

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

NOKIA

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

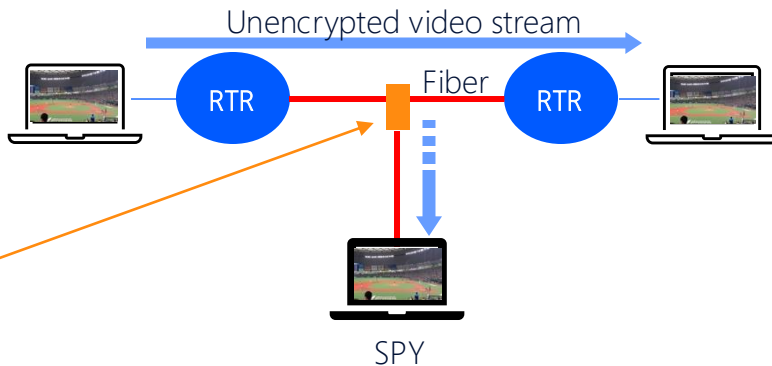
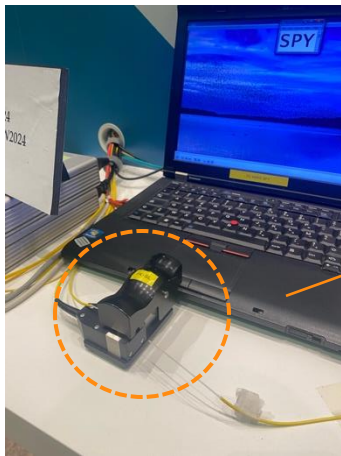
- ◆ このままの認識で良いと思われませんか？
- ◆ 閉域網=安全=NWとしての暗号化は不要？
- ◆ トランスポートレイヤでの暗号化の必要性やユーザ要求ってありますか？

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

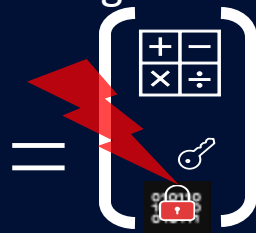
- IBM: Heron R2 156 qubits, two-level system mitigation to help reduce the impact of an important source of noise <2024/11>
(<https://www.ibm.com/quantum/blog/qdc-2024>)
- Google: Willow 大幅なError率の低減、現在のスパコンで 10^{25} 年かかる計算を5分で出来る可能性 <2024/12>
(<https://blog.google/technology/research/google-willow-quantum-chip/>)
- 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>)

