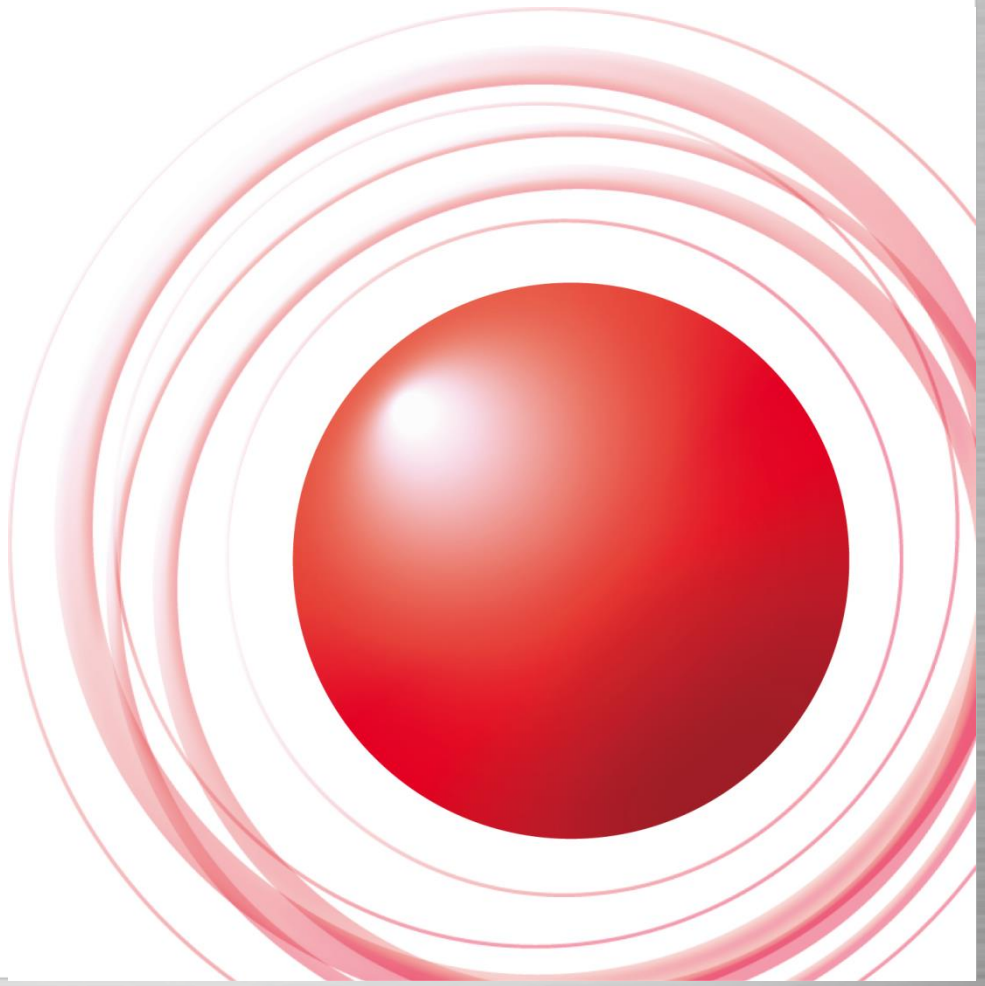
法人向けメールサービスにおける Submission踏み台問題の状況とその対策

IIJ Internet Initiative Japan



2014/10/08

株式会社インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation

今日のアジェンダ

- 法人向けサービスの踏まれspamの状況
- IIJの法人向けサービスにおける対策の歴史
  - 国別送信流量制限の導入とその効果
  - outbound spam filterの導入とその効果

自己紹介

- 島村 充 (しまむら みつる)
- IIJに2006年に新卒入社して、配属当初からメールサービスの運用・開発・企画と、ほぼメール一筋
- 顧客参照用DNSの運用も (半分趣味)
  - Internet Week 2011

