閉域網のトランスポートセキュリティって必要？
IEEE802.1AE MACSecの拡張による柔軟な暗号化の実現

鹿志村康生
yasuo.Kashimura@nokia.com

自己紹介

鹿志村　康生: yasuo.kashimura@nokia.com

Nokia Solutions&Networks IP**製品事業部**

<経歴>

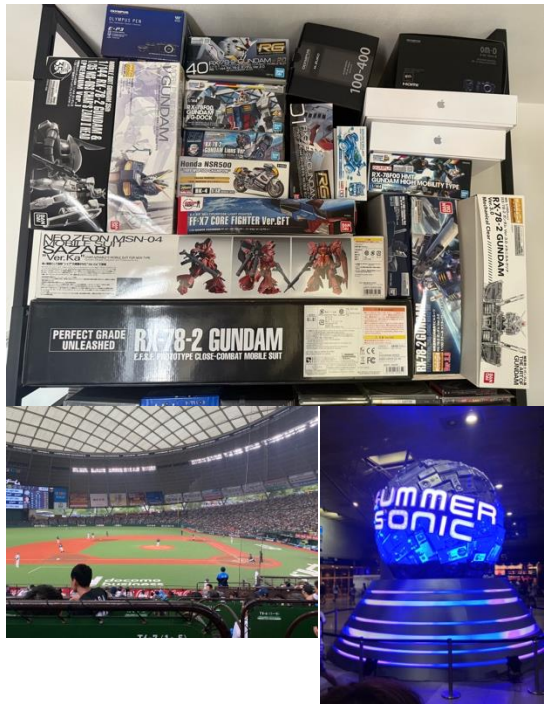
1997~2001　NTT/NTT**コムウェア**
　　社内NW**設計/構築**

2001~2008　Cisco
　　SP/Ent Presales/Consulting SE, Multicast/IPv6

2008~2017　Alcatel-Lucent

2017~　Nokia
　　日本/APAC**顧客向け**Presales/Consulting,
　　MPLS**とか**VPN**とか**SR**とか色々**
　　2010**年より日本担当**IP**製品責任者**

<趣味>
積みプラ、音楽、野球/ライブ/フェス観戦、飛行機、写真



閉域網って安全？
閉域網のセキュリティってどう考えてますか？

ネットワーク上を流れるデータの安全性

<従来の認識>

閉域網=安全

- 通信設備は全て管理された場所にある
- 多くのアプリケーションは暗号化されている

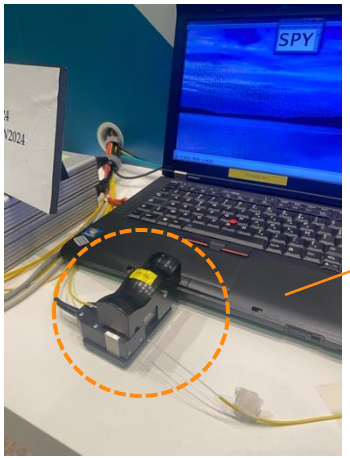
=>データ盗聴の心配はない

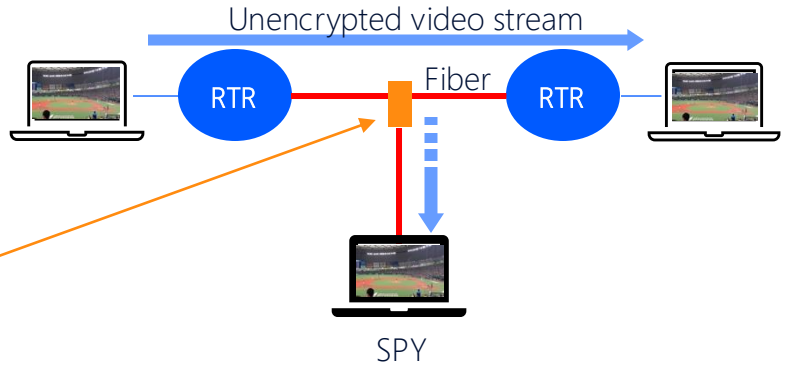
- このままの認識で良いと思われますか？
- 閉域網=安全=NWとしての暗号化は不要？
- トランスポートレイヤでの暗号化の必要性やユーザ要求ってありますか？

光ファイバーからのデータ傍受

やろうと思えば割と簡単に出来ちゃう

JANOG48 LT **光ファイバからの盗聴**(PacketLight **山口さん**)
https://www.janog.gr.jp/meeting/janog48/wp-content/uploads/2021/07/janog48-lt2-yamaguchi.pdf





量子コンピューターのNWへの脅威
量子コンピューターの実用化、近くなるQ-Day

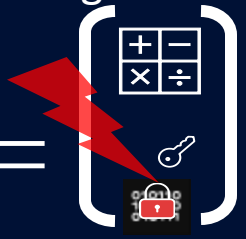
- IBM: Heron R2 156 qubits, two-level system mitigation to help reduce the impact of an important source of noise <2024/11>
(https://www.ibm.com/quantum/blog/qdc-2024)

