Vol.2015-IOT-28 No.2
2015/3/5

POPプロクシを用いたDKIM検証システムの実装

福山 雅深[1,a)]　大岩 美春[1,b)]　山井 成良[1,c)]　北川 直哉[1,d)]

概要：近年，金融機関や政府，地方行政団体等に詐称したメールを送信して，不正に金銭を窃取する事例が多く発生しており，メールの差出人や内容の信憑性を確保することが求められている．DKIM は送信ドメイン認証技術の一つであり，送信側が付加した電子署名をメール受信時に検証し，送信されたメールが正当な送信者から改竄なく配送されたかを判断することができる．しかし，DKIM 検証機構は，特に受信サーバ側ではそれほど普及していない．本論文では，通常メールサービス提供者の受信サーバで行う検証処理を，メールサービス利用者が設置した POP プロクシを用いて検証し，その結果を各ユーザに通知するシステムについて報告する．

キーワード：DKIM，送信ドメイン認証，電子メール，POP プロクシ

Implementation of DKIM Verification System Using POP Proxy

Masami Fukuyama[1,a)]　Miharu Oiwa[1,b)]　Nariyoshi Yamai[1,c)]　Naoya Kitagawa[1,d)]

Abstract: Recent years, many attackers send many emails spoofed as those sent from a bank or a government etc., and are getting money by fraud. DKIM is one of the sender domain authentication method, it can be determined whether the sent email is delivered without alteration from a legitimate sender by verifying the electronic signature at the receiving time. However, DKIM verification mechanism is not prevalent especially in the receiving server. In this paper, we propose a system that verifies the DKIM signature by a POP proxy in place of a receiving server and notifies the result to each user.

Keywords: DKIM, Sender Domain Authentication, E-mail, POP Proxy

1. はじめに

近年，個人の PC，タブレット端末，スマートフォン等の端末から簡単に様々な金融取引を行うことができるインターネットバンキングやオンライントレード等のサービスを世界中の多くの金融機関が扱っており，多くの人々に利用されている．

インターネットバンキング等のサービスでは，振込等の取引が行われた際や，サービスメンテナンス情報などをユーザに通知する際に電子メールを使用することが多い．この仕組みを利用して，悪意を持った者が，金融機関になりすましたメールを送り，本物の金融機関のサイトに酷似した偽のページに誘導したうえで，利用者のインターネットバンキングのアカウント情報（ID，パスワード）を盗むという犯罪がここ数年で急増している．従来，取引や業務に関する通知は，通帳，店舗での張り紙，郵送で行われてきたが，これらの通知をメールで受信する場合には，そのメールの送信元が正当な相手からなのかを確認できる仕組みが求められている．

本論文では，メールの送信元の認証の仕組みである送信ドメイン認証のうち，DKIM について，POP プロクシを用いた検証方法の提案と，その有効性を報告することを目的とする．

[1] 東京農工大学
Tokyo University of Agriculture and Technology, Koganei, Tokyo 184–8588, Japan
[a)] 50012268052@st.tuat.ac.jp
[b)] 50012268006@st.tuat.ac.jp
[c)] nyamai@cc.tuat.ac.jp
[d)] nakit@cc.tuat.ac.jp

2. なりすましメールの問題点

電子メールのうち，送信者名，送信者アドレス，件名，本文を偽装して送信されるメールをなりすましメールと呼ぶ．なりすましメールは，金融機関や各種オンラインサービス等を装い，フィッシング詐欺を狙った spam メールの配信に使用される．

近年では，送信者アドレスや送信者名を実在する金融機関等を装い，メール受信者が実際の組織からのメールであると誤って判断をするように，件名や本文が巧妙に作られたなりすましメールが送信されている．このようなメールには本文に URL が記載されており，URL を開くと，本物の金融機関のサイトによく似せた偽のページ（フィッシングサイト）が表示され，インターネットバンキングの ID やパスワードの入力が求められ，これに入力した ID やパスワードは攻撃者に送信される．攻撃者は，このようにして不正に取得した情報を使用し，被害者の銀行口座から不正に送金や出金を行う．

警察庁の発表 [1] によると，なりすましメールが関係するものも含め，インターネットバンキングでの不正送金の金銭的被害は，2013 年ごろより急増しており，被害総額は年間 14 億円を超えている (表 **1**).

