平成 25 年 6 月 21 日

近畿大学メールサービス利用者　各位

総合情報システム部

送信ドメイン認証の導入について

このたび、東大阪キャンパスではなりすましメール対策として、一部のメールアドレスを対象に、送信ドメイン認証を導入することとなりました。
つきましては下記をご確認いただき、ご活用ください。

記

1.　送信ドメイン認証とは

送信ドメイン認証とは、送信者のメールアドレス（From）が正規なものであることを証明する技術です。多くの迷惑メールは、送信者のメールアドレスを偽って送っているため、こうした「なりすまし」を排除するための技術です。

ドメインとは、メールアドレスの@以下の記述を意味します。
⇒test@kindai.ac.jp であれば、kindai.ac.jp がドメインです。

2.　近畿大学で導入する送信ドメイン認証技術

送信ドメイン認証にはいくつか種類がありますが、本学では、最も簡単かつ有効である「SPF レコードによる送信ドメイン認証」を導入します。
SPF レコードとは、メール受信時にそのメールアドレスを見て、それが正規なサーバーから発信されているか否かを検証するものです。
設定方法は、
（1）SPF レコードを自ドメインの DNS サーバに記述
（2）受信メールサーバ側に、SPF レコードを見てスパム判断基準とする設定を行う
上記２点です。本学では、（2）はスパムメールゲートウェイで設定済み（判断基準の１つ）ですので、（1）の作業のみ実施いたします。

メールアドレスの「なりすまし」は容易に出来てしまい、近年では有名企業や自治体のメールアドレスになりすまして迷惑メールやウィルスメールが送付されるなど、多くの問題が発生しています。
近畿大学のメールアドレスが「なりすまし」に利用されることによって、メール攻撃の加害者と判断され、ブラックリストに登録されることも起こり得ますので、送信ドメイン認証を導入し、本学のメールアドレスの信頼性を確保する必要があります。

図１　なりすましにより発生する問題

ただ、今回導入する SPF レコードは、「なりすまし」メールの送信・受信を完全に防止するものではありません。

多くのメールサービスでは、SPF レコードで「なりすまし」メールと判断した場合でも、迷惑メールの判断基準の 1 つとして利用するだけで、標準の設定では削除等の処理はしない場合が殆どです。また、NTT docomo や au、Softbank といった通信キャリアでは、SPF レコードを見て「なりすまし」メールか否か判断する設定を利用者側で実施することができるため、本学でも SPF レコードを導入し、標準化を進めたいと考えております。

なお、WIDE プロジェクトによると、日本のドメイン（ac.jp や co.jp 等）の SPF レコードの普及率は 43.89%、日経平均採用銘柄(225)では、29.3%となっております。

どちらも 1 年以上前の情報のため、現在では更に普及率は上がっていると思われます。

【参考】

http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

http://www.hde.co.jp/press/pressrelease/release.php?rd=201202080

3. 導入対象ドメイン・導入時期

【対象ドメイン】

「kindai.ac.jp」

（東大阪キャンパスの Kindai Mail でご利用のアドレス：～@kindai.ac.jp）

【実施時期】

2013 年 7 月 8 日（月）10:00 に、「kindai.ac.jp」の DNS サーバに SPF レコードを追記いたします。

「～@kindai.ac.jp」のメールを使っている人のみが対象です。

kindai.ac.jp に SPF レコードを先行導入し、特に動作に問題がなければ、次に職員用ドメインである「itp.kindai.ac.jp」に送信ドメイン認証を適用いたします。

学部・学科でご利用のドメインについては、各学部のネットワーク管理者の先生方に、総合情報システム部から個別にご相談させていただきます。

4. 設定内容

DNS サーバに以下の SPF レコードを記述します。

[IN TXT "v=spf1 ip4:163.51.0.0/16 ip4:157.13.0.0/16 ip4:202.250.120.0/25 ip4:61.113.102.200/29 include:_spf.google.com ~all]

