第4章　送信ドメイン認証技術導入手順

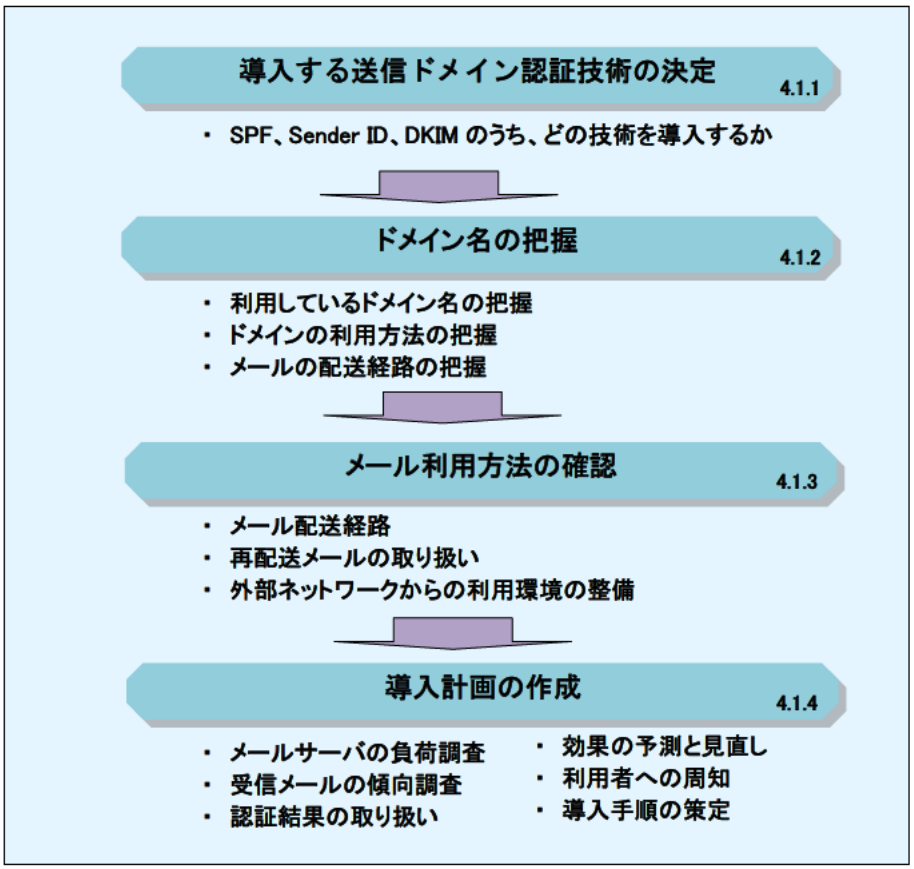
第４章　送信ドメイン認証技術導入手順

送信ドメイン認証技術は、メールの送信側と受信側の双方が協調することによって成り立っています。送信ドメイン認証技術は、既存のメール配送の仕組み（SMTP）に直接影響を与えることなく下位互換的に導入することができますので、メールの送信側と受信側のどちらの立場からでも導入することができます。

本章では、送信ドメイン認証技術の導入に際し、事前に検討しておくべきことや、それぞれの送信ドメイン認証技術について、送信側と受信側のそれぞれの側での実際の作業内容、導入後の運用にあたり注意すべき点などについて解説します。

4.1　事前準備

送信ドメイン認証技術の導入に際し、予め検討しておくべき事項がいくつか存在します。どの技術を導入すべきか、送信側と受信側のどちらから導入すべきか、導入の時期をどう判断するか、という基本的な検討のほか、 送信ドメイン認証技術を正しく機能させるためのメールの運用部分についても検討が必要です。



図表４－１　事前準備

例えば、メール送信側として、送信ドメイン認証技術を導入したにもかかわらず、それが正しく運用されなければ、送信者情報を偽装していないにもかかわらず認証が失敗するようなメールが流通してしまう可能性があります。そのようなメールが多くなれば、そのドメイン名自体の信用も失われてしまう可能性があります。

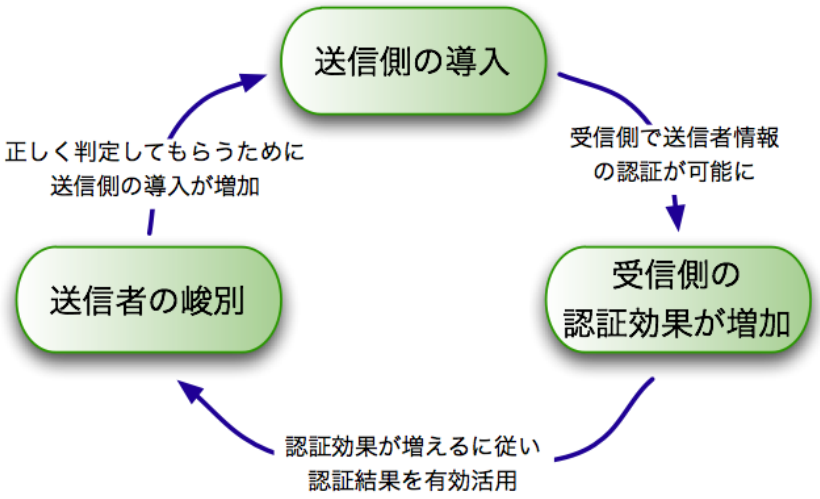
また、メールの受信側では、送信ドメイン認証技術を利用することにより得られた認証結果をどのように利用すべきなのかを考える必要があります。そのためには、実際のメールの配送形態でどのような認証結果が得られる可能性があるのかを正しく理解し、これらメール配送の事情に合わせた検討が予め必要になります。

以下では、送信ドメイン認証技術の導入にあたり、事前に検討すべき内容について具体的に解説するとともに、それらが送信ドメイン認証技術において、どのような意味があるのかについて補足して説明します。

4.1.1　導入する送信ドメイン認証技術の決定

前述のとおり、送信ドメイン認証技術では、メールの送信側と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、送送側と受信側の双方での導入が同程度進むことが望ましいものです。