    キャッシュDNSサーバとフィルタリングの実例
  - dnsops.jp/dnssec.jp参加

IIJの法人向けメールサービス

- IIJセキュアMXサービス SecureMX
  - セキュリティ重視・高機能
    - メールゲートウェイ(GW)型 (メールボックスは顧客側)
    - メールボックス型 (完全アウトソース)
- IIJポストオフィスサービス
  - 昔からあるサービス ('98/07/01~)
    - メールボックス型

法人向けメールサービスでの踏まれspam状況 (1)

- 発生傾向(増える時期など)はコンシューマー向けメールサービスの状況とほぼ変わらない
  - 件数はコンシューマー向けよりは相当少ない
- 巻き添え顧客からのクレームが増加傾向
- 顧客ごとに出口IPアドレスを分けるなど、出来ると良いだろうが、リソースなどが厳しい
- 踏まれた顧客の対応と同時に、巻き添え顧客への説明も対応が必要
- 合わせると、コンシューマー向けと同じくらい大変か…？

法人向けメールサービスでの踏まれspam状況 (2)

- 企業のITリテラシー・危機管理体制は様々
  - 何度も踏まれる企業というのは割と居る
    ※ 抜かれたのは同じタイミングで、利用された時期が違う可能性はある
  - 全く問題ないという企業も多い
- spam送信＞アカウントロック＞顧客通知
  - 対応フローはコンシューマー向けと同様
  - ウイルススキャンをしてもらうとマルウェアが検知されたり、されなかったり

法人向けメールサービスでの特徴 (1)

- コンシューマー向けサービスと異なり、(顧客毎の設定で)送信元IPアドレスを制限することができる場合がある
  - ある顧客が、顧客ネットワーク出口からのみメール送信をする場合、これを適用可能
  - 「制限を適用された認証ID(ドメイン)は登録したIPアドレスからのみ送信可能」という設定
  - 送信元IPアドレスを制限していると、踏まれてもspam送信を防ぐことが可能
  - 一度踏まれた顧客には、制限の有効化の検討をおねがいしている

法人向けメールサービスでの特徴 (2)

- 認証ID単位の流量制限がしづらい
  - メルマガ、システムからのメール送信での利用
  - 無辜の顧客にとっては、「余計な制限が入る」ということにしかならない
  - 後から制限をかける場合、顧客の理解を得ることが難しい
- メルマガ送信をしている認証IDだけ流量制限を緩める？
  - 顧客が多いとすべてを把握するのは困難
  - 顧客からの申告ベースで緩めたり

踏まれspamとの戦いの歴史 (1)

- 古き良き時代

  ごくたまに(年1回？) 踏まれてspam大量送信

  ↓

  DNSBLに載る(早朝にレポートを飛ばしている) or queueが溜まりすぎてメールサーバーが過負荷でアラート

  ↓

  アカウントロックして、溜まっているqueueを退避して、delist申請

  巻き添えを受けたお客様からのクレームもそれほど多くはない状況

踏まれspamとの戦いの歴史 (2)

- メールが重要になってきた時代
  - ＝DNSBLに載って不達になると燃える時代
  - DNSBL監視に加え、送信MTAのqueue数監視
    - 宛先、流量などにも依るが派手に送られると検知まで3,4時間程度。低レートだと検知できないことも
  - 踏まれspamの発生件数が少ないときはこれでもなんとかなっていた

踏まれspamとの戦いの歴史 (3)

- 徐々に発生頻度が増えてくる
  (踏まれspam問題の顕在化)
- 踏まれspam送信の傾向を精査
  - 認証IDあたりの送信通数はあてにならない
    - メルマガやシステムからのメールなどを送っている顧客がたくさんいるため
  - 認証IDあたりの送信元IPアドレス数に着目
    - botnetから送られるので、異常に多くなる。しかも海外
  - 日次で集計で顧客対応

踏まれspamとの戦いの歴史 (4)

- 踏まれspamの発生件数の激増
  - 毎日のように発生するようになる
  - spam送信が重なるため、DNSBLに載る回数も多くなる
  - お客様からのクレーム数も増加
- 送信流量制限の導入 (2013/10末適用)
  - メールボックス型のみ。GW型は適用不可
  - 「1認証IDあたり10分でXXX通まで送信可能」
    - それ以上はtemplfail。下回る分は送信可能
  - 導入時(前)に多数の問い合わせ

