コンシューマ向けメールサービスでの Submission踏み台問題の現状と対策

- Open Computer Network -

2014/10/08
NTTコム ソリューション&エンジニアリング株式会社
阿部 敏一(tosikazu@ocn.ad.jp)

自己紹介

所属: NTTコム S&E株式会社 エンジニアリング事業部

氏名: 阿部 敏一(あべ としかず)

略歴:
2000/08　OCNのメール保守運用業務に着任
2013/09　OCNのメール系各種雑務に担務替え

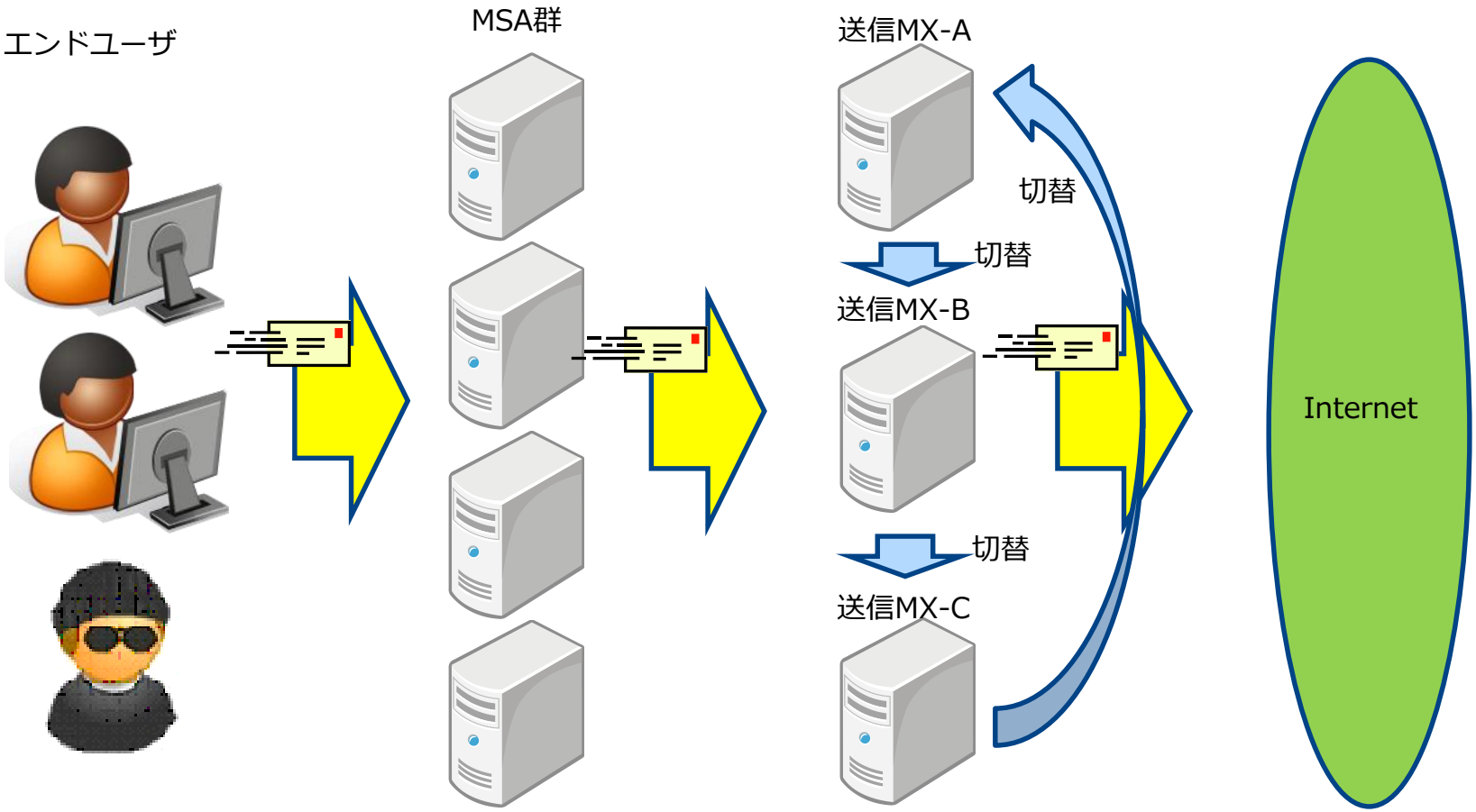
趣味:
自転車全般(ロードバイク、マウンテンバイク等々)

Submission踏み台 今までの対策

各社さんでも実施かと思いますが…

- 各種レートコントロール(パラメータチューニング)
- IPアドレス切り替え(MXのローテーション運用)
- 宛先毎のメール配送ルート変更(その時々で色々と)
- DNSBLにIPアドレスが登録されないように祈る
  (祈りが届いた試しはないですが…)

IPアドレス切り替えについて



一定期間で送信MXを切り替えて運用してます

そしていたちごっこ

対策をスルーされるまでの期間(実体験)

