Product Brief

タレスCN6140 マルチリンク ネットワーク 暗号化装置

最大40 Gbpsのスケーラブルで
信頼性の高い移動中データの
暗号化を実現

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

リアルタイムの低遅延とほぼゼロのオーバーヘッドという、ネットワークパフォーマンスへのニーズを満たすことが実証された高速ネットワーク暗号化により、移動中データの保護を実現します。データセンターやクラウド全体でネットワークを経由して送信されるデータに対して、妥協のないセキュリティを提供します。

タレスCN6140マルチリンクネットワーク暗号化装置（CN6140）は、ダークファイバーや、メトロまたはワイドエリアイーサネットネットワーク（MANまたはWAN）を移動するすべての音声、ビデオ、データ通信を、最大40 Gbps（4x10）のフルラインレートで透過的に暗号化するように設計されたマルチポート（1 Gbps または 10 Gbps）の、信頼性の高い暗号化装置です。

パフォーマンス

CN6140は、高パフォーマンスな暗号化装置です。全二重モードでパケットロスなしに最高速度で動作します。FPGA（フィールドプログラマブルゲートアレイ）技術を採用したCN6140のカットスルーアーキテクチャは、データフレームを受信と同時に処理します。これにより、すべてのパケットサイズで一貫した低遅延を実現し、パフォーマンスを最適化します。スループットは、プロトコルのゼロオーバーヘッドモードで最大化されます。1Uのユニットで、一般的なハードウェアベースの暗号化装置よりも30～60%少ない消費電力で動作します。

スケーラビリティ

CN6140は、イーサネット規格に準拠しているため、主要ベンダーの業界標準ネットワーク機器と完全に相互運用可能です。マルチポート設計により、最大40 Gbps（4x10 Gbps）の可変速度ライセンスを提供します。また、設置が簡単で費用対効果に優れています。「全自動」のシンプルさと、アプリケーションとプロトコルの透過性を設計の基本原則としており、実装、運用、管理が容易で、必要なリソースを最小限に抑えられます。デバイスは、メンテナンス、機能拡張、セキュリティアップデートのために、簡単にフィールドアップグレードが可能です。タレスネットワーク暗号化装置製品ファミリー全体との完全な互換性により、エンドユーザーはあらゆるネットワーク環境で安全なデータ伝送を実現できます。

認定されたセキュリティ

世界最高レベルのセキュリティを誇る組織に採用されている、耐タンパ性を備えたCN6140は、コモンクライテリアとFIPS 140-2 Level 3要件に対する認定を申請中で、標準ベースのエンドツーエンド認証暗号化とクライアント側の鍵管理をサポートしています。高度なセキュリティ機能には、トラフィックフローセキュリティ、幅広い楕円曲線（Safe Curves、Brainpool、NIST）のサポートが含まれます。VLANベースの暗号化は、ハブアンドスポーク環境に一意の鍵ペアを提供し、正しく構成されていないトラフィックから保護します。信頼性の高い環境であり、暗号化装置はネストされた暗号化もサポートしています。

最先端の鍵管理

CN6140は、外部鍵サーバーに頼る必要がありません。堅牢なフォールトトレラントセキュリティアーキテクチャと耐タンパ性を備えたシャーシを提供します。物理的および仮想的な職務分掌により、権限のあるユーザーのみが鍵にアクセスできるようになります。暗号鍵は、デバイスの耐タンパ性エンクロージャ内のハードウェアにおいて安全に生成および保管され、物理的に鍵を抜き取ろうとする不正が試みられた場合、デバイスはゼロ化されます。

CN6140はハードウェアベースの乱数発生器をサポートしており、外部生成されたエントロピーを固有鍵の生成と配布に使用できます。将来を見据えて暗号化装置は、量子鍵配布（量子暗号）と量子乱数生成をサポートしています。

次世代高速暗号化

クリプトアジリティ

タレスネットワーク暗号化装置は、クリプトアジリティ（暗号の俊敏性）を備えており、幅広い楕円曲線やカスタム曲線に対応したカスタマイズ可能な暗号化をサポートしています。また、独自のエントロピー機能の持ち込みも可能です。クリプトアジャイルなプラットフォームは将来を見据えた設計であり、次世代アルゴリズムやカスタムアルゴリズムを迅速に展開できます。量子の脅威に対応するため、タレスネットワーク暗号化装置はすでに量子鍵配布（QKD）と量子乱数生成（QRNG）機能を活用して、将来を見据えたデータセキュリティを実現しています。