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

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

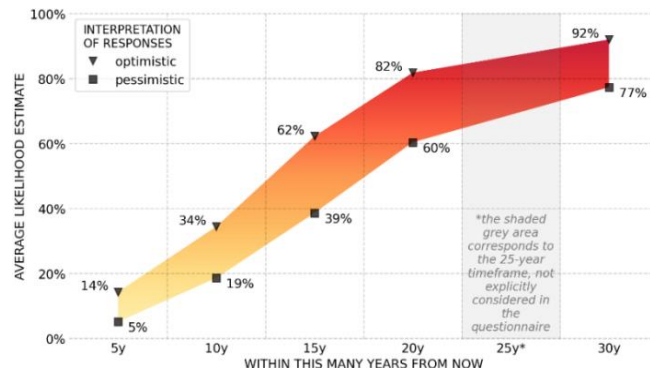


現在の非対称暗号化



2024 OPINION-BASED ESTIMATES OF THE LIKELIHOOD OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIME

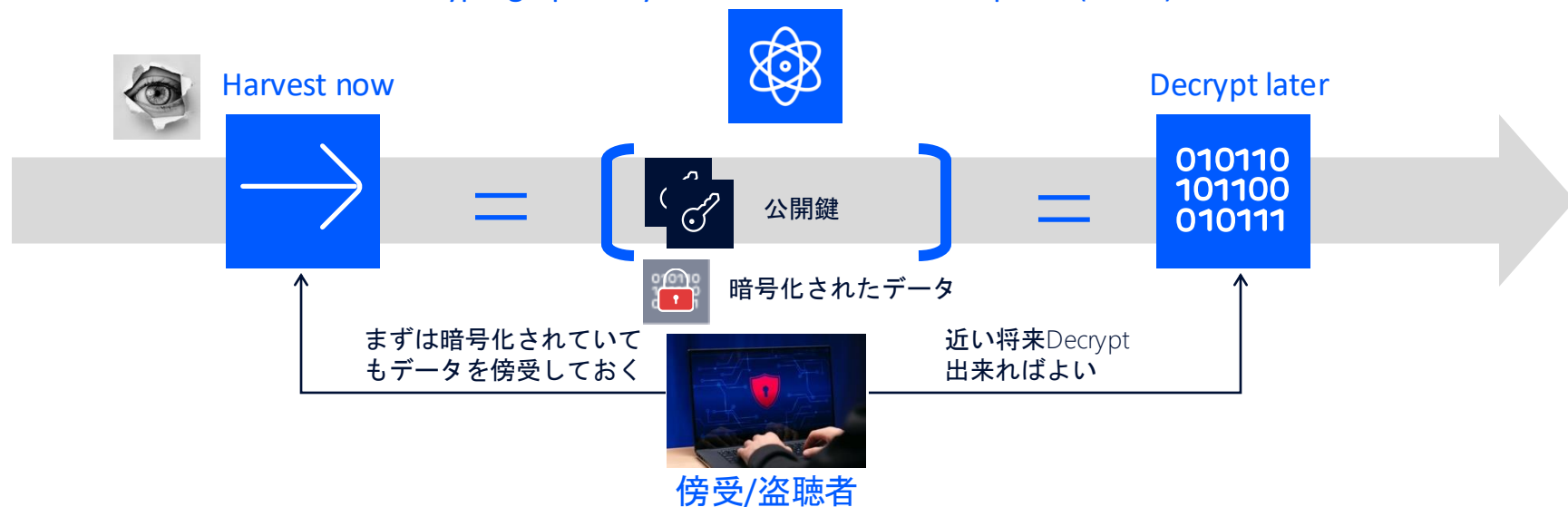
Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents



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

Cryptographically Relevant Quantum Computer (CRQC)



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

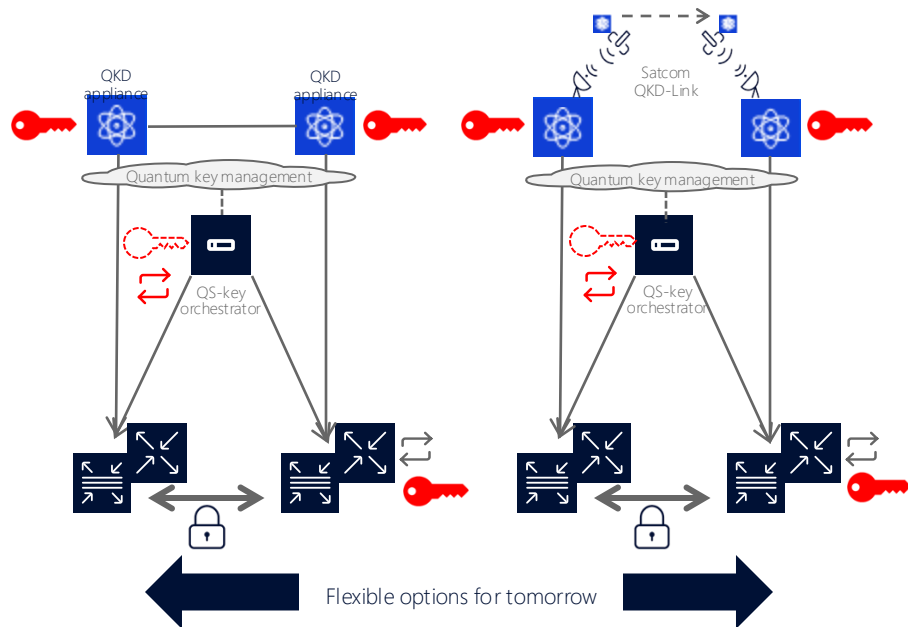
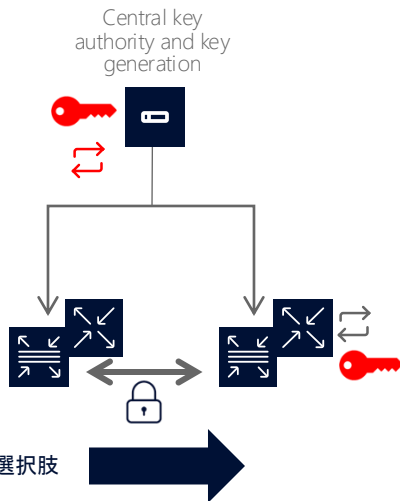
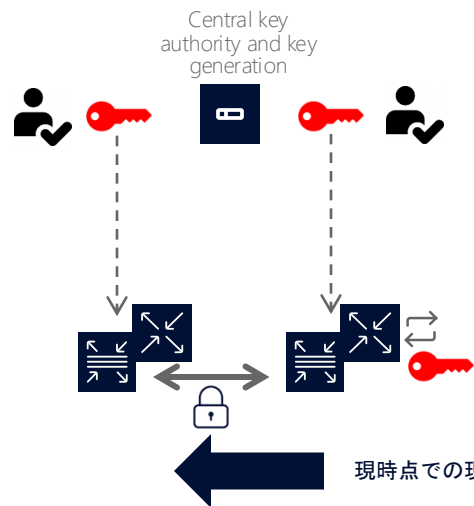
(参考)Post-Quantum対応のための重要な部分：QKD

