情報の利用・管理 / サイバーセキュリティ　7-1

テレワークでのマイナンバー等の取扱い

弁護士　白石 和泰
弁護士　溝端 俊介

Question

テレワークを行っている従業員に、個人情報やマイナンバーを取り扱わせる際の留意点は何ですか。

Answer

可能な限りテレワークにおいて個人情報やマイナンバー（以下、「マイナンバー等」と総称）を取り扱わせることは避けるべきです。

どうしても取り扱わせざるを得ない場合には、自宅でのマイナンバー等の取扱いが社内規程に抵触しないか、当該規程が定める手続を履践しているかを確認した上、担当者以外の者がマイナンバー等を閲覧等できないような措置を適切に講じさせなければなりません。

具体的には、鍵のかかる個室で施錠の上作業させたり、少なくともドアや窓にPCの画面を向けて作業することを禁止した上で、画面への覗き見防止フィルターの貼付を義務化したりし、気が緩みがちなテレワークについて会社で作業する場合以上に徹底した教育・指導を行うことが重要です。

また、担当者の作業環境についてシンクライアント（必要最低限の機能のみを有するPCでの作業環境）を実装したり、少なくともセキュリティ対策ソフトを常に最新のものとしたりするなど可能な限りのセキュリティ措置を施すとともに、万一マイナンバー等が記録されたPCや電子媒体等を持ち運ぶ際には、強固なパスワードロックをかけるなど、技術的安全管理措置も講じる必要があります。

1. はじめに

個人情報については個人情報の保護に関する法律（個人情報保護法）20 条が、特定個人情報（いわゆるマイナンバー）については行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法（マイナンバー法））12 条が、個人情報や特定個人情報（以下、「マイナンバー等」と総称します。）についての安全管理措置義務を定めています。

安全管理措置の内容については、個人情報保護委員会がガイドライン[1]を策定してその手法を例示しており、基本方針の策定、個人データの取扱いに係る規律の整備、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置が挙げられます。

通常業務を前提とした安全管理措置がすでに整備されていたとしても、テレワークにより作業環境が変化するため、テレワークの環境に合わせた対応が必要です。

もっとも、必要な対応を行ったとしても、テレワークでは、通常の勤務体制に比べて、これらの安全管理措置の水準は下がりがちです。そのため、テレワークにおいてマイナンバー等を取り扱わせることは可能な限り避けるべきですが、どうしても取り扱わせざるを得ない場合には、以下の対応をとることが考えられます。なお、マイナンバー等に限られない一般的なサイバーセキュリティについては、Q7-2 もご参照ください。

2. 個人データの取扱いに係る規律の整備

まず、個人データの取扱いに係る規律の整備としては、現行の社内規程がテレワークに対応したものかどうか確認し、対応していない場合は適切な規定を導入する必要があります。たとえば、「マイナンバーを記録した媒体を社外に持ち出してはならない」というような規定がされている場合があります。対策としては、「以下の場合に限り、社外で取り扱うことができる」として、後述する安全管理措置を自宅で行っている場合には、社外でのマイナンバー等の取扱いを認めることが考えられます。

3. 組織的安全管理措置

次に、組織的安全管理措置としては、テレワークでのマイナンバー等の取扱状況を確認し、漏洩等の事案に対応する体制を整備しなくてはなりません。会社の管理する建物内でマイナンバー等の取扱いがされる場合と、テレワークの場合とでは、確認プロセスも変化することが想定されます。そのため、通常の管理部署に加え、テレワークを統括する部署を新設することが考えられます。また、テレワークにおいては、不祥事が起きた際の上司への報告について、対面での業務に比べ心理的なハードルが上がってしまい、通常のレポーティングラインがうまく機能しない可能性があります。そのような事情も踏まえた上で、漏洩が起きた際のエスカレーションの取り決めをする等の対策が必要になります。なお、通常のレポーティングラインを補完するための内部通報制度の活用については、Q7-3 もご参照ください。

4. 人的安全管理措置

[1] 個人情報の保護に関する法律についてのガイドライン（通則編）
（https://www.ppc.go.jp/files/pdf/190123_guidelines01.pdf）、特定個人情報の適正な取扱いに関するガイドライン（事業者編）
（https://www.ppc.go.jp/files/pdf/my_number_guideline_jigyosha.pdf）

人的安全管理措置としては、テレワーク下でのマイナンバー等の取扱いに関する留意事項について、研修などにより教育・指導を行う必要があります。テレワークでの作業環境構築についての手引きやマニュアルを作成し交付することに加え、そのうち重要なポイントについてはWeb 会議等で直接説明を加えることが考えられます。

漏えい等のマイナンバー等の不適正な取扱いは人為的ミスが原因で発生することが多いため、気が緩みがちなテレワークについて会社で作業する場合以上に徹底した教育・指導を行うことが最も重要です。

5. 物理的安全管理措置

物理的安全管理措置については、担当者以外の者がマイナンバー等を閲覧等できないような措置を適切に講じさせなければなりません。ガイドラインでは、間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等が例示されています。それを踏まえて、テレワークにおける具体的な対応としては、鍵のかかる個室で施錠の上作業させたり、少なくともドアや窓にPC の画面を向けて作業することを禁止した上で、画面への覗き見防止フィルターの貼付を義務化したりすることが考えられます。喫茶店や電車内等の他人が行きかう場所での作業を慎むべきことは言うまでもありません。

また、マイナンバー等の取扱い業務以外にも、業務において、Web 会議システムを利用した会議を行い、画面共有を行うこともあるかと思います。その際に、マイナンバー等を取り扱っている画面が万が一にも共有等されないよう、会議開始前にマイナンバー等が含まれるファイルを閉じることを徹底するということも、テレワークにおける物理的安全管理措置としては重要です。

6. 技術的安全管理措置

技術的安全管理措置については、外部からの不正アクセス等の防止及び情報システムの使用に伴う漏えい等の防止を行う必要があります。

担当者の作業環境についてシンクライアント（必要最低限の機能のみを有するPC での作業環境）を実装したり、少なくともセキュリティ対策ソフトを常に最新のものとしたりするなど可能な限りのセキュリティ措置を施すとともに、(持ち運ばない場合であっても不正アクセス等の防止のためにパスワードロックをかけておくべきですが)万一マイナンバー等が記録されたPC や電子媒体等を持ち運ぶ際には特に、当該PC や電子媒体等及びマイナンバー等が含まれるファイルに強固なパスワードロックをかける（強固なパスワードロックが施されていることを確認する）などの措置も講ずる必要があります。Web 会議システム等を利用する際も、セキュリティ上疑念のあるアプリケーションの使用は避け、かつ、適切なセキュリティ措置が講じられているとされるアプリケーションであっても、常に最新のバージョンのものを利用するようにしてください。

また、テレワーク環境では物理的な監視ができないために、USB メモリ等に書き出してマイナンバー等を持ち出すことが容易になってしまいます。その対策として、PC 等にファイル転送の検知ソフトをインストールしておく、PC 等を書き出し禁止の設定にしておく等の対策が考えられます。

以上