Outline of Legal Points to Remember on Introducing Sender Domain Authentication Technologies

■ Sender Domain Authentication and Port 25 Blocking

Sender domain authentication (*1) and port 25 blocking (*2) are introduced as effective anti-spam email technologies. These technologies are interpreted as actions to confirm information on communications (e.g., the source domain, and IP address) against the intention of the parties and take certain measures using the information for the purpose of filtering or refusing the reception of specific emails.

*1. E.g., SPF, DKIM, and DMARC. *2. Outbound Port 25 Blocking (OP 25 B) and Inbound Port 25 Blocking (IP 25 B)

■ Legal Points to Remember

The Telecommunications Business Act stipulates that the secrecy of communications being handled by a telecommunications carrier shall not be violated and that no telecommunications carrier shall engage in unfair and discriminatory treatment with regard to the provision of telecommunications services. The act of disadvantageously treating the communications of a specific person after checking and using his/her secrecy of communications is likely to fall under the scope of the infringement of his/her secrecy of communications or the discriminatory treatment of the person unless there are legitimate business acts and justifiable causes.

Telecommunications Business Act (Act No. 86 of 1984)

Article 4 (Protection of Secrecy)

The secrecy of communications being handled by a telecommunications carrier shall not be violated.

Article 6 (Fairness in Use)

No telecommunications carrier shall engage in unfair and discriminatory treatment with regard to the provision of telecommunications services.

While each of the above technologies has been widely adopted as effective spam countermeasures. However, depending on the implementation method of each technology, it can conflict the protection of the secrecy of communications and the prohibition of discriminatory treatment prescribed in the Telecommunications Business Act. Accordingly, it is necessary to summarize all problems for the implementation of the technologies legally.

As stated on the next page and “Outline of Legal Points to Remember on Introducing Sender Domain Authentication Technologies,” the following items are considered feasible under certain conditions. Accordingly, it is desirable for internet service providers (ISPs) to promote the legitimate introduction of the above technologies.

- Sender domain authentication and port 25 blocking as legitimate business acts and justifiable causes for noncompliance with the Act, and legally possible to conduct them.
- Filtering based on the result of sender domain authentication by acquiring comprehensive agreement.

■ Conditions to Recognize Sender Domain Authentication and Port 25 Blocking as Legitimate Business Acts and Justifiable Causes for Noncompliance with the Act

Generally, in order for legitimate business practices to be accepted, **(1) the necessity and legitimacy of actions** and **(2) the necessity of means** are required.

(1) The necessity and legitimacy of actions: All the sender domain authentication technologies and port 25 blocking are considered to satisfy (1) under circumstances where a lot of emails are transmitted and received because it is necessary to prevent obstacles such as a delay in email delivery caused by spam e-mails.

(2) The necessity of means: Each of the above technologies is used within the minimum necessary range to achieve the purpose and there are no alternative restrictive methods. Therefore, the technologies are considered to satisfy (2) as well.

Accordingly, the introduction of each of the above technologies is recognized as a legitimate business practice and justifiable cause.

■ Users' Consent Necessary to Implement Filtering based on Sender Domain Authentication

(1) If the service is provided at the request of users while the initial settings for the service are turned OFF, it is generally considered that the consent of the users is valid.

(2) In the case of providing the service with initial settings turned ON, the preliminary comprehensive agreement in service contracts, if any, to have the users relinquish their benefit of protecting the secrecy of communications is not considered to be the effective consent of the users and not allowed because of the following reasons: 1) It does not comply with the nature of such contracts and 2) The object of the consent is unclear.

* If the following conditions are satisfied, however, even if the service is provided with the initial settings turned ON, it is considered that the effective consent of the users has been acquired.

1) The users can arbitrarily make setting changes even after their consent.
2) Regardless of whether the consent is absent or present, other service conditions remain unchanged (*1).
3) The object and scope of the consent are clearly limited.
4) In the case of average users, it is reasonably presumed that average users will agree (the endorsement of the same with reliable data (*2) is required).
5) An adequate explanation about the content of the filtering service is required in advance (by following procedures similar to the explanation of important matters prescribed in Article 26 of the Act).

*1. It is not a problem to provide the filtering service at a reasonable fee.
*2. It is possible to conduct a questionnaire survey on users sampled at random.

■ Requirements Not Considered Illegal Discriminatory Treatment

If the service is applied uniformly to users to the extent that the above requirements are satisfied, the service is not considered to fall under unreasonable discriminatory treatment.