

SEO tool	https://totheweb.com/learning_center/tool-test-google-title-meta-description-lengths/			
Column A	Column B Competitor site #1	Column C Competitor site #2	Alternative version #1	Alternative version #2
			Provide an alternative to column B	Provide a 2nd alternative to column C
Main title	VPNとは？日本で本当に必要？仕組みと重要性を検証 2022年	VPNとは？その仕組みは？初心者向けガイド2022年版	VPNの仕組みとは？日本で必要な理由は？ポイントを解説 2022	VPNの機能とは？ビギナー向け解説 2022年版
Breadcrumb 4 or 5 words used for mobile view.Needs to fit on one short line	VPNとは？	VPNとは？その仕組みは？	VPNについて	VPNとその機能とは？
SEO Title tag (check in SEO tool) Max 580pixels	VPNとは？日本で本当に必要？仕組みと重要性を検証 2022年	VPNとは？その仕組みは？初心者向けガイド2022年版	VPNの仕組みとは？日本で必要な理由は？ポイントを解説 2022	VPNの機能とは？ビギナー向けガイド 2022年版
Slug needs to be 3 or 4 words)	vpnとその重要性-初心者向けvpnガイド/	vpnの初心者完全ガイド/	VPNの仕組みと重要性をやさしく解説/	VPNビギナー用ガイド完全版/
meta description (check in SEO tool) Max 920 pixels	VPNは本当に必要なのでしょうか？iPhoneなどスマホでの必要性、プライバシー保護やセキュリティ対策に役立つVPNの仕組みを検証していきます。	この初心者向けガイドで、「VPNとは何ですか？」、「VPNはどのように機能しますか？」などの質問に対する回答をご覧ください。クリックして、詳細な記事をお読みください。	日本でVPNが必要な状況とは？VPNの仕組みを解説しながら、VPNを使っていることや、VPNが個人情報やデータの保護にどう役立つのかを解説します。	VPNの基本的な仕組みや、VPNの役割についての質問にお答えします。これを読めば、ビギナーの方でも今日から簡単にVPNをご使用いただけます。

<https://www.comparitech.com/blog/vpn-privacy/what-is-a-vpn-connection/>

Title:VPN接続とは何か、その役割とは、どう設定するのか？

VPNについて、またVPNを利用した方がいい理由について説明します。VPNの設定方法と、最適なVPNプロバイダーを詳しくご紹介していきます。

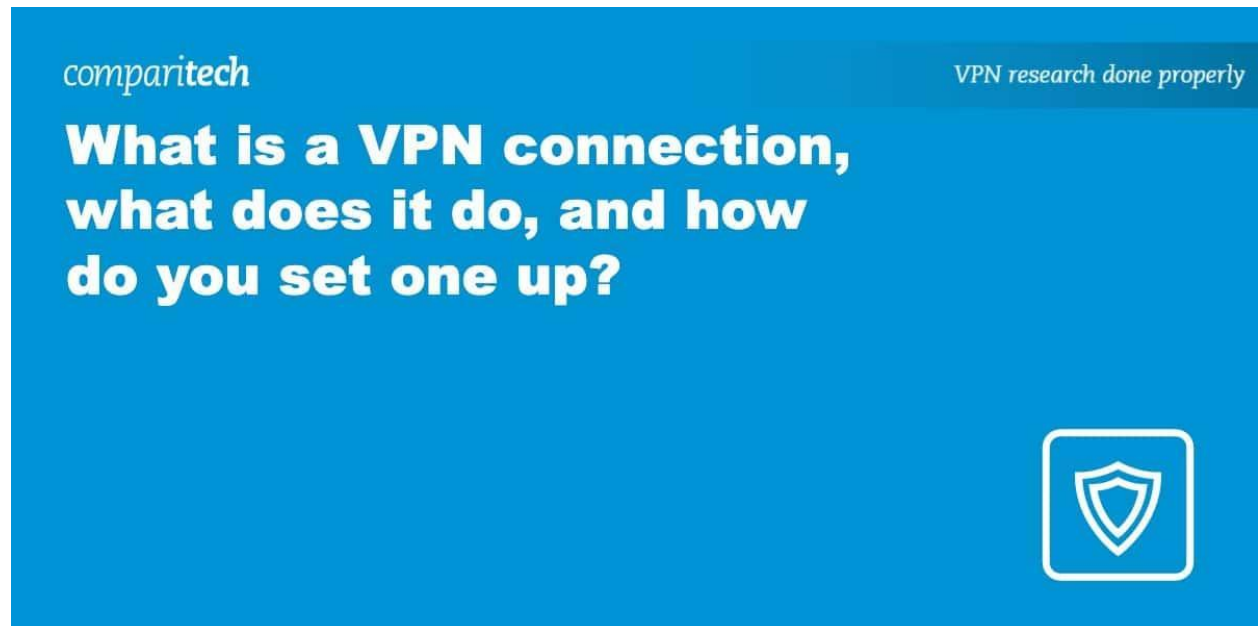


Image alt text: VPN接続とは何か

近年、VPNという用語をより頻繁に耳にするようになったのではないのでしょうか。VPNは、Virtual Private Network(仮想プライベートネットワーク)の略で、オンラインでのアクティビティをより安全にするなどの目的で使用されます。その目的のひとつだけをとってみても、当社はすべての人にVPNの使用を推奨しています。

VPNには、セキュリティの向上以外にも、地理的制限のあるコンテンツのブロックを解除したり、政府の検閲を回避したりできるという利点があります。VPNについてもっと知りたいなら、当社のウェブサイトはうってつけの場所です。ここでは[日本向けのおすすめのVPN](#)(とあまりおすすめできないVPN)を継続的にレビューし、テストしていますので、必要な知識をすべてお伝えすることができます。[日本でIPアドレス](#)を取得するのに適したVPNもテストし、レビューしています。

この記事では、VPNとは何か、どのように機能するのか、VPNで何ができるのかについて、より詳しく説明します。また、適切なVPNサービスを選択するためのいくつかのヒントを提供し、トップクラスのVPNプロバイダーについてお伝えします。それでは始めましょう！

