LIONIC
Security Solution Provider

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

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

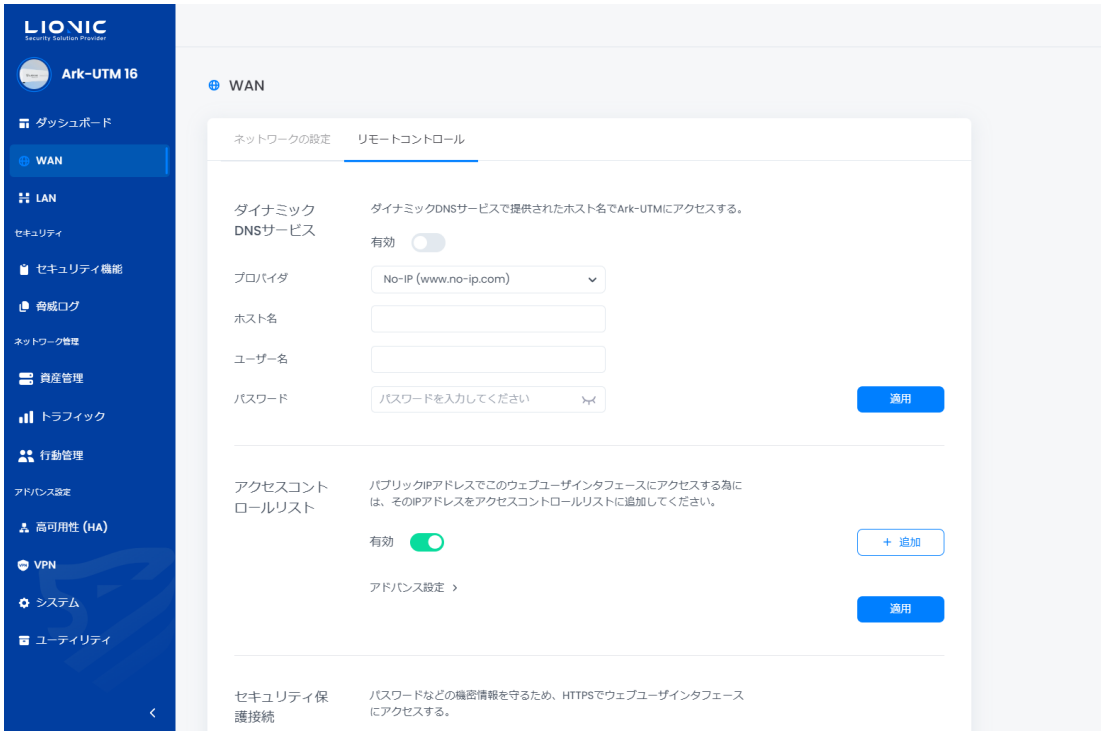
1. Ark-UTM 16 を電源に接続してください。
2. Ark-UTM 16 の WAN ポートと ISP から提供されたルーターの LAN ポートをイーサネットケーブルで接続してください。
3. Ark-UTM 16 の LAN ポートとパソコンまたはノートパソコンをイーサネットケーブルで接続してください。
4. パソコンまたはノートパソコンの IP 設定を以下のようにしてください
   - IP アドレス：10.254.254.50
   - ネットマスク：255.255.255.0
5. 設定完了後、ブラウザーで https://10.254.254.254/ にアクセスしてください。

ログインページ

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。
7. 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。

WAN-ネットワークの設定

8. 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。



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。

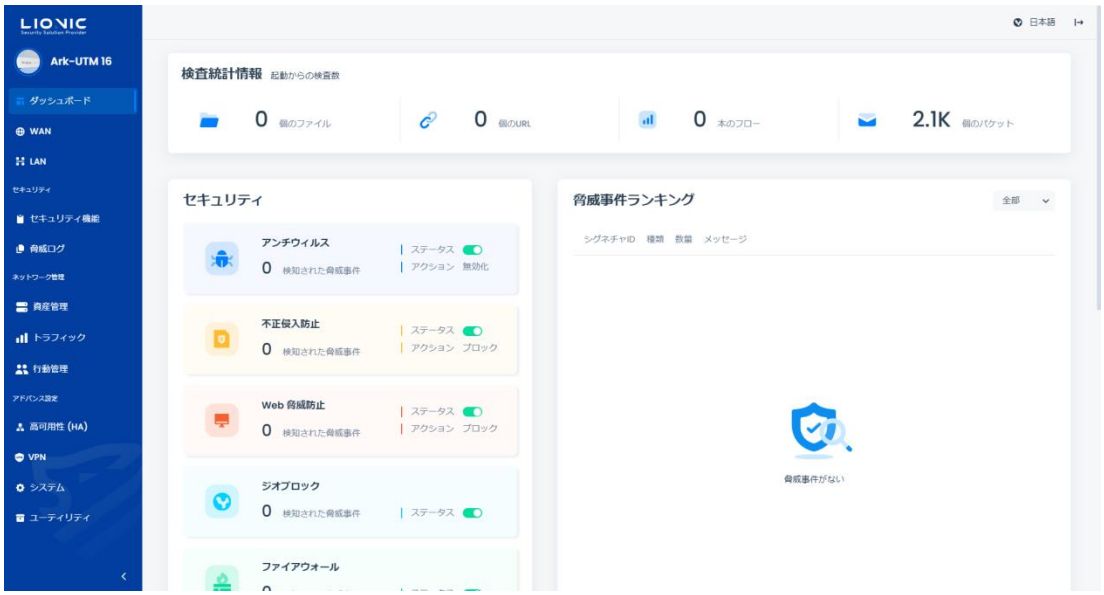
アドバンス設定：

- 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。

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。



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。

ダッシュボード-2

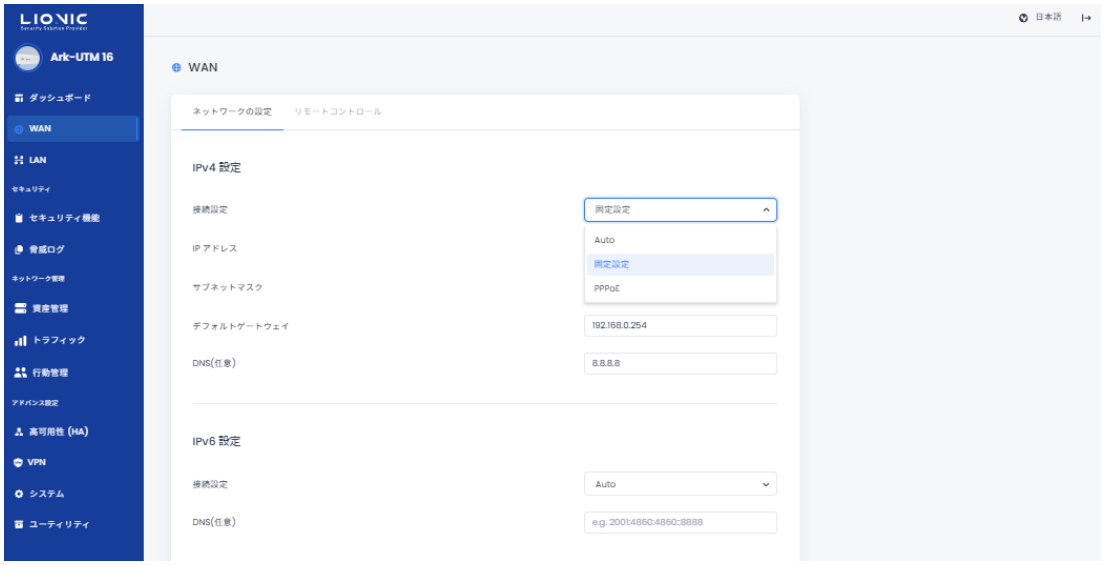
トラフィックモニター：Ark-UTM 16 を通過したアップロード/ダウンロードの通信速度とトラフィック量が表示されます。

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。



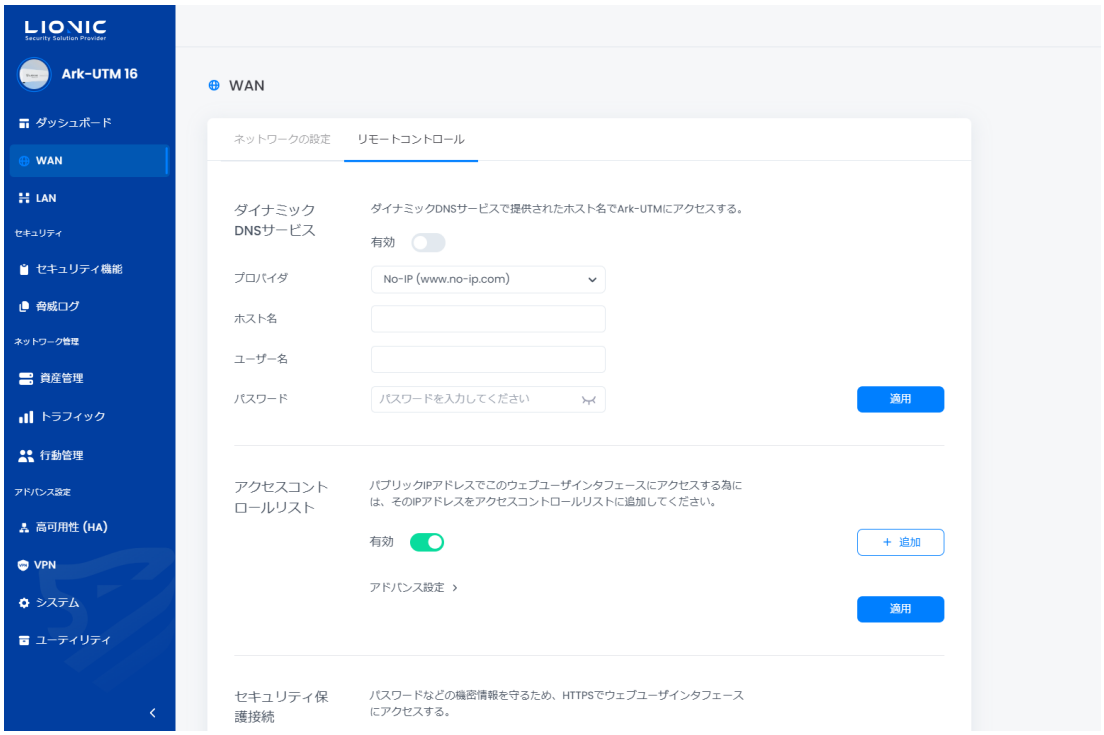
WAN-ネットワークの設定

- **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。



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。
3. 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。

