

USB Deviceserver & USB Dongleserver

myUTN ユーザーマニュアル macOS

USB Deviceserver: myUTN-50a、myUTN-55、myUTN-2500

USB Dongleserver: myUTN-80、myUTN-800

メーカと窓口

SEH Computertechnik GmbH Suedring 11 33647 Bielefeld Germany (ドイツ) 電話:+49 (0)521 94226-29 FAX:+49 (0)521 94226-99 サポート:+49 (0)521 94226-44 電子メール:info@seh.de ホームページ:http://www.seh-technology.jp



文書

種類:ユーザーマニュアル myUTN ユーザーマニュアル macOS バージョン:4.1 | 2021-07

法律情報

SEH Computertechnik GmbH はあらゆるマニュアルの記載事項が正確であるよう努めておりますが、万 一誤りを見つけられた場合には、上記の住所にご連絡ください。SEH Computertechnik GmbH は、誤り または脱落についていかなる責任も負いません。本マニュアルの記載事項は予告なく変更されることが あります。

マニュアル原文はドイツ語バージョンです。他の言語のバージョンに優先して効力を持つものとしま す。この文書のドイツ語以外の言語バージョンはすべて、原文からの翻訳です。

無断複写、転載を禁じます。SEH Computertechnik GmbH による事前承諾なしの複写や他の複製行為、 翻訳を禁じます。

© 2021 SEH Computertechnik GmbH

この文書に記載されている商標、登録商標および製品名は、それぞれの会社(所有者)に帰属します。

目次

1	一般情報	1
1.1	製品	1
1.2		
1.3	サポートとサービス	4
1.4	安全の確保	4
1.5	最初のステップ	5
C		C
2	官理力法	0
2.1	myUTN Control Center による管理	6
2.2	SEH UIN Manager による管理	8
2.3	電子メールによる管理	11
3	ネットワーク設定	13
3.1	IPv4 パラメータの設定方法	13
3.2	IPv6 パラメータの設定方法	15
3.3	WLAN を設定する方法	16
3.4	DNS を設定する方法	17
3.5	SNMP の設定方法	18
3.6	Bonjour の設定方法	19
3.7	電子メール (POP3 と SMTP) を設定する方法	19
3.8	VLAN 環境での UTN サーバの利用方法 (myUTN-80 以降のみ)	
4	デバイス設定	24
4 4.1	デバイス設定 デバイス時間の設定方法	 24
4 4.1 4.2	デバイス設定 デバイス時間の設定方法 説明の記述内容を設定する方法	 24 24 24
4 4.1 4.2 4.3	デバイス設定 デバイス時間の設定方法	 24 24 24 25
4 4.1 4.2 4.3 4.4	デバイス設定 デバイス時間の設定方法 説明の記述内容を設定する方法 USB ポートに名前を割り当てる方法 USB ポートを無効にする方法 (myUTN-80 以降のみ)	24
4 4.1 4.2 4.3 4.4 4.5	デバイス時間の設定方法	24 24 24 25 25 26
4 4.1 4.2 4.3 4.4 4.5 4.6	 デバイス設定 デバイス時間の設定方法 説明の記述内容を設定する方法 USB ポートに名前を割り当てる方法 USB ポートを無効にする方法 (myUTN-80 以降のみ) UTN (SSL) ポートの設定方法 メッセージを取得する方法 (myUTN-80 以降のみ) 	24 24 25 25 26 26
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7	 デバイス時間の設定方法	24 24 24 25 25 26 26 27
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8	デバイス時間の設定方法	24 24 25 25 26 26 26 27 28
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5	 デバイス時間の設定方法	24 24 25 25 26 26 26 27 28 30
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1	 デバイス時間の設定方法	24 24 24 25 25 26 26 26 27 28 30
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2	 デバイス設定 デバイス時間の設定方法	24 24 25 25 26 26 26 27 28 26 27 28 30 30 32
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3	 デバイス設定 デバイス時間の設定方法	24 24 24 25 25 26 26 26 27 28 30 30 32 33
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4	 デバイス設定 デバイス時間の設定方法	24 24 25 25 26 26 26 27 28 26 27 28 30 30 32 33 34
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5	 デバイス設定 デバイス時間の設定方法	24 24 25 25 26 26 26 26 27 28 26 27 28 26 27 28 30 30 30 32 30 34 34
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5 5.6	 デバイス設定 デバイス時間の設定方法	24 24 25 25 26 26 26 27 28 26 27 28 30 30 32 33 34 34 34 37
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5 5.6 5.7	 デバイス設定 デバイス時間の設定方法	24 24 25 25 26 26 26 26 27 28 26 27 28 26 27 28 30 30 30 31 32 33 34 34 37 37
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 5 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8	 デバイス設定 デバイス時間の設定方法	24 24 25 25 26 26 26 27 28 26 27 28 26 27 28 30 30 32 33 30 32 33 34 37 37 37

6.1	USB 接続を暗号化する方法	
6.2	myUTN Control Center への接続を暗号化する方法	
6.3	SSL/TLS 接続の暗号化強度を設定する方法	
6.4	myUTN Control Center へのアクセスを保護する方法 (ユーザアカウント)	
6.5	・ UTN サーバのポートをブロックする方法 (TCP ポートアクセス制御)	
6.6	USB デバイスへのアクセスを制御する方法 (myUTN-80 以降のみ)	
6.7	USB デバイスの種類をブロックする方法	
6.8	証明書の使用方法	
6.9	ネットワーク認証を設定する方法 (IEEE 802.1X)」	
7 ;	メンテナンス	
7.1	UTN サーバを再起動する方法	
7.2	更新の手順	
7.3	設定をバックアップする方法	
7.4	パラメータを初期値にリセットする方法	60
8 *	靖 足	
81	田語集	62
8.7	トラブルシューティング	
83	パラメータリスト	
8.J	SEH LITNI Manager - 機能の概要	07 01
UT	JEITOTH Multuget 1次HCッパ外女	····· ノー

1 一般情報

- 製品 ⇨ 🖹 1
- 説明書 ⇨ 🗎 3
- ・ サポートとサービス ⇔ 🗎 4
- 安全の確保 ⇔ 🖽 4
- ・ 最初のステップ ⇔ 🖹5

1.1 製品

目的

UTN サーバは、USB Deviceserver と USB Dongleserver から構成されます。TCP/IP ネットワークを介し、USB Deviceserver の場合はネットワーク非対応の USB デバイス (USB ハードディスクドライブ、USB プリンタ、など)が利用でき、USB Dongleserver の場合はネットワーク非対応の USB ドングルが利用できます。使用する USB デバイスや USB ドングルを UTN サーバの USB ポートに接続すると、UTN (UTN = USB to Network)機能に対応するソフトウェアツールの「SEH UTN Manager」により、USB デバイスや USB ドングルとクライアント間に仮想の USB 接続が確立されます。接続された USB デバイスや USB ドングルは、ローカル接続とまったく同じ状態で使用できます。

システム要件

UTN サーバは、TCP/IP ネットワークで使用するよう設計されています。 SEH UTN Manager は、次のシステムで実行できます。

- Microsoft Windows (32/64-Bit; Windows 10 以降, Server 2012 R2)
- macOS 10.9⁻¹
- Linux (Debian 10, Ubuntu 20.0.4, Red Hat Enterprise Linux 8, Oracle 8, CentOS 8, SUSE Linux Enterprise 15.1, openSUSE Leap 15.1)²
- IPv4 TCP/IP ネットワーク

^{1.} macOS 11.x (Big Sur)では、USBデバイスのサポートが制限されており、Apple Silicon (Apple M1チップ)ベースのMacでは動作しません。

^{2.} Linuxシステムは多種多様であるため、インストールの成功は保証できません。インストールはお客様ご 自身の責任で行ってください。

重要:

アイソクロナス USB デバイス (カメラ、マイク、スピーカなど)への対応は 次の環境に依存します。

- オペレーティングシステム:
 - Windows
 - Linux
- UTN サーバモデル (各製品情報を参照してください。)
- ・ ソフトウェアバージョン
 - UTN サーバのファームウェア / ソフトウェア:14.5.5 以降
 - SEH UTN Manager: 3.1.4 以降

このマニュアルは macOS 環境での使用について説明します。他の環境での使用については、該当する システム用のユーザーマニュアルを参照してください。詳細は、「説明書」⇔ ■3 の章を参照してください。

関連製品との組合せ

UTN サーバを他の SEH Computertechnik GmbH 製品と組み合わせることで、デバイスを環境に合わせて 理想的に使用することができます。

<u>Service</u>^{plus}

myUTN-80 および myUTN-800 Dongleserver のサービス契約には、Service^{plus} パッケージが利用できま す。Service^{plus} パッケージでは、Dongleserver のメーカ保証を 36 ヶ月から 60 ヶ月に延長します。また、 製品に不具合がある場合は、先出しの代替品をすぐに受け取ることができます。Service^{plus} パッケージ は別途購入が必要です。 詳細情報:

http://www.seh-technology.jp/services/service-packages.html



<u>ラックマウントキット</u>

Dongleserver を完全かつ安全に保管するためには、Rack Mount Kit (RMK)を推奨します。このインストールキットにより、Dongleserver を 19 インチのサーバラックに取り付けることができます。 詳細情報:

http://www.seh-technology.jp/products/rack-mount-kits.html



1.2 説明書



最新の説明書は、当社の次のウェブサイトからダウンロードしてください:<u>http://www.seh-technology.jp</u>

-般情報

該当する説明書

UTN の説明書は、次のように構成されています。

クイック・インストール案内	印刷、PDF	安全に関する情報、技術データ、ハードウェア設置に 関する説明、適合宣言
ユーザーマニュアル	PDF	UTN の設定および管理についての詳細な説明。次のシ ステムに関して、システム固有の説明をしています。 ・Windows ・macOS ・Linux
オンラインヘルプ	HTML	ウェブインターフェイス「myUTN Control Center」の 使用方法についての情報。 (オンラインヘルプは、ウェブインターフェイスのメニューの一部 でダウンロードは必要ありません。)
製品情報	印刷、PDF	機能および技術データ
パンフレット	印刷、PDF	
Open Source 使用許諾	オンライン	http://www.seh-technology.jp/services/licenses.html

記号および凡例

本書では、様々な記号と表記が使用されています。

警告 警告には、細心の注意が必要な重要な情報が含まれます。警告に従 わない場合、誤動作することがあります。 警告 このメモには、正常動作に関する重要な情報が含まれます。 重要: 重要な情報 ✓ 必要事項 操作を始める前に準備が必要な要件を示します。 ・ 箇条書き(ブレット) リスト 1. 箇条書き(番号) 手順の説明 ᅛ 結果 実行した操作の結果 ヒント 推奨事項および役立つアドバイス ⇒₿ 参照(説明書内でハイパーリンクが使用できます。) 太字 ボタン名、メニュー項目、選択項目などの画面の用語 Courier (コマンドライン、スクリプトなどのコード、パス名。 固有名は、「」内に示します。 「固有名」

1.3 サポートとサービス

SEH Computertechnik GmbH では広範囲なサポートを提供しています。ご質問がある場合は、当社の窓 口までご連絡ください。



 月曜~木曜
 午前

 金曜
 午前

午前8:00~午後4:45 午前8:00~午後3:15



+49 (0)521 94226-44



support@seh-technology.jp

製品に関する情報は、すべて当社の次のウェブサイトからダウンロードできます:



http://www.seh-technology.jp



1.4 安全の確保

本書やパッケージ、デバイス本体に記載された安全規定および警告は、すべて読み遵守してください。 誤った使用方法を避けることで、人体への悪影響や製品の故障を防ぐことができます。

目的用途

UTN サーバは、TCP/IP ネットワーク上で使用します。また、オフィス環境での使用を意図して設計されています。ネットワークユーザは、このサーバによりネットワーク非対応の USB デバイスを利用することができます。

不正使用

myUTN の説明書に記載されている機能に適合しないデバイスの使用は、すべて不正使用とみなされます。

安全規定

UTN サーバを初めてセットアップする前に、「クイック・インストール案内」の安全規定を読み遵守してください。この説明書は、印刷物としてパッケージに同梱されています。

警告

本書に記載されたすべての警告を読み遵守してください。警告は、危険と判断される操作説明の箇所に、次のように表記されています。



責務および保証

安全規定と警告を遵守しなかった結果による、人への傷害や財産の損失および間接的損害について、 SEH Computertechnik GmbH は一切の責任を負いません。遵守しなかった場合はまた、保証に関する申 し立ては無効となります。

デバイスの改造と修理

ハードウェアおよびソフトウェアの改造やデバイスの修理は許可されていません。デバイスの修理が必要な場合は、当社サポートまでご連絡ください。⇔ ■4

1.5 最初のステップ

- 1. 人への傷害およびデバイスへの損傷を避けるため、セキュリティ規定を読み遵守ください。⇔ ■4
- 2. ハードウェアを設置します。ハードウェアの設置には、UTN サーバのネットワークと USB デバイス、 電源への接続が含まれます。 ⇔ □ 「クイック・インストール案内」
- 3. ソフトウェアをインストールします。ソフトウェアのインストールには、必要な「SEH UTN Manager」ソフトウェアツールをクライアントにインストールし、IP アドレスを割り当てる作業が 含まれます。⇔ □ 「クイック・インストール案内」
- 4. 最適な形でネットワークに組み込み、十分に保護されるように UTN サーバを設定してください。設定方法はすべて、この説明書に説明されています。
- 5. SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用 します。⇔
 [●]30



2 管理方法

UTN サーバは、いくつかの方法で管理、設定および保守することができます。

- ・ myUTN Control Center による管理 ⇒ 🗈 6
- SEH UTN Manager による管理 ⇔ 🗎 8
- ・ 電子メールによる管理 ⇔ 🖹 11

2.1 myUTN Control Center による管理

UTN サーバには、ユーザインターフェイスである myUTN Control Center が装備され、インターネット ブラウザ (Safari、) で起動できます。

UTN サーバは、myUTN Control Center から設定、監視および保守することができます。

- ・ myUTN Control Center をブラウザで起動する ⇔ 🗈 6
- myUTNSEH UTN Manager から Control Center を起動する ⇔ 🗈 6
- 制御機器 ⇨ 🖹 7

myUTN Control Center をブラウザで起動する

- ✓ UTN サーバがネットワークと電源に接続されていること。
- ✓ UTN サーバに有効な IP アドレスが設定されていること。⇔
 ¹³
- 1. ブラウザを開きます。
- 2. UTN サーバの IP アドレスを URL に入力します。
- → myUTN Control Center がブラウザに表示されます。



重要:

myUTN Control Center が表示されない場合は、ゲートウェイが設定されていることを確認し (⇔ 🖹 13)、ブラウザのプロキシ設定も確認してください。

myUTNSEH UTN Manager から Control Center を起動する

- ✓ UTN サーバがネットワークと電源に接続されていること。
- ✓ UTN サーバに有効な IP アドレスが設定されていること。⇔ 🖹 13
- 1. SEH UTN Manager を起動します。
- 2. 選択リストから UTN サーバを選択します。
- 3. メニューバーから、UTN サーバ 構成を選択します。
- → ブラウザが起動して、myUTN Control Center が表示されます。

制御機器

	1	10.168.1.88/network/ipv4_jp.html Č	4 ① 5 P 6 製品と会社情報 I サイトマップ I
MYUTN	Control C	enter	SEH
ホーム	ネットワーク デバイス	セキュリティ メンテナンス	
TOW	myUTN-80 — ネットワーク —	IPv4	_
10002478	3 IPv4 の状態		
IPv4	IPアドレス	10.168.1.88	
IPv4 VLAN IPv6	サブネットマスク	255.255.254.0	
DNS	ゲートウェイ	10.168.0.228	
SNMP 電子メール	設定方法	dhcp	7
Bonjour	IPv4 の構成		2
	自助		
	DHC	●オン○オフ	
	BOOTI	● ●オン ○オフ ● ●オン ○オフ	
	IPアドレス	10.168.1.88	
	サブネットマスク	255.255.254.0	
	ゲートウェイ	10.168.0.228	
		保存して再起動する リセット	
			Copyright © 2017 SEH Computertechnik GmbH.

⊠ 1: myUTN Control Center

1	メニュー項目	メニュー項目を選択(マウスをクリック)すると、使用可能なサブ メニューが左側に表示されます。
2	サブメニュー項目	サブメニューの項目を選択すると、対応するページとその内容が表 示されます。
3	ページ	メニューの内容
4	製品と会社情報	メーカの連絡先および製品の詳細情報
5	サイトマップ	myUTN Control Center の全体図が表示され、myUTN Control Center のすべてのページに直接アクセスできます。
б	フラグ	言語の選択
7	?アイコン	オンラインヘルプ

2.2 SEH UTN Manager による管理

「SEH UTN Manager」は、SEH Computertechnik GmbH が開発したソフトウェアツールです。SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用されます。

- 機能 ⇨ 🖹 8
- ・ バージョン ⇔ 🗎 9
- ・インストール ⇒ 10
- ⇒ ≞10

機能

このソフトウェアは、ネットワーク内の USB デバイスを使用するクライアントすべてにインストールします。SEH UTN Manager を起動すると、ネットワークをスキャンして、接続された UTN サーバを検出します。検出されたすべての UTN サーバとそのサーバに接続された USB デバイスが選択リストに表示されます。UTN サーバに接続された USB デバイスを使用するには、UTN サーバを「選択リスト」に追加します。選択リストに表示されたデバイスを管理して、接続された USB デバイスを使用することができます。SEH UTN Manager の操作については、「SEH UTN Manager の操作」⇔ ■30 の章で詳しく説明します。

警告 UTN (⇔ 🗈1) と対応する SEH UTN Manager は IPv4 ネットワークでのみ機能し ます
 ょ 9 。 IPv6 単独のネットワークでは myUTN Control Center (⇔ ≧6) のみが UTN サー バの管理に利用できます。

00	😢 A	dministrator: SEH UTN	l Manager		
UTNA	lanager				CEL
	anager				JLII
3	2			5	
選択リスト	UTN サーバ/デバイス	▲ ステータス	プロパティ		
	192.168.0.140		ポート名	USB フラッシュ ドライブ	
更新	USB フラッシュ ドライブ (ポート 1	l) 使用可能	ボート番号	1	
400.40r			ボートのステータス	使用可能	
編果			追加機能	-1	
	-		<u> </u>	オフ	
			日馴深作	+ 7	
有効化			日期佐航 接続されたデバイフ	12	P
			支航されたアバイス	Flash Drive	
無効化			マテータス	体田可能	
			製造メーカー	Alcor Micro Corp. (0x058f)	
Λ			製品	Flash Drive (0x6387)	
<u> </u>					

図 2: SEH UTN Manager

- 1 メニューバー
 - 利用できるメニュー項目
- 2 選択リスト 選択された UTN サーバと接続された USB デバイスを表示します。
- 3 選択リスト編集用ボタン ネットワーク上で UTN サーバを検索し、任意のデバイスを選択す るためのダイアログを起動します。⇔ 🗟 30
- 4 ポート接続管理用ボタン USB ポート (⇔
 ³2) に接続された USB デバイスへの接続を確立、または接続 (⇔
 ³3) を中断します。
- 5 プロパティ表示領域 選択された UTN サーバ、または USB デバイスの情報を表示しま す。⇔
 37

SEH UTN Manager の使用方法の詳細は、⇔ □□「SEH UTN Manager オンラインヘルプ」を参照してくださ い。オンラインヘルプを起動するには、SEH UTN Manager のメニューバーから、ヘルプ – オンラインヘ ルプ を選択します。

重要: SEH UTN Manager の一部の機能は表示されない、または非アクティブとし て表示される場合があります。それは、次の要因に依存します。 ・ 選択リストの種類と場所 クライアント側のユーザ権限およびグループのメンバシップ • クライアントのオペレーティングシステム ・ 製品に固有なセキュリティメカニズムの設定 ・ UTN サーバおよび各 USB ポートの状態 詳細は、「SEH UTN Manager – 機能の概要」 ⇒ 🖻 91 の章を参照してください。

バージョン

SEH UTN Manager には 2 つのバージョンがあります。

- ・ フルバージョン: グラフィカルユーザインターフェイス (⇔ 図 2 ≧8) と詳細な機能を備えた SEH UTN Manager です。
- ・ ミニマルバージョン(グラフィカルユーザインターフェイスなし) コマンドライン(「utnm」⇔ ■40)および 自動化プログラム(「UTN Actions」⇔ ■34)のみを使用します。

両方のバージョンとも、「SEH UTN Service」がバックグラウンドで動作しシステム起動後に自動的にア クティブになります。

さらに、次のユーザグループが区別されます。

- ・ 管理者権限のあるユーザ(管理者)
- ・管理者権限のないユーザ(標準ユーザ)

重要

機能によっては管理者だけが設定できます。詳細は、「SEH UTN Manager – 機能の概要」 ⇔ 🖻 91 の章を参照してください。 インストール

SEH UTN Manager を使用するには、プログラムを macOS オペレーティングシステムのコンピュータに インストールする必要があります。SEH UTN Manager のインストールファイルは、SEH Computertechnik GmbH の次のウェブサイトにあります:

http://www.seh-technology.jp/services/downloads.html



以上以上以上以上インストールファイルは macOS システム用の「*.pkg」ファイルとして入手できます。 インストールファイルには SEH UTN Manager の両方のバージョンが含まれています。

- ✓ macOS 10.9 以上
- ✓ インストールには管理者権限が必要です。
- ✓ 管理者パスワードを知っている必要があります。
- 1. SEH UTN Manager のインストールファイルを起動します。
- 2. インストールルーチンに従います。
- → SEH UTN Manager がクライアントにインストールされます。

プログラムの起動

SEH UTN Manager をアイコンで識別します: 🌺 プログラムは、使用するオペレーティングシステムの 通常方法で起動します。

更新

プログラムの更新を手動または自動で確認できます。詳細は ⇔ 🚇「SEH UTN Manager オンラインヘル プ」で確認してください。

2.3 電子メールによる管理

UTN サーバを電子メールにより管理することで、インターネットを使用 (リモートアクセス) できる任意のコンピュータから管理することができます。

管理方法

- ・ UTN サーバステータスの取得
- ・ UTN サーバパラメータの取得
- UTN サーバの更新

そのためには、コマンドを電子メールのヘッダに書き込みます。⇔ 表1 🗈 11

表1: コマンドとコメント:

