

後手に回りがちな IoTセキュリティをどうすべきなのか

株式会社ソラコム

本日のハッシュタグ



#soracom

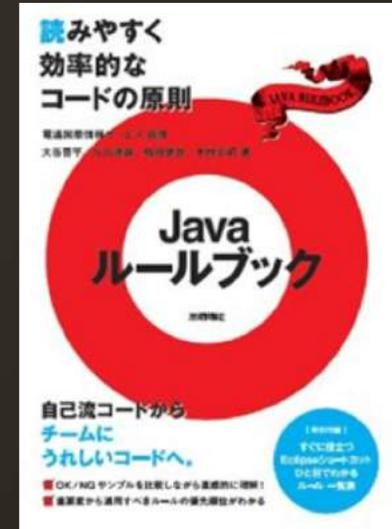
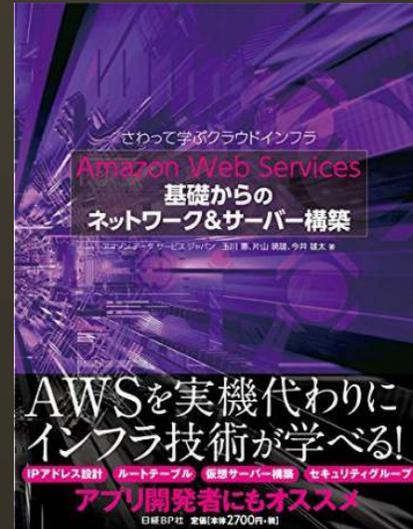
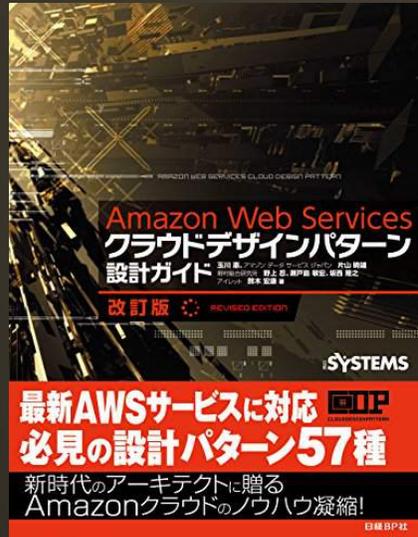


@SORACOM_PR



<https://www.facebook.com/soracom.jp/>

- 名前：片山 暁雄
- 所属：株式会社ソラコム
 - 執行役員
 - プリンシパルソフトウェアエンジニア
- 好きなプログラミング言語：
 - Java



- 名前：福島 拓
- 所属：株式会社ソラコム
 - ソフトウェアエンジニア
 - SORACOM Junctionを担当
- 好きな場所：
 - 海とビーチ



Agenda

- SORACOMの解決するIoTの課題
- IoTセキュリティに必要な機能
 - 閉域網での接続
 - 通信回線の管理
 - 通信の監視・制御
 - デバイスの認証/認可
 - アプリケーションの認証/認可
 - デバイス自体の保護
- まとめ

《 SORACOMが解決する課題 》

IoT (Internet of Things)

モノ

インターネット

クラウド



クラウドにつながるモノは、2020年に
数十億～数百億？

プロトタイピングから実運用までが容易に

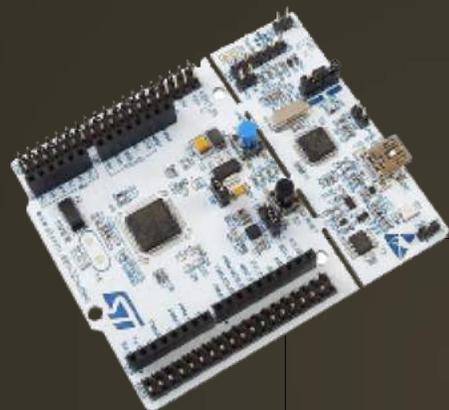


SORACOM
Technology Camp 2018

モノ



Arduino



STM32 Nucleo



Raspberry Pi Zero



ESP-WROOM-02

クラウド



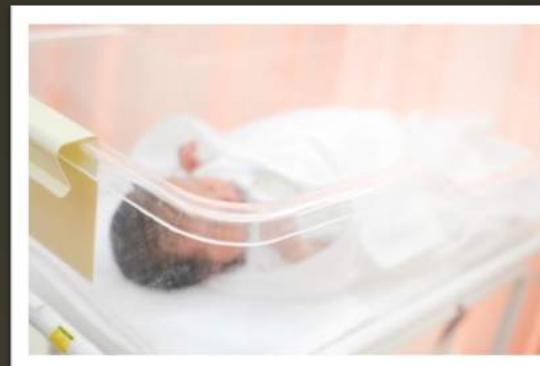
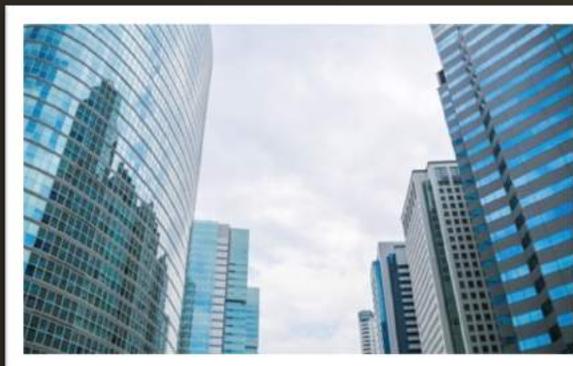
Amazon Web Services



Google Cloud Platform

Microsoft Azure

IoTの活用が期待される分野

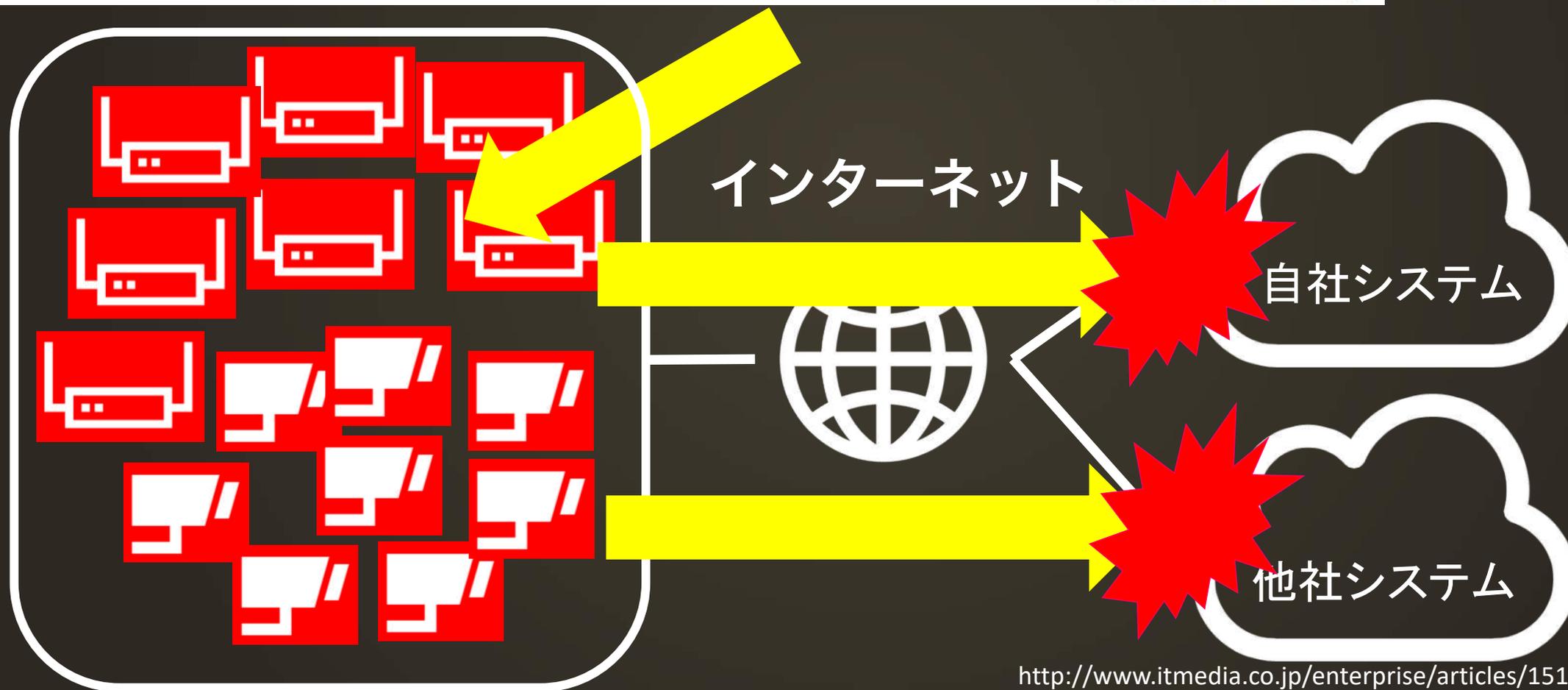


重要なビジネス基盤 / 社会基盤へ

多数メーカーの組み込み機器に同一の秘密鍵、盗聴攻撃の恐れ

影響を受ける製品はルータやIPカメラ、VOIP電話など多岐にわたる。HTTPS通信に割り込む中間者攻撃を仕掛けられて情報が流出する恐れもある。

[鈴木聖子, ITmedia]



モノ

インターネット

クラウド



セキュリティ
通信の管理

ソラコムでの解決策

モノ

インターネット

クラウド





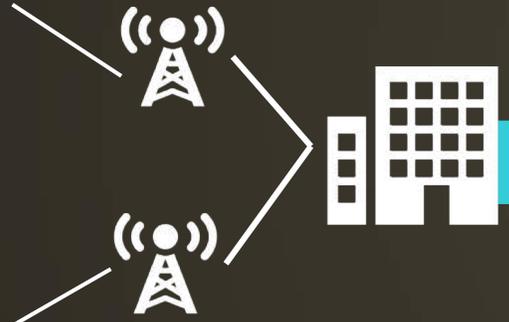
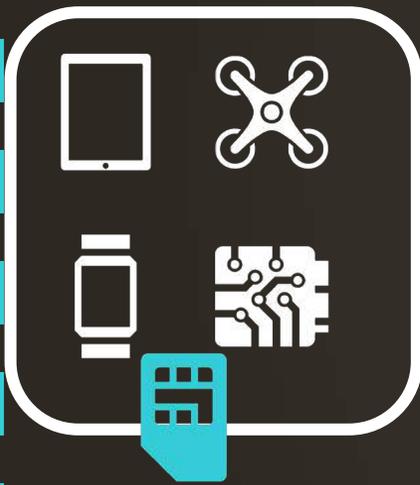
モノ

