Press Release

2020 年 2 月 12 日
株式会社 TwoFive

TwoFive、被害が起きる前に、迅速かつ適切な対応を可能にする なりすましメール対策支援クラウドサービスを拡充

DMARC をすり抜ける類似ドメイン詐称検知サービスを追加
認証失敗を日次アラート通知し管理者の利便性を向上

株式会社 TwoFive（本社：東京都中央区、社長 末政 延浩）は、なりすましメール対策支援クラウドサービス「DMARC / 25 Analyze」の機能強化とサービス拡充を発表しました。
「DMARC / 25 Analyze」は、なりすましメール対策に有効な送信ドメイン認証技術「DMARC（ディーマーク）」の認証結果レポートを、集計・可視化して解析するサービスで、被害が起きる前に迅速かつ適切な対応を可能にします。今回、DMARC 認証結果をアラートメールで日次送信する機能などを追加し、セキュリティ担当者やメール管理者の利便性を向上しました。また、DMARC などの送信ドメイン認証だけでは見抜けないなりすましメールの手口である「類似ドメイン詐称（本物に似せたドメイン）」を検知するサービスを追加し、検知結果を日次でメールアラート送信します。これにより、DMARC だけでは検知できないなりすましメールから派生する脅威を軽減することが可能となります。

送信元を詐称したフィッシングメール（なりすましメール）は依然として猛威をふるっており、最近では、フィッシングメールによるコンピュータウィルス「Emotet（エモテット）」の感染被害も多数報じられています。なりすましメールは、このようなウィルス感染の入り口として利用されたり、標的型攻撃やフィッシングサイトへの誘導に利用されますが、なりすまされた企業や組織は、ブランド価値や信用に傷がつき、お客様を護る対応に追われるなど、甚大な損害を被ります。
DMARC は、なりすましメール対策の切り札となる新しい仕組みとして注目され、総務省はじめ、セキュリティに関わる企業や団体がその普及に努めています。DMARC の導入は、SPF や DKIM と同様に DNS レコードを 1 行追加するだけなので難しくはありませんが、なりすまし対策として効果的に運用するのは容易ではありません。

「DMARC / 25 Analyze」は、DMARC で提供される膨大な XML 形式のフィードバック情報（DMARC レポート）を集計・可視化して解析し、なりすまし対策に効果的に活用できるよう支援します。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流通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。
TwoFive は、2017 年から同サービスを提供開始し、現在、月間約 20 億通以上の認証結果を解析していますが、なりすましメール被害の実態やその対策の必要性に対する認識が高まり、DMARC を導入する企業が増加

（※1）していることから、既存ユーザーからの意見や要望も反映して、セキュリティ担当者やメール管理者の負荷を抑えながら、より迅速かつ確実になりすましメールを把握できるよう機能を強化しました。具体的には、なりすまし対策が適切かどうか、管理者は定期的に「DMARC / 25 Analyze」の管理画面にアクセスして確認していましたが、あらかじめ閾値を設定しておくことで DMARC 認証結果を日次でメールアラートを送ります。これにより、管理画面にアクセスすることなく異常を把握できます。

サイバー犯罪者が本物のドメインを詐称する一つの手口として類似ドメインを使う方法があります。これは、人間が視認した時に誤解しやすい攻撃用のメールドメイン（模倣ドメイン）を新たに作成・悪用し、そのメールドメインに DMARC を設定して認証を成功させる方法で、国内でも多くの被害実例があります（※2）。今回、「DMARC / 25 Analyze」のサービスに、類似ドメイン詐称日次アラートを追加し、TwoFive が所有するスレットインテリジェンス（脅威データベース）を使って、本物のドメイン（ブランド）に似せたドメイン名を悪用したフィッシングメールの情報を提供します。
また、直近 1 ヶ月分のデータを TwoFive のセキュリティアナリストが分析した診断レポートを提供し、現在のメールシステムのなりすましメール対策状況やポリシー変更に向けたチェックポイントを定期的にコンサルティングします。

TwoFive は、なりすましの理解を深めセキュリティ対策を促進するためのポータルサイト（※3）での情報発信、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、DMARC の普及促進、なりすましメール撲滅に寄与してまいります。

※1　BANDAI SPIRITS 様の導入事例を以下でご覧いただけます。
https://www.twofive25.com/news/20190115_DMARC25.html
※2　類似ドメイン詐称について以下をご参照ください。
https://www.naritai.jp/introduction_domain.html
※3　なりすまし対策ポータルサイト「ナリタイ」
https://www.naritai.jp/index.html

◆「DMARC / 25 Analyze」拡充ポイント

(1) 類似ドメイン詐称日次アラート
本物のドメイン（ブランド）に似せたドメイン名を悪用したフィッシングメールが流通していた場合に、その情報をメールで通知して、管理者にお知らせします。これにより、管理者は顧客や取引先に対してフィッシングメールの注意喚起を迅速化できます。日次アラートでは、詐称タイプ（サブドメイン詐称、スクワッティングドメイン詐称、フレンドリーネーム詐称、パークドメイン詐称など）別の件数と、実際の検体メールの一部ヘッダー情報を記載します。

●類似ドメイン詐称アラートの例

詐称タイプ	具体例　（example.com の場合）
存在しないサブドメイン	spam123.example.com
部分一致ドメイン	example-spam123.com
TLD 違いドメイン	example.xyz
Friendly Name 詐称	表示名に本物のドメインが記載されている
パークドメイン詐称	パークドメイン設定されたドメイン

(2) 認証失敗日次アラート
管理ドメインそれぞれに対して、DMARC 認証結果が悪化した場合にメールで通知して、管理者にお知らせし

ます。これにより、管理者は DMARC レポートの分析結果を確認するために管理画面にアクセスする手間を軽減します。日次アラートでは、設定した閾値と計測値を記載します。

●認証失敗日次アラート画面

●認証失敗アラート設定画面

(3) 送信グループ分析

従来は、送信元 IP アドレスごとの認証結果を集計していましたが、ホスト名を組織ドメインごとにグループ分けして、認証結果を見やすくしました。これにより、利用している送信代行サービスや自社のメールサーバーを分類して、DKIM や SPF の改善が必要な箇所が見つけやすくなります。

●送信グループ分析画面

(4) 定期的な診断レポートとコンサルティング

直近 1 ヶ月分のデータを TwoFive のアナリストが分析し、現在のメールシステムのなりすましメール対策状況やポリシー変更に向けたチェックポイントをコンサルティングします。

[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、ソフトウェア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。

「DMARC / 25 Analyze」には「Standard」、「Professional」の 2 つのサービス区分があり、今回拡充した上記 (1)～(3)の新機能/新サービスは、Professional で提供します。サービス区分の詳細は以下をご参照ください。

https://www.twofive25.com/service/dmarc25.html

■株式会社 TwoFive 社について

https://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：加瀬 080-9805-0025
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。

https://www.twofive25.com/news/20200212_dmarc25.html

◆添付資料◆

[送信ドメイン認証について]

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。

◆送信ドメイン認証と DMARC の仕組み