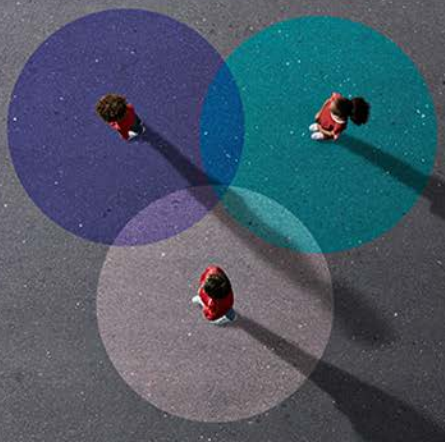
テレワーク導入における セキュリティ対策

2020年4月



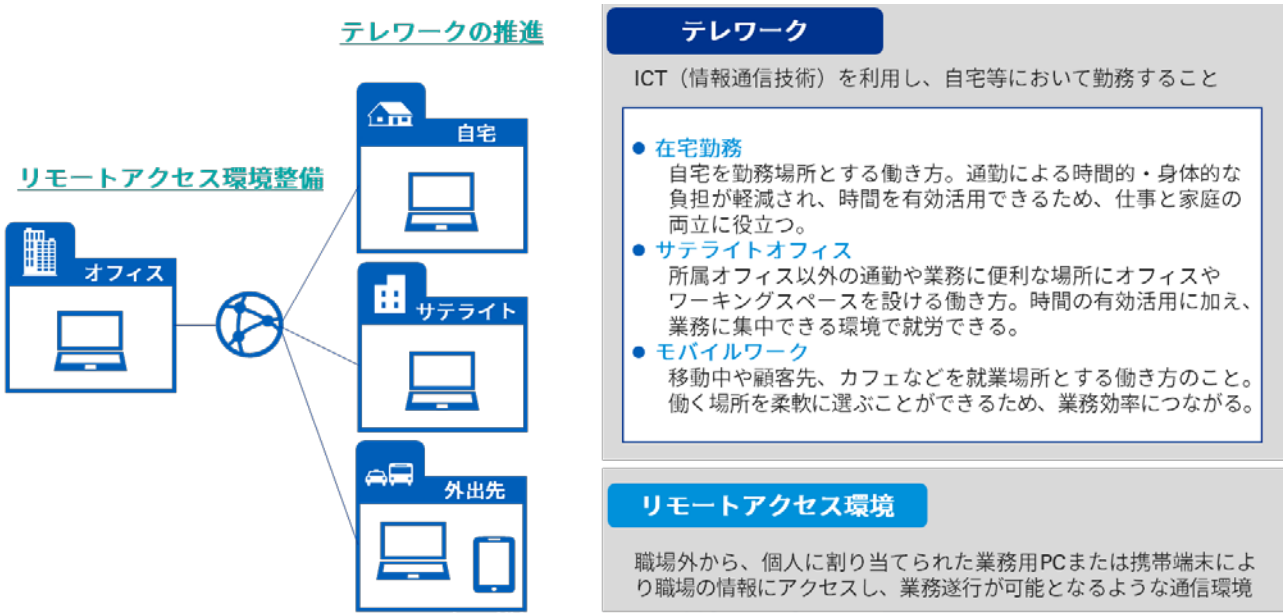
新型コロナウイルス感染症（以下、COVID-19）拡大防止のための施策として、テレワークを導入する企業が増加しています。テレワーク導入においては、保護された社内ネットワーク外から社内の業務情報へアクセスすることになるため、これまで企業が導入していたセキュリティ対策とは異なる対応が求められるようになります。テレワークにおけるセキュリティを検討する際には、各社のテレワークの導入状況に応じた適切な施策を実施する必要があります。

