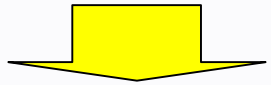
JEAGアップデート　迷惑メールの現状とその対策について
～送信ドメイン認証技術 Recommendation とその後 ～

KDDI株式会社
FMCプラットフォーム開発部
開発4グループリーダー
本間 輝彰

なぜ、送信ドメイン認証技術が必要か！

n 迷惑メールに多く見受けられる特徴

- Ø *迷惑メールの多くは送信元を詐称*
- Ø *正規のメールサーバを経由せず専用サーバから直接送信*
  - ü 送信元が固定でなくなっている（Bot経由が主流へ）
- Ø フィッシングなどの詐欺行為の出現



n 迷惑メールの対策には

- Ø 送信者情報を詐称出来ない仕組みの導入が必要
  - ü SMTP AUTH
  - ü *送信ドメイン認証技術*
- Ø 送信元が明確になれば対策がし易くなる
- Ø 正規の送信元からのメールを正しく受信出来る

送信ドメイン認証技術とは

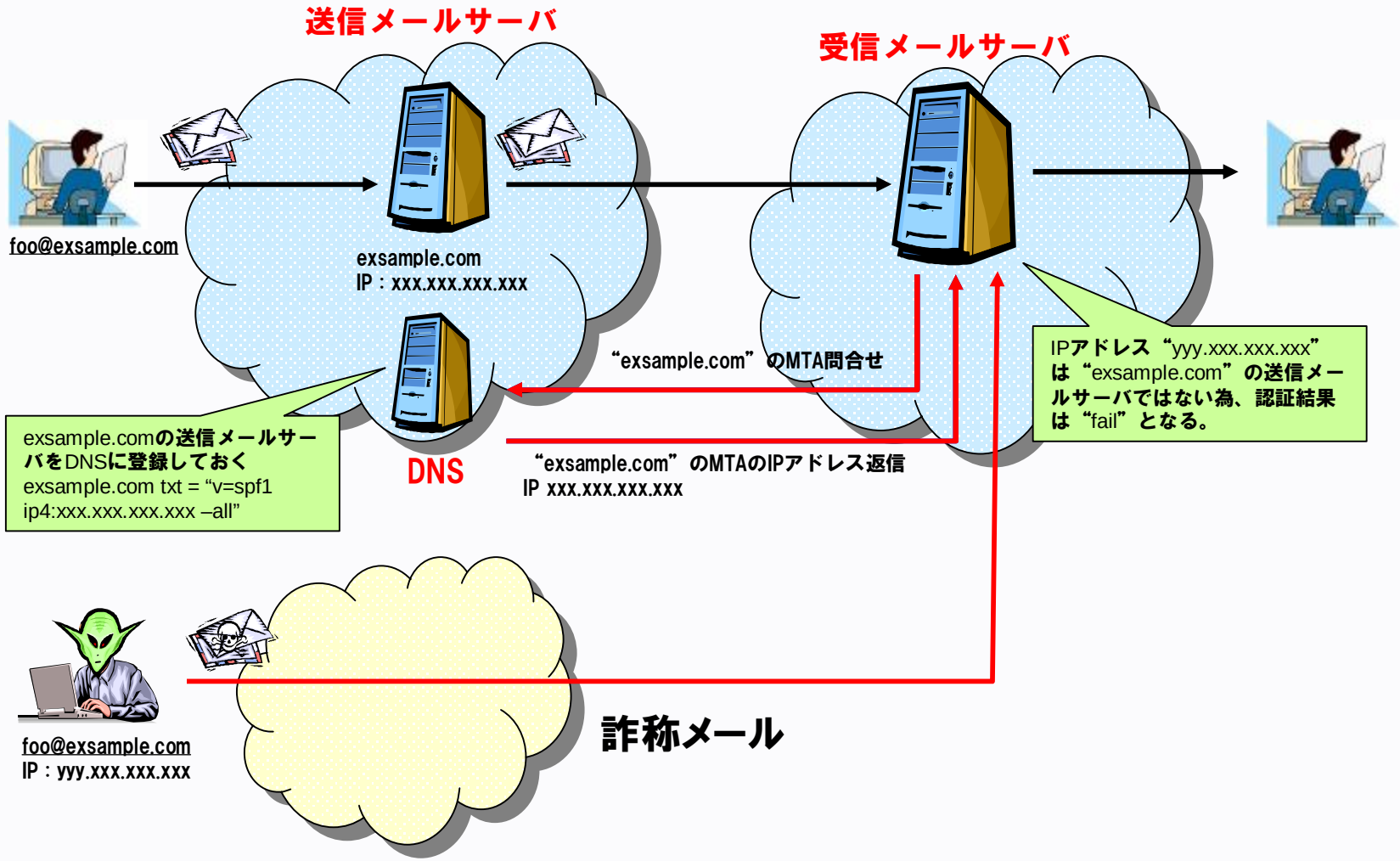
n 送信ドメイン認証技術とは

- Ø 送信側がドメイン単位でメール送信元情報を表明
- Ø 受信側が正規のメールサーバから出たものかを認証
- Ø ***送信側と受信側で協力して初めて成立する技術***
- Ø 既存のメール配送の上位互換として存在

n 送信ドメイン認証技術には二つの種類が存在

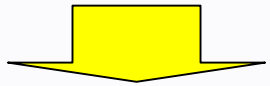
- Ø 送信元をネットワーク的に判断
