SORACOM Technology Camp 2020

SORACOM で守る IoT のエンドツーエンド・セキュリティ

SORACOM Technology Camp 2020

本日のハッシュタグ

SORACOM Technology Camp 2020

#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
  - 課金担当

公式ワークブック
SORACOM実装ガイド

日経BP社より3月19日発刊
Kindle版/単行本版

SORACOMサービスとIoTデバイスの
利用方法を
9つのハンズオンを通して解説

Amazonにて予約開始
https://www.amazon.co.jp/dp/4296105590

Agenda

SORACOM Technology Camp 2020

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

SORACOM Technology Camp 2020

《 SORACOMが解決するIoTの課題 》

IoT（Internet of Things）

SORACOM Technology Camp 2020

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 2020

モノ

Arduino

STM32 Nucleo

Raspberry Pi Zero

ESP-WROOM-02

クラウド

Amazon Web Services

Microsoft Azure

Google Cloud Platform

IoTの活用が期待される分野

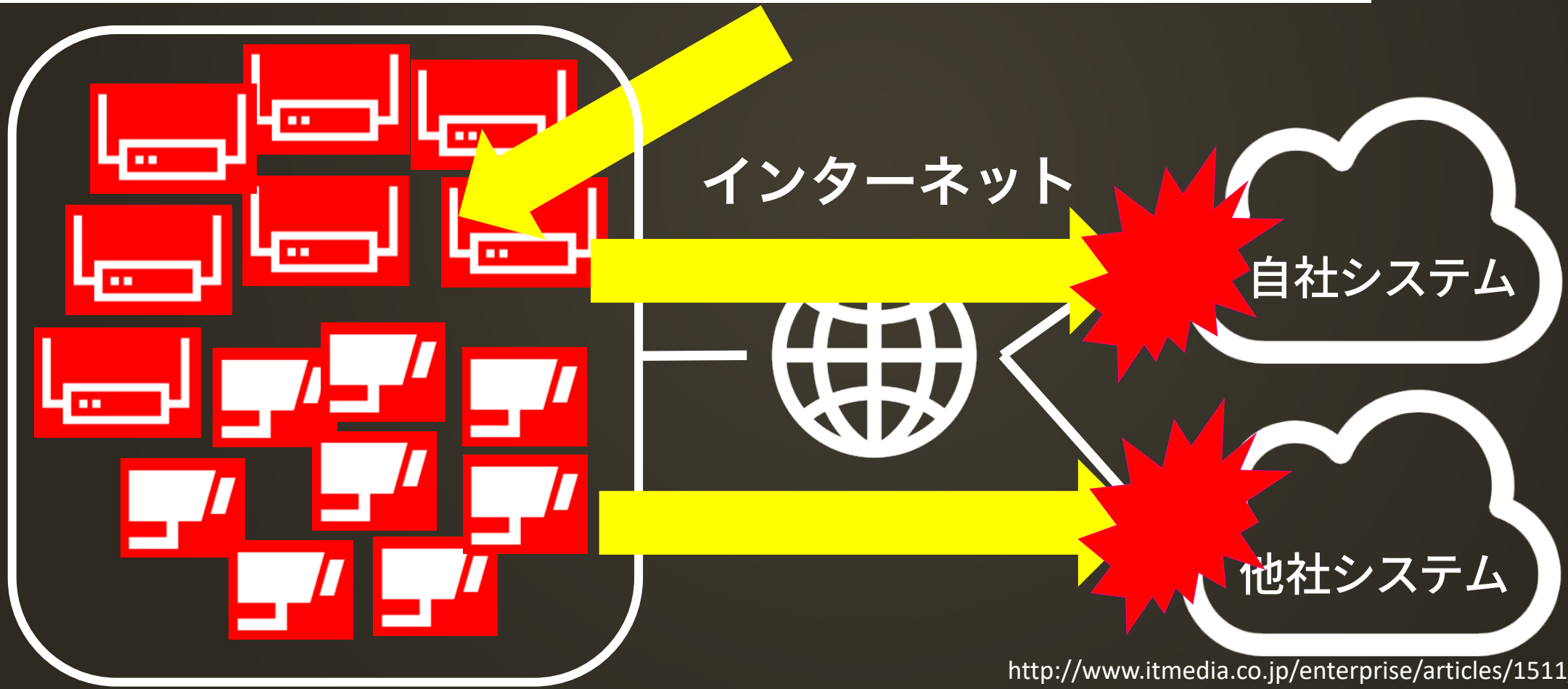
SORACOM Technology Camp 2020

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]



http://www.itmedia.co.jp/enterprise/articles/1511/26/news046.html

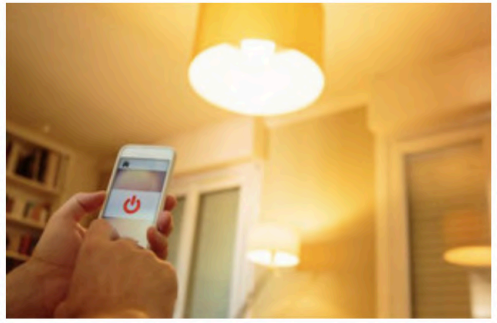
イギリス政府
「消費者向けIoTデバイスのデフォルトパスワード設定の規制」を法案化

Press release

Government to strengthen security of internet-connected products

New legislation to improve security standards of internet-connected household devices

Published 27 January 2020
From: Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and Matt Warman MP



A new law will protect millions of users of internet-connected household items from the threat of cyber hacks, Digital Minister Matt Warman announced today.

The plans, drawn up by the Department for Digital, Culture, Media and Sport (DCMS), will make sure all consumer smart devices sold in the UK adhere to the three rigorous security requirements for the Internet of Things (IoT).

These are:

- All consumer internet-connected device passwords must be unique and not resettable to any universal factory setting
- Manufacturers of consumer IoT devices must provide a public point of contact so anyone can report a vulnerability and it will be acted on in a timely manner
- Manufacturers of consumer IoT devices must explicitly state the minimum length of time for which the device will receive security updates at the point of sale, either in store or online

The sale of connected devices is on the rise. Research suggests there will be 75 billion internet connected devices, such as televisions, cameras, home assistants and their associated services, in homes around the world by the end of 2025.

https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products

IoTの課題

SORACOM Technology Camp 2020

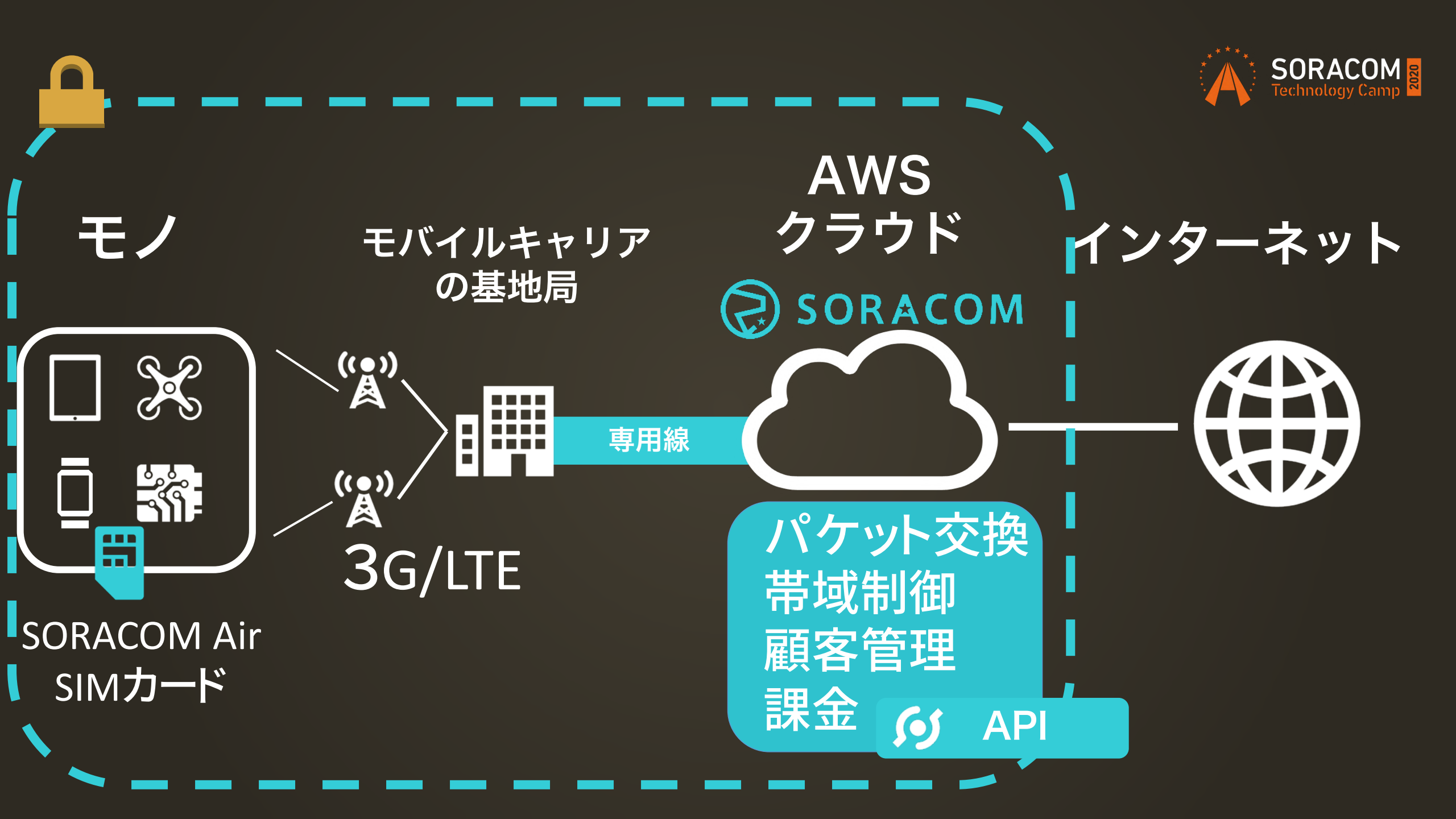
モノ　　インターネット　　クラウド

セキュリティ
通信の管理

ソラコムでの解決策

SORACOM Technology Camp 2020

モノ　　インターネット　　クラウド


SORACOM Technology Camp 2020
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
専用線
3G/LTE
SORACOM Air
SIMカード
パケット交換
帯域制御
顧客管理
課金
API

