

Web GUI マニュアル LionFilter 200

バージョン 1.0 更新日付 2025/05





LionFilter 200 マニュアル

版權聲明

Copyright © 2025, Lionic Corp.; all rights reserved.

商標

LIONIC は Lionic Corp. の商標です。 WireGuard は Jason A. Donenfeld の商標です. No-IP は Vitalwerks Internet Solutions, LLC の商標です。

Disclaimer

鴻璟科技は、本マニュアルに記載された製品や手順について、新規追加または変更を行う権利を留保し、正確な情報を提供することを目的としています。本マニュアルには、予期せぬ印刷ミスが含まれる可能性があるため、そのようなエラーを修正するために定期的に情報を変更する場合があります。

Technical Support Lionic Corporation

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



目次

管理画面にログイン	
概要	6
ダッシュボード	8
WAN	
ネットワークの設定	
リモートコントロール	
LAN	
接続モード	
LAN	
DHCP	
ポート転送	
静的ルート設定	
セキュリティ機能	
全般	
アンチウイルス、不正侵入防止、マルウェアサイト防止	
ジオブロック	22
アンチスパム	
ファイアウォール	23
例外サイト	25
SSL/TLS 検知	
脅威ログ	28
資産管理	
トラフィック	
トラフィックモニター	
QoS	
行動管理	
ポリシー	34
ジオブロック	
イベント	



VPN $\forall - n - \dots$	37
WireGuard VPN	
IPSEC SITE-TO-SITE VPN	
システム	41
デバイス	41
サーバー	43
通知	46
ファームウェア更新	47
設定値の保存と復元	
パスワードの変更	49
管理の履歴	
サマリーレポート	51
ユーティリティ	52



4.

管理画面にログイン

- 1. LionFilter 200 を電源に接続して、電源スイッチを ON にしてください。
- LionFilter 200 の WAN ポートと ISP から提供されたルーターの LAN ポートをイーサ ネットケーブルで接続してください。
- LionFilter 200 のマネジメントポート(MGMT)とパソコンまたはノートパソコンをイ ーサネットケーブルで接続してください。DHCP で自動的にパソコンまたはノートパ ソコンに IP アドレスを割り当てます。
 - LionFilter 200 LionFilter 200 modem / router / switch 安徳方法
- 5. IP アドレスを取得した後、パソコンまたはノートパソコンにてウェブブラウザを開いて、https://myfilter.lionic.com/にアクセスしてください。

	LionFilter 200へようこそ	
LionFilter 200 ウィルス、不正侵入、マルウェアサイトから ネットワークを守る	ログイン パスワードでサインイン パスワード	*
バージョン 25.6.2	ログイン	

ログインページ



- 6. ログインのデフォールトのパスワードはデバイスの裏側に記載されている S/N 番号 です。
- ログインした後、[WAN]のページで LionFilter 200 のネットワーク設定をしてください。

LIONIC Security Solution Provider			● 日本語 →
LionFilter 200	WAN		
コ ダッシュボード	ネットワークの設定 リモートコントロール		
🕀 WAN			
# LAN	IPv4 設定		
セキュリティ			
当 セキュリティ機能	接続設定	Auto	^
● 脅威ログ	DNS	Auto	
ネットワーク管理		固定設定	
8 資産管理		PPPoE	
III トラフィック	IPv6 設定		
▲ 行動管理	接続設定	Auto	~
アドバンス設定	DNS	例: 2001:4860:4860::8888	

WAN-ネットワークの設定

- * 付記:設定完了後、マネジメントポートを LAN ポートとして使用する場合、[システム] >[デバイス] のページでマネジメントポートを無効にしてください
- 最新のウイルス、侵入、フィッシング、詐欺検出および防止機能を利用するために、 ライセンスキー(アクティベートコード)を購入し、インターネットに接続されてい る状態で、[システム] > [デバイス] > [アクティベートコード]のフィールドに入力し、 「アクティベートする」をクリックすると、ライセンスが有効になります。
- * 付記:アクティベートコードは、半角英数字 20 文字で構成されています。適用に成功すると、ライ センスが有効になります。アクティベートコードが無い場合やアクティベートできない場合、ご購入 の窓口にご連絡ください。



概要

ダッシュボード:

[ダッシュボード]では LionFilter 200 のシステム情報と装置情報が表示されます。

「検査統計情報」、「脅威の事象情報」、「ステータス」、「装置情報」などが含まれま す。

WAN:

[WAN] では LionFilter 200 の外部接続が設定できます。

WAN IP アドレスの自動取得、固定設定、PPPoE の設定などです。

LAN :

[LAN] では LionFilter 200 の接続モードが設定できます。デフォールトの[ブリッジモード] から[ルーターモード]に変更すると、DHCP IP 予約、ポート転送と静的ルートが設定できます。

セキュリティ:

- **セキュリティ機能:**アンチウイルス、不正侵入防止、マルウェアサイト防止、ファ イアウォールの各セキュリティ機能のポリシーが設定できます。
- **脅威ログ**:各セキュリティ機能の脅威事象のログが表示されます。

網路管理:

- 資産管理: 資産管理の機能は LAN 側の装置を認識し、特定の資産のネットワークア クセスを許可または拒否にします。
- トラフィック:各LAN 端末のトラフィック使用量を一覧表示し、帯域幅の管理を行うことができます。
- 行動管理:特定なコンテンツ、またはアプリケーションを管理できます。

アドバンス設定:



- VPN: LionFilter 200 はモバイル端末までも保護できます。
 VPN 機能を起動すると、モバイル端末が安全なネットワークを経由し、セキュリティが強化されます。
- システム:こちらではシステム設定の変更ができます。
 ライセンス管理、外部サーバーの設定、ファームウェア更新や設定値の保存と復元、
 管理履歴などが含まれます。
- ユーティリティ:こちらではトラブルシューティングツールを提供します。
 ネットワークツール、コマンドラインツール、システムログの書き出しなどです。

7



ダッシュボード

LionFilter 200 のシステム情報と装置情報をこのページで表示します。 「検査統計情報」、「脅威の事象情報」、「ステータス」、「装置情報」な どが含まれます。

		◎ 日本語 +
ionFilter 200	検査統計情報 起動からの検査数	
■ ダッシュボード		
⊕ wan	【 個のファイル グ 8/9 個のURL	IK 本のフロー ISK 個のパケット
∺ LAN		
セキュリティ	セキュリティ	脅威事件ランキング 全部 〜
🗎 セキュリティ機能		
● 骨威ログ	アンチウィルス ステータス 〇	シグネチャID 種類 数量 メッセージ
ネットワーク管理	0 検知された骨威事件 アクション 無効化	8060000101 Intrusion 11 TCP SYN Port Scan Lvl: 10 ports within 30 seconds
資産管理		8401714009 Intrusion 2 SQL SQL Injection
・11 トラフィック		
1 1 行動管理		8401/10001 intrusion 2 SERVER Joomia D1 Register SQL injection attack
アドバンス設定	Web 脅威防止	8100027101 Intrusion 2 SERVER-WEBAPP Joomla DT Register SQL injection at
VPN		100000001003 Web 1 secure.eicar.org
Ф У Х 7 4		
言 ユーティリティ	ジオブロック	
<	▶ 0 検知された脅威事件 ステータス	

ダッシュボード-1

検査統計情報:LionFilter 200 が起動から検査されたファイル数、URL 数、フロー数、 パケット数が表示されます。

セキュリティ:LionFilter 200 が最近検知した脅威事象の数、各セキュリティ機能の ステータスとアクションを表示します。

脅威の数値及びアクションをクリックすると各機能の脅威ログやセキュリティ機能のページに飛びます。

脅威事件ランキング:各セキュリティ機能で検知された脅威ログのすべてや、各種類の検知回数ランキングが表示されます。





ダッシュボード-2

トラフィックモニター:LionFilter 200 を通過したアップロード/ダウンロードの通信 速度とトラフィック量が表示されます。

装置情報:LionFilter 200 のデバイス名(変更できます)、MAC アドレス、ライセンス状況、ファームウェアのバージョン、各セキュリティ機能のシグネチャのバージョンと更新時間、WAN IP アドレス、システム時刻、稼動時間、メモリとストレージ及び CPU の使用率が表示されます。



WAN

ネットワークの設定

このページではネットワーク環境によって、[Auto]、[固定設定]、[PPPoE]の 中から選択し、IPv4 や IPv6 の設定を行うことが出来ます。デフォルトの設定 は[Auto]です。[固定設定]や[PPPoE]を使う場合は、ISP やネットワーク管理 者にお問い合わせください。

LIONIC		
LionFilter 200	🔁 WAN	
ノ ュボード		
N	ネットワークの設定 リモートコントロール	
	10:4 9/章	
71	IPV4 設定	
ュリティ機能	接続設定	固定設定
成ログ	IPアドレス	Auto
ワーク管理		固定設定
管理	サブネットマスク	PPPoE
フィック	デフォルトゲートウェイ	192.168.0.1
的管理	DNS	8.8.8
2		
7 <u>7</u> 4	IPv6 設定	
T Z U T Z	接続設定	Auto
<	DNS	「別: 2001:4860:4868 888

WAN-ネットワークの設定

- Auto:DHCPサーバからIPアドレスを取得します。 DHCPサーバを含むルーターの後ろに配置するのが最適です。
- 固定設定:指定された「IP アドレス」と「サブネットマスク」と「デフォルトゲートウェイ」と「DNS」を入力してください。
- PPPoE: PPPoE: ISP から指定された「ユーザー名」と「パスワード」を入力して ください。
- VLAN: LionFilter 200 が VLAN のネットワークに配置された時、こちらで VLAN ID を入力してください。
- * 付記: PPPoE を使用する場合は、アクセスコントロールリスト (ACL) が原因で LionFilter 200 の管 理画面にアクセスできない可能性が有ります。