これにより、「～@kindai.ac.jp」を送信者（From）とするメールは、近畿大学東大阪・奈良・大阪狭山・和歌山・広島・福岡キャンパスおよび Gmail から送信されたものであれば正規のメールとしますが、Yahoo メールや個人契約のプロバイダのメールサーバから送信した場合、「なりすまし」メールとなり、迷惑メールの判断基準の 1 つとなる場合があります。

表 2　判断基準

KindaiMail（WEB メール含む）	正規なメールと判断
近畿大学東大阪・奈良・大阪狭山・和歌山・広島・福岡キャンパス内の 163.51/16、157.13/16、202.250.120.0/25 の IP アドレスを付与されたメールサーバや端末	
Gmail の WEB メールや smtp.gmail.com からの送信	
Yahoo メールや個人契約のプロバイダ	「なりすまし」メールと判断

5.　導入後の注意点

前項のとおり、「@kindai.ac.jp」のメールを Gmail や大学キャンパス内で使っている利用者については正規の利用として判断されるため、いままでどおりお使いいただけますが、自宅のプロバイダ等を送信メールサーバとして利用されている方については、以下のようなパターンで「なりすまし」メールと判断されてしまうことが稀にあります。

「なりすまし」メールと判断された場合の動作は、受信側のメールシステムにより異なりますが、迷惑メールと認識され、迷惑メールフォルダで受信されることがあります。なお、通常のメールの場合は送信相手に届かなかった場合は、エラーメールが返送されますが、「なりすまし」メールと判断した場合は、受信側のメールシステム・転送設定などの条件により、エラーメールが返送されないことが稀にあります。

【パターン①】

学外（自宅や外出先）からのメール送信時に「user01@kindai.ac.jp」を送信者（From）とし、個人で契約しているプロバイダからメールを送信した場合、「kindai.ac.jp」ドメインのメール送信を許可されていないメールサーバからの送信となるため、「なりすまし」メールとなり迷惑メールと送信先に判断される場合があります。

