取扱説明書（操作用）

セキュリティゲートウェイ　SG6 シリーズ

形式 **SG6-N**

目次

1. はじめに

このたびは、弊社の製品をお買い上げいただき誠にありがとうございます。
SG6 をご使用いただく前に、下記事項をご確認ください。

1.1 ご使用いただく前に

1.1.1 取扱説明書の対応バージョン

本取扱説明書の対応バージョンは以下のとおりです。

●本体バージョンについて

- 本取扱説明書は、形式:SG6-N 本体バージョン 1.0 以降に対応しています。
- 本体バージョンの確認方法については、「4.1 メンテナンス」を参照してください。
- 変更内容については、「5.3 変更履歴」を参照してください。

1.1.2 注意事項

1. 機器使用について

●取扱いについて

- 本体の取外または取付を行う場合は、危険防止のため必ず、電源を遮断してください。
- 製品に外力を加えないでください。
- 製品をシンナーなどの有機溶剤で拭かないでください。

●設置について

- 屋内でご使用ください。
- 塵埃、金属粉などの多いところでは、使用しないでください。
- 振動、衝撃は故障の原因となることがあるため極力避けてください。
- 周囲温度が 0 ～ 40℃を超えるような場所、周囲湿度が 10 ～ 90 % RH を超えるような場所や結露するような場所でのご使用は、寿命・動作に影響しますので避けてください。
- 清浄な雰囲気中に設置してください。シンナー、アセトン、ホルマリン、亜硫酸ガスなど、有機性ガス雰囲気中での長時間の使用は避けてください。
- 直射日光が当たる場所には絶対に放置しないでください。

●配線について

- 配線は、ノイズ発生源(リレー駆動線、高周波ラインなど)の近くに設置しないでください。
- ノイズが重畳している配線と共に結束したり、同一ダクト内に収納することは避けてください。

●その他

- 本器は電源投入と同時に動作しますが、すべての性能を満足するには 10 分の通電が必要です。

2. 電波について（無線 LAN タイプ J のみ）

●日本国外での使用に関する注意事項

・ 国内電波法認証取得済みです。日本国内でのみ使用できます。海外の電波法認証の予定については、弊社ホットラインまでお問合せください。

●技適マークについて

・ 本器は電波法における小電力データ通信システムの無線局設備で無線免許の必要はありません。
・ 本器に技適マークが表示されていますが、電波法認証は内蔵の無線モジュールで取得しています。無線モジュールにも技適マークが貼付されています。

●分解改造について

・ 本器を分解、改造しないでください。

●無線 LAN 2.4 GHz 帯に関する注意事項

・ 本器の使用周波数（2.4 GHz）帯では、電子レンジ等の産業・科学・医療用機器のほか、工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）および特定小電力無線局（免許を要しない無線局）、ならびにアマチュア無線局（免許を要する無線局）が運用されています。

1. 本器を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局ならびにアマチュア無線局が運用されていないことを確認してください。
2. 万一、本器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止した上、弊社ホットラインまでご連絡いただき、混信回避のための処置等（例えばパーティションの設置など）についてご相談ください。
3. その他、本器から移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して有害な電波干渉の事例が発生した場合など何かお困りのことが起きたときは、弊社ホットラインまでお問合せください。

●無線 LAN 5 GHz 帯に関する注意事項

・ 本器の IEEE802.11a と IEEE802.11n のチャネルは以下のチャネルに対応しています。
W52（5.2 GHz 帯 36、40、44、48 ch）、W53（5.3 GHz 帯 52、56、60、64 ch）、
W56（5.6 GHz 帯 100、104、108、112、116、120、124、128、132、136、140 ch）
なお、34、38、42、46ch（J52）を使用するアクセスポイントとは通信できません。
・ W53、W56 を使用する場合、アクセスポイントには法令により次のような制限があります。
各チャネルの通信開始前に、1 分間レーダ波を検出します。その間は通信できません。
通信中にレーダ波を検出した場合、自動的にチャネルを変更します。その間は通信が中断されることがあります。
5.2 ／ 5.3 GHz 帯（W52 ／ W53）は電波法により屋外使用が禁止されています。

●DFS 機能について

・ DFS 対応の W53、W56 チャネルに設定時は、気象レーダ波を検出した場合、電波干渉を避けるために、チャネルを変更する必要がありますので注意してください。
・ 起動後 1 分間、当該チャネルにレーダ波がないかの確認を行うため、少なくとも 1 分以上の時間が必要となります。
・ 起動時もしくは起動中にレーダ波が検出された場合、設定チャネルとは別のチャネルを使用しなければならないため、別のチャネルで起動する場合があります。
・ 設定 DFS 対応チャネルで起動後も、運用中にチャネルを変更する場合があります。

・ レーダ波を検出した場合、検出後 30 分間電波を停止する必要があるため、30 分間は検出チャネルを使用できません。

●IEEE802.11n の 40 MHz システムについて

・ 40 MHz システムの使用設定を ON にする場合には、周囲の電波状況を確認して他の無線局に電波干渉を与えないことを事前に確認してください。
・ 万一、他の無線局において電波干渉が発生した場合には、すぐに 40 MHz システムの使用設定を OFF にしてください。

●セキュリティに関する注意事項

・ 本器は有線 LAN ケーブルの代わりに、無線 LAN で通信するため、通信内容を盗み見られたり、不正侵入の問題が発生する可能性があります。セキュリティ設定を行うことによって、問題が発生する可能性を少なくすることができます。セキュリティの設定を行わないで使用した場合の問題点を十分理解した上で、お客様の判断と責任でセキュリティ設定を行ってください。

1.1.3 関連機器

●ローカル認証局作成支援ソフトウェア（形式：LCA-SG）

ソフトウェアは、弊社のホームページよりダウンロードが可能です。

2. 仕様

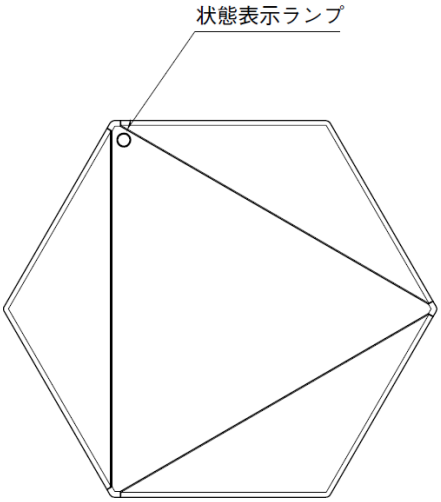
2.1 一般仕様

項　目	内　容
ネットワーク設定	本体 IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS アドレス
無線機能*	「5.2.5 無線 LAN」を参照ください
搭載プロトコル	IP、TCP、ICMP、TLS、DNS(Client)、SNTP(Client)、DHCP(Server)、HTTP
動作モード	標準／逆接続 「2.4 動作仕様」を参照ください。
標準モード	クライアント、サーバ
逆接続モード	クライアント／サーバ
受付ポート数 （標準モード）	クライアント:1／2／4／8 サーバ:1／2／4／8
接続数 （標準モード）	受付ポート数 1 の場合:1 受付ポート当たり 64 受付ポート数 2 の場合:1 受付ポート当たり 32 受付ポート数 4 の場合:1 受付ポート当たり 16 受付ポート数 8 の場合:1 受付ポート当たり 8
受付ポート数 （逆接続モード）	クライアント:　8 サーバ:8
接続数 （逆接続モード）	1 受付ポート当たり 8
暗号通信	TLS1.2
暗号スイート	TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
証明書	X.509v3
状態表示ランプ	緑／赤／黄
時刻	SNTP 自動時刻修正、手動時刻修正
コネクション監視	キープアライブ、送信タイムアウト

