SORACOM

SORACOM Conference
"Discovery"

IoT通信の監視・制御・セキュリティの選択肢
～SORACOM Junctionの活用～

トレンドマイクロ株式会社 IoT 事業推進本部 ソリューション推進部 津金 英行 様
東京大学 大学院情報学環 大学院学際情報学府 教授 中尾 彰宏 様
株式会社ソラコム ソフトウェアエンジニア 福島 拓
株式会社ソラコム CTO 安川 健太

2017 July 5th

Thanks to our Sponsors

SORACOM Conference "Discovery"

Platinum

class method
infoteria
uhuru
Orchestrating a brighter world NEC

Gold

HITACHI Inspire the Next
HANDS LAB
amazon web services
オージス総研
b-en-g
I-O DATA
TREND MICRO
life.augmented
MAGLAB

Silver

aroba 株式会社アロバ
WingArc 1st
we connect
株式会社ヴァル研究所
Serverworks
HULFT DataSpider
PALTEK
OPTEX Sensing Innovation
MKI 三井情報株式会社
加賀デバイス株式会社
Infocorpus
GiSupply
HIOKI
elecs エレックス工業株式会社
elastic
ComDesign
brains
ACCESS

SORACOM Conference "Discovery"

本日のハッシュタグ

#discovery2017

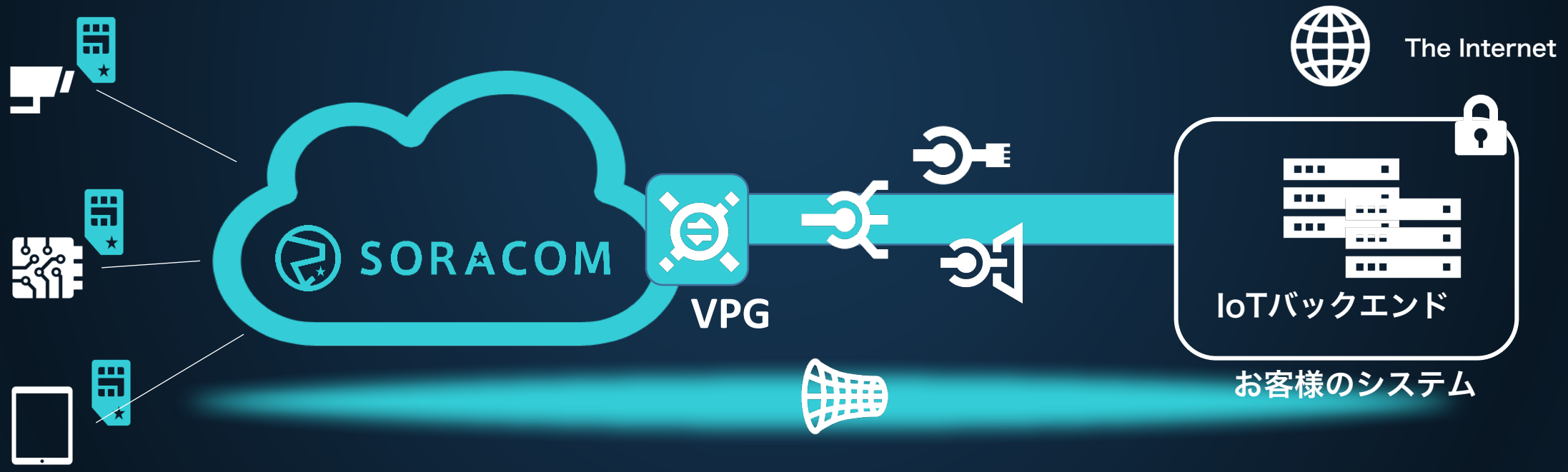
@SORACOM_PR

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

SORACOMのネットワークサービス

SORACOM Conference "Discovery"

- Amazon VPCとプライベート接続 → SORACOM Canal
- プライベートクラウドと専用線／VPN接続 → SORACOM Direct/Door
- デバイスとサーバを単一の仮想L2サブネットに接続 → SORACOM Gate



Virtual Private Gateway (VPG)を通してお客様のシステムと接続

お客様の声に耳を傾けると

SORACOM Conference "Discovery"

- 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？

お客様が自分のデバイスの通信だけを自由に監視・制御できる仕組みは作れないか？

SORACOM Conference "Discovery"

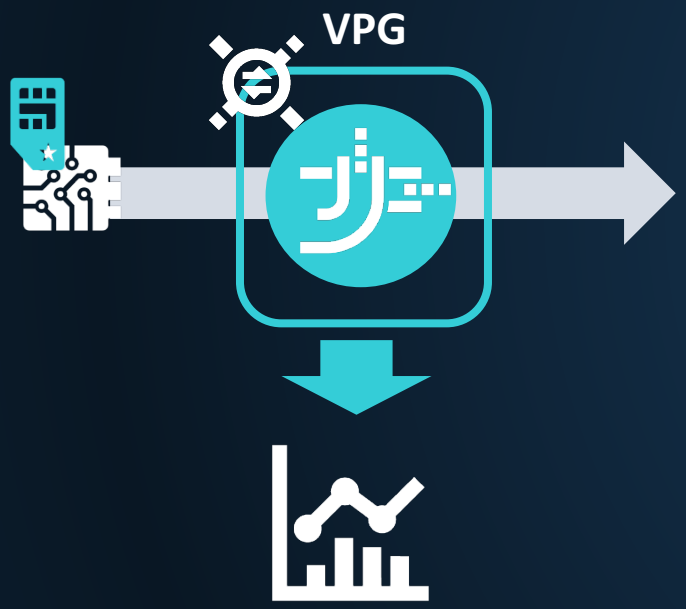
SORACOM Junction

透過型トラフィック処理サービス

SORACOM Junction：
VPGに追加される3つのトラフィック処理機能

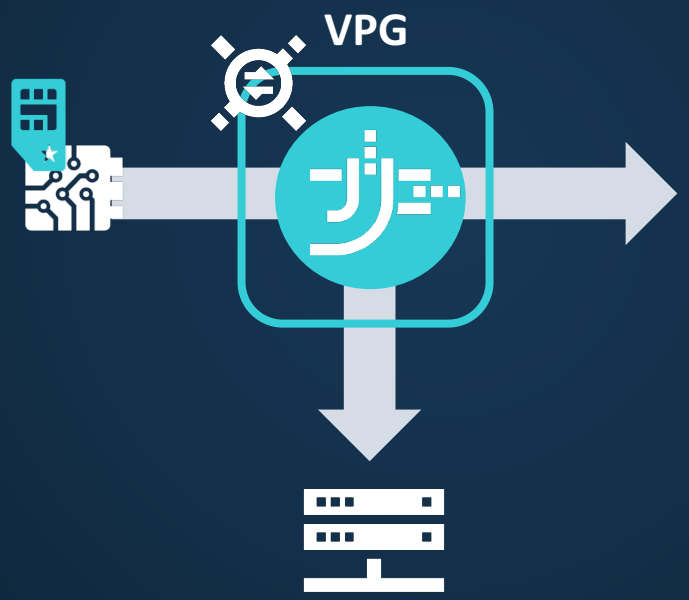
SORACOM Conference "Discovery"

Inspection



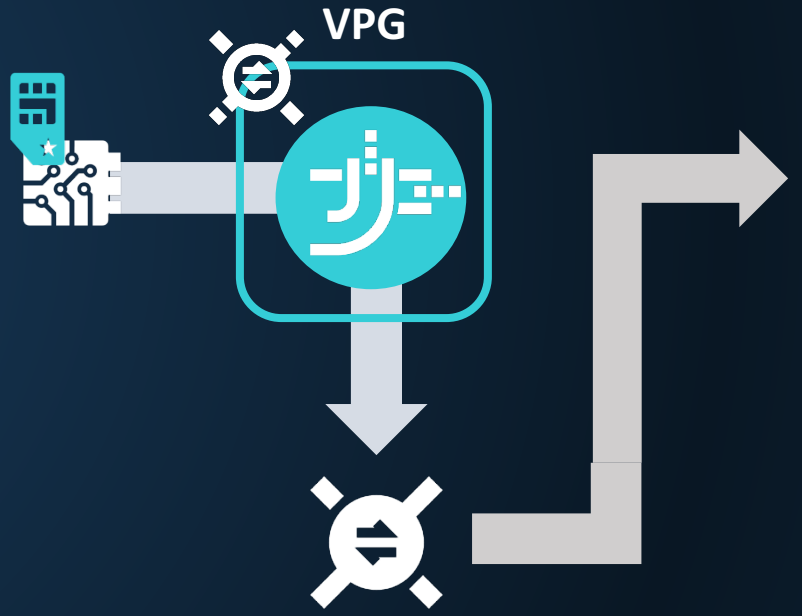
パケットフローを解析して
統計情報を出力

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

SORACOM Junctionでお客様の声にお応え

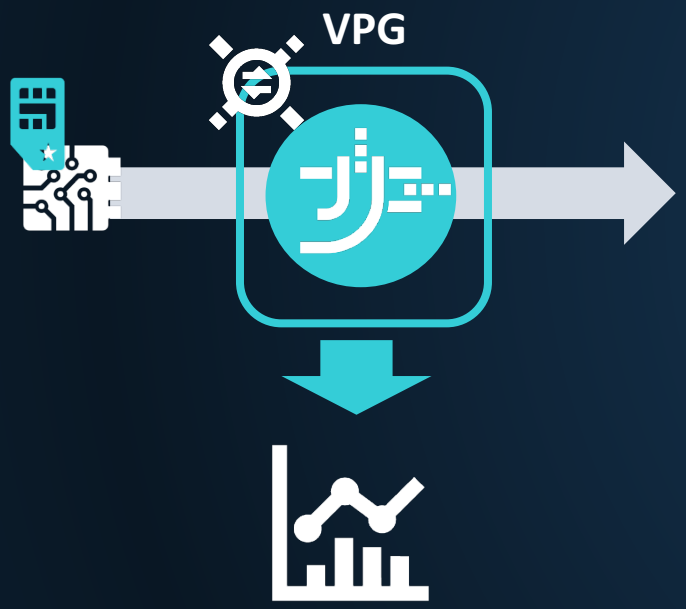
SORACOM Conference "Discovery"

- 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：
VPGに追加される3つのトラフィック処理機能

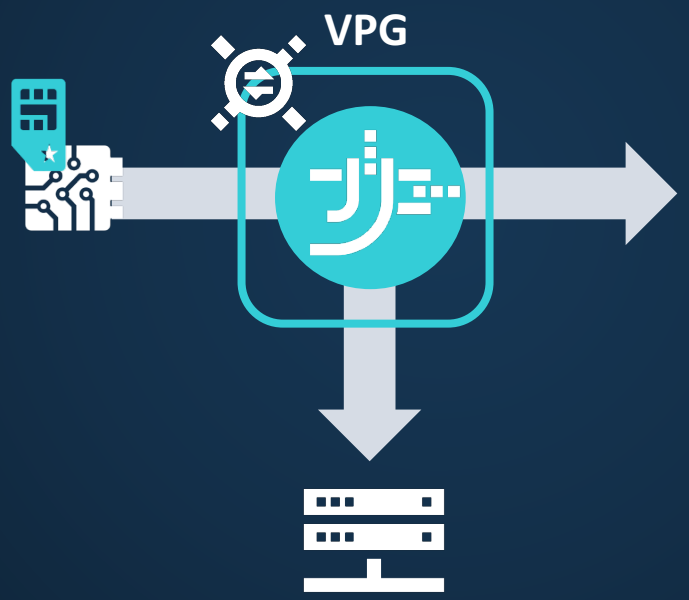
SORACOM Conference "Discovery"