VPN接続とは何ですか。また、どのように機能しますか？

一般的なVPNは、VPNプロバイダーが運営する、世界中に点在するサーバーのネットワークから構成されています。ユーザーがVPNサービスにサインアップし、デバイスを接続すると、2つの重要なことが起こります。

VPN接続の主要な要素は以下の通りです：

- 接続された機器との間を往来するトラフィックはすべて暗号化されます。
- 暗号化されたトラフィックは、ユーザーが選択したロケーションにある中間サーバーを経由します。

この2つの機能を別々に紹介して、そのメリットを説明していきます。

VPNは、すべてのインターネットトラフィックを暗号化します

すべてのトラフィックを暗号化することで、オンラインアクティビティを監視されることがなくなります。つまりすべての情報が安全であるということです。トラフィックが傍受されても、それが解読されることはありません。VPNを利用しない場合、お使いのインターネットサービスプロバイダー（ISP）は、訪問したサイト、使用したアプリケーション、ダウンロードしたファイルなど、すべてのオンラインアクティビティを見ることができます。VPNを使用している場合は、プロバイダーはこうしたことができません。

つまり、ネットワークを監視しているかもしれない第三者にアクティビティを見られないことがない、ということでもあります。第三者とは、学校やオフィスなどのネットワーク管理者、政府機関、あるいはハッカーなどです。出張が多く、[公共Wi-FiWi-Fiのホットスポットを頻繁に](#)利用する方は、特にハッカーが脅威となるかもしれません。ハッカーは、安全が確保されていないネットワークに潜んで情報を盗み

出そうとすることが分かっています。安全性を確保するために、オープンWi-Fiネットワークに接続する際には[毎回VPNを使用する](#)べきです。

VPNを利用すれば、詮索される心配をせずに、通常のネット利用が可能になります。これには、ブラウジング、[ストリーミング](#)、[トレント](#)、[ゲーム](#)など、インターネットに接続して行うあらゆるアクティビティが含まれます。多くの企業が、通信とプロセスの安全性、機密情報の漏洩防止、ハッカーに対する脆弱性の低減の手段としてVPNを利用しています。

VPNは合法なのか、疑問に思われるかもしれません。ほぼすべての国で、完全に[VPNの使用は合法](#)です。

VPNは使用中のIPアドレスを隠します

では、中間サーバーについてはどうでしょうか。実はここからが面白い部分です。

ネットワーク内の各ハードウェアは、インターネットプロトコルアドレス(IPアドレス)と呼ばれる固有の識別子を持っています。これはご使用のISPによって割り当てられるもので、訪問するウェブサイトには訪問者のおおまかな所在地を晒してしまうことがあります。

VPNユーザーが接続するサーバーの場所を選べることは先に述べたとおりです。どのプロバイダーも、利用者が設置国を基準にしたサーバーの選択を許可しています。プロバイダーによっては、より具体的に都市名を指定させてくれる場合もあります。

いずれにせよ、接続が完了すると、既存のIPアドレスは完全に隠され、選択した場所のIPアドレスに置き換えられます。IPアドレスは、ウェブサイトがお客様のデバイスの位置を検出するために使用されます。多くのサイトでは、IPアドレスのみに基づいてコンテンツへのアクセスをブロックしています。

