Email Security in the Modern Age
—Password-protected ZIPs and DMARC Sender Authentication

1.1 Introduction

We reported on trends in spam and virus numbers in the periodic observation report in IIR Vol. 51 last June (https://www.iij.ad.jp/en/dev/iir/051.html). Two points to note in that context are that, at the time, we had received up to 200 times the amount of spam received in the previous year, and that the virus Emotet was encrypting itself in ZIP files to avoid virus scans and thus running rampant.

In this issue, we look at two security enhancements IIJ has undertaken to protect itself from such threats. One is to eliminate the use of encrypted ZIP files, and the other is to tighten up DMARC. We would like to see all readers do the same and hope this article will be helpful in that regard.

1.2 IIJ Blocks Encrypted ZIP Files

1.2.1 Background to Blocking Encrypted ZIP File

IIJ changed its company-wide policies to, as a general rule, block encrypted ZIP files attached to emails as of January 26, 2022[*1].

A common practice in Japan when attaching files to emails is to encrypt them in a password-protected ZIP file and send the password to that file in a separate email as a way of preventing files from being missent[*2]. But not only is this largely ineffective in preventing information from being missent, it also has the fatal flaw of circumventing virus scans, and CISA (the US's Cybersecurity and Infrastructure Security Agency) recommends blocking the receipt of such files for this reason[*3].

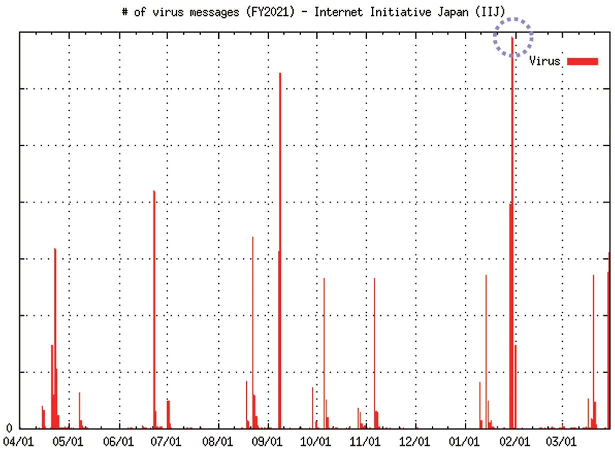


Figure 1: Viruses Arriving at IIJ Honeypots (April 2021 – March 2022)

And as mentioned, the quite rampant virus Emotet uses this method, and we can expect other viruses that do the same to appear in the future. To protect not only IIJ's internal data but also the important data our customers and business partners entrust us with, we made a management decision to not leave this risk unchecked, in accord with which we have been implementing a top-down response.

1.2.2 Preparing to eliminate encrypted ZIP files

This change of policy proceeded as follows.

- Information Systems Department explained the situation to the Risk Management Office and management
- Management explained the risks and outlined its plans internally
- Information Systems Department began working on steps to implement countermeasures
- Risk Management Office worked on a unified set of rules
- Explanation provided to internal departments and schedule mapped out
- Explanation provided to customers and business partners
- Policy changed

It took about a year from when management outlined its plans until the final change of policy took place. Our careful preparations have meant that we have experienced no major disruptions in the six months or so since.

1.2.3 Effect of Eliminating Encrypted ZIP Files

Coincidentally, the weekend following the day on which we began blocking encrypted ZIP files brought confirmation that Emotet, which was supposed to have been taken down, had made a comeback. It also appeared prominently at the end of January in IIJ's honeypots, as Figure 1 shows. IIJ's setup blocks the virus at the gateway so it is never received, and we thus had early confirmation of this being highly effective. Our internal network was thus kept safe.

[*1] IIJ's press release: "Changes to our operations regarding password protected .zip files sent as an attachment followed by a separate email containing the password (PPAP)" (https://www.iij.ad.jp/en/ppap/).

[*2] A practice also known as PPAP in Japan.

[*3] CISA, "Emotet Malware" (https://www.cisa.gov/uscert/ncas/alerts/aa20-280a).