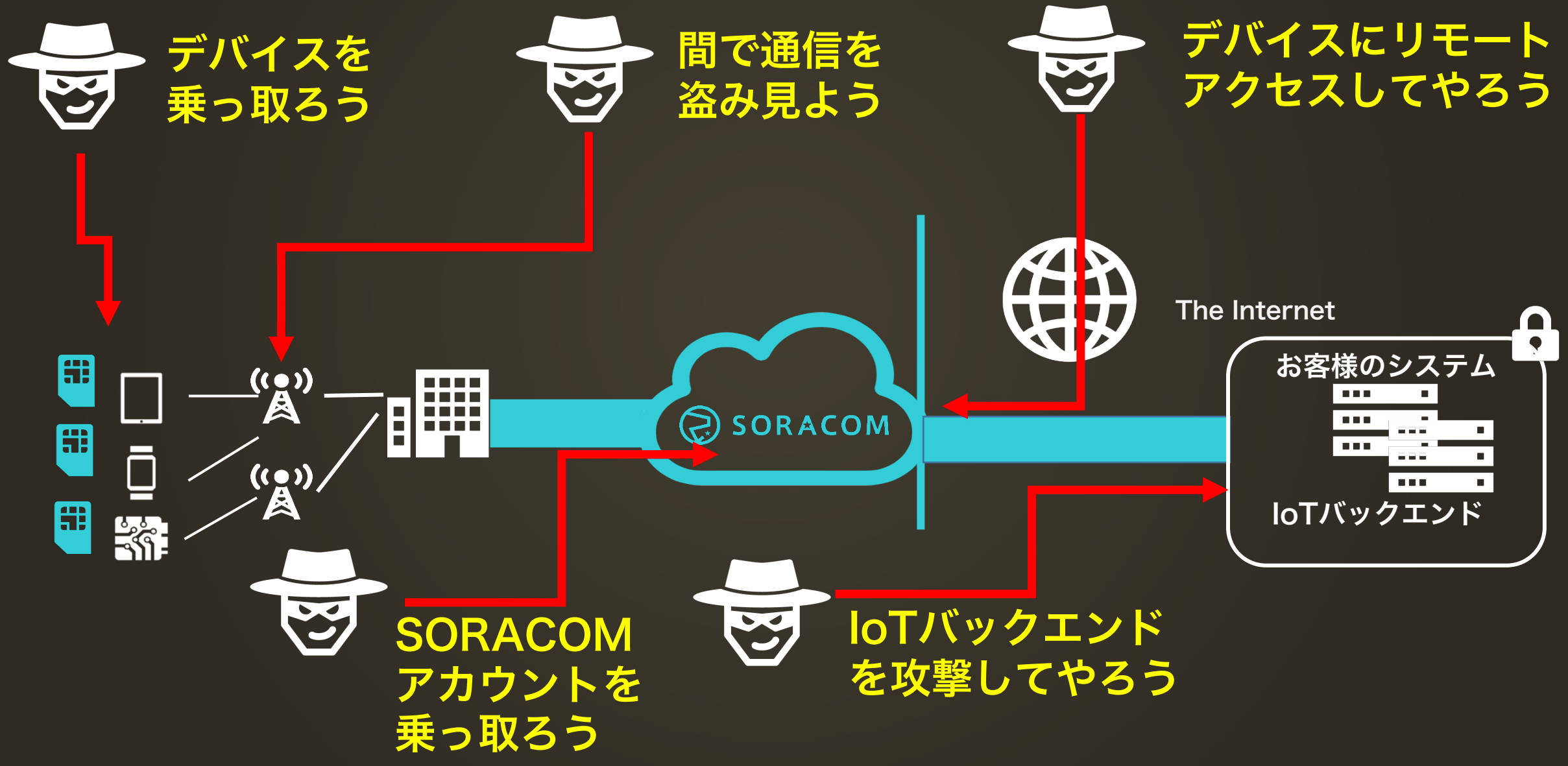
SORACOM Technology Camp 2020

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

SORACOM Technology Camp 2020

《 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

SORACOM Technology Camp 2020

- 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

IoTテクノロジー民主化のためのプラットフォーム

SORACOM Technology Camp 2020

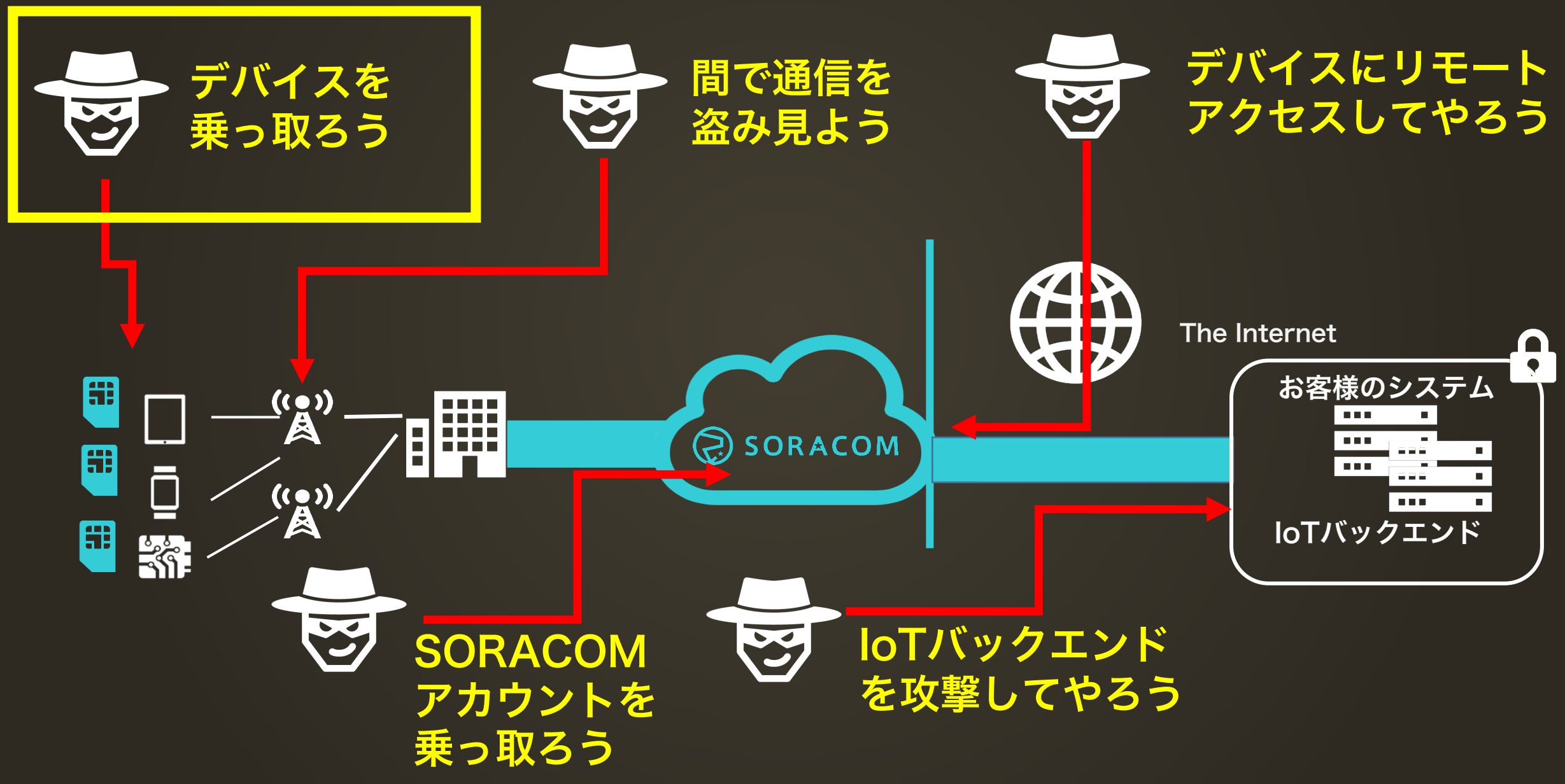
インタフェース	Web インターフェース User Console	API Web API Sandbox	アクセス権限管理 SORACOM Access Management	ライブラリ & SDKs CLI(Go), Ruby, Swift	開発者サポート Developer Support
アプリケーション	データ収集・蓄積 SORACOM Harvest Data / Files		ダッシュボード作成/共有 SORACOM Lagoon		エッジプロセッシング SORACOM Mosaic
	データ転送支援 SORACOM Beam		クラウドアダプタ SORACOM Funnel		クラウドファンクション SORACOM Funk
	SIM認証・証明 SORACOM Endorse		デバイス管理 SORACOM Inventory		セキュアプロビジョニング SORACOM Krypton
ネットワーク	デバイスLAN SORACOM Gate		透過型トラフィック処理 SORACOM Junction		オンデマンドリモートアクセス SORACOM Napter
	プライベート接続 SORACOM Canal		専用線接続 SORACOM Direct		仮想専用線 SORACOM Door
デバイス	USB ドングル / セルラーモジュール / マイコンモジュール / ボタン / カメラ				
コネクティビティ	IoT向けデータ通信 SORACOM Air for Cellular (2G, 3G, LTE) / LPWA (LoRaWAN, Sigfox, , LTE-M) / アップロード専用SIM				

SORACOM Global Platform

SORACOM Technology Camp 2020

《 デバイス自体の保護 》

狙われるIoTシステム



デバイスへの物理的な攻撃

SORACOM Technology Camp 2020

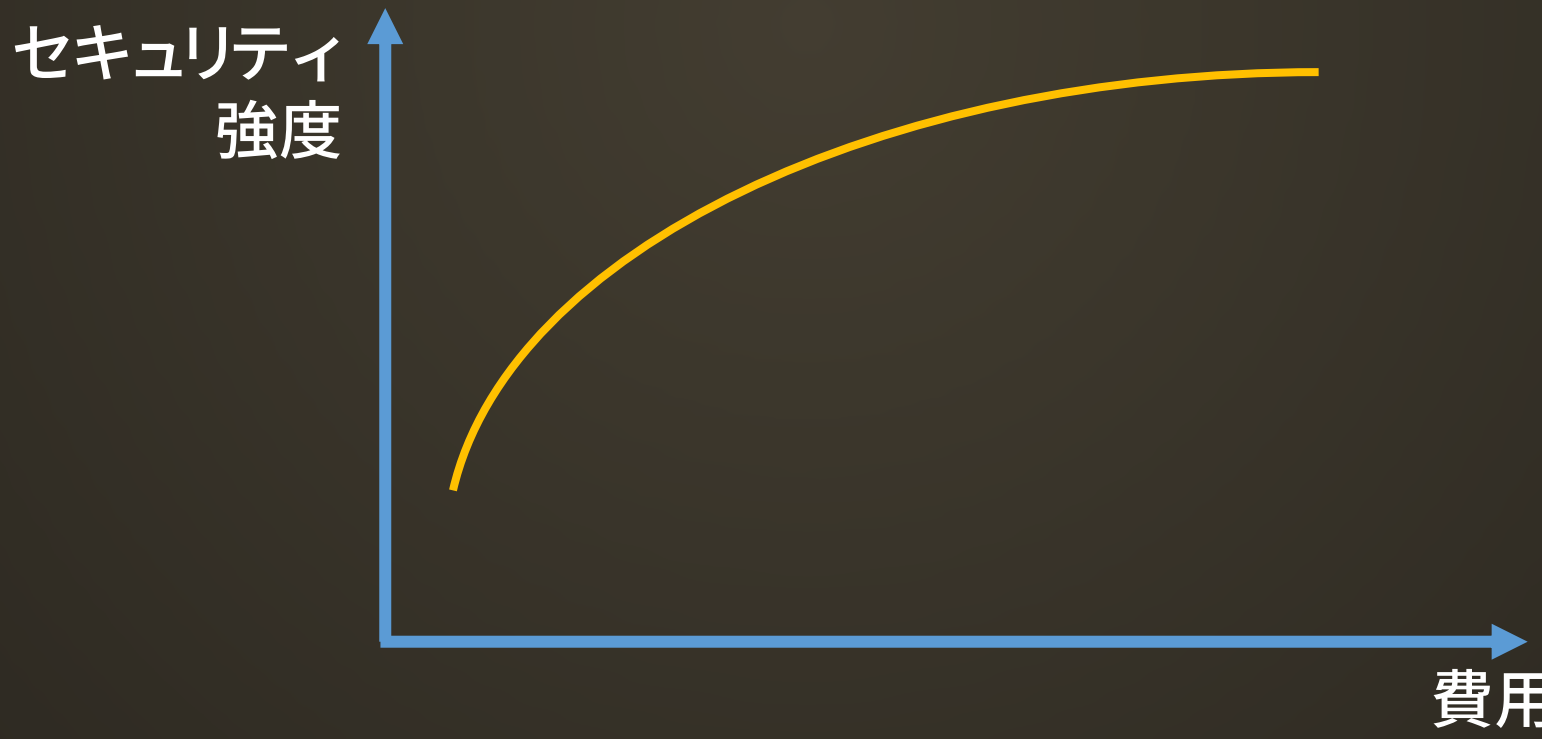
- 破壊・盗難
- 不正侵入・改ざん

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
コネクテッドカー	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S/W	OTA9	
			ソフトウェア署名	OTA6	OWASP9
	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

https://www.ipa.go.jp/files/000052459.pdf

物理攻撃への対策

- 盗難・改竄発生時の損失をみながら、費用対効果で対応を検討することが重要
  - 物理的な損失と、データなどの論理的な損失
- 盗難・改竄がある前提で、発生時の対応を設計する



Platform Security Architecture(PSA)

SORACOM Technology Camp 2020

IoTデバイス

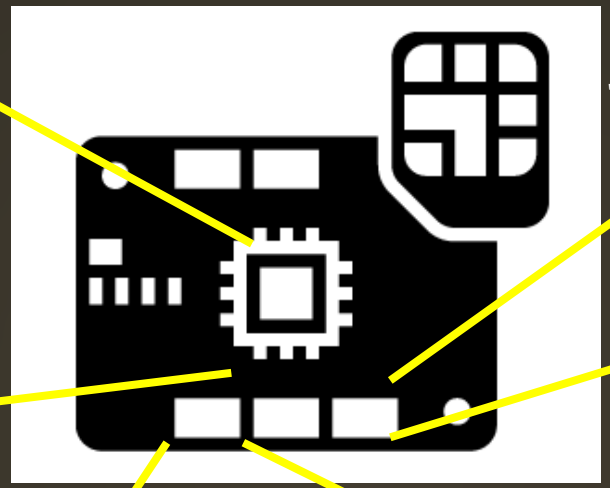
MCU(Cortexなど)

CPU

ID

Flash

公開鍵の
ハッシュ



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

署名

公開鍵

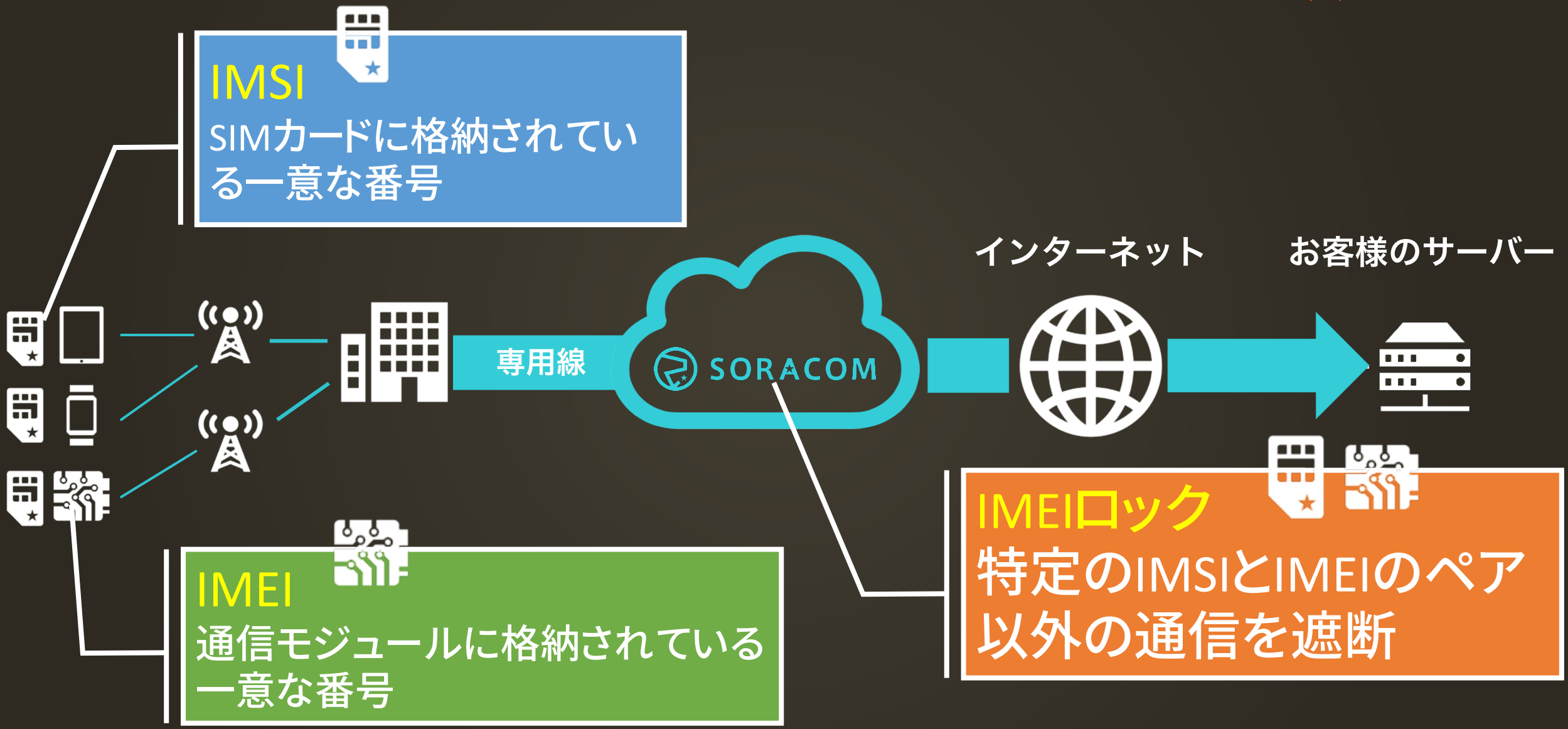
ファームウェア

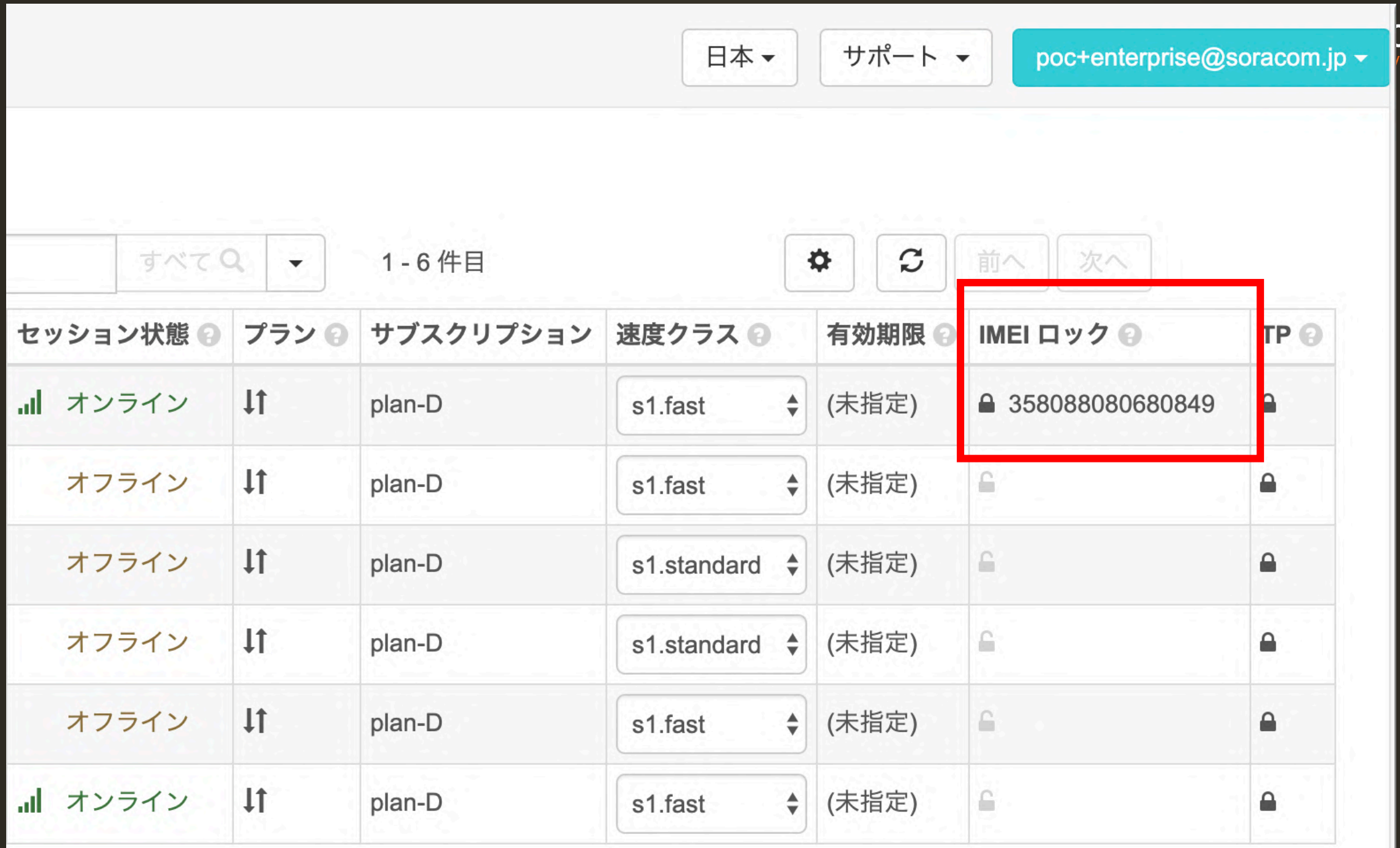
2.秘密鍵で、公開鍵と
ファームウェアを署名
ブート時に署名を確認 (Trusted boot)
ファームウェアアップデート時も
署名を確認（firmware update)

