

Legal Notes on Introduction of Sender Domain Authentication Technology on Receiving Side

(1) Protection of Secrecy of Communications and Prohibition of Unfair Discriminatory Treatment Prescribed in Telecommunications Business Act	1
(2) Sender Domain Authentication on Receiving Side	2
(Reference) Domain Authentication Technology and Action Not to Return Error Email	6
(3) Filtering Action Falling under Infringement of Secrecy of Communications	7
(Supplement) About Acquisition of Parties' Consent in DMARC	9
(4) Outbound Port 25 Blocking (OP25B)	12
(5) Inbound Port 25 Blocking (IP25B)	16

Protection of secrecy of communications

Telecommunications Business Act

Article 4 The secrecy of communications being handled by a telecommunications carrier shall not be violated.

1. Applicability of the secrecy of communications

The secrecy of communications refers to items, including the following ones, from which the semantic content of communication will be inferred: (1) The content of individual communication and (2) The date, time, and locations of individual communication, the names, addresses, residences, and identification codes, such as the telephone numbers, of the communication party, and the number of times of communication.

Transmission domains related to individual emails fall under the scope of route information related to individual communications, and are secured secrets of communications because they are constituent elements of communications.

2. Falling under Infringement of Secrecy of Communications

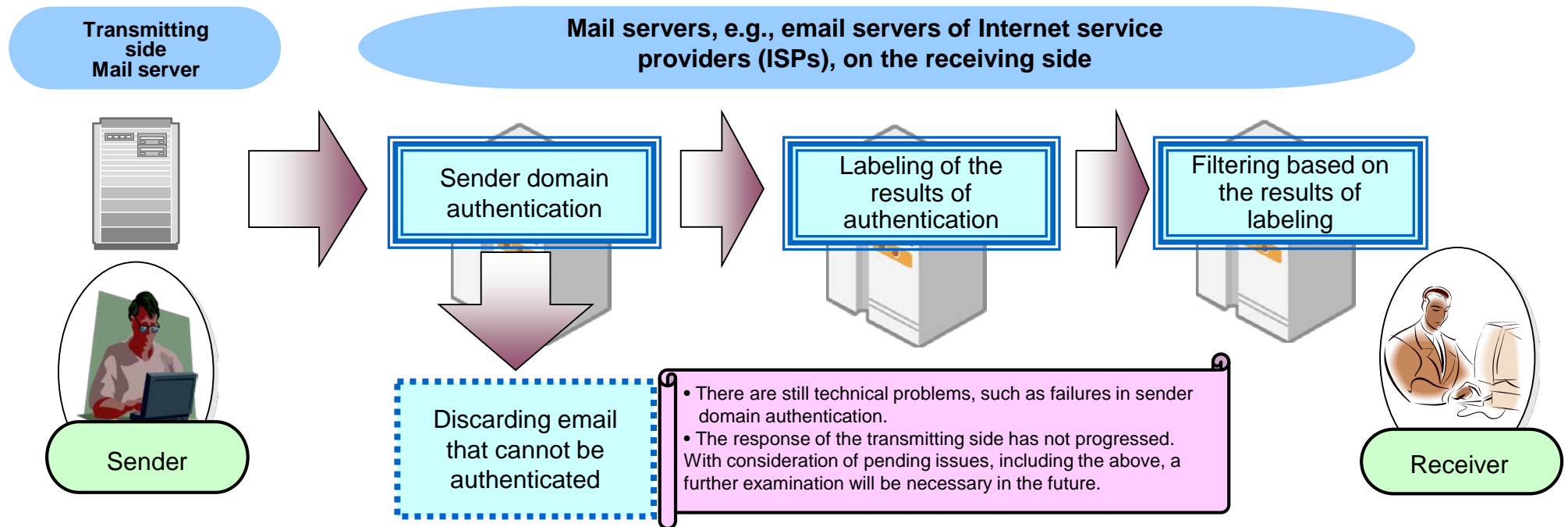
Acts of infringing on the secrecy of communications include the act of using the secrecy of communications against the will of the senders or receivers.

Prohibition of unfair discriminatory treatment

Telecommunications Business Act

Article 6 No telecommunications carrier shall engage in unfair and discriminatory treatment with regard to the provision of telecommunications services.

