Protecting Our Customers from Ever More Sophisticated Cyberattacks

1.1 A New Era for Email

A year has passed since our last report on this topic[*1], and the email industry saw huge changes in 2023.

In the first half of this article, we report on the latest attack methodology observed by IIJ and discuss the new countermeasures we have started taking against these threats. In the second half, we report on the dramatic changes in sender authentication technology DMARC compliance rates observed over the past year.

Email infrastructure is crucial in providing organizations a means of both internal and external communication, but it is difficult to make changes once that infrastructure is built. But with attack methods and security trends ever changing, organizations face a constant need to take countermeasures. Why not take this opportunity to review your email infrastructure?

1.2 Protecting Customers from Threats

1.2.1 What is Abuse Protection?

Email services are constantly being abused as a means of sending phishing (fraudulent) emails.

In general, most ISPs (Internet service providers) and hosted email services use the combination of an email account user ID and password (credentials) for SMTP authentication, only allowing users to send emails if that authentication is successful. This authentication is used to identify users and to protect the email service from unauthorized use by third parties.

Malicious actors, however, are always stealing user credentials by some means or another and using email services to send phishing emails (account hijacking)[*2]. IIJ is not alone here. This activity occurs at other ISPs and on other companies' services, and this sort of unwelcome and fraudulent behavior on the Internet is commonly referred to as abuse.

1.2.2 Effects of Abuse

What happens when malicious actors exploit email services to send phishing emails?

In recent years, instead of simply sending unwanted advertising emails (spam), malicious actors have turned to phishing emails as a way of stealing the IDs and passwords for web services and apps from their victims, the recipients of phishing emails. Their ultimate goal is one of financial gain—stealing IDs and passwords from users duped by phishing emails enables them to then steal bank account details and credit card numbers. With the use of cloud services becoming increasingly more prevalent in recent years, this sort of activity is becoming more and more prominent.

Naturally, most email services prohibit users from sending phishing emails under their terms of use. Malicious actors are attempting to increase their attack success rates by sending large numbers of phishing emails in a very short period of time before their ability to send emails is restricted due to terms of use violations, in what is a truly shotgun approach.

*1 IIR Vol. 59 (https://www.iij.ad.jp/en/dev/iir/059.html).

*2 Some time ago, there were cases of passwords being discovered via brute-force credential attacks, but this itself is abuse and an inefficient method. In almost all cases these days, phishing emails are sent out successfully on the first try without any prior authentication attempts, so it is natural to assume that malicious actors are using some means of obtaining credentials in advance.

1.2.3 Problems of Abuse

Leaving this situation unchecked not only exposes the targeted users to harm but also adversely impacts on email services in the following ways.

- When malicious actors use email services to send out large volumes of phishing emails, this can overload the IT equipment, leading to service disruptions and reduced availability ((1) and (2) in Figure 1).
- The transmission of phishing emails results in the email service being recorded as a phishing email source by destination email servers, security vendors, etc., such that emails from other legitimate users are identified as spam and blocked at those destinations ((3) and (4) in Figure 1).
- The impact of this can be long-lived since some security vendors draw on threat intelligence from other security vendors, such that it takes time for threat intelligence to be removed from everywhere it has been recorded ((6) and (7) in Figure 1).

Hence, to ensure stability and to prevent other customers from being adversely impacted on IIJ's email service, IIJ Secure MX Service, we immediately investigate any cases of abuse and work around the clock to protect our equipment by, for example, forcibly changing email service user credentials and blocking certain communications.

