[DESCRIPTION]

[Title of Invention]

AUTHENTICATION APPARATUS, AUTHENTICATION SYSTEM, AND AUTHENTICATION METHOD

[Technical Field]

[0001]

The present invention relates to an authentication apparatus, an authentication system, and an authentication method for performing authentication of a user in an online system or the like and, particularly, to an authentication apparatus, an authentication system, and an authentication method for performing risk-based authentication.

[Background Art]

[0002]

Services for purchasing articles and performing transactions at financial institutions such as banks via the Internet have been provided. Conventionally, a method of authenticating a user by receiving an ID and a password from the user has been employed. However, passwords are readily intercepted by a third party and carry a high risk of impersonation by a wrongdoer. Therefore, techniques are being proposed for increasing authentication strength by combining a password-based authentication method with an authentication method using biological information, an authentication method using an IC card, an authentication method using a hardware token, and the like.

[0003]

A risk-based authentication method is proposed which determines an identity of a user by acquiring information such as types of an OS and a browser, an IP address, a location of use, and an access time slot of an access source terminal and analyzing and modeling fragmentary behavioral patterns of the user. With a risk-based authentication method, a behavioral pattern of a user is analyzed based on an access log of at the time of login and the like, a risk value of each transaction is calculated, and an authentication method or an authentication strength is changed in accordance with a risk level based on a policy of a service provider.

[0004]

As an authentication system adopting such a risk-based authentication method, PTL 1 discloses an authentication system in which business servers of a plurality of corporations share an authentication server which performs risk-based authentication.

[0005]

PTL 2 discloses a risk-based authentication system including: an authentication server which performs rule analysis, behavioral analysis, and policy application in accordance with an authentication rule and which evaluates a risk level of a target access; and a risk information acquisition server which regularly acquires risk information on the Internet from an external server and which updates the authentication rule on the authentication server based on acquired risk information, wherein a risk level evaluation result is changed in accordance with a change in risk information and, accordingly, a determination level of executing

additional authentication is changed.

[Citation List]

[Patent Literature]

[0006]

[PTL 1]

Japanese Patent Application Publication No. 2011-215753

[PTL 2]

Japanese Patent No. 5191376

[Summary of Invention]

[Technical Problem]

[0007]

With the conventional risk-based authentication system described above, an authentication rule is not updated unless new risk information is acquired from an external server. Therefore, even if there is an authentication request that is strongly suspected of being fraudulent or the like, the authentication request cannot be immediately reflected in the authentication rule (a risk determination condition).

[0008]

The present invention has been made in consideration of the conventional circumstances described above and an object thereof is to provide an authentication apparatus, an authentication system, and an authentication method which updates a risk determination condition based on a suspicious authentication request.

[Solution to Problem]

[0009]

An authentication apparatus according to a first invention includes: a risk determination table which stores a risk determination condition for calculating a risk level of an access from a user to a business apparatus; a determination unit which receives access information of the user and an inquiry about an authentication type from the business apparatus, which determines the risk level of the access based on the access information and the risk determination condition, and which identifies the authentication type with respect to the user based on the risk level; a first response unit which responds to the business apparatus with the authentication type identified by the determination unit; an authentication processing unit which receives a user-input password in accordance with the authentication type and an authentication request from the business apparatus and performs an authentication process of the user based on the user-input password; a second response unit which responds to the business apparatus with an authentication result by the authentication processing unit; an update condition table which stores an update condition for updating the risk determination condition; and an update unit which updates the risk determination condition when the authentication request from the business apparatus satisfies the update condition.

[0010]

Favorably, the authentication apparatus according to the first invention further includes an authentication history table which stores an authentication request received from the business apparatus and an authentication result corresponding to the

authentication request, wherein the update unit compares a plurality of authentication requests and authentication results stored in the authentication history table with the update condition.

[0011]

Favorably, in the authentication apparatus according to the first invention, the risk determination condition includes an IP address list describing at least one IP address, the access information includes an IP address of the user, the authentication request includes a user ID and the IP address of the user, the determination unit detects whether or not an IP address included in the access information is described in the IP address list and, when the IP address is described, calculates a higher risk level than when the IP address is not described, and when a prescribed number or more of authentication requests with a same IP address and different user IDs are stored in the authentication history table within a prescribed time, the update unit adds the IP address to the IP address list.

[0012]

Favorably, the authentication apparatus according to the first invention further includes a second determination unit which searches the risk determination table based on a user ID included in the authentication request, wherein the risk determination condition includes a user ID list describing at least one user ID, the authentication request includes process contents requested by the user, the second determination unit detects whether or not a

user ID included in the authentication request is described in the user ID list and, when the user ID is described, notifies the authentication processing unit, the authentication processing unit determines an authentication result to be a failure based on the notification from the second determination unit, and when a prescribed number or more of authentication requests with prescribed process contents and a same user ID are stored in the authentication history table within a prescribed time, the update unit adds the user ID to the user ID list.

[0013]

An authentication system according to a second invention includes: a first authentication apparatus which receives first access information of a user and an inquiry about an authentication type from a first business apparatus, determines a first risk level of an access from the user to the first business apparatus, identifies an authentication type with respect to the user based on the first risk level and responds to the first business apparatus, receives a user-input password in accordance with the authentication type and an authentication request from the first business apparatus, performs an authentication process of the user based on the user-input password, and responds to the first business apparatus with an authentication result; a second authentication apparatus which receives second access information of the user and an inquiry about an authentication type from a second business apparatus, determines a second risk level of an access from the user to the second business apparatus, identifies an authentication type with

respect to the user based on the second risk level and responds to the second business apparatus, receives a user-input password in accordance with the authentication type and an authentication request from the second business apparatus, performs an authentication process of the user based on the user-input password, and responds to the second business apparatus with an authentication result; and a common risk determination table which stores a common risk determination condition for calculating a risk level of an access from the user to the first business apparatus or the second business apparatus, wherein the first authentication apparatus includes a first update condition table storing a first update condition for updating the common risk determination condition, determines the first risk level based on the first access information and the common risk determination condition, and updates the common risk determination condition when the authentication request from the first business apparatus satisfies the first update condition, and the second authentication apparatus includes a second update condition table storing a second update condition for updating the common risk determination condition, determines the second risk level based on the second access information and the common risk determination condition, and updates the common risk determination condition when the authentication request from the second business apparatus satisfies the second update condition.