コマンド	オプション	説明
<コマンド>	get status	UTN サーバステータスページを取得します。
	get parameters	UTN サーバパラメータリストを取得します。
	set parameters	UTN サーバに採用される少なくとも1つのパラメータをUTN サーバに送信します。
		パラメータとその値を電子メールの本文に書き込みます。 < パラメータ > = < 値 >
		構文と値はパラメータリストから検出できます。⇔ №67
	update utn	メールに添付したソフトウェアにより、自動更新を実行しま す。
	help	リモートメンテナンス情報のページを取得します。
[< コメント >]		説明用の任章のテキスト文。

命令の表記規約は次のとおりです。

- ・ 大文字、小文字を区別しない
- 複数の空白文字を許可
- ・最大長:128バイト
- ASCIIフォーマットのみ読み込み可能

また、更新を実行またはパラメータを変更するために TAN を実行する必要があります。開始するには、 TAN を含むステータスページ (⇔表1 🖹 11) を電子メールで取得する必要があります。受信した TAN を電 子メールの本文に入力します。その後に、空白文字を1字入れます。

- ✓ DNS サーバが UTN サーバ ⇔
 ■17 上で設定されていること。
- ✓ 電子メールが受信できるように、UTN サーバに POP3 サーバ上の電子メールアドレスが設定されていること。
- ✓ POP3 と SMTP のパラメータが UTN サーバ上で設定されていること。⇔ ■19
- 1. 電子メールのプログラムを起動します。
- 2. 新しい電子メールを作成します。
 - 受信者として UTN アドレスを入力します。
 - 件名に命令を入力します。cmd: < コマンド > [< コメント >] コマンドとコメント: ⇒ 表 1 11.
 - TANの適用が可能な場合は、それを電子メールの本文に入力します。
- 3. 電子メールを送信します。
- → UTN サーバがその電子メールを受信し、命令を実行します。

例

UTN サーバパラメータリストを取得する場合

- 宛先:UTNserver@company.com
- 件名:cmd: get parameters
- 「設定」パラメータリストを設定する場合
- 宛先:UTNserver@company.com
- 件名:cmd: set parameters
- メール本文: TAN = nUn47ir79Ajs7QKE sys descr = <Your description>

3 ネットワーク設定

UTN サーバをネットワークに最適な形で組み込むには、次のように設定してください。

- IPv4 パラメータの設定方法 ⇔ 🖹 13
- ・ IPv6 パラメータの設定方法 ⇔ 🖹 15
- WLAN を設定する方法 ⇒

 ¹⁶
- DNS を設定する方法 ⇔ 🖹 17
- SNMP の設定方法 ⇔ 🗎 18
- Bonjour の設定方法 ⇔ 🗎 19
- ・ 電子メール (POP3 と SMTP) を設定する方法 ⇔
 ¹⁹
- ・ VLAN 環境での UTN サーバの利用方法 (myUTN-80 以降のみ) ⇔
 ^{●22}

3.1 IPv4 パラメータの設定方法

ハードウェアのインストールで (ð & 「ハードウェアインストールガイド」)、UTN サーバはネットワークに接続されます。UTN サーバは、次に IP アドレスが BOOTP (Bootstrap Protocol) または DHCP (Dynamic Host Configuration Placed) ブートプロトコルにより動的に取得されているかを確認します。いずれの方法でも取得できない場合、INU サーバは Zeroconf により、Zeroconf に予約されたアドレス範囲 (169.254.0.0/16) から自らに IP アドレスを割り当てます。

重要: UTN サーバは、IPv6 ネットワークに接続している場合、IPv6 アドレスを追 加で受信します。⇔ 🗎15

UTN サーバに割り当てられた IPv4 アドレスは「SEH UTN Manager」ソフトウェアツールにより検出する ことができます。この手順は通常、初期セットアップ時に実行します (ð&「クイック・インストール案 内」)。



例えば Safari の Bonjour ウェブサイト検索を使用することにより、IP アドレスを Bonjour で決定することもできます。

UTN サーバを適切な形で TCP/IP ネットワークに組み込むために、様々な IPv4 パラメータの設定や、静的 IP アドレスを手動で UTN サーバに割り当てることもできます。

- myUTN Control Center から IPv4 パラメータを設定する ⇔
 ¹³
- SEH UTN Manager から IPv4 アドレスを設定する ⇔ 🗈 14
- IPv4 アドレスを SEH UTN Manager から決定して IPv4 パラメータを設定する ⇔
 ■14

myUTN Control Center から IPv4 パラメータを設定する

- 1. myUTN Control Center を起動します。
- 2. **ネットワーク IPv4** を選択します。
- 3. IPv4 パラメータを設定します。⇔表 2 🗈 14
- 4. 保存して再起動するをクリックして確定します。
- → 設定が保存されます。

表2: IPv4 パラメータ

パラメータ	説明
DHCP BOOTP ARP/PING	DHCP、BOOTP、ARP/PING プロトコルを、有効または無効にします。 DHCP および BOOTP による IP アドレスの割り当ては、これらのプロトコルの 1 つがネットワークに実装されている場合、自動的に実行されます。 Zeroconf によって割り当てられた IP アドレスを変更するには、ARP および PING コマンドを使用することができます。この実装状況は、システムにより 異なります。使用するオペレーティングシステムの説明書を参照してください。
	UTN サーバへの IP アドレス割り当て後は、これらのオプションを無効にすることを推奨します。
IPアドレス	UTN サーバの IP アドレスです。
サブネットマスク	UTN サーバのサブネットマスクです。 サブネットマスクは、大規模なネットワークの論理的なサブネットワークへの 分割に使用します。UTN サーバをサブネットワークで使用する場合は、サブ ネットワークのサブネットマスクが必要です。
ゲートウェイ	LITN サーバが使用するネットワークの標準ゲートウェイの IP アドレスです。

ゲートウェイにより、外部ネットワークから IP アドレスを指定できます。

SEH UTN Manager から IPv4 アドレスを設定する

- ✓ UTN サーバが選択リストに表示されていること ⇒ ■30。
- 1. SEH UTN Manager を起動します。
- 2. 選択リストから UTN サーバを選択します。
- 3. メニューバーから、UTN サーバ IP アドレスの設定を選択します。 IP アドレスの設定ダイアログが表示されます。
- 4. 関連する TCP/IP パラメータを入力します。
- 5. **OK**をクリックします。
- → 設定が保存されます。

IPv4 アドレスを SEH UTN Manager から決定して IPv4 パラメータを設定する SEH UTN Manager は、接続された INU サーバをネットワークから検索します。

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること ⇔
 ^{B8}。
- 1. SEH UTN Manager を起動します。
- 選択リストに何も入力されていません。ダイアログに対して、はいで確認します。
 このダイアログが表示されず、メインのダイアログ画面が表示される場合は、メニューバーで選択リスト 編集を選択します。
 プロレストの頃先 ダイアログボキニナれます。

選択リストの編集ダイアログが表示されます。

3. ネットワークリストから INU サーバを選択します。



- 4. ショートカットメニューで、IP アドレスの設定を選択します。
- IP アドレスの設定ダイアログが表示されます。
- 5. 関連する TCP/IP パラメータを入力します。

6. **OK** をクリックします。

→ 設定が保存されます。

3.2 IPv6 パラメータの設定方法

重要:

IPv6 (Internet Protocol version 6) は、より一般的な IPv4 (Internet Protocol version 4) の後継バージョンで す。IPv6 は以前と同様の基本機能を提供しますが、他に 2³² (IPv4) に代わる 2¹²⁸ (IPv6) の拡張された IP アドレス領域や自動設定などの多くの利点があります。

> IPv6のアドレス表記は IPv4 と異なります。IPv6 アドレスは、128 ビットで 構成されます。IPv6 アドレスの標準形式は、8 フィールドです。各フィール ドには、16 ビットを表す 4 つの 16 進数が含まれています。 例:2001:db8:4:0:2c0:ebff:fe0f:3b6b

Web ブラウザで URL として使用する場合、IPv6 アドレスは角括弧で囲う必要があります。これにより、ポート番号を IPv6 アドレスの一部と間違えられることを防止できます。

例:http://[2001:db8:4:0:2c0:ebff:fe0f:3b6b]:443

この URL としてのアドレス形式は、IPv6 に対応するブラウザ以外は使用で きません。

UTN サーバは、IPv6 ネットワークに組み込むことができます。



UTN (⇔ 🗈 1) と対応する SEH UTN Manager は IPv4 ネットワークでのみ機能します。

IPv6 単独のネットワークでは myUTN Control Center (⇔ 🖹6) のみが UTN サー バの管理に利用できます。

UTN サーバは、IPv4 アドレスの他に1つ以上の IPv6 アドレスも自動的に受信します。UTN サーバをネットワークに最適な形で組み込むために、IPv6 パラメータを設定することができます。

- 1. myUTN Control Center を起動します。
- 2. ネットワーク IPv6 を選択します。
- 3. IPv6 パラメータを設定します。⇔ 表 3 🖹 15
- 4. 保存して再起動するをクリックして確定します。
- ▶ 設定が保存されます。

表3: IPv6 パラメータ

パラメータ	説明
IPv6	UTN サーバの IPv6 機能を、有効または無効にします。
自動設定	UTN サーバへの IPv6 アドレスの自動割り当てを、有効または無効にします。
IPv6 アドレス	IPv6 ユニキャストアドレスを指定します。このアドレスは n:n:n:n:n:n:n の形 式で UTN サーバに手動で割り当てます。
	• 各「n」は、アドレスの8つの16ビット要素の1つの16進数の値を示します。
	• フィールド内の先頭のゼロは省略できます。
	• IPv6 アドレスは、連続するフィールドの内容がすべてゼロ (0) である場合、 短縮バージョンを使用して入力または表示できます。この場合、2 つのコロ
	ン (::) を使用します。

パラメータ	説明
ルータ	UTN サーバが要求を送信する宛先の静的ルータを手動で指定します。
プレフィックス長	IPv6 アドレスのサブネットプレフィックスの長さを設定します。64 の値があ らかじめ設定されています。 アドレス範囲 (ネットワークなど)は、プレフィックスを使用して指定します。 指定するには、プレフィックス長 (使用するビット数)を 10 進数で IPv6 アドレ スに追加し、その 10 進数の先頭にスラッシュ (A を付けます

3.3 WLAN を設定する方法

「myUTN-55」は、WLAN (Wireless Local Area Network) デバイスで次の規格に対応しています。

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n



myUTN Control Center では、ネットワーク – WLAN で現在の WLAN 設定を 表示できます。

UTN サーバを最適な形でネットワークに組み込むには、WLAN パラメータを WLAN 設定 (ネットワーク 名、暗号化、など)と一致するように設定します。そのためには、UTN サーバがすでに WLAN に組み込 まれ、アドレス指定できる必要があります。初期設定については、使用する製品の ð&「クイック・イ ンストール案内」で説明されています。

- ✓ WLANの設定の知識があること。
- ✓ UTN サーバが WLAN 範囲内にあること。



■女・ UTN サーバは、ネットワークが変更されると、新たな IP 設定を受信します。 この場合、myUTN Control Center への接続が中断します。

- 1. myUTN Control Center を起動します。
- 2. **ネットワーク** WLAN を選択します。
- 3. WLAN パラメータを設定します。⇒ 表 4 🗎 16
- 4. 保存して再起動するをクリックして確定します。
- ▶ 設定が保存されます。

表4: WLAN パラメータ

パラメータ	説明
モード	 通信モード(ネットワークインフラストラクチャ)を指定します。 アドホック:WLANは分散化されたアドホックネットワークで、デバイスがお互いに(ピアツーピアで)通信します。 インフラストラクチャ:WLANは、アクセスポイント/ルータが中央の通信ハブとして機能するインフラストラクチャネットワークです。アクセスポイントは、固定ネットワークにケーブル接続されています。
ネットワーク名 (SSID)	SSID (Service Set Identife) としても知られている WLAN のネットワーク名を入 力します。

ネットワーク設定

パラメータ	説明
ローミング	ローミング (アクセスポイント / ルータの切り替え) を、有効または無効にし ます。複数の (同一設定の) アクセスポイント / ルータがある広域に跨る WLAN で UTN サーバの位置を変更すると、ローミングがアクティブな場合に、 UTN サーバは接続ロスのない良好な信号へと自動的に切り替わります。 (インフラストラクチャモードのみ)
チャンネル	 WLAN のチャンネル(周波数範囲)を入力します。 (アドホックモードのみ) 警告 国から許可された WLAN チャンネルのみを使用してください。 UTN は、多くのチャンネルに対応するグローバルな製品です。一方で、チャンネルは各国の法令によって規制されています。したがって、UTN は使用する国で禁止されたチャンネルにも対応している場合があります。 国の規制には、各自が注意してください。
暗号化方式	WLAN を保護する暗号化方式を選択します。 重要: WEP には 16 進数キーを使用することを推奨します。 アクセスポイント / ルータによっては、ASCII フォーマットの WEP キーを 16 進数フォーマットへ変換します。この場合は、UTN サーバ上の ASCII キーとアクセスポイント / ルータ上の 16 進数が一致しません。
WEP キーを使用	使用する WEP キーを指定します。
≠-1~4	 WEP キーを指定します。4つの WEP キーが利用できます。キーの種類によってWEP キーの最大文字数と使用できる文字セットが決定されます。 重要: アクセスポイントが複数の WEP キーに対応する場合は、アクセスポイントのキー番号と UTN サーバが同一であることを確認してください。 例: ABCDE は、両方のデバイスで2つの番号を持つ必要があります(ただし、アクセスポイントが1、UTN サーバが2ではありません)。
PSK	Wi-Fi Protected Access (WPA) 用の Pre Shared Key (PSK) を指定します。
認証方式	WLAN で使用している認証メカニズムを選択します。 詳細は、「ネットワーク認証を設定する方法 (IEEE 802.1X)」」 ⇔ 🖹 55 を参照して ください。

3.4 DNS を設定する方法

DNS はドメイン名を IP アドレスに変換するサービスです。DNS を有効にしてサーバを指定する場合に、ホスト名を IP アドレスの代わりに入力できるようにします。

例:タイムサーバ設定 (⇔ 🖹 24) に 10.168.0.140 の代わりに ntp.server.de を使用。



ネットワークが適切に設定されていると、UTN サーバは DNS 設定を DHCP により自動的に受信します。自動的に割り当てられた DNS サーバは、手動 設定よりも常に優先されます。

- ✓ ネットワークに DNS サーバがあること。
- 1. myUTN Control Center を起動します。
- 2. ネットワーク DNS を選択します。
- 3. DNS パラメータを設定します。⇒表5 18
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

表5: DNS パラメータ

パラメータ	説明
DNS	DNS サーバによる名前解決を、有効または無効にします。
プライマリ DNS サーバ	プライマリ DNS サーバの IP アドレスを指定します。
セカンダリ DNS サーバ	セカンダリ DNS サーバの IP アドレスを指定します。 セカンダリ DNS サーバは、プライマリ DNS サーバが利用できない場合に 使用されます。
ドメイン名(サフィックス)	既存の DNS サーバのドメイン名を指定します。

3.5 SNMP の設定方法

SNMP (Simple Network Management Protocol) は、ネットワークの構成要素を設定、監視するためのプロトコルです。このプロトコルは、監視対象デバイスと監視側装置 (SNMP 管理ツール) との間の通信を 制御します。情報は読み込んで変更することができます。

SNMP には3つのバージョンがあり、UTN はバージョン1および2 に対応しています。

SNMPv1

SNMPv1 は最初の最も単純な SNMP のバージョンです。SNMPv1 のデメリットは、コミュニティ(コ ミュニティグループ、監視側装置、監視対象デバイス)の不安定なアクセス制御ですが、この構成要素 は容易に管理できます。コミュニティには、読み取り専用と読み取り/書き込みの2種類があります。 コミュニティ名はその両方で、監視側装置と監視対象デバイス間で使用されるパスワードでもありま す。パスワードは平文で送信されるため、十分に保護されていません。

SNMPv3

SNMPv3 は最新の SNMP バージョンです。特長は、暗号化および認証などの拡張と新たなセキュリティです。そのために、SNMP のユーザ名とパスワードを監視側装置に対し作成する必要があります。次に このユーザを UTN サーバ側に設定する必要があります。

また、ユーザアカウントは myUTN Control Center へのアクセスにも使用されます。セキュリティ - デバイスへのアクセス から指定します。「myUTN Control Center へのアクセスを保護する方法 (ユーザアカウント)」 ⇒ ■47

- ✓ SNMPv3 ユーザを、監視側装置に作成すること。(SNMPv3 のみ)
- ✓ 監視側装置の SNMPv3 ユーザが UTN サーバ ⇔ ■47 上に指定されていること。(SNMPv3 のみ)

- 1. myUTN Control Center を起動します。
- 2. **ネットワーク** SNMP を選択します。
- 3. SNMP パラメータを設定します ⇒ 表 6 🗈 19。
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

表6: SNMP パラメータ

パラメータ	説明				
SNMPv1	SNMPv1 を有効または無効にします。				
読み取り専用	コミュニティに対する書き込み禁止を、有効または無効にします。				
コミュニティ	SNMP コミュニティ名:監視側装置に設定されている名前を入力します。 重要: デフォルト名は「public」です。その名前は、読み取り/書き込み コミュニティに共通で使用されます。セキュリティの要件から、名前をできるだけ早く変更することを推奨します。				
SNMPv3	SNMPv3 を有効または無効にします。				
ハッシュ	ハッシュアルゴリズムを定義します。				
アクセス権	SNMP ユーザのアクセス権を設定します。				
暗号化	暗号化の方法を指定します。				

3.6 Bonjour の設定方法

Bonjour は、TCP/IP ネットワークで自動的にデバイスやサービスを検出する技術です。 UTN サーバは Bonjour を使用して、

- IP アドレスを検証します。
- ネットワークサービスをアナウンスし検索します。
- ホスト名と IP アドレスの整合します。
- 1. myUTN Control Center を起動します。
- 2. ネットワーク Bonjour を選択します。
- 3. Bonjour パラメータを設定します。⇔表 7 🖹 19
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

表7: Bonjour パラメータ

パラメータ	説明
Bonjour	Bonjour を有効または無効にします。
Bonjour 名	UTN サーバの Bonjour 名を設定します。
	UTN サーバは、この名前を Bonjour サービスのアナウンスに使用します。
	Bonjour 名を入力しなかった場合は、デフォルト名 (デバイス名 @ICxxxxxx) が
	使用されます。

3.7 電子メール (POP3 と SMTP) を設定する方法

UTN サーバは電子メール (⇔ ■11) により管理することができ、電子メールでステータスとエラーメッセージを送信する通知サービス (⇔ ■26) を提供します。この機能を使用するには、電子メールプロトコ

ルの POP3 と SMTP を UTN サーバ上にセットアップする必要があります。

UTN サーバなどのクライアントは、メールサーバから電子メールを取り込むために POP3 (Post Offe Protocol Version 3)を使用します。POP3 を UTN サーバ上でセットアップし、電子メールで管理できるよ うにする必要があります。

SMTP (Simple Mail Transfer Protocol) を、電子メールの送信と転送のために使用します。UTN サーバは、 電子メールによる管理および通知サービスのために SMTP を必要とします。

- POP3 を設定する ⇒ 🖹 20
- SMTP を設定する ⇒ 🖹 20

POP3 を設定する

- ✓ UTN サーバのユーザアカウントが POP3 サーバ上にセットアップされていること。
- 1. myUTN Control Center を起動します。
- 2. ネットワーク 電子メールを選択します。
- 3. POP3 パラメータを設定します。⇔ 表 8
 [●]20
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

表8: POP3 パラメータ

パラメータ	説明
POP3	POP3 の機能を有効または無効にします。
POP3 - サーバ名	POP3 サーバを IP アドレスまたはホスト名で指定します。 ホスト名での指定は、DNS サーバが事前設定されている場合にのみ可能です。
POP3 - サーバーポート	電子メールの受信用に UTN サーバが使用するポートを指定します。 POP3 のポート番号は 110 です。SSL/TLS (パラメータ「POP3 - セキュリティ」 ⇔ [■] 20) のデフォルトポート番号は 995 です。必要に応じて、POP3 サーバの説 明書を参照してください。
POP3 - セキュリティ	使用する認証方法を設定します。 ・ APOP: POP3 サーバにログオンするときにパスワードを暗号化します。 ・ SSL/TLS: POP3 サーバとの通信全体を暗号化します。暗号強度は、暗号化 プロトコルと暗号化レベルで設定されます ⇔ ■46。
POP3 - メールのチェック 間隔	POP3 サーバをチェックして電子メールを確認する時間間隔を分単位で指定し ます。
POP3 - メールサイズの上 限数	UTN サーバが許容する電子メールの最大サイズを Kbyte 単位で設定します。 (0 = 無制限)
POP3 - ユーザ名	POP3 サーバにログインするために UTN サーバが使用するユーザ名を設定します。
POP3-パスワード	POP3 サーバにログインするために UTN サーバが使用するユーザパスワードを 設定します。

SMTP を設定する

✓ UTN サーバのユーザアカウントが SMTP サーバ上にセットアップされていること。

- 1. myUTN Control Center を起動します。
- 2. ネットワーク 電子メールを選択します。
- 3. SMTP パラメータを設定します ⇔ 表 9 🖹 21。
- 4. 確定するには、保存をクリックします。
- ▶ 設定が保存されます。