電子メールの配送に関するプロトコルである SMTP では，メールの From:ヘッダで示される送信者アドレスと，SMTP セッション時の MAIL FROM:コマンドの引数で示されるアドレスが一致しなければならないという規則はない [2]．このため，送信者のメールアドレスの詐称を防ぐことは困難であり，なりすましメールが大量に流通する原因となっている．

このように，なりすましメールによる被害が多く発生していることから，何らかの対策が必要である．しかし，なりすましメールの本文やリンク先のフィッシングサイトは巧妙化しており，ユーザが判断するのは難しい．そのため，なりすましメールの流通を抑制したり，ユーザに配信された場合でも，なりすましメールであることに気づかせる対策技術は重要である．

3. 送信ドメイン認証

3.1 概要

なりすましメールを検出するための仕組みとして，送信ドメイン認証が提案されている．送信ドメイン認証は，メール送信者がドメイン名を詐称していた場合に，これを検出するものである．メール送信側はあらかじめ検証に用いるための情報を公開しておき，受信者側ではメール受信時にその情報を使用して，送信されたメールの正当性を検証を行う．

表 **1** 近年のインターネットバンキングの被害

年	被害件数（件）	被害額（億円）
2013	1315	14.06
2012	64	0.48
2011	165	3.08

3.2 SPF と SenderID の仕組み

SPF（Sender Policy Framework）は，最も広く利用されている送信ドメイン認証方式である．日本国内においては，大手プロバイダーを経由する受信メール全体のうち，90%程度が SPF による認証が可能となっている [3].

SPF では，認証を次のように行う [4]．送信側ではあらかじめ，自ドメインの権威 DNS サーバの TXT レコードに，SPF レコードを記述し，公開する．SPF レコードには，そのドメインのメールアドレスを使って送信する可能性のある MTA の IP アドレスを宣言する．例えば，example.com の DNS サーバの SPF レコードに

v=spf1 +ip4:192.0.2.0/24 -all

と記述すると，送信者アドレスのドメイン名が example.com のメールで，IP アドレスが 192.0.2.0/24 に含まれる IP アドレスの MTA から配送されていれば，そのメールは送信ドメインのなりすましをしていないという宣言となる．

受信側では，SMTP 通信の接続元 IP アドレスとエンベロープ From に記述されているドメインを基に認証を行う．エンベロープ From のドメイン名の DNS サーバにアクセスし，SPF レコードを取得する．接続元の IP アドレスが，SPF レコードに記述されているものであれば，なりすましメールではないと判断される．

このように，SPF は送信ドメインを詐称したメールの検出に有力な技術であるが，メールヘッダを書き換えずに別のサーバへ転送されたメールは，正当なメールであっても認証に失敗する問題を抱えている．メールの転送が行われると，エンベロープ From のドメイン名は変わらないが，受信ホストとの SMTP 通信時の接続元 IP アドレスは別のサーバのものとなる．従って，送信者のドメイン名と SMTP 接続元の IP アドレスの組み合わせが，SPF レコードで宣言されているものと異なり，認証に失敗してしまう．

SenderID は，SPF から派生した方式で，基本的な仕組みは SPF と同じである．SPF がエンベロープ From のドメインを認証の対象とするのに対し，Sender ID ではヘッダ内の複数の情報から PRA（Purported Responsible Address）と呼ばれるアドレスを決定し，それを認証の対象とする [5].

3.3 DKIM の仕組み

DKIM（Domainkeys Identified Mail）は，電子署名方式の送信ドメイン認証である [6]．DKIM による送信ドメイン認証は以下に示すように行う（図 **1**）.

