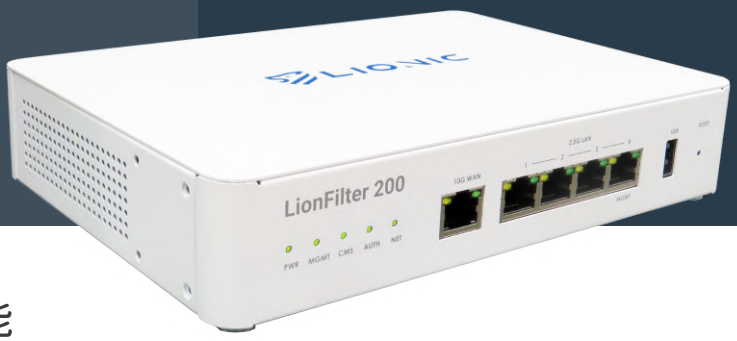
LionFilter 200

Next-Generation Firewall

- 10G WANポートと4つの2.5G LANポートのハイスピードネットワーク
- 企業向けのセキュリティ：アンチウイルス、不正侵入防止、Web脅威防止、DoS攻撃の検知とネットワーク行動管理
- 最新のウィルスデータベースを使用し、AI技術でゼロデイ攻撃に対し、リアルタイム保護を提供
- IPSec Site-to-Site VPNを搭載し、Site-to-Site VPNを提供
- 低遅延保護モードはネットワークの安定性とセキュリティを両立
- 中央管理システム (CMS)で、効果的に複数のLionFilter 200を管理



機能

ハイスピードネットワークの内容検知

LionFilter 200は、10G WANポートと4つの2.5G LANポートを搭載し、高速な通信を実現します。特許を取得し、市場で認められたディープパケットインスペクション（DPI）技術を採用し、アンチウイルス、不正侵入防止、Web脅威防止、ジオブロック、アンチスパム、ファイアウォール、およびSSL/TLS検知など、企業向けの包括的なネットワークセキュリティ機能を提供します。これにより、あらゆる環境下でウイルスを駆除し、悪意のあるコンテンツや攻撃を効果的に阻止できます。

AIでセキュリテ強化

クラウドAIエンジンにより、ゼロデイ攻撃や未知のウイルス、さらには動的に変化する悪意のあるサイトやフィッシングサイトを検知できます。また、マルウェアやボットネットによる攻撃を防止します。

IPSec Site-to-Site VPN, WireGuard Client-to-Site VPN

IPSecとWireGuardのプロトコルを搭載し、Site-to-Site VPNおよびClient-to-Site VPNを提供します。社内だけでなく社外でもセキュアな環境を実現し、情報漏洩やデータ破壊を防止します。

ネットワーク行動管理とスマートQoS

LionFilter 200は指定されるIPアドレス範囲内の装置に実行されるアプリケーションを制御でき、Webサイトのカテゴリでアクセス許可/拒否にします。なお、装置のトラフィックを監視、統計し、スマートQosを行います。

低遅延保護モードはネットワークの安定性とセキュリティを両立

ネットワーク遅延に極めて敏感な環境において、低遅延保護モードはパケットをリアルタイムで複製・スキャンし、脅威をブロックします。既存の接続に影響を与えることなくネットワーク遅延を抑え、迅速な対応とリアルタイムなデータ処理を実現し、システムの安定した運用を確保します。

複数の設備をリモートで管理できる中央管理システムをサポート

管理者は中央管理システム(CMS)で、複数の設備を監視できます。そして、シグネチャ更新、ライセンス管理*、ファームウェアを更新など行えます。

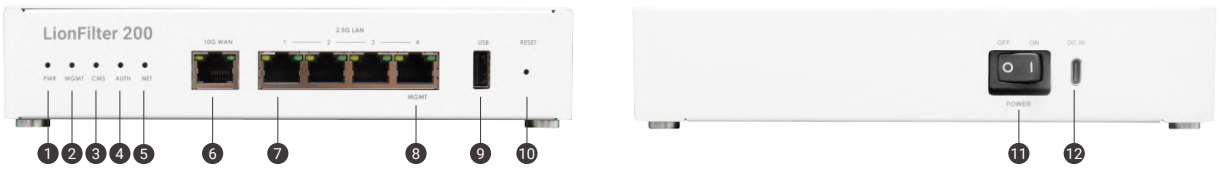
* シグネチャの更新とクラウドAI機能はライセンスが必要です。

パフォーマンス

機能有効化	
スループット(全セキュリテ機能有効化)	*4 Gbps*
同時セッション数	*500K*

全セキュリテ機能有効化: アンチウィルスと不正侵入防止とWeb 脅威防止を有効にします

外観・各部名称



1 電源
2 MGMT(マネジメント)
3 CMS
4 ライセンス
5 インターネット
6 WANポート
7 8 LANポート(1-4)
8 マネジメントポート
9 USBポート
10 リセット
11 電源スイッチ
12 DC電源入力

