Design and Implementation of a DMARC Verification Result Notification System

Naoya Kitagawa, Toshiki Tanaka,
Masami Fukuyama, Nariyoshi Yamai

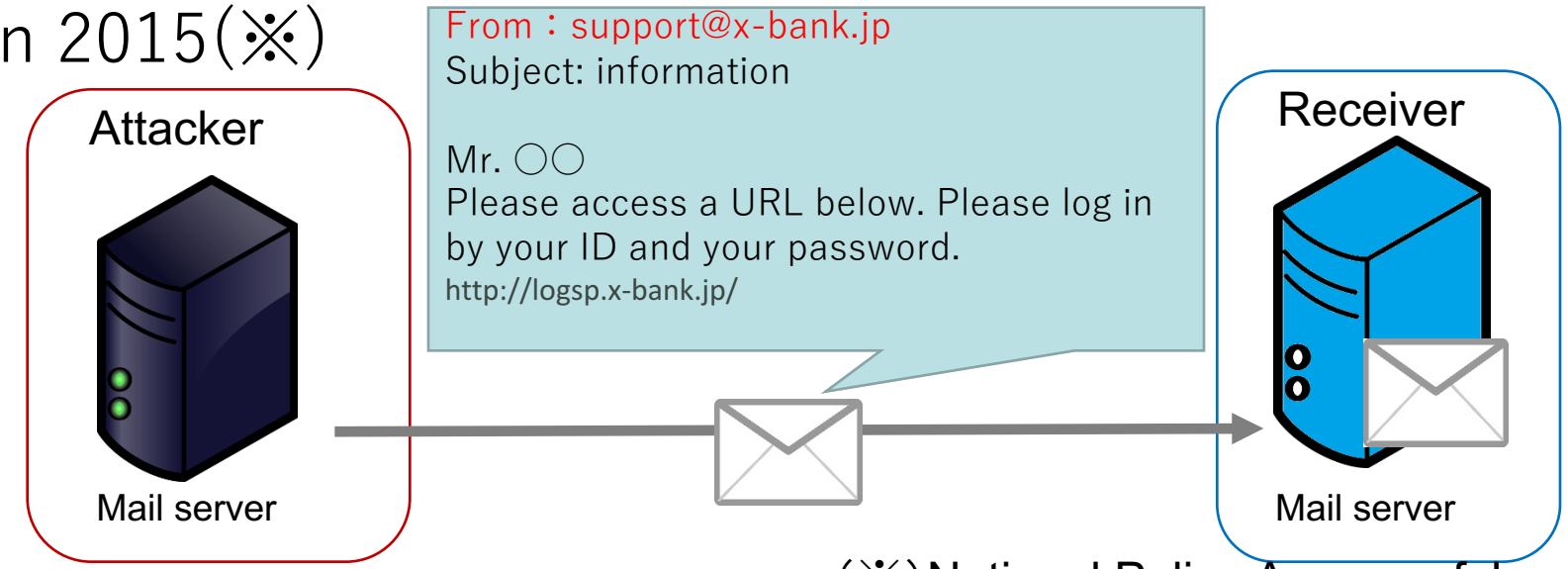
Tokyo University of Agriculture and Technology, Japan

APAN42@Hong Kong

Spoofed E-mails

- Aim to steal the receivers' personal information
  - Spammers pretend to be a bank or a public organization
- Number of damage in Japan

⇒ 1,495 cases, 3.1 billions yen (30 million USD) lost in 2015(※)

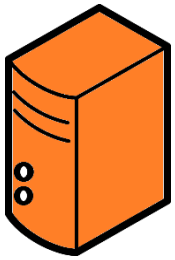


(※) National Police Agency of Japan(2015)

Countermeasures for Spoofed Mails

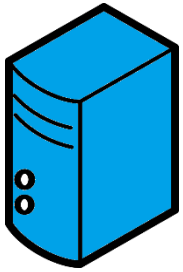
- Sender Domain Authentication
  - Detect sender's domain name spoofing
  - Typical methods
    - SPF (Sender Policy Framework)
    - DKIM (Domainkeys Identified Mail)