  （*SPF : Sender Policy Framework*）
- Ø 送信時に電子署名をメールに付与
  （DKIM : DomainKeys Identified Mail）

送信ドメイン認証(SPF)のしくみ



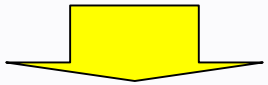
送信ドメイン認証(SPF)の普及にむけて

- メール送信側で導入を実施
  - 送信側の導入実施　→　受信側の判断が容易に
    → 導入しない送信元は不利に　→　送信側の導入の増加
  - ***送信側はSPFの記述を推奨（DNSへSPFレコード記述のみでOK!）***



- JEAG Sender Auth SWGにて送信ドメイン認証技術について検討を実施（計8回のSWGを開催）
- ***JEAGではRecommendationを作成し、普及を促進中***

http://jeag.jp/
http://jeag.jp/news/pdf/SenderAuthRecommendation.pdf

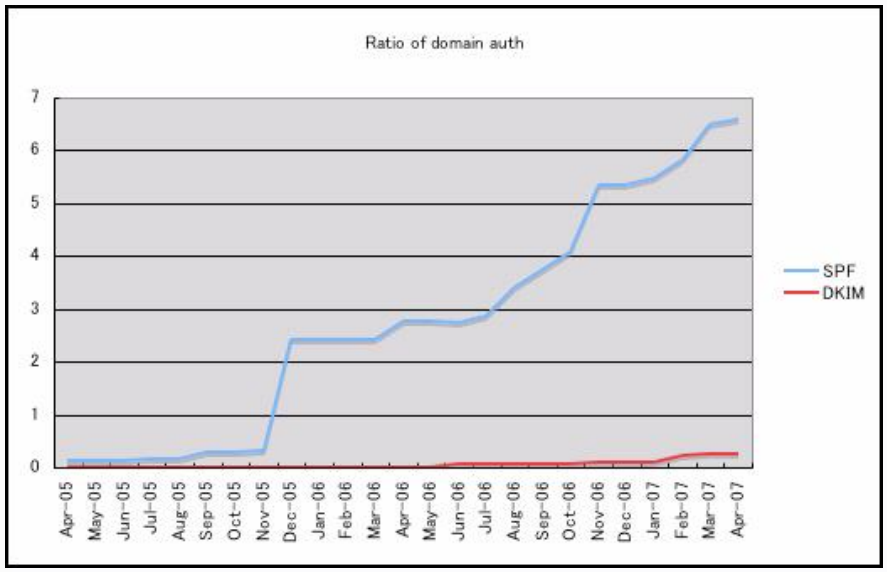


- ***送信ドメイン認証によるラベリング行為は、総務省にて、正当業務行為（違法性阻却事由あり）と解釈出来ると提示されている。***

ISPによる受信側における送信ドメイン認証導入に関する法的な留意点（第3回迷惑メール対策カンファレンス）
http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html#jigyosha

