

Product Brief

# タレスCN9120 ネットワーク 暗号化装置

100 Gbpsの高速暗号化で  
移動中データの保護を実現

[cpl.thalesgroup.com](http://cpl.thalesgroup.com)

**THALES**  
Building a future we can all trust

タレスCN9120ネットワーク暗号化装置は、毎秒100,000,000,000ビットという信頼性の高いデータ暗号化を実現し、データセキュリティ(100 Gbps)および高速ネットワークパフォーマンスを超低遅延(2  $\mu$ S未満)で提供します。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、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ビッグデータやメガデータに対しても、妥協のないセキュリティを提供します。

データ量が増加し続け、広帯域サービスの需要が高まる中、CN9120は、100 Gbpsの最高速度で前進する組織にとって理想的なソリューションです。CN9120は、ダークファイバーや、メトロ、ワイドエリア、キャ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、100 Gbpsの高セキュアなフルラインレートで暗号化するように設計された、信頼性の高い暗号化装置です。プロバイダーネットワーク、データセンター相互接続、災害復旧リンクの暗号化に最適であり、マルチポイントツーマルチポイント環境を含むあらゆるネットワークトポロジをサポートします。



## パフォーマンス

### CN9120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(2  $\mu$ S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
- ホットスワップ対応のファンにより、フィールドサービスが可能

CN9120は超高パフォーマンスな暗号化装置であり、全二重モードで100 Gbpsのラインレートで動作します。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CN9120のアーキテクチャは、リアルタイムデータ処理と高スループットを可能にします。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ユニットで、最小限の電力消費とラックスペースで動作します。

## パフォーマンス

CN9120は、標準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。「Bump in the Wire」設計により、100 Gbpsの暗号化に対する、ベンダーにとらわれないドロップインネットワークのアプローチを提供します。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。

## 認定されたセキュリティとクリプトアジリティ

セキュリティ意識の高い組織向けに設計された、耐タンパ性を備えたCN9120は、コモンクライテリアEAL4+およびFIPS 140-2 Level 3の認定申請中で、自動ゼロタッチ鍵管理をサポートしています。

クリプトアジリティ(暗号の俊敏性)を可能にするCN9120の高度なセキュリティ機能には、幅広い楕円曲線(Safe Curves、Brainpool、NIST)のサポートが含まれます。カスタム曲線とカスタムエントロピーは、暗号化ソフトウェアの標準機能です。

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。

## 最先端の鍵管理

CN9120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るよ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。CN9120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	CN9120
<b>プロトコルと接続性</b>	
最大速度	100 Gbps
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	あり
ネットワークインターフェース	QSFP28
<b>セキュリティ</b>	
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
自動鍵管理	あり
<b>暗号化とポリシー</b>	
AES 256ビット鍵	あり
暗号化モード	CTR
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	あり
<b>認定取得：申請中</b>	
コモンクライテリア、FIPS、NATO、UC APL*に対応する設計	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 $\mu$ S

## 管理

フロントパネルからすべてのインターフェースにアクセス	あり
SMC/CM7およびSNMPv3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/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
ホットスワップ可能な二重化AC電源	あり
ユーザーによる交換が可能なファンとバッテリー—二重の冗長性	あり
すべてのCNシリーズ暗号化装置との相互運用性	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 256 ビット鍵 X.509証明書(CTR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、NTP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
- TACAS+サポート
- RADIUSサポート

### 設置

- 寸法: 435 mm x 43 mm x 480 mm /17.1" x 1.7" x 18.9"
- 1U 19インチラックマウント可能
- 重量: 8 kg /17.6 lbs

### 電力要件

- AC入力: 100~240V AC、1.5 A、50/60 Hz
- 消費電力: 80 W(標準)

### 規制上の安全性

- UL Listed(申請中)
- 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)、55022 (CE)
- EN 60950-1 (CE)、61000-3-2 (CE)、61000-3-3 (CE)
- IEC 60950-1第2版
- ICES-003(カナダ)
- AS/NZS 60950-1、CISPR 22 (RCM)

#### 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%

## 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。