Inspection



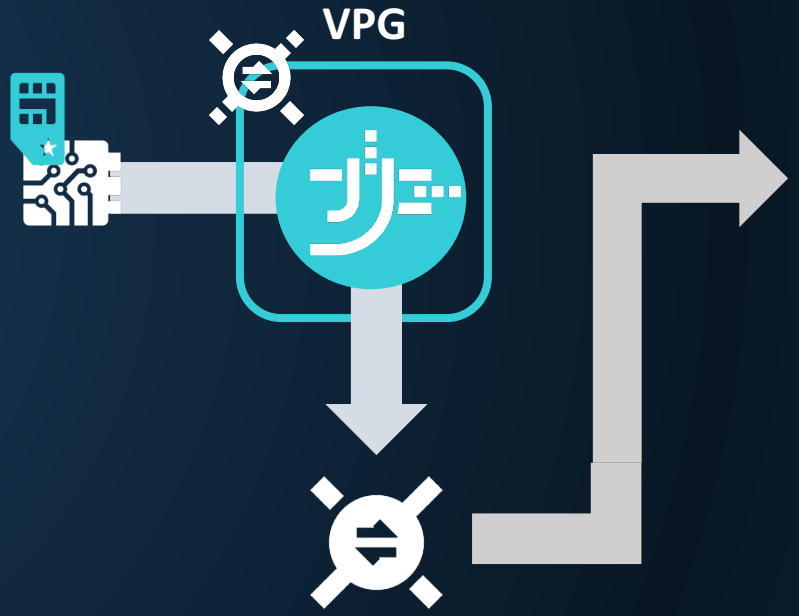
パケットフローを解析して
統計情報を出力

Mirroring



パケットのコピーを指定の
宛先に転送

Redirection

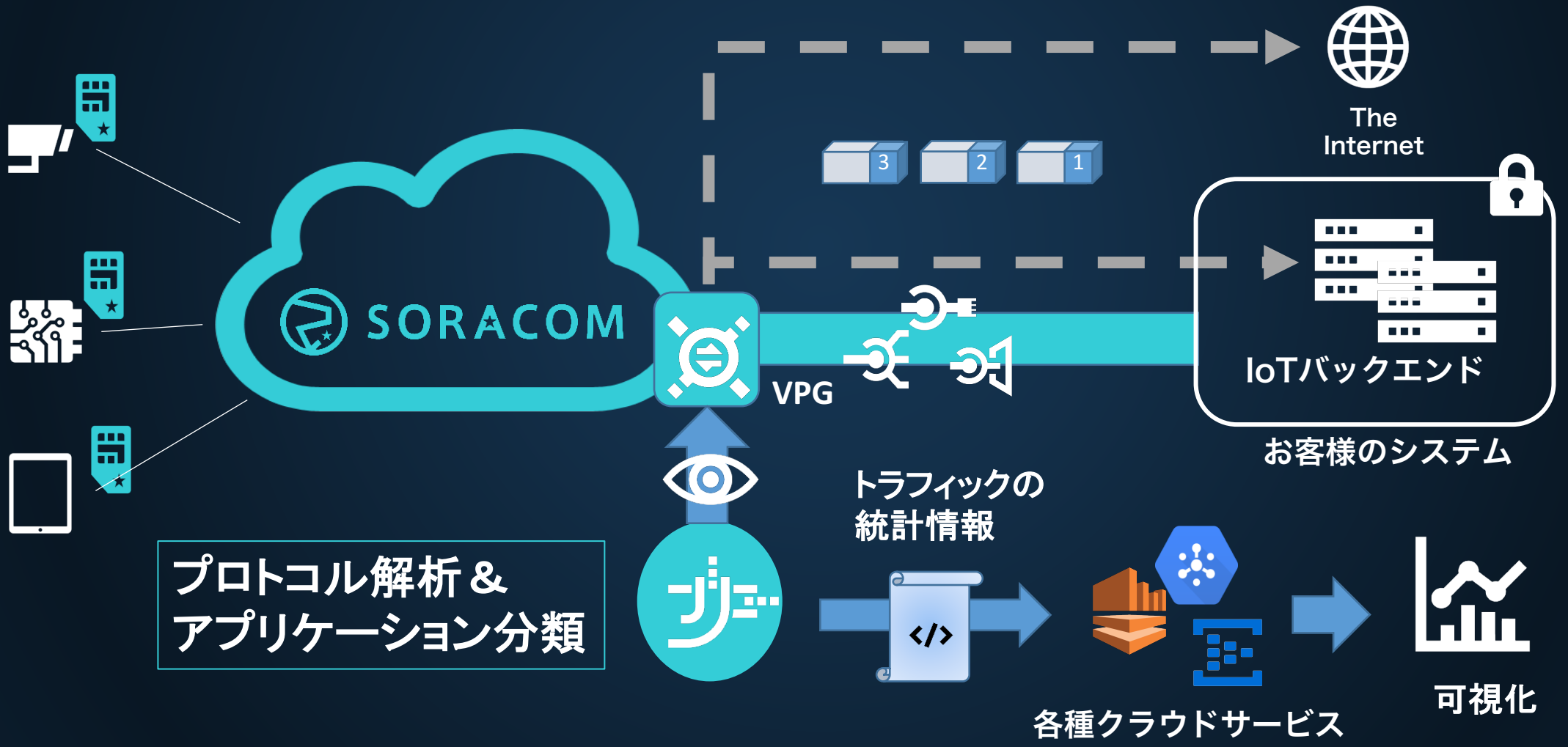


パケットを指定の
ゲートウェイ経由で転送

SORACOM Junction: Inspection

SORACOM Conference "Discovery"

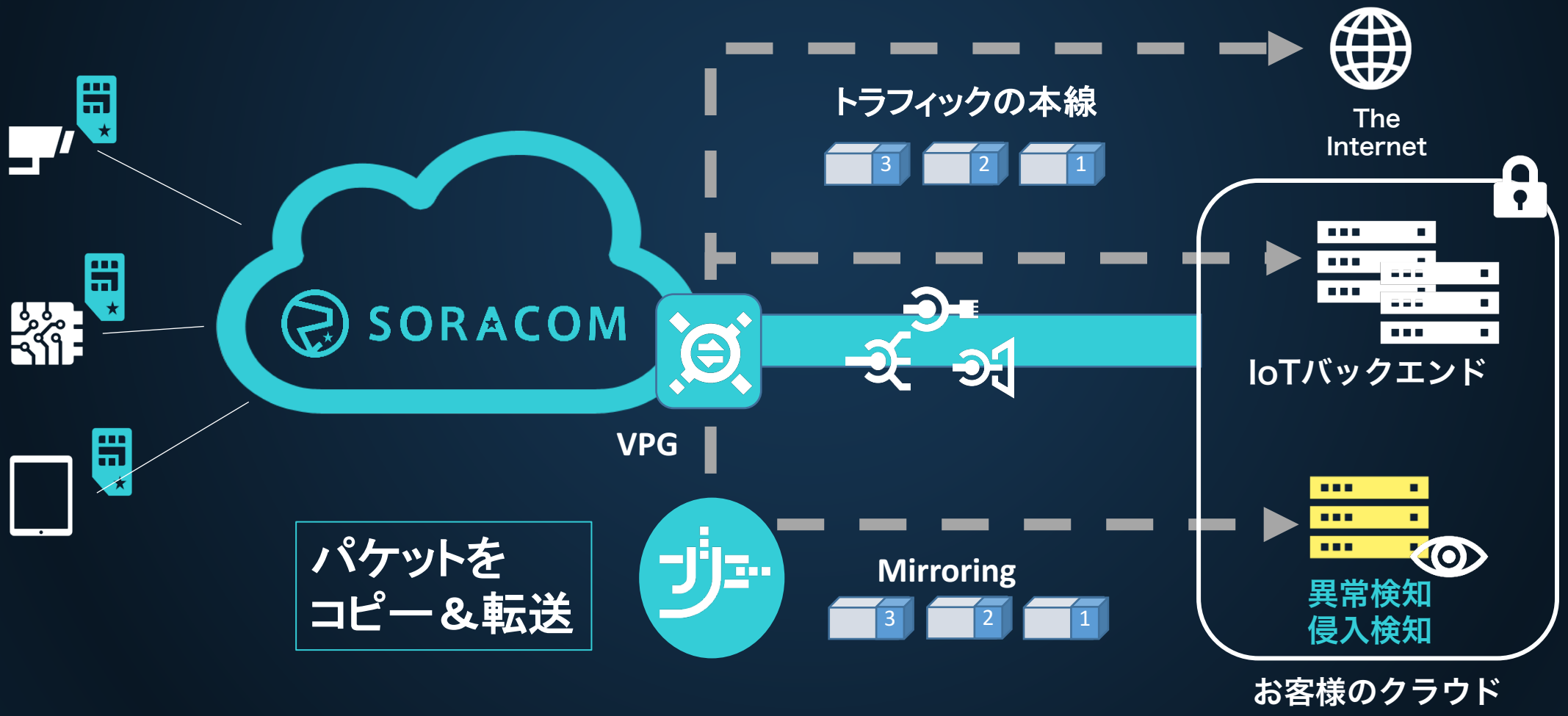
- VPGを通過するトラフィックの統計情報をレポート



SORACOM Junction: Mirroring

SORACOM Conference "Discovery"

- パケットのコピーをお客様のパケット解析エンジンに転送



SORACOM Conference "Discovery"

実際にSORACOM Junctionで
トラフィックの可視化や異常検知をする様子

SORACOM Conference "Discovery"

株式会社 ソラコム
ソフトウェアエンジニア
福島　拓

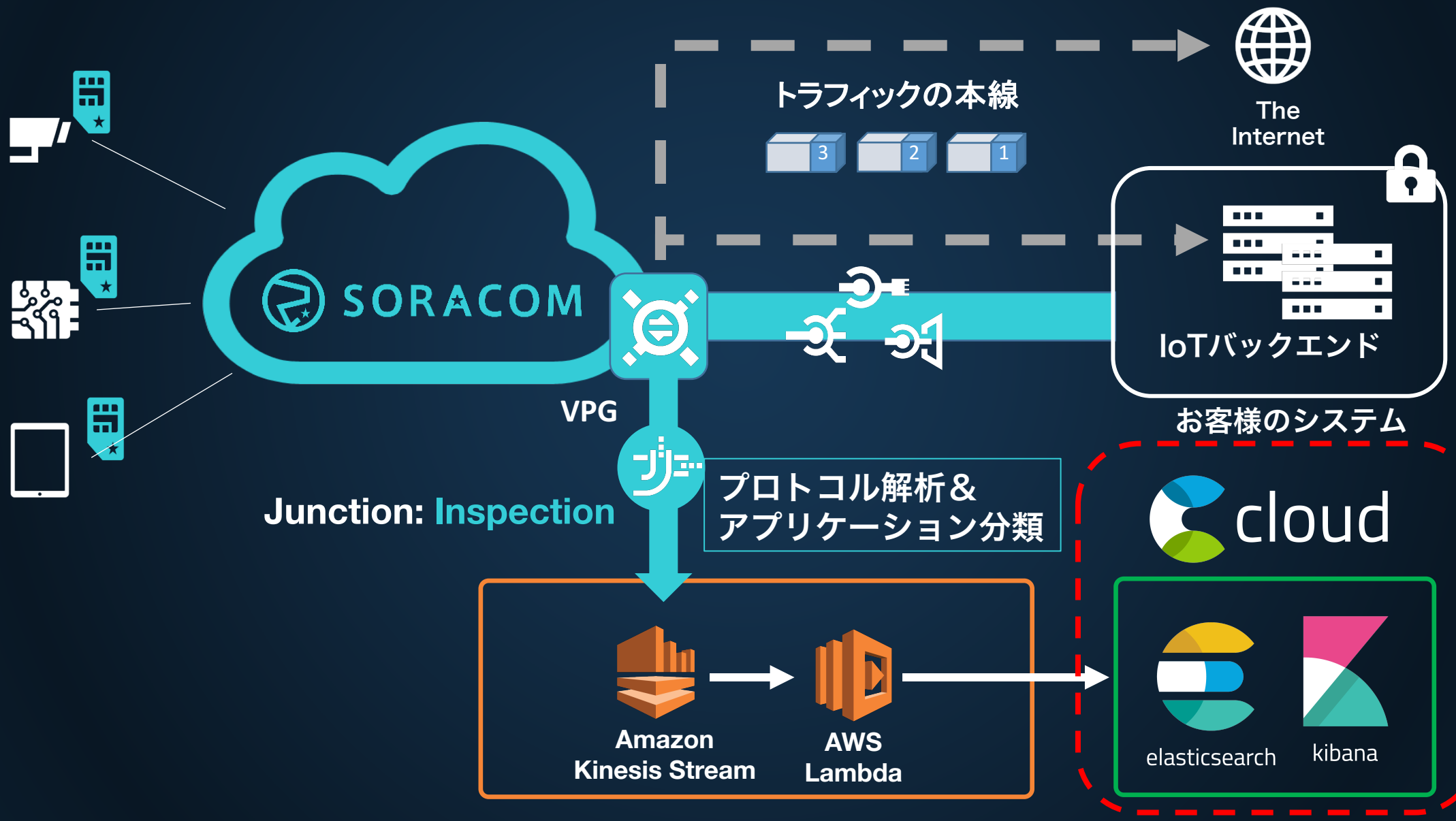
Junctionパートナーソリューション例

SORACOM Conference "Discovery"

