Countermeasures against Transmission of Illegitimate Emails on Large-Scale Email Systems

3.1 Introduction

For many years, IIJ has offered large-scale email system construction and email ASP services for service providers that have anywhere from hundreds of thousands to millions of users. Operating a large-scale email system requires considerable know-how, and in particular significant knowledge and experience is needed to incorporate effective countermeasures against the improper use of email. Since most of the work performed by email system administrators involves responding to improper use of the email system and associated troubleshooting, systematically implementing thorough countermeasures can reduce the workload while also contributing significantly to providing stable services to end users.

Trends in improper use shift on a daily basis, so email system administrators end up locked in a game of cat-and-mouse as they deal with each issue as it arises. Even if you consistently deal with improper use, it is difficult to reduce it, and this tends to be a futile struggle that is physically draining. On the other hand, it is possible to curtail improper use considerably by implementing mechanisms that allow you to focus systematically on key points.

Here we examine and explain several countermeasures against the improper use of email that have been effective, based on experience implementing and operating them on a variety of email systems. The countermeasures described here include those that require service providers to define a services agreement and obtain user consent, so we must note that individual service providers will need to consider whether each of the measures is appropriate for them.

3.2 The Importance of Countermeasures Against the Improper Use of Email

When an end user sends email using a service provider's email server, generally either SMTP authentication is performed by the MUA or Webmail is used. Although an authentication ID and password are necessary for SMTP authentication and the use of Webmail, if the user sets a password that is easy to guess, or if the PC itself is infected with a virus, these credentials are more likely to be leaked. There are many cases where spam is sent by impersonating a legitimate end user using authentication IDs and passwords leaked in this manner.

Spam generally involves the repeated automatic transmission of large volumes of email. As a result, email systems are flooded with email, which is ultimately sent over the Internet. When a large volume of spam is sent over the Internet, the outgoing IP address of the email system is recognized as the spam source and added to a blacklist on the Internet side. Being added to a blacklist has the following kinds of effects (Figure 1).

