5 送信者認証・課金

京都大学学術情報メディアセンター
中村 素典　motonori@media.kyoto-u.ac.jp

spam メールの増加を助長している原因の 1 つとして送信者詐称（スプーフィング（spoofing），なりすまし）が挙げられる．メールにおける送信者情報はメールのヘッダやエンベロープを介して受け渡され，一般にユーザはこの情報を見て誰からのメールであるかを判断している．したがって，これらの送信者情報が詐称されると，メールを受信したユーザを騙すことが容易になると考えられる．ここでいう送信者詐称とは，送信者を示すこれらのメールアドレスを詐称する行為のことをいう．

このように送信者を詐称できてしまうのは，現在のメールシステムでは送信者情報を正しく設定しなくても指定した宛先にメールが届くからにほかならない．特に spam メールの場合は，メールの本文の内容が相手に届くことが重要かつそれだけで十分であるため送信者詐称が行われやすい．送信者を詐称することにより送信者の追跡を比較的困難にすることができ，ゾンビやウイルスに感染した PC の発見を遅らせ延命させることができる．また，送信先として指定した受信者が存在していなかった場合等に送り返されてくるエラー通知メールも spam メールを送信する spammer やウイルスにとっては不必要なものであり，多量に返送されるエラー通知メールやウイルス検出通知メールの受信を回避する上でも送信者の詐称は効果的である．

架空ドメイン名を用いた送信者詐称の対策は DNS を参照したドメインの存在確認によって可能であるが，これが広く実施されるようになると実際に存在するドメインを用いた詐称の割合が増加することとなった．特に最近登場した phishing と呼ばれる詐欺の手口では，送信者が実際の金融機関等に見えるように詐称できることを利用している．

送信者詐称を防止する機能を現在のメールシステムに追加することができれば，phishing 等の送信者の詐称を利用した悪用が防止でき，有害なメールの送信源の特定が容易になるとともに，送信者情報に基づく spam の確実な受信制御（受信拒否やフィルタリング）が可能になると期待される．

■ 送信者認証としての送信ドメイン認証

送信者を特定し認証するための手段としては，たとえば PGP や S/MIME といった電子署名に基づく個人ベースの認証方式が知られている．しかし，これらの方式はいまだ広く普及しておらず，このような個人ベースの認証手法をここ数年で急速に普及させることは困難である．また，個人ベースで送信者の詐称を防止する別の手法として，チャレンジ・レスポンス（Challenge & Response）方式が知られている．毎回変化するキーワードをいったん返送し，それを含んだメールが再送されてくることで，送信者が実在し，かつ，実際にメールを送る意図があることを確認するものであり，ウイルスや spam の送信者がこのような応答を行わないことを利用している．しかし，この方式は相手に手間をかけることや，メーリングリスト等の受信には適さないといった点で現実的でない．

このようなことから，spam 対策としての送信者認証を急速に推進するためには，個々のユーザに負担をかけない方式を開発しサーバ側で対策を行うことが望ましい．

インターネットにおける SMTP に基づくメールシステムにおいて詐称防止を考慮すべき送信者情報としては，ヘッダに含まれるの送信者アドレスとエンベロープの送信者アドレスがある．メールとしてやりとりされるデータはヘッダとボディから構成され，ヘッダでは主として From: フィールドに送信者情報が記録される．

ヘッダの送信者情報はメールの受信者に誰からのメールであるかを提示する際に用いられるとともに，基本的に返信時の送信先アドレスとしても利用される．一方，エンベロープの送信者アドレスは SMTP を用いた配送処理の際に制御情報として受け渡されるもので，配送エラーが発生した場合の通知先として利用される．SMTP の際にこれらの情報がやりとりされる様子を図 -1 に示す（行頭の C: はクライアント（送信側）からのメッセージ，行頭の S: はサーバ（受信側）からのメッセージを示す）．

```
     (Connection Established)
S:   220 mail.example.edu ESMTP Ready
C:   HELO term.example.com
S:   250 Hello term.example.com
C:   MAIL FROM: <alice@example.com>
     （エンベロープの送信者情報）
S:   250 <alice@example.com> ... OK
C:   RCPT TO: <bob@example.edu>
S:   250 <bob@example.edu> ... OK
C:   DATA
S:   354 Go ahead
C:   Subject: test message
C:   From: alice@example.com
     （ヘッダの送信者情報）
C:   To: bob@example.edu
C:
C:   This is a test message
C:
C:   -- Alice
C:   .
S:   250 Message accepted
C:   QUIT
```