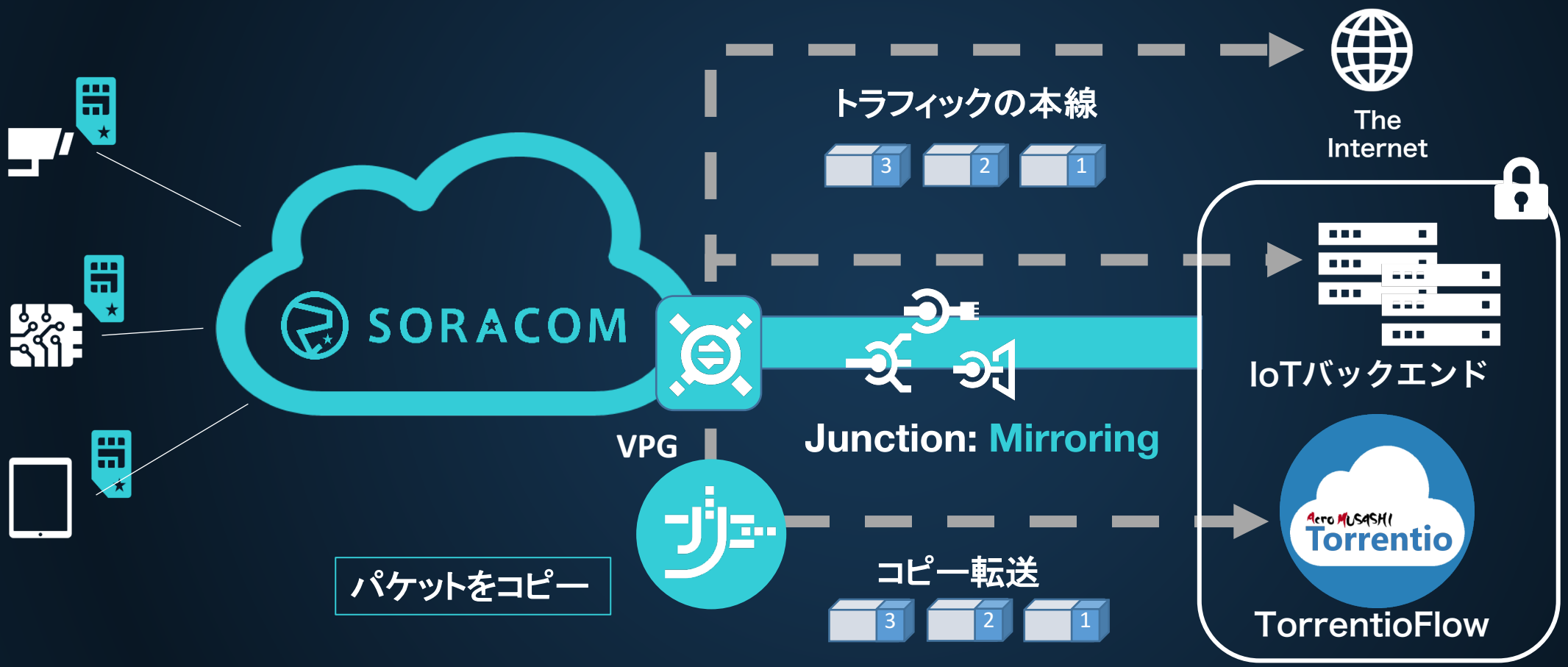
- Junction: Inspection
  - Elastic様
    - Elastic Cloud，ElasticsearchおよびKibanaによる可視化
- Junction: Mirroring
  - Acroquest様
    - TorrentioFlowの機械学習による異常検知、通知

SORACOM Junction: Inspection

SORACOM Conference "Discovery"



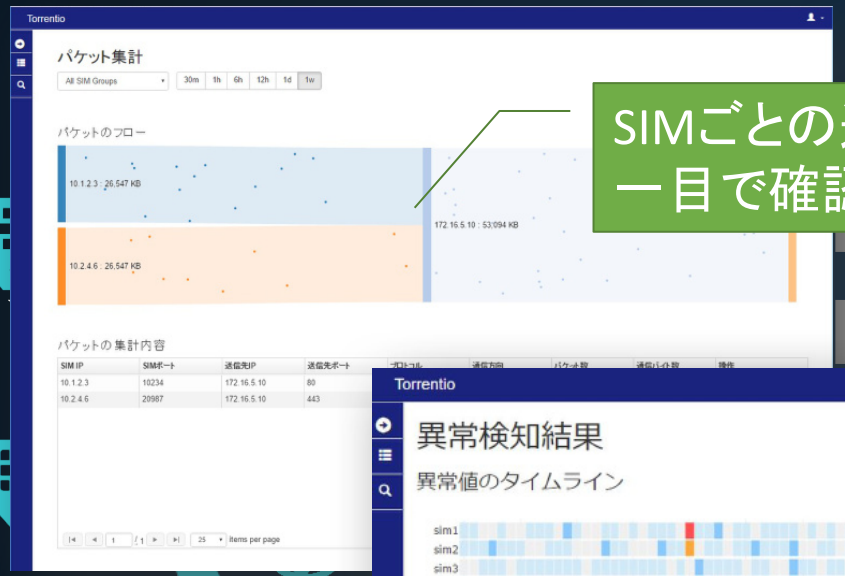
SORACOM Junction: Mirroring



- 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

SORACOM Conference "Discovery"



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

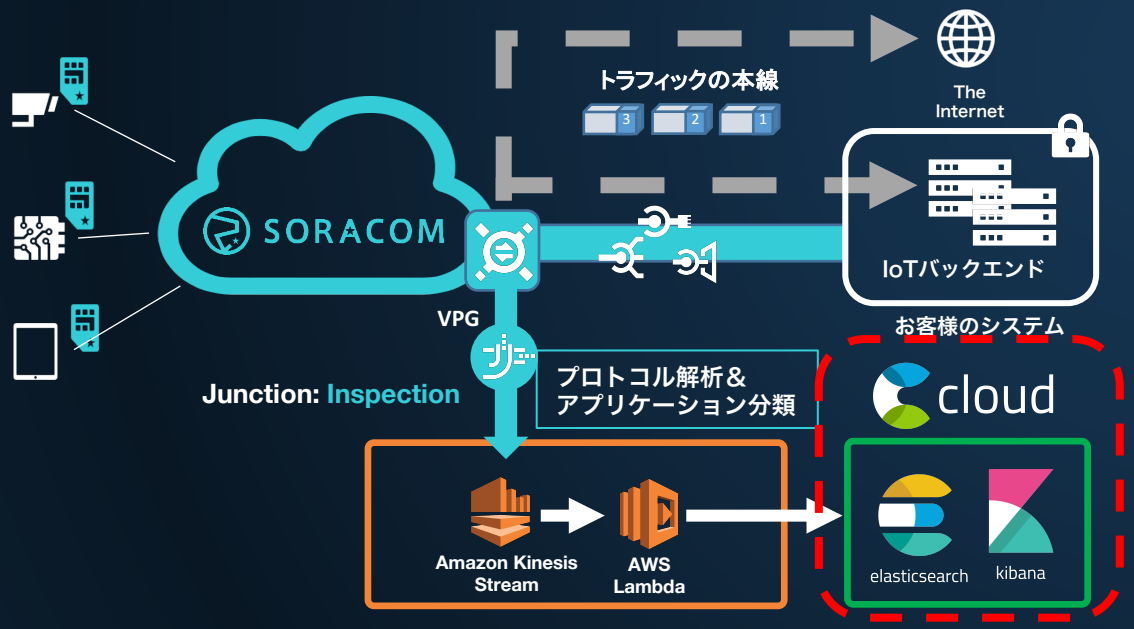
TorrentioFlow

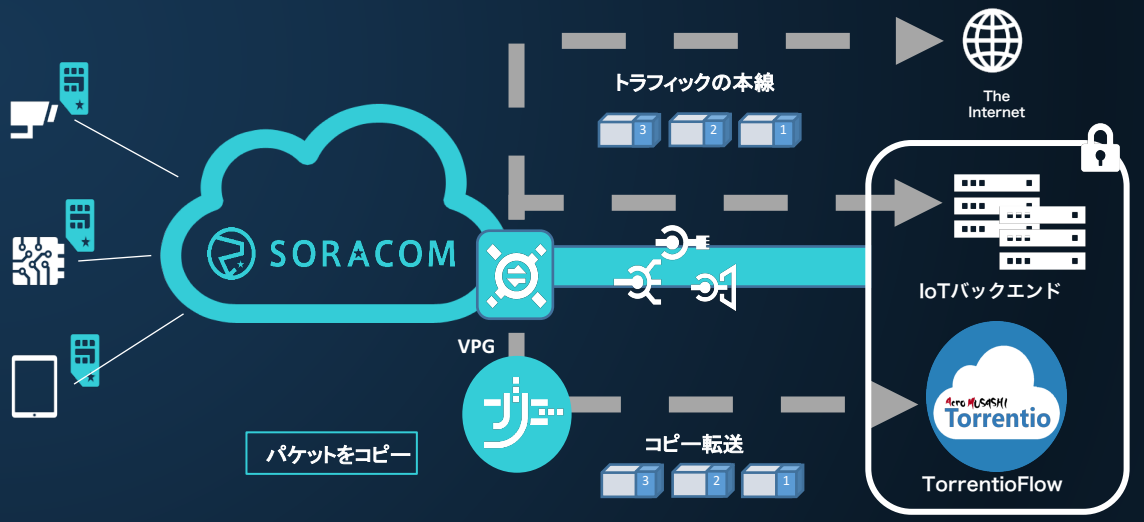
- 個別フローのリアルタイム分析・可視化
- 機械学習による異常検知・リスク分析
- 異常の通知

Junctionを利用したパケット解析

SORACOM Conference "Discovery"

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になります。





- 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でお客様の声にお応え

SORACOM Conference "Discovery"

- 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？

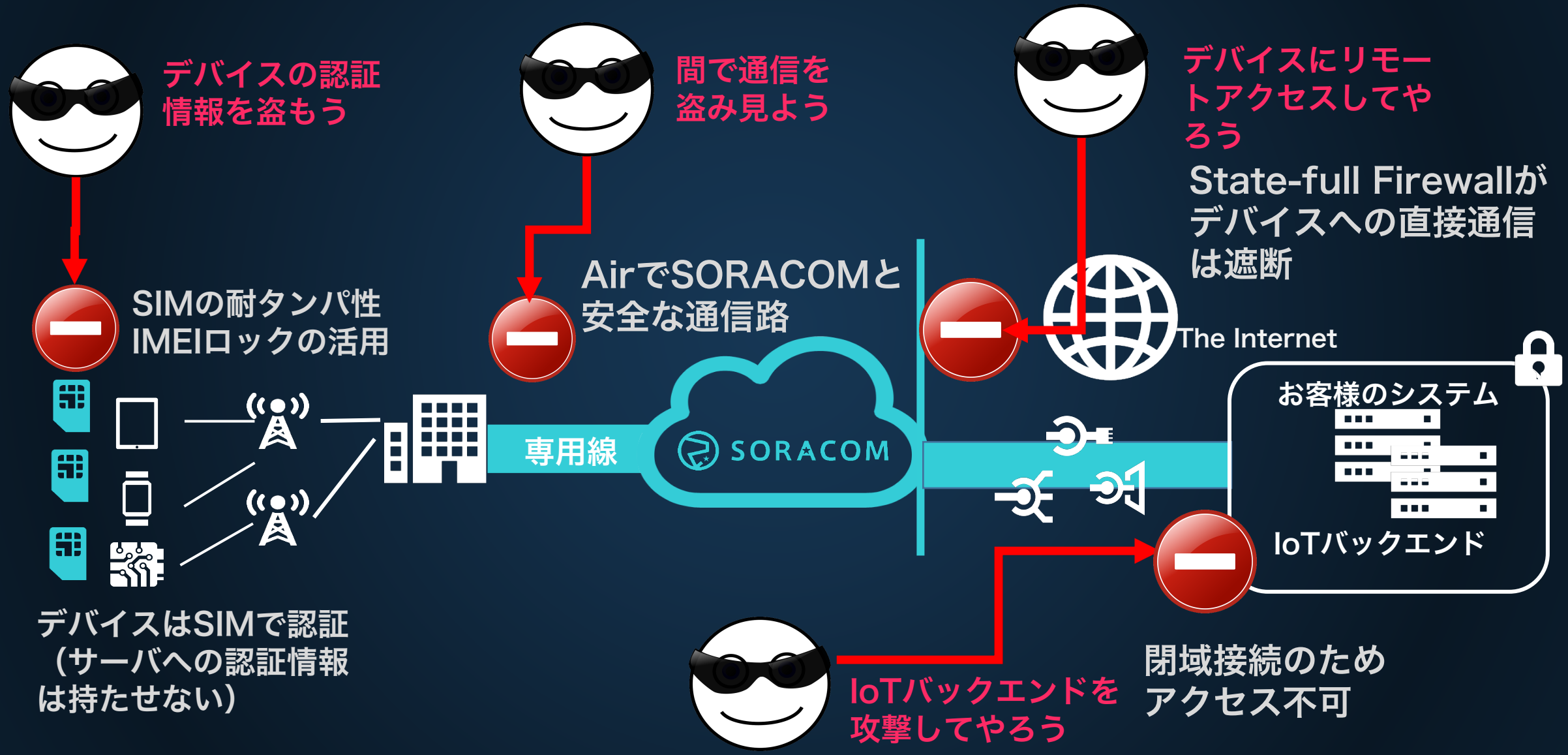
SORACOM Junctionでお客様の声にお応え

SORACOM Conference "Discovery"

