Eメール認証のベストプラクティス – SPF、DKIM、およびDMARCを導入する最適な方法

内容

概要

このガイドでは、現在使用されている3つの主要なEメール認証テクノロジー（SPF、DKIM、およびDMARC）について説明し、実装のさまざまな側面について説明します。実際のEメールアーキテクチャに関するいくつかの状況と、Cisco Eメールセキュリティ製品セットに実装するためのガイドラインについて説明します。これは実践的なベストプラクティスガイドであるため、より複雑な資料の一部は省略されます。必要に応じて、特定の概念を簡素化または要約して、提示された内容を理解しやすくします。

製品知識の要件

このガイドは、詳細レベルのドキュメントです。この資料を読み進めるには、Cisco Eメールセキ

ユリティアプライアンス(ESA)の製品知識をCisco Eメールセキュリティフィールドエンジニアの認定レベルにまで引き上げる必要があります。さらに、読者はDNSとSMTPの強力なコマンドとその動作を持っている必要があります。SPF、DKIM、およびDMARCの基本に精通していることがプラスです。

電子メール認証：概要

送信者ポリシーフレームワーク(SPF)

Sender Policy Frameworkは2006年にRFC4408として初めて公開されました。現在のバージョンはRFC7208で指定され、RFC7372で更新されています。SPFは主にリターンパス(MAIL FROM)アドレスを認証しますが、SMTP HELO/EHLO引数（SMTPカンバセーション中に送信される送信者のゲートウェイのFQDN）も認証することを推奨します（およびメカニズムを提供します）。

SPFは、非常に単純な構文のTXTタイプDNSリソースレコードを使用します。

```
spirit.com       text = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.sprit.com
a:mx4.spf.protection.outlook.com all"
```

上記のSpirit Airlinesの記録では、@spirit.comアドレスからの電子メールを特定の/24サブネット、FQDNで識別される2台のマシン、およびMicrosoftのOffice365環境から送信することができます。最後の「~all」修飾子は、レシーバに対して、他のソースをソフト障害（SPFの2つの障害モードの1つ）と見なすように指示します。送信者は、失敗したメッセージに対して受信者が行うべきことを指定せず、どの程度まで失敗するかを指定しないことに注意してください。

一方、Deltaは異なるSPF方式を採用しています。

```
delta.com text = "v=spf1 a:smtp.hosts.delta.com
include:_spf.vendor.delta.com -all"
```

必要なDNSクエリの数を最小限に抑えるために、Deltaは自身のすべてのSMTPゲートウェイをリストする単一の「A」レコードを作成しました。また、「_spf.vendor.delta.com」のベンダーに対して個別のSPFレコードを提供します。また、SPFで認証されていない**メッセージをハード**フェイルする手順（「–all」修飾子）も含まれています。 ベンダーのSPFレコードをさらに調べることができます。

```
_spf.vendor.delta.com text = "v=spf1 include:_spf-delta.vrli.com
include:_spf-ncr.delta.com a:delta-spf.niceondemand.com
include:_spf.airfrance.fr include:_spf.qemailserver.com
include:epsl1?all
```

したがって、送信者@delta.comからの電子メールは、例えばAir Franceの電子メールゲートウェイから正規に送信される可能性があります。

一方、Unitedでは、よりシンプルなSPF方式を使用しています。

```
united.com text = "v=spf1 include:spf.enviaremails.com.br
include:spf.usa.net include:coair.com ip4:161.215.0.0/16
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx all"
```

社内メールゲートウェイ以外にも、電子メールマーケティングプロバイダー(「usa.net」および

「enviaremails.com.br」)、従来のContinental Air Linesゲートウェイ、MXレコード (「MX」メカニズム) に記載されているすべてのものが含まれます。 MX(ドメインの着信メールゲートウェイ)は発信と同じでない可能性があることに注意してください。小規模な企業では通常は同じですが、大規模な組織では、受信メールを処理する個別のインフラストラクチャと、送信メールを処理する個別のインフラストラクチャが用意されます。

また、上記のすべての例では、追加のDNS参照 (「含む」メカニズム) を幅広く使用しています。 ただし、パフォーマンス上の理由から、SPF仕様では、最終レコードの取得に必要なDNSルックアップの総数を10に制限しています。10レベルを超えるDNS再帰を使用するSPFルックアップは失敗します。

Domain Keys Identified Mail(DKIM)

RFC 5585、6376、および5863で指定されているDKIMは、次の2つの歴史的な提案を統合したものです。YahooのDomainKeysとCiscoのIdentified Internet Mail。送信者が発信メッセージを暗号化して署名し、電子メールヘッダー(「DKIM-Signature」)に署名 (および他の検証メタデータ) を含める簡単な方法を提供します。 送信者はDNSで公開キーを発行するため、受信者はキーを取得してシグニチャを確認することが容易になります。DKIMは物理メッセージの送信元を認証しませんが、送信元が送信者組織の秘密キーを所有している場合、送信元の代わりに電子メールを送信することが暗黙的に許可されるという事実に依存します。

DKIMを実装するために、送信組織は1つ以上の公開キーペアを生成し、DNSの公開キーをTXTレコードとして公開します。各キーペアは「セレクタ」によって参照されるため、DKIM検証者はキーを区別できます。発信メッセージが署名され、DKIM-Signatureヘッダーが挿入されます。

```
DKIMv=1a=rsa-sha1;c=/s=united;d=news.united.com;h=MIME-Version:Content-
Type:Content-Transfer-Encoding:Date:To:From:Reply-To:Subject:List-
Unsubscribe:Message-
ID;i=MileagePlus@news.united.com;bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=;

b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JIFTNLO8j4DG
mH1
MMTyYgwYqT01rEwL0V8MEY1MzxTrzijkLPGqt/sK1WZt9pBacEw1fMWRQLf3BxZ3jaYtLoJL
O MRWXTGOWDFHU35CsFG2CNYLo=
```

