Messaging Technology
The Spread of DMARC as a Spoofed Email Countermeasure

1.1 Introduction

Here we report on trends in email with a focus on spam, as well as technological trends in anti-spam measures.

Since our first volume in 2008, we have reported on trends in the ratio of spam detected in incoming email on IIJ's email services as an indicator of changes in the volume of spam. Because of the renewal of the email system this fiscal year, however, this will be our last report in the current format. Going forward, we will report in a new format whenever there are major changes or shifts.

Regarding trends in technology, we continue to discuss sender authentication technology and report on the status of its adoption. We also give an overview regarding the implementation of DMARC sender authentication technology, for which certain legal matters were sorted out last year.

1.2 Spam Trends

In this section we report on changes in the ratios of spam detected by the spam filter provided through IIJ's email services, as an indicator of spam trends. This time we examine the results of all previous surveys, covering the period from Week 23 of 2008 (the week starting June 2, 2008) to Week 52 of 2017 (the week starting December 25, 2017), which covers exactly 500 weeks (Figure 1).

The average ratio of spam for 2017 was 30.5%. The average for 2016 was 39.9%, so the 2017 figure represents a decrease of 9.4 percentage points, but in 2015 the average was 24.7%, so the ratio is not simply falling. In fact, spam continues to include many phishing emails that spoof prominent companies, and malicious spam that leads to the execution of ransomware seems to be on the rise recently.

1.2.1 Phishing Email Authentication Results

In the previous report (Vol.35), we discussed the results of using sender authentication on spam disguised to appear as though it came from Microsoft. Since then, we have continued to observe phishing emails purporting to be from high-profile companies.

The Council of Anti-Phishing Japan publishes information*[1] on phishing emails, so it is important to check whether incoming email is one of the phishing emails in recent circulation before opening URLs or HTML files within. However, the use of sender authentication technology offers an easier way to detect phishing emails. Many major companies already have implemented DMARC, enabling DMARC authentication to be used to detect the spoofing of sender information.

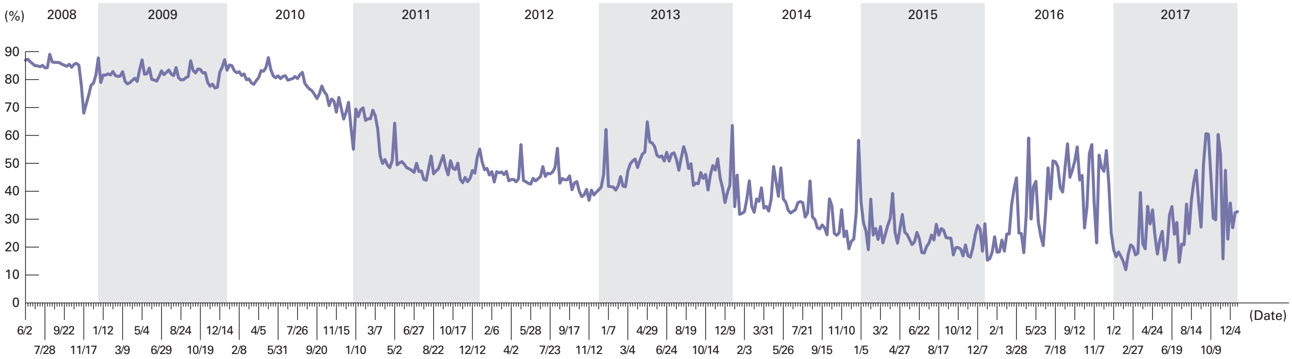


Figure 1: Spam Ratio Trends

*1 Council of Anti-Phishing Japan: Phishing-Related News (http://www.antiphishing.jp/news/alert/) (in Japanese).

