

SUN CORPORATION

Rooster **NSX**

機能説明書

はじめに

本機能説明書では、Web 設定ツールについて解説しています。

本製品を活用するための参考資料としてご利用ください。

なお、LAN/WAN の配線、インターネットへの接続などの機能を使用する際の設定例については説明していません。

これらに関しては、下記の設定例集をご覧ください。

- <https://www2.sun-denshi.co.jp/config-example/>

また、Web 設定ツールはレスポンシブデザインを採用しており、ブラウザの設定で見え方が異なることがあります。

■ 表記について

本機能説明書では、安全にお使いいただくために、守っていただきたい事項に次のマークを表示しております。



人体に危険を及ぼしたり、装置に大きなダメージを与えたりする可能性があることを示しています。必ずお守りください。



機能停止を招いたり、各種データを消してしまったりする可能性があることを示しています。十分に注意してください。



関連する情報を記載しています。参考にお読みください。

■ 商標について

「Rooster」は、サン電子株式会社の登録商標です。

Oracle と Java は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。

その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。

本文中の各社の商標または登録商標には、TM、®マークは表示していません。

■ GPL / LGPLライセンスについて

本製品は、GPL / LGPL の適用ソフトウェアを使用しております。オープンソースとしての性格上著作権による保証はなされておきませんが、本製品につきましては保証書、および取扱説明書記載の条件により当社による保証がなされています。GPL / LGPL のライセンスにつきましては、以下の URL をご覧ください。

- <http://www.gnu.org/licenses/gpl.html>
- <http://www.gnu.org/licenses/lgpl.html>

変更済み GPL 対象モジュール、その配布方法につきましては、サン電子（株）サポートセンターにご連絡ください。なお、配布時発生する費用はお客様のご負担となります。

- ▶ 本取扱説明書の画面イメージは開発中のものです。実際の画面とは多少異なる場合があります。

安全上のご注意(必ずお守りください)

ここに記載している注意事項は、安全に関わる重要な内容ですので、必ず守ってください。本取扱説明書では、安全上の注意事項を「警告」と「注意」に区分しています。



警告

この表示を無視して、間違った取り扱いをした場合、人が死亡または重傷を負う可能性が想定される内容を示しています。



注意

この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関する拡大損害を示しています。



禁止

禁止行為（してはいけないこと）を示しています。



強制

強制行為（必ずしなければいけないこと）を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。いずれも重要な内容を記載していますので、必ず守ってください。

 **警告**

本製品を分解したり、改造したりしないでください。

→ 感電、火災、故障の原因になります。



近くに雷が発生したときには AC アダプタまたは電源ケーブルを本体から抜いてご使用をお控えください。

→ 落雷が火災、感電、故障の原因となるときがあります。



本製品に水などの液体をかけたり、異物を入れたりしないでください。

→ 感電や火災の原因になります。

万一、本製品に液体がかかったり、異物が入ったりした場合は、AC アダプタまたは電源ケーブルを本体から抜いて、点検修理を依頼してください。



製品から煙、異臭、異常音が発生した場合は、AC アダプタまたは電源ケーブルを本体から抜き、本製品を接続している機器からケーブルを取り外してください。また、点検修理を依頼してください。

→ 火災の原因になります。



電源ケーブルを傷つけないでください。

→ 感電、火災の原因になります。



AC アダプタは、AC100V コンセントに接続してください。また、本製品を設置、移動する時は、電源プラグを抜いてください。

→ 故障、火災の原因になります。



梱包のポリ袋などは、小さいお子様の手の届く所に置かないでください。

→ 小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げる危険があります。



電源プラグは確実に根元まで差し込んでください。また、電源プラグとコンセントの間のほこりは、定期的（半年に一回程度）に取り除いてください。

→ 電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災の恐れがあります。

 **注意****禁止**

この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないでください。

→ 本製品の故障や破損などによって、発煙、発火、感電の原因になります。下記の環境には、特にご注意ください。

- 製品周囲の温度や湿度が極端に高い、または低い場所
- 結露がある場所
- 急激な温度変化が起きる場所
- ほこりが多い場所
- 静電気が発生しやすい場所
- 腐食性のガスが発生する場所
- 水などがかかりやすい場所
- 振動や衝撃が加わるような不安定な場所
- 油煙が当たる場所
- 直射日光が当たる場所
- 製品周囲に発熱する器具や燃えやすい物がある場所
- 周囲に置いてある物との間に適切な空間がない場所

**禁止**

専用の AC アダプタまたは規格に合った電源以外を使用しないでください。

→ 他の電源を使用すると、故障、火災の原因になります。

**禁止**

本製品を壁等に固定する際には、オプション品として用意している専用の固定セット（取り付け金具、ネジ）を使用してください。他の取り付け金具およびネジの使用や直接のネジ止めによる固定は行わないでください。

**強制**

30cm 以上の高さから落とした場合は、使用を中止し、点検、修理を依頼してください。

→ そのまま使用すると、重大な事故になる可能性があります。

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

医用電気機器近くでの取り扱いについて

本記載の内容は「医療機関における携帯電話等の使用に関する指針(平成 26 年 8 月 19 日)」（電波環境協議会）および「各種電波利用機器の電波が植込み型医療機器等へ及ぼす影響を防止するための指針(平成 28 年 11 月)」（総務省）を参考にしています。

警告



強制

医療機関(病床数 20 床未満の診療所も含む)では次のことを守って使用してください。ただし本装置の使用については、各医療機関の指示に従うようにしてください。

- 本装置を医用電気機器に密着して使用しないでください。
- 本装置を病室、診療室で使用する場合には、医用電気機器から 1m 程度以上離してください。
- 待合室、ロビー、食堂、廊下、エレベータホール等で医用電気機器を使用している患者がいる場合、本装置を医用電気機器から 1m 程度以上離してください。
- 手術室、集中治療室 (ICU)、検査室、治療室には本装置を持ち込まないでください。



強制

本装置を植込み型医療機器の装着部位から 15cm 程度以上離してください。

→ 15cm 程度の離隔距離が確保できない恐れがある場合には、事前に本装置の電源を切ってください。

自宅療養などにより医療機関の外で、埋込み型医療機器を使用される場合には、電波による影響について個別に医用電気機器メーカーなどにご確認ください。

ご使用時の取り扱いについて

■ ご使用にあたってのお願い

- 本製品周辺で静電氣的障害を発生させないでください。
→ 本製品は、静電気に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。
- 本製品はていねいに取り扱ってください。
→ 本製品に強いショックを与えると破損の原因になります。
- 本製品のお手入れは、電源を切った状態で行ってください。
→ 誤動作や故障の原因になります。
- 本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。汚れがひどい場合は、柔らかい布に台所中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布で仕上げてください。
→ 揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては破損の原因になります。

地球環境保全のため、次のことにご協力ください。

- 本製品および付属品は、不燃物として処分してください。
- 廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。
- 一般ごみとして、家庭で焼却処分しないでください。
- 処分方法によっては有害物質が発生する可能性があります。

■ ご注意

- 本製品は日本の法規制に準拠しており、日本国内での使用を想定して設計しています。
→ 海外でのご使用をお考えの場合は、弊社までご相談ください
- 本製品は、医療・原子力・航空・海運・軍事・宇宙産業など 人命に関わる場合や高度な安全性・信頼性を必要とするシステムや機器としての使用またはこれらに組み込んだ使用を意図した設計・製造はしていません。このようなシステムや機器としての使用またはこれらに組み込んで本製品が使用されることで、お客様 もしくは第三者に損害が生じて、かかる損害が直接的または間接的または付随的なものであるかどうかにかかわらず、当社としましては一切の責任を負いません。お客様の責任において、このようなシステムや機器としての使用またはこれらに組み込んで使用する場合には、事前に使用環境・条件を考慮し十分に評価を実施した上でご使用ください。
- 一般の電話機やテレビ・ラジオなどをお使いになっている近くで使用すると、影響を与える場合がありますので、なるべく離れた場所でご使用ください。
- 強い磁界の中や腐食性のガスの中で使用したり保管したりしないでください。故障の原因となります。
- 高精度な制御や微弱な信号を取り扱う電子機器の近くでは、本装置の電源を切ってください。電波により電子機器が誤作動するなどの悪影響を及ぼす原因となります。

【ご注意いただきたい電子機器の例】

補聴器、植込み型心臓ペースメーカーおよび植込み型除細動器、その他医用電気機器、その他の自動制御機器など。植込み型心臓ペースメーカーおよび植込み型除細動器、その他医用電気機器を使用される方は、各位用電気機器メーカーもしくは販売業者に電波による影響についてご確認ください。

- 取扱説明書について、次の点にご注意ください。
 1. 本製品は無線によるデータ通信を行うことができる装置です。本製品の不具合、誤動作又は停電、回線障害、その他の外部要因によって通信障害が発生したために生じた損害等については、当社としては責任を負いかねますので、あらかじめご了承ください。
 2. 本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。
 3. 本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。
 4. 本取扱説明書の内容につきましては、万全を期して作成致しましたが、万一ご不審な点や、ご不明な点、誤り、記載漏れ、乱丁、落丁、その他お気づきの点等ございましたら、当社までご連絡ください。
 5. 適用した結果の影響につきましては、3項にかかわらず責任を負いかねますので、ご了承ください。
 6. 本取扱説明書で指示されている内容につきましては、必ず従ってください。本取扱説明書に記載されている内容を無視した行為や誤った操作によって生じた障害や損害につきましては、保証期間内であっても責任を負いかねますので、ご了承ください。

設定の入力及び保存について

■ 入力値について

Web 設定ツールは、基本的に半角英数字のみの入力をサポートしております。
全角文字や、記号の入力値はサポートしておりませんのでご注意ください。

※URL やアドレス等の一部設定項目は半角の「.」（ドット）、「-」（ハイフン）、「_」（アンダースコア）等の半角記号をご使用いただけます。

■ 設定の保存について

Web 設定ツールの共通項目であるに保存ボタンについて説明します。

保存 & 適用

設定の変更及び、実動作へ反映します。

保存

設定の変更を行います。実動作には反映されません。

リセット

入力中の設定を取り消します。

設定の保存

現在の動作に反映されている設定をフラッシュメモリへ保存します。

保存されていない変更: 1

実動作へ反映していない設定を表示します。
※「1」は変更した設定件数です。

元に戻す

保存されていない変更: 1

の内容を取り消します。

■ 一括更新について

Web 設定ツールでは設定追加、変更後に **保存** を実行した場合、実動作には反映しません。

保存

を押下後に実動作への反映を行う場合、

保存されていない変更: 1

Web 設定ツールの画面右上の **保存されていない変更: 1** 選択し、

保存 & 適用

を実行することで、保存されている変更を実動作へ反映することができます。

目次

はじめに.....	2
安全上のご注意(必ずお守りください).....	3
医用電気機器近くでの取り扱いについて.....	6
ご使用時の取り扱いについて.....	7
設定の入力及び保存について.....	9
1 章 ステータス.....	13
1-1 概要.....	13
1-1-1 システム.....	13
1-1-2 通信ボード.....	14
1-1-3 メモリー.....	15
1-1-4 ネットワーク.....	16
1-1-5 DHCP リース.....	17
1-1-6 ダイナミック DNS.....	17
1-2 ファイアウォール.....	18
1-2-1 テーブル:Filter.....	19
1-2-2 テーブル:NAT.....	19
1-2-3 テーブル:Mangle.....	19
1-2-4 テーブル:Raw.....	19
1-2-5 表示内容について.....	19
1-3 経路情報.....	21
1-3-1 ARP.....	21
1-3-2 稼働中の IPv4 経路情報.....	21
1-4 システムログ.....	22
1-5 カーネルログ.....	23
1-6 プロセス.....	24
1-7 リアルタイム・グラフ.....	25
1-7-1 負荷.....	25
1-7-2 トラフィック.....	26
1-7-3 ネットワーク接続.....	27
1-8 トリガーグループ.....	28
1-9 IPsec.....	29
1-9-1 IPsec ステータス.....	29
1-10 PPTP サーバ.....	31
1-11 L2TP/IPsec サーバ.....	32
1-12 遮断ログ.....	33
1-13 通過ログ.....	35

2章	システム	37
2-1	システム	37
2-1-1	システム・プロパティ.....	37
2-1-2	時刻設定.....	39
2-2	管理画面	41
2-2-1	パスワード設定.....	41
2-2-2	SSH アクセスに関する設定	42
2-3	システムログ	44
2-3-1	一般設定.....	44
2-3-2	転送先の設定	45
2-4	Web 設定ツール.....	46
2-5	電源制御	47
2-5-1	ハードウェア電源制御.....	47
2-5-2	ソフトウェア電源制御(日数)	49
2-5-3	ソフトウェア電源制御(曜日指定)	51
2-6	おやすみモード	53
2-6-1	タイマーモード	53
2-6-2	スケジュールモード	54
2-7	パッケージ管理.....	57
2-8	ブートエリア	59
2-9	バックアップ	60
2-10	設定の消去	61
2-11	診断情報の取得	62
2-12	再起動 / シャットダウン	63
3章	サービス	64
3-1	SunDMS	64
3-2	Bacsoft IoT Platform	65
3-3	ダイナミック DNS	66
4章	ネットワーク	69
4-1	インターフェース.....	69
4-1-1	インターフェース一覧	69
4-1-2	インターフェースの作成.....	70
4-1-3	プロトコル: 静的アドレス.....	72
4-1-4	プロトコル: DHCP クライアント	74
4-1-5	プロトコル: PPP	77
4-1-6	プロトコル: PPPoE	79
4-1-7	プロトコル: VPN.....	82

4-1-8	プロトコル:Unmanaged	84
4-1-9	ファイアウォール設定.....	86
4-1-10	DHCP サーバー.....	87
4-2	モバイル.....	90
4-2-1	通信事業者選択.....	90
4-2-2	接続先通信事業者選択.....	91
4-3	プロファイル.....	92
4-3-1	プロファイル一覧.....	92
4-3-2	プロファイル設定.....	93
4-4	DHCP 及び DNS.....	95
4-5	ホスト名.....	100
4-6	静的ルーティング.....	101
4-6-1	IPv4 静的ルーティング.....	101
4-6-2	ルートセクタ.....	103
4-7	ファイアウォール.....	104
4-7-1	一般設定.....	104
4-7-2	ゾーン設定.....	106
4-7-3	ポートフォワーディング設定.....	110
4-7-4	トラフィック・ルール設定.....	113
4-7-5	送信元 NAT 設定.....	117
4-8	トリガー.....	120
4-8-1	リンク状態.....	121
4-8-2	ハートビート.....	122
4-8-3	アクション設定.....	124
4-8-4	アクション:再起動.....	125
4-8-5	アクション:LED.....	126
4-8-6	アクション:トリガー.....	127
4-8-7	アクション:ウェイト.....	128
4-8-8	アクション:ルート.....	129
4-9	IPsec.....	130
4-10	PPTP サーバ.....	133
4-11	L2TP/IPsec サーバ.....	137
4-12	診断機能.....	142

1章 ステータス

この章では、本装置の Web 設定ツールのステータスについて説明します。

1-1 概要

概要

[ステータス] - [概要] ページについて説明します。

概要ページでは、本装置のステータス全般を確認できます。

1-1-1 システム

- 本装置のシステムに関する情報を表示します。

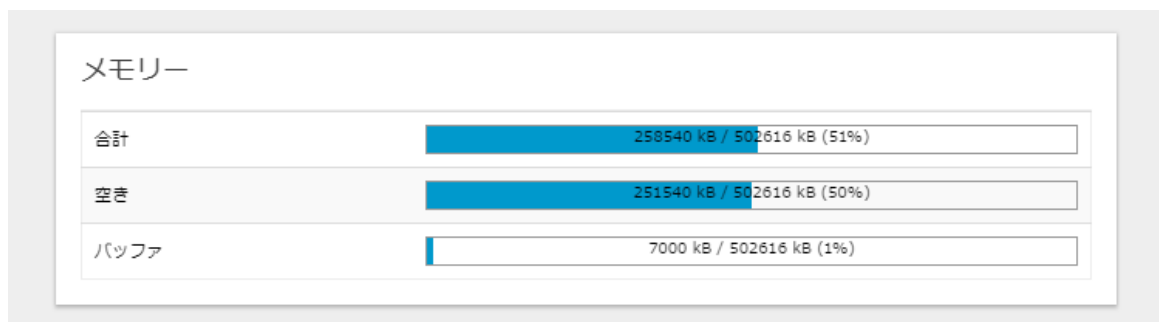


The screenshot shows the 'Rooster NSX' status page. At the top, there is a blue header with a menu icon, the text 'Rooster NSX', and two buttons: '設定の保存' (Save Settings) and '自動更新 オン' (Auto Update On). Below the header, the title 'ステータス' (Status) is displayed. The main content area is titled 'システム' (System) and contains a table with the following information:

ホスト名	NSX
製造番号	NSX000EXAMPLE
モデル	NSX7000
ファームウェア・バージョン	RoosterOS NSX7000 1.4.0 B9
カーネルバージョン	4.4.14
時刻	Wed Apr 10 19:36:23 2019
起動時間	22h 45m 48s
システム平均負荷	0.58, 0.16, 0.05
現在のブートエリア	a-side
次回起動時のブートエリア	a-side

1-1-3 メモリー

- 本装置のメモリーの使用状況を表示します。



メモリーの表示内容

項目	内容
合計	使用可能なメモリの合計を表示します。
空き	空き領域を表示します。
バッファ	カーネルが使用中ですが、開放可能な領域を表示します。

1-1-4 ネットワーク

- 本装置のデフォルトルートのインタフェース情報を表示します。



IPv4 WAN ステータスは有効なデフォルトルートが存在しない場合、表示されません。

ネットワーク

IPv4 WAN ステータス

	タイプ: static
	アドレス: 203.0.113.1
	ネットマスク: 255.255.255.0
	ゲートウェイ: 203.0.113.254
	DNS 1: 203.0.113.253
	接続中: 0h 3m 15s

アクティブコネクション 43 / 16384 (0%)

■ ネットワークの表示内容

項目	内容
IPv4 WAN ステータス	デフォルトルートとして選択されているインタフェース情報です。
アクティブコネクション	本装置のファイアウォールが監視しているコネクション数を表示します。

■ IPv4 WAN ステータスの表示内容

項目	内容
タイプ	プロトコルタイプを表示します。 詳細は「4-1 インターフェース」を参照ください。
アドレス	インタフェースの IP アドレスを表示します。
ネットマスク	インタフェースのネットマスクを表示します。
ゲートウェイ	ネクストホップを表示します。
DNS 1	DNS サーバを表示します。
接続中	インタフェースの UP 状態の経過時間を表示します。

1-1-5 DHCPリース

- 本装置の DHCP サーバとしてのリース情報を表示します。

DHCPリース			
ホスト名	IPv4-アドレス	MAC-アドレス	残りリース時間
PC	192.168.62.192	00:00:5e:00:53:FF	11h 43m 57s

DHCPリースの表示内容

項目	内容
ホスト名	リース先のホスト名です。
IPv4-アドレス	リースしたアドレスです。
MAC-アドレス	リース先の MAC アドレスです。
残りリース時間	リースしたアドレスが無効になるまでの残り時間です。

1-1-6 ダイナミックDNS

- ダイナミック DNS の情報を表示します。

ダイナミックDNS				
設定	次のアップデート	Lookup ホスト名	登録IP	ネットワーク
example	2019-04-20 11:14	■■■■.suncomm.net	203.0.113.11	IPv4 / ppp0

ダイナミックDNSの表示内容

項目	内容
設定	ダイナミック DNS の設定名を表示します。
次のアップデート	次の更新時間を表示します。
Lookup ホスト名	登録する予定のアドレスと一致しているか参照する為のホスト名を表示します。
登録 IP	ダイナミック DNS に登録したアドレスを表示します。
ネットワーク	ダイナミック DNS に登録するネットワーク情報を表示します。

1-2 ファイアウォール

概要

[ステータス] - [ファイアウォール] ページについて説明します。

ファイアウォールページでは、本装置のファイアウォールの設定状態とコネクション追跡の監視状態を確認できます。

テーブル

- 本装置のファイアウォールの設定情報を表示します。

☰ Rooster NSX
設定の保存

ファイアウォール・ステータス

テーブル: Filter カウンタのリセット ファイアウォールの再起動

チェーン INPUT (ポリシー: ACCEPT, パケット: 0, トラフィック: 0.00 B)									
パケット	トラフィック	ターゲット	プロトコル	イン	アウト	送信元	送信先	オプション	
24	2.27 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	/* ifw3 */	

チェーン FORWARD (ポリシー: DROP, パケット: 0, トラフィック: 0.00 B)									
パケット	トラフィック	ターゲット	プロトコル	イン	アウト	送信元	送信先	オプション	
0	0.00 B	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	/* ifw3: user chain for forwarding */	

チェーン OUTPUT (ポリシー: ACCEPT, パケット: 0, トラフィック: 0.00 B)									
パケット	トラフィック	ターゲット	プロトコル	イン	アウト	送信元	送信先	オプション	
24	2.27 KB	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	/* ifw3 */	

テーブル: NAT

チェーン PREROUTING (ポリシー: ACCEPT, パケット: 36, トラフィック: 1.93 KB)									
パケット	トラフィック	ターゲット	プロトコル	イン	アウト	送信元	送信先	オプション	
36	1.93 KB	prerouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	/* ifw3: user chain for prerouting */	

チェーン POSTROUTING (ポリシー: ACCEPT, パケット: 3, トラフィック: 191.00 B)									
パケット	トラフィック	ターゲット	プロトコル	イン	アウト	送信元	送信先	オプション	
3	191.00 B	postrouting_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	/* ifw3: user chain for postrouting */	

テーブル: Mangle

チェーン FORWARD (ポリシー: ACCEPT, パケット: 0, トラフィック: 0.00 B)									
パケット	トラフィック	ターゲット	プロトコル	イン	アウト	送信元	送信先	オプション	
0	0.00 B	TCPMSS	tcp	*	eth1	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x02 /* ifw3: wan (mtu_fix) */ TCPMSS clamp to PMTU	

