

Product Brief

THALES

CYBERSECURITY

CN7108 ネットワーク 暗号化装置

過酷な環境に
対応した設計：
現場最前線向けの
堅牢な暗号化

cpl.thalesgroup.com

CN7108ネットワーク暗号化装置(CN7108)は、HSE(High Speed Encryptor:高速ネットワーク暗号化装置)ポートフォリオを、軍事・産業・IoT・リモートの最前線という新たな領域にまで拡張するものです。堅牢な産業グレードハードウェアを基盤に特定用途向けに設計されたCN7108は、FIPS 140-3認証取得済みで、量子耐性かつクリプトアジリティを備えたデータ転送の暗号化を、最大1Gbpsで提供します。MIL-STD-810G準拠、広範な温度耐性、筐体サイズ・消費電力・コストの最適化により、最も過酷な環境下でのミッションクリティカルな運用に必要な、信頼性の高いセキュリティを実現します。



認証済みセキュリティとクリプトアジリティ

CN7108は、**FIPS 140-3レベル1認証**を取得した暗号化を提供し、AES-128/256鍵、X.509 RSA/ECC認証、認証付きGCM/CTRモードに対応しています。CN7108は**量子耐性**を備え、NIST PQC標準およびハイブリッド暗号方式をサポートしています。また、Cryptographic SDK(CSDK)を通じて、主権型またはカスタム暗号方式の利用も可能です。

ネットワークパフォーマンスの最大化

CN7108は、最大1Gbpsの暗号化スループットで、データ転送の安全なリアルタイム保護を提供します。**トランスポート非依存モード(TIM)**により、Ethernet、MPLS、衛星通信、セルラー通信、インターネットなど、さまざまな通信手段において、レイヤー2、3、4でトンネル不要・低オーバーヘッドの暗号化を実現します。

拡張性と柔軟性

コンパクトかつ堅牢なCN7108は、寸法132.8×100×34.8 mm(5.2×3.9×1.4インチ)、重量約420 g(0.93 lbs)です。改ざん検知機能付き筐体により、現場での物理的セキュリティを確保します。-40 °C~+85 °C(-40 °F~+185 °F)の温度範囲で動作し、MIL-STD-810G準拠の耐衝撃・耐振動性能を備え、ファンレスのソリッドステート構造により静音かつ信頼できる運用を実現します。ポイントツーポイント、ハブ&スポーク、フルメッシュの各トポロジーをサポートし、サイズ・重量・消費電力に制約のある環境への展開に最適化されています。また、すべてのタレスHSEとの完全な相互運用性を備えており、既存ネットワークへのシームレスな統合が可能です。

CN7108を選ぶ理由

- FIPS 140-3認証取得済み、量子耐性の暗号化
- 堅牢な産業グレードハードウェア、MIL-STD-810G準拠
- 堅牢かつ改ざん検知機能付き筐体による物理的セキュリティ強化
- 過酷な環境下でも最大稼働時間を実現する信頼性の高い設計
- -40 °C~+85 °C(-40 °F~+185 °F)の動作温度範囲
- リモートエッジ、IoT、軍事用途向けに最適化
- 自動化されたゼロタッチ鍵管理機能
- タレスHSEポートフォリオとの完全な相互運用性

高度な暗号化と鍵管理

CN7108は、イーサネット暗号化モードにおいて、**X.509証明書とRSA/ECDH鍵交換**を採用しています。トランスポート非依存モード(TIM)では、**NIST認定の鍵生成方式を使用し、完全前方秘匿性を備えた堅牢かつ量子耐性のあるデータ保護を実現します**。また、CipherTrust Data Security Platform(統合データセキュリティプラットフォーム)を含む外部の鍵管理サーバーとの統合も可能です。

LINEおよびVLANモードにより、Ethernetサービス上のユニキャスト、マルチキャスト、ブロードキャストトラフィックを暗号化でき、VLANごとに固有の暗号鍵を用いて暗号化の分離を確保します。

ユーザーフレンドリーな管理

直感的な**一元管理**により、CN7108は、他のタレスHSE製品スイートと同様に、「全自動」のシンプルさと、プロトコルとネットワークの透過性を提供します。CN7108は、Syslog、NTP、SNMPv3、アラームおよびイベントログ、セキュアな管理チャネルに対応しています。ファームウェアのアップグレードはUSB経由で可能で、ローカル設定はSSH対応のシリアルコンソールから行えます。

CN7108の概要

パフォーマンス	最大1Gbpsの暗号化スループット
暗号技術	AES-128/256、RSA/ECC、GCM/CTR、PQC対応、CSDKによる主権型/カスタム暗号方式
インターフェイス	ギガビットイーサネット×2、ギガビット管理ポート×2、USB、シリアルコンソール
管理	CM7, SMC, Syslog, SNMPv3, NTP
環境仕様	温度: -40 °C ~ +85 °C (-40 °F ~ +185 °F) MIL-STD-810G 準拠の耐衝撃・耐振動設計、ファンレス
ハードウェア設計	132.8×100×34.8 mm (5.2×3.9×1.4インチ)、約420 g (0.93 lbs)
電源	9-42V DC入力、オプションのPoE
認証取得	FIPS 140-3レベル1、MIL-STD-810G

仕様

パフォーマンス

- スループット: 1Gbpsの全二重ラインレート暗号化

暗号セキュリティ

- AES-128/256暗号化、GCM/CTRモード
- X.509 RSA/ECC証明書
- FIPS 140-3レベル1認証取得済み暗号モジュール
- 量子対応(NIST PQC標準に準拠)
- CSDKによるカスタム暗号方式

インターフェイス

- RJ45ギガビットイーサネット(ローカル/ネットワーク)×2
- RJ45ギガビットイーサネット(管理)×2
- USBポート(ファームウェアアップグレード、デバッグ)
- SSH対応シリアルコンソール

環境仕様

- 動作温度: -40 °C ~ +85 °C (-40 °F ~ +185 °F)
- 湿度: 5% ~ 95% (結露なきこと)
- MIL-STD-810G 準拠の耐衝撃・耐振動設計
- ファンレス、ソリッドステート筐体

物理仕様

- 寸法: 132.8×100×34.8 mm (5.2×3.9×1.4インチ)
- 重量: 約420 g (0.93 lbs)
- 堅牢かつ改ざん検知機能付き筐体による物理的セキュリティ強化

電源

- 入力: 9-42 V DC、最大3.33 A (負荷に応じて30~155 W)
- オプションのPoE

管理

- 一元管理 - CM7およびSMCに対応
- SNMPv3, Syslog, NTP、監査/イベントログ記録
- アラームおよびイベント通知

SWaP

- サイズ・重量・消費電力を最適化

規制上の安全性・適合性

- CE (欧州適合)
- FCCパート15 (米国)
- ICES-003 (カナダ)
- EMC (エミッションとイミュニティ)
- IEC/EN 62368-1 (IT機器の安全性)
- RoHS, WEEE, REACH環境適合

タレスについて

タレスはデータセキュリティのグローバルリーダーとして、世界中で高い信頼を得ているさまざまな組織が、あらゆる場所で重要なアプリケーション、機密データ、およびIDを包括的に保護できるよう支援しています。タレスは、革新的なサービスと統合プラットフォームを通じて、リスクの可視化、サイバー攻撃の防御、そしてコンプライアンスギャップの解消を可能にし、毎日数十億人の消費者に安心して信頼性の高いデジタルエクスペリエンスを提供します。