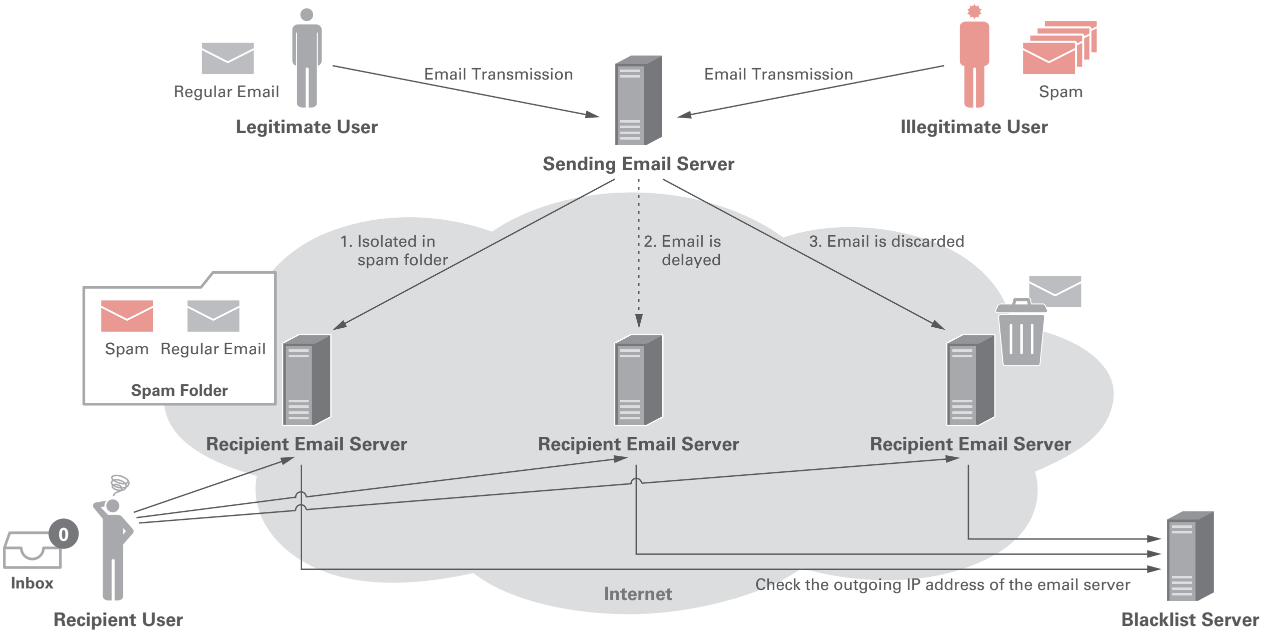


Figure 1: Impact of Illegitimate Email Transmissions

1. Regular email is detected as spam (in many cases Gmail, Hotmail, Yahoo.com, or a mobile phone carrier email service).
2. Email is delayed.
3. Email is discarded, and not delivered at all.

To be removed from a blacklist, it is necessary to eliminate the cause and restore normal service. However, many aspects of investigating the cause and implementing countermeasures involve trial and error, and this process can be quite exhausting for system administrators, so effective countermeasures against the improper use of email are a crucial part of system operations.

3.3 Trends in Illegitimate Email Transmissions

The nature of illegitimate email transmissions changes from moment to moment. Based on current trends, most illegitimate email is sent from overseas locations, as in the following examples.

1. A large volume of email is sent from overseas using a single authentication ID.
2. A large amount of email is sent simultaneously from overseas using multiple authentication IDs.
3. A large volume of email is sent from overseas using Webmail.

Basically, because all of these involve email being sent from overseas locations, it is possible to implement effective countermeasures against the sending of illegitimate email if a mechanism for determining the country of origin based on the email source IP address is available.

To implement such a mechanism, it is necessary to create a database that distinguishes countries based on the source IP address, along with a system that enables this to be used easily. There are several varieties of country database, such as MaxMind GeoIP2, but each differs in terms of whether they cost money or are free, whether support is available, whether they contain information other than country designations (regional level designations, Gmail's range discrimination, etc.), and whether they are updated frequently, so it is necessary to select one that matches your needs.

There are also ways to use country databases via API or by downloading and formatting them. Large-scale email systems on a service provider level tend to need to refer to country databases more often, because they receive a large volume of email, and

