サイバーセキュリティ対策セミナー / JIPDEC

IoTデータ"超"分散処理時代を迎え、CSIRT見直しのポイント

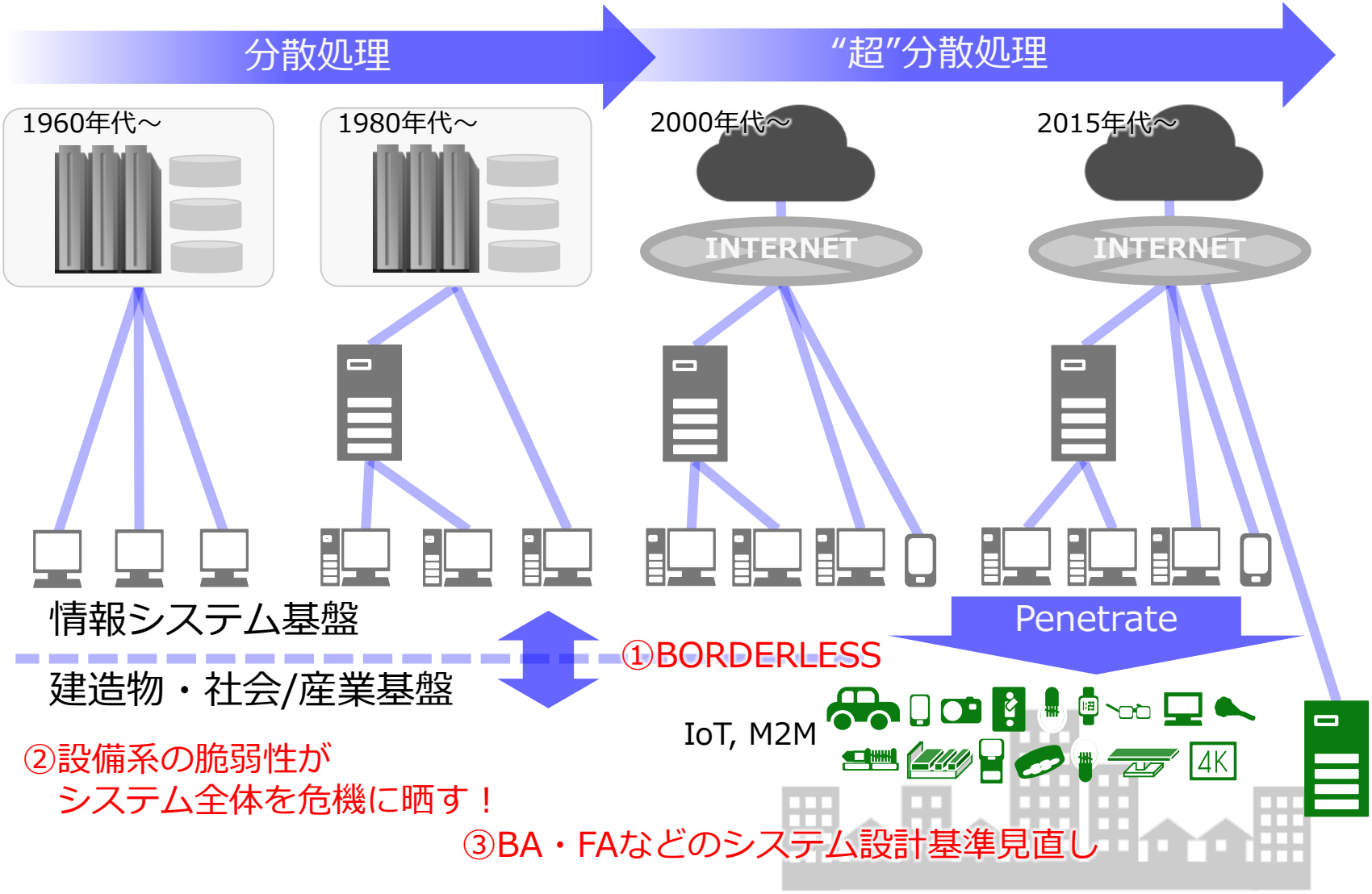
アライドテレシス株式会社
専務取締役 CMO-Global 川北 潤

Allied Telesis

1. ”超”分散処理で、ネットワークが変わる

IoTデバイスは、さまざまな社会の物理構造体に溶け込んでいく。