署名の形式は非常に簡単です。"a"タグは署名に使用されるアルゴリズムを指定し、"c"は[1]を使用する正規化スキームを指定し、"s"はセレクタまたはキー参照で、"d"は署名ドメインです。残りのDKIM-Signatureヘッダーは、メッセージ固有です。「h」は署名済みヘッダーをリストし、「i」は署名済みユーザのIDをリストし、最後にヘッダーは2つの別々のハッシュで終了します。「bh」は署名済みヘッダーのハッシュで、「b」はメッセージ本文のハッシュ値です。

DKIM署名メッセージを受信すると、受信者は次のDNSクエリを作成して公開キーを検索します。

```
<selector>._domainkey.<>
```

DKIM-Signatureヘッダーで指定されているとおりに実行します。上記の例では、クエリは「united._domainkey.news.united.com」です。

```
united._domainkey.news.united.com text = "g=*\;k=rsa\;n=" ""
"postmaster@responsys.com" "with" "any" "questions" "about" "this"
"signing"
```

```
"\;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drGFTMXX/Q
2KkWgl333333
hO4v6dTy5Qmxcuv5AwqxLiz9d0jBaxtuvYALjlGkxmk5MemgAOcCr97GlW7Cr11eLn87qdTm
yE5Levn
TXxVDMjIfQJt6OFzmw6Tp1t05NPWh0PbyUohZYt4qpcbiz9Kc3UB2IBwIDAQAB\;"
```

返されたDNSレコードには、キーと他のオプションパラメータが含まれています。[2]

DKIMの主な問題は、最初の仕様では送信者がDKIMを使用する広告が許可されなかったことです。したがって、メッセージが署名なしで届いた場合、受信者が署名すべきであることを知る簡単な方法はなく、その場合は最も信頼できない可能性があります。1つの組織は複数のセレクタを使用できるため（ほとんどの場合）、ドメインがDKIM対応かどうかを「推測」するのは簡単ではありません。これをカバーするために別規格のAuthor Domain Signing Practicesが開発されましたが、2013年に使い方が低く、その他の問題が廃止され、後継が不要になりました。

ドメインベースのメッセージ認証、レポート、および準拠(DMARC)

DMARCは、カバーされている3つの電子メール認証テクノロジーの中で最も若いテクノロジーであり、SPFとDKIMの両方の欠点に対処するために特別に開発されました。他の2つとは異なり、メッセージのHeader Fromを認証し、他の2つによって以前に実行されたチェックにリンクします。DMARCはRFC7489で規定されています。

SPFおよびDKIMでのDMARCの付加価値は次の要素で構成されます。

- 使用可能なすべてのID（HELO、MAIL FROMおよび/またはDKIM署名ドメイン）がFromヘッダーに揃っていることを確認します（完全に一致または従属）
- 送信者ドメインの所有者が、受信者が失敗したメッセージを処理する方法に関するポリシーを指定するための手段を提供する
- 送信者のドメイン所有者に対して、失敗したメッセージを通知するためのフィードバック機能を提供するため、SPF/DKIM/DMARCポリシー割り当てのフィッシング攻撃または工ラーを簡単に特定できます

また、DMARCはシンプルなDNSベースのポリシー配布メカニズムも使用します。

```
_dmarc.aa.com text =
"v=DMARC1\;p=none\;fo=1\;ri=3600\;rua=mailto:american@rua.agari.com,mail
to:dmarc@aa.com\;ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com
```

DMARCポリシー仕様で必須のタグは「p」で、失敗メッセージに使用するポリシーを指定します。次の3つのうちいずれかにすることができます。none、quarantine、reject。

最も頻繁に使用されるオプションパラメータは、レポートに関連しています。「rua」はURL(mailto:またはPOSTメソッドを使用するhttp:// URL)を使用して、特定のドメインから送信されるように報告された失敗するすべてのメッセージに関する日次の集約レポートを送信します。「ruf」は、障害が発生したすべてのメッセージに関する即時の詳細な障害レポートを送信するURLを指定します。

仕様に従って、受信者はアドバタイズされたポリシーに従う必要があります。そうでない場合は、集約レポートの送信者ドメイン所有者に通知する必要があります。

DMARCの中心的な概念は、いわゆるIDアライメントです。識別子の整列は、メッセージがDMARC検証を通過する方法を定義します。SPF識別子とDKIM識別子は別々に配置され、メッセ

ージはDMARC全体を渡すために何かを渡す必要があります。ただし、DMARCポリシーのオプションでは、1つのアラインメントが通過しても、もう1つのアラインメントが失敗しても、エラーレポートの生成を要求できます。上の例では、"fo"タグが"1"に設定されていることがわかります。

メッセージがDKIMまたはSPF識別子のアライメントに準拠するには、厳格でリラックスした2つの方法があります。厳密な準拠とは、ヘッダーのFromのFQDNが、DKIM署名の署名ドメインID（「d」タグ）またはSPFのMAIL FROM SMTPコマンドのFQDNと完全に一致している必要があることを意味します。一方、Relaxedでは、Header From FQDNを前述の2つのサブドメインのサブドメインにすることができます。 これは、電子メールトラフィックをサードパーティに委任する際に重要な意味を持ちます。これについては、このドキュメントで後述します。

SPF導入に関する考慮事項

レシーバ用SPF

SPF検証は、Cisco EメールセキュリティアプライアンスまたはクラウドEメールセキュリティ仮想アプライアンスで設定するのは簡単です。このドキュメントの以降の部分では、ESAに関するすべての参照にCESも含まれます。

SPF検証はメールフローポリシーで設定されます。グローバルに実行する最も簡単な方法は、適切なリスナーの[Default Policy Parameters]セクションで有効にすることです。 着信および発信メール収集に同じリスナーを使用している場合は、「RELAYED」メールフローポリシーのSPF検証が「Off」に設定されていることを確認します。

