社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38（49）
2007／7／20

部分完全性保証技術 PIAT: 送信ドメイン認証への適用

東角 芳樹† 伊豆 哲也† 武仲 正彦† 吉岡 孝司†

† 株式会社富士通研究所 セキュアコンピューティング研究部
〒 211-8588 神奈川県川崎市中原区上小田中 4-1-1
E-mail: †{yhigashi,izu,takenaka,yoshioka}@labs.fujitsu.com

あらまし 近年, 電子メイルの送信ドメイン認証方式 DKIM (DomainKeys Identified Mail) が注目を集めている. DKIM では, 電子メイルの送信者のドメイン (送信ドメイン) はメイルのヘッダとボディへの署名を生成し, その情報をヘッダに追加する. 受信者はその署名を検証することでドメイン認証を行う. DKIM は PKI を必ずしも必要としないことから導入するための敷居が低く, また既存の内容ベースの SPAM メイル判定に替わる技術としても利用できることから, Yahoo! や Cisco などの主導によって標準化が急速に進められている. しかし電子メイルの送信の途中でヘッダが書き換えられる場合, 受信者による検証は失敗するという問題が知られており, DKIM をメイリングリストへ適用する場合には格段の注意が必要となる. 実際, 標準化においてもメイリングリストへの適用は詳細に検討されており, メイリングリストのドメインも署名を追加することが推奨されている. 本稿は吉岡・武仲によって提案された部分完全性保証技術 PIAT の DKIM への適用について検討・提案を行う. PIAT を用いることで, 特にメイリングリストのドメインが署名を追加しない場合でも, 受信者による送信者のドメイン認証が可能となる.

キーワード 電子メイル, 送信ドメイン認証, SPAM, DKIM, 部分完全性保証技術, PIAT

Partial Integrity Assurance Technology PIAT: An Application to Sender Domain Authentication

Yoshiki HIGASHIKADO†, Tetsuya IZU†, Masahiko TAKENAKA†, and Takashi YOSHIOKA†

† FUJITSU LABORATORIES Ltd.,
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, 211-8588, Japan
E-mail: †{yhigashi,izu,takenaka,yoshioka}@labs.fujitsu.com

Abstract Recently, the sender domain authentication protocol DKIM (DomainKeys Identified Mail) attracts much attention, in which the sender domain adds a signature header generated from headers and body of the original email, and the sender domain authentication is achieved by a verification of the signature. Since DKIM does not require PKI, and it can be used as a SPAM protection different from previous content-based methods, DKIM is actively being standarized by Yahoo! and Cisco. However, it is pointed out that a verification will fail when headers are chaged before it is reached to the receiver, and carefull treatments are reuiqred when DKIM is applied to mailing-lists. In fact, it is strongly recommended in the standarization that a mailing-list domain should add the signature to the revised email. This article proposes to combine DKIM and PIAT, the partial integrity assurance technology proposed by Yoshioka and Takenaka, so that the original sender domain authentication will be successfull even when headers are changed by a mailing-list domain but a signature is not generated to the revised email.

Key words E-document, sender domain authentication, SPAM, DKIM, partial integrity assurance technology, PIAT

1. はじめに

インターネット時代を迎え，電子メイルは新しい社会基盤 (インフラ) となっている．電子メイルの普及の背景として，送受信コストが既存手段よりも圧倒的に安価であることが挙げられるが，同時に，メイルの大量配信 (SPAM メイル) が社会問題にもなっている．従来の多くの SPAM メイル判定はメイル内容の意味解析を利用しているが，判定の手間が大きいこと，また誤判定が除去できないことから，新しい判定方式が望まれている．