The lead up to implementing this series of policy shifts involved coordinating among a diverse range of internal stakeholders, including Risk Management, Information Systems, Sales, and Public Relations. Overhauling long-standing methods can be painful at times, but putting off responses to risks will solve nothing. We recommend taking swift action before serious incidents occur.

1.2.4 Are There Alternatives?

The topic of alternatives goes hand in hand with discussion about abandoning encrypted ZIP files. As we discussed in IIR Vol. 51, any alternative will have its pros and cons.

IIJ understands this well and accordingly offers three ways of sharing files with external parties.

The first is company-wide shared online storage, and this is probably the most orthodox method discussed as an alternative. It has its risks, however. An internal control-related drawback to archiving emails in online storage is that it can be difficult to trace the files later, and it may also confound efforts to detect insider crime because large amounts of files can be exfiltrated via a single URL.

The second is to send attachments as is. Encrypted ZIP files are not very effective in the case of missent emails, and they circumvent virus scans, so one may conclude that simply sending the files as is would be fine. In the case of some business partners, external Web access from within the recipient’s company systems is not permitted, so sending the files directly is an option in those cases.

The third is to continue using the traditional encrypted ZIP method. This constitutes an exception. Email interactions involve both the sending and receiving of emails, so there are still cases in which some organizations and business partners have no choice but to use the old method. We enable exceptions in such cases, subject to a full understanding of the risks and approval by the relevant organizational heads.

Combining these three methods with an email audit system serves to ameliorate the drawbacks of each (Table 1).

To reiterate, blocking encrypted ZIP files across the board will mean you are no longer exposed to viruses such as Emotet. And even while this work is being done, attackers will be aiming at their next target. Changing company-wide policies can take time, so we recommend you begin working on a response right away.

1.3 IIJ Tightens DMARC Policy

1.3.1 Background to Tightening of DMARC Policy

IIJ introduced its DMARC policy in 2013, and for some time used p=none, which is a declaration to external domains that nothing should be done about emails that fail DMARC authentication. Even with p=none, it is possible to publish a DMARC record and receive DMARC reports. Aggregating the statistical data in those reports makes it possible to detect email spoofing, which is useful in terms of protecting your domain’s brand. The IIJ Secure MX Service, a SaaS offering, also provides users with the ability to automatically aggregate DMARC reports and review the statistical data.

	Advantages	Risks/Problems	+	Email audit system
1. Use online storage	• Virus scanning can be done on the storage side of things • Can be effective against information being missent in some cases • Can send and receive large files	• File tracking/tracing is difficult, which is a drawback for internal control • Difficult to detect internal crimes where files are exfiltrated		
2. Send files attached as is	• Virus scanning can be done on the gateway • No additional equipment or investment required • Applicable to any environment, regardless of who the recipient is	• No countermeasures against information being missent		
3. Conventional encrypted ZIP method (exception granted)	• No need to change conventions	• Avoids virus scans, so is unprotected and risky • Emails are rejected by some recipient systems • Cumbersome, requires effort on the receiving end • Hinders operational streamlining and automation		

Table 1: Typical Advantages and Risks of Alternatives

Phishing emails and sender-spoofing emails that cleverly evade spam filters have become common in recent years, necessitating a multifaceted approach to the various email threats out there. As a provider of corporate email security SaaS, IIJ made the decision to change its policy to p＝quarantine to strengthen internal email security.

1.3.2 Sender Authentication

Before discussing IIJ's implementation of DMARC, we will first review sender authentication technology. SPF, DKIM, and DMARC are widely used for sender authentication across the globe, with each being defined by an RFC (Table 2).

Table 3 shows the three available DMARC policies. It is important to note that a DMARC policy is merely a request from the sender asking email recipients to treat emails in a certain way. The receiving system will not necessarily handle emails as requested. A DMARC policy has no effect unless the email analysis system on the receiving end has functionality or filters for performing DMARC validation, but the point is that companies can demonstrate the validity of their domain by declaring a DMARC policy to the outside world.

Until fairly recently, the email filtering process had been left up to recipients, but with DMARC policies, we now have a revolutionary framework for email filtering that lets senders ask recipients to treat emails that fail DMARC authentication in a certain way.