[0014]

Favorably, in the authentication system according to the second

invention, the first authentication apparatus includes an individual risk determination table storing an individual risk determination condition for calculating a risk level of an access from the user to the first business apparatus, the first update condition table stores a third update condition for updating the individual risk determination condition, and the first authentication apparatus updates the individual risk determination condition when the authentication request from the first business apparatus satisfies the third update condition.

[0015]

An authentication method according to a third invention is an authentication method by an authentication apparatus including a risk determination table which stores a risk determination condition for calculating a risk level of an access from a user to a business apparatus, a determination unit, a first response unit, an authentication processing unit, a second response unit, an update condition table which stores an update condition for updating the risk determination condition, and an update unit, the authentication method including the steps of: causing the determination unit to receive access information of the user and an inquiry about an authentication type from the business apparatus, determine the risk level of the access based on the access information and the risk determination condition, and identify the authentication type with respect to the user based on the risk level; causing the first response unit to respond to the business apparatus with the authentication type identified by the determination unit;

causing the authentication processing unit to receive a user-input password in accordance with the authentication type and an authentication request from the business apparatus to perform an authentication process of the user based on the user-input password; causing the second response unit to respond to the business apparatus with an authentication result by the authentication processing unit; and causing the update unit to update the risk determination condition when the authentication request from the business apparatus satisfies the update condition.

[0016]

An authentication method according to a fourth invention is an authentication method by a common risk determination table which stores a common risk determination condition for calculating a risk level of an access from a user to a first business apparatus or a second business apparatus, a first authentication apparatus including a first update condition table which stores a first update condition for updating the common risk determination condition, and a second authentication apparatus including a second update condition table which stores a second update condition for updating the common risk determination condition, the authentication method comprising: causing the first authentication apparatus to execute the steps of: receiving first access information of a user and an inquiry about an authentication type from the first business apparatus, determining a first risk level of an access from the user to the first business apparatus based on the first access information and the common risk determination condition, and

identifying an authentication type with respect to the user based on the first risk level; responding to the first business apparatus with the identified authentication type; receiving a user-input password in accordance with the authentication type and an authentication request from the first business apparatus and performing an authentication process of the user based on the user-input password; responding to the first business apparatus with an authentication result; and updating the common risk determination condition when the authentication request from the first business apparatus satisfies the first update condition, and causing the second authentication apparatus to execute the steps of: receiving second access information of the user and an inquiry about an authentication type from the second business apparatus, determining a second risk level of an access from the user to the second business apparatus based on the second access information and the common risk determination condition, and identifying an authentication type with respect to the user based on the second risk level; responding to the second business apparatus with the identified authentication type; receiving a user-input password in accordance with the authentication type and an authentication request from the second business apparatus and performing an authentication process of the user based on the user-input password; responding to the second business apparatus with an authentication result; and updating the common risk determination condition when the authentication request from the second business apparatus satisfies the second update condition.

[Advantageous Effects of Invention]

[0017]

According to the present invention, since an update unit compares an authentication request from a business apparatus with an update condition stored in an update condition table and updates a risk determination condition when the update condition is satisfied, the risk determination condition can be immediately updated based on an authentication request from a business server which accompanies a processing request from a user. In addition, since an authentication request from a business apparatus is used to determine whether or not to update a risk determination condition, the risk determination condition can be promptly updated without having to acquire new risk information from an external server and a security level of user authentication can be increased.

[Brief Description of Drawings]

[0018]

[Fig. 1]

Fig. 1 is a configuration diagram of an authentication system according to an embodiment of the present invention.

[Fig. 2]

Fig. 2 is a diagram showing an example of an access history table.

[Fig. 3]

Fig. 3 is a diagram showing an example of a risk determination update condition table.

[Fig. 4]

Fig. 4 is a diagram showing a hardware configuration example of

a server.

[Fig. 5]

Fig. 5 is a sequence diagram of an authentication process according to a present embodiment.

[Fig. 6]

Fig. 6 is a configuration diagram of an authentication system according to a first modification.

[Fig. 7]

Fig. 7 is a configuration diagram of an authentication system according to a second modification.

[Fig. 8]

Fig. 8 is a diagram showing flows of a risk level calculation process and a risk determination table updating process.

[Fig. 9]

Fig. 9 is a diagram showing an example of a risk determination update condition table.

[Description of Embodiment]

[0019]

Hereinafter, an embodiment of the present invention will be described in detail.

[0020]

Fig. 1 is a configuration diagram of an authentication system according to an embodiment of the present invention. As shown in Fig. 1, the authentication system includes a business server 1 and an authentication server 2. A user operates a user terminal 3 to access the business server 1 and use a service provided by the

business server 1. In response to a request from the business server 1, the authentication server 2 performs personal authentication based on risk-based authentication with respect to a user of the user terminal 3 having accessed the business server 1 and notifies an authentication result to the business server 1 being the request source.

[0021]

The user terminal 3 is coupled to the business server 1 via a network 4 such as the Internet. For example, the user terminal 3 is a personal computer, a tablet terminal, a smart phone, a mobile phone, or an intelligent home appliance, includes an input unit for receiving various input (a login ID, a password, and the like) from the user, a display unit for displaying various types of information, and a communicating unit for coupling the network 4, and has similar functionality to a browser.