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

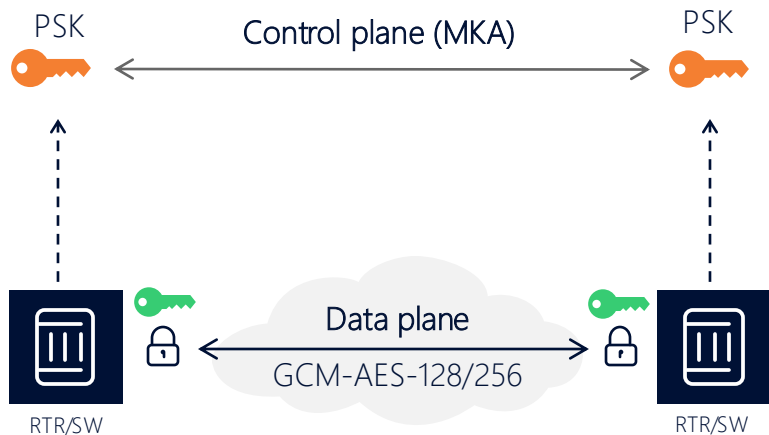
Layer3	IPsec	セッションセットアップが複雑、相互接続性 機器によってはThroughputに制限 Post-Quantum対応はRFC 8784, draft-hu-ipsecme-pqt-hybrid-auth等進行中
Layer2	MACsec	多くの機器でサポート ラインレートでの暗号化 比較的シンプル Post-Quantum対応可能
Layer1	OTNsec	伝送機器でのL1 Encryption 多くの伝送機器がサポート Post-Quantum対応可能

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

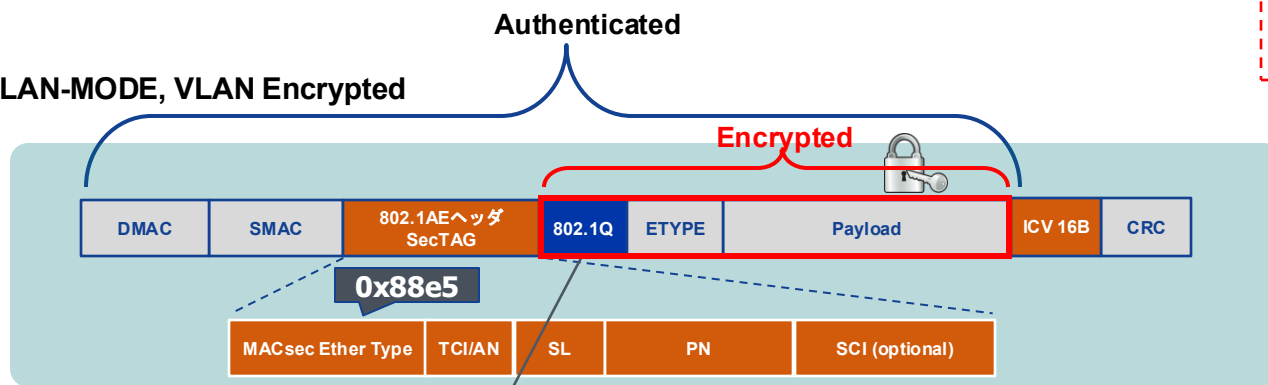
- IEEE 802.1AEで規定
- MACレイヤーでのEncryption
- IPsecよりもシンプルなセットアップ
- MKA(MACsec Key Agreement)による鍵交換/管理
- AES128/256でのデータプレーン暗号化
- 比較的安価なSwitch含む多くのEthernet機器(Router/Switch)でHWサポート
 - BRCM MACsec PHY
 - BRCM Jericho2c+/3
 - Nokia FP5 chipset(E5)
 - Cisco Silicon One



