ASTIRA®

Panasonic IoT Threat Intelligence

蓄積される膨大な 「脅威インテリジェンス」を製品セキュリティ対策へ活用

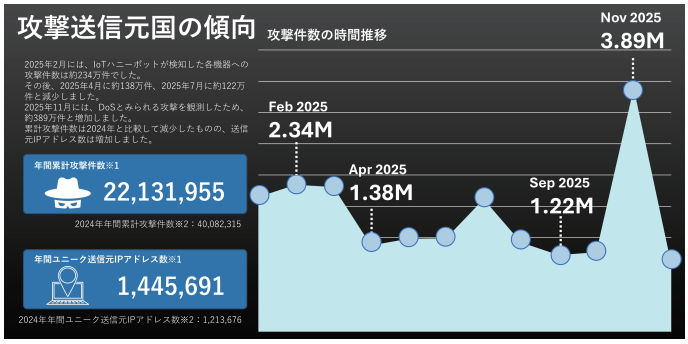
IoT 製品に対する世界中からの膨大なサイバー攻撃やマルウェア検体を収集・分析しています。
日々蓄積される「脅威インテリジェンス」をパナソニックの製品セキュリティ対策へフィードバックすることで、製品ライフサイクル全体でのセキュリティ対策を強化しています。

IoT製品へのサイバー攻撃を分析して対策に活用

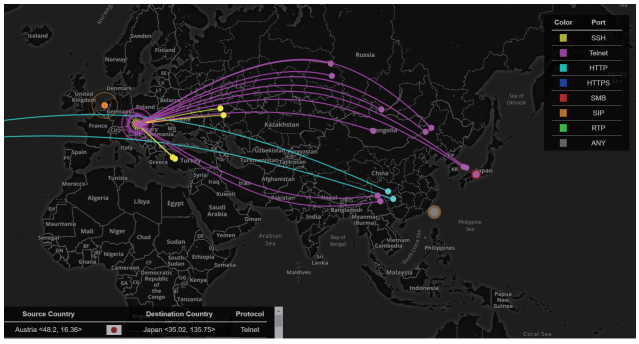
IoT 製品がサイバー攻撃を受けると、お客様が製品を利用できなくなるだけではなく、踏み台や DDoS などの攻撃に悪用されることがあります。

サイバー攻撃の手口は常に進化しており、開発段階では想定・検出できなかった脆弱性が出荷後に明らかになり、攻撃に利用されるリスクがあります。

パナソニックでは、世界中からのサイバー攻撃の動向を収集・分析する ASTIRA® を運用し、得られた「脅威インテリジェンス」を製品セキュリティ対策の強化に役立てています。



攻撃傾向を分析・活用（2025 年事例）



リアルタイムで攻撃情報を収集

IoT 製品におけるセキュリティ対策のベストプラクティスを国際会議で発信

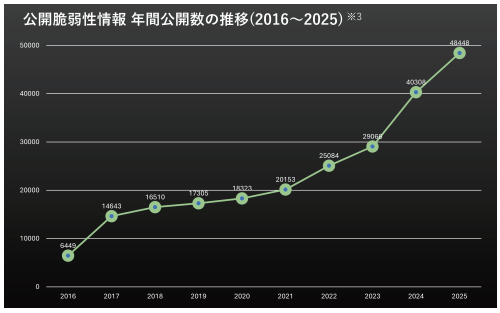
パナソニックでは業界に先駆けて PSIRT※1 を構築・運用してきた知見と、ASTIRA® で得られた最新のサイバー攻撃の傾向から、IoT 製品におけるセキュリティ対策のベストプラクティスを国際会議を通じて広く発信し、業界全体のセキュリティ向上に努めています。

Black Hat	CODE BLUE	その他の国際会議
世界最大規模セキュリティカンファレンス 2019（Europe）/ 2023(USA)	日本最大規模セキュリティカンファレンス 2019 / 2023 / 2024 / 2025	HITCON / FIRST Annual Conference、など

