



# USB デバイスサーバ

myUTN-50

myUTN-52

myUTN-54

dongleサーバ myUTN-80

SDCardserver myUTN-120

Scannerserver myUTN-130

myUTN-150



# ユーザーマニュアル

製造元：  
SEH Computertechnik GmbH  
Suedring 11  
33647 Bielefeld  
Germany  
電話：+49 (0)521 94226-29  
FAX: +49 (0)521 94226-99  
サポート：+49 (0)521 94226-44  
(日本) 0570-02-3666  
電子メール：info@seh.de  
Web サイト：http://www.seh-technology.jp



この QR コード (meCard) をスマートフォンで読み取ってください。

文書：  
種類：ユーザーマニュアル  
タイトル：USB デバイスサーバ  
バージョン：2.0

### 重要な Web サイトへのリンク：

保証延長について：<http://www.seh-technology.jp/guarantee>  
サポートに関するお問い合わせ & インフォメーション：<http://www.seh-technology.jp/support>  
販売に関するお問い合わせ & インフォメーション：<http://www.seh-technology.jp/sales>  
ダウンロード：<http://www.seh-technology.jp/services/downloads/myutn.html>

InterCon は SEH Computertechnik GmbH の登録商標です。

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、万一誤りを見つげられた場合には、上記に記載されている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。

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。

© 2013 SEH Computertechnik GmbH

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

# 目次

<b>1 一般情報</b> .....	<b>5</b>
1.1 myUTN .....	6
1.2 説明書 .....	7
1.3 サポートとサービス .....	10
1.4 安全の確保 .....	11
1.5 最初のステップ .....	12
1.6 IP アドレスの UTN サーバへの保存 .....	13
<b>2 管理方法</b> .....	<b>17</b>
2.1 myUTN Control Center による管理 .....	17
2.2 SEH UTN Manager による管理 .....	19
2.3 InterCon-NetTool による管理 .....	26
2.4 電子メールによる管理 (myUTN-80 以降のみ) .....	28
2.5 デバイスのステータスボタンによる管理 .....	30
<b>3 ネットワーク設定</b> .....	<b>31</b>
3.1 IPv4 パラメータの設定方法 .....	31
3.2 IPv6 パラメータの設定方法 .....	34
3.3 DNS の設定方法 .....	36
3.4 SNMP の設定方法 .....	37
3.5 Bonjour の設定方法 .....	38
3.6 POP3 と SMTP の設定方法 (myUTN-80 以降のみ) .....	39
3.7 WLAN の設定方法 (myUTN-54 のみ) .....	42
<b>4 デバイス設定</b> .....	<b>47</b>
4.1 説明を設定する方法 .....	48
4.2 デバイス時間の設定方法 .....	48
4.3 UTN (SSL) ポートの設定方法 .....	49
4.4 USB デバイスに名前を割り当てる方法 .....	50
4.5 USB ポートの電源を制御する方法 (myUTN-80 以降のみ) .....	50
4.6 USB スキャナのデータストリームを圧縮する方法 (myUTN-130 のみ) .....	51
4.7 通知サービスの利用方法 (myUTN-80 以降のみ) .....	52
4.8 ドングルで保護されたソフトウェアへのアクセス (myUTN-80 のみ) または USB デバイスへのアクセス (myUTN-150 のみ) を VLAN で管理する方法 .....	54

<b>5 SEH UTN Manager の操作</b> .....	<b>56</b>
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 .....	57
5.2 USB デバイスを選択リストに追加する方法 .....	58
5.3 USB デバイスをクライアントに接続する方法 .....	59
5.4 USB デバイスとクライアント間の接続を解除する方法 .....	60
5.5 使用中のデバイスを要求する方法 .....	61
5.6 デバイス接続とプログラムの開始を自動化する方法 .....	62
5.7 USB デバイスに関する情報を取得する方法 .....	67
5.8 複数の参加者用の選択リストを管理する方法 .....	68
<b>6 セキュリティ</b> .....	<b>73</b>
6.1 SSL/TLS 接続の暗号化レベルを設定する方法 .....	73
6.2 myUTN Control Center へのアクセスを制御する方法 .....	75
6.3 UTN サーバへのアクセスを制御する方法 (TCP ポートアクセス制御) .....	77
6.4 USB デバイスへのアクセスを制御する方法 (myUTN-80 以降のみ) .....	79
6.5 証明書の正しい使用方法 .....	82
6.6 認証方法を使用する方法 .....	88
6.7 データ転送を暗号化する方法 .....	94
<b>7 メンテナンス</b> .....	<b>96</b>
7.1 UTN パラメータを保護する方法 (バックアップ) .....	97
7.2 UTN パラメータを初期設定値にリセットする方法 .....	98
7.3 更新 (アップデート) の実行方法 .....	101
7.4 UTN サーバを再起動する方法 .....	102
<b>8 付録</b> .....	<b>103</b>
8.1 用語集 .....	103
8.2 パラメータリスト .....	106
8.3 LED 表示 .....	123
8.4 SEH UTN Manager - 機能の概要 .....	124
8.5 トラブルシューティング .....	127
8.6 付加ツール「utnm」 .....	131
8.7 図リスト .....	136

# 1 一般情報



この章では、デバイスおよび付属の説明書、また安全上の注意について説明します。  
UTN サーバを有効に使用方法やデバイスの正しい操作方法を確認できます。

## 必要な情報

- 「myUTN」 ⇨ 6
- 「説明書」 ⇨ 7
- 「サポートとサービス」 ⇨ 10
- 「安全の確保」 ⇨ 11
- 「最初のステップ」 ⇨ 12
- 「IP アドレスの UTN サーバへの保存」 ⇨ 13

## 1.1 myUTN

### 目的

myUTN (myUSB to Network) は、ネットワーク非対応の USB デバイス (ハードディスク、プリンタなど) を、ネットワーク経由でアクセス可能にします。USB デバイスは、UTN サーバの USB ポートに接続します。



「ドングルサーバ」 (myUTN-80) は、USB ドングル専用に設計されました。



「Scannerserver」 (myUTN-130) は、USB スキャナ専用に設計されました。

「SEH UTN Manager」は、USB デバイスのアクセスを管理するソフトウェアツールです。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、すべてのクライアントにインストールします。SEH UTN Manager は、ネットワーク内に存在する、使用可能なすべての USB デバイスを表示し、クライアントと USB デバイスとの接続を確立します。

### システム要件

myUTN は、TCP/IP ベースのネットワークで使用できます。SEH UTN Manager は、次のシステムで使用するために設計されました。

- Windows XP 以降
- Mac OS X 10.6.x、Mac OS X 10.7.x (64-bit)、OS X 10.8.x

### 手順と基本機能

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の範囲は任意に設定できます。検出されたすべての UTN サーバは、接続されているデバイスとともにネットワークリストに表示されます。必要なデバイスが選択され、選択リストに追加されます。選択リストのデバイスは、クライアントに接続できます。

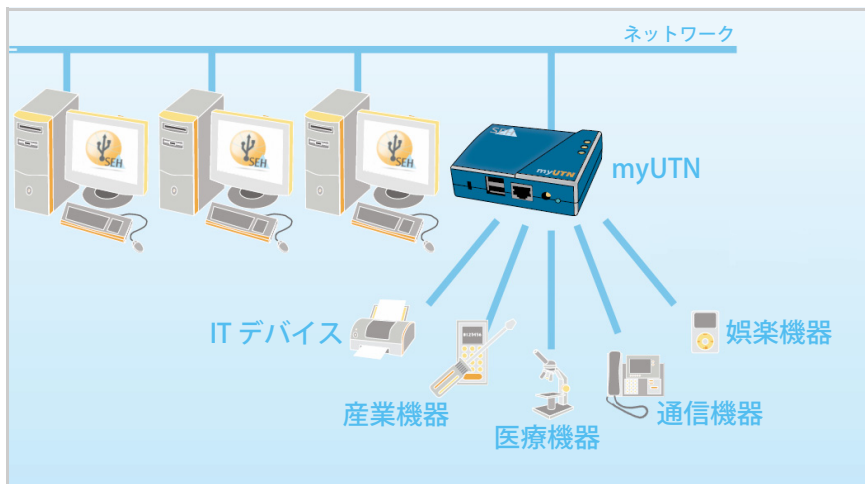


図 1：ネットワーク内の UTN サーバ

## 1.2 説明書

### 適用範囲と内容

本書は、いくつかのバージョンの USB Deviceserver と Dongle Server、Scanner Server、また SDCardserver について記載しています。そのため、記載されている機能が、お使いの製品に対応しない場合があります。また、表示されているイラストとお使いのデバイスが異なる場合があります。

お使いの製品が対応する機能については、UTN サーバ各モデルのデータシートを参照してください。この説明書で使用する製品カテゴリ名は、次の通りです。

- USB Deviceserver → UTN サーバ
- Dongle Server → UTN サーバ
- Scanner Server → UTN サーバ
- SDCardserver → UTN サーバ
- Dongle → USB デバイス
- SD カードリーダー → USB デバイス
- USB スキャナ → USB デバイス

## 説明書の構成

myUTN の説明書は、次のように構成されています。



PDF

**ユーザーマニュアル**

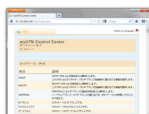
myUTN の設定および管理について詳細に説明しています。



印刷された PDF

**クイック・インストール案内**

セキュリティ、ハードウェアの設定、および初期操作の手順について説明しています。



HTML

**オンラインヘルプ (myUTN Control Center)**

「myUTN Control Center」の使用方法について、詳しく説明しています。



HTML

**オンラインヘルプ (SEH UTN Manager)**

ソフトウェアツール「SEH UTN Manager」の使用方法について、詳しく説明しています。

## 説明書の特長

この説明書は、モニタで参照できる電子文書として作成されています。多くのプログラム（例：Adobe® Reader®）が備えているブックマークナビゲーション機能を使用して、文書構造の全体を参照できます。

また、関連情報へのハイパーリンクも設定されています。印刷する場合は、プリンタの設定を「両面印刷」または「小冊子印刷」にしておくことをお奨めします。

この文書で使用される  
専門用語







この文書で使用される技術用語は、用語集で説明されています。用語集には、技術情報やバックグラウンド情報の概要が記載されています。⇒ 103 を参照してください。



## 記号と表記規則

本書では、様々な記号が使用されます。それらの意味について、次の表に一覧表示します。

表 1：説明書内の表記規則

記号 / 表記規則	説明
 <b>警告</b>	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。
 <b>注意</b>	注意には、細心の注意が必要な情報が含まれます。
 <b>手順</b> 1. 記号	「手」の記号は、操作手順の始まりを示します。各手順がその後が続いて説明されます。
 <b>確認</b>	矢印の記号は、操作結果について確認します。
<input checked="" type="checkbox"/> <b>必要事項</b>	チェック記号は、操作を始める前に準備が必要な要件を示します。
<input type="checkbox"/> <b>オプション</b>	四角の記号は、手順と選択可能なオプションを示します。
•	中点は、箇条書き表示で使われます。
	各章の要約を示します。
⇒ 	文書内の参照するページを示します。PDFファイルでは、この記号をクリックするとそのページにジャンプできます。
<b>太字</b>	ボタンやメニュー項目などの製品の用語は、太字で表記されます。
<code>Courier</code>	コマンドライン（半角アルファベットの部分のみ）は Courier フォントで表記されます。
「固有名詞」	固有名詞はかぎ括弧「」で表記されます。

## サポート

## 1.3 サポートとサービス

問題が解決されない場合は、ホットラインに問い合わせてください。SEH Computertechnik GmbH では幅広いサポートを実施しています。



午前 9 : 00 ~ 午後 6 : 00 月~金曜日 (祝日を除く)



0570-02-3666



support@seh-technology.jp

## 最新のサービス

SEH Computertechnik GmbH のホームページ <http://www.seh-technology.jp/> では、次のようなサービスを提供しています。



- 最新のファームウェア / ソフトウェア
- 最新のツール
- 最新の説明書
- 最新の製品情報
- 製品データシート
- その他多数

## 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ている安全規定および警告は、すべて読んで遵守してください。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。

安全規定と警告を遵守しなかったために生じた、人体の損傷や財産の損害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、保証に関する申し立ては無効となります。

目的用途	UTN サーバは TCP/IP ネットワークで使用できます。myUTN を使うと、ネットワーク非対応の USB デバイスに、ネットワークを経由してアクセスできます。UTN サーバはオフィス環境向けに設計されています。
不正使用	この説明書に記載されている myUTN の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。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。
安全規定	UTN サーバの初期操作を開始する前に、クイック・インストール案内の安全規定に留意してください。クイック・インストール案内はパッケージに同梱されています。
警告	本書中に記載されている、すべての警告を読んで遵守してください。警告は、危険だと思われる操作説明の箇所に、次のように表記されています。



---

**警告!**

---

## 1.5 最初のステップ

この節では、迅速な操作準備に必要な情報を説明します。

### 手順

1. 人体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んで遵守ください。⇒[11](#)を参照してください。
  2. ハードウェア設定を実行します。ハードウェア設定では、UTN サーバをネットワーク、USB デバイス、電源に接続します。「クイック・インストール案内」を参照してください。
  3. IP アドレスが UTN サーバに保存されていることを確認します。⇒[13](#)を参照してください。
  4. ソフトウェアツール SEH UTN Manager をクライアントにインストールして起動します。⇒[19](#)を参照してください。
  5. 使用するデバイスが選択リストに追加されます。⇒[58](#)を参照してください。
  6. クライアントと USB デバイスとの接続をアクティブにします。⇒[59](#)を参照してください。
- ☞ 接続が確立され、クライアントが USB デバイスを使用できるようになります。

## 1.6 IP アドレスの UTN サーバへの保存

### IP アドレスの必要性

IP アドレスは、IP ネットワーク内でネットワークデバイスをアドレス指定するために使用します。ネットワーク内でデバイスをアドレス指定できるように、TCP/IP ネットワークプロトコルは UTN サーバ内に IP アドレスを保存することを要求します。

### UTN サーバが IP アドレスを取得する方法

UTN サーバの IP アドレスは、最初のインストール時に自動的に割り当てることができます。ブートプロトコルにより、IP アドレスが UTN サーバに自動的に割り当てられます。ブートプロトコルの「BOOTP」と「DHCP」は、出荷時に有効に設定されています。

UTN サーバがネットワークに接続されると、UTN サーバはブートプロトコルの BOOTP または DHCP から IP アドレスを取得できるかどうか確認します。いずれのプロトコルからも取得できない場合、ZeroConf によって予約されたアドレス範囲（169.254.0.0/16）から、UTN サーバが自ら IP アドレスを割り当てます。

UTN サーバがブートプロトコルにより自動的に IP アドレスを受け取ると、任意に設定可能な IP アドレスを UTN サーバに保存することができます。UTN サーバに割り当てられた IP アドレスは、ソフトウェアツールの「SEH UTN Manager」と「InterCon-NetTool」により決定または変更ができます。⇒ 17 を参照してください。

IP アドレスを割り当てるいくつかの方法を、次の通り説明します。

### 自動的に IP アドレスを割り当てる方法

- 「ZeroConf」⇒ 14
- 「BOOTP」⇒ 14
- 「DHCP」⇒ 14
- 「自動設定（IPv6 標準）」⇒ 15

### 手動で IP アドレスを割り当てる方法

- 「InterCon-NetTool」⇒ 15
- 「SEH UTN Manager」⇒ 15
- 「myUTN Control Center」⇒ 16
- 「ARP/PING」⇒ 16

## ZeroConf

IP アドレスがブートプロトコルにより割り当てられない場合、UTN サーバは、ZeroConf により自ら IP アドレスを割り当てます。このとき、UTN サーバは、ZeroConf に予約されたアドレス範囲 (169.254.0.0/16) からランダムに IP アドレスを選択します。



IP アドレスの名前解決には、Bonjour のドメイン名サービスを利用することができます。⇒[38](#) を参照してください。

## BOOTP

UTN サーバは BOOTP に対応しています。UTN サーバの IP アドレスを BOOTP サーバで割り当てることができます。

### 必要事項

☑ 「BOOTP」パラメータが有効になっていること。⇒[31](#) を参照してください。

☑ BOOTP サーバがネットワーク内で利用できること。

UTN サーバはネットワークに接続されると、BOOTP ホストに IP アドレスとホスト名を問い合わせます。BOOTP ホストは応答して、IP アドレスを含むデータパケットを送信します。この IP アドレスが、UTN サーバに保存されます。

## DHCP

UTN サーバは DHCP に対応しています。UTN サーバの IP アドレスを、DHCP サーバで動的に割り当てることができます。

### 必要事項

☑ 「DHCP」パラメータが有効になっていること。⇒[31](#) を参照してください。

☑ DHCP サーバがネットワーク内で利用できること。

ハードウェアの設定が完了すると、UTN サーバは DHCP サーバに対して、ブロードキャストクエリの方法で IP アドレスを要求します。DHCP サーバは、ハードウェアアドレスに基づき UTN サーバを識別し、データパケットを UTN サーバに送信します。

このデータパケットには、UTN サーバの IP アドレス、デフォルトゲートウェイ、および DNS サーバの IP アドレスが含まれています。これらのデータは UTN サーバに保存されます。

## 自動設定 (IPv6 標準)

UTN サーバは 1 つの IPv4 のアドレスと複数の IPv6 のアドレスを同時に持つことができます。IPv6 ネットワークでの IP アドレスの自動割り当てには、IPv6 標準が使用されます。IPv6 ネットワークに接続されると、UTN サーバは追加のリンクローカル IP アドレスを IPv6 アドレス範囲から自動的に取得します。

UTN サーバは、そのリンクローカル IP アドレスを使用してルータを検索します。UTN サーバは、いわゆる「Router Solicitations」(RS) を特別のマルチキャストアドレス FF02::2 に対して送信します。応答可能なルータは、それに対して要求された情報を含む「Router Advertisement」(RA) を返します。

グローバルなユニキャストアドレス範囲からのプレフィックスにより、UTN サーバは自らのアドレスを構成できます。UTN サーバは、単に最初の 64 ビット (プレフィックス FE80::) を RA で送信されたプレフィックスで置き換えます。

### 必要事項

- ☑ 「IPv6」パラメータが有効になっていること。
- ☑ 「自動設定」パラメータが有効になっていること。



IPv6 アドレスの割当てを設定する方法は、⇒[34](#) を参照してください。

## InterCon-NetTool

InterCon-NetTool は、SEH Computertechnik GmbH が開発した、SEH ネットワークデバイスを管理するソフトウェアです。InterCon-NetTool の IP ウィザードを使用して、IP アドレスなどの TCP/IP パラメータを設定できます。IP ウィザードにより、必要な IPv4 アドレスを手動で入力し、そのアドレスを UTN サーバに保存できます。InterCon-NetTool で IPv4 アドレスを設定する方法は、⇒[33](#) を参照してください。

## SEH UTN Manager

SEH UTN Manager により、必要な IPv4 アドレスを手動で入力し、そのアドレスを UTN サーバに保存できます。SEH UTN Manager で IPv4 アドレスを設定する方法は、⇒[32](#) を参照してください。

## myUTN Control Center

myUTN Control Center により、必要な IP アドレスを手動で入力し、そのアドレスを UTN サーバに保存できます。

- myUTN Control Center で IPv4 アドレスを設定する方法は、⇒[31](#) を参照してください。
- myUTN Control Center で IPv6 アドレスを設定する方法は、⇒[34](#) を参照してください。

## ARP/PING

ハードウェアアドレスへの IP アドレスの割り当てを、ARP テーブルを使用して行うことができます。ARP テーブルは内部システムファイルで、割り当て内容を一時的に保存します（約 15 分）。ARP テーブルは ARP プロトコルにより管理されています。

「arp」と「ping」コマンドにより、UTN サーバに IP アドレスを保存できます。UTN サーバの IP アドレスがすでに設定されている場合、「arp」と「ping」コマンドを使用して新規に IP アドレスを保存することはできません。

ただし、ZeroConf に予約されたアドレス範囲（169.254.0.0/16）内の IP アドレスは「arp」および「ping」コマンドによって上書きできません。

「arp」コマンドは ARP テーブルの編集に使用されます。「ping」コマンドは、IP アドレスを含むデータパケットを UTN サーバのハードウェアアドレスに転送します。データパケットの送受信が正常に完了すると、UTN サーバは IP アドレスを永続的に保存します。

「arp」および「ping」コマンドの実装は、使用するシステムに依存します。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。

### 必要事項

- 「ARP/PING」パラメータが有効になっていること。⇒[32](#) を参照してください。

ARP テーブルの編集：

構文：arp -s <IP アドレス> <ハードウェアアドレス>

例：arp -s 192.168.0.123 00-c0-eb-00-01-ff

UTN サーバに新しい IP アドレスを割り当てます。

構文：ping <IP アドレス>

例：ping 192.168.0.123



## 2 管理方法



UTN サーバは、いくつかの方法で管理および設定ができます。この章では、様々な管理オプションについて概説します。

各管理方法がどのような場合に適しているか、どのような機能に対応しているのかについて説明します。

### 必要な情報

- 「myUTN Control Center による管理」⇒17
- 「SEH UTN Manager による管理」⇒19
- 「InterCon-NetTool による管理」⇒26
- 「電子メールによる管理（myUTN-80 以降のみ）」⇒28
- 「デバイスのステータスボタンによる管理」⇒30

### 2.1 myUTN Control Center による管理

#### 対応する機能

myUTN Control Center は、UTN サーバの管理および監視能に必要なすべての機能を備えています。

myUTN Control Center は UTN サーバに格納され、ブラウザソフトウェア（Internet Explorer、Mozilla Firefox、Safari）で表示できます。

#### 必要事項

- UTN サーバがネットワークに接続され、電源が供給されていること。
- UTN サーバに有効な IP アドレスが設定されていること。

#### 手順

1. ブラウザを開きます。
  2. UTN サーバの IP アドレスを URL で入力します。
- 🔗 myUTN Control Center - ホームページが表示されます。



myUTN Control Center が表示されない場合は、ブラウザのプロキシ設定を確認してください。

myUTN Control Center は、ソフトウェアツールの「SEH UTN Manager」または「InterCon-NetTool」からも起動できます。

#### myUTN Control Center の起動

- InterCon-NetTool から myUTN Control Center を起動するには、デバイスリストの UTN サーバを選択して、メニューバーから**アクション (A) - ブラウザの起動**を選択します。
- SEH UTN Manager から myUTN Control Center を起動するには、選択リストの UTN サーバを選択して、メニューバーから **UTN サーバ-構成**を選択します。




図 2 : myUTN Control Center - ホーム

## myUTN Control Center の構造

使用できるメニュー項目はナビゲーションバー(上)にあります。メニュー項目を選択すると (マウスをクリック)、使用可能なサブメニューが左側に表示されます。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右側に表示されます。

