「スマートフォン利用シーンに潜む脅威 Top10 2023」ガイド
【第一回】フィッシング・スミッシングメール対策【付録１】

強化された！～ iOS18 のパスワード管理

2024 年 11 月 21 日

日本スマートフォンセキュリティ協会（JSSEC）
利用部会

作成： 本間 輝彰　KDDI 株式会社
校閲： 松下 綾子　アルプスシステムインテグレーション株式会社
北村 裕司　サイバートラスト株式会社
中村 丈洋　株式会社 SHIFT SECURITY
三池 聖史　特定非営利活動法人日本ネットワークセキュリティ協会

文書管理番号 JSSEC-R-20240331-1

目 次

1. はじめに

JSSEC 利用部会では、フィッシング・スミッシング対策についての啓発活動に注力しています。その一環として、2024 年 7 月に、「スマートフォン利用シーンに潜む脅威 Top10 2023」の解説ガイド、「【第一回】 フィッシング・スミッシング メール対策1」を公開しました。

上記のガイドの中で、「パスワードマネージャによるサービス利用」、「パスキー（FIDO2 ～ 例：指紋・顔認証）の利用」を対策解説として説明しています。

本「付録 1」では、2024 年 9 月 17 日に Apple からリリースされた iOS18 において、パスワード機能が強化されたことを受け、iOS17 のパスワード機能と比較しながら、最適な利用方法の解説を行います。

パスワードマネージャとは

パスワードマネージャは、（Password） Authenticator などとも呼ばれる、パスワードを管理する機能です。

パスワードマネージャを利用すると、各サービスのパスワードがデバイスに安全に保存され、該当のサービスを利用する時に自動でパスワードが入力されます。つまり、利用者はパスワードを覚えておく必要がなくなるのです。逆に言えば、パスワードが自動入力されないサイトは、フィッシングサイトなど不正サイトの可能性があります。その場合には、注意深くそのサイトを利用することで、詐欺等の被害を防ぐことができます。

iOS ではパスワードマネージャが OS 標準の機能として備わっており、iOS17 では、図 1 左に示す通り、「設定」画面から「パスワード」を選択することでパスワードの設定管理が可能となっていました。

一方、iOS18 では、図 1 右に示す通り、パスワードマネージャの機能が独立し、新たに「パスワード」アイコンが表示されるようになりました。アイコン「パスワード」をタップして開くことで、パスワードの設定管理が可能です。また、機能ごとにメニューが分けられ、「パスキー」の設定をしているサービスや、「コード（ワンタイムパスワード）」を設定しているサービスが、容易に確認可能になりました。さらに、Wi-Fi のパスワードも本機能で管理可能です。

[1] スマートフォン利用シーンに潜む脅威 Top10 2023」ガイド【第一回】 フィッシング・スミッシング メール対策
https://www.jssec.org/smartphone-use-10threats202301