モバイルキャリア
の基地局

AWS
クラウド

インターネット

SORACOM



3G/LTE

専用線



パケット交換
帯域制御
顧客管理
課金

API

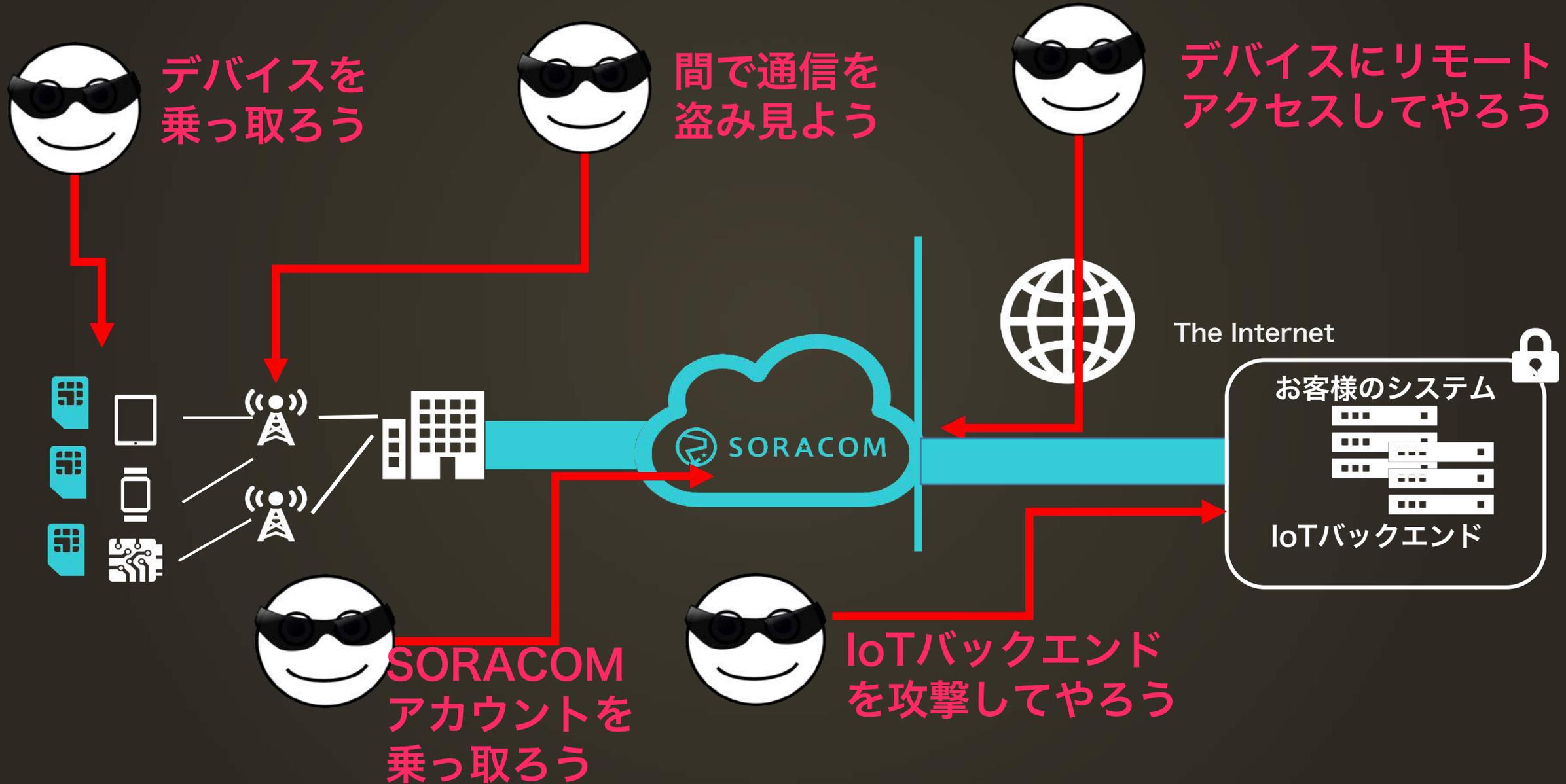
SORACOM Air
SIMカード

クラウドに直結する、 セキュアでプログラム制御可能な 通信を提供



《 IoTセキュリティに必要な機能 》

狙われるIoTシステム



ポイント

- 設計時からセキュリティについて考える
 - デバイス/サーバを必要以上にさらさない
 - なるべくデバイスにデータを置かない
- 費用対効果の観点も必要
- SORACOMにビルトインされた機能を使う

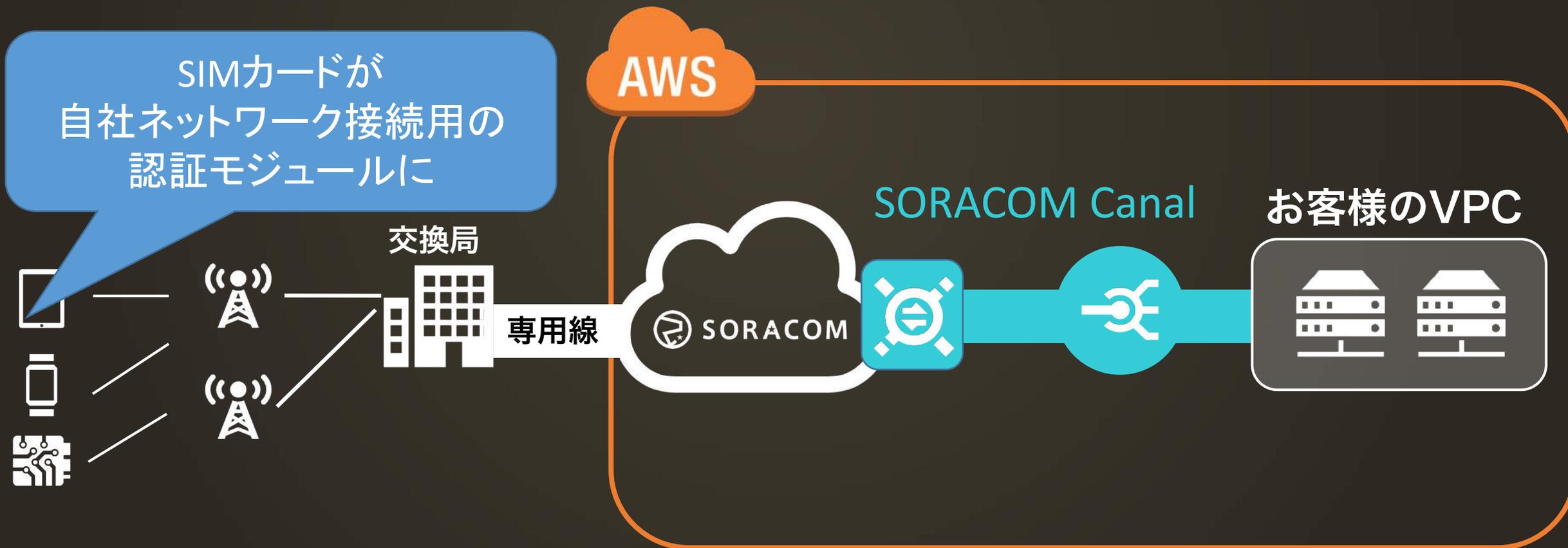


《 閉域網での接続 》

SORACOM Canal - AWS 閉域網接続

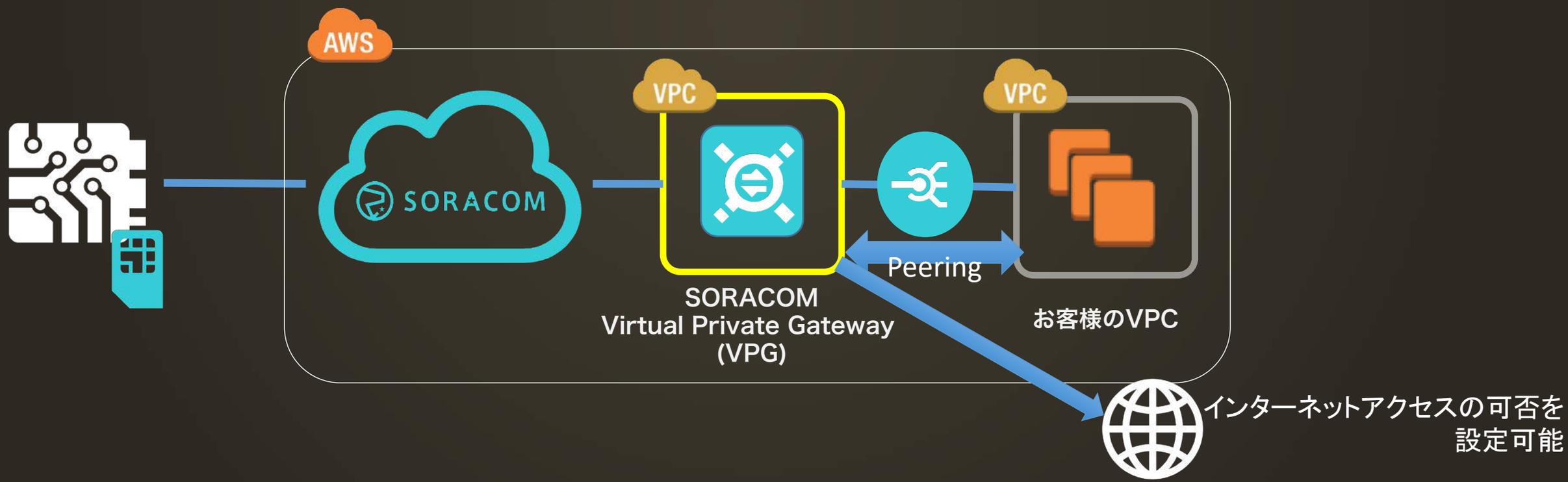
SORACOM の VPC とお客様の VPC との間でプライベート接続
インターネットを介さず、セキュアにデータ通信 -> 詳細はA5

※ VPC: Virtual Private Cloud = AWS の中でプライベートネットワークをつくるための仕組み



SORACOM Canalによる接続詳細

- SORACOM Virtual Private Gateway (VPG)とお客様のAmazon VPCをピアリング接続
- デバイスから、VPC内のサーバのプライベートIPアドレスに接続可能
 - VPGでNATされる



