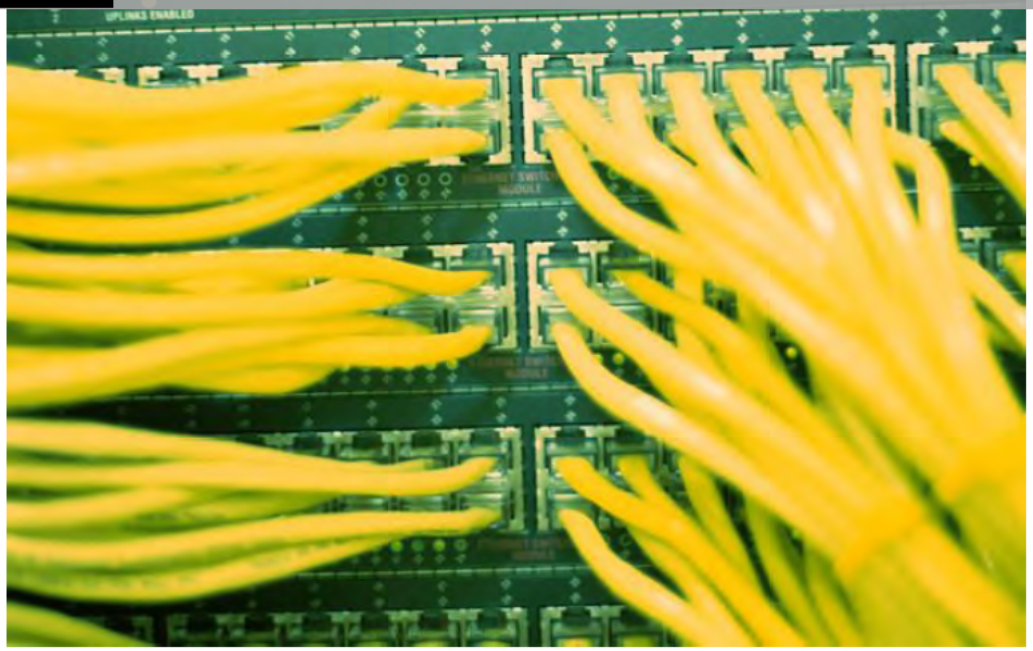
第６章　ホスティングサービスでの対応



第６章　ホスティングサービスでの対応

本章では、送信ドメイン認証技術を適用する際に、メールホスティングサービスを提供する事業者特有の対応方法、課題、解説などを示します。

サービス提供方法の違い、DNS サーバの管理の違いによるホスティングサービスの分類について、メールサービスに関連する DNS サーバについて、送信側・受信側の対応方法などについて、以下で解説します。

6.1　ホスティングサービスの分類

メールホスティングサービスとは、通信事業者や ISP・ASP 事業者（以下「ホスティング事業者」といいます。）が、自社設備を用いて、主に企業などにメール機能を提供するサービスです。このメールホスティングサービスは、メールサーバの割当てや DNS サーバの管理の状況により、それぞれ以下のように分類できます。

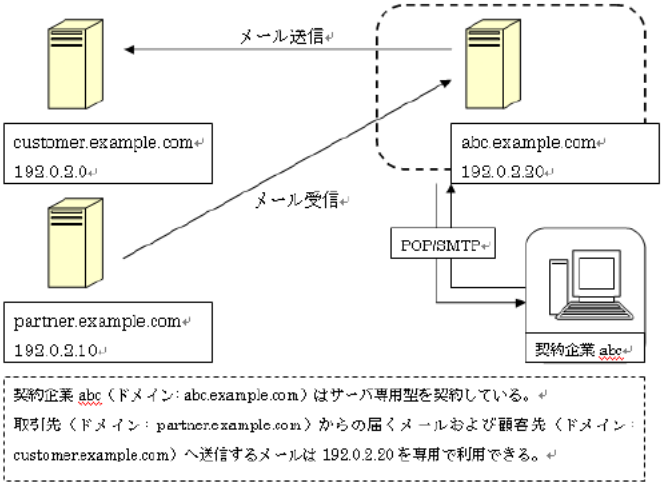
6.1.1　メールサーバによる分類

メールホスティングサービスは、メールサーバの割当てにより、「サーバ専用型」、「サーバ共用型」、「ゲートウェイ型」の 3 つに分類できます。

6.1.1.1　サーバ専用型

サーバ専用型は、１つの契約ドメイン（企業）に対して、１つ又は１つの集合体のメールサーバを「専用」で割り当てる形でメール送受信機能を提供するサービス形態です（図表６－１）。

