ゲートウェイアプライアンス仕様

	2530	2550	2560	2570	2580	1900	2000
エンタープライズトラフィックのパフォーマンス							
NGTX 脅威対策 スループット *1	0.75 Gbps	1 Gbps	1.85 Gbps	2.5 Gbps	3.2 Gbps	4 Gbps	5 Gbps
NGFW スループット *2	1.2 Gbps	1.6 Gbps	3.75 Gbps	5 Gbps	9 Gbps	8 Gbps	10 Gbps
RFC 3511, 2544, 2647, 1242のパフォーマンス（試験環境）							
ファイアウォール 1518バイト UDPパケット	3 Gbps	4 Gbps	11.6 Gbps	15,5 Gbps	20 Gbps	32 Gbps	40 Gbps
VPN暗号スループット	1.4 Gbps VPN AES-GCM 1452B		4 Gbps VPN AES-GCM 1452B		4.5 Gbps VPN AES-GCM 1452B	5 Gbps VPN AES-128	6 Gbps VPN AES-128
1秒あたりの接続数	16,000	20,000	53,000	62,000	72,000	90,000	100,000
同時接続数	1,000,000		2,000,000			4,200,000	
ソフトウェア							
セキュリティ	ファイアウォール、VPN、ユーザー認識、QoS、アプリケーション制御、URLフィルタリング、IPS、アンチボット、アンチウイルス、アンチスパム、サンドボックス						
ユニキャスト／マルチキャスト ルーティングおよびクラスタリング	OSPFv2, BGPv4 and 4++, RIP, PIM (SM, DM, SSM), IGMP, ClusterXL High Availability						
リモートアクセスユーザー数	100		200		1,000	1,000	
ハードウェア							
WANポート	1 x 1GbE RJ45/SFP		1 x 1GbE RJ45		1 x 1GbE RJ45/SFP 1 x 10GbE RJ45/SFP+	1x 10/100/1000Base-T RJ-45 1x 1GbE RJ45/SFP	
DMZポート	1 x 1GbE RJ45/SFP		1 x 1GbE SFP		1 x 1GbE RJ45/SFP 1 x 10GbE RJ45/SFP+	1x 10/100/1000Base-T RJ-45 1x 1GbE RJ45/SFP	
LANポート *3	6 x 1GbE RJ45		8 x 1GbE RJ45 and 2 x 10GbE SFP+		8 x 1GbE RJ45 2 x 2.5GbE RJ45	16x 1GbE RJ45 2x 2.5GbE RJ45 4x 10GbE/1GbE SFP+	
コンソールポート	1x USB-C				1x USB-C 1x RJ-45コンソールポート		
USBポート	1x USB 3.0					2x USB 3.0ポート	
Wi-Fiと周波数帯	Wi-Fi 7 2x2 2.4Ghz + 5Ghz		Wi-Fi 7 4X4 2.4Ghz + 5Ghz + 6Ghz		—		
物理仕様							
筐体	デスクトップサイズ、壁面取付け					1 RU	
寸法（幅×奥行×高さ）	210 x 170 x 42 mm				210 x 209x 42 mm	430 x 300 x 44 mm	
重量	0.87kg				0.988 kg	6.76 kg	
使用環境							
動作中/保管	0ºC ～ 40ºC / -45ºC ～ 60ºC（5～95%、非結露）						
電力要件							
AC入力	100 – 240V, 47 – 63 Hz					100 – 240V, 50 – 60 Hz	
電源	12V／3.3A・40W 電源アダプター （Wi-Fi非搭載モデル用）		12V／5A・60W 電源アダプター（冗長化対応） （Wi-Fi搭載モデル用）			冗長化された150W電源2基	
消費電力（最大）	26.01W（Wi-Fi非搭載時）／31.28W（Wi-Fi搭載時）／35.5W（Wi-Fi＋5G搭載時）					93.6W	
認証							
安全性 | エミッション | 環境規格	CB IEC 62368-1, CE LVD EN62368-1, UL62368-1, ASNZS 62368.1 / CE, FCC IC, VCCI, ASNZS ACMA / ROHS, REACH, WEEE, ISO14001					UL/c-UL 62368-1 , IEC 62368-1 CB / EMC; EMI EN55024, EN55032クラスB, VCCI, AS, NZS CISPR 32, IC ICES 03, FCC: パート15クラスB / RoHS, REACH, WEEE	

