



■商品構成

構成	V80スタンダードモデル 5年/6年タイプ	V80ハイスピードモデル 5年/6年タイプ	V80WスタンダードWi-Fiモデル 5年/6年タイプ
UTM本体 UTM (統合脅威管理) BP-X1CPシリーズ			
導入時設置/設定サービス	○ (導入時)		
ソフトウェアライセンス	5年/6年 ライセンス付属		
ヘルプデスク、UTM監視サービス、 オンサイトハードウェア保守	5年/6年間		
簡易定期レポート (月1回メール配信)	5年/6年間		

■商品価格

商品名	品番	価格
V80スタンダードモデル 5年タイプ	Y9CA35PV	オープン
V80スタンダードモデル 6年タイプ	Y9CA36PV	オープン
V80ハイスピードモデル 5年タイプ	Y9CA55PV	オープン
V80ハイスピードモデル 6年タイプ	Y9CA56PV	オープン
V80WスタンダードWi-Fiモデル 5年タイプ	Y9CA35PW	オープン
V80WスタンダードWi-Fiモデル 6年タイプ	Y9CA36PW	オープン

■主な仕様

モデル	V80スタンダード	V80ハイスピード	V80WスタンダードWi-Fi
ハードウェア			
WAN	10/100/1000Base-T RJ-45ポート × 1		
LANスイッチ	10/100/1000Base-T RJ-45ポート × 5		
Wi-Fiオプション	— (無し)		IEEE802.11 b/g/n/ac MIMO 3x3
無線対応電波帯域	— (無し)		2.4/5GHz ※バンド同時利用不可
スペック※2			
脅威対策スループット	340Mbps	450Mbps	340Mbps
接続数/秒	10,500	14,000	10,500
同時接続数	500,000	500,000	500,000
寸法			
形状	デスクトップ		
寸法 (幅×奥行×高さ)	210 × 160 × 37.5 mm	210 × 160 × 37.5 mm※3	
重量	0.43 kg	0.44 kg※3	

※2: SMB (小規模オフィス) の実環境に近づけたトラフィック (HTTPを含む) と基本的なルール、NAT、ロギングや最新の脅威対策機能をオンにした状態で稼働しています。

※3: アンテナ部を除く。

• Check Point Software Technologies、Check Point、ThreatCloudは、Check Point Software Technologies Ltd.あるいはその関連会社の商標または登録商標です。

• Wi-FiはWi-Fi Allianceの登録商標です。

• その他商品名、会社名およびロゴは各社の登録商標または商標です。

• 製品の仕様は予告なく変更することがあります。

シャープマーケティングジャパン株式会社
ビジネスソリューション社

〒261-8520 千葉県美浜区中瀬1丁目9番2号

■お求めは信用と技術を誇る当店で

このカタログの内容は、2022年4月現在のものです。

SHARP

Be Original.