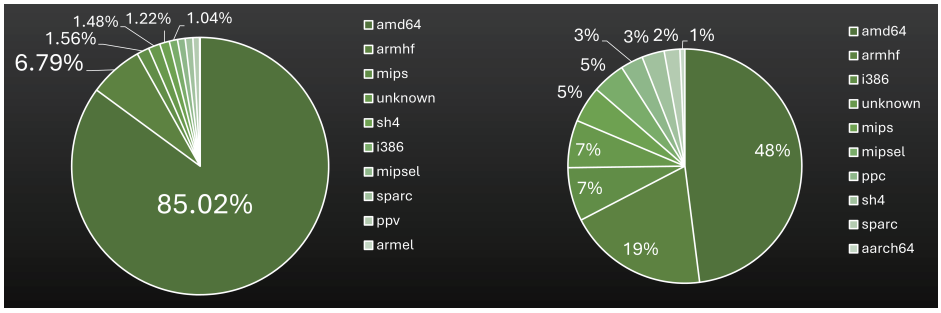
※1 Product Security Incident Response Team

攻撃者の狙いの変化を分析し、能動的に製品セキュリティ施策へ反映

継続的にサイバー攻撃をモニタリングすることで、攻撃者がよく利用する脆弱性や、攻撃テクニックの変化を捉えることができ、製品セキュリティ検査の項目拡充など、能動的な製品セキュリティ対策に生かすことができます。



脆弱性の公開数（年次）



マルウェアが狙う CPU アーキテクチャの変化
（2024/2025 年の比較 ）

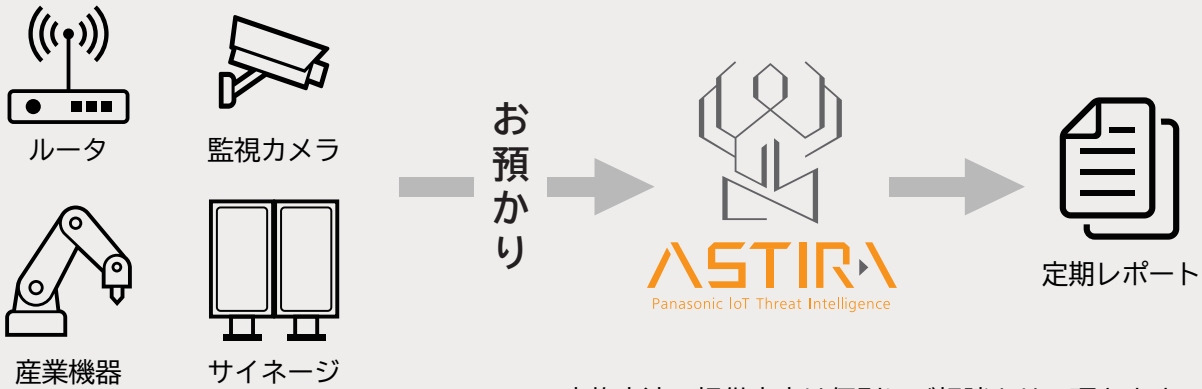
ASTIRA® を御社製品のモニタリングに活用しませんか？

欧州 CRA（Cyber Resilience Act）に代表される各国法規制により、
IoT 製品に求める製品セキュリティ対策の要求レベルは向上してきています。

製品ライフサイクル全体にわたってセキュリティレベルを維持するためには、製品に対する継続的なモニタリングが重要です。御社製品を ASTIRA® へ接続することで初期費用を抑えてモニタリングを開始することが可能です。

IoT 製品へのサイバー攻撃モニタリングを通じた、製品セキュリティ対策の強化に関心がございましたらお気軽にご相談ください。

サービスイメージ



（接続機器の一例）

実施方法、提供内容は個別にご相談させて頂きます。
PoC も実施しておりますのでお気軽にご相談ください。

[お問合せ先]
パナソニック ホールディングス株式会社
製品セキュリティセンター製品セキュリティグローバル戦略部
Email: astira@ml.jp.panasonic.com

- 記載されている内容は 2026 年 5 月現在のものです。
  予告なしに変更する場合もございますので予めご了承ください。
- 本サービスは法人のお客様を対象としています。個人のお客様は対象外とさせて頂きます。