

InterSecVM/SG v4.2

SSL-VPN 設定手順書

目次

1. はじめに	2
1.1 本書について	2
1.2 用語説明	2
1.3 機能概要	3
1.4 クライアント環境要件	4
2. SSL-VPN 手順.....	5
2.1 設定から接続、切断までの流れ	5
2.2 SG の設定	6
2.2.1 SSL-VPN 設定.....	6
2.2.2 サーバー証明書の発行	7
2.2.3 ユーザーの登録(手動).....	8
2.2.4 ユーザーの登録(CSV)	9
2.2.5 補足) SSL-VPN 設定とユーザー登録について	11
2.2.6 クライアント証明書発行のための設定.....	12
2.2.7 サービスの起動.....	13
2.2.8 FW ルールの登録.....	13
2.3 クライアント証明書の発行および取得	14
2.4 サーバーの設定.....	16
2.5 クライアントの設定.....	17
2.6 接続/切断	18
3. 注意・制限事項.....	19

1. はじめに

1.1 本書について

本手順書は、InterSecVM/SG(以下 SG) シリーズの SSL-VPN の設定手順書です。

1.2 用語説明

本書で使用する用語を表 1.2-1 に示します。

表 1.2-1 用語説明

用語	説明
OpenVPN	OpenVPN Technologies, Inc. を中心に開発が行われているオープンソースの VPN (Virtual Private Network) ソフトウェア。 参考) https://www.openvpn.jp/

1.3 機能概要

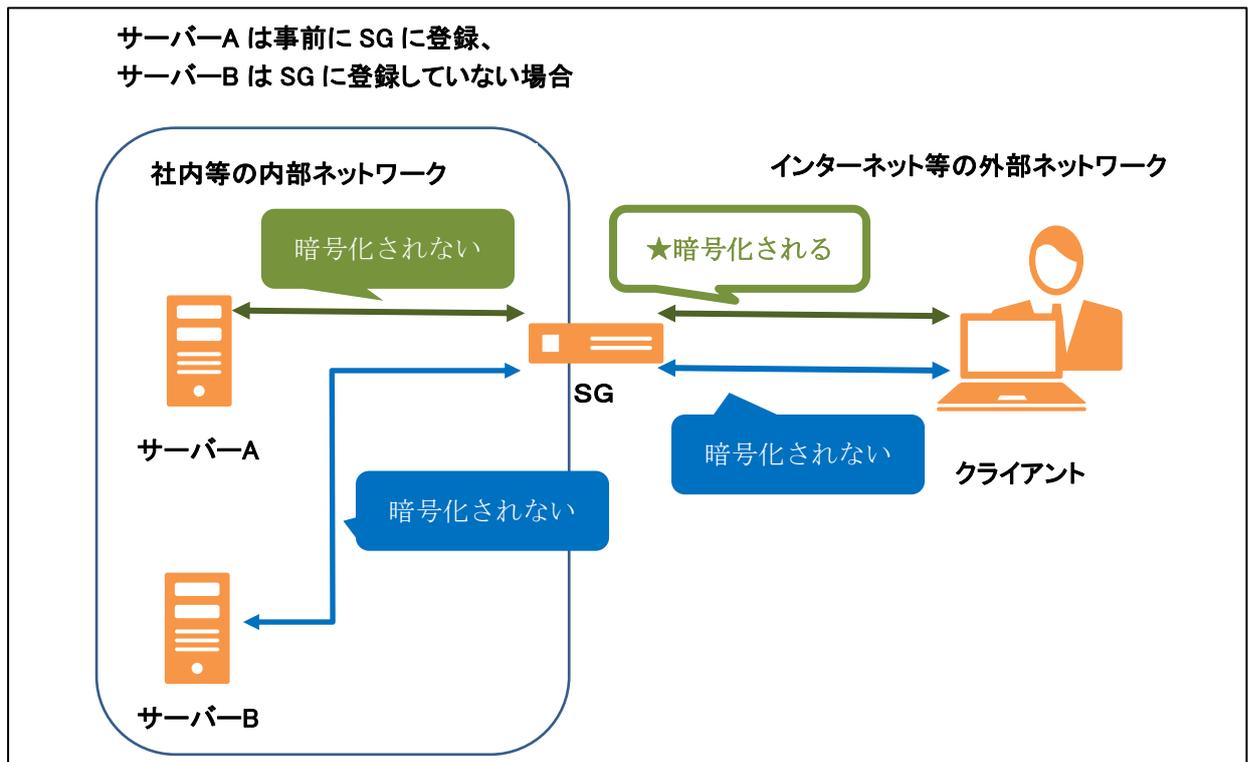
SGはオープンソースのOpenVPNを使用して、SSL-VPNを実現しております。
クライアントにもOpenVPNを導入いただくことにより、SSL-VPNが使用可能です。