これについては、[リモートコントロール]のページの説明をご参照ください。



リモートコントロール

セキュリティ強化の為、プライベート IP アドレスしか LionFilter 200 の管理 画面にアクセスできません。

グローバル IP アドレスからアクセスする場合は予めこのページで設定を行っ てください。

			♥ 日本語 日
LionFilter 200	WAN		
■ ダッシュボード	2	115-1-27-1-0-1	
🕀 WAN	A DIE DE DURACE	9 C - F-12 F-14	
# LAN	ダイナミック	ダイナミックDNSサービスで提供されたホスト名でLionFilterにアクセスする。	
セキュリティ	DNSサービス	有效	
≧ セキュリティ機能	プロバイダ	No-IP (www.no-ip.com)	
● 脅威ログ	ホスト名		
ネットワーク管理			
	1-7-2		
11 トラフィック	パスワード	パスワードを入力してください 😽 適用	
 行動管理			
アドバンス設定	アクセスコント	パブリックIPアドレスでこのウェブユーザインタフェースにアクセスする為に	
VPN	ロールリスト		
¢ >274		有効 + 追加	
言 ユーティリティ		アドバンス設定 >	
		通用	
<			

リモートコントロール-ダイナミック DNS サービス/アクセスコントロールリスト

ダイナミック DNS サービス (DDNS)

LionFilter 200 にはダイナミック DNS (DDNS) クライアントを搭載しています。

先ずダイナミック DNS サービスのプロバイダに登録してください。 そして下記のフィールドに指定された内容を入力してください。

- プロバイダ:プロバイダ*を選択してください(付記1)。
- ホスト名:登録されたホスト名を入力してください。
- ユーザー名:登録されたユーザー名を入力してください。
- パスワード:登録されたパスワードを入力してください。

入力後、[適用]をクリックしてください。そしてダイナミック DNS サービスを有効にして ください。

設定完了後リモートからホスト名で LionFilter 200 の管理画面にアクセスできます(附 註 2)。



- * 付記:
- 1. 現段階は No-IP をサポートします。
- 2. 適用後或いは IP アドレスを変更した際、プロバイダの更新時間がかかりますので、すぐにアクセ スできない可能性が有ります。この場合は少しお待ちください。
- LionFilter 200 はプライベート IP アドレスを使い、ルーター経由でインターネットに接続する場合、ルーターにて DDNS とポート転送 (Port Forwarding)を設定してください。

アクセスコントロールリスト (ACL)

セキュリティ強化のためにプライベート IP アドレスしか LionFilter 200 の管理画面にアク セスできません。グローバル IP アドレスからアクセスする場合、その IP アドレスをアク セスコントロールリスト (ACL) に追加してください。

手順1:[+追加]をクリックします。

手順2:管理画面にアクセスするグローバル IP アドレスを入力します。

手順3:[適用]をクリックします。

· 許可されたプライベート IP しか管理画面にアクセスできません

有効にすると、すべてのプライベート IP アドレスではなく、指定されたプライベート IP アドレス及びサブネットしか管理画面にアクセスできません。管理画面にアクセスするの IP アドレス及びサブネットを追加してください。

グローバル IP アドレスが確認できない場合(例えば、動的 IP アドレスを使う時)、アク セスコントロールリストを無効*にすれば、すべてのグローバル IP アドレスが管理画面に アクセスできます。

* 付記:セキュリティが原因で[アクセスコントロールリスト]を無効にすると、[セキュリティ保護接続] が強制的に使われます。





セキュリティ保護接続

[セキュリティ保護接続]を使うと、HTTPS しか LionFilter 200 の管理画面にアクセスでき ません。なお、[アクセスコントロールリスト]が無効にされると、[セキュリティ保護接続] は強制的に使われます。



LAN

接続モード

LionFilter 200 は二つの接続モードをサポートしています。ネットワークの環境によって選択してください。

LIONIC Security Solution Provider		♥ 日本語
LionFilter 200	H LAN	
ज ダッシュボード	接続モード LAN DHCP ボート転送 静的ルート設定	
🕀 WAN		
∺ LAN		
セキュリティ	接続モード	
≧ セキュリティ機能		
● 脅威ログ		
ネットワーク管理	フリッジモード ルーターモード	
📑 資産管理	「SIDがレンマanice」とおくなし デムやルーターを提供した場合	
ル トラフィック		
土 、行動管理		
アドバンス設定	通用	
🗢 VPN		
<		

LAN-接続モード

- ブリッジモード

[ブリッジモード]では LionFilter 200 はブリッジ接続を提供し、LAN 側の装置には IP を配布しません。このモードは LionFilter 200 のデフォルトの設定です。DHCP サーバを含むルーターの後ろに配置するのが最適です。

- ルーターモード

[ルーターモード]で LionFilter 200 は DHCP サーバとルーターの機能を提供します。 グローバル IP アドレスが一つしかない環境で最適です。

お使いのネットワーク環境に相応しいモードを選択し、[適用]をクリックしてください。 LionFilter 200 は接続モードを変更します。変更している間はネットワークが一時的に切 断され、管理画面に再度ログインする必要があります。



LAN

[ルーターモード]で LAN 側の IP アドレッシングを設定できます。LAN 側の IP アドレスを 入力し、[適用]をクリックすると、DHCP サーバは自動的に指定された範囲内の IP アドレ スを配布します。

LIONIC Security Solution Provider			♥ 日本語 I→
LionFilter 200	# LAN		
■ ダッシュボード	接続モード IAN DHCP ポート転送 静的ルート設定		
⊕ wan			
∺ LAN	IAN IR アドレフの設定		
セキュリティ			
🎽 セキュリティ機能	IP アドレス	10.254.254.254	
● 脅威ログ	サブネットマスク	255.255.255.0/24 🗸	
ネットワーク管理	アドバンス設定 ~		
🚍 資産管理	NAT なしのルーティング		
II トラフィック	有効		
▲ 行動管理	IP アドレス	192.168.1.2	
アドバンス設定	サブネットマスク	255.255.255.0/24 🗸	
C VPN	○ NATなしのルーティングのLANにてDHCPサーバを有効にします		
· · /		適用	

LAN-LAN IP

- NAT なしのルーティング

[ルーターモード]で NAT を使用しない第二のネットワークを設定できます。 第二のネットワークの情報を入力し、[適用]をクリックしてください。



DHCP

[ルーターモード]で、LionFilter 200 は DHCP サーバの機能を提供します。

グローバル IP アドレスが一つしかない環境に於いて、この機能で LAN 側の複数の装置に IP を配布することができます。

LIONIC Security Solution Provider				● 日本語 →
LionFilter 200	H LAN			
■ ダッシュポード	接続モード IAN			
⊕ wan	150% C 1 CON	DIG OF THESE BEION FROM		
∺ LAN		÷		
セキュリティ				
≧ セキュリティ機能	有効			
● 脅威ログ	開始 IP アドレス	10.254.254.1		
ネットワーク管理	終了 IP アドレス	10.254.254.253		
🔗 資産管理				
1 トラフィック				
↓、 行動管理	DHCP IP 予約			+ ルールを追加する
アドバンス設定				
C VPN	MACアドレス	IPアドレス	説明(任意)	
± · · · · · · · · · · · · · · · · ·				通用

LAN-DHCP

DHCP サーバー設定

- 有効:DHCP サーバーのスイッチです。
- 開始 IP アドレスと終了 IP アドレス: DHCP サーバが配布する IP アドレスの範囲を 指定します。

DHCP IP 予約

- 特定のデバイスに固定 IP アドレスを割り当てる必要がある場合は、そのデバイスの MAC アドレスと希望する IP アドレスを入力し、[適用]をクリックしてください。

* 付記:そのデバイスは IP アドレスを更新する必要があるかもしれません。



ポート転送

[ルーターモード]で LionFilter 200 はポート転送機能を提供します。WAN から LAN 側の 装置をアクセスする際、この機能で特定のポート番号宛てに届いたパケットを LAN 側の装 置に転送します。

LIONIC Security Solution Provider		♥ 日本語 I→
LionFilter 200	H LAN	
ज ダッシュポード	接続モード LAN DHCP ポート転送 静的ルート設定	
⊕ wan		
∺ LAN	ポート転送	「「」」「「た冷かする」
セキュリティ	· Toolea	+ 10-10 C ALIAI 9-5
📋 セキュリティ機能	WAN側ボート番号 転送先ボート番号 転送先IPアドレス プロトコル 説明(任音)	
● 脅威ログ		
ネットワーク管理	827 109 192.168.70.215 BOTH V	Û
📑 資産管理		適用
III トラフィック		
1 行動管理		
アドバンス設定		
C VPN		
+ · / <		

LAN-ポート転送

静的ルート設定

[ルーターモード] では、LionFilter 200 は静的ルート機能を提供します。

LIONIC Security Solution Provider				⑦ 日本語 I→
LionFilter 200	H LAN			
■ ダッシュボード	接続モード LAN DHCP	ポート転送 静的ルート設定		
⊕ wan				
H LAN	静的ルート設定 200時期をチェー	1. A + Z		
セキュリティ	HTUSTU I DIAL HEIDHAK (T. T.)	// 90		+ 1-11 210/11 9 5
当 セキュリティ機能	ネットワークアドレス	ネットマスク	ゲートウェイ	インタフェース
ネットワーク管理	172.215.0.0	255.255.0.0	172.215.198.27	LAN V Ü
🚍 資産管理				適用
II トラフィック				

