Messaging, Malware and Mobile Anti-Abuse Working Group

# M³AAWG パークドメインを保護するベストコモンプラクティス

## M³AAWG Protecting Parked Domains Best Common Practices

2015 年 12 月更新

目次



## I. エグゼクティブサマリー

多くの組織や個人はドメインを使用したり限られた状況で使用したりすることを意識せずにドメインを登録します。これらのドメイン (またはサブドメイン) は電子メールトラフィックを送受信することを目的としていません。たとえば、悪意のある行為者がドメインを取得して悪用することを防ぐためにドメインを登録することができます。これを防御登録といいます。これらのドメインは「パーク」されています。他の例では、ドメインまたはサブドメインは電子メールサービスが有効になっていないウェブサイトを含むためだけに使用されます。

メールボックスプロバイダーはそのようなドメインが必要な識別子を持っているという条件で、受信メールを非常に効果的に認証するための手法を使っています。この Messaging, Malware and Mobile Anti-Abuse Working Group のベストプラクティス文書では電子メールの送受信を目的としていないドメインまたはサブドメインを示すために使用できる識別子について説明しています。

## II. 問題の提示

パークドメインが電子メールを送受信しないことを知らせる電子メール認証レコードを広報しなかった場合、第三者がこの種のドメインを悪用する機会が提供されます。攻撃は通常2つの条件の結果です。

- ドメインはよく知られているドメインに似ています
- ドメインに評価されたレピュテーションがありません

実際に確認されているこのような攻撃は、電子メール認証技術を適切に使用することで軽減できます。特定の種類のSPF[1]、DKIM[2]、DMARC[3]およびMX[4]レコードのDNSでの広報は電子メールを送受信しないドメインを示すために使用できます。受信者はこれらのレコードに頼って、そのようなドメインからのものである電子メールを拒否することができます。

## III. DNS (Domain Name System)

### SPF (Sender Policy Framework)

パークドメインを含む電子メールを送信しないドメインは「裸の」-all と呼ばれる SPF TXT レコードを DNS に広報する必要があります。このタイプの TXT レコードの例は次のとおりです:

example.com TXT "v=spf1 -all"

このレコードはドメイン「example.com」宛てに電子メールを送信する権限のある IP が無いことを示しています。

ワイルドカードレコードが組織の DNS ポリシーによって許可されていない限り、潜在的な各サブドメインのレコードを作成する必要があるため、サブドメインの保護はより複雑です。 このタイプのレコードは次のとおりです:

*.example.com TXT "v=spf1 -all"

### DKIM (DomainKeys Identified Mail)

DKIM レコードは、パブリックキーを示すためにドメインキーエントリにリンクされているセレクタに基づいています。 例えば:

selector1._domainkey.example.com TXT "v=DKIM1; p=32AB567E34F..."

キーが失効したことを示す正しい方法は p に値を設定しないことです (http://tools.ietf.org/html/rfc6376#section-3.6.1[5]を参照)。

セレクタを確実に見つけるために、次のワイルドカード登録を使用できます:

*._domainkey.example.com TXT "v=DKIM1; p="

このレコードは「example.com」というドメインの DKIM キーの有効期限が切れていることを示しています。サブドメインを扱う場合はワイルドカードを使用する必要があります:

*.example.com TXT "v=DKIM1; p="

この上位レベルのワイルドカードは SPF レコードをオーバーロードする可能性があります。 他に使用されていないパークドメインの場合、ここに示す 2 つのレコードは問題になりません。

有効な DKIM 署名のない電子メールは DKIM 署名が全くない場合と同様に扱う必要がありますが、期限切れの鍵を持つ電子メールは通常、より慎重に扱われます。

## DMARC (Domain-based Message Authentication, Reporting & Conformance)

パークドメインを含む電子メールを送信しないドメインは DNS で DMARC TXT レコードを広報し、"p=reject" を指定する必要があります。このタイプの TXT レコードの例は次のとおりです:

_dmarc.example.com TXT "v=DMARC1; p=reject;

rua=mailto:rua@example.com; ruf=mailto:ruf@example.com"

RUA[6]タグを含めることはドメイン所有者が悪用の可能性についての集約レポートを受け取ることを可能にするのに重要です。 RUF[7]タグの存在はオプションですが、失敗レポートを受け取り、必要に応じて悪用の可能性についてフォローアップできるようにすることをお勧めします。 RUF タグを使用すると、悪用されているドメインが大量の失敗レポートを受信することがあります。

関連するドメインは「裸の」-all として公開されており、そのドメインから送信されることを目的とした DKIM で電子メールに署名していないため、そのような電子メールは DMARC ポリシーを適用するメールボックスプロバイダーによって拒否されるべきです。 DMARC は、設計上、組織ドメインのサブドメインに対して機能するため、別のレコードを作成する必要がありません。

理論的には DMARC レコードは冗長である可能性があり、SPF または DKIM レコードを持つ必要は明らかにありませんが、すべての受信者が DMARC を実装するわけではありません。

ドメイン自体が電子メールを受信しない場合、RUA と RUF は以下のように電子メールを受信する別のドメインを指定しなければなりません:

_dmarc.example.com TXT "v=DMARC1; p=reject;

rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"

example.com._report._dmarc.example.net TXT "v=DMARC1"

RUA または RUF タグを変更する必要があるため、パークドメインごとに DMARC レコードを変更するのは面倒です。 この場合、CNAME[8]レコードを使用できます:

_dmarc.example.com CNAME _dmarc.parked.example.net.

_dmarc.parked.example.net TXT "v=DMARC1; p=reject;

rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"

*._report._dmarc.example.net TXT "v=DMARC1"

## Null Mx

電子メールの受信者は電子メールに返信できることを確認することがあります。たとえば、エンベロープの MAIL-FROM (5321.From)、ヘッダーの From (5322.From) または「Reply-To」などのヘッダーに示されている john@example.com から電子メールを受信する可能性があります。この場合、受信者はドメイン example.com の MX、A または AAAA レコードの存在を検索することでこのアドレスに電子メールで返信できることを確認しようとします。

残念なことに、ドメインによってはウェブサイトのみに使用され、SMTP に使用されるポート 25 をリッスンせずに A レコードまたは AAAA レコードあるいはその両方を持つことになります。 DNS チェックを行うことは中程度の資源集約的ですが、ポート 25 が待機していることを確認することは非常に資源集約的です。

ドメインが電子メールの受信を目的としていないことを示すための推奨される方法は次の null MX レコード[9]を公開することです:

example.com MX 0.

すべてのサブドメインで機能させるためにはワイルドカードを使用する必要があります:

*.example.com MX 0.

上記の方法は電子メール受信者のほんの一部で実装されています。受信者が MX レコードの存在を確認するだけではそのレコードが null MX レコードであることを確認できず誤った結論に至ることがあります。2015 年後半の時点で、M³AAWG はまだ標準を実装していない受信者との最大の互換性を保つためにドメインに A レコードまたは AAAA レコードあるいはその両方がある場合に限り null MX レコードの使用を推奨します。

### SOA (Start of Authority)

SOA[10]を使用して責任のある当事者が到達可能であることを示すこともできます。おそらく別のドメインで:

example.com SOA ns.example.com hostmaster.example.net 2013020801
900 600 86400 3600

## IV. 例

この章では、さまざまなシナリオで追加する DNS レコードについて説明します。各レコードの説明については上記のⅢ章を参照してください。

### A. 単一のパークドメイン

example.com. TXT "v=spf1 -all"

*.example.com. TXT "v=spf1 -all"

*.example.com. TXT "v=DKIM1; p="

_dmarc.example.com. TXT "v=DMARC1; p=reject;

rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"

example.com._report._dmarc.example.net TXT "v=DMARC1"

### B. 単一のパークドメインと A または AAAA レコード

example.com. TXT "v=spf1 -all"

*.example.com. TXT "v=spf1 -all"

*.example.com. TXT "v=DKIM1; p="

_dmarc.example.com. TXT "v=DMARC1; p=reject;

rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"

example.com._report._dmarc.example.net TXT "v=DMARC1"

example.com. MX 0 .

example.com. A 192.168.0.1

sub.example.com. A 192.168.0.1

sub.example.com. MX 0 .

