テレワークと個人情報保護
働き方改革、パンデミックや非常事態に備えて

テレワークは、働く女性や男性の子育て環境の整備として、通常業務の効率化とワーク・ライフ・バランスの向上手段として、その他様々な働き方改革の実現手段としてニーズがあると同時に、ＢＣＰ（Business Continuity Plan：事業継続計画）を策定する際に、パンデミック発生時、激甚災害発生時やその他社会的混乱が発生した場合の有効な対策としても検討されています。そこで、テレワークを実施するに当たって留意すべき事項を、個人情報保護及び情報セキュリティの観点から確認することとします。テレワークとは、ネットワークを介して特定の事業所外から業務を行う形態を意味しており、営業担当者が外出先からネットワークを介して業務を行うことなどの広範な業務の実施形態も含まれますが、今回は、特に在宅勤務を行う場合を念頭に置き検討することとします。

１　ＢＣＰとテレワーク

２０２０年に入り、新型コロナウイルスが猛威を振るい、全世界的拡散と被害の拡大により企業活動も深刻な影響を受けるに至っています。学校に対する一斉休校の要請や不要不急の外出の見合わせの要請、各種イベントの中止や見送りが決定される事態にも及んでおり、重大な社会的、経済的影響を与えることが避けられない状況です。こうした状況の発生は、事業の遂行を困難意志、著しい影響を及ぼします。その際に、どのように事業を継続するのか、あるいは、事業への影響を軽減するのか、更には、より早く元の事業の実施状況に復旧させるかという課題への対策を策定し、準備し、実行することがＢＣＰです。

ＢＣＰの中で、従業員が事業所に出勤することが困難であったり、公共交通機関を用いた移動が困難であったりする場合の対策として、テレワークを導入することを検討されてきた事業者も多いと考えます。あらかじめ、綿密な計画、準備が進められている事業者においては、当該計画に基づき実行するとこになりますが、一方で、こうした準備が十分に行き届かずにいた事業者においては、取り急ぎ環境整備を行う等の対応に追われていることと思われます。

２　ＢＣＰ対応としてテレワークで実行する業務内容の整理とその効果

ＢＣＰでは、事業の中核に影響を与える現象はどのようなものであるかを人、物、金、時間の観点から分析することが重要となります。この過程で、事業を継続するために最低限必要となる守るべき事業活動を洗い出します。この守るべき事業活動は、事業者の規模、事業の性格などにより様々ですから一律に決めることはできません。

ソフト開発を中心とした情報サービスに関する事業であるなら、システム開発の仕事を、ネットワークを介して協調して実施することが可能ですし、打ち合わせに関しても様々なツールを用いて各担当者が自宅から参加し実施することも可能になります。一方、HWを中心とした製造業である場合には、工場設備の稼働が必須であり、担当者が出勤せざるを得ないという事情も考えられます。こうした業態でも、営業活動や受発注業務に関しては、完璧ではないにせよ、ネットワークを駆使して業務を行うことは可能であり、経理や人事といった事務領域においても同様でしょう。借入金や買掛金等の債務がある場合、その支払いが滞れば、事業の継続が困難になることも想定できます。

自社の仕事の中で、どの部分をテレワークで実施することができ、それを実施することによる効果、実施す

ること自体に意味があるのかを評価することが重要になります。

３　働き方改革としてのテレワーク

ＢＣＰにおけるテレワークは、事業継続に重大な影響を与える事態が発生した場合の対応策としてテレワークを検討するというものでしたが、通常の事業実行環境下においても、異なる視点からテレワークを導入することが考えられます。子育て環境の整備、業務効率とワーク・ライフ・バランスの向上、その他働き方改革としてのテレワークの導入です。

こうした場合にも、どの業務がテレワークに適しているのか、テレワーク環境を整備することにより、通常の業務と変わらずに実行できる仕事はどのようなものであるかを洗い出します。例えば、営業活動を行う場合、必ずしも所属する営業拠点に出向かなくとも、自宅から提案書や見積書を携えて客先に向かい営業活動を実施することは可能であり、会社への接続可能なＰＣと資料を出力するためのプリンターがあれば必要十分な環境を整えることができるし、あるいは更に一歩進めて、電子的に資料を客先に提出し併せてペーパーレスも同時に達成することが可能となります。