(1) 送信側では，あらかじめ公開鍵と秘密鍵を用意し，自

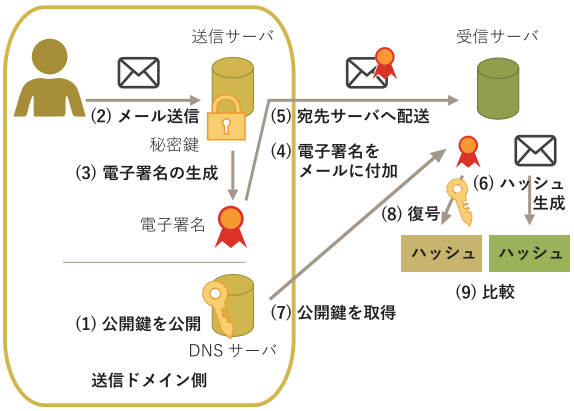

図 1　DKIM による送信ドメイン認証の流れ

ドメインの権威 DNS サーバの TXT レコードに公開鍵を公開する．

(2) ユーザがメールを送信すると，署名なしのメールが送信メールサーバに配送される．

(3) 送信メールサーバは，メールのヘッダと本文からハッシュを作成し、ハッシュに対して秘密鍵で電子署名を生成する．

(4) 生成した電子署名データや，署名対象のヘッダ，署名のアルゴリズム，本文のハッシュ値などの情報をセミコロン区切りの文字列にし，メールヘッダの “DKIM-Signature” ヘッダに付加する．

(5) 電子署名つきのメールを宛先メールサーバに配送する．

(6) 受信サーバでは，受信したメールのヘッダと本文からハッシュを作成する．

(7) また，受信したメールの “DKIM-Signature” ヘッダに指定されている権威 DNS サーバから公開鍵を取得し，電子署名からハッシュを取り出す．

(8) 受信したメールのハッシュと電子署名から取り出したハッシュを比較して一致すれば，認証成功とする．

また，DKIM は電子署名を用いた方式であるため，認証が成功すれば，配送途中でのメールの改竄が行われていないことの確認にもなる．SPF では正しく認証できない転送メールについても，電子署名方式の DKIM では正しく認証することができる．

3.4　DKIM の現状と問題点

一方で，DKIM に対応したメールサーバや MUA が少ないという問題点が挙げられる．例えば，日本国内においては，大手プロバイダーを経由する受信メールのうち，総量の 40%程度しか DKIM の認証ができていない [7]．ドメイン数で見ても同じ傾向が見られ，送信側として DKIM 認証に対応していると考えられるドメインの数は，”.jp” ドメインでは全体の 0.5%程度である [8][*1]．送信ドメイン認証は，その恩恵を受けるためには，送信側または受信側のどちらかではなく，両方で対応する必要がある．このような理由から，DKIM は今後より広く普及していくことが求められる．

[*1] この調査では，”.jp” ドメインの権威 DNS サーバアクセスし，DKIM，DomainKeys のポリシの有無で判定している

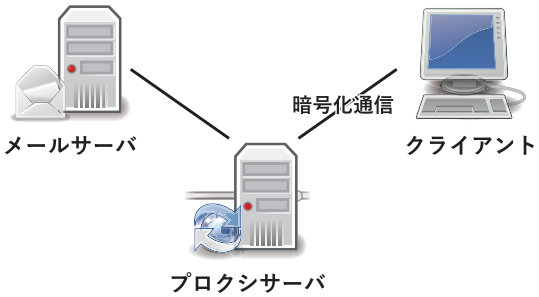

図 2　POP プロクシを介した通信経路

表 2　メールの受信環境の例

項目	メールサーバ
サーバ名	pop.example.jp
プロトコル	POP/SSL
アカウント名	Taro
パスワード	abc123

表 3　プロクシ利用時の MUA の設定

項目	設定値
サーバ名	myproxy
プロトコル	POP/SSL
アカウント名	Taro%pop.example.jp
パスワード	abc123

4.　DKIM 検証システム

4.1　システムの概要

本節では，利用する受信メールサーバが DKIM 認証に対応していない場合でも，検証に対応できるシステムについて述べる．また，DKIM 検証の結果を利用者に通知する方法を提案する．

通常，メールクライアントは，メールサーバから直接メールを受信するが，本システムでは　POP プロクシサーバを経由させて受信するため，メール受信時の通信経路は図 **2** のようになる．