(2) Sender Domain Authentication on Receiving Side



1. Legal nature of sender domain authentication technology

Although there are differences technically, from a legal point of view, SPF, DKIM, and DMARC are all considered to be actions to take certain measures if the reception server of emails cannot authenticate (check) the sender domain of each email.

2. Legal problems

Whether the labeling of emails (on the premise of filtering of emails, including the rejection of reception, based on the results of the labeling) in the case of a failure in sender domain authentication on the receiving side causes any problems in relation to the Telecommunications Business Act.

Specifically, whether the above action causes the following issues.

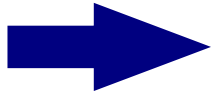
- Whether the action constitutes the act of infringing on the secrecy of communications prescribed in Article 4 of the Telecommunications Business Act.
- Whether the action constitutes unfair discriminatory treatment prescribed in Article 6 of the Telecommunications Business Act.

Conclusion

- Sender domain authentication is the act of mechanically authenticating the sender domain of an email in the server on the receiving side and perform the labeling of the email against the will of the communications parties if the email is not authenticated. The act, however, constitutes the infringement of the secrecy of communications prescribed in Article 4 of the Telecommunications Business Act.
- In the case of implementing this to reduce the possibility of obstacles in sending and receiving emails, such as delays in services caused by massive quantities of spam emails transmitted, however, sender domain authentication is recognized as a legitimate business practice and justifiable cause.
- Furthermore, sender domain authentication is permitted as a legitimate business practice. Therefore, unless it is applied to specific limited users, the act is not considered to constitute unfair discriminatory treatment prohibited by Article 6 of the Telecommunications Business Act.
- As described above, legal issues over sender domain authentication can be cleared. Therefore, ISPs' proactive introduction of the same along with a filtering service that will be described later is desirable.

Study on Infringement of Secrecy of Communications (1)

The infringement of the secrecy of communications (the use of the secrecy of communications against the will of the sender or receiver) will be constituted by mechanically performing the sender domain authentication of emails in the server on the receiving side and labelling the emails against the will of the communications parties in the case of a failure in authentication.



Constitutes the infringement of the secrecy of communications unless the consent of the parties is obtained.

The infringement of the secrecy of communications may be constituted by mechanically performing the sender domain authentication of emails in the server on the receiving side and labeling the emails against the will of the communications parties in the case of a failure in authentication. **The act, however, will be permitted regardless of the consent of the communications parties if there are grounds for restraining illegality (e.g., legal self-defense, emergency evacuation, or legitimate business conduct).**

1. Legitimate self-defense and emergency evacuation relevance

Transmission domain authentication is a measure to prevent trouble in email transmission and reception and always taken regardless of whether trouble in email transmission and reception is imminent or not.

For this reason, it does not always satisfy the conditions of legitimate self-defense or emergency evacuation, and cases that do not correspond to legitimate self-defense or emergency evacuation are assumed.

2. Legitimate appropriateness of business conduct

Legitimate business conduct needs to satisfy (1) the legitimacy and necessity of the conduct (2) the appropriateness of the means.

(1) Justification and necessity of actions

- Most emails that spoof the senders are spam emails
- The senders of most unsolicited email are camouflaged.
- Unsolicited emails sent as a means of advertisement promotion can reasonably be estimated to be transmitted to a large number of people at one time unless there are exceptional circumstances.

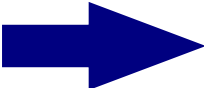
It can be presumed that emails spoofing the sending domains are being sent to a large number of people at one time.

Therefore, in order to reduce the risk of obstacles in sending and receiving emails, such as delay in services caused by spam emails that are massively transmitted, **the legitimacy and necessity of performing sender domain authentication and labeling the results are recognized.**


(2) Necessity of means

- Sender domain authentication infringes on the sender's route information on the sender domain, which, however, does not exceed the necessary limit of the purpose (the act of labeling for filtering).
- Other anti-spam measures such as OP25B and sender authentication also exist. These technologies may not always work on spam emails transmitted by camouflaging the sender domains.

Therefore, the act of labeling the result of sender domain authentication is considered a proper method.



It can be interpreted as a legitimate business practice (with grounds for restraining illegality).