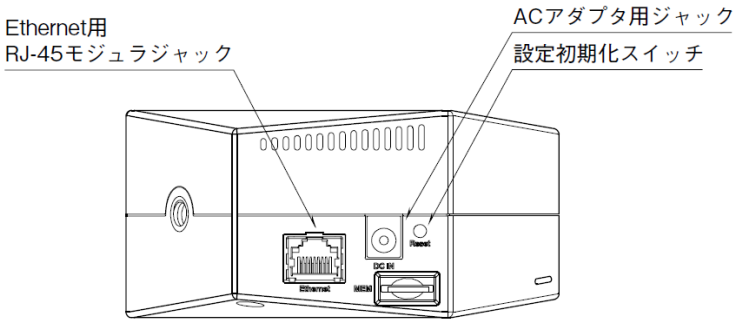
*無線 LAN タイプ J のみ

2.2 各部の名称

■前面図



■側面図



●状態表示ランプ

表示色	状　態	動　作
緑色	点灯	供給電源 ON／動作中
	点滅	設定変更に伴う再起動待ち
黄色	点灯	本体起動中
	点滅	ファームウェアアップデート中／設定値初期化中
赤色	点灯	設定異常／起動時 SNTP 失敗／EEPROM 故障時
—	消灯	電源 OFF／機器異常

●設定初期化スイッチ

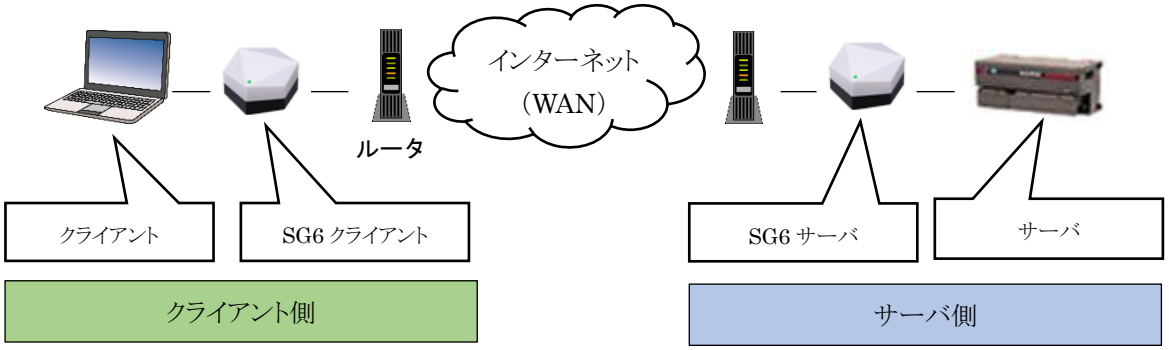
3 秒以上長押しすることで、SG6 の証明書を削除し設定を初期化することができます。設定初期化後は、自動で再起動します。

2.3 導入仕様

SG6 では、クライアント側に設置されるものを「SG6 クライアント」、サーバ側に設置されるものを「SG6 サーバ」と呼びます。1 台の SG6 は「SG6 クライアント」と「SG6 サーバ」の両機能を内蔵しているため、逆方向での同時使用も可能です。

下図に、その概要を示します。ここでは、SG6 はルータと機器との間に設置されていますが、これは論理上の接続を表したもので、物理的には SG6 と機器は並列にルータに接続されます。

システム構築には、基本的に 2 台以上の SG6 が必要となります。また、クライアント側およびサーバ側の LAN 環境内に SG6 を設置する必要があります。このため、物理的な場所を特定できないクラウドサーバ等との通信には、使用できません。



2.3.1 導入前

TCP/IP 準拠の産業用通信プロトコル(例. Modbus/TCP)は多数存在し、これら通信プロトコルに対応した機器(例. R7E)も同様です。Modbus/TCP は、認証や通信暗号化の仕組みを備えていません。よって、R7E のような機器を直接インターネット(WAN)に接続すると、セキュリティ面において大きな問題が発生します。

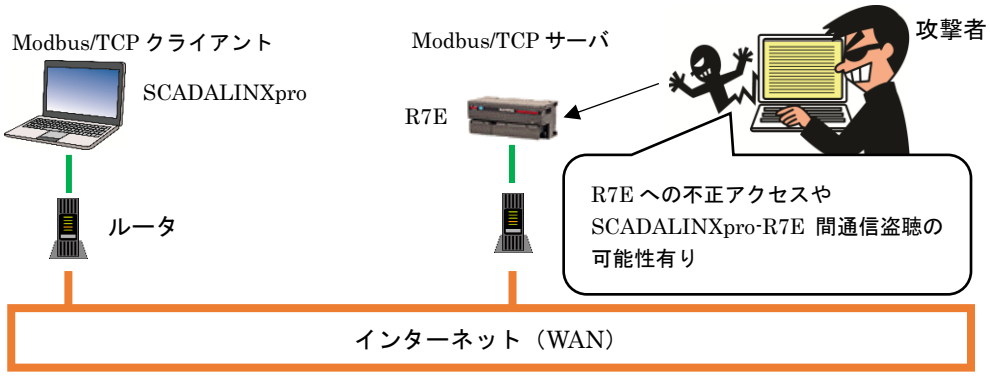


図 Modbus/TCP 機器の WAN 接続例(直接)

上図は、SCADALINXpro から R7E に WAN 経由でアクセスし、遠隔監視／操作を行う場合の接続例です。この場合は、SCADALINXpro がクライアント、R7E がサーバとなります。R7E は SCADALINXpro からの接続を待ちますが、Modbus/TCP には認証の仕組みがないため、攻撃者からの接続をも許可してしまいます。このため、攻撃者に R7E の入力値を読まれる、出力値を操作されてしまうといった、なりすましのリスクが発生します。さらに、SCADALINXpro－R7E 間の通信は暗号化されていないため、これを盗聴・改ざんされてしまう恐れもあります。

2.3.2 導入後

SG6 を用いると、TCP/IP 準拠の産業用通信プロトコル（Modbus/TCP など）を TLS 対応させることができます。
よって、インターネットを経由したセキュアな通信が可能になります。

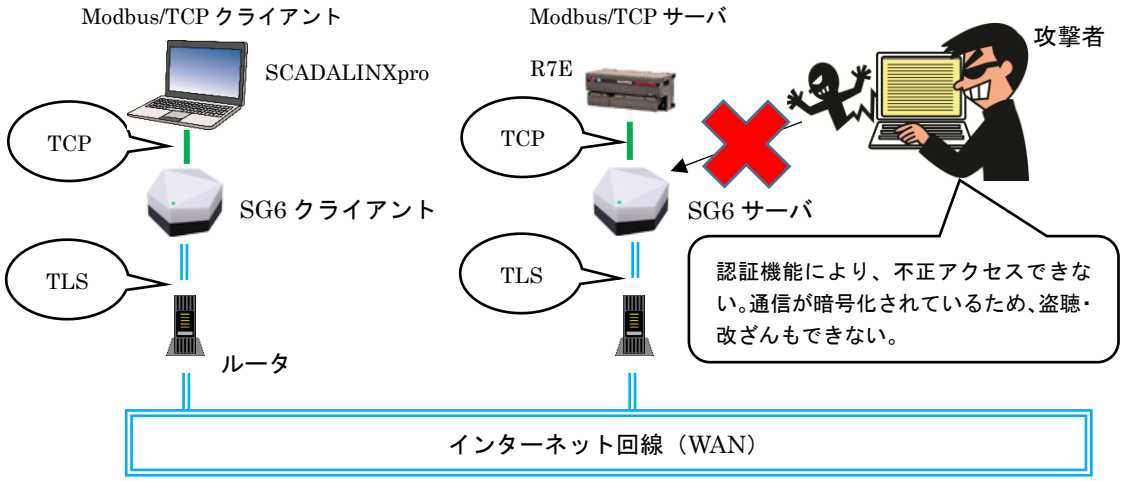


図 Modbus/TCP 機器の WAN 接続例（SG6 経由）

上図に、SG6 を用いた場合の接続例を示します。
この場合、直接インターネットに接続されるのは、SG6 クライアントおよび SG6 サーバになります。したがって、攻撃者による攻撃対象もこれらに限定され、SCADALINXpro や R7E への直接攻撃は不可能となります。