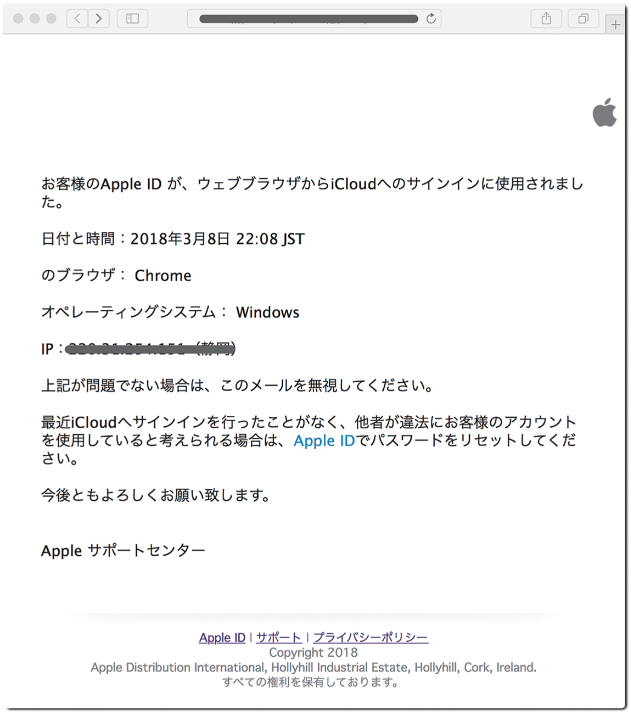
Taking Apple as an example, emails supporting SPF, DKIM, and DMARC are sent for emails related to iCloud login. Phishing emails that have been sent recently use the same email.apple.com domain name as the genuine one in the sender information (RFC5322. From) email header. Naturally, SPF fails (softfail) because the sender is different, and DMARC authentication fails (fail) due to the lack of a DKIM signature (none). Moreover, because the DMARC record policy for email.apple.com is set to reject (p=reject), emails like this will not be delivered when determining whether to receive email in accordance with DMARC specifications.

Many emails purporting to be from Rakuten Ichiba or Rakuten Card are also still being sent. Similarly, these use the rakuten.co.jp or mail.rakuten-card.co.jp domain names in the sender information header, but a DMARC record has been configured for both domain names. As a result, DMARC authentication fails in each case, so it is easy to detect spoofed email. As the implementation of DMARC sender authentication progresses, it will be possible to eliminate this kind of unwanted email. Also, when managing domain names that are easily spoofed, it is best to configure DMARC records as a countermeasure for spoofing.

1.2.2 New Email Threats

The IC3 (Internet Crime Complaint Center) of the FBI in the United States published an Internet Crime Report for 2017[*2]. The topics covered in 2017 included BEC[*3] and ransomware.

BEC is a type of fraud where email recipients are tricked into sending money using sophisticated techniques. It was reported that the IC3 received 15,690 complaints in 2017, representing a loss of over 675 million dollars.



お客様のApple ID が、ウェブブラウザからiCloudへのサインインに使用されました。

日付と時間：2018年3月8日 22:08 JST

のブラウザ： Chrome

オペレーティングシステム： Windows

IP：[redacted]

上記が問題でない場合は、このメールを無視してください。

最近iCloudへサインインを行ったことがなく、他者が違法にお客様のアカウントを使用していると考えられる場合は、Apple IDでパスワードをリセットしてください。

今後ともよろしくお願い致します。

Apple サポートセンター

Apple ID | サポート | プライバシーポリシー
Copyright 2018
Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland.
すべての権利を保有しております。

Figure 2: Email Spoofing Apple

[*2] FBI, "Latest Internet Crime Report Released" (https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718).

[*3] BEC: Business Email Compromise.

In Japan, a major airline company was also tricked by an email misrepresented as being from a business partner requesting a change of remittance account in September 2017, and they made headlines when they announced in December of the same year that this resulted in damages of over 300 million yen. Of course, most email users may think they would never be fooled by such fraudulent email. But the fact is that many have fallen victim, and according to reports these crimes are prepared meticulously using very sophisticated techniques. To avoid meeting a similar fate, it is first necessary to implement robust technological countermeasures.

The WannaCry ransomware that was big news in Japan and other countries in May 2017 is a type of malicious program (malware) in a broad sense of the term. When a ransomware infection occurs, important files are encrypted and demands are made for payment by virtual currency or other means to obtain the decryption key. There are a variety of infection vectors, but one of these includes targeted attacks, so it is crucial to implement email countermeasures as well. Unlike conventional malware business models (obtaining confidential information to sell separately on the black market etc.), this method involves new techniques where money is obtained directly from the victim by demanding payment in virtual currency, preventing the recipient from being traced.

