迷惑メール対策推進協議会
Anti-Spam mail Promotion Council

電子メールのなりすまし対策

―送信ドメイン認証技術でなりすましを防ぐ―

なりすましの問題

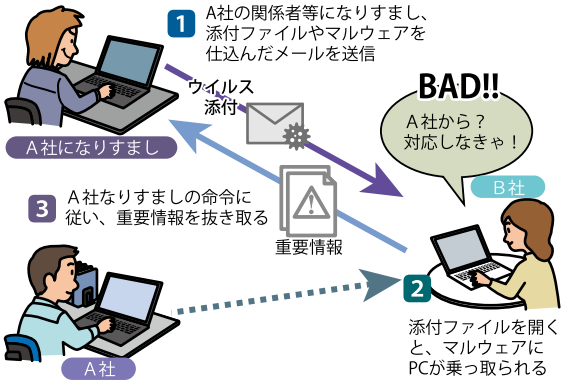
電子メールは、簡易で便利なコミュニケーションツールとして広く普及しています。

電子メールの通信は、SMTP（シンプル・メール・トランスファー・プロトコル）という通信手順が用いられています。しかし、この通信手順の規格は1970年代に策定されたもので、送り手が誰であるかを確認する仕組みが備わっていません。そのため、いわゆる「なりすまし」が容易にできてしまい、近年では、次のような多くの問題が引き起こされています。

■ 有名企業等になりすまされ、マルウェアに感染させられる

知り合いや有名企業などになりすましたメールに添付されたファイル等を開いたり、記述されたURLをクリックすることで、マルウェアに感染させられる恐れがあります。これにより例えば、外部からコントロールされるボットにさせられたり、PC内部や接続されたネットワーク上にある情報を窃取されたり、操作過程で得られる個人情報などが盗まれる、といった被害が起きています。

特に、最近では、特定の相手を狙い、送信者情報を詐称するとともに、タイトル、本文等に巧妙な記述をすることによって、添付ファイルを開かせたり、URLをクリックさせることで、マルウェアに感染させ、重要な情報を抜き出す「標的型攻撃メール」が引き続き多数確認されています。

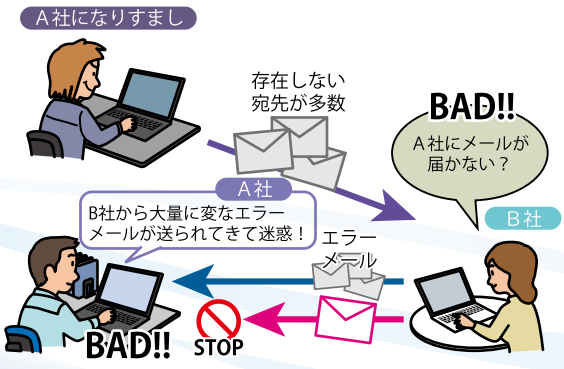


※正規の送信者になりすまされ、マルウェアに感染させられて、重要情報を窃取される危険
※フィルタリング（A社からのメールしか受けない設定）をしていても、届いてしまう

■ 大量のエラーメールが返送されてしまう

送信者情報を確認できない設定をしていると、受け取るべきメールかどうかの判断ができず、迷惑メールと判断されてメールが届かない恐れがあります。また、なりすましを防ぐ設定をしないドメインは、迷惑メールの送信者情報に悪用され、ドメインの価値自体を低下させる可能性もあります。

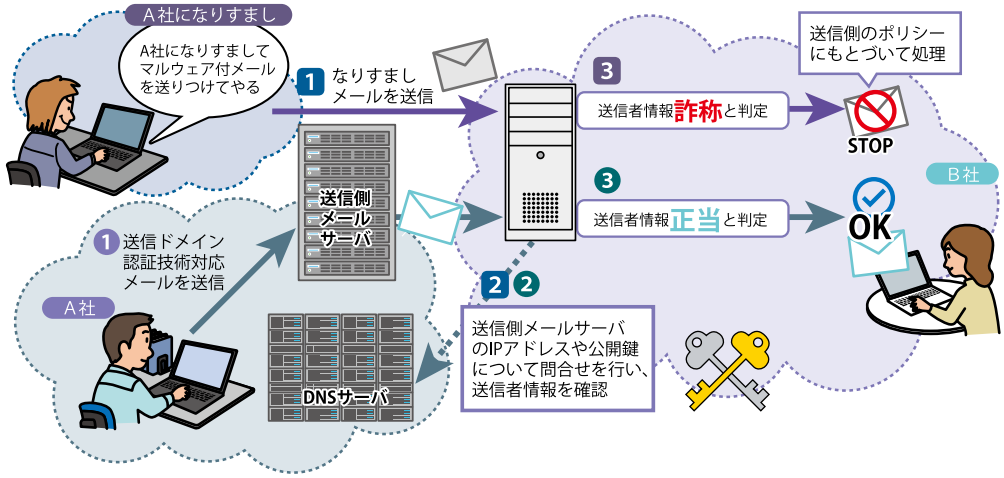
自らのドメインを送信者情報に悪用されてしまった場合、迷惑メールと判断されてエラーメールとなって返送されてきます。大量に送信されたなりすましメールの返送によって、メールの受信設備に悪影響を与える可能性があります。



