

# 4 Messaging Technology

Previously this was published as the "Email Technical Report." From this volume we have changed the name to "Messaging Technology."

## 4.1 Introduction

Messaging Technology summarizes the latest trends in spam, technical countermeasures to spam, etc. For trends in spam, the results of a variety of analyses conducted based on various information obtained from the Spam Filter feature provided in IJ email services will be presented. Since the flow of email varies depending on the day of the week, in order to more easily understand the trends, the data was aggregated in one-week units and analyzed focusing on the changes in the data.

This survey covers a period of 13 weeks or 91 days, from the 14th week of 2009 (3/30/2009 to 4/5/2009) to the 26th week (6/22/2009 to 6/28/2009).

Regarding trends in email technologies, we explain the implementation status of sender authentication technologies on the receiving side, and examples of DKIM usage.

## 4.2 Trends in Spam

This section provides a report focused on the trends in the ratio of spam detected by the Spam Filter feature provided by IJ and analysis results related to sources of spam.

### 4.2.1 Ratio of Spam

The weekly trends in the ratio of spam over a period of 91 days from the 14th week of 2009 to the 26th week are shown in Figure 1. The ratio of spam averaged 81.6% of all incoming emails during this period. The average value was almost the same level as the previous period (81.5%), but for this period several distinct changes in the ratio trends were observed. The ratio was highest during the 19th week (5/4/2009 to 5/10/2009) at 87.1%.

Similarly to previous trends, as this period includes a series of public holidays in May, the volume of general business email was lower, and due to this the relative ratio of spam increased. However, from this period actual volumes of spam received also increased dramatically. In particular, spam increased from the 18th week (4/27/2009) to the 22nd week (5/25/2009), trending at a high ratio of over 80%.

Following this, spam entered a slight declining trend from the 23rd week (6/1/2009). During this period, the US Federal Trade Commission announced on June 4, 2009\*1 that they had shut down network access for Pricewert LLC, an ISP, which had become a hotbed of spyware, phishing, and child pornography. Pricewert also did business under the names such as 3FN and APS Telecom, and also reportedly operated servers for controlling botnets (command and control servers), similar to Mc-Colo\*2, which was shut down in November, 2008. It is believed that the shutdown of Pricewert's network weakened botnet activity, and reduced spam volume. However, as a dramatic decrease of the magnitude of the McColo case\*3 was not observed, it

is conceivable that either the affected botnets were of a small scale, or the sender had knowledge of the shutdown in advance, and took some form of remedial measures.

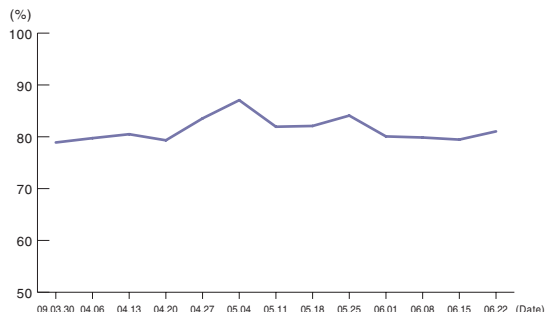


Figure 1: Ratio Proportion of Spam

\*1 <http://www.ftc.gov/opa/2009/06/3fn.shtm>.

\*2 Explanation in IIR Vol.2 ([http://www.ij.ad.jp/development/iir/pdf/iir\\_vol02\\_mail.pdf](http://www.ij.ad.jp/development/iir/pdf/iir_vol02_mail.pdf)).

\*3 In the 47th week of 2008 (11/17 to 11/23), the ratio of spam dropped to 68%.

### 4.2.2 Sources of Spam

Figure 2 shows the source countries of spam during this period.

In this survey, as in the previous one, the top source of spam was Brazil (BR), accounting for 11.8% of the total. This is a slight increase over the previous survey, in which Brazil accounted for 11.3% of total spam. The United States ranked 2nd (US) at 11.4%, the same ranking it held for the previous survey (Vol.3, 10.9%), and the survey before that (Vol.2, 14.4%).