サイバー/フィジカル、個別に進化してきたセキュリティも融合されるべき。

Society 5.0
デジタルコンバージェンス

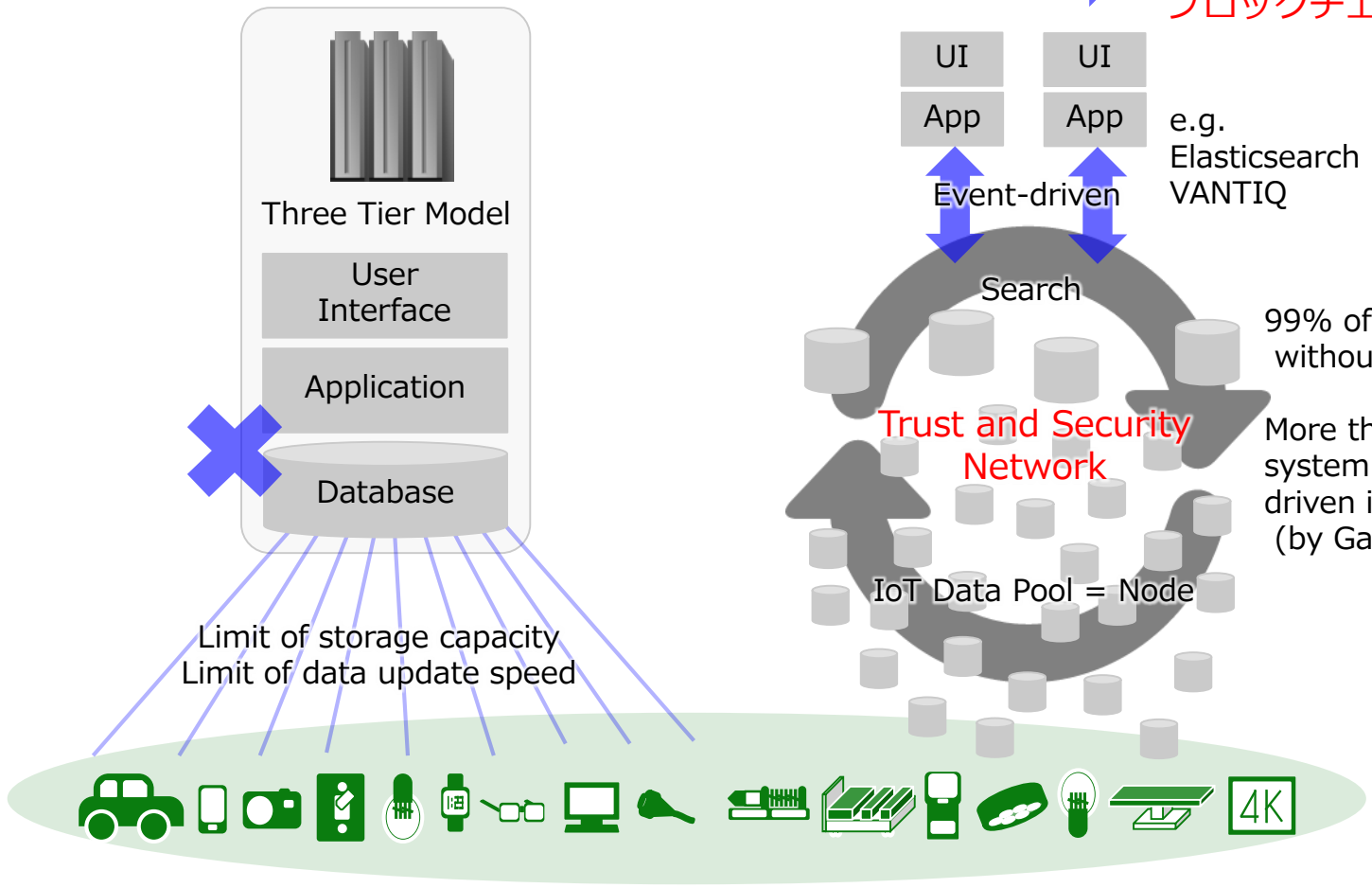


2. ”超”分散処理で、データの流れが変わる

IoTデータ”超”分散処理によりシステム設計の常識が変わる。
更新型データベースシステムから、イベントドリブン型システムへ。
これまで以上に、ネットワークが重責を担う。