LAN-静的ルート設定



セキュリティ機能

すべてのセキュリティ機能の設定が提供されており、利用目的に応じて保護 内容を調整することができます。

全般

スキャンモード

- リアルタイム保護モード:リアルタイムのパケットスキャンによって即時に脅威を 遮断し、企業、金融機関、医療機関など高いセキュリティが求められる環境に適用 です。リアルタイムで脅威をブロックし、ネットワーク環境の安全を確保します。
- 低遅延保護モード:リアルタイムのパケットミラーリングスキャンにより、元の通信へのネットワーク遅延の影響を最小限に抑えて、スマートファクトリーや自動化生産ラインなど、ネットワーク遅延に非常に敏感な環境に適用です。迅速な対応とリアルタイムデータ処理を実現し、システムの安定運用を確保します。

SMBのディープスキャン: SMB プロトコルを通じて転送されるファイルや不正侵入に対して、完全なスキャンを実施します。

* 付記: [SMB のディープスキャン]を無効にすると、スキャンにかかる時間を短縮できますが、アンチウイ ルスシステムおよび不正侵入防止に対する保護能力が低下します。



セキュリティ機能-全般



アンチウイルス、不正侵入防止、マルウェアサイト防止

LionFilter 200 はディープ・パケット・インスペクション (Deep packet inspection)の独自技術で下記の三つのセキュリティ機能を提供しています。

- **アンチウイルス**:パケットからウイルスを検出し、ウイルスファイルを 無効化します。
- 不正侵入防止:パケットからサイバー攻撃を検出し、ブロックします。
- Web 脅威防止: 悪意があるサイトにアクセスするセッションを検出し、 ブロックします。

[セキュリティ機能]のページで上記の三つのセキュリティ機能を設定できます。

セキュリテ ィ機能	アンチウイルス	不正侵入防止	Web 脅威防止
有効	有効 / 無効	有効 / 無効	有効 / 無効
アクション	ログ / ログとウイルス を無効化する	ログ / ログとブロッ クする	ログ / ログとブロッ クする
アドバンス 設定	- クラウドデータベー スーでスキャンする - AI で未知のウイルス を検知	 総当たり攻撃の防止 プロトコル異常の防止 ポートスキャンと DoS 攻撃の防止 脅威が検出された場合に は PCAP を保持する 	- AI で動的な悪意のあ る URL を検知 - 第三者データーベー ス
ホワイトリ スト	ホワイトリストの一覧 と削除	ホワイトリストの一覧 と削除	ホワイトリストの一覧 と削除



LIONIC Security Solution Provider	◎ 日本語 →
LionFilter 200	■ セキュリティ機能
ज ダッシュポード	全般 アンチウィルス 不正侵入防止 Web 骨震防止 ジオブロック アンチスバム ファイアウォール 例外のURL/IPアドレス SSL / TLS 検知
⊕ WAN	
Ħ LAN	全般
セキュリティ	
📋 セキュリティ機能	有効
● 脅威ログ	アクション ログとウィルスを無効化する(Destroy) ~
ネットワーク管理	
二 資産管理	アドバンス設定
11 トラフィック	クラウドデータベースでスキャンする(未接続)
↓ 行動管理	クラウドデータベースでスキャンすると、より完全な保護を提供できますが、一部のファイルを転送する際の通 信速度に影響します。
アドバンス設定	
C VPN	AIで未知のウィルスを検知
/ <	AIでファイルを分析し、未知のウィルスを検知します。 注意 :この機能は「クラウドデータベースでスキャンする」を有効にして、ライセンス、インターネットのアク セスが必要があります。

セキュリティ機能

- **有効**:各セキュリティ機能のスイッチです。デフォルトは有効です。
- **アクション:**脅威事件が検出された際のアクションです。
 - ログ:脅威事件が[脅威ログ]に記録されます。
 - ログとウイルスを無効化する:脅威事件が[脅威ログ]に記録され、そしてウ イルスファイルを無効化します。
 - ログとブロックする:脅威事件が[脅威ログ]に記録され、そして該当するセッションをブロックします。
- クラウドデータベースでスキャンする:アンチウイルス機能は、ローカルのシグネ チャで照合する他にクラウドデータベースも利用できます。ライセンスの有効期限 内、LionFilter 200 がインターネットに接続できる環境に設置されている場合、こ の機能を有効にすれば完璧な保護を提供します。
- AI で未知のウイルスを検知:この機能を有効にすると、LionFilter 200 のクラウド アンチウイルスは、クエリを受信した際に、近隣の他のサーバー上の複数のアンチ ウイルスエンジンを同時にスキャンします。
- 総当たり攻撃の防止:この機能を有効にすると、LionFilter 200の[不正侵入防止] は、短時間内に集中して失敗したログイン試行を検出できます。発生頻度が警戒値 を超えた場合、LionFilter 200 は、頻度に応じて[脅威ログ]に表示するか、さらに接 続をブロックします。
- プロトコル異常の防止:この機能を有効にすると、LionFilter 200 の[不正侵入防止] は 通信プロトコルの規範に適合しない異常なパケットを検出し、ブロックします。



- ポートスキャンと DoS 攻撃の防止:
 - TCP、TCP ハーフコネクション(ハーフオープン)、UDP、ICMP、SCTP、
 IP プロトコルによる短時間での接続急増に対する DoS 攻撃を防止する。.
 - 大量の異常フォーマットのパケットを送信するデバイスをブロックする。
 - TCP SYN スキャン、TCP RST スキャン、UDP スキャンなどのポートスキャンの試行をブロックする。
- **脅威が検出された場合には PCAP を保持する:**この機能を有効にすると、LionFilter 200は[不正侵入防止]で脅威を検出した際に 脅威と見なされたパケットを保存し、 後続の分析に使用できるようにします。
- AI で動的な悪意のある URL を検知: この機能を有効にすると、LionFilter 200 は接 続先の URL とクラウドデータベースを照合し、人工知能 DGA 検出モデルを使用し て、この URL が DGA によって生成された悪意のある URL かどうかを判定します。
- 第三者データーベース:外部から悪意のあるサイトのリストを導入できます。

LIONIC Security Solution Provider			● 日本語 I→
LionFilter 200	第三者データーベース		
■ ダッシュボード			
🖶 WAN	データーベースのURL	URL	
# LAN	HTTP Basic認証		
セキュリティ		ユーザー名	
セキュリティ機能		パスワード ×	
 ・ ・ ・	更新頻度	時間	逸用
ネットワーク管理			
📑 資産管理	前回の更新日時	2025年5月7日 1:25:08	今すぐ更新する
11 トラフィック	件数	0	
1 行動管理	既存のデータベース	書き出す	
アドパンス設定			
C VPN			
± · -= ·	ホワイトリスト		

Web 脅威防止-アドバンス設定

- ホワイトリスト:過検知が発生した際、この機能で過検知を回避します。
 - ホワイトリストの追加: [脅威ログ]のページで過検知の脅威事件を探し出し、
 [+]をクリックして、ホワイトリストに追加します。
 - ホワイトリストの一覧と削除:こちらで追加されたホワイトリストのルールの一覧表示と削除が行えます。



ジオブロック

設定された国や地域に基づき、該当地域からの攻撃をブロックしたり、情報 がその地域に流出するのを防止します。

LIONIC Security Solution Provider		♥ 日本語	l→
LionFilter 200	■ セキュリティ機能		
■ ダッシュポード	今辺 マンチウノルフ 天正母1歳小 Work 母螺旋小 パナブロック マンチフバル フライマウィール 母校内(の) 加マビルフ	cci / tic tean	
⊕ wan		SSET TES BEAU	
H LAN	۵. ۵.		
セキュリティ	王成		
🍵 セキュリティ機能	このサイトまたは製品には、以下から入手可能なIP2LocationLITEデータが含まれています。https://lite.jp2location.com		
 ・ ・ ・	有効		
ネットワーク管理	ブロックされる国. 地域を選択		
🚍 資産管理			
11 トラフィック	下記の間、地域からの通信をフロック:		
≛ 、行動管理	アジア 中華 人 民 共和国 (CN)		
アドバンス設定			
C VPN	下記の間、地域に送る通信をブロック:		
+ · · - · ·	РУР		
<	中華人民共和国 (CN)		

セキュリティ機能-ジオブロック

手順1:ジオブロックを有効にします。

手順2:
をクリックして、許可/拒否の国や地域を選択します。

手順3:各設定値を入力します。

手順4:[はい]をクリックした後、実行します。

- ホワイトリスト: 拒否された国や地域が例外の IP アドレスを追加できます。

アンチスパム

[アンチスパム]を有効にすると、スキャン結果に基づいて、メールの件名欄には以下のようなラベルが付けられます:

- [Spam]:スパムメール
- [III-URL]:本文に悪意のある URL を含む場合
- [Virus]:添付ファイルにウイルスを含む場合



		♥ 日本語	∣→
LionFilter 200	■ セキュリティ機能		
■ ダッシュボード	全般 アンチウィルス 不正得入防止 Wah 登留防止 ジオブロック アンチスパム ファイアウォール 偏効のURI /Pアドレス	SSI / TIS 樟知	
⊕ wan			
H LAN	今顧		
セキュリティ	±1%		
🎽 セキュリティ機能	[アンチスパム]を有効にすると、スキャン結果に基づいて、メールの件名欄には以下のようなラベルが付けられます:		
	 [spam] :スパムメール [m-uR.] :本文に悪意のあるURLを含む場合 		
ネットワーク管理	 [Virus] : 添付ファイルにウイルスを含む場合 注音: VIAN 無功時のみ使用できます。 		
🚍 資産管理			
III トラフィック			
▲ 行動管理	フィルタリングラベル		
アドバンス設定			
• VPN	適切なレベルでスパムメールをフィルタリングします。同時に、正当な電子メールが過検知されないようにします。		
	() 嚴格		
<	積極的にスパムメールをフィルタリングします。不蕾なメールも含まれます。		