SG6 クライアント～SG6 サーバ間の接続は、TLS の相互認証により行われます。これは双方が保持する電子証明書を交換するもので、ログイン／パスワード認証よりも安全とされている方式です。これにより、認証した相手からの接続を許可しつつ、攻撃者によるなりすまし接続を拒否できます。さらには、TLS の暗号化により、盗聴・改ざんのリスクからも解放されます。

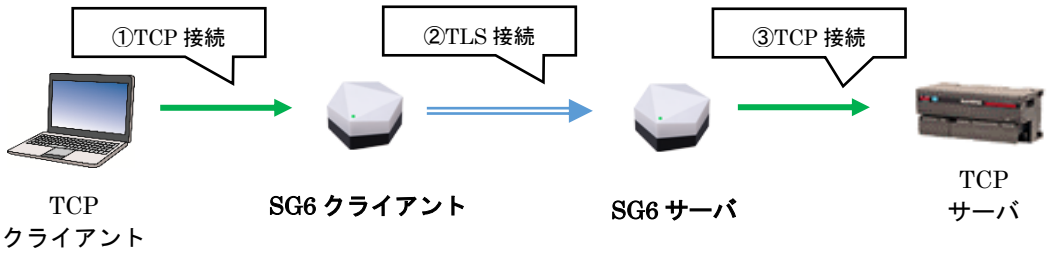
結果、回線や装置はそのままで、WAN を経由した安全な通信を実現できるようになります。

2.4 動作仕様

2.4.1 標準モード

1. 接続

TCP クライアントが、SG6 経由で TCP サーバに接続する場合の手順を下図に示します



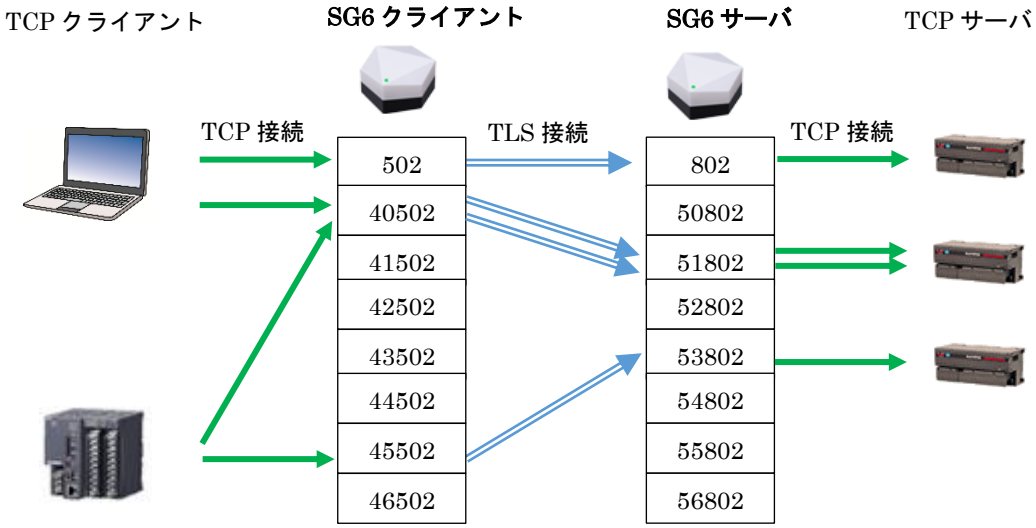
処理	内 容
①	TCP クライアントは、SG6 クライアントに TCP 接続します。両者は LAN 接続されているため、接続先はローカル IP アドレスとなります。
②	①の接続を受けて、SG6 クライアントは SG6 サーバに TLS 接続します。この接続は、インターネットを経由した WAN 環境下で行われます。したがって、SG6 サーバを固定グローバル IP アドレスもしくはダイナミック DNS により、外部から特定可能としておく必要があります。
③	②の接続を受けて、SG6 サーバは TCP サーバに TCP 接続します。両者は LAN 接続されているため、接続先はローカル IP アドレスとなります。

SG6 クライアントは、最大 8 つの受付ポートを使用して TCP クライアントからの TCP 接続を待つことができます。TCP 接続数は合計で 64 のため、これを使用する受付ポート数(1／2／4／8)で割った数が 1 受付ポート当たりの最大接続数になります。各受付ポートには、対応する SG6 サーバのグローバルアドレスを設定します。

SG6 サーバは、最大 8 つの受付ポートを使用して SG6 クライアントからの TLS 接続を待つことができます。TLS 接続数は合計で 64 のため、これを使用する受付ポート数(1／2／4／8)で割った数が 1 受付ポート当たりの最大接続数になります。各受付ポートには、対応する TCP サーバのローカルアドレスを設定します。

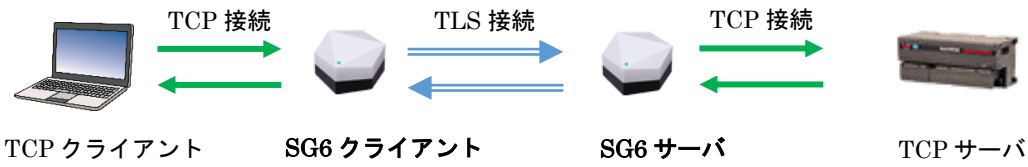
複数台の SG6 導入による、N 対 N のセキュア通信も可能です。さらに、1 台の SG6 にはクライアント機能とサーバ機能が共存しているため、逆方向からも接続できます。

次ページに、受付ポートの設定例を示します。



2. 転送

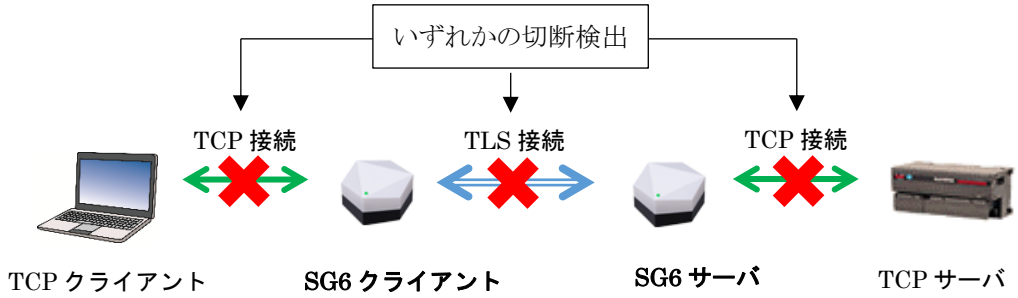
接続後は、TCP 通信の内容には関与せず、TCP 接続と TLS 接続間での転送をおこないます。



機　能	動　作
SG6 クライアント	・TCP クライアントから受信したデータを TLS 接続したサーバに送信します ・TLS 接続したサーバから受信したデータを、TCP クライアントに送信します。
SG6 サーバ	・TLS 接続したクライアントから受信したデータを TCP サーバに送信します ・TCP サーバから受信したデータを、TLS 接続したクライアントに送信します。

3. 切断

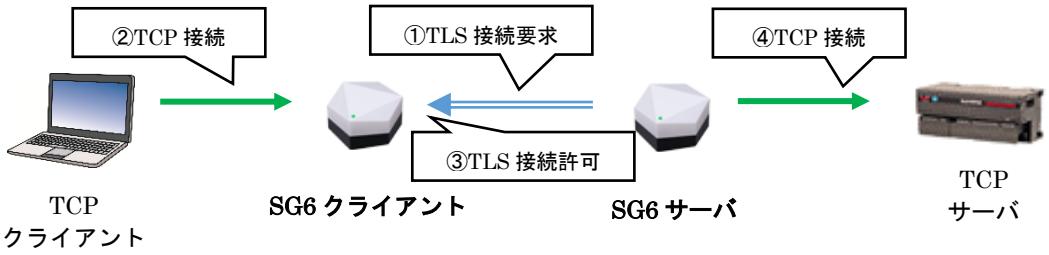
SG6 クライアントおよび SG6 サーバは、TLS もしくは TCP の一方の切断を検出時に、もう片方の接続も切断します。