“超”分散処理 = “超”連携処理

＜社会の仕組みも変わる＞
企業間サプライチェーン
シェアードエコノミー
ブロックチェーン決済

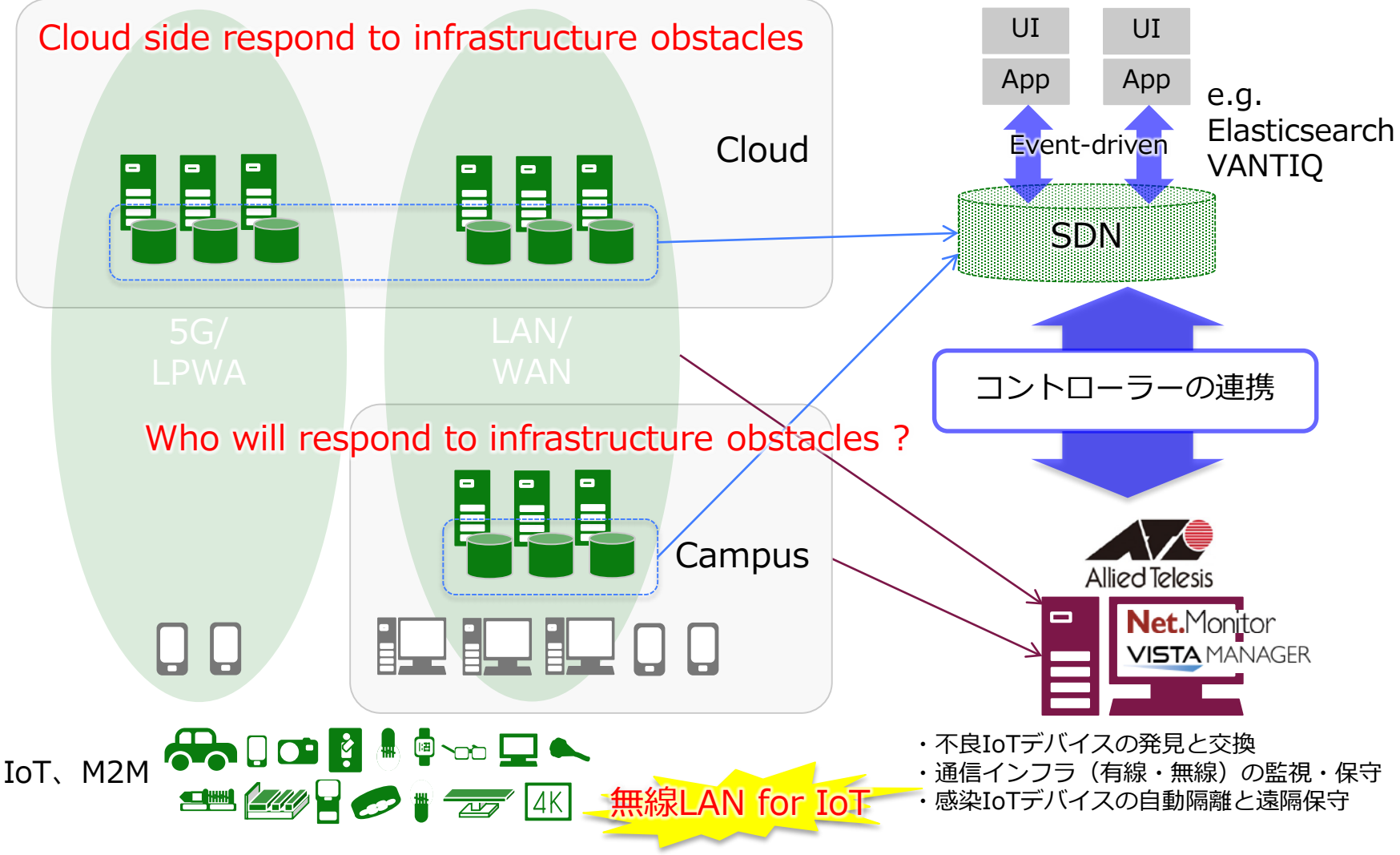


99% of data is discarded without using it.

