

アカウントを失わないためのログイン・復旧準備チェックリスト

2026年10月22日更新・第1版 | webtechnote.com | <https://webtechnote.com/tools/account-recovery-readiness-checklist>

このシートに、パスワード、バックアップコード、復旧コード、アカウントID、電話番号、復旧メールなどの秘密を書き込まないでください。復旧の成功を保証するものではありません。

1. 重要なアカウントを絞る

- ・ 主なメールアカウントと、Apple・Google・Microsoftなどの基盤アカウント
- ・ 利用しているパスワードマネージャー、銀行・決済・買い物のアカウント
- ・ SNS・メッセージ、仕事やWebサイト管理のアカウント（該当する場合）
- ・ 実際のID、連絡先、認証情報はこのシートに書かない

2. 普段のログインと復旧経路を確認する

- ・ 対応するサービスで、パスキーやFIDOベースのログインと多要素認証を検討した。
- ・ パスワードを使う場合は、そのサービス専用で使い回していない。
- ・ 復旧用連絡先が現在も使え、公式の復旧ページを広告や見知らぬ番号に頼らず見つけれられる。
- ・ 対応する場合だけ、バックアップコード・復旧コードを通常のログイン経路とは別の安全な場所に保管した。
- ・ 古い認証方法を外す前に、確認済みの復旧経路を残した。

パスキーは偽サイトへパスワードを入力するリスクを減らす助けになりますが、復旧の準備とは別に確認します。

3. 端末やパスキーを失った場合を理解する

- ・同期型のパスキーは、同じパスキープロバイダーの別端末で利用できる場合がある。
- ・端末に結び付くパスキーでは、端末を失うと別の認証方法や復旧経路が必要になる場合がある。
- ・同期型であっても、プロバイダーへのアクセス喪失やプラットフォーム移行で復旧が必要になる場合がある。

4. 古いアクセスと、入れないときの確認

- ・使っていない端末・セッション、不要な連携アプリ、古い連絡先は、別の確認済み経路があることを確かめてから外す。
- ・入れないときは、公式サイトや公式アプリから独立して確認した復旧手順を使う。
- ・予期しないメッセージや広告だけに出ている復旧リンク・サポート番号を信用しない。
- ・まだアクセスできる場合は、認証情報、復旧連絡先、端末・セッション、認証方法、連携アプリを確認する。

出典（確認先） IPA「インターネットサービスへの不正ログインによる被害が増加中」 <https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html> IPA「情報セキュリティ10大脅威 2026 解説書」 https://www.ipa.go.jp/security/10threats/omgdg50000008fi8-att/kaisetsu_2026_soshiki.pdf FIDO Alliance「パスキー: パスワードレス認証」 <https://fidoalliance.org/passkeys-2/?lang=ja> FIDO Alliance「Synced Passkey Deployment」 https://fidoalliance.org/wp-content/uploads/2024/05/Synced-Passkey-Deployment_-Emerging-Practices-for-Consumer-Use-Cases_2024-Final.pdf

年に一度、またはIPA・FIDOの案内や主要プラットフォームの挙動が大きく変わったときに見直します。PDFの最新版とHTML版は <https://webtechnote.com/tools/account-recovery-readiness-checklist> を確認してください。