Effectiveness of Defensive Action and IIJ’s Approach to Sender Domain Authentication (ARC)

2.1 New Initiatives to Protect Our Customers: Effectiveness of Defensive Action

2.1.1 Building on the Previous Report

In our previous report, we discussed the issue of malicious actors hijacking email accounts and exploiting email services to send, for example, phishing emails.

When email services are misused by malicious actors, not only are phishing email recipients targeted by attacks but other customers also using the email service are impacted by reduced availability of service infrastructure, reduced deliverability to destination email services, and the like. This sort of unwelcome and fraudulent behavior on the Internet occurs not only on IIJ’s services but also on those of other ISPs and third parties on a daily basis. It is commonly referred to as abuse, and a challenge has been that only post-incident responses were possible.

As such, we launched a new initiative on May 1, 2024, under the IIJ Secure MX Service contract terms in an effort to maintain email service quality and protect our customers[*1]. This initiative involves detecting preparations for improper use and restricting communications to the extent necessary before phishing emails are actually sent out to prevent abuse from occurring in the first place.

2.1.2 Effectiveness of Defensive Action

While abuse responses involve taking action against abuse that has already occurred, we refer to this new initiative as defensive action because it protects customers by detecting preparations for abuse ahead of time.

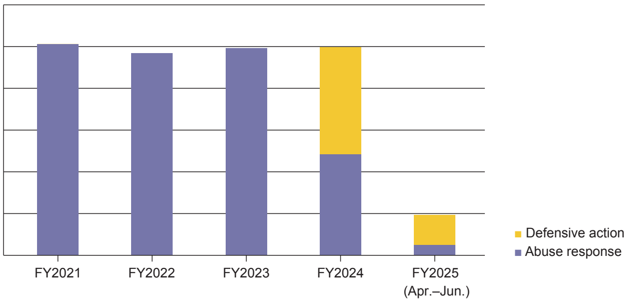

Figure 1: Comparison of abuse response and defensive action incident counts

Roughly a year has now passed since we initiated this defensive action program, and in this article, we report on the effects it has had.

Figure 1 is a stacked bar chart aggregating the number of abuse response and defensive action cases. The vertical axis represents the number of abuse or defensive incidents, while the horizontal axis represents fiscal years (April of one year to March of the following year). For reference, we also include data going back three years before (FY2021) we commenced defensive action.

As is evident from the graph, while the number of abuse response incidents was virtually constant over the previous three years, our defensive action starting in FY2024 has roughly halved the number of abuse response cases.

As explained at the beginning, when abuse responses occur, email service quality is compromised and engineers must undertake unplanned work. Through defensive action, we have been able to eliminate around 50% of these factors.

The fact that defensive action can restrict the transmission of emails in advance and thus prevent abuse means that we are suppressing the transmission of phishing emails and the like from IIJ’s network. With email, the sender and recipient perspectives are two sides of the same coin, so defensive action can be regarded as a technical initiative that supports the stable operation of Internet infrastructure and contributes to improved reliability, thus making it highly effective.

While the FY2025 data only go up to June due to publication timing, even more interesting findings have emerged. While we saw roughly equal proportions of abuse response and defensive action during FY2024, the three months of data for FY2025 indicate that the proportion of defensive action cases has increased relative to abuse response cases.

[*1] For a detailed background and information on this initiative, see IIR Vol.63 (https://www.iij.ad.jp/dev/report/iir/063/01.html).

Making IIJ's email service infrastructure difficult for malicious actors to exploit can be expected to gradually deter abuse. From a service product owner's perspective, as the number of abuse response cases decreases, engineer resources can be redirected toward other initiatives such as operational improvements, quality enhancements, and customer support.

At IIJ, we will continue working to protect our customers going forward.

2.2 IIJ's Approach to Sender Authentication (ARC)

2.2.1 Background and Overview of Our Approach

Following Google's and Yahoo's 2023 announcements that they would be requiring sender authentication (SPF, DKIM, DMARC), IIJ took steps to ensure its internal systems were compliant.