In the current survey results, the gap between the top two countries and those ranked 3rd and below increased slightly. China ranked 3rd (CN, 6.9%), South Korea 4th (KR, 5.6%), Turkey 5th (TR, 5.4%), and India 6th (IN, 5.3%). Comparing these results with those from the previous survey, there are a few changes in ranking, but the top six countries remain the same. Japan (JP, 2.6%) was ranked 11th, the same ranking it held in the previous survey.

The weekly trends in the ratio of spam from these 6 countries and Japan are shown in Figure 3. Brazil maintains a high ratio each week, but we can see that the ratio for the United States drops after mid-May. The ratio of spam from China has dropped slightly since it ranked in 1st place in the survey before last (Vol.2), but it has been gradually returning to a high level since June, so caution is once again required.

As the majority of spam sent to Japan is sent from overseas, we believe that the international coordination of anti-spam measures is essential.

### 4.2.3 International Anti-Spam Measure Trends

As can be seen from the data we have presented, high volumes of spam are still being sent. The same trend can be seen both in Japan and internationally. It is said that the source of most spam is bots that infect Consumer PCs with malware, and control them from outside the network.

Japan has constructed an environment that prevents spam being sent using bots such as these through the widespread implementation of OP25B<sup>\*4</sup>, which restricts the sending of email directly to external networks from dynamic IP addresses. Japan is not the first country to introduce OP25B technology, as some ISPs including major ones in the United States have already introduced it. After the establishment of the MAAWG<sup>\*5</sup> group for combating international spam, OP25B received attention as an effective technology for defending against senders of spam. After intensive discussions, Japan's JEAG<sup>\*6</sup> published a recommendation for OP25B<sup>\*7</sup>, and due to this it was rapidly adopted in Japan.

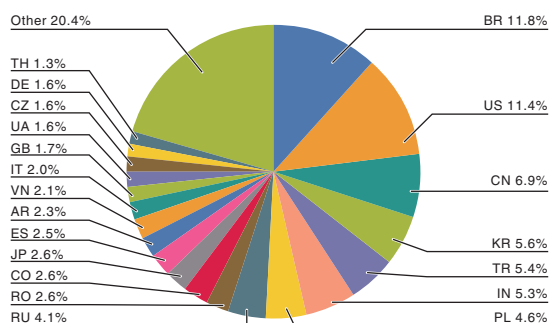


Figure 2: Sources of Spam

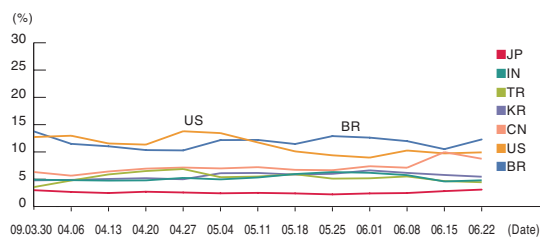


Figure 3: Trends in Sources of Spam

\*4 Outbound Port 25 Blocking

\*5 See Internet Topics for more information about MAAWG (Messaging Anti-Abuse Working Group).

\*6 JEAG (Japan Email Anti-Abuse Group) is a working group founded by Japan's major Internet service providers (ISPs) and mobile telecommunication carriers to counter spam email abuse (<http://www.ij.ad.jp/en/news/pressrelease/2005/0315.html>).

\*7 See "The Japan Email Anti-Abuse Group (JEAG) Drafts Recommendations on the Fight against Spam E-mail" at the following URL. (<http://www.ij.ad.jp/en/news/pressrelease/2006/0223.html>).

It should be possible to reduce the volume of spam that Japan receives from overseas through the adoption of OP25B in wider areas. For this reason, IJ has continued its efforts to accelerate the introduction of OP25B, advocating its effectiveness and presenting a technological overview of it to other countries through opportunities such as MAAWG international conferences and activities in coordination with the government. OP25B has been introduced in some areas as a result, but in many areas progress towards its introduction is faltering for a number of reasons. We will explain the details of this on another occasion, and we plan to continue pushing for the introduction of OP25B.

Regarding trends in countermeasures against senders of spam, moves to shut down networks thought to be controlling botnets continue in the United States, as evidenced by the network shutdown of McColo in November, 2008, and Pricewert in June, 2009. Shutting down communications from the control source that sends commands to bots certainly has a greater temporary impact than disinfecting each bot individually. However, there is a possibility that the controllers of botnets that send spam have implemented countermeasures of their own, and have already introduced new technology, as the impact of Pricewert's recent shutdown seemed to be limited. There have already been reports<sup>\*8</sup> of the existence of new botnets that transmit commands using peer-to-peer technology, with no specific control source. As long as the sending of spam remains a viable business practice, it is conceivable that this kind of innovation of sending methods will continue.

