

宛先アドレスの変更検出による SPF 転送問題解決手法

清家 巧[†] 岡山 聖彦^{††} 河野 圭太^{††} 中村 素典^{†††} 山井 成良^{††}

[†] 岡山大学大学院自然科学研究科 〒700-8530 岡山県岡山市津島中 3-1-1

^{††} 岡山大学総合情報基盤センター 〒700-8530 岡山県岡山市津島中 3-1-1

^{†††} 国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2

E-mail: †seike@dist.cne.okayama-u.ac.jp , ††{okayama,keita,yamai}@cc.okayama-u.ac.jp,
†††motonori@nii.ac.jp

あらまし 近年, 増え続ける spam への技術的対策として SPF と呼ばれる送信ドメイン認証が広まりつつある. しかし, SPF には転送された電子メールを正しく認証が行えない問題がある. そこで本稿では, 宛先アドレスの変更履歴をメールヘッダから検出することで, 転送元サーバに新たな機能を要しない転送への対応手法を提案する. 実験環境において, 提案手法により認証情報を公開しているドメインのメールの約 88.3%, SPF で認証失敗したメールの約 69.5%で認証が成功することを確認した.

キーワード 電子メール, SPF, 送信ドメイン認証, spam

A Solving Method for SPF Forwarded Mail Problem by Tracing Recipient Addresses

Takumi SEIKE[†], Kiyohiko OKAYAMA^{††}, Keita KAWANO^{††},

Motonori NAKAMURA^{†††}, and Nariyoshi YAMAI^{††}

[†] Graduate School of Natural Science and Technology, Okayama University

3-1-1, Tsushima-naka, Okayama-shi, Okayama, 700-8530 Japan

^{††} Information Technology Center, Okayama University

3-1-1, Tsushima-naka, Okayama-shi, Okayama, 700-8530 Japan

^{†††} National Institute of Informatics 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430 Japan

E-mail: †seike@dist.cne.okayama-u.ac.jp , ††{okayama,keita,yamai}@cc.okayama-u.ac.jp,

†††motonori@nii.ac.jp

Abstract Recently, one of sender authentication methods called SPF has been popularized as Anti-spam technology. However, SPF has a problem that the forwarded e-mail could not be authenticated. In this paper, we propose a solving method for SPF forwarded mail problem by tracing changing history of recipient address. According to the experiments, 88.3% of mails were authenticated with in the proposed method, and 69.5% of mails failed by the original SPF were authenticated in the proposed method.

Key words E-mail, SPF, Sender Authentication, spam

1. はじめに

電子メールは WWW と並んでインターネットで最も普及しているサービスの一つである. 一方, 電子メールはセキュリティ的にも問題の多いサービスのひとつでもある. 特に, spam メールは増加の一途を辿っており社会

的にも大きな問題となるなど, 増え続ける spam メールへの対策が一層重要なものとなっている.

spam 対策の一環として, 送信ドメインの詐称を検出可能な技術である送信ドメイン認証が脚光を浴びつつある. 送信ドメイン認証とは, それ自体は正当な電子メールと spam メールの判定を行う技術ではなく, 認証に成

功することによって電子メールと送信元のドメインを結びつける技術である。

送信ドメイン認証の代表的な手法として、SPF(Sender Policy Framework) [1] が挙げられる。SPF は IP アドレスとバウンスアドレス (送信者アドレス) を利用した送信ドメイン認証で、送信側の設定としてドメインがメールの送信に利用する IP アドレスを DNS で公開するだけで送信ドメイン認証が可能となるため、現在最も普及しており、急速に利用できる環境が広がっている。

一方、SPF は転送された電子メールに対して送信ドメイン認証が行えない問題点を持つ。この問題を解決するための手法として、SenderID [2] における PRA(Purported Responsible Address) [3] の利用や SRS(Sender Rewriting Scheme) [4] などの提案がなされている。しかし、これらの提案は転送を行う MTA(メールサーバ) に新たな機能を導入することを前提としている。そのため、多くの MTA が新たな機能を導入しなければこの問題に効果を発揮することは出来ない。

