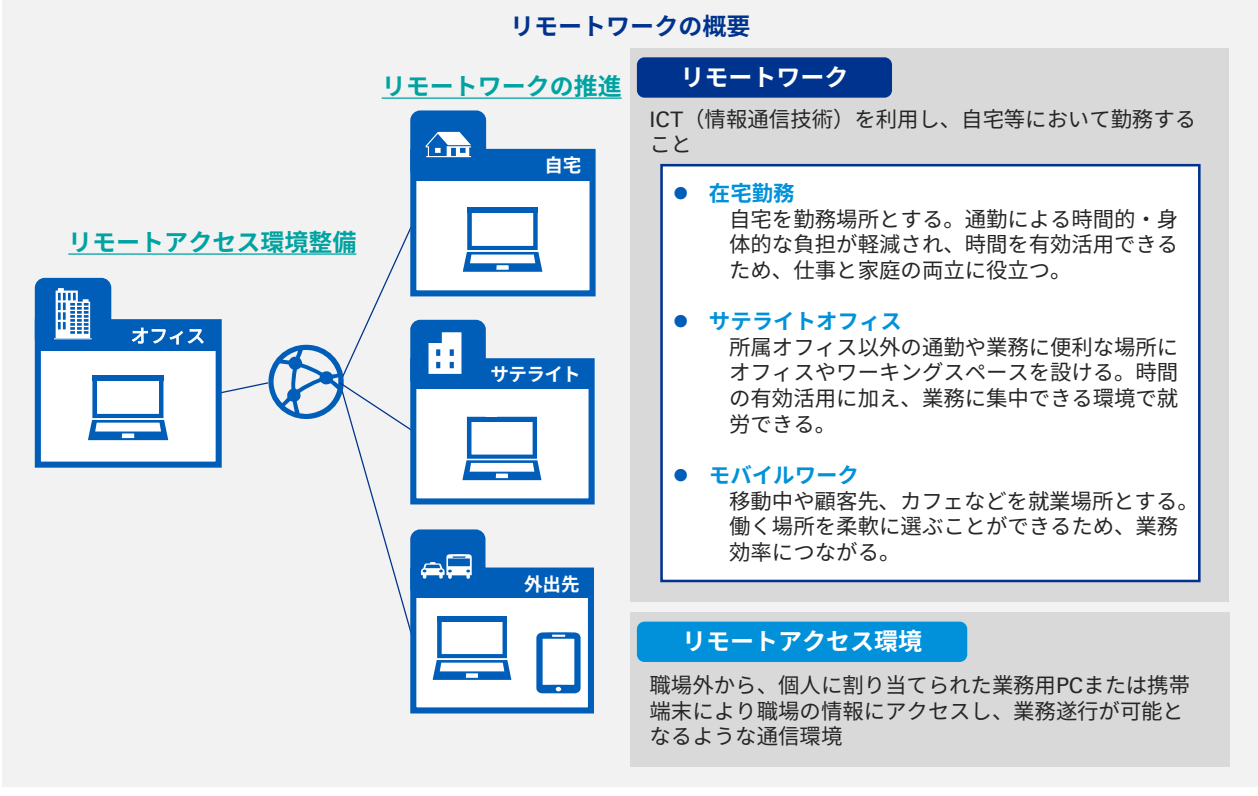
リモートワーク導入におけるセキュリティ対策

新型コロナウイルス感染症（COVID-19）拡大防止のための施策として、リモートワークを導入する企業が増加していますが、保護された社内ネットワークの外側から社内の業務情報へアクセスすることになるため、これまで企業が導入していたセキュリティ対策とは異なる施策が求められます。リモートワークにおけるセキュリティを検討する際には、各社の導入状況に応じて適切な施策が必要です。KPMGは、各企業のリモートワーク導入に不可欠なセキュリティ対策を支援します。

リモートワークの概要と現状

従前より、多様な働き方を実現する制度の一つとして推奨されてきたリモートワークの導入は、オフィスだけでなく、自宅・サテライトオフィス・外出先で勤務が可能となり、多様な働き方を実現できます。例えば、子育て中の人や介護をしている人でも離職することなく働き続けることができるため、企業では、社員にとっての働きやすさの提供を目的として、リモートワークの導入を検討してきました。



昨今のCOVID-19の感染防止のために、全社員を在宅勤務とする企業が増えており、そのためのシステム・労務環境整備を短期間で進めています。

しかし、在宅勤務はCOVID-19対策のための暫定的な対処ではなく、収束後も継続して利用され続ける可能性が考えられます。「ニューノーマル」と呼ばれるように、企業が導入した在宅勤務環境を中心にサテライトオフィスやモバイルワークも含めた各種リモートワークをもとにして、事業と組織の再構築が進むことが予想されます。そのため、今後も継続することを前提に、在宅勤務環境を整備することが重要です。