経理、人事のような仕事も、かなりの部分の業務をリモート環境で実施することは可能であり、テレワークとしての取り組みを導入し易い業務といえるでしょう。資料作成の為の打合せや作業の実施状況に関する確認等は、ＰＣやスマホ、タブレット等を用いネットワーク越しに実行することも、今なんらデメリットもなく実施できるため、抵抗感なく受け入れられる業務実施形態です。更には、決済行為に関しては、電子データによる電子決済を用いれば、書類を持ち回ることもなく、業務効率の向上と迅速化、省資源（環境対応）にも寄与することができるでしょう。当然、こうした取り組みはＢＣＰとしての対策にも貢献するものであり、実行可能な所から着手できるということから、導入検討への障壁も少ないと考えられます。

気になる費用対効果の点では、業務の効率化が達成できれば見合うものとなり、通勤時間の削減、通勤時における事故等のリスク削減、あるいは、子育てを行いながらも、結果的には、業務に従事することができる時間を増加させることも可能で、事業実施の生産性を損なうことなく子育て支援環境を整備することが可能となります。

４　テレワークでアクセスする情報の整理

テレワークで実施する業務が決まれば、次に考えるべきことは、業務の実施に当たってどのような経営資源が必要となるかを洗い出さなければなりません。とりわけ、どのような情報源にアクセスする必要性があるかは、個人情報保護及び情報セキュリティの観点から極めて重要になります。

普段は社内のネットワーク（イントラネット）からのみアクセスすることが可能な情報源に、外部からネットワークを介してアクセスすることが必要となる場合では、その安全性に関して検討を加えなければなりません。また、誰が、どの情報にアクセスする必要があるのかを明確にすることも必要です。通常の業務遂行形態の中でも、アクセス権限の分析、設計とアクセス制御の実施は重要な課題ですから、平素から技術的安全管理措置として適切な取り組みができているならば、この課題については新たに多くの工数を必要とすることはないはずです。

５　基本方針（実施方法とセキュリティ・ポリシー）の策定

誰にテレワークを許可するのか、アクセス権限とその制御はどのように行うのか、識別証方式をどうするのか、更には、ＢＹＯＤ（Bring Your Own Device）、即ち対象者の持つ私的な機器の利用（ここでは、必ずしも

Ｂｒｉｎｇ（持ち運び）のみではなく家庭内に設置されている機器を含む）を許容するのか否かなど、テレワークを行うにあたっての実施方法とセキュリティ・ポリシーを定め、実際の対策に反映して行くことが大切です。基本方針をしっかり定めておきませんと、木を見て森を見ないような、矛盾だらけの仕組みの導入や方法やセキュリティ対策の実施になりかねません。

６　自動化・省人化の検討

テレワークの具体的実施方法を検討する前に、自動化・省人化の可能性を整理しておくことも大切です。業務を分析し、標準化を行った上で、それをシステムとし組み立てておきます。情報セキュリティや個人情報保護での問題発生の最も多い原因は、人によるミスです。テレワークを導入した際には、ネットワークを介して広範な業務を実施する可能性がある訳ですから、人的ミスが発生すれば、それによる個人がうける被害、事業者が受ける損失は大きなものとなる可能性があります。その発生機会を減少させるために、自動化・省人化は大変有用なものであり、検討する価値のある施策です。

７　テレワークの導入と規律の整備

個人情報の保護に関する法律についてのガイドラインにおいて、実施すべき安全管理措置の一つとして定められているのが、個人データの取扱いに関する規律の整備です。テレワークを導入しようとする場合は、テレワークにおいて取り扱うことになる個人データの基本的な取扱ルールを定めて置くことが重要です。ルールの定め方は、事業者の規模や事業の性格等により変わりますので、一律に決められる訳ではありません。

特に気を付けるべきことは、業務の実施状況を、お互いにその場で確認できる環境ではない場所で担当業務を実施することになりますで、不正な取扱いが発生しないよう歯止めを掛けておくことが重要です。故意ではなく、勘違いや不注意でも不正な取扱いは発生する可能性があります。こうしたことが発生しないよう、確認方法、承認方法等業務を行う上で関連して必要となる手続きについても取決めておきます。

