「マルチメディア，分散，協調とモバイル
(DICOMO2017) シンポジウム」 平成29年6月

ディスプレイネームをユーザ認証に利用した なりすましメール対策手法

山井 成良[1]

概要：差出人を詐称した「なりすましメール」は標的型攻撃の発端として頻繁に利用され，その対策は急務である．特に正規ユーザのアカウントを不正入手し，ディスプレイネーム（表示名）を詐称したなりすましメールを発信されると，従来の送信ドメイン認証技術を適用してもディスプレイネームの詐称を検出する効果は期待できない．そこで，本稿ではユーザが MSA（Mail Submission Agent）に普段使用するディスプレイネームを予め登録しておき，送信メッセージ中のディスプレイネームが MSA に登録されたものと一致しない限りメッセージの送出を許可しないようにする方法を提案する．これにより，たとえアカウント情報が漏洩したとしてもなりすましメールの送信を抑制する効果が期待できる．

A Countermeasure against Spoofed Emails Using Display Name as a User Authenticator

Nariyoshi Yamai[1]

1. はじめに

電子メールは社会活動を支える重要なコミュニケーション手段の 1 つであり，必要不可欠な存在となっている．一方，電子メールは不特定多数のユーザとメッセージをやり取りできることからセキュリティ上多くの問題を抱えており，特に広告，フィッシング詐欺，マルウェア配布などを目的に不特定多数のアドレス宛に一方的に送りつけられる迷惑メールの蔓延は大きな社会問題となっている．最近では大規模ボットネットの摘発，OP25B（Outbound Port 25 Blocking）[1] など，迷惑メール送信を抑止する取り組みが進みつつあり，電子メール全体に占める迷惑メールの割合は 2010 年夏頃の約 90%から最近では約 55%まで減少してきている [2], [3]．しかし，迷惑メール送信の手口も巧妙化されてきており，たとえば OP25B を回避するためにプロバイダ等が運用する MSA（Message Submission Agent）の正規の ID とパスワード（以下，これらをまとめてアカウント情報と呼ぶ）を不正な方法で取得し，これらを用いて正規ユーザになりすまして MSA から迷惑メールを送信する手口 [*1] が横行している．

```
From:  TOKAI MAIL SYSTEM <xxxxxxx@students.towson.edu>
```

図 1　詐称されたディスプレイネーム（一部匿名化）

また，多くの迷惑メールでは，**図 1** のように差出人のメールアドレスや差出人や宛先の氏名を表記するために用いられるディスプレイネーム（表示名）を詐称した「なりすましメール」となっており，このようなメールを受信したユーザが騙されるケースが後を絶たない．特に，標的型攻撃では，2015 年 5 月に発生した日本年金機構の事例 [4] や，2016 年 3 月に発生した JTB 子会社の事例 [5] などにおいて，攻撃の発端としてなりすましメールが用いられ，被害が深刻になってきている．

このような迷惑メール，特に差出人アドレスを詐称したなりすましメールへの対策として，SPF[6]，DKIM[7]，DMARC[8] 等の送信ドメイン認証技術が知られている [1]．現時点では普及率がそれほど高くないなどの問題点はあるものの，これらの技術を用いれば，差出人アドレスの詐称についてはこれを正しく検出できる効果がある程度期待できる．ところが，差出人や宛先の氏名を表記するために用

[1] 東京農工大学
Tokyo University of Agriculture and Technology

[*1] 一般に submission spam，MSA 踏み台送信などと呼ばれる．

いられるディスプレイネーム（表示名）は利用可能な文字列にあまり制限がなく，送信者が RFC5322.From（ヘッダ From）[9] に付随して設定された文字列がそのまま表示されることが多い．そのため，差出人アドレスは詐称せずに正規ユーザのものをそのまま使用し，ディスプレイネームだけ実在の企業や人物に詐称したなりすましメールを正規の MSA 経由で発信されると，従来の送信ドメイン認証技術ではこれを検出できず，被害がより深刻化する可能性がある．

そこで，本稿では一般にディスプレイネームはユーザの使用する MUA（Mail User Agent）にアカウント情報とともに登録され，これが変更されることは稀である点に着目し，アカウント情報が漏洩した場合でもディスプレイネームを詐称したなりすましメールを容易に送信できない仕組みを提案する．具体的には，ユーザが MSA に予め使用するディスプレイネームを登録しておき，送信メッセージ中のディスプレイネームが MSA に登録されたものと一致しない限りメッセージの送出を許可しないようにする．これによりなりすましメールの送信を抑制し，その被害を軽減する効果が期待できる．

