第3版 (2024年4月1日)

テレワーク実施におけるセキュリティセルフチェックリスト

Reserve LINK

本資料は、**総務省「テレワークセキュリティガイドライン 第４版」**に基づき、弊社のテレワーク実施におけるセキュリティ対策について自己点検し、まとめたものです。

本書の第三者への開示はご遠慮願います

尚、各項目については弊社業務に合わせ一部変更・追加を行っている場合があります。

大分類		No.	確認内容	対応	詳細・補足
テレワークセキュリティ対策のポイント					
(ア)	経営者が実施すべき対策	1	経営者は、テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、その内容に応じて見直しを行う。	○	ISMSの運用ルール、運用スケジュールに則り情報セキュリティポリシーの確認をしています。
		2	社内で扱う情報について、その重要度に応じたレベル分けを行った上で、テレワークでの利用可否と利用可の場合の取扱方法を定める。	○	PC等の機器及び取り扱う情報についてテレワークでの利用についての利用可否、運用ルールを定めています。
		3	テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、定期的に教育・啓発活動を実施させる。	○	ISMSの運用ルールに則り定期的なセキュリティに対する教育を実施させています。また、テレワークに特化した教育に関しても実施の指示をしています。
		4	情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を整えるとともに、事故時の対応についての訓練を実施させる。	○	ISMSの運用ルール、運用スケジュールに則り訓練の実施をさせています。
		5	テレワークにおける情報セキュリティ対策に適切な理解を示した上で、必要な人材・資源に必要な予算を割り当てる。	○	情報セキュリティ管理者に対しテレワークに関するセキュリティ対策を含め、セキュリティ対策の検討及び実施の指示をしています。
(イ)	システム管理者が実施すべき対策	1	システム全体を管理する重要な立場であることを自覚し、情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。	○	情報セキュリティポリシーを根底とするISMSの運用等をルール化しセキュリティの維持を図りまた、定期的な内部監査によりそれらを評価しています。
		2	情報のレベル分けに応じて、電子データに対するアクセス制御、暗号化の要否や印刷可否などの設定を行う。	○	情報の重要度に応じアクセス可能な人員の制限及び権限分けを行いアクセス制御を実施しています。
		3	テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、定期的に教育・啓発活動を実施する。	○	ISMSの運用ルールに則り定期的にセキュリティに関する教育を実施しています。
		4	情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を確認するとともに、事故時の対応についての訓練を実施する。	○	ISMSの運用ルールに則り定期的にセキュリティに関する訓練を実施しています。
		5	フィルタリング等を用いて、テレワーク勤務者が危険なサイトにアクセスしないように設定する。	○	セキュリティソフトの導入及びそれらを最新の状態となるように設定をしています。
		6	テレワーク勤務者がテレワーク端末にアプリケーションをインストールする際は申請させ、情報セキュリティ上の問題がないことを確認した上で認める。	△	PCにインストールされたアプリケーションはシステム管理者が随時確認できる状態となっており、また利用を禁止されたアプリケーションは実行できない仕組みを導入しています。
		7	貸与用のテレワーク端末にウイルス対策ソフトをインストールし、最新の定義ファイルが適用されているようにする。	○	貸与用の端末は、通常の業務利用端末と同等の管理をしておりシステム管理者が状態の確認を随時チェックできる体制となっています。
		8	貸与用のテレワーク端末のOS及びソフトウェアについて、アップデートを行い最新の状態に保つ。	○	システム管理者の管理の下、定期的にアップデートを実施しています。
		9	私用端末をテレワークに利用させる際は、その端末に必要な情報セキュリティ対策が施されていることを確認させた上で認める。	○	私用PCによる業務は原則禁止とし、会社支給の管理されたPCを用いています。
		10	ランサムウェアの感染に備え、重要な電子データのバックアップを社内システムから切り離した状態で保存する。	○	重要な電子データは社内システムとは切り離された場所もしくは複数の認証が必要な場所にバックアップされています。
		11	金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。	○	迷惑メールフィルタの利用をしています
		12	台帳等を整備し、貸与するテレワーク端末の所在や利用者等を管理する。	○	ISMSの運用ルールに則り、持ち出し可能な機器及びそれらの状態を管理しています。
		13	テレワーク端末において無線LAN の脆弱性対策が適切に講じられるようにする。	○	テレワークで利用する全PCにセキュリティソフトをインストールし、管理者が状態を確認できるようにしています。