The IC3 reports that 1,783 complaints were identified as ransomware in 2017, causing over 2.3 million dollars in damages. This year, ransomware attacks in the U.S. city of Atlanta in March also caused extensive damages[*4].

1.3 Trends in Email Technologies

Here we report on trends in the adoption and standardization of DMARC sender authentication and other related technologies. We also examine the legal handling that is important when implementing it in Japan.

1.3.1 DMARC Penetration

DMARC authentication is implemented for email received on IIJ email services. Figure 3 shows trends in the monthly average DMARC authentication results up until April 2018.

In the latest incoming email survey results for April 2018, the ratio of all email for which DMARC authentication was possible climbed to 19.3%, a record high among surveys to date. The ratio for pass authentication results was also the highest ever, at 12.2%. DMARC is still not at a level where it could be called widespread, but the number of domain names implementing it is growing at a steady rate.

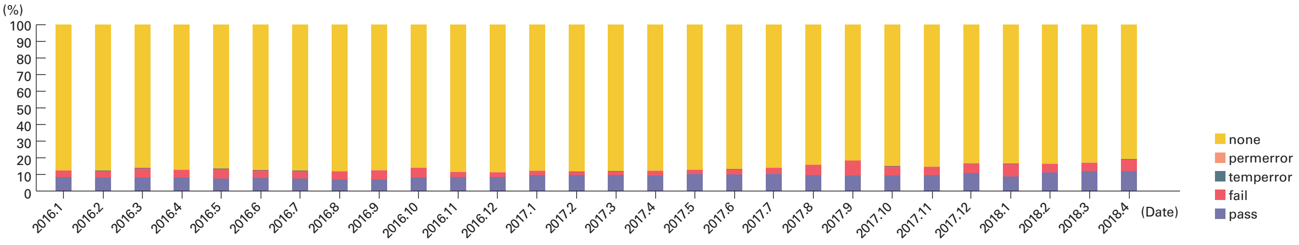


Figure 3: DMARC Authentication Result Trends

[*4] The City of Atlanta, "Ransomware Cyberattack Information" (https://www.atlantaga.gov/government/ransomware-cyberattack-information).

Next, Figure 4 shows sender authentication result combinations for April 2018, including SPF and DKIM. For example, the DMARC+SPF+DKIM data category (8.8%) indicates the ratio of email that produced a pass result for DMARC, SPF, and DKIM collectively. In other words, we found that the most prevalent combination for domain names that could be authenticated with DMARC was domains that implemented both SPF and DKIM. This is the same combination as in the previous survey (Vol.35). The authentication with the highest ratio was SPF (35.4%). Including combinations with other authentications, the total pass rate for SPF is 69.3%, and we surmise that ease of implementation is a factor in its popularity. In the latest March 2018 report data[*5] from the Ministry of Internal Affairs and Communications, the pass rate was over 90%.

Conversely, items marked "!(...)" indicate the ratio for which the authentication technology combinations listed in the brackets failed, and did not produce a single pass result. From Figure 4, we can see that "!(SPF)" by itself had the highest authentication failure rate at 6.5%. Although it is possible that the sender domain name is being spoofed, we believe that a considerable portion is email received after being forwarded, which is a case that SPF cannot authenticate properly.

Next, Figure 5 shows the ratio of domain names that could be authenticated using DMARC by TLD (Top-Level Domain). The TLD that succeeded most frequently were the ".com" domains (58.4%). Next were the ".jp" domains (7.0%), which produced results starkly different to the ".com" domains. Considering that this is incoming email in Japan, you could say the ratios are high for Australia[*6] (".au," 4th, 2.8%) and the United Kingdom[*7] (".uk," 6th, 2.1%), where implementation is being encouraged at the government agency level.

Based on volume, com shifts to 53.6% and jp to 43.4%, and these two TLDs account for the majority of DMARC domain names.

