**Check Maillog**

**1. Mail log site access**

| 1) Search the domain on the customer inquiry site  2) Check the server IP or host of the domain  3) In the Internet URL search bar  Server IP or host/hanbiro\_mrtg/maillog search  ex) 211.234.116.225/hanbiro\_mrtg/maillog or mail1.hanbiro.com/hanbiro\_mrtg/maillog  -Mail log site can only be accessed from office IP (112.223.124.139) and VPN IP (222.231.27.246)  **Reset**: Reset search results  **Excel Download**: Search results can be saved in Excel file format.    You can search for results (success/delay/failure), date, title, sender, and recipient.  In the case of a log, you can check the log by clicking the document shape display under the content on the right. |
| --- |

**2. Mail log**

| **-Receiving success log**  **1. INBOX**  If the log ends in INBOX at the end, the mail is sent to the inbox.    **2. ALIAS**  If the log ends with ALIAS at the end, the account is forwarded to the email set as a virtual account      **3. FORWARD**  If the log ends with FORWARD at the end, it will be forwarded to the forwarding mail set in the account.      Without saving during forwarding setup / Check after saving  When setting without saving, no mail is left and forwarded to the mail set for forwarding  **4. AUTO-SPLIT**  When checking the log, if it ends with AUTO-SPLIT at the end, the account is using the automatic classification function.  Receiving to the mailbox set for automatic classification      **5. HBWhite**  If registered on the white list, it will be sent to the inbox      **-Outgoing success log**  **Remote host said**: When sending mail, it is the information received from the receiving mail server.  The connection to the receiving mail server was successful.  If the log contains the message Remote host said 250 OK when sending mail successfully  If there is a corresponding success log, but it is not received by the receiving side, confirmation of the receiving side is required.      **-Outgoing failure**  When checking the mail failure log, for some reason through the part after the remote host said in the log  You can guess if it failed.  **1. When sending mail to an account that does not exist**      **2. When sending to an unknown domain**      **3. When rejected by the receiving side Sniper equipment**  If the receiving side is using spam filter equipment and is blocked by spam filter equipment            **4. SMTP connection failure**  If there is a problem with the recipient's mail server, IP is blocked by the recipient, or the network connection is unstable    **5. Mail format is wrong**  When the mail received from the recipient is blocked because the mail format is incorrect    **6. If the mail content is blocked by the recipient's receiving policy**    **-Receive failure**  **1.BANS**  When checking the log, if it ends with BANS at the end, use the Hanbiro receive blocking function to set the sending email address.      **2. SPF Blocking**  Mail receiving block when sending by altering to large portal domains such as Naver, Gmail, and Hanmail  -In case of successful reception but classified as spam  **1.BAYESIAN**  If it is classified as spam due to spam learning, the customer directly classified it as spam or the spam manager  Classified and automatically classified as spam due to accumulated learning data          **2. RBL**  Real-time Blocking List, which means a real-time blacklist. When mail is received, it is sent to KISA, senderbase, spamhaus, etc.  If the sender's IP is registered on the RBL site, it is classified as spam.  **3. VIRUS Spicious**  Suspicious virus e-mail attachment or link contains suspicious virus or executable files, or  If you include a word, it is classified as spam.    **3. VIRUS malicious url**  In case the mail contains a virus (malicious) url and is classified as spam mail    **4. file type block**  If a customer has set up to block receiving attachments, it is classified as spam when receiving an e-mail with a file of that extension attached.    **5. SPF**  When using Outlook, SMTP authentication is not checked, or when the sent address is altered to the currently used domain  Classified as spam |
| --- |