As part of this process, we discovered that ARC (Authenticated Received Chain) authentication was failing when forwarding to Microsoft 365 (M365). ARC plays a role in preventing false positives under DMARC policies by reevaluating SPF and DKIM authentication results during email forwarding and adding those results and signature information to the headers. The email headers at time of verification contained the string arc=fail (47), as shown below, indicating an authentication failure.

```
ARC-Authentication-Results: i=2; mx.microsoft.com 1; spf=fail (sender ip is
...) smtp.rcpttodomain=iijsmxstg.onmicrosoft.com
smtp.mailfrom=iij.ad.jp; dmarc=pass (p=reject sp=reject pct=100) action=none
header.from=iij.ad.jp; dkim=pass (signature was verified) header.d=iij.ad.jp;
arc=fail (47)
```

To determine whether this issue originated from IIJ's systems or from processing performed on other email systems, we conducted ARC verification tests with multiple providers.

Table 1 summarizes the forwarding test results for the providers involved. IIJ-office is the email system used internally at IIJ for business operations, while SMX is the IIJ Secure MX Service, a different email system.

2.2.2 Inquiring About the Issue

To identify the cause of the ARC authentication failures, we performed signature verification using dkimpy, a Python library that complies with RFC 6376 and RFC 8617. This confirmed that ARC-Message-Signature (AMS) verification was succeeding for emails from IIJ to M365.

```
>>> import dkim
>>> dkim.ARC(open("iijsmx-forward-365-arc-fail-20231127.eml","br").read()).verify()
```

```
(b'fail', [{'instance': ..., ...; spf=... smtp.rcpttodomain=... smtp.mailfrom=...;
dmarc=... action=... header.from=...; dkim=... header.d=...; arc=fail (47)\r\n',
'ams-domain': ..., 'ams-selector': ..., 'ams-valid': True, 'as-domain': ...,
'as-selector': ..., 'cv': ..., 'as-valid': ...}], "x= ...")
```

Given these results and our growing suspicions, we contacted Microsoft. The response was that arc=fail was occurring because hash values did not match during ARC signature verification, suggesting the possibility that the message had been modified after signing.

Before the hash value is calculated, the email content is normalized. Our investigation revealed that while IIJ was using the simple algorithm, M365 was using the relaxed algorithm.

Normalization is the process of converting email content into a standardized format, in compliance with RFC 6376, the DKIM standard. RFC 6376 defines two normalization algorithms for headers and body content: the "simple" and the "relaxed" algorithm. The simple algorithm keeps line breaks and other whitespace as is, faithfully preserving the content as sent. In contrast, the relaxed algorithm ignores line breaks and other whitespace and consolidates all whitespace sequences into a single space character.

RFC 8617, the ARC standard, explicitly states that ARC follows DKIM syntax and processing. For the bh (body hash) tag, in particular, it requires hash values to be calculated on the normalized body content, just as with DKIM.

Forwarding path	i=1	i=2	i=3	ARC result
IIJ-office → SMX → Google → FastMail	IIJ-office	SMX	Google	fail
IIJ-office → SMX → Google → Microsoft	IIJ-office	SMX	Google	fail
IIJ-office → SMX → FastMail	IIJ-office	SMX	-	pass
IIJ-office → SMX → Microsoft	IIJ-office	SMX	-	fail

Table 1: Forwarding Test Results for Each Provider

We also informed Microsoft that the hash values generated by IIJ services matched those from Gmail and OSS implementations, and that M365's normalization algorithm might differ from what other services and OSS use. But because we could not completely rule out the possibility that IIJ's email systems were the cause of the arc=fail, Microsoft said that investigating the issue would be difficult and thus closed the inquiry.

2.2.3 Reinvestigating and Identifying the Issue

Subsequently, in response to arc=fail incidents identified in other cases, we corrected issues on the IIJ side and, as a temporary measure, switched from simple to relaxed for the body normalization algorithm. We had expected this change to resolve the ARC authentication failure issue, but we continued to observe incidences of arc=fail, prompting another detailed investigation.

