Latest Trends in Spam

2.1 Introduction

In the Messaging Technology section of the IIR, we report on email trends with a focus on spam, as well as technical information related to spam countermeasures.

The volume of spam itself has dropped dramatically compared to when this report was first published (2008), but as reported in a range of media, threats to security continue to grow. Current email systems face the challenge of finding ways to mitigate security threats, simply from the perspective of eliminating annoyance. From an attacker’s viewpoint, email is one of few routes able to deliver data into organizations that are protected in a variety of ways, so we expect it will continue to be exploited in a range of attack attempts.

In this article, we report on trends in the ratio of spam over the course of a year, as well as topics related to spam that occurred during this period. We will also discuss the trends and penetration in Japan for DMARC and related technologies, which are effective anti-spam solutions.

2.2 Spam Trends

In this section, we look at changes in spam trends, based on trends in the ratios of spam detected by the spam filter provided through IIJ’s email services.

As we have done up until now, trends in the ratio of incoming emails determined to be spam relative to the overall volume of incoming emails collated by week are shown using graphs and other means.

The graph in Figure 1 that indicates spam ratio trends incorporates 122 weeks’ worth of data, covering more than two years from 2015, including the period of more than a year since the last IIR report (Vol.31). Specifically, this covers the period from week 1 of 2015 (the week starting December 29, 2014) to week 17 of 2017 (the week starting April 24, 2017). See IIR Vol.27 and Vol.31 for information about data previous to this.

The average ratio of spam for fiscal 2016 was 38.5%. The ratio for fiscal 2015 was 24.2%, which means last fiscal year there was an increase of 14.3% over the previous fiscal year. For the past few years the ratio had been on the decline, but from last fiscal year an upward trend seems to have emerged. As shown in the graph in Figure 1, the ratio varies enormously in fiscal 2016, but it is increasing as a whole.

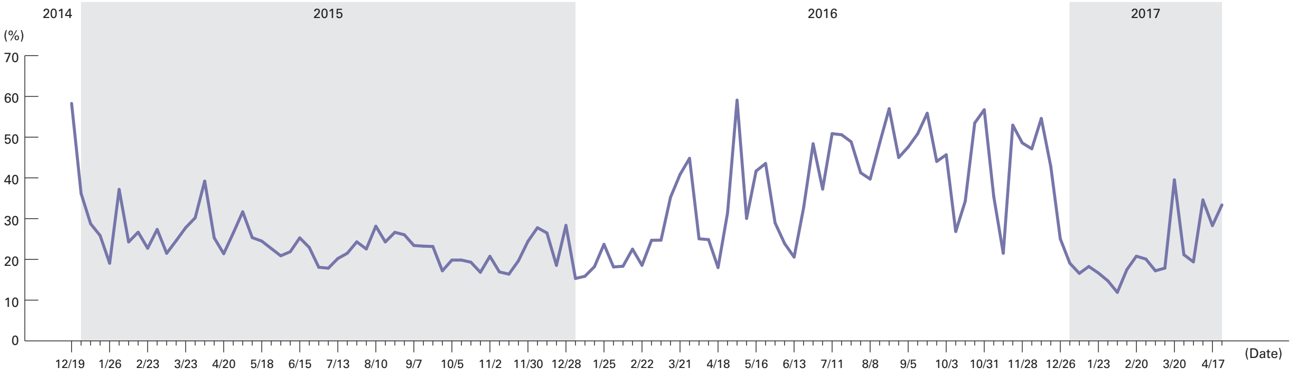


Figure 1: Spam Ratio Trends

© 2017 Internet Initiative Japan Inc.

The graph in Figure 1 indicates a sudden decrease in spam between mid-December 2016 and March 2017. A similar trend can also be seen in an article by Sophos[*1], which reported that this seems to be due to a drop in Necurs botnet activity. Later the ratio of spam began to move higher again after March 2017, so it appears this drop in botnet activity was temporary.

2.2.1 Unauthorized Use of Sender Domains

Phishing is one of the more malicious forms of spam. This is a technique for stealing important information such as IDs and passwords by tricking users into clicking URLs in spam, taking them to a fake site that imitates a genuine one where they are prompted to input these details. Recently, there have been many cleverly crafted examples such as phishing emails or fake sites written in Japanese to target Japanese users, and a National Police Agency report[*2] indicates that this is continuing to cause financial damage.

