

## **Appendix 2.**

## **DKIM レコードの記述例**



## Appendix 2. DKIM レコードの記述例

本節では、DKIM レコードの記述例について説明します。

### Appendix 2.1 DKIM レコードの例

DKIM レコードは SPF レコードに比べる指定する内容は簡単ですが、バージョンの記述など間違えないように気をつけて記述するようご注意ください。DKIM レコード公開後に必ず、試験的にメールを送信して認証成功するかどうかを確認することが必要です。

#### Sample 1: 一般的な DKIM レコード

```
k100430._domainkey.example.co.jp IN TXT "v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqSPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS
4a9tO9roiT+VyyyMflBoTdMNEWoXUMHafPkgOFPI5YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lg
PRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

#### Sample 2: t=y の指定により試験的運用であることを示す

```
k100429._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; t=y; p=MIGfMA0GCSqGSIb
3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqSPFzZUUb1nNqMj7ozyv/Q0Www
GJ+bdS4a9tO9roiT+VyyyMflBoTdMNEWoXUMHafPkgOFPI5YO52pZM40bdXY/qtfT2nglJqS53zFFqB36q
HoN9lgPRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

## Appendix 2.2 DKIM レコードの間違い例

文法的に間違っただKIMレコードを公開すると、受信側では permerror と扱われ、せっかく公開しても正しく扱われないことになってしまうばかりでなく、受信側で認証を pass したメール以外受信しないようなサー

ビスを提供していた場合、メールが届かなくなる可能性があります。

ここでは以下に間違いやすい例を示しますので、これらを参考に誤った記述が少なくなることを期待します。

### Sample 1: 誤った FQDN 上に DKIM レコードを公開している (その1)

直接該当ドメインの TXT レコードとして公開しています。DKIM の場合、SPF とは異

なり、"セレクトア.\_domainkey" サブドメインに公開する必要があります。

(誤)

```
example.co.jp IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdmNEWoXUMHafPgkOFPI5
YO52pZM40bdXY/qtfT2nglJ"
```

(正)

```
k100429._domainkey.example.co.jp IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdmNEWoXUMHafPgkOFPI5
YO52pZM40bdXY/qtfT2nglJ"
```

### Sample 2: 誤った FQDN 上に DKIM レコードを公開している (その2)

セレクトアを使わないで、サブドメインの \_domainkey 以下に直接キーのレコードを記述しています。正しくは、"セレクト

ア.\_domainkey" サブドメインに公開する必要があります。

(誤)

```
._domainkey.example.co.jp IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdmNEWoXUMHafPgkOFPI5
YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/IC5Bx+wIDAQAB"
```

(正)

```
K100429._domainkey.example.co.jp IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
W7HmqsPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdmNEWoXUMHafPgkOFPI5
YO52pZM40bdXY/qtfT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfIwD58ISU/IC5Bx+wIDAQAB"
```

### Sample 3: 公開鍵方式指定の誤り

公開鍵方式の指定をハッシュの方式と間違えてあります (k=sha1 ではなく k=rsa)。

(誤)

```
k100429._domainkey.example.com. IN TXT"v=DKIM1; k=sha1; t=y;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqSPFzZUU
b1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPI5YO52pZM40bdX
Y/qttT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

(正)

```
K100429._domainkey.example.co.jp IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
W7HmqSPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPI5
YO52pZM40bdXY/qttT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

### Sample 4: バージョン記述の誤り

DKIM のバージョンを間違えています (v=DKIM1.0 ではなく、v=DKIM1)。

(誤)

```
k100429._domainkey.example.com. IN TXT"v=DKIM1.0; k=rsa; t=y;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqSPFzZUU
b1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPI5YO52pZM40bdX
Y/qttT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

(正)

```
K100429._domainkey.example.co.jp IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
W7HmqSPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPI5
YO52pZM40bdXY/qttT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

### Sample 5: バージョン記述の位置の間違え

タグの順番を間違えています。v= タグがレコードの先頭に必要です。

(誤)

```
k100429._domainkey.example.com. IN TXT"k=rsa; v=DKIM1; t=y;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOooW7HmqSPFzZUU
b1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPI5YO52pZM40bdX
Y/qttT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

(正)

```
K100429._domainkey.example.co.jp IN TXT
"v=DKIM1;k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDwDc+AabcditzcdHYwOoo
W7HmqSPFzZUUb1nNqMj7ozyv/Q0WwwGJ+bdS4a9tO9roiT+VyyyMfIBoTdMNEWoXUMHafPgkOFPI5
YO52pZM40bdXY/qttT2nglJqS53zFFqB36qHoN9lgPRwP/e+ScCPlwHkcfwD58ISU/IC5Bx+wIDAQAB"
```

## Appendix 2.3 DKIM のレコードの確認方法の例

現行の送信ドメイン認証技術は、認証情報及びポリシーの公開のために DNS 上に TXT レコードを公開する手法が一般的であるため、これを調査することにより、任意のドメインが送信ドメイン認証技術に対応しているか、ある程度調べることができます。

Appendix 1.3 と同様に、以下では、例として、UNIX host コマンドの TXT レコードオ

プションを利用していますが、同様のクエリが発行できれば問題ありません。このような操作を行うことにより、有効なレスポンスがあるかどうかでレコードの有無を判断できます。

### DKIM / DomainKeys レコード

```
$ host -t txt selector._domainkey.example.com  
selector._domainkey.example.com descriptive text "k=rsa%; t=y%; p=(中略)%; n=A 768 bit key%;"
```

### DKIM ADSP レコード

```
$ host -t txt _adsp._domainkey.example.com  
_adsp._domainkey.example.com descriptive text "dkim=all"
```

ただし、DKIM の場合は、ドメインに加えて前述のセレクトラが分からなければ確認することは困難です。

また、そもそも、これらの DNS レコードは、送信者が試験として一時的に設置してい

る可能性もあり、DNS レコードが存在しているからといって送信ドメイン認証技術に対応しているかは断定できません。したがって、以上のような確認方法は、あくまで補助的な確認方法となることに注意して下さい。