More than 50% of the system will be Event-driven in 2020.
(by Gartner Report)

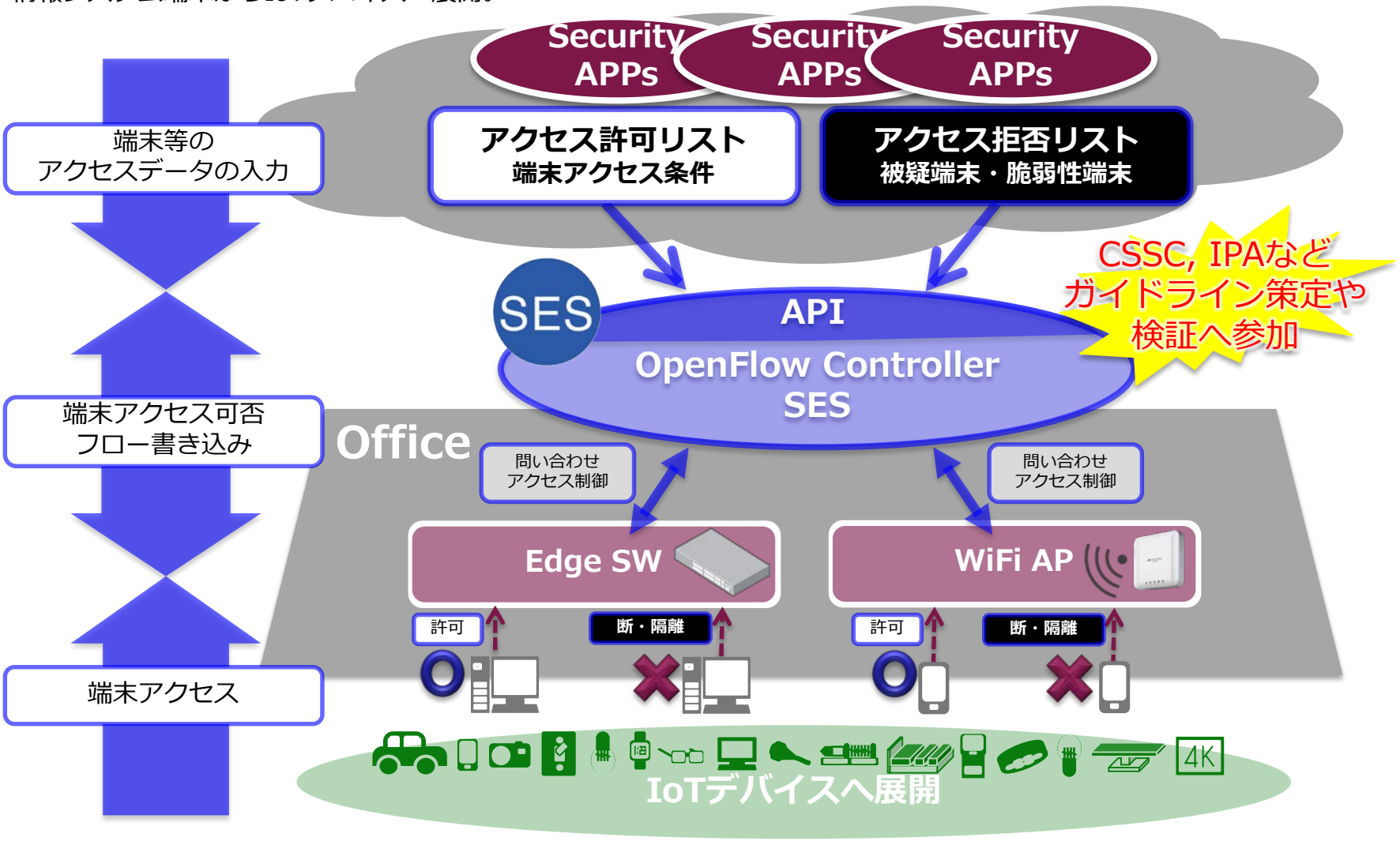
3. ”超”分散処理で、再びキャンパスサイドに脚光

NorthからSouthまで連携する超分散処理システムの保守は、クラウドサービスに頼っているだけでは解決しない。
IoTデバイスが広がるキャンパス側の保守が要となる。
LPWA/5Gで全てのIoTデータがクラウドに直収されるわけではない。通信費用も課題。