2. 従来のなりすましメール対策と問題点

前節で述べたように，なりすましメール対策として SPF，DKIM，DMARC 等の送信ドメイン認証技術がよく知られている．また，特に送信に特化した対策として差出人アドレスチェックが挙げられる．以下ではこれらの対策とその問題点について述べる．

2.1 送信ドメイン認証

送信ドメイン認証は差出人アドレスのドメイン部分が詐称されていないかどうかを受信側で確認可能とする技術である．代表的な方法として，SPF[6]，DKIM[7]，DMARC[8] が知られている．

2.1.1 SPF

代表的な送信ドメイン認証技術のうち，SPF（Sender Policy Framework）は，送信元 IP アドレスに基づく送信ドメイン認証技術である．この技術では，まず，ドメイン管理者は自身が管理するドメインから電子メールを送信する場合に使用する MTA（Mail Transfer Agent）の IP アドレスを DNS サーバに SPF レコードとして登録しておく．受信 MTA はメッセージを受信する際に RFC5321.From（エンベロープ From）アドレスのドメイン部に対応する SPF レコードを取得し，送信元 IP アドレスが SPF レコードで宣言された IP アドレス群に含まれるかどうかにより送信ドメインが詐称されていないかどうかを判断する．

SPF は比較的導入が簡単であるため，日本では 2017 年 2 月時点 *2 で約 50%の普及率を達成している [11]．ただし，受信者が転送設定を行っていると，転送先では最初の送信元とは異なる IP アドレスからこのメッセージを受信することになるため，認証に失敗する場合が多いという問題点がある．また，認証に利用される差出人アドレスは MUA で表示される RFC5322.From ではなく，エラー時の返送先アドレスとして用いられる RFC5321.From であるため，なりすましメール抑制の効果が低いといえる．

2.1.2 DKIM

DKIM（DomainKeys Identified Mail）は電子署名に基づく送信ドメイン認証技術である．この技術では，ドメイン管理者は予め公開鍵暗号方式に基づいて秘密鍵と公開鍵を作成し，そのうち公開鍵を DNS で公開し，また MTA ではメッセージ送信時に秘密鍵を用いて電子署名（DKIM 署名）を作成し，これヘッダ中に埋め込むようにする．受信 MTA は受信したメッセージから電子署名を取り出し，DNS で入手した公開鍵を用いてメッセージ全体（本文および差出人アドレスを含む一部のヘッダ）に改竄がないかどうかを判断する．この方法では差出人アドレスだけでなく，ディスプレイネームを含めてメッセージが改竄されたかどうかを検証することができる．また，DKIM では送信元 IP アドレスを送信ドメイン認証に用いないため，転送されても認証を正しく行うことができる．

しかし，なりすましメールが MSA を踏み台にして送信された場合，DKIM 署名はなりすました差出人アドレスに対して作成されるため，受信側では送信ドメイン認証に成功し，なりすましを検出することができない．また，DKIM では差出人メールアドレスとは異なるドメインの署名（第三者署名）を許容しているため，なりすましメールの送信者が自身の管理するドメインの第三者署名を作成して DKIM 認証に成功するなりすましメールを送信することが可能である．さらに DKIM は送信 MTA に署名付与機能を追加する必要があることから，SPF より普及率が低く，2017 年 2 月時点における日本での普及率が 30%に達していない [12] 点も問題である．

2.1.3 DMARC

DMARC（Domain-based Message Authentication, Reporting, and Conformance）は SPF と DKIM を併用 *3 し，それぞれの技術による送信ドメイン認証が失敗した場合に送信元ドメインにその報告を行ったり，両方の技術による送信ドメイン認証に失敗した場合に送信元ドメインが定めたポリシーに応じて受信ドメインがそのメッセージの処理を決定できたりする枠組みを提供するものである．DMARC では認証に用いられる差出人メールアドレスは RFC5322.From であり，また SPF 認証では RFC5321.From と RFC5322.From が同一ドメインか親子ドメインのものであること，DKIM 認証の場合は第三者署名ではない（署