1.2.4 Abuse and Secrecy of Communications

In Japan, Article 4 of the Telecommunications Business Act prohibits actions such as revealing or obtaining telecommunications handled by telecommunications carriers[*3*4]. However, when abuse has been explicitly recognized and it is highly likely that, if it is left unchecked, service users will become complicit in illegal acts that infringe on the rights of others or become

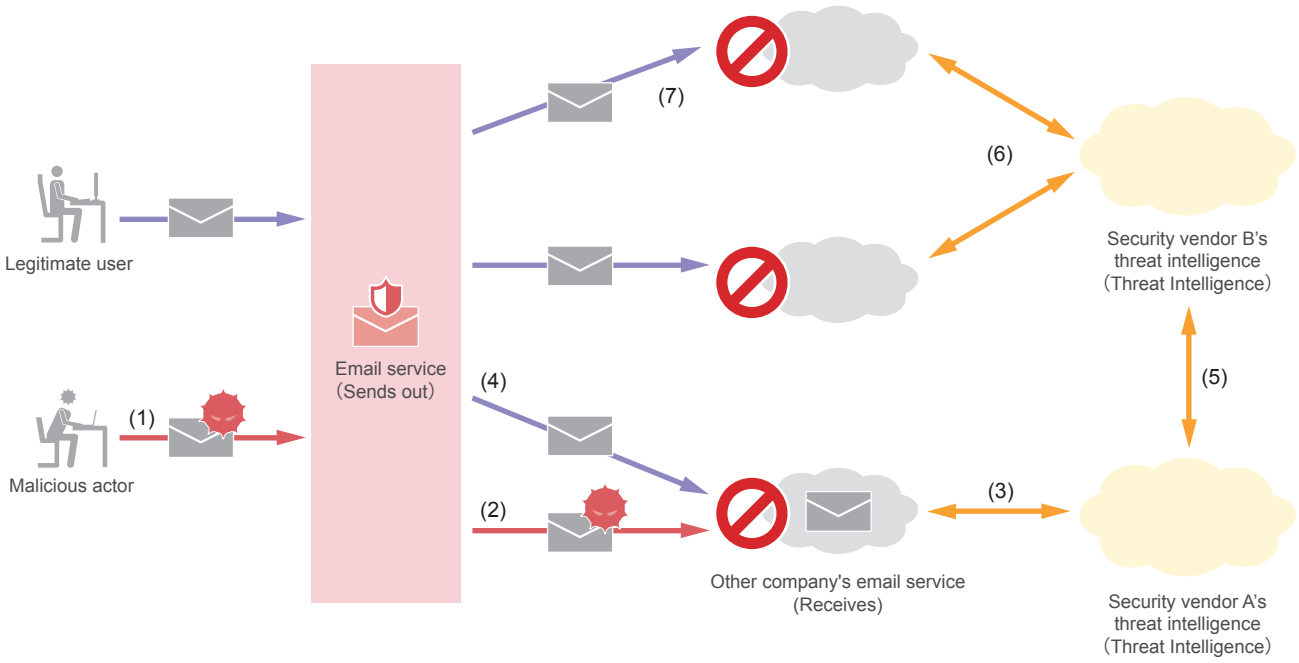

Figure 1: Adverse Impact of Abuse on Email Services

*3 This concept of secrecy of communications originally referred to postal correspondence. It is the right to prevent third parties from knowing when, by who, and with whom communications are taking place, and what the content of those communications is. In Japan, this also applies to the Internet, but countries that deal with it in this way are in the minority worldwide, and censorship is considered to be legal in the vast majority of countries. "Only four countries, including Japan, do not monitor or interfere with the Internet" (Yasuhiko Taniwaki, Kyoyo to shite to no Internet [The Internet as Culture, in Japanese], Nikkei BP, 2023; Freedom House (US-based NPO) survey, https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf).

*4 A postal worker must look at the front of a postcard to know which recipient's mailbox to put it in, and similarly, on the Internet, communications cannot be delivered unless the IP packet headers, and in the case of email the content of the SMTP protocol content, are seen. Hence, such actions are categorized as those that, while violating the secrecy of communications, are still legitimate business activities.

victims themselves, the illegality of those (normally prohibited) actions involving telecommunications, when taken to prevent such outcomes, can be waived on the basis that they fall into the category of emergency measures or legitimate business activities.

