

# Web GUI マニュアル Ark-UTM 16

バージョン 1.4.1 更新日付 2025/02



Lionic Corp. www.lionic.com



# Dual Ark-UTM 16 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	4
概要	7
ダッシュボード	9
WAN	
ネットワークの設定	
リモートコントロール	
LAN	15
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	19
アンチウィルス、不正信入防止、マルウェアサイト防止	19
ジオブロック	
ファイアウォール	
例外サイト	24
SSL / TLS 検知	25
脅威ログ	
資産管理	29
トラフィック	30
トラフィックモニター	
QoS	
行動管理	
ホリンー	
1 ハノト <b>古可田州 (114)</b>	
高リ用注 (HA)	
<b>VPN</b> サーバー	



システム	40
デバイス	40
サーバー	
通知	44
ファームウェア更新	46
設定値の保存と復元	47
パスワードの変更	
管理の履歴	
サマリーレポート	50
ユーティリティ	51
— , , , , , , , , , , , , , , , , , , ,	



## 管理画面にログイン

- 1. Ark-UTM 16 を電源に接続してください。
- Ark-UTM 16 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。
- Ark-UTM 16 の LAN ポート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。
- 4. パソコンまたはノートパソコンの IP 設定を以下のようにしてください
  - IP アドレス: 10.254.254.50
  - ネットマスク: 255.255.255.0
- 5. 設定完了後、ブラウザーで <u>https://10.254.254.254/</u>にアクセスしてくだ さい。





- 6. ログイン画面が表示された後、S/N 番号(デバイスの裏側に記載されている)をパスワードとしてログインしてください。
- ログインした後、[WAN]のページで Ark-UTM 16 のネットワーク設定を してください。



Ark-UTM 16	WAN		
🖬 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			
H LAN	IPv4 設定		
セキュリティ	II V T BAAL		
■ セキュリティ機能	接続設定	圖定設定	~
● 脅威ログ	IPアドレス	10.10.27.87	
ネットワーク管理	サブネットマフク	255 255 255 0/24	
📑 資産管理	55491425	200200.2000724	Ť
↓ トラフィック	デフォルトゲートウェイ	10.10.0.1	
<b>二代</b> 行動管理	DNS(任意)	8.8.8.8	
アドバンス設定			
👗 高可用性 (HA)			
O VPN	IPV6 設正		
♦ \$	接続段定	Auto	~
■ ユーティリティ	DNS(任意)	e.g. 2001:4860:4860:3888	
		- 3	

WAN-ネットワークの設定

- Ark-UTM 16 が有効な IP 設定を取得した後、パソコンまたはノートパソ コンの IP 設定を元に戻してください。その後、以下の方法で管理画面に アクセスできます:
  - Ark-UTM 16 とパソコンまたはノートパソコンが同じサブネット内のプライベートIP アドレスを持っている場合、パソコンやノートパソコンは https://myark.lionic.com/のURLから管理画面にアクセスできます。
  - Ark-UTM 16 がグローバル IP アドレスを持ち、パソコンまたはノートパソコンが 別のグローバル IP アドレスでインターネットに接続している場合は、上述の手順 で https://10.254.254.254/ にアクセスし、管理画面にログインしてください。 [WAN] > [リモートコントロール]のページで[アクセスコントロールリスト]を無 効にするか、またはパソコンまたはノートパソコンのグローバル IP アドレスを[ア クセスコントロールリスト]に追加してください。設定完了後、Ark-UTM 16 の LAN に接続したパソコンまたはノートパソコンは https://myark.lionic.com/ の URL から管理画面にアクセスできるようになります。



LIONIC Security Solution Provider			
Ark-UTM 16	🖶 WAN		
■ 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			
Ħ 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Ark-UTM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	フーザー名		
📑 資産管理			
<b>↓  </b> トラフィック	729-1	バスリートを入力してくたさい 🖓	2017
<b>上</b> 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 は、そのIPアドレスをアクセスコントロールリストに追加してください。	
👗 高可用性 (HA)		有效	+ 追加
• VPN			
• > <b>Z</b> FL		アドバンス設定 >	適用
■ ユーティリティ			
<	セキュリティ保 護接続	パスワードなどの機密情報を守るため、HTTPSでウェブユーザインタフェース にアクセスする。	

WAN-リモートコントロール



#### 概要

#### ダッシュボード:

[ダッシュボード]では Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 の接続モードが設定できます。

[ブリッジモード]から[ルーターモード]に変更すると、DHCP IP 予約とポート転送設定 ができます。

#### セキュリティ:

- **セキュリティ機能:**アンチウィルス、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:

- 資產管理: 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:特定のコンテンツ、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:

- 高可用性 (HA): 二台以上の Ark-UTM を HA グループにすると、ネットワーク異常 が発生した際に自動的に切り替わり、ネットワークの中断が発生しなくなります。



- VPN: Ark-UTM 16 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。

8



## ダッシュボード

Ark-UTM 16 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
Ark-UTM 16	検査統計情報 記動からの検査数		
ダッシュボード			1100
WAN	📄 0 ตดวราน 🤗 0 ตดบหน	<ul> <li>0 本のフロー</li> </ul>	2.1K 個のパケット
LAN			
U <del>7</del> -4	741127	效威事件ランキング	全部、マ
2キュリティ機能		1100 122	
育成ログ	<b>アンチウィルス</b> ステータス	シヴネチャID 種類 数量 メッセージ	
ワーク管理	●         検知された脅威事件         アクション 無効化		
資産管理			
トラフィック	▲正使入防止 ステータス ●		
行動管理	● 検知された脅威事件 アラフヨン フロラウ		
12282	Wob 您顾踪止		
高可用性 (HA)			
PN	Терменик ринке		
システム	ジオブロック	脅威事件がない	
ユーティリティ	● 検知された脅威事件 ステータス		
	ファイアウォール		

