Press Release

2017 年 6 月 21 日
株式会社 TwoFive

企業になりすました不正メール被害撲滅のために
なりすまし対策に有効な DMARC レポートを集計・可視化する
クラウドサービスを提供開始

顧客保護の立場でセキュリティを強化し、ブランド価値と信頼性を守る
なりすましメールの被害が起きる前に適切な対応が可能に

株式会社 TwoFive（本社：東京都千代田区、社長 末政 延浩）は、企業や団体になりすました不正メールへの対策を支援する新サービス「DMARC / 25」を発表し、その第一弾として、メール送信状況を解析するクラウドサービス「DMARC / 25 Analyze」を提供開始します。
「DMARC / 25 Analyze」は、なりすましメール対策の新しい仕組みとして注目される DMARC（ディーマーク）で提供される膨大な XML 形式の認証結果情報（DMARC レポート）を集計・可視化して解析し、Web ベースの分かり易いレポートを提供します。なりすましの疑いのあるメール送信を検知した場合、レポート上に警告を表示し、管理者に通知します。
このサービスを利用することにより、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迅速に検知できます。 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。

◆送信ドメイン認証の現状と DMARC の概要
攻撃者がメールの送信者情報を詐称して送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 KeysIdentified 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、依然として送信者のメールアドレスを詐称し、金融機関、コマースサイト、宅配サービスなどの企業やブランドを装った業務メールに見せかけて、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抜きとる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おり、さらなる対策が求められています。

現在の送信ドメイン認証技術（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。

◆「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 24 時間ごとに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。

◇なりすまし検知

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っ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
（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）
・通常のメール：DMARC の認証に成功している

◇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
・ホストの地理情報：ホストの所在地を地図上に表示
・Whois 情報：ドメインの所有者情報を表示

◇なりすまし検知アクション

なりすましを検知した場合、GUI 上で警告します。また、今後、サービス利用者（メール管理者など）のメールアドレスに通知する他、以下の対応を予定しています。（2017 年 12 月以降順次対応を予定）

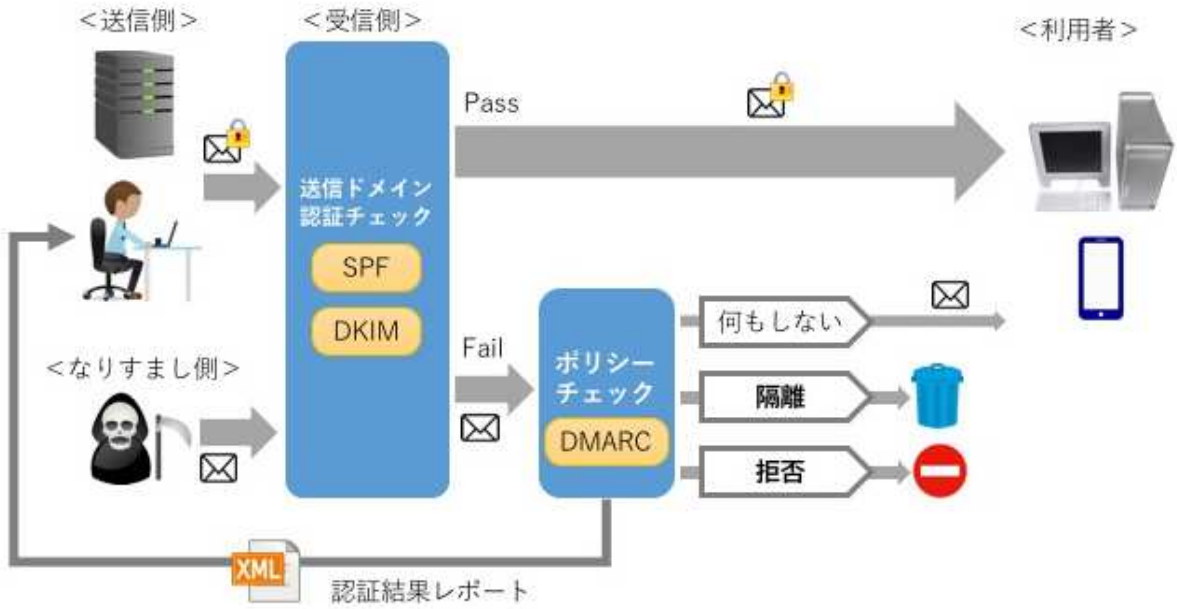
・ブラックリスト連携：各種公開 RBL 運用者に対して、継続的になりすましメールを送信しているホストの情報を共有します。

・セキュリティベンダー連携：各種迷惑メールフィルターの提供者に対して、継続的になりすましメールを送信しているホストの情報を共有します。
・Take down：継続的になりすましメールを送信しているホストへメールや電話を実施してなりすましメールの送信停止を要求します。
・セキュリティに関する公的機関との連携：各種迷惑メールフィルターの提供者に対して、継続的になりすましメールを送信しているホスト情報を共有します。