Sender



Publish the information for domain authentication at their own DNS server

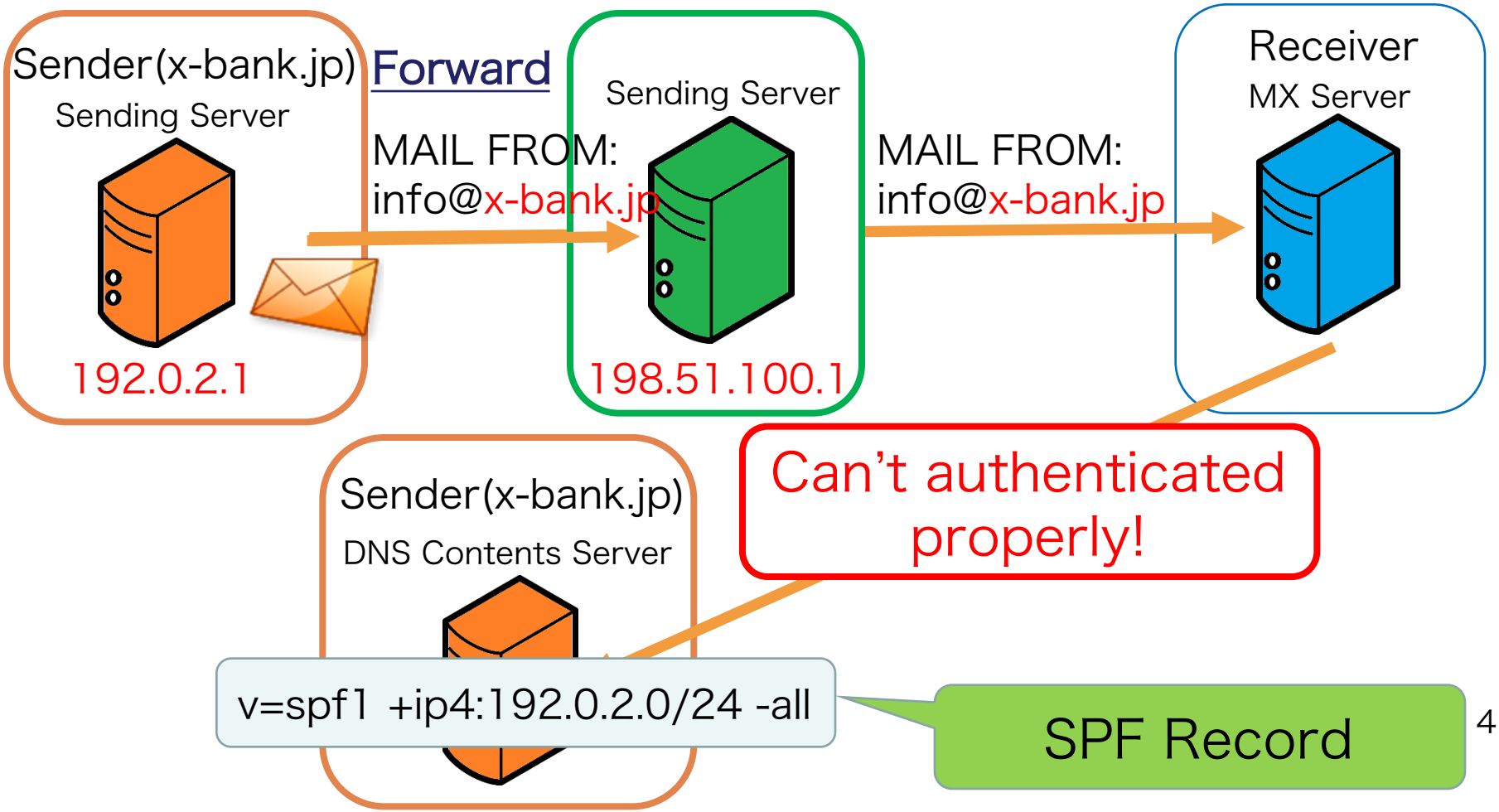
Receiver



Verify by using information that is published by the sender's domain

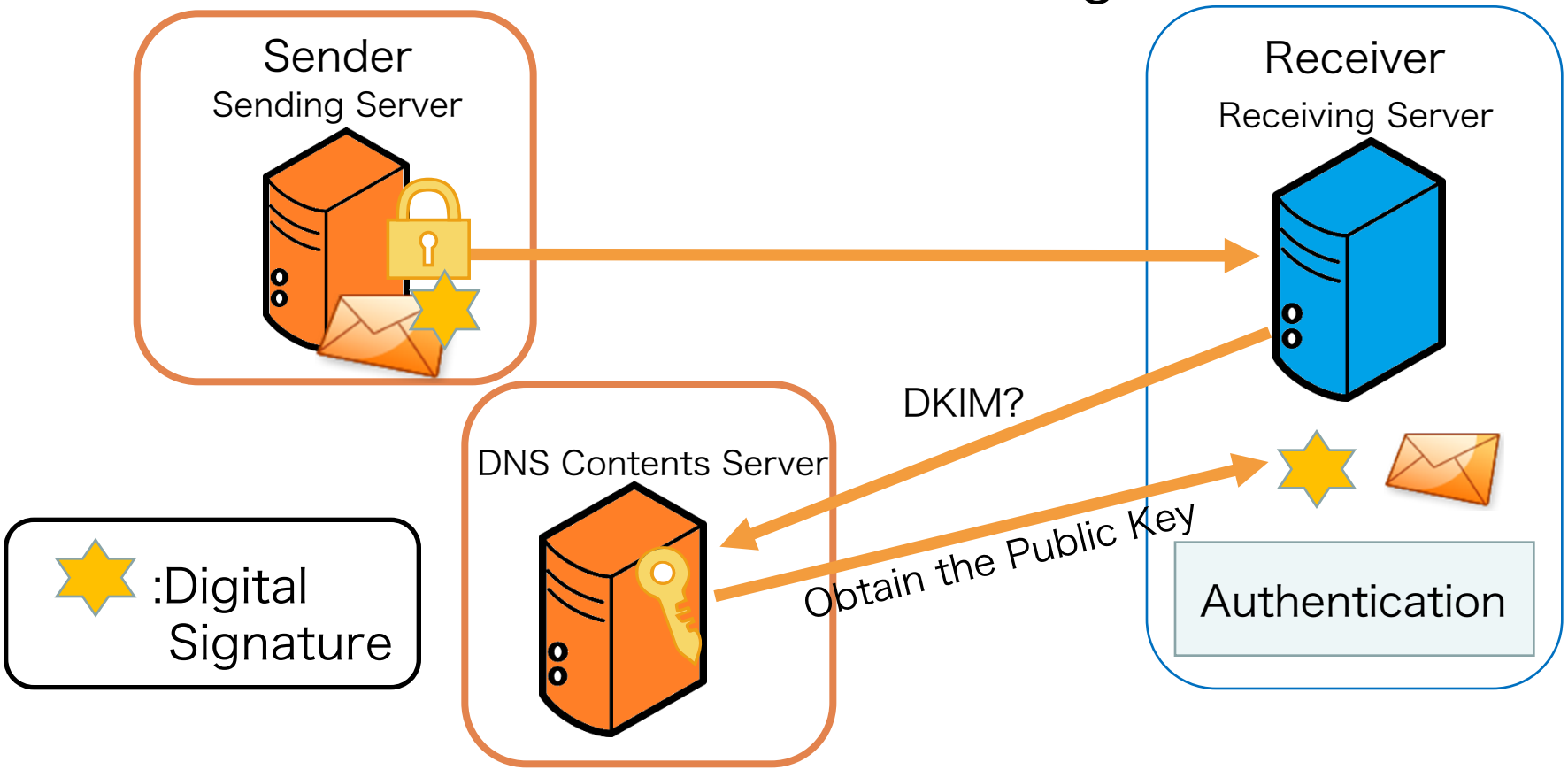
Sender Policy Framework (SPF)

