量子暗号通信ソリューション特集

プレスリリース
東芝とPacketLight、DWDMリンクにおけるQKDとの接続を検証

ホワイトペーパー
PacketLightレイヤー1暗号化ソリューションの強化

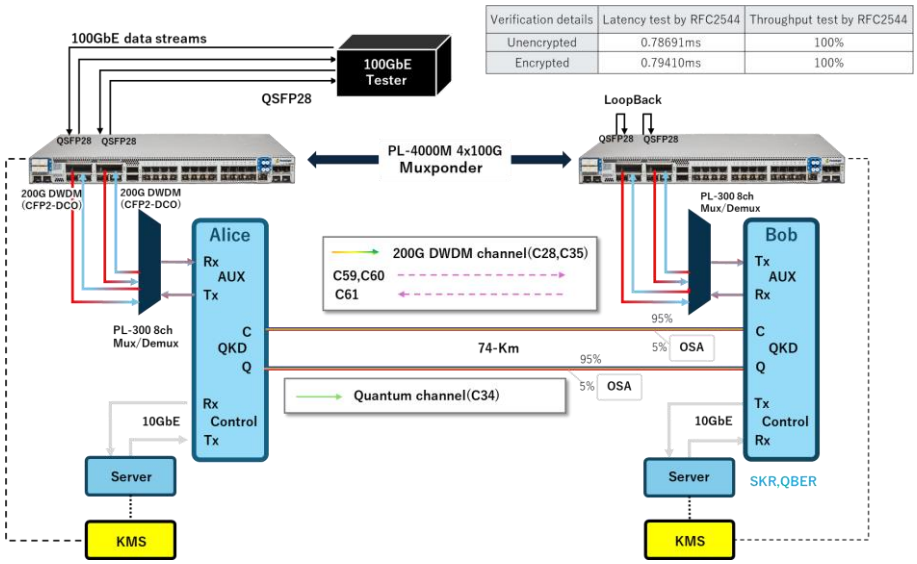
東芝とPacketLight、DWDMリンクにおけるQKDとの接続を検証

DWDMおよびOTN機器のリーディングプロバイダーであるPacketLight Networks社の国内総代理店であるアイランドシックスは、量子鍵配送（Quantum Key Distribution：QKD）技術のリーディングカンパニーである東芝デジタルソリューションズ社(以下、東芝)の協力を得て、DWDMリンク上でQKDシステムの実用化に向けた実証実験を行い成功したことを発表します。

現在のQKDシステムでは、ベンダー間の相互接続性とDWDM上での多重化が課題でした。本実証実験では、効率的でセキュアかつスケーラブルな量子セキュア通信ネットワークの構築を目的として、東芝のQKDシステムとPacketLight社のOTN暗号化伝送機能のシステムソリューション化の可能性を検証しました。2月に開催されたさっぽろ雪まつりに合わせて行われた国立研究開発法人情報通信研究機構（NICT：エヌアイシーティー）主催の雪まつり実験（注）において、札幌と沖縄の２会場でそれぞれ行いました。

東芝とアイランドシックスの合同プロジェクトチームは、従来のDWDMデータ信号とQKDを同時に伝送し、QKD暗号による量子セキュアなデータ伝送を実証する一連の詳細な評価を通じて、QKDと光ネットワークインフラとの互換性を検証し、その実用性を示しました。
さっぽろ雪まつり期間中の札幌会場では多重QKDリンクを、沖縄(北部広域ネットワーク)会場では70km超の長距離QKDリンクを実証し、2種類のQKDネットワークでの実証を行いました。

沖縄(北部広域ネットワーク)での実証実験の様子



Verification details	Latency test by RFC2544	Throughput test by RFC2544
Unencrypted	0.78691ms	100%
Encrypted	0.79410ms	100%