言語を設定するには、メニュー項目の**ホーム**を選択します。選択する言語の国旗を選択してください。

**製品と会社情報**には、メーカーの連絡先や製品の詳細情報が表示されます。**サイトマップ**には、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。

他のすべての項目は、UTN サーバの設定に関するメニューです。これらの詳細は、myUTN Control Center の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開くには、 アイコンをクリックします。

## 2.2 SEH UTN Manager による管理

### 適用範囲

「SEH UTN Manager」は、USB デバイスへのアクセスを管理するソフトウェアツールです。SEH UTN Manager は、ネットワーク内に存在する、使用可能なすべての UTN サーバと USB デバイスを表示し、クライアントと USB デバイスとの接続を確立します。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。

### 基本機能

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の範囲は任意に設定できます。

ネットワークスキャン後、検出されたすべての UTN サーバは、接続されているデバイスとともに「ネットワークリスト」に表示されます。リストから使用するデバイスを選択して、「選択リスト」に追加します。選択リストにあるデバイスは、設定や、クライアントへの接続が可能です。

### 自動操作じどうそうさ

SEH UTN Manager は、特に次のような自動操作に対応しています。

- **自動起動:** ユーザのコンピュータが起動すると、SEH UTN Manager が有効になります。
- **自動接続:** この機能により、SEH UTN Manager が起動すると、デバイス接続が自動的にアクティブになります。
- **自動切断:** この機能は、設定時間の経過後にデバイス接続を自動的に無効化します。
- **オンデマンド印刷:** 印刷ジョブを受信すると、USB デバイス（プリンタまたは複合機）とクライアントとの接続が自動的に確立されます。印刷ジョブが完了すると、接続は自動的に解除されます。
- **UTN アクションを作成する:** UTN アクションは、デバイス接続を自動的にアクティブまたは非アクティブにするプログラムです。また、UTN アクションはデバイス接続と連携して、アプリケーションを自動的に起動または終了します。
- **付加ツール「utnm」:** USB デバイスをアクティブまたは非アクティブにするためのツールです。そのコマンドは、オペレーティングシステムのコマンドラインインタフェースから入力して実行します。別の方法としては、スクリプトを記述します。

## バージョン間の相違

インストールおよびプログラム  
の起動

## SEH UTN Manager のバージョン

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
- ミニマルバージョン（グラフィカルユーザインタフェースなし）

バージョン間の大きな相違は、フルバージョンにはグラフィカルユーザインタフェース（GUI）が装備されている点です。GUI はプログラムをグラフィック画像の形式で表示して、UTN サーバの検索機能や管理機能など、USB デバイスをより簡単に利用できる拡張機能を提供します。

ミニマルバージョンの SEH UTN Manager は、コマンドラインインタフェースおよび UTN アクションでのみ使用できます。ミニマルバージョンは次の用途で使用できます。

- 特定のデバイスを単にアクティブ / 非アクティブにする。「UTN アクションを作成する：SEH UTN Manager インタフェースを使わずに自動化されたデバイス接続とプログラムの開始」⇒ 65 を参照してください。
- スクリプトを使用して、USB デバイスのアクティブ / 非アクティブを自動化する。「付加ツール「utnm」」⇒ 131 を参照してください。



一般的な使用には、フルバージョンを推奨します。ミニマルバージョンは上級者のみが使用してください。

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有効になります。このサービスは、通常の管理方法で制御できます。

また、次のユーザグループを区別します。

- 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）

**自動接続、自動切断、およびオンデマンド印刷機能は、管理者権限のあるユーザのみが設定できます。**

SEH UTN Manager を使用するには、プログラムを Windows、または Mac OS X のオペレーティングシステムで動作するコンピュータにインストールする必要があります。オペレーティングシステムごとに、個別のインストールファイルが使用できます。SEH UTN Manager のインストー

ルファイルは、SEH Computertechnik GmbH のホームページで入手できます。

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

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。インストール時に必要なバージョンを選択できます。

また、Windows ではサイレントインストールが可能です。

## Windows

インストールファイルは Windows システム用の「\*.exe」として入手できます。

### システム要件


- ☑ SEH UTN Manager は、Windows XP 以降に対応しています。
- ☑ インストールは、管理権限のあるユーザのみが実行できます。

### 手順

1. SEH UTN Manager のインストールファイルを起動します。
  2. インストール手順に従います。
- ☞ SEH UTN Manager がクライアントにインストールされます。



サーバベースの環境（Citrix XenApp、Microsoft Remote Desktop サービス /Terminal サービス）や仮想化環境（VMware, Citrix XenDesktop, Microsoft HyperV など）で使用する場合、Windows 側に必要なドライバがないことがあります。インストールルーチンはインストール進行中に使用できるドライバを確認します。ドライバがない場合、別のインストーラ（「SEH UTN Manager 用 USB ドライバ」）が起動します。このインストーラは、必要なドライバのインストールを準備します。

SEH UTN Manager を起動するには、SEH UTN Manager アイコン  をダブルクリックします。アイコンはデスクトップの Windows スタートメニューにあります。

(スタート → すべてのプログラム → SEH Computertechnik GmbH → SEH UTN Manager)



SEH UTN Manager 実行しようとする、Windows のユーザアカウント制御が確認を求めてくる場合があります。

## システム要件

## Mac OS X


インストールファイルは Mac システム用の「\*.pkg」として入手できます。

- ☑ SEH UTN Manager は、Mac OS X 10.6.x、Mac OS X 10.7.x (64-bit)、OS X 10.8.x に対応しています。
- ☑ インストールは、管理権限のあるユーザのみが実行できます。

 手順

1. SEH UTN Manager のインストールファイルを起動します。
  2. インストール手順に従います。
- ☞ SEH UTN Manager がクライアントにインストールされます。

SEH UTN Manager を起動するには、「SEH UTN Manager.app」ファイル

 をダブルクリックします。

(アプリケーション → SEH UTN Manager.app)

## サイレントインストール (Windows)

サイレントインストールはユーザ側の入力なしで実行できます。初期設定は次のとおりです。

- フルバージョン
- クライアント側のすべてのユーザに対してインストール
- インストール先ディレクトリは、`%PROGRAMFILES%\SEH Computertechnik GmbH\SEH UTN Manager`  
(`%PROGRAMFILES%` は「プログラム」フォルダの Windows 環境変数。パスは、コマンドラインで次のように設定できます：`echo %PROGRAMFILES%`)

## 利点と目的

サイレントインストールは時間の節約になります。ログインスクリプトにより、SEH UTN Manager を多数のクライアントに自動的にインストールできます。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。

## システム要件

- ☑ SEH UTN Manager は、Windows XP 以降に対応しています。
- ☑ インストールは、管理権限のあるユーザのみが実行できます。



SEH UTN Manager をインストールすると、SEH Computertechnik GmbH の使用許諾とソフトウェア使用に関する契約に同意したものと自動的に見

なされます。契約書は、SEH Computertechnik GmbH のホームページから入手できます。

<http://www.seh-technology.com/services/licenses/software-license-agreement.html>

### 手順

1. コマンドラインインタフェースを開きます。
  2. SEH UTN Manager のインストールファイルがあるディレクトリに移動します。
  3. コマンドシーケンスを入力します。「構文およびコマンド」⇒23 を参照してください。
  4. 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。

### 構文およびコマンド

構文は次のとおりです。

```
"sehutnmanager-win-X.X.X.exe" /S [< コマンド >]
```

次のコマンドがサポートされています。

コマンド	説明
/s	サイレントインストールの実行（画面出力なし）
/u	既存のインストールの更新
/srv	ミニマルバージョン（グラフィカルユーザインタフェースなし）のインストール
?	ヘルプページの表示



コマンドは必ず大文字で記述します。

### バージョンの変更

SEH UTN Manager のどちらかのバージョンがインストールされている環境で、バージョンを変更する場合は、先にインストール済みのバージョンをアンインストールしてください。

### 更新

SEH UTN Manager の更新状況に関する情報を取得できます。更新プログラムがある場合、コンピュータにインストールファイルをコピーしてプログラムをインストールできます。更新すると、初期設定は、既存のバージョンに応じて変更されます。

## プログラム構造

プログラムが起動すると、メインダイアログが表示され、次の項目が確認できます。このダイアログは、表示または非表示を選択した項目によって異なります。

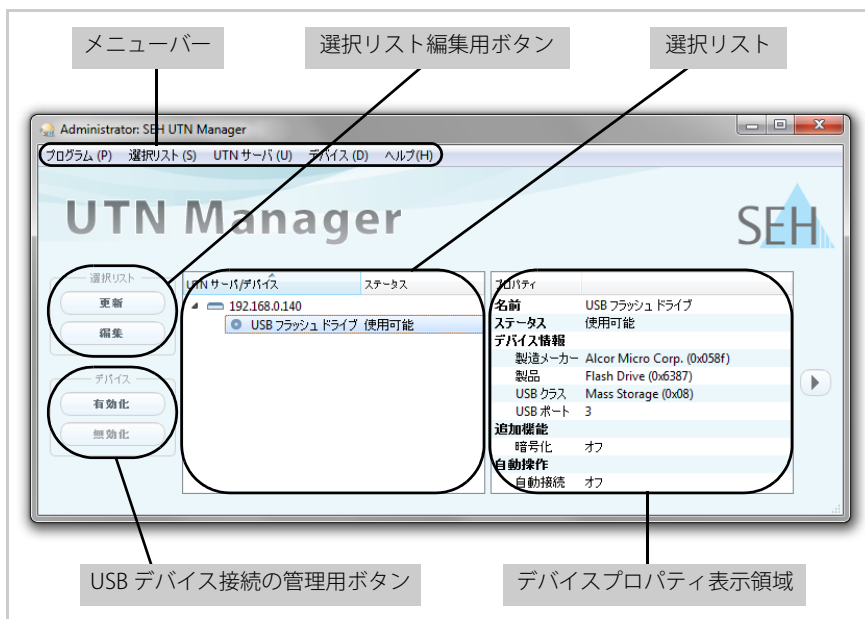


図 3：SEH UTN Manager - メインダイアログ

## 対応する機能

SEH UTN Manager は、次の機能を提供します。

- ・ 「USB デバイスを選択リストに追加する」 ⇒ 158
- ・ 「USB デバイスをクライアントに接続する」 ⇒ 159
- ・ 「USB デバイスとクライアントの接続を解除する」 ⇒ 160
- ・ 「使用中の USB デバイスを要求する」 ⇒ 161
- ・ 「デバイス接続とプログラムの開始を自動化する」 ⇒ 162
- ・ 「UTN サーバに IPv4 アドレスを割り当てる」 ⇒ 132
- ・ 「myUTN Control Center の起動」 ⇒ 117
- ・ 「ロックされた USB デバイスへのアクセスを許可する」 ⇒ 180
- ・ 「複数の参加者用選択リストを管理する」 ⇒ 168





---

SEH UTN Manager の使用方法の詳細は、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、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。

---

SEH UTN Manager の機能は、次の条件に従い無効として表示する、または非表示にすることができます。

- 組み込まれている UTN サーバ機種
- 選択リストの種類と場所
- クライアントのユーザ権限
- 製品に固有なセキュリティメカニズムの設定



---

詳細は、「SEH UTN Manager - 機能の概要」⇒[124](#) を参照してください。

---

## 2.3 InterCon-NetTool による管理

InterCon-NetTool は、SEH Computertechnik GmbH が開発した、SEH ネットワークデバイス（プリントサーバ、TPG、ISD、UTN サーバなど）を管理するソフトウェアです。InterCon-NetTool を使うことで、ネットワークデバイスごとの各種機能が設定できます。

### 基本機能

InterCon-NetTool を起動すると、ネットワークをスキャンして、接続されているネットワークデバイスを検出します。スキャンするネットワークの範囲は任意に設定できます。検出されたすべてのネットワークデバイスは、「デバイスリスト」に表示されます。

デバイスリストは、必要に応じて内容を変更できます。デバイスリストのデバイスを選択して設定できます。

### インストールおよびプログラムの起動

InterCon-NetTool を使用するには、プログラムを Windows、または Mac OS X のオペレーティングシステムで動作するコンピュータにインストールする必要があります。オペレーティングシステムごとに、個別のインストールファイルが使用できます。InterCon-NetTool のインストールファイルは、SEH Computertechnik GmbH のホームページで入手できます。


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

## Windows

インストールファイルは Windows システム用の「\*.exe」として入手できます

### 手順

1. InterCon-NetTool のインストールファイルを起動します。
  2. 言語を選択します。
  3. インストールルーチンに従います。
- ☞ InterCon-NetTool がクライアントにインストールされます。

InterCon-NetTool を起動するには、InterCon-NetTool アイコン  をダブルクリックします。アイコンはデスクトップの Windows スタートメニューにあります。

(スタート → すべてのプログラム → SEH Computertechnik GmbH → InterCon-NetTool)


InterCon-NetTool の設定は「NetTool.ini」ファイルに保存されます。このファイルは、現在ログインしているユーザのユーザフォルダに保存されています。

## Mac OS X

インストールファイルは Mac システム用の「\*.dmg」として入手できます。

### 📁 手順

1. InterCon-NetTool のインストールファイルを開きます。  
ファイルの内容が表示されます。
  2. 「\*.pkg」ファイルを起動します。
  3. インストールルーチンに従います。
- 🔗 InterCon-NetTool がクライアントにインストールされます。

InterCon-NetTool を起動するには、「Intercon-NetTool.app」ファイル  をダブルクリックします。

(アプリケーション → SEH UTN Manager.app)

プログラムの設定は「InterCon-NetTool.ini」ファイルに保存されます。このファイルは「/Users/ユーザ名/Library/Preferences/InterCon-NetTool」ディレクトリにあります。

プログラムが起動すると、メインダイアログが表示され、次の項目が確認できます。このダイアログは、項目を表示または非表示の選択をすることによって表示内容が異なります。

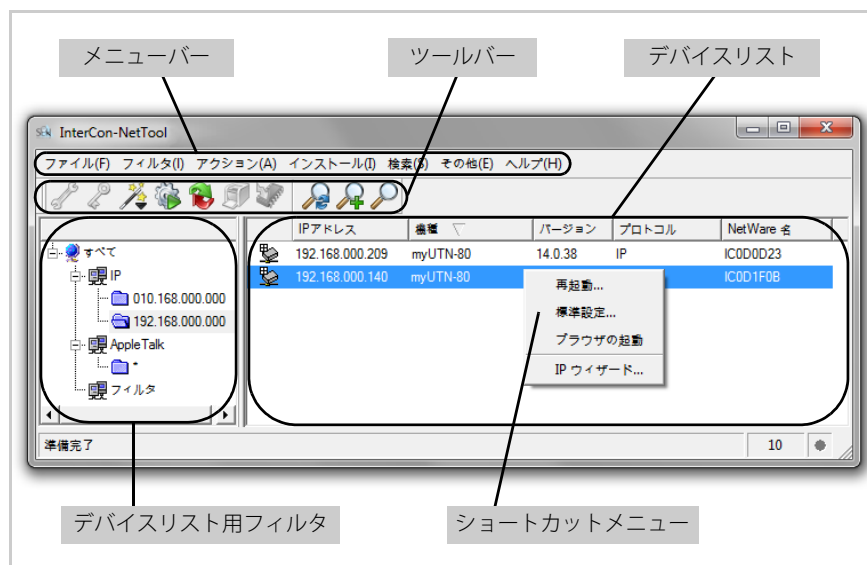


図 4：InterCon-NetTool - メインダイアログ

## 対応する機能

InterCon-NetTool を使用すると、次を実行できます。

- 「UTN サーバに IPv4 アドレスを割り当てる」⇒[133](#)
- 「UTN サーバを再起動する」⇒[102](#)
- 「UTN サーバのパラメータ値を初期設定にリセットする」⇒[99](#)
- 「myUTN Control Center を起動する」⇒[17](#)
- 「BIOS モードから標準モードに切り替える」⇒[127](#)



InterCon-NetTool の使用方法の詳細は、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、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。

## 2.4 電子メールによる管理（myUTN-80 以降のみ）

電子メールを使うことで、インターネットが使用できる任意のコンピュータから UTN サーバを管理できます。

## 機能性

電子メールを使用して、次のことができます。

- UTN サーバ情報の送信
- UTN サーバパラメータの設定
- UTN サーバ上での更新の実行

## 必要事項

- ☑ DNS サーバが UTN サーバで設定されていること。⇒[36](#) を参照してください。
- ☑ 電子メールを受信することができるように、UTN サーバが、POP3 サーバ上に電子メールアドレスを持つユーザとして設定されていること。
- ☑ POP3 と SMTP のパラメータが UTN サーバで設定されていること。⇒[39](#) を参照してください。

## 電子メールによる命令の送信

電子メールで UTN サーバを管理するには、電子メールの件名に適切な命令を入力して送信します。

## 手順

1. 電子メールプログラムを開きます。
2. 新しい電子メールを作成します。

## 命令の構文とフォーマット

3. UTN サーバのアドレスを受信者として入力します。
  4. 件名にコマンドを入力します。「命令の構文とフォーマット」⇒129を参照してください。
  5. 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て、命令を実行します。

件名に入力する命令の構文は、次の通りです。

cmd:< コマンド > [< コメント >]

次のコマンドがサポートされています。

コマンド	オプション	説明
< コマンド >	get status	UTN サーバのステータスページを送信。
	get parameters	UTN サーバのパラメータリストを送信。
	set parameters	パラメータを UTN サーバに送信。 構文と値はパラメータリストから取得できません。⇒106を参照してください。 パラメータと値は電子メール本文への入力が必要です。
	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。
	help	リモートメンテナンスに関する情報を含むページを送信。
[< コメント >]		説明用の任意のテキスト文。

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

## TAN によるセキュリティ

UTN サーバでの更新やパラメータ変更には、TAN が必要になります。最新の TAN は、UTN サーバから電子メールで（例えばステータスページを受領する際に）取得します。TAN は電子メール本文の最初の行に入力します。その後、空白文字を 1 字入れます。

## パラメータ変更

パラメータ変更は、次の構文で電子メールの本体に組み込みます。

<パラメータ> = <値>

構文と値はパラメータリストから取得できます。⇒106 を参照してください。

例 1： この電子メールによって、UTN サーバは電子メールの送信者にパラメータリストを送信します。

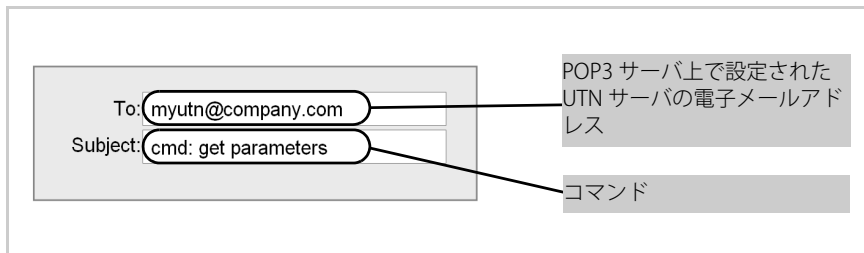


図 5：電子メールによる管理 - 例 1

例 2： この電子メールは、UTN サーバ上で「説明」パラメータを設定しています。

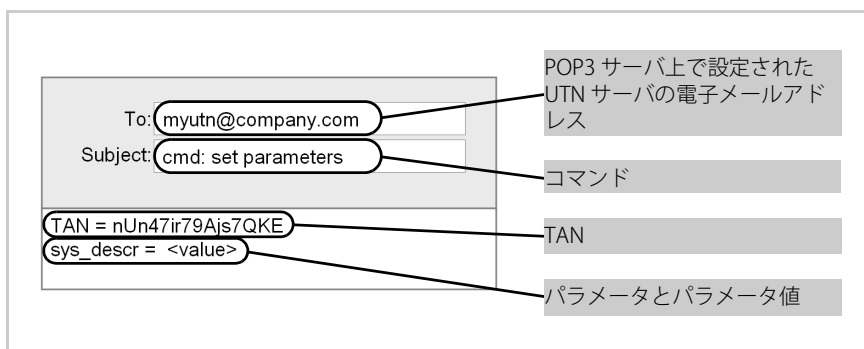


図 6：電子メールによる管理 - 例 2

## 2.5 デバイスのステータスボタンによる管理

UTN サーバには LED、リセットボタン、および各種のポートがあります。これらのコンポーネントについては、「クイック・インストール案内」で説明しています。

リセットボタンを使用すると、UTN サーバのパラメータ値を初期設定にリセットできます。⇒99 を参照してください。

## 3 ネットワーク設定



UTN サーバを TCP/IP ネットワークへ適切に組み込むために、様々な設定を指定できます。この章では、UTN サーバが対応するネットワーク設定について説明します。

### 必要な情報

- 「IPv4 パラメータの設定方法」⇒[31](#)
- 「IPv6 パラメータの設定方法」⇒[34](#)
- 「DNS の設定方法」⇒[36](#)
- 「SNMP の設定方法」⇒[37](#)
- 「Bonjour の設定方法」⇒[38](#)
- 「POP3 と SMTP の設定方法 (myUTN-80 以降のみ)」⇒[39](#)
- 「WLAN の設定方法 (myUTN-54 のみ)」⇒[42](#)

### 3.1 IPv4 パラメータの設定方法

TCP/IP (Transmission Control Protocol over Internet Protocol) は、複数の接続に対してデータパケットを転送し、ネットワーク機器間の接続を確立します。

ブートプロトコルの DHCP および BOOTP は、TCP/IP プロトコルに属します。UTN サーバを TCP/IP ネットワークへ適切に組み込むため、様々な IPv4 パラメータを設定できます。IP アドレスの割り当てにの詳細は、[313](#) を参照してください。

### 選択できる作業

- 「myUTN Control Center を使用し IPv4 パラメータを設定する」⇒[31](#)
- 「SEH UTN Manager を使用し IPv4 アドレスを設定する」⇒[32](#)
- 「InterCon-NetTool を使用し IPv4 パラメータを設定する」⇒[33](#)

### myUTN Control Center を使用し IPv4 パラメータを設定する

#### 手順

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 [32](#) を参照してください)。

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。 プロトコルは、UTN サーバに IP アドレスを保存する様々な方法を提供します。 (「IP アドレスの UTN サーバへの保存」⇒ 13 を参照してください) UTN サーバに IP アドレスを割り当てたあとは、これらのオプションを無効にすることをお奨めします。
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。
ゲートウェイ	UTN サーバのゲートウェイアドレスです。

## SEH UTN Manager を使用し IPv4 アドレスを設定する

### 必要事項

- 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。⇒ 19 を参照してください。
- UTN サーバが選択リストに追加されていること。⇒ 58 を参照してください。

### 手順

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. 適切な 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。