IIJ's agreements with its users prohibit any acts that constitute abuse, and as a party to these agreements, IIJ has the ability to take various measures to deal with clear violations of the agreements.

1.2.5 Discovery of Preparations for Abuse

In the past few years, we have, through our daily operations, discovered multiple instances of test mailouts whereby someone, rather than sending phishing emails out all of a sudden, sends out a number of seemingly harmless emails a few days beforehand. The following is an example of the type of information included in the email subject line:

Email address; login ID; password; SMTP server name; port number; number sent; auth. method
Example:
`iij-taro@example.jp;iij-taro;password;mail.securemx.jp;465;2;LOGIN`

The email addresses in the recipient field of such emails are thought to be collecting the results of reconnaissance activities, and a causal link has become clear in that actual phishing emails are sent out a few days later (Figure 2).

At this preparatory stage, however, we cannot really say that these actions violate the rights of others or even that there is a high likelihood of such a violation, so we cannot necessarily label this as abuse. So even though we were aware of this preparatory stage of events, we had no basis for taking specific action until abuse actually occurred. This was a very frustrating situation for us as operators of equipment that is supposed to protect our customers while maintaining quality of service.

1.2.6 IIJ's New Initiatives

As it was, we were hamstrung and unable to protect our customers. And so we knew we needed to put a new framework in place. Bringing in IIJ's support and legal departments, we set about designing a framework for restricting communications to the extent necessary before phishing emails were actually sent out whenever we detected these sorts of preparations for the improper use of our services.

Table 1 describes the benefits of taking action before phishing emails are sent out.

After much discussion with everyone involved, we decided to implement this into our agreements through the following steps.

- Provide all customers with a detailed explanation of our new initiatives in advance.
- Also make changes that incorporate specific provisions into the IIJ Secure MX Service terms and conditions so that customers are fully aware of the changes.

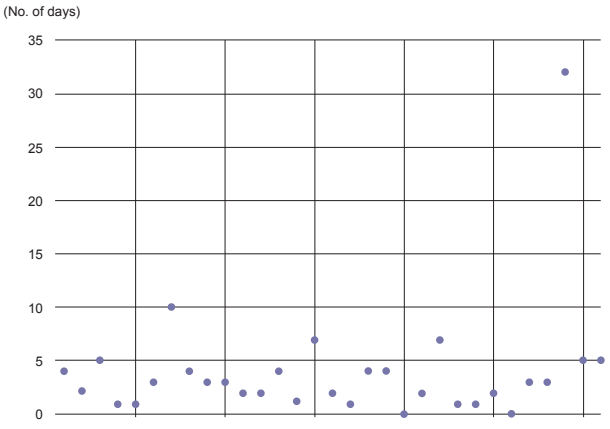

Figure 2: No. of Days After Reconnaissance that Actual Abuse Occurred (During a Particular Period)

Table 1: Benefits of Countermeasures

From perspective of	Benefits
Email service operator (IIJ)	・Can take countermeasures before phishing emails are sent, preventing service disruptions and avoiding a situation in which emails do not reach their destinations
Users	・Can detect credential breaches early ・Can limit the damage caused by email interceptions and information breaches

We have sent notifications to our existing customers' administrators, so please take a look. The relevant terms of service were included in the May 1, 2024 revision. Please refer to Article 12 (Dealing with the risk of misuse, etc.) of the IIJ Secure MX Service Individual Regulations.

Incidentally, while we refer to action taken against abuse that has already happened as our abuse response, when we detect preparations for improper use and take action to protect our customers in advance, we call this defensive action.

1.2.7 IIJ's Defensive Action

We initially discovered these reconnaissance activities in the course of our daily operations, but there is only so much we can do manually. So we have now harnessed illumino[*5], a large-scale log analysis platform deployed internally at IIJ, to use machine learning to detect events likely to constitute preparations for improper use of our services (Figure 3)[*6].