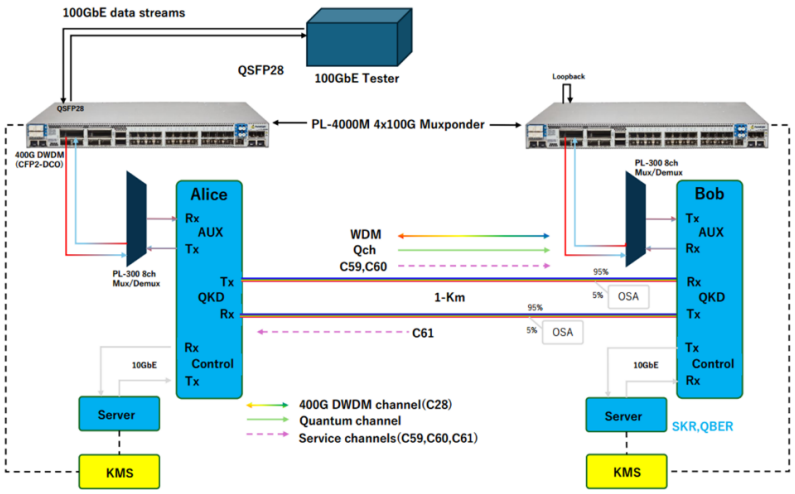
東芝QKDシステム

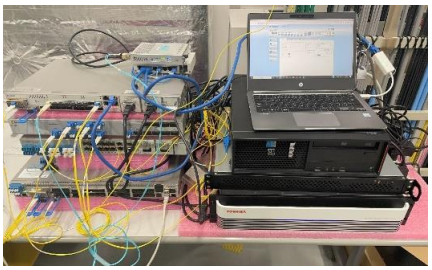
試験用映像伝送装置

沖縄(北部広域ネットワーク)での長距離QKDリンク構成図

沖縄における長距離QKDリンクは東芝の長距離QKDシステムと、PacketLightのPL-4000Mマックスポンダを使用し、量子チャネルが1550nmで動作する74kmの長距離リンク上で2つの200G波長を伝送しました。リンク性能は100Gテスターで測定され、RFC2544規格に準拠した100%のスループットと低遅延を示しました。

札幌での実証実験の様子





上図：
PacketLight PL-4000M, PL-300他
左図：
札幌での多重QKDリンク構成図

札幌における多重QKDリンクは東芝の多重QKDシステムと、PacketLightのPL-4000M マックスポンダを使用して400G波長を伝送し、量子チャネルは1310nmで多重化され動作しました。東芝の多重QKDシステムは、量子チャンネルにOバンドを使用することで、データ通信チャンネルにCバンドを利用でき、データを運ぶ光ファイバーを共有した運用ができます。 PacketLightと東芝は、QKDで保護された信号が同じ光ファイバーネットワーク上で従来のデータ伝送と同じ空間を共有できることを実証し、QKD技術が光ファイバーを別途用意することなく、現在の既存ネットワークに容易に導入できることを示しました。既存の光ファイバーネットワーク上でQKDを使用することで、QKD伝送に専用光ファイバーを使用する必要がなくなるため、大幅なコスト削減と展開速度の向上が実現します。

東芝デジタルソリューションズ株式会社
ICTソリューション事業部ＱＫＤ事業推進室 シニアフェロー
村井信哉氏のコメント

アイランドシックス様との実証実験が成功したことをうれしく思います。東芝グループでは、東芝欧州社・ケンブリッジ研究所にて、1999年に基礎研究を開始して以来、多くの世界初となる技術を実証し、量子暗号通信技術をリードしてきました。今回の実験によりPacketLight社機器と接続した環境での動作が確認されたことで、より多くのお客様が利用できるようになりました。今後も量子暗号通信の普及に向け、パートナー様と連携したソリューション提供を進めてまいります。

毎年開催される雪まつり実験は、NICT主催のもと、企業・大学・研究機関が参加し、最新の技術を検証する実験に参加する場です。研究者、技術者、学生が実践的な実施・運用を通じて技術的な知見を共有する貴重な場となっています。

（注）NICTの総合テストベッド研究開発推進センターが主催し2024年2月に行われた「超高精細映像を用いた広域映像配信実証実験」で、NICTと産学官約70組織がそれぞれ技術や人材、機材を持ち寄り、札幌・東京・大阪・沖縄などの複数拠点を結んで実施 されました。