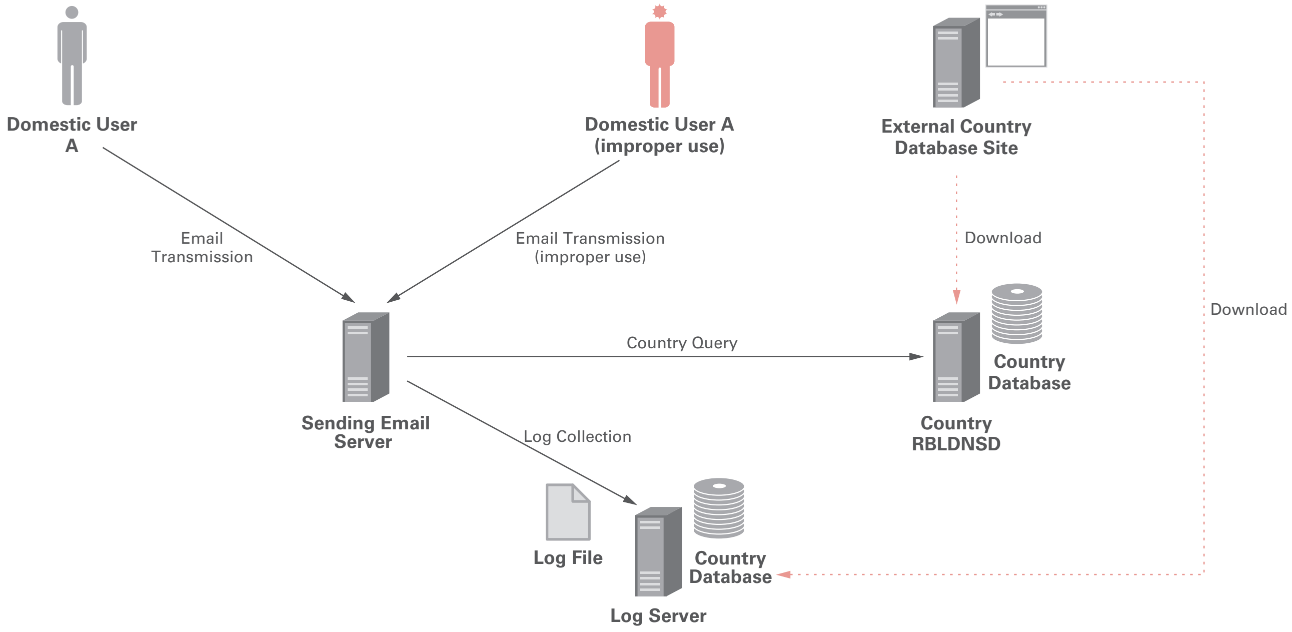


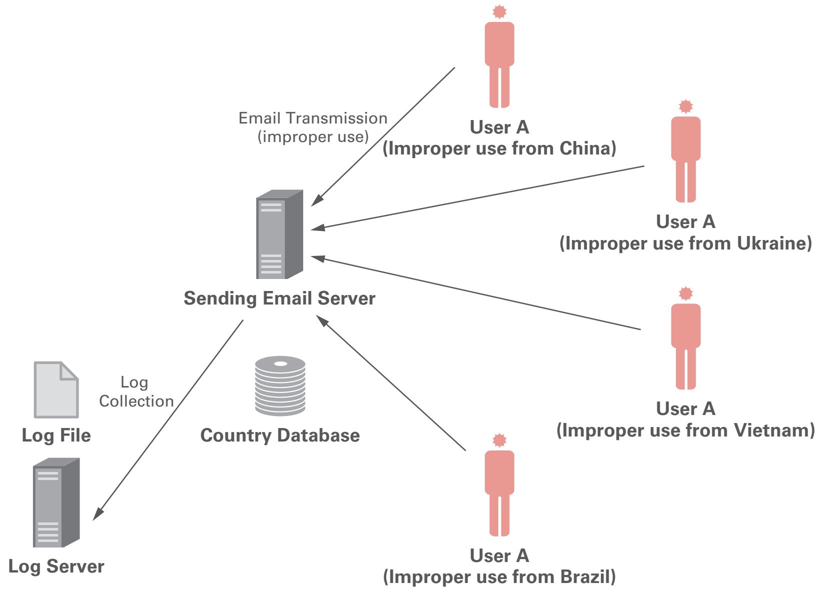
Figure 2: Overview of Country Data Detection System

based on experience the country data do not need to be updated very often, so we believe that downloading and shaping the data is a suitable approach in this case. The downloaded country databases are used for log analysis and real-time identification of countries on the email server, which I will explain later. Figure 2 shows a sample configuration.

3.4 Detecting Overseas Sources Using Email Logs

Typically, email server logs contain the authentication IDs and source IP addresses used for SMTP authentication. Creating a program to analyze email server logs using the aforementioned country databases enables analysis of the number of transmissions by country and the total number of emails sent for each authentication ID, making it possible to easily identify illegitimate email (Figure 3).

- **When email is sent from multiple countries within a few hours**
  For example, if emails are sent from China, Ukraine, Vietnam, and Brazil at approximately the same time using the same authentication ID, because there is no way for the user to be in different places around the world simultaneously, this makes it easier to determine that the authentication ID has been used illegitimately and take action to stop email being sent from these sources.
- **When a large volume of email is sent from a single overseas country**
  There are still many cases where a large volume of email is sent from a single overseas country. In this case, unlike the previous one, it may be hard to determine whether it is clearly an illegitimate use of email. However, if the number of emails sent within a certain period greatly exceeds a commonsense amount, it may be necessary to temporarily suspend email transmissions from the source in question. There are also cases where a large volume of legitimate email is sent from an overseas office, so adding certain authorization IDs to a whitelist is also something that must be considered.