大半の SPAM メイルは未知の送信者から送信されていることから，新しい判定基準として送信者の身分証明 (IP アドレスや送信ドメイン) を用いる方式が有力視されている．例えば SIDF (Sender ID Framework) は Microsoft によって提案された IP アドレスベースの認証技術であるが [5]，同社の特許出願によって実装が遅れたことや，転送メイルを正しく認証できないケースがあることなどから，広く普及するには至っていない．他方で DKIM (DomainKeys Identified Mail) は送信ドメインベースの認証方式であり [1]，Yahoo! などが提案していた DomainKeys と Cisco などが提案していた Internet Identified Mail (IIM) を統合した技術である (ただし実質的には DKIM は DomainKeys に類似している)．DKIM では，電子メイルの送信者のドメイン (送信ドメイン) はメイルのヘッダとボディへの署名を生成し，その情報を `DKIM-Signature:` ヘッダとして追加する．受信者はその署名を検証することでドメイン認証を行う(注1)．このとき送信者の公開鍵は送信ドメインの DNS サーバから取得するため，PKI に比べて導入するための敷居が低いことが知られている．このため，Yahoo!, Cisco, Sendmail, PGP の主導によって，標準化 (RFC 化) が急速に進められている(注2)．

しかし，電子メイルの送信の途中でヘッダが書き換えられる場合，DKIM の検証は失敗するという性質が知られている．特にメイリングリストは `Subject:` ヘッダを書き換える (例えばメイリングリストの名称とナンバリングを `Subject:` ヘッダに挿入する) ことが多いため，DKIM をメイリングリストへ適用するには格段の注意が必要となる．実際，標準化においてもメイリングリストの適用は詳細に検討されており，例えばメイリングリストのドメインにおいて送信ドメインの認証を行い，認証に成功した場合に，メイリングリストに関する新しいヘッダを追加した上で署名を生成し，再度 `DKIM-Signature:` ヘッダを追加することを推奨している．

このように DKIM は参加ユーザが署名を生成・検証するという理想的な状況では能力を発揮するが，逆に，一部の参加ユーザが署名を生成・検証しない場合，十分な能力を発揮することができない．例えば DKIM をメイリングリストへ適用する場合，電子メイルの送信ドメインが署名を生成するか否か，メイリングリストのドメイン (ML ドメイン) が署名を生成するか否かが問題となるここで状況を表 1 のように分類した場合，(A) のように送信ドメインも ML ドメインも署名を生成する場合は問題ない．また (B) や (D) のように送信ドメインがそもそも署名を生成しない場合には，このようなメイルは受信を拒否するという意味で問題が生じない．しかし (C) のように送信ドメインが署名を生成するのに，ML ドメインが署名を生成せずにヘッダを書き換える場合は議論の余地がある．この場合，ヘッダの書き換えによって送信ドメインの署名検証には失敗することになるが，DKIM の推奨する状況ではないことから仕方ないと考えることもできる．しかしそのメイルを受信者がメイリングリストを介さずに受信すれば正しく受信されるのだから，DKIM の想定外だからといって除外するのは，ペナルティとして重すぎると考える方が自然であろう．特に DKIM があまり使用されていない現状から，参加ユーザがすべて DKIM を使用する利用的な状況に移行していく間には，(C) のような状況は十分に起こりえる．従って，ヘッダのオリジナル内容と，書き換え後の内容への変更を保証する技術を確立することは，DKIM の普及を促進させるためにも必須である(注3)．

		送信ドメイン	
		署名する	署名しない
メイリングリスト ドメイン	署名する	(A)	(B)
	署名しない	(C)	(D)

表 1　送信ドメインとメイリングリストドメインの署名の有無

本稿は吉岡・武仲によって提案された部分完全性保証技術 PIAT [6] の DKIM への適用について検討・提案を行う．PIAT は，部分文書に分割された文書の内容が変更された場合に，変更前後の内容 (あるいは変更前からの差分) に対する署名を生成・保持することで，変更前の内容の正当性，変更後の内容の正当性，変更者などを保証する技術である(注4)．提案方式では，`Subject:` ヘッダのように書き換えられる可能性のあるヘッダのオリジナルの内容と署名をヘッダとして保持することで，ML ドメインが署名を生成しない場合でも，受信者によるオリジナルヘッダの検証を可能とする．