踏まれspamとの戦いの歴史 (5)

- 送信流量制限が決め手にならない…
  - それなりに効果はあるが、検知して対応するまでは、流量制限の上限値でspamを送られてしまう
    - 稀にtempfailが1回でも返ると送信を止めるbotもいた
  - 1日あたりの送信通数制限も導入すると効果があるのは分かっているが、メルマガ・システムからの配信などがあるため適用するのが厳しい
    - コンシューマー向けサービスでは1日1000通の制限を2007年に実施済

踏まれspamとの戦いの歴史 (6)

- そもそも踏まれspamは海外のbotnetから送られるのがほとんどなので、そういった送信にフォーカスして絞ればいいのでは？

  → 流量制限への国別スコアリングの導入

  - 送信元IPアドレスの国によって流量制限の重みづけを変える (詳細後述)
  - 2014/02末適用。かなり効いた

踏まれspamとの戦いの歴史 (6)

- 最後の一手、outbound spam filter
  - メールボックス型の顧客のspam送信は国別送信流量制限の導入によってかなり抑えられた
  - GW型には意味がない
    - 送信元はすべて顧客MTA
    - 顧客MTAがopen relayになっていたり…
    - そもそも流量制限自体適用できない
- 顧客送信メールに対して、spamかチェック
  - 2014/06末導入

国別流量制限 (1)

- あるIPアドレスがどこの国に属しているかというデータベースがある
- submission時のsrc IPアドレスでlookupして、認証ID毎のメール送信通数に重みを付ける

例)

- 日本: 1通送信→1通分
- 中国・アメリカ: 1通送信→3通分
- ロシア・ポーランド: 1通送信→10通分
  (過去spamが頻繁に送られている国)
- その他の国: 1通送信→ 5通分
  ※ 実際の設定値とは異なります

国別流量制限 (2)

- 言いかえると…
  - 日本から送れば: 10分100通まで送れる 場合に
  - アメリカ(のみ)から: 10分33通まで
  - ロシア(のみ)から: 10分10通まで

国別流量制限 (3)

- 留意点 (はまった所)
  - gmailで別のMSAを利用して投稿をすることができる (サーバー、認証ID、パスワードを設定)
    - このサーバーのIPアドレスがUS
    - USからの送信なので、スコアがちょっと高めになっていて、送信可能数が少なめになる
    - 意図した挙動ではあるが、spam送信しているわけではなく、よろしくないのでgmailからは1通分に変更
      - maillogに残っていたIPアドレスをwhoisで検索して、IPアドレスブロックで登録…
    - 今後ここからもspamが…？

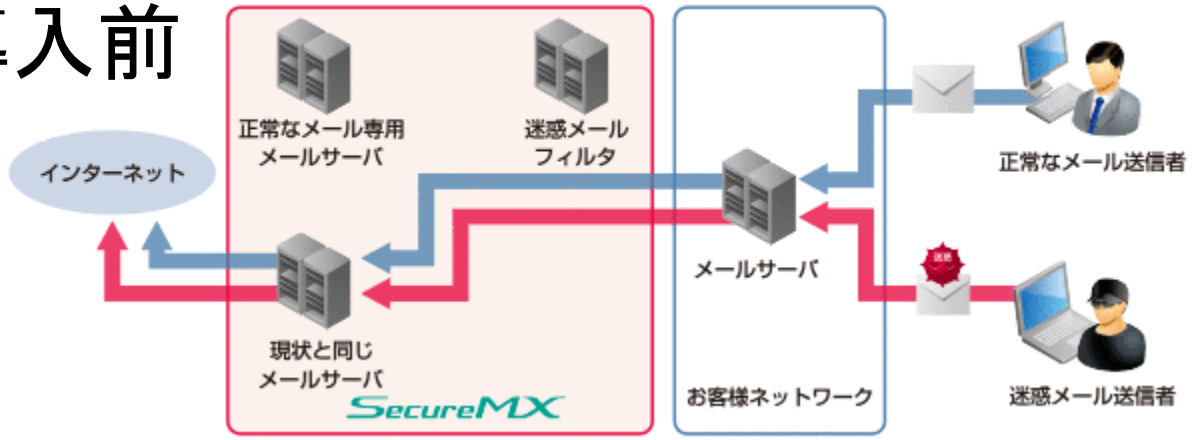
outbound spam filter概要 (1)