図 1　パスワードマネージャ画面（左：iOS17、右：iOS18）

2. パスワード管理

前述の通り、iOS では各サービスのパスワードを保存・管理する機能が具備されています。

iOS17 では、図 1 に示す通り、設定画面から、「パスワード」を選択することで保存しているパスワードの一覧が確認可能です。

一方、iOS18 では図 2 左のパスワード画面にて「すべて」を選択することで、図 2 右に示す通り、登録されているパスワードを一覧できます。

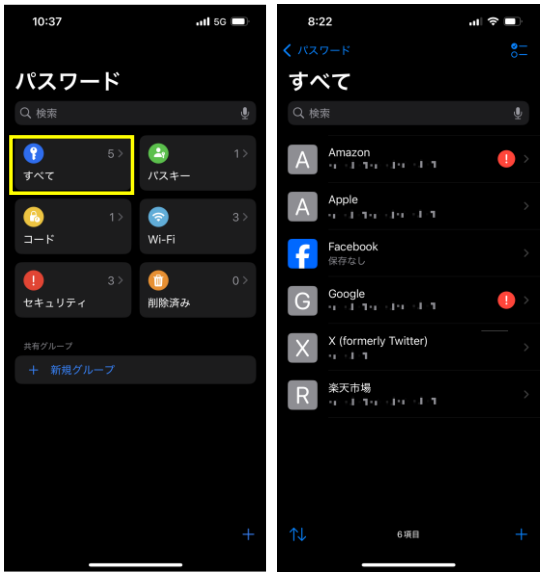

図 2　iOS18 パスワード画面

例えば、各サービスを利用した時、パスワードを入力すると、図 3 に示す通り「パスワードを保存しますか？」と、パスワード保存についての確認画面が表示されます。ここで、「パスワードを保存」を選択するとパスワードが保存され、「すべて」（パスワードの一覧）の画面で確認ができるようになります。

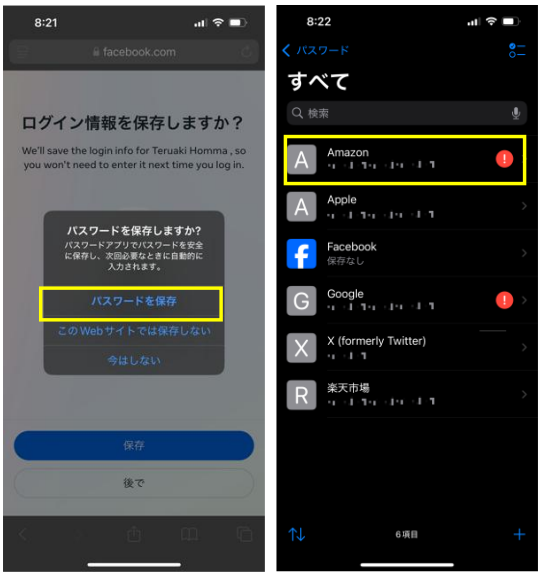

図 3　パスワード保存画面（例：Amazon）

さらに、iOS18 では、図 4 で示すように「この Web サイトではパスワードを保存しない」を選択しても、図 5 中央の「すべて」の画面の通り「保存なし」と表示されるようになりました。したがって、パスワードを記憶させたくない場合に「パスワードを保存しない」を選択しても、利用しているサービス一覧として管理することができます。また、表示されている各アカウントを選択すると、Web サイトへのリンクも記載されており、そのアカウントが使用されているサービスへ直接アクセスすることが可能です。セキュリティリスクの軽減という点では、自分が利用しているサービスを利用する時、このパスワード管理画面からアクセスすればフィッシング詐欺などの被害抑制に繋がると考えられます。

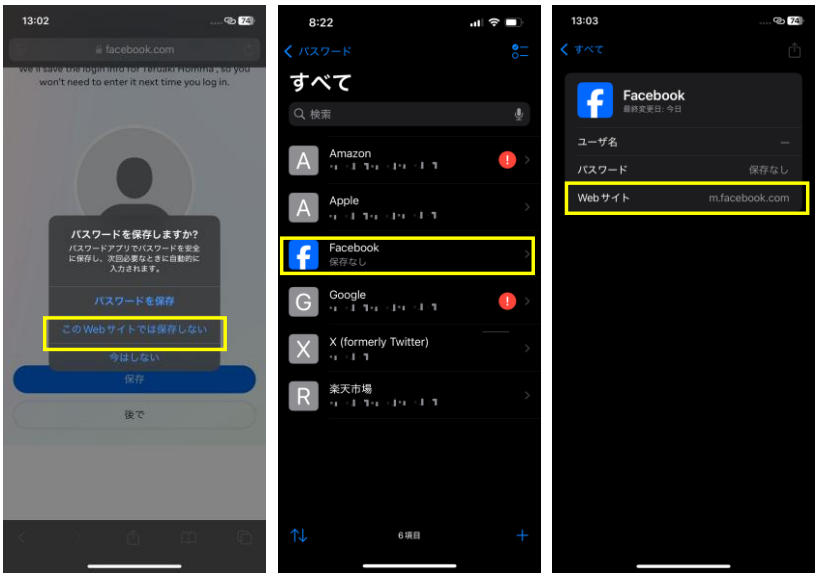

図 4　パスワード保存しない場合（例：Facebook）

さらに図 5 で示す通り、「すべて」の画面のアカウントを選択すると、各アカウントのパスワードの設定方法も確認できます。サービス登録時に、パスワードを自動設定した場合は「強力なパスワード」、利用者が個別に設定した場合は「カスタムパスワード」、Apple アカウントを使ってログインなら「Apple でサインイン」、と表示されます。

