メールドメイン認証の設定・ログ解析・導入について

松元　隆二

九州工業大学 管理本部技術部・飯塚地区

要旨 (総合技術研究会 2025 筑波大学・口頭発表 2025 年 3 月 7 日)

大規模なメールサービスである Google の gmail および米 Yahoo が 2024 年 2 月からメールを受信する時の条件であるメールドメイン認証を強化した。その対応に向けて、九州工業大学で筆者の関係するメールシステムで行った、DKIM 設定・ML の DKIM 対応・ドメイン認証 DKIM のログ(DMARC レポート)解析および問題になりそうな学内サーバへの報告作業について述べる。

1. Google のメールドメイン認証強化

2023 年 10 月 Google はメールドメイン認証の強化を発表。2024 年 2 月に導入予告。関連記事として下記が参考になる。

`https://www.itmedia.co.jp/news/articles/2402/20/news109.html`
実は 2 月 1 日からメールが届いていないかも？Gmail ガイドラインで事業者、利用者が知っておくべきこと

そもそも、メールは差出人(From:)の偽装が可能。インターネットが学術ネットだった 1990 年代はほとんど偽装がなかった。近年、第三者が差出人を偽装して、フィッシングメールや SPAM メールを送信する問題が多発。問題を対策するため、メールドメイン認証 SPF/DKIM/DMARC がある。

2. メールドメイン認証技術

2.1. SPF (Sender Policy Framework)

差出人のドメインごとに信頼する送信メールサーバの IP アドレスを限定する技術。ドメインを定義している権威 DNS に IP アドレス等を設定する。

```
$ dig +short example.com txt  (※dig は DNS の情報を参照するコマンド)
"v=spf1 ip4:192.0.2.0/24 ~all"
```

差出人が*@example.com のメールの送信元のメールサーバの IP アドレスとして 192.0.2.0/24 は信頼できるという指示。それ以外の IP アドレス(~all/チルダ all)は不正メールの可能性あるが受信拒否はしないという指示。もし(-all/マイナス all)の場合は受信拒否して欲しいという指示になる。

※あくまで**希望**であり、受信メールサーバに SPF を参照する設定がなければ、受信が行われる。

参考：上記の応用で、下記のように定義すると、

```
$ dig +short example.jp txt
"v=spf1 -all"
```

差出人が*@example.jp のメールをすべて拒否してほしいという指示(希望)になる。

2.2. DKIM / DMARC

DKIM (DomainKeys Identified Mail)とは差出人のドメインごとに公開鍵暗号署名をする技術。ドメインを定義している権威 DNS に公開鍵を設定。送信メールサーバに秘密鍵を設定。送信メールサーバが秘密鍵で署名。受信メールサーバが DNS の公開鍵で署名を確認する。「作成者署名」と「第三者署名」がある。詳細は後述。

DMARC (Domain-based Message Authentication、Reporting and Conformance）とは DKIM のポリシー設定。DKIM 署名が無い場合の取扱いや DKIM のログの送信先を権威 DNS に設定。詳細は後述。

差出人のメールアドレス(From)には 2 種類あり、メールのヘッダに記載される「ヘッダ From」と、メールサーバが内部的に用いる「エンベロープ From」の違いがある。(SMTP プロトコル/RFC821 で「RCPT TO」で指定する値。)

以降区別して記載する。「ヘッダ From」と「エンベロープ From」は同じ場合がほとんどだが、異なる場合もある。DKIM では「ヘッダ From」を用いる。SPF は「エンベロープ From」を用いる。

3. メールドメイン認証導入前の状況

私の管理するサーバは、SPF については以前より設定していた。 DKIM/DMARC については未設定。Google がメールドメイン認証の強化した 2024 年 2 月時点では夏休みに検証を考えていた。Google のメールドメイン対策の強化は流量が少ないサーバは対象外となるため、2024 年 2 月の時点では影響は出ないと考えていた。

しかし、教員より 5 月に教員向けの 5 学科のトップドメインのメールサーバ(以降「学科メールサーバ」と記載)に DKIM 設定希望があった。学外にメールを送ったら受信拒否されたらしい。

