

長期休暇における情報セキュリティ対策 ～システム利用者向け～



社内の情報セキュリティのルールをしっかり
守ってインシデントが起こらないように注意
してほしいニャ



ウイルスに感染したかも、情報漏えいしたかも
と思ったら、上司やシステム管理者等にすぐに
連絡してください！

長期休暇前の対策

- ☐ **機器やデータの持ち出しルールの確認と遵守**
長期休暇に社外での対応が必要となるパソコン等の機器やデータ等の情報を持ち出す場合は、持ち出しルールを事前に確認し遵守してください。
- ☐ **使用しない機器の電源OFF**
長期休暇中に使用しない機器は電源をOFFにしてください。

長期休暇中の対策

- ☐ **持ち出した機器やデータの厳重な管理**
自宅等に持ち出したパソコン等の機器やデータは、ウイルス感染や紛失、盗難等によって情報漏えい等の被害が発生しないよう、厳重に管理してください。

長期休暇明けの対策

- ☐ **修正プログラムの適用**
長期休暇中に公開された各種ソフトウェアの修正プログラムを、システム管理者の指示に従ってインストールしてください。
- ☐ **定義ファイルの更新**
電子メールの送受信やウェブサイトの閲覧等を行う前に、長期休暇中に公開されたセキュリティソフトの定義ファイル（パターンファイル）を更新して、最新の状態にしてください。
- ☐ **持ち出した機器等のウイルスチェック**
組織内で利用する前にセキュリティソフトでウイルススキャンを行ってください。
- ☐ **不審なメールに注意**
不審なメールを受信していた場合、「添付ファイルは開かず」、「本文中のURLにはアクセスせず」、各組織のシステム管理者に報告し、指示に従ってください。