リモートワークにおけるセキュリティリスクと対策の進め方

リモートワークは働き方改革を目的として検討されてきましたが、これまでは広く活用されている状況とは言えませんでした。リモートワークによる情報漏洩リスクが懸念され、導入に踏み切れなかった企業が多かったと考えられます。

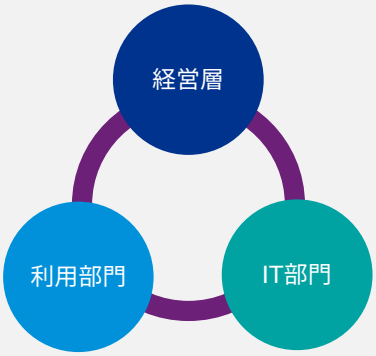
COVID-19対策としてリモートワークを導入した企業においても、セキュリティの不安を持ちつつ導入を始めた企業が存在します。当該企業ではセキュリティ対策の必要性を理解しているものの、事業継続のために在宅勤務を急遽実施することとなったため、網羅的なセキュリティ対策が実施される前にリモートワークに踏み切っています。

リモートワークに関するセキュリティ対策が不十分な場合には、改めて検討することが必要です。その際は、リモートワークのビジョン・目標を明確にしたうえで、勤務制度の整備は組織風土を変革しながら、**ガバナンス・システム**の両面における各種施策を導入することが不可欠です。

■ セキュリティガバナンス構築

リモートワークにおけるセキュリティを確保するためには、脅威と対策を洗い出し、現状とのギャップを踏まえてガイドラインやルールを策定することが必要となります。ルール策定においては、リモートワークの運用に係る諸問題に対して、組織的な対応が重要なため、IT部門だけでなく、経営層・IT部門・利用部門が三位一体となった体制・仕組みを構築することが求められます。

経営層・IT部門・利用部門が三位一体となった体制・仕組みの構築



- ◆ リモートワークに係る情報セキュリティポリシー・ガイドラインの策定
- ◆ リモートワークに係る定期的な教育・啓蒙活動
- ◆ 事故発生を想定した連絡体制の整備・訓練
- ◆ 必要人材・資源・予算の割り当て
- ◆ リモートワーク運用に係るモニタリング・見直し指示

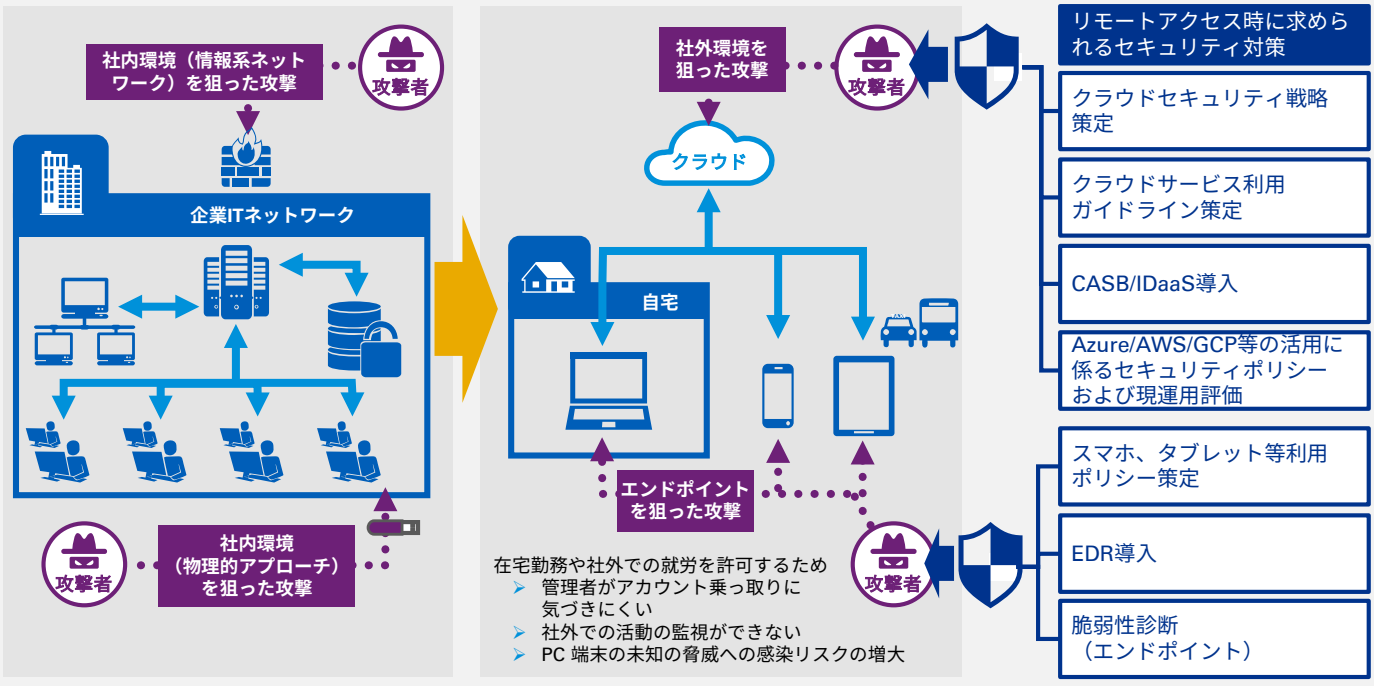
- ◆ リモートワークセキュリティにおけるシステム対策の実施（マルウェア、端末の紛失・盗難、重要情報の盗聴等）
- ◆ システム運用ルールの整備
- ◆ 外部サービスの利用に対する運用ルール等の整備
- ◆ リモートワーク運用に係る連絡体制の整備・報告