つまり、IPアドレスを置き換えることができれば、自分のロケーションを偽装して、どこか別のロケーションにいるように見せかけることができるのです。

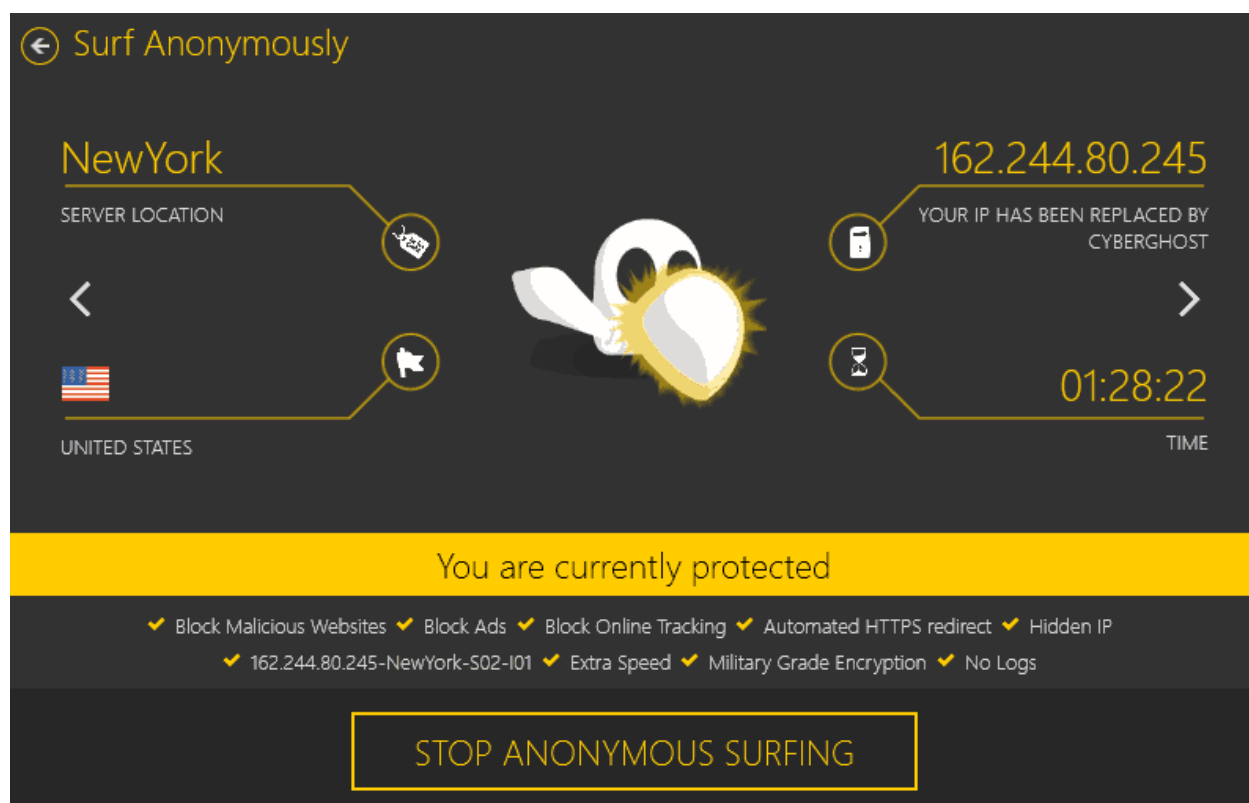


Image alt text: CyberGhost サーフィン情報

これには、いくつかの大きなメリットがあります：

地理的制限のあるコンテンツへのアクセス

以下のような地理的制限のあるWebサイトへのアクセスを可能にします：

サイトの種類	例
人気ストリーミングサイト	Netflix 、 Hulu 、 HBO 、 Amazon Prime Video 、 BBC iPlayer
スポーツ専用ストリーミングサイト	beIN sports 、 ESPN 、 BT Sport 、 Eurosport
ニッチなストリーミングサイト	Screambox 、 Twitch 、 Hotstar

ストリーミング配信元によりアクセスが許可されている地域のVPNサーバーに接続するだけで、ご希望のコンテンツを楽しむことができます。

政府による検閲の回避

VPNを利用すると、居住国ではブロックされている可能性のあるサイトにアクセスすることができます。例えば、国によっては、Facebook、Google、YouTube、Skype、WhatsAppなどをブロックしている場合があります。VPNを介してこれらのサイトにアクセスする場合、トラフィックは仲介のVPNサーバーを経由してトンネリングされます。VPNサーバーは検閲リストに載っていないため、トラフィックはブロックされず、問題なく検閲対象のコンテンツにアクセスすることができます。

匿名でのトレント

ほとんどのVPNプロバイダーは、共有IPアドレスを使用しています。つまり、IPアドレスが割り当てられると、他のユーザーも同じものを使用することになります。このため、トレントのようなアクティビティを追跡して特定のユーザーを割り出すことは事実上不可能です。トラフィックが暗号化されているため、ISPなどの詮索者は、どのような方法を使っても何がダウンロードされているかを知ることはできません。一方、詮索者がトレントネットワークに接続していれば、著作権侵害のケースと同様、何がダウンロードされているかを知ることができるようになります。しかし、VPN接続をしていれば、身元を知られることはないでしょう。

VPNのセットアップ方法

一度VPNプロバイダーを選んでしまえば、一般的にVPNサービスの利用は簡単です。プロバイダーによって多少の違いはありますが、基本的な手順は以下の通りです。

VPN接続のセットアップ方法は以下の通りです：

1. ご自身のニーズを満たしてくれる、評判の良いプロバイダーを選びましょう。当社のおすすめは[NordVPN](#)です。
2. トライアルまたは有料プランに申し込みます。通常はプロバイダーのウェブサイトから申し込みますが、中には関連アプリから契約できるものもあります。(モバイルデバイスでは一般的)
3. 通常メールで送信されるVPNの資格情報をメモします。
4. お使いのOSに対応したアプリをダウンロードし、インストールします。ほとんどのトッププロバイダーは、WindowsとMacOS用のデスクトップクライアント、およびAndroidとiOS用のモバイルアプリを提供しています。一部は、他のOSやデバイスに手動で設定することができます。
5. アプリを起動し、資格情報を使ってサインインします。
6. 必要であれば、設定や環境設定を調整してください。
7. サーバーの場所を選択し、アプリが接続を確認するのを待ちます。
8. インターネットやその他のアプリケーションは、通常通りご利用ください。

もし、これらの手順で何か問題があれば、VPNプロバイダーのカスタマーサポートチームにお問い合わせください。

VPNの選び方

VPNを選択する際には、様々なポイントに注意する必要があります。以下は簡単なチェックリストですが、後ほどそれぞれをもう少し詳しく掘り下げていきます。

以下がVPNを選ぶ際のポイントです：

1. 地理的制限のあるコンテンツへのアクセス
2. 高速スピード
3. 強力な暗号化と+αのセキュリティ機能
4. 最小限のロギング
5. マルチプラットフォーム対応
6. 金額に見合った価値
7. 優れたカスタマーサポート

1.地理的制限のあるコンテンツへのアクセス

VPNを利用する最大の理由の1つは、Netflix、Hulu、BBC iPlayerなど、地理的制限のあるサイトへのアクセスです。これらのウェブサイトの多くは、VPNの利用を取り締まっています。こうしたサイトは、VPN由来のIPアドレスを突き止めるためにリソースを割き、積極的にブロックしています。つまり、実際の居住国のVPNサーバーに接続していても、プロキシエラーが表示される可能性があるのです。

