RFC 6541
Authorized Third-Party Signature
概要

- RFC 6541
  - DomainKeys Identified Mail (DKIM) Authorized Third-Party Signature
- ATPS とは？
  - Authorized Third-Party Signature の略
  - 第三者署名を作成者署名と同格に扱うための方法
  - Experimental な状態のプロトコルだが、有効性が認められれば Standard Track に進めたい、と著者は考えている

- ドメイン所有者
  - DNS に ATPS レコード(TXT レコード)を追加
- 署名者(第三者署名)
  - DKIM-Signature に atps, atpsh タグを追加
    - d= に署名者のドメインを指定
    - atps= に RFC5322.From のドメイン(=ADMD) を指定
    - atpsh= にハッシュアルゴリズム(または none)を指定
- 検証者
  - RFC5322.From のドメインが atps= のドメインに一致したら DNS で ATPS レコードを検索
  - レコードが有効なら、送信者署名と同格として扱う

- ATPS レコード
  - TXT レコードとして追加
  - ホスト部は以下の書式

```
<atps-domain>._atps.<admd-domain>
```

  - atps-domain は以下のいずれか指定可能
    - 平文(ドメインそのもの)
    - ハッシュ＋Base32 したもの(ドメイン長上限対策)
  - 値の書式は DKIM レコードと同じ
    - 有効なタグは以下のもの
      - v= : 必須:バージョン番号を指定。”ATSP1” のみ有効。
      - d=: 推奨: atsp-domain 部を平文で指定

- DNS ATSP レコードの例
  - 送信者：example.com
  - 署名者：one.example.com, two.example.com

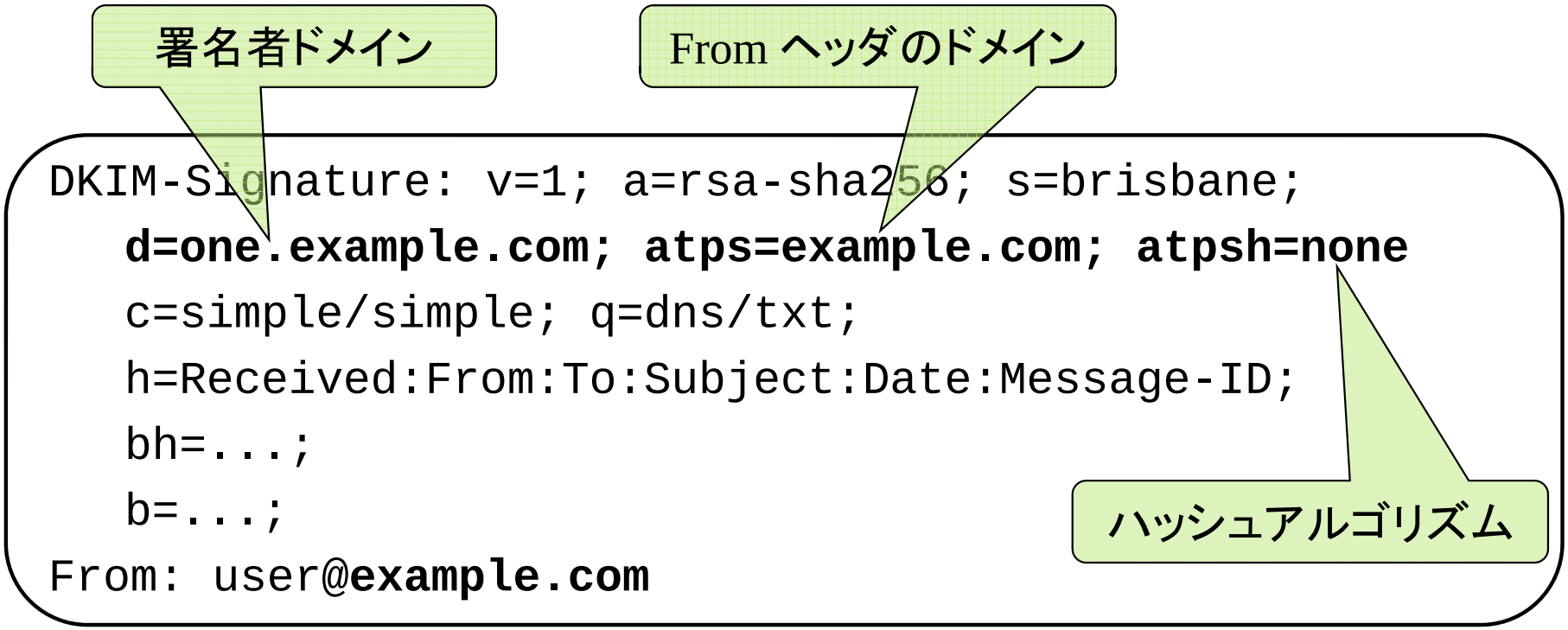
署名者ドメイン
（atpsh=none）

```
one.example.com._atps.example.com. ¥
                    IN TXT   “v=ATSP1”
ZTZGRRV3F45A4U6HLDKBF3ZCOW4V2AJX._atps.example.com. ¥
                    IN TXT   “v=ATSP1; d=two.example.com”
```

ハッシュ化（+Base32）後の署名者ドメイン
（atpsh=sha1）

署名者ドメイン
（平文）

- DKIM-Signature の例
  - 送信者: example.com
  - 署名者: one.example.com



dkim.jp

・ Authentication-Results の例

```
Authentication-Results: example.net;
   dkim=pass header.i=@example.com;
   dkim-atps=pass
From: user@example.com
```

ATSP の認証結果

dkim-atps の値	意味
none	メールに atps タグ付きの有効な DKIM 署名が存在しない
pass	ATPS の認証処理が（少なくとも1つ）成功した
fail	ATPS の認証処理が以下のどちらかの理由で全て失敗した -RFC5322.From のドメインが atps= の値に一致しない -DNS に該当の ATPS レコードが存在しない
temperror	ATPS の認証処理が一時的エラーで完了できなかった
permerror	ATPS の認証処理が永続的エラーで完了できなかった

- ATSP クエリの生成手順
  1. DKIM-Signature の atpsh=　の値に従いハッシュアルゴリズムを選択
     - 無効な値であれば ATSP は無効とする
  2. d= タグの値を取得し、小文字に正規化
  3. 正規化した値を 1. で選択したアルゴリズムに従いハッシュ値を計算し、Base32 で表示可能文字列に変換
  4. 3. で変換した文字列の末尾に “._atps.” を付加
  5. 4. の文字列の末尾に atps= タグの値を付加
  6. 5. の文字列を用いて DNS TXT レコードを検索

- ATSP クエリ応答の処理
  - 有効な ATSP レコードが返された場合、署名者ドメインは ADMD により承認されたドメインであると示されたと判定する
  - 有効な ATSP レコードが返されない場合、署名は通常の第三者署名と判定する
  - エラーが返された場合、上記どちらかの判定が出来ないため、処理を中断しあとで再度処理するべきである
- 評価結果の解釈
  - ADMD により承認されたドメインであると示されたら、作成者署名と同様に取り扱う

- 適用例
  - 第三者署名を付加する送信事業者
    - お客様側で ATPS レコードを登録する必要あり
    - DKIM レコードを登録してもらうのにくらべれば鍵管理がないぶん楽？
    - 乗り換えがしづらくなるのでは？
  - メーリングリストはやっぱり救えない
    - ドメイン所有者から見れば、特定少数の署名者ドメインが対象