Messaging

1.1 30 Years with Email

IIJ celebrated its 30th anniversary last year, and over those years we have created and released many services. Among Internet infrastructure services, email in particular has one of the longest histories. Many new services continue to come to life, but where there is a beginning, there is also eventually an end. Safely bringing live services to a close with minimal impact on customers can be far more difficult than creating new services, a fact that is often underappreciated.

In the first half of this chapter, we reflect on the IIJ Post Office Service, which IIJ retired last year after 24 years in operation. In the second half, we report on recent debate around sender authentication technology DMARC and on email route encryption observed on IIJ's email services.

1.2 IIJ Post Office Service

The IIJ Post Office Service is an email hosting service for business customers that allows you to send and receive emails via your own domain name.

To start using the service, all a customer does is point the MX record(s) on their DNS server to IIJ. This sort of functionality is something that all hosting providers offer these days, but according to our records, we launched the service in July 1998[*1][*2]. The service provided unlimited mail storage capacity, with the ability to save received email for 14 days.

Date	Press release
July 2001	Virus protection (antivirus) functionality added[*3]
December 2002	IIJ Mail Gateway Service started. Email audit option added[*4]
March 2003	MailViewer (webmail feature) offered as standard[*5][*6]
October 2004	Spam filter option added[*7]
October 2006	IIJ Secure MX Service started[*8]
January 2010	Support for sender authentication technology DKIM[*9]
June 2010	Support for IPv6 as standard

Table 1: History of the IIJ Post Office Service

Being directly connected to IIJ's high-quality backbone, the service offered stability. It was naturally well received by customers, and with email becoming an essential tool for businesses, the service also became well known within IIJ as one that sales reps had no trouble marketing.

In the years following its launch, we continued to add functionality and related services (Table 1).

1.2.1 Challenges of a Long-running Service

All companies naturally want to build and develop their services in such a way as to generate as much revenue and profit as possible, and to continue providing those services for a long time. This is precisely how the IIJ Post Office Service has evolved, making it one of the services that have contributed greatly to IIJ's growth.

Yet with long-running services like this, the following three challenges sooner or later present themselves.

■ (1) The software cannot support the latest technology

Software innovation is constantly evolving. This will no doubt be all too familiar to you if you're a software engineer. While something may have represented the latest technology when first developed, jump forward just a few years and you'll find newer technologies and better frameworks being developed.

Adding revisions to old code and playing catch up with the latest trends is quite a challenging task under such circumstances, and it requires a high level of motivation, not to mention skill.

[*1] IIJ, "Launch of the IIJ Post Office Service" (https://www.iij.ad.jp/news/pressrelease/1998/pdf/postoffice.pdf, in Japanese).

[*2] Microsoft released Windows 98 the same month, July 1998.

[*3] IIJ, "IIJ to launch antivirus service on July 1" (https://www.iij.ad.jp/news/pressrelease/2001/pdf/po-virusprotection.pdf, in Japanese).

[*4] IIJ, "IIJ launches the IIJ Mail Gateway Service to help medium-sized enterprises stop information breaches" (https://www.iij.ad.jp/news/pressrelease/2002/pdf/iij-mgw.pdf, in Japanese).

[*5] IIJ, "IIJ adds the new MailViewer feature to the IIJ Post Office Service" (https://www.iij.ad.jp/news/pressrelease/2003/pdf/0327.pdf, in Japanese).

[*6] The iconic Gmail webmail service was launched in 2004 on an invitation-only basis.

[*7] IIJ, "IIJ bolsters the anti-spam features of its business email outsourcing service" (https://www.iij.ad.jp/news/pressrelease/2004/pdf/0928.pdf, in Japanese).

[*8] IIJ, "IIJ Launches the IIJ Secure MX Service for comprehensive email risk management" (https://www.iij.ad.jp/news/pressrelease/2006/pdf/0905.pdf, in Japanese).

[*9] IIJ, "IIJ adds support for DKIM sender authentication to the IIJ Post Office Service" (https://www.iij.ad.jp/news/pressrelease/2010/pdf/po_dkim_2.pdf, in Japanese).