本機能により、SGを経由してクライアントが「SGに事前に登録した特定のサーバー」と通信した場合に、クライアントとSG間が暗号化されます。なお、その先のSGと特定のサーバー間は暗号化されません。

事前に登録していないサーバーへの通信時はSGを経由しても暗号化されません。暗号化対象となる通信の種類は、webアクセス、FTP、メール等限定されず、すべての通信が対象となります。

なお下記機能は提供しておりません。

- ・LAN間接続
- ・クライアントとしてSGを使用すること
- ・不特定サーバーの指定
※サーバーは、「特定のサーバー以外のサーバー」といった指定はできません。
- ・インターネット上のサーバーとの通信の暗号化
※暗号化されるのはSGとクライアント間となるため、インターネット上の通信(SGとサーバー間の通信)は暗号化されません。



1.4 クライアント環境要件

OpenVPN が使用可能なものであれば、Windows、Android、iOS、Linux 等が使用可能です。
OpenVPN で使用可能な環境は、OpenVPN.jp のホームページを参照ください。

<https://www.openvpn.jp/>

OpenVPN がベースとなっています Windows 版の vpnux Client のご利用も可能です。

<http://www.vpnux.jp/>

下記の機種については SG と接続実績がございます。下記以外の OS の接続は、OpenVPN の保証の範囲内で可能ですが、導入前に、お客様にて事前評価を実施いただけますようお願いいたします。

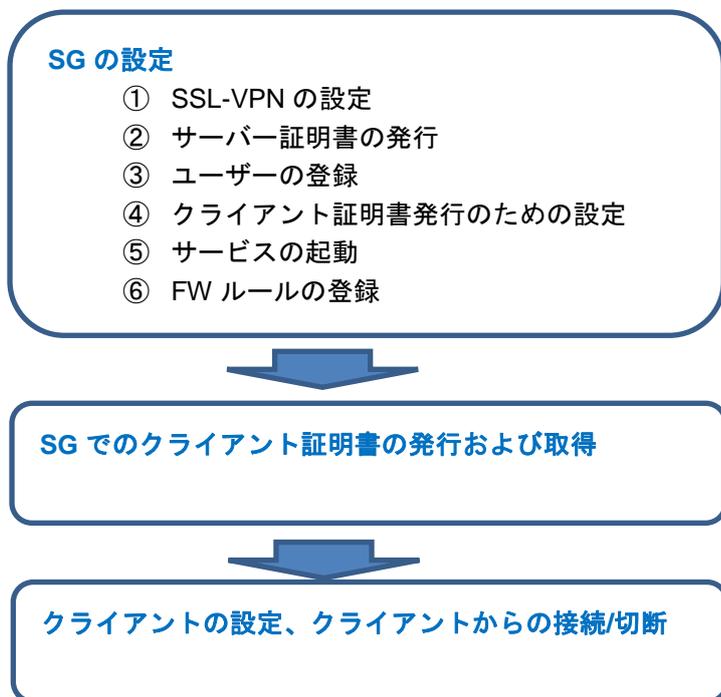
Linux(RHEL6 32bit)	OpenVPN 2.4.6-1
Linux(CentOS7 64bit)	OpenVPN 2.4.6-1 for CentOS7 x86_64
Andoird(v8.0.0)	OpenVPN Connected ver3.0.5
Windows(WS2016)	OpenVPN 2.4.6 I602、vpnux Client 1.4.6.2-2.4.3_01

検証時、SG に搭載している OpenVPN のバージョンは、「OpenVPN 2.4.6-1 for CentOS7 x86_64」となります。SG が提供する脆弱性対応のパッチを適用することにより、OpenVPN のバージョンが変更となる場合がございます。