1.3.3 Preparing to Implement Sender Authentication

To change your DMARC policy, you simply change your DMARC record, but your SPF record must be published and your DKIM signature implemented before doing so. A DMARC policy evaluates whether email is valid based on SPF and DKIM, so the point is to not create a situation in which your employees send out non-sender-authenticated email.

The following preparations are key here.

(1) Ensure employees are aware that company emails should only ever be sent from company email addresses (and the company email system)
(2) Consolidate email exit points to reduce the cost of implementing sender authentication
(3) (After implementing a DMARC policy) Regularly check the DMARC reports

Let's look at these three steps in detail.

■ (1) Employee awareness

At IIJ, several types of emails are sent out from the iij.ad.jp domain.

- Business emails sent by IIJ employees
- Notification emails sent out by system devices
- Announcements sent to customers

p=	When dmarc=fail, the recipient is asked to
none	do nothing
quarantine	quarantine the email
reject	reject the email

Table 3: DMARC Policies

Sender authentication	RFC	Overview
SPF	7208[*1]	By publishing an SPF record, administrators can declare to external parties that email sent from the IP addresses listed in the record is legitimate.
DKIM	6376[*2]	Electronically signing an email makes it possible to verify whether the content of the email has been tampered with.
DMARC	7489[*3]	Senders specify how recipients should handle emails that fail SPF or DKIM authentication.

[*1] https://datatracker.ietf.org/doc/rfc7208
[*2] https://datatracker.ietf.org/doc/rfc6376
[*3] https://datatracker.ietf.org/doc/rfc7489

Table 2: Characteristics of Sender Authentication

Previously, employees sent business emails out from various different internal servers. This was addressed by having the Information Systems Department manage the internal email system exit points and, ultimately, enacting a policy prohibiting employees from sending out emails using @iij.ad.jp other than from the internal email system, continuously monitoring transmissions sent from inside the company out onto the Internet, and sending notifications to users who violate the policy telling them to discontinue that behavior.

There were also problems with the emails being sent from the various internal systems. At IIJ, a number of services are operated by different departments, and email alerts and notifications were being sent out from all over the place. Currently, the department that controls each service sets up a unified exit point for all emails sent out by the service.

In addition, some group companies and regional offices had devices set up to send out email alerts using iij.ad.jp as the sender address, so we notified the people responsible for those devices and asked them to follow the IIJ policy.

(2) Consolidation of email exit points

As noted above, the consolidation of email exit points is an important consideration in performing sender authentication.

In SPF records, email source IP addresses can be given in CIDR notation, so you can keep records from becoming verbose by masking off the email exit points using a /32 or /31 prefix, or possibly by going as wide as /28 or so, and this also allows you to reduce operating costs when adding or changing exit points. When there are a number of IP addresses from which email can be emitted, repeatedly using the “include” mechanism can hamper the SPF evaluation process or cause it to fail unintentionally because information has been left out (note that RFC 7208 limits the number of DNS lookups resulting from “include”terms in an SPF record to 10).