## 必要事項

## InterCon-NetTool を使用し IPv4 パラメータを設定する

- ☑ InterCon-NetTool がクライアントにインストールされていること。⇒ 26 を参照してください。
- ☑ マルチキャストでのネットワークスキャンが InterCon-NetTool で有効になっていること。
- ☑ ネットワーク内のルータがマルチキャスト要求を転送できること。

 手順

1. InterCon-NetTool を起動します。
2. デバイスリストから、UTN サーバを選択します。  
UTN サーバはデバイスリストの「ZeroConf」の下に表示され、ZeroConf に予約されたアドレス範囲 (169.254.0.0/16) 内の IP アドレスが割り当てられています。
3. メニューバーから、インストール - IP ウィザードを選択します。  
IP ウィザードが開始されます。
4. ウィザードの指示に従います。  
☞ 設定が保存されます。

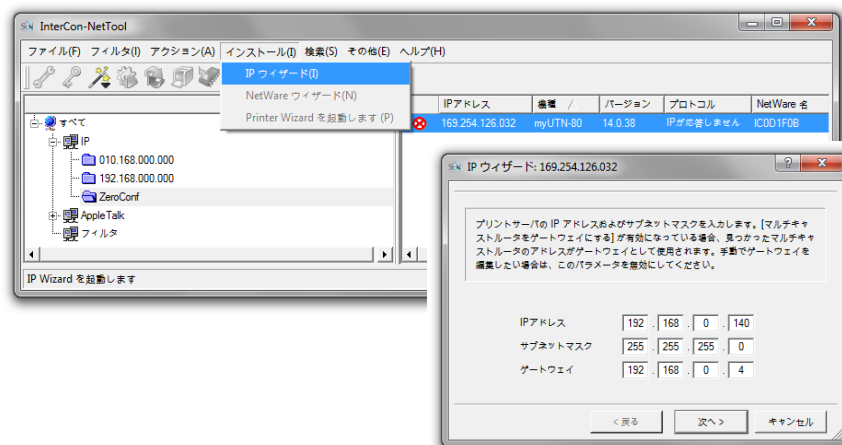


図 7：InterCon-NetTool - IP ウィザード

## 3.2 IPv6 パラメータの設定方法

UTN サーバは、IPv6 ネットワークに組み込むことができます。

### IPv6 の利点

IPv6 (Internet Protocol version 6) は、より一般的な IPv4 の後継バージョンです。IPv6 と IPv4 は、OSI モデルのネットワーク層の標準プロトコルで、ネットワーク経由のデータパケットのアドレス指定およびルーティングを制御します。IPv6 の導入には、多くの利点があります。

- IPv6 により、IP アドレス空間は  $2^{32}$  個 (IPv4) から  $2^{128}$  個 (IPv6) に増加します。
- 自動設定と再番号割り当て
- ヘッダ情報の縮小によるルーティングの効率化
- IPSec、QoS、マルチキャストなどの、統合サービス
- モバイル IP

### IPv6 アドレスの構造

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、16 ビットを示す 4 つの 16 進数が含まれます。

各フィールドはコロン (:) で区切られます。

**例:** fe80 :0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4

フィールド内の先行するゼロは省略できます。

**例:** fe80 :0 : 0 : 0 : 0 : 10 : 1000 : 1a4

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 (::) が使用されます。ただし、2 つのコロンは 1 つのアドレスで 1 回のみ使用できます。

**例:** fe80 : : : : : 10 : 1000 : 1a4

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 (ブラケット) で囲う必要があります。これにより、ポート番号が IPv6 アドレスの一部に間違えられることを防止できます。

**例:** http://[2001:608:af:1::100]:443



IPv6 形式の URL は、IPv6 に対応するブラウザでのみ使用できます。

## 使用できる IPv6 アドレスのタイプ

IPv6 アドレスには、様々なタイプがあります。IPv6 アドレスのプレフィックスは、IPv6 アドレスのタイプに関する情報を提供します。

- ユニキャストアドレスは、グローバルにルーティングできます。これらのアドレスは一意です。ユニキャストアドレスに送信されるパケットは、このアドレスに割り当てられたインターフェースのみに届きます。ユニキャストアドレスのプレフィックスは「2」または「3」です。
- エニーキャストアドレスは、複数のインターフェースに割り当てられます。つまり、このアドレスに送信されるデータパケットは様々なデバイスに届きます。エニーキャストアドレスの構文は、ユニキャストアドレスの構文と同じです。違いは、エニーキャストアドレスが多数のインターフェースから1つを選択するという点です。エニーキャストアドレス専用のパケットは、最も近いインターフェース（ルータのメトリックスに従って）に届きます。エニーキャストアドレスは、ルータのみで使用します。
- マルチキャストアドレスは、帯域幅圧迫することなく、同時に複数のインターフェースにデータパケットを送信できます。マルチキャストアドレスは、プレフィックス「ff」で認識できます。

### 手順

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 ⇨ 35 を参照してください）。
  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	UTN サーバに割り当てられた IPv6 ユニキャストアドレスを、n:n:n:n:n:n:n:n の形式で手動で設定します。各「n」は、アドレスの8つの16ビット要素の1つの16進値を示します。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（::）が使用されます。

パラメータ	説明
ルータ	ルータの IPv6 ユニキャストアドレスを指定します。UTN サーバは「Router Solicitations」(RS) をこのルータに送信します。
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。アドレス範囲は、プレフィックスによって示されます。プレフィックス長 (使用するビット数) が IPv6 アドレスに追加され、10 進値で指定されます。この 10 進値は「/」で区切られます。

### 3.3 DNS の設定方法

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 を使用すると、ドメイン名を IP アドレスに割り当てたり、IP アドレスをドメイン名に割り当てることができます。ネットワークで DNS サーバが使用可能であれば、UTN サーバに DNS を使用することができます。

設定処理中にドメイン名を使用する場合、最初に DNS を有効にして設定する必要があります。DNS は、例えばタイムサーバの設定に使用されます。

#### 手順

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 4 ⇨ 36 を参照してください)。
  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 : DNS パラメータ

パラメータ	説明
DNS	DNS 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します。
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。

## 3.4 SNMP の設定方法

SNMP (Simple Network Management Protocol) は、ネットワークの構成要素を管理、監視するための標準プロトコルです。このプロトコルは、監視対象デバイスと監視側装置間の通信を制御します。

SNMP を使用すると、ネットワーク構成要素 (例: UTN サーバ) が提供する管理情報を読み込んで編集できます。UTN サーバは、SNMP のバージョン 1 と 3 に対応しています。

### SNMPv1

SNMP コミュニティは、アクセス保護の基本的な形式です。コミュニティでは、多数の SNMP マネージャがグループ化されます。次に、そのコミュニティに (読み取り / 書き込み) アクセス権が割り当てられます。一般的なコミュニティ文字列は、「public」です。



SNMPv1 のコミュニティ文字列は平文で転送されるため、十分に保護されていません。

### SNMPv3

SNMPv3 は SNMP 標準の強化バージョンで、アプリケーションとユーザベースのセキュリティモデルが改善されています。SNMPv3 は、簡潔さとセキュリティの概念が特徴です。

#### 手順

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 5 ⇨ 37 を参照してください)。
  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 5 : 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	コミュニティの書き込み保護を、有効または無効にします。
コミュニティ	SNMP コミュニティの名前です。 SNMP コミュニティは、同じアクセス権を持つ複数の参加者をグループにまとめるという、アクセス保護の基本的な形式です。
SNMPv3	SNMPv3 を有効または無効にします。

パラメータ	説明
ユーザ名	SNMP ユーザの名前を設定します。
パスワード	SNMP ユーザのパスワードを設定します。
ハッシュ	ハッシュアルゴリズムを設定します。
アクセス権	SNMP ユーザのアクセス権を設定します。
暗号化	暗号化の方法を設定します。

### 3.5 Bonjour の設定方法

Bonjour を使用することで、TCP/IP ベースのネットワーク内のコンピュータ、デバイスおよびネットワークサービスが自動的に認識されます。

UTN サーバは、次の Bonjour 機能を使用します。

- ZeroConf により割り当てられた IP アドレスの確認
- IP アドレスへのホスト名の割り当て
- デバイスのホスト名や IP アドレスの情報なしで、サーバサービスの位置を特定。

ZeroConf (「ZeroConf」⇒ 14 を参照) から割り当てられた IP アドレスを確認する際に、UTN サーバはネットワークにクエリを送信します。IP アドレスがすでにネットワーク上の別の場所に割り当てられている場合、UTN サーバはメッセージを受信します。次に、UTN サーバは別の IP アドレスで新たなクエリを送信します。その IP アドレスが使用可能な場合、IP アドレスは UTN サーバに保存されます。

追加の Bonjour 機能には、ドメイン名サービスが使用されます。Bonjour ネットワークでは中枢の DNS サーバがないため、各デバイスおよびアプリケーションは独自の小規模な DNS サーバを持ちます。

この統合型の DNS サーバ (mDNS) は、ネットの参加者すべてから情報を収集して管理します。mDNS サーバは、従来の DNS サーバの機能に加え、各参加者の IP アドレス、サービス名、また提供されているサービスも保存します。

#### 手順

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 6 ⇒ 39 を参照してください)。

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 6 : 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 サービスに使用します。Bonjour 名が入力されない場合、デフォルト名（デバイス名 @ICxxxxxx）が使用されます。

### 3.6 POP3 と SMTP の設定方法（myUTN-80 以降のみ）

通知サービス (⇒ 52) と電子メールによるリモートメンテナンス (⇒ 28) を正しく動作させるためには、POP3 および SMTP のプロトコルを UTN サーバ上で設定する必要があります。

#### POP3

「POP3」(Post Office Protocol Version 3) は、クライアントがメールサーバから電子メールを取り込む際に使用する転送プロトコルです。UTN サーバを電子メールで管理するには POP3 が必要です。

#### SMTP

「SMTP」(Simple Mail Transfer Protocol) は、ネットワーク内の電子メールの送信を制御するプロトコルです。UTN サーバを電子メールで管理して通知サービスを運用するには、SMTP が必要です。

#### 選択できる作業

- 「POP3 を設定する」 ⇒ 39
- 「SMTP を設定する」 ⇒ 40

### POP3 を設定する

#### 手順

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 7 ⇒ 40 を参照してください。
  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 7：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設定します。 ホスト名は、DNS が事前に設定された場合にのみ使用できます。
POP3 - サーバポート	UTN サーバが電子メールを受信するときに使用するポートを設定します。ポート番号 110 があらかじめ設定されています。SSL/TLS を使用する場合はポート番号 995 を入力します。
POP3 - セキュリティ	使用する認証方法を設定します (APOP / SSL/TLS)。SSL/TLS を使用する場合、暗号強度は暗号化レベルで設定されます ⇨ 73。
POP3 - メールのチェック間隔	POP3 サーバから電子メールを受信する間隔を分単位で設定します。
POP3 - メールの上限数	UTN サーバが許容する電子メールの最大サイズをキロバイト単位で設定します。 (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 サーバが使用するパスワードを設定します。

## SMTP を設定する

### 手順

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 8 ⇨ 41 を参照してください
  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 8：SMTP パラメータ

パラメータ	説明
SMTP - サーバ名	SMTP サーバを IP アドレスまたはドメイン名で設定します。 ホスト名は、DNS が事前に設定された場合にのみ使用できます。
SMTP - サーバーポート	UTN サーバが SMTP サーバに電子メールを送信するときに使用するポート番号を設定します。ポート番号 25 があらかじめ設定されています。
SMTP - TLS	TLS を有効または無効にします。 セキュリティプロトコル TLS (Transport Layer Security) は、UTN サーバと SMTP サーバ間の送信を暗号化するために使用されます。暗号強度は暗号化レベルで設定されます ⇨ 73。
SMTP - 送信者名	電子メール送信で UTN サーバが使用する電子メールアドレスを設定します。 <u>メモ</u> ：送信者の名前とユーザ名は同一である可能性があります。
SMTP - ログイン	ログイン時の SMTP 認証を、有効または無効にします。
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 サーバにログインするために UTN サーバが使用するパスワードを設定します。
SMTP - セキュリティ (S/MIME)	S/MIME による電子メールの暗号化と署名を、有効または無効にします。
SMTP - 電子メールの署名	電子メールの署名を設定します。 送信者が作成した署名によって、受信者はその送信者を本人であると確認でき、電子メールが改ざんされていないことを確認できます。電子メールの署名を行うには S/MIME 証明書が必要です。⇨ 82
SMTP - 完全な暗号化	電子メールの暗号化を設定します。 暗号化された電子メールは、受信者のみが開いて読むことができます。暗号化を行うには S/MIME 証明書が必要です。⇨ 82
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。電子メールを読むために、多くの電子メールのクライアントは公開キーの添付を要求します。

### 3.7 WLAN の設定方法 (myUTN-54 のみ)

UTN サーバの機種「myUTN-54」は WLAN に対応しています。このため、ネットワーク内の UTN サーバを無線で操作できます。

#### WLAN の役割

WLAN は、ネットワークコンポーネント間の無線接続を確立する無線技術です。WLAN テクノロジは、IEEE 802.11 系の標準に定義されています。myUTN-54 は、IEEE 802.11b、IEEE 802.11g、および IEEE 802.11n 標準に対応しています。

無線技術を使用するため、myUTN-54 には追加パラメータがあります。⇒ 45 を参照してください。myUTN Control Center では、メニュー項目 **ネットワーク - WLAN** から現在の WLAN 設定を表示できます。

#### 接続ステータス

myUTN Control Center の次のアイコンは、現在の接続ステータスを示しています。



無線ネットワーク内の UTN サーバ



有線ネットワーク内の UTN サーバ

#### WLAN セキュリティ

権限のないユーザの無線 LAN へのログオン、インターネットやネットワークリソースへのアクセスを防止します。UTN サーバでは、複数のセキュリティメカニズムを使用できます。

初期値	メカニズム	
	暗号化	認証
WEP	WEP (オープンシステム / 共有キー)	---
WEP + EAP	WEP (オープンシステム)	802.1x/EAP
WPA (パーソナルモード)	TKIP/MIC	PSK
WPA2 (パーソナルモード)	AES-CCMP	PSK
WPA (エンタープライズモード)	TKIP/MIC	802.1x/EAP
WPA2 (エンタープライズモード)	AES-CCMP	802.1x/EAP

## WEP

WEP (Wired Equivalent Privacy) は、RC4 暗号化アルゴリズムをベースにした IEEE 802.11 準拠の暗号化方式です。データ暗号化および認証のメカニズムを提供します。WEP は、キーを使用して通信全体を暗号化します。アクセスポイントが暗号化されている場合は、アクセスポイントと UTN サーバに同一の WEP キーを使用する必要があります。



一部のアクセスポイントは、ASCII テキストとして入力された WEP キーを任意の 16 進数の値に変換します。この場合、アクセスポイントの WEP キーと UTN サーバの WEP キーは一致しません。このため、16 進数の WEP キーの使用を推奨します。

## WPA/WPA2

WEP とは対照的に、WPA (Wi-Fi Protected Access) は、より高度なメカニズムでキーを交換します。交換キーは、セッション開始時のみ使用されます。以降はセッションキーが使用されます。キーは定期的に再生成されます。WPA メカニズムは、接続の開始時に認証を要求します。

「パーソナルモード」では、認証は事前共有キー (PSK : Pre Shared Key) により行われます。PSK は、8 ~ 63 の半角英数字で構成されるパスワードです。「エンタープライズモード」では、EAP 認証方法が使用されます。

認証後、個別の 128 ビットのキーがデータ暗号化に使用されます。データの暗号化には、TKIP (Temporal Key Integrity Protocol) および AES (Advanced Encryption Standard) の暗号化方式が利用できます。

## 認証

デバイスまたはユーザがネットワーク内のリソースにアクセスする前に、認証方法を使用して識別情報を確認できます。UTN サーバは、認証方法として EAP (Extensible Authentication Protocol) の様々な方式を提供します。詳細は、「認証方法を使用する方法」⇒[88](#) を参照してください。

## 選択できる作業

- 「無線ネットワークで UTN サーバ (myUTN-54) を利用する」⇒[44](#)
- 「UTN サーバを有線ネットワークに接続する」⇒[46](#)

## 無線ネットワークで UTN サーバ (myUTN-54) を利用する

無線ネットワーク内で UTN サーバを操作するには、WLAN および UTN サーバのセキュリティ設定が、無線ネットワークのセキュリティ設定と一致している必要があります。



UTN サーバを設定するには最初に、ネットワークコネクタ RJ-45 により有線ネットワークとの接続を確立する必要があります。「クイック・インストール案内」を参照してください。

### 必要事項

- ☑ UTN サーバがネットワークに接続され、電源が供給されていること。
- ☑ UTN サーバが IP アドレスにより有線ネットワークに認識されていること。⇒ 13 を参照してください。

### 手順

1. myUTN Control Center を起動します。
  2. **ネットワーク - WLAN** を選択します。  
利用可能な WLAN がネットワークリストに表示されます。UTN サーバを接続する WLAN を決定します。
  3. WLAN のパラメータを、使用する WLAN のパラメータと一致するように設定します。表 9 ⇒ 45 を参照してください
  4. **WLAN** にチェックマークを付け、UTN サーバの WLAN モジュールを有効にします。
  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。
  6. UTN サーバからネットワークケーブル (RJ-45) を取り外します。  
有線ネットワークから切断されます。
- ☞ UTN サーバが WLAN モードに自動的に切り替わります。  
WLAN との接続が確立されます。



ネットワークの変更中に、UTN サーバが新しい IP アドレスを取得するとき、myUTN Control Center への接続が中断されます。

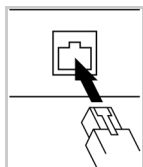
表 9：WLAN パラメータ

パラメータ	説明
モード (通信モード)	<p>通信モードを設定します。通信モードによって、UTN サーバをインストールするネットワークの構造が異なります。次の 2 つのモードを使用できます。</p> <ul style="list-style-type: none"> <li>- 「アドホック」モードでは、UTN サーバは他の WLAN クライアントと直接通信します (ピアツーピア)。</li> <li>- 「インフラストラクチャ」モードは、複数のデバイスが分散して設置された大規模な無線ネットワークの設定に適しています。デバイス間の通信は、ネットワークに接続されたアクセスポイントを介して行われます。アクセスポイントは、暗号化または認証により保護できます。</li> </ul>
ネットワーク名 (SSID)	<p>SSID を設定します。無線ネットワークの ID は、SSID (Service Set Identifier) またはネットワーク名と呼ばれます。それぞれの無線 LAN には、無線ネットワークを明確に識別するために、SSID が設定できます。SSID は、無線 LAN のアクセスポイントで設定されます。無線ネットワークにアクセスする各デバイス (PC、UTN サーバなど) は、同一の SSID を使用して設定する必要があります。</p>
ローミング	<p>ローミングの使用を有効または無効にします。ローミングとは、1 つの無線セルから次の無線セルに移動することを意味します。UTN サーバは、最も強い信号のアクセスポイントを使用します。UTN サーバが別のアクセスポイント領域に向かって移動しているとき、途中で無線セルへの接続が切断されることなく、自動的に次の無線セルに切り替えられます。「ローミング」パラメータは、「インフラストラクチャ」モードでのみ設定が可能です。</p>
ローミングレベル	<p>UTN サーバの送信電力は、「ローミングレベル」パラメータにより設定できます。初期設定値は 65-dbm です。「ローミングレベル」パラメータは、「インフラストラクチャ」モードでのみ設定が可能です。</p>
チャンネル (周波数範囲)	<p>データ通信の送信帯域となるチャンネル (周波数範囲) を設定します。本製品は、2.4GHz ISM 帯域を使用します。1 チャンネルには、22MHz の帯域幅があります。隣接するチャンネル間の距離は、5MHz です。チャンネル 3 があらかじめ設定されています。「チャンネル」パラメータは、「アドホック」モードでのみ設定が可能です。隣接するチャンネルが重複すると、干渉の原因になります。複数の WLAN を狭い範囲で操作する場合、2 つのチャンネル間に最低 5 チャンネルの距離が必要です。WLAN 製品の使用に際しては国の定める条例を遵守し、法律で認められたチャンネル以外は使用しないでください。</p>

パラメータ	説明
暗号化の方法	「WLAN セキュリティ」⇒ <a href="#">図42</a> を参照してください。
認証方法	「認証」⇒ <a href="#">図43</a> を参照してください。

## UTN サーバを有線ネットワークに接続する

有線ネットワークとの接続を確立するには、ネットワークケーブル (RJ-45) を UTN サーバに接続します。UTN サーバは、自動的に有線ネットワークに切り替わります。



## 4 デバイス設定



UTN サーバで、デバイス時間、UTN ポート、通知サービスなどの設定ができます。この章では、デバイスの設定を説明します。

### 必要な情報

- 「説明を設定する方法」⇒[48](#)
- 「デバイス時間の設定方法」⇒[48](#)
- 「UTN (SSL) ポートの設定方法」⇒[49](#)
- 「USB デバイスに名前を割り当てる方法」⇒[50](#)
- 「USB ポートの電源を制御する方法 (myUTN-80 以降のみ)」⇒[50](#)
- 「USB スキャナのデータストリームを圧縮する方法 (myUTN-130 のみ)」⇒[51](#)
- 「通知サービスの利用方法 (myUTN-80 以降のみ)」⇒[52](#)
- 「ドングルで保護されたソフトウェアへのアクセス (myUTN-80 のみ) または USB デバイスへのアクセス (myUTN-150 のみ) を VLAN で管理する方法」⇒[54](#)

## 4.1 説明を設定する方法

UTN サーバには、任意の説明を割り当てられます。説明を付けることで、ネットワーク内で使用できるデバイスの概要が理解しやすくなります。

### 手順

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** に任意の名前を入力します。
  4. **保存して再起動する** をクリックして確定します。
- 🔄 データが保存されます。



接続している USB デバイスに名前を指定する場合は、📄50 を参照してください。

## 4.2 デバイス時間の設定方法

UTN サーバのデバイス時間は、ネットワーク内のタイムサーバ (SNTP サーバ) により管理できます。タイムサーバはコンピュータネットワークを構成するデバイスで、基準時計から読み取った実時間の情報をクライアントに配信します。UTN サーバでは、タイムサーバを IP アドレスまたはホスト名で設定します。

### UTC

UTN サーバは、「UTC」(協定世界時) を基準として使用します。UTC は時間の標準として使用される基準時です。

### タイムゾーン

タイムサーバから受信する時間は、必ずしもローカルタイムゾーンに対応していないことがあります。地域や時間差 (夏時間のように国独自の制度を含む) による差異は、「タイムゾーン」パラメータを使用して対処できます。

### 必要事項

- タイムサーバがネットワークに接続されていること。

### 手順

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. タイムサーバの IP アドレスまたはホスト名を、**タイムサーバ**欄に入力します。  
(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。)
  5. **タイムゾーン**リストからローカルタイムゾーンのコードを選択します。
  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。

