第11回
迷惑メール対策カンファレンス

次に見据えるべきスパム対策
～display-name のなりすまし問題～

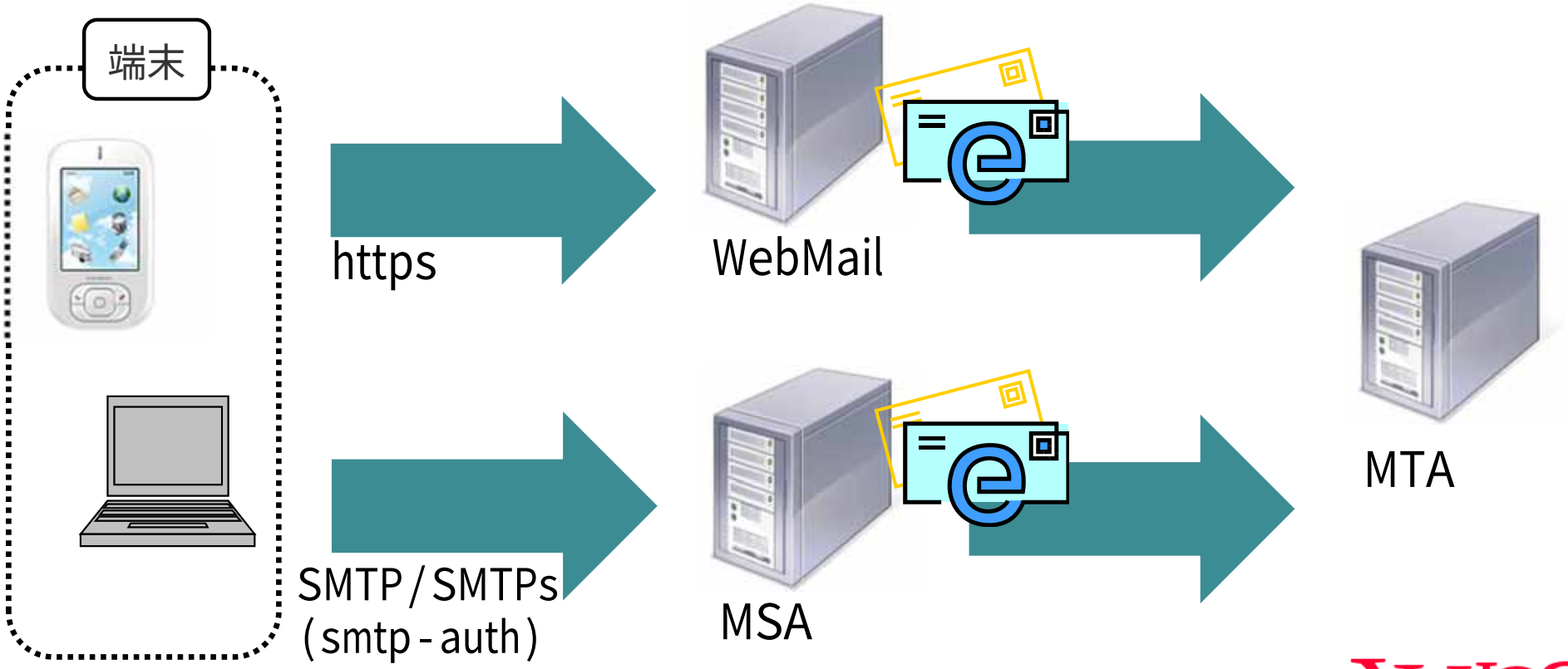
ヤフー株式会社
パーソナルサービスカンパニー メール本部
鈴木康平

実際に発生している・発生しうる問題
(ヤフー発の) 銀行なりすましメールの事例紹介

Yahoo!メール メール送信システム概況

* 「WebMail」と「MSA(SMTP)」の2種類
* 最近はPC利用からスマホ利用へのシフトが進行
* スマホ利用形態は「メールアプリ」や「IMAP/SMTP」等