Furthermore, if it is implemented uniformly as a measure permitted as a legitimate business practice, it does not fall under the scope of unfair discriminatory treatment prescribed in Article 6 of the Telecommunications Business Act.

1. Applicability of the infringement of the secrecy of communications

Transmission domains related to individual emails fall under the scope of route information related to individual communications, and are secured secrets of communications because they are constituent elements of communications.

In the case of mechanically checking the sender domains of emails with unknown destinations and not returning error emails to the sender servers if no sender domain authentication is possible on the receiving side, the case is considered to constitute the act of using the secrecy of communications against the will of the sender or receiver.



Constitutes the infringement of the secrecy of communications unless the consent of the parties is obtained.

2. Legitimate appropriateness of business conduct

(1) Justification and necessity of actions

- It can be presumed that emails spoofing the senders' domains are being sent to a large number of people at a time.
- Most unsolicited emails received by mail servers are unknown destination emails. Therefore, **the necessity and legitimacy of the act of not returning error emails for destination unknown emails are recognized** if they cannot be authenticated. Because the act is recognized to reduce the possibility of trouble in sending and receiving of emails caused by the traffic of a large amount of destination unknown emails and error emails as a result of junk emails transmitted in bulk.

*A failure in the sender domain authentication of an email suggest that the mail server as the sending source has not actually sent the email, in fact. Therefore, it is meaningless to return an error email to the transmitting side stating that it could not be delivered from the server on the receiving side.

(2) Necessity of means

Sender domain authentication infringes on the sender's route information on the sender domain, which, however, does not exceed the necessary limit of the purpose (the act of not returning error emails for destination unknown emails failing in sender domain authentication).



It can be interpreted as a legitimate business practice.

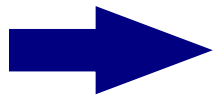
(3) Filtering Action Falling under Infringement of Secrecy of Communications

Whether the filtering of emails based on the labeling of the emails as a result of sender domain authentication causes any problems in relation to the Telecommunications Business Act.

Specifically, whether the above action causes the following issues.
Whether the action constitutes the act of infringing on the secrecy of communications prescribed in Article 4 of the Telecommunications Business Act.

• **Applicability of the infringement of the secrecy of communications**

The infringement of the secrecy of communications (the use of the secrecy of communications against the will of the sender or receiver) will **be constituted** by filtering and detecting the secrecy of specific communications falling under predetermined conditions and processing the emails against the will of the communications parties (e.g., blocking or disposing of the emails).



Constitutes the infringement of the secrecy of communications unless the consent of the parties is obtained.

The filtering of an email is an act for the receiver. Therefore, in principle, it does not fall under the scope of justifiable causes, such as a legitimate business practice, be carried out regardless of the intention of the receiver.

Therefore, it is necessary to obtain the effective consent of the parties.

About the Consent of the Parties to the Introduction of Filtering

- (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
 - 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.