テーブル: Raw

チェーン内にルールがありません。

1-2-1 テーブル:Filter

「4-7-1 一般設定」、「4-7-2 ゾーン設定」、「4-7-4 トラフィック・ルール設定」で設定されたフィルタリングの情報を表示します。

1-2-2 テーブル:NAT

「4-7-2 ゾーン設定」で設定されたマスカレード設定、「4-7-3 ポートフォワーディング設定」、「4-7-5 送信元 NAT 設定」の情報を表示します。

1-2-3 テーブル:Mangle

本装置では設定項目はありません。

1-2-4 テーブル:Raw

「4-7-4 トラフィック・ルール設定」で設定されたコネクション追跡の情報を表示します。

1-2-5 表示内容について

ファイアウォール・ステータスの表示内容について説明します

■ ファイアウォール・ステータスの表示内容

項目	内容
パケット	条件に一致したパケット数を表示します。
トラフィック	条件に一致したパケット数を表示します。
ターゲット	<p>下記 3 つの設定された条件に一致したパケットに対するアクションを表示します。</p> <p>ACCEPT : 許可 REJECT : 拒否 DROP : 遮断</p> <p>その他の表示については設定名（チェーン名）です。</p>
プロトコル	条件を適用するプロトコルを表示します。
イン	条件を適用する受信インタフェースを表示します。
アウト	条件を適用する送信インタフェースを表示します。
送信元	条件を適用する送信元アドレスを表示します。
送信先	条件を適用する宛先アドレスを表示します。
オプション	条件を適用するプロトコルのタイプや状態を表示します。 また、トラフィック・ルールの設定名も表示します。

接続状態

- 本装置のコネクション追跡の情報を表示します。

接続状態

```
ipv4 2 tcp 6 48 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63274 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 udp 17 53 src=192.168.62.192 dst=192.168.62.1 sport=55812 dport=53 packets=1 bytes=77 src=192.168.62.1 dst=192.168.62.1
ipv4 2 udp 17 53 src=192.168.62.192 dst=192.168.62.1 sport=55811 dport=53 packets=1 bytes=77 src=192.168.62.1 dst=192.168.62.1
ipv4 2 tcp 6 63 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63293 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 108 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63351 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 68 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63299 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 88 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63323 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 udp 17 72 src=127.0.0.1 dst=127.0.0.1 sport=44405 dport=53 packets=2 bytes=110 src=127.0.0.1 dst=127.0.0.1 sport=53 dp
ipv4 2 tcp 6 38 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63260 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 43 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63267 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 53 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63279 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 93 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63328 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 118 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63367 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 udp 17 62 src=127.0.0.1 dst=127.0.0.1 sport=54710 dport=53 packets=2 bytes=110 src=127.0.0.1 dst=127.0.0.1 sport=53 dp
ipv4 2 tcp 6 83 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63317 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 98 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63333 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 118 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63357 dport=443 packets=33 bytes=4413 src=192.168.62.1
ipv4 2 tcp 6 108 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63350 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 udp 17 37 src=192.168.62.192 dst=192.168.62.1 sport=57828 dport=53 packets=1 bytes=61 src=192.168.62.1 dst=192.168.62.1
ipv4 2 tcp 6 53 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63280 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 33 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63255 dport=443 packets=7 bytes=812 src=192.168.62.1
ipv4 2 tcp 6 98 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63334 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 58 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63287 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 73 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63306 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 7439 ESTABLISHED src=192.168.62.103 dst=192.168.62.1 sport=63369 dport=443 packets=7 bytes=1786 src=192.168.62.1
ipv4 2 tcp 6 78 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63312 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 83 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63318 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 38 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63261 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 103 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63344 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 udp 17 67 src=127.0.0.1 dst=127.0.0.1 sport=52096 dport=53 packets=2 bytes=110 src=127.0.0.1 dst=127.0.0.1 sport=53 dp
ipv4 2 tcp 6 117 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63365 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 tcp 6 68 TIME_WAIT src=192.168.62.103 dst=192.168.62.1 sport=63300 dport=443 packets=7 bytes=816 src=192.168.62.1
ipv4 2 udp 17 53 src=192.168.62.192 dst=192.168.62.1 sport=53719 dport=53 packets=1 bytes=60 src=192.168.62.1 dst=192.168.62.1
```

1-3 経路情報

概要

[ステータス] - [経路情報] ページについて説明します。

経路情報ページでは、本装置の ARP と有効な経路情報を確認できます。

1-3-1 ARP

- 現在の ARP テーブルを表示します。

☰ Rooster NSX
設定の保存

経路情報

このシステムでは、現在以下のルールが有効になっています。

ARP

IPv4-アドレス	MAC-アドレス	インタフェース
192.168.62.103	00:00:00:00:00:00	eth0
192.168.62.192	FF:FF:FF:FF:FF:FF	eth0

1-3-2 稼働中のIPv4経路情報

- 現在有効な経路情報を表示します。

稼働中の IPv4-経路情報

ネットワーク	ターゲット	IPv4-ゲートウェイ	メトリック	テーブル	タイプ
eth1	0.0.0.0/0		0	main	UNICAST
eth0	192.168.62.0/24		0	main	UNICAST
eth1	203.0.113.0/24		0	main	UNICAST

1-4 システムログ

概要

[ステータス] - [システムログ] ページについて説明します。

システムログページでは、本装置に保存されているシステムログを表示できます。

システムログ

- 本装置に保存されているシステムログを表示します。



保存されているシステムログを取得し表示する為、データ量が非常に多くなる可能性があります。

Rooster NSX 設定の保存

システムログ

ログの操作

システムログファイルを全て消去する: 削除

① 全てのシステムログファイルを削除します。

```
Apr 3 18:39:41 NSX root: example
```

ログの操作

項目	内容
システムログファイルを全て消去する	本装置に保存されているシステムログを全て消去します。

1-5 カーネルログ

概要

[ステータス] - [カーネルログ] ページについて説明します。

カーネルログページでは、本装置に保存されているカーネルログを表示できます。

カーネルログ

- 本装置に保存されているカーネルログを表示します。



保存されているカーネルログを取得し表示する為、データ量が非常に多くなる可能性があります。

Rooster NSX

設定の保存

カーネルログ

```
[ 0.000000] Booting Linux on physical CPU 0x0
[ 0.000000] Linux version 4.4.14 (yusato@debian) (gcc version 5.3.0 (OpenWrt GCC 5.3.0 B9)) #1 SMP Thu Mar 2
[ 0.000000] CPU: ARMv7 Processor [412fc09a] revision 10 (ARMv7), cr=10c5387d
[ 0.000000] CPU: PIPT / VIPT nonaliasing data cache, VIPT aliasing instruction cache
[ 0.000000] Machine model: NSX7000
[ 0.000000] Memory policy: Data cache writealloc
[ 0.000000] On node 0 totalpages: 131072
[ 0.000000] free_area_init_node: node 0, pgdat 8087afc0, node_mem_map 9fb79000
[ 0.000000]   Normal zone: 1152 pages used for memmap
[ 0.000000]   Normal zone: 0 pages reserved
[ 0.000000]   Normal zone: 131072 pages, LIFO batch:31
[ 0.000000] PERCPU: Embedded 13 pages/cpu @9fb47000 s23080 r8192 d21976 u53248
[ 0.000000] pcpu-alloc: s23080 r8192 d21976 u53248 alloc=13#4096
[ 0.000000] pcpu-alloc: [0] 0
[ 0.000000] Built 1 zonelists in Zone order, mobility grouping on. Total pages: 129920
[ 0.000000] Kernel command line: console=ttymx2,115200 rw rooster_os_boot_mode=kitting rooster_os_target_sys
[ 0.000000] rooster-os-boot-mode: 1, rooster-os-smack-strict-mode: ON
[ 0.000000] rooster-os-developer-mode: OFF
[ 0.000000] rooster-os-boot-option: 0
[ 0.000000] PID hash table entries: 2048 (order: 1, 8192 bytes)
[ 0.000000] Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
[ 0.000000] Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
[ 0.000000] Memory: 494956K/524288K available (5815K kernel code, 512K rwdata, 1920K rodata, 472K init, 8139K
[ 0.000000] Virtual kernel memory layout:
[ 0.000000]   vector : 0xffff0000 - 0xffff1000   (   4 kB)
[ 0.000000]   fixmap : 0xffc00000 - 0xffff0000   (3072 kB)
[ 0.000000]   vmalloc : 0xa0800000 - 0xff800000   (1520 MB)
[ 0.000000]   lowmem  : 0x80000000 - 0xa0000000   ( 512 MB)
[ 0.000000]   modules : 0x7f000000 - 0x80000000   (   16 MB)
[ 0.000000]     .text : 0x80008000 - 0x80795f04   (7736 kB)
[ 0.000000]     .init : 0x80796000 - 0x8080c000   (  472 kB)
[ 0.000000]     .data : 0x8080c000 - 0x8088c388   (  513 kB)
[ 0.000000]     .bss  : 0x8088c388 - 0x8107f0f0   (8140 kB)
[ 0.000000] SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[ 0.000000] Running RCU self tests
[ 0.000000] Hierarchical RCU implementation.
[ 0.000000]   RCU lockdep checking is enabled.
[ 0.000000]   RCU restricting CPUs from NR_CPUS=4 to nr_cpu_ids=1.
[ 0.000000] RCU: Adjusting geometry for rcu_fanout_leaf=16, nr_cpu_ids=1
[ 0.000000] NR_IRQS:16 nr_irqs:16 16
[ 0.000000] L2C-310 erratum 769419 enabled
[ 0.000000] L2C-310 enabling early BRESP for Cortex-A9
[ 0.000000] L2C-310 full line of zeros enabled for Cortex-A9
[ 0.000000] L2C-310 ID prefetch enabled, offset 1 lines
[ 0.000000] L2C-310 dynamic clock gating enabled, standby mode enabled
[ 0.000000] L2C-310 cache controller enabled, 16 ways, 256 kB
[ 0.000000] L2C-310: CACHE_ID 0x410000c8, AUX_CTRL 0x76430001
[ 0.000000] Switching to timer-based delay loop, resolution 333ns
[ 0.000000] sched_clock: 32 bits at 3000kHz, resolution 333ns, wraps every 715827882841ns
[ 0.000049] clocksource: mxc_timer1: mask: 0xffffffff max_cycles: 0xffffffff, max_idle_ns: 637086815595 ns
```

1-6 プロセス

概要

[ステータス] - [プロセス] ページについて説明します。
プロセスページでは、本装置で実行中のプロセス一覧を確認できます。

プロセス

- 現在の実行中のプロセスを表示します。



再起動、停止、強制終了ボタンを実行した後の動作についてはサポートの対象外です。

≡ Rooster NSX 設定の保存

プロセス

このリストは現在システムで動作しているプロセスとそのステータスを表示しています。

PID	所有者	コマンド	CPU使用率 (%)	メモリ使用率 (%)	再起動	停止	強制終了
2671	root	/usr/sbin/rsyslogd -n -i /var/run/rsyslogd.pid	0%	0%	再起動	停止	強制終了

プロセスの表示内容

項目	内容
PID	PID を表示します。
所有者	実行ユーザを表示します。
コマンド	プロセスの実行コマンドを表示します。
CPU 使用率 (%)	CPU 使用率を表示します。
メモリ使用率 (%)	メモリ使用率を表示します。
再起動	実行中プロセスに HUP シグナルを送信します。
停止	実行中プロセスに TERM シグナルを送信します。
強制終了	実行中プロセスに KILL シグナルを送信します。

1-7 リアルタイム・グラフ

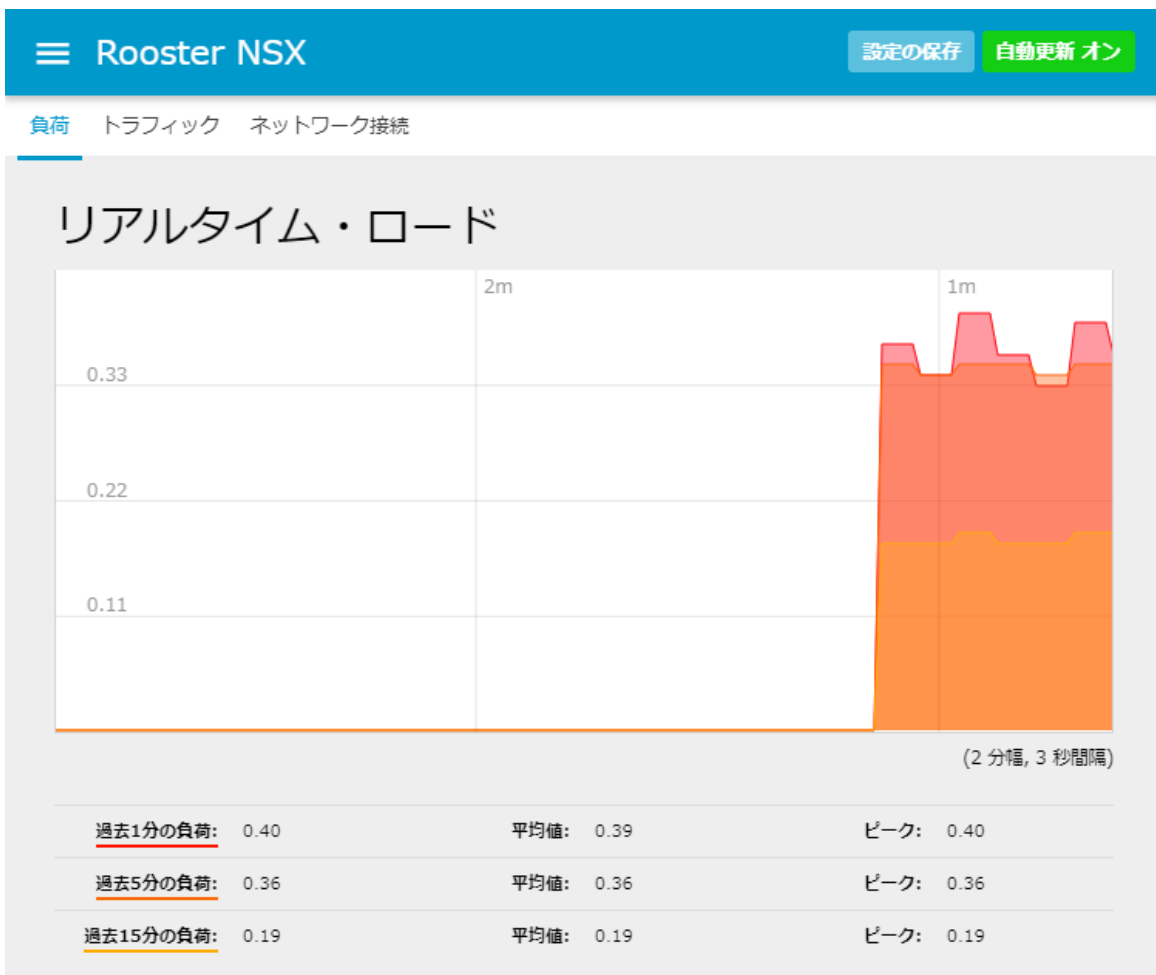
概要

[ステータス] - [リアルタイム・グラフ] ページについて説明します。

リアルタイム・グラフページでは、システムの平均負荷、インタフェースのトラフィック、アクティブなコネクションをグラフとして確認できます。

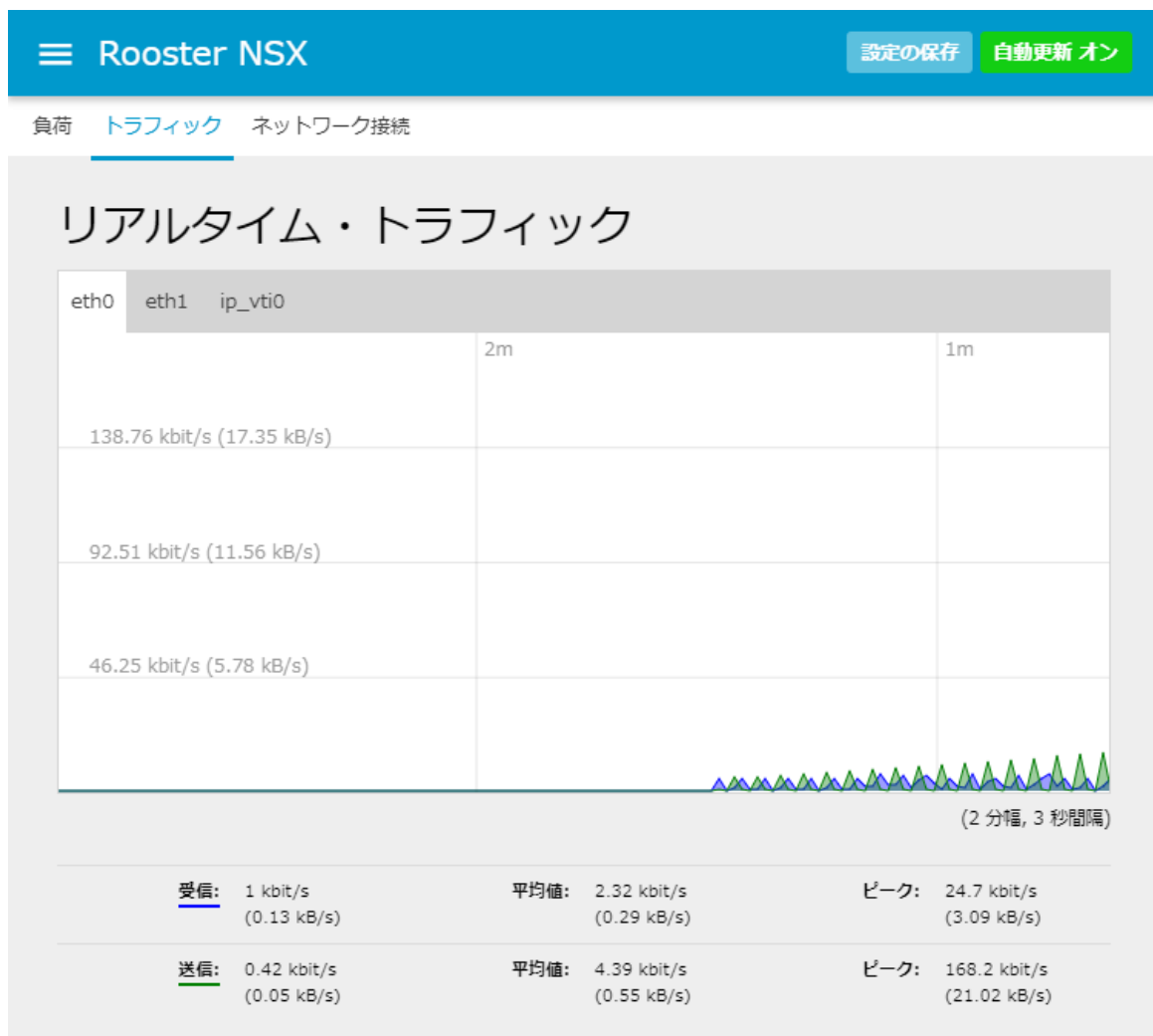
1-7-1 負荷

- 過去1分以内、5分以内、15分以内のシステムの平均負荷を3秒間隔で表示します。



1-7-2 トラフィック

- 各インタフェースのトラフィック量を3秒間隔で表示します。



1-7-3 ネットワーク接続

- アクティブな接続の情報を 3 秒間隔で表示します。

Rooster NSX

設定の保存

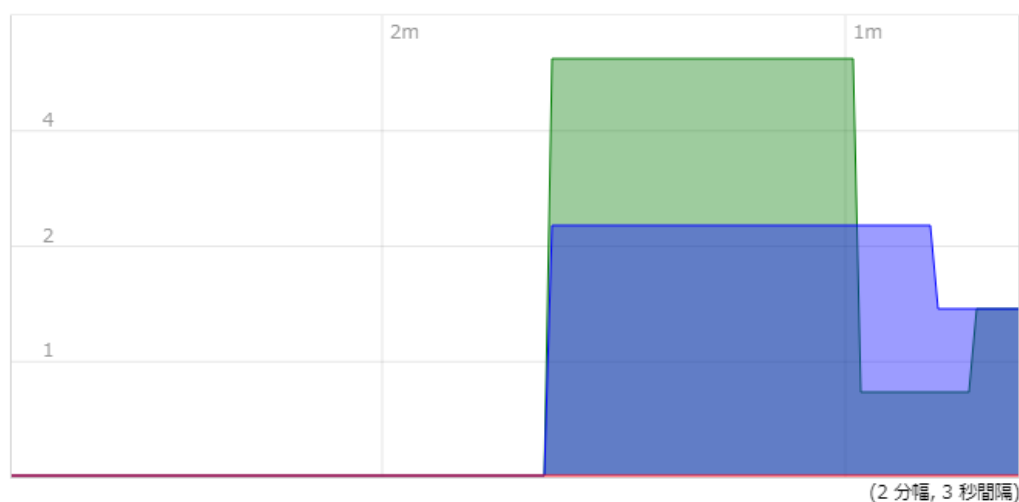
自動更新 オン

負荷 トラフィック ネットワーク接続

リアルタイム・接続

このページでは、現在アクティブなネットワーク接続を表示します。

アクティブ接続



<u>UDP</u> :	0	平均値:	0	ピーク:	3
<u>TCP</u> :	1	平均値:	1	ピーク:	5
<u>その他</u> :	0	平均値:	0	ピーク:	0

ネットワーク	プロトコル	送信元	送信先	転送
IPV4	TCP	192.168.62.103:58908	192.168.62.1:443	67.76 KB (236 パケット)

1-8 トリガーグループ

概要

[ステータス] - [トリガーグループ]ページについて説明します。

トリガーグループのステータスページでは、設定されているトリガーグループの有効、無効の状態を一覧で確認できます。

トリガーグループのステータス

- 「4-8 トリガー」に設定されているトリガーの状態を確認できます。

☰ Rooster NSX 設定の保存

トリガーグループのステータス

trigger-group	status
group1	enable
group2	disable

ステータスセクション

項目	内容
trigger-group	「4-8 トリガー」に設定されているトリガーの設定名を表示します。
status	設定の有効無効を表示します。 ※disable の場合は、設定されたイベントが発生しても、アクションは実行されません

1-9 IPsec

概要

[ステータス] - [IPsec] ページについて説明します。

IPsec ページでは、IPsec の設定情報、IPsec 接続情報を確認できます。

1-9-1 IPsecステータス

- IPsec 現在の状態を表示します。
- 下記表示例は IPsec 接続完了時の状態です。

Rooster NSX

[設定の保存](#)

