fido ALLIANCE

Yahoo! JAPAN's password-free authentication reduced inquiries by 25%, sped up sign-in time by 2.6x

Overview

Yahoo! JAPAN is one of the largest media companies in Japan, providing services such as search, news, e-commerce, and e-mail. Over 50 million users log in to Yahoo! JAPAN services every month.

Over the years, there were many attacks on user accounts and issues that led to lost account access. Most of these issues were related to password usage for authentication.

With recent advances in authentication technology, Yahoo! JAPAN has decided to move from password-based to passwordless authentication.

Why passwordless?

As Yahoo! JAPAN offers e-commerce and other money-related services, there's a risk of significant damage to users in the event of unauthorized access or account loss.

The most common attacks related to passwords were password list attacks and phishing scams. One of the reasons why password list attacks are common and effective is many people's habit of using the same password for multiple applications and websites.

The following figures are the results of a survey conducted by Yahoo! JAPAN.

50 % use the same ID and password on six or more sites

60 % Use the same password across multiple sites

70 % use a password as the primary way to login

Users often forget their passwords, which accounted for the majority of password-related inquiries. There were also inquiries from users who had forgotten their login IDs in addition to their passwords. At their peak, these inquiries accounted for more than a third of all account-related inquiries.

By going passwordless, Yahoo! JAPAN aimed to improve not only security, but also usability, without placing any extra burden on users.

From a security perspective, eliminating passwords from the user authentication process reduces the damage from list-based attacks, and from a usability perspective, providing an authentication method that does not rely on remembering passwords prevents situations where a user is unable to login because they forgot their password.

Yahoo! JAPAN’s passwordless initiatives

Yahoo! JAPAN is taking a number of steps to promote passwordless authentication, which can be broadly divided into three categories:

1. **Provide an alternative means of authentication to passwords.**
2. **Password deactivation.**
3. **Passwordless account registration.**

The first two initiatives aimed at existing users, while passwordless registration is aimed at new users.

1. Providing an alternative means of authentication to passwords

Yahoo! JAPAN offers the following alternatives to passwords.

1. **SMS authentication**
2. **FIDO with WebAuthn**

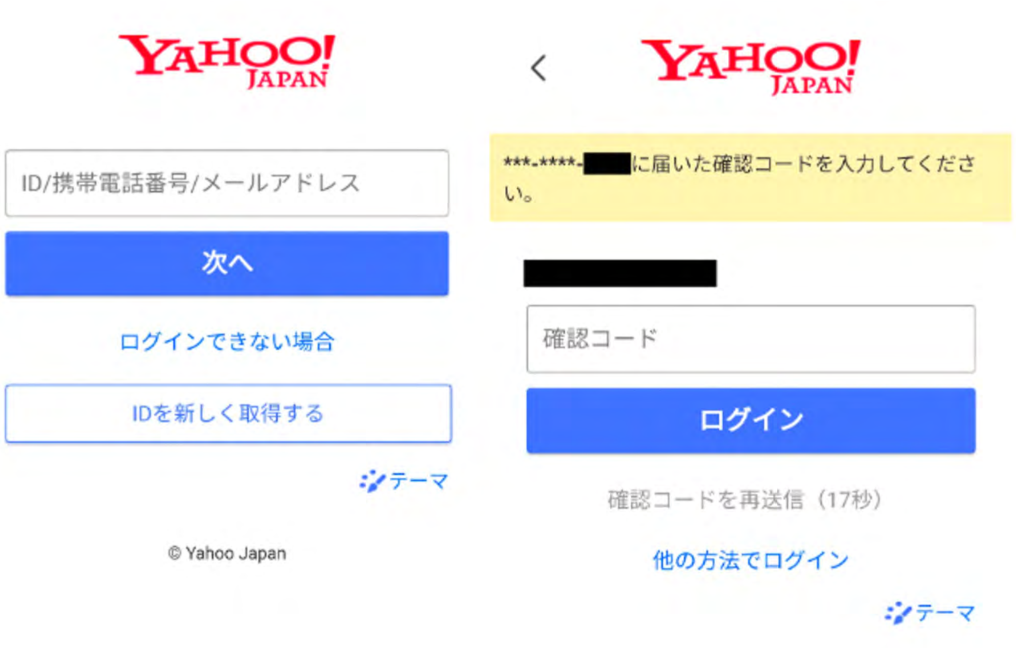
In addition, we also offer authentication methods such as e-mail authentication, password combined with SMS OTP (one time password), and password combined with email OTP.