		14	社外から社内システムへアクセスするための利用者認証について、技術的基準を明確に定め、適正に管理・運用する。	○	会社で定めたセキュアな接続方法でのみ接続できる状態とし運用しています。
		15	テレワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。また、社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、アクセス状況を監視するとともに、不必要なアクセスを遮断する。	○	会社で定めたセキュアな接続方法でのみ接続できる状態とし運用しています。また、社内ネットワークとインターネットの境界にはUTMを設置し不正なアクセスは遮断するように設定されています。
		16	社内システムへのアクセス用のパスワードとして、強度の低いものを用いることができないように設定する。	○	社内のパスワードポリシーを規定し運用しています。また、アクセスには複数の認証が必要となる状態としています。
		17	メッセージングアプリケーションを含むSNSに関する従業員向けの利用ルールやガイドラインを整備し、その中でテレワーク時の利用上の留意事項を明示する。	○	ISMSの運用ルールに則り定期的に左記を含むセキュリティに関する教育を実施しています。
		18	ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、情報漏えいにつながる恐れのある利用方法を禁止する。	○	ISMSの運用ルールに則り定期的にセキュリティに関する教育を実施し、また、権限の整備などを行いアクセスに制限を設けています。
(ウ)	テレワーク勤務者が実施すべき対策	1	テレワーク作業中は、利用する情報資産の管理責任を自らが負うことを自覚し、情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、定期的に実施状況を自己点検する。	○	ISMSの運用ルールに則り定期的にセキュリティに関する教育を実施しています。
		2	テレワークで扱う情報について、定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。	○	情報資産の重要度に応じ、利用可能な人員及びそれらのセキュアなアクセス方法をルール化しています。
		3	定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、情報セキュリティに対する認識を高めることに務める。	○	ISMSの運用ルールに則り定期的にセキュリティに関する教育を実施しています。
		4	情報セキュリティ事故の発生に備えて、直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、事故時に備えた訓練に参加する。	○	ISMSの運用ルールに則り定期的にセキュリティに関する訓練を実施しています。
		5	マルウェア感染を防ぐため、OSやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。	○	OSやブラウザは自動で最新の状態とする設定を原則としており、またIT資産管理ソフトを導入しシステム管理者が随時その状態をチェックできる仕組みとなっています。
		6	アプリケーションをインストールする際は、システム管理者にその旨を申請し、許可を受けたアプリケーションのみをインストールする。	△	PCにインストールされたアプリケーションはシステム管理者が随時確認できる状態となっており、また利用を禁止されたアプリケーションは実行できない仕組みを導入しています。
			（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、安全性に十分留意して選択する。	○	私用端末での業務は原則禁止しています。
		7	作業開始前に、テレワーク端末にウイルス対策ソフトがインストールされ、最新の定義ファイルが適用されていることを確認する。	○	ウイルス対策ソフトは最新の状態となるよう設定されています。また、システム管理者が随時その状態をチェックできる仕組みとなっています。
		8	作業開始前に、テレワーク端末のOS及びソフトウェアについて、アップデートが適用され最新の状態であることを確認する。	○	OSは最新の状態となるよう設定されています。また、システム管理者が随時その状態をチェックできる仕組みとなっています。
		9	テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、スマートフォン、タブレット等に関しては不正な改造（脱獄、root 化等）を施さない。	○	業務には支給された機器を利用することを原則としています。
		10	テレワーク作業中にマルウェアに感染した場合、その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。	○	定期的なセキュリティに関する社内研修等での周知や端末へのセキュリティソフトのインストールを行いマルウェア感染防止をしています。
		11	オフィス外に情報資産を持ち出すとき、その原本を安全な場所に保存しておく。	○	情報資産は持ち出しの有無によらず、重要な情報はバックアップを取得しています。
		12	機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。やむを得ない場合は必ず暗号化して保存するとともに、端末や電子データの入った記録媒体（USBメモリ等）等の盗難に留意する。	○	USBメモリ等の記録媒体の利用は原則禁止しており、PCから外部媒体への書き出しはできないように機械的な制御がされています。
		13	機密性が求められる電子データを送信する際には必ず暗号化する。	○	ISMSの運用ルールで定められたルールに基づき利用しています。
		14	無線LAN 利用に伴うリスクを理解し、テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。	○	テレワークにおける社内ルールに明示し周知徹底をしています。
		15	第三者と共有する環境で作業を行う場合、端末の画面にプライバシーフィルターを装着したり、作業場所を選ぶ等により、画面の覗き見防止に努める。	○	テレワークにおける社内ルールに明示し周知徹底をしています。
		16	社外から社内システムにアクセスするための利用者認証情報（パスワード、ICカード等）を適正に管理する。	○	テレワークにおける社内ルールに明示し周知徹底をしています。
		17	インターネット経由で社内システムにアクセスする際、システム管理者が指定したアクセス方法のみを用いる。	○	社内で決められているセキュアな接続方法でのみアクセスを可能としています。
		18	テレワークで使用するパスワードは、使い回しを避け、一定以上の長さで他人に推測されにくいものを用いるように心がける。	○	社内のパスワード設定ポリシーを周知徹底し運用しています。

		19	メッセージングアプリケーションを含むSNSをテレワークで利用する場合、社内で定められたSNS利用ルールやガイドラインに従って利用するようにする。	○	ISMSの運用ルールで定められたルールに基づき利用しています。
		20	テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、社内ルールで認められた範囲で利用する。	○	ISMSの運用ルールで定められた範囲での利用を原則としています。