図-1　SMTPの際の送信者情報のやりとりの様子

phishing防止のためにはヘッダの送信者情報を詐称から守ることが有効であり，エラー通知メール等によるDoSアタック現象を根元で防止するためにはエンベロープの送信者情報を詐称から守ることが有効である．

ところで，現在のインターネットにおけるメールシステムはDNSの上に構築されている．メールの受信のためには，自分のドメインに対するMXレコードをDNSに定義し，どのホスト（IPアドレス）がそのドメイン宛のメールの受信に対して責任を持つかを公示する．DNSはドメインごとに権限委譲・分散管理され，その内容はドメインの管理者によって維持される．一般ユーザがDNSの内容を自由に操作することは許されないため，ドメインに関する情報やポリシーを安全に公示するための仕組みとして利用されている☆1．

このDNSによる情報公示の仕組みをメールの送信者認証に応用することができれば，比較的少ないコストで送信者認証が実現できると期待できる．

DNSにおけるMXレコードの定義はメールアドレスのドメイン部（@の右側部分）を単位とする配送先の指示であるが，同様にして送信者アドレスのドメイン部に対する認証を行うための定義をDNSに追加することは比較的容易である．ドメイン部の詐称を防ぐことができれば，ユーザ部の詐称があったとしても当該ドメインの責任において対処させることが技術的に可能であると考えられる．そこで，メールアドレスのドメイン部の詐称防止技術の確立に向けたさまざまな検討が進められている．このようにメールアドレスのドメイン部に対する認証のことをドメイン認証と呼ぶ．

現在検討が進められているドメイン認証技術には，IPアドレスに基づくものと，電子署名に基づくものがある．

IPアドレスに基づくドメイン認証

DNSにおけるMXレコードと同様にしてメールの送信に対して責任を持つホストのIPアドレス情報を提供（ポリシーとして公開）すれば，メールの受信時にDNSで示されているIPアドレスとの一致を確認することによって，そのドメインのポリシーに沿った送信であるかを確認することができる．このような考え方に基づいた方式がIPアドレスに基づくドメイン認証である．

IPアドレスに基づくドメイン認証の方式の統一と規格化に向けての作業はIETF（Internet Engeneering Task Force）のMARID（MTA Authorization Records in DNS）WGにおいて行われた☆2．

WGではIPアドレスに基づくドメイン認証のための方式を2004年中に標準化し，2005年中に実装・評価を進め，2006年中に移行する，という目標の下，Sender-IDと呼ばれる方式の検討が進められた．Sender-IDはSPF（Sender Policy Framework，当初Sender Permitted Fromと呼ばれた）とCaller-IDがベースとなっている．

Sender-IDは次の要素から成り立っている．

- ヘッダの送信者の認証（PRA）
- エンベロープの送信者の認証（MFROM）
- 送信側ドメインのポリシーのDNSへの定義（SPFレコード）

【ヘッダの送信者の認証】

メールのヘッダのうちのFrom:やSender:といったフィールドには送信者のメールアドレスが記載される．さらにヘッダには再送信の際に利用されるResent-From:やResent-Sender:といったフィールドも定義されている．このうち，どのフィールドに含まれる送信者ア

☆1 DNSのセキュリティ上の問題点に対する対策についてはDNSSEC等の導入が検討されており，メールの配送という立場からはDNSのセキュリティ上の問題は考慮する必要はないと考えられる．
☆2 2004年3月に韓国ソウルで行われた第59回IETF会合においてBOFが開催され，その後WGとなった．

ドレスを認証のための情報として利用すべきかを規定するのが PRA（Purported Responsible Address in E-Mail Messages）である[1]．PRA では，これらのヘッダフィールドに対して次に示すような優先順位を設定している（細かな例外は略）．

（1）最初に出現する Resent-Sender:
　（先行する Resent-From: や Received: 等がある場合は無視）
（2）最初に出現する Resent-From:
（3）Sender:（複数存在する場合は無視）
（4）From:（複数存在する場合は無視）