- 顧客の送信したメールに対してもantispam製品でscan
  - 適用するのは個別同意を得た顧客のみ

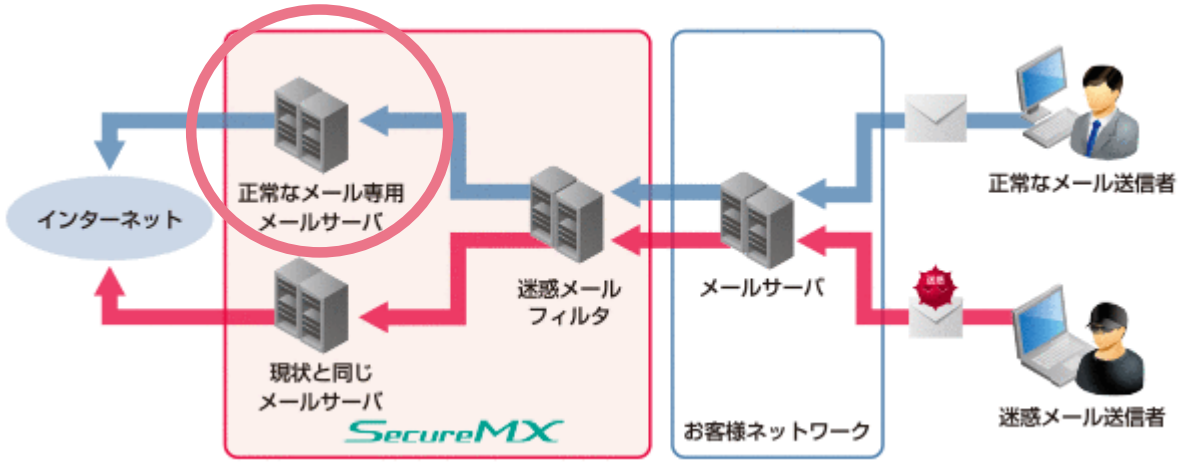
    (新規顧客に対しては、サービス契約時に同意をいただく)
- 「きれいな出口」を新設
- not spamのメールは「きれいな出口」から送信し、spam判定されたメールは「今までの出口」から送信
  - 「きれいな出口」がDNSBLに載る可能性が低下

outbound spam filter概要 (2)

■ 導入前



■ 導入後　↓「きれいな出口」を新設



送信メールへの迷惑メールフィルタ適用、および判定結果に基づく送信サーバの切替について

送信メールの送信先サーバへの到達性向上を目的として以下を実施いたしますので、ご確認のうえ、同意願います。

背景

昨今SMTP認証に使うメールアカウントのIDやパスワードの情報が、ウイルス感染等何らかの手段で盗まれ、正当な利用者ではない第三者により、迷惑メールの送信に悪用される事象が発生しております。

IIJセキュアMXサービスにおきましても、一部のお客様になりすました第三者による迷惑メールの大量送信が多発しており、お客様の送信した正常なメールが送信先サーバにおいて迷惑メールとして配信拒否される原因となっております。

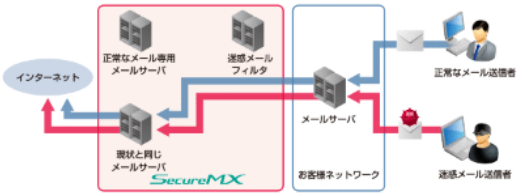
対策の概要

現状、お客様の送信されたメールは迷惑メールか否かに関わらず全て同じ送信メールサーバから送信されます。
本対策ではお客様の送信されたメールに対して迷惑メールフィルタを適用し、ヘッダ、本文等の情報から迷惑メールか否かを判定、迷惑メールと判定されないメールは正常なメール専用の送信サーバから送信します。