- 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を活用したIoTシステムの場合

SORACOM Conference "Discovery"



残るセキュリティ上の課題

SORACOM Conference "Discovery"

- 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

SORACOM Conference "Discovery"

トレンドマイクロ株式会社
IoT 事業推進本部 ソリューション推進部
津金 英行 様

SORACOM Conference “Discovery” 2017

トレンドマイクロ IoTセキュリティ

2017年7月5日

トレンドマイクロ株式会社
IoT事業推進本部 ソリューション推進部
津金 英行

トレンドマイクロのビジョン

デジタルインフォメーションを

安全に交換できる世界の実現

IoTのセキュリティ脅威事例

ホテルの電子カードキーシステム

オーストリアのホテルで客室の電子カードキー　システムがランサム　　ウェアに感染、宿泊客　を部屋から閉め出し

http://thehackernews.com/2017/01/ransomware-hotel-smart-lock.html

建物のドア開閉＆防犯システム

市販されている建物のリモート管理システムの脆弱性をつき、警報やドアロックのすべての機能が遠隔から制御可能なことを実験で証明

http://blog.trendmicro.com/let-get-door-remote-root-vulnerability-hid-door-controllers/

ベビーモニター＆監視カメラ

米国でネットにつないだベビーモニターから見知らぬ人の声で突然幼児に話しかける

http://kdvr.com/2015/04/21/couple-whose-baby-monitor-was-hacked-has-message-for-other-families/

自動車のハッキング

高速で走る自動車へ遠隔からの攻撃で、ハンドルやブレーキシステムを制御することが可能なことを実験で証明

https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

IoT機器を悪用するDDoS攻撃

感染デバイスがボット化し
サイバー攻撃に悪用されるケースも

利用企業が、被害者から
加害者になるビジネスリスク

75万通
スパムメール
-**冷蔵庫**など-

2014年

5万/秒
HTTPリクエスト
-**2.5万台監視カメラ**-

2016年 6月

12万/秒
HTTPSリクエスト
-**4.7万**台の**監視カメラ**,
ホームルータ, サーバなど-

8月

9月20日
KrebsOnSecurity

620Gbps
DDoS攻撃
-**18万**台の**IoT**機器-

9月21日
OVH

1Tbps
-**14.5万**台の**IoT**機器-

10月21日
Dyn

1.2Tbps
-約**10万**台の**IoT**機器-

Mirai
ソースコード
公開

なぜIoT機器が狙われるのか

常時接続

- 365日24時間接続可能

脆弱性

- 複数の攻撃ポイント
- 侵入が比較的容易
- セキュリティ対策が不十分な機器が多い

低コスト

- IoT機器のボット化はPCよりも攻撃の費用対効果が高い

管理者不在

- 未アップデート機器が多い
- アフターサービスが未熟な製品が存在

閉域接続なら安全？

閉域でも内部からの脅威発生リスクあり

- デバイス製造段階でのセキュティ脅威の混入
- オフラインでの侵入（外部メディア接続、持ち込み端末等）

しかし、個々のデバイスでの対策には限界あり

- **多種多様**
- **大量、広域に展開**
- **限られたリソース（プロセッサ、メモリ等）**

ソラコム x トレンドマイクロ

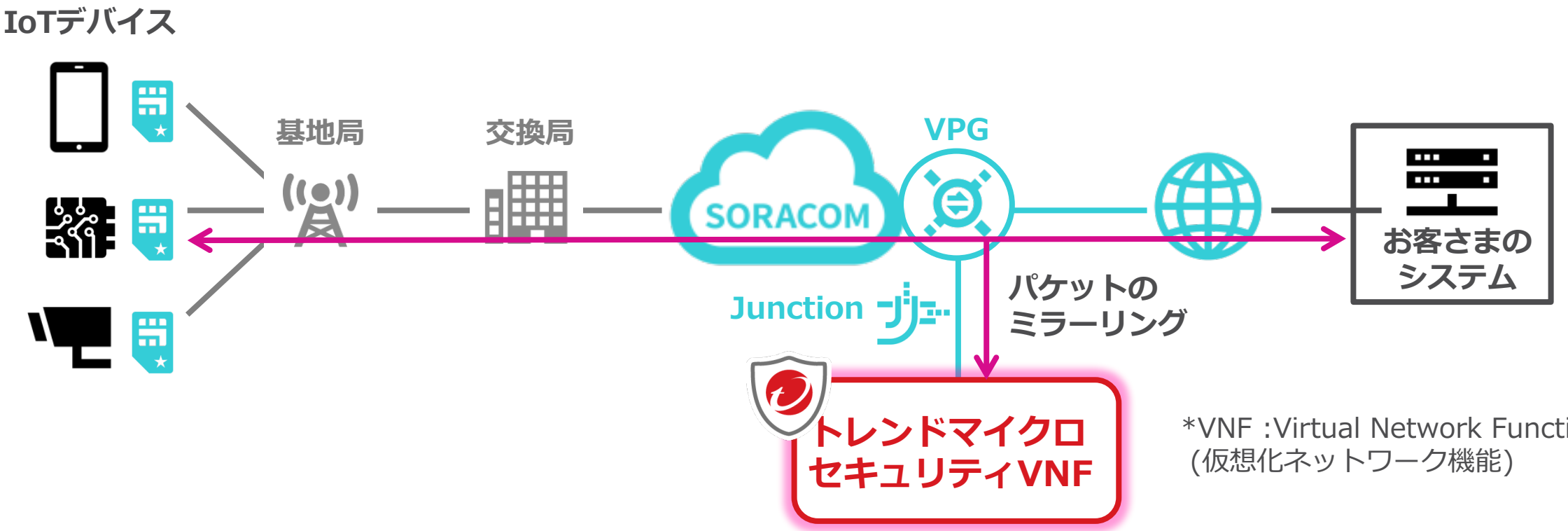
X

セキュアIoTプラットフォーム
- プライベート接続
- デバイス認証、暗号化 等

ネットワークセキュリティ技術
- セキュリティ脅威検出
- 不正サイトアクセス検知 等

より高度で効果的なIoTセキュリティの実現

SORACOM Junction x トレンドマイクロ セキュリティVNF

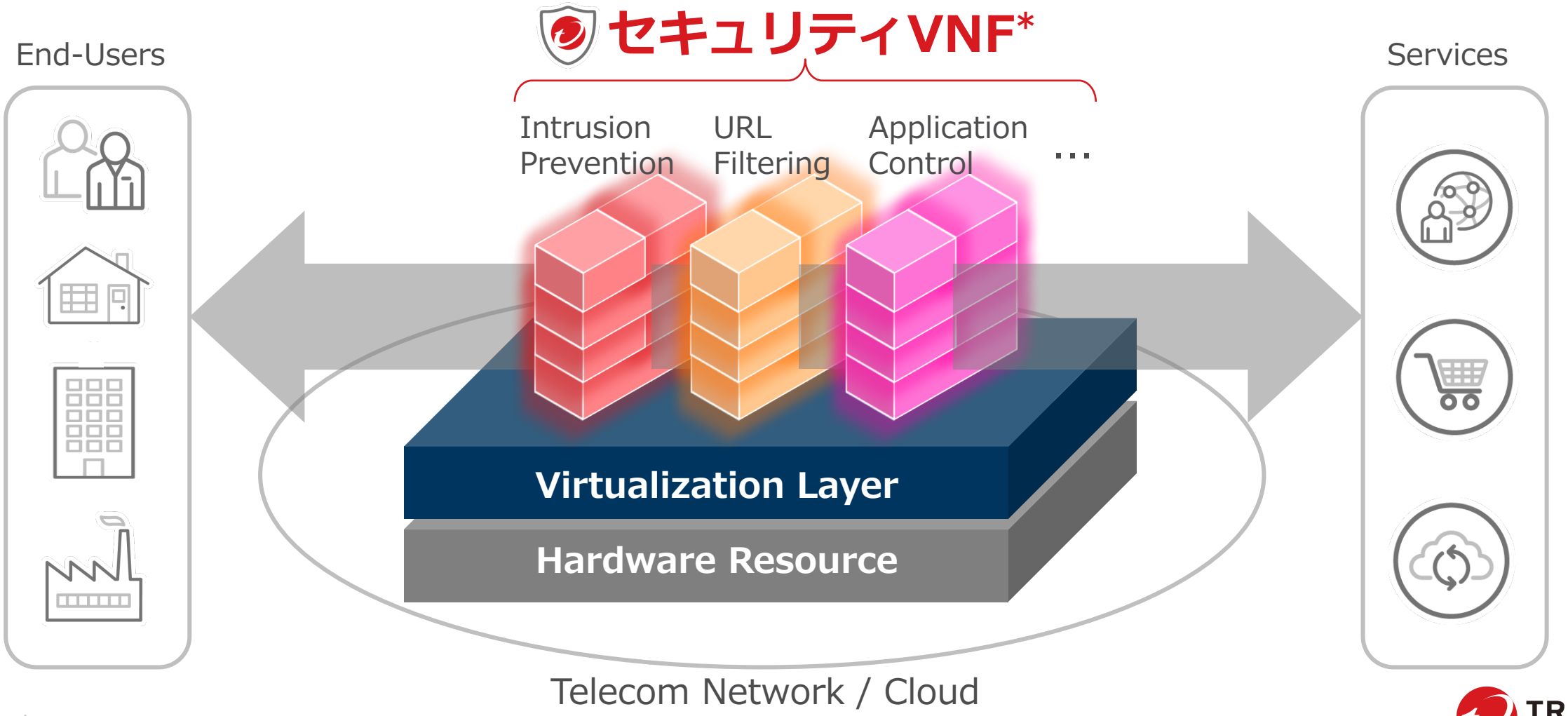


*VNF :Virtual Network Function
(仮想化ネットワーク機能)

