2026年11月10日
株式会社ソラコム

「IoT・フィジカル AI システム　セキュリティ診断・堅牢化サービス」を提供開始

脆弱性の「発見」から、対策の「実装・再検証」まで提供

株式会社ソラコム（本社：東京都港区、代表取締役社長 CEO 玉川 憲）は、IoT やフィジカル AI をはじめ、ネットワークにつながるシステムを対象とした「IoT・フィジカル AI システム　セキュリティ診断・堅牢化サービス」を、2026 年 11 月 10 日より提供開始します。本サービスは、システムの脆弱性を診断し、リスクの発見から対策の設計・実装・再検証までを支援するものです。



近年、Web サービスやクラウドを狙ったサイバー攻撃の脅威は情報漏洩にとどまらず、現実世界の機器・設備にまで及ぶリスクが現実のものとなっています。IoT やフィジカル AI の普及に伴い、デバイス、通信経路、クラウド、アプリケーションのいずれか一箇所の弱点が、設備の誤動作や停止を引き起こす場合もあります。システムの安全性確保には、これらの多様な技術構成要素に、一貫したセキュリティポリシーの適用が求められます。そのためには、従来のセキュリティ診断で対象となる個別要素の評価に加え、要素間の接続点や連携まで含めてシステム全体を評価することが不可欠です。

本サービスは、ソラコムが AI/IoT 通信プラットフォーム SORACOM をグローバルに提供し、さまざまな分野のユースケースから培ってきた、セキュリティを考慮した設計・運用のノウハウを活かしています。ソラコムが定めるリスクポイントに基づき、AI エージェントも活用して、効率的な診断が可能です。診断で検出したリスクに応じて、ネットワークの閉域化、通信の制限・フィルタリング、通信経路の暗号化、認証の強化など、具体的な対策の設計から実装までを支援します。

さらに、SORACOM をご利用の IoT システムでは、デバイス側とクラウド側の通信経路上に位置する SORACOM プラットフォームを「対策の実施点」として活用し、書面による合意に基づき、それぞれとの連携設定を診断するとともに、必要な対策の実装までを支援します。また、将来的なシステム構成の見直しや、SIM/eSIM を活用した認証・鍵交換の仕組みの導入にも対応します。

製造、物流、エネルギー、インフラ、ビルなどで IoT システムを運用する企業や、ロボット・フィジカル AI など現実世界で動作するシステムを開発・導入する企業、IoT 製品・サービスを提供する事業者を対象としています。SORACOM のご利用有無を問わず、システムの一部分のみといった場合も、お問い合わせいただけます。

本サービスは、同日に発表した「SORACOM フィジカル AI Suite」を構成するサービスのひとつです。SORACOM の各サービスについては、当該プレスリリースをご参照ください。

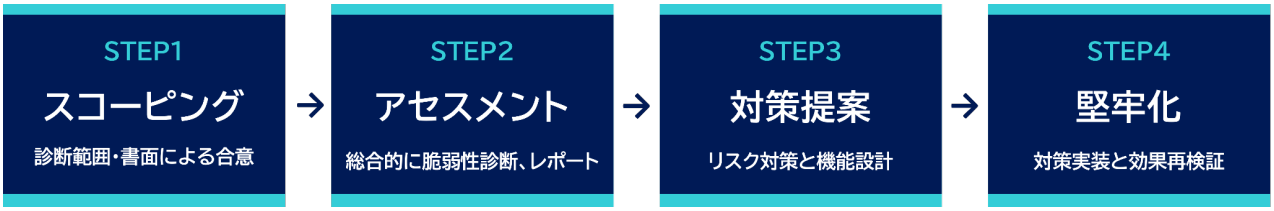
ソラコムは、セキュリティを「後から付け足すもの」ではなく、IoT・フィジカル AI の設計・運用の前提と位置づけています。本サービスを通じて、診断から実装まで伴走し、安心して IoT・フィジカル AI を活用できる社会の実現に貢献します。

IoT・フィジカル AI システム　セキュリティ診断・堅牢化サービス

提供開始日
2026 年 11 月 10 日

サービスの特徴

- **エンドツーエンドの一体診断**：デバイス・通信経路・クラウドを一体で診断し、個々の機器やシステムだけでなく、それらの接続点に潜むリスクまで幅広く評価
- **診断から実装までのワンストップ対応**：対策の設計・実装・再検証までを担い、対応の停滞を防止
- **ネットワーク層での即時対策**：大幅な構成変更を伴わずに、ネットワークの閉域化、通信先の制限・フィルタリング、対象システムの通信状態のモニタリングとレポーティングを適用
- **将来を見据えたリアーキテクティングの提案と実施支援**：SIM/eSIM などのハードウェア認証モジュールを用いた認証・鍵交換の導入や、通信経路の暗号化などを支援