- Google: Willow **大幅なError率の低減、現在のスパコンで10^{25}年かかる計算を5分で出来る可能性** <2024/12>
(https://blog.google/technology/research/google-willow-quantum-chip/)

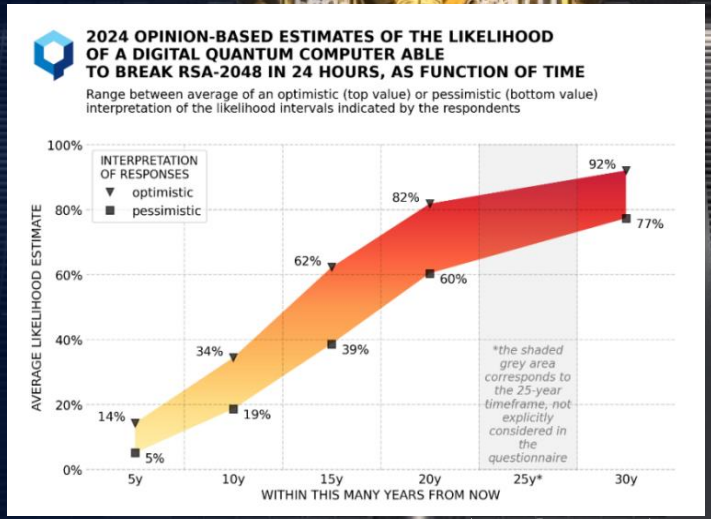
- NTT: **室温動作可能な量子コンピューター、汎用型光量子計算プラットフォームの開発**105Heron R2 156 qubits, two-level system mitigation to help reduce the impact of an important source of noise
(https://group.ntt/jp/magazine/blog/quantum_01/
https://group.ntt/jp/newsrelease/2024/11/08/241108a.html)

Quantum paradigm

量子コンピューターの暗号への利用、shorのアルゴリズム



現在の非対称暗号化

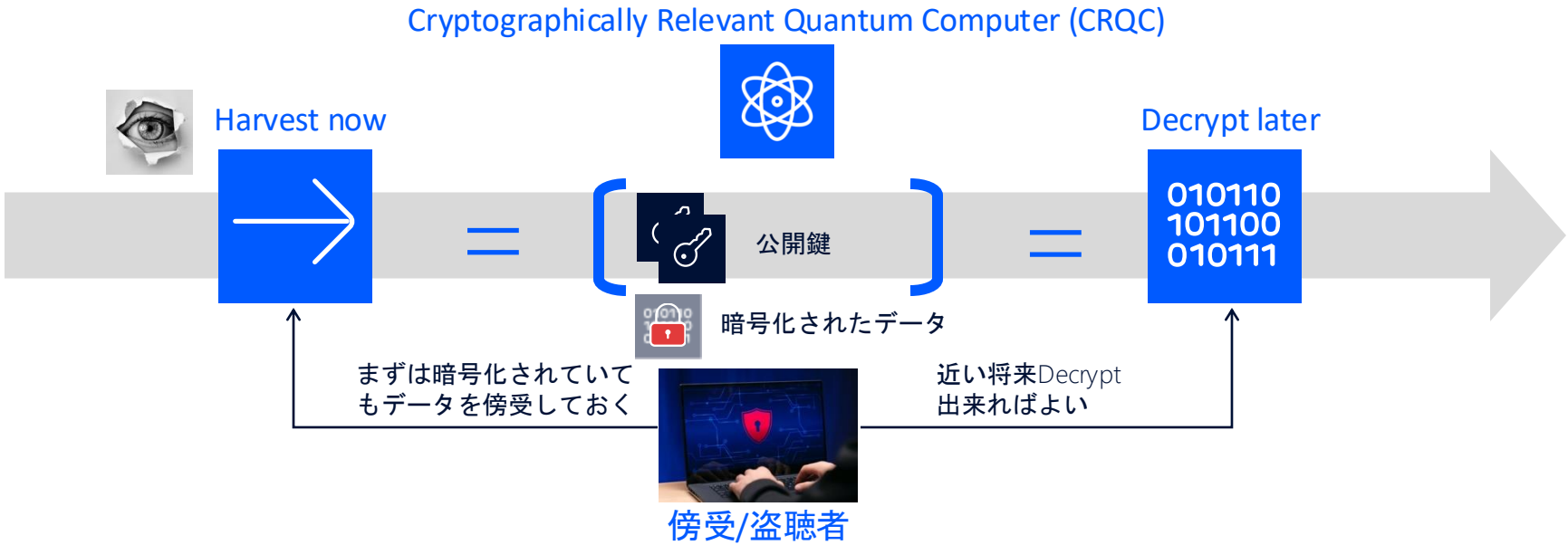


14-62%の確率で今後5-15年の間に量子コンピューターが24時間以内にRSA-2048をBreak出来るようになると予想

(https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/)