はじめに

世界は、プライベートでも仕事でも、あらゆる場面でデジタル・コミュニケーションに依存するようになった。
今日の相互接続された世界では、個人、企業、政府を問わず、データセキュリティが最大の関心事となっています。PacketLightのレイヤー1暗号化は、光ファイバーネットワークで伝送されるデータの機密性と完全性を保証します。

このソリューションはGCM-AES-256暗号化標準に基づき、P-384曲線とSHA-384認証によるDiffie-Hellman (DH) 楕円曲線鍵交換アルゴリズムを使用しています。送信データの完全な透明性を維持しながらセキュリティを提供し、データの完全性を強化しながら配信可能性を確保します。また、このソリューションは光ファイバー盗聴を検知し、警報を発することができます。

PacketLightのレイヤー1暗号は、トランスポンダとマックスポンダに組み込まれており、OTN、イーサネット（LAN）、ファイバーチャネル（SAN）を含む様々なサービスに信頼性の高いセキュリティを提供します。

サイバー攻撃の高度化と量子コンピュータの発展により、光ファイバネットワークが危険にさらされる可能性があり、セキュリティの強化と鍵交換方法の強化が求められています。
本書では、光ファイバーによる量子暗号の世界を掘り下げ、量子鍵配送（QKD）がPacketLightのレイヤー1光暗号化ソリューションをどのように強化するかを探ります。

図 1: レイヤー1暗号化によるポイント・ツー・ポイント・ネットワーク

PacketLightとQKDの相互運用性

Diffie-Hellman鍵交換の強みは、その強固なセキュリティにあります。公開鍵がサイト間でオープンに交換されるにもかかわらず、秘密鍵を導こうとする盗聴者は離散アルゴリズム問題に直面することになり、安全でない通信チャネル上でも潜在的な攻撃者から共有秘密を安全に守ることができます。Diffie-Hellman鍵交換は非常に安全であると考えられていますが、量子コンピュータの出現により、これらの高度に洗練された量子コンピュータでも破れない方法で鍵交換を強化する必要が出てくるかもしれません。QKDはこの要求に応えます。実際の暗号化は、AES 256標準を使用し、FIPS 140-2/3およびCommon Criteria EEAL2の認証を受けたPacketLightによって行われます。

QKDとは？

QKD 量子鍵配送は、量子力学の基本原理を活用したセキュアな量子通信プロトコルで、2者間で暗号鍵を確立・配送します。QKDは、相互接続された2つのネットワーク・サイト（アリス・サイトのAとボブ・サイトのB）で同一の鍵を作成し、情報を直接交換することなく、光ファイバー上で「手がかり」を伝送することで重要な役割を果たす光子を使用して通信チャネルを確立します。QKDは、量子物理学の原理を利用して機密データの伝送を保護し、盗聴やハッキングの試みに対する耐性を保証します。このプロセスを用いて、QKDは当事者間で高度に安全で解読不可能な暗号鍵が共有されることを保証し、量子レベルの保護で通信を保護します。

統合の成功

PacketLightのDWDM/OTN装置は、DWDMネットワーク上で大容量、高信頼性、柔軟なデータ伝送を実現し、QKD技術の統合に最適です。QKDは、CバンドまたはOバンド（1310nm）で実装することができます。これらの方法をレビューし、それぞれの利点を検証します。

統合をテストするために、PacketLightの装置をポイント・ツー・ポイントのネットワーク構成にセットアップし、ネットワークの両側に装置をセットアップして、以下の機能をテストし、実証しました。

- QKDシステムとPacketLight装置間の相互運用性
- 実トラフィック条件下におけるQKDシステムの性能
- 一般的なファイバーシナリオにおける性能
- アラームと故障からの復帰