SPFではポリシーアクションの指定が許可されないため、SPF検証（および後で説明するようにDKIM）はメッセージを検証し、実行された各SPFチェックのヘッダーセットを挿入するだけです。

```
Received-SPF:(mx1.hc4-93.c3s2.smtpi.com:

  united.5765@envfrm.rsys2.com12.130.136.195

  permitted sender) identity=mailfrom;

  client-ip=12.130.136.195;receiver=mx1.hc4-93.c3s2.smtpi.com;

  envelope-from="united.5765@envfrm.rsys2.com";

  x-sender="united.5765@envfrm.rsys2.com";

  x-conformance=sidf_compatible;x-record-type="v=spf1"

Received-SPF:(mx1.hc4-93.c3s2.smtpi.com:



  postmaster@omp.news.united.com) identity=helo;

  client-ip=12.130.136.195;receiver=mx1.hc4-93.c3s2.smtpi.com;

  envelope-from="united.5765@envfrm.rsys2.com";
```

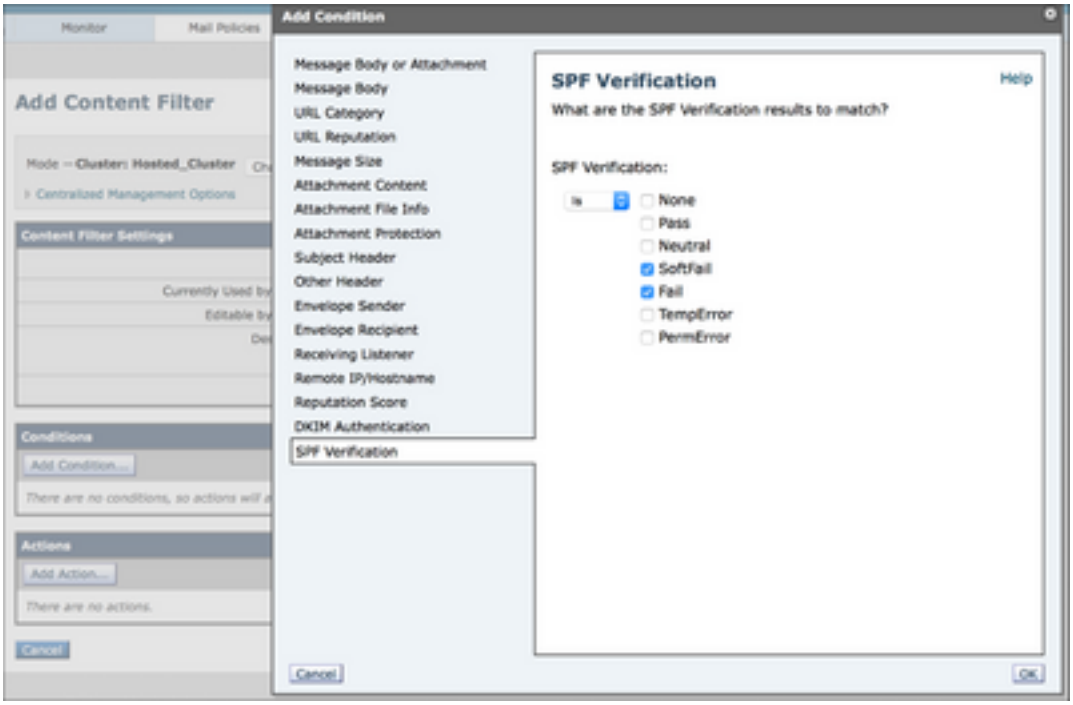
```
x-sender="postmaster@omp.news.united.com";

x-conformance=sidf_compatible
```

このメッセージでは、2つの「ID」がSPFによって確認されていることに注意してください。仕様に基づく「mailfrom」と、同様に推奨される「helo」です。メッセージは正式にSPFを渡します。これは、SPFコンプライアンスに関連するものだけであるためです。一部のレシーバは、HELO IDにSPFレコードを含めない送信者を許可することがあります。したがって、SPFレコードに送信メールゲートウェイのホスト名を含めることをお勧めします。

メールフローポリシーがメッセージを確認したら、実行するアクションをローカル管理者が設定します。これは、メッセージフィルタルールSPF-status() [3]を使用するか、または同じルールを使用して着信コンテンツフィルタを作成し、適切な着信メールポリシーに適用することで行われます。

図1:SPF検証コンテンツフィルタ条件



推奨されるフィルタアクションは、失敗したメッセージ（SPFレコード内の"-all"）をドロップし、ポリシー隔離でソフトフェイル（"~all" in the SPFレコード）のメッセージを検疫することです。ただし、これはセキュリティ要件によって異なる場合があります。一部のレシーバは、失敗したメッセージにタグを付けるか、目に見えるアクションを実行せずに管理者に報告します。

最近、SPFの人気が大幅に高まっていますが、多くのドメインが不完全または誤ったSPFレコードを公開しています。安全な側に置くには、すべてのSPF障害メッセージを隔離し、しばらくの間は隔離を監視して、「false positive」がないことを確認します。

他のドメインまたはサードパーティに電子メールサービスを提供する場合

サードパーティに電子メール配信サービスまたはホスティングサービスを提供する場合、メッセージを独自のSPFレコードに配信するために使用するホスト名とIPアドレスを追加する必要があります。これを行う最も簡単な方法は、プロバイダーが「包括的」なSPFレコードを作成し、顧客にSPFレコードに「含む」メカニズムを使用させることです。

```
suncountry.com text = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148
ip4:146.88.177.149 ip4:67.109.66.68 ip4:198.179.134.238
ip4:107.20.247.57 ip4:207.87.182.66 ip4:199.66.248.0/22 include:cust-
spf.exactarget.com all"
```