Harvest Now, Decrypt Later

量子コンピューターの脅威には今から備えておくべきという考え方



情報の有効性が長期に渡るもの(国家機密、医療/金融データ、個人情報等)は
“Decrypt Later”でも情報の重要性が失われない

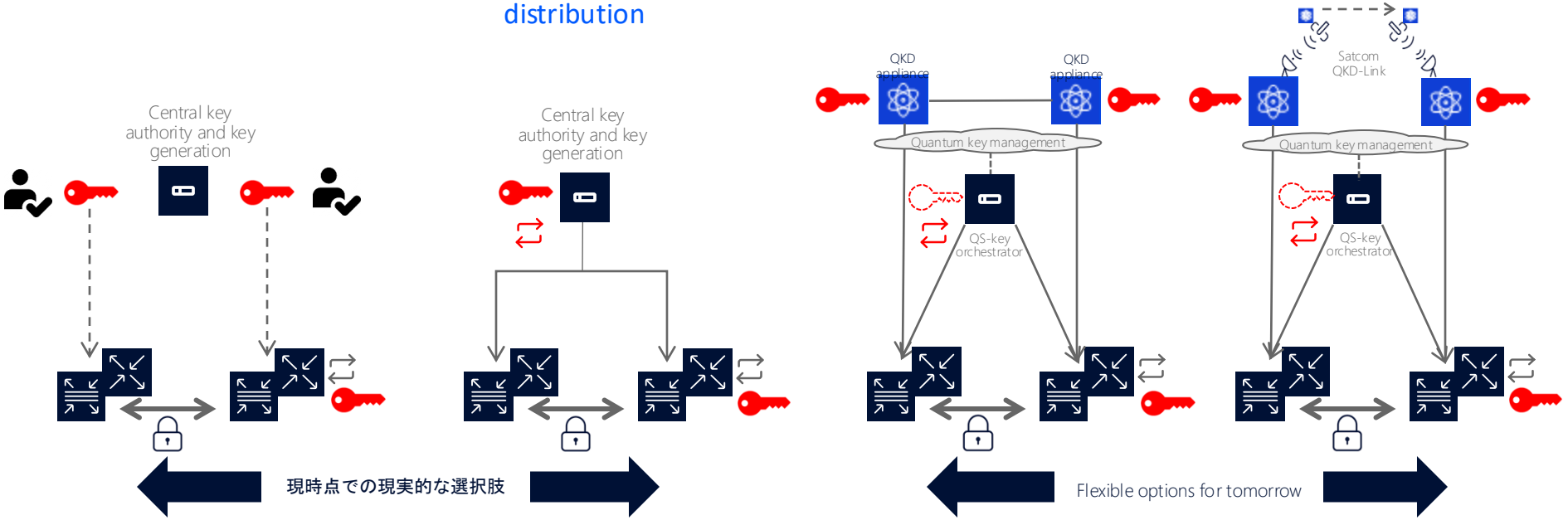
(参考)Post-Quantum対応のための重要な部分：QKD

Quantum Key Distribution

Pre-Shared Keyの
Manual distribution

Pre-Shared Keyの
Automated symmetric
distribution

Pre-SharedのQKDアプライアンスによる
QKD distribution



各レイヤにおける暗号化

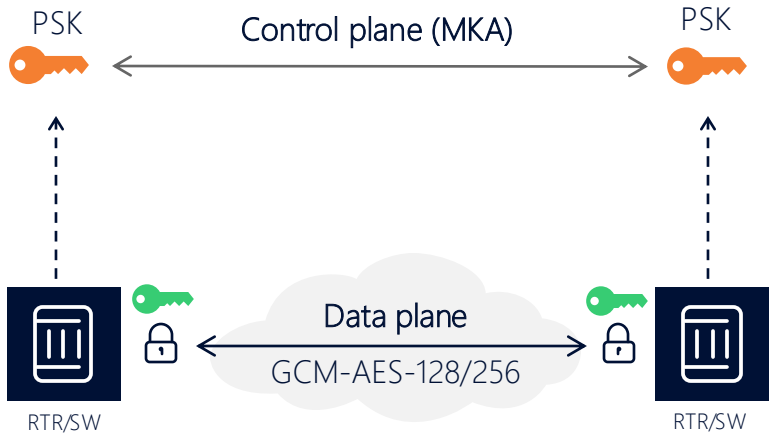
Layer3	IPsec	**セッションセットアップが複雑、相互接続性** **機器によってはThroughputに制限** Post-Quantum**対応は**RFC 8784, draft-hu-ipsecme-pqt-hybrid-auth**等進行中**
Layer2	MACsec	**多くの機器でサポート** **ラインレートでの暗号化** **比較的シンプル** Post-Quantum**対応可能**
Layer1	OTNsec	**伝送機器での**L1 Encryption **多くの伝送機器がサポート** Post-Quantum**対応可能**

トランスポートNWでの暗号化技術: MACsec

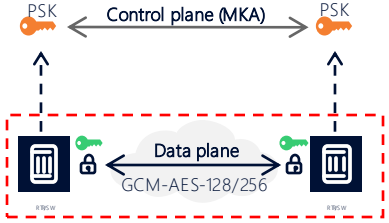
MACsec概要(1)