以上の規則に従って条件を満たす最も優先されるフィールドに含まれる送信者アドレスを認証の対象として扱う．メールの中継や転送の際には，PRA に基づいた認証を通過できるように，中継や転送を行うメールサーバに対応するメールアドレスを含むより優先されるフィールドの追加を行う．そうすることにより，正当な中継・転送であることを示すことができる．alice@example.com から bob@example.edu に送られるメールのヘッダを，PRA に基づいて書き換える例を以下に示す．

事例 1　転送（フォワード）の場合

```
From: alice@example.com
To: bob@example.edu
Resent-From: bob@example.edu
Resent-To: bob@example.org
```

事例 2　メーリングリスト

```
From: alice@example.com
To: list@example.edu
Resent-From: owner-list@example.edu
```

事例 3　異なる ISP からの送信

```
From: alice@example.com
To: bob@example.edu
Sender: alice@example.net
```

事例 4　ゲストサービス

```
From: alice@example.com
To: bob@example.edu
Recent-From: guest@example.net
```

ただし，事例 3,4 については，From: に指定したいアドレスを持つ組織のメールサーバが VPN（Virtual Private Network）経由であるいは SMTP AUTH 等による認証つきの MSA（Message Submission Agent）機能を組織外に対して提供し，組織外からのメールの送信は必ずこの MSA を利用するようにできれば必要のないものである（そのためには ISP 側の協力が必要）．

【エンベロープの送信者の認証】

SMTP ではエンベロープで受け渡される送信者アドレスは 1 つだけである☆3．したがってヘッダにおける PRA のような送信者アドレスを選択するアルゴリズムは必要とされない．ただし，エンベロープの送信者アドレスは，エラー通知等の際に NULL（<>）を指定することが許されており，認証のための情報として利用することができない．そのような場合は，SMTP の HELO/EHLO コマンドで渡されるクライアントのホスト名を利用して認証を行う☆4．

ところで，ヘッダの送信者情報の認証の際に考慮したメールの転送等に関する問題は，エンベロープの送信者情報の認証の際にも発生する．通常は転送等の際に送信者アドレスは書き換えられないので認証に失敗することになる．しかし，認証のために書き換えてしまうと本来の送信者アドレスが伝達できなくなり，配送エラーが発生した際にエラー通知の返送先となる情報が失われてしまう☆5．このような場合について，Sender-ID の仕様ではホワイトリスト等を利用したり後述の SPF レコードで表現されるポリシーにアドレスを追加するといった対応を推奨している．

【SPF レコード】

あるドメインが，そのドメインの名前を含むメールアドレスを送信者とするメールについて，どのような IP アドレスを持つメールサーバから送信することを許すか，というポリシーを DNS に定義するための仕様が SPF レコードフォーマットである[2]．

SPF では，DNS における新たなレコードタイプとして SPF RR（Resource Record）を定めているが，現在広く利用されているネームサーバに新たに追加し普及させるには時間がかかるため，当面は TXT レコードを利用することになっている．レコードのデータはテキストで表現され，たとえば次のように記述される．

☆3　エンベロープにおける SUBMITTER オプションによる拡張は PRA に基づく判定を先行して行うためのものである．
☆4　HELO/EHLO で通知されるホスト名のみに基づく提案として Certified Server Validation（CSV）があるが，これは送信者認証を目的とするものではない．
☆5　Sender-ID のベースの 1 つである旧 SPF では，SRS（Sender Rewriting Scheme）と呼ばれる，メールアドレスのローカル部（@ の左側部分）にオリジナルのアドレスを埋め込む手法の利用も想定していた．SPF Classic（後述）では SRS の利用については消極的なようである．

```
spf2.0/mfrom,pra +mx +a:colo.example.com/28
    -all
```

この例では，最初にエンベロープ（mfrom）およびヘッダ（pra）の両方の送信者アドレスに対する認証ポリシーの定義であることが示されている．続けて当該ドメインのMXレコードから得られるIPアドレス，および，colo.example.comに対するIPアドレスに/28のマスクを適用したアドレス範囲からのみ送信され，それ以外からは送信されない（-all）旨が記述されている．“+”や“-”はプリフィックスと呼ばれ，アドレスがマッチした際に受信側に期待する動作を示すものである．プリフィックスには次のようなものがある．

- \+ Pass（認められたアドレス）
- \- Fail（認めていないアドレス）
- ~ SoftFail（Neutralと Failの中間）
- ? Neutral（ポリシーの未定義と同値）

