セキュアリモートアクセス

運用マニュアル

[システム管理者さま向け]

2024 年 5 月 29 日　Version 12.0

ソニービズネットワークス株式会社

改定履歴

Version	リリース日	改訂内容
5.0	2018 年 3 月 29 日	Version1.4.0 へのバージョンアップに伴い、以下の項目の手順を追加・修正しました。 ・「2　制限事項」に FAQ のリンクを追記しました。 ・P.13「シリアル ID が登録されない場合」の対応フローに、シリアル ID 確認方法について追記しました。 ・「4　アカウント設定」の内容を追加・修正しました。 ・「7-7　デバイス割当てインポート」を追加しました。 ・「7-8　デバイス割当てエクスポート」を追加しました。 ・「8-1　プロキシ設定」に注意点を追記しました。 ・「9　ローカルセグメント」にクライアント端末側の設定内容について追記しました。 ・「10-1　ユーザプロファイル送信」を「10-1　ユーザプロファイル個別送信」に修正しました ・「10-2　ユーザプロファイル一括送信」を追加しました。 ・「10-6　ユーザプロファイル一括登録手順」を追加しました。 ・「12-1　認証履歴」および「12-2　接続履歴」に注意点を追記しました。
5.1	2018 年 5 月 11 日	・8-1-1　プロキシ設定の重要項目を修正しました
6.0	2018 年 7 月 12 日	Version1.5.0 へのバージョンアップに伴い、以下の項目の手順を修正しました。 ・「5-2　デバイス ID の自動登録」の内容を修正しました。 ・「5-3　通知メール宛先」の内容を修正しました。 ・「10-1　ユーザプロファイル個別送信」の内容を修正しました。 ・「10-2　ユーザプロファイル一括送信」の内容を修正しました。
6.1	2018 年 11 月 14 日	・「5-2 デバイス ID の自動登録」の内容を修正しました。 ・「7-1 デバイス追加」の内容を修正しました。

Version	リリース日	改訂内容
6.2	2019年03月20日	Version1.6.0 へのバージョンアップに伴い、以下の項目の手順を修正しました。 ・「7-1 デバイス追加」の内容を修正しました。 ・「10-1 ユーザプロファイル個別送信」の内容を修正しました。 ・「10-2 ユーザプロファイル一括送信」の内容を修正しました。 ・「12-3 デバイス ID 登録処理履歴」の内容を修正しました。
6.3	2019年04月15日	・「1-2 サービス構成」の内容を修正しました。
7.0	2019年07月17日	Version1.7.0 へのバージョンアップに伴い、以下の項目の手順を修正しました。 ・マニュアル名を「スタートアップマニュアル」から「運用マニュアル」に変更しました。 ・「1-1 本マニュアルについて」の内容を修正しました。 ・「1-2 サービス構成」の内容を修正しました。 ・「2 制限事項」の内容を修正しました。 ・「5-1 認証タイプ」に Azure Active Directory 設定を追加しました。 ・「6-1 ユーザ作成」の内容を修正しました。 ・「6-2 CSV によるユーザー一括登録」の内容を修正しました。 ・「12-1 認証履歴」の内容を修正しました。
7.1	2020年07月03日	・「5-1 認証タイプ」の内容を修正しました。
8.0	2020年12月11日	Version1.8.0 へのバージョンアップに伴い、以下の項目の手順を追加・修正しました。 ・「1-2 サービス構成」の内容を修正しました。 ・「5-1 認証タイプ」の内容を修正しました。 ・「5-2 デバイス ID の自動登録」の内容を修正しました。 ・「7 デバイス設定」の内容を修正しました。 ・「14 サポート体制」を追加しました。
8.1	2021年4月12日	・「1-2 サービス構成」の内容を修正しました。 ・「5-2 デバイス ID の自動登録」の内容を修正しました。 ・「7-1 デバイス追加」の内容を修正しました。
8.2	2021年6月7日	・「1-2 サービス構成」の内容を修正しました。 ・「5-2 デバイス ID の自動登録」の内容を修正しました。 ・「7-1 デバイス追加」の内容を修正しました。

9.0	2022 年 3 月 17 日	Version2.1.0 へのバージョンアップに伴い、以下の項目の手順を追加・修正しました。 ・「1-1 本マニュアルについて」の内容を修正しました。 ・「1-2 サービス構成」の図を修正しました。 ・「9 ローカルセグメント」の内容を修正しました。 ・「10-1 ユーザプロファイル個別送信」の内容を修正しました。 ・「10-2 ユーザプロファイル一括送信」の内容を修正しました。 ・「12 スプリットトンネル」を追加しました。 ・「13-1 認証履歴」の内容を修正しました。
9.1	2022 年 3 月 17 日	・「12 スプリットトンネル」の内容を修正しました。
10.0	2022 年 4 月 5 日	・窓口変更に伴い、窓口情報を修正しました。
10.1	2022 年 5 月 26 日	・「12 スプリットトンネル」の内容を修正しました。
11.0	2023 年 3 月 23 日	Version2.2.0 へのバージョンアップに伴い、以下の項目の手順を追加・修正しました。 ・「8 プロキシ」の内容を修正しました。 ・「9 ローカルセグメント」の内容を修正しました。 ・「11 ファイアウォール」の内容を修正しました。 ・「12 スプリットトンネル」の内容を修正しました。
12.0	2024 年 5 月 29 日	・Microsoft 社による「Azure Active Directory」の名称変更に伴い、図を更新しました。 「Azure Active Directory」 → 「Microsoft Entra ID」へ名称変更しました。 ・「1-2 サービス構成」の内容を修正しました。 ・「5-1.認証タイプ」の内容を修正しました。 ・「6-2 CSV によるユーザー括登録」の内容を修正しました。 ・「7-2 デバイスインポート」の内容を修正しました。

Version ナンバー変更ガイドライン

誤字脱字の修正、文書・図・表の差し替えなど手順の変更がない場合：例 Ver 1.0 ⇒ Ver 1.1

サービスのバージョンアップ、仕様変更に伴う手順の変更がある場合：例 Ver 1.0 ⇒ Ver 2.0

目次

1 はじめに 9
1-1 本マニュアルについて 9
1-2 サービス構成 11
2 制限事項 19
3 マネージメントツールのログイン／ログアウト 20
3-1 マネージメントツールへのログイン方法 20
3-2 マネージメントツールからのログアウト方法 21
4 アカウントの設定 22
4-1 アカウントの変更 22
4-2 メールアドレスの変更 23
4-3 パスワードの変更 25
4-4 パスワードの再設定 26
5 全体設定 29
5-1 認証タイプ 29
5-2 デバイス ID の自動登録 35
5-3 通知メール宛先 37
5-4 DNS サーバ 38
5-5 VPN ネットワークアドレス 38
6 ユーザ設定 39
6-1 ユーザ作成 39
6-2 CSV によるユーザ一括登録 41
6-3 ユーザ情報のエクスポート 45
6-4 ユーザ毎の接続許可 46
6-5 ユーザの削除 47
7 デバイス設定 49
7-1 デバイス追加 49
7-2 デバイスインポート 54
7-3 デバイスエクスポート 58
7-4 デバイス毎の接続許可 59
7-5 デバイスの削除 60
7-6 デバイス割当 61
7-7 デバイス割当インポート 64

7-8 デバイス割当エクスポート 67
7-9 デバイス割当解除 68

8 プロキシ設定 70
8-1 プロキシ設定 70
8-2 プロキシの適用 72
8-3 プロキシの適用解除 74

9 ローカルセグメント設定 77
9-1 ローカルセグメント設定 78
9-2 ローカルセグメントの適用 78
9-3 ローカルセグメントの適用解除 80

10ユーザプロファイル設定 83
10-1ユーザプロファイル個別送信 83
10-2ユーザプロファイル一括送信 86
10-3デバイス ID の登録 88
10-4ユーザプロファイル毎の接続許可 91
10-5ユーザプロファイル削除 92
10-6ユーザプロファイル一括登録手順 93

11ファイアウォール設定 99
11-1ファイアウォール設定の新規作成 100
11-2ファイアウォール設定のユーザプロファイル割当解除 105
11-3ファイアウォール設定の優先順位 108
11-4ファイアウォール設定の複製 110
11-5ファイアウォール設定の削除 112
11-6ユーザプロファイル毎ファイアウォール設定適用状況の確認 114

12スプリットトンネル設定 116
12-1スプリットトンネル設定の新規作成 117
12-2スプリットトンネル設定の複製 122
12-3スプリットトンネル設定の削除 124

13利用履歴 126
13-1認証履歴126
13-2接続履歴127
13-3デバイス ID 登録処理履歴 128
13-4操作履歴130

14各種参考情報 131

15サポート体制 132
15-1お問い合わせ窓口 132
15-2ご連絡前のお願い 132
15-3切り分け調査のご協力のお願い 132

1 はじめに

1-1 本マニュアルについて

このたびは、セキュアリモートアクセスサービスをご契約いただき、ありがとうございます。

セキュアリモートアクセスはユーザ認証、デバイス認証と暗号化により、インターネット経由でもセキュアな通信を実現し、自宅や外出先のスマートデバイス・PC からお客さまネットワーク、bit-drive データセンター内クラウドサーバへアクセスします。

> **重要**
> - 本サービスでは、クライアントソフトウェアとして”Cisco AnyConnect”を利用しています。クライアント OS によって、クライアントソフトウェアの名称が変わりますのでご注意ください。

セキュアリモートアクセスの設定マニュアルは、マネージメントツールの各種設定を記載した管理者さま向け「運用マニュアル」と、管理者さま向けの各種設定について最低限の機能(基本的な VPN 接続が可能となる)を記載した「クイックガイド」、クライアントソフトウェアの各種設定を記載したご利用者さま向け「ユーザガイド」の 3 種類のマニュアルを用意しております。

本マニュアルでは、管理者さま向けの各種設定について記載しています。

なお、各種マニュアルの位置づけは下表のとおりです。

設定内容	マニュアル名	
全体共通設定 （管理者さま向け）	クイックガイド 簡易手順	運用マニュアル 詳細手順　※本資料
クライアント端末設定 （ユーザさま向け）	ユーザガイド	

> **重要**
> - 本サービスのご利用にあたり、クライアント端末設定も行う必要がございます。「ユーザガイド」も併せてご確認ください。

セキュアインターネットゲートウェイ"Cisco Umbrella"とセキュアリモートアクセスを連携させたい場合、Umbrella 側で設定する Umbrella ポータルサイトでの作業につきましては弊社にて実施のうえ、提供いたします。

Umbrella モジュールにつきましては、セキュアインターネットゲートウェイ"Cisco Umbrella"のサイトでも入手可能ですが、セキュアリモートアクセスのサイトにも同様のモジュールを入手いただけます。

詳細につきましては、セキュアインターネットゲートウェイ"Cisco Umbrella"のマニュアルをご参照ください。

https://www.bit-drive.ne.jp/support/technical/cisco-umbrella/

セキュアリモートアクセスには以下のようにサービス固有の用語があります。

【セキュアリモートアクセスのサービス固有用語】

- ✓ ローカルセグメントアクセス

  セキュアリモートアクセスクライアント端末が VPN 接続中に物理的に接続されているサブネットに対するアクセス。

- ✓ スプリットトンネルアクセス

  セキュアリモートアクセスクライアント端末が VPN を経由した通信と端末から直接アクセスする通信とを分けて管理する機能です。

- ✓ 外部インターネット接続

  セキュアリモートアクセスクライアント端末が VPN 接続中に行う Web アクセス。

- ✓ デバイス ID

  デバイス認証に使用する識別 ID の総称。

  補足デバイス ID は、下記シリアル ID と MAC アドレスから選択できます。

- ✓ シリアル ID

  セキュアリモートアクセスクライアント端末固有の ID。

- ✓ ユーザプロファイル

  セキュアリモートアクセスユーザ毎に払い出される個々の設定ファイル。

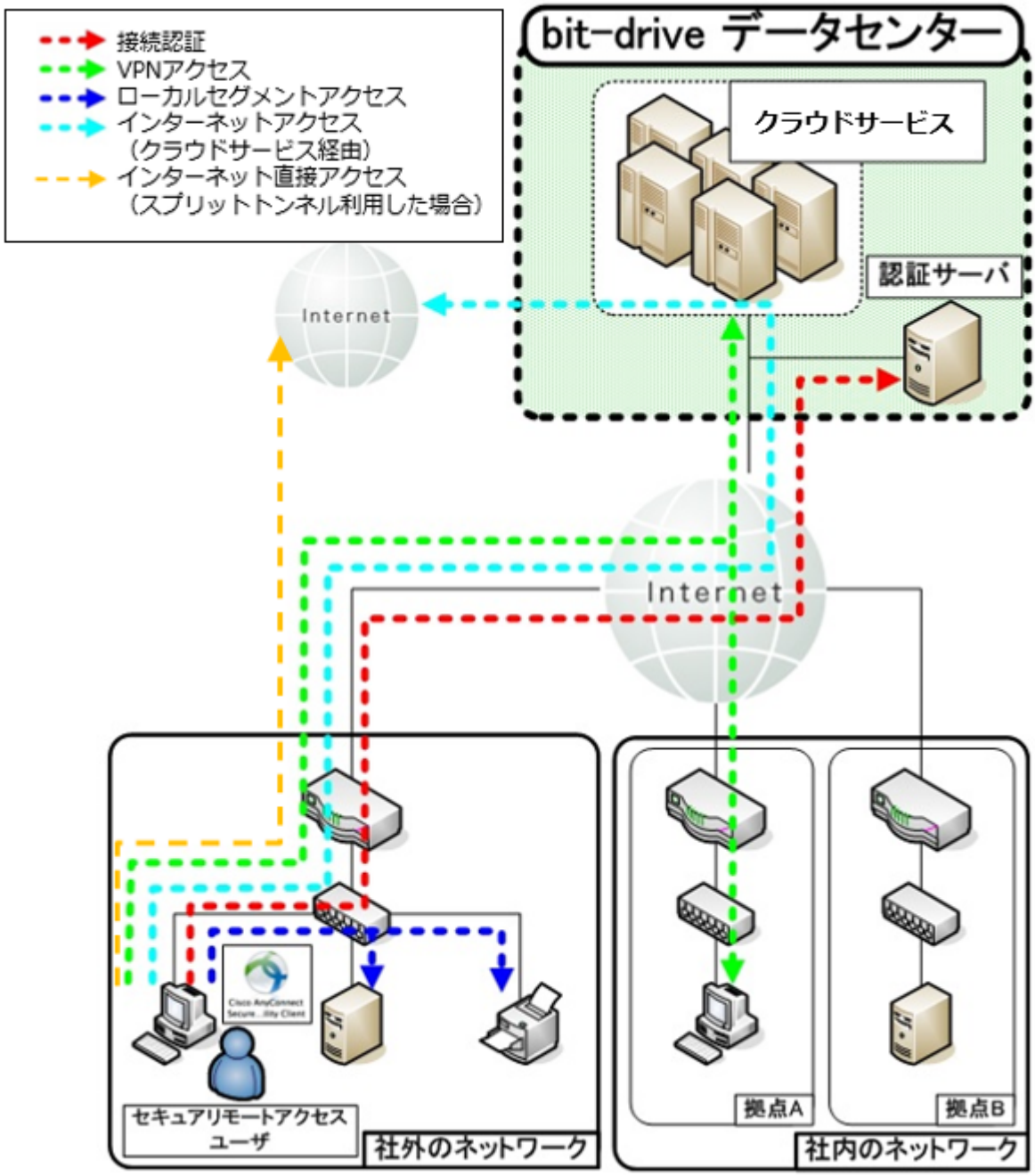
1-2　サービス構成

【接続構成】

セキュアリモートアクセス利用時の簡易的な接続構成図は以下になります。

点線はセキュアリモートアクセスを使用してお客さまネットワーク、bit-drive データセンターに接続する際のルートです。

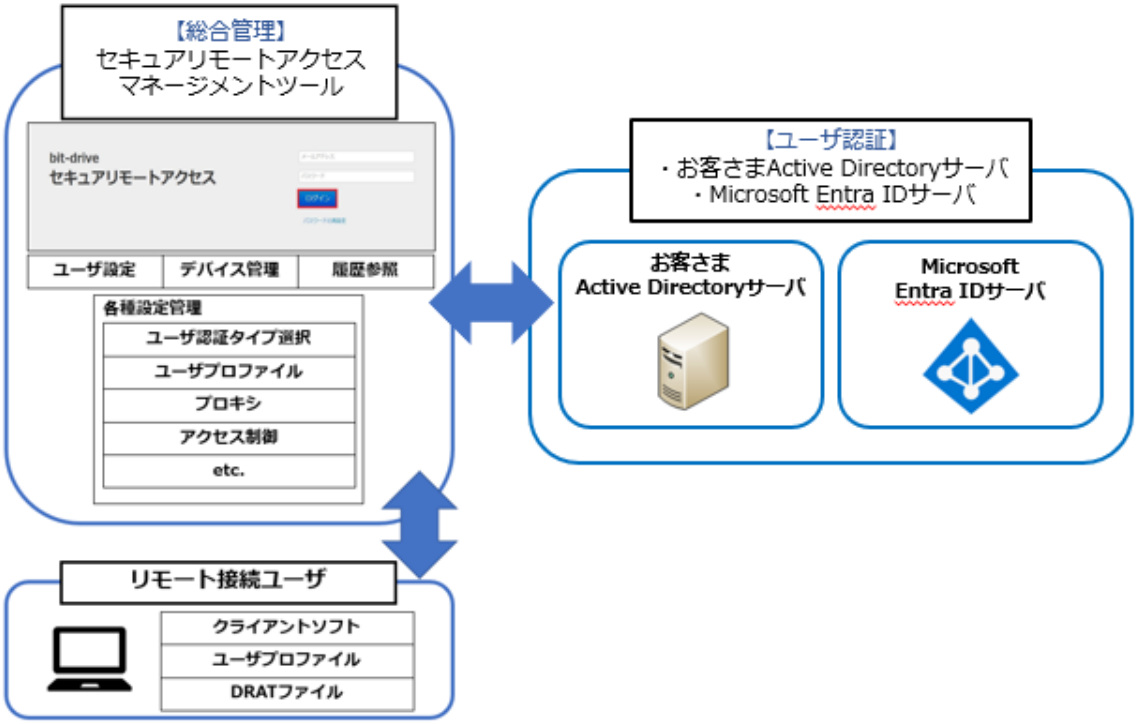
> **重要**
> - bit-drive データセンター内のクラウドサーバを使用する場合は、それぞれ別途契約が必要です。



【管理構成】

セキュアリモートアクセス利用時の管理構成概要図は以下になります。

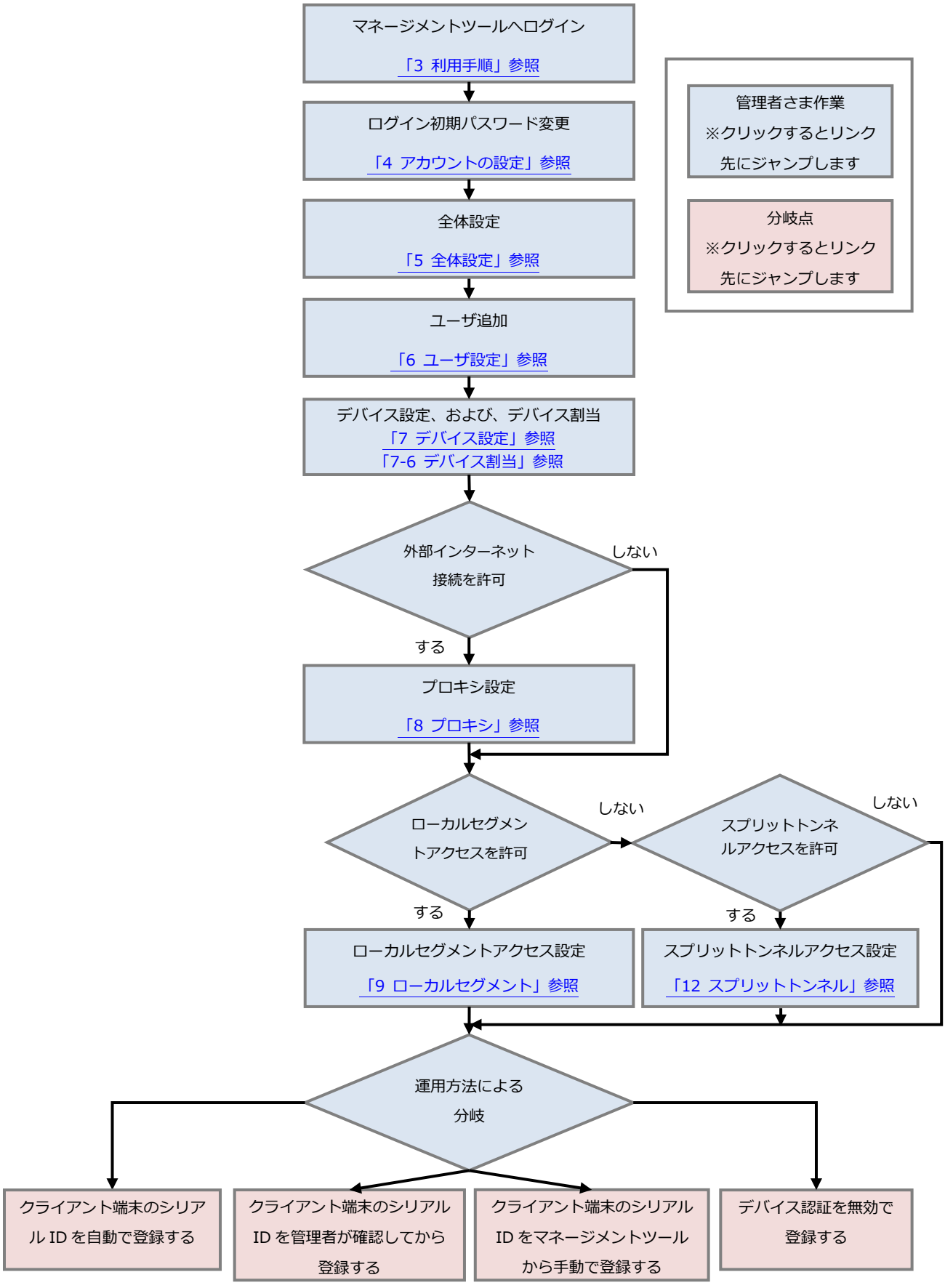
> **重要**
> - ユーザ認証には、お客さま Active Directory サーバ、Microsoft Entra ID サーバのいずれか 1 つが必要となります。