仕様

商品名	LionFilter 200
ハードウェア	RAM : 2GB
	Flash : 4GB
	WAN : 1 x RJ45 (10 Gbps)
	LAN : 4 x RJ45 (2.5 Gbps, 1 of them can configure as MGMT Port)
インジケーターランプ	PWR, MGMT, CMS, AUTH, NET
電源	Type C DC 12V / 2A
温度範囲 耐久性	0~40°C
寸法	210 W x 40 H x 150 D (mm)
認証	VCCI/BSMI/CE/FCC

機能リスト

セキュリティ

産業向けインターネットセキュリティ技術

- FTP、HTTP、SMB など一般的なプロトコルでのウイルス検出。
- ハイブリッド ウイルス スキャン
- ウイルスファイル破壊
- 実行ファイルのスキャン
- オフィスドキュメントのスキャン
- 圧縮ファイルのスキャン
- メールと添付ファイルのスキャン
- ランサムウェア検知機能
- トロイの木馬検知機能
- クラウドウィルススキャン
- サイバー攻撃ブロック
- 総当たり攻撃の検知
- ポートスキャンの検知
- DoS攻撃の検知
- プロトコル異常動作の検出
- Server Message Block (SMB)の不正侵入防止
- ボットネット攻撃検出
- 仮想パッチの即時更新
- 安全ではないwebサイトにアクセスをブロック
- ドメイン名チェック
- URLチェック
- IPv4およびIPv6チェック
- メール内容の悪質サイトを検知
- 悪質・フィッシングサイトのクラウドデータベース
- カスタマイズワイトリスト
- 攻撃源の分析とジオブロック
- TCPとUDPプロトコルに対応カスタマイズのファイアウォール
- ファイアウォールルールのスケジュール
- 許可/拒否するwebサイトリスト
- 検出した脅威の詳細情報リスト
- 脅威ログをエクスポート(CSV形式)
- 不正侵入のオンラインThreatpediaを提供
- 外部の悪質・フィッシングサイトデータベースを使用できる
- AIで動的に変化する悪意のあるサイトやフィッシングサイトを検知
- AIでゼロデイ攻撃や未知のウイルスを検知
- リアルタイムの保護モード
- 低遅延の保護モード

ネットワーク構成

既存のネットワーク構成にシームレスに統合

- デフォルトで簡単に導入できるブリッジモード
- DHCPサーバとポート転送機能を搭載するルーターモード
- スマホなどの移動端末はVPNで保護を受けられる
- VLANをサポート
- カスタマイズのProxyサーバでLionicクラウドサービスをアクセスできる
- 静的ルート設定とNATのアドバンス設定
- カスタマイズのDHCP設定
- Site-to-Site VPN(IPSec)

ネットワーク管理

ネットワーク行動管理とスマートQoS

- スマートQoS
- トラフィックの監視、管理
- 装置の認識と管理
- Webサイト内容の分類と管理
- アプリケーションの認識と管理

監視管理

進化しているセキュリテ

- 直感的なユーザーインターフェース
- DDNSをサポート
- リモート管理者のアクセス権限管理
- 暗号化された接続で安全なアクセスを実現
- VPNサーバーへのアクセスに2要素認証
- 検査済みトラフィックの概要
- 検出した脅威の統計情報
- システムリソースを監視
- Lionicクラウドサービスのライセンス管理
- 自動的サマリーレポートを作成
- システム負荷の自己診断
- ネットワークセキュリティリスク評価
- セキュリテポリシーとシステム設定の保存と復元
- システム再起動のスケジュール
- システムユーザーのアクティビティ
- ファームウェアとシグネチャの自動更新
- ユーザー定義によるシスログサーバーを設定、詳細なシステム状態を収集
- カスタマイズNTPサーバー設定
- 脅威検知通知メール
- ネットワーク診断ツール
- システムログのエクスポート
- SNMPでシステム稼働状況を監視
- 専用のMGMT Port

中央管理システム

有効的なリモート管理システム

- 動作状況のサマリーをビジュアル化
- ダッシュボードで防御の状態が見える
- リモートで装置を設定できる
- 装置のグループのセキュリテポリシーを作る、適用する
- 脅威ログをエクスポート(CSV形式)
- シグネチャの更新
- リモートでファームウェアを更新
- 脅威検知通知メール
- システムユーザーのアクティビティ履歴
- システムユーザの権限管理
- バッチで複数の装置をコントロール
- リモートでシステムログをエクスポート
- リモートでライセンスをバッチ処理する

LionFilter 200
安全なネットワーク環境を実現します

LIONIC
Security Solution Provider

連絡窓口
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com

Lionic Corp.
https://www.lionic.com/
1F-C6, No.1, Lising 1st Rd.,
Science-Based Industrial Park,
Hsinchu City 300, Taiwan, R.O.C.