ICTソリューションシリーズ
UTMソリューション

UTM(統合脅威管理)ソリューション

Unified Threat Management



テレワーク拡大により増大するネットワーク脅威の対策に

SHARP UTM BP-X1CPシリーズ

チェック・ポイント・ソフトウェア・テクノロジーズ社製ベースエンジン採用

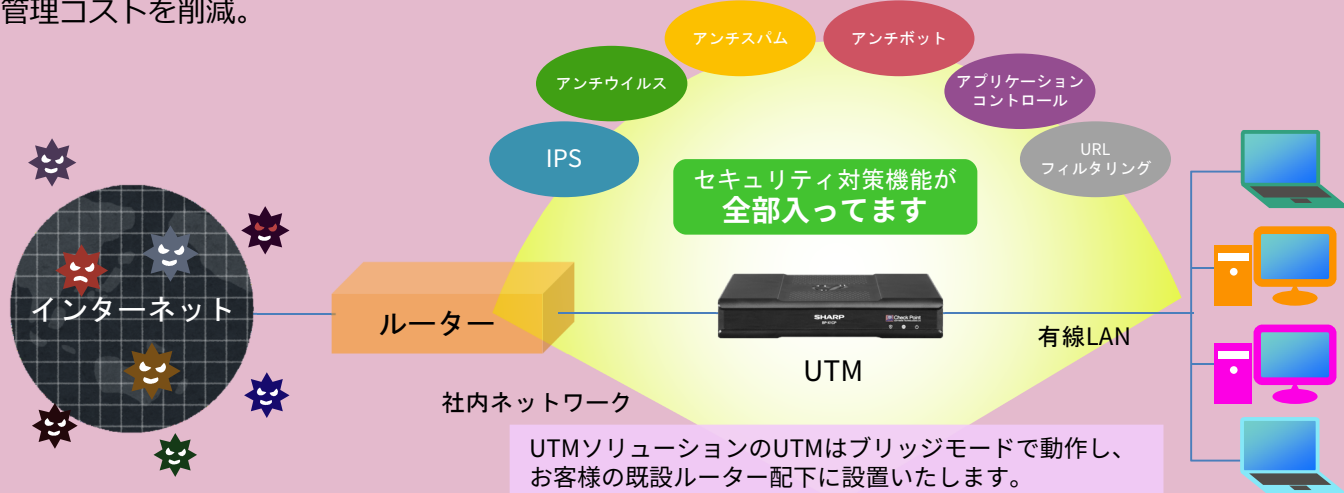
UTM (統合脅威管理) ソリューション

企業のネットワークセキュリティ対策に求められるさまざまな機能を一体化、複数のセキュリティを統合的に管理することでコスト削減と安心・安全を提供します。



■ UTM (統合脅威管理) セキュリティ ■

異なるバラバラなセキュリティ対策機能を1つに統合し運用管理コストを削減。



ポイント1 外部からの脅威を防御

- IPS**
 - 脅威の振る舞いとシグネチャに基づく、数千種類におよぶ外部からの攻撃に対する防御機能を提供します。
- アンチウイルス**
 - 脅威情報配信サービス「ThreatCloud™」から配信されるリアルタイムのウイルス・シグネチャとアノマリ・ベースの検出機能を使用して、マルウェアをゲートウェイで検出し遮断することで、ネットワークの手前でマルウェアを阻止し、パソコンへの影響を防ぐことができます。
- アンチスパム**
 - 送信者のIPレピュテーションをチェックすることにより、スパムやマルウェアを接続レベルでブロックします。
 - 画像を利用したスパムや各国語のスパムなど、最新のスパムパターン・ベースで検出します。
 - メッセージ本文と添付ファイルのスキャンなどにより、多様なウイルスおよびマルウェアをブロックします。

ポイント3 ネットワークの利用を制限

- URLフィルタリング**
 - URLのカテゴリ毎にWebアクセスの許可・禁止・制限の設定ができます。
 - 特定のURLをホワイト・リストとブラック・リストに登録することでポリシーをきめ細かく調整ができます。
- アプリケーションコントロール**
 - 9,700以上のWeb 2.0アプリケーションや約25万のウィジェット*1を識別し、その利用を禁止または制限するきめ細かいポリシーをユーザーやグループごとに容易に作成することが可能になります。

ポイント2 内部からのリスクを軽減

- アンチボット**
 - ボットに感染したパソコンを検出し、ボットと指令 (C&C) サーバと呼ばれる制御システム間の通信を遮断して、被害を予防できます。
-
- ① ボットに感染したパソコンを検知
- ② ボットの通信を遮断
- 社内ネットワーク
- コマンド&コントロール

ポイント4 リアルタイムな防御情報を配信

- ThreatCloud™**
 - 脅威情報配信サービス「ThreatCloud™」は、世界中にあるゲートウェイから収集した情報をもとに、ゲートウェイに対して防御情報をアップデートするクラウドサービスになります。
-
- Check Point ラボでの検証
- マルウェア対策機関からの情報提供
- 世界中にあるゲートウェイから収集した情報
- グローバルな脅威情報をThreatCloud™に反映し、ゲートウェイに自動配信。

*1: 各識別別は、2022年4月時点のCheck Point AppWiki (<https://appwiki.checkpoint.com/appwikisdb/public.htm>) に基づきます。