(Supplement) About Acquisition of Parties' Consent in DMARC

1. Overview of DMARC

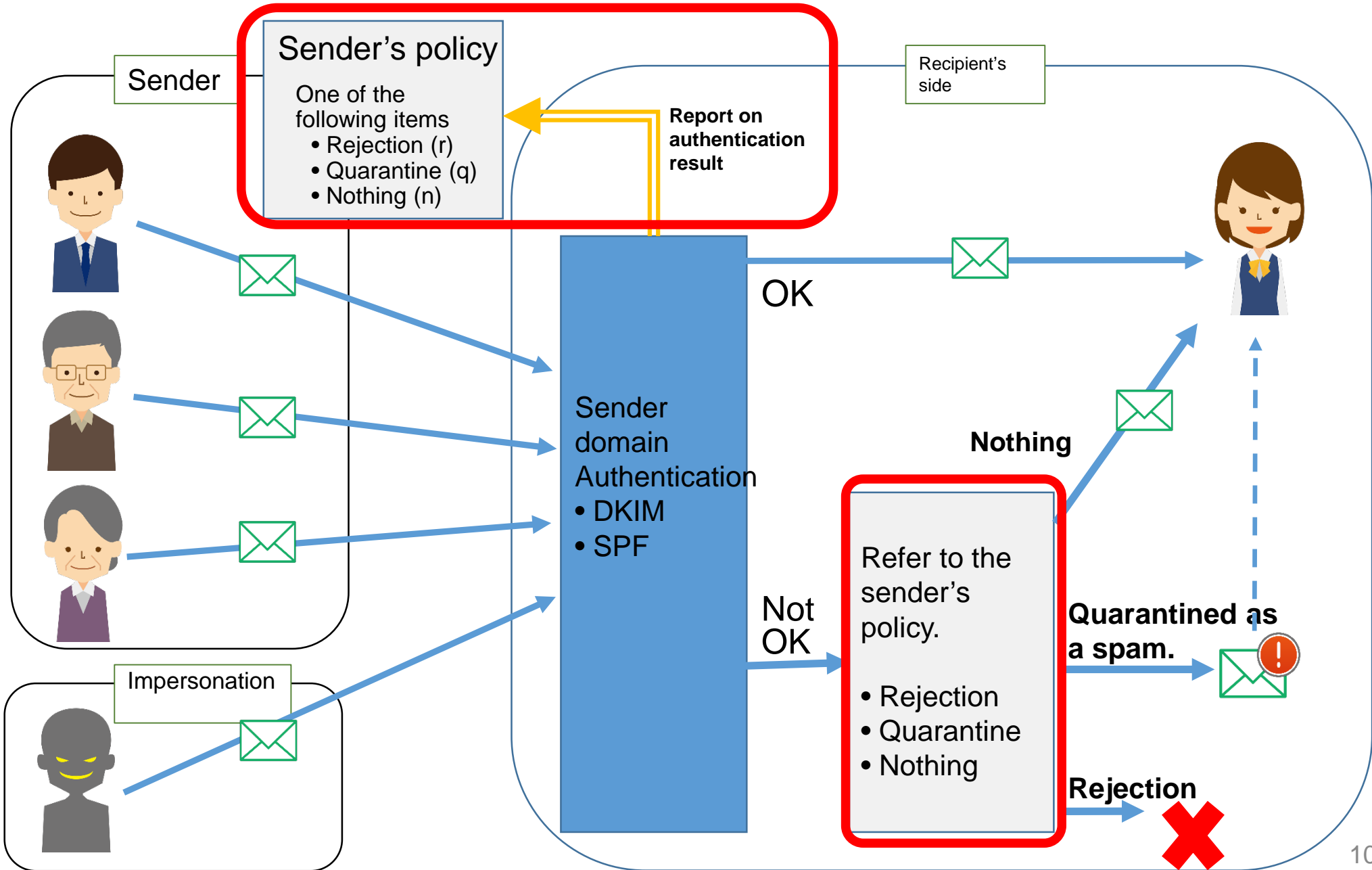
- (1) The domain administrator declares a handling policy of e-mail transmitted under the domain name in the case of a failure in the domain authentication of the e-mail at the time of reception and discloses the e-mail address to which the report described in (3) below is to be sent.
- (2) With consideration of the handling policy specified in (1), either one of the following processes shall be applied to the e-mail that has a failure in the Domain Keys Identified Mail and Sender Policy Framework (DKIM and SPF) authentication on the reception server side.
 - Nothing is done: Delivered to the recipient as it is.
 - Quarantine: Quarantined by indicating the failure in authentication (treated as a spam).
 - Rejection: Deleted from the reception server (the recipient does not recognize the existence of the e-mail).
- (3) The receiving server sends a report on the authentication result in (2) to the destination mail address specified by the sender domain administrator.

2. Legal Issue

Legally,

- Case (2) **is interpreted as an act of authenticating (checking) the transmission domain of the e-mail in the receiving server and taking certain measures if it cannot be authenticated.**
- Case (3) **is interpreted as an act of reporting information on a communications message that cannot be authenticated to the sender domain administrator or a party designated (e.g., the ISP, an analyst, etc.) by the sender domain administrator.** Both of them apparently can fall under **the act of infringing the confidentiality of communication prescribed in Article 4 of the Telecommunications Business Act,** and whether it is possible or not to apply them will be an issue.

Overview of DMARC



Agreement of the parties on the introduction of DMARC

From the following reasons, **in principle, service providers are not allowed to have users abandon their confidential interests of communications in accordance with prior comprehensive agreements and such agreements are not understood as the constitution of the users' effective consent:** (1) Not complying with the nature of agreements (2) The subject of the consent is unclear.