リモートコントロール-セキュリティ保護接続

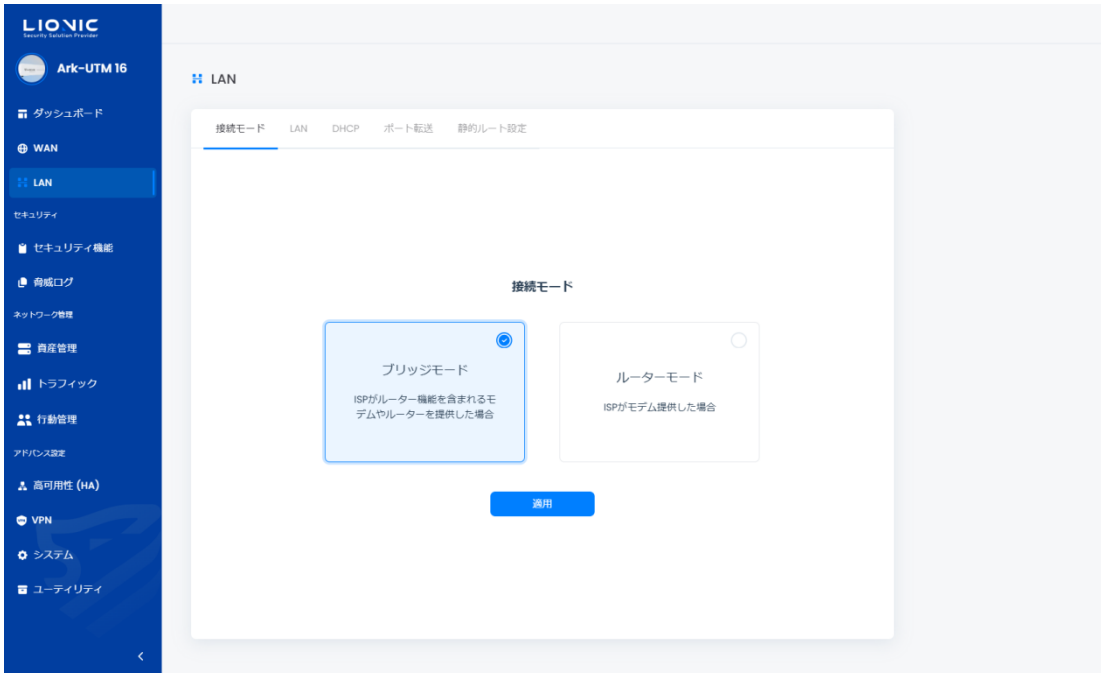
セキュリティ保護接続

[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。



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。

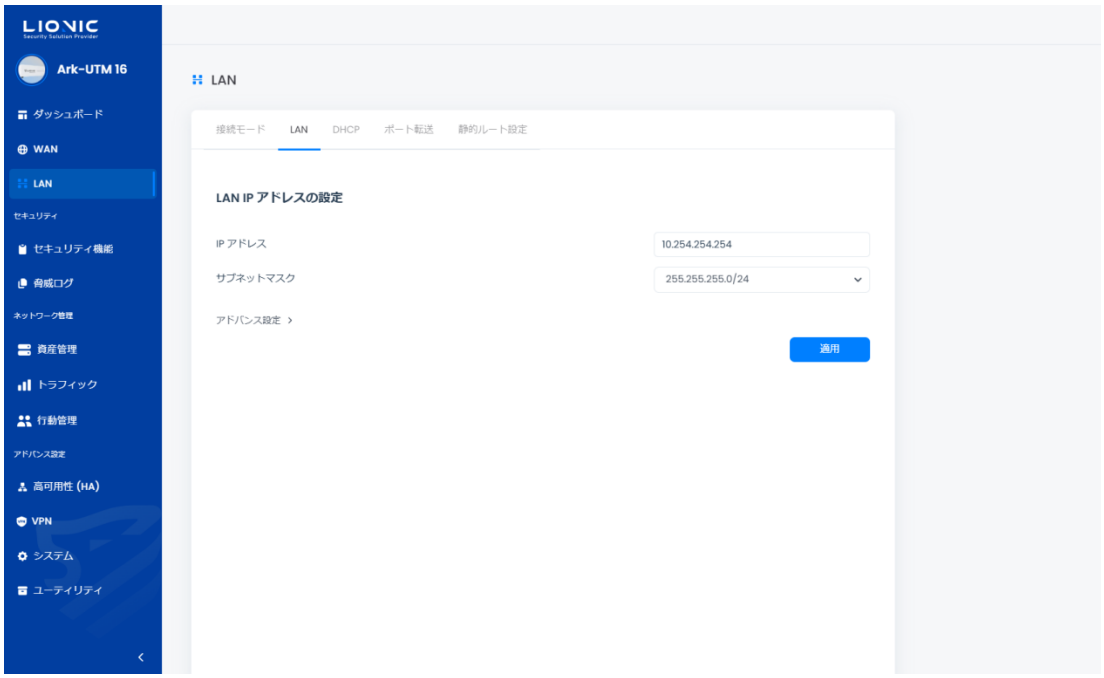
- **ルーターモード**

  [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。



LAN-LAN IP

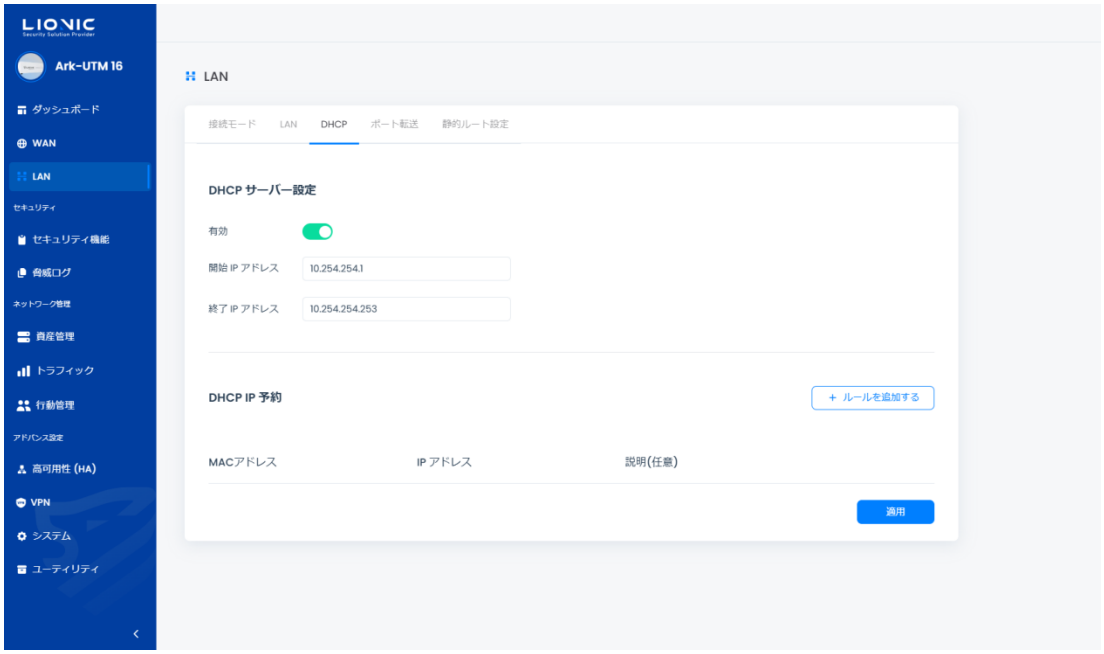
- **NAT なしのルーティング**

  [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。



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。

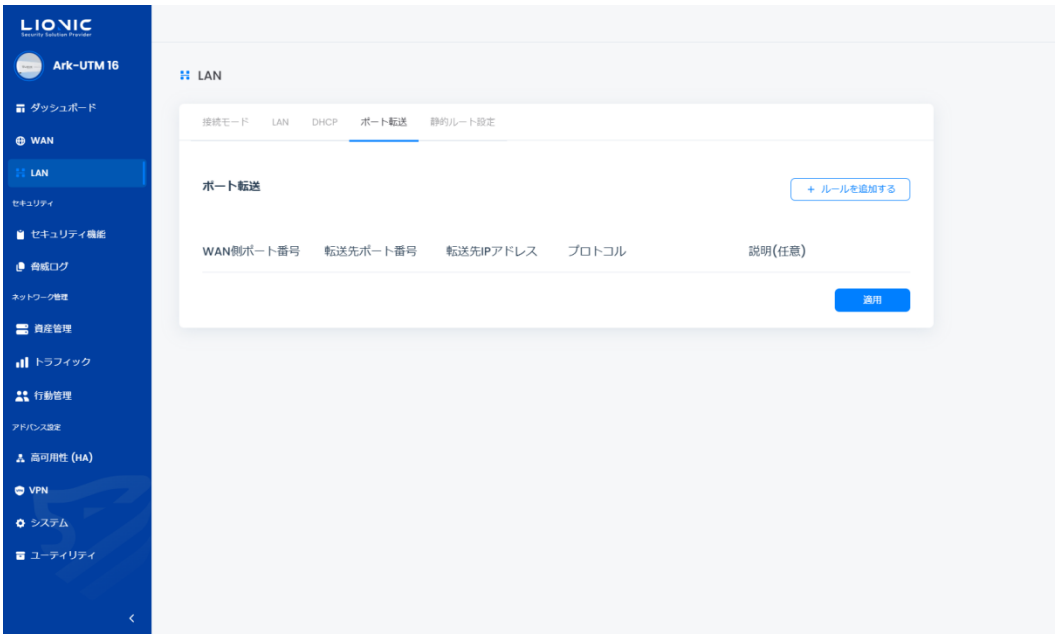
DHCP IP 予約

- 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

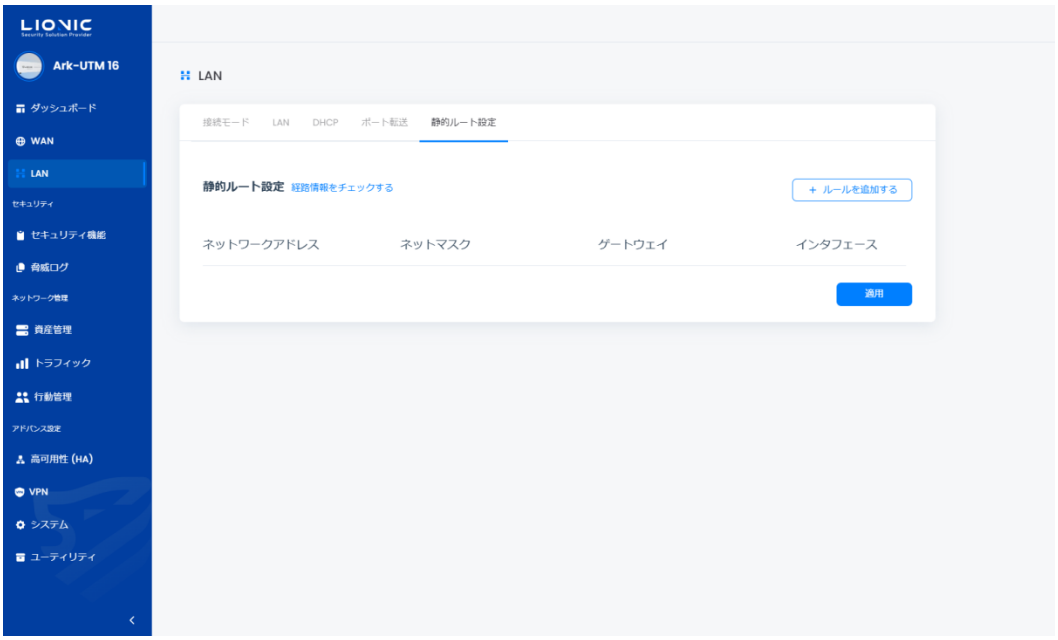
[ルーターモード]で Ark-UTM 16 はポート転送機能を提供します。WAN から LAN 側の装置をアクセスする際、この機能で特定のポート番号宛てに届いたパケットを LAN 側の装置に転送します。



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。