*2 これ以降，評価対象ドメイン数が 500 から 50 に変更されたため．DKIM，DMARC についても同様．

*3 SPF，DKIM のいずれか一方だけ使用することも可能．

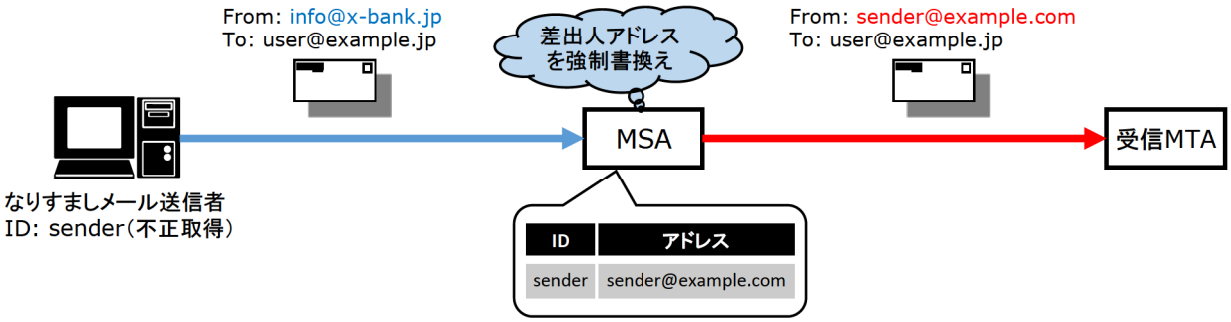


図 2　差出人アドレスの強制書換え

名者が RFC5322.From と同一ドメインか親子ドメインに属する）ことが要求されるため，なりすましメール抑制効果は比較的高いといえる．

しかし，なりすましメールが MSA を踏み台にして送信された場合，受信側ではなりすましを検出することができない問題点は依然として残されている．また，DMARC は第三者署名を許容しないため，メールサービスをアウトソーシングしている組織では導入が困難か導入に手間がかかることもあり，2017 年 2 月時点における日本での普及率が 20%強 [13] と DKIM よりもさらに低い点も問題である．

2.2　差出人アドレスチェック

特になりすましメールの送信に特化した対策として，差出人アドレスチェックが挙げられる．これは，MSA において送信者認証を行った後，メッセージの差出人アドレスが認証されたユーザに対応付けられたものかどうかチェックを行い，このチェックに失敗した場合には送信を許可しない，あるいは差出人メールアドレスを書き換えるなどの処理を行うことでなりすましメールの送信を抑止する方法である．特に，差出人アドレスチェックに失敗した場合に送信を許可しない方法では，差出人メールアドレスを詐称した MSA 踏み台送信を抑止する効果が期待できる．

差出人メールアドレスを書き換える場合の例を図 **2** に示す．MSA は各ユーザ ID に対応する正規の差出人アドレスを保持しており，メッセージ中の差出人アドレスが正規の差出人アドレスに一致しなければこれを強制的に正規のものに書き換えてから送信する．既に一部のメールサービスではチェックに失敗したメッセージの送信を許可しない機能が提供されていることが文献 [1] では報告されている．

しかし，この方法では差出人メールアドレスを詐称は防止できるが，ディスプレイネームだけを詐称したなりすましメールの送信は防止できない．一般に，ディスプレイネームは同一のユーザであっても，特に複数の MUA を使用している場合では常に同一のものを使うとは限らないため，強制的な書換えや送信の抑止を行うような単純な方法を採用するのは問題がある．

3.　ユーザ認証におけるディスプレイネームの利用

3.1　提案方式の概要

前節で述べたように，従来のなりすましメール対策技術にはそれぞれ問題がある．特に差出人メールアドレスは詐称せず，ディスプレイネームだけを詐称したなりすましメールを MSA が踏み台にして送信された場合，上記のいずれの方法でもこれを防止することはできない．

ここで，ディスプレイネームの通常の使い方を考察すると，正規ユーザはたとえ複数の端末を利用する場合であっても個々の端末上の MUA にユーザ名，パスワードなどとともにディスプレイネームを登録しており，これらのディスプレイネームを変更することは稀である．また，MSA 踏み台送信を行う不正送信者は通常は乗っ取ったアカウントの正しいディスプレイネームを知っていない．これらの特徴に着目すると，ディスプレイネームは複数の正答を持つ一種のパスワードとして利用することが可能である．

そこで，本研究では予め MSA に送信者が使用するディスプレイネームを登録しておき，それが RFC5322.From に付随するディスプレイネームと一致しない限りメッセージの送出を許可しないようにする．MSA に登録するディスプレイネームは複数でもよく，そのいずれかに RFC5322.From に付随するディスプレイネームが一致すれば送信を許可するようにする．

