

サービスの特長

NET JOE Basicのような製品はUTM（Unified Threat Management）と呼ばれています。UTMの特徴はウィルス検知、侵入検知、Web脅威検知を回線を丸ごと包括処理する仕組であり、拠点単位でのサイバーセキュリティ対策に最適なサービスとなります。

PCなどにインストールされているアンチウイルスソフトや、OSに付属するファイアウォールなど、従来の端末毎セキュリティ機能と異なるのは、端末ではなくネットワーク全体を保護できる点にあります。そのため、IOT機器などの従来型セキュリティでは保護するのが難しかった部分までカバーすることができるのです。

LAN全体を低コストで守る	PC、タブレット、オフィス機器、監視カメラなど、ネットワーク内の機器すべてのセキュリティがこの1台で完結。導入や運用コストを低く抑えられます。
コンパクトで強力なUTM	ファイアウォール、アンチウイルス、IPSをはじめ、複数の強力なインターネットセキュリティ機能を手のひらサイズにまとめた先進UTMです。
ルーターにつなぐだけ	特別な設置工事も専門知識も不要。在宅勤務や出張でも手軽に持ち運んですぐに設置できます。※初期設置調整は1次販売代理店が行います。
常に、最新の対策	自動的にアップデートを行い、最新のウィルス定義に更新。日々変化する攻撃に追従する対策機能を提供します。
高速スキャン	攻撃スキャンのスループット約700Mbpsという高いパフォーマンス。従来のUTMにありがちな速度遅延を抑え、業務にストレスを与えません。

※本サービスはすでに国内5000社/団体様にご利用いただいております。国交省運輸安全委員会においても導入いただいております。
※万一に備えたサイバー保険付き商品もございます。詳細はお問い合わせください。

製品仕様

コンパクトな本体に、強力なセキュリティ攻撃対策を実装したハードウェアです

商品名	AIR Wolf NET JOE Basic		
ハードウェア	CPU : Qualcomm IPQ4018, ARMv7 4コア, 716MHz	ネットワークプロテクション	ファイアウォール
	Memory : 256MB		侵入防御 (IPS)
	Flash : 512MB		侵入検知 (IDS)
イーサネット	WAN x 1ポート、LAN x 1ポート	Web脅威対策	URLフィルタリング
			アンチフィッシング
			Webアンチウイルス
接続可能端末台数	無制限	アンチウイルス、アンチマルウェア	Windowsファイル共有 (CIFS)
セキュリティ性能	約700Mbps以上 (脅威保護スループット*)		ファイル共有 (FTP)
電源	ユニバーサルスイッチング電源アダプタ 100-240V AC IN, 12V DC		暗号化されていない圧縮ファイル (ZIP/GZIP/RAR)
サイズ (mm)	幅116 x 高さ25 x 奥行91	(管理機能) ログ	各サービスのログ取得
重量 (g)	135	(管理機能) 自動アップデート	アンチウイルスパターンファイル
			Webフィルタリング

脅威保護スループット* ファイアウォール、アンチウイルスおよびIPSを有効にして、メーカー試験環境にて測定。
※契約期間内に万が一故障があった場合は無償で交換いたします。無償交換は、同等以上の仕様の商品を提供する場合があります。

サービス価格

※基本的に5年間、60回払いのサービスご利用契約となります。初期費用（ハード料金）及び初期設置調整を含んだ月額サービス料金は1万円弱となります。業種毎の詳細資料がございます。販売代理店からご説明させていただきます。
UTMサービスにありがちな、運用料金やメンテナンス費用などの追加費用は一切発生いたしません。
詳細なサービス料金は販売代理店にお問い合わせください。

日々脅威が増すサイバー攻撃 絶対に漏洩してはいけない情報があります

サイバー攻撃は多様化し、大企業だけではなくあらゆる事業者がターゲットに。
対策すべきセキュリティレベルは今や
最新で最大強度のものが求められています。

しかしながらセキュリティ強化には大きな費用と管理の手間を要します。
中小事業所に必要とされるのは、運用管理不要&安価でありながら、
サイバー攻撃から最高レベルで事業者様を守るサービスです。

情報漏洩の際に失うものは 金銭だけではなくそれまでに培った 信用や信頼といった事業継続の根幹です



中小事業者様の事業所に
サイバー攻撃の脅威に対し
最大限のセキュリティを

ネットワークの入り口で
脅威をシャットアウト!!

