

SouthSIDE主体の SD-LAN/WANとは

SouthSIDE SDNは
Network AI (Autonomous Intelligence) へと
進化する

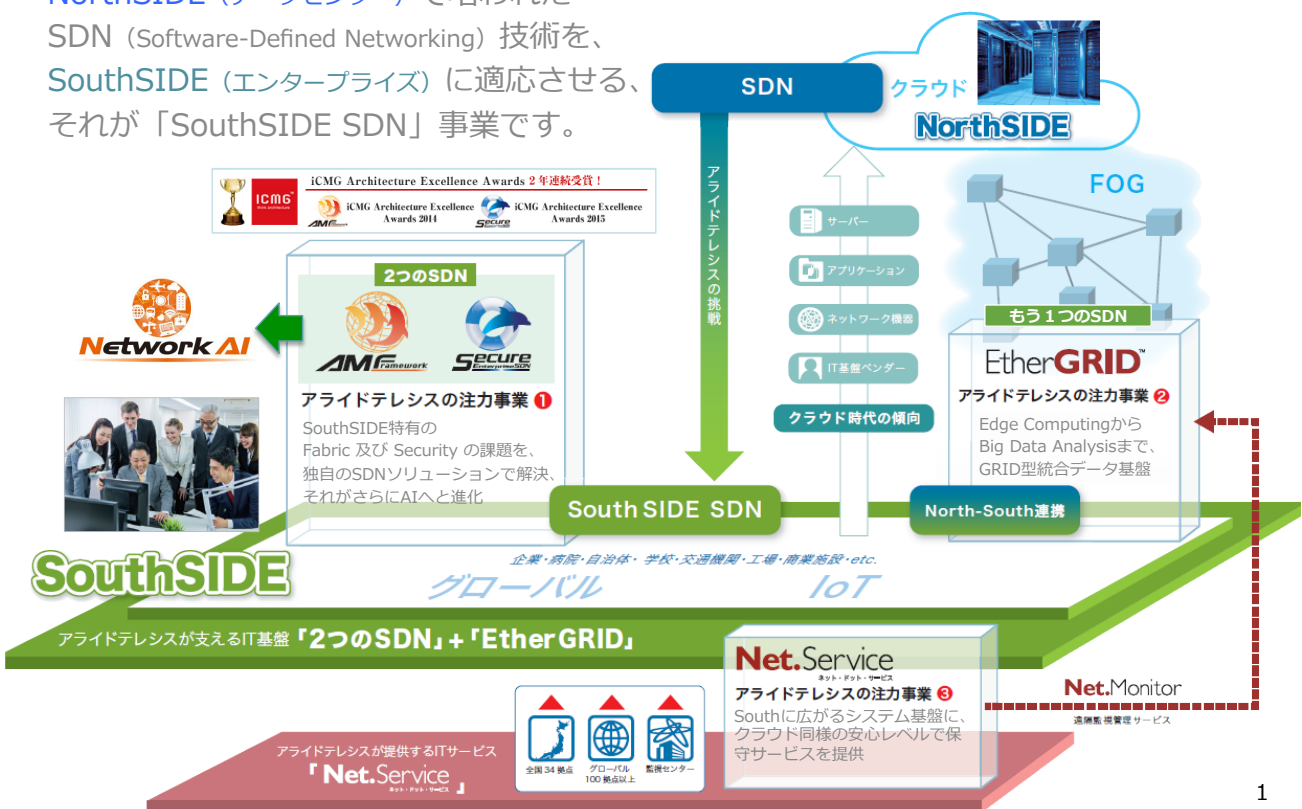
MPLS-Japan 初参加

アライドテレシス株式会社
専務取締役 CMO-Global 川北 潤
2016年11月7日

1

1. アライドテレシスが取り組む事業の概要

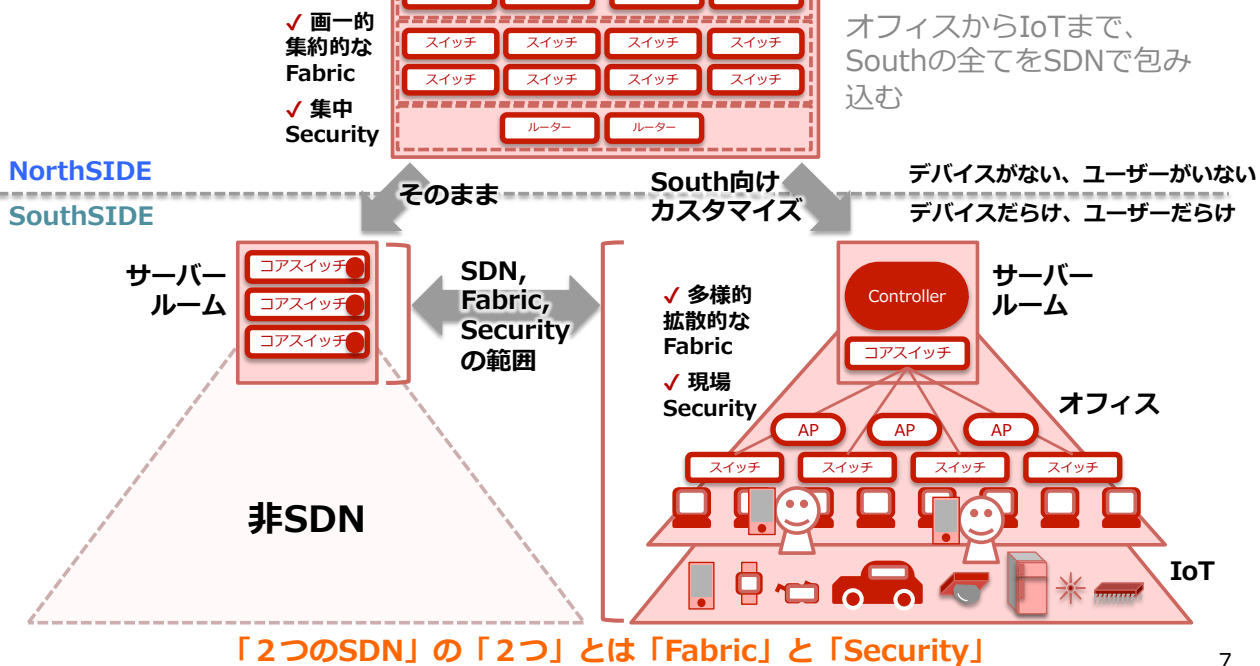
NorthSIDE (データセンター) で培われた
SDN (Software-Defined Networking) 技術を、
SouthSIDE (エンタープライズ) に適応させる、
それが「SouthSIDE SDN」事業です。



