セキュアリモートアクセス

クイックガイド

[システム管理者さま向け]

2024 年 5 月 29 日　Version 5.0

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
1.0	2019 年 7 月 17 日	初版リリース
1.1	2020 年 6 月 25 日	・「3-1 認証タイプ」の内容を修正しました。
2.0	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・画像を修正しました ・「3-1 認証タイプ」の内容を修正しました。 ・「4-2 デバイス設定」の内容を修正しました。 ・「6 サポート体制」を追加しました。
2.1	2021 年 4 月 12 日	・「4-2 デバイス設定」の内容を修正しました。
2.2	2021 年 6 月 7 日	・「4-2 デバイス設定」の内容を修正しました。
3.0	2022 年 3 月 17 日	・Version2.1.0 へのバージョンアップに伴い、以下の項目の内容・画像を修正しました。 ・「1-1 サービス構成」の内容を修正しました。 ・「4-4 ユーザプロファイル設定」の内容を修正しました。
4.0	2022 年 4 月 5 日	・窓口変更に伴い、窓口情報を修正しました。
4.1	2023 年 3 月 23 日	・「5.プロキシ設定」の画像を修正しました。
5.0	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。 ・「1-1.サービス構成」の内容を修正しました。 ・「3-1.認証タイプ」の内容を修正しました。 ・「4-2 デバイス設定」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

1.1　本ガイドについて

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サービスは、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や bit-drive データセンター内クラウドサービスへアクセスすることができます。

本クイックガイドでは、管理者さま向けの各種設定について最低限の機能に限定した（基本的な VPN 接続が可能となる）ケースを想定し、その手順を記載しております。

初めて設定する場合など、設定手順の流れを把握する際にご活用いただけます。

より高度で詳細な設定を行う際には、運用マニュアルを参照願います。
なお、各種マニュアルの位置づけを下表のとおりです。

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　※本資料	運用マニュアル 詳細手順
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。

