amnimo™ | Network Shield

デジタルサイネージの画面を、乗っ取らせない。

「広告を受け取って映すだけだから、セキュリティは要らない」。そう思われがちなサイネージこそ、狙われやすい入口です。

なぜサイネージが狙われるのか

- **インターネットから丸見え**: 費用を抑えるため、閉じた網ではなく、グローバル IP の付く一般の SIM を使うことが多い。世界中からの総当たりやポートの調査に、いつもさらされます
- **STB は更新されない**:「一度置いたら壊れるまでそのまま」になりがち。数年前の弱点（CVE）が残ったままの OS や遠隔操作のソフトが動いています
- **管理用の入口を開けたまま**: 保守のために、STB の遠隔操作（VNC など）をポート転送で外に公開している例があります
- **数が多く、見る人がいない**: 数百〜数千台が全国に散らばり、夜は誰も画面を見ていません

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
画面の乗っ取り	深夜、全国の店舗の画面に不適切な映像や偽の避難指示。SNS で一気に広まり、広告主と店舗のブランドが傷つく	STB の弱点を突く通信と、遠隔操作の入口への総当たりを見つけて止める。遠隔操作の入口を外に公開していたら、画面で警告する
ボット化と通信費の急増	Mirai などに感染し、他社への攻撃や犯罪の中継に使われる。従量課金の回線で高額の請求、回線の停止	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）。危険な行き先をふさぐ。外向きの通信量が急に増えたら知らせる
カメラの映像の流出	視聴者の属性を見るカメラの生の映像が、外へ送られる	カメラの映像（RTSP）の入口を外に公開していたら警告する。中の端末から危険な相手への通信を見つける
本社・配信の仕組みへの侵入	サイネージを足場に、VPN を通って配信サーバーや本社のネットワークへ	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）

1 台ずつ見に行かずに済む

- **今の amnimo ルーターに入れるだけ**: 箱も工事も要りません。無償でお使いいただけます
- **通知は 1 か所に**: 全国の機器の検知と遮断が、本部の Slack・Teams・メールに届きます。数千台あっても、見るのは 1 つのチャネル
- **慌てなくてよい**: 攻撃が今の設定で中まで届いたかを機器が判定するので、届いていない攻撃で夜中に呼び出されません

amnimo Network Shield だけでは防げないこと

- 配信の仕組み（CMS）そのものが乗っ取られ、正規の配信経路で不適切なコンテンツが送られた場合は、通常の配信と見分けられません。CMS のアカウントの多要素認証、配信の承認の手順と組み合わせてください
- 暗号化された通信の中身は検査しません。筐体を開けて USB 機器を挿すなどの物理的な攻撃は、筐体の鍵や設置場所の管理で防いでください

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.