2. SSL-VPN手順

2.1 設定から接続、切断までの流れ

手順の流れは下記となります。



2.2 SG の設定

2.2.1 SSL-VPN 設定

- ① 「サービス > SSL-VPN 機能」画面で「SSL-VPN 設定を追加」ボタンを押下、下記の「SSL-VPN 設定追加」画面を開きます。

SSL-VPN設定追加

サービス > SSL-VPN機能 > SSL-VPN設定追加 [\[戻る\]](#) [\[ヘルプ\]](#)

SSL-VPN設定

設定名:

SSL接続用ポート番号:

最大同時接続クライアント数:

SSL-VPN通信プロトコル:

仮想ネットワーク: /

公開セグメント: /

- ② SSL-VPN の設定を行い、「設定」ボタンを押下します。設定項目の説明は下記です。

項目	説明
設定名	任意の設定名を記載します。 最大で 128 バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)、ピリオド(.)が使用できます。全角文字（日本語）も使用できます。
SSL 接続用ポート番号	SSL 接続用ポート番号を指定します。 初期値は 1194 です。他の SSL-VPN 設定の SSL 接続用ポート番号と重複しないように設定してください。
最大同時接続クライアント数	同時に接続するクライアント数です。すべての SSL-VPN 設定で合計 100 名まで登録可能です。
SSL-VPN 通信プロトコル	SSL-VPN 接続時のプロトコルをプルダウンメニューから選択します。TCP もしくは UDP が使用できます。 このプロトコルは、SG とクライアント間の SSL-VPN のプロトコルであり、クライアントとサーバ間の通信のプロトコルではございません。 例えばここで UDP を選択し、クライアントとサーバ間が SMTP 通信を行った場合、SG とクライアント間の SSL-VPN 通信で、SMTP のパケットを UDP でカプセル化致します。 初期値は UDP です。特に変更の必要がなければ UDP のままご使用ください。
仮想ネットワーク	SSL-VPN 接続時に自動的に割り当てられる仮想ネットワークのアドレス及びネットマスクを設定します。SG とクライアントにすでに設定されている IP アドレス、他の SSL-VPN の設定で使用している本値とは重複しないような値としてください。またネットマスクは 16 ビット未満の指定はできません。
公開セグメント	クライアントに接続許可するサーバが属するネットワークのアドレスおよびネットマスクを設定します。

2.2.2 サーバー証明書の発行

- ① 「サービス > SSL-VPN 機能」画面で、「SSL サーバ証明書」ボタンを選択します。

- ② 「サービス > SSL-VPN 機能 > SSL サーバ証明書」画面で「自己署名形式の SSL サーバ証明書作成」ボタンを押下し、下記の「サーバ証明書作成」画面を開き、証明書の情報を入力し設定ボタンを押下しますとサーバー証明書が作成されます。

設定項目	説明
国コード	証明書に設定する国コードを入力してください。
都道府県名	証明書に設定する都道府県名を入力してください。
市区町村名	証明書に設定する市区町村名を入力してください。
会社名	証明書に設定する会社名を入力してください。
部門名	証明書に設定する部門名を入力してください。
サーバ名	証明書に設定するサーバ名を入力してください。

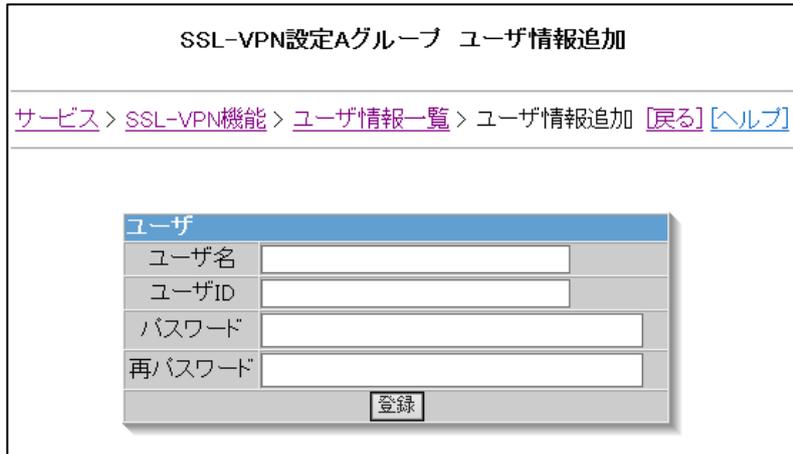
2.2.3 ユーザーの登録(手動)