本件は学外のメールサーバで行われた自動転送の問題と考えている。メールサーバの設定でメールを自動転送や ML を経由すると送信メールサーバの IP アドレスが変わるため SPF が失敗する。SPF が失敗したため、受信メールサーバで DKIM 署名を確認。DKIM 署名が無いため、受信拒否という流れ。

なお、一部メールサーバでは自動転送時は「エンベロープ From」を書き換えてこの問題を回避している。内部的な差出人である「エンベロープ From」を書きかえてもメール本文や「ヘッダ From」は変更されない。

同様の問題が ML(メーリングリスト)にもある。詳細は後述。

4. メールドメイン認証導入の流れ

以下の流れで今回導入した。

- 7 月: 技術部のメールサーバに DKIM+DMARC 設定。技術部を人身御供にした。
- 9 月: 学科メールサーバに DKIM 署名導入。DMARC はテストモード。DKIM のログの収集開始。学科に周知時、一部研究室メールサーバの設定変更が必要な可能性について周知。詳細は後述。
- 11 月上旬: 問題になりそうな研究室メールサーバに周知。
- 12 月上旬: 改善が見られない研究室メールサーバに再周知。
- 12 月末: DMARC をテストモードから実運用設定に変更。

5. 具体的な設定など

5.1. DKIM 設定の流れ

試験導入として 7 月から技術部メールサーバに設定を行った。フリーソフトで構築されてり、OS は AlmaLinux8 であり MTA として postfix を用てる。AlmaLinux8 には opendkim が標準で含まれている。opendkim は DKIM 署名および検証を行うソフトウエアである。opendkim で DKIM 公開鍵と秘密鍵を作成し、秘密鍵を opendkim に設定し、公開鍵を技術部権威 DNS に設定した。 下記は設定例。「selector」はドメインで定義した任意文字列。

```
$ dig +short selector._domainkey.kiban-i.kyutech.ac.jp txt

"v=DKIM1; k=rsa; " "p=公開鍵 part1/250 文字程度" "公開鍵 part2/250 文字程度"
```

公開鍵は 500 文字程度ある。長い文字列を DNS に登録するとエラーになるため DNS ソフトのマニュアル等を参照してほしい。DNS が ISC BIND の場合は opendkim が登録用のサンプルを自動生成する。

DKIM 署名・検証ツールはフリーソフトだと他に rspamd などある。細かいことを行わないなら opendkim。細かい設定をするなら rspamd が良いが設定がかなり複雑。

権威 DNS に公開鍵を設定後、送信メールサーバの MTA(postix 等)に設定を行う。設定を行うと、送信時に下記のような署名/DKIM-Signature が自動挿入される。後述するが、この時に第三者のメールアドレスに署名しないよう注意。

```
-- DKIM 署名例/メールのヘッダに記載 --

From: hoge@example.ac.jp

DKIM-Signature: v=1; a=rsa-sha256; d=技術部 example.ac.jp

                    (各種補助情報); b=秘密鍵による署名
```

学科メールサーバは有償ソフトで構築されており、OS は RedHatEL8、MTA は有償ソフト(以降有償ソフトと記載)を導入しているが、マニュアルには公開鍵と秘密鍵作成は opendkim で作成するよう記載があった。署名作成と署名の検証は商用ソフトが行っている。

次に受信側で DKIM が正しく検証されているかの確認だが、もちろん受信メールサーバの MTA に DKIM 検証を行う設定が必要になる。gmail や Microsoft 系のフリーメールなどは DKIM 検証に対応しているため、確認に利用することも可能。検証結果は受信メールのヘッダ部分(Authentication-Results)を確認する。権威 DNS の公開鍵とメール本文の署名/DKIM-Signature を用いて正しい署名であるか検証が行われる。

```
-- DKIM 署名の検証結果 /メールのヘッダに記載 --

Authentication-Results: spf=pass (sender IP is 192.0.2.2)

 smtp.mailfrom=sub.example.ac.jp; dkim=pass (signature was verified)
```

dkim=pass となってれば DKIM 署名の検証に成功している。検証失敗や署名が無い場合は fail や none になる。

上記のような流れで DKIM 署名を設定できる。注意点として、DKIM は差出人偽装を防ぐ技術であって、アンチスパムではない。2024 年以降スパムにも DKIM 署名が行われていることが多い。