メール送信の流れ

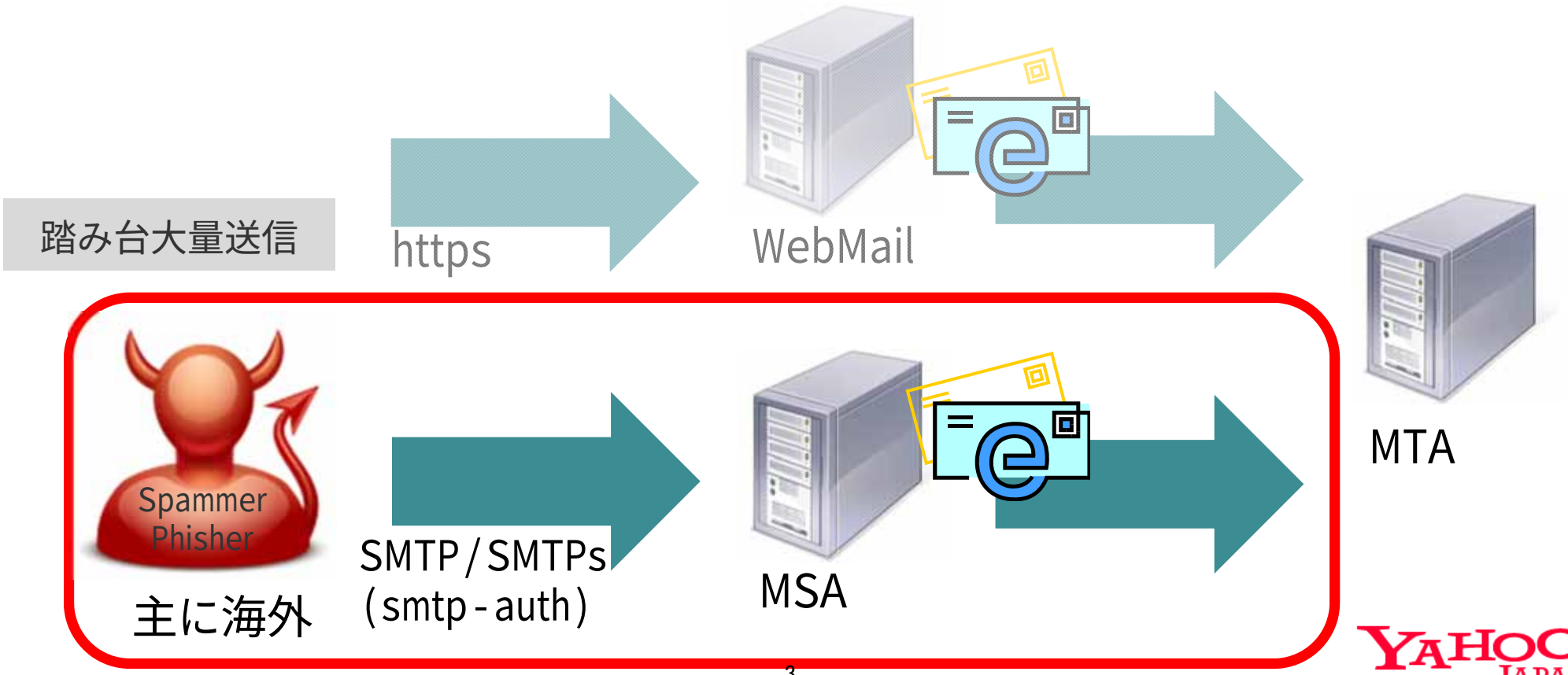


YAHOO! JAPAN

MSAの踏み台問題

踏み台問題が顕著に

- 昨年末(2013年末)あたりから
- 発信元は海外
- MSA経由
- ユーザー「見に覚えのないバウンスメールが届く」



なりすましメール 実例1

Header

Received - SPF: pass ・・・
Authentication - Results: mta502.mail.kks.yahoo.co.jp
from=yahoo.co.jp; … dkim=pass (ok); header.i=@yahoo.co.jp
Subject: 【○○○○銀行】本人認証サービス
From: ○○○○銀行 <yahoo_hanako@yahoo.co.jp>
To: yahoo_taro@example.com