セキュアリモートアクセスの初期設定簡易フロー図は以下になります。

共通部分以降の設定に関しては、運用方法に沿ったものを選択してください。

【共通部分】

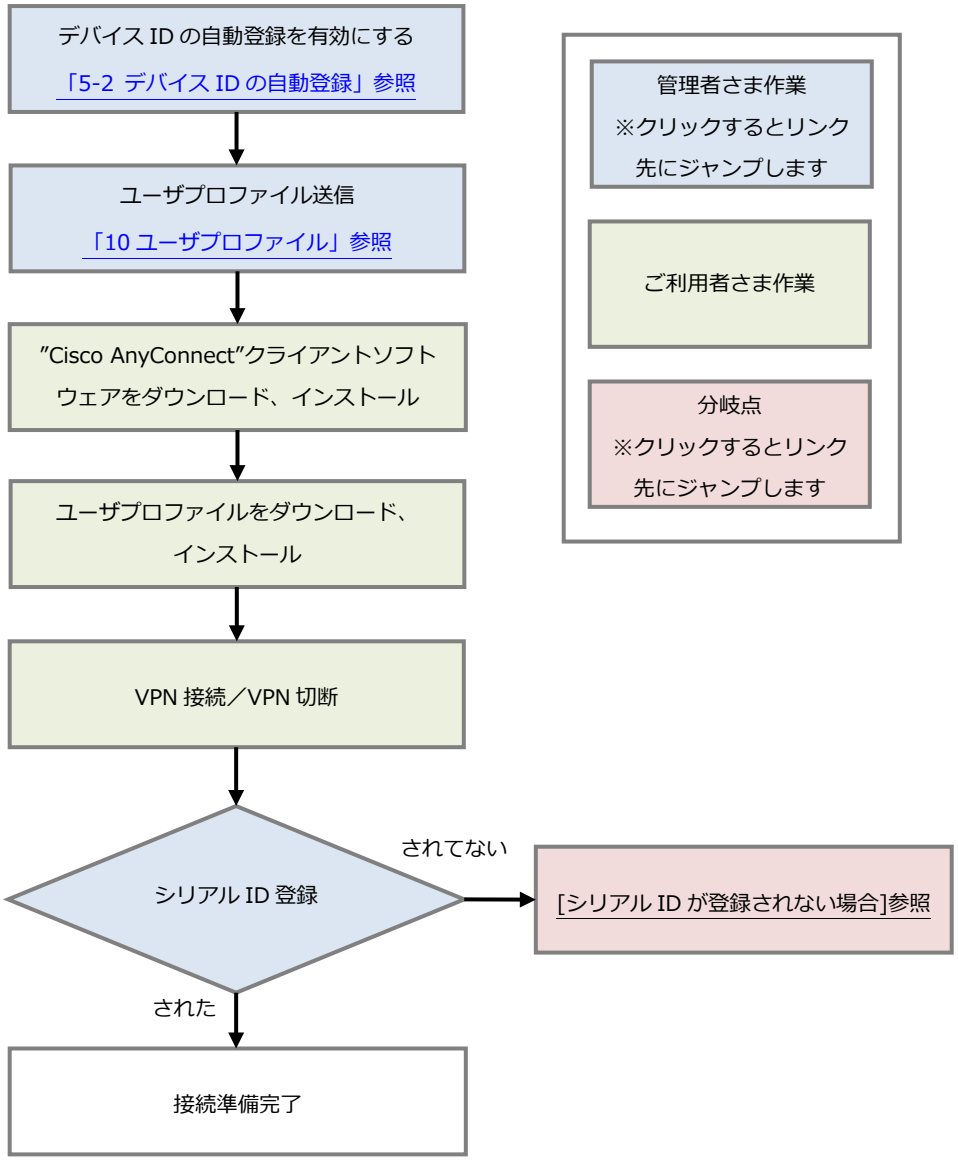


【クライアント端末のシリアル ID を自動で登録する場合】

こちらのフローでは初回接続時にクライアント端末のシリアル ID がマネージメントツールに自動で登録されます。

初回接続は、シリアル ID の登録のみ自動で行われ、再接続することにより VPN 接続が確立されます。

”Cisco AnyConnect”クライアントソフトウェアのインストールなど、ご利用者さま作業の詳細手順は別マニュアルの「ユーザガイド」を確認してください。

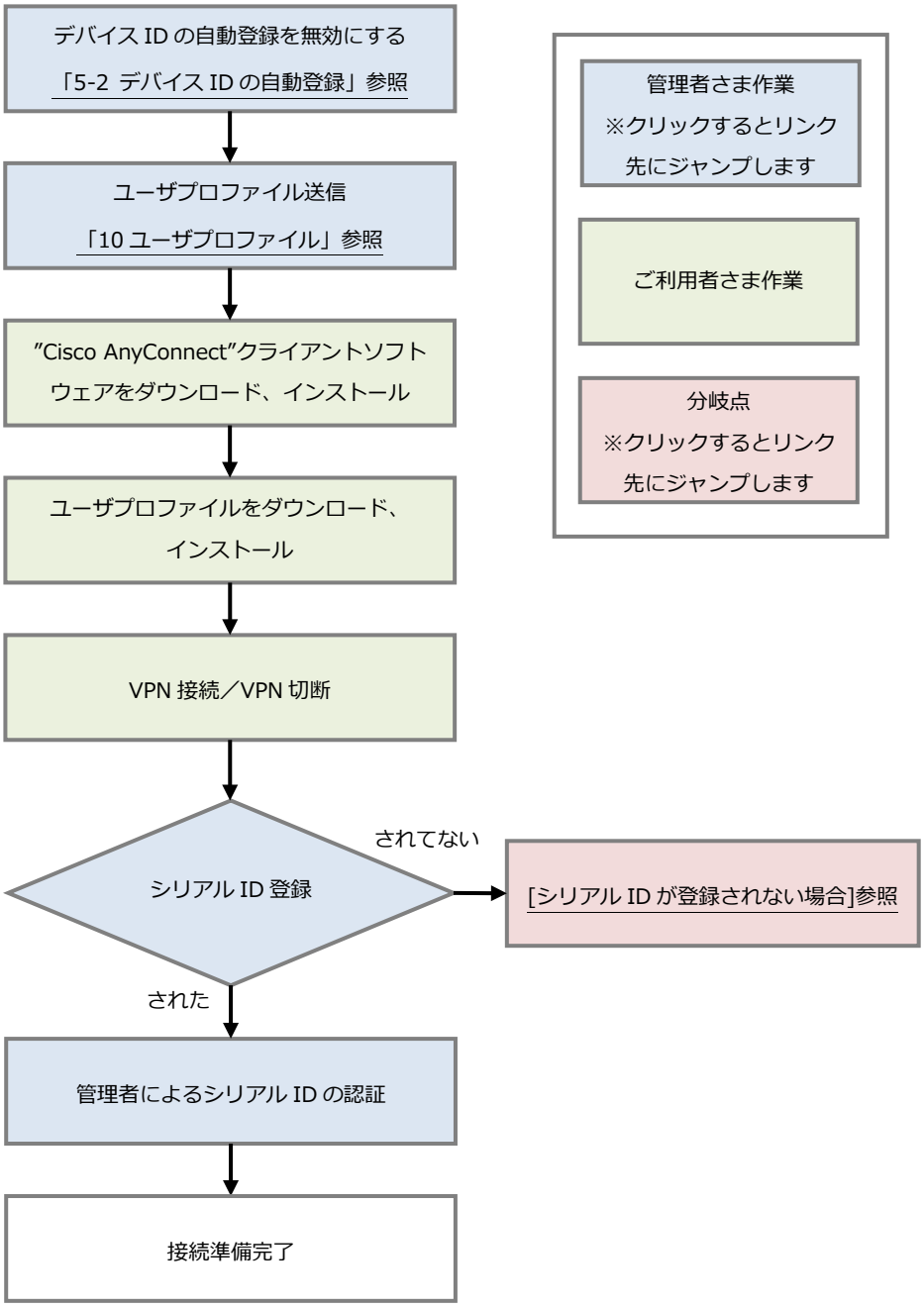


【クライアント端末のシリアル ID を管理者が確認してから登録する場合】

こちらのフローでは初回接続時にクライアント端末のシリアル ID がマネージメントツールに通知されます。

セキュアリモートアクセスの利用を許可する端末のシリアル ID と相違がなければ、承認を行ってください。承認後再接続すると VPN 接続が確立されます。

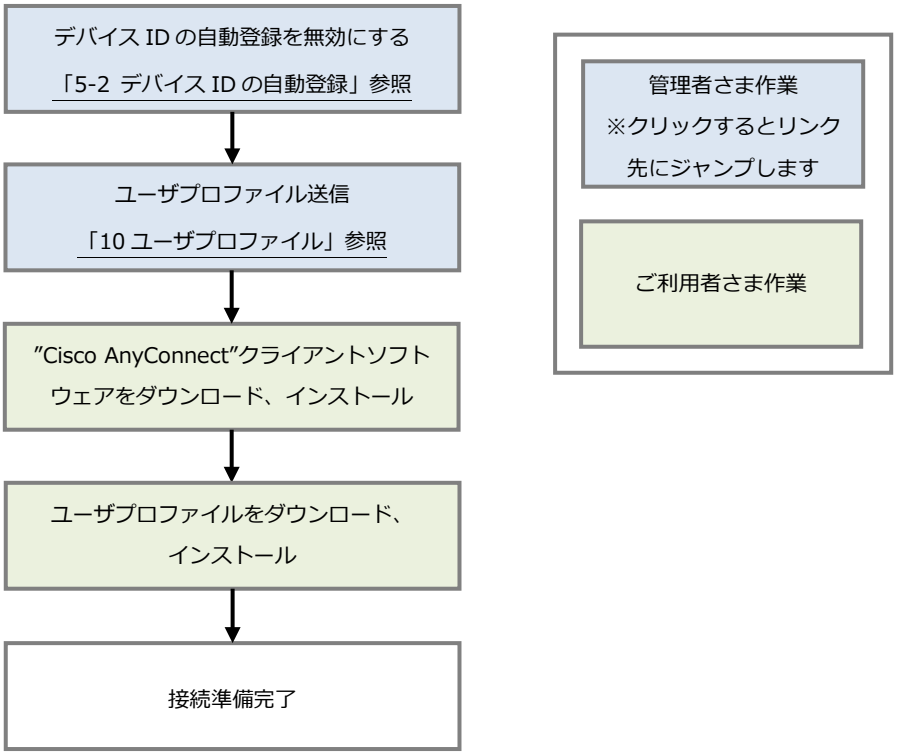
”Cisco AnyConnect”クライアントソフトウェアのインストールなど、「ご利用者さま作業」の詳細手順は別マニュアルの「ユーザガイド」を確認してください。



【クライアント端末のシリアル ID をマネージメントツールから手動で登録する場合】

こちらのフローではクライアント端末のシリアル ID をマネージメントツールに手動で設定します。手動で設定することにより、初回接続から VPN 接続が確立されます。

”Cisco AnyConnect”クライアントソフトウェアのインストールなど、「ご利用者さま作業」の詳細手順は別マニュアルの「ユーザガイド」を確認してください。



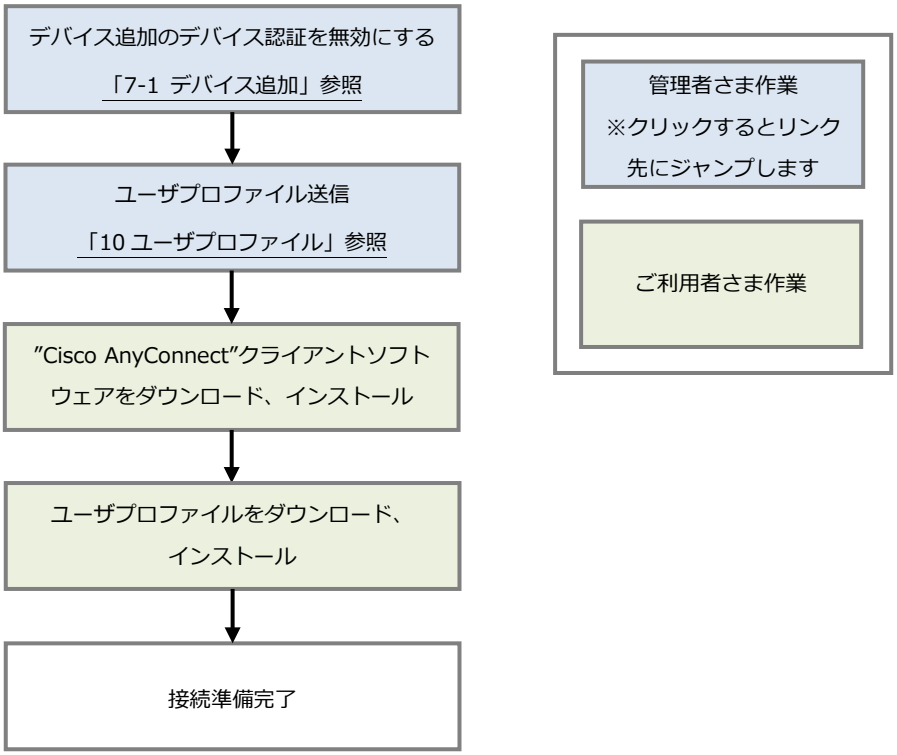
【デバイス認証を無効で登録する場合】

こちらのフローではクライアント端末のシリアル ID を利用せずに VPN 接続を行う事ができます。

重要

- 「デバイス認証」の「無効」設定は、固有のデバイス ID を持たず、デバイス認証を行なうことができないデバイス利用を想定した設定となります。
  上記以外のデバイスによる「無効」設定もご利用可能ではありますが、よりセキュリティの高い「有効」設定を推奨しております。

”Cisco AnyConnect”クライアントソフトウェアのインストールなど、「ご利用者さま作業」の詳細手順は別マニュアルの「ユーザガイド」を確認してください。



【シリアル ID が登録されない場合】

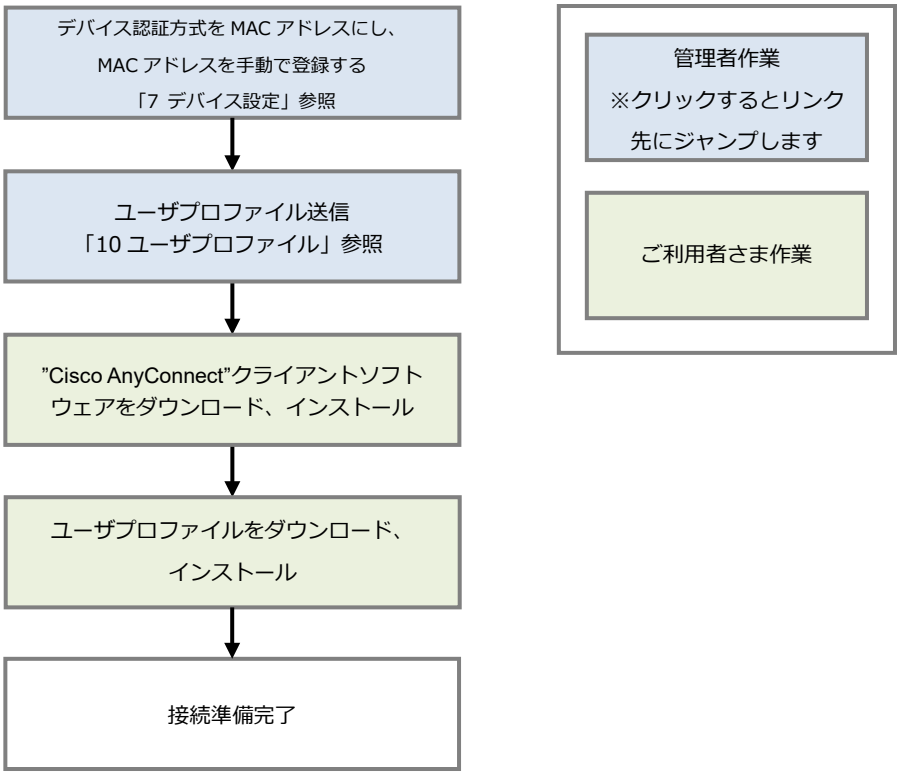
シリアル ID（シリアルナンバー）が特殊もしくは、存在しない OEM 製品などでセキュアリモートアクセスを利用する場合は、シリアル ID で利用することはできません。

デバイス認証方式を MAC アドレスに設定し、ご利用ください。

”Cisco AnyConnect”クライアントソフトウェアのインストールなど、「ご利用者さま作業」の詳細手順は別マニュアルの「ユーザガイド」を確認してください。

重要

- デバイス認証方式が MAC アドレスの場合、マネージメントツールに MAC アドレスを手動で登録する必要があります。
- シリアル ID の手動確認方法は、ユーザガイドに掲載されている、各 OS の『【参考情報】シリアル ID の確認』項目を参照してください。



2 制限事項

本マニュアルに記載されている内容以外の機能および作業に関しましては、サポート対象外となりますのでご注意ください。

セキュアリモートアクセスを利用するにあたり以下の制限事項があります。

- Active Directory および Microsoft Entra ID のユーザ設定にて「ユ―ザーは次回ログオン時にパスワード変更が必要」にチェックが入っており、パスワード変更をしていない場合は、セキュアリモートアクセスの認証に失敗します。

  このチェックを外すもしくは、パスワードの変更を行った後、再度接続を行ってください。

- ファイアウォール設定にて行う設定は双方向での通信が制御されます。片方向のみの制御はできません。

  【例】

  ファイアウォール設定の宛先 IP アドレスに 192.168.1.1 に対する通信破棄設定を行った場合

  セキュアリモートアクセスクライアント端末から 192.168.1.1 に対する通信と 192.168.1.1 からセキュアリモートアクセスクライアント端末に対する通信が破棄されます。

- セキュアリモートアクセスクライアント端末同士の通信はできません。

- セキュアリモートアクセスクライアント端末に対する以下の作業は管理者権限を持つアカウントで実施してください。
  - ”Cisco AnyConnect”クライアントソフトウェアのインストール、アンインストール
  - ユーザプロファイルのインストール

- ソフトバンク　モバイル回線の Android OS は、セキュアリモートアクセスの仕様上利用できません。

- セキュアリモートアクセスクライアント端末にリモートデスクトップ経由でログインしている場合、セキュアリモートアクセスは利用できません。

- デバイス認証方法に関しては、セキュアリモートアクセスクライアント端末で一意に設定され、セキュリティの強固なシリアル ID 認証を推奨します。

  シリアル ID（シリアルナンバー）が特殊もしくは、存在しない OEM 製品などでセキュアリモートアクセスを利用する場合は、デバイス認証方法を MAC アドレス認証にしてください。

- セキュアリモートアクセスを MAC アドレス認証で利用する場合は、認証に使用する MAC アドレスが登録されているネットワークアダプタは有効になっている必要があります。

- スプリットトンネル機能とローカルセグメント機能を同時に使用することはできません。

制限事項の詳細やその他情報に関しましては、以下 FAQ をご参照ください

https://faq2.bit-drive.ne.jp/support/traina-faq/result?ds=&inquiryWord=&selectedDataSourceId=16&categoryPath=152

3 マネージメントツールのログイン／ログアウト

マネージメントツールより、ユーザ設定やデバイス設定などの各種設定を行うことができます。

3-1 マネージメントツールへのログイン方法

1. Web ブラウザにて、以下 URL にアクセスします。

   URL:https://acmt.ravpn.bit-drive.ne.jp

2. ログイン画面が表示されるので、それぞれ下記の項目を入力し、「ログイン」をクリックします。

項目	入力値・内容
メールアドレス	契約時に送付される「登録内容通知」に記載されております。
パスワード	契約時に送付される「登録内容通知」に記載されております。

メモ
- ログインするための【メールアドレス】と【パスワード】に関しては、契約時に送付される「登録内容通知」をご確認ください。
- ここでご使用いただくログイン【メールアドレス】は「管理者アカウント」となり、管理者アカウントを追加および削除することはできません。

重要
- パスワードを 5 回以上間違えると、パスワードロックがかかります。
- パスワードロックは 30 分後に自動解除されます。

3. マネージメントツールのトップ画面が表示されます。

以上で、マネージメントツールへのログイン方法は終了です。

3-2 マネージメントツールからのログアウト方法

1. 赤枠の  をクリックします。

2. プルダウンメニューから「ログアウト」をクリックします。

3. ログアウトを完了すると、下記のログイン画面が表示されます。

以上で、マネージメントツールからのログアウト方法は終了です。

4 アカウントの設定

アカウント設定より、マネージメントツールにログインする際のメールアドレス、パスワードを変更することができます。

4-1 アカウントの変更

1. 赤枠の  をクリックします。

2. プルダウンメニューから「アカウント設定」をクリックします。

3. 現在設定されているアカウント情報が表示されます。

重要

- メンテナンス通知メール等、弊社から配信される本サービスに関わる通知に関しては、お申込み時に登録された技術担当者さま宛に通知されます。

  技術担当者さま情報はマネージメントツールから変更することはできません。ご変更の際は、NURO Biz インフォメーションデスクまでご連絡ください。

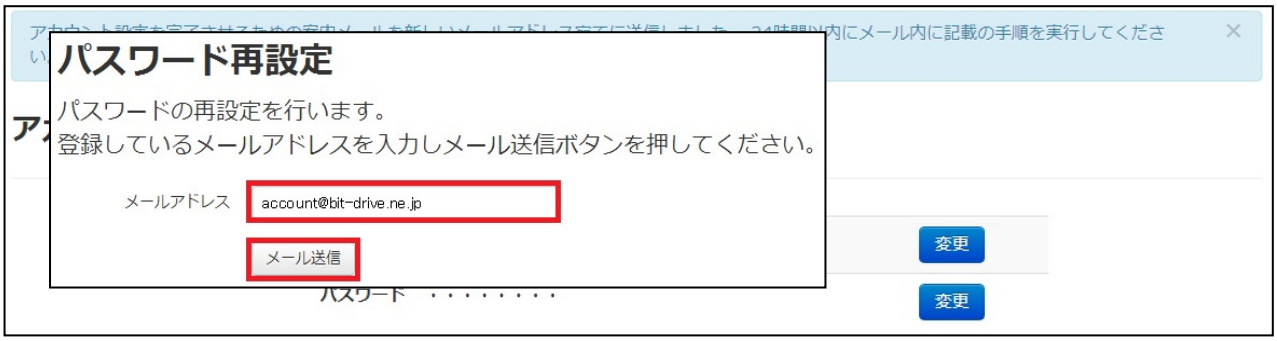
4-2　メールアドレスの変更

1. メールアドレスの欄にある、「変更」をクリックします。

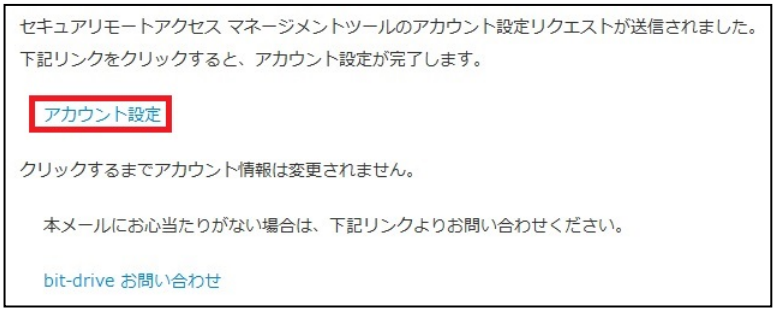
2. 「変更」をクリックすると、下記の画面が表示されます。すべて入力後、右下の「登録」ボタンをクリックします。

項目	入力値・内容
現在のパスワード	現在のパスワード（画面には表示されません）
新しいメールアドレス	変更後のメールアドレス（画面には表示されません）
新しいメールアドレスの確認	変更後のメールアドレス（画面には表示されません）

3. 以下の画面が表示され、登録した新しいメールアドレス宛にアカウント設定のメールが送信されます。



4. 登録した新しいメールアドレスで以下の内容のメールを受信し、「アカウント設定」をクリックします。



5. メールアドレスの変更が完了すると、以下の画面が表示されます。

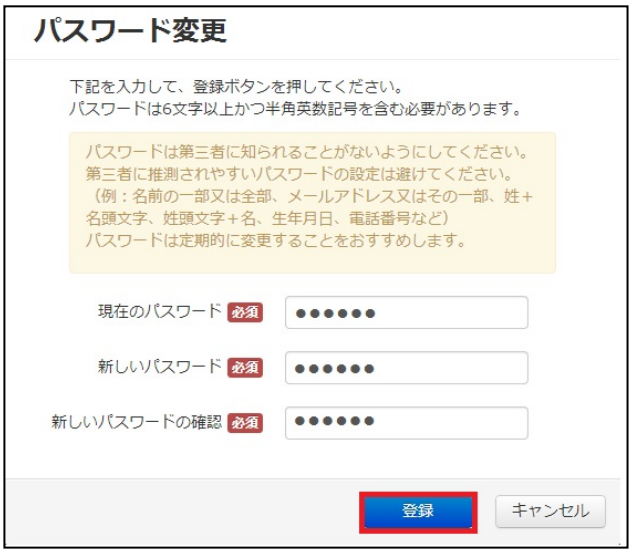
以上で、メールアドレスの変更は終了です。

4-3　パスワードの変更

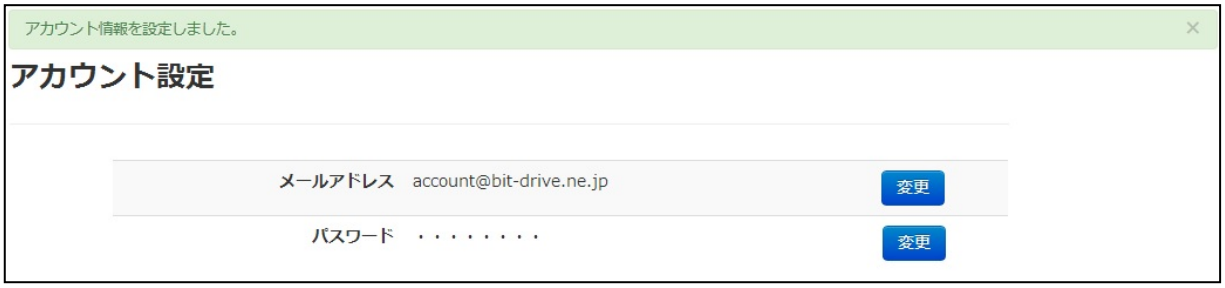
1. パスワードの行にある、「変更」をクリックします。

2. 「変更」をクリックすると、下記の画面が表示されます。すべて入力後、右下の「登録」ボタンをクリックします。

項目	入力値・内容
現在のパスワード	変更前のパスワード（画面には表示されません）
新しいパスワード	変更後のパスワード（画面には表示されません）
新しいパスワードの確認	変更後のパスワード（画面には表示されません）



3. パスワードの変更が完了すると、以下の画面が表示されます。



以上で、パスワードの変更は終了です。

4-4 パスワードの再設定

ログインアカウントのメールアドレスが使用できる場合は、マネージメントツールからパスワードの再設定を行うことができます。

重要

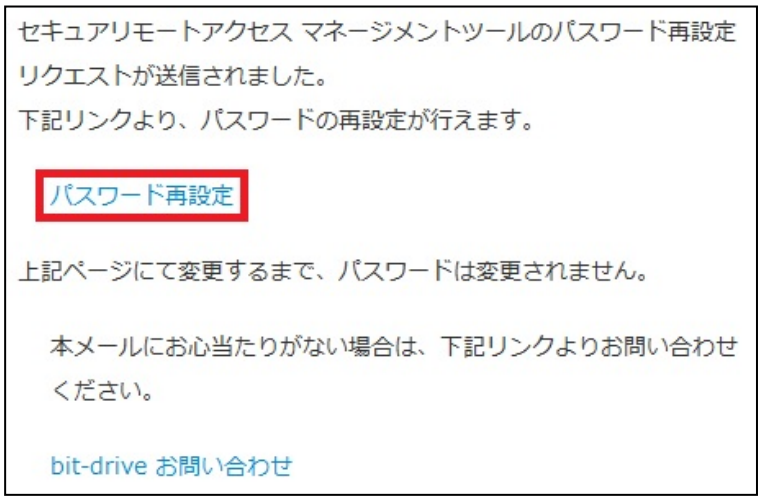
- メールアドレス・パスワードの両方が分からない場合は、NURO Biz サポートデスクまでご連絡ください。アカウント情報の初期化を実施させていただきます。初期化後のアカウント情報は、契約時に送付される「登録内容通知」のアカウント情報と同じものになります。

1. 下記のログイン画面において、右側の「パスワードの再設定」をクリックします。

2. 「パスワード再設定」画面の「メールアドレス」欄にて、登録しているメールアドレスを入力し「メール送信」をクリックします。

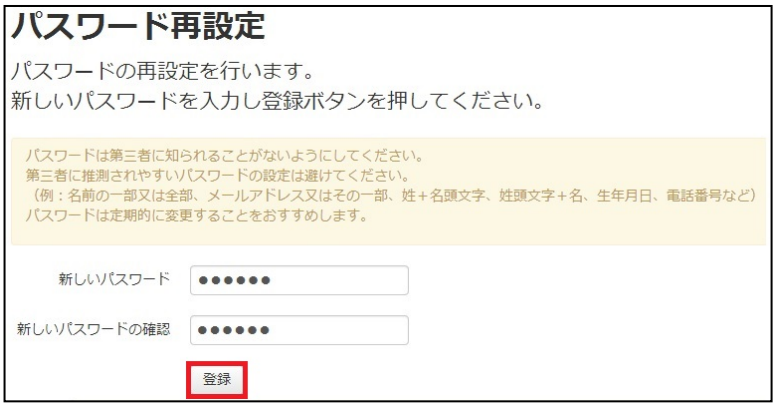
3. 下記のメッセージが表示されます。

4. 指定したメールアドレスで以下の内容のメールを受信し、「パスワードの再設定」をクリックします。



5. 以下の画面が表示されます。すべて入力後、「登録」ボタンをクリックします。

項目	入力値・内容
新しいパスワード	変更後のパスワード（画面には表示されません）
新しいパスワードの確認	変更後のパスワード（画面には表示されません）



6. パスワードの変更が完了すると、以下の画面が表示されます。

以上で、パスワードの再設定は終了です。

5 全体設定

全体設定より、ユーザ認証方法やデバイス ID の自動登録許可設定などを行なうことができます。

全体設定に関する設定は「全体設定」タブから行ないます。

5-1 認証タイプ

1. セキュアリモートアクセスのユーザ認証方法は 2 つあります。「認証タイプ」欄にて、どちらの認証方法を採用するか選択します。

① Active Directory

Active Directory に登録されているユーザがセキュアリモートアクセスの利用ユーザとして追加できるようになり、Active Directory と連携し認証をします。

② Microsoft Entra ID

Microsoft Entra ID に登録されているユーザがセキュアリモートアクセスの利用ユーザとして追加できるようになり、Microsoft Entra ID と連携し認証をします。

2. Active Directory を選択した場合
Active Directory を選択すると、Active Directory 設定画面が表示されます。下記のように入力し、設定をクリックします。

重要

- それぞれの項目の詳細に関しては、以下の【参考情報】を確認ください。

  Active Directory 設定を行う際は、プライマリ Active Directory が起動しており、セキュアリモートアクセス認証サーバ[10.255.254.136]との疎通がとれる必要があります。