5.2. DMARC 設定の流れ

DKIM のポリシー設定である DMARC には下記のような可能。

- 送信先のメールサーバに受信ポリシー設定(SPF 同様あくまで希望の設定)

  p=none: テスト導入用。DKIM 署名の検証に失敗しても無条件で受信。

  p=quarantine(隔離する): DKIM 署名の検証に失敗した場合はスパム。

  p=reject: DKIM 署名の検証に失敗した場合は受信拒否。

- DMARC レポート送信依頼の設定(受信メールサーバが対応している場合のみ送付される)

rua:mailto:メールアドレス:　DMARC レポート(DKIM のログ)の送信を希望する場合メールアドレスを設定。DMARC で受信拒否したメールのログは送ってこない。

ruf:mailto:メールアドレス:　DMARC で受信拒否したログを送付。未対応のところが多い。

設定例：

```
$ dig +short _dmarc.example.ac.jp txt

"v=DMARC1; p=quarantine; sp=none; (実際は改行なし)

 rua=mailto:root@example.ac.jp; ruf=mailto:root@example.ac.jp; fo=1"
```

導入当初は DMARC を p=none として、rua/ruf を設定し、ログの収集を開始した。受信拒否したメールのログ(ruf)はほぼ来ないため導入時から p=quarantine/reject にするのは勧めない。実運用で p=reject にしているところは少ない。執筆時点で私が把握しているのは携帯電話の ezweb.ne.jp と米 yahoo.com のみ。

5.3. DMARC レポート

DMARC で設定したメールアドレスに以下のような XML がメールで送付される。下記は学科メールサーバから hotmail にメールを送ったあと、hotmail(Microsoft)から送られてきた DMARC レポートのヘッダ部分の抜粋。

```
------------------------------
<report_metadata>
    <org_name>Outlook.com</org_name>
    <email>省略</email>
    <report_id>省略(report_id は頻繁にコリジョンあるので注意)</report_id>
    <date_range>
      <begin>1740528000</begin>  <end>1740614400</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>sub.example.ac.jp</domain>  学科ドメイン
    <adkim>r</adkim> <aspf>r</aspf>
    <p>quarantine</p> DMARC 受信ポリシー
    <sp>none</sp>
    <pct>100</pct>
    <fo>1</fo>
  </policy_published>
------------------------------
```

DMARC レポート抜粋。個々の受信のレポート。

```
-----------
  <record>
    <row>
      <source_ip>学科メールサーバ IP アドレス</source_ip>
      <count>1</count> 同じ内容のメールのレポートはまとめられます。
      <policy_evaluated>
        <disposition>none</disposition> none は受信を行ったという意味。
                                          ほかに、quarantine と reject があります。
        <dkim>pass</dkim> DKIM 成功。失敗時は fail
        <spf>pass</spf> SPF 成功。失敗時は fail
      </policy_evaluated>
    </row>
    <identifiers>
      <envelope_to>送り先の hotmail ドメイン</envelope_to>
      <envelope_from>学科ドメイン</envelope_from>
      <header_from>学科ドメイン</header_from>
    </identifiers>
    <auth_results>
      (細かい情報/省略)
    </auth_results>
  </record>
</feedback>
-----------
```

5.4. DKIM「作成者署名」と「第三者署名」

有償ソフトで構築した学科メールサーバ(sub.example.ac.jp)のメールを調べると想定外の DKIM 署名が付与されていた。自動転送したメールに無条件に DKIM 署名が付与されている！！

例えば下記のようなメール転送を行った場合(example.com は学外の第三者とする)

- ヘッダ From: hoge@example.com → 学科メールサーバ・自動転送→研究室メールサーバ

研究室メールサーバに届いたメールを確認すると、学科メールサーバが第三者のメールのヘッダ From に対して DKIM 署名を行っている。

-- DKIM 第三者署名例/メールのヘッダに記載 --

From: hoge@example.com ←第三者(学外)の無関係なヘッダ From

DKIM-Signature: v=1; a=rsa-sha256; d=sub.example.ac.jp;←本学が署名

--

第三者のヘッダ From に対しての署名を DKIM 第三者署名という。

一部のメールサービス(Microsoft365 等)がホスティングしているメールドメインに対して第三者署名を行う事があるが、フリーメールサービス(gmail/hotmail/outlook.com)等で自動転送メールに無条件に第三者署名を行うサービスは確認できなかった。(本学の生涯メールサービスは Microsoft がホスティングしている。2024 年 11 月までは Microsoft の第三者署名だったが、現在は作成者署名。)