SORACOM Direct - 専用線接続

SORACOM と AWS 外のクラウドや DC を 専用線で接続するサービス



SORACOM Door – IPsec VPN

SORACOMとAWS外のクラウドやDCを IPsec VPNで接続するサービス



お客様事例: コマツ様

KOMATSU
SMART CONSTRUCTION

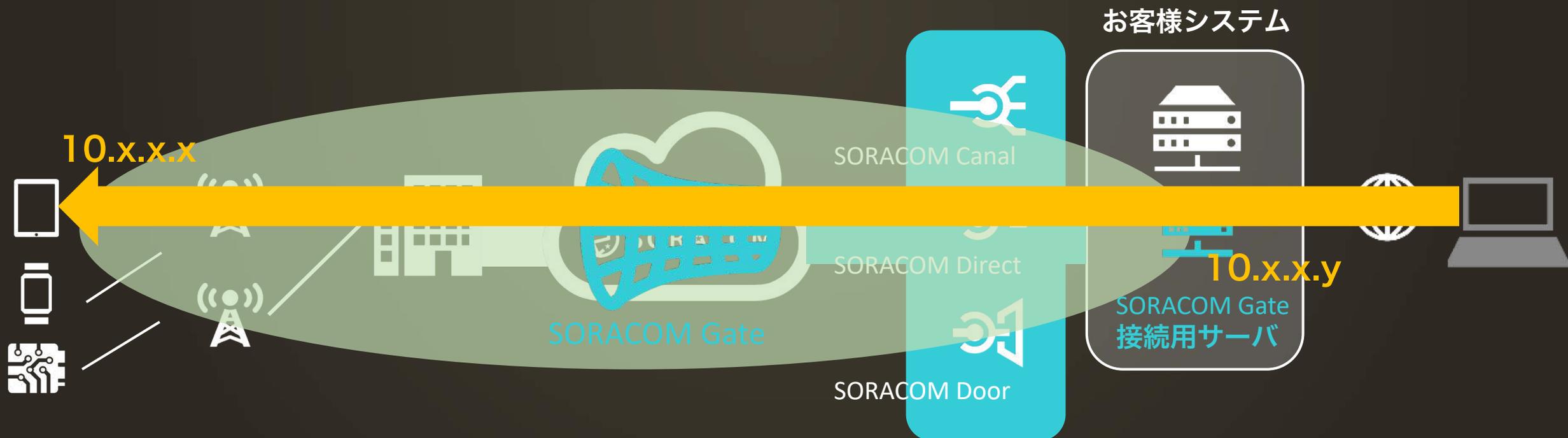


「ICT建機との高速でセキュアな通信を実現」

SORACOM Gateにより
ICT建機とクラウドシステムを
シームレスに接続
施工現場のIoT活用に貢献

SORACOM Gate - デバイス LAN 接続

デバイスとクラウドを1つの大きなプライベートLANに
クラウドからのリモートアクセスを可能にするサービス



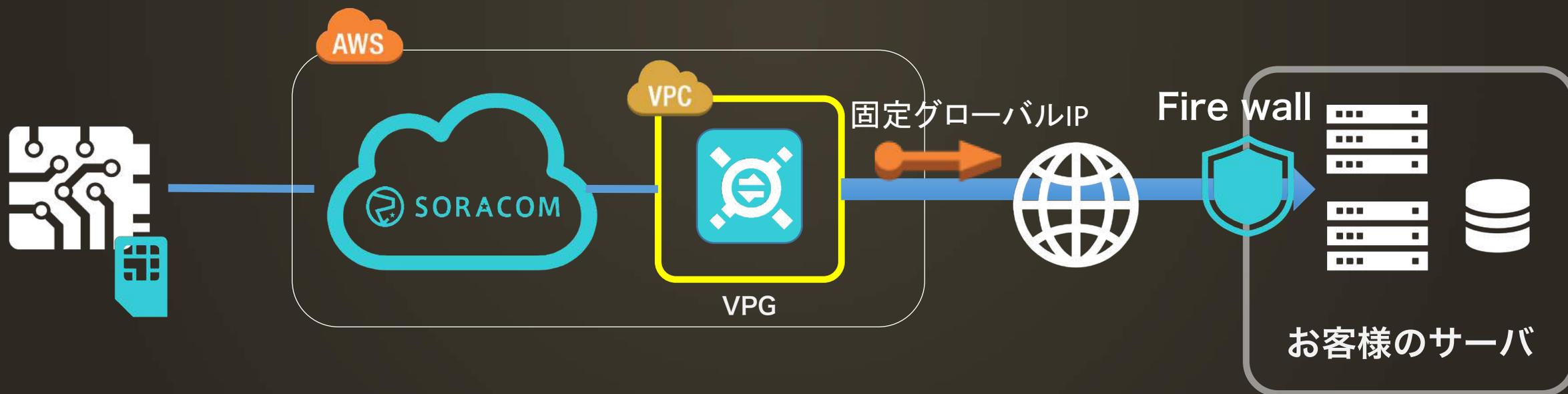
閉域網での接続

- 端末から自社システムまでの閉域網接続を容易に実現
- 通信の分析/可視化も実現



固定IPアドレスオプション

- SORACOM Virtual Private Gatewayの出口グローバルIPアドレスを固定するオプション
- VPGからくる通信のソースIPを固定できるため、受け側のサーバのFWにIPアドレス制限が出来る



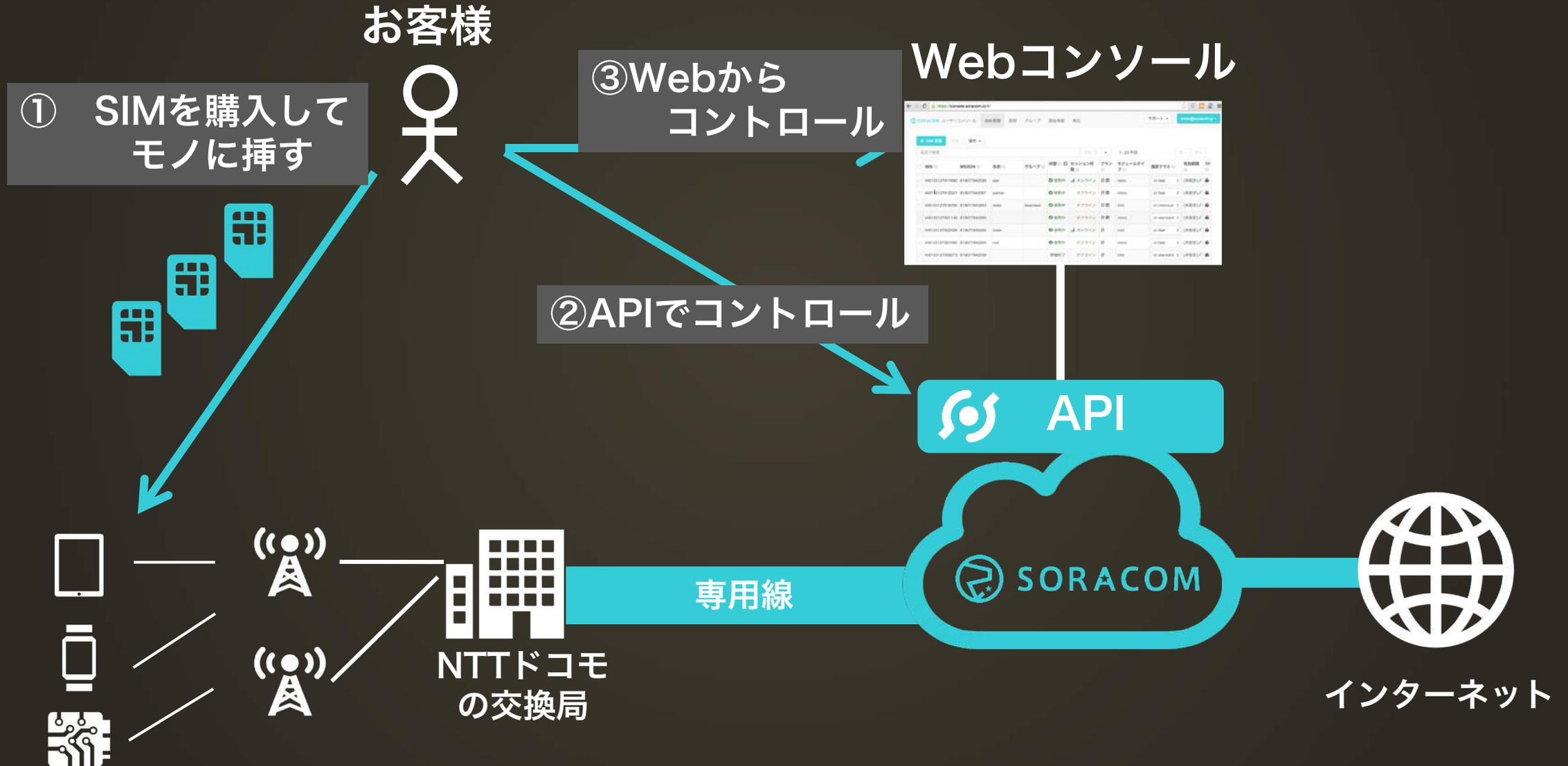
《 通信回線の管理 》

SIMカード

- Subscriber Identity Module
 - 利用者の認証モジュール
- 高い耐タンパ性
- SIMごとに認証、暗号化キー提供
- モバイル通信で認証と暗号化を担保



SORACOM Air



SORACOM Air

- API
 - 通信速度の変更
 - SIMの停止/解約
 - 通信量/利用料の取得
 - タグ付け
 - グループ etc
- SDK/CLIも提供

システムの自動化
SIMの一括管理

SORACOM API

SORACOM API v1

Auth

Show/Hide | List Operations | Expand Operations

POST	/auth	Authenticate Operator
POST	/auth/password_reset_token/issue	Issue Operator Password Reset Token
POST	/auth/password_reset_token/verify	Verify Operator Password Reset Token

Operator

Show/Hide | List Operations | Expand Operations

POST	/operators/{operator_id}/token	Generate Authentication Token
POST	/operators/{operator_id}/password	Update Operator Password
POST	/operators/{operator_id}/support/token	Generate Token for Support Console
POST	/operators	Create Operator
POST	/operators/verify	Verify Operator
GET	/operators/{operator_id}	Get Operator

Subscriber

Show/Hide | List Operations | Expand Operations

GET	/subscribers	List Subscribers
POST	/subscribers/{imsi}/register	Register Subscriber
GET	/subscribers/{imsi}	Get Subscriber
POST	/subscribers/{imsi}/update_speed_class	Update Subscriber speed class
POST	/subscribers/{imsi}/activate	Activate Subscriber
POST	/subscribers/{imsi}/deactivate	Deactivate Subscriber
POST	/subscribers/{imsi}/terminate	Terminate Subscriber