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)

IMEIロック

SORACOM Technology Camp 2020




日本
サポート
poc+enterprise@soracom.jp
すべて
1 - 6 件目
前へ
次へ
セッション状態
プラン
サブスクリプション
速度クラス
有効期限
IMEI ロック
TP
オンライン
plan-D
s1.fast
(未指定)
358088080680849
オフライン
plan-D
s1.fast
(未指定)
オフライン
plan-D
s1.standard
(未指定)
オフライン
plan-D
s1.standard
(未指定)
オフライン
plan-D
s1.fast
(未指定)
オンライン
plan-D
s1.fast
(未指定)

位置情報表示

SORACOM Technology Camp 2020

☐	440103224981970	松本	情報システム部管理グループ	使用中	オフライン	⇅	plan-D	s1.standard	(未指定)
☐	440103225416285	片山(タブレット)	情報システム部管理グループ	使用中	オフライン	⇅	plan-D	s1.fast	(未指定)
☐	440103225456536	松井	情報システム部管理グループ	使用中	オンライン	⇅	plan-D	s1.fast	(未指定)

SIMの位置表示
（通信基地局表示）

基地局の情報をもとに位置情報を表示して

SORACOMユーザー向けデバイス補償サービス

SORACOM Technology Camp 2020

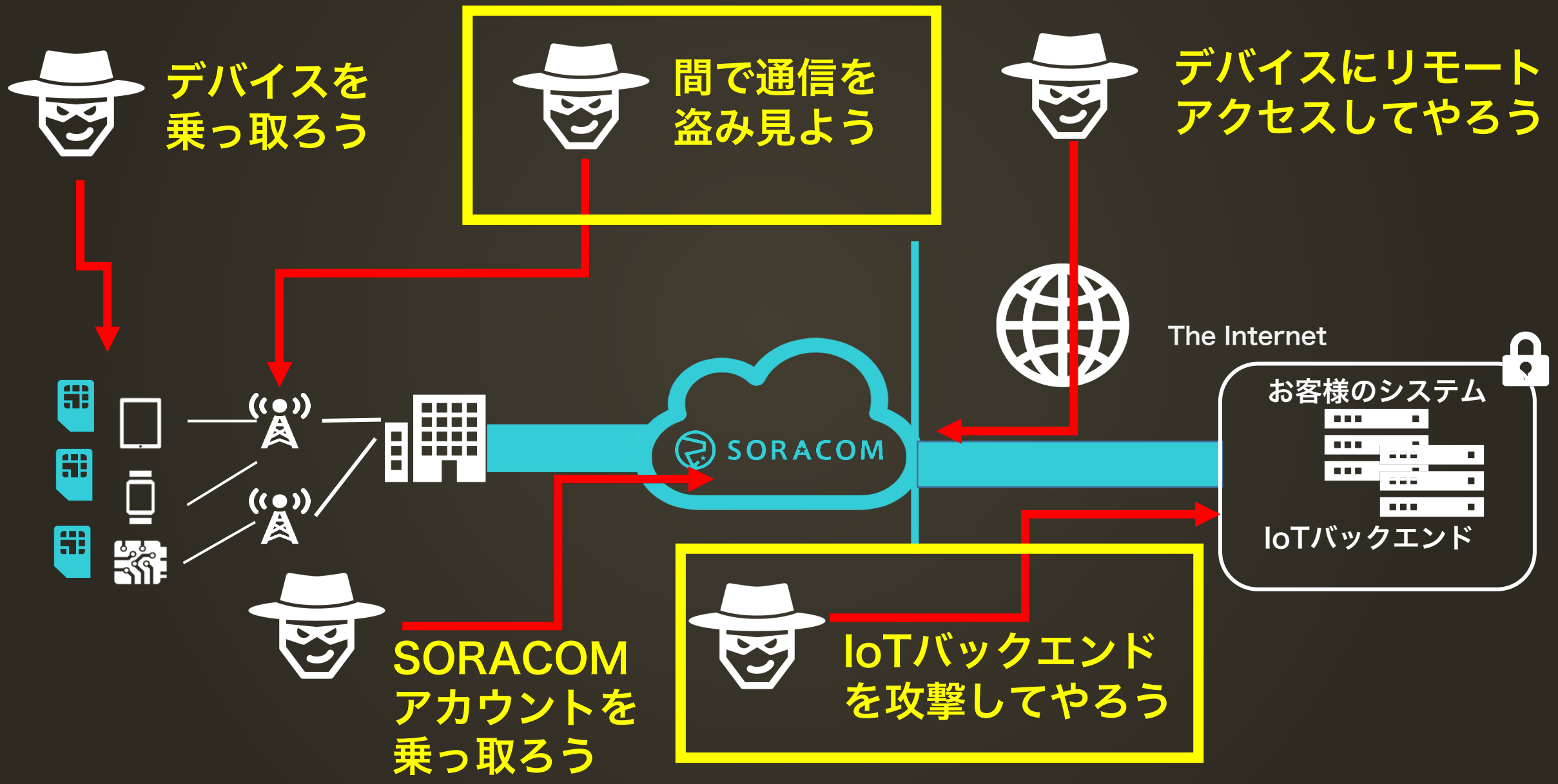
https://iot-device-insurance.tokiomarine-e.jp/

TOKIO MARINE NICHIDO

SORACOM Technology Camp 2020

《 デバイスの認証/認可 》

狙われるIoTシステム



- スマートフォンの場合
  - 人が認証情報を入力できる

- IoTデバイスの場合
  - IoTデバイス自身に認証情報を持たせる必要がある
    - 全デバイスで同じ認証情報 -> NG
    - デバイスごとに認証情報を持たせる
      - どのように認証情報を持たせるか?
      - 認証情報の漏洩をどう防ぐか？

SIMカード

SORACOM Technology Camp 2020

- 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
  - SIMごとにユニークIDが使える
- モバイル通信で認証と無線の暗号化を担保

SORACOM Technology Camp 2020

《アプリケーションの認証/認可》

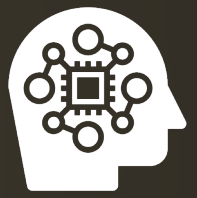
デバイスとクラウドの直接連携の問題点

SORACOM Technology Camp 2020

デバイス

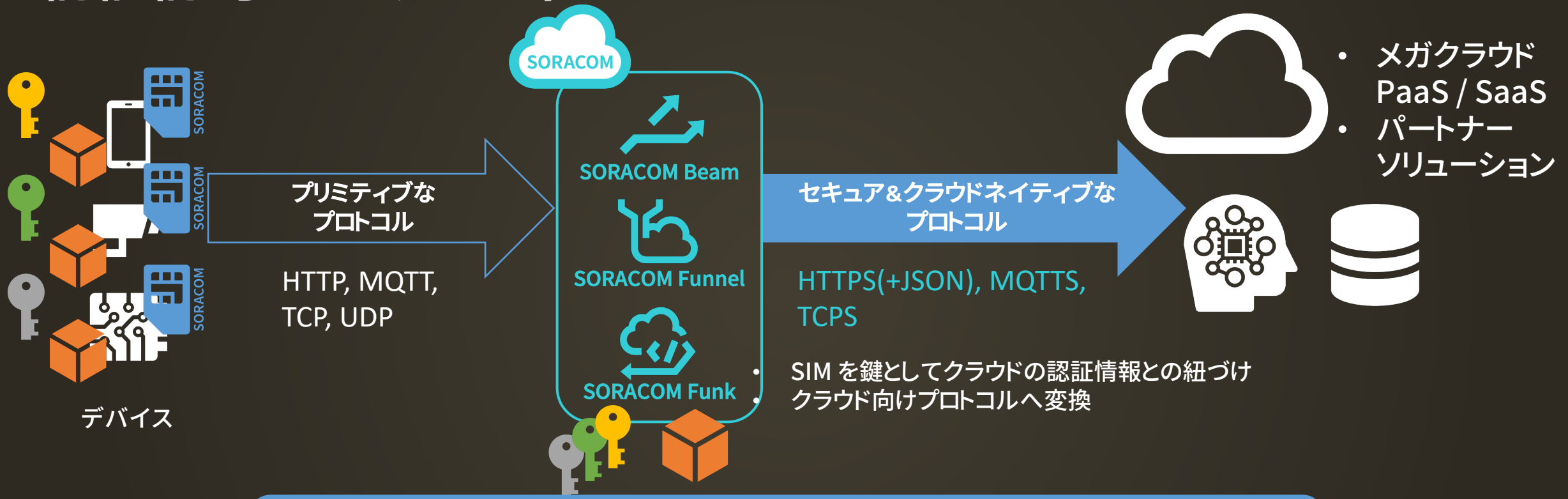
セキュア&クラウドネイティブな
プロトコル

- メガクラウド
  PaaS / SaaS
- パートナー
  ソリューション



SDK や認証情報のインストール
証明書などの更新作業

SORACOM Beam / Funnel / Funk による 認証認可のセキュア化



SDK や認証情報をデバイスから取り払ってシンプル化

セキュリティの向上

キーローテーションなどの工数削減

Beam/Funnel/Funkの利点

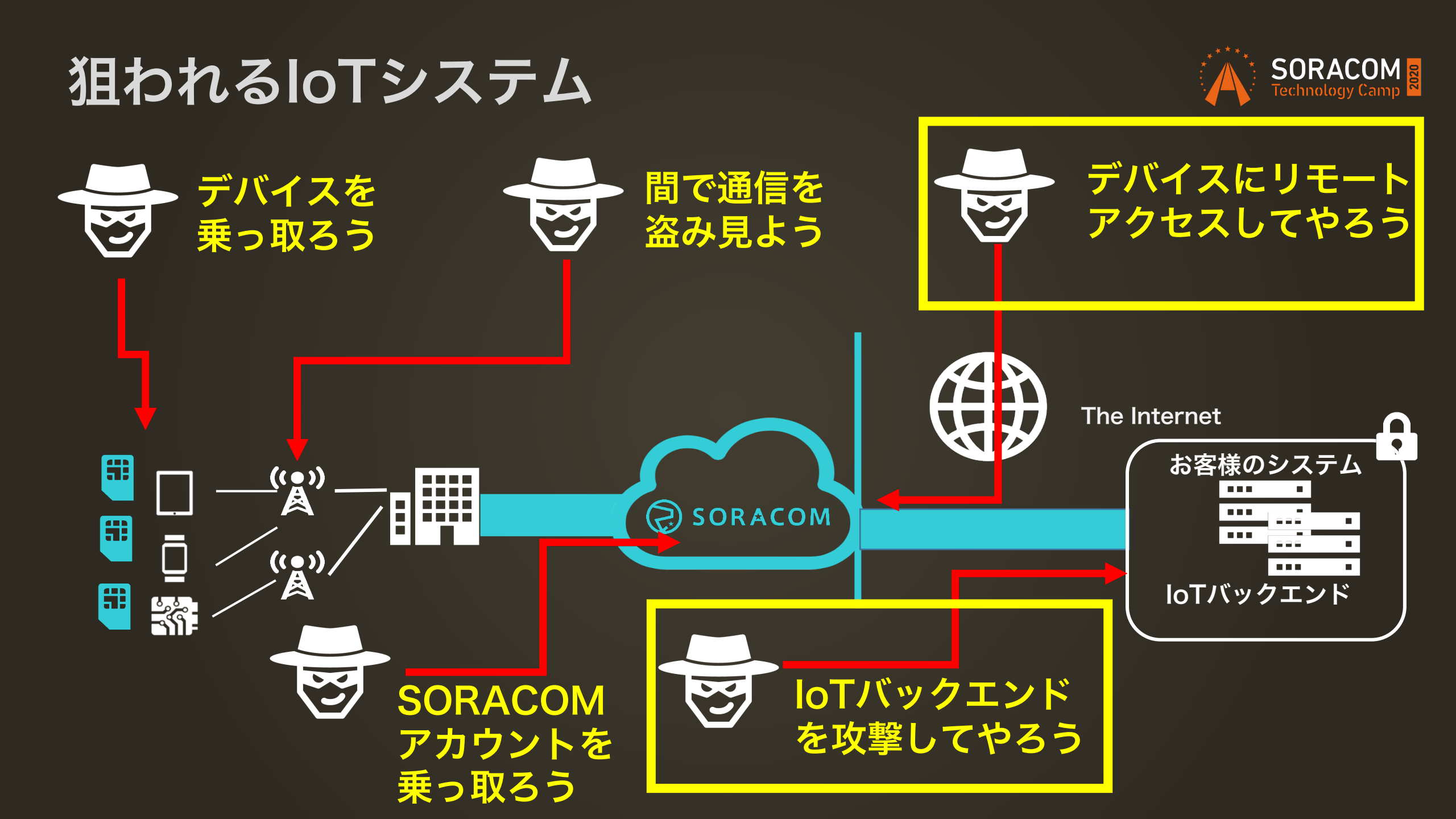
SORACOM Technology Camp 2020

- デバイス側には、SIM以外の認証情報が不要
  - デバイスごとに認証情報を入れる必要がない
  - クラウドに接続するためのSDKが不要
  - デバイス側をシンプルに保てる
- 実現できない処理
  - 対応クラウドサービス以外へのアクセス
    - 例：Amazon S3
  - セルラー通信以外の利用