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。

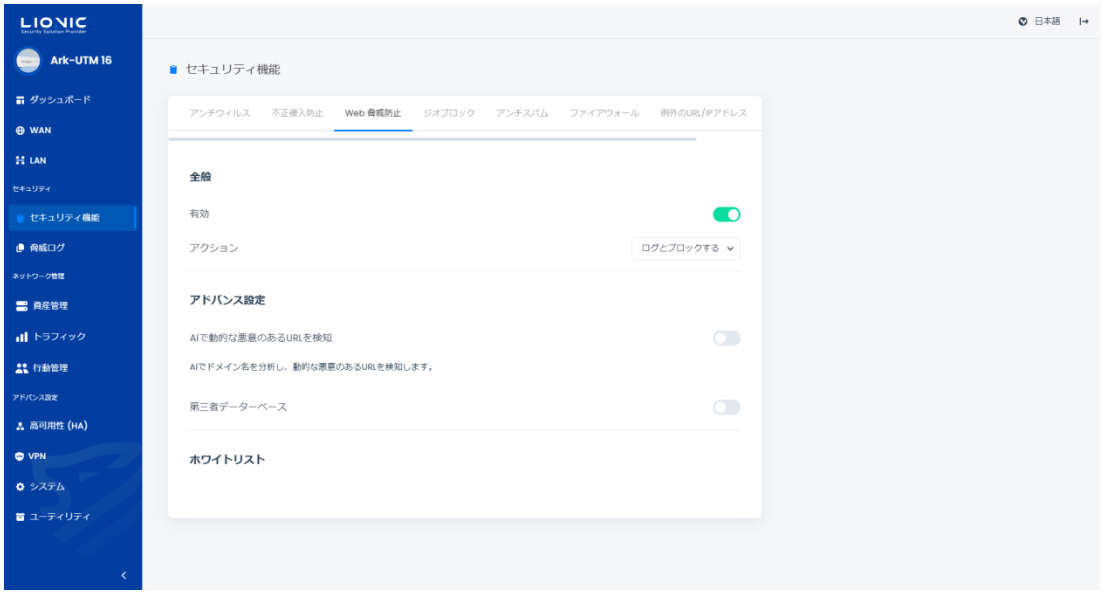
セキュリティ機能	アンチウィルス	不正侵入防止	Web 脅威防止
有効	有効 / 無効	有効 / 無効	有効 / 無効
アクション	ログ / ログとウィルスを無効化する	ログ / ログとブロックする	ログ / ログとブロックする
アドバンス設定	クラウドデータベースーでスキャンする AI で未知のウィルスを検知	総当たり攻撃の防止、プロトコル異常の防止、ポートスキャンと DoS 攻撃の防止、脅威が検出された場合には PCAP を保持する	AI で動的な悪意のある URL を検知 第三者データーベース
ホワイトリスト	ホワイトリストの一覧と削除	ホワイトリストの一覧と削除	ホワイトリストの一覧と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

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。

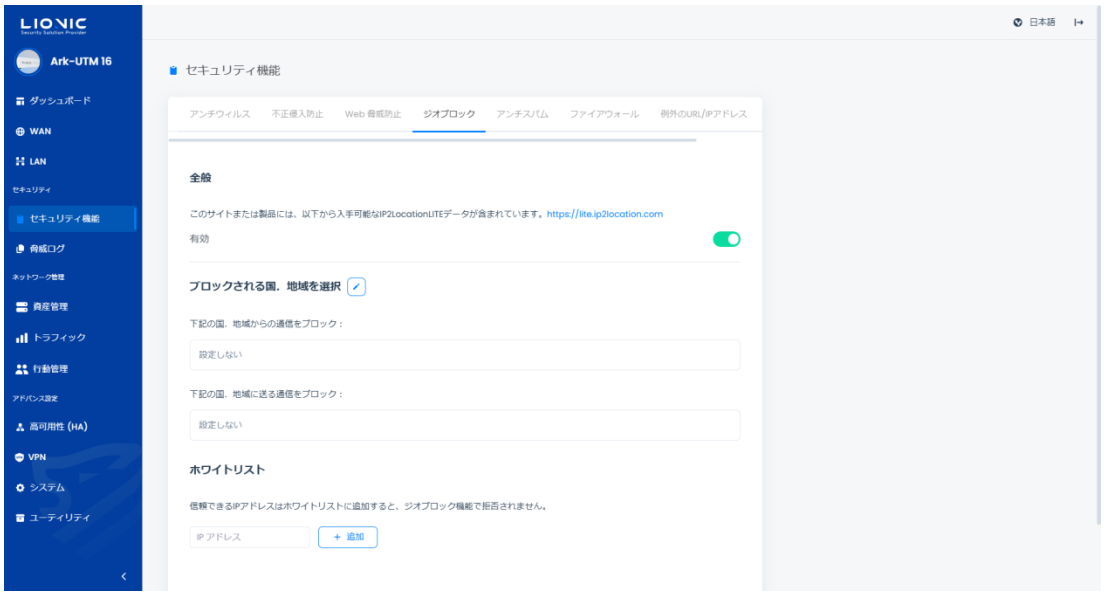
- **脅威が検出された場合には PCAP を保持する：**この機能を有効にすると、Ark-UTM 16 は[不正侵入防止]で脅威を検出した際に、脅威と見なされたパケットを保存し、後続の分析に使用できるようにします。
- **AI で動的な悪意のある URL を検知：**この機能を有効にすると、Ark-UTM 16 は接続先の URL とクラウドデータベースを照合し、人工知能 DGA 検出モデルを使用して、この URL が DGA によって生成された悪意のある URL かどうかを判定します。
- **第三者データーベース**:外部から悪意のあるサイトのリストをインポートできます。