巻末の付録に、クイックガイドの設定項目一覧とその説明を記載しております。
事前に準備頂きたい設定値やパラメータもございますので、ご確認をお願いいたします。

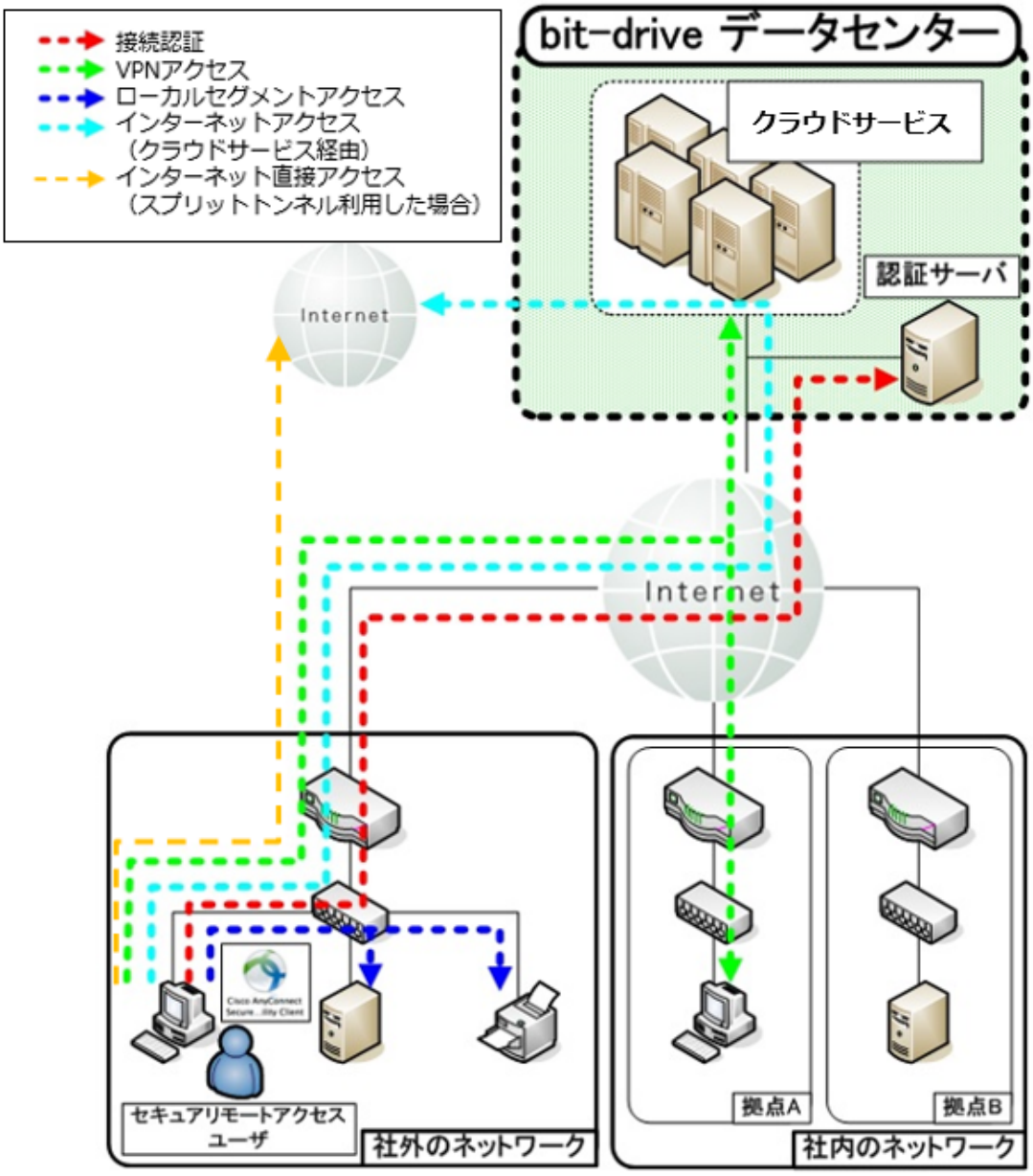
1-1　サービス構成

【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。
> - ローカルセグメントアクセスの設定方法については、「運用マニュアル」を参照願います。