- Verifying the validity of sending mail server



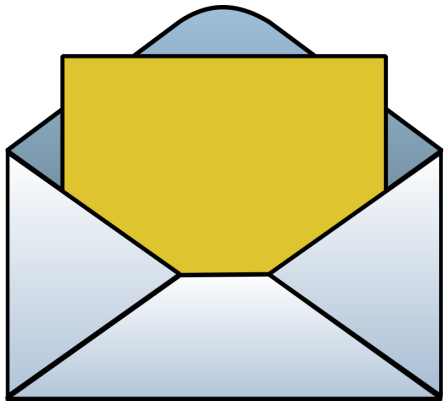
Domainkeys Identified Mail (DKIM)

- Verify the following:
  - Spoofing of the sending domain
  - Falsification of the mail message



Problems of DKIM (1)

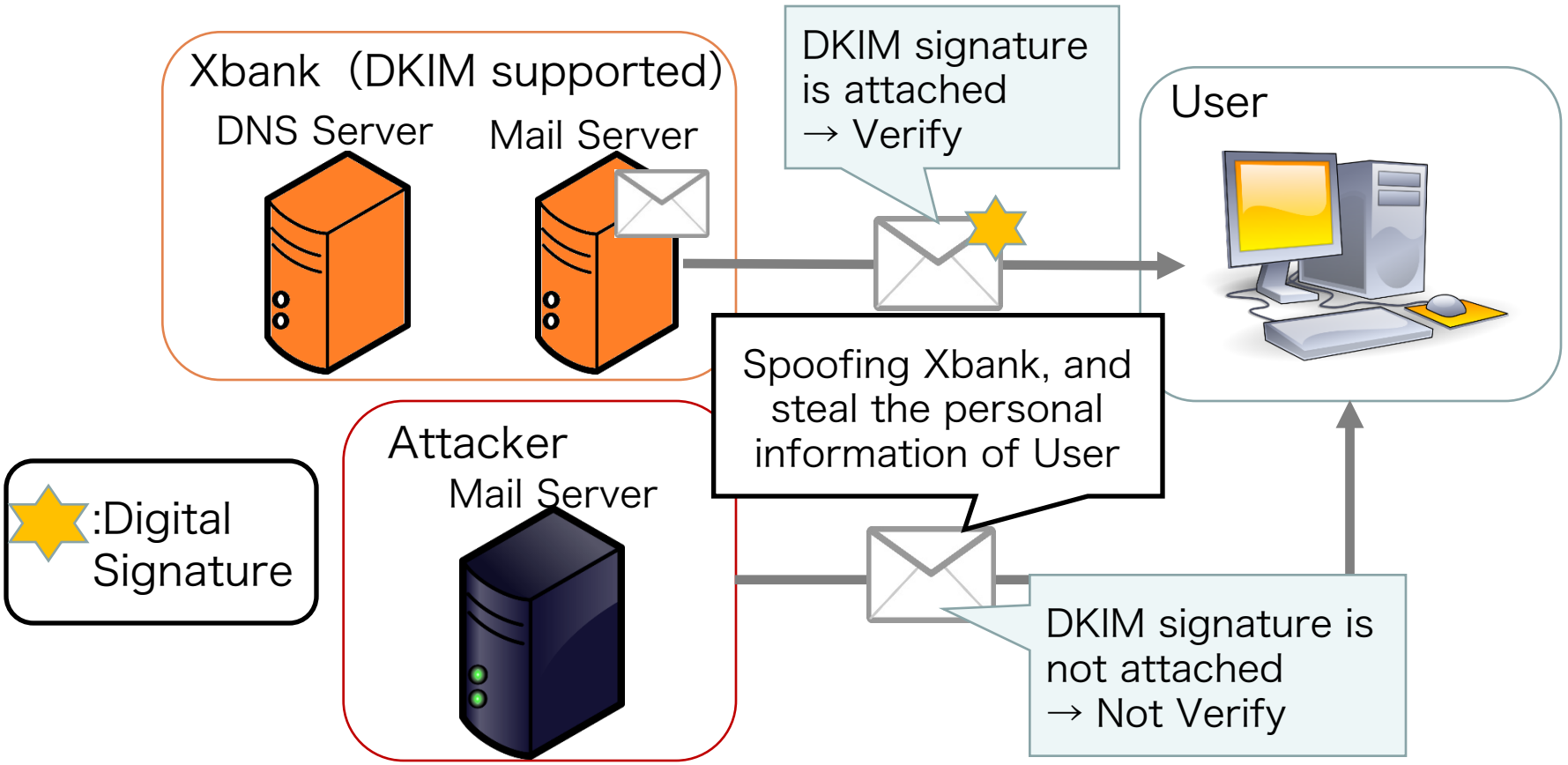
- Cannot verify the signature generated domain
  - DKIM Permits even a “d=” domain different from the Envelope-From domain