そこで本稿では、宛先アドレスの変更検出による転送問題への解決手法を提案する。提案手法では、メールヘッダから取得できる宛先変更履歴に着目し、現在の宛先アドレスに変更される直前の宛先アドレスを転送を行ったドメインとみなし、送信元 IP アドレスを転送を行ったドメインによって認証することで、最終的な受信メールサーバの対応のみで SPF による認証を行う。これにより、転送が発生したメールに対して送信ドメイン認証が可能となる。

以降、2 章で従来の送信ドメイン認証の問題点をあげ、3 章で提案手法について述べるとともに、安全性の考察を行い、4 章の評価実験の内容とその結果を示し、5 章で総括を行う。

2. SPF と転送メール問題

本章では、通常の SPF の動作と、転送問題に対する従来の解決手法とその問題点を示す。

2.1 SPF

SPF による送信ドメイン認証では、送信側は電子メールの送信元となる IP アドレスやホスト名を DNS の SPF レコード (多くの組織では TXT レコードで代替) として外部に公開する。公開される SPF レコードには、SPF バージョン指定が 1 つと、IP アドレスと限定子の組が 1 つ以上含まれる。限定子とは、IP アドレスに対する認証結果を指定する。SPF での認証結果と SPF レコードで利用される限定子を表 1 に示す。

受信側の SPF による認証結果は表 1 中のいずれかとなる。送信側は公開する SPF レコード中で IP アドレスに対して限定子を用いて認証情報を設定する。

受信側組織での SPF による認証手順を図 1 を用いて説

表 1 SPF の認証結果

認証結果	限定子	意味
pass	+	送信ドメイン認証成功
neutral	?	none と同様に扱う
none		送信ドメインで SPF レコードが未公開
temperror		DNS エラーなどによる認証失敗
permerror		SPF レコードのフォーマットエラー
softfail	~	fail と neutral の中間
fail	-	メールを破棄してもよい

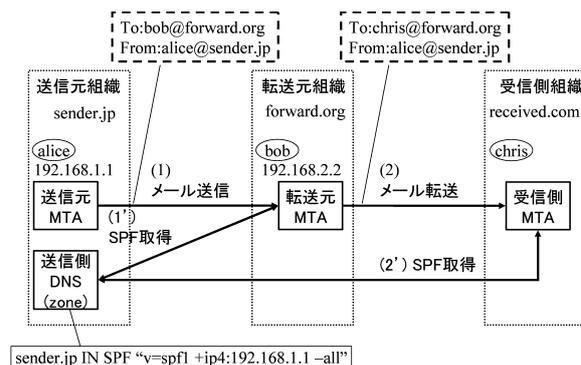


図 1 SPF による送信ドメイン認証手法とその問題点

明する。また、図中の To:と From:はそれぞれ SMTP [5] での宛先とバウンスアドレスを示す。

図 1 中で “forward.org” は以下のような動作を行う。

(1) メールを送信元 IP アドレス “192.168.1.1” を取得
 (1’) From: のドメイン部を基に SPF レコードを取得
 “forward.org” ではこの手順により取得した情報を基に SPF による認証を行う。この場合は送信元 IP アドレスである “192.168.1.1” は “sender.jp” で公開されている SPF レコードの “+ip4:192.168.1.1” と一致し、限定子が “+” であるので認証結果は pass となる。

2.2 SPF における転送問題

本稿における転送の意味を定義する。一般的に電子メールにおいて “転送” とは二つの意味を持つ。一つは、ユーザが電子メールの送受信に利用する MUA から、自身に到着したメールのコピーを他のユーザに送信したいときに利用する転送機能であり、もう一つは、メールサーバにメールが到着した際に、ユーザの操作なしで自動的に設定された他のメールアドレスへ到着したメールを送信する動作を指す。本稿においては、“転送” という用語は後者の意味でのみ使用するものとする。