● Log for email transmission from China (example of connection from China IP address: 1.0.*.*** using the authorization ID: example@example.com)

```
May 25 03:34:09 server11 smmta[16316]: AUTH=server, relay=from.example.com [1.0.*.***] (may be forged), authid=example@example.com, mech=PLAIN, bits=0
May 25 03:34:09 server11 smmta[16316]: w4OIY9On016316: from=from@example.com, size=0, class=0, nrcpts=1, proto=ESMTP, daemon=MSA, tls_verify=NONE, auth=PLAIN, relay=from.example.com [1.0.*.***] (may be forged)
```

● Log for email transmission from Brazil (example of connection from Brazil IP address: 23.97.*.*** using the authorization ID: example@example.com)

```
May 25 03:35:23 server11 smmta[16319]: AUTH=server, relay=from.example.com [23.97.**.***] (may be forged), authid=example@example.com, mech=PLAIN, bits=0
May 25 03:35:23 server11 smmta[16319]: w4P5Y60n028961: from=from@example.com, size=0, class=0, nrcpts=1, proto=ESMTP, daemon=MSA, tls_verify=NONE, auth=PLAIN, relay=from.example.com [23.97.**.***] (may be forged)
```

Figure 3: Detecting Improper Use Through Log Analysis

This sort of log-based approach is a versatile and effective method because it can be applied to the majority of email systems. However, the batch processing method often used for logs hinders the ability to respond in real time, and in some cases, systems have been hit with 10,000 or more emails before illegitimate transmissions were suspended, resulting in senders being added to a blacklist. This means that for large-scale email systems, there are times when simply analyzing email logs is not effective enough.

3.5 Implementing Real-Time Overseas Country Detection on Email Servers

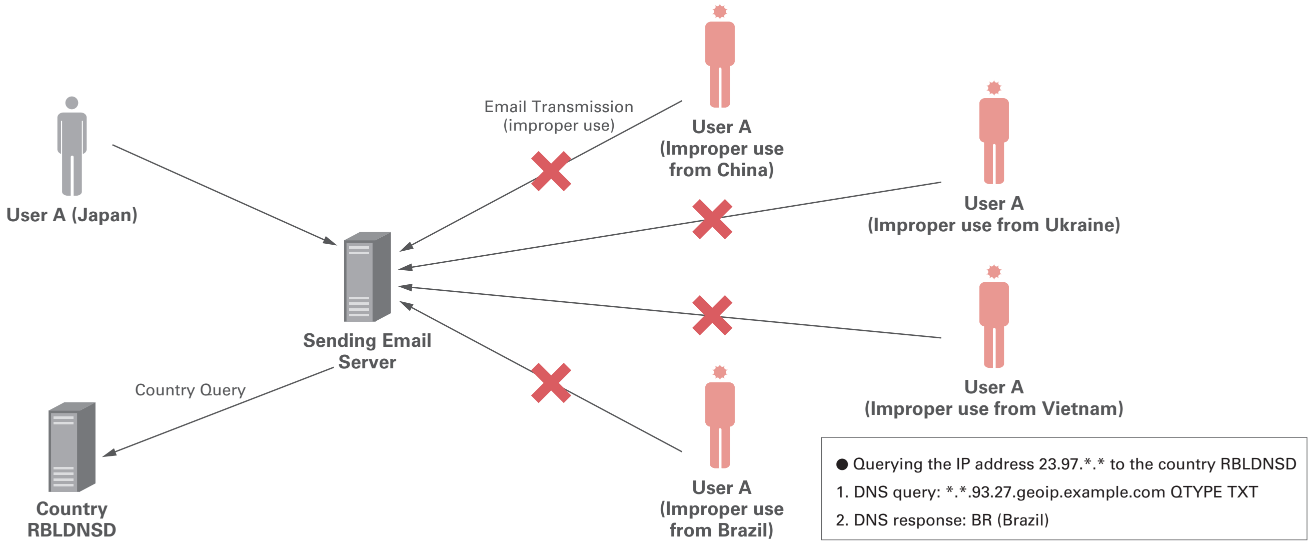
There is a way to detect the originating country in real time by having the email server query a country database (such as an independently built RBLDNSD for countries) with the source IP address of the sender (Figure 4). Because this method enables real-time detection at the email server level, it is possible to identify email sent from multiple countries within the same time period as illegitimate and immediately suspend transmission. This enables you to eliminate the delay before a suspension is imposed, which was the issue with email log analysis. As a result, you can prevent situations where you only notice large volumes of email after it is sent, so implementing this solution can have a significant impact.