Recently, some telecommunications carriers have introduced a technique called Walled Garden<sup>\*9</sup> as a countermeasure against the senders of spam. Walled Garden is a technique for isolating communications from users thought to be sending spam in a specific location, instead of passing them through to the Internet directly. This makes it possible to analyze bot behavior, and implement security measures by alerting general users who are unintentionally carrying out unauthorized communications because of a malware infection. For example, by guiding all Web access (HTTP/HTTPS) to a specific page, it is possible to suggest the use of Windows Update or the execution of anti-virus software, and prevent the PC from connecting to the Internet until it is cleaned. However, there are many issues with the Walled Garden technique, such as the identification of sources that are behaving suspiciously, and the preparation of a system for responding to inquiries from users who have been guided to Walled Garden.

OP25B can suppress the sending of spam, but it cannot respond to DDoS attacks that use bots, for example. Recently, there have been incidents of government-related Websites in the United States and South Korea becoming inaccessible, and reports suggest that botnets were responsible for these attacks. Because of this, we believe that the introduction of OP25B is not enough, and that efforts to maintain a clean network environment by combining OP25B with the Walled Garden technique are necessary.

---

\*8 HotBots'07 (<http://www.usenix.org/events/hotbots07/tech/>).

\*9 MAAWG has published their best practices for Walled Garden ([http://www.maawg.org/about/whitepapers/MAAWG\\_Walled\\_Garden\\_BP\\_2007-09.pdf](http://www.maawg.org/about/whitepapers/MAAWG_Walled_Garden_BP_2007-09.pdf)).

## 4.3 Trends in Email Technologies

### 4.3.1 Trends in Sender Authentication Technologies

The WIDE project survey results\*<sup>10</sup> that we have also cited several times in the past provide insight into the implementation status of sender authentication technologies on the sending side for the Japan domain (“jp” domain). These results allow us to confirm the implementation ratio on the sending side, and in particular the high rate of publication of SPF records (3.99% as of August, 2009). Meanwhile, let us look at how the implementation of sender authentication technologies is progressing on the email receiving side.

The Japan Data Communications Association has carried out a survey of sender authentication technology implementation status, targeted at businesses such as ISPs and mobile telecommunication carriers that provide email services to a wide range of consumers, and published the results\*<sup>11</sup>. According to the survey results, as of July 2, 2009, 13 of the 41 companies that participated in the survey were carrying out receiving-side authentication using SPF (Sender Policy Framework) or SenderID. This comes to a ratio of approximately 31.7%, or an even lower penetration rate of approximately 22.6% when data is limited to ISPs. The implementation ratio of DKIM on the receiving side was lower still, at approximately 14.6%.

Many enterprises did not participate in this survey, and the volume of email and number of accounts handled by each participant vary, so this is not a straightforward indication of the penetration rate of sender authentication technologies. However, given that this survey was targeted at telecommunications carriers, our honest impression is that these numbers are lower than they should be. New functions must be added in order to carry out authentication on the receiving side, so a clear-cut comparison cannot be made, but the results compare extremely unfavorably with the high penetration rates seen on the sending side. We believe that to accelerate implementation on the receiving side there is a need to further clarify the effects and benefits of implementation.

### 4.3.2 About DKIM Usage

In our last report we gave an overview of the DKIM authentication structure and processing on the sending and receiving sides. This time, we will explain the benefits and practical applications of DKIM.

DKIM authenticates the sender of an email by attaching a digital signature that cannot be created unless the sender has the private key. The digital signature is created from the email body and headers, so as long as the source information is not changed, verification is possible at any time provided that the public key for verifying the signature can be obtained. This means that unlike network-based SPF/SenderID, there is no chance of authentication failing due to email being forwarded. This is a significant advantage of DKIM.

Conversely, one case in which DKIM authentication fails is when a mailing list name or counter is added to the Subject header in a mailing list. The addition of strings such as this constitutes modification of the email, so the digital signature does not match, and authentication fails. This is often brought up as one of the disadvantages of DKIM.

