March 3, 2022
OVAL Corporation

To Our Valued Customers and Partners,

Subject: Suspicious Malware Emails

Thank you for your continuous support.

We would like to express our sincere apologies to customers and partners who have received malware emails appearing to be sent disguised as existing personnel of our group.

Since March 1, 2022, it has been revealed that suspicious emails have been sent from third parties disguised as our group and personnel.
We are currently working on an urgent investigation, but we recognize that there is a high possibility that information such as email address and email content has been exploited by "Emotet". If you have received any suspicious emails, there is a risk of computer malware infection or guidance to harmful sites, thus please make sure to ignore and delete the entire email. (Even if you open the email, make sure not to open attached files and delete the entire email.)

If you receive emails from our group personnel whose displayed name and email address do not match, or even if the displayed name and email address are correct, the sent email is from past, or if you find anything unusual in the content, please do not access links in the email or open attached files and confirm with us if the email was sent from our group or personnel.

Currently we are making investigations and working to prevent spread or secondary damage but in response to this event, we will further investigate the facts and strive to introduce effective measures to prevent spread of damage and recurrence. We will continue to strengthen information security measures.

We appreciate your kind understanding and cooperation.

With best regards.