3.2　システムの構成と動作例

本手法は現時点では対策方法の一提案に過ぎず，設計や実装はまだ行っていない．また，本手法の評価は社会実験を行う必要があり，現時点では非常に困難である．そこで，以下では現時点で想定している，単純な提案システムの構成およびその動作を例示する．

提案システムは図 **3** に示すように MSA および MSA が呼び出す milter（mail filter）プログラムから構成される．milter プログラムには（ユーザ ID，アドレス，ディスプレイネームリスト）の 3 つ組レコードを格納するデータベースを持ち，たとえば Web インタフェースを用いてユーザが（複数の）ディスプレイネームを事前に登録しておくよ

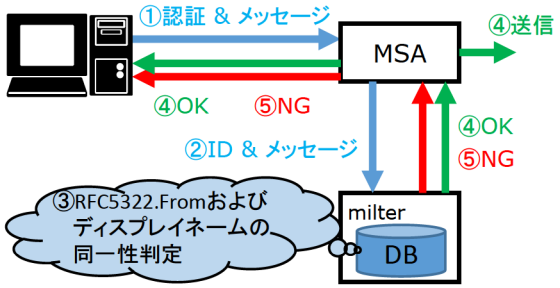


図 3　提案システムの構成と動作

うにする．また，合理的な理由があれば，1 つのユーザ ID に対して複数のアドレスの使い分けを許容してもよい．その場合には 1 つのユーザ ID に対して複数の 3 つ組レコードがデータベースに登録されることになる．

本システムの想定している動作を以下に示す．なお，各ステップの番号は図 3 中の番号に対応している．

(1) MSA は端末との間でユーザ認証を行い，これに成功すると端末からメッセージを受け取る．但し，この時点では端末との間の SMTP セッションは維持したままで，メッセージの受理，拒否応答は返さない．

(2) MSA は milter プログラムに認証済みのユーザ ID やエンベロープ情報とともに，メッセージ（ヘッダおよび本文）を送る．

(3) milter プログラムは MSA からユーザ ID とメッセージを受け取ると，ヘッダから RFC5322.From およびこれに付随するディスプレイネームを取り出し，ユーザ ID をキーとしてデータベースから得たアドレスおよびディスプレイネームリストと照合を行う．

(4) もしメッセージ中の RFC5322.From がデータベース中のアドレスと一致し，さらにメッセージ中のディスプレイネームがデータベース中のディスプレイネームリストのいずれかの要素と一致すれば，milter はこのメッセージを受理する応答を MSA に返す．MSA は端末に受理応答を返し，このメッセージを送信する．

(5) そうでなければ，milter はメッセージを拒否する応答を MSA に返す．MSA は端末に拒否応答を返す．

なお，milter にコマンド M で渡される差出人アドレスは RFC5321.From であり，ディスプレイネームを含まないため，実装の際には混同しないように注意が必要である．

3.3　考えられる問題点と対策

本節では現時点で考えられる提案方法の問題点とその対策について述べる．

まず，アカウント情報が漏洩している状況では，提案方法を導入してもなりすましメールの送信は可能ではないかという懸念がある．これはディスプレイネームが公開情報であるため，なりすましメール送信者がこれを取得し，メール送信時に同じディスプレイネームを設定することは容易であるためである．しかし，この場合は差出人メールアドレスとディスプレイネームは詐称されていないため，受信者が容易には騙されないと思われる．したがって，提案方法の有効性は十分期待できる．

これに対するなりすましメール送信者の対抗策として，なりすましメール送信者が不正取得したアカウント情報を悪用して新しいディスプレイネームを MSA に登録し，なりすましメールを送信する方法が考えられる．この方法によるなりすましメール送信への対抗策として，たとえば新たなディスプレイネームを MSA に登録する際には 2 要素認証を必要とするなど，アカウント情報がたとえ漏洩したとしても，それだけでは新しいディスプレイネームを MSA に登録できないようにする方法が有効であると思われる．

