DKIMの抱える問題点とその対策

北川 直哉

東京農工大学大学院 工学研究院 先端情報科学部門

DKIM検証で見破れないなりすまし例 (1)

- DKIM Signatureに対応していないドメインへのなりすまし
  - 某大手宅配業者([redacted].co.jp)の例

（正当な送信の場合）本物メールはDKIM検証できない

- Header-Fromドメイン名 = [redacted].co.jp
- DKIM Signatureドメイン名 = DKIM非対応のため無し

（想定されるなりすまし例） DKIM対応で信頼確保を狙う

- Header-Fromドメイン名 = [redacted].co.jp
- DKIM Signatureドメイン名 = attacker.com

DKIM検証で見破れないなりすまし例 (2)

- DKIM Signatureを意図的に付加しないなりすまし
  - 東京農工大学教職員メール(cc.tuat.ac.jp)の例

（正当な送信の場合）Office365利用のためMicrosoftが署名

・Header-Fromドメイン名 = cc.tuat.ac.jp
・DKIM Signatureドメイン名 = cc.tuat.onmicrosoft.com

（想定されるなりすまし例）受信側は署名がなければ検証せず

・Header-Fromドメイン名 = cc.tuat.ac.jp
・DKIM Signatureドメイン名 = DKIM署名なし

DKIM検証で見破れないなりすまし例 (3)

- 悪意ある第三者ドメインによるDKIM署名
  - 東京農工大学教職員メール(cc.tuat.ac.jp)の例

（正当な送信の場合）Microsoftによる第三者署名
・Header-Fromドメイン名 = cc.tuat.ac.jp
・DKIM Signatureドメイン名 = cc.tuat.onmicrosoft.com

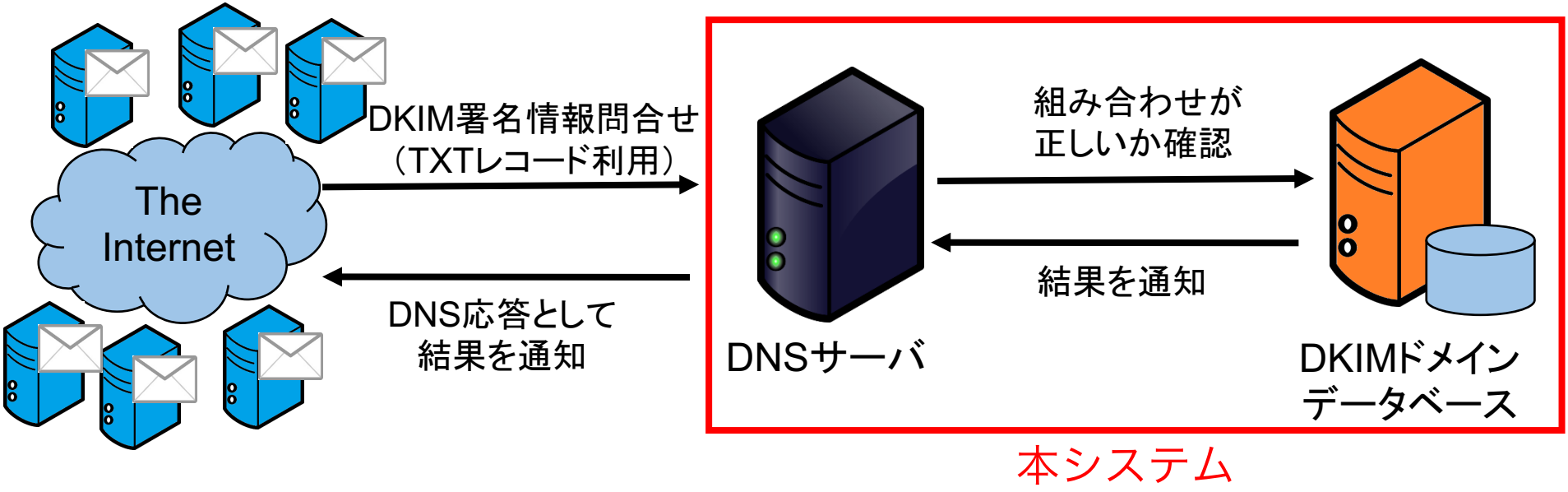
（想定されるなりすまし例）上の例も第三者ドメインだが…
・Header-Fromドメイン名 = cc.tuat.ac.jp
・DKIM Signatureドメイン名 = attacker.com