割り当てられたメールサーバから送信されるメールは、すべて１つの契約ドメイン（企業）からのメールに限られます。

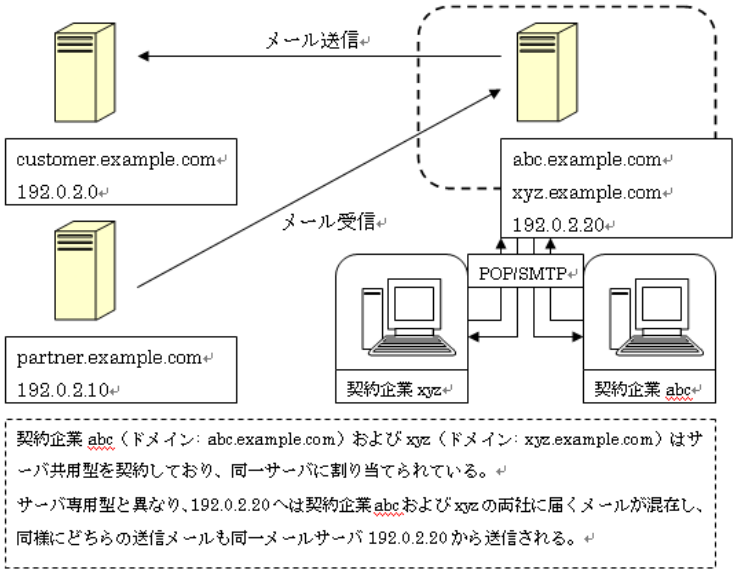


図表６－１　サーバ専用型のホスティング事業者の例

6.1.1.2　サーバ共用型

サーバ共用型は、複数の契約ドメイン（企業）に対して、１つ又は１つの集合体のメールサーバを「共用」で割り当てる形でメール送受信機能を提供するサービス形態です（図表６－２）。