2.4.2 逆接続モード

1. 接続

TCP クライアントが、SG6 経由で TCP サーバに接続する場合の手順を下図に示します。



処理	内 容
①	SG6 サーバは、装置起動直後から SG6 クライアントへの TLS 接続を試みます。この時点では、まだ SG6 クライアントはこの接続要求を受け付けません。この接続要求は、インターネットを経由した WAN 環境下で行われます。したがって、SG6 クライアントを固定グローバル IP アドレスもしくはダイナミック DNS により、外部から特定可能としておく必要があります。
②	TCP クライアントは、SG6 クライアントに TCP 接続します。両者は LAN 接続されているため、接続先はローカル IP アドレスとなります。
③	②の接続を受けて、SG6 クライアントは SG6 サーバからの TLS 接続要求を受け付けます。
④	③の接続を受けて、SG6 サーバは TCP サーバに TCP 接続します。両者は LAN 接続されているため、接続先はローカル IP アドレスとなります。

SG6 クライアントは、最大 8 つの受付ポートを使用して SG6 サーバからの TLS 接続を待つことができます。1 受付ポート当たりの TLS 最大接続数は、8 です。

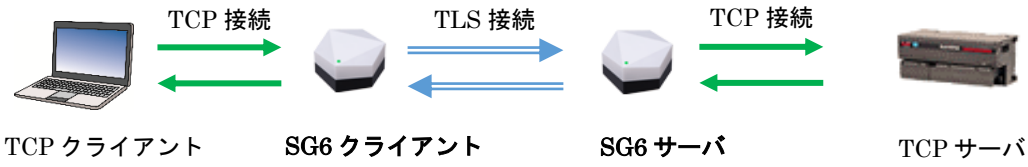
さらに、SG6 クライアントは、最大 8 つの受付ポートを使用して TCP クライアントからの TCP 接続を待つことができます。1 受付ポート当たりの TCP 最大接続数は、8 です。
SG6 クライアントは、1 つの TCP 接続検知時に 1 つの TLS 接続を受け入れ、これらをペアリングしデータ転送状態に移行します。TCP 接続検知後 10 秒以内に TLS 接続できない場合は、TCP 接続を切断します。

SG6 サーバは、装置起動直後からあらかじめ設定された SG6 クライアントへの TLS 接続を試みます。同受付ポートへの TLS 接続数は、8 です。
この 8 接続のうちの 1 つが接続成功すると、あらかじめ設定された TCP サーバに TCP 接続してこれらをペアリングし、データ転送状態に移行します。TLS 接続検知後 10 秒以内に TCP 接続できない場合は、TLS 接続を切断します。

逆接続モードでは、1 台の SG6 でクライアント機能またはサーバ機能のどちらか一方のみが動作可能です。

2. 転送

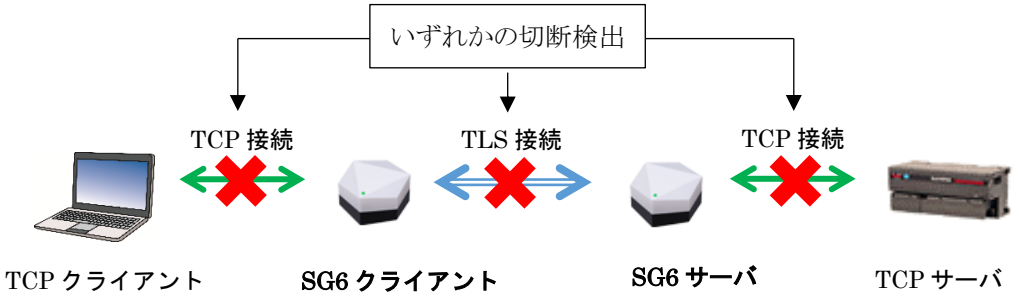
接続後は、TCP 通信の内容には関与せず、TCP 接続と TLS 接続間での転送をおこないます。



機　能	動　作
SG6 クライアント	・TCP クライアントから受信したデータを TLS 接続したサーバに送信します ・TLS 接続したサーバから受信したデータを、TCP クライアントに送信します。
SG6 サーバ	・TLS 接続したクライアントから受信したデータを TCP サーバに送信します ・TCP サーバから受信したデータを、TLS 接続したクライアントに送信します。

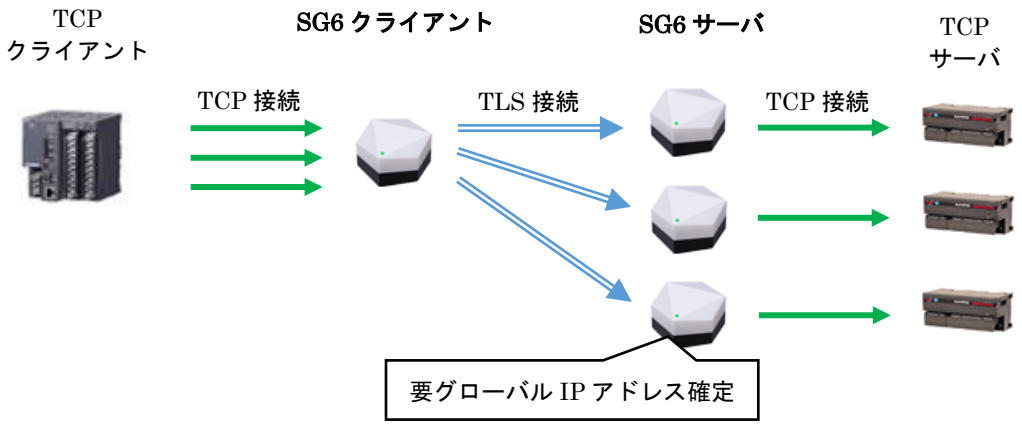
3. 切断

SG6 クライアントおよび SG6 サーバは、TLS もしくは TCP の一方の切断を検出時に、もう片方の接続も切断します。



4. 逆接続モードの利点

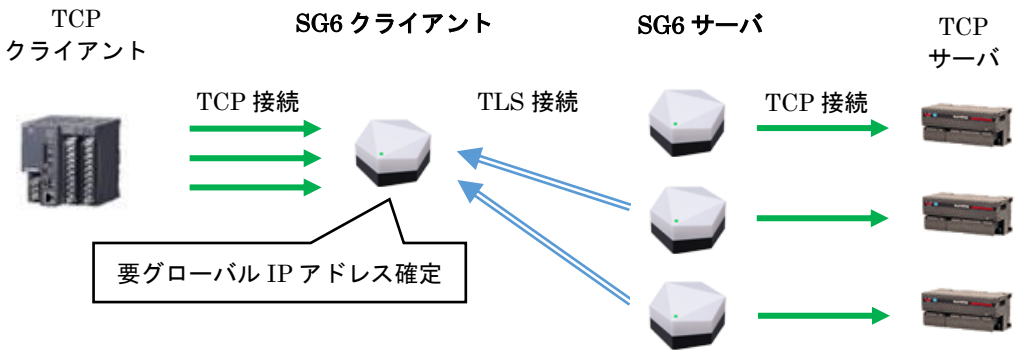
下図のように、1 拠点の TCP クライアントから 3 拠点の TCP サーバに標準モードの SG6 経由でアクセスする場合、サーバ 3 拠点分の固定 IP アドレスもしくは DDNS 契約が必要になります。
この状態からサーバ拠点を追加する場合は、その拠点数分の同契約が必要になります。