送信ドメイン認証の国内の普及状況

WIDE プロジェクトは、JPRS と共同研究契約を結び、2005年4月から送信ドメイン認証の普及率測定しており、その調査結果を以下に示す。



登録型	登録数	MX	SPF	DK
AD (JPNIC会員)	291	248	37	2 (4)
AC (大学系教育機関)	3368	3184	189	2 (6)
CO (一般企業)	305042	284775	26660	614 (630)
GO (政府機関)	884	746	46	0 (1)
OR (会社以外の団体)	22703	21283	1949	31 (35)
NE (ネットワークサービス)	17435	13358	745	43 (54)
GR (任意団体)	8513	7275	546	13 (16)
ED (小・中・高校など主に18歳未満を対象とする各種学	4447	4059	191	2 (2)
地域型 (都道府県名、政令指定都市名、市町村名)	3265	2699	76	2 (3)
汎用JPドメイン	540168	363424	15716	905 (977)
合計	908329	702092	46161	1614 (1728)

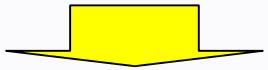
2007年4月末現在、JPドメインにおける送信ドメイン認証技術のおおよその普及率

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

着実に、国内のSPFの記述率は増えている
（4月末現在、約6.6%）

送信ドメイン認証普及にむけての課題認識

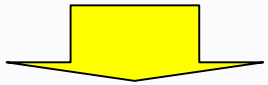
- 送信ドメイン認証の仕組み、影響、効果が認知されていない。
- 社内へ十分説明出来ない、もしくは、そもそも十分理解ししていない。
  - Ø 導入のインパクト、影響、等
- SPFの記述方法や設定方法などを説明する媒体が無い。（少ない）
  - Ø 記述したくても、記述方法が判らない為、導入できない。
- 受信側の対応が少なく、書くメリットがない。
  - Ø 実影響が出ていない為
  - Ø 認証結果をどう扱うかが不明確。（passとnoneの区別がない）
- メールを受信するエンドユーザに効果を訴求しづらい。
  - Ø エンドユーザへの効果に対して、導入の障壁が高い。
  - Ø 顧客へどのようなメリットがあるのか見えにくい。



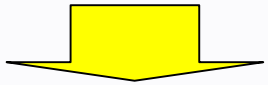
実際の問題として、ISP/ASPのSPFレコードの記述率は高いが、業界によっては全く対応出来ていない所もある。

アドレス詐称の実態

これまでの迷惑メールのアドレス詐称状況は、大手ASP等のフリーメールアドレスのドメインを詐称してメールを送信するケースが多かった。
しかしながら、最近では大手ISPのドメインを詐称して送信される数も多くなってきている。



さらには、**メールマガジン等のメールアドレスを詐称**して、あたかもそのメールマガジンを語って送ってくるメールも出始めている。
最近では、**一般企業のドメインを詐称した**迷惑メールも出現している。