*1 Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot, SandBlast Zero-Day Protection
*2 Includes Firewall, Application Control, IPS
*3 FleXi Port対応：WANポートとして設定、変更可能

CHECK POINT™
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒105-0001東京都港区虎ノ門1丁目2-8　虎ノ門琴平タワー25F
https://checkpoint.com/jp

◆記載の社名および商品名は、各社の登録商標です。
◆記載されている製品の内容・仕様は2025年12月現在のものです。予告なしに変更する場合がございます。
◆また、製品写真は出荷時のものと異なる場合があります。
◆本製品は日本国内仕様であり、弊社では海外の保守サービスおよび技術サポートは行なっておりません。

お問合わせ

©2025 CheckPoint Software Technologies Ltd. All rights reserved

Quantum
Spark™

Check Point

“守る”を、次世代へ。
進化するサイバーセキュリティ

Quantum Spark

Check Point
Network
Security
Appliance

CHECK POINT™

“強さ”と“簡単さ”をひとつに

Quantum Spark 2500シリーズは、あらゆる拠点やオフィス環境に対応したオールインワン型セキュリティゲートウェイです。
Wi-Fi 7・10GbE対応、最大3.2Gbpsの防御性能を備え、ファイアウォールからIPS、ゼロフィッシングまで主要機能を1台で提供。
直感的な管理で運用も簡単です。

進化した機能で、新たな脅威に備える — 2500シリーズ新機能

最新のR82ソフトウェアにより、
ランサムウェアやフィッシングによるエクスプロイト攻撃から保護する性能は業界No.1

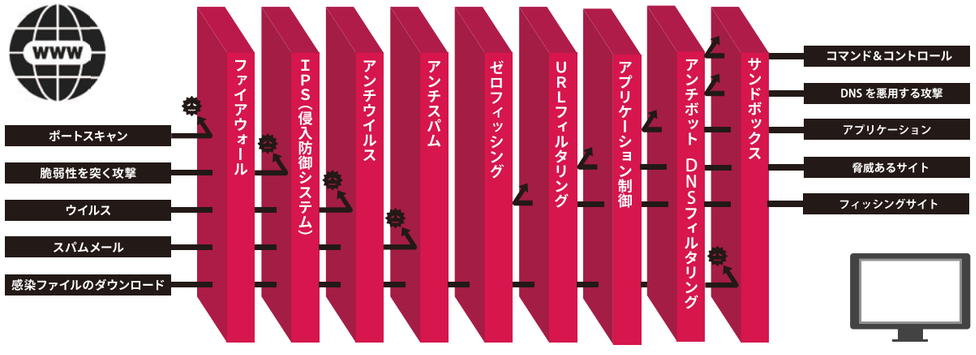
Wi-Fi7対応により、ワイヤレスユーザーのインターネット速度を30%向上

BYPASS
FONIC（フェイルオープン・ネットワーク・インターフェース・カード）により、
電源OFFや障害時でも通信をバイパス可能。
*Fonicは2530/2550/2560/2570の Wired model のみの対応となります

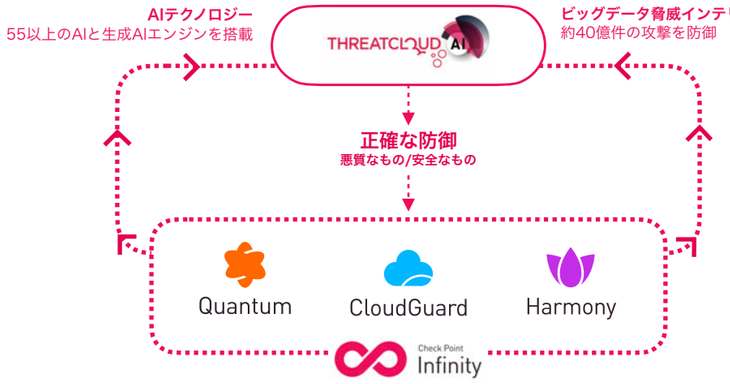
脅威対策スループットの向上により、セキュリティ検査速度が大幅UP

さらに強化された業界最高レベルのオールインワンソリューション

UTM（Unified Threat Management, 統合脅威管理）は、インターネット上の様々な脅威に対し、
多段階の防御を提供するネットワークセキュリティソリューションです。
最新のR82ソフトウェアでは、新たに「ゼロフィッシング」と「DNSセキュリティ」機能を搭載しました。
既知・未知のフィッシング攻撃やDNSを悪用した不正通信をリアルタイムに検知・遮断し、
総合的な防御力をさらに強化しました。