導入のための費用は導入する技術によって差があり、技術によっては送信側ではほとんど費用がかかりませんが、いずれの技術でも、受信側での導入には受信時に認証するという新たな機能の追加が必要になるので、新たに費用か発生することになります。そのため、まず送信側の導入を増やすことによって、受信側での認証可能なメールの割合を高め、導入効果が得られやすい環境を作ることが普及を進めていくために必要となります。



図表４－２ 普及のサイクル

送信ドメイン認証技術のうち、送信側の導入費用が低い技術は、ドメインを管理するDNS 上に、導入時に SPF レコードを記述すればメールの送信ごとの処理が不要なSPF/SenderID です。そのため、導入費用の低さからも、まず SPF/SenderID の送信側の

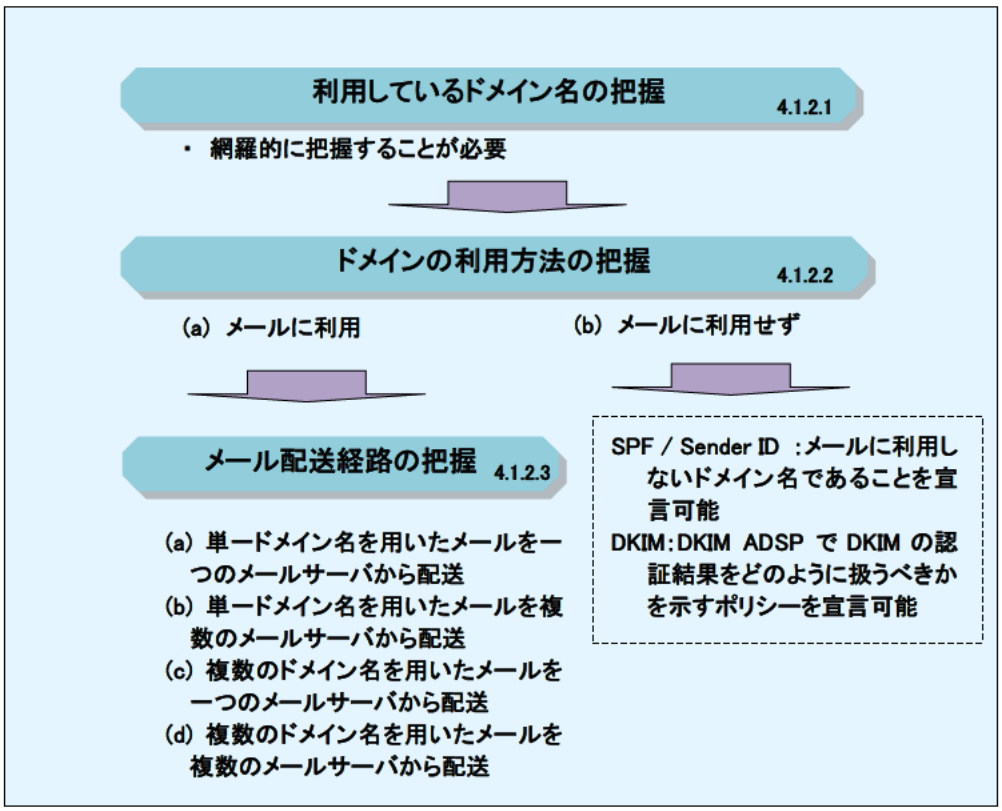
導入は、全てのドメインにおいて実施すべきです。実際に幾つかの導入状況の調査結果からも、SPF レコードの宣言率が高く、SPF/SenderID の送信側の導入が進んでいることが分かります。

受信側については、SPF レコードの宣言率が高いことから、SPF/SenderID の認証機能の導入が効果が得やすいでしょう。SPF と SenderID では、送信者情報の種類に違いがありますが、SPF レコードの形式はバージョン番号を除いて同じですので、可能であれば SPF/SenderID の両方の認証ができる機能の導入が望ましいと考えられます。

DKIM については、送信側の導入にあたっても、 SPF/SenderID に比べて導入のための費用はかかりますが、メールの送信者情報が詐称されているかどうかを認証する以外にも、メール本体が改変されていないことの判別もできること、電子署名というメールの配送経路に依存しない技術を利用するため、配送経路上の各メールシステムに変更を加えることなく多くの利用局面で利用できることなど、SPF/SenderID にはない利点があります。そのため、DKIM の導入については、送信するメールの重要度や受信しているメールに係る送信側での DKIM の導入割合などを考慮し、導入を進めるべきです。

4.1.2　ドメイン名の把握

次に、自組織内で利用しているドメイン名を把握しなければなりません。具体的には、利用しているドメイン名の把握、ドメインの利用方法の把握、メール配送経路の把握が必要です。



図表４－３　ドメイン名の把握

4.1.2.1　利用しているドメイン名の把握

まず、自組織内で利用しているドメイン名自体を正しく把握しなければなりません。

その際、メールに利用しているドメインについて把握することはもちろんですが、それ以外に、ドメイン名の構造上存在する上位ドメインや、メール以外の用途に使っているDNS で参照可能なドメイン名についても確認することが必要です。

4.1.2.2　ドメインの利用方法の把握

ドメイン名を把握したあとは、それぞれのドメインの利用方法を確認しなければなりません。

ドメインの利用方法は、メール利用の観点からは、大きく以下のように分類することができます。

(a) メールに利用しているドメイン名
(b) メールに全く利用していないドメイン名

(a) については、メールの配送経路を把握すること、適切な送信ドメイン認証技術の送信側の設定をすることが必要です。メールの配送経路の把握については、4.1.2.3 を参照して下さい。

(b) については、SPF / Sender ID では、メールに利用しないドメイン名であることをSPF レコードで宣言することができます。この設定方法の詳細については、3.2.3 を参照してください。DKIM では 、DKIM ADSP でDKIM の認証結果をどのように扱うべきかを示すポリシーを宣言できます。例えば、電子署名が付与されていないメールを破棄するような方針 (discardable) を宣言することで、勝手にドメイン名を利用するようなメールを防ぐことができます。DKIM ADSP については、3.4.6 を参照してください。