We actually did not start using Splunk for defense purposes; we were originally looking at using it to conduct investigations that would help streamline our abuse response. But it was in the course of these investigations that we uncovered these abuse preparations. We wondered whether we could use machine learning to detect this sort of activity as well, and our efforts to improve accuracy in this regard resulted in us being able to detect such preparatory actions with a fairly high probability.

1.2.8 Conclusion

The fact that the telecommunications companies through which people's communications and data pass are heavily regulated in terms of how they conduct their business is not that well known among ordinary consumers. Yet the Internet connects the entire world together. When we take action to protect our customers from malicious actors, these actions are always accompanied by efforts to protect the secrecy of communications, and we are mindful of striking a balance between these two objectives in the course of our operations.

At IIJ, we will continue working to protect our customers from the ever more sophisticated cyberattacks they face.

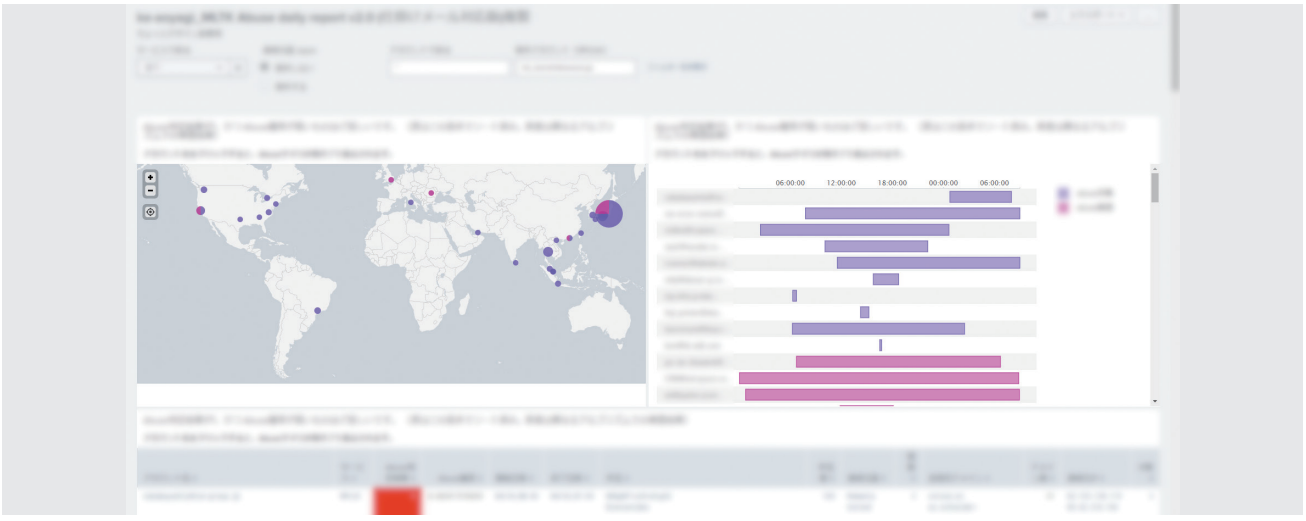

Figure 3: Splunk Dashboard for Defensive Action

*5 "illumino—IIJ's Internal Data Analytics Platform", Internet Infrastructure Review Vol. 57 (https://www.iij.ad.jp/en/dev/iir/057.html).
*6 For examples of how we use Splunk, see "Japanese Text Analysis Using Splunk", Internet Infrastructure Review Vol. 48 (https://www.iij.ad.jp/en/dev/iir/048.html).

1.3 The Big Push for Sender Authentication

1.3.1 Calls for DMARC Support in the Financial Industry and Related Developments

In February 2023, Japan's Ministry of Internal Affairs and Communications, National Police Agency, and Ministry of Economy, Trade and Industry called on financial institutions such as credit card companies to implement DMARC policies as a means of combating email spoofing[*7].