ご覧のように、Sun Countryには独自の制御下にある電子メールもありますが、マーケティング電子メールはサードパーティにアウトソーシングされています。参照レコードを展開すると、マーケティングメーリングサービスプロバイダーが使用している現在のIPアドレスのリストが表示されます。

```
cust-spf.exacttarget.com text = " v=spf1 ip4:64.132.92.0/24
ip4:64.132.88.0/23 ip4:66.231.80.0/20 ip4:68.232.192.0/20
ip4:199.122.120.0/21 ip4:207.67.38.0/24 ip4:207.67.98.192/27
ip4:207.250.68.0/24 ip4:43.22.0/28 4:198.ip4:136.ip4:136.ip4:13.13 -all
```

この柔軟性により、電子メールサービスプロバイダーは、DNSレコードを変更するために各顧客に連絡しなくても規模を拡張できます。

サードパーティの電子メールサービスを使用する場合

前の段落と同様に、サードパーティの電子メールサービスを使用していて、完全にSPF検証済みのメールフローを確立する場合は、自分のSPFレコードを自分のメールフローに含める必要があります。

```
jetblue.comv=spf1 include:_spf.qualtrics.com ?all
```

JetBlueはQualtrics分析サービスを使用し、Qualtricsからの正しいSPFレコードを含めるだけで必要です。同様に、他のほとんどのESPは、顧客のレコードに含めるSPFレコードを提供します。

ESPまたはEメールマーケターがSPFレコードを提供しない場合は、自分のメールゲートウェイを直接リストする必要があります。ただし、これらの記録を正確に保つことはユーザの責任であり、プロバイダーがゲートウェイを追加したり、IPアドレスやホスト名を変更したりすると、メールフローが危険にさらされる可能性があります。

SPFを意識していないサードパーティからのさらなる危険は、リソースの共有によってもたらされます。ESPが同じIPアドレスを使用して複数の顧客の電子メールを配信する場合、ある顧客が同じインターフェイスを介して別の顧客を装ってSPF有効なメッセージを生成することは技術的に可能です。このため、SPF制限を設定する前に、MSPのセキュリティポリシーと電子メール認証の認識を調査する必要があります。SPFがインターネット上の信頼の基本的なメカニズムの1つである理由を考慮し、質問に対する回答がない場合は、MSPの選択を再検討することを強く推奨します。 セキュリティだけでなく、SPF、DKIM、DMARCおよびその他の送信者のベストプラクティス[4]は、MSPが提供を保証しています。MSPがそれに従っていない場合、または誤って従っている場合、は大きな受信システムでの信頼性を低下させ、遅延やメッセージのブロックを可能にします。

（サブ）電子メールトラフィックのないドメイン

現在、ほとんどの組織はマーケティング目的で複数のドメインを所有していますが、企業の電子メールトラフィックにアクティブに使用するのは1つだけです。SPFが実稼働ドメインに正しく展開されている場合でも、不正なアクターは、組織のアイデンティティをスプーフィングするために電子メールにアクティブに使用されていない他のドメインを使用できます。SPFは、Eメールトラフィックを生成しないドメイン（およびサブドメイン！）に対して、特別な「すべて拒否」

SPFレコードを通じてこの問題が発生することを防止できます。SPFカウンシルのWebサイトであるopenspf.orgは優れた例です。

SPFの委任は単一のドメインでのみ有効であるため、使用しているサブドメインに対して、電子メールを生成しない可能性がある「すべての」SPFレコードを公開することも重要です。実稼働ドメインに「通常」のSPFレコードがある場合でも、トラフィックのないサブドメインに「すべての拒否」レコードを追加するよう余分な努力を払ってください。繰り返しになりますが、受信は送信に相当しないことに注意してください。ドメインは電子メールを受信するのはもっともですが、送信元になることはありません。これは、短期間のマーケティングドメイン（イベント、期間限定プロモーション、製品発表など）に非常に当てはまります。これらのドメインに着信する電子メールは実稼働ドメインに配信され、それらの電子メールへの応答は実稼働ドメインから配信されます。これらの短期間のドメインには有効なMXレコードが含まれますが、電子メールの送信元がないことがSPFレコードで識別される必要があります。