2. DKIM

本節では，送信ドメイン認証方式 DKIM (DomainKeys Identified Mail) [1] の処理概要を簡単に説明する．

2.1 DKIM の処理概要

電子メイルの送信者のドメイン (送信ドメイン) は，DKIM の検証で用いる公開鍵を自らの DNS サーバにあらかじめ公開しておく．

電子メイルが送信される場合，送信ドメインは送信メイルのボディとヘッダに対する署名を生成し，送信メイルに

(注1)：さらには，IIM のような送信者単位の認証も可能である．

(注2)：2007 年 5 月に DKIM 規格は RFC 4871 として承認され，現在は Proposed Standard のフェーズにある．

(注3)：DKIM では署名対象ヘッダを任意に選択することが可能であるため，メイリングリストが書き換えるヘッダが事前に明らかである場合には，そのヘッダを署名対象ヘッダから除外することで，書き換えによる署名の無効化を防ぐこともできる．しかしその場合，除外されたヘッダの内容への保証は失われてしまう．

(注4)：部分文書の秘匿を目的とした PIAT 署名 [4] は，PIAT を墨塗り署名として実現させた場合に相当する．

```
DKIM-Signature: v=1; a=rsa-sha256; s=brisbane;
  d=example.com; c=simple/simple; q=dns/txt;
  i=joe@football.example.com;
  h=Received: From: To: Subject: Date: Message-ID;
  bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
  b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4y
    AUoqOB4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+Na
    hM6L/LbvaHutKVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDN
    H6mZckBdrIx0orEtZV4bmp/YzhwvcubU4=;
```

図 1 DKIM-Signature: ヘッダの例

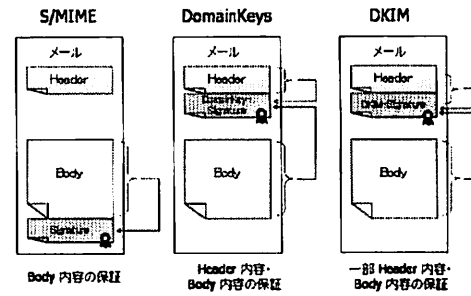

図 2 S/MIME, DomainKeys, DKIM の比較

DKIM-Signature: ヘッダを追加した上で送信する. ここで DKIM-Signature: ヘッダは (";" をセパレータとして) "タグ=値" を列挙した構造となっており, 生成された署名も署名タグ (b=) の値として DKIM-Signature: ヘッダ内に保持される. なお, DKIM の署名アルゴリズムには RSA 署名 (RSASSA-PKCS1-v1_5 RSA) が使用されており [2], ハッシュ関数として SHA-256 (デフォルト) または SHA-1 が選択可能となっている.

DKIM-Signature: ヘッダを持つメイルを受信した受信ドメインは, (必要ならば) 指定された送信ドメインから公開鍵を取得し, DKIM-Signature: ヘッダ内の署名を検証する. 署名検証の結果は Authentication-Results: ヘッダとして追加され, 最終的にそのメイルを受信するか否かは受信者の判断に委ねられる.

DKIM-Signature: ヘッダの例として, DKIM の仕様書 [1] で紹介されている例を図 1 に示す [1]. ここで h は署名対象ヘッダを, b は署名を表すタグである (これ以外のタグの説明は省略する). このように DKIM では署名対象ヘッダを選択することが可能であるが, From: ヘッダは必ず指定されなければならないとされている.

2.2 DomainKeys との比較

DomainKeys は DKIM のベースとなった技術であるため, 両者の共通点は多い. 主な違いは, 署名対象ヘッダの選択が DomainKeys では任意だったのに対し (このため DomainKeys の署名対象ヘッダは, デフォルトである全ヘッダであることが多かった) DKIM では必須となっている点と, DKIM では送信者の認証が可能になっている点である. このように DomainKeys と DKIM は目的を同じにした類似技術であるものの, 異なる規格として扱われており, 併用が可能であるように設計されている.

