

Personal authentication system of low load that anyone can use

PASSLOGIC authentication system



Passlogy Co., Ltd.



- Date of establishment: February 24, 2000
- Directors: Representative Director (president) Hideharu Ogawa
Vice president Noritsugu Kiyose
Director Mikiko Kajiwara
Director Yoshiyuki Uenishi
Director Yuichiro Ishii (patent attorney)
Director Keiko Yoshida (certified public accountant)
Auditor Motohiko Mitsuno
Auditor Kunio Namekata
- Capital: 137,500,000 yen
- Address of headquarters: 3-2-2 Ogawamachi Kanda Chiyoda-ku Tokyo
- Business duties: Security software development and sales
- Main business: Personal authentication technology: PASSLOGIC (Registered trademark)
Public authentication technology: Seamless Sign On (Registered trademark)
Single sign-on : ASP Core Base
Public authentication service: “PASSLOGI !” (Registered trademark)
- Main customer: Gaitame.Com Co., Ltd.
Fujitsu Ltd.
NTT Communications
Canon System Solutions Inc.
- Holding patent: Acquired: 2 (Japan 1 USA 1)
Applied: 15 (Japan 7 USA 3 Others (PCT) 5)

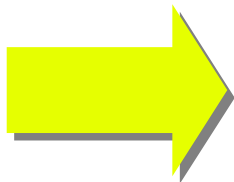


Users request stronger authentication.

- From ZDNet JAPAN "70 percent or more users want stronger authentication for online trading"
(2006/3/24 <http://japan.zdnet.com/news/sec/story/0,2000052528,20099271,00.htm>)

RSA security announced the result of a questionnaire survey concerning what people in the United States think about the security of financial institutions on March 24. The investigation was carried out over the Internet in November, 2005, and the number of effective answers was 402.

The result was that 73% of people with bank accounts want stronger authentication than logging on with an ID and password when online banking.