IPsecステータス

```
000 using kernel interface: netkey
000 interface lo/lo 127.0.0.1@4500
000 interface lo/lo 127.0.0.1@500
000 interface eth0/eth0 192.168.62.1@4500
000 interface eth0/eth0 192.168.62.1@500
000 interface eth1/eth1 192.168.63.1@4500
000 interface eth1/eth1 192.168.63.1@500
000
```

一部省略

```
000
000 Connection list:
000
000 "example": 192.168.62.0/24===192.168.63.1<192.168.63.1>...192.168.63.2<192.168.63.2>===192.168.64.0/24;
000 "example": oriented; my_ip=unset; their_ip=unset
000 "example": xauth us:none, xauth them:none, my_username=[any]; their_username=[any]
000 "example": modecfg info: us:none, them:none, modecfg policy:push, dns1:unset, dns2:unset, domain:unset, bar
000 "example": labeled_ipsec:no;
000 "example": policy_label:unset;
000 "example": ike_life:3600s; ipsec_life:28800s; replay_window:32; rekey_margin:540s; rekey_fuzz:100%; keyi
000 "example": retransmit-interval:500ms; retransmit-timeout:60s;
000 "example": sha2-truncbug:no; initial-contact:no; cisco-unity:no; fake-strongswan:no; send-vendorid:no; send-no
000 "example": policy:PSK+ENCRYPT+TUNNEL+PFS+UP+AGGRESSIVE+IKEV1_ALLOW+IKEV2_ALLOW+SAR
000 "example": conn_prio:24,24; interface:eth1; metric:0; mtu:unset; sa_prio:auto; sa_tfc:none;
000 "example": nflog-group:unset; mark:5/0x7ffffff,5/0x7ffffff; vti-iface:ipsec0; vti-routing:yes; vti-shared:no;
000 "example": newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "example": IKE algorithms wanted: AES_CBC(7)_256-MD5(1)-MODP1536(5)
000 "example": IKE algorithms found: AES_CBC(7)_256-MD5(1)-MODP1536(5)
000 "example": IKE algorithm newest: AES_CBC_256-MD5-MODP1536
000 "example": ESP algorithms wanted: AES(12)_256-MD5(1)
000 "example": ESP algorithms loaded: AES(12)_256-MD5(1)
000 "example": ESP algorithm newest: AES_256-HMAC_MD5; pfsgrp=<Phase1>
000
000 Total IPsec connections: loaded 1, active 1
000
000 State Information: DDoS cookies not required, Accepting new IKE connections
000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)
000 IPsec SAs: total(1), authenticated(1), anonymous(0)
000
000 #2: "example":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 27942s; newe
000 #2: "example" esp.af84e3e7@192.168.63.2 esp.32b1f31c@192.168.63.1 ref=0 rethim=0 Traffic: ESPin=0B ESP
000 #1: "example":500 STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 2500s; new
000
```

IPsecステータスの表示内容

項目	内容
Connection list	「4-9IPsec」の有効な設定の詳細情報を表示します。
Total IPsec Connections	現在の IPsec 接続状態を表示します。 Connection list の設定に紐づく IKE SA、IPsec SA の状態を表示します。

Total IPsec Connectionsの表示内容

IPsec 接続の状態について説明します。

項目	SA 状態	内容
ISAKMP SA の状態	STATE_AGGR_I2 (sent AI2, ISAKMP SA established)	アグレッシブモードで ISAKMP SA が確立した状態です。
	STATE_AGGR_I1 (sent AI1, expecting AR1)	アグレッシブモードの ISAKMP SA の生成で停止しています。 アルゴリズムや事前共有鍵、識別子等の設定をご確認ください。
	STATE_MAIN_I4 (ISAKMP SA established)	メインモードで ISAKMP SA が確立した状態です。
	STATE_MAIN_I3 (sent MI3, expecting MR3)	メインモードの ISAKMP SA の生成で停止しています。 事前共有鍵や識別子等の設定をご確認ください。
	STATE_MAIN_I2 (sent MI3, expecting MR3)	メインモードの ISAKMP SA の生成で停止しています。 事前共有鍵や識別子等の設定をご確認ください。
IPsec SA の状態	STATE_MAIN_I1 (sent MI1, expecting MR1)	メインモードの ISAKMP SA の生成で停止しています。 アルゴリズム等の設定をご確認ください。
	STATE_QUICK_I2 (sent QI2, IPsec SA established)	IPsec SA が確立した状態です。
	STATE_QUICK_I1 (sent QI1, expecting QR1)	IPsec SA の生成で停止しています。 PFS や、ローカルネットワーク等の設定をご確認ください。

1-10 PPTPサーバ

概要

[ステータス]- [PPTP サーバ] ページについて説明します。

PPTP サーバページでは、PPTP 接続状態を一覧で確認できます。

接続状態

- PPTP サーバに接続されたクライアントの状態を確認できます。



Rooster NSX

設定の保存 自動更新 オン

PPTPサーバ

接続状態

インタフェース	状態	クライアント名	クライアント IPアドレス
pptp1	起動時間: 0h 1m 12s RX: 48.46 KB (204 パケット) TX: 2.80 KB (24 パケット) IPv4: 192.168.0.1/32	user	192.168.0.20

接続状態の表示内容

項目	内容
インタフェース	クライアントとの接続で使用されているインタフェース名を表示します。
クライアント名	クライアントが使用しているユーザ名を表示します。
クライアント IP アドレス	クライアントに割り当てたアドレスを表示します。

1-11 L2TP/IPsecサーバ

概要

[ステータス] - [L2TP/IPsec サーバ] ページについて説明します。

L2TP/IPsec サーバページでは、L2TP/IPsec の接続状態を一覧で確認できます

接続状態

- L2TP/IPsec サーバに接続されたクライアントの状態を確認できます。

☰ Rooster NSX 設定の保存 自動更新 オン

L2TP/IPsecサーバ

接続状態

インタフェース	状態	クライアント名	クライアント IPアドレス
l2tp1	起動時間: 0h 2m 18s RX: 52.50 KB (318 パケット) TX: 3.23 KB (40 パケット) IPv4: 192.168.1.1/32	user	192.168.1.20

接続状態の表示内容

項目	内容
インタフェース	クライアントとの接続で使用されているインタフェース名を表示します。
クライアント名	クライアントが使用しているユーザ名を表示します。
クライアント IP アドレス	クライアントに割り当てたアドレスを表示します。

1-12 遮断ログ

概要

[ステータス] - [遮断ログ]ページについて説明します。

遮断ログページでは、遮断したパケットのログを一覧で確認できます

遮断ログの操作

- 遮断ログの「再読み込み」・「ダウンロード」・「削除」を行うことができます。

ボタン項目の説明

項目	内容
最新ログ再読み込み	最新の遮断ログを再読み込みし、表示を更新します。
全ての遮断ログをダウンロード	遮断ログを csv ファイルとしてダウンロードします。
全ての遮断ログを削除	全ての遮断ログを削除します。

遮断ログ

- 遮断ログを一覧で確認できます。

遮断ログ

[前へ](#)
[次へ](#)

番号	時間	タイプ	プロトコル	送信元IP	送信元ポート	送信先IP	送信先ポート	ゾーン名	受信	送信	結果
3998	2020/12/24 13:55:35	DROP	ICMP	192.168.63.100	0	192.168.63.1	0	wan	eth1		終了
3997	2020/12/24 13:55:34	DROP	ICMP	192.168.63.100	0	192.168.63.1	0	wan	eth1		終了
3996	2020/12/24 13:55:34	DROP	ICMP	192.168.63.100	0	192.168.63.1	0	wan	eth1		終了
3995	2020/12/24 13:55:34	DROP	ICMP	192.168.63.100	0	192.168.63.1	0	wan	eth1		終了
3994	2020/12/24 13:55:34	DROP	ICMP	192.168.63.100	0	192.168.63.1	0	wan	eth1		終了
3993	2020/12/24 13:55:34	DROP	ICMP	192.168.63.100	0	192.168.63.1	0	wan	eth1		終了
3992	2020/12/24 13:55:32	DROP	ICMP	192.168.63.100	0	192.168.63.1	0	wan	eth1		終了

ボタン項目の説明

項目	内容
前へ	現在位置から前の 100 件を表示します。
次へ	現在位置から次の 100 件を表示します。

ログの表示内容

項目	内容
番号	ログに記録された通し番号を表示します。
時間	パケットを処理した時間を表示します。
タイプ	パケットの処理タイプを表示します。 REJECT:パケットを拒否した場合には表示されます。 DROP:パケットを遮断した場合には表示されます。
プロトコル	パケットのプロトコルを表示します。 TCP・UDP・ICMP 以外は番号で表示されます。
送信元 IP	パケットの送信元 IP アドレスを表示します。
送信元ポート	パケットの送信元ポートを表示します。
送信先 IP	パケットの送信先 IP アドレスを表示します。
送信先ポート	パケットの送信先ポートを表示します。
ゾーン名	パケットを処理したゾーン名を表示します。
受信	パケットを受信したインタフェース名を表示します。
送信	パケットを送信したインタフェース名を表示します。
結果	結果を表示します。 終了:パケットの監視を終了した場合に出力されます。 タイムアウト:監視セッションで2分以上通信が行われなかった場合に出力されます。

1-13 通過ログ

概要

[ステータス] - [通過ログ]ページについて説明します。

通過ログページでは、通過したパケットのログを一覧で確認できます

通過ログの操作

- 通過ログの「再読み込み」・「ダウンロード」・「削除」を行うことができます。

ボタン項目の説明

項目	内容
最新ログ再読み込み	最新の通過ログを再読み込みし、表示を更新します。
全ての通過ログをダウンロード	通過ログを csv ファイルとしてダウンロードします。
全ての通過ログを削除	全ての通過ログを削除します。

通過ログ

- 通過ログを一覧で確認できます。

通過ログ

前へ

次へ

番号	時間	プロトコル	方向	送信元IP	送信元ポート	送信先IP	送信先ポート	ゾーン名	受信	送信	結果
610	2020/12/24 15:39:02	TCP	IN	192.168.62.50	58394	192.168.62.1	443	lan	eth0		終了
609	2020/12/24 15:39:01	TCP	IN	192.168.62.50	58393	192.168.62.1	443	lan	eth0		終了
608	2020/12/24 15:39:00	TCP	IN	192.168.62.50	58389	192.168.62.1	443	lan	eth0		終了
607	2020/12/24 15:39:00	TCP	IN	192.168.62.50	58390	192.168.62.1	443	lan	eth0		終了
606	2020/12/24 15:38:52	UDP	IN	192.168.62.50	49391	192.168.62.1	53	lan	eth0		終了
605	2020/12/24 15:37:02	UDP	IN	192.168.62.50	58458	192.168.62.1	53	lan	eth0		終了
604	2020/12/24 15:37:01	UDP	IN	192.168.62.50	49859	192.168.62.1	53	lan	eth0		終了

ボタン項目の説明

項目	内容
前へ	現在位置から前の 100 件を表示します。
次へ	現在位置から次の 100 件を表示します。

ログの表示内容

項目	内容
番号	ログに記録された通し番号を表示します。
時間	パケットを処理した時間を表示します。
プロトコル	パケットのプロトコルを表示します。 TCP・UDP・ICMP 以外は番号で表示されます。
方向	パケットの方向を表示します。
送信元 IP	パケットの送信元 IP アドレスを表示します。
送信元ポート	パケットの送信元ポートを表示します。
送信先 IP	パケットの送信先 IP アドレスを表示します。
送信先ポート	パケットの送信先ポートを表示します。
ゾーン名	ゾーン名を表示します。
受信	パケットを受信したインタフェース名を表示します。
送信	パケットを送信したインタフェース名を表示します。
結果	結果を表示します。 終了：パケットの監視を終了した場合に出力されます。 タイムアウト：監視セッションで 2 分以上通信が行われなかった場合に出力されます。

2章 システム

この章では、本装置のシステムに関する設定について説明します。

2-1 システム

概要

[システム] - [システム] ページについて説明します。

システム設定ページでは、本装置のホスト名、Web 設定ツールの言語、時刻の調整機能を設定できません。

2-1-1 システム・プロパティ

一般設定

- 本装置のホスト名及びタイムゾーンを設定できます。

ボタン項目の説明

項目	内容
ブラウザの時刻と同期ボタン	Web 設定ツールでアクセスしている端末の時刻を本装置に設定します。

タブ項目の説明

項目	内容
言語とスタイルタブ	Web 設定ツールの使用言語の設定項目を表示します。

設定項目の説明

項目	内容
ホスト名	本装置のホスト名を設定します。
タイムゾーン	本装置のタイムゾーンを設定します。

言語とスタイル

- 本装置のホスト名及びタイムゾーンの設定が行えます。

Rooster NSX

設定の保存 自動更新 オン

システム

このページではホスト名やタイムゾーンなどの基本的な設定を行うことができます。

システム・プロパティ

一般設定	言語とスタイル
言語	auto ▼
デザイン	Rooster ▼

タブ項目の説明

項目	内容
一般設定タブ	ホスト名及びタイムゾーンの設定項目を表示します。

設定項目の説明

項目	内容
言語	Web 設定ツールの使用言語を設定します。 auto : 言語を自動的に識別します。 English : 英語を使用します。 日本語(japanese) : 日本語を使用します。

2-1-2 時刻設定

NTP

- NTP サーバに問い合わせを行い、自動的に時刻を調整します。



NTP とモバイルによる時刻調整は併用できません。

時刻設定

NTP モバイル

NTPクライアント機能を有効にする

NTPサーバー候補 ntp.jst.mfeed.ad.jp



ntp.nict.jp



タブ項目の説明

項目	内容
モバイル	通信モジュールを用いて時刻を調整する設定項目を表示します。

設定項目の説明

項目	内容
NTP クライアント機能を有効にする	NTP クライアント機能が有効になります。
NTP サーバ候補	NTP クライアントが問い合わせを行う NTP サーバのアドレスを設定します。

モバイル

- 通信モジュールを用いて自動的に時刻を調整します。



本機能を使用するためには別途 SIM を用意し、PPP の設定を行う必要があります。

NTP とモバイルによる時刻調整は併用できません。

時刻設定

NTP

モバイル

モバイル機器の時間を使っての時間同期を有効にする



モバイル端末装置の時間を使用した時間同期を有効にします。

インターバル時間(分) 1440

タブ項目の説明

項目	内容
NTP	NTP クライアントの設定項目を表示します。

設定項目の説明

項目	内容
モバイル機器の時間を使っての時間同期を有効にする。	通信モジュールによる時刻調整が有効になります。
インターバル時間 (分)	時刻調整の間隔 (分) を指定できます。

2-2 管理画面

概要

[システム] - [管理画面] ページについて説明します。

管理画面設定ページでは、本装置のパスワードの設定や、SSH アクセスに関する設定を行うことができます。

2-2-1 パスワード設定

本装置 Web 設定ツールのログインパスワードの変更を行えます。

☰ Rooster NSX 設定の保存

ルーター・パスワード

デバイスの管理者パスワードを変更します。


パスワード 

確認 

設定項目の説明

項目	内容
パスワード	変更後のパスワードを入力します。
確認	変更後のパスワードを再入力します。

ボタンの説明

項目	内容
	入力された文字を表示します。

2-2-2 SSHアクセスに関する設定

SSHサーバ

- 本装置のSSHサーバに関する設定を行えます。

SSHアクセス

SSHサーバに関する設定を行うことができます。

SSHサーバを有効にする

ポート 22

① 受信ポートを指定します。

パスワード認証

① SSH パスワード認証を許可します。

キープアライブの間隔【秒】 0

① セッションを維持するために送信するデータの送信間隔を1~3600で指定できます。空欄か0の場合はキープアライブは行われません。

アイドルタイムアウトの間隔【秒】 300

① 無通信状態が続いた場合にsshセッションを切断するまでの間隔を300~3600で指定できます。0を指定した場合、アイドルタイムアウトは行われません。

設定項目の説明

項目	内容
SSHサーバを有効にする	SSHサーバ機能を有効にし、SSHアクセスできるようにします。
ポート	SSHサーバが待ち受けを行うポートを設定します。
パスワード認証	SSHサーバのパスワード認証機能を有効にします。
キープアライブの間隔【秒】	SSHサーバとのSSHセッション維持のためのデータを送信する間隔を設定します。
アイドルタイムアウトの間隔【秒】	SSHサーバ、クライアント間で無通信の時間が続いた場合に、SSHセッションを切断するまでのタイムアウト時間を設定します。

SSHキー

- SSH で使用する公開鍵の設定を行えます。



root タブは設定できません。suncorp タブを選択し、suncorp ユーザに公開鍵を設定してください。

SSHキー

SSH公開鍵認証で使用するSSH公開鍵を1行ずつペーストしてください。

root suncorp

SSHキー設定の説明

項目	内容
suncorp タブ	suncorp ユーザーの SSH 公開鍵を設定します。

2-3 システムログ

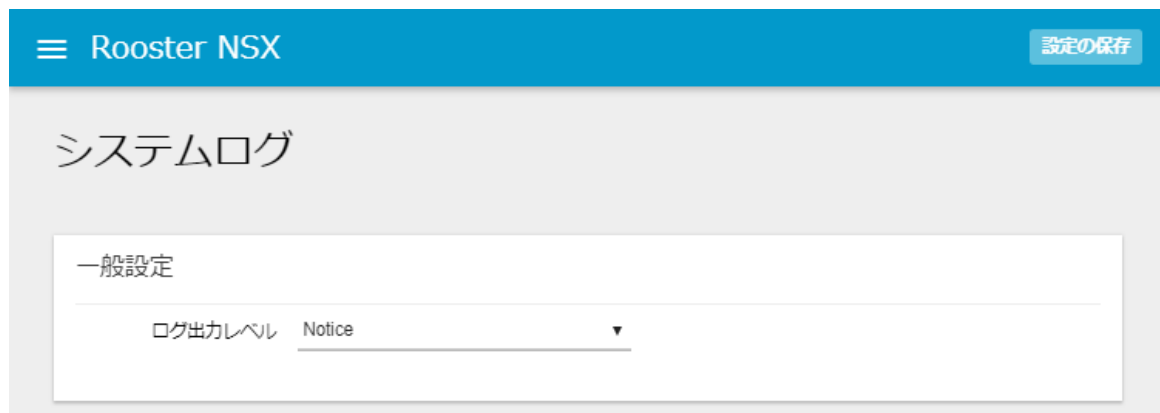
■ 概要

[システム] - [システムログ] ページについて説明します。

システムログ設定ページでは、システムログに関する設定を行うことができます。

2-3-1 一般設定

本装置に保存するシステムログのログレベルを設定します。



Rooster NSX

設定の保存

システムログ

一般設定

ログ出力レベル Notice ▼

■ 設定項目の説明

項目	内容
ログ出力レベル	システムログファイルに出力するログのレベルを設定します。

2-3-2 転送先の設定

外部に設置した syslog サーバにシステムログを転送する設定をします。

転送先の設定

外部システムログ・サーバー	203.0.113.2
外部システムログ・サーバーポート	514
外部システムログ・サーバープロトコル	udp ▼
フォーマット	Traditional ▼

設定項目の説明

項目	内容
外部システムログ・サーバー	システムログの転送先アドレスを設定します。
外部システムログ・サーバーポート	システムログの転送先のサーバーポートを設定します。
外部システムログ・サーバープロトコル	転送先のサーバのプロトコルを設定します。 udp : プロトコル UDP を指定します。 tcp : プロトコル TCP を指定します。
フォーマット	転送するシステムログのフォーマットを設定します。 Traditional : RFC3164 で定められたフォーマットです。 Modern : RFC5424 で定められたフォーマットです。

2-4 Web設定ツール

概要

[システム] - [Web 設定ツール] ページについて説明します。

Web 設定ツールへのアクセスに関わる設定ができます。



Rooster NSX 設定の保存

Web設定ツール

一般設定

HTTP待ち受けポート 80

HTTPS待ち受けポート 443

プライベートIP フィルタ

パブリックIPを持っている場合、プライベートIPからのアクセスを禁止します。

設定項目の説明

項目	内容
HTTP 待ち受けポート	HTTP の待ち受けポートを設定します。
HTTPS 待ち受けポート	HTTPS の待ち受けポートを設定します。
プライベート IP フィルタ	一部特殊な環境からのプライベート IP アドレスによるアクセスを禁止します。 通常の同一ネットワークからのアクセスには影響ありません。



待ち受けポートを変更すると、Web 設定ツールとのセッションが切断されます。

2-5 電源制御

概要

[システム] - [電源制御] ページについて説明します。

電源制御ページでは、自動的に再起動を行う設定ができます。



【電源制御の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=reboot>

2-5-1 ハードウェア電源制御

- ハードウェアによる時刻監視で再起動を行います。

☰ Rooster NSX 設定の保存

電源制御

電源制御の設定を行います。電源制御では自動的な再起動処理を行います。

ハードウェア電源制御

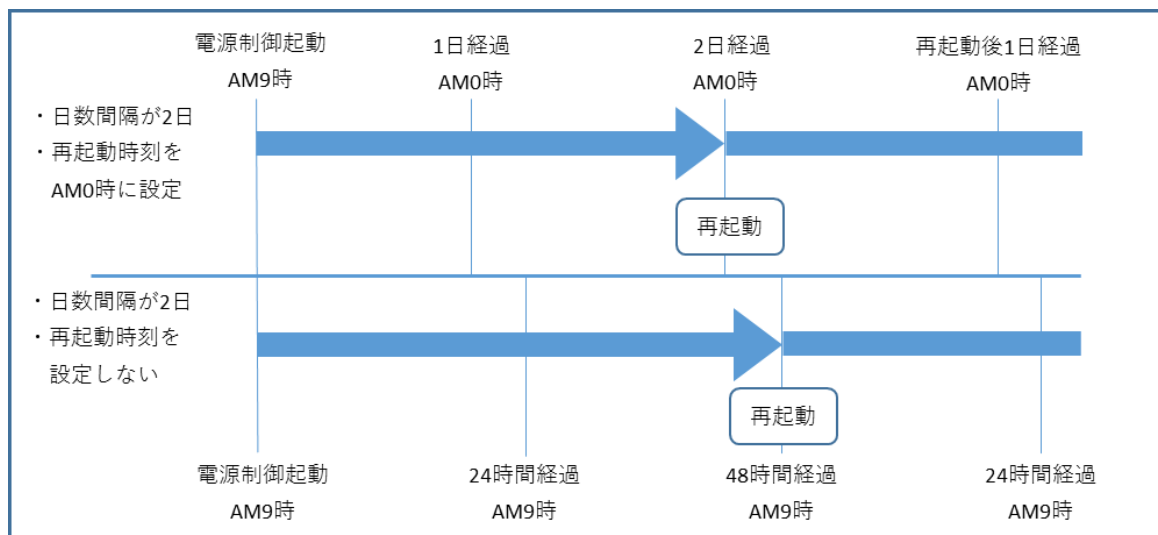
有効にする	<input checked="" type="checkbox"/>
間隔 (日)	1 ▼
再起動時刻を指定する	<input checked="" type="checkbox"/>
再起動時刻 (時)	0 ▼