- **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。



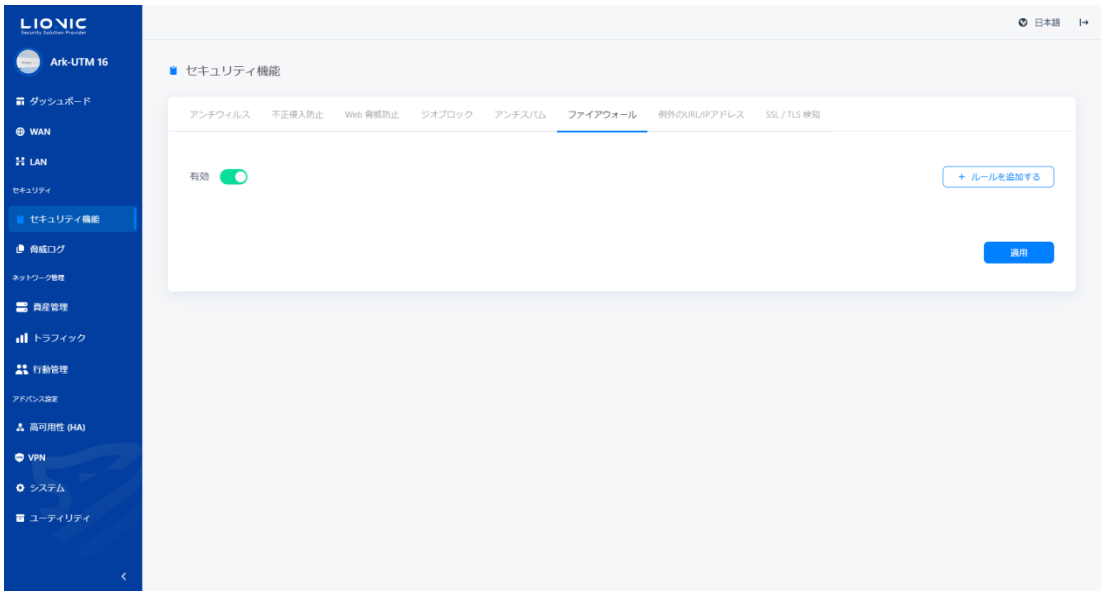
セキュリティ機能-ジオブロック

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。



セキュリティ機能-ファイアウォール

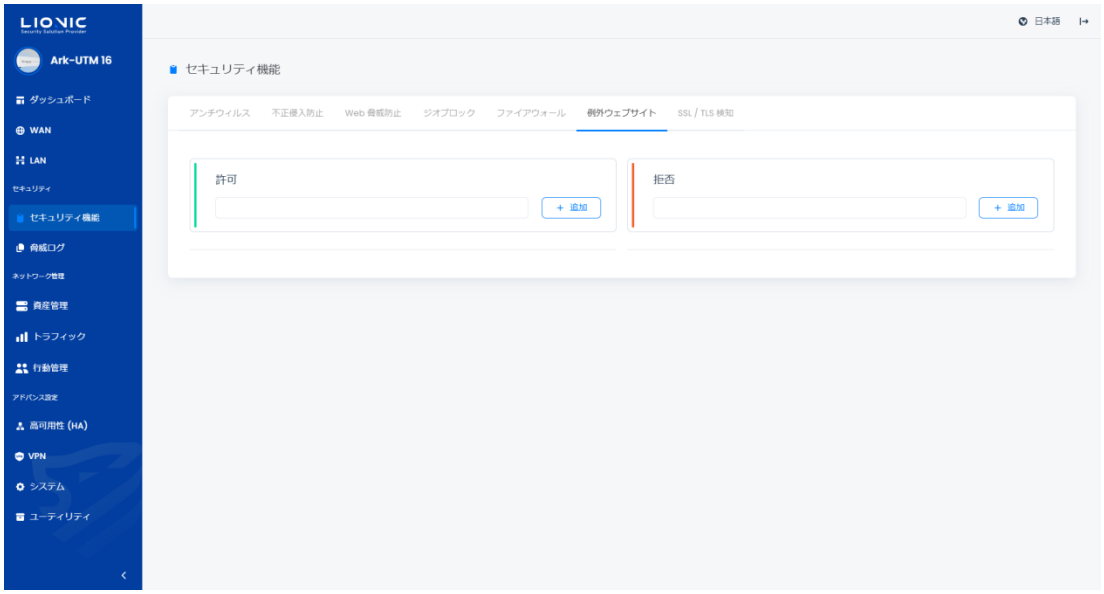
手順一：ファイアウォールを有効にします。（デフォルトは有効です）
手順二：[+ルールを追加する]をクリックします。
手順三：各フィールドに入力します。
手順四：[適用]をクリックした後、実行します。

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。



セキュリティ機能-例外サイト

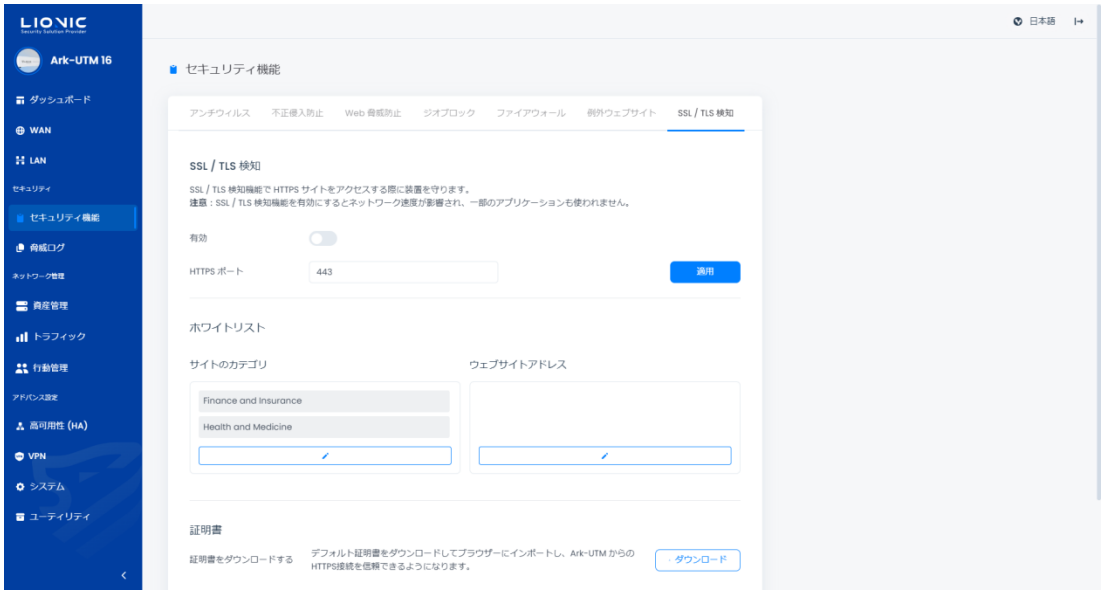
手順一：許可または拒否する予定の URL や IP アドレスを入力します。
手順二：[+追加]をクリックした後、実行します。

* 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。



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。

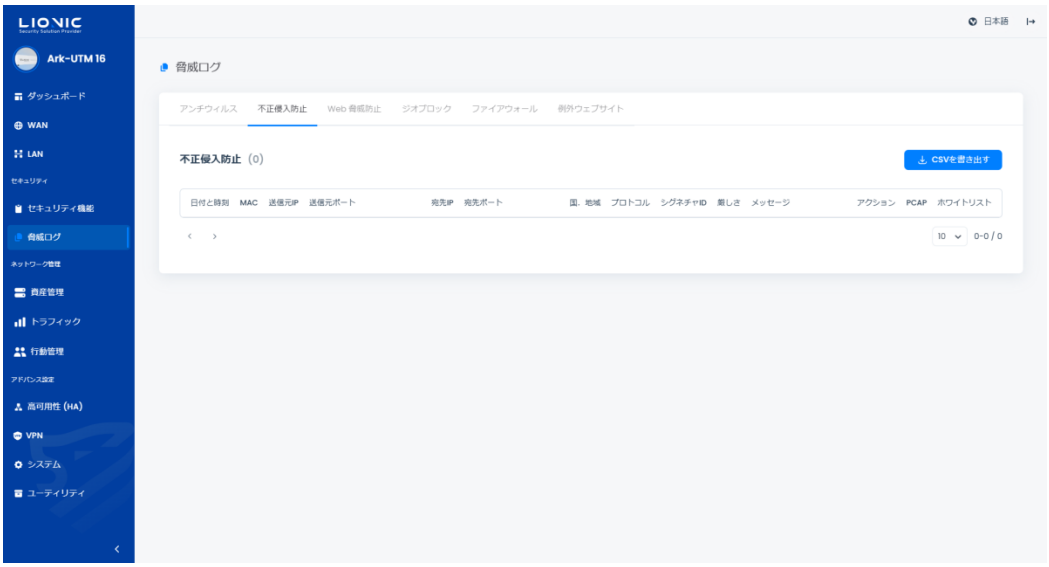
- **証明書をダウンロードする：**Ark-UTM 16 のデフォルトの証明書をダウンロードできます。この証明書をブラウザーにインポートすると、Ark-UTM からの HTTPS 接続を信頼します。
- **証明書のインポート：**独自の証明書を Ark-UTM にインポートすることで、接続の互換性を向上させることができます。

* 付記：

1. 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、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。