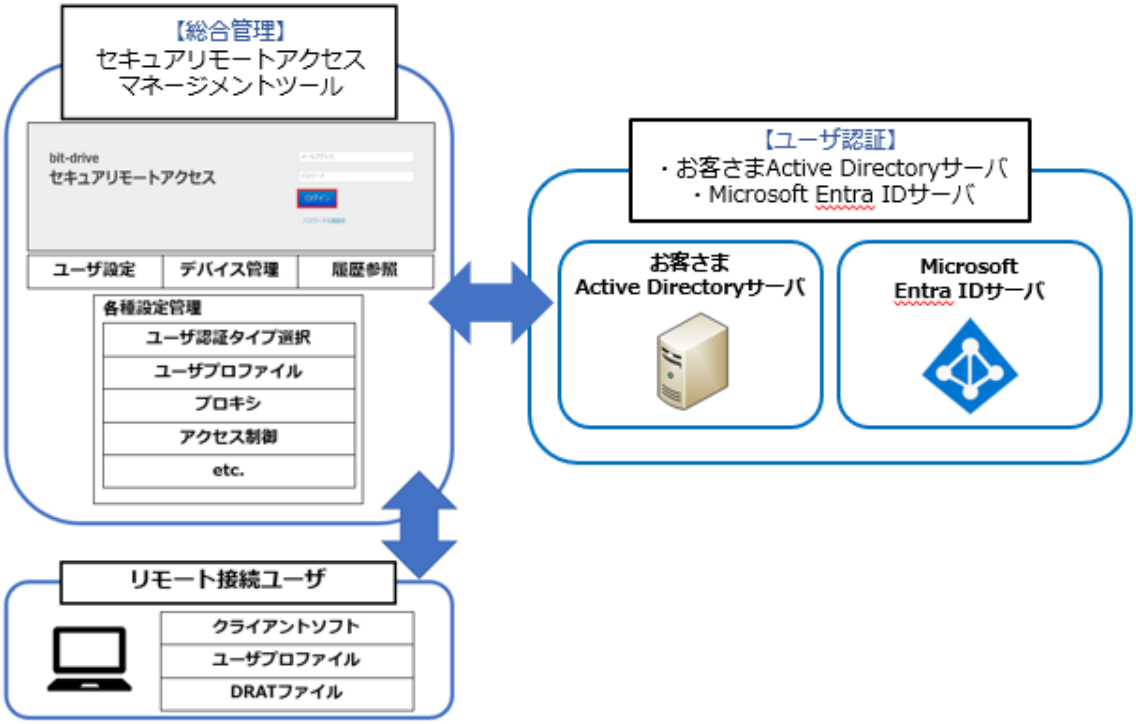


【管理構成】

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 のいずれか 1 つが必要となります。
- ファイアウォールの詳細設定については、「運用マニュアル」を参照願います。



2 ログイン・パスワード変更

1. Web ブラウザにて、以下 URL にアクセスします。

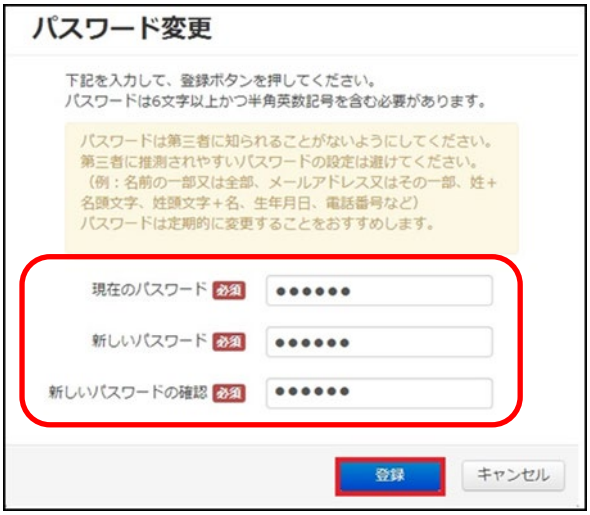
   URL:https://acmt.ravpn.bit-drive.ne.jp

2. ログイン画面が表示されるので、ご契約時に送付しております登録内容通知に記載されたログイン情報を入力し「ログイン」をクリックします。

3. ログイン後、画面右上のアカウント名の横にある▼をクリックし、「アカウント設定」をクリックします。

4. パスワードの「変更」をクリックします。

5. パスワード変更画面で現在のパスワードと新しいパスワードをそれぞれ入力し、「登録」をクリックします。



3 全体設定

全体設定では、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。メニューバーに表示されている「全体設定」をクリックします。

3-1 認証タイプ

セキュアリモートアクセスで利用するユーザ認証を設定します。

ユーザ認証方法は、お客さま所有の Active Directory サーバを利用してユーザ認証する方法、お客さま所有の Microsoft Entra ID サーバを利用してユーザ認証する方法の 2 つから選択できます。

1. 初期設定では認証タイプが「未選択」となっているため  をクリックし、ユーザ認証方法を選択します。

- **「Active Directory サーバ」を選択の場合**

  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ます。

  下記の画面が表示されますので、Active Directory サーバの「ホスト名」、「IP アドレス」、「ドメイン名」、「管理者パスワード」を入力し、「設定」をクリックします。

重要

- 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の IP アドレス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。

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

- **「Microsoft Entra ID サーバ」を選択の場合**

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ます。
下記の画面が表示されますので、Microsoft Entra ID サーバの「アプリケーション ID」、「アプリケーションパスワード」、「ドメイン名」、「管理者ユーザ名」、「管理者パスワード」、「シークレット有効期限」を入力し、「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。