“+”以外のプリフィックスは，DNSに定義したポリシーに反するIPアドレスからメールが送信された場合に受信側に期待する動作を指示するものであるが，Sender-IDの導入初期においては“-”を避け“~”または“?”が利用されることが多い．

なお，先頭のspf2.0は，ベースとなったSPFに基づく記述（v=spf1で始まる）と区別するためのものである☆6．

【Sender-IDとSPF Classic】

Sender-IDの仕様検討の際に，その一部であるPRAに対して，その起源となったCaller-IDを提案していたMicrosoft Corp.が知的所有権（IPR: Intellectual Property Rights）を主張し規格の標準化作業に混乱を招くという事態が発生した．現時点ではこの混乱は収まっているようであるが，その影響としてMARID WGは解散し，Sender-IDの強制力のある“Standard”としてのRFC化は頓挫してしまうこととなった．混乱を避けた仕様として，PRAを利用しない旧SPFを基にしたSPF Classicと呼ばれる方式も検討された[3]．SPF ClassicではPRAを利用しないため，エンベロープの送信者のみの認証となる．

SPF Classicでは，SPF Recordにv=spf1で始まるレコードを定義する．Sender-IDでは，v=spf1で始まるレコードはspf2.0/mfrom,praと読み替えることになっているので，PRAによる認証を避けるためには“spf2.0/pra ?all”といったレコードを併せて登録しておく必要がある．

■ 電子署名を利用した認証

メールの送信側においてドメイン名に対応する公開鍵暗号方式に基づいた鍵を用意し，送信側メールサーバで秘密鍵を用いて署名を行い，受信側メールサーバで公開鍵を用いて署名の検証を行うことで，個々のユーザの環境に依存することなく電子署名を用いた認証を実現することができる．このような電子署名に基づく方式は，間に中継を行うメールサーバが存在したとしても中継するメールサーバが署名の検証を妨げるような改変を行わない限り両端のメールサーバの拡張だけで認証機構が実現できる（すなわちend-to-endの認証方式である）．

電子署名を利用した認証方式としては，Yahoo! Inc.のDomainKeys[4]の実装および試行が先行しているが，Cisco Systems Inc.のIIM（Identified Internet Mail）[5]をDomainKeysと統合しようとする動きもある☆7．

電子署名に基づいて送信者認証を行うためには，メールに含まれる送信者情報に対する署名を行うのは当然であるが，さらに署名されていない部分を改竄したリプレイアタックを防止するため，少なくとも本文や日付情報に対して署名されていることも重要である．

電子署名に関する情報はメールのヘッダあるいは本文のいずれかに添付する必要があるが，DomainKeysではヘッダに含める方式を採用している（図-2のDomainKey-Signature: フィールド）☆8．

図-2のDomainKey-Signature: フィールドには，署名アルゴリズム（a=），鍵のセレクタ（s=），使用された鍵に対応づけられたドメイン名（d=），公開鍵の配布方法（q=），署名対象（h=），署名情報（b=）が含まれている．この例では署名対象はヘッダのFrom:，To:，Date:，Subject:および本文である．セレクタを用いることで1つのドメイン名に対し用意された複数の鍵を選択して利用することが可能となる．DNSを用いた公開鍵の配布の例を図-3に示す．

DomainKeysでは，公開鍵とともに認証を受ける際のそのドメインポリシーもDNSを用いて公示する．図-3の例では，試行中であることを示す“t=y”，当該ドメインからのメールはすべて署名されることを示す

☆6 ちなみに，Caller-IDではポリシーの定義にXMLが用いられていたが，Sender-IDではXMLを用いないシンプルな方式が採用された．
☆7 これらの提案は，2004年8月に開催された第60回IETF会合（米国カリフォルニア州サンディエゴ）でのMASS（Message Authentication Signature Standards）BOFで議論された．その後MASSはWGにはならなかった．
☆8 MIME形式を利用する手法も提案されているが，MIMEに対応していない処理系との親和性が悪い可能性がある．

```
DomainKey-Signature: a=rsa-sha1; s=xyz;
  d=football.example.com; c=simple; q=dns;
  h=from:to:date:subject; b=dzdVyOfAKCdLXd
  JOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVo
  G4ZHRNiYzR;
Received: from dsl4.football.example.com
  by submitserver.football.example.com
  with SUBMISSION;
  Fri, 11 Jul 2003 21:01:54 -0700 (PDT)
From: "Joe SixPack" <joe@football.example.
  com>
To: "Suzie Q" <suzie@shopping.example.net>
Subject: Is dinner ready?
Date: Fri, 11 Jul 2003 21:00:37 -0700 (PDT)
Message-ID: <20030712040037.46341.5F8J@foo
  tball.example.com

Hi.

We lost the game. Are you hungry yet?

Joe.
```