ダッシュボード-1

検査統計情報:Ark-UTM 16 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:** Ark-UTM 16 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。

機能名称及び数値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全てや、各種類の 検知回数ランキングが表示されます。



	ファイアウォール	
Ark-UTM 16		
シュポード		
	トラフィックモニター 男在 日海 海湾	装置情報
	週間还反	myArk /
ュリティ機能	0 bit/s	MAC / AABBCC0CF5F2 ライセンスの有効期限 / 2025年4月7日 14:45:35
ゆ	0 bit/s	IN HE N
æ	0 bit/s	27901 /
理		システム時刻 2025年1月8日10:05
マック	- ジェレロ UFL25 UFL25 UFL35 UFL40 UFL40 UFL35 U5L30 U5L10 U5L10 U5L10 U5L10	稼動時間 6分 20
理	トラフィック量	メモリ使用率 ストレージ使用率
	0 bytes	22% 46%
⊈ (HA)	0 bytes	
	0 bytes	CPU使用率
4	0 bytes	
イリティ	04:18 04:25 04:33 04:40 04:48 04:55 05:03 05:10 05:18	40% 20%
	<ul> <li>ダウンロード</li> <li>アップロード</li> </ul>	04:18 04:25 04:33 04:40 04:48 04:55 05:03 05:10

ダッシュボード-2

トラフィックモニター: Ark-UTM 16 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:Ark-UTM 16 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。

Gerariny Salution Provider		
Ark-UTM 16	WAN	
ダッシュボード		
WAN	ネットワークの設定 リモートコントロール	
LAN	IPv4 設定	
ユリティ		
セキュリティ機能	接続設定	固定設定
育威ログ	IPアドレス	Auto
ットワーク管理		周定設定
首座管理	サブネットマスク	PPPoE
	デフォルトゲートウェイ	192.168.0.254
トマノイツク	DNS(在會)	8888
行動管理		
>282		
高可用性 (HA)	IPv6 設定	
PN		
システム	接続設定	Auto 🗸
ユーティリティ	DNS(任意)	e.g. 2001/4860:4860:8888

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: Ark-UTM 16 が VLAN のネットワークに配置された時、こちらに 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 Ark-UTM 16 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 Ark-UTM 16 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。

LIONIC Security Solution Provider			
Ark-UTM 16	WAN		
■ ダッシュポード	ネットワークの設定	リモートコントロール	
WAN			
# 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Ark-UTMにアクセスする。	
セキュリティ	DNSサービス	有効	
🎽 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	<b>フ</b> _#_タ		
📑 資産管理	1-9-4		
<b>↓ </b> 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
<b>二、</b> 行動管理			
アドバンス設定	アクセスコント ロールリスト	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 は、そのIPアドレスをアクセスコントロールリストに追加してください。	
👗 高可用性 (HA)		有效	+ 追加
😁 VPN			
• >774		アドバンス設定 >	適用
■ ユーティリティ			
<	セキュリティ保 護接続	パスワードなどの機密情報を守るため、HTTPSでウェブユーザインタフェース にアクセスする。	

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)

Ark-UTM 16 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 Ark-UTM 16 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。
- Ark-UTM 16 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 Ark-UTM 16 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。

手順一:[+追加]をクリックします。

- 手順二: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。
- 手順三:[適用]をクリックします。

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、全てのグローバル 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。

アドバンス設定		
▲ 高可用性 (HA)	セキュリティ保護接続	パスワードなどの機密情報を守るため、HTTPSでウェブユーザインタフェース にアクセスする。
C VPN		セキュリティ保護投続を使う
• >776		有効にすると、すべてのアクセスがHTTPSになります。アクセスコントロール リストが無効につれると、このオプションが発動的に有効になります。
🖬 ユーディリティ		
<		

リモートコントロール-セキュリティ保護接続



## 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 Ark-UTM 16 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

Ark-UTM 16 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。

Ark-UTM 16	H LAN			
ज ダッシュボード	培練工_R LAN	DHOR ポート転送 静的リートの本		
⊕ WAN	3860 C - 1- DAN	DHCF /K-THRAS 18743/V-THRAE		
H LAN				
🗎 セキュリティ機能				
● 脅威ログ		接続モ	- 14	
ネットワーク管理				
📑 資産管理				
<b>↓  </b> トラフィック		ノリッジモード	ルーターモード	
<b></b> 行動管理		デムやルーターを提供した場合	ISPがモデム提供した場合	
アドバンス設定				
👗 高可用性 (HA)		201		
C VPN				
• > <b>7</b> 52				
■ ユーティリティ				

#### LAN-接続モード

#### - ブリッジモード

[ブリッジモード]では Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 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。Ark-UTM 16 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。

Ark-UTM 16	# LAN	
≣ ダッシュボード		
⊕ WAN	SERVE IN DAM DRUP JIC INDUCE REPORT INSTE	
H LAN		
🎽 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		通用
↓】 トラフィック		
<b>二、</b> 行動管理		
アドバンス設定		
👗 高可用性 (HA)		
VPN		
• >725		
🖬 ユーティリティ		

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、Ark-UTM 16 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。