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。

3-2　デバイスの自動登録

端末認証に使用するクライアントのデバイス ID を、初回接続時に自動登録するか選択します。

デバイス ID の自動登録の青文字「無効」をクリックすると下記のように吹き出しが表示されますので「有効」を選択し、青色のチェックボタンをクリックします。

> **重要**
> - デバイス ID の自動登録は例外を除き有効を推奨しますが、お客さまの環境やセキュリティポリシーなどにより、無効にすることも可能です。詳しくは別紙の運用マニュアルをご参照ください。

「デバイス ID の自動登録」が『有効』の場合、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。

「自動登録失敗時の通知」は「あり」を推奨します。次項にある「通知メール宛先」に自動登録失敗時の通知メールが送信されます。

3-3 通知メール宛先

デバイス ID 自動登録が失敗した場合に、メール通知するための管理者メールアドレスを登録します。「自動登録失敗時の通知」は「あり」を推奨します。通知先メールアドレスは複数登録できます。

1. 通知メール宛先欄の赤枠の「登録なし」をクリックすると下記の画面のように吹き出しが表示されますので、通知先のメールアドレスを入力し、青のチェックボタンをクリックします。
通知メールアドレスを複数登録する場合は、改行してメールアドレスを入力します。

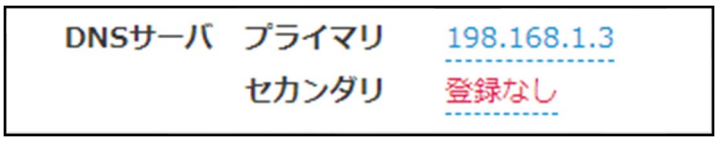
2. 表示が「登録なし」から設定したメールアドレスに変更され設定完了となります。

3-4 DNS サーバ

クライアント接続時に端末へ配布する DNS サーバの IP アドレスを登録します。

1. DNS サーバのプライマリ欄の「登録なし」をクリックすると下記のように吹き出しが表示されますので、利用する DNS サーバの IP アドレスを入力し、青色のチェックボタンをクリックします。

2. 「登録なし」から設定した IP アドレスに表示が変更され設定完了となります。



セカンダリのアドレスの設定が必要な場合、プライマリと同様の手順で設定することができます。

4 接続設定

接続設定では利用するユーザやデバイスの登録などを行います。

各設定で CSV ファイルをインポートして複数のユーザ・デバイスを同時に登録することもできますので詳しくは別紙の運用マニュアルをご参照ください。

4-1 ユーザ設定

セキュアリモートアクセスで接続を許可するユーザを登録します。

1. メニューバーの「接続設定」タブから「ユーザ設定」をクリックします。

2. 「ユーザ追加」をクリックします。

3. 追加可能ユーザには全体設定の認証タイプで選択したサーバからユーザ情報を取得し、表示します。
セキュアリモートアクセスで利用するユーザを追加可能ユーザから選択し、赤枠ボタンをクリックします。すべてのユーザを追加する場合は青枠ボタンを選択します。
対象ユーザが追加するユーザに移動したことを確認し、「設定」をクリックします。

4-2　デバイス設定

各ユーザが利用する端末を識別するため、デバイス名(任意の名前)を登録します。

1. メニューバーの「接続設定」タブから「デバイス設定」をクリックします。

2. 「デバイス追加」をクリックします。

3. デバイス追加の画面が表示さますので、次のページを参考に入力します。入力後、「設定」ボタンをクリックします。

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。 ※「無効」選択では、主にデバイス ID を使用した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でもご利用可能ではありますが、推奨しておりません。
デバイス認証方式	※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」」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

4. デバイス追加が完了するとデバイス設定一覧に表示されます。

後ほど設定する「デバイス割当」を行うと下記のように対象デバイス欄が黒文字に変更され、デバイス削除ができなくなります。割当解除することで対象デバイス頼が青文字に戻り、デバイス削除が行えます。

test_device_009	Windows	無効	-	-
test_device_01	Windows	無効	-	-
TEST_DEVICE_02	Mac	有効	MACアドレス	登録なし