ユーザーを1名単位で追加する方法です。後述の CSV での登録を利用すれば、最大 1000 人を1回で登録することができます。

- ① 「サービス > SSL-VPN 機能」画面で、ユーザーを登録したい SSL-VPN 設定の「登録ユーザー一覧」を選択します。



- ② 「サービス > SSL-VPN 機能 > ユーザ情報一覧」の「一覧の末尾にユーザ情報を追加」ボタンを押下し、下記の「ユーザ情報追加」画面を開きます。



- ③ ユーザーの設定を行い、「設定」ボタンを押下します。設定項目の説明は下記です。

設定項目	説明
ユーザ名	任意のユーザ名を指定します。最大で 128 バイト、二重引用符(")とカンマ(,)を含めることはできません。
ユーザ ID	任意のユーザ ID を指定します。最大で 15 バイトまでの小文字の英字、数字、ハイフン(-)、アンダースコア(_)を受け付けます。全ての SSL-VPN グループに登録しているユーザ ID の中で、一意である必要があります。
パスワード	ユーザがクライアント証明書を取得する際に SG にログインするためのパスワードを指定します。8 文字から 16 文字までで入力します。大文字小文字の英字、数字、ハイフン(-)、アンダースコア(_)を受け付けます。
再パスワード	上記と同じパスワードを再度入力します

2.2.4 ユーザーの登録(CSV)

CSV の登録では、1回で最大 1000 人のユーザーを登録できます。

CSV 登録を行った場合、クライアント証明書作成まで同時に行います。詳細は「2.3 クライアント証明書の発行および取得」を参照ください。

- ① 「サービス > SSL-VPN 機能」画面で、ユーザーを登録したい SSL-VPN 設定の「登録ユーザー一覧」を選択します。



- ② 「サービス > SSL-VPN 機能 > ユーザ情報一覧」の「CSV ファイルからユーザ情報を一括登録」ボタンを押下し、「一括登録」画面を開きます。
- ③ CSV ファイルを指定し「実行」ボタンを押下します。

CSV ファイルの形式は下記となります。すべて必須項目です。

カラム	項目	入力規則
1	ユーザ ID	任意のユーザ ID を指定します。最大で 15 バイトまでの小文字の英字、数字、ハイフン(-)、アンダースコア(_)を受け付けます。全ての SSL-VPN グループに登録しているユーザ ID の中で、一意である必要があります。
2	ユーザ名	任意のユーザ名を指定します。最大で 128 バイト、二重引用符(")とカンマ(,)を含めることはできません。二重引用符 (") を含めた場合は削除して登録します。
3	パスワード	ユーザがクライアント証明書を取得する際に SG にログインするためのパスワードを指定します。8 文字から 16 文字までで入力します。大文字小文字の英字、数字、ハイフン(-)、アンダースコア(_)を受け付けます。
4	パスフレーズ	秘密鍵のパスフレーズを指定します。最大で 12 バイトまでの、二重引用符 (")、一重引用符 (')、空白、円マーク("¥")を除く、ASCII 印刷可能文字を受け付けます。
5	有効期限	クライアント秘密鍵・証明書の有効期限を 1~2 桁の数字で指定します。単位は月数(1 か月=30 日)となります。最大は 99 です。0 とした場合は有効期限は 1 年となります。