受信側では正しい署名ドメイン名を知る術がない！

DKIM署名の信頼性検査システム

各送信ドメインにおいてこれらをDKIM検証と合わせてチェック

- DKIM署名の有無
- 送信ドメイン名とDKIM署名ドメイン名の組み合わせ



B. Rienthong, N. Kitagawa, N. Yamai,“Countermeasure of Spoofed e-mails by checking the validity of DKIM signature”, Workshop on Internet Architecture and Applications 2016, Taipei, Nov. 2016

データベースシステムへの問合せ例

- （注）現在のところ非公開のサービスです

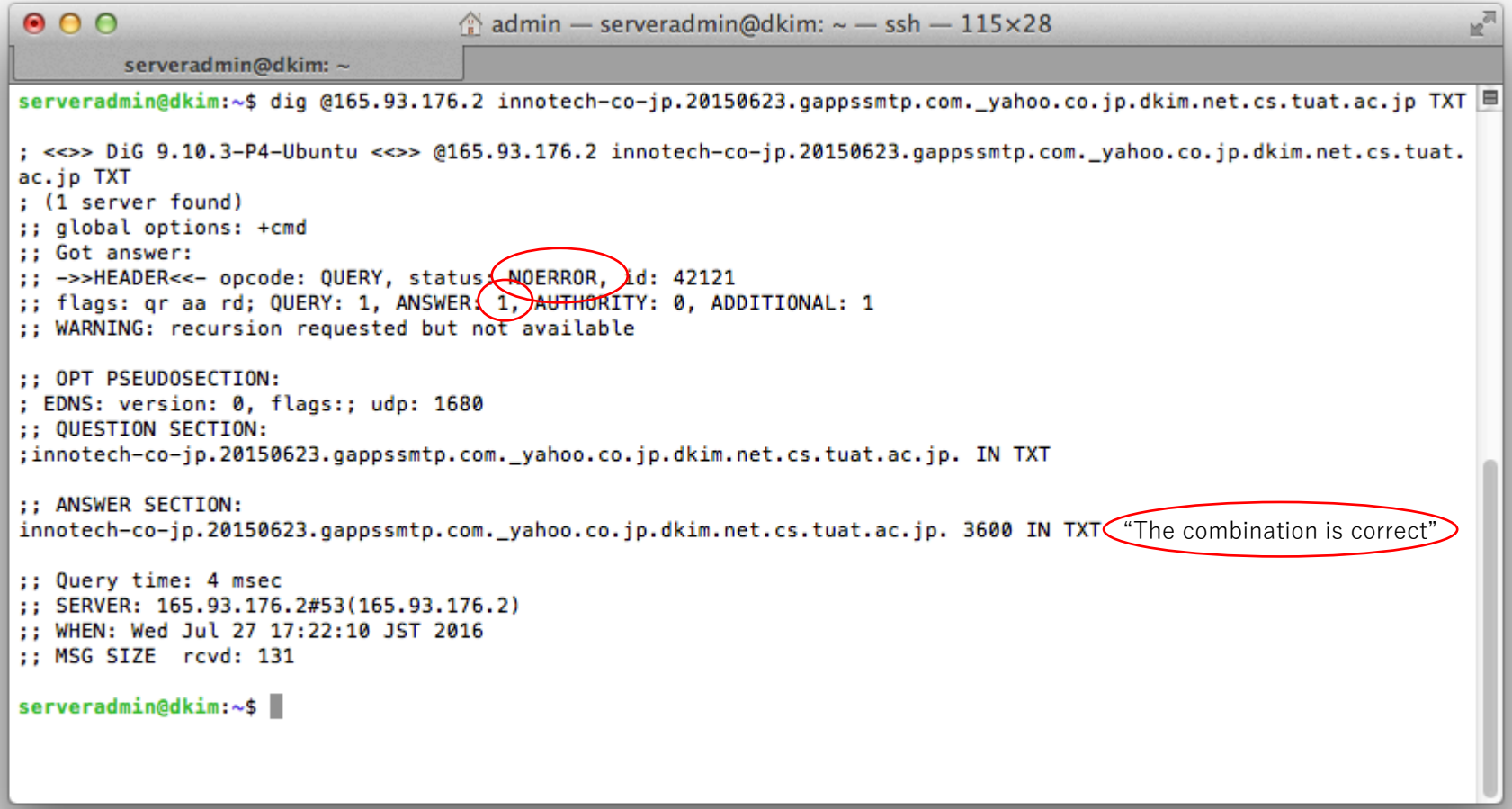
DKIM署名ドメイン名._送信元ドメイン名.本システムのFQDN TXT

（以下のようなメールの場合の問合せ例）

innotech-co-jp.20150623.gappssmtp.com._yahoo.co.jp.本システムのFQDN TXT

Picture from:https://wordtothewise.com/2014/04/brief-dmarc-primer/

応答結果（組み合わせが正当な場合）



応答結果（組み合わせが不正な場合）

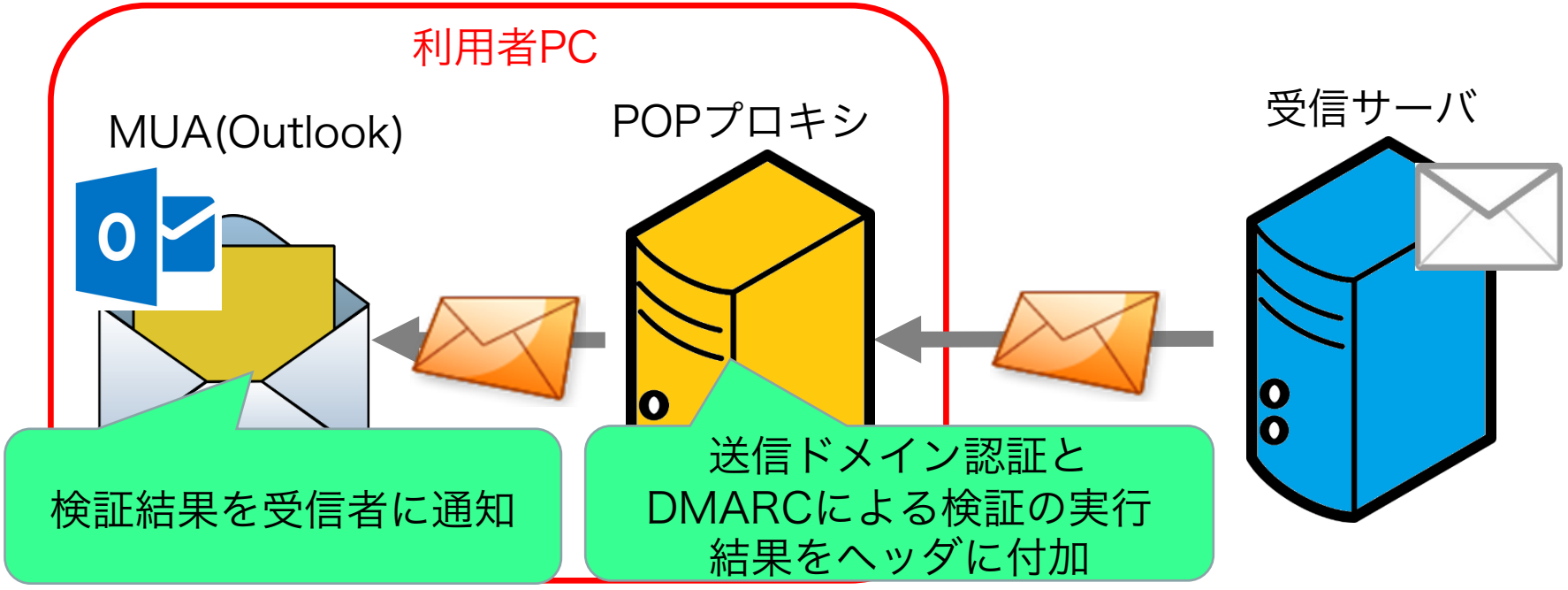
admin — serveradmin@dkim: ~ — ssh — 115×28

serveradmin@dkim: ~

```
serveradmin@dkim:~$ dig @165.93.176.2 gappssmtp.com._yahoo.co.jp.dkim.net.cs.tuat.ac.jp TXT

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @165.93.176.2 gappssmtp.com._yahoo.co.jp.dkim.net.cs.tuat.ac.jp TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 45154
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1680
;; QUESTION SECTION:
;gappssmtp.com._yahoo.co.jp.dkim.net.cs.tuat.ac.jp. IN TXT

;; AUTHORITY SECTION:
dkim.net.cs.tuat.ac.jp. 3600    IN      SOA     dkim.net.cs.tuat.ac.jp. admin.dkim.net.cs.tuat.ac.jp. 1 10800 3600
604800 3600

;; Query time: 0 msec
;; SERVER: 165.93.176.2#53(165.93.176.2)
;; WHEN: Wed Jul 27 17:27:44 JST 2016
;; MSG SIZE  rcvd: 120

serveradmin@dkim:~$
```

