# Trey Research Corporation

仮想プライベート ネットワーク: Fabrikam, Inc. の技術的な概要

**2023 年 12 月 18 日**

**仮想プライベート ネットワーク (VPN)**  は、ネットワーク トラフィックの暗号化に役立つ一般的なネットワーク セキュリティ ソリューションです。[VPN はセキュリティで保護されたトンネルとして機能し、インターネット トラフィックを暗号化するため、サード パーティがアクティビティを追跡したりデータを盗んだりすることは困難です](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)。

## VPN の実装の長所:

* VPN は、インターネット トラフィックを暗号化することで、プライバシーとセキュリティのレイヤーを提供します。これにより、サード パーティがアクティビティを追跡し、データを盗むのが困難になります。
* VPN は、空港またはライブラリでパブリック Wi-Fi を使用しているときにハッキングされないようにするのに役立ちます。これは、VPN がセキュリティで保護されたトンネルとして機能し、インターネット トラフィックを暗号化するためです。
* [VPN を使用すると、インターネット サービス プロバイダーは、コンピューターとの間で送受信されるすべてのトラフィックが VPN のサーバーを経由するため、または VPN が](https://www.bing.com/aclk?ld=e83gkJ29qbmUu8cYkNgVfaCjVUCUx3vCyorXNIwmWui8A8rISGT4ATMfXuQu_8nGJifMsVNZrD0_vVyNtSvYRynbmDYfM2jUvwoREzv_CIrOKnWn2gIEyYOWegOAxJPNIFOUp5hBSGQU35pxcSs4Qxqzw59vf63cS8Oh_e_94A9QZD8MND&u=aHR0cHMlM2ElMmYlMmZ3d3cudnBubWVudG9yLmNvbSUyZmluLXVzYS1iZXN0LXZwbiUzZmtleXdvcmQlM2R2cG4lMjUyMHJhbmtpbmclMjZnZW8lM2QxMTA3MzUlMjZkZXZpY2UlM2QlMjZ1dG1fc291cmNlJTNkYmluZyUyNmFkaWQlM2Q3NjIxMDA1Nzk0MzY4MCUyNm1zY2xraWQlM2Q3NTEzMDFiNzM2MTQxZTY2ZTBiZDY0MTA0MzJlYjBkYw&rlid=751301b736141e66e0bd6410432eb0dc) [1](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/) を使用するために支払うサーバーを経由するため、アクセスしたサイトを把握できないようにすることができます。
* [VPN は、IP アドレスをマスクしてインターネット接続を暗号化することで、コンテンツ 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/) の地理的制限をバイパスできます。VPN サーバーに接続すると、インターネット トラフィックが VPN サーバー経由でルーティングされ、新しい IP アドレスが割り当てられます。[これにより、別の場所からインターネットにアクセスしているかのように表示され、コンテンツの地理的制限をバイパスできます](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## VPN の実装の短所:

* 接続速度は ISP よりも遅くなる可能性があります。[これは、VPN によって、インターネット トラフィックに対する暗号化とルーティングのレイヤーが追加されるため2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)。
* VPN の使用は、一部の独裁国では禁止されています。[一部の国では、VPN は禁止されているか、](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)[2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)厳しく規制されています。
* 無料の VPN を使用すると、広告、マルウェア、漏洩のリスクがあります。[無料VPNは、第三者の広告主にユーザーデータを販売したり、](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)[2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)ウェブサイトに広告を挿入したりする場合があります。

