FIDO ALLIANCE
simpler stronger authentication

MIXI Promotes a "Safe and Seamless Login Experience" with Passkey Deployment Across Both Consumer and Enterprise Environments

The Business Challenge

From the outset, MIXI ID pursued a passwordless approach, adopting an email-based one-time password (OTP) method. However, this proved insufficient against the rising threat of real-time phishing attacks, while the flow of opening an email app, retrieving a code, and entering it was cumbersome for users. For services that involve payment functions in particular, there was a strong need for a mechanism that could deliver both high authentication strength and excellent user experience.

Internally, the company also faced the challenge of balancing enhanced security with operational efficiency, while accommodating shared PC usage and continuously evolving OS environments.

Decision to deploy Passkeys

To address these challenges, MIXI introduced FIDO2-compliant passkey authentication to MIXI ID in 2024. Leveraging the WebAuthn API offered by web applications and browsers, users can now log in smoothly and password-free using the biometric authentication built into their smartphones and PCs.

In addition, **passkey authentication was made mandatory** for administrative tools in the payment system, enabling stronger security operations without reliance on passwords.

MIXI also advanced its internal enterprise security environment by adopting YubiOn Portal, provided by SoftGiken (a FIDO Alliance member), together with YubiKey from Yubico (a FIDO Alliance board member). This strengthened physical security for shared PCs and logon authentication, creating a unified, cloud-managed two-factor authentication environment for both Windows and macOS. As a result, MIXI achieved both stronger authentication for shared terminal logons and greater operational efficiency.

Why FIDO was chosen

While the company also utilizes Apple and Google social logins, there were clear reasons for adopting FIDO authentication as one of its primary methods:

- Trust in security and interoperability based on international standards
- Smooth and practical user experience enabled by platform-provided Passkey Autofill
- Strong security with biometrics combined with the convenience of passwordless login

Corporate overview:

MIXI

MIXI, Inc. (hereafter MIXI) is one of Japan's leading internet companies, best known for its popular mobile game MONSTER STRIKE, among other entertainment services, with tens of millions of users. The company has also expanded into sports and lifestyle businesses, providing services that enrich the daily lives of a broad range of generations.

The company's MIXI ID serves as a common account platform enabling users to access multiple services seamlessly. In recent years, it has also been adopted by flagship titles, continuing to grow its user base.
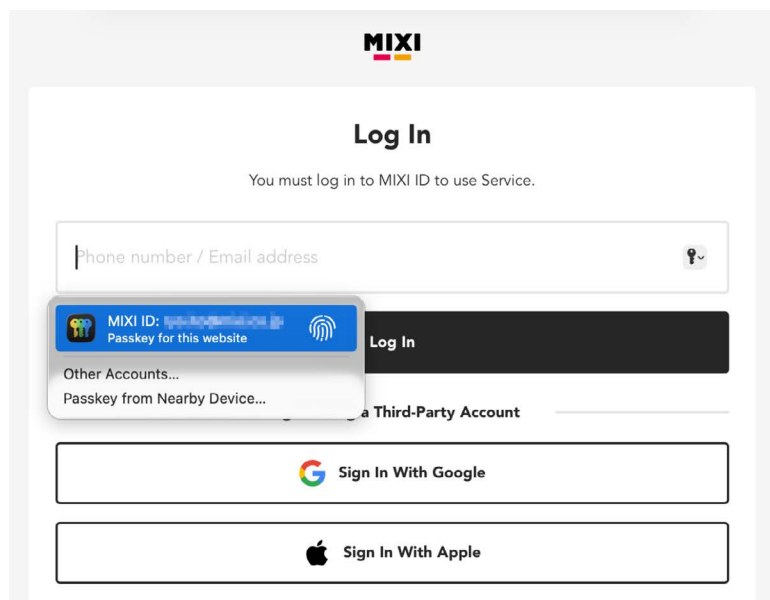
Login Screen Image
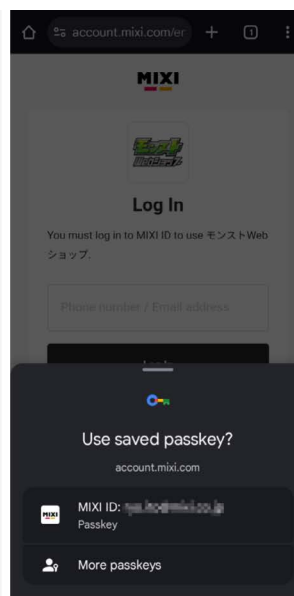
Impact of adoption

Currently, more than **25% of MIXI ID users have registered a passkey**, and adoption is steadily expanding. Helpdesk enquiries caused by issues with OTPs —such as "delays/resending of authentication codes" and "input errors"—have decreased, helping to reduce support costs.

For users, the experience of being able to log in safely and quickly is spreading, further reinforcing trust in MIXI's authentication infrastructure.

Within the enterprise environment, the introduction of YubiOn Portal **enabled a shift from ledger-based authentication management to cloud-based management**, ensuring real-time visibility into the latest authentication status. It also supports Windows Remote Desktop usage and has been highly praised by employees.

Overcoming Implementation Challenges

In some early deployments at other companies, confusing error messages such as "Passkey not found" created user difficulties. MIXI avoided this issue by timing its rollout to coincide with the point at which **Passkey Autofill** had become sufficiently mature across major OS platforms, **successfully preventing user confusion**.

The adoption of YubiOn Portal required detailed policy settings, but thanks to extensive documentation and flexible configuration features, the IT team was able to implement and operate the system smoothly.

Looking ahead

MIXI expects passkey authentication to become widely adopted across services and evolve from its current optional status into a primary authentication method. The company intends to expand its use across more service areas, contributing to the realization of a passwordless society.

Finally, Ryo Ito of MIXI, who shared insights for this case study, commented:
"FIDO authentication delivers strong phishing resistance and high security, but there are still challenges such as account recovery from environments where passkeys are unavailable. It's important to correctly recognize these issues and refer to the FIDO Alliance's published design and implementation guidelines and checklists when adopting FIDO authentication.

As passkey authentication becomes more widespread, we are already seeing its positive impact with MIXI ID. FIDO/Passkeys are a rare technology that can simultaneously provide excellent UX and robust security at low cost. Going forward, we look forward to the evolution of the ecosystem to support an even wider variety of use cases."