入力例) sample.csv

```
userid, username, password,passphrase,12
```

(注意) SG が動作している環境の HW スペックによっては、CSV の登録時に、ブラウザのタイムアウト

表示や画面無反応、内部エラーが発生することがあります。

その場合は下記を実施ください。繰り返し本事象が発生する場合は、CSV の人数を減らして登録ください。

●タイムアウト表示や 5 分経過しても画面が無反応の場合

「サービス > SSL-VPN 機能 > ユーザ情報一覧」画面を再度表示し、ユーザー一覧の全件数（一覧左上表示）を確認。

-CSV に記載したユーザの数だけ追加された場合は正常に登録されているため作業は不要です。

-CSV に記載したユーザの数だけ追加されていない場合は、次の“登録結果に「(内部エラー)」と表示された場合” の手順を実施ください。

●登録結果に「(内部エラー)」と表示された場合

・本事象発生時に使用した CSV ファイルで一括削除を実施。

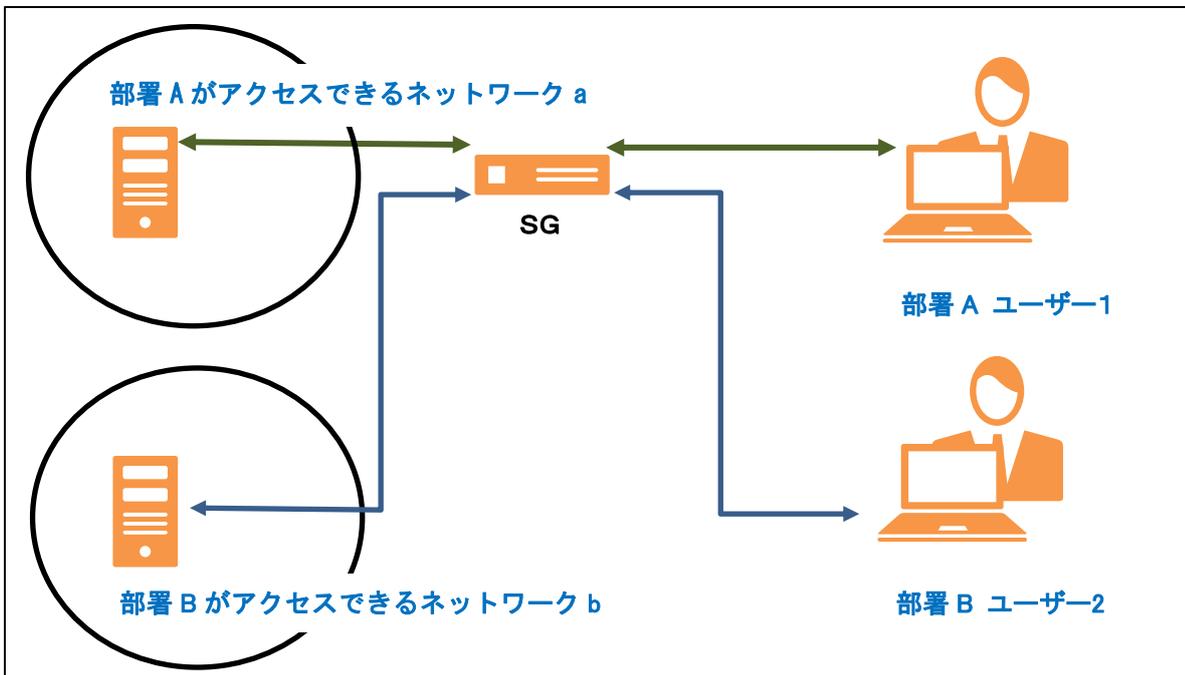
・再度一括登録を実施。

なお、内部エラー以外のエラーの発生時は、画面のエラー内容に従い CSV ファイルを修正し再度登録ください。前回正常に登録済みのユーザーは重複している旨表示されますが問題ございません。