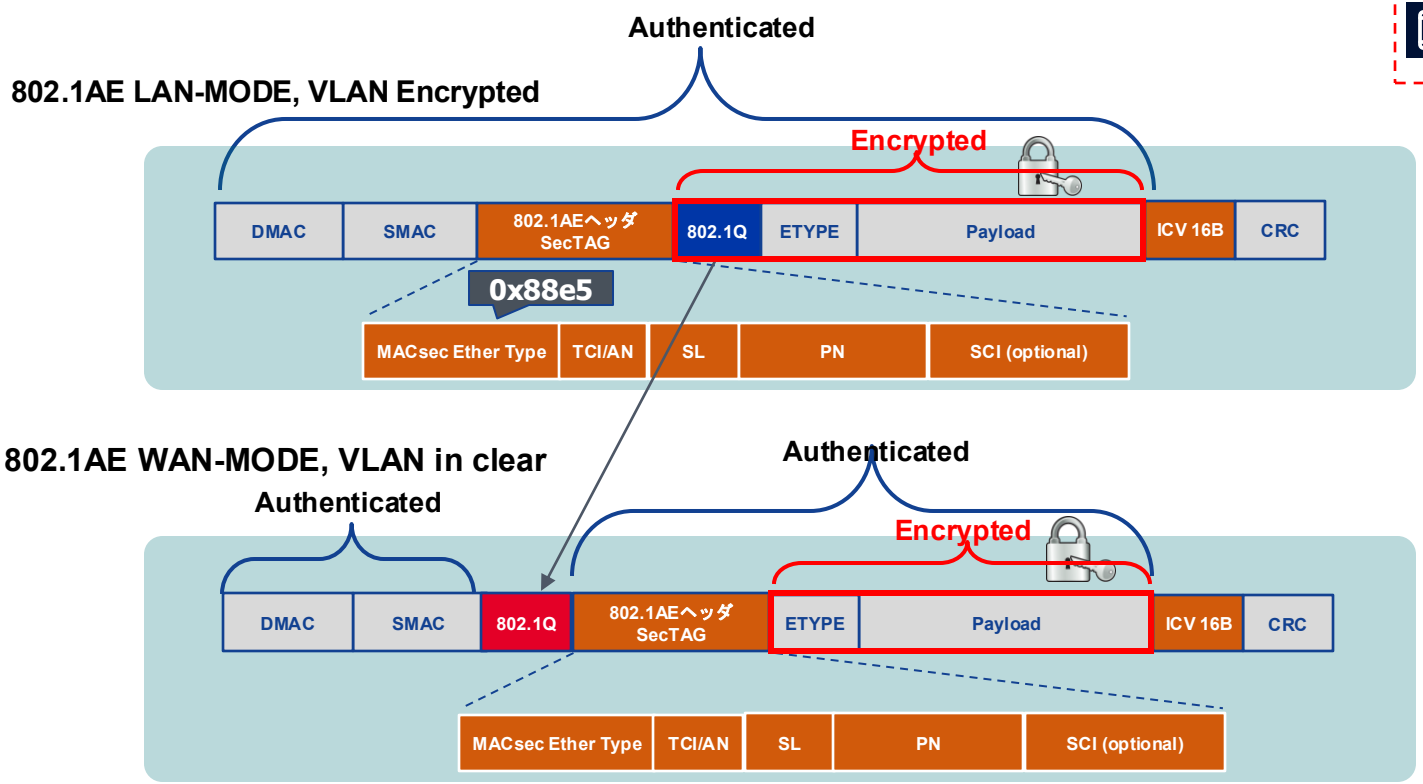
Ethernetレイヤでの暗号化

- IEEE 802.1AEで規定
- MACレイヤーでのEncryption
- IPsecよりもシンプルなセットアップ
- MKA(MACsec Key Agreement)による鍵交換/管理
- AES128/256でのデータプレーン暗号化
- 比較的安価なSwitch含む多くのEthernet機器(Router/Switch)でHWサポート
  - BRCM MACsec PHY
  - BRCM Jericho2c+/3
  - Nokia FP5 chipset(E5)
  - Cisco Silicon One