- ◆ リモートワークに係る情報セキュリティポリシーの遵守
- ◆ リモートワークに係るシステム運用ルールの遵守
- ◆ リモートワーク運用の定期的な自己点検の実施
- ◆ リモートワーク運用に係る連絡体制の整備・報告

■ テクノロジー領域に係るセキュリティ対策

リモートワーク環境においては、ネットワークやデバイスが企業の統制外に置かれるため、企業ITネットワークで担保されていたセキュリティが保証されません。安全なリモートワーク環境を実現するためには、既存のセキュリティ対策だけでなく、リモートアクセスを前提とした新たな施策が重要となります。

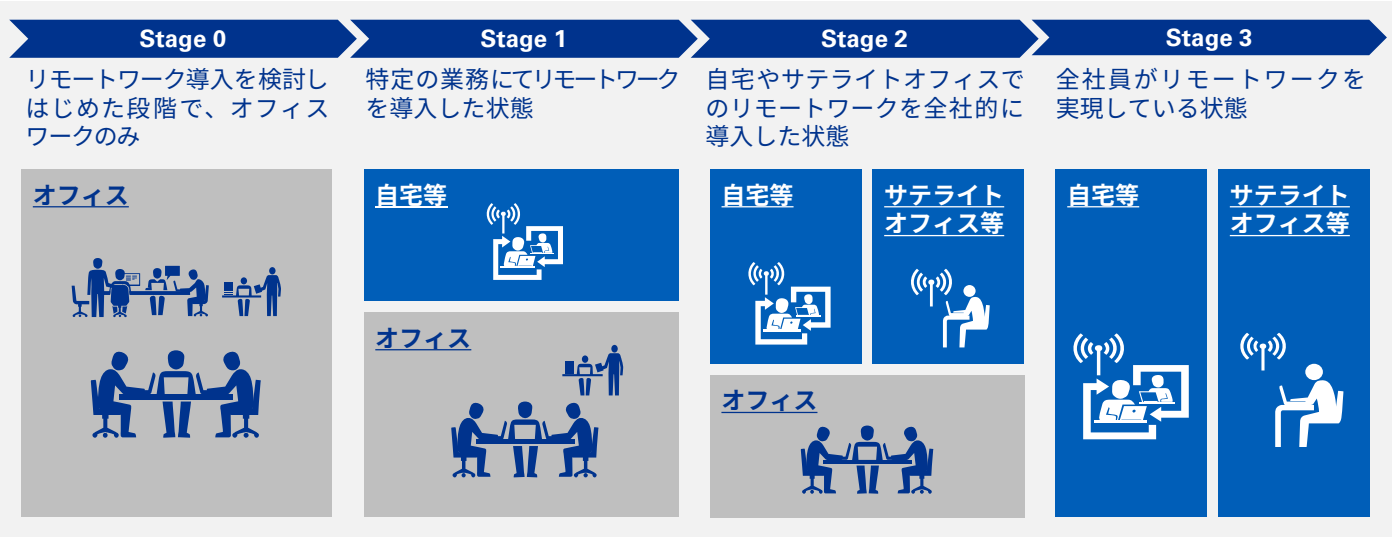
リモートワーク環境において想定される攻撃とセキュリティ対策の例



リモートワーク活用の段階と検討項目

■ リモートワーク活用における4つの段階

リモートワーク導入を検討しはじめるStage 0を経て、次のStage 1では特定業務において在宅勤務が導入され、部分的なリモートワークが開始されます。Stage 2になると、リモートワークの対象業務が広がるとともに勤務場所も広がります。例えば、自宅だけでなく、サテライトオフィス等での勤務も認められるようになります。最終段階であるStage 3においては、全社員がオフィス以外でも業務を遂行できる環境となります。