専用型とは異なり、割り当てられたメールサーバから送信されるメールには、共用している他社ドメインからのメールも混在することになります。

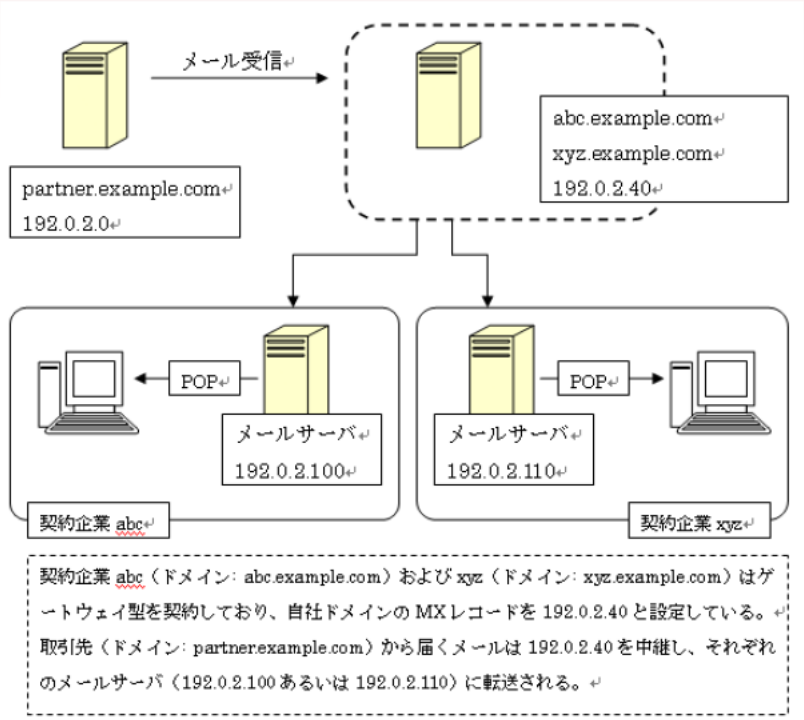


図表６－２　サーバ共用型のホスティング事業者の例

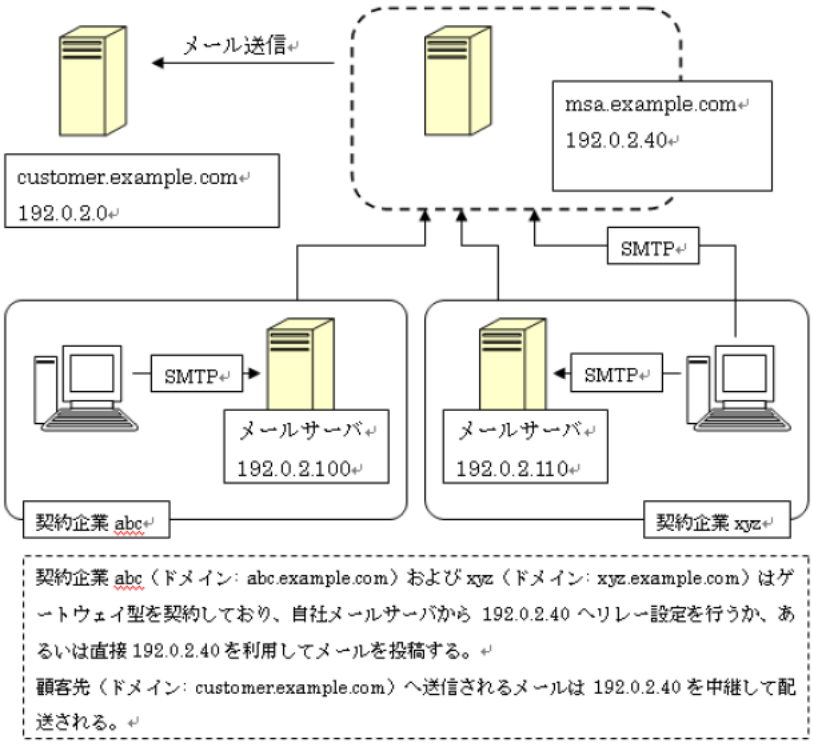
6.1.1.3　ゲートウェイ型

ゲートウェイ型は、契約ドメイン（企業）に対して、MX サーバやフィルタリングサーバ、投稿サーバを割り当てる形で、主に迷惑メール対策機能やウイルス対策機能、監査機能などを提供するサービス形態です（図表６－３、図表６－４）。

ゲートウェイ型のうち受信メールサーバの場合、ホスティング事業者はゲートウェイ用 MX サーバのみ提供し、メールデータを蓄積するメールボックス機能や投稿サーバなどの機能は提供しません。反対に、ゲートウェイ型のうち送信メールサーバの場合、契約企業のメールサーバが設定するリレー先サーバ（あるいは投稿サーバ）を提供し、MX サーバは提供しません。



図表６－３　ゲートウェイ型のホスティング事業者の例（受信）



図表６－４　ゲートウェイ型のホスティング事業者の例（受信）

6.1.2　DNS サーバによる分類

メールホスティングサービスは、DNS サーバの管理により、「DNS 自社管理型」、「DNS ホスティング型」、「DNS 提供型」の 3 つに分類できます。

6.1.2.1　DNS 自社管理型

DNS 自社管理型は、契約企業ドメインの DNS サーバを、契約企業自身で管理する形態です。ホスティング事業者は、契約企業のメールサーバは管理しますが、DNS サーバの管理（MX レコードや TXT レコードの登録・更新・削除）は行いません。

6.1.2.2　DNS ホスティング型

DNS ホスティング型は、契約企業ドメインの DNS サーバを、ホスティング事業者側が代行して管理する形態です。ホスティング事業者は、契約企業のメールサーバとともに DNS サーバの管理も行います。