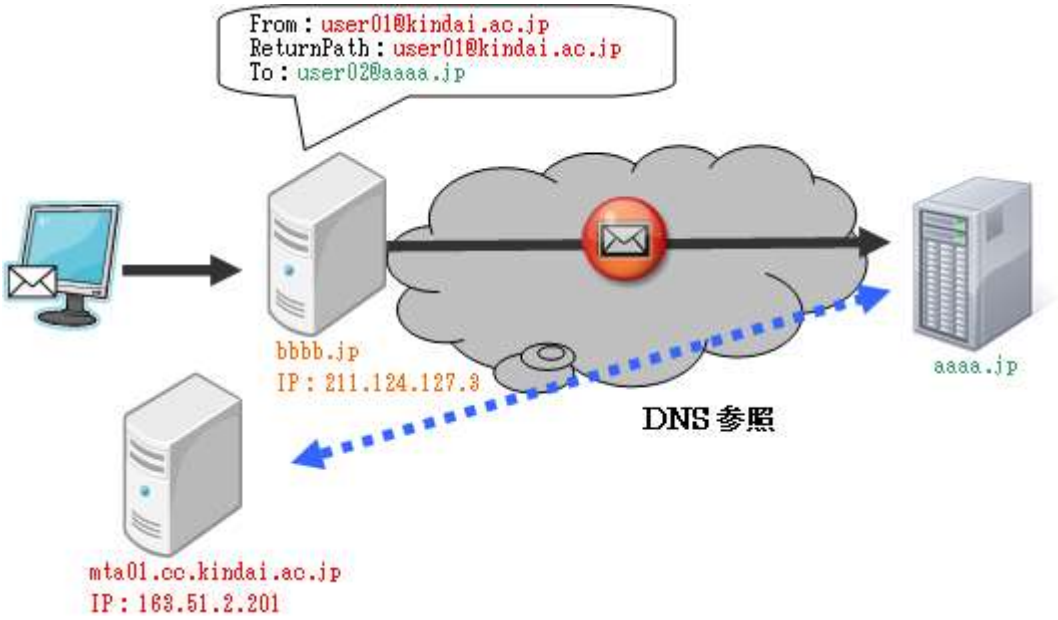

図３　「なりすまし」メールと判断される例

・「aaaa.jp」のメールサーバが ReturnPath「user01@kindai.ac.jp」のメールを受信する。

・「aaaa.jp」のメールサーバは DNS サーバに ReturnPath のドメイン「kindai.ac.jp」の SPF レコードを問い合わせる。

・問い合わせの結果、近畿大学の IP アドレスは「163.51/16」であり、「user01@kindai.ac.jp 」のメールを送信してきた「bbbb.jp」サーバは「163.51/16」の IP アドレスではないので、近畿大学からのメールではなく、「なりすまし」メールと判断する。

【対応方法】

Gmail からの送信は正当なメールとしていますので、KindaiMail の WEB メールから送信する、または、メーラーの送信時に使用する SMTP サーバを「smtp.gmail.com」に変更してください。

【パターン②】

「user01@kindai.ac.jp」から「user03@bbbb.jp」（「user02@aaaa.jp」へ転送）にメールを送信する場合、転送するサーバである「bbbb.jp」のメールサーバは、「kindai.ac.jp」ドメインのメール送信を許可されていないメールサーバのため、「なりすまし」メールとなり、迷惑メールと判断され、迷惑メールフォルダで受信される場合があります。