For a service with a lengthy history, it becomes difficult to respond to the ever-changing Internet security requirements as well as customer demands for new features and improvements.

■ (2) Efforts to address vulnerabilities come up against limits

Your task isn't over once you've developed a piece of software. You then need to address the seemingly daily reports of vulnerabilities as well as the need for ongoing software maintenance to deal with eventual middleware end-of-life. It's also important to note that with service release cycles in general, software maintenance is a far longer-term undertaking than initial development.

For example, we continued to provide the IIJ Post Office service through six generations and seven types of OSs, replacing the OS each time support ended. This sort of maintenance and development is crucial when it comes to maintaining service quality. But the truth is that it is also a rather unglamorous undertaking. It does not yield as many visible changes as new feature development, and it also carries the risk of introducing new bugs because you're modifying something that already works, and these aspects can be difficult to convey to customers, sales reps, and management.

■ (3) The development history and background may be unclear

With older IIJ services, it was not uncommon for the team that developed the service to be responsible for running it as well. While an advantage of this approach is that the service is run by those who are most familiar with it, making it possible to recover quickly in the event of failure, the disadvantage here is that it does not incentivize documentation and it impedes the transfer of skills to new team members. The IIJ Post Office Service fell into this category.

So as time passes and the number of people from the original development team still running the service decreases, the development and operation of the service ends up being handled by people who were not involved in the planning and launch phase. And when they encounter any undocumented parts of the service, these newer team members have no option but to guess at the original development motivations. They increasingly find themselves asking, "Why is it like this?", which raises the barriers to maintenance development and maintenance itself considerably.

1.2.2 Service Termination Decision and Roadmap

We continued to push ahead with the service against this backdrop, but we eventually came up against technological issues that would prevent us from extending the service's life any further.

We explained this situation to the Steering Committee, and at an internal meeting attended by people from the operation, development, and support departments in 2018, the decision was made to discontinue the IIJ Post Office service in four years' time. We laid out the following action plan.

- Set the service end date
- Establish teams to support the transition to the successor service (IIJ Secure MX Service)
- Develop and implement migration support functionality for the IIJ Secure MX Service
- Internal announcement
- Announcement to customers
- Check on individual progress with sales reps

To minimize the impact of the service termination on customers' businesses, we contacted every single one of our sales reps to confirm progress. This is a fairly involved, hands-on task, but the decision to discontinue the service was our own after all, so after a careful preliminary investigation, roughly a year before the actual service termination date, we began working with the sales team and got the cross-departmental process underway.

1.2.3 Calling Curtains on 24 Years of History

On September 30, 2022, the IIJ Post Office Service was quietly retired. We apologize to our customers for any inconvenience caused by the termination of this service.

As a member of a technology department, I don't usually have the opportunity to thank customers directly, so I would like to take this opportunity to express my sincere gratitude to everyone who has used the IIJ Post Office Service over the years. Thank you very much for your support.

The IIJ Secure MX Service is now available as the successor to the IIJ Post Office Service. We humbly ask for your continued support of IIJ's services.

1.2.4 To Customers Who Were Using the IIJ Post Office Service

We have a final request for customers who were using the IIJ Post Office Service.

> If the TXT record for your domain contains
> include:spf.po.2iij.net
> please be sure to delete this.

We are currently performing a post-service cleanup and will delete this SPF record soon.

Any customers who inadvertently leave the IIJ Post Office Service include tag ("include:spf.po.2iij.net") in their email domain's SPF record are likely to experience sender authentication failures (permerror) at email destinations once we have deleted this record. This could hobble your domain's spoofing countermeasures.

We have contacted those customers who are reachable via our sales reps, but if you're reading this, please take this opportunity to check on your end.

1.3 DMARC 2.0 (M^{3}AAWG Topic)

The first in-person M^{3}AAWG meeting in three years took place in San Francisco in February 2023. M^{3}AAWG (the Messaging, Malware, and Mobile Anti-Abuse Working Group), established in 2004, is an organization that facilitates discussion with a focus on email and other messaging technologies. In recent years, the focus of discussion has broadened beyond email, with a number of companies and academic institutions engaged in areas such as SMS and social media messaging also getting involved. M^{3}AAWG participants include MSPs (mailbox service providers) like IIJ, ESPs (email service providers), server hosting providers, academic institutions, DNS Federation, and security vendors that offer antispam/antivirus engines.