DKIM導入に関する考慮事項

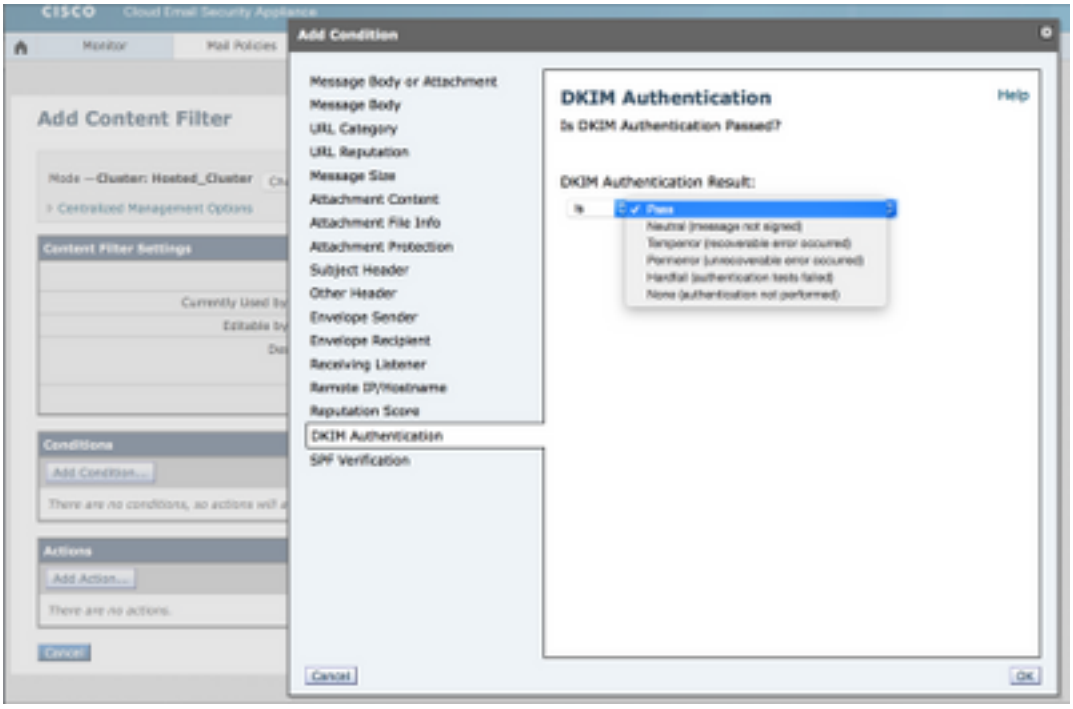
レシーバ用DKIM

ESAでのDKIM検証の設定は、SPF検証に似ています。メールフローポリシーのデフォルトポリシーパラメータで、DKIM検証を「オン」にします。繰り返しますが、DKIMはポリシーの指定を許可しないため、これはシグニチャを確認し、「Authentication-Results」ヘッダーを挿入するだけです。

```
Authentication-Results:mx1.hc4-93.c3s2.smtpi.comdkim=pass (signature
verified) header.i=MileagePlus@news.united.com
```

DKIM検証結果に基づくアクションは、コンテンツフィルタで実行する必要があります。

図2:DKIM検証コンテンツフィルタ条件



単純なSPFとは異なり、DKIMは実際のメッセージテキストを操作するため、一部のパラメータが制限されることがあります。オプションで、DKIM検証プロファイルを作成し、異なる検証プロファイルを異なるメールフローポリシーに割り当てることができます。これにより、受け入れるシ

グ二チャのキーサイズを制限し、キー取得の失敗アクションを設定し、DKIM検証の詳細を設定できます。

メッセージが複数のゲートウェイを通過する際に、複数回の署名が可能になるため、複数のシグ二チャを伝送できます。メッセージがDKIM検証に渡されるため、署名はすべて検証する必要があります。デフォルトでは、ESAは最大5つのシグ二チャを確認します。

SMTPと電子メールの歴史的なオープン性と、インターネット全体の（肯定的な）変化への適応が難しいため、メーリングリストのマネージャがメッセージを直接中継して変更したり、メッセージを新しいメッセージに添付せずに直接転送したりするなど、DKIMシグ二チャが失敗する場合があります。そのため、一般的に、DKIMに障害が発生したメッセージに対するベストプラクティスは、メッセージをドロップするのではなく、検疫またはタグ付けになります。

DKIMとの署名準備

RELAYED Mail Flow PolicyでDKIM署名をオンにする前に、キーを生成/インポートし、DKIM署名プロファイルを作成し、DNSで公開する必要があります。

単一のドメインに署名する場合、プロセスは簡単です。キーペアを生成し、[Mail Policies]の[Domain Keys]セクションに単一の署名プロファイルを作成し、プロファイルの準備が整ったら、[DNS Text Record]の下の[Generate]オプションをクリックします。DNSで生成されたキーを公開します。最後に、メールフローポリシーでDKIM署名をオンにします。

複数の異なるドメインに対して署名する場合は、複雑になります。この場合、次の2つのオプションがあります。

1. 単一の署名プロファイルを使用して、すべてのドメインに署名します。「プライマリ」ドメインのDNSゾーンに（単一の）公開キーを格納し、DKIMシグ二チャがそのキーを参照します。この技術は以前はESPに採用されることが多く、大規模なサインインを可能にしながら、個々の顧客のDNSスペース[5]と対話する必要はありませんでした。
2. サインインするドメインごとに個別の署名プロファイルを作成します。これにより、より複雑な初期設定が可能になりますが、将来に向けて柔軟に移行できます。各ドメインのキーペアを作成し、[Profile Users]セクションに1つのドメイン（およびそのサブドメイン）のみを指定するプロファイルを作成し、その特定のドメインのDNSゾーンに関連する公開キーを公開します。

選択肢#1は最初から簡単ですが、最終的にDMARCを壊してしまうことを覚えておいてください。DMARCでは署名ドメインIDをヘッダーの送信元に合わせる必要があるため、DKIMによるIDの合わせは失敗します。SPFを正しく設定し、DMARC検証をパスするためにSPF IDのアライメントに依存すると、これを回避できる場合があります。

ただし、最初からオプション#2を実装することで、DMARCを心配する必要がなくなり、単一のドメインに対して署名サービスを取り消したり再設定したりすることは非常に簡単です。 また、サードパーティのドメインに**一部の電子メールサービ**スを提供する場合は、ほとんどの場合、これらのサービスから使用するキーを取得する必要があります（およびESAにインポートします）。 このキーはドメイン固有であるため、個別のプロファイルを作成する必要があります。

サードパーティの電子メールサービスを使用する場合

一般的に、DKIM署名を使用し、電子メール処理（マーケティング電子メールなど）の一部をサードパーティにオフロードする場合は、実稼働で使用するキーと同じキーを使用しないでください。これは、DKIMにセレクタが存在する主な理由の1つです。代わりに、新しいキーペアを生成し

、DNSゾーンのパブリック部分を公開し、秘密キーを相手に配信する必要があります。これにより、実稼働のDKIMインフラストラクチャを変更することなく、問題が発生した場合に備えて、そのキーを迅速に取り消すことができます。

