



長期休暇に伴う社内体制の整備

長期休暇中のサイバー攻撃・自然災害に備えて準備をしましょう

BCP対策できていますか？

会社の大切な情報を守るため、従業員の安全確認のために
長期休暇前に今一度確認しておきましょう！

※**Business Continuity Plan** = 事業継続計画



セキュリティ対策

チェックしてみましょう！！



休暇前

- ☐ 緊急連絡体制が定められている
- ☐ 重要データのバックアップができています
- ☐ 使用しない機器が電源OFFになってる

休暇後

- ☐ 修正プログラムの適応、定義ファイル更新ができています
- ☐ 各種ログの確認ができています
- ☐ 不審なメールに注意することを徹底している

<https://www.ipa.go.jp/security/anshin/measures/vacation.html>



安否確認

チェックしてみましょう！！



- ☐ 安否確認システムが導入されている
- ☐ 緊急連絡網の整備と定期的な更新がされている
- ☐ 避難経路・避難場所など災害時の行動マニュアルが周知されている

チェックが入らなかった項目は裏面で詳細を確認しましょう →

長期休暇に入る前に 社内で必要な対策とは

長期休暇時は様々な脅威や問題が発生しやすいです。
特に長期休暇時のサイバー攻撃や、休暇中の災害に備えて
今の段階から対策しましょう。



必要なBCP対策とは



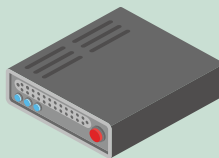
1. 社内ルール策定

- ・インシデント、災害時の発生時の連絡先策定。
IT機器持ち出し時のルール周知



2. セキュリティ対策

- ・休暇中も外部からの攻撃を防ぐ
・アクセス制限で情報漏洩防止



3. クラウドバックアップ

- ・社内データを自動でバックアップ
・遠隔地バックアップで災害時の復旧を迅速に



4. グループウェア

- ・災害時の安否確認が迅速に確認可能に
・モバイル対応で外出先から、情報共有へ



長期休暇前だからこそ、セキュリティと情報共有の見直しを！

万が一のトラブルに備えた対策にまよったら・・・

是非ご相談ください！

注意喚起
ルール徹底



サイバー攻撃
ランサムウェア？

オンラインでの
ご相談も承っております！

当社にご相談ください！