I mentioned that the implementation of DMARC is being encouraged at government agencies in Australia and the United Kingdom. The Department of Homeland Security (DHS) in the United States has also decided to enhance email and Web security at federal agencies (BOD 18-01)[*8]. This decision requires that DMARC records be configured with at minimum a "p=none" policy within 90 days. Also, a "p=reject" policy must be configured within a year. As already reported, if a "p=reject" and DMARC record policy is configured, it is more likely that the email recipient will reject messages when DMARC authentication fails. In short, to declare "p=reject", the email system, including SPF and DKIM settings, must be properly managed to prevent legitimate email from failing DMARC authentication. In this sense, it could be said that the U.S. DHS made a very important decision. We hope that the government and municipalities of Japan also look into doing this.

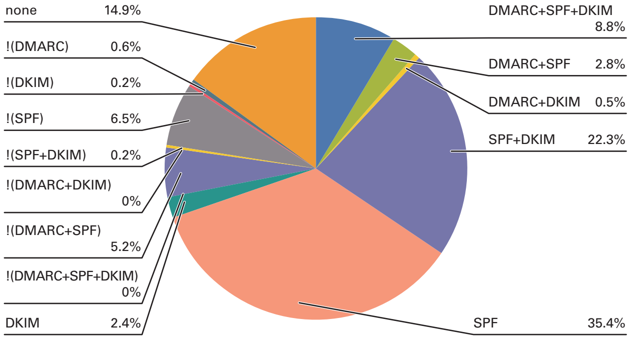


Figure 4: Sender Authentication Result Combinations (April 2018)

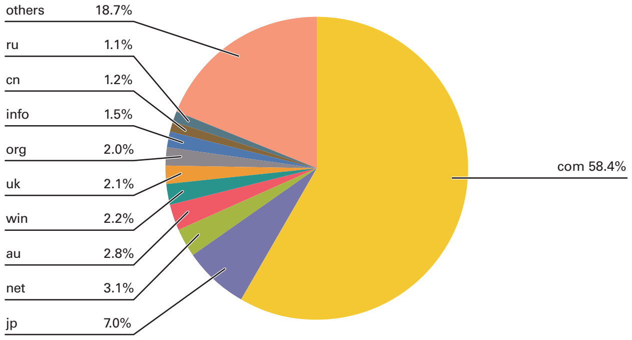


Figure 5: Ratio of Domain Names Authenticated Using DMARC by TLD

[*5] Ministry of Internal Affairs and Communications: Statistical Data (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei) (in Japanese).

[*6] DMARC, "Australian Government Agency Recommends DMARC, DKIM, and SPF" (https://dmarc.org/2016/08/australian-government-agency-recommends-dmarc-dkim-and-spf/).

[*7] DMARC, "DMARC Required For UK Government Services By October 1st" (https://dmarc.org/2016/06/dmarc-required-for-uk-government-services-by-october-1st/).

[*8] DHS, "Binding Operational Directive 18-01" (https://cyber.dhs.gov/bod/18-01/).

1.3.2 Implementation on the ".JP" Domain

Between April 2005 and May 2012, the WIDE Project entered into a joint research agreement with the Japan Registry Services (JPRS) that manages ".jp" domain names, and measured the deployment ratio of SPF and other technologies on these domains[*9]. This period coincided perfectly with the popularization of SPF, so the data proved invaluable for analogizing the degree of change and its effect.

Now the Ministry of Internal Affairs and Communications has decided to start these surveys again with DMARC added to promote its spread[*10]. As for specific methods, the Japan Data Communications Association, a subcontractor for the Ministry of Internal Affairs and Communications, will enter into a joint research agreement with JPRS. I am also taking part in these surveys as a visiting researcher for the Japan Data Communications Association.

According to the survey results published by the Ministry of Internal Affairs and Communications as of January 2018[*5] (Table 1), the SPF configuration ratio of domain names used for email was 56.9% overall. Because the deployment ratio for SPF that we were investigating in the WIDE Project was the overall ratio of SPF records configured versus the number of domains where MX records were configured, the method of calculation is slightly different from the deployment ratio mentioned above. Using the same criteria, it would be 58.1% as of January 2018. For the WIDE Project, the deployment ratio was 43.89% as of May 2012, so using the same criteria, this represents an increase of about 14.2 percentage points.

