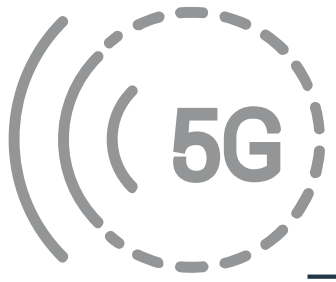
５G時代の通信インフラに関わる セキュリティリスク対策

A10ネットワークス株式会社

Reliable Security Always™

5Gの用途



低遅延 (>1ms)

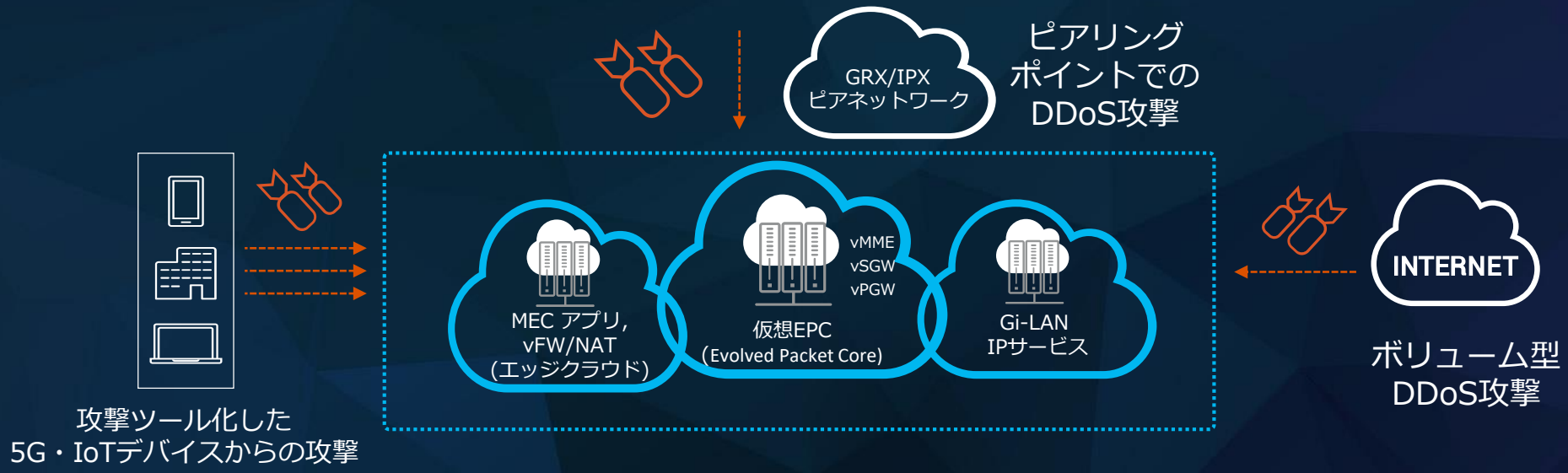
高密度(100x)

高帯域(20Gbps)

通信クライアントの主役は
人からモノへ

交通	産業	モビリティ	サービス
交通制御 自動運転 公共交通システム	スマート農業 スマートホーム スマートファクトリー	ウルトラハイスピード コネクティビティ イベントエクスペリエンス AR / VR	ヘルスケア 監視・モニタリング 公衆安全 緊急対応

通信インフラのセキュリティがますます重要になる



5Gによりセキュリティ脅威が増加

4X

2年間にわたる
DDoS攻撃サイズの平均*

12M

5Gインフラを攻撃できる
DDoS攻撃ツールの数*

62%

5GにおいてDDoS攻撃
防御が最も重要*

*出典: SecurityIntelligence.com, SC Magazine, IHS Markit

本日ご説明したいこと

- サービス不能攻撃（DDoS攻撃）が増加する可能性があること
- IoT機器向けのセキュリティ対策が必要になってくること
- 暗号化通信についての取り扱いについて見直しが必要

DDoSによるサイバー攻撃とは？

攻撃者	コマンド・コントロール
攻撃ツール	IoTボットネット　オープンサーバー　感染したゾンビボットネット
攻撃	
被害者	データセンタ　ネットワーク　アプリケーション　ユーザー

攻撃者が、
様々な攻撃ツールを用いて、攻撃対象のサービスを利用できなくなるようにする
サイバー攻撃

海外ではライフラインに関わるインフラに対する攻撃も発生

増大するセキュリティの脅威

4x

2年間で拡大した
平均DDoS攻撃規模

1250億

2030年までに”武器化”される
可能性があるIoTデバイス

29%

ボットネットによる
インターネット
トラフィック

1. SecurityIntelligence.com ; 2. IHS Markit ; 3. SC Magazine