QKDの仕組みは？

QKDは、量子力学に基づいて2者間で暗号鍵を確立する、安全性の高い量子通信プロトコルです。メッセージの暗号化と復号化のために、両者だけが知っている共有の秘密鍵を生成することができます。光子が重要な役割を果たし、光ファイバー上で「手がかり」を送信することで、相互接続されたサイトで同一の暗号鍵を作成し、直接の情報交換を不要にします。このプロセスは、極めて安全で解読不可能な暗号鍵を保証し、盗聴やハッキングに対する量子レベルの保護を提供します。 QKDのユニークな特性は、暗号鍵を侵害しようとする第三者の試みを検知する能力です。量子システムを測定し、乱れを特定することで、盗聴者は不注意にも検出可能な異常を引き起こします。量子の重ね合わせやもつれを利用することで、盗聴の試みを検出する通信システムの実装が可能になります。盗聴がある閾値以下であれば、セキュア・キーが生成され、機密性が保証されます。そうでない場合、安全な鍵は生成されず、データの完全性を保護するために通信が終了します。

QKDアーキテクチャ

QKD を使用する暗号化は、特定の数学関数の計算の難しさに依存する従来の鍵交換方法とは対照的に、量子力学の基礎に依存しており、使用される一方向関数を逆にする実際の複雑さについては数学的証明を提供できません。各サイトには2種類のノードがあります。

SAEs (secured application entity) –

PacketLightが提供するデータ転送ノードで、暗号化/復号化を使用します。

KMEs (key management entity) –

QKD ノードは QKD 供給者から提供され、量子鍵の作成に責任を負います。

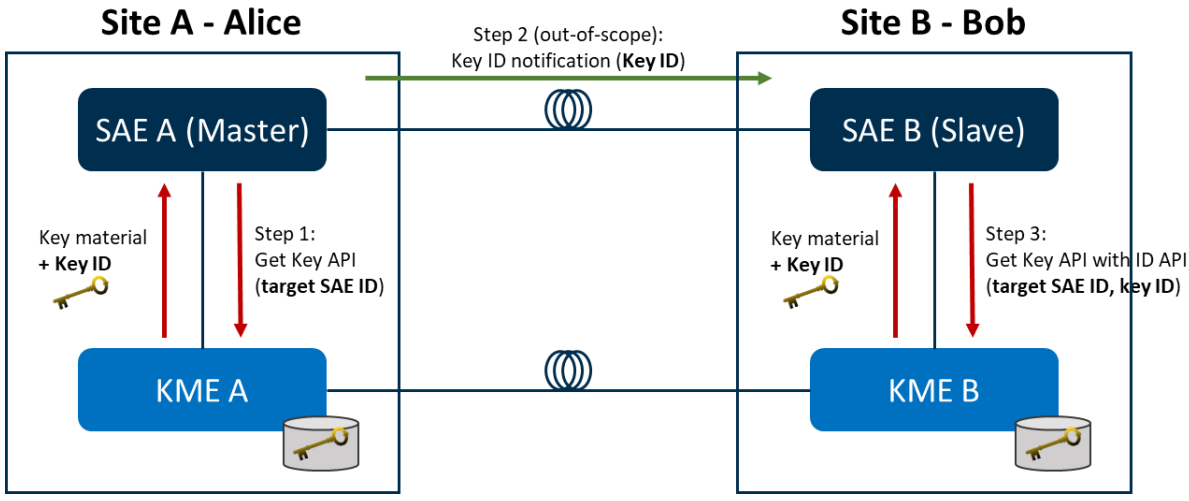


図 2: レイヤー1暗号化とQKDを使用する2つのノード

アーキテクチャの内訳

各データ転送のSAEノードは、標準的なセキュアなREST APIプロトコルを使用してローカルのKMEノードから次の量子鍵を受け取ります。2つのKMEノードはQKD スキームを使用して、量子安全ビットで構成される同一の鍵リストを双方で作成します。同じサイト内の複数のSAEが同じローカルKMEを使用することもあります。

