Messaging Technology

1.1 Introduction

According to the Council of Anti-Phishing Japan's reports[*1], the number of phishing cases reported to the council is rising rapidly. April 2020 saw 11,645 cases reported, an increase of 1,974 vs. the previous month (March 2020) and a hefty 9,257-case year-on-year rise (vs. April 2019). The substance of these cases shows a large volume of phishing impersonating major companies that maintain an online presence. Indeed, I have also received a number of such emails. The Subject header and the display name and local part of the From header generally look the part, but the sender domain name is often completely different. And because fraudulent emails impersonating government agencies may be on the rise, countermeasures should be taken by both email recipients as well as owners of domains likely to be spoofed.

As we have repeatedly reported, sender authentication is effective against phishing and other forms of email spoofing. Those who send phishing emails are aware of these measures, however, so using them properly is important to ensure effectiveness. Further, some posit that the rise in these emails reflects the recent social situation, so it may persist for some time yet.

In this issue, we report on the prevalence of sender authentication technologies (SPF, DKIM, DMARC) that are effective against email spoofing. We also discuss how to use the results of sender authentication against the type of phishing emails currently circulating. We also report on the JPAAWG 2nd General Meeting, held last year.

1.2 Sender Authentication Rates

It is now 14 years since the first SPF (Sender Policy Framework) specification, RFC 4408[*2], was published in April 2006. This was later followed by the DKIM specification, which uses digital signatures, and eventually DMARC, which uses SPF and DKIM authentication results. We report on the current prevalence of these sender authentication technologies.

*1 Council of Anti-Phishing Japan, monthly reports listing (https://www.antiphishing.jp/report/monthly/, in Japanese).

*2 Subsequently revised in April 2014 as RFC 7208.

1.2.1 Results Based on Emails Received

Given the practical implications, the percentage breakdown of authentication results for received emails can be considered important from the perspective of studying sender authentication deployment rates. IIJ's email services provide the ability to perform SPF, DKIM, and DMARC sender authentication upon email receipt. This feature returns a "none" result for each method if the received email cannot be authenticated. So the proportion of received emails that do not return "none" can be interpreted as the deployment rate for received emails.

Figure 1 shows the breakdown of SPF authentication results for emails received in April 2020. The "none" result accounts for 12.1%, meaning that the deployment rate was 87.9%. This is a 2.2%pt increase vs. the rate of 85.7% reported a year ago in IIR Vol. 43. The figure for "pass", meaning SPF authentication was successful, rose 9%pt from 70.1% in April 2019 to 79.1% in April 2020. So the proportion of authentication failures (hardfail, softfail, and neutral in the case of SPF) also fell by 6.4%pt, indicating a rise in emails not spoofing as far as SPF is concerned. The increase in phishing reports, however, implies that spoofed emails are not themselves in decline. That is, spoofed emails that are not spoofing as far as SPF is concerned may be on the rise.

Figure 2 breaks down DKIM authentication results for emails received in April 2020. The "none" result accounts for 51.7% (48.3% deployment rate), a 10.5%pt drop from 62.2% a year earlier, meaning that the deployment rate increased 10.5%pt. Implementing DKIM as a sender requires some effort as it requires adding a DKIM digital signature on the sending email server. The current deployment rate is by no means adequate, but 13 years since the first DKIM specification was released in RFC 4871, it has finally spread to around half of all emails received (in terms of emails received on IIJ services).

Figure 3 breaks down DMARC authentication results for emails received in April 2020. The "none" result accounts for 75.4%, indicating a deployment rate of 24.6%, a 1.5%pt increase vs. a year earlier. This is a very small increase relative to SPF, which in practical terms is now