If the following conditions are satisfied, however, it can be considered that the users' effective consent is acquired even if DMARC is provided on the basis of the comprehensive agreements.

- 1) The users can make setting changes by themselves at any time.
- 2) All other service conditions remain the same regardless of the presence or absence of the consent. (*1)
- 3) The subject and scope of the consent is clarified.
- 4) When sending a report on the result of domain authentication, neither the body nor subject of the e-mail is included in the content of the report. (*2)
- 5) An adequate explanation for the content of DMARC is given in advance (through procedures pursuant to the explanation of important matters prescribed in Article 26 of the Telecommunications Business Act). (* 3)

*1. There is no problem providing a filtering service including DMARC for a reasonable charge.

*2. None of the header information related to the content of the e-mail, including the main body and the subject header information, is contained.

*3. DMARC needs to explain the following points to each user clearly.

1) Blocking based on the policy.

- Information on blocking.

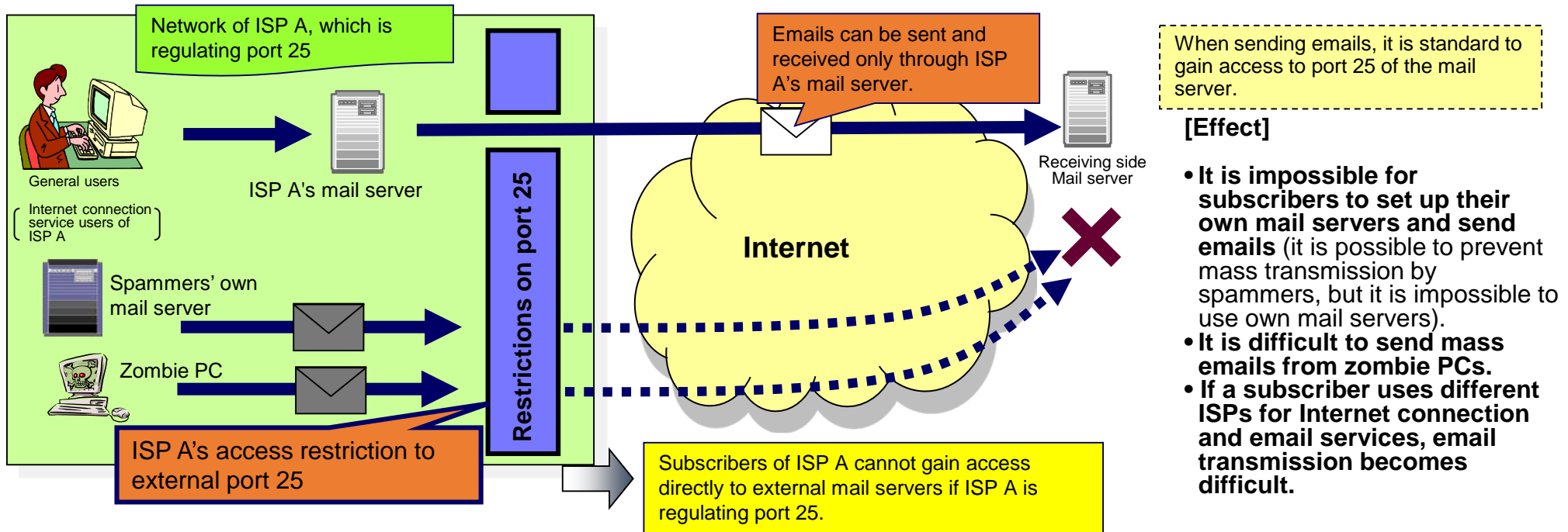
- Information that the users cannot confirm the content of the e-mail that has been blocked.

2) Making a report according to the request of the sender domain administrator.

- Matters to be included in the report.

- The fact that the above matter is sent to the destination designated by the sender.

(4) Outbound Port 25 Blocking (OP25B)



1. Legal nature of OP25B

The act of an ISP as a telecommunications carrier to automatically detect the IP address and port number of the sender (and receiver*) of each email passing through the router under the ISP's control and management and mechanically single out and block emails transmitted through other mail servers to port 25 from dynamic IP addresses (closing port 25 to reject the access).