■ リモートワーク活用の各段階における検討項目

リモートワーク開始を検討するStage 0では、リモートアクセスを実現するための端末準備を検討します。端末としては、業務用ノートPCの支給だけでなくBYOD（Bring Your Own Device：私有デバイスの業務活用）の可否も検討します。

リモートワークが導入されたStage 1では、社外にて機密情報を扱うことになるため、端末におけるセキュリティのさらなる強化が検討ポイントとなります。

Stage 2では、リモートワークを効率的に実施するためにクラウド等の社外ネットワークの整備が検討課題となります。

Stage 3では、全社員が同時にリモートワークを実施することでVPN等の社内ネットワーク設備がひっ迫するため、最適となる社内ネットワークを検討することが求められます。

	検討項目	対処ポイント
Stage 0	モバイルデバイスとして、BYODの利用を許可すべきか検討する	モバイルデバイス
	デスクトップPCからノートPCに移行した際のセキュリティリスクを評価し、対策をとる	モバイルデバイス
	リモートアクセスを許可する際に、社内ネットワークに対して実施すべきセキュリティ対策を検討する	社内ネットワーク
Stage 1	持ち出しPCの盗難・紛失が発生した際にデータ漏洩を防止する仕組みを導入する	モバイルデバイス
	持ち出しPCのプライベート利用を制限する	モバイルデバイス
	会社が許可していない外部サービスへアクセスすることを制限する（LINE等の業務利用を制限する）	社外ネットワーク
Stage 2	リモートワーク推進の上で利用しているクラウドでのセキュリティ対策を評価し、必要な対策を追加する	社外ネットワーク
	各種システムにアクセスする際、アクセス対象に応じて多要素認証を実施する	社外ネットワーク 社内ネットワーク
Stage 3	全社員が一斉にVPN等を利用するため、ネットワークや各種デバイスを増強する	社内ネットワーク
	委託先会社の社員も社外からアクセスするため、ユーザに応じて各種システムへのアクセス権限を変更する	社内ネットワーク
	社外アクセスに関するログが通常より大量に出力されるため、通常とは異なるセキュリティ監視体制を構築する	社内ネットワーク

KPMGによるリモートワークセキュリティ対策支援

■ セキュリティガバナンス構築支援

リモートワークセキュリティ戦略策定支援

リモートワークセキュリティは、自社の業務環境と今後のIT・デジタル戦略およびリモートワーク計画を十分に考慮し、適切なゴールを設定することが重要です。システムおよびガバナンスの観点から企業のリモートワークセキュリティにおける目指す姿の定義および実現プランの策定を支援します。

リモートワークセキュリティ管理体制整備支援

リモートワーク実施時のセキュリティに係る脅威およびリスク、それらに対するコントロールについて、公的ガイドラインを参考に既存の状況を評価し、不足している統制を整理します。その後、リモートワークセキュリティに係る規程類や体制の整備・見直し、執行までを支援します。

■ テクノロジー領域に係るセキュリティ対策支援

リモートワークの活用を進めるために検討すべき「モバイルデバイス」「社外ネットワーク」「社内ネットワーク」の3つのテクノロジー領域について、KPMGが包括的に支援します。

	検討項目	支援内容
モバイルデバイス 	BYODの利用許可判断	リモートワークセキュリティガイドライン整備支援
	プライベート利用の制限	リモートワークセキュリティガイドライン整備支援
	持ち出しPCのセキュリティ対策	脆弱性診断（エンドポイント）
	端末からの情報漏えい対策	DLP導入支援
社外ネットワーク 	許可されていないクラウドの利用制限	CASB導入支援
		クラウドセキュリティソリューションの評価支援
	利用するクラウドのセキュリティ強化	クラウドセキュリティアーキテクチャ設計支援
	本人認証の厳密化	ID管理構想策定支援
		特権ID管理構想策定支援
社内ネットワーク 	不正侵入への対策	多層防御最適化支援
	社外からのアクセス制御（委託先を含む）	ID管理構想策定支援
		特権ID管理構想策定支援
	ネットワークの増強	リモートアクセスにおけるネットワーク最適化支援
	セキュリティ監視・運用の強化	エンドポイント監視体制構築支援

KPMGコンサルティング株式会社

T：03-3548-5111
E：kc@jp.kpmg.com

home.kpmg/jp/kc