常に意識しておきたい！

IT-BCP事前対策チェックリスト

No.	項目	内容	☑
1	運営体制	危機的事象が発生した時の役割分担が組織内で共有されているか？ （例：業務継続対応者、情報セキュリティインシデント対応者の分担）	
2		危機的事象が勤務時間中に起こった場合、勤務時間外に起こった場合それぞれについて、①従業員、②システム保守会社、③顧問先企業への連絡体制、連絡手段を整備しているか?	
3		経営者、業務継続対応者、情報セキュリティインシデント対応者、システム担当者が参集できない場合の代替要員や各情報システムの緊急マニュアルを整備しているか?	
4	情報資産の確認	事務所が保有している情報資産の棚卸し及び当該情報資産の価値（＝危機的事象によって被る被害総額の概算）を認識しているか？	
5	優先業務・情報システム	危機的事象が発生した時に何の業務を優先するべきかを決めているか？ （優先業務：　　）	
6		優先業務に必要な情報システムは何か？ （必要な情報システム：　　）	
7		優先業務に必要となる情報システムを継続・復旧するための対策を立てているか？ （例：バックアップへの切替、代替サービスの確保、紙申請、手作業） （対策：　　）	
8	予防対策	基本的な情報セキュリティ対策を実施できているか？ 参考：IPA『5分でできる！情報セキュリティ自社診断』 https://www.ipa.go.jp/security/guide/sme/5minutes.html	
9		データのコピー又はバックアップをとっているか？ （方法：　　）	
10		ログを取得しているか？	
11		事務所で使用している情報システムごとに、故障や停止時の対応策を検討しているか？	
12		特定個人情報及び個人情報について適切な保護措置を講ずる体制を整備しているか？（例：SRPⅡ認証の取得等）	
13		事務所で作業が困難になった場合に備えて、リモートワーク体制を整備しているか？	
14		情報システムの盗難・損傷・破壊・消失を防止するための耐災害対策は行っているか？（例：施錠保管、転倒防止、消火設備）	
15		サイバーリスク補償に関する保険の必要性を理解しているか？	
16		危機的事象発生時の対応についての教育・訓練を実施しているか？	
17	顧問先企業との取り決め	顧問先企業と緊急時の取扱いを決めているか？（例：緊急時には前月と同じ条件で給与計算をする等）	