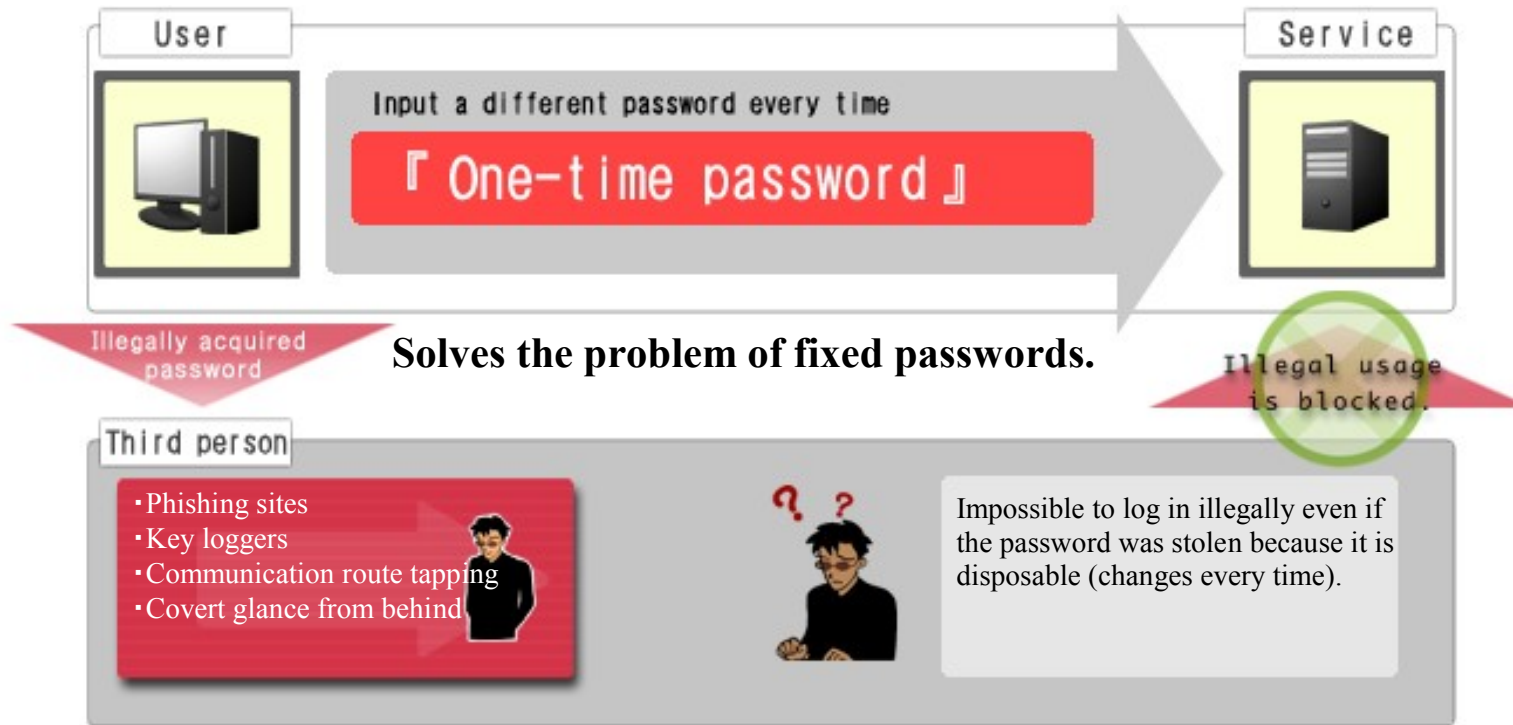


- **Users want a stronger authentication method than "ID + password".**
- **Security can be strengthened by introducing the one-time password.**



PASSLOGIC achieves a safer, better security environment.

■ Merit of introducing the PASSLOGIC method



■ Superior to existing authentication systems

Merit 1

- Easy operation
 - Intuitive operation using an image
 - Mechanism that is easy to remember and difficult to forget



To page 5

Merit 2

- Distributing equipment to end users is unnecessary.
 - Problems like the equipment breaking down (dead battery) and loss never occur.
 - Burden of the operation management and regular capital investment can be reduced.



To page 6



Merit 1 Easy operation

Intuitive operation using images, easy to remember and hard to forget

First, users register a shape such as a 'V'. A password is then created based on the image that is easy to remember and that cannot be guessed by others. That's the key point of the PASSLOGIC system.

The PASSLOGIC matrix changes every time the system is used. Users never enter the same password twice (One Time Password).



1	2	1	5	0	5	1	6	9	2	6	3
6	5	1	0	9	7	6	9	4	5	2	3
2	6	8	8	5	2	0	2	0	2	1	5
9	6	1	3	0	5	6	4	7	9	1	2

The password to input is: 15830266



0	2	3	1	4	5	6	7	9	8	1	0
4	5	4	8	1	2	0	6	1	8	7	0
1	2	1	5	0	2	5	9	6	3	5	6
4	5	1	7	9	7	8	2	0	5	4	7

The password to input is: 05179207

Users can extract the password from any shape they desire.



4	0	6	2	0	6	9	2	3	6	3	9
0	4	7	8	8	2	5	4	2	4	1	0
0	3	1	4	1	6	3	0	8	7	1	6
1	3	0	7	5	5	7	9	8	5	3	9

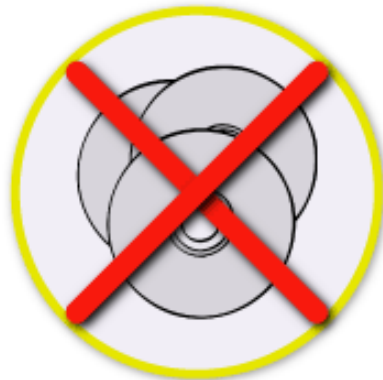
The password to input is: 41759899

PASSLOGIC is one of the leading authentication systems in Japan and has close to 300,000 licensed users.