DKIM（同じドメインのメッセージは複数の異なるキーで署名できる）には必要ありませんが、サードパーティが処理する電子メールには別のサブドメインを提供することをお勧めします。これにより、メッセージの追跡が容易になり、後でDMARCの実装をよりクリーンにすることができます。例として、Lufthansaからの複数のメッセージから次の5つのDKIM-Signatureヘッダーを検討します。

```
DKIMv=1a=rsa-sha1;c=/s=lufthansa;d=newsletter.milesandmore.com;

DKIMv=1a=rsa-sha1;c=/s=lufthansa2;d=newsletter.lufthansa.com;

DKIMv=1a=rsa-sha1;c=/s=lufthansa3;d=lh.lufthansa.com;

DKIMv=1a=rsa-sha1;c=/s=lufthansa4;d=e.milesandmore.com

DKIMv=1a=rsa-sha1;c=/s=lufthansa5;d=fly-lh.lufthansa.com;
```

Lufthansaは、2つの主要な生産ドメイン（lufthansa.comとmilesandmore.com）の5つの異なるサブドメインに分割された5つのキー（セレクタ）を使用していることがわかります。 つまり、これらはそれぞれ独立して制御でき、それぞれ異なるメッセージングサービスプロバイダーにアウトソーシングできます。

DMARC導入に関する考慮事項

レシーバ用DMARC

ESAでのDMARC検証はプロファイルベースですが、DKIMとは異なり、デフォルトプロファイルは仕様に準拠するように編集する必要があります。ESAのデフォルトの動作では、お客様から明示的に指示されない限りメッセージをドロップすることがないため、デフォルトのDMARC検証プロファイルでは、すべてのアクションが[No Action]に設定されます。また、正しいレポート生成を有効にするには、「メールポリシー」のDMARCセクションの「グローバル設定」を編集する必要があります。

プロファイルが設定されると、DMARC検証は、他の2つと同様に、[メールフローポリシー(Mail Flow Policies)]の[デフォルトポリシー設定(Default Policy Settings)]セクションで設定されます。必ずボックスにチェックを入れて集約フィードバックレポートを送信してください。これは、送信者にとってDMARCの最も重要な機能です。現時点では、ESAはメッセージ単位の障害レポート（DMARCポリシーの「ruf」タグ）の生成をサポートしていません。

DMARCポリシーアクションは送信者から推奨されるため、SPFやDKIMとは異なり、プロファイル設定以外で設定可能な特定のアクションはありません。コンテンツフィルタを作成する必要はありません。

DMARC検証では、Authentication-Resultsヘッダーに次のフィールドが追加されます。

```
Authentication-Results:mx1.hc4-93.c3s2.smtpi.comdkim=pass
header.i=MileagePlus@news.united.com;dmarc=pass (p=none dis=none)
d=news.united.com
```

上記の例では、DMARCがDKIM識別子の配列に基づいて検証され、送信者が要求したポリシーが「none」であることが確認されています。これは、現在DMARC導入の「モニタ」段階にあることを示します。

他のドメインまたはサードパーティに電子メールサービスを提供する場合

DMARC準拠のためのESPの最大の懸念は、適切なIDのアライメントを実現することです。DMARCを計画する際は、SPFが正しく設定されていること、関連する他のすべてのドメインがSPFレコードに発信ゲートウェイを持っていること、および主にMAIL FROMとHeader FromのIDに異なるドメインを使用して送信しない。このエラーは、電子メール通知または警告を送信するアプリケーションによって最も頻繁に発生します。アプリケーション作成者は、電子メールのIDの不一致による影響を主に認識していないためです。

前述のように、ドメインごとに個別のDKIM署名プロファイルを使用し、[ヘッダーの送信元(Header From)]で使用されている署名対象のドメインを署名プロファイルが正しく参照していることを確認します。独自のサブドメインを使用している場合は、1つのキーで署名できますが、DMCポリシー("adkim="r")でDKIMへの準拠を緩めるように設定してください。

一般に、直接制御できない多数のサードパーティに対して電子メールサービスを提供する場合は、配信が最も可能性が高い電子メールの送信方法に関するガイドライン文書を作成することをお勧めします。ユーザ間の電子メールは一般的に適切に動作するため、これは主に前述の例でアプリケーション作成者のポリシー文書として機能します。

サードパーティの電子メールサービスを使用する場合

サードパーティを使用して電子メールトラフィックの一部を配信する場合、最適な方法は、別のサブドメイン（または完全に異なるドメイン）をサードパーティプロバイダーに委任することです。これにより、必要に応じてSPFレコードを管理し、個別のDKIM署名インフラストラクチャを持ち、実稼働トラフィックを妨げることはありません。その後、アウトソース電子メールのDMARCポリシーは、社内のポリシーと異なる場合があります。前述のように、サードパーティが配信する電子メールを考慮する場合は、IDが一致し、DMKIMおよびSPFへの準拠がDMCポリシーで適切に設定されていることを必ず確認してください。

（サブ）電子メールトラフィックのないドメイン

以前の電子メール認証テクノロジーに比べてDMARCが改善されたもう1つの点は、サブドメインの処理方法です。デフォルトでは、特定のドメインのDMARCポリシーがすべてのサブドメインに適用されます。DMARCポリシーレコードを取得する際に、ヘッダーからFQDNレベルでレコードが見つからない場合、受信者は送信者の組織ドメイン[6]を決定し、そこでポリシーレコードを検索する必要があります。

ただし、組織ドメインのDMARCポリシーでは、明示的なDMARCポリシーが公開されていないサブドメインに適用される個別のサブドメインポリシー（DMARCレコードの「sp」タグ）を指定することもできます。

SPFの章で前述したシナリオでは、次のことを行います。

1. 電子メールの正当なソースであるサブドメインに対して**明示的**なDMARCレコードを発行します。
2. 組織ドメインポリシーレコードで「拒否」のサブドメインポリシーを公開し、非送信ドメインをスプーフィングする電子メールを自動的に拒否します

このような電子メール認証の構造は、インフラストラクチャとブランドを最大限に保護します。

DMARC固有の問題

DMARCには潜在的な問題がいくつかあります。これらはすべて、DMARCが依存する他の認証テクノロジーの性質と欠点に起因します。問題は、DMARCが電子メールを拒否するポリシーを積極的にプッシュし、メッセージ内のすべての異なる送信者IDを関連付けることによってそれらの問題を表面化させることです。