6.1.2.3　DNS 提供型

DNS 提供型は、契約企業ドメインの DNS サーバのみをホスティング事業者が代行して管理する形態です。ホスティング事業者は、契約企業の DNS サーバは管理しますが、メールサーバの管理は行いません。

この場合には、DNS 自社管理型とも異なり、契約企業、メールサーバのみを管理するホスティング事業者、DNS サーバのみを管理するホスティング事業者の三者が登場します。

6.2　送信側の対応

ホスティング事業者は、契約企業が自社ドメインを差出人としてメールを送信する際に、SPF / Sender ID 及び DKIM に適合したメール送信環境を準備しなければなりません。

以下、SPF / Sender ID の対応、DKIM の対応について解説します。

6.2.1　SPF / Sender ID の対応

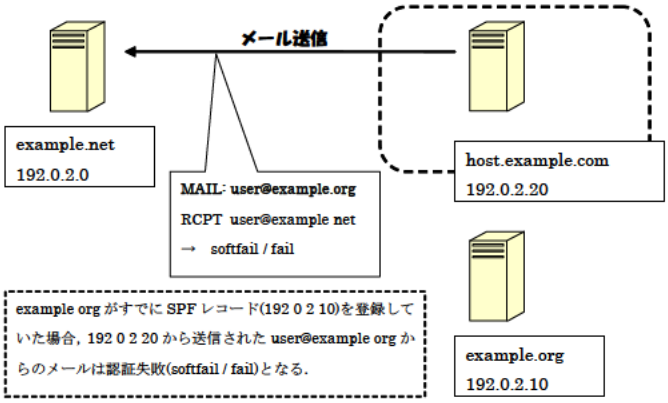
ホスティング事業者が送信側で SPF / Sender ID を導入する場合には、第４章で解説した一般的な対応のほか、以下のような事項についての対応を行わなければなりません。

6.2.1.1　SPF/SenderID 利用の確認

ホスティング事業者は、事前に SPF / Sender ID を利用することのメリットやデメリットを契約企業へ説明し、利用の確認を行わなければなりません。

例えば、4.1.3.4 で解説したとおり、契約企業が、登録したドメイン以外の差出人アドレスを用いてメール送信を利用している場合（図表６－５）には、SPF / Sender ID を利用することで認証結果が fail / softfail になる可能性があります。

説明内容については、第４章を参考にして、契約企業向けの説明資料を事前に準備することが推奨されます。



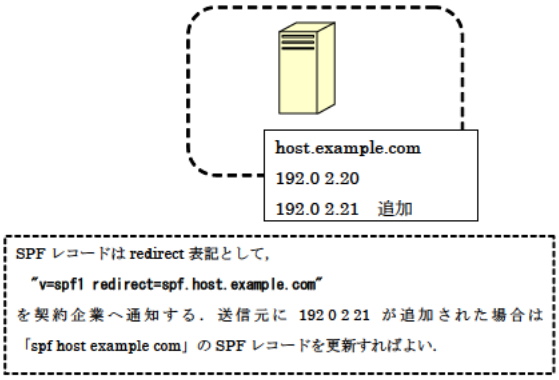
図表６－５　自社ドメイン以外のメール送信の例

6.2.1.2　SPF レコード登録に必要な情報の通知

DNS 自社管理型の場合には、SPF レコードの登録作業を契約企業自身が行わなければなりません。

この場合に、ホスティング事業者は、送信元となる IP アドレスなどの必要な情報を契約企業へ通知することが必要です。また、ホスティング事業者は、契約企業に対して、”redirect” で呼び出せるドメインなどを通知することが推奨されます（図表６－６）。送信元を IP アドレスで通知すると、IP アドレ

スの追加・削除のたびに、それぞれの契約企業に対して通知を行うことになりますが、”redirect” で呼び出せるドメインなどを通知することにより、IP アドレスの追加・削除があっても、通知しなくてもすむことになるためです。



図表６－６　SPF レコード (redirect) の利用例

また、ホスティング事業者は、契約企業に対して、”redirect” ではなく ”include” を用いて送信側のメールサーバを指定させることもできます。この場合には、契約企業側で認証結果の扱いをカスタマイズすることができます。

