2026年7月7日
株式会社ソラコム

# IoTシステムのネットワークセキュリティを強化する「VPGトラフィックフィルタリング」機能の提供開始

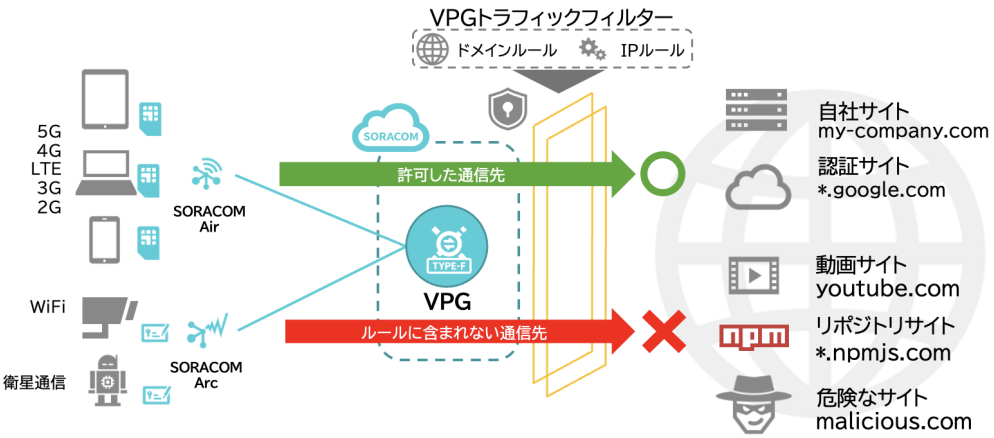
## VPGを利用するIoTデバイスの通信先を、IPアドレス・ドメイン名・ポート・プロトコル単位できめ細かく制御

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プラットフォーム「SORACOM」において、Virtual Private Gateway（VPG）の付加価値サービスとして、ネットワークセキュリティを強化する「VPGトラフィックフィルタリング」機能を2026年7月7日より提供開始します。

IoTによって、あらゆるモノがネットワークにつながり、現実世界をデータとして扱えるようになりました。さらに、デバイスが周囲を認識し、クラウドやサーバーと連携して動作するフィジカルAIの時代に向けて、つながるモノの数と通信の重要度はますます高まっています。

特に、製造業、金融業、警備業など高いセキュリティ要件が求められる業界では、規制やガイドラインの強化を背景に、製品やネットワークのセキュリティを強化する動きが広がっています。「VPGトラフィックフィルタリング」機能は、こうした業界が求めるネットワークレベルのセキュリティ強化を支援します。

ソラコムはこれまでも、認証、暗号化、アクセス制御など複数のレイヤーでセキュリティに取り組んでいます。ネットワークセキュリティの中核を担うのが、閉域網接続です。VPGは、SORACOMプラットフォーム上に構築されるお客さま専用のネットワークゲートウェイであり、許可しないアクセス先のフィルタリングやお客さまネットワークとのプライベート接続を、お客さま自身で設定できます。VPGにより、サーバーからデバイス、デバイス間の通信が可能となるサービスも利用でき、双方向でのセキュリティを実現してきました。



「VPGトラフィックフィルタリング」機能は、SORACOMプラットフォーム上のファイアウォール機能です。お客さまがSORACOM Air for セルラーとSORACOM Arcを利用するIoTデバイスからの通信を、カスタム定義された条件に基づいて柔軟に制御できるようにします。宛先IPアドレス、ポート番号、プロトコル、ドメイン名を組み合わせた条件に基づいて、デバイスからのアウトバウンドトラフィックをきめ細かくフィルタリングできるため、IoTシステム全体のセキュリティを一元的に管理できます。許可リスト方式により、信頼できる宛先のみへの通信を許可し、それ以外の意図しない通信を遮断することで、デバイスが万が一マルウェアに感染した場合でも被害の拡大を最小限に抑えられます。

想定されるユースケースとしては、センサーや機器から収集したIoTデータを、特定のエントリポイントに送信するケースや、IT統制や情報セキュリティルール、業界標準や各種規制への対応で通信先を許可された送信先のみに厳密に制限するケースがあげられます。また、運用中のIoTデバイスが万が一悪意を持って書き換えられてしまった場合は、意図しない通信先へデータ送信を命令されても、データ送信を防ぐことができます。

これらの設定はSORACOMユーザーコンソールから直感的に行えるほか、SORACOM APIを利用したプログラマブルな変更にも対応します。

「VPGトラフィックフィルタリング」機能は、VPG Type-F、Type-F2、Type-Gに対応します。ご利用には別途お申し込みが必要です。

ソラコムは「IoTテクノロジーの民主化」を掲げ、IoTを軸に最新技術をより使いやすく提供することで、多くの活用事例とイノベーションの創出を目指してまいります。

## VPGトラフィックフィルタリング機能の詳細

提供開始日

2026年7月7日

サービス概要

VPGを利用するSORACOM Air for セルラー、SORACOM Arcが直接アクセスできる宛先を、宛先IPアドレス、ポート番号、プロトコル、ドメイン名（FQDN）の条件で制御できる、クラウドベースのファイアウォール機能です。

**2つのフィルタリング方式**

- **IPフィルタリング（IPルール）**：デバイスからの送信トラフィックを、宛先IPアドレス、プロトコル、ポート番号に基づいて許可（allow）／拒否（deny）します。
- **FQDNフィルタリング（ドメインルール）**：デバイスからのアウトバウンドトラフィックを、宛先FQDN、プロトコル、ポート番号に基づいて制御します。ドメイン名指定にはワイルドカードによるパターンマッチング（例：*.example.com）をサポートします。

ご利用イメージ


## 主な利点

- **セキュリティ強化**：許可リスト方式により不要な通信を遮断し、信頼できる宛先のみを許可。プロトコルおよびポートレベルできめ細かく制御
- **コスト最適化**：予期しない、または許可されていない通信を事前に遮断し、データ使用量を削減。グループベースの設定により、多数のデバイスを効率的に管理
- **コンプライアンスサポート**：業界の規制およびセキュリティポリシーに準拠したネットワーク制御を実装

## 想定されるユースケース

- **IoTデバイスの通信制限**：センサーデバイスが特定のクラウドサーバーとのみ通信するよう制限し、その他すべてを拒否することで、デバイス侵害時の被害を最小限に抑制
- **地域別アクセス制限**：特定の地域のサーバーIPレンジのみを許可することで、データ主権要件への対応や、特定地域へのデータ送信を禁止する規制への準拠を支援
- **プロトコル制限**：HTTPSのみを許可し、暗号化されていない通信を遮断。平文通信を防ぎ、中間者攻撃のリスクを軽減
- **マルチステージ/マルチテナント環境**：VPGごとに異なるフィルタリング設定を適用。開発環境では緩やかに、本番環境では厳格な許可リスト制御を行う運用も実現

**対応VPGタイプ**

- VPG Type-F、Type-F2、Type-G

**料金**

- ご利用形態や構成により異なります。

**ご利用方法**

- ご利用には別途お申し込みが必要です。以下よりお問い合わせください。
  - https://soracom.jp/contact/

## ソラコムについて

AI/IoT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。
IRサイト https://soracom.com/ja/ir
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
IRニュースレター登録：https://soracom.com/ja/ir/newsletter

## 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
担当：田渕
pr@soracom.jp