SPF はこの転送に関して問題を抱えている。これを図 1 の例を用いて説明する。

図 1 で問題になるのは、受信側組織において (2) で IP アドレス “192.168.2.2” と送信ドメイン “sender.jp” を取得し、(2’) で “sender.jp” の SPF レコードを取得して SPF による認証を行うと、送信ドメイン認証は失敗して

しまう点である。これは、転送の際にバウンスアドレスが変更されず“sender.jp”のままであるにもかかわらず、認証に利用する IP アドレスは“forward.org”のものであるために発生する。

2.3 転送問題に対する従来の解決手法とその問題点

SPF における送信ドメイン認証における転送問題の解決手法として複数の手法が提案されている。それらの提案は、転送を行う組織に新しい機能を要求した。

例えば、SenderID で PRA による認証を行うには PRA の決定に利用するメールヘッダを付与する機能の追加、SRS ではバウンスアドレスの書換を行う機能を要求する。

しかし、転送を行う組織への解決手法の導入で SPF の転送問題を解決するには、全ての MTA で解決手法の導入を行う必要があり、SPF の利点である導入の容易さの利点が失われている。

3. 宛先アドレス変更検出による SPF 転送問題の解決手法

本章では送信組織や転送組織では従来の SPF と同様の情報を公開されている状況で、SPF での転送問題を受信組織のみの対応で解決する手法を提案する。

3.1 提案手法の概要

提案手法では、従来の SPF 転送問題解決手法の問題点を踏まえて、電子メールの送信や転送を行う MTA に新規の機能を要求せずに、受信を行う組織の MTA のみの対応で、転送への対応を行うことを目標とする。

この目標を達成するために、現在運用されている多くの MTA では電子メールの送受信時に宛先アドレスをヘッダに付与することに着目した。転送が発生した場合には宛先アドレスが変更されるため、ヘッダに宛先アドレスの変更の痕跡が残る。このときに、転送を行ったユーザは変更される直前の宛先アドレスであると考えられる。この変更される直前の宛先アドレスを SPF による認証に利用することで SPF 転送問題の解決を目指す。これ以降、本稿では現在の宛先アドレスに変更される直前の宛先アドレスを“転送元アドレス”と呼ぶ。

提案手法により抽出される転送元アドレスを図 2 によって例示する。提案手法では図 2 で示すような転送元アドレスを利用して SPF 転送問題の解決を図る。

図 2 において“received.com”の MTA はまず、転送元アドレスである“bob@forward.org”をメールヘッダから抽出する。次にこの転送元アドレスを基に“forward.org”の SPF レコードを取得し、SPF の認証を行うと認証が成功する。転送元アドレスの抽出手法については 3.2 節で詳しく述べる。

3.2 宛先アドレス変更の検出

提案する送信ドメイン認証手法の核となるメールヘッダからの転送元アドレスの抽出手法について述べる。

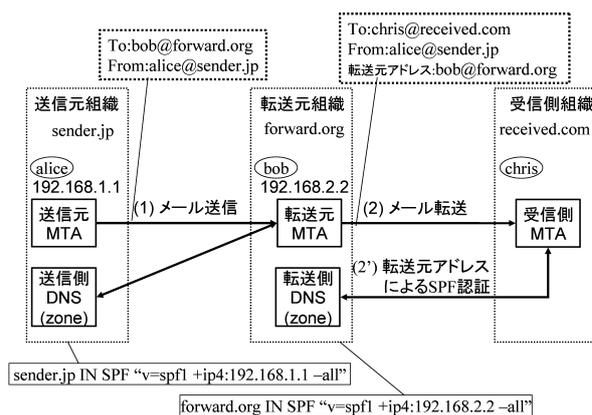


図 2 提案手法の動作

一般的な MTA は、電子メールの受信時またはローカル配送時に宛先アドレスをメールヘッダ内に記述する。最も普及している MTA である sendmail と、postfix や qmail が付与するヘッダについて、図 3 に示す。この