設定項目の説明

項目	内容
有効にする	ハードウェア電源制御が有効になります。
間隔 (日)	指定した日数経過すると再起動を行います。
再起動時刻を指定する	再起動を行う時刻を指定できます。
再起動時刻 (時)	再起動を行う時刻を 0 時～23 時の範囲で指定できます。(1 時間単位)

■ ハードウェア電源制御の動作説明

- 時刻を設定した場合、ハードウェア電源制御が有効になった時刻から、設定時刻に「間隔（日）」の回数到達する時刻に再起動します。
- 時刻を設定しない場合、ハードウェア電源制御が有効になった時刻から、「間隔（日）×24 時間」後に再起動します。



2-5-2 ソフトウェア電源制御(日数)

- システムの時刻で指定された時刻に日数をカウントし、再起動を行います。
- ソフトウェア電源制御では、PPP の回線接続状態を監視できます。

ソフトウェア電源制御

有効にする

回線接続中に強制再起動

再起動時刻 (時) 0 ▼

再起動時刻 (分) 0 ▼

再起動間隔 日数 ▼

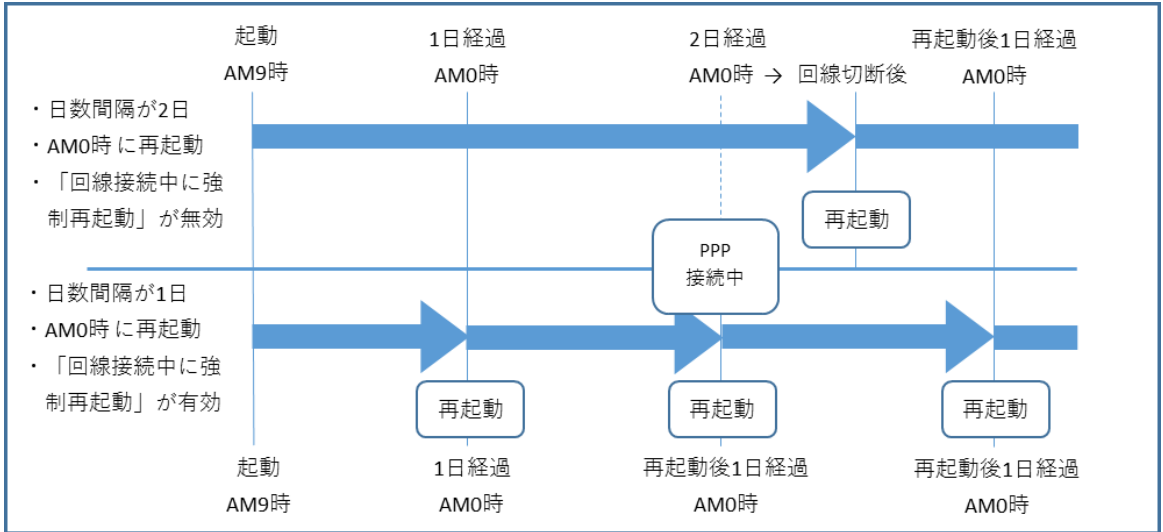
間隔 (日) 1 ▼

設定項目の説明

項目	内容
有効にする	ソフトウェア電源制御が有効になります。
回線接続中に強制再起動	有効にした場合、PPP 回線が接続中の場合でも強制的に再起動を行います。 無効の場合、PPP 回線が切断されるのを待ちます。
再起動時刻 (時)	再起動を行う時刻を指定できます。 0 時～23 時を指定できます。
再起動時刻 (分)	再起動を行う時刻を指定できます。 0 分～59 分を指定できます。
再起動間隔	再起動を行う間隔を「日数」または「曜日指定」の 2 つを指定できます。
間隔 (日)	指定した日数経過すると再起動を行います。

ソフトウェア電源制御(回数)の動作説明

- 起動したタイミングに関わらず、指定時刻に再起動します。
- 「回線接続中に強制再起動」が無効な場合、再起動のタイミングで PPP が接続中の場合は PPP の切断を待ってから再起動します。



2-5-3 ソフトウェア電源制御(曜日指定)

- システムの時刻を利用して指定された曜日・時刻に再起動を行います。

ソフトウェア電源制御

有効にする

回線接続中に強制再起動

再起動時刻 (時) 0 ▼

再起動時刻 (分) 0 ▼

再起動間隔 曜日指定 ▼

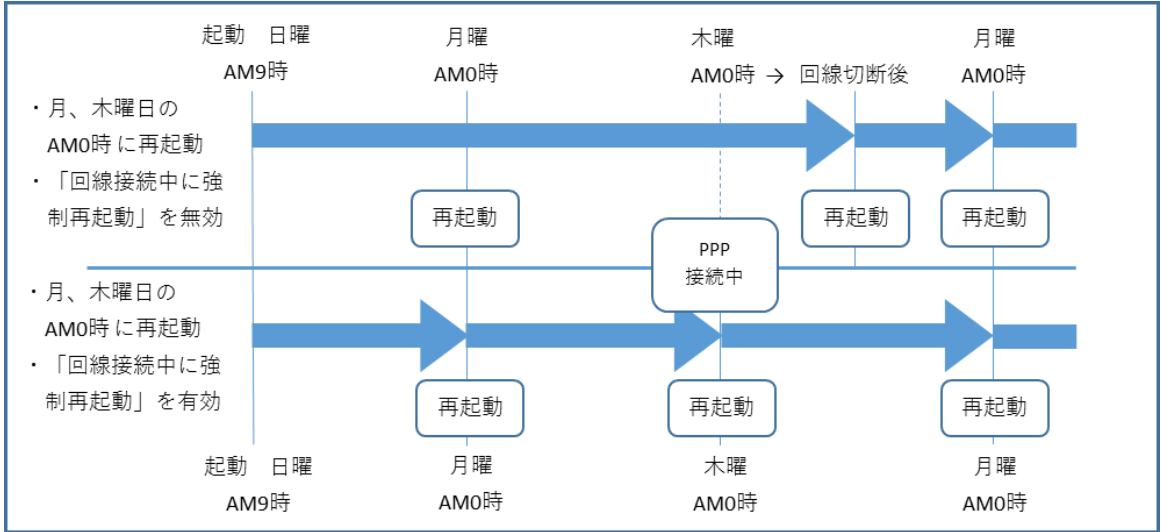
間隔 (曜日) 日 月 火 水 木 金 土

■ 設定項目の説明

項目	内容
有効にする	ソフトウェア電源制御が有効になります。
回線接続中に強制再起動	有効にした場合、PPP 回線が接続中の場合でも強制的に再起動を行います。 無効の場合、PPP 回線が切断されるのを待ちます。
再起動時刻 (時)	再起動を行う時刻を指定できます。 0 時～23 時を指定できます。
再起動時刻 (分)	再起動を行う時刻を指定できます。 0 分～59 分を指定できます。
再起動間隔	再起動を行う間隔を「日数」または「曜日指定」の 2 つを指定できます。
間隔 (曜日)	指定した曜日に再起動を行います。

■ ソフトウェア電源制御(曜日)の動作説明

- 指定した曜日・時刻に再起動を行います。
- ソフトウェア電源制御が有効になってから次の「間隔(曜日)」の設定時刻に再起動します。
- 「回線接続中に強制再起動」が無効な場合、再起動のタイミングで PPP が接続中の場合は PPP の切断を待ってから再起動します。



2-6 おやすみモード

概要

[システム] - [おやすみモード] ページについて説明します。

おやすみモードは本装置をスリープ状態にすることで動作中の機能が停止し、消費電力を下げることができます。おやすみモードページでは、スリープ状態への移行条件を設定できます。



スリープ状態へ移行すると全機能が停止する為、下記アクションが発生するまで本装置は操作できなくなります。

タイマーモード : SMS の受信

スケジュールモード : スケジュールで指定したレジャーム時刻、又は SMS の受信

【おやすみモードの設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=sleep>

2-6-1 タイマーモード

- タイマーモードを設定すると PPP の切断状態が一定時間続いた場合におやすみモードへ移行します。



「3-2Bacsoft IoT Platform」の設定が有効な場合、おやすみモードに移行しません。

モバイル通信の接続設定が未設定の場合、おやすみモードに移行しません。
「4-2 モバイル」の接続設定を行ってください。

通信モジュールのソフトウェアバージョンが「11-15」以前の場合、利用できません。
「1-1-2 通信ボード」をご確認ください。



タイマーモードは SMS 着信でおやすみモードから復帰します。

SMS が利用できない SIM の場合、おやすみモードから復帰できず、本装置が操作できなくなります。

必ず SMS が利用可能な SIM で「4-2 モバイル」の接続設定を行ってください。

Rooster NSX

設定の保存

一般設定 スケジュール

おやすみモード

おやすみモードの設定を行います。

おやすみモード設定

おやすみモードを有効にする

動作モード タイマーモード ▼

サスペンドまでの待機時間 (分) 10 ▼

設定項目の説明

項目	内容
おやすみモードを有効にする	おやすみモードへの移行が有効になります。
動作モード	おやすみモードへの移行条件を設定できます。 タイマーモード : PPP の切断状態が一定時間続くと移行します。 スケジュールモード : 指定した曜日、時間に移行します。
サスペンドまでの待機時間 (分)	タイマーモードで有効な設定で、本項目で指定した時間、PPP の切断状態が続くとおやすみモードへ移行します。

2-6-2 スケジュールモード

- 指定した曜日・時刻の間、おやすみモードへ移行します。
- おやすみモード移行中に SMS を受信した場合、一時的に復帰します。

Rooster NSX

[設定の保存](#)
[一般設定](#) [スケジュール](#)

おやすみモード

おやすみモードの設定を行います。

おやすみモード設定

おやすみモードを有効にする

動作モード スケジュールモード

タブ項目の説明

項目	内容
スケジュール	スケジュールの詳細設定を行うページを表示します。

設定項目の説明

項目	内容
おやすみモードを有効にする	おやすみモードへの移行が有効になります。
動作モード	おやすみモードへの移行条件を設定できます。 タイマーモード : PPP の切断状態が一定時間続くと移行します。 スケジュールモード : 指定した曜日、時間に移行します。

■ スケジュールモード(スケジュール設定一覧)

- 現在のスケジュール情報を表示します。

☰ Rooster NSX
設定の保存

一般設定
スケジュール

おやすみモード

スケジュール一覧

サスペンド曜日	サスペンド時刻	レジューム曜日	レジューム時刻		
土曜日	00:00	日曜日	23:59	編集	消去
追加					

■ タブ項目の説明

項目	内容
一般設定	おやすみモードの有効、無効、モード選択を行うページを表示します。

■ スケジュール一覧の説明

項目	内容
サスペンド曜日	おやすみモードへ移行する曜日を表示します。
サスペンド時刻	おやすみモードへ移行する時刻を表示します。
レジューム曜日	おやすみモードから復帰する曜日を表示します。
レジューム時刻	おやすみモードから復帰する時刻を表示します。
編集	設定済みのスケジュールの編集が行えます。
消去	設定済みのスケジュールを削除できます。
追加	新たにスケジュールを追加できます。

■ スケジュールモード(スケジュールの設定)

- 追加・編集を押下するとスケジュールの設定画面を表示します。

≡ Rooster NSX

設定の保存

保存されていない変更: 1

一般設定 スケジュール

おやすみモード - スケジュール設定

スケジュール設定

サスペンド曜日	土曜日	▼
サスペンド時刻	00:00	
レジャー曜日	日曜日	▼
レジャー時刻	23:59	

■ スケジュール設定項目の説明

項目	内容
サスペンド曜日	おやすみモードへ移行する曜日を指定できます。 日曜日～土曜日を設定できます。
サスペンド時刻	おやすみモードへ移行する時刻が指定できます。 00:00～23:59 を設定できます。
レジャー曜日	おやすみモードから復帰する曜日を指定できます。 日曜日～土曜日を設定できます。
レジャー時刻	おやすみモードから復帰する時刻が指定できます。 00:00～23:59 を設定できます。

2-7 パッケージ管理

概要

[システム] - [パッケージ管理] ページについて説明します。

パッケージ管理画面では、本装置のファームウェアや、本装置上で動作するプログラムパッケージを管理できます。サン電子が提供するパッケージの他、お客様が作成された独自のパッケージをインストール、アンインストールできます。

memo

パッケージのインストール/アンインストールを行った場合、再起動が必要です。

回線状況などにより、ファイルアップロードに時間がかかる場合があります。
その場合は、正常な結果が表示されない場合があります。

【パッケージのインストール方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=package>

Rooster NSX

設定の保存

パッケージ管理

パッケージのインストール/アンインストール

パッケージのインストール:

ファイルを選択 選択されていません

インストール

① ファームウェアの更新とパッケージの更新が出来ます。RSYS,RFRM,RTARファイルを指定してください。
回線状況などにより、ファイルアップロードに時間がかかる場合があります。
その場合は正常な結果が表示されないことがあります。

パッケージの署名を無視する:

① チェックを有効にすると、署名のないパッケージをインストールすることができます

パッケージのアンインストール:

adopt-openjdk-java - 11.0.1.13.1

アンインストール

① Add-onアプリケーションのみアンインストールできます。

パッケージリスト

```
Current:
Rooster-NSX-7000 - 1.5.0 - RoosterOS system file
system-nsx7000 - 1.5.0 - RoosterOS base system
adopt-openjdk-java - 11.0.1.13.1
----
```

```
Another:
Rooster-NSX-7000 - 1.5.0 - RoosterOS system file
system-nsx7000 - 1.5.0 - RoosterOS base system
adopt-openjdk-java - 11.0.1.13.1
```

ボタンの説明

項目	内容
インストール	「ファイル選択エリア」で選択されたパッケージをインストールします。
アンインストール	選択されたパッケージをアンインストールします。

設定項目の説明

項目	内容
パッケージのインストール	ファイル選択エリア： インストールするパッケージファイルを選択します。
パッケージの署名を無視する	パッケージの署名を無視します。 ※このチェックボックスにチェックを行うことで、パッケージ署名のない、パッケージもインストールできます。
パッケージのアンインストール	選択エリア： アンインストールするパッケージを選択します。

パッケージリストの表示内容

項目	内容
Current	現在システムが使用しているファームウェアの領域にインストールされたパッケージを表示します。
Another	現在システムが使用していないファームウェアの領域にインストールされたパッケージを表示します。

2-8 ブートエリア

概要

[システム] - [ブートエリア] ページについて説明します。

本装置には長期的に安定した動作を実現する為に、ファームウェアの領域を2つ持っています。

ブートエリアページでは、明示的に起動するブートエリアを変更できます。



本装置起動時にファームウェアの領域でエラーが発生した場合に、自動的に別の面のファームウェアを使用します。

☰ Rooster NSX
設定の保存

ブートエリア

現在のブートエリア

a-side

ブートエリアの変更

別の面 ▼ エリアの変更

現在のブートエリアの表示内容

項目	内容
現在のブートエリア	現在システムが使用しているブート領域を表示します。

設定項目の説明

項目	内容
ブートエリアの変更	別の面 :
	現在システムが使用しているブート領域とは別の領域を選択します。
	A面 :
	A面を選択します。
	B面 :
	B面を選択します。

2-9 バックアップ

概要

[システム] - [バックアップ] ページについて説明します。

バックアップページでは、フラッシュメモリに保存された設定（起動時に適用されるコンフィグ）をバックアップファイルとしてダウンロードできます。

また、ダウンロードしたファイルを本装置にアップロードして設定の復元が行えます。



「バックアップから復元する」を実行後、設定の反映は再起動後に行われます。

【バックアップ機能の利用方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=backup>



設定の復元を行うと、フラッシュメモリに保存された設定は上書きされます。

☰ Rooster NSX

設定の保存

設定のバックアップ

バックアップ / 復元

バックアップのダウンロードをクリックしてバックアップファイルのアーカイブをダウンロードしてください。

バックアップアーカイブのダウンロード:

バックアップのダウンロード

バックアップファイルを復元するには、以前にダウンロードしたバックアップアーカイブをここにアップロードします。

バックアップから復元する:

ファイルを選択

選択されていません

アーカイブをアップロード

ボタンの説明

項目	内容
バックアップのダウンロード	フラッシュメモリに保存された設定ファイルをバックアップとしてダウンロードします。
アーカイブをアップロード	「バックアップのダウンロード」で取得した設定ファイルを本装置のフラッシュメモリに保存します。

設定項目の説明

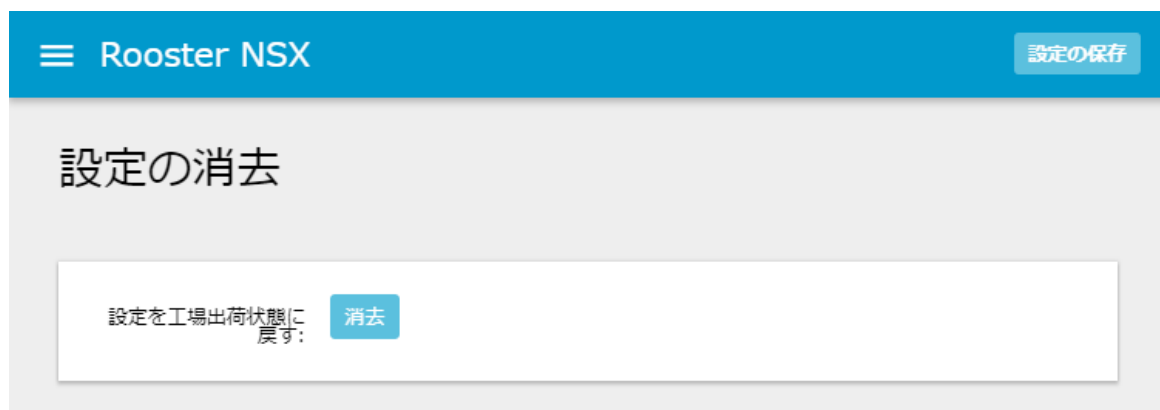
項目	内容
ファイルを選択	「バックアップのダウンロード」で取得したファイルを指定してください。

2-10 設定の消去

概要

[システム] - [設定の消去] ページについて説明します。

設定の消去ページでは、フラッシュメモリに保存された設定を全て消去し、工場出荷状態に初期化できません。



ボタン項目の説明

項目	内容
消去	設定を工場出荷状態へ戻します。

2-11 診断情報の取得

概要

[システム] - [診断情報の取得] ページについて説明します。

診断情報の取得ページでは、本装置の現在の情報をまとめたファイルを取得できます。



取得できるファイルは、弊社解析用の特殊なファイルです。



使用状態により、取得ファイルが非常に大きくなる場合があります。

☰ Rooster NSX 設定の保存

診断情報の取得

診断情報の取得には時間がかかります。ダウンロードボタンをクリックした後は、ページを閉じたりせず、そのままお待ちください。

診断情報の取得: [ダウンロード](#)

ボタン項目の説明

項目	内容
ダウンロード	本装置で診断情報の収集が行われ、結果ファイルがダウンロードされます。

2-12 再起動 / シャットダウン

概要

[システム] - [再起動 / シャットダウン] ページについて説明します。

本装置の再起動とシャットダウンを行うことができます。



再起動又はシャットダウンを実行すると、フラッシュメモリに保存されていない設定は破棄されます。**設定の保存**の実行が必要かご確認ください。



本装置を安全に終了させるため、電源を切る前に必ずシャットダウンを行ってください。シャットダウン実行後、本装置のLED状態を確認してから電源をお切りください。

☰ Rooster NSX

設定の保存

再起動 / シャットダウン

デバイスのオペレーティングシステムを再起動

再起動を実行

デバイスのシャットダウン

デバイスをシャットダウンする

ボタン項目の説明

項目	内容
再起動を実行	再起動します。
デバイスをシャットダウンする	シャットダウンします。

3章 サービス

この章では、本装置が提供するソリューションサービス用の設定について説明します。

3-1 SunDMS

概要

[サービス] - [SunDMS] ページについて説明します。

SunDMS ページでは、本装置が SunDMS サーバへ接続を行う為の環境設定を変更できます。



「SunDMS」は弊社が提供するサービスで、「デバイスの遠隔集中管理」に対応しています。

詳細については以下の URL をご覧ください。

<https://www.sun-denshi.co.jp/sc/dms/>

【SunDMS の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=sundms>

Rooster NSX

設定の保存

SunDMS

SunDMSの設定を行います。

接続先設定

SunDMS機能を無効にする

DMSサーバアドレス

DMSサーバポート

プロキシサーバアドレス

プロキシサーバポート

ノーマルポーリングのみ使用する

設定項目の説明

項目	内容
SunDMS 機能を無効にする	SunDMS エージェント機能が停止します。
DMS サーバアドレス	SunDMS サーバと接続する為のアドレスを設定できます。
DMS サーバポート	接続先ポート番号を設定できます。
プロキシサーバアドレス	プロキシサーバのアドレスを設定できます。
プロキシサーバポート	プロキシサーバのポート番号を設定できます。
ノーマルポーリングのみ使用する	ノーマルポーリング設定で動作します。

3-2 Bacsoft IoT Platform

概要

[サービス] - [Bacsoft IoT Platform] ページについて説明します。

Bacsoft IoT Platform 設定ページでは Bacsoft IoT Platform の使用・不使用を設定できます。



「Bacsoft IoT Platform」は弊社が提供するサービスで、PLC（プログラマブルロジックコントローラ）および産業機器や様々なセンサーデバイスなどに対して「機器情報の収集、管理」、「機器の状態監視、異常通報」、「機器の制御」、「データ保存」等のサービスを提供しています。