Merit 2 Not necessary to distribute equipment to the end user

■ PASSLOGIC requires no special hardware



No special software needed



No special hardware needed



Synchronization unnecessary

With past products, it was necessary to prepare both calculator hardware called tokens and special conversion programs for users.



There is no need for additional hardware with the PASSLOGIC authentication method. End users can commence using it in their past log environments.

* Names of the company, product, and service in this presentation are the trademarks or registered trademarks of each company.



Comparison with other OTP products

Authentication method	PASSLOGIC	SecurID	SAFWORD
Image figure	<p>Random numbers table</p>	<p>Hard Token</p> <p>Soft Token</p>	<p>Hard Token</p> <p>Soft Token</p>
Usage	<p>① Access specified URL. ② One-time ticket (random numbers table) is issued. ③ Extract a figure of arbitrary position from the random numbers table to authenticate.</p>	<p>① A one-time ticket is displayed on the hard and soft tokens every 60 seconds. (automatic generation) ② Displayed content + PIN (password number) is inputted and authenticated. *PIN occasionally not used.</p>	<p>① PIN (password number) is inputted to the hard token. ① Access specified URL and input PIN. ② One-time ticket is issued. ③ Displayed content is inputted and authenticated</p>
Password table	○: The correct answer is not displayed.	×: The correct answer is displayed on the screen of the hard and soft tokens.	×: The correct answer is displayed on the screen of the hard and soft tokens.
Authentication method	Challenge & response method	Time synchronization method	Selection of counter synchronization and challenge & response
Password form	Figure from 4 to 16 digits extracted from random numbers table (Users freely set the number of digits)	Six digit figure (Occasionally used in combination with PINs)	6-8 digit alphanumeric characters
Ticket issue machine Risk at the theft	○: Because the user individually maintains positional information (password generation logic) in the random numbers table, the risk level is low.	×: Because the password is displayed as it is, the risk level is high.	×: Because the password is displayed as it is, the risk level is high.
Probability which individual specific information is seen through	Changes with the size and the number of digits of the random numbers table. 【 When size of random numbers table is 4×4】 4 digits ··· 1/16 ⁴ 16 digits ··· 1/16 ¹⁶ 【When size of random numbers table is 4×12】 4 digits ··· 1/48 ⁴ 16 digits ··· 1/48 ¹⁶	Probability which a third party can guess the PIN (password number of four fixed digits). Combination of ten figures 1/10000 *If a PIN is not used, it is impossible to calculate.	Probability which a third party can guess the PIN (password number of four fixed digits). Combination of ten figures 1/10000
System administrator	○: Administrator can intensively manage the authentication by software.	×: Burden of operation due to flat batteries, replacement, failure, and loss, etc. is large. ○: Administrator can intensively manage the authentication by software.	×: Burden of operation due to flat batteries, replacement, failure, and loss, etc. is large. ○: Administrator can intensively manage the authentication by software.
Users	○: A hardware token is not necessary (Web browser only has to be used to display the random numbers table).	×: The hard token must be carried besides the communication terminal. △: Special software must be installed.	×: The hard token must be carried besides the communication terminal. △: Special software must be installed.

* Names of the company, product, and service in this presentation are the trademarks or registered trademarks of each company.