4. アライドテレシスの取り組み ①

各種デバイスをネットワークで守るSES（Secure Enterprise SDN）。
各種セキュリティシステムと連携し、デバイスからの通信を許可・遮断・隔離。
情報システム端末からIoTデバイスへ展開。



4. アライドテレシスの取り組み ②

SES連携、セキュリティAPPs一覧。
エコシステムによって、IoTデバイス対応を促進する。

2018年4月1日時点・詳細は次のURLにてご確認下さい
https://www.allied-telesis.co.jp/solution/applications/

次世代ファイアウォール/UTM・アプリケーションゲートウェイ

WatchGuard Firebox シリーズ
SONICWALL SonicWall
SOPHOS XG Firewall
Barracuda NextGen Firewall Fシリーズ
paloalto PA・VM シリーズ
FORTINET FortiGate
Allied Telesis AT-AR3050S/4050S
i-FILTER

標的型攻撃対策アプライアンス・監視/分析/異常検知・IoT/IIoT対策向け監視/分析/異常検知

DAMBALLA
FireEye NX シリーズ
Deep Discovery™ Inspector
VISUACT X
Flowmon Driving Network Visibility
NIRVANA-R
SECURITY MATTERS
Zingbox

エンドポイントセキュリティ・不正操作対策・検疫/脆弱性対策・連携支援ツール

Yara!
Protect Cat プロテクトキャット Powered by Cylance
ISM CloudOne ふるまい検知オプション
Zerona Zerona PLUS
ウイルスバスター™ Corp.
LanScope Cat
ISM CloudOne
秀
Adiscon WinSyslog
Kiwi Syslog Server

IT資産管理・人事管理

LanScope Cat
ISM CloudOne
SKYSEA Client View
System Support best1
LIP

生体認証・入退室管理・RADIUS認証

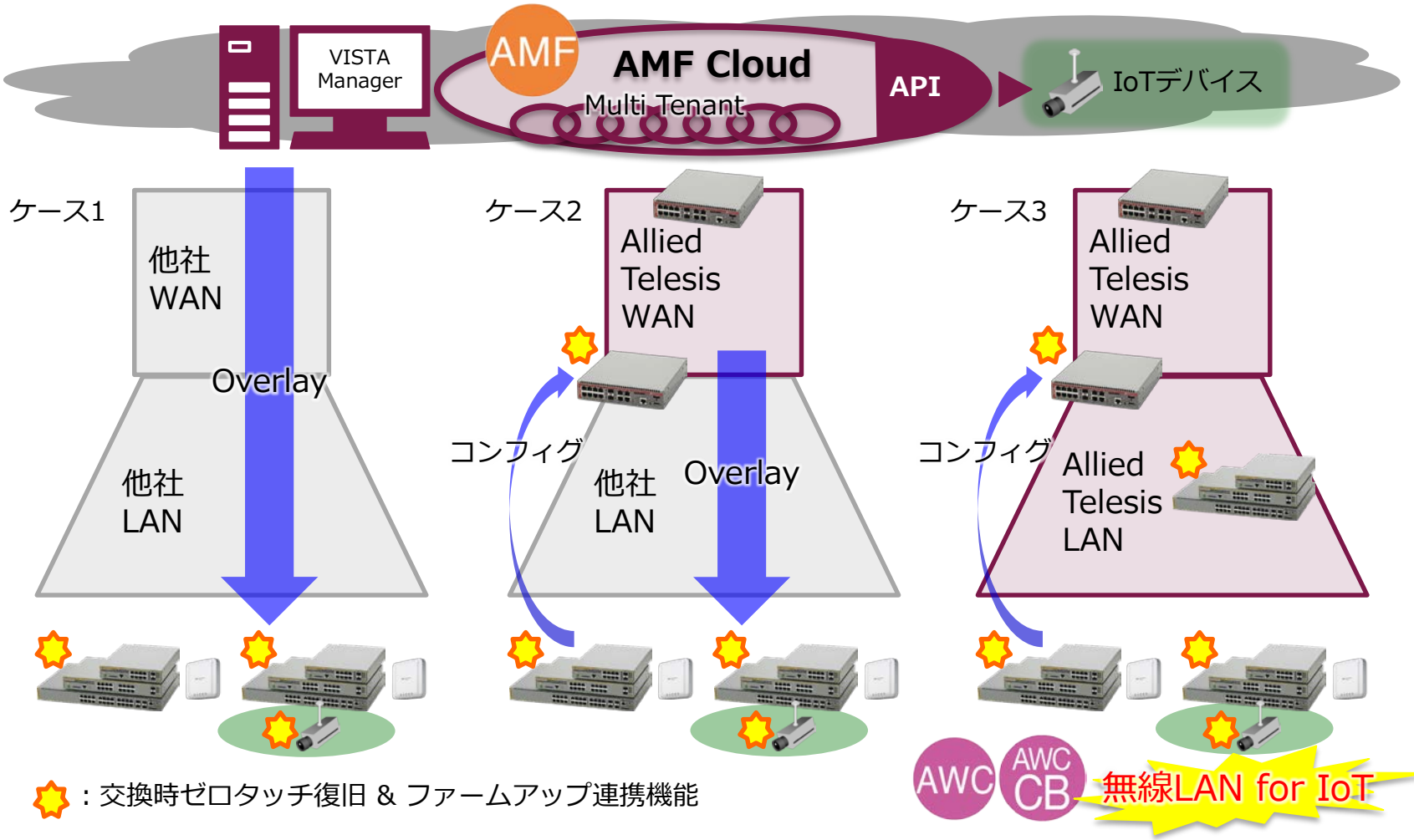
Taikoban
Finger Authentication EVE FA
Webvisor
iBAOS-FX