* Closing port 25 to reject emails for specific destinations. For example, in the case of implementing the OP25B of only emails to a mobile phone company, it is necessary to check whether or not the destination is the mail server of the mobile phone company.

2. Legal problems

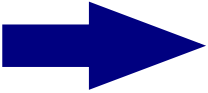
Specifically, the following points become questions of whether the above act conflicts with Telecommunications Business Act.

- Whether the action constitutes **the act of infringing on the secrecy of communications prescribed in Article 4 of the Telecommunications Business Act.**
- Whether the action constitutes **unfair discriminatory treatment prescribed in Article 6 of the Telecommunications Business Act.**

Conclusion

- OP25B corresponds to the act of infringing on the secrecy of communications prescribed in Article 4 of the Telecommunications Business Act. The reason is that it is a measure to check the sender's IP address and port number of each email as a component of the communication and block the email according to the result.
- However, if the following facts are present, it can be considered that OP25B is recognized as a legitimate business practice and its illegality is restrained.
 - 1) There is no mass transmission using the mail server of the ISP.
 - 2) There is massive transmission from dynamic IP addresses not via the mail server of the ISP.
 - 3) There are no alternative means implemented to the necessary extent not violating the secrecy of communications.
- OP25B rejects emails that meet certain conditions, where the infringement of the secrecy of communications (using the secrecy of communications against the will of the senders or receivers) is allowed as a legitimate business practice. As long as it is applied to specific parties, it is not considered to be unfair discriminatory treatment prohibited by Article 6 of the Telecommunications Business Act.
- As described above, legal issues over OP25B can be cleared. Therefore, ISPs' proactive introduction of the same is desirable.

The act of an ISP's detection of the IP address and port number of the sender of each email passing through the router under the ISP's control and management and single out and block emails transmitted through other mail servers to port 25 from dynamic IP addresses **falls under the infringement of the secrecy of communications. That is, the use of the secrecy of communications against the will of the sender or receiver.**



OP25B corresponds to the act of infringement of the secrecy of communications unless there is consent of the parties.

The act of an ISP's detection of the IP address and port number of the sender of each email passing through the router under the ISP's control and management and single out and block emails transmitted through other mail servers to port 25 from dynamic IP addresses falls under the infringement of the secrecy of communications. That is, the use of the secrecy of communications against the will of the sender or receiver. The act, however, will be **permitted regardless of the consent of the communications parties if there are grounds for restraining illegality (e.g., legal self-defense, emergency evacuation, or legitimate business conduct).**

1. Legitimate self-defense and emergency evacuation relevance

OP25B is a **measure** to prevent trouble in email transmission and reception and **always taken** regardless of whether trouble in email transmission and reception as a result of the mass transmission of emails is imminent or not.

For this reason, it does not always satisfy the conditions of legitimate self-defense or emergency evacuation, and **cases that do not correspond to legitimate self-defense or emergency evacuation are assumed.**

2. Legitimate appropriateness of business conduct

Legitimate business conduct needs to satisfy (1) the legitimacy and necessity of the conduct (2) the appropriateness of the means.

(1) Justification and necessity of actions

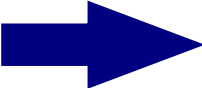
- There is no massive transmission using the mail server of the ISP.
- There is massive transmission from dynamic IP addresses not via the mail server of the ISP.
- The uniform rate control for the entire traffic is insufficient as a prevention measure for mass transmission.

If the above facts are present, it can be considered that the necessity and validity of transmission control of emails from dynamic IP addresses not via the mail server of the ISP is recognized as a legitimate business practice and its illegality is restrained in order to properly maintain and manage the network and operate the mail service.

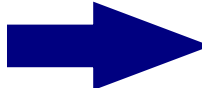
(2) Necessity of means

- OP25B infringes on the sender's route information on the IP address and port number, which, however, does not exceed the necessary limit of the purpose.
- A number of other measures (e.g., sender domain authentication and sender authentication in the server) are taken. OP25B, which is a countermeasure taken by the ISP on the transmitting side for preventing transmission of unsolicited emails on the Internet, is considered to be a considerable method for attaining the goal of proper management of email service.