4-3 デバイス割当

登録したユーザとデバイス名の紐付ける設定を行います。

1. メニューバーの「接続設定」から「デバイス割当」をクリックします。

2. 割り当てるユーザの「割当」ボタンをクリックします。

3. 「割当可能デバイス」から割り当てるデバイスを選択し、赤枠ボタンをクリックします。すべてのデバイスを割り当てる場合は、青枠ボタンをクリックします。
選択したデバイスが「割当デバイス」に移動したこと確認し、「適用」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。」と表示されたら設定完了です。

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。

4-4 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接続許可されているユーザへプロファイル送付を行い、リモート接続できるよう設定にします。

1. メニューバーの「接続設定」タブから「ユーザプロファイル設定」をクリックします。

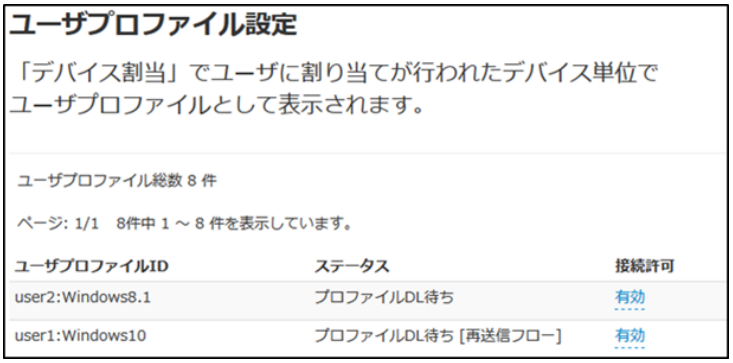
2. デバイス割当でユーザに割り当てが行われたデバイス単位でユーザプロファイルとして表示されます。通知対象ユーザのステータスが「メールを送信してください。」と表示されますので、「送信」をクリックします。

3. ユーザプロファイルダウンロード通知で送信する「メールアドレス」、「件名」、「URL 有効期限」、「ダウンロード回数」を入力し「送信する」をクリックします。

重要

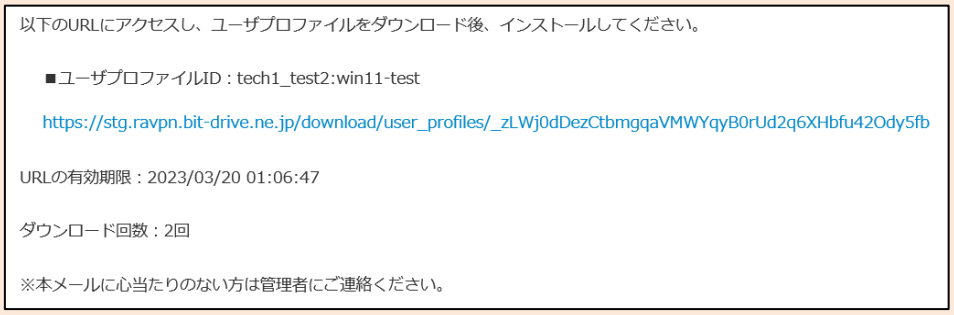
- プロファイルを送信するメールアドレスとメールの件名は任意のものに変更することができます。
- ユーザプロファイルのダウンロード URL の有効期限は『1～30 日』の間で設定できます。
- ダウンロード回数は『1～5、無制限』の内から設定できます。
- 有効期限、指定されたダウンロード回数を超えた場合、URL からダウンロードができなくなります。有効期限内にダウンロードできなかった場合は、再度ユーザプロファイルの送信を行ってください。

4. 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」に変更されます。



重要

- ユーザプロファイルの送付先には以下のようなメールが届きます。ご利用さまの端末で“Cisco AnyConnect”クライアントソフトをインストール後に、受信したメールの URL からプロファイルのダウンロードするよう依頼してください。
  “Cisco AnyConnect”クライアントソフトのインストール手順やプロファイルのインストール手順については別紙の「ユーザマニュアル」をご参照ください。