1

2. 2つのSDN ①カスタマイズしたポイント

NorthのSDN技術をそのままSouthに転用しても、サーバールーム内では使えない

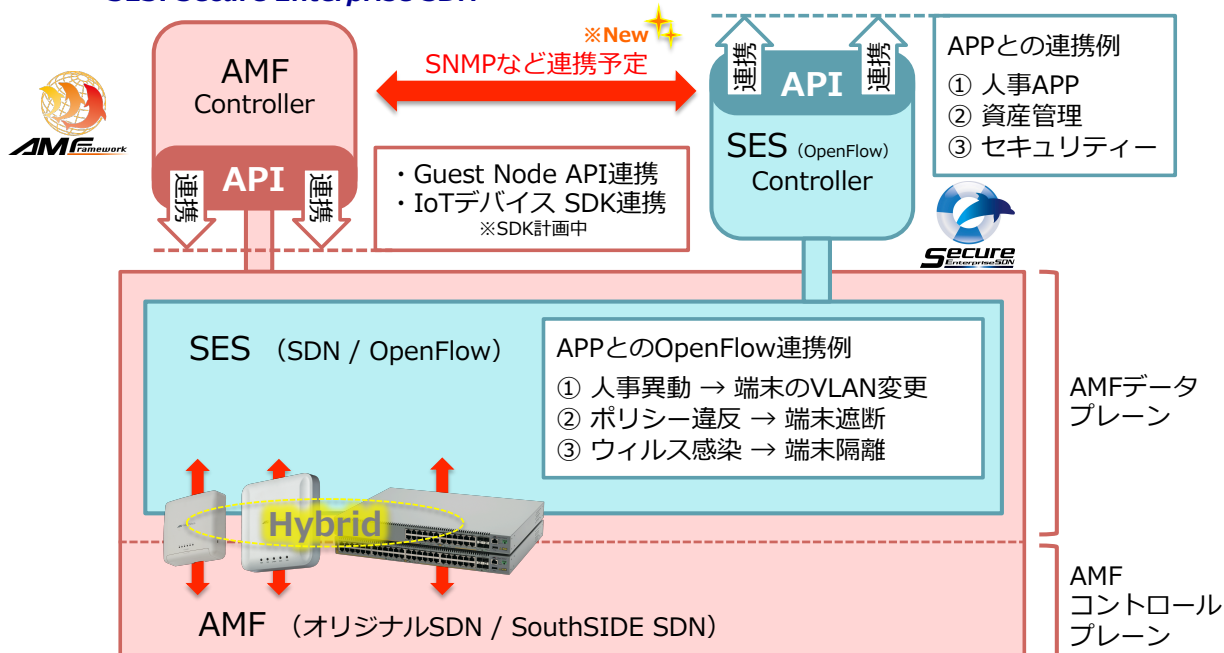


7

2. 2つのSDN ②AMFとSESの関係

2つのSDNとは…

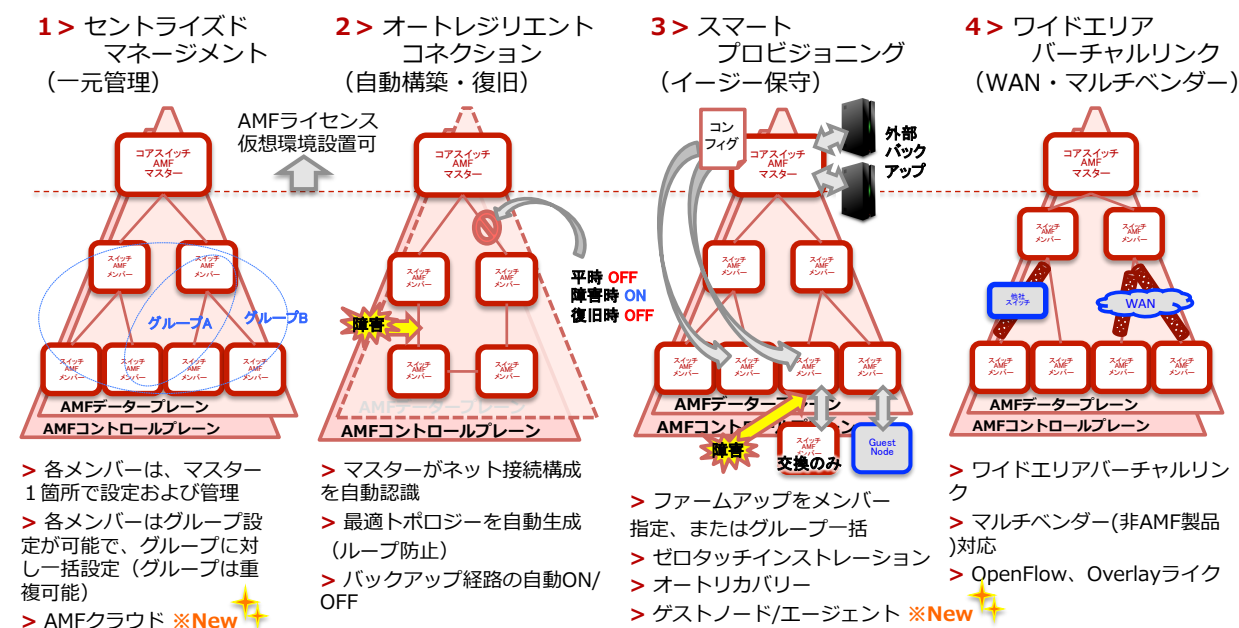
- > AMFでトポロジーを解決（安定したデータプレーンを構築）
AMF: Allied-Telesis Management Framework
- > SESは、そのデータプレーン上でOpenFlowによるAPP連携の通信制御
SES: Secure Enterprise SDN