Credit card companies and the like have long been increasingly plagued by the damage caused by email spoofing, with observers exclaiming the need for countermeasures, and the official call to action seems to have set off an earnest push to take steps in that direction. This is evident from the increase in the DMARC compliance rate for financial industry domains shown in Figure 4[*8].

Only around 20% of domains had published DMARC policies as of January 2023, but one year later in January 2024, that figure had increased to 80%. Yet, many domains that have published DMARC policies still have them declared with p=none. For DMARC to be properly effective, they need to change this to p=quarantine or p=reject. A major move toward this happened in the financial industry in 2023, but a look at Japanese domains as a whole reveals that many companies are yet to make this change (Figure 5)[*9].

We will continue to focus on developments in this area in the hopes that other industries will follow the financial industry in implementing DMARC policies.

1.3.2 Google and Yahoo in the US Unveil Policy of Blocking Emails With No Sender Authentication

In October 2023, Google and Yahoo in the US announced that from February 2024 they would be blocking emails that do not support sender authentication. Both Google and Yahoo are plagued by huge volumes of spam and bulk mail every day, and to block such emails from coming into

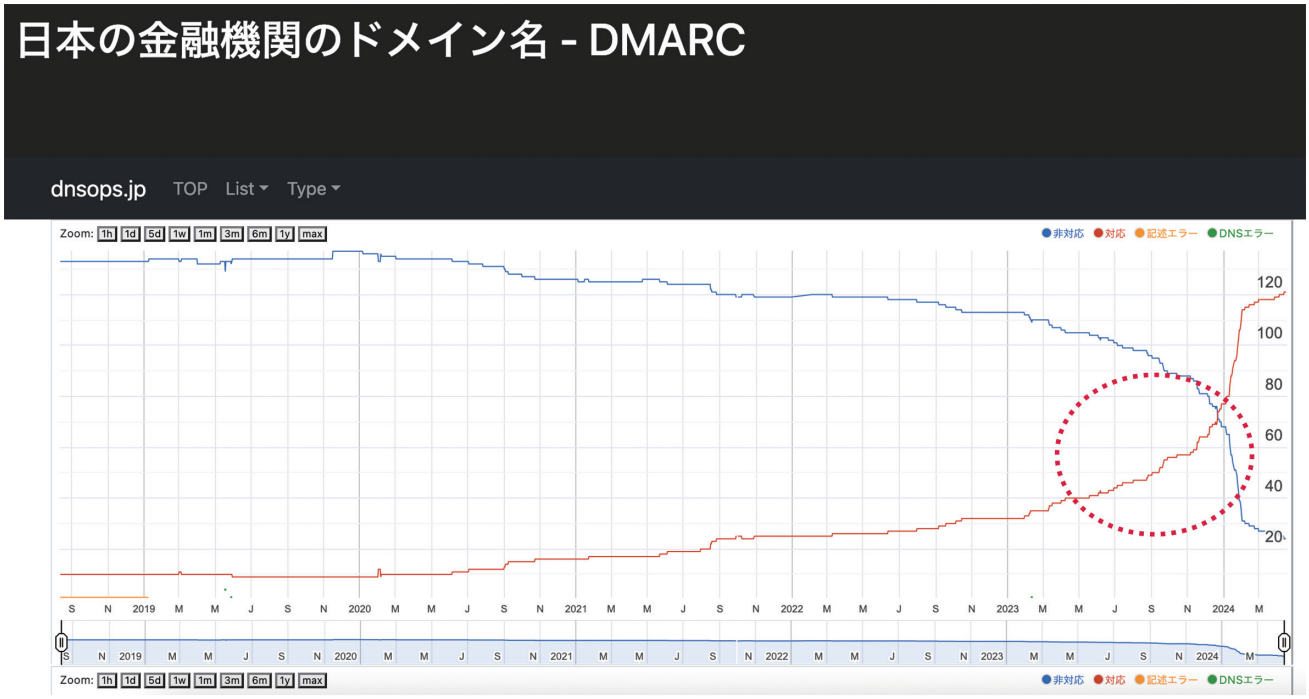

Figure 4: DMARC Compliance on Japanese Financial Institution Domains

*7 Ministry of Internal Affairs and Communications, "Call for Credit Card Companies etc. to Bolster Phishing Countermeasures" (https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000184.html, in Japanese).