これによりお客様が送信された正常なメールの送信先サーバへの到達性向上が期待できます。

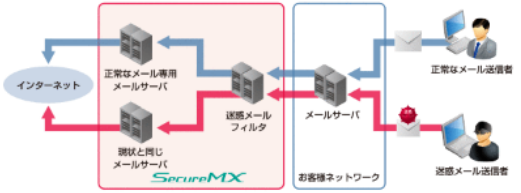
動作

- 対策適用前(現状)
  現状と同じ送信メールサーバから送信します。



- 対策適用後
  1. 迷惑メールと判定されたメール
     現状と同じ送信メールサーバから送信します。

  2. 迷惑メールと判定されない正常なメール
     正常なメール専用の送信サーバから送信します。



注意事項

1. 本対策の適用は契約単位で行われます。
2. 特定のドメインまたはメールアドレスを適用外にすることはできません。
3. 迷惑メール判定結果のお客様への通知は行いません。
   また判定結果によるサービスでの配送拒否、隔離は行いません。
4. メールボックスオプション、メールボックスプラスオプションでの契約ドメイン宛のメール、転送設定により転送されたメールは適用外です。
5. 適用ボタン押下後に即時本対策が適用されます。取り消しの際には、お客様窓口までその旨、お申し出ください。
6. 適用後、このページは非表示になります。

同意確認

以下、チェックボックスにチェックし、適用ボタンを押下してください。

☐ 送信メールに対する迷惑メールフィルタの判定結果に基づく送信サーバ切替に同意します。

適用　戻る

同意画面

outbound spam filter概要 (3)

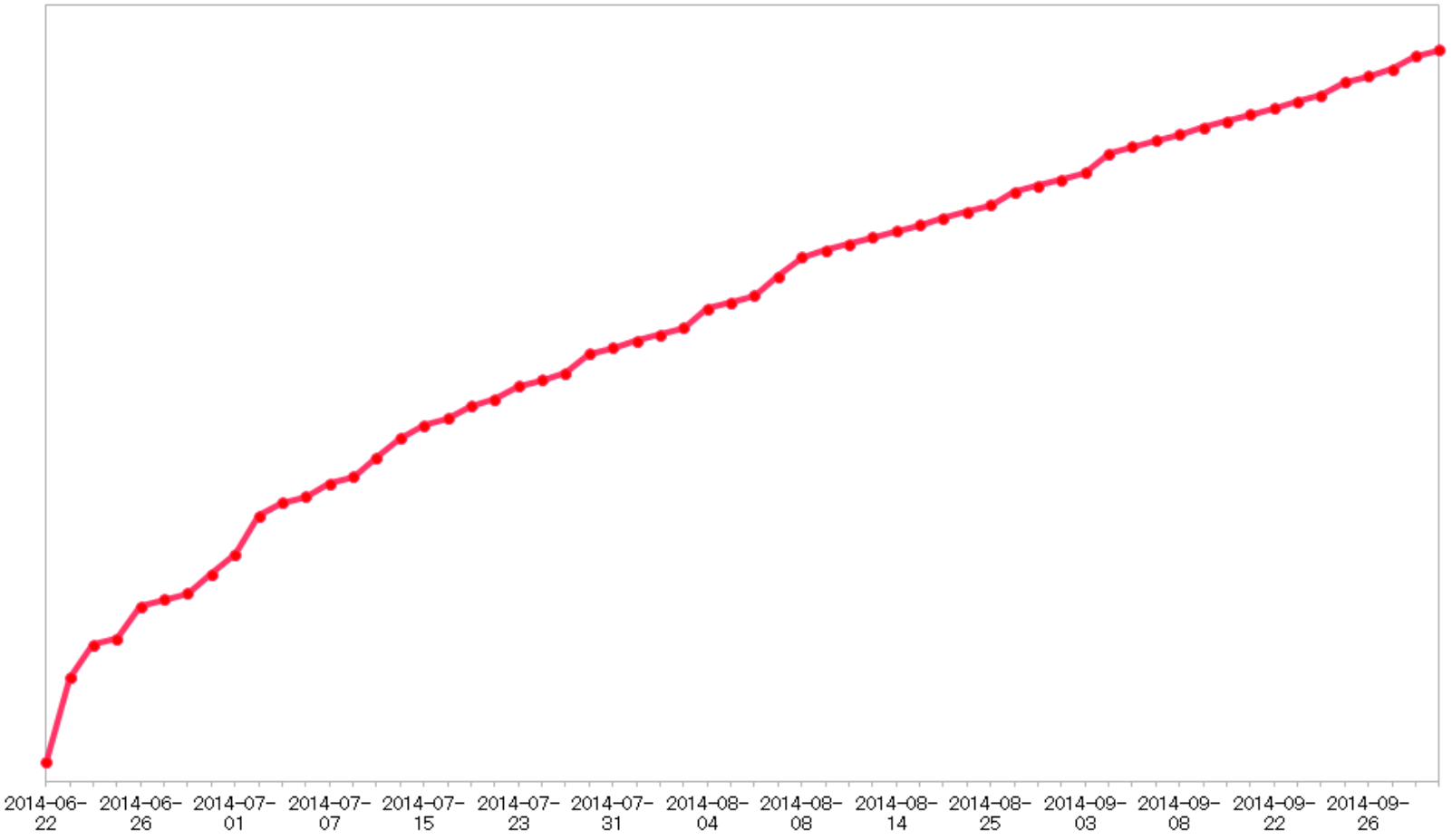
- spam判定されたメールの出口を「今までの出口」にした理由
  - 同意することに対するインセンティブを持たせたい
    - 同意しないと、他顧客の踏まれspam送信に巻き込まれる出口のまま
- 同意することによるデメリットはない
  - F/Pが発生しても「今までの出口」から送信はされる
    - 逆に、止めたりするとF/Pが発生した際にまずい…
  - 受信側同様、人間が中身を見ているのではない