8

3. AMF概要

AMFの主要機能



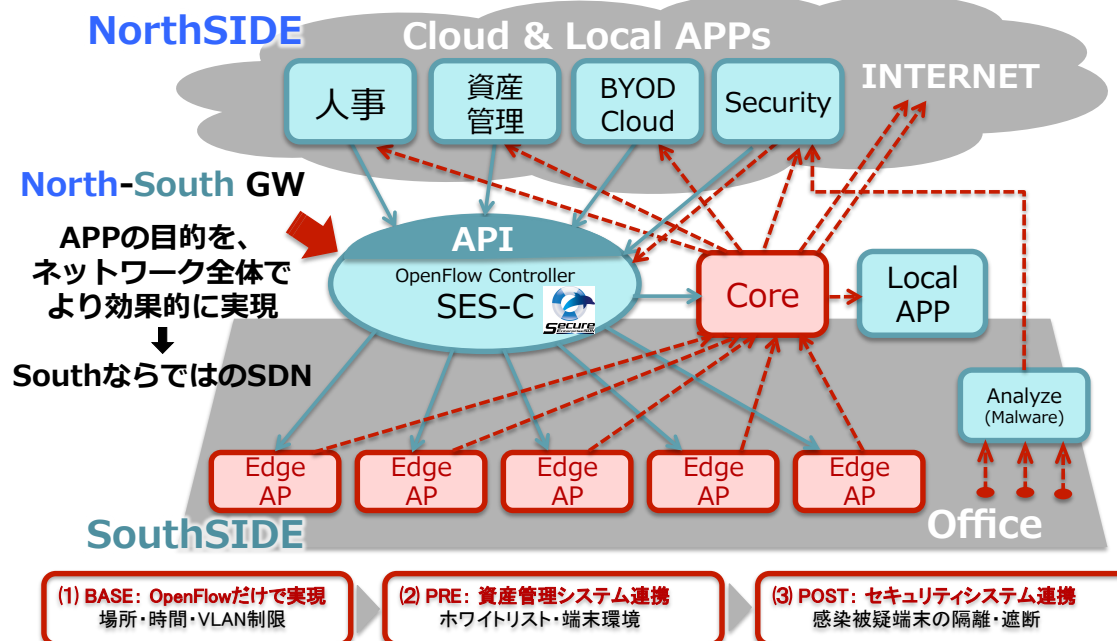
✓ 現場を歩き回らずに設定・運用保守 ✓ 障害復旧は同機種に交換作業のみ
データセンターには存在しない、エンタープライズ向けオリジナルSDN

5

4. SES概要 ①全体構成

SES-C (Controller) と各セキュリティシステムとの連携イメージ

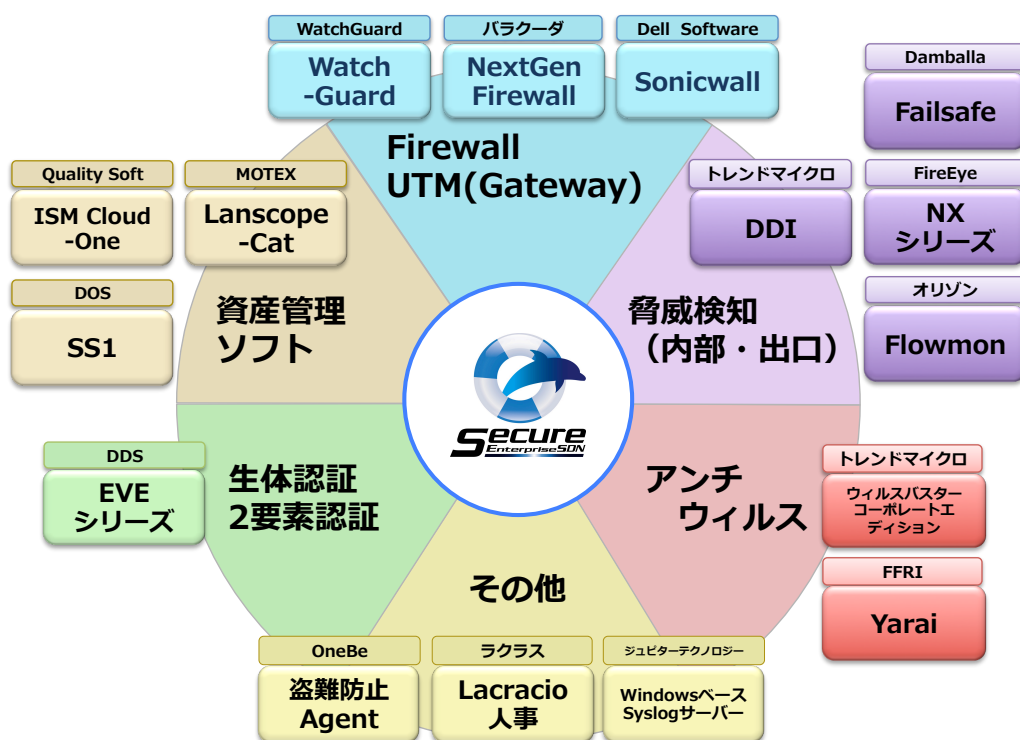
- > APPのステータスで、SouthSIDEの通信フローを変更・制御
- > NorthSIDE - SouthSIDE 連携APIを標準化
- ①CSV-IF ②Syslog-IF ③SNMP TRAP-IF