SORACOM Technology Camp 2020

《 閉域網での接続 》

狙われるIoTシステム

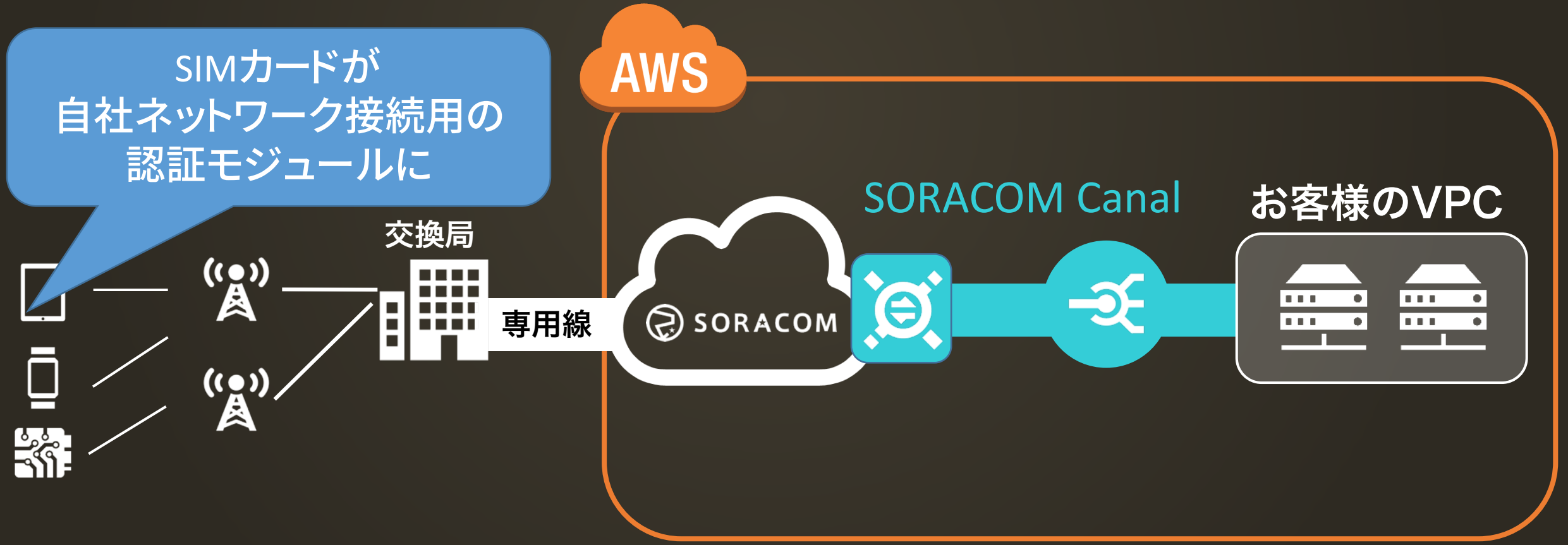


SORACOM Canal - AWS 閉域網接続

SORACOM Technology Camp 2020

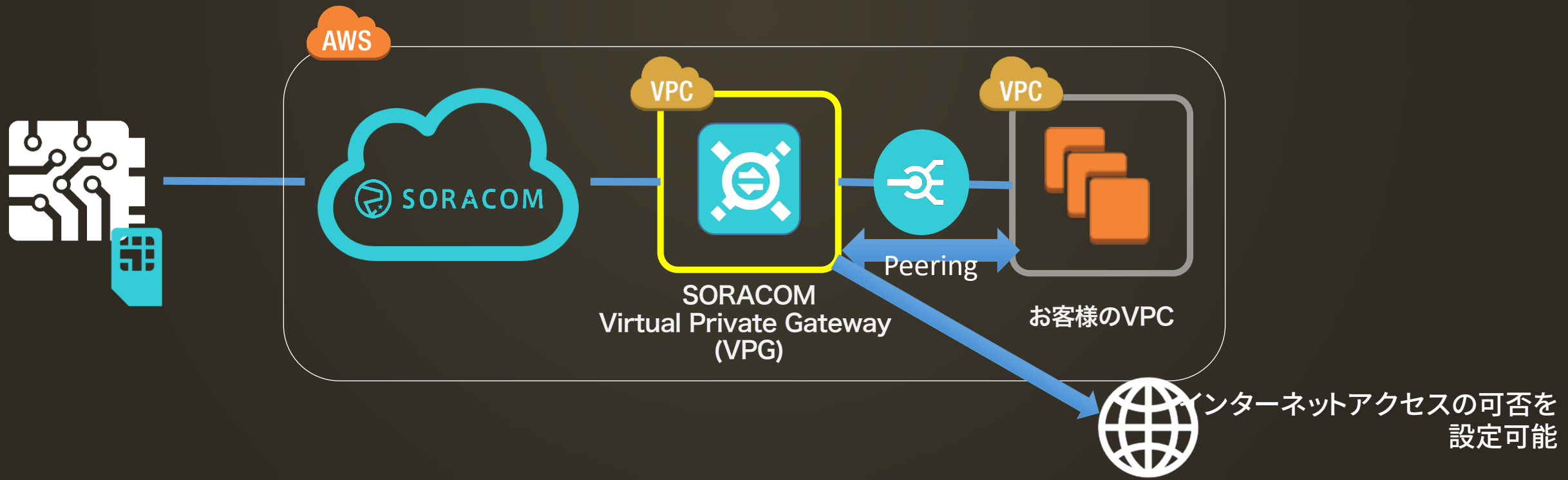
SORACOM の VPC とお客様の VPC との間でプライベート接続
インターネットを介さず、セキュアにデータ通信

※ 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



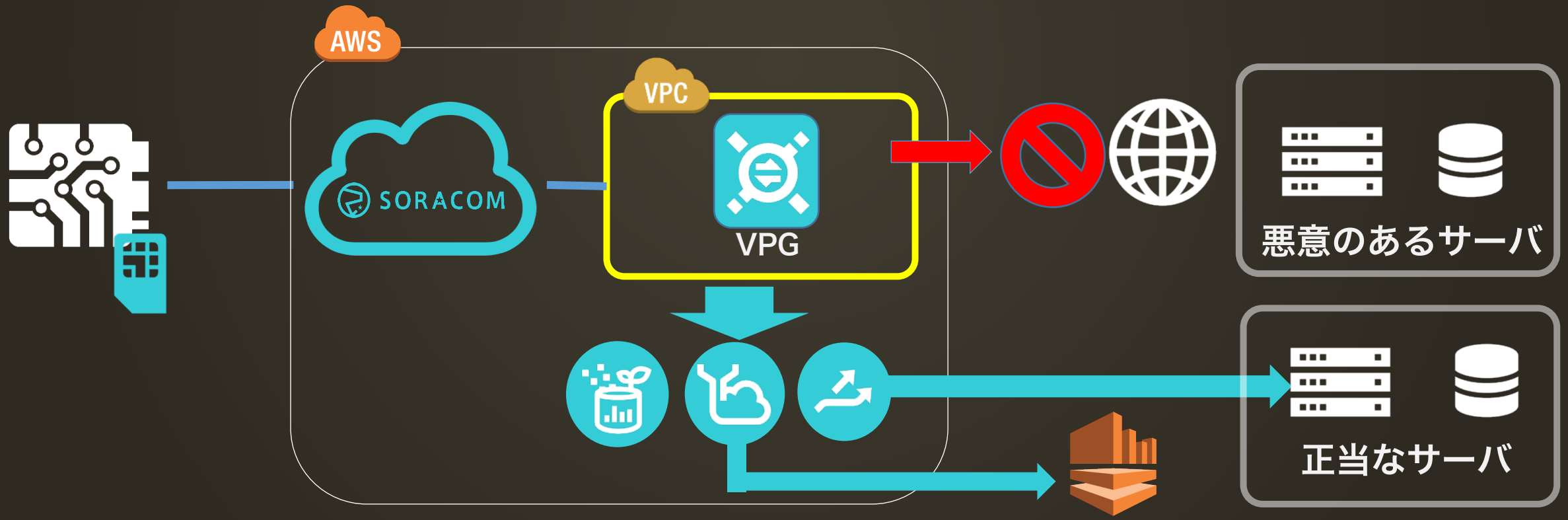
SORACOM Canalによる接続詳細

- 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



アウトバウンドの制御

- SIMから特定の接続先にしか接続できないよう制限が可能
- デバイスが意図せず外部に接続しないようにできる



```
pi@raspberrypi:~ $
```

Menu SORACOM Japan Support sorao@soracom.jp

+ Register SIM | Details | Actions

Raspberry | Any

Items 1 - 1 (1 selected)

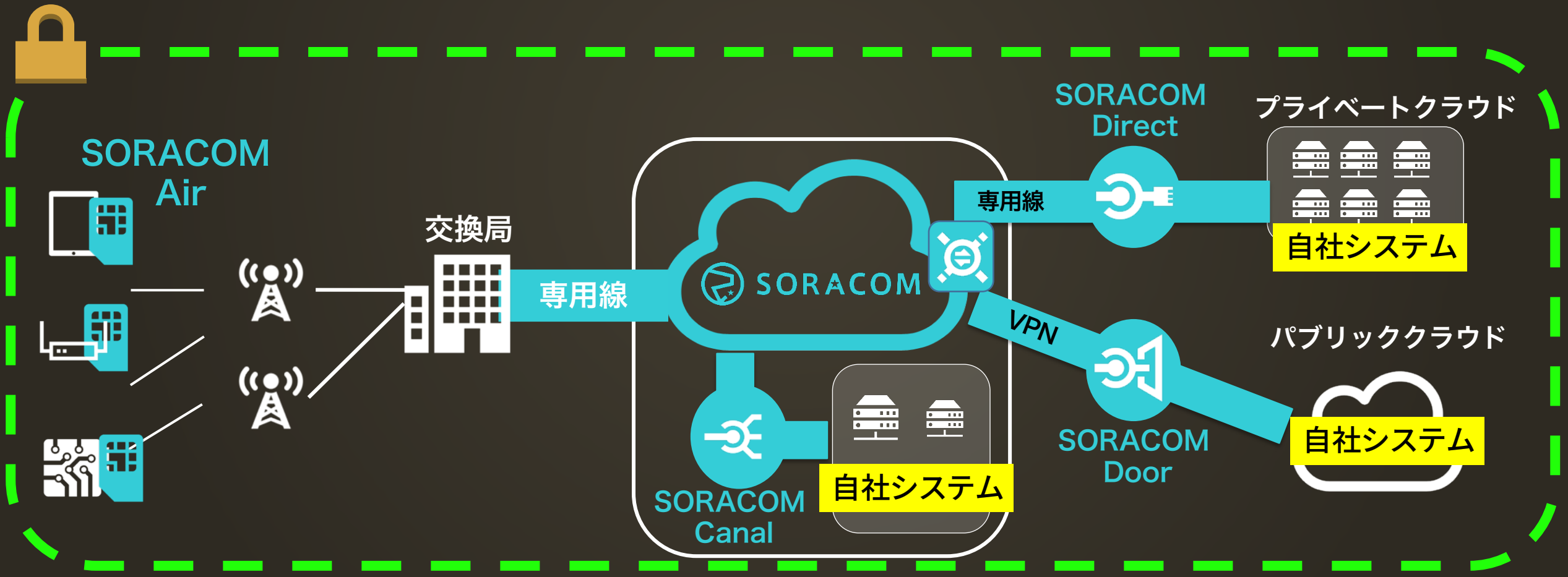
Previous Next

Name	Group	Status	Session	Plan	Speed class	Expiry Date / Time	IMEI Lock	TI
RaspberryPi		Active	Online		s1.fast	(Not specified)		

Items per page 100

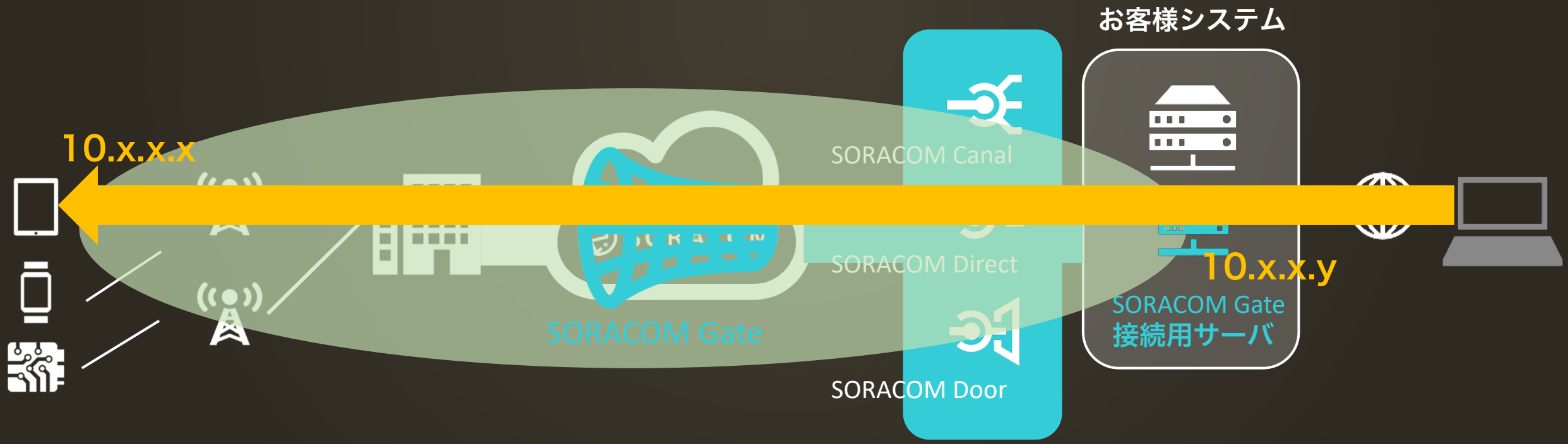
閉域網での接続

- 端末から自社システムまでの閉域網接続を容易に実現



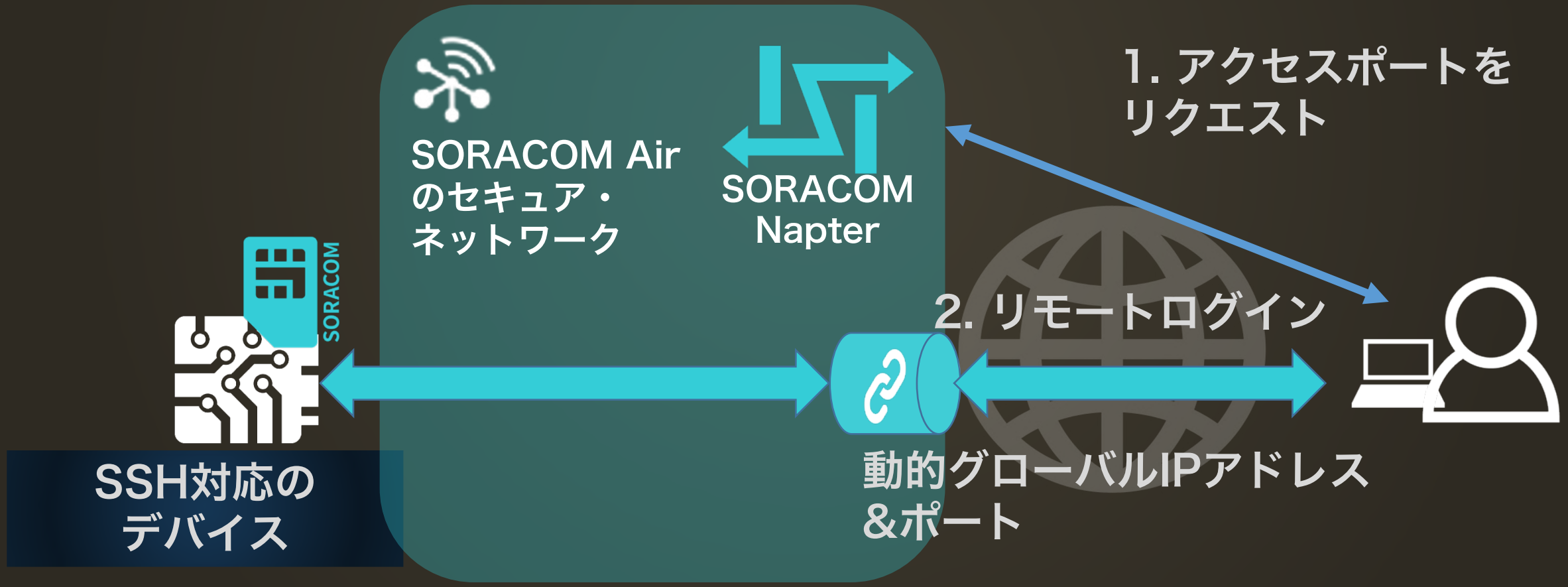
SORACOM Gate

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



SORACOM Nater

通常時は閉域、遠隔操作時だけ外部から接続



SORACOM Technology Camp 2020

《 通信の監視・制御 》

デバイスの乗っ取りリスク

SORACOM Technology Camp 2020

- 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

どう検知するか?