	特徴
redirect	契約ドメインに同一の SPF レコードを設定することができ、管理しやすい。
include	各契約企業ごとに認証結果のポリシーを変更することができる。

※ redirect, include については、3.2.4.2 を参照

図表６－７　SPF レコード(redirect, include)の特徴

6.2.1.3　SPF レコード登録のサポート

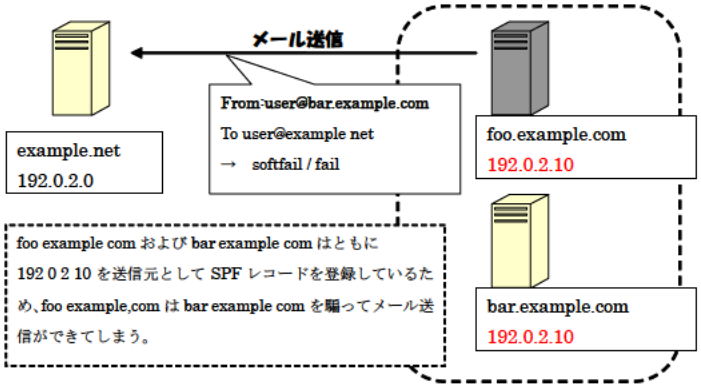
契約企業側の管理者が SPF レコードの記述方法に詳しくないことも考えられますので、DNS 自社管理型の場合には、ホスティング事業者は、SP F レコードの記述方法の説明や契約企業の要求に合った SPF レコードの作成準備を行うことが推奨されます。また、Appendix 1 で紹介している記述例や間違えの例を参考にして、契約企業側の SPF レコード登録をサポートすることが推奨されます。

6.2.1.4　サーバ共用型でのユーザ管理体制

サーバ共用型の場合には、ホスティング事業者は、契約ドメインの送信状況を随時監視しなければなりません。また、ホスティング事業者は、SPF / Sender ID の認証結果が pass とならないメールの送信を禁止したり、発信元 IP アドレスを分けるなどの対策をとる

ことが推奨されます。

これは、同一サーバに収容されているドメインの SPF レコードも同一となりますので、悪意のあるユーザがいた場合に、同一収容された契約ドメインの From ヘッダアドレスやリバースパスを騙って、正当なメールを送信することができてしまうためです（図表６－８）。



図表６－８　サーバ共用型でのなりすましメール例

また、サーバ共用型の場合では、同一サーバ（IP アドレス）に割り当てられた他社ドメインによって、SPF / Sender ID の認証結果が fail / softfail するメールを大量に送信されてしまい、その結果割り当てられたメールサーバが迷惑メールの送信元として認知されてしまう危険性があるためです。すなわち、他社ドメインのメール送信が、無関係である自社ドメインの送信メールに影響を及ぼし、最悪の場合は送信メールの不達が生じるものです（お隣さん問題）。

6.2.2　DKIM の対応

ホスティング事業者が送信側で DKIM を導入する場合には、第４章で紹介した一般的な対応のほか、以下のような事項についての対応を行わなければなりません。

6.2.2.1　DKIM 利用の確認

ホスティング事業者は、SPF / Sender ID の場合と同様に、事前に DKIM を利用することのメリットやデメリットを契約企業へ説明し、利用の確認を行わなければなりません。

例えば、契約企業が自社ドメイン以外の差出人アドレスを用いてメール送信に利用している場合には、電子署名を作成する際に利用したドメインと From ヘッダアドレスのドメインが一致しない可能性があります。

具体的な説明内容については、第４章を参考にして、契約企業向けの説明資料を事前に準備することが推奨されます。

また、電子署名を作成する際に利用したドメインと From ヘッダアドレスのドメインの違いによって、いくつかのサービス仕様が考えられますので（図表６－９）、ホスティング事業者は、契約企業の送信ポリシーと照らし合わせて実装を行うことが推奨されます。