### 4.3 UTN (SSL) ポートの設定方法

UTN サーバとクライアント間のデータ転送には、共通ポートが使用されます。接続のタイプにより、2つのポート方式を使用できます。

#### UTN ポート

非暗号化接続とは、クライアントと UTN サーバが UTN ポート経由で通信することを意味します。ポート番号 9200 があらかじめ設定されています。

#### UTN SSL ポート

暗号化接続とは、クライアントと UTN サーバが UTN SSL ポート経由で通信することを意味します。ポート番号 9443 があらかじめ設定されています。暗号化接続を使用する場合は、ポートの暗号化を有効にしてください。☞[図94](#)を参照してください。



UTN ポートや UTN SSL ポートは、ファイアウォールで遮断しないでください。

UTN サーバのポート番号は必要に応じて変更できます。

#### 必要事項

- クライアントにインストールされた SEH UTN Manager が現在のポート番号を受信するには、SNMPv1 パラメータを有効にする必要があります。☞[図37](#)を参照してください。

#### 手順

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. **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。

## 4.4 USB デバイスに名前を割り当てる方法

USB デバイスに任意の名前を割り当てることができます。説明を付けることで、ネットワーク内で使用できるデバイスの概要が理解しやすくなります。

### 手順

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. **名前欄**に任意のデバイス名を入力します。
  4. **保存**をクリックして確定します。
- 🔄 設定が保存されます。

## 4.5 USB ポートの電源を制御する方法 (myUTN-80 以降のみ)

USB ポートの電源を有効または無効にできます。この操作で、USB デバイスへ電源を供給または遮断できます。



USB ポートへの電源は、初期設定で有効になっています。

### 利点と目的

この機能により、USB デバイスの電源を手動で切断、または再接続する必要なしにオン/オフすることができます。設定されていない状態の USB デバイスは、USB ポートの電源を遮断してから再接続することで再起動できます。

### 手順

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. **電源**にチェックマークを付けます。
  4. **保存**をクリックして確定します。
- 🔄 USB ポートの電源が、接続または遮断されます。

## 4.6 USB スキャナのデータストリームを圧縮する方法（myUTN-130 のみ）

myUTN-130 は、ハードウェアベースのデータ圧縮機能を装備しています。この機能により、USB スキャナのデータストリームを圧縮できます。圧縮処理によってデータストリーム量が縮小されると、送信量と送信時間を削減できます。

### 手順

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. **圧縮** にチェックマークを付けます。
  4. **保存** をクリックして確定します。
- ☞ USB スキャナのデータストリームが圧縮されます。

圧縮は、クライアント側で、SEH UTN Manager のデバイスプロパティの下に表示されます。

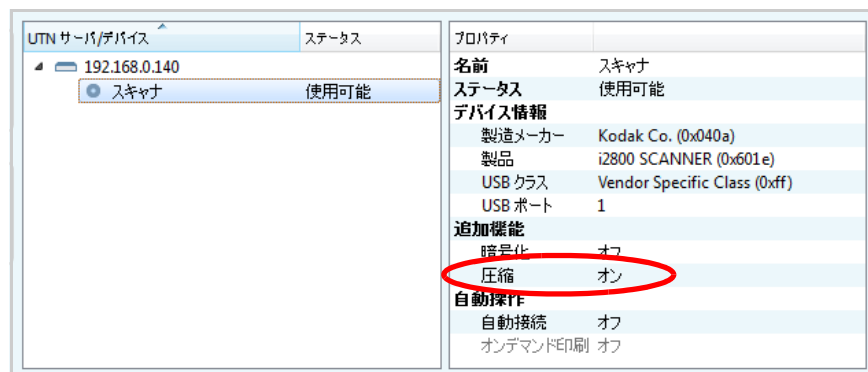


図 8：SEH UTN Manager - 圧縮

## 4.7 通知サービスの利用方法（myUTN-80 以降のみ）

UTN サーバからの通知を、電子メールや SNMP トラップの形式で受信できます。この通知サービスは、最大 4 人の受信者に対して、時間と場所を問わず様々なイベントの情報を通知します。

次のメッセージタイプが選択できます。

- ステータス通知は、受信者に UTN サーバと接続された USB デバイスの状態について定期的に通知します。
- イベント通知は、受信者に UTN サーバの特定のイベントについて、電子メールまたは SNMP トラップで通知します。通知するイベントは、次の通りです。
  - UTN サーバの再起動
  - USB デバイスの UTN サーバへの接続、または UTN サーバからの切断
  - USB デバイスのアクティブ化または非アクティブ化

### 選択できる作業

- 「ステータス通知の送信を設定する」 ⇨ 52
- 「電子メールでのイベント通知を設定する」 ⇨ 53
- 「SNMP トラップでのイベント通知を設定する」 ⇨ 53

### ステータス通知の送信を設定する

#### 必要事項

- SMTP のパラメータが UTN サーバで設定されていること。⇨ 39 を参照してください。
- DNS サーバが UTN サーバで設定されていること。⇨ 36 を参照してください。

通知サービスには、最大 2 人の電子メールの受信者を指定できます。

#### 手順

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. 時間間隔を指定します。
  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。

## 必要事項

## 電子メールでのイベント通知を設定する

- ☑ SMTPのパラメータがUTNサーバで設定されていること。⇒[39](#)を参照してください。
- ☑ DNSサーバがUTNサーバで設定されていること。⇒[36](#)を参照してください。

通知サービスには、最大2人の電子メールの受信者と、メッセージタイプを指定できます。

 手順

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. **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。

## SNMPトラップでのイベント通知を設定する

通知サービスには、最大2人のSNMPトラップの受信者と、メッセージタイプを指定できます。

 手順

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指定します。
  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. **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。

## 4.8 ドングルで保護されたソフトウェアへのアクセス（myUTN-80のみ）またはUSBデバイスへのアクセス（myUTN-150のみ）をVLANで管理する方法

UTN サーバは、VLAN（仮想ローカルエリアネットワーク）に対応しています。1つの物理ネットワークを複数のVLANに分割し管理すると、性能およびセキュリティの面で便利です。

VLANが複数のスイッチにまたがる場合は、いわゆるVLT（VLAN trunks）が使用できます。VLTは、様々なVLANからのデータを単一接続で転送する際に使用します。単独のポートとバンドルされたポートの両方が使用できます。

UTN サーバは、USBポートを使用したVLANデータの転送に対応しています。USBポートを使用して転送するには、VLANをUTNサーバに認識させ、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。

### 利点と目的

VLANは、ドングルで保護されたソフトウェアへのアクセスの管理（myUTN-80）またはUSBデバイスへのアクセスの管理（myUTN-150）に使用できます。それにより、ネットワークに参加する特定のグループに対して、ドングルで保護された一定量のソフトウェアライセンスまたはUSBデバイスを提供できます。

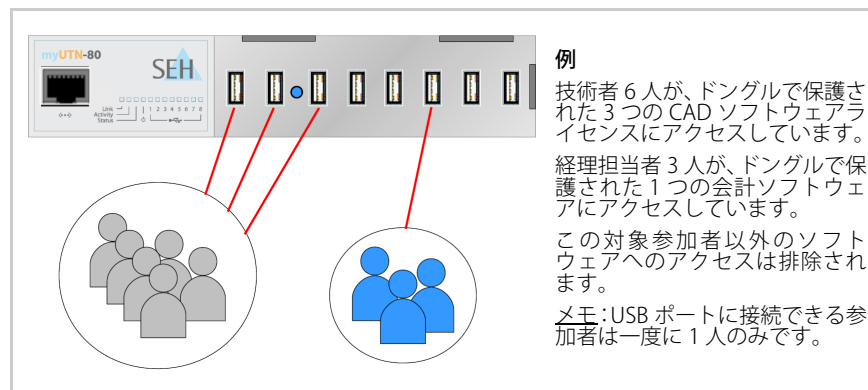


図 9 : USB ポート単位での VLAN の割り当て

### 選択できる作業

- 「VLAN を入力する」 ⇒ 55
- 「USB ポートに VLAN を割り当てる」 ⇒ 55

## VLAN を入力する

### 手順

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. VLAN パラメータを設定します。表 10 ⇨ 55 を参照してください
  4. **保存**をクリックして確定します。
- ☞ 設定が保存されます。

表 10 : IPv4 VLAN パラメータ

パラメータ	説明
VLAN	VLAN データの転送を、有効または無効にします。
IP アドレス	VLAN 内にある UTN サーバの IP アドレス
サブネットマスク	VLAN 内にある UTN サーバのサブネットマスク
VLAN ID	VLAN を識別するための ID (0 ~ 4096)。 0 = タグなしマルチホーム IP アドレス

## USB ポートに VLAN を割り当てる

### 手順

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. **保存**をクリックして確定します。
- ☞ 設定が保存されます。

## 5 SEH UTN Manager の操作



SEH UTN Manager は、USB デバイスへのアクセスを管理するソフトウェアツールです。この章では、SEH UTN Manager に USB デバイスを組み込む方法と、クライアントと USB デバイスとの接続を確立する方法を示します。

### 必要な情報

- 「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」⇒[57](#)
- 「USB デバイスを選択リストに追加する方法」⇒[58](#)
- 「USB デバイスをクライアントに接続する方法」⇒[59](#)
- 「USB デバイスとクライアント間の接続を解除する方法」⇒[60](#)
- 「使用中のデバイスを要求する方法」⇒[61](#)
- 「デバイス接続とプログラムの開始を自動化する方法」⇒[62](#)
- 「USB デバイスに関する情報を取得する方法」⇒[67](#)
- 「複数の参加者用の選択リストを管理する方法」⇒[68](#)



## 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

ネットワーク内にある UTN サーバと接続されている USB デバイスをネットワークリストに表示するには、ネットワークをスキャンする必要があります。マルチキャストを使用し、任意に範囲を指定して、ネットワークをスキャンできます。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。

### 選択できる作業

- 「検索パラメータを指定する」⇒[57](#)
- 「ネットワークをスキャンする」⇒[57](#)

### 検索パラメータを指定する

#### 必要事項

- ☑ 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。⇒[19](#) を参照してください。

#### 手順

1. SEH UTN Manager を起動します。
  2. Windows: メニューバーから、**プログラム - オプション**を選択します。  
Mac: メニューバーから、**SEH UTN Manager - 環境設定**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** をクリックして確定します。
- ☞ 設定が保存されます。

### ネットワークをスキャンする

#### 必要事項

- ☑ 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。⇒[19](#) を参照してください。

#### 手順

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。
  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 サーバおよび USB デバイスが、ネットワークリストに表示されます。

## 5.2 USB デバイスを選択リストに追加する方法

ネットワークスキャンで検出された UTN サーバは「ネットワークリスト」に表示されます。接続された USB デバイスを使用するには、そのデバイスを UTN サーバとともに SEH UTN Manager の選択リストに割り当てる必要があります。

### 必要事項

- ☑ 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。⇒ 19 を参照してください。
- ☑ 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。

### 手順

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. ネットワークリストから使用する UTN サーバを選択します。
  4. **追加**をクリックします。  
(必要に応じて、ステップ 2 と 3 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デバイスが、選択リストに表示されます。

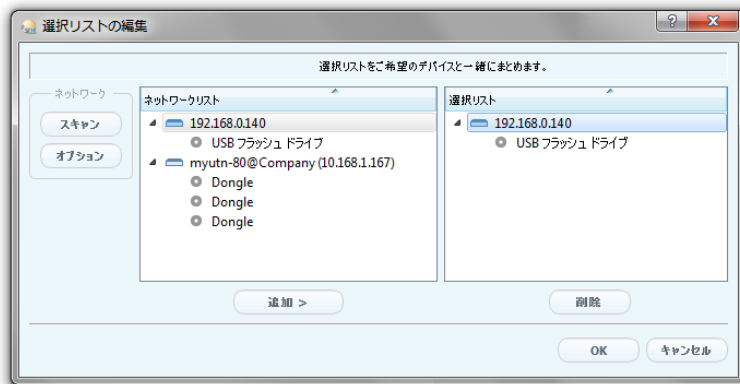


図 10 : SEH UTN Manager - 選択リストの編集



UTN サーバを、IP アドレスで指定して選択リストに直接追加するには、メニューバーから、**選択リスト - 追加**を選択します。

## 必要事項

## 5.3 USB デバイスをクライアントに接続する方法

UTN サーバに接続された USB デバイスは、クライアントに接続できます。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。

- ☑ 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。⇒ 図 19 を参照してください。
- ☑ USB デバイスが選択リストに表示されていること。⇒ 図 58 を参照してください。
- ☑ 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) を、すべて満たしていること。対象の USB デバイスをメーカー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お奨めします。
- ☑ USB デバイスが、別のクライアントに接続されていないこと。

## 📄 手順

1. SEH UTN Manager を起動します。
  2. 選択リストで、対応する USB デバイスを選択します。
  3. メニューバーから、**デバイス - 有効化** を選択します。
- 👉 接続が確立されます。



図 11 : SEH UTN Manager - デバイスの有効化

## 5.4 USB デバイスとクライアント間の接続を解除する方法

USB デバイスが不要になった場合は、USB デバイスの接続を解除します。解除すると、他のネットワーク参加者はその USB デバイスにアクセスできるようになります。

通常は、ユーザが SEH UTN Manager から接続を解除します。管理者が myUTN Control Center から接続を解除することもできます。また、一部の自動操作による接続は自動的に切断されます。(⇒[62](#))

### 選択できる作業

- 「SEH UTN Manager からデバイスの接続を解除する」⇒[60](#)
- 「myUTN Control Center からデバイスの接続を解除する」⇒[60](#)

### 必要事項

#### SEH UTN Manager から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。⇒[19](#) を参照してください。

#### 手順

1. SEH UTN Manager を起動します。
2. 選択リストで、対応する USB デバイスを選択します。
3. メニューバーから、**デバイス - 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

#### 手順

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. セキュリティのクエリを確認します。
- ☞ 接続が解除されます。

## 5.5 使用中のデバイスを要求する方法

他のユーザが使用しているデバイスを要求することができます。

他のユーザは、ポップアップウィンドウで要求の通知を受け取ると、要求された USB デバイスへの接続を終了できます。デバイスが共有されている場合は、USB デバイスと要求元のクライアント間の接続が自動的に確立します。

### 必要事項

- ☑ 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。⇒[図39](#)を参照してください。
- ☑ SEH UTN Manager が、USB デバイスを使用してい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。⇒[図39](#)を参照してください。
- ☑ SEH UTN Manager が両方のクライアントで実行されていること。
- ☑ USB デバイスが選択リスト上に表示されていること。⇒[図39](#)を参照してください。

### 手順

1. 選択リストで、対応する USB デバイスを選択します。
  2. メニューバーから、**デバイス - 要求**を選択します。
- 🔄 デバイス要求が、そのデバイスを使用しているユーザに送信されます。

## 選択できる作業

## 5.6 デバイス接続とプログラムの開始を自動化する方法

デバイス接続とプログラムの開始は、多くの方法で自動化できます。それらは、様々な自動操作によって実現できます。

- 「SEH UTN Manager プログラムを起動後にデバイスを自動的にアクティブにする（自動接続）」 ⇨ 62
- 「設定時間後、デバイスへの接続を自動的に切断する（自動切断）」 ⇨ 63
- 「印刷ジョブ受信時に USB デバイスとクライアント間の接続を自動的に作成する（オンデマンド印刷）」 ⇨ 64
- 「UTN アクションを作成する：SEH UTN Manager インタフェースを使わずに自動化されたデバイス接続とプログラムの開始」 ⇨ 65
- 「付加ツール「utnm.exe」を使用する」 ⇨ 131

### SEH UTN Manager プログラムを起動後にデバイスを自動的にアクティブにする（自動接続）

この機能により、SEH UTN Manager が起動すると、デバイス接続が自動的にアクティブになります。



設定できるのは管理者のみです。

## 必要事項

- ☑ 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。⇨ 19 を参照してください。
- ☑ USB デバイスが選択リストに表示されていること。⇨ 58 を参照してください。

#### 手順

1. SEH UTN Manager を起動します。
  2. 選択リストで、対応する USB デバイスを選択します。
  3. メニューバーから、**デバイス - 設定**を選択します。
  4. 「SEH UTN Manager プログラムの起動後、デバイスが自動的にアクティブになります。（自動接続）」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。

## 設定時間後、デバイスへの接続を自動的に切断する（自動切断）

USB デバイスへの接続は、この機能により設定時間が過ぎると自動的に切断できます。設定した時間内で 1 回のみ接続を延長することも任意で有効にできます。この設定は、UTN サーバ上のすべての USB デバイスに適用されます。

データのロスやエラーを防止するため、設定時間の 2 分前に、ユーザに注意メッセージが送信されます。延長設定が有効な場合は、延長の承認または拒否を確認するメッセージも表示されます。



自動切断後にそのデバイスが利用できるかどうか通知を受け取るように設定できます。そのためには、デバイスが利用できる場合の通知を設定してください。⇒[図67](#)を参照してください。

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、アイドル時間をなくします。



設定できるのは管理者のみです。

### 必要事項

- ☑ 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。⇒[図39](#)を参照してください。
- ☑ 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。⇒[図39](#)を参照してください。

### 手順

1. SEH UTN Manager を起動します。
2. Windows: メニューバーから、**プログラム - オプション**を選択します。  
Mac: メニューバーから、**SEH UTN Manager - 環境設定**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. **デバイスの自動切断**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**（10～525 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。

## 印刷ジョブ受信時に USB デバイスとクライアント間の接続を自動的に作成する（オンデマンド印刷）

印刷ジョブを受信すると、USB デバイス（プリンタまたは複合機）とクライアントとの接続が自動的に確立されます。印刷ジョブが完了すると、接続は自動的に解除されます。



設定できるのは管理者のみです。

### 必要事項

- ☑ 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。⇒[■19](#)を参照してください。
- ☑ USB デバイスが選択リストに表示されていること。⇒[■58](#)を参照してください。



### 手順

1. SEH UTN Manager を起動します。
  2. 選択リストで、対応する USB デバイスを選択します。
  3. メニューバーから、**デバイス - 設定**を選択します。
  4. **オンデマンド印刷**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。



この機能を使用するには、クライアント側でプリンタの設定（ドライバのインストール）をする必要があります。



## UTN アクションを作成する: SEH UTN Manager インタフェースを使わずに自動化されたデバイス接続とプログラムの開始

UTN アクションを作成できます。UTN アクションは、デバイス接続を自動的にアクティブまたは非アクティブにするプログラムです。また、UTN アクションはデバイス接続と連携して、アプリケーションを自動的に起動または終了します。

UTN アクションに設定された処理は、ファイルを実行す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ので、ユーザが SEH UTN Manager インタフェースを起動する必要はありません。すなわち、UTN アクションはフルバージョンおよびミニマルバージョンで使用できます。

SEH UTN Manager のウィザードに従って、UTN アクションを作成できます。次の UTN アクションが作成できます。

- ウィザードは デバイスをアクティブにするための UTN アクションを 1 つ、また非アクティブするための UTN アクションを 1 つ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デバイスをアクティブにするアクションを自動的に作成します。また、アプリケーションを終了したあとでデバイスを非アクティブするように指定することもできます。
- 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 アクションが作成できます。次の UTN アクションを作成できます。
  - デバイスをアクティブまたは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。
  - アプリケーションを起動して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デバイス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。スクリプトが自動的に作成されると、スクリプトを編集できます。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。

### 必要事項

- ☑ 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。⇒ 39 を参照してください。
- ☑ USB デバイスが選択リストに表示されていること。⇒ 58 を参照してください。

## 📄 手順

1. SEH UTN Manager を起動します。
  2. 選択リストで、USB デバイスを選択します。
  3. メニューバーから、**デバイス - 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 アクションを実行できます。

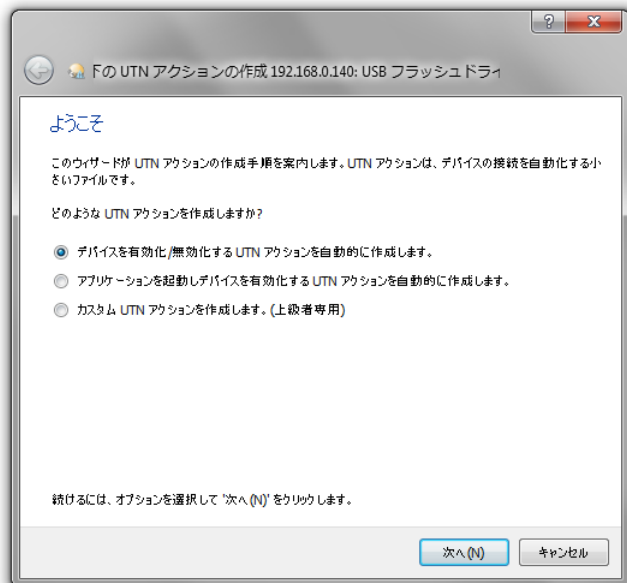


図 12 : UTN アクションの作成ダイアログ

- ヒント 1** 保存後、ショートカット (Windows) または app (Mac) は任意の場所に移動して名前を変更できます。
- ヒント 2** 上級者専用 (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) : Windows では、ショートカットの対象にコマンドラインが含まれています。コマンドラインは必要に応じて編集できます。Mac では、app のスクリプトを必要に応じて編集できます (パス: Contents/Resources/script)。
- ヒント 3** 上級者専用 (スクリプト) : 作成したスクリプトは、簡単なテキストエディタで編集できます。

## 5.7 USB デバイスに関する情報を取得する方法

USB デバイスのステータス情報を参照できます。自動通知を設定することもできます。USB デバイスが使用可能になると、通知されます。

### 選択できる作業

- 「ステータス情報を表示する」⇒[図67](#)
- 「メッセージを設定する（現在、Windows のみの対応）」⇒[図67](#)

### ステータス情報を表示する

#### 必要事項

- ☑ 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。⇒[図19](#)を参照してください。
- ☑ USB デバイスが選択リストに表示されていること。⇒[図58](#)を参照してください。

#### 手順

1. SEH UTN Manager を起動します。
2. 選択リストで、対応する USB デバイスを選択します。
- ☞ ステータス情報が「プロパティ」領域に表示されます。

### メッセージを設定する（現在、Windows のみの対応）

#### 必要事項

- ☑ 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。⇒[図19](#)を参照してください。
- ☑ USB デバイスが選択リストに表示されていること。⇒[図58](#)を参照してください。

#### 手順

1. SEH UTN Manager を起動します。
2. 選択リストで、対応する USB デバイスを選択します。
3. メニューバーから、**デバイス - 設定**を選択します。  
**デバイス設定**ダイアログが表示されます。
4. **メッセージ**の下のオプション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。  
ネットワーク参加者が USB デバイスへの接続を無効にすると、「デスクトップ通知」が生成されます。