*8 Domain status of Japanese banks - DMARC (https://stats.dnsops.jp/chart/jp-bank/dmarc).

*9 Domain status of Japanese organizations - DMARC (https://stats.dnsops.jp/chart/all/dmarc).

their servers, the companies moved to block all emails that do not support sender authentication.

Sender authentication technologies include SPF, published in 2006 (RFC 4408), DKIM, published in 2007 (RFC 4871), and DMARC, published in 2014 (RFC 7208). In 2023, nine years after its release in 2014, DMARC was still not all that widely adopted (Figure 5)[*10*11].

The revelation that global heavyweights Google and Yahoo, which handle some of the biggest email volumes in the world, would be adopting a “no auth, no entry” policy shocked IT providers around the world. Email delivery rates are a key service indicator for mass email senders, so the move created an impetus for them to adopt DMARC with all due haste.

In the immediate wake of this, M^{3}AAWG (Messaging Anti-Abuse Working Group), which works to combat spam globally, hosted an emergency Q&A session on the announcements with representatives from Google and Yahoo at its October 2023 meeting. The session was intense, with participants, predominantly hailing from email senders around the world, asking, for instance, what level of commitment would be required and whether emails would really be blocked if they did not comply.

Subsequently, at the November 2023 meeting of JPAAWG, a working group that discusses Internet security in Japan, the matter was taken up predominantly by operators of email businesses in Japan. Of course, it is not just bulk senders but also domain owners in the form of companies and mailbox providers that need to respond to the move, and we at IIJ had also been working on a response for IIJ’s our own business and personal services.

We Our email services already had a system ready for sender authentication technologies (SPF, DKIM, and DMARC) IIJ’s