While it is important to try to prevent the receipt of phishing emails such as these, and not get caught out if they do slip through, measures for preventing the abuse of your sender information in these emails must also be considered.
Alerts were also issued frequently on the Council of Anti-Phishing Japan website[*3] and by Microsoft[*4]. Between January and March 2017 there were several incidents involving the mass sending of phishing emails disguised to appear as though they came from Microsoft. In each case the subject line (Subject: header) was written in Japanese, and just counting the emails I personally received there were the examples listed in Table 1.

These emails initially used the following domains as sender information, with the same domain used in the URL for links in the email HTML.

```
microsoft-securityprotection-support.com
support-securityprotection-microsoft.com
```

In each of these emails sent in March, a different domain was used for the sender information[*5], but a fixed URL was used for email links.

Notably, the sender domains all had “none” in the authentication results of sender authentication technology (SPF, DKIM, and DMARC). I attempted to perform basic analysis of emails that I did not receive directly, and in almost all cases the SPF authentication result was “none.” In statistical data from the Ministry of Internal Affairs and Communications[*6], the latest survey results show a “none” ratio of 9.26%, so it is possible that domains that do not support SPF were intentionally chosen for the mass emails sent in March.

Furthermore, although the emails I received were mostly transmitted from sources overseas, the TLD of the domain used was “jp” in about 80% of cases. It is possible that “jp” domains were used on purpose because the emails were written in Japanese, but we believe the fact there are this many “jp” domains that do not support SPF is an issue we will need to tackle in the future.

Date	Subject
Jan 12	ご注意！！OFFICEのプロダクトキーが不正コピーされています。
January 30	ご注意！！OFFICEのプロダクトキーが不正コピーされています。
March 17	警告！！マイクロソフトのプロダクトキーが不正コピーされている恐れがあります。
March 31	[大切]マイクロソフトのプロダクトキーが不正コピーされた警告です！

Table 1: Subject Line of Emails Spoofed to Appear from Microsoft

[*1] Global spam drops by more than half - now what? (https://nakedsecurity.sophos.com/2017/02/22/global-spam-drops-by-more-than-half-now-what/).

[*2] State of Threats in Cyberspace in 2016 (http://www.npa.go.jp/kanbou/cybersecurity/H28cyber_jousei.pdf) (in Japanese).

[*3] Phishing Posing as Microsoft (https://www.antiphishing.jp/news/alert/microsoft_20170331.html) (in Japanese).

[*4] Circulation of suspicious emails posing as from Microsoft (https://www.microsoft.com/ja-jp/office/2016/attention5.aspx) (in Japanese).

[*5] Sender information includes the From header (RFC5322.From) displayed in the MUA (mailer), as well as the From envelope (RFC5321.From) used for email delivery, and in this case the same domain was used for both.

[*6] Aggregated Sender Authentication Results (SPF) (as of December 2016) (http://www.soumu.go.jp/main_content/000468608.pdf) (in Japanese).

© 2017 Internet Initiative Japan Inc.

For example, SPF configuration is required even for domains not used for email. The "Sender Authentication Technologies Manual - Second Edition"*7 published by the Anti-Spam mail Promotion Council provides the following sample description for domains that do not send email. This configuration example will always produce a "fail" result for SPF.

```
Sample 6: Domains that do not send email

When a domain you manage will not send any emails at all,
use "-all" to advertise this.

  example.org. IN TXT "v=spf1 -all"
```

A configuration example using the details above is also proposed as Recommendation 2 in the "JEAG Recommendations - Sender Authentication" published in February 2006. Furthermore, RFC 7505*8 that was issued recently indicates methods for configuring "Null MX" records not used for email, and this includes SPF configuration examples.

Sender-side domains need to implement sender authentication technology to ensure email is delivered to recipients, but we believe it is also necessary to remember to perform configuration for protecting domains, to prevent them being abused to send spam.

2.3 Trends in Email Technologies

Here we will report on the adoption status and technological trends regarding the sender authentication technology that is also an effective spam countermeasure, with a particular focus on DMARC*9.

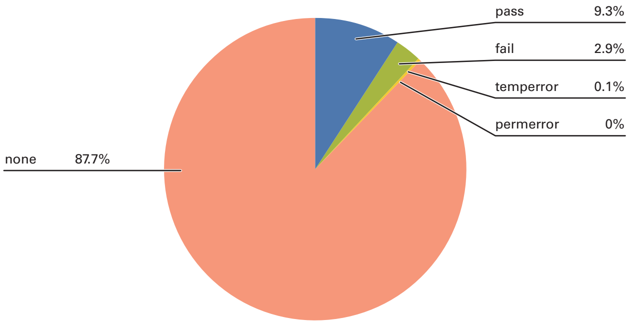


Figure 2: DMARC Authentication Result Ratios (April 2017)

DMARC is a technology based on the SPF and DKIM sender authentication technologies. It makes it possible to send and receive more legitimate emails easily by specifying recipient policies from the sender side, and enabling the receipt of recipient authentication results in report form. The adoption of DMARC is expected to spread in the coming years, in part to create this kind of environment.