6

4. SES概要 ②連携APPs

SES連携APP/サービスが急増中！

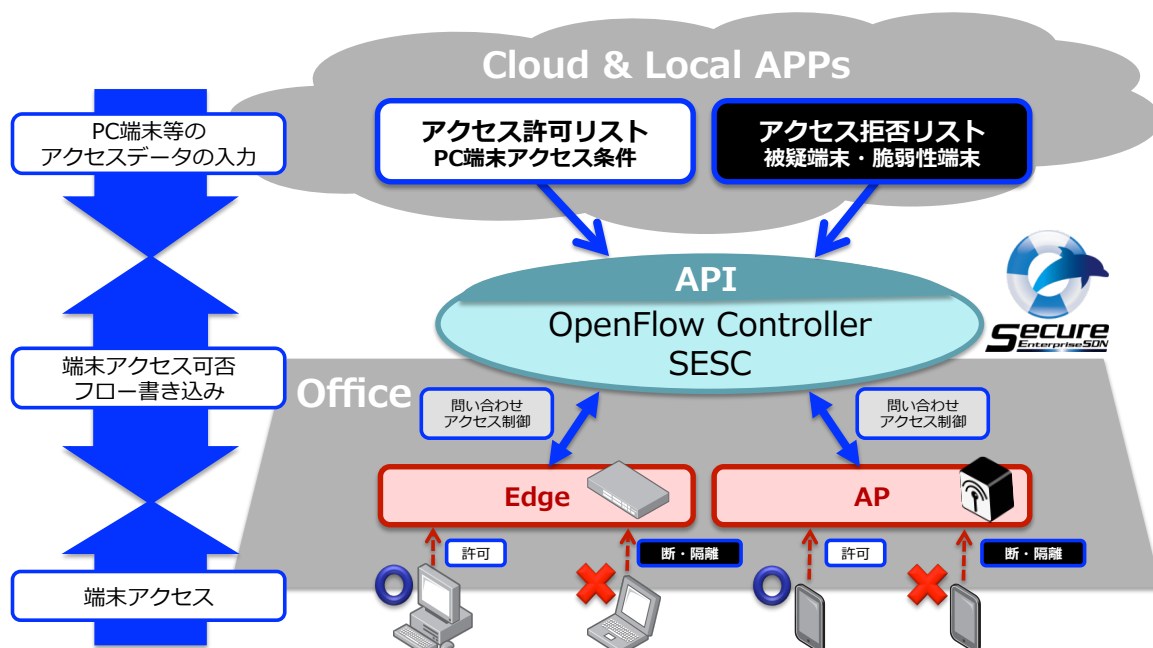


15

4. SES概要 ③仕組み

SESC (SESコントローラー) の主要機能

➢ 様々なアプリケーションとエッジ機器 (スイッチ/無線アクセスポイント) を連携させ、エンドポイントセキュリティの強靭性を向上させる。

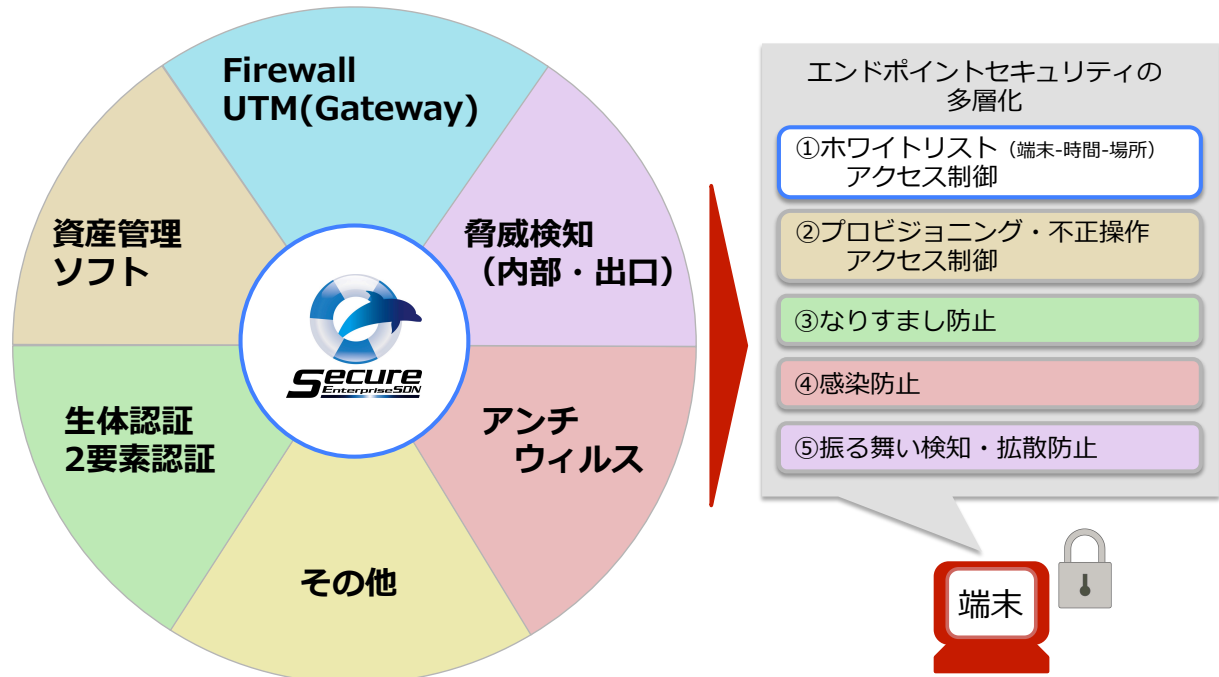


8

4. SES概要 ④多層化の効果

SES: Secure Enterprise SDN

SESは様々なカテゴリーのセキュリティソリューションと連携
その結果、“エンドポイントセキュリティ”は多層化され強固になる

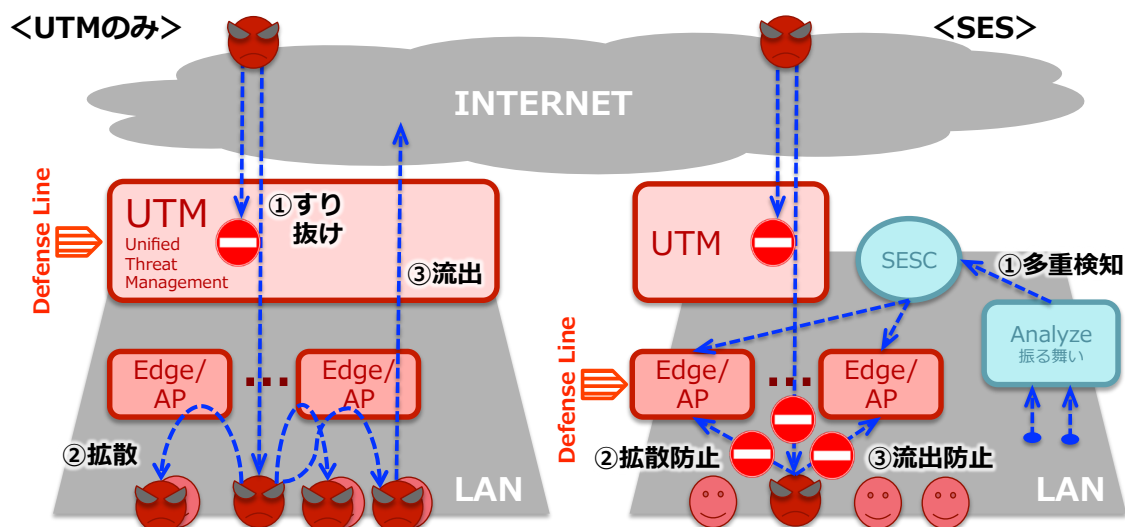


15

4. SES概要 ⑤ディフェンスライン

SESの代表的な導入効果

- > UTM/FWでは、端末単位の隔離ができない
- > SESなら“ディフェンスライン”を、Edge/APへ下げて遮断/隔離



UTM（ファイアウォール）単体では万全ではない。
すり抜け・内部感染・拡散・流出など、
様々な脅威が散在している。

感染端末や違反/未登録端末をEdge/APで
遮断/隔離し、拡散・情報流出を防止。
更に内部での振る舞い検知など、脅威を多
重に検知しEdge/APで遮断/隔離。