As with our first inquiry, we conducted tests of forwarding to other providers while examining the values in the email headers more closely. When we tested both empty-body emails and emails containing text as specimens, we found that for empty-body emails, the bh tag hash values differed between IIJ and M365. IIJ requested that Microsoft correct this issue.

```
ARC-Message-Signature: i=3; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-
AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-
Exchange-AntiSpam-MessageData-1;
 bh=47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=;

b=P0BjQ+kWDc+ghsJ3atV7ElnsRM8v6qSXVbWk+sT59USGlCYId0vvOL5H0s5sfLj58Ow4HnWmYG9RN8As9
rDEBb3IlWihg13+kPDEM8/S3HydFI58bT3KjHuWzM5UGH3MBv+lriGKciDpbDRhnlaz2mvZNnBMuBqCD0eD
8NAa3soY6oP8/jh6t692dWiDRD9pI+D8ho9VhpRZw1SFQ7UIJAtWMLNuY6YG9WlGXmdSi9nCALdhBzwGjod
1Xx0/+RnxLZQAg56eSYYAqCTC5At/YbCjK8b6Yk7+MLcuJBAL/JYAy69uJiBcNo3sroAbnjp7zhgi4FvILn
oM3pMvzFidnA==

ARC-Message-Signature: i=2;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713333099;x=1713937899;bh=frcCV1k9oG9oKj3dpUqdJg1PxRT2RSN/XK
      dLCPjaYaY=;b=XT741y7ourI4cRnEqfSt2iNOXIsKAbHFNGzRrMz0R/Rfnm/UuewENteicKQbQZ
      A5E6dfKj1osLQvWGSIwUDQjb405Y0yt3PS/rrV4Eb+LmfvXLGdbVCUT7Q8HPchkyIXgy6D2LEB3
      eF69Br0MF97GW2jz5YF9Dj51I6VuytabrDa31B1w62ENmz7N/gTT62aAPYLUBuHL9DhuJi1d9lm
      +uZLh3ia8iswz8FxZDkuRbrBWQu8eyzinlPyqAfUdPcTbERf+GuGDOfkFyL2NHUg4HUHGaaoqQI
      yt3Vuqt31eM/Uz75LGcPITpRWPGUxZviMLTMiV/Jeoxd4CA2+wbEcOg==

ARC-Message-Signature: i=1;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713333098;x=1713937898;bh=frcCV1k9oG9oKj3dpUqdJg1PxRT2RSN/XK
      dLCPjaYaY=;b=T0diE3VZQzYgPWNPb3mPL/hc9Bsw/xc2LOvdgzq5D/P19MlMswEm7oO7a1pKgr
      EvtHRelRPQFCPFP4p5Fc6/CFITiMjRBBDLaqBguN3VsbjwyRbp1BSTzFzEm8+/2hI6hFri6XwfY
      TmfiE799hedDK5XoFCjURuT/gv4MSFjdTzLkdZY2M4CY00fHPiM9g7av9aJU3OYfku8DUrFev4t
      dIWI/7jT6tRpsN/roh3WEb1j3ll9YUqTMMOhN4fzO2Teo+4BCLxjGVZLL60iglOA8tkO899QtCo
      aDJqM8BeSWFc0m8WO1CYTg92HukBJQphxb3g8XMayEB0n6B3sQ20E0A==
```