表9: SMTP パラメータ

パラメータ	説明
SMTP - サーバ名	SMTP サーバを IP アドレスまたはホスト名で指定します。 ホスト名での指定は、DNS サーバが事前設定されている場合にのみ可能です。
SMTP - サーバーポート	UTN サーバおよび SMTP サーバが通信に使用するポートを指定します。 SMTP のデフォルトポート番号は 25 です。SSL/TLS (パラメータ「SMTP – SSL/ TLS」 \Rightarrow $@21$) に対して、SMTP は初期値でポート 587 (STARTSSL/STARTTLS) また は以前のポート 465 (SMTPS) を使用します。必要に応じて、SMTP サーバの説 明書を参照してください。
SMTP – SSL/TLS	SSL/TLS を有効または無効にします。 SSL/TLS は UTN から SMTP サーバへの通信を暗号化します。暗号強度は、暗号 化プロトコルと暗号化レベルで設定されます ⇔ №46。
SMTP - 送信者名	UTN サーバが電子メールの送信に使用する電子メールアドレスを設定します。 多くの場合、送信者の名前と電子メールアカウントのユーザ名は同一になりま す。
SMTP - ログイン	SNMP の認証を有効または無効にします。電子メールを送信する場合、UTN は 自己認証のために自らのユーザ名とパスワードを SMTP サーバに送信します。 ユーザ名 (パラメータ「SMTP - ユーザ名」 ⇔ ■21) およびパスワード (パラメー タ「SMTP - パスワード」 ⇔ ■21) を入力します。 SMTP サーバの中には、不正使用 (スパム)を防止するために SMTP 認証を必要
SMTP - ユーザ名	SMTP サーバにログインするために UTN サーバが使用するユーザ名を設定します。
SMTP - パスワード	SMTP サーバへのログインに使用する UTN サーバのパスワードを設定します。
SMTP - セキュリティ (S/MIME)	電子メールセキュリティ規格の S/MIME (Secure/Multipurpose Internet Mail Extensions)を、有効または無効にします。S/MIME は電子メールに署名するた め (「SMTP - 電子メールの署名」 ⇔ №21) または電子メールを暗号化 (「SMTP - 完全な暗号化」 ⇔ №21) するために使用されます。任意の機能を有効にします (「SMTP - 公開キーの添付」 ⇔ №21)。
SMTP - 電子メールの署名	電子メールの署名を有効にします。受信者は、署名を使用して送信者の識別情報をチェックできます。署名は電子メールが改ざんされていないことを証明します。 電子メールに署名を使用するには S/MIME 証明書が必要です。⇔ №50
SMTP - 完全な暗号化	電子メールの暗号化を有効にします。暗号化された電子メールは、対象の受信 者のみが開いて読むことができます。 暗号化には S/MIME 証明書が必要です ⇔ ᠍50。
SMTP - 公開キーの添付	公開キーを電子メールと一緒に送信します。 多くの電子メールクライアントが、電子メールを表示するキーを必要としま す。

3.8 VLAN 環境での UTN サーバの利用方法 (myUTN-80 以降のみ)

UTN サーバは、802.1Q に従い VLAN (Virtual Local Area Network) に対応しています。 VLAN は、物理ネットワークを論理的なサブネットワークに分割します。各サブネットワークは自らの ブロードキャストドメインを持つため、サブネットワーク間でのデータパケットの交換はできません。 VLAN は構築されたネットワークのセキュリティを強化するために使用されます。

各 USB デバイスは VLAN に割り当てることができます。VLAN データを USB ポート経由で転送するには、 最初に VLAN を UTN サーバに入力する必要があります。次に、データ転送に使用する USB ポートを指定 した VLAN にリンクする必要があります。

USB デバイスへのアクセスは、特に VLAN を使用すると調整することができます。例えば、ネットワークユーザのうち指定したグループのみが特定の USB デバイスを使用するようにできます。
 VLAN をユーザの環境に実装する方法を確認した上で、UTN サーバをセットアップしてください。

- IPv4 管理 VLAN を設定する ⇔ 🖹 22

IPv4 管理 VLAN を設定する

- 1. myUTN Control Center を起動します。
- 2. ネットワーク IPv4 VLAN を選択します。
- 3. IPv4 VLAN パラメータを設定します。⇔ 表 10 🖹 22
- 4. 確定するには、保存をクリックします。
- 5. 設定が保存されます。

表10: IPv4 管理 VLAN パラメータ

パラメータ	説明
IPv4 管理 VLAN	IPv4 管理 VLAN データの転送を、有効または無効にします。 この設定を有効にした場合、SNMP は IPv4 管理 VLAN でのみ利用できます。
VLAN ID	IPv4 管理 VLAN を識別するための ID (0 ~ 4096) です。
IPアドレス	UTN サーバの IP アドレスです ⇔ 🖹 13。
サブネットマスク	UTN サーバのサブネットマスクです ⇔ 🗎 13。
ゲートウェイ	UTN サーバが使用しているネットワークの標準ゲートウェイの IP アドレスで す ⇔ 🖹 13。 ゲートウェイにより、外部ネットワークから IP アドレスを指定できます。
任意の VLAN から のアクセス	IPv4 クライアント VLAN を介した UTN サーバへの管理者アクセス (Web) を、 有効または無効にします。 この設定が有効な場合、UTN サーバはすべての VLAN を介して管理できます。
LAN からのアクセス (タグなし)	タグなしの IPv4 パケットを介した UTN サーバへの管理者アクセスを、有効または無効にします。 この設定が無効な場合、UTN サーバは VLAN を介してのみ管理できます。



IPv4 クライアント VLAN を設定する

- 1. myUTN Control Center を起動します。
- 2. ネットワーク IPv4 VLAN を選択します。
- 3. IPv4 VLAN パラメータを設定します。⇔表 11 🖹 23
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

表11:IPv4 クライアント VLAN パラメータ

パラメータ	説明
VLAN	IPv4 クライアント VLAN データの転送を、有効または無効にします。
IPアドレス	IPv4 クライアント VLAN 内にある UTN サーバの IP アドレスです。
サブネットマスク	IPv4 クライアント VLAN 内にある UTN サーバのサブネットマスクです。
ゲートウェイ	IPv4 クライアント VLAN のゲートウェイアドレスです。
VLAN ID	IPv4 クライアント VLAN を識別するための ID (0 ~ 4096) です。



Auto-fll を使用して、VLAN、IP アドレスおよびサブネットマスクをその値 でライン1から自動的に埋めます。VLAN ID は1つずつカウントアップさ れます。

USB ポートに IPv4 クライアント VLAN を割り当てる

- 1. myUTN Control Center を起動します。
- 2. セキュリティ USB ポートアクセスを選択します。
- 3. VLANの割り当てリストから、VLANをUSBポートに割り当てます。
- 4. 確定するには、保存をクリックします。
- ▶ 設定が保存されます。

4 デバイス設定

- UTN (SSL) ポートの設定方法 ⇔ 🖹 26
- ・ メッセージを取得する方法 (myUTN-80 以降のみ) ⇔ 26
- ・ 音響信号の設定方法 (myUTN-800 のみ) ⇔ 27
- ・ ディスプレイに表示する項目を決定する方法 (myUTN-800 のみ) ⇔ 28

4.1 デバイス時間の設定方法

UTN サーバのデバイス時間は、ネットワーク上の SNTP タイムサーバ (簡易ネットワーク時刻プロトコル)により設定できます。タイムサーバは、ネットワーク内のデバイスの時間を同期します。 今日優先される時刻標準として「UTC」(協定世界時)が使用されています。地域に応じてタイムゾーンで補正されます。



重要:

適切に設定されたネットワーク上で、UTN サーバはタイムサーバ設定を DHCP により自動的に受信します。自動的に割り当てられたタイムサーバ は、手動で設定されたタイムサーバより常に優先されます。

デバイス設定

- ✓ ネットワークにタイムサーバがあること。
- 1. myUTN Control Center を起動します。
- 2. デバイス 日付 / 時間を選択します。
- 3. 日付/時間にチェックマークを付けます。
- 4. **タイムサーバ**欄に、タイムサーバの IP アドレスまたはホスト名を入力します。 (ホスト名が指定できるのは、DNS サーバがあらかじめ設定されている場合にのみです。 ⇔
 ^[]17)
- 5. **タイムゾーン**リストから、ローカルのタイムゾーンのコードを選択します。
- 6. 確定するには、保存をクリックします。
- → 設定が保存されます。

4.2 説明の記述内容を設定する方法

UTN サーバには、任意の説明を割り当てることができます。これにより、ネットワーク内で利用できる デバイスの概要がわかりやすくなります。



- 1. myUTN Control Center を起動します。
- 2. **デバイス 説明**を選択します。
- 3.ホスト名、説明および担当者の任意の名前を入力します。
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

表12:解説

パラメータ	説明
ホスト名	IP アドレスに代わるデバイス名。名前により、例えば複数の UTN サーバを使 用している場合、ネットワーク上で UTN サーバを容易に識別できます。 myUTN Control Center および SEH UTN Manager に表示されます。
説明	場所や所属部門などのデバイスの説明。 myUTN Control Center および SEH UTN Manager に表示されます。
担当者	デバイス管理者などの担当者。 myUTN Control Center に表示されます。

4.3 USB ポートに名前を割り当てる方法

初期設定で、接続された USB デバイスの名前は myUTNControl Center と SEH UTN Manager の USB ポートに表示されます。デバイスメーカが設定した名前は、曖昧で不正確な場合があります。

この理由から、例えば対応するソフトウェア名のような自由に設定できる名前を USB ポートに割り当て ることができます。そのような名前を付けることで、ネットワーク内で使用できる USB デバイスの概要 が理解しやすくなります。

- 1. myUTN Control Center を起動します。
- 2. **デバイス USB ポート**を選択します。
- 3. ポート名欄に任意の名前を入力します。
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

4.4 USB ポートを無効にする方法 (myUTN-80 以降のみ)

初期設定では、すべての USB ポートがアクティブです。USB ポートを、電源を遮断または再確立することで非アクティブ化(再度アクティブ化)にすることができます。 非アクティブ化

- 不要な USB デバイスがネットワークに接続できないようにするために、使用していない USB ポート を非アクティブにします。(非アクティブ状態の USB ポートは、SEH UTN Manager で表示されません。)
- USB ポートを非アクティブにして再度アクティブ化することで、不定な状態の接続された USB デバイスを再起動します。(USB デバイスを手作業で取り外して再接続する必要がありません。)
- 1. myUTN Control Center を起動します。
- 2. **デバイス USB ポート**を選択します。
- 3. USB ポートの前のオプションにチェックマークを付ける、またはチェックマークを外します。
- 4. 確定するには、保存をクリックします。
- → USB ポートが、無効または有効になります。

4.5 UTN (SSL) ポートの設定方法

警告

UTN サーバ (接続された USB デバイスを含む)とクライアント間のデータ転送に、共有ポートを使用します。ポートは接続の種類に依存します。

- ・ <u>暗号化されていない</u> USB 接続: UTN ポート (デフォルト: 9200)
- ・ <u>暗号化された</u> USB 接続 (⇔
 [●]44): UTN SSL ポート (デフォルト: 9443)



UTN ポートや UTN SSL ポートは、セキュリティ対策 (ファイアウォール) で 遮断しないでください。

例えばポート番号がネットワーク上の他のアプリケーションですでに使用されている場合、ポート番号 を変えることができます。変更は UTN サーバ上で実行し、クライアントにインストールされた SEH UTN Manager に SNMPv1 でリレーされます。

- ✓ SNMPv1 が有効なこと。⇔
 ■18
- 1. myUTN Control Center を起動します。
- 2. デバイス UTN ポートを選択します。
- 3. UTN ポート、または UTN SSL ポート欄にポート番号を入力します。
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

4.6 メッセージを取得する方法 (myUTN-80 以降のみ)

UTN サーバは次のような様々な メッセージを送信することができます。

- ステータス通知: UTN サーバや接続された USB デバイスの状態を通知する電子メールを定期的に送信します。
- ・ 電子メールまたは SNMP トラップによるイベント通知
 - USB デバイスが UTN サーバに接続されている /UTN サーバから切断されている
 - USB ポート (接続された USB デバイスへの接続など)が、アクティブ化または非アクティブ化されている。
 - UTN サーバの再起動
 - 電源が遮断または再確立されている (myUTN-800 のみ)
 - ネットワーク接続が遮断または再確立されている (myUTN-800 のみ)
 - SD カードが UTN サーバに挿入されている / UTN サーバから取り外されている (myUTN-800 のみ)
 - SC カードが使用できない (myUTN-800 のみ)
- ・ ステータス通知の送信を設定する ⇔ 🗎 26
- SNMP トラップでのイベント通知を設定する ⇔
 [■]27

ステータス通知の送信を設定する

ステータス通知は、最大2人の受信者に送信できます。

- ✓ SMTP がセットアップされていること。⇒
 ¹⁹
- ✓ DNS がセットアップされていること。⇒ ■17
- 1. myUTN Control Center を起動します。
- 2. デバイス 通知を選択します。
- 3. 電子メールアドレス欄に受信者を入力します。



- 4. ステータス通知領域の受信者にチェックマークを付けます。
- 5. 間隔を設定します。
- 6. 確定するには、保存をクリックします。
- → 設定が保存されます。

電子メールでのイベント通知を設定する

- イベント通知は、最大2人の受信者に送信できます。
- ✓ DNS がセットアップされていること ⇔
 ■17。
- 1. myUTN Control Center を起動します。
- 2. デバイス 通知を選択します。
- 3. 電子メールアドレス欄に受信者を入力します。
- 4. メッセージタイプのオプションに、チェックマークを付けます。
- 5. 確定するには、保存をクリックします。
- → 設定が保存されます。

SNMP トラップでのイベント通知を設定する

イベント SNMP トラップは、最大2人の受信者に送信できます。

- ✓ SNMPv1 または / および SNMPv3 がセットアップされていること。⇔
 ■18
- 1. myUTN Control Center を起動します。
- 2. デバイス 通知を選択します。
- 3. SNMP トラップの領域で、受信者を IP アドレスとコミュニティにより設定します。
- 4. メッセージタイプのオプションに、チェックマークを付けます。
- 5. 確定するには、保存をクリックします。
- → 設定が保存されます。

4.7 音響信号の設定方法 (myUTN-800のみ)

myUTN-800 Dongleserver は、次の場合に音によるフィードバックを返します。

- ・ USB ドングルが接続されたとき
- Dongleserver の再起動
- パラメータがリセットされたとき

音響信号はオフにできません。

さらに任意で、次のイベントに対する音響フィードバックを設定できます。

- 1個の電源だけが動作
- SD カードのエラー(読み取り/書き込みエラー、SD カードなし)
- 1つのネットワーク接続のみが確立されてるとき



このオプションの音響信号は、ディスプレイパネル上のエラーメッセージ を完全に補完します ⇔
¹28。

- 1. myUTN Control Center を起動します。
- 2. デバイス 通知を選択します。
- 3. 音響信号領域で、任意のメッセージタイプのオプションにチェックマークを付けます。
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

4.8 ディスプレイに表示する項目を決定する方法 (myUTN-800のみ)

Dongleserver myUTN-800 は、前面にディスプレイパネルが装備され、次の情報を表示できます。

- 識別子:任意に設定できる名前で初期値で表示されます。初期値:DS)
- エラー状態:次のイベントが発生したときに表示できる任意の通知:
 - 1個の電源だけが動作
 - SD カードのエラー(読み取り/書き込みエラー、SD カードなし)
 - 1つのネットワーク接続のみが確立されてるとき
 - エラーはコードで表示されます。
 - 表13:エラーコード

テキスト	説明	トラブルシューティング
DS (各識別子)	Dongleserver が使用できます。	_
RS	Dongleserver が再起動します。	-
DL	Dongleserver にファームウェア / ソフ トウェアが読み込まれます。その後、 Dongleserver が更新されます。	_
E1	2 つの電源のうち1 つが動作していま せん。 アクティブでない接続は、ドットの点 灯で示されます。(左のドット、左の 電源、右のドット、右の電源)	ケーブル接続と電圧源を確認します。
E2	サポート外のファイルシステムで フォーマットされた SD カードは、読 み書きができません。	 SD カードを FAT32、FAT16、または FAT12 のファイルシステムでフォーマットします。 SD カードが正確に機能していることを 確認します。
E3	この SD カードは読み取り専用です。	SD カードの書き込み禁止を解除します。
E4	カードリーダに利用できる SD カード がありません。	SD カードを SD カードリーダに挿入します。 ・ 種類: SD または SDHC ・ ファイルシステム FAT32、FAT16、また は FAT12
E5	両方のネットワーク接続の一方にリン クがありません。	ケーブル接続とネットワークを確認します。

- 識別子を設定する ⇒ ■28
- エラー通知を有効にする ⇒ ■29

識別子を設定する



複数の myUTN-800 が1つのサーバラック、または同じ場所に設置されて であめの前次のころうころです。
 であるときに、デバイスを識別するための識別子を使用します。

- 1. myUTN Control Center を起動します。
- 2. デバイス 説明を選択します。
- 3. 任意の説明を識別子(ディスプレイパネル)欄に入力します。 (最大2半角文字;A~Z、0~9)E+数字の組合せは、エラーに使用するため指定できません。

- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。



図3: ディスプレイパネル myUTN-800

エラー通知を有効にする

- 1. myUTN Control Center を起動します。
- 2. デバイス 通知を選択します。
- 3. ディスプイパネル領域で、メッセージタイプのオプションにチェックマークを付けます。
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。



オプションの音響信号は、ディスプレイパネル上のエラーメッセージを完 全に補完します。⇔
¹²7

5 SEH UTN Manager の操作

「SEH UTN Manager」は、SEH Computertechnik GmbH が開発したソフトウェアツールです。SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用されます。

- ・ ネットワーク内の UTN サーバと USB デバイスを検索する方法 ⇔ 🖹 30
- ・ USB デバイスへの接続を確立する方法 ⇔
 В32

- SEH UTN Manager をグラフィカルユーザインターフェイスなしで使用する方法 (utnm) ⇔ №40

5.1 ネットワーク内の UTN サーバと USB デバイスを検索する方法

SEH UTN Manager ソフトウェアツールは、UTN サーバに接続された USB デバイスへの接続を確立し管理 するために使用されます。

SEH UTN Manager を起動すると、ネットワークをスキャンして、接続された UTN サーバを検出します。 スキャンするネットワーク範囲は任意に設定できます。検索はマルチキャストや設定可能な IP 範囲から 実行できます。初期値は、ローカルネットワークセグメント内でのマルチキャスト検索に設定されてい ます。

検出されたすべての UTN サーバとそのサーバに接続された USB デバイスが「ネットワークリスト」に 表示されます。UTN サーバに接続された USB デバイスを使用するには、UTN サーバを「選択リスト」に 追加します。

UTN サーバを直接選択リストに追加することもできます。これを実行するには、サーバの IP アドレスが 分かっていなければなりません。

- ・ 検索パラメータを設定する ⇔ 🗎 30
- ・ ネットワークをスキャンする ⇔
 ■31
- UTN サーバを IP アドレスにより追加する ⇔
 ■32

検索パラメータを設定する

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔ ■8
- 1. SEH UTN Manager を起動します。
- メニューバーから、SEH UTN Manager プリファレンスを選択します。 オプションダイアログが表示されます。
- 3. ネットワークスキャンタブを選択します。
- 4. IP 範囲検索にチェックマークを付け、少なくとも1つのネットワーク範囲を指定します。
- 5. OKをクリックします。
- → 設定が保存されます。

ネットワークをスキャンする

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔ ■8
- 1. SEH UTN Manager を起動します。
- メニューバーから、選択リスト 編集を選択します。
 選択リストの編集ダイアログが表示されます。
- 3. スキャンをクリックします。
- ネットワークがスキャンされます。検出された UTN サーバと USB デバイスが、ネットワークリスト に表示されます。

UTN サーバを選択リストに追加する

- ✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇔ ■8
- ✓ UTN サーバがネットワークスキャンで検出され、ネットワークリストに表示されていること。
- 1. SEH UTN Manager を起動します。
- 2. メニューバーから、選択リスト 編集を選択します。 選択リストの編集ダイアログが表示されます。
- 3. 選択リストから使用する UTN サーバを選択します。
- 追加をクリックします。
 (必要に応じて、2と3の手順を繰り返し実行します。)
- 5. OK をクリックします。
- → UTN サーバおよび接続された USB デバイスが、選択リストに表示されます。

	選択リストをご希望のデパ	「イスと一緒	にまとめます。
ネットワーク			
	ネットワークリスト		選択リスト
スキャン	IC0D0D23 (10.168.1.127)		IC0D0D23 (10.168.1.127)
	▶ USB フラッシュ ドライブ (ポート 1)		▶ USB フラッシュ ドライブ (ポート 1)
オプション	myutn-80@company (10.168.1.246)		
	▶ HASP v0.06 (ボート 1)		
	▶ HASP v0.06 (ポート 2)		
	追加 >		削除
			OK = ++\+
			OK TYPE

図 4: SEH UTN Manager - 選択リストの編集

UTN サーバを IP アドレスにより追加する

- ✓ SEH UTN Manager (フルバージョン) がクライアントにインストールされていること。⇔ ■8
- ✓ UTN サーバの IP アドレスが分かっていること。
- 1. SEH UTN Manager を起動します。
- UTN サーバ 追加を選択します。 サーバの追加ダイアログが表示されます。
- 3. ホスト名または IP アドレスの欄に、UTN サーバの IP アドレスを入力します。
- UTN ポートや UTN SSL ポート (⇔
 ¹26) を変更した場合は、UTN- ポートと UTN-SSL- ポート欄に各 ポート番号を設定してください。
- 5. OKをクリックします。
- → UTN サーバおよび接続された USB デバイスが、選択リストに表示されます。

5.2 USB デバイスへの接続を確立する方法

USB デバイスをクライアントに接続する場合は、クライアントと USB デバイスが接続された UTN サーバの USB ポート間のポイントツーポイント接続を確立します。クライアントは、UTN サーバに接続された USB デバイスを、直接クライアントに接続された USB デバイスと同じ感覚で使用できます。

	重要:			
(🛛)	複合 USB デバ	「イスの特殊なケース		
	特定のタイプ 択リストはそ デバイスは、 構成され、す	の USB デバイスを UTN のポートに複数の USB ラ 複合 USB デバイスです。 べて 1 つのハウジングに	サーバの USB z デバイスを表示 ハブと 1 台以 組み込まれてい	ポートに接続すると、選 します。このタイプの 上の USB デバイスから います。
	複合 USB デバ USB デバイス 合、組み込ま します。仮想 より異なりま バイスを使用	イスが接続されたポー はすべてそのユーザのク れた各 USB デバイスは、 USB ポートの数が制限で す。制限数に達すると、 することができません。	への接続が確 ライアントに打 UTN サーバの され、ポート数 その UTN サー	立すると、表示される _{接続されます。} この場 仮想 USB ポートを使用 は UTN サーバの機種に バでそれ以上の USB デ
	UTN サーバ	仮想 USB ポート数	UTN サーバ	仮想 USB ポート数
	myUTN-50a	6	myUTN-800	40
	myUTN-55	6	myUTN- 2500	12
	myUTN-80	16		