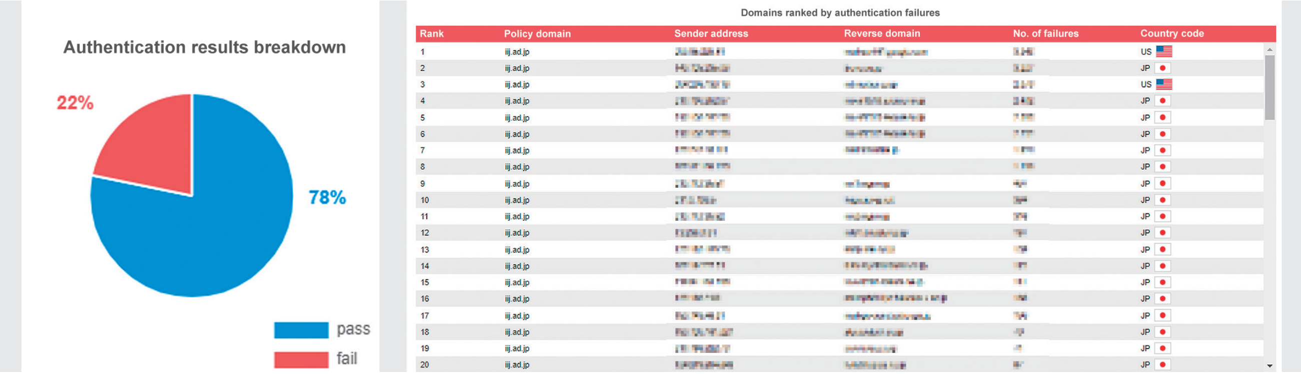
(3) Regularly checking DMARC reports

IIJ receives DMARC reports (rua) from all over the place. That is, we regularly receive reports from a range of organizations informing us of the results of sender authentication on emails their systems have received from @iij.ad.jp. Since we control the email exit points, we can basically assume that any emails not actually coming from those exit points are spam, but we have observed some cases in which this was not true, and based on this information we have been gradually asking the relevant business units to update their policies.

- Alert emails
  There were cases in which SPF/DMARC was failing because the envelope from address in network devices, server monitoring systems, and the like had been arbitrarily set to iij.ad.jp.
- Promotional and recruiting emails
  These often use external SaaS offerings, and in some cases the envelope from address in the system had been set to iij.ad.jp and emails sent out with no consideration given to sender authentication.

1.3.4 Decision to Change DMARC Policy

The DMARC policy can also be progressively tightened to “quarantine” or “reject”. IIJ decided to implement a p = quarantine DMARC policy because it still allows emails to be received even if the recipient filters them according to the DMARC policy.



Domains ranked by authentication failures

Rank	Policy domain	Sender address	Reverse domain	No. of failures	Country code
1	iij.ad.jp	[redacted]	[redacted]	[redacted]	US 🇺🇸
2	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
3	iij.ad.jp	[redacted]	[redacted]	[redacted]	US 🇺🇸
4	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
5	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
6	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
7	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
8	iij.ad.jp	[redacted]		[redacted]	JP 🇯🇵
9	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
10	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
11	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
12	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
13	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
14	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
15	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
16	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
17	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
18	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
19	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵
20	iij.ad.jp	[redacted]	[redacted]	[redacted]	JP 🇯🇵

Figure 2: February 2022 DMARC Report Summary for iij.aj.jp
Authentication Results Breakdown (left), Top 20 Domains for Authentication Failures (right)

■ Actual procedure

The procedure itself is very simple: you simply overwrite your DMARC record from p=none to p=quarantine. We omit the details here, but before doing the overwrite, you need to have an SPF record published and a DKIM signature implemented.

It takes a mere 10 minutes, even counting the time taken to confirm the record after it has been overwritten (Figure 3).

Within DMARC records, the adkim and aspf parameters, respectively for DKIM and SPF, allow you to specify the alignment mode for the authentication identifier (domain). They are set to either r (relaxed mode) or s (strict mode), the choice of which determines whether the organization's domain and the Header From field must match.

For example, if the organization's domain is example.com and the Header From field is system@alert.example.com, then SPF in alignment mode r will return a pass authentication result. In s mode, however, the domains must match exactly, so DMARC will fail in this case. The rua field specifies where DMARC reports are to be sent, and the aggregated results shown in the previous section represent a visualization of the reports received at dmarc-rua@dmarc.iij.ad.jp.

■ Post-change impact

IIJ changed its DMARC record on December 15, 2021.

After the change, we kept a close eye on inquiries and other developments but noted no major disruptions. Some people may consider a change of DMARC record to be a difficult undertaking, but we can report that it actually does not have that much of an impact, and DMARC lets you declare to email recipients that "our systems only send out emails that are in accordance with our policies, so please go ahead and quarantine or reject any non-compliant emails", so we encourage you to consider implementing it on your own systems.

In the past, IIJ's honeypots have observed a high volume of spoofed emails being sent with domains for which DMARC policies had not been declared. For organizations that need to ensure the legitimacy of email content (financial institutions, government agencies, etc.), we recommend adopting DMARC because it allows a clear distinction to be made between legitimate and spoofed emails.

During the writing of this article, we adopted a p=quarantine DMARC policy for IIJ and monitored the situation for a few weeks, and once we had determined there to be no real impact on business emails, the DMARC record was changed to p=reject as of March 23, 2022. As with the change to p=quarantine, this also did not result in any inquiries or concerns being raised internally.

