日経225のDMARC導入率は62.2%で、1年間で12.4%増加 / なりすましメール対策実態調査の最新結果を発表

2023年5月18日

TwoFive、なりすましメール対策実態調査の最新結果を発表

・日経225のDMARC導入率は62.2%で、1年間で12.4%増加
・大学のDMARC導入率は、全体の9.4%のみ
・BIMI対応は3,724ドメイン / 252ドメインで設定不備を確認

メッセージングセキュリティのリーディングカンパニーである株式会社TwoFive（本社：東京都中央区、代表取締役 末政 延浩）は、なりすましメール対策実態調査の最新結果を発表しました。
今回は、送信ドメイン認証技術DMARC導入実態について、日経225企業が管理・運用する5,261ドメインに加えて、教育機関として大学（国立、公立、私立、短大合わせて1,114校が管理・運用する4,060ドメイン）を対象として調査しました。
また、なりすましメール対策の最新技術規格であるBIMIに対応したメールドメインの推移やその傾向について調査しました。

日経225企業は、2023年5月
時点で、140社（62.2%）が少なくとも1つのドメインでDMARCを導入し、昨年同月と比較すると1年間で12.4%増加しており、なりすましメール対策への意識が高まっています。一方、大学は、全体ではDMARC導入率が9.4%にとどまっています。
DMARCに対応したドメインでは、なりすましメールとして処理される確率が高くなることから、攻撃者はDMARC未対応のドメインを選ぶことになり、DMARC導入はなりすまされるリスクを軽減する抑止力にもなります。大学などの教育機関も、今後のなりすましメール対策への理解の向上と対応が期待されます。

BIMI（Brand Indicators for Message Identification）は、bimigroup.orgによって策定された新しい技術規格であり、なりすましメール対策であるDMARCを使って、メールの送信者情報の一部として認証済みのロゴを表示することで、受信者は正規のメールを見分けやすくなります。
2023年4月
時点では、3,724ドメインがいち早くDNS上にBIMIレコードを設定しており、BIMIへの注目が高まりつつあります。しかしながら、ロゴの認証マーク証明書（VMC：Verified Mark Certificates）を設定している865ドメインの29.1%にあたる252ドメインに、何らかの設定不備

が見られることも確認されています。

TwoFiveは、DMARCおよびBIMIの導入技術支援を提供していますが、今後も、DMARCおよびBIMI導入を促進する啓発活動や効果的に運用するためのサポートに尽力して参ります。

調査結果のサマリーは以下の通りです。

※調査結果のグラフを以下でご覧いただけます。
https://www.twofive25.com/news/20230518_dmarc_report.html
・日経225企業DMARC導入状況
・日経225企業 DMARC導入ドメインのポリシー設定状況
・教育機関のDMARC導入状況
・教育機関のDMARCポリシー設定状況
・BIMI対応メールドメイン状況
・ BIMI設定不備の内訳

◆ 日経225企業のDMARC導入実態について

日経225企業は、全225社の内140社（62.2%）が少なくとも一つのドメインでDMARCを導入しており、調査を開始した2022年2月
から見ると27.1%、昨年同月と比較すると1年間で12.4%増加しています。
この140社が運用するDMARC導入済み971ドメインの内、強制力のあるポリシー（quarantine、reject）に設定しているのは、現時点で全体の31.7%であり、none設定によるモニタリング段階が大半で、１年前（33.5%）から全体比率は増えていません。

DMARCレポートは、社員による想定しないメール送信、意図しない経路でのメール送信などが発見でき、メールの使われ方を可視化できます。従って、none設定であっても、可視化する意識が高まっていることは歓迎するべき状況ではありますが、今後、強制力のあるポリシーに変更して、なりすましメールを制御する段階にステップアップしていくことが期待されます。