※自動的に返したつもりのエラーメールで、迷惑メール送信者と勘違いされ、他のメールもブロックされてしまう恐れ

送信ドメイン認証技術DMARCによる解決

送信ドメイン認証技術に対応することにより、自らのドメインの信頼性を確保するとともに、なりすましメールを見破ることができます。



このようなりすましメールの防止策として、「送信ドメイン認証技術」があります。送信ドメイン認証技術とは、受信者が受け取ったメールについて、送信者情報が詐称されているかどうかをドメイン単位で確認可能とする技術で、インターネットの標準規格にもなっています。

送信ドメイン認証技術を利用するためには、送信側と受信側の双方で、メールサーバとDNSに新たな設定や機能を追加することが必要となります。しかし、従来の通信手順の標準規格に直接影響をあたえることなく導入することができ、また、送信側と受信側のどちらからでも導入することができます。さらに、メールサーバでの対応ですので、個々の利用者が対応するのではなく、メールサーバを管理しているプロバイダや企業などが対応することになります（受信側でなりすましの確認結果を利用したり、なりすましメールに対するドメイン管理側のポリシーを確認することで、フィルタリングなどに利用するなどの対策を行います。）。

■ なりすましメールにより被害が生じた事例

（1）国の機関が標的型メールにより情報漏洩に発展した事例

2015年5月にメールに示されていたURLをクリック、また添付ファイルを開封したことにより不正プログラムに感染。外部サーバとの通信により、組織内部にあった顧客情報約125万件が外部に情報漏洩しました。

報告書からは、受信時のウイルスチェックは実施していたが、未知のウイルスに対しては対策ができず結果としてすり抜けたことが示されている。送信されたメールの事例も示されているが、送信元のドメインが正しく利用されているのか、送信者との関係から不自然な点が無いかなどの確認が必要だったと考えられます。

（2）大手旅行代理店がなりすましメールによる情報漏洩

2016年３月に、グループ会社が取引先を偽装したなりすましメールの添付ファイルを開封し実行したことにより感染。最大798万件の個人情報が流出した可能性があると報道されました。送信元に確認メールを送信したが不達であったことから、実在しない送信者情報を利用したことが推測できます。

送信ドメイン認証技術を導入する必要性

送信ドメイン認証技術は、メールの送信側・受信側の双方が導入することによって、はじめて認証が可能になるため、送信側・受信側の双方で対応することが求められています。現在、多くのインターネットサービスプロバイダでは、既に送信側および受信側として送信ドメイン認証技術の導入が進んでいます。メール配信事業者でも、送信側として送信ドメイン認証技術の導入が進んでいます。

■ 送信側

自らのドメインになりすまされたメールが送信されることにより、受信者が個人情報等の重要な情報を窃取される等の被害に遭う恐れがあります。また、メールに利用しないドメインであっても、正しい設定をしないと送信者情報に悪用される場合があります。こうしたことが起きると、自らのドメインの信頼性が低下するだけでなく、社会的にも大きな問題となる恐れがあります。

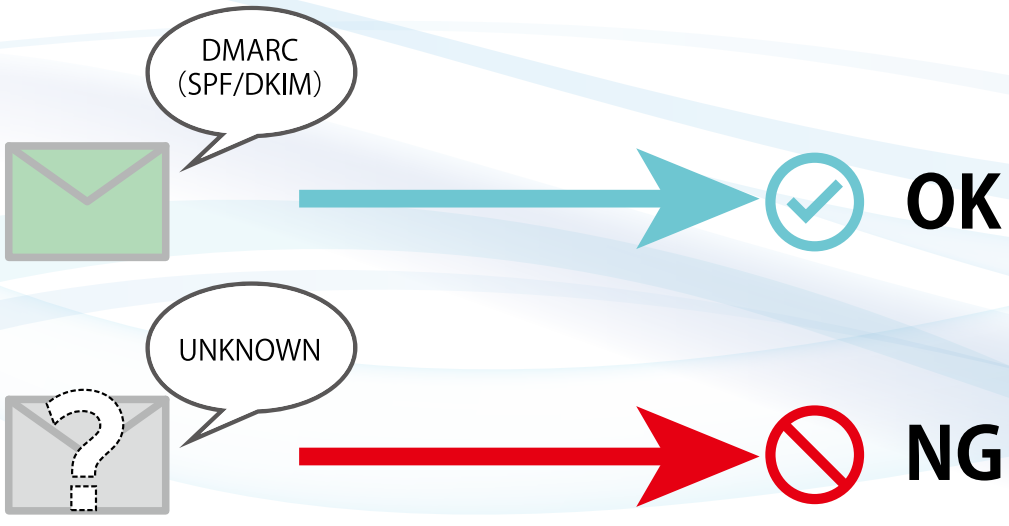
また、既に受信側で送信ドメイン認証技術を導入しているインターネットサービスプロバイダ等の中には、送信ドメイン認証技術に対応していないメールの評価を低くしたり、認証が失敗したメールを受信拒否するところもあります。

