Product Brief

タレスCN4020 ネットワーク暗号化装置

コンパクト設計で 高パフォーマンスな 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

タレスCN4010ネットワーク暗号化装置（CN4010）は、光インターフェースと、FIPSおよびコモンクライテリアの認定を受けた、信頼性の高いフルラインレートでのイーサネット暗号化を提供します。CN4020は、汎用性の高いユーザー構成可能な使いやすいプラットフォームで、x（ FTTx）構成に対して、高セキュアなフルラインレートでのネットワーク暗号化を提供します。低コストで高効率のネットワーク暗号化を保証する専用ハードウェア暗号化ソリューションとして、最先端の高性能、光インターフェース接続、低電圧エレクトロニクスを活用し、すべての音声、ビデオ、データ通信をワイヤスピードで暗号化します。CN4020は、コンパクトなデスクトッププロファイルで、中小企業（SME）の商業部門や、最大1 Gbpsの光インターフェースのネットワークニーズを持つ大企業向けの、エントリーレベルのHSEソリューションとして設計されています。また、広範囲に分散したコンピューティング環境や複数の支社拠点にも適しています。

CN4020暗号化装置が選ばれる理由

信頼できるセキュリティ

- 真のエンドツーエンドの、認証された暗号化
- 最先端の自動ゼロタッチ鍵管理
- FIPS 140-2 L3、コモンクライテリア、NATO、UC APLに対応する設計
- 世界35カ国以上の市場をリードする民間企業や政府機関が採用

最大のネットワークパフォーマンス

- マイクロ秒の遅延（10 μS未満）
- ほぼゼロのオーバーヘッド
- 自己修復機能により最大限の稼働時間を実現

スケーラブルかつシンプル

- ポイントツーポイント、ハブアンドスポーク、フルメッシュ
- サードパーティの管理ツールから完全に監査可能なアラームおよびイベントログ

パフォーマンス

CN4020は、高セキュアな暗号化装置です。洗練されたデスクトッププロファイル内で、ポイントツーポイント、ハブアンドスポーク、メッシュ環境において、全二重モードでパケットロスなしに100/1000　Mbpsのフルラインレートで動作し、ネットワークを暗号化します（オプションでラックマウント変換キットが付属）。信頼性の高いアプライアンスとして、CN4020には次のような利点もあります。

- 安全な耐タンパ性を備えた専用ハードウェア
- 標準ベースの暗号化アルゴリズム
- エンドツーエンドの、認証されたネットワーク暗号化
- 自動「ゼロタッチ」暗号鍵管理

スケーラビリティ

CN4020は、「Bump in the Wire」設計と最大1 Gbpsの可変速度ライセンスを提供し、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、ネットワーク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。

CN4020は、タレスネットワーク暗号化装置製品ファミリーと完全に相互運用可能であるため、単一のプラットフォームで標準化し、ネットワーク上の移動中データを保護することができます。CN4020の光インターフェースに加え、オプションで電気（銅線）インターフェースコンバータも用意されており、現在銅線を使用しているお客様に将来を見据えたソリューションを提供し、幅広いFTTxシナリオに対応します。

認定されたセキュリティ

耐タンパ性を備えたCN4020は、コモンクライテリアおよびFIPS 140-2 Level 3の認定を取得済みで、標準ベースのエンドツーエンド認証付き暗号化、自動鍵管理をサポートし、強力なAES 256ビットアルゴリズムを利用しています。アプライアンスを将来にわたって保証するために、暗号化装置は量子鍵配布に対応しており、デバイス間の安全な通信を保証します。

最先端の鍵管理

CN4020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。

CN4020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。

CN4020 Encryptor At-A-Glance

モデル	CN4020
プロトコルと接続性	
最大速度	1 Gbps
ジャンボフレームのサポート	✓
プロトコルおよびアプリケーション透過性	✓
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	✓
自動ネットワーク検出と接続確立	✓
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	✓
柔軟な暗号化ポリシーエンジン	✓
AES-GCM暗号化によるパケット単位の機密性および完全性	✓
自動鍵管理	✓
暗号化とポリシー	
AES 128または256ビット鍵	✓
CFB、CTR、GCM暗号化モード	✓
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	
MACアドレスまたはVLAN IDに基づくポリシー	✓
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	✓
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	✓
FPGAベースのカットスルーアーキテクチャ	✓
遅延（マイクロ秒/暗号化装置あたり）	< 10μS
管理	
フロントパネルLEDディスプレイ通知	✓
SMCおよびCM7を使用した一元的な構成と管理	✓
外部認証局（X.509v3）のサポート	✓
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）	✓
NTP（タイムサーバー）のサポート	✓
CRLおよびOCSP（証明書）サーバーのサポート	✓
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	✓
外部プラグパック	✓

仕様

暗号化

- AES 128または256ビット鍵 X.509証明書
- 公開鍵基盤（PKI）に完全準拠

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）
- または暗号化されたインターフェース経由（インバンド）
- SNMPv3リモート管理
- IPv4およびIPv6対応
- 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

設置

- デスクトップおよび付属のラックマウントキット
- 寸法: （幅Wx高さHx奥行D）-(W:180 mm/7.1”、D:126 mm/5.0”、H:32 mm/1.3”)
- 重量: 0.5 kg /1.1 lbs

インターフェース

- SFPインターフェース
- シリアルコンソール、8ピンモジュラージャック
- RJ45 LANコネクタ

電力要件

- DC入力12V DC、消費電力7W
- AC プラグパック100-240V AC、60-50Hz、0.7A

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
- 改ざん防止マーキング
- アンチプロービングバリア

規制

- EN 60950-1 (CE)
- IEC 60950-1第2版
- AS/NZS 60950.1
- 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）
- ICES-003（カナダ）
- EN 55022 (CE)

- AS/NZS CISPR 22 (RCM)
- EN 61000-3-2 (CE)
- EN 61000-3-3 (CE)
- EN 55024 (CE)

環境仕様

- RoHS対応
- 最高動作温度: 40°C /104°F
- 40°C /104°F動作時の相対湿度0～80%

*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。