ほとんどの問題は、メーリングリストとメーリングリスト管理ソフトウェアで発生します。電子メールがメーリングリストに送信されると、すべての受信者に再配布されます。ただし、元の送信者の送信者アドレスを持つ結果の電子メールは、メーリングリストのマネージャのホスティングインフラストラクチャによって配信されるため、SPFによるヘッダーのチェックに失敗します(ほとんどのメーリングリストのマネージャはエンベロープ送信者(MAIL FROM)と元の送信者のアドレス)。

DMARCはSPFに失敗するため、DKIMに依存する可能性がありますが、ほとんどのメーリングリストのマネージャはメッセージにフッターを追加したり、リスト名を付けたタグの件名を追加したりするため、DKIM署名の検証が失敗します。

DKIMの著者は、この問題に対するいくつかの解決策を提案しています。これらはすべて、すべての送信元アドレスでリストのアドレスを使用し、別の方法で元の送信元アドレスを示すメーリングリストのマネージャに要約されます。

同じような問題は、元のメッセージをSMTP経由で新しい受信者にコピーするだけで転送されるメッセージから発生します。ただし、現在使用されているほとんどのメールユーザエージェントは、新しいメッセージを正しく作成し、転送されたメッセージをインラインまたは新しいメッセージの添付ファイルとして含めます。この方法で転送されたメッセージは、転送ユーザが通過するとDMARCを通過します（もちろん、元のメッセージの信頼性は確立できません）。

電子メール認証を実装するアクションプランの例

テクノロジー自体はシンプルですが、完全なEメール認証インフラストラクチャを実装する道は長く、曲がりくねっています。小規模な組織や制御されたメールフローを持つ組織では、非常に簡単ですが、大規模な環境では非常に困難です。大規模な企業が実装プロジェクトを管理するためにコンサルティングを雇うことは珍しくありません。

ステップ 1：DKIM

DKIMは、署名されていないメッセージには拒否が発生しないため、比較的影響を受けません。実際に実装する前に、前述のすべてのポイントを考慮してください。署名を委任する可能性のあるサードパーティに連絡し、サードパーティがDKIM署名をサポートしていることを確認し、セレクタ管理戦略を検討してください。組織によっては、異なる組織単位に対して個別のキー（セレクタ）を保持する場合があります。追加のセキュリティのためにキーの定期的なローテーションを検討することもできますが、転送中のすべてのメッセージが配信されるまで、古いキーを削除しないでください。

重要なサイズには特に注意が必要です。一般的に「より優れている」が、メッセージごとに2つのデジタル署名（正規化など）を作成することはCPUのコストが高く、発信メールゲートウェイのパフォーマンスに影響を与える可能性があることを考慮する必要があります。計算オーバーヘッドのため、2048ビットが使用可能な最大の実用的なキーサイズですが、ほとんどの導入では、

1024ビットのキーがパフォーマンスとセキュリティの間で大きな妥協を成します。

DMARCの後続の実装を成功させるには、次の手順を実行する必要があります。

1. サブドメインを含め、送信するすべてのドメインを特定します
2. DKIMキーを生成し、各ドメインの署名プロファイルを作成する
3. サードパーティに関連する秘密キーを提供する
4. 関連するDNSゾーンのすべての公開キーを公開する
5. サードパーティが署名を開始する準備ができていることを確認する
6. すべてのESAでDKIMのRELAYEDメールフローポリシーへの署名を有効にする
7. 第三者に署名の開始を通知する

ステップ 2：SPF

SPFの適切な実装は、Eメール認証インフラストラクチャの実装で最も時間がかかり、面倒な作業です。Eメールは非常にシンプルで、セキュリティとアクセスポイントから完全にオープンな方法で使用できたため、組織は従来から使用できるユーザや方法に対して厳密なポリシーを適用していませんでした。このため、今日のほとんどの組織では、内外の異なるEメールソースをすべて把握できていません。SPFを実装する唯一の最大の問題は、現在あなたの代わりに正当に電子メールを送信しているユーザを検出することです。

調べる項目は次のとおりです。

1. 明確なターゲット：Exchangeまたはその他のグループウェアサーバまたは送信メールゲートウェイ
2. 外部通知を生成する可能性のあるDLPソリューションまたはその他の電子メール処理システム
3. 顧客と対話する情報を送信するCRMシステム
4. 電子メールを送信できるさまざまなサードパーティアプリケーション
5. 電子メールを送信できるラボ、テスト、その他のサーバ
6. 外部の電子メールを直接送信するように設定されたパーソナルコンピュータおよびデバイス

組織の環境は異なるため、上記のリストは完全ではありませんが、何を探すかについて一般的なガイドラインとして考慮する必要があります。（ほとんどの）電子メールソースが特定されたら、一歩前に戻って、既存のソースをすべて承認する代わりに、リストをクリーンアップします。理想的には、送信メールはすべて送信メールゲートウェイを通じて配信され、いくつかの正当な例外が発生します。独自のマーケティングメールソリューションを使用している場合、またはサードパーティのマーケティングメールソリューションを使用している場合は、実稼働の電子メールゲートウェイとは別のインフラストラクチャを使用する必要があります。メール配信ネットワークが非常に複雑な場合は、SPFの現在の状態の文書化に進むことがありますが、将来の状況のクリーンアップには時間がかかります。

同じインフラストラクチャ上で複数のドメインにサービスを提供する場合は、単一のユニバーサルSPFレコードを作成し、「include」メカニズムを使用して個々のドメインで参照する必要があります。SPFレコードが広すぎないことを確認します。たとえば、/24ネットワーク内の5台のマシンだけがSMTPを送信する場合は、ネットワーク全体ではなく、5つの個々のIPアドレスをSPFに追加します。記録を可能な限り具体的に作成し、悪意のある電子メールが個人情報を侵害する可能性を最小限に抑えることを目指します。

