



DMARC/25 Analyze 導入事例

ファンへのなりすましメールは許さない！

「プレミアムバンダイ」が導入する、なりすましメール対策「DMARC / 25 Analyze」とは？

取り扱う製品は「機動戦士ガンダム」「美少女戦士セーラームーン」など……

子供から大人までの幅広いに楽しまれている「ガンプラ」と呼ばれる「ガンダムシリーズ」のプラモデルになじみの深い人も多いだろう。

こうしたガンプラや超合金シリーズなどは現在、株式会社 BANDAI SPIRITS (バンダイスピリッツ) から発売されている。2018年に株式会社バンダイからハイターゲット向け事業を引き継いで設立された、バンダイナムコグループの企業だ。

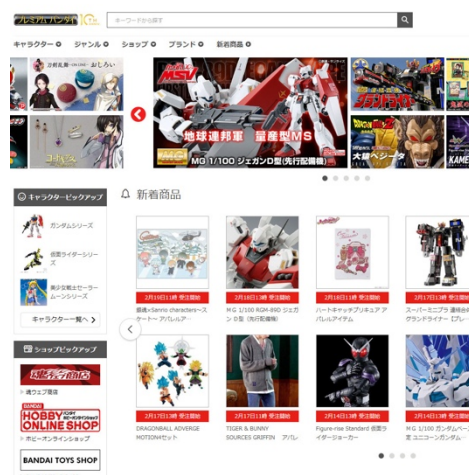
BANDAI SPIRITS では、バンダイ公式 EC サイト「プレミアムバンダイ」も運営している。2009年に、当初は子供向けとしてオープンし、現在では限定品の販売などに力を入れ、「子供から大人まで24時間楽しめる」をモットーとしている。

そしてプレミアムバンダイでは、発信元をなりすまし「なりすましメール対策」として、株式会社 TwoFive の「DMARC / 25 Analyze」を導入した。結果的に、ブランド価値と信用を守りながら、「機動戦士ガンダム」「美少女戦士セーラームーン」「仮面ライダー」「ワンピース」などの商品を扱うプレミアムバンダイを安心して利用してもらえる仕組みを構築できたという。

ちなみに、導入された DMARC / 25 Analyze は、なりすましメール対策技術「DMARC」[*1]のレポートを可視化し解析するクラウドサービスだ。

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・可視化することで、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なる。また、DMARC の認証結果をメールで通知する機能を備えるほか、TwoFive が所有する脅威データベースに基づき、本物のドメインを人間が誤認しやすく模倣した「類似ドメイン詐称」を検知する。

プレミアムバンダイで DMARC / 25 Analyze を導入した理由や、その効果について、BANDAI SPIRITS のネット戦略室 EC プラットフォームチームの大橋功氏 (アシスタントマネージャー) と武井一将氏 (チーフ) に話を聞いた。



株式会社 BANDAI SPIRITS が運営するバンダイ公式 EC サイト「プレミアムバンダイ」

[*1]……「DMARC」は、メールを送信するドメインの DNS に設定を記述しておくことで、受信側で SPF や DKIM といった送信ドメイン認証に失敗した (なりすましが疑われる) メールについて、そのドメイン側にレポートを送る仕組みである。

米国では政府機関が送信するメールに DMARC の設定が義務付けられている。国内においては、2017年7月に総務省が DMARC の導入留意点を定めており、2020年3月からはヤフーでも採用されることが決まっている。

「本当にプレミアムバンダイからのメールですか？」——なりすましや各種メール送信で見えなかった課題

——DMARC / 25 Analyze の導入に至った、背景や課題について教えてください。

[大橋氏] 昨今、世の中にセキュリティインシデントが増えています。特に EC サイトの立場でいうと、なりすましメールの危険性を感じていました。

我々は「機動戦士ガンダム」「美少女戦士セーラームーン」「仮面ライダー」「ワンピース」などの強い IP の商品ブランドを扱っており、これらを支持いただいているお客さまによって、支えられているのが「プレミアムバンダイ」です。万一、これらをかたるメールなどが現れ、お客さまに損害を与えてしまうのは大きな問題です。



BANDAI SPIRITS ネット戦略室 EC プラットフォームチームの
大橋功氏 (アシスタントマネージャー)

ですから、「大きな問題が起きる前に、しっかりした対策ができないか？」ということで検討しました。

[武井氏] なりすましを防ぐというのに加えて、「仮になりすましがあっても積極的に検知できない」というのも問題でした。

たまにお客さまから、「こういうメールが来たのですが、本当に御社のメールですか？」と問い合わせをいただくことがあります。その際、いままででは注文履歴やメルマガ (メールマガジン) の送信時間などを照合して、本当に送ったかどうかを確認していたため、時間や工数がかかっていました。

このように、申告ベースで時間をかけてしか見えなかったものを、数値ベースで見られるようにしたいという気持ちがありました。入れて安心するだけでなく、導入後の効果や判定結果などを集計するところまで含めて検討しました。