セキュリティ機能-アンチスパム

- フィルタリングラベル:標準/厳格フィルタリングの厳密度を設定します。
- **信頼できる送信者:**完全なメールアドレスまたはドメイン名を入力してください。 (demo@lionic.com & *@lionic.com)。

* 付記:本機能は VLAN 無効時のみ使用できます。

ファイアウォール

LionFilter 200 には上記のセキュリティ機能の他に、基本的なファイアウォールを提供します。



	♥ 日本語	I
LionFilter 200	■ セキュリティ機能	
冨 ダッシュボード	全般 アンチウィルス 不正使入防止 Web 音威防止 ジオブロック アンチスパム ファイアウォール 例外のURL/IPアドレス SSL / TLS 検知	
⊕ wan		
H LAN	有効 () キルールを追加する	
 ● 音威ログ 	名前 有効 ログ プロトコル 送信元P 送信元ボート 宛先P 🗙	
ネットワーク管理	New Rule ANY V 1010.0.9 ANY 1010.82.7	
😑 資産管理	20.5ポート アクション スケージュール 毎週 開始 終了	
III トラフィック		
二、 行動管理	道度	
アドバンス設定		
• VPN		
± ·/ <		

セキュリティ機能-ファイアウォール

手順1:ファイアウォールを有効にします。(デフォルトは有効です)

手順2:[+ルールを追加する]をクリックします。

手順3:各フィールドに入力します。

手順4:[適用]をクリックした後、実行します。

ファイアウォールのフィールドの解説:

- 名前:該当するルールの名前です。
- 有効:該当するルールの有効 / 無効を選択します。
- ログ:該当するルールが検知された後、[脅威ログ]に表示されるかどうかの設定で す。
- プロトコル: TCP / UDP / ICMP/ IPv6-ICMP 或いは ANY (すべてのプロトコル)。
- 送信元 IP、送信元ポート、宛先 IP、宛先ポート:該当するルールの検知条件です。
- アクション:該当するルールのアクションです。(許可 / 拒否)
- スケージュール:該当ルールの有効時間およびスケジュールの設定です。



例外サイト

例外サイトに追加されたサイトとの通信はすべて許可または拒否になります。

LIONIC Security Solution Provider		♥ 日本語	l→
LionFilter 200	■ セキュリティ機能		
■ ダッシュボード	全般 アンチウィルス 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 例外のURL/P7ドレス	SSL / TLS 検知	
⊕ wan			
H LAN			
セキュリティ	許可	ログ 🔵	
i セキュリティ機能		+ 追加	
● 脅威ログ			
ネットワーク管理			
算座管理			
11 トラフィック			
▲【 行動管理】			
<			

セキュリティ機能-例外サイト

手順1:許可または拒否する予定の URL や IP アドレスを入力します。 手順2:[+追加]をクリックした後、実行します。

- **ログ:有効にすると**・ドメイン名或いは IP アドレスがブロックされた場合、[脅威 ログ]に表示されます。

* 付記:

キーワードを入力すると、そのキーワードを含むドメイン名のすべてのサイトがブロックされます。
 例:「abc」と入力した場合、「www.abc.com」や「demo.abcdef.com」などがブロックされます。
 パスをブロックするには、ドメイン名とパスの両方を指定する必要があります。
 例:「www.abc.com/path/」と入力すると、「www.abc.com/path/」以下のすべてのパスおよびファイルがブロックされます。

2. 大型ウェブサイトは複数のサーバからのコンテンツで作成する可能性があります。

この場合はサイトのすべてのサーバを許可や拒否にしないと、アクセスする或いはブロックすることができません。



SSL / TLS 検知

[SSL/TLS 検出]を有効にすると、LionFilter 200 は SSL または TLS で暗号化さ れたパケットを検知し、HTTPS サイトの閲覧時のセキュリティを向上させま す。

* 付記: [SSL/TLS 検出]を有効にすると、ネットワークの通信速度に影響を与える可能性があり、一部のアプリケーションが正常に動作しなくなる場合があります。

LIONIC Security Solution Provider							♥ 日本語	l→
LionFilter 200	🎽 セキュリティ機能							
■ ダッシュボード	全般 アンチウィルス	不正侵入防止 Web 脅威防止	ジオブロック フ	アンチスパム	ファイアウォール	例外のURL/IPアドレス	SSL / TLS 検知	
⊕ WAN								
🗄 LAN	SSL / TLS 検知							
セキュリティ	SSL / TLS検知機能で、HTTPS	サイトにアクセスする際に端末を保	護します。					
📋 セキュリティ機能	注意: SSL / TLS 検知機能を有	T効にするとネットワーク速度が影響	『され、一部のアプリケー	ションも使われませ	せん。VLAN 無効時(Dみ使用できます。		
● 脅威ログ	有効							
ネットワーク管理	HTTPS ポート	443					適用	
📑 資産管理								
川 トラフィック	ホワイトリスト							
1 行動管理	サイトのカテゴリ		<i>ф</i> .	ェブサイトアドし	~~			
アドバンス設定	Finance and Insurance							
C VPN	Health and Medicine							
± · / <		1				/		

セキュリティ機能- SSL/TLS 検知

- **有効**: [SSL/TLS 検出]のスイッチです。デフォルトは無効です。
- **HTTPS ポート**: HTTPS 接続で使用するポートをカスタマイズできます。*・デフォ ルトは 443 です。複数のポートを設定する場合は、半角の「,」で区切ってください。
- ホワイトリスト:ウェブサイトをホワイトリストに追加すると、LionFilter 200 は そのウェブサイトの暗号化されたパケットを検出しなくなります。互換性やプライ バシーの理由で暗号化パケットを検知されたくない場合は、信頼できるウェブサイ トをホワイトリストに追加してください。
 - サイトのカテゴリ:LionFilter 200 は、複数のウェブサイトカテゴリをホワ イトリストのオプションとして提供しています。特定のウェブサイトカテゴ リをホワイトリストに追加すると、そのカテゴリに該当するウェブサイトの 暗号化パケットが検知されなくなります。



- ウェブサイトアドレス:カスタマイズのフィールドを提供します。信頼できるウェブサイトのアドレスをホワイトリストに追加すると、該当するウェブサイトのは暗号化パケットが検知されなくなります。
- 証明書をダウンロードする:LionFilter 200 のデフォルトの証明書をダウンロード できます。この証明書をブラウザーにインポートすると、Pico-UTM からの HTTPS 接続を信頼します。
- **証明書のインポート**:独自の証明書を Pico-UTM にインポートすることで、接続の 互換性を向上させることができます。
- * 付記:
- HTTPS 接続で使用するポートをカスタマイズする場合、他のネットワークサービスで一般的に使用されるポート(例:FTP用のポート 20、21 や SMTP 用のポート 25 など)は避けてください。 これにより、ポートの競合問題を防ぐことができます。
- 2. [SSL/TLS 検出]を有効にした後の互換性を向上させるために、LionFilter 200 は一部の信頼できる サービス (Google、Apple、Microsoft など)のアドレスをホワイトリストに追加しています。



脅威ログ

脅威事件が検知された後、その情報は各機能の[脅威ログ]のページに表示されます。

						♥ 日本
LionFilter 200	 脅威ログ 					
■ ダッシュボード	アンチウィルス	不正侵入防止	Web 脅威防止 ジオブロック ファイアウォール	例外のURL/IPアドレス		
⊕ wan						
tetaufra	不正侵入防止 (1	7)			بل	CSVを書き出す
≧ セキュリティ機能	日付と時刻	重大さ	メッセージ	送信元IP	送信元ポート	宛先IP
脅威ログ	2025/05/05 23:46	low	TCP SYN Port Scan Lv1: 10 ports within 30 seconds	192.168.8.35	57070	192.168.8.84
ネットワーク管理	2025/04/28 08:49	() Medium	SQL SQL Injection	2001:b030:7123:300:d6e:e629:a23d:6886	51404	2400:8902::f03c:91
 資産管理 トラフィック 	2025/04/28 08:49	() Medium	SERVER Joomla DT Register SQL injection attack	2001:b030:7123:300:d6e:e629:a23d:6886	51404	2400:8902::f03c:91
1 「シジィック	2025/04/28 08:49	! High	SERVER-WEBAPP Joomla DT Register SQL injection attempt	2001:b030:7123:300:d6e:e629:a23d:6886	51404	2400:8902::f03c:91
アドバンス設定	2025/04/28 08:44	! Medium	SQL SQL Injection	192.168.8.84	56429	139.162.104.220
C VPN	2025/04/28 08:44	! Medium	SERVER Joomla DT Register SQL injection attack	192.168.8.84	56429	139.162.104.220
	2025/04/28 08:44	! High	SERVER-WEBAPP Joomla DT Register SQL injection attempt	192.168.8.84	56429	139.162.104.220

脅威ログ

- **CSV を書き出す**:脅威事件を **CSV** ファイル形式で出力します。
- ホワイトリスト:過検知が発生した際、この機能で過検知を回避します。
 - ホワイトリストの追加:[脅威ログ]のページで過検知の脅威事件を抽出し、
 [+]をクリックして、ホワイトリストに追加します。
 - ホワイトリストの一覧と削除:[セキュリティ機能]のページで一覧と削除が 行えます。

Lionic Confidential 2025



LIONIC Threat Encyclopedia		
Web	shell.PHP.Hydra	Inbound Connection
S	Summary	
s	Signature ID	8011276100
F	Rule Category	Malware-activity
s	Severity	Medium
c	Created Date	2020-03-20
	Jpdate Date	2020-03-20
• •	Details	
,	Affected Products	Any unprotected system is at risk of being compromised.
	Affected OS	Windows , Linux , MacOS , IOS , Android , Other
	Description	This event is used to identify traffic associated with trojan activity, which may include commands and requests for files or other stages from a control server. This indicates that an attacker might have compromised the system, potentially leading to damage or a data breach.

