

製品仕様

	アイテム	UTM-T80
パフォーマンス仕様	FWスループット	2Gbps
	UTMスループット	1Gbps
	接続クライアント数 (推奨)	80
	VPNトンネル	1k
	Max同時接続数	1.2Million
	同時接続数/秒	14k
インターフェース仕様	10 / 100 / 1000M GEポート	6
	USBインターフェース	2
	コンソール	RJ45*1
	消費電力	60W
	電源	AC100~240V 47~63H2
その他 ハードウェア仕様	寸法 (mm)	210.5×210.5×33
	重さ (kg)	1.52
	ラック	Desktop

センドバック保守(無償)

- お使いのUTMの調子が悪い。
- 修理中にUTMがないとウイルスに感染しないか心配。
- コールセンターへ販売店様を通じて連絡。
- 交換機を入手。



ヴィーナステックジャパン株式会社

〒151-0053
東京都渋谷区代々木三丁目25番3号
あいおいニッセイ同和損保新宿ビル12階
TEL.03-4405-4576 FAX.03-5357-1419
<http://www.venustechjapan.com>

製品についてのお問い合わせ

202302

Venustech

Venusense UTM-T80



守ることは、
強くすること。

UTMの導入で、 今すぐ御社のセキュリティレベルを アップしませんか？

うちの会社だけは大丈夫!!
だと思っていないですか？

セキュリティソフトを
パソコンに入れているから
大丈夫

Macを使っているから
大丈夫

個人情報の漏えいなどの
トラブルは一度もないから
大丈夫

パソコンのセキュリティ
設定をしているから