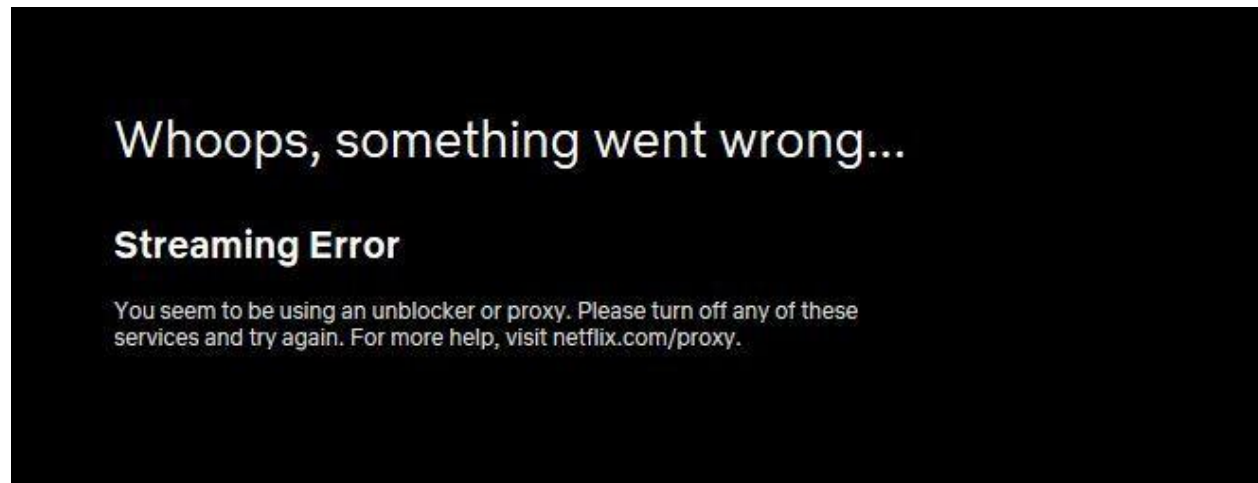


Image alt text:Netflixのプロキシエラー。

幸い、一部のVPNプロバイダーは先手を打っているため、ユーザーは未だにこうしたコンテンツへのアクセスを楽しむことができます。しかし、これにはリソースが必要なので、まだすべてのプロバイダーが参入しているわけではありません。制限付きコンテンツへのアクセスを優先するのであれば、選択したプロバイダーがこれを重視しているかどうかを確認する必要があります。

2.高速な回線速度

トラフィックが中間サーバーを経由するため、VPNを使用するとインターネット速度が若干遅くなります。VPNサービスによっては、回線速度に与える影響が大きいものもあります。ブラウジングに顕著な影響を与えるほど回線速度が落ちる場合もあれば、大容量ファイルのダウンロードやアップロードなどを行ったときにのみ影響を実感する場合もあります。

当社がVPNサービスをレビューする際は、速度に細心の注意を払い、ランキングに反映させています。当社は定期的にトップ[VPNの](#)スピードパフォーマンスをテストしており、リンク先のチャートで最新の結果を見ることができます。

3.強力な暗号化と追加のセキュリティ機能

実用性の他にも、ご自身のデータが安全かを確認する必要があります。つまり、VPNサービスには強力な暗号化を想定しておく必要があるのです。一般的に128ビットと256ビットのAES暗号が使用されており、これらは非常に安全であると考えられています。

調べてみると、プロトコルという言葉にも出くわすはずです。これは、VPNがデータを送信する際のフォーマットです。プロトコルの違いにより、セキュリティや速度のレベルが異なります。当社は通常、オープンソースで公開監査の対象となるOpenVPNプロトコルを推奨しています。[その他の一般的なプロトコル](#)には、L2TP/IPSec、SSTP、IKEv2、PPTPなどがあります。PPTPは最も安全性が低く、最後の選択肢に留めておくべきです。

また、トップランクのVPNには、以下のような追加機能が搭載されています：

- **DNSリーク対策**：DNSリクエストが暗号化されたVPNトンネルの外部に送信されないようにします。
- **キルスイッチ**：VPN接続が切断された場合、インターネット接続を切断します。
- **自動的なWi-Fi保護**：Wi-Fiホットスポットに接続するたびにVPN接続を開始します。
- **DdoS対策用サーバー**：[DDoS攻撃](#)から守るための専用サーバー。

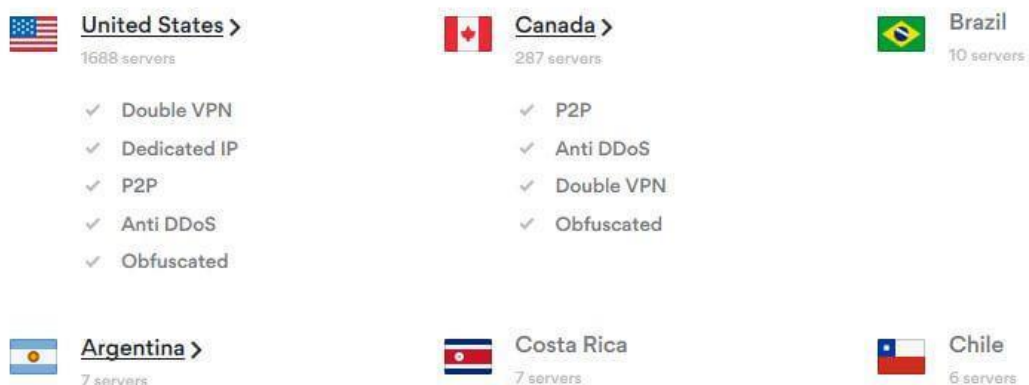


Image alt text:NordVPNのVPNサーバーの所在地。

Image caption:NordVPNのサーバーの所在地の一部には、DdoS対策機能が装備されているとの記載があります。

最も重要な追加セキュリティ機能は、DNSリーク対策とキルスイッチですが、その他にも特定のニーズに応じて重要になってくる機能があるかもしれません。

4.最小限のロギング

ほとんどのプロバイダーは何らかのログを残していますが、ログの種類は様々なため、それぞれを検討する必要があります。まず、アクセスしたウェブサイトやダウンロードしたファイルなどのトラフィックログがあります。信用に足るVPNプロバイダーなら、いかなる種類のトラフィックログも保存していないはずです。「ノーログ」「ゼロログ」という表現は、通常このようなロギングを指しています。

一方、多くのプロバイダーが接続ログを記録しています。これらは通常、使用した帯域幅、接続回数や接続時間などのメタデータの形式を取ります。これらの情報が保持されている場合は、トラブルシューティングやデータ通信の上限を超えないようにする目的で使用されます。重要なのは、IPアドレスを含む個人を特定できる情報をプロバイダーに記録されないことです。

さらに匿名性を高めたいのであれば、サインアップ時に最小限の情報だけを要求するVPNを探すとよいでしょう。多くのプロバイダーは、ビットコインやその他の暗号通貨を使った支払いオプションを提供しています。また、[Torブラウザ](#)でアクセスできるように、自社サイトの.onionバージョンを持つプロバイダーもあります。例えば、ExpressVPNはビットコインを受け入れ、.onionサイトを持っているので、使い捨てメールアドレスを使用すれば、ほぼ匿名でサインアップできます（完全に匿名というわけにはいきませんが）。