[0022]

The business server 1 includes a business processing unit 11, an authentication type inquiry unit 12, and an authentication request unit 13.

[0023]

When there is an access from the user terminal 3, the business processing unit 11 acquires an access source IP address and terminal information of the user terminal 3. Terminal information will be described later. When a process requiring authentication is requested from the user terminal 3, the business processing unit 11 transmits an authentication screen in accordance with an

authentication type identified by the authentication server 2 to the user terminal 3. In this case, an authentication type refers to a type of authentication method with respect to the user of which examples include password authentication using a fixed password and two-factor authentication which combines password authentication with hardware token authentication. When the authentication type is two-factor authentication, the authentication screen includes an input field for inputting a fixed password and an input field for inputting a password displayed on a hardware token. When the process requiring authentication is a login process, the authentication screen also includes an input field for a user ID. An identification method of an authentication type by the authentication server 2 will be described later.

[0024]

When authentication by the authentication server 2 is a success and the user operating the user terminal 3 is determined as a legitimate user, the business processing unit 11 executes processing of a transaction by performing a prescribed business process and responding to the user terminal 3 with a processing result. On the other hand, when authentication by the authentication server 2 is a failure, the business processing unit 11 notifies the user terminal 3 of an authentication failure and once again transmits an authentication screen to the user terminal 3.

[0025]

When there is an access from the user terminal 3, in preparation

of a login process from a user, the authentication type inquiry unit 12 transmits the access source IP address and the terminal information of the user terminal 3 acquired by the business processing unit 11 to the authentication server 2 and inquires about an authentication type corresponding to the login process of the user. When a process requiring authentication is requested from the user terminal 3 after login, the authentication type inquiry unit 12 transmits the access source IP address and the requested process to the authentication server 2 and inquires about an authentication type corresponding to the process requested by the user. The authentication type inquiry unit 12 acquires an authentication type identified by the authentication server 2 in response to the inquiry.

[0026]

When a password input by the user to the authentication screen of the user terminal 3 is notified from the user terminal 3, the authentication request unit 13 transmits the user-input password, a user ID, and an IP address to the authentication server 2 and requests an authentication process. The authentication request unit 13 acquires an authentication result from the authentication server 2.

[0027]

The authentication server 2 includes a risk determination unit 21, an authentication type response unit 22, a risk determination table 23, an authentication processing unit 24, a risk determination update unit 25, an authentication result response unit 26, an

authentication table 27, an authentication history table 28, and a risk determination update condition table 29.

[0028]

The risk determination unit 21 identifies an authentication type corresponding to a login process by the user or a process requested by the user to the business server 1 in response to an inquiry from the authentication type inquiry unit 12 of the business server 1. The risk determination unit 21 calculates a risk level based on access information such as the IP address and the terminal information received from the business server 1 together with the authentication type inquiry and on a risk determination condition registered in the risk determination table 23, and identifies an authentication type.

[0029]

The risk determination condition registered in the risk determination table 23 is a condition used when calculating a risk level of an access from the user terminal 3. For example, access history and terminal information at the time of access such as shown in Fig. 2 are registered in an access history table (not shown), and the risk determination unit 21 analyzes a past behavioral pattern of the user from the access history and the terminal information, compares the past behavioral pattern with access information received from the business server 1 based on the risk determination condition, and calculates a risk level. In this case, access history includes access date and time, an IP address of an access source, and the like. Terminal information includes OS

information indicating an OS or a browser running on the user terminal 3, browser information such as a browser version or a language setting, and CPU information indicating a CPU mounted to the user terminal 3.

[0030]

When a degree of matching between the access information received from the business server 1 and the past behavioral pattern is high, the risk level is low, and when the degree of matching is low, the risk level is high.

[0031]

In the risk determination table 23, an IP address list describing IP addresses that are highly likely to be wrongdoers and a conditional expression that determines a high risk level when the user’s IP address received from the business server 1 matches an IP address in the IP address list are registered as a risk determination condition.

[0032]

The risk determination unit 21 identifies an authentication type with respect to the user based on the calculated risk level. For example, the risk determination unit 21 calculates three risk levels from level 1 to level 3, identifies password authentication as the authentication type in the case of level 1 (low risk), identifies two-factor authentication as the authentication type in the case of level 2, and determines to block an authentication process (authentication disabled) in the case of level 3 (high risk).

[0033]

The authentication type response unit 22 notifies the business server 1 of the authentication type identified by the risk determination unit 21.

[0034]

The authentication processing unit 24 receives a user-input password, a user ID, an IP address, and the like together with an authentication request from the authentication request unit 13 of the business server 1. A fixed password of a user, a calculation formula for a one-time password, and the like are registered in the authentication table 27, and the authentication processing unit 24 uses the information to determine whether or not the password received from the business server 1 is legitimate. Authentication is a success when the password received from the business server 1 is legitimate and a failure when the password is not legitimate.

[0035]

When the authentication processing unit 24 receives an authentication request from the authentication request unit 13, the authentication processing unit 24 registers the user ID and the IP address, contents of the process requested from the user, and an authentication result in the authentication history table 28. Authentication requests received from the authentication request unit 13 within a prescribed time and authentication results with respect to the authentication requests are registered in the authentication history table 28.

[0036]

The authentication result response unit 26 responds to the business

server 1 with an authentication result by the authentication processing unit 24.

[0037]

The risk determination update unit 25 refers to the risk determination update condition table 29 based on an authentication request and an authentication result registered in the authentication history table 28 and determines whether or not to update the risk determination condition in the risk determination table 23. An update condition for updating the risk determination condition and an update process to be performed when the update condition is satisfied are registered in the risk determination update condition table 29. Every time an authentication process is performed by the authentication processing unit 24, the risk determination update unit 25 checks whether an authentication request satisfying the update condition registered in the risk determination update condition table 29 is not performed and, when performed, immediately executes a corresponding update process.