2.3 S/MIME との比較

DKIM の目的は送信ドメインの認証であるのに対し, S/MIME [3] における署名の目的はボディの内容保証である. このように両者は異なる目的を持った技術であり, 併用も可能である.

S/MIME, DomainKeys, DKIM のイメージを図 2 に示す.

3. PIAT の DKIM への適用

本節では DKIM をメイリングリストに適用する際に生じる問題点を述べるとともに, 部分完全性保証技術 PIAT を用いた解決方法を提案する.

3.1 DKIM の問題点

DKIM の署名はオリジナルメイルのヘッダとボディから生成されているため, 電子メイルの送信の途中でヘッダが書き換えられる場合, DKIM は検証に失敗する. 特にメイリングリストは Subject: ヘッダを書き換える (例えばメイリングリストの名称とナンバリングを Subject: ヘッダに追加する) ことが多いため, DKIM をメイリングリストへ適用するには格段の注意が必要となる. 以下では簡単のため, メイリングリストサーバは電子メイルの受信ドメイン・送信ドメインとしての機能を持っており, 受信したメイルの Subject: ヘッダのみを書き換えて登録メンバに配信する場合を考える.

DKIM をメイリングリストに適用する場合に生じるこのような問題は標準化においても十分に意識されており, 次のような解決先が推奨されている: メイリングリストのドメイン (ML ドメイン) はまず受信メイルの DKIM 認証を行う. 送信ドメインが署名を付与していなかったり (つまり受信メイルに DKIM-Signature: ヘッダが付与されていなかったり), DKIM 認証に失敗する場合には, その受信メイルを破棄する. DKIM 認証に成功した場合には, メイリングリストに関する新しいヘッダを追加した上で署名を生成し, 再度 DKIM-Signature: ヘッダを追加・配信する.

このように参加ユーザ (送信ドメイン, ML ドメイン) が署名を生成・検証するという理想的な状況では, DKIM をメイリングリストに適用しても問題は生じない. しかし, DKIM があまり使用されていない現状から, 参加ユーザが DKIM を使用する理想的な状況へ移行していく間には, 一部のユーザが署名を生成・検証しない場合も許容すべきである. このとき, DKIM を使用していないユーザよりも使用しているユーザがまず保護されるべきであろうから, 送信ドメインが署名を生成するのに, ML ドメインが署名を生成せずにヘッダを書き換える場合を許容することが望ましい. このように, ヘッダのオリジナル内容と, 書き換え後の内容への変更を保証する技術を確立することは, DKIM の普及を促進させるためにも必須であると考える.

3.2 PIAT の DKIM への適用

前節で述べた問題に対し, 本節では部分完全性保証技術 PIAT を用いた解決方法を提案する.

吉岡・武仲によって提案された部分完全性保証技術 PIAT

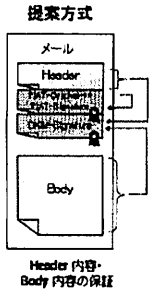

図 3 提案方式の概要

(Partial Integrity Assuarance Technology) は, 文書内容が変更されながら運用されていく場面において, 変更前後の内容の正当性や, 変更者を保証する技術である [6]. 部分文書という構成単位に分割された文書に対し, PIAT は各部分文書のハッシュ値を求め, それらハッシュ値の連接に対する署名をオリジナル署名として生成する. 文書の内容が変更された場合, 変更者は各文書のハッシュ値と, それらハッシュ値の連接に対する署名を変更後の署名として生成する. 検証者は 2 つの署名の検証によって 2 つのハッシュ値の連接の正当性を確認するとともに, 2 つのハッシュ値の連接を比較することで, どの部分文書が変更されたかを知ることができる (さらにはその部分文書が誰によって変更されたかも知ることができる).