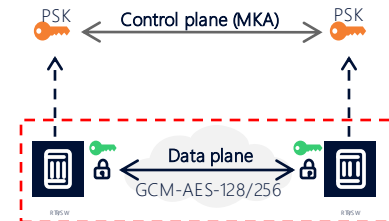
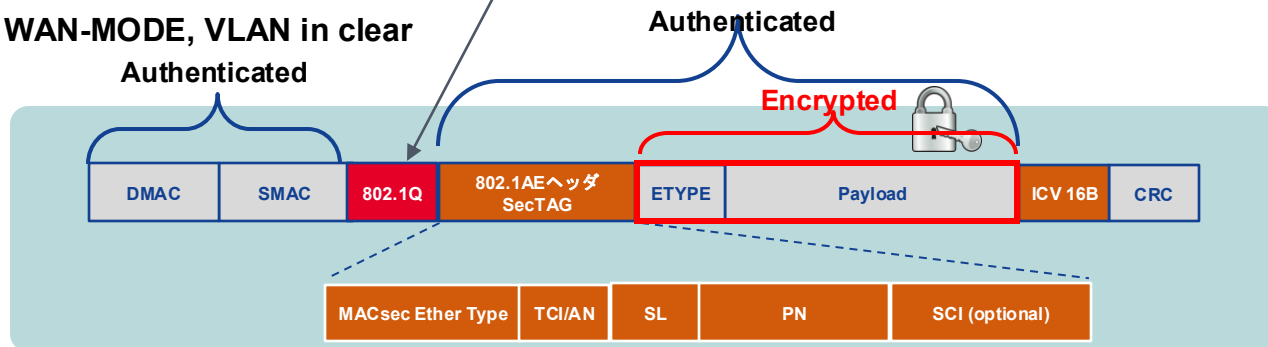
MACsec概要(2)

データプレーンパケットフォーマット

802.1AE LAN-MODE, VLAN Encrypted



802.1AE WAN-MODE, VLAN in clear



TCI: TAG Control Information

AN: Association Number

SL: Short Length

PN: Packet Number

SCI: Secure Channel Identifier

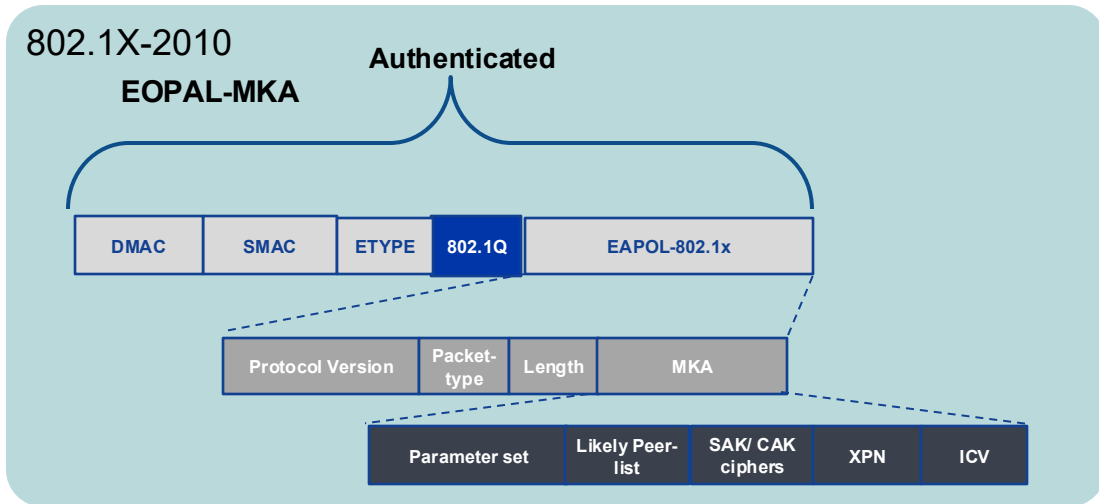
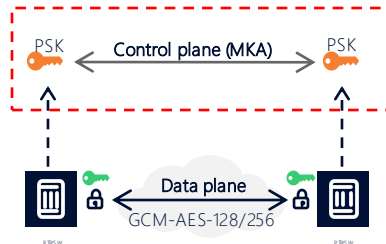
ICV: Integrity Check Value

