amnimo™ | Network Shield

無人の拠点の「見張り役」を、見張る。

機械警備の通報装置、防犯カメラ、録画機。夜も休日も動き続ける機器は、攻撃する側にとっても狙いやすい入口です。

なぜ機械警備・遠隔監視が狙われるのか

- **録画機とカメラは IoT ボットの一番の標的**: Mirai などのボットは、録画機やカメラの初期のパスワードと古い弱点を狙って、世界中で感染を広げています
- **映像の入口を開けたまま**: スマートフォンから映像を見るために、録画機やカメラの入口をポート転送で外に公開している例があります
- **無人で、気づくのが遅い**: 拠点に人がいない時間が長く、乗っ取られても、映像が見られなくなるまで誰も気づきません
- **警備センターとつながっている**: 拠点の回線は、VPN で警備センターや管理の仕組みにつながっていることが多い

起こりうること

起こりうること	被害	amnimo Network Shield でできること
映像の覗き見・流出	店舗やオフィスの中の映像が、外から見られる・持ち出される	録画機・カメラの入口（RTSP など）を外に公開していたら、画面で警告する。入口への総当たりや弱点を突く通信を見つけて止める
録画機・カメラのボット化	他社への攻撃や犯罪の中継に使われ、回線が遅くなる・止められる。従量課金なら通信費が急増	ボットの指令役との通信を見つけて止める（AR10・AR20 の小さい構成でも残す）。外向きの通信量が急に増えたら知らせる
警備センターへの侵入	拠点を足場に、VPN を通って警備センターや管理の仕組みへ	VPN の回線も見張りの対象に選べる（インターフェースとして見える VPN。導入のときにご相談ください）
見張りの空白	回線や機器の異常で、知らないうちに監視が止まる	見張りが止まった、通信を受け取れなくなった、といった異常も通知する

警備の現場に合わせた作り

- **止まっても通信は止めない**: 見張りの仕組みに何かあっても、通報や映像の通信は通し続けます
- **今の amnimo ルーターに入れるだけ**: 拠点に行かずに入れられます。無償でお使いいただけます
- **センターでまとめて受け取る**: 拠点ごとの検知を、センターの Slack・Teams・メールに集められます

amnimo Network Shield だけでは防げないこと

- 録画機やカメラのパスワードの変更と、ファームウェアの更新は、機器の側で行ってください。amnimo Network Shield は、それを補う見張り役です
- 暗号化された通信の中身は検査しません。通報装置の電源や回線を物理的に切られることは防げません

注記 ・記載の内容は 2026 年 11 月時点のもので、予告なく変わることがあります ・攻撃のすべてを検知・防止できるものではありません ・記載の会社名・製品名は、各社の商標または登録商標です

アムニモ株式会社 お問い合わせ https://support.amnimo.com/hc/ja/requests/new

©2026 amnimo Inc.