  ※ファイアウォールなどで通信制限を行われている場合には、セキュアリモートアクセス認証サーバ IP アドレスの許可設定を行なってください。
- セカンダリ Active Directory がある場合は、セカンダリの項目も必ず入力してください。セカンダリの項目が入力されていない場合、プライマリがダウンしたとしても、セカンダリに切り替わりません。
- Active Directory において、各ユーザのログオン先設定で制限を掛けている場合、セキュアリモートアクセスのコンピュータ名「DG*****-AC01-RD」が登録されていないと、接続できません。「Active Directory 設定」完了後、Active Directory 側でセキュアリモートアクセスで利用するコンピュータ「DG*****-AC01-RD」が登録されますので、各ユーザのログオン先設定に追加してください。
- [DG****-AC01-RD]は、セキュアリモートアクセスサービスにおける弊社認証サーバとなります。弊社認証サーバはお客さま Active Directory にドメイン参加した上で認証の動作を行なっておりますので、お客さま Active Directory 側におきましても、[DG****-AC01-RD]を削除しないようご注意ください。

※上記内容は設定例です。実際の設定内容はお客さま環境に併せて入力してください。

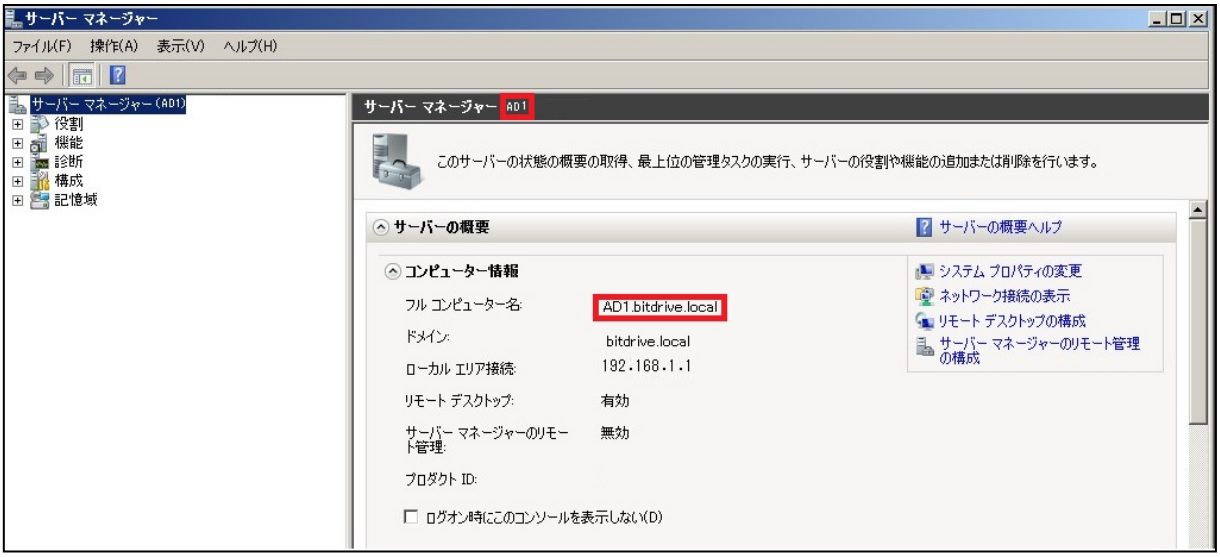
項目	入力値・内容
ホスト名（プライマリ）【必須】	Active Directory のホスト名 **※フルコンピュータ名のドメイン名より前の部分がホスト名となります**
IP アドレス（プライマリ）【必須】	Active Directory の IPv4 アドレス
ホスト名（セカンダリ）	セカンダリ Active Directory のホスト名 **※フルコンピュータ名のドメイン名より前の部分がホスト名となります**
IP アドレス（セカンダリ）	セカンダリ Active Directory の IPv4 アドレス
Active Directory ドメイン名【必須】	Active Directory ドメイン名
管理者ユーザ名	Active Directory の管理者アカウント
管理者パスワード【必須】	Active Directory の管理者パスワード
NetBIOS ドメイン名	NetBIOS ドメイン名と Active Directory ドメイン名に差異がある Active Directory をご利用の場合、Active Directory の NetBIOS ドメイン名

- **【参考情報】**

Active Directory の<ホスト名>、<IP アドレス>、<Active Directory ドメイン名>は、Active Directory の「サーバーマネージャー」から確認できます。以下の順にクリックし、「サーバーマネージャー」を起動します。「サーバーマネージャー」でのそれぞれの確認方法は対応する項目を確認してください。

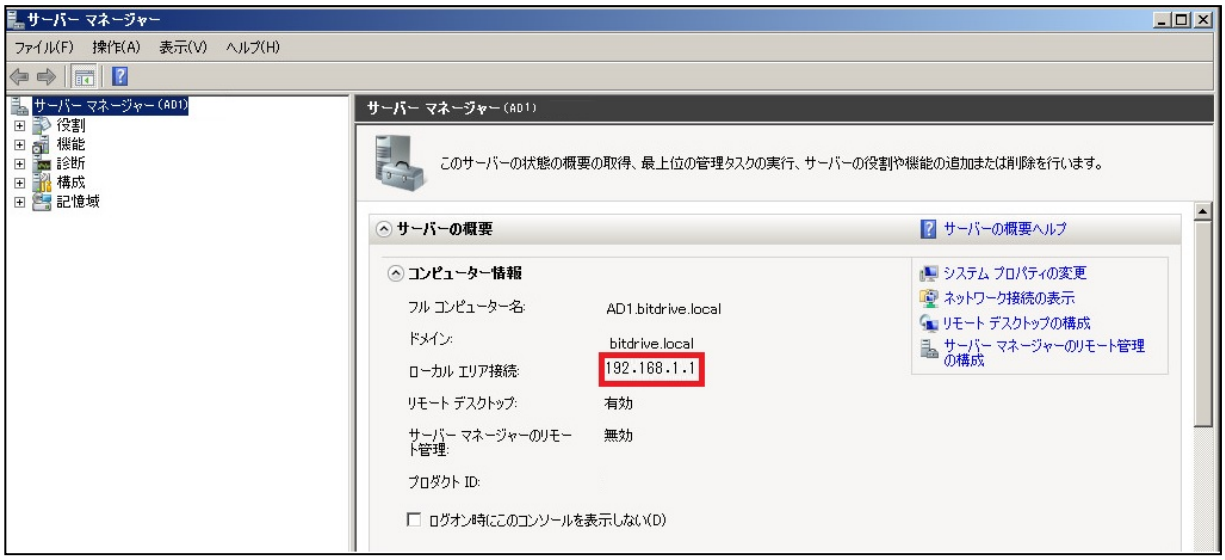
<ホスト名>
以下の赤枠の部分がホスト名です。

重要
- フルコンピュータ名のドメイン名より前の部分がホスト名です。



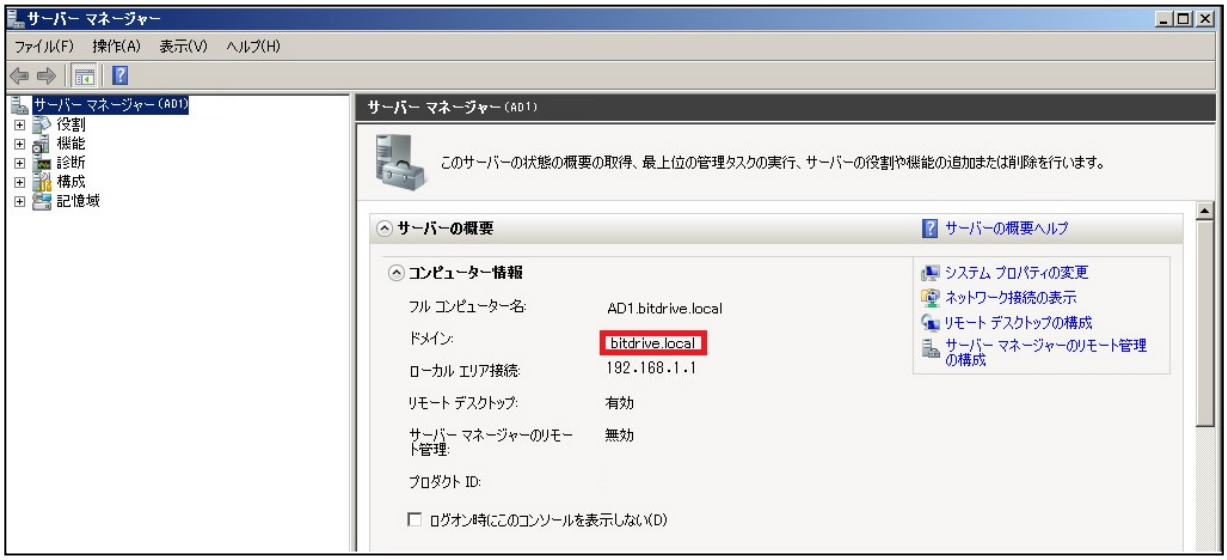
<IP アドレス>

以下の赤枠の部分が IP アドレスです。



<Active Directory ドメイン名>

以下の赤枠の部分が Active Directory ドメイン名です。



<NetBIOS ドメイン名>

NetBIOS ドメイン名は Active Directory のコマンドプロンプト上から確認できます。

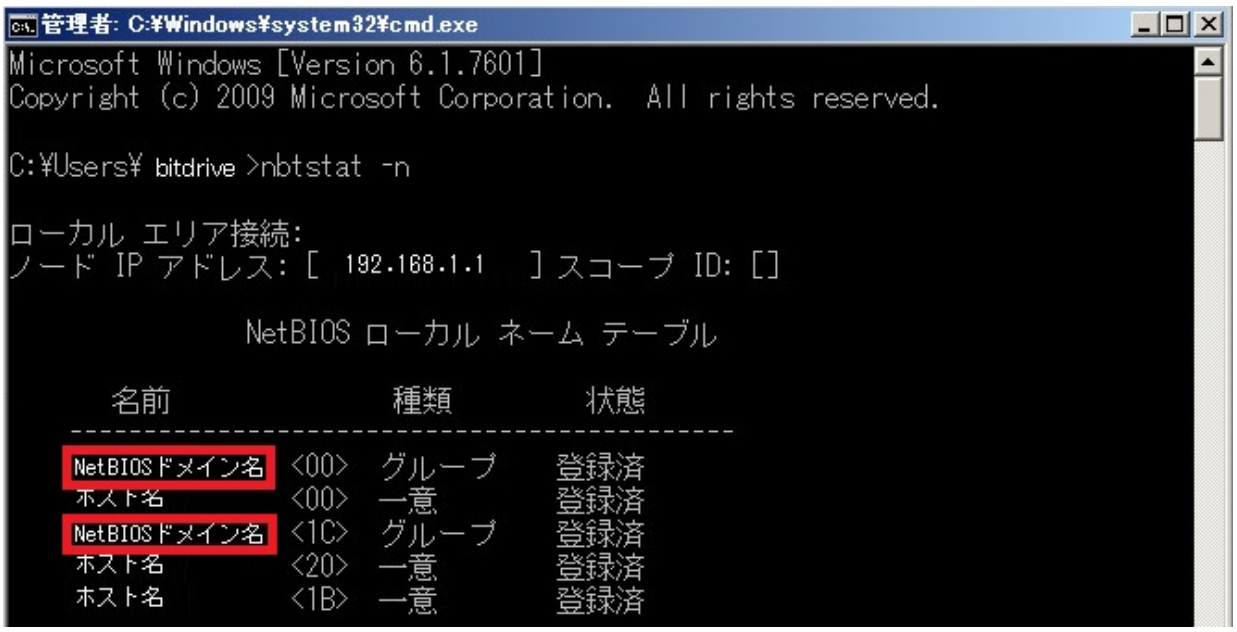
以下の順にクリックし、「コマンドプロンプト」を起動します。

「スタート」→「すべてのプログラム」→「アクセサリ」→「コマンドプロンプト」

「コマンドプロンプト」に、以下のコマンドを入力します。

“nbtstat -n”

以下の赤枠が NetBIOS ドメイン名です。



以上で、認証タイプの設定は終了です。

3. Microsoft Entra ID を選択した場合
Microsoft Entra ID を選択すると、Microsoft Entra ID 設定画面が表示されます。下記のように入力し、設定をクリックします。

重要

- Microsoft Entra ID の仕様により、管理者ユーザの認証には多要素認証が必要となります。
  しかし、セキュアリモートアクセスでは Microsoft Entra ID の多要素認証の機能に対応しておりません。
  そのため、管理者ユーザ名には多要素認証を設定されていないユーザ名にてご登録ください。

メモ

- Microsoft Entra ID 管理センターよりセキュアリモートアクセス用にアプリケーションの作成が必要です。
  作成手順に下記 URL より[Microsoft Entra ID ユーザガイド]をご参照ください。
  https://www.bit-drive.ne.jp/support/technical/azuread/
- 作成したアプリケーションからアプリケーション ID、アプリケーションパスワードなど必要情報をご確認ください。

※上記内容は設定例です。実際の設定内容はお客さま環境に併せて入力してください。

項目	入力値・内容
アプリケーション ID【必須】	Microsoft Entra ID の「アプリケーション登録」より確認したアプリケーション ID
アプリケーションパスワード【必須】	Microsoft Entra ID の「アプリケーション登録」より作成したアプリのクライアントシークレットキー
ドメイン名【必須】	Microsoft Entra ID で使用中のドメイン名
管理者ユーザ名【必須】	Microsoft Entra ID に登録しているアカウント ※@以降は不要です。 ※一般ユーザでも指定可能です。 ※多要素認証を有効にしている管理者ユーザ名は利用できません。
管理者パスワード【必須】	上記アカウントに紐づくパスワード
シークレット有効期限【必須】	Microsoft Entra ID の「アプリケーション登録」より作成したアプリのシークレット有効期限 ※有効期限を設定することで、6 ヶ月前より毎月メールで期限を通知することができます。

5-2 デバイス ID の自動登録

1. デバイス認証に使用する ID の種類と登録方法を確認します。

メモ
- セキュアリモートアクセスでは、デバイス認証を行うために使用する ID をデバイス ID と定義しています

下表の通り、端末によって使用可能なデバイス ID が異なります。
なお、自動登録は管理者によるマネージメントツールへのデバイス ID 登録作業を省略できる機能です。設定手順の詳細については、次ページをご参照ください。

端末	自動登録	手動登録
Windows	シリアル ID	シリアル ID or MAC アドレス (選択可)
ARM 版 Windows	シリアル ID	シリアル ID or MAC アドレス (選択可)
MacOS	シリアル ID	シリアル ID or MAC アドレス (選択可)
iOS	シリアル ID	シリアル ID
Android	端末固有の ID	端末固有の ID

メモ
- シリアル ID は端末機種によってはシリアル番号とも表記されます。
- Android 端末は、"Cisco AnyConnect"クライアントソフトウェアがクライアント端末固有の値を収集、これをデバイス ID として利用します。

2. シリアル ID を利用したデバイス認証を行う場合、初回接続時にデバイス ID の自動登録および、自動登録失敗時の通知を行うかプルダウンメニューから選択します。

① 「デバイス ID の自動登録」が『有効』の場合

> **重要**
> - MAC アドレスを利用したデバイス認証を行う場合、この機能は利用できません。管理者さまにて手動で登録を行ってください。

初回接続時にシリアル ID が自動で登録されます。

ただし、初回接続時はシリアル ID の登録を行う処理のみとなり、VPN は確立しません。

一旦切断し、再度接続すると VPN ネットワークアドレスが割り当てられ、VPN を確立します。

② 「デバイス ID の自動登録」が『無効』の場合

> **重要**
> - iOS をご利用の場合、「Cisco AnyConnect」では、UDID をシリアル ID として利用することができないため、デバイス ID の自動登録を「有効」にしてご利用ください。

予め手動でシリアル ID を登録するもしくは、初回接続時にシリアル ID の登録を許可してください。

シリアル ID の手動登録方法に関しては「7-1　デバイス追加」を、シリアル ID の登録を許可する方法に関しては、「10-3　デバイス ID の登録」をご確認ください。

③ 「自動登録失敗時の通知」が『有効』の場合

「デバイス ID の自動登録」が『有効』かつ「自動登録失敗時の通知」が『有効』の場合、5-3 で設定した通知メール宛先に、自動登録が失敗した旨メールで通知することが可能です。

以上で、デバイス ID の自動登録は終了です。

5-3　通知メール宛先

以下何れかの条件に合致した場合、指定したメールアドレスに通知メールが送信されます。

・「デバイス ID の自動登録」が「無効」かつシリアル ID を利用したデバイス認証を行う場合
シリアル ID 登録に関するメールが送信されます。

・「デバイス ID 自動登録」が『有効』かつ「自動登録失敗時」の通知が『有効』の場合
デバイス ID の自動登録失敗時にメールが送信されます。

> **重要**
> ● MAC アドレスを利用したデバイス認証を行う場合、この機能は利用できません。
> 管理者さまにて手動で登録を行ってください。

通知先として登録するメールアドレスを複数指定することもできます。

以上で、通知メール宛先設定は終了です。

5-4　DNS サーバ

セキュアリモートアクセス接続中に使用する DNS サーバを自動で設定させます。

補足　プライマリ、セカンダリ両方を設定できます。

赤枠内の点線部をクリックし、指定したい DNS サーバの IP アドレスを入力します。

補足　セキュアリモートアクセスを利用するクライアント端末のメーラがメールサーバを名前で指定している場合、メールサーバの名前を解決できる DNS サーバを設定してください。

※上記内容は設定例です。実際の設定内容はお客さま環境に併せて入力してください。

以上で、DNS サーバの設定は終了です。

5-5　VPN ネットワークアドレス

セキュアリモートアクセス利用中は、こちらに記載されているネットワークアドレスの範囲で IP アドレスがランダムで割り振られます。

補足　割り振られる IP アドレスは指定できません。

以上で、VPN ネットワークアドレスの設定は終了です。

6 ユーザ設定

ユーザに関する設定は「接続設定」タブの「ユーザ設定」画面から行います。

6-1 ユーザ作成

1. 「ユーザ追加」をクリックします。

2. サブ画面が表示されます。以下の方法でユーザの追加を行います。

① 「追加可能ユーザ」の中からユーザを個別に追加する場合

「追加可能ユーザ」の中から、追加するユーザを選択し、赤枠 [>] のをクリックします。

選択したユーザが「追加するユーザ」に移動します。

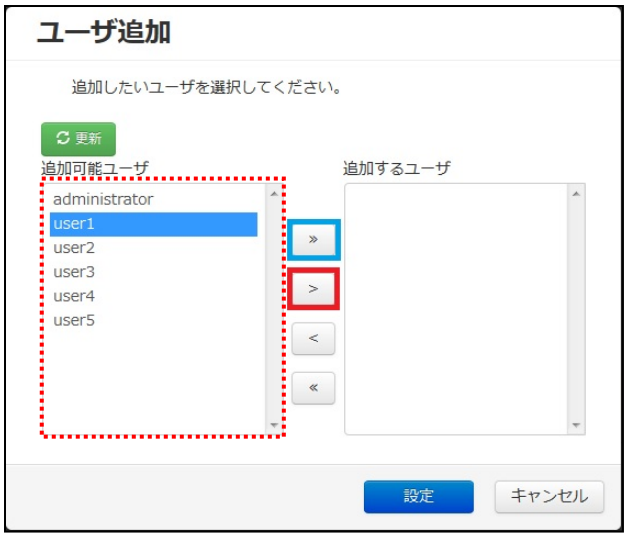
② 「追加可能ユーザ」の中からすべてのユーザを追加する場合

青枠の [»] をクリックします。

「追加可能ユーザ」の中のすべてのユーザが「追加するユーザ」に移動します。

- 「追加可能ユーザ」にユーザを追加する方法は以下になります。

A) 「全体設定」の「認証タイプ」を「Active Directory」もしくは「Microsoft Entra ID」に設定している場合、「5 全体設定」で指定した「Active Directory」もしくは「Microsoft Entra ID」サーバにて、ユーザ追加を行ってください。



3. 選択したユーザが「追加するユーザ」に移動した事を確認し、「設定」ボタンをクリックします。

4. 「ユーザを追加しました。」というメッセージが表示され、ユーザが新規追加されます。

以上で、ユーザ作成は終了です。

6-2 CSV によるユーザー括登録

CSV 形式のファイルから一括でユーザー登録を行なうことが可能です。
本作業では、新規ユーザーの一括登録手順を記載します。
補足 Microsoft Excel 2010 を利用した例を記載します。

重要
- CSV によるユーザー括登録を行ったユーザが「全体設定」の「認証タイプ」で指定した「Active Directory」もしくは「Microsoft Entra ID」に存在しない場合、そのユーザはセキュアリモートアクセスを利用できません。
「Active Directory」もしくは「Microsoft Entra ID」にユーザ追加を行ってください。
- 既に登録しているユーザー情報が CSV ファイルに含まれていた場合は、エラーとなり、インポートされません。

1. 以下のように CSV 形式のファイルを作成します。

一行目は必ず、以下の画像のように「ユーザ名」、「メールアドレス」、「接続許可」としてください。

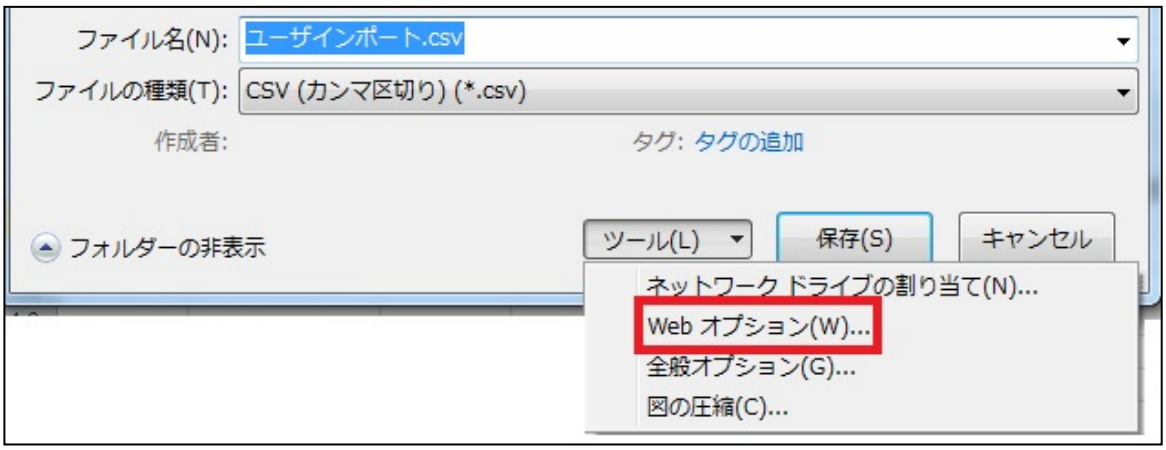
重要
- ユーザ名、接続許可に関しては入力必須項目です。

	A	B	C	D
1	ユーザ名	メールアドレス	接続許可	
2	user2		有効	
3	user3		有効	
4	user4		有効	
5	user5		有効	

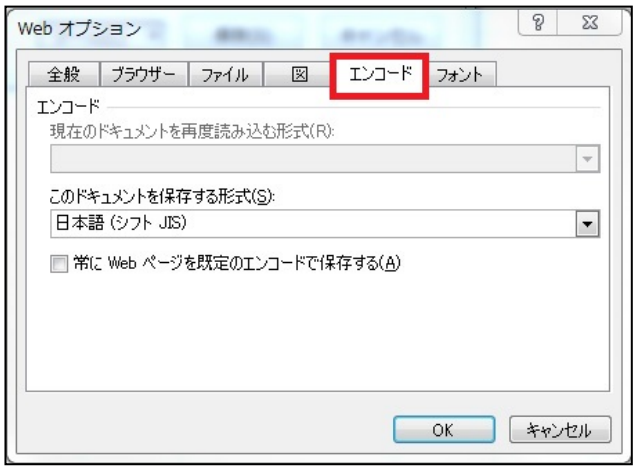
2. 記入後、「名前を付けて保存」を行います。

ファイル名を入力し、ファイルの種類を「CSV（カンマ区切り）（*.csv)」に設定し、文字コードを指定します。「ツール」をクリックします。

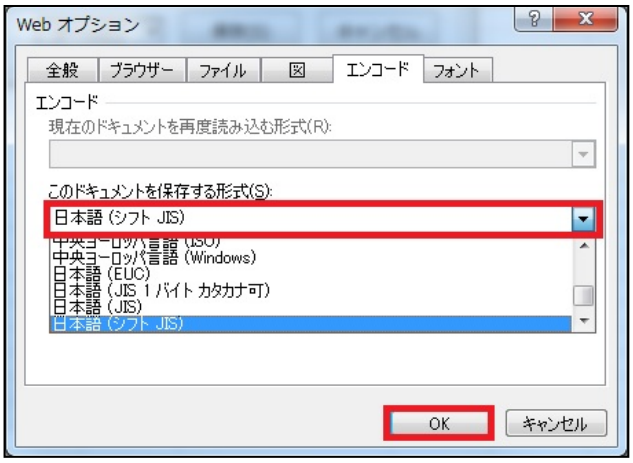
3. 「Web オプション（W）」をクリックします。



4. 「エンコード」タブをクリックします。



5. 赤枠をクリックすると、「ドキュメントを保存する形式」一覧が表示されますので、「Shift-JIS」もしくは、「UTF-8」を選択し、「OK」をクリックします。