Important

Yahoo! JAPAN restricts their service to phone carriers operating inside Japan and prohibits VoIP SMS.

SMS authentication

SMS authentication is a system which allows a registered user to receive a six-digit authentication code through SMS. Once the user receives the SMS, they can enter the authentication code in the app or website.

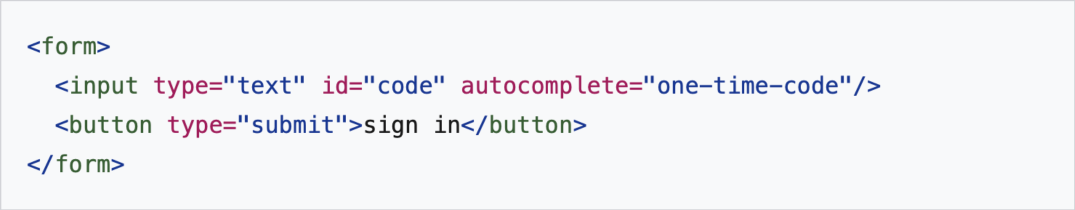


-*-[redacted]に届いた確認コードを入力してください。

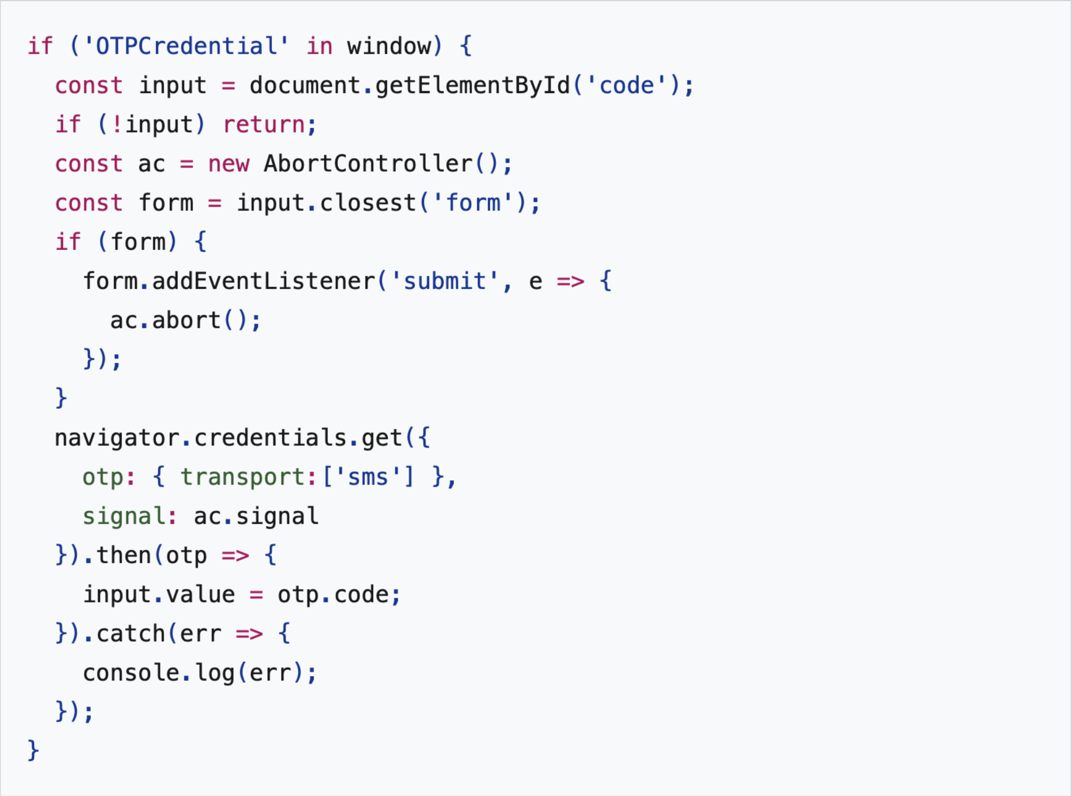
[redacted]

Apple has long allowed iOS to read SMS messages and suggest authentication codes from the text body. Recently, it's become possible to use suggestions by specifying "one-time-code" in the autocomplete attribute of the input element. Chrome on Android, Windows, and Mac can provide the same experience using the WebOTP API.