5. マルチプラットフォーム対応

検討中のVPNがお持ちの全デバイスに対応したアプリを提供していることを確認する必要があります。手動での設定も可能な場合が多いですが、使いやすいアプリがあるに越したことはありません。**Windows、MacOS、iOS、Android**は一般的にカバーされていますが、プロバイダーによっては、これらのうち1つ以上のアプリが欠落している場合があります。



Image alt text: 各種プラットフォーム用ダウンロードボタン

Linuxユーザーの場合、専用アプリを作るプロバイダーは多くありませんが、多くのプロバイダーが同OSのサポートを提供しています。また、ルーターレベルでトラフィックを保護したい場合、ほとんどのVPNはそこでも役に立ちます。多くは特定のタイプのルーターに設定することができ、中にはすでに自社VPNに対応したルーターを販売している企業もあります。実際、ExpressVPNはルーターのファームウェアを自社で作っています。

6. コストパフォーマンス

大抵の買い物をするときと同様に、選択したVPNにはコストパフォーマンスを求めたいですね。無料のVPNの危険性については後述しますが、有料のオプションになると、価格に幅があります。金額と価値について考える際には、このリストにあるすべての項目を考慮したいところですが、さらにいくつかのポイントがあります。

1つは、提供される同時接続数です。1つのプランですべてのデバイスをカバーでき、他に料金を支払う必要がない状態が理想的です。業界標準は同時接続数5台ですが、もっと少ない台数のところもあれば、もっと多いところもあります。

また、帯域幅に上限があるかどうかも重要なポイントです。

	Most Popular ✓	
Lite	12 Months	1 Month
\$0.00	\$5.79 per month	\$9.95 per month
• Test Keenow for FREE • <u>Daily 512MB Data Cap</u> • Unblock U.S. Content Only • No Netflix Unblocking • <u>No VPN Access</u> • No Privacy Protection • No Security Protection • No Virtual WiFi • Standard Level Support	• Unlimited Bandwidth • Worldwide Servers • Smart DNS & VPN Access • Enhanced Security & Privacy • Bypass ISP Throttling • Virtual WiFi (Windows 7+) • Platinum Level Support	• Unlimited Bandwidth • Worldwide Servers • Smart DNS & VPN Access • Enhanced Security & Privacy • Bypass ISP Throttling • Virtual WiFi (Windows 7+) • Platinum Level Support
	Billed \$69.50 (instead of \$127.20) every 12 months	Billed \$9.95 (instead of \$16.50) every month
	30-day money-back guarantee	7-day money-back guarantee

Image alt text:Keenowの価格表。

Image caption:Keenowの無料プランでは、1日あたり512MBという上限が設定されています。

これだと一般的なブラウジングにはあまり関係ないかもしれませんが、ストリーミングやトレントの利用が制限される可能性があります。ほとんどの有料VPNは帯域幅を無制限に提供していますが、中には帯域幅に上限を設けている下位パッケージもあります。

7.優れたカスタマーサポート

VPNを使用する場合、どこかの時点で支援が必要になる可能性があります。設定がうまくできない、目的のコンテンツにアクセスできない場合などに、カスタマーサポートが必要になるでしょう。

ほとんどのVPNプロバイダーは、セットアップガイド、トラブルシューティングのヒント、FAQの回答などのオンラインサポートセクションを提供しています。

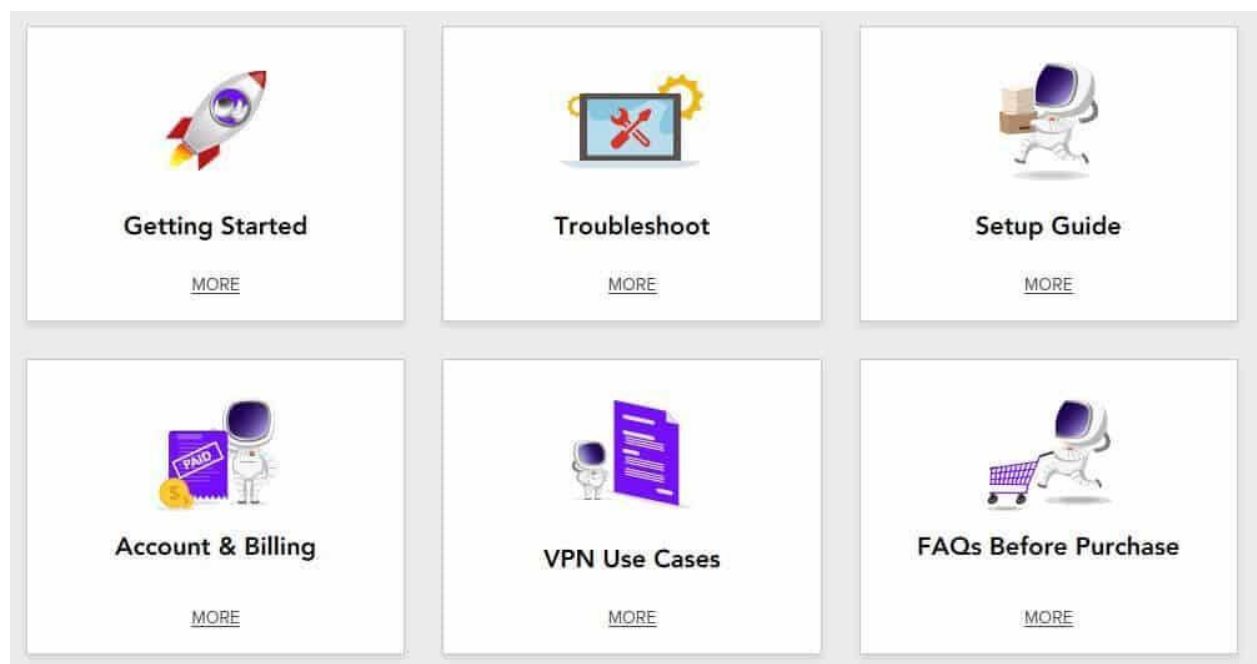


Image alt tag: PureVPNのサポートセンター

Image caption: PureVPNは、非常に充実したサポートセンターを提供しています。

また、ヒューマンサポートが必要な場合は、メールでチケットを送信するオプションを提供しているところがほとんどです。これは便利ですが、回答には数時間から数日、場合によっては数週間かかることもあります。即時の対応が必要な場合には、理想的ではありません。