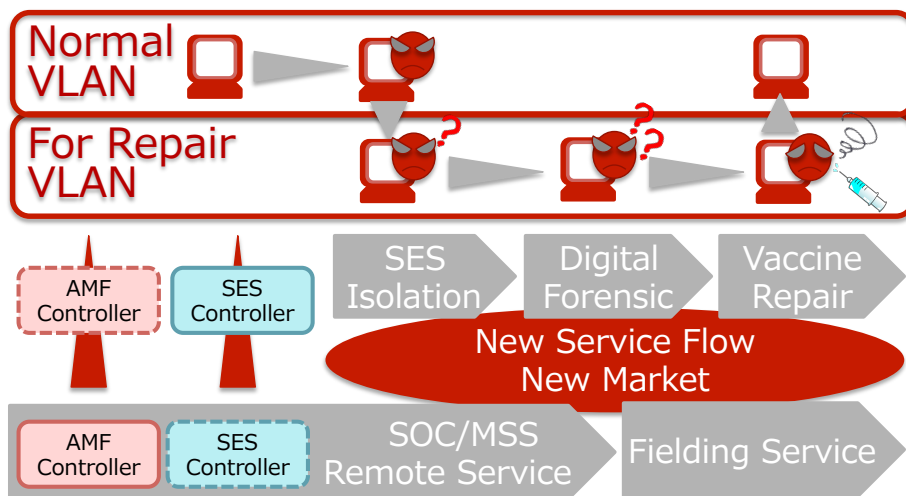
10

5. 2つのSDNで進化する保守フロー

2つのSDNで実現する新しい保守フロー「Isolation Adapter」

> セキュリティAPP・エンドポイントセキュリティと連携し、新たな保守サービス事業が実現

クライアントネットワーク



<SES系>

- ①遠隔隔離:
各APPとSES連携し感染端末を自動隔離
- ②遠隔フォレンジック:
- ③遠隔ワクチン/ワイプ:
- ④遠隔復旧:
各APPとSES連携し修復端末を自動復旧
- ⑤現地サービス:
遠隔での「②③④」が困難な場合の現地サービス

<AMF系>

- ①遠隔設定:
AMF/SES対応ネットワーク機器のコンフィグなどを一元管理・遠隔管理
- ②遠隔復旧:
障害時、現地は交換作業だけで自動復旧

✓NECフィールドイング様 “セキュリティインシデントサポートサービス”開始！
“セキュリティテクニカルセンター” 開設！
その他、大手サービスベンダーも計画中！

11

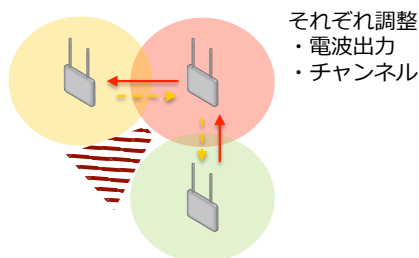
6. Network AI (Autonomous Intelligence) へと進化するSDN ①-2



①京都大学共同研究AWC (Autonomous Wave Control) その1

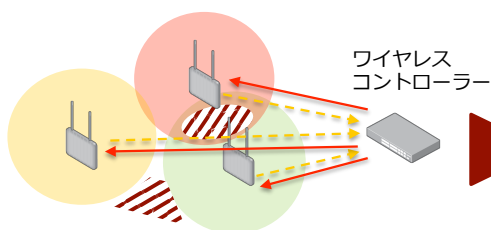
方式A : AP間で調整

→ 1対1で調整のためムラが発生



方式B : コントローラで調整

→ 平均値で調整のためムラが発生



AWC方式 :

ゲーム理論 (相互依存)
・送信電力制御法
・チャンネル選択法

各APの接続構成を全体把握して
電波出力・チャンネルを最適化



サイトサーベイ 必要

サイトサーベイ 不要

12

6. Network AI (Autonomous Intelligence) へと進化するSDN ①-2

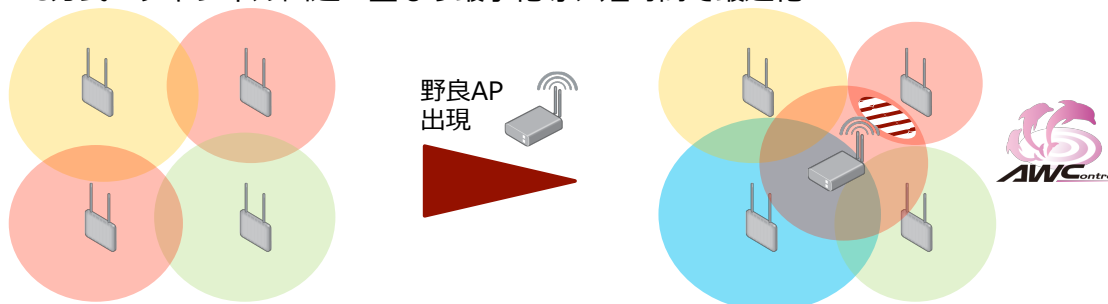


①京都大学共同研究AWC (Autonomous Wave Control) その2

従来方式：電波出力およびチャンネル調整困難→遠慮



AWC方式：チャンネル回避・重なり最小化等、短時間で最適化



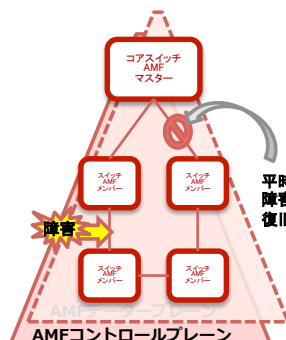
13

6. Network AI (Autonomous Intelligence) へと進化するSDN ②

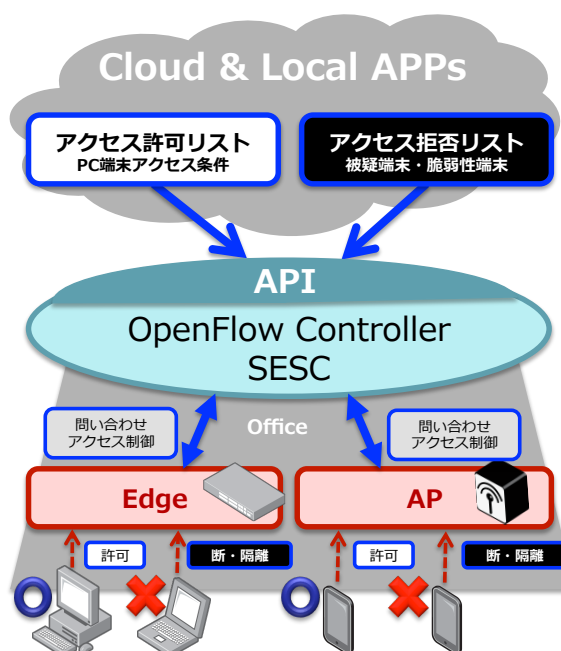
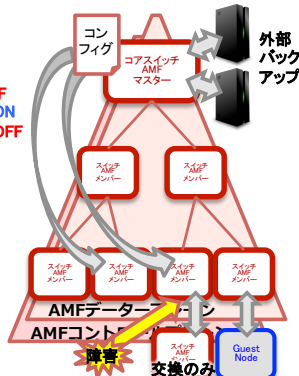