For example:



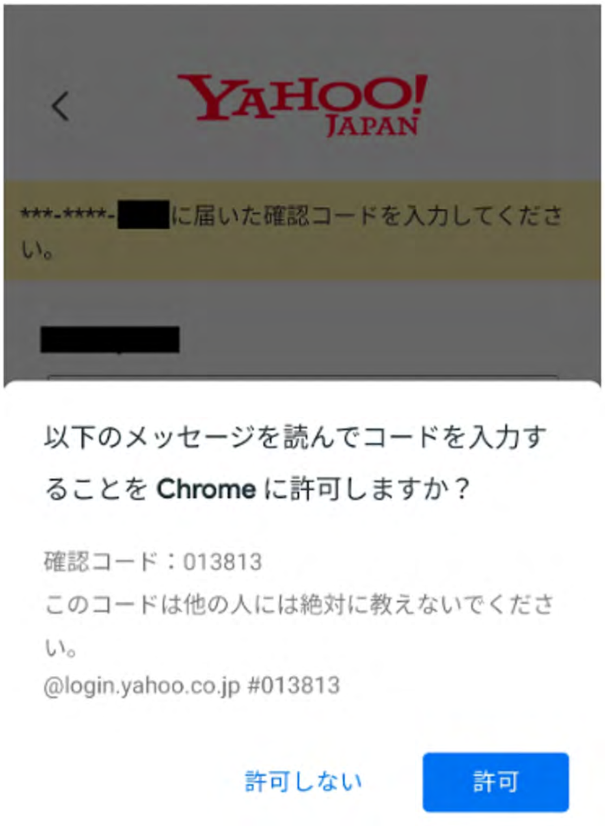
```
<form>
  <input type="text" id="code" autocomplete="one-time-code"/>
  <button type="submit">sign in</button>
</form>
```



```
if ('OTPCredential' in window) {
  const input = document.getElementById('code');
  if (!input) return;
  const ac = new AbortController();
  const form = input.closest('form');
  if (form) {
    form.addEventListener('submit', e => {
      ac.abort();
    });
  }
  navigator.credentials.get({
    otp: { transport:['sms'] },
    signal: ac.signal
  }).then(otp => {
    input.value = otp.code;
  }).catch(err => {
    console.log(err);
  });
}
```

Both approaches are designed to prevent phishing by including the domain in the SMS body and providing suggestions only for the specified domain.

For more information about the WebOTP API and autocomplete=”one-time-code”, check out SMS OTP form best practices.



-*-[redacted]に届いた確認コードを入力してください。

[redacted]

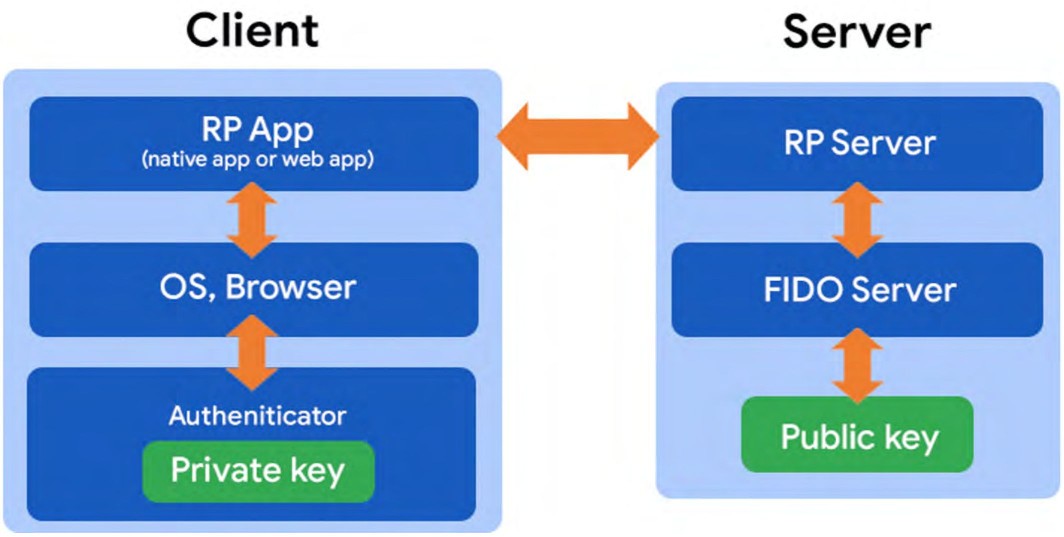
以下のメッセージを読んでコードを入力することを Chrome に許可しますか？

確認コード：013813
このコードは他の人には絶対に教えないでください。
@login.yahoo.co.jp #013813

FIDO with WebAuthn

FIDO with WebAuthn uses a hardware authenticator to generate a public key cipher pair and prove possession. When a smartphone is used as the authenticator, it can be combined with biometric authentication (such as fingerprint sensors or facial recognition) to perform one-step two-factor authentication. In this case, only the signature and the success indication from the biometric authentication are sent to the server, so there is no risk of biometric data theft.