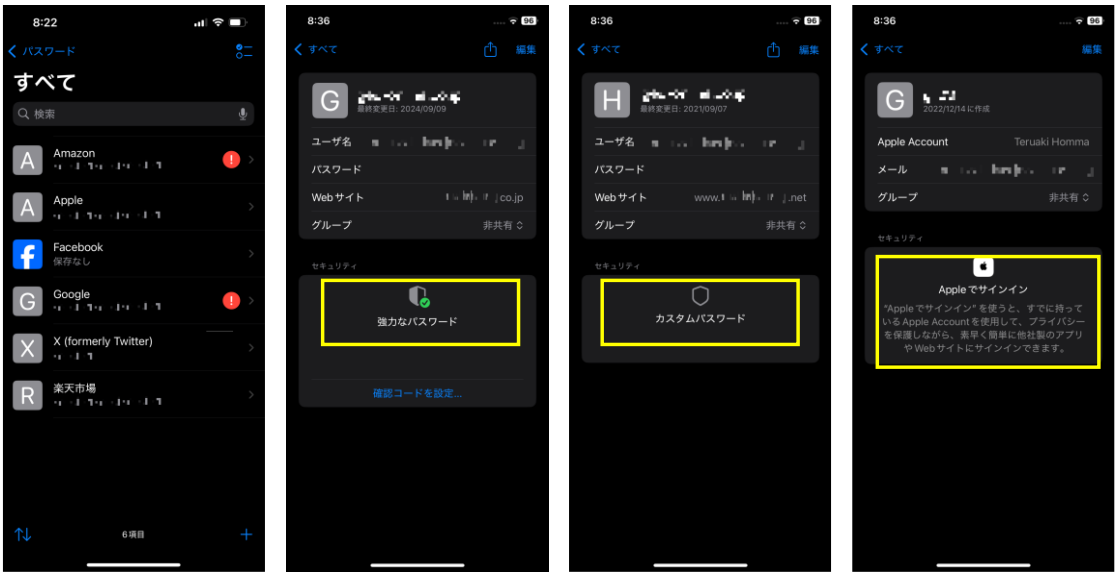

図 5　iOS18 各パスワード画面

また、設定しているパスワードにセキュリティ上の問題があると考えられる場合には、図 6 の「すべて」の画面で黄色枠に示す通り、アカウント横に⓵で表示され、⓵で表示されているアカウントを選択すると「漏洩の危険があるパスワード」、「使い回されたパスワード」、「安全なパスワードではありません」などと問題点が表示され、パスワードの変更が促されます。このような警告が表示された場合は、安全性を確認の上、必要に応じてパスワード変更等の対処が推奨されます。