Check Point全ての製品と接続される、世界最先端の脅威インテリジェンス ThreatCloud AI



55以上の AIと
機械学習のテクノロジーにより
未知の脅威を特定してブロック

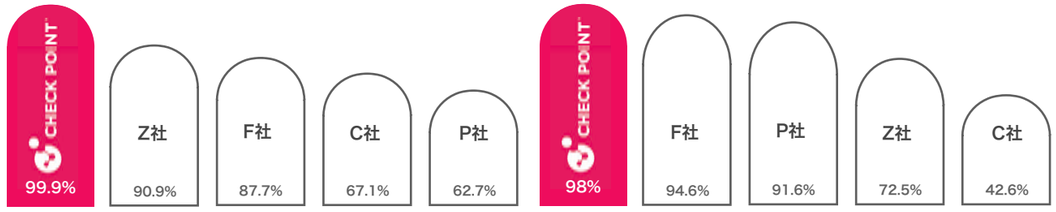
ネットワーク、クラウド、
Eメール、エンドポイント、
モバイル、およびチェック・ポイント・リサーチ（CPR）から、豊富な脅威やテレメトリー情報を収拾し、AIを利用した評決エンジンにより未知・ゼロデイの脅威を正確に検出します。

業界を代表する評価機関が認めた、高水準のセキュリティ性能

Miercom

2025セキュリティ・ベンチマーク・レポート
ゼロデイ + ワンデイマルウェア防御率
リアルタイム脅威防御を評価した際にも、
Check Pointは第1位に選ばれました。
それも過去3年連続での快挙です。

IPSの防御率
Check Point は**業界トップレベルの98%の防御率!!**



出典：https://miercom.com/wp-content/uploads/2025/02/Miercom-Check-Point-NGFW-CONFIDENTIAL-SR241113M-3FEB2025.pdf

“守る”だけで終わらない、企業の価値を高めるセキュリティへ

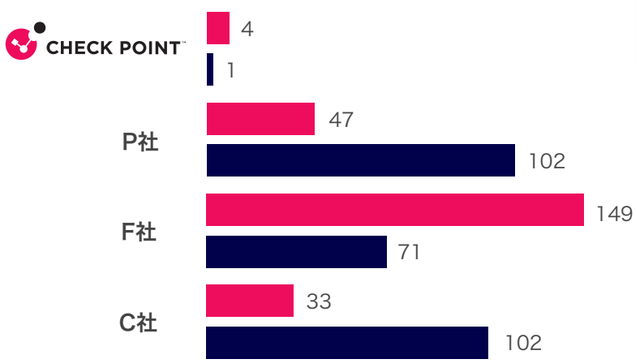
Quantum Spark 2500シリーズは、セキュリティ装置を超えた次世代プラットフォームです。
IPv6 IPoE対応の高速通信、Smart Accelによる最適化、IoT可視化、脆弱性の少ない堅牢設計などを備え、
「守る力」だけでなく「つながる力」「見える力」「安心できる運用」を提供します。

IPv6 IPoE + IPv4 over IPv6接続について

インターネットマルチフィード株式会社	transix IPv４接続 (DS-Lite)	DS-Lite
	transix IPv４接続 （固定IP）	IPIP
株式会社朝日ネット	v6 コネクト DS-Lite接続	DS-Lite
	v6 コネクト IPIP接続	IPIP
アルテリア・ネットワークス株式会社	クロスパス (Xpass) – 可変	DS-Lite
	クロスパス (Xpass) – 固定IP 1/8/16	IPIP
株式会社JPIX	「v6プラス」固定IPサービス	IPIP
株式会社NTTコミュニケーションズ	OCNバーチャルコネクト(動的IP/固定IP)	MAP-E
BBIX株式会社	OCX光/V6IX（固定IP）	IPIP
株式会社ビッグローブ	v6オプション（動的IP/固定IP）	MAP-E/IPIP