Body

(平成26年7月12日更新)「[redacted]銀行」ではアカウントの安全性認証を行われるため、
お客様はアカウントが凍結?休眠されないように、直ちにアカウントをご認証ください。

本人認証サービス

なりすましメール 実例2

Header

Body

Received-SPF: pass …
Authentication-Results: mta545.mail.kks.yahoo.co.jp
from=yahoo.co.jp; … dkim=pass (ok); header.i=@yahoo.co.jp
Subject: ○○○○銀行 – メールアドレスの確認
From: ○○○○銀行 <yahoo_hanako@yahoo.co.jp>
To: yahoo_taro@example.com

お使いのメールアドレスを確認してください

メールアドレスを確認する

display-name で必ず銀行名を騙っている（視認性の悪用）
Fromアドレスを騙らない（DMARCはpass）

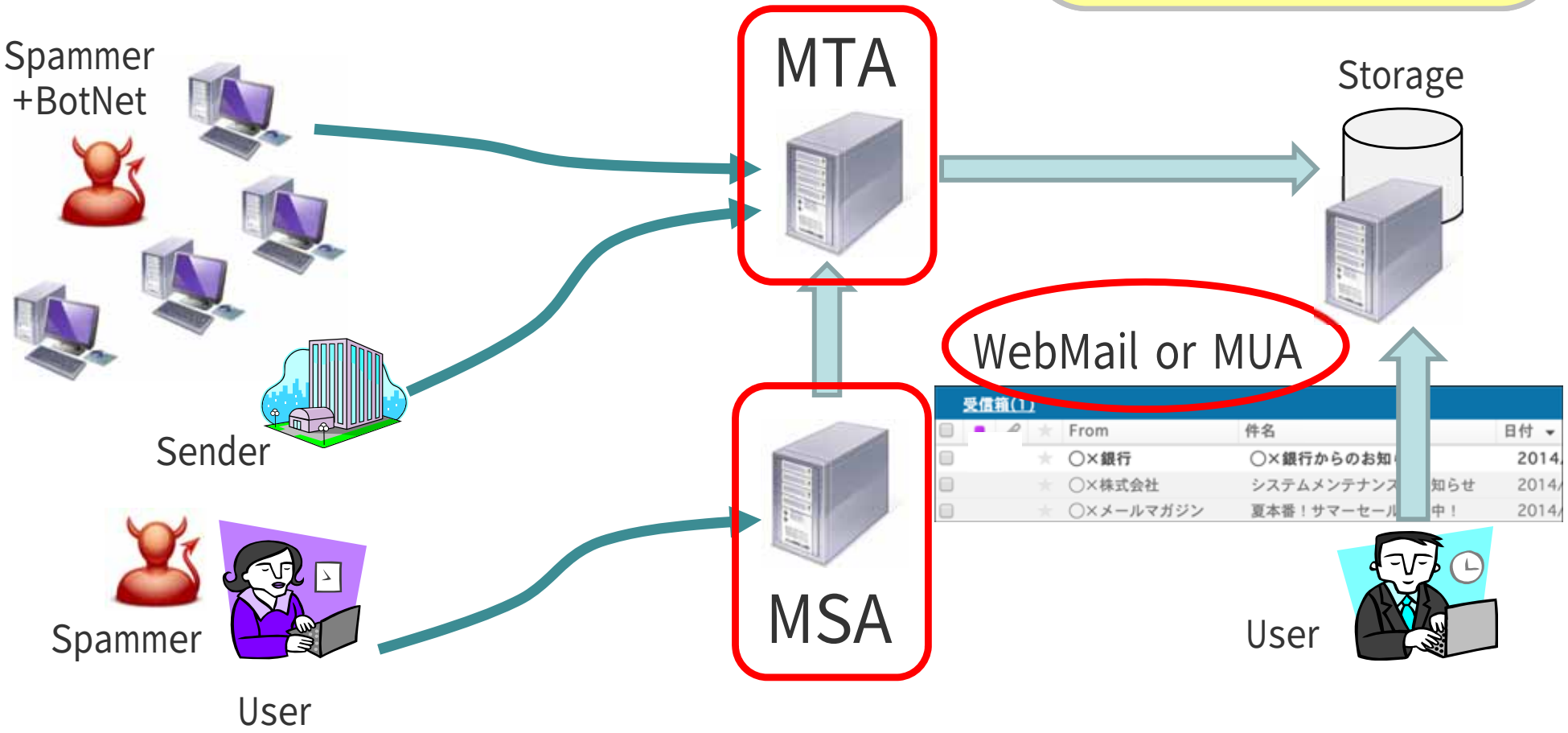
display-name 考えられる対策や課題

display-name問題の対策ポイント

MSAでの対応

MTAでの対応

WebMail or MUA での対応

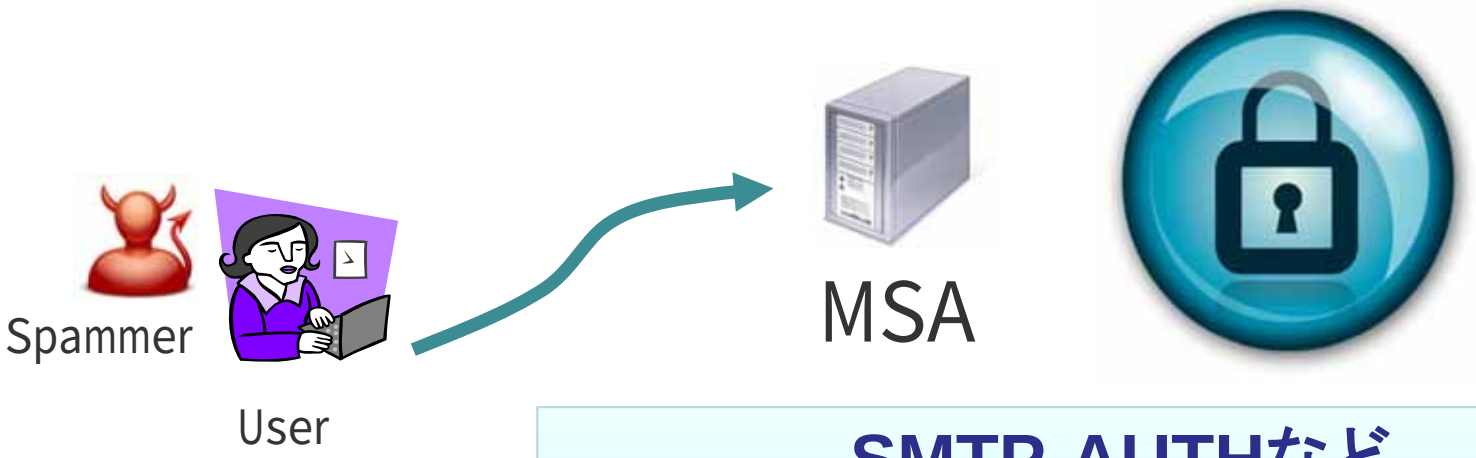


display-name問題に対して
直接的、または間接的に効果があるであろう対策を考えてみる

MSAで考えられる対策（1/2）

前提条件にあたるであろう対策

* SMTP認証
* 送信ドメイン認証 (DKIM,SPF)
* AuthID と MAIL FROM の一致性確認
* AuthID と RFC5322.From の一致性確認