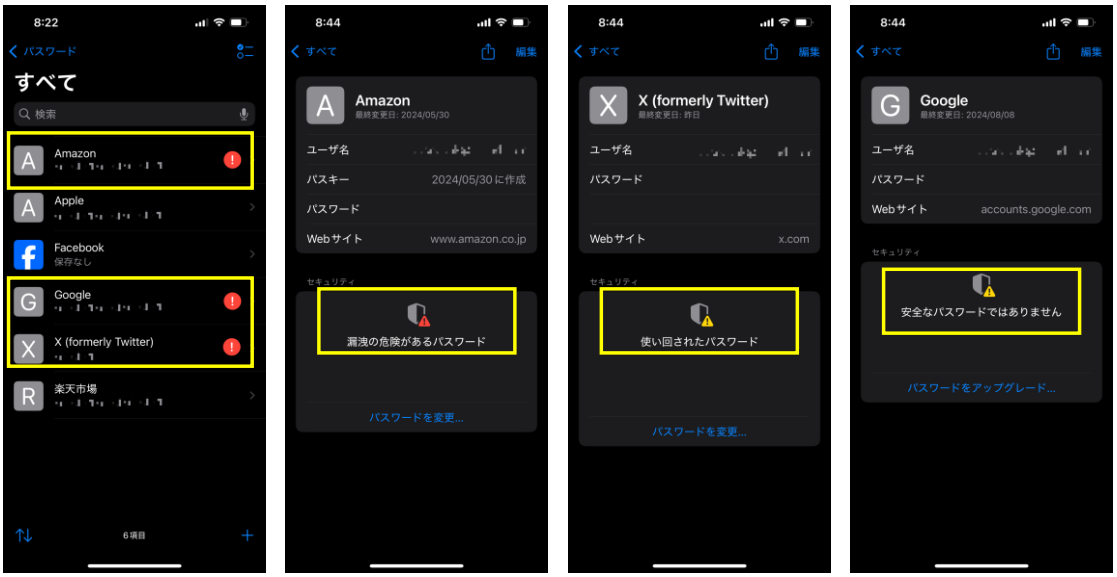

図 6　iOS18 各パスワード画面（セキュリティ警告あり）

3. コード（ワンタイムパスワード）

コードとは、ソフトウェアワンタイムパスワードによる二要素認証のためのキー情報です。各サービスへのログイン時に使われる二要素認証を行う時、SMS やメールで送信されるワンタイムパスワード等の代わりに使われる認証手段で、利用サービス例としては、Twitter が挙げられます。

NIST（米国／National Institute of Standards and Technology）が発行している SP800-63B では、SMS を使ったワンタイムパスワードの利用を非推奨としていることもあり、代替手段としてソフトウェアワンタイムパスワードが利用されるようになりました。

iOS のパスワードマネージャは、各サービスの利用開始時にワンタイムパスワードが設定されると、パスワードマネージャ上のパスワード情報と紐づけます。そのため、各サービスへログインした時、図 7 に示す通り、紐づけられたワンタイムパスワードを確認することができます。。

iOS17 でワンタイムパスワードを利用する際は、図 7 左の「パスワード」画面で該当のアカウントを開き、表示された確認コードをワンタイムパスワードとして利用することになります。

この場合、登録しているアカウントが多数ある場合は、該当のアカウントを探すのに手間が掛かるのが難点です。一方、iOS18 では、図 7 右の「パスワード」画面で「コード」を選択すると、コード一覧が表示されます。そして、該当のサービスのコードをワンタイムパスワードとして利用します。複数のサービスでワンタイムパスワードを設定している場合は、複数のコードが表示されるので、利用するサービスのワンタイムパスワードを利用します。

なお、iOS17、iOS18 ともに、表示されているコードを長押しすることでコード自体をコピーすることができます。つまり、「コードをコピーし、ワンタイムパスワード入力画面にペースト」することで、コードを覚えることなく利用可能です。