こうしたことから、送信側において、送信ドメイン認証技術に対応することが求められています。

■ 受信側

受信側では、送信側で正しい送信者情報を名乗っているかを認証するために、送信ドメイン認証技術に対応することが求められています。これにより、例えば標的型攻撃メールやフィッシングメールのように送信者情報を偽装したメールについて送信者を確認することが可能となります。さらに、送信ドメイン認証結果を活用することにより、受信メールを選別し、迷惑メール対策をより効率的・効果的に行うことが可能となります。

すなわち、なりすましメールを見分けることで、その後のフィルタリング等の処理が、より適切に行えるようになります。一般の利用者の方も、プロバイダのサービスを利用することにより、対応が可能です（サービスの提供の有無や内容は、プロバイダにより異なります。）。



送信ドメイン認証技術DMARC

送信ドメイン認証技術は、ネットワーク方式のSPFと電子署名方式のDKIMの２つの異なる方式があり、さらにそれらの認証結果を活用するDMARCによってより効果的に機能します。

ネットワーク方式の送信ドメイン認証技術　SPF

ネットワーク方式の送信ドメイン認証技術SPFは、送信元のメールサーバのIPアドレスをもとにして認証します。

この方式では、送信側の導入コストがほぼ皆無であるなど、送信側の導入の容易さが長所となっています。このため送信側では、メールに利用しないドメインも含め全てのドメインについて、まずSPFの設定をすることが望まれます。

一方で、後述するようにメールの転送時に認証が失敗することがありますので、送信側としてのDKIMの導入も検討する必要があります。

電子署名方式の送信ドメイン認証技術　DKIM

電子署名方式の送信ドメイン認証技術は、公開鍵暗号技術という暗号技術を利用して認証します。この方式には、DomainKeys Identified Mail(DKIM) という標準規格があります。

この方式では、メールの配送経路によらない認証のため、ネットワーク方式のようなメール転送時の認証失敗がほとんど発生しないという長所があります。また、メール本文の改ざんも検知することができるという長所もありますが、逆にメーリングリストのようにメール本文などを変更するサーバを経由した場合には、認証が失敗するという課題があります。

さらに、電子署名の作成を委託する第三者署名を利用した場合、DKIMとしては認証ができても、認証したドメインと送信者情報が異なるためにDMARCでの認証が失敗する場合があります。

総合的な送信ドメイン認証技術DMARC

DMARCは、SPFとDKIMの認証結果を利用して、総合的に送信ドメイン認証を行う技術です。

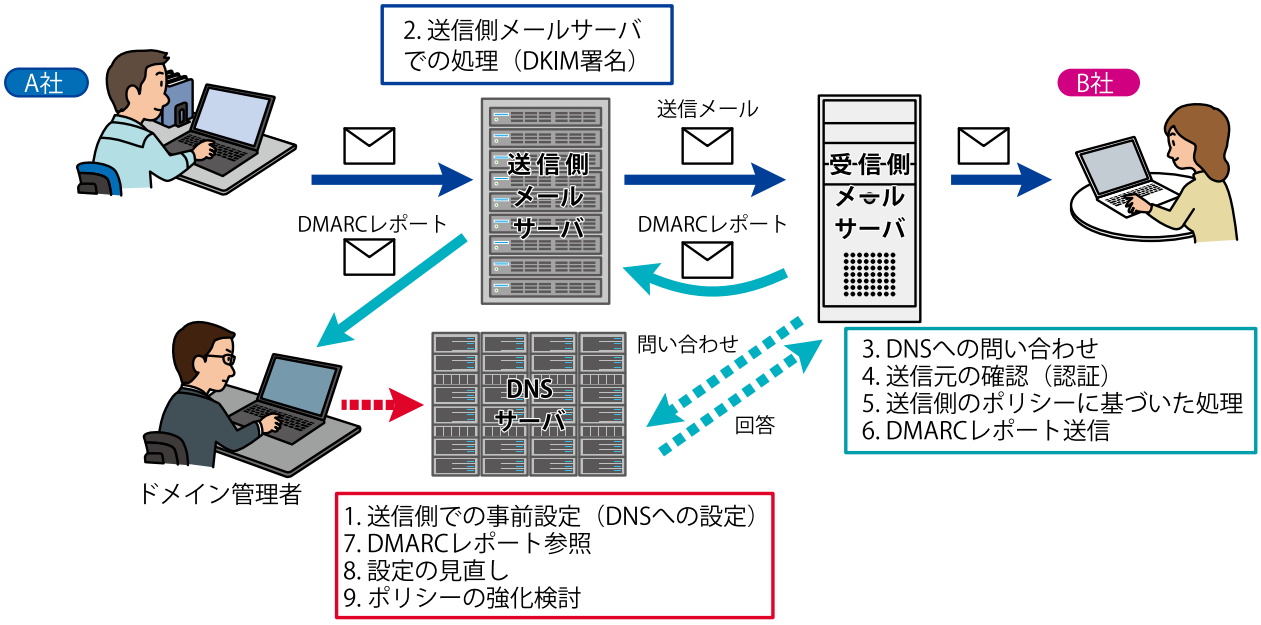
既にSPFあるいはDKIMを導入していれば、送信側でのDMARC導入はとても簡単にできます。DMARCでは、SPFあるいはDKIMの認証結果を利用するため、双方の長所を生かした認証ができます。