幸い、多くのプロバイダーがライブチャットカスタマーサポートを提供しているため、その場でサポートを受けることができます。この種のサービスは通常、外部に委託されるため、プライバシーを重視す

るユーザーには不向きかもしれません。また、より専門的な問題については、チケットの送信を求められることがあります。それでも、年中無休24時間のライブチャットは嬉しい特典ですから、注目しておきたいポイントです。

トップクラスのVPNプロバイダー

VPNが必要な理由と、VPNを選ぶ際に考慮すべきポイントをご理解いただけたことでしょう。これでVPNパッケージにサインアップする準備が整いました。当社は多数のプロバイダーのサービスをテストし、当社のおすすめのVPNをリストアップしました。

1. [NordVPN](#)
2. [Surfshark](#)
3. [ExpressVPN](#)
4. [CyberGhost](#)
5. [Private Internet Access](#)
6. [PrivateVPN](#)
7. [AtlasVPN](#)

もう少し詳しく考察して、これらのVPNの特徴について学んでみましょう。

[1.NordVPN](#)

[1. NordVPN](#)



APPS AVAILABLE:



Website: www.NordVPN.com

Money-back guarantee: 30 DAYS

Instructions - please also translate this text from the image above

- 編集部推薦
- 利用可能なアプリ
- ウェブサイト
- 返金保証

[NordVPN](#)は手堅い選択肢で、5,000台以上のサーバーから成る巨大なネットワークを持っています。その多くは、ストリーミング、ダブルVPN、Tor over VPN、DdoS対策などに特化しています。同VPNサービスは、セキュリティとプライバシーを後押ししてくれます。ログを残さず、自動Wi-Fi保護機能を搭載しています。アプリはWindows、MacOS、iOS、Androidにダウンロードでき、一度に6台のデバイスをカバーすることが可能です。

メリット:

- 世界60カ国で5,000台以上のサーバーを運用
- スピードとセキュリティの面で妥協をしない低予算プロバイダー
- ログを残さないため、個人情報を保護することが可能
- 24時間体制のチャットサポート

デメリット:

- デスクトップアプリに慣れるまで少し時間がかかる

当社の評価トップのVPN: [Nord VPNは当社のおすすめNo.1です。](#)ストリーミングの際に確実に動作します。最大6台まで同時接続可能。30日間返金保証。

NordVPNのレビュー全文は[こちら](#)。



Translation for the banner above

NordVPNクーポン

2年プラン契約で70%OFF

割引を利用する

割引は自動的に適用されます

2.Surfshark

[Surfshark](#)は、ログを残さないという確固たるポリシーを持つ、安全性の高いVPNです。アプリは、Windows、macOS、iOS、Androidで利用できます。強固なAES暗号化機能を備え、さらに高速化を実現するWireGuardをはじめとした、安全性の高いVPNプロトコルを選択できます。同VPNは、キルスイッチ、難読化、マルウェア対策、DNSリーク対策など、多数の高度な機能を備えています。サーバーが65カ国以上に設置されているため、地理的制限や検閲を回避するのに最適なVPNです。

メリット:

- すべてのプラットフォーム向けにアプリを提供
- トレントをサポート
- 超高速スピード
- 接続数無制限
- 人気のストリーミングサービスに対応

デメリット:

- 各サーバーの速度に若干の差がある

ずば抜けた価値: [Surfsharkはコストパフォーマンスがいい](#)と言えます。すべての人気ストリーミングプラットフォームへのアクセスに使えます。約20のNetflixリージョンにアクセス可能です。ゲームやトレントのための超高速接続が期待できます。接続数は無制限です。30日間返金保証付きです。

Surfsharkのレビュー全文は[こちら](#)。

Surfsharkクーポン

2年プラン契約で2ヶ月間無料

[割引を利用する](#)

割引は自動的に適用されます

[3.ExpressVPN](#)

このVPNプロバイダーは、トップクラスのオールラウンダーです。世界94カ国に股がるサーバーネットワークで、豊富なロケーションからお選びいただけます。[ExpressVPN](#)は強力な暗号化を使用し、キルスイッチなどの追加セキュリティ機能を備えています。高速通信が可能で、人気のストリーミングサービスをロック解除できます。同時接続は5台まで可能で、Linuxを含む主要なOSでアプリが利用できます。

メリット:

- 帯域やデータ量に制限のない超高速回線
- トップクラスのセキュリティとプライバシー保護機能
- 様々なOSに対応したユーザーフレンドリーなアプリ
- 年中無休24時間のライブチャットサポート

デメリット:

- 他のプロバイダーより若干高額

高品質なオールラウンダー:[もう1つの有力なオプションです](#)。圧倒的な速さと信頼性の高いサービスを誇ります。地理的制限のある主要なストリーミングサービスや、制限付き・検閲対象コンテンツのブロック解除を得意としています。トップクラスのプライバシーとセキュリティ機能で、ログを残しません。30日間の返金保証で、リスクなくお試しください。

ExpressVPNの詳細なレビューは[こちら](#)。

ExpressVPNクーポン

割引: 年額プランで49%OFF

[割引を利用する](#) >

クーポンは自動的に適用されます

[4.CyberGhost](#)

[CyberGhost](#)は、拡張中のネットワークを運営し、強力なセキュリティと高速スピードを組み合わせ、もう1つの手堅いオールラウンダーと言えます。よくストリーミングをするなら、CyberGhostクライアントからストリーミング元を選択するだけで、自動的に適切なサーバーに接続されます。この低価格プロバイダーはログを残さないで、データの安全性も確保できます。5台の同時接続が可能で、デスクトップとモバイルデバイス用のアプリが用意されています。