◆ 大学のDMARC導入実態について

調査対象は、1,114大学 / 4,060ドメインで、内訳は、国立大学：86校/
1,691ドメイン、公立大学：99校/ 321ドメイン、私立大学：625校/
1,393ドメイン、短期大学：304校/ 655ドメインです。
結果は、全体では、DMARC導入率が9.4%にとどまり、日経225企業の結果と比較すると非常に低く、なりすましメール対策が進んでいないと考えられます。
また、DMARC導入ドメインのうち、86.6%はポリシーがnoneであり、日経225企業と同様に、強制力のあるポリシー（quarantine、reject）への切り替えも今後の課題です。

◆ BIMIに対応メールドメインの調査

BIMIは、DMARCやVMCを利用して、正規の送信者が所有するブランドロゴを、メールアプリケーションの受信箱に表示する機能で、送信者は受信者に対してメールの真正性を証明でき、受信者は

安心してメールを開封できるようになると期待されます。

Google、Appleなどが提供する主要メールサービスはBIMI対応を開始しており、今回の調査では2023年4月
現在、3,724ドメインがいち早くDNS上にBIMIレコードを設定していましたが、ロゴの所有証明のために必要となるVMCを設定しているのは865ドメイン（設定率：23.2%）でした。BIMIに対応している主要メールサービスはVMCを必須条件としていることから、今後この設定率は高まるものと期待されます。
一方、VMCを設定している865ドメイン中252ドメイン（29.1%）には、何らかの設定不備が確認されました。設定不備で最も多いのがVMCに指定されたドメイン名とBIMIレコードのドメイン名が一致しないケース（122ドメイン）。それ以外では、VMCの有効期限が過ぎたケース（58ドメイン）と、画像情報の不一致（33ドメイン）が確認されました。

◆ 今回発表するなりすましメール対策実態調査について

◇調査時期：2023年1月 ～5月
◇調査対象：日経225企業が管理・運用する5,261ドメイン
教育機関が管理運用するドメイン（1,114大学、4,060ドメイン）
TwoFiveが利用・流通を確認したBIMI対応メールドメイン 3,724ドメイン

◇調査方法：調査対象ドメインおよびサブドメインのDNSレコードを調査
◇主な調査結果：各企業のドメインごとに以下の状況を把握しています。
・DMARCを導入しているかどうか
・DMARCのポリシー設定状況
「none（何もしないで受け取る）」「quarantine（隔離）」「reject（拒否）」
・BIMIレコード設定状況、VMCの指定状況、設定不備の分析

※TwoFiveは、DMARC導入などのなりすましメール対策実態について継続的に調査しています。
過去の調査結果を以下でご覧いただけます。
https://www.twofive25.com/news/20220519_dmarc_report.html
https://www.twofive25.com/news/20221110_dmarc_report.html

※DMARCの仕組み、TwoFiveが提供するクラウド型DMARC分析サービス「DMARC / 25 Analyze」の詳細は以下をご参照ください。
https://www.dmarc25.jp/

※BIMIの仕組み、TwoFiveが提供するBIMI 技術サービスの詳細は以下をご参照ください。
https://www.twofive25.com/service/bimi.html

■株式会社TwoFiveについて

https://www.twofive25.com/
株式会社TwoFiveは、大手ISP、ASP、携帯事業者、大手企業の大規模電子メールシステムインフラの構築・サポートで長年経験を蓄積した技術者集団により、メールシステムの構築、メールセキュリティ、スレッドインテリジェンスを事業の柱として2014年に設立。国内外の優れた製品/ソリューションに技術サービスを組み合わせて提供してきました。現在は、所属する業界団体や関連

サービスの提供ベンダーと協業し、メールシステムだけでなく、多様なメッセージング分野の新しい課題に取り組んでいます。また、海外ベンダーとの充実したネットワークを活かして、メッセージング分野に限定せず、日本のDXを支える優れた製品・ソリューションを日本市場に紹介しています。東京本社の他、ハノイにベトナム支社があり、開発、サポートを行っています。

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