情報セキュリティ対策　14のチェックポイント

組織的な対策

No.	項目	備考
1	テレワーク可能な業務・役職を整理し、起こりゆるリスクを想定した	部署ごとでなく、業務ごとに出社の要不要を検討
2	パソコンなど機器使用に関するリスクと対策を想定した	盗難・紛失、破損などが想定される
3	ネットワーク接続に関するリスクと対策を想定した	安全性が担保されていない回線、知らない宛先のメールに注意
4	ファイル管理に関するリスクと対策を想定した	閲覧時のリスクと共有時のリスクがある
5	チャットやビデオ会議など、コミュニケーションに関するリスクと対策を想定した	パスワードの設定不備、ビデオ会議URLの共有方法に注意
6	経営陣と情報システム部門で定めたルールをガイドライン化した	担当部署と経営陣が連携してガイドラインを作成
7	ガイドラインを社内で配布し、理解促進のために研修等を行った	説明会や研修でリスクや対策を啓蒙することが重要

テレワーク利用者の対策

No.	項目	備考
1	セキュリティリスクについて理解するための研修に参加した	社内研修だからと軽視せず、セキュリティ意識を高める
2	パソコンにセキュリティ対策ソフトをインストールした	ソフトだけでなく、パソコンのOSのバージョンも常に最新に
3	パソコンなど機器の紛失・盗難時の対策を施した	万一の際の情報伝達ラインについても確認しておく
4	会社が定めたネットワーク環境を利用している	個人の判断だけで公衆回線を利用しない
5	会社が定めたファイル管理の手法・ツール等を利用している	会社としてクラウドサーバーを活用すると誤送信の際も安全
6	会社が定めたコミュニケーションツールを利用している	取引先が指定したツールなど、外部サービスの利用範囲を確認
7	万一セキュリティ問題が発生した際の、対応方法を理解している	防止策だけでなく、有事の際の対応方法も把握しておく