ソラコムユーザ様の通信トラフィックに潜む
セキュリティ脅威の可視化・制御が可能に！

トレンドマイクロ セキュリティVNF

NFVおよびクラウド環境向け仮想化ネットワークセキュリティ機能



*VNF：Virtual Network Function

トレンドマイクロ セキュリティVNF 提供機能

侵入防御

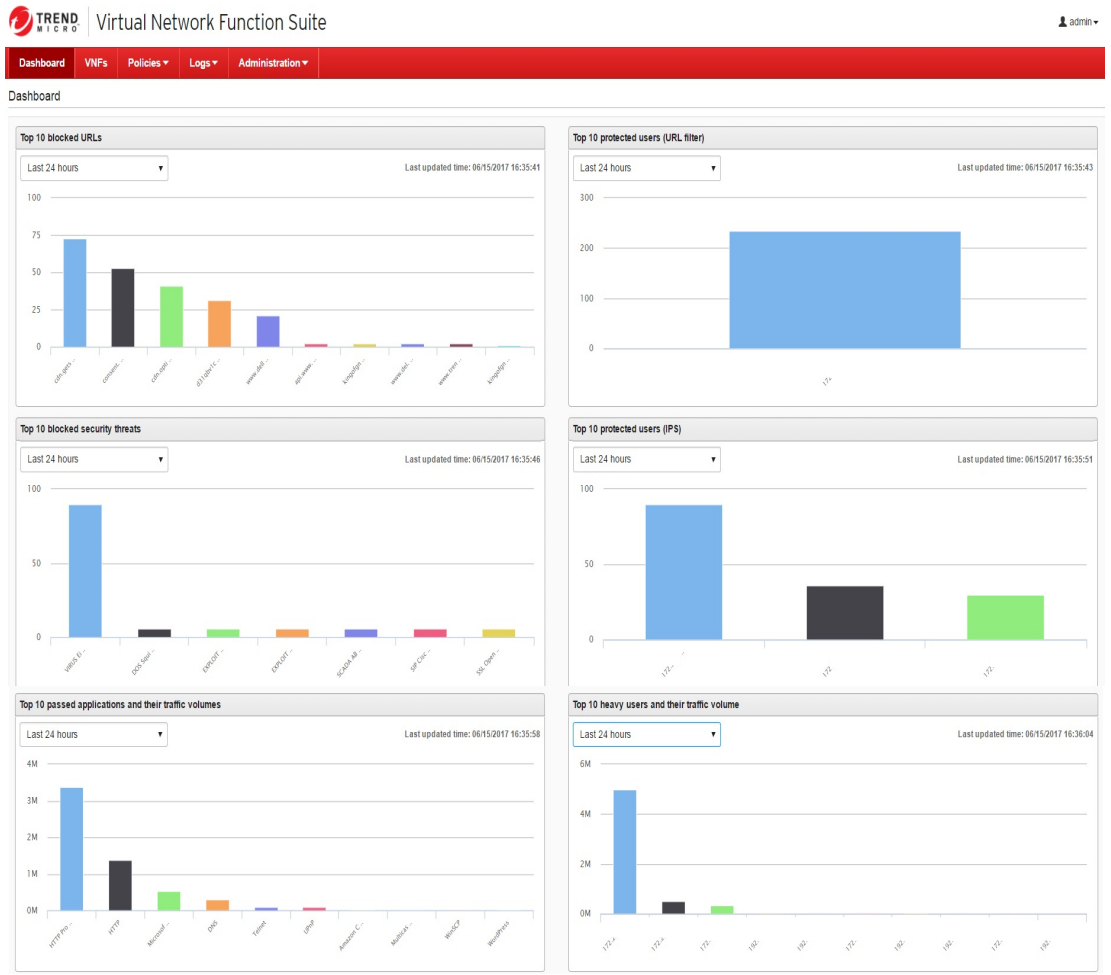
- 侵入防止システム (IPS) により、脆弱性を狙った通信を検知/ブロック

Web脅威対策

- 不正Webサイトへのアクセスをブロック、不正プログラムの感染、詐欺サイトや改ざんサイトへのアクセスを防止

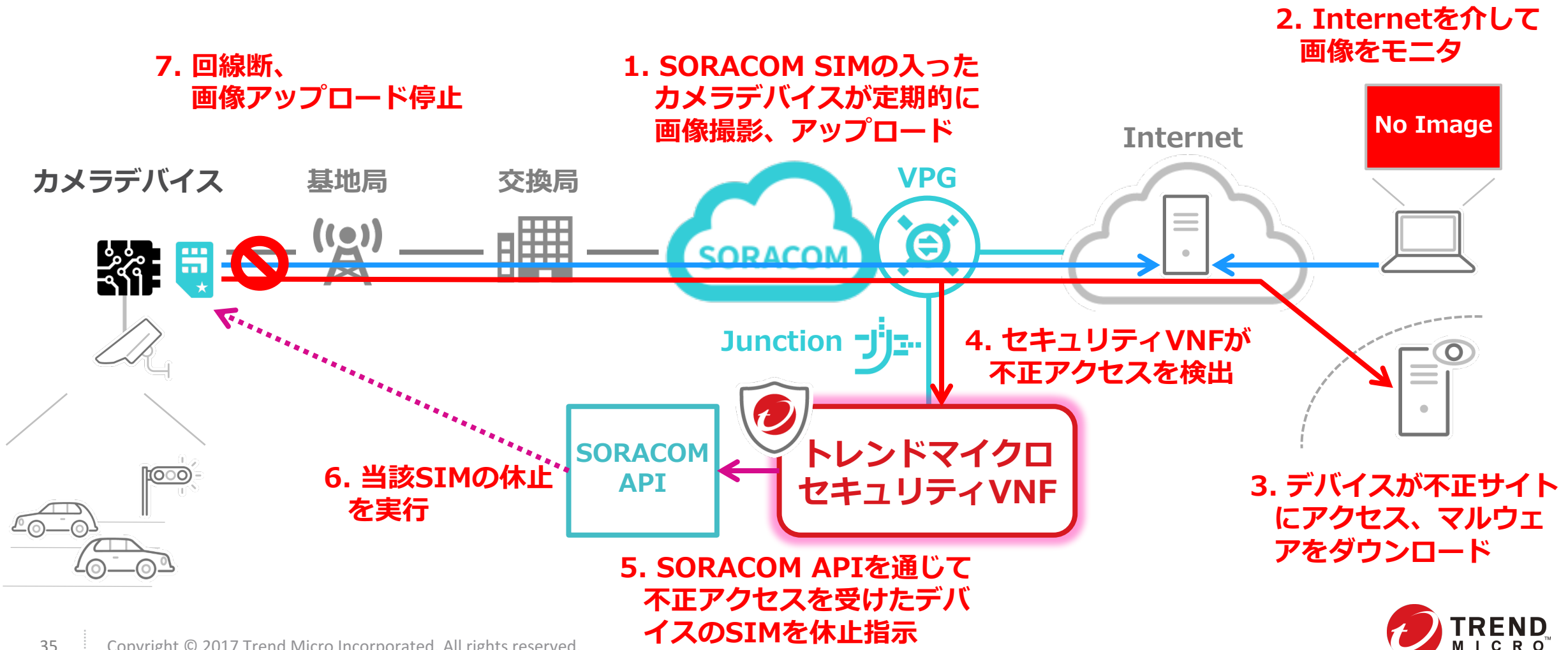
アプリケーション制御

- アプリの利用状況を可視化、許可されていないアプリの実行を防止



トレンドマイクロ セキュリティVNF デモ

トラフィック中のセキュリティ脅威検出をトリガーにした自動通信遮断



新しいIoTセキュリティサービスを
お試しいただけます！

SORACOM
Junction

X

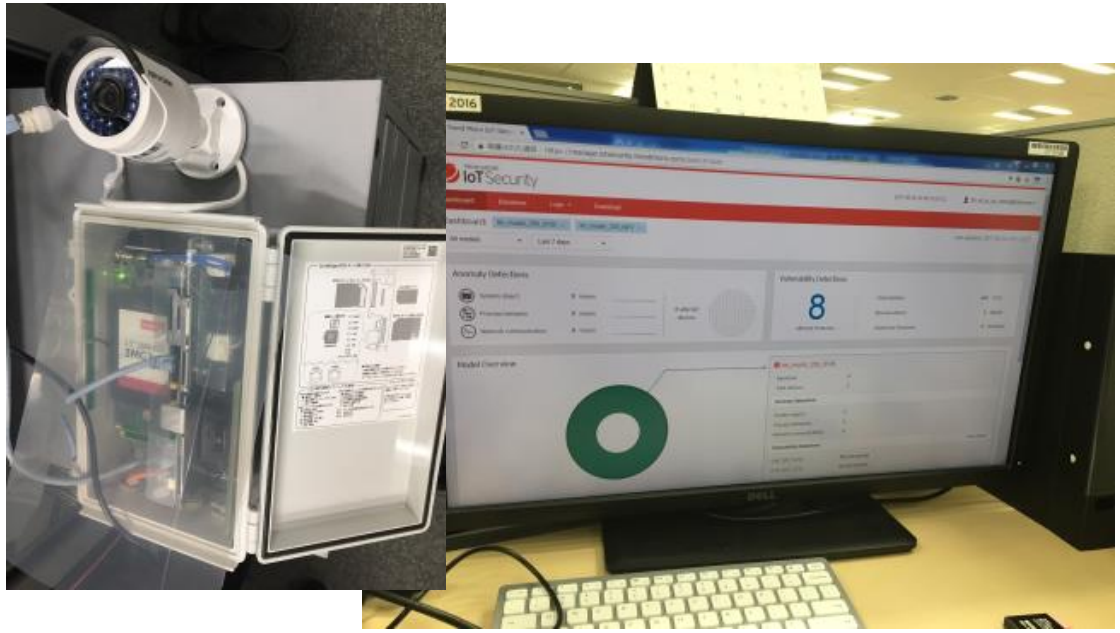
トレンドマイクロ
セキュリティVNF

ぜひお問い合わせください！

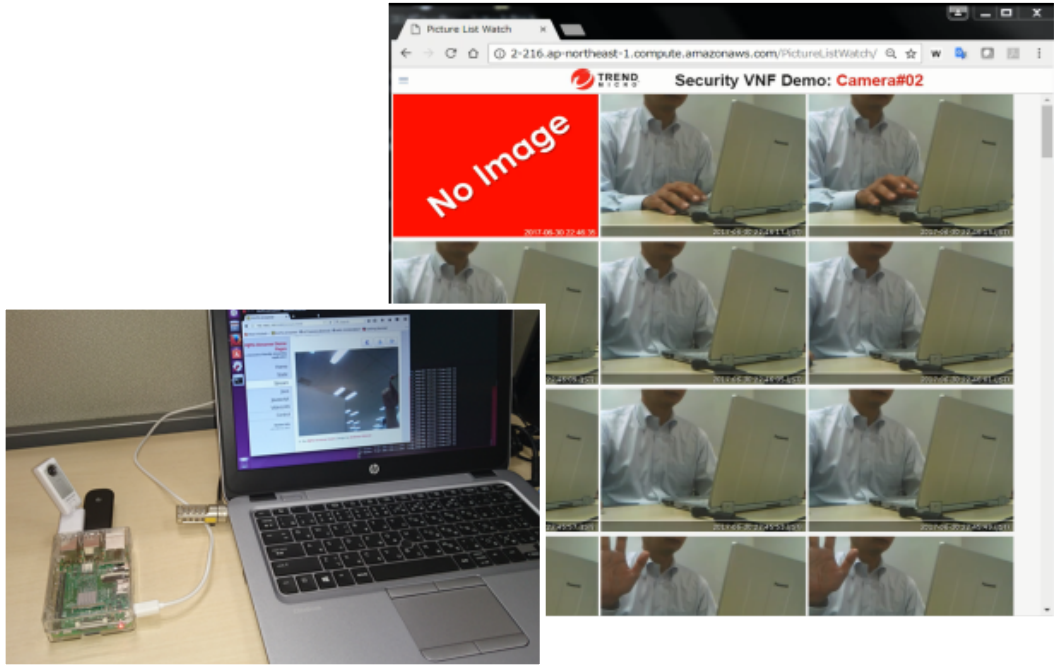
SORACOM Discovery:
トレンドマイクロ ブース展示

トレンドマイクロ IoTセキュリティソリューション

デバイス組み込み型 セキュリティSDK



セキュリティVNF



X

Thank you

TREND MICRO™

SORACOM Junctionでお客様の声にお応え

SORACOM Conference "Discovery"

- 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でお客様の声にお応え

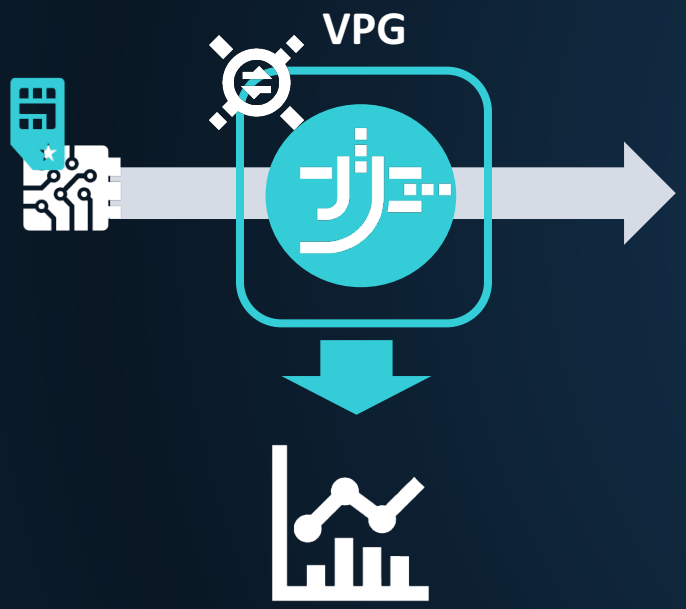
SORACOM Conference "Discovery"