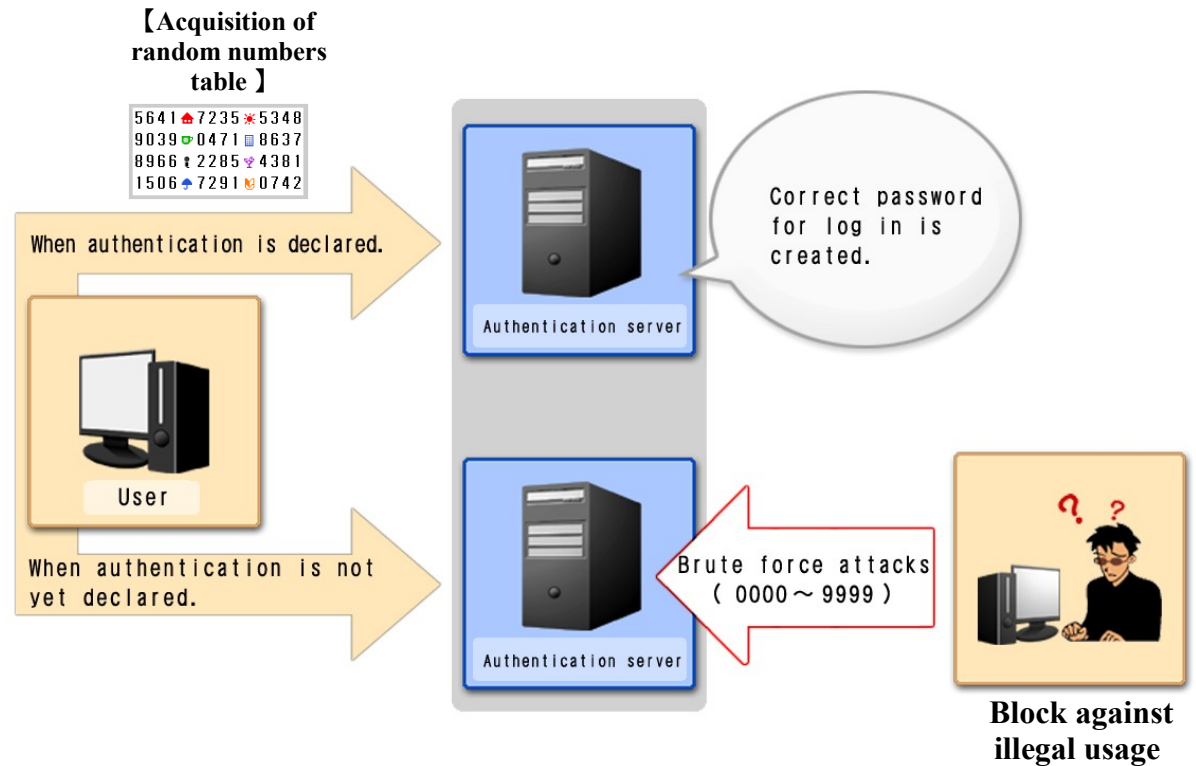
Further security improvement : 1

Prevents brute force attacks

PASSLOGIC completely prevents "brute force attacks " in which passwords are repeatedly inputted.

With PASSLOGIC , the "correct answer" cannot occur as long as the random numbers table has not been acquired.

In short, even if a third party tested all possible passwords from 0000 to 9999 (*1), they will never get the right one. (*1) With four digit passwords used for ATMs etc.



	PASSLOGIC	Token-type one-time password
Brute force attack	○ Preventable	× Unpreventable



Further security improvement: 2

Prevents random lock attacks

In general, if usage of a regulated time (three times etc.) fails, a password is invalidated.

Therefore if the purpose is to merely make it unusable (locked), a suitable password can be inputted three times in a row and after failing the password will be invalid.

It is possible to invalidate a password with only the ID when attacks are made to lock users out. All users can be locked out by randomly inputting suitable IDs and then inputting the wrong password until it is invalidated.

These attacks can be called **indiscriminate cyber terrorism** and can cause a lot of damage to corporations.

With past security, there is no essential solution to this even when token-type one-time passwords, for example SecurID etc, are used.

PASSLOGIC can eliminate this type of risk which could occur in the future.

	PASSLOGIC	Token-type one-time password
Indiscriminate lock attack	○ Preventable	× Unpreventable

* Names of the company, product, and service in this presentation are the trademarks or registered trademarks of each company.