## インストールの詳細:

* [VPN は、VPN クライアントを実行しているシステムと VPN サーバーの間に暗号化されたトンネルを確立し、その後、トンネルを経由してエンタープライズ ネットワークの残りの部分にトラフィックをプロキシ](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/)。手順を次に示します。
  1. VPN クライアントがユーザーのデバイスにインストールされ、デバイスと VPN サーバー間のすべてのトラフィックが暗号化されます。
  2. VPN サーバーはトラフィックを復号化し、目的の宛先に転送します。
  3. 宛先サーバーは、VPN サーバーにトラフィックを送信して要求に応答します。
  4. VPN サーバーはトラフィックを暗号化し、VPN クライアントに送り返します。
  5. [VPN クライアントはトラフィックを復号化し、ユーザーのデバイス](https://www.bing.com/aclk?ld=e8OcZUYHFbvxJgBgmEWpxgCzVUCUz-UOb13n9w7mOCOGgLkPnDhd3Uh-ipDjPE6Hpo4QBuX2o2EUlY6g5-dRpoq53O3haHMQ8RcFRpVU95xD1yO9RVjEOu3gsgBNFb6xmA-Gvbq-gT8RFWo2P6R0BeJBd5LyAIvbSKlU_DPbqAqdr2ubUB&u=aHR0cHMlM2ElMmYlMmZ3d3cub3BlcmEuY29tJTJmZmVhdHVyZXMlMmZmcmVlLXZwbiUzZnV0bV9zb3VyY2UlM2RiaW5nJTI2dXRtX21lZGl1bSUzZHBhJTI2dXRtX2NhbXBhaWduJTNkVVMlMjUyMC0lMjUyMFBlcmZvcm1hbmNlJTI1MjBNYXglMjUyMC0lMjUyMEVOJTI2dXRtX2NvbnRlbnQlM2QlN2Jhc3NldEdyb3VwSWQlN2QlMjZtc2Nsa2lkJTNkZDVhYzJiMDEzNDM2MWVkNDRmNGE0ZWE2NDA1MDk5MjIlMjZ1dG1fdGVybSUzZHd3dy5vcGVyYS5jb20&rlid=d5ac2b0134361ed44f4a4ea640509922) [1](https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html)に送信します。
* AKS Backup をインストールおよび構成するには、次の手順に従います。
  1. お使いのコンピューターに JSON ファイル を作成します。
  2. [スタート] をクリックし、[設定] をクリックして設定メニューを開きます。
  3. [設定] メニューで、[ネットワークとインターネット] をクリックして VPN をクリックします。
  4. [VPN 接続を追加する] を選択します。
  5. VPN 接続ウィンドウを追加すると、いくつかのタスクを実行できます。
  6. 変更を保存します。

## リスク軽減策

* 攻撃者は、以前からリモート作業を脅威ベクトルとして認識してきました。リモート作業環境は、いくつかの理由で攻撃者にとって特に魅力的です。まず、ホーム ネットワーク環境は専門的に管理されていません。最も重要なことは、ホーム ネットワーク上のより多くのシステムが定期的に修正プログラムを適用されておらず、その多くが脆弱性の軽減に関して古くなっていることを意味します。エンタープライズ ネットワーク上で永続化するには、システムを悪用した攻撃者が検出を回避し、修復に抵抗する必要があります。ここでも、ホーム ネットワークは攻撃者にとってよりフレンドリです。通常、脅威の検出はほとんど存在しません。また、PC の再インストール時や実行時間が遅いためにインベントリから削除された場合など、付随的な修復が行われます。リモート作業環境をセキュリティで保護するには、ゼロトラストの前提条件をさらに拡張することが不可欠です。[単に敵対的であると見なすべきネットワークではなく、企業の管理下にないすべてのものが](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/)。
* [最新のソフトウェア パッチとセキュリティ構成を使用して、作業環境へのリモート接続に使用されている VPN、ネットワーク インフラストラクチャ デバイス、デバイスを更新](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons) [6](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a)。

## 実装のベスト プラクティス

企業ネットワークに VPN を実装するためのベスト プラクティスは次のとおりです。

* [カスタム コードを使用して TLS](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/) 経由でトラフィックを送信する Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPN よりも一般的にリスクが低く、セキュリティが強化された、インターネット キー Exchange/インターネット プロトコル セキュリティ (IKE/IPSec) など、受け入れられている標準を使用する標準ベースの VPN を選択します。
* 強力な暗号化で VPN を使用します。VPN で使用される暗号化アルゴリズム、認証アルゴリズム、プロトコルが強力で FIP 検証されていることを検証します。[可能な場合は、多要素認証 (MFA) を使用するようにすべての VPN を構成し、パスワードベースの認証をデジタル証明書 (スマートカードに格納) によるクライアント認証に置き換えます](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)。
* ソフトウェアの脆弱性を管理します。VPN の脆弱性の悪用は、サイバー犯罪者の一般的な攻撃ベクトルです。脆弱性修正プログラムの適用に関する強力な実績を持つ VPN ベンダーを選択し、ソフトウェアの部品表 (SBOM) を要求して、サードパーティのコードが最新で安全であることを検証します。また、潜在的な侵入を検出するために、実行中にコードの検証を実行できる製品を探します。[VPN を展開したら、定期的にソフトウェア更新プログラムを確認し、](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)を適用します。
* 使用するサージに備える。[IT セキュリティ担当者は、大量の使用](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/) [2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)に備えて VPN の制限をテストする必要があります。
* 無料の VPN は使用しないでください。[無料の VPN を使用すると、広告、マルウェア、漏洩のリスク 3](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/)。