SPFとDKIMのアラインメントを修正してDMARC障害を解決する

内容

問題

特定のドメインからの電子メールは、DMARC検証エラーにより、Cisco Secure Email Gateway(CES/ESA)によってブロックされます。メッセージトラッキングの分析により、これらの電子メールが作業キューに保持され、隔離または拒否されていることが示され、意図した受信者に到達できません。

環境

- Cisco Secure Email Gateway(CES/ESA)アプライアンス
- SPF、DKIM、およびDMARCポリシーが設定され、適用されている

解決方法

SPF/DKIMアライメント概要表（例）

メカニズム	線形ステータス	エンベロープ/シグニチャドメイン	開始ヘッダードメイン	ロジック
SPF	整列	sender@example.com	sender@example.com	直接一致
SPF	整列	sender@child.example.com	sender@example.com	親ドメインの

				一致
SPF	整列していません	sender@test.com	sender@example.com	ドメインの不一致
DKIM	整列	example.com	sender@example.com	直接一致
DKIM	整列	example.com	sender@child.example.com	リラックスモードの一致
DKIM	整列していません	example.com	sender@test.com	ドメインの不一致

送信者との調整（推奨）

- 送信者のドメイン管理者と協力し、ヘッダーレベルでSPFとDKIMが適切に連携するように設定することで、DMARCの障害を修復します。
- 送信者は次のことを行う必要があります。
  - SPFで検証されたMAIL FROMまたはHELO/EHLO IDで使用されているドメインが、電子メールのFromヘッダーのドメインと一致していることを確認します。
  - DKIM署名のd=タグで指定されたドメインがFromヘッダードメインと一致するDKIM署名を実装します。
  - 目的の調整モード（厳密または緩和）とレポートオプションを適用するようにDMARCポリシーが正しく設定されていることを確認します。
- このアプローチでは、認証されたドメインと可視のFromヘッダードメインの整合に重点を置くことにより、DMARC障害の根本原因に対処します。これは、長期的なEメールの配信性にとって重要です。

DMARC例外の作成（代替）

- 送信者による修復が不可能な場合は、特定の送信者アドレスに対してESAデバイス上で例外を作成し、DMARCチェックをバイパスします。

- これは一時的な回避策であり、モニタリングを伴う必要があります。

監視と検証

- 変更を実装した後、目的の受信者へのアラート電子メールの配信を監視します。
- メッセージトラッキングログを確認して、DMARC障害が解決されたことを確認します。
- 配信の問題が解決されない場合は、更新されたメッセージ追跡データの分析を続行します。

原因

電子メールの検疫または拒否の主な原因は、SPFとDKIMのアライメントの問題によるDMARC検証の失敗です。これらの障害は、SPFおよびDKIMレコードが正しくパブリッシュできても、電子メールの交換時に認証されるドメインがFromヘッダードメインと一致しないため、電子メールが検疫されることを示しています。

DMARC、SPF、およびDKIMのアライメントについて：

- SPFはMAIL FROMまたはHELO/EHLO SMTPコマンド内のドメインを認証し、DMARCに準拠するためにこのドメインがFromヘッダー内のドメインと一致している必要があります。
- DKIMは、d=タグで指定された署名ドメインを持つ暗号署名を使用します。これは、Fromヘッダードメインと一致している必要があります。
- DMARCはSPFとDKIMを基盤として構築され、認証済みドメインの少なくとも1つがFromヘッダードメインと正確に（ストリクトモード）またはサブドメインとして（緩和モード）連携することを要求します。

このドメインの関連付けが失敗すると、SPFレコードとDKIMレコード自体が正しく公開され、有効であっても、DMARCの失敗とそれに続く電子メールの拒否または検疫が発生します。

この連携の焦点により、認証済みIDと可視送信者IDが確実に一致するため、スプーフィングが防止され、電子メールの信頼性が向上します。

関連コンテンツ

- SPFアライメント情報
- DKIMアライメント情報
- Eメール認証のベストプラクティス – SPF、DKIM、およびDMARCの最適な導入方法 – シスコ
- ESAでのDKIM検証に基づく着信フィルタの設定：シスコ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。