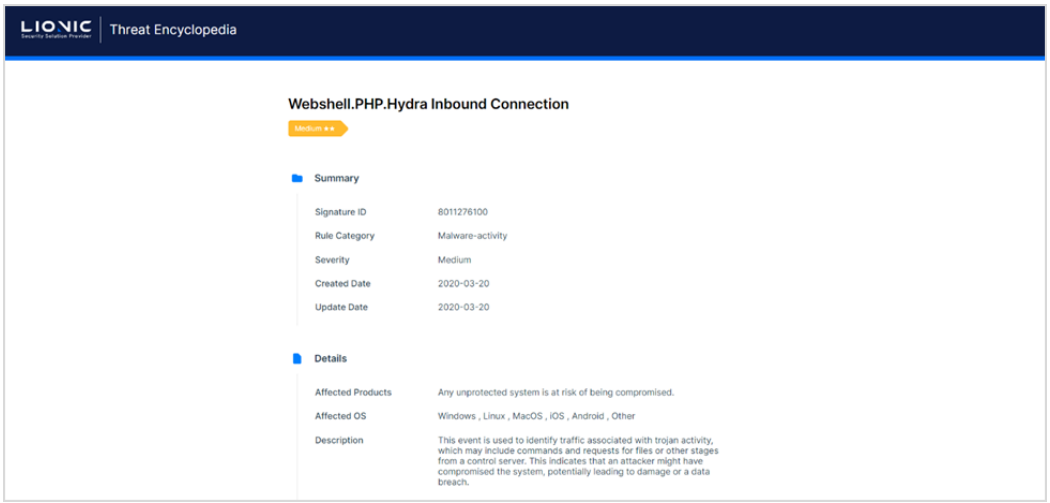
脅威ログ

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ます。



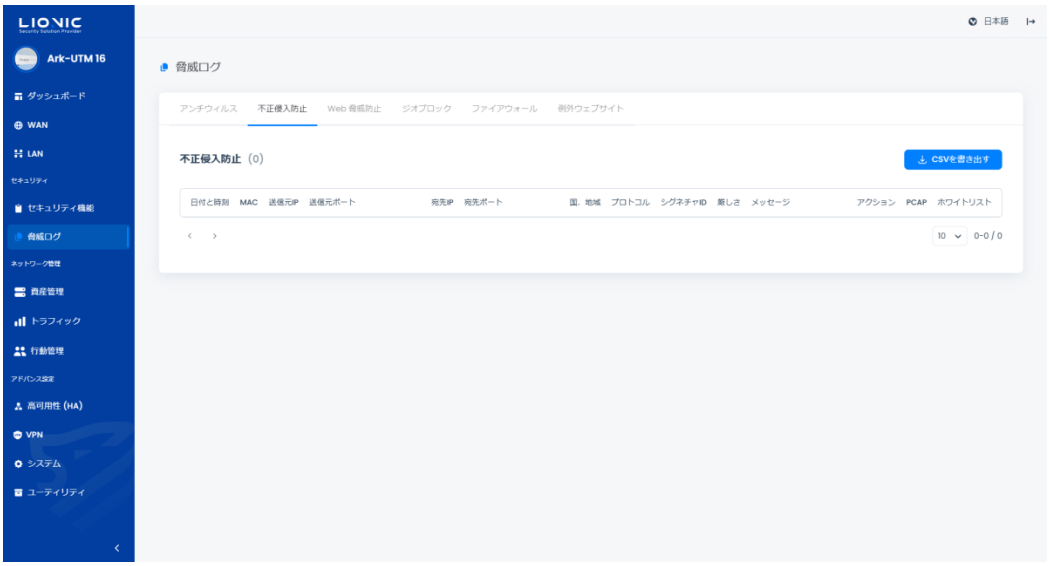
脅威ログ

- **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。



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。
-



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。

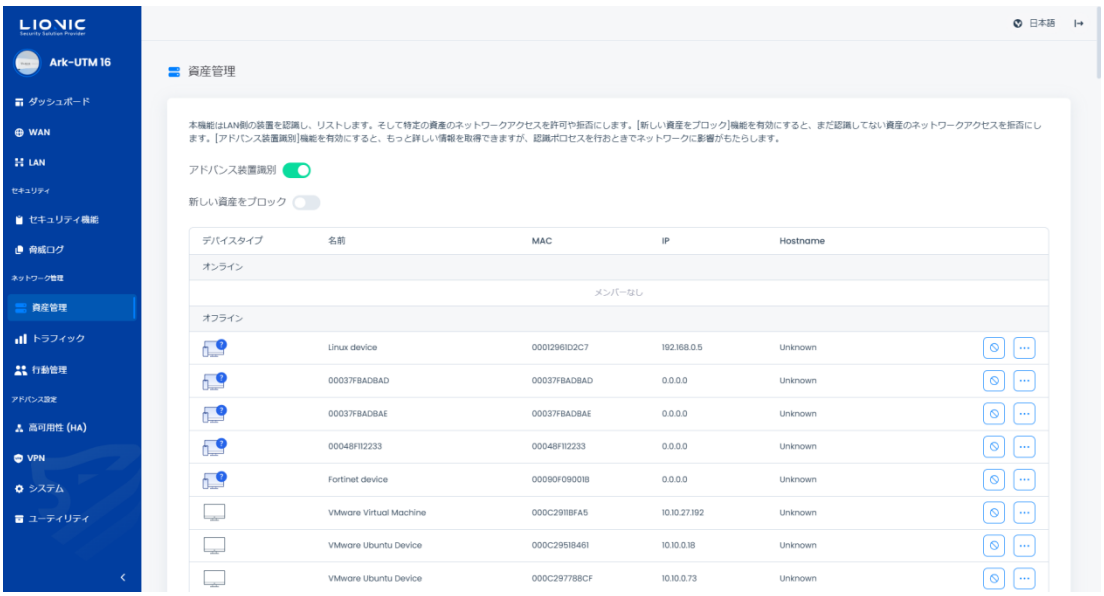
資産管理

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。



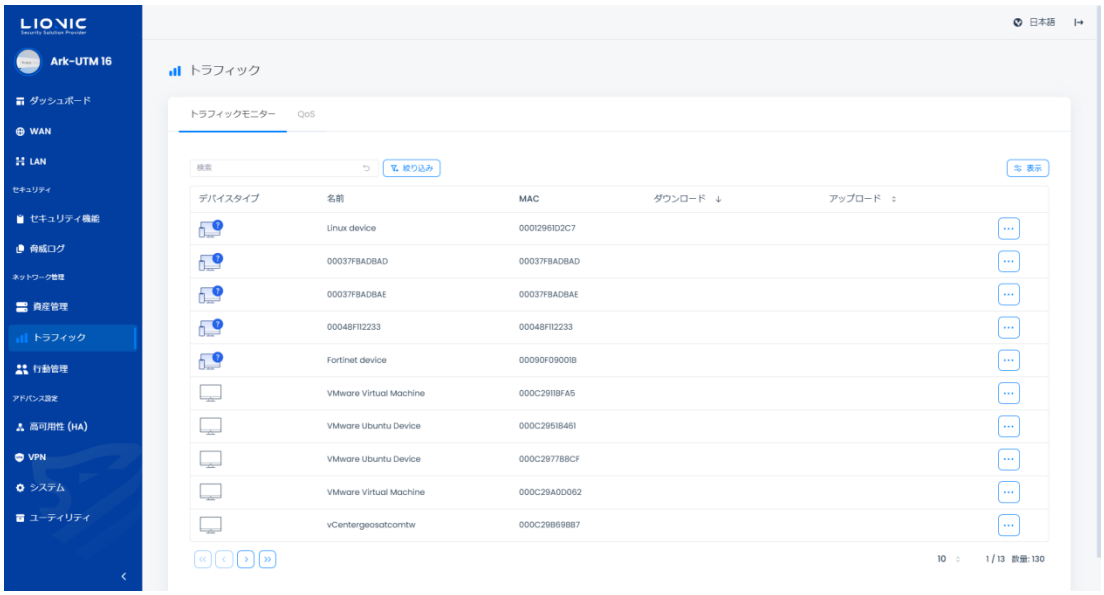
資産管理

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

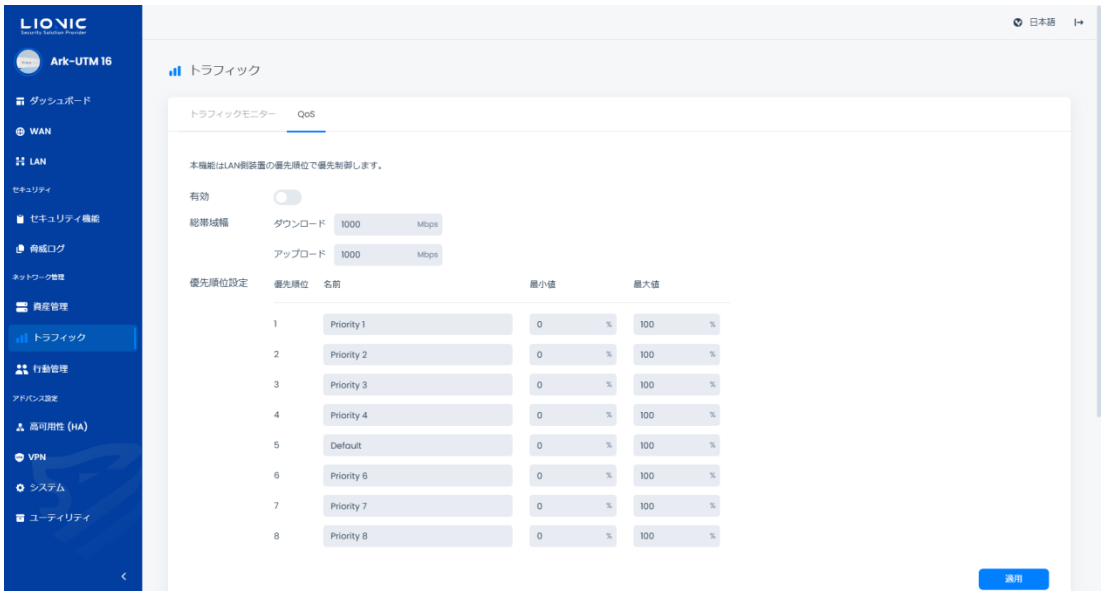
LAN 端末のリアルタイムのダウンロードおよびアップロードのトラフィックを表示し、多い順または少ない順に並べ替えて表示できます。



