栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER

「エッジデバイス」が狙われています!!

サイバー攻撃の攻撃者は、世界中の企業や家庭のエッジデバイスを乗っ取り、それらを束ね、大規模なボットネット（匿名攻撃ネットワーク）を構築し、攻撃の踏み台（通信の経由地）としています。

※　エッジデバイス
　ネットワークに接続するときに末端に設置することで、内部と外部をつなぐ役割を果たす機器（デバイス）

2026年４月、英国が作成した国際アドバイザリー（日本も参加）は、中国の情報セキュリティ企業によって構築されたボットネット「RaptorTrain」が中国に関連するサイバー攻撃に利用されていることを公表しました。

同アドバイザリーでは、すべての組織が取り組むべき最初の防御策として、「エッジデバイスの把握」を挙げています。

※　国際アドバイザリー
　国家機関や国際機関が連携し、特定のサイバー攻撃に関する技術的な分析結果や防御策などをまとめた共同文書

①「エッジデバイスの把握」が対策の第一歩

自社のネットワークの境界に接続されている機器（エッジデバイス）をもれなく把握することが対策の第一歩となります。

【エッジデバイスの例】
　ネットワーク機器：ルーター、VPNゲートウェイ等
　IoT機器：ウェブカメラ、ビデオレコーダー、NAS等

②「エッジデバイスの状態」も把握しましょう

次に、企業において存在するエッジデバイスがどのような状態にあるのかを把握しましょう。

- デバイス本体を制御するソフトウェアのバージョンは最新のものか
- 最新のセキュリティパッチが適用されているか
- メーカーのサポートが終了し、脆弱性が放置されていないか
- パスワードが初期設定のままになっていないか等

あなたの機器がサイバー攻撃の「隠れ蓑」に！
まずは「エッジデバイス」の把握から！