脅威ログ- Threat Encyclopedia

- Threat Encyclopedia: [不正侵入防止]の脅威ログにて、シグネチャ ID をクリック すると該当不正侵入の情報と対策を参考できます。

											•
LionFilter 200	ॖ 脅威□	グ									
ダッシュボード	アンチャ	フィルス 不	正侵入防止 Web 脅威防止	: ジオブロ	コック	ファイアウォ	ール 例外のい	RL/IPアドレス			
9 WAN											
LAN	不正備	入防止 (17)									CSVを書き出す
キュリティ	1 12 13	(17)									
セキュリティ機能		送信元ポート	宛先IP	宛先ボート	国.地域	プロトコル	MAC	シグネチャID	アクション	PCAP	ホワイトリス
育威ログ		57070	192.168.8.84	5060		TCP	D45D64C28082	8060000101	LOG	ダウンロード	+
ットワーク管理	3d:6886	51404	2400:8902::f03c:91ff:fe1f:992e	8080	JP	HTTP	D45D64C2B082	8401714009	BLOCK	ダウンロード	+
資産管理	3d:6886	51404	2400:8902::f03c:91ff:fe1f:992e	8080	JP	HTTP	D45D64C28082	8401710001	BLOCK	ダウンロード	+
トラフィック	3d:6886	51404	2400:8902::f03c:91ff:fe1f:992e	8080	JP	HTTP	D45D64C28082	8100027101	BLOCK	ダウンロード	+
17801官址 ドバンス設定		56429	139.162.104.220	8080	JP	HTTP	D45D64C28082	8401714009	BLOCK	ダウンロード	+
VPN		56429	139.162.104.220	8080	JP	HTTP	D45D64C2B082	8401710001	BLOCK	ダウンロード	+
		56429	139.162.104.220	8080	JP	HTTP	D45D64C2B082	8100027101	BLOCK	ダウンロード	+

脅威ログ-PCAP のダウンロード

- - 脅威が検出された場合には PCAP を保持する:不正侵入防止の脅威ログにて[PCAP]

 > [ダウンロード]をクリックすると、パケットをダウンロードして、さらに詳細な 分析を行うことができます。
- * 付記: [セキュリティ機能] > [不正侵入防止] > [脅威が検出された場合には PCAP を保持する]の機能 を有効にすることが必要です。



資産管理

資産管理の機能は LAN 側の装置を認識し、特定の資産のネットワークアクセ スを許可または拒否にします。

- アドバンス装置識別:もっと詳しい情報を取得できます。
- * 付記:識別プロセス中にネットワークの使用に影響を与える可能性があります。
- 新しい資産をブロック:識別されない装置をブロックします。

					◎ 日本語
LionFilter 200	■ 資産管理				
■ ダッシュボード					
⊕ wan	本機能はLAN側のま 情報を取得できま	麦置を認識し、リスト化します。そして特定の装置(すが、情報取得プロセスにおいてネットワーク状態	のネットワークアクセスを許可 に影響を与える場合がありま	可や拒否できます。[アドバンス装置識別 す。[新規の装置をブロック]機能を有効	別]機能を有効にすると、より詳しい hにすると、まだ承認していない装置
H LAN	のネットワークア	クセスを拒否します。		10 famesters et al trancetta	
セキュリティ	アドバンス装置	歳別 🛑			
≧ セキュリティ機能	新規の装置をブロ	コック 🔵			
● 脅威ログ	デバイスタイプ	名前	MAC	IP	
ネットワーク管理	オンライン (1)				
📑 資産管理	Ļ	LionFilter-00112233442C-myfilter		192.168.8.35	•••
11 トラフィック	オフライン (30)	в)			
↓ 行動管理		AD-DC02		192.168.0.202	
アドバンス設定		VMware Ubuntu Device		192.168.1.247	
🗢 VPN	<u> </u>	VMware svn.lionic.com		192.168.0.220	©

資産管理



トラフィック

トラフィック管理機能では 各LAN 端末のトラフィック使用量を一覧表示し、 帯域幅の管理を行うことができます。

トラフィックモニター

LAN 端末のリアルタイムのダウンロードおよびアップロードのトラフィックを表示し、多い順または少ない順に並べ替えて表示できます。

						♥ 日本語	→
LionFilter 200	il トラフィック						
ज ダッシュポード	トラフィックモニター	QoS					
⊕ wan							
Ħ LAN	検索	5 🕏 絞り込み	J			\$ 表示	
セキュリティ	デバイスタイプ	名前	MAC	ダウンロード ↓	アップロード ≎		
🎽 セキュリティ機能		PM-Heidi		8.5 Kbps	16 Kbps		
				0.0 1000	its repo		
ネットワーク管理		AD-DC02					
資産管理		VMware Ubuntu Device					
11 トラフィック		VMware svn.lionic.com					
↓、 行動管理		SOD					
アドバンス設定		VMware Ubuntu Device					
© VPN		VMware wwws.lionic.com					
× · · - · · · · · · · · · · · · · · · ·		AD-PROD				•••	

トラフィック-トラフィックモニター



QoS

LionFilter 200 は、特定の送信元 IP、宛先 IP、または宛先ポートに対して帯域幅の管理を 行い、そのトラフィックに高い優先度を与えます。

LIONIC Security Solution Provider							⑦ 日本語 I→
LionFilter 200	ul トラフィック						
■ ダッシュポード	トラフィックエーィ	- 005					
🖶 WAN	F99499E=:	«— Q03					
∺ LAN	→ ₩45/+1 AN/0/注意	▲ () () () () () () () () () ()	こ 唐 什 先 1 201 - 主 チ				
セキュリティ	本 成能はLAN 回表	2001327676112	1187元6111日しま9。				
🗎 セキュリティ機能	有効						
● 脅威ログ	市公中学习以中国	9990-	- F 1000 Mbps				
ネットワーク管理		アップロ-	- K 1000 Mbps				
一 資産管理	優先順位設定	優先順位	名前	最小値	最大值		
11 トラフィック		1	Priority 1	0 2	100	%	
** 行動管理		2	Priority 2	0 9	100	%	
アドバンス設定		3	Priority 3	0 2	100	%	
C VPN		4	Priority 4	0 9	100	%	
		5	Default	0 9	100	%	
<		6	Priority 6	0	100	×	

トラフィック-QoS

手順1: QoS を有効にします。

手順2:ダウンロード/アップロードの帯域幅を設定します。

手順3:優先順位や帯域幅の割合を設定し、QoS ルールで使用します。

* 付記:8つの優先順位(priority)を提供し、優先度は1番目が最も高く、8番目が最も低いです。5番 目の優先順位がデフォルトです。

手順4:[適用]をクリックした後、実行します。

優先順位	設定	優先順位	名前	最小値		最大值	
		1	Priority 1	99	%	100 %	
		2	Priority 2	0	%	100 %	
		3	Priority 3	0	%	100 %	
		4	Priority 4	0	%	100 %	
		5	Default	30	%	100 %	
		6	Priority 6	0	%	100 %	
		7	Priority 7	0	%	100 %	
		8	Priority 8	0	%	100 %	

トラフィック-Qos-優先順位設定



- 手順5:[+ルールを追加する]をクリックします。
- 手順6:各フィールドに入力します。
- 手順7:[適用]をクリックした後、実行します。

名前	有効	優先順位	送信元IP	宛先IP	宛先ポート	
QoS 01		1 0	192.168.10.9	192.168.82.7	ANY	
夕前	右袖	原生晒荷		穷生地	空生ギート	
Default		5 °	ANY	ANY	ANY	

トラフィック-Qos-QoS ルール



行動管理

行動管理は特定なコンテンツのカテゴリ、或いはアプリケーションをブロッ クできます。ユーザーは、自分のニーズに合わせて設定を調整して、家族や スタッフが不適切なコンテンツの影響を受けないように守ることができます。

LIONIC Security Solution Provider	♥ 日本語	→
LionFilter 200	<u>業</u> 行動管理	
■ ダッシュボード	#U9- 7625	
⊕ wan		
Ħ LAN		
セキュリティ	行動管理は、不適切なウエフサイトやアブリケーションをブイルタリングし、特定の国、地域との接触をブロッグすることができます。 注意:上位のポリシーは値先度が高いため、接続がそれに一致した場合、他のポリシーの検査は行われません。	
≧ セキュリティ機能		
● 脅威ログ	+ <i>ル</i> - <i>ル</i> 220095	
ネットワーク管理	Branch A rule 有效 🔵 🕝 🕫	
🚔 資産管理		
↓ トラフィック		
1 行動管理	Branch B rule 有效	
アドパンス設定		
C VPN	Success	
* **7=1.	設定が適用されました!	Â

行動管理

ポリシー

[+ルールを追加する]をクリックして、新しいルールを追加します。ポリシー管理ページで ルールを編集、および削除できます。上位のルールにはより高い優先順位があり、検査は 上から順に行われます。接続がいずれかのルールの条件に一致した場合、そのルールに設 定されたアクションが実行され、その接続に対する以降のルールの検査は行われません。



		♥ 日本語 I→
LionFilter 200	♣ 行動管理	
■ ダッシュボード		
⊕ wan	Branch A rule 🖌	前のページに戻る
H LAN		
セキュリティ	管理節用 〇	+ ルールを追加する
🗎 セキュリティ機能		
● 育威ログ	Address ANY	×
ネットワーク管理		
🚍 資産管理		
山 トラフィック	ウェブサイト内容の管理 ①	+ ルールを追加する
2 行動管理		
アドバンス設定		×
• VPN		
★ \$,7∓1. <	アプリケーションの管理 ①	+ ルールを追加する