図 -2　DomainKeys で署名されたメールの例

“o=-”，実装上の問題に対するレポートの送り先を示す“r=”を含んでいる．受信側では，メールの受信の際にこのポリシーに基づいて処理を行う．

DomainKeys に限らず電子署名を利用した方法では，メールの配送中におけるヘッダや本文への改変が問題となる．文字コード（charset）や transfer-encoding 等の自動変換は当然として，ヘッダにおけるスペースの数や改行位置，メーリングリストサーバに多く見られる Subject: に対する加工や Received: の削除，さらに本文の先頭や末尾への広告や連絡等の追加といったものが，起こり得る改変として容易に想像される．メールの送信の際に何らかの加工が必要な場合は，すべての加工を施した後に電子署名を付加するようシステムを構成しなければならない．

電子署名を行うための秘密鍵は，通常ドメイン内に設置された送信用メールサーバ（MSA）に保持され電子署名の生成時に利用する．したがって，外出先から当該ドメインのアドレスを送信者としたメールを送信しようとする場合は，秘密鍵を保持しているサーバを MSA として送信することが原則となる．ただし，DomainKeys ではセレクタが指定できるため，必要なユーザに対してのみ別の鍵を用意し，通常の MSA を経由させずにユーザが

```
$ORIGIN example.com.
; セレクタ xyz に対応する公開鍵
xyz._domainkey IN TXT "g=; k=rsa;
  p=MEwwDQYJKoZIhvcNAQEB ... IDAQAB"

; ポリシーの定義
_domainkey IN TXT "t=y; o=-;
  r=reports@example.com;"
```

図 -3　DomainKeys での DNS 定義

自力で署名を付加するような利用方法も可能となっている．

2 つの認証方式の利用方法

IP アドレスに基づく認証方式と電子署名に基づく認証方式にはそれぞれ異なる得失がある．前者はメーリングリストサーバ等でのヘッダや本文の書き換えに強く（PRA で得られるアドレスを維持する限り），後者は転送等に強い（中継のためのメールサーバが介在することによる IP アドレスの変化に強い）．したがって，これらの手法はいずれか一方があれば十分な認証ができるというものではなく，両者を相補的に利用することでより効果的な認証を行うことが可能となると考えられる．

それぞれの認証方式はどちらも，メールの受信を行う際の，そのメールの送信の正当性を検証するためのドメイン名の抽出方法と，そのドメインから公示される送信ポリシーの取得方法，そして，ポリシーに基づく正当性の検証方法を定めている．検証の結果，送信ポリシーに反しているメールの扱いは基本的に受信側に委ねられる．送信者認証技術が普及するまでの移行期間においては，送信ポリシーに反していたからといって，直ちにメールの受信を拒否するのは性急である．検証の結果はユーザが参照できるようにメールのヘッダに付加し，送信ポリシーに反したメールは従来の spam 対策フィルタの適用を行うことが望ましい．一方，送信ポリシーに適合する場合は詐称されていないものとして優先的に受信させる．

ところで，送信者認証はあくまでも送信者の詐称を防止する技術であり，すぐさま spam の撲滅に結びつくものではない．すなわち，送信者アドレスの詐称がなかったとしても，そのメールが spam メールでないという判断はできない．すでに，spammer の一部は，自分の保有するドメインに対して送信ポリシーを正しく定義し，送信者詐称を行わずに spam を送信してきている．しかし，送信者のアドレスが信頼できるものとなれば，個々

のアドレスに基づく処理が容易となる．そこで，spam対策の観点からは，さらに送信されるメールに関してのドメインの品質に対する公的な認定（accreditation）や他の受信者からの評判（reputation）に基づく判定処理が必要となる．すでにDNSBLの類やBonded Sender Program（後述）といったIPアドレスベースのサービスは存在しており，ドメイン認証技術が普及していくことによりドメインベースのサービスも広がっていくことになると期待される．