Quantum Spark 2500シリーズは、IPv6 IPoEとIPv4 over IPv6（DS-Lite / IPIP / MAP-E）に対応し、
新しいネットワーク環境でも高速で柔軟な通信を実現します。
IPv6によるネイティブ接続と、既存のIPv4システムの併用が可能なため、移行時の互換性や手間の心配は
ありません。さらに、transix、v6プラス、OCNバーチャルコネクトなど主要VNEにも対応し、
今後の通信環境の変化にも安心して備えられます。

脆弱性の少なさ



近年、多くの製品で脆弱性が相次いで発見され、
それを悪用したサイバー攻撃が急増しています。
脆弱性は攻撃者にとって格好の“侵入口”となり、
一度侵入されると情報漏えいや業務停止などの
深刻な被害を招きます。

Check Point製品は脆弱性が極めて少なく、
安定した運用が可能になり、お客様の環境において
不要なトラブル対応を減らすことができます。
この「脆弱性の少なさ」こそが、Check Pointが
世界で選ばれ続ける 大きな理由の一つです。

出典： vendors security advisories web pages & https://tiny.cc/urgency Updated Apr 28, 2025

・巧妙な偽装URLを見抜けず、社員が何度もアクセスしてしまうんです…　注意喚起だけでは限界で…
・新しい手口のフィッシングサイトが次々出てきて、どれが安全なのか、判断ができない…
・「取引先を装ったリンクをクリックしてしまい、情報を摂取されたかも」と、報告が増えていて正直ヒヤヒヤで…

企業担当者様の声

そのお悩み、解決します!!

ゼロデイ攻撃を防ぐ、ゼロフィッシング機能

ゼロフィッシング機能は、業界をリードする機械学習アルゴリズムと特許取得済みの検査技術を活用し、
巧妙化するフィッシング攻撃をリアルタイムで防御する機能です。
多くのサイバー攻撃の入り口となる未知のゼロデイ攻撃や既知のフィッシングサイトへのアクセスを防ぎ、企業を脅威から守ります。

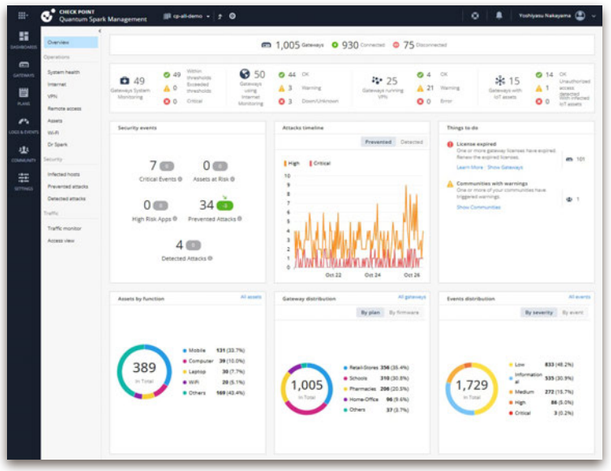
URLベースのリアルタイム・フィッシング防御

URLの特徴を分析します。
機械学習により危険と判定されたURLは
即座にブロックされます。

ブラウザ内でのゼロフィッシング対策

ブラウザに読み込まれるWEBページをスキャンします。
AIがクラウド上で分析し、フィッシングのリスクがある場合は
即座にアクセスをブロックします。

Spark Management



Quantum Spark™

クラウド型の管理ポータルから、複数拠点や機器を一括で運用!!

拠点追加やポリシー変更も遠隔で簡単に行えるため、
運用負荷を大きく削減します。
現地作業や高度な専門知識が不要になることで、
運用コストの低減とトラブル対応の迅速化を実現し
限られたITリソースでも安心してセキュリティを
維持できます。

レポートと運用支援で、セキュリティを“守る”から“活かす”へ

企業のセキュリティは、もはや「守るだけ」では不十分です。
Quantum Sparkシリーズは、脅威や通信状況を可視化するレポート機能と、運用負荷を軽減する
マネージドサービスにより、セキュリティを“守る仕組み”から“成長を支える戦略”へと進化させます。
「見える化」と「任せられる環境」によって、限られた人員でも最適な対策と柔軟な運用が可能になります。

レポート機能について

シンプルで直感的な日本語レポートを標準提供

1. 脅威の検出状況
2. 帯域を消費している上位のカテゴリ、サイト、ユーザの表示と詳細データへのリンク
3. 下りと上りそれぞれのトラフィックの帯域消費量
4. アプリケーション別の帯域消費状況
5. アンチボット機能で検出したボットの活動状況
6. 高リスクアプリケーションの利用状況と、高リスクアプリケーションを利用している上位のユーザ

企業が抱える通信環境への悩みも、レポートが解決の糸口に!!