参考情報 - ステータス一覧

ユーザプロファイル設定画面のステータスではステータス情報が表示されます。

ステータス名	ステータス説明
デバイス ID 登録処理を行ってください。	• ユーザプロファイルダウンロード通知メール送信後、ユーザによってメール内の URL にアクセスしプロファイルがダウンロードされると、「プロファイル DL 待ち」から左記に表示が変更されます。 • Cisco AnyConnect に指定のユーザで初回ログインすることでデバイス ID 登録が自動で行われます。
URL の期限が切れました。再度メール送信してください。	• ユーザプロファイルダウンロード通知メール送信後、管理者によって送信時に設定された URL 有効期限期間内にユーザがメール内の URL にアクセスしなかった場合、「プロファイル DL 待ち」から左記に表示が変更されます。 • 再度ユーザプロファイルダウンロード通知メールを送信するなど対応を行ってください。
プロファイル DL 待ち [再送信フロー]	• ユーザプロファイルダウンロード通知メール送信後、指定した URL 有効期限内に URL にアクセスしなかった場合など再度通知メール送信が必要になった場合、再送信すると「プロファイル DL 待ち」から左記に表示が変更されます。 • 対象ユーザに最新のユーザプロファイルダウンロード通知メールの URL にアクセスを依頼してください。
接続準備完了	• ユーザプロファイルダウンロード通知メール送信後、ユーザによってメール内の URL にアクセスしプロファイルがダウンロードされ、Cisco AnyConnect に指定のユーザで初回ログインしデバイス ID が登録された場合、「プロファイル DL 待ち」から左記に表示が変更されます。 • VPN 接続が可能になります。

5 プロキシ設定

5-1 プロキシ利用設定

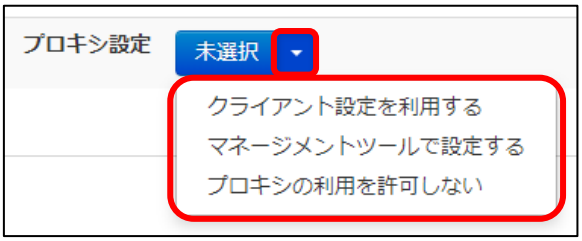
セキュアリモートアクセス利用時にプロキシサーバを利用する場合に以下の設定を行います。

1. メニューバーの「接続管理」タブから「プロキシ設定」をクリックします。

重要

- 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。

2. 初期設定ではプロキシ設定が「未選択」となっているため  をクリックし、お客さまのご利用環境に合わせたプロキシ設定を選択します。



- **「クライアント接続設定を利用する」を選択の場合**

  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設定が適用されます。

  下記の画面が表示されますので、「設定」をクリックしてください。

重要

- 設定後、プロキシ適用設定が必要になりますので「5-2 プロキシ適用」の手順を行ってください。

- **「マネージメントツールで設定する」を選択の場合**

  マネージメントツール上のプロキシ設定が適用されます。

  下図のプロキシ設定画面が表示されますので、プロキシサーバの「アドレス」、「ポート」、「プロキシ適用除外リスト」を入力し、「設定」をクリックします。

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

重要

- 設定後、プロキシ適用設定が必要になりますので「5-2 プロキシ適用」の手順を行ってください。

- **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適用させません。

5-2　プロキシ適用

「マネージメントツールで設定する」、「クライアント設定を利用する」を選択した場合、プロキシを適用させるプロファイルを選択します。

1. 適用プロファイルの「一覧表示／変更」をクリックします。

2. プロキシ設定画面が表示され、プロキシ設定の適用を個別のユーザプロファイルごとに設定を行うか、すべてのプロファイルに設定を行うかを黄色枠のプルダウンから選択します。
個別のプロファイルごとに設定する場合、設定するプロファイルを選択し、赤枠をクリックするとプロキシ適用プロファイルに移動します。
設定するプロファイルが移動したことを「設定」をクリックします。

重要

- プロキシ設定を「クライアント接続設定を利用する」と選択した場合、「プロキシ適用プロファイル」欄に対象プロファイルを適用させないとリモート接続ができなくなります。