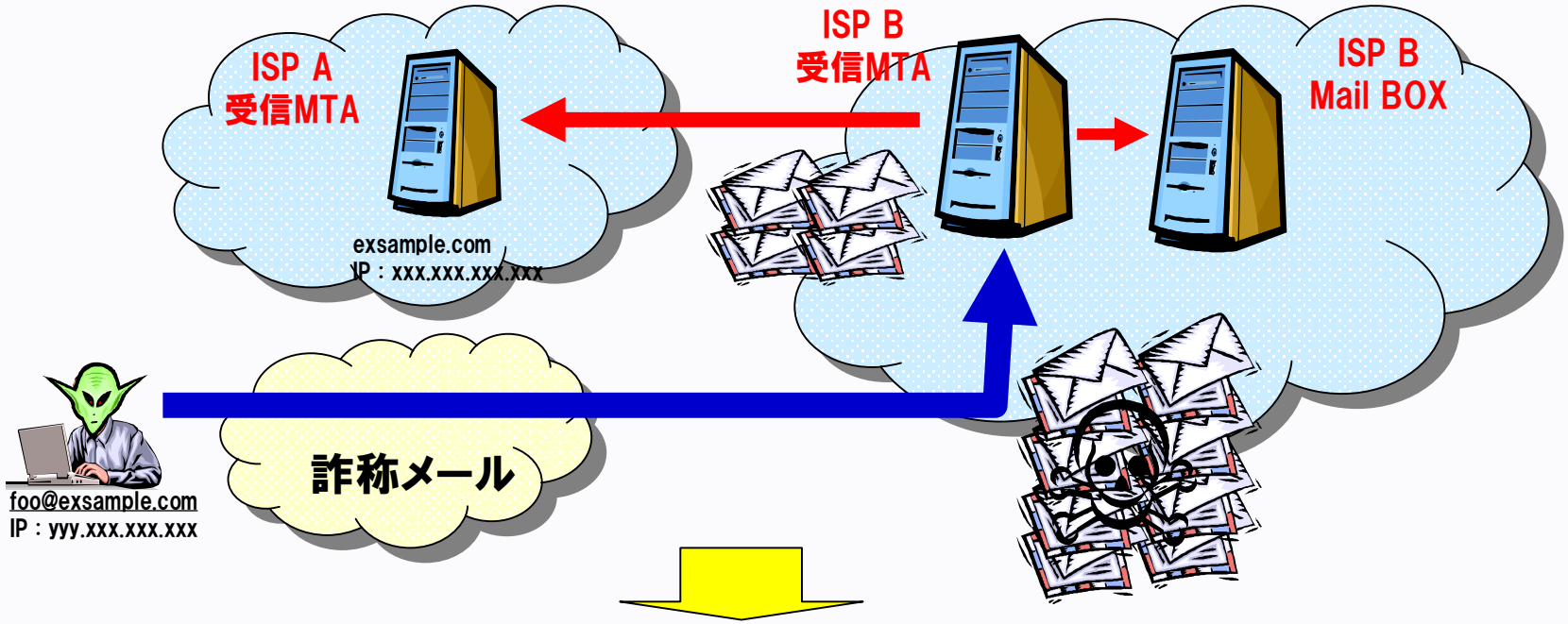
自社のドメインを守る為にも、SPFの記述は必須となってきている。

SPFレコードを記述すると？

- 受信側で認証を行う事で、ドメイン詐称が出来ない基盤が確立される。
- 受信側の負荷増加が気になる。
  - 確かに認証負荷は増加するが、迷惑メール全体が減る事で、相殺出来る事は期待出来る筈。
  - DNSの参照回数をすくなくなる記述を推奨。
- SPFレコードの記述を誤ると、認証エラーになる危険がある！？
  - 記述ミスしているドメインも若干見受けられるのは事実。
  - “?all”記述して試験を行って後に、“~all”や“-all”に変更する等で対処は可能。