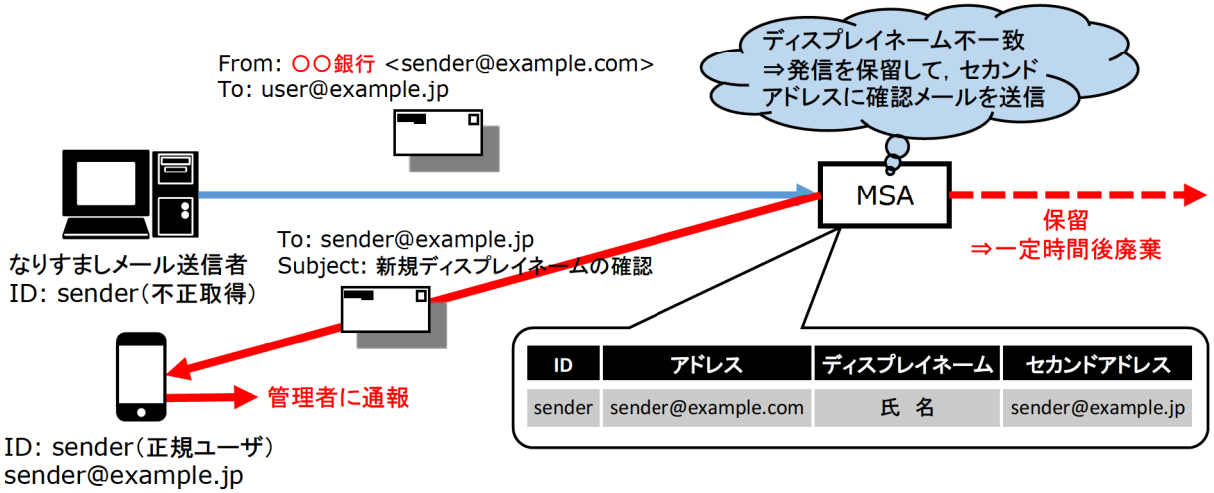
また，正規のユーザが複数のディスプレイネームを事前に登録するのは利便性を損ねる可能性がある．この問題への対策として，ディスプレイネームの事前登録の代わりに，ディスプレイネームが不一致の場合にはそのメッセージの送信を保留して 2 要素認証を要求し，これに成功した場合には不一致だったディスプレイネームをディスプレイネームリストに追加登録するようにする方法が考えられる．これにより，ユーザの負担を比較的小さくできるだけでなく，アカウント情報の漏洩に早期に気づく効果も期待できる．図 4 に 2 要素認証としてセカンドアドレスに確認メールを送る方法を用いた場合の動作を示す．

さらに，提案方法を導入していない MSA がどこかに存在すれば，その MSA を踏み台にしてなりすましメールを送信できるので，インターネット全体ではなりすましメールの送信を抑制できないという指摘が考えられる．この指摘は事実であるが，提案方法を導入した MSA が普及すれば，その分だけなりすましメールの流通量を減らすことが可能であると思われる．また，たとえば日本の主要なメールサービスで提案方法が採用された場合，海外から発信されたなりすましメールは GeoIP[14] など IP アドレスから地理情報を得るサービスを用いれば比較的容易に判別可能になると思われる．実際に，これと同様の議論が成り立つ OP25B については多くのプロバイダで導入された結果，迷惑メールの減少につながっているという実績がある．

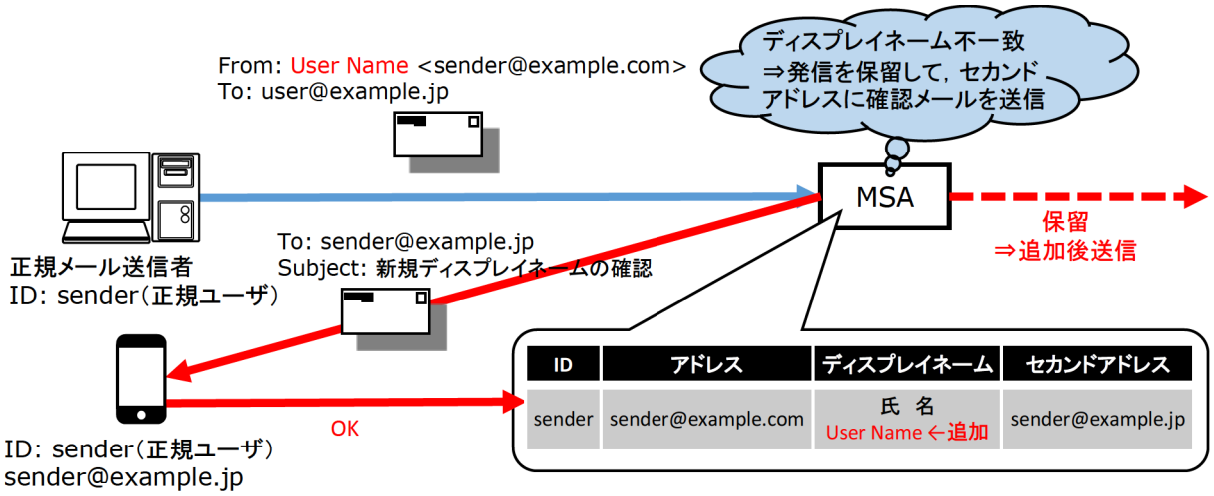
なお，この対策手法ではたとえば悪意を持つ利用者が無料メールサービスのアカウントを取得し，そのアカウントを使用してなりすましメールを送信する手口には効果がない．しかし，この手口は少なくとも日本国内では特定電子メール法 [15] に違反し，処罰の対象になるため，一定の抑止力が働いていると考えられる．