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

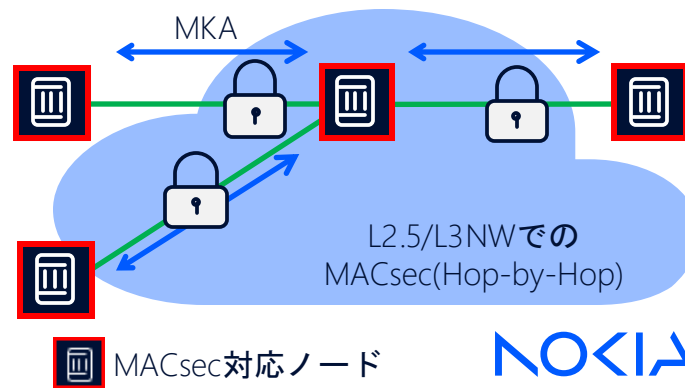
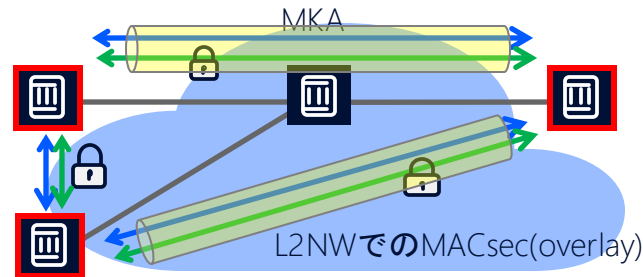
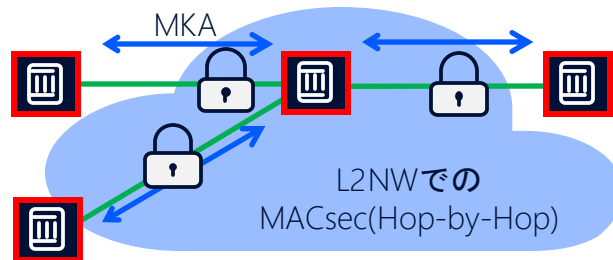
L2ネットワーク (pure-Eth/over L2svc)