[0038]

Fig. 3 shows an example of registered contents of the risk determination update condition table 29. For example, when authentication requests with respect to X1 (where X1 is an integer equal to or larger than 2) or more of user IDs are made from a same IP address within a prescribed time and all of the authentication requests result in an authentication failure, the risk determination update unit 25 determines that it is highly likely that the IP address belongs to a wrongdoer, immediately adds the

IP address to the IP address list in the risk determination table 23, and updates the risk determination condition.

[0039]

When authentication requests with respect to X2 (where X2 is an integer larger than X1) or more of user IDs are made from a same IP address within a prescribed time, even if there is an authentication process that results in an authentication success, the risk determination update unit 25 immediately adds the IP address to the IP address list in the risk determination table 23 and updates the risk determination condition. This is because, conceivably, a wrongdoer had made authentication requests with respect to a large number of user IDs and there is an authentication process of which a password had matched by coincidence.

[0040]

As the business server 1 and the authentication server 2 described above, a computer including a CPU (central processing unit) 401, a main memory 402, a network interface 403, and a non-volatile storage apparatus 404 as shown in Fig. 4 can be respectively used. For example, the non-volatile storage apparatus 404 is an HDD (hard disk drive) or an SDD (solid state drive) and stores a program to be executed by the CPU 401. The respective functions of the business server 1 and the authentication server 2 are realized as the CPU 401 loads the program stored in the non-volatile storage apparatus 404 to the main memory 402 and executes the program.

[0041]

Next, an authentication process by the authentication system

according to the present embodiment will be described with reference to the sequence diagram shown in Fig. 5. In Fig. 5, an authentication process accompanying a login by a user and an authentication process when a process requiring authentication is requested after login will be described.

[0042]

[Step S101] The user operates the user terminal 3 and accesses the business server 1. At this point, the business processing unit 11 acquires an access source IP address and terminal information of the user terminal 3.

[0043]

[Step S102] The authentication type inquiry unit 12 of the business server 1 inquires the authentication server 2 about a type of an authentication process to be performed with respect to a login process of the user. At this point, the authentication type inquiry unit 12 transmits access information including the access source IP address and the terminal information acquired in step S101 to the authentication server 2.

[0044]

[Step S103] In response to the inquiry from the authentication type inquiry unit 12, the risk determination unit 21 of the authentication server 2 calculates a risk level of the access from the user and identifies a type of an authentication process in accordance with the risk level.

[0045]

For example, the risk determination unit 21 compares the present

access from the user with a past behavioral pattern of the user based on access history and terminal information registered in the access history table, and calculates a risk level based on a comparison result. In addition, for example, the risk determination unit 21 detects whether or not an access source IP address of the present access from the user is included in the IP address list registered in the risk determination table 23 and, when included, increases the risk level.

[0046]

Furthermore, the risk determination unit 21 identifies a type of an authentication process based on the calculated risk level. For example, the risk determination unit 21 identifies password authentication using a fixed password as the authentication type.

[0047]

[Step S104] The authentication type response unit 22 notifies the business server 1 of the authentication type identified by the risk determination unit 21.

[0048]

[Step S105] The business processing unit 11 of the business server 1 transmits an authentication screen in accordance with the authentication type identified by the authentication server 2 to the user terminal 3.

[0049]

[Step S106] The user inputs a user ID and a password to the authentication screen of the user terminal 3. The input user ID and password are notified to the business server 1 from the user

terminal 3. For example, the user inputs a memorized fixed password.

[0050]

[Step S107] When a password is notified from the user terminal 3, the authentication request unit 13 of the business server 1 transmits the password together with a user ID and an IP address to the authentication server 2 and makes an authentication request.

[0051]

[Step S108] The authentication processing unit 24 of the authentication server 2 performs an authentication process in accordance with the authentication request from the business server 1. Specifically, the authentication processing unit 24 collates a password registered in the authentication table 27 with the password received from the business server 1 together with the authentication request and determines a match/mismatch of a collation result. When the collation result is a match, a determination that the access is from a legitimate user is made and the authentication succeeds. When the authentication is a success, the authentication processing unit 24 registers an access date and time, an IP address, terminal information, and the like of the present access in the access history table. On the other hand, when the collation result does not match, the authentication fails. The example shown in Fig. 5 assumes that a login process has succeeded.

[0052]

When the authentication processing unit 24 receives an

authentication request, the authentication processing unit 24 registers the user ID and the IP address, contents of the process requested from the user (in this case, a login process), and the authentication result in the authentication history table 28.

[0053]

[Step S109] The authentication result response unit 26 responds to the business server 1 with the result of the authentication process by the authentication processing unit 24.

[0054]

When the authentication is a success, the business processing unit 11 of the business server 1 executes a login process of the user. On the other hand, when the authentication is a failure, the business processing unit 11 notifies the user terminal 3 of an authentication failure and once again transmits an authentication screen to the user terminal 3.

[0055]

[Step S110] The risk determination update unit 25 refers to the risk determination update condition table 29 based on the authentication request and the authentication result registered in the authentication history table 28 and determines whether or not to update the risk determination condition in the risk determination table 23. When the update condition is satisfied, the risk determination update unit 25 immediately performs an update process of the risk determination table 23.

[0056]

For example, when authentication requests with respect to X2 or

more of user IDs from a same IP address are registered in the authentication history table 28 within a prescribed time, the risk determination update unit 25 immediately adds the IP address to the IP address list in the risk determination condition and updates the risk determination condition. The updated risk determination condition is used for subsequent calculations of risk levels by the risk determination unit 21.

[0057]

[Step S111] After login, the user operates the user terminal 3 and requests a process that requires authentication.

[0058]

[Step S112] When a process that requires authentication is requested from the user terminal 3, the authentication type inquiry unit 12 of the business server 1 inquires the authentication server 2 about a type of an authentication process to be performed. At this point, the authentication type inquiry unit 12 notifies the authentication server 2 of access information including an access source IP address and terminal information. The authentication type inquiry unit 12 may further notify the authentication server 2 of a user ID and the requested process.