◆「DMARC / 25」のメニュー構成

「DMARC / 25」は、メール送信側向けとして「DMARC / 25 Analyze」の他に、なりすましをさせないために送信ドメイン認証を利用可能にする「DMARC / 25 Sender」、および、メール受信側向けになりすましメールの侵入防止のためにDMARC認証のフィルタリングを行う「DMARC / 25 Defender」があります。いずれも、サービスプロバイダーとの連携などにより、今後順次提供していきます。

◆送信ドメイン認証とDMARCの仕組み



◆「DMARC / 25 Analyze」を先行導入しているユーザー様からのコメント

◇株式会社ココナラ 取締役 CTO 恵比澤 賢 様

「coconala（ココナラ）は、個人が自分の知識やスキルを売り買いできるオンラインマーケットです。お客様が快適に安心、安全にお取引を楽しめるように、決済システム、個人情報管理など、独自に様々な取り組みを行っていますが、メールは、お客様とのコミュニケーション手段の主体であることから、なりすましメールへの対応は非常に重要な課題であると認識しており、今回、DMARC の送信ドメイン技術とDMARC/25 の利用を開始しました。DMARC/25 は、すべてのメール送信状況を分かり易く把握できるので、弊社になりすましたメール送信が発生した場合にも、即座に適切に対応できると期待しています。今後も、メールセキュリティで豊富な経験と実績のある TwoFive のサービスを活用して、なりすまし対策に積極的に取り組みたいと考えています。」

◇株式会社パイプドビッツ

「パイプドビッツでは、企業や官公庁のお客様が安心してメールを送信し、受信者にメールが届くように、DMARC をはじめとした送信ドメイン認証技術を活用しています。金融機関や宅配業者などのフィッシングメール被害が増加している昨今において、TwoFive が提供する DMARC/25 が被害抑制の一翼を担うと考えています。」

◇チーターデジタル株式会社

「チーターデジタル株式会社（※）としてもお客さまに安全なコミュニケーションツールを提供するために、DMARC の普及は重要であると考え、取り組みをすすめている。DMARC/25 のようなツールが国内で提供されていることはとても有意義である。また、ツールだけでなく導入において手厚く柔軟なサポートも DMARC の普及に寄与すると考えています。」

※2017 年 6 月 8 日付で社名がエクスペリアンジャパン株式会社より変更となりました。

[補足資料]

◇SPF （SenderPolicyFramework）

送信設備の IP アドレスを公開し、受信設備で送信元 IP を検証する方法。「送信元ドメイン名」と「送信元メールサーバ」の整合性を確認し、正当なメールサーバからメールが送信されているか否かを確認する方式。2016 年 6 月時点での SPF 普及率は 93.14%（※1）と高い普及率を保っている。

※1 出典：総務省「送信ドメイン認証結果の集計(SPF) (2016 年 6 月時点)」

◇DKIM（DomainKeysIdentifiedMail）

電子署名方式の送信ドメイン認証方式。送信側で電子メールに電子署名を付加し、受信側でその電子署名を照合して送信者のドメインの認証を行う。メッセージのヘッダや本文を元に電子署名を作成するため、中継 MTA などで電子署名または電子署名の元になった電子メールのデータが変更されなければ、たとえメールが転送されたとしても転送先において認証が可能になる。2016 年 6 月時点での DKIM の普及率は、45.79%（※2）と徐々に普及率が増加しています。

※2 出典：総務省「送信ドメイン認証結果の集計(DKIM)（2016 年 6 月時点）」

◇DMARC（ディマーク：Domain-based Message Authentication、Reporting & Conformance）
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のポリシーを、ドメイン管理者側が宣言するための仕組み。既に米国では多くの ISP が DMARC 対応を進めるなど、普及率が高まっており、Twitter 社は日次 1 億 1000 万通のなりすましメールが 1,000 通に激減、PayPal 社ではクリスマスシーズンに 2,500 万通もの迷惑メールを遮断するなど、非常に高い効果をあげている。日本国内では、迷惑メール対策推進協議会が中心となり DMARC 普及策に取り組んでいる。

■株式会社 TwoFive 社について

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。

■報道関係者お問い合わせ

株式会社 TwoFive
担当：末政（すえまさ）TEL 090-8041-3771 / 谷口 TEL 080-2021-8067
info@twofive25.com

※読者お問い合せ先は以下をご掲載ください。
info@twofive25.com TEL：03-5704-9948

※本プレスリリースの画像を以下にアップしています。
http://www.twofive25.com/news/20170621_DMARC25.html