VPN・プロキシ・Torの違いと、VPNを選ぶときの確認項目シート

1の表で、それぞれが何をするものかを見比べます。VPNを使うと決めたら、3の項目を候補ごとに上から確かめます。

確認日：2026-10-21（サービスの内容や画面名は変わることがあります）

1. 3つの違い

	VPN（個人向けのVPNサービス）	プロキシ	Tor（Tor Browser）
しくみ	自分の機器から、VPN事業者の出口サーバーまでの通信をすべて暗号化する	代わりにインターネットにつなぐコンピューターやソフト（「代理」）。会社などの内部のネットワークとインターネットの間に置かれる	Torネットワークのリレー（サーバー）からランダムに選ばれた3つを通して送る
暗号化される範囲	出口サーバーまで。その先の通信は暗号化されない	サービスの説明で確かめる	Torネットワークまでとその中。宛先のサイトまでの暗号化はサイトしだい（HTTPS）
守られる通信	どのソフト・アプリの通信も	サービスの説明で確かめる	Torを通すように設定したアプリ（Tor Browser）の通信だけ
相手のサイトから見えるもの	VPNサーバーの場所からの接続（海外のサーバーだと、使えなくなるサービスがある）	サービスの説明で確かめる	Torネットワークからの接続（自分のIPアドレスではない）
気をつけること	通信はVPN事業者を通る。接続が切れると、暗号化されないまま通信を続けるサービスもある	サービスの説明で確かめる	遅く感じることがある。Tor経由をブロックするサイトがある。いつもと違う国からのアクセスとして、銀行などでアカウントがロックされることがある。ログインしたり名前を入れたりすれば、相手に自分だと分かる。完全な匿名は保証されない

VPNもTorも、宛先のサイトまで暗号化されるとは限りません。URLが https:// で始まるかを確かめます。

2. VPNを使う前にできること（公衆Wi-Fi）

- [ ] 近くの掲示（ステッカーなど）で、だれが提供するWi-Fiか、ネットワーク名（SSID）が案内と同じかを確かめる
- [ ] URLが正しく、https:// で始まっているか確かめる
- [ ] パソコンのファイル共有をオフにする
- [ ] 暗号化されていないWi-Fiしかないときは、スマホの回線やテザリングを使う

3. VPNを選ぶときの確認項目（1列に1社）

項目	見る所	候補A	候補B
運営会社と、無料ならどんな意図・ビジネスモデルで提供しているか	公式サイトの会社情報		
プライバシーポリシー（何を集めるか・VPNと関係ない個人情報を集めていないか）	プライバシーポリシー		
ノーログポリシー（閲覧履歴やIPアドレスの記録を取らない方針）が明文化されているか	公式サイト、アプリの説明		
VPNが切れたとき、VPNを通らない通信を止める機能があるか（キルスイッチなどと呼ばれる）	機能の説明、ヘルプ		
サーバーの場所（国内にあるか）	サーバーの一覧		
速さ	お試し期間は料金のページで確かめ、速さは自分で使って試す		
Google Play の認証バッジ（Androidのとき）	アプリのページの「データセーフティ」		
料金（公式ページで確認）	料金のページ		
確かめた日	—		

※認証バッジがあっても、安全が完全に保証されるわけではない。

※Androidでは、端末によっては、設定アプリのVPNの設定に、VPNを通らない通信を止める項目がある。

4. Torを使うとき

- [ ] Tor Browser は公式のダウンロードページから入れる（Tor Browser は無料。お金を求める「Tor Browser」は偽物）
- [ ] VPNとTorを一緒に使わない（プライバシーを損なわずに併用する方法を知っている上級者でない限り、公式はすすめていない）

出典：国家サイバー統括室（NCO）「インターネットの安全・安心ハンドブック」、総務省「公衆Wi-Fi利用者向け 簡易マニュアル」「国民のためのサイバーセキュリティサイト」用語集、The Tor Project 公式サポート、Google（Android 公式サイトの記事、2025年6月）、Google Play ヘルプ、Android ヘルプ、Android Enterprise ヘルプ