大丈夫

もしかして、御社のネットワークは
サイバー攻撃の脅威に
さらされているかもしれません。

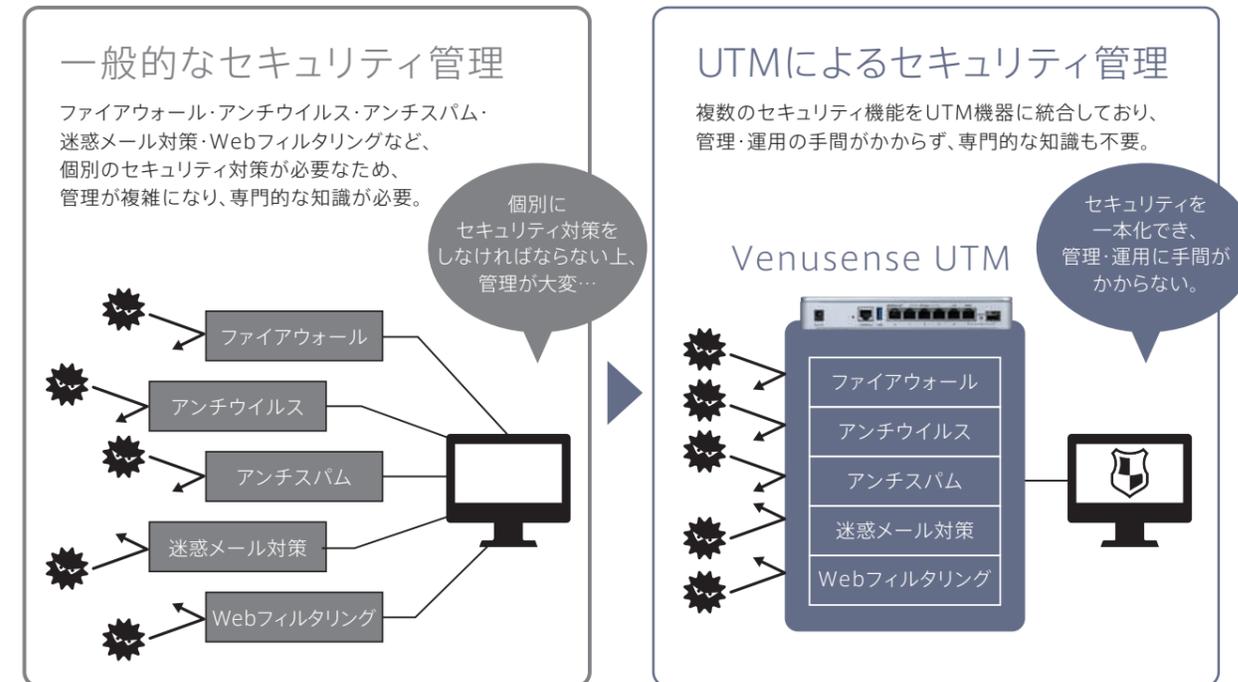
預かった社員の
マイナンバーの漏えい
には罰則規定も…

一定期間の経過後、
突然ウイルスに
変わるものも…

Venusense UTMが、 社内ネットワークを守る。



Venusense UTMは、複数のセキュリティ機能が統合されているため、
これ一台で企業のセキュリティレベルを飛躍的にアップできます。



- 電源ランプ
専用のACアダプタを接続すると
電源が供給されます。
- コンソールポート
工事者の上級メンテナンス用ポート
です。一般的に利用しません。
- USBポート
工事者のメンテナンス用のデータの
アップ・ダウンロードの際に使用します。
- 管理用MGMT
工場出荷状態ではLAN0ポートが
工事者設定用ポートでその他の
ポートは利用できません。
- LAN1~LAN3ポート
端末側と接続するための
ポートです。
- LAN4ポート
PPPoEモードの際に
端末を接続するポートです。
- WANポート
上部ネットワークと
接続をする為のポートです。

UTMがテレワークや出先でも未知の脅威からPCを守る。

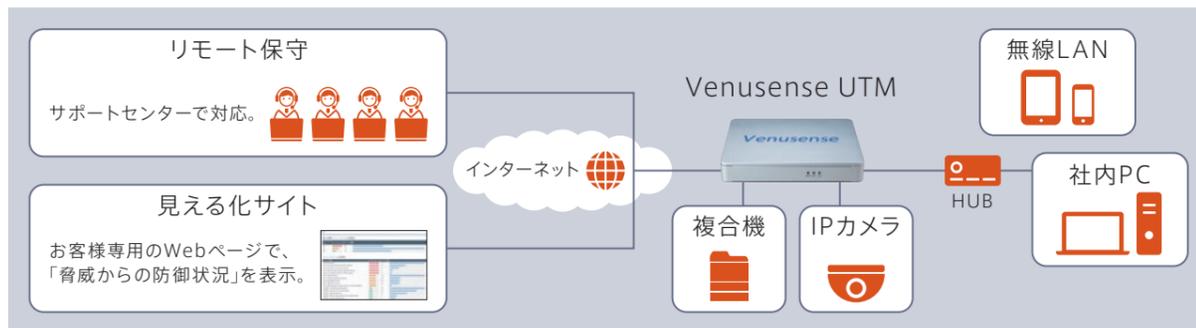


UTM-T80 正面パネル

特長

- さまざまなセキュリティ機能を搭載
- VCloudによりUTMの一元管理を実現
- IPSは業界トップのセキュリティレベルを実現
- 管理・運用の手間がなく、専門知識が不要
- 高いスループット性能があり、快適に使用可能
- 遠隔リモート保守機能搭載