The following diagram shows the server-client configuration for FIDO. The client authenticator authenticates the user with biometrics and signs the result using public key cryptography. The private key used to create the signature is securely stored in a TEE (Trusted Execution Environment) or similar location. A service provider that uses FIDO is called an RP (relying party).



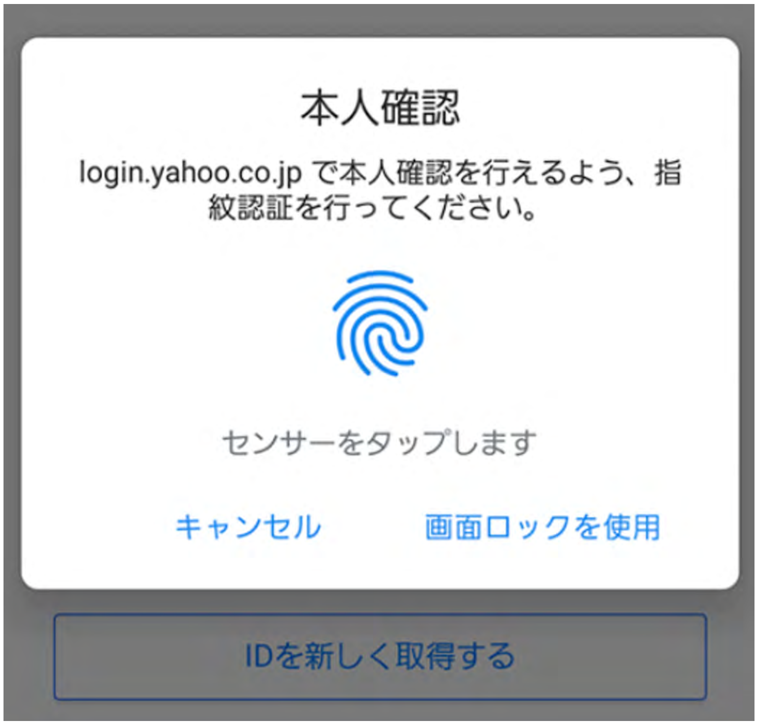
Once the user performs the authentication (commonly with a biometric scan or PIN), the authenticator uses a private key to send a signed verification signal to the browser. The browser then shares that signal with the RP's website.

The RP website then sends the signed verification signal to the RP's server, which verifies the signature against the public key to complete the authentication.

For more information, read authentication guidelines from the FIDO Alliance.

Yahoo! JAPAN supports FIDO on Android (mobile app and web), iOS (mobile app and web), Windows (Edge, Chrome, Firefox), and macOS (Safari, Chrome). As a consumer service, FIDO can be used on almost any device, which makes it a good option for promoting passwordless authentication.

Operating System	Support for FIDO
Android	Apps, Browser (Chrome)
iOS	Apps (iOS14 or later), Browser (Safari 14 or later)
Windows	Browser (Edge, Chrome, Firefox)
Mac (Big Sur or later)	Browser (Safari, Chrome)



本人確認

login.yahoo.co.jp で本人確認を行えるよう、指紋認証を行ってください。

センサーをタップします

Sample Yahoo! JAPAN prompt to authenticate with FIDO.

Yahoo! JAPAN recommends that users register for FIDO with WebAuthn, if they've not already authenticated through other means. When a user needs to log in with the same device, they can quickly authenticate using a biometric sensor.

Users must set up FIDO authentication with all devices they use to log in to Yahoo! JAPAN.

To promote passwordless authentication and be considerate of users who are transitioning away from passwords, we provide multiple means of authentication. This means that different users can have different authentication method settings, and the authentication methods they can use may differ from browser to browser. We believe it's a better experience if users log in using the same authentication method each time.