## 5.8 複数の参加者用の選択リストを管理する方法

### 選択リストの役割

選択リストは、SEH UTN Manager の主要部分です。ネットワークに組み込まれたすべての UTN サーバと接続された USB デバイスを、その状態とともに表示します。表示された USB デバイスは、クライアントに接続して使用できます。選択リストは、必要なデバイスの追加や削除など、必要に応じて編集および設定することができます。

選択リストは、SEH UTN Manager.ini ファイルとして保存されます。

選択リストには、次の 2 種類があります。

- グローバル選択リスト
- ユーザ固有の選択リスト

### 利点と目的

管理者は、選択リストの種類をユーザ管理と組み合わせて使用し、ネットワーク上で利用可能な UTN サーバへのアクセスを制御できます。

すべてのユーザは最初に同じ選択リストを使用します。

または、各ユーザはユーザ固有の選択リストを使用できます。アクセスを制御するには、事前設定された選択リストのファイルをユーザ固有のディレクトリに配置します。 .ini ファイルへの書き込み権限を無効にすることで、各ユーザに対して SEH UTN Manager の機能の利用を制限、制御できます。

次に、選択リストの種類を詳細に説明します。

### グローバル選択リスト

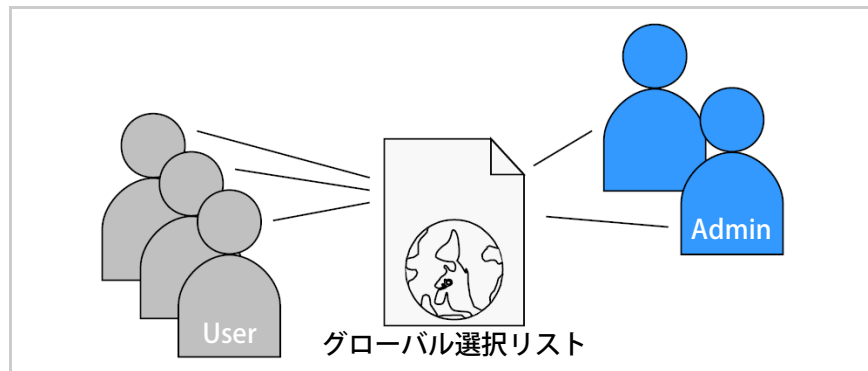


図 13：グローバル選択リスト

### グローバル選択リストの特長

## ユーザ固有の選択リスト

- 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。
- ユーザがアクセスできるのは、選択リストに表示されたデバイスのみです。
- デバイスの使用権限がないユーザーは選択リストに表示されず、デバイスにアクセスできません。
- 選択リストは、管理者のみが編集できます。

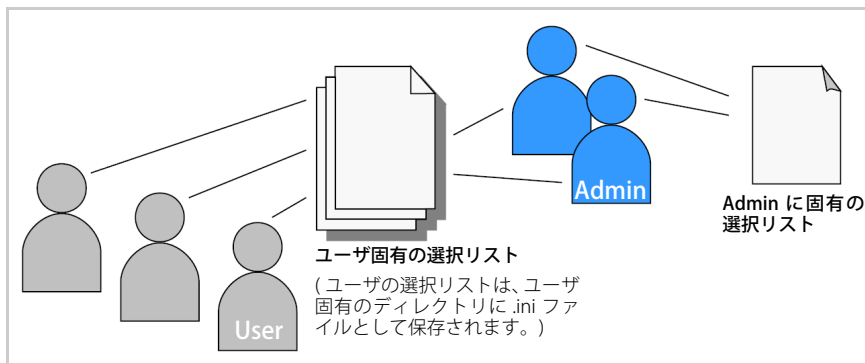


図 14：ユーザ固有の選択リスト

### ユーザ固有の選択リストの特長

- 各ユーザは、自分専用の選択リストを所有します。管理者は全員、同じ選択リストを所有します。
- 選択リストは、管理者または書き込み権限のあるユーザのみが編集できます。
- 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。)
- 各ユーザの選択リストは、次の場所に.iniファイルで保存されます。  
Windows: %APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini  
Mac: \$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini

%APPDATA% は、Windows のユーザ用環境変数です。カレントユーザのパスは、コマンドラインを使用して次のように設定できます。echo %APPDATA%

例:

**Windows XP:**

echo %APPDATA% は C:\Users\User name\AppData\Roaming を返します。

+

\SEH Computertechnik GmbH\SEH UTN Manager.ini

**.ini ファイルのフルパス:**

C:\Users\User name\AppData\Roaming\SEH Computertechnik GmbH\SEH UTN Manager.ini

\$HOME は、Mac のユーザフォルダ用環境変数です。カレントユーザのパスは、コマンドラインを使用して次のように設定できます。echo \$HOME

例:

**Mac OS X 10.7.5 (Lion):**

echo \$HOME は /Users/User name を返します。

+

.config/SEH Computertechnik GmbH/SEH UTN Manager.ini

**.ini ファイルのフルパス:**

/Users/User name/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini

## 選択できる作業

- 「すべてのユーザにグローバル選択リストを提供する」 ⇨ 70
- 「ユーザ固有の選択リストを提供する」 ⇨ 71
- 「事前設定の選択リストをユーザに提供する」 ⇨ 71
- 「ユーザ固有の選択リストを保護する」 ⇨ 72

## 必要事項

### すべてのユーザにグローバル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。⇨ 19 を参照してください。

#### 手順

1. 管理者ユーザーで、SEH UTN Manager を起動します。
2. 選択リストを構成します。「USB デバイスを選択リストに追加する方法」⇨ 58 を参照してください。

## 必要事項

3. Windows: メニューバーから、**プログラム - オプション**を選択します。  
Mac: メニューバーから、**SEH UTN Manager - 環境設定**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。

## ユーザ固有の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。⇒[19](#) を参照してください。

 手順

1. 管理者ユーザーで、SEH UTN Manager を起動します。
  2. Windows: メニューバーから、**プログラム - オプション**を選択します。  
Mac: メニューバーから、**SEH UTN Manager - 環境設定**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。
- ☞ 設定が保存されます。各ユーザは、自分専用の選択リストを使用します。ユーザの選択リストは、ユーザ固有のディレクトリに .ini ファイルとして保存されます。「ユーザ固有の選択リスト」⇒[69](#) を参照してください。




---

管理者は、1 つの選択リストを共有します。

---

## 必要事項

## 事前設定の選択リストをユーザに提供する

- 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。⇒[19](#) を参照してください。

 手順

1. 管理者ユーザーで、SEH UTN Manager を起動します。

2. ユーザ用の選択リストを構成します。「USB デバイスを選択リストに追加する方法」⇒[図58](#)を参照してください。
  3. Windows: メニューバーから、**プログラム - オプション**を選択します。  
Mac: メニューバーから、**SEH UTN Manager - 環境設定**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. **ユーザ選択リスト**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。
  7. 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、次のパスに保存します。  
Windows: %APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini  
Mac: \$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini  
(「ユーザ固有の選択リスト」⇒[図69](#)を参照してください。)
- ☞ 各ユーザは、事前設定された自分専用の選択リストにアクセスします。

## ユーザ固有の選択リストを保護する

事前設定されたユーザ固有の選択リストを使用する場合は、ユーザが選択リストを変更しないようにリストを保護することをお奨めします。

ユーザの選択リストは、次の場所に「SEH UTN Manager.ini」ファイルで保存されています。

Windows: %APPDATA%\SEH Computertechnik GmbH\SEH UTN Manager.ini

Mac: \$HOME/.config/SEH Computertechnik GmbH/SEH UTN Manager.ini

(「ユーザ固有の選択リスト」⇒[図69](#)を参照してください。)

オペレーティングシステムのコントロールパネルから、.ini ファイルを読み取り専用ファイルにします。これを実行するには、クライアント側の管理者権限が必要です。

「SEH UTN Manager.ini」ファイルを読み取り専用にすると、選択リストで使用できる SEH UTN Manager の機能はすべて無効になります。



## 6 セキュリティ



UTN サーバに最適なセキュリティを確保するために、多くのメカニズムが利用できます。この章では、これらのセキュリティメカニズムを使用する方法について説明します。

次のセキュリティメカニズムは、必要に応じて設定し、アクティブにすることができます。

### 必要な情報

- 「SSL/TLS 接続の暗号化レベルを設定する方法」⇒[73](#)
- 「myUTN Control Center へのアクセスを制御する方法」⇒[75](#)
- 「UTN サーバへのアクセスを制御する方法 (TCP ポートアクセス制御)」⇒[77](#)
- 「USB デバイスへのアクセスを制御する方法 (myUTN-80 以降のみ)」⇒[79](#)
- 「証明書の正しい使用方法」⇒[82](#)
- 「認証方法を使用する方法」⇒[88](#)
- 「データ転送を暗号化する方法」⇒[94](#)

### 6.1 SSL/TLS 接続の暗号化レベルを設定する方法

UTN サーバ上の次の接続は、SSL/TLS で暗号化できます。

- 電子メール：POP3 (⇒[39](#))
- 電子メール：SMTP (⇒[39](#))
- myUTN Control Center への Web アクセス：http (⇒[75](#))
- 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 ポート (⇒[94](#))

### 暗号化レベル

暗号化強度、さらに接続の安全性は暗号化レベルで設定します。

### 暗号スイート

各暗号化レベルは、いわゆる暗号スイートの集まりです。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す。暗号スイートは、暗号強度 (ビット単位) に応じてグループ化され、暗号化レベルを形成します。UTN サーバが対応する暗号スイート、すなわち暗号化レベルを形成する暗号スイートは使用されているプロトコル (SSLv2、SSLv3、TLSv1) により決定します。

## 接続の確立

セキュアな接続を確立する場合、対応する暗号スイートのリストを通信相手に送信し、使用する暗号スイートを取り決めます。既定では、当事者双方で対応する暗号スイート中の最も強力なスイートが使用されます。双方で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。



接続を正常に確立するためには、UTN サーバの通信相手（例えばブラウザ）は選択した暗号レベルの暗号スイートに対応している必要があります。問題が発生する場合は、別のレベルを選択、または UTN サーバのパラメータをリセットしてください。⇒98 を参照してください。

次の暗号化レベルが選択できます。

- **クライアント互換**：暗号強度 40 ～ 256 ビットの暗号スイートを使用します。
- **低レベル**：低レベルの暗号強度 56 ビットの暗号スイートのみを使用します。（高速接続）
- **中レベル**：暗号強度 128 ビットの暗号スイートのみを使用します。
- **高レベル**：高い暗号強度 128 ～ 256 ビットの暗号スイートのみを使用します。（低速接続）

### 手順

1. myUTN Control Center を起動します。
2. **セキュリティ - SSL 接続**を選択します。
3. **暗号化領域**から、暗号化レベルを選択します。
4. **保存して再起動する**をクリックして確定します。
5. 設定が保存されます。



個別の SSL 接続状態に関する詳細情報（暗号スイートなど）は、**SSL 接続の状態 - 詳細**から、詳細ページを参照してください。

## 6.2 myUTN Control Center へのアクセスを制御する方法

myUTN Control Center に対して、Web および SNMP を使用した管理者権限によるアクセスを保護できます。

### 選択できる作業

- 「許可された Web 接続の種類を指定する」 ⇨ 75
- 「パスワードにより Web アクセスを保護する」 ⇨ 76
- 「VLAN アドレスからの Web アクセスを許可または拒否する (myUTN-80 および myUTN-150 のみ)」 ⇨ 76
- 「VLAN アドレスからの SNMP アクセスを許可または拒否する (myUTN-80 および myUTN-150 のみ)」 ⇨ 77



myUTN Control Center は、SNMP のセキュリティ概念で保護することもできます。この概念には、ユーザグループとアクセス権の管理が含まれています。詳細は、「SNMP の設定方法」⇨37 を参照してください。

### 許可された Web 接続の種類を指定する

#### 接続の種類 (HTTP/HTTPS)

myUTN Control Center への Web アクセスは、許可する接続の種類 (HTTP/HTTPS) を選択することで安全を確保できます。

HTTPS のみで接続を許可する場合、myUTN Control Center への管理者権限による Web アクセスは、SSL/TLS によって保護されます。暗号強度は暗号化レベルで設定されます ⇨73。

SSL/TLS は、UTN サーバの識別情報を確認するための証明書を要求します。いわゆる「ハンドシェイク」の際に、クライアントはブラウザを介して証明書を要求します。この証明書は、ブラウザ側での受諾が必要です。ご使用のブラウザソフトウェアの説明書を参照してください。SSL/TLS 接続が必要な URL は「https」で始まります。

#### 手順

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. **Web** 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. **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。

## パスワードにより Web アクセスを保護する

myUTN Control Center を不正な Web アクセスから保護するために、パスワードを使用できます。パスワードを設定した場合、myUTN Control Center にアクセスすると、スタートページのみが表示され、先に進むことができません。メニューの項目を選択すると、パスワードを入力するように求められます。



また限定できないユーザ名を入力するよう求められます。パスワードの入力要求時は、この欄を空欄のままにしておきます。



### 手順

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. **Web** 領域で、**パスワード**欄にパスワードを入力します。
  4. パスワードを再入力します。
  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。

## VLAN アドレスからの Web アクセスを許可または拒否する (myUTN-80 および myUTN-150 のみ)

VLAN アドレスから myUTN Control Center への、管理者権限による Web アクセスを拒否できます。



### 手順

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. **Web** 領域で、**VLAN アクセス**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. **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。

## VLAN アドレスからの SNMP アクセスを許可または拒否する (myUTN-80 および myUTN-150 のみ)

VLAN アドレスから myUTN Control Center への、管理者権限による SNMP アクセスを拒否できます。

### 手順

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. **SNMP 領域の VLAN アクセス**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. **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。

## 6.3 UTN サーバへのアクセスを制御する方法 (TCP ポートアクセス制御)

### TCP ポートアクセス制御

UTN サーバへのアクセスを制御できます。これを実行すると、UTN サーバの様々な TCP ポートタイプをロックします。UTN サーバへのアクセスが許可されたネットワーク要素は、例外に設定してロック対象から除外できます。UTN サーバは、例外として設定されたネットワーク要素から送信されるデータパケットのみを受け入れます。

### セキュリティレベル

ロック対象のポートタイプは、「セキュリティレベル」領域で設定する必要があります。次のカテゴリを選択できます。

- UTN アクセスのロック (UTN ポートのロック)
- TCP アクセスのロック (TCP ポート: HTTP/HTTPS/UTN のロック)
- すべてをロック (IP ポートのロック)

### 例外

ネットワーク要素 (クライアント、DNS サーバ、SNTP サーバなど) をポートのロックから除外するには、これらを例外として設定します。この場合、アクセスが許可されたネットワーク要素の IP アドレスまたは MAC アドレス (ハードウェアアドレス) を「例外」領域に入力する必要があります。次の点に留意してください。

- 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設定できます。

## テストモード

「テストモード」により、アクセス保護の設定を確認できます。テストモードがアクティブな場合、UTN サーバが再起動されるまで、アクセス保護は有効のままです。再起動すると、アクセス保護は無効になります。



「テストモード」オプションは、初期設定でアクティブになっています。テスト後は、アクセス保護を継続するために、テストモードを非アクティブにする必要があります。

 手順

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、対象の保護を選択します。
5. **例外**領域で、ポートのロック対象から除外するネットワーク要素を設定します。IP アドレスまたは MAC 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。
6. **テストモード**がオンであることを確認してください。
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が有効になります。
8. ポートアクセスと、UTN サーバの設定が可能であることを確認してください。



myUTN Control Center から UTN サーバにアクセスできなくなった場合は、デバイスを再起動してください。⇒ 102 を参照してください。

9. **テストモード**のチェックマークを外します。
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。ポートアクセス制御がアクティブになります。  
ポートへのアクセスが制限されます。

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

UTN サーバに接続された USB デバイスへのアクセスは、USB ポートで制御できます。各 USB ポートには、2 つのセキュリティ方法が利用できます。両方の方法を組み合わせて使用することも可能です。

### USB ポートキー制御

キー制御に使用する USB ポートのキーは、myUTN Control Center から指定します。キーを入力すると、USB ポートに接続された USB デバイスは、不要なアクセスから保護されます。

USB デバイスは、SEH UTN Manager に表示されなくなります。この設定は、ユーザが USB デバイスへの変更や USB デバイスとの接続ができなくなることを意味します。

USB デバイスを使用可能にするには、クライアントの USB ポートにキーを入力する必要があります。これは、SEH UTN Manager から実行します。myUTN Control Center のキーを変更すると、ユーザは再度、USB デバイスへのアクセス許可を失います。

### USB ポートのデバイス 割り当て

デバイス割り当てとは、myUTN Control Center により、USB デバイスを各 USB ポートに永続的に割り当てることです。これにより、USB デバイスは割り当てられた USB ポートのみで動作します。

デバイス割り当てによって、USB ポートおよび USB デバイスのセキュリティを確実に設定します。割り当てられた USB デバイス以外のデバイスが USB ポートに接続された場合、そのデバイスは操作できません。

### 選択できる作業

- 「USB デバイスへのアクセスを遮断する」 ⇨ 80
- 「USB デバイスへのアクセスブロックを解除する」 ⇨ 80
- 「USB ポートのデバイス割り当てを指定する」 ⇨ 81
- 「USB ポートアクセス制御を無効にする」 ⇨ 81

## USB デバイスへのアクセスを遮断する

USB デバイスへのアクセスを制御する場合、myUTN Control Center から USB ポートのキーを指定する必要があります。

### 手順

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. 対応する USB ポートの**方式**リストから、**ポートキー制御**のエントリを選択します。
  4. **キーの生成**をクリック、または**キー**の欄に任意のキーを入力します (半角 64 文字以内)。
  5. **保存**をクリックして確定します。
- ☞ 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。

## USB デバイスへのアクセスブロックを解除する

ユーザが、USB ポートキー制御で保護された USB デバイスにアクセスするには、SEH UTN Manager からクライアントに適切なキーを入力する必要があります。

### 手順

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. **UTN サーバ**のメニューバーから、**USB ポートキーの設定**のコマンドを選択します。  
**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 ポートにキーを入力します。
  5. **OK**をクリックします。
- ☞ USB デバイスへのアクセスが共有されます。USB デバイスが選択リストに表示され、操作できるようになります。



## USB ポートのデバイス割り当てを指定する

UTN サーバの USB デバイスを切り替えて、任意な操作ができないように、USB デバイスを永続的に USB ポートに割り当てることができます。

### 手順

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. 対応する USB ポートの**方式**リストから**デバイス割り当て**のエントリを選択します。
  4. **保存**をクリックして確定します。
- 🔗 設定が保存されます。「USB ポート」の下に表示された USB デバイスのみが、その USB ポートで操作できるようになります。

USB ポートに、新たに接続された USB デバイスの割り当てを作成する場合は、「デバイスの再割り当て」をクリックしてください。

## USB ポートアクセス制御を無効にする

USB ポートへのアクセス制御を無効にすると、接続された USB デバイスへのアクセス制御も無効になります。

### 手順

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. 対応する USB ポートの**方式**リストから --- エントリを選択します。
  4. **保存**をクリックして確定します。
- 🔗 USB ポートアクセス制御が無効になります。接続された USB デバイスが操作できます。

## 6.5 証明書の正しい使用方法

UTN サーバには独自の証明書管理機能があります。この章では、推奨される証明書の使用方法について説明します。

### 証明書の役割

証明書は、TCP/IP ベースのネットワークでデータを暗号化し、通信相手を認証するために使用できます。証明書は、キー（公開キー）と署名を含む電子メッセージです。

### 利点と目的

証明書を使用すると、様々なセキュリティメカニズムを利用できます。UTN サーバの証明書には、次のような目的があります。

- ネットワーク内で UTN サーバの識別情報を確認する。「EAP-TLS を設定する」⇒[79](#) を参照してください。
- myUTN Control Center への管理者権限によるアクセスが HTTPS (SSL/TLS) で保護されている場合、UTN サーバ/クライアントを認証する。



証明書を使用する場合は、UTN サーバ上の証明書が不正ユーザにより削除されないよう、myUTN Control Center への管理者権限アクセスをパスワードで保護することを推奨します。⇒[76](#) を参照してください。

### 使用できる証明書

UTN サーバでは、自己署名証明書と CA 証明書の両方を使用できます。これらの証明書は次のように識別できます。

- 出荷時には、自己署名証明書（**デフォルト証明書**）が UTN サーバに保存されています。可能な限り迅速に、デフォルト証明書を自己署名証明書または CA 証明書に交換することをお奨めします。
- **自己署名証明書**には、UTN サーバによって作成されたデジタル署名が含まれます。
- **CA 証明書**は、認証機関（CA）によって署名された証明書です。
- CA 証明書の信頼性は、認証機関が発行した**ルート証明書**によって検証できます。ルート証明書は、ネットワークの認証サーバに保存されます。
- **S/MIME 証明書** (\*.pem ファイル) は、UTN サーバが送信する電子メールに署名して、それを暗号化するために使用されます。対応する秘密キーは自らの証明書として、PKCS#12 フォーマット (\*.p12 ファイル) で目的の電子メール用プログラム (Mozilla Thunderbird、Microsoft Outlook など) にあらかじめインストールする必要があります。電子メールが暗号化されている場合、この秘密キーにより検証されて表示されます。(myUTN-80 以降のみ)

次の証明書を UTN サーバに同時にインストールできます。

- 自己署名証明書 ×1
- CA 証明書、または PKCS#12 証明書 ×1
- ルート証明書 ×1
- S/MIME 証明書 ×1 (myUTN-80 以降のみ)

CA 証明書の認証要求を生成することもできます。すべての証明書は個別に削除できます。既存の証明書は、新しい証明書をインストールまたは生成すると上書きされます。

PKCS#12 証明書は、一度も認証要求がない、または CA 証明書がインストールされていない場合のみインストールできます。

認証情報ステータス		
自己署名証明書:	インストール済み	 
CA 認証情報:	未インストール	
認証要求:	作成済み	 
S/MIME 証明書:	未インストール	
ルート証明書:	未インストール	

図 15 : myUTN Control Center - 証明書


## 選択できる作業

- 「証明書を表示する」 ⇒ 84
- 「自己署名証明書の作成方法」 ⇒ 84
- 「CA 証明書の認証要求を作成する」 ⇒ 85
- 「CA 証明書を UTN サーバに保存する」 ⇒ 86
- 「ルート証明書を UTN サーバに保存する」 ⇒ 86
- 「PKCS#12 証明書を UTN サーバに保存する」 ⇒ 87
- 「S/MIME 証明書を UTN サーバに保存する (myUTN-80 以降のみ)」 ⇒ 87
- 「証明書を削除する」 ⇒ 88

## 証明書を表示する

UTN サーバにインストールされた証明書や認証要求は、表示し参照することができます。

### 手順

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. 証明書のアイコン  を選択します。
- 🔗 証明書が表示されます。