脆弱性の診断から対策の実装・再検証まで、4 つのステップで支援します。

STEP 1｜スコーピング
診断対象・手法・実施ルールを事前に確認・合意したうえで診断を開始します。

STEP 2｜アセスメント（診断）
役割の異なる複数の AI エージェントのチームが連携し、サーバー・デバイス・通信経路に対して包括的な脆弱性診断（ペネトレーションテスト：攻撃者の視点で侵入を試み、弱点を探すテストを含む）を実施します。診断結果は技術レポートとして提出します。

STEP 3｜対策提案
検出されたリスクに対して、ミドルウェアの導入や必要なコンポーネントの開発・運用も視野に入れた対策を提案します。SORACOM のプラットフォーム機能を活用した対策についても設計します。

STEP 4｜堅牢化
提案した対策に基づいて設定変更や構成の実装を行い、対策の効果を再検証します。

診断例

- **IoT・エッジデバイス診断**

  インターネットに接続されて稼働する IoT 機器やロボット端末を対象に、疑似的な攻撃により安全性を診断します。エンドポイントへのペネトレーションテストをはじめ、ハードウェア・OS レイヤーのファイアウォール設定、鍵交換方式、通信プロトコルの安全性、機器内における認証情報の保管状態などを多角的に診断し、乗っ取りや不正利用の脅威に備えます。

- **ネットワーク・通信経路診断**

  デバイスからクラウドに至る通信経路を対象に、インターネット側からの到達性、暗号化強度の不足、SIM の不正持ち出し・流用リスク（IMEI ロックの設定状況など）、想定外の宛先への通信の有無などを総合的に診断します。SORACOM をご利用の環境では、コンソール上のセキュリティ設定や通信状態（通信先・通信量・頻度など）の確認に加え、単発の診断にとどまらない継続的な通信モニタリング・異常検知基盤の構築までを支援します。

- **サーバー・Web アプリケーション診断**

  Web サービス、クラウド環境、サーバーを対象に、包括的な脆弱性診断（ペネトレーションテストを含む）により、外部から悪用可能な脆弱性を幅広く検出して、不正アクセスや情報漏洩につながるリスクを未然に防ぎます。

詳細・お問い合わせ

- ご利用料金は、ご利用内容に応じて個別にお見積もりします。
-
- お申し込みは、お問い合わせページからご連絡ください。
- https://soracom.jp/iot-physical-ai-security_services/

参考

IoT・フィジカル AI システムにおける想定リスクと SORACOM による対策例:

想定されるリスク	推奨される対策
① 外部からの不正アクセス・攻撃	閉域網によるインターネットからの直接アクセスの隔離
② 許可されていない外部宛先への通信	通信先・ポートの制限および IP 固定化
③ SIM 盗難・他端末での不正流用	特定端末以外からの通信ブロック
④ 認証情報(鍵・証明書)の漏洩	端末への鍵保存を行わない安全な配布・更新
⑤ 信頼できないネットワークでの盗聴・改ざん	Wi-Fi 等を経由する通信の暗号化
⑥ マルウェア感染等による不審な通信の発生	異常検知時の即時通信遮断
⑦ 保守用のアクセスポイントへの攻撃	送信元を限定したアクセス
⑧ 平文による通信の傍受	インターネット経路へ出る前に暗号化

ソラコムについて

AI/IoT 通信プラットフォーム SORACOM は、世界 200 以上の国と地域でつながる IoT 通信を軸に、IoT を活用するために必要となるアプリケーションやデバイスなどをワンストップで提供しています。製造、エネルギー、決済などの産業 DX から、イノベーティブなスタートアップ、農業や防災など持続可能な地域社会を支える取り組みに至るまで、さまざまな業界・規模のお客様にご活用いただいています。

ソラコムコーポレートサイト https://soracom.com

ソラコムの IR サイトでは、決算情報・IR 資料など、株主・投資家様向け情報を掲載しています。
公式 IR サイト・ニュースレター
・IR サイト
https://soracom.com/ja/ir
・IR ニュースレター登録
https://soracom.com/ja/ir/newsletter
・IR データ(AI 向け) 利用ガイド
https://soracom.com/ir-data/ai/ir data book latest README.md
・IR データ(AI 向け) CSV
https://soracom.com/ir-data/ai/ir data book latest.csv

関連レポート・公式 SNS
・シェアードリサーチレポート
https://sharedresearch.jp/ja/companies/147A
・ソラコム IR 公式 note
https://note.com/soracom_ir
・ソラコム IR 公式 X
https://x.com/SORACOM_IR

本ニュースに関するお問い合わせ

株式会社ソラコム　広報　田渕

pr@soracom.jp