詳細については、以下の URL をご覧ください。

<https://www.sun-denshi.co.jp/sc/bacsoft/>

※Bacsoft IoT Platform をご使用の際は、別途お申し込みが必要です。詳細につきましては、上記 URL もしくは、弊社営業部までお問い合わせください。



Bacsoft IoT Platform を利用する場合、以下機能が無効になります。

- ・ Web 設定ツール、本装置の LED による信号強度の表示
- ・ 「2-1-2 時刻設定」のモバイルによる時刻調整機能
- ・ 「2-6 おやすみモード」のタイマーモード機能
- ・ 「4-3 プロファイル」の SMS コールバック機能

Rooster NSX

設定の保存

Bacsoft IoT Platform

Bacsoft IoT Platformの設定を行います。

Bacsoft IoT Platform設定

Bacsoft IoT Platform
を使用する

- ① チェックすると以下の機能を無効にします：
- Webブラウザ・LEDによる信号強度表示
 - モバイル端末装置の時間を使用した時間同期
 - おやすみモードのタイマーモード
 - SMSコールバック

設定項目の説明

項目	内容
Bacsoft IoT Platform を使用する	Bacsoft IoT Platform を使用する場合、チェックします。

3-3 ダイナミックDNS

概要

[サービス] - [ダイナミック DNS] ページについて説明します。

ダイナミック DNS ページでは、suncomm.DDNS の環境設定を行うことができます。



ダイナミック DNS サービス「suncomm.DDNS」は、固定 IP アドレスを取得する事なくドメイン名（〇〇〇.suncomm.net）でインターネット上のサーバ等にアクセスする事を可能とする「Rooster（ルースター）」専用のサービスです。

詳細については、以下の URL を参照してください。

<https://www.sun-denshi.co.jp/sc/ddns/>

【ダイナミック DNS の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=dynamicdns>

☰ Rooster NSX

設定の保存
自動更新 オン

ダイナミックDNS

ダイナミックDNSを使用することで、IPアドレスが変更されても固定のホスト名を使ってルーターにアクセスすることができます。

概要

設定	Lookup ホスト名 登録IP	有効	最後のアップデート 次のアップデート	プロセスID 開始 / 停止	
example	████████.suncomm.net 203.0.113.11	<input checked="" type="checkbox"/>	2019-04-17 11:14 2019-04-20 11:14	PID: 23560	編集 消去

新しいDDNS設定:

設定

DDNS設定名

追加

ボタン項目の説明

項目	内容
編集	追加済みの設定を編集します。
消去	設定を消去します。
追加	設定を追加します。DDNS 設定名を入力後、押下ください。

設定項目の説明

項目	内容
有効	DDNS の設定を有効にします。
設定	DDNS の設定名を入力します。

基本設定

- suncomm.DDNS サービスを利用する為のユーザ名、パスワード設定等を行えます

Rooster NSX

[設定の保存](#)

ダイナミックDNS

ダイナミックDNSを使用することで、IPアドレスが変更されても固定のホスト名を使ってルーターにアクセスすることができます。

Details for: example

選択したDDNSサービスの詳細を設定します

基本設定 詳細設定 タイマー設定 ログファイルの表示

有効

このオプションが無効になっている場合、サービスは開始できません

Lookup ホスト名

IPアップデートが発生した場合または検証の際に使用するホスト名/FQDN

IPアドレスバージョン IPv4

DDNSサービスプロバイダ

ドメイン

ユーザー名

パスワード 

設定項目の説明

項目	内容
有効	設定を有効にします。
Lookup ホスト名	登録した IP アドレスを確認する為のホスト名を設定します。
DDNS サービスプロバイダ	suncomm.DDNS を指定できます。 ※「手動設定」はサポートしない機能です。
ドメイン	IP アドレスの登録先のドメイン名を設定します。 suncomm.DDNS は「Lookup ホスト名」と「ドメイン」は同じ値を設定します。
ユーザー名	ユーザー名を設定します。
パスワード	パスワードを設定します。

詳細設定

- suncomm.DDNS サービスに登録する IP アドレス等の環境設定が行えます。

Rooster NSX

[設定の保存](#)

ダイナミックDNS

ダイナミックDNSを使用することで、IPアドレスが変更されても固定のホスト名を使ってルーターにアクセスすることができます。

Details for: example

選択したDDNSサービスの詳細を設定します

基本設定	詳細設定	タイマー設定	ログファイルの表示
IPアドレスソース [IPv4]	ネットワーク		
	ⓘ DDNSプロバイダに送信されるIPv4アドレスからシステムを読み込むソースを定義します		
ネットワーク [IPv4]	ppp0		
	ⓘ IPv4アドレスからシステムを読み込むネットワークを定義します		
プロキシサーバ			
	ⓘ オプション: 検出及び更新用のプロキシサーバ フォーマット: [user:password@]proxyhost:port		
ログ出力レベル	Notice		
	ⓘ ログメッセージをシステムログに書き込みます。重大なエラーは常にシステムログに書き込まれます。		
Log to file	<input checked="" type="checkbox"/>		
	ⓘ 詳細なメッセージをログファイルに書き込みます。 ファイル: "/var/log/ddns/example.log"		

設定項目の説明

項目	内容
IP アドレスソース	登録する IP アドレスの取得元を設定します。 「4-1-1 インターフェース一覧」ページのインターフェースを選択できるようになります。
ネットワーク	「4-1-1 インターフェース一覧」で設定されたインターフェースから登録する IP アドレスを取得します。
プロキシサーバ	プロキシサーバを指定できます。
ログ出力レベル	DDNS サービスのログ出力レベルを変更できます。



タイマー設定、ログファイルの表示の設定は、バージョン 1.5.0 ではサポートしない機能です。

4章 ネットワーク

この章では、本装置のネットワーク設定について説明します。

4-1 インターフェース

概要

[ネットワーク] - [インターフェース] ページについて説明します。

LAN のアドレスやモバイル通信用のインタフェース設定を行えます。

プロトコル毎に設定が異なりますので、使用方法にあったページを参照ください。

4-1-1 インターフェース一覧

- 「インターフェース一覧」はインタフェースのステータス表示、インタフェースの追加・編集・削除、インタフェースの接続・切断が行えます。

Rooster NSX

設定の保存 自動更新 オン

インターフェース

インターフェース一覧

ネットワーク	ステータス	動作
ETH0 eth0	起動時間: 0h 2m 45s MAC-アドレス: 00:00:5E:00:53:00 RX: 206.97 KB (1708 パケット) TX: 902.20 KB (1572 パケット) IPv4: 192.168.62.1/24	接続 停止 編集 消去
ETH1 eth1	起動時間: 0h 0m 53s MAC-アドレス: 00:00:5E:00:53:01 RX: 12.93 KB (202 パケット) TX: 0 B (0 パケット)	接続 停止 編集 消去
PPP0 ppp-ppp0	RX: 0 B (0 パケット) TX: 0 B (0 パケット)	接続 停止 編集 消去

インターフェースの新規作成...

ボタン項目の説明

項目	内容
接続	インタフェースを有効にし、ネットワークへ接続します。
停止	インタフェースを無効にし、ネットワークから切断します。
編集	インタフェースの設定を行います。
消去	インタフェースを削除します。
インターフェースの新規作成	インタフェースを追加します。

4-1-2 インターフェースの作成

- 「インターフェース一覧」ページの「インターフェースの新規作成」をクリックすると「インターフェースの作成」ページを表示します。
- プロトコルや紐付くインターフェースを設定できます。
- インターフェースの「一般設定」、「詳細設定」についてプロトコル別の説明を参照ください。

☰ Rooster NSX
設定の保存

インターフェースの作成

新しいインターフェースの名前

① 使用可能な文字は右記の通りです: A-Z, a-z, 0-9, _

注意: インターフェース名の長さ ② 名前の最大長は、自動プロトコル/ブリッジプレフィックス(br-, 6in4-, pppoe- etc.)を含めて15文字です。

新しいインターフェースのプロトコル 静的アドレス ▼

複数のインターフェースを指定してブリッジを作成します

インターフェースの指定

- イーサネットアダプタ: "eth0" ([eth0](#))
- イーサネットアダプタ: "eth1" ([eth1](#))
- イーサネットアダプタ: "ip_vti0"
- 新しいインターフェース:

概要へ戻る
送信

ボタン項目の説明

項目	内容
送信	入力した内容でインターフェースを作成します。

■ 設定項目の説明

項目	内容
新しいインターフェースの名前	インターフェース名を設定します。
新しいインターフェースのプロトコル	インターフェースが使用するプロトコルを選択します。 詳細は「プロトコルの説明」を参照ください。
複数のインターフェースを指定してブリッジを作成します	複数のインターフェースを一つのインターフェースに統合してブリッジ接続する場合にチェックを入れます。
インターフェースの指定	インターフェースに対応したアダプタを選択するか、「新しいインターフェース」を選択してインターフェース名を設定します。 「複数のインターフェースを指定してブリッジを作成します」にチェックを入れた場合は、一つ以上のインターフェースを選択します。

■ プロトコルの説明

項目	内容
静的アドレス	IP アドレスを手動設定する場合に選択します。
DHCP クライアント	DHCP サーバから IP アドレスを取得する場合に選択します。
Unmanaged	IPsec を使用する場合に選択します。
PPP	PPP でインターネットに接続する場合に選択します。
PPPoE	有線 WAN 回線を使用して PPP でインターネットに接続する場合に選択します。
VPN	PPTP、L2TP/IPsec を使用する場合に選択します。

4-1-3 プロトコル:静的アドレス

■ 一般設定 (静的アドレス)

- IP アドレスに関する設定が行えます。

☰ Rooster NSX

設定の保存
自動更新 オン

インターフェース - ETH1

このページではネットワークインターフェースの設定を行うことができます。

一般設定
詳細設定
デバイス設定
ファイアウォール設定

ステータス
起動時間: 0h 30m 20s
MAC-アドレス: 00:00:5E:00:53:01
eth1 **RX:** 69.44 KB (1085 パケット)
TX: 0 B (0 パケット)

プロトコル
静的アドレス
▼

IPv4 アドレス

IPv4 ネットマスク

▼

IPv4 ゲートウェイ

IPv4 ブロードキャスト

DNSサーバーを手動で設定

+

■ 設定項目の説明

項目	内容
プロトコル	プロトコルを「静的アドレス」から変更する場合、他のプロトコルを選択します。
IPv4 アドレス	IP アドレスを設定します。
IPv4 ネットマスク	ネットマスクを設定します。 適切なネットマスクを選択するか、手動設定を選択してネットマスクを設定します。
IPv4 ゲートウェイ	デフォルトゲートウェイを設定します。
IPv4 ブロードキャスト	ネットワークのブロードキャストアドレスを設定します。
DNS サーバーを手動で設定	DNS サーバを設定します。

■ 詳細設定(静的アドレス)

☰ Rooster NSX

設定の保存

自動更新 オン

インターフェース - ETH1

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定 詳細設定 デバイス設定 ファイアウォール設定

デフォルトで起動する

MACアドレスを上書きする 00:00:5E:00:53:01

MTUを上書きする 1500

ゲートウェイ・メトリックを使用する 0

■ 設定項目の説明

項目	内容
デフォルトで起動する	システム起動時にインターフェースを作成します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。
MAC アドレスを上書きする	インターフェースが使用する MAC アドレスを設定します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。
MTU を上書きする	インターフェースの MTU 値を設定します。
ゲートウェイ・メトリックを使用する	ルーティングのメトリックを設定します。

4-1-4 プロトコル:DHCPクライアント

■ 一般設定 (DHCPクライアント)

- DHCP クライアントとして動作し、リクエスト時のホスト名を設定できます。



【DHCP クライアントの設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=dhcp-client>

☰ Rooster NSX

設定の保存
自動更新 オン

インターフェース - ETH1

このページではネットワークインターフェースの設定を行うことができます。

一般設定
詳細設定
デバイス設定
ファイアウォール設定

ステータス	<div style="font-size: 0.8em; color: #ccc;"> 起動時間: 0h 12m 38s MAC-アドレス: 00:00:5E:00:53:03 RX: 86.83 KB (884 パケット) TX: 415.54 KB (504 パケット) IPv4: 192.168.62.244/24 </div>
プロトコル	<div style="border-bottom: 1px solid #ccc; display: flex; align-items: center;"> DHCP クライアント ▼ </div>
DHCPリクエスト時に送信するホスト名	<div style="border-bottom: 1px solid #ccc; display: flex; align-items: center;"> PC </div>

■ 設定項目の説明

項目	内容
プロトコル	「DHCP クライアント」から変更する場合は他のプロトコルを選択します。
DHCP リクエスト時に送信するホスト名	DHCP リクエスト時に送信するホスト名を設定します。

■ 詳細設定 (DHCPクライアント)

- DHCP クライアントの詳細設定が行えます。

☰ Rooster NSX

設定の保存

自動更新 オン

インターフェース - ETH1

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定	詳細設定	デバイス設定	ファイアウォール設定
デフォルトで起動する	<input checked="" type="checkbox"/>		
ブロードキャスト・フラグを使用する	<input type="checkbox"/>		① DOCSIS 3.0を使用するいくつかのISPでは必要になります
デフォルトゲートウェイを使用する	<input checked="" type="checkbox"/>		① チェックされていない場合、デフォルトルートを設定しません。
ピアから通知されたDNSサーバーを使用する	<input checked="" type="checkbox"/>		① チェックされていない場合、通知されたDNSサーバーアドレスを無視します。
ゲートウェイ・メトリックを使用する	0		
DHCPリクエスト時に送信するクライアントID			
DHCPリクエスト送信時のベンダークラスを設定			
MACアドレスを上書きする	00:00:5e:00:53:03		
MTUを上書きする	1500		

設定項目の説明

項目	内容
デフォルトで起動する	システム起動時にインターフェースを作成します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。
ブロードキャスト・フラグを使用する	ブロードキャスト・フラグをオンにします。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。
デフォルトゲートウェイを使用する	デフォルトゲートウェイを追加します。 チェックされていない場合、追加しません。
ピアから通知された DNS サーバーを使用する	DHCP サーバから通知された DNS サーバを使用します。
DNS サーバーを手動で設定	「ピアから通知された DNS サーバーを使用する」のチェックを外すと表示・設定できます。 DNS サーバを設定します。
ゲートウェイ・メトリックを使用する	ルーティングのメトリックを設定します。
DHCP リクエスト時に送信するクライアント ID	DHCP リクエスト時に送信するクライアント ID を設定します。 ※バージョン 1.5.0 ではサポートしない機能です。
DHCP リクエスト送信時のベンダークラスを設定	DHCP リクエスト時に送信するベンダークラスを設定します。 ※バージョン 1.5.0 ではサポートしない機能です。
MAC アドレスを上書きする	インターフェースが使用する MAC アドレスを設定します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。
MTU を上書きする	インターフェースの MTU 値を設定します。

4-1-5 プロトコル:PPP

■ 一般設定 (PPP)

- PPP でインターネット接続を行う為のプロファイル設定が行えます。
- 固定 IP アドレスを取得する設定が行えます。



PPP 接続を行うには「4-2 モバイル」、「4-3 プロファイル」の設定が必要です。

【PPP の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=ppp>

☰ Rooster NSX

設定の保存
保存されていない変更: 3
自動更新 オン

インターフェース - PPP0

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定	詳細設定	ファイアウォール設定
ステータス	RX: 0 B (0 パケット) TX: 0 B (0 パケット) <small>ppp-ppp0</small>	
プロトコル	PPP ▼	
IPアドレス割り当て方法	IPCP ▼	
プロファイル	▼	

■ 設定項目の説明

項目	内容
プロトコル	「PPP」から変更する場合は他のプロトコルを選択します。
IP アドレス割り当て方法	IP アドレスの設定方法を選択します。 IPCP : サーバから割り当てられる IP アドレスを使用する場合に選択します。 Static : 固定 IP アドレス、ネットマスクを設定する場合に選択します。
IP アドレス	IP アドレス割り当て方法に「Static」を選択すると表示・設定できます。 IP アドレスを設定します。
ネットマスク	IP アドレス割り当て方法に「Static」を選択すると表示・設定できます。 適切なネットマスクを選択するか、手動設定を選択してネットマスクを設定します。
プロファイル	プロファイル設定で設定したプロファイルが表示されます。 PPP 接続に使用するプロファイルを選択します。

■ 詳細設定 (PPP)

- PPP 接続後のインタフェースに関する設定ができます。

☰ Rooster NSX

設定の保存

保存されていない変更: 3

自動更新 オン

インターフェース - PPP0

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定

詳細設定

ファイアウォール設定

デフォルトで起動する デフォルトゲートウェイを使用する

? チェックされていない場合、デフォルトルートを設定しません。

ゲートウェイ・メトリックを使用する 0

ピアから通知された DNS サーバーを使用する

? チェックされていない場合、通知された DNS サーバーアドレスを無視します。

MTU を上書きする auto

? auto, 576-65535

■ 設定項目の説明

項目	内容
デフォルトで起動する	システム起動時にインタフェースを作成します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。
デフォルトゲートウェイを使用する	このインタフェースをデフォルトゲートウェイとするルート設定を追加します。 チェックされていない場合、追加しません。
ゲートウェイ・メトリックを使用する	「デフォルトゲートウェイを使用する」をチェックすると表示・設定できます。 ルーティングのメトリックを設定します。
ピアから通知された DNS サーバーを使用する	DHCP サーバから通知された DNS サーバを使用します。
DNS サーバーを手動で設定	「ピアから通知された DNS サーバーを使用する」のチェックを外すと表示・設定 できます。 DNS サーバを手動で設定します。
MTU を上書きする	インタフェースの MTU 値を設定します。

4-1-6 プロトコル: PPPoE

■ 一般設定 (PPPoE)

- 有線 WAN 回線でインターネット接続を行う為の設定が行えます。



【PPPoE の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=pppoe>

☰ Rooster NSX

設定の保存

保存されていない変更: 2

自動更新 オン

インターフェース - ETH1

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定 詳細設定 デバイス設定 ファイアウォール設定

ステータス RX: 0 B (0 パケット)
pppoe-eth1 TX: 0 B (0 パケット)

プロトコル PPPoE ▼

PAP/CHAP ユーザー名 _____

PAP/CHAP パスワード _____

Access Concentrator 自動

🔔 空欄の場合、自動検知を行います

サービス名 自動

🔔 空欄の場合、自動検知を行います

■ 設定項目の説明

項目	内容
プロトコル	「PPPoE」から変更する場合は他のプロトコルを選択します。
PAP/CHAP ユーザー名	ISP 指定のユーザー名を設定します。
PAP/CHAP パスワード	ISP 指定のパスワードを設定します。
Access Concentrator	PPPoE で接続するアクセスコンセントレータの名前を設定します。
サービス名	PPPoE で接続するサービス名を設定します。

■ 詳細設定 (PPPoE)

- PPP 接続後のインターフェースに関する設定ができます。

☰ Rooster NSX

設定の保存

保存されていない変更: 2

自動更新 オン

インターフェース - ETH1

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定

詳細設定

デバイス設定

ファイアウォール設定

デフォルトで起動する デフォルトゲートウェイを使用する

🔗 チェックされていない場合、デフォルトルートを設定しません。

ゲートウェイ・メトリックを使用する 0

ピアから通知されたDNSサーバーを使用する

🔗 チェックされていない場合、通知されたDNSサーバーアドレスを無視します。

LCP echo 失敗数しきい値 0

🔗 設定回数のLCP echo 確認失敗後、ピアノードがダウンしているものと見なします。0を設定した場合、失敗しても無視します。

LCP echo 送信間隔 5

🔗 設定された秒間隔でLCP echoリクエストを送信します。失敗数しきい値を設定した場合のみ、機能が有効になります。

無通信監視時間 0

🔗 設定した秒数後に、使用していない接続を閉じます。0を設定した場合、接続を維持します。

MTUを上書きする 1500

設定項目の説明

項目	内容
デフォルトで起動する	システム起動時にインタフェースを作成します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。
デフォルトゲートウェイを使用する	デフォルトゲートウェイを使用します。チェックされていない場合、デフォルトルートを設定しません。
ゲートウェイ・メトリックを使用する	「デフォルトゲートウェイを使用する」をチェックすると表示・設定できます。ルーティングのメトリックを設定します。
ピアから通知された DNS サーバーを使用する	サーバから通知された DNS サーバを使用します。
DNS サーバーを手動で設定	「ピアから通知された DNS サーバーを使用する」のチェックを外すと表示・設定できます。 DNS サーバーを設定します。
LCP echo 失敗数しきい値	切断動作をするまでの連続失敗回数を設定します。
LCP echo 送信間隔	LCP Echo Request の送信間隔（秒）を設定します。
無通信監視時間	指定した秒数の間、データ通信が行われない場合に接続を切断します。空欄の場合や「0」を設定した場合は無通信監視を行いません。
MTU を上書きする	インタフェースの MTU 値を設定します。

4-1-7 プロトコル:VPN

■ 一般設定 (VPN)

- PPTP、L2TP / IPsec で使用するインターフェースで、設定項目はありません。

memo	PPTP サーバ、L2TP / IPsec サーバを使用するには「4-10PPTP サーバ」、「4-11L2TP/IPsec サーバ」、「4-7 ファイアウォール」の設定が必要です。
	【PPTP サーバの設定方法】 https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=pptp
	【L2TP / IPsec サーバの設定方法】 https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=l2tp-ipsec

☰ Rooster NSX

設定の保存
保存されていない変更: 4
自動更新 オン

インターフェース - VPN0

このページではネットワークインターフェースの設定を行うことができます。

一般設定
詳細設定
デバイス設定
ファイアウォール設定

ステータス

RX: 0 B (0 パケット)
vpn0 **TX:** 0 B (0 パケット)

プロトコル
VPN ▼

■ 設定項目の説明

項目	内容
プロトコル	「VPN」から変更する場合は他のプロトコルを選択します。

■ 詳細設定 (VPN)

- PPTP、L2TP / IPsec で使用するインターフェースで、設定項目はありません。

☰ Rooster NSX 設定の保存 保存されていない変更: 4 自動更新 オン

インターフェース - VPN0

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定 **詳細設定** デバイス設定 ファイアウォール設定

デフォルトで起動する

■ 設定項目の説明

項目	内容
デフォルトで起動する	システム起動時にインターフェースを作成します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。

4-1-8 プロトコル: Unmanaged

■ 一般設定 (Unmanaged)