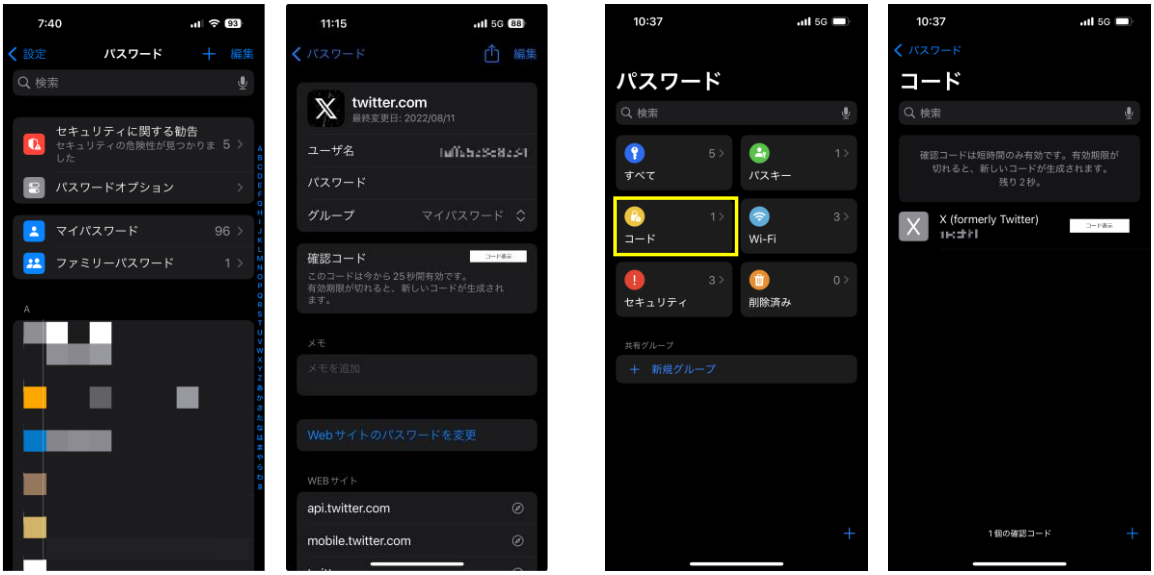

図 7　コード画面（左：iOS17、右：iOS18）

4. パスキー

パスキーは、FIDO2 の技術を使った安全な認証方式です。利用者は、生体認証などで、該当サービスの利用が可能になります。
パスキーを使うとパスワードレスとなり、パスワード漏洩による被害を防ぐことが可能になります。そのため、金融や EC サービスなどを中心に、広まりつつあります。

iOS では、パスキーも、パスワードマネージャで管理しているパスワードと紐づけられます。各サービスのログイン時にパスキーが設定されると、図 8 に示す通り、パスキーの設定確認が可能になります。

パスキーが設定されているサービスを確認したい場合、iOS17 では、図 8 左のパスワード画面から各アカウントを開くことで確認することが可能です。したがって、iOS17 では、どのサービスでパスキーを設定しているかを容易に把握できないという難点があります。一方、iOS18 では、図 8 右のパスワード画面にて、「パスキー」を選択すると、パスキーを設定されているアカウントの確認が可能です。また、一覧で表示されるため、どのアカウントがパスキーを設定しているか一目でわかります。