- 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：
VPGに追加される3つのトラフィック処理機能

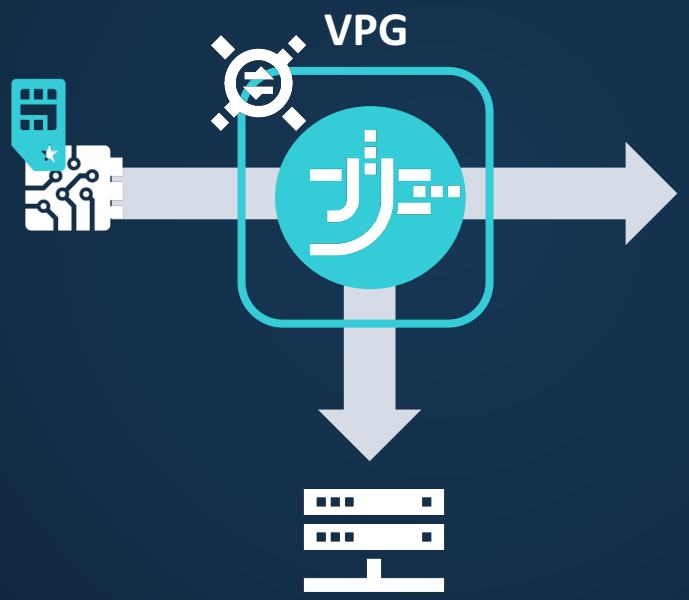
SORACOM Conference "Discovery"

Inspection



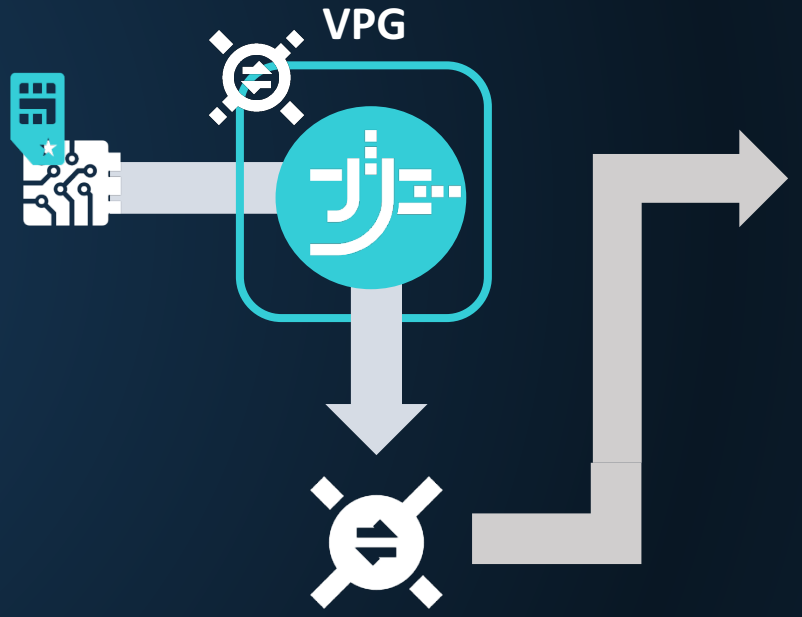
パケットフローを解析して
統計情報を出力

Mirroring



パケットのコピーを指定の
宛先に転送

Redirection

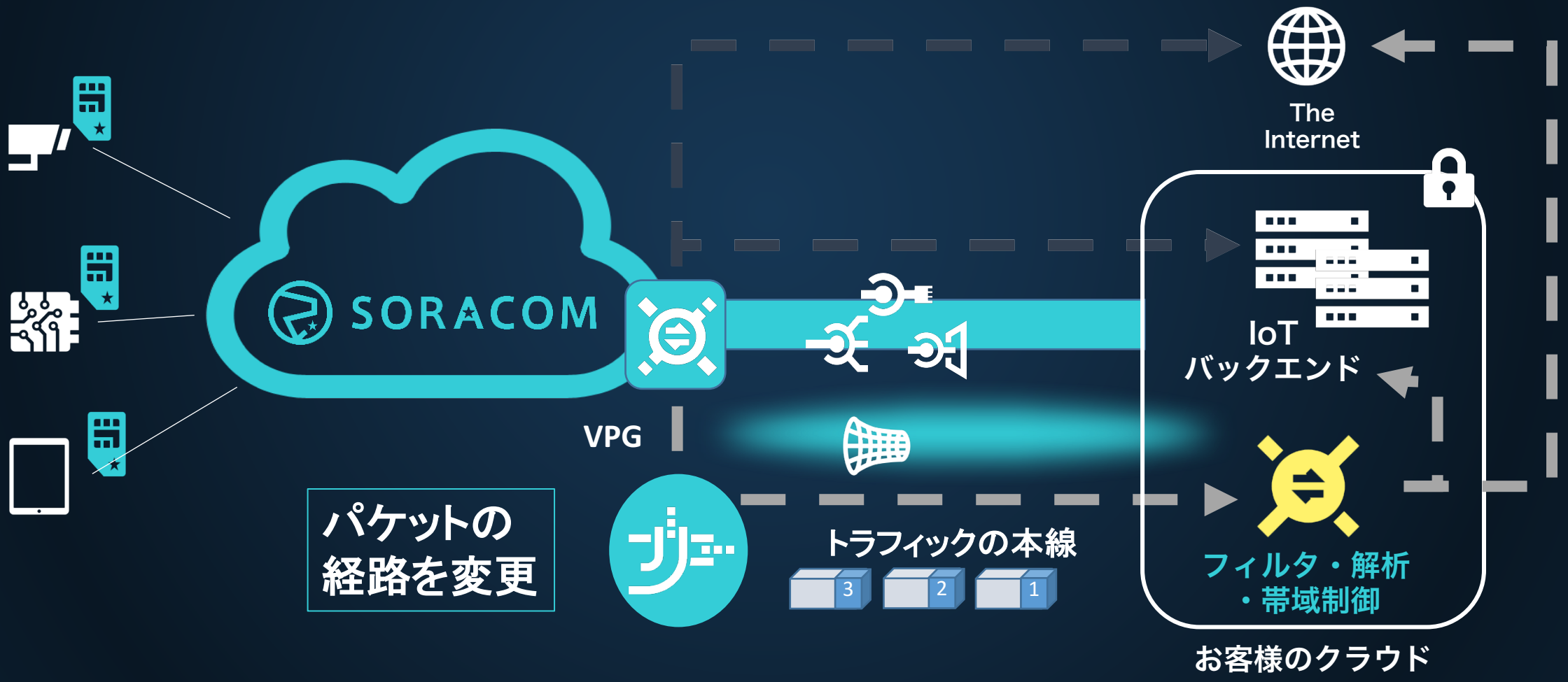


パケットを指定の
ゲートウェイ経由で転送

SORACOM Junction: Redirection

SORACOM Conference "Discovery"

- パケットを指定のゲートウェイ経由で転送



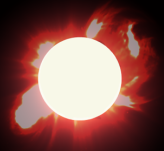
SORACOM Conference "Discovery"