クライアントの MUA では，メールサーバから直接受信する場合には表 **2** に示すように設定するが，本システムを利用し，プロクシサーバを経由して受信する際には表 **3** のように設定する．プロクシサーバがメールサーバに接続するときの通信方式は，平文，暗号化通信の両方に対応しているが，ポートの指定がない場合，平文は 110/TCP，暗号化通信には 995/TCP を既定値とする．特にポートを指定するときは，表 3 に示すアカウント名の末尾にポート番号を付加し，“Taro%pop.example.jp:10110” のように記述する．

プロクシサーバで実行する POP プロクシのプログラ

ムに，取得したメールの DKIM 検証を行い，その結果を “X-DKIM-Check” ヘッダとしてメールヘッダに付加するよう，Perl で実装したモジュールを組み込んだ．DKIM 検証の結果は，”pass”，”fail” または”none” のいずれかを返す．”pass” は DKIM の検証ができ，そのメールがなりすましである可能性が低い，”fail” は DKIM の検証ができたが，なりすましメールである可能性が高い，”none” は，送信側が対応していなかった等の理由で DKIM の検証ができなかったことを意味する．

4.2 システムの動作手順

システムの動作手順を以下に示す．

(1) プロクシサーバは，クライアントからメール受信要求をされると，メールサーバからメールを取得する．
(2) 取得したメールについて，DKIM の検証を行う．
(3) DKIM の検証結果を，“X-DKIM-Check” のヘッダとしてメールに付加し，クライアントに配送する．
(4) DKIM の検証結果をもとに，プロクシサーバまたは MUA で通知の処理を実行する．

4.3 システムの評価方法

プロクシサーバでの DKIM 検証動作と，ユーザへの通知を確認するために，DKIM に対応していない受信メールサーバに対して，DKIM に対応した送信メールサーバからメール送信を行った．なお，送信メールサーバが DKIM に対応している場合，プロクシサーバによる検証に成功するため，検証失敗の通知を確認することができない．したがって，この評価では，メール配送経路の途中でメール本文の書き換えを行い，擬似的に DKIM 検証の失敗例を再現した．

4.4 DKIM 検証結果の通知

プロクシサーバで DKIM 認証をした結果は，以下の 4 つの方法で通知されるようにする．

方式 A メッセージの書き換え

方式 A では，プロクシサーバが通知の処理をする．プロクシサーバでの DKIM 検証結果が “fail” になったとき，そのメールはなりすましメールである可能性が高いことを伝えるものに書き替え，オリジナルのメッセージを引用形式で追加し，クライアントに配送する（図 **3**）．ヘッダはオリジナルのまま書き換えない．これを行うモジュールを Perl で作成し，プロクシプログラムに組み込んだ．

この方法では，オリジナルのメッセージを残しておくことで，受信者がなりすましメールの内容を信じたり，フィッシングサイトへのリンクを開いたりする危険性がある．一方で，DKIM 検証結果に誤りがあった場合でも，受信者はオリジナルのメッセージを読むことができるため，受信者が本来読めるものが読めなくなることはなくなる．