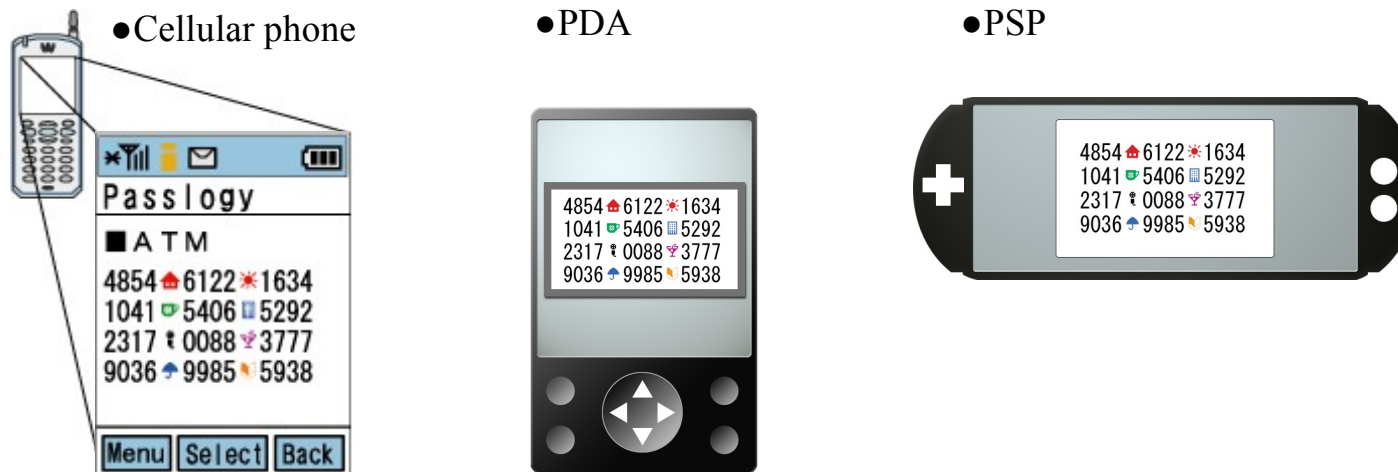
Use the usual authentication method when you go out

If a browser function is installed, the PASSLOGIC random numbers table can be displayed on any device.

That is, devices such as cellular phones, PDAs, and portable game machines (PSP) that people often have with them can be used as PASSLOGIC display equipment.

PASSLOGIC, which can be used irrespective of the location is exactly the type of authentication method needed in this ubiquitous information age.

Supports use from a variety of mobile terminals.

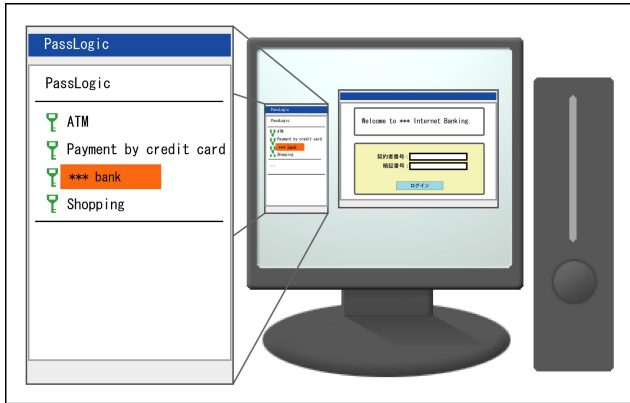


* Names of the company, product, and service in this presentation are the trademarks or registered trademarks of each company

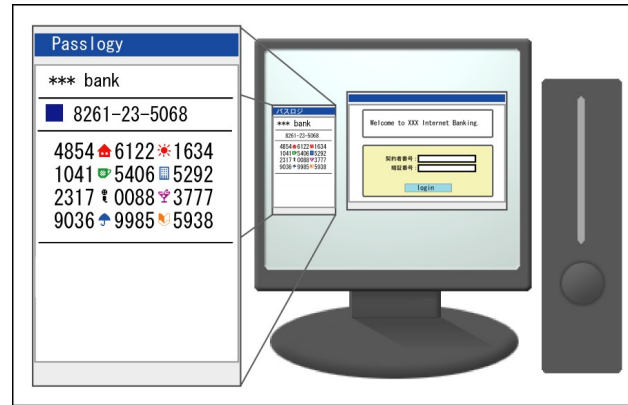


PASSLOGIC

① Access the PC PASSLOGIC menu screen and select the service



② Extract the positional information from the displayed random numbers table and use it as the password