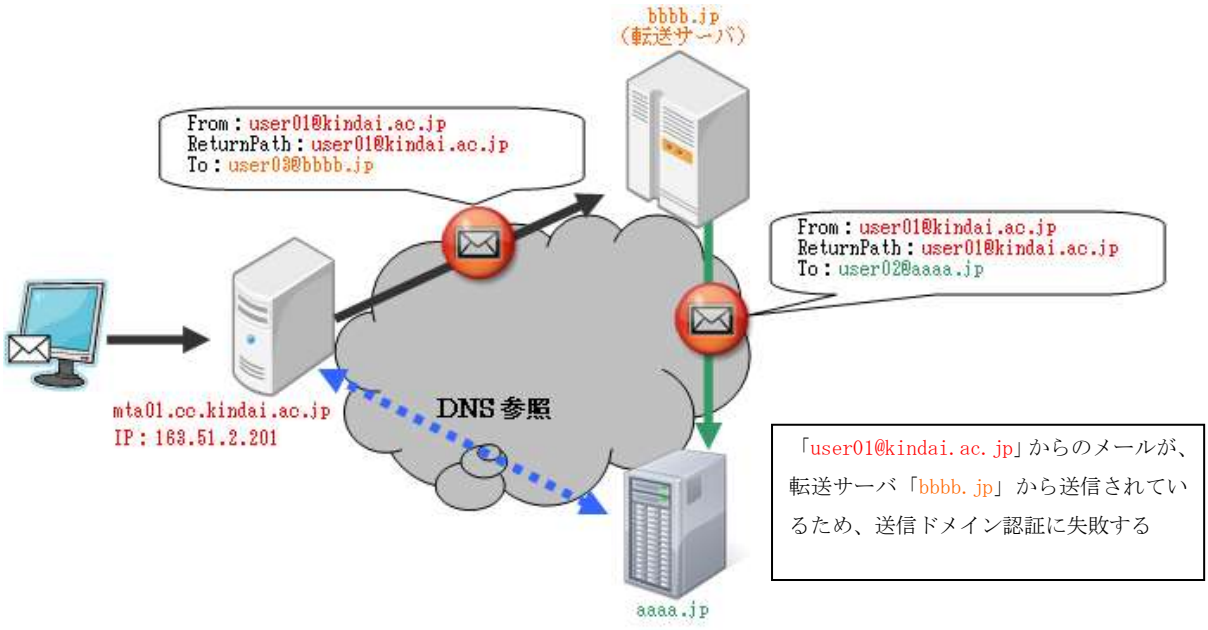

図 4　なりすましと判断される例

【対応方法】

ユーザー側で行える対応として、転送先（上記の例では「aaaa.jp」）で迷惑メールと判定された場合、ホワイトリストに登録する、などが考えられます。

また、転送元での対応として、転送元のメールサーバが送信者情報（return-path）を変更する方法があります。

これは Gmail に実装されている技術のため、「@kindai.ac.jp」の利用者については、このパターン②でメールが転送されないという事象は発生しません。

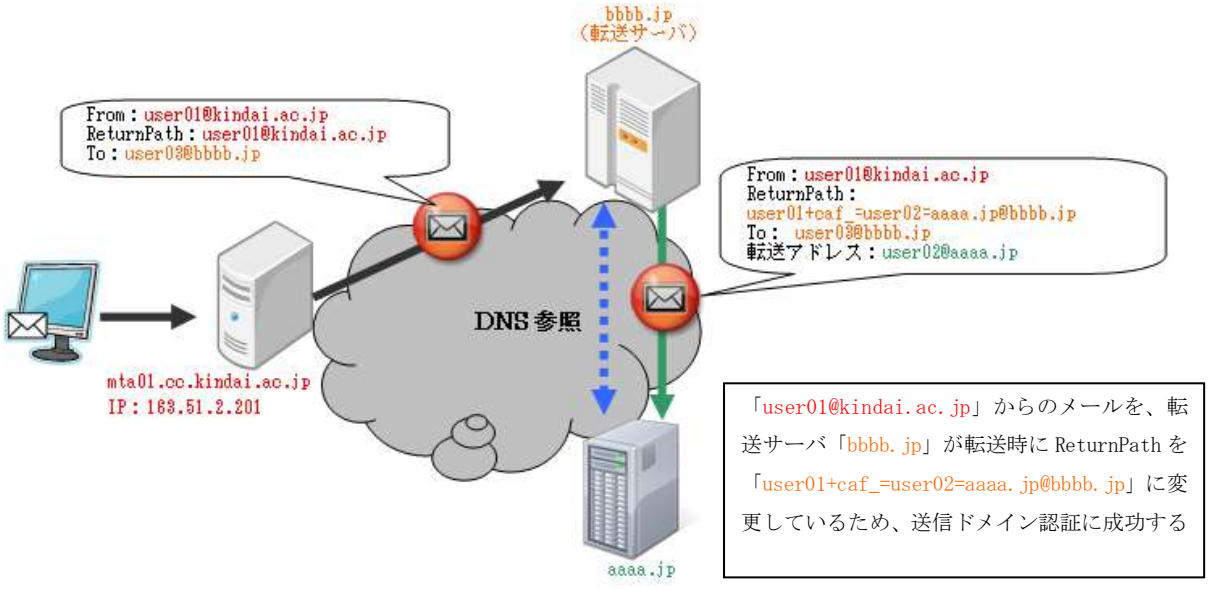

図 5　転送元メールサーバが送信者情報（return-path）情報を書き換える例

6. 参考

国内外の多くのドメインにて送信ドメイン認証の普及が進んでいます。

SPF レコードによる送信ドメイン認証では、上述の【パターン②】のような、転送時に問題が発生しますが、送信者情報を変更する仕組みや、転送前の情報を参照する仕組みはあまり実装されておらず、多くのメールシステムでは、迷惑メールと判定された場合はユーザーによるホワイトリストでの対応を行っています。

※ Kindai Mail（Gmail）、学内教員用メール（DEEPMail）では送信者情報（Return-path）を変更する仕組みが実装されています。

参考までに一般的な SPF レコードの主な判定例は以下のようになります。

表 3　一般的な SPF レコードの判定例

Fail SoftFail Neutral	図 3 のようなケースでメールを送信した場合で、送信ドメイン認証に失敗しているため、「なりすまし」メールと判断されます
None	受信したメールサーバが送信者の SPF レコードを確認したが、送信者のドメインに SPF レコードの設定が無いため、「なりすまし」メールであるかの判定が出来ないメールと判断します
Pass	図 2 のようなケースでメールを送信した場合で、送信ドメイン認証に成功しており、近畿大学からの送信メールと判断します

7. お問い合わせ先

総合情報システム部
メールアドレス：kudos_support@ml.kindai.ac.jp

以上