Ark-UTM 16	H LAN			
₩ ダッシュポード	培练工_ド IAN DUCP	北山下新洋 静的儿山下的字		
⊕ WAN	SKALE I. LAN DIGP	715 T-983425 - 9829-2722 - T-98542		
H LAN	DHCP サーバー設定			
📋 セキュリティ機能	有効			
● 脅威ログ	開始 IP アドレス 10.254.25	4.1		
ネットワーク管理	終了 IP アドレス 10.254.25	4.253		
📑 資産管理				
■ 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				
👗 高可用性 (HA)	MACアドレス	IP アドレス	説明(任意)	
I VPN				適用
o >725				
■ ユーティリティ				

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 Ark-UTM 16 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。

Ark-UTM 16	H LAN	
■ ダッシュポード	1918-11-12 IAM DUCD 47-1-1-124 88011-1-1274	
⊕ WAN	22.04 C L. OHA DUCL N. LAND HARDIN LANCE	
H LAN	ボート転送	- 川一川本治州大子
セキュリティ	··· · · · · · · · · · · · · · · · · ·	T TO TO EXEMPTS
📋 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PPアドレス プロトコル	1981(任音)
● 脅威ログ		mn-13 (1716V)
ネットワーク管理		適用
📑 資産管理		
<b>ill</b> トラフィック		
<b>土</b> 行動管理		
アドバンス設定		
♣ 高可用性 (HA)		
VPN		
• システム		
■ ユーティリティ		
<		

#### LAN-ポート転送

#### 静的ルート設定

[ルーターモード] では、Ark-UTM 16 は静的ルート機能を提供します。

Ark-UTM 16	H LAN			
₩ ダッシュボード	地線モード LAN DHCP	式一下新兴 <b>静的儿一下的</b> 字		
⊕ WAN	3000 to 1 0701 07100	The France Harrison Franks		
H LAN	静的儿一卜龄定 经路债现发手工	w <del>クオ</del> ス		
キュリティ	INFORM THAT TRANSPORT	///0		+ 10-108.0019 S
🗎 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
育成ログ				
ットワーク管理				適用
。 資産管理				
トラフィック				
行動管理				
ドバンス設定				
🛔 高可用性 (HA)				
VPN				
• >776				
ユーティリティ				

LAN-静的ルート設定



## セキュリティ機能

#### アンチウィルス、不正侵入防止、マルウェアサイト防止

Ark-UTM 16 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。

- **アンチウィルス**:パケットからウィルスを検出し、ウィルスファイルを 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	アンチウィルス	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 / ログとウィルス 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	クラウドデータベース ーでスキャンする	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	Al で動的な悪意のある URL を検知
設定	AI で未知のウィルスを 検知	止、脅威が検出された場合 には PCAP を保持する	第三者データーベース
ホワイトリ	ホワイトリストの一覧	ホワイトリストの一覧と削	ホワイトリストの一覧
スト	と削除	除	と削除



ark-UTM 16	■ セキュリティ機能
■ ダッシュポード ⊕ WAN	<b>アンチウィルス</b> 不正優入防止 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JRQ/Pアドレス
計 LAN セキュリティ	全般
セキュリティ機能	有效
● 脅威ログ	アクション ログとウィルスを無効化する(Destroy)  マ
ネットワーク管理	アドバンス設定
↓  トラフィック	クラウドデータベースでスキャンする (株式茶み)
* 行動管理 7ドバンス設定	クラウドデータベースでスキャンすると、より光全な保護を提供できますが、一部のファイルを転送する原 の遺伝達度に影響します。
👗 高可用性 (HA)	AIで未知のウィルスを検知
● VPN ● システム	AIでファイルを分析し、未知のウィルスを検知します。 建築:この機能は「クラウドデータベースでスキャンする」を明効にして、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。
<b>■</b> ユーディリティ	ホワイトリスト

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。
  - ログとウィルスを無効化する:脅威事件が[脅威ログ]に記録され、そしてウ ィ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:アンチウィルス機能は、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、Ark-UTM 16 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 で未知のウィルスを検知: Lionic のクラウドスキャンには AI ウイルス対策エンジンが搭載されており、ゼロデイウイルスの検出が可能です。この機能を有効にすると、AI 技術を活用してゼロデイウイルスを検出します。
- 総当たり攻撃の防止:この機能を有効にすると、Ark-UTM 16 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、Ark-UTM 16 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、Ark-UTM 16 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、Ark-UTM
   16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、Ark-UTM 16 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インポートできます。

LIONIC Security SetUSen Provider	
ark-UTM 16	■ セキュリティ機能
ダッシュボード	アンチウィルス 不正確入街止 Web <b>音感防止</b> ジオブロック アンチスパム ファイアウォール 例外のJRJ/Pアドレス
WAN	
AN .	
ユリティ	至版
セキュリティ機能	有効
脅威ログ	アクション ログとプロックする 🗸
トワーク管理	
資産管理	アドバンス設定
トラフィック	AIで動的な悪意のあるURLを検知
行動管理	AIでドメイン名を分析し、動的な悪意のあるURLを検知します。
レス設定	第三者データーペース
高可用性 (HA)	
VPN	ホワイトリスト
システム	
ユーティリティ	
<	

