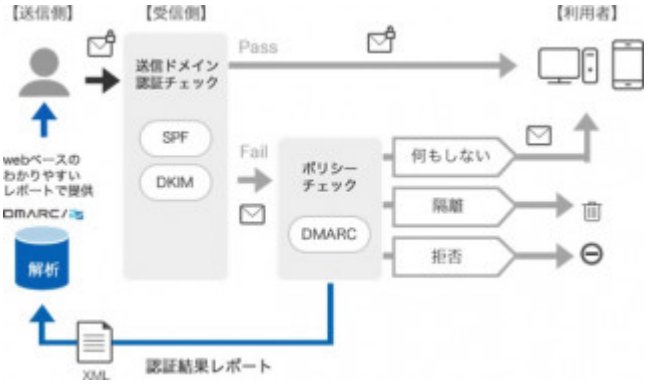
BANDAI SPIRITSが、なりすましメール撲滅の切り札「DMARC」を導入し、可視化サービス「DMARC/25 Analyze」を採用。公式ショップ「プレミアムバンダイ」を詐称する犯罪メールを迅速に把握し、ブランド価値と信頼を守る



株式会社TwoFive（本社：東京都中央区、社長 末政 延浩）は、株式会社BANDAI SPIRITS（本社：東京都港区、代表取締役社長 川口 勝）が、なりすましメール対策の世界標準技術であるDMARCを導入し、TwoFiveのDMARC可視化クラウドサービス「DMARC / 25 Analyze」を採用したことを発表します。
「DMARC / 25 Analyze」は、DMARCで提供される膨大なXML形式の認証結果情報（DMARCレポート）を解析して可視化します。
BANDAI SPIRITSは、企業のブランド価値や信用を護るために様々な対策を講じてきましたが、「DMARC / 25 Analyze」の採用は、これらの取り組みと連携して効果を最大化するものです。

◆ 採用の背景と効果

BANDAI SPIRITSは、さまざまな人気キャラクター製品を販売するバンダイ公式通販サイト「プレミアムバンダイ」を運営しており、受注・発送などの連絡やメルマガによる各種キャンペーン・プロモーションなど、数百万人規模の顧客とのコミュニケーション手段としてメールが不可欠です。
そして昨今、金融機関、ECサイト、宅配サービスなどになりすまして偽メールを大量送信して、口座情報やクレジットカード番号などを盗むフィッシングメールや、ウィルスをばらまく標的型攻撃などの事件が継続的に発生していることから、BANDAI SPIRITSは、「プレミアムバンダイ」のブランド価値と信用を護るために、スパム・ウィルスフィルター、送信ドメイン認証SPF / DKIM、JIPDECの「安心マーク」などを積極的に導入してきました。これらの取り組みに続いて今回採用した「DMARC / 25 Analyze」により、以下のようなメリットが得られます。

・
自社のドメインが不正利用されていないか確認することができ、なりすましの疑いがあるメール

送信を専用の管理画面で確認できます。
また、なりすましの疑いがあるメールが受信サーバーでどのように扱われたかを確認できます。
・
万一不正な送信に利用された場合でも、フィッシングメールの存在や内容を的確に把握できるので、自社のメールを受信する可能性のある顧客やビジネスパートナーに警告通知するなどにより、被害を抑止することが可能です。
・
各部署が展開するキャンペーンにおける顧客へのメール活用状況を的確に把握し、なりすましメール対策の設定不備等を迅速に発見することができます。
・ 導入済みのなりすまし対策ソリューションが効力を発揮しているかどうかを確認できます。
・ システムのリプレースや
クラウド環境の利用状況が変化した場合に、なりすましメール対策が維持されているかを確実に把握することができます。

◆ DAMRCの普及促進に寄与

DMARCは、なりすましメール撲滅の切り札とされる業界標準技術で、世界的に導入が加速して成果が上がっていますが、日本では導入が遅れているのが実情です。
TwoFiveが提供する「DMARC / 25
Analyze」は、DMARCの活用をより簡単にし、効果を最大化するためのサービスで、追加の設備投資の必要はなく、既存のメールサーバに導入・設定すればすぐに使用開始できます。TwoFiveは、DAMRCを理解するための勉強会、「DMARC /
25」サービス、DMARC導入のコンサルティングサービスなどの提供を通じて、DAMRCがより幅広い企業の導入に採用されるよう、今後も普及促進に寄与してまいります。