SORACOM Air

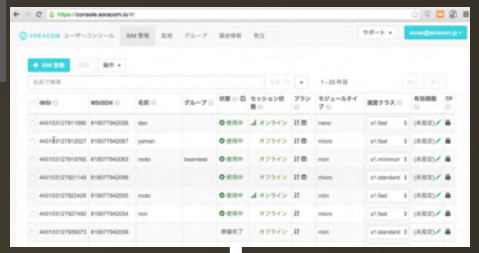
SORACOM Technology Camp 2020

お客様

① SIMを購入して モノに挿す

③Webから コントロール

Webコンソール



②APIでコントロール

API

SORACOM

専用線

NTTドコモ の交換局

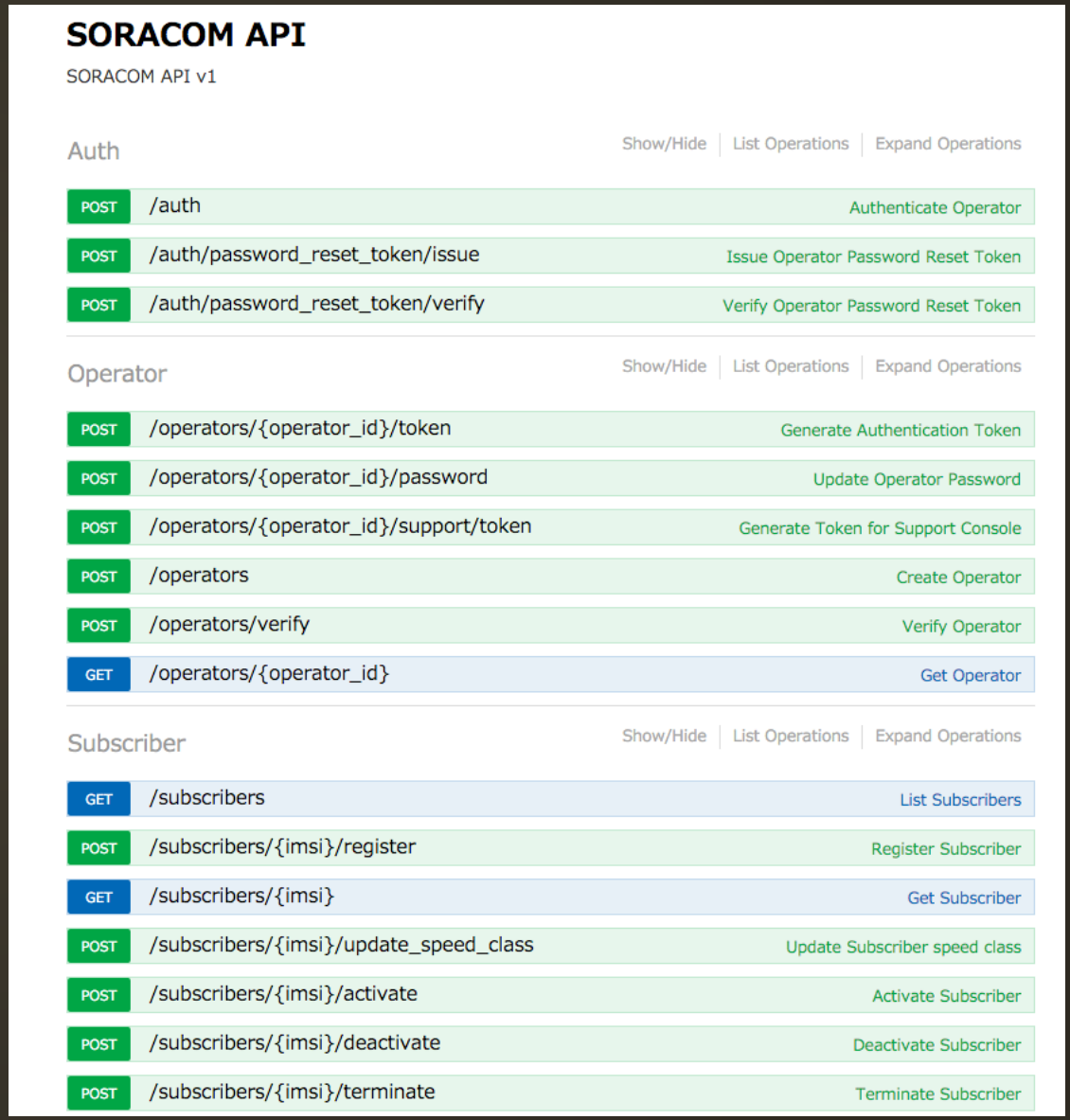
インターネット

SORACOM Air

SORACOM Technology Camp 2020

- 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

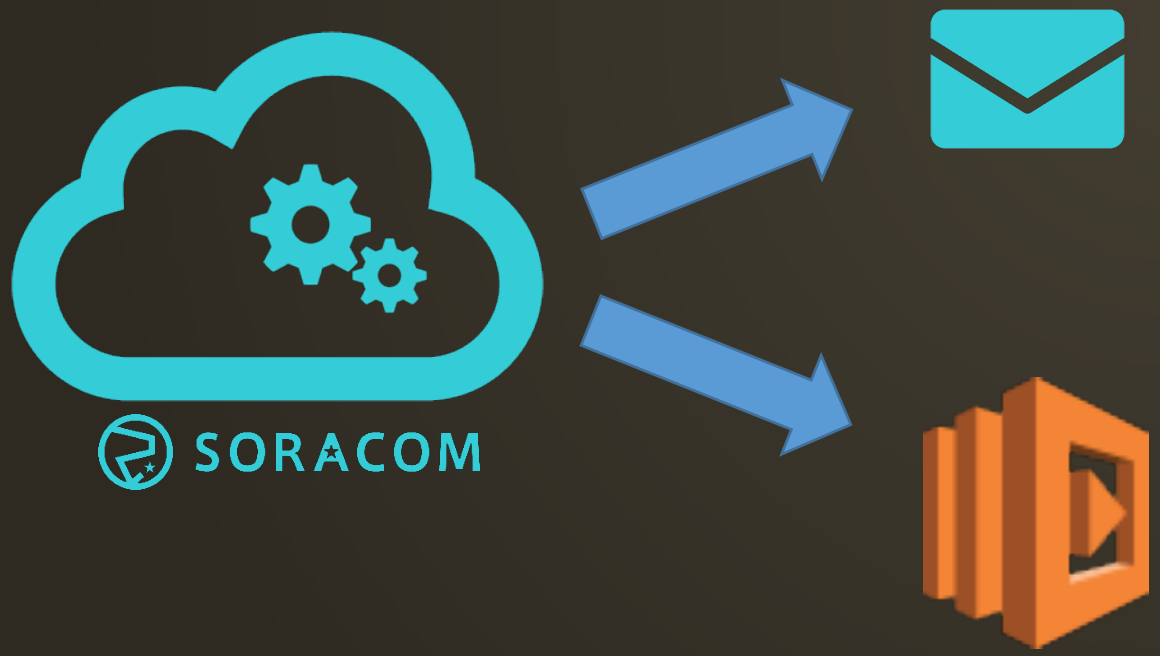
Subscriber — Show/Hide | List Operations | Expand Operations