東京大学 大学院情報学環
大学院学際情報学府 教授
中尾 彰宏 様

IoT Dynamics

東京大学大学院情報学環
中尾彰宏

FLARE



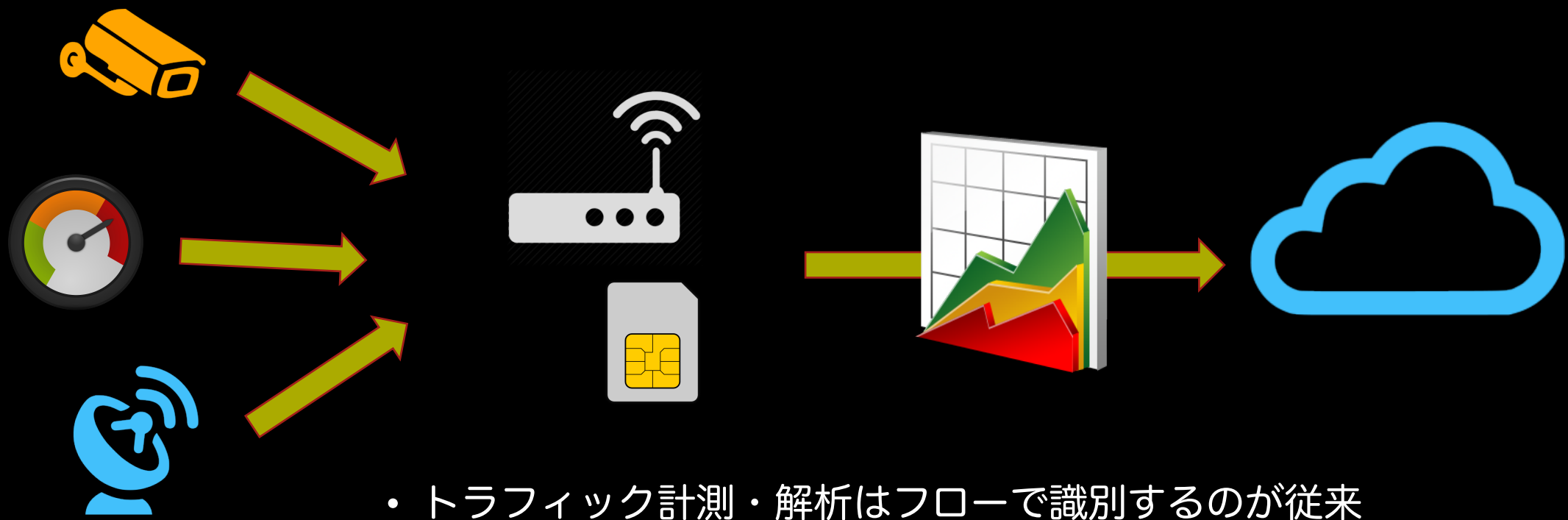
Enabling Deeply Programmable Network

NakaoLab @ The University of Tokyo

X

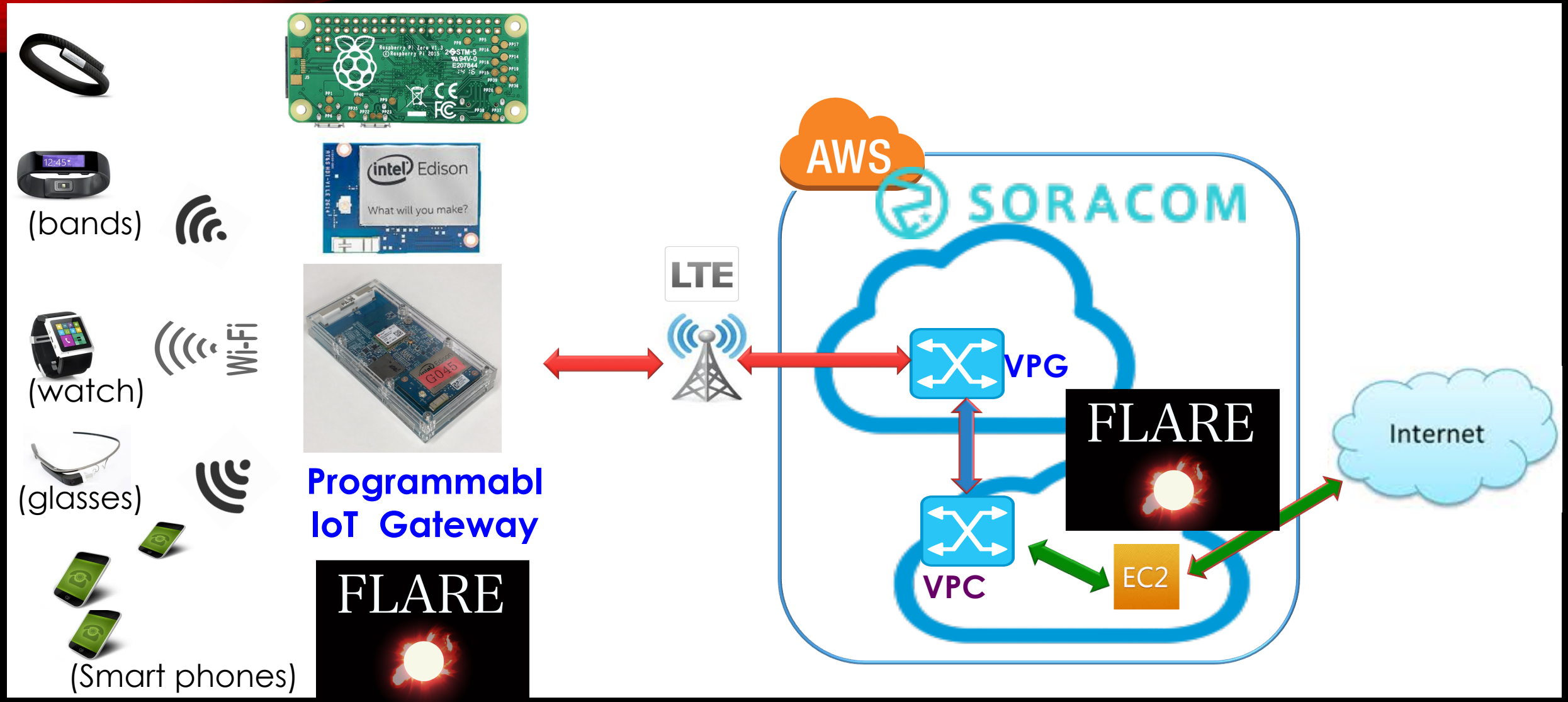
IoT MVNO における課題

- 通信コストの削減
- セキュリティ
  - トラフィックの詳細解析による通信利用の最適化

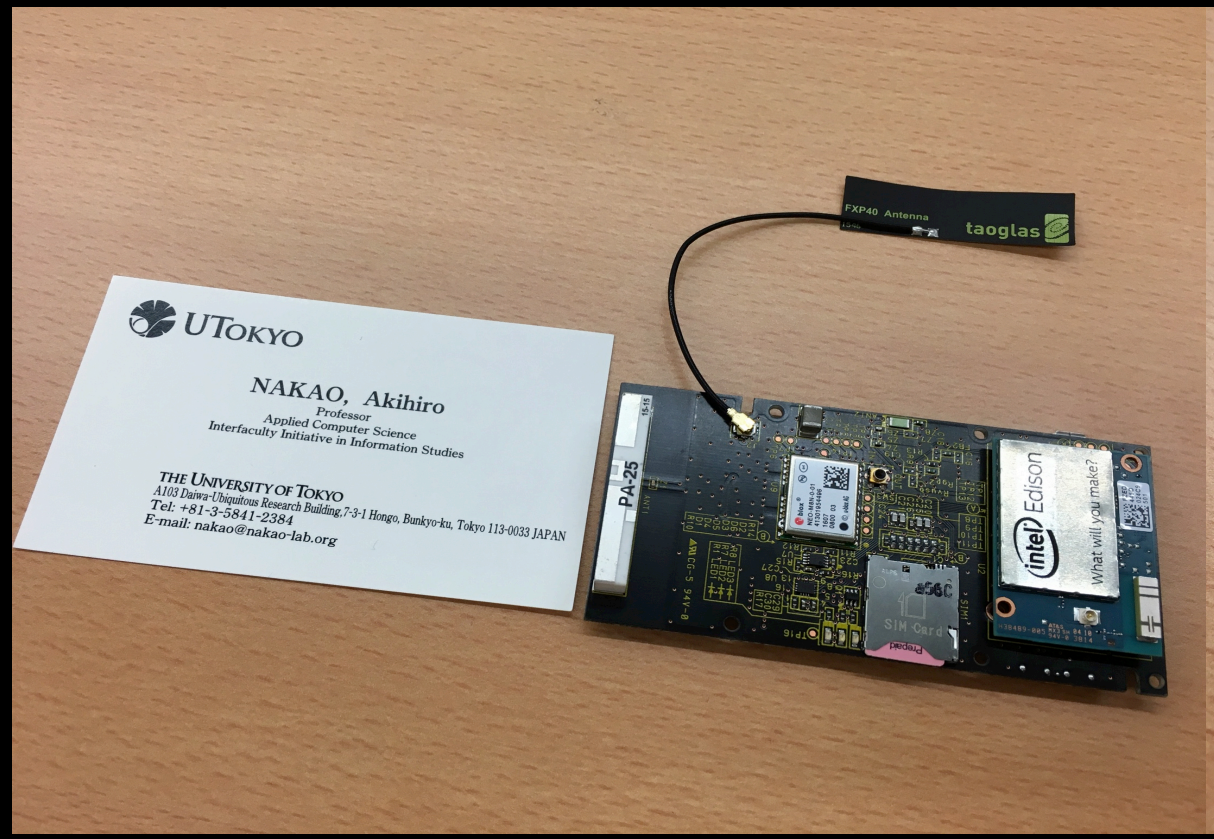


- トラフィック計測・解析はフローで識別するのが従来
- 今後は、より詳細にアプリ・サービス毎で識別することが重要

FLARE x Soracom Junction



Programmable IoT Gateway



3G/LTE/WiFi/BLE/GPS/ジャイロ/加速度　LoRa WAN対応予定(2017/8)
Raspberry Pi Zero W 対応予定（2017/8)

AI/機械学習によるトラフィック制御

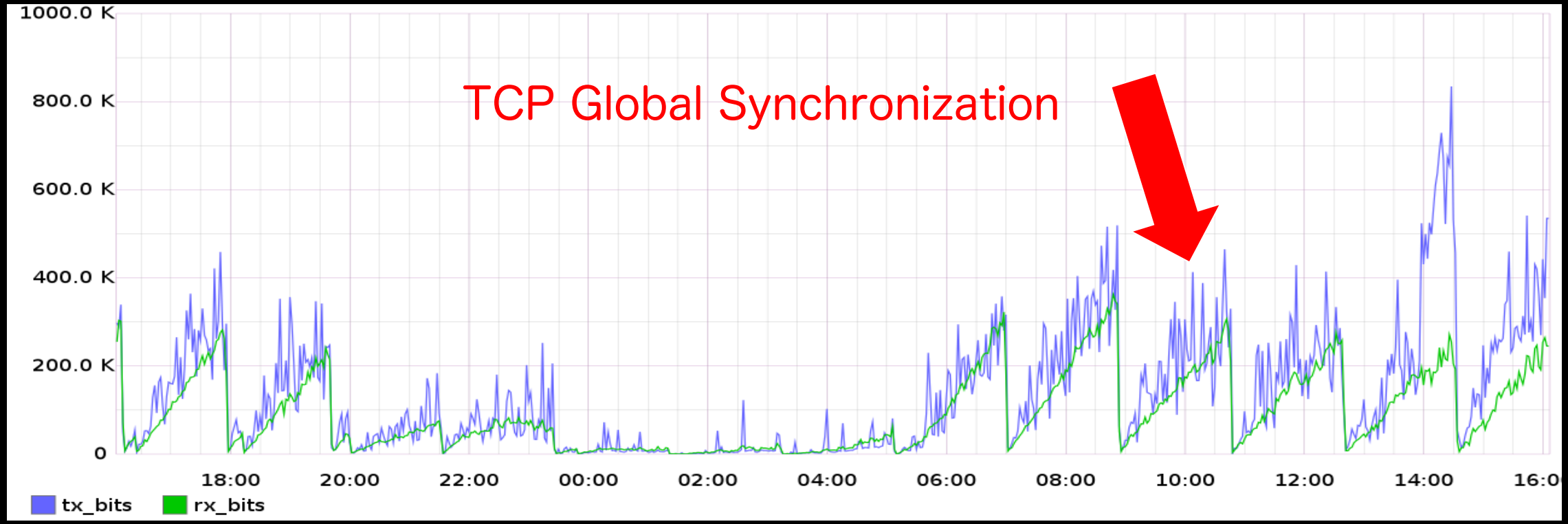
データ入力

データ出力

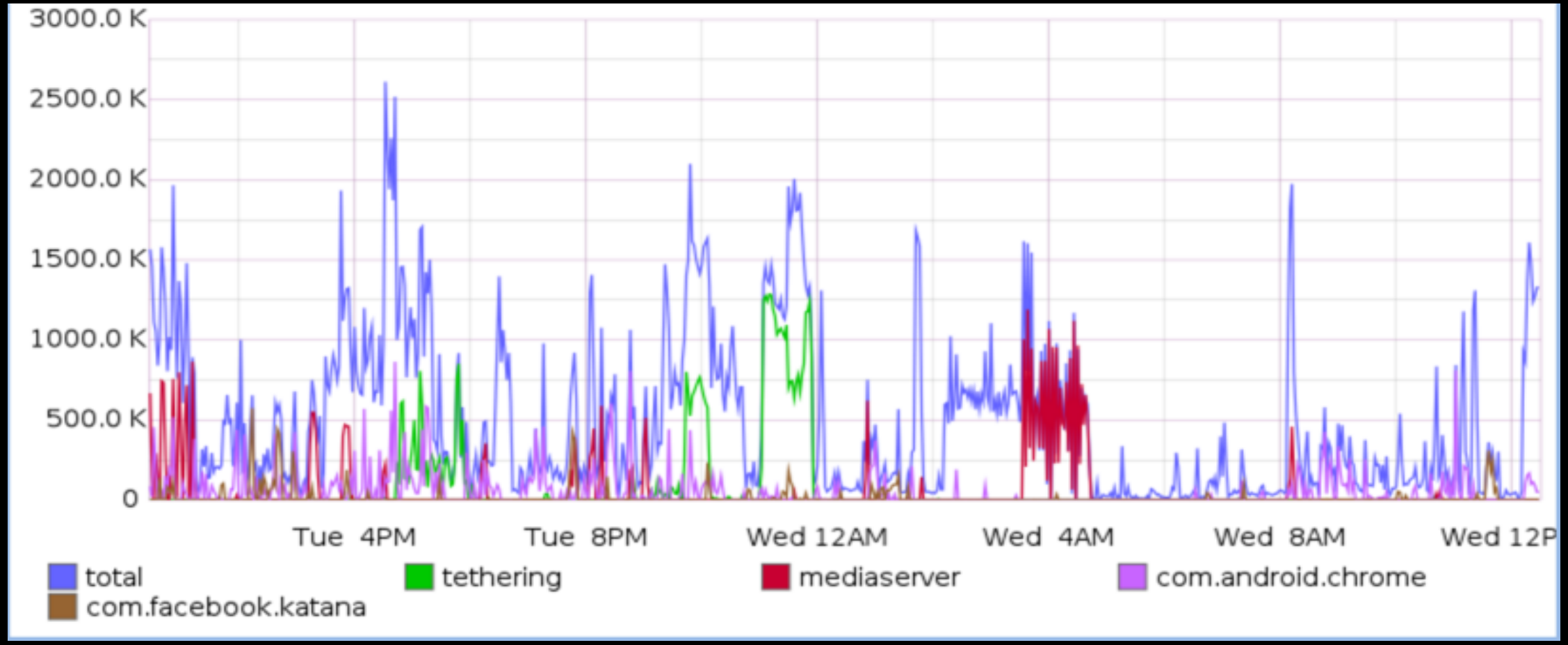
高度トラフィック分類（アプリ同定）
異常検知（Anomaly Detection）
異常予測
トラフィック量予測

