【緊急事態宣言解除後のセキュリティ・チェックリスト】

1. **停止したシステムの再稼働における注意事項**

|  |  |
| --- | --- |
|  | 長期間停止していたシステムの動作確認を行う |
|  | 長期間停止していたシステム構成機器のセキュリティ対策の最新化を行う  （OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等） |

1. **テレワークで社外に持ち出した機器を社内NWに接続する際の注意事項**

|  |  |
| --- | --- |
|  | 持ち出した機器（端末や外部記憶媒体等）が紛失していないか棚卸し確認する |
|  | 端末のセキュリティ対策が最新化されているか確認する  （OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等） |
|  | 持ち出した機器（端末や外部記憶媒体等）がマルウェアに感染していないか確認する |
|  | 無許可のソフトウェアがインストールされていないか確認する |
|  | テレワーク期間中に、社内システムに不正アクセスされていないかログ等を確認する |
|  | 社内NWに接続した端末から不審な通信が行われていないか監視を一定期間強化する |

1. **緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い**

|  |  |
| --- | --- |
|  | 緊急措置として許可した私物端末利用（BYOD）の利用実態について確認する（私物端末のセキュリティ対策やマルウェア感染の有無、私物端末に保存されていた業務関連資料の削除確認等） |
|  | 緊急措置としてテレワークを許可していた業務やルールを変更した業務のリスクを再評価する |
|  | 再評価により、リスクが許容できると判断された業務については、引続きテレワークを継続すべく、必要に応じてセキュリティポリシー等の改訂を行うことを検討する |
|  | 再評価により、リスクが高いと判断された業務については、一旦元の運用に戻し、テレワークができる手段を検討したうえで、テレワークの可否を判断する |

1. **Withコロナフェーズに向けた、業務見直しとセキュリティ対策**

|  |  |
| --- | --- |
|  | 第二波など緊急事態宣言の再要請に備え、業務移行の手順、必要なサービスを整理する |
|  | テレワークにより負荷が集中した従業員や業務の洗い出しと対応の見直しを行う |
|  | テレワークにより負荷が集中したサービスの洗い出しと対応の見直しを行う |
|  | テレワークにより業務効率が下がった業務の洗い出しと対応の見直しを行う |
|  | テレワークにできなかった業務の洗い出しと今後の対応について検討する |
|  | 脱押印のためのオンラインワークフローや電子署名サービスの導入について検討する |
|  | 社内業務だけでなく、顧客や外部委託先との契約上、テレワーク化することができない業務やサービスについて、テレワークができる手段を検討し、顧客や外部委託先と協議の上、必要に応じて契約条件の見直しを検討する |
|  | 今までのIT投資やセキュリティ対策の優先順位を見直し、テレワークを前提とした社内IT投資やセキュリティ対策について検討する |
|  | テレワークを前提としたシステム構成管理やログ設定の見直しを行う |
|  | クラウドサービスや社内外で安全かつシームレスに業務を実施するためのゼロトラストネットワークの導入を推進する |
|  | テレワークを前提としたセキュリティインシデント発生時の体制や対応について再検討を行うと共に、そのための教育や訓練を行う |
|  | これを機会に、リスクの再評価を行い、セキュリティポリシーにおいて形骸化した項目を見直すと共に、社員等への周知やセキュリティリテラシーの向上を行う |