本稿では、各企業において導入が急速に進んでいるテレワークに関して、その現状とセキュリティリスク、および求められる対策について解説します。

テレワーク導入の現状

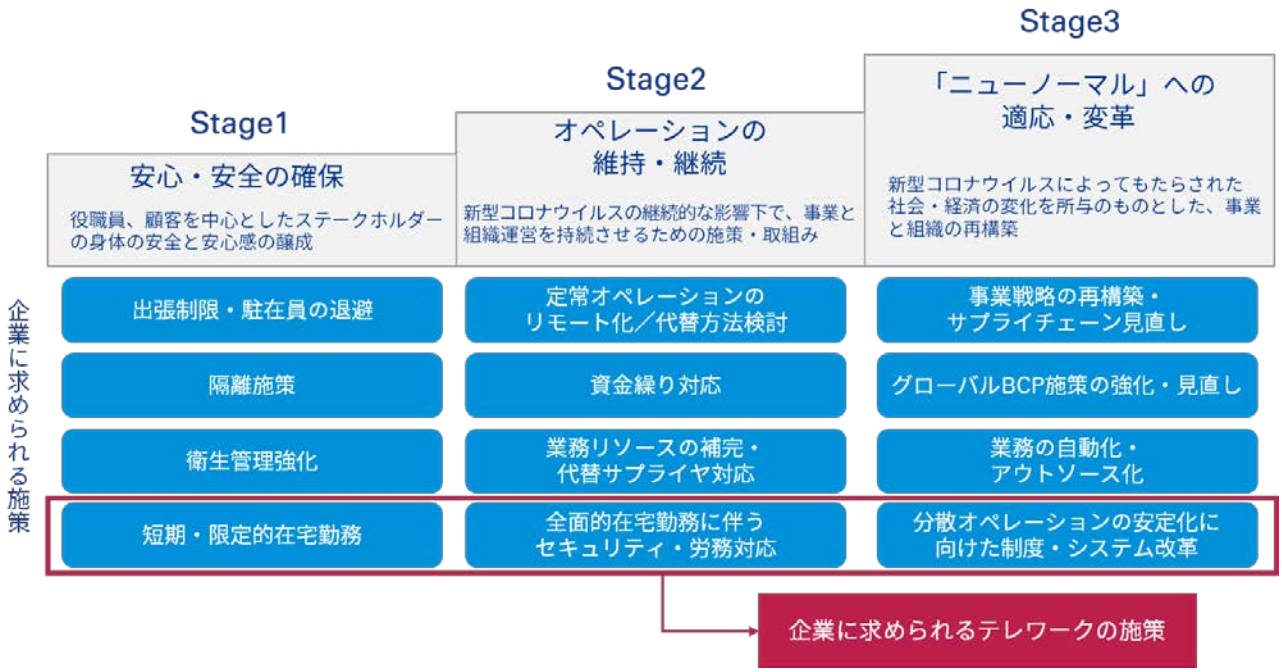
テレワークの導入は、従前より、多様な働き方を実現する制度の1つとして推奨されてきました。テレワークの導入により、オフィスだけでなく、自宅・サテライトオフィス・外出先からの勤務が可能となり、多様な働き方が実現されます。例えば、子育て中の人や介護をしている人でも離職することなく働き続けることができるようになります。そのため、企業では、社員にとっての働きやすさの提供を目的として、テレワークの導入を検討してきました。

【図1】テレワークの概要



しかし今、企業は、COVID-19の拡大防止を目的として、テレワークの導入を求められています。オフィスワークや限定的な在宅勤務導入ではなく、全社員が在宅勤務へと勤務形態を移行することが要求されています。そのため、多くの企業が、在宅勤務を実現するためのシステム・労務環境整備を短期間で進めています。

