愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R7-34号
個人向け
組織向け

年末年始の長期休暇に向けた
情報セキュリティ対策をしましょう!!

愛知県警察 サイバー犯罪対策課 サイバー犯罪対策通信 第R7-7号 組織向け

長期休暇における情報セキュリティ対策 ～経営者＆システム管理者向け～

長期休暇中は、いつもと違う状況となり、会社でセキュリティインシデントが発生したときに、対応が遅れたり、思わぬ被害が発生するおそれがあるニャ！しっかり対策をとるニャ

長期休暇前の対策

- □ **緊急連絡体制の確認**
  不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認してください。
- □ **社内ネットワークへの機器接続ルールの確認と遵守**
  長期休暇中にメンテナンス作業などで社内ネットワークへ機器を接続する予定がある場合は、社内の機器接続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サーバ等の機器は電源をOFFにしてください。

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OS（オペレーティングシステム）や各種ソフトウェアの修正プログラムが公開されている場合があります。
- □ **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定義ファイルを更新し、最新の状態にしてください。
- □ **サーバ等における各種ログの確認**
  何らかの不審なログが記録されていた場合は、早急に詳細な調査等の対応を行ってください。

もしも被害に遭ってしまったら
最寄りの警察署に通報・相談を！

愛知県警察 サイバー犯罪対策課 サイバー犯罪対策通信 第R7-8号 組織向け

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。

愛知県警察 サイバー犯罪対策課 サイバー犯罪対策通信 第R7-9号 個人向け

長期休暇における情報セキュリティ対策 ～個人向け～

長期休暇中の対策

- □ **行楽等の外出前や外出先でのSNS投稿に注意**
  SNSに書き込んだ内容によっては、長期休暇中に不在であることが知られてしまったり、撮影した写真をSNSに投稿したことでトラブルに発展したりすることがあります。

- □ **偽のセキュリティ警告に注意**
  システムエラーやウイルスに感染している等の偽の警告を表示させ、サポート窓口に電話を促すような画面は『**サポート詐欺**』です。
  電話をかけてしまうとパソコンを遠隔操作され個人情報等を盗まれ、最終的にサポート名目で料金を請求されます。
  もし偽の警告画面が表示された場合は、慌てずまずは身近な家族や友人に相談してください。
  偽の警告画面は、**インターネット閲覧ソフトを強制終了するか、パソコンを再起動すれば消すことができます。**

- □ **メールやSMS（ショートメッセージ）、SNSでの不審なURLに注意**
  来荏の企業などを騙った不審なメールの本文中のURLにアクセスすることでウイルスに感染したり、フィッシングサイトに誘導されたりする可能性があります。
  不審なサイトへ誘導するURLは、SMS（ショートメッセージ）で送られてくる場合や、SNSで投稿されている場合もありますので、被害に遭わないように注意してください。
  フィッシングサイトで情報を入力してまった場合は、**パスワードの変更、カード会社への連絡等**、入力した情報の悪用を防ぐ対応をしてください。

サイバー犯罪対策通信は、X（旧ツイッター）や
愛知県警察ホームページにて公開しています！
サイバー犯罪被害防止対策にぜひご活用ください！

愛知県警察
ホームページ

サイバー犯罪対策課
X（旧ツイッター）