DMARCでは、認証が失敗した場合のメールの取り扱いを送信側でポリシーとして宣言できます。これにより、なりすましメールが重大な問題となるメールに対しては、受け取らないといった強いポリシーを受信側に伝えることができるようになります。さらにDMARCでは、ドメイン管理者（送信側）が、ポリシー設定の判断を助けるために、メール受信側が送信するDMARCレポートの宛先を、DMARCレコードに設定することができます。

	SPF	DKIM	DMARC
名称	Sender Policy Framework RFC 7208	DomainKeys Identified Mail STD 76, RFC 6376	Domain-based Message Authentication, Reporting, and Conformance　RFC 7489
特徴	送信元をネットワーク的に判断 （送信元のIPアドレスにより確認）	送信時に電子署名をメールに付加 （電子署名の検証により判断）	SPFあるいはDKIMの認証結果を利用 （送信側でポリシーを設定、認証結果のレポート機能）
導入コスト	送信側はほぼ皆無（DNSの記述のみで１通ずつの処理は不要） 受信側では一定の処理が必要	送信側は相対的に高め （１通ずつ署名作成・付加が必要） 受信側では一定の処理が必要	既にSPF，DKIMを導入していれば送信側はほぼ皆無 （DNSの記述のみ） 受信側では一定の処理が必要
長所	送信側の導入の容易さ（特にコスト面） 普及が進んでいる	メール本文の改ざんも検知 メールの配送経路に影響されない	送信側の導入の容易さ 認証失敗時のふるまいをポリシー指定可能
短所	メール転送時に認証失敗する場合がある	配送経路上でメール内容が変更されると認証失敗 第三者署名ではDMARC認証に失敗する場合がある（DNS設定の工夫で回避できる場合がある）	SPFとDKIM双方が失敗する場合には認証が失敗する

DMARC認証の手順の概要

DMARCで認証するには、SPFあるいはDKIMの導入が前提になります。いずれの方式でも、認証するためには、送信側のDNS設定や送信側と受信側のメールサーバでの処理が必要となります。DMARCでの認証の流れについて説明します（実際の処理はもっと複雑ですが、模式化して簡単に説明しています。）。



(1) 送信側のDNSでSPFレコードおよびDMARCレコードを設定。
DKIMを利用するには、送信側のメールサーバで、認証に用いる公開鍵暗号技術による鍵ペア（公開鍵、秘密鍵）を生成し、公開鍵をDNSサーバでDKIMレコードとして公開。

(2) DKIMを利用するには、個別のメールの送信にあたり、メールの内容（ヘッダ・本文）の情報を用い、(1)の秘密鍵により電子署名を作成し、メールに添付。

(3) 受信側のメールサーバでは、メールを受信した際に、SPFとDKIMそれぞれで送信者となるドメインのDNSサーバに、それぞれの設定レコードを問い合わせる。
メールヘッダの送信者情報のドメインから、DMARCレコードを問い合わせる。

(4) SPFおよびDKIMそれぞれで認証処理を行う。
SPFおよびDKIMの認証結果とDMARCレコードからDMARCの認証処理を行う。

(5) DMARCの認証結果とDMARCレコードのポリシーから受信処理を判断する。
DMARC認証が失敗した場合、DMARCのポリシー通りの処理を実施するかどうかを受信側であらかじめ検討しておく必要がある。