SES + Cyber Security Labs

4. アライドテレシスの取り組み ③

AMF（AlliedTelesis Management Flamework）で実現する、インテリジェントIoTデバイス管理。

一元管理: ネットワーク機器類をセンターで一元管理。現場にネットワークに詳しい担当者は不要。
ゼロタッチ: 障害発生時、同じ機種に交換するだけで自動復旧。周囲の機器がコンフィグ情報をバックアップ。
IoTデバイス連携: API連携により、インテリジェントIoTデバイスのファームアップやコンフィグ変更をネットワーク側から実行。



5. CSIRT見直し必至

CSIRTマニュアルの、事実上不可能な初動・やってはいけない初動は見直すべき。

実例1「LANケーブルを切り離し窓口に連絡する」

→ マルウェアは夜中や週末に暴れるので不可能　→ 自動隔離へ

→ マルウェアは抜線すると証拠隠滅するため、フォレンジックができない　→ 検疫VLAN隔離へ

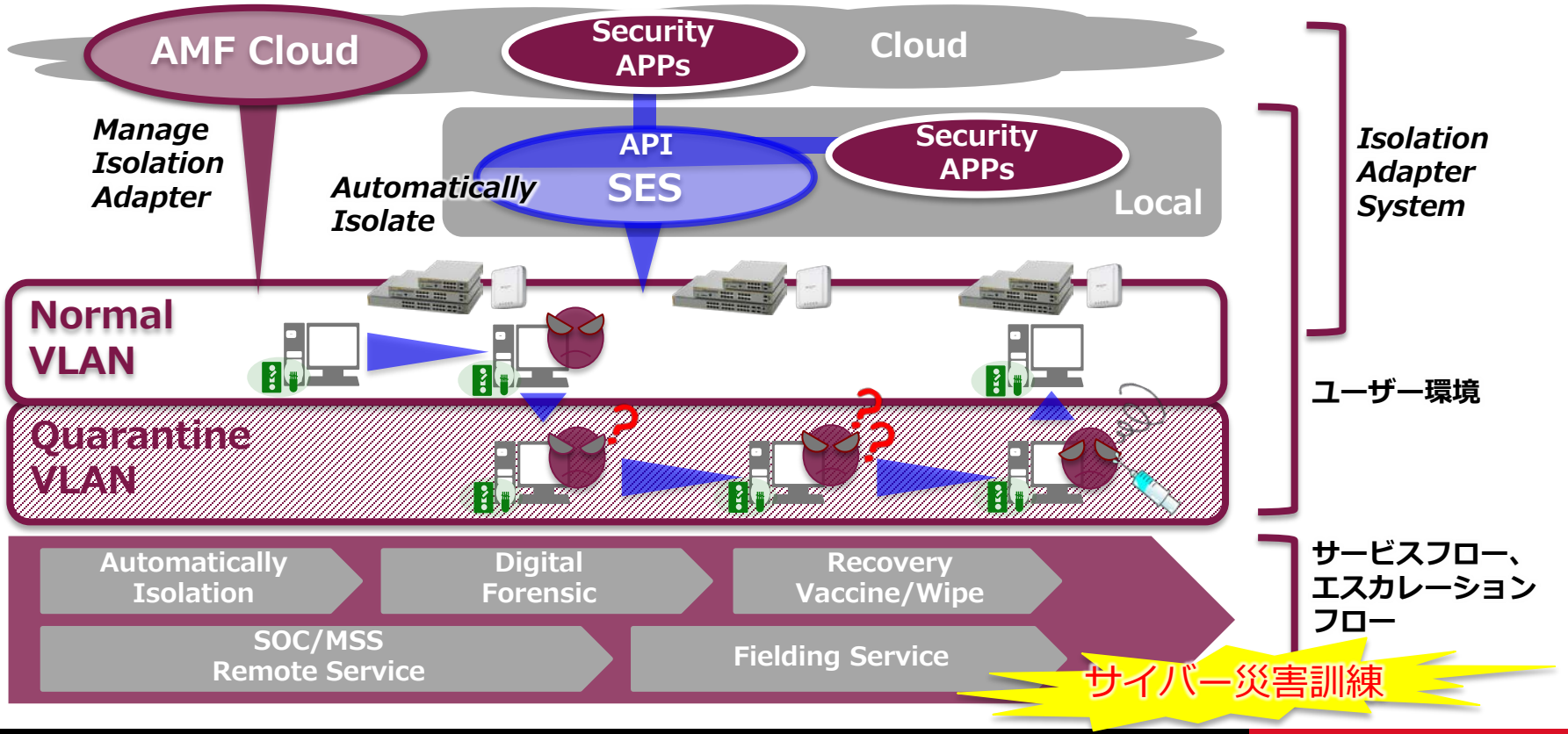
→ 無線LAN接続の場合、抜線できない　→ 検疫VLAN隔離へ

実例2「電磁波を遮断するシールドボックスに感染端末を隔離する」「無線LANの通信圏外へ端末を移動し保管する」

→ 非現実的な対応　→ 検疫VLAN隔離へ