AI/機械学習によるトラフィック制御・最適化（考えるネットワーク）

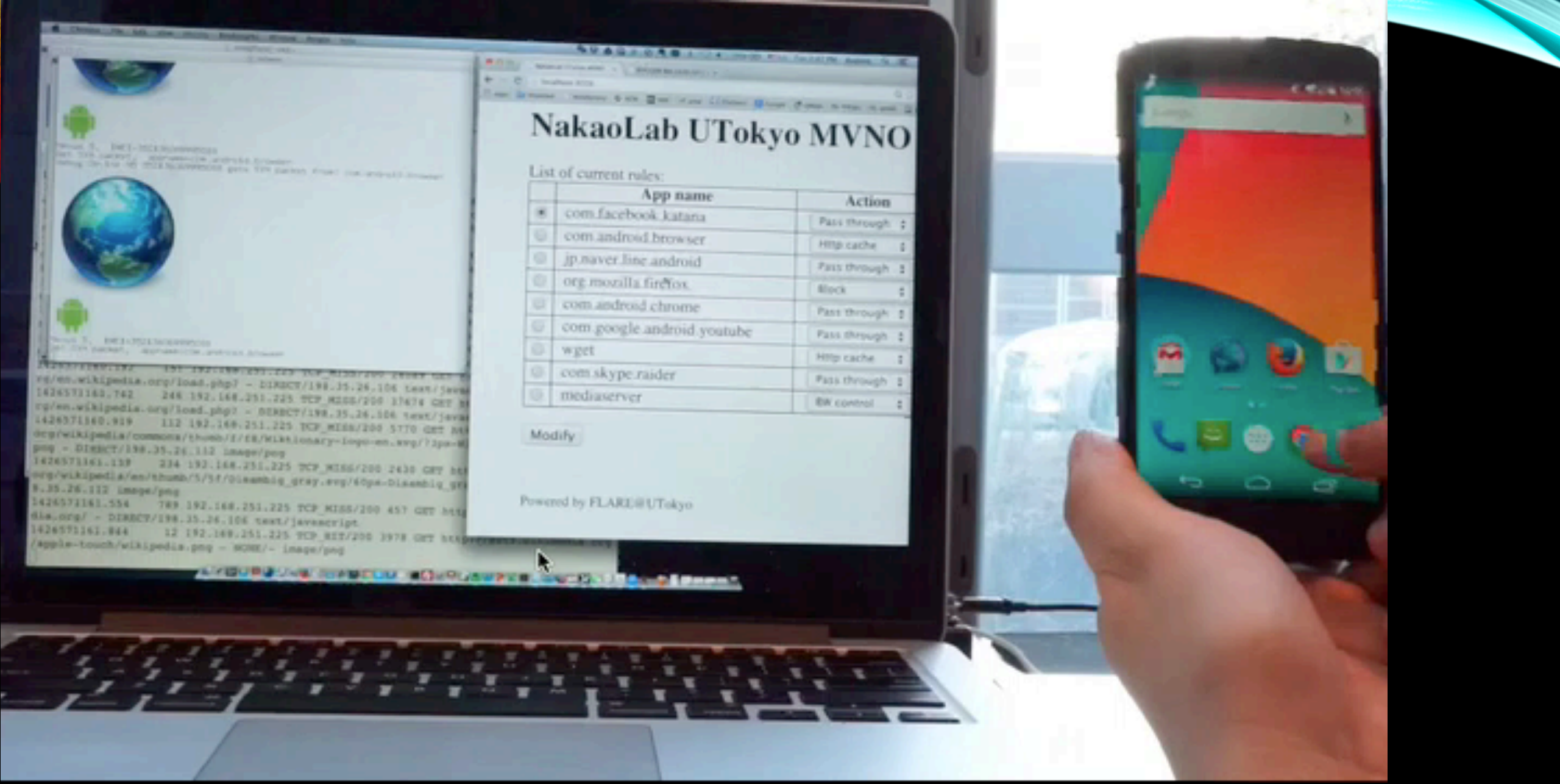
トラフィックの異常検知



アプリ毎のトラフィック統計を取得可能

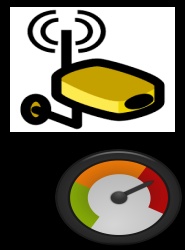


網内アプリケーション同定の実験


NakaoLab UTokyo MVNO
List of current rules:
App name
Action
com.facebook.katana
Pass through
com.android.browser
Http cache
jp.naver.line.android
Pass through
org.mozilla.firefox
Block
com.android.chrome
Pass through
com.google.android.youtube
Pass through
wget
Http cache
com.skype.raider
Pass through
mediaserver
BW control
Modify
Powered by FLARE@UTokyo

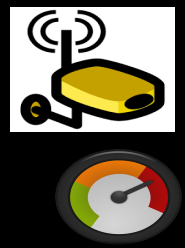
投機的データ収集の必要性
Speculative Data Collection

従来のデータ収集・解析



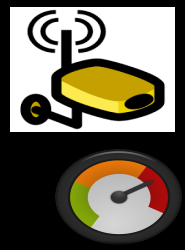
データソース → 受動的データ収集 → データ解析

投機的データ収集・解析



データソース → 投機的データ収集 → 教師データ生成

リアルタイムで教師データを生成するため
有用なサンプルが発するデータにアノテーション付加



データソース → 投機的サンプリング 機械学習 → 母集団 データ解析

IoT MVNO の今後

- アプリケーション毎のトラフィック制御
  - セキュリティ
  - 通信コスト削減・最適化
  - アプリケーション同定（機械学習・ＡＩ）
- 網内機械学習によるトラフィック最適化と制御自動化
  - 「考えるネットワーク」(In-Network Deep Learning)
- MVNOのためのエッジコンピューティング

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
- 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

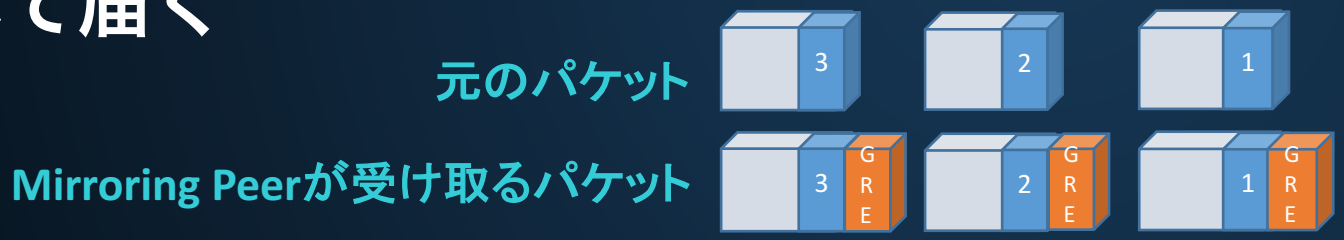
これらをFunnel同様に設定すれば出力開始

Mirroringの動作詳細

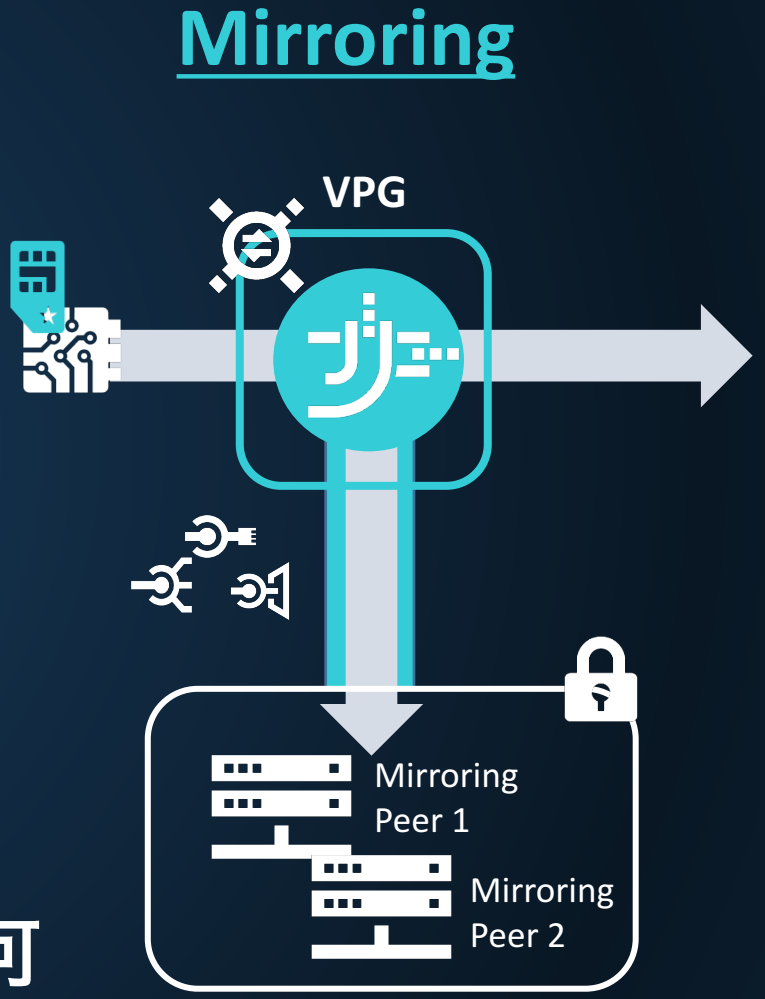
SORACOM Conference "Discovery"

- 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



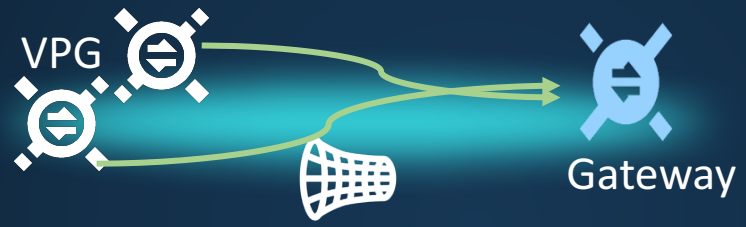
- Mirroring PeerはGREを受信できるように設定することでトラフィックをモニタリング可



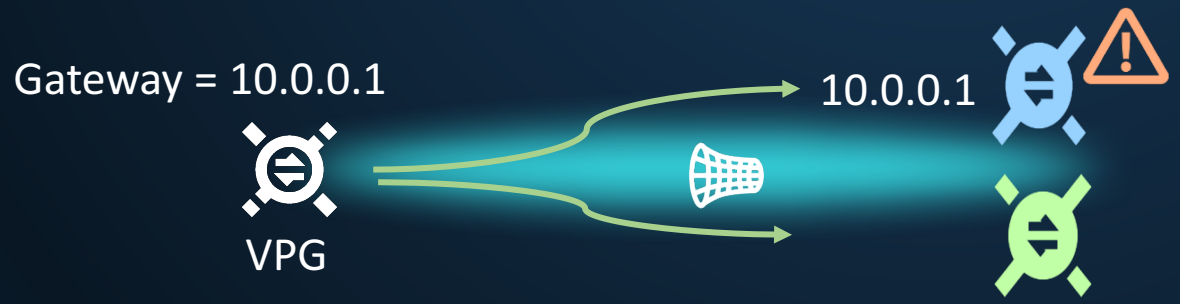
Redirectionの動作詳細

SORACOM Conference "Discovery"

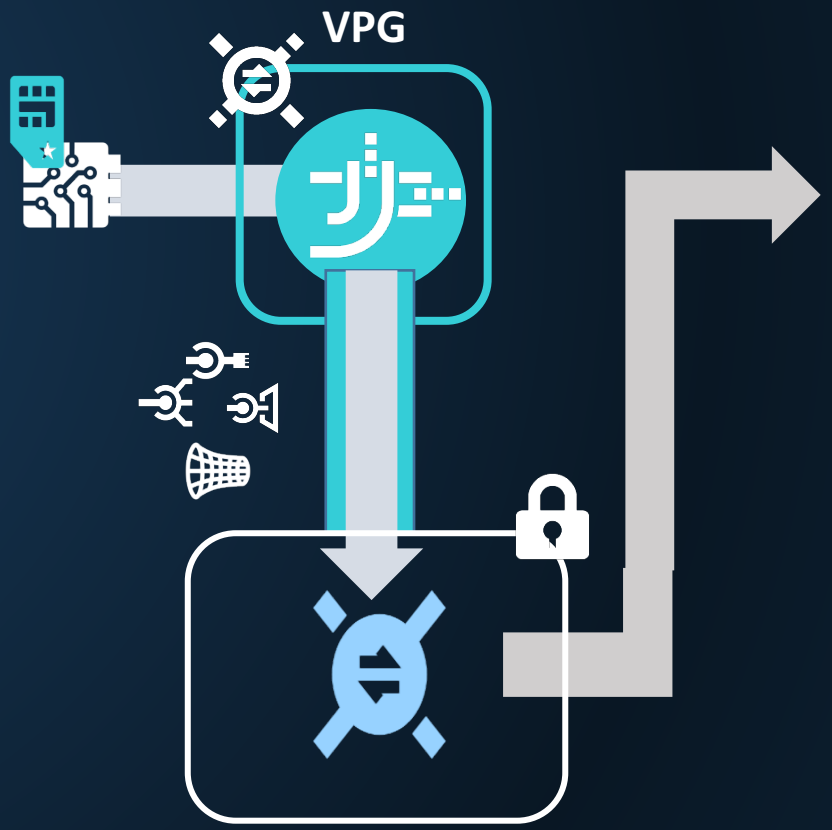
- 仮想L2サブネット上のPeerをGatewayとしてパケットを転送
  - vxlanに対応



- 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の料金

SORACOM Conference "Discovery"

Junction 利用料金

Junction 利用料金 15円/時間

ミラーリング機能、リダイレクション機能、インスペクション機能のいずれかを利用した場合に、Junction利用料金の対象となります。同時に複数の機能を使用しても基本料金は変わりません。

Junction インスペクション利用料金

Junction インスペクション利用料金：100円/時間

インスペクション機能を利用した場合に対象となります。
該当する VPG を使用する SIM 1万枚までとなります。1万枚以上での利用を検討されているお客様は こちらよりお問い合わせください。

おわりに

SORACOM Conference "Discovery"

- SORACOM Junctionの3つの機能を紹介
  - Inspection： 統計情報のレポート
  - Mirroring： トラフィックのコピーを転送
  - Redirection： トラフィックの向き先を変更

SORACOM上のシステムのOperatorである皆様

トラフィックを自由自在に操って新たな世界を

SORACOM Conference "Discovery"

《 株式会社ソラコムのビジョン 》

世界中のヒトとモノをつなげ
共鳴する社会へ

SORACOM Conference
"Discovery"

SORACOM