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

SORACOM Technology Camp 2020

- 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

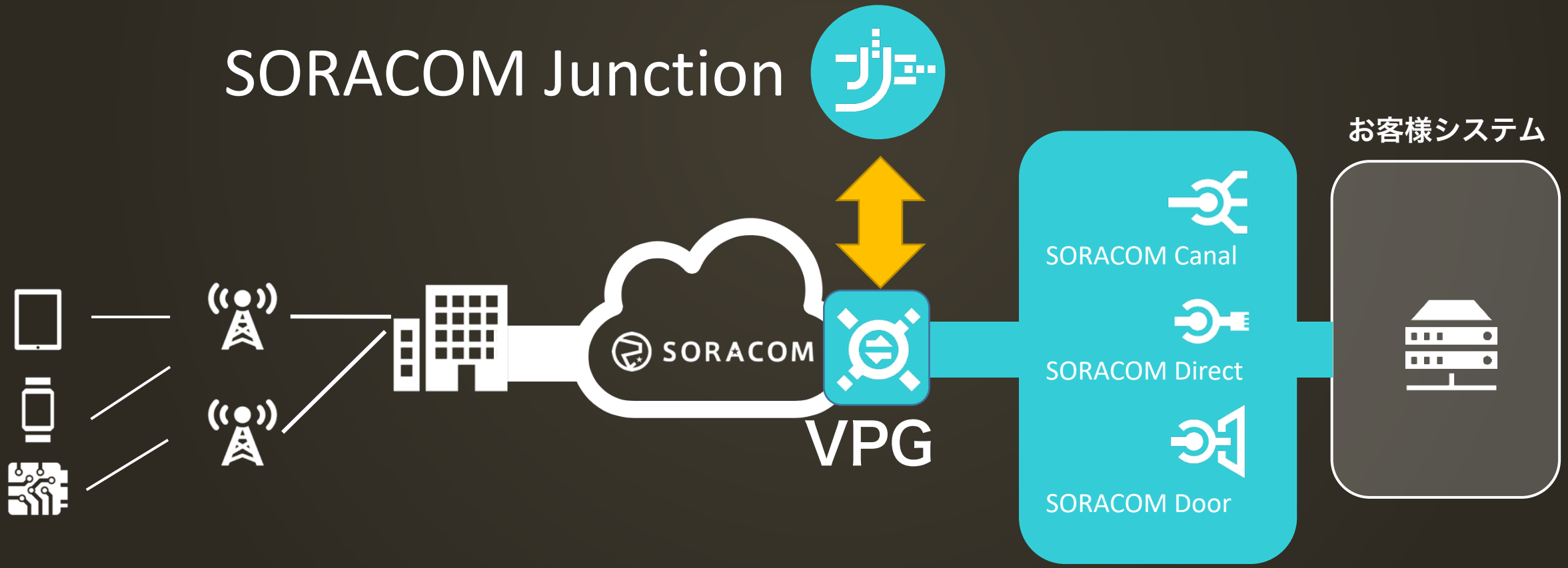


- SIMの1日の通信データ量が一定のしきい値を超えたらSIMを停止
- 通算のデータ通信量が一定のしきい値を超えたらSIM を解約

SORACOM Junction

SORACOM Technology Camp 2020

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

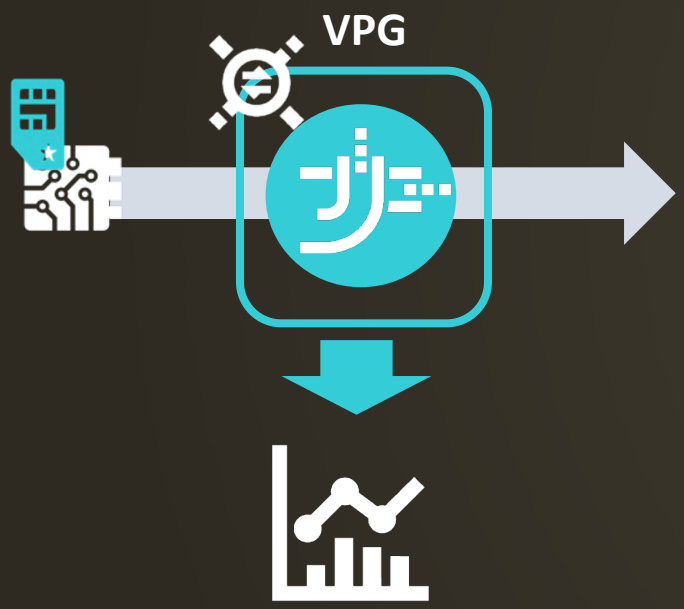


SORACOM Junction

3つのトラフィック処理機能

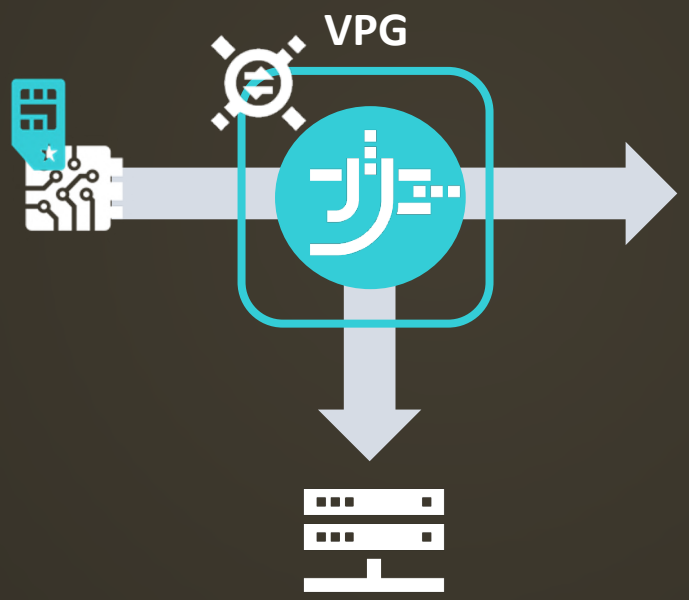
SORACOM Technology Camp 2020

Inspection



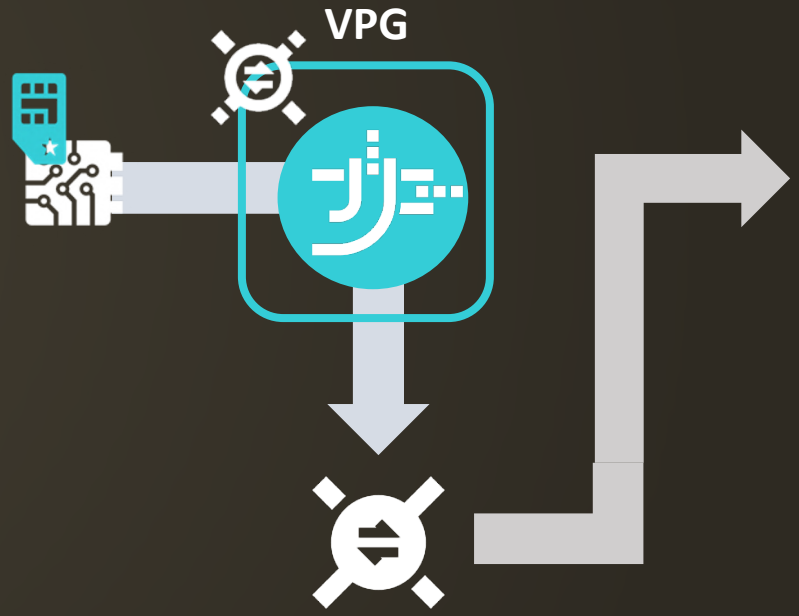
パケットフローを
解析して
統計情報を出力

Mirroring



パケットの
コピーを指定の
宛先に転送

Redirection

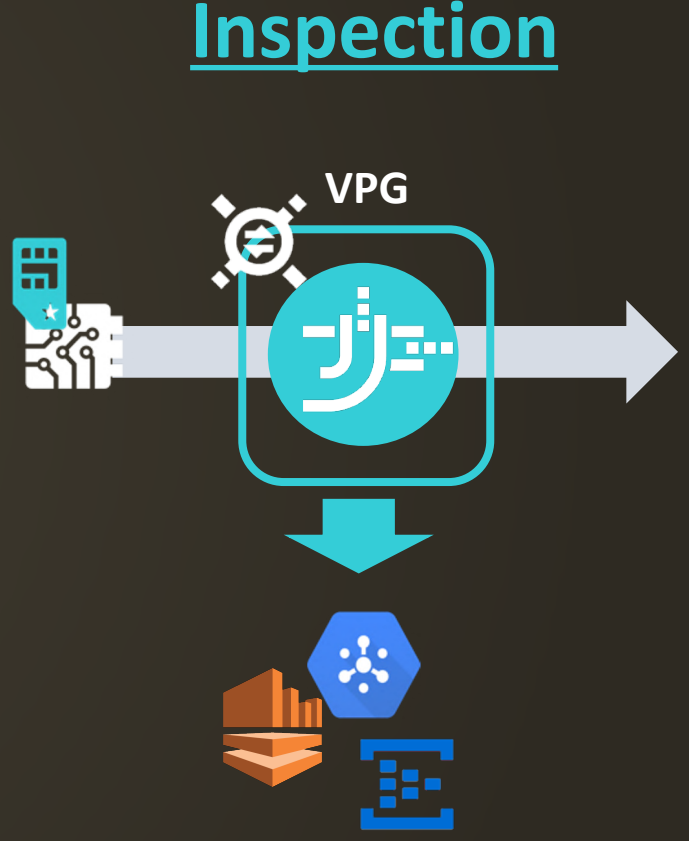


パケットを指定の
ゲートウェイ経由に
転送

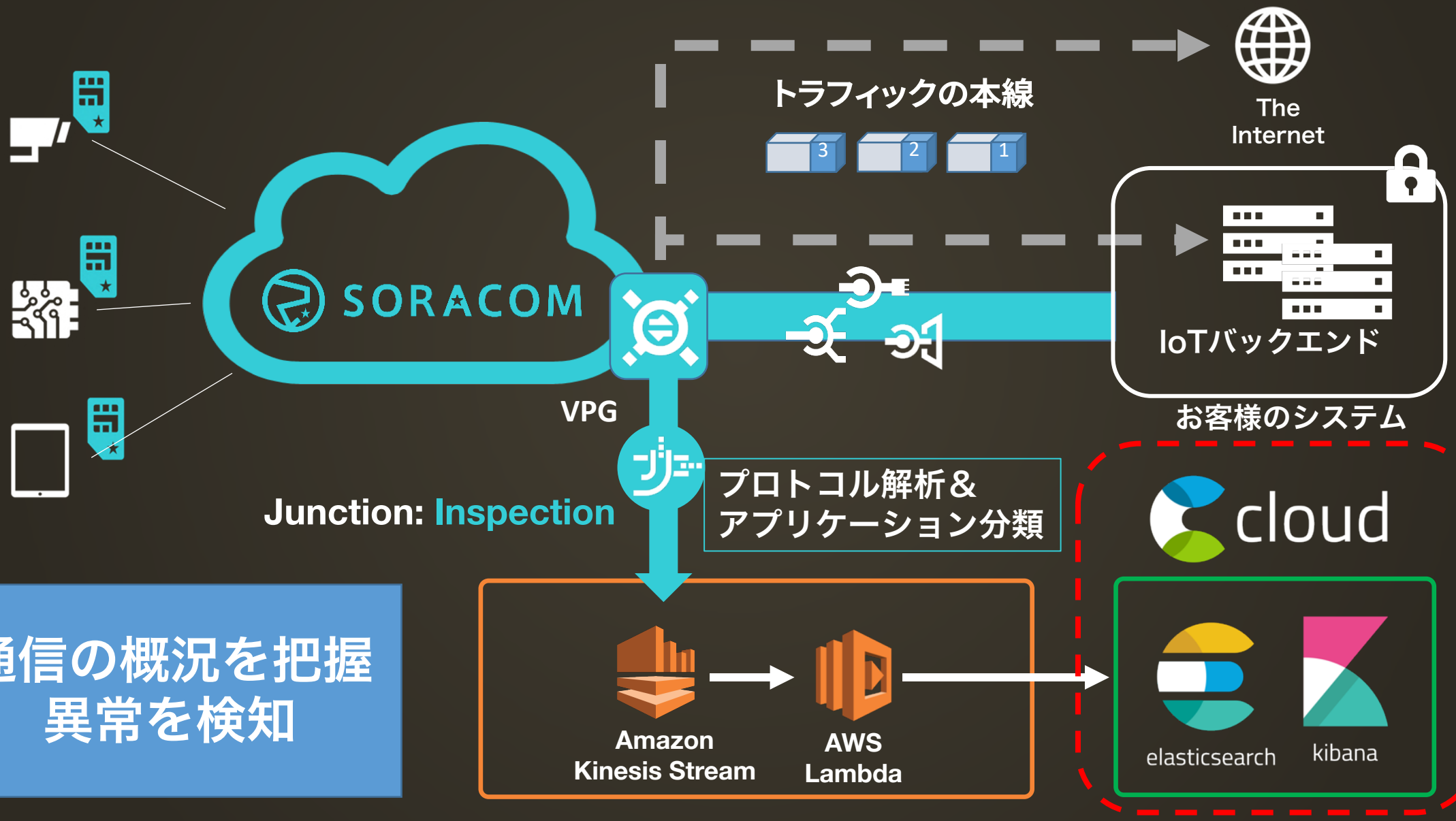
Inspectionの動作詳細

- 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
  - クレデンシャル

これらをFunnel同様に設定すれば出力開始



SORACOM Junction: Inspection



Soracom - Title

Realtime VPG Metric Monitor Running on Elastic Cloud

Soracom - Gauge Ethernet Bytes

Ethernet Bytes
4,546,117

Soracom - Gauge IP Bytes

IP Bytes
4,420,513

Soracom - Gauge Average Packet Size

Average Packet Size
451

Soracom - Gauge Max Packet Size

Max Packet Size
1,358

Soracom - Gauge > 0

Packets > 0
4,192

Soracom - Gauge > 64

Packets > 64
342

Soracom - Gauge > 128

Packets > 128
45

Soracom - Gauge > 256

Packets > 256
129

Soracom - Gauge > 1024

Packets > 1024
5,759

Soracom - Gauge > 1500

Packets > 1500
0

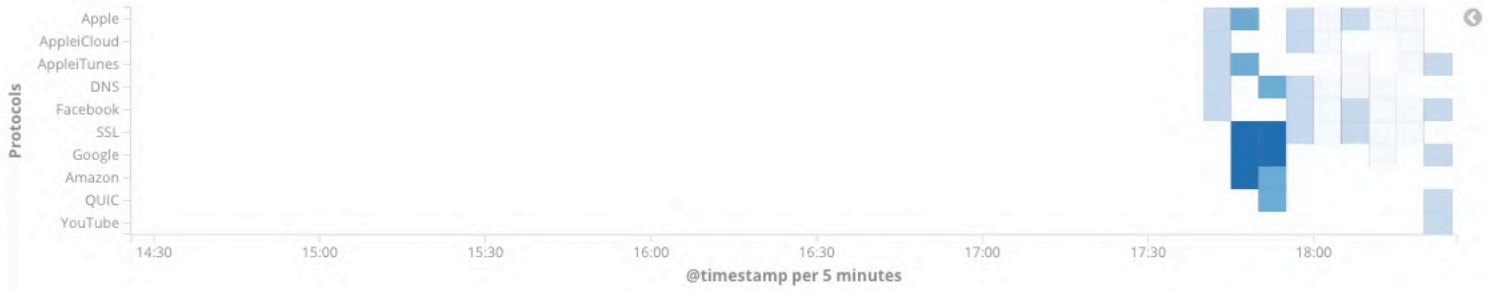
Soracom - Bar Bytes

Soracom - Tag Cloud Protocols

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

NTP Google Facebook DNS SSL HTTP QUIC NetFlix Amazon Apple ICMP YouTube AppleiCloud Twitter Instagram

