HITACHI
Inspire the Next

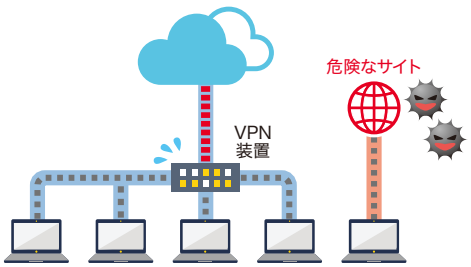
HIBUN

快適で安全なテレワーク環境を実現できていますか？

働き方改革の一環として以前から
導入を進めていた企業も多い「テレワーク」。
最近では、パンデミック対策としてテレワークへの
意識の高まりと取り組みがより一層進みました。
しかし、業務効率やセキュリティまでを考慮せず
テレワークを導入している企業も
多いのではないでしょうか…。

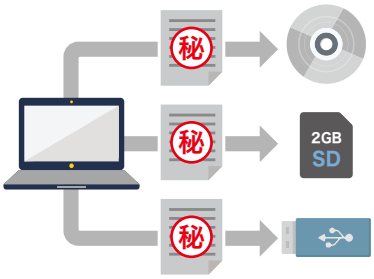
テレワークを導入する際の、さまざまな課題

VPNへのアクセス集中による業務効率低下



VPNへのアクセスが集中すると、クラウドサービスの画面が固まるなど業務に支障をきたします。
また、それを回避しようとVPNを利用しないでいると、危険なサイトにアクセスしてしまい、マルウェアに感染したり、不正に情報をアップロードして情報が漏洩するリスクが高まります。

内部不正による情報漏洩



テレワークでは抑止する人の目がないため不正が起きやすい環境と言えます。
そのため、私物デバイスなどに不正にデータをコピーし、情報が漏洩するリスクがあります。

PCの脆弱性を突いたサイバー攻撃

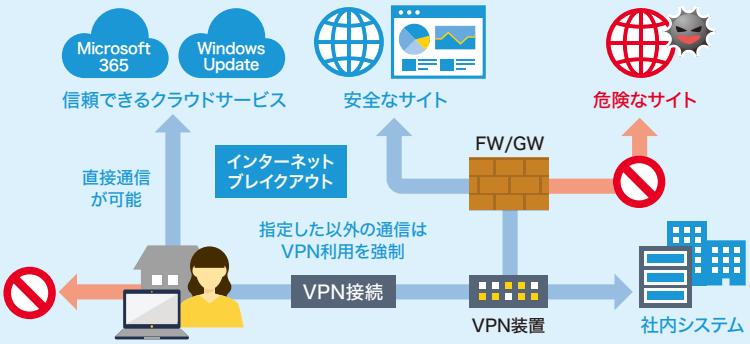
社内ネットワークに接続していないPCを管理できず、セキュリティ対策をユーザー任せにしていると、最新のセキュリティポリシーを適用せずに脆弱性のあるままPCを利用してしまうなど、サイバー攻撃に遭う可能性があります。

株式会社 日立ソリューションズ

秘文は安全にテレワークを行うための セキュリティ機能を提供します。

インターネットブレイクアウトで 業務効率化とセキュリティ強化を両立

インターネットブレイクアウトにより、信頼できるクラウドサービスには直接接続させることで、VPNへのアクセス集中を回避します。またそれ以外の通信は、VPNの利用を強制させ社内と同等のセキュリティでインターネットを利用でき、危険なサイトからのマルウェア感染や、情報の不正アップロードといったリスクを低減できます。さらに、VPN利用だけではなく、リモートアクセスツールへの強制も同様に可能です。

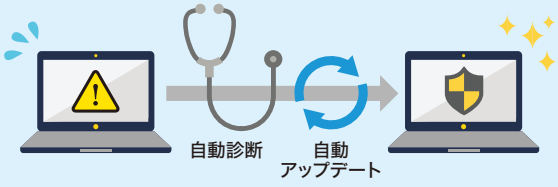


操作ログの取得とデバイス制御で 内部不正を防止

サーバーがクラウド上にあるので、社内に接続していないクライアントPCの操作ログも取得でき、内部不正を抑止できます。またデバイス制御により、私物デバイスなどへの情報の不正コピーを防止します。

自動脆弱性診断と自動アップデートで サイバー攻撃対策

社内ネットワークだけでなく、外出先や自宅など利用環境を問わずクライアントPCを一元管理できます。日々変わるセキュリティ脅威に対し、サイバー攻撃で狙われやすい脆弱性を自動で診断し、必要なセキュリティパッチが適用されていない場合は、自動アップデートさせることも可能です。



秘文パッチの自動配信で 常に最新のセキュリティを適用

秘文のパッチが新たにリリースされた場合に、秘文パッチをクライアントPCへ自動的に配信します。またクライアントPCのセキュリティ情報をクラウドで収集し可視化することで、セキュアな運用の徹底を支援します。

HIBUN

秘文 統合エンドポイント管理サービス

秘文 統合エンドポイント管理サービスは、利用環境を問わず自動脆弱性診断などによりエンドポイントのセキュリティを管理し、脅威から守ります。また、デバイスの利用や接続先ネットワークの制御、暗号化などによって情報漏洩を防止可能です。
さらに、クラウドでサーバーの機能を提供するため、手軽かつ低コストに導入できます。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/hibun/sp/

S16S-21-03 | 2021.03