2.3.1 DMARC Penetration

DMARC authentication is implemented for emails received on IIJ's email services. The graph in Figure 2 shows the latest DMARC authentication result ratios for emails received in April

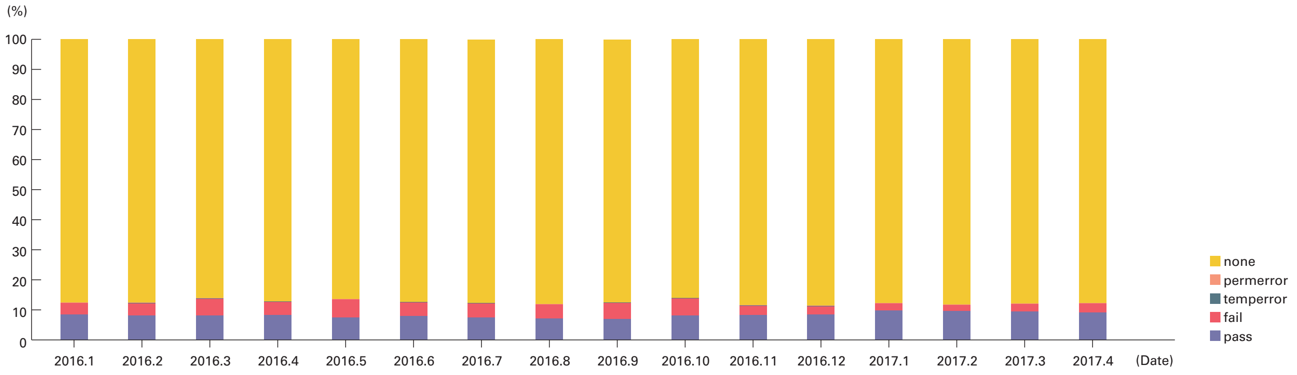


Figure 3: DMARC Authentication Result Ratio Trends

*7 Sender Authentication Technologies Manual - Second Edition (http://www.dekyo.or.jp/soudan/anti_spam/report.html#dam) (in Japanese).

*8 RFC7505: A "Null MX" No Service Resource Record for Domains That Accept No Mail (https://www.ietf.org/rfc/rfc7505.txt).

*9 Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489 (https://www.ietf.org/rfc/rfc7489.txt).

© 2017 Internet Initiative Japan Inc.

2017. The authentication results that show "none" indicate that the sender domain for emails received has not implemented DMARC. The ratio for "none" is 87.7%, which indicates that close to 90% of emails received still do not support DMARC.

Next, Figure 3 shows trends in authentication result ratios from January 2016. Unfortunately, the ratio for "none" is steady at around 87%, resulting in almost no change. If SPF and DKIM have already been implemented, DMARC can be implemented on the sender side by simply creating a DMARC record, so we believe that the low rate of authentication is due to DMARC not being well recognized in Japan.

2.3.2 Popularizing Use of DMARC

To verify the low recognition rate of DMARC, we examined combinations of authentication results for SPF, DKIM, and DMARC for emails received (Figure 4). As with Figure 1, the period examined was April 2017.

When authentication for any of these technologies produced a "pass" result, this is shown. For example, the DMARC+SPF+DKIM data category indicates that authentication produced a "pass" result for DMARC, SPF, and DKIM (a ratio of 6.7% on the graph). On the other hand, data enclosed in "!()" indicates combinations of authentication technologies that had no "pass" results, instead producing a "fail" or similar result in the authentication results. For example, the "(! SPF)" data category with a ratio of 12.5% indicates that authentication was not possible using DKIM and DMARC ("none" authentication results), and SPF alone produced a "hardfail," "softfail," or "neutral" authentication result.

In this graph, 56.5% of results showed authentication was not possible using DMARC, but possible using SPF, DKIM, or both. In other words, it demonstrates that more than half of emails received originated from senders who could perform DMARC authentication by merely creating a DMARC record, potentially enabling the DMARC penetration rate to be improved. Of course, in some cases a DMARC record may not have been created because DMARC authentication simply isn't possible, perhaps due to issues with third-party signatures. However, even in these cases there is little negative impact on the current status as long as a strong DMARC policy is not set, so we believe that the low penetration rate is affecting awareness.