To meet these requirements, it's necessary to track previous authentication methods and link this information to the client by storing it in the form of cookies, etc. We can then analyze how different browsers and applications are used for authentication. The user is asked to provide appropriate authentication based on the user's settings, the previous authentication methods used, and the minimum level of authentication required.

2. Password deactivation

Yahoo! JAPAN asks users to set up an alternative authentication method and then disable their password so that it cannot be used. In addition to setting up alternative authentication, disabling password authentication (therefore making it impossible to sign in with only a password) helps protect users from list-based attacks.

We've taken the following steps to encourage users to disable their passwords.

- Promoting alternative authentication methods when users reset their passwords.
- Encouraging users to set up easy-to-use authentication methods (such as FIDO) and disable passwords for situations that require frequent authentication.
- Urging users to disable their passwords before using high-risk services, such as e-commerce payments.

If a user forgets their password, they can run an account recovery. Previously this involved a password reset. Now, users can choose to set up a different authentication method, and we encourage them to do so.

3. Passwordless account registration

New users can create password-free Yahoo! JAPAN accounts. Users are first required to register with an SMS authentication. Once they've logged in, we encourage the user to set up FIDO authentication.

Since FIDO is a per-device setting, it can be difficult to recover an account, should the device become inoperable. Therefore, we require users to keep their phone number registered, even after they've set up additional authentication.

Key challenges for passwordless authentication

Passwords rely on human memory and are device-independent. On the other hand, the authentication methods introduced thus far in our passwordless initiative are device-dependent. This poses several challenges.

When multiple devices are used, there are some issues related to usability:

- When using SMS authentication to log in from a PC, users must check their mobile phone for incoming SMS messages. This may be inconvenient, as it requires the user's phone to be available and easy to access at any time.
- With FIDO, especially with platform authenticators, a user with multiple devices will be unable to authenticate on unregistered devices. Registration must be completed for each device they intend to use.

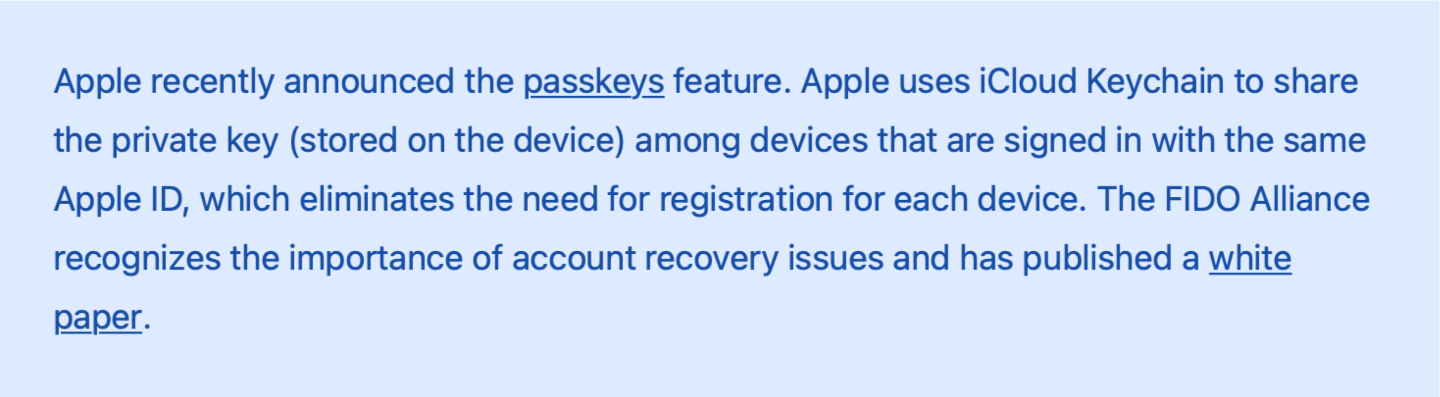
FIDO authentication is tied to specific devices, which requires they remain in the user's possession and active.

- If the service contract is canceled, it will no longer be possible to send SMS messages to the registered phone number.
- FIDO stores private keys on a specific device. If the device is lost, those keys are unusable.

Yahoo! JAPAN is taking various steps to address these problems.

The most important solution is to encourage users to set up multiple authentication methods. This provides alternative account access when devices are lost. Since FIDO keys are device-dependent, it is also good practice to register FIDO private keys on multiple devices.