MACsec概要(2)
データプレーンパケットフォーマット





TCI: TAG Control Information

AN: Association Number

SL: Short Length

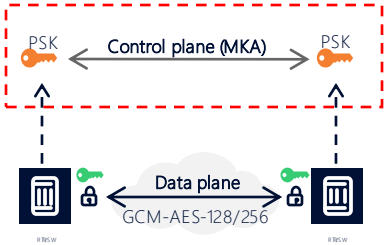
PN: Packet Number

SCI: Secure Channel Identifier

ICV: Integrity Check Value

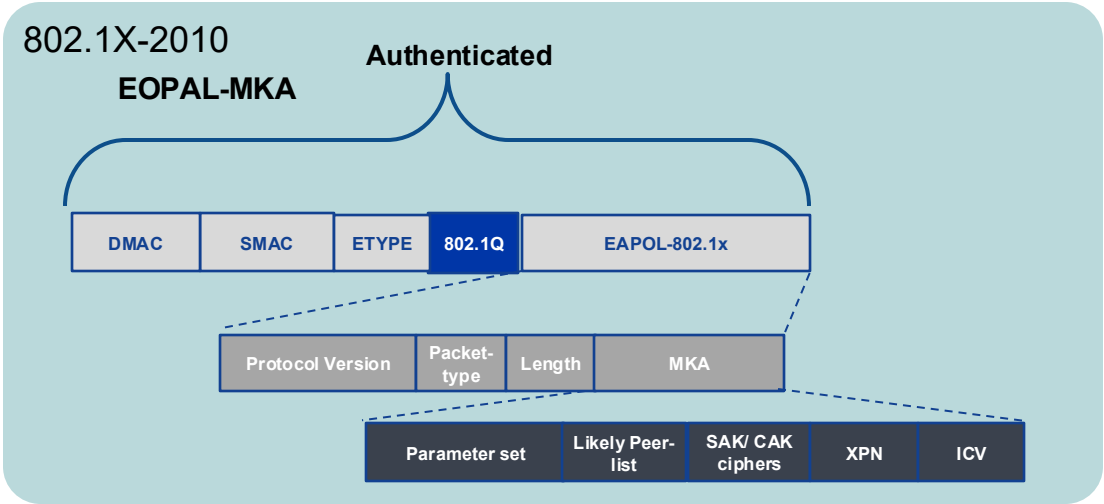
MACsec概要(3)

MKA(MACsec Key Agreement)/コントロールプレーン



MKA (MACsec Key Agreement)

- 802.1xフレームワークを使用、データプレーン暗号化で使用するSKA(Secure Association Key)を交換/管理
- DMACは01:80:c2:00:00:03のMulticast MACをDestinationとする(LLDPと同じ)
- CAK(Connectivity Association Key)を共有しSAKを生成
- MACsecのセキュアチャネルが確率しないとL2プロトコルは動作しない
- 対抗のMACsecデバイス(ピア)を識別しCA(Connectivity Association)を形成
- PNによるリプレイ攻撃防御
- ICV (integrity check value)での整合性検証



MACsec概要(4)

MACsecでのネットワーク構成

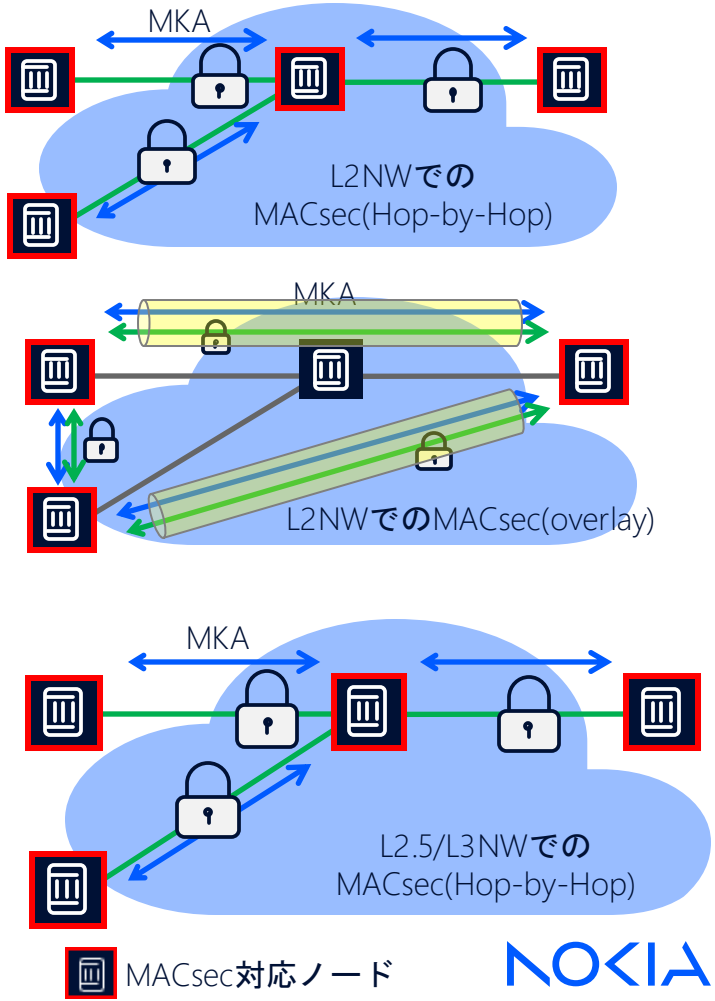
L2ネットワーク(pure-Eth/over L2svc)

- 802.1xパケットのtunneling、WAN-modeの使用等でoverlay L2でのEnd-to-End L2暗号化が可能
- Per-port/Un-tag/vlanでの暗号化
- Point-to-PointまたはAny-to-Anyの接続性

L2.5/L3ネットワーク(IP/MPLS/SR)