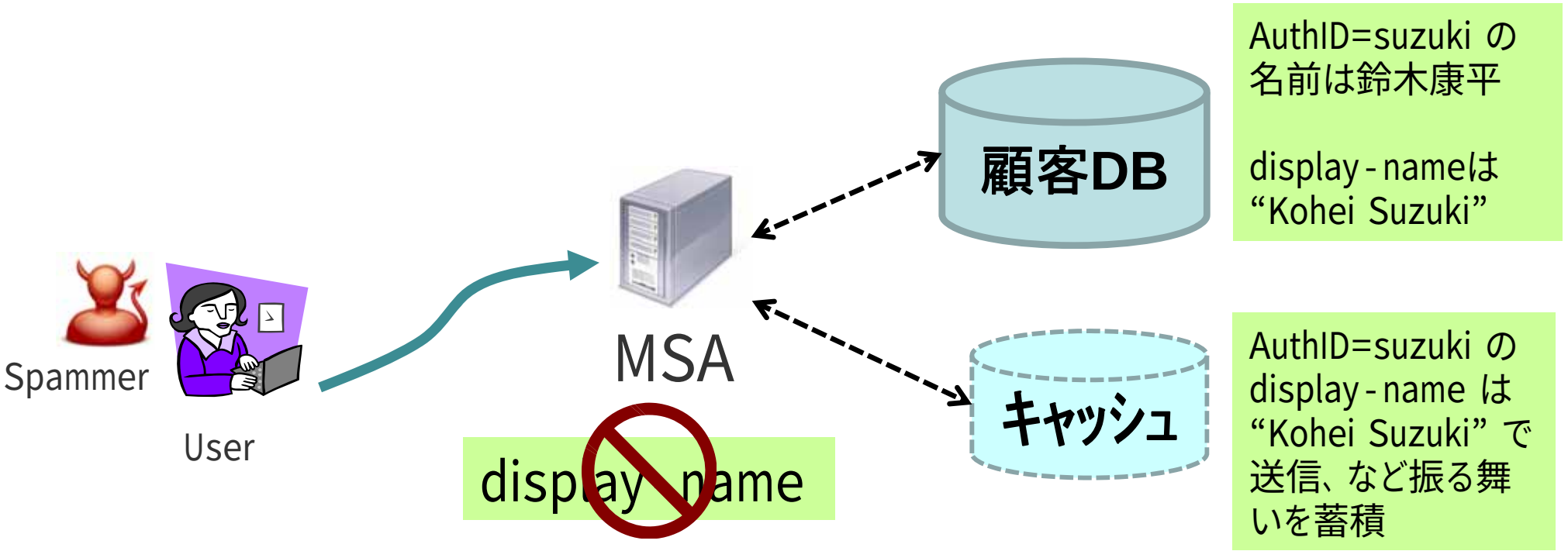


SMTP-AUTHなど
基本的な機能提供はしっかりやる

MSAで考えられる対策（2/2）

display-name のマナーチェック