2.2.5 補足) SSL-VPN 設定とユーザー登録について

SSL-VPN 設定とユーザー登録の設定例です。

例) 部署 A と部署 B でアクセスできるネットワークを分ける場合



下記のように設定します。

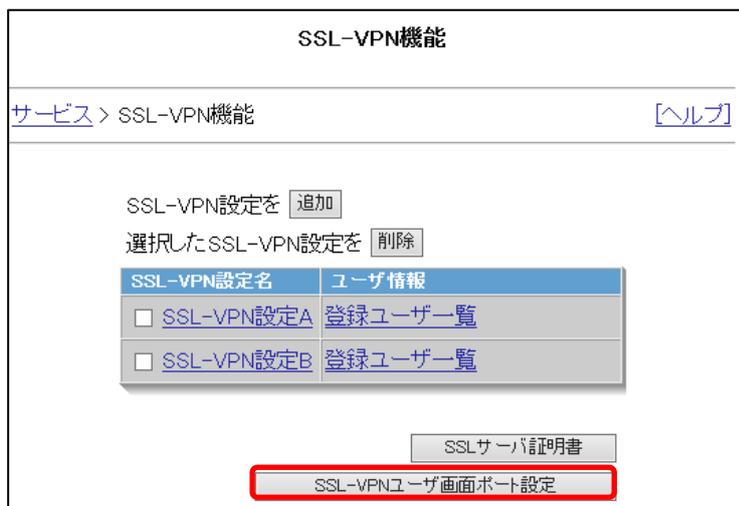
項目	部署 A	部署 B
設定名	SSL-VPN 設定 A	SSL-VPN 設定 B
SSL 接続用ポート番号	1194	1195 ※SSL-VPN 設定 A とは異なるポート番号を設定します。SG は接続されてきたポート番号をみて、どの SSL-VPN 設定か判断します。
仮想ネットワーク	192.168.201.0/24	192.168.202.0/24 ※SSL-VPN 設定 A とは異なるネットワークを指定します。また SG やクライアントが属しているネットワークと重複しないネットワークにする必要があります。
公開セグメント	192.168.11.0/24 ※ネットワーク a のアドレス	192.168.12.0/24 ※ネットワーク b のアドレス
ユーザー	ユーザー 1	ユーザー 2

また SSL-VPN 設定に関する各種設定の制限は下記です。

項目	最大値	補足
SSL-VPN 設定数	3	ユーザーを最大 3 グループにわけ、それぞれに公開セグメントを設定することができます。
1つの SSL-VPN 設定における公開セグメントの登録数	10	1 つの SSL-VPN 設定における公開セグメントの登録数は 10 となります。
ユーザー数	1 万人	SG に登録するユーザーは最大 1 万人となります。(例 SSL-VPN 設定 1 にユーザー 8000 人を登録している場合、SSL-VPN 設定 2 のユーザーは 2000 人まで登録可能となります。)
SSL の最大同時接続数	100 人	SG にて検証済みの最大同時接続数です。SG 全体の数となります。これを超えた場合にエラーにするなどの制限は設けておりません。

2.2.6 クライアント証明書発行のための設定

- ① 「サービス > SSL-VPN 機能」画面で、「SSL-VPN ユーザ画面ポート設定」を選択します。
 ※SSL サーバ証明書をまだ作成していない場合は本ボタンがグレーアウトされていますので、先にサーバ証明書の作成を行ってください。



- ② 「サービス > SSL-VPN 機能 > SSL-VPN ユーザ画面ポート設定」画面に、任意のポート番号を設定してください。

※初期値は 18443 となります。また、SG に設定している他のポート番号と重複はできません。

※このポート番号は、クライアント証明書の発行および、取得時に使用します。

2.2.7 サービスの起動

※注意：SSL-VPN の設定を変更した場合は、SSL-VPN サービスの再起動を行ってください。

- ① 「サービス」画面の、SSL-VPN 機能の「起動」ボタンを選択します。



- ② OS 起動時状態について、必要に応じて本画面にて「OS 起動時の状態」を変更ください。

2.2.8 FW ルールの登録

- ① 「ファイアウォール > 詳細設定 > ルール設定 (サイト共通)」画面で下記のルールを登録します。
FW ルールの追加方法の詳細につきましては、画面のヘルプを参照ください。

●クライアント証明書取得のアクセス許可

処理 : 許可

発信元 : 任意、もしくは、アクセスを制限したい場合は、アクセス許可を行うクライアントの IP アドレスかネットワークを指定。

宛先 : ファイアウォール自身

通信種別 : 例) tcp/18443

tcp は固定。

“2.2.6 クライアント証明書発行のための設定”で設定したポート番号を指定。

記録、コメント : 必要に応じて設定ください。

●SSL-VPN 接続のアクセス許可

処理 : 許可

発信元 : 任意、もしくは、アクセスを制限したい場合は、アクセス許可を行うクライアントの IP アドレスかネットワークを指定。

宛先 : ファイアウォール自身

通信種別 : 例) udp/1194

“2.2.1 SSL-VPN 設定”で設定した“SSL-VPN 通信プロトコル”、および

“2.2.1 SSL-VPN 設定”で設定した“SSL 接続用ポート番号”を指定。

記録、コメント : 必要に応じて設定ください。

※クライアントの公開セグメントに対するアクセス許可の登録は不要です。

- ② 「ファイアウォール > 詳細設定 > ルール設定」画面で「編集結果を適用ボタン」を適用します。

2.3 クライアント証明書の発行および取得

下記の手順でクライアント証明書を取得ください。

- ① 別の PC より、ブラウザで下記にアクセスします。

https://[SG のアドレス]:[ポート番号(※1)]