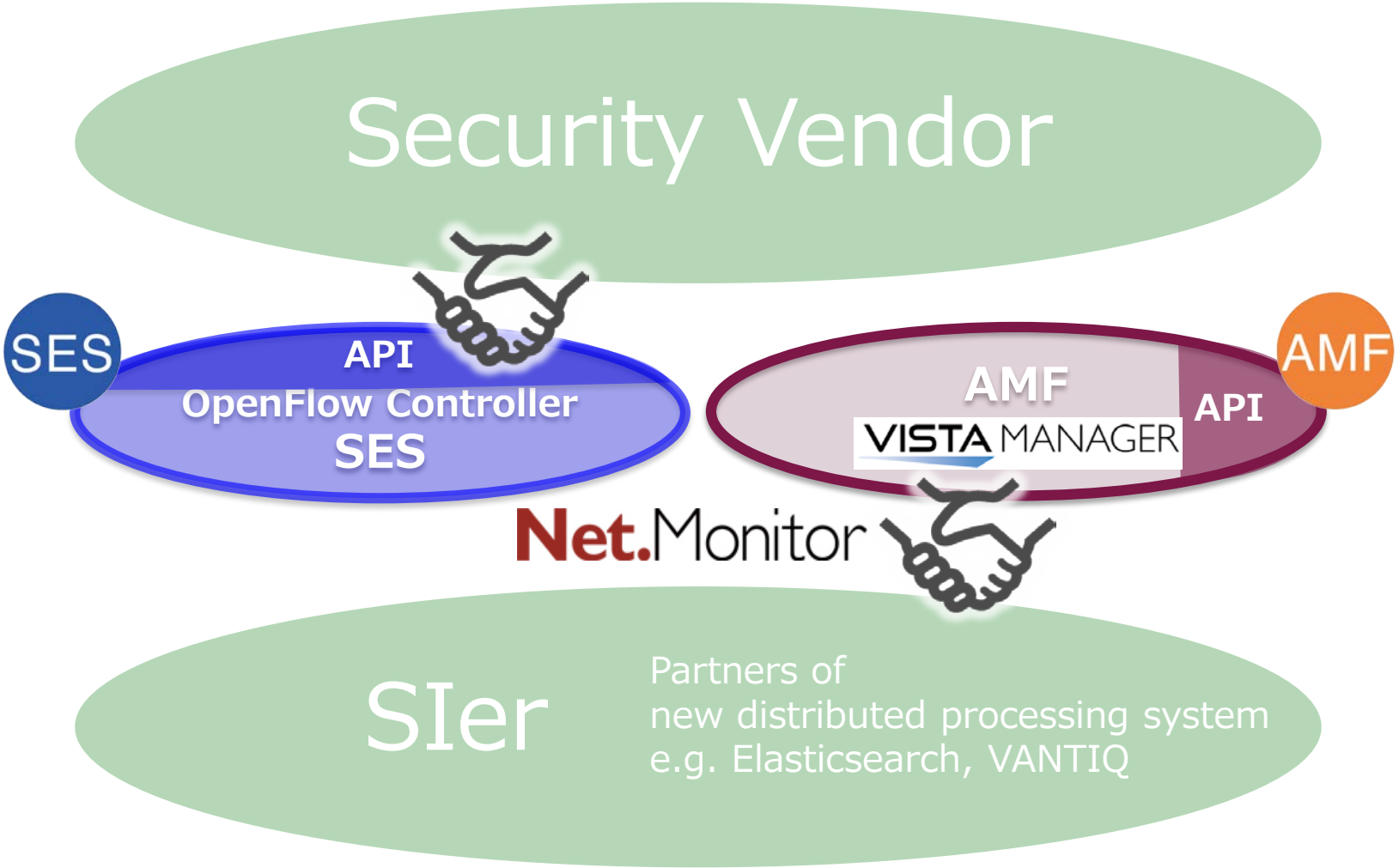
※これからは、IoTデバイスも含めたCSIRTマニュアル作りが必要

※総務省サイバーセキュリティタスクフォースが「IoTセキュリティ総合対策（H.29/10）」を公表

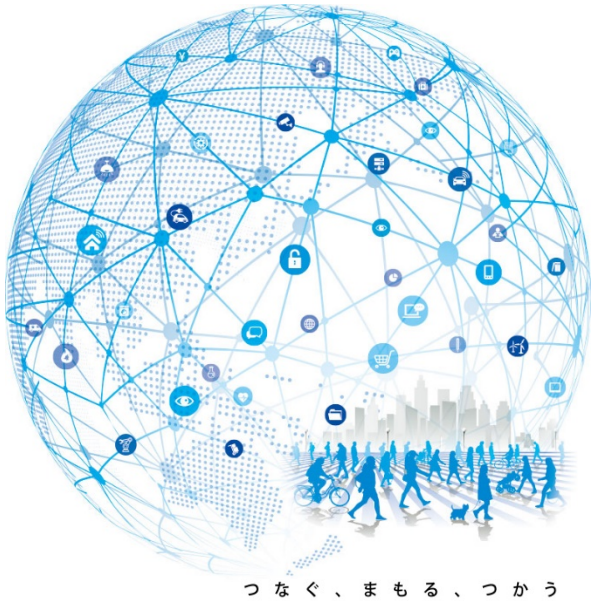


6. Exchangeカンファレンスについて

“超”分散処理時代を迎え、ネットワーク技術およびサービス連携（エコシステム）は、
セキュリティだけでなく、システム全体に広がっていくべき



ご静聴ありがとうございました



ネットワークセキュリティのパイオニア
アライドテレシス

Allied Telesis