学科メールサーバの挙動は表現を変えると、本学が第三者のメールに対して公開鍵暗号署名を行なっているのと同義。スパムメールならスパムに署名を行っていると同義。

有償ソフトのためバグレポートを行ったが仕様という回答。どうにもならないので、このまま運用している。

6. 周知作業

11 月上旬に DMARC レポートを解析して学内周知。メールドメイン認証に対応しないと、将来的に Gmail 等から受信拒否される可能性を挙げた。主な問題点としては 2 点。

6.1. 差出人偽装

研究室のメールサーバより、学科メールサーバのメールアドレスをヘッダ From 設定して送信している例が多数。メールシステムから見ればヘッダ From の偽装と違いは無い。DMARC レポートを解析して、本設定を行っている研究室を摘出。

```
<source_ip>研究室のメールサーバ IP アドレス</source_ip>
<policy_evaluated>
  <disposition>none</disposition> 受信は成功
  <dkim>fail</dkim> DKIM 失敗・正確には DKIM 署名が無い。
  <spf>pass</spf> 学内 IP なので SPF は pass だが、通常は SPF も fail になる。
</policy_evaluated>
```

該当教員に対して、メールリーダーの SMTP サーバとして学科メールサーバを指定するよう依頼。もしくは、ヘッダ From の偽装を行うのをやめ、研究室のメールサーバのヘッダ From を指定するよう依頼。

6.2. ML の問題(DKIM 破壊対策)

研究室等で ML(メーリングリスト)を運用して DKIM 署名を壊している例が多数ある。

ML はメールのタイトルに連番を付与して本文にフッタ等を追加するため、学科メールサーバが付与した DKIM 署名が壊れる。DKIM 署名が壊れると、DMARC レポートの<auth_results>の欄で DKIM 署名が付与されているが、失敗していると報告あります。

```
<auth_results>
  <dkim>
    <domain>学科ドメイン</domain>
    <selector>DKIMセレクタ</selector>
    <result>fail</result>
  </dkim>
</auth_results>
```

ML の DKIM 破壊に対応するには、

- ML でメールを一切加工しない。/etc/aliases に直接メールアドレスを記載する ML は加工しないため、DKIM 署名がそのまま使える。

  研究室などでは本対応を行ったところが多かったようだ。

  ※詳細不明だが DKIM 未対応の FML8 系(?)で本文を一切加工しないようにしたら DKIM 署名が未破壊という報告あり。

- (あまり好ましくないが)ML サーバで DKIM 第三者署名を付与。未確認だがおそらく DKIM の検証は成功すると思う。

- DKIM に対応した ML サーバに変更する。mailman2, mailman3 などが対応。

具体的には ヘッダ From を ML のアドレスに書き換える。ヘッダ From を書き換えると、DMARC は ML のアドレスのドメインの設定を参照するようになるため、学科のメールサーバの DMARC は見ない。

※研究室ドメインが学科ドメインのサブドメインの場合は DMARC に sp=none の設定が必要。

※ヘッダ From を書き換えたあと、ML サーバで DKIM 作成者署名を付与すればさらに良い。

※mailman2 はサポート終了しているので注意してほしい。RedHatEL8 系には含まれるが保守は終了している。参考情報: https://access.redhat.com/ja/solutions/6999894

※mailman3 は RPM パッケージ等がなくソースコードからインストールする必要がある。

参考: Google が提供している ML サービス googlegroups では、差出人が gmail の場合は From の書き換えは行わず、gmail の DKIM 作成者署名が付与される。差出人が gmail 以外の場合は From の書き換えが行われ,googlegroups の DKIM 作成者署名が付与される。

7. DMARC 本格導入

12 月末に DMARC をテストモード p=none から実運用の p=quarantine に変更。導入から 3 ヶ月すぎたが特に苦情は来てないので、たぶんうまく動いているのではないかな?