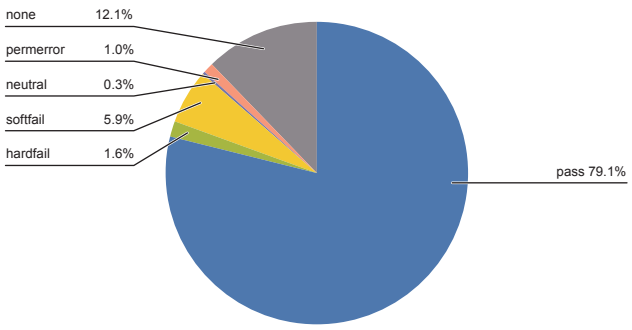

Figure 1: Breakdown of SPF Authentication Results

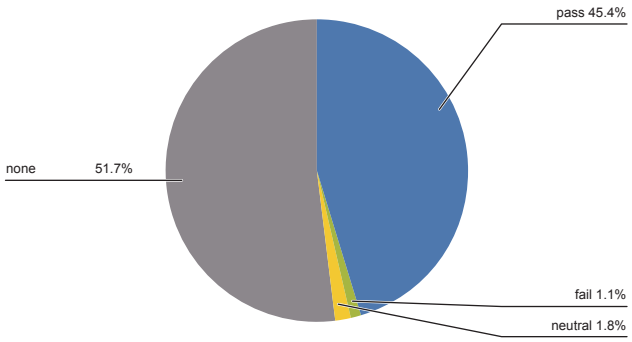

Figure 2: Breakdown of DKIM Authentication Results

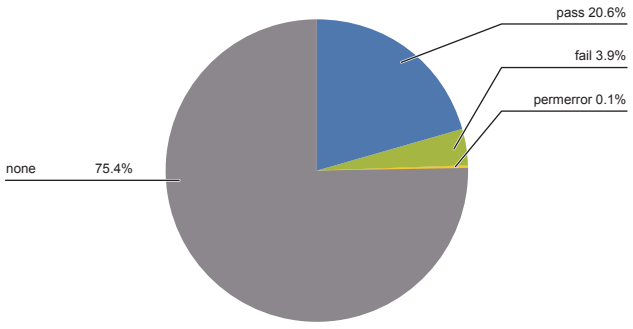

Figure 3: Breakdown of DMARC Authentication Results

almost fully deployed, and DKIM, which generally entails an implementation cost. Deploying DMARC requires either SPF or DKIM, or both, to be present, but if that requirement is satisfied, DMARC can be implemented by simply publishing a DMARC record (text resource record) on the DNS, as is done with SPF. There is no need to look at the sending email server's exit point, so DMARC records should actually be easier to configure. We still do not know whether the meagre increase in deployment relative to SPF and DKIM reflects a simple lack of recognition or administrators being unclear about the motivation for publishing a DMARC record. We intend to continue advocating for the broader deployment of DMARC ahead.

Figure 4 shows the breakdown of DMARC certification results over time, from January 2016. Rather than April 2020 being an extremely low point for DMARC, the graph instead shows that while there is a gradual increase in sender domains supporting DMARC, that growth is very slow.

Figure 5 breaks down the TLDs (top level domains) of domain names that passed DMARC authentication. The percentages are not relative to the volume of emails received; they indicate TLD counts as a proportion of the total number of separate DMARC domain names (unique domain names). The .com TLD had the largest pie piece at 53.2%. Second was .net with 9.5%, and Japan's .jp domain name was third with 6.7%. Among domain names that passed SPF authentication, .com was again the most common TLD, so there was no major difference in the rankings.

