

# リモートワーク中の社員を守る8つの鍵



最新のリモートチームは、オンラインでつながって仕事をやり遂げられる人たちが様々な形で集まって、成り立っています。つまり、正社員、契約社員、フリーランス、ベンダー、パートナーなどの様々なユーザーたちが同じツールを使って一緒に働くということです。企業データがホストされている場所がどこであっても、遅延なく保護するために何をしていますか？遅延することなく、最新のリモートチームを保護するための8つのベストプラクティスをご紹介します。



## 1. 内部管理されたアプリケーションへのアクセス保護

ビジネスの内部アプリケーションを保護するために、従来のVPNを使用しているかもしれませんが、社員が大規模に遠距離から接続するため、そのモデルでは崩壊しかねません。さらにVPNは非常にpermissive（寛容）なので、玄関先から入ってくるものを全て信頼してしまうという悪い面があります。

最新のソリューションは、ゼロトラスト(信頼せずに必ず確認する)モデルを採用しています。つまり、VPNのフラストレーションやパフォーマンス低下を引き起こさずにデジタル的にデータのパケット全てに問い合わせを行います。



## 2. インターネット上の脅威からチームを保護する

SaaSアプリケーションの様々な組み合わせを活用している場合、チームは潜在的にインターネットの未開の地に晒される可能性があるということです。歴史的に見ると、企業は、脅威のスキャンニングのためにアウトバウンドインターネットをルーティングしてリクエストをHQに戻してきましたが、スピードが遅く、規模によっては防御できません。

チームの仕事を停止させることなく、最新の脅威を特定し、阻止する方法が必要です。



## 3. どこにいても、企業データを保護する

ビジネス上最も価値のあるデータがSaaSベンダー、内部アプリケーション、パブリッククラウドなど様々なところにある場合があります。このデータがオンプレミスとクラウドベースのサービスの組み合わせをサポートするようにデザインされた保護を必要とするところだけに、このデータが送信されるようにします。

# リモートワーク中の社員を守る8つの鍵



## 4.だれもが理解できるツールを活用する

チームにとって、セキュリティに対する取り組みが頭痛のタネである場合、ITスタッフは重荷に感じます。従業員は内部ツールの使用を諦めてしまうかもしれません(さらに悪いケースは回避策を講じることです)。

それなら、すでにチームが使っているGoogleまたはOktaログインなど、チームにとっておなじみのシステムを使ってもいいではありませんか？



## 5.契約社員を迅速に追跡する

今の時代、人員は流動的です。契約社員やその他の外部パートナーがあなたのチームと協力して働く場合、仕事初日から必要なものを全て揃えておくことは重要だと言えます。—しかし、それ以上であってははいけません。一度、仕事が完了したら、彼らに与えられていた権限が取り消されていると確信できることが必要です。

最新の認証ソリューションが、契約社員がすでに使っている可能性が高い広く利用可能無料サービスを含めて様々なIDプロバイダーとシームレスに連携します。



## 6.ツールを見つけやすくする

優秀なリモートチームが、従業員が必要な時に必要なツールを見つけやすくしてくれます。アプリlaunchpadは、ユーザーがアクセスできるアプリケーション全てを一つの簡単でグラフィックなダッシュボードにすることで、溢れかえるツールの海で助けてくれる救命ボードになるようにデザインされています。

他のlaunchpadよりも優れているものがあります。あなたのlaunchpadが、きめ細かい権限をサポートしているか、従業員がアクセスする必要のあるツールだけを表示しているかを確認してください。



## 7.古い問題に新しいソリューションを検討する

レガシーアプリケーションで身動きが取れなかったなら、これが数多くある完成度の高いSaaSソリューションの一つを考えるいいチャンスかもしれません。保護するために適切なツールがある場合、SaaSアプリは高度な機能性、継続的な更新、多くの企業が一括の前払いよりも長期にわたって処理が楽になるサブスクリプションモデルを提供します。



## 8.何かがダウンする前に注意喚起

オフィスのダッシュボードが真っ暗になることがあります。それはあなたのインサイトが必要とされているということではありません。Security Information and Event Management (SIEM) プラットフォームにエクスポートする柔軟性を備え、広範囲なロギングと全てのリクエストの監査をサポートするソリューションを使っているか、確認してください。

安全なアンロックと高速リモートワークを  
今すぐあなたのチームに [@ teams.cloudflare.com](https://teams.cloudflare.com)