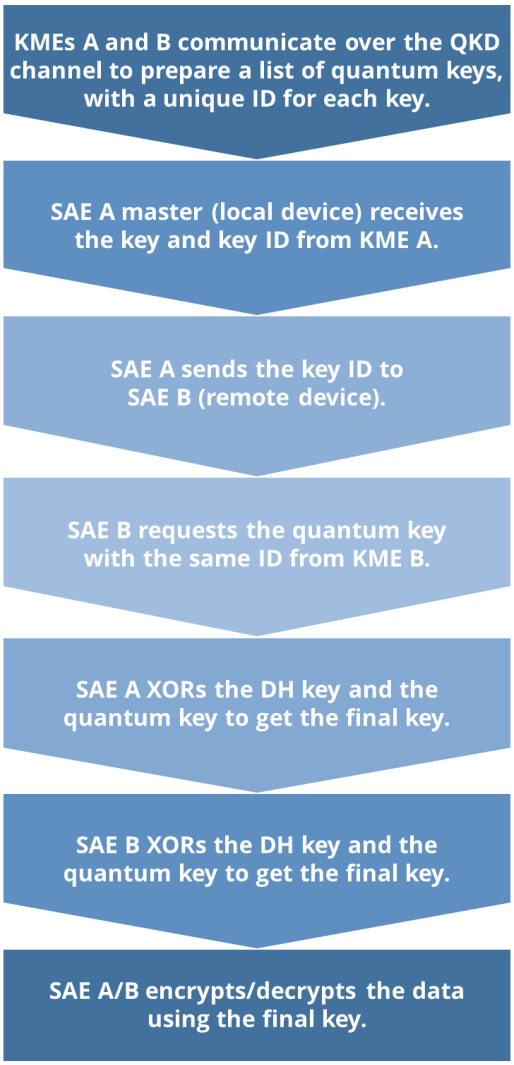


図 3: QKDメカニズムのプロセス

DWDM/OTNネットワークへのQKDの追加

暗号化ビットは量子チャネル（Qチャネル）を介して伝送されます。
これに加えて、QKDノードには専用の波長チャネルを通過するクロックと、GCCチャネルまたはOSCチャネルを通過するウェイサイド管理が必要となります。Qチャンネルを追加するには2つのアプローチがあり、それぞれに利点と欠点があります。

1.専用ダークファイバーの追加

2.既存の波長を利用

専用ファイバーによるQKD

量子チャネルは繊細です。量子チャネルを通過する光子は距離とノイズと戦わなければならず、特に長距離では信号の品質に悪影響を及ぼします。例えば40km以上の距離を伝送する信号には、マルチプレクサのような追加デバイスが必要で、減衰が加わり、信号の質が低下します。サイト間にQチャンネル専用のダークファイバーを追加することで、QKDの伝送がよりスムーズになります。このため、QKDユニット間にクロック（Cバンド）用の波長を割り当てる必要があります（トラフィック波長と多重化）

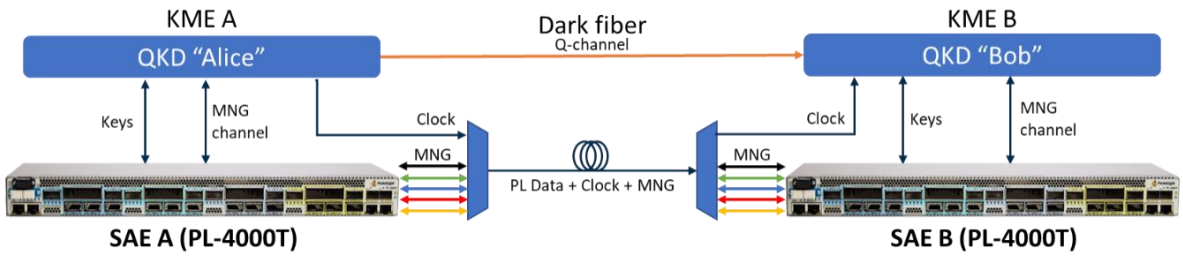


図 4: QKD専用ダークファイバーによるポイント・ツー・ポイント・ネットワーク

その他の技術情報

- 管理(OSC)チャネルは1510nmの波長を使用
- 最大距離/リンクバジェット：最大100km
- キー・レート：最大1Kbit/秒（4キー/秒）

既存の波長を利用したQKD

この方式では、QKDユニット用に専用チャネルが割り当てられ、クロック用（Cバンド）とQチャネル用（1310nm）の別々の波長がトラフィック波長と多重化されます。この方式の主な利点の1つは、追加インフラが不要なため、費用対効果が高いことです。ただし、両方の目的で同じ光ファイバーを使用するとノイズが発生し、暗号化距離が制限されることに注意してください。