イベントハンドラー

- 一定の条件を満たした時にアクションを起こすことが可能
- 異常な通信量を検知して通信遮断、などが可能



- SIMの1日の通信データ量が一定のしきい値を超えたらSIMを停止
- 通算のデータ通信量が一定のしきい値を超えたらSIMを解約

《 通信の監視・制御 》

SORACOM Junction

SIMの通信を透過型にトラフィック分析・処理できるサービス

SORACOM Junction



VPG



SORACOM Canal

SORACOM Direct

SORACOM Door

お客様システム



SORACOM Junction

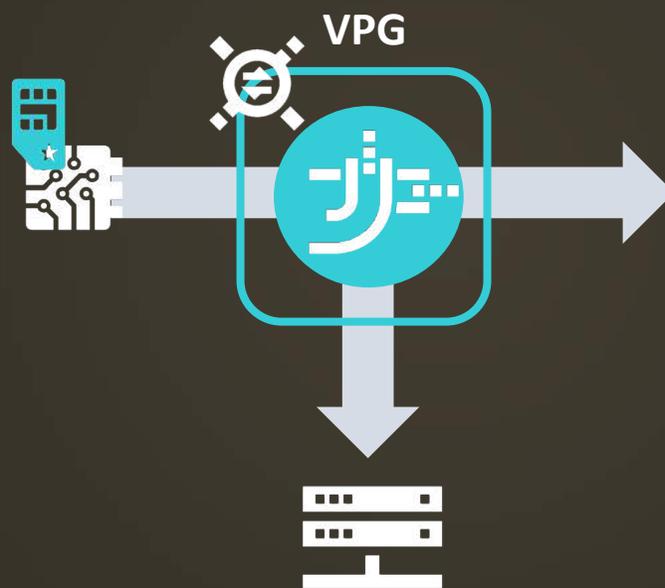
3つのトラフィック処理機能

Inspection



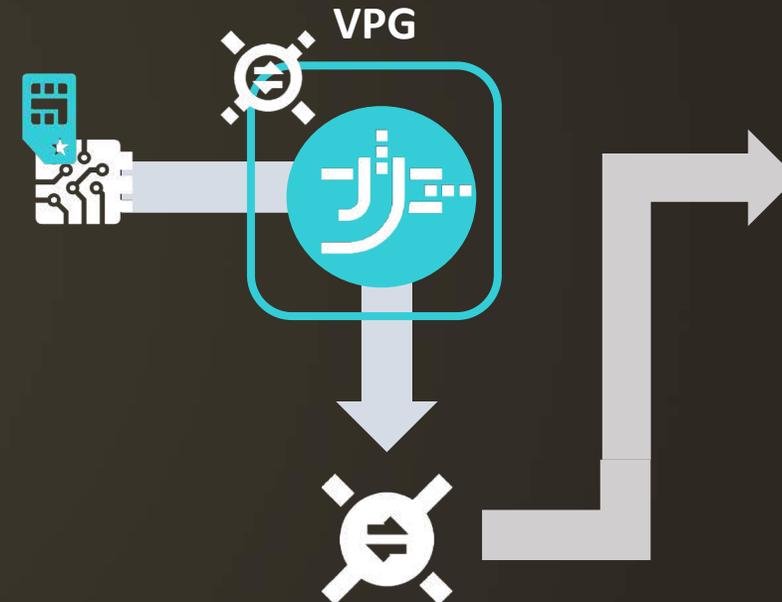
パケットフローを
解析して
統計情報を出力

Mirroring



パケットのコピー
を指定の宛先に
転送

Redirection



パケットを指定の
ゲートウェイ経由
で転送

Inspectionの動作詳細

- 一定間隔でトラフィックを収集・分類して統計
情報を計算
 - パケットサイズ、データサイズ
 - プロトコル
 - 接続先など
- 出力はJSONフォーマット
- SORACOM Funnelが対応するサービスに出力
 - サービス
 - リソースID
 - クレデンシヤル

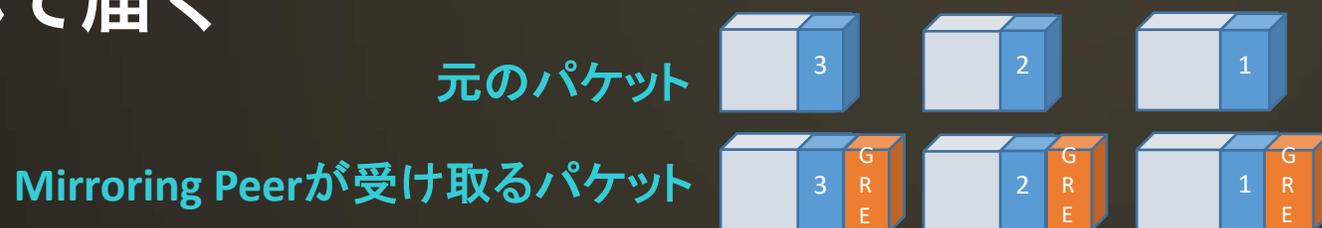
これらをFunnel同様に
設定すれば出力開始



Mirroringの動作詳細

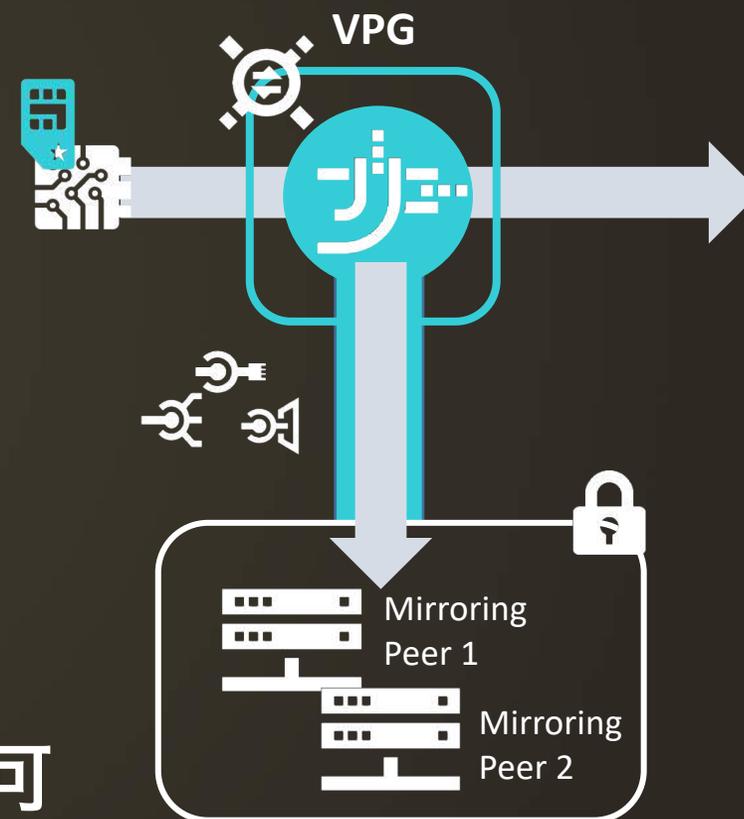
- Canal / Direct / Door接続されたホストをMirroring Peerとして追加
 - 2ホストまで登録可

- コピーされたパケットはGREでカプセル化されて届く



- Mirroring PeerはGREを受信できるように設定することでトラフィックをモニタリング可

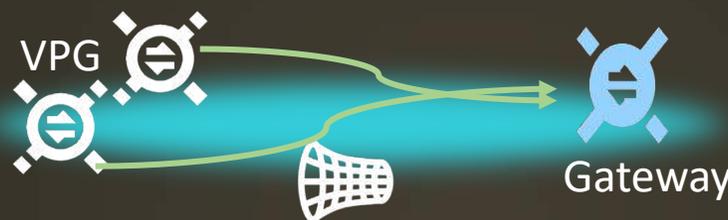
Mirroring



Redirectionの動作詳細

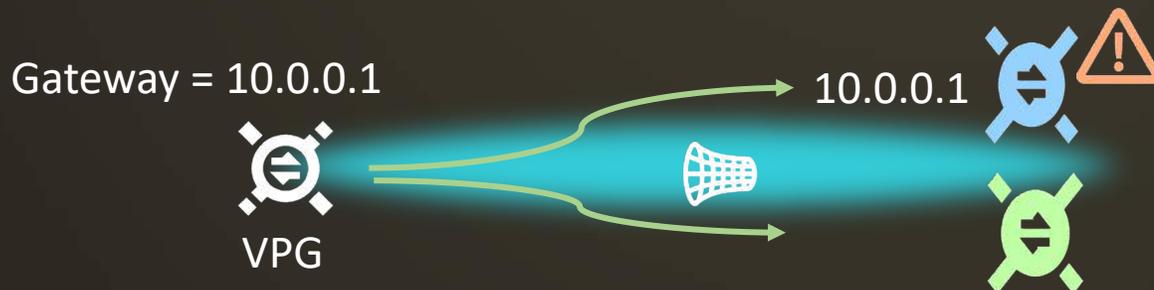
- 仮想L2サブネット上のPeerをGatewayとしてパケットを転送

- vxlanに対応

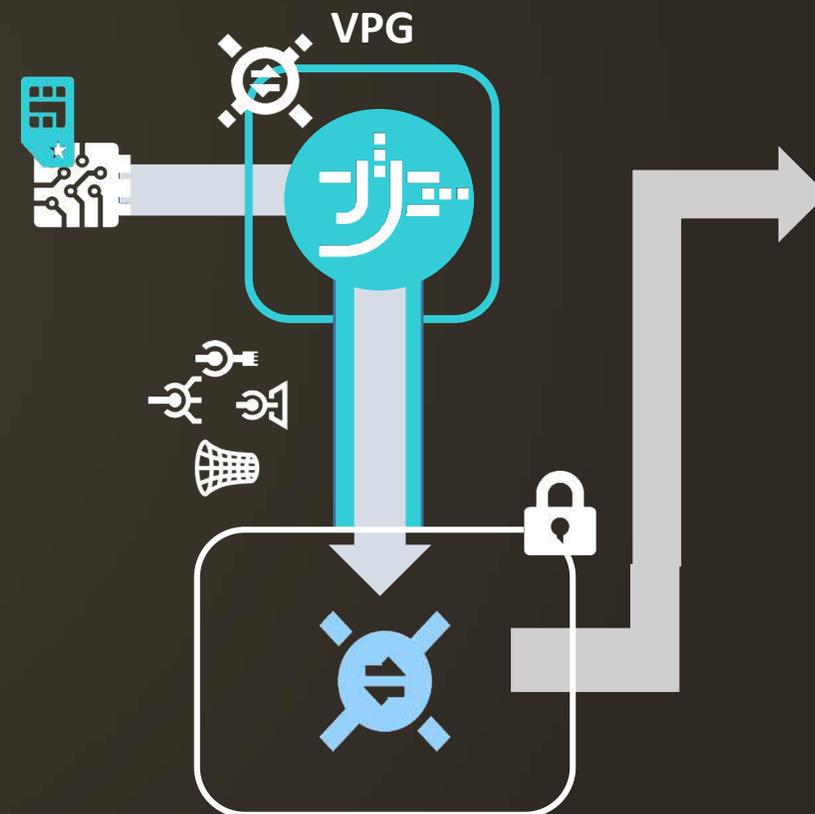


- 指定できるGateway Peerは1つ

- トラフィック制御点を1つに
- 障害対応はスタンバイノードへのアドレス付け替えで可



Redirection





- デバイスの通信の概況を把握したり異常を検知する方法はないか？
- デバイス自体のセキュリティは？
マルウェアの脅威への対処は？
- アプリケーションごとに異なる通信制御を適用することはできないか？