This will be the first attempt to survey the configuration of DMARC records on ".jp" domain names. Although the adoption ratio proportional to incoming email (flow rate) on IIJ's email services was 19.3%, unfortunately, the actual ratio of configured ".jp" domains averaged out to just 0.6% of the total. The first SPF survey result produced by the WIDE Project was 0.1%, so we hope this ratio continues to grow. We have mentioned the initiatives by government agencies in the United Kingdom, Australia and the United States, and hopefully use will spread among government agencies in Japan as well. SPF actually has a high adoption ratio of 92.3% on the ".go.jp" domains used by government agencies in Japan. The ".lg.jp" domains often used by local government bodies also have an adoption ratio of 75.7%, which is the second highest by attribute type.

It is easier to configure DMARC records than SPF records, which require outbound email servers to be checked, so I believe if SPF records are already set up, we should start by configuring DMARC records with a "p=none" policy.

Attribute	No. of Domains	No. MX Set	No. SPF Set	SPF Set (%)	No. DMARC Set	DMARC Set (%)
AD.JP	252	212	140	66.0	6	2.8
AC.JP	3596	3367	2086	62.0	10	0.3
CO.JP	403955	380239	252961	66.5	1089	0.3
GO.JP	582	428	395	92.3	1	0.2
OR.JP	35146	33012	21043	63.7	71	0.2
NE.JP	13044	10617	5590	52.7	99	0.9
GR.JP	6112	5438	2884	53.0	27	0.5
ED.JP	5230	4852	2854	58.8	21	0.4
LD.JP	1652	1216	921	75.7	2	0.2
Geographic/Prefecture Type	13414	7530	3959	52.6	28	0.4
General-use	988365	756800	391728	51.8	5565	0.7
Total	1471349	1203711	684561	56.9	6919	0.6

Table 1: Survey Results for Sender Authentication Technology Configuration on ".JP" Domains

[*9] WIDE Project, "Measurement Results on Deployment Ratio of Domain Authentications" (http://member.wide.ad.jp/wg/antispam/stats/index.html.en).

[*10] Ministry of Internal Affairs and Communications, "Survey on the Configuration Status of Sender Authentication Technology on '.JP' Domain Names" (http://www.soumu.go.jp./menu_news/s-news/01kiban18_01000035.html) (in Japanese).

1.3.3 Trends in Standardization Including Related Technologies

So-called technical standards on the Internet such as DMARC are published in written form by the IETF (Internet Engineering Task Force)*[11] as RFC (Request for Comments) documents. At the IETF, WGs (Working Groups) are created for each area under deliberation, and matters such as technical specifications are discussed within these WGs, ultimately leading to an RFC being issued. I attended the IETF 101 meeting held in March 2018, so here I report on recent IETF affairs and email-related circumstances.

IETF meetings are held three times a year. Generally, a venue in Europe, North America, or Asia is selected. The IETF 101 meeting was held in the European city of London. The next IETF 102 meeting is scheduled to be held in Montreal, Canada in July. It was reported that there were 1,189 attendees at the IETF 101 meeting. Conference rooms and time slots are organized in advance for each WG, and multiple WG meetings are held at the same time. Usually, each WG has a single meeting, but for WGs with many participants that are deemed to need more time for discussion, several meetings are held. Also, some WGs don't hold any meetings at all, so when you participate in an IETF meeting, you need to confirm the schedule ahead of time. Recently, more and more people have been participating online instead of attending in person. But if you have an opinion to share, it is best to be physically present at the venue.

At the IETF dmarc WG the DMARC specifications were issued as RFC 7489, and the specifications for ARC (Authenticated Received Chain) are currently being examined. Furthermore, improvements (mainly dealing with email redelivery issues etc.) to the DMARC Informational RFC that was issued are also being discussed to make it a Standards Track document, along with discussion about the information included in DMARC reports.

Other currently active WGs related to email include the dcrup WG that discusses cryptographic algorithms and additional key length for DKIM, and the jmap WG that is evaluating the new JMAP access protocol for replacing IMAP and SMTP using JSON format data.

In principle, anyone can participate in discussions at the IETF, which makes it possible to gather a wide range of opinions, but there do seem to be issues with technical specifications taking a long time to solidify. Discussions and reciprocal communication tests on email-related technology are carried out at M^{3}AAWG*[12], so it seems that RFCs are formulated comparatively quickly in this case.