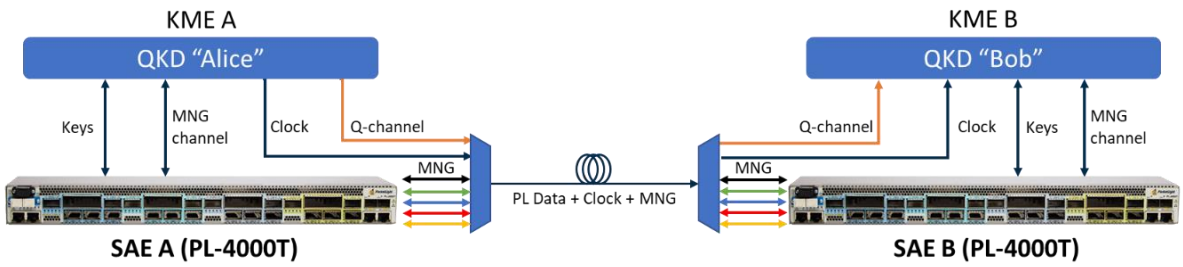


図 5: 既存の光ファイバー(インフラ)を利用したQKD

その他の技術情報

- 管理(OSC)チャネルは1510nmの波長を使用
- 最大距離/リンクバジェット：最大60km
- キー・レート：最大1Kbit/秒（4キー/秒）

テストと検証プロセス

PacketLightの装置とQKD技術の統合に成功したことは、量子通信技術と光ネットワーキング機能の進歩における重要なマイルストーンとなります。量子通信システムと光ネットワーキング・インフラストラクチャとの互換性は、統合ソリューションの最適な性能、安定性、信頼性を保証するための厳格なテストを経て証明されました。

QKDサプライヤーとの協力により、量子通信ソリューションと光ネットワーキング・インフラを組み合わせることの可能性が実証され、シンプルさと拡張性に重点を置きながら、安全で効率的なデータ伝送の新たな可能性が解き放たれました。PacketLight装置はベンダーにとらわれず、どのようなQKDソリューションとも連携できます。

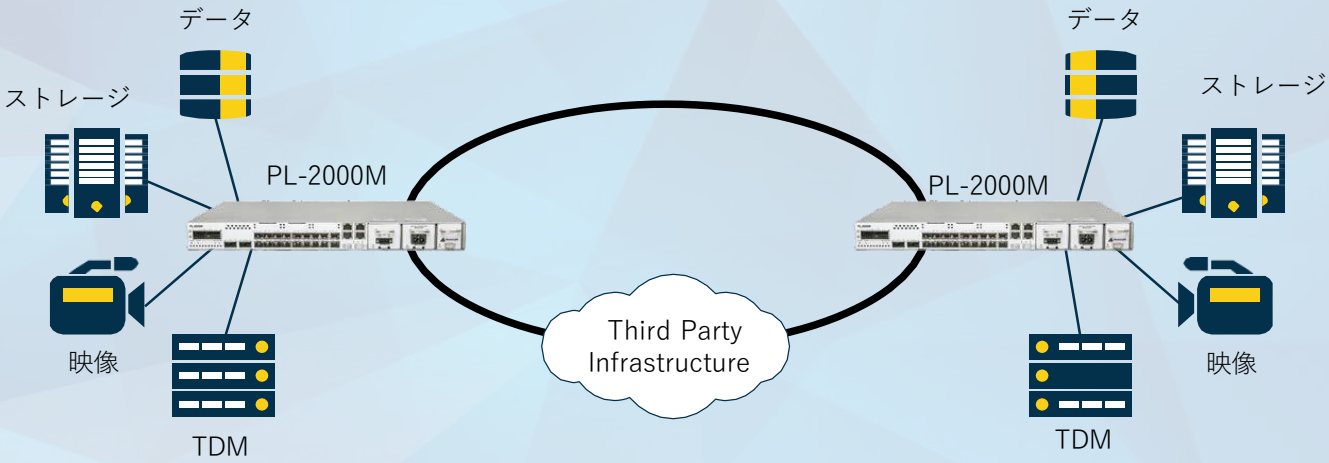
PacketLight™ NETWORKS

PacketLight社は、20年以上にわたる光ファイバーネットワーキングの経験を生かし、キャリアグレードのDWDMおよびOTN機器を提供することで、光ファイバーレイヤ全体のトランスポートソリューションを提供し、CAPEXおよびOPEXを削減します。PacketLight社のソリューションにより、通信事業者、データセンター、企業、コンテンツプロバイダー、ダークファイバープロバイダー、大学、政府・防衛機関は、大容量データ配信の需要に卓越したサービスで応えることができます。