例) https://192.168.1.1:18443

(※1) 「2.2.6 クライアント証明書発行のための設定」で「SSL-VPN ユーザ画面ポート設定」で設定した設定したポート番号

※本画面は http でのアクセスは不可で https 固定となります。

※SSL-VPN のサービスが起動していない場合はアクセスできませんのでサービスを起動ください。サービスの起動方法は、「2.2.7 サービスの起動」を参照ください。

- ② ユーザー登録時に指定したユーザーID、パスワードでログインします。
- ③ 下記画面が表示されましたらパスワードの再設定を行ってください。

パスワード変更	
パスワード	<input type="password"/>
再パスワード	<input type="password"/>
<input type="button" value="更新"/>	

- ④ 下記の画面の「クライアント証明書一覧」ボタンを選択します。

ユーザー情報	
ユーザー情報	
ssl1セグメントの下記ユーザへのログインに成功しました。	
ユーザーID	usr1
<input type="button" value="ログアウト"/> <input type="button" value="パスワード変更"/> <input type="button" value="クライアント証明書一覧"/>	

- ⑤ 下記の画面の「自己署名形式のクライアント証明書作成」ボタンを選択します。なお、CSVでユーザー登録をされている場合、すでに証明書が作成されています。証明書の再作成が不要でしたら、⑦から実施ください。

クライアント証明書一覧

[ユーザ情報](#) > クライアント証明書一覧

クライアント証明書一覧

クライアント証明書 :

登録されていません

- ⑥ 各項目に入力し設定ボタンを押下しますと、クライアント証明書が作成されます。

クライアント証明書作成

[ユーザ情報](#) > [クライアント証明書一覧](#) > クライアント証明書作成 [\[戻る\]](#)

クライアント証明書作成

パスフレーズ :

パスフレーズ (再入力) :

有効期限 (月) :

※一ヶ月30日で有効期限を計算します。

設定項目	説明
パスフレーズ	秘密鍵のパスフレーズを指定します。 二重引用符 ("), 改行コード、半角カタカナを除く、1~12文字の任意の文字列で指定します。
パスフレーズ(再入力)	上記と同じパスフレーズを再度入力します。
有効期限(月)	クライアント秘密鍵・証明書の有効期限を1~2桁の数字で指定します。 単位は月数(1か月=30日)となります。最大は99です。

- ⑦ 下記の画面の実行ボタンを選択し、証明書のダウンロードを行います。

クライアント証明書一覧

[ユーザ情報](#) > クライアント証明書一覧

クライアント証明書一覧

クライアント証明書 :

ダウンロード	ファイル名	発行日	有効期限
<input style="border: 2px solid red;" type="button" value="実行"/>	GROUP0_usr1-20180518220254	2018/05/18 22:02:54 JST	2026/07/05 22:02:54 JST

2.4 サーバーの設定

公開セグメントのサーバーの設定は随時お客様の環境に応じて見直してください。

(例) FW 設定、静的ルーティング等)

なお、クライアント宛での静的ルーティングを設定する場合、クライアントの IP アドレスは、“2.2.1 SSL-VPN 設定”で設定した“仮想ネットワーク”のアドレスとなります。

公開セグメントのサーバーに関する不明点は、公開セグメントのサーバーの管理者にお問い合わせをお願いいたします。

2.5 クライアントの設定

下記にクライアントの設定例を記載いたします。

クライアント製品によって、画面構成、パラメータ名等異なりますので設定方法については各製品のホームページやドキュメント等を参照ください。

なお、クライアントの公開セグメント宛てのルーティングの設定は不要です。公開セグメント宛てのルーティング設定は、SSL-VPN 接続時に自動的に行われます。

例) 「vpnuix Client」の場合

The screenshot shows the 'vpnuix Client' configuration window titled 'プロファイルの編集'. It is divided into '一般設定' (General Settings) and '詳細設定' (Detailed Settings).