3. プロキシ適用の完了後、メニューバーの「接続設定」タブから「デバイス設定」をクリックし、対象デバイスのプロキシ設定が「有効」になっていることを確認します。

接続許可	プロキシ設定	ローカルセグメント設定
有効	デバイス未割当	デバイス未割当
有効	有効	有効

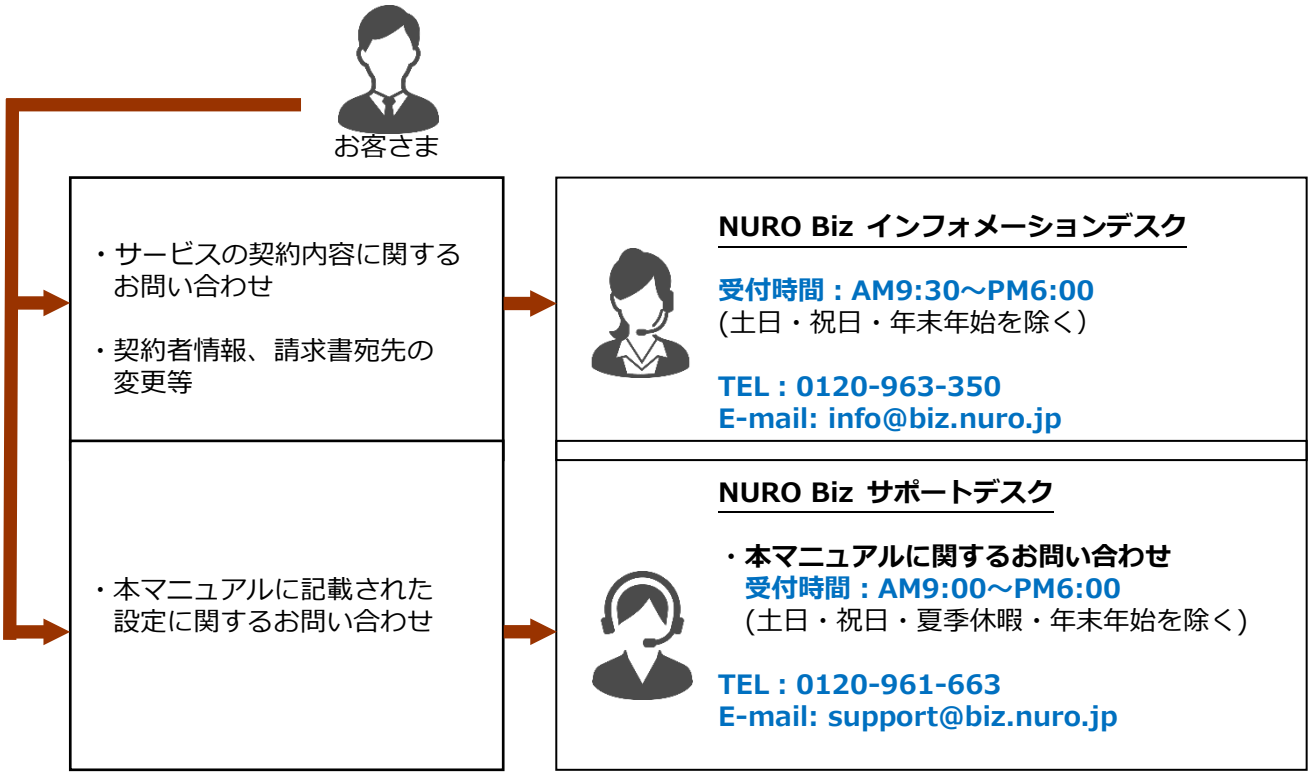
以上で「クイックガイド」の管理者さま設定は終了です。
リモート接続を行うには引き続きご利用者さまの端末設定が必要となりますので別紙の「ユーザマニュアル」をご参照ください。