- **Env Fromでの制限強化**
  - **⇒ 1週間程度で解析された模様**
- **SMTP認証の制限強化**
  - **⇒ 3日程度で解析された模様**
- **レートコントロールのロジック追加やパラメータチューン**
  - **⇒ 最速だと1日程度で解析されるケースも**

ガイドライン改定

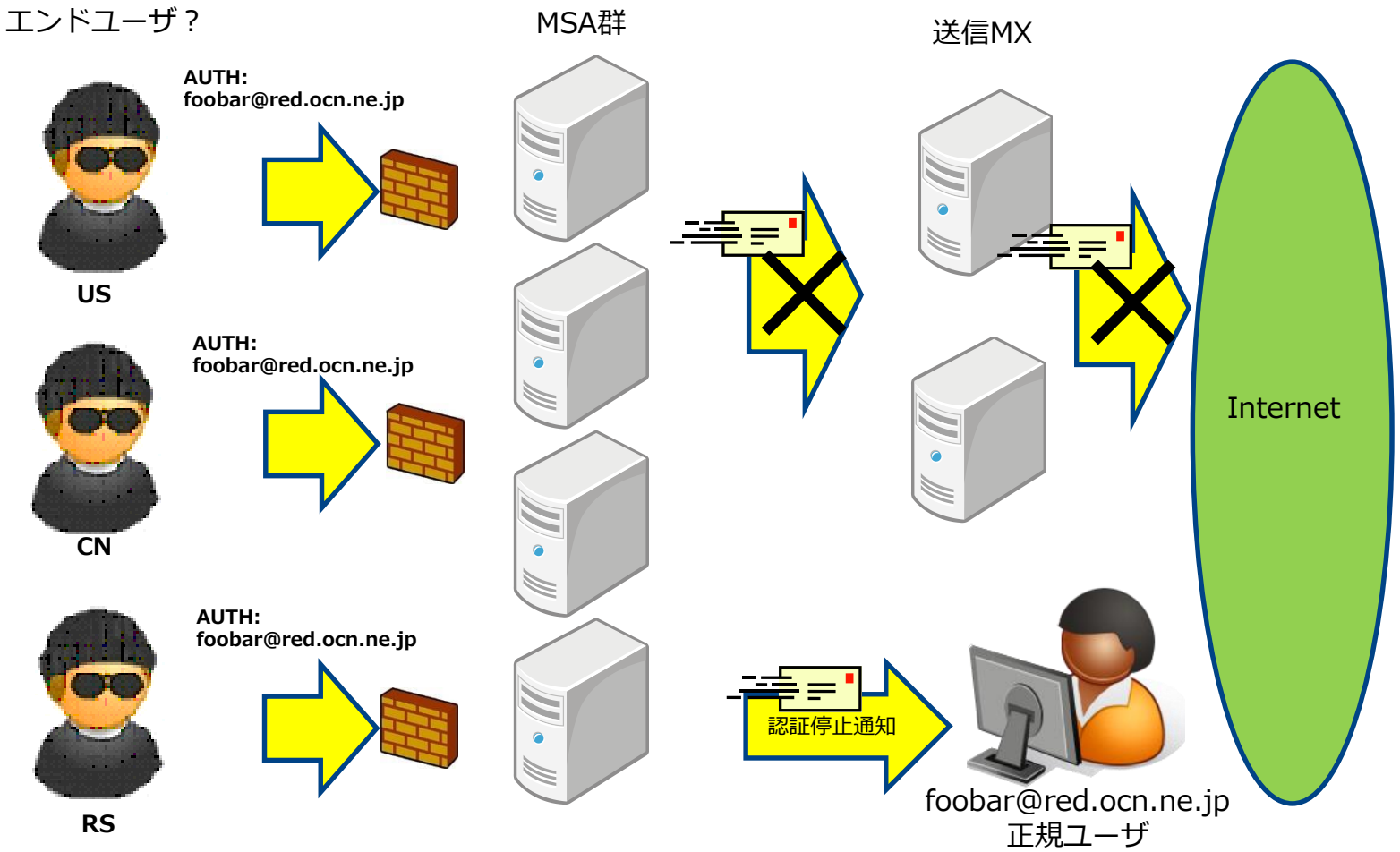
今年はこんな感じで検討がされました

【総務省】
電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会
第一次とりまとめ(2014/04/04)
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000074.html

【インターネットの安定的な運用に関する協議会】
電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン
改定(2014/07/22)
http://www.jaipa.or.jp/topics/?p=695