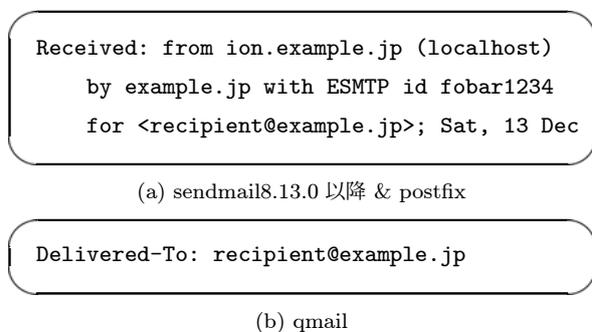


図 3 転送元アドレス抽出に利用するヘッダの例

図は“recipient@example.jp”を宛先としたメールを受信した際に付与されたヘッダのうち、提案手法で利用する部分を抜粋したものである。同図 (a) の“Received”は sendmail や postfix でのメールの受信時に付与され、(b) の“Delivered-To”は qmail や古いバージョンの postfix での配信時に付与される。これらのヘッダは追加される際にメールヘッダの先頭に追加されることが RFC5322 [6] やそれぞれの実装のドキュメントで記述されている。そのため、メールヘッダの先頭から調査し、現在の宛先アドレスとヘッダに含まれる宛先アドレスが異なるときのヘッダのアドレスが転送元アドレスとなる。

宛先アドレスの変更が検出された場合には転送と見なして、提案手法による転送元アドレスを利用した送信ドメイン認証を行う。一方、現在の宛先アドレスと異なるヘッダのアドレスが検出されなければ、転送が行われていないと見なしてバウンスアドレスを利用した通常の SPF による認証を行えばよい。

3.3 提案手法の動作手順

提案手法の動作をフローチャートとして図 4 に示す。

電子メール受信時にこの図に従って電子メールに対して適用する送信ドメイン認証手法の結果を決定する。

図 4 からわかるように、バウンスアドレスによる認証

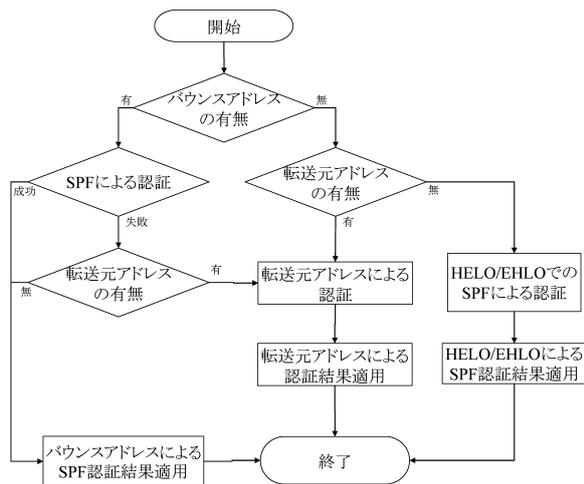


図4 SPFと提案手法を組み合わせた認証結果決定手順

が失敗するかバウンスアドレスが存在しない場合に、転送元アドレスが抽出できれば転送元アドレスによる認証結果を利用する設計となっている。通常のSPFで認証可能な場合や転送元アドレスが抽出できない場合は通常のSPFによる認証結果を利用する。

3.4 提案手法の安全性に関する考察

本節では提案手法の安全性に関する考察を行う。本手法では新たに“転送元アドレス”という概念を用いて送信ドメイン認証を行っているため幾つかの懸念が生じる。それらの懸念とそれに対する考察を以下に記述する。

(1) SPFとの相違点

提案手法を運用する際には、“転送元アドレス”による認証結果は直前の転送組織に対する認証結果であることに注意する必要がある。これはSenderIDにおけるPRAの利用やSRSなどの転送元で対応する手法でも同様であるため提案手法だけの問題ではないが、運用の際に注意を払う必要がある。

(2) 転送元アドレス抽出の失敗

転送元アドレスの抽出に失敗する例として、以下のようなものと考えられる。

(a) 複数の宛先を持つ電子メール

複数の宛先を持つ場合、sendmailなどでは抽出に利用するフィールドが省略されることがある。しかし、転送の際に同時に複数のユーザに転送することは考えにくいいため、問題となることはない。