> “PacketLightの暗号化ソリューションが、お客様のネットワークセキュリティを最大化するためにどのように役立つかをご覧ください。”

DWDM及びOTNデバイスの開発・製造メーカー

- ◆メトロ、 ショートホール、ロングホーの光伝送ネットワーク
- ◆大容量, 低遅延,の光ネットワークインフラ
- ◆DWDM技術でファイバー利用率の最大化
- ◆データ、ストレージ、ビデオ、音声プロトコルを合わせて伝送
- ◆既存のDWDM/OTNインフラをエイリアン波長で拡張
- ◆Layer-1暗号によるセキュアトランスポート（認証取得済み）
- ◆OTDRとOSAによる非侵入型の光ファイバ診断とモニタリング
- ◆標準規格に準拠したOTNマックスポンダおよびトランスポンダ
- ◆設定、管理、監視を容易にするNMS



製品ラインアップ

PL-4000T
1.6T トランスポンダ/マックスポンダ

PL-4000M
400G マックスポンダ

PL-2000M
200G マックスポンダ

PL-2000
20G OTN マックスポンダ

PL-2000T
800G WDM

PL-1000TN
10G DWDM OTN トランスポンダ

産業分野

DCI　放送　政府機関　金融　教育　通信事業者　プロバイダ　公共施設

Our Range of Products

レイヤー1
暗号化

低消費電力

1Uラックマウント

マルチオペ
レーション
モード

Pay As You Grow

コスト効率的
なソリュー
ション

	DCI	Metro	Long Haul
400G	PL-4000T T PL-4000G T	PL-4000T T	PL-4000T T
100G	PL-2000T T PL-2000DC T PL-2000M T PL-4000G T PL-4000T M PL-4000M M	PL-2000T T PL-2000DC T PL-2000M T PL-4000T M PL-4000M M	PL-2000T T PL-2000M T PL-4000T M PL-4000M M
8/16/32G	PL-1000TE T PL-2000M M PL-4000M M PL-2000ADS A M	PL-2000M M PL-4000M M PL-2000AD A M	PL-2000M M PL-4000M M PL-2000AD A M
10/25/40G	PL-1000TE T PL-2000M M PL-4000M M PL-2000ADS A M	PL-1000TN T PL-2000M M PL-4000M M PL-2000AD A M	PL-1000TN T PL-2000M M PL-4000M M PL-2000AD A M
1-4G	PL-1000TE T	PL-2000 A M	PL-2000 A M

Infrastructure					
Diagnostics	ROADM	EDFA	Raman	Mux/Demux	DCM
PL-1000D	PL-1000RO	PL-1000IL	PL-1000R	PL-300	PL-300
NWS			Support		
PacketLight LightWatch			PL-Care		

T Transponder　M Muxponder　A ADM　レイヤー1暗号化

主なメリット

- レイヤー1暗号化
- ネットワーク管理システム
- mux/demux、EDFA、光スイッチ、DCM（オプション）内蔵
- シンプルな設置・設定
- 低遅延での持続が可能
- ペイ・アズ・ユー・グロウ・アーキテクチャー
- 高い波長利用率
- 1Uサイズ

アプリケーション

- データセンター間相互接続
- エイリアン波長
- ファイバー監視と診断
- ビデオトランスポート
- レイヤー1暗号化
- マルチモードファイバーソリューション

活用シーン

- キャリア＆ISPs
- ダークファイバープロバイダー
- 公共
- 研究＆教育機関
- エンタープライズ
- スマートシティ
- 金融
- 政府関係
- ブロードキャスト

PacketLight™
NETWORKS

国内総代理店
株式会社アイランドシックス

packetlight@iland6.com
www.packetlight.jp