システム構成



主なセキュリティ機能

Firewall

社内ネットワークと外部ネットワークの間で接続を監視。外部からの攻撃を受けた場合は通信を遮断することで、社内ネットワークを保護します。

Anti-Virus

700万を超えるウイルスパターンに対応している、アンチウイルスソフトを採用。ネットワーク上の5種の通信監視をサポートし、感染したファイルを遮断します。

Anti-Spam

無差別に送られてくる迷惑メールを検知。同一のメールサーバーから送られるメールを制御するほか、差出人認証、宛先認証などの技術でスパムを防止します。

URL Filter

情報漏えいや不正アクセスなどの危険が高いWebサイトへのアクセスを制限。日々更新されるブラックリストに基づき、自動的にアクセスを制限します。

VPN

共有ネットワーク上にプライベートネットワーク（仮想的な専用線）を構築する際、ネットワーク間のデータ通信を暗号化。データ改ざんや情報漏えいを防ぎます。

Log&Report

専用サーバーからフィルタリングの結果を吸い上げて分析。攻撃内容やユーザーの閲覧状況についてレポートを作成するなど、セキュリティ評価と強化を支援します。

SSL VPN

webブラウザさえあれば通信可能なリモートアクセスVPNのことです。VPN接続をする2点間をSSL暗号通信でつなぎます。

SD-WAN

複数のWAN回線をアクティブ回線として有効に利用するハイブリッドWAN技術により、柔軟なトラフィック制御を可能とします。

VenusEye ※オプションになります。

サイバー攻撃からの脅威を、24時間365日、監視、分析、検知し、新たなウイルスの情報を更新します。

UTMのパフォーマンス維持が可能

世界中から収集した脅威データをクラウド上で分析処理をすることで、UTM側での処理は行いません。従って、ネットワーク処理の遅れやPCメモリへの影響はございません。



ウイルス定義を
24h更新



お客様側ネットワーク

VenusEyeで日々収集されるデータ

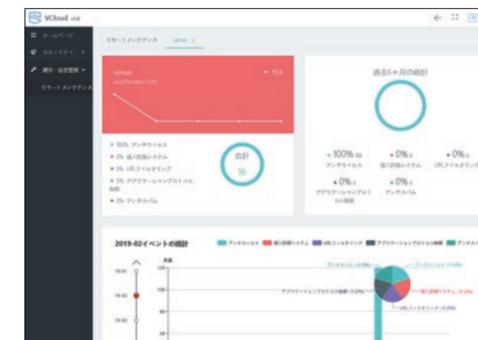


- ドメイン
 - URL
 - ファイルHASH値
 - データファイル
- 等の新たな脅威データを24時間リアルタイムで収集・監視・分析・処理

日々作られる新種の脅威を高速検知しUTMの遮断率を高めます。

VCloud ※オプションになります。

運用管理からウイルス等の攻撃や防御情報を可視化。リアルタイムで確認できるサービスです。



UTMのセキュリティ機能

ウイルスなどの攻撃や防御情報を可視化。セキュリティに関わる様々な対策内容の結果について、リアルタイムで確認できるサービス

V SERIES ※オプションになります。

UTMのセキュリティ機能に加え、各PCへのセキュリティ機能を付け加えました。
また、PCの操作ログを記録することにより、社内の情報漏洩防止が可能となります。

**エンドポイントセキュリティ
20ライセンス 5・6・7年対応**

1. VI 集中管理機能

[ユーザ情報]

各PCでのスキャン状況やDB更新状況の一元管理が可能。PCの資産管理としても活用可能。

2020年1月にMicrosoftサポートが切れたWindows7は台数を把握しておかないと。

[ポリシー作成]

部署や役職毎にセキュリティレベルを設定可能。

P2Pやメッセージ、Web利用中に突然表示される「偽セキュリティソフト」との通信もブロック。

2. VI 集中管理機能

各PCでのスキャン状況やDB更新状況の一元管理が可能。
部署や役職毎にセキュリティレベルを設定可能。



3. VII 内部統制・業務管理システム

PC操作ログ

内部からの情報漏洩の抑止・防止対策は中小企業事業者でも必須！
内部不正をさせない管理・監視体制を！

- PC操作ログを長期保存 → 情報漏えい対策
- データ持出しを記録 → 情報漏えい抑止
- PC業務を管理 → 業務改善・残業縮小

毎日のPCの操作をログとして記録し、管理者にメールで通知します。



時間帯毎のパソコンの作業内容の詳細が確認できます

パワーポイントで営業資料を作成している。

業務中に「Facebook」？ 業務内容をアップしているかも？

業務に関係無いサイトを見ている！！

同じ作業内容を時系列で表示

4. 無料ウイルス駆除サービス

万が一ウイルスに感染した場合には、PCに対しリモートでウイルス駆除をサポートします。

