RFC5617
DomainKeys Identified Mail (DKIM)
Author Domain Signing Practices (ADSP)
概要

概要

- RFC5617

  DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)

- ADSP とは

  DKIMの認証結果をどのように扱うべきかを、メール送信者がメール受信者に対して公開する枠組み。受信側はその方針をチェックすることができる（ADSP check）

用語の定義･説明

dkim.jp

用語	説明
著者 (Author)	著者アドレスの所有者 (メッセージ作成者)
著者アドレス (Author Address)	Fromヘッダフィールド中の電子メールアドレス。複数アドレスの場合は、そのメッセージは複数の著者アドレスを有することになる。
著者ドメイン (Author Domain)	著者アドレスの@の右側部分 (@自体は除く)
ADS (Author Domain Signature)	DKIM署名エンティティ(DKIM-Signatureヘッダフィールド中のd=tag など)のドメインと著者ドメインとが同じである有効な署名を指す。 (例) From：hoge@domain.example DKIM-Signature d=domain.example 上記の場合、ADSを有するという
ADSP (Author Domain Signing Practices)	著者ドメイン署名方針：DKIMの認証結果をどのように扱うべきかを定義したもの

ADSP の用法

著者ドメインとメッセージ中の署名によって受信者はADSP検索から有益な情報を得るが、その情報量は様々。

- メッセージに有効な署名が存在しない場合
  → ADSP結果は直接メッセージに関連したものになる。
- メッセージにADSがある場合
  → そのメッセージがそのドメインに対する何らかのADSPに準拠していることは既知であるため、ADSPはそのドメインに関する新情報を提供しない。
- メッセージにADS以外の有効な署名がある場合
  → 受信者はそのメッセージの評価に署名とADSP結果の両方を使うことができる。

ADSP の結果

著者アドレスに対するADSP検索は以下の4種類の結果のうち
ひとつを生成する。

1. このドメインからのメッセージにADSがあるかないかは不明（ドメインは存在するがADSPレコードが見つからない場合）
2. このドメインからのすべてのメッセージはADSで署名されている
3. このドメインからのすべてのメッセージはADSで署名されており廃棄可能である
4. このドメインは対象外である。すなわち、ドメインがDNSに存在しない

ADSP レコードの説明

ADSP レコードは、送信者側の権威 DNS サーバに TXT レコードとして登録する

_adsp._domainkey.<ドメイン名> TXT　"dkim=<設定値>"

設定値	説明
unknown	このドメインから送信されるメールは著者ドメインで署名されているか不明
all	このドメインから送信されるメールはすべて著者ドメインで署名されている
discardable	このドメインから送信されるメールはすべて著者ドメインで署名されている。著者ドメインで署名されていない。 メッセージは破棄を推奨

- 上記設定値以外の値は "unknown" と解釈される
- ワイルドカードを含むADSPレコードを発行してはならない

ADSP 検索の流れ

受信者側では以下の流れで ADSP レコードを検索する。

#	説明
1	著者ドメインでDNSを検索する (どんな TYPE でも良いが、MX が妥当)
2	1. の結果が、その著者ドメインはDNSに存在しない (NXDOMAIN) の場合、そのドメインが範囲外であることを示すエラーで終了しなければならない。
3	DNS ADSPレコード (_adsp._domainkey.<ドメイン名>) を検索する
4-a	3. の結果が、NOERROR かつ 単一レコード かつ 有効なADSPレコードの場合、そのレコードを使用して終了する。
4-b	3. の結果が、NXDOMAIN またはレコードのない NOERROR の場合、ADSP レコードはない。
4-c	3. の結果が、複数のレコードが含まれる または 非有効なレコードが含まれている場合、ADSP結果は確定しない。
4-d	3. の結果が、SERVFAILの場合、結果を返さずに似終了する。この場合、メッセージを待ち行列に入れる、一時的な失敗を示す SMTP エラーを返す対応が可能)

照合結果（Authentication-Results）

dkim.jp

ADSP を照合した結果、受信者側では以下のように情報を残す。

Authentication-Results: dkim-adsp=<code>

code	意味
none	DKIM ADSPレコードは発行されなかった。
pass	このメッセージには有効なADSが付いている(有効なADSはあらゆるADSPポリシを満たすため、この結果に対するADSP検証の実行は必要ない。)
unknown	メッセージに有効なADSは見つからず、発行されたADSPは”unknown”である。
fail	メッセージに有効なADSは見つからず、発行されたADSPは”all”である。
discard	メッセージに有効なADSは見つからず、発行されたADSPは”discardable”である。
nxdomain	著者のDNSドメインに対するADSP評価が、著者のDNSドメインが存在しないことを示した。
temperror	一時的なDNSエラーなどの短期的な性質のエラーのためにADSPレコードを取得できなかった。後の試行では最終的な結果が生成されるかもしれない。
permerror	長期的なDNSエラーなどの回復不可能なエラーのためにADSPレコードを取得できなかった。後の試行でも最終的な結果が生成されそうにない。