- Hop-by-Hopでの暗号化
- 上位IP/MPLS/SRレイヤはシームレス
- 各HopでL2.5/L3トラフィックのDrop/Add可能

L2 onlyだとけっこうめんどい？
適用箇所限られる？



MACsecについて

標準方式としては割と昔(2006年)からある方式
既に多くの機器がMACsecに対応
＝＞

- 皆さんMACsec使われてますか？
- 使い勝手はどうですか？

MACsecを活用した新たな方式
ANYsec(標準化活動はこれから)

ANYsec概要

MACsec方式の活用による柔軟な暗号化

IEEE 802.1AE
MACsec**標準的な暗号化**

WAN-MODE MACsec**暗号化**
(VLAN tag**は**Clear)

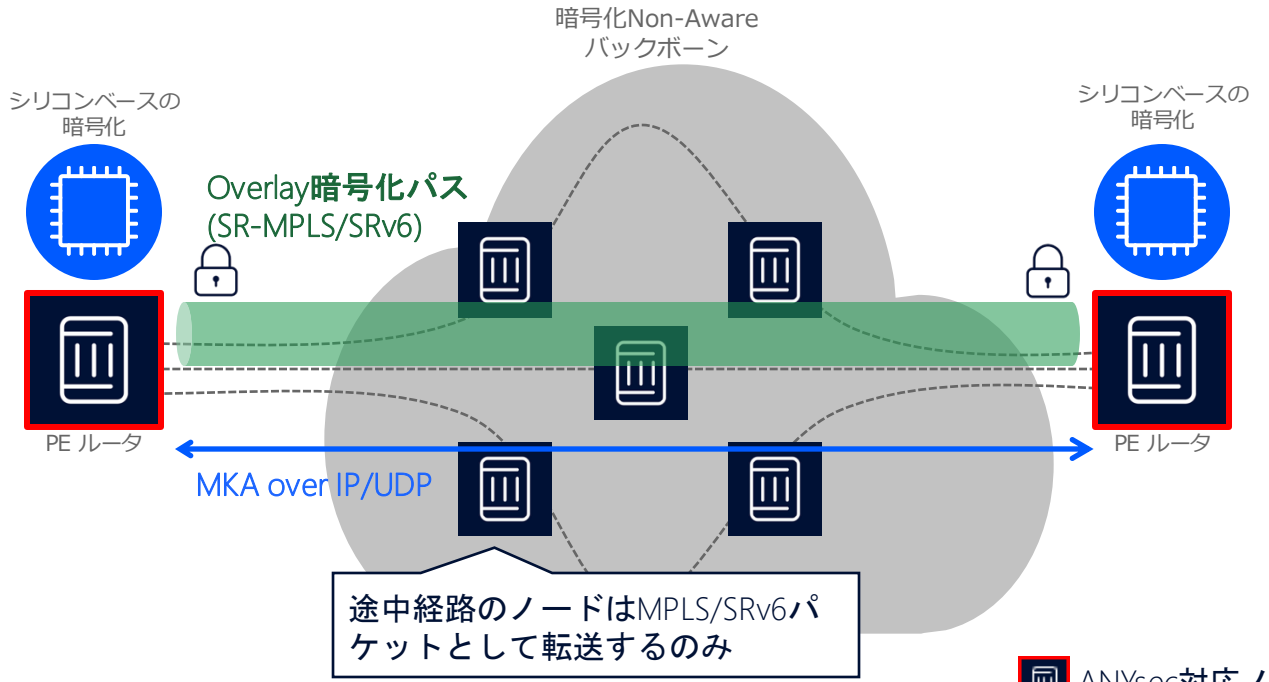
ANYSsec at L2.5(MPLS/SR-MPLS)
- MPLS/SR-MPLS path**の暗号化**
- MPLS label**は**Clear