これに対し、SG6 を逆接続モードで使用する場合は、下図のようになります。SG6 間の接続方向が標準モードの時とは逆になるため、固定 IP アドレスもしくは DDNS 契約が必要となるのはクライアント 1 拠点分のみです。
サーバ拠点を追加してもこの構成は同じため、アドレス確定の手間を省くことができます。

また、追加するサーバ拠点に既設のインターネット回線があれば、それを流用できることもできます。さらに、変動 IP アドレスが割り振られる格安 SIM を挿入したモバイルルータも使用できます。

反面、標準モードと比較し自由度は低くなってしまいます。

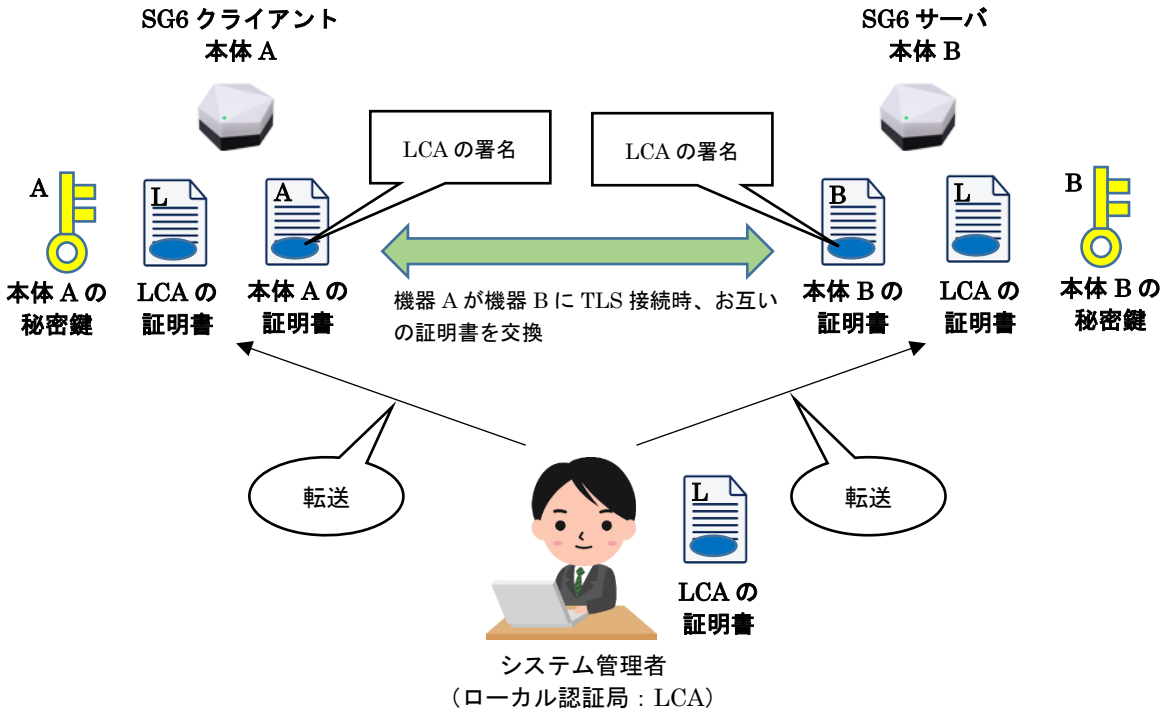


2.4.3 認証

SG6 は、TLS 接続時に相互認証(サーバ認証・クライアント認証)を行います。この認証を行うには、システム管理者は最初にローカル認証局(LCA)を構築する必要があります。具体的には 1 台の PC 内に構築することになるのですが、この PC を外部から隔離し、厳重に保管してください。
LCA の構築には、ローカル CA 作成支援ツール(形式:LCA-SG 「3.2 LCA-SG」を参照)をご利用ください。LCA を構築時、LCA の証明書が作成されます。これは、電子データ(ファイル形式)として PC 内に保存されます。

次に、LCA-SG を用いて本体用の証明書を作成し、SG6 に転送します。TLS 接続時には SG6 がお互いの証明書を交換しますが、これらには LCA の署名が入っています。これが間違いなく先に構築した LCA の署名であることを確認するには、その LCA の証明書が必要になります。このため、SG6 への本体証明書転送時には、LCA の証明書も合わせて転送されます。さらには、暗号通信時に必要な本体秘密鍵(ファイル形式)も転送されます。
結果として、転送毎に 3 つのファイルが送信されることになります。

下図の例では 2 台の SG6 を用いていますが、SG6 の使用台数分同じ作業を行ってください。



サーバ認証およびクライアント認証の手順は TLS で規格化されたものであり、SG6 独自のものではありません。
詳細については、TLS の仕様書や解説等を参照ください。

3. 設定

3.1 準備するもの

下記のものをご準備ください。

- SG6（クライアント／サーバ）
- ローカル認証局作成支援ソフトウェア（形式：LCA-SG）※
- 上記それぞれの取扱説明書※
- パソコン
- LAN ケーブル

※弊社ホームページよりダウンロードが可能です。

3.2 設定の流れ

SG6 を使用するにあたり、下記の手順で設定を行います。

設定画面の表示
SG6 にブラウザから接続し、設定用の画面を表示します。

▼

システムの設定
ログイン方法、ネットワーク、無線 LAN の設定を行います。

▼

アプリケーションの設定
自動時刻修正、ネットワーク変換機能の設定を行います。

▼

証明書の転送
LCA-SG からセキュア通信に必要な証明書の転送を行います。
転送時は 3.4.1 **ログイン方法の設定**で設定する ID、PASSWORD を使用します。詳細は LCA-SG の取扱説明書を参照ください。

ご注意

●設定用のポートを開放してインターネット経由での接続は安全ではありません。必ず、LAN 内から設定を行うようにしてください。
●LCA-SG の通信用のポートを開放してインターネット経由での接続は安全ではありません。必ず、LAN 内から設定を行うようにしてください。
●バックアップ電池を搭載していないため起動時に時刻がリセットされます。
リセット後の時刻は以下となります。
・工場出荷時設定：2020 年 1 月 1 日 0:00:00
・LCA-SG から証明書転送済み：証明書を転送したときの転送元 PC の時刻
●ルータの設定変更が必要な場合があります。ルータ設定については「5.2.4 ルータ設定」を参照して下さい。

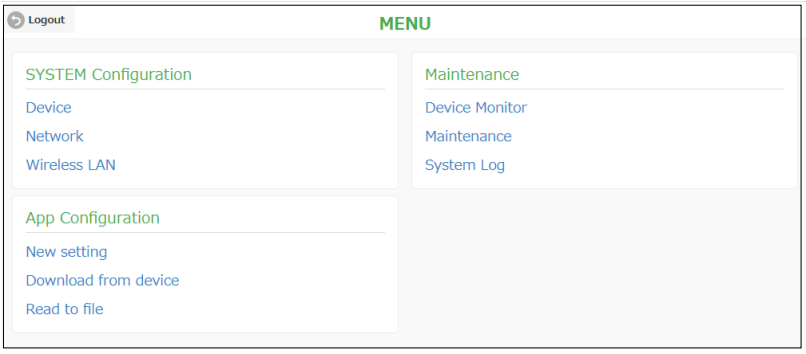
3.3 設定画面の表示

SG6 は、設定用の Web サーバ機能を持っています。SG6 設置後は、Ethernet を介して PC の Web ブラウザから初期設定を行ってください。工場出荷時設定は下表の通りとなっておりますので、設定する際には PC の IP アドレスを 192.168.0.5 等の通信可能なアドレスに設定し、SG6 と Ethernet ケーブルで接続してください。

ネットワーク設定	内　容
IP アドレス	192.168.0.10
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	0.0.0.0
DNS アドレス	0.0.0.0
ポート番号	8080

① Web ブラウザで http://192.168.0.10:8080/ に接続すると「SIGN IN」画面が表示されます。
② ID（初期値：admin）、PASSWORD（初期値：admin）を入力し、「Login」をクリックしてください。

