CLAIMS

1. An AI-based mail management method comprising:

obtaining user information and information about malicious mails received by each user account;

training a previously generated artificial intelligence model with features of malicious mails received by each user account, based on the user information and the information about malicious mail;

providing diagnostic information about types of malicious mails received by a specific user by inputting an account of the specific user to the trained artificial intelligence model, wherein the diagnostic information is statistical information including a probability or percentage of receiving a plurality of types of malicious mail;

comparing the types of malicious mails according to the provided diagnostic information with the types of malicious mails actually received at a user account; and

modifying and refining a parameter included in the artificial intelligence model based on a result of the comparison.

2. The AI-based mail management method of claim 1, wherein the training comprises:

applying an input value indicating information about a plurality of users and information about malicious mails by each user, to an input neuron of the artificial intelligence model; and

determining a parameter value of a plurality of layers constituting the artificial intelligence model by feeding back an output value obtained as a result of the applying of the input value.

3. The AI-based mail management method of claim 1, further comprising

providing information about a solution to prevent reading of a malicious mail as the types of malicious mails to be received by the specific user is determined.

4. The AI-based mail management method of claim 1, wherein the user information comprises

at least one of occupation and age of a user, and

the malicious mail information comprises

at least one of the types of malicious mails, detection of a malicious mail, and information about damage due to a malicious mail.

5. The AI-based mail management method of claim 1, wherein the types of malicious mails comprise

at least one of mail address misrepresentation, similar domain use, header forgery and alteration, and malicious code insertion.

6. The AI-based mail management method of claim 1, further comprising:

assigning each of a plurality of mails received at at least one user account to a plurality of virtual areas that are predefined; and

dynamically controlling the assigning of resources needed for detecting malicious mails in each of the plurality of virtual areas.

7. An AI-based mail management apparatus comprising:

a communicator configured to obtain user information and information about malicious mails received by each user account;

a memory storing a previously generated artificial intelligence model; and

a processor configured to train the artificial intelligence model with features of malicious mails received by each user account based on the user information and the information about malicious mail, and providing diagnostic information about the types of malicious mails to be received by a specific user by inputting an account of the specific user to the trained artificial intelligence model,

wherein the diagnostic information is statistical information including a probability or percentage of receiving a plurality of types of malicious mail,

wherein the processor is further configured to:

compare the types of malicious mails according to the provided diagnostic information with the types of malicious mails actually received at a user account, and

modify and refine a parameter included in the artificial intelligence model based on a result of the comparison.

8. The AI-based mail management apparatus of claim 7, wherein the processor is further configured to:

apply an input value indicating information about a plurality of users and information about malicious mails by each user, to an input neuron of the artificial intelligence model; and

determine a parameter value of a plurality of layers constituting the artificial intelligence model by feeding back an output value obtained as a result of the applying of the input value.

9. The AI-based mail management apparatus of claim 7, wherein the processor is further configured to

provide information about a solution to prevent reading of a malicious mail as the types of malicious mails to be received by the specific user is determined.

10. The AI-based mail management apparatus of claim 7, wherein the user information comprises

at least one of occupation and age of a user, and

the malicious mail information comprises

at least one of the types of malicious mails, detection of a malicious mail, and information about damage due to a malicious mail.

11. The AI-based mail management apparatus of claim 7, wherein the types of malicious mails comprise

at least one of mail address misrepresentation, similar domain use, header forgery and alteration, and malicious code insertion.

12. The AI-based mail management apparatus of claim 7, wherein the processor is further configured to:

assign each of a plurality of mails received at at least one user account to a plurality of virtual areas that are predefined; and

dynamically control the assigning of resources needed for detecting malicious mails in each of the plurality of virtual areas.

13. A non-transitory computer readable recording medium having recorded thereon a program for executing the method defined in claim 1.