- **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。

		<ul> <li>日本語</li> </ul>
	■ セキュリティ機能	
ज ダッシュポード	アンチウンルフ 天正高1時中 Wah 奇感的中 <b>ジナブロック</b> アンチフバム ファノアウォール 部務内100/1071511.7	
⊕ WAN		
H LAN		
キュリティ	全版	
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://Re.jp2location.com	
● 脅威ログ	有効	
ットワーク世程	ブロックされる国。地域を選択 📝	
<b>)</b> 資産管理		
■ トラフィック	下記の道、地域からの遺信をプロック:	
1. 行動管理	設定しない	
ドバンス設定	下記の国、地域に送る通信をブロック:	
。高可用性 (HA)	設定しない	
VPN	*076176	
>ステム		
コーティリティ	信頼できるIPアドレスはホワイトリストに追加すると、ジオプロック機能で担否されません。	
	<ul> <li>Pアドレス + 追加</li> </ul>	
<		

セキュリティ機能-ジオブロック

手順一:ジオブロックを有効にします。

手順二: 
をクリックして、許可/拒否の国や地域を選択します。

手順三:各設定値を入力します。

手順四:[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。



## ファイアウォール

Ark-UTM 16 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。

LIONIC		♥ 日本語
Security Solution Provider		
Ark-UTM 16	■ セキュリティ機能	
■ ダッシュポード		
WAN	アンチワイルス 不正便入防止 Web 層風防止 ジオフロック アンナスパム ファイアウォール 例外のURL/Pアトレス SSL / TLS 接知	
H LAN		
セキュリティ	有効	+ ルールを追加する
ビセキュリティ機能		
● 脅威ログ		通用
ネットワーク管理		
📑 資産管理		
ⅠⅠ トラフィック		
<b>1</b> 行動管理		
アドバンス設定		
👗 高可用性 (HA)		
VPN		
0 2776		

セキュリティ機能-ファイアウォール

手順一: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)

- 手順二:[+ルールを追加する]をクリックします。
- 手順三:各フィールドに入力します。

手順四:[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/ANY。
- 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全て許可または拒否になります。

	© 8	本語 I→
ark-UTM 16	■ セキュリティ機能	
■ ダッシュポード	マッチウィルフ 天天道11日本 Makaを開始本 がイブロック ファイブウォール <b>200パープサイト</b> 60 (15:850	
⊕ WAN	アプラフィルス 小正387A91圧 Web Haka91圧 フィントロック ファイアフィール 997アエンフィード 333/113/0001	
H LAN		
セキュリティ	許可 拒否	
セキュリティ機能		
● 育成ログ		
ネットワーク管理		
📑 資産管理		
<b>山</b> トラフィック		
<b></b> 行動管理		
アドバンス設定		
👗 高可用性 (HA)		
O VPN		
• •7774		
■ ユーディリティ		
<		

セキュリティ機能-例外サイト

手順一: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。 手順二:[+追加]をクリックした後、実行します。

\* 付記: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全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、Ark-UTM 16 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 SubJew Provider		♥ 日本語
Ark-UTM 16	■ セキュリティ機能	
ダッシュボード	マッチウノルフ 太正員1時止 Wab 鼻底防止 ジオブロック ファイアウォール 副外ウップサイト Sti / Ti S M T	
WAN		
LAN	SSL / TLS 検知	
1977	SSL/TLS 時知職能で HTTPS サイトをアクセスする際に装置を守ります。 体書・SSL/TLS 時知職能を有効にすスとなっい「ワーク物度が影響なか」一部のアプロパーシュンチ後かかません。	
セキュリティ機能	2018、354 Fit3 (Roomany)で行われたケッシュアック2020/39/目でに、 ロロンアクソフ・プロア Unit(Fita Erio)	
脅威ログ	有效	
トワーク管理	HTTPS ボート 443 通用	
資産管理		
トラフィック	ホワイトリスト	
行動管理	サイトのカテゴリ ウェブサイトアドレス	
パンス設定	Finance and Insurance	
高可用性 (HA)	Health and Medicine	
VPN		
システム		
ユーティリティ	証明書	
<	経時書をダウンロードする デフォルト経時書をダウンロードしてブラウザーにインボートし、Ark-UTM からの ・ダウンロード	

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、Ark-UTM 16 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: Ark-UTM 16 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:Ark-UTM 16 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、Ark-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 Ark-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。
- [SSL/TLS 検出]を有効にした後の互換性を向上させるために、Ark-UTM 16 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

LIONIC Security Solution Provider		6
Ark-UTM 16	<ul> <li>         ・         ・         ・</li></ul>	
■ ダッシュポード	アンチウィルス <b>不正義入為止</b> Web 登録次止 ジオブロック ファイアウォール 前外ウェブサイト	
⊕ WAN		
H LAN	<b>不正侵入防止</b> (0)	CSVを書
セキュリティ		
セキュリティ機能	日付と時刻 MAC 送信元PP 送信元ポート 売先PP 売先ポート 国、地域 プロトコル シグネチャロ 厳しさ メッセージ	アクション PCAP ホワイト
<ul> <li>         ・ 角減ログ     </li> </ul>	( )	10 🗸
ネットワーク管理		
🚍 資産管理		
<b>ル</b> トラフィック		
<b></b> 行動管理		
アドバンス設定		
▲ 高可用性 (HA)		
TVPN		
• >775		
■ ユーティリティ		

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 Threat Encyclopedia		
Wet	oshell.PHP.Hydra	Inbound Connection
•	Summary	
	Signature ID	8011276100
	Rule Category	Malware-activity
	Severity	Medium
	Created Date	2020-03-20
	Update 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 sever. This indicates that an attacker implify thave 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。