[0059]

[Step S113] In response to the inquiry from the authentication type inquiry unit 12, the risk determination unit 21 of the authentication server 2 calculates a risk level of the access from the user and identifies a type of an authentication process in accordance with the risk level. The risk determination unit 21

calculates the risk level using the risk determination condition updated in step S110.

[0060]

A different risk level may be calculated in accordance with the process requested from the user. For example, when the business server 1 provides an Internet banking service, a higher risk level may be calculated for a transfer process as compared to a balance confirmation process.

[0061]

The risk determination unit 21 may detect whether or not the access source IP address of the present access from the user is included in the IP address list registered in the risk determination table 23 and, when included, increase the risk level.

[0062]

The risk determination unit 21 identifies a type of an authentication process based on the calculated risk level. For example, the risk determination unit 21 identifies two-factor authentication which combines password authentication with hardware token authentication as the authentication type.

[0063]

[Step S114] The authentication type response unit 22 notifies the business server 1 of the authentication type identified by the risk determination unit 21.

[0064]

[Step S115] The business processing unit 11 of the business server 1 transmits an authentication screen in accordance with the

authentication type identified by the authentication server 2 to the user terminal 3.

[0065]

[Step S116] The user inputs a password to the authentication screen of the user terminal 3. The input password is notified to the business server 1 from the user terminal 3. For example, the user inputs a memorized fixed password and a password displayed on a hardware token.

[0066]

[Step S117] When a password is notified from the user terminal 3, the authentication request unit 13 of the business server 1 transmits the password together with a user ID and an IP address to the authentication server 2 and makes an authentication request.

[0067]

[Step S118] The authentication processing unit 24 of the authentication server 2 performs an authentication process in accordance with the authentication request from the business server 1. Specifically, the authentication processing unit 24 collates a password registered in the authentication table 27 with the password received from the business server 1 together with the authentication request and determines a match/mismatch of a collation result. When the collation result is a match, a determination that the access is from a legitimate user is made and the authentication succeeds. On the other hand, when the collation result does not match, the authentication fails.

[0068]

When the authentication processing unit 24 receives an authentication request, the authentication processing unit 24 registers the user ID and the IP address, contents of the process requested from the user, and the authentication result in the authentication history table 28.

[0069]

[Step S119] The authentication result response unit 26 responds to the business server 1 with the result of the authentication process by the authentication processing unit 24.

[0070]

When the authentication is a success, the business processing unit 11 of the business server 1 executes processing of a transaction by performing a prescribed business process and responding to the user terminal 3 with a processing result. On the other hand, when the authentication is a failure, the business processing unit 11 notifies the user terminal 3 of an authentication failure and once again transmits an authentication screen to the user terminal 3.

[0071]

[Step S120] The risk determination update unit 25 refers to the risk determination update condition table 29 based on the authentication request and the authentication result registered in the authentication history table 28 and determines whether or not to update the risk determination condition in the risk determination table 23. When the update condition is satisfied, the risk determination update unit 25 immediately performs an update process of the risk determination table 23. The updated risk

determination condition is used for subsequent calculations of risk levels by the risk determination unit 21.

[0072]

When a process requiring authentication is once again requested from the user, a return is made to step S111.

[0073]

As described above, according to the present embodiment, a risk determination condition registered in the risk determination table 23 can be immediately updated based on an authentication request from the business server 1 accompanying a processing request from the user. For example, when a suspicious authentication request that is strongly suspected of being fraudulent or the like is made, the authentication request can be immediately reflected in the risk determination condition. Accordingly, even when a login process is completed based on a suspicious authentication request, since the risk determination condition is updated in real-time, the risk level can be raised and authentication strength can be increased when a process requiring authentication is subsequently requested. In addition, the risk determination condition can be updated in the authentication server 2 without having to acquire new risk information from an external server and a security level of user authentication can be increased.

[0074]

The authentication system according to the embodiment described above can be applied to, for example, Internet banking. The business server 1 corresponds to a business server of a bank. A

user accesses and logs into the business server 1 using the user terminal 3 and performs processes such as balance confirmation, transfer, and deposit. For example, when an authentication request accompanying login is suspicious, the authentication request matches a risk determination update condition, and the risk determination condition is updated in real-time, since an authentication type with high authentication strength is identified according to the updated risk determination condition with respect to a subsequent transfer process, the security level can be increased.

[0075]

[First modification]

Fig. 6 is a configuration diagram of an authentication system according to a first modification. The first modification differs from the embodiment shown in Fig. 1 in that a second risk determination unit 200 is provided in the authentication server 2. A high-risk user ID list describing user IDs highly suspected of being attacked by wrongdoers is registered in the risk determination table 23. In addition, an update condition and an update process for adding, when a prescribed process is performed a prescribed number of times in a certain time by a same user ID, the user ID to the high-risk user ID list are registered in the risk determination update condition table 29.

[0076]

The second risk determination unit 200 detects whether or not a user ID received together with an authentication request from the

authentication request unit 13 of the business server 1 is included in the high-risk user ID list and delivers a detection result to the authentication processing unit 24.

[0077]

When the user ID received together with the authentication request is included in the high-risk user ID list, the authentication processing unit 24 determines that the authentication is a failure even if the user-input password is legitimate. On the other hand, when the user ID received together with the authentication request is not included in the high-risk user ID list, the authentication processing unit 24 performs an authentication process and registers the authentication request and an authentication result in the authentication history table 28.

[0078]

The risk determination update unit 25 refers to the risk determination update condition table 29 based on the authentication request and the authentication result registered in the authentication history table 28 and determines whether or not to update the risk determination table 23 (the risk determination condition). When a prescribed process is performed a prescribed number of times in a certain time by a same user ID, the risk determination update unit 25 immediately adds the user ID to the high-risk user ID list in the risk determination table 23 and updates the risk determination condition.

