

安全なテレワーク導入をご支援します by STNet

新型コロナウイルスへのリスク対策として様々な企業でテレワークが導入されました。その多くは、出張・外出制限に対応するお試しプランです。働く人たちの感染リスクは回避できたとしても、そこには新たなリスクが存在します。テレワークを緊急対応に留めず、さらなる効率的な働き方に変えていくため、やるべきことや様々なツールをご提案いたします。

勤怠管理システム等



労務環境とセキュリティ対策の整備

● 労務管理ソフトの導入

資産、勤怠、名刺、文書等の管理、承認フローなど事業運営には欠かせないルーティーン。効率的な労務管理に加えて、テレワーク状況を可視化することができます。

★ 労務管理ソリューションなど



● コミュニケーションの改善

WEB会議やチャットなどのツールの活用が拡大しています。自社の業務に合った使いやすくコストパフォーマンスの良いものを全社運用し、コミュニケーションの改善と生産性の向上を図りましょう。

★ WEBコミュニケーションツール



● セキュリティ対策

クラウドや外部とのデータ連携が増えてくるはず。その時に個人情報漏洩など事業にとって大きなリスクが。安心して利用するために自社の課題に合ったセキュリティ対策が必要です。

★ 現状の可視化

セキュリティ診断

★ 入口・出口対策



★ 内部対策



ネットワーク環境の充実化

セキュアで高品質なネットワーク



● 安全なリモート接続環境

サテライトオフィスや自宅から社内サーバーにアクセスする場面が増えます。なりすましによる情報漏洩を回避するための仕組みが必要です。

★ プライベートネットワーク (VPN) 構築およびリモートデスクトップソリューション



★ MDM (モバイルデバイス管理)



● 社内ネットワークの高度化

テレワークでよくあるのが、皆が社内サーバーにアクセスして繋がらないこと。セキュアでストレスフリーなネットワークに充実させましょう。

★ 帯域確保型企業向けインターネット



★ 高品質の拠点間閉域ネットワーク



★ 格安スマホ



★ 個人向けインターネット等



万一の自社システム部門閉鎖時のリスク対応

感染に伴い作業不可

● 監視・運用業務のアウトソース

自社の情報システム部門スタッフが感染症を発症すれば、そのオペレーションセンターを閉鎖しなければなりません。このような事態になれば、日々の運用業務に支障をきたすだけでなく、サーバー等の障害時に機器メーカー等が駆け付け復旧対応することもできないため、サーバー等を安心・安全な場所に預けて、運用保守を含めてアウトソースすることが有効です。これは、自然災害に備えたBCP対策の強化にも繋がります。

★ 専門スタッフによる運用保守代行、障害時のサポート



★ セキュリティ運用監視サービス