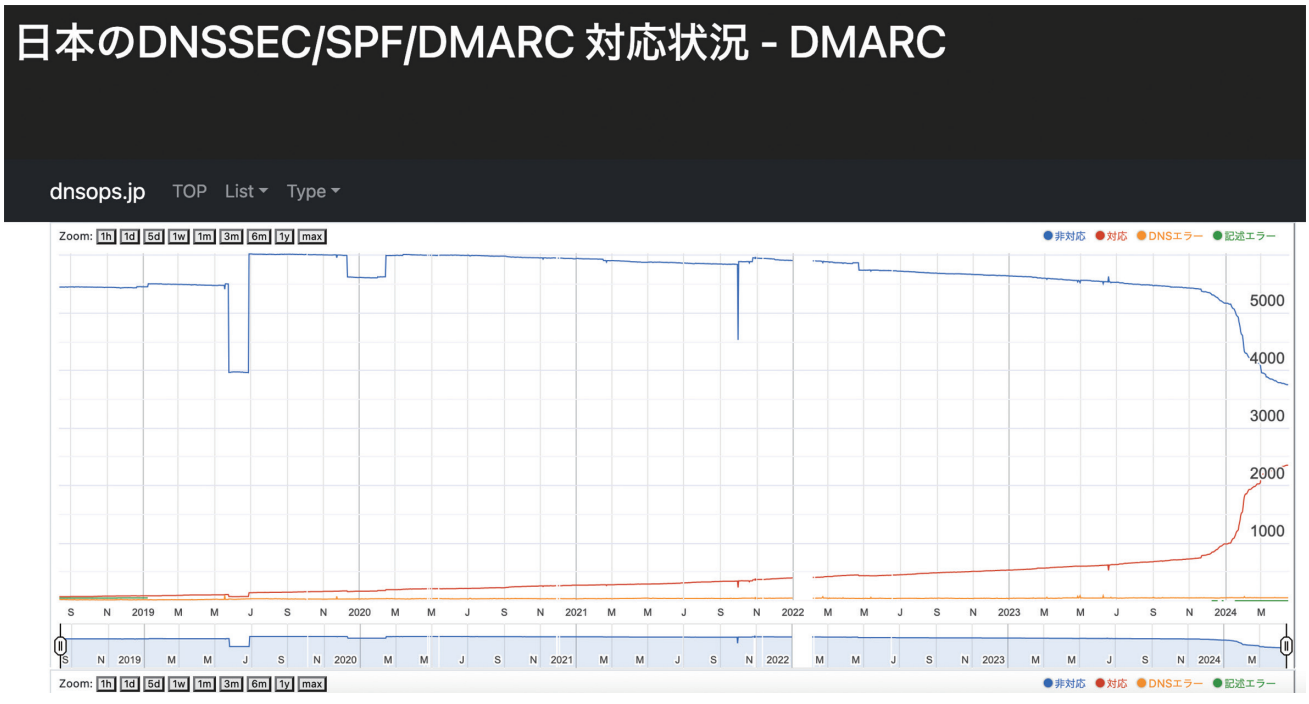

Figure 5: DMARC on Japanese Domains

*10 Domain status of Japanese organizations - DKIM (https://stats.dnsops.jp/chart/all/dkim).
*11 Domain status of Japanese organizations - DMARC (https://stats.dnsops.jp/chart/all/dmarc).

services for business customers, but customers they needed to make configuration changes and take certain steps themselves to get the features working, so we experienced a huge increase in customer inquiries about sender authentication at the end of 2023.

The efforts of the various businesses, corporations, and organizations resulted in a dramatic change in sender authentication compliance rates for emails received on the IIJ Secure MX Service (Figure 6).

The proportion of emails with DKIM signatures increased by just over 15%, and the proportion of sender domains with DMARC records (those other than none in the DMARC pie chart) increased by over 30%pt, from 42% to 75%. Given the 2022 figure was 32%, it looks like the number of organizations that have implemented DMARC records has increased for the reasons discussed above.

That said, all this does is confirm that DMARC records exist. We have not looked at whether the DMARC policies use p=none, p=quarantine, or p=reject. Domain owners should change from p=none to p=quarantine or p=reject to keep tabs on DMARC reports.

1.3.3 Problems with Sender Authentication Technologies

With the use of cloud services rising in recent years, the incidence of companies sending emails from on-premises equipment directly out onto the Internet is in decline. And so some have begun to argue that an assessment of SPF records alone is insufficient to ensure email trustworthiness.

Also, in order to send emails from multiple cloud services, some domains have been observed to exceed the limit of 10 DNS lookups when resolving SPF records, causing the SPF record lookup itself to return an error.