outbound spam filterの効果 (1)

- 同意顧客: 全体の1/3社程度
- 通常時のメール流量比: 今まで:きれい=10:1
  - 規模の大きな顧客が未同意なため
- 同意顧客数の推移
  - 導入直後にそれなりの件数
  - その後は日々ぽつぽつと。緩やかではあるが、着実に増加

outbound spam filterの効果 (2)

- 同意顧客数の推移



outbound spam filterの効果 (3)

- DNSBLへの掲載回数
  - 国別送信流量制限の適用時期あたりからほとんど載っておらず、効果は不明
    - 国別送信流量制限の効果
    - そもそも、踏まれspamの発生件数が低下している

しかし、効果は大きいとはずと考えています

outbound spam filterの効果 (4)

- 実際のspam送信時の検知率
  - ケースA: 検知率50%
  - ケースB: 検知率90%
  - ケースC: 検知率90%
  - ケースD: 検知率5%
  - 受信側より検知率は悪い印象だが、相当にケースバイケース
    - パターンファイルで対応しているspamか？
    - 送信の終息が早いか、長く続くか

⇒実際に効果はある。

困っている各社さん、是非導入しましょう

outbound spam filterその他 (1)

- 顧客からよくある質問
  - 「もしspamと誤判定されたら、送ったメールはどうなる？」
  - 「同意すると、どういうメリットがある？」
  - 「同意した場合に、何かデメリットはあるか？」
  - 「同意する以外に(顧客側で)何かやらなくてはならないことはあるか？」
    - 「SPFレコードに追加が必要か？」
    - 「なんとなく不安」など
- 説明すれば、納得して同意いただけている

outbound spam filterその他 (2)

- 会場から聞かれそうな質問
  - コンシューマー向けにはどうか？
    - 同様に効果は大きいはず。困っているなら導入するべき
    - 一律適用のための5条件
      http://www.slideshare.net/softest/isp-32320513/23
  - ライセンスフィーは？
    - 受信側と共通で、全アカウントで受信側のantispamがかかっているので、今までと変わらない
  - outbound spam filterの次の対策は？
    - 今のところは考えていない。まずは全顧客適用を目指す

IIJ Internet Initiative Japan

Any Questions?

Ongoing Innovation