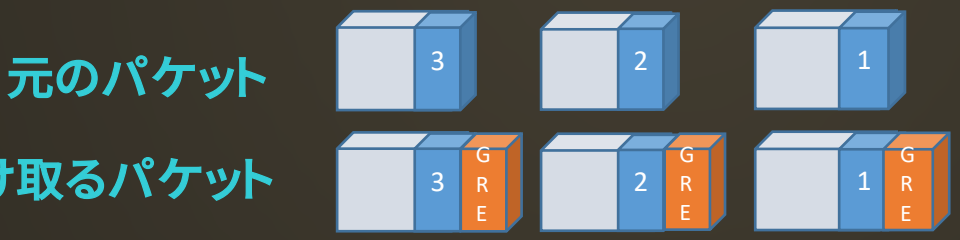
Soracom - Swimlane Protocols



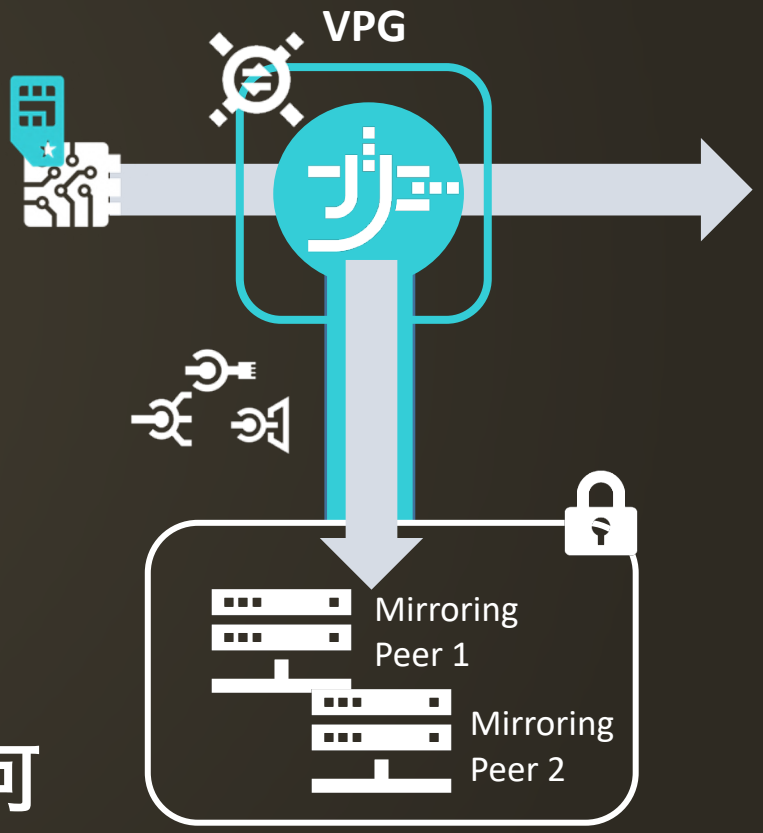
Mirroringの動作詳細

- 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

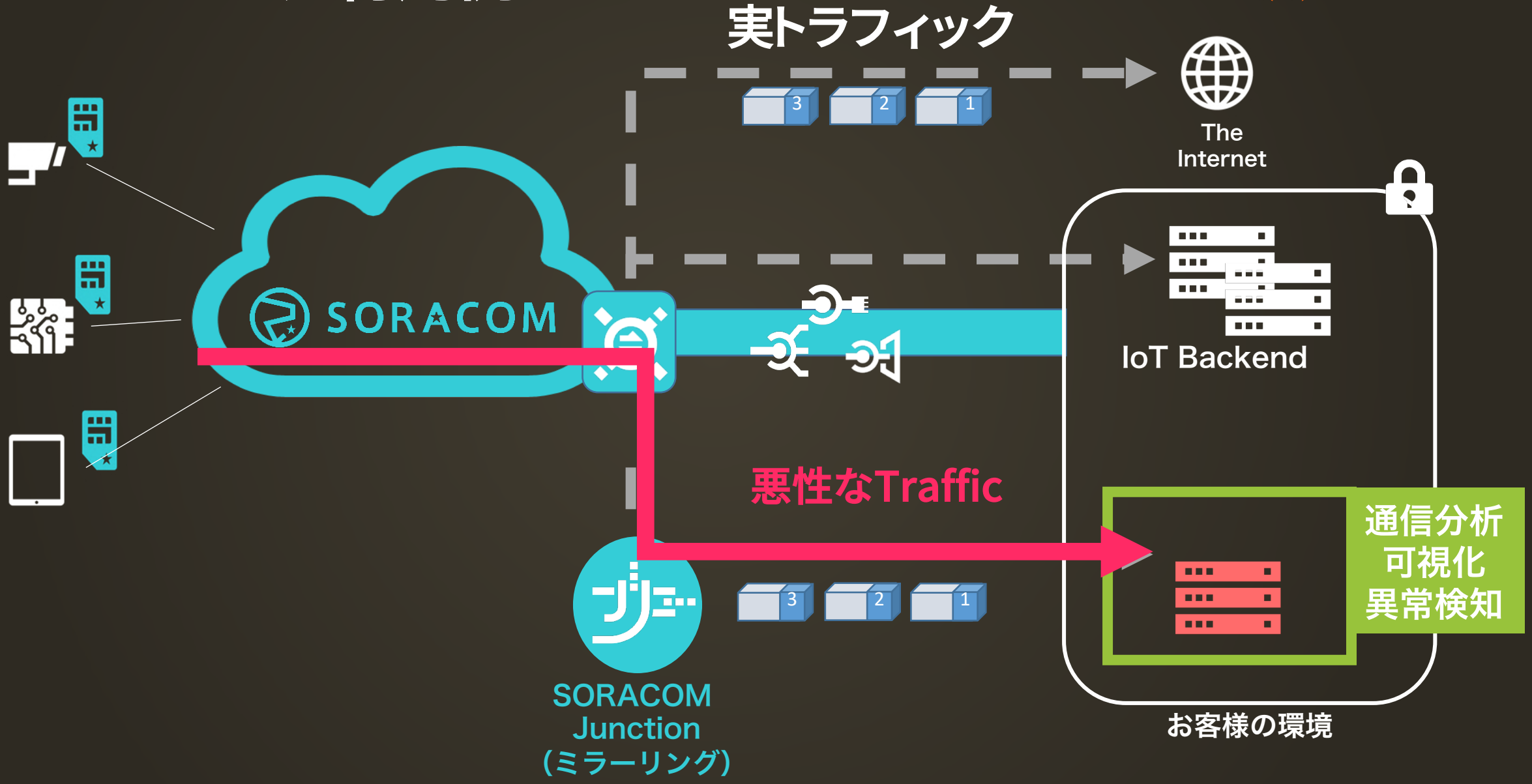
- コピーされたパケットはGREでカプセル化されて届く



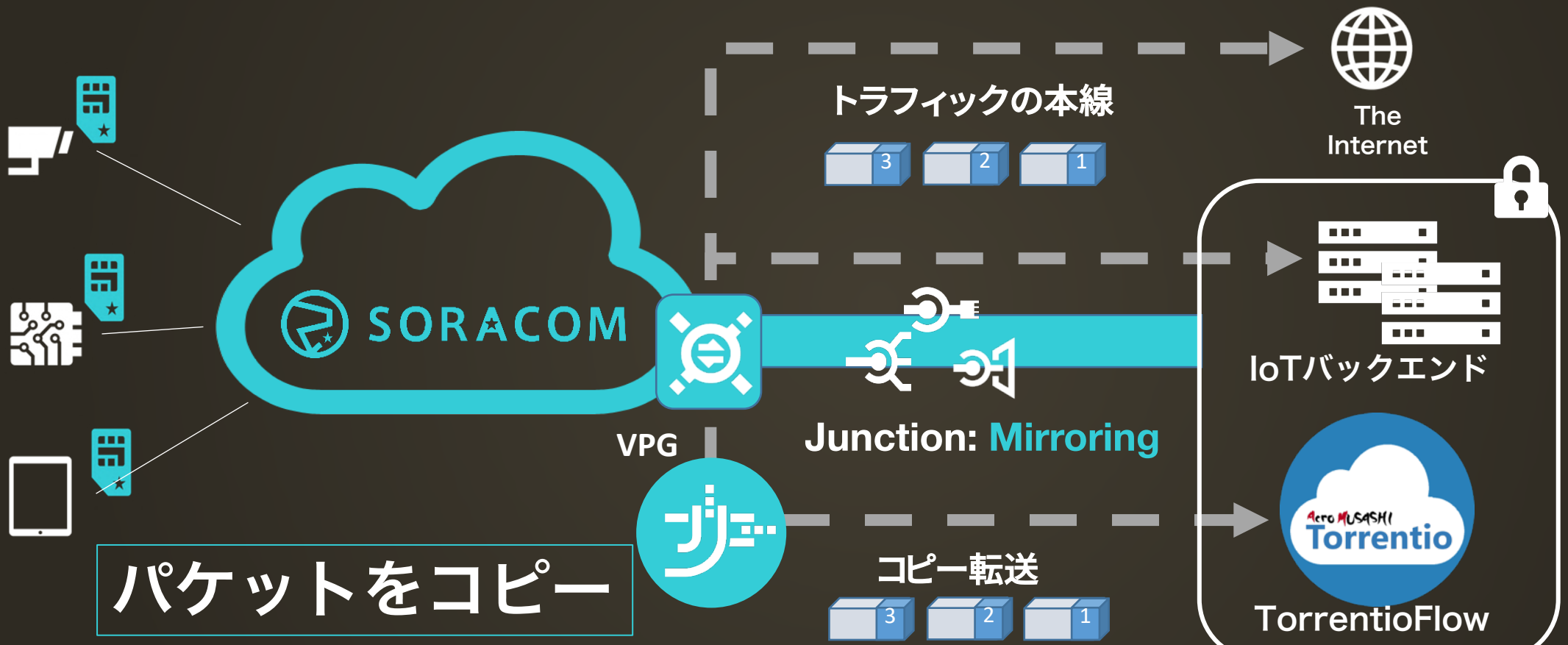
- Mirroring PeerはGREを受信できるように設定することでトラフィックをモニタリング可



ミラーリング利用例


実トラフィック
3
2
1
The Internet
SORACOM
IoT Backend
悪性なTraffic
3
2
1
通信分析
可視化
異常検知
SORACOM
Junction
(ミラーリング)
お客様の環境

パートナー様ソリューションの利用例



- 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

パートナー様ソリューションの利用例

SORACOM Technology Camp 2020

SIMごとの通信状況を
一目で確認できる

異常検知の結果を
分かりやすく可視化

異常な通信データ

トラフィックの本線

3 2 1

The Internet

IoTバックエンド

ion: Mirroring

ピー転送

2 1

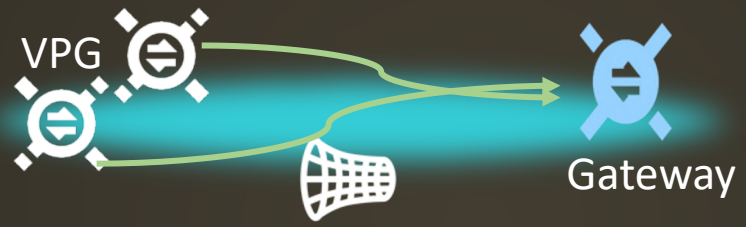
Aero MUSASHI Torrentio

TorrentioFlow

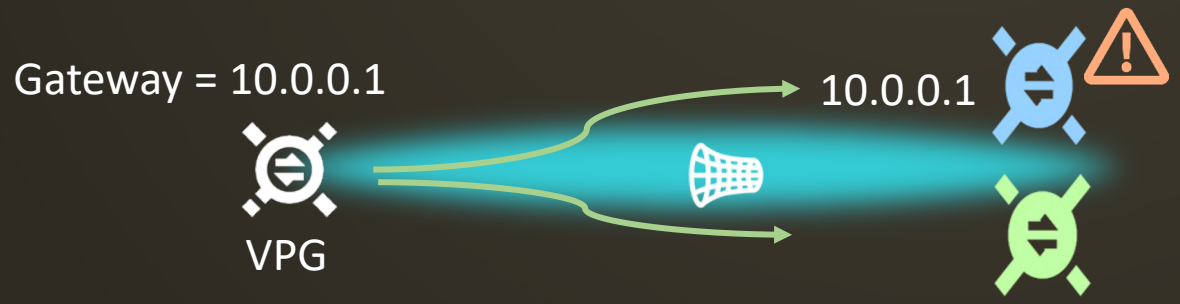
- 個別フローのリアルタイム分析・可視化
- 機械学習による異常検知・リスク分析
- 異常の通知

Redirectionの動作詳細

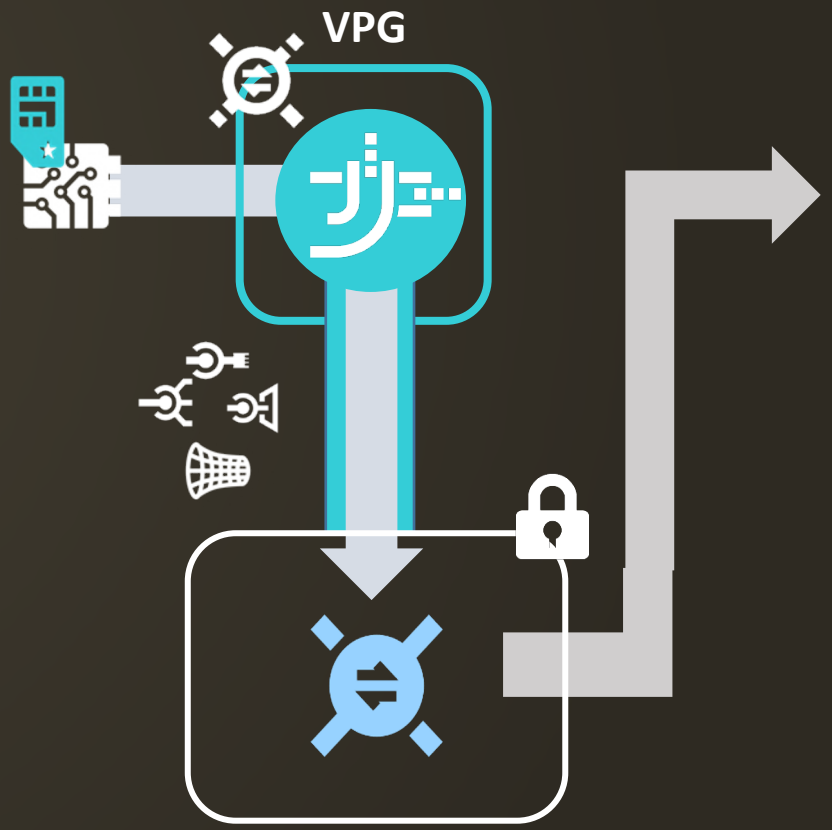
- 仮想L2サブネット上のPeerをGatewayとしてパケットを転送
  - vxlanに対応



- 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



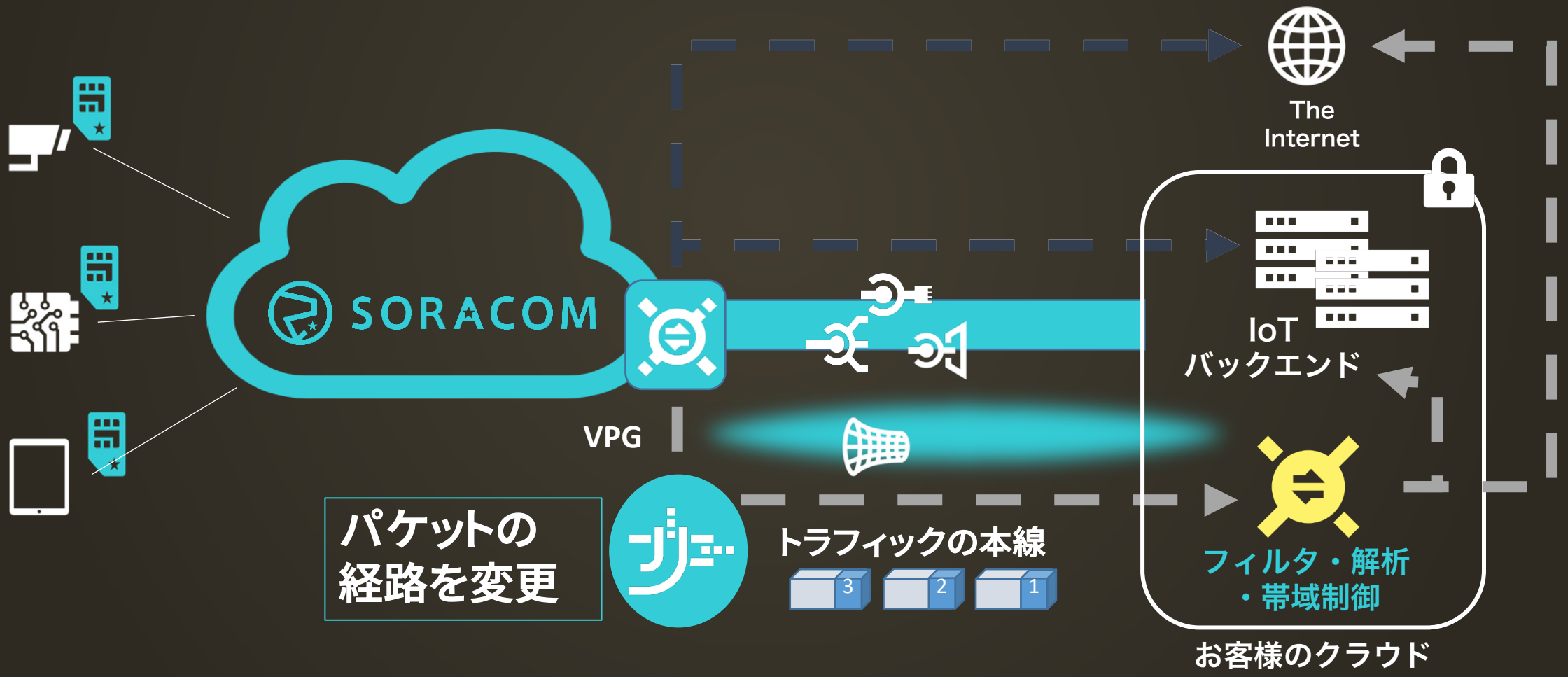
Redirection



SORACOM Junction: Redirection

SORACOM Technology Camp 2020

・パケットを指定のゲートウェイ経由で転送



Junctionパートナーソリューション例

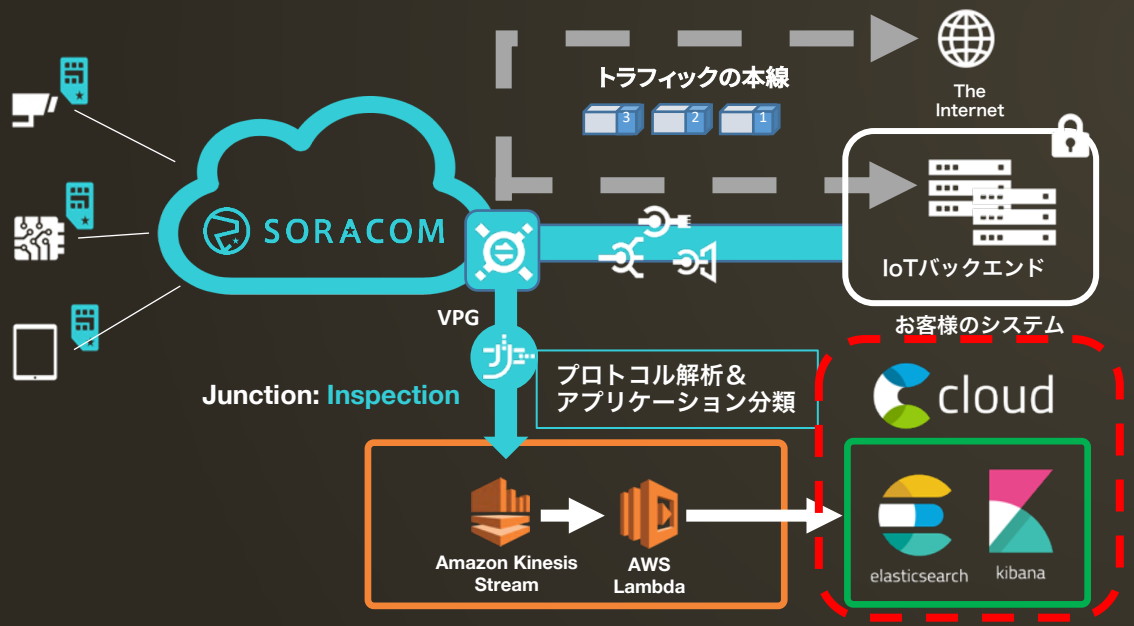
SORACOM Technology Camp 2020

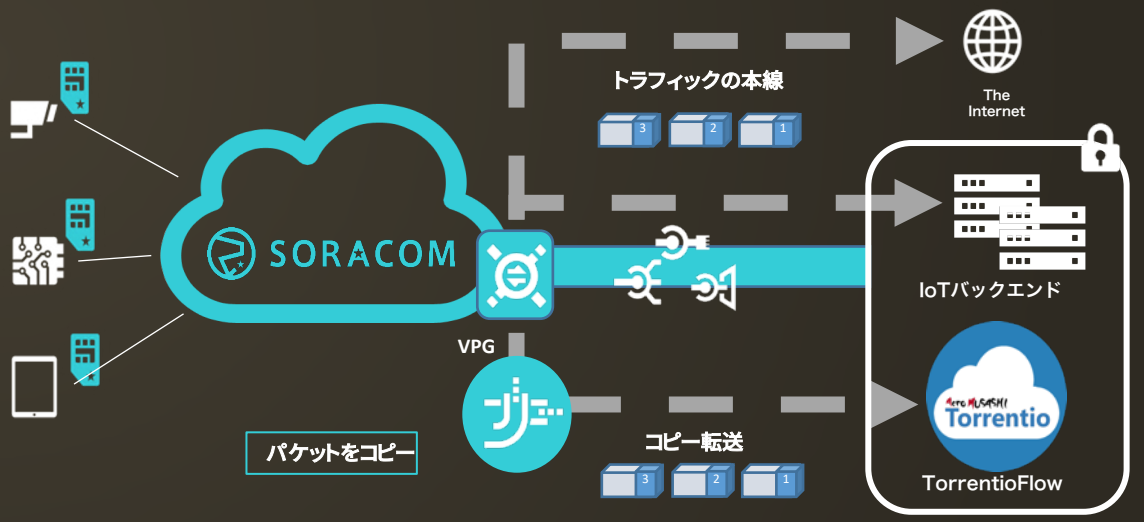
- Junction: MirroringによるDPI、IPS、可視化
  - Palo Alto Networks社
    - VM-Series
  - Sandvine社
    - Procera PacketLogic