Mail Header
…
DKIM-Signature:v=1; a=rsa-sha256;
c=relaxed/relaxed;
d=spammer.com; s=20120113;
…
From: <info@x-bank.com>

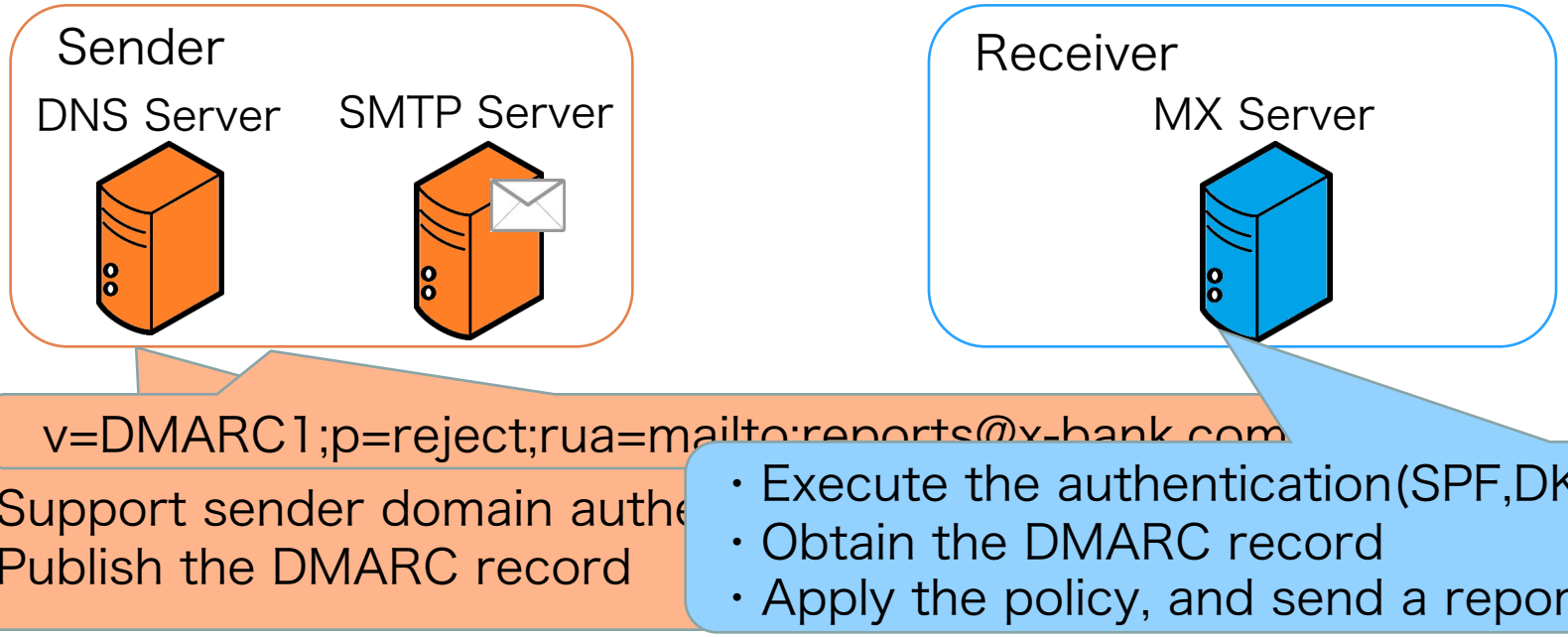
Problems of DKIM (2)