②もともと「2つのSDN」はAIを目指している
社会に無尽に広がるIoTデバイスに最適な、自律管理&メンテナンス

> オートレジリエント
コネクション
(自動構築・復旧)



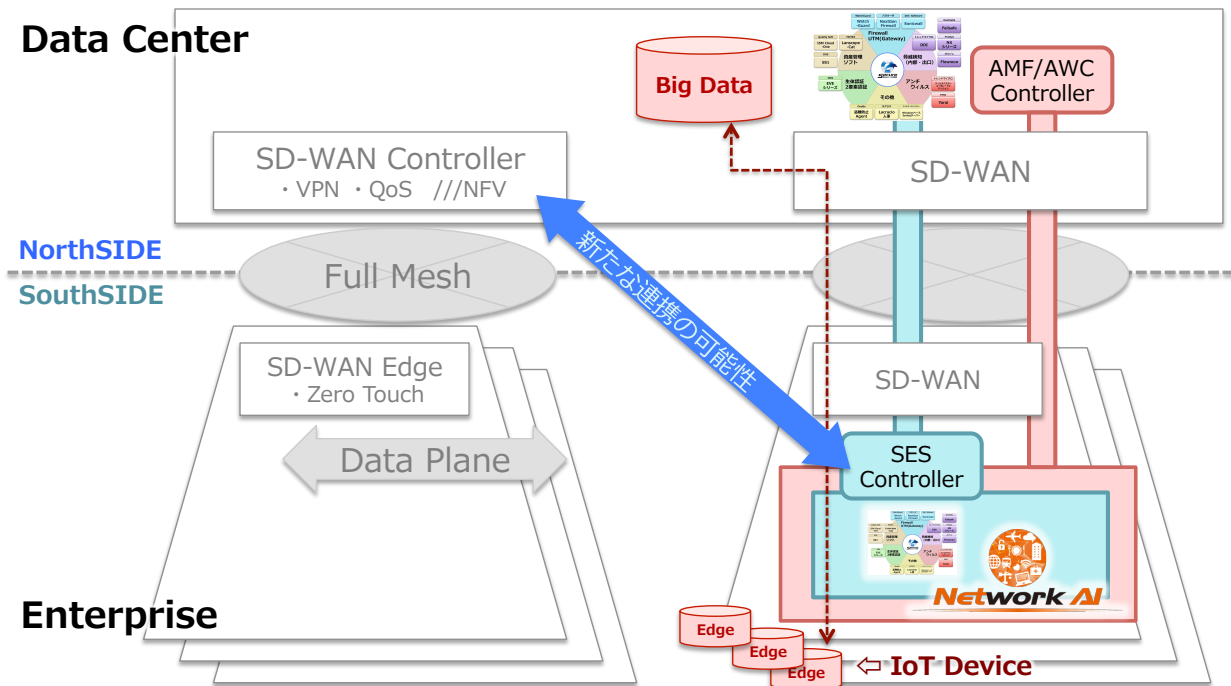
> スマート
プロビジョニング
(イージー保守)



14

7. SouthSIDE主体のSD-LAN/WAN

SouthSIDE（エンタープライズ）の興味は、結果的にAPPやデータが効率的・効果的・安全に使えるかどうか。そこでアライドテレシスでは、APP連携やデータ連携に重きを置いてNorthSIDEとSouthSIDEの関係づくりを進めている。



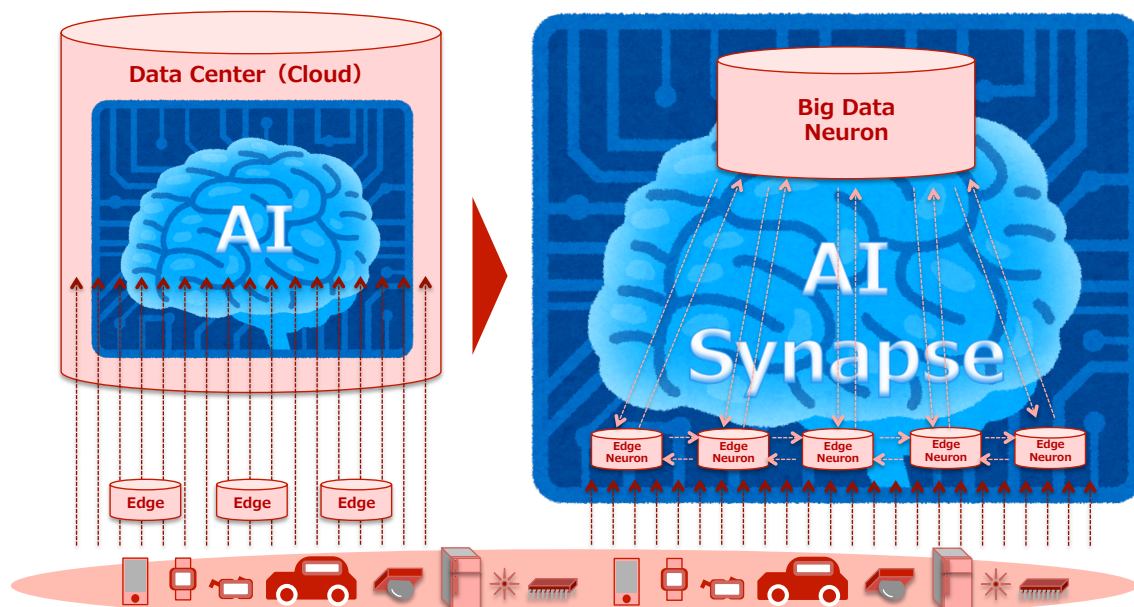
15

8. IoT Data Exchange ①AIの進化を予見

IoTとAIは密接な関係にある。AIはBig Data上で思考するが、そのBig Dataは社会に無尽に広がるIoTデバイス（センサー）が発したデータを集めたものだ。今後は、集めてからAIが機能するのではなく、集める段階からAIが機能する（Synapseが飛び交う）ように進化することが考えられる。

現在のAI: クラウドに閉じこもった構造で、IoTデータが集まってからでないと機能しない。

GRID AI: サーチ技術と融合し、欲しいデータをトローリングするが、機械学習で効率的にデータを集める。この時、サーチ（トローリング）はAIの一部となる。それはあたかも、脳内のニューロンとシナプスの関係のようだ。