Accordingly, for the achievement of the purpose, it is considered a necessary and appropriate method for each ISP to check the IP address and port number of the sender of each email passing through the router under the ISP's control and management and single out and block emails transmitted directly through other mail servers to port 25 from dynamic IP address.

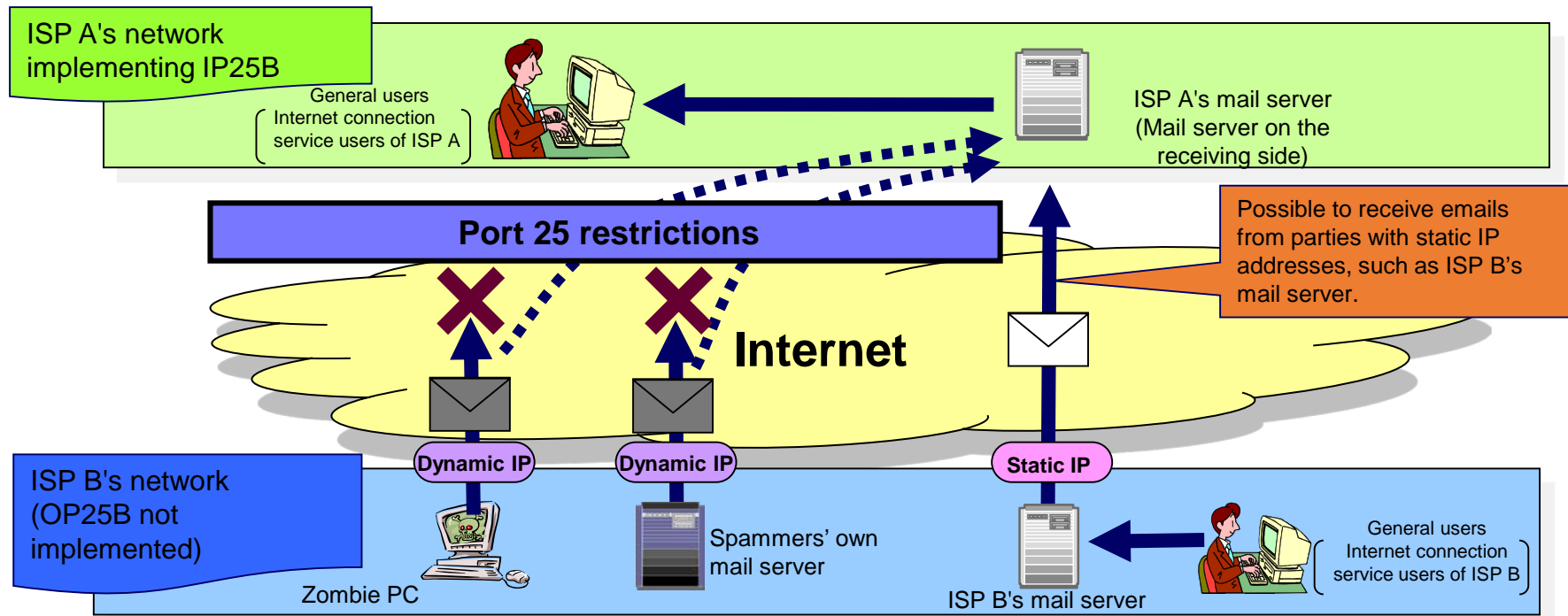


OP25B can be interpreted as a legitimate business practice (with grounds for restraining illegality).



Furthermore, if it is implemented uniformly as a measure permitted as a legitimate business practice, it does not fall under the scope of unfair discriminatory treatment prescribed in Article 6 of the Telecommunications Business Act.

(5) Inbound Port 25 Blocking (IP25B)



1. Legal nature of IP25B

IP25B is implemented by each ISP as a telecommunications carrier. IP25B automatically detects the IP address and port number of the sender (and receiver*) of each email passing through (flowing into) the router under the ISP's control and management. Then it mechanically singles out and blocks (by closing port 25 to reject) emails transmitted directly through other mail servers to port 25 from IP addresses confirmed to be dynamic IP address (or listed in an IP address list provided from the sender's ISP).

2. Legal problems

Specifically, a study is made to consider whether the above action causes the following issues.