Junctionパートナーソリューション例

- Junction: **Inspection**

- Elastic様

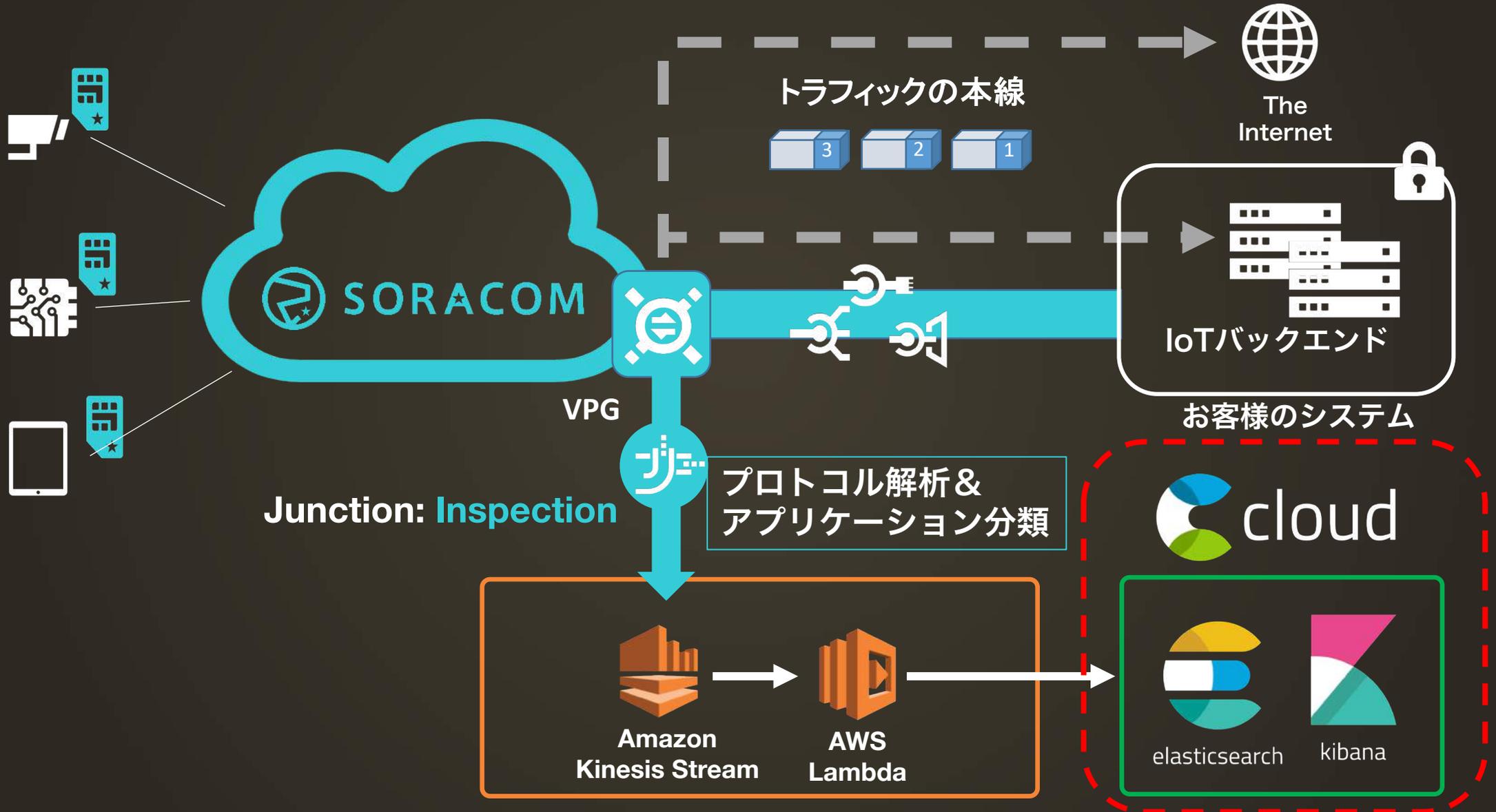
- Elastic Cloud, ElasticsearchおよびKibanaによる**可視化**

- Junction: **Mirroring**

- Acroquest様

- TorrentioFlowの**機械学習による異常検知、通知**

SORACOM Junction: Inspection



VPG / VPG

ID a2a493fb-3573-4cdc-9d95-fd9ac96d8305

Name Junction-Test 

Status Running

CIDR Range for device subnet 10.128.0.0/9

Use Internet Gateway Yes 

Basic settings

Junction settings

Advanced settings

SORACOM Junction: Inspection

OFF

Service Amazon Kinesis Streams 

Destination https://kinesis.ap-northeast-1.amazonaws.com/junction-inspection-escloud

Credentials set kinesis-dev  

Save Inspection Settings

SORACOM Junction: Mirroring

Destination	Description	Status
-------------	-------------	--------

- Discover
- Visualize
- Dashboard
- Timelion
- Graph
- Dev Tools
- Monitoring
- Management

Add a filter +

Soracom - Title

Realtime VPG Metric Monitor Running on Elastic Cloud

Soracom - Gauge Ethernet Bytes



Soracom - Gauge IP Bytes



Soracom - Gauge Average Packet Size



Soracom - Gauge Max Packet Size



Soracom - Gauge > 0



Soracom - Gauge > 64



Soracom - Gauge > 128



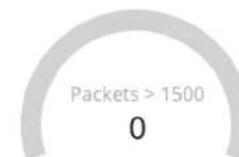
Soracom - Gauge > 256



Soracom - Gauge > 1024



Soracom - Gauge > 1500



Soracom - Bar Bytes



Soracom - Tag Cloud Protocols

The container is too small to display the entire cloud. Tags might be cropped or omitted.

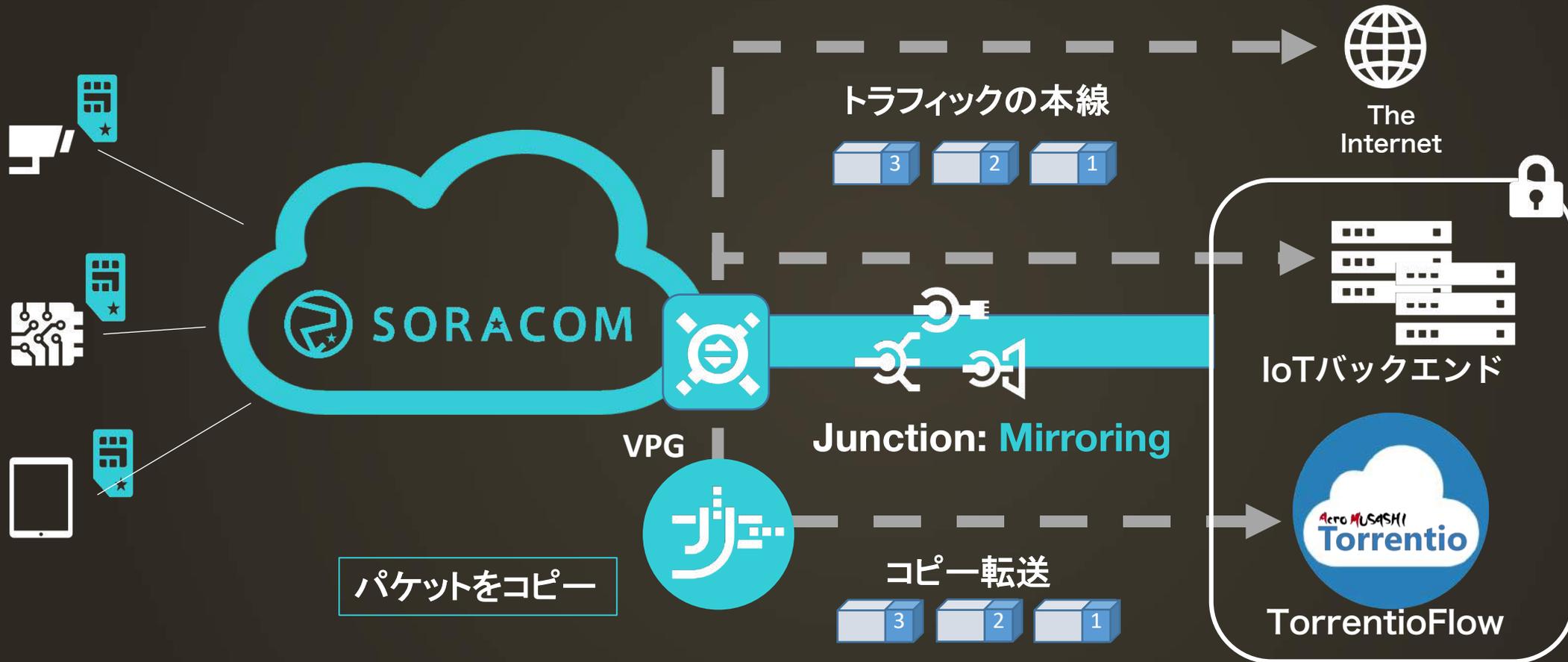


Soracom - Swimlane Protocols



- elastic
- Logout
- Collapse

SORACOM Junction: Mirroring



- 個別フローのリアルタイム分析・可視化
- 機械学習による異常検知・リスク分析
- 異常の通知

SORACOM Junction: Mirroring





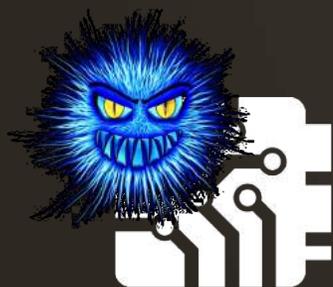
- デバイスの通信の概況を把握したり異常を検知する方法はないか？
- デバイス自体のセキュリティは？
マルウェアの脅威への対処は？
- アプリケーションごとに異なる通信制御を適用することはできないか？