However, currently most mailing lists already add information to the Subject header and change sender information in advance, making them a system for redelivering email to mailing list members, rather than simply a way to process the forwarding of email. In other words, mailing list systems become the sender of email to be delivered, and from the perspective of DKIM, we believe that signatures should be attached on the mailing list system side to begin with. For this reason, we recommend avoiding the issue of DKIM authentication failing due to mailing lists by creating digital signatures at the time of delivery.

\*<sup>10</sup> Survey Results on Deployment Ratio of Sender Authentication Technologies published by WIDE (<http://member.wide.ad.jp/wg/antispam/stats/index.html.en>).

\*<sup>11</sup> Sender Authentication Implementation Status (<http://www.dekyo.or.jp/soudan/auth/>).

There is another benefit of making DKIM digital signature authentication possible from the email body alone. For example, when the sender of a mail magazine receives feedback such as subscription cancelations or suggestions for improvement, they will generally want to confirm that the user is the recipient of the mail magazine. In this case, if the sender of the mail magazine attaches a DKIM digital signature at the time of delivery, users sending feedback can attach the email that was originally sent to reauthenticate the attached email, making it possible to confirm whether or not they really sent the email. Additionally, IETF has published ARF (Abuse Reporting Format), which can also be used as a format for feedback such as this, as an Internet Draft, and its standardization is being discussed. (Figure 4)

#### 4.4 Conclusion

In this volume's Messaging Technology, we introduced recent trends in countermeasures against senders of spam, such as countermeasures against controllers of botnets, and the Walled Garden technique that is gaining momentum as a defense against spam senders alongside OP25B. The sending of spam is a business for those who send it, and they are innovating technology on a daily basis to devise new ways of ensuring their spam is delivered. Comprehensive countermeasures that encapsulate the sending and receiving of email and best practices for network management are becoming necessary. We will continue to introduce such countermeasure technologies in this whitepaper in the future.

We are faced with the fact that, compared with SPF/Sender ID that only requires an SPF record to be set and published one time, implementation of DKIM is not progressing very rapidly. It is conceivable that cost-effectiveness is one of the factors behind this, so we would like to continue to promote the implementation of DKIM by introducing its merits and utilization methods.

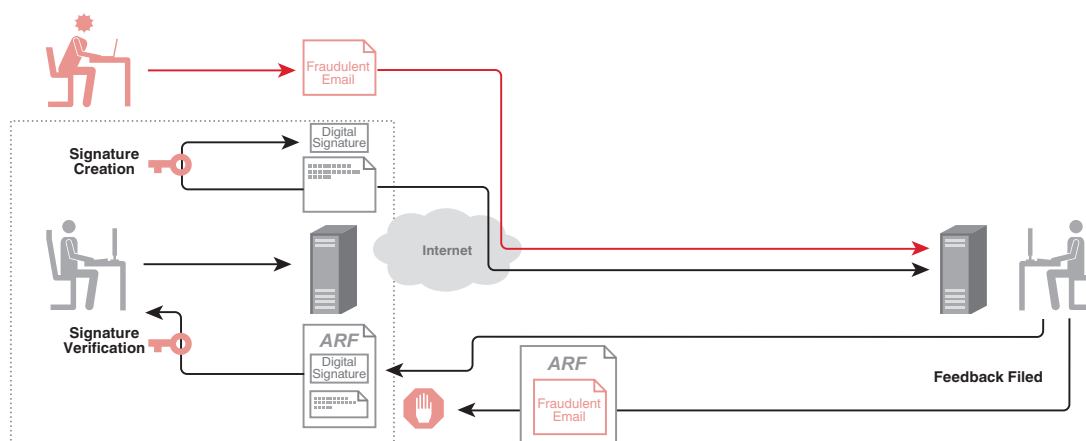


Figure 4: Example of Using DKIM with ARF

Author:

**Shuji Sakuraba**

Shuji Sakuraba is a Senior Program Manager in the Service Promotion Section of the Messaging Service Division in IJ Network Service Department. He is engaged in the research and development of messaging systems. He is involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He is a MAAWG member and JEAG board member. He is a member of the Council for Promotion of Anti-Spam Measures and administrative group. He is also a member of Internet Association Japan's Anti-Spam Measures Committee.