- IPsec で使用するインターフェースで、設定項目はありません。



IPsec を使用するには「4-9IPsec」、 「4-7 ファイアウォール」 の設定が必要です。

【IPsec の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=ipsec>

☰ Rooster NSX

設定の保存
自動更新 オン

インターフェース - UNMANAGED

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定
詳細設定
デバイス設定
ファイアウォール設定

ステータス unmanage0 RX: 0 B (0 パケット)
TX: 0 B (0 パケット)

プロトコル Unmanaged ▼

■ 設定項目の説明

項目	内容
プロトコル	「Unmanaged」 から変更する場合は他のプロトコルを選択します。

■ 詳細設定 (Unmanaged)

- IPsec で使用するインターフェースで、設定項目はありません。

☰ Rooster NSX 設定の保存 自動更新 オン

インターフェース - UNMANAGED

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定 詳細設定 デバイス設定 ファイアウォール設定

デフォルトで起動する

■ 設定項目の説明

項目	内容
デフォルトで起動する	システム起動時にインターフェースを作成します。 ※バージョン 1.5.0 ではサポートしない機能です。設定を変更しないで下さい。

4-1-9 ファイアウォール設定

■ ファイアウォール設定(全プロトコル共通)

- インタフェースが使用するファイアウォール設定を選択、又は新規作成が行えます。



ファイアウォールの詳細は、「4-7 ファイアウォール」を参照ください。

☰ Rooster NSX

設定の保存

自動更新 オン

インターフェース - ETH0

このページではネットワークインターフェースの設定を行うことができます。

一般設定

一般設定 詳細設定 デバイス設定 **ファイアウォール設定**

ファイアウォールゾーンの作成 / 割り当て

- lan: eth0:
- wan: eth1: ppp0:
- 設定しない -又は- 作成: _____

① このインターフェースに設定するファイウォール・ゾーンを選択してください。設定しないを選択すると、設定済みのゾーンを削除します。また、作成フィールドにゾーン名を入力すると、新しくゾーンを作成し、このインターフェースに設定します。

■ 設定項目の説明

項目	内容
	インタフェースに設定するファイウォールのゾーン設定を選択します。
ファイアウォールゾーンの作成 / 割り当て	lan :
	LAN 側インタフェースとして使用する場合に選択します。
	wan :
	WAN 側インタフェースとして使用する場合に選択します。
	設定しない -又は- 作成 :
	設定済みのゾーンを削除する場合に選択します。
	作成に名前を入力すると、新たなゾーンを作成します。

4-1-10 DHCPサーバー

- プロトコルに「静的アドレス」を選択したインターフェースは、DHCP サーバの待ち受けインターフェースとして設定できます。



DHCP サーバの設定は「4-4DHCP 及び DNS」で行えます。

Rooster NSX

[設定の保存](#)[自動更新 オン](#)

DHCPサーバー

このインターフェース
にはDHCPサーバーが
設定されていません

[DHCPサーバーを設定](#)

ボタン項目の説明

項目	内容
DHCP サーバーを設定	DHCP サーバの待ち受けインターフェースになります。

一般設定

- このインターフェースがリースする IP アドレスの範囲、リース時間の設定が行えます。



IP アドレスの固定割り当ての設定は「4-4 DHCP 及び DNS」で行えます。

Rooster NSX

設定の保存

保存されていない変更: 3

自動更新 オン

DHCPサーバー

一般設定 詳細設定

インターフェースを無視する

このインターフェースではDHCP機能を使用しません。

開始

リースを開始するIPアドレス

終了

リースする最後のIPアドレス

リース時間 12h

リースアドレスの有効時間を入力します。最小設定値は2分です。(2m).

設定項目の説明

項目	内容
インターフェースを無視する	DHCP サーバの待ち受けインターフェースの対象外になります。
開始	リース開始 IP アドレスを設定します。
終了	リース最終 IP アドレスを設定します。
リース時間	IP アドレスのリース時間を設定します。

■ 詳細設定

- IP アドレスのリースに関するオプション設定が行えます。

☰
Rooster NSX

設定の保存
保存されていない変更: 3
自動更新 オン

DHCPサーバー

一般設定
詳細設定

ダイナミック DHCP

🔗 クライアントに対して動的にDHCPアドレスを割り振ります。無効に設定した場合、静的リースのみを行います。

IPv4-ネットマスク _____

🔗 クライアントへ通知するネットマスクを上書きします。通常は、設定されているサブネットから計算されます。

DHCPオプション _____

🔗 追加のDHCPオプションを設定します。(例: "6,192.168.2.1,192.168.2.2" と設定することで、クライアントに指定のDNSサーバーを通知します。)

■ 設定項目の説明

項目	内容
ダイナミック DHCP	一般設定で行った IP アドレスの範囲でクライアントに IP アドレスをリースします。 チェックを外すと静的リースのみ行います。 ※静的リースの設定は「4-4 DHCP 及び DNS」で行えます。
IPv4-ネットマスク	クライアントへ通知するネットマスクを設定します。 「4-1-3 プロトコル：静的アドレス」のネットマスク設定と異なるネットマスクを通知する場合に設定します。
DHCP オプション	DHCP オプションを設定します。下記のフォーマットで設定します。詳細については RFC2132 を参照してください。 コード,値

4-2 モバイル

概要

[ネットワーク] - [モバイル] ページについて説明します。

使用する SIM の通信事業者を設定できます。



PPP 接続を行うには「4-1-5 プロトコル : PPP」、「4-3 プロファイル」の設定が必要です。

【PPP の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=ppp>

4-2-1 通信事業者選択

- SIM の通信事業者を選択できます。

☰ Rooster NSX
設定の保存

モバイル

通信事業者設定

通信事業者 KDDI ▼

MVNO

設定項目の説明

項目	内容
通信事業者	SIM の通信事業者を選択します。
MVNO	「通信事業者」で KDDI、ソフトバンクを選択した場合に表示・設定できます。 MVNO SIM を使用する場合はチェックを入れます。

通信事業者設定の説明

項目	内容
NTT ドコモ	MVNO を含む NTT ドコモの SIM を使用する場合に選択します。
KDDI	KDDI の SIM を使用する場合に選択します。
ソフトバンク	ソフトバンクの SIM を使用する場合に選択します。
ローミング	ローミング用の SIM を使用する場合に選択します。

4-2-2 接続先通信事業者選択

- ローミングのSIMの場合、接続先の通信事業者を選択できます。

☰ Rooster NSX
設定の保存

モバイル

通信事業者設定

通信事業者 ローミング ▼

接続先通信事業者 自動 ▼

🔗 接続に使用する通信事業者を設定します。

ASC

🔗 自律接続維持機能です。常時接続設定のプロファイルを使用している場合に有効です。

設定項目の説明

項目	内容
接続先通信事業者	接続先の通信事業者を選択します。

接続先通信事業者設定の説明

項目	内容
自動	自動的に通信事業者を選択します。
NTT ドコモ	NTT ドコモのネットワーク（44010）に接続します。
KDDI	KDDIのネットワーク（44051）に接続します。
ソフトバンク	ソフトバンクのネットワーク（44020）に接続します。

ASC設定の説明

項目	内容
ASC	<p>自律接続維持システム（ASC）を有効にします。</p> <p>ASCはモバイル通信環境のネットワークへの接続状態を確認し、一定時間接続が行えなかった場合に通信モジュールの再起動を行うことでネットワーク接続の復旧を試みます。</p>



ASCは常時接続の設定を行っている場合に有効です。

4-3 プロファイル

概要

[ネットワーク] - [プロファイル] ページについて説明します。

PPP 接続用のプロファイルに関する設定が行えます。



PPP 接続を行うには「4-1-5 プロトコル : PPP」、「4-2 モバイル」の設定が必要です。

【PPP の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=ppp>

4-3-1 プロファイル一覧

- プロファイルの新規登録、登録済みプロファイルの修正・削除を選択できます。

ボタン項目の説明

項目	内容
編集	登録済みのプロファイルを編集します。
削除	登録済みのプロファイルを削除します。
追加	プロファイルを新規に登録します。

プロフィール一覧の表示内容

項目	内容
プロフィール名	登録済みのプロフィール名を表示します。
ユーザー名	PPP 接続時の認証に使用するユーザ名を表示します。
APN	PPP 接続先の APN を表示します。

4-3-2 プロファイル設定

- PPP 接続時の接続先、ユーザ名等の情報を設定できます。
- ご契約のインターネットサービスプロバイダ（以下 ISP）等から提供された情報をあらかじめ用意してください。

≡ Rooster NSX

設定の保存

保存されていない変更: 1

プロファイル - 名前設定なし

プロファイル名

ユーザー名

パスワード 

APN

プロトコル種別 IP

認証プロトコル 自動

接続 常時接続

LCP echo キープアラ
イブ機能を有効にする


LCP echo 失敗数しき
い値 5

 1-10

LCP echo 送信間隔 10

 1-60

無通信監視時間 0

 無通信状態が続いた場合にPPP接続を切断するまでの間隔を1~3600(秒)で指定できます。空欄の場合や0を指定した場合は無通信監視を行わずPPP接続を維持します。

SMSコールバック

 SMS受信でネットワークに接続します。

KDDI CRGを利用する

■ 設定項目の説明

項目	内容
プロファイル名	プロファイルの名前を設定します。
ユーザー名	通信事業者指定のユーザ名を設定します。指定がない場合、入力は不要です。
パスワード	通信事業者指定のパスワードを設定します。指定がない場合、入力不要です。
APN	通信事業者指定の APN を設定します。
プロトコル種別	通信事業者指定のプロトコルを選択します。指定がない場合、「IP」を選択してください。
認証プロトコル	通信事業者指定の認証プロトコルを選択します。指定がない場合、「自動」を選択してください。 自動：認証先の認証方法にあわせてます。 CHAP：認証に CHAP を使用します。 PAP：認証に PAP を使用します。
接続	PPP 接続の発信方法を選択します。 常時接続： 自動接続します。回線が切断された場合には自動で再接続処理を行います。 手動接続： 自動接続を行いません。PPP 接続の都度、発信・切断処理が必要です。 オンデマンド接続： LAN 側機器や本装置のサービスによる発信要求があった場合に接続します。
LCP echo キープアライブ機能を有効にする	LCP Echo Request による疎通確認を行います。
LCP echo 失敗数しきい値	「LCP echo キープアライブ機能を有効にする」にチェックを入れる则表示・設定できます。 切断動作をするまでの連続失敗回数を設定します。
LCP echo 送信間隔	「LCP echo キープアライブ機能を有効にする」にチェックを入れる则表示・設定できます。 LCP Echo Request の送信間隔（秒）を設定します。
無通信監視時間	指定した秒数の間、データ通信が行われない場合に回線接続を切断します。 空欄の場合や「0」を設定した場合は無通信監視を行いません。
SMS コールバック	本装置が SMS を受信すると回線接続を行います。 KDDI CRG からの SMS を受信すると回線接続を行います。
KDDI CRG を使用する	「SMS コールバック」にチェックを入れる则表示・設定できます。 KDDI のクローズド リモート ゲートウェイ (CRG) で利用する場合、設定してください。

4-4 DHCP 及び DNS

概要

[ネットワーク]- [DHCP 及び DNS] ページについて説明します。

DHCP 及び DNS 設定ページでは、DHCP サーバ及び、DNS に関する設定を行う事ができます。



DHCP サーバの待ち受けインタフェースの設定は「4-1-10DHCP サーバー」で行います。

DHCPサーバー有効/無効

- DHCP サーバ機能を停止する設定を追加できます。

Rooster NSX

設定の保存 自動更新 オン

DHCP 及び DNS

Dnsmasq は [DHCP](#)サーバーと [NAT](#)ファイアウォールの為の [DNS](#)フォワードを複合したサービスです。

DHCPサーバー 有効 / 無効

追加

ボタン項目の説明

項目	内容
追加	DHCP サーバを有効／無効の切り替え設定を行えるようになります。

追加を押下後の画面

DHCPサーバー 有効 / 無効

消去

DHCPサーバーを使う

設定項目の説明

項目	内容
DHCP サーバを使う	DHCP サーバ機能の有効／無効が設定できます。 チェックを外すと DHCP サーバ機能が停止します。

■ サーバー設定(一般設定)

- DHCP サーバ及び DNS サーバの設定ができます。

サーバー設定

一般設定	詳細設定
ドメイン必須	<input checked="" type="checkbox"/>
ⓘ DNS名の無い DNSリクエストを転送しません。	
Authoritative	<input checked="" type="checkbox"/>
ⓘ ローカルネットワーク内のみの DHCPとして使用する。	
ローカルサーバー	<input type="text"/>
ⓘ ローカルドメインを指定します。このドメインにマッチする名前は転送されず、DHCPまたは、ホストファイルのみから解決されます。	
ローカルドメイン	<input type="text"/>
ⓘ DHCP名とホストファイルエントリに追加されたローカルドメインサフィックス	
ログクエリー	<input type="checkbox"/>
ⓘ 受信したDNSリクエストをsyslogへ記録します。	
DNSフォワーディング	<input type="text" value="/example.org/10.1.2.3"/> ⓘ
ⓘ 問い合わせを転送するDNS サーバーのリストを設定します	
DNSリバインディング・プロテクション	<input type="checkbox"/>
ⓘ RFC1918の応答を破棄します。	
ローカルサービスのみ	<input checked="" type="checkbox"/>
ⓘ DNSサービスを提供しているサブネットインターフェイスにDNSサービスを制限します。	
Non-wildcard	<input type="checkbox"/>
ⓘ ワイルドカードアドレスではなく特定のインターフェイスにのみバインドします。	

■ 設定項目の説明

項目	内容
ドメイン必須	ドメインのないリクエストは上位の DNS サーバへ転送しません
Authoritative	ローカルネットワーク内のみの DHCP として使用します。
ローカルサーバー	ローカルドメインに一致した問い合わせを転送する DNS サーバを設定します。
ローカルドメイン	ローカルドメインを設定します。
ログクエリー	受信した DNS リクエストを syslog へ記録します
DNS フォワーディング	問い合わせを転送する DNS サーバを設定します。
DNS リバインディング・プロテクション	RFC1918 の応答を破棄します。
ローカルサービスのみ	同一ローカルネットワークからの問い合わせのみ応答するようになります。
Non-wildcard	※バージョン 1.5.0 ではサポートしない機能です。

■ サーバー設定(詳細設定)

- DHCP サーバ及び DNS サーバの設定ができます。

サーバー設定

一般設定	詳細設定
ロギングを抑制する	<input type="checkbox"/>
	① DHCP要求等をシステムログに記録するのを抑制します。
順にIPアドレスを割り当てる	<input type="checkbox"/>
	① 利用可能な最も小さいアドレスから順にIPアドレスを割り当てます。
プライベートフィルタ	<input checked="" type="checkbox"/>
	① ローカルネットワークへの逆引きを転送しません。
Filter useless	<input type="checkbox"/>
	① パブリックDNSサーバーが返答できなかったリクエストを転送しません。
ローカライズクエリ	<input checked="" type="checkbox"/>
	① 複数のIPが利用可能な場合は、要求しているサブネットに応じてホスト名をローカライズします。
拡張ホスト設定	<input checked="" type="checkbox"/>
	① ホストファイルから提供される名前にローカルドメインサフィックスを追加します。
ネガティブキャッシュを行わない	<input type="checkbox"/>
	① 無効なリプライをキャッシュしません。(例: 存在しないドメインからの返答など)
追加のサーバーファイル	<input type="text"/>
	① このファイルにはドメイン固有またはフルアップストリームDNSサーバーの場合、'server = / domain / 1.2.3.4'や 'server = 1.2.3.4'のような行を含めることができます。
問い合わせの制限	<input type="checkbox"/>
	① リゾルバファイルの順番に、DNSサーバーに問い合わせを行います。
偽のNXDOMAINを無視する	67.215.65.132 
	① 偽のNXDOMAIN結果を提供するホストのリスト
DNS サーバーポート	53
	① DNSクエリを受信するポート
DNS クエリポート	全て
	① DNSクエリを送信する送信元ポートを固定します。
最大 DHCP リース	無期限
	① DHCPリースの許可される最大数
最大 EDNS0 パケットサイズ	1280
	① EDNS.0 UDP パケットサイズの許可される最大数
最大 並列処理クエリ	150
	① 並列DNSクエリの許可される最大数

サーバー設定セクション【詳細設定タブ】

項目	内容
ロギングを抑制する	DHCP 要求等のシステムログ出力を一部停止します
順に IP アドレスを割り当てる	最も小さな IP アドレスから順にクライアントへ割り当てます。
プライベートフィルター	ローカルネットワークへの逆引きを転送しません。 ※バージョン 1.5.0 ではサポートしない機能です。
Filter useless	パブリック DNS サーバが返答できなかったリクエストを転送しません。 ※バージョン 1.5.0 ではサポートしない機能です。
ローカライズクエリ	※バージョン 1.5.0 ではサポートしない機能です。
拡張ホスト設定	「4-5 ホスト名」の名前にローカルドメインを追加します。
ネガティブキャッシュを行わない	無効なりプライをキャッシュしません。 ※バージョン 1.5.0 ではサポートしない機能です。
追加のサーバーファイル	DNS サーバの問い合わせ先を追加します。 ※バージョン 1.5.0 ではサポートしない機能です。
問い合わせの制限	※バージョン 1.5.0 ではサポートしない機能です。
偽の NXDOMAIN を無視する	※バージョン 1.5.0 ではサポートしない機能です。
DNS サーバーポート	DNS クエリを受信するポートを設定します。
DNS クエリポート	DNS クエリを送信する送信元ポートを固定します。
最大 DHCP リース	リースする IP アドレスの最大数を設定します。
最大 EDNS0 パケットサイズ	EDNS.0 パケットサイズの許可される最大値を設定します。
最大並列処理クエリ	DNS クエリを最大いくつまで並列に処理するか設定します。

アクティブなDHCPリース

- DHCP サーバのリース情報を表示します。

DHCPリース

ホスト名	IPv4-アドレス	MAC-アドレス	残りリース時間
PC	192.168.62.192	00:00:5e:00:53:FF	11h 43m 57s

DHCPリースの表示内容

項目	内容
ホスト名	リース先のホスト名です。
IPv4-アドレス	リースしたアドレスです。
MAC-アドレス	リース先の MAC アドレスです。
残りリース時間	リースしたアドレスが無効になるまでの残り時間です。

静的リース

- IP アドレスの固定割り当て設定を追加できます。

静的リース

静的リース機能は、DHCPクライアントに対して固定のIPアドレス及び一時的なホスト名をアサインします。また、クライアントは対応するリースを使用するホストがその1台のみで、かつ静的なインターフェース設定にする必要があります。追加 ボタンを押して、新しくエントリーを作成してください。MAC-アドレス はそのホストを識別し、IPv4-アドレス には払いだす固定のアドレスを設定します。また、ホスト名 はそのホストに対して一時的なホスト名をアサインします。

ホスト名	MAC-アドレス	IPv4-アドレス	リース時間		
	00:00:00:00:00:00	▼	192.168.62.102 ▼	12h	消去
PC	▼	▼	192.168.62.50 ▼	12h	消去

追加

設定項目の説明

項目	内容
ホスト名	IP アドレスの固定割り当てを行うホスト名を設定します。
MAC-アドレス	IP アドレスの固定割り当てを行う MAC アドレスを設定します。
IPv4-アドレス	割り当てる IP アドレスを設定します。
リース時間	IP アドレスの割り当て期間を設定します。

4-5 ホスト名

概要

[ネットワーク] - [ホスト名] ページについて説明します。

本装置上で名前解決を行うホスト名を設定できます。

Rooster NSX 設定の保存

ホスト名

ホストエントリー

ホスト名	IPアドレス
example.com	203.0.113.30 ▼

追加 消去

設定項目の説明

項目	内容
ホスト名	名前解決に使用するホストの名前を設定します。
IP アドレス	ホスト名の IP アドレスを設定します。

4-6 静的ルーティング

概要

[ネットワーク] - [静的ルーティング] ページについて説明します。

静的ルーティングページでは、静的ルーティング設定及びルートセレクタの設定を行えます。

4-6-1 IPv4静的ルーティング

- 静的ルーティングを追加できます。



インタフェースを指定するには、先に「4-1 インターフェース」を設定する必要があります。

IPv4静的ルーティング設定

☰ Rooster NSX
設定の保存

経路情報

特定のホスト又はネットワークに、どのインターフェース及びゲートウェイを通して通信を行うか、経路情報を設定します。

IPv4 静的ルーティング

インタフェース	ターゲット	IPv4-ネットマスク	IPv4-ゲートウェイ	メトリック
	ホストIP または ネットワーク	ターゲットがネットワークの場合		
eth1 ▼	0.0.0.0	0.0.0.0	192.168.64.1	0
ppp0 ▼	0.0.0.0	0.0.0.0		0

追加

IPv4静的ルーティング設定

エイ	メトリック	MTU	テーブル	タイプ	
					特別な経路設定
0		1500		Not specified ▼	消去
0		1500	2	Not specified ▼	消去

ボタン項目の説明

項目	内容
追加	ルーティング設定を追加できます。
消去	ルーティング設定を消去できます。

設定項目の説明

項目	内容
インタフェース	ルーティングで使用するインタフェースを設定します。 「4-1 インターフェース」の設定が対象となります。
ターゲット	宛先ネットワークアドレスを設定します。
IPv4 ネットマスク	ネットマスクを設定します。
IPv4 ゲートウェイ	ゲートウェイを設定します。
メトリック	メトリックを設定します。
MTU	MTU を設定します
テーブル	ルーティングテーブルを設定します。 ルーティングテーブルを指定した場合、通常のルーティングでは使用されず、ルートセレクトと併用して設定することになります。
タイプ	特別なルーティングを設定する為の項目です。 Not specified : 通常のルーティング設定です。 Unreachable : Destination Unreachable を応答するようになります。 Blackhole : パケットを破棄するようになります。

4-6-2 ルートセクタ

- ルートセクタでパケット毎に参照するルーティングテーブルを指定できます。
- 静的ルーティング設定で、ルーティングテーブルを指定した経路が追加できます。

ルートセクタ設定

ルートセクタ

priority	送信元IPとネットマスク	送信先IPとネットマスク	受信インターフェース
	0.0.0.0/24	0.0.0.0/24	0x00~0x1eで指
10	192.168.62.10	192.168.63.1	eth0 ▼