By fine-tuning the implementation, it is also possible to apply suspensions to only email from overseas and not the entire system, reducing the impact on end users whose usage takes place predominantly in Japan. This also offers a superior experience from the perspective of user support.

That said, implementing a real-time detection function on an email server requires the introduction of a Milter program, the modification of OSS email servers such as Postfix and Sendmail, or the use of a commercial email server with programming functions (such as Cloudmark Security Platform for Email or Vade Secure). Although the benefits of implementation are significant, the high degree of technical difficulty involved is a concern to some. In fact, when implementing this solution in the past, carefully performing repeated tests to ensure quality required a considerable amount of time.

3.6 Countermeasures Against Transmission of Illegitimate Emails via Webmail

The abovementioned countermeasures against the transmission of illegitimate emails were aimed at the sending of email using SMTP authentication, but the transmission of illegitimate email by Webmail is also on the rise. Several typical varieties of Webmail software are available in the Japanese email industry, and although each uses completely different methods to perform login and email transmission, the fact is that large volumes of email have been sent in formats corresponding to each software application. It has also been reported that the outbox is emptied and the user logged out once the emails have been sent so that no trace of the email having been sent via Webmail remains, and my impression is that this sort of improper use is becoming significantly more sophisticated.



● Querying the IP address 23.97.*.* to the country RBLDNSD
1. DNS query: *.*.93.27.geoip.example.com QTYPE TXT
2. DNS response: BR (Brazil)

Figure 4: Real-Time Detection of Improper Use

Generally, because the recipient email server does not know the source IP address of email transmitted via Webmail, the country detection detailed above is hard to perform. As a result, it is difficult to detect improper use, and therefore Webmail is targeted by attackers as a secondary method of sending illegitimate email. To counter this, we adopted Webmail software that can embed source IP addresses in the email headers, and we also implemented controls using header information on the email server side (Figure 5). By taking this approach, the email server is able to detect countries in real time, making early detection and countermeasures against improper use possible. Webmail is also modified to prevent accounts affected by improper use from using it, or to suspend its use from overseas.