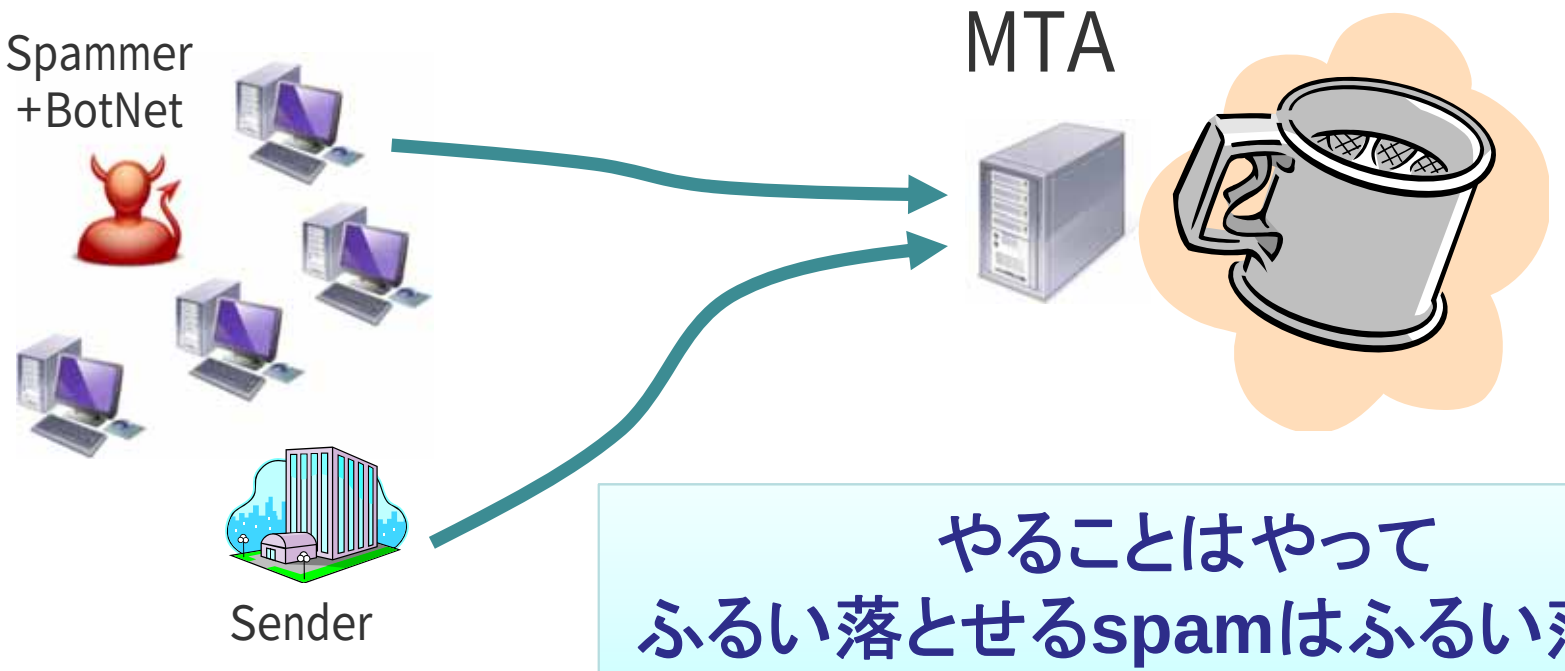
* 顧客名との一致性、顧客名への強制上書き
* 過去の表示名との一致性（ふるまい検知）
* display-name内でのアドレス利用禁止
* display-name自体の利用を禁止