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔ ■8
- ✓ USB ポートが選択リスト上に表示されていること。⇒ ■30
- ✓ クライアント側は、USB デバイスをローカルで操作する(直接クライアントに接続する)ために必要 な条件(ドライバのインストールなど)がすべて満たされていること。対象の USB デバイスをメーカ の説明書に従って実際にローカルでクライアントに接続し、動作を確認することを推奨します。
- ✓ USB ポートが、別のクライアントに接続されていないこと。
- 1. SEH UTN Manager を起動します。
- 2. 選択リストからポートを選択します。
- 3. メニューバーから、ポート 有効化を選択します。
- → USB デバイスとクライアント間の接続が確立されます。
SEH UTN Manager の操作

myUTN ユーザーマニュアル macOS

	 無効化(D) リクエスト 削除(R) UTN アクションの作成(C) 設定(S) 1anager 	nistrator: SEH UTN Mana	iger 3.0.14		SEH
選択リスト	UTN サーバ/デバイス	▲ ステータス	プロパティ		
	IC0D0D23 (10.168.1.127)		ポート名	USB フラッシュ ドライブ	
更新	▶ USB フラッシュ ドライブ (ポー	ト 1) 使用可能	ポート番号	1	
			ポートのステータス	使用可能	
編集			追加機能		
			暗号化	オフ	
π-ト			自動操作		
本 か化			自動接続	オフ	
19 X016			接続されたデバイス		
年加化			▼ 名前	Flash Drive	
##X0/16			ステータス	使用可能	
			製造メーカー	Alcor Micro Corp. (0x058f)	
			製品	Flash Drive (0x6387)	
			USB クラス	Mass Storage (0x08)	

図 5: SEH UTN Manager – USB ポートのアクティブ化

5.3 USB デバイスとクライアント間の接続を解除する方法

USB デバイスがクライアントに接続されている場合、その接続タイプはポイントツーポイントです。接続が確立されている間、その USB デバイスは他のクライアントに接続することができないため、他の ユーザは使用できません。そのため、使用しなくなった USB デバイスへの接続はすぐに解除する必要が あります。

USB デバイスとクライアント間の接続を解除するには、クライアントと USB デバイスが接続している UTN サーバの USB ポート間の接続を非アクティブにします。

- 通常は、ユーザが SEH UTN Manager で接続を解除します。⇔ ■33
- ・ また、管理者が myUTN Control Center から接続を非アクティブ化することもできます。⇔
 ■33

SEH UTN Manager でデバイスの接続を解除する

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔
 ■8
- ✓ USB ポートが選択リスト上に表示されていること。⇔
 ¹ ³⁰
- ✓ USB ポートが、クライアントに接続されていること。⇔
 ¹
 ³²
- 1. SEH UTN Manager を起動します。
- 2. 選択リストからポートを選択します。
- 3. メニューバーから、ポート 無効化を選択します。
- → 接続が解除されます。

myUTN Control Center からデバイスの接続を解除する

- ✓ USB ポートが、クライアントに接続されていること。⇔ ■32
- 1. myUTN Control Center を起動します。
- 2. **ホーム**を選択します。
- 3. 接続済みデバイスリストから、アクティブな接続を選択し 🐼 アイコンをクリックします。
- 4. セキュリティクエリを確認します。
- → 接続が解除されます。

5.4 使用中の USB デバイスをリクエストする方法

USB デバイスがクライアントに接続されている場合、その接続タイプはポイントツーポイントです。接 続が確立されている間、その USB デバイスは他のクライアントに接続することができないため、他の ユーザは使用できません。

使用中の USB デバイスを使用する場合は、リクエストすることができます。他のユーザはその開放リク エストをポップアップウィンドウで受信します。ユーザがリクエストに応じて、USB デバイスへの接続 を非アクティブにして開放すると、リクエストしたクライアントと USB デバイス間の接続がアクティブ になります。

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔
 ^{®8}
- ✓ SEH UTN Manager (フルバージョン)が、USB デバイスを使用するユーザのクライアントにインストールされていること。⇔ ■8
- ✓ SEH UTN Manager (グラフィカルユーザインターフェイス付きのフルバージョン)が双方のクライア ントで実行されていること。
- ✓ USB ポートが選択リスト上に表示されていること。⇒ ■30
- ✓ USB ポートが別のユーザに接続されていること。⇔ ■32(ただし、自動接続でない状態。)
- 1. 選択リストからポートを選択します。
- 2. メニューバーから、ポート リクエスト を選択します。
- ▶ 開放リクエストが送信されます。

5.5 USB デバイス接続とプログラムの開始を自動化する方法

UTN サーバの USB ポートと接続された USB デバイスへの接続は自動化することができます。これにより、複雑な作業が単純化されます。

- ・ USB デバイスが接続されているときの自動的な接続(自動接続)⇔
 24
- ・ 印刷ジョブ受信時の USB デバイスとクライアント間の自動接続 (オンデマンド印刷) ⇔
 ^[35]



この章では、自動操作のセットアップに使用する SEH UTN Manager の機 能について説明します。スクリプトに関する専門知識がある場合は、 「utnm」ツールの使用を推奨します。⇔ ■40

USB デバイスが接続されているときの自動的な接続(自動接続)

自動接続は、USB デバイスが USB ポートに接続されるとすぐに、自動的に USB ポートと接続された USB デバイスへの接続を確立します。自動接続は、各 USB ポートと USB ポートに接続されたすべての USB デバイスに対する操作がアクティブにできなければなりません。

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔ ■8
- ✓ USB ポートが選択リスト上に表示されていること。⇔
 ¹30
- ✓ クライアントに管理者としてログオンしていること。
- 1. SEH UTN Manager を起動します。
- 2. 選択リストから UTN サーバを選択します。
- 3. メニューバーから、UTN サーバ 自動接続を有効化を選択します。 自動接続を有効化ダイアログが表示されます。
- 4. 対象の USB ポートにチェックマークを付けます。
- 5. **OK** をクリックします。

→ 設定が保存されます。USB ポートと接続された USB デバイスへの接続が自動的にすぐにアクティブ になります。USB デバイスを切断して再接続すると、再び接続が自動的に確立されます。

重要: 自動接続によりアクティブ化され確立した USB ポート接続を手動で非アクティブにすると、自動接続の設定も非アクティブになります。自動接続を再び使用するには、再度設定する必要があります。

設定時間後に接続を自動的に非アクティブ化(自動切断)

自動切断は、事前に設定した時間が経過すると USB ポートと接続された USB デバイスへの接続を非アク ティブにします。時間切れの 2 分前に、データ損失とエラー状態を防止するために、ユーザは接続の非 アクティブ化を要請する通知を受信します。任意で、設定した時間内に 1 回のみ接続の延長をアクティ ブに設定することができます。この場合、ユーザは表示された通知のポップアップで、接続の延長を選 択または拒否することができます。

自動切断機能は、多くのネットワーク参加者が限られた数のデバイスを利用できるようにし、アイドル 時間を削減します。

✓SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔ ■8
 ✓UTN サーバが「デバイスの自動切断」領域に表示されていること。⇔ ■30

- ✓クライアントに管理者としてログオンしていること。
- 1. SEH UTN Manager を起動します。
- 2. メニューバーから、SEH UTN Manager プリファレンスを選択します。
- **オプション**ダイアログが表示されます。
- 3. **自動操作**タブを選択します。
- 4. 自動切断領域で、該当する UTN サーバのステータスにチェックマークを付けます。
- 5. 時間範囲 (10~-9999分)を設定します。
- 6. 任意で延長にチェックマークを付けます。
- 7. **OK**をクリックします。
- → 設定が保存されます。

印刷ジョブ受信時の USB デバイスとクライアント間の自動接続 (オンデマンド印刷)

オンデマンド印刷は、印刷ジョブの受信時に、クライアントと USB デバイス (プリンタや多機能デバイ ス) が接続された USB ポート間の接続を自動的に確立します。

印刷ジョブが完了すると、接続は自動的に解除されます。

- ✓ USB ポートが選択リスト上に表示されていること。⇒
 ¹30
- ✓ USB ポートが、別のクライアントに接続されていないこと。
- ✓ クライアントに管理者としてログオンしていること。
- 1. SEH UTN Manager を起動します。
- 2. 選択リストからポートを選択します。
- メニューバーから、ポート 有効化 を選択します。 接続が確立されます。デバイスがインストールされます。印刷オブジェクトがクライアント上に作 成されます。
- メニューバーから、ポート 設定を選択します。
 ポート設定ダイアログが表示されます。
- 5. デバイスの自動接続領域で、オンデマンド印刷にチェックマークを付けます。
- 6. **OK**をクリックします。

設定が保存されます。

- 7. メニューバーから、ポート **無効化**を選択します。 接続が解除されます。
- → オンデマンド印刷がセットアップされます。

UTN アクションを作成する: SEH UTN Manager インターフェイスを使用しない自動化されたポート接続 とプログラム起動

UTN アクションは、接続された USB デバイスを含む USB ポートへの接続を自動化するスクリプトを含む 小さなファイルです。スクリプトに設定された内容は、ファイルが実行されると自動的に実行されま す。「SEH UTN Service」はバックグラウンドで動作するため、ユーザが SEH UTN Manager インターフェ イスを起動する必要はありません。UTN アクションはフルバージョン (⇔ ■8) およびミニマルバージョン (⇔ ■8) で使用できます。

UTN アクションは、接続のアクティブ化のような単純なシナリオのみでなく、時間遅延により接続をア クティブ化してアプリケーションを起動するような複雑な操作も設定できます。UTN アクションは、 ウィザードで作成できます。ウィザードは、フルバージョン (⇔ ■8)の SEH UTN Manager でのみ利用で きます。次のような UTN アクションが作成できます。

- デバイスをアクティブまた非アクティブにする UTN アクション。
 ウィザードは、USB ポートとポートに接続された USB デバイスをアクティブにする1つの UTN アクションと、非アクティブにする1つの UTN アクションを自動的に作成します。両方の UTN アクションはデスクトップに保存されます。
- アプリケーションを起動してデバイスをアクティブにする UTN アクション ユーザがアプリケーションを選択すると、ウィザードは、アプリケーションを起動して USB ポートとポートに接続された USB デバイスをアクティブにする UTN アクションを自動的に作成します。また、アプリケーションの終了後にポートを非 アクティブにする指定もできます。
- カスタム UTN アクション(上級者専用)
 ウィザードを活用することで、カスタム UTN アクションを作成できます。次のアクションを作成できます。
 - USB ポートとポートに接続された USB デバイスを、アクティブおよび非アクティブにする UTN アクション。様々なオプションを設定できます。
 - アプリケーションの起動、および USB ポートとポートに接続された USB デバイスをアクティブにするスクリプトまた、 アプリケーション起動の遅延設定や、アプリケーション終了後に USB ポートを非アクティブにする設定など、追加のオ プションを指定できます。最後に、SEH UTN Manager により自動的に作成された完全な UTN アクションを保存します。



- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔ ■8
- ✓ USB ポートが選択リスト上に表示されていること。⇔ ■30
- 1. SEH UTN Manager を起動します。
- 2. 選択リストからポートを選択します。
- 3. メニューバーから、ポート UTN アクションの作成を選択します。 UTN アクションの作成ダイアログが起動します。
- 4. ウィザードの指示に従います。
- → UTN アクションが作成されます。作成されたファイルをダブルクリックすると、UTN アクションが 実行されます。

日 〇 〇 🔮 以	5の UTN アクションの作成 IC0D0D23 (192.168.0.107): USB フラッシュ ドライブ (ポート 1)
SFH	ようこそ
	このウィザードが UTN アクションの作成手順を案内します。UTN アクションは、デバイスの接続を自動 化する小さいファイルです。
	どのような UTN アクションを作成しますか?
	● デパイスを有効化/無効化する UTN アクションを自動的に作成します。 ● アプリケーションを起動しデパイスを有効化する UTN アクションを自動的に作成します。 ● カスタム UTN アクションを作成します。(上級者専用)
	続けるには オブションを選択して ウィ (ハ)' をクリックします.
	< 戻る(B) 次へ(N) >

図6: UTN アクションの作成



アプリは任意の場所に移動して、保存した後に名前を変更することができ ます。



(上級者専用)USB デバイスをアクティブまたは非アクティブにするカスタム UTN アクションは、作成後に編集できます。これを実行するには、アプリ内のスクリプトを編集します(パス:Contents/Resources/script)。



上級者モード(スクリプト):作成したスクリプトは、テキストエディタで 編集できます。

5.6 USB ポートと USB デバイスのステータス情報を検索する方法

USB ポートと USB デバイスのステータスは、いつでも確認できます。

- 1. SEH UTN Manager を起動します。
- 2. 選択リストから USB ポートを選択します。
- → ステータス情報がプロパティ領域に表示されます。

5.7 選択リストを使用してユーザのアクセス権を管理する方法

選択リストは、SEH UTN Manager の主要な要素で、組み込まれたすべての UTN サーバを表示します。 USB デバイスは、それが接続している UTN サーバが選択リスト上にある場合のみに使用できます。(⇔ ■30) 選択リストを制御することで、結果的に UTN サーバと接続された USB デバイスへのユーザアクセ スを制御できます。

初期値では、すべてのクライアントユーザが SEH UTN Manager のグローバル選択リストを使用します が、クライアントユーザに対してユーザ固有の選択リストを設定することができます。そのリストは ユーザが任意に編集ができます。または、クライアント管理者がユーザ権限を制限して、設定した UTN サーバのみを使用できるリストを提供することも可能です。 表14:グローバルとユーザ選択リストとの相違点

グローバル選択リスト



- 1つのクライアントのすべてのユーザが、同じ 選択リストを使用します。
- ユーザは、選択リストに表示されたすべての デバイスにアクセスできます。
 (ただし、myUTN Control Center でセキュリ ティメカニズムが指定されていない場合に限 定されます。)
- ・ リストの保存場所:Library

管理者リスト 管理者リスト 管理者リスト 管理者

ユーザ選択リスト

- 各ユーザは、自分専用の選択リストを所有し ます。 すべての管理者は同じ選択リストを所有しま す。 ユーザは、選択リストに表示されたすべての デバイスにアクセスできます。 (ただし、myUTN Control Center でセキュリ ティメカニズムが指定されていない場合に限 定されます。) リスト(「ini」-ファイル)の保存場所: \$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini (\$HOME は macOS のユーザフォルダ用の環境変 数です。現在のユーザのパスは次のコマンド ラインで決定できます:echo \$HOME 例 macOS 10.15.7 (Catalina): echo \$HOME は /Users home/User name を与えます +.config/SEH Computertechnik GmbH/SEH UTN Manager.ini ini ファイルのフルパス: /Usershome/User name/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini)
- 選択リストは、管理者が編集できます。
- ・選択リストは、管理者または書き込み権限の あるユーザが編集できます。
 ini-ファイルに対し読み取り専用の権限のみ ユーザは、選択リストを編集できず、SEH UTN Managersへのアクセスも制限されます。



SEH UTN Manager で使用できる機能(選択リスト編集など)は、選択リストの種類(グローバルまたはユーザ)とクライアント上のユーザアカウントの種類(管理者/ユーザ、ini-ファイルへの書き込み権限がある/ないユーザ)に依存します。分類の詳細は、「SEH UTN Manager – 機能の概要」 ➡ 圖91 を参照してください。

- ・ 設定が保存されます。各ユーザは、個別の(所定の)選択リストを使用します。管理者は、1つの選択リストを共有します。「SEH UTN Manager.ini」-ファイルへの書き込み権限を制限する ⇔ 🗎 39

すべてのユーザにグローバル選択リストをセットアップする

初期値ではグローバル選択リストが使用されます。

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔ ■8
- ✓ システムに管理者としてログオンしていること。
- 1. SEH UTN Manager を起動します。
- 2. 選択リストを構成します。⇔ ■30
- 3. メニューバーから、SEH UTN Manager プリファレンスを選択します。 オプションダイアログが表示されます。
- 4. 選択リストタブを選択します。
- 5. グローバル選択リストにチェックマークを付けます。
- 6. **OK**をクリックします。
- → 設定が保存されます。1つのクライアントのすべてのユーザが、同じ選択リストを使用します。

ユーザ選択リストを提供する

- ✓ SEH UTN Manager (フルバージョン)がクライアントにインストールされていること。⇔
 ■8
- ✓ システムに管理者としてログオンしていること。
- 1. SEH UTN Manager を起動します。
- 2. メニューバーから、SEH UTN Manager プリファレンスを選択します。 オプションダイアログが表示されます。
- 3. 選択リストタブを選択します。
- 4. ユーザ選択リストにチェックマークを付けます。
- 5. OKをクリックします。
- オプション:次の手順で所定の選択リストを提供します。
- 6. 対象のデバイスを含む選択リストを作成します。⇔ ■30
- メニューバーから、選択リスト エクスポートを選択します。
 エクスポート先ダイアログが表示されます。
- 8. 「SEH UTN Manager.ini」を、次のユーザディレクトリに保存します。 \$HOME/.confg/SEH ComputertechnikCenb H/SEH UTN Manager.ini (⇔表 14 🗎 38)

設定が保存されます。各ユーザは、個別の(所定の)選択リストを使用します。管理者は、1つの選択リ ストを共有します。「SEH UTN Manager.ini」-ファイルへの書き込み権限を制限する

ユーザ選択リストは、ユーザ自身がセットアップし編集することができます。

UTN サーバへのユーザアクセスを制限して、リストをユーザに提供することもできます。これを実行す るには、管理者はユーザ (⇔
[®]39) に対する所定のリストを保存して、「SEH UTN Manager.ini」-ファイル へのユーザアクセスを読み取り専用に制限します。ユーザ権限を読み取り専用に制限することで、選択 リストに関するすべての SEH UTN Manager 機能が、対象のユーザに対して無効になります。

オペレーティングシステムの通常の方法で、ini-ファイルを読み取り専用ファイルにします。詳細は、 オペレーティングシステムの説明書を参照してください。

5.8 SEH UTN Manager をグラフィカルユーザインターフェイスなしで使用 する方法 (utnm)

SEH UTN Manager には 2 つのバージョンがあります。⇔
■8 ミニマルバージョンでは、グラフィカル ユーザインターフェイスなしで使用できます。これを実行するには、オペレーティングシステムの端末 から「utnm」ツールを利用して UTN 機能を使用します:

- ・ 直接。コマンドを特定の構文で入力して実行
- ・ 特定構文のコマンドを含むスクリプト。コマンドラインインタープリタにより自動的に順次実行



スクリプトを使用して、ポートのアクティブ化のような頻繁に使用するコ マンドシーケンスを自動化します。

ログインスクリプトなどを使用し、スクリプトの実行を自動化することが できます。

- 構文 ➡ 🗎 40
- ・ コマンド ⇒ ■40
- ・ リターン情報 ⇔ 🗎 42
- ・端末から utnm を使用する ⇔
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
 ¹
- ・ utnm スクリプトを作成する ⇔ 🗎 43

構文

utnm -c "コマンド文字列" [-< コマンド>]

実行ファイル「utnm」は、「SEH UTN Manager.app」にあります。/usr/bin/ にシンボリックリンクが あります。

コマンド

コマンドの規則

- 未定義の要素は、適切な値(例:サーバ=UTN サーバのIP アドレスまたはホスト名)で置換されます。
- 角括弧内の要素は任意です。
- ・ 大文字、小文字を区別しません。
- ・ ASCII フォーマットのみ読み込み可能です。

コマンド	説明
-c " <u>コマンド文字列</u> " または	コマンドを実行します。コマンドは、コマンド文字列で詳しく指定 します。コマンド文字列:
command " <u>コマンド文字列</u> "	・ activate <u>サーバポート番号</u> USB ポートと接続された USB デバイスへの接続をアクティブに します。
	 activate <u>サーバ</u> ベンダ ID (VID) 製品 ID (PID) 複数の同じ USB デバイスが UTN サーバに接続されている場合 に、USB ポートと最初に接続された USB デバイスを設定された ID でアクティブにします。
	・ deactivate <u>サーバポート番号</u> USB ポートと接続された USB デバイスへの接続を非アクティブ にします。
	・ set autoconnect = true false <u>サーバポート番号</u> USB ポートへの自動接続 (⇔ 🖹34) を、有効または無効にします。
	 set portkey='port key' <u>サーバポート番号</u> USBのポートキー (⇔ ■49) をシステム上にローカルで保存します。このように、USB ポートキーは常に自動的に送信されるため、毎回コマンドで指定する必要がありません。-k <u>USB ポートキーまたは</u>key <u>USB ポートキー</u>(次を参照)。 (USB ポートキーを削除するために使用するコマンド文字列: set portkey= <u>サーバポート番号</u>)
	● 重要: このコマンドは、USB デバイスを利用できる目的のみ で、キーを正式に設定します。 USB ポートキーは、myUTNControl Center ⇒ ■49 で設 定します。
	 find ネットワークセグメント内のすべての UTN サーバを検索して、 検出した UTN サーバをその IP アドレス、MAC アドレス、機種、 およびソフトウェアバージョンとともに表示します。
	・ getlist <u>サーバ</u> UTN サーバに接続された USB デバイスの概要 (ポート番号、ベ ンダ ID、製品 ID、ベンダ名、製品名、デバイスクラス、ステー タスなど)を表示します。
	 state <u>サーバポート番号</u> USB ポートに接続された USB デバイスの状態を表示します。
-h または	ヘルプページを表示します。

--help

SEH UTN Manager の操作

コマンド	説明
-k <u>USB ポートキー</u> または key <u>USB ポートキー</u>	USB ポートキーを指定します。 \Rightarrow 画49 重要: このコマンドは、USB デバイスを利用できる目的のみ で、キーを入力します。 USB キーが毎回自動的に送信されるように、それを正式 にシステムに保存するには、-c " <u>コマンド文字列</u> " ま たはcommand " <u>コマンド文字列</u> " コマンドを使用し ます(上記を参照)。 USB ポートキーは、myUTNControl Center \Rightarrow 画49 で設 定します。
-mr または machine readable	getlist コマンド文字列の出力をタブで区切り、find の出力をコ ンマで区切ります。
-nw または no-warnings	警告メッセージを抑制します。
-o または output	コマンドラインの出力を表示します。
-p <u>ポート番号</u> または port <u>ポート番号</u>	代替の UTN ポートを使用します。 UTN ポート番号を変更した場合に、このコマンドを使用します (⇔ ᠍26)。
-q または quiet	出力を抑制します。
-sp <u>ポート番号</u> または ssl-port <u>ポート番号</u>	代替の SSL/TLS 暗号化された UTN ポートを で使用します。 <u>UTN SSL</u> ポート番号を変更した場合に、このコマンドを使用します (⇔ ≧26)。
-t <u>秒</u> または -timeout <u>秒</u>	コマンド文字列 activate および deactivate のタイムアウトを設 定します。
-v または version	utnm のバージョン情報を表示します。