メリット:

- 世界60カ国で3,700台以上のサーバーを運用
- 初心者に優しいアプリを搭載した低価格オプション
- 非常に使い勝手がいい。地理的制限付きサイトやコンテンツのブロックを解除する
- 強力な暗号化と徹底したプライバシーポリシー

デメリット:

- 高度な機能の制御が必要な場合には不向き

ストリーミングに最適: [CyberGhostは、多くの地理的制限付きコンテンツへのアクセスを提供](#)し、使いやすいアプリは初心者にも最適です。強固なプライバシーとセキュリティを備えています。競合他社と比べると、ブロックを解除できるストリーミングサイトの数が劣ります。各種プランには45日間の返金保証が付いています。

CyberGhostのレビュー全文は[こちら](#)。

CyberGhostクーポン

3年プラン契約で82%OFF

[割引を利用する](#) >

割引は自動的に適用されます

[5.Private Internet Access](#)

[Private Internet Access](#)は、安全性が高く、Redditなどのプラットフォームでユーザーから高く評価されることの多い、米国拠点の人気プロバイダーです。あらゆるプラットフォーム向けにアプリを提供している、高いカスタマイズ性を誇るノーログVPNです。そのアプリは、キルスイッチ、難読化、DNSリーク対策など、多くの高度な機能を備えています。Netflix USとBBC iPlayerへのアクセスに使えます。また、WireGuard接続を導入し、さらなる高速化を実現しています。また、30日間の返金保証を利用して、安心してお試しください。

メリット:

- 高度なカスタマイズが可能なアプリ
- ログを残さない。自動キルスイッチ、無線LAN保護機能付き
- 世界75カ国にサーバーを設置
- 最大10台まで接続可能
- 高速接続

デメリット:

- カスタマーサポートのレスポンスがやや遅い
- 競合他社に比べ、国際的なストリーミングプラットフォームとの連携が少ない

[プライバシーに強いVPN](#): アメリカを拠点としたノー[ログVPN](#)で、ログを残さないという主張を何度も法廷で立証しています。すべてのプラットフォーム向けにアプリを提供しています。高度な機能とカスタマイズのオプションを多数揃えています。トレントをサポートしています。Netflix USに使えます。30日間返金保証付き。

PIAのレビューは[こちら](#)。

Private Internet Accessクーポン

3年プラン契約で80%OFF

[割引を利用する](#) >

割引は自動的に適用されます

[6.PrivateVPN](#)

多くの競合他社よりも新しく、小規模なプロバイダーである[PrivateVPN](#)には、様々なメリットがあります。高速な通信スピードと、多数の人気ストリーミングサイトのブロックを解除できることで知られています。さらに、データをログに残さない安全性も備えています。価格も手ごろで、同時接続数は6台、主要なOSに対応したアプリも用意されており、改めて検討する価値は十分にあるでしょう。

メリット:

- 各種人気ストリーミングサイトのブロック解除で好評を博している
- 当社テストで驚くべき速度が明らかに
- 最大6台のデバイスを同時接続可能

デメリット:

- 新顔プロバイダーのため現在進行形でネットワークを拡張中で、選択できるサーバーの数が少ない
- サポートスタッフは欧州の営業時間内にのみ対応

良好なスピード: [PrivateVPNは家族での使用に適したオプションです](#)。HDストリーミングには概ね適しています。同一アカウントで最大6台まで使用可能。プライバシーやセキュリティ機能が充実しています。サーバー台数がもっと増えれば嬉しいところ。24時間365日のサポートはありません。30日間返金保証付き。

PrivateVPNの詳細なレビューは[こちら](#)。

PrivateVPNクーポン

3年プラン契約で85%OFF

[割引を利用する](#) >

割引は自動的に適用されます

[7. AtlasVPN](#)

[AtlasVPN](#)は、Netflix、iPlayer、Hulu、HBO Maxといった多数の国際的ストリーミングプラットフォームへのアクセスに使える、高速で信頼性の高いVPNです。WireGuardの実装により、ストリーミングに最適なVPNとなっています。また、ログを残さないポリシーと強力なAES暗号化により、高い安全性を確保しています。また、キルスイッチやDNSリーク防止機能も備えています。さらに同VPNはお手頃で、30日間の返金保証付きでトライアル可能です。

メリット:

- ストリーミングサービスとの相性は抜群
- 強固なセキュリティ
- 同時接続数無制限
- 個人を特定できるようなログを残さない
- 高速スピード

デメリット:

- より詳細なプライバシーポリシーがあればなお良い
- カスタマーサービスの対応が悪い
- 中国では使えない

満足のいくスピード: [AtlasVPNは常に](#)ストリーミングをしたい人向けのオプションとして名前が挙がります。高速Wireguardコネクションを搭載。世界31カ国にサーバーを設置。すべてのプラットフォーム向けに秀逸なアプリを提供しています。強力なセキュリティと優れたパフォーマンス。トレントをサポートしています。30日間返金保証付き。

AtlasVPNの完全レビューは[こちら](#)。

AtlasVPNクーポン

3年プラン契約で82%OFF

[割引を利用する](#) >

クーポンは自動的に適用されます

VPN接続に関するFAQ

VPNは何のためにあるのですか？

これについては上記で詳しく説明しましたが、ここではVPNで何ができるのか、簡単におさらいしておきましょう。VPNは、お使いのデバイスを往来するすべてのトラフィックを暗号化し、ユーザーの実際のIPアドレスを隠蔽します。以下のようなケースに使用できます：

- 地理的制限のあるストリーミングサイトのブロックを解除する。
- 中国やUAEなどの国で検閲対象となっているコンテンツへのアクセス
- ISPなどの詮索者がトラフィックを読み取れないようにする
- 公共Wi-Fiへの接続を保護し、ハッカーを寄せ付けない
- 匿名でのトレント
- 詐欺警告を誘発せずに海外のオンライン・バンキングにアクセスできる