When text was present, the bh tag hash values appeared to be the same.

```
ARC-Message-Signature: i=3; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-
AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-
Exchange-AntiSpam-MessageData-1;
 bh=KXMY6AzIdALlOzgkBat5CPcMk0Vqq3IozVvMgC0v4D0=;

b=hoDE5ZJ2ZnJuUTrPAsRdaZjjfsIHGRAH16O7Syq0uNPc7MPkKWyCUaRhU5JR14hg+TIClmfdauNL9nLN6
MDPrdAWBGwQr00h8fQrcy4AHrK206Cex9YV07/AjBu7eO09ld7wTWr3IwJc8wzQ83CYXQ4AIoXqK+mzsXo8
rQDOaPOxgTmNwvfGm+Q0Q5AdNzoesniZdAfmC1ZjKw774bezqKlTEY9P9ylwQPyQ830nHpbToug4PlQN5la
QReb2wxFVQUzfY8Wser0l/31hzuM1kB1Regz9o9+gRBJiMs3YBP4ENLUOqp0Oq7dUhIDhZ9T++hGHvNZtZN
Ckheo4HIClOw==

ARC-Message-Signature: i=2;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713333207;x=1713938007;bh=KXMY6AzIdALlOzgkBat5CPcMk0Vqq3IozV
      vMgC0v4D0=;b=zLi0vrLrkhYhpkGqnKJ2IyYywsXPSc3vGsVUjV5UOzuX+Pg3VdgwdXgXDbANw9
      PdpDJ/uBklbyU0v52Vw7Sa8RPiB3QdaZOfLoIyEa3uDAGqy7cKd+yAXfnkBGQoZhP8ddkT8yQZz
      uK9/Vz0F5tQb+RTzkjjugHuavng6OKA1YTCIYPB654uqicxyx+L6TwLzajKv20TKZIDYq6fpQFO
      4vW0bclHa4hKk91lkI7yAPZ6WpuhZv6S9ySnIs6PujDSXYV2GEMcu8aTa4VHAXNGLu3zqtS2Btx
      cW6EGC3/xGDxI0BaU9Itr/73vwH3ZNilw2uE0xbhxkehShmL1hZns2A==

ARC-Message-Signature: i=1;a=rsa-sha256;c=relaxed/relaxed;d=securemx.jp;h=
      Content-Type:MIME-Version:Subject:Message-Id:To:From:Date:DKIM-Signature;s=
      arc20190303;t=1713333205;x=1713938005;bh=KXMY6AzIdALlOzgkBat5CPcMk0Vqq3IozV
      vMgC0v4D0=;b=heR13lSXC71wKTNdzf9UmnChz5/bqf5L2qZ5X7i8xTsk2x2o42rqKN9Fzpweeb
      Lplf9Msm09ki7XWRJMQci3oi+Ut5Z7Hmjo3UdTrbMjaT621GPKID+gVbDpKxCDlWiCzc5ox3wrw
      MYDoM6A/2rQwjXsgTMoWovEmxyB795Db1y+J5dyCzkpWcJ/2JEXBU0PbQ4Qr1Ofkzq7Rsum5Cyi
      lHeXJw64GDbbh6uY5j1HM92CtGo9Ejw+r6c63snjJURvfrjCcB11hgrx84CclJw9klt9PtUct7P
      +l90RENzLmpelNYa0w9Y2LAGjRztzayIunJnvw0WJ1uniz6iuufwJkA==
```

Section 3.4.4 of RFC 6376, which ARC follows, states that trailing line breaks must not be removed even in relaxed mode.

M365, however, was calculating hash values with such trailing line breaks removed, which is why the bh tag values did not match.

When we contacted Microsoft citing this RFC specification, the company acknowledged that the issue was on the M365 side.

2.2.4 Conclusion

ARC adoption rates remain low compared with other sender authentication methods such as SPF, DKIM, and DMARC, with many email systems yet to implement ARC authentication. Possible reasons for this are that not setting up ARC authentication does not currently cause major problems, and that RFC 8617, the ARC RFC, is still designated as Experimental.

Google's sender guidelines also recommend using ARC authentication if regularly forwarding email. Additionally, if ARC is not implemented properly, this can prevent SPF and

DKIM verification from being performed correctly during the forwarding process, and depending on DMARC policies, emails may be rejected, potentially affecting email deliverability.

The cooperation of intermediary systems that forward email is crucial for ARC. IIJ will continue supporting sender authentication technologies, including ARC, and strive to improve email reliability and deliverability.