International M^{3}AAWG meetings are held three times a year, typically in San Francisco around February, somewhere in Europe around June, and in a North American city around October.

The February meeting covered a range of themes, with the session on DMARC 2.0 offering a particularly lively discussion. In this section, I summarize some key information on DMARC 2.0[*10] as of April 2023.

M^{3}AAWG meetings are private, so I am unable to disclose details of what was discussed. The information here is based solely on what is available publicly. Also note that while IETF documents also use the term DMARC-bis, here I refer to DMARC 2.0 throughout for consistency.

DMARC is a sender authentication technology currently used on the Internet and is defined as an international specification in RFC 7489[*11]. A number of changes are under consideration for DMARC 2.0. The main ones are as follows.

- While RFC 7489 is classified into the Informational category, the aim is to make DMARC 2.0 a standard.
- Use of DNS Tree Walk instead of the Public Suffix List for DMARC policy discovery.
- Removal of some tags and addition of new tags.

1.3.1 Public Suffix List and DNS Walk Tree

The Public Suffix List[*12] is a list maintained by volunteers who manage domains called eTLDs (Effective TLDs). It was once maintained by Mozilla, known for products like Firefox and Thunderbird, and is now handled by volunteers.

[*10] IETF, Datatracker (https://datatracker.ietf.org/doc/draft-ietf-dmarc-dmarcbis/).

[*11] IETF, Datatracker (https://datatracker.ietf.org/doc/html/rfc7489).

[*12] GitHub, publicsuffix/list (https://github.com/publicsuffix/list).

Common domains for Japan on this list include co.jp and ne.jp, and domains used by local governments are also listed.

RFC 7489 notes the problem of not being able to search for or determine organizational domains for domains not registered on the Public Suffix List. DMARC 2.0 solves this problem by using DNS Tree Walk to determine the organizational domain and search for DMARC policies when DMARC evaluation is performed.

Domain owners who register and publish DMARC records need not make any changes. Meanwhile, for IIJ and other mailbox providers that provide services like the IIJ Secure MX service, which receives email and evaluates DMARC records, it may be necessary to modify the program used when evaluating domains.

1.3.2 Removal of Tags and Addition of New Tags

Table 2 shows the planned tag removals and additions for DMARC 2.0. Here, a point of concern for operators like IIJ that receive DMARC reports or filter using DMARC records is when exactly to discontinue/commence support for the old/new tags. The DMARC record for each domain is implemented by the organization that manages that domain, and each organization can update its record when it sees fit. Hence, we will need to carefully determine exactly when to end support for tags slated for removal and when to commence support for tags slated to be added.

1.4 Report on the Uptake of Sender Authentication and STARTTLS

1.4.1 Sender Authentication Data

As in IIR Vol. 55, here we chart (Figure 1) the proportion of emails received by the IIJ Secure MX service for which sender authentication was supported.

Looking at the SPF verification results, the proportions are almost the same as last time, but DKIM pass and DMARC pass have each increased by around 8 points each. It is evident that even in Japan the number of companies implementing DKIM signatures and setting DMARC policies as a means of combating email spoofing is rising, albeit gradually. In February 2023, Japan's Ministry of Internal Affairs and Communications asked credit card companies to adopt DMARC to bolster their phishing email defenses[*13].