6. 文字コードの設定後、「保存（S）」をクリックします。

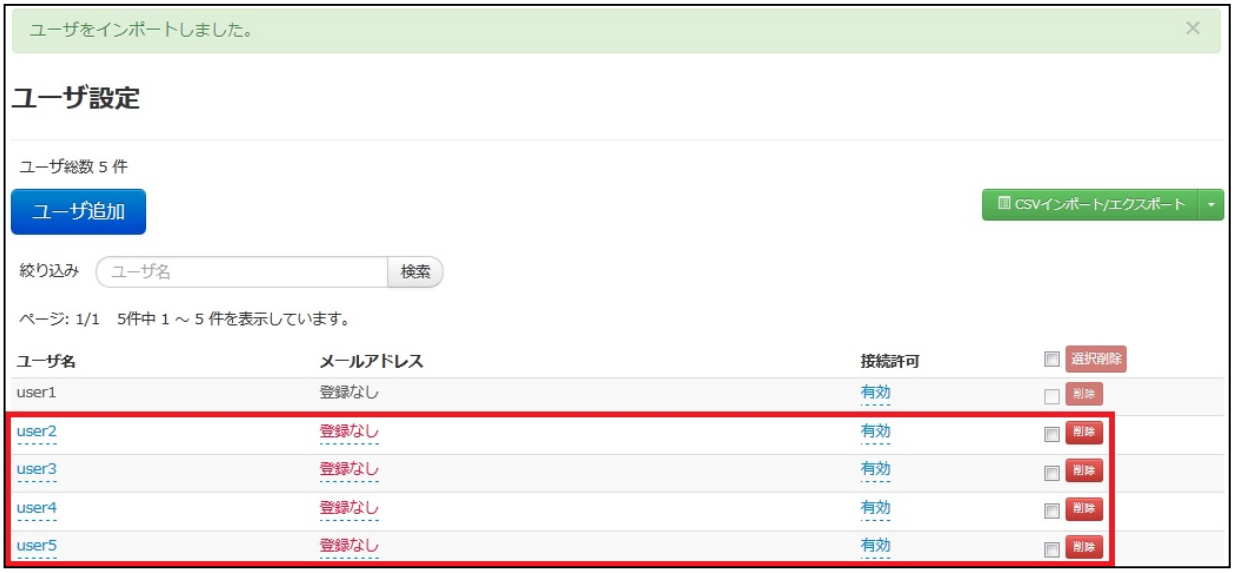
7. 「CSV インポート/エクスポート」の  をクリックします。

8. 「CSV インポート」をクリックします。

9. 「参照」をクリックし、インポートするファイルを選択します。

10. 「インポート」をクリックします。

11. 「ユーザをインポートしました。」というメッセージが表示され、赤枠のようにユーザが新規追加されます。



以上で、CSV によるユーザー一括登録は終了です。

6-3　ユーザ情報のエクスポート

1.　「CSV インポート/エクスポート」の  をクリックします。

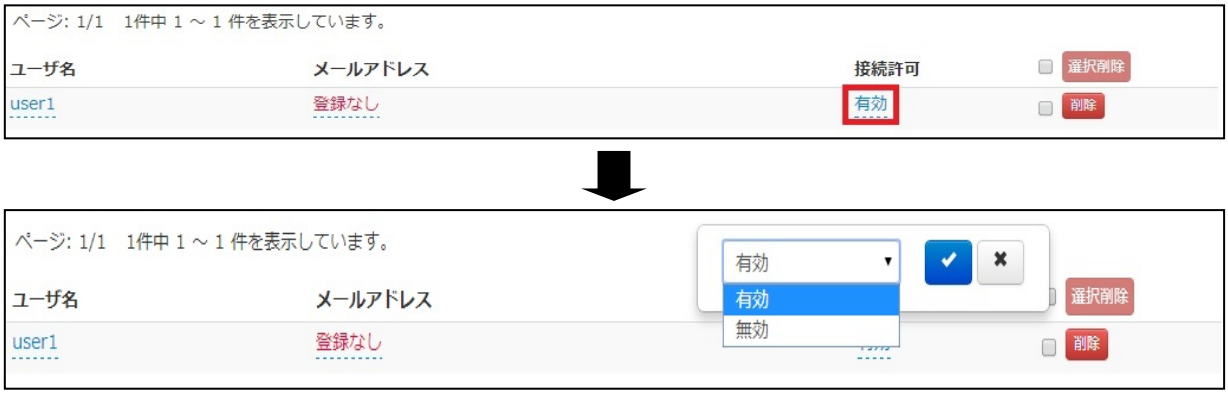
2.　「CSV エクスポート」をクリックすると、現在登録されているユーザ情報がダウンロードできます。

以上で、ユーザ情報のエクスポートは終了です。

6-4　ユーザ毎の接続許可

各ユーザに対して、セキュアリモートアクセスの接続許可の可否を設定できます。

1. 該当ユーザ行の「接続許可」欄をクリックして、プルダウンから指定します。



①　「接続許可」が『有効』の場合

該当のユーザはセキュアリモートアクセスを利用できます。

②　「接続許可」が『無効』の場合

該当のユーザはセキュアリモートアクセスを利用できません。

以上で、ユーザ毎の接続許可は終了です。

6-5　ユーザの削除

重要

- デバイスが割当たっているユーザは削除できません。
- 事前にデバイスの割当を解除してから、ユーザを削除してください。

1. 「ユーザ名」が青文字の場合、該当のユーザはデバイス割当が行われていない事を示します。「ユーザ名」が黒文字の場合、該当のユーザはデバイス割当がされている事を示します。

2. 該当ユーザがデバイス割当されていない事を確認し、赤枠の「削除」をクリックします。

メモ

- 削除の横にあるチェックボックスにチェックを入れ、青枠の「選択削除」をクリックすると、選択したユーザをまとめて削除できます。

3. 下記のポップアップが表示されますので、「OK」をクリックします。

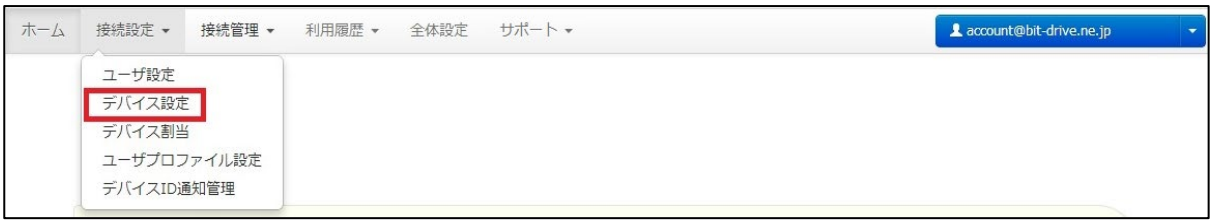
4. 「ユーザを削除しました。」というメッセージが表示され、削除対象のユーザが一覧より無くなります。

以上で、ユーザの削除は終了です。

7 デバイス設定

デバイスに関する設定は「接続設定」タブの「デバイス設定」画面から行います。

> **重要**
> - 設定したデバイスをユーザに割当てる作業に関しては、「デバイス設定」画面からではなく、「デバイス割当」の画面で行います。デバイス割当の方法に関しましては、「7-6 デバイス割当」をご確認ください。



7-1 デバイス追加

1. 「デバイス追加」ボタンをクリックします。

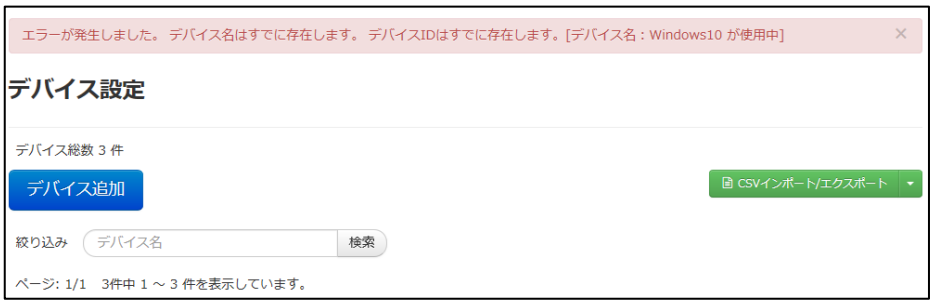
2. デバイス追加の画面が表示されますので、以下を参考に入力します。入力後、右下の設定ボタンをクリックします。

重要

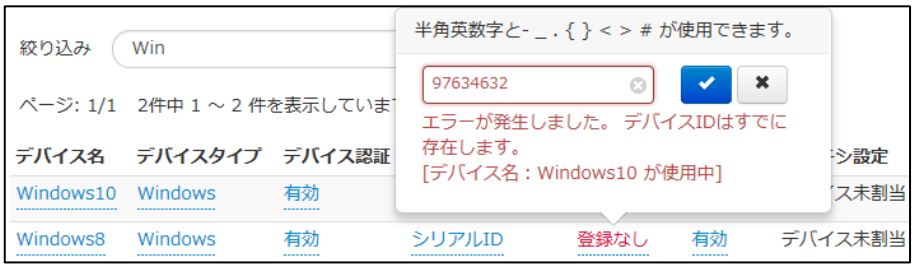
- デバイス ID の登録は文字列が長いため、自動登録を推奨します。自動登録では、初回接続時にデバイス ID が管理サーバに対して送信されます。
- 「全体設定」にてデバイスの自動登録が有効の場合は、デバイス ID の登録は必要ありません。無効の場合はデバイス ID の登録を行う必要があります。
- 「Cisco AnyConnect」では、UDID をシリアル ID として利用できないため、デバイス ID の自動登録を「有効」にしてご利用ください。
- 「デバイス認証」の「無効」設定は、固有のデバイス ID を持たないデバイス利用を想定しています。
  上記以外のデバイスによる「無効」設定もご利用可能ではありますが、よりセキュリティの高い「有効」設定を推奨しております。

項目	入力値・選択値・内容
デバイス名【必須】	任意の名称 （半角英数字と、「 - 」、「 _ 」、「 . 」(ドット)が利用可能です）
接続許可【必須】	プルダウンにて「有効」、「無効」より選択
デバイスタイプ【必須】	プルダウンにて、「Windows」、「Mac」、「iOS」、「Android」より選択
デバイス認証【必須】	プルダウンにて「有効」、「無効」より選択 ※デバイス認証では、デバイス固有のデバイス ID による認証の有無を設定することが可能です。 「無効」を選択された場合、デバイス ID による認証が行われなくなります。
デバイス認証方式【必須】	※デバイス認証を「有効」に選択している場合のみ表示されます デバイス認証方式を「シリアル ID」、「MAC アドレス」から選択 ※デフォルトの設定では、「シリアル ID」が選択されており、デバイス認証方式はセキュリティの強固な「シリアル ID」を推奨します。MAC アドレス認証は、「シリアル ID」の存在しない端末もしくは、特殊な端末でのみ使用することを推奨します ※デバイスタイプに「iOS」、「Android」が選択されている場合、「MAC アドレス」を選択することはできません。
シリアル ID	※デバイス認証方式を「シリアル ID」に選択している場合のみ表示されます 手動でシリアル ID を登録する際は下記の情報を入力してください。(「Windows」、「Mac」、「iOS」の場合はシリアルナンバー、「Android」の場合は"Cisco AnyConnect"クライアントソフトウェアのシステム情報にございます「デバイス ID」を入力してください) 尚、シリアル ID の手動確認方法は、ユーザガイドに掲載されている、各 OS の『【参考情報】シリアル ID の確認』項目を参照してください。
MAC アドレス	※デバイス認証方式を「MAC アドレス」に選択している場合のみ表示されます Windows/Mac の場合のみ指定可能です。 デバイス認証方式を「MAC アドレス」に選択している場合は、認証に使用するネットワークアダプタに登録されている「MAC アドレス」（12:34:56:78:90:ab 形式で入力してください） ※セキュアリモートアクセスを利用する際は、認証に使用する MAC アドレスが登録されているネットワークアダプタが有効になっている必要があります

3. 「デバイスを追加しました。」というメッセージが表示され、デバイスが追加されます。デバイス追加時にデバイス ID もしくは MAC アドレスがすでに他のデバイスで利用されている場合は、エラーが表示されます。



4. 点線がある項目は、クリックすることで変更できます。
デバイス ID もしくは MAC アドレスの変更時、すでに他のデバイスで利用されている場合は、エラーが表示されます。



以上で、デバイス追加は終了です。

7-2 デバイスインポート

CSV 形式のファイルから一括でデバイス追加を行なうことが可能です。
本作業では、新規デバイスの一括追加手順を記載します。
補足 Microsoft Excel 2010 を利用した例を記載します。

1. 以下のように CSV 形式のファイルを作成します。

一行目は必ず、以下の画像のように「デバイス名」、「デバイスタイプ」、「デバイス認証方法」、「デバイス ID」、「接続許可」、「デバイス認証」としてください。

重要
- 「デバイス名」、「デバイスタイプ」、「接続許可」、「デバイス認証」に関しては必須項目となります。

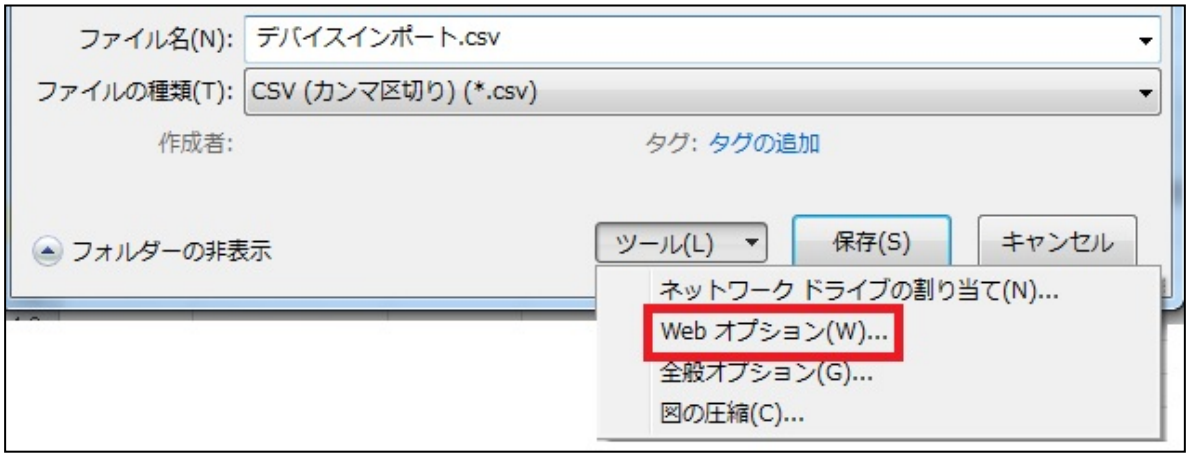
  ※デバイス認証を「有効」に設定される場合、「デバイス認証方法」の入力が必須となります。
- 既に登録しているデバイス情報が CSV ファイルに含まれていた場合は、エラーとなり、インポートされません。

	A	B	C	D	E	F
1	デバイス名	デバイスタイプ	デバイス認証方法	デバイスID	接続許可	デバイス認証
2	Windows10	Windows	シリアルID		有効	有効
3	Windows10_ARM	Windows			有効	無効

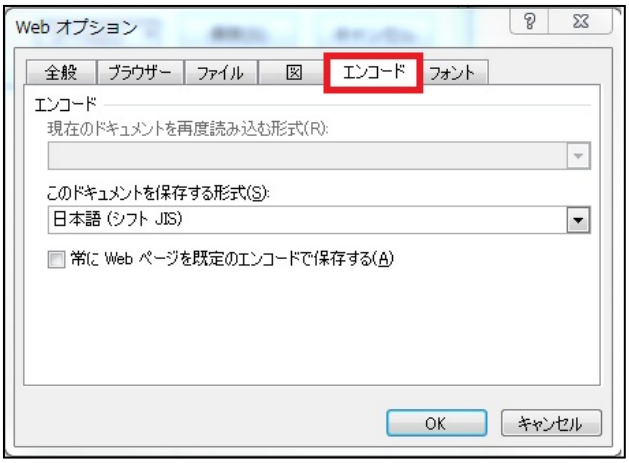
※上記内容は設定例です。実際の設定内容はお客さま環境に併せて入力してください。

2. 記入後、「名前を付けて保存」を行います。ファイル名を入力し、ファイルの種類を「CSV（カンマ区切り）（*.csv）」に設定した後、文字コードを指定します。「ツール」をクリックします。

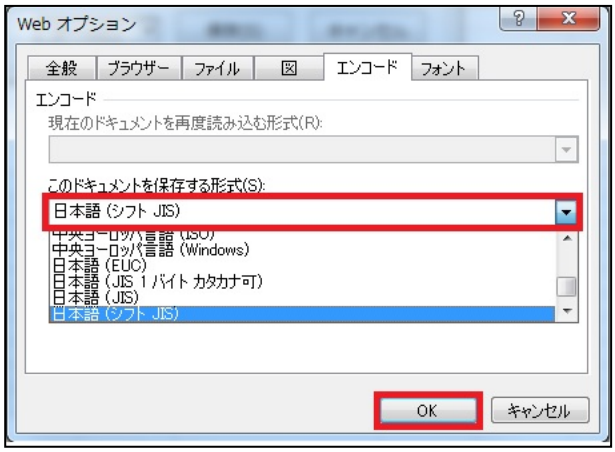
3. 「Web オプション」をクリックします。



4. 「エンコード」タブをクリックします。

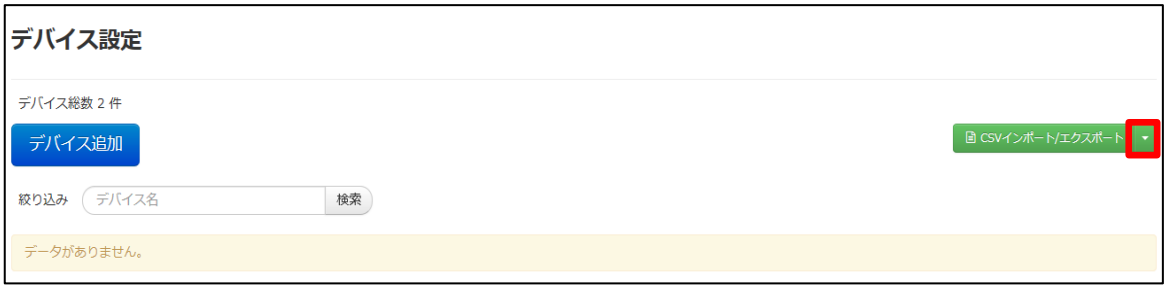


5. 赤枠をクリックすると、「ドキュメントを保存する形式」一覧が表示されますので、「Shift-JIS」もしくは、「UTF-8」を選択し、「OK」をクリックします。



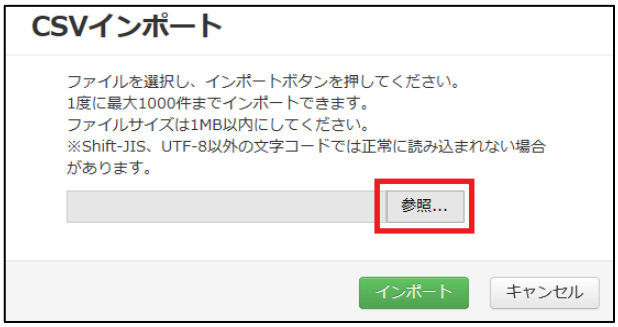
6. 文字コードの設定後、「保存（S）」をクリックします。

7. 「CSV インポート/エクスポート」の  をクリックします。



8. 「CSV インポート」をクリックします。

9. 「参照」をクリックし、インポートするファイルを選択します。



10. 「インポート」をクリックします。

11. 「デバイスをインポートしました。」というメッセージが表示され、赤枠のようにデバイスが新規追加されます。

以上で、デバイスインポートは終了です。

7-3　デバイスエクスポート

1.　「CSV インポート/エクスポート」の▼をクリックします。

2.　「CSV エクスポート」をクリックすると、現在登録されているデバイス情報がダウンロードできます。

以上で、ユーザエクスポートは終了です。

7-4　デバイス毎の接続許可

各デバイスに対して、セキュアリモートアクセスの使用許可の可否を設定できます。

1. 該当デバイス行の「接続許可」欄をクリックし、プルダウンから指定します。

①　「接続許可」が『有効』の場合

該当のデバイスはセキュアリモートアクセスを利用できます。

②　「接続許可」が『無効』の場合

該当のデバイスはセキュアリモートアクセスを利用できません。

以上で、デバイス毎の接続許可設定は終了です。

7-5　デバイスの削除

重要

- ユーザに割り当たっているデバイスは削除できません。
- 事前にデバイス割当を解除してから、デバイスの削除を行ってください。

「デバイス名」が青文字の場合、該当のデバイスはユーザへの割当が行われていない事を示します。

「デバイス名」が黒文字の場合、該当のデバイスはユーザへの割当が行われている事を示します。

デバイス名	デバイスタイプ	デバイス認証	デバイス認証方法	デバイスID	接続許可	プロキシ設定	ローカルセグメント設定	選択削除
Windows10	Windows	有効	シリアルID	97634632	有効	デバイス未割当	デバイス未割当	削除
Windows8	Windows	有効	シリアルID	登録なし	有効	デバイス未割当	デバイス未割当	削除

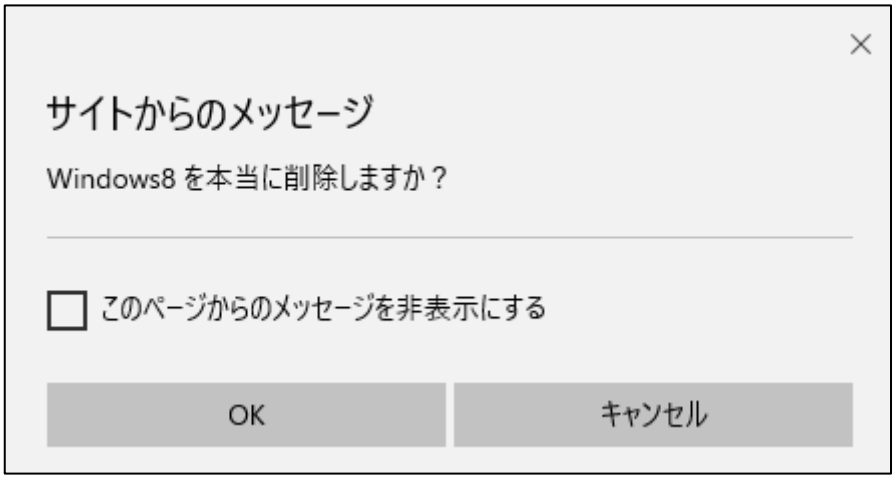
1. 該当デバイスがユーザに割当されていない事を確認し、右端にある赤枠の削除をクリックします。

メモ

- 削除の横にあるチェックボックスにチェックを入れ、青枠の「選択削除」をクリックすると、選択したデバイスをまとめて削除できます。

デバイス名	デバイスタイプ	デバイス認証	デバイス認証方法	デバイスID	接続許可	プロキシ設定	ローカルセグメント設定	選択削除
Windows10	Windows	有効	シリアルID	97634632	有効	デバイス未割当	デバイス未割当	削除
Windows8	Windows	有効	シリアルID	登録なし	有効	デバイス未割当	デバイス未割当	削除

2. 下記のポップアップが表示されますので、「OK」をクリックします。



3. 「デバイスを削除しました。」というメッセージが表示され、削除対象のデバイスが一覧より無くなります。

以上で、デバイスの削除は終了です。

7-6　デバイス割当

登録したデバイスをどのユーザに割り当てるか設定します。

1. ホーム画面上にて、「デバイス割当」タブをクリックします。「デバイス割当」画面が表示されます。

2. 「デバイス割当ユーザ」欄の右端の「割当」をクリックします。

3. サブ画面が表示されます。以下の方法でデバイスの割当をします。

① 「割当可能デバイス」の中から個別でデバイスを割当てる場合

「割当可能デバイス」の中から、割当するデバイスを選択し、赤枠の [>] をクリックします。

選択したデバイスが「割当デバイス」に移動します。

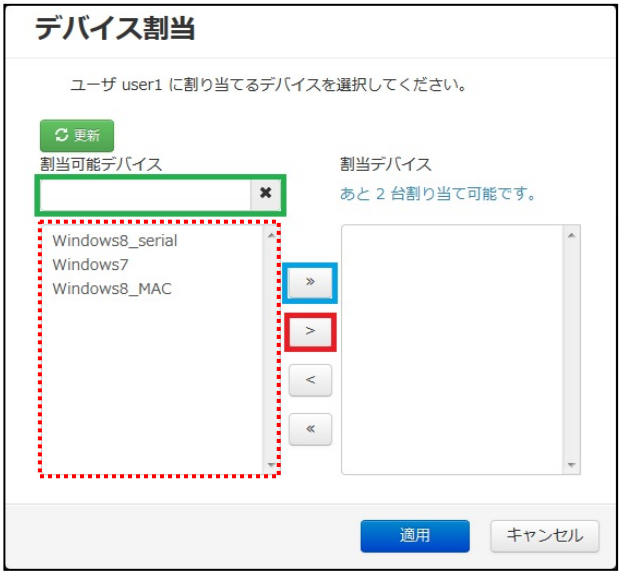
> **メモ**
> - 緑枠内に、デバイス名を入れると、絞り込みができます。

② 「割当可能デバイス」の中からすべてのデバイスを割当てる場合

青枠の [»] をクリックします。

「割当可能デバイス」の中のすべてのデバイスが「割当デバイス」に移動します。

> **重要**
> - 初期契約では 1 ユーザで 2 端末まで利用できます。
> - 1 ユーザで 3 端末以上利用する場合は、オプション契約にて利用可能端末数を追加してください。
> - オプション契約に関しては、NURO Biz インフォメーションデスクまでお問い合わせください。



4. 選択した割当可能デバイスが「割当デバイス」に移動した事を確認し、「適用」ボタンをクリックします。

5. 「ユーザ【ユーザ名】へのデバイス割当を変更しました。」というメッセージが表示され、デバイス割当対象としたユーザの「デバイス割当数」の値が増えます。

以上で、デバイス割当は終了です。

7-7　デバイス割当インポート

補足　Microsoft Excel 2010 を利用した例を記載します。

1. 以下のように CSV 形式のファイルを作成します。

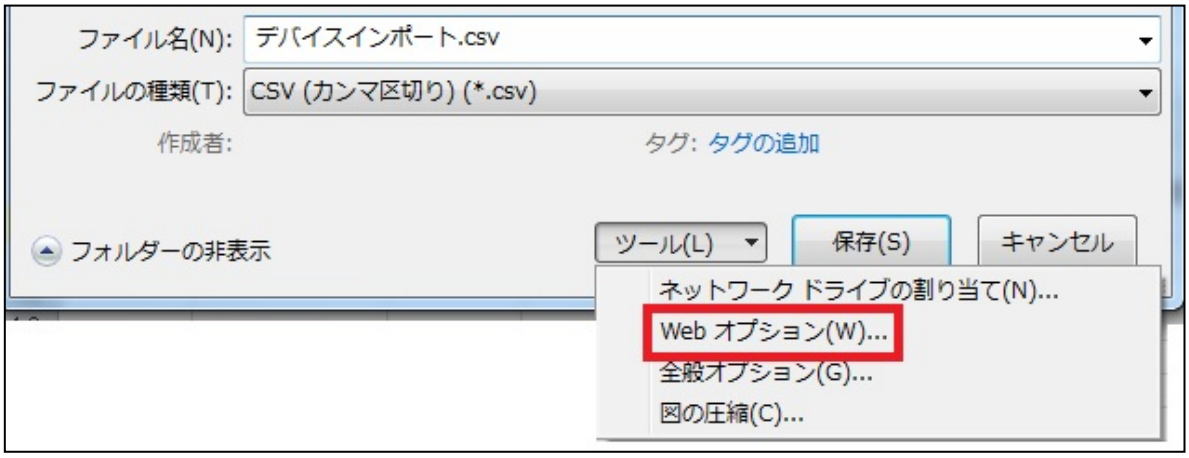
重要
- 一行目は必ず、以下の画像のように「ユーザ名」、「デバイス名」としてください
- 割り当てる「ユーザ名」、「デバイス名」は事前に登録しておく必要があります

	A	B
1	ユーザ名	デバイス名
2	user1	Windows7_serial
3	user2	Windows8_serial

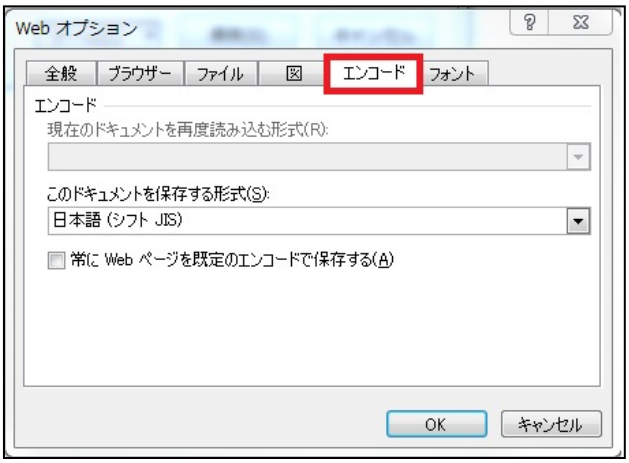
※上記内容は設定例です。実際の設定内容はお客さま環境に併せて入力してください。

2. 記入後、「名前を付けて保存」を行います。ファイル名を入力し、ファイルの種類を「CSV（カンマ区切り）（*.csv）」に設定した後、文字コードを指定します。「ツール」をクリックします。

