名前: 日付: 得点:

チェックポイント 10

VPN FAQ

インタラクティブ ワークシートと学習ガイド

出典: VPN.com の VPN ガイド: **https://www.vpn.com/vpn/**

VPNとは ワークシート

チェックポイント 10: VPN FAQ – 基礎（パート A）

仮想プライベートネットワークの利用について、見込み客からよくある質問と回答を確認しましょう。

Q1: VPN とは何で、どのような仕組みですか?

仮想プライベートネットワーク(VPN)は、インターネット接続を暗号化し、通信を安全なリモートサーバー経由で送ります。これにより公開IPアドレスが隠れ、VPNトンネルを通る通信について、ローカルネットワークの観察者やISPに見える情報が限られます。

Q2: なぜ VPN を使うべきですか?

VPNはデジタルプライバシーを守り、カフェや空港などの公共Wi-Fiでの接続を保護します。また、ISPが暗号化された通信の種類を識別できない場合には、通信内容に応じた速度制限を減らせる可能性があり、地域制限を回避して世界中のコンテンツにアクセスでき、リモートワークのリソースを守る助けにもなります。

Q3: VPN を使えば、オンラインで完全に匿名になれますか?

いいえ。VPN は IP アドレスを隠してトラフィックを暗号化しますが、ブラウザーのクッキー、ログイン中のアカウント（Google や Facebook など）、ブラウザーのフィンガープリント、あるいは VPN プロバイダーがデータを記録している場合には、追跡される可能性があります。

Q4: VPN はインターネット速度を遅くしますか?

はい、わずかにあります。暗号化の処理とVPNサーバーまでの物理的な距離により、遅延とオーバーヘッドが加わります。影響の大きさは、プロバイダー、プロトコル、サーバーまでの距離、端末、ネットワークの状況によって異なります。

Q5: VPN を使うことは合法ですか?

VPNの使用は多くの国で合法ですが、VPNサービスを制限、規制、またはブロックしている地域もあります。使用する前に、現在のローカルの法律を確認してください。詳しくは、VPN.comの合法性に関するガイドをご覧ください。

チェックポイント 10: VPN FAQ – 基礎（パート B）

仮想プライベートネットワークの利用について、見込み客からよくある質問と回答を確認しましょう。

Q6: 無料 VPN を使えますか?

無料 VPN は、広告、機能の制限、利用状況の分析、データ上限、その他の収益化モデルに頼っている場合があります。利用する前に、プロバイダーのプライバシーポリシー、所有者、監査、ビジネスモデルを確認してください。

Q7: 「ノーログ」ポリシーとは何ですか?

ノーログポリシーは、プロバイダーが保持しないとしている活動データや接続データを説明するものです。正確な範囲は異なるため、読者はポリシーと独立監査の結果を確認してください。

Q8: 最適な VPN を選ぶにはどうすればよいですか?

監査済みのノーログポリシー、強力なプロトコル（WireGuard、OpenVPN）、安全なサーバーの所在地、高速な通信、RAM のみのサーバー、キルスイッチ機能、そして（5/9/14 アイズのような）情報共有同盟の外にある管轄を探しましょう。

Q9: スマートフォンとスマートテレビで VPN を使えますか?

はい。最近のVPNプロバイダーは、iOS、Android、macOS、Windows、Linux、スマートテレビ向けの専用アプリのほか、家庭内ネットワークのすべての機器を保護するルーター設定も提供しています。

Q10: キルスイッチとは何ですか?

キルスイッチは、VPN接続が切れたときにデバイスを自動的にインターネットから切断するセキュリティ機能です。これにより、暗号化されていないデータや本当のIPアドレスの漏えいを防ぎます。

チェックポイント 10: VPN FAQ – 応用（パート C）

仮想プライベートネットワークと安全なトンネリングプロトコルの、技術面と構造面を探ります。

Q1: WireGuard、OpenVPN、IKEv2 の違いは何ですか?

WireGuardは、約4,000行のコードしかない最新の軽量プロトコルで、高速な通信と素早い接続時間を実現します。OpenVPNは、実績のある非常に安全なオープンソースプロトコルです。IKEv2は、ネットワークを切り替えたときに素早く再接続できるため、モバイルデバイスに最適です。 [4]

Q2: ダブル VPN またはマルチホップルーティングとは何ですか?

マルチホップは、トラフィックを 2 台以上の VPN サーバーに順番に経由させます。これにより暗号化の層がもう 1 つ加わり、一方のサーバーが侵害されても、2 番目のホップから本当の IP アドレスを隠しておくのに役立ちます。

Q3: WebRTC リークとは何で、VPN はそれをどう防ぎますか?

WebRTCは、VPNが有効でも、実際のローカルIPアドレスとパブリックIPアドレスを明らかにする可能性があるブラウザープロトコルです。プレミアムVPNは、デスクトップ/モバイルアプリやブラウザー拡張機能でWebRTCリクエストをブロックまたは偽装します。

Q4: RAM 専用サーバーとは何で、なぜ重要ですか?

従来型のサーバーはデータをハードドライブに書き込むため、押収されたり侵害されたりする可能性があります。RAMのみ(ディスクレス)のサーバーは、完全に揮発性メモリ(RAM)上で動作します。サーバーを再起動または電源オフにすると、メモリ内のデータは消去されます。

Q5: 難読化は VPN のブロックをどう回避しますか?

難読化（「ステルス VPN」とも呼ばれます）は、VPN トラフィックを通常の HTTPS トラフィック（ポート 443）に見せかけます。これにより、政府や学校・職場のネットワークが VPN をブロックするために使うディープパケットインスペクション（DPI）を回避しやすくなる場合があります。

チェックポイント 10: VPN FAQ – 応用 (パート D)

仮想プライベートネットワークと安全なトンネリングプロトコルの、技術面と構造面を探ります。

Q6: スプリットトンネリングとは何で、いつ使うべきですか?

スプリットトンネリングでは、どのアプリを暗号化された VPN トンネル経由にし、どのアプリを直接インターネットに接続するかを選べます。機密性の高い銀行アプリは VPN 経由にし、ローカルのゲームは直接接続して、VPN による遅延を避けるために使います。

Q7: 前方秘匿性(PFS)はどう機能しますか?

PFS は、セッションごとに一意の一時的な暗号鍵が生成されるようにします。将来、秘密鍵が漏えいしても、各セッションが独立した鍵を使っているため、過去や将来のセッションの復号には使えません。

Q8: 5/9/14 Eyes 同盟とは何で、なぜ気にする必要がありますか?

管轄はプロバイダーが直面しうる法的手続きに影響しますが、実際のプライバシーリスクは、プロバイダーが保持するデータ、技術的なアーキテクチャ、所有者、透明性レポート、監査履歴にも左右されます。

Q9: DNS リーク保護とは何ですか?

DNSリーク防止は、ウェブサイトの検索クエリ(DNSクエリ)を、ISPのサーバーではなくVPNのプライベートで暗号化されたDNSサーバー経由で送信させます。これにより、ISPがあなたの訪問先サイトを追跡するのを防ぎます。

Q10: VPN は ISP によるインターネットの速度制限を回避できますか?

場合によります。ISP が特定の通信だけを選んで遅くしている場合は VPN が役立つことがありますが、混雑、データ容量の上限、アカウント単位の速度制限、ネットワーク品質の低さを克服することはできません。

技術参考資料と出典

このワークシート全体で使われている、引用された出版物、暗号仕様、公式文書の標準。

学術・業界の参考資料

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637