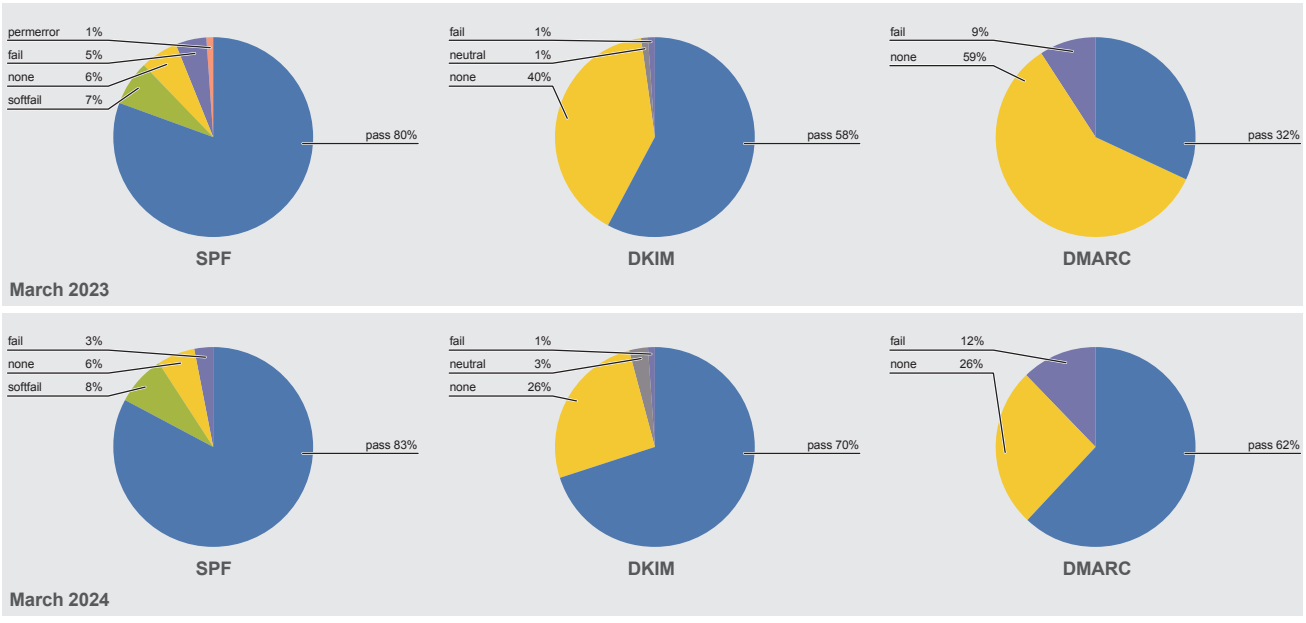

Figure 6: Sender Authentication Compliance Rates for Emails Received on Secure MX (2023 vs. 2024)

To avoid this, some providers offer services that use CNAME records to bundle the records pointed to via the SPF include mechanism into a single record. The original reason for the SPF include limit is that SPF records with many inclusions could act as DNS lookup amplifiers[*12].

Some cloud services specify SPF records with a huge number of IP address ranges, and when using your own domain name to send email from these types of cloud services, you can avoid the SPF limits by implementing DKIM signatures so that emails pass DKIM sender authentication.

Even so, DKIM is not a panacea, and you need to take action against DKIM replay attacks and properly manage DKIM key expiration terms[*13].

When it comes to DMARC too, service providers have a deep history of dealing with DKIM signature validation failures caused by long-established email mechanisms whereby headers are rewritten after emails are DKIM signed, as can happen with forwarded emails and mailing lists, for example.

ARC is designed to avoid these sorts of DKIM validation failures by re-signing emails after headers have been changed, but as with DKIM, it is left up to the receiving servers to decide which signing domains to trust.

Many issues remain to be addressed in the area of sender authentication, and IIJ is committed to tackling them by collecting and disseminating crucial information, participating in the development of IETF standards, and so forth[*14]. Efforts to support SPF, DKIM, and DMARC sparked by the recent Google and Yahoo announcements are just beginning, and it's crucial to remember that ongoing effort will be needed with respect to all of these issues.

1.1 A New Era for Email, 1.2 Protecting Customers from Threats
Isamu Koga
Manager, Mail Service Management Section, Application Service Department, Network Division, 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 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 M^{3}AAWG, WIDE Project, and openSUSE.

1.3 The Big Push for Sender Authentication
Yusuke Imamura
Lead Engineer, Mail Service Management 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.

*12 IETF Datatracker, 11. Security Considerations, 11.1. Processing Limits (https://datatracker.ietf.org/doc/html/rfc7208#section-11.1).
*13 IETF, DKIM Replay Problem Statement (https://www.ietf.org/archive/id/draft-ietf-dkim-replay-problem-00.html).
*14 IETF Datatracker, The Authenticated Received Chain (ARC) Protocol (https://datatracker.ietf.org/doc/html/rfc8617).