また，DKIM 検証結果が “pass” または “none” となった場合には何も通知しない．

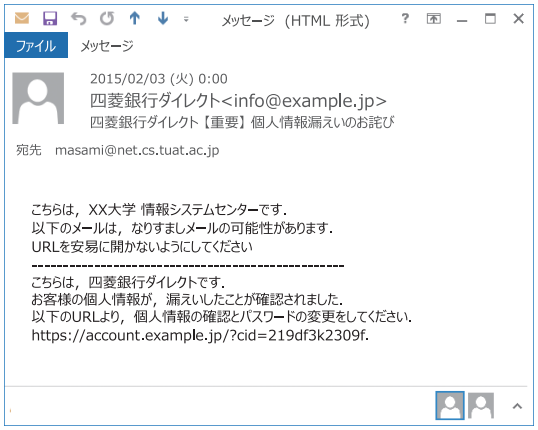

図 3 方式 A でりすましメールを引用形式にした注意喚起メール

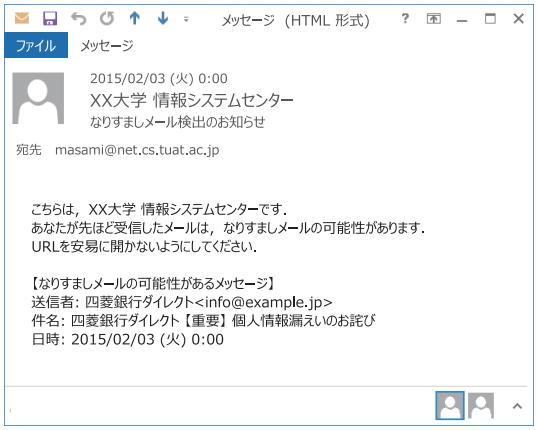

図 4 方式 B で別途送信される注意喚起メール

方式 B 注意喚起メールの送信

方式 B では，方式 A と同様にプロクシサーバが処理を行うが，クライアントへの通知方法が異なる．この方式では，オリジナルのメールを通常通り配送した後に，なりすましメールである可能性が高いことを注意喚起する通知メールを別途送信する（図 **4**）．これを行うモジュールを Perl で作成し，プロクシプログラムに組み込んだ．

方式 A と比較すると，オリジナルのメッセージが改変されないため，受信者のプライバシーを配慮することができる．一方で，なりすましメールが大量に送信された場合，オリジナルのメール一通ごとに注意喚起メールがプロクシサーバからクライアントに送信されるため，トラヒックの混雑や，ネットワーク機器への負荷が高くなる可能性が考えられる．

この方法では，通知メールをオリジナルのメールの受信者に送るだけでなく，例えば本システムを導入している学校や企業の情報システム担当者に，該当メー

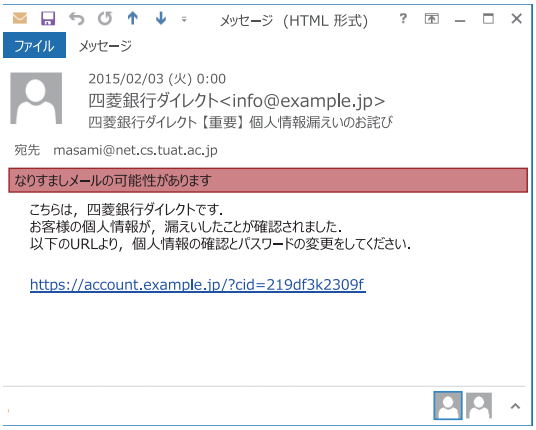

図 5　方式 C でなりすましメールを受信したときの MUA の画面

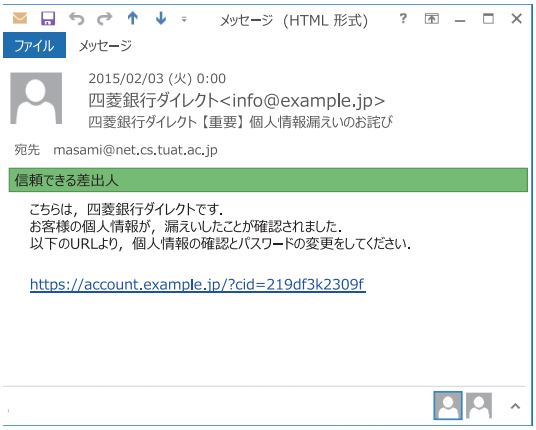

図 6　方式 C で正当なメールを受信したときの MUA の画面

ルのヘッダ情報を送ることも検討できる．また，通知メールを定期的に集計することでなりすましメールの傾向を把握し，状況に応じて学生や社員への注意喚起を行うために利用することも考えられる．

方式 C MUA でのラベル設定

方式 C では，MUA の「ラベル」や「タグ」の機能を利用する．多くの MUA には，あらかじめフィルタやルールの条件を設定しておくことで，それに一致した受信メールに自動でラベルやタグをつけることのできる，「フィルタ」や「メッセージルール」と呼ばれる機能がある．本システムでは，Microsoft Outlook 2013（以下，Outlook）の仕分けルール機能で，DKIM 検証結果が成功したメールには緑色のタグ，失敗したメールには赤色のタグがつくように設定した（図 **5**，図 **6**）．この方式では，ラベルが付加されたメールを開くと，多くの MUA では，色付きのバーやマーク，文字が表示されるようになっているため，受信者はそれを見て，メールがなりすましの可能性があるかどうかを確認することができる．一方で，MUA の標準の機能を使っているおり，受信者への通知は限られた UI でしか行えず，通知が小さく表示されることが多い．そのため，人によっては気づかない可能性がある．