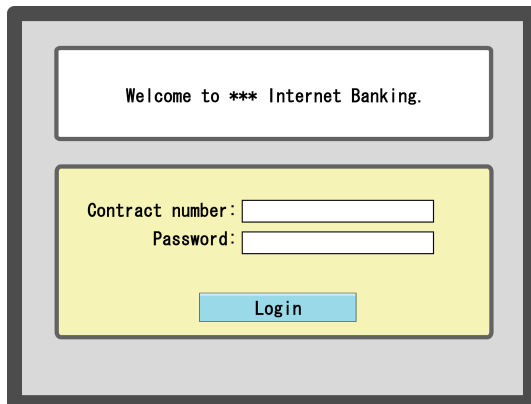


The password of this time

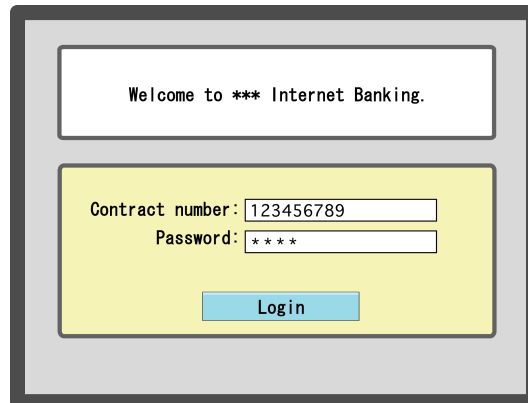
1 2 9 0

Service used

① Access the log in screen of the service used.



② Enter the contract number and password number



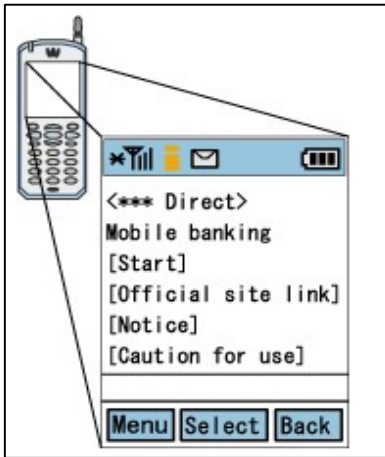
Point
Usage is the same with any system.

**Authentication complete.
The service is available.**

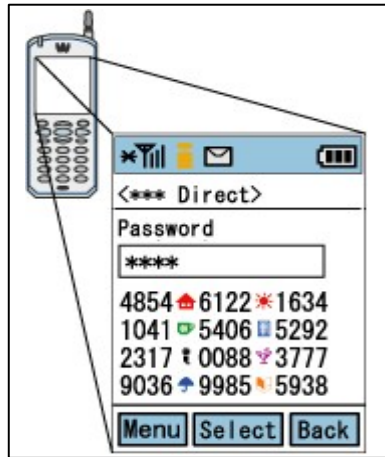


A random numbers table is displayed, unlike past systems.

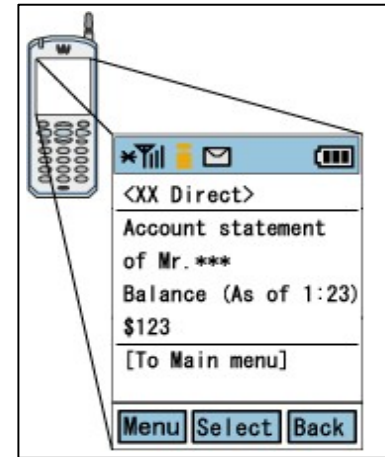
① Access the mobile banking screen.