## 自己署名証明書の作成方法



すでに自己署名証明書が UTN サーバで作成されている場合、最初にその証明書を削除してください。⇒[88](#) を参照してください。

### 手順

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. **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 11 ⇒[84](#) を参照してください
  5. **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。完了までに数分かかることがあります。

表 11：証明書作成用パラメータ

パラメータ	説明
共通名	証明書を明確に識別するために使用します。UTN サーバへの証明書の割り当てを明確に示す、UTN サーバの IP アドレスやホスト名の使用をお奨めします。入力できる文字数は、最大 64 半角文字です。
電子メールアドレス	電子メールアドレスを指定します。入力できる文字数は、最大 40 半角文字です。(任意入力)
組織名	UTN サーバを使用する会社を指定します。入力できる文字数は、最大 64 半角文字です。
組織単位	会社の部課、係名を指定します。入力できる文字数は、最大 64 半角文字です。(任意入力)

パラメータ	説明
場所	会社が本拠を置く地域を指定します。入力できる文字数は、最大 64 半角文字です。
都道府県名	会社が本拠を置く都道府県（日本以外の場合は州等）を指定します。入力できる文字数は、最大 64 半角文字です。（任意入力）
ドメインコンポーネント	付加属性の入力ができます。（任意入力）
国	会社が本拠を置く国を指定します。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
発行日時	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。
期限切れ日時	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。
RSA key length	- 使用する RSA キー長を設定します。 - 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）

## CA 証明書の認証要求を作成する

CA 証明書を使用する準備として、認証機関に送信する認証要求を UTN サーバで作成します。認証機関は、認証要求に基づいて CA 証明書を作成します。証明書は、Base64 フォーマットで作成する必要があります。



すでに認証要求が UTN サーバで作成されている場合、最初にその認証要求を削除してください。⇒ 88 を参照してください。

### 手順

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 11 ⇒ 84 を参照してください
5. **要求の作成**をクリックします。認証要求の作成が開始されます。完了までに数分かかることがあります。
6. **アップロード**を選択して、認証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、認証要求として認証機関に送信します。  
受け取った CA 証明書は、UTN サーバに保存してください。⇒[86](#) を参照してください。

## CA 証明書を UTN サーバに保存する



すでに CA 証明書が UTN サーバにインストールされている場合、その証明書は上書きされます。

### 必要事項

- 認証要求が、当日より前の日付で作成されていること。⇒[85](#) を参照してください。
- 証明書は、Base64 フォーマットで作成されていること。

### 手順

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. **要求された認証情報** をクリックします。
  4. **参照** をクリックします。
  5. CA 証明書を指定します。
  6. **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。

## ルート証明書を UTN サーバに保存する

UTN サーバは、ネットワーク内の識別情報を検証する複数の認証方法を提供します。認証方法の「EAP-TLS」を使用する場合、認証サーバ (RADIUS) のルート証明書を UTN サーバにインストールする必要があります。⇒[90](#) を参照してください。



すでにルート証明書が UTN サーバにインストールされている場合、その証明書は上書きされます。

### 必要事項

- 証明書は、Base64 フォーマットで作成されていること。

### 手順

1. myUTN Control Center を起動します。

## 必要事項

2. **セキュリティ - 証明書**を選択します。
  3. **ルート証明書**を選択します。
  4. **参照**をクリックします。
  5. ルート証明書を入力します。
  6. **インストール**をクリックします。
- ☞ ルート証明書が UTN サーバに保存されます。

## PKCS#12 証明書を UTN サーバに保存する

PKCS#12 形式の証明書は、秘密キーとその証明書を保存し、パスワードにより保護するために使用します。



すでに PKCS#12 証明書が UTN サーバにインストールされている場合、その証明書は上書きされます。

- 証明書は、Base64 フォーマットで作成されていること。
- 認証要求が存在しないこと。認証要求の削除方法は、☞ 88 を参照してください。
- CA 証明書がインストールされていないこと。CA 証明書の削除方法は、☞ 88 を参照してください。

### 手順

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. **参照**をクリックします。
  5. PKCS#12 証明書を指定します。
  6. パスワードを入力します。
  7. **インストール**をクリックします。
- ☞ PKCS#12 証明書が UTN サーバに保存されます。

## S/MIME 証明書を UTN サーバに保存する (myUTN-80 以降のみ)

S/MIME 証明書 (\*.pem ファイル) は UTN サーバが送信する電子メールに署名して、それを暗号化するために使用されます。




すでに S/MIME 証明書が UTN サーバにインストールされている場合、その証明書は上書きされます。

#### 手順

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. **参照**をクリックします。
  5. S/MIME 証明書を指定します。
  6. **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。

### 証明書を削除する

#### 手順

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. 削除する証明書の  アイコンを選択します。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。

## 6.6 認証方法を使用する方法

認証を使用することで、ネットワークを不正アクセスから保護できます。UTN サーバは、様々な認証方式に対応できます。この節では、対応する方式と、これらの方式を UTN サーバに設定する方法を説明します。

#### IEEE 802.1x の役割

IEEE 802.1x 標準は、各種の認証プロトコルおよび鍵管理プロトコルの基本構造を提供します。IEEE 802.1x により、ネットワークへのアクセスを制御できます。ユーザは、ネットワークデバイスからネットワークにアクセスする前に、ネットワーク内で認証される必要があります。認証に成功すると、ネットワークへのアクセスが開放されます。

#### EAP の役割

標準 IEEE 802.1x は、EAP (拡張認証プロトコル) に基づいています。EAP は、多くの認証方式のための汎用プロトコルです。EAP により、ネットワークデバイスと認証サーバ (RADIUS) 間で、標準化された認証方式を使用できます。最初に使用する認証方式 (TLS、PEAP、TTLS など) を決



## RADIUS の役割

定し、それを関連するすべてのネットワークデバイスに設定する必要があります。

RADIUS (Remote Authentication Dial-In User Service) とは、認証およびアカウントの管理システムであり、ユーザのログイン情報を確認し、ユーザが求めるリソースへのアクセスを許可します。

UTN サーバは、保護されたネットワーク内で自己認証を行うために、様々な EAP 認証方法に対応しています。

## 選択できる作業

- 「EAP-MD5 を設定する」⇒[89](#)
- 「EAP-TLS を設定する」⇒[90](#)
- 「EAP-TTLS を設定する」⇒[91](#)
- 「PEAP を設定する」⇒[92](#)
- 「EAP-FAST を設定する」⇒[93](#)

## EAP-MD5 を設定する

### 利点と目的

EAP-MD5 は、デバイスまたはユーザの識別情報を確認し、ネットワークリソースへのアクセスを許可します。EAP-MD5 ネットワーク認証を行うように、UTN サーバを設定できます。これにより、UTN サーバは保護されたネットワークに確実にアクセスできるようになります。

### 基本機能

EAP-MD5 は、RADIUS サーバによるユーザベースの認証方法を記述します。UTN サーバは、RADIUS サーバでユーザ（ユーザ名とパスワードを使用）として設定されている必要があります。次に、UTN サーバで認証方法 EAP-MD5 を有効にし、ユーザ名とパスワードを入力する必要があります。

### 必要事項

- UTN サーバが、RADIUS サーバでユーザ（ユーザ名とパスワードを使用）として設定されていること。

#### 手順

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 サーバ上に UTN サーバを設定するために使用する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

### 利点と目的

EAP-TLS (Transport Layer Security) は、デバイスまたはユーザの識別情報を確認し、ネットワークリソースへのアクセスを許可します。EAP-TLS ネットワーク認証を行うように、UTN サーバを設定できます。これにより、UTN サーバは保護されたネットワークに確実にアクセスできるようになります。

### 基本機能

EAP-TLS は、RADIUS サーバによる証明書ベースの認証方法を記述します。その目的で、証明書が UTN サーバと RADIUS サーバ間で交換されます。UTN サーバと RADIUS サーバ間の暗号化 TLS 接続は、この処理中に確立されます。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とされます。RADIUS サーバと UTN サーバは、その証明書を検証する必要があります。相互認証に成功すると、ネットワークへのアクセスが開放されます。

各デバイスで証明書が必要なため、PKI (公開キー基盤) が使用可能であることが必要です。ユーザパスワードは必要ありません。



EAP-TLS 認証を使用する場合は、次の手順通りに実行してください。この手順が守られない場合、ネットワーク内の UTN サーバはアドレス指定できないことがあります。その場合は、UTN サーバのパラメータをリセットする必要があります。⇒ 98 を参照してください。

### 手順

- UTN サーバで認証要求を作成します。⇒ 85 を参照してください。
- 認証要求と認証サーバを使用して、CA 証明書を作成します。
- UTN サーバに CA 証明書をインストールします。「CA 証明書を UTN サーバに保存する」⇒ 86 を参照してください。
- 認証サーバのルート証明書を UTN サーバにインストールします。「ルート証明書を UTN サーバに保存する」⇒ 86 を参照してください。
- UTN サーバで、認証方法「EAP-TLS」を有効にします。

### 手順

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 **TLS**を選択します。
  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。

## EAP-TTLS を設定する

### 利点と目的

EAP-TTLS (Tunneled Transport Layer Security) は、デバイスまたはユーザの識別情報を確認し、ネットワークリソースへのアクセスを許可します。EAP-TTLS ネットワーク認証を行うように、UTN サーバを設定できます。これにより、UTN サーバは保護されたネットワークに確実にアクセスできるようになります。

### 基本機能

EAP-TTLS は、2つのフェーズで構成されます。


- フェーズ 1 では、UTN サーバと RADIUS サーバ間の TLS 暗号化チャンネルが確立されます。RADIUS サーバのみが、CA によって署名された証明書を使用して自己認証を行います。このプロセスは、「外部認証」とも呼ばれます。
- フェーズ 2 では、TLS チャンネル内の通信のために、追加の認証方法が使用されます。EAP 定義の方法や以前の方法 (CHAP、PAP、MS-CHAP および MS-CHAPv2) に対応しています。このプロセスは、「内部認証」とも呼ばれます。

この方式の利点は、RADIUS サーバのみが証明書を必要とすることです。したがって、PKI は必要ありません。さらに、TTLS はほとんどの認証プロトコルに対応します。

### 必要事項

- UTN サーバが、RADIUS サーバでユーザ (ユーザ名とパスワードを使用) として設定されていること。

#### 手順

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 サーバ上に UTN サーバを設定するために使用する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. 接続をより安全にするために、UTN サーバに RADIUS サーバのルート証明書をインストールすることもできます。(⇒86)
  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

### 利点と目的

PEAP (Protected Extensible Authentication Protocol) は、デバイスまたはユーザの識別情報を確認し、ネットワークリソースへのアクセスを許可します。PEAP ネットワーク認証を行うように、UTN サーバを設定できます。これにより、UTN サーバは保護されたネットワークに確実にアクセスできるようになります。

### 基本機能

PEAP の場合 (EAP-TTLS と比較。⇒ 91 を参照してください)、暗号化 TLS (Transport Layer Security) チャンネルが、UTN サーバと RADIUS サーバ間に確立されます。RADIUS サーバのみが、CA によって署名された証明書を使用して自己認証を行います。

TLS チャンネルは、追加の EAP 認証方法 (例: MSCHAPv2) 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。

この方式の利点は、RADIUS サーバのみが証明書を必要とすることです。したがって、PKI は必要ありません。PEAP では、TLS の利点を活用し、ユーザパスワードやワンタイムパスワードなど、様々な認証方法に対応しています。

### 必要事項

- ☑ UTN サーバが、RADIUS サーバでユーザ (ユーザ名とパスワードを使用) として設定されていること。

#### 手順

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 サーバ上に UTN サーバを設定するために使用する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. 接続をより安全にするため、UTN サーバに RADIUS サーバのルート証明書 (⇒ 86) をインストールすることもできます。
  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

### 利点と目的

EAP-FAST (Flexible Authentication via Secure Tunneling) は、デバイスまたはユーザの識別情報を確認し、ネットワークリソースへのアクセスを許可します。EAP-FAST ネットワーク認証を行うように、UTN サーバを設定できます。これにより、UTN サーバは保護されたネットワークに確実にアクセスできるようになります。

### 基本機能

EAP-FAST はデータ転送を保護するためにチャンネルを使用します (EAP-TTLS の場合と同様。⇒ 91 を参照してください)。主な相違点は、EAP-FAST は認証のために証明書を必要としないことです (証明書の使用は任意に選択できます)。

PACs (Protected Access Credentials) は、チャンネルの設定に使用されます。PACs とは、最大で次の 3 つのコンポーネントを含む証明書です。

- UTN サーバと RADIUS サーバ間の事前共有キーを含む共有秘密キー。
- UTN サーバがネットワークリソースにアクセスしようとする、UTN サーバに提供され、RADIUS サーバに表示される不透明な部分。
- クライアントにとって有効な他の情報。(オプション)

EAP-FAST では、2 つの方法を使用して PACs を生成します。

- 手動配信メカニズムは、管理者が構成しネットワークに安全であると見なす、すべてのメカニズムです。
- 自動配信の場合、PAC の配信のみでなく、UTN サーバ認証を保護するために暗号化チャンネルが確立されます。

### 必要事項

- ☑ UTN サーバが、RADIUS サーバでユーザ (ユーザ名とパスワードを使用) として設定されていること。

#### 手順

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 **FAST** を選択します。
  4. RADIUS サーバ上に UTN サーバを設定するために使用する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。

## 6.7 データ転送を暗号化する方法

クライアントと UTN サーバ（および接続された USB デバイス）間のデータ転送を暗号化することができます。



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。

暗号化接続とは、クライアントと UTN サーバが UTN SSL ポート経由で通信することを意味します。ポート番号 9443 があらかじめ設定されています。ポート番号の変更方法は、[⇒ 49](#) を参照してください。

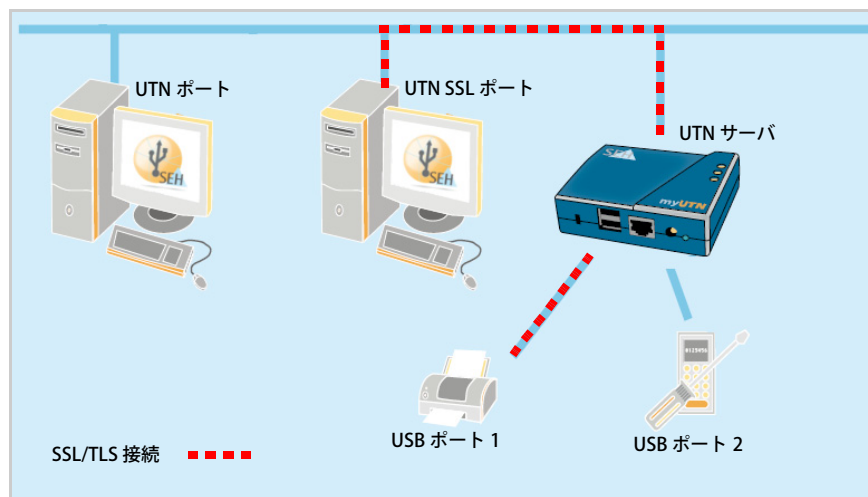


図 16：ネットワーク内の UTN サーバ - SSL/TLS 接続

SSL/TLS 接続を使用する場合は、関連するポートで暗号化を有効にしてください。暗号強度は暗号化レベルで設定されます [⇒ 73](#)。

### 手順

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 ポートで、その暗号化を有効にします。
  4. **保存** をクリックして確定します。
- ☞ クライアントと USB デバイス間のデータが暗号化され送信されます。

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

UTN サーバ/デバイス	ステータス	プロパティ
192.168.0.140		名前 USB フラッシュドライブ
USB フラッシュドライブ	使用可能	ステータス 使用可能
		デバイス情報
		製造メーカー Alcor Micro Corp. (0x058f)
		製品 Flash Drive (0x6387)
		USB クラス Mass Storage (0x08)
		USB ポート 3
		追加機能
		暗号化 オン
		自動操作
		自動接続 オフ

図 17 : SEH UTN Manager - 暗号化

## 7 メンテナンス



UTN サーバでは、様々な種類のメンテナンスを行うことができます。この章では、パラメータ値の保護とリセットについて説明します。また、再起動とデバイス更新の方法も説明します。

### 必要な情報

- 「UTN パラメータを保護する方法（バックアップ）」⇒1097
- 「UTN パラメータを初期設定値にリセットする方法」⇒1098
- 「更新（アップデート）の実行方法」⇒1101
- 「UTN サーバを再起動する方法」⇒1102



## 7.1 UTN パラメータを保護する方法（バックアップ）

UTN サーバのすべてのパラメータ値（パスワード以外）は、パラメータファイル「< デフォルト名 >\_parameter.txt」に保存されます。

パラメータファイルは、ローカルクライアントにバックアップコピーとして保存することもできます。バックアップにより、いつでも安定した設定状態に復帰できます。


コピーした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、設定済みファイルを 1 つまたは複数の UTN サーバにダウンロードできます。このファイルに含まれるパラメータ値は各デバイスに引き継がれます。

### 選択できる作業

- 「パラメータ値を表示する」 ⇒ 1097
- 「パラメータファイルを保存する」 ⇒ 1097
- 「パラメータファイルを UTN サーバに読み込む」 ⇒ 1098

### パラメータ値を表示する

#### 手順


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。



パラメータの詳細な説明は、「パラメータリスト」⇒ 106 を参照してください。

### パラメータファイルを保存する

#### 手順

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。
4. ブラウザを使用して「< デフォルト名 >\_parameter.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コピーされ保護されます。

## パラメータファイルを UTN サーバに読み込む

### 手順

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. **参照**をクリックします。
  4. 「< デフォルト名 >\_parameter.txt」ファイルを指定します。
  5. **インポート**をクリックします。
- ☞ ファイルのパラメータ値が UTN サーバに適用されます。

## 7.2 UTN パラメータを初期設定値にリセットする方法

UTN サーバのパラメータを初期設定値（工場出荷時の設定）にリセットすることができます。リセットすると、以前設定したパラメータはすべて削除されます。インストールされた証明書は削除されません。



パラメータをリセットすると、UTN サーバの IP アドレスが変更されて、myUTN Control Center との接続が失われることがあります。

リセットを推奨する状況

例えば、UTN サーバの設置場所を変更して別のネットワークで UTN サーバを使用する場合に、パラメータをリセットする必要があります。別のネットワークに UTN サーバを設定する場合は、設置場所を変更する前に、パラメータを初期設定にリセットする必要があります。

選択できる作業

- 「myUTN Control Center でパラメータをリセットする」⇒99
- 「InterCon-NetTool でパラメータをリセットする」⇒99
- 「リセットボタンでパラメータをリセットする」⇒99



デバイスのステータスボタンを使用すると、パスワードを入力せずにパラメータをリセットできます。

## myUTN Control Center でパラメータをリセットする

### 手順

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。
  3. **初期設定**をクリックします。
- 🔗 パラメータがリセットされます。

## InterCon-NetTool でパラメータをリセットする

### 手順

1. InterCon-NetTool を起動します。
  2. デバイスリストから UTN サーバを選択します。
  3. メニューバーから、**アクション (A) - 初期設定**を選択します。
  4. **終了**をクリックします。
- 🔗 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

UTN サーバには LED、リセットボタン、および各種のポートがあります。これらのコンポーネントについては、「クイック・インストール案内」で説明しています。

リセットボタンを使用すると、UTN サーバのパラメータ値を初期設定にリセットできます。リセット処理は 2 つのフェーズに分かれています。

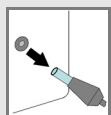
- フェーズ 1 の間に、デバイスは強制的にリセットモードになります。リセットモードの間に、パラメータがリセットされます。
- フェーズ 2 で、デバイスが再起動されます。



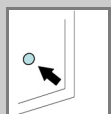
**重要：リセットモードでは、Activity LED（黄色）と Status LED（緑色）が同時に点滅します。この点滅は 5 回繰り返されます。LED が点滅している間にステータスボタンを放します。ステータスボタンを押し続けていると、デバイスは BIOS モードに切り替わります。BIOS モードに切り替わった場合は、リセットを再試行してください。**

フェーズの説明は、次の通りです。

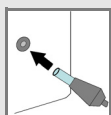
## [フェーズ 1] リセット



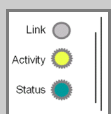
UTN サーバのスイッチを切ります。  
(電源ソケットを外す)



リセットボタンを押し続けます。

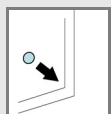


UTN サーバのスイッチを入れます。  
(電源ソケットを差し込む)



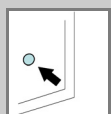
Activity LED と Status LED が同時に点滅するまで待機します。

リセットモードが有効になります。



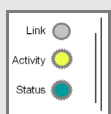
リセットボタンを約 2 秒で放します。

LED が交互に点滅します。

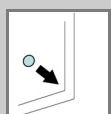


再びリセットボタンを押し続けます。

LED が同時に点滅します。

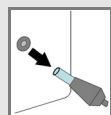


数秒後、Activity LED のみが点滅します。

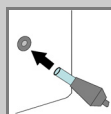


リセットボタンを放します。

## [フェーズ 2] 再起動



UTN サーバのスイッチを切ります。  
(電源ソケットを外す)



UTN サーバのスイッチを入れます。  
(電源ソケットを差し込む)

## 7.3 更新（アップデート）の実行方法

UTN サーバで、ソフトウェアとファームウェアの更新を実行できます。更新することで、新しく開発された機能が使用できるようになります。

### 更新中に起きること

更新中に、既存のファームウェア/ソフトウェアは新しいバージョンで上書きされ、置き換えられます。デバイスのパラメータの初期設定は変更されません。

### 更新を推奨する状況

機能の一部が正常に動作しない場合、または SEH Computertechnik GmbH が、新しい機能またはバグ修正を含む新しいソフトウェアまたはファームウェアのバージョンをリリースした場合、更新を実行する必要があります。

UTN サーバにインストールされたソフトウェアとファームウェアのバージョンを確認します。バージョン番号は、myUTN Control Center のホームページ、または InterCon-NetTool の製品リストに記載されています。

### 更新ファイルの入手方法

最新のファームウェアおよびソフトウェアファイルは、次の SEH Computertechnik GmbH のホームページからダウンロードできます。

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



すべての更新ファイルには、専用の「readme」ファイルがあります。「readme」ファイルに記載された情報を確認してください。

### 手順

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. **参照**をクリックします。
  4. 更新ファイルを選択します。
  5. **インストール**をクリックします。
- ☞ 更新が実行されます。UTN サーバが再起動します。

選択できる作業

## 7.4 UTN サーバを再起動する方法

パラメータの変更後や更新の実行後には、UTN サーバは自動的に再起動します。UTN サーバが未定義状態の場合は、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」 ⇨ 102
- 「InterCon-NetTool から UTN サーバを再起動する」 ⇨ 102