Add/remove	Tag	Description
Add	np	Flag specifying policy for non-existent subdomains (taken from RFC 9091)
Add	psd	Flag indicating whether Public Suffix Domain or not
Add	t	Flag retaining some of the functionality of the pct flag (see below)
Remove	pct	Flag declaring the percentage of messages to which the DMARC policy is applied
Remove	rf	Format to be used for DMARC failure reports
Remove	ri	Interval requested between aggregate DMARC reports (defaults to once a day, higher values to be accommodated on a best-effort basis)

Table 2: Tags Slated to be Added/Removed in DMARC 2.0

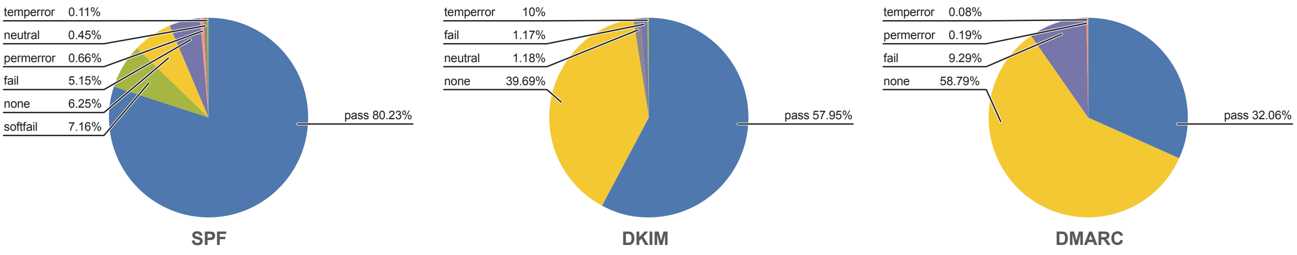

Figure 1: Proportion of Sender Authentication Support for Emails Received by the IIJ Secure MX Service

[*13] Ministry of Internal Affairs and Communications, "Call for credit card companies and the like to bolster anti-phishing measures" (https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000184.html, in Japanese).

1.4.2 Inbound/Outgoing STARTTLS data

For several years now, the idea of bringing an end to PPAP (colloquial Japanese term for the practice of sending encrypted, password-protected ZIP files via email) has frequently been raised when it comes to discussing security issues around email.

There have been media reports about some companies taking steps to end PPAP in response to the spread of the Emotet virus, which we have covered in previous editions of the IIR, but PPAP continues to pop up all the time as an Internet security issue in Japan.

IIR Vol. 55, published a year ago, explained that IIJ was blocking PPAP, but here I would like to approach these issues from the perspective of encrypting communication routes instead of encrypting email attachments.

For companies, PPAP provides a way of encrypting attachments in a form that is easily recognized by employees who send email and by humans working with the email transmission system, but if the emails to which files are attached can themselves be encrypted, this would probably reduce the risk of information breaches. So here we take a look at what proportion of emails received from the Internet and emails sent out over the Internet on the IIJ Secure MX Service were exchanged over TLS over the twelve months from April 2022 to April 2023.

The IIJ Secure MX Service supports the encryption of routes when sending and receiving emails[14].

The SMTP email transfer protocol uses the STARTTLS protocol extension for TLS transfers. Once a connection with the other server is established, subsequent communications are sent over TLS, with the Envelope From, Envelope To, and DATA (email header and body) fields sent using the supported TLS version and encryption method. If the other server does not support TLS, the email is sent as plain text[15].

Figure 2 graphs the proportion of emails received on the IIJ Secure MX Service that used STARTTLS over the twelve months from April 2022 to April 2023.

The IIJ Secure MX Service is used by a wide range of business customers, so we observe connections coming in from all sorts of servers on the Internet.

Depending on the day, we observe attacks targeting specific customers and phishing emails that are more or less broadcast to many different recipients.

These emails come from a whole range of servers on the Internet, and it seems that many of the servers send emails without encrypting the SMTP communications using STARTTLS.

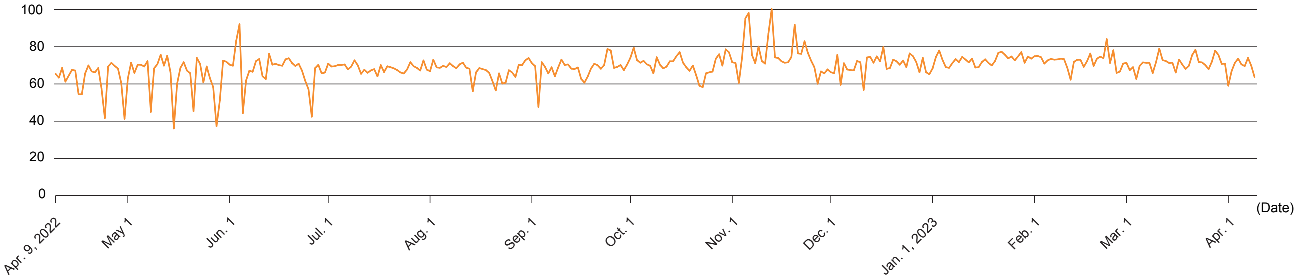

Figure 2: Proportion of Emails Received on the IIJ Secure MX Service Using STARTTLS (Apr. 2022 – Apr. 2023)