行動管理-ルールの編集

✓をクリックして、ルールの編集ページに移動し、複数の管理タイプを追加できます。

手順1:管理範囲の[+ルールを追加する]をクリックして、管理範囲を設定します。

手順2:管理する予定の IP アドレスや MAC アドレスを選択します。

手順3:各項目の[+ルールを追加する]をクリックし、内容とアクションを設定します。

手順4:[適用]をクリックした後、実行します。

手順5: 「前のページに戻る]をクリックしポリシー管理ページに戻ります。

ルール設定について:

- 管理範囲: IP アドレスや MAC アドレスを設定し、管理します。必須項目です。
 ウェブサイト内容の管理:ウェブサイトのコンテンツで管理します。
- **アプリケーションの管理:**アプリケーションを認識し、管理します。
- **ウェブサイトの管理**:指定のサイトを許可や拒否で管理します。

ジオブロック

ユーザーが設定した国や地域に基づき、グループに対して当該地域からの着信接続をブロ ックするか、またはグループ内のデバイスが当該国・地域への接続をブロックします。



LIONIC Security Solution Provider	ジオブロック
LionFilter 200	このサイトまたは製品には、以下から入手可能なIP2LocationLITEデータが含まれています。https://lite.jp2location.com
罰 ダッシュポード	有効
⊕ WAN	ブロックされる国・地域を選択 🕐
Ħ LAN	下記の国、地域からの通信をブロック:
セキュリティ	設定しない
当 セキュリティ機能	下記の国、地域に送る過信をブロック:
● 育威ログ	設定しない
ネットワーク管理	
資産管理	4747F
1 1 197799	信頼できるIPアドレスはホワイトリストに追加すると、ジオブロック機能で拒否されません。
行動管理	IPアドレス + 適加
	道用
<	

行動管理-ジオブロック

手順1:ジオブロックを有効にします。。

手順2: 🕢 をクリックして、許可/拒否の国や地域を選択します。

手順3:各設定値を入力します。

手順4:[はい]をクリックした後、実行します。

- ホワイトリスト: 拒否された国や地域が例外の IP アドレスを追加できます。

イベント

行動管理の検知結果はイベントのページで現されます。[CSV を書き出す]をクリックして 検知結果を CSV ファイル形式で出力します。

					〇 日本語
LionFilter 200	二 行動管理				
ダッシュボード	#U>- 142				
WAN					
LAN	イベント (29)				.↓. CSVを書き出す
キュリティ					
セキュリティ機能	日付と時刻 MAC	送信元IP	名前	メッセージ	アクション
育威ログ	2025/05/08 11:13 D45D64C2B08	2 192.168.8.84	Branch A rule	[Advertisments and Pop-Ups] incoming-telemetry.thunderbird.net	BLOCK
トワーク管理	2025/05/08 11:07 D45D64C2B08	2 192.168.8.84	Branch A rule	[Advertisments and Pop-Ups] mobile.events.data.microsoft.com	BLOCK
資産管理	2025/05/08 11:05 D45D64C2808	2 192.168.8.84	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
トラフィック	2025/05/08 11:00 D45D64C2B08	2 192.168.8.84	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
1 行動管理	2025/05/08 10:37 D45D64C2B08	2 192.168.8.84	Branch A rule	[Advertisments and Pop-Ups] mobile.events.data.microsoft.com	BLOCK
ドバンス設定	2025/05/08 10:25 D45D64C2B08	2 10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] incoming-telemetry.thunderbird.net	BLOCK
VPN	2025/05/08 10:25 D45D64C2B08	2 10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
★ シフテル く	2025/05/08 10:20 D45D64C2B08	2 10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK

行動管理-イベント



VPN サーバー

この VPN の機能で LionFilter 200 はモバイルネットワークやフリーWi-Fi までも守れます。

VPN 経由で LionFilter 200 の LAN 側にない装置もセキュリティ機能から保護 できます。

 Version Version			♥ 日本語	→
Image: Normal System Wiedward PSec that System Wiedward PSec that System Wiedward Dクライアントアグリをモバイル堪たインストールし、下記のプロファイルの中の一つで設定した後、VPNでインターネットに 歴史すればLionFileeのセキュリティ復後を受けられます。 that System 建建: DDNS が必要な場合、新しいプロファイルを追加する前に DDNS を設置してください。 that System DSR 認識を有効にする in トラフィック 「外防 いた WebGuard の クライアントを接続した後、https://DJ07.21L/opt/vpn にアクセスし、ワンタイムバスワードを 入力してください。 that System + 新しいプロファイルを追加する that System + 新しいプロファイルを追加する that System + 新しいプロファイルを追加する	LionFilter 200	• VPN		
セキュリティ ・ セキュリティ ・ セキュリティ ・ ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ・ロ	₩ LAN	WireGuard IPSec		
● セネリアイ構能 WheeQuardのクライアントアプリをモバイル場末にインストールし、下記のブロファイルの中の一つて設定した後、VPNでインターネットに 総営すればLionFilterのセキュリティ保護を受けられます。 ● 分成ログ 注意: DDNS が必要な場合、新しいプロファイルを追加する前に DDNS を設置してください。 オットワーク9種 VPNサーバーを起動する ● 方気 たな ● ● プレアハ ● ● マPN ● ● システム ● ● ジステム ●	セキュリティ			
	🗎 セキュリティ機能	WireGuardのクライアントアプリをモバイル堪末にインストールし、下記のプロファイルの中の一つで設定した後、VPNでインターネットに 接続すればLionrillerのセキュリティ保護を受けられます。		
 ネットワーク程 アドバース超差 アドバース通道 アドバース超差 アドバース超差 アドバース 超差 アドバース 超差	 育威ログ 	注意:DDNS が必要な場合、新しいプロファイルを追加する前に DDNS を設置してください。		
 読 資産管理 二段用認証を有効にする	ネットワーク管理	VPNサーバーを起動する		
・II トラフィック 新加した場合は、WireGuard のクライアントを接続した後、https://t0.07.211.i/otp/vpn にアクセスし、ワンタイムパスワードを 入力してください。 * 行動管理 + 新しいプロファイルを追加する * VPN 数定欄1 /	📑 資産管理	二段階認証を有効にする		
** 行動管理 アドバンスR2 • VPN • システム · ジンデム · ジ	III トラフィック	有効にした場合は、WireGuard のクライアントを接続した後、https://l0.107.211.1/otp/vpn にアクセスし、ワンタイムパスワードを 入力してください。		
アドバンス設定 ● VPN ● システム	主 : 行動管理			
● VPN ● システム 設定檔1 / ×	アドパンス設定	+ 新しいブロファイルを追加する		
O システム 設定檔1 / ×	🗢 VPN			
	• >Z74	設定欄1 / ×		
コーティリティ オフライン 器 VPN用QRコード よ ダウンロード	コ ーティリティ	オフライン 競 VPN用QRコード よ ダウンロード		

VPN サーバー- WireGuard

WireGuard VPN

予め準備すること:

WireGuard ダウンロードし、保護された装置にインストールしてください。

設定の手順:

- 手順1:[VPN サーバーを起動する]を有効にします。
- 手順2:[+新しいプロファイルを追加する]をクリックします。
- 手順3:
 - モバイル端末の場合、[QR コードを表す]をクリックし、WireGuard のアプリ で QR コードをスキャンして設定完了です。



パソコンやノートパソコンなどの端末の場合、[ダウンロード]をクリックし、
 ダウンロードされたプロファイルを WireGuard のクライアントにインポート
 して設定完了です。

設定完了後、セキュリティ機能が必要な場合、WireGuardのアプリやクライアントを実行し、VPN 経由でインターネットにアクセスしてください。

* 付記:

- ダイナミック DNS サービス (DDNS)を使う場合、必ず DDNS 設定完了後、次に VPN サーバを 設定します。
- LionFilter 200 は、プライベート IP アドレスを使いルーター経由でインターネットに接続する場合、ルーターにて LionFilter 200 のプライベート IP アドレスと Port 51820 をルーターのポート転送(Port Forwarding)機能に追加し、プロファイル内の LionFilter 200 の IP アドレスをルーターのIP アドレスやドメイン名に書き換えてください。
- 3. VPN の接続が異常の際、WireGuard クライアントで VPN 接続を再起動してください。

VPN サーバーで二段階認証を有効にします:

[二段階認証を有効にする]を有効にすると、VPN サーバーに接続する際、LionFilter 200 を通じてインターネットにアクセスするために、ワンタイムパスワードを入力する必要があります。これにより、VPN サーバーのアカウントセキュリティが強化されます。

予め準備すること:

- 1. WireGuard ダウンロードし、保護された装置にインストールしてください。
- 2. Google Authenticator などの OTP アプリをインストールしてください。

設定の手順:

- 手順1: [VPN サーバーを起動する]と[二段階認証を有効にする]を有効にします。
- 手順2:[+新しいプロファイルを追加する]をクリックします。
- 手順3:プロファイル内の[二段階認証の QR コード]をクリックします。
- 手順4:OTP アプリで二段階認証の QR コードをスキャンします。
- 手順5:
 - モバイル端末の場合、[QR コードを表す]をクリックし、WireGuard のアプリ で QR コードをスキャンして設定完了です。



パソコンやノートパソコンなどの端末の場合、[ダウンロード]をクリックし、
 ダウンロードされたプロファイルを WireGuard のクライアントにインポート
 して設定完了です。

接続の手順:

- 手順1:WireGuard クライアントを開き、VPN を接続します。
- 手順2:OTP アプリを開き、ワンタイムパスワードを取得します。

手順3:ブラウザーで<u>http://mypico.lionic.com/otp/vpn</u>にアクセスし、ワンタイム パスワードを入力します。

二段階認証完了後、VPN を通じて LionFilter 200 からインターネットにアクセスできるよ うになります。

* 付記:WireGuard VPN を設定すると、PPPoE 接続における QoS 機能は無効になります。

IPSec Site-to-Site VPN

IPSec Site-to-Site VPN 異なる地理的拠点(例えば、企業の本社と支社)間で セキュアな通信経路を確立し、双方のローカルネットワークを安全に相互接 続できるようにします。

LIONIC Security Selution Provider		◎ 繁中 →
LionFilter 200	• VPN	
罰 儀表板	WireGuard IPSec	
⊕ 網際網路		
計 區域網路	Sita-to-Site VPN	
安全防護		
■ 安全規則	+ 建立新設定檔	
資安記錄	IF 2	
網路管理	2 回 unknown	
📑 資產管理		
₀1 流量管理		
1 1、行為管理		
道路設定		
VPN		
◎ 系統管理		
■ 系統工具		
<		

VPN サーバー-IPSec



設定の手順:

手順1:「+新しいプロファイルを追加する」をクリックします。

手順2: 各項目に設定値を入力します。

- 名前: プロファイル名
- 有効: 有効/無効を切り替え
- IKE Version: IKE (Internet Key Exchange) バージョン
- Remote Address (リモートアドレス): 接続先の IP アドレス
- Remote Subnet (リモートサブネット): 接続先のサブネットマスク
- Local Subnet (ローカルサブネット): 自ネットワークのサブネット

Authentication

- Method :

- Pre-shared Key : 両端で同じパスワードを設定し、Phase の相互認証時に使用

- Signature : 公開鍵と秘密鍵の証明書による認証。2 組のサーバー証明書が必要

- PSK:共有する暗号鍵

Phase

- Method:データ転送時の暗号化方式
- Authentication:暗号化方式の認証方法
- Diffie-Hellman Groups:公開鍵暗号方式であるディフィー・ヘルマン鍵交換(DH 鍵交換)において、鍵の強さを決定するパラメータです。
- Key Lifetime (秒): AES 暗号鍵を何秒ごとに自動更新するかを指定

名前	LF_2	#Phase 1	
有効		Proposal	+ 追加
IKE Version	IKEV1 IKEV2		Encryption AES256 that Authentication SHA256 that The Share and Sh
Network		Diffie-Hellman Groups	_ 32 _ 31 _ 30 _ 29 _ 21 _ 20 _ 19 _ 1 _ 17 _ 16 _ 15 ♥ 14 ♥ 5 _ 2 _ 1
Remote Address	1.164.32.41	#Bhase 2	
Remote Subnet	10.254.254.0/24	Proposal	+ 追加
Local Subnet	192.168.2.0/24		Encryption AES256 \circ Authentication SHA256 \circ 📋
Authentication	Pro-shared Voy	Diffie-Hellman Groups	_ 32 _ 31 _ 30 _ 29 _ 21 _ 20 _ 19 _ 1 _ 17 _ 16 _ 15 ✔ 14 ✔ 5 _ 2 _ 1
PSK		Key Lifetime(seconds)	86400



システム

デバイス

		● 日本語 →
LionFilter 200	o システム	
ज ダッシュポード	デバイス サーバ 通知 ファールウェア軍師 珍宝値の保存と復元 パスワードの変更 蔓頭の景原 サフリール	<i>ж</i> -ь
⊕ wan		
∺ LAN	ライヤンフ管理	
セキュリティ		
≧ セキュリティ機能	ライセンスの状況 アクティベートしている	
● 脅威ログ	ライセンスの有効期限 2026年5月8日 8:33:25	
ネットワーク管理	ライセンス更新のコード AAAA-BBBB-CCCC-DDDD	適用
📑 資産管理		
III トラフィック	ロイン時刻	
▲、行動管理		
アドバンス設定	日付と時刻 Thu May 8 11:51:43 CST 2025 (Asia/Taipei)	
VPN	タイムゾーン Auto ~	
A 2-7=1	インターネット時刻サーバと同期する 0.openwrt.pool.ntp.org ①	
<	Lopenwrt.pool.ntp.org	

システム-デバイス

ライセンスの管理

ライセンス情報、アクティベート状況の確認、及び更新をします。

メッセージ	ライセンスの状況	
ライセンスの有効期限 有効です		
まだアクティベートしていない	アクティベートしていません	
期限切れ	期限が切れました	
14:22 24:27 エ ニ	ライセンスサーバに問い合わせできません。	
1入ル唯応エノー	ライセンスが確認できません。	

- **ライセンスのアクティベート**:初めて LionFilter 200 を使う際、インターネットに 接続できる環境でアクティベートコード(付記1)を入力し、[アクティベートする] をクリックしてください。



- ライセンスの更新: LionFilter 200 は期限切れの 30 日前に案内が表示されますお早めにサブスクリプション(付記 2)してください。ライセンス更新コードを取得した後、コードを入力し、[適用]をクリックしてください。
- * 付記:
- アクティベートコードは、半角英数字 20 文字で構成されています。適用に成功すると、ライセン スが有効になります。アクティベートコードが無い場合やアクティベートできない場合、ご購入 の窓口にご連絡ください。
- ライセンス更新のコードは、半角英数字16文字で構成されています。適用に成功すると、ライセンスの有効期限が延長されます。サブスクリプションをご希望の場合、ご購入の窓口にご連絡ください。

日付と時刻

LionFilter 200 のシステム時刻の設定。

- タイムゾーン:現地のタイムゾーンを設定してください。
- インターネット時刻サーバと同期する:[+]で NTP サーバが追加できます



マネジメントポート(MGMT)

マネジメントポートはブリッジモードのみに対応しており、LionFilter 200 が DHCP を通 じて接続されたデバイスに IP アドレスを割り当てます。有効にすると、MGMT ポートは WAN 側への接続ができなくなります。無効にすると、MGMT ポートは通常の LAN ポー トとして使用できます。

* 付記:マネジメントポートと VLAN 機能は同時に使用できません。VLAN 機能を使用するには、先に マネジメントポートを無効にしてください。

LIONIC	日1丁と時刻			
Security Solution Provider	日付と時刻	Thu May 8 12:03:40 CST 2025 (Asic	ı/Taipei)	
LionFilter 200	タイムゾーン	Auto	~	
■ ダッシュポード	インターネット時刻サーバと同期する	0.openwrt.pool.ntp.org	٥	
⊕ wan		1.openwrt.pool.ntp.org	Ū	
∺ LAN		2.openwrt.pool.ntp.org	٥	
セキュリティ		3.openwrt.pool.ntp.org	Ŭ	+ 適用
≧ セキュリティ機能				
● 脅威ログ				
ネットワーク管理				
資産管理				
III トラフィック	マネジメントポート			
▲ 行動管理	有効			
アドバンス設定	有効化にすると、マネジメントポート(LANポ マネジメントポートけ通常のLANポートとして	ート4)はインターネットに接続できません。 毎日できます	。無効化にすると、	
C VPN				
× 27≠1.				
<				

システム-マネジメントポート

サーバー

LIONIC Security Solution Provider	•	日本語	l→
LionFilter 200	• システム		
■ ダッシュポード	デバイス サーパ 通知 ファームウェア更新 設定値の保存と復元 パスワードの変更 管理の服務 サマリーレポート		
⊕ wan			
₩ LAN	CMS		
セキュリティ			
🎽 セキュリティ機能	CMSサーバ 提続済み cmsdemo.cloud.lionic.com		
● 脅威ログ	アドバンス設定 > 適用		
ネットワーク管理			
資產管理			
11 トラフィック	Proxy		
土 : 行動管理	URL 例: http://10.254.25410:8888 テストする 逸用		
アドバンス設定			
© VPN	Svelog		
****	o you ag		
<	有効		

システム-サーバー



CMS

CMS は複数の LionFilter 200 をコントロールできます。CMS が設置された後、[CMS サ ーバ]のフィールドに CMS のアドレスを入力し、[適用]をクリックしてください。CMS を お求めの際は、ご購入の窓口にご連絡ください。

- CMSからファームウェアとシグネチャをダウンロードする:このアドバンス機能は、 インターネットに接続できない場合に使用されます。関連するご要望がある場合は、 ご購入窓口にご連絡ください。
- ファイアウォールと例外ウェブサイトのログを CMS に送る: CMS のストレージ使用効率を向上させるため、LionFilter 200 は CMS 設定後、デフォルトでアンチウイルスシステム、不正侵入防止、Web 脅威防止の3つの主要なセキュリティログのみをアップロードします。この機能を有効にすると、ファイアウォールおよび例外サイトのログも CMS にアップロードされます。

Proxy

Proxy 機能は、インターネットに直接接続できない LionFilter 200 をサポートし、Lionic のクラウドサービスを通じて完全なセキュリティ保護機能を提供します。LionFilter 200 を内部ネットワークに配置する場合、Proxy のアドレスを入力し、[適用]をクリックするこ とで、LionFilter 200 はプロキシを通じて Lionic のクラウドサービスを利用できます。必 要があれば、ネットワーク管理者にお問い合わせください。

Syslog

Syslog サーバーは、LionFilter 200 の稼働履歴を収集できます。独自の Syslog サーバーを 使用している場合は、各設定値を入力し[適用]をクリックしてください。

SNMP

SNMP はリモートで LionFilter 200 の稼働状況を監視できます。SNMP サーバー (v2c やv3)を導入している場合は、各設定値を入力してから[適用]をクリックしてください。

	アドバンス設定 > 適用
LionFilter 200	
ダッシュボード	SNMP
WAN	有効
LAN	バージョン V2c ~
リティ	
セキュリティ機能	
脅威ログ	SNMPv2c
ワーク管理	
資産管理	コミュニティ名 public
トラフィック	アクセスできるIPアドレスリスト IPV4 + 追加
行動管理	
(ンス設定	道用
/PN	
2.771.	