4.1.2.3　メールの配送経路の把握

次に、メールに利用しているドメインについて、そのドメインを用いて送信されるメールの外部への配送経路を把握しなければなりません。

配送される形態としては、大きく分けて、次の４つが考えられます。

(a) 単一ドメイン名を用いたメールを一つのメールサーバから配送
(b) 単一ドメイン名を用いたメールを複数のメールサーバから配送
(c) 複数のドメイン名を用いたメールを一つのメールサーバから配送
(d) 複数のドメイン名を用いたメールを複数のメールサーバから配送

(a) の場合には、そのドメインを利用するメールの出口（メールサーバ）が一つのメールサーバであることを、利用する送信ドメイン認証技術を用いて設定することになります。

(b) の場合としては、送信効率を上げるために複数のメールサーバを利用しているような場合や、同じドメイン名を利用した特定のメールの配信を外部委託しているような場合があります。この場合にも、利用する送信ドメイン認証技術で、それぞれの送信側のメールサーバが、そのドメインから配送されるメールの正しい出口（メールサーバ）であること

を設定できます。

(c) の場合としては、メールの利用目的別に複数のドメインを併用している場合や、組織ごとにサブドメインを利用しているものの、全体の規模としてそれほど大きくないために、メールサーバを集約している場合などが考えられます。また、メールサービスを外部の複数の組織（ドメイン名）に提供している、いわゆるホスティングサービスの場合などもあります。さらに、(b) のメール配送業務を複数受託し、複数のドメイン名を送信者情報として利用する場合も、この形態に含まれます。

図表４－４　送信者情報の利用権限の確認

(d) の場合には、クラウドサービスを用いたホスティングに多く見られる形態で、複数のドメインで複数のサーバを共有している場合があります。また、(b) と (c) の組合せのケースもあります。これらの場合には、(b)、(c) における対応を組み合わせることで正しい設定が可能です。

4.1.3　メールの利用方法の確認

事前準備の最後に、メールの利用方針を決定

この場合には、それぞれのドメインが同じメールの出口を示すことで、受信側の認証に問題は生じません。

なお、いずれの形態であっても、メールが外部に配送される前に、そのメールで利用されるドメイン名の利用権限を送信者が適切に有しているかを、何らかの方法で確認することが必要です。この確認が適切に行われていないと、利用権限のない者がドメイン名を詐称して不正なメールを外部に配送することができてしまいます。こうしたことが行われると、送信ドメイン認証技術を設定していたことによって、受信側のメールサーバで、詐称されたメールの認証に成功してしまい、かえって問題となってしまいかねません。

しなければなりません。

具体的には、メールの配送経路の方針、再配送を行うメールの利用方針、複数のドメインを利用する場合の方針、外部ネットワークから利用する場合の方針のそれぞれについて決定が必要です。

4.1.3.1　方針検討の必要性

メールの送信に利用するドメイン名と、実際のメールの配送経路は、これまで比較的柔軟

に運用されてきました。しかし、迷惑メールがメール流量の大部分を占めるようになってきた現在では、正しいメールが適切に受信できるようにするために、メールの利用方針を適切に決定し、運用することが必要です。

送信ドメイン認証技術が適切に機能するようにするためには、正規に送信されるメールが、送信側で利用するドメイン名に対応した正しい出口（メールサーバ）からのみ配送されるようになっていることが重要になります。

技術革新に伴い、メールの利用形態は多様化してきています。例えば、携帯電話の通信網を利用したデータ通信端末や無線 LAN のアクセスポイントなどモバイル環境は急速に普及してきており、それに伴い、これらの回線を利用したメールの利用も増えてきています。

また、業務として利用するメールや、個人で利用しているメール、ウェブメールなどアクセス端末をあまり選ばずしかも無料で利用可能なメールなど、同一の個人が複数のメールアドレスを利用するようになっています。

こうしたメールの利用形態の多様化を踏まえ、それぞれのドメインごとにメールが適切に受信できるようにするための対応が必要となりますが、それについては、技術的に対応可能な部分や、利用方針に基づく運用によるべき部分もあります。

以下では、メールの利用方針を決定し、それに基づく運用を適切に行う必要がある部分として、次の点について、詳細に検討します。

- メールの配送経路（4.1.3.2）
- 再配送メールの取り扱い（4.1.3.3）
- 外部ネットワークからの利用環境の整備（4.1.3.4）

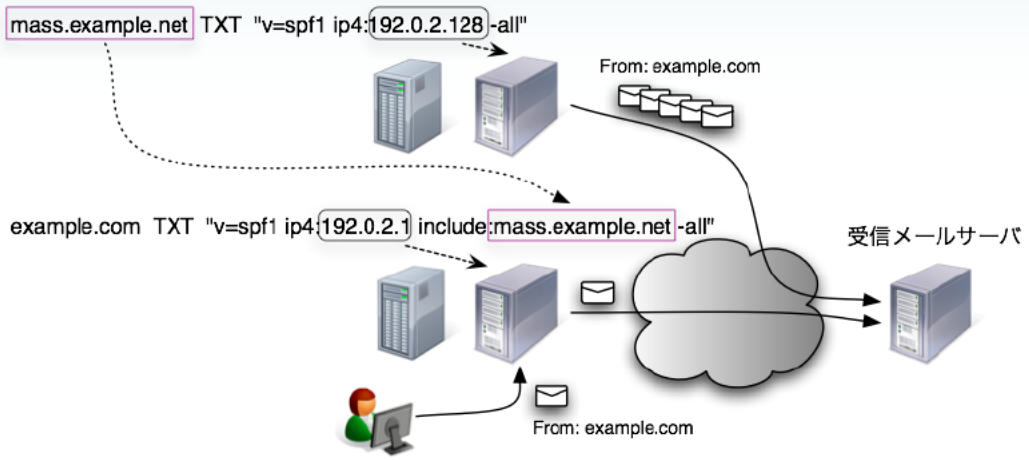
4.1.3.2　メールの配送経路

メールの利用形態としては、（典型的なものとして）１対１のコミュニケーションを目的としたものがあります。そのような場合には、送信に用いられるメールサーバが特定できますので、送信ドメイン認証技術の導入にあたっても、そのメールサーバを利用ドメイン名の出口（メールサーバ）として設定することになります。