## Internet Topics: Messaging Anti-Abuse Working Group

### ■ About MAAWG

With global spam on the increase, IJ was among the 19 international telecommunications carriers and ISPs who established MAAWG (Messaging Anti-Abuse Working Group)\*<sup>1</sup> on January 19, 2004\*<sup>2</sup>. As a founding member of MAAWG, IJ has participated in MAAWG activities for the past five years. Here we will introduce the details of MAAWG activities and present a summary of the 16th General Meeting held in June, 2009.

MAAWG members include a variety of companies involved with email, such as major ISPs, ESPs (Email Service Providers), and email delivery contractors and vendors. As of the end of 2008, the number of members has risen to 161 companies. The main activities of MAAWG involve countermeasures against the unauthorized use of email to spread spam and viruses. In recent years, however, many issues such as countermeasures against botnets that are the source of such problems and the malware (unauthorized programs) behind these botnets have also become topics of discussion. As a result of its activities, MAAWG has published a variety of documents such as recommendations, best practices, and whitepapers. These are also made available to non-members, and can be obtained from the MAAWG Website.

A wide variety of companies involved with email currently participate as MAAWG members. Members participate in discussions covering a number of fields, such as the Technical Committee for discussing technical matters, the Collaboration Committee for discussing operational issues, and the Public Policy Committee that carries out activities such as coordination with law enforcement agencies and international organizations. Another characteristic of MAAWG is the variety of discussions that are held based on a specific theme or on the role of participants, such as the Senders SIG for sender organizations or the ISP Closed Colloquium for which participation is limited to ISPs.

MAAWG members meet face-to-face at the General Meeting that is held three times each year, but in addition to this also share information and opinions on published documents on an everyday basis using a mailing list. An Abuse Contact Database has also been created so that members can contact each other directly, and this contributes to improving the international email environment through its use to confirm status when the transmission of email between ISPs is not going smoothly.

### ■ 16th MAAWG General Meeting

The General Meeting is a precious opportunity for MAAWG members to meet each other face-to-face. In recent years they have been held around February and October in North America, and in June in Europe. Here we will present the details of the 16th General Meeting held in Amsterdam in the Netherlands from June 8 to June 11.

When MAAWG was established there were open sessions in which anyone could participate, but currently only MAAWG members and invited guests can participate in the meeting. As making details of the meeting public is prohibited, we cannot discuss the details of each session, but we will present a summary.

The meeting held in Europe, partly due to it being the headquarters of international organizations such as the ITU and the OECD, tends to be higher participation from those involved in government. A large number of organizations were in attendance at this meeting, such as the Council of Europe and Europol, the United States FTC and the Netherlands OPTA (Independent Postal and Telecommunication Authority), with each presenting information about the initiatives they are undertaking. This year there was a record number of attendees for the meeting held in Europe, with over 270 individuals from 19 countries participating, demonstrating the high level of interest and also the seriousness of the issues faced in this field.

The General Meeting is normally held over three days, with sessions on a variety of topics continuing from 8:30 A.M. to 6:00 P.M. Most sessions are related to email, and as multiple sessions are held concurrently, participants spend most of the day cooped up in the hotel that serves as the meeting place. Social events are also held to cultivate friendships between members, and this is an opportunity to meet out of the hotel and discuss solutions to everyday problems and for collaborations between companies.

JEAG (Japan Email Anti-Abuse Group)\*<sup>3</sup>, which counters spam e-mail abuse in Japan, was founded after the establishment of MAAWG. JEAG also coordinates with MAAWG, with JEAG members participating in MAAWG General Meetings as guests, and introducing JEAG's activities and initiatives in Japan. As a founding member of both, IJ will continue to be extremely active, serving as a bridge between Japan and international organizations.

Author:

**Shuji Sakuraba**

Shuji Sakuraba is a Senior Program Manager in the Service Promotion Section of the Messaging Service Division in IJ Network Service Department.



\*1 <http://www.maawg.org/>

\*2 <http://www.ij.ad.jp/news/pressrelease/2004/0119.html>

\*3 <http://www.jeag.jp/>