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。



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。

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。

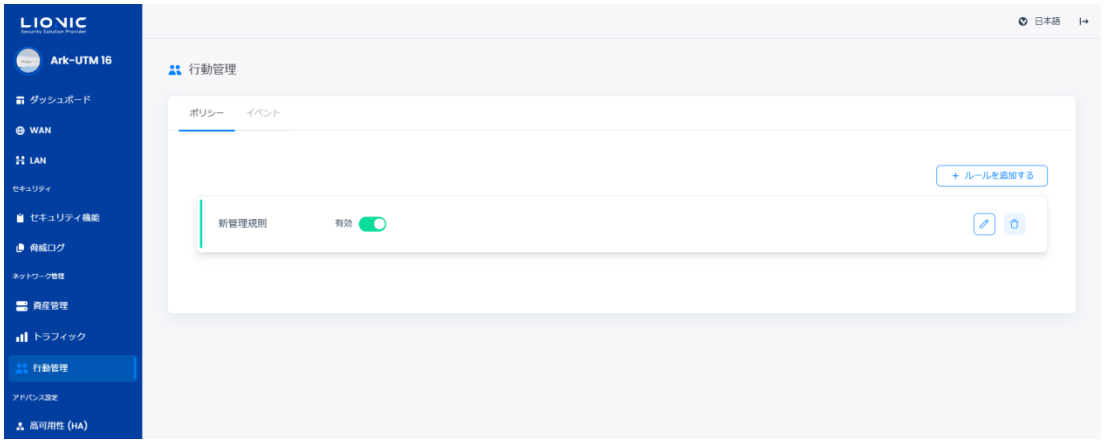
手順六：各フィールドに入力します。

手順七：[適用]をクリックした後、実行します。

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。



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。

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：

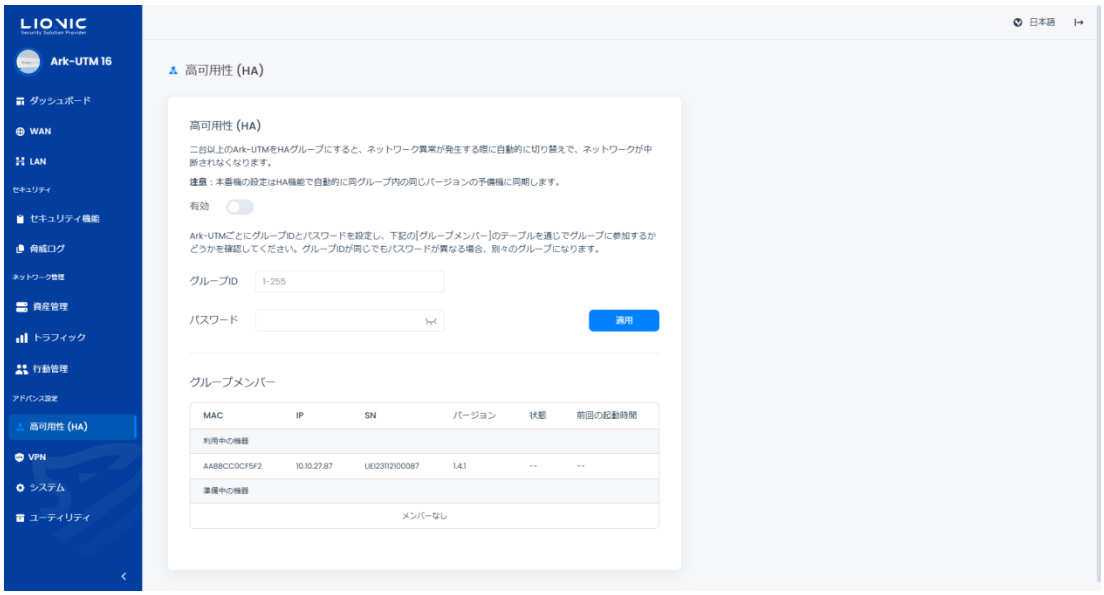
- 管理範囲：IP アドレスや MAC アドレスを設定して管理します。必須項目です。
- **ウェブサイト内容の管理：**ウェブサイトのコンテンツを管理します。
- **アプリケーションの管理：**アプリケーションを認識して管理します。
- **ウェブサイトの管理：**指定したサイトを許可または拒否で管理します。

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。



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。

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：

1. 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。
2. 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。

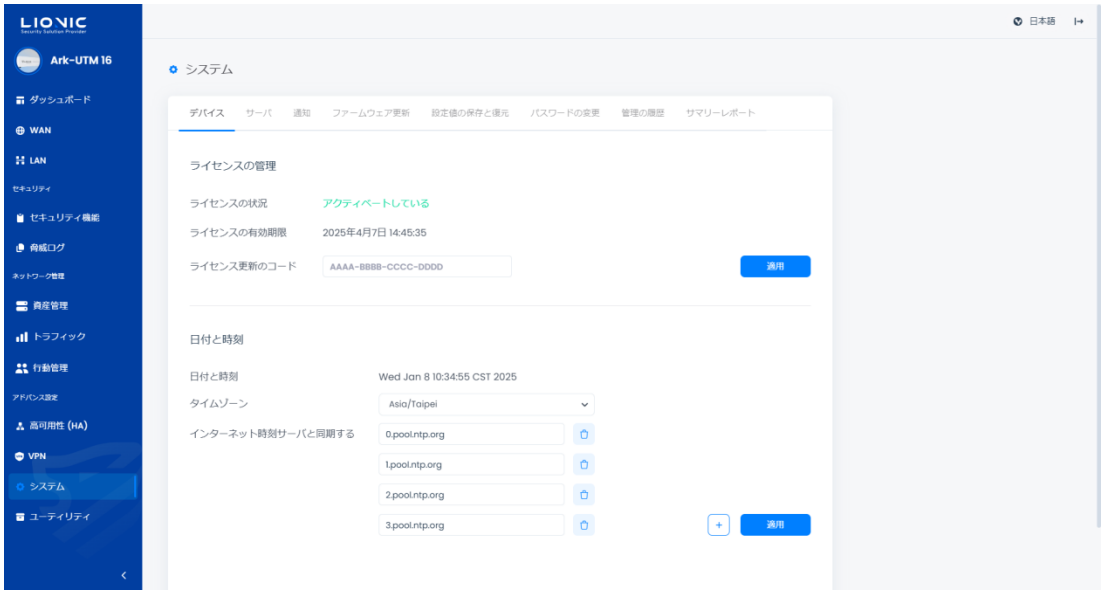
手順二：OTP アプリを開き、ワンタイムパスワードを取得します。

手順三：ブラウザーで https://myark.lionic.com/otp/vpn 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



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
状況確認エラー	ライセンスサーバに問い合わせできません。 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：

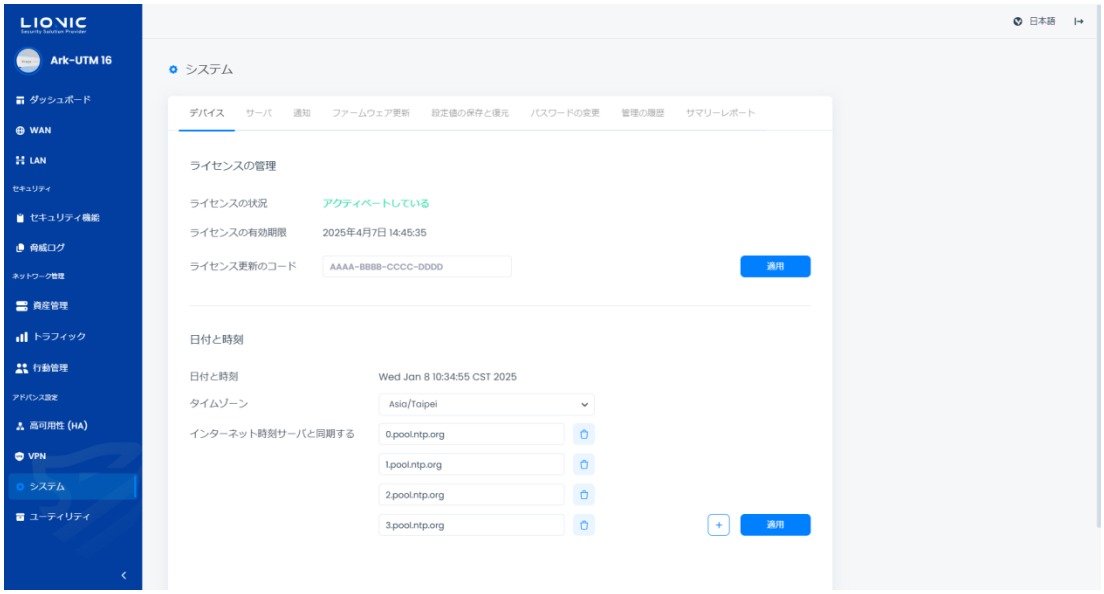
1. アクティベートコードは、半角英数字 20 文字で構成されています。適用に成功すると、ライセンスが有効になります。アクティベートコードが無い場合やアクティベートできない場合、ご購入の窓口にご連絡ください。
2. ライセンス更新のコードは、半角英数字 16 文字で構成されています。適用に成功すると、ライセンスの有効期限が延長されます。サブスクリプションをご希望の場合、ご購入の窓口にご連絡ください。