メールの利用形態には、そのような一般的なメール配送以外にも、顧客へのアナウンスや特定の参加者への連絡網といった多数の宛先への一斉送信などがあります。メールの大規模配信を行う場合には、送信中に通常のメールが阻害されたりすることがないように専用のメールサーバを利用することがあります。また、こうした配送処理を効率よく行うために、専門の外部事業者へ委託することがあります。これらの場合に利用する送信者情報のドメイン名については、次の２つの考え方があります。

(a) 大量送信用の専用ドメイン名を利用
(b) 通常のメールと同じドメイン名を利用

(a) としては、サブドメインを新たに作成する場合や、別のドメイン名を取得する場合などが考えられます。この場合には、専用ドメイン名を使って配送する出口（メールサーバ）を特定し、それぞれのメールサーバで適切な送信ドメイン認証技術を導入することになります。



図表４－５　大量送信用の専用ドメインを利用する例

(b) には、メールの受信側にとって同じ組織からのメールであるという印象を強く受けるため、信用度が比較的高くなるといった利点があります。その場合には、大量送信されるメールは、通常のメールとは配送出口（メールサーバ）が異なりますので、そのドメイン名に対する送信ドメイン認証技術の設定に、これら大量送信を行うメールサーバを追加する必要があります。

例えば、SPF / Sender ID の場合には、SPF レコードに、これら大量送信を行うメールサーバを追加することになります。大量送信を行うメールサーバの管理が別組織で行われていたり、外部委託されたりしている場合には、それら実際の管理元で別のドメイン名で SPF レコードを宣言してもらい、それを "include" などの機構を使って取り込むことができます。これにより、大量送信を行うメールサーバが追加されたり、何らかの事情で IP アドレスが変更されたりした場合でも、通常のメールサーバのドメイン名の管理側にその都度連絡をすることなく、独立して運用することができます。

DKIM の場合には、電子署名の作成に利用する秘密鍵の管理の問題がありますので、外部委託している場合で秘密鍵を共有できる関係にないときなどには、(b) の方法を採ることはできず、署名ドメイン自体を別ドメインとし、それぞれで鍵の管理と運用を行うことが必要になります。

4.1.3.3　再配送メールの取り扱い

これまで利用されてきたメール利用形態の一つに、メールを一旦受信した後、外部へ再配送するような場合があります。具体的には、メールを転送するときやメーリングリストで再送するときなどです。これらの再配送処理にあたっては、送信ドメイン認証技術として考慮しなければならない事項があります。これらは、それぞれの送信ドメイン認証技術で、影響の受け方や対処方法が異なりますので、4.2 で解説します。

いずれの技術を利用する場合でも、再配送を行う際には、メール受信時に事前に認証を行い、その認証結果をメールヘッダに記録し

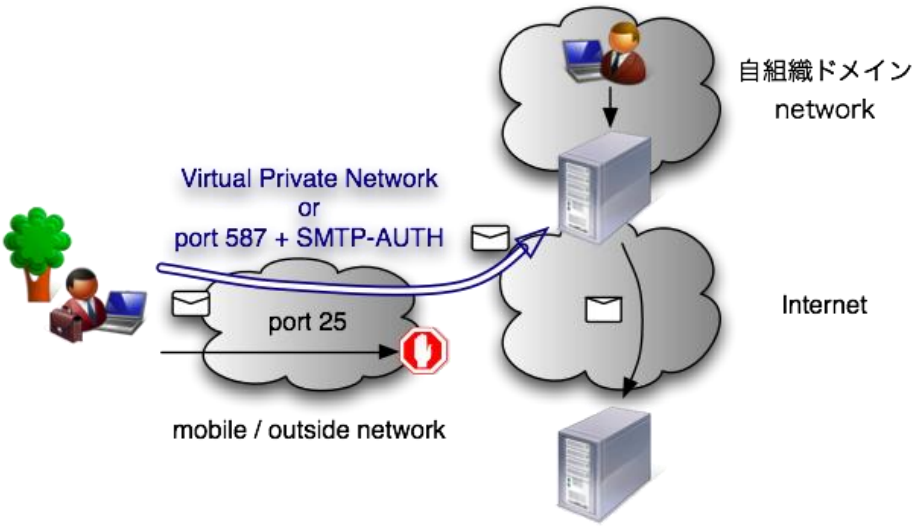
た上で再配送したり、正しく認証できたメールだけを再配送したりするなどの考慮が必要です。

4.1.3.4　外部ネットワークからの利用環境の整備

モバイル環境や社外滞在先など、外部ネットワークからメールを送信することがあります。

自組織で運営している送信用のメールサーバは、通常、セキュリティ上の観点からファイアーウォールなどを用意し、インターネット側から直接通信ができないような内部ネットワークに設置されています。そのため、外部ネットワーク上からメール送信を行うことを可能とするためには、別途 VPN などの通信手段を用意し、内部ネットワークにアクセス可能にする方法や、外部ネットワークからアクセスできる位置に送信メールサーバを用意する方法などがあります。

このような場合には、ネットワーク接続に利用している回線が OP25B を実施している可能性がありますので、メール配送に使われる 25 番ポートではなく、メール投稿用の 587 番ポートを使えるように設定することが必要です。また、送信者を正しく識別するために、SMTP AUTH (送信者認証) による認証を行うべきであり、認証方式についても、パスワードがそのままネットワークに流れない方式 (例えば CRAM-MD5 など) を利用すべきです。