追加

ルートセクタ設定

TOS	経路テーブル
0x00~0x1eで指定してください。また、ビットの有効範囲は2~5bit目です。(000[1111]0)	
0x1e	2 消去

ボタン項目の説明

項目	内容
追加	ルートセクタ設定を追加できます。
消去	ルートセクタ設定を消去できます。

設定項目の説明

項目	内容
priority	ルートセクタの優先度設定を行えます。
送信元 IP とネットマスク	送信元の IP アドレス又はネットワークアドレスを設定します。
送信先 IP とネットマスク	送信先の IP アドレス又はネットワークアドレスを設定します。
受信インタフェース	ルートセクタの対象とする受信インタフェースを設定します。
TOS	IP ヘッダに含まれる TOS フィールドの 4~7bit を 16 進数で指定します。
経路テーブル	本設定が参照するルーティングテーブルを設定します。

4-7 ファイアウォール

概要

[ネットワーク] - [ファイアウォール] ページについて説明します。

ファイアウォールページでは IP フィルタリング、MAC フィルタリング、NAT、コネクション追跡等の設定が行えます。



【ファイアウォールの設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=filter>

【MAC アドレスによるファイアウォールの設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=mac-filter>

4-7-1 一般設定

- 一般設定画面では、デフォルトポリシー及びゾーンの設定を行うことができます。
- ゾーンの設定はゾーンに含まれるインタフェースを対象とした設定です。

Rooster NSX

設定の保存

一般設定 ポートフォワーディング トラフィック・ルール

ファイアウォール - ゾーン設定

ファイアウォール機能は、各ネットワークインターフェース上にゾーンを作成してトラフィックの制御を行います。

一般設定

SYN-Floodプロテクションを有効にする

無効なパケットを遮断する

受信 許可 ▼

送信 許可 ▼

転送 拒否 ▼

タブ項目の説明

項目	内容
ポートフォワーディング	Destination NAT の設定ページを表示します。
トラフィック・ルール	フィルタリングルールの設定ページを表示します。

■ 設定項目の説明

項目	内容
SYN-Flood プロテクションを有効にする。	SYN-Flood 攻撃を防ぎます。
無効なパケットを遮断する。	無効なパケットに対するコネクション追跡を行いません。 ※バージョン 1.5.0 ではサポートしない機能です。
受信	受信のデフォルトポリシーを設定します。 許可：パケットを受信します。 拒否：受信パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：受信パケットを破棄します。（送信元に ICMP エラーを返しません）
送信	送信のデフォルトポリシーを設定します。 許可：パケットを送信します。 拒否：送信パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：送信パケットを破棄します。（送信元に ICMP エラーを返しません）
転送	転送のデフォルトポリシーを設定します。 許可：パケットを転送します。 拒否：転送パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：転送パケットを破棄します。（送信元に ICMP エラーを返しません）

4-7-2 ゾーン設定

- ゾーン設定ではゾーンに含まれるインタフェースの送信、受信、転送のポリシー設定ができます。



1つのインタフェースが複数のゾーンに属することは出来ません。
ゾーンのパケットログ記録を有効に設定すると、スループット等のパフォーマンスに影響を及ぼします。

ゾーン

ゾーン ⇒ 転送	受信	送信	転送	マスカレード	MSSクランプ	
lan: eth0: ⇒ wan	許可 ▼	許可 ▼	許可 ▼	<input type="checkbox"/>	<input type="checkbox"/>	編集 消去
wan: eth1: ppp0: ⇒ REJECT	拒否 ▼	許可 ▼	拒否 ▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	編集 消去

[追加](#)

ゾーンの表示内容

項目	内容
ゾーン⇒転送	ゾーン間の転送設定の状態を表示します。 「受信ゾーン ⇒ 転送先ゾーン」の表示です。 ゾーン間の転送が許可されていない場合、デフォルトポリシーに従います。

ボタン項目の説明

項目	内容
追加	ゾーンを追加できます。
編集	ゾーン設定の詳細設定が行えます。
消去	ゾーン設定を消去できます。 ゾーンが削除されたインタフェースはデフォルトポリシーに従います。

設定項目の説明

項目	内容
受信	ゾーンに含まれるインタフェースの受信ポリシーを設定します。 許可：パケットを受信します。 拒否：受信パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：受信パケットを破棄します。（送信元に ICMP エラーを返しません）
送信	ゾーンに含まれるインタフェースの送信ポリシーを設定します。 許可：パケットを送信します。 拒否：送信パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：送信パケットを破棄します。（送信元に ICMP エラーを返しません）
転送	ゾーンに含まれるインタフェースの転送ポリシーを設定します。 許可：パケットを転送します。 拒否：転送パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：転送パケットを破棄します。（送信元に ICMP エラーを返しません）
マスカレード	マスカレードが有効になります。 転送パケットの送信元 IP 書き換えを行います。
MSS クランプ	MSS（Maximum Segment Size）を自動的に調整します。

ゾーンの詳細設定

- ゾーン間の転送設定や、ゾーンに含まれるインタフェースの送信、受信、転送のポリシー設定が行えます。

Rooster NSX

[設定の保存](#)
[一般設定](#) [ポートフォワーディング](#) [トラフィック・ルール](#)

ファイアウォール - ゾーン設定 - ゾーン "lan"

ゾーン "lan"

このセクションでは、lanの標準的な動作を設定します。受信及び送信オプションは、このゾーンに対して入出力するトラフィックに対する標準のポリシーを設定し、転送オプションは、ゾーン間の転送トラフィックに対する標準のポリシーになります。対象ネットワークは、どのネットワーク設定がこのゾーンに属するかを設定します。

一般設定 詳細設定

名前

受信 ▼

送信 ▼

転送 ▼

マスカレード

MSSクランプ

対象ネットワーク

作成:

内部ゾーン転送

下記の設定は、このゾーン (lan) とその他のゾーン間の転送ポリシーを制御します。宛先ゾーンへの転送は、"lan" から転送されたトラフィックに対して転送を許可します。送信元ゾーンからの転送は、別のゾーンから "lan" への転送を許可します。トラフィック転送設定は、一方であり、例えばlanからwanへの転送設定は、wanからlanへの転送を許可しません。

宛先ゾーンへの転送を許可する: wan:

送信元ゾーンからの転送を許可する: wan:

ゾーン "lan"

このセクションでは、lanの標準的な動作を設定します。受信及び送信オプションは、このゾーンに対して入出力するトラフィックに対する標準のポリシーを設定し、転送オプションは、ゾーン間の転送トラフィックに対する標準のポリシーになります。対象ネットワークは、どのネットワーク設定がこのゾーンに属するかを設定します。

一般設定 詳細設定

遮断ログを有効にする

通過ログを有効にする

ゾーンの詳細設定項目「一般設定」タブの説明

項目	内容
名前	ゾーンの名前を設定します。
受信	<p>ゾーンに含まれるインタフェースの受信ポリシーを設定します。 wan ゾーンの対象ネットワークが eth1、ppp0 の場合、受信の許可を行うと eth1、ppp0 の受信が可能になります。</p> <p>許可：パケットを受信します。 拒否：受信パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：受信パケットを破棄します。（送信元に ICMP エラーを返しません）</p>
送信	<p>ゾーンに含まれるインタフェースの送信ポリシーを設定します。 wan ゾーンの対象ネットワークが eth1、ppp0 の場合、送信の許可を行うと eth1、ppp0 の送信が可能になります。</p> <p>許可：パケットを送信します。 拒否：送信パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：送信パケットを破棄します。（送信元に ICMP エラーを返しません）</p>
転送	<p>ゾーンに含まれるインタフェースの転送ポリシーを設定します。 wan ゾーンの対象ネットワークが eth1、ppp0 の場合、転送の許可を行うと eth1 と ppp0 間の転送が可能になります。 eth0 と eth1 間の転送は、「内部ゾーン転送」設定を行う必要があります。</p> <p>許可：パケットを転送します。 拒否：転送パケットを拒否します。（送信元に ICMP エラーを返します） 遮断：転送パケットを破棄します。（送信元に ICMP エラーを返しません）</p>
マスカレード	<p>マスカレードが有効になります。 転送パケットの送信元 IP 書き換えを行います。</p>
MSS クランプ	MSS (Maximum Segment Size) を自動的に調整します。
対象ネットワーク	ゾーンに属するインタフェースを指定します。

■ ゾーンの詳細設定「詳細設定」タブの説明

- パケットログ記録の有効・無効を切り替えることができます。

■ ゾーンの詳細設定項目「詳細設定」の説明

項目	内容
遮断ログを有効にする	パケット遮断ログ記録機能が有効になります。 対象のゾーンで遮断したパケットをログに記録します。
通過ログを有効にする	パケット通過ログ記録機能が有効になります。 対象のゾーンを通過したパケットをログに記録します。

■ 内部ゾーン転送設定項目の説明

- ゾーン間の転送設定です。
- 同一ゾーンに含まれるインタフェース間の転送は、ゾーンの転送ポリシーに従います。



ゾーン間の転送設定を行っていない場合、デフォルトポリシーに従います。

項目	内容
宛先ゾーンへの転送を許可する	ゾーンが受信したパケットを、別のゾーンへ転送することを許可します。
送信元ゾーンからの転送を許可する	別のゾーンから転送されてくるパケットを許可します。

4-7-3 ポートフォワーディング設定

- Destination NAT（以下 DNAT）設定の一覧表示と設定追加、編集、削除、優先度の変更が行えます。

☰ Rooster NSX
設定の保存

一般設定 ポートフォワーディング トラフィック・ルール

ファイアウォール - ポートフォワーディング

ポートフォワーディングは、インターネット上のリモートコンピュータから、プライベートなネットワーク上の、特定のコンピュータやサービスへのアクセスを可能にします。

ポートフォワーディング

名前	Match	Forward to	有効	ソート	
test	IPv4-TCP, UDP 送信元 全てのホスト (wan) Via 全てのルーターIP	IP 192.168.63.1, port 12345 in lan	<input checked="" type="checkbox"/>	^ v	編集 消去

転送設定の新規作成:

名前	プロトコル	外部ゾーン	外部ポート	内部ゾーン	内部IPアドレス	内部ポート	
転送設定の新:	TCP+UDP	wan		lan			追加

■ タブ項目の説明

項目	内容
一般設定	デフォルトポリシー、ゾーンの設定ページを表示します。
トラフィック・ルール	フィルタリングルールの設定ページを表示します。

■ ボタン項目の説明

項目	内容
ソート	優先度の変更が行えます。ポートフォワーディング設定一覧の上から順に優先度が高くなっており、上下のアイコンで優先度を変更します。
編集	DNAT の設定を変更します。
消去	DNAT のルールを削除します。
追加	DNAT のルールを追加します。

■ 設定項目の説明

項目	内容
有効	設定を有効化します。
名前	DNAT の設定名です。
プロトコル	DNAT の対象になるプロトコルを指定します。
外部ゾーン	DNAT の対象にするパケットの受信ゾーンを指定します。 詳細設定の「送信元ゾーン」です。
外部ポート	DNAT の対象にする宛先ポート番号を指定します。
内部ゾーン	DNAT のルールでパケットの宛先 IP アドレス、ポートを書き換えた後、送信先のゾーンを指定します。
内部 IP アドレス	書き換え後の宛先 IP アドレスを指定します。
内部ポート	書き換え後の宛先ポート番号を指定します。

■ ポートフォワーディングの詳細設定

- 送信元、宛先等を指定して DNAT が行えます。

Rooster NSX

[設定の保存](#)

一般設定 [ポートフォワーディング](#) [トラフィック・ルール](#)

Rule is enabled **無効**

名前 test

プロトコル TCP+UDP

送信元ゾーン

- lan: eth0:

 wan: eth1: ppp0:

送信元MACアドレス

① 設定されたMACアドレスと一致した受信したトラフィックが対象になります。

送信元IPアドレス 全て

① 設定されたIPアドレス (または範囲) と一致した受信したトラフィックが対象になります。

送信元ポート 全て

① 設定されたクライアントホストの送信元ポート(またはポート範囲)からの受信トラフィックと一致したトラフィックのみを対象にします。

外部IPアドレス 全て

① 設定された宛先IPアドレスと一致した受信トラフィックが対象になります。

外部ポート

① 設定された宛先ポート(またはポート範囲)に一致した受信トラフィックが対象になります。

内部ゾーン

- 全てのゾーン

 lan: eth0:

 wan: eth1: ppp0:

内部IPアドレス 192.168.63.1 (00:80:F3:75:01:67)

① ルールに一致した受信トラフィックを、設定された内部ホストへ転送します。

内部ポート 12345

① ルールに一致した受信トラフィックを、内部ホストの設定されたポートへ転送します。

NATループバックを有効にする

ボタン項目の説明

項目	内容
Rule is enabled	設定の有効、無効を切り替えます。

設定項目の説明

項目	内容
名前	DNAT の設定名です。
プロトコル	DNAT の対象にするプロトコルを指定します。
送信元ゾーン	DNAT の対象にするパケットの受信ゾーンを指定します。
送信元 MAC アドレス	DNAT の対象にするパケットの送信元 MAC アドレスを指定します。 MAC アドレスを指定する場合、同時に IP アドレスの指定は行えません。
送信元 IP アドレス	DNAT の対象にするパケットの送信元 IP アドレスを指定します。
送信元ポート	DNAT の対象にするパケットの送信元ポート番号を指定します。
外部 IP アドレス	DNAT の対象にするパケットの宛先 IP アドレスを指定します。
外部ポート	DNAT の対象にする宛先ポート番号を指定します。
内部ゾーン	宛先 IP アドレス、ポートを書き換えた後の宛先ゾーンを指定します。
内部 IP アドレス	書き換え後の宛先 IP アドレスを指定します。
内部ポート	書き換え後の宛先ポート番号を指定します。
NAT ループバックを有効にする	NAT ループバックを有効にします。 LAN 側からのパケットを本装置で受信させ、LAN 側の宛先へ書き換えて転送したい場合に有効にする機能です。

4-7-4 トラフィック・ルール設定

- フィルタリング設定の一覧表示と設定追加、編集、削除、優先度の変更が行えます。



wan ゾーンから lan ゾーンへの転送ルールの場合、送信元ゾーンに wan ゾーンを設定し、宛先ゾーンに lan ゾーンを設定します。

Rooster NSX

[設定の保存](#)

一般設定 ポートフォワーディング トラフィック・ルール

ファイアウォール - トラフィック・ルール

トラフィック・ルールの設定では、ゾーン間を行き来するパケットのポリシーを設定します。例えば、特定のホスト間や、ルーターのWANポートへのトラフィックの拒否を設定することができます。

トラフィック・ルール

名前	Match	アクション	有効	ソート		
testfilter	IPv4-TCP, UDP 送信元 全てのホスト (wan) 宛先 全てのルーターIP (デバイス)	Accept input	<input checked="" type="checkbox"/>	^	v	編集 消去

ポートの開放:

名前	プロトコル	外部ポート	
受信ルールの新規作成	TCP+UDP		追加

転送ルールの新規作成:

名前	送信元ゾーン	宛先ゾーン	
転送ルールの新規作成	lan	wan	追加及び編集...

タブ項目の説明

項目	内容
一般設定	デフォルトポリシー、ゾーンの設定ページを表示します。
ポートフォワーディング	ポートフォワーディングの設定ページを表示します。

ボタン項目の説明

項目	内容
ソート	優先度の変更が行えます。 トラフィック・ルール設定は上から順に優先度が高くなります。
編集	設定を変更します。
消去	設定を削除します。
追加	受信ルールとして設定を追加します。
追加及び編集	転送ルールとして設定を追加します。

■ 設定項目の説明

項目	内容
有効	設定を有効化します。
名前	トラフィックルールの設定名です。
プロトコル	フィルタリングの対象にするプロトコルを指定します。
外部ポート	フィルタリングの対象にするポート番号を指定します。
送信元ゾーン	フィルタリングの対象にする受信時のゾーンを指定します。
宛先ゾーン	フィルタリングの対象にする宛先のゾーンを指定します。

■ トラフィック・ルールの詳細設定

- 送信元、宛先、対象のゾーン等のフィルタリングルールを設定できます。

☰ Rooster NSX

[設定の保存](#)[一般設定](#) [ポートフォワーディング](#) [トラフィック・ルール](#)

ファイアウォール - トラフィック・ルール - testfilter

Rule is enabled 無効

名前 testfilter

アドレスファミリの制限 IPv4 ▼

プロトコル TCP+UDP ▼

ICMPタイプ的一致 any ▼ 送信元ゾーン デバイス (output) 全てのゾーン lan: eth0:  wan: eth1:  ppp0: 

送信元MACアドレス 全て ▼

送信元アドレス 全て ▼

送信元ポート 全て

宛先ゾーン デバイス (input) 全てのゾーン (forward) lan: eth0:  wan: eth1:  ppp0: 

宛先アドレス 全て ▼

宛先ポート 全て

アクション 許可 ▼

ボタン項目の説明

項目	内容
Rule is enabled	設定の有効、無効を切り替えます。

設定項目の説明

項目	内容
名前	DNAT の設定名です。
プロトコル	DNAT の対象にするプロトコルを指定します。
ICMP タイプの一致	プロトコルに ICMP を指定した場合、ICMP タイプを指定できます。
送信元ゾーン	送信元ゾーンを指定します。 デバイス (output) : 送信パケットに対するフィルタリングルールになります。
送信元 MAC アドレス	DNAT の対象にする送信元 MAC アドレスを指定します。 MAC アドレスを指定する場合、同時に IP アドレスの指定は行えません。
送信元アドレス	DNAT の対象にする送信元 IP アドレスを指定します。
送信元ポート	DNAT の対象にする送信元ポート番号を指定します。
宛先ゾーン	宛先ゾーンを指定します。 デバイス (input) : 本装置宛のパケットに対するフィルタリングルールになります。
宛先アドレス	宛先 IP アドレスを指定します。
宛先ポート	宛先ポート番号を指定します。
アクション	ルールに一致した際のアクションを設定します。 許可: 受信、送信、転送を許可します。 拒否: パケットを拒否します。(送信元に ICMP エラーを返します) 遮断: パケットを破棄します。(送信元に ICMP エラーを返しません) コネクション追跡を行わない: 対象パケットのコネクション追跡を行いません。



MAC アドレスを指定する場合、同時に IP アドレスの指定はできません。

送信元ゾーンにデバイス (output) を設定すると送信ルールになります。
この場合、宛先ゾーンに「デバイス (input)」を指定できません。

宛先ゾーンにデバイス (input) を設定すると受信ルールになります。
この場合、宛先ゾーンに「デバイス (output)」を指定できません。



「コネクション追跡を行わない」を設定すると、受信許可、送信拒否のポートに対して echo request を送信したとき、送信が制限されている為、受信は出来ても echo reply に失敗します。

4-7-5 送信元NAT設定

- 送信元 NAT 設定の一覧表示と設定追加、編集、削除、優先度の変更が行えます。

送信元NAT

送信元NAT設定は、複数のWANアドレスを内部のサブネットにマッピングするような、出力トラフィックに対する送信元IPアドレスのきめ細かい制御を行うマスカレードの設定フォームです。

名前	Match	アクション	有効	ソート	
testNAT	全て ALL 送信元 全てのホスト (lan) 宛先 全てのホスト (wan)	送信元 IP 192.168.63.1 にリライト	<input checked="" type="checkbox"/>	^ v ▲ ▼	編集 消去

SNATルールの新規作成:

名前	送信元ゾーン	宛先ゾーン	変換後送信元IP	変換後送信元ポート	
SNATルール0	lan ▼	wan ▼	リライトしない ▼	リライトしない ▼	追加及び編集...

