# 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

このドキュメントの参照 URL:
https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bcp-2022-06-jp.pdf

**2022 年 6 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すぐに利用するわけではないドメインや限定的に使用するためのドメインを登録しています。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。

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。よく知られているドメインに似ているドメインは特にこのような攻撃を受けやすくなります。

特定の種類の SPF[1]、DMARC[2]および MX[3]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。このようなワイルドカードを使用したレコードは次のとおりです:

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

### DKIM (DomainKeys Identified Mail)

パークドメインの DKIM[4]レコードは広報する必要はなく、実際に何も公開されるべきではありません。

パークドメインの DKIM レコードが広報されない場合、パークドメインを使用して DKIM 署名を偽造しようとするメールは、DNS に公開鍵が存在しないため、検証に失敗することになります。

### 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。関連するドメインは「裸の」-all として公開されており、そのドメインを使った DKIM 公開鍵を広報していないので、このドメインを使おうとする電子メールは、SPF または DKIM をパスするアライメントされたドメインを得ることが不可能であるため、すべての DMARC 検証チェックに失敗します。したがって、このドメインを偽装したメールは、DMARC ポリシーを適用している受信ドメインによって拒否されるはずです。

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”
```

DMARC 集約レポートの送信先アドレスを指定する「rua」タグ[5]を含めることはオプションです。

この場合、「rua」タグはオプションとします。なぜなら、集約レポートは認証設定に微調整が必要な有効なメールストリームを特定するのに最も有効だからです。パークドメインの場合、有効なメールストリームはないはずなので、認証設定に手を加える必要はないはずです。それでも、一部のドメイン所有者にとっては、悪用がどの程度防止されているかを知る手がかりとして、この集約レポートは興味深いものでしょう。ドメイン所有者の中には、集約レポートの処理結果(ディスポジション・ビット)がドメインの公開 DMARC ポリシーを尊重していないことを示す場合、レポート生成者に働きかけることを選ぶ人もいるかもしれません。しかし、拒否ポリシーを持つメールを隔離だけするメールボックスプロバイダは、彼らのやり方を変えようとする努力に抵抗するかもしれません。

ドメイン自体が電子メールを受信しない場合、「rua」タグ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”
```

DMARC プロトコル仕様[6]では、このような「サードパーティ・レポーティング」のために、DMARC レポートを受け取るドメインもそのようなレポートを受け取ることに同意したことを確認するレコードを DNS で広報することを要求しています。このレコードは、次の例のようなものです:

```
example.com._report._dmarc.example.net TXT “v=DMARC1;”
```

**Null MX**

電子メールの受信者はメッセージを受け取る前に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。そのような受信者は、受信メールのメッセージにある Return-Path や From 電子メールアドレスのドメインパートが存在するか、ドメインに関連する MX、A、AAAA レコードを確認することで検証しようとするかもしれません。

ドメインがウェブサイトだけに使われ、実際に受信メールの接続を受け付けずに、A および/または AAAA レコードを持っている場合があります。そのようなドメインは存在テストには合格するが、そのようなドメインにメールを配信することは不可能でしょう。

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[7]を公開することです:

```
example.com MX 0.
```

null MX の場合、DNS レコードの右側のホスト名は「からの」ドットです。

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.
```

**SOA (Start of Authority)**

postmaster や abuse などのロールアカウントが存在し、与えられたドメインの適切な連絡先(例: postmaster@example.com, abuse@domain.com )となることが(RFC2142 により)期待されています。null MX レコードを発行するドメインでは、ドメインが受信メールを受け入れないため、この仮定は成り立ちません。しかし、そのドメインの責任者に連絡を取る必要がある場合もあるため、ドメインの SOA レコード[8]を使用して、そのドメインの連絡先情報を伝達する必要があります。

SOA レコードは、DNS レコードの特殊なタイプで、DNS サーバが権限を主張する DNS 名前空間の一部に開始点を印つけるものです。「example.com」ドメインの SOA レコードの例は、次のようになります:

```
example.com SOA ns.example.net hostmaster.example.net 2022040200 3600 7200
86400 86400
```

ここでは

- `example.com` は所有しているドメインです。
- `SOA` は `DNS` の資源レコードタイプです。
- `ns.example.net` はそのドメインの一次権威 `DNS` サーバのホスト名です。
- `hostmaster.example.net` はそのドメインの責任者のメールボックスを指定します。最初のドットの前のラベルはローカルメールボックス名を表しますので、ここでのアドレスは *hostmaster@example.net* です。
- `2022040200` は*シリアル番号*と呼ばれ、ドメインのバージョンを表す番号です。これはしばしば `YYYYMMDDxx` の形式で表され、`1` 日あたり最大 `100` 回の変更という基本的な変更追跡システムを可能にするので、ここでは `2022` 年 `4` 月 `2` 日に公開されたドメインの最初のバージョンとなります。
- `3600` はセカンダリサーバがプライマリサーバに更新を確認するまでの時間を秒単位で表した数値です。M³AAWG はパークドメインには `1` 時間、アクティブドメインにはより短い時間を推奨しています。
- `7200` はセカンダリサーバが失敗した更新を再試行するまでの時間を秒単位で表した数値です。M³AAWG はパークドメインには `2` 時間を推奨しています。
- 最初の `86400` はセカンダリサーバがそのデータを古いとみなすべき、最後の更新からの最大秒数です。M³AAWG はパークドメインには `1` 日を推奨しています。
- 2 番目の 86400 は TTL (Time To Live)を明示的に宣言していないレコードの最小 TTL を秒単位で表したものです。これは問い合わせサーバが再度応答を求めるまでにどれくらいの期間キャッシュしておくかを示すもので、M³AAWG はパークドメインには 1 日を推奨しています。

# 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. MX 0 .
*.example.com. TXT “v=spf1 -all”
*.example.com MX 0 .
_dmarc.example.com. TXT "v=DMARC1; p=reject; rua=mailto:rua@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. A 192.168.0.1
example.com. TXT "v=spf1 -all"
example.com. MX 0 .
*.example.com. A 192.168.0.1
*.example.com. TXT “v=spf1 -all”
*.example.com. MX 0 .
sub.example.com. A 192.168.0.1
sub.example.com. MX 0 .
sub.example.com. TXT “v=spf1 -all”
_dmarc.example.com. TXT "v=DMARC1; p=reject; rua=mailto:rua@example.net”
example.com._report._dmarc.example.net TXT “v=DMARC1;”
```

**c)** 複数のパークドメイン

```
example.com. TXT "v=spf1 -all”
example.com. MX 0 .
*.example.com. TXT “v=spf1 -all”
*.example.com. MX 0 .
_dmarc.example.com. CNAME _dmarc.parked.example.net.
example.org. TXT "v=spf1 -all"
example.org. MX 0 .
*.example.org. TXT “v=spf1 -all”
*.example.org. MX 0 .
_dmarc.example.org. CNAME _dmarc.parked.example.net.
_dmarc.parked.example.net TXT "v=DMARC1; p=reject; rua=mailto:rua@example.net”
example.com._report._dmarc.example.net TXT “v=DMARC1;”
example.org._report._dmarc.example.net TXT “v=DMARC1;”
```

## V. 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。ドメイン所有者はドメインベースのリスト(IP ベースのリストではなく)を公開している DNSBL プロバイダへドメイン所有者のパークドメインを DNSBL に含めることに関心があるかどうかを問い合わせることができます。このような要請はドメイン所有者が将来そのドメインを使用してメールを送信することはないと 100%確信している場合にのみ行うべきです。なぜなら、このようなリストを元に戻すことは困難だからです。ドメインが譲渡される可能性があり、新しい譲受人がそのドメインを電子メールに使用する可能性がある場合、この方法は推奨されません。

## VI. 結論

この文書はパークドメインの管理者がそのドメインが電子メールを送信していないことを DNS で広報するためのベストプラクティスを説明しています。メールボックスプロバイダなどがこの情報を有効に活用できる保証はありませんが、このプラクティスに従うことで、少なくともドメイン所有者がその事実を公表するためにできることはすべて行ったということを確認することができます。

## VII. 参照

[1]SPF – Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 https://www.rfc-editor.org/rfc/rfc7208

[2]DMARC – Domain-based Message Authentication, Reporting and Conformance, https://www.rfc-editor.org/rfc/rfc7489

[3]MX – Mail Exchanger Record, see Domain Names - Implementation and Specification, https://www.rfc-editor.org/rfc/rfc1035

[4]DKIM – DomainKeys Identified Mail (DKIM) Service Overview, https://www.rfc-editor.org/rfc/rfc5585 and DomainKeys Identified Mail (DKIM) Signatures, https://www.rfc-editor.org/rfc/rfc6376

[5]RFC 7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC), Section 6.3, General Record Format, https://www.rfc-editor.org/rfc/rfc7489#section-6.3

[6]CNAME – Canonical Name record, see Domain Names - Implementation and Specification, https://www.rfc-editor.org/rfc/rfc1035

[7]A "Null MX" No Service Resource Record for Domains That Accept No Mail, https://www.rfc-editor.org/rfc/rfc7505

[8]SOA – Start of Authority record, see Domain Names - Implementation and Specification, https://www.rfc-editor.org/rfc/rfc1035

As with all best practices that we publish, please check the M[3]AAWG website (m3aawg.org) for updates to this document.



この文書は JPAAWG (Japan Anti-Abuse Working Group) 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。https://www.jpaawg.org/

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