3.7 User Control over the Use of Email from Overseas Locations

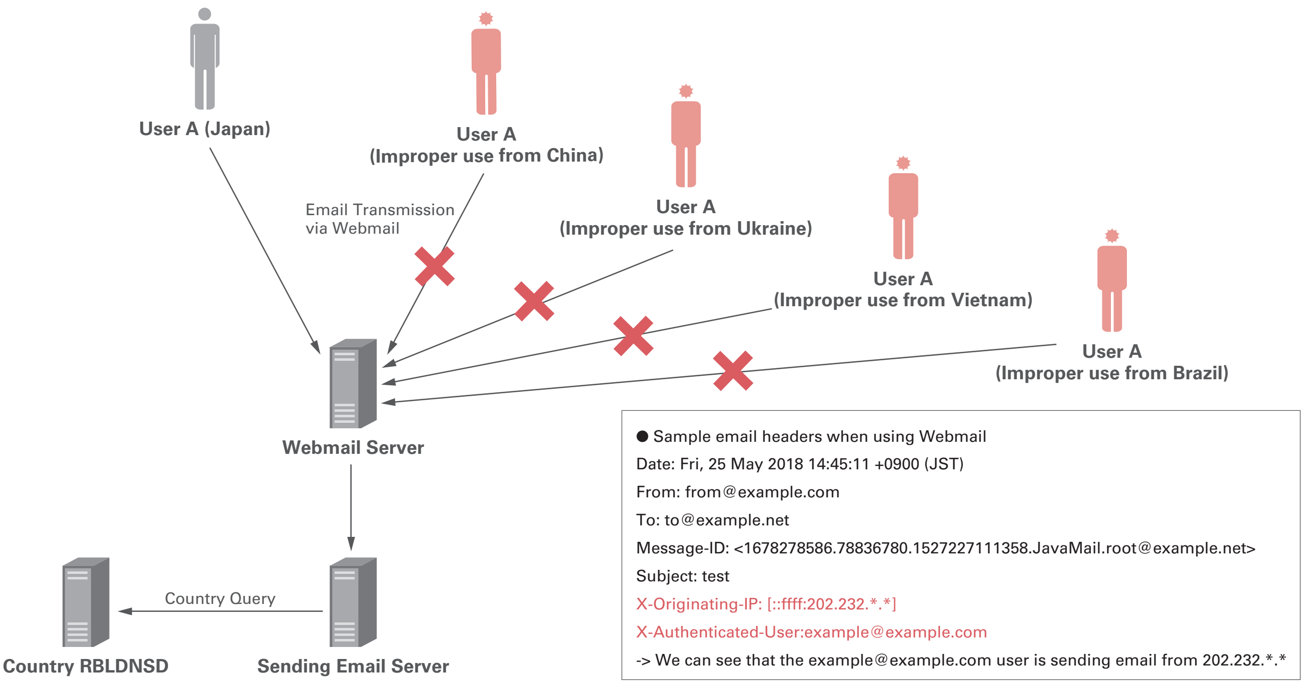
You can also leave control of email access from overseas locations up to the user (Figure 6). Specifically, this method involves having users select whether to allow the transmission of email using SMTP authentication, the transmission of Webmail, and the receipt of POP/IMAP email from overseas, applying access control on a user-by-user basis on the email server side.

This makes it possible to restrict the transmission and receipt of email from overseas as well as Webmail logins under normal circumstances, while also providing the ability to enable these options from the management screen when on an overseas business trip or vacation.

This method is useful because giving end users the choice makes it easier to obtain their permission, while also serving to raise awareness of how access from overseas can easily lead to improper use. That said, as it is necessary to get consent from users to restrict access from overseas by default, it may not significantly reduce the improper use of email.

3.8 Countermeasures against SMTP Connection DoS Attacks

To stray from the topic a bit, one example of illegitimate email transmissions is where email server connections are deliberately exhausted by directing a high volume of SMTP connections at the server for a sustained period using multiple authentication IDs. This is a sophisticated type of DoS attack that identifies and exploits the timeout mechanism of email servers. These attacks



● Sample email headers when using Webmail
Date: Fri, 25 May 2018 14:45:11 +0900 (JST)
From: from@example.com
To: to@example.net
Message-ID: <1678278586.78836780.1527227111358.JavaMail.root@example.net>
Subject: test
X-Originating-IP: [::ffff:202.232.*.*]
X-Authenticated-User:example@example.com
-> We can see that the example@example.com user is sending email from 202.232.*.*