### myUTN Control Center から UTN サーバを再起動する

#### 手順

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。

### InterCon-NetTool から UTN サーバを再起動する

#### 手順

1. InterCon-NetTool を起動します。
  2. デバイスリストから UTN サーバを選択します。
  3. メニューバーから、**アクション (A)- 再起動** を選択します。
  4. **終了** をクリックします。
- 🔄 UTN サーバが再起動します。

## 8 付録



この付録には、用語集、UTN サーバのパラメータリスト、および索引リストが含まれています。

### 必要な情報

- 「用語集」⇒103
- 「パラメータリスト」⇒106
- 「LED 表示」⇒123
- 「SEH UTN Manager - 機能の概要」⇒124
- 「トラブルシューティング」⇒127
- 「付加ツール「utnm」」⇒131
- 「図リスト」⇒136

### 8.1 用語集

この用語集には、メーカー固有のソフトウェアソリューションに関する情報、およびネットワークテクノロジーで使用される専門用語が含まれています。

### 必要な情報

#### メーカー固有のソフトウェアソリューション

- 「myUTN Control Center」⇒104
- 「InterCon-NetTool」⇒104
- 「SEH UTN Manager」⇒104

#### ネットワークテクノロジー

- 「ハードウェアアドレス」⇒104
- 「IP アドレス」⇒105
- 「ホスト名」⇒105
- 「ゲートウェイ」⇒105
- 「サブネットマスク」⇒105
- 「デフォルト名」⇒105

## myUTN Control Center

UTN サーバは、myUTN Control Center から設定および監視できます。myUTN Control Center は UTN サーバに格納され、ブラウザソフトウェア (Internet Explorer、Mozilla Firefox、Safari) で表示できます。

## InterCon-NetTool

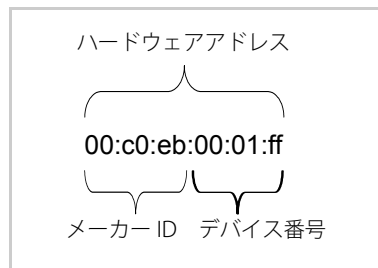
InterCon-NetTool ソフトウェアは、SEH Computertechnik GmbH により開発され、あらかじめ指定されたネットワーク内で SEH のネットワークデバイスを管理するために使用されます。

## SEH UTN Manager

SEH UTN Manager は、USB デバイスへのアクセスを管理するソフトウェアツールです。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 は、ネットワーク内に存在するすべての USB デバイスの可用性を示し、クライアントと USB デバイス間の接続を確立します。

## ハードウェアアドレス

UTN サーバは、世界でただ 1 つのハードウェアアドレスを使用してアドレス指定できます。通常、このアドレスは MAC アドレスまたはイーサネットアドレスと呼ばれます。メーカーが、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 の 16 進数で構成されます。最初の 6 つの数字は、メーカーを表し、後の 6 つの数字は各デバイスを特定します。



ハードウェアアドレスは、筐体や SEH UTN Manager、または InterCon-NetTool で確認できます。

ハードウェアアドレス内の区切りの使用は、プラットフォームにより異なります。ハードウェアアドレスを入力する際は、次の表記規則に注意してください。

オペレーティングシステム	表記	例
Windows	ハイフン	00-c0-eb-00-01-ff
UNIX	コロンまたはピリオド	00:c0:eb:00:01:ff or 00.c0.eb.00.01.ff



**IP アドレス**

IP アドレスは、ネットワーク内の各ノードに固有のアドレスです。つまり、IP アドレスは、ローカルネットワーク上に1つしかありません。IP アドレスは通常、システム管理者によって割り当てられます。このアドレスは、UTN サーバに保存して、ネットワーク内部で確実にアドレス指定できるようにする必要があります。

**ホスト名**

ホスト名は、IP アドレスのエイリアスです。ホスト名は、ネットワーク内の UTN サーバを一意に識別し、覚えやすくします。

**ゲートウェイ**

ゲートウェイを使用して、外部ネットワークから IP アドレスを指定できます。ゲートウェイを使用する場合は、myUTN Control Center から、関連するパラメータを設定できます。

**サブネットマスク**

サブネットマスクを活用して、大規模ネットワークをサブネットワークに分割できます。この場合、IP アドレスのユーザ ID は様々なサブネットワークに割り当てられます。UTN サーバは、出荷時には、サブネットワークを使用しないように設定されています。サブネットワークを使用する場合は、myUTN Control Center から、UTN サーバの関連するパラメータを設定できます。

**デフォルト名**

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ます。デバイス番号は、ハードウェアアドレスの最後の6桁で構成されます。



デフォルト名は、myUTN Control Center または InterCon-NetTool で確認できます。

## 必要な情報

## 8.2 パラメータリスト

この章では、使用可能なすべての UTN サーバパラメータを概説します。パラメータリストでは各パラメータの機能と値の詳細を示します。

- 「パラメータリスト - IPv4」 ⇒ 107
- 「パラメータリスト - IPv4 VLAN (myUTN-80 および myUTN-150 のみ)」 ⇒ 107
- 「パラメータリスト - IPv6」 ⇒ 108
- 「パラメータリスト - Bonjour」 ⇒ 109
- 「パラメータリスト - SSL 接続」 ⇒ 109
- 「パラメータリスト - Web アクセス」 ⇒ 109
- 「パラメータリスト - TCP ポートアクセス」 ⇒ 110
- 「パラメータリスト - UTN ポート」 ⇒ 111
- 「パラメータリスト - 暗号化」 ⇒ 111
- 「パラメータリスト - USB ポートアクセス (myUTN-80 以降のみ)」 ⇒ 111
- 「パラメータリスト - USB ポート」 ⇒ 112
- 「パラメータリスト - DNS」 ⇒ 113
- 「パラメータリスト - SNMP」 ⇒ 113
- 「パラメータリスト - 日付 / 時間」 ⇒ 114
- 「パラメータリスト - 説明」 ⇒ 115
- 「パラメータリスト - 認証」 ⇒ 115
- 「パラメータリスト - POP3 (myUTN-80 以降のみ)」 ⇒ 116
- 「パラメータリスト - SMTP (myUTN-80 以降のみ)」 ⇒ 117
- 「パラメータリスト - 通知 (myUTN-80 以降のみ)」 ⇒ 118
- 「パラメータリスト - WLAN (myUTN-54 のみ)」 ⇒ 120



UTN サーバの現在のパラメータ値を表示するには、「パラメータ値を表示する」⇒ 97 を参照してください。

表 12：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 アドレスを指定します。
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を指定します。
ip_gate [ゲートウェイ]	有効な IP アドレス	0.0.0.0	UTN サーバのゲートウェイアドレスを指定します。
ip_dhcp [DHCP]	on/off	on	DHCP プロトコルを有効または無効にします。
ip_bootp [BOOTP]	on/off	on	BOOTP プロトコルを有効または無効にします。
ip_auto [ARP/PING]	on/off	on	ARP/PING による IP アドレスの割り当てを、有効または無効にします。

表 13：パラメータリスト - IPv4 VLAN (myUTN-80 および myUTN-150 のみ)

パラメータ	値	初期値	説明
ipv4vlan_on_1 ~ ipv4vlan_on_8 [VLAN]	on/off	off	VLAN データの転送を、有効または無効にします。
ipv4vlan_addr_1 ~ ipv4vlan_addr_8 [IP アドレス]	有効な IP アドレス	192.168. 0.0	VLAN 内にある UTN サーバの IP アドレスを指定します。
ipv4vlan_mask_1 ~ ipv4vlan_mask_8 [サブネットマスク]	有効な IP アドレス	255.255. 255.0	VLAN 内にある UTN サーバのサブネットマスクを指定します。
ipv4vlan_id_1 ~ ipv4vlan_id_8 [VLAN ID]	0 ~ 4096 [1 ~ 4 半角文字、0 ~ 9]	0	VLAN を識別するための ID を指定します。 0 = タグなしマルチホーム IP アドレス
ipv4vlan_web [VLAN アクセス]	on/off	on	VLAN アドレスによる myUTN Control Center への Web の管理者アクセスを許可または拒否します。

パラメータ	値	初期値	説明
ipv4vlan_snmp [VLAN アクセス]	on/off	on	VLAN アドレスによる myUTN Control Center への管理上の SNMP アクセスを許可または拒否します。

表 14：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_addr [IPv6 アドレス]	n:n:n:n:n:n	::	n:n:n:n:n:n の形式で、UTN サーバに割り当てられた IPv6 ユニキャストアドレスを手動で設定します。 各「n」は、アドレスの 8 つの 16 ビット要素の 1 つの 16 進値を示します。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せん。この場合、2 つのコロン (::) が使用されます。
ipv6_gate [ルータ]	n:n:n:n:n:n	::	ルータの IPv6 ユニキャストアドレスを指定します。UTN サーバは「Router Solicitations」(RS) をこのルータに送信します。
ipv6_plen [プレフィックス長]	0 ~ 64 [1 ~ 2 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。 アドレス範囲は、プレフィックスによって示されます。プレフィックス長 (使用するビット数) が IPv6 アドレスに追加され、10 進値で指定されます。この 10 進値は「/」で区切られます。
ipv6_auto [自動設定]	on/off	on	UTN サーバの IPv6 アドレスの自動割り当てを、有効または無効にします。

表 15 : 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 サービスを有効化 / 無効化します。
bonjour_name [Bonjour 名]	最大 64 半角文字 [a ~ z、A ~ Z、0 ~ 9]	[デフォルト名]	UTN サーバの Bonjour 名を設定します。

表 16 : パラメータリスト - SSL 接続

パラメータ	値	初期値	説明
security [暗号化]	1 ~ 4 [1 文字]	2	SSL/TLS 接続に使用する暗号化レベルを設定します。 1 = 低レベル (56 ビット) 2 = 中レベル (128 ビット) 3 = 高レベル (128 - 256 ビット) 4 = クライアント互換 (40 - 256 ビット)

表 17 : パラメータリスト - Web アクセス

パラメータ	値	初期値	説明
http_pwd [パスワード]	最大 64 半角文字 [a ~ z、A ~ Z、0 ~ 9]	[空白]	myUTN Control Center への管理者アクセスに使用するパスワードを設定します。
http_allowed [許可された接続]	on/off	on	myUTN Control Center に対して許可されたタイプの接続 (HTTP/HTTPS) を設定します。 接続タイプとして HTTPS のみが選択されている場合 [http_allowed = off]、myUTN Control Center への管理者アクセスは、SSL/TLS で保護されます。

表 18 : 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	選択したポートのロックを、有効または無効にします。
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にします。 テストモードでは、アクセス制御を使用してパラメータセットをテストできます。テストモードがアクティブな場合、アクセス保護は UTN サーバが再起動されるまでの間、有効であり続けます。
protection_level [セキュリティレベル]	protec_utn protec_tcp protec_all	protec_utn	ロックするポートタイプを指定します。 - UTN ポート - TCP ポート - すべてのポート (IP ポート)
ip_filter_on_1 ~ ip_filter_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_filter_1 ~ ip_filter_8 [IP アドレス]	有効な IP アドレス	[空白]	IP アドレスにより、ポートロックから除外する要素を設定します。
hw_filter_on_1 ~ hw_filter_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_filter_1 ~ hw_filter_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	ハードウェアアドレスにより、ポートロックから除外する要素を設定します。

表 19：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 半角文字、0 ~ 9]	9200	UTN ポートの番号を設定します。
utn_sslport [UTN SSL ポート]	1 ~ 9443 [1 ~ 4 半角文字、0 ~ 9]	9443	UTN SSL ポートの番号を設定します。

表 20：パラメータリスト - 暗号化

パラメータ	値	初期値	説明
utn_sec_1 ~ utn_sec_8 [USB ポート]	on/off	off	USB ポートの SSL/TLS 暗号化を、有効または無効にします。 暗号化が有効な場合、クライアントと（USB ポートに接続された）USB デバイス間のペイロードは暗号化され送信されます。

表 21：パラメータリスト - USB ポートアクセス（myUTN-80 以降のみ）

パラメータ	値	初期値	説明
utn_heartbeat	1 ~ 1800 [1 ~ 4 半角文字、0 ~ 9]	180	<b>このパラメータを使用するには、必ず SEH のサポートチームと相談してください。</b>
utn_accctr_1 ~ utn_accctr_8 [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と使用を制限する方法を指定します。 --- = 保護なし ids = デバイス割り当て key = ポートキー制御 keyids = デバイス割り当てとポートキー制御
utn_keyval_1 ~ utn_keyval_8 [キー]	最大 64 半角文字 [a ~ z, A ~ Z, 0 ~ 9]	[空白]	接続された USB デバイスをアクセスから保護するキーを指定します。

パラメータ	値	初期値	説明
utn_prodid_1 ~ utn_prodid_8 [USB デバイス]			各 USB ポートに割り当てられた USB デバイスの製品 ID を示します。
utn_vendid_1 ~ utn_vendid_8 [USB デバイス]			各 USB ポートに割り当てられた USB デバイスのベンダ ID を示します。
utn_2vlan_1 ~ utn_2vlan_8 [VLAN の割り当て]	0 ~ 9 [1 半角文字] (⇒ 107 を参照してください。)	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 22 : 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_8 [名前]	最大 32 半角文字 [a ~ z、A ~ Z、0 ~ 9]	[空白]	USB デバイスの説明を任意で入力します。
utn_comp_1 [圧縮]	on/off	off	USB ポートに接続されている USB デバイスに対するデータ圧縮を、無効または有効にします (myUTN-130 のみ)。
utn_poff_1 ~ utn_poff_8 [電源]	on/off	off	USB ポート (ポートに接続されている 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 On on = 電源 Off
utn_postreset_1 ~ utn_postreset_8	on/off	off	このパラメータを使用するには、必ず SEH のサポートチームと相談してください。



表 23 : パラメータリスト - DNS

パラメータ	値	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]	既存の DNS サーバのドメイン名を設定します。
dns_primary [プライマリ DNS サーバ]	有効な IP アドレス	0.0.0.0	プライマリ DNS サーバの IP アドレスを設定します。
dns_secondary [セカンダリ DNS サーバ]	有効な IP アドレス	0.0.0.0	セカンダリ DNS サーバの IP アドレスを設定します。セカンダリ DNS サーバは、プライマリ DNS サーバが使用できない場合に使用します。

表 24 : 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	コミュニティの書き込み保護を、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 コミュニティの名前を設定します。SNMP コミュニティは、同じアクセス権を持つ複数の参加者をグループにまとめるという、アクセス保護の基本的な形式です。
snmpv3 [SNMPv3]	on/off	on	SNMPv3 を有効または無効にします。
any_name [ユーザ名]	最大 64 半角文字 [a ~ z, A ~ Z, 0 ~ 9]	anonymous	SNMP ユーザグループ 1 の名前を設定します。
any_pwd [パスワード]	最大 64 半角文字 [a ~ z, A ~ Z, 0 ~ 9]	[空白]	SNMP ユーザグループ 1 のパスワードを設定します。

パラメータ	値	初期値	説明
any_rights [アクセス権]	--- [なし] readonly readwrite	readonly	SNMP ユーザグループ 1 のアクセス権を設定します。
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設定します。
any_cipher [暗号化]	--- [なし] aes des	---	SNMP ユーザグループ 1 の暗号化の方法を設定します。
admin_name [ユーザ名]	最大 64 半角文字 [a ~ z, A ~ Z, 0 ~ 9]	admin	SNMP ユーザグループ 2 の名前を設定します。
admin_pwd [パスワード]	8 ~ 64 半角文字 [a ~ z, A ~ Z, 0 ~ 9]	administ rator	SNMP ユーザグループ 2 のパスワードを設定します。
admin_rights [アクセス権]	--- [なし] readonly readwrite	readwrite	SNMP ユーザグループ 2 のアクセス権を設定します。
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設定します。
admin_cipher [暗号化]	--- [なし] aes des	---	SNMP ユーザグループ 2 の暗号化の方法を設定します。

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。

パラメータ	値	初期値	説明
ntp_tzone [タイムゾーン]	UTC、GMT、EST、 EDT、CST、CDT、 MST、MDT、PST、 PDT など。	CET/CES T (EU)	タイムゾーンは、タイムサー バから受信した時刻と現地時 刻との違いを正しく調整する ために使用します。

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]	UTN サーバのホスト名を指定 します。
sys_descr [説明]	最大 64 半角文字 [a～z、A～Z、0 ～9]	[空白]	説明を自由に入力します。
sys_contact [担当者]	最大 64 半角文字 [a～z、A～Z、0 ～9]	[空白]	説明（担当者の説明）を自由 に入力します。

表 27：パラメータリスト - 認証

パラメータ	値	初期値	説明
auth_typ [認証方法]	--- [なし] MD5 TLS TTLS PEAP FAST	---	ネットワーク内の UTN サーバ を識別するために使用する EAP 認証の方式を設定します。
auth_name [ユーザ名]	最大 64 半角文字 [a～z、A～Z、0 ～9]	[空白]	認証サーバ (RADIUS) に保 存する UTN サーバの名前を設 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]	認証サーバ (RADIUS) に保 存する UTN サーバのパスワー ドを設定します。
auth_intern [内部認証]	--- [なし] PAP = PAP CHAP = CHAP MSCHAP2 = MS-CHAPv2 EMD5 = EAP-MD5 ETLS = EAP-TLS	---	EAP 認証の方式である TTLS と PEAP、また FAST に使用する 内部認証の方式を設定します。

パラメータ	値	初期値	説明
auth_extern [PEAP/EAP-FAST オプション]	--- [なし] PLABEL0 = PEAPLABEL0 PLABEL1 = PEAPLABEL1 PVER0 = PEAPVER0 PVER1 = PEAPVER1 FPROV1 = FASTPROV1	---	EAP 認証の方式である TTLS と PEAP、また FAST に使用する外部認証の方式を設定します。
auth_ano_name [匿名の名前]	最大 64 半角文字 [a ~ z, A ~ Z, 0 ~ 9]	[空白]	EAP 認証の方式である TTLS と PEAP、また FAST の暗号化されていない部分の匿名の名前を設定します。
auth_wpa_addon [WPA アドオン]	最大 255 半角文字 [a ~ z, A ~ Z, 0 ~ 9]	[空白]	オプションの WPA 拡張機能を指定します。

表 28 : 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設定します。ホスト名は、DNS が事前に設定された場合にのみ使用できます。
pop3_poll [メールのチェック間隔]	1-10080 [1-5 半角文字、0 ~ 9]	2	POP3 サーバから電子メールを受信する時間間隔を分単位で設定します。
pop3_port [サーバーポート]	1 ~ 65535 [1-5 半角文字、0 ~ 9]	110	UTN サーバが電子メールを受信するときに使用する POP3 のポートを設定します。SSL/TLS を使用する場合はポート番号 995 を入力します。
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。

パラメータ	値	初期値	説明
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 サーバが使用するパスワードを設定します。
pop3_sec [セキュリティ]	0 = --- (セキュリティなし) 1 = APOP 2 = SSL/TLS	0	認証方法を設定します。
pop3_limit [メールの上限数]	0 ~ 4096 [1-5 半角文字、0 ~ 9、0 = 無制限]	10	UTN サーバが許容する電子メールの最大サイズをキロバイト単位で設定します。

表 29 : 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 アドレスまたはドメイン名で設定します。 ホスト名は、DNS が事前に設定された場合にのみ使用できます。
smtp_port [サーバーポート]	1 ~ 65535 [1-5 半角文字、0 ~ 9]	25	UTN サーバが SMTP サーバに電子メールを送信するときに使用するポート番号を設定します。
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 サーバにログインするために UTN サーバが使用するパスワードを設定します。
smtp_sender [送信者名]	最大 128 半角文字	[空白]	電子メール送信で UTN サーバが使用する電子メールアドレスを設定します。 ✕王：送信者の名前とユーザ名は同一である可能性があります。

パラメータ	値	初期値	説明
smtp_ssl [TLS]	on/off	off	TLS を有効または無効にします。 セキュリティプロトコル TLS (Transport Layer Security) は、UTN サーバと SMTP サーバ間の送信を暗号化するために使用されます。
smtp_auth [ログイン]	on/off	off	ログイン時の SMTP 認証を、有効または無効にします。
smtp_sign [セキュリティ (S/MIME) ]	on/off	off	S/MIME による電子メールの暗号化と署名を、有効または無効にします。
smtp_attpkey [公開キーの添付]	on/off	on	公開キーの電子メールへの添付を、有効または無効にします。
smtp_encrypt [完全な暗号化] [電子メールの署名]	on/off	off	電子メールの署名および暗号化を設定します。 off = 署名 on = 暗号化

表 30 : 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
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 トラップアドレスを設定します。
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を指定します。
trapdev [USB デバイスが接続または切断された場合にトラップを送信]	on/off	off	USB デバイスが UTN サーバに接続されたとき (または取り外されたとき) の SNMP トラップの送信を、有効または無効にします。
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。

パラメータ	値	初期値	説明
trapact [USB デバイスをアクティブまたは非アクティブにした場合にトラップを送信]	on/off	off	USB デバイスをアクティブまたは非アクティブにしたときの SNMP トラップの送信を、有効または無効にします。
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_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（または取り外された）ときの電子メール通知を、有効または無効にします。
noti_act_1 noti_act_2 [USB デバイスをアクティブまたは非アクティブにした場合に電子メールを送信]	on/off	off	USB デバイスをアクティブまたは非アクティブにしたときの電子メールの送信を、有効または無効にします。
noti_stat_1 noti_stat_2 [ステータス通知]	on/off	off	受信者 1 または 2 へのステータス通知メールの定期送信を、有効または無効にします。
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送信を、有効または無効にします。
notistat_d [間隔]	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	al	ステータス通知メールを送信する時間間隔を指定します。
notistat_h [hh]	1 = 1. 時間 2 = 2. 時間 3 = 3. 時間 など	0	ステータス通知メールを送信する時間を指定します。

パラメータ	値	初期値	説明
notistat_tm [mm]	0 = 00 分 1 = 10 分 2 = 20 分 3 = 30 分 4 = 40 分 5 = 50 分 6 = 00 分	0	ステータス通知メールを送信する時間を指定します。

表 31：パラメータリスト - WLAN (myUTN-54 のみ)

パラメータ	値	初期値	説明
wifi [WLAN]	on/off	on	UTN サーバの WLAN モジュールを、有効または無効にします。
wifi_mode [モード]	adhoc infra	adhoc	通信モードを設定します。通信モードによって、UTN サーバをインストールするネットワークの構造が決まります。次の 2 つのモードを使用できます。 - アドホック - インフラストラクチャ
wifi_channel [チャンネル]	1-14 (国による)	3	データ通信全体の送信先チャンネルを設定します。干渉が発生する場合は、チャンネル (周波数範囲) を変更する必要があります。 <b>WLAN 製品の使用に際しては国の定める条例を遵守し、法律で認められたチャンネル以外は使用しないでください。</b>
wifi_name [ネットワーク名 (SSID)]	最大 64 半角文字 [a ~ z, A ~ Z, 0 ~ 9, _、-]	SEH	SSID を設定します。無線ネットワークの ID は、SSID (Service Set Identifier) またはネットワーク名と呼ばれます。それぞれの無線 LAN には、無線ネットワークの明確な識別に使用する設定可能な SSID があります。