トランスポート非依存モード

ネットワーク暗号化市場に変革をもたらすタレスネットワーク暗号化装置は、トランスポート非依存モード（TIM; Transport Independent Mode）を提供する業界初の製品であり、ネットワークレイヤーに依存せず（レイヤー2、レイヤー3、レイヤー4）、プロトコルにとらわれない移動中データの暗号化を実現します。レイヤー3をサポートすることで、タレスネットワーク暗号化装置は、重要なデータを保護するために、TCP/IPルーティングを使用してより多くの構成オプションをネットワークオペレーターに提供します。

CN9120暗号化装置の概要

モデル	CN6140
プロトコルと接続性	
最大速度	100 Gbps
レート制限オプション	1x1 Gbps～4x10 Gbps	あり
ジャンボフレームのサポート	あり
プロトコルおよびアプリケーション透過性	あり
ユニキャスト、マルチキャスト、ブロードキャストトラフィックの暗号化	あり
自動ネットワーク検出と接続確立	QSFP28
セキュリティ	
耐タンパ性と改ざん防止機能を備えたエンクロージャ、アンチプロービングバリア	あり
柔軟な暗号化ポリシーエンジン	あり
AES-GCM暗号化によるパケット単位の機密性および完全性	あり
自動鍵管理	
暗号化とポリシー	
AES 128または256ビット鍵	あり
CFB、CTR、GCM暗号化モード	CTR
オプションでサードパーティによる量子鍵配布（QKD）をサポート	あり
MACアドレスまたはVLAN IDに基づくポリシー	あり
ネットワーク停止時に自己修復可能な鍵管理	
認定取得	
コモンクライテリア、FIPS	あり
パフォーマンス	
低オーバーヘッドの全二重ラインレートでの暗号化	あり
FPGAベースのカットスルーアーキテクチャ	あり
遅延（マイクロ秒／暗号化装置あたり）	<2 μS
管理	
フロントパネルLEDディスプレイ通知	あり
SMCおよびCM7を使用した一元的な構成と管理	あり
外部認証局（X.509v3）のサポート	あり
SNMPv3を使用したリモート管理（インバンドおよびアウトオブバンド）	あり
NTP（タイムサーバー）のサポート	あり
CRLおよびOCSP（証明書）サーバーのサポート	あり
保守性と相互運用性	
現場でのファームウェアのアップグレード	あり
二重化冗長AC/DC電源	あり
プラグ可能な光SFP+	あり

仕様

物理セキュリティ

- アクティブ／パッシブタンパ検出および鍵消去暗号化
- AES 128または256ビット鍵 X.509証明書（CFB、CTR、GCMモード）
- ハードウェアベースの乱数発生器

デバイス管理

- 専用管理インターフェース（アウトオブバンド）
- 暗号化されたインターフェース（インバンド）
- SNMPv3リモート管理
- IPv4およびIPv6対応
- Syslogのサポート
- アラーム、イベント、監査ログ
- コマンドラインシリアルインターフェース
- TACACS+サポート

設置

- 寸法: 447 mm x 43 mm (1U) x 328 mm /17.6” x 1.7” x 12.9”
- 19インチラックマウント可能
- 重量: 8.5 kg /18.7 lbs

電力要件

- AC入力: 100～240V AC、1.5A、60/50Hz
- DC入力: 40.5～60 VDC、2.0A
- 消費電力: 50W（標準）

規制上の安全性

- UL Listed
- EMC（エミッションとイミュニティ）
- FCC 47 CFRパート15（米国）
- EN 55024 (CE, 60950-1 (CE)、61000-3-2 (CE)、61000-3-3 (CE)
- IEC 60950-1第2版
- ICES-003（カナダ）

環境仕様

- RoHS対応
- 最高動作温度: 50°C /122°F
- 40°C /104°F動作時の相対湿度0～80%
- AS/NZS 60950-1、CISPR 22 (C-Tick)

すべての仕様は発行時点のものであり、予告なく変更される場合があります。

タレスについて

今日の企業は、決定的な意思決定を行うために、クラウド、データ、ソフトウェアに依存しています。そのため、世界で評判の高いブランドや最大手の組織は、クラウドやデータセンターからデバーク全体に至るまで、作成、共有、保存場所を問わず機密情報やソフトウェアを保護し、それらへのアクセスを安全に確保するために、タレスに信頼を寄せています。当社のソリューションは、企業がクラウドに安全に移行し、自信を持ってコンプライアンスを達成し、何百万人もの消費者が毎日利用するデバイスやサービスにおいて、ソフトウェアからより大きな価値を生み出すことを可能にします。

cpl.thalesgroup.com
お問い合わせ先 – Email: cpl.jpsales@thalesgroup.com
すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。