一致しない送信者("~all")のsoftfailオプションから開始します。 100%ご自身が電子メールのソースをすべて特定したことを確認した後にハードフェイル(-all)に変更する**だけです**。それ以外の場合は、実稼働メールが失われる危険性があります。後でDMARCを実装し、しばらくの間モニタ

モードで実行すると、見落としたシステムを特定し、SPFレコードを更新して完了できるようになります。SPFをハードウェア障害に設定するだけで安全です。

ステップ 3：DMARC

DKIMとSPFを可能な限り設定したら、DMARCポリシーを作成します。前の章で説明した状況をすべて考慮し、複雑なEメールインフラストラクチャを使用している場合は、複数のDMARCレコードを展開する準備をします。

レポートを受信する電子メールエイリアスを作成するか、それらを取り込むことができるWebアプリケーションを作成します。これには厳密に定義された電子メールアドレスは使用されませんが、rua@domain.com、dmarc.rua@domain.com、mailauth-rua@domain.comなどの記述的な電子メールアドレスは役立ちます。オペレータがこれらのアドレスを監視し、SPF、DKIMおよびDMARC設定を適切に変更するプロセスが存在することを確認するか、スプーフィングキャンペーンの場合はセキュリティチームに警告します。最初は、SPFおよびDKIMの設定中に失われた可能性のあるすべてをカバーするようにレコードを調整するため、ワークロードは大きくなります。しばらくすると、レポートにはスプーフィングの試行だけが示されます。

最初に、DMARCポリシーを「none」に設定し、フォレンジックオプションを設定して、失敗したチェック(「fo=1」)に関するレポートを送信します。これにより、トラフィックに影響を与えることなく、SPFとDKIMのエラーが迅速に検出されます。送信したレポートの内容に問題がなければ、セキュリティポリシーと設定に応じて、ポリシーを「検疫」または「拒否」に変更します。繰り返しますが、誤検出に関して、受信したDMARCレポートを継続的に分析するオペレータがいることを確認してください。

DMARCを完全かつ正しく実装することは、小規模でも短期間でもありません。一部の結果 (およびDMARCの正式な「実装」) は、不完全なレコードのセットと「なし」のポリシーを公開することで得られますが、送信者の組織とインターネット全体の両方にとって、すべての人がその能力を最大限に実装することが最善です。

スケジュールについては、一般的なプロジェクトの個々のステップの概要を示します。繰り返しますが、各組織が異なるため、次の点は正確ではありません。

1 .DKIMのプランニングと準備	2 ~ 4週間
2. DKIMテストの実行	2 週間
3. SPF：正当な送信者ID	2 ~ 4週間
4.DMARC方針準備	2 週間
5. SPFおよびDMARCレコードのテストの実行	4 ~ 8週間
6. SPFテストをハードウェアで実行	2 週間
7.検疫/拒否で実行されるDMARCテスト	4 週間
8. DMARCレポートのモニタリングと、それに応じたSPF/DKIMの適用	連続

小規模な組織では、ほとんどのステップ、特にステップ3と4の短い期間が発生する可能性があります。Eメールインフラストラクチャがどれだけシンプルであるかに関係なく、テストの実行中に十分な時間を割り当て、見逃したフィードバックの詳細を監視します。

大規模な組織では、より厳しいテスト要件を持つ同じ手順の期間がさらに長くなる可能性があります。複雑な電子メールインフラストラクチャを持つ企業が、電子メール認証の実装の技術的な側面だけでなく、プロジェクト全体を管理し、チームや部門間で調整するために、外部のヘルプを雇用することは珍しくありません。

その他の参考資料

- SPFの参照サイト：http://www.openspf.org
- DKIM理事会：http://www.dkim.org
- DMARCのメインWebサイト。The Trusted Domain Project:http://www.dmarc.org
- dmarcian - DMARCの著者の1人であるTim Draegenが運営するヘルプおよびリソースサイト。「ツール」セクションを参照してください。http://www.dmarcian.com
- Online Trust Allianceのレコード検証ツール：https://otalliance.org/resources/spf-dmarc-record-validator
- DMARC Record Assistant:DMARCレコードの作成に役立つもう1つの便利なツールです。http://www.kitterman.com/dmarc/assistant.html
- SPFレコードテストツール：http://www.kitterman.com/spf/validate.html
- 「嫌な奴じゃないぞ。Deep Dive Into Email Authentication Techniques」、Cisco Live 2014プレゼンテーションBRKSEC-3770:https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1]正規化は、このドキュメントの範囲外です。DKIMの正規化の詳細については、「参考資料」セクションの資料を参照してください。

[2] DKIM DNSレコードパラメータも、このドキュメントの範囲外です。

[3]メッセージフィルタの作成は、このドキュメントの範囲外です。詳細については、AsyncOS for Emailユーザガイドを参照してください。

[4] M3AAWGは、ほとんどの業界で採用され、尊重されている優れたベストプラクティスを定義しました。送信者のベストプラクティスに関するドキュメントは、https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdfから入手できます

[5]この動作は、元々DKIMがMAIL FROMまたはHeader Fromに記載されたメッセージソースを検証しないという事実を利用します。確認するのは、署名ドメインID（ DKIM Signatureの"d"パラメータ、および署名プロファイルの"Domain Name"パラメータ）が、メッセージの署名に使用されるペアの公開キーを実際にホストしていることを示すだけです。送信者の信頼性は、「From」ヘッダーに署名することによって暗示されます。[Profile Users]セクションで署名するすべてのドメイン（およびサブドメイン）を必ずリストしてください。

[6]通常、TLD以下のドメイン1レベルまたは関連するccTLDプレフィックス（.ac.uk、.com.sgなど）