2.3 Sharp Surge in Phishing Emails Targeting Japan

At the end of 2024, we observed one of the largest volumes of phishing emails on record on IIJ's email services. Figure 2 plots the number of emails received by IIJ-operated honeypots that were classified as spam.

From around the end of November, the total volume of phishing emails increased sharply, peaking around year-end. The phishing emails during this period spoofed entities such as Amazon, Sagawa Express, tax offices (e-Tax), and the ETC usage inquiry service, with the content of all messages being fake replicas of legitimate emails. The tax office phishing emails, in particular, coincided with the tax filing season, presumably in a bid to increase attack success rates.

According to the Council of Anti-Phishing Japan's monthly report on phishing[*2], December 2024 saw the highest number of phishing reports on record, mirroring the trend IIJ had observed. These findings indicated that not only IIJ but other ISPs also were observing a similar trend, and that many phishing emails targeting Japan were being sent out. The report's summary notes that Japanese organizations are lagging behind when it comes to security measures such as sender authentication, making it easier for phishing emails to reach users than in other countries.

We continue to observe high levels of phishing emails in 2025, and continued vigilance is crucial.

Incidentally, we also reported on such a surge in phishing emails in IIR Vol. 51[*3], published in June 2021. That was back during the rapid rise in remote work amid the COVID-19 pandemic, and we also observed phishing emails exploiting that situation. And in 2019, Emotet, which spread via password-protected ZIP file attachments, wreaked havoc in Japan, with widespread impacts being confirmed.

Hence, phishing emails and viruses repeatedly cycle through periods of dormancy and resurgence, constantly changing tactics and adapting to the times.

Security measures are therefore not a set-and-forget affair; they must be continuously reviewed and strengthened in response to evolving threats. This is an endless battle and an ongoing investment, and it requires organization-wide effort. IIJ will continue its unwavering efforts to maintain a safe and secure environment.

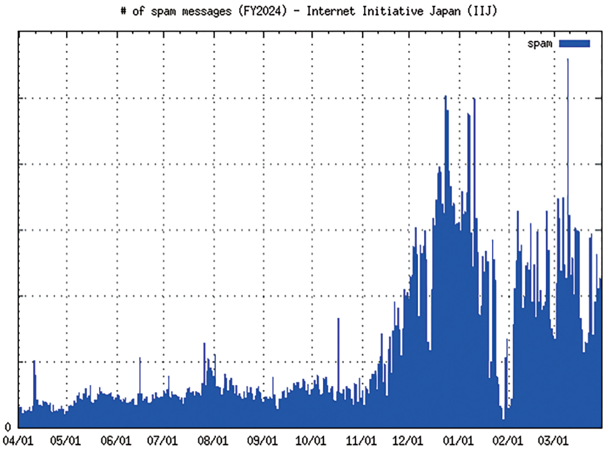

Figure 2: Spam Emails Arriving at IIJ Honeypots

[*2] Council of Anti-Phishing Japan, Monthly Report: December 2024 Phishing Report Status (https://www.antiphishing.jp/report/monthly/202412.html, in Japanese).

[*3] Internet Infrastructure Review (IIR) Vol.51 (https://www.iij.ad.jp/en/dev/iir/051.html).

2.4 Sender Authentication and Transport Encryption Statistics

Figures 3–6 show a percentage breakdown of sender authentication results aggregated from IIJ's email services as part of ongoing monitoring. The observations cover the month of March 2025.

Since our previous report, the percentage of successful sender authentications (pass) has decreased across all metrics. We know that sender authentication adoption in Japan, particularly DMARC, has increased significantly following the release of Google's sender guidelines[*4][*5].

Thus, when this is considered alongside the data in Figure 2, the natural interpretation is that phishing emails that do not support sender authentication or that fail authentication checks have become dominant in the data relative to normal email, causing the overall pass rate to decline

Starting with this report, we have added aggregate results for ARC. Not all organizations are necessarily required to support ARC, but the IIJ Secure MX Service for enterprise email security added support for ARC signatures for received emails from 2019.