【図2】COVID-19対応の3つのステージ



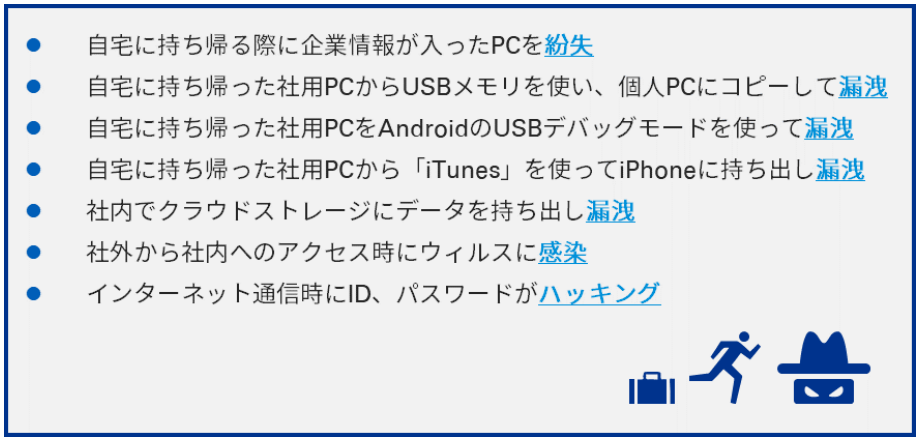
導入された在宅勤務はCOVID-19対策のための暫定的な対処ではなく、COVID-19がピークアウトしても、今後も利用され続けると考えられます。「ニューノーマル」と呼ばれるように、すでに実現された在宅勤務環境をもとにして、事業と組織の再構築が進むことが予想されます。そのため、今後も継続することを前提とした、在宅勤務の実施が必要と思われます。

テレワークにおけるセキュリティリスクと対策の進め方

テレワークは、働き方改革を目的として検討されてきましたが、これまではテレワークが広く活用されている状況とは言えませんでした。導入が広がらなかった理由の1つにセキュリティへの不安が挙げられます。例えば、図3に示したようなリスクが存在したため、テレワーク導入に踏み切れなかった企業もあったのではないでしょうか。

同様に、COVID-19への対策の際にも、セキュリティの不安が解消されずに導入を始めた企業もあるかと思います。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、すべてのセキュリティ対策が取られる前にテレワークに踏み切ったと予想されます。

【図3】テレワーク導入において企業が想定しているリスク



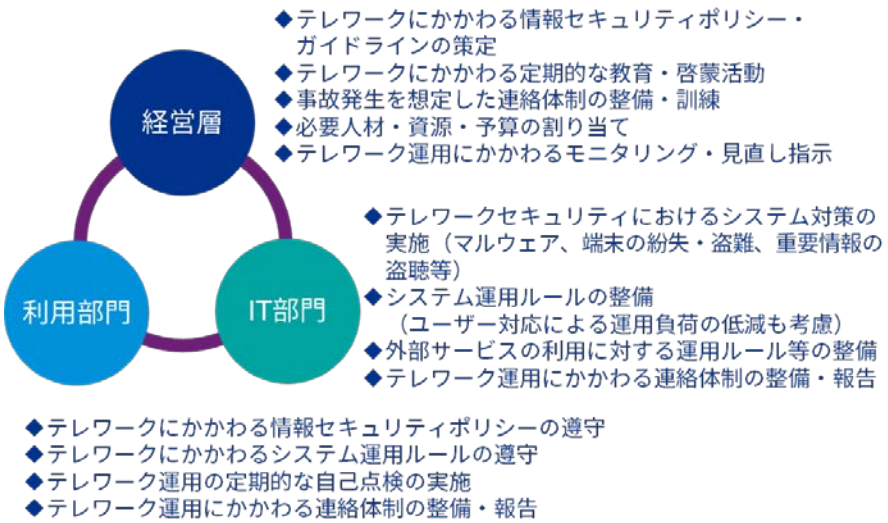
テレワークに関する網羅的なセキュリティ対策が取られていない場合には、改めてセキュリティ対策を検討することをお勧めします。検討にあたっては、テレワークのビジョン・目標を明確にしたうえで、勤務制度の整備、組織風土を変革しながら、**ガバナンスとシステム**の両面における各種施策を導入していくべきと考えます。

ガバナンスにかかわるセキュリティ施策

テレワークのセキュリティを確保するためには、テレワークにおける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求められます。