② Positional information is extracted from the random numbers table. Enter the password.



③ Log in is successful and the service is available.



The password is extracted according to the positional information decided beforehand.

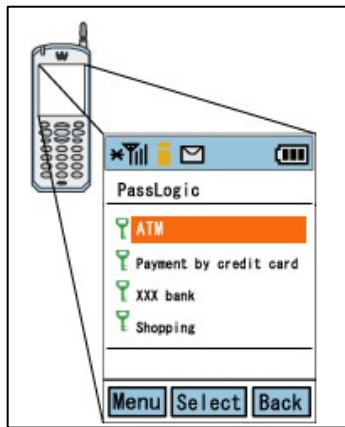
The password of this time

1 2 9 0

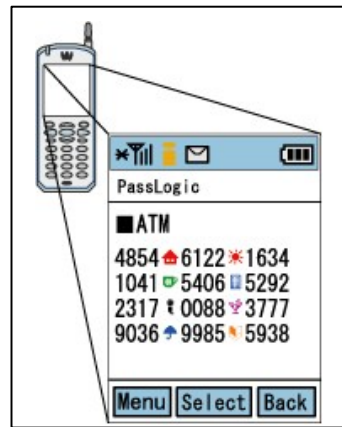


Mobile terminal

① Access the PASSLOGIC menu screen of and select service



② Extract the positional information from the displayed random numbers table and use it as the password



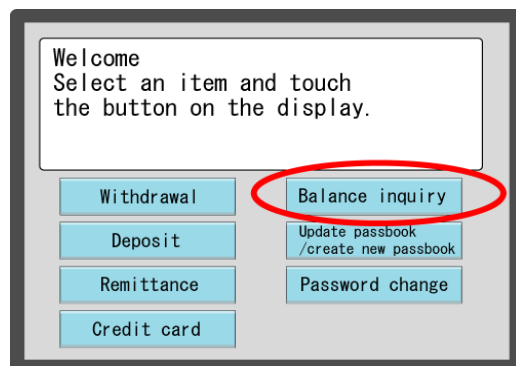
Password of this time

1 2 9 0

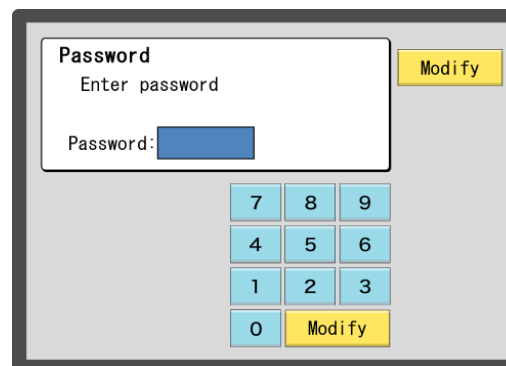
Point
Usage is the same with any system.

ATM terminal

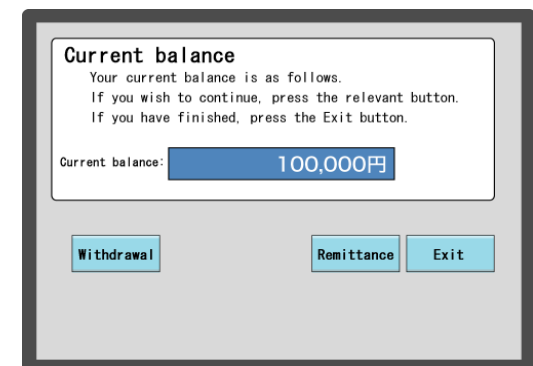
① Press the Balance inquiry button on the ATM menu.



② Enter the password.