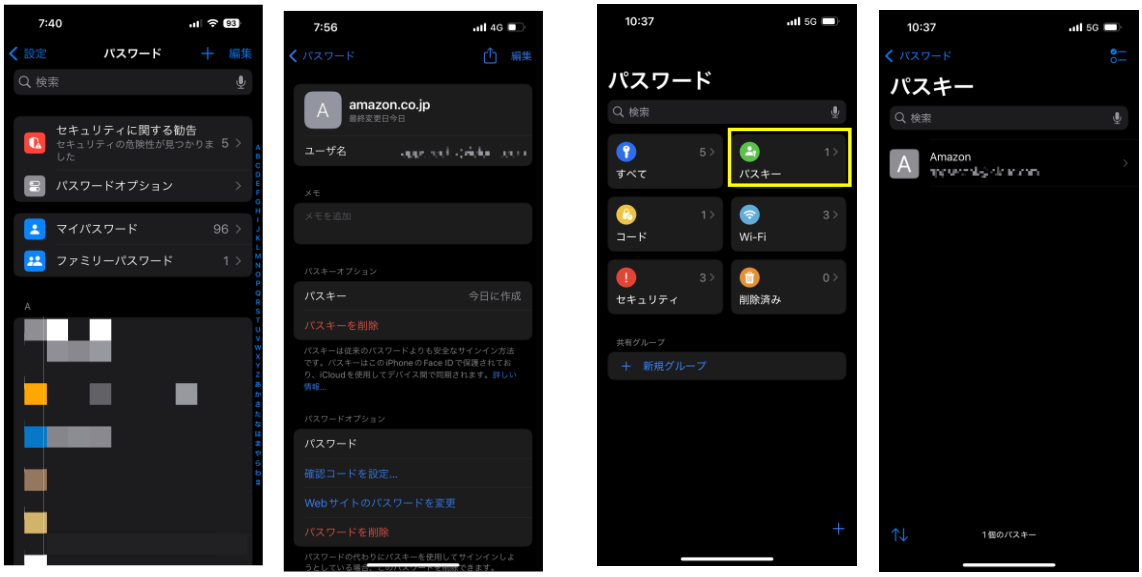

図 8　パスキー画面（左：iOS17、右：iOS18）

5. セキュリティ

パスワードマネージャでは、設定したパスワードにセキュリティ上の問題がある場合は警告が表示されます。

iOS17 では、図 9 左の「パスワード」画面の通り、画面上部に「セキュリティに関する勧告」として表示されます。さらに「セキュリティに関する勧告」を選択すると、図 9 右の「セキュリティに関する勧告」画面に示す通り、問題のあるアカウントが表示されます（実際の画面では勧告事由も表示）。

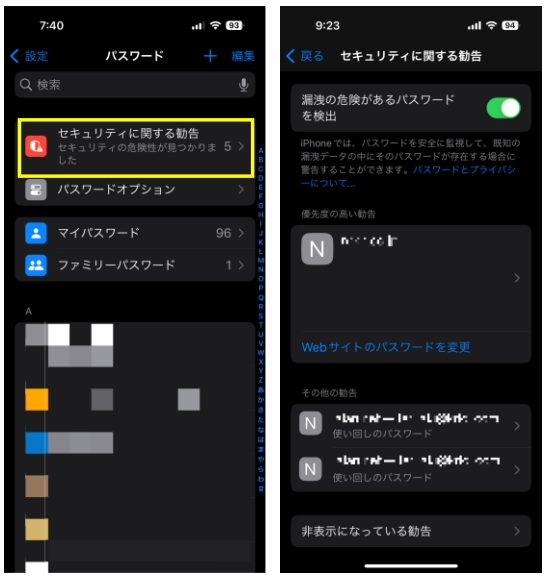

図 9　iOS17 セキュリティに関する勧告画面

一方、iOS18 では、図 10 左の「パスワード画面」にて「セキュリティ」を選択すると、「セキュリティ画面」にセキュリティ上問題のあるパスワードを一覧で表示されます。さらに、問題となるパスワードを選択することで、パスワードがどのレベルで危険なのかという説明が表示され、危険度に合わせて対象方法が表示されます。