テレワークの実施マニュアル等を制定し、その中で手順、実施環境に関する物理的、技術的必要事項を定めておくと良いでしょう。個人が所有する機器を使用することを前提とする場合は、危険性の高いソフトウエアや安全性が確認されていないソフトウエアがインストールされていると、重大な事態を招いてしまう可能性がありますので、必須事項と禁止事項を物理的、技術的安全措置として定めておきます。業務で使用するために提供している機器を自宅に持ち帰って使用する場合には、移送時及び自宅保管時の安全性の確保についても決めておくことが望まれます。

８　組織的安全管理措置

組織的安全管理措置として、実施すべき事項は以下のとおりです。各々の事項について、テレワークの特性を考慮し実施します。

①　組織体制の整備

「安全管理措置を講ずるための組織体制を整備しなければならない」

テレワークにより個人情報保護の体制が大きく変わるわけではありません。しかし、同一事業所内で仕事を行うわけではありませんので、問題発生時の連絡体制等を徹底しておくことが重要です。

②　個人データの取扱いに係る規律に従った運用

「あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない」

テレワークは、規律の整備で作成した、実施マニュアルに従って実施することになります。運用においては、決まりに従って正しく実施できているかを確認する手段を用意しておくことが大切になります。確認手段は、実施記録の取得、週報などによる実施状況の報告の提出がその方法となりますが、データのアクセス状況などの記録が仕組みとして残るようにすると効率的です。人手を使って入力していると、正しく記録が残らない場合が発生し易くなります。

③　個人データの取扱状況を確認する手段の整備

「個人データの取扱状況を確認するための手段を整備しなければならない」

規律に従った運用において、確認手段について記述しましたが、更に、業務に用いる個人データが、分散して存在することにもなりますので、誰がどのデータを保有しているかについて整理しておくことが重要です。

個人データの取扱状況を適切に確認できるようにするためには、個人情報データベースの台帳を整備することが効果的対策です。個人情報データベース等の台帳で管理すべき項目としては、個人情報データベース等の名称、管理番号、件数、個人データに含まれる項目、利用目的、取得方法、管理部署、管理責任者、利用部署、利用者、保管方法（システムその他）、保管媒体、廃棄期限、廃棄方法等です。一度作った台帳も、事業の実施状況から変化することもあり得ますので、最低でも１年に１回の更新を行うことが望まれます。

更に、テレワークを行う場合には、テレワークでの利用の有無、テレワークによる利用者、アクセス方法などを項目として加えることにより、どのデータがテレワークにより利用されているのかが容易に管理できるようになります。

④　漏えい等の事案に対応する体制の整備

「漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない」

問題発生時の連絡体制の整備に加え、テレワークの仕組に起因した漏えい等の事案が発生した場合の原因の究明方法を、技術的な対応も考慮した上で取り決めておくと良いでしょう。顔を合わせて業務を行う場合と異なり、テレワークでは、日々のコミュニケーションが限定的になりがちです。従って、問題発生の状況に応じて、どのような経路で報告・連絡を行うのか、報告・連絡を行う時期（タイミング）、報告・連絡内容はどのようなものにするのか、対策のための会議の開催・運営方式をどのようにするかを取り決めておくと、円滑な問題解決が行えるようになります。

⑤　取扱状況の把握及び安全管理措置の見直し

「個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない」

実施状況の記録、問題発生状況、あるいは、過剰な取り決めはないのか、業務を行うに当たっての利便性が削がれていないか等、様々な観点から記録や事実に基づき点検、監査と改善を行います。テレワークについて特に着目して確認する方法もありますが、通常の点検、監査の一環として取り組んでもかまいません。

９　人的安全管理措置

人的安全管理措置として、実施すべき事項は以下のとおりですが、テレワークの特性を考慮した対応が必要です。

①　従業者の教育

「従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない」
個人データの取扱いに関して遵守すべき事項の周知徹底の一環として、テレワークの実施手順等について十分に教育を行います。特に、物理的な安全性を確保するための意識付け、情報セキュリティ上の注意事項、技術的な安全性確保の徹底に関する意識付けを行うことが重要です。