6 サポート体制

6-1 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。



6-2 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。

6-3 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。

付録 – クイックガイド設定項目一覧

設定項目		説明	設定値、推奨値、ご準備頂きたいパラメータなど		メモ欄	ページ
ログイン		マネージメントツールにログインします。	登録内容通知に、マネジメントツールのURL、管理者ログイン名、初期パスワードが記載されています。 初回ログイン時には、初期パスワードを変更してください。			8
全体設定	認証タイプ	セキュアリモートアクセスで利用するユーザ認証を設定します。 お客さま所有のActive Directoryサーバを利用してユーザ認証する方法、お客さま所有のMicrosoft Entra IDサーバを利用してユーザ認証する方法の2つから選択します。	お客さま所有 Active Directoryサーバ ご利用の場合	設定には、Active Directoryサーバのホスト名、IPアドレス、Active　Directoryドメイン名、管理者パスワードが必要ですので、ご準備ください。	ホスト名： IPアドレス： ActiveDirectoryドメイン名： 管理者パスワード：	9
			お客さま所有 Microsoft Entra IDサーバ ご利用の場合	設定には、Microsoft Entra IDサーバのアプリケーションID、アプリケーションパスワード、ドメイン名、管理者ユーザ名、管理者パスワード、シークレット有効期限が必要ですので、ご準備ください。	アプリケーションID： アプリケーションパスワード： ドメイン名： 管理者ユーザ名： 管理者パスワード： シークレット有効期限：	
	デバイスIDの自動登録	端末認証に使用するクライアントのデバイスIDを、初回接続時に自動登録するかどうかを選択します。	例外を除き『有効』を推奨します。特殊端末利用時や、お客さまセキュリティポリシーなどにより、無効とすることも可能です。その際は、運用マニュアルを参照ください。			13
	通知メール宛先	デバイスID自動登録が失敗した際、メール通知するための管理者メールアドレスを登録します。	管理者メールアドレス(複数登録可)をご準備ください。		メールアドレス：	14
	DNSサーバ	クライアント接続時に端末へ配布するDNSサーバのIPアドレスを登録します。	DNSサーバのIPアドレス(プライマリ、セカンダリ)をご準備ください。		IPアドレス：	14
接続設定	ユーザ設定	セキュアリモートアクセスで接続を許可するユーザを登録します。	認証タイプで設定したサーバから、ユーザリストが取得できるので、許可するユーザを選択し登録します。 CSVファイルをインポートして、複数ユーザを同時に登録することも可能です。 その際は、運用マニュアルを参照ください。		接続を許可するユーザとデバイス名のリスト ユーザ　デバイス名①　デバイス名② 例 suzuki　Win-123　IOS-456	16
	デバイス設定	各ユーザが利用する端末を識別するため、デバイス名(任意の文字列)を登録します。	お客さまにてデバイス名を決めてください。本クイックガイドでは、デバイス名以外の設定項目は、推奨値で設定します。特殊ケースなどは運用マニュアルを参照ください。			17
	デバイス割当	ユーザ設定で登録したユーザとデバイス名を紐付ける設定です。	1ユーザに対し2端末(デバイス)まで登録可能です。 使用するユーザとデバイスが一致しないと接続できません。			20
	ユーザプロファイル設定	セキュアリモートアクセスへの接続を許可するためにデバイスと紐づいたユーザにプロファイルを送信します。	セキュアリモートアクセスを利用するユーザのメールアドレスをご準備ください。 メール内に添付されたURLには、管理者さまの設定によりアクセス制限（「URL有効期限」、「ダウンロード回数」）がございますので、ご注意ください。		メールアドレス：	21
接続管理	プロキシ設定	端末接続時に利用するプロキシを設定します。	①クライアントの設定を利用する、②マネジメントツールで設定する、③プロキシ利用を許可しない、の３つが選択可能ですので、お客さまポリシーなどに従い選択してください。 マネージメントツールから指定する場合には、プロキシサーバのIP、ポート番号、適用除外リストが必要となります。		マネージメントツールから指定する場合 IPアドレス： ポート番号： 適用除外リスト：	24