課題	社内ネットワークに接続するスマートフォンやIoT機器が増えたことで、業務通信が不安定に。しかし原因が特定できず、対策も遅れていた。	高速回線を導入しているにもかかわらず、業務システムの応答が遅く、原因の特定が困難だった。	私的なSNSや動画サイトへのアクセスが多く、業務効率の低下や情報漏えいリスクが懸念されていた。	TeamsやZoomなどのクラウドアプリが遅延・切断を起こし、生産性や社内外のコミュニケーションに支障が出ていた。
レポート活用による導入事例	レポート機能により、端末・アプリごとの通信量を可視化し、不要なトラフィックが業務を阻害している実態を明確化。帯域制御とアプリケーション制御の対策を実施し、安定したネットワーク環境を維持している。	通信内容を詳細に可視化したレポートで、不要なバックアップ通信や動画アクセスが原因であることを明確化。URLフィルタリングと帯域制御により業務システムの応答が改善。	URLカテゴリ別アクセスレポートを活用し、私的利用の実態を数値で経営層に提示。アクセス制御ポリシーにより、ネットワーク負荷が軽減し、業務効率が向上。	アプリ別通信量の分析レポートで、非業務トラフィックが帯域を圧迫している原因を特定。Smart Accelによる通信最適化により、オンライン会議の品質が安定し、生産性が向上。

セキュリティ管理の人材や時間をサポートする、マネージドサービス

導入後でも、クラウド上で設定変更が出来ます

- リモートで機器の状態を確認
- 設定の追加・変更をリモートで実施
- メールによるセキュリティレポートを定期配信（月次/週次/日次より選択）
- 障害時、リモートでログを取得し調査が可能

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社について

CHECK POINT

今日までのセキュリティ技術の基盤を提供

1993年イスラエルに設立、FireWall-1と特許取得済みのステートフル・インスペクション技術を開発。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
日本法人設立：1997年　International HQ : Tel Aviv, Israel
105-0001 東京都港区虎ノ門1-2-8 虎ノ門琴平タワー 25F

世界88カ国＋に展開
200社 + テクノロジーパートナー
6,000社 + チャネルパートナー

Quantum Spark™

Solution MAP

安全なネットワーク Quantum

- **Maestro** ハイパースケール データセンター
- **VPN** 仮想プライベート リモートアクセス
- **Force** エンタープライズ ファイアウォール
- **SD-WAN** 最適化された 接続性
- **Spark** SMBスイート
- **Rugged** ICSセキュリティ
- **DDoS プロテクター** ハイパースケール データセンター
- **IoT プロテクト** IoTセキュリティ
- **Smart-1 Cloud** セキュリティ マネジメント

安全なクラウド CloudGuard

- **Network** クラウド ファイアウォール
- **WAF** ウェブアプリケーション ファイアウォール
- **API Security** APIの保護
- **Secure AI** LLMの確保

安全なユーザー&アクセス Harmony

- **Endpoint** エンドポイントの 高度な脅威保護
- **Browse** ウェブブラウザ向け 脅威防御
- **SASE** インターネットアクセス プライベートアクセス
- **Mobile** モバイル 脅威保護
- **Email& collaboration** Emailとコラボレーション ツール保護
- **SaaS** SaaSアプリケーションの 脅威対策

セキュリティ・オペレーション&サービス Check Point Infinity Platform Services

セキュリティオペレーション

- **XDR/XPR** 拡大防御対応
- **Playblocks** オーケストレーション オートメーション
- **Event** イベントの 安全な統合と可視化
- **ERM** 外部リスクの管理と軽減

AIツール

- **Threat Cloud AI** AI駆使の 脅威インテリジェンス
- **AI Copilot** AIによる セキュリティの自動化
- **AI Cloud Protect** AIインフラの保護
- **Gen AI protect** GenAIアプリの セキュリティ

グローバルサービス

- **Assessment and Risks** 脅威とリスクの アセスメント
- **Managed Security** 運用型セキュリティサービス
- **ProfessionalServices** デザイン&デプロイ
- **TrainingPrograms** チームを教育
- **Incident Response** 検出とデジタルフォレンジック