システム-サーバー



通知

[通知]機能を使用すると、脅威事件を検出した際に、その情報を指定されたメールアドレ スに送信できます。また、検出履歴、脅威統計、システム異常ログなどの情報を週報や日 報として定期的にまとめ、指定されたメールアドレスへ送信することも可能です。

			♥ 日本語 →
LionFilter 200	• システム		
■ ダッシュボード	デバイス サーバ 通知	11 ファームウェア更新 脱字値の保存と復元 パスワードの変更 管理の問題 サマリーレポート	
⊕ WAN			
# LAN			
セキュリティ	言語	English 🗸	
🗎 セキュリティ機能			
	メール通知		
ネットワーク管理	額度	□毎月 □毎週 □毎日 □登底が検知された際	
資産管理			
III トラフィック	SMIPT-A	smtp.mail.com	
1 行動管理	SMTPポート	25	
アドバンス設定	SMTPアカウント	user@mail.com	
• VPN	SMTPパスワード	パスワードを入力してください	
* \$17#1. <	通知先	user@moil.com	適用

システム-通知

言語

通知メールと統計レポートの言語を選択します(中国語/英語/日本語)。

メール通知

- 頻度:

- 毎月:毎月1日の 0:00 に月報を送信します。
- 毎週:毎週日曜の 0:00 に週報を送信します。
- 毎日:毎日の 0:00 に日報を送信します。
- 脅威が検知された際:リアルタイムで脅威情報を送信します。
- SMTP サーバ、ポート、アカウントとパスワード:通知メールと統計報告の送信設定です。
- 通知先:受信者のメールアドレス。

各設定値を入力して[適用]をクリックして設定を完了です。[テストする]をクリックしてテ ストメールを送信して設定が正しいかどうかを確認できます。

* 付記:送信アカウントは Gmail の場合、Gmail の二段階認証を有効し、App Password を[SMTP パ スワード]に入力してください。



ファームウェア更新

[ファームウェア更新]このページで新しいファームウェアがリリースされた 際、案内が表示されます。

[書き込み]をクリックして更新を行います。

LIONIC Security Solution Provider		♥ 日本語	l→
LionFilter 200	• システム		
ज ダッシュボード	デバイス サーバ 通知 ファームウェア更新 設定値の保存と復元 バスワードの変更 管理の履歴 サマリーレポート		
⊕ WAN			
H LAN	白野市町 ムのフェ ノム・フル目的のパーパーンフォー () 更新する		
^{ゼキュリティ}	日期更新 マのファームウェアは戦新のハーションです。 自後で更新する		
● 脅威ログ			
ネットワーク管理	手動更新 キャップロード		
🚍 資産管理			
11 トラフィック			
<u>▲</u> 【行動管理			
アドバンス設定			
A \$2771			
<			

システム-ファームウェア更新

- **あとで更新する:**ネットワークの混雑していない時間帯にファームウェアを更新するように、更新日時を予約指定できる機能を提供します。これにより、適切な日時を設定してファームウェア更新を行います。

トラブルシューティングの際、手動更新の必要があれば、[+アップロード]をクリックして ファームウェアファイルを選んでください。

* 付記:ファームウェアを更新すると、再起動が原因でネットワークが一時的に切断されます。



設定値の保存と復元

[設定値の保存と復元]この機能ではLionFilter 200の設定をバックアップします。

バックアップファイルは元の LionFilter 200 だけでなく、他の LionFilter 200 にも復元できます。

トラブルシューティングや LionFilter 200 の配置台数が少ない時に使われま す。

LIONIC Security Solution Provider		♥ 日本語	∣→
LionFilter 200	• システム		
■ ダッシュボード	デバイス サーバ 通知 ファールウェア原係 発生値の保存と得 示 パスワードの変更 等限の原原 サフリーレポート		
⊕ wan	THE THE AND THE ADDRESS OF THE ADDRE		
# LAN	保友 【存在】ボタンをクリックして、 硬本の設定内容をファイルに存在する。	古	
セキュリティ			
盲 セキュリティ機能			
● 育威ログ	復元 [復元]ボタンをクリックして、保存したファイルから設定内容を復元する。 ファイルを選択 復	元	
ネットワーク管理			
アドバンス設定			
• VPN			
A \$1771			
<			

システム-設定値の保存と復元

* 付記:LionFilter 200 の配置台数が多いの場合は CMS で管理するのがお薦めです。



パスワードの変更

LionFilter 200 の管理画面のログインパスワードを変更する際、新しいパスワ ードを入力し、[適用]をクリックしてください。

LIONIC Security Solution Provider						۲	日本語	∣→
LionFilter 200	• システム							
■ ダッシュポード	デバイス サーバ	通知 ファールウェア軍新 設定値の保存と復去	パスワードの変更	管理の尿尿	サマリーレポート			
⊕ wan		ALM FY AFLY LON INALMOVING CIC/U		El AL COMPUL				
∺ LAN	パスワードの変更	8 admin						
セキュリティ								
当 セキュリティ機能	新しいパスワード	パスワードを入力してください						
● 脅威ログ	確認用パスワード	パスワードをもう一度入力してください 🖌				適用		
ネットワーク管理								
音 資産管理								
11 トラフィック								
≛ 、行動管理								
アドバンス設定								
© VPN								
* \$17=1								
<								

システム-パスワードの変更



管理の履歴

[管理の履歴]このページでは LionFilter 200 の管理者に対し、管理画面で設定 変更の記録が表示されます。

LIONIC Security Solution Provider		♥ 日本語 →
LionFilter 200	• システム	
ज ダッシュポード	デバイス サーバ 添和 フェールウィア用料 知史値の使力と指示 パフロードの空用 美調介目	(原 サフリーレポート
⊕ wan		
H LAN		
セキュリティ	副注 (55)	
当 セキュリティ機能	日付と時刻 ユーザー名 送信元PP メッセージ	
● 脅威ログ	2025/05/08 11:55 admin 192.168.27.27 Sign in	
ネットワーク管理	2025/05/08 11:52 admin 192.188.27.27 Change connection mode	
資産管理	2025/05/08 11:49 admin 192.188.27.27 Sign in	
11 トラフィック	2025/05/08 11:26 admin 192.188.27.27 Sign in	
▲: 行動管理	2025/05/08 11:22 admin 192.168.27.27 Change connection mode	
アドバンス設定	2025/05/08 10:36 admin 192.168.27.27 Sign in	
e vpn	2025/05/08 10:33 admin 192.168.27.27 Change connection mode	
* **7=1.	2025/05/08 08:33 admin 192.168.27.27 Activate license	
<	2025/05/08 08:33 admin 192.168.27.27 Sign in	

システム-管理の履歴



サマリーレポート

[サマリーレポート]このページで日報・週報・月報がリアルタイムに生成され ます。

LIONIC Security Solution Provider		● 日本語 →
LionFilter 200	o システム	
冒 ダッシュボード	デバイス サーバ 通知 ファームウェア更新 設定値の保存と復元 バスワードの変更 管理の履歴 サマリーレポート	
⊕ WAN		
Ħ LAN	LionFilter 200 サマリーレボート	
セキュリティ		
🎽 セキュリティ機能	24時間 / 7日間 / 30日間	合 印刷
● 脅威ログ		
ネットワーク管理	LionFilter 日報 LIONIC	
📑 資産管理	2025年05月08日 2025年05月08日	
11 トラフィック	MAC / ライセンスの布括制篇 / 0002233440C ライセンスの布括制篇 / 2026年 05 月 08 日	
上 、行動管理		
アドパンス設定		
🗢 VPN	バージョン 25.0.2 システム負荷 サイバーリスク アンデライルスのバージョン 30.1134 mm mm mu m m m m m m m m m m m m m m m	
• \$ 774	不正保入防止のバージョン 5.1123 Web 倒成防止のバージョン 2.0.1652 ♀ ♀	
■ ユーティリティ		
	検査統計情報 地名24时间00米南欧计律组	
	ファイル URL フロー パケット	
<	3 3К 3К 226К	

システム-サマリーレポート



ユーティリティ

LIONIC Security Solution Provider		● 日本語 I→
LionFilter 200	コーティリティ	
■ ダッシュポード	ツール コマンドラインツール システルログ シグネチャの電転 亜好動 加密化	
⊕ wan		
H LAN		
セキュリティ	ping V Ipv4.google.com kun	
🗎 セキュリティ機能		
● 脅威ログ		
ネットワーク管理		
■ 資産管理		
III トラフィック		
上 ,行動管理		
アドバンス設定		
C VPN		
• システム		
🖬 ユーティリティ		
<		

ユーティリティ

LionFilter 200 は下記のツールを提供します:

- ネットワークツール:ping、traceroute、nslookup ツールでネットワークの接続
 問題を探します。
- **コマンドラインツール**:アドバンスのツールです。 ご使用前にテクニカルサポート窓口にご連絡ください。
- **システムログ:**システムログを書き出し、テクニカルサポート窓口に送付し、問題 点を探します。

クラッシュレポートを送信:システム異常が発生した際には、クラッシュレポートを作成し、 弊社に送信して問題点を確認いたします。

- **シグネチャの更新:**手動でシグネチャファイル。をアップロードし、システムの問 題点を探します。
- **再起動:**LionFilter 200 を再起動します。
- 初期化: LionFilter 200 を工場出荷時の設定に戻します。
- * 付記: ライセンスの有効期限内にインタネット接続とシステムが正常に作動していると、シグネチャ は自動的に更新されます。

LionFilter 200 Makes Security Simple



© Copyright 2025 Lionic Corp. All rights reserved.

Sales Contact 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.