- Cannot verify the mails without DKIM signature

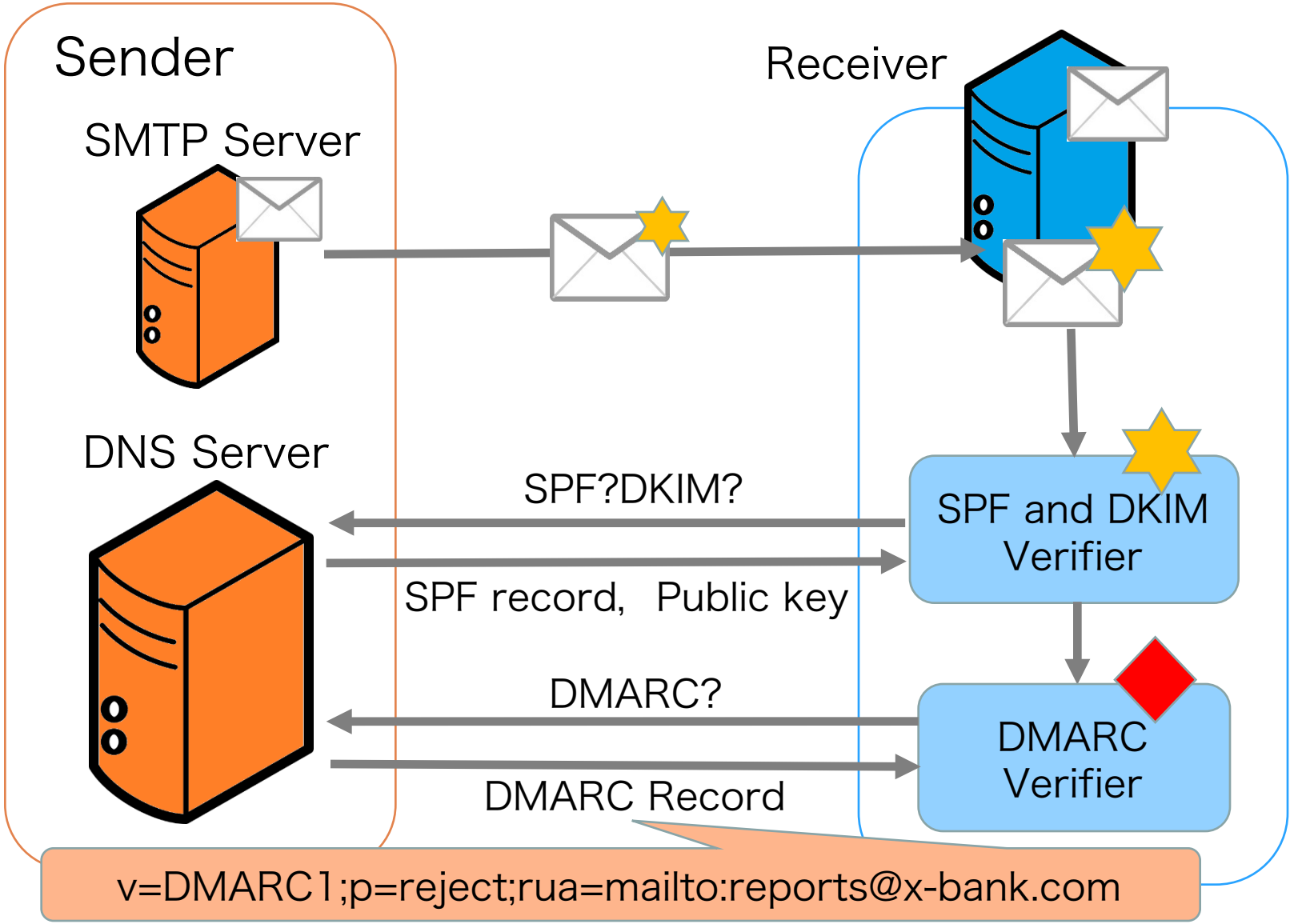


“DMARC” (Domain-based Message Authentication, Reporting, and Conformance)

- Sender can specify the emails handling in the case of sender domain authentication failure
  - Authenticate by SPF and/or DKIM
  - Sender specifies the handling policy in “p=” tag (none, quarantine, reject)
  - Reporting function (failure and aggregate report)



Flow of DMARC authentication



About DMARC

- Alignment
  - DMARC gets failed even if the domain for verification (SPF&DKIM) is different from Header-From domain
  - If cannot authenticate the legitimacy of domain, apply the DMARC policy
- Unfortunately, DMARC has a low deployment rate...
  - 38.6% in USA, 22.6% in Germany, 15.1% in Japan（※）

（※）https://eggert.org/meter/dmarc (accessed: 28th July 2016)

Statistics of DMARC policy

2016	February	March	April
p=none	1,473 (81.65%)	1,261 (82.31%)	1,821 (77.79%)
p=quarantine	123 (6.82%)	93 (6.07%)	209 (8.93%)
p=reject	192 (10.64%)	170 (11.10%)	305 (13.03%)
Error	16 (0.89%)	8 (0.52%)	6 (0.26%)
Total (domains)	1,804	1,532	2,341

About 80% of DMARC compliant domains publish “none” as the policy

Many DMARC compliant domains want to obtain aggregate reports?

An example of spoofed e-mail

- DKIM：Without DKIM Signature
- SPF：Sender's IP address [42.127.236.162], unmatched
  - citibank.com: DMARC supported

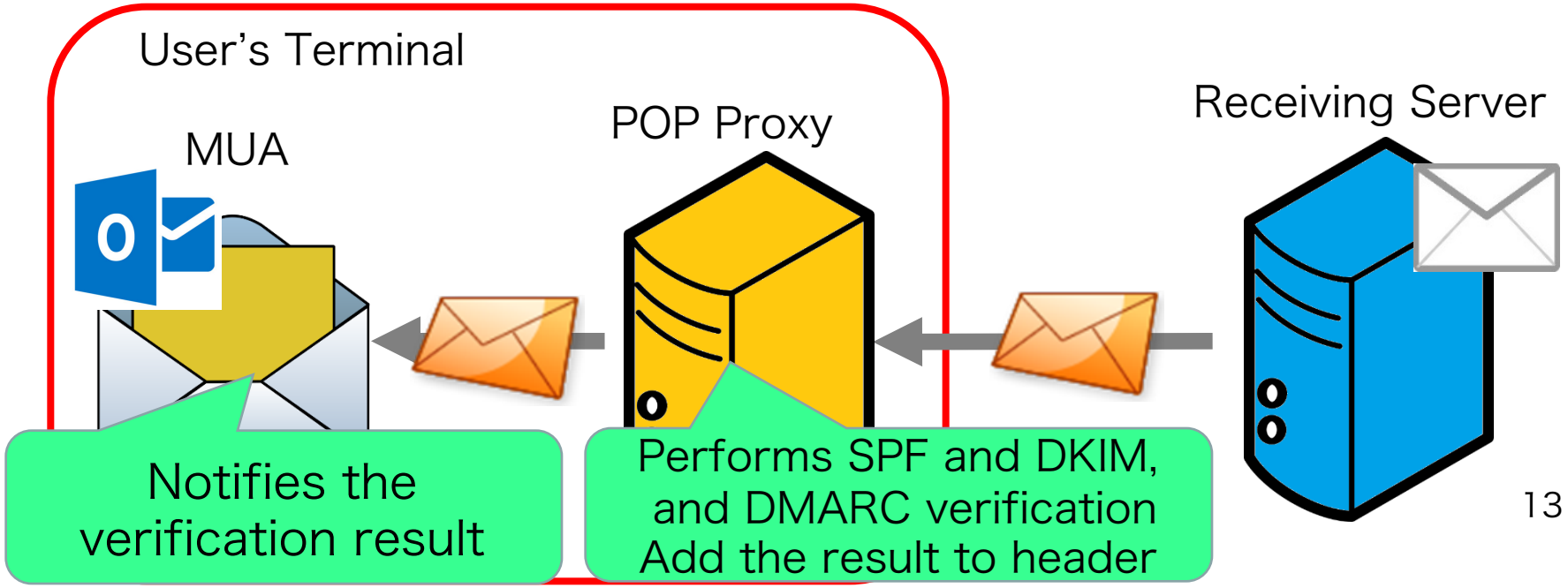
```
C:¥Users¥Tanaka>dig +short citibank.com txt
"google-site-verification=kZISuG305lKpwO_y-LOv8wR6wuDt8TVjeU8hzFVlI4s"
"v=spf1 a:mail.citigroup.com ip4:217.29.160.12 ip4:84.45.73.5 include:spf-00123c
01.pphosted.com ~all"

C:¥Users¥Tanaka>dig +short spf-00123c01.pphosted.com txt
"v=spf1 ip4:67.231.153.0/24 ip4:67.231.145.0/24 ip4:67.231.149.0/24 ip4:67.231.1
52.48"
```

```
C:¥Users¥Tanaka>dig +short _dmarc.citibank.com txt
"v=DMARC1; p=reject; rua=mailto:citi@rua.agari.com,mailto:dmarc.reports.rua@citi
.com"
```