(b) MTAへの依存

Sendmailのバージョン8.12.11(Release日時2004/01/19)以前では、転送元アドレス抽出に利用するヘッダが付与されない。また、未確認であるが、特殊な設定を施しているMTAやセキュリティ製品などは提案手法で利用する情報を付与しない可能性がある。これは、RFC5322[6]などで転送元アドレス抽出に利用するヘッダを付与することを強制しないためである。

(c) MXレコードの設定への依存

宛先アドレスのドメイン部がDNSのCNAMEレコードによって指定されている場合、転送でない場合にも、ヘッダ上は宛先が変更されたように見えるために提案方式の適用失敗の原因になる。これを避けるには転送元アドレス抽出の際にCNAMEが適用されていないか確認する必要がある。

4. 評価実験

本章では、実際の電子メールに対して提案手法の有効性を確認するために行った性能評価実験の内容とその結果について述べる。

4.1 評価実験環境と実験内容

実験環境は岡山大学総合情報基盤センターで実際に運用しているメールゲートウェイの一部で行った。岡山大学の情報基盤センターで運用されているメールゲートウェイでは学外から学内へのメール全てを受信し、内部の学内MTAへ中継している。図5のccsb1とccsb2が外部のネットワークから直接メールを受け取り、内部のccinets1とccinets2ではウィルス対策ソフトウェアやspam対策ソフトウェアが稼動している。

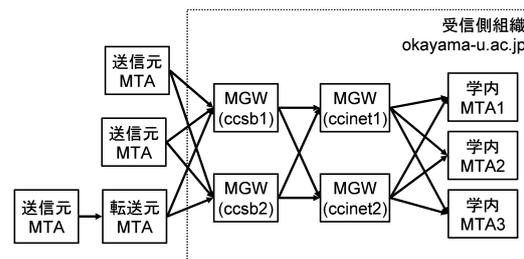


図5 岡山大学の電子メールの配送

本実験では、spam対策ソフトウェアであるSpamAssassinのプラグインとして提案手法とSPFの送信ドメイン認証を実行するプラグインを作成し、図5中のccinets1で動作しているSpamAssassinに導入した。

実験を行ったccinets1では、外部から直接のSMTPのセッション受け入れていない。そのため、今回の実験では直前のccsb1やccsb2で付与されるヘッダから、送信元IPアドレスやバウンスアドレスなど提案手法による認証に必要な情報を取得し検証に利用している。

プラグインではそれぞれの認証結果をサーバのログとメールヘッダに記述する。本実験ではサーバログに出力された結果から以下の情報を取得した。

- 総メール数
- 認証に利用するドメインの有無
 - － バウンスアドレス
 - － 転送元アドレス
- それぞれの認証手法での評価結果
 - － pass 送信ドメイン認証結果が“pass”

表 2 提案手法と SPF の認証成功数

認証手法	認証成功の内訳			合計 認証 成功数
	バウンス アドレス	転送元 アドレス	helo/ehlo	
SPF	230182	-	660	230842
提案手法	230182	6832	641	237655
			対象メール数	2340710

表 3 認証結果内訳
認証結果内訳数 (a)

	認証用 アドレス 無し	SPF により 認証済	送信ドメイン 認証結果			対象メール数
			pass	none	other	
SPF	18734	-	230182	1405114	686680	2340710
提案手法	2064295	230182	6832	36403	2998	

認証結果内訳割合 (b)

	認証用 アドレス 無し	SPF により 認証済み	送信ドメイン 認証結果 (%)			メール 合計 (%)
			pass	none	other	
SPF	0.8	-	9.8	60.0	29.3	100.0
提案手法	88.2	9.8	0.3	1.6	0.1	100.0

- none SPF レコードが未公開で認証結果が “none”
- other “pass” や “none” 以外の認証結果
- SPF での helo/ehlo による認証結果