デバイスの乗っ取りリスク

- デバイスに物理的にアクセスして悪用されるリスク
- デバイス側にマルウェア等が仕込まれることのリスク



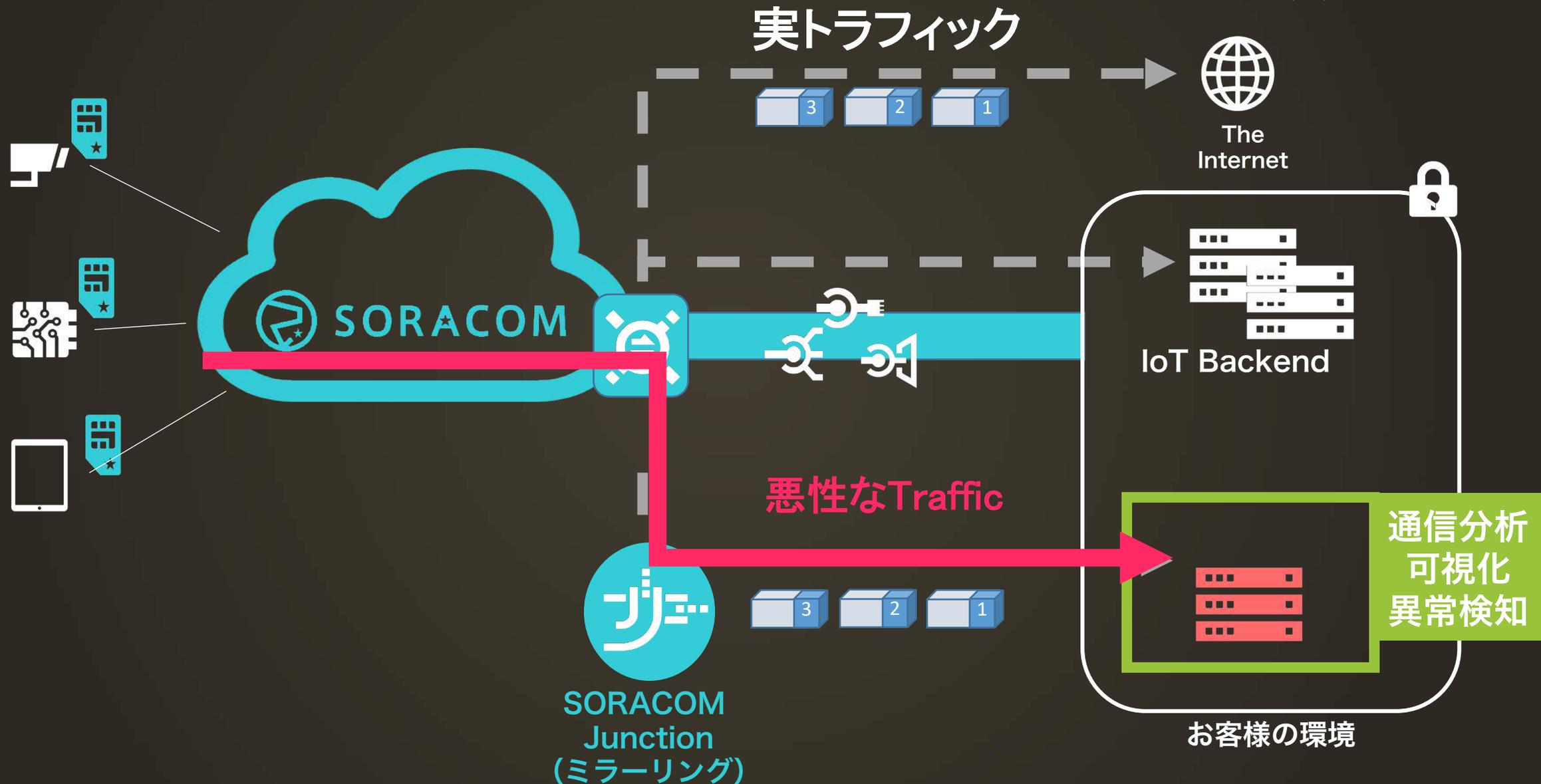
デバイスにマルウェアを仕込もう



Junctionパートナーソリューション例

- Junction: **Mirroring**による**DPI、IPS、可視化**
 - Trend Micro様
 - Virtual Network Function Suites(VNFS)
 - Palo Alto Networks様
 - VM-Series
 - Sandvine様
 - Procera PacketLogic

ミラーリング利用例

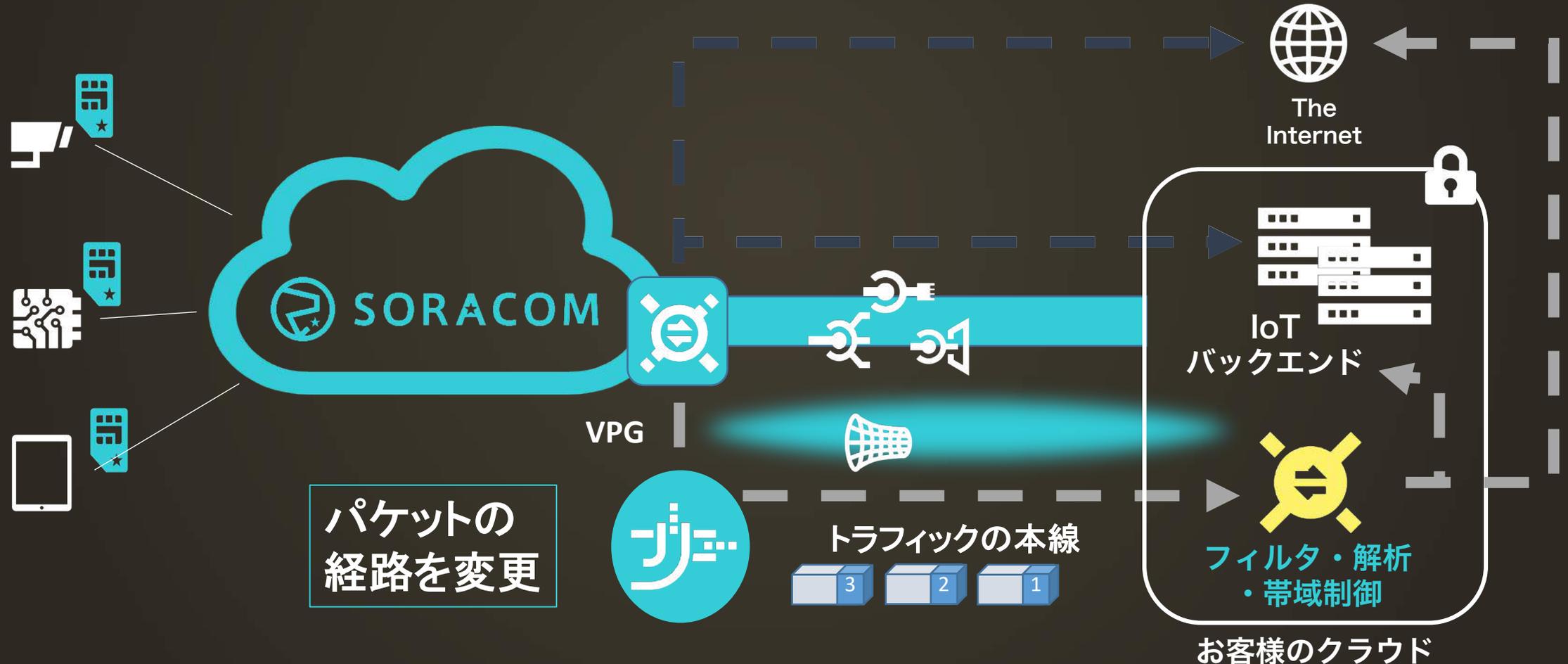




- デバイスの通信の概況を把握したり異常を検知する方法はないか？
- デバイス自体のセキュリティは？マルウェアの脅威への対処は？
- アプリケーションごとに異なる通信制御を適用することはできないか？

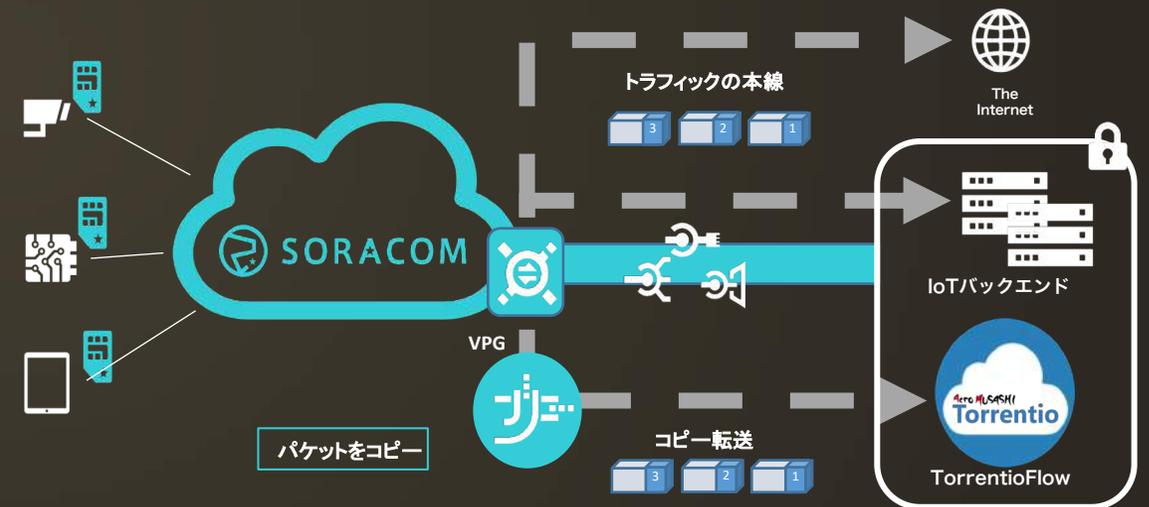
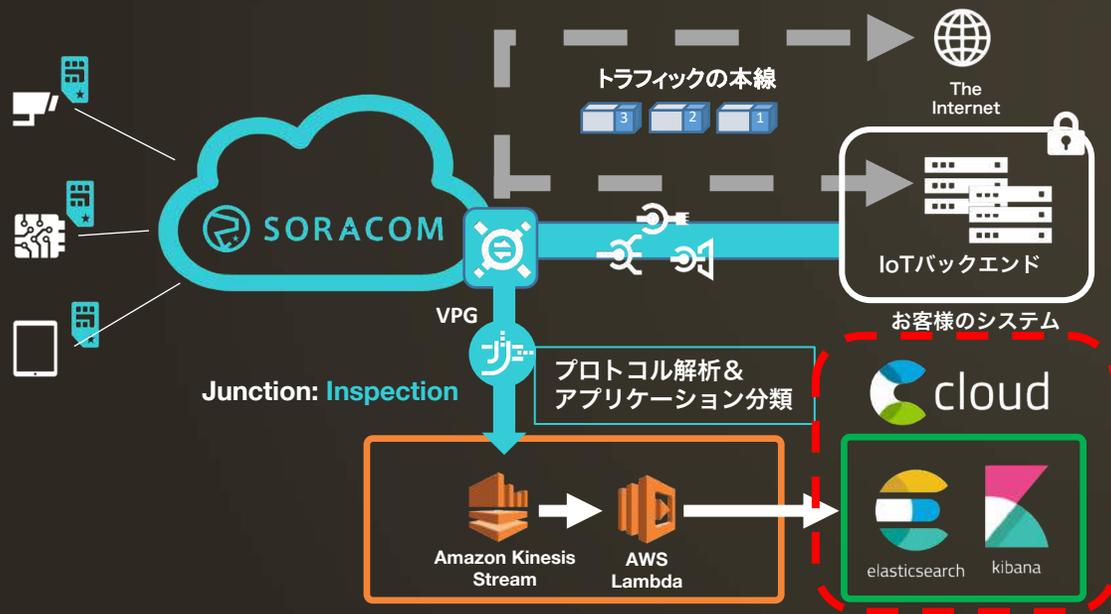
SORACOM Junction: Redirection

- パケットを指定のゲートウェイ経由で転送



Junctionを利用したパケット解析

パートナーソリューションと組み合わせることで、
自由な分析や可視化が可能



- ・ 個別フローのリアルタイム分析・可視化
- ・ 機械学習による異常検知・リスク分析
- ・ 異常の通知

《 デバイスの認証/認可 》

SIMカード

- Subscriber Identity Module
 - 利用者の認証モジュール
- 高い耐タンパ性
- SIMごとに認証、暗号化キー提供
- モバイル通信で認証と暗号化を担保



IMEIロック

IMSI 

SIMカードに格納されている
一意な番号



専用線

 SORACOM

インターネット

お客様のサーバー



IMEI 

通信モジュールに格納されている
一意な番号

IMEIロック  

特定のIMSIとIMEIのペア
以外の通信を遮断

《 アプリケーションの認証/認可 》

SIMカード

- Subscriber Identity Module
 - 利用者の認証モジュール
- 高い耐タンパ性
- SIMごとに認証、暗号化キー提供
- モバイル通信で認証と暗号化を担保



SORACOM Beam - セキュアなプロキシ



SIMカードの認証を活用し
本来デバイスに実装するべき接続先設定や暗号化等を
SORACOM へオフロード

HTTP → HTTPS
MQTT → MQTTS
TCP → TCP over SSL
UDP → HTTPS
...

