

# 送信ドメイン認証

2005年5月10日

パナソニックネットワークサービス株式会社

池田武

# インターネットのメール

- SMTPというプロトコル(通信手順)でメールを中継する。
- 1982年にRFC821として公開されてから、基本的な部分はほとんど変更されていない。
- 当時は技術者たちの狭いネットワークで使用されていたため、性善説の手順であったものが、そのまま不特定多数の世界に広がったため、問題が顕在化している。

# SMTPの問題点

- ヘッダ中の送信者アドレス(From:)は簡単に詐称できる。
- プロトコル中の送信者アドレス(MAIL FROM)は簡単に詐称できる。
- 自分宛のメールであれば、送信者がどのようなMTA(メールサーバ)を使用しているても受信する。
- 送信者を偽装した詐欺メール(Phishing)を防げない。

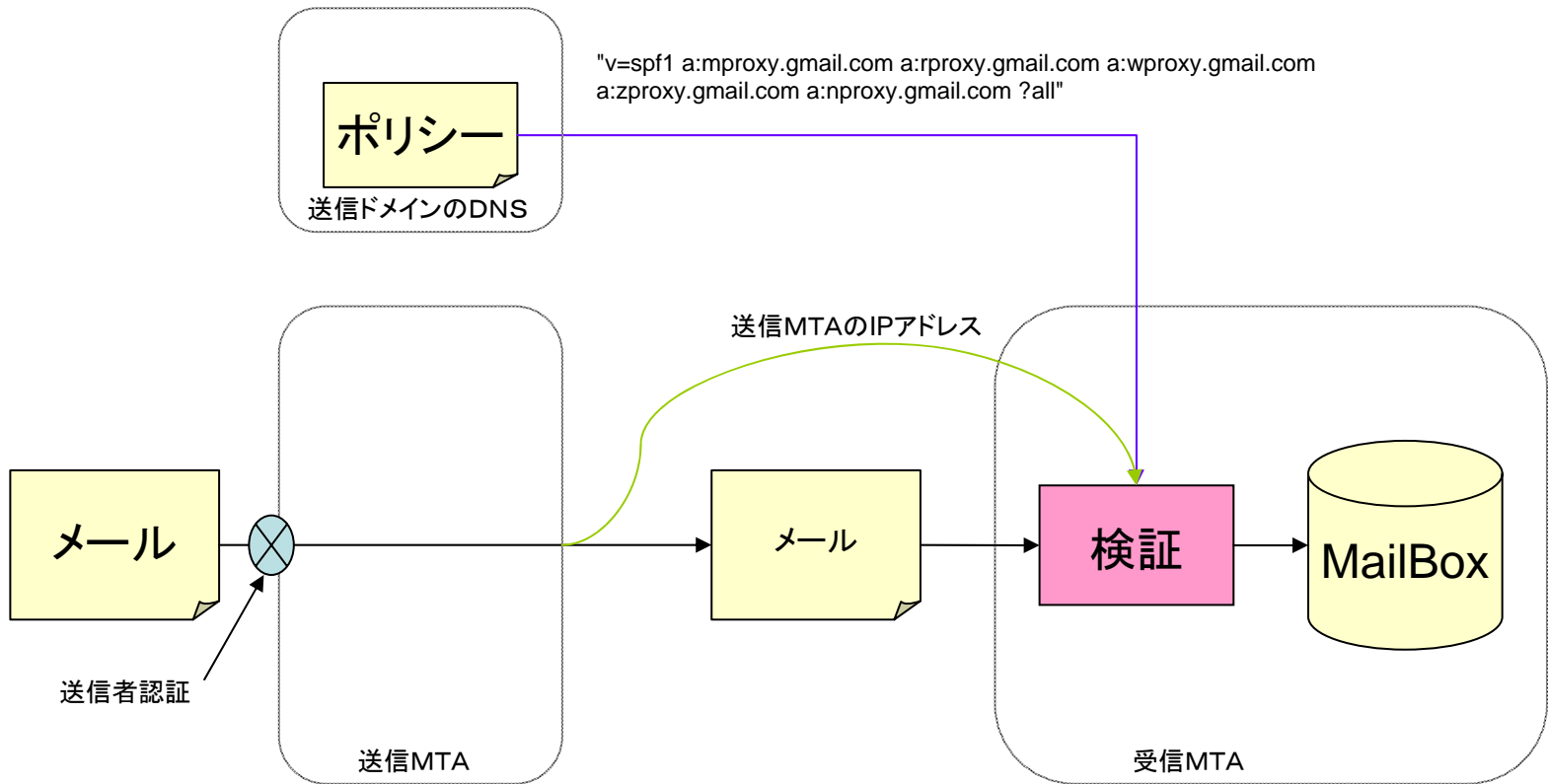
# 詐称防止の方法

- 電子署名による本人認証(S-MIME等)。
  - メールアドレスによって送信者個人を特定可能。
  - MTAに依存しない。送信者の署名を受信者が検証。
  - メール以外の手段(WebPage等)で公開されている証明書を信頼する。証明書の署名者(Verisign等)を信頼する。自動化は難しい。
- DNSベースによる送信ドメイン認証。
  - 送信ドメインの正当性をDNSを用いて検証する。個人の特定をすることは難しい。
  - MTA間で検証を行い、送受信者は認証を意識しない場合が多い。
  - DNSの権限者＝ドメインの権限者であることにより検証結果を信頼する。自動化が容易。