これらの情報を 2008 年 11 月 30 日午前 4 時から 2009 年 1 月 11 日午前 4 時までの 42 日間分のログから収集し、それぞれの手法の実験環境における認証成功数や認証成功率、それぞれの手法ごとの比較を行う。

4.2 評価実験の結果と考察

本節では評価実験の結果を示し、その結果に対して考察を行う。

提案手法と SPF それぞれの認証成功数とその内訳を表 2 として示す。この表では、提案手法は SPF より成功数が多いものの、転送元アドレスを基に認証された電子メールの数は SPF により認証された電子メールの数に比べると非常に少ない。この原因を次の表 3 で示す。表 3 では、HELO/EHLO の情報を基に認証が成功したメールはすべて認証用アドレス無しに分類し、認証結果を前節で示した pass, none, other で示している。

表 3(b) から転送元アドレスが取得できない場合が 88.2%あることが分かる。この点から、提案手法と SPF の間で大きな違いが発生しない主な原因として転送された電子メールが少ないことが考えられる。

図 4 で示したように、転送元アドレスによる送信ドメイン認証は SPF で認証が成功せず転送元アドレスが取得できるメールに適用される。そのうち、SPF レコード

表 4 認証に利用するメールアドレスと認証結果

利用する アドレス	認証可能 メール数	送信ドメイン認証結果		
		pass	none	other
バウンス	2324046	230182	1405114	686680
転送元	66212	23091	40073	3048
全メール数	2342780			

表 5 認証に利用するメールアドレスと認証成功率 (%)

認証に利用するアドレス	認証成功率 (%)	認証成功率 (none 除く)(%)
バウンスアドレス	9.91	25.11
転送元アドレス	34.87	88.34

が公開されているドメインにのみ “none” 以外の認証結果が得られる。これらの条件を満たすものが 9830 通存在し、全体のうち 0.4%に相当する。この 9830 通中、6832 通 (69.5%) が認証成功となり SPF で認証失敗したものを救済できる。

このように、提案手法は適用できる範囲が転送された電子メールに限定されるために、提案手法によって電子メール全体に対して劇的に認証成功数が増えることは無い。しかし、本稿で対象としている転送された電子メール群に対しては高い認証成功率を示している。以降、転送元アドレスを用いた場合の認証成功率についてまとめた結果を示す。

バウンスアドレスでの認証成功率と転送元アドレスの認証成功率の比較を行う。提案手法と SPF のそれぞれの手法で認証に用いるメールアドレスを取得できた数と、そのアドレスを用いた場合の認証結果について表 4 として示す。この表では、認証に利用するメールアドレスを取得できたメール数を “認証可能メール数” のレコードに示し、その認証結果の内訳を示している。

まず、転送元アドレスで認証可能なメール数がバウンスアドレスよりかなり少なくなっている。これは、先ほどと同様に提案手法が転送されたメールを対象としているためであり、提案手法の有効性の評価には影響しない。

次に、表 4 の結果を元とした認証成功率を表 5 に示す。この表において、“認証成功率” では、送信ドメイン認証が成功したメール (pass) が送信ドメインを取得できたメール群の中でどの程度の割合であるかを示す。また、“認証成功率 (none を除く)” では、SPF レコードを公開していなかったメール (none) を上記の計算から除外した場合を示す。

表 5 より他の認証に利用するアドレスと比較して、転送元アドレスを利用した認証の成功率がバウンスアドレスと比較して非常に高いことが分かる。これは、SPF と異なり転送元アドレスは転送元 MTA が付与した情報であるため、SPF より高い成功率が得られたと考えられる。次に転送元アドレスとバウンスアドレスにより認証し

表 6 SPF と提案手法の比較
(a)SPF と提案手法の認証結果の数

		バウンスアドレス による認証結果			合計
		pass	none	other	
転送元アドレス による 認証結果 (通)	pass	16259	2866	3809	22934
	none	3670	31882	3215	38767
	other	50	1550	1446	3046
合計		19979	36298	8470	64747