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



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

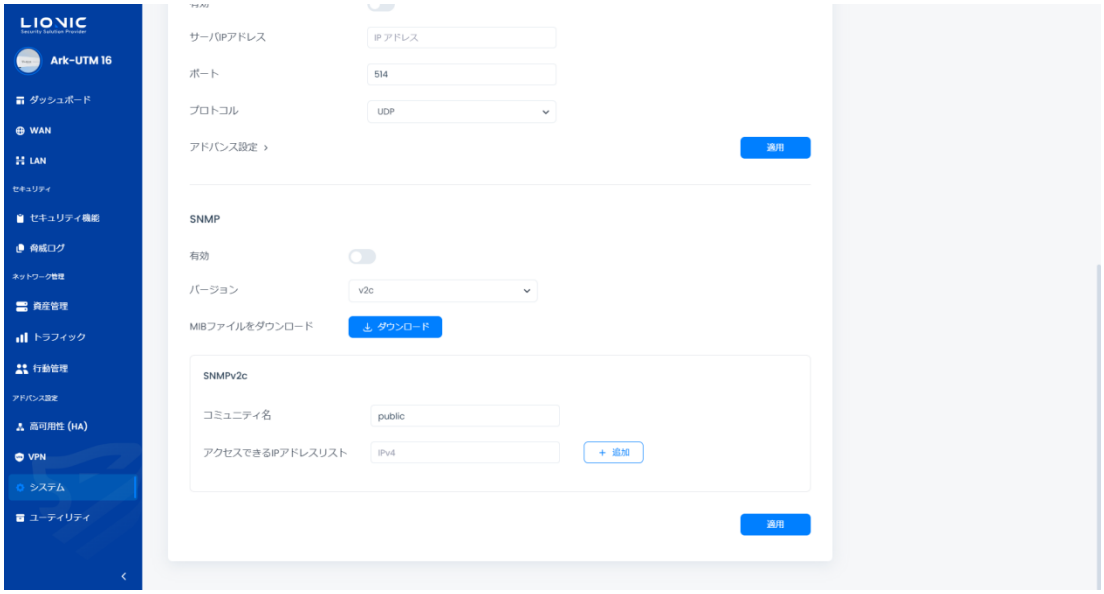
Proxy 機能は、インターネットに直接接続できない Ark-UTM 16 をサポートし、Lionic のクラウドサービスを通じて完全なセキュリティ保護機能を提供します。Ark-UTM 16 を内部ネットワークに配置する場合、Proxy のアドレスを入力し、[適用]をクリックすることで、Ark-UTM 16 はプロキシを通じて Lionic のクラウドサービスを利用できます。必要があれば、ネットワーク管理者にお問い合わせください。

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。

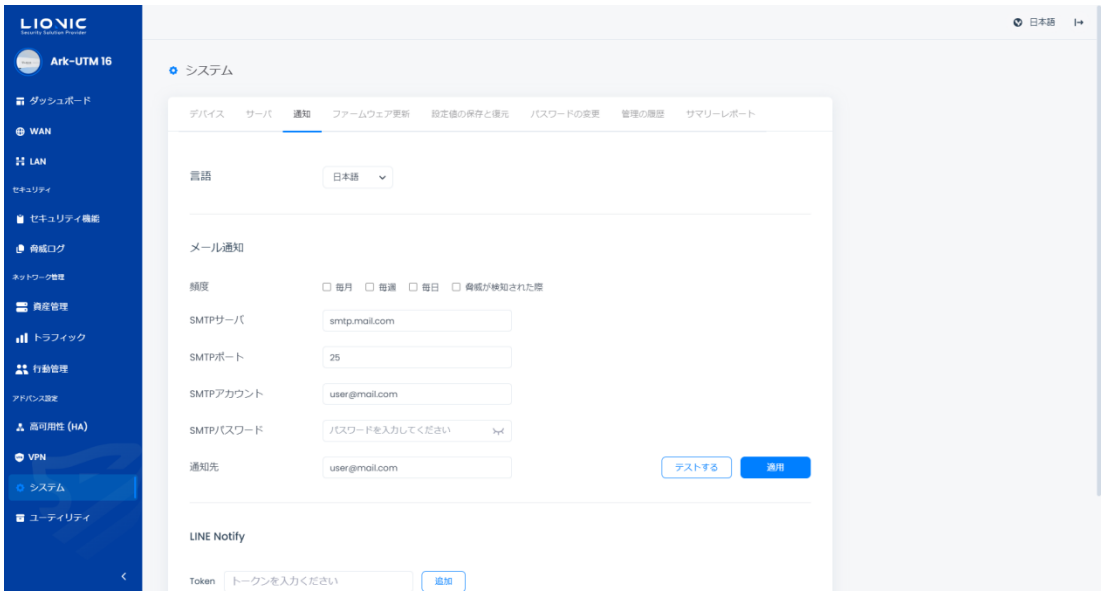
SNMP

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。



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。



システム-通知

言語

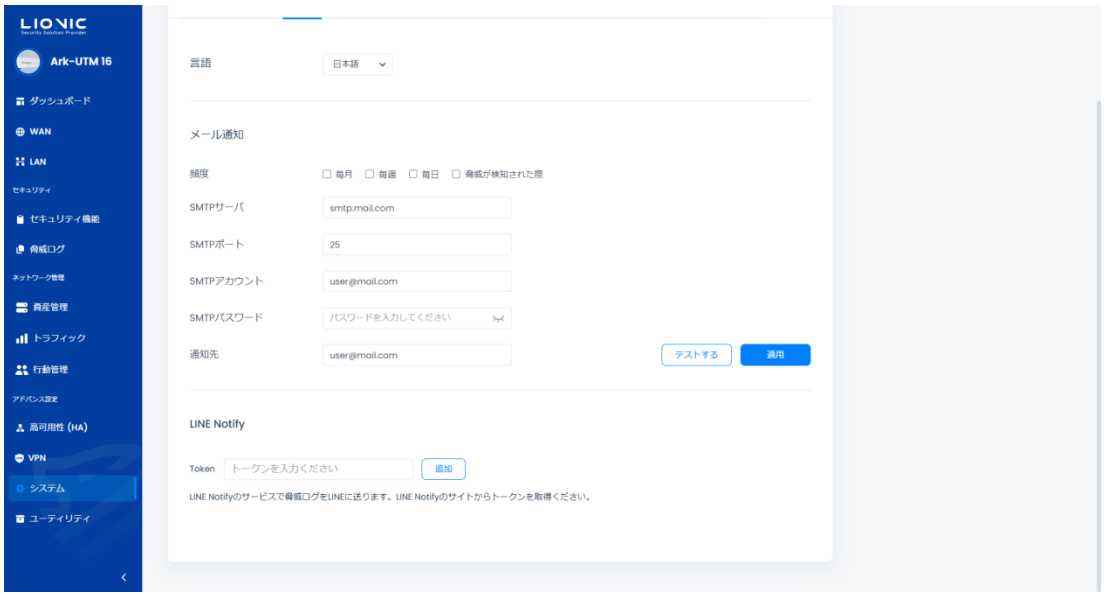
通知メール、統計レポート、および LINE メッセージの内容の言語を選択します (中国語/英語/日本語) 。