- 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

=>

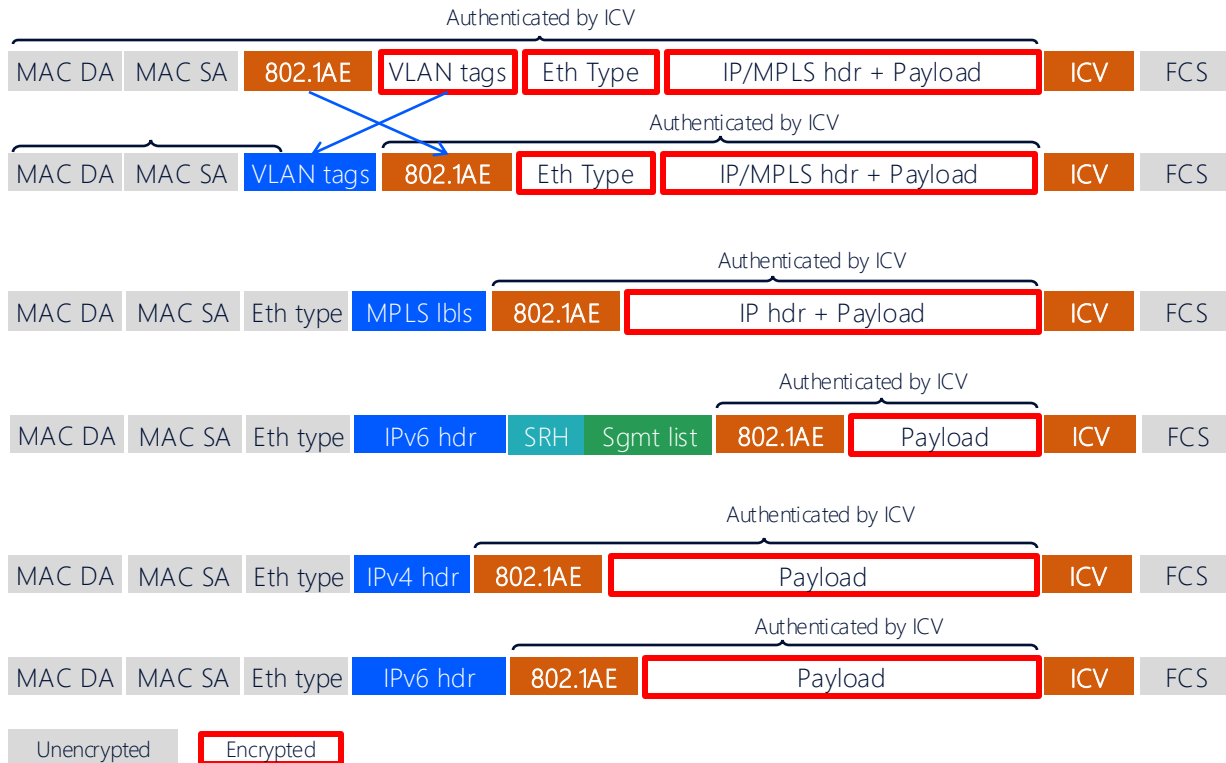
- ◆ 皆さんMACsec使われていますか？
- ◆ 使い勝手はどうですか？

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を活用した様々なレイヤでの暗号化



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

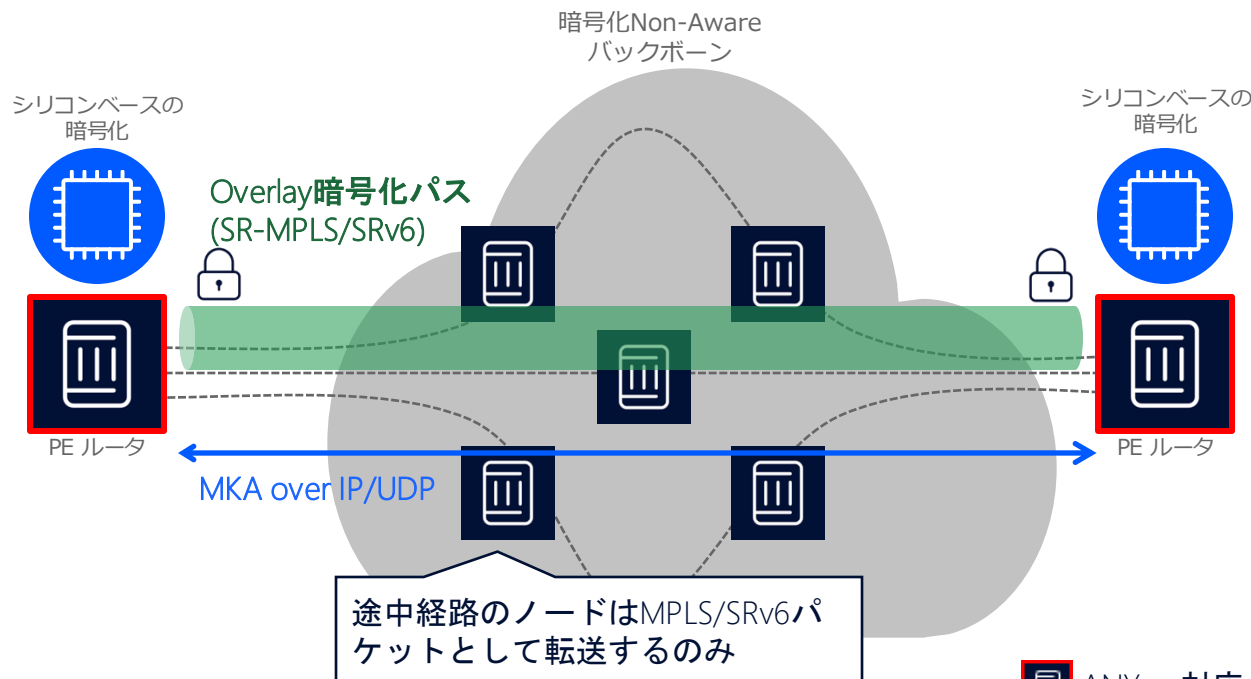
- SRv6 pathの暗号化
- SRv6 hdr/sgmtはClear

ANYsec at L3

- IP Flowの暗号化
- IP headerはClear

ANYsecによるOverlay暗号化パス

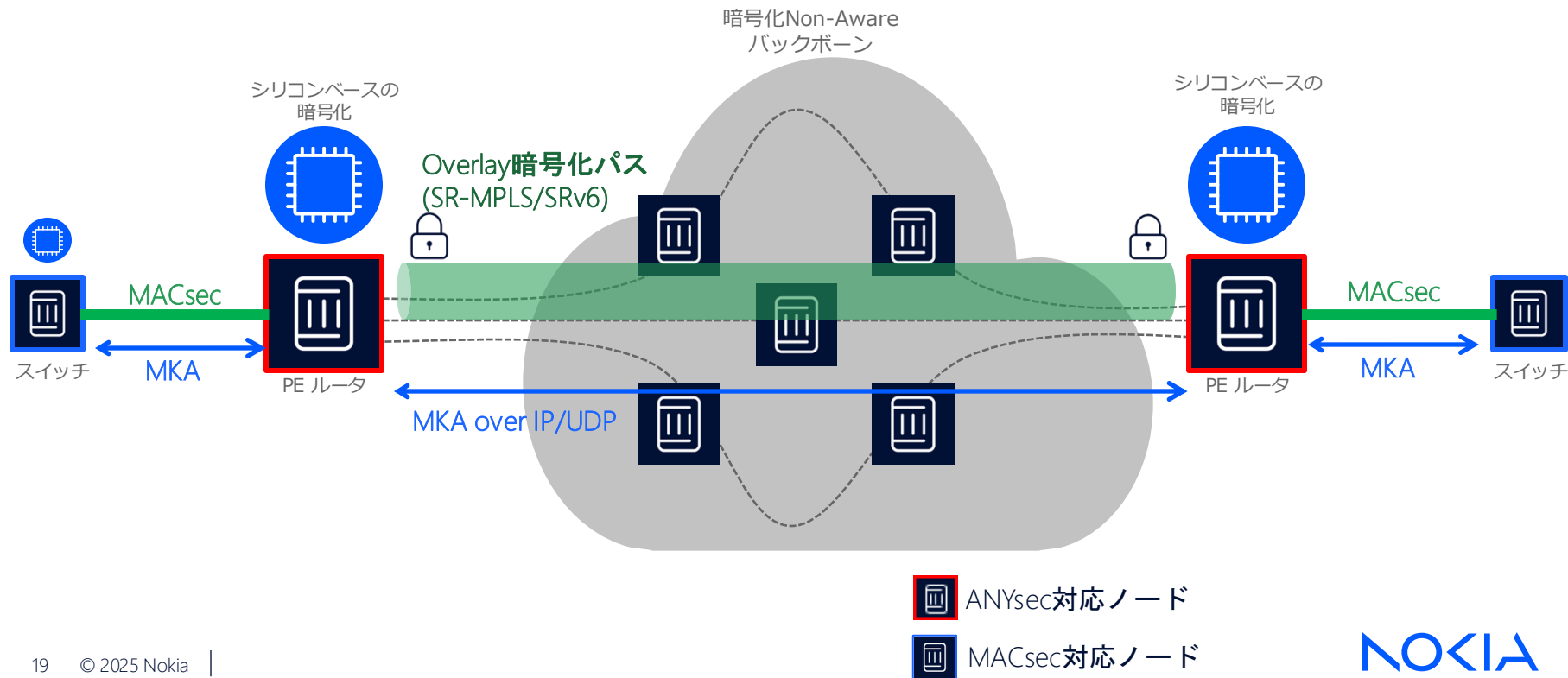
柔軟に大容量暗号化パスを構築可能



- 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

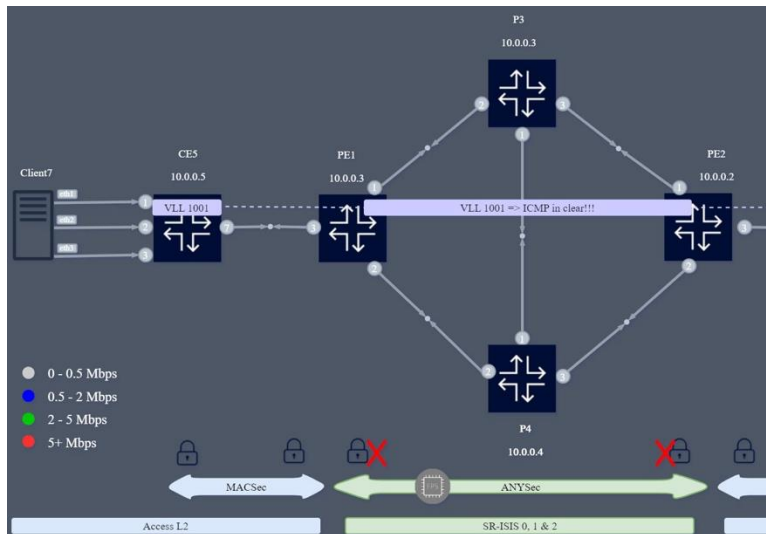
エッジでのMACsecとの組み合わせによるEnd-to-End暗号化



ANYsec実装例

Over SR-MPLS Container Lab上のデモ

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