*11 IETF (https://www.ietf.org).

*12 M^{3}AAWG (https://www.m3aawg.org)

1.3.4 Legal Matters

To implement SPF, DKIM, and DMARC on the recipient side, it is necessary to reference email delivery information and email body text for authentication, so as a general rule you must get permission from email users to do this. Of these, SPF and DKIM enable the detection of large quantities of spoofed emails through sender authentication, so it was determined that under certain conditions the labeling of authentication results without prior consent is a legitimate business activity and can be deemed legal*[13].

Meanwhile, with the new DMARC sender authentication technology, the domain administrator on the sending side can specify how to handle emails that fail authentication using the policy values set in the DMARC record. For example, this means if you set the policy to "p=reject", large quantities of spoofed emails are rejected and there is no need to deliver unwanted email to recipients. However, although legal matters regarding sender authentication technologies such as SPF and DKIM had been sorted out as far as the labeling of authentication results is concerned, this was not the case for processes such as DMARC where receipt is rejected.

In light of this,, we cleared up the remaining issues for implementing DMARC, including new methods for processing on the recipient side, through discussion centered around the Anti-Spam mail Promotion Council and other groups. The details have been published by the Ministry of Internal Affairs and Communications*[13]. These matters deal with recipient-side processing methods based on DMARC policies and DMARC reports. There are two types of DMARC report: aggregate reports and failure reports. For aggregate reports, comprehensive agreement means that individual consent is not required, enabling the recipient to transmit them to the sender. Failure reports, like error emails, include the details of the message that was originally sent. Consequently, it was determined that care should be taken when sending them to domain administrators that may not be party to the email communication. Therefore, when sending a failure report through comprehensive agreement, there is now a condition that it should not include the body or subject (content of the subject header) of the email that was originally sent. One of the aims of a failure report is to determine whether email that was sent actually failed authentication or is spoofed email. Even if the original outgoing email is not included in its complete form, it should be possible to determine whether it is legitimate email from other header information included in the failure report, so we believe the present limitations still provide sufficiently useful information.

We hope that clearing up these matters will help move the implementation of SPF, DKIM, and DMARC forward on the recipient side as well.

*13 Ministry of Internal Affairs and Communications, "Legal Matters Concerning the Sender Authentication, etc." (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html) (in Japanese).

1.4 Conclusion

This year (2018) marks 10 years since the Anti-Spam mail Promotion Council, in which parties interested in spam countermeasures take part, was established[14]. In 2014, LAP 10 Tokyo was held in Japan as the tenth annual meeting of LAP (London Action Plan, now UCEnet), an international government agency meeting on anti-spam measures. Also in 2014, the 10th anniversary meeting of M^{3}AAWG, in which I have participated since its establishment, was held in Boston, United States.

In times gone by, 10 years seemed like a fairly lengthy period, although not an eon by any stretch. But like dog years, time seems to move faster in the IT industry these days, and 10 years now feels rather like a rather deep expanse of time. And yet the spam situation does not seem to have improved much at all, and as someone who has been involved in this industry for many years, I feel a fair amount of responsibility for this. At the same time, however, considering that in a worst-case situation email could become unusable, I still feel like I have made a contribution of sorts. Seeing how multiple chat applications are now being used with a focus on mobile devices, I also believe that the way communication tools are used will continue to change in the future. As I am in a position to consider new mechanisms such as these, I will continue to strive to address current email issues, evaluate new ways to communicate, and work to prevent similar issues from appearing there as well.

Author:
Shuji Sakuraba
Mr. Sakuraba is a Senior Manager of the Application Service Department of the Network Division, IIJ.
He is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment.
He has been a member of M^{3}AAWG since its establishment. 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. Additionally, he is chairman of Internet Association Japan's Anti-Spam Measures Committee. He is also a member of the Email Security Conference program. Furthermore, he is a visiting researcher for the Japan Data Communications Association.

[14] Anti-Spam Consultation Center (https://www.dekyo.or.jp/soudan/contents/anti_spam/index.html) (in Japanese).