16

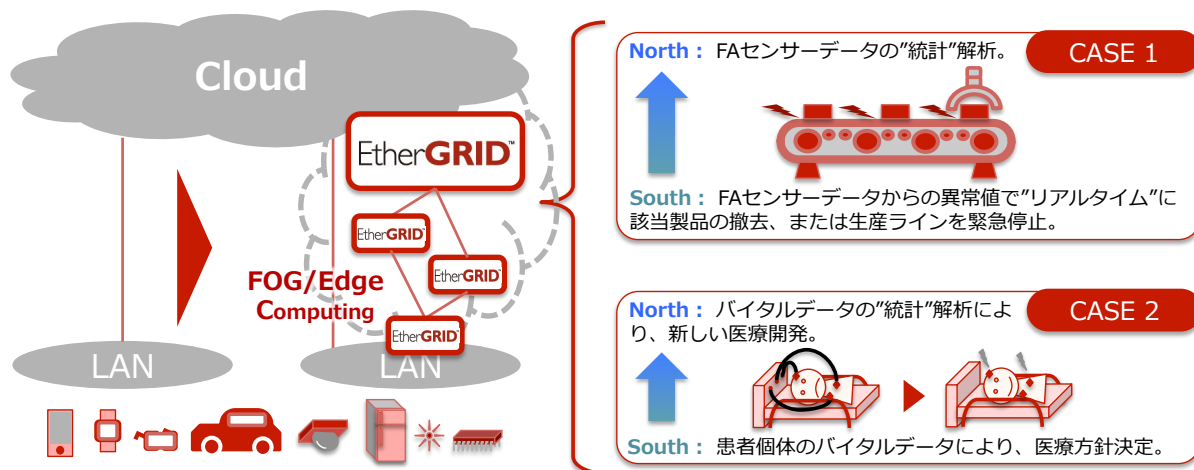
8. IoT Data Exchange ②IoTデータはマルチユース

IoTデータの利用目的はそれぞれである。Edgeでの利用目的はリアルタイムな分析、データセンタでは統計的な分析が多い。

さて、複数のIoTセンサーを個々の目的別に設置するのは難しく、今後はIoTデータの流通（マーケットプレイス）が行われるだろう。1つのIoTセンサーは複数のAnalysis APPやAI APPに使われ、1つのAPPは複数のIoTデータの海をサーチする。N対Nの関係である。

この時、N対Nのマーケットプレイス基盤はEdge（IoTデータの発生源）からクラウドまで、GRID型になっていることが望まれる。

また各データに共通フォーマット（Schema）など決められるはずもなく、Schema LessのSearch Engineの活用が期待がかかる。



<IoTデータがマーケットプレイス化する内容のレポート（McKinsey）>

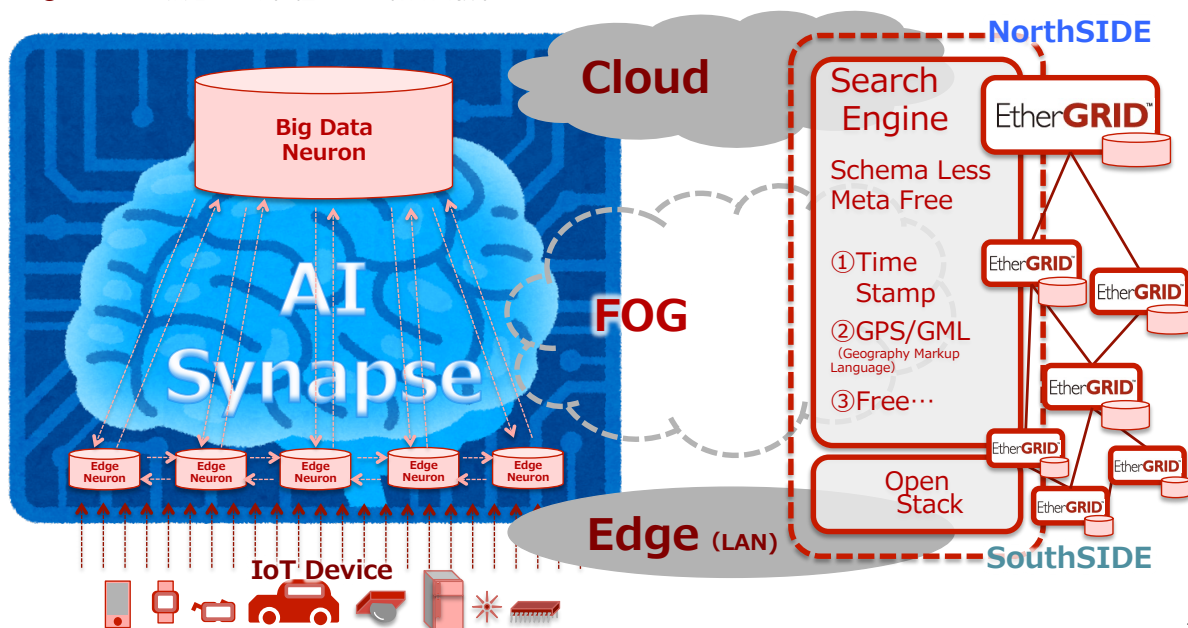
<http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a-successful-internet-of-things-data-marketplace>

17

8. IoT Data Exchange ③GRID AIの基盤設計

GRID AIのシステム基盤には次の特徴を要求される。

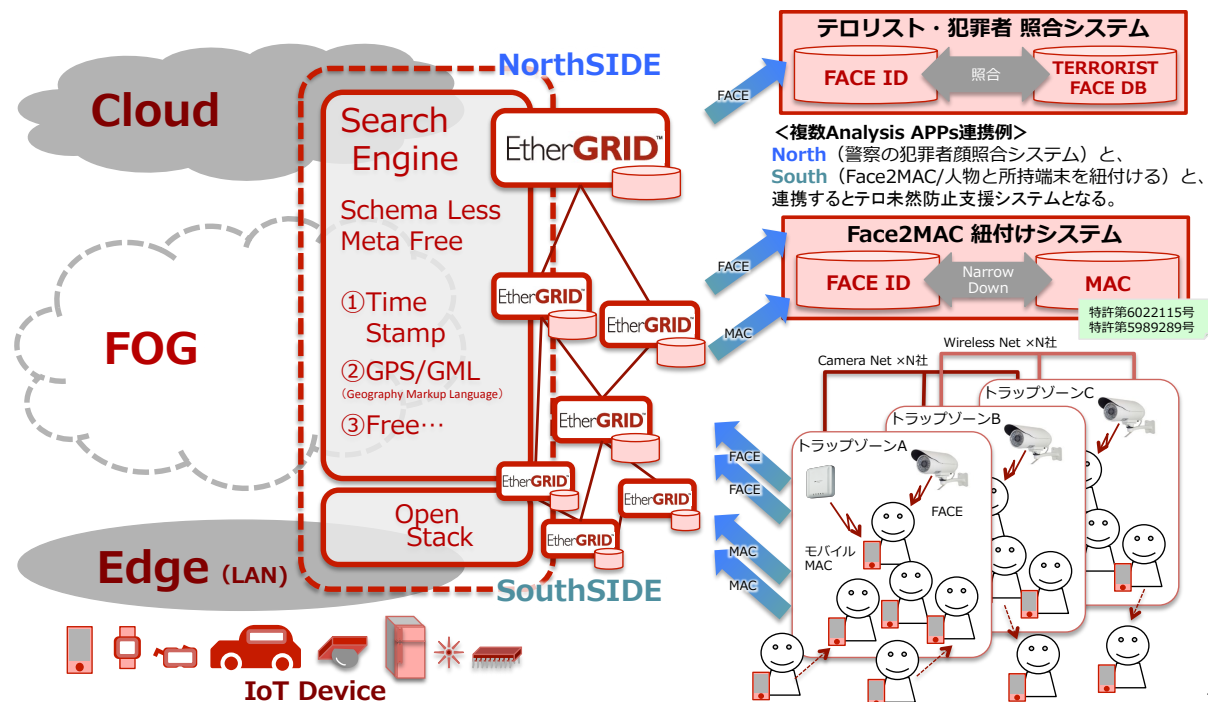
- ①: 新しい物理ディスクの追加が簡単にできる。→ OpenStack + ?
- ②: 新しいEdge（データプール）の追加が簡単にできる。→ Search Engine + ?
- ③: 無数のデータプールを検索したり、連携させることができる。→ Internet + ?
- ④: データフォーマット（Schema）はフリー。→ Search Engine + ?
- ⑤: データを流通させる仕組み。→ 特許出願中