■ 送信側によるコスト負担モデル

spam対策の別の方法として，送信側にコスト負担をさせる仕組みを導入する方向の検討も行われている．

【電子切手（E-Postage）】

いくつかの方式が提案されているが，基本的には，送信側は銀行等から購入した電子切手を添付したメールを送信し，受信側では添付されている電子切手が有効であったメールについて，通常のブラックリストやフィルタによるチェックを回避させて受信する，といった流れとなる．電子切手は再利用できないが，換金や返金する手段が考慮されているものもある．

【供託金制度】

送信側が供託金を拠出する方式としては，IronPort Systems Inc.によるBonded Sender Program（以下BSP）が有名である．これは金融や行政，その他商取引等の顧客とのメールのやりとりが重要な組織に対して，問題なくメールを送信できるようにするための仕組みで，いわゆるDNSBLのホワイトリスト版である．まず，BSPへの送信側としての参加を希望する組織は，供託金（bond）を拠出し審査を経た後にメールの送信に利用するIPアドレスをSBPが提供するホワイトリストへの登録を受ける．受信側としての参加は無償で，受信側ではメールの受信の際に送信元のIPアドレスをホワイトリストで照合し，登録があればspamでないものとして扱う．そのようなメールの中にspamが含まれていた場合はBSPへ苦情が集まり，苦情の件数に応じて供託金からの引き落としが発生する．さらに状況が悪化するとホワイトリストから削除される．このような枠組みと第三者機関であるTRUSTeによる監査によってホワイトリストの品質が維持される．

【プル型通信モデルの導入】

現在のようなプッシュ型のメール配信システムでは，無差別に送られてきたspamメールの未読時の一時保存のためのコスト（特にストレージ）は受信側が負担しなければならない．これをプル型の配信形態に移行させることで，受信側のストレージに対するコストを削減し，送信側にコスト負担をさせようという考え方である．しかし，プル型に移行することで失われる利便性も少なくないため，安直に移行できるものではない．

■ まとめ

spamの持つさまざまな問題点のうち，送信者の詐称を防止しphishing等による詐欺を技術的に撲滅するには送信者認証技術の確立とその普及が不可欠である．さらに，spam対策のためにはaccreditationやreputationとの連携が重要となる．

送信者認証技術の普及には，送信側ドメインと受信側ドメインの積極的な協力が必要であることは言うまでもないが，ユーザやアプリケーション開発者の協力も重要である．まず，ドメインの送信ポリシーに従うようにユーザはドメインのMSAを介してメールの送信を行う必要がある．そのためにはアプリケーションがSMTP AUTHやTLSといったMSAにアクセスする際に必要となる機構を備える必要がある．さまざまな事情によりMSAが限定できないような場合には，サブドメインごとに異なる送信ポリシーを定義し，ユーザが場所に応じたサブドメインの使い分けを行うことも必要かもしれない．また，メールを受信する立場からは，特に移行期間においては受信拒否は行われず認証結果がヘッダに残されるのみとなるため，アプリケーションがユーザに認証結果を提示する機構を持つことも重要である．

さらに，送信者認証のためにDNSが多用されることになるが，ポリシーの複雑な定義を避け極力DNSの問合せ回数が少なくなるようにするとともにDNSのパケットサイズが512オクテットを超えないようにする配慮も当面は必要であろう．

参考文献
1）Lyon, J.: Purported Responsible Address in E-Mail Messages, Internet-Draft: draft-lyon-senderid-pra-00(2004).
2）Lyon, J., Wong, M. : Sender ID: Authenticating E-Mail, Internet-Draft: draft-lyon-senderid-core-00(2004).
3）Wong, M. and Schlitt, W.: Sender Policy Framework: Authorizing Use of Domains in E-MAIL, Internet-Draft: draft-schlitt-spf-classic-00(2004).
4）Delany, M.: Domain-based Email Authentication Using Public-KeysAdvertised in the DNS (DomainKeys), Internet-Draft: draft-delany-domainkeys-base-02(2005).
5）Fenton, J. and Thomas, M.: Identified Internet Mail, Internet-Draft: draft-fenton-identified-mail-02(2005).

（平成17年6月15日受付）