提案方式では, 送信ドメインは `DKIM-Signature:` ヘッダを付与した上で, DKIM とは別個に選択されたヘッダに対する署名を生成し, `PIAT-Signature:` ヘッダ内に保持する. ここで選択されるヘッダは送信の途中で書き換えられるものとする. また選択されたヘッダの内容は `PIAT-Original-**:` ヘッダとして保管される. 例えば PIAT によって `Subject:` ヘッダが選択された場合, このヘッダに対する署名が生成された上で, その内容が `PIAT-Original-Subject:` ヘッダとして保管される. そして受信ドメインにおいて, `PIAT-Original-**:` ヘッダは `PIAT-Signature:` ヘッダによって検証されることになる.

`PIAT-Signature:` ヘッダは, オリジナルのヘッダ内容に対する正当性を保証している. 特に ML ドメインが署名を DKIM をサポートしない場合, つまり署名を生成せずに `Subject:` ヘッダを書き換える場合, このとき受信ドメインによる `DKIM-Signature:` の検証が失敗するのに対し, しかし `PIAT-Signature:` ヘッダによる `PIAT-Original-Subject:` ヘッダの検証を通じて, 送信者ドメインから送信された時点での `Subject:` ヘッダの正当性を確認することが可能となる.

なお上記の説明では, 簡単のため, `PIAT-Signature:` はヘッダだけを対象としたが, (メイルのボディは書き換えられないという仮定のもとで) メイルのボディの検証が必要な場合には, 署名生成対象に含めることも可能である. メイリングリストによっては ML ドメインが `Subject:` ヘッダ以外のヘッダを書き換えることも考えられるが, 同様に PIAT を拡張することも可能である (この場合, 署名データは複数でも良いし, 1 つに集約させることも可能である).

4. ま と め

部分完全性保証技術 PIAT の DKIM への適用方式を提案した. 提案方式を用いると, メイリングリストのドメインが署名を生成しない場合でも, 送信ドメインが PIAT 署名を生成することによって, 変更前のヘッダ内容の正当性を保証することが可能となる.

本稿では電子メイルのボディは書き換えられない場合を想定したが, メイリングリストでは (広告の挿入などによって) ボディが書き換えられる場合もあるため, 提案方式のさらなる拡張は課題である. また, 本稿では DKIM の補完技術として PIAT の適用を考察したが, PIAT だけを用いた送信ドメイン認証も可能である. 特に複数のメイリングリストへのメイル送信が必要な場合, 各メイリングリストが書き換えるヘッダは一般には異なっている. `DKIM-Signature:` の生成時にヘッダを選択することで, このような状況に理論的には対処することができるが, 実用的には対処が厳しいことも考えられる. このような場合, 各ヘッダに対する PIAT による署名を付与することで, さまざまなメイリングリストに柔軟に対応することが可能である. しかし具体的なアルゴリズムの詳細については, 別稿にて報告の予定である.

文 献

[1] IETF, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007. `http://www.ietf.org/rfc/rfc4871.txt`

[2] IETF, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003. `http://www.ietf.org/rfc/rfc3447.txt`

[3] IETF, "S/MIME Version 3 Message Specification", RFC 2633, June 1999. `http://www.ietf.org/rfc/rfc2633.txt`

[4] T. Izu, N. Kanaya, M. Takenaka and T. Yoshioka, "PIATS: A Partially Sanitizable Signature Scheme", *ICICS 2005*, LNCS 3783, pp.72-83, Springer, 2005.

[5] Microsoft. "Sender ID Frame work". `http://www.microsoft.com/japan/mscorp/safety/technologies/senderid/default.mspx`

[6] 吉岡 孝司, 武仲 正彦, "電子文書の訂正・流通を考慮した部分完全性保証技術の提案", 第 3 回情報科学技術フォーラム (*FIT 2004*), M-066, 2004 年 9 月.