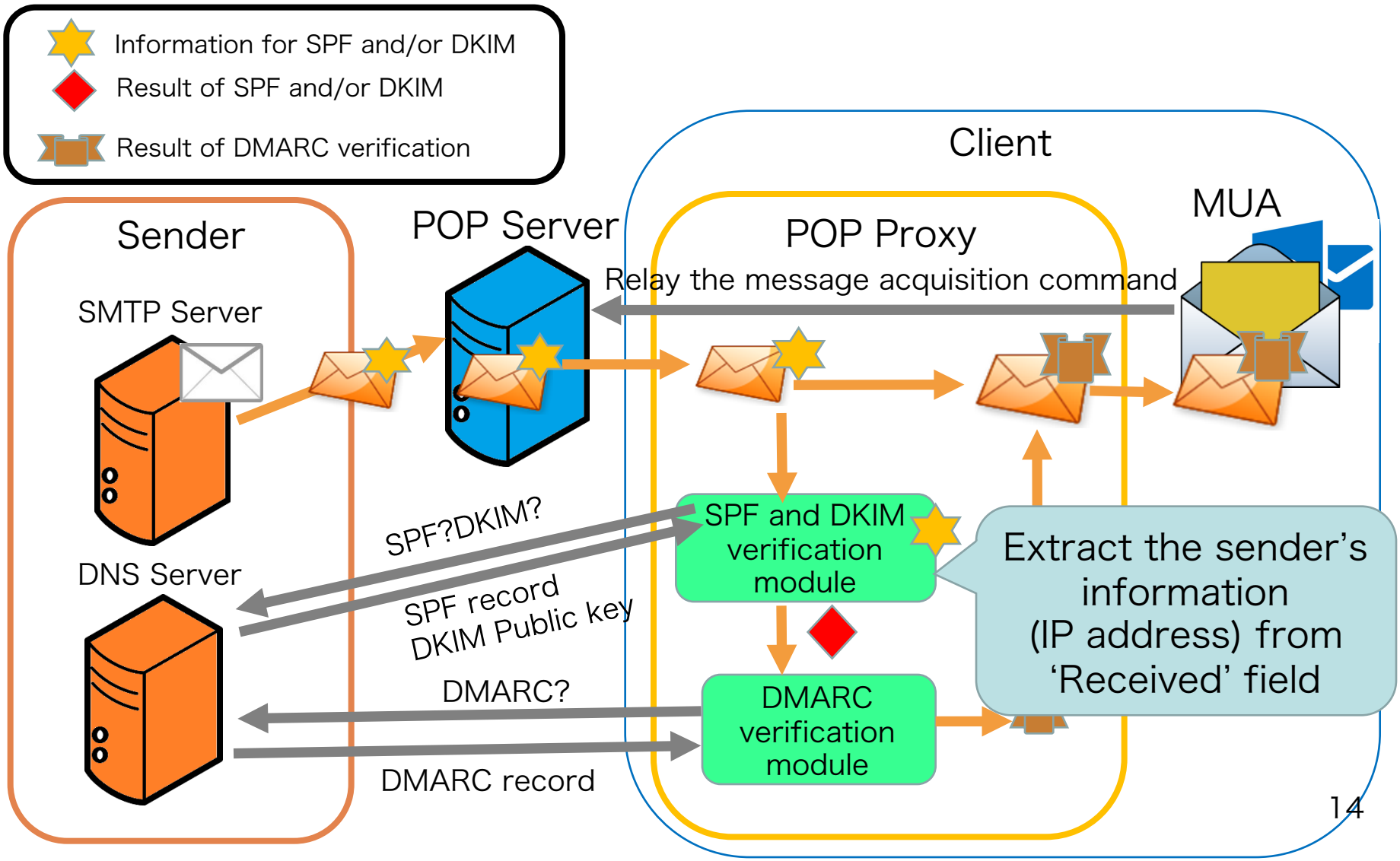
DMARC policy is applied to this mail

DMARC Verification result notification system

- Apply the DMARC policy to spoofed e-mails
- Execute in user's terminal for easy installation
- Notify the verification result to users, and alert if the e-mail is hazardous