ルール策定においては、テレワーク運用にかかわる諸問題に対して、組織的に対応できる力の向上が必要となります。そのため、IT部門だけではなく、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重要です。

【図4】テレワークにおける体制・仕組みの整備

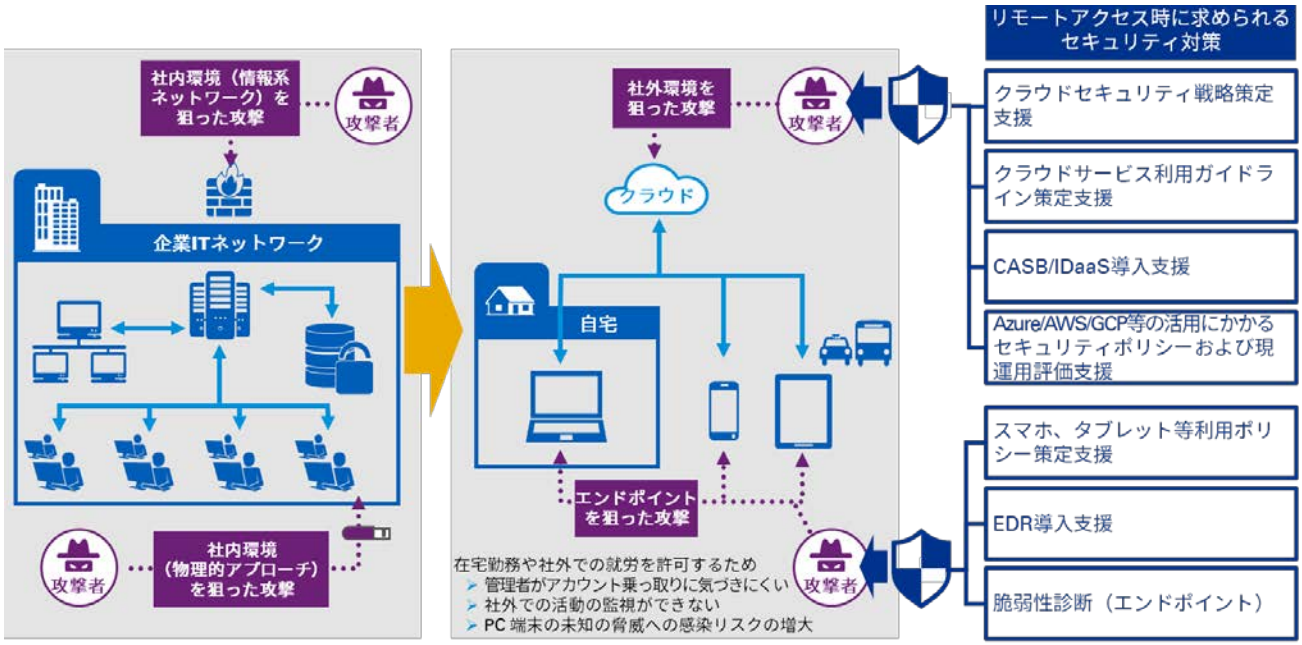


システムにかかわるセキュリティ対策

セキュアなテレ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はなく、リモートアクセスを前提としたセキュリティ施策が求められます。

オフィスで勤務する場合には、企業ITネットワークにてセキュリティが担保されていました。しかし、テレ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ネットワークにて担保されていたセキュリティは保証されません。そのため、新たなセキュリティ対策が必要となります。