(6) 受信時の認証結果を元にDMARCレポートを送信する。

(7) DMARCレコードでレポートを受信する設定にしている場合は、受信したレポートを参照し、正規のメールが認証失敗していないかを確認する。

(8) 正規のメールが認証失敗している場合は、失敗しているSPFあるいはDKIMの設定見直しを実施する。

(9) 正規のメールの認証失敗が発生していない場合は、送信しているメールの用途も検討の上、DMARCポリシーの強化等を行う。

DMARC導入の手順

送信ドメイン認証技術DMARCの導入にあたっては、あらかじめ検討しておくべき事項がいくつかあります。以下で、送信ドメイン認証技術DMARCの導入の手順の概要を、簡単に説明します。SPFとDKIMの導入手順の詳細は、「送信ドメイン認証技術導入マニュアル」などをご覧ください。

STEP 1　SPFおよびDKIMの導入

メールの送信側としては、まずSPFレコードの設定をします。SPFレコードを設定するには、対象となるドメインでメール送信する出口（メールサーバ）を把握する必要があります。DKIMを導入する場合も同様に、電子署名を追加するために出口の把握が必要になります。インターネットサービスプロバイダ等のメールサービスを利用している場合や、クラウド型のメールサービスを利用している場合は、それぞれのサービス提供事業者に確認が必要です。

メールの受信側としては、SPFおよびDKIM、DMARCの認証機能を受信メールサーバに組み込む作業が必要となります。いずれの機能も既にオープンソースでも提供されています。

STEP 2　DMARCレコードを設定

既にSPFやDKIMを送信側として導入している場合は、DMARCレコードを設定することでDMARCを送信側として導入したことになります。DMARCレコードの設定では、認証が失敗したメールの取り扱いをポリシーとして設定することが主な作業です。最初は受信側が認証できるように“none”のポリシーから始めるのが良いでしょう。

STEP 3　DMARCレポートの受信準備

DMARCでは、認証結果を2種類のレポートで把握することができます。これらレポートを受信するための準備（メールアドレスの作成）をしましょう。準備ができたら、DMARCレコードにレポートの宛先を設定します。集約レポートは、圧縮されたXMLデータとして送られてきますので、参照するには分析環境が必要となります。レポート分析を外部に委託する方法もあります。

STEP 4　SPFおよびDKIM設定のみなおし

DMARCレポートを受信し、内容を確認できるようになったら、認証が失敗しているメールを調査しましょう。詐称されて認証失敗しているケースは正しく認証できていますので問題ありません。正規のメールが認証失敗している場合は、SPFあるいはDKIMの設定の見直しが必要になります。

こうした正規のメールの認証失敗が続いている間は、DMARCのポリシーを強くしないほうが良いでしょう。

STEP 5　DMARCポリシーの検討

DMARCレポートを参照し、正規のメールが認証失敗しないことが確認できたら、DMARCのポリシーを“quarantine”あるいは“reject”に設定してみましょう。DMARC認証をしているメールサービスでは、既にDMARCのポリシーに基づいた受信処理をしている事業者があります。ポリシーの強化は、利用者への周知等も含め慎重に検討の上実施すべきです。

DMARC導入後の運用

送信ドメイン認証技術を導入した後も、その認証状況を確認し、問題が生じないようにすることが必要となります。

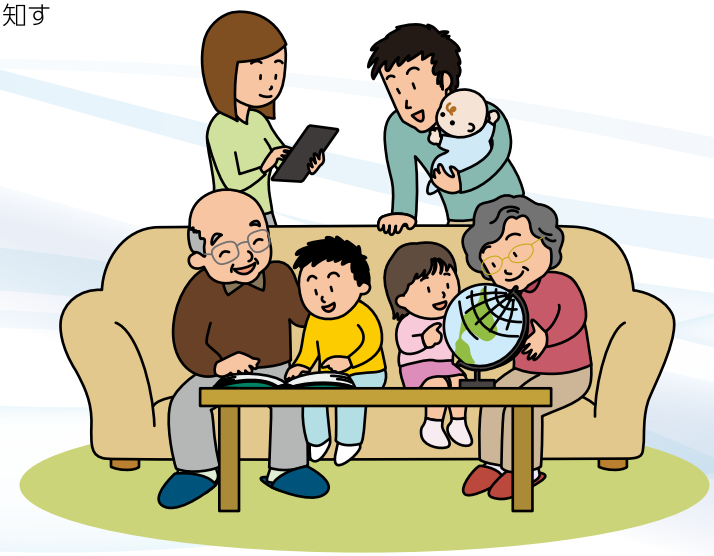
DMARCでは、認証結果をDMARCの集約レポートとして受け取ることができますので、正規のメールサーバから送信されたメールが正しく認証できているかを確認することができます。もし、認証が失敗した原因がSPFであれば、SPFレコードの設定を確認したり、DKIMを導入することで認証失敗が回避できないかを検討することが必要となります。