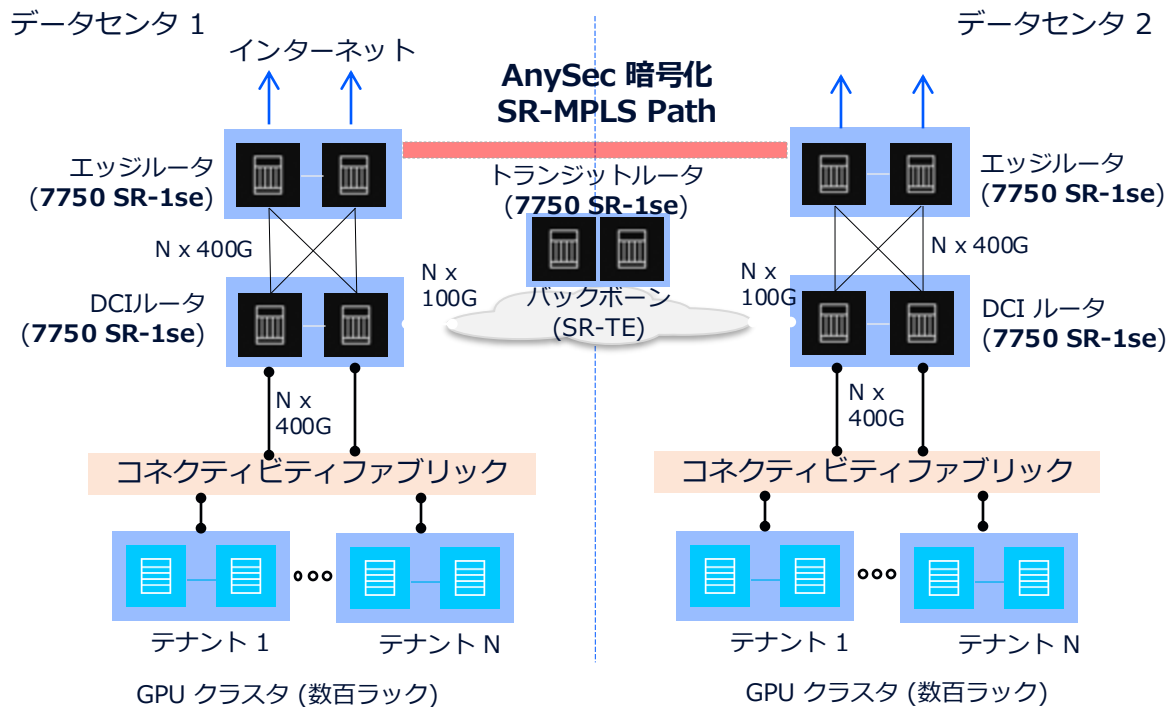


Wireshark packet capture window showing MACsec frames. The packet list shows three MACsec frames. The packet details pane shows the structure of a MACsec frame, including the MultiProtocol Label Switching Header and the 802.1AE Security tag.

No.	Time	Source	Destination	Protocol	Length	Info
6397	1090.114054	0c:00:11:79:67:...	0c:00:8e:0d:6e:01	MACSEC	160	MACsec frame
6401	1091.114085	0c:00:8e:0d:6e:...	0c:00:11:79:67:01	MACSEC	160	MACsec frame
6402	1091.116199	0c:00:11:79:67:...	0c:00:8e:0d:6e:01	MACSEC	160	MACsec frame

Frame 6416: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface -, id 0
> Ethernet II, Src: 0c:00:11:79:67:01 (0c:00:11:79:67:01), Dst: 0c:00:8e:0d:6e:01 (0c:00:8e:0d:6e:01)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2
> MultiProtocol Label Switching Header, Label: 16101, Exp: 0, S: 0, TTL: 255
> MultiProtocol Label Switching Header, Label: 2002, Exp: 0, S: 1, TTL: 255
802.1AE Security tag
> 0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
.... ..00 = AN: 0x0
Short length: 0
Packet number: 912
System Identifier: 00:00:00_00:07:d2 (00:00:00:00:07:d2)
Port Identifier: 1
ICV: 28bb61d28cd0acc01bbe3d37a51bbc18
Data (102 bytes)
Data: 0e5002e0529f16b5c667430cd976bf3d898545e5879dfd44bd86420dc1e6172dc15d4130...
[Length: 102]

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>

◆ どのくらい気にされてますか？

NOKIA