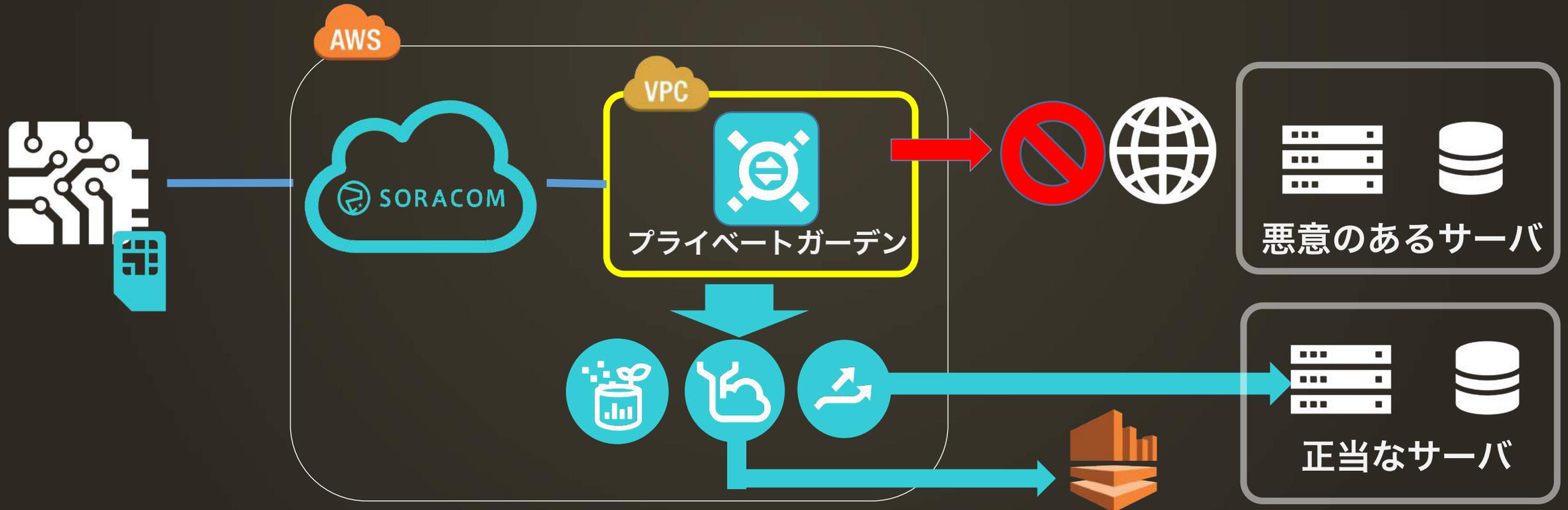
SORACOM Funnel - クラウドアダプタ



SIMカードの認証を活用し送信先を指定するだけで
クラウド連携を実現
デバイスへの各種SDKのインストールが不要

プライベートガーデン

- SIMからSORACOMのアプリケーションサービスとNTPにしか接続できない制限をつけるためのサービス
- デバイスが意図せず外部に接続しないようにできる
- グループ設定のVPGに「プライベートガーデン」を指定



+ Register SIM Details Actions

Raspberry

Items 1 - 1 (1 selected)

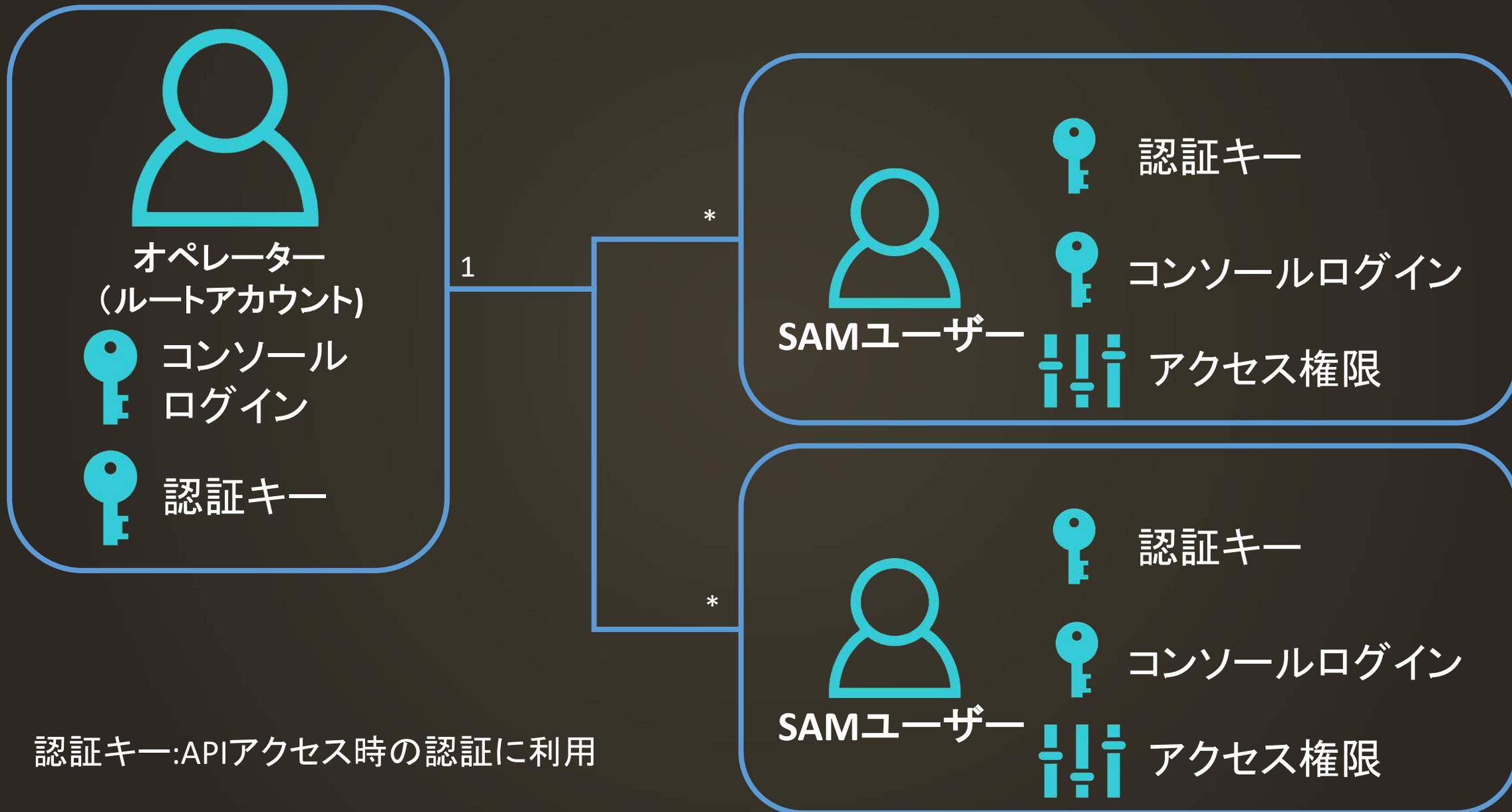
Previous Next

<input checked="" type="checkbox"/>	Name ?	Group ?	Status ?	Session ?	Plan ?	Speed class ?	Expiry Date / Time ?	IMEI Lock ?	TI
<input checked="" type="checkbox"/>	RaspberryPi		Active	Online	↑↓	s1.fast	(Not specified)		

Items per page 100

《 SORACOMアカウントの保護 》

SORACOMアカウントの構成



認証キー:APIアクセス時の認証に利用

SORACOM Access Management

子ユーザーを作成し、認証情報とAPI単位の権限管理ができる



The screenshot shows the SORACOM Access Management interface. At the top, there is a navigation bar with the SORACOM logo and several menu items: SIM 管理, 監視, グループ, 課金情報, 発注, セキュリティ, and サポート. The 'セキュリティ' (Security) menu item is highlighted. On the left side, there is a sidebar with three main sections: 'ユーザー' (Users), 'ロール' (Roles), and '認証情報ストア' (Credential Store). The 'ユーザー' section is active, and a '+ ユーザー作成' (Create User) button is visible. Below this, there is a table listing existing users with columns for '名前' (Name) and '概要' (Summary).

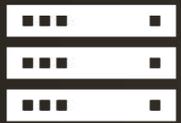
名前	概要
developer	開発用ユーザー
my-user	SAMユーザー
payment	経理用
test	テストユーザー
yaman	開発者

ユーザーごとのアクセス権限管理(例)