一般設定 (General Settings):

- プロファイル名: []
- VPNサーバー: []
- ポート: 1194
- デバイス: TAP TUN
- プロトコル: UDP (推奨) TCP
- 拡張設定:
 - LZO圧縮を有効にする
 - mssfixの値を下げる (不安定な回線の場合)
 - サーバー側のアドレス変更を許容する
- 拡張機能:
 - ID/パスワード認証拡張機能を使用

詳細設定 (Detailed Settings):

- 認証:
 - CA証明書: 未設定
 - ID/パスワード認証を使用
 - 証明書認証 (PKI) を使用
- ID/パスワード認証:
 - ユーザーID: []
 - パスワード: []
 - ユーザーIDとパスワードを保存
- 証明書認証 (PKI):
 - 証明書: 未設定
 - 秘密鍵: 未設定
 - パスワード: []
 - 秘密鍵/パスワードを保存

Buttons: 保存 (Save), 閉じる (Close)

SG と接続時に設定いただく内容は下記です。下記以外は、必要に応じて入力ください。

設定項目	説明
VPN サーバー	SG の IP アドレス、もしくは FQDN を入力します。
ポート	“2.2.1 SSL-VPN 設定 “で設定した “SSL 接続用ポート番号” を入力します。
デバイス	“TUN “を選択します。
プロトコル	“2.2.1 SSL-VPN 設定 “で設定した “SSL-VPN 通信プロトコル” を入力します。
LZO 圧縮を有効にする	オフ (有効にしない) にします。
CA 証明書	“2.3 クライアント証明書の発行および取得” でダウンロードしたクライアント証明書を解凍後、中にはいていた ca.crt ファイル” を指定します。
証明書認証(PKI)を使用	オン (使用する) にします。
証明書	“2.3 クライアント証明書の発行および取得” でダウンロードしたクライアント証明書を解凍後、中にはいていた “GROUPxxxxx.crt ファイル(xxxx はランダム)” を指定します。
秘密鍵	“2.3 クライアント証明書の発行および取得” でダウンロードしたクライアント証明書を解凍後、中にはいていた “GROUPxxxxx key ファイル(xxxx はランダム)” を指定します。
パスワード	“2.3 クライアント証明書の発行および取得” でクライアント証明書作成時に指定した “パスフレーズ “を入力します。

2.6 接続/切断

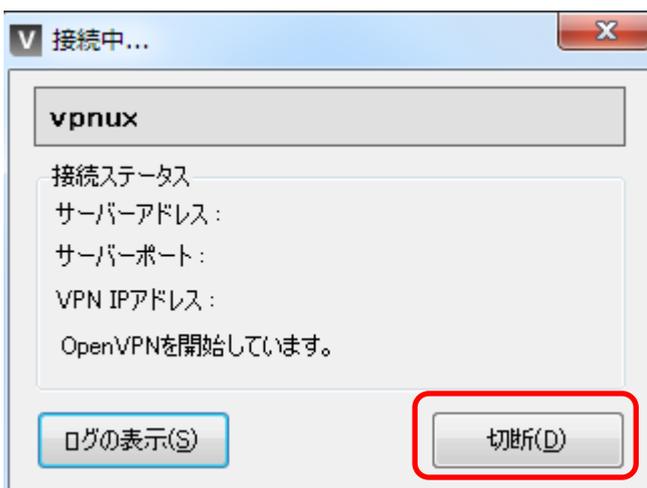
SSL-VPN の接続/切断はクライアントから実施します。SG から SSL-VPN の接続、切断を行うことはできません。下記にクライアントの操作例を記載しますが、詳細は各製品のホームページやドキュメント等を参照ください。

例) 「vpnuX Client」の場合

- 接続時：必要なパラメータを記載し、接続ボタンを押下します。



- 切断時：切断ボタンを押下します。



3. 注意・制限事項

- ・SGに搭載するOpenVPNは、使用するバージョンやクライアントのOS種別によって、接続性や機能が異なる場合がございます(※)。SGのSSL-VPN機能は、OpenVPNの動作に準拠します。

※クライアントのOSがAndroidの場合とLinuxの場合で、通信タイムアウト時の動作が異なる事例が確認されております。

以上