図表４－６　SMTP AUTH による認証

最近では、ホテルなどの環境でもインターネット接続サービスが提供されるようになってきていますが、これらの環境では特に注意が必要です。

特に、欧米のホテルなどでは、ネットワークの不正利用を防ぐ目的で、メール配送に使われる 25 番ポートを用いて直接インターネットへの通信ができず、一度アプリケーション型のファイアーウォールなどで通信が終端されていることがあります。そのため、外部からアクセス可能な送信用メールサーバを用意している場合で、MUA からは通常どおり送

信が行われたように見えても、実際には自組織の送信用メールサーバを経由せず、ホテルなどが用意しているファイアーウォールから送信される場合があります。この場合には、メールの受信側では、受信したメールが、そのメールのドメインの本来の出口（メールサーバ）から送信されているメールではないために、認証が失敗することがありますので、注意が必要です。

4.1.4　導入計画の作成

送信ドメイン認証技術の導入に際しては、技術自体の違いやそれに関連した運用上の特徴以外に、より実際的な側面についても検討し、具体的な導入計画を作成することが必要です。

その検討の際には、以下に挙げた観点が参考になるでしょう。

(a) メールサーバの負荷調査
(b) 受信メールの傾向調査
(c) 認証結果の取り扱い
(d) 効果の予測と見直し
(e) 利用者への周知
(f) 導入手順の策定

4.1.4.1　メールサーバの負荷調査

メール送信側に DKIM を導入する場合や、メール受信側で認証を行う場合には、メールサーバに新たな機能を追加することが必要です。この機能追加により、メールサーバの負荷が高くなりますので、導入前には既存のメールサーバの負荷状態を把握することが必要です。CPU などのリソースの負荷は、いずれの技術を導入する場合でも高くなります。また、受信側で認証を行うことにより DNS の参照回数が増えるため、ネットワーク帯域や DNS のキャッシュサーバの負荷などの考慮も必要になります。

一般にメールの流量は、時間帯によってばらつきがありますし、ピーク時に極端に負荷が高くなる場合もあります。導入に際しては、予め一定の期間の負荷状況を計測し、予想される負荷の上昇分を重ねた上で、設備設計を行うことが必要です。

4.1.4.2　受信メールの傾向調査

受信側では、広く受信メールの傾向を調査することによって、導入する技術の判断に役立てることができます。例えば、既に送信者情報を詐称したメールに困っている場合や、取引先など受け取るべきメールが把握できている場合には、認証の効果を予め予測することができます。予め受け取るべきメールが明確である場合は、それらのメールの送信側で導入している技術を受信側でも導入するべきです。

送信側についても、受信側で認証している技術が予め分かる場合には、導入に際して、参考となるでしょう。

4.1.4.3　認証結果の取り扱い

受信側では、認証の結果の利用方法も予め決めておくことが必要です。メールヘッダに認証結果を示すだけなのか、認証が成功した特定のドメインをホワイトリスト的に優先的に配送するのか、誤認証の可能性がないドメインで認証が失敗した場合に隔離するのかなど、認証結果を有効利用する方法はいくつか

あります。受信メールの傾向調査と合わせて、それぞれの認証結果と送信元のドメインに応じた、効果的な取り扱いの方針を決めることになります。

また、メールは多様な用途で用いられるため、メールシステム全体で一律に適用できない認証結果に基づいた処理も、個々のメール受信者が MUA などで個別に設定することにより、認証結果を有効に利用できる場合があります。メールサービス提供者やメールシステムの管理者は、こうした設定例などをマニュアル等で利用者に周知すると良いでしょう。

4.1.4.4　効果の予測と見直し

受信側では、事前に受信メールの調査を行うことにより、認証による効果を予測することができます。また、送信ドメイン認証技術を導入するメールサーバは、今後も増えてくることが予想されますので、導入時だけでなく、継続してメールの傾向を把握することが有効です。これは、導入時には見送った技術がより機能するようになっていたり、認証結果をより効果的に活用できるようになっていたりするなどによるものです。

4.1.4.5　利用者への周知と導入手順の策定

送信ドメイン認証技術を導入する際には、予めメールの利用者に対して、送信側及び受信側での運用ポリシーを事前に説明しておくことも必要です。特に送信側の利用ポリシーについては、送信ドメイン認証技術の対象としているドメイン以外のドメインを送信者情報として利用しないよう周知しておくことが重要です。メールの受信側で認証が失敗するような使い方をしてしまうことによって、そのドメインやメールの送信元の評価が低下してしまう可能性があります。

また、メールは絶え間なく送受信されていることから、メールシステムへの送信ドメイン認証技術の導入やそれに基づく新たな機能追加、仕様変更などは、頻繁にできない場合もあります。このため、手順を決めて、計画的に導入を進めることが必要です。

さらに、メールを送受信している相手の導入状況も変化していきますので、日頃のメール送受信の状況の把握とともに、その結果に基づいた新たな機能追加や仕様変更などの見直しについて、予め計画を立てることも必要となります。

4.2　一般的な導入手順

送信ドメイン認証技術には、ネットワーク方式の SPF/SenderID と、電子署名方式の DKIM の二つの技術があります。それぞれの技術についての概要、導入に際しての注意点については、第 3 章で解説しています。

ここでは、一般的な導入手順について、送信側での対応を中心に、それぞれの技術ごとに解説します。また、導入に際して既存のメールの使われ方との関係や、問題が生じる場合の対処方法について解説します。

4.2.1 SPF/SenderID

SPF と SenderID は、送信者を認証するために送信元の IP アドレスを利用するネットワーク方式であること、認証のために送信側のドメイン (DNS) 上にある SPF レコードを利用するなど、多くの共通点があります。ここでは、両方の技術について、導入手順のほか、そのままでは認証がうまくできない課題と対処方法などについて解説します。

4.2.1.1 SPF/SenderID の導入手順

SPF/SenderID を送信側に導入するためには、対象とする送信者情報のドメインに対して SPF レコードを宣言することが必要になります。

DNS サーバを自組織で管理している場合や、運用を委託しているサービスで、DNS の資源レコードをある程度自由に編集できるような場合には、4.1.3.2 で示したようにメールの配送経路 (出口) を正しく把握した後、それをもとに SPF レコードを記述することになります。この場合、送信側の導入に際して特別な費用は発生しません。