[0079]

In this case, the prescribed process is, for example, a transfer

process of an upper-limit amount. When a transfer process of the upper-limit amount is repetitively performed in a short time, the process is highly suspected of being performed by a wrongdoer. Therefore, by adding the user ID to the high-risk user ID list in the risk determination table 23, having the second risk determination unit 200 detect whether or not a user ID received together with an authentication request is included in the high-risk user ID list prior to an authentication process for subsequent transfer processes, and notifying the authentication processing unit 24 of a detection result, illegal transfer processes can be prevented.

[0080]

[Second modification]

Figs. 7 to 9 represent a second modification. Fig. 7 is a configuration diagram of an authentication system according to the second modification. As shown in Fig. 7, the authentication system according to the second modification includes two business servers 1A and 1B, an authentication server 2A used by the business server 1A, an authentication server 2B used by the business server 1B, and a common authentication server 5 which is accessible from the authentication servers 2A and 2B. The business servers 1A and 1B have a similar configuration to the business server 1 according to the embodiment described earlier. In addition, the authentication servers 2A and 2B have a similar configuration to the authentication server 2 according to the embodiment described earlier.

[0081]

The common authentication server 5 includes a common risk determination table 51 which can be referred to and updated by the authentication servers 2A and 2B. A common risk determination condition used when calculating a risk level of an access from the user terminal 3 is registered in the common risk determination table 51. For example, in the common risk determination table 51, a high-risk IP address list describing IP addresses that are extremely likely to be wrongdoers and a conditional expression that determines that the risk level is extremely high when a user's IP address received from the business server 1A or 1B matches an IP address in the high-risk IP address list are registered as a common risk determination condition.

[0082]

Fig. 8 shows configurations of the authentication servers 2A and 2B and the common authentication server 5 in the authentication system shown in Fig. 7. In addition, Fig. 8 shows flows (flows of data) of a risk level calculation process and a risk determination table updating process by the authentication servers 2A and 2B.

[0083]

Risk determination units 21A and 21B, authentication type response units 22A and 22B, risk determination tables (individual risk determination tables) 23A and 23B, authentication processing units 24A and 24B, risk determination update units 25A and 25B, authentication result response units 26A and 26B, authentication tables 27A and 27B, authentication history tables 28A and 28B, and

risk determination update condition tables 29A and 29B of the authentication servers 2A and 2B respectively correspond to the risk determination unit 21, the authentication type response unit 22, the risk determination table 23, the authentication processing unit 24, the risk determination update unit 25, the authentication result response unit 26, the authentication table 27, the authentication history table 28, and the risk determination update condition table 29 of the authentication server 2 shown in Fig. 1.

[0084]

Fig. 9 shows an example of registered contents of the risk determination update condition tables 29A and 29B. For example, when authentication requests with respect to X1 (where X1 is an integer equal to or larger than 2) or more of user IDs are made from a same IP address within a prescribed time and all of the authentication requests result in an authentication failure, the risk determination update units 25A and 25B determine that it is highly likely that the IP address belongs to a wrongdoer, immediately add the IP address to the IP address list in the risk determination tables 23A and 23B, and update the risk determination condition.

[0085]

For example, when authentication requests with respect to X2 (where X2 is an integer larger than X1) or more of user IDs are made from a same IP address within a prescribed time and all of the authentication requests result in an authentication failure, the

risk determination update units 25A and 25B immediately add the IP address to the high-risk IP address list in the common risk determination table 51 and update the common risk determination condition.

[0086]

The threshold X1 of the update condition for updating a risk determination condition (an individual risk determination condition) of its own server may differ between the risk determination update condition table 29A and the risk determination update condition table 29B. This is because a required security level differs depending on the business server. When a high security level is required, the threshold X1 is set to a small value.

[0087]

Favorably, the update condition for updating the common risk determination condition of the common risk determination table 51 is the same with the risk determination update condition table 29A and the risk determination update condition table 29B. This is because the common risk determination table 51 is shared by a plurality of authentication servers and having the respective authentication servers update the common risk determination condition according to a same criterion (update condition) is more favorable than having each authentication server update the common risk determination condition according to its own criterion (update condition).

[0088]

As shown in Fig. 8, when there is an inquiry about an authentication

type from the business server 1A, the risk determination unit 21A of the authentication server 2A calculates a risk level of an access from a user by referring to the risk determination table 23A and the common risk determination table 51 and identifies a type of an authentication process in accordance with the risk level. For example, the risk determination unit 21A detects whether or not an access source IP address of the present access from the user is included in the high-risk IP address list registered in the common risk determination table 51 and, when included, increases the risk level to a highest level.

[0089]

The risk determination update unit 25A refers to the risk determination update condition table 28A based on the authentication request and the authentication result registered in the authentication history table 28A and determines whether or not to update the risk determination table 23A or the common risk determination table 51. When an update condition for updating the risk determination table 23A is satisfied, the risk determination update unit 25A immediately performs an update process of the risk determination table 23A. In addition, when a condition for updating the common risk determination table 51 is satisfied, the risk determination update unit 25A immediately performs an update process of the common risk determination table 51.

[0090]

The updated risk determination table 23A and the updated common risk determination table 51 are used for subsequent calculations

of risk levels by the risk determination unit 21A.

[0091]

Processes similar to the authentication server 2A are performed by the authentication server 2B.

[0092]

Risk determination conditions of the risk determination tables 23A and 23B are respectively updated by the risk determination update units 25A and 25B of their own servers. On the other hand, the common risk determination condition of the common risk determination table 51 is updated by the risk determination update units 25A and 25B. When calculating a risk level, the risk determination unit 21A of the authentication server 2A can refer to the common risk determination condition updated by the risk determination update unit 25B of the authentication server 2B. In addition, when calculating a risk level, the risk determination unit 21B of the authentication server 2B can refer to the common risk determination condition updated by the risk determination update unit 25A of the authentication server 2A.