ボタン項目の説明

項目	内容
ソート	優先度の変更が行えます。送信元 NAT 設定の上から順に優先度が高くなっており、上下のアイコンで優先度を変更します。
編集	送信元 NAT 設定を変更します。
消去	送信元 NAT 設定を削除します。
追加及び編集...	送信元 NAT 設定を追加します。

設定項目の説明

項目	内容
有効	設定を有効化します。
名前	送信元 NAT ルールの設定名です。
送信元ゾーン	送信元 NAT の対象にする受信ゾーンを指定します。
宛先ゾーン	送信元 NAT の対象にする宛先ゾーンを指定します。
変換後送信元 IP	書き換え後の送信元 IP アドレスを指定します。
変換後送信元ポート	書き換え後の送信元ポートを指定します。

送信元NATの詳細設定

送信元 NAT の条件を細かく設定します。

Rooster NSX

[設定の保存](#)

一般設定 ポートフォワーディング **トラフィック・ルール**

ファイアウォール - トラフィック・ルール - SNAT testNAT

このページでは、各トラフィックルールの送信元・宛先ホストの設定などの詳細設定を行うことができます。

Rule is enabled **無効**

名前 testNAT

プロトコル All protocols ▼

① "-- 手動設定 --"を選択し、プロトコルをスペースで区切って入力することで複数のプロトコルを指定することができます。

送信元ゾーン

全てのゾーン

lan: eth0: 

wan: eth1:  ppp0: 

送信元IPアドレス 全て ▼

送信元ポート 全て

① 設定されたクライアントホストの送信元ポート(またはポート範囲)からの受信トラフィックと一致したトラフィックが対象になります。

宛先ゾーン

lan: eth0: 

wan: eth1:  ppp0: 

宛先IPアドレス 全て ▼

宛先ポート 全て

① 設定された宛先ポート(またはポート範囲)に一致した転送トラフィックが対象になります。

SNAT IPアドレス 192.168.63.1 (eth1) ▼

① ルールに一致したトラフィックの送信元アドレスを設定した値にリライトします。

SNAT ポート リライトしない

① ルールに一致したトラフィックの送信元ポートを設定した値にリライトします。空欄にした場合、IPアドレスのみを書き直します。

ボタン項目の説明

項目	内容
Rule is enabled	設定の有効、無効を切り替えます。

設定項目の説明

項目	内容
名前	送信元 NAT の設定名です。
プロトコル	送信元 NAT の対象にするプロトコルを指定します。
送信元ゾーン	送信元 NAT の対象にする受信ゾーンを指定します。
送信元 IP アドレス	送信元 NAT の対象にする送信元 IP アドレスを指定します。
送信元ポート	送信元 NAT の対象にする送信元ポート番号を指定します。
宛先ゾーン	送信元 NAT の対象にする宛先ゾーンを指定します。
宛先 IP アドレス	送信元 NAT の対象にする宛先 IP アドレスを指定します。
宛先ポート	送信元 NAT の対象にする宛先ポート番号を指定します。
SNAT IP アドレス	書き換え後の送信元 IP アドレスを指定します。
SNAT ポート	書き換え後の送信元ポートを指定します。

4-8 トリガー

概要

[ネットワーク] - [トリガー] ページについて説明します。

トリガー機能は設定されたイベント（インタフェースのリンクアップ、ダウン、ハートビートの到達、不到達等）を契機に、複数のアクション（本装置の再起動、ルート設定変更、ユーザーLEDの制御等）を行う機能です。



【トリガーの設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=trigger>

☰ Rooster NSX
設定の保存

トリガー

トリガー

トリガー名	有効	
group1	<input checked="" type="checkbox"/>	編集 消去
group2	<input type="checkbox"/>	編集 消去

新しいトリガーグループ:

名前

新しいトリガーグループ

追加

トリガーの表示内容

項目	内容
トリガー名	登録されたトリガーの設定名を表示します。
有効	トリガー設定を有効に設定します。チェックを外すと無効になります。

ボタン項目の説明

項目	内容
編集	登録済みのトリガーを編集します。
削除	登録済みのトリガーを削除します。
追加	トリガーを新規登録します。

設定項目の説明

項目	内容
新しいトリガーグループ	新規登録するトリガーの設定名を入力します。

4-8-1 リンク状態

- リンク状態が変化すると設定したアクションが実行されます。

☰ Rooster NSX
設定の保存

トリガーの詳細

トリガーの詳細

トリガーグループ名	group1
イベント	Link ▼
リンクステータス	Link Down ▼
<u>インタフェース</u>	eth1 ▼

設定項目の説明

項目	内容
トリガーグループ名	トリガーの名前を設定します。
イベント	<p>アクションを作動させる契機となるイベントの種別を選択します。</p> <p>Link : インタフェースのリンク状態の変化を契機にします。</p> <p>Heartbeat : 指定した宛先へのハートビートを送信し、その結果を契機にします。</p>
リンクステータス	<p>契機とするインタフェースのリンク状態を設定します。</p> <p>選択したインタフェースが選択した状態に変化するとアクションが動作します。</p> <p>Link Up : リンク状態がダウンからアップに変化するとアクションを実行します。</p> <p>Link Down : リンク状態がアップからダウンに変化するとアクションを実行します。</p> <p>両方（リンクアップかリンクダウン） : リンク状態が変化するとアクションを実行します。</p>
インタフェース	監視するインタフェースを選択します。

4-8-2 ハートビート

- 指定した宛先にハートビート（ping）を実行します。
- ハートビートの実行結果（成功、失敗）を契機に設定したアクションが実行されます。

Rooster NSX

[設定の保存](#)

トリガーの詳細

トリガーの詳細

トリガーグループ名	group2
イベント	Heartbeat ▼
送信先	203.0.113.10 ⑦ IPv4アドレスまたはFQDN
モード	Unreachable ▼
送信元IP	⑦ IPv4アドレス
インタフェース	ppp0 ▼
間隔	600 ⑦ パケットの送信間隔 (秒)
閾値	5 ⑦ 送信失敗回数の閾値
タイムアウト	10 ⑦ 応答待機時間 (秒)

設定項目の説明

項目	内容
トリガーグループ名	トリガーの名前を設定します。
イベント	アクションを作動させる契機となるイベントの種別を選択します。 Link : インタフェースのリンク状態の変化を契機にします。 Heartbeat : 指定した宛先へのハートビートを送信し、その結果を契機にします。
送信先	ハートビートの送信先 IP アドレスを設定します。
モード	契機とするハートビートの結果を選択します。 Reachable : ハートビートが成功するとアクションを実行します。 Unreachable : ハートビートが失敗するとアクションを実行します。
送信元 IP	ハートビートの送信元 IP アドレスを設定します。
インタフェース	ハートビートの送信で使用するインタフェースを設定します。
間隔	ハートビートの送信間隔を設定します。
閾値	ハートビートの失敗と判断する不到達の回数を設定します。 ハートビートの不到達閾値に設定した回数連続して発生すると、ハートビートの失敗と判断します。
タイムアウト	ハートビートのタイムアウト時間を設定します。 タイムアウト時間を経過してもハートビートの送信先から応答が得られないと不到達になります。

4-8-3 アクション設定

- 「4-8-1 リンク状態」、「4-8-2 ハートビート」のイベント発生時に実行するアクションを設定します。



アクションは上から順に実行されます。

アクションの詳細

アクションタイプ	詳細	ソート		
led	[led_type:off]	<input type="button" value="↑"/> <input type="button" value="↓"/>	<input type="button" value="編集"/>	<input type="button" value="消去"/>
新しいトリガーアクション:				
<input type="button" value="追加"/>				

トリガーの表示内容

項目	内容
アクションタイプ	実行するアクションの種別を表示します。
詳細	アクションの詳細を簡易的に表示します。
ソート	アクションの実行順番を変更できます。

ボタン項目の説明

項目	内容
編集	登録済みのアクションを編集します。
削除	登録済みのアクションを削除します。
追加	アクションを新規登録します。

4-8-4 アクション:再起動

- イベント発生時に本装置の再起動を実行します。

☰ Rooster NSX 設定の保存 保存されていない変更: 8

アクションの詳細

アクションの詳細

アクション	再起動	▼
再起動対象	CPU	▼

設定項目の説明

項目	内容
アクション	イベント発生時に実行するアクションを設定します。
再起動対象	本装置の再起動を行います。

4-8-5 アクション:LED

- イベント発生時に本装置に内蔵されている「USER」LEDの制御を実行します。

☰ Rooster NSX 設定の保存 保存されていない変更: 8

アクションの詳細

アクションの詳細

アクション	Led	▼
LEDタイプ	点灯	▼

設定項目の説明

項目	内容
アクション	イベント発生時に実行するアクションを設定します。
LEDタイプ	ユーザLEDを制御します。
	点灯: LEDを点灯します。
	点滅: LEDの点灯⇒消灯を繰り返します。
	消灯: LEDを消灯します。

4-8-6 アクション:トリガー

- イベント発生時に設定済みのトリガーの有効/無効を切り替えます。

☰ Rooster NSX

設定の保存
保存されていない変更: 8

アクションの詳細

アクションの詳細

アクション	トリガー	▼
対象のトリガーグループ名	test	▼
状態	有効	▼

設定項目の説明

項目	内容
アクション	イベント発生時に実行するアクションを設定します。
対象のトリガーグループ名	設定済みのトリガー名を選択します。
状態	<p>選択したトリガーの有効/無効を切り替えます。</p> <p>有効：</p> <p style="margin-left: 20px;">選択したトリガー設定の状態を有効にし、 イベント発生時にアクションが実行される状態になります。</p> <p>無効：</p> <p style="margin-left: 20px;">選択したトリガー設定の状態を無効にし、 イベント発生時にアクションが実行されない状態になります。</p> <p>ハンドオーバー：</p> <p style="margin-left: 20px;">選択したトリガー設定の状態を有効にし、 このアクションが設定されているトリガーの状態を無効にします。</p>

4-8-7 アクション:ウェイト

- 次のアクション実行までの待ち時間を設定できます。

☰ Rooster NSX 設定の保存 保存されていない変更: 8

アクションの詳細

アクションの詳細

アクション	ウェイト	▼
待ち時間		

🔔 1~600[秒]

設定項目の説明

項目	内容
アクション	イベント発生時に実行するアクションを設定します。
待ち時間	次のアクションまでの待ち時間を設定します。 指定秒数後にアクションを作動させたい際に使用します。

4-8-8 アクション: ルート

- イベント発生時にルートの追加・削除が行えます。

☰ Rooster NSX

設定の保存
保存されていない変更: 8

アクションの詳細

アクションの詳細

アクション	ルート ▼
ルートタイプ	追加 ▼
送信先IP	<small>🔗 IPv4アドレスとネットマスク 例 : 0.0.0.0/24</small>
<small>インタフェース名またはIPv4アドレス</small>	-- 選択してください -- ▼ <small>🔗 インタフェース名または接続先のゲートウェイアドレス 例 : 0.0.0.0</small>

設定項目の説明

項目	内容
アクション	イベント発生時に実行するアクションを設定します。
ルートタイプ	ルートの追加／削除を選択します。 追加 : ルートテーブルに設定を追加します。 削除 : ルートテーブルから該当する設定を削除します。
送信先 IP	ルートの宛先アドレス（ネクストホップ）、又はネットワークを設定します。 IP アドレス、ネットワークアドレスを指定できます。
インタフェース名または IPv4 アドレス	送信元のインタフェース、又はゲートウェイの IP アドレスを設定します。

4-9 IPsec

概要

[ネットワーク] - [IPsec] ページについて説明します。

IPsec 設定ページでは、IPsec 接続で使用する認証設定や暗号化方式の設定を行うことができます。



IPsec を使用するには「4-1-8 プロトコル : Unmanaged」と「4-7 ファイアウォール」の設定が必要です。

【IPsec の設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=ipsec>

IPsec設定一覧

☰ Rooster NSX
設定の保存

IPsec

IPsec 概要

名前	仮想インターフェース	相手側接続IPアドレス	自装置側接続IPアドレス	コメント
example	ipsec0	0.0.0.0	%eth1	開始 停止 編集 消去

追加

ボタン項目の説明

項目	内容
開始	IPsec 接続を開始します。
停止	IPsec 接続を切断します。
編集	追加済みの設定を編集できます。
消去	設定を消去できます。
追加	設定を追加できます。

IPsecの表示内容

項目	内容
名前	設定名を表示します。
仮想インターフェース	IPsec で使用するインターフェース名を表示します。
相手側接続 IP アドレス	IPsec トンネルの宛先を表示します。
自装置側接続 IP アドレス	IPsec トンネルの送信元を表示します。
コメント	設定で追加したコメントを表示します。

IPsec詳細設定

- IPsecの暗号化や、認証に関する設定が行えます。

☰ Rooster NSX
設定の保存

	名前	example
	<u>仮想インターフェース</u>	ipsec0 ▼
	IKEバージョン	1 ▼
	モード設定	アグレッシブモード ▼
	接続種別	イニシエータ ▼
	常時接続	<input type="checkbox"/>
	経路自動追加	<input checked="" type="checkbox"/>
	ハッシュアルゴリズム	md5 ▼
	暗号化アルゴリズム	aes256 ▼
	PFSグループ	modp1536 ▼
	PFSを有効にする	<input checked="" type="checkbox"/>
	事前共有鍵	<input type="text"/>
	IKE Life Time	3600
	IPsec Life Time	28800
	相手側接続IPアドレス	0.0.0.0
	相手側ローカルネットワーク	192.168.63.0/24
	相手側識別子	<input type="text"/>
	自装置側接続IPアドレス	%eth1
	自装置側ローカルネットワーク	192.168.62.0/24
	自装置側識別子	<input type="text"/>
	コメント	<input type="text"/>
	Dead Peer Detection	<input checked="" type="checkbox"/>
	DPD送信間隔	30
	DPDタイムアウト	120

設定項目の説明

項目	内容
名前	設定名を設定します。
仮想インタフェース	使用する仮想インタフェース名を設定します。
IKE バージョン	IKE バージョンを設定します。
モード設定	IKEv1 の場合、アグレッシブモードとメインモードを設定します。
接続種別	イニシエータ、レスポンドを設定します。
常時接続	イニシエータの場合にのみ有効です。 IPsec の設定が有効な場合に自動的に接続を開始します。
経路自動追加	IPsec 設定追加時に、相手側ローカルネットワーク宛の経路を自動的に追加します。
ハッシュアルゴリズム	ハッシュアルゴリズムを設定します。 md5、sha1、sha256、sha384、sha512 を設定できます。
暗号化アルゴリズム	暗号化アルゴリズムを設定します。 aes256、3des を設定できます。
PFS グループ	DH グループを設定します。 modp1024、modp1536、modp2048、modp3072、modp4096、modp6144、modp8192、DH22、DH23、DH24 を設定できます。
PFS を有効にする	PFS を有効にします。
事前共有鍵	Pre-Shared Key 方式で認証を行います。 認証用の共有鍵を設定します。
IKE Life Time	ISAKMP SA のライフタイム（秒）を設定します。
IPsec Life Time	IPsec SA のライフタイム（秒）を設定します。
相手側接続 IP アドレス	IPsec トンネルの宛先を設定します。
相手側ローカルネットワーク	IPsec トンネルの対象となる宛先ネットワークを指定します。
相手側識別子	接続相手の識別子を設定します。
自装置側接続 IP アドレス	IPsec トンネルの送信元を設定します。 PPP 等の動的 IP アドレスのインタフェースを指定する場合、「%ppp0」のように「%」を加えたインタフェース名を設定できます。
自装置側ローカルネットワーク	IPsec トンネルの対象となる送信元ネットワークを指定します。
自装置側識別子	本装置の識別子を設定します。
コメント	設定一覧で表示されるコメントを設定します。
Dead Peer Detection	DPD を有効にすると、ピアとの疎通を確認します。
DPD 送信間隔	DPD の送信間隔（秒）を設定します。
DPD タイムアウト	DPD 応答待ち時間（秒）を設定します。

4-10 PPTPサーバ

概要

[ネットワーク] - [PPTP サーバ] ページについて説明します。

PPTP サーバに関する設定を行うことができます。

memo

PPTP サーバを使用するには「4-1-7 プロトコル : VPN」、「4-7 ファイアウォール」の設定が必要です。

【PPTP サーバの設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=pptp>

一般設定

- PPTP サーバの認証プロトコルや、同時接続数の設定が行えます。

The screenshot shows the configuration page for a PPTP Server in the Rooster NSX interface. The page title is "PPTPサーバ" and the breadcrumb is "PPTPサーバ". There are two tabs: "一般設定" (General Settings) and "詳細設定" (Detailed Settings). The "一般設定" tab is active. The configuration includes:

- PPTPサーバを有効にする**: Checked (☑).
- 認証プロトコル**: PPTP (☐), CHAP (☐), MSCHAP-V2 (☑).
- 割り当て開始IP**: 192.168.0.20. A note below indicates it is the first IP address assigned to remote devices.
- 割り当て個数[個]**: 30. A note below indicates a maximum of 100 IP addresses can be assigned.
- 割り当てるインターフェイス**: pptp1. A note below indicates it is the interface used for PPTP sessions.

Buttons for "設定の保存" (Save Settings) and "メモ" (Memo) are visible in the top right corner.

■ 設定項目の説明

項目	内容
PPTP サーバを有効にする	PPTP サーバ機能を有効にします。
認証プロトコル	認証方式を選択します。 PAP : PAP 方式を指定します。 CHAP : CHAP 方式を指定します。 MSCHAP-V2 : MSCHAP-V2 方式を指定します。
割り当て開始 IP	クライアントに割り当てる最初の IP アドレスを設定します。
割り当て個数	PPTP で使用する、割り当て IP アドレスの個数を設定します。 ユーザーの個数分指定します。
割り当てるインタフェース	クライアントの接続に使用するインタフェースを設定します。 事前に「4-1-7 プロトコル : VPN」の設定を接続の数だけ作成してください。

■ 詳細設定

☰ Rooster NSX
設定の保存

PPTPサーバ

PPTPサーバ

一般設定
詳細設定

サーバのIP

LCP echoを有効にする

MTU

MRU

MPPE required no40 no56 stateless

■ 設定項目の説明

項目	内容
サーバの IP	PPTP サーバのアドレスを設定します。
LCP echo を有効にする	LCP echo による監視を有効にします。 本項目をチェックした場合、下記 Lcp-echo インターバル【秒】、Lcp-echo 失敗閾値【回】を設定します。
Lcp-echo インターバル【秒】	Lcp-echo を送信する間隔を秒単位で設定します。
Lcp-echo 失敗閾値【回】	Lcp-echo に連続で失敗した際に PPTP 接続を切断する閾値を設定します。
MTU	PPTP 接続時にインタフェースの MTU を設定します。
MRU	PPTP 接続時にインタフェースの MRU を設定します。
MPPE	MPPE の設定をします。 認証方式に MSCHAP-V2 を指定した場合に有効な設定です。

認証設定

- PPTP クライアントのユーザ設定が行えます。



接続の数だけクライアントの設定を行ってください。

認証

ユーザ名または、パスワードがない認証情報は無視されます。

ユーザー名	パスワード	固定IPアドレス割り当て
user	*****	クライアント個別にIPアドレスを割り当てることができます。
		<input type="checkbox"/>
<input type="button" value="追加"/>		<input type="button" value="消去"/>

設定項目の説明

項目	内容
ユーザー名	認証時に使用するユーザー名を設定します。
パスワード	認証時に使用するパスワードを設定します。
固定 IP アドレス割り当て	特定のクライアントに割り当てる固定の IP アドレスを設定します。

4-11 L2TP/IPsecサーバ

概要

[ネットワーク] - [L2TP/IPsec サーバ] ページについて説明します。

L2TP/IPsec サーバ設定ページでは、L2TP/IPsec サーバに関する設定を行うことができます。



L2TP / IPsec サーバを使用するには「4-1-7 プロトコル : VPN」、「4-7 ファイアウォール」の設定が必要です。

【L2TP / IPsec サーバの設定方法】

<https://www2.sun-denshi.co.jp/config-example/?cat=47&tag=l2tp-ipsec>



「4-9IPsec」との同時使用はサポート対象外です。

お使いの端末によって本装置と接続できないことがあります。

■ 一般設定

- L2TP/IPsec で使用する IP アドレスの設定や、暗号化、認証に関する設定が行えます。

☰ Rooster NSX

設定の保存

L2TP/IPsecサーバ

L2TP/IPsecサーバ

一般設定 詳細設定

L2TP/IPsec serverを
有効にする

自装置アドレス 203.0.113.1

① IPsecトンネルを張る際に使用する自身のデバイスのアドレス

ハッシュアルゴリズム sha1 ▼

暗号化アルゴリズム aes256 ▼

PFSグループ modp2048 ▼

IPsec 事前共有鍵 secret

認証プロトコル PAP CHAP MSCHAP-V2

割り当て開始IP 192.168.1.20

① リモートデバイスに割り当てる最初のIPアドレス

割り当て個数[個] 30

① 次の数まで割り当てることができます。100 IP

割り当てるインター
フェイス l2tp1 ▼ 

① L2TP/IPsecセッションに使用するインターフェイス

■ 設定項目の説明

項目	内容
L2TP/IPsec server を有効にする	L2TP / IPsec サーバ機能を有効にします。
自装置アドレス	接続を待ち受ける自装置のアドレスを設定します。 IP アドレスまたは、インタフェース名を指定できます。
ハッシュアルゴリズム	ハッシュアルゴリズムを設定します。 md5、sha1、sha256、sha384、sha512 を設定できます。
暗号化アルゴリズム	暗号化アルゴリズムを設定します。 aes256、3des を設定できます。
PFS グループ	DH グループを設定します。 modp1024、modp1536、modp2048、modp3072、modp4096、modp6144、 modp8192、DH22、DH23、DH24 を設定できます。
IPsec 事前共有鍵	Pre-Shared Key 方式で認証を行います。 認証用の共有鍵を設定します。
認証プロトコル	認証方式を選択します。 PAP : PAP 方式を指定します。 CHAP : CHAP 方式を指定します。 MSCHAP-V2 : MSCHAP-V2 方式を指定します。
割り当て開始 IP	クライアントに割り当てる最初の IP アドレスを設定します。
割り当て個数	L2TP / IPsec で使用する、割り当て IP アドレスの個数を設定します。 ユーザーの個数分設定します。
割り当てるインタフェース	クライアントの接続に使用するインタフェースを設定します。 事前に「4-1-7 プロトコル : VPN」の設定を接続の数だけ作成してください。

■ 詳細設定

☰ Rooster NSX 設定の保存

L2TP/IPsecサーバ

L2TP/IPsecサーバ

一般設定	詳細設定
サーバIP	192.168.1.1
MTU	
MRU	

■ 設定項目の説明

項目	内容
サーバの IP	L2TP / IPsec サーバのアドレスを設定します。
MTU	接続時にインターフェースの MTU を設定します。
MRU	接続時にインターフェースの MRU を設定します。

認証設定

- L2TP / IPsec クライアントのユーザ設定が行えます。



接続の数だけクライアントの設定を行ってください。

認証

ユーザ名または、パスワードがない認証情報は無視されます。

ユーザー名	パスワード	固定IPアドレス割り当て
user	*****	クライアント個別にIPアドレスを割り当てることができます。
		<input type="checkbox"/>

設定項目の説明

項目	内容
ユーザー名	認証時に使用するユーザー名を設定します。
パスワード	認証時に使用するパスワードを設定します。
固定 IP アドレス割り当て	特定のクライアントに割り当てる IP アドレスを設定します。

4-12 診断機能

概要

[ネットワーク] - [診断機能] ページについて説明します。

診断機能では構築したネットワーク環境の確認を Web 設定ツール上で行うことができます。

ping コマンドによる到達性の確認、tracertoute コマンドによるネットワークの経路確認、nslookup コマンドによる DNS サーバへの問い合わせ確認が行えます。

Rooster NSX 設定の保存

診断機能

ネットワーク・ユーティリティ

PING

TRACEROUTE

NSLOOKUP

ボタン項目の説明

項目	内容
PING	設定された宛先へ ping コマンドを実行し、結果を表示します。
TRACEROUTE	設定された宛先へ tracertoute コマンドを実行し、結果を表示します。
NSLOOKUP	DNS サーバへ問い合わせを行い、結果を表示します。

設定項目の説明

項目	内容
PING	ping の送信先を設定します。
TRACEROUTE	tracertoute の送信先を設定します。
NSLOOKUP	DNS サーバへの問い合わせるホスト名を設定します。

サポートのご案内

■ ご質問・お問い合わせ

NSX に関するご質問やお問い合わせは、弊社サポートセンターへご連絡願います。

サポートセンター

- 電話 0587-53-7606
- FAX 0587-55-0815
- メール support-suncomm@sun-denshi.co.jp
- 受付時間 月曜～金曜 10:00～16:00（12:00～13:00 を除く）
祝祭日、弊社休日を除く

Rooster NSX 機能説明書 Ver.1.5.0R2

サン電子株式会社

2021 年 1 月発行

(210107)