It is easy to implement DMARC on the sender side. For example, to configure a DMARC record for the "iij.ad.jp" domain, create a "_dmarc" subdomain, and try using the following settings in the TXT resource record.

```
_dmarc.iij.ad.jp IN TXT "v=DMARC1; p=none"
```

If SPF or DKIM are implemented, this is all you need to do for the initial configuration. The "p=" parameter is a value indicating the processing policy that the sender requests of the recipient when authentication fails, and the values that can be set are shown in Table 2. Because "none" is a value that does not require quarantine or rejection of receipt, even if authentication fails with SPF, DKIM, DMARC, there is no adverse effect on recipients that process correctly according to DMARC specifications. This demonstrates that DMARC is easier to configure than SPF records, since it isn't necessary to examine details such as the IP address of the sender's email server.

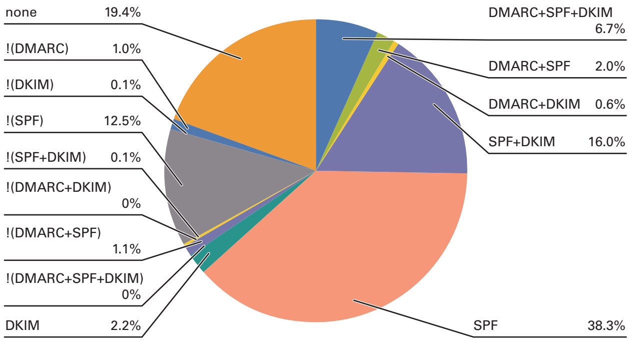


Figure 4: Sender Authentication Result Combinations (April 2017)

Furthermore, if the "rua =" and "ruf =" parameters are configured correctly, it is possible to receive reports on authentication results from email recipients that support this function. Referencing these reports enables you to do things

policy	Meaning
none	No specific processing is requested.
quarantine	Request that emails be treated as suspicious (quarantine or tag, etc.).
reject	Request that (SMTP based) receipt be rejected.

Table 2: DMARC Record Policies

that were previously not possible, such as identify the email transmission route when SPF or DKIM authentication has not been performed correctly, or learn the location and volume of email sent fraudulently in your organization’s name. This allows you to make modifications so that the delivery path of legitimate emails is authenticated correctly, and set DMARC policies such as a stronger “reject” so that spoofed emails are not delivered to the recipient.

However, the aggregate reports that can be received by specifying “rua =” are XML format data delivered as compressed MIME format emails, so some preparation is necessary to reference data. Recently, there are also services that receive these reports on your behalf and present them as visual data, so using methods like these is another option.

2.3.3 Delegation of DMARC Reports

Some configuration is required to send DMARC reports to addresses outside your own domain, or in other words to delegate the receipt of reports. This is to prevent unnecessary reports being sent to an unrelated third party by specifying them as the report recipient without permission, and sending large numbers of spoofed emails. You must configure settings to enable the DMARC report delegator and delegatee to see the relationship between each other. Specifically, when the URI indicated in the DMARC record report destination is unrelated to the domain of that record, it is necessary to perform DNS configuration on the delegatee side as shown in Figure 5.

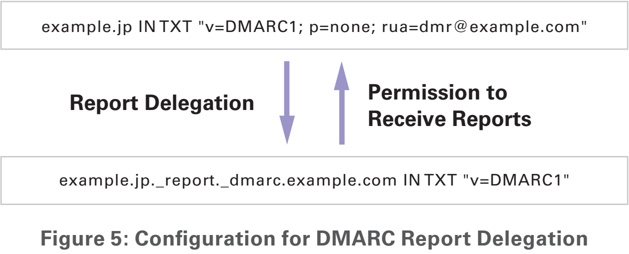
Figure 5 shows a case in which “example.com” is specified as the delegatee for the reports of “example.jp.” In this case, “v = DMARC 1” is configured in the TXT resource record at “example.jp._report._dmarc.example.com” on the “example.com” side, indicating that it will receive the DMARC reports of “example.jp.” Email recipients that send reports confirm the delegation relationship by referring to the DNS at the time of transmission.

2.3.4 DMARC Policies

One method for gauging DMARC adoption and the spread of sender authentication technology as a whole involves checking the policies configured in the DMARC record. In other words, if the ratio of domains with stronger policies set is high, we consider that there is almost no possibility of legitimate emails failing authentication. Figure 6 shows the ratio of DMARC policy declarations for each domain.