リターン情報

コマンドの実行後、リターン情報はコマンドが正常に実行されたかどうかを示します。リターン情報は、戻り値(リターンコード)と組み合わされたステータスとなります。出力が抑制されると(「-quiet」⇔ ■42)、値のみが返されます。

リターン情報は、例えばスクリプトの中で処理を進める方法を決定するために使用することができます。

戻り値	説明
0	コマンドは正常に実行されました。
20	アクティブ化が失敗しました。
21	非アクティブ化が失敗しました。
23	すでにアクティブになっています。
24	すでに非アクティブになっている、または利用できません。
25	アクティブ化が失敗しました。別のユーザがデバイスを含む USB ポートをアクティブにしています。
26	検出されません。USB ポートに接続されたデバイスがない、または USB ポートキー (⇔ ۩49) が見つからない、もしくは間違っています。
29	検出されません。この <u>VID</u> および <u>PID</u> を持つ <u>USB</u> デバイスが接続されていません。
30	アイソクロナス USB デバイスに対応していません。
31	UTN ドライブエラー。SEH Computertechnik GmbH のサポート部門にご連絡ください。 ☆ 🛯 4
40	UTN サーバへのネットワーク接続がありません。
41	UTN サーバへの暗号化接続が確立できません。
42	UTN Service への接続がありません。
43	DNS 解決に失敗しました。
44	権限が不十分です (管理者権限が必要です)。
47	この機能には対応していません。
200	エラー (エラーコード表示)
端末から ut	tnmを使用する

- ✓ SEH UTN Manager がクライアントにインストールされていること。⇔ ■8
- ✓ UTN の IP アドレスまたはホスト名が分かっていること。
- 1. 端末を開きます。
- 2. コマンドを入力します。「構文」⇔ ■40 および「コマンド」⇔ ■40 を参照してください。
- 3. 入力内容を確認します。
- → コマンドシーケンスが実行されます。

例:IP アドレス 10.168.1.167 の UTN サーバのポート 3 上にある USB デバイスをアクティブにする utnm -c "activate 10.168.1.167 3"

utnm スクリプトを作成する

- ✓ SEH UTN Manager がクライアントにインストールされていること。⇔ ■8
- ✓ UTN の IP アドレスまたはホスト名が分かっていること。
- ✓ 使用するオペレーティングシステム上でスクリプトを作成し使用する方法を理解していること。 必要に応じて、オペレーティングシステムの説明書を参照してください。
- 1. テキストエディタを開きます。
- 2. コマンドのシーケンスを入力します。「構文」⇔ ■40、「コマンド」 ⇒ ■40 および「リターン情報」 ⇒ ■42を参照してください。
- 3. ファイルを実行スクリプトとしてクライアントに保存します。
- → スクリプトが保存されて使用できます。

6 セキュリティ

UTN サーバは、様々なセキュリティメカニズムにより保護することができます。メカニズムが搭載され た UTN サーバのみでなく、接続された USB デバイスも保護します。UTN もまた、ネットワークに実装 された保護メカニズムの中に組み込むことができます。

- USB 接続を暗号化する方法 ⇒ ■44
- ・ myUTN Control Center への接続を暗号化する方法 ⇔ 🗎 45
- SSL/TLS 接続の暗号化強度を設定する方法 ⇒ ■46
- ・ myUTN Control Center へのアクセスを保護する方法 (ユーザアカウント) ⇔ 🗎 47
- ・ UTN サーバのポートをブロックする方法 (TCP ポートアクセス制御) ⇔ 🗎 48
- USB デバイスの種類をブロックする方法 ⇔ ■50
- ・
 証明書の使用方法
 ゅ
 ■50

myUTN Control Center へのアクセスをユーザアカウントで規制し、セキュリティ関連の設定が不正な改ざんから保護してください。



セキュリティには、SNMP および VLAN も使用できます。

- 「SNMPの設定方法」⇒ ■18

6.1 USB 接続を暗号化する方法

USB 接続を保護するには、クライアントと UTN サーバに接続された USB デバイス間のデータ転送を暗号 化します。暗号化は、各接続すなわち各 USB ポートを個別にアクティブにする必要があります。



里要: ペイロードのみが暗号化されます。管理データおよびログデータは、暗号化 せずに送信されます。

暗号化プロトコルの SSL (Secure Sockets Layer) とその後継の TLS (Transport Layer Security) が暗号化に使



SEH UTN Manager は、**低**暗号化レベルに対応していません。暗号化した USB 接続との組合せで**低レベル**をセットアップすると、接続を確立すること ができません。

できる限り高い暗号化レベルを使用してください。

接続が暗号化されていると、クライアントと UTN サーバは UTN SSL ポートを介して通信します。その ポート番号は、初期値で9443です。そのポートがすでに別のアプリケーションなどによりネットワー



図7: UTN サーバ - ネットワーク内の SSL/TLS 接続

- 1. myUTN Control Center を起動します。
- 2. セキュリティ 暗号化を選択します。
- 3. USB ポートの暗号化を有効にします。
- 4. 確定するには、保存をクリックします。
- → クライアントと USB デバイス間のデータ転送が暗号化されます。

暗号化接続は、クライアント側で、SEH UTN Manager のプロパティの下に 表示されます。

UTN サーバノデバイス	▲ ステータス	プロパティ	
	- ~/ /~		
▼ ⊟ IC0D0D23 (10.168.1.127)		W-1-4	USB / 7 9 9 1 F 7 1 /
▶ USB フラッシュ ドライブ (ポート 1)	使用可能	ポート番号	1
		ポートのステータス	使用可能
		追加加加起	
		暗号化	オン
		自動操作	
		自動接続	オフ
		接続されたデバイス	
		▼ 名前	Flash Drive
		ステータス	使用可能
		製造メーカー	Alcor Micro Corp. (0x058f)
		製品	Flash Drive (0x6387)
		USB クラス	Mass Storage (0x08)

図 8:SEH UTN Manager - 暗号化

6.2 myUTN Control Center への接続を暗号化する方法

myUTN Control Center への 接続は、SSL (Secure Sockets Layer) およびその後継の TLS (Transport Layer Security) プロトコルを使用して暗号化することができます。

- HTTP:<u>非</u>暗号化接続
- HTTPS 暗号化接続

暗号強度は、暗号化プロトコルと暗号化レベルで設定されます ⇔ [®]46。暗号化接続の確立が必要に なると、クライアントはブラウザを介して証明書を要求します (⇔ [®]50)。証明書はブラウザが承認で きる必要があります。ブラウザソフトウェアの説明書を参照してください。

警告
現在のブラウザは低レベルのセキュリティ設定に対応していません。低レベ ル設定では接続を確立できません。
次の組合せは使用 <u>しない</u> でください:暗号化プロトコル HTTPS と低暗号化 レベル

- 1. myUTN Control Center を起動します。
- 2. **セキュリティ デバイスへのアクセス**を選択します。
- 3. 接続領域の HTTP/HTTPS または HTTPS のみにチェックマークを付けます。
- 4. 確定するには、保存をクリックします。
- → 設定が保存されます。

6.3 SSL/TLS 接続の暗号化強度を設定する方法

UTN サーバに対する接続は双方向とも、SSL (Secure Sockets Layer) およびその後継の TLS (Transport Layer Security) プロトコルを使用して暗号化することができます。

- ・ 電子メール: POP3 (⇔ 🖹 19)
- ・ 電子メール: SMTP (⇔ 🖹 19)
- myUTN Control Center への Web アクセス: http (⇔
 [●]45)

・ クライアントと UTN サーバ (および接続された USB デバイス)間のデータ転送: USB 接続 (⇔ №46) 暗号化の強度、さらに接続の安全性は暗号化プロトコルと暗号化レベルで設定します。両方とも選択可 能です。

各暗号化レベルとは、暗号スイートの集合です。暗号スイートとは、セキュアな接続を確立するために 使用される4つの暗号アルゴリズムの標準シーケンスで、暗号化強度に基づき暗号化レベルへとグルー プ化されます。UTNサーバが対応する暗号化レベルを形成する暗号スイートは、選択した暗号化プロト コルにより決定されます。2つの暗号化レベルから選択できます。

- 任意:暗号化は、通信当事者の双方で自動的にネゴシエートされます。双方が対応する最も高い暗 号化が常に選択されます。
- ・ 低レベル:低レベルの暗号化強度の暗号スイートのみを使用します。(高速データ転送)
- ・ 中レベル
- ・ 高レベル:高レベルの暗号化強度の暗号スイートのみを使用します。(低速データ転送)

セキュアな接続を確立する際に、使用するプロトコルと対応する暗号スイートのリストを通信相手に送 信します。使用する暗号スイートを取り決めます。初期値では、当事者双方が対応する暗号スイート中 で最も強力なスイートが使用されます。

UTN サーバの通信相手が、選択したプロトコルに対応していない場合や、 当事者の双方が対応する暗号スイートがない場合、SSL/TLS 接続は確立され ません。

問題が発生する場合は、別の設定を選択する、または UTN サーバのパラ メータをリセットしてください。⇔ ■60



UTN サーバとその通信相手とで自動的に設定をネゴシエートする場合は、 双方とも 任意に設定してください。この設定を使用すると、セキュアな接 続が確立できる可能性が最も高くなります。

1. myUTN Control Center を起動します。

警告

- 2. **セキュリティ SSL 接続**を選択します。
- 3. 暗号化プロトコル領域から、任意の暗号化プロトコルを選択します。



警告

現在のブラウザは SSL に対応していません。使用するブラウザが最新のバー ジョンで、myUTN Control Center へのアクセスに SSL および HTTPS のみの 組合せを設定している場合 (⇔ ■45) は、接続が確立できません。 TLS (および SSL 以外)を使用してください。



重要:

UTN サーバが対応するプロトコルは、製品のハードウェアおよびインス トールされたファームウェア / ソフトウェアにより異なります。

4. 暗号化レベル領域から、任意の暗号化レベルを選択します。



警告

現在のブラウザは、低レベルの暗号スイートに対応していません。使用する ブラウザが最新のバージョンで、myUTN Control Center へのアクセスに**低 レベル** および HTTPS のみの組合せを設定している場合 (⇔ ■45) は、接続が 確立できません。

できる限り高い暗号化レベルを使用してください。



警告

SEH UTN Manager は、低暗号化レベルに対応していません。暗号化した USB 接続 (⇔ ■44) との組合せで低レベルをセットアップすると、接続を確立 することができません。 できる限り高い暗号化レベルを使用してください。

- 5. 確定するには、保存をクリックします。
- → 設定が保存されます。



個別の SSL/TLS 接続状態の詳細 (対応する暗号スイートなど)は、SSL 接続の状態 - 詳細の詳細ページを参照してください。

6.4 myUTN Control Center へのアクセスを保護する方法(ユーザアカウント)

初期値では、UTN をネットワーク内で検出できる場合、myUTN Control Center にアクセスできるユーザ に制限はありません。UTN を不正な設定から保護するために、2 種類のユーザアカウントをセットアッ プできます。

- 管理者:myUTN Control Centerへのフルアクセス。対象のユーザは、すべてのページの設定を変更 することができます。
- 読み取り専用ユーザ:myUTN Control Center への最小限のアクセス。対象のユーザは、「ホーム」ページのみを閲覧できます。

ユーザアカウントをセットアップした後で myUTN Control Center を起動するとログイン画面が表示されます。2 種類のログイン画面から選択できます。

- ユーザのリスト:ユーザ名が表示されます。パスワードの入力のみが必要です。
- 名前とパスワードのダイアログ:ニュートラルなログイン画面で、ユーザ名とパスワードの入力が 必要です。(より高い保護度)

ユーザアカウントによりマルチログインが可能になります。アカウントはユーザ単独でもユーザのグ ループでも使用できます。同時に最大16ユーザまでログインできます。

重要:

myUTN Control Center アクセスのユーザアカウントは SNMP にも使用しま す ⇔
ฏ18。ユーザアカウントのセットアップ時に考慮してください。

より強力なセキュリティとして、セッションタイムアウトを使用することができます。設定したタイム アウト時間内にまったく操作をしなかった場合、ユーザは自動的にログアウトされます。

- 1. myUTN Control Center を起動します。
- 2. **セキュリティ デバイスへのアクセス**を選択します。
- 3. 2 種類のユーザアカウントを設定します。ユーザアカウントの領域で、ユーザ名とパスワードを入力 します。



パスワードの入力内容を確認する場合は、文字として表示することができ ます。

- 4. Control Center へのアクセス制限にチェックマークを付けます。
- 5. ログイン画面の種類を、ユーザのリストと名前とパスワードから選択します。
- セッションタイムアウトにチェックマークを付け、セッション時間欄にタイムアウトが有効になる 時間を分単位で入力します。
- 7. 確定するには、保存をクリックします。
- → 設定が保存されます。

6.5 UTN サーバのポートをブロックする方法 (TCP ポートアクセス制御)

UTN サーバへのアクセスを、「TCP ポートアクセス制御」を使用してポートをブロックすることで制限 できます。ポートをブロックすると、このポートを使用するプロトコルやサービスは UTN サーバとの接 続を確立できなくなるため、攻撃による影響が少なくなります。

セキュリティレベルでブロックするポートの種類を設定します:

- UTN アクセス (UTN ポートのブロック)
- TCP アクセス (TCP ポート: HTTP/HTTPS/UTN のブロック)
- ・ すべてのポート (IP ポートのブロック)

例外を設定して、クライアントや DNS サーバなどの任意のネットワーク構成要素が UTN サーバとの接続を確立できるようにする必要があります。



警告

「テストモード」では、設定をテストするときにユーザ自身は除外されない ように、初期値でアクティブに設定されています。UTN が再起動するまで 設定はアクティブになり、以降のアクセスは制限されません。 設定のテストが正常に終了後、アクセス制御が正式に設定されるように、テ ストモードを非アクティブにする必要があります。

- 1. myUTN Control Center を起動します。
- 2. **セキュリティ TCP ポートアクセス**を選択します。
- 3. ポートアクセス制御にチェックマークを付けます。
- 4. セキュリティレベル領域から、任意の暗号化レベルを選択します。
- 5. **例外**領域で、UTN サーバにアクセスするネットワーク構成要素を設定します。IP または MAC (ハードウェア) アドレスを入力して、オプションにチェックマークを付けます。

重要: • MAC アドレスはルータを通して配信されません。 • ワイルドカード (*) を使用すると、サブネットワークを指定できます。

- 6. テストモードが有効であることを確認します。
- 7. 保存して再起動するをクリックして確定します。 設定が保存されます。
- デバイスを再起動するまで、ポートアクセス制御はアクティブです。
- 8. mvUTN Control Center に接続できることを確認する場合は、ポートアクセスをチェックします。



myUTN Control Center に接続できない場合は UTN サーバを再起動してくだ さい ⇔
ів 58。

- 9. **テストモード**を非アクティブにします。
- 10. 保存して再起動するをクリックして確定します。
- → 設定が保存されます。

6.6 USB デバイスへのアクセスを制御する方法 (myUTN-80 以降のみ)

USB ポートと接続された USB デバイスへの接続を制限できます。

- USB ポートキー制御: USB ポートにキーが設定されています。USB ポートと接続された USB デバイ スのいずれも SEH UTN Manager に表示されず、USB デバイスは使用できません。USB ポートのキー が SEH UTN Manager に入力されている場合のみ、USB ポートおよび接続された USB デバイスが表示 されます。
- USB ポートのデバイスの割り当て:特定のUSB デバイスが USB ポートに接続されます。これは USB ポートと USB デバイスを、USB デバイスのベンダ ID (VID) および製品 ID (PID) とリンクさせることで 実現します。VID と PID の組合せは特定の USB デバイス機種に固有です。この特定機種の USB デバ イスのみが USB ポートで使用できます。この方法により、USB デバイスを他のポートに接続しても セキュリティ設定を迂回できないことが保証されます。



- USB ポートキーをセットアップする ⇒
 ¹
 ¹
- USB ポートのデバイス割り当てをセットアップする ⇔
 ¹ 50

USB ポートキーをセットアップする

USB ポートのキーが myUTN Control Center に設定されています。

- 1. myUTN Control Center を起動します。
- 2. セキュリティ USB ポートアクセスを選択します。
- 3. 任意の USB ポートの**方法**リストに進み**ポートのキー制御**を選択します。
- 4. キーの生成をクリックする、またはキー欄に任意のキーを(最大 64 ASCII 文字で)入力します。
- 5. 確定するには、保存をクリックします。
- → 設定が保存されます。USB デバイスへのアクセスが保護されます。

機能を非アクティブにするには、方法リストに進み --- を選択します。

USB ポートキーを入力する (USB デバイスを解除する)

USB ポートのキー制御で保護された USB デバイスを利用するには、対応するキーをクライアントの SEH UTN Manager に入力する必要があります。

- 1. SEH UTN Manager を起動します。
- 2. 選択リストから UTN サーバを選択します。
- 3. メニューバーから、UTN サーバ USB ポートキーの設定を選択します。 USB ポートキーの設定ダイアログが表示されます。
- 4. 対応する USB ポートのキーを入力します。
- 5. **OK**をクリックします。
- → アクセスが許可されます。USB ポートと接続された USB デバイスが選択リストに表示され、使用できるようになります。

USB ポートのデバイス割り当てをセットアップする

- 1. myUTN Control Center を起動します。
- 2. **セキュリティ USB ポートアクセス**を選択します。
- 3. 任意の USB ポートの方法リストに進みデバイス割り当てを選択します。
- 4. デバイスの再割り当てをクリックします。 USB デバイス欄に、USB デバイスの VID および PID が表示されます。
- 5.確定するには、**保存**をクリックします。
- → 設定が保存されます。割り当てられた USB デバイス機種のみが、その USB ポートで操作できるよう になります。

機能を非アクティブにするには、方法リストに進み---を選択します。

6.7 USB デバイスの種類をブロックする方法

USB デバイスは、機能に応じて分類されています。例えば、キーボードのような入力デバイスは 「Human Interface Device」(HID) グループに分類されます。

USB デバイスは、HID クラスの USB デバイスとして提供されますが、不正な使用が後を絶ちません (いわゆる「BadUSB」)。

UTN サーバを保護するために、HID クラスに分類される入力デバイスをブロックできます。

- 1. myUTN Control Center を起動します。
- 2. **セキュリティ デバイスへのアクセス**を選択します。
- USB デバイス領域で、入力デバイス (HID クラス) を無効にするにチェックマークを付ける、または チェックマークを外します。
- 4. 確定するには、保存をクリックします。
- ▶ 設定が保存されます。

6.8 証明書の使用方法

UTN サーバには独自の証明書管理機能があります。ディジタル証明書はデータセットで、人間やオブ ジェクトまたは組織の識別情報を確認します。TCP/IP ネットワークでは、データの暗号化および通信相 手の認証に使用されます。

UTN では次の場合、証明書が必要です。

- ・ 電子メール通信 (SSL/TLS を介した POP3/SMTP) を保護する ⇔
 ¹⁹
- クライアントと接続された USB デバイス間の接続を保護する ⇔ ■44

- myUTN Control Center (HTTPS) への接続を保護する ⇔ 🛙 45
- UTN サーバでは次の証明書が使用できます。
- 自己署名証明書 x 1 UTN サーバにより生成され UTN サーバ自体の署名による証明書です。この証明書は UTN サーバの識別情報を確認します。
- クライアント証明書 (要求した証明書または PKCS#12 証明書) x 1 この証明書は、認証局 (CA) という付加的な信頼できる機関の協力で UTN サーバの識別情報を確認し ます。
 - 要求した証明書:最初のステップとして、証明書の要求は UTN サーバ上で生成され認証局に送信 されます。次のステップで、認証局は要求に基づき UTN サーバ に対して証明書を作成して署名し ます。
 - PKCS#12 証明書:証明書の交換フォーマット。UTN サーバ用にパスワード保護された PKCS#12 フォーマットで保存された証明書を、認証局に生成させます。その PKCS#12 ファイル (したがって、その中の証明書)を UTN サーバにトランスポートしてインストールします。
- S/MIME 証明書 x 1

UTN サーバは、自身が送信する電子メールの署名、暗号化に S/MIME 証明書を使用します。対応する秘密キー (PKCS#12 フォーマット)は、電子メールを検証し必要に応じて復号化できるように、自らの証明書として電子メールプログラム (メール など.) にインストールしておく必要があります。(myUTN-80 以降のみ)

CA 証明書(ルート CA 証明書)x1~32
 認証局に対して識別情報を確認するために発行される証明書です。CA 証明書は、各認証局が発行した証明書を検証するために使用されます。UTN サーバの場合、それは通信相手の証明書で識別情報(信頼チェーン)を検証するために発行されます。複数のレベルの公開キーインフラストラクチャ(PKIs)に対応しています。

重要:

出荷時には、デフォルト証明書が UTN サーバに保存されています。この証明書は、SEH Computertechnik GmbH が各デバイスごとに発行します。

- 証明書を表示する ⇔ 🗈 51
- ・ 自己署名証明書を作成する ⇔ №52
- ・ 証明書を要求しインストールする (要求した証明書) ⇔ 153

- CA証明書をインストールする ⇔
 ¹ ¹ ¹ ¹ ¹ ¹ ¹
- 証明書を削除する ⇔ 🖹 54

証明書を表示する

- ✓ 証明書が UTN サーバにインストールされていること。
- 1. myUTN Control Center を起動します。
- 2. **セキュリティ 証明書**を選択します。
- 3. 🝳 アイコンで証明書を選択します。
- → 証明書が表示されます。

自己署名証明書を作成する



自動署名証明書の場合、UTN サーバにインストールできるのは 1 つのみです。

新たな証明書を作成する場合は、最初に既存の証明書を削除する必要があり ます。⇔
¹■54

1. myUTN Control Center を起動します。

重要:

- 2. セキュリティ 証明書を選択します。
- 3. 自己署名証明書をクリックします。
- 4. 適切なパラメータを入力します。⇒表 15 152
- 5. 作成 / インストールをクリックします。
- → 証明書が作成されインストールされます。完了までに数分必要な場合があります。

表15: 証明書作成用パラメータ

説明
任意の証明書名です。(最大 64 半角文字)
 デバイスと証明書を明確に一致させること ができるように、UTN サーバの IP アドレス、またはホスト名を使用してください。
UTN サーバの担当者の電子メールアドレスです。 (最大 40 半角文字、任意)
UTN サーバを使用する会社の名前です。 (最大 64 半角文字)
会社の部門または課の名前です。 (最大 64 半角文字、任意)
会社の場所です。 (最大 64 半角文字)
会社が本拠を置く地域です。 (最大 64 半角文字)
付加属性の入力ができます。 (任意入力)
Subject Alternative Names (サブジェクトの別名:SAN) の入力ができま す。別のホスト名 (ドメインなど) の入力に使用します。 (任意入力。半角 255 文字以内)
会社が本拠を置く国です。ISO 3166 に従い 2 文字の国コードを入力します。 例:DE = ドイツ、GB = 英国、US = 米国
証明書が有効となる日付を指定します。指定日以降に有効になります。
証明書が無効となる日付を指定します。指定日に無効になります。
使用する RSA キーの長さを指定します。 - 512 ビット(高速暗号化および復号化) - 768 ビット - 1024 ビット(標準暗号化および復号化) - 2048 ビット(低速暗号化および復号化)

セキュリティ

myUTN ユーザーマニュアル macOS

証明書を要求しインストールする(要求した証明書)

認証局により UTN サーバに対して発行された証明書は、UTN サーバで使用できます。 使用するには、最初に証明書要求を作成し、認証局に送信します。認証局は要求に基づき、UTN サーバ に対して個別に証明書を作成します。この証明書を UTN サーバにインストールします。



- 1. myUTN Control Center を起動します。
- 2. セキュリティ 証明書を選択します。
- 3. 認証要求をクリックします。
- 4. 必要なパラメータを入力します。⇒表 15 152
- 5. **要求の作成**をクリックします。 証明書の要求が送信されます。完了までに数分必要な場合があります。
- 6. **アップロード**を選択して、要求をテキストファイルに保存します。
- 7. **OK**をクリックします。
- 8. テキストファイルを、証明書の要求として認証局に送信します。 認証局は、証明書を作成して要求元に送信します。

重要: 証明書は「base64」形式であることが必要です。

- 9. 要求された認証情報をクリックします。
- 10. パスワードボックスにパスワードを入力します。
- 11. インストールをクリックします。
- → 要求した証明書が UTN サーバに保存されます。

PKCS#12 証明書をインストールする



すでに PKCS#12 証明書が UTN にインストールされている場合は、最初にその証明書を削除してください。⇔

⁶54

- ✓ 証明書は「base64」形式であること。
- 1. myUTN Control Center を起動します。
- 2. セキュリティ 証明書を選択します。
- 3. PKCS#12 認証情報をクリックします。
- 4. PKCS#12 証明書を認証情報ファイル欄に入力します。
- 5. パスワードを入力します。
- 6. **インストール**をクリックします。
- → PKCS#12 証明書が UTN サーバにインストールされます。

S/MIME 証明書をインストールする (myUTN-80 以降のみ)



重要:

すでに S/MIME 証明書が UTN にインストールされている場合は、最初にその 証明書を削除してください。⇔ ា54

- ✓ 証明書は「pem」形式であること。
- 1. myUTN Control Center を起動します。
- 2. **セキュリティ 証明書**を選択します。
- 3. S/MIME 証明書をクリックします。
- 4. S/MIME 証明書を認証情報ファイル欄に入力します。
- 5. **インストール**をクリックします。
- → S/MIME 証明書が UTN サーバに保存されます。

CA 証明書をインストールする

- ✓ 証明書は「base64」形式であること。
- 1. myUTN Control Center を起動します。
- 2. セキュリティ 証明書を選択します。
- 3. CA 認証情報をクリックします。
- 4. CA 証明書を認証情報ファイル欄に入力します。
- 5. インストールをクリックします。
- → CA 証明書が UTN サーバに保存されます。

証明書を削除する



myUTN Control Center への暗号化された (HTTPS ⇔ №45) 接続を確立するに は、証明書 (自己署名 /CA/PKCS#12) が必要です。該当する証明書が削除さ れると、myUTN Control Center に接続できなくなります。 この場合は、UTN サーバを再起動してください ⇔ №58。UTN サーバは、新 たな自己署名証明書を生成します。それを使用してセキュアな接続を確立す ることができます。

- ✓ 証明書が UTN サーバにインストールされていること。
- 1. myUTN Control Center を起動します。
- 2. セキュリティ 証明書を選択します。
- 3. Q アイコンで削除する証明書を選択します。
 証明書が表示されます。
- 4. 削除をクリックします。
- ▶ 証明書が削除されます。

6.9 ネットワーク認証を設定する方法 (IEEE 802.1X)」

認証とは、識別情報の立証および検証です。認証により、許可されたデバイスのみがネットワークにア クセスできるため、不正利用から保護されます。

UTN は、EAP (拡張認証プロトコル) に基づく IEEE 802.1X 規格に従った認証に対応しています。

IEEE 802.1X に従いネットワーク内で認証を使用している場合は、UTN サーバを参加させることができます。

- EAP-TLS を設定する ⇔ 🖹 55
- EAP-TTLS を設定する ⇔ 🖹 56
- PEAP を設定する ⇔ 🖹 56
- EAP-FASTを設定する ⇔ 🖹 57

EAP-MD5 を設定する

EAP-MD5 (Message Digest #5) は、RADIUS サーバによるユーザベースの認証方式です。最初に、RADIUS サーバ上で UTN サーバのユーザ (ユーザ名およびパスワード) を作成する必要があります。その後 UTN サーバ上で EAP-MD5 をセットアップします。

✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。

- 1. myUTN Control Center を起動します。
- 2. セキュリティ 認証を選択します。
- 3. 認証方法リストから MD5 を選択します。
- 4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを 入力します。
- 5. 保存して再起動するをクリックして確定します。
- → 設定が保存されます。

EAP-TLS を設定する

EAP-TLS (Transport Layer Security) RADIUS サーバによる相互の証明書ベースの認証です。この方法では、 UTN サーバと RADIUS サーバが暗号化された TLS 接続を通じて証明書を交換します。 RADIUS サーバと UTN サーバの両方に、CA により署名された有効なデジタル証明書が必要です。した

RADIUS サーハと UTN サーハの両方に、CA により著名された有効なテンタル証明書か必要です。した がって、PKI (公開キーインフラストラクチャ) が必要になります。



警告

次の順序に従い作業してください。この順序に従って実行しなかった場合、 ネットワーク内で UTN サーバに接続できなくなることがあります。 その場合は、UTN サーバのパラメータをリセットしてください ⇔
■60。

- 1. UTN サーバ上で証明書の要求を作成します ⇒ №53。
- 2. 証明書の要求および認証サーバを使用して、証明書を作成します。
- 3. UTN サーバに要求した証明書をインストールします ⇔ №53。
- 認証サーバ (RADIUS) の証明書を発行した認証局のルート CA 証明書を UTN にインストールします ⇒ ¹
 ⁶⁵⁴
 ⁶
- 5. myUTN Control Center を起動します。
- 6. セキュリティ 認証を選択します。
- 7. 認証方法リストから TLS を選択します。
- 8. EAP ルート証明書のリストから、ルート CA 証明書を選択します。
- 9. 保存して再起動するをクリックして確定します。
- → 設定が保存されます。

EAP-TTLS を設定する

EAP-TTLS (Tunneled Transport Layer Security) では、機密情報の交換に TLS で保護されたトンネルが使用 されます。この方式は、次の 2 つのフェーズで構成されます。

- 1. 外部認証:暗号化された TLS (Transport Layer Security) トンネルが UTN サーバと RADIUS サーバ間に 作成されます。そのために、RADIUS サーバが、CA の署名済みの証明書を使用して UTN に対し自己 認証をします。
- 2. 内部認証:トンネル内では、認証 (CHAP、PAP、MS-CHAP または MS-CHAPv2 による) が発生しま す。
- ✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。
- ✓ 接続を確立する間のセキュリティ強化(オプション)のために、認証サーバ(RADIUS)の証明書を発行した認証局のルート CA 証明書が UTN にインストールされていること ⇔

 [●] 54。
- 1. myUTN Control Center を起動します。
- 2. セキュリティ 認証を選択します。
- 3. 認証方法リストから TTLS を選択します。
- 4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを 入力します。
- 5. TLS チャンネル内の通信を保護するための設定を選択します。
- 6. 接続を確立する間のセキュリティを強化します(オプション)。 EAP ルート証明書のリストから、ルート CA 証明書を選択します。
- 7. 保存して再起動するをクリックして確定します。
- → 設定が保存されます。

PEAP を設定する

PEAP (保護拡張認識プロトコル)により、暗号化 TLS (Transport Layer Security) トンネルが、UTN サーバ と RADIUS サーバ間に確立されます。そのために、RADIUS サーバが、CA の署名済みの証明書を使用し て UTN に対し自己認証をします。TLS チャンネルは、付加的な EAP 認証方式 (MSCHAPv2 など) によっ て保護できる別の接続を確立するために使用されます。

- ✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。
- ・ 接続を確立する間のセキュリティ強化(オプション)のために、認証サーバ(RADIUS)の証明書を発行した認証局のルート CA 証明書が UTN にインストールされていること ⇔
 ◎54。
- 1. myUTN Control Center を起動します。
- 2. セキュリティ 認証を選択します。
- 3. 認証方法リストから PEAP を選択します。
- 4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを 入力します。
- 5. TLS チャンネル内の通信を保護するための設定を選択します。
- 6. 接続を確立する間のセキュリティを強化します (オプション)。 EAP ルート証明書のリストから、ルート CA 証明書を選択します。
- 7. 保存して再起動するをクリックして確定します。
- → 設定が保存されます。

EAP-FAST を設定する

EAP-FAST (Flexible Authentication via Secure Tunneling) は、Cisco 社が開発した特定の EAP 方式です。 EAP-TTLS (⇔
⑤56) および PEAP (⇔
⑥56) と同様に、セキュアなトンネルがデータ伝送を保護しますが、こ のサーバは証明書による自己認証をしません。代わりに、PACs (Protected Access Credentials) が使用さ れます。

- ✓ UTN サーバのユーザアカウントが RADIUS サーバ上にセットアップされていること。
- 1. UTN Control Center を起動します。
- 2. セキュリティ 認証を選択します。
- 3. 認証方法リストから FAST を選択します。
- 4. RADIUS サーバ上で UTN サーバ用にセットアップするユーザアカウントのユーザ名とパスワードを 入力します。
- 5. チャンネル内の通信を保護するための設定を選択します。
- 6. 保存して再起動するをクリックして確定します。
- → 設定が保存されます。



7 メンテナンス

UTN サーバは次の方法でメンテナンスできます。

- ・ UTN サーバを再起動する方法 ⇔ №58
- 更新の手順 ⇒ 1158
- ・ 設定をバックアップする方法 ⇔ 🗎 59
- ・ パラメータを初期値にリセットする方法 ⇔ ■60

7.1 UTN サーバを再起動する方法

パラメータの変更後やアップデート後に、UTN サーバは自動的に再起動します。UTN サーバが認識され ない場合は、UTN サーバを手動で再起動することもできます。

- ・ myUTN Control Center から UTN サーバを再起動する ⇔ 🗈 58

myUTN Control Center から UTN サーバを再起動する

- 1. myUTN Control Center を起動します。
- 2. メンテナンス 再起動を選択します。
- 3. 再起動をクリックします。
- → UTN サーバが再起動します。

リセットボタンで UTN サーバを再起動する

1. デバイスの再起動ボタンを短く押します。

→ UTN サーバが再起動します。

7.2 更新の手順

UTN サーバは、ソフトウェアおよびファームウェアの更新ができます。新しいファームウェア / ソフト ウェアには、新たな機能やエラー修正が含まれています。

UTN サーバにインストールされているファームウェア / ソフトウェアのバージョン番号は、myUTN Control Center のホームページまたは。

最新のファームウェア / ソフトウェアのファイルは、次の SEH Computertechnik GmbH ウェブサイトで 入手できます:

http://www.seh-technology.jp/services/downloads.html



既存のファームウェア/ソフトウェアのみが更新され、設定は保持されます。



- 1. myUTN Control Center を起動します。
- 2. メンテナンス 更新を選択します。
- 3. アップデートファイルをファイルの更新欄に指定します。



4. **インストール**をクリックします。

→ 更新が実行されます。その後、UTN サーバが再起動します。

7.3 設定をバックアップする方法

UTN サーバのすべての設定値 (パスワード以外)は、「< デフォルト名 >_parameter.txt」ファイルに保存されます。

このパラメータファイルは、バックアップ用コピーとしてローカルクライアントに保存できます。バックアップにより、常に安定した設定状態が復元できます。

バックアップファイルのパラメータ値は、テキストエディタで編集できます。編集後、そのファイルを 1 台以上の UTN サーバにダウンロードできます。ダウンロード後に、デバイスはそのファイルのパラ メータ値を採用します。

Dongleserver の myUTN-800 には自動バックアップ機能もあります。パラメータ値および UTN サーバに インストールされた証明書を、自動的に接続された SD カードに保存します。パラメータや証明書が変 更されると、バックアップは自動的に更新されます。設定を別の UTN サーバに転送するには、SD カー ドをその別デバイスに挿入します。コールドブート (電源の遮断と復旧)後に、設定は自動的に読み込 まれます。



盗難や紛失により SD カードが悪用されると、サーバ環境(証明書、パスワード)が危険な状態になります。 自動バックアップを使用する場合は、UTN サーバを必要なあらゆる対策で 保護しなくてはなりません。

- ・ パラメータファイルを保存する ⇔ 🖹 59
- パラメータファイルを UTN サーバに読み込む ⇔ ■60

パラメータ値を表示する

- 1. myUTN Control Center を起動します。
- 2. メンテナンス パラメータのバックアップを選択します。
- 3. 🔇 アイコンをクリックします。
- ▶ 現在のパラメータ値が表示されます。

パラメータファイルを保存する

- 1. myUTN Control Center を起動します。
- 2. メンテナンス パラメータのバックアップを選択します。
- 3. 🖹 アイコンをクリックします。
- 4. ブラウザを使用して「< デフォルト名 >_parameters.txt」ファイルをローカルシステムに保存します。
- ▶ パラメータファイルがバックアップされます。



パラメータファイルを UTN サーバに読み込む

- 1. myUTN Control Center を起動します。
- 2. メンテナンス パラメータのバックアップを選択します。
- 3. パラメータファイル欄に「< デフォルト名 >_parameters.txt」ファイルを指定します。
- 4. **インポート**をクリックします。
- → UTN サーバはファイルのパラメータ値を採用します。

自動バックアップ (myUTN-800 のみ)

- ✓ SD カードが UTN サーバに接続されていること。
- ✓ SD カードのファイルシステムが FAT12、FAT16、または FAT32 であること。
- ✓ SD カードに 1 MB の利用できる空き容量があること。

(工場出荷時には、上記の要件が保証されています。)

- 1. myUTN Control Center を起動します。
- 2. **メンテナンス SD カード**を選択します。
- 3. パラメータのバックアップにチェックマークを付けます。
- 4. 保存をクリックします。
- → 設定が保存されます。

7.4 パラメータを初期値にリセットする方法

例えば UTN を別のネットワークに設置する場合、UTN を初期値にリセットすることができます。すべての設定が工場出荷時の設定になります。インストール済みの証明書は削除されません。



エタ・ UTN サーバの IP アドレスがリセットにより変更されると、myUTN Control Center への接続が遮断される場合があります。 必要に応じて新しい IP アドレスを設定してください ⇔ 🖹 13。

設定は、リモートアクセス (myUTN Control Center) または UTN サーバのリセットボタンにより変更でき ます。



UTN Control Center のパスワードを忘れた場合、UTN サーバをリセットボ タンでリセットすることができます。リセットする場合は、パスワードが 必要ありません。



myUTN-800:パラメータをリセットする前に、SD カードを UTN サーバから 取り出してください。SD カードを取り出さないと、UTN サーバはカードに 保存されたパラメータ値を読み込みます (自動バックアップ ⇔ ា59)。

- myUTN Control Center でパラメータをリセットする ⇔ ■60
- ・ リセットボタンでパラメータをリセットする ⇔ ■61

myUTN Control Center でパラメータをリセットする

- 1. myUTN Control Center を起動します。
- 2. メンテナンス 初期設定を選択します。
- 初期設定をクリックします。 セキュリティクエリが表示されます。



4. セキュリティクエリを確認します。

┗ パラメータがリセットされます。

リセットボタンでパラメータをリセットする リセットボタンにより、UTN サーバのパラメータを初期値にリセットすることができます。

- リセットボタンを 5 秒間押します。 UTN サーバが再起動します。 (Dongleserver myUTN-800 は再起動時にビープ音を発します。)
- → パラメータがリセットされます。

8 補足

この補足には、用語集やトラブルシューティングおよび本説明書のリストが含まれています。

- ・ 用語集 ⇨ 🗎 62

- SEH UTN Manager 機能の概要 ⇔ 🗎 91

8.1 用語集

複合 USB デバイス

複合 USB デバイスは、ハブと1台以上の USB デバイスから構成され、すべて1つの筐体に組み込まれています。ドングルは多くの場合、複合 USB デバイスです。

複合 USB デバイスが UTN サーバの USB ポートに接続されていると、組み込まれている USB デバイス はすべて myUTN Control Center および SEH UTN Manager の選択リストに表示されます。ポート接続が アクティブになると、表示された USB デバイスはすべてそのユーザのクライアントに接続されます。 複数の USB デバイスの場合、1 つのみのポート接続をアクティブにすることはできません。

デフォルト名

メーカにより割り当てられたデバイス名で変更することができません。同一の UTN サーバを複数使用 している場合は、この名前でデバイスを識別できます。

UTN サーバのデフォルト名は、2 つの文字「IC」とデバイス番号で構成されています。デバイス番号は、ハードウェアアドレスの後半の6桁で構成されています。

デフォルト名は myUTN Control Center で確認できます。

ハードウェアアドレス

ハードウェアアドレス (イーサネットアドレス、物理アドレスまたは MAC アドレスともいう)は、ネッ トワークインターフェイスの全世界で通用する一意な識別子です。同一の UTN サーバを複数使用して いる場合は、この名前でデバイスを識別できます。

メーカが、デバイスのハードウェアにこのアドレスを設定しています。アドレスは 12 個の 16 進数で 構成されています。最初の6つの数字はメーカを表し、後の6つの数字で各デバイスを識別します。 数字を区切る文字はプラットフォームにより異なります。OS X/macOS ではコロン (:) が使用されます。



ハードウェアアドレスは、筐体上や SEH UTN Manager で確認できます。

myUTN Control Center

myUTN Control Center は UTN サーバのユーザインターフェイスです。UTN サーバは、myUTN Control Center から設定および監視することができます。

myUTNControl Center へはインターネットブラウザ (Safari など) からアクセスします。 詳細はこちら:⇔ ■6

SEH UTN Manager

「SEH UTN Manager」は、SEH Computertechnik GmbH が開発したソフトウェアツールです。SEH UTN Manager は、UTN サーバに接続された USB デバイスへの接続を確立し管理するために使用されます。 詳細はこちら:⇔
■8

8.2 トラブルシューティング

この章では、いくつかの不具合を中心に、不具合の内容、状態、修復方法を説明しています。

補品

問題

- UTN サーバ:接続が確立できない ⇔ 🗈 64
- myUTN Control Center: 接続が確立できない ⇔ ■64
- ・ myUTN Control Center:ユーザ名やパスワードを忘れた ⇔ ■65
- SEH UTN Manager: USB デバイスが表示されない ⇔ 🗎 65
- SEH UTN Manager: USB ポートには1つのデバイスのみが接続されているにもかかわらず、複数の USB デバイスが表示される ⇔ ■66
- SEH UTN Manager:機能が利用できない、または非アクティブになっている ⇔ ■66

修復

<u>UTN サーバ:BIOS モード</u>

ファームウェアが正常に機能しソフトウェアに問題がある場合、UTN サーバは BIOS モードに切り替わります。例えば、ソフトウェアの更新が適切ではない場合、BIOS モードになることがあります。



- LED が BIOS モードを示します。
- ・ Status LED が消灯
- Activity LED が一定間隔に点滅



警告 BIOS モードでは UTN サーバは利用できません。 当社のサポート部門にご連絡ください ⇔ №4。

<u>UTN サーバ:接続が確立できない</u>

ネットワーク内の UTN サーバを検出し、TCP/IP 接続によりアクセスできますが、SEH UTN Manager か らの接続が確立できません。

考えられる原因:

- ファイアウォールや他のセキュリティソフトウェアが通信をブロックしている。
 ファイアウォールやセキュリティソフトウェアの例外に、UTN ポートまたは UTN SSL ポートを追加してください。例外に追加する方法については、該当するファイアウォールやセキュリティソフトウェアの説明書を参照してください。
- SEH UTN Manager 内と UTN サーバ上のポート番号が一致しない。ポート番号を変更したときに SNMPv1 が非アクティブであったため、変更が SEH UTN Manager に送信できません ⇔
 ¹ ■26。

<u>myUTN Control Center: 接続が確立できない</u>

考えられるエラー原因を取り除いてください。確認:

ケーブルの接続

・ UTN サーバの IP アドレス ⇔ 🖹 13

ブラウザのプロキシ設定(詳細はブラウザの説明書を参照してください)

考えられるエラー原因を取り除いた後も、まだ接続が確立できない場合は、次の保護メカニズムが原因の可能性があります。

- ・ SSL/TLS (HTTPS) によりアクセスが制限されている ⇔ ■45。
- アクセスが SSL/TLS (HTTPS) により制限され、証明書 (自己署名 /CA/PKCS#12) が削除された ⇔
 ¹ 50。 UTN サーバのパラメータを初期値にリセットしてください ⇔
 ¹ 60。その過程で新しい証明書が作成 されます。