SPFとDKIMを導入していても、メーリングリストへ送信した場合など、メールの再配送条件によってはいずれでも失敗する場合があります。こうした状況では、DMARCのポリシーを強化せず、メーリングリスト機能の見直しやARC（Authenticated Received Chain）の導入などで回避できないかを検討してみてください。

利用者への周知

送信ドメイン認証技術の導入にあたり、利用者に周知しておくべき点がいくつかあります。

メールを送信する際に、例えば、会社のメールアドレスを用いて、自宅で契約しているインターネットサービスプロバイダからメールを送信する場合、送信されるメールはそのドメインのメールを許可されているサーバ以外からの送信となるため、受信側でなりすましと判断されてしまうことがあります。従って、このような方法でのメール送信は行わないように周知することが必要です。また、DMARCレコードで強いポリシー（p=reject）を設定する場合は、認証が失敗した場合にポリシー通りに受信を拒否される場合がありますので、事前にDMARCレポートを参照するなど、認証失敗が無いことを十分に確認しておくことが必要です。さらに、メール利用者に、DMARC認証が失敗するメールを送信しないよう周知しておくことも必要となります。



同意の取得

送信ドメイン認証技術の導入にあたり、あらかじめ利用者に同意を得ておくべき事項があります。

送信ドメイン認証技術は、受信側メールサーバにおいて電子メールの送信ドメインを認証し、その結果に基づいてフィルタリング等の措置を講じるためのものですが、その過程で利用者へのメールを確認することとなるため、電気通信事業法にも定められている通信の秘密の保護との関係で問題が生じないように実施する必要があります。

現在、総務省において、認証等の処理のそれぞれの段階について、以下のように整理されており、この範囲内で実施することが可能です。

① 送信ドメインを認証し、その結果をラベリングすること

→大量送信される迷惑メールにより生じるサービス遅延等の支障のおそれを減少させるための正当業務行為として実施可能

② ラベリングされた結果に基づき、フィルタリングを行うこと　及び

③ DMARCにおいて、レポートを送付すること

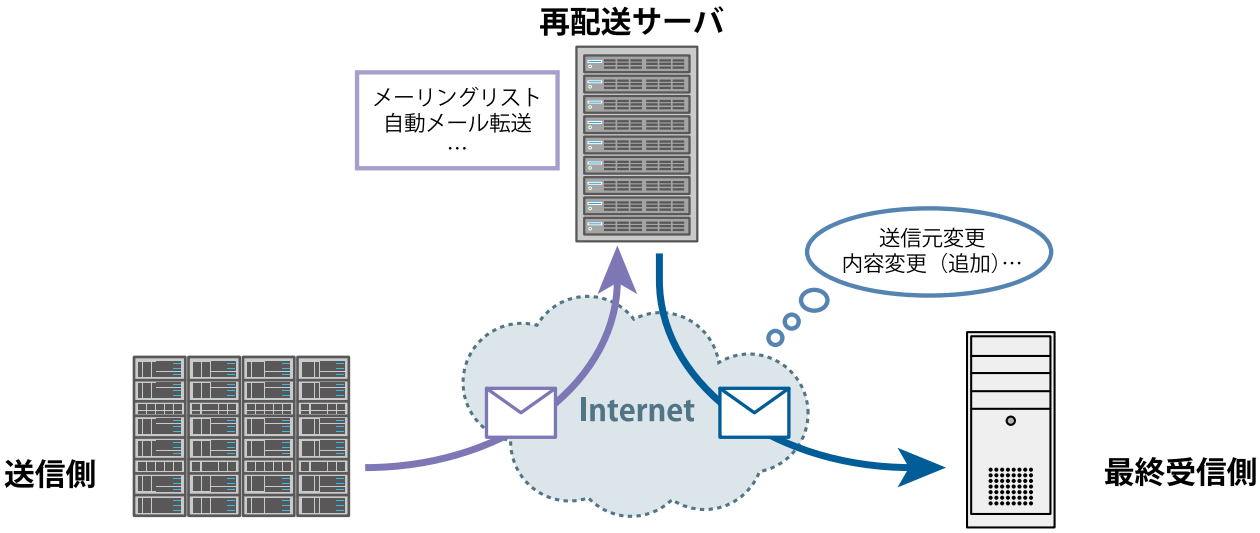
→事前に利用者に対して十分な説明を行うことや、事後的に利用者が任意に同意を撤回できることなどの一定の要件を満たす場合、約款等で利用者の同意を取得することで実施可能
（ただし、レポート内容にメール本文及び件名が含まれないことが前提とされています。）