(b)SPF と提案手法の認証結果の比率 (none 除外)

		バウンスアドレス による認証率 (%)		合計
		pass	other	
転送元アドレス による認証結果 (%)	pass	75.40	17.66	93.06
	other	0.23	6.71	6.94
合計		75.63	24.37	100.00

た結果を比較した表を示す。この際、比較に使った電子メールは、表 6 では提案手法で利用する転送元アドレスと SPF で利用するバウンスアドレスの両方が取得できたものを抽出したメール群である。多くのメールは、宛先の変更が検出されているため転送されたメールかメーリングリストであると思われる。

手法ごとの比較を行う際に SPF レコードを公開していないドメインのために比較が難しくなるので、表 6(b) ではいずれかで認証結果 “none” が出た場合を表 6(a) から削除して、認証成功率を計算している。

まず、表 6(b) に注目すると一般的に SPF は転送に問題があると言われているが、表 6(b) の認証率によると 75.63% は正しく SPF による認証が行われている。この原因として以下のようなものが考えられる。

- SPF を考慮しているメーリングリスト

投稿用のアドレスに投稿した際に、SPF による認証が成功するバウンスアドレスを設定し、メーリングリストに登録されているユーザへ配信する電子メールが考えられる。この場合、提案手法では投稿用のアドレスから転送されたように見えるため、SPF も提案手法も正しく動作する。また、多数の人に配信されるために多数カウントされる。このような判定が行われるメーリングリストを実際に確認しており、これが主な原因と思われる。

- 認証に適さないドメイン

SPF レコードが公開されるドメインのうち、全ての IP アドレスに対して認証結果 “pass” を許すようなドメインの存在が確認されている。

- 他の解決手法の適用

転送の際にバウンスアドレスの書換により SPF 転送問題に対応する MTA が存在する可能性がある。その場合、転送問題は発生しないが、提案手法でも正しく認証が行える。

これらの原因はプライバシー上の理由により電子メールの宛先や送信ドメイン認証に利用するアドレスの追跡調査が行えないため、全て考察によるものであることを留意する。

表 6(b) では SPF の認証成功率 75.63% に対して、提案手法は 93.06% という非常に高い認証成功率を達成している。また、従来の SPF で送信ドメイン認証が成功しなかった電子メール 5255 通のうち 3809 通 (約 72.48%) で提案手法による送信ドメイン認証が可能であった。

この結果から、提案手法の宛先アドレスの変更が確認されたメール群に対する高い認証成功率を確認し、従来の SPF では認証が正しく行えないメールに対して、提案手法により送信ドメイン認証が高い確率で成功することを確認した。

5. むすび

本稿では、SPF による送信ドメイン認証での転送問題解決の一手法を提案した。

多くの MTA で付与されるメールヘッダを基に宛先アドレスが変更される前のアドレスを転送元アドレスとして送信ドメイン認証に利用することで、転送を行う組織に特別な機能を導入することなく SPF 転送問題の解決を図った。

また、提案手法の有効性の確認を実際に運用されている電子メールシステム上で行い、多くの転送されたと思われる電子メールに対して提案手法が有効に動作することを確認した。

今後の課題としては、ヘッダに含まれた宛先アドレスの履歴を SPF 以外の用途で利用する事や、提案手法と他の spam 対策手法との連携技術の検討が挙げられる。

文 献

- [1] M. Wong, W. Schlitt: “Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1,” RFC4408, April 2006.
- [2] J. Lyon, M. Wong: “Sender ID: Authenticating E-Mail,” RFC 4406, April 2006.
- [3] J. Lyon: “Purported Responsible Address in E-Mail Messages,” RFC 4407, April 2006.
- [4] Shevek: “The Sender Rewriting Scheme,” <http://www.libsrs2.org/srs/srs.pdf>
- [5] J. Klensin: “SIMPLE MAIL TRANSFER PROTOCOL,” RFC 5321, October 2008.
- [6] P. Resnick, Ed.: “Internet Message Format,” RFC 5322, October 2008.