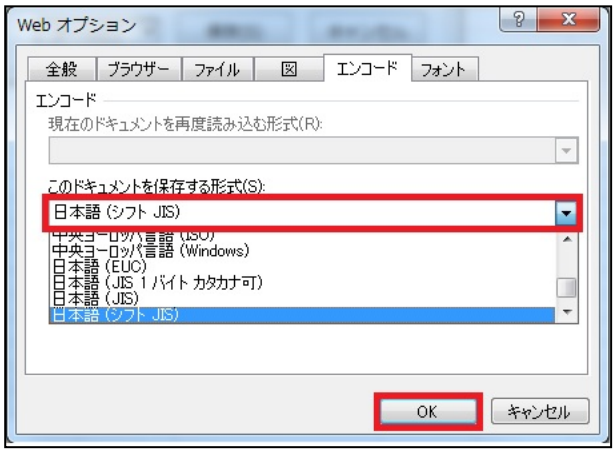
3. 「Web オプション」をクリックします。



4. 「エンコード」タブをクリックします。

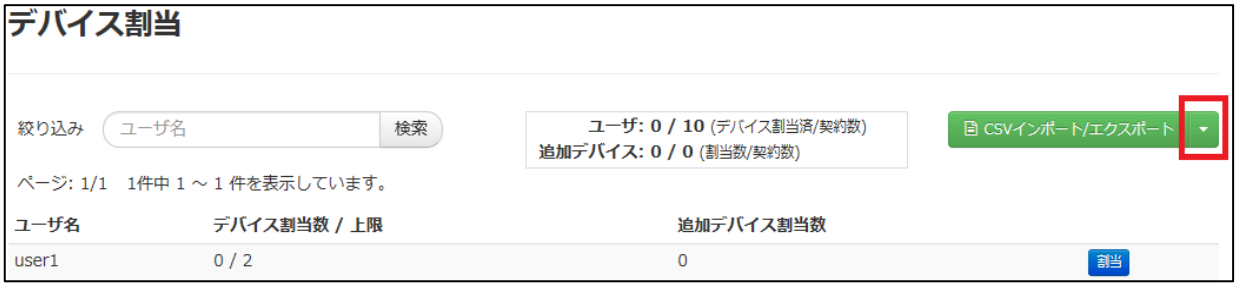


5. 赤枠をクリックすると、「ドキュメントを保存する形式」一覧が表示されますので、「Shift-JIS」もしくは、「UTF-8」を選択し、「OK」をクリックします。



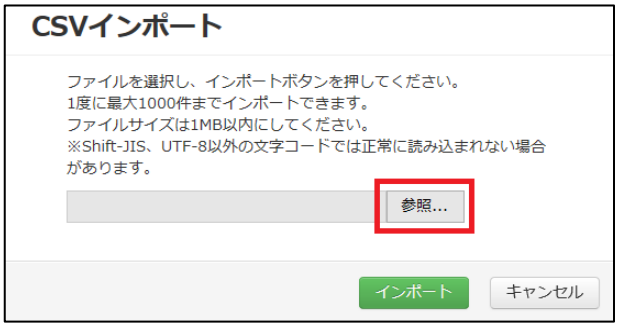
6. 文字コードの設定後、「保存（S）」をクリックします。

7. 「CSV インポート/エクスポート」の■をクリックします。



8. 「CSV インポート」をクリックします。

9. 「参照」をクリックし、インポートするファイルを選択します。



10. 「インポート」をクリックします。

11. 「ユーザプロファイルを割当てました。」というメッセージが表示され、赤枠のようにデバイスが割当されます。

以上で、デバイス割当インポートは終了です。

7-8　デバイス割当エクスポート

1. 「CSV インポート/エクスポート」の  をクリックします。

2. 「CSV エクスポート」をクリックすると、現在登録されているデバイス割当情報がダウンロードできます。

以上で、デバイス割当エクスポートは終了です。

7-9　デバイス割当解除

1.　「デバイス割当ユーザ」欄の右端の「割当」をクリックします。

2.　サブ画面が表示されます。以下の方法でデバイスの割当解除をします。

①　「割当デバイス」の中から個別でデバイス割当解除する場合

「割当デバイス」の中から、割当を解除するデバイスを選択し、赤枠　＜　のをクリックします。

選択したデバイスが「割当可能デバイス」に移動します。

②　「割当デバイス」の中からすべてのデバイスを割当解除する場合

青枠の　«　をクリックします。

「割当デバイス」の中のすべてのデバイスが「割当可能デバイス」に移動します。

3. 選択したデバイスが「割当可能デバイス」に戻った事を確認し、「適用」ボタンをクリックします。

4. 「ユーザ【ユーザ名】へのデバイス割当を変更しました。」というメッセージが表示され、デバイス割当対象としたユーザの「デバイス割当数」の値が減ります。

以上で、デバイス割当解除は終了です。

8 プロキシ設定

セキュアリモートアクセス利用時に使用するプロキシサーバの設定は、「接続管理」タブの「プロキシ設定」画面から行います。

8-1 プロキシ設定

1. 自動で設定させるプロキシを選択します。赤枠の  をクリックします。

> **重要**
> - セキュアリモートアクセス利用中にインターネットアクセスを行う場合は、インターネットアクセスが可能なプロキシサーバを自動で設定させるようにしてください。
> - スマートフォン端末(Android)については、仕様上「マネージメントツールで設定する」は利用できません。各 OS の詳細な動作については FAQ をご参照ください。

① クライアント設定を利用する

セキュアリモートアクセス利用時も、セキュアリモートアクセスクライアント端末に設定されているプロキシサーバを利用します。

② マネージメントツールで設定する

セキュアリモートアクセス利用時に使用するプロキシサーバの設定をします。

「マネージメントツールで設定する」をクリックするとサブ画面が表示されます。

項目	入力値・内容
アドレス【必須】	プロキシサーバの IPｖ4 アドレス
ポート【必須】	プロキシサーバのポート番号
プロキシ適用除外リスト	プロキシの適用を除外するリストを;（セミコロン）で区切る ※ *（アスタリスク）をワイルドカード文字として使用できます

上記を入力後、「設定」をクリックします。

※上記内容は設定例です。実際の設定内容はお客さま環境に併せて入力してください。

③ プロキシの利用を許可しない

セキュアリモートアクセス利用時にプロキシを利用させない設定です。

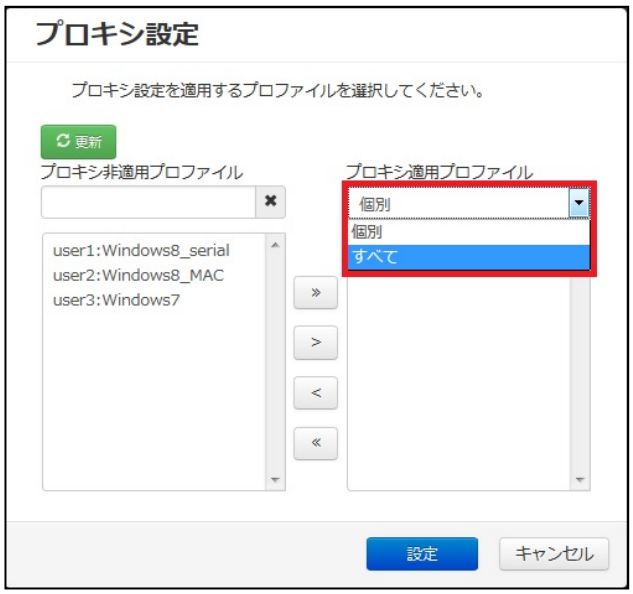
以上で、プロキシ設定は終了です。

8-2　プロキシの適用

1.　「一覧表示/変更」をクリックします。

2.　サブ画面が表示されます。プロキシ設定の適用をユーザプロファイル毎にするか、すべてのユーザプロファイルにするか選択します。「プロキシ適用プロファイル」の上段から、プルダウンメニューにて「個別」もしくは、「すべて」をクリックします。

項目	選択値・内容
個別	「プロキシ非適用プロファイル」から「プロキシ適用プロファイル」へ移動させたユーザプロファイルが対象となります **※　プロキシ設定後に作成されたユーザプロファイルは自動では対象となりません**
すべて	すべてのユーザプロファイルが対象となります **※　プロキシ設定後に作成されたユーザプロファイルも対象となります**



3. プロキシ設定の適用をユーザプロファイル毎（「プロキシ適用デバイス」の上段を「個別」）にしている場合は、以下の方法でユーザプロファイルに設定を適用します。

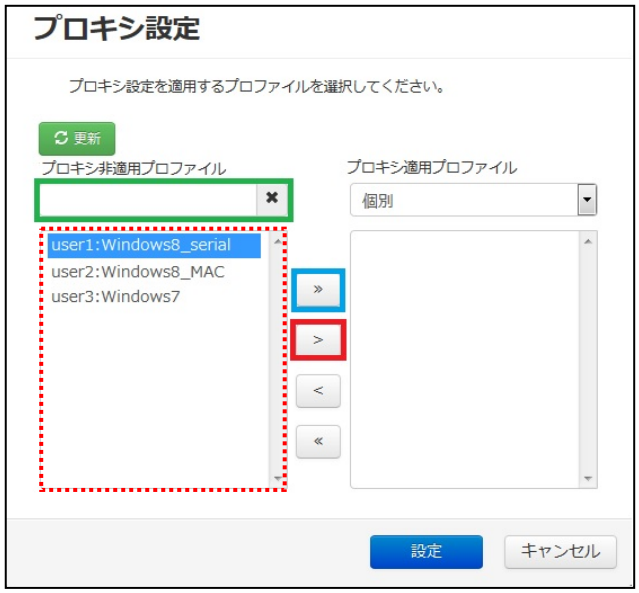
① 「プロキシ非適用プロファイル」中から個別でユーザプロファイル設定を適用させる場合

「プロキシ非適用プロファイル」の中から、追加するユーザプロファイルを選択し、赤枠の ＞ をクリックします。選択したユーザプロファイルが「プロキシ適用プロファイル」に移動します。

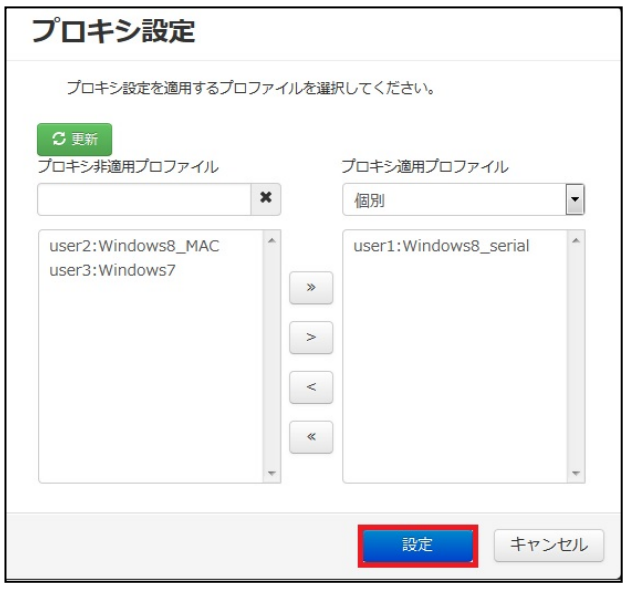
補足 緑枠内にユーザプロファイル ID を入れると、絞り込みができます。

② 「プロキシ非適用プロファイル」中からすべてのユーザプロファイル設定を適用させる場合

青枠の » をクリックします。「プロキシ非適用プロファイル」の中のすべてのユーザプロファイルが「プロキシ適用プロファイル」に移動します。



4. 選択したもしくは、すべてのユーザプロファイルが「プロキシ適用プロファイル」に移動した事を確認し、「設定」をクリックします。



5. 「プロキシ設定を変更しました。」というメッセージが表示されます。

以上で、プロキシ設定は終了です。

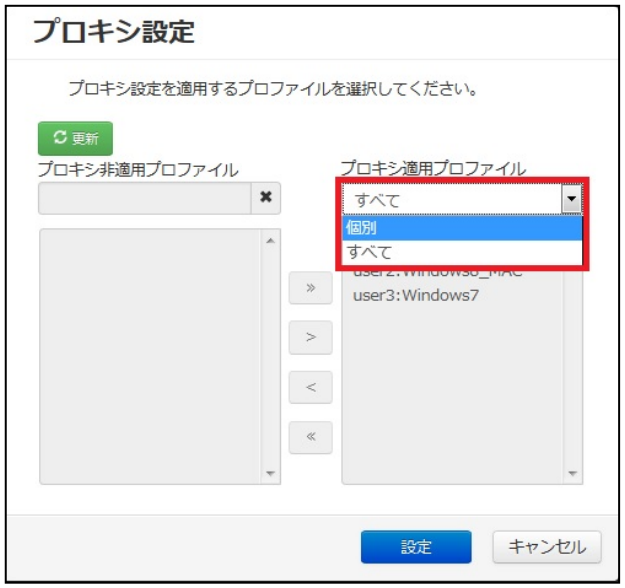
8-3 プロキシの適用解除

1. 「一覧表示/変更」をクリックします。

2. サブ画面が表示されます。

メモ

- 「プロキシ適用プロファイル」の上段の欄が「すべて」になっている場合は、プルダウンメニューにて「個別」をクリックし、設定をクリックするとすべてのユーザプロファイルが解除されます。



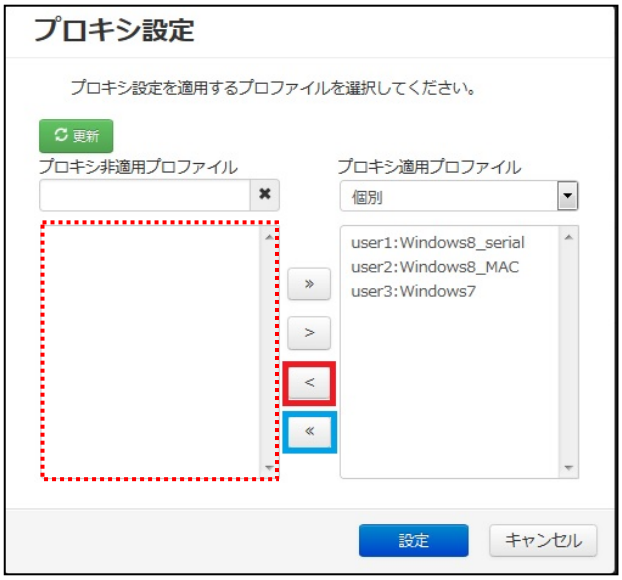
3. 以下の方法で、プロキシ設定の適用をユーザプロファイル毎で解除します。

① 「プロキシ適用プロファイル」中から個別でユーザプロファイル設定適用を解除させる場合

「プロキシ適用プロファイル」の中から、適用解除するユーザプロファイルを選択し、赤枠の [<] をクリックします。選択したユーザプロファイルが「プロキシ非適用プロファイル」に移動します。

② 「プロキシ適用プロファイル」中からすべてのユーザプロファイル設定適用解除させる場合

青枠の [«] をクリックします。「プロキシ適用プロファイル」の中のすべてのユーザプロファイルが「プロキシ非適用プロファイル」に移動します。



4. 選択したもしくは、すべてのユーザプロファイルが「プロキシ非適用プロファイル」に移動した事を確認し、「設定」をクリックします。

5. 「プロキシ設定を変更しました。」というメッセージが表示されます。

以上で、プロキシの適用解除は終了です。

9 ローカルセグメント設定

セキュアリモートアクセスでは、クライアント端末が接続されているセグメントをローカルセグメントと定義しており、本項目の設定を行うことにより、セキュアリモートアクセス利用中にローカルセグメントへのアクセスができるようになります。

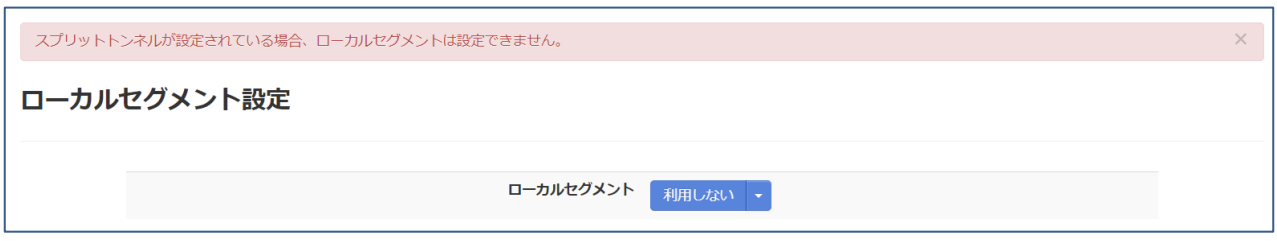
なお、「1-2　サービス構成」の青い点線がローカルセグメントアクセスを示しています。

ローカルセグメントに関する設定は、「接続管理」の「ローカルセグメント設定」画面から行います。

重要

- ローカルセグメントアクセスを行う場合、クライアントソフトェア側の設定も必要です。設定箇所についてはユーザガイドをご参照ください。
  ※クライアント側の設定はデフォルトで有効になっています。
- スプリットトンネル機能が有効になっていた場合、ローカルセグメントアクセスを利用することはできません。

※スプリットトンネル機能が有効であった場合、ローカルセグメントは設定できない旨の注意が表示されます。



9-1 ローカルセグメント設定

1. 赤枠の  をクリックします。ローカルセグメント利用を許可する場合は、「利用する」を選択します。

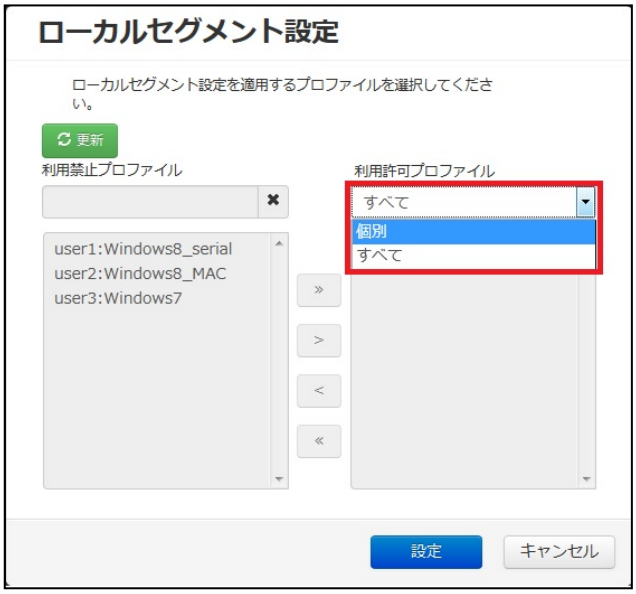
以上で、ローカルセグメント設定は終了です。

9-2 ローカルセグメントの適用

1. 「一覧表示/変更」をクリックします。

2. サブ画面が表示されます。ローカルセグメント設定の適用をユーザプロファイル毎にするか、すべてのユーザプロファイルにするか選択します。「利用許可プロファイル」の上段の欄から、プルダウンメニューにて「個別」もしくは、「すべて」をクリックします。

項目	選択値・内容
個別	「利用禁止プロファイル」から「利用許可プロファイル」へ移動させたユーザプロファイルが対象となります **※ ローカルセグメント設定後に作成されたユーザプロファイルは自動では対象となりません**
すべて	すべてのユーザプロファイルが対象となります **※ ローカルセグメント設定後に作成されたユーザプロファイルも対象となります**



3. ローカルセグメント設定の適用をユーザプロファイル毎（「プロキシ適用デバイス」の上段を「個別」）にしている場合は、以下の方法でユーザプロファイルを適用します。

① 「利用禁止プロファイル」の中から個別でユーザプロファイルに設定を適用させる場合

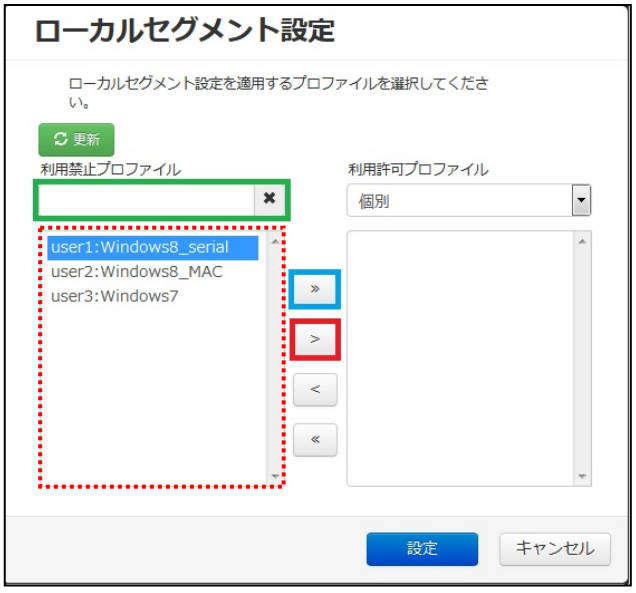
「利用禁止プロファイル」の中から、追加するユーザプロファイルを選択し、赤枠 [>] のをクリックします。

選択したユーザプロファイルが「利用許可プロファイル」に移動します。

補足 緑枠内にユーザプロファイル ID を入れると、絞り込みができます。

② 「利用禁止プロファイル」の中からすべてのユーザプロファイルに設定を適用させる場合

青枠の [»] をクリックします。「利用禁止プロファイル」の中のすべてのユーザプロファイルが「利用許可プロファイル」に移動します。



4. 選択したもしくは、すべてのユーザプロファイルが「利用許可プロファイル」に移動した事を確認し、「設定」をクリックします。

5. 「ローカルセグメント設定を変更しました。」というメッセージが表示されます。

以上で、ローカルセグメントの適用は終了です。

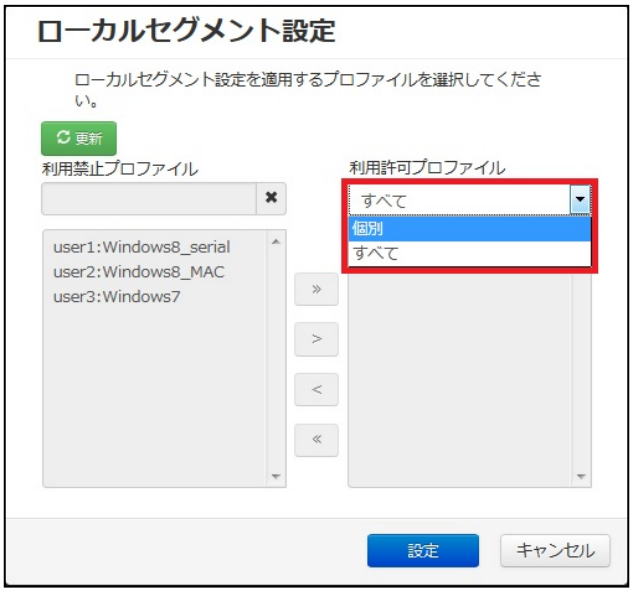
9-3 ローカルセグメントの適用解除

1. 「一覧表示/変更」をクリックします。

2. サブ画面が表示されます。

メモ

- 「利用禁止プロファイル」の上段の欄が「すべて」になっている場合は、プルダウンメニューにて「個別」をクリックし、設定をクリックするとすべてのユーザプロファイルが解除されます。



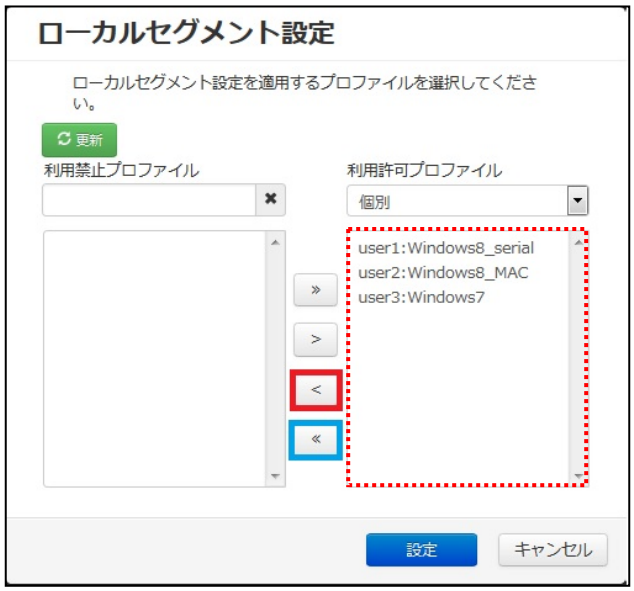
3. 以下の方法で、ローカルセグメント設定の適用をユーザプロファイル毎で解除します。

① 「利用許可プロファイル」の中から個別でユーザプロファイルの設定を適用解除させる場合

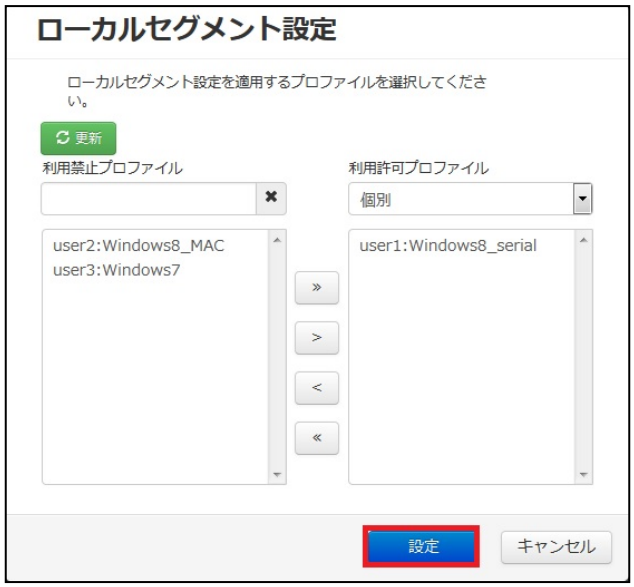
「利用許可プロファイル」の中から、適用解除するユーザプロファイルを選択し、赤枠の < をクリックします。選択したユーザプロファイルが「利用禁止プロファイル」に移動します。

② 「利用許可プロファイル」の中からすべてのユーザプロファイル設定を適用解除させる場合

青枠の « をクリックします。「利用許可プロファイル」の中のすべてのユーザプロファイルが「利用禁止プロファイル」に移動します。



4. 選択したユーザプロファイルが「利用禁止プロファイル」に移動した事を確認し、「設定」をクリックします。



5. 「ローカルセグメント設定を変更しました。」というメッセージが表示されます。

以上で、ローカルセグメントの適用解除は終了です。

10　ユーザプロファイル設定

接続許可されているユーザへのプロファイル送付は「接続設定」タブの「ユーザプロファイル設定」画面から行います。

10-1 ユーザプロファイル個別送信

1. ユーザプロファイルを個別に送信する場合は、通知対象ユーザの選択送信欄にある「送信」をクリックします。

2. 下記の画面が表示されますので、ユーザプロファイルダウンロード通知を送信するメールの宛先、件名、URL 有効期限、ダウンロード回数を入力します。
入力後、「送信する」をクリックします。