### C. 複数のパークドメイン

example.com. TXT "v=spf1 -all"

*.example.com. TXT "v=spf1 -all"

*.example.com. TXT "v=DKIM1; p="

_dmarc.example.com. CNAME _dmarc.parked.example.net.

example.org. TXT "v=spf1 -all"

*.example.org. TXT "v=spf1 -all"

*.example.org. TXT "v=DKIM1; p="

_dmarc.example.org. CNAME _dmarc.parked.example.net.

⋮

_dmarc.parked.example.net TXT "v=DMARC1; p=reject;

rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"

*._report._dmarc.example.net TXT "v=DMARC1"

## V. 迷惑行為の報告

ドメインが電子メールを受信しない場合、アドレス abuse@example.com は機能しません。迷惑行為の苦情の取り扱いを確実にするために、M³AAWGはドメインのWHOISレコードへの迷惑行為の連絡窓口の追加および abuse.net での迷惑行為の連絡先の登録をお勧めします。

## VI. DNSBL / RPZone (DNS Block Lists / Response Policy Zone)

電子メールの受信者が DNS ブロックリストをチェックするのは一般的です。 パークドメインのリストを使用して電子メールをブロックすることはできますが、これまでこのような機能を提供している組織はありません。

## VII. 結論

メールボックスプロバイダーは受信メールを認証するために効果的な手法を使用しています - そのようなドメインに必要な識別子がある場合。この M³AAWG ベストプラクティス文書は「パーク」ドメインまたはサブドメインが電子メールの送受信を目的としていないことを示すために使用できる識別子について説明しています。

## VIII. 参照

[1] SPF - Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1
http://www.openspf.org/RFC 7208
[2] DKIM DomainKeys Identified Mail, http://www.dkim.org/RFC 5585
and DKIM DomainKeys Identified Mail, draft-ietf-dkim-deployment-11,
http://dkim.org/specs/draft-ietf-dkim-deployment-11.html
[3] DMARC - Domain-based Message Authentication, Reporting & Conformance,
https://tools.ietf.org/html/rfc7489
[4] MX - Mail Exchanger Record, see Domain Names - Implementation and Specification,
https://tools.ietf.org/html/rfc1035
[5] RFC 6376 DomainKeys Identified Mail (DKIM) Signatures, Section 3.6.1 Textual Representation,
http://tools.ietf.org/html/rfc6376#section-3.6.1
[6] RUA - Reporting URI for Aggregate reports, see DMARC.org, "DMARC Overview,"
http://www.dmarc.org/overview.html
[7] RUF - Reporting URI for Forensic reports, see DMARC.org, "DMARC Overview,"
http://www.dmarc.org/overview.html
[8] CNAME - Canonical Name record, see Domain Names - Implementation and Specification,
https://tools.ietf.org/html/rfc1035
[9] A "Null MX" No Service Resource Record for Domains That Accept No Mail,
https://tools.ietf.org/html/rfc7505
[10] SOA – State Of Authority record, see Domain Names - Implementation And Specification,
https://tools.ietf.org/html/rfc1035

M³AAWG が公開している全ての文書と同様、この文書の更新については M³AAWG ウェブサイト (www.m3aawg.org) をチェックして下さい。



この文書はインターネット協会 (Internet Association Japan) によって産業界への貢献を目的として翻訳されたものです。
http://www.iajapan.org/

訳者: 北崎 恵凡 (Ayachika Kitazaki) <kitazaki [at] gmail.com>