[0093]

As described above, by providing the common risk determination table 51 which can be referred to and updated from the authentication servers 2A and 2B, when there is a processing request from a wrongdoer to one of the business servers 1A and 1B, information such as an IP address of the wrongdoer can be added to the common risk determination table 51 and shared by the authentication servers 2A and 2B. Since the common risk determination condition of the

common risk determination table 51 is updated by a plurality of authentication servers, latest information on wrongdoers is reflected and the security level of user authentication can be further increased.

[0094]

Since the authentication servers 2A and 2B respectively include the risk determination tables 23A and 23B, risk-based authentication according to individual conditions can be performed by referring to the risk determination tables 23A and 23B.

[0095]

When the authentication system shown in Figs. 7 and 8 is applied to Internet banking, the business servers 1A and 2B can be respectively regarded as a business server of a bank A and a business server of a bank B. When a suspicious authentication request is made from the bank A business server 1A to the authentication server 2A, the authentication server 2A adds an IP address of a user having accessed the bank A business server 1A to the common risk determination table 51 and updates the common risk determination condition in real-time. When a user with the same IP address accesses the bank B business server 1B, since the authentication server 2B can refer to the common risk determination condition updated by the authentication server 1A and identify an authentication type with high authentication strength with respect to a login process by the user, the security level can be increased. As described above, when a suspicious authentication request is made at a given bank, the information (an IP address of a user)

can be immediately used to calculate a risk level of authentication at other banks. Moreover, generally, while it is pointless from the perspective of the bank B to register a high-risk user ID of the bank A to the common risk determination table 51 since user IDs differ from one bank to another even for a same person, when a user accesses a plurality of bank business servers from a specific terminal, a common IP address is used regardless of which bank is accessed. Therefore, the effect produced by registering a high-risk IP address in the common risk determination table 51 is significant.

[0096]

In addition, since the authentication servers 2A and 2B respectively include the risk determination tables 23A and 23B, the banks A and B can independently configure risk determination conditions. In this manner, a risk determination condition independently configured by each bank and a common risk determination condition shared and updated by a plurality of bank can be applied in parallel.

[0097]

In the second modification described above, at least one of the authentication servers 2A and 2B may be configured by adding the second risk determination unit 200 described earlier. In addition, in at least one of the authentication servers 2A and 2B, the risk determination update unit 25A or 25B may be configured to only update the common risk determination condition of the common risk determination table 51 without updating the risk determination condition of the risk determination table 23A or 23B.

[0098]

While Figs. 7 and 8 show an example where two business servers and two authentication servers are provided, three or more business servers and three or more authentication servers may be provided and the three or more authentication servers may be configured to share the common risk determination table 51.

[0099]

Each of a plurality of business servers may be regarded as a business server corresponding to each transaction channel such as a personal computer, a mobile phone, and a smart phone. When a suspicious authentication request is made on a given transaction channel, the information (an IP address of a user or the like) can be immediately used to calculate a risk level of authentication on other transaction channels and the security level can be increased.

[0100]

At least a part of the authentication server 2 according to the embodiment described earlier may be configured by hardware or by software. When configured by software, a program realizing at least a part of the functions of the authentication server 2 may be housed in a recording medium such as a flexible disk and a CD-ROM to be read and executed by a computer. The recording medium is not limited to an attachable and detachable recording medium such as a magnetic disk and an optical disk and may be a fixed recording medium such as a hard disk apparatus and a memory.

[0101]

The program realizing at least a part of the functions of the

authentication server 2 may be distributed via a communication line (including wireless communication) such as the Internet. In addition, the program may be distributed via a wired line or a wireless line such as the Internet or distributed by being stored in a recording medium in an encrypted state, a modulated state, or a compressed state.

[0102]

The present invention is not limited to the embodiment described above and components may be modified when implementing the present invention without departing from the gist of the invention. In addition, a plurality of components disclosed in the embodiment described above may be combined with each other as appropriate or several components may be deleted from all components described in the embodiment. Furthermore, components of different embodiments may be combined with each other as appropriate.

[0103]

While the present invention has been described in detail in a specific aspect thereof, it will be obvious to those skilled in the art that various modifications may be made without departing from the spirit and scope of the present invention.

This application is based on, and claims priority from, Japanese Patent Application No. 2014-050476, filed March 13, 2014, the entire contents of which are incorporated herein by reference.

[Reference Signs List]

[0104]

1 Business server

2 Authentication server

3 User terminal

4 Network

11 Business processing unit

12 Authentication type inquiry unit

13 Authentication request unit

21 Risk determination unit

22 Authentication type response unit

23 Risk determination table

24 Authentication processing unit

25 Risk determination update unit

26 Authentication result response unit

27 Authentication table

28 Authentication history table

29 Risk determination update condition table

[CLAIMS]

[Claim 1]

An authentication apparatus, comprising:

a risk determination table configured to store a risk determination condition for calculating a risk level of an access from a user to a business apparatus;

a determination unit configured to receive access information of the user and an inquiry about an authentication type from the business apparatus, determine the risk level of the access based on the access information and the risk determination condition, and identify the authentication type with respect to the user based on the risk level;

a first response unit configured to respond to the business apparatus with the authentication type identified by the determination unit;

an authentication processing unit configured to receive a user-input password in accordance with the authentication type and an authentication request from the business apparatus and perform an authentication process of the user based on the user-input password;

a second response unit configured to respond to the business apparatus with an authentication result by the authentication processing unit;

an update condition table configured to store an update condition for updating the risk determination condition; and

an update unit configured to update the risk determination condition

when the authentication request from the business apparatus satisfies the update condition.