重要

- プロファイルを送信するメールアドレスとメールの件名は任意のものに変更することができます。
- ユーザプロファイルのダウンロード URL の有効期限は『1～30 日』の間で設定できます。
- ダウンロード回数は『1～5、無制限』の内から設定できます。

※個別送信時の受信メールの一例

3. ユーザプロファイルダウンロード通知が送信されると、ステータスが「プロファイル DL 待ち」に変わります。2 回目以降の送信では、ステータスが「プロファイル DL 待ち[再送信フロー]」に変わります。

以上で、ユーザプロファイル送信は終了です。

10-2 ユーザプロファイル一括送信

1. 複数のユーザプロファイルをまとめて送信する場合は、送信したいプロファイルの選択送信欄のチェックボックスをチェックし、「選択送信」ボタンをクリックします。

2. 下記の画面が表示されますので、ユーザプロファイルダウンロード通知を送信するメールの宛先、件名、URL 有効期限を入力します。入力後、「送信する」をクリックします。

重要

- プロファイルを送信するメールアドレスとメールの件名は任意のものに変更することができます。
- ユーザプロファイルのダウンロード URL の有効期限は『1～30 日』の間で設定できます。
- ダウンロード回数は『1～5、無制限』の内から設定できます。

※一括送信時の受信メールの一例

【セキュアリモートアクセス】ユーザプロファイル登録のご案内

以下のURLにアクセスし、ユーザプロファイルをダウンロード後、インストールしてください。

■ユーザプロファイルID：user-0013:device-0013

https://stg.ravpn.bit-drive.ne.jp/download/user_profiles/yoqqedkUSbrnYqBLkku58ZgLEkIiO3TI9cKQMHl2G3po

■ユーザプロファイルID：user-0014:device-0014

https://stg.ravpn.bit-drive.ne.jp/download/user_profiles/bLEcxg5ZdvS2QOKTqMns7mwEFDppCqSdbUjXmDigpfMI

■ユーザプロファイルID：user-0015:device-0015

https://stg.ravpn.bit-drive.ne.jp/download/user_profiles/nHk7OYiZXzQj1sIKx6WyEG5D8eQes6fQKYNYMFTW2kuB

URLの有効期限：2021/12/08 15:33:01

ダウンロード回数：1回

※本メールに心当たりのない方は管理者にご連絡ください。

3. ユーザプロファイルダウンロード通知が送信されると、ステータスが「プロファイル DL 待ち」に変わります。2 回目以降の送信では、ステータスが「プロファイル DL 待ち[再送信フロー]」に変わります。

ユーザプロファイル設定

「デバイス割当」でユーザに割り当てが行われたデバイス単位で
ユーザプロファイルとして表示されます。

ユーザプロファイル総数 4000 件

絞り込み　ユーザ名/デバイス名　検索

ページ: 2/334　4000件中 13 ～ 24 件を表示しています。

ユーザプロファイルID	ステータス	接続許可		
user-0013:device-0013	プロファイルDL待ち [再送信フロー]	有効	再送信	削除
user-0014:device-0014	プロファイルDL待ち	有効	再送信	削除
user-0015:device-0015	プロファイルDL待ち	有効	再送信	削除

以上で、ユーザプロファイル送信は終了です。

10-3 デバイス ID の登録

重要

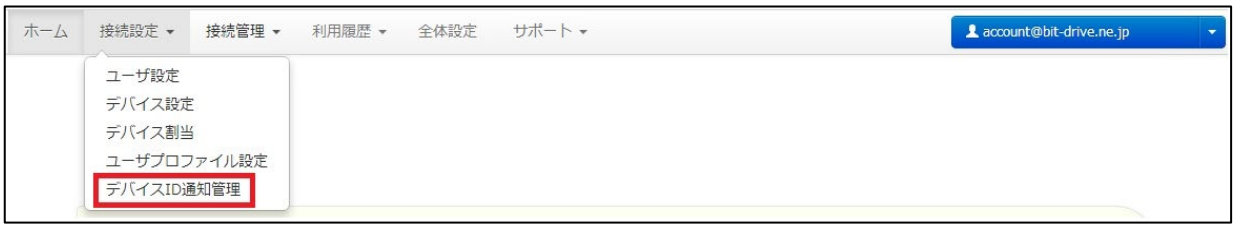
- 全体設定にて「デバイス ID の自動登録」を「有効」にしているもしくは、デバイス追加の際にデバイス ID を事前に手動登録している場合は、本作業を行う必要はありません。
- 認証方法を MAC アドレスにしている場合、本機能は利用できません。

1. ユーザプロファイルダウンロード通知からユーザプロファイルのダウンロードが行われると、該当のユーザのステータスが「デバイス ID 設定を行ってください。」になります。

重要

- 設定した URL 有効期限を経過してもユーザプロファイルのダウンロードが行われていない場合、ステータスが「URL の期限が切れました。再度メール送信してください。」という表記になります。再度ユーザプロファイルの送信を行ってください。

2. デバイス ID の登録は「接続設定」タブの「デバイス ID 通知管理」画面から行います。

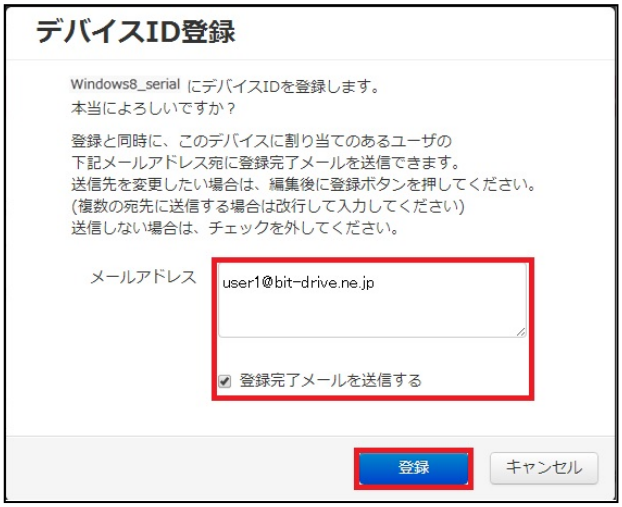


3. セキュアリモートアクセスクライアント端末にて、ユーザプロファイルのインストールが完了し、VPN 接続を行うと、以下のように表示されます。内容を確認し、「登録」をクリックします。内容に問題がある場合は「登録拒否」をクリックします。

> **重要** ● デバイス ID 登録を行うまでは、VPN 接続を確立させることはできません。

補足 チェックボックスにチェックをいれ、青枠の「一括管理」をクリックすると、一括登録もしくは、一括登録拒否ができます。

4. 下記の画面が表示されます。利用者さまに完了通知メールを送る際は、「登録完了メールを送信する」にチェックを入れ、メールアドレスを入力し、「登録」をクリックします。



5. メールアドレスを入力した場合、以下の内容のメールが送信されます。

> **重要** ● チェックボックスを外すと上記のメールは送信されません。

管理者によりご使用のデバイスのIDが正式に登録されました。

ただ今から セキュアリモートアクセス が通常利用いただけます。

6. デバイス設定画面の「デバイス ID」欄に「デバイス ID」が登録されます。

以上で、デバイス ID の登録は終了です。

10-4 ユーザプロファイル毎の接続許可

各ユーザプロファイルに対して、セキュアリモートアクセスの使用許可の可否を設定できます。

1. 該当プロファイル行の「接続許可」欄をクリックして、プルダウンメニューから指定します。

① 「接続許可」が有効の場合

該当のユーザプロファイルは、セキュアリモートアクセスを利用できます。

② 「接続許可」が無効の場合

該当のユーザプロファイルは、セキュアリモートアクセスを利用できません。

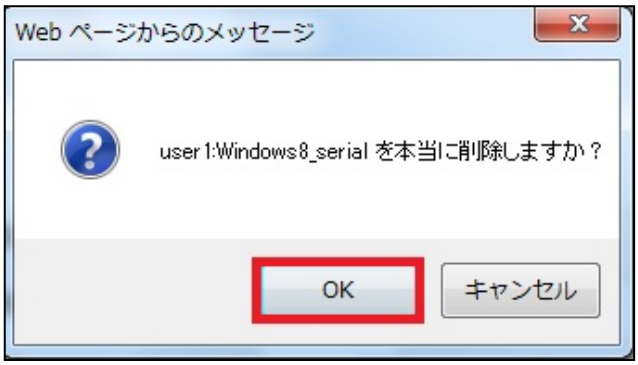
以上で、ユーザプロファイル毎の接続許可は終了です。

10-5 ユーザプロファイル削除

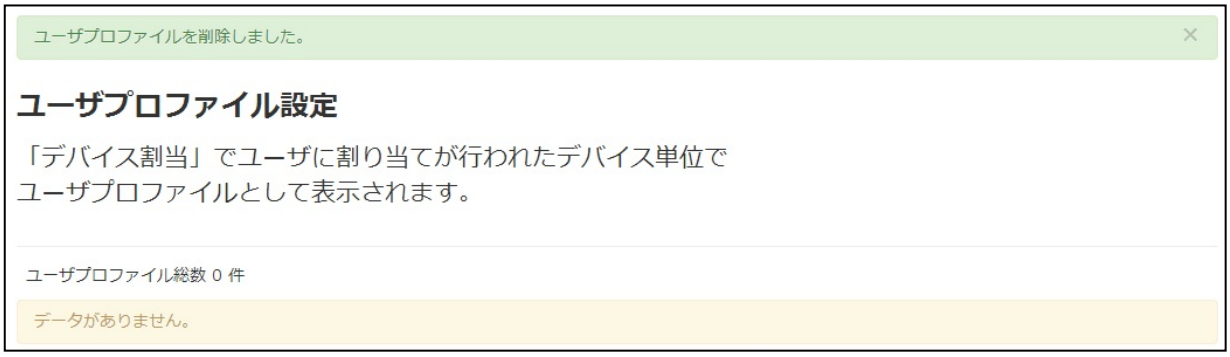
1. 該当ユーザプロファイル行の「削除」をクリックしてください。

> メモ
> - 削除の横にあるチェックボックスにチェックを入れた状態で青枠の「選択削除」をクリックすると、選択したユーザプロファイルをまとめて削除できます。

2. 以下のポップアップが表示されますので、「OK」ボタンをクリックします。



3. 「ユーザプロファイルを削除しました。」というメッセージが表示され、削除対象のユーザプロファイルが一覧より削除されます。



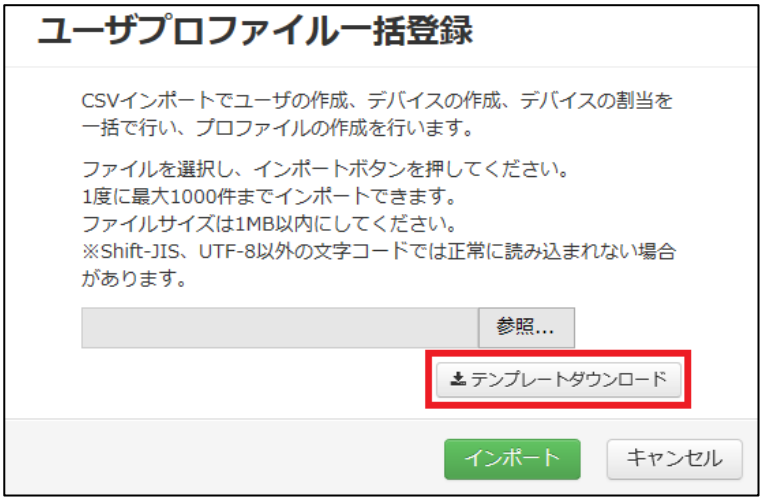
以上で、ユーザプロファイル削除は終了です。

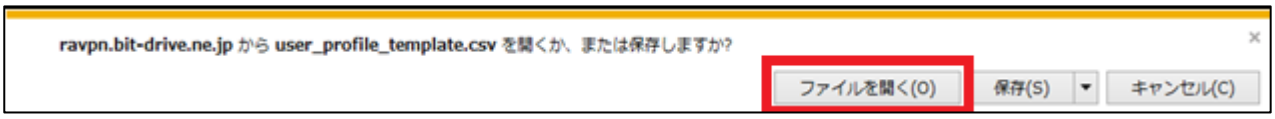
10-6 ユーザプロファイル一括登録手順

CSV インポートにて、ユーザ設定、デバイス設定、デバイス割当、ユーザプロファイル送信を一括して実施することができます。

1. ユーザプロファイル一括登録は「接続設定」タブの「ユーザプロファイル設定」画面から行います。

2. テンプレートダウンロードよりテンプレートをダウンロードし、インポートに使用するデータを作成します。





3. ダウンロードしたテンプレートを基に以下のように CSV 形式のファイルを作成します。

補足 Microsoft Excel 2010 を利用した例を記載します。

重要 一行目は必ず、以下の画像のように項目名が必須です。

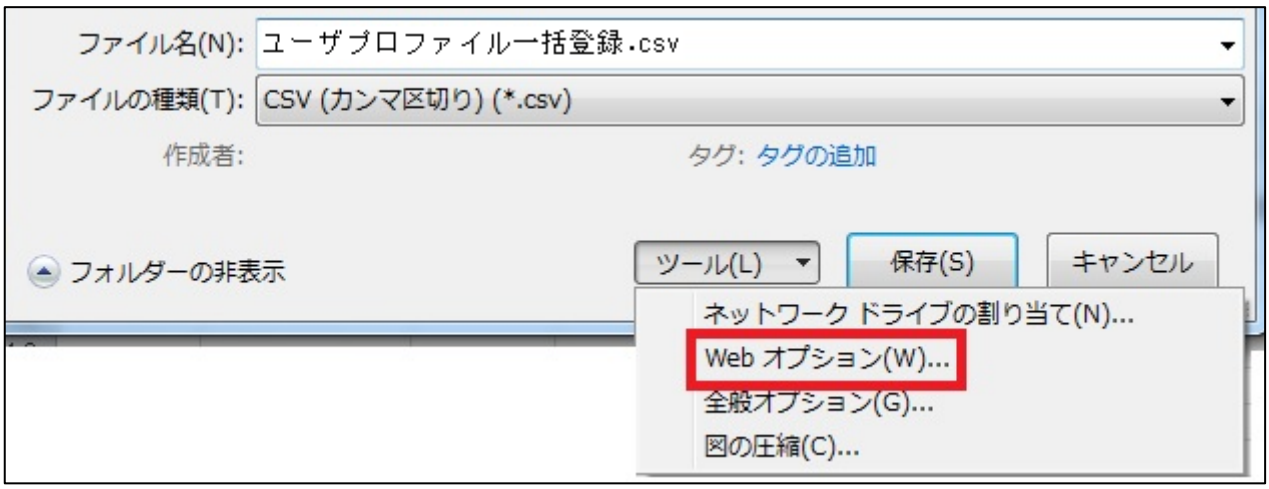
- デバイスタイプは「Windows、Mac、iOS、Android」から選択してください。
- デバイス認証方法は PC 端末の場合「シリアル ID、MAC アドレス」から、モバイル端末は「シリアル ID」のみ選択できます。
- メールアドレス、デバイス ID のみ任意項目になります。
- ユーザ、デバイスともに新規登録するため、重複する組み合わせの場合、登録エラーになります。

	A	B	C	D	E	F
1	ユーザ名	メールアドレス	デバイス名	デバイスタイプ	デバイス認証方法	デバイスID
2	user4		Windows10_serial	Windows	シリアルID	
3	user5		Windows10_serial2	Windows	シリアルID	
4	user6		Windows10_MAC	Windows	MACアドレス	

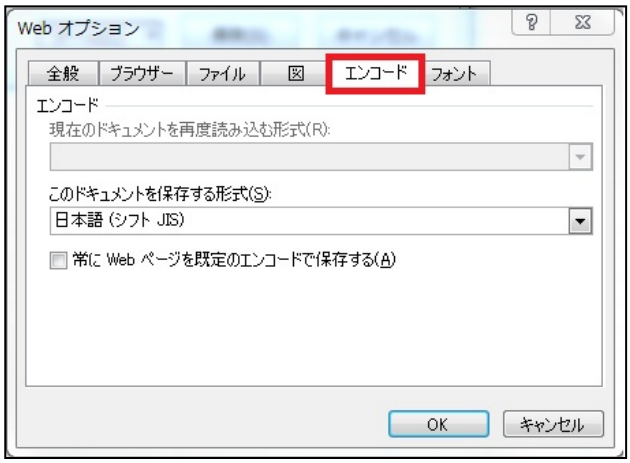
※上記内容は設定例です。実際の設定内容はお客さま環境に併せて入力してください。

4. 記入後、「名前を付けて保存」を行います。ファイル名を入力し、ファイルの種類を「CSV（カンマ区切り）（*.csv）」に設定した後、文字コードを指定します。「ツール」をクリックします。

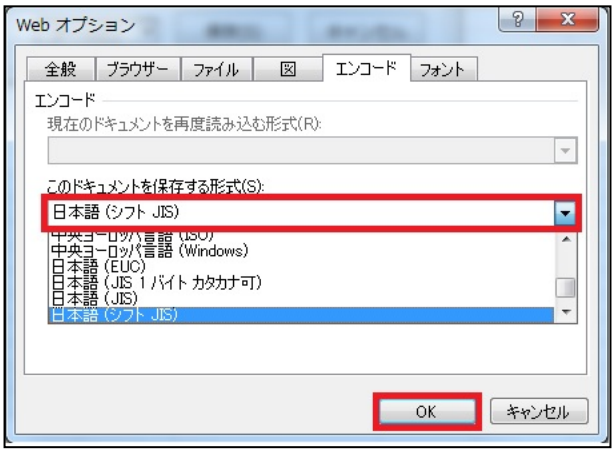
5. 「Web オプション」をクリックします。



6. 「エンコード」タブをクリックします。



7. 赤枠をクリックすると、「ドキュメントを保存する形式」一覧が表示されますので、「Shift-JIS」もしくは、「UTF-8」を選択し、「OK」をクリックします。



8. 文字コードの設定後、「保存（S）」をクリックします。

9. ユーザプロファイル一括登録画面にて、作成した csv ファイルを参照し、インポートボタンをクリックします。

10. 表示された内容に問題がなければ CSV インポートをクリックし、ユーザプロファイルの送信方法を選択します。

重要

エラーが発生した場合は、以下項目に誤りがないか確認してください。

- デバイスタイプは「Windows、Mac、iOS、Android」から選択してください。
- デバイス認証方法は PC 端末の場合「シリアル ID、MAC アドレス」から、モバイル端末は「シリアル ID」のみ選択できます。
- メールアドレス、デバイス ID のみ任意項目になります。
- ユーザ、デバイスともに新規登録するため、重複する組み合わせの場合、登録エラーになります。また、複数のプロファイルのメールアドレスに同じメールアドレスが指定されている場合もエラーとなります。

【ユーザプロファイルを送信しない】

本画面ではプロファイルを送信しません。別途 10-1 もしくは 10-2 を参照してプロファイルを送信してください。

【各プロファイルに設定された Email 宛にプロファイルを送信する】

※csv ファイルにアドレスが指定されている場合

各アドレスに個別にユーザプロファイルに送信します。

※csv ファイルにメールアドレスが指定されていない場合

メールアドレスが未設定の場合は、本画面で指定したアドレスに全てのユーザプロファイルが 1 通ずつ送信されます。

【指定した Email 宛に全てのプロファイルを送信する】

本画面で指定した Email アドレス宛に、1 通のメールでまとめてユーザプロファイルを送信します。

以上で、ユーザプロファイル一括登録手順は終了です。

11　ファイアウォール設定

ファイアウォール設定とは一部のアクセス（ポート、プロトコルなど）を制限したい場合に設定します。ユーザプロファイル毎に制御が可能です。ファイアウォールに関する設定は「接続管理」タブの「ファイアウォール設定」画面から行います。

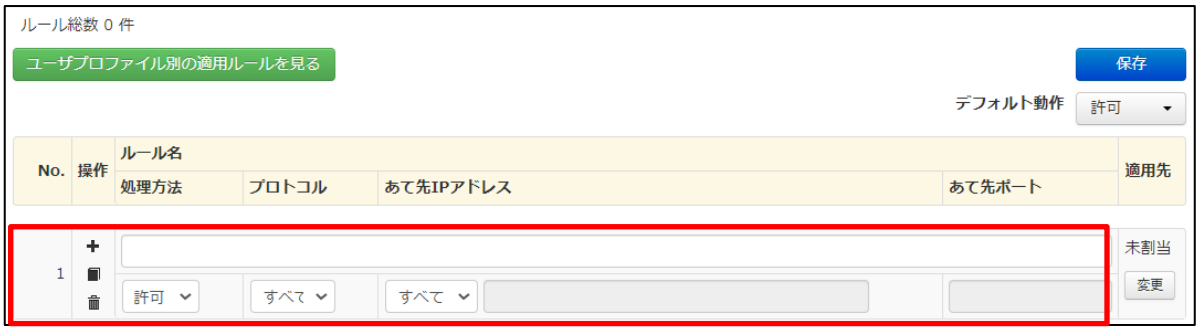
11-1 ファイアウォール設定の新規作成

1. 赤枠の「＋」をクリックするとルール作成画面が表示されます。

2. 赤枠内を以下のように記入します。

項目	入力値・選択値・内容
処理方法	プルダウンにて「許可」、「破棄」を選択。 「許可」：「プロトコル」・「あて先 IP アドレス」・「あて先ポート」についてアクセスを許可します。 「破棄」：「プロトコル」・「あて先 IP アドレス」・「あて先ポート」についてアクセスを禁止します。

項目	入力値・選択値・内容
プロトコル	プルダウンにて「すべて」、「TCP」、「UDP」、「ICMP」を選択。 「すべて」：「あて先 IP アドレス」に対して、全プロトコル共通のルールを適用します。 「TCP」：「あて先 IP アドレス」・「あて先ポート」に対して TCP プロトコルのルールを適用します。 「UDP」：「あて先 IP アドレス」・「あて先ポート」に対して UDP プロトコルのルールを適用します。 「ICMP」：「あて先 IP アドレス」に対して ICMP プロトコルのルールを適用します。
あて先 IP アドレス	左側プルダウンにて「すべて」、「IP 指定」を選択。 「すべて」：すべての IP アドレスに対してルールを適用します。 「IP 指定」：指定した IP アドレスに対してルールを適用します。 ※　ネットワークアドレス表記（例：192.168.1.0/24）または、ホストアドレス（例：192.168.1.2）を指定で記入します。この表記以外での登録はできません。
あて先ポート	プロトコルが「TCP」および「UDP」の場合、ポート番号（0~65535）を記述。 「23」のように単独の指定、「137-139」の様な範囲指定ができます。 ※　プロトコルが「すべて」および「ICMP」の場合は設定できません。



【例】

例として以下の設定でファイアウォールルールを作成します。

項目	入力値・選択値・内容
ルール名	EXAMPE
処理方法	「破棄」
プロトコル	「TCP」
あて先 IP アドレス	「IP 指定」
	192.168.1.0/24
あて先ポート	80-88

3. デフォルト動作の処理を選択します。赤枠をクリックすることで「許可」、「破棄」を選択します。

4. 作成したルールを適用させるユーザプロファイルを選択します。赤枠の「変更」をクリックします。

5. サブ画面が表示されます。ルールの適用をユーザプロファイル毎にするか、すべてのユーザプロファイルにするか選択します。「ルール適用一覧」の上段の欄から、プルダウンメニューにて「個別」もしくは、「すべて」をクリックします。

重要 ● 1 つのユーザプロファイルに適用できるルール数は 30 件までとなります。

項目	選択値・内容
個別	「ユーザプロファイル一覧」から「ルール適用一覧」へ移動させたユーザプロファイルが対象となります。 **※ ファイアウォール設定作成後に作成されたユーザプロファイルは自動では対象とはなりません。**
すべて	すべてのユーザプロファイルが対象となります。 **※ ファイアウォール設定作成後に作成されたユーザプロファイルも対象となります。**

6. ルールの適用をユーザプロファイル毎（「ルール適用一覧」の上段を「個別」）にしている場合は、以下の方法でユーザプロファイルの適用をします。

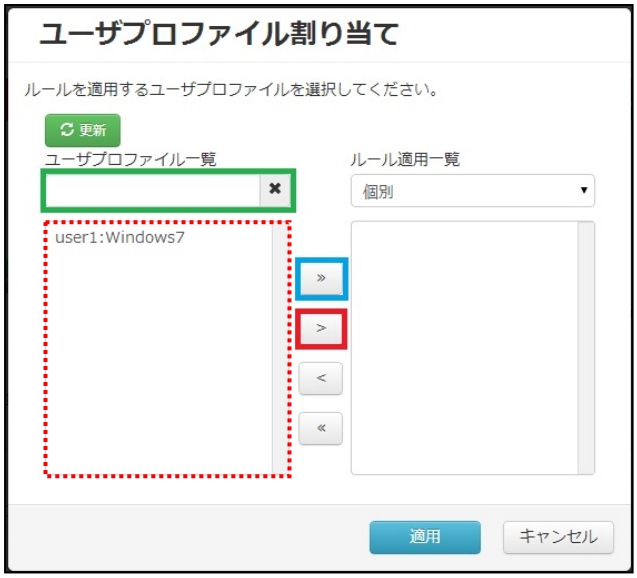
① 「ユーザプロファイル一覧」の中から個別でユーザプロファイルに設定を適用させる場合

「ユーザプロファイル一覧」の中から追加するユーザプロファイルを選択し、赤枠 ＞ のをクリックします。選択したユーザプロファイルが「ルール適用一覧」に移動します。

補足 緑枠内に、ユーザプロファイル ID を入れると、絞り込みができます。

② 「ユーザプロファイル一覧」の中からすべてのユーザプロファイルに設定を適用させる場合

青枠の » をクリックします。「ユーザプロファイル一覧」の中のすべてのユーザプロファイルが「ルール適用一覧」に移動します。



7. 選択したユーザプロファイルが「ルール適用一覧」に移動した事を確認し、「適用」をクリックします。

8. 「保存」をクリックすると、作成したルールが保存されます。

9. 「ファイアウォールルールを○件設定しました。」というメッセージが表示されます。

以上で、ファイアウォール設定の新規作成は終了です。

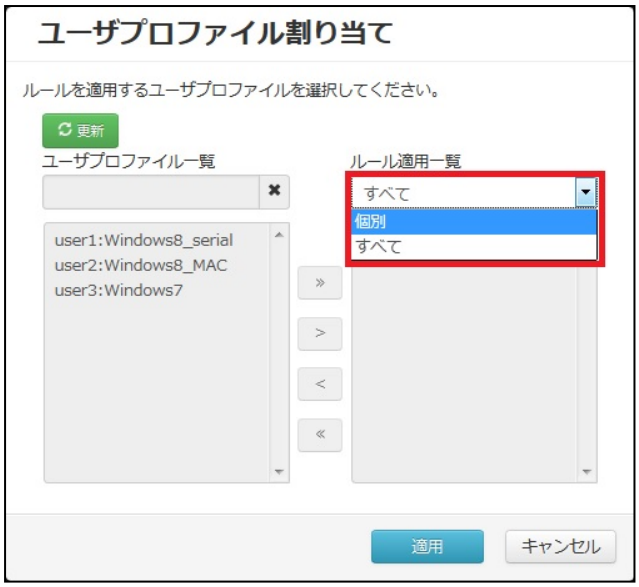
11-2 ファイアウォール設定のユーザプロファイル割当解除

1. 作成したユーザプロファイル割当を解除したいルールの「変更」をクリックします。

2. サブ画面が表示されます。

メモ

- 「ルール適用一覧」の上段の欄が「すべて」になっている場合は、プルダウンメニューにて「個別」をクリックし、設定をクリックするとすべてのユーザプロファイルが解除されます。



