

OUCH!

Connect 月間セキュリティ啓発ニュースレター

仮想プライベートネットワーク(VPN)

はじめに

外出中、例えば地元のレストランやカフェにいる時、または旅行でホテルや空港に滞在している時に、インターネットにアクセスするため、公衆Wi-Fiが必要になったことがありませんか。こうした公衆用のネットワークはどの程度安全で、誰かがあなたのオンラインでの動向を見ているかもしれないと考えたことはないでしょうか。あるいは、自宅で契約しているISP（インターネットサービスプロバイダ）を信用しておらず、あなたのオンラインでの動向をISPに監視されないようにしたいと考えたことはないでしょうか。そんな時は、VPN（VIRTUAL PRIVATE NETWORK：仮想プライベートネットワーク）と呼ばれる技術を使用して、あなたのオンラインでの活動やプライバシーを保護しましょう。VPNとは、あなただけの暗号化されたトンネルを作成する技術であり、この技術によって、他人があなたの動向を盗み見たり、監視したりすることが非常に困難になります。また、VPNは現在地を隠してくれるため、訪問したウェブサイトには自分の居場所を特定されにくくなるというメリットもあります。

どのように機能するのか

VPNは、あなたが選択したVPNプロバイダに対して、プライベートで暗号化されたトンネルを作成することで使えるようになります。全てのオンラインでの活動は、このトンネルを通してVPNプロバイダのネットワークを経由し、意図した宛先に到達します。例えば、あなたはフロリダ州タンパにいて、ドイツのミュンヘンにあるVPNサーバに接続するとしましょう。すると、あなたがアクセスする全てのウェブサイトは、あなたがミュンヘンからアクセスしているようにしか見えなくなります。このVPNは誰でも簡単に使うことができます。最初のステップは、信頼できるVPNプロバイダを探すことです。その後そのプロバイダでアカウントを作成します（たいていの場合、VPNプロバイダのサービスに課金することが必要になるでしょう）。アカウントを作成したら、プロバイダのVPNソフトウェアをインストールして設定します。ここまで準備ができたなら、あとは普段と同じようにインターネットにアクセスするだけです。インストールしたVPNソフトウェアが暗号化されたトンネルを作成し、あなたが特別意識しなくてもオンラインでのプライバシーの保護してくれるようになります。

VPNプロバイダの選択

あなたのオンラインでの活動は、あなたが選択したVPNプロバイダが提供できる範囲でのみセキュアでプライベートなものになります。必ず信頼できるプロバイダを選択しましょう。VPNプロバイダを選択する際の重要なポイントを次に挙げます。



ログの取得：ログを全く残さず、プライバシーに特化しているサービスを探しましょう。あなたのVPNプロバイダがログを全く取得しないのであれば、あなたがオンラインで何をしていたのか、他人が過去にさかのぼって確認することは困難になります。



プロバイダの所在地：VPNプロバイダは様々な国に存在します。必ず厳しいプライバシー法が制定されている国が所在地となっているプロバイダを選択しましょう。プライバシー関連の法律が少ない、もしくは規制が弱い国のVPNプロバイダは、あなたに関する情報が強制的に開示させられてしまう可能性があります。



サーバ：あなたが必要としている国にサーバが置かれているVPNサービスを探しましょう。VPNプロバイダは、世界中で何千台に及ぶサーバを有しています。インターネットにアクセスした際に、通信が特定の国から送られているように見せる必要がある場合、選択したVPNプロバイダがその要求を満たせるか確認する必要があります。



互換性：様々な機種のコピュータやモバイル機器で動作するサービスを探しましょう。例えば、WINDOWSノートパソコンとタブレット、IPHONEを使用している場合、これら全てのデバイスで動作するVPNサービスが必要になります。

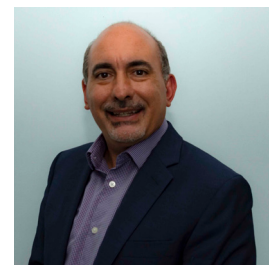


無料のサービスを避ける：「無料の」VPNサービスには特に気を付けましょう。彼らがどのように利益を得ているのか、またいかにしてビジネスを継続しているのかを考える必要があります。無料のサービスはあなたの情報を収集し、販売する可能性があります。

VPNは、あなたのオンラインでのプライバシーを保護する素晴らしい技術です。しかし、VPNはコンピュータやデバイス、オンラインアカウントをセキュアにするものではありません。そのため、VPNを使用している場合、デバイスのアップデートやスクリーンロックの使用、全てのアカウントに対する強力なユニークなパスワードの設定といった、基本的なセキュリティ対策を常に実施するように心がけてください。

ゲストエディタ

フィル・ジョンジー氏 (@peakreflections) は、セキュリティやフォレンジクス、監査の分野で業務経験を持つ、フロリダ州パームビーチ郡に住むIT専門家です。ジョンジー氏は、デジタルフォレンジクスとセキュリティ基礎のSANS認定資格を有しており、OUCHのコミュニティ審査委員を務めています。彼は、セキュリティを万人にとって身近なものにするための活動を続けています。



リソース

パスワードとその管理を容易なものにする:

<https://www.sans.org/u/Sd8>

モバイル機器の安全性を確保するために:

<https://www.sans.org/u/Sdd>

マルウェアの侵入を阻止する:

<https://www.sans.org/u/Sdi>

OUCH!はSANS Security Awareness プログラムによって発行され、Creative Commons BY-NC-ND 4.0 licenseに従って配布されます。このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。翻訳その他に関しては、www.sans.org/security-awareness/ouch-newsletter までお問合せください Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: 小山 裕之, 時田 剛