

長期休暇の前後に講ずるべき対策について

長期休暇の時期は、システム担当者や管理者が長期間不在になる場合も多く、サイバーセキュリティのリスクが高まります。

長期休暇の前後に講ずるべき対策をまとめましたので、対応を検討してください。

1. 長期休暇前

○対処手順や連絡体制の確認

休暇中にインシデントが発生した場合に備え、対処手順や連絡体制を再確認しておきましょう。

○バックアップの取得

重要データのバックアップを取得し、必要な場合にはバックアップからの復元が可能なことを確認しておくことが重要です。また、バックアップデータの保管場所についても検討し、ネットワークから切り離れた安全な場所に保存するようにしましょう。

○アクセス制御

アクセス権限が適切か、不要なアカウントがないか確認しましょう。VPN等、外部からアクセス可能な機器の設定も確認しましょう。

○ソフトウェアの脆弱性対策

ソフトウェアのセキュリティパッチ適用やバージョンアップなどを実施し、脆弱性への対策を実施しましょう。休暇中に脆弱性が発表された場合の対応についても決めておきましょう。

○利用機器に関する対策

IT機器のファームウェアを更新し、脆弱性への対策を実施しましょう。休暇中に使用しない機器は、シャットダウンして不正アクセスやマルウェア感染などのリスクを軽減しましょう。

2. 長期休暇後

○メールへの対処

不正なリンクや添付ファイルを含むメールに注意する必要があります。特に、送信元が不審なメールについては開封せず、報告して組織内で情報共有をしましょう。

3. その他

詳細はIPAのホームページをご確認下さい。

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

【本件の問合せ先】

茨城県警察本部サイバー企画課

電話：029-301-0110

長期休暇に向けて、セキュリティ対策は万全ですか？

セキュリティ対策責任者・システム担当者向け

休暇前

対処手順・連絡体制

重要

- 長期休暇期間中の**監視体制**を確認する。
- 必要に応じ、システムアラート等の監視体制を強化する。
- セキュリティインシデントの**対処手順**を確認し、**連絡体制を更新**する。

⚠ 長期休暇期間中に認知したインシデントの対応が休暇明けとなり、被害が拡大した事例も！

休暇前

バックアップ

重要

- 重要なデータや機器設定ファイルに対する**バックアップ対策**を実施する。
- バックアップデータはネットワークから切り離し、変更不可とするなどの対策を検討する。

⚠ ランサムウェア攻撃により、大切なバックアップも暗号化されてしまう被害が出ています！

休暇前

アクセス制御

- アクセス権限の確認、多要素認証の利用、不要なアカウントの削除等により、**本人認証を強化**する。
- 利用者にパスワードが単純でないか確認させる。
- 外部ネットワークからアクセス可能な**機器へのアクセスは必要なものに限定**する。

休暇前

ソフトウェアの脆弱性対策

- 脆弱性対策の状況を確認し、必要に応じて**セキュリティパッチの適用**や**ソフトウェアのバージョンアップ**を行う。
- 長期休暇期間中に公表された重要な脆弱性情報に対応するための体制を整える。

休暇前

利用機器に関する対策

- 機器（サーバ、パソコン等、通信回線装置、特定用途機器（防犯カメラなど）等）の**ファームウェアを最新にアップデート**する。
- 長期休暇期間中に使用しない機器の**電源を落とす**。

休暇後

電源を落としていた機器に関する対応

- 長期休暇期間中に電源を落としていた機器は、端末起動後、**最初に不正プログラム対策ソフトウェア等の定義ファイルを確認**する。
- **最新の状態になっていない場合は、更新**してから、利用を開始する。

休暇後

ソフトウェアの脆弱性対策

- 長期休暇期間中における脆弱性情報を確認し、必要に応じて**セキュリティパッチの適用**や**ソフトウェアのバージョンアップ**を行う。
- 直ちに実施することが困難な場合は、リスク緩和策を講じる。

休暇後

不正プログラム感染の確認

- 長期休暇期間中に持ち出しが行われていたパソコン等が不正プログラムに感染していないか、不正プログラム対策ソフトウェア等で確認する。

休暇後

各種ログの確認

- サーバ等の機器に対する**不審なアクセス**がないか、VPN、ファイアウォール、監視装置等ログやアラートで確認する。
- 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を行う。

情報システム利用職員向け

休暇前

機器やデータの持ち出しルールの確認と遵守

- 端末や外部記録媒体等の持ち出しは、**組織内の安全基準等に則った適切な対応**（持ち出し・持ち込みに関する内規の遵守等）を徹底する。
- 持ち出した機器の**不正プログラム感染や、紛失、盗難による情報漏えい等の被害が発生しないように管理**する。

休暇前

利用機器に関する対策

- 不正アクセスを防止するため、長期休暇期間中に使用しない機器の**電源を落とす**。

休暇後

電子メール

- 電子メールを確認する前に、利用機器のOS・アプリケーションに対する**修正プログラムの適用**や不正プログラム対策ソフトウェア等の**定義ファイルの更新**等を実施する。
- **不審な添付ファイルを開いたり、リンク先にアクセスしたりしない。**
- 不審な点があれば、電子メールを開封する前に、**電話等、別の手段で確認**する。