最新且つ最強のUTM



AIR Wolf NET JOE Basic



製造

IP Dream

※AIR Wolf NET JOE Basicは、株式会社IP DREAMの商標です。

1次販売代理店



代表的なサイバー攻撃の例



サイバー攻撃は日々変化していて、一部を対策しても、被害を完全に防ぐことは困難です。

▼ 以下は現在多くの中小事業所が行っている対策。

感染させない、感染を広げない
サイバー攻撃を防ぐ4つのアプローチ

1. 情報機器

情報機器のセキュリティを最新に保つ

情報機器にセキュリティソフトを導入し、マルウェア感染を防ぎます。日々変化するマルウェアに対抗するため、常に最新バージョンを保ちます。

2. ネットワーク

セキュアなネットワークを構築する

不正アクセスを防ぐ手段として、IDS、IPS、ファイアウォールなどを導入して、信頼できる通信のみを許可します。

3. 従業員教育

セキュリティ・リテラシーを向上させる

標的型メールや、フィッシングサイトによる攻撃に騙されないように、従業員のリテラシー教育を行います。

4. 情報管理

機器、ソフトの状況を管理する。

利用している情報機器、ソフトウェア、マルウェア対策ソフトの定義ファイルの状況を管理します。

しかし、これだけ多くの対策を徹底するには費用も過大となり、管理運用も簡単ではありません。

小・中規模拠点向けセキュリティ・ゲートウェイ
AIR Wolf NET JOE Basic
この1台でサイバー攻撃を撃退！



典型的な攻撃パターンを検知するコアテクノロジー
ディープ・パケット インスペクション

- 1 ウイルス検知** ウイルスを検知して、ブロック・破棄します。
- 2 侵入検知** ボットネット、ドメインハイジャック、ランサムウェア感染などのネットワーク侵入を検知して、ブロックします。
- 3 Web脅威検知** フィッシング、マルウェア、インジェクションなどの悪意のあるWeb脅威を検知して、ブロックします。

- セキュリティープログラムは、常に全世界の最新の脅威に対応し、自動的に更新されます。
- PC端末等（エンドポイント）の既存セキュリティソフトは併用してください。
- 極めて低いハードウェアの故障率。5年使用においても故障率1%未満。故障時は無償対応。
- 回線丸ごと漏れなく防御するので、ネットワーク接続のプリンタや複合機などのIOT機器も防御。
※近年はIOT機器のセキュリティリスクが注目されています。

製造パートナー：Lionic Corporation（台湾）
DPIシリコンIP、DPIベースのコンテンツ管理ソフトウェアエンジン、DPIシグネチャの開発を続けています。
米国、ヨーロッパ、台湾、中国で特許を取得しています。Cisco、NEC、Razerなどのグローバル企業がこのテクノロジーが採用されています。

事業所のネットワークの入り口に設置するだけで、事務所内の情報機器をワンストップでサイバー攻撃から守ります。

事業所のネットワーク接続イメージ

事業所への導入はかんたん。事業所のルーターにつなぐだけ。面倒な管理運用は一切ありません。



- ✓ 設置工事不要
- ✓ 初期設定不要
- ✓ 専門知識不要
- ✓ 設置後即座に稼働

- ・全世界の最新脅威をリアルタイム更新
- ・24時間365日、最新のセキュリティをリモート更新。
- ・ネット回線の入り口ですべての脅威を撃退。
- ・稼働状況は専用アプリで一目瞭然！