LIONIC		♥ 日本語 1
Security Solution Privater		
	<ul> <li>         ·          ·          ·</li></ul>	
■ ダッシュポード	アンチウィルス 不正便入防止 Web 負張防止 ジオブロック ファイアウォール 例外ウェブサイト	
⊕ WAN		
H LAN	不正侵入防止 (0)	
ビキュリティ 自 セキュリティ機能	日付と時刻 MAC 送磁元F 送磁元ポート 宛先IP 亮先ポート 国、地域 プロトコル シグネチャルの 厳しさ メッセージ	アクション PCAP ホワイトリスト
<ul> <li>         ・ ・ ・</li></ul>		10 🗸 0-0/0
ネットワーク世界		
📑 資産管理		
<b>山</b> トラフィック		
<b>::</b> 行動管理		
アドバンス設定		
▲ 高可用性 (HA)		
C VPN		
• >72777		
■ ユーティリティ		
<		

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: Ark-UTM 16 で無効化またはブロッ クされた脅威ログにて[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。



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
ark-UTM 16	<b>al</b> トラフィック					
ダッシュボード	トラフィックモニター Qo	S				
∋ WAN						
キュリティ	<sup>夜雨</sup> デパイスタイプ	5 14 取り込み 名前	MAC	ダウンロード ↓	アップロード 。	~ 费示
セキュリティ機能	<b>.</b>	Linux device	00012961D2C7			
ットワーク管理		00037FBADBAD	00037FBADBAD			····
2 資産管理		00037FBADBAE	00037F6ADBAE			····
「行動管理	6 <b>.9</b>	Fortinet device	00090F09001B			
ドバンス設定		VMware Virtual Machine	000C2911BFA5			
。高可用性 (HA) VPN		VMware Ubuntu Device	000C29518461 000C297788CF			
• ⇒ <b>⊼</b> ∓∆		VMware Virtual Machine	000C29A0D062			
ユーティリティ		vCentergeosatcomtw	000C29B69BB7			
	«<>>»					10 0 1 / 13 数量:130

トラフィック-トラフィックモニター



## QoS

Ark-UTM 16 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 Subtries Provider								
ark-UTM 16	<b>al</b> トラフィック	,						
ज ダッシュポード	トラフィックモー	々— 0os						
⊕ WAN		Q00	-					
H LAN	本機能はLAN側装	置の優先順位で(	歴先制御します。					
	有効							
📋 セキュリティ機能	総帯域幅	ダウンロー	1000	Mbps				
● 脅威ログ		アップロー	× 1000	Mbps				
ネットワーク管理	優先順位設定	優先順位	名前		最小值		最大值	
資産管理		1	Priority 1		0	%	100	×
		2	Priority 2		0	2	100	8
1. 行動管理		3	Priority 3		0	2	100	5
アドバンス設定		4	Priority 4		0		100	
👗 高可用性 (HA)			Priority 4		0	~	100	~
O VPN			Derault		0	70	100	~
• > <b>7</b> 76		0	Priority 6		0	*	100	%
🖬 ユーティリティ		7	Priority 7		0	26	100	25
		8	Priority 8		0	%	100	%

トラフィック-QoS

- 手順一: QoS を有効にします。
- 手順二:ダウンロード/アップロードの帯域幅を設定します。
- 手順三: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、1番目が最も高く、8番目が最も低い優先度です。5番目の優先順位がデフォルトです。
- 手順四:[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	0	%	100	%
	2	Priority 2	0	%	100	%
	3	Priority 3	0	%	100	%
	4	Priority 4	0	%	100	%
	5	Default	0	%	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



手順五:[+ルールを追加する]をクリックします。 手順六:各フィールドに入力します。 手順七:[適用]をクリックした後、実行します。

+ ルールを追加す						oSルール
	宛先ポート	宛先IP	送信元IP	優先順位	有効	名前
	ANY	ANY	ANY	5 0		Default

トラフィック-Qos-QoS ルール



## 行動管理

行動管理は特定の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。

		⑦ 日本語 Ⅰ→
Ark-UTM 16	<b>弐</b> 行動管理	
■ ダッシュボード	ポリシー イベント	
⊕ WAN		
H LAN		
セキュリティ		エリレールを通知する
■ セキュリティ機能	新管理規則 有効	
● 脅威ログ		
ネットワーク管理		
🚍 資産管理		
<b>ill</b> トラフィック		
11 行動管理		
アドバンス設定		
👗 高可用性 (HA)		

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 ルールを編集して削除できます。

	新管理規則 /		前のページに戻
ark-UTM 16			
ダッシュボード	管理範囲 ①		+ ルールを追加する
WAN		情報が無い	
LAN			
コリティ	ウェブサイト内容の管理 の		+ ルールを追加する
セキュリティ機能			
育成ログ		情報が無い	
ワーク管理			
資産管理	アプリケーションの管理 0		+ ルールを追加する
トラフィック			
行動管理		情報が無い	
「ンス設定			
高可用性 (HA)	ウェブサイトの管理 ①		+ ルールを追加する
VPN			
システム		情報が無い	
ユーティリティ			適用
<			



ルールの編集ページで、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:管理対象の IP アドレスや MAC アドレスを選択します。

手順3:管理したい項目を選択し、[+ルールを追加する]をクリックし、内容と動作を設定します。

手順4:[適用]をクリックして、実行します。

手順5:「前のページに戻る]をクリックして、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 アドレスを設定して管理します。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を管理します。
- **アプリケーションの管理:**アプリケーションを認識して管理します。
- **ウェブサイトの管理:**指定したサイトを許可または拒否で管理します。