ポイント5

充実したワンストップサービスで導入後も安心

導入時

設置・設定

専任スタッフにより、お客様のネットワーク環境に合わせた設置・設定を行います。



運用

ヘルプデスク

電話によるお客様からのお問い合わせに、専任のスタッフが対応します。

リモート保守

お客様からのお問い合わせに応じて、軽微な設定変更をお客様ご了解の上、対応します。

オンサイトハードウェア保守

万が一の不具合、ネットワーク利用に関する問い合わせなどに対し、必要に応じて訪問対応します。

監視サービス

ゲートウェイからのログ情報を取得し、稼働状況を監視します。



V80WスタンダードWi-Fiモデルについて

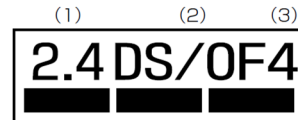
電波干渉に関するご注意

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局 (免許を要する無線局) 及び特定小電力無線局 (免許を要しない無線局) 並びにアマチュア無線局 (免許を要する無線局) が運用されています。

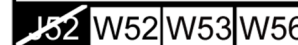
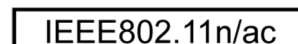
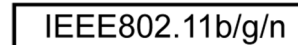
- この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局並びにアマチュア無線局が運用されていないことを確認して下さい。
- 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、お買い上げの販売店にご連絡頂き、混信回避のための処置等 (例えば、パーティションの設置など) についてご相談して下さい。
- その他、この機器から移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して有害な電波干渉の事例が発生した場合など何かお困りのことが起きたときは、お買い上げの販売店へお問い合わせください。

現品表示の意味

本製品と梱包箱には、以下に示す現品表示が記載されています。



- 2.4 : 2.4GHz帯で使用する無線設備を表しています。
- DS/OF : 変調方式がDSSS方式およびOFDM方式であることを示しています。
- 4 : 想定される与干渉距離が40m以下であることを示しています。
- : 2,400MHz ~ 2,483.5MHz の全帯域を使用し、かつ移動体識別装置の帯域を回避可能であることを意味しています。



- 5GHz帯 (IEEE802.11n/ac) で使用するチャンネルは、36, 40, 44, 48ch (W52) と 52, 56, 60, 64ch (W53) と 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140ch (W56) です。
- W52 (5.2GHz帯/36, 40, 44, 48ch), W53 (5.3GHz帯/52, 56, 60, 64ch), W56 (5.6GHz帯/100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140ch) が利用できます。

本製品は、ご購入の国または地域外では使えません。無線LANで使用できるチャンネル・周波数は国や地域により異なります。

無線通信に関するご注意

本機は2.4GHz帯または5GHz帯の無線通信を行っています。
 ・本製品には、電波法に基づく小電力データ通信システムの無線局として、工事設計認証を受けた無線設備を内蔵しています。本製品を使用するときに無線局の免許は必要ありません。また、日本国内のみ使用できます。
 ・本製品は、工事設計認証を受けていますので、分解/改造をすると法律で罰せられることがあります。
 ・電波法により5.2GHz帯(W52)、5.3GHz帯(W53)は屋外利用禁止です。(法令により許可された場合を除く)
 ・製品および付属品の不正な改造、指定以外の代替品等は使用しないでください。製品および付属品の不正な改造、指定以外の代替品等の使用により発生した故障や不具合については、当社は一切その責任を負いませんので、あらかじめご了承ください。

無線LAN製品ご使用時におけるセキュリティに関するご注意

無線LANでは、LANケーブルを使用する代わりに、電波を利用してパソコン等と無線親機間で情報のやり取りを行うため、電波の届く範囲であれば自由にLAN接続が可能であるという利点があります。その反面、電波はある範囲内であれば障害物 (壁等) を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

通信内容を盗み見られる

- 悪意ある第三者が、電波を故意に傍受し、
 - ・IDやパスワード又はクレジットカード番号等の個人情報
 - ・メールの内容
 等の通信内容を盗み見られる可能性があります。

不正に侵入される

- 悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
 - ・個人情報や機密情報を取り出す (情報漏洩)
 - ・特定の人物になりすまして通信し、不正な情報を流す (なりすまし)
 - ・傍受した通信内容を書き換えて発信する (改ざん)
 - ・コンピュータウイルスなどを流し、データやシステムを破壊する (破壊)
 などの行為をされてしまう可能性があります。

本来、無線LAN製品は、セキュリティに関する仕組みを持っていますので、その設定を行って製品を使用することで、上記問題が発生する可能性は少なくなります。セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

なお、無線LANの仕様上、特殊な方法によりセキュリティ設定が破られることもありまますのでご理解の上、ご使用ください。