メールの運用自体を外部委託している場合や ISP のメールサービスを利用している場合には、第 5 章以降を参考に、それぞれ設定して下さい。なお、DNS の運用を外部委託していて、自由に編集が行えないような場合には、委託先に SPF レコードの設定依頼が必要になりますので、送信側の導入に際し、費用が発生する場合があります。

SPF/SenderID を受信側に導入し、メールの受信時に認証するためには、受信メールサーバへの新たな機能追加が必要になります。すなわち、受信側での認証を行うためには、送信元の IP アドレスが必要になりますので、原則として、外部から直接メールを受けるサーバ上に認証機能を追加する必要があります。例えば、迷惑メールフィルタ機能を提供するサーバで、送信ドメイン認証機能も提供するものがありますが、その機能を用いるためには、そのサーバが外部からのメールを直接受ける位置にあるかどうかの確認が必要です。

オープンソースの MTA として広く使われている Sendmail や Postfix では、MTA の拡張機能を外部プログラムとして追加できるように、milter インターフェースが標準で提供されています。この milter インターフェースを利用した認証機能を実現するものが、同様にオープンソースとして公開されていますので、それを利用することもできます。

商用のメールサーバを利用している場合や外部のメールサービスを利用している場合には、その開発元やサービス提供元に問い合わせて下さい。その場合には、認証機能の追加には、新たに費用が発生する可能性がありますので、確認が必要です。

図表４－７ SPF/SenderID の導入

4.2.1.2 課題と対策

ネットワーク方式の送信ドメイン認証技術は、メールの再配送時に認証が失敗してしまうという問題があります。これは、メールの再配送時に、メールを一旦受け取った後、送信者情報をそのままにして、新たな受信者へメールを再配送してしまうことに起因する問題です。

具体的な事例としては、メール転送や古い実装のメーリングリストサーバで発生することがわかっています。

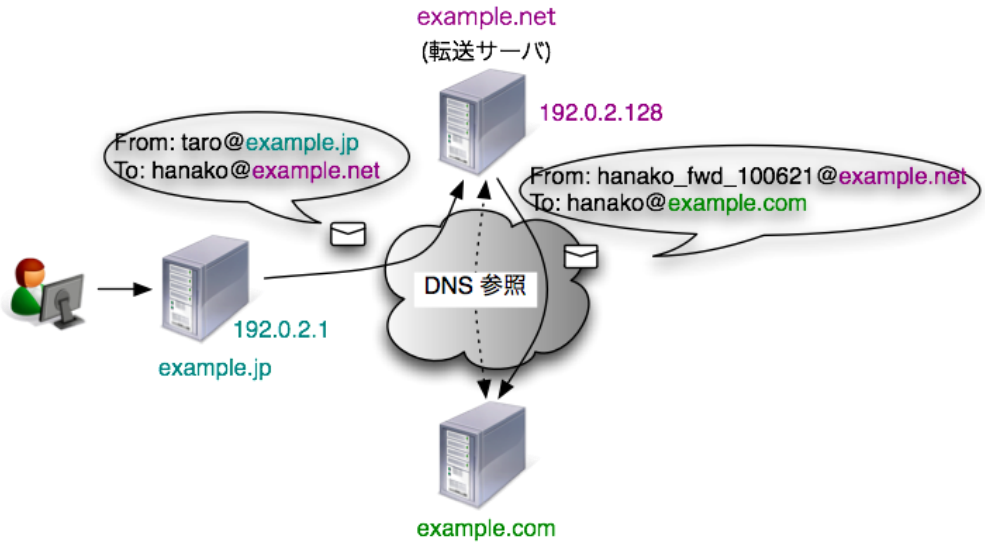
図表４－８ メール再配送による認証失敗の例

この問題を回避するには、メールの再配送時に、送信者情報をメールの再配送元のドメインに書き換える必要があります。

現時点でそれほど広く運用されているものではありませんが、メールの転送に関しては、以下の方法を用いることで、転送先でも正しく認証を行うことができるようになります。

まず、SPF の場合には、リバースパスを送信者情報として認証しますので、転送時に認証が失敗しないようにするために、転送を行う際のリバースパスとして、元の送信者のリバースパスを利用するのではなく、転送元（転送者）のドメインを含むメールアドレスを利用する方法があります。

この場合、転送時にすべてのメールのリバースパスを単純に書き換えてしまうと、メールがループする可能性がありますので、転送時に利用するリバースパスは、転送者のメールアドレスをそのまま利用するのではなく、例えば、図表４-9 のように、メールアドレスのローカルパート部分を工夫して、エラーメールとして戻ってきた場合や、さらに再転送されてきた場合に区別ができるようにすることが必要となります。このようにすることで、転送したメールが何らかの事情で戻ってきた場合に、さらに転送を繰り返さないことにより、不要なループを防ぐことができます。



図表４－９　メール転送への対応の例

Sender ID の場合には、送信者情報として PRA を用いて認証しますので、メールの転送時に、PRA で優先的に使われるヘッダ(Sender ヘッダなど)に、転送元のドメインを含んだメールアドレスを送信者情報として付加すれば問題ありません。

メーリングリストに関しては、リストメンバの管理のために、エラーメールの送信先を示すリバースパスには、メーリングリストの管理用のメールアドレスを指定するようになっています。そのため、SPF では、リストメ

ンバ側で認証が失敗するようなケースはほとんどなくなっています。

しかし、一部の古い実装のサーバプログラムのメーリングリスト機能では、PRA として From ヘッダより優先度の高いヘッダを付けないものがあり、そうした実装では、SenderID では、リストメンバ側で認証が失敗してしまいます。

このため、メーリングリスト機能を使う場合には、メーリングリスト側からメンバへの送信時に、Sender ヘッダなどにメーリングリスト管理用のメールアドレスを追加する機能を持った、最近の実装のサーバプログラムを利用することが推奨されます。