18

8. IoT Data Exchange ④展開例（Face2MAC）

様々な監視カメラのオーナー（警備会社、飛行場、コンビニ、マンション管理室など）がいる。同じく様々なWiFi-APのオーナーがいる。
警察は、横断的にメタデータ“Face”を探し、見つかった実データ（顔イメージ）を入手し、テロリストDBと照合をかける。
Face2MACシステムは、トラップゾーンを決める。ゾーンに発生したメタデータ“Face”を探し、一方で同じゾーンに発生した“MAC”アドレスを入手する。
複数のゾーンでタイムスライスによる変化を分析し、両者の紐付け（誰がどの端末を所持しているか）を絞り込む。
警察がテロリストを発見すると、そのテロリストが所持している可能性の高い端末アドレス情報を提供できる。



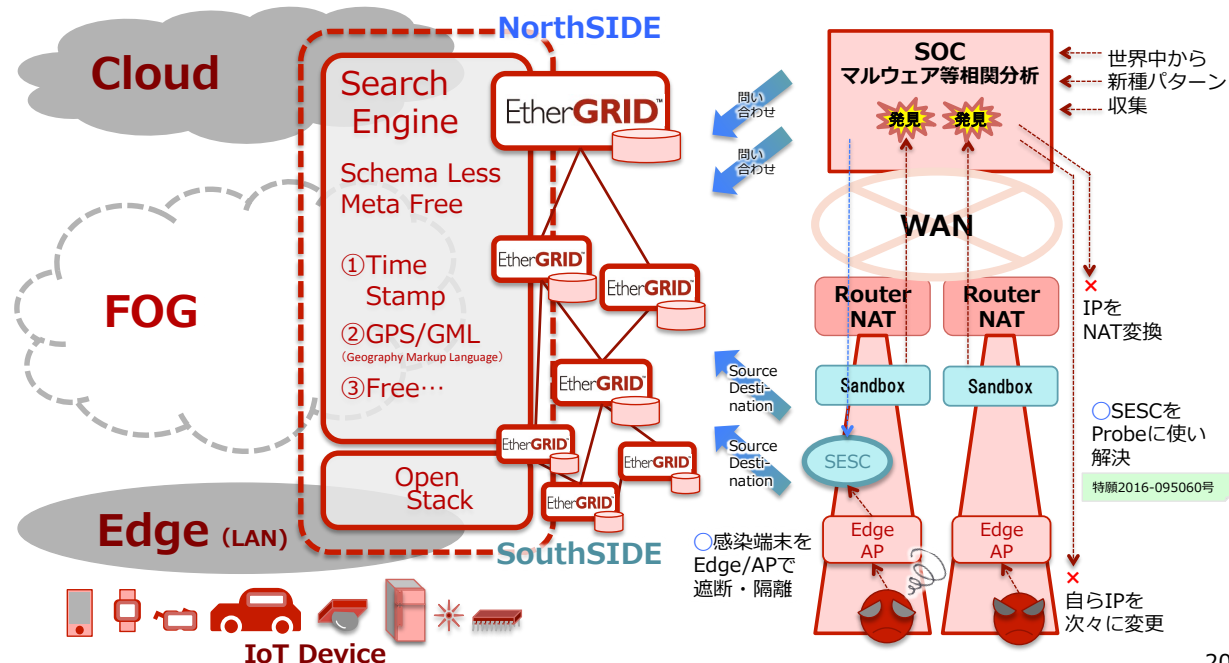
19

8. IoT Data Exchange ⑤展開例（連携セキュリティ）

マルウェア等の脅威は日に日に巧妙化し、その攻撃パターンの収集や分析は、ゼロデイ問題や最新パターン情報の収集力を考えれば、エンタープライズのLAN上よりもSOC（データセンター）で行われることが望ましい。しかし、WAN越えによるNAT変換や、マルウェア自身のIP変更により、SOC側で脅威を発見しても、どの端末の通信を遮断・隔離すればよいのか即座に判断がつかない。

RouterからNAT変換のログ情報を抽出して紐づけする方法もあるが、既存Routerにその機能やパフォーマンスを求めることは難しい。

そこでOpenFlowの特性を利用し、この問題を解決する。通信開始時にEdgeからSESC（OpenFlow Controller）に通信の可否について問い合わせがいく。この時に収集できるsource/destination情報をSOCと共有することで、対象を特定することができる。



20

9. SouthSIDE SDN Exchange (エコシステム)

SouthSIDE SDNマーケットのエコシステム“ SouthSIDE SDN Exchange”



お申し込みはこちらまで↓↓↓↓↓

https://www.allied-teselis.co.jp/event/seminar/exchange2016_2/index.html

✓ C社,J社は自前で
APPを品揃え

✓ H社は特定技術と提携

✓ SouthSIDE SDN市場
を、中立・オープンにエ
コシステム化できるのは、
アライドテレシスだけ

Create Together,
a New Market!
2016下期 カンファレンス
11/17 大阪・11/25 品川
連続開催予定



2016上期カンファレンスの様子 名古屋・品川 21



Allied Telesis

ご静聴ありがとうございました