③ ログインに成功すると「MENU」画面が表示されます。



項　目	内　容
Logout	設定画面をログアウトし、「SIGN IN」画面に戻ります。

項　目	内　容
SYSTEM Configuration	ログイン方法、ネットワーク、無線 LAN*の設定を行います。
App Configuration	自動時刻修正、ネットワーク変換機能の設定を行います。
Maintenance	バージョンの確認、手動時刻修正等のメンテナンスを行います。

*無線 LAN を搭載する「無線 LAN タイプ J」のみ項目が表示され、設定が可能です。

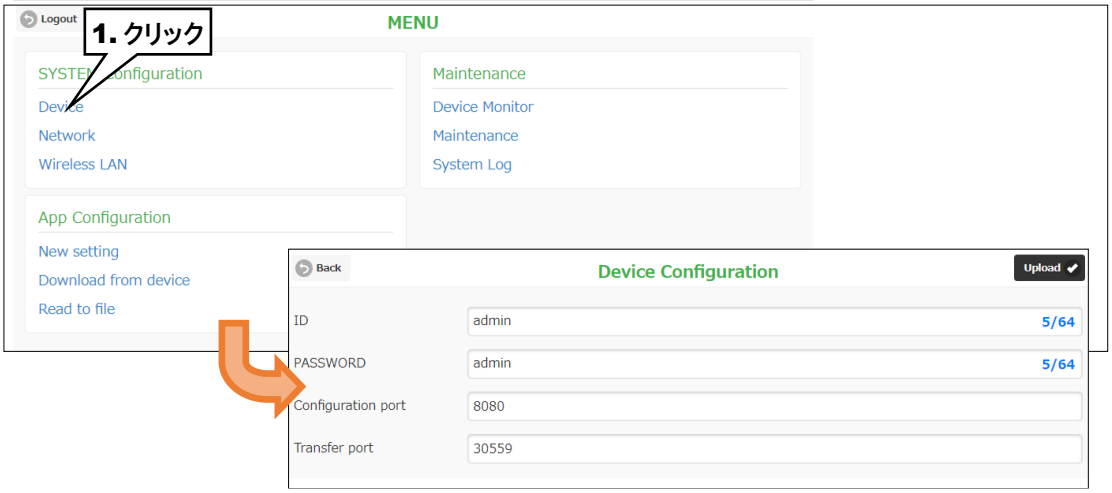
3.4　システムの設定

ログイン方法、ネットワーク、無線 LAN の設定を行います。

3.4.1　ログイン方法の設定

SG6 の設定画面にログインするための設定を行います。

① 「MENU」画面の「Device」をクリックすると、「Device Configuration」画面が表示されます。

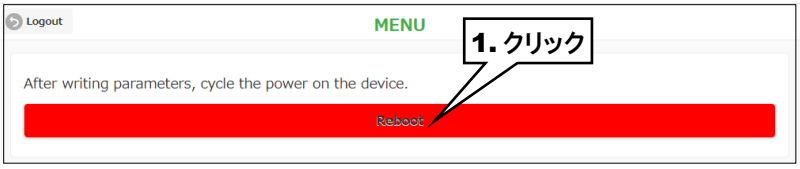


項　目	内　容
Upload	設定を SG6 に転送します。転送に成功すると「MENU」画面に戻ります。
Back	「MENU」画面に戻ります。

設定項目	内　容	初期値
ID	設定および LCA-SG 転送用ユーザーID を設定します。	admin
PASSWORD	設定および LCA-SG 転送用パスワードを設定します。	admin
Configuration port	設定画面に接続するためのポート番号を設定します。	8080
Transfer port	LCA-SG と接続するためのポート番号を設定します。	48565

② 「Upload」をクリックすると、SG6 へ設定値を転送し、「MENU」画面に戻ります。

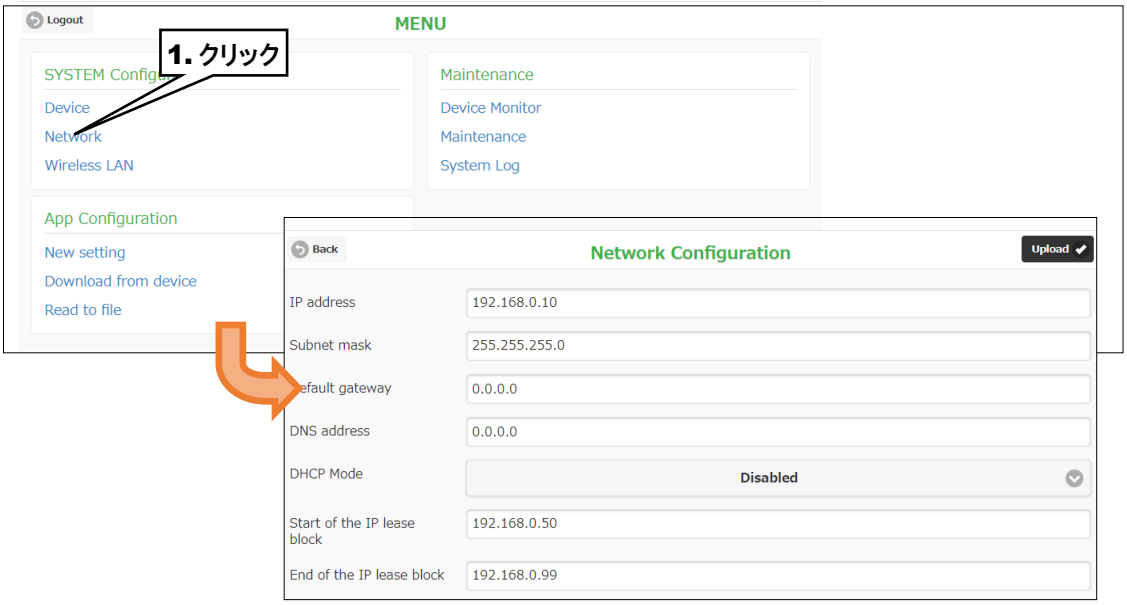
③ 設定転送後は「MENU」画面に「Reboot」ボタンが表示されますので、「Reboot」をクリックし、SG6 の再起動と設定の反映を行います。他に設定を変更する場合は再起動せず、そのまま設定変更を継続します。



3.4.2 ネットワークの設定

SG6 のネットワーク、簡易 DHCP サーバ機能に関する設定を行います。

① 「MENU」画面の「Network」をクリックすると、「Network Configuration」画面が表示されます。



項　目	内　容
Upload	設定を SG6 に転送します。転送に成功すると「MENU」画面に戻ります。
Back	「MENU」画面に戻ります。

設定項目	内　容	初期値
IP address	IP アドレスを設定します。	192.168.0.10
Subnet mask	サブネットマスクを設定します	255.255.255.0
Default gateway	外部ネットワークにつながるルータのアドレスを設定します。	0.0.0.0
DNS address	DNS アドレスを設定します。 外部ネットワークと通信しない LAN 限定で使用する場合は、DNS の設定は、0.0.0.0（使用しない）のままでかまいません。	0.0.0.0
DHCP mode	DHCP サーバの有効（Enabled）、無効（Disabled）を設定します。 DHCP サーバが有効な場合、本器が DHCP クライアントに配布するアドレスと設定値の対応は以下となります。 配布アドレス / 設定項目 IP アドレスの範囲 / Start of the IP lease block, End of the IP lease block サブネットマスク / Subnet mask デフォルトゲートウェイ / Default gateway DNS アドレス / DNS address	Disabled
Start of the IP lease block	DHCP サーバで配布する IP アドレスの範囲を設定します。	192.168.0.50
End of the IP lease block	DHCP サーバで配布する IP アドレスの範囲を設定します。	192.168.0.99