イベント

行動管理の検知結果はイベントページで表示されます。[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できます。



## 高可用性 (HA)

二台以上の Ark-UTM を HA グループに設定すると、ネットワーク異常が発生した際に自動的に切り替わり、ネットワークの中断がなくなります。

LIONIC Security Statution Provider						
ark-UTM 16	👗 高可用性 (HA)					
≣ ダッシュポード						
WAN	高可用性 (HA)					
H LAN	二台以上のArk-UTMを 断されなくなります。	HAグループにする	らと、ネットワーク異常	常が発生する際に自	動的に切り替け	えで、ネットワークが中
ミキュリティ	<b>注意</b> :本番機の設定は	HA機能で自動的に	同グループ内の同じハ	(ージョンの予備機	に同期します。	
≧ セキュリティ機能	有効					
- ● 育成ログ	Ark-UTMごとにグルー どうかを確認してくだ	ブIDとパスワード さい。グルーブID	を設定し、下記の[グル が同じでもパスワード:	レープメンバー]のう が異なる場合、別々	Fーブルを通じ 2 のグループに	でグループに参加するか なります。
ネットワーク管理	(1) - TID 10					
■ 資産管理	-500-510	55				
J	パスワード		7	ĸ		適用
1. 行動管理	グループメンバー					
アドバンス設定	MAC	IP	SN	バージョン	状態	前回の起動時間
1. 高可用性 (HA)	利用中の機器					
VPN	AABBCC0CF5F2	10.10.27.87	LIEI23112100087	1.4.1		
• システム	準備中の機器					
■ ユーティリティ			メンバー	なし		
<						

高可用性 (HA)

- 有効: [高可用性 (HA)]のスイッチです。デフォルトでは無効になっています。
- **グループ ID**: グループ ID を設定します。範囲は 1~255 です。
- パスワード:グループのパスワードを設定します。

HA 機能を使用するすべての Ark-UTM 16 で、[グループ ID]と[パスワード] を設定してく ださい。その後、[グループメンバー]のテーブルで正しいグループに参加しているか確認 します。[グループ ID]と[パスワード]が一致している場合、[グループメンバー]のテーブル に他の HA グループメンバーが表示されます。一方、[グループ ID] が同じでも [パスワー ド]が異なる場合は、別々のグループが形成されます。

#### 設定の手順:

手順1:2台 Ark-UTM 16の WAN IP アドレスを設定し、同じプライベートネットワークに設置されることを確認します。



手順 2: 番号 1 の Ark-UTM 16 の LAN ポートをパソコンまたはノートパソコンに接続します。

手順3:ブラウザーで https://myark.lionic.com/をアクセスします。

手順4:管理画面にログインして、[高可用性(HA)]のページにアクセスします。

手順 5: [有効]をクリックして、グループ ID(1~255)とパスワードを入力して、[適用] をクリックします。

手順6:設定完了後、番号2のArk-UTM 16のLAN ポートをパソコンまたはノート パソコンに接続します。手順3と手順4を繰り返します。

手順7:[高可用性(HA)]のページにて、[有効]をクリックして,番号1と同じグループ IDとパスワードを入力して、[適用]をクリックします。

手順8:設定完了後、2台の Ark-UTM 16の LAN ポートを同じネットワークスイッチ に接続します(下図のように)。これで HA の設定が完了します。



HA のネットワーク構成図

\* 付記: Active の Ark-UTM 16 のセキュリティ機能の設定を変更すると、 同グループ内で同じファー ムウェアバージョンの Ark-UTM 16 は全て自動的に同期されます。



## VPN サーバー

この VPN の機能で Ark-UTM 16 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 Ark-UTM 16 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。

ark-UTM 16	• VPN
ダッシュボード	
WAN	VPNサーバー
LAN	WireGuardのクライアントアプリをモバイル海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AdvalのAdvitica」レニィの様を受けられます
	注意、DNS が必要な場合、新しいプロファイルを追加する前に DDNS を確実してください。
≧ セキュリティ機能	VPNサーバーを起動する
<ul> <li>         ・ ・ ・</li></ul>	二段階認証を有効にする 有効にした場合は、WinGuard のクライアントを接続した後、http://b01072011/ata/vanにアクセスし、ワンタイルパスワードを入
ットワーク管理	Solic Of Helles Introduce OFFIFIFIELDARON Care Indepted and Control Field Processing Street Field Control Field Street
<ul> <li>■ R体 E 体</li> <li>・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	
有動管理	+ 新しいフロファイルを追加する
ドバンス設定	707r-1µ1 / X
。高可用性 (HA)	オフライン 2011年1月10日日 100000000000000000000000000000000
VPN	
) > <b>Z</b> 76	
ユーティリティ	

VPN サーバー

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:

- 手順一:[VPN サーバーを起動する]を有効にします。
- 手順二:[+新しいプロファイルを追加する]をクリックします。
- 手順三:
  - 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。
- Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16 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、Ark-UTM 16 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:

- 手順一: [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。
- 手順二:[+新しいプロファイルを追加する]をクリックします。
- 手順三: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。
- 手順四:OTP アプリで二段階認証の QR コードをスキャンします。
- 手順五:
  - 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:



手順一:WireGuard クライアントを開き、VPN を接続します。

手順二:OTP アプリを開き、ワンタイムパスワードを取得します。

手順三:ブラウザーで<u>https://myark.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 Ark-UTM 16 からインターネットにアクセスできるようになります。