- 開発者

- コンソールログインと認証キーを許可
- SIMの解約以外の操作はOK



- 監視プログラム

- 認証キーのみ許可
- GETメソッド（読み取り）のみ許可



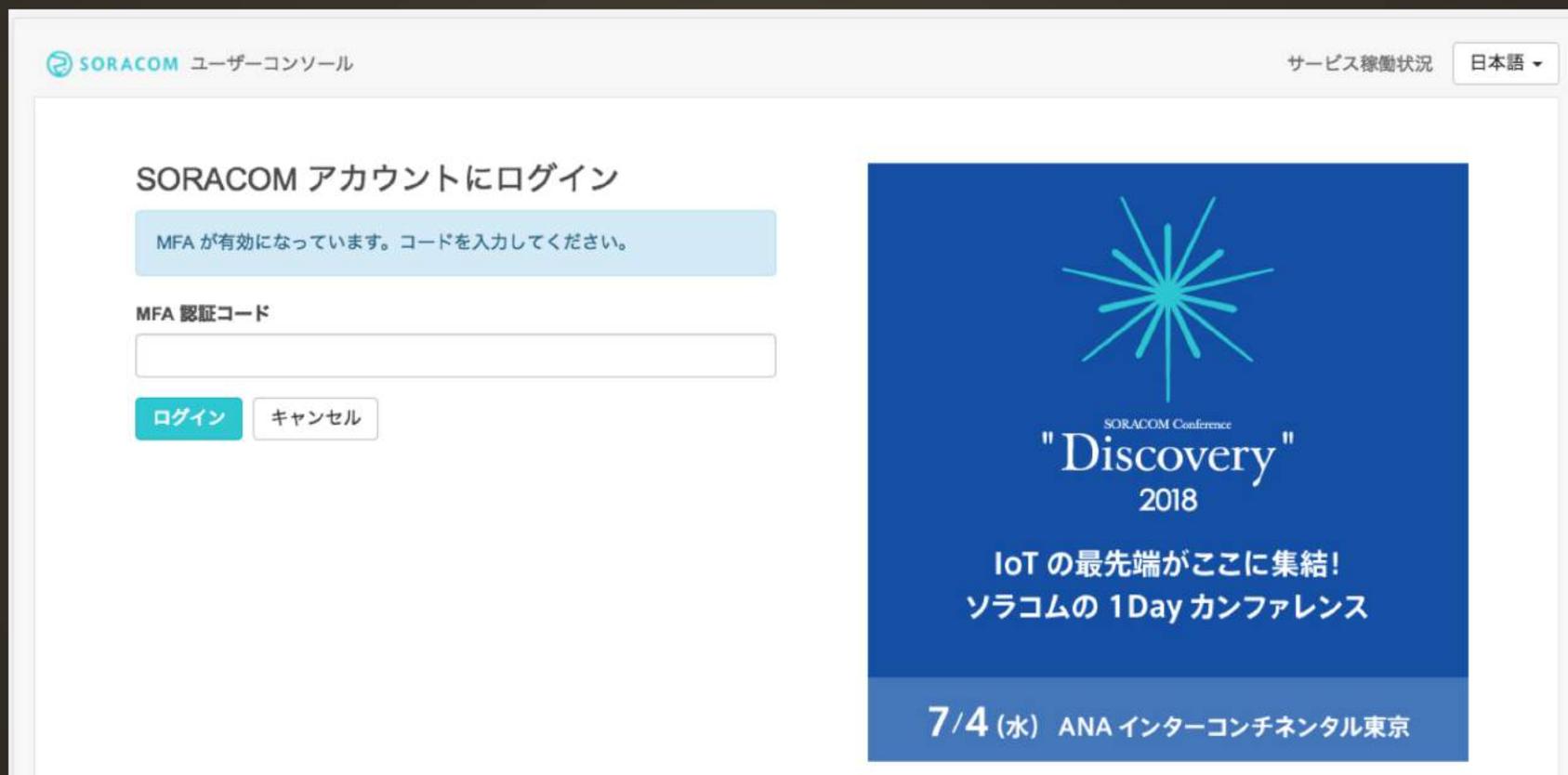
- 調達担当

- コンソールログインのみ可能
- 課金と発注のみ利用可能
- SIM操作は一切NG

SORACOMアカウントのMFA機能

ルートアカウントのコンソールログイン時にMFA(多要素認証)が利用可能に

- ・SAMユーザーは順次対応



The screenshot shows the SORACOM user console interface. At the top left, it says "SORACOM ユーザーコンソール". At the top right, there are links for "サービス稼働状況" and a language dropdown set to "日本語". The main heading is "SORACOM アカウントにログイン". Below this, a light blue box contains the message: "MFA が有効になっています。コードを入力してください。". Underneath is a label "MFA 認証コード" followed by an empty input field. At the bottom of the form are two buttons: "ログイン" (Login) and "キャンセル" (Cancel). On the right side of the page, there is a blue promotional banner for the "SORACOM Conference 'Discovery' 2018". The banner features a starburst logo and text: "IoT の最先端がここに集結! ソラコム の 1Day カンファレンス". At the bottom of the banner, it states "7/4 (水) ANA インターコンチネンタル東京".

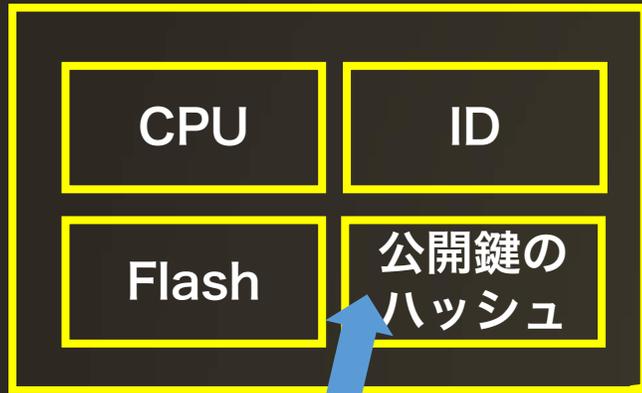
《 デバイス自体の保護 》

デバイスへの物理的な攻撃

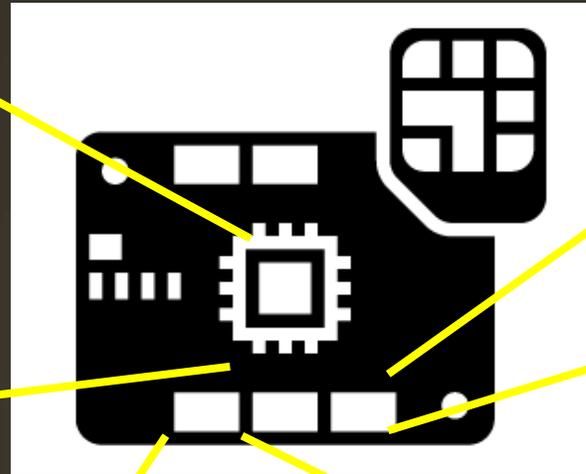
脅威		対策候補			
発生箇所	脅威名	対策名	他のガイドとの関係		
			OTA	OWASP	
ECU	ウイルス感染	脆弱性対策	OTA5, OTA11		
		ホワイトリスト制御			
		ソフトウェア署名	OTA6,	OWASP9	
	不正改造	耐タンパーH/W	OTA37	OWASP10	
		耐タンパーSW	OTA9		
		ソフトウェア署名	OTA6	OWASP9	
コネクテッドカー	ECU・センサー間通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8
	車載ネットワーク内 (ECU ・ ECU 間等)通信	盗聴・改ざん	通信路暗号化	OTA2	OWASP8
	OBD-II ポート	不正アクセス	脆弱性対策	OTA5, OTA11	
ユーザ認証			OTA13, OTA14, OTA15, OTA16	OWASP2, OWASP8	
FW 機能				OWASP3	
不正コマンド		メッセージ認証			
	DoS 攻撃	DoS 対策		OWASP3	

Platform Security Architecture(PSA)

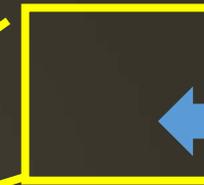
MCU(Cortexなど)



IoTデバイス



セキュアメモリ



通信用の一時鍵の記録や暗号化処理の実施など、実行時におけるセキュアなメモリ環境での処理
(Trusted secure functions)

1. 製造時にセキュアなプロセスで書き込み

(Trusted device initialization)

Firmware



2. 秘密鍵で、公開鍵とファームウェアを署名
ブート時に署名を確認 (Trusted boot)
ファームウェアアップデート時も署名を確認 (firmware update)

この仕組みを実現する

フレームワーク(Firmware framework)と
ハードウェア(Hardware system architecture)

《まとめ》

狙われるIoTシステム



デバイスを
乗っ取る

- PSAの利用
- SIMの認証を利用
- SORACOM Junctionで監視
- APIで通信遮断



間で通信を
盗み見よう

- SIMの認証を利用
- セルラーの暗号化
- 閉域接続の利用



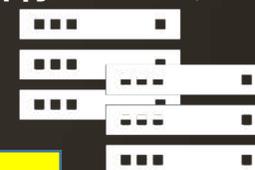
デバイスにリモート
アクセスしてやろう

- グローバルIPをSIMに付与しない
- SORACOM Gateの利用



The Internet

お客様のシステム



バックエンド

- Canal/Direct/Doorの利用
- 固定IPアドレス機能の利用



SORACOM
アカウントを
乗っ取る

- SAMを利用した権限管理
- MFAの活用



IoTバックエンド
を攻撃してやろう



開発者サイト・ブログのご紹介



開発者サイト

<https://dev.soracom.io/jp/>

各サービスのGetting Started
を用意しています



SORACOM ブログ

<https://blog.soracom.jp/>

最新の技術情報アップデートを
いち早くお届けします

SORACOM User Group 本日開催



- 時間 18:00 – 20:00
- 参加費 500円

多数のライトニングトークや特別企画をご紹介します！



Try! SORACOM チャレンジキャンペーン

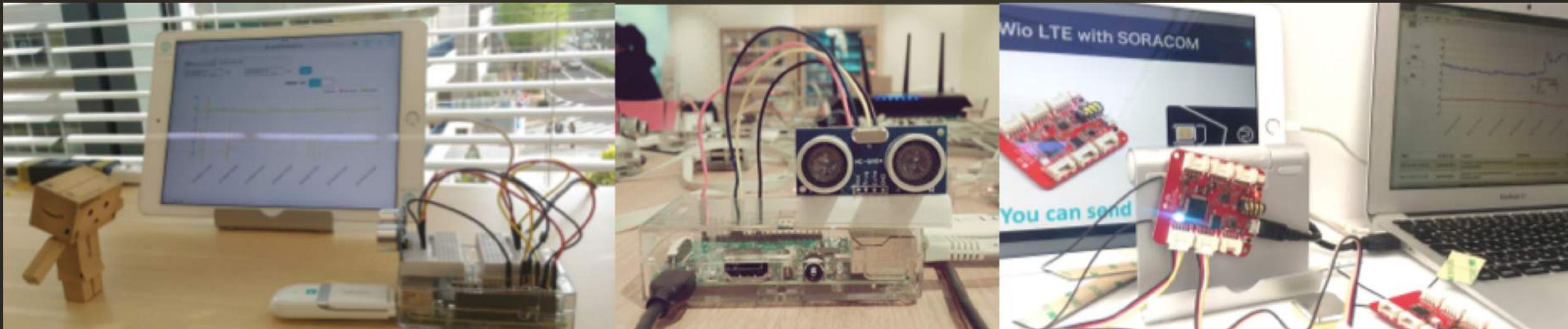


～記事を書いてノベルティをゲットしよう～

期間：4月26日～6月30日

対象：企業・個人問わずどなたでも参加可能

内容：SORACOMを使った電子工作や、Deep Diveな記事を書いた方にクールなノベルティをプレゼントします



今日から IoT を始めよう！ 体験キット本日販売中



Grove IoT スターターキット for SORACOM

7種類のGroveセンサーとSIMが搭載可能なデバイスで
素早くプロトタイピングが可能

(税抜価格：15,980円)



SORACOMの願い



クラウド ⇒ 多くのビジネス、Webサービス
SORACOM ⇒ 多くのIoTビジネス、システム

たくさんの
IoTプレイヤーが生まれますように

世界中のヒトとモノをつなげ
共鳴する社会へ



SORACOM