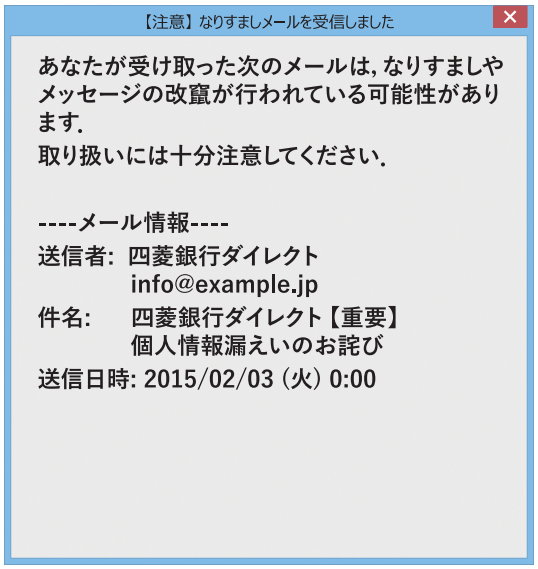

図 7　方式 D でのアドインによるポップアップ通知

方式 D MUA でのポップアップ通知

方式 D では，MUA の機能拡張（アドイン）の機構を用いる．アドインは，Outlook や Mozilla Thunderbird，Becky! など多くの MUA が対応している．アドインを利用すると，受信したメールの “X-DKIM-Check” ヘッダが “fail” であったときに，それを知らせるポップアップウィンドウが表示される．この方法では，方法 C のラベルやタグを使ったときとは異なり，通知画面を開発者が自由に設計することができるため，ユーザは通知に気付きやすくなる．

本システムでは，Outlook 用のソフトウェア開発キットを利用し，C# でアドインを実装した．DKIM 検証結果が失敗したメールを受信すると，ポップアップウィンドウに当該メールの件名や送信者名，日時の情報と注意を呼びかける文章が表示されるようにした（図 **7**）．

5. おわりに

メール受信時の DKIM 認証は，通常は受信メールサーバが行う．しかし，DKIM はまだ普及段階の途中にあるため，対応しているサーバは少ない．本システムは，学校や企業の運用する受信メールサーバが DKIM に対応していない場合でも，本システムを部局等で導入することで，独自に DKIM 認証を行うことができるようになる．また，プロクシサーバを設置することで，学校や企業の IT 管理者がなりすましメールの通知方法などを柔軟に変更したり，統計情報によって利用者への注意喚起を行うこともできる．

今後の課題として，利用者にとってどの通知方法が好ましいかを調査するとともに，ユーザ毎に通知方法を変更できるようにすることが考えらえる．

参考文献

[1] 警察庁：平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について (online), 入手先 ⟨http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf⟩ (2015.02.03).
[2] J. Klensin: *"Simple Mail Transfer Protocol," RFC5321*, IETF(2008).
[3] 総務省：送信ドメイン認証結果の集計 (SPF) (online), 入手先 ⟨ http://ww.soumu.go.jp/ main_content/000312503.pdf ⟩ (2014.02.03).
[4] M. Wong and W. Schlitt: *"Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1," RFC4408*, IETF(2006).
[5] J. Lyon, Microsoft Corp., M.Wong and pobox.com: *"Sender ID: Authenticating E-Mail," RFC4406*, IETF(2006).
[6] D. Crocker, Ed., Brandenburg InternetWorking, T. Hansen, Ed., AT&T Laboratories, M. Kucherawy, Ed. and Cloudmark: *"DomainKeys Identified Mail (DKIM) Signatures," RFC6376*, IETF(2011).
[7] 総務省：送信ドメイン認証結果の集計 (DKIM) (online), 入手先 ⟨ http://www.soumu.go.jp/main_content/000312504.pdf ⟩ (2014.02.03).
[8] WIDE プロジェクト：ドメイン認証の普及率に対する測定結果 (online), 入手先 ⟨ http://member.wide.ad.jp/wg/antispam/stats/ ⟩ (2014.02.03).