4.2.2 DKIM

DKIM では、送信者情報が正しく表明されているかどうかを、公開鍵暗号方式を利用した電子署名を検証することによって認証します。このため、ネットワーク方式とは異なり、メールの配送経路に影響を受けないという大きな利点があります。その反面、メールの送信側にも電子署名を作成して添付する負担が生じます。

ここでは、DKIM の導入手順のほか、運用上課題となる点について解説します。

4.2.2.1 DKIM の導入手順

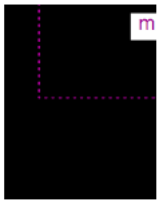
DKIM を送信側に導入するためには、メールの送信時に電子署名を作成し、それをメールヘッダ(DKIM-Signature) として追加する機能が必要になります。

SPF/SenderID と同様に、オープンソースの MTA である Sendmail や Postfix の milter インターフェースを利用することにより、DKIM の電子署名の作成機能を追加することができます。

DKIM では、電子署名の作成に公開鍵暗号技術を使いますので、予め電子署名を作成するときに利用する秘密鍵と、電子署名を検証するために利用する公開鍵を用意する必要があります。オープンソースの OpenDKIM プロジェクトでは、これら鍵のペアを作成するスクリプトプログラムもソースコード一式の中に含まれていますので、これを利用して鍵ペアを生成することもできます。商用のメールサーバを利用している場合や外部のメールサービスを利用している場合には、その開発元やサービス提供元に問い合わせて下さい。DKIM を送信側に導入するためには、新たに費用が発生する可能性がありますので、確認が必要です。

DKIM を受信側に導入する場合には、メールサーバに対して、電子署名を検証し、認証処理を行う機能の追加が必要になります。

この受信側の認証機能も OpenDKIM プロジェクトで提供されています。商用のメールサーバやメールサービスを利用している場合で導入を検討している場合には、提供元に確認が必要です。送信側への導入と同様に、新たに費用が発生する可能性がありますので、確認が必要です。

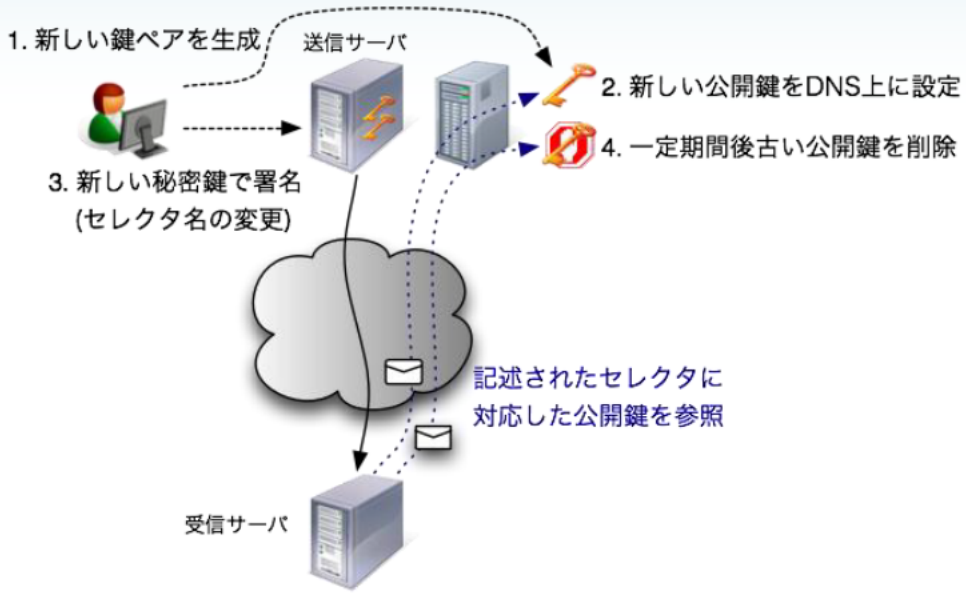


図表４－１０　メール転送への対応の例

4.2.2.2 鍵の管理と運用

DKIM の電子署名を作成するために必要な秘密鍵は、外部に漏れないようにきちんと管理しなければなりません。秘密鍵がわかってしまうと、認証に成功する DKIM の電子署名を第三者が勝手に作成できてしまうことになり、そのドメインに対する認証の意味がなくなってしまいます。

また、DKIM で利用する鍵のペアは、セキュリティ上の観点から、定期的に変更することが望ましいとされています。鍵のペアの変更にあたっては、公開鍵は、DNS の仕組みを利用してメール受信側に渡されますので、ある時期を境に鍵ペアを変更しても、 DNS の伝播の問題で正しい鍵の組み合わせにならない可能性があることに注意が必要です。この点については、DKIM では、3.4.2 で解説したように、同一ドメイン上に、セレクタを利用して複数の鍵を DNS 上に同時に公開することができますので、この仕組みを利用し、セレクタ値と、それが指し示す公開鍵に対応した秘密鍵を切り替えることにより、電子署名の作成に利用する鍵を見かけ上瞬時に切り替えることができます。以下に、鍵を切り替える手順を示します。



図表４－１１　鍵の切替え手順

新たに利用するセレクタ名は、予め取得できないように、なるべく予測しづらい名称（例えば、番号や続きが連想される名称は避ける）を利用すると良いでしょう。予め公開鍵がわかると、解読のための時間が増えることになり、危険性も増すおそれがあるからです。また、特別な事情がない限り、古いセレクタ名（鍵ペア）に戻すことはせずに、常に新しいセレクタを用意し続けるべきです。

このセレクタの仕組みをうまく活用すれば、例えば、ハッシュ長が短い SHA-1 を利用している場合でも、頻繁に鍵を変更していくことによって、ある程度のセキュリティを保つことができます。これにより、送受信側ともに、電子署名の作成・検証に必要となる処理能力を抑えることもできます。しかし、絶対に詐称されては困るような大事なメールには SHA-1 は利用すべきではありませんし、新たな攻撃手段が開発されて、より脆弱性が高まった場合にも利用すべきではありません。