[Claim 2]

An authentication apparatus according to claim 1, further comprising an authentication history table configured to store an authentication request received from the business apparatus and an authentication result corresponding to the authentication request, wherein

the update unit is configured to compare a plurality of authentication requests and authentication results stored in the authentication history table with the update condition.

[Claim 3]

An authentication apparatus according to claim 2, wherein

the risk determination condition includes an IP address list describing at least one IP address,

the access information includes an IP address of the user,

the authentication request includes a user ID and the IP address of the user,

the determination unit is configured to detect whether or not an IP address included in the access information is described in the IP address list and, when the IP address is described, calculates a higher risk level than when the IP address is not described, and when a prescribed number or more of authentication requests with a same IP address and different user IDs are stored in the authentication history table within a prescribed time, the update unit adds the IP address to the IP address list.

[Claim 4]

An authentication apparatus according to claim 3, further comprising a second determination unit configured to search the risk determination table based on a user ID included in the authentication request, wherein

the risk determination condition includes a user ID list describing at least one user ID,

the authentication request includes process contents requested by the user,

the second determination unit is configured to detect whether or not a user ID included in the authentication request is described in the user ID list and, when the user ID is described, notifies the authentication processing unit,

the authentication processing unit is configured to determine an authentication result to be a failure based on the notification from the second determination unit, and

when a prescribed number or more of authentication requests with prescribed process contents and a same user ID are stored in the authentication history table within a prescribed time, the update unit adds the user ID to the user ID list.

[Claim 5]

An authentication system, comprising:

a first authentication apparatus configured to receive first access information of a user and an inquiry about an authentication type from a first business apparatus, determine a first risk level of an access from the user to the first business apparatus, identify

an authentication type with respect to the user based on the first risk level and respond to the first business apparatus, receive a user-input password in accordance with the authentication type and an authentication request from the first business apparatus, perform an authentication process of the user based on the user-input password, and respond to the first business apparatus with an authentication result;

a second authentication apparatus configured to receive second access information of the user and an inquiry about an authentication type from a second business apparatus, determine a second risk level of an access from the user to the second business apparatus, identify an authentication type with respect to the user based on the second risk level and respond to the second business apparatus, receive a user-input password in accordance with the authentication type and an authentication request from the second business apparatus, perform an authentication process of the user based on the user-input password, and respond to the second business apparatus with an authentication result; and

a common risk determination table configured to store a common risk determination condition for calculating a risk level of an access from the user to the first business apparatus or the second business apparatus, wherein

the first authentication apparatus includes a first update condition table configured to store a first update condition for updating the common risk determination condition, and is configured to determine the first risk level based on the first access

information and the common risk determination condition, and update the common risk determination condition when the authentication request from the first business apparatus satisfies the first update condition, and

the second authentication apparatus includes a second update condition table configured to store a second update condition for updating the common risk determination condition, and is configured to determine the second risk level based on the second access information and the common risk determination condition, and update the common risk determination condition when the authentication request from the second business apparatus satisfies the second update condition.

[Claim 6]

An authentication system according to claim 5, wherein

the first authentication apparatus includes an individual risk determination table configured to store an individual risk determination condition for calculating a risk level of an access from the user to the first business apparatus,

the first update condition table is configured to store a third update condition for updating the individual risk determination condition, and

the first authentication apparatus is configured to update the individual risk determination condition when the authentication request from the first business apparatus satisfies the third update condition.

[Claim 7]

An authentication method by an authentication apparatus including a risk determination table which stores a risk determination condition for calculating a risk level of an access from a user to a business apparatus, a determination unit, a first response unit, an authentication processing unit, a second response unit, an update condition table which stores an update condition for updating the risk determination condition, and an update unit, the authentication method comprising the steps of:

causing the determination unit to receive access information of the user and an inquiry about an authentication type from the business apparatus, determine the risk level of the access based on the access information and the risk determination condition, and identify the authentication type with respect to the user based on the risk level;

causing the first response unit to respond to the business apparatus with the authentication type identified by the determination unit;

causing the authentication processing unit to receive a user-input password in accordance with the authentication type and an authentication request from the business apparatus and perform an authentication process of the user based on the user-input password;

causing the second response unit to respond to the business apparatus with an authentication result by the authentication processing unit; and

causing the update unit to update the risk determination condition when the authentication request from the business apparatus satisfies the update condition.

[Claim 8]

An authentication method by a common risk determination table which stores a common risk determination condition for calculating a risk level of an access from a user to a first business apparatus or a second business apparatus, a first authentication apparatus including a first update condition table which stores a first update condition for updating the common risk determination condition, and a second authentication apparatus including a second update condition table which stores a second update condition for updating the common risk determination condition,

the authentication method comprising:

causing the first authentication apparatus to execute the steps of:

receiving first access information of a user and an inquiry about an authentication type from the first business apparatus,

determining a first risk level of an access from the user to the first business apparatus based on the first access information and the common risk determination condition, and identifying an authentication type with respect to the user based on the first risk level;

responding to the first business apparatus with the identified authentication type;

receiving a user-input password in accordance with the authentication type and an authentication request from the first business apparatus and performing an authentication process of the user based on the user-input password;

responding to the first business apparatus with an authentication result; and

updating the common risk determination condition when the authentication request from the first business apparatus satisfies the first update condition, and

causing the second authentication apparatus to execute the steps of:

receiving second access information of the user and an inquiry about an authentication type from the second business apparatus,

determining a second risk level of an access from the user to the second business apparatus based on the second access information and the common risk determination condition, and identifying an authentication type with respect to the user based on the second risk level;

responding to the second business apparatus with the identified authentication type;

receiving a user-input password in accordance with the authentication type and an authentication request from the second business apparatus and performing an authentication process of the user based on the user-input password;

responding to the second business apparatus with an authentication result; and

updating the common risk determination condition when the authentication request from the second business apparatus satisfies the second update condition.