3. 以下の方法で、ルールの割当をユーザプロファイル毎で適用解除します。

① 「ルール適用一覧」の中から個別でユーザプロファイルの割当を適用解除させる場合

「ルール適用一覧」の中から、適用解除するユーザプロファイルを選択し、赤枠 < のをクリックします。選択したユーザプロファイルが「ユーザプロファイル一覧」に移動します。

② 「ルール適用一覧」の中からすべてのユーザプロファイルの割当を適用解除させる場合

青枠の « をクリックします。「ルール適用一覧」の中のすべてのユーザプロファイルが「ユーザプロファイル一覧」に移動します。

4. 選択したユーザプロファイルが「ユーザプロファイル一覧」に移動した事を確認し、「適用」をクリックします。

5. 「保存」をクリックすると、変更を行ったルールが保存されます。

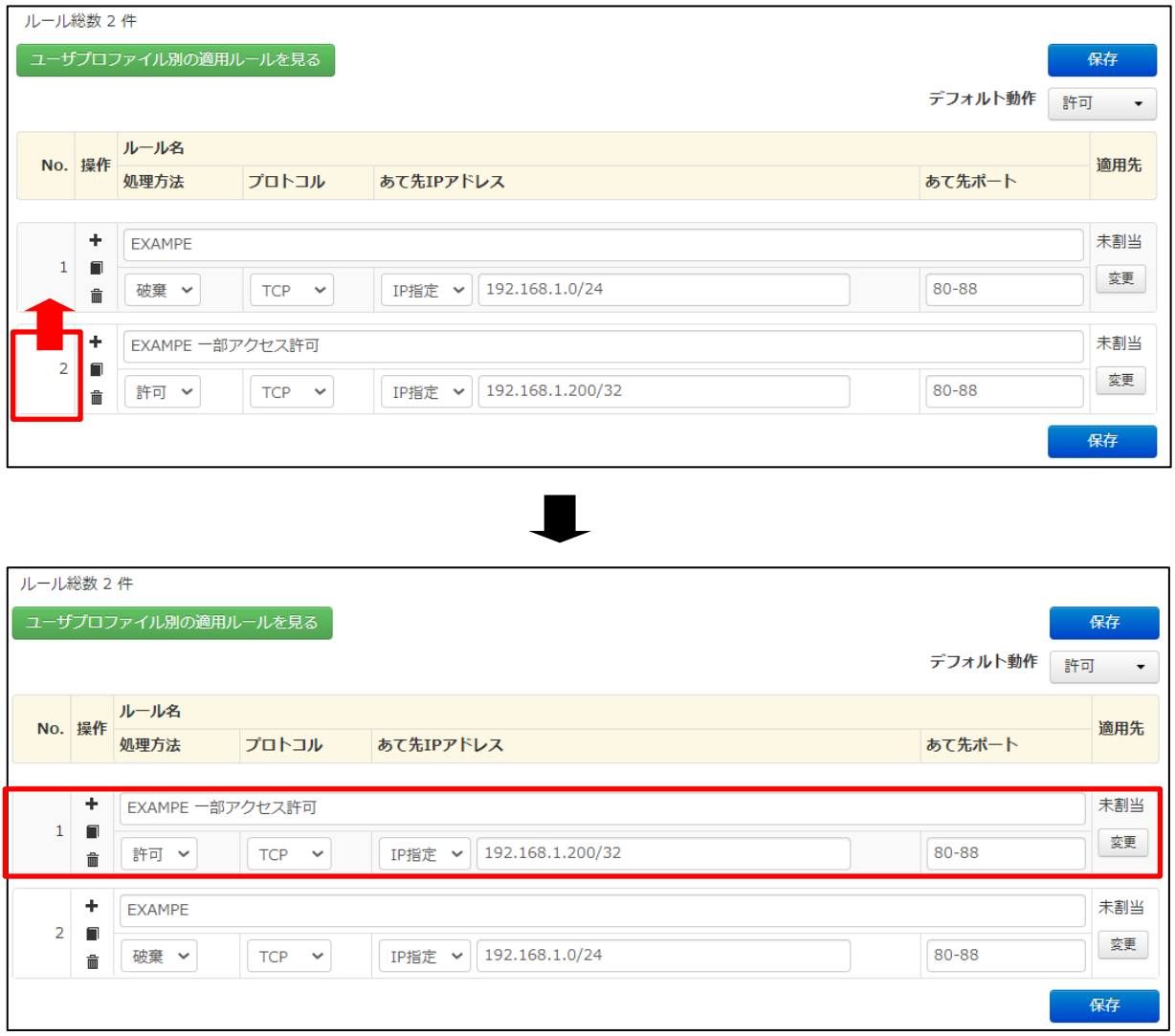
6. 「ファイアウォールルールを○件設定しました。」というメッセージが表示されます。

以上で、ファイアウォール設定のユーザプロファイル割当解除は終了です。

11-3 ファイアウォール設定の優先順位

ファイアウォールルールが複数ある場合、赤枠の「No.」欄が優先順位となります。ファイアウォールルールが複数適用されているユーザプロファイルがあった場合、「No.」が小さいものから適用されていきます。

1. 優先順位は赤枠のように「No.」欄を”ドラッグ&ドロップ"することにより変更できます。



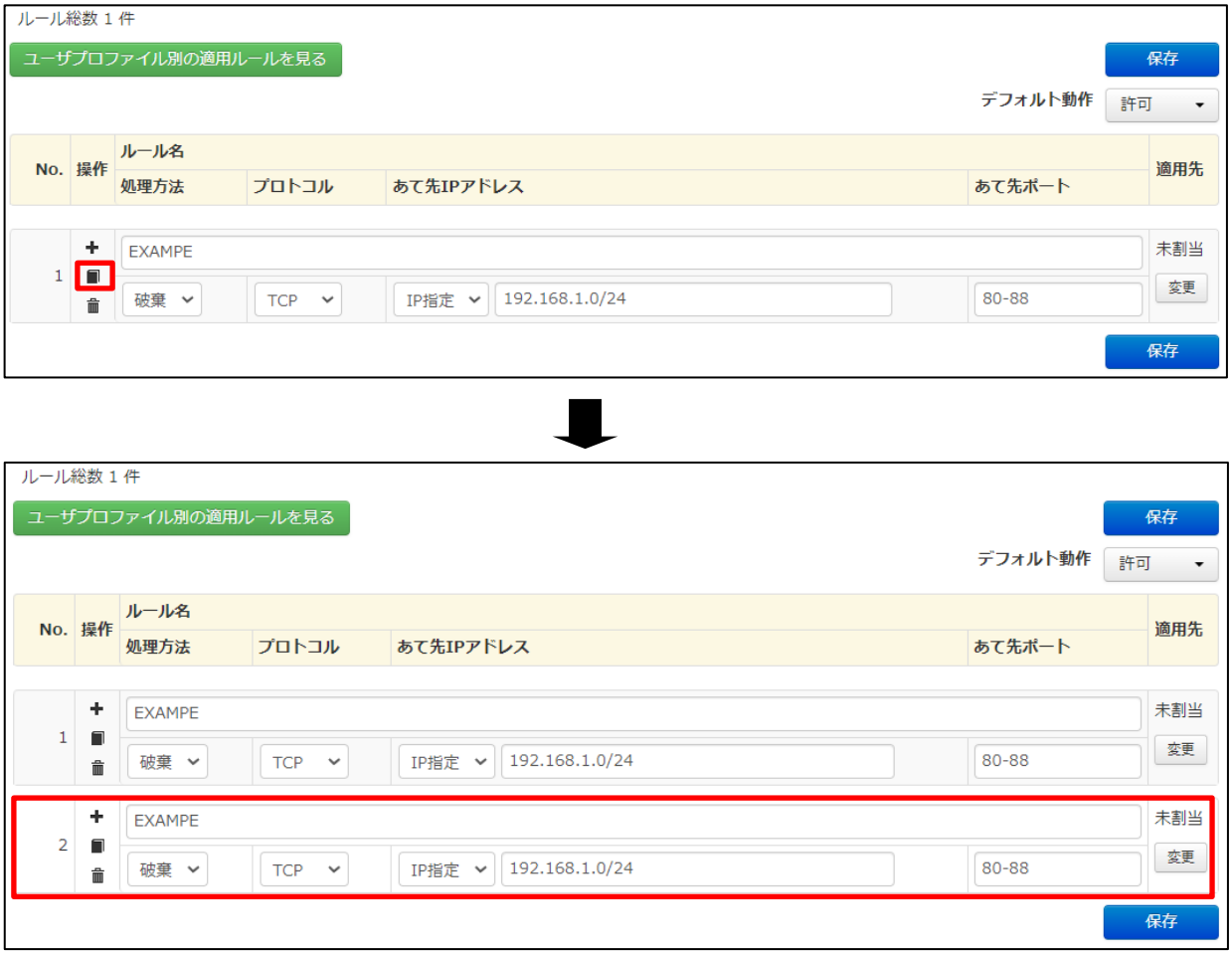
2. 「保存」をクリックすると、優先順位を変更した状態で保存されます。

3. 「ファイアウォールルールを○件設定しました。」というメッセージが表示されます。

以上で、ファイアウォール設定の優先順位は終了です。

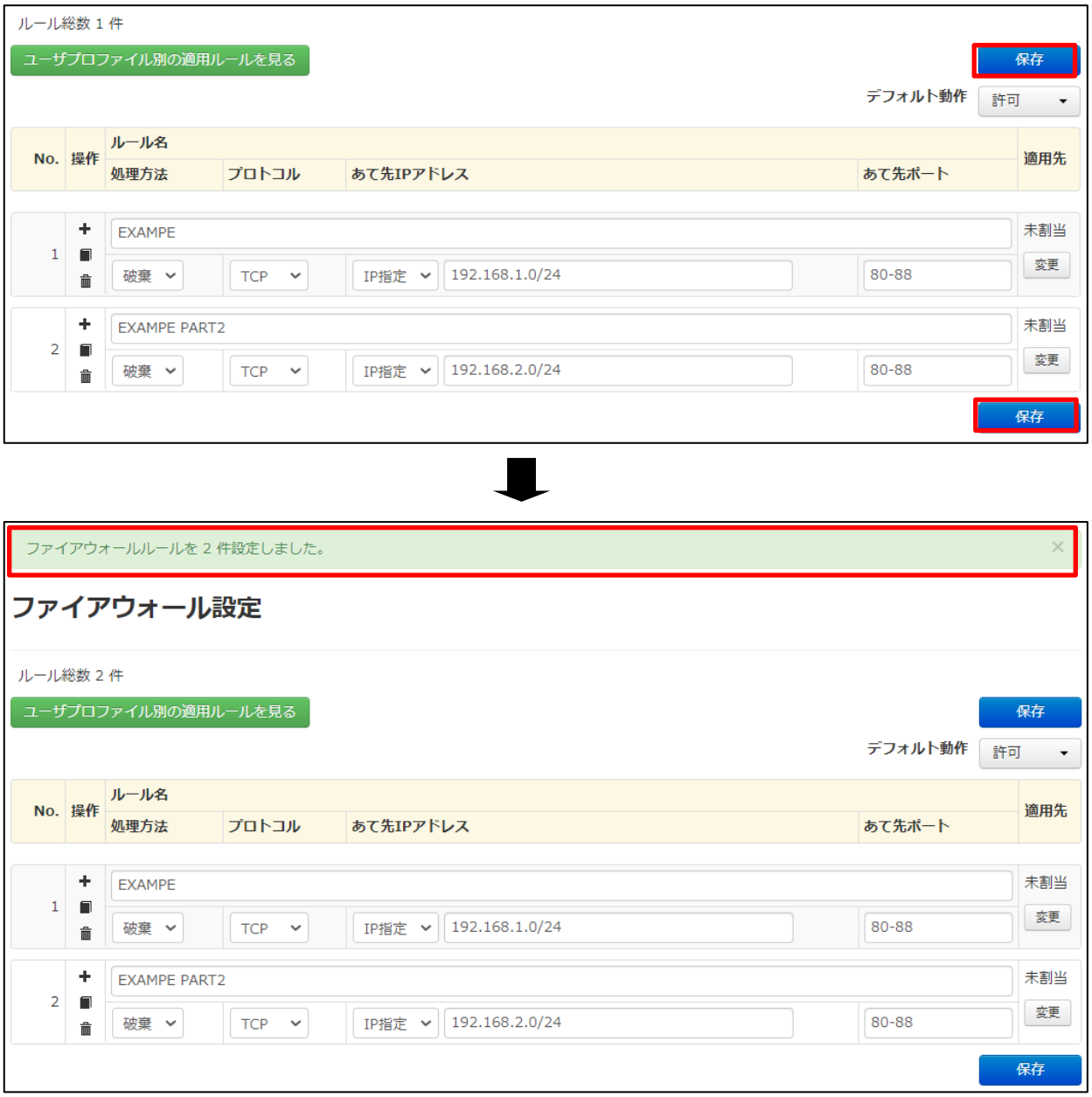
11-4 ファイアウォール設定の複製

1. 赤枠をクリックすると、作成したルールを複製できます。



2. 複製したルールを編集できます。

3. 「保存」をクリックし、「ファイアウォールルールを○件設定しました。」というメッセージが表示されます。



以上で、ファイアウォール設定の複製は終了です。

11-5 ファイアウォール設定の削除

1. 赤枠をクリックすると、作成したルールを削除できます。

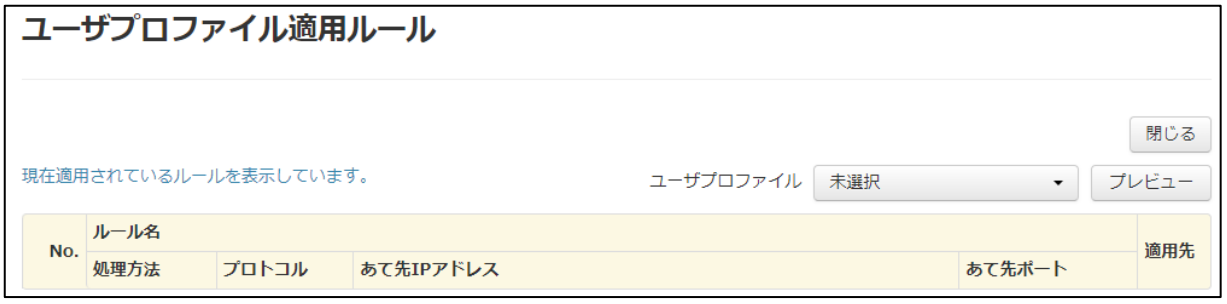
2. 「保存」をクリックし、「ファイアウォールルールを○件設定しました。」というメッセージが表示されます。

以上で、ファイアウォール設定の削除は終了です。

11-6 ユーザプロファイル毎ファイアウォール設定適用状況の確認

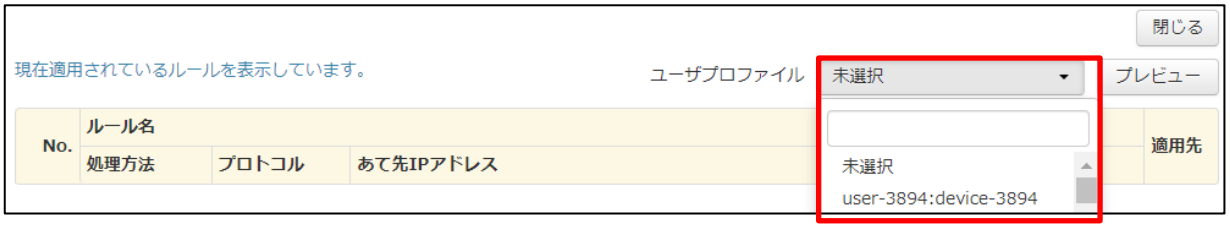
1. 赤枠をクリックすると、ユーザプロファイル毎に適用されているファイアウォール設定の割当を確認できます。

2. 以下のサブ画面が表示されます。赤枠をクリックします。



3. ファイアウォール設定の適用状況を確認したいユーザプロファイル ID をクリックします。

補足 緑枠内にユーザプロファイル ID を入れると、絞り込みができます。



4. ファイアウォール設定の適用状況を確認できます。赤枠の「プレビュー」をクリックすると、「保存」を行っていない編集中のルールも含めた形で表示されます。

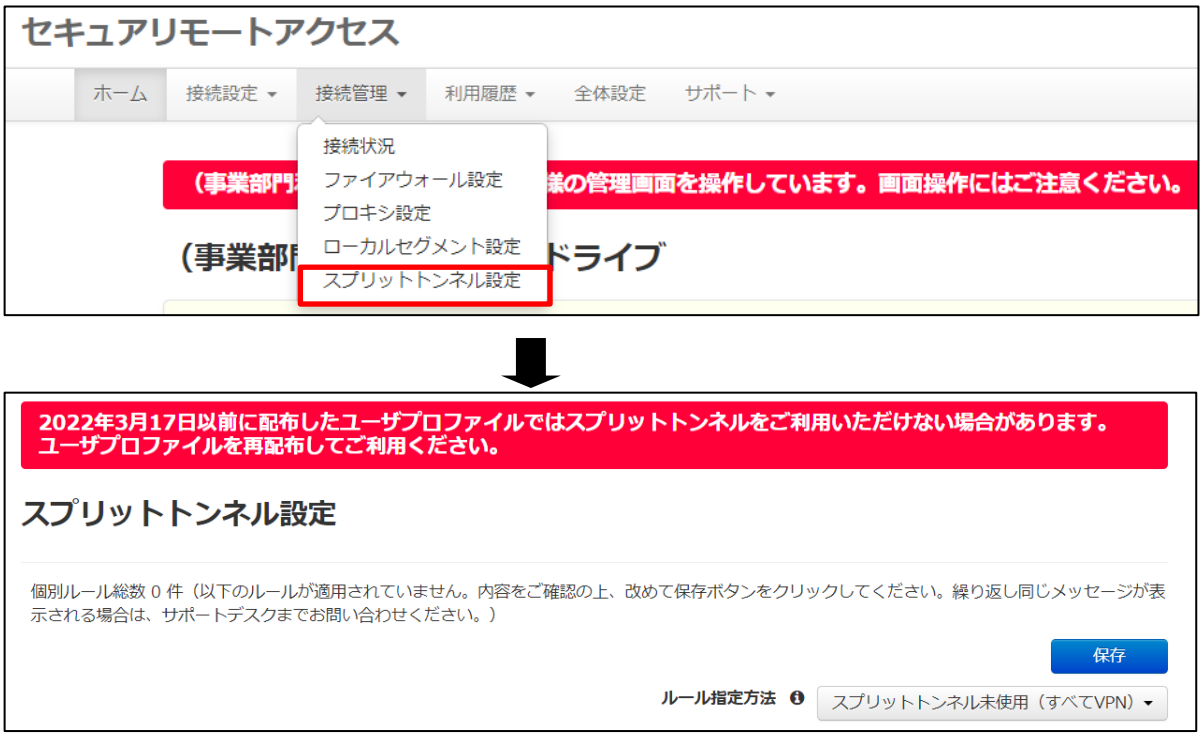
以上で、ユーザプロファイル毎ファイアウォール設定適用状況の確認は終了です。

12　スプリットトンネル設定

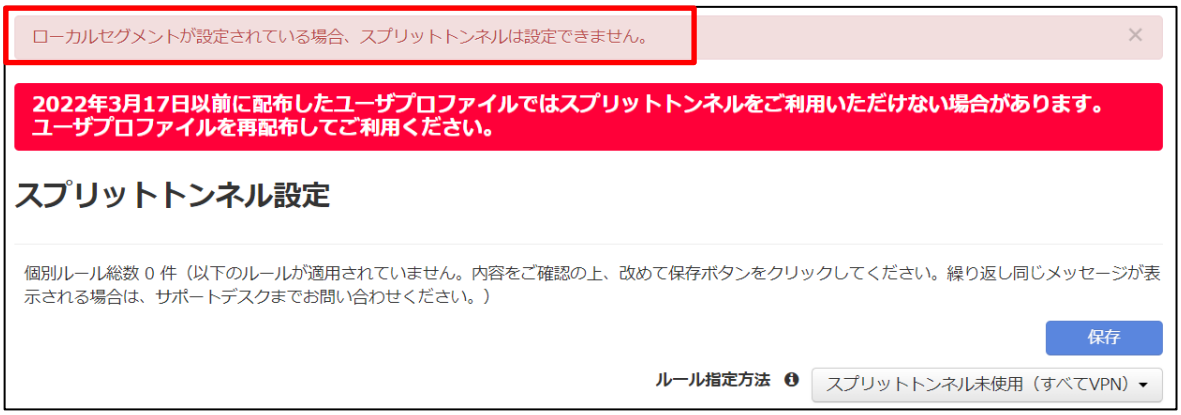
スプリットトンネル機能とは、一部のアクセス（IP アドレス、ドメイン）に対して通信経路を制限したい場合に設定します。スプリットトンネルに関する設定は「接続管理」タブの「スプリットトンネル設定」画面から行ないます。

重要

- ローカルセグメントが設定されている場合、スプリットトンネル設定はできません。
- 2022 年 3 月 17 日以前に配布したユーザプロファイルではスプリットトンネルをご利用いただけません。
  ご利用の場合は、ユーザプロファイルを再配布してご利用ください。

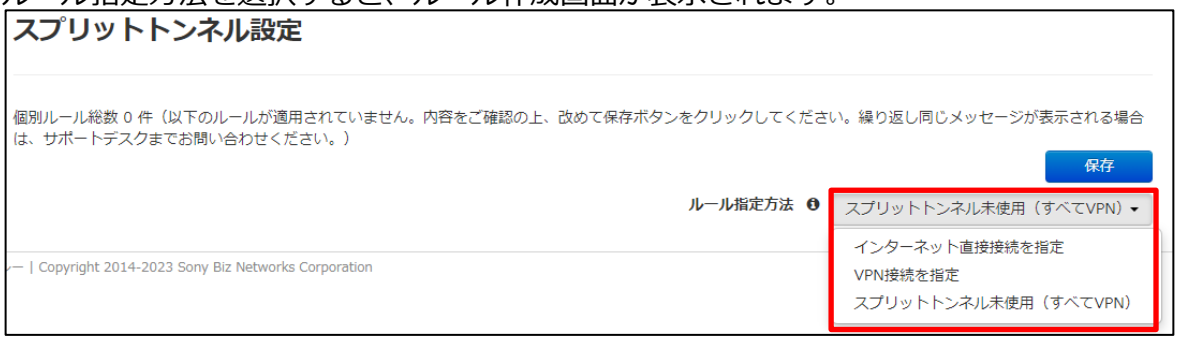


※ローカルセグメント設定が有効であった場合、スプリットトンネル機能をご利用いただけない旨の注意が表示されます。



12-1 スプリットトンネル設定の新規作成

1. ルール指定方法を選択すると、ルール作成画面が表示されます。



2. ルール指定方法により、表示される項目が異なります。
各ルール指定方法で表示される内容については、下記表をご参照ください。

項目	入力値・選択値・内容
ルール指定方法	プルダウンにて下記 3 つのルールからいずれかを選択 ※初期設定は「スプリットトンネル未使用（すべて VPN）」 ○「スプリットトンネル未使用（すべて VPN）」 すべての通信は VPN 内へ送信されます。 ○「VPN 接続を指定」 VPN 内へ送信する宛先を指定できます。 指定していない宛先は端末から直接アクセスします。 「VPN 接続を指定」を選択した場合、個別ルールの設定が可能です。 ○「インターネット直接接続を指定」 端末から直接アクセスする宛先を指定できます。 指定していない宛先は VPN 内へ送信されます。 「インターネット直接接続を指定」を選択した場合、 グループルール、個別ルールの設定が可能です。

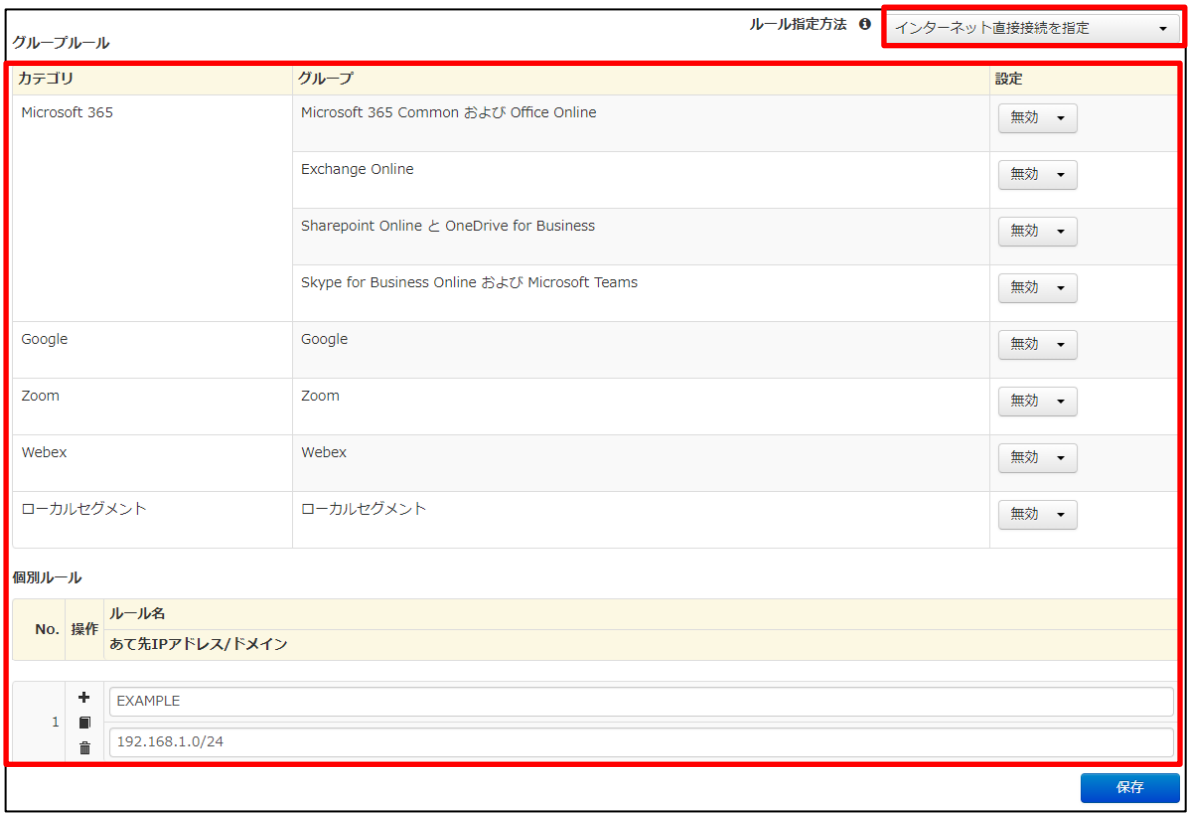
項目	入力値・選択値・内容
ルール指定方法	グループルールでは、有効にしたカテゴリのあて先 IP アドレスに対して接続元の WAN 回線の IP アドレスからアクセスします。 各カテゴリの IP アドレスは以下のリンク先より引用 しています。 ●Microsoft365 Microsoft 365 Common および Office Online Exchange Online Sharepoint Online と OneDrive for Business Skype for Business Online および Microsoft Teams Microsoft は Microsoft365 で使用される IP アドレスを 「最適化」「許可」「既定」３つのカテゴリに分類しています。 新しい Office 365 エンドポイントのカテゴリ 「既定」は、CDN などを利用していることから IP アドレス非公開の為、ローカルブレイクアウトの対象外となります。 **●Google** Google API とサービスのデフォルトのドメインで使用される IP アドレス 対象は、goog.json から cloud.json を除いた IP アドレスとなります。 **●Zoom** Zoom のネットワーク ファイア ウォールまたはプロキシサーバーの設定 Zoom CDN は、ローカルブレイクアウトの対象外となります。 **●Webex** Webex メディアサービスの IP サブネット ●ローカルセグメント 接続元ローカルセグメントの IP アドレスとなります。
個別ルール名	任意の個別ルール名を入力します。