DMARC verification result notification system



Implementation of our system

User's PC

POP Proxy(Cygwin)

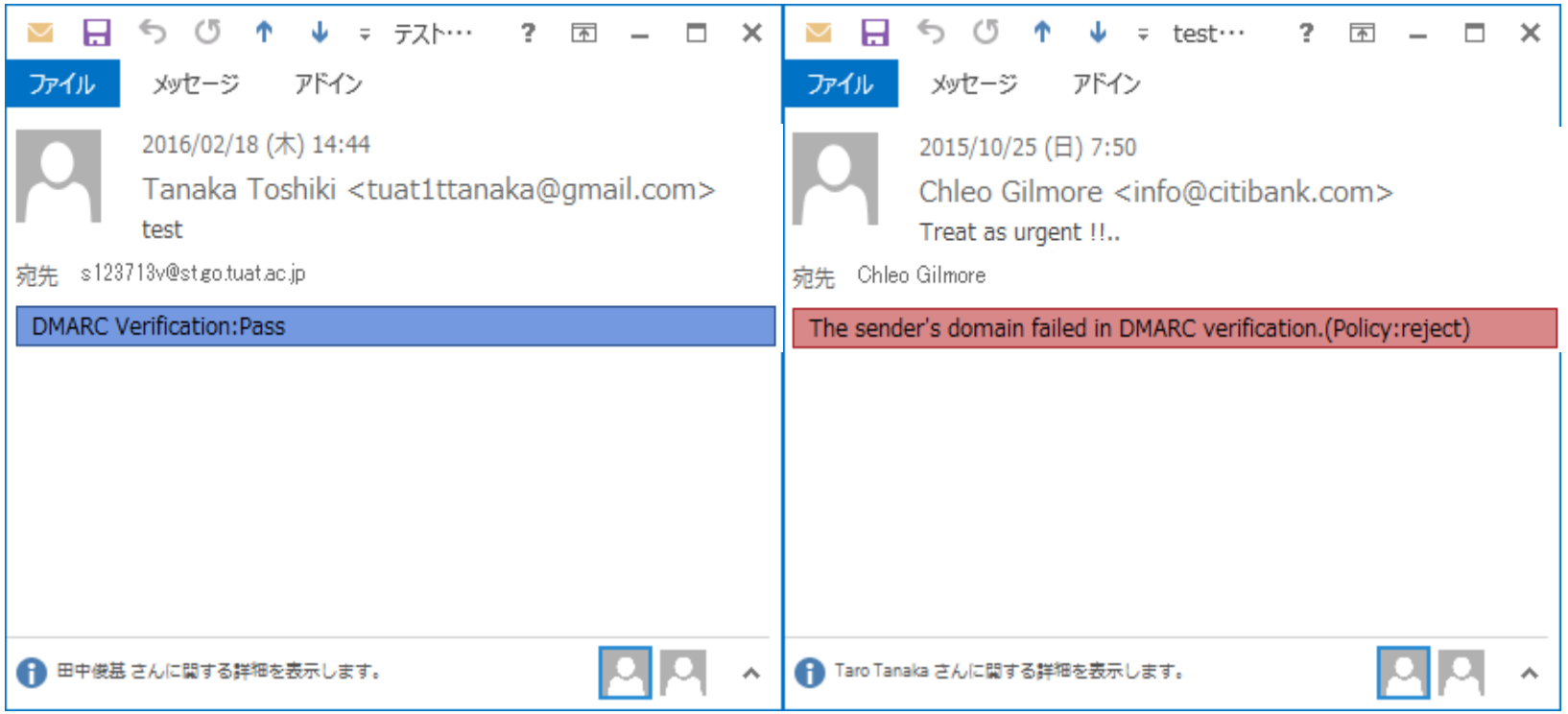
- Using and Modifying the following Perl modules
  - Modified Net::Server::POP3proxy (POP proxy)
  - Mail::DKIM::Verifier (DKIM verification)
  - Mail::SPF (SPF verification)
  - Mail::DMARC (DMARC verification)
- Addition of verification result to mail header

MUA(Outlook)

- Notify the verification result using MUA function and the extension function
- Using "Label" function of Outlook
- Pop-up alert by using add-on of Outlook Outlook