デバイスをリセットするとすべての設定が失われ、IP アドレスも変更される 場合があります。 必要に応じて新しい IP アドレスを設定してください ⇔ 🖹 13。

myUTN Control Center:ユーザ名やパスワードを忘れた

myUTN Control Center へのアクセスが制限されているときにアクセス認証情報を忘れてしまった場合 は、UTN サーバを初期値にリセットすることができます。リセットすると、初期値ではアクセス規制さ れていない myUTN Control Center を利用できるようになります。



デバイスをリセットするとすべての設定が失われ、IP アドレスも変更される 場合があります。 必要に応じて新しい IP アドレスを設定してください ⇔ 🖻 13。

<u>SEH UTN Manager: USB デバイスとの接続が確立できない</u>

考えられる原因:

- USB デバイスが、すでに別のクライアントに接続されています。
 他のユーザが接続を終了するのを待つ、またはデバイスをリクエストします ⇔
 ¹³⁴。
- USB デバイスのドライバソフトウェアがクライアントにインストールされていません。
 その USB デバイスのドライバソフトウェアをインストールします。インストールする方法は、該当する USB デバイスの説明書を参照してください。

<u>SEH UTN Manager: USB デバイスが表示されない</u>

考えられるエラー原因を取り除いてください:最初に、UTN サーバに USB デバイスが接続されているこ とを確認してください。

確認後も USB デバイスがまだ表示されない場合は、次の問題が原因である可能性があります。

- 複数の複合 USB デバイス (⇔ ■62) が UTN サーバに接続されている。組み込まれた USB デバイスはそれぞれ、UTN サーバの 仮想 USB ポートを使用しますが、仮想 USB ポートの数は制限されています。 制限数に達すると、その UTN サーバではそれ以上 USB デバイスを使用できません (⇔ ■32)。
- USB ポートキーが、その USB デバイスに対してアクティブになっている ⇔ ■49。
 USB ポートのキーが SEH UTN Manager に入力されているときだけ、USB ポートおよび接続された USB デバイスが表示されます。

<u>SEH UTN Manager: USB ポートには1つのデバイスのみが接続されているにもかかわらず、複数の USB</u> デバイスが表示される

考えられる原因:

- ・ USB ハブの が、UTN サーバの USB ポートに接続されている。
- 接続された USB デバイスが、複合 USB デバイスである (⇔ ■62)。複合 USB デバイスは、ハブと1台 以上の USB デバイスから構成され、すべて1つの筐体に組み込まれています。USB ポートへの接続 が確立されると、表示された USB デバイスはすべてそのユーザのクライアントに接続されて使用で きるようになります。

<u>SEH UTN Manager:機能が利用できない、または非アクティブになっている</u>

考えられる原因:

- 使用するクライアントユーザアカウントに、必要な管理者権限がない。それにより、SEH UTN Manager でのユーザ権限も制限されます。詳細は、「SEH UTN Manager – 機能の概要」⇔
 191 の章を 参照してください。
 SEH UTN Manager を管理者権限で起動します。方法は、オペレーティングシステムの説明書を参照 してください。
- 接続した USB デバイスが、特定の機能に対応していない。(例:ハードディスクが「オンデマンド印刷」機能に対応していない。)

8.3 パラメータリスト

UTN サーバはその設定をパラメータに保存します。パラメータは直接、次の目的に使用します。

- 電子メールによる管理 ⇔ 🗎 11
- ・ 設定のバックアップ(パラメータの表示、編集、および他のデバイスへの読込み)⇔ 159

次の表にすべてのパラメータおよびその値を示します。表を参考に前述の操作に使用することができま す。

補足

- 表 16 「パラメータリスト IPv4」 ⇔ 🗎 68
- ・ 表 17 「パラメータリスト IPv6」⇔ 🗎 69

- ・ 表 20 「パラメータリスト Bonjour」 ⇒
 ¹
- ・ 表 22 「パラメータリスト SMTP (myUTN-80 以降のみ)」 ⇔
 1/3
- 表 23 「パラメータリスト IPv4-VLAN (myUTN-80 以降のみ)」
 ■75
- ・ 表 24 「パラメータリスト WLAN (myUTN-55 のみ)」 ⇔ 🗎 76
- ・表25「パラメータリスト 日付 / 時間」 ⇒ ■78
- ・表 26 「パラメータリスト 説明」⇔ 1878

- 表 29「パラメータリスト 通知 (myUTN-80 以降のみ)」 ⇔ 🗎 80
- ・ 表 30 「パラメータリスト ディスプレイ (myUTN-800 のみ)」 ⇔ 🗎 83
- ・ 表 31 「パラメータリスト 音響信号 (myUTN-800 のみ)」 ⇔ 🗎 83
- 表 32 「パラメータリスト SSL/TLS 接続」 ⇔ 🖹 84
- ・ 表 33 「パラメータリスト myUTN Control Center セキュリティ」 ⇔ 🗎 85

- 表 36「パラメータリスト USB デバイス種類のブロッキング」
 ■88
- 表 37 「パラメータリスト IPv4-VLAN (myUTN-80 以降のみ)」⇔ ■88
- ・ 表 38 「パラメータリスト 認証」⇔ 🗎 89
- ・ 表 39 「パラメータリスト バックアップ (myUTN-800 のみ)」 ⇔ 🗎 90

表16:パラメータリスト - IPv4

パラメータ	値	初期値	説明
ip_addr [IP アドレス]	有効な IP アドレス	169.254.0.0/ 16	UTN サーバの IP アドレスです。
ip_mask [サブネットマスク]	有効な IP アドレス	255.255.0.0	UTN サーバのサブネットマスクです。 サブネットマスクは、大規模なネットワー クをサブネットワークへと論理的に分割す るために使用します。UTN サーバをサブ ネットワークで使用する場合は、サブネッ トワークのサブネットマスクが必要です。
ip_gate [ゲートウェイ]	有効な IP アドレス	0.0.0.0	UTN サーバが使用するネットワークの標準 ゲートウェイの IP アドレスです。 ゲートウェイにより、外部ネットワークか ら IP アドレスを指定できます。
ip_dhcp [DHCP]	on/off	on	DHCP プロトコルを、有効または無効にしま す。 DHCP がネットワーク内で有効な場合、IP ア ドレスは自動的に割り当てられます。
ip_bootp [BOOTP]	on/off	on	BOOTP プロトコルを、有効または無効にし ます。 BOOTP がネットワーク内で有効な場合、IP アドレスは自動的に割り当てられます。
ip_auto [ARP/PING]	on/off	on	ARP/PING プロトコルを、有効または無効に します。 Zeroconf によって割り当てられた IP アドレ スを変更するには、ARP および PING コマン ドを使用することができます。この実装状 況は、システムにより異なります。使用す るオペレーティングシステムの説明書をお 読みください。



UTN サーバが IP アドレスを受信した後すぐに、DHCP、BOOTP および ARP/PING を非アクティブにすることを推奨します。
表17:パラメータリスト - IPv6

パラメータ	値	初期値	説明
ipv6 [IPv6]	on/off	on	UTN サーバの IPv6 機能を、有効または無効 にします。
ipv6_auto [自動設定]	on/off	on	UTN サーバへの IPv6 アドレスの自動割り当 てを、有効または無効にします。
ipv6_addr [IPv6 アドレス]	n:n:n:n:n:n:n	::	 IPv6 ユニキャストアドレスを指定します。 このアドレスは n:n:n:n:n:n の形式で UTN サーバに手動で割り当てます。 各「n」は、アドレスの 8 つの 16 ビット 要素の 1 つの 16 進数の値を示します。 フィールド内の先頭のゼロは省略できます。 IPv6 アドレスは、連続するフィールドの 内容がすべてゼロ (0) である場合、短縮 バージョンを使用して入力または表示できます。この場合、2 つのコロン (::) を使 用します。
ipv6_gate [ルータ]	n:n:n:n:n:n:n:n	::	UTN サーバが要求を送信する宛先の静的 ルータを、手動で指定します。
ipv6_plen [プレフィックス長]	0~64 [1~2個の半角文 字:0~9]	64	IPv6 アドレスのサブネットプレフィックス の長さを設定します。64 の値があらかじめ 設定されています。 アドレス範囲(ネットワークなど)は、プレ フィックスを使用して指定します。指定す るには、プレフィックス長(使用するビット 数)を10 進数で IPv6 アドレスに追加し、そ の10 進数の先頭にスラッシュ(/)を付けま す。

表18:パラメータリスト - DNS

パラメータ	值	初期値	説明
dns [DNS]	on/off	on	DNS サーバによる名前解決を、有効または 無効にします。
dns_domain [ドメイン名]	最大 255 半角文字 [a~z、A~Z、 0~9]	[空白]	プライマリ DNS サーバの IP アドレスを指定 します。
dns_primary [プライマリ DNS サーバ]	有効な IP アドレス	0.0.0.0	セカンダリ DNS サーバの IP アドレスを指定 します。 セカンダリ DNS サーバは、プライマリ DNS サーバが利用できない場合に使用されます。
dns_secondary [セカンダリ DNS サーバ]	有効な IP アドレス	0.0.0.0	既存の DNS サーバのドメイン名を指定しま す。

表19:パラメータリスト - SNMP

パラメータ	値	初期値	説明
snmpv1 [SNMPv1]	on/off	on	SNMPv1 を有効または無効にします。
snmpv1_ronly [読み取り専用]	on/off	off	コミュニティに対する書き込み禁止を、有 効または無効にします。
snmpv1_community [コミュニティ]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	public	SNMP コミュニティ名: 監視側装置に設定されている名前を入力します。
snmpv3 [SNMPv3]	on/off	on	SNMPv3 を有効化または無効化します。
any_hash [ハッシュ]	md5 sha	md5	SNMP ユーザグループ 1 のハッシュアルゴリ ズムを指定します。
any_rights [アクセス権]	 readonly readwrite	readonly	SNMP ユーザグループ 1 のアクセス権を設定 します。 =[なし]
any_cipher [暗号化]	 aes des		SNMP ユーザグループ1 の暗号化の方法を設 定します。 =[なし]
admin_hash [ハッシュ]	md5 sha	md5	SNMP ユーザグループ 2 のハッシュアルゴリ ズムを指定します。
admin_rights [アクセス権]	 readonly readwrite	readwrite	SNMP ユーザグループ 2 のアクセス権を設定 します。 =[なし]
admin_cipher [暗号化]	 aes des		SNMP ユーザグループ 2 の暗号化の方法を設 定します。

● **重要:** UTN サーバのユーザアカウントは SNMP ユーザアカウントとしても使用されます ⇔ 18。ユーザアカウントのセットアップ時に考慮してください。

表20:パラメータリスト - Bonjour

パラメータ	値	初期値	説明
bonjour [Bonjour]	on/off	on	Bonjour を有効または無効にします。
bonjour_name [Bonjour 名]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[デフォルト 名]	myUTN サーバの Bonjour 名を設定します。 myUTN サーバは、この名前を Bonjour サー ビスのアナウンスに使用します。Bonjour 名 が入力しなかった場合は、デフォルト名 (デ バイス名 @ICxxxxx) が使用されます。

表21:パラメータリスト - POP3 (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
pop3 [POP3]	on/off	off	POP3 の機能を有効または無効にします。
pop3_srv [サーバ名]	最大 128 半角文字	[空白]	POP3 サーバを IP アドレスまたはホスト名で 指定します。 ホスト名での指定は、DNS サーバが事前設 定されている場合にのみ可能です。
pop3_port [サーバポート]	1~65535 [1~5 個の半角文 字:0~9]	110	電子メールの受信用に UTN サーバが使用す るポートを指定します。 POP3 のポート番号は 110 です。SSL/TLS (パラメータ「POP3 - セキュリティ」⇔ ≧20) のデフォルトポート番号は 995 です。必要 に応じて、POP3 サーバの説明書を参照して ください。
pop3_sec [セキュリティ]	0~2 [1桁の数字: 0~2]	0	 使用する認証方法を設定します。 APOP: POP3 サーバにログオンするとき にパスワードを暗号化します。 SSL/TLS: POP3 サーバとの通信全体を暗 号化します。暗号強度は、暗号化プロト コルと暗号化レベルで設定されます ⇔ ■46。 0 = セキュリティなし 1 = APOP 2 = SSL/TLS
pop3_poll [メールのチェック間 隔]	1~10080 [1~5 個の半角文 字:0~9]	2	POP3 サーバをチェックして電子メールを確認する時間間隔を分単位で指定します。
pop3_limit [メールサイズの 上限]	0~4096 [1~4個の半角文 字:0~9]	4096	UTN サーバが許容する電子メールの最大サ イズを Kbyte 単位で設定します。 0 = 無制限
pop3_usr [ユーザ名]	最大 128 半角文字	[空白]	POP3 サーバにログインするために UTN サーバが使用するユーザ名を設定します。
pop3_pwd [パスワード]	最大 128 半角文字	[空白]	POP3 サーバにログインするために UTN サーバが使用するユーザパスワードを設定 します。

表22:パラメータリスト - SMTP (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
smtp_srv [サーバ名]	最大 128 半角文字	[空白]	SMTP サーバを IP アドレスまたはホスト名 で設定します。 ホスト名での指定は、DNS サーバが事前設 定されている場合にのみ可能です。
smtp_port [サーバポート]	1~65535 [1~5 個の半角文 字:0~9]	25	UTN サーバおよび SMTP サーバが通信に使 用するポートを指定します。 SMTP のデフォルトポート番号は 25 です。 SSL/TLS (パラメータ「SMTP – SSL/TLS」 \Rightarrow 121) に対して、SMTP は初期値でポート 587 (STARTSSL/STARTTLS) または以前のポート 465 (SMTPS) を使用します。必要に応じて、 SMTP サーバの説明書を参照してください。
smtp_ssl [SSL/TLS]	on/off	off	SSL/TLS を有効または無効にします。 SSL/TLS は UTN から SMTP サーバへの通信 を暗号化します。暗号強度は、暗号化プロ トコルと暗号化レベルで設定されます ⇔ ■46。
smtp_sender [送信者名]	最大 128 半角文字	[空白]	UTN サーバが電子メールの送信に使用する 電子メールアドレスを設定します。 多くの場合、送信者の名前と電子メールア カウントのユーザ名は同一になります。
smtp_auth [ログイン]	on/off	off	SNMP の認証 (SMTP AUTH) を有効または無 効にします。電子メールを送信する場合、 UTN は自己認証のために自らのユーザ名と パスワードを SMTP サーバに送信します。 ユーザ名 (パラメータ「SMTP - ユーザ名」
smtp_usr [ユーザ名]	最大 128 半角文字	[空白]	SMTP サーバにログインするために UTN サーバが使用するユーザ名を設定します。
smtp_pwd [パスワード]	最大 128 半角文字	[空白]	SMTP サーバへのログインに使用する UTN サーバのパスワードを設定します。
smtp_sign [セキュリティ (S/MIME)]	on/off	off	電子メールセキュリティ規格の S/MIME (Secure/Multipurpose Internet Mail Extensions)を、有効または無効にします。 S/MIME は、電子メールの署名 (パラメータ 「SMTP - 電子メールの署名」 \Rightarrow $@21$)または暗 号化 (パラメータ「SMTP - 完全な暗号化」 \Rightarrow @21)に使用します。対象の機能を (「SMTP - 公開キーの添付」 \Rightarrow $@21$ により)有効にしま す。

パラメータ	値	初期値	説明
smtp_attpkey [公開キーの添付]	on/off	on	公開キーを電子メールと一緒に送信します。 多くの電子メールクライアントが、電子 メールを表示するキーを必要とします。
smtp_encrypt [完全な暗号化] [電子メールの署名]	on/off	off	on = 電子メールの暗号化をアクティブにし ます。暗号化された電子メールは、対象の 受信者のみが開いて読むことができます。 暗号化には S/MIME 証明書が必要です ⇒ 1050。 off = 電子メールの署名をアクティブにしま す。受信者は、署名を使用して送信者の識 別情報をチェックできます。署名は電子 メールが改ざんされていないことを証明し ます。
			電子メールに署名を使用するには S/MIME 証 明書が必要です。⇔

表23: パラメータリスト - IPv4-VLAN (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
ip4vlan_mgmt [IPv4 管理 VLAN]	on/off	off	IPv4 管理 VLAN データの転送を、有効また は無効にします。 この設定を有効にした場合、SNMP は IPv4 管理 VLAN でのみ利用できます。
ip4vlan_mgmt_id [VLAN ID]	0~4096 [1桁から4桁の数 字:0~9]	0	IPv4 管理 VLAN を識別するための ID です。
ip4vlan_mgmt_any [任意の VLAN からの アクセス]	on/off	off	IPv4 クライアント VLAN を介した UTN サー バへの管理者アクセス (Web) を、有効また は無効にします。 この設定が有効な場合、UTN サーバはすべ ての VLAN を介して管理できます。
ip4vlan_mgmt_unta g [LAN からのアクセス (タグなし)]	on/off	on	タグなしの IPv4 パケットを介した UTN サー バへの管理者アクセスを、有効または無効 にします。この設定が無効な場合、UTN サーバは VLAN を介してのみ管理できます。
ipv4vlan_on_1 ~ ipv4vlan_on_20 [VLAN]	on/off	off	IPv4 クライアント VLAN データの転送を、 有効または無効にします。
ipv4vlan_addr_1 ~ ipv4vlan_addr_20 [IP アドレス]	有効な IP アドレス	192.168.0.0	IPv4 クライアント VLAN 内にある UTN サー バの IP アドレスです。
ipv4vlan_mask_1 ~ ipv4vlan_mask_20 [サブネットマスク]	有効な IP アドレス	255.255.255. 0	IPv4 クライアント VLAN 内にある UTN サー バのサブネットマスクです。
ip4vlan_gate_1 ~ ip4vlan_gate_20 [ゲートウェイ]	有効な IP アドレス	0.0.0.0	IPv4 管理 VLAN での IP ゲートウェイアドレ スゲートウェイにより、外部ネットワーク から IP アドレスを指定できます。
ipv4vlan_id_1 ~ ipv4vlan_id_20 [VLAN ID]	0~4096 [1~4 個の半角文 字:0~9]	0	IPv4 クライアント VLAN を識別するための ID です。
utn_2vlan_1 ~ utn_2vlan_20 [VLAN の割り当て]	0~9 [1桁の数字: 0~9]	0	USB ポートに VLAN を割り当てます。 0 = すべて 1 = VLAN 1 2 = VLAN 2 など 9 = なし

表24:パラメータリスト - WLAN (myUTN-55のみ)

パラメータ	値	初期値	説明
wif <u>i</u> mo de [モード]	adhoc infra	adhoc	 通信モード(ネットワークインフラストラ クチャ)を指定します。 アドホック:WLANは分散化されたアド ホックネットワークで、デバイスがお互 いに(ピアツーピアで)通信します。 インフラストラクチャ:WLANは、アク セスポイント/ルータが中央の通信ハブ として機能するインフラストラクチャ ネットワークです。アクセスポイント は、固定ネットワークにケーブル接続さ れています。
wif <u>in</u> a n e [ネットワーク名 (SSID)]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9、_、-]	SEH	SSID (Service Set Identife) としても知られ ている WLAN のネットワーク名を入力しま す。
wif <u>ic</u> hannel [チャンネル]	1~14 [1~2 個の半角文 字:0~9]	3	 WLAN のチャンネル(周波数範囲)を入力します。 (アドホックモードのみ) 警告 国から許可された WLAN チャンネルのみを使用してください。 UTN は、多くのチャンネルに対応するグローバルな製品です。 一方で、チャンネルは各国の法令によって規制されています。 したがって、UTN は使用する国で禁止されたチャンネルにも対応している場合があります。 国の規制には、各自が注意してください。
wif <u>ie</u> ncrypt [暗号化方式]	 WepOpen WepShared TKIP AES TKIP2 AES2 AESTKIP AESTKIP2 Auto		WLAN を保護する暗号化方式を選択します。 =なし WepOpen = WEP(オープンシステム) WepShared = WEP(共有キー) TKIP = WPA(TKIP) AES = WPA(AES) TKIP2 = WPA2(TKIP) AES2 = WPA2(AES) AESTKIP = WPA(AES/TKIP) AESTKIP2 = WPA2(AES/TKIP) Auto = WPA(自動)

パラメータ	値	初期値	説明
wif <u>ik</u> eyi d [WEP キーを使用]	0~4 [1桁の数字: 0~4]	0	使用する WEP キーを指定します。 0=キーなし 1=キー1 2=キー2 3=キー3 4=キー4
wif <u>i</u> vk ey1 \sim wif <u>i</u> vk ey4 [$\neq -1 \sim 4$]	キーの種類により 異なります。 文字数: 64 ASCII=5 64 HEX = 10 128 ASCII= 13 128 HEX= 26 文字セット: $16 進数 = 0 \sim 9$ 、 $a \sim f$ 、 $A \sim F$ ASCII = 0 ~ 9、a ~ z、 $A \sim Z$	[空白]	 WEP キーを指定します。4つの WEP キーが利用できます。 重要: WEP には 16 進数キーを使用することを推奨します。 アクセスポイント / ルータによっては、ASCII フォーマットのWEP キーを 16 進数フォーマットへ変換します。この場合は、UTN サーバ上の ASCII キーとアクセスポイント / ルータ上の 16 進数が一致しません。
wifi॒ps k [PSK]	8~63 個の半角 文字	[空白]	WPA (Wi-Fi Protected Access) 用の PSK (Pre Shared Key) を指定します。
wif <u>ir</u> caming [ローミング]	on/off	off	ローミング(アクセスポイント/ルータの切り替え)を、有効または無効にします。複数の(同一設定の)アクセスポイント/ルータがある広域に跨るWLANでUTNサーバの位置を変更すると、ローミングがアクティブな場合に、UTNサーバは接続ロスのない良好な信号へと自動的に切り替わります。 (インフラストラクチャモードのみ)

表25:パラメータリスト-日付/時間

パラメータ	値	初期値	説明
ntp [日付 / 時間]	on/off	on	タイムサーバ (SNTP) の使用を、有効または 無効にします。
ntp_server [タイムサーバ]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	pool.ntp.org	タイムサーバを IP アドレスまたはホスト名 で指定します。 ホスト名での指定は、DNS サーバがあらか じめ設定されている場合にのみ可能です。 重要: 適切に設定されたネットワーク 上で、UTN サーバはタイムサー バ設定を DHCP により自動的に 受信します。自動的に割り当て られたタイムサーバは、手動設 定より常に優先されます。
ntp_tzone [タイムゾーン]	UTC、GMT、EST、 EDT、CST、CDT、 MST、MDT、PST、 PDT など。	CET/CEST (EU)	協定世界時 (UTC) を、地域および国独自の制度 (夏時間など)に従い補正します。