There was a high ratio of 76.4% “none” results, but the ratio for “reject” was 11.0%. The fact that over 10% of domains have the strongest policy set means that sender authentication technology is gradually spreading. It also indicates that a certain number of administrators use authentication results to avoid receiving unwanted email. We’d like to continue keeping an eye on increases in the ratio of emails that can be authenticated using DMARC, as well as the ratio of stronger DMARC policies.

Regarding “error” results, these indicate DNS errors such as when a domain cannot be referenced afterwards due to the time difference between the receipt of DMARC authenticated emails and the referencing of DMARC records for investigation. Although this represented a comparatively high ratio of 6.1%, there may be a few cases in which a domain name or its DMARC record was launched just so they were received.



```
example.jp IN TXT "v=DMARC1; p=none; rua=dmr@example.com"
```

```
example.jp._report._dmarc.example.com IN TXT "v=DMARC1"
```

Figure 5: Configuration for DMARC Report Delegation

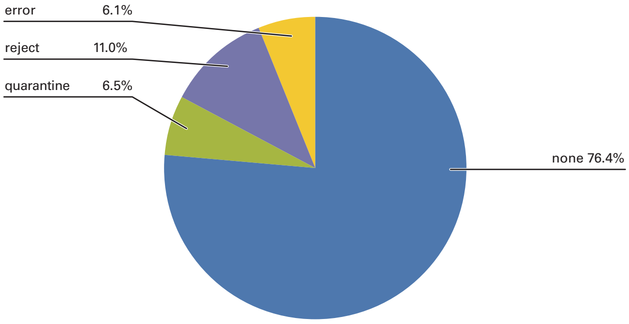


Figure 6: DMARC Policy Ratios (April 2017)

© 2017 Internet Initiative Japan Inc.

2.3.5 DNS Side Support

When configuring DMARC records, it may be necessary to deal with the parties that provide DNS services. As mentioned above, DMARC records require a "_dmarc" subdomain. A subdomain called "_report" is necessary for the delegation of DMARC reports, and "_domainkeys" is also required to implement DKIM. However, it appears there are cases in which this "_" (underscore) character cannot be used by DNS providers. For this reason, when implementing DKIM or DMARC it is necessary to check the specifications of the DNS service used for your domain.

Furthermore, in recent years email systems are used on cloud services provided by other companies more and more often. When implementing DKIM on such services, it is typical to use a third-party signature for electronic signatures, but DMARC authentication fails with third-party signatures. This is because the sender domain in the header doesn't match the domain of the cloud service that creates the signature. When you manage both domains, key management such as the configuration and updating of DKIM keys can be done with relative ease, but if each management is different, some kind of coordination will be necessary. To resolve this issue, Microsoft has demonstrated a method using the DNS CNAME record*10. However, it appears that depending on the DNS service you use, it may not be possible to use this CNAME record at all, or configure the TXT resource record to be indicated by the CNAME record. It is also necessary to confirm cloud-based email services and DNS services in advance to deal with this.

2.4 Conclusion

As we have reported several times, the issue of spam is clearly shifting from quantity to quality, and in terms of quality it is becoming more dangerous. Recently, ransomware has been a global issue, encrypting files on a PC after infection, then demanding money in exchange for the decryption key. There also continue to be incidents thought to involve infection by malicious programs (malware) that cause information leaks by stealing information stored on PCs. It goes without saying that measures to prevent infection by ransomware and malware are necessary to stop incidents like this occurring. However, such measures, including identifying the infection route, are not easy to implement.

Under these circumstances, we have developed and proposed technology for implementing a range of measures in our email systems, while maintaining the previous structure as far as possible. In particular, we believe that sender authentication technology is approaching its completed form as a countermeasure for email spoofing through DMARC. Of course, there are issues such as those surrounding indirect mailflows and third-party signatures, but methods have been identified for shoring up these systems using a certain level of technical operation or ARC (Authentication Results Chain). In Japan, there are also quite a few legal issues concerning the implementation of such technical measures. In response to these issues in the past, points of note have been put together regarding the implementation of OP25B (Outbound Port 25 Blocking), as well as the SPF and DKIM sender authentication technologies. For DMARC there are also similar challenges regarding the application of DMARC policy and the sending of DMARC reports. Discussion of issues such as these is currently centered around the Anti-Spam mail Promotion Council.

As stated in this report, DMARC is still yet to be popularized, and I believe the main reason for this is the low awareness level of DMARC itself. We strongly desire to contribute to raising such awareness through this report, and would like to see DMARC become widespread from the perspective of email security 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 M3AAWG 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.

[*10] Use DKIM to validate outbound email sent from your custom domain in Office 365 (https://technet.microsoft.com/en-us/library/mt695945(v=exchg.150).aspx).