	DKIM 利用方法	サービス仕様の例
1	すべての送信メールに電子署名を作成する方式	・From ヘッダアドレスが自社ドメインの場合は送信者署名となり、From ヘッダアドレスが自社ドメイン以外の場合は第三者署名となる
2	自社ドメインのメールだけに電子書名を作成する方式	・From ヘッダアドレスが自社ドメインの場合は送信者署名となりますが、From ヘッダアドレスが自社ドメイン以外の場合は、電子署名を作成しない ・どちらの場合もメール送信は許可する
3	自社ドメインのメールだけ送信を許可する方式	・From ヘッダアドレスが自社ドメインの場合は送信者署名となるが、From ヘッダアドレスが自社ドメイン以外の場合は、メール送信を許可しない

図表６－９　DKIM 利用方法とそのサービス仕様の例

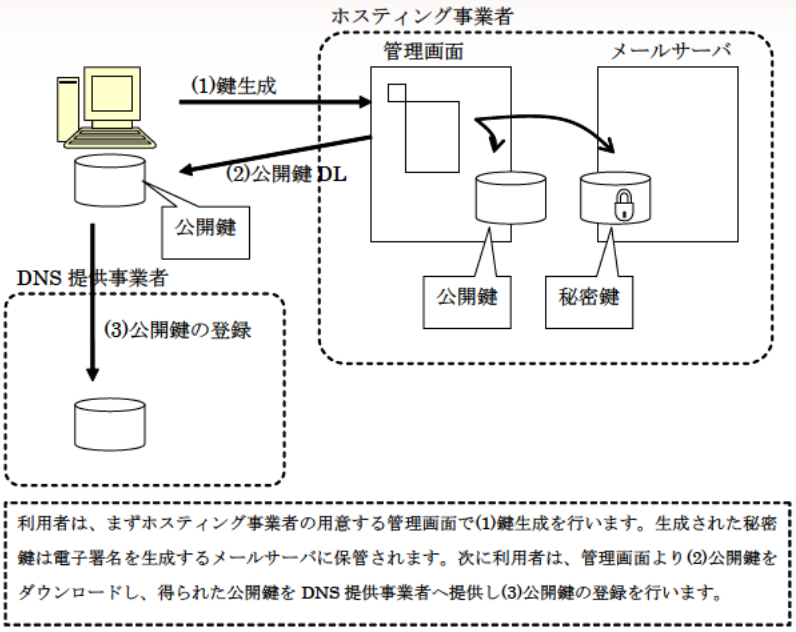
6.2.2.2　公開鍵の通知

DNS 自社管理型の場合には、公開鍵の登録作業は契約企業が行うことが必要です。ホスティング事業者は、公開鍵・セレクタなどの必要な情報を契約企業へ通知することが必要です。電子署名の解読行為を防止するために、定期的な公開鍵と秘密鍵の更新を行うことが推奨されますので、ホスティング事業者は、公開鍵と秘密鍵の更新のたびに、この手続を行うことが必要です。

6.2.2.3　公開鍵登録のサポート

DNS 自社管理型の場合には、契約企業側の管理者が公開鍵レコードに詳しくないことが考えられますので、ホスティング事業者は、公開鍵レコードの記述方法の説明や公開鍵レコードの作成準備を行うことが必要です。

また、DNS 提供型のように、メールサーバをホスティングする事業者と DNS をホスティングする事業者が異なる場合には、公開鍵と秘密鍵の管理方法が課題となります。ホスティング事業者は、ブラウザなどから操作できる管理画面などを用意し、公開鍵と秘密鍵の生成と、公開鍵のダウンロード機能を提供することが推奨されます（図表６－１０）。この機能を利用して、契約企業側の管理者は DNS 提供事業者への公開鍵提供と公開鍵の登録をすることができます。



図表６－１０　ホスティング事業者の提供する公開鍵と秘密鍵の管理システムの例

6.3　受信側の対応

ホスティングサービスでは、ホスティング事業者の設備で受信側の対応を行うことが必要です。第３章で紹介した一般的な対応のほか、以下のような事項についての対応を行うことが必要です。