Next, we look at transport encryption (STARTTLS) data from the IIJ Secure MX Service. Figure 7 shows the types and percentages of transport encryption for received emails. PLAIN indicates no transport encryption.

Nearly 70% of received email communications used transport encryption, and TLSv1.3 accounted for close to half. As reported in Section 2.3, we saw a surge in phishing emails in December, and the graph here shows an increase in the proportion of TLSv1.2 around December. These results indicate that TLS-encrypted communications were also being used to send phishing emails at that time.

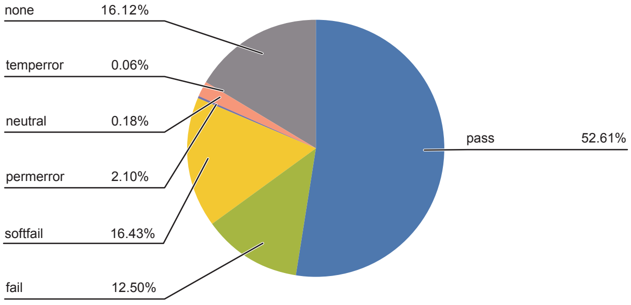

Figure 3: Breakdown of SPF Authentication Results

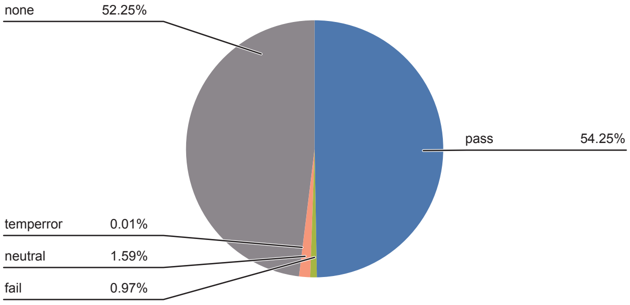

Figure 4: Breakdown of DKIM Authentication Results

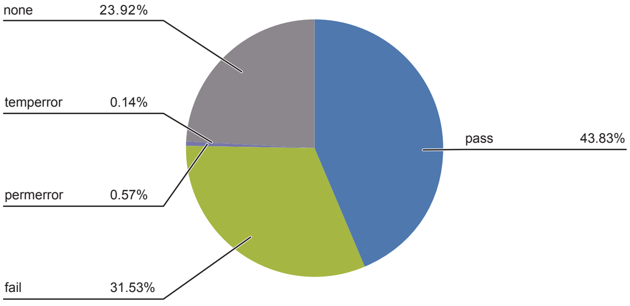

Figure 5: Breakdown of DMARC Authentication Results

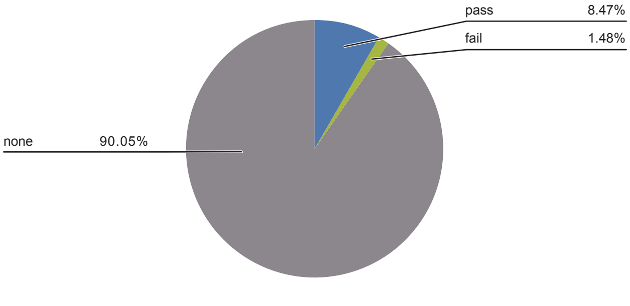

Figure 6: Breakdown of ARC Authentication Results

[*4] Email sender guidelines, Google (https://support.google.com/a/answer/81126).

[*5] DNSOPS.JP Statistics, Domain status of Japanese organizations – DNSSEC/SPF/DMARC (https://stats.dnsops.jp/chart/all/dmarc).

Figure 8 plots the proportion of emails sent from the IIJ Secure MX Service that used transport encryption. Due to equipment limitations, we can only show the aggregate proportion here, but it is evident that close to 100% of communications are encrypted.

When we last reported on this in IIR Vol. 59[*6], the proportion was fluctuating around 80–90%, so about two years on, it seems safe to say that email, like the Web, has entered the era of always-on TLS.