ANYSsec at SRv6
- SRv6 path**の暗号化**
- SRv6 hdr/sgmt**は**Clear

ANYsec at L3
- IP Flow**の暗号化**
- IP heade**は**Clear

ANYsecによるOverlay暗号化パス

柔軟に大容量暗号化パスを構築可能

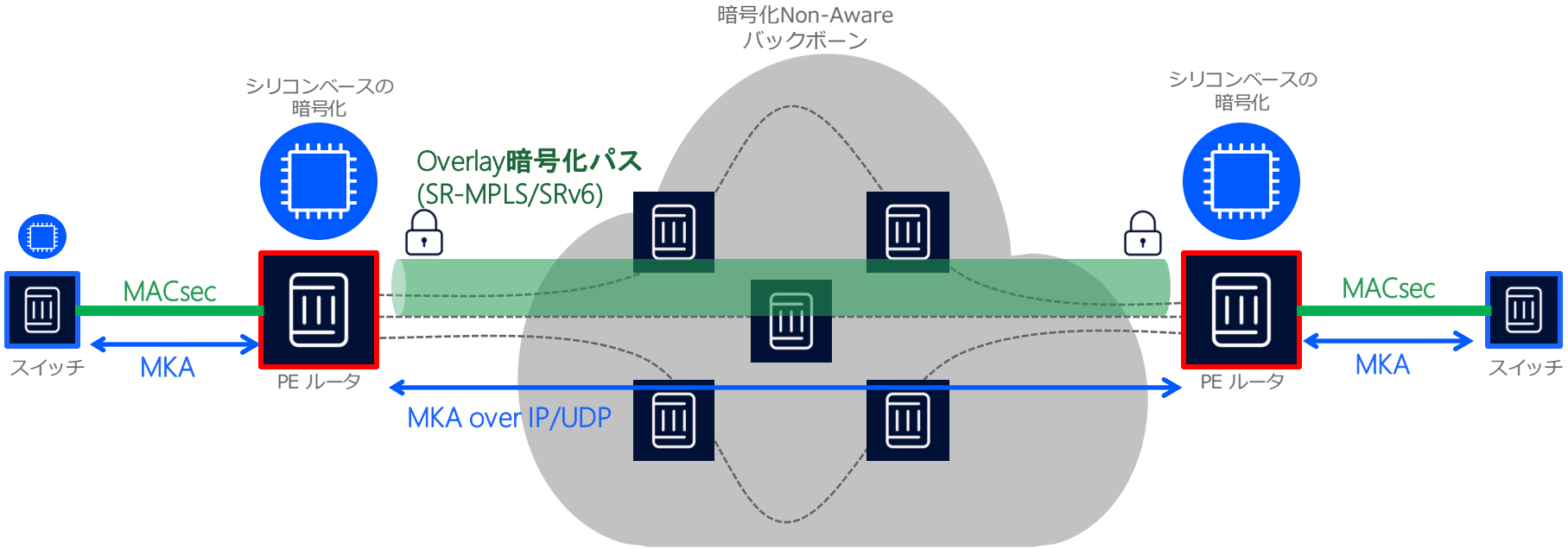


- 標準方式を活用
- HW処理による大容量低遅延暗号化処理
- Underlay方式に合わせた柔軟な暗号化レイヤの指定が可能
- 暗号化Overlay tunnel/path
- 暗号化スライスのような新たなサービスの可能性