Junctionを利用したパケット解析

SORACOM Technology Camp 2020

パートナーソリューションと組み合わせることで、デバイスの異常検知や乗っ取り検知が可能



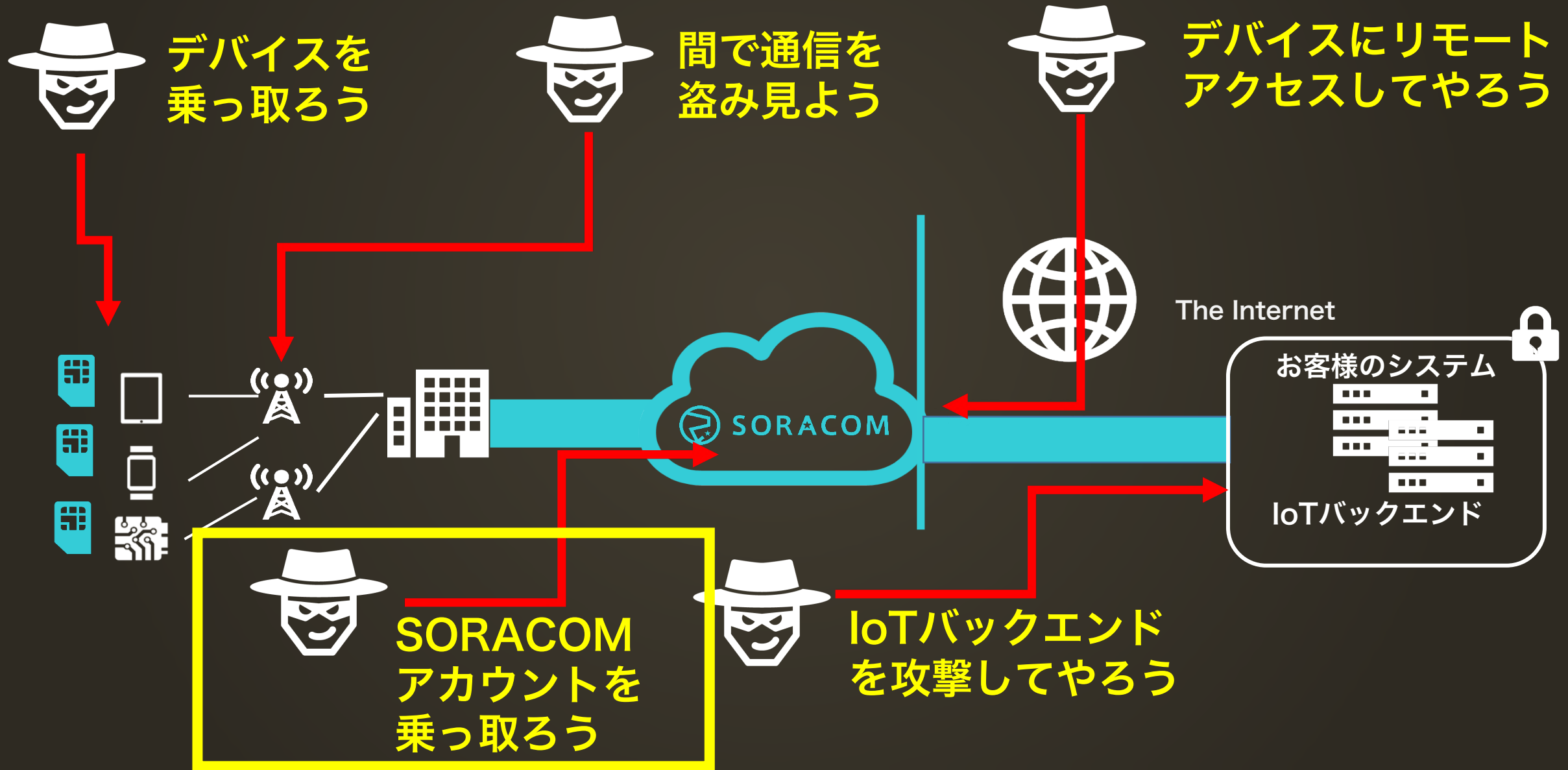


- 個別フローのリアルタイム分析・可視化
- 機械学習による異常検知・リスク分析
- 異常の通知

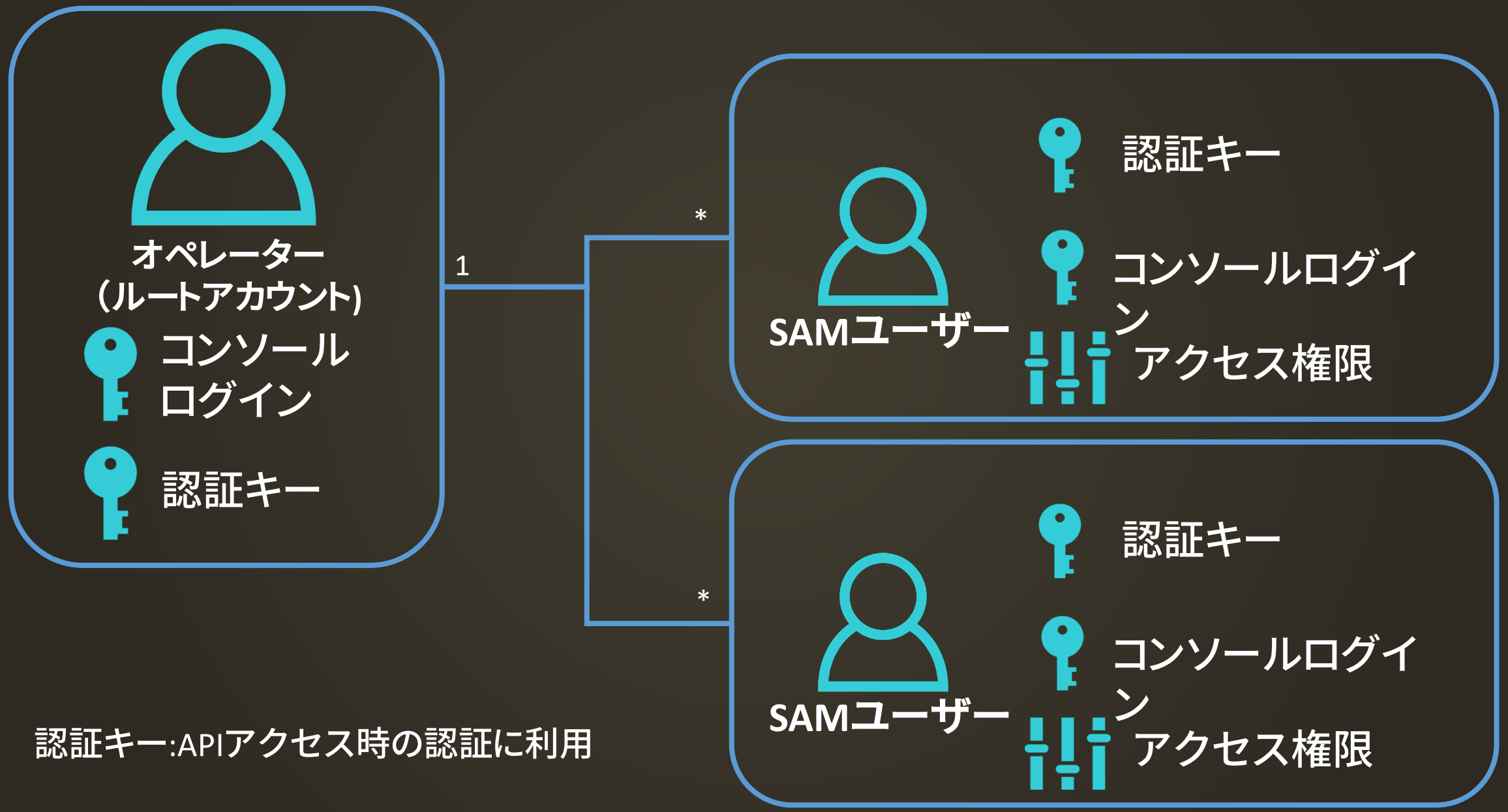
SORACOM Technology Camp 2020

《 SORACOMアカウントの保護 》

狙われるIoTシステム



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

SORACOM Technology Camp 2020

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

ユーザーごとのアクセス権限管理(例)

SORACOM Technology Camp 2020

- 開発者
  - コンソールログインと認証キーを許可
  - SIMの解約はNG

- 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

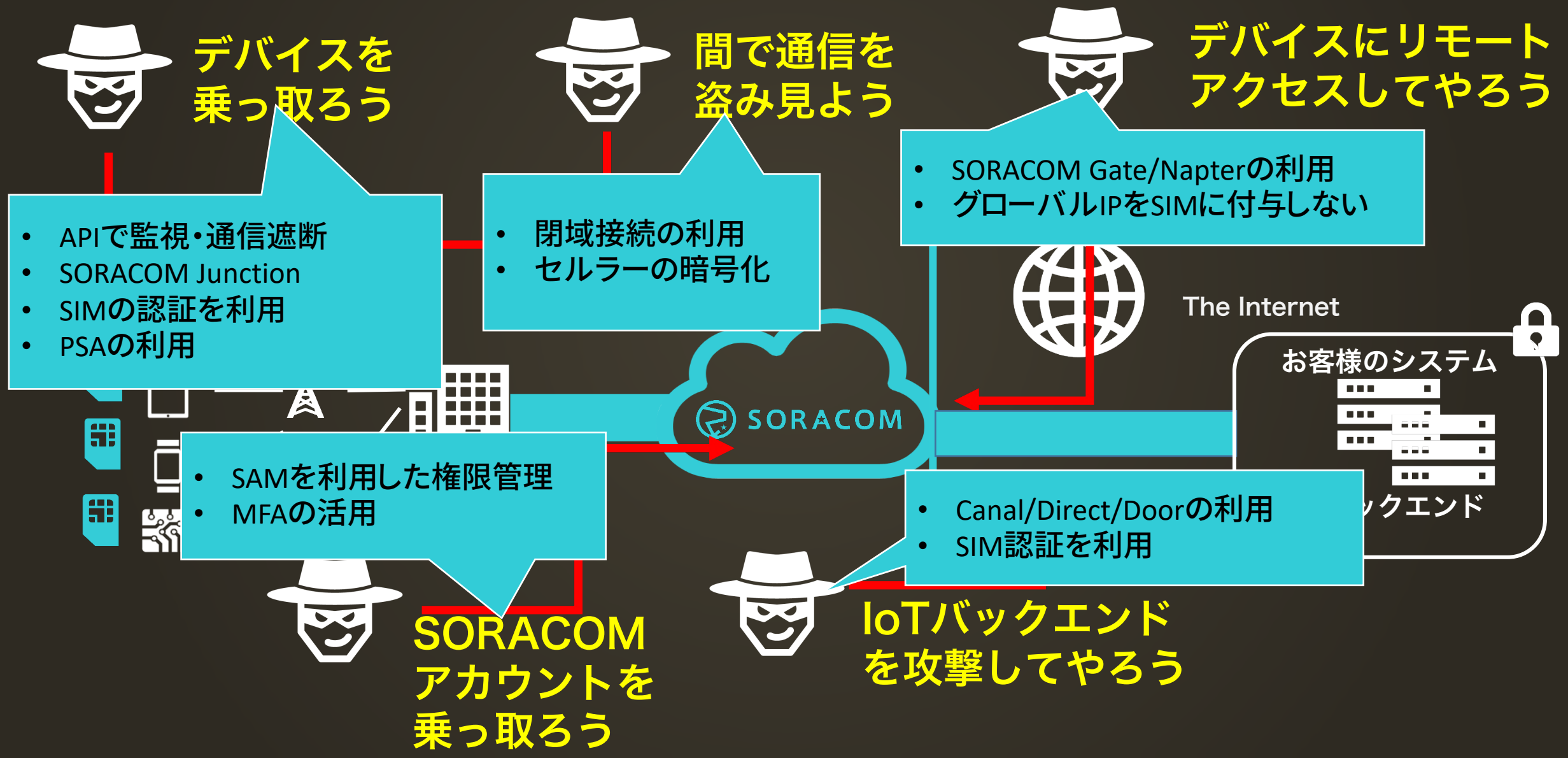
SORACOM Technology Camp 2020

コンソールログイン時にMFA(多要素認証)が利用可能

SORACOM Technology Camp 2020

《 まとめ 》

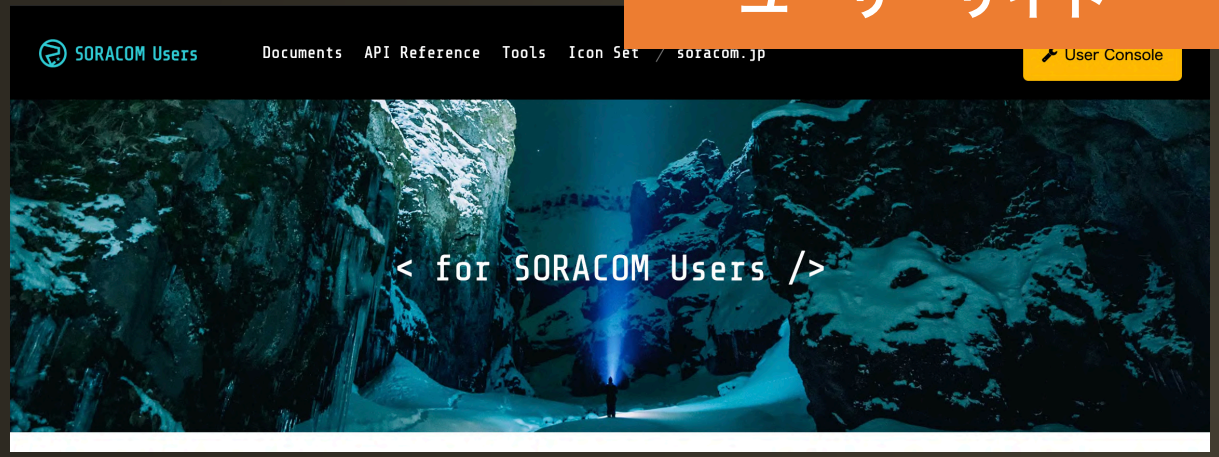
狙われるIoTシステム



ユーザーサイト・ブログのご紹介

SORACOM Technology Camp 2020

ユーザーサイト



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の願い

SORACOM Technology Camp 2020

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

SORACOM Technology Camp 2020

世界中のヒトとモノをつなげ
共鳴する社会へ

SORACOM