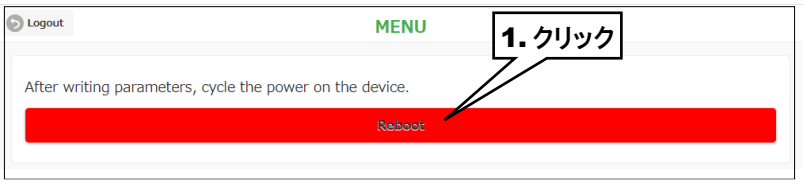
ご注意

●配布 IP アドレスの範囲と DNS アドレスは、必ず SG6 と直接（デフォルトゲートウェイを介さないで）通信可能なアドレス範囲を設定してください。直接通信できないアドレス範囲を設定した場合の正常動作は保証できません。

●同じネットワーク内に別の DHCP サーバがすでに設置してある場合は、本機能を有効にしないでください。両方のサーバ機能が衝突し、正常動作しません。

② 「Upload」をクリックすると、SG6 へ設定値を転送し、「MENU」画面に戻ります。

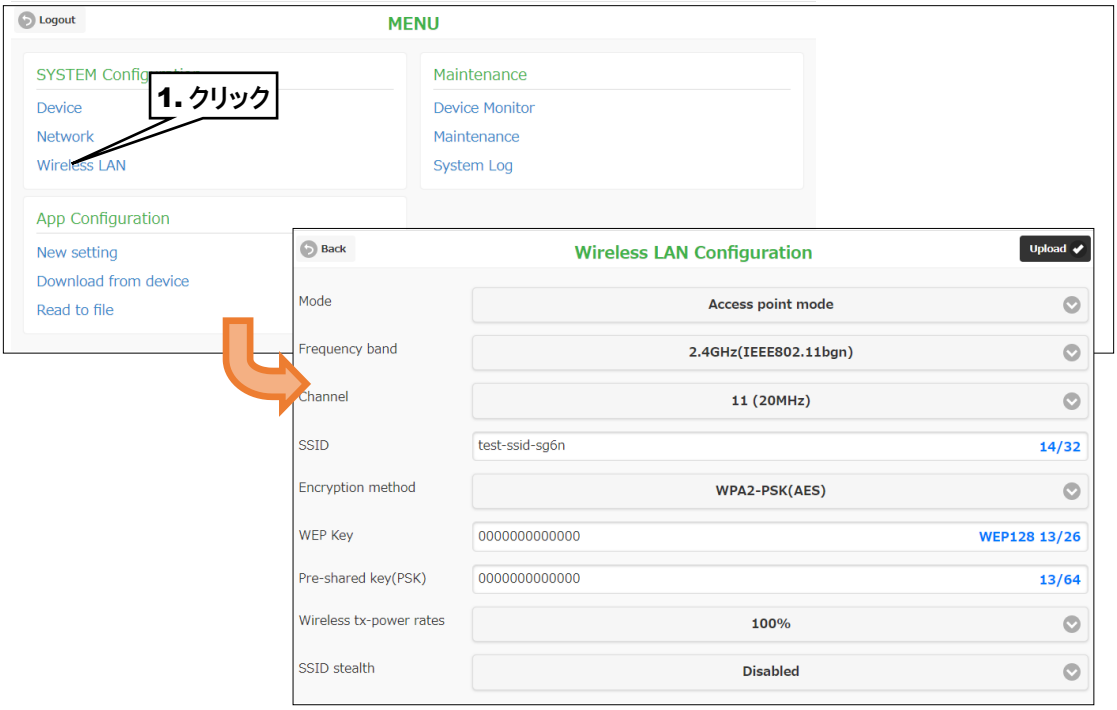
③ 設定転送後は「MENU」画面に「Reboot」ボタンが表示されますので、「Reboot」をクリックし、SG6 の再起動と設定の反映を行います。他に設定を変更する場合は再起動せず、そのまま設定変更を継続します。



3.4.3 無線 LAN の設定

SG6 の無線 LAN に関する設定を行います。
本設定は、無線 LAN を搭載する「無線 LAN タイプ J」のみで表示、設定が可能です。

① 「MENU」画面の「Wireless LAN」をクリックすると、「Wireless LAN Configuration」画面が表示されます。

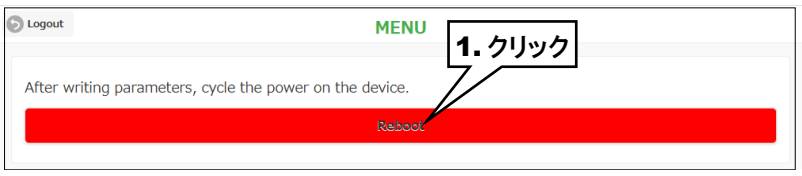


項　目	内　容
Upload	設定を SG6 に転送します。転送に成功すると「MENU」画面に戻ります。
Back	「MENU」画面に戻ります。

<table>
<tr><th>設定項目</th><th>内　容</th><th>初期値</th></tr>
<tr><td>Mode</td><td>無線 LAN の機能を設定します。
Access point mode / Off から選択します。
詳細は「5.2.5.1 アクセスポイント」を参照してください。</td><td>Access point mode</td></tr>
<tr><td>Frequency band</td><td>無線で使用する周波数帯域を設定します。
2.4GHz(IEEE802.11bgn) / 5GHz(IEEE802.11an)から選択します。</td><td>2.4GHz
(IEEE802.11bgn)</td></tr>
<tr><td>Channel</td><td>無線で使用するチャネルを設定します。
詳細は「5.2.5.2 使用可能チャネルと帯域幅」を参照してください。</td><td>11 (20MHz)</td></tr>
<tr><td>SSID</td><td>ネットワーク名を 32 文字の任意の文字列で設定します。</td><td>test-ssid-sg6n</td></tr>
<tr><td>Encryption method</td><td>無線で使用する暗号化方式を設定します。
None / WEP / WPA-PSK(TKIP) / WPA-PSK(AES) /
WPA2-PSK(TKIP) / WPA2-PSK(AES)から選択します。</td><td>WPA2-PSK(AES)</td></tr>
<tr><td>WEP Key</td><td>暗号化の種類で WEP を選択時、無線接続に使用するキーを設定します。
キーは WEP 64 と WEP128 の 2 種類の暗号強度により下記の 2 種類の長さの文字で設定します。
<table>
<tr><th>項　目</th><th>内　容</th></tr>
<tr><td>WEP64</td><td>5 文字の ASCII 文字、または 10 桁の 16 進数</td></tr>
<tr><td>WEP128</td><td>13 文字の ASCII 文字、または 26 桁の 16 進数</td></tr>
</table></td><td>0000000000000</td></tr>
<tr><td>Pre-shared key(PSK)</td><td>暗号化の種類で WPA、WPA2 を選択時に設定します。
8～63 文字の ASCII 文字、または 64 桁の 16 進数で設定します。</td><td>0000000000000</td></tr>
<tr><td>Wireless tx-power rates</td><td>無線の送信出力強度を 100% / 70% / 50% / 35% / 25%から選択します。
無線送信出力を制限することにより、無線の到達距離の範囲を短くして、他の無線への影響を少なくすることができます。</td><td>100%</td></tr>
<tr><td>SSID stealth</td><td>SSID ステルスの有効（Enabled）、無効（Disabled）を設定します。
SSID ステルスを有効にすると SG6 はネットワーク名（SSID）を周りの機器に通知しなくなります。無線ステーションから SG6 の SSID を探索できなくなります。</td><td>Disabled</td></tr>
</table>