【図5】テレ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

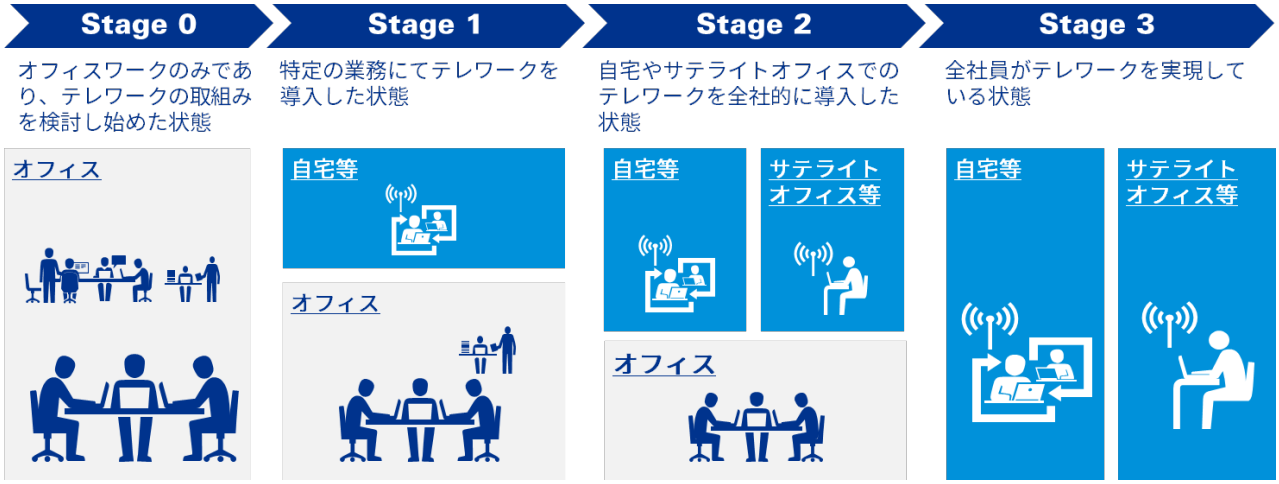


テレワーク活用の段階と各段階における検討項目

テレワークの導入においては、図6のように4つのStage（ステージ）に分類できると考えます。

最初のStage 0においてはテレワーク導入を検討している状態でありオフィスワークのみですが、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テレワークが開始されます。Stage 2になると、テレ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、自宅等だけでなく、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。テレワーク活用の最終段階であるStage 3においては、全社員がオフィス以外でも業務が遂行できる環境となります。

【図6】テレワーク活用の段階



テレワーク活用を進めるために検討すべき項目は、Stageごとに異なります。

テレ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することになります。端末としては、業務用ノートPCの支給だけでなく、BYOD利用の可否も検討します。

テレワークが導入されたStage 1においては、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。テレワークの導入により、社外にて機密情報を扱うことになるため、端末でのセキュリティ対策が重要となります。

Stage2においては、テレ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。社外にて効率的に進めるうえでは、クラウドを活用することをお勧めします。

Stage 3において、社内ネットワークを検討する必要が発生します。全社員が同時にテレワークを実施すると、VPN等の社内ネットワーク設備がひっ迫します。そのため、テレワークにとって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。

【図7】 各Stageにおける検討項目

	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	端末
	デスクトップPCからノートPCに移行した時のセキュリティリスクを評価し、対策をとる	端末
	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	端末
	持ち出しPCのプライベート利用を制限する	端末
	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	テレ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、NWや各種デバイスの増強する	社内ネットワーク
	委託先会社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える	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によるテレワークセキュリティ対策支援

KPMGでは、企業のテレワーク導入に関するセキュリティ対策を支援します。

テレワークセキュリティガイドライン整備支援
BYODの利用許可判断／プライベート利用の制限

脆弱性診断（エンドポイント）
持ち出しPCのセキュリティ対策

DLP導入支援
端末からの情報漏えい対策

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
許可されていないクラウドの利用制限

クラウドセキュリティアーキテクチャ設計支援
利用するクラウドのセキュリティ強化

ID管理構想策定支援／特権ID管理構想策定支援
本人認証の厳密化

多層防御最適化支援
不正侵入への対策

ID管理構想策定支援／特権ID管理構想策定支援
社外からのアクセス制御（委託先を含む）

リモートアクセスにおけるネットワーク最適化支援
ネットワークの増強

エンドポイント監視体制構築支援
セキュリティ監視・運用の強化

KPMGコンサルティング株式会社

03-3548-5111
kc@jp.kpmg.com

home.kpmg/jp/kc