JP AAWG JAPAN ANTI-ABUSE WORKING GROUP

M3AAWG ドキュメント解説 ~ Parked Domains Best Common Practices ~

株式会社インターネットイニシアティブ

今村 侑輔

[前座] Parked Domain とは

- 日本語だと「予約ドメイン」、「確保ドメイン」のような意味
- 企業の代表ドメインに類似したドメインや利用を終了したドメインなどを用いたブランド悪用を防ぐためにドメイン取得**だけ**をすることがある
- 例
  - jpaawg.org (もともとのドメイン)
  - ipaawg.org (j と i を見間違う)
  - jpaavvg.org (w と vv を見間違う)
  - jpaaawg.org (a が1つ多い)
  - jpaawg.jp (TLD(トップレベルドメイン)違い)
  - jpaawg.net
  - jpaawg.com
  - etc…

Parked Domain BCP

- 防衛的に取得したドメイン、Webサイト専用でメールを使わないドメインなど、利用有無にかかわらず “メール送受信に使わない” ことが確定しているドメイン/サブドメインに対してどういう設定をするのがよいか、が書かれている



Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Protecting Parked Domains Best Common Practices

https://www.m3aawg.org/M3AAWG-Protecting-Parked-Domains-BCP-update-2022-06

Updated June 2022

JPAAWG

SPF

- メールを送信しないことを示すため、SPFで -all を公開する。

example.com TXT "v=spf1 -all"

- サブドメインも保護する場合は、可能ならワイルドカードを使う。

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

DKIM

- パークドドメインには DKIM レコードを公開しない。
- DKIM公開鍵が存在しなければ、そのドメインを使った偽装署名は検証に失敗する。

DMARC

- DMARCは p=reject を公開する。

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

- SPFは -all、DKIMは未設定なので、そのドメインをFromに使うメールはDMARC認証に失敗し、受信側が拒否できる。
- rua による集計レポート送信先の指定は任意。メールを受けないドメインの場合、レポート送信先は別の受信可能なドメインにする必要がある。

Null MX

- メールを受信しないことを明示するため、Null MXを設定する。

example.com MX 0 .

- サブドメインも保護する場合は、可能ならワイルドカードを使う。

*.example.com MX 0 .

SOA

- postmaster@ や abuse@ が存在しない場合でも、ドメイン責任者への連絡先は必要になる。
- そのため、SOAレコード内の責任者メールボックス情報を適切に設定することが推奨されている。

補足

- DNSBLやRPZone※1のようなドメインベースのブロックリストに、Parked Domain を掲載してもらう選択肢もある。
- ただし、そのドメインを将来メール用途で使う可能性がある場合は推奨されない。
- いったん掲載されると解除が難しいことがあるため、完全にメール用途で使わないと確信できる場合に限るべき。

※1 Response Policy Zone の略、DNSキャッシュフィルタリングに用いる

まとめ

- Parked Domain では、下記をDNSに公開することで、そのドメインがメールを送受信しないことを明確に示せる。

  SPF –all

  DMARC p=reject

  Null MX

  適切なSOA連絡先

- これにより、受信側がなりすましメールを拒否しやすくなり、ドメイン所有者として可能な限り悪用防止の意思表示を行える。

Thank you