１０　物理的安全管理措置

物理的安全管理措置として、実施すべき事項は以下のとおりです。在宅勤務を想定した場合では、実施場所は自宅となります。業務を実施する者が、自宅において家族と生活を共にしている場合についても想定しておかなければなりません。同一の場所であれば、同居者が問題を発生させてしまう可能性も考慮しなければなりません。

①　個人データを取り扱う区域の管理

「個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（以下「管理区域」という。）及びその他の個人データを取り扱う事務を実施する区域（以下「取扱区域」という。）について、それぞれ適切な管理を行わなければならない」

事業所における区域の分離と必要な管理や対策は徹底できたとしても、在宅での仕事環境は、区域を分離することが困難な場合も多くあります。ネットワークを介して、自宅のリビングや食卓で仕事を行うことも多いはずです。この場合の留意点は、なによりも整理整頓の徹底であり、様々な媒体に記録された個人情報等が散逸しないよう注意することが重要です。

自宅においてテレワークを行う場合、取扱区域としてテレワークの実施環境が含まれます。どのような安全性を求めるかを定義しておくことが重要となります。

②　機器及び電子媒体等の盗難等の防止

「個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない」

できるだけ自宅に情報を残さないことが理想ですが、完全に実施できない場合も存在します。自宅において業務用のために保有していた個人情報が、盗み出された事例もあります。徹底した自宅の施錠、侵入防止策、保管場所の工夫等の施錠管理を行うことが必要です。また、家族に対しては、仕事の情報があるために施錠を徹底する様、協力を要請することも重要です。また、ＩＴ機器ごと盗まれたケースもあるため、技術的対策も併用し、シンクライアント化によるデータ保有の制限と盗難対策、あるいは、暗号化の徹底などの対策を実施しておく必要があるでしょう。

テレワークを行うに当たって端末のシンクライアント化は、安全対策として非常に有効ですが、必須条件とはいえません。例えば、技術的安全管理措置としてＰＣの利用に関して、ＢＩＯＳロック機能を用いる、生体認証を用いる、ストレージの暗号化を行う等の対策を複層的に実施すれば、盗難、紛失時における安全性は格段に向上します。費用の負担も大きくなく容易に導入でき、効果の高い方法を組み合わせることも、一つの選択肢です。

③　電子媒体等を持ち運ぶ場合の漏えい等の防止

「個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない」

自宅への持ち運び時の注意、媒体に対する対策を、持ち運び時と自宅保管時の双方を視野に入れ実施します。会社保有の機器を使用する場合は、置き忘れによる紛失や車上荒らし等による盗難被害が多く発

生しているため、運搬する際の注意事項の徹底が重要です。

④ 個人データの削除及び機器、電子媒体等の廃棄

「個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元できない手段で行わなければならない」

在宅勤務においては、不必要となった個人データを廃棄する方法を決めておくことも重要な課題です。電子機器等は、事業所の持ち運びルールに従って廃棄するようにすれば個別の問題発生の可能性は減少します。但し、持ち運び時には細心の注意が必要です。紙媒体に関しては、対象者に粉砕性能が高い小型のシュレッターを提供し、粉砕処理をした上での廃棄を徹底させる、あるいは、回収ボックスを備え付け、定期的に事業所に送り、廃棄する方法等が考えられます。業者による移送中に紛失が起きたという事例もありますので、残留リスクがあることを認識しておかなければなりません。

１１　技術的安全管理措置

技術的安全管理措置として、実施すべき事項は以下のとおりですが、テレワークでは、その性質上、技術的な安全対策が極めて重要となります。テレワークで実施可能となる業務内容の種類、重要度が増す程、念には念を入れた対策が必要です。セキュリティ対策の強化は、時として利便性を犠牲にする場合もありますが、サイーバー攻撃が一層激化している今日においては、安全性に軸足を置いた対策が重要であるといえるでしょう。