6.3.1　認証結果の解説と利用方法の提示

送信ドメイン認証技術による認証結果を Authentication-Results ヘッダに記録する場合には、契約企業に対して Authentication-Results ヘッダに関する説明を行い、必要であればメールクライアント側での適切なフィルタリングの指導を行うことが必要です。

ホスティング事業者は、第３章を参考にした説明資料を準備することが推奨されます。

6.3.1.1　判定結果の確認

契約企業にフィルタリングの指導をする準備として、該当ドメイン宛の受信メールのうち、適切に送信ドメイン認証が実施された割合を調査します。受信メールの多くが fail / softfail と判定されているドメインのうち、契約企業とやり取りをされている顧客が含まれる場合は、フィルタリングのホワイトリスト対象を講じることが考えられます。この場合には、該当するドメインをリスト化して、契約企業に確認してもらうことが推奨されます。

受信メールの多くが neutral / none と判定されている契約企業の場合は、フィルタリングによる効果が低いため、この指導は見送ることが推奨されます。

6.3.1.2　契約企業への説明とメールクライアント側へのフィルタリング指導

契約企業に対して、契約ドメイン宛の受信メールの判定結果及びフィルタリングによって得られる効果を報告します。ホスティング事業者は、メールクライアント側で設定すべきフィルタリング条件の設定をサポートするとよいでしょう。

6.3.2　認証結果によるフィルタリング実施

メールクライアント側のフィルタリングでは、ホスティング事業者の設備コストは直ちに効果がでるとはいえませんが、今後送信側の対応が進むとエンドユーザ側での様々な活用が進むと予想されております。

ホスティング事業者は、メールの隔離、拒否、破棄などのサーバ側でのフィルタリング機能を準備することが推奨されます。サーバ側のフィルタリング機能を実装するにあたっては、以下の点について考慮することが必要です。

6.3.2.1　フィルタリング利用を選択できる機能の提供

特にサーバ共用型の場合には、フィルタリング機能を利用する契約企業と利用しない契約企業が共存する場合が想定されますので、ホスティング事業者は、契約ドメインごとにフィルタリング設定の有効・無効を管理する

ことが必要です。

6.3.2.2　ドメイン単位のホワイトリスト機能の提供

6.3.2.1 で解説したとおり、送信元ドメインによってはすべてのメールの送信元に対して送信ドメイン認証技術に対応していない場合があります。言い換えれば、認証結果が fail / softfail であっても受信すべき送信元ドメインが存在することになります。このため、ホスティング事業者は、各契約ドメインごとに、ホワイトリスト機能を提供し、必要なメールの不達を防ぐことが必要です。

6.3.2.3　なりすましメールの措置を選択できる機能の提供

フィルタリング結果で送信者情報が偽装されているメール（なりすましメール）であると判定された場合には、それらのメールは何らかの措置（隔離、ラベリング、拒否等）がとられることが推奨されます。ホスティング事業者は、このような措置として複数の選択肢を用意し、契約企業にリスクと効果をかんがみて、設定してもらうことが推奨されます。ホスティング事業者の用意する措置としては、以下のようなアクションが考えられます。

	仕様	特徴
ヘッダに目印を記録	X ヘッダ又は Subject ヘッダなどになりすましと認識できる目印を記録する	・受信すべきメールの不達を防止することができるが、契約企業のユーザがメールクライアントでフィルタリング設定をする手間が生じる
隔離して受信	ごみ箱や迷惑メールボックスなど、受信箱とは別の場所に受信する	・受信すべきメールの不達を防止することができるが、隔離されていることで False Positive が発生した場合にユーザが受信を見落とす可能性がある ・ゲートウェイ型では提供できない
SMTP で拒否する	なりすましメールと判定された時点で、SMTP 応答で該当メールを拒否する	・なりすましメールが契約企業のユーザに着信しなくなるが、ホワイトリストが適切に設定されていない場合には、メール不達が生じる
NDR をメールサーバで破棄	なりすましメールと判定されたメールのうち、NDR については SMTP レスポンスを正常応答したのち、メールサーバ内で破棄する	・不要な NDR によるコストが軽減されるが、通常のメールについては他の施策と組み合わせて実装する必要がある

図表６－１１　なりすましメールの措置の例