電子メールについては、先の資料にあった通りだが、それ以外の事も色々言及されているので、一見の価値あり。

ガイドライン改定に則って対策してみた



複数の国から短時間で同一IDでのSMTP認証一時停止および、正規ユーザへの自動通知機能実装

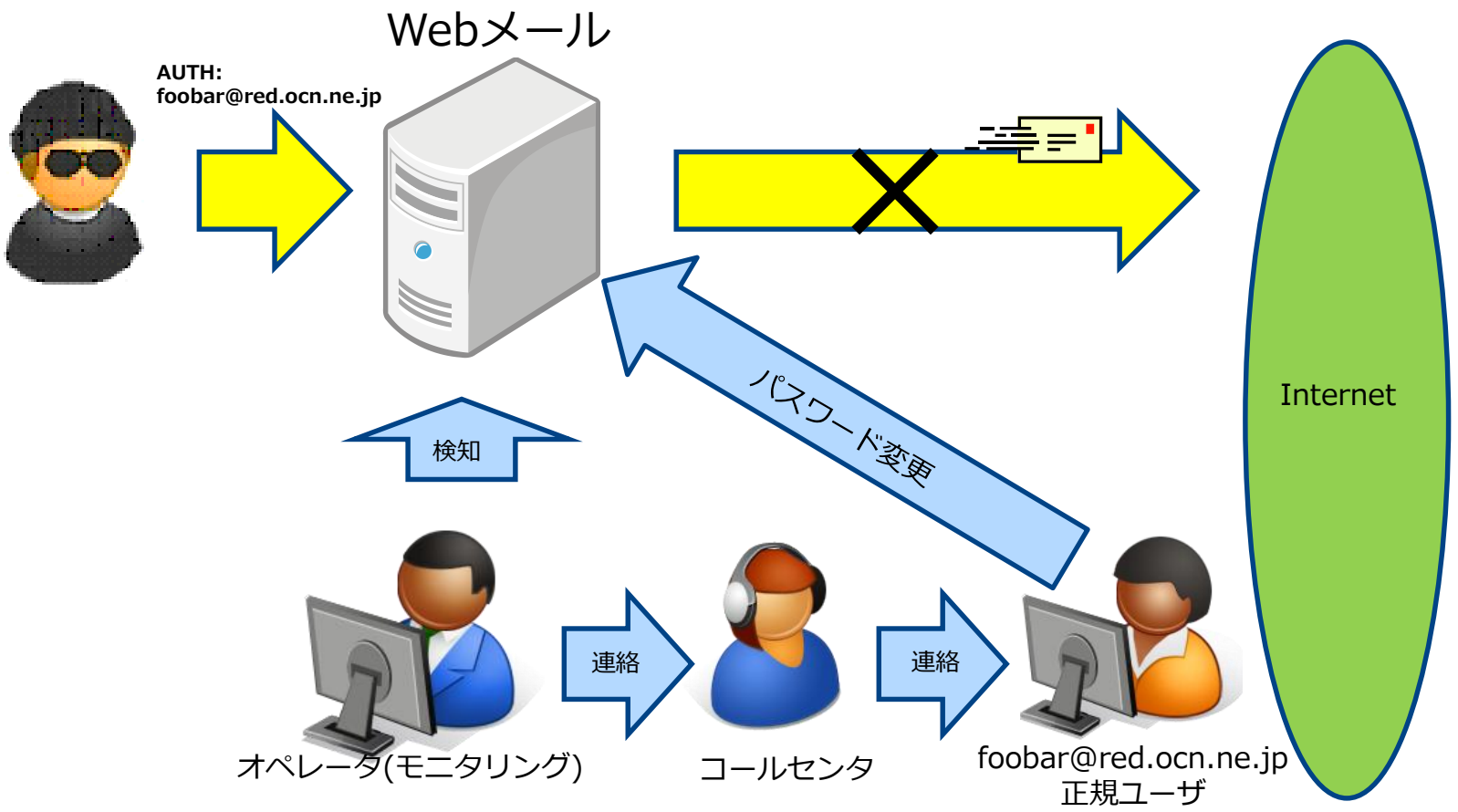
状況(トラフィック)

会場限り

MSA接続元IPアドレスの国別データ

会場限り

(余談)Webメールも踏み台になっていたので



オペレータが検知したものを、コールセンタ経由で
ユーザに連絡を実施し、パスワード変更を促している

今後考えてみたい方法や実装(1)

＊Submission踏み台

・基本的には、引き続きいたちごっこ。相手に合わせて対応するしかない。
・Outbound Filteringあたりは有望な気がする。

今後考えてみたい方法や実装(2)

＊Webメール踏み台

・アドレス、パスワードを盗用されないことも、当然大事だが、現実として盗用されているので、それに対する対策を実施する必要はある。

・OpenID側で、こんな実装を追加してもいいかもしれない。

→ リスクベース認証。

→ パスワードのexpire。もしくは期限が来たら毎回変更を促す画面を出してみる。

→ SMS等を使った多要素認証(一部のみ実装)。

今後考えてみたい方法や実装(3)

＊対策を実施する上で
・ユーザのネットリテラシや、アナウンスと兼ね合いもあり、
どこまで何を実施できるかも含めて、検討が必要。
(他社さんはどうしているんだろうか…)

ご清聴ありがとうございました。