——実際になりすましの被害などに遭っていたのでしょうか。

[大橋氏] 一番大きい課題は、メール送信についてわれわれが見えていなかったことだと思っています。お客さまにちゃんと届いているのか、なりすましされていないかということが、お客さまからの問い合わせがあって初めて見える状態でした。

また、さまざまなセキュリティ対策製品を導入していましたが、なりすましメールの被害が拡大する中で、なりすまし対策をどうするかが見えていませんでした。

——世の EC サイト全般で、なりすましメールが問題になっているのでしょうか。

[武井氏] 感覚的には、問題になっていると思います。自分がユーザーとして EC サイトを使っていて「このようななりすましメールが出回っているので、クリックしないでください」という連絡をもらうことがあります。ひとごとではないと思っています。

——プレミアムバンダイで送信するメールはどのぐらいの規模でしょうか。

[大橋氏] メルマガが月に 2000 万通です。そのほか注文などの自動配信メールが、月に 1 億弱、数千万通ほどあります。そのほか認証確認のメールなどもあります。

「人力で確認」が「すぐに確認」にメールの送信状況や設定の不備も素早く把握

——DMARCはまだ知名度が高くありませんが、どのようなところからDMARCとDMARC / 25 Analyzeの導入に至ったのでしょうか。

[大橋氏]最初はSPFやDKIMなどを導入した中で、さらにDMARCという技術を知り、SlerなどからDMARC / 25 Analyzeの情報をもらって導入しました。

[武井氏]DMARC / 25 AnalyzeはDMARCレポートの解析では有名でしたし、トライアル導入してみて、当社にフィットしていると判断して導入しました。

トライアルを2018年の夏ごろに開始し、正式に導入したのが2019年1月です。本番環境に入れて、3カ月ぐらい検証しました。

[大橋氏]その際のポリシーについては、なによりメールの到達率を下げないことを最重視して、TwoFiveやSlerと相談の上で設定しました。

——トライアルや本番導入での印象は。

[武井氏]管理画面がグラフィカルでわかりやすいのが好印象でした。そのほか、さまざまな機能についてTwoFiveから教えてもらいました。

まず現れた効果として、プレミアムバンダイのドメインを利用して外部ASPサービスからメールを送信していたのですが、設定に不備があったことがわかりましたので、早速そこを改善しました。

なりすましの面では、まず導入当初に正しいメールの率が99.21%でした。ASPサービスの不備を是正して99.47%になりました。ほとんどなりすましはありませんが、その数字を可視化できたことが最大の成果です。



BANDAI SPIRITS ネット戦略室 ECプラットフォームチームの武井一将氏(チーフ)

[武井氏]具体的ななりすまし被害というのはなかったのですが、当社のオペレーションミスによって、お客さまから「なりすましでしょうか？」と質問を受け、DMARC / 25 Analyzeで確認したことが1件ありました。

これまでは人力でログから確認したり、お客さまにヒアリングしたりする必要があったため、工数と時間がかかっていたのが、DMARC / 25 Analyzeによってすぐに確認できるようになりました。

——導入について会社の理解はすんなり得られましたか。

[大橋氏]はい。個人情報やセキュリティ、消費者保護などの問題について、経営層もよく耳にして意識していたので、問題はありませんでした。

——担当者の人数は。

[武井氏]システム担当が数名で、それにプラスしてパートナーのSlerがいます。

[大橋氏]このメンバーで、グローバルにわたるECサイトである「プレミアムバンダイ」の運営や、ID基盤、コーポレートサイトの開発など、ネットにかかわることを担当しています。そのため、パートナーのSlerが大きな役割を果たしています。

DMARC /25 Analyze についても、パートナーがレポート画面を見て、われわれはそこからレポートを受けて行動しています。パートナーとは隔週でミーティングしているほか、TwoFive もまじえて四半期に 1 回ミーティングしています。



「類似ドメインの取得」もシステムで検知、海外展開への基盤としても

——今後、なりすましメールなどの対策はどうしていくでしょうか。

[武井氏]プレミアムバンダイではいま、海外に力を入れていますので、これから、なりすましメールなども増えることが考えられます。すでに、名前の類似したドメインが取得されている動きは観測しています。そうした類似ドメインの取得も、DMARC /25 Analyze の機能とパートナーとの連携で検知していきます。

[大橋氏]攻撃者も日々進化しています。それを防ぐ対策をしていくために、常に最新のセキュリティ対策を続けていきます。

[武井氏]例えばメールについては、送信ドメイン認証に合格したメールに送信者のロゴを表示する BIMi (Brand Indicators for Message Identification) といった新しい規格も生まれてきています。そうした安全安心のための新技術についても関心をもちつつ、お客さまを混乱させないよう普及状況を見ながら検討していきたいと思えます。

——最後にメッセージを。

[大橋氏]プレミアムバンダイは予算をかけていろいろ対策をしています。個人情報流失など起こさないように、今後も取り組んでいきます。

引用元記事: <https://internet.watch.impress.co.jp/docs/topic/special/1235886.html>