Bounce spamの問題

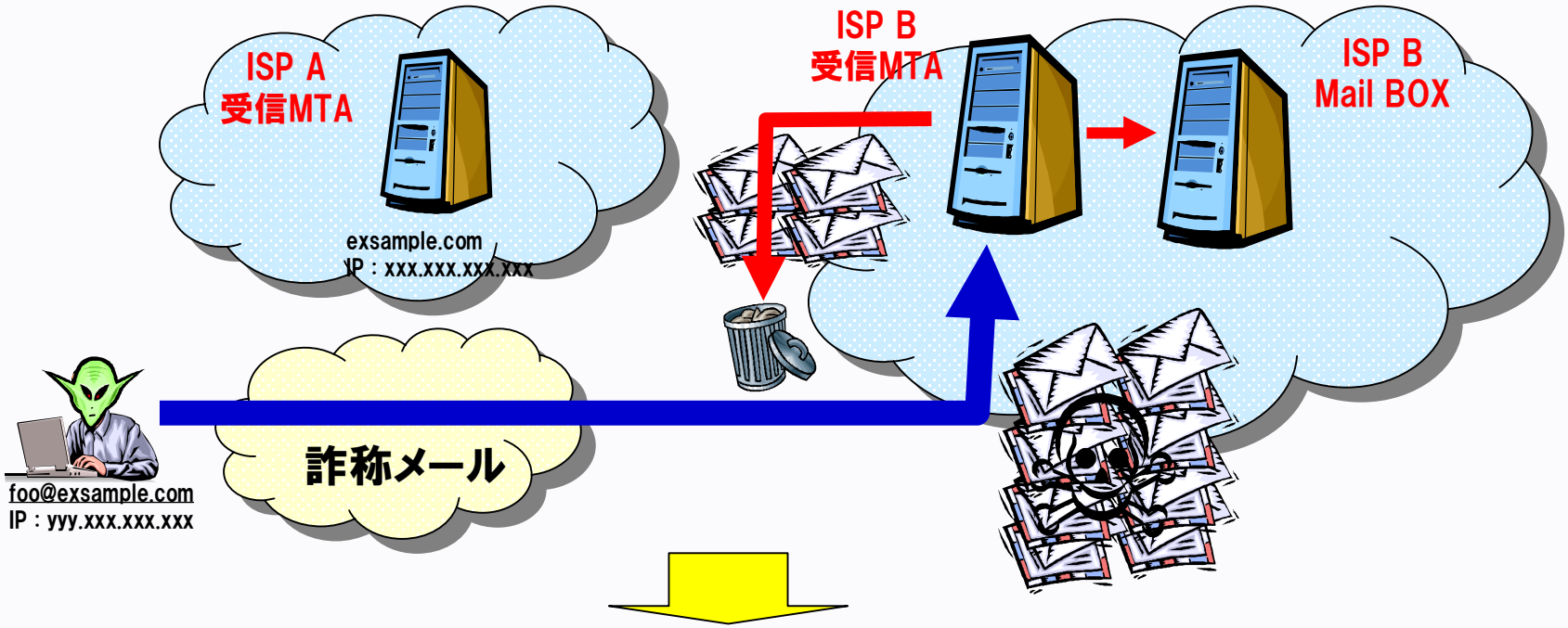
メールサーバの構成によっては、受信MTAでユーザ情報を持っていない、ハーベスティング対策でメールをすべて受信する設定としている、等の場合、存在しない宛先へメールが来た場合、エラーメール（NDR）返信が一般的である。しかしながら、迷惑メールで送信ドメインを詐称され大量の存在しない宛先のメールが送信された場合、受信側ではなりすまされたドメインに大量のNDRを返信する事となり（Bounce spam）問題となる。



なりすまされ易いドメインは、これが大きな問題となっているらしい。

SPF認証結果の応用（NDR破棄）

SPF認証結果で、エラーとなった場合、そのメールは詐称したアドレスからのメールと判断し、NDRを破棄する事で、受信側は不要な送信なくすことが出来、詐称されたドメイン側も不要なメールを受信しないですむ事となる。