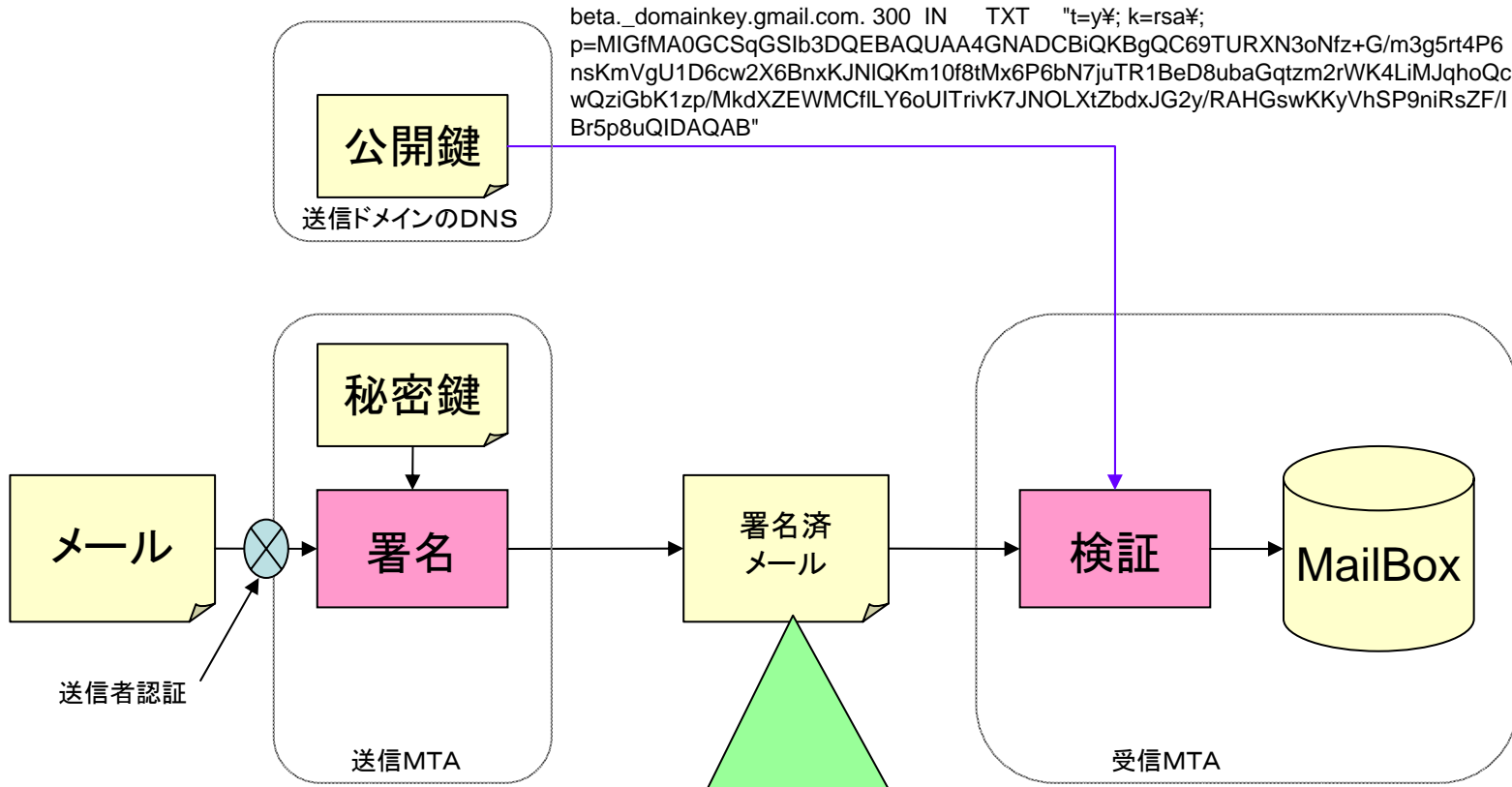
# 送信ドメイン認証の種類

- SPF/Sender ID(MFROm)
  - SMTPプロトコルのMAILFROMを元に送信サーバのIPアドレスが正しいかを検証。
- Sender ID(PRA)
  - ヘッダ中のFrom:やSender:を元に送信サーバのIPアドレスが正しいかを検証。
- DomainKeys
  - ヘッダ中の送信サーバでの署名を元にFrom:やMessage-ID:等が正しいかを検証。

