HORNETSECURITY

FACT SHEET

DMARC MANAGER

DMARC、DKIM、SPFを適切かつ簡単に管理し、フィッシングやなりすましなどからドメインを保護し、企業のブランド価値を保護します

DKIM
Domain Keys Identified Mail

メールにデジタル署名することで、受信者はそのメールの送信者が誰であるか、メールが改ざんされていないことを確認可能にします。

SPF
Sender Policy Framework

ドメインを認証し、そのドメイン名でメールを送信できる唯一のドメインであることを証明します。

DMARC
Domain-based Message Authentication, Reporting and Conformance

メールボックスを常に正常に保ち、DKIMまたはSPFに適合できなかったメールをどのように扱うかを決定します。

多くの企業にとって、メール認証の管理は頭痛の種です。特に複数のドメインを管理している企業にとって、DMARC、DKIM、SPFを適切に設定し維持することは大きな課題となっています。DMARCが適切に設定されていないと、企業の送信者評価が低下し、なりすましメールによる攻撃に対して脆弱な状態に陥るリスクがあります。同時に、GoogleやYahooなどが求める厳しい要件を満たすことは、さらに複雑な問題を包含します。また、メールキャンペーンのパフォーマンスを把握できないことや、企業内で隠れたメール行為が行われていることなども、企業が直面する厄介な問題です。スパムフォルダーではなく、送信先のメールボックスに確実にメールが届くようにしたいという企業の希望は、適切なメールセキュリティなしには実現できません。

DMARC、DKIM、SPFを簡単、確実に設定し、企業のブランド価値を保護しましょう

何が影響を受けるのか？

メールによるコミュニケーション

DMARC Managerが何をするのか？

コンプライアンスへの遵守

DMARCやDKIM、SPFを適切かつ容易に設定、維持

DNSレコードの容易な管理

DNSレコードを即座に追加、変更

なりすましの防止

ドメイン経由でメール送信している送信者情報を包括的に取得

何が可能になるのか？

認証基準を遵守することでメール配信を確実にし、企業のブランド価値を保護

HORNETSECURITY

FACT SHEET

機能

ドメイン設定ツール：複数のドメインのTLS設定に加えて、DMARC、DKIM、SPFの適切な設定、管理が直感的で分かりやすいインターフェースを用いて可能にします。DMARC　Managerを使用すると、SPF/DMARCレコードの管理やDNSの変更を即座に行うことが可能です。

ステータスダッシュボード：管理対象のドメイン、認証済みおよび未認証の送信者数、認証済みおよび未認証の送信メール数、DMARCに適合したメール数と不適合となったメール数など、さまざまな統計情報を含む包括的な情報を表示します。

メール送信者分析：ドメインからメールを送信している送信者の包括的な情報を表示します。メール数、認証ステータス（DMARC適合または不適合）、送信者の分類（認証済または未認証）、配信可能性、送信者評価、脅威レベルの詳細を表示します。

BIMIによるメールのブランディング：ドメインがDMARCに適合していると、対応する受信トレイにおいてメールの横にロゴが表示されるBIMIが利用可能となり、メールキャンペーンの効率、ブランド認知度、信頼性を最大限に向上します。

SMTP-TLS暗号：SMTP-TLS暗号によって、メールを確実、安全に送信します。暗号化されず配信できなかったメールに関する詳細なレポートを表示し、メールコミュニケーションのセキュリティレベルを向上します。

不適合レポートとアラート：不適合レポートは、DMARCに不適合だったメールに関する詳細情報をリアルタイムに表示し、ドメイン名を名乗って誰がメールを送信しているのか、また、特定のメールがなぜ送信に失敗したのかを表示します。さらに、アラートを設定することで、各種イベントが発生した際には指定したメールアドレスへ通知メールが送信され、脅威へのより迅速な対応が可能になります。