1.4 Sender Authentication Data

1.4.1 Sender Authentication Adoption Rates

Two years have now passed since the global rise of telework, and 2021 was a year that witnessed many cyberattacks based on emails using the Emotet virus.

Figures 4–6 show the aggregated sender authentication results as a percentage of total for email services provided by IIJ for the period April 2021 to March 2022.

```
$ dig _dmarc.iij.ad.jp txt

;; ANSWER SECTION:
_dmarc.iij.ad.jp. 3600 IN TXT "v=DMARC1; p=none; adkim=s; aspf=s; rua=mailto:dmarc-rua@dmarc.iij.ad.jp"
```

DMARC record for iij.ad.jp before the change

```
$ dig _dmarc.iij.ad.jp txt

;; ANSWER SECTION:
_dmarc.iij.ad.jp. 3600 IN TXT "v=DMARC1; p=quarantine; adkim=s; aspf=s; rua=mailto:dmarc-rua@dmarc.iij.ad.jp"
```

DMARC record for iij.ad.jp after the change

Figure 3: DMARC Record for iij.ad.jp Before and After the Change

Comparing the figures here with those reported in IIR Vol. 51 (https://www.iij.ad.jp/en/dev/iir/051.html), we note that the DKIM and DMARC pass ratios have increased. The DKIM pass ratio is up a few percentage points from last time, which may possibly indicate a moderate increase in the adoption of SaaS by companies amid the telework era. With the DMARC pass ratio also on the rise, the picture is one of interest in sender authentication increasing, albeit gradually.

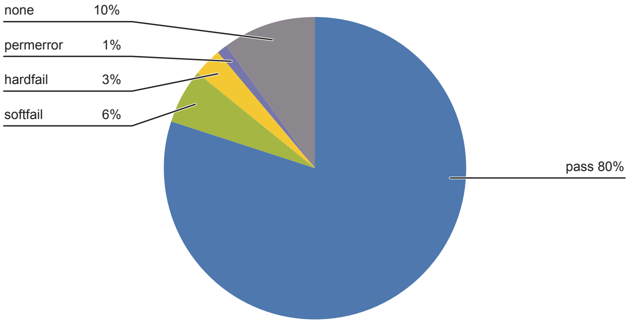


Figure 4: Breakdown of SPF Authentication Results

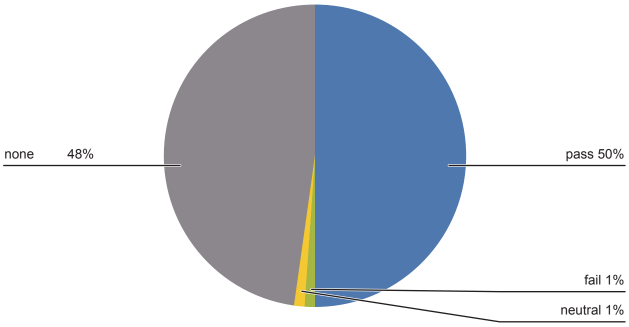


Figure 5: Breakdown of DKIM Authentication Results

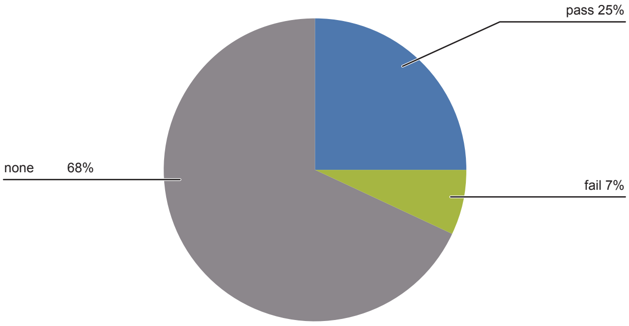


Figure 6: Breakdown of DMARC Authentication Results

Isamu Koga

Manager, Operation & Engineering 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 communicates information about the latest attack methods, trends in spam, and countermeasures.

Yusuke Imamura

Engineer, Operation & Engineering 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.