4.　まとめ

本稿では，詐称目的に悪用されているディスプレイネームが一種のパスワードとして利用できることに着目し，メッセージ中に含まれるディスプレイネームが予め MSA 登録



(a) なりすましメール送信者が送信を試みた場合



(b) 正規ユーザが送信を試みた場合

図 4 ディスプレイネーム不一致時の動作例

されているものと一致しないと送信できない方法を提案した．これにより，たとえアカウント情報が漏洩したとしても MSA 踏み台送信およびなりすましメールの送信を抑制する効果が期待できる．この方法は提案段階であり，またこの方法を実装したシステムがあったとしても有効性の検証は非常に困難であるが，本稿の公表によりこの方法が多くのメールサービスで導入され，結果として MSA 踏み台送信およびなりすましメールの送信の減少につながることを期待する．

参考文献

[1] 迷惑メール対策推進協議会：迷惑メール対策ハンドブック 2016 (オンライン)，入手先 ⟨http://www.dekyo.or.jp/soudan/image/anti_spam/book/2016/2016MHB_all.pdf⟩ (参照 2017-05-04)，2016 年 12 月.

[2] Symantec Corporation: State of Spam & Phishing Report — A Monthly Report, No.45, Symantec Corporation (online), available from ⟨https://www.symantec.com/content/dam/symantec/docs/security-center/archives/spam-report-sept-10-en.pdf⟩ (accessed 2017-05-04).

[3] Symantec Corporation: Internet Security Threat Report, Vol.21, Symantec Corporation (online), available from ⟨https://www.symantec.com/content/dam/symantec/docs/security-center/archives/istr-16-april-volume-21-en.pdf⟩ (accessed 2017-05-04), April 2016.

[4] サイバーセキュリティ戦略本部: 日本年金機構における個人情報流出事案に関する原因究明調査結果，内閣サイバーセキュリティセンター (オンライン)，入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf⟩ (参照 2017-05-04)，2015 年 8 月.

[5] 株式会社ジェイティービー: 不正アクセスによる個人情報流出の可能性について —現状報告と再発防止策—，株式会社ジェイティービー (オンライン)，入手先 ⟨https://www.jtbcorp.jp/jp/160824.html⟩ (参照 2017-05-04)，2016 年 8 月.

[6] Kitterman, S.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, RFC7208,

IETF, April 2014.
[7] Crocker, D., Hansen, T. and Kucherawy, M.: DomainKeys Identified Mail (DKIM) Signatures, RFC6376, IETF, September 2011.
[8] Kucherawy, M. and Zwicky, E (Eds.): Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489, IETF, March 2015.
[9] Resnick, P. Ed.: Internet Message Format, RFC5322, IETF, October 2008.
[10] Klensin, J.: Simple Mail Transfer Protocol, RFC5321, IETF, October 2008.
[11] Eggert, L.: SPF Deployment Trends (online), available from ⟨https://eggert.org/meter/spf⟩ (accessed 2017-05-04).
[12] Eggert, L.: DKIM Deployment Trends (online), available from ⟨https://eggert.org/meter/dkim⟩ (accessed 2017-05-04).
[13] Eggert, L.: DMARC Deployment Trends (online), available from ⟨https://eggert.org/meter/dmarc⟩ (accessed 2017-05-04).
[14] Maxmind Developer Site: "GeoIP Products << Maxmind Developer Site (online), available from ⟨http://dev.maxmind.com/geoip/⟩ (accessed 2017-05-04).
[15] 特定電子メールの送信の適正化等に関する法律，平成 14 年 4 月 17 日法律第 26 号，平成 14 年 7 月 1 日施行，平成 23 年 6 月 24 日最終改正.