The Google Transparency Report[*7] also provides percentage data for email transport encryption, which indicate a largely identical trend. The inclusion of STARTTLS as a requirement in Google's sender guidelines released in 2023 likely had a substantial impact here.

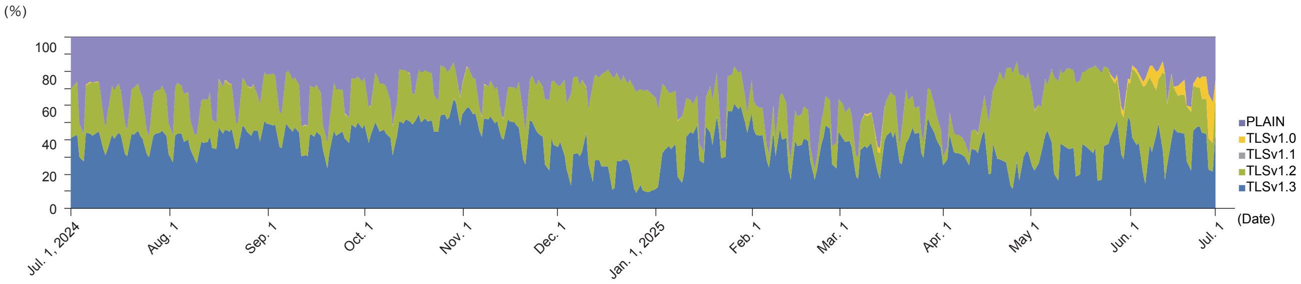

Figure 7: Proportion of Received Emails Using Transport Encryption

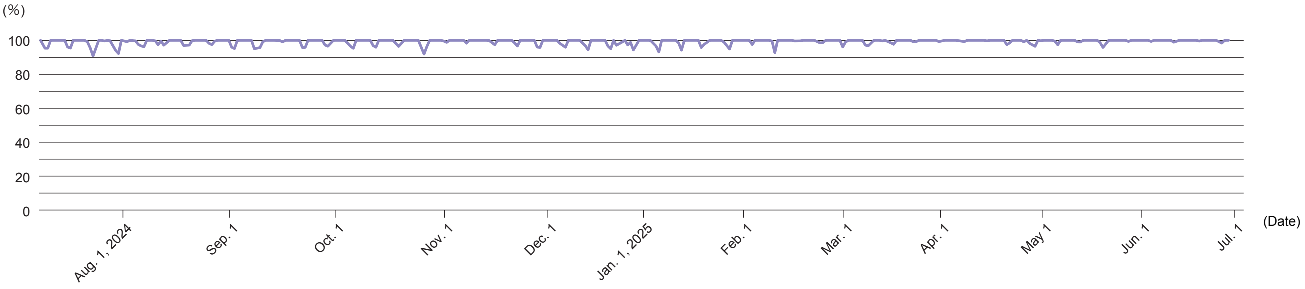

Figure 8: Proportion of Sent Emails Using Transport Encryption

2.1 New Initiatives to Protect Our Customers: Effectiveness of Defensive Action, 2.3 Sharp Surge in Phishing Emails Targeting Japan, 2.4 Sender Authentication and Transport Encryption Statistics

samu Koga

Manager, Application Service Management Section, Application Service Department 2, Network Division, IIJ
Mr. Koga joined IIJ in 2007. He is engaged in the operation of email services and ID governance management services. To keep customers' email boxes safe, he serves as a communicator and public speaker on the latest attack methods, trends in spam, and countermeasures. He is also involved in a wide range of community activities, including M3AAWG, WIDE Project, and openSUSE.

2.2 IIJ's Approach to Sender Authentication (ARC)

Shunpei Yamashita

Mail Service Development Section, Application Service Department 2, Network Division, IIJ
Mr. Yamashita joined IIJ in 2021. He is engaged in the development of email services.

[*6] Internet Infrastructure Review (IIR) Vol.59 (https://www.iij.ad.jp/en/dev/iir/059.html).

[*7] Transparency Report, Google (https://transparencyreport.google.com/safer-email/overview).