個人で導入できるDMARC検証システム

- 受信するメールに対しDMARCによる検証を実行
- POPプロクシで検証を実行，利用者PC上で実装
- 利用者に検証結果を通知し，危険な場合は警告



N. Kitagawa et al., “Design and Implementation of a DMARC Verification Result Notification System”, The 13th APAN Research Workshop, Hong Kong, Aug. 2016.

検証結果の通知パターン

- 適用されたポリシに応じて通知方法を組み合わせる

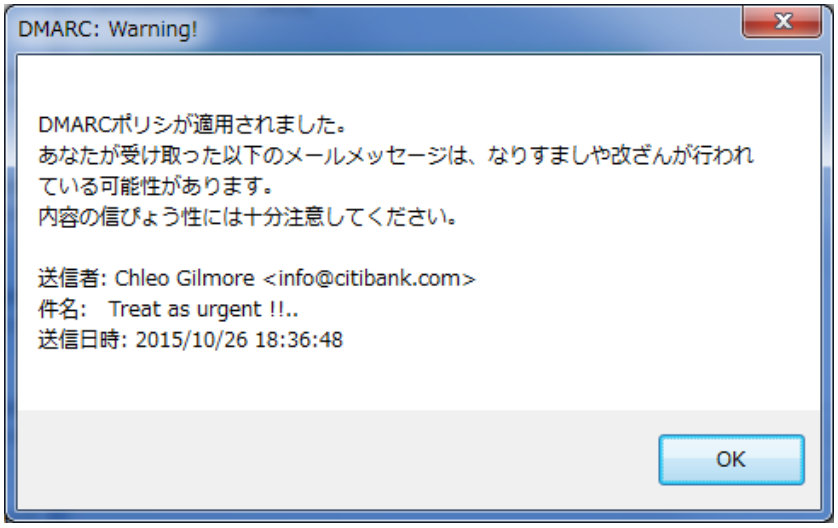
検証結果	pass	none	quarantine	reject	other
ラベル	○	○	○	○	○
ポップアップ				○	

※other(検証を行えない場合)

なりすましメール通知例

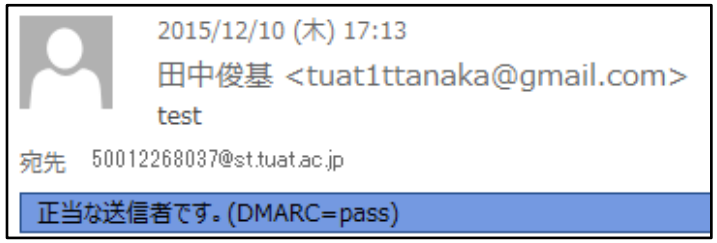
- 「citibank.com」を騙るメール
  - SPF認証：送信元IPアドレスは「citibank.com」のSPFレコードに含まれていない
  - DKIM検証：DKIM署名が付加されていないため検証不可
  - DMARC：DMARCレコードを公開しており，DMARCポリシを「reject」に設定

ラベルによる通知例

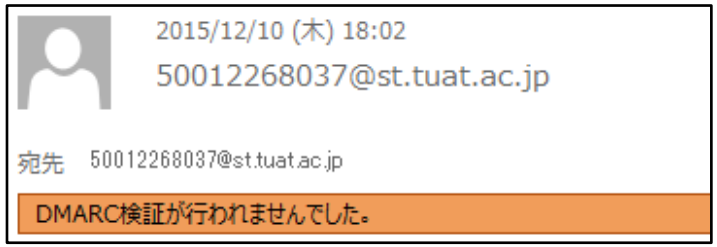


ポップアップによる警告例

検証結果の通知



検証にパス



検証不可
(ポリシの間違い，未公開)

ポリシ適用

ポリシ適用
(アラインメントに失敗)

DMARC検証プラグイン公開のお知らせ

- 一般社団法人インターネット協会（IA japan）公式ページにて，近日公開予定です.
- Outlook 2013/2016 に対応
- インストーラ完備で，簡単に導入できます！
- 多くのご利用と，ご意見・ご感想をお待ちしております.