送信ドメイン認証と通信の秘密の保護の関係については、総務省webサイトで詳細に説明されていますのでそちらを参照してください。

※総務省サイト　http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html

注意点

DMARCで正しく認証できない条件には、何らかの設定間違いによって、SPFとDKIMの両方の認証が失敗する場合と、いずれかで認証できたとしても、メールヘッダ（From:）上の送信者のドメインと異なる場合とがあります。さらに、最初にメール送信したときにDMARCが正しく認証できたメールであっても、メール転送やメーリングリストを経由するメール再配送時には正しく認証できないことがあります。



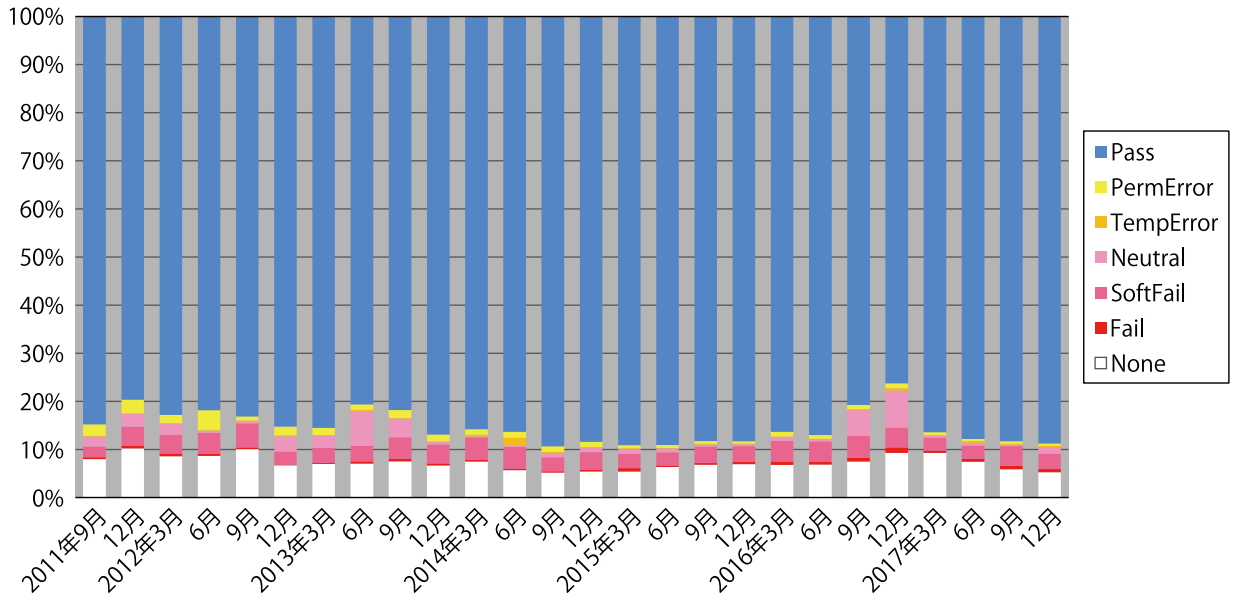
自動メール転送をすると、転送先では直近のメール送信元が最初のメールサーバと異なりますので、SPF認証が失敗します。この場合、最初に送信するメールがDKIMを導入していれば、DKIMとしては認証できますので、DMARCでも認証することができます。メール転送される可能性がある場合には、DKIMの導入も合わせて実施することが必要となります。

メーリングリストサーバでは、リストメンバへの再配送時にメールの表題（Subject:ヘッダ）に通し番号などの情報を追加する機能がよく使われます。この場合、メール情報の改変となりますので、DKIMの署名があわず認証が失敗します。また、SPFについても、メール配送上の送信者がメーリングリストのドメインを利用する場合が多いので、この場合にはSPFの認証はできても、認証したドメインと、メーリングリストに投稿された送信者のドメインが異なりますので、DMARCとしては認証が失敗します。こうしたメーリングリストの問題に対しては、メーリングリスト機能でメールを改変しないようにするか、ARC（Authenticated Received Chain）などの新しい技術の導入が必要になります。