Notification of DMARC verification result

(1)Label addition example in Outlook2013

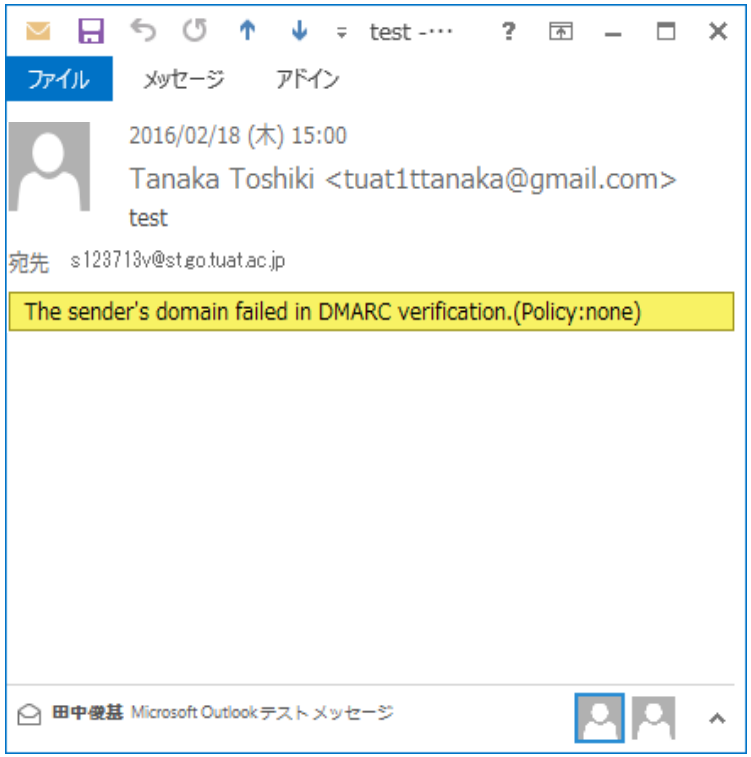


Pass for the verification

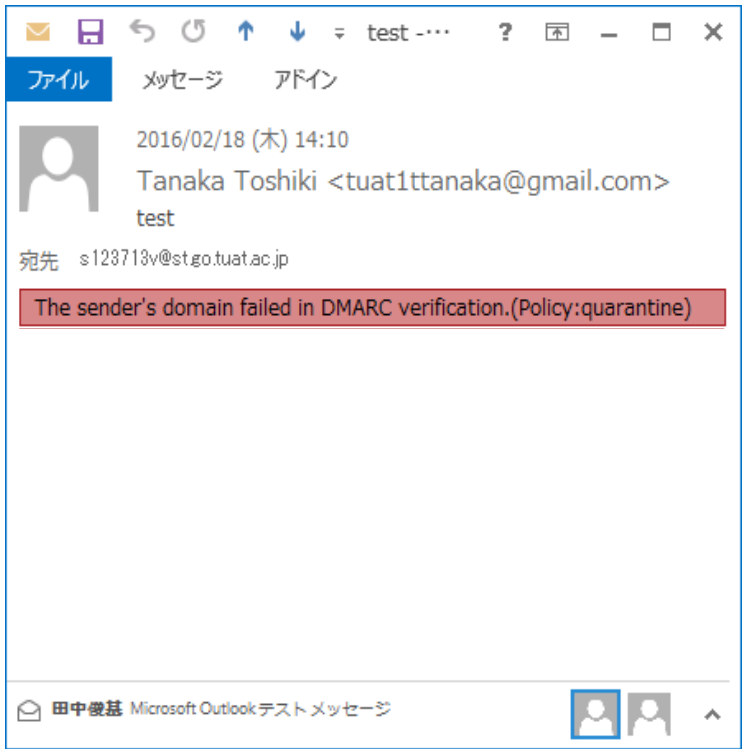
Apply the policy (reject)

Notification of DMARC verification result

(1) Label addition example in Outlook2013



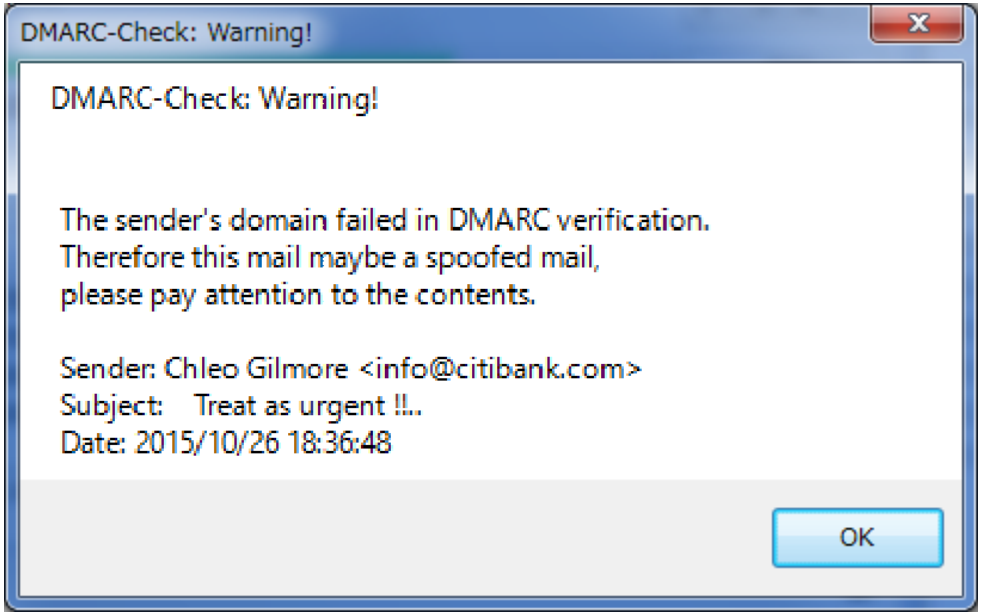
Apply the policy (none)



Apply the policy (quarantine)

Notification of DMARC verification result

(2) Pop-up alerting when the applied policy was “reject”



Notification patterns of verification results

Verification result	pass	none	quarantine	reject
Label	○	○	○	○
Popup				○

Statistics of DMARC policy

2016	February	March	April
p=none	1,473 (81.65%)	1,261 (82.31%)	1,821 (77.79%)
p=quarantine	123 (6.82%)	93 (6.07%)	209 (8.93%)
p=reject	192 (10.64%)	170 (11.10%)	305 (13.03%)
Error	16 (0.89%)	8 (0.52%)	6 (0.26%)
Total (domains)	1,804	1,532	2,341

Our system utilizes all policies

Conclusion

- Implementation a spoofed emails alerting system using DMARC verification
  - Notify spoofed emails more accurately based on the results of sender domain authentication
- Implement the verifications and the result notification module on a user's PC
  - Easy installation: Users can install the system even if the mail server does not support DMARC verification
  - Contribution to the spread of DMARC
- Future work
  - Support for IMAP proxy version