[14] IIJ, "Route encryption" (https://www.iij.ad.jp/en/biz/smx/other.html#anc_02).

[15] ietf.org, "SMTP Service Extension for Secure SMTP over Transport Layer Security" (https://www.ietf.org/rfc/rfc3207.txt).

The wide fluctuations in the STARTTLS readings from April to May 2022 probably reflect the fact that Emotet was proliferating at the time and thus sending itself out from a lot of Internet-connected servers.

Figure 3 graphs STARTTLS usage for emails sent out onto the Internet from IIJ Secure MX Service servers.

Route encryption is used for outgoing emails from the IIJ Secure MX Service unless the destination server does not support STARTTLS, so as is evident, a higher proportion of these communications are encrypted than is the case with received emails.

For many years, IIJ has also provided an automatic attachment encryption feature, but we plan to discontinue this within the next few years as a means of combating viruses that exploit encrypted ZIP files like Emotet.

While route encryption and the encryption of email attachment contents are not conceptually all that comparable, our hope is that these data will prove useful in efforts to break free from PPAP.

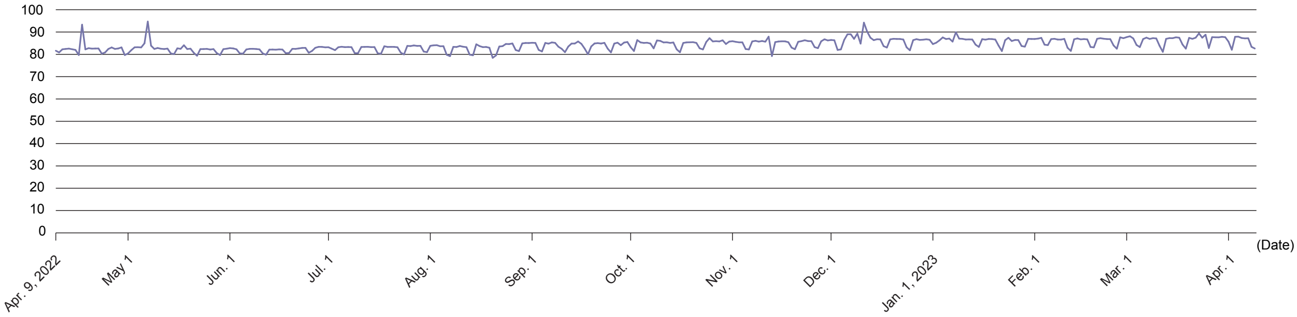

Figure 3: Proportion of Emails Sent on the IIJ Secure MX Service Using STARTTLS

1.1 30 Years with Email, 1.2 IIJ Post Office Service

Isamu Koga
Manager, Operation & Engineering Section, Application Service Department, Network Division & (concurrently) Member of the President's Office, IIJ

Mr. Koga joined IIJ in 2007. He is engaged in the operation of email services and investigates email-related trends in the wild. To keep customers' email boxes safe, he communicates information about the latest attack methods, trends in spam, and countermeasures. He is also involved in a wide range of community activities, including M^{3}AAWG, WIDE Project, and openSUSE.

1.3 DMARC 2.0 (M^{3}AAWG Topic), 1.4 Report on the Uptake of Sender Authentication and STARTTLS

Yusuke Imamura
Lead Engineer, Operation & Engineering Section, Application Service Department, Network Division, IIJ

Mr. Imamura joined IIJ in 2015. He is engaged in the operation of email services. His past experience working at IIJ Europe benefits him in fulfilling his global role.