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。



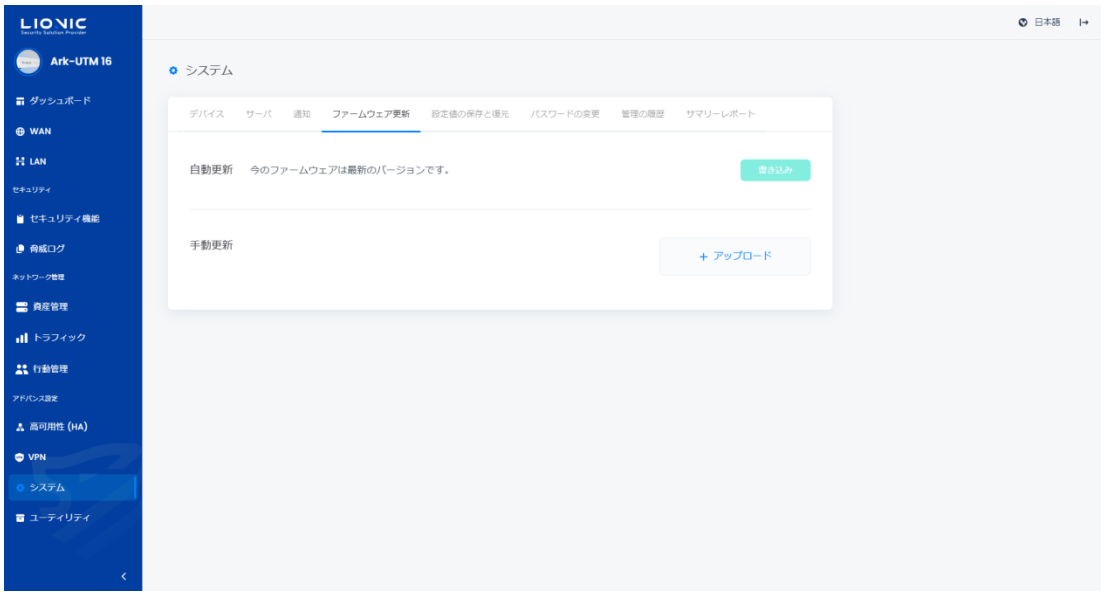
システム-通知-Line Notify

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。



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

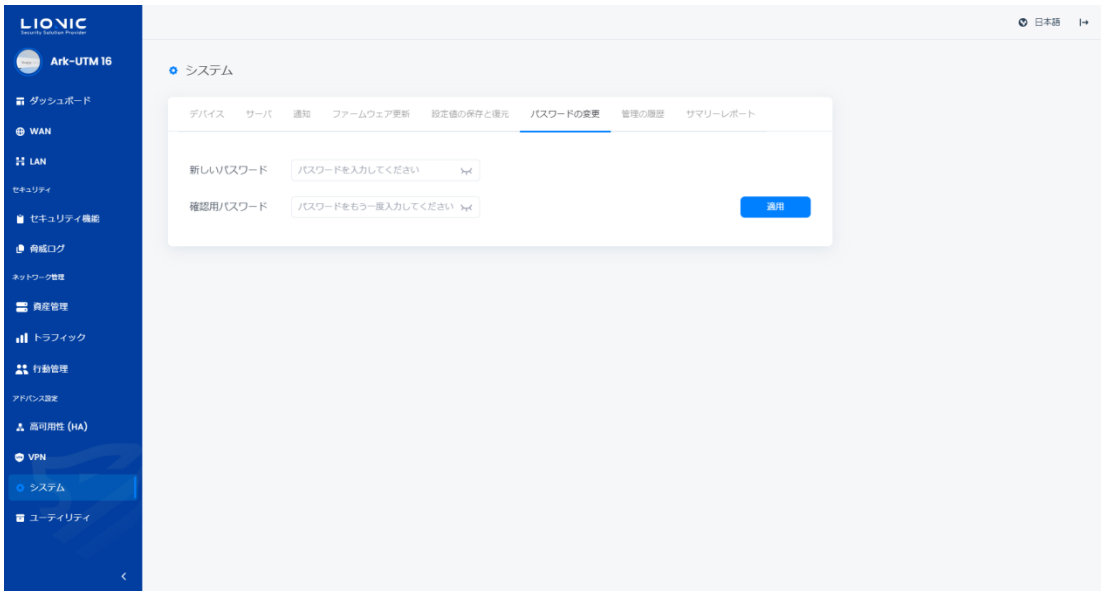
[設定値の保存と復元]この機能では Ark-UTM 16 の設定をバックアップします。
バックアップファイルは元の Ark-UTM 16 だけでなく、他の Ark-UTM 16 にも復元できます。
トラブルシューティングや Ark-UTM 16 の配置台数が少ない時に使われます。

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

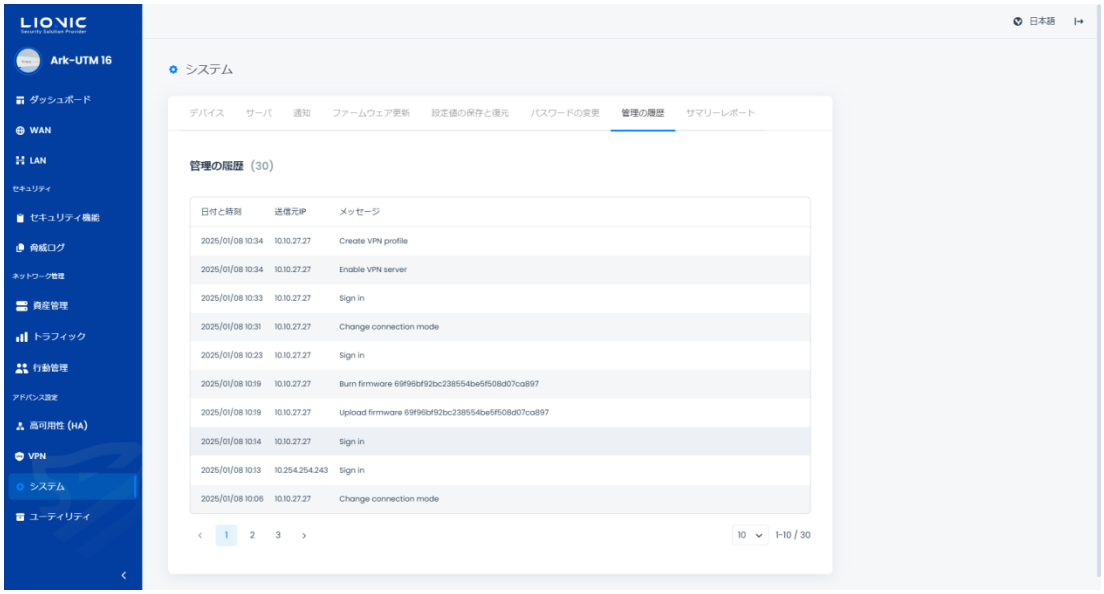
Ark-UTM 16 の管理画面のログインパスワードを変更する際、新しいパスワードを入力し、[適用]をクリックしてください。



システム-パスワードの変更

管理の履歴

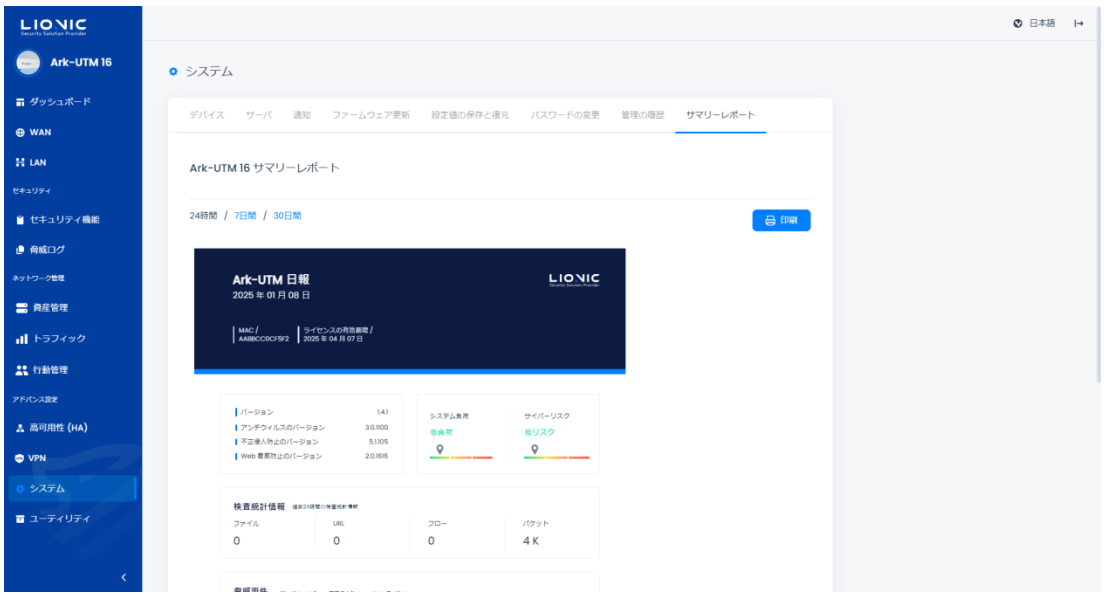
[管理の履歴]このページでは Ark-UTM 16 の管理者に対し、管理画面で設定変更の記録が表示されます。



システム-管理の履歴

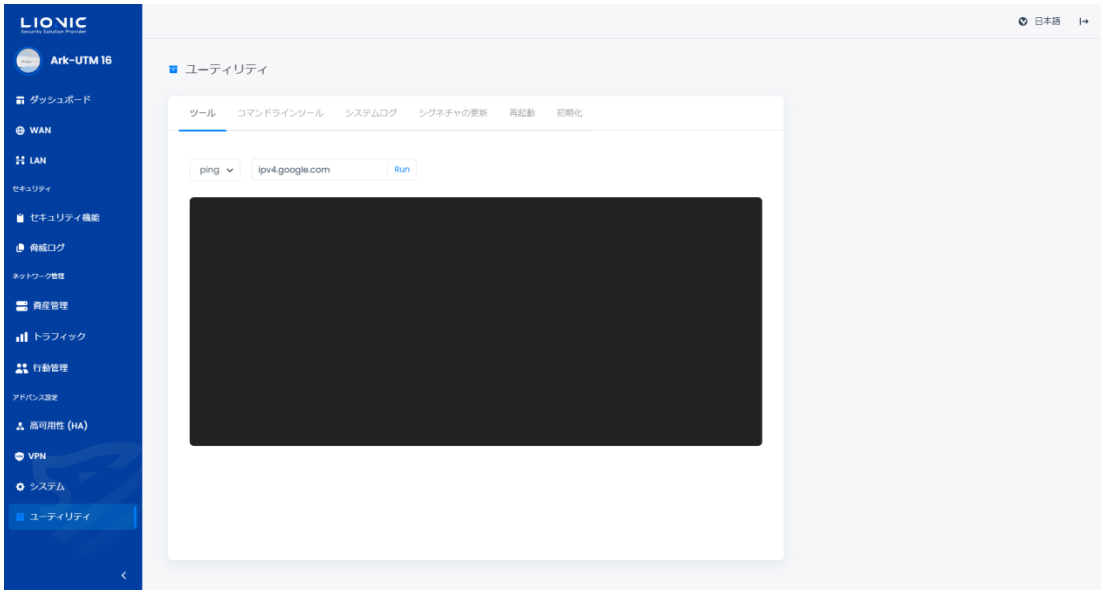
サマリーレポート

[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。



システム-サマリーレポート

ユーティリティ



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

LIONIC
Security Solution Provider

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.