システム

## デバイス

ark-UTM 16	• システム			
ダッシュボード	デバイス サーバ 通知 ファール	ウェア亜新 設定値の保存と復立	パフロードの空声 一般研究	原原 サマリーレポート
ZAN			7007 10304 B/200	
LAN	ライセンスの管理			
U∓∢	ライヤンスのは空 アクティス			
マキュリティ機能	ライセンスの方効明度 2005年4月	17日 14:45:25		
滅ログ	2020447	J/EI 14.40.50		
7-7世理	ライセンス更新のコード AAAA-BE	BBB-CCCC-DDDD		递用
庭管理				
トラフィック	日付と時刻			
動管理	日付と時刻	Wed Jan 8 10:34:55 CST 2025		
シス語定	タイムゾーン	Asia/Taipei	~	
可用性 (HA)	インターネット時刻サーバと同期する	0.pool.ntp.org	0	
VPN		1.pool.ntp.org	٥	
システム		2.pool.ntp.org	Ð	
ユーティリティ		3.pool.ntp.org	0	+ 第川

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 夜家大马	ライセンスサーバに問い合わせできません。
1、11、11、11、11、11、11、11、11、11、11、11、11、1	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 Ark-UTM 16 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: Ark-UTM 16 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

Ark-UTM 16 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



サーバー

ark-UTM 16	• システム			
<b>ボ</b> ダッシュボード	デバイス サーバ 通知 ファームパ	1ェア更新 設定値の保存と復元	パスワードの空車 管理の	周囲 サマリーレポート
⊕ WAN				
t lan	ライセンスの管理			
¥⊐IJデイ	ライセンスの状況 アクティベ	ートしている		
セキュリティ機能	ライセンスの有効期限 2025年4月	7日 14:45:35		
脅威ログ				10.00
~ワーク管理	ライゼンス更新のコート AAAA-BB	BB-CCCC-DDDD		280开1
真産管理				
<b>トラフィック</b>	日付と時刻			
7動管理	日付と時刻	Wed Jan 8 10:34:55 CST 202	5	
282	タイムゾーン	Asia/Taipei	~	
可用性 (HA)	インターネット時刻サーバと同期する	0.pool.ntp.org	0	
N		1.pool.ntp.org	0	
גדע		2.pool.ntp.org	Ċ	
ューティリティ		3.pool.ntp.org	0	+ 通用
<				

システム-サーバー

## CMS

CMS は複数の Ark-UTM 16 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、Ark-UTM 16 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 Ark-UTM 16 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。Ark-UTM 16 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、 Ark-UTM 16 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、Ark-UTM 16 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 Ark-UTM 16 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、各設定値を入力した後、[適用]をクリックしてください。

	HAU			
	サーバIPアドレス	IP アドレス		
Ark-UTM 16				
- Alarkan 18-12	ボート	514		
	プロトコル	UDP	•	
⊕ WAN	アドバンス設定 >			38/11
H LAN				
セキュリティ				
セキュリティ機能	SNMP			
● 脅威ログ	有効			
ネットワーク管理	バージョン	v2c	~	
資産管理	MIBファイルをダウンロード	↓ <i>∛</i> ウン□−ド		
▲ トラフィック				
<u></u> 行動管理	SNMPv2c			
アドバンス設定	727-74	a della		
👗 高可用性 (HA)	121-714	public		
C VPN	アクセスできるIPアドレスリス	h IPv4	+ 追加	
○ システム				
🖬 ユーティリティ				通用
<				



#### 通知

[通知]機能を使用すると、Ark-UTM 16 が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したり、指定された LINE アカウントへ LINE メッセージで通知し たりできます。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。

Ark-UTM 16	• システム		
ダッシュボード		20 ファーノウェア用料 設す途の点々と道言 パフロードの水用 酸锶の用用 サブリーレゼート	
WAN	57/12 5-7/ 18	N ファームフェア支付 MOEDBOARTCRON バスフードの支支 単元の開始 ライワーレルート	
AN		247	
71		口不超 >	
キュリティ機能			
成ログ	メール通知		
ワーク管理	頻度	□ 毎月 □ 毎週 □ 毎日 □ 脅戦が検知された際	
自在管理	SMTPサーバ	smtp.mail.com	
ラフィック	SMTP#	75	
)管理	SMILW- F	23	
ス設定	SMTPアカウント	user@mail.com	
可用性 (HA)	SMTPパスワード	パスワードを入力してください	
	通知先	user@mail.com テストする 適用	
7L			
ティリティ	LINE Notify		
<	Token トークンを入力	ください 通知	

システム-通知

#### 言語

通知メール、統計レポート、および LINE メッセージの内容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。

LIONIC Security Solution Provider	_							
	言語	日本語 🗸						
冒 ダッシュボード								
⊕ WAN	メール通知							
H LAN	相度	□ 毎月 □ 毎週 □ 毎日 □ 番岐が神知された際						
セキュリティ	SMTD#= //							
≧ セキュリティ機能	SMIPU-A	smtp.mail.com						
● 脅威ログ	SMTPボート	25						
ネットワーク管理	SMTPアカウント	user@mail.com						
資産管理	SMTPパスワード	パスワードを入力してください						
<b>ill</b> トラフィック	通知先	Liter@moil.com						
<b>土</b> 行動管理	10/10/0	uaergenten.com						
アドバンス設定								
▲ 高可用性 (HA)	LINE Notify							
O VPN	Tokenトークンを入力	にたさい 追加						
0 9772	LINE Notifyのサービスで脅い	LINE Notifyのサービスで脅威ログをUNEに送ります。LINE Notifyのサイトからトークンを取得ください。						
■ ユーティリティ								
<								