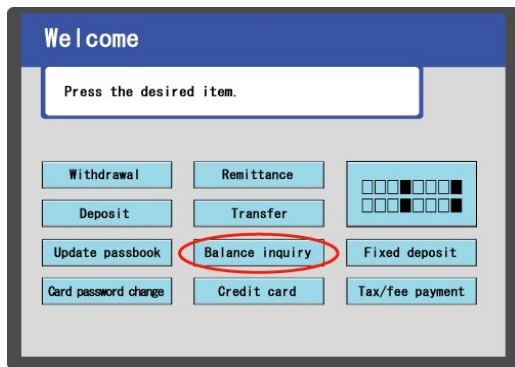
③ Authentication complete. The service is available.



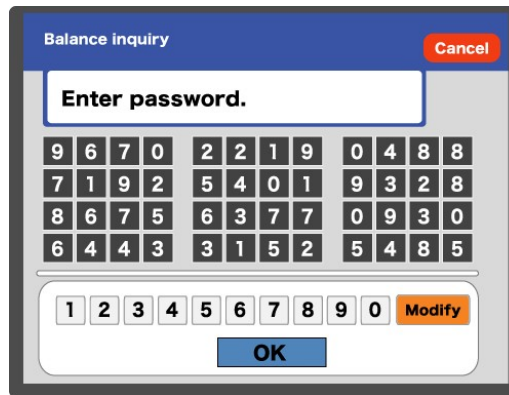


A random numbers table is displayed, unlike past systems.

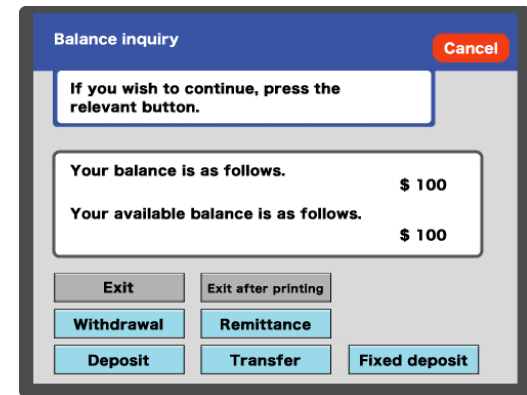
① Press the Balance inquiry button on the ATM menu



② Positional information is extracted from the random numbers table. Enter the password.



③ Authentication complete. The service is available.



The password is extracted according to the positional information decided beforehand.

The password this time

7 8 6 4



Introducing PASSLOGIC



The mechanism of PASSLOGIC is intuitive with acknowledged ease of use. However, we recommend the registration set is distributed so as to ensure a smooth introduction for most people.

Those mentioned below should be included in the registration set.

- Customers using PASSLOGIC for the first time



Manual which plainly explains authentication methods

- Customers who can not remember where to extract it from



Extraction card for customer that records the extraction position

- Customers who have forgotten the extraction position

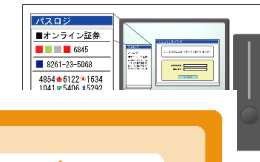


Recovery key for re-registration

Consultations for operation and explanation material are available for end users. Please feel free to contact us.

Explanation material

Notice of temporary password
 Thank you for your *** bank Internet Banking Service application.
 This explains the "PASSLOGIC" system of this service and gives you the initial password.
 Unlike previous password or memory systems with numbers and characters, PASSLOGIC stores the position in a table. The system has excellent robustness and availability.
 The following screen is displayed when you log into Internet Banking.



※を順番に入力することでパスワードとなります。

※出しますので、お客様はパスワード欄

PASSLOGIC extraction card

*** Online banking
 Name:*** ** ***
 Contract number:123-456-7890

□	□	□	□	□	□	□	□	□	□	□	3
□	□	□	□	4	□	□	□	□	□	□	□
□	□	□	□	□	□	□	□	1	□	□	□
□	2	□	□	□	□	□	□	□	□	□	□

Extraction card for customers



Questions related to this new technology can be forwarded to e-mail: tech@passlogy.com.

Any inquiries regarding sales can be sent to e-mail: sales-os@passlogy.com.