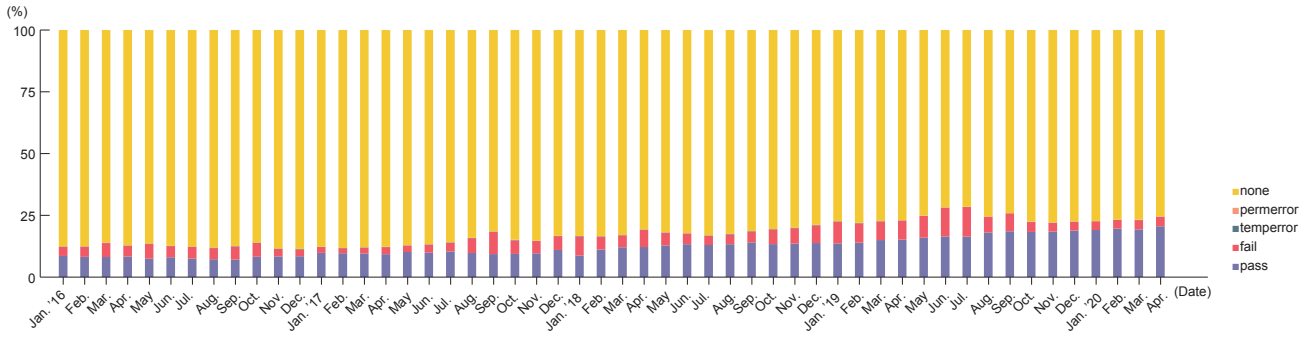

Figure 4: Breakdown of DMARC Authentication Results Over Time

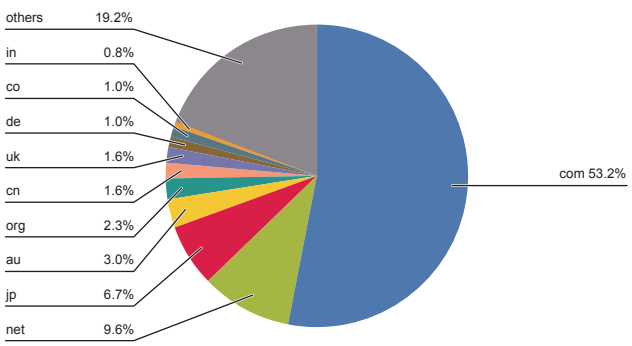

Figure 5: TLD Breakdown for DMARC Domain Names

1.2.2 Results Based on Domain Names

Another view on sender authentication technology is provided by looking at how many records for each sender authentication technology are registered for registered domain names. To do this, we have to set a scope and obtain all domain names within that scope.

As reported in IIR Vol. 39, we are studying jp domain names in collaboration with Japan Registry Services (JPRS), and we currently have a joint research agreement with Internet Association Japan (IAjapan). I am taking part in the studies as a member of IAJapan.

DKIM needs the DKIM selector name to acquire the digital signature information (DKIM record), but since the selector is specified in the email header, the domain name alone is insufficient to determine the DKIM record's location. It is sometimes possible to guess whether a DKIM record has been created[*3], but this is not always accurate. This is why only study results on the prevalence of SPF and DMARC, and not DKIM, are published[*4]. In each case, the proportions are based on domain names that have MX resource records, enabling us to determine that the domain name is used for email. There are, of course, ways of configuring SPF and DMARC records (and, recently, MX resource records too) for non-email domain names, but we'll cover the details of that another time.

Here, we report on the latest study results for SPF and DMARC. In March 2018, when our study began, SPF was on an average of 57.3% of all jp domain names. Our latest results, for May 2020, show a 7.8%pt increase to 65.1%.

Figure 6 plots DMARC deployment on jp domain names. From 0.57% in March 2018, it rose 0.62%pt to 1.19% in May 2020. So the rate doubled over roughly two years, but it was low to begin with and the increase itself was very small relative to that for SPF, so both readings were very low. By domain type, DMARC is currently most prevalent on go.jp domains, but only with a 5.4% reading. SPF has 92.4% prevalence on go.jp, so we hope to see similar efforts to drive increasing use of DMARC records on all jp domains.

1.2.3 Sender Authentication as a Measure Against Email Spoofing

Government agencies and so forth are implementing a range of measures under the current societal situation, and email communications are set to increase as part of that process. Online purchasing and the like is also on the rise as people avoid going out. As a reflection of this, fraud via phishing and email spoofing may be on the rise.

For example, emails impersonating Amazon are frequent and adopt a number of patterns, but emails from the actual Amazon support SPF, DKIM, and DMARC, so sender authentication will tell you if an email is spoofed or not. And the Amazon SPF record ends with "-all", so an SPF authentication failure always returns the strongest result of "fail". The DMARC policy is also set to the relatively strong "p=quarantine". So Amazon seems to have actively adopted sender

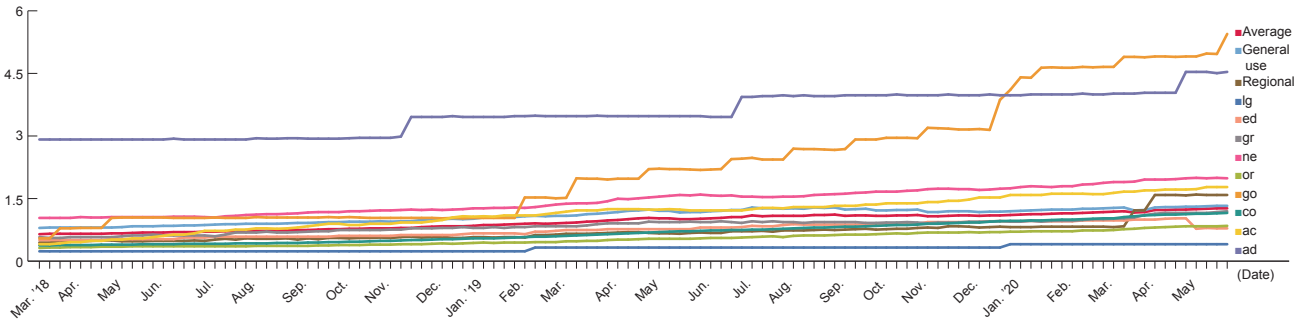

Figure 6: DMARC Deployment on jp Domain Names[*5] Over Time

*3 How to Measure Deployment Ratio of Domain Authentications (http://member.wide.ad.jp/wg/antispam/stats/measure.html.en).
*4 Anti-spam Measures | Statistical Data (https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei, in Japanese).
*5 Regional (newly registered) includes prefectural domain names.