表26:パラメータリスト - 説明

パラメータ	値	初期値	説明
sys_name [ホスト名]	最大 64 半角文字 [a~z、A~Z、 0~9]	[空白]	IP アドレスに代わるデバイス名。名前により、例えば複数の UTN サーバを使用している場合、ネットワーク上で UTN サーバを容易に識別できます。 myUTN Control Center および SEH UTN Manager に表示されます。
sys_descr [説明]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	場所や所属部門などのデバイスの説明。 myUTN Control Center および SEH UTN Manager に表示されます。
sys_contact [担当者]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	デバイス管理者などの担当者。 myUTN Control Center に表示されます。

表27:パラメータリスト - USB ポート

パラメータ	値	初期値	説明
utn_tag_1 ~ utn_tag_20 [ポート名]	最大 32 半角文字 [a~z、A~Z、 0 ~ 9]	[空白]	USB ポートの名前を任意で入力します。
utn_pof <u>f</u> 1 ~ utn_pof <u>f</u> 20 [ポート]	on/off	off	USB ポート (ポートに接続された USB デバ イス) への電源供給を、無効または有効にし ます。 off= 電源有効 on = 電源無効

表28:パラメータリスト - UTN ポート

パラメータ	値	初期値	説明
utn_port [UTN ポート]	1~9200 [1~4 個の半角文 字:0~9]	9200	UTN ポート (暗号化接続用)の数を指定しま す。
utn_sslport [UTN SSL ポート]	1~9443 [1~4 個の半角文 字:0~9]	9443	UTN SSL ポート (暗号化接続用)の数を指定 します。

表29:パラメータリスト - 通知 (myUTN-80 以降のみ)					
パラメータ	値	初期値	説明		
mailto_1 mailto_2 [電子メールアド レス]	有効な電子メール アドレス 最大 64 半角文字	[空白]	通知の受信者の電子メールアドレスを設定 します。		
noti_stat_1 noti_stat_2 [ステータス通知]	on/off	off	受信者1または2への定期的なステータス 通知を、有効または無効にします。		
notistat_d [間隔]	al su mo tu we th fr sa	al	ステータス通知を送信する日(間隔)を指定 します。 al=毎日 su=日曜日 mo=月曜日 tu=火曜日 we=水曜日 th=木曜日 fr=金曜日 sa=土曜日		
notistat_h [時]	0~23 [1~2個の半角文 字:0~9]	0	ステータス通知を送信する時(時間)を指定 します。 1=1時間 2=2時間 3=3時間 など		
notistat_tm [分]	0~5 [1桁の数字: 0~5]	0	ステータス通知を送信する時(分)を指定し ます。 0=00分 1=10分 2=20分 3=30分 4=40分 5=50分		
noti_dev_1 noti_dev_2 [USB デバイスが接続 または切断された場 合に電子メールを送 信]	on/off	off	USB デバイスが UTN サーバに接続された後、 または UTN サーバから取り外された後の電 子メール通知を、有効または無効にします。		
noti_act_1 noti_act_2 [USB ポートがアク ティブまたは非アク ティブになったとき に電子メールを送信]	on/off	off	USB ポート (すなわち接続された USB デバ イスへの接続) がアクティブまたは非アク ティブになった後の電子メール通知を、有 効または無効にします。		

80

ny	yUTN	ユーザ	ーマニ	ュアル	レ macOS	
----	------	-----	-----	-----	---------	--

パラメータ	値	初期値	説明
noti_pup_1 noti_pup_2 [UTN サーバが再起動 した場合に電子メー ルを送信]	on/off	off	UTN サーバが再起動したときの電子メール 通知を、有効または無効にします。
noti_pwr_1 noti_pwr_2 [電源が遮断または接 続されたときに電子 メールを送信]	on/off	off	UTN サーバの 2 つの電源のうち 1 つが遮断 または接続されたときの電子メール通知を、 有効または無効にします。 (myUTN-800 のみ)
noti_lnk_1 noti_lnk_2 [ネットワーク接続が 遮断または確立され たときに電子メール を送信]	on/off	off	UTN サーバの 2 つのネットワーク接続のうち 1 つが遮断または接続されたときの電子 メール通知を、有効または無効にします。 (myUTN-800 のみ)
noti_sdinout_1 noti_sdinout_2 [SD カードが接続ま たは切断されたとき に電子メールを送信]	on/off	off	SD カードが UTN サーバに接続された後、ま たは UTN サーバから取り外された後の電子 メール通知を、有効または無効にします。 (myUTN-800 のみ)
noti_sdunusable_1 noti_sdunusable_2 [SD カードが使用で きないときに電子 メールを送信]	on/off	off	SD カードが使用できない場合の電子メール 通知を、有効または無効にします。 (myUTN-800 のみ)
trapto_1 trapto_2 [アドレス]	有効な IP アドレス	0.0.0.0	受信者の SNMP トラップアドレスです。
trapcommu_1 trapcommu_2 [コミュニティ]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	public	受信者の SNMP トラップコミュニティです。
trapdev [USB デバイスが接続 または切断されたと きにトラップを送信]	on/off	off	USB デバイスが UTN サーバに接続された後、 または UTN サーバから取り外された後の SNMP トラップ通知を、有効または無効にし ます。
trapact [USB ポートがアク ティブまたは非アク ティブになったとき にトラップを送信]	on/off	off	USB ポート (接続された USB デバイスへの 接続など) がアクティブまたは非アクティブ になった後の SNMP トラップ通知を、有効 または無効にします。

パラメータ	値	初期値	説明
trappup [UTN サーバが再起動 した場合にトラップ を送信]	on/off	off	UTN サーバが再起動したときの SNMP ト ラップの送信を、有効または無効にします。
trap_pwr [電源が切断または接 続されたときにト ラップを送信]	on/off	off	UTN サーバの 2 つの電源のうち 1 つが遮断 または接続されたときの SNMP トラップ通 知を、有効または無効にします。 (myUTN-800 のみ)
trap_lnk [ネットワーク接続が 遮断または確立され たときにトラップを 送信]	on/off	off	UTN サーバの 2 つのネットワーク接続のう ち1 つが遮断または接続されたときの SNMP トラップ通知を、有効または無効にします。 (myUTN-800 のみ)
trap_sdinout [SD カードが接続ま たは切断されたとき にトラップを送信]	on/off	off	SD カードが UTN サーバに接続された後、ま たは UTN サーバから取り外された後の SNMP トラップ通知を、有効または無効にし ます。 (myUTN-800のみ)
trap_sdunusable [SD カードが使用で きないときにトラッ プを送信]	on/off	off	SD カードが使用できない場合の SNMP ト ラップ送信を、有効または無効にします。 (myUTN-800 のみ)

表30:パラメータリスト – ディスプレイ (myUTN-800のみ)

パラメータ	値	初期値	説明
dis_def [識別子 (ディスプレ イパネル)]	1~2個の半角文 字 [A-Z、0-9、E+数 字の組合せは、エ ラーに使用するの で、指定できませ ん ⇔ ≧28。]	SD	UTN サーバの前面のディスプレイパネルに 表示される名前 (ID) を設定します。
dis_pwr [1 個の電源だけが電 力を供給していると きにエラーを表示]	on/off	on	2 つの電源のうち1 つだけが、UTN サーバに 電力を供給しているときにディスプレイパ ネルに表示するエラーを、有効または無効 にします。 エラーはコードで表示されます ⇔ ■28。
disp_sdc [SD カードのエラー を表示]	on/off	on	UTN サーバに SD カードが挿入されていな い、または SD カードが使用できないとき にディスプレイパネルに表示するエラー メッセージを、有効または無効にします。 エラーはコードで表示されます → ■28。
disp_lnk [1 つのネットワーク 接続のみが確立され たときにエラーを表 示]	on/off	on	UTN サーバの2つのネットワーク接続の うち 1 つのみが確立されたときにディス プレイパネルに表示されるエラーメッセー ジを、有効または無効にします。 エラーはコードで表示されます ⇔ ■28。

表31:パラメータリスト - 音響信号 (myUTN-800のみ)

パラメータ	値	初期値	説明
beepPwr [1 個の電源のみが電 力を供給]	on/off	off	UTN サーバに 2 つの電源のうち1つの みが電源を供給しているときに発信される 音響信号を、有効または無効にします。
beepSDc [SD カードエラー]	on/off	off	UTN サーバに挿入された SD カードがな い、または SD カードが使用できないとき に発信される音響信号を、有効または無効 にします。
beepLnk [1 つのネットワーク 接続のみが確立]	on/off	off	UTN サーバの2つのネットワーク接続の うち 1 つのみが確立したときに発信され る音響信号を、有効または無効にします。

表32:パラメータリスト - SSL/TLS 接続

パラメータ	値	初期値	説明
sslmethod [暗号化プロトコル]	any sslv3 tls10 tls11 tls12	any	<pre>SSL/TLS 接続に使用する暗号化プロトコルを 指定します。 any = 任意(自動ネゴシエーション) sslv3 = SSL 3.0 tls10 = TLS 1.0 tls11 = TLS 1.1 tls12 = TLS 1.2</pre>
セキュリティ [暗号化レベル]	1~4 [1桁の数字: 1~4]	4	 SSL/TLS 接続に使用する暗号化レベルを指定します。 1 = low(低) 2 = medium(中) 3 = high(高) 4 = any(自動ネゴシエーション) 警告 現在のブラウザは、低レベルの暗号スイートに対応していません。現在のブラウザとHTTPSのみの設定でmyUTN Control Center(⇔ ■45)へのアクセスに低レベルを使用すると、接続は確立できません。 できる限り高い暗号化レベルを使用してください。
			警告 SEH UTN Manager は、低暗号化 レベルに対応していません。暗 号化した USB 接続との組合せで 低レベルをセットアップすると、 接続を確立することができません。 できる限り高い暗号化レベルを 使用してください。

myUTN ユー†	デーマニュアル macOS
-----------	---------------

表33:パラメータリスト - myUTN Control Center セキュリティ

パラメータ	値	初期値	説明
http_allowed [接続]	on/off	on	myUTN Control Center への接続に使用する 接続タイプ (HTTP/HTTPS) を指定します。 on = HTTP/HTTPS off= HTPS のみ 暗号強度は、暗号化プロトコルと暗号化レ ベルで設定されます。 $= 46$ 。 警告 現在のブラウザは低レベルのセ キュリティ設定に対応していま せん。低レベル設定では接続を 確立できません。 次の組合せは使用しないでくだ さい:暗号化プロトコルHTTPS と低暗号化レベル。 接続が確立すると、UTN サーバの識別情報 が検証されます。そのために、クライアン トはブラウザから証明書を要求します ($=$))。証明書はブラウザが承認できる必要 があります。ブラウザソフトウェアの説明 書を参照してください。
sessKeys [Control Center への アクセス制限]	on/off	off	 myUTN Control Center のユーザアカウント を、有効または無効にします。有効の場合 は、myUTN Control Center が起動するとき にログイン画面が表示されます。 重要: ユーザアカウント(ユーザ名お よびパスワード)を設定します。
admin_name [管理者 - ユーザ名]	最大 64 半角文字 [a~z、A~Z、 0~9]	admin	管理者ユーザアカウント用のユーザ名を設 定します。 重要: SNMPv3 admin アカウントの ユーザ名も設定します ⇔ ■18。
admin_pwd [管理者 - パスワード]	8~64個の半角文 字 [a~z、A~Z、 0~9]	administrator	管理者ユーザアカウント用のパスワードを 設定します。 重要: SNMPv3 admin アカウントのパ スワードも設定します ⇔ ■18。
any_name [読み取り専用ユ ーザ - ユーザ名]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	anonymous	読み取り専用ユーザアカウント用のユーザ 名を設定します。 重要: SNMPv3 ユーザアカウントの ユーザ名も設定します⇔ ■18。

パラメータ	値	初期値	説明
any_pwd [読み取り専用ユ ーザ - パスワード]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	読み取り専用ユーザアカウント用のパス ワードを設定します。 重要: SNMPv3 ユーザアカウントのパ スワードも設定します⇔ ■18。
sessKeyUList [ログイン画面の 表示]	on/off	on	ログイン画面の種類を設定します。 on=ユーザリストを表示します。パスワー ド入力のみが必要になります。 off=ニュートラルなログイン画面で、ユー ザ名とパスワードの入力が必要です。
sessKeyTimer [セッションタイムア ウト]	on/off	on	セッションタイムアウトを有効または無効 にします。
sessKeyTimeout [セッションタイムア ウト]	120~3600 [3~4個の半角文 字:0~9]	600	タイムアウトが有効になるまでの時間 (秒単 位)。

表34:パラメータリスト - TCP ポートアクセス

パラメータ	値	初期値	説明
protection [ポートアクセス 制御]	on/off	off	選択されたポートの UTN サーバなどへの接 続のブロッキングを、有効または無効にし ます。
protection_level [セキュリティレ ベル]	protec_utn protec_tcp protec_all	protec_utn	ブロックするポートタイプを指定します。 protec_utn= UTN アクセス (UTN ポート) protec_tcp= TCP アクセス (TCP ポート: HTTP/HTTPS/UTN) protec_all= すべてのポート (IP ポート)
ip_flter_on_1 ~ ip_flter_on_8 [IP アドレス]	on/off	off	ポートロックの例外を、有効または無効に します。
ip_flter_1 ~ ip_flter_8 [IP アドレス]	有効な IP アドレス	[空白]	ポートブロックから除外するネットワーク 構成要素を IP アドレスで指定します。 重要: ワイルドカード (*) を使用する と、サブネットワークを指定で きます。
hw_fiter_on_1 ~ hw_fiter_on_8 [MAC アドレス]	on/off	off	ポートロックの例外を、有効または無効に します。
hw_flter_1 ~ hw_flter_8 [MAC アドレス]	有効なハードウェ アアドレス	00:00:00:00: 00:00	ポートロックの対象から除外する要素を、 MAC アドレス (ハードウェアアドレス)を 使用して指定します。 重要: MAC アドレスはルータを通して 配信されません。
protection_test [テストモード]	on/off	on	テストモードを有効または無効します。 警告 テストモードでは、設定をテストするときにユーザ自身は除外されないように、初期値でアクティブに設定されています。 UTN が再起動するまで設定はアクティブになり、以降のアクセスは制限されません。 設定のテストが正常に終了後、アクセス制御が正式に設定されるように、テストモードを非アクティブにする必要があります。

表35:パラメータリスト - USB 接続の暗号化

パラメータ	値	初期値	説明
utn_sec_1 ~ utn_sec_20 [USB ポート]	on/off	off	USB ポート (USB デバイスなど) とクライア ント間の接続の SSL/TLS 暗号化を、有効ま たは無効にします。 重要: ペイロードのみが暗号化されま す。管理データおよびログデー タは、暗号化せずに送信されま す。

表36:パラメータリスト - USB デバイス種類のブロッキング

パラメータ	値	初期値	説明
utn_hid [入力デバイス (HID クラス) を無効にす る]	on/off	on	入力デバイス (HID - ヒューマンインター フェイスデバイス) のブロッキングをアク ティブまたは非アクティブにします。 on = ブロッキング無効

表37: パラメータリスト - IPv4-VLAN (myUTN-80 以降のみ)

パラメータ	値	初期値	説明
utn_accctrt_1 ~ utn_accctrt_20 [方法]	 ids key keyids		USB ポートと、ポートに接続された USB デ バイスへのアクセスおよび使用を制限する 方法を指定します。 = 制限なし ids= デバイス割り当て key= ポートキー制御 keyids= デバイス割り当て、およびキー制御
utn_keyval_1 ~ utn_keyval_20 [≠—]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	ポートキー制御を使用するときの、USB お よび接続された USB デバイスのキーを設定 します。
utn_vendprodIDs_1 ~ utn_vendprodIDs_20			デバイス割り当てにより USB ポートに割り 当てられた USB デバイスの VID (ベンダ ID) と PID (製品 ID) を指定します。
[USB デバイス]			USB デバイスの VID および PID は不明 な場合が多いため、myUTN Control Center を使用することを推奨します。 m y UTN Control Center を使用する と VID および PID が自動的に検出され 入力されます。

表38:パラメータリスト - 認証

パラメータ	値	初期値	説明
auth_typ [認証方式]	 MD5 TLS TTLS PEAP FAST		UTN サーバが参加するネットワーク内で使 用される認証方式を設定します。 = なし MD5 = EAP-MD5 TLS = EAP-TLS TTLS = EAP-TTLS PEAP = PEAP FAST = EAP-FAST
auth_name [ユーザ名]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	RADIUS サーバ上で、EAP 認証方式の MD5、 TTLS、PEAP および FAST 用に UTN サーバを 設定するために使用するユーザ名を設定し ます。
auth_pwd [パスワード]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	RADIUS サーバ上で、EAP 認証方式の MD5、 TTLS、PEAP および FAST 用に UTN サーバを 設定するために使用するパスワードを設定 します。
auth_intern [内部認証]	 PAP CHAP MSCHAP2 EMD5 ETLS		EAP 認証方式の TTLS、PEAP および FAST に 使用する内部認証の種類を指定します。 =なし PAP = PAP CHAP = CHAP MSCHAP2 = MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS
auth_extern [PEAP/EAP-FAST オプション]	PLABELO PLABEL PVERO PVER1 FPROV1		EAP 認証方式の TTLS、PEAP および FAST に 使用する外部認証の種類を指定します。 = なし PLABEL0 = PEAPLABEL0 PLABEL1 = PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1 = FASTPROV1
auth_ano_name [匿名の名前]	最大 64 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	EAP 認証方式の TTLS、PEAP および FAST の 非暗号化部分に使用する匿名の名前を指定 します。
auth_wpa_addon [WPAアドオン]	最大 255 半角文字 [a ~ z、A ~ Z、 0 ~ 9]	[空白]	EAP 認証方式の TTLS、PEAP および FAST に 使用する WPA 拡張を任意で指定します。

表39: パラメータリスト – バックアップ (myUTN-800のみ)

パラメータ	値	初期値	説明
autoSync [パラメータのバック アップ]	on/off	on	パラメータ値、パスワードおよび証明書の、 接続された SD カードへの自動バックアップ を、有効または無効にします。

表40: パラメータリスト - その他

パラメータ	値	初期値	説明	
utn_heartbeat	1~1800 [1桁から4桁の数 字:0~9]	180		警告 このパラメータを使用するには、 必ず SEH のサポートチームに相 談してください。
utn_pof t ur a_1 ~ utn_pof t ur a_20	0~100 [1~3 個の半角文 字:0~9]	0		警告 このパラメータを使用するには、 必ず SEH のサポートチームに相 談してください。
utn_prereset_1 ~ utn_prereset_20	on/off	off		警告 このパラメータを使用するには、 必ず SEH のサポートチームに相 談してください。

8.4 SEH UTN Manager – 機能の概要

SEH UTN Manager で非アクティブになる (グレイアウトされる)機能は、次の様々な要因で決定されます。

- 選択リストモード
 - グローバル
 - ユーザ
- ・ クライアントのオペレーティングシステム (Windows、macOS、Linux)
- クライアントユーザアカウント
 - 管理者
 - 標準ユーザ
- *.ini ファイル(選択リスト)への書き込み権限



管理者は、ユーザに個別の機能を提供する際に、こうした要因を使用でき ます。

次の表に概略を示します。表に基本的に利用できる機能を示しています。また次の理由で、個別の機能 が表示されない、または非アクティブとして表示されます。

- ・ UTN サーバがその機能に対応していない
- ・ 接続された USB デバイスがその機能に対応していない
- ・ セキュリティ対策が実装されている

表41:SEH UTN Manager - 機能の概要、macOS

	グローバル 選択リスト		ユーザ選択リスト		
	管理者	ユーザ	管理者	ユーザ (読 み取り / 書 き込み *.ini)	ユーザ (読み取り / 書き込みな し *.ini)
メニュー					
選択リスト - 編集	\checkmark	×	\checkmark	\checkmark	×
選択リスト - エクスポート	\checkmark	x	\checkmark	×	×
選択リスト - リフレッシュ	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
UTN サーバ - 構成	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
UTN サーバ - IP アドレスの設定	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
UTN サーバ - 自動接続の有効化	\checkmark	x	\checkmark	×	×
UTN サーバ - USB ポートキーの設定	\checkmark	x	\checkmark	\checkmark	×
UTN サーバ - 追加	\checkmark	x	\checkmark	\checkmark	×
UTN サーバ - 削除	\checkmark	x	\checkmark	\checkmark	×
UTN サーバ - リフレッシュ	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
ポート - 有効化	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
ポート - 無効化	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
ポート - リクエスト	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
ポート - 削除	\checkmark	×	\checkmark	×	×
ポート - UTN アクションの作成	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark
ポート - 設定	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark

myUTN ユーザー	マニュアル macOS
------------	-------------

- L.	15		
74			
- T	-		
		-	

	グロ- 選択!	ーバル ノスト	ユーザ選択リスト			
	管理者	ユーザ	管理者	ユーザ (読 み取り / 書 き込み *.ini)	ユーザ (読み取り / 書き込みな し *.ini)	
ボタン						
選択リスト - リフレッシュ	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	
選択リスト - 編集	\checkmark	×	\checkmark	\checkmark	×	
ポート - 有効化	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	
ポート - 無効化	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	
「プログラム - オプション」ダイアログ	「プログラム‐オプション」ダイアログ					
ネットワークスキャン - マルチキャス ト検索	\checkmark	×	\checkmark	×	×	
ネットワークスキャン - IP 範囲検索	\checkmark	×	\checkmark	×	×	
プログラム - プログラムの更新	\checkmark	×	\checkmark	×	×	
自動操作 - プログラムの開始 (自動起動)	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	
自動操作 - 自動切断	\checkmark	×	\checkmark	×	×	
選択リスト - 選択リストモード	\checkmark	×	\checkmark	×	×	
選択リスト - 自動リフレッシュ	\checkmark	×	\checkmark	×	×	
「ポートの設定」ダイアログ						
デバイスの自動接続 - オンデマンド印刷	\checkmark	×	\checkmark	×	×	
プラグインモード	\checkmark	×	\checkmark	x	×	