システム-通知-Line Notify

## LINE Notify

LINE メッセージで通知する場合、LINE Notify の公式サイトから LINE Token を取得し, Token のフィルターに入力し、[追加]をクリックした後、LINE アプリでリアルタイムに脅 威情報を受信できます。



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 Lurity SubJSun Provider	
Ark-UTM 16	• システム
ポード	デバイス サーバ 運知 <b>ファールウェア専新</b> 粉字体の存在と復元 パスワードの変更 管理の原因 サマリーレポート
	自動更新 今のファームウェアは最新のパージョンです。
4	
ュリティ機能	
にグ	手動更新 + アップロード
52 5	
管理	
フィック	
理	
ε	
1性 (HA)	
4	
ィリティ	
<	

システム-ファームウェア更新

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 Ark-UTM 16 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 Ark-UTM 16 だけでなく、他の Ark-UTM 16 に も復元できます。

トラブルシューティングや Ark-UTM 16 の配置台数が少ない時に使われます。



システム-設定値の保存と復元

\* 付記: Ark-UTM 16 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

Ark-UTM 16 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。

e Ark-UTM 16	<ul> <li>システム</li> </ul>	
<b>≣</b> ダッシュポード		
⊕ WAN	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 パスワードの変更 管理の原題 サマリーレポート	
H LAN	新レスリイスワード パスワードを入力してください	
🖹 セキュリティ機能	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 ディ 適用	
● 脅威ログ	· · · · · · · · · · · · · · · · · · ·	
ネットワーク管理		
📑 資産管理		
↓ トラフィック		
<b>土</b> 行動管理		
アドバンス設定		
👗 高可用性 (HA)		
C VPN		
〒 ユーティリティ		

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 Ark-UTM 16 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。

		〇 日本語 H
Ark-UTM 16	• <i>&gt;</i>	
ज ダッシュポード	デルイフ サール 連ね ファールウェア亜鉛 粉水池の身友と探索 パフロードの空草 <b>装装の展算</b> サブリーレポート	
⊕ WAN	2241X 2-1/ 2011 27-2222 Xell and Double 1001 1/X2-1/082X #460/802 242-0/K-1-	
H LAN	管理の服歴 (30)	
セキュリティ		
セキュリティ機能	日付と時刻 送償元P メッセージ	
● 育威ログ	2025/01/0810:34 10.10.27.27 Create VPN profile	
ネットワーク管理	2025/01/08 10:34 10:10:27:27 Enable VPN server	
📑 資産管理	2025/01/0810:33 10.10.27.27 Sign in	
<b>↓ </b> トラフィック	2025/01/0810:31 10.10.27.27 Change connection mode	
<b>**</b> 行動管理	2025/0/08 10:23 10:10.27:27 Sign in	
アドバンス設定	2025/01/081019 10.10.27.27 Burn firmware 66/66bf/92bc238564be6/508d07ca897	
👗 高可用性 (HA)	2025/01/081019 10.10.27.27 Upload firmware 89f96bf92bc238554be6f508d07ca897	
D VPN	2025/01/081014 10.10.27.27 Sign in	
0 \$2776	2025/01/081013 10.254.264.243 Sign in	
	2025/01/0810.06 10.10.27.27 Change connection mode	
■ ⊥- <del>7</del> 49 <del>7</del> 4	< 1 2 3 > 10 v H0/30	
,		

システム-管理の履歴

49



## 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。

<b>k-UTM 16</b> 이 シスラ	-4						
ボード	ス サーパ 通知	ファームウェア更新	所 設定値の保存と後	元 パスワードの変更	管理の履歴	サマ	マリーレポー
Ark-	JTM 16 サマリーレボ						
ティ機能 24時間	/ 7日間 / 30日間						
	Ark-UTM 日報			LIONIC			
	2020 4 01 /3 08 []						
(90	MAC / 5-1 AABBCC0CF5F2 202	センスの有効顧問 / 5 年 04 月 07 日					
	パージョン	141					
A)	アンチウィルスのパージョ	> 3.0.1100	システム負荷	サイバーリスク <b>低リスク</b>			
	<ul> <li>不正電へ100±00パージョ</li> <li>Web 費差防止のパージョ</li> </ul>	> 2.0.1616	0	Ŷ			
	检查级計畫器 988268	20484F88					
リティ	ファイル	URL	70-	パケット			

システム-サマリーレポート



## ユーティリティ

LIONIC Security Salution Provider		◎ 日本語 日	•
ark-UTM 16	■ ユーディリティ		
■ ダッシュポード	ソール、 コマンドラインツール、 システムログ シグタチャの声話 正反動 初期化		
⊕ WAN			
H LAN	ping v ipv4.google.com Run		
セキュリティ			
🗎 セキュリティ機能			
● 脅威ログ			
ネットワーク管理			
🚍 資産管理			
<b>山</b> トラフィック			
<b>よい</b> 行動管理			
アドバンス設定			
素 高可用性 (HA)			
C VPN			
• > <b>7</b> 5			
■ ユーディリティ			
<			

ユーティリティ

Ark-UTM 16 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。
- **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:** Ark-UTM 16 を再起動します。
- 初期化: Ark-UTM 16 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。

# Dual Ark-UTM 16 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.con

1F-C6, No.1, Lising 1st Rd., Science-Based Industrial Park, Hsinchu City 300, Taiwan, R.O.C.