# SPF/Sender ID



# DomainKeys



```
beta._domainkey.gmail.com. 300 IN TXT "t=y#; k=rsa#;  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC69TURXN3oNfz+G/m3g5rt4P6  
nsKmVgU1D6cw2X6BnxKJNIQKm10f8tMx6P6bN7juTR1BeD8ubaGqtm2rWK4LiMJqhoQc  
wQziGbK1zp/MkdXZEWMcfILY6oUITrivK7JNOLXtZbdxJG2y/RAHGswKKyVhSP9niRsZF/  
Br5p8uQIDAQAB"
```

```
DomainKey-Signature: a=rsa-sha1; q=dns; c=noFWS; s=beta;  
d=gmail.com; h=received:message-id:from:to:references:  
subject: date:mime-version:content-type:content-transfer-  
encoding:x-priority:x-msmail-priority:x-mailer:x-mimeole;  
b=QScqTY4lJuxOronDbmebrN6dYrcYFScF9hrfwKDv35fPICNbg  
5ldGc+twXQ2ajvnadO8uyUquXQZzNc1EC6xJ7WPYrG1WHRjvl  
bbHEN3vdOff8CxxBZVfC3QemBqMaLsyOux994c6K+uKyGOx3  
XFLv1McaiFinwxnaVTLmeDdDk
```

# 課題【転送】

- SPF/SenderID(MFROOM)
  - 対応不可。
  - SMTPプロトコルの拡張が検討されている。
- SenderID(PRA)
  - Resent-Fromヘッダに転送元のアドレスを入れることにより可能。
- DomainKeys
  - 問題なし。



# 課題【メーリングリスト】

- SPF/SenderID(MFROM)
  - MLプログラムによってMAILFROMがML管理者として発信されるため問題なし。
- SenderID(PRA)
  - SenderまたはResent-FromヘッダをML管理者とすることにより可能。
- DomainKeys
  - MLで再署名することにより可能
  - MLがSubjectやReceivedを書き換えるため、署名対象を除外する必要あり。

# 課題【第三者投稿サーバ】

- SPF/SenderID(MFROm)
  - 対応不可。
  - SMTPプロトコルの拡張が検討されている。
- SenderID(PRA)
  - Senderヘッダに送信サーバのメールアカウントを入れることにより可能。
- DomainKeys
  - 認証アカウントのドメインで署名することは可能だが、それに意味があるのか？

# 運用ポリシー上の課題

- SPF/SenderID

- 記述の最後に、`?all / ~all / -all`をつけて、正規サーバ以外のポリシーを公開する。
  - `?all`は正規サーバ以外も受信して、事後のフィルタ等に処理を任せるため効果が薄い。(Neutral)
  - `~all`は、受信MTAがGraylist対応の場合には一時的エラーを返して、再送を促す。(SoftFail)  
Graylistとは、Sendmail等のMTAならばちゃんと再送するが、Spammerは、そのような面倒はしないという考え方にもとづくもので、ある程度の効果が期待されるが、採用するには管理DBを持ったリアプライアンス製品を購入するためのコストが発生する。
  - `-all`は正規サーバ以外を認めず、受信側MTAで恒久的エラーを返してしまうため厳しすぎる。(Fail)
- ISP系は `?all` で、企業系は `-all` が現実的か？

# 運用ポリシー上の課題

- DomainKeys
  - 署名に使用するヘッダをどのようにするかをポリシーで決めることが可能。
  - 対象ヘッダを増やせばそれだけ偽装されにくくなるが、運用性が落ちる。
  - ex. Subject: や Received: を含めると、メーリングリストでの書き換えに対応できない。

# JPドメインの対応状況

ゾーン	総数	MX	SPF	DK	SPF%	DK%
汎用	352856	224528	310	21	0.138	0.009
AC	3161	2967	8	0	0.270	0.000
AD	301	256	4	1	1.563	0.391
CO	270323	250595	180	9	0.072	0.004
ED	4315	3881	0	0	0.000	0.000
GO	841	726	0	0	0.000	0.000
GR	9207	7838	12	0	0.153	0.000
LG	2784	997	0	0	0.000	0.000
NE	17308	13203	59	7	0.447	0.053
OR	19921	18557	16	2	0.086	0.011
地域	4151	3487	4	0	0.115	0.000
合計	685168	527035	593	40	0.113	0.008

2005年4月 WIDE/JPRS共同調査