パラメータ	値	初期値	説明
wifi_encrypt [暗号化の方法]	--- [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 (Auto)	---	WLAN への不正アクセスを防ぐ暗号化方式を設定します。
wifi_keyid [WEP キーを使用]	1 = key 1 2 = key 2 3 = key 3 4 = key 4	0	使用する WEP キーを設定します。
wifi_wepkey1 wifi_wepkey2 wifi_wepkey3 wifi_wepkey4 [キー 1 ~ 4]	文字の最大数は、選択したキーの種類により異なります。 64 ASCII = 5 64 HEX = 10 128 ASCII = 13 128 HEX = 26	[空白]	使用する WEP キーを設定します。4 つの WEP キーを使用できます。 次の文字を入力できます。 ・16 進法 = 0 ~ 9, a ~ f, A ~ F ・ASCII = 0 ~ 9, a ~ z, A ~ Z
wifi_psk [PSK]	8 ~ 63 半角文字	[空白]	WPA (Wi-Fi Protected Access) 用の事前共有キー (PSK) を設定します。

パラメータ	値	初期値	説明
wifi_roaming [ローミング]	on/off	off	ローミングの使用を有効または無効にします。 ローミングとは、1つの無線セルから次の無線セルに移動することを意味します。UTNサーバは、最も強い信号のアクセスポイントを使用します。UTNサーバが別のアクセスポイント領域に向かって移動しているとき、自動的に次の無線セルに切り替えられ、この間に無線セルへの接続が中断することはありません。
wifi_dbmroam [ローミングレベル]	0 ~ 100 [1 ~ 3 半角文字、0 ~ 9]	0	UTNサーバの送信出力 (-dBm) を設定します。

## 8.3 LED 表示

UTN サーバは LED を備えています。LED は、UTN サーバの状態を示します。



サーバが起動している最中の LED の動作は、ここでの説明とは異なります。

LED	アクション	色	説明
Link	常に点灯	緑色	ネットワークに接続しています。
	常に消灯	-	ネットワークへの接続がありません。
Activity	不定間隔で点滅	黄色	ネットワークデータパケットの交換を示します。
Status	常に消灯	-	USB デバイスの接続がありません。 注意：Activity LED が同時に一定間隔で点滅するときは、BIOS モードに入ることを示します。BIOS モードに入ると、UTN サーバは機能しません。⇒ 127 を参照してください。
	常に点灯	緑色	少なくとも 1 つの USB デバイスに接続していることを示します。
	3 回点滅	緑色	ZeroConfig IP アドレスが割り当てられていることを示します。 注意：ZeroConf 範囲外の IP アドレスを使用することを推奨します。
	2 回点滅	緑色	割り当てられた IP アドレスが、0.0.0.0 に対応していないか、または ZeroConf 範囲外のアドレスであることを示します。



UTN サーバの機種「myUTN-80」、「myUTN-120」、「myUTN-130」、「myUTN-150」には異なる LED があります。LED の説明については、クイック・インストール案内を参照してください。

## 8.4 SEH UTN Manager - 機能の概要

SEH UTN Manager の機能は、無効状態として表示する（グレイアウト）、または非表示にすることができます。次の要因に依存します。

- 選択リストモードの設定（グローバルリスト / ユーザリスト）
- ユーザグループ
  - 「Administrator」グループに属するユーザ
  - 「Administrator」グループに属さないユーザ
    - + \*.ini ファイル（選択リスト）に書き込み権限があるユーザ
    - + \*.ini ファイル（選択リスト）に書き込み権限がないユーザ

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。

概要を次の表に示します。

- 「SEH UTN Manager - 機能の概要、Windows」⇒[125](#)
- 「SEH UTN Manager - 機能の概要、Mac」⇒[126](#)



表には基本的に利用できる機能を示しています。また、個別の機能は表示されない、または無効として表示されます。次の要因に依存します。

- 組み込まれている UTN サーバ機種
- 製品に固有なセキュリティメカニズムの設定

表 32 : SEH UTN Manager - 機能の概要、Windows

	グローバル選択リスト		ユーザ固有の選択リスト		
	Admin	User	Admin	User (rw) (INI)	User (r) (INI)
<b>メニュー</b>					
選択リスト - 編集	✓	✗	✓	✓	✗
選択リスト - エクスポート	✓	✗	✓	✗	✗
選択リスト - 更新	✓	✓	✓	✓	✓
UTN サーバ - 構成	✓	✓	✓	✓	✓
UTN サーバ - IP アドレスの設定	✓	✓	✓	✓	✓
UTN サーバ - USB ポートキーの設定	✓	✗	✓	✓	✗
UTN サーバ - 追加	✓	✗	✓	✓	✗
UTN サーバ - 削除	✓	✗	✓	✓	✗
UTN サーバ - 更新	✓	✓	✓	✓	✓
デバイス - 有効化	✓	✓	✓	✓	✓
デバイス - 無効化	✓	✓	✓	✓	✓
デバイス - リクエスト	✓	✓	✓	✓	✓
デバイス - 削除	✓	✗	✓	✗	✗
デバイス - UTN アクションの作成	✓	✓	✓	✓	✓
デバイス - 設定	✓	✓	✓	✓	✓
<b>ボタン</b>					
選択リスト - 更新	✓	✓	✓	✓	✓
選択リスト - 編集	✓	✗	✓	✓	✗
デバイス - 有効化	✓	✓	✓	✓	✓
デバイス - 無効化	✓	✓	✓	✓	✓
<b>「プログラム - オプション」 ダイアログ</b>					
ネットワークスキャン - マルチキャスト検索	✓	✗	✓	✗	✗
ネットワークスキャン - IP 範囲検索	✓	✗	✓	✗	✗
プログラム - 言語	✓	✓	✓	✓	✓
プログラム - プログラムメッセージ	✓	✗	✓	✗	✗
プログラム - プログラムのアップデート	✓	✗	✓	✗	✗
自動操作 - プログラムの開始 (自動起動)	✓	✓	✓	✓	✓
自動操作 - デバイスの自動切断 (自動切断)	✓	✗	✓	✗	✗
選択リスト - 選択リストモード	✓	✗	✓	✗	✗
選択リスト - 自動リフレッシュ	✓	✗	✓	✗	✗
<b>「デバイス設定」 ダイアログ</b>					
デバイスの自動接続 - 自動接続	✓	✗	✓	✗	✗
デバイスの自動接続 - オンデマンド印刷	✓	✗	✓	✗	✗
メッセージ	✓	✓	✓	✓	✓

✓ = アクティブ  
✗ = 非アクティブ (グレイアウト)

r = 読み取り専用  
rw = 読み書き可能  
INI = \*.ini ファイル (⇒ 68)

表 33 : SEH UTN Manager - 機能の概要、Mac

	グローバル選択リスト		ユーザ固有の選択リスト		
	Admin	User	Admin	User (rw) (INI)	User (r) (INI)
<b>メニュー</b>					
選択リスト - 編集	✓	×	✓	✓	×
選択リスト - エクスポート	✓	×	✓	×	×
選択リスト - 更新	✓	✓	✓	✓	✓
UTN サーバ - 構成	✓	✓	✓	✓	✓
UTN サーバ - IP アドレスの設定	✓	✓	✓	✓	✓
UTN サーバ - USB ポートキーの設定	✓	×	✓	✓	×
UTN サーバ - 追加	✓	×	✓	✓	×
UTN サーバ - 削除	✓	×	✓	✓	×
UTN サーバ - 更新	✓	✓	✓	✓	✓
デバイス - 有効化	✓	✓	✓	✓	✓
デバイス - 無効化	✓	✓	✓	✓	✓
デバイス - リクエスト	✓	✓	✓	✓	✓
デバイス - 削除	✓	×	✓	×	×
デバイス - UTN アクションの作成	✓	✓	✓	✓	✓
デバイス - 設定	✓	✓	✓	✓	✓
<b>ボタン</b>					
選択リスト - 更新	✓	✓	✓	✓	✓
選択リスト - 編集	✓	×	✓	✓	×
デバイス - 有効化	✓	✓	✓	✓	✓
デバイス - 無効化	✓	✓	✓	✓	✓
<b>「プログラム - オプション」 ダイアログ</b>					
ネットワークスキャン - マルチキャスト検索	✓	×	✓	×	×
ネットワークスキャン - IP 範囲検索	✓	×	✓	×	×
プログラム - プログラムメッセージ	Windows でのみ有効				
プログラム - プログラムのアップデート	✓	×	✓	×	×
自動操作 - プログラムの開始 (自動起動)	✓	✓	✓	✓	✓
自動操作 - デバイスの自動切断 (自動切断)	✓	×	✓	×	×
選択リスト - 選択リストモード	✓	×	✓	×	×
選択リスト - 自動リフレッシュ	✓	×	✓	×	×
<b>「デバイス設定」 ダイアログ</b>					
デバイスの自動接続 - 自動接続	✓	×	✓	×	×
デバイスの自動接続 - オンデマンド印刷	✓	×	✓	×	×
メッセージ	Windows でのみ有効				

✓ = アクティブ  
 × = 非アクティブ (グレイアウト)

r = 読み取り専用  
 rw = 読み書き可能  
 INI = \*.ini ファイル (⇒ 68)

## 8.5 トラブルシューティング

この章では、一部の問題とその解決策について説明します。

### 問題

- 「UTN サーバが、BIOS モードに入る合図を示す」⇒127
- 「SEH UTN Manager の機能の一部が見えない、有効にならない、または表示が不明瞭である」⇒129
- 「UTN サーバとの接続が確立できない。」⇒129
- 「USB デバイスとの接続が確立できない。」⇒129
- 「myUTN Control Center との接続が確立できない。」⇒129
- 「パスワードが使用できなくなった」⇒130

### 考えられる原因

ファームウェアが正常に機能していても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。たとえば、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。次の場合、UTN サーバは BIOS モードに入る合図を示します。

- Activity LED（黄色）が一定間隔で点滅し、
- Status LED（緑色）が点灯していない。



---

**BIOS モードに入ると、UTN サーバは機能しません。**

---

UTN サーバが BIOS モードに入ると、InterCon-NetTool のデバイスリストにフィルタ「BIOS モード」が自動的に作成されます。UTN サーバはこのフィルタ内に表示されます。

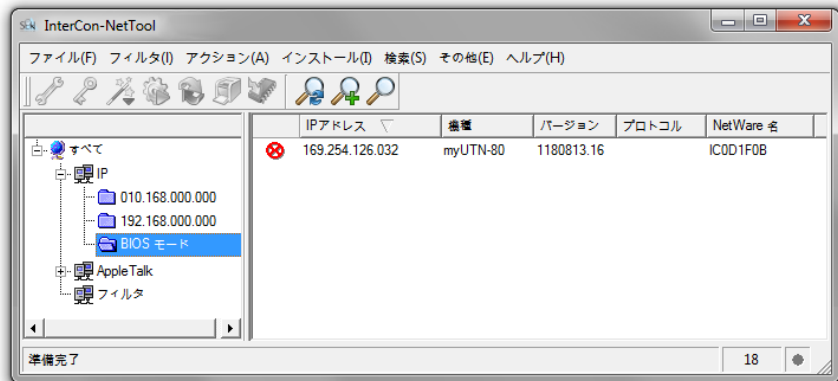


図 18 : InterCon-NetTool - BIOS モードの UTN サーバ

UTN サーバを BIOS モードから通常モードに切り替えることができるように、UTN サーバにソフトウェアを読み込む必要があります。

#### 手順

1. InterCon-NetTool を起動します。
  2. デバイスリストから UTN サーバを選択します。  
(UTN サーバは「BIOS モード」フィルタの下にあります。)
  3. メニューバーから、**インストール - IP ウィザード**を選択します。  
IP ウィザードが開始されます。
  4. ウィザードの指示に従って、IP アドレスを UTN サーバに割り当てます。  
IP アドレスが保存されます。
  5. UTN サーバ上でソフトウェアの更新を実行します。⇒ 101 を参照してください。
- 🔗 ソフトウェアが UTN サーバに保存されます。UTN サーバが通常モードに切り替わります。



## 考えられる原因

**SEH UTN Manager の機能の一部が見えない、有効にならない、または表示が不明瞭である**

- 使用するユーザアカウントに必要な管理者権限が付与されていない。SEH UTN Manager のユーザ権限に関連する問題です。「SEH UTN Manager - 機能の概要」⇒[124](#) 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。)

SEH UTN Manager を管理者で起動します。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。

## 考えられる原因

**UTN サーバとの接続が確立できない。**

UTN サーバとクライアントにインストールされた SEH UTN Manager 間のデータ転送には、共通ポートが使用されます。⇒[49](#)

- ポート番号が同一ではない。  
現在のポート番号を、クライアントにインストールされた SEH UTN Manager に転送できない。「SNMPv1」パラメータが無効になっている。⇒[37](#) を参照してください。
- 通信がファイアウォールによって遮断されている。

## 考えられる原因

**USB デバイスとの接続が確立できない。**

- USB デバイスへのアクセス制御が有効になっている。⇒[79](#)
- 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ない。
- USB デバイスが、すでに別のクライアントに接続されている。

**myUTN Control Center との接続が確立できない。**

考えられるエラー原因を取り除いてください。最初に、次を確認します。

- 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

これらが正常であるのにも関わらず接続が確立できない場合は、次の保護メカニズムが原因になっている可能性があります。

- アクセスが SSL/TLS (HTTPS) で保護されている。⇒[75](#)
- TCP ポートアクセス制御が有効になっている。⇒[77](#)
- パスワード保護が有効になっている。⇒[76](#)

### パスワードが使用できなくなった

myUTN Control Center へのアクセスはパスワードで保護できます。パスワードが使用できなくなった場合は、UTN サーバのパラメータ値を初期設定にリセットすると、myUTN Control Center にアクセスできるようになります。⇒[98](#) 以前の設定は削除されます。

## 8.6 付加ツール「utnm」

**utnm** 付加ツールの「utnm」は、SEH Computertechnik GmbH により myUTN 用に開発されました。USB デバイスをアクティブまた非アクティブにするためのツールです。

**使用** utnm で USB デバイスをアクティブまたは非アクティブにするには、オペレーティングシステムのコマンドラインインタフェースから、指定された構文でコマンドを入力して実行します。

または、USB デバイス用のスクリプトを記述します。スクリプトには、指定された構文でコマンドを記述します。スクリプトを実行すると、コマンドラインインタプレタにより、コマンドが 1 つずつ自動的に実行されます。

**利点と目的** utnm を使用すると、SEH UTN Manager (ミニマルバージョンの SEH UTN Manager ⇨ 19) のインタフェースをインストールすることも起動することはありません。

スクリプトの使用により、デバイスのアクティブ化など、頻繁に使用するコマンドシーケンスを自動化することができます。スクリプトは、ログインスクリプトなどを使用して自動的に実行できます。

- 選択できる作業**
- 「コマンドラインインタフェースを使用する」⇨ 131
  - 「スクリプトを作成する」⇨ 132

### コマンドラインインタフェースを使用する

- 必要事項**
- SEH UTN Manager がクライアントにインストールされていること。⇨ 19 を参照してください。
  - UTN サーバの IP アドレスまたはホスト名を確認済みであること。

#### 手順

1. コマンドラインインタフェースを開きます。
2. コマンドシーケンスを入力します。「構文およびコマンド」⇨ 132 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。

## 必要事項

## 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。⇒[19](#) を参照してください。
- ☑ UTN サーバの IP アドレスまたはホスト名を確認済みであること。

 手順

1. テキストエディタを開きます。
  2. コマンドシーケンスを入力します。「構文およびコマンド」⇒[132](#) を参照してください。
  3. ファイルを実行可能なスクリプトとして保存します。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。
- ☞ スクリプトが保存されます。スクリプトの使用に関する情報は、オペレーティングシステムの説明書に記載されています。

## 構文およびコマンド

構文は次のとおりです。

**Windows**

```
"<パス utnm.exe>" /c "<コマンド文字列>" [/<コマンド>]
```



「utnm.exe」ファイルは、SEH UTN Manager のプログラムフォルダ内にあります。

**Mac**

```
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」に格納されています。そこへのショートカットは /usr/local/bin/ というフォルダに保存されています。

次のコマンドがサポートされています。

コマンド	説明
<p>c "&lt;コマンド文字列&gt;"</p> <p>または</p> <p>command "&lt;コマンド文字列&gt;"</p>	<p>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。次のコマンド文字列が使用できます。</p> <ul style="list-style-type: none"> <li>• activate &lt;UTN サーバ&gt;&lt;ベンダ ID&gt;&lt;製品 ID&gt; [&lt;ポート番号&gt;] USB デバイスへの接続をアクティブにします。UTN サーバに同じ製品 ID とベンダ ID を持つ USB デバイスが複数ある場合、ポート ID が指定されていれば最初に認識されたデバイスをアクティブにします。</li> <li>• deactivate &lt;UTN サーバ&gt;&lt;ベンダ ID&gt;&lt;製品 ID&gt; [&lt;ポート番号&gt;] USB デバイスへの接続を非アクティブにします。USB 大容量ストレージデバイスを取り外すときは、「eject」コマンドを使用します。他のデバイスに対しては、「plugout」を使用します。</li> <li>• plugin &lt;UTN サーバ&gt;&lt;ベンダ ID&gt;&lt;製品 ID&gt; [&lt;ポート番号&gt;] USB デバイスへの接続をアクティブにします。UTN サーバに同じ製品 ID とベンダ ID を持つ USB デバイスが複数ある場合、ポート ID が指定されていれば最初に認識されたデバイスをアクティブにします。</li> <li>• plugout &lt;UTN サーバ&gt;&lt;ベンダ ID&gt;&lt;製品 ID&gt; [&lt;ポート番号&gt;] SB デバイスへの接続を非アクティブにします。 (デバイスの「plugging out」に相当) <b>メモ:</b> 「deactivate」コマンドの使用を推奨します。</li> <li>• eject &lt;UTN サーバ&gt;&lt;ベンダ ID&gt;&lt;製品 ID&gt; [&lt;ポート番号&gt;] (USB 大容量ストレージデバイス用) USB デバイスを取り外します。通信が正しく終了した場合に限り、デバイス接続は非アクティブになります。 <b>メモ:</b> 「deactivate」コマンドの使用を推奨します。</li> <li>• state &lt;UTN サーバ&gt;&lt;ベンダ ID&gt;&lt;製品 ID&gt;&lt;ポート番号&gt; USB デバイスの状態を表示します。</li> <li>• getlist &lt;UTN サーバ&gt; UTN サーバに接続されている USB デバイスの概要 (ポート、ベンダ ID、製品 ID、メーカー名、製品名、デバイスクラス、およびステータスなど) を示します。</li> <li>• set autoconnect = true false &lt;UTN サーバ&gt;&lt;ベンダ ID&gt;&lt;製品 ID&gt;&lt;ポート番号&gt; USB デバイスが接続され、なおかつ使用されていない場合、デバイスへの接続を自動的にアクティブにします。</li> </ul>
<p>p [&lt;ポート番号&gt;]</p> <p>または</p> <p>port [&lt;ポート番号&gt;]</p>	<p>UTN サーバ上の別の USB ポートを使用します。</p>

コマンド	説明
sp または ssl-port	UTN サーバ上の別の USB ポートを、SSL 暗号化を利用して使用します。
k <USB ポートキー> または key <USB ポートキー>	USB ポートキーを指定します。 ポートキー制御に使用する USB ポートのキーは、USB ポートに接続した USB デバイスを不要なアクセスから保護するために、myUTN Control Center から指定します (⇒ 79)。この USB デバイスにアクセスするには、適切なキーを入力する必要があります。
t <秒> または timeout <秒>	「activate」、「deactivate」、「plugin」、「plugout」、および「eject」コマンドのタイムアウト時間を指定します。
nw または no-warnings	警告メッセージを抑制します。
q または quiet	出力を抑制します。
o または output	コマンドラインの出力を示します。
v または version	utnm のバージョン情報を示します。
? または help	ヘルプページの表示。

コマンドの表記規約は次のとおりです。

- <UTN サーバ> = UTN サーバの IP アドレスまたはホスト名
- <ベンダ ID> = USB デバイスのベンダ ID
- <製品 ID> = USB デバイスの製品 ID
- 角括弧（ブラケット）内の要素は任意です
- 大文字、小文字を区別しない
- ASCII フォーマットのみ読み込み可能

## 戻り値

戻り値	説明
0	USB デバイスは利用できます。
20	USB デバイスの接続に失敗しました。
21	USB デバイスの切断に失敗しました。
22	USB デバイスの取り外しに失敗しました。
23	USB デバイスはすでに接続されています。
24	USB デバイスはすでに切断されています。
25	USB デバイ스에他のユーザが接続しています。
26	USB デバイ스에到達できません。
27	USB デバイ스의状態が不明です。
100	不明なコマンドです。
101	UTN サーバが見つかりません。UTN サーバが存在しない、または DNS 解決に失敗しました。
103	ポートキーが長すぎます。

## 例

USB デバイスをアクティブにする。コマンドおよび構文

**Windows**

```
"<パス utnm.exe>" /c "activate <UTN サーバ><ベンダ ID><製品 ID> [<ポート番号>]"
```

実際例：

```
"C:\Program Files\SEH Computertechnik GmbH\SEH UTN Manager\utnm.exe" /c "activate 192.168.0.140 0x0d7d 0x1400 4"
```

**Mac**

```
utnm -c "activate <UTN サーバ><ベンダ ID><製品 ID> [<ポート番号>]"
```

実際例：

```
utnm -c "activate 10.168.1.167 0x058f 0x6387 3"
```

## 8.7 図リスト

ネットワーク内の UTN サーバ	7
myUTN Control Center - ホーム	18
SEH UTN Manager - メインダイアログ	24
InterCon-NetTool - メインダイアログ	27
電子メールによる管理 - 例 1	30
電子メールによる管理 - 例 2	30
InterCon-NetTool - IP ウィザード	33
SEH UTN Manager - 圧縮	51
USB ポート単位での VLAN の割り当て	54
SEH UTN Manager - 選択リストの編集	58
SEH UTN Manager - デバイスの有効化	59
UTN アクションの作成ダイアログ	66
グローバル選択リスト	68
ユーザ固有の選択リスト	69
myUTN Control Center - 証明書	83
ネットワーク内の UTN サーバ - SSL/TLS 接続	94
SEH UTN Manager - 暗号化	95
InterCon-NetTool - BIOS モードの UTN サーバ	128