

サイバーセキュリティ パートナーシップだより



令和4年3月2日 山口県警察本部生活環境課

サイバーセキュリティ対策の強化について

報道によると、トヨタ自動車は、自社の取引先企業がコンピュータ・ウイルスに感染した影響でシステム障害が発生したため、国内のすべての工場の稼働を停止したと発表しました。

昨今の社会情勢を踏まえると、サイバー空間における脅威は深刻な情勢にあることから、各企業・団体においてサイバーセキュリティ対策の強化を図るようお願いします。

基本的なセキュリティ対策

ウイルス（マルウェア）感染被害防止

- メールの添付ファイルを不用意に開かない。
- メール文中の URL を不用意にクリックしない。
- 定期的な OS のアップデート、セキュリティ対策ソフトの更新



脆弱性を狙ったサイバー攻撃、Web サイト改ざん被害防止

- 自社内の IoT 機器を含む情報資産の保有状況の確認
- 自社で使用しているインターネットへの接続を制御する VPN 装置やゲートウェイ等の脆弱性を確認し、脆弱性に対応した最新のセキュリティパッチを適用する。

※ 情報処理推進機構（IPA）や JPCERT/CC のホームページにて、機器の脆弱性情報が確認できます。

不正アクセス被害防止

- アカウントのパスワード設定の見直し（単純なものにしない）
- アクセス権限の確認と不要なアカウントの削除（人事異動等により管理されていないアカウントがないか等）

インシデント発生時の適切な対処

※インシデント～情報および制御システムの運用におけるセキュリティ上の問題として捉えられる事象のこと

（例）情報流出、フィッシングサイト、不正侵入、マルウェア感染、Web サイト改ざん、Dos（DDos）攻撃等

- (1) データ消失等に備えたデータのバックアップの実施
- (2) データの復旧手順の確認
- (3) インシデント認知時の対処手順の確認
- (4) インシデント発生時の対外応答や社内連絡体制等の準備（警察への通報）



山口県警察本部サイバー犯罪相談窓口

TEL 083-922-8983

mail cyber.soudan@police.pref.yamaguchi.lg.jp

サイバー犯罪に関する広報資料

山口県警 サイバー防犯

で

検索