普及状況

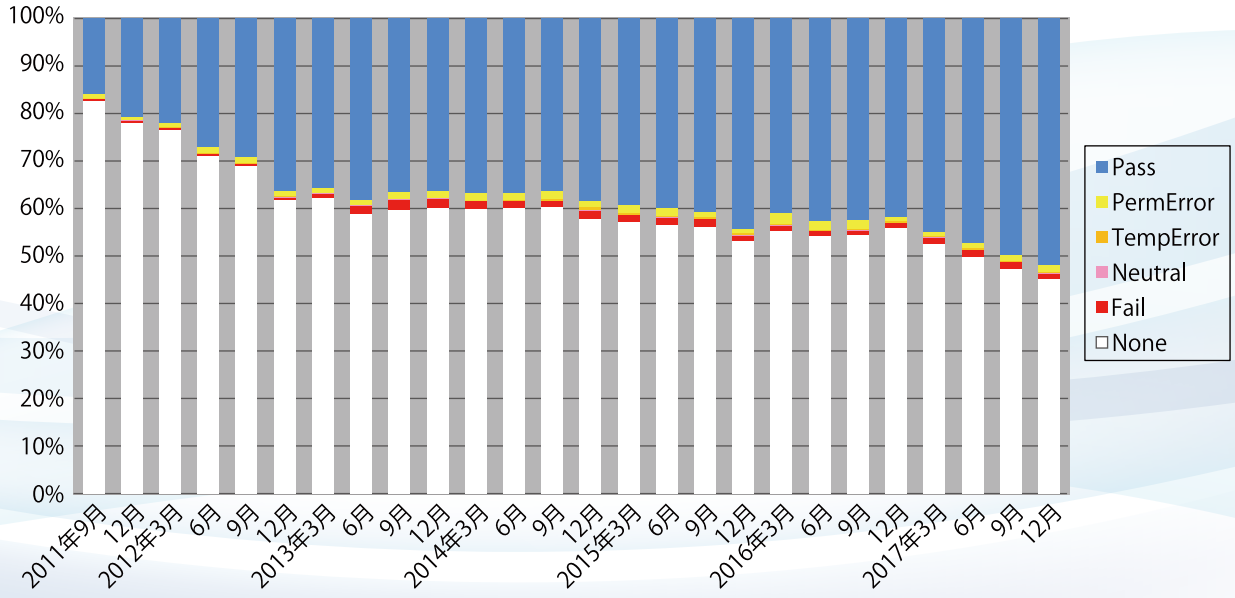
わが国で実際に流通しているメールでのネットワーク方式の送信ドメイン認証技術（SPF）への対応状況についての調査では、約９割のメールがSPFを導入していることがわかります。一方、電子署名方式の送信ドメイン認証技術（DKIM）への対応状況についての調査では、約５割のメールがDKIMを導入していることがわかります。DMARCで正しく認証するためにも、DMARCに加えてDKIMも今後のさらなる普及が期待されます。

実際に流通している電子メールにおけるSPFの対応状況



（出典）電気通信事業者7社の協力により総務省作成

実際に流通している電子メールにおけるDKIMの対応状況



（出典）電気通信事業者4社の協力により総務省作成

参考資料

関連RFC

RFC4954	SMTP Service Extension for Authentication SMTPでの送信者の認証方式であるSMTP-AUTHの標準規格
RFC5321	Simple Mail Transfer Protocol 電子メールのプロトコルであるSMTPの標準規格
RFC5322	Internet Message Format 電子メールの形式に関する標準規格
RFC6376 STD76	DomainKeys Identified Mail（DKIM）Signatures 送信ドメイン認証技術の一方式であるDKIMの標準規格
RFC7208	Sender Policy Framework（SPF）for Authorizing Use of Domains in Email, Version 1 送信ドメイン認証技術の一方式であるSPFの標準規格
RFC7489	Domain-based Message Authentication, Reporting, and Conformance（DMARC） 送信ドメイン認証技術DMARCの事実上の標準規格
RFC7601	Message Header Field for Indicating Message Authentication Status 認証結果のヘッダーへの記録方式の標準規格

Messaging, Malware, Mobile Anti-Abuse Working Group（M³AAWG）

迷惑メール対策等に関わる各種ベストプラクティスを公表
https://www.m3aawg.org/published-documents

一般財団法人インターネット協会

送信ドメイン認証技術を含む迷惑メール対策の技術紹介などを提供
http://salt.iajapan.org/wpmu/anti_spam/

一般財団法人日本データ通信協会 迷惑メール相談センター

プロバイダ等での送信ドメイン認証技術の導入状況を公表
https://www.dekyo.or.jp/soudan/contents/auth/

迷惑メール対策推進協議会（本協議会）

迷惑メール対策に関連する資料を公表
https://www.dekyo.or.jp/soudan/contents/anti_spam/

総務省　電気通信消費者情報コーナー　迷惑メール対策

迷惑メール対策に関する法制度等に関する資料を公表
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html

迷惑メール対策推進協議会 Anti-Spam mail Promotion Council

事務局　一般財団法人日本データ通信協会　迷惑メール相談センター
（本件に関するお問い合わせ先）q-meiwaku-mail-kyogikai@dekyo.or.jp

2018年６月
一般財団法人
日本データ通信協会
Japan Data Communications Association