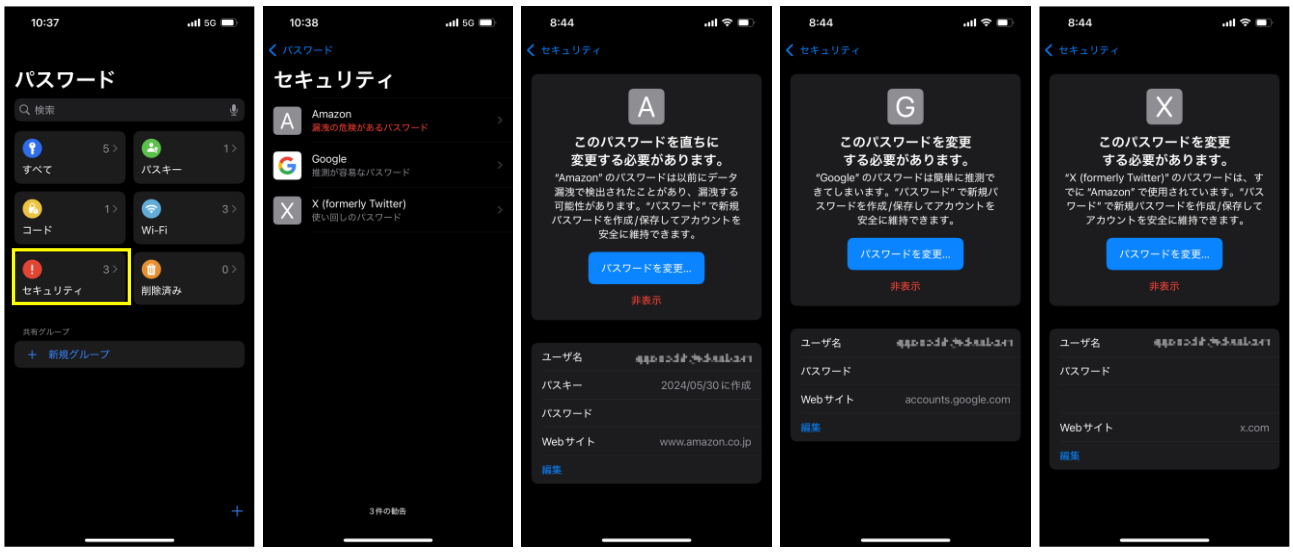

図 10　iOS18 セキュリティ

なお、iOS17、iOS18、どちらにおいても、セキュリティの問題が指摘されたパスワードについては見直しを検討することが推奨されます。

6. Wi-Fi

iOS18 では、パスワード管理機能で、新たに Wi-Fi のパスワードも管理可能になりました。

図 11 の「パスワード」画面で Wi-Fi を選択すると、登録済（過去に接続した）Wi-Fi のアクセスポイントの一覧が表示されます。あわせて本画面で各アクセスポイントの接続方式も確認できます。

この時、「セキュリティに保護されていないネットワーク」と表示されているアクセスポイントは、盗聴のリスクがあるため、利用にあたっては十分注意して利用することが推奨されます。
さらに、本画面から利用不要なアクセスポイントを削除することもできます。普段使わないアクセスポイントは削除しておくことが望ましく、意図せず自動で接続してしまうことを防ぐためにも、削除も考慮しておきましょう。

なお、キャリア Wi-Fi などデフォルトで設定されているアクセスポイントは、管理対象外であり、登録削除することはできません。図 11 では、「au_Wi-Fi2」が該当します。

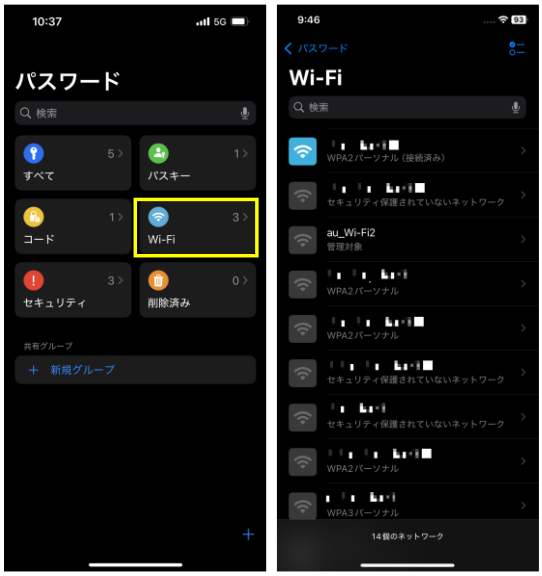

図 11　iOS18 Wi-Fi 画面

7. まとめ

パスワード管理機能は、安全にパスワードを管理するためにも有用です。機能を十分理解した上で、ぜひ利用してみてください。

さらに、iOS18 では、パスワードの管理機能が大きく向上しました。iOS18 にアップデート可能な iPhone を利用している場合は、積極的にアップデートして新しいパスワード機能を利用することが推奨されます。しかしその際、アップデートによる他のアプリへの影響については別途注意が必要です。

フィッシング詐欺など、インターネット上の詐欺の主な目的はパスワードの搾取であり、その被害件数は非常に多いです。パスワードを安全に管理するためは、パスワード管理機能をうまく利用すると良いでしょう。

■参考

スマートフォン利用シーンに潜む脅威 Top10 解説ガイド（No.1：フィッシング） | JSSEC