

[CLAIMS]

[Claim 1]

A method of blocking access of a threatening user, the method comprising:

(a) executing an application on a user terminal;

5 (b) collecting, by the user terminal, access information and transmitting the access information to a server unit;

(c) determining, by the server unit, whether a user is a target whose access is to be blocked on the basis of the access information , wherein step (c) comprises:

10 (c1) storing, by the server unit, the access information transmitted from the user terminal; and

(c2) determining, by the server unit, whether the user is a target whose access is to be blocked on the basis of the access information, and wherein when it is determined in step (c2) that the user is not the target whose access is to be blocked, step (c) further comprises:

15 (c3) detecting, by the server unit, hacking threats;

(c4) counting hacking threat detections; and

(c5) determining whether a threat detection count is included in a preset access block value, and an administrator sets the preset access block value according to the threat detection count;

20 (d) transmitting, by the server unit, a normal execution code or a blocking message to the user terminal according to a result of the determination; and

(e) executing the user terminal according to the normal execution code or the blocking message.

[Claim 2]

25 The method of claim 1, wherein step (b) comprises:

(b1) collecting the access information including information on the user terminal or information on a user who possesses the user terminal; and

(b2) transmitting the access information to the server unit.

[Claim 3]

The method of claim 1, wherein, when it is determined in step (c2) that the user is the target whose access is to be blocked, (d) is performed to transmit the blocking message.

[Claim 4]

5 The method of claim 1, wherein, when the server unit detects no hacking threat in step (c5), step (d) is performed to transmit the normal execution code.

[Claim 5]

 The method of claim 1, wherein, when it is determined in step (c5) that the threat detection count is included in the preset access block value, step (d) is
10 performed to transmit the blocking message.

[Claim 6]

 The method of claim 1, wherein, when it is determined in step (c5) that the threat detection count is not included in the preset access block value, step (d) is performed to transmit the blocking message.

15 [Claim 7]

The method of claim 1, wherein step (d) comprises:

(d1) transmitting, by the server unit, the blocking message to the user terminal; and

(d2) transmitting, by the server unit, the normal execution code to the user terminal.

[Claim 8]

The method of claim 1, wherein step (e) comprises:

(e1) receiving, by the user terminal, the blocking message or the normal execution code from the server unit; and

(e2) determining whether the user terminal has received the normal execution code.

[Claim 9]

The method of claim 8, wherein, when it is determined in step (e2) that the user terminal has received the normal execution code, step (e) further comprises (e3) allowing access of the user terminal.

[Claim 10]

The method of claim 8, wherein, when it is determined in step (e2) that the user terminal has not received the normal execution code, step (e) further comprises (e4) outputting a threat detection message.

20