◆「DMARC / 25 Analyze」サービスの概要

メール受信側の認証結果を報告するDMARCレポートでは、多数のメール受信サーバーが生成する膨大な情報をXML形式で提供されるので、認証状況を迅速に判断するためには、集計して分かり易く可視化する必要があります。「DMARC / 25
Analyze」サービスは、メールを利用するすべての企業や団体が、特別な専門知識がなくてもDMARCレポートを適切に活用できるように支援します。
「DMARC / 25
Analyze」サービスは、ライセンスの購入や設備投資は不要で、簡単な設定だけですぐに使用開始できます。

◇なりすまし対策結果の解析

DMARCの認証情報（DMARCレポート）を集計して以下に分類します。
・なりすまし疑い：第三者がなりすまして送信した可能性の高いメール
・転送メール：認証に失敗しているが、転送された正規のメールである可能性が高いメール
・認証失敗：送信者は正規のユーザーの可能性が高いが、何らかの技術的な問題で認証に失敗しているメール
（ドメイン管理者が把握していないネットワークからの送信など）
・正規のメール：DMARCの認証に成功しているメール

◇送信ホストの解析

メールを送信したホストの情報をGUIでドリルダウンして表示します。
・ホスト名：送信元IPアドレスの逆引きホスト名を取得
・RBLチェック：RBLチェックを実施
・メール送信数：ホストから送られたメールの総件数を表示

◇処理結果の解析

送信したメールが「受信」「隔離」「拒否」のいずれの処理がされたかを把握することができます。
・受信（none）：宛先でそのまま受信した場合
・隔離（quarantine）：ポリシーに従い、なりすましと判定されたメールがスパムメールとして隔離された場合
・拒否（reject）：ポリシーに従い、なりすましと判定されたメールが拒否されて届いていない場合

◇DKIMセレクターの管理

メールドメインで利用している DKIM 鍵（セレクター）の流通状況を分析することができます。

◇共通ホワイトリスト

独自に収集した転送サーバーリスト（共通ホワイトリスト）を活用して、DMARCの認証に失敗したメールの中で正規のメールである可能性が高いメールをラベリングできます。

◆ SFP / DKIMとDMARCについて

攻撃者がメールの送信者情報を詐称して送信するなりすましメールを、受信するエンドユーザーが不正メールと判断することが難しいことから、送信者の身元を判別するためにメールドメインを認証する送信ドメイン認証技術への取り組みが10年以上前に始まりました。現在、IPアドレスに基づくSPF （Sender Policy Framework）と電子署名に基づくDKIM（Domain Keys Identified Mail）の2つの方法が主流となっており、普及率は高まりつつあります。
しかしながら、SPF / DKIMでは、認証に失敗した場合に、なりすましメールなのか、何らかの技術的な問題が発生しているだけなのか判断することが難しく、受信するべきメールを受信できなくなる可能性を懸念して、認証に失敗した（なりすましの可能性のある）メールでも、多くの場合は受信拒否、破棄しないのが現状です。また、正しいメールであるにもかかわらず認証に失敗してしまった場合、送信者側がその原因となる問題を発見する方法が標準で備わっていません。
そこで、SPFとDKIMの認証結果の情報を利用してなりすましメールの脅威撲滅を目指す仕組みとして登場したのがDMARC（Domain-based Message Authentication, Reporting & Conformance）です。DMARCは、SPF / DKIMの認証に失敗したメールを受信側がどう扱うべきか（動作を指定しない /none、隔離する / quarantine、拒否する / reject）のポリシーを、送信側（ドメイン管理側）で設定できるので、認証に失敗したメールを不正メールと断定して適切に破棄できます。また、ドメイン認証設定の正当性を確認し、配信したメールの状況を把握できるよう、受信側の認証結果をDMARCレポートとして送信者が受け取るこ

とができます。

■株式会社TwoFiveについて

http://www.twofive25.com/
株式会社TwoFiveは、大手ISP、ASP、携帯事業者の電子メールシステムインフラで長年経験をつんだメールシステムの技術者集団により2014年に設立されました。日本の電子メール環境を向上させることを使命としてベンダーニュートラルな立場で最適な技術とサービスを組み合わせ、メールシステムの設計・構築、電子セキュリティなどについてコンサルティング、ならびに各種レピュテーションデータを提供しています。

Generated by ぷれりりプレスリリース
https://www.prerele.com