authentication technology and bolstered defences against email spoofing. A point to note about detecting Amazon spoofing emails is the need to check that the authenticated domain name is correct. In Japan, Amazon uses the amazon.co.jp domain name. Many of the spoofed emails use completely unrelated domain names and are set up so as to pass SPF and DMARC. The Subject header and the display name in the From header contain the string "Amazon". So ensuring that the authenticated domain name is also checked is key to avoid being defrauded.

Of the jp domain name types shown in Figure 6, lg.jp, which is used by local governments and such, has consistently had the lowest DMARC deployment rate since our study began. Of course, local governments do not only use lg.jp, but the deployment rates shown indicate what proportion of domains with MX records have a DMARC record configured, and the proportion of those with an SPF record was a high 80.7%, coming in behind go.jp. So here again, to protect against spoofed emails, administrators first of all need to configure a DMARC record to protect the sender domain in the header. And to determine just how many emails are spoofing the domain, they also need to get set up to receive DMARC reports so they can constantly monitor what is happening.

1.3 JPAAWG 2nd General Meeting

The JPAAWG 2nd General Meeting (GM) took place at Bellesalle Iidabashi First on November 14–15, 2019 (Figure 7). As in 2018, it was held in conjunction with IAJapan's Anti-Spam Conference. And as with the 1st GM, IIJ was again a platinum sponsor.

In light of the 1st GM's outcomes, the following new ideas were tried at the 2nd GM.

1. Hold meeting over two days
2. Welcome many speakers and attendees from abroad, including M³AAWG members
3. Hold training sessions (paid)
4. Conduct Open Round Table discussions

Open Round Table (ORT) sessions are held at every M³AAWG General Meeting[*6], allowing participants to gather and discuss topics of interest to them. ORTs can even be the point of inception for documents like new technical specifications and Best Practices, making them one of the driving forces behind M³AAWG's activities. JPAAWG set five themes for the sessions, and JPAAWG members served as moderators to facilitate balanced discussion involving all participants. JPAAWG hopes to continue hosting activities like ORTs to provide a forum for discussing issues and thinking about solutions.

We wanted to hold the JPAAWG 3rd General Meeting in a similar format in 2020. Under present circumstances, however, a large gathering does not look all that viable. We are in the process of considering what sort of format would work, so we will provide notice on the website[*7] once a decision is made.

*6 Messaging, Mobile and Malware Anti-Abuse Working Group (https://www.m3aawg.org).
*7 Japan Anti-Abuse Working Group (JPAAWG) (https://www.jpaawg.org/).

1.4 Conclusion

I attended the JANOG45 meeting held in Sapporo over January 22–24, 2020, and made a presentation in the "Current State of Phishing and Countermeasures" session. I went because I felt it was important for a large number of people in the field to be aware that adoption of sender authentication technologies, DMARC in particular, is low, as discussed in this report. At the M³AAWG 48th General Meeting in San Francisco over February 17–20, 2020, we again held a JPAAWG BoF group meeting, and in a session titled "State of Messaging Anti-Abuse in Japan", I presented on JPAAWG's activities along with other JPAAWG/M³AAWG members.

So in 2020, we had opportunities to present both in Japan and abroad, and we were all set to continue communicating our key insights with increased vigor. But the situation took a turn, as you know, and forced a rethink of the format in which meetings are held. Yet our work is aimed at promoting the proper use of the various tools available on the Internet, so even under circumstances such as these, I think we should continue working to make communication happen and ensure that those tools are not misused.

Figure 7: Photo taken at the JPAAWG 2nd General Meeting

Shuji Sakuraba

Senior Manager, Application Service Department, Network & Cloud Division, IIJ. Mr. Sakuraba is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with related external organizations aimed at bringing about safe and secure messaging environments. He has been a member of M³AAWG since its establishment. He is the chair of the Japan Anti-Abuse Working Group (JPAAWG). He is acting chairperson of the Anti-Spam mail Promotion Council (ASPC) and a member of its administrative group, as well as chief examiner for the Technology Workgroup. He is a visiting researcher at Internet Association Japan and chairman of its Anti-Spam Measures Committee. He is a visiting researcher at JIPDEC.