ANYsec対応ノード

ANYsecによるOverlay暗号化パス

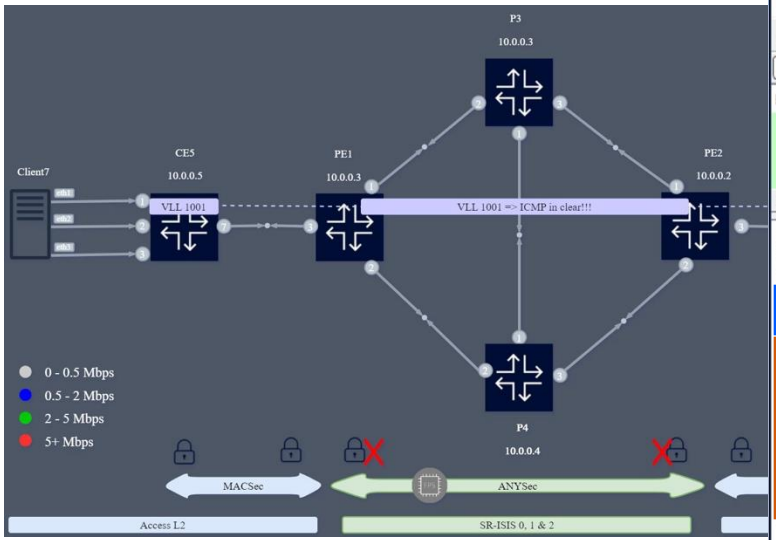
エッジでのMACsecとの組み合わせによるEnd-to-End暗号化

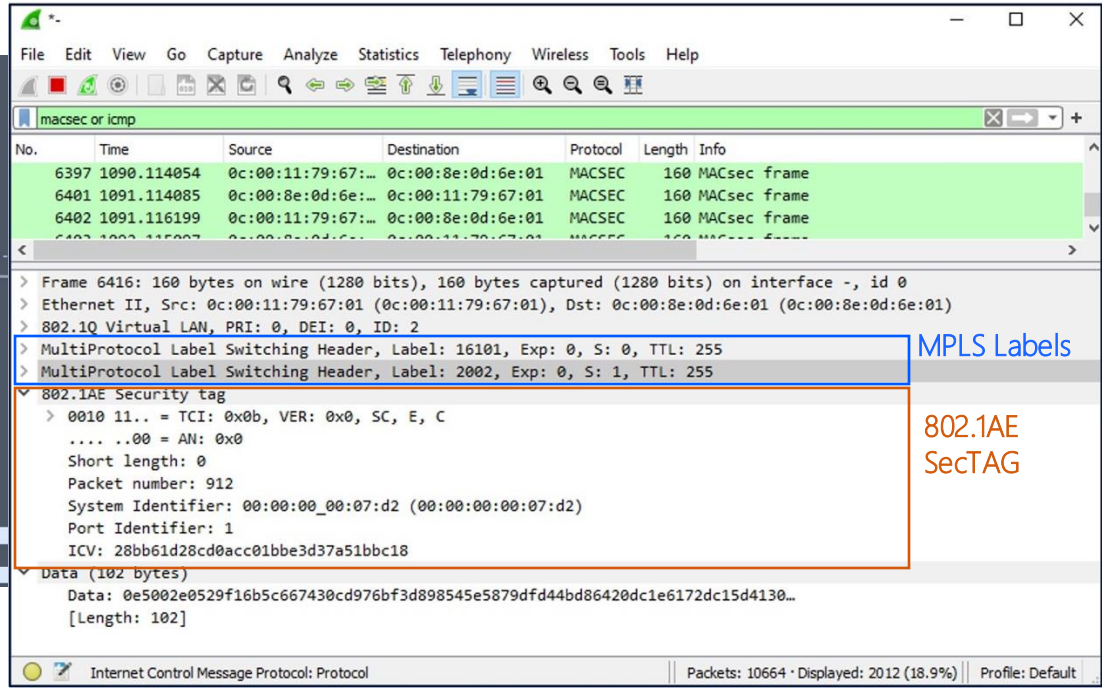


ANYsec実装例

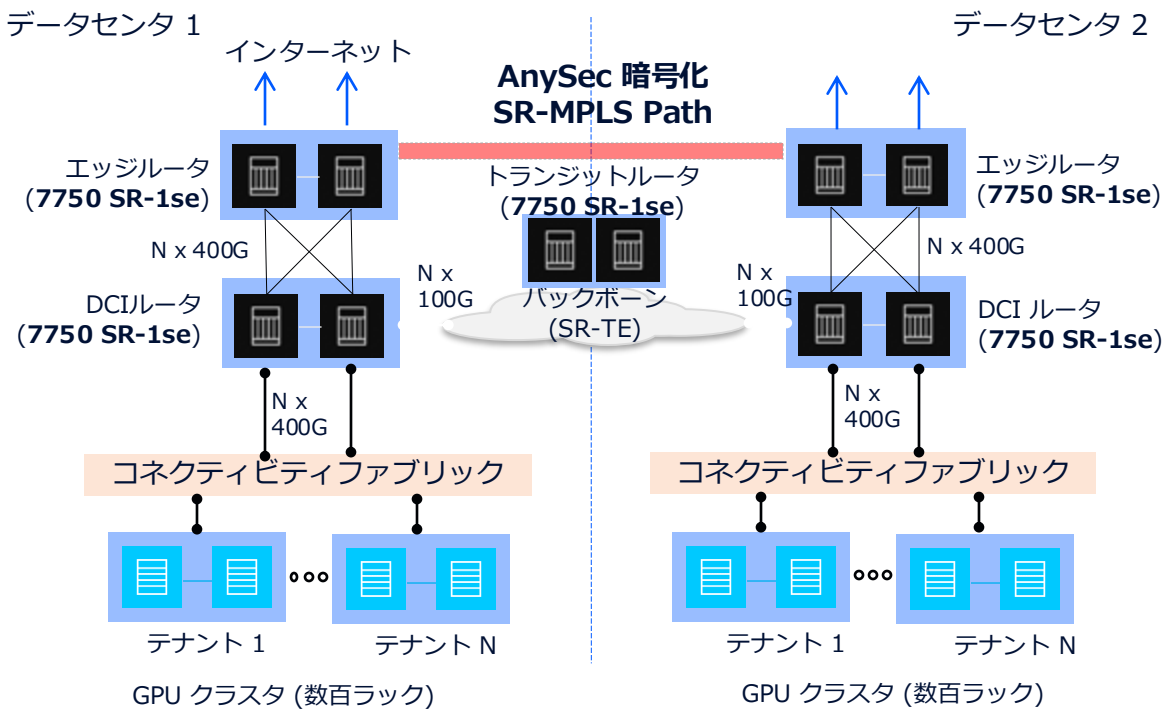
Over SR-MPLS　Container Lab上のデモ

https://github.com/srl-labs/sros-anysec-macsec-lab





ANYsec導入事例: US AI Cloud (GPUaaS) – DC 間接続



サービス内容

- **GPUaaS、ストレージなど**
- **初期導入は 400G、将来的に800G**
- **セキュアで暗号化通信が可能なデータセンタ相互接続サービス**

DC 相互接続ルータ要件

- DC 相互接続ルータは以下のサポートが必要:
  - VXLAN, e/iBGP, BGP-EVPN, BGP RR
  - MPLS, セグメントルーティング, QoS, NETCONF/YANG
- バックボーン経由の e2e 暗号化用の ANYSEC
- スケール: 大規模 VXLAN トンネル
- SDN コントローラ (NSP/NRC) – SR 監視、パス制御など

議論

<トランスポートセキュリティについて>

- ◆閉域網のセキュリティってどう考えますか？
  閉域網=安全=NWとしての暗号化は不要？
- ◆トランスポートレイヤでの暗号化の必要性やユーザ要求
  ってありますか？

<MACsecについて>

- ◆ 皆さんMACsec使われてますか？
- ◆ 使い勝手はどうですか？

<耐量子暗号化について>

- ◆ どのぐらい気にされてますか？


NOKIA