DMARC レポートの解析結果をもとに事前連絡を行ったのは学内のサーバのみ。学外の ML サーバについても問題が起きる可能性のある ML サーバがある可能性があったが、報告は行ってない。学外の場合、ML サーバなのか、SPAM なのか区別が難しい。

そもそも、gmail 等がメールドメイン対策を強化しているため、DKIM が壊れている場合は受信拒否などの影響がでることは周知のはずである。まじめにサービス提供している ML サーバならすでに提供しているはずだ。

なお、学科メールサーバ利用者へ周知の時点で、学外の ML サーバの問題については言及した。送信エラーなどが起きている可能性がある場合は、ML を使っている利用者が各自報告するように依頼。

8. 参考情報

8.1. DMARC レポート解析時の注意点など

受信に成功時の DMARC レポートは、多くの場合、本文がないメールに圧縮した xml を添付ファイルとして送付される。本学に届いた例では以下の MIME で送ってきた。

```
Content-Type: application/gzip
```

→ Microsoft 系、米 Yahoo、その他多数

```
Content-Type: application/zip
```

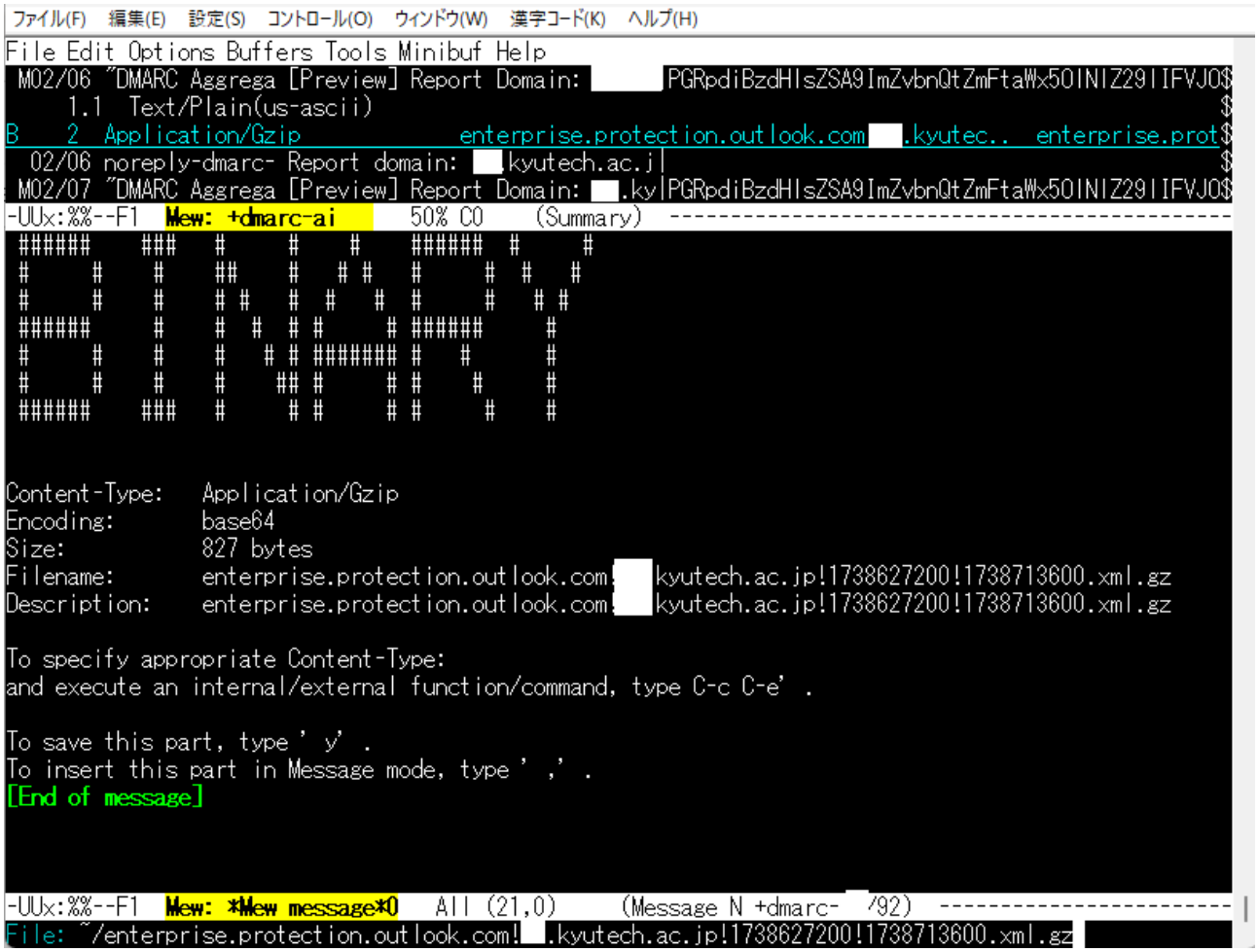
→ Google 系、その他多数

```
Content-Type: application/octet-stream
```

→ ZIP ファイルが添付。trendmicro

→ gzip ファイルが添付。Amazon のクラウドサービス(?)