MTAで考えられる対策（1/2）

前提条件にあたるであろう対策

* 送信ドメイン認証 (DMARC)
* ドメインレピュテーション

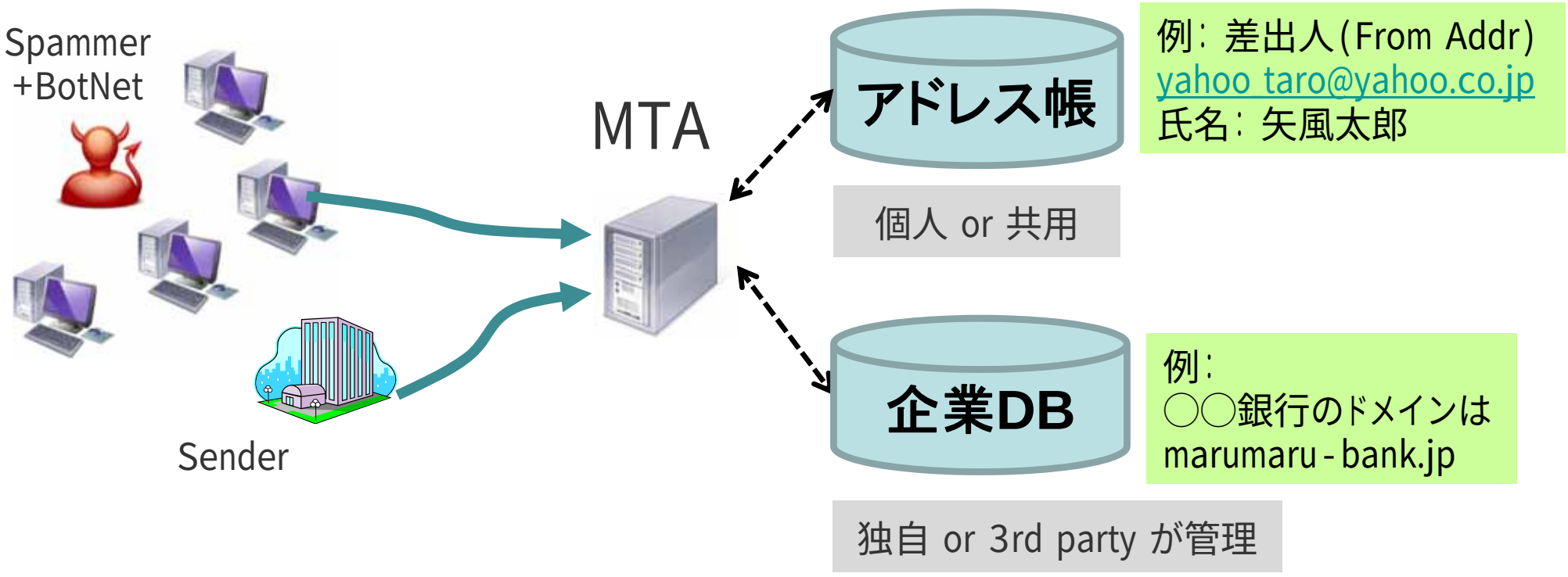


やることはやって
ふるい落とせるspamはふるい落とす

MTAで考えられる対策（2/2）

display-name のマナーチェック

* アドレス帳 (display-name, address) との一致性
* 企業名 (銀行等) との一致性・不一致性
* 信頼できなければspam判定する等
  - display-name削除はやりすぎ？



WebMailで考えられる対策（1/2）

見せ方をどうするか

* display-nameを非表示
  - spam判定したメールならば現実的？
* display-nameのみではなくメールアドレスも表示
* アドレス帳とのマッチング
  - マッチした差出人はdisplay-nameをアドレス帳のものに上書き
  - マッチしない差出人はdisplay-nameを表示しない
  - マッチしないメールはメール自体を見せない

yahoo taro@yahoo.co.jp
矢風 太郎

WebMail or MUA

User

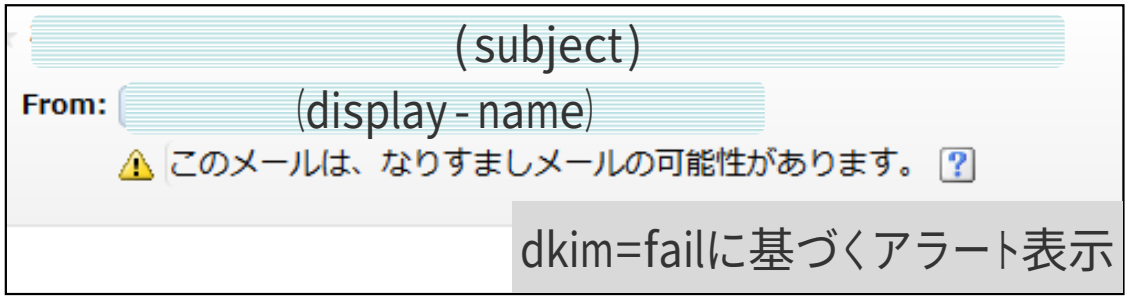
Fromヘッダが
“Taro Yahu” <yahoo_taro@yahoo.co.jp>
であっても UI上は 矢風 太郎 と表示

WebMailで考えられる対策 (2/2)