Figure 5: Detecting Illegitimate Email Transmissions via Webmail

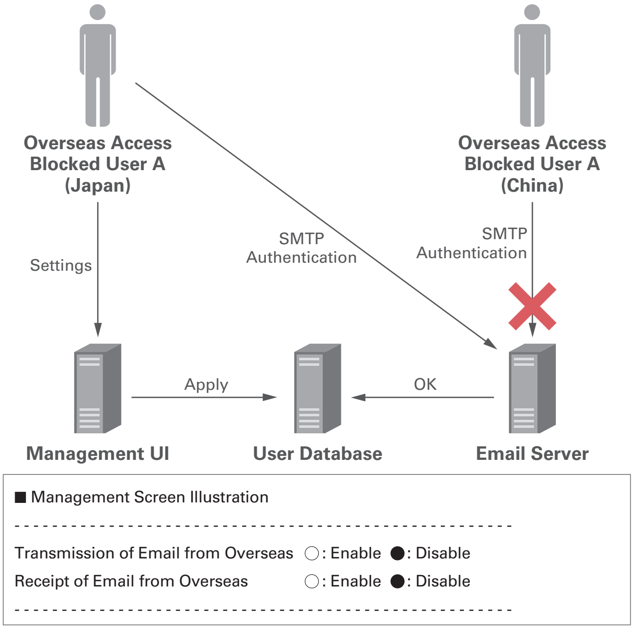
frequently prevent new SMTP connections from being made at all, which has a significantly adverse impact on the provision of services (Figure 7).

One common method for dealing with sustained SMTP connections is to reduce the timeout period for the email server. Because the standard timeout period for email servers is often long, when deploying a server it is necessary to fine-tune the timeout period appropriately. Meanwhile, RFC 5321 (Simple Mail Transfer Protocol) defines recommended values for SMTP timeout under 4.5.3.2 Timeouts. Timeouts cannot be shortened in many cases because careless configuration can impact the transmission of legitimate email, so there are limitations to adjusting them.

Other methods include periodically checking the number of SMTP connections, and when this number approaches the system's limit, determining which sessions have a long idle timeout and disconnecting them from the server side (using the tcpkill command, etc.). By disconnecting SMTP sessions targeted at accounts affected by improper use, this also makes it more difficult for SMTP sessions to accumulate, reducing the risk of SMTP connection DoS attacks.

3.9 Conclusion

There are many measures for counteracting the transmission of illegitimate emails on large-scale email systems, so you need to combine multiple methods effectively. Implementation is costly and requires technical expertise, but considering the significant reductions to email service maintenance and system administrator workload, along with increased motivation, we believe that some form of countermeasures against the transmission of illegitimate emails are essential. I hope this article serves to aid the stable operation of email systems.



■ Management Screen Illustration

Transmission of Email from Overseas ○: Enable ●: Disable
Receipt of Email from Overseas ○: Enable ●: Disable

Figure 6: User Control over the Use of Email from Overseas Locations

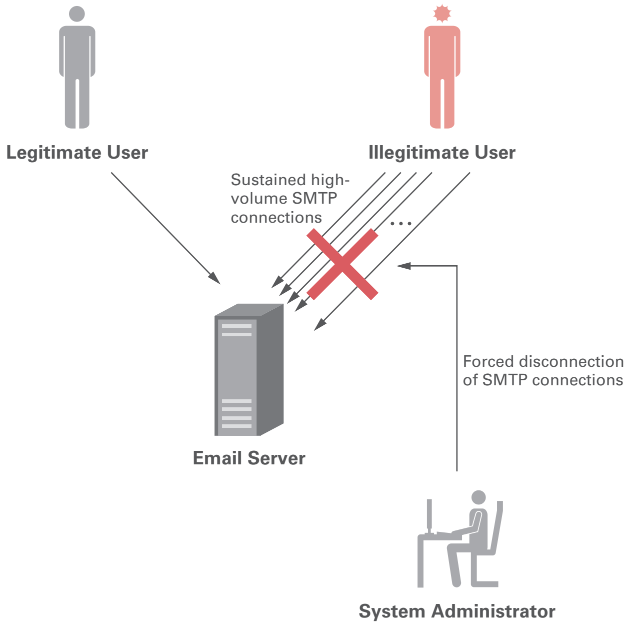

Legitimate User
Illegitimate User
Sustained high-volume SMTP connections
Email Server
Forced disconnection of SMTP connections
System Administrator

Figure 7: SMTP Connection DoS Attacks

Author:
Shigehiro Kinugasa
Manager, Mail Solutions Section, Enterprise Solutions Department, Cloud Division, IIJ