項目	入力値・選択値・内容
あて先 IP アドレス/ドメイン	個別ルールとして、指定した IP アドレス、もしくは指定したドメインに対してルールを適用します。 ※「あて先 IP アドレス」の場合、ネットワークアドレス/プレフィックス長の形式で入力してください。 ※「ドメイン」の場合、ドメインの形式で入力してください。 ※iOS ではドメイン指定でのスプリットトンネルをご利用いただけません。 ご利用の場合には、あて先 IP アドレスをご指定ください。

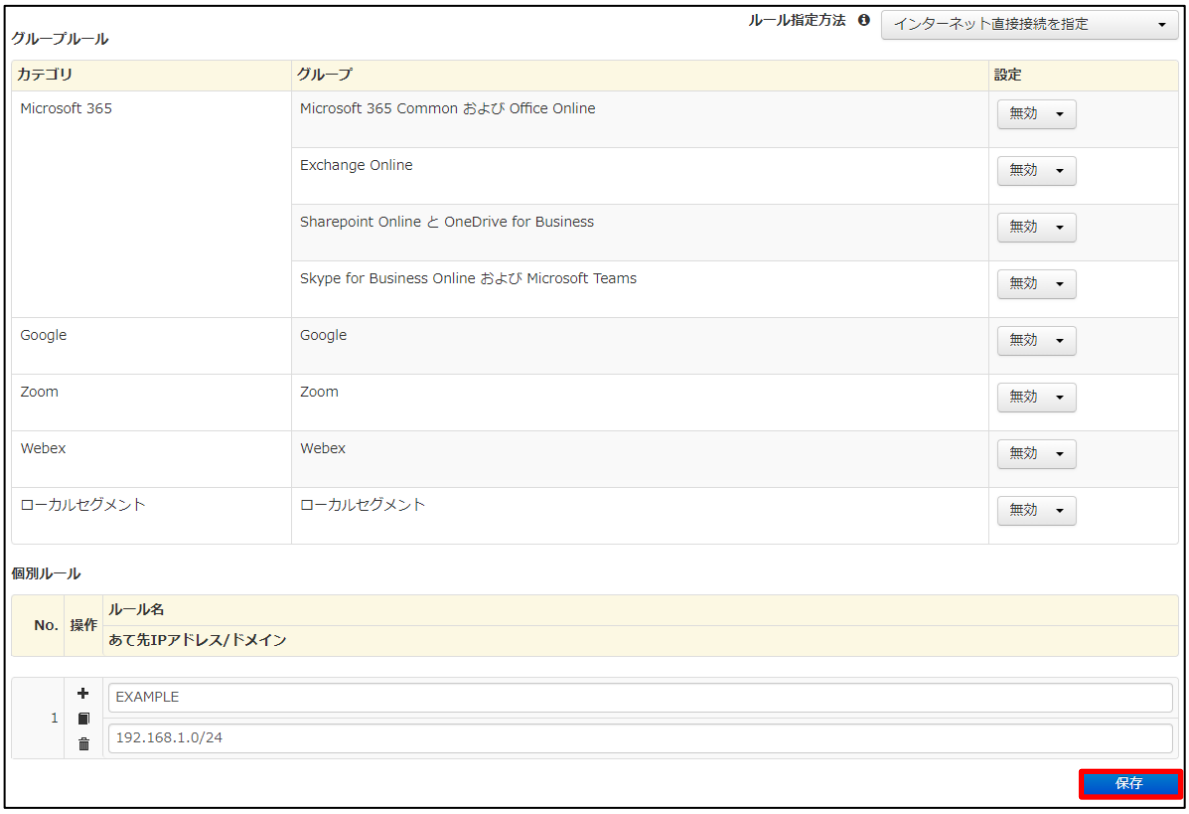
【例】

例として以下の設定でスプリットトンネルルールを作成します。

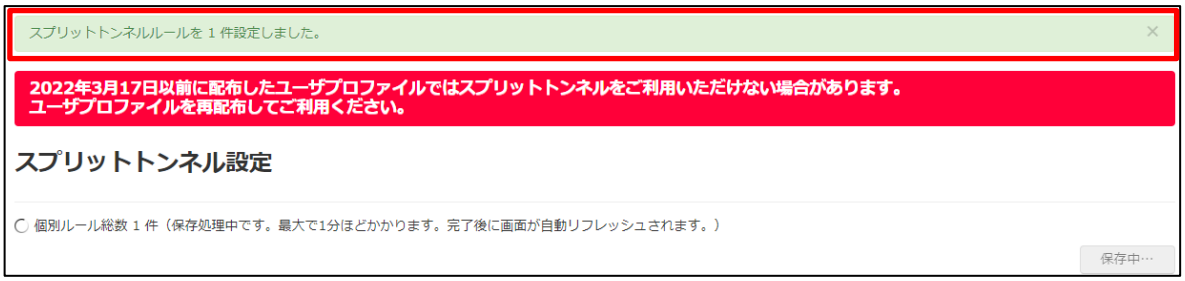
項目	入力値・選択値・内容
基本動作	「インターネット直接接続を指定」
グループルール	すべて「無効」 ※初期設定では、すべてのグループで「無効」です。
個別ルール名	「EXAMPLE」
あて先 IP アドレス/ドメイン	192.168.1.0/24



3. 「保存」ボタンをクリックすると、作成したルールが保存されます。

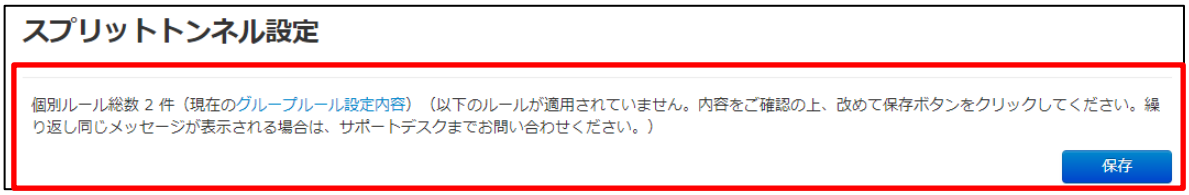


4. 「スプリットトンネルルールを○件設定しました。」というメッセージが表示されます。
個別ルール総数 ○件（保存処理中です。最大で 1 分ほどかかります。完了後に画面が自動リフレッシュされます。）



重要

設定したルールが適用されない場合、下図のように表示されます。
内容をご確認の上、改めて保存ボタンをクリックしてください。
繰り返し同じメッセージが表示される場合は、サポートデスクまでお問い合わせください。

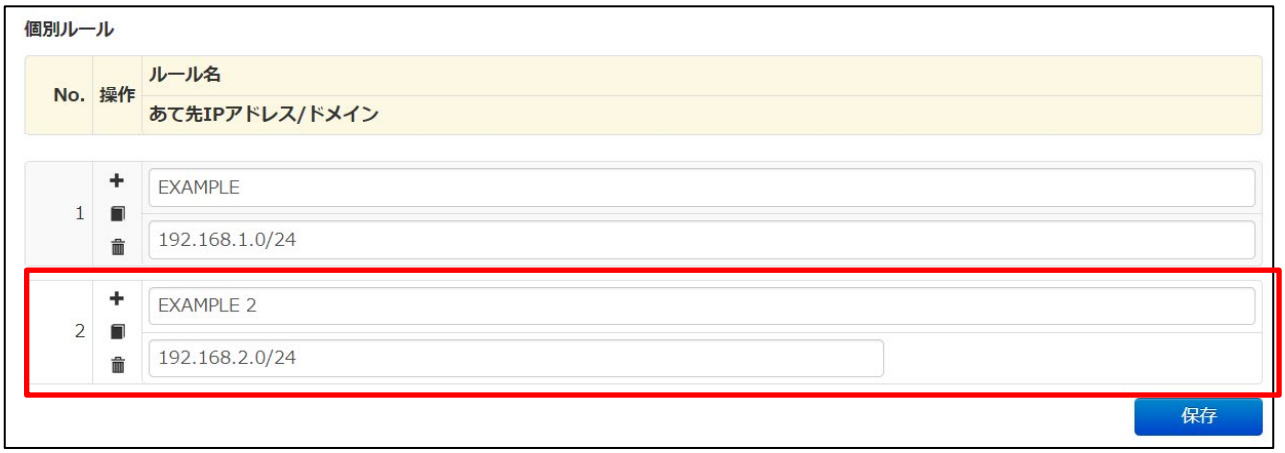


以上で、スプリットトンネル設定の新規作成は終了です。

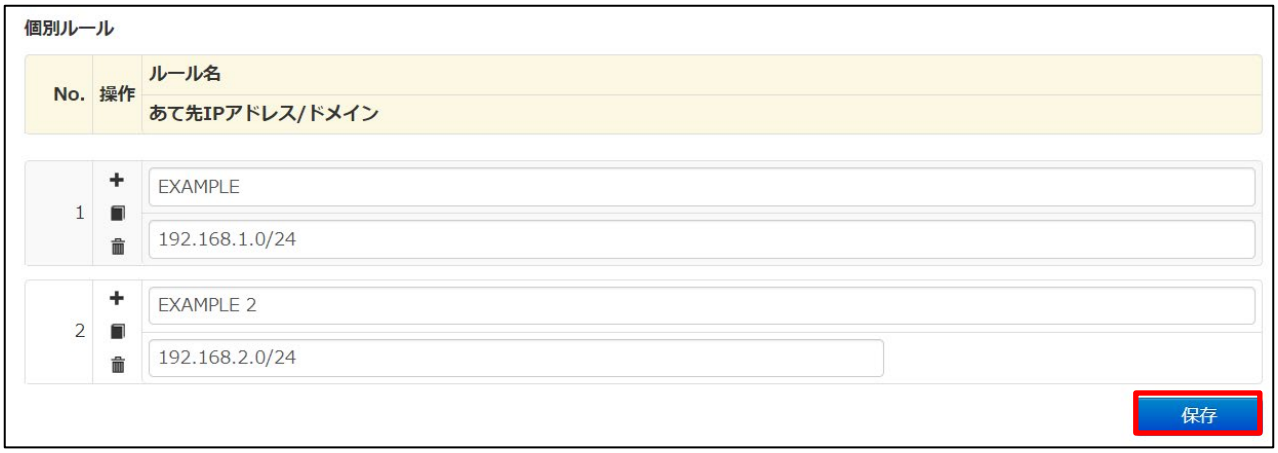
12-2 スプリットトンネル設定の複製

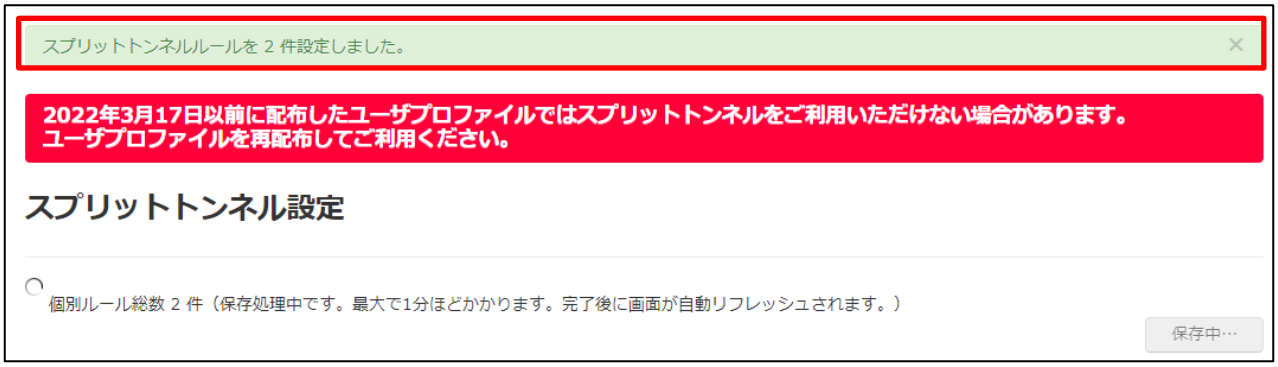
1. 赤枠をクリックすると、作成したルールを複製できます。

2. 複製したルールを編集できます。



3. 「保存」をクリックし、「スプリットトンネルルールを○件設定しました。」というメッセージが表示されます。
※個別ルール総数 ○件（保存処理中です。最大で 1 分ほどかかります。完了後に画面が自動リフレッシュされます。）

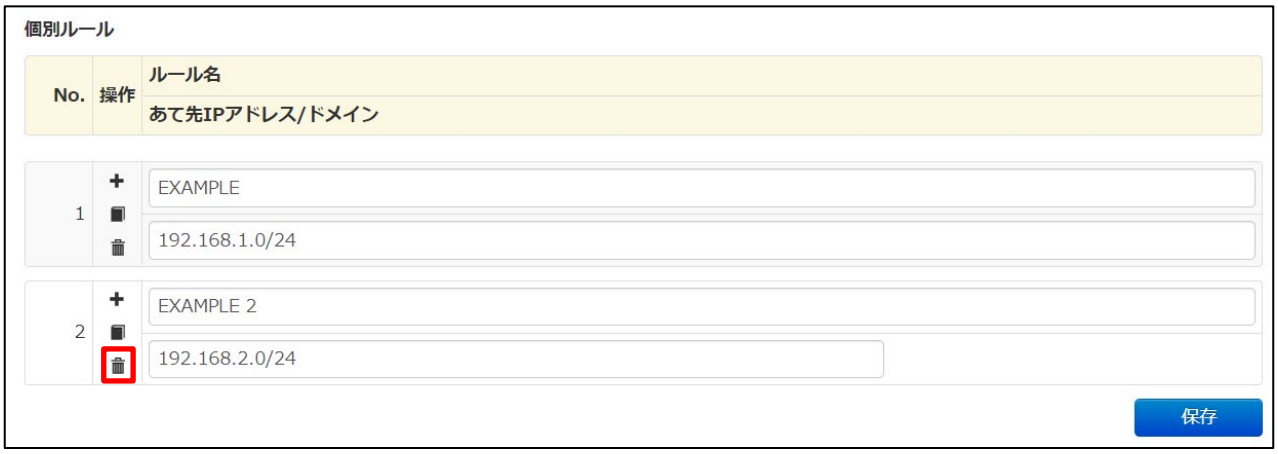




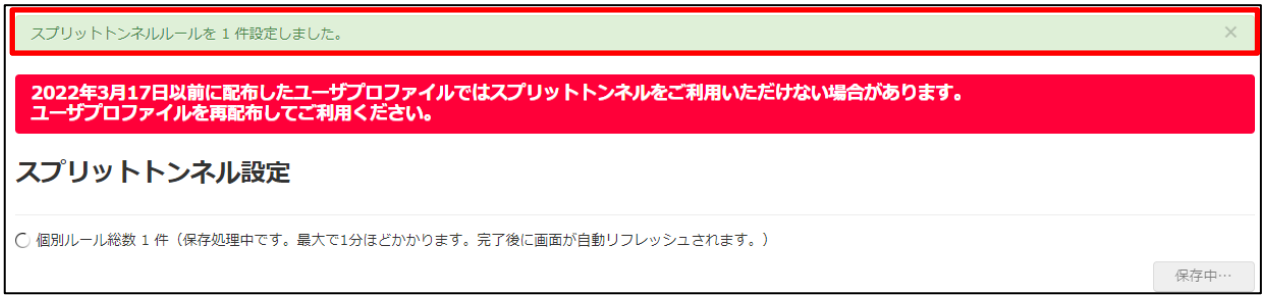
以上で、スプリットトンネル設定の複製は終了です。

12-3 スプリットトンネル設定の削除

1. 赤枠をクリックすると、作成したルールを削除できます。



2. 「保存」をクリックし、「スプリットトンネルルールを○件設定しました。」というメッセージが表示されます。
※個別ルール総数 ○件（保存処理中です。最大で 1 分ほどかかります。完了後に画面が自動リフレッシュされます。）



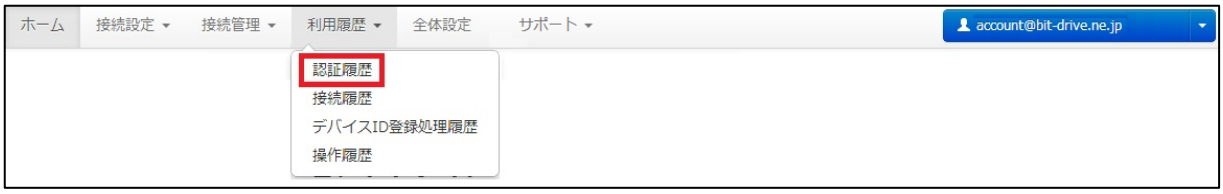
以上で、スプリットトンネル設定の削除は終了です。

13　利用履歴

13-1 認証履歴

1. 「利用履歴」タブの「認証履歴」から認証履歴を確認できます。

> メモ
> - 認証履歴は 6 ヶ月保存され、赤枠をクリックすると CSV エクスポートができます。
> - VPN 接続中の履歴は認証履歴に表示されます。
> - VPN 切断後の履歴は接続履歴に表示されます。



2. 「失敗理由」と「考えられる原因と対処方法」につきましては弊社お客さまサポートのよくあるご質問(FAQ)に掲載しておりますので、ご確認ください。

https://faq2.bit-drive.ne.jp/support/traina-faq/

以上で、認証履歴は終了です。

13-2 接続履歴

1. 「利用履歴」タブの「接続履歴」から接続履歴を確認できます。

メモ
- 接続履歴は 6 ヶ月保存され、赤枠をクリックすると CSV エクスポートができます。
- VPN 接続中の履歴は認証履歴に表示されます。
- VPN 切断後の履歴は接続履歴に表示されます。

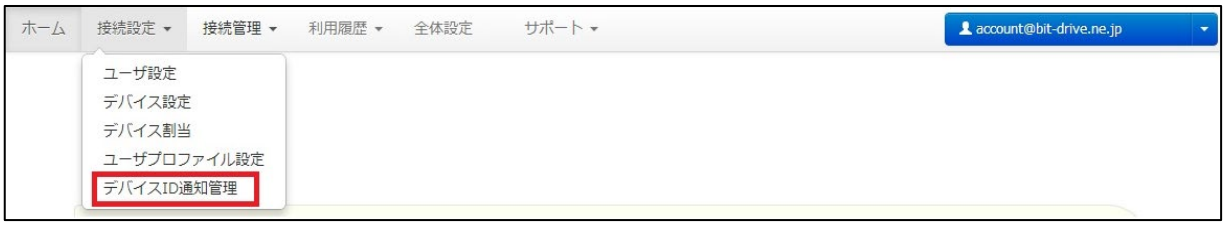
以上で、接続履歴は終了です。

13-3 デバイス ID 登録処理履歴

1. 「利用履歴」タブの「デバイス ID 登録処理履歴」からデバイス ID 登録処理履歴を確認できます。

> **メモ**
> ● デバイス ID 登録処理履歴は 6 ヶ月保存され、赤枠をクリックすると CSV エクスポートができます。

2. また、直近のデバイス ID 登録処理履歴に関しては、「接続設定」の「デバイス ID 通知管理」でも確認できます。



3. 「処理内容」が「エラー」となった際に表示される「メッセージ」と「考えられる原因と対処方法」の一覧は以下になります。該当の「メッセージ」が表示された場合、「考えられる原因と対処方法」をご確認ください。

メッセージ	考えられる原因と対処方法
エラーが発生しました。デバイス ID は 200 文字以内で入力してください。	デバイス ID が 201 文字以上の文字長となっている可能性があります デバイス自体の ID は変更できないため、デバイス設定より該当デバイスを MAC アドレス認証でご登録ください
エラーが発生しました。デバイス ID に使用禁止文字が含まれています。	デバイス ID に使用禁止文字が使用されている可能性があります ※使用可能文字は「半角英数字」および「-」「_」「.」「{」「}」「<」「>」「#」となります デバイス自体の ID は変更できないため、デバイス設定より該当デバイスを MAC アドレス認証でご登録ください
エラーが発生しました。デバイス ID はすでに存在します。[デバイス名：XX が使用中]	すでに該当デバイス ID が他のデバイスで使用されているため、デバイス設定より重複しているデバイスのデバイス ID を削除してください
エラーが発生しました。	弊社にてエラー詳細を確認する必要があります 恐れ入りますが NURO Biz サポートデスクまでお問い合わせください

以上で、デバイス ID 登録処理履歴は終了です。

13-4 操作履歴

1. 「利用履歴」タブの「操作履歴」から操作履歴を確認できます。

> メモ
> - 操作履歴は 6 ヶ月保存され、赤枠をクリックすると CSV エクスポートができます。

以上で、操作履歴は終了です。

14　各種参考情報

弊社が提供しているマニュアル・よくあるお問い合わせ内容については、以下のページを参照してください。

- サービスに関するマニュアル・ソフトウェアダウンロード
  https://www.bit-drive.ne.jp/support/download/index.html

- サービスに関するよくあるご質問(FAQ)
  https://faq2.bit-drive.ne.jp/support/traina-faq/

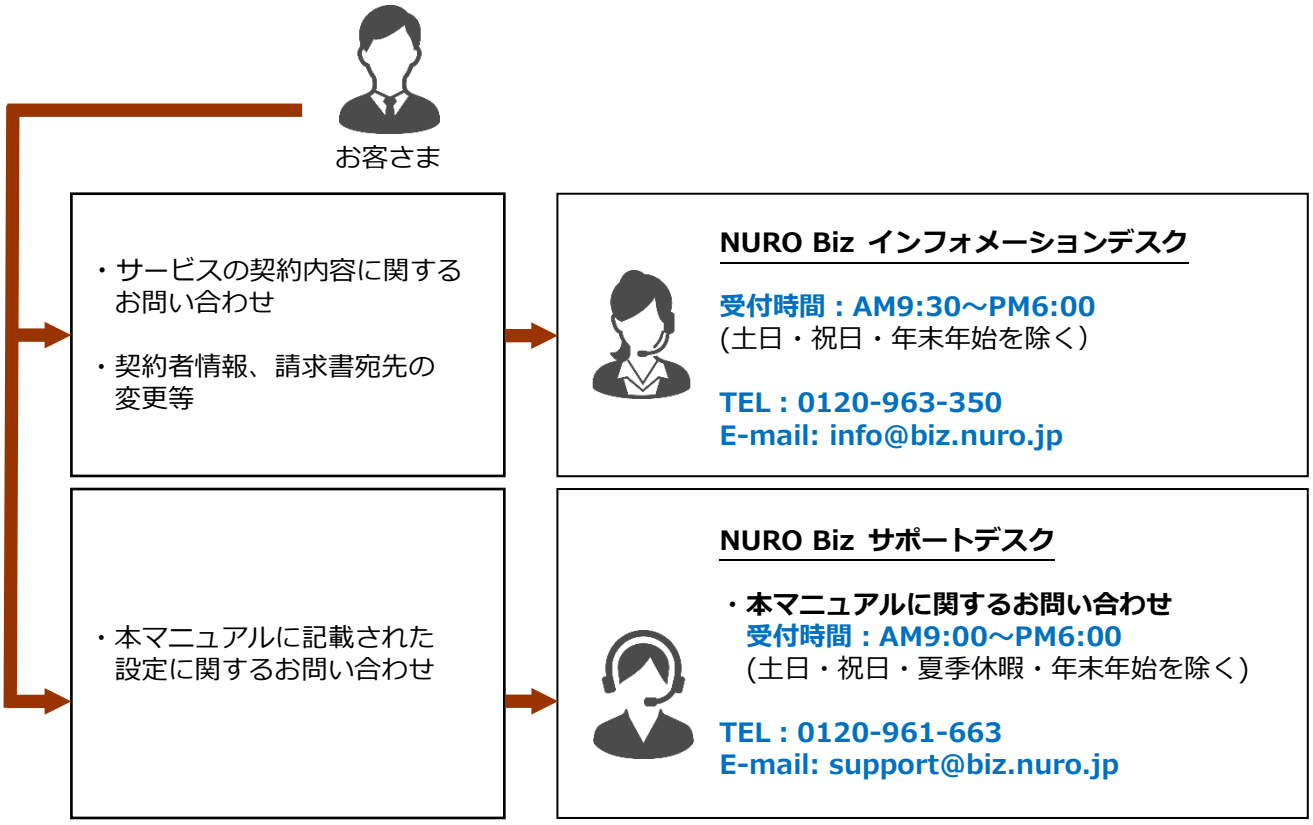
- その他、弊社が提供しているサービスに関するマニュアル・よくあるお問い合わせ
  https://www.bit-drive.ne.jp/support/index.html

15　サポート体制

15-1 お問い合わせ窓口

本サービスのサポート体制は以下の通りです。

お問い合わせいただく際には、次ページの確認事項を確認の上、ご連絡をお願いします。



15-2 ご連絡前のお願い

1. お問い合わせ際は『会社名』、『サービス名』をご記載ください。お客さま情報を迅速に確認してスムーズに対応を進めることができます。

2. お問い合わせの内容は技術的な確認になりますので、極力、申込時にご登録いただいたお客さまの技術担当者様の方から、お問い合わせいただきますようお願いいたします。

15-3 切り分け調査のご協力のお願い

状況に応じて、切り分け調査のため、お客さまにご協力をお願いする場合がございますので、ご理解、ご協力をお願いいたします。