送られてきた DMARC レポートをファイルに保存する作業は、メールリーダーMew で手作業で保存している。



次に、受信拒否時の DMARC レポート(ruf)はほとんど送られてこないため、定まった形式があるのかよくわからない。(以降明記してない場合の DMARC レポートは受信成功時の DMARC レポート)

次に、DMARC レポートのファイル名は次の形式が多い

「受信メールサーバ!送信メールサーバ!開始日付!終了日付.xml」

上記の形式なのに、同じファイル名の DMARC レポートを複数送ってくるメールサーバがある。多くの場合中身が同じなので、確認面倒なので上書きしている。

DMARC レポートには「report_id」というシリアルぽい文字列が含まれるがコリジョンが頻発する。report_id が同じなのに中身が違うファイルを送ってくるところがある。多くの場合、

- レポートの差出人のメールアドレスが異なる。

  メールのドメインが異なっても、メールのホスティングサービスで同じサービスを用いている場合に report_id のコリジョンが発生する模様。

  `<date_range><email> ... </email></date_range>`

- 日付の範囲が異なるだけで他は中身が同じ。

  おそらくバグっぽい。複数のメールドメインで確認。

  `<date_range><begin> ... </begin><end> ... </end></date_range>`

DMARC レポートの解析には Python の自作ソフトを用いた。Python3 に含まれる XML パーザーで解析エラーになる XML を送ってくるところがある。目視確認しても XML のどの記述の問題かわからないのでファイルを捨てる事にした。EU 圏のフリーメール会社の模様なので、ASCII 範囲外の文字がどこかに入っている可能性がある。

8.2. ARC (Authenticated Received Chain)

ML やメール転送時やのメールドメイン認証として ARC がある。ARC も DKIM 同様に公開鍵・秘密鍵を用いて署名および検証をする。しかし DKIM を壊した状態(dkim=fail)で ARC を付与して各種フリーメールで確認したが、スパムと判断されたり受信拒否されたりする場合が多い。この挙動は ARC の仕様上はどうなっているのか把握してないが、ARC を付与しても DKIM が壊れていたらダメと考えたほうが良い。

検証結果は下記にまとめている。検証したのは 2024 年 9 月。

`https://qiita.com/qiitamatumoto/items/18b171b6bbcfbb346b30`

メールドメイン認証関係で検証した結果

メールドメイン認証 ARC を署名・検証する openarc は中継メールサーバで正常な ARC 署名を付与しても受信メールサーバで ARC 署名の検証に失敗する事が多かった(私の設定作業にミスがなければ)。そのため、rspamd を用いて署名付与・検証の確認をした。検証に失敗する原因はよくわからないが openarc を用いる場合は正常なメールが検証失敗になってないか十分確認して運用してほしい。

9. 終わりに

学内でも質問があったが、学科メールサーバで送信時に DKIM 署名は行っているが、受信時は DKIM 署名の検証は行わず、メールサーバソフトのアンチスパム機能を用いている。学内の研究室メールサーバからは現在でも差出人偽装されたメールは多数届く。

教育的・技術的には悲しい意見だが、今後さらにメールドメイン認証は強化されると予想されるため、メールドメイン認証に未対応のメールサーバを運用するぐらいなら廃止して大学の計算機センター等のメールサービスや外部サービスの利用を考えた方がよいだろう。

再掲になるが、DKIM 署名はヘッダ From の偽装防止技術。現在はスパムにも DKIM 署名が行われているので、アンチスパムとしての機能は半減している。

10.謝辞

本報告書で述べた設定作業は九州工業大学情報工学研究院・情報基盤室の業務として行った。情報基盤室の皆様には大変お世話になりました。