どのVPNでもセキュリティとプライバシーを保護してくれますか？

VPNはオンラインセキュリティとプライバシーを保護するべきですが、必ずしもそうしてくれるとは限りません。多くのVPNは、漏洩などの脆弱性を抱えており、プライバシーやセキュリティの観点からは使い物になりません。残念ながら、VPNのコストは必ずしも品質に直結しません。

とはいえ、無料のVPNは、しばしばメリットよりもデメリットが大きいことに注意する必要があります。こうした企業は、直接お金を請求してこなくても、何らかの形でユーザーから利益を得ているのです。

多くの企業はユーザーの活動を追跡し、広告主に販売するためのプロフィールを構築しています。また、[VPNアプリの中には、マルウェアを搭載しているもの](#)や、安全性を誇張しているものもあります。

無料のVPNを使用することはできますか？

様々なVPNサービスを調べ始めると、間違いなく大量の[無料サービス](#)に出くわすでしょう。もちろん、こうしたサービスを無料で使えるのは魅力的に映るでしょう。しかし、先の回答で述べたように、こうした無料サービスは、プライバシーやセキュリティの面が不十分になりがちです。そう聞いてもまだピンと来ない方は、ユーザーエクスペリエンスの面からも検討してみてください。

先ほど、ユーザーのプロフィールが広告主に販売される可能性について触れました。サービスによっては、閲覧中に訪れたサイトに広告やクッキーを注入したり、VPNクライアント自体に広告を設置したりするだけです。

しかし、それだけではありません。無料VPNサービスは、通常、非常に多くのユーザーを抱え、その全員が限られた容量の少数のサーバーを共有しています。そのため、待ち時間が長くなりがちで順番待ちシステムを採用することになります。また、接続できたとしても、速度が遅く、信頼性が低い接続のため、目的のサイトにアクセスできない可能性があります。

当社としては通常、これらのポイントを考慮して、どうしても止むを得ない場合以外は無料のVPNサービスを利用しないことをお勧めしています。

VPNの使用は難しいですか？

VPNは驚くほど強力なツールですが、初心者でも非常に簡単に使用できます。上記のハウツーセクションの手順に従うだけで、すぐに使用可能になります。上記のリストにあるVPNは、いずれも直感的に操作できるアプリを提供しています。しかし、様々な設定を扱うのが不安な方は、CyberGhostのような、導入後すぐに簡単に使える初心者向けのVPNを選ぶとよいかもしれません。

VPNが動作しているか確認するにはどうすれば良いですか？

VPNアプリは、VPNサーバーへの接続が確立されたことを明確に表示するはずですが、接続されているかどうか（そして接続先が正しいかどうか）を自分で確認したい場合は、IPアドレスを調べることができます。whatismyipaddress.comにアクセスすると簡単です。さらに一歩進んで、VPNから情報が漏れていないことを確認したい場合は、browserleaks.comなどのツールを使用してもいいでしょう。

VPNが動作しない場合は？

他のソフトウェアと同様、VPNを動作させようとする際に、問題に直面することがあるかもしれません。幸いなことに、VPN業界は非常に競争が激しいため、提供するサポートのレベルに関して、各サービスが互いにしのぎを削っているのが通例です。高い評価を得ているプロバイダーの多くは、ウェブサイトで多くのチュートリアルやFAQを提供し、メールでの問い合わせには1日か2日以内に対応しています。トップランクのVPN（上記のリストにあるものを含む）は、ライブチャットでのサポートを提供しており、多くの場合、24時間体制です。

これらのオプションをすべて試してもVPNがうまく機能しない場合、多くのVPNが返金保証を提供しています。

プロバイダーが現在使っているデバイス用のアプリを提供していない場合はどうすればよいですか？

各種VPNプロバイダーは、提供するアプリの種類を増やしており、その多くは、最も一般的なOS（Windows、MacOS、iOS、Android）以外にも対象を広げています。例えば、Linux用のアプリを提供しているところがあれば、Amazon Fire TV用のアプリを提供しているところもあります。

これ以外にも、家庭にはインターネットに接続された機器がたくさんあるため、サポートされていない機器を接続したくなる可能性はあります。このような場合、いくつかの選択肢が考えられます（これら

の選択肢が利用可能かどうか、また設定方法については、VPNプロバイダーのウェブサイトを参照してください）。

- VPNのOpenVPN設定ファイルを使用して、お使いのデバイスにVPNを手動で設定できる場合があります。
- 一部のVPNでは、AndroidベースのOSを搭載した特定のデバイスを保護するために、Android APKを直接ダウンロードすることができます。
- 多くのVPNは、家庭用ルーターでの手動設定に対応しています。これにより、ルーターに接続されたすべての機器を同時に保護することができます。

VPNとプロキシの違いは何ですか？

コンテンツのストリーミングを主な目的とする場合、DNSプロキシプロバイダーがその役割を担っている、という主張を目にしたことがあるかもしれません。しかし、Netflixはこうしたサービスをいとも簡単にブロックします。実際のところ、Netflixはプロキシを使ったアクセスに目を光らせているため、上手くいく確率は低いでしょう。

VPNとDNSプロキシの大きな違いは、暗号化です。後者はトラフィックを暗号化しないため、アクティビティが公開されます。つまり、ISP、ネットワーク管理者、ハッカー、その他あらゆる詮索者が、あなたがオンラインで何をしているかを見ることができるのです。

さらに、DNSプロキシは無料のVPNと多少似たところがあり、一般的に選択できるロケーションが多くありません。この問題をクリアしており、ストリーミングサービスで確実に動作するプロキシとして、ExpressVPN MediaStreamerのDNSサービスがあります。このサービスはすべてのサブスクリプションに付属しており、VPNサービスとの併用、または単独で 사용할 ことができます。

もう一つ注意すべき点は、これらのサービスが情報の販売や広告の挿入、その他の怪しげなビジネス手法といった、無料VPNと同様の手口を使用している場合が多いということです。