その他の対策

* 正しいメールの強調表示
* アラート表示
* バウンサーページ

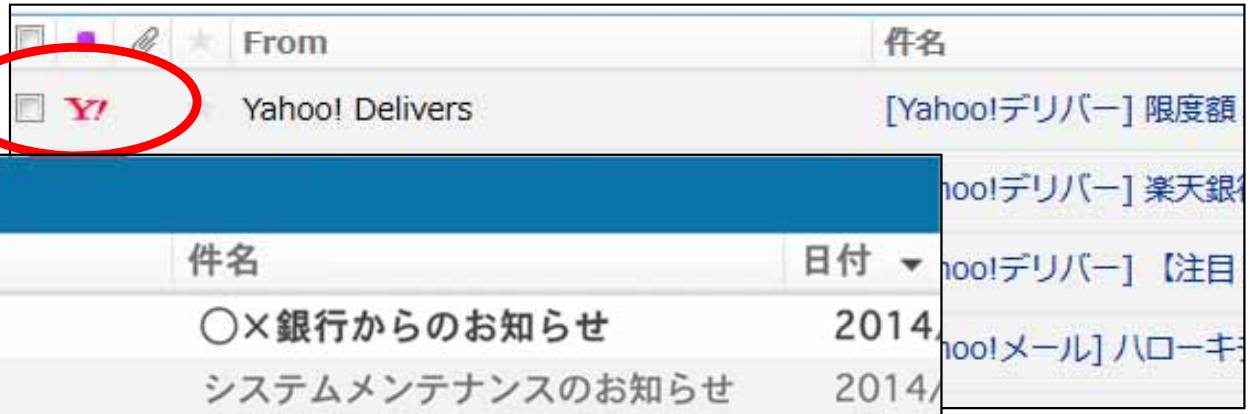
バウンサーページ



dkim=failに基づくアラート表示

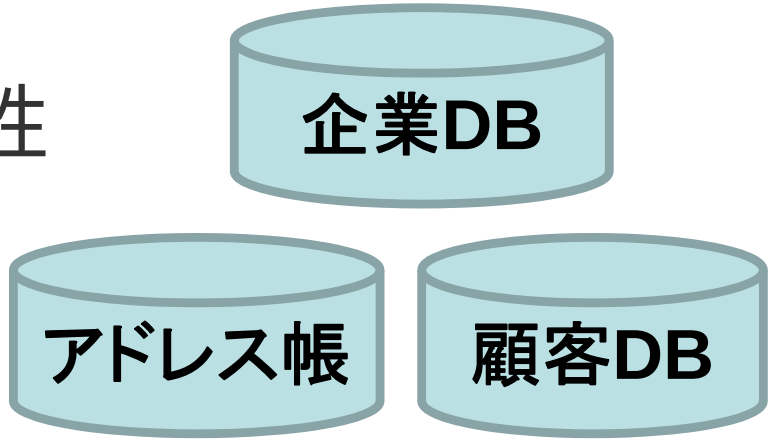
安心マーク

Y!アイコン



display-name問題 対策に向けた課題

- display-nameの表記揺れ
  - From: “鈴木康平” <kohei.suzuki@example.com>
  - From: “Kohei Suzuki” <kohei.suzuki@example.com>
  - From: “◯部△課 鈴木” <kohei.suzuki@example.com>
- DB（顧客情報、企業情報、レピュテーション）との連携、精度
  - display-nameは自由度の高い情報
  - 正確に管理し、ユーザの期待どおりの連携、精度で実行できるのか
- アドレス帳との連携/精度/信頼性
  - アドレス帳管理のコスト
  - アドレス帳はDBより乗っ取りが容易



display-name問題 対策に向けた課題

- display-nameの上書きや非表示
  - 健全なメールは利便性、視認性が犠牲になるケースも
    - 例： ローカルパートがランダムな文字列
  - 仕様変更のインパクト
    - 例： MUAで設定したdisplay-nameは採用せず、AuthIDに紐付いた表示名で強制的に送信メールを上書きすると仕様変更したときのサポートコスト

- 個人事業主のメールマガジン
  - display-nameの規制強化をしたISP、そこを利用する個人事業者にとって影響は大きい

- 法律の問題
  - display-nameの解析、上書き、禁止や削除（非表示）
  - 送信者偽装か、正当業務行為か

display-name問題　まとめ

- 対策すべき対策はやっておく
  - SMTP認証、送信ドメイン認証技術（DKIM,SPF,DMARC）など
- display-name問題に銀の弾丸は存在しない
  - 今後、さらに問題となっていく可能性がある
  - ここにあげたものは有効であろう対策の例
  - とはいえ、これは良さそうと感じた対策、できそうな対策は検討して対策を進めていくべき

display-name問題を課題と認識し、少しずつでも対策を協議、検討し、実施していくことが大切

EOP