4.2.2.3 課題と対策

DKIM では、メール本体の電子署名の対象となっている部分が改変されない限り、認証が失敗することはありません。逆にいえば、Subject ヘッダやメール本文にフッタ情報などを追加するようなメーリングリスト機能では、リストメンバでのメール受信時に認証が失敗する可能性があります。このような場合には、メーリングリスト側で投稿者からのメールを受け取るときに認証を行い、その結果も含めて DKIM で再署名するなどの対応が必要になります。

DKIM の課題として、もっとも難しいものは、電子署名のポリシーの問題です。DKIM では、認証の対象となるのは、正確には、送信者情報ではなく、署名者の情報になります。つまり、電子署名がないメール（署名者の情報がないメール）に対しては、認証が全くで

きないことになります。その結果として、受け取ったメールがたまたま電子署名の対象としていないメールだったのか、誰かが詐称して送ってきたメールなのかの判断ができないことになります。この点は、メールにもともと備わっている送信者情報を利用する SPF/SenderID と DKIM の大きな違いの１つです。

この問題に対応するため、DKIM には、3.4.6 で解説した DKIM ADSP の仕組みが追加されました。送信側で ADSP を表明することにより、送信する全てのメールに電子署名が添付されているはずなのか (dkim=all) 、一部だけなのか（dkim=unknown)を送信側が示すことができます。

しかし、この対応策については、まだ問題が残っています。3.4.6.2 で解説したとおり、ADSP を表明するのは、From ヘッダ上のメールアドレスのドメイン名のサブドメインですので、メール配信を請け負う事業者が、顧客のドメインを From ヘッダに利用し、実際の電子署名の作成を事業者側が行うような、いわゆる第三者署名をどう認証するのか、が問題となります。また、同様のケースとして、メーリングリストの問題もあります。

DKIM は、ドメインを自ら管理し、そのドメインを送信者情報及び署名者情報として使う場合には、とてもうまく機能しますが、メールの利用形態は多様化していますので、それぞれの使い方にうまく適合させるための工夫も必要になってきています。現在もこうした議論は続いておりますので、こうした問題をうまく解決し、適合できるようになることが期待されます。

4.3 運用

送信ドメイン認証技術を導入後にも、その効果を維持するために、日々正しく運用することが必要です。メールシステムの管理者は、受信側に必要とされるメールを正しく送信することにより、そのドメインの信頼性を高めていくことができます。また、送信ドメイン認証技術では、メールサーバだけでなく DNS も重要な役割になっていますので、DNS が正しく機能するような運用が必要になってきます。

4.3.1 メールサーバの運用

送信ドメイン認証技術は、送信者情報が詐称されているかどうかを認証する技術ですが、認証されたドメインが、必要なメールを送信しているドメインなのか、迷惑メールを送信するドメインなのかまでは判断しません。

そのため、受信側での迷惑メール対策としては、送信ドメイン認証技術による認証に加え、ドメイン自体を評価する仕組みが別途必要になります。

また、送信側では、送信ドメイン認証技術を導入しても、そのメールサーバから実際に迷惑メールが送信されてしまえば、ドメインの信用は低下してしまいます。そのため、せっかく送信ドメイン認証技術を導入したにもかかわらず、評判の悪いドメインだと判断されないように、関係のない第三者が勝手にメールサーバを利用できないようにきちんと設定し、管理することが必要になります。例えば、SMTP-AUTH のパスワードに安易な文字列を設定できないようにしたり、自らのメールサーバを利用するメール送信者の PC に不正プログラム (マルウェア) が混入されて

パスワードが漏洩しないようにしたりという対策を講じなければなりません。また、業務的なものを除いて短時間で大量にメールが送信されていないか、短時間で地理的に離れた場所からメール送信されていないかなどの監視等も必要になる場合もあります。

4.3.2 DNS の運用

送信ドメイン認証技術では、送信側から受信側へ伝える、認証に必要な各種情報を DNS を利用して受け渡しします。そのため、メールの送信側ドメインの DNS が常に正しく動作していることが必要です。

4.3.2.1 DNS の状態監視

送信側の DNS に何らかの問題があり、受信側で、SPF レコードや DKIM の公開鍵の情報が取得できなかった場合には、認証結果は temperror (一時的な失敗) となり、正しく認証できません。認証結果の temperror を受信側でどのように扱うかにもよりますが、送信側で送信ドメイン認証技術に関する情報を正しく設定していたとしても、利用している DNS が不安定だったり、何らかの問題があって正しく情報が引き出せない状態にあったりすると、場合によっては受信側で受け取ってもらえないことになり、送信ドメイン認証技術を導入していない場合よりも悪い結果となる可能性もあります。

また、送信側の DNS からの応答が遅かったり、応答を返さないなど不安定な状態にあったりする場合には、受信側での認証処理に負荷がかかる原因になります。特に、大量のメールを受けているメールの受信者には、深刻な問題となる可能性があります。 3.2.4.3 で解説したとおり、SPF や Sender ID での SPF レコードの記述方法で、DNS の参照回数に上限が決められているのも、受信側での認証時の処理を軽減させる意味が含まれています。

送信側のドメインの管理元は、DNS の状態を監視したり、きちんと運用体制が整っている外部のサービスプロバイダを利用したりするなど、 DNS の維持管理を心がけるべきです。

4.3.2.2 DNS の TTL

DNS では、問合せを高速に処理するために、キャッシュの仕組みがあります。このキャッシュの仕組みとその TTL は、SPF レコードや DKIM の公開鍵の変更時の伝播時間と密接な関係があります。TTL の値を大きくすることで、送信側ドメインの DNS へのアクセス回数を少なくする ことができますが、一方で SPF レコードや DKIM の公開鍵や DSP レコードを変更した場合に、受信側のメールサーバに反映されるまでに時間が長くなってしまいます。

送信側のドメインで、これら DNS 上の情報を変更する場合には、予め利用している DNS の TTL 値を把握したうえで、その時間に合わせて十分情報が伝播した後に、システムの変更や鍵の変更をする必要があります。DNS の TTL 値の変更が可能な場合には、前もって TTL 値を短い時間に設定しておくと、変更作業までの時間を短くすることができます。