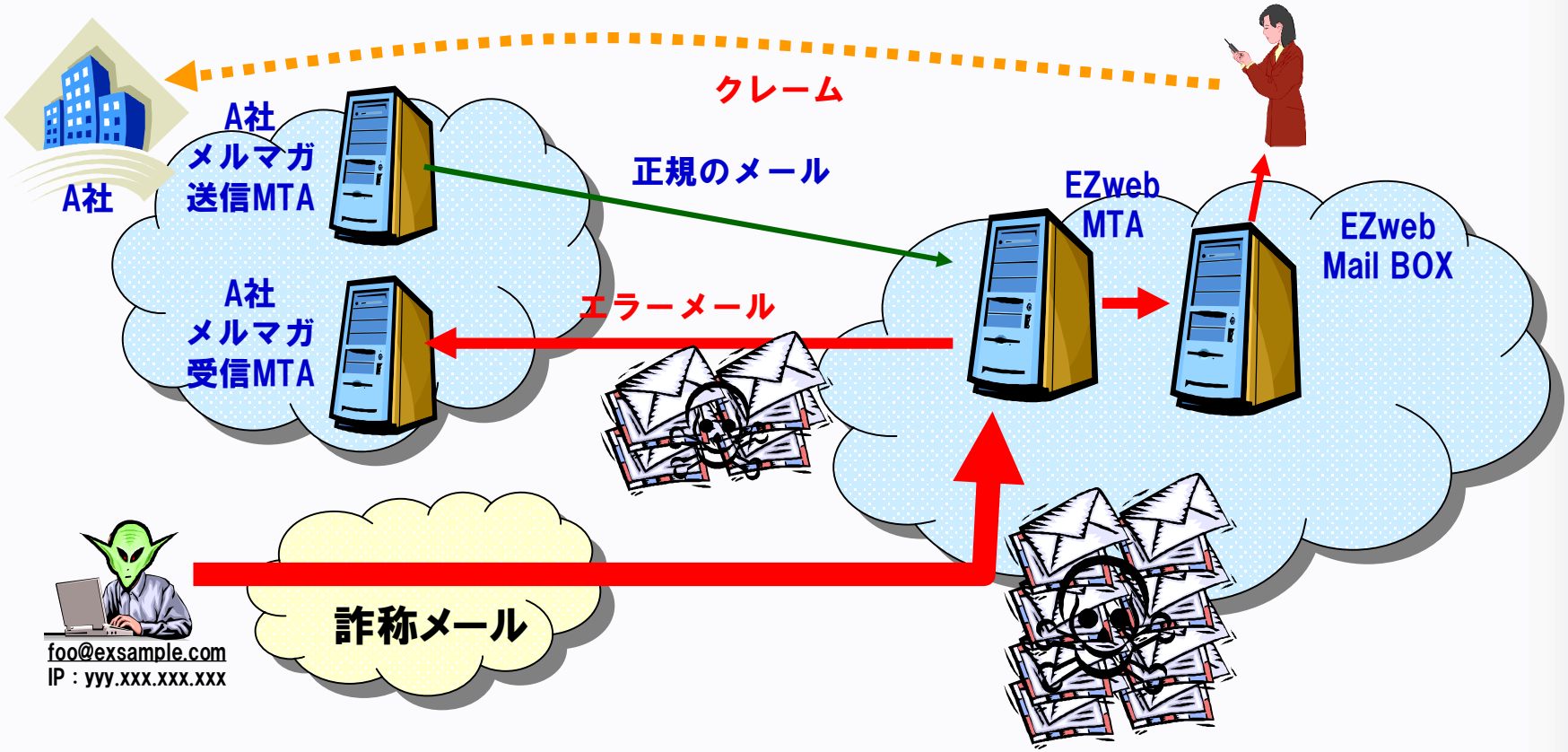


本対応は、JEAG Recommendationでも、参考情報として提案をしている。また、総務省にて、正当業務行為（違法性阻却事由あり）と解釈出来ると提示されている。

ISPによる受信側における送信ドメイン認証導入に関する法的な留意点（第3回迷惑メール対策カンファレンス）
http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html#jigyosha

アドレス詐称問題の一例と対策例

某メールマガジンのメールアドレスを語って、迷惑メールの送信を実施。存在しない宛先のエラーメールがBounce SPAMとして返信されるに加え、ユーザのクレームもA社に入る事となる。

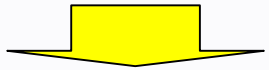


対策として、A社はSPFレコードを記述。これにより、Bounce SPAMはすべてなくなった。さらには、ユーザが送信ドメイン認証規制を利用する事で、この詐称メールのブロックも可能となっている。

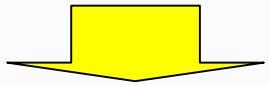
送信ドメイン認証のさらなる普及にむけて

- ***認知のさらなる向上が必須***

  SPF Publish運動 → Inbound Check
  → ドメインレピュテーション
  → spam撲滅



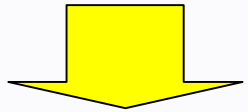
- 技術解説、導入手順、転送問題
  - Ø 対策方法の立案
- ***Inbound Checkにおいて、None（SPF未記述）は怪しいと思わせる***
  - Ø 認証結果を利用出来るメールリーダ等も必要



JEAGのTechnical WGでは、送信ドメイン認証の普及を目指し、ISP/ASPのメール管理者のみならず、広く大きな人を対象としてDocumentの作成に着手。

考察

- SPFレコード記述の普及率は、確実に伸びてきている。
- SPFの認証結果や応用利用も有効性は確認出来つつある。
- 送信ドメイン認証技術の単体利用ではなく、他の技術との連携や応用も必要である。
- 送信ドメイン認証技術もSPF、DKIMの2つを組み合わせる事でさらなる効果が期待出来る。（DKIMの活用については、JEAG内で別途検討中。）



- SPFレコードの記述の普及により、その認証結果をメールの受信に活用する事が有効になる。今後は、SPF認証結果を実施・採用が増え、これに循環する形でSPFの記述が普及するという循環的な普及を期待する。


Designing The Future
KDDI