Alternatively, users can use the WebOTP API to pass SMS verification codes from an Android phone to Chrome on a PC.



Apple recently announced the passkeys feature. Apple uses iCloud Keychain to share the private key (stored on the device) among devices that are signed in with the same Apple ID, which eliminates the need for registration for each device. The FIDO Alliance recognizes the importance of account recovery issues and has published a white paper.

We believe that addressing these issues will become even more important as passwordless authentication spreads.

Promoting passwordless authentication

Yahoo! JAPAN has been working on these passwordless initiatives since 2015. This began with the acquisition of FIDO server certification in May 2015, followed by the introduction of SMS authentication, a password deactivation feature, and FIDO support for each device.

Today, more than 30 million monthly active users have already disabled their passwords and are using non-password authentication methods. Yahoo! JAPAN's support for FIDO started with Chrome on Android, and now more than 10 million users have set up FIDO authentication.

As a result of Yahoo! JAPAN's initiatives, the percentage of inquiries involving forgotten login IDs or passwords has decreased by 25% compared to the period when the number of such inquiries was at its highest, and we have also been able to confirm that unauthorized access has declined as a result of the increase in the number of passwordless accounts.

Since FIDO is so easy to set up, it has a particularly high conversion rate. In fact, Yahoo! JAPAN has found that FIDO has a higher CVR than SMS authentication.

25 %

Decrease in requests for forgotten credentials

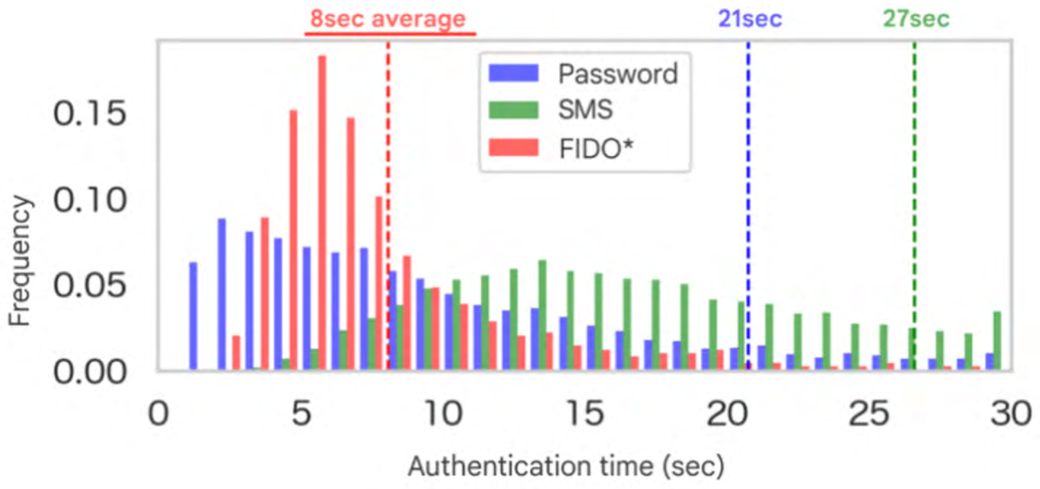
74 %

Users succeed with FIDO authentication

65 %

Succeed with SMS verification

FIDO has a higher success rate than SMS authentication, and faster average and median authentication times. As for passwords, some groups have short authentication times, and we suspect that this is due to the browser's autocomplete=”current-password”.



Comparison of authentication time
(FIDO2 based biometric, password and SMS)
* includes PIN entry on biometric failure

On average, FIDO takes 8 seconds to authenticate, while passwords take 21 seconds, and SMS verification takes 27.

The greatest difficulty for offering passwordless accounts is not the addition of authentication methods, but **popularizing the use of authenticators**. If the experience of using a passwordless service is not user-friendly, the transition will not be easy.

We believe that to achieve improved security we must first improve usability, which will require unique innovations for each service.

Conclusion

Password authentication is risky in terms of security, and it also poses challenges in terms of usability. Now that technologies supporting non-password authentication, such as WebOTP API and FIDO, are more widely available, it's time to start working toward passwordless authentication.

At Yahoo! JAPAN, taking this approach has had a definite effect on both usability and security. However, many users are still using passwords, so we will continue to encourage more users to switch to passwordless authentication methods. We will also continue improving our products to optimize the user experience for passwordless authentication methods.

Source: https://web.dev/yahoo-japan-identity-case-study