① アクセス制御

「担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない」

テレワークで実施する業務を洗い出し、アクセスする必要があるデータを特定することは、先に触れたとおりです。テレワークにおいて、事業所内と同様のデータへのアクセスを許すべきか、限定的とすべきかについては、テレワークを導入する狙いと期待する効果によって変化します。不正アクセス防止対策の実施内容にも影響を与えますので、慎重な検討が必要になります。

事業所内と同様とすれば、システムの改修等に係る手間が減少することも考えられますが、アクセス制御、識別認証、ネットワークの接続方法等、綿密な安全対策を取るべきです。

② アクセス者の識別と認証

「個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない」

ネットワークを経由して業務システムを利用する場合、万一、不正アクセスが発生すれば甚大な被害が発生する場合もあります。このため利用者に対する識別と認証は極めて重要です。ＩＤを入力し、パスワードのような知識要素を入力し、更に、スマートフォン（所有要素）に送ったセキュリティコードを入力することで初めて利用できるようにするなどの、多要素認証を導入することが望まれます。他の要素として、顔認証等の生体要素を用いる方法も有用です。

日常業務に用いるメールアドレスをＩＤとする方法は、外部の者から察知される可能性も高いため、安全性を減じる場合もあり得ますので注意すべきです。

③ 外部からの不正アクセス等の防止

「個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウエアから保護する仕組みを導入し、適切に運用しなければならない」

在宅勤務の場合、自宅で導入しているネットワーク回線を利用するケースが殆どではないでしょうか。家族と同じＷｉ－Ｆｉルータを使用する場合もあり得ます。個人で、自宅にファイアウォールを導入し、安全性を高めているケースは少ないと考えられますが、基本的な設定を行った機器をテレワーク用に提供し、設置する方法も考えられます。また、事業所側の受け口とＰＣをＶＰＮ（Virtual Private Network）で結び、安全な接続を行う方法、端末に電子証明を送り、特定の機器からの接続のみを許す方法等、安全な仕組みを選定することが重要です。

自宅内で他の者が利用するＮＡＳ（Network Attached Storage）等にデータを収容しない等、安全性の確保とルールの徹底が必要不可欠となります。当然、パスワードの使い回しなどはあってはなりません。自宅のネットワーク機器の管理権限のパスワードが、初期設定のままであると容易に不正な侵入を許してしまうことになり、そうした被害の例も多く存在しま。

自宅内におけるネットワークは、家族の他の者が私的に利用するものと同じ物を使用しているケースが殆どでしょうが、理想的には、家庭内においても、私的なものと仕事用のネットワークをセグメント分けし、相互に乗り入れができないようにすることが望ましい方法です。こうした道具類は、個人の負担で導入させるものではなく、事業者が決めた方式に従い、事業者から供与するべきと考えます。

機器へのウイルス対策ソフトウエアの導入は必須であり、最新状態に保つ必要があります。また、利用する機器のソフトウエア等は最新の状態を保ち、脆弱性排除のための更新ソフトウエアは、迅速に適用しなければなりません。標的型攻撃等でウイルス感染し、端末を乗っ取られ、情報流出につながったケースもありますので、技術的対策に加えて、不審なメールへの対応力を高めるための従業者の訓練なども有効な手立てです。

個人所有の機器を利用する場合は、不正侵入を防止する等の観点から、導入すべきソフトと導入禁止のソフトウエアを明確にしておくことが必須です。エッジデバイスの監視が可能なソフトウエアも存在し、不正ソフトの起動防止等の効果があるのですが、個人的な活動までモニタリングできてしまう点から、導入すべきかについては慎重な検討が必要で、また、導入する場合は本人との合意形成が必要不可欠となります。

④ 情報システムの使用に伴う漏えい等の防止

「情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない」

不正アクセス防止の項目において、ネットワークを介した安全な接続について触れましたが、テレワークの性質上、電子メールを用いた情報交換が多くなると考えられます。人的ミスの中において、非常に多く発生しているのが電子メールの誤送信であるため、この防止策についても検討しておきます。一定時間送信せずに電子メールを保留し、取り消すことができるようにする仕組みの導入も有効です。

テレワークの導入に関する留意点を、安全管理措置を中心に確認・検討しましたが、事業者としては、自社の体力やテレワークの有効性を勘案しつつ、安全性の高い方法での導入が進むことを望みます。