

サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和8年
10月14日
Vol.26

△ 情報漏洩防止に向けたセキュリティ対策の徹底 △ 全国的に不正アクセス等による情報漏洩が複数確認されています。

対処手順・連絡体制

重要

- 社内ネットワークの**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。



アクセス制御

重要

- 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。



バックアップ

- 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！

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。
- 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。



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



電源を落としていた機器に関する対応

- 一定期間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。



ソフトウェアの脆弱性対策

- 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。



不正プログラム感染の確認

- 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。



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。



セキュリティ対策責任者・システム担当者向け

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。



利用機器等に関する対策

- 不正アクセスを防止するため、休暇期間中に使用しない機器の**電源を落とす**。
- 不要になった個人情報等は端末等から**削除**する。



情報システム利用職員向け

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。



もしも被害に遭ってしまったら、すぐに警察に通報・相談を！

最寄りの警察署又はサイバー犯罪相談窓口



<https://www.npa.go.jp/bureau/cyber/soudan.html>



愛媛県警察本部サイバー犯罪対策課

TEL 089-934-0110(代) / #9110