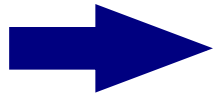
- Whether the action constitutes **the act of infringing on the secrecy of communications prescribed in Article 4 of the Telecommunications Business Act.**
- Whether the action constitutes **unfair discriminatory treatment prescribed in Article 6 of the Telecommunications Business Act.**

Conclusion

- IP25B corresponds to the act of infringing on the secrecy of communications prescribed in Article 4 of the Telecommunications Business Act. The reason is that it is a measure to check each sender's IP address and port number of each email as a component of the communication and block the email according to the result.
- However, if the following facts are present, it can be considered that IP25B is recognized as a legitimate business practice and its illegality is restrained.
 - 1) There is almost no massive transmission from the static IP addresses of other ISPs.
 - 2) There is massive email transmission from the dynamic IP addresses of other ISPs.
 - 3) The uniform rate control for the entire traffic is insufficient as a prevention measure for mass transmission.
- IP25B rejects emails that meet certain conditions, where the infringement of the secrecy of communications (using the secrecy of communications against the will of the senders or receivers) is allowed as a legitimate business practice. As long as it is applied to specific parties, it is not considered to be unfair discriminatory treatment prohibited by Article 6 of the Telecommunications Business Act.
- As described above, legal issues over IP25B can be cleared. Therefore, ISPs' proactive introduction of the same is desirable.

Study on Infringement of Secrecy of Communications (1)

The act of an ISP's detection of the IP address and port number of the sender of each email passing through the router under the ISP's control and management and single out and block emails transmitted directly through other mail servers to port 25 from dynamic IP addresses **falls under the infringement of the secrecy of communications. That is, the use of the secrecy of communications against the will of the sender or receiver.**



IP25B corresponds to the act of infringement of the secrecy of communications unless there is consent of the parties.

The act falls under the infringement of the secrecy of communications (i.e., the act of an ISP's detection of the IP address and port number of the sender of each email passing through the router under the ISP's control and management and single out and block emails transmitted directly through other mail servers to port 25 from dynamic IP addresses) **However, will be permitted regardless of the consent of the communications parties if there are grounds for restraining illegality (e.g., legal self-defense, emergency evacuation, or legitimate business conduct).**

1. Legitimate self-defense and emergency evacuation relevance

IP25B is a **measure** to prevent trouble in email transmission and reception and **always taken** regardless of whether trouble in email transmission and reception as a result of the mass transmission of emails is imminent or not.

For this reason, it does not always satisfy the conditions of legitimate self-defense or emergency evacuation, and cases that **do not correspond to legitimate self-defense or emergency evacuation are assumed.**

2. Legitimate appropriateness of business conduct

Legitimate business conduct needs to satisfy (1) the legitimacy and necessity of the conduct (2) the appropriateness of the means.

(1) Justification and necessity of actions

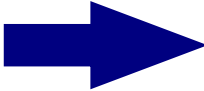
- There is almost no massive transmission from the static IP addresses of other ISPs.
- There is massive email transmission from the dynamic IP addresses of other ISPs.
- The uniform rate control for the entire traffic is insufficient as a prevention measure for mass transmission.

If the above facts are present, it can be considered that the necessity and validity of transmission control of emails from dynamic IP addresses not via the mail server of the ISP is recognized as a legitimate business practice in order to properly maintain and manage the network and operate the mail service.

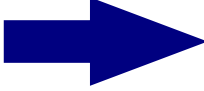
(2) Necessity of means

- IP25B infringes on the sender's route information on the IP address and port number, which, however, does not exceed the necessary limit of the purpose.
- A number of other measures (e.g., sender domain authentication and OP25B) are taken. IP25B, which is a countermeasure taken by the ISP on the receiving side for preventing transmission of unsolicited emails on the Internet, is considered to be an appropriate and necessary method for the attainment of the goal of proper management of email service.

Accordingly, **for the achievement of the purpose, it is considered a necessary and appropriate method for each ISP to check the IP address and port number of the sender of each email passing through the router under the ISP's control and management and single out and block emails transmitted directly through other mail servers to port 25 from dynamic IP address.**



IP25B can be interpreted as a legitimate business practice (with grounds for restraining illegality).



Furthermore, if it is implemented uniformly as a measure permitted as a legitimate business practice, it does not fall under the scope of unfair discriminatory treatment prescribed in Article 6 of the Telecommunications Business Act.