HORNETSECURITY

DMARC MANAGER
なりすましメールの対策

信頼はビジネスメールコミュニケーションの基盤ですが、サイバー犯罪者はメールのなりすましによってこれを悪用します。信頼されたドメインや個人になりすまして詐欺を行うことで、BEC（ビジネスメール詐欺）攻撃につながることも少なくありません。

なりすましメールがもたらす影響：

» 詐欺メール（ニセの請求書など）による**金銭的損失**
» なりすましが引き起こす**信頼性の低下**によって顧客やパートナーからの信頼を失う
» **フィッシング攻撃のリスクが高まり**、機密データが漏えいする

DMARC：なりすましメールに対する防御策

DMARC（Domain-based Message Authentication, Reporting & Conformance）は、企業のなりすましメール対策に役立つ強力なメール認証プロトコルです。**SPF**および**DKIM**と併用することでドメインから送信されるメールが認証されたもののみであることを保証し、ブランドとコミュニケーションチャネルを保護します。

仕組み：

SPFは送信サーバーのSPFレコードをチェックし、メールが承認されたIPアドレスから送信されたことを確認します。IPアドレスがSPFレコードに記載されている場合は適合となり、記載されていない場合は不適合となります。

DKIMは、メールが送信ドメインの秘密鍵で暗号署名されているかを確認し、対応する公開鍵で検証します。一致した場合は適合となり、そうでない場合は不適合となります。

DMARCは、メールの「送信元」アドレスが、SPFとDKIMがそれぞれのチェックで検証したものと同じメールドメインと一致しているかを確認します。

送信ドメインのDMARCレコードのポリシータグ（**"p"**）は、チェック結果に基づいて受信サーバーにメールをどのように処理するか指示します。

HORNETSECURITY

DMARC、DKIM、SPFの設定と維持管理は、複数のドメインを持つ企業やドメインごとに異なる要件を持つ場合の管理に、多くの課題が生じる可能性があります。

DMARC MANAGERでDMARCの悩みを解決

DMARC MANAGAERによって

» ドメイン名でメールを送信しているすべての送信者を把握し、ドメイン所有者に制御権を取り戻すことで、ブランドの評判を強化し、保護します

» DMARC、DKIM、SPFを複数のドメインに対して適切かつ簡単に設定、維持できます

» メール配信と認証の状況を把握することで、正しいメールとなりすましの可能性を特定できます

» GoogleやYahooなどが求める認証基準に準拠し、メールが確実に配信されるようにすることで、メールによるマーケティングを強化します

» PCI DSS、NIST、GDPR、HIPPAなどの業界およびグローバル規制への準拠を強化します

Sales-Japan@hornetsecurity.com | www.hornetsecurity.com/ja/

Vade Japan株式会社, Hornetsecurity Group