② 「Upload」をクリックすると、SG6 へ設定値を転送し、「MENU」画面に戻ります。

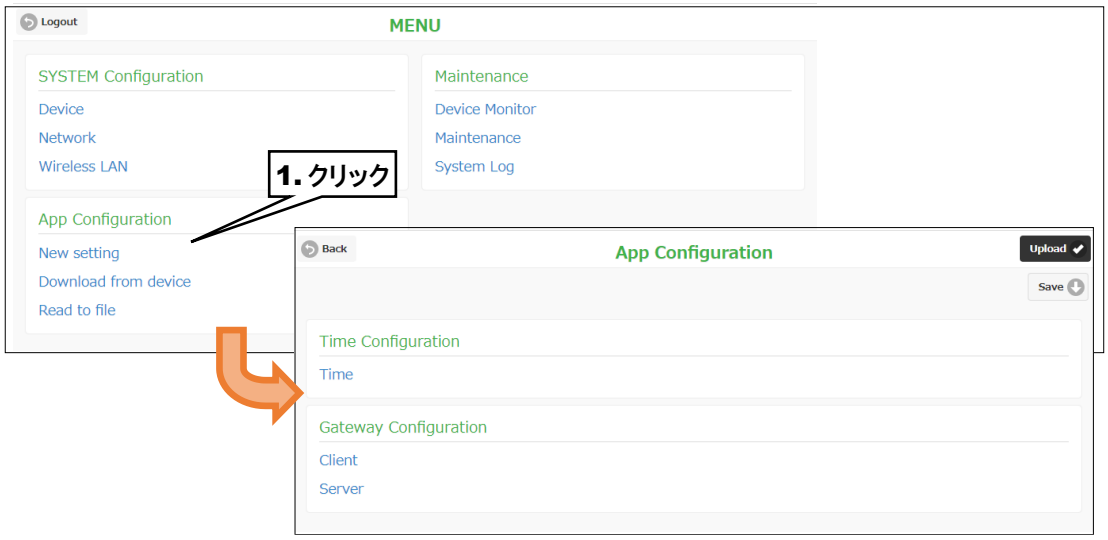
③ 設定転送後は「MENU」画面に「Reboot」ボタンが表示されますので、「Reboot」をクリックし、SG6 の再起動と設定の反映を行います。他に設定を変更する場合は再起動せず、そのまま設定変更を継続します。



3.5 アプリケーションの設定

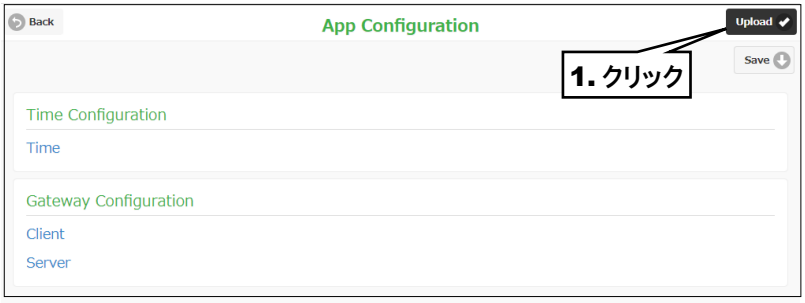
自動時刻修正、ネットワーク変換機能の設定を行います。

① 「MENU」画面の App Configuration から設定方法を選択すると「App Configuration」画面が表示されます。



設定方法	内　容
New setting	初期値から設定変更します。
Download from device	SG6 に保存されている設定値を読み出して設定変更します。
Read to file	ファイルに保存した設定値を読み出して設定変更します。

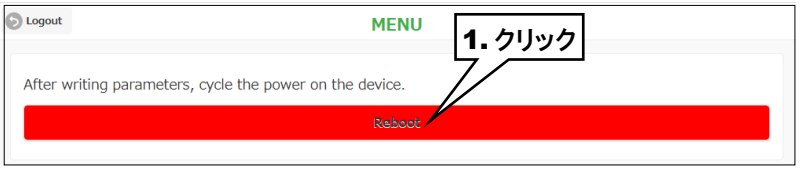
② 設定を変更し、「Upload」をクリックし、設定値を転送します。設定内容は各設定項目を参照してください。



項　目	内　容
Upload	設定を SG6 に転送します。
Save	ファイルに設定値を保存します。
Back	「MENU」画面に戻ります。

設定項目	内　容
Time Configuration	自動時刻修正に関する設定を行います。
Gateway Configuration	ネットワーク変換に関する設定を行います。

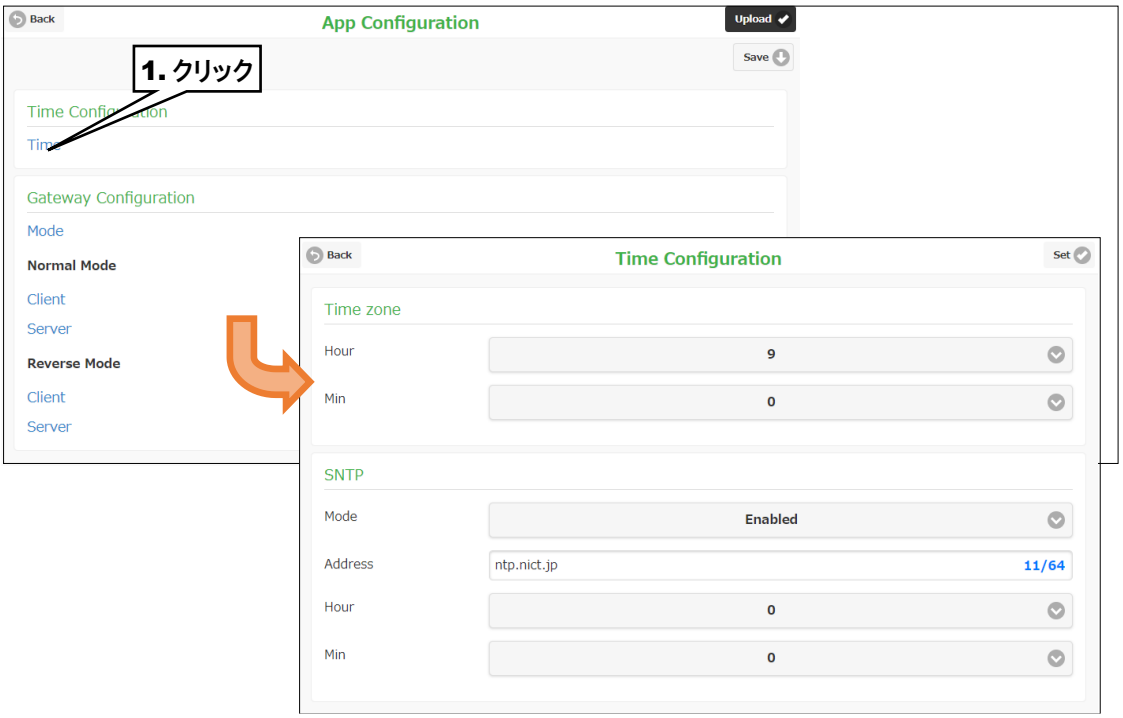
③ 「Back」をクリックし「MENU」画面に戻ります。設定転送後は「MENU」画面に「Reboot」ボタンが表示されますので、「Reboot」をクリックし、SG6 の再起動と設定の反映を行います。他に設定を変更する場合は再起動せず、そのまま設定変更を継続します。



3.5.1 自動時刻修正の設定

SG6 のローカル時間、自動時刻修正の設定を行います。

① 「App Configuration」画面の「Time」をクリックすると、「Time Configuration」画面が表示されます。



項　目	内　容
Set	設定を確定し、「App Configuration」画面に戻ります。
Back	「App Configuration」画面に戻ります。

設定項目		説　明	初期値
Time zone	Hour	タイムゾーンを-12:00～+13:59 の範囲で設定します	+09:00
	Min		
SNTP	Mode	SNTP クライアント機能の有効（Enabled）、 無効（Disabled）を設定します。 SNTP クライアント機能を有効にすると、起動時および設定された時刻で自動時刻修正を行います。	Enabled
	Address	SNTP のサーバを IP アドレスまたはドメインネーム 64 文字以内で設定します。 入力可能ドメインネーム 1 文字目：半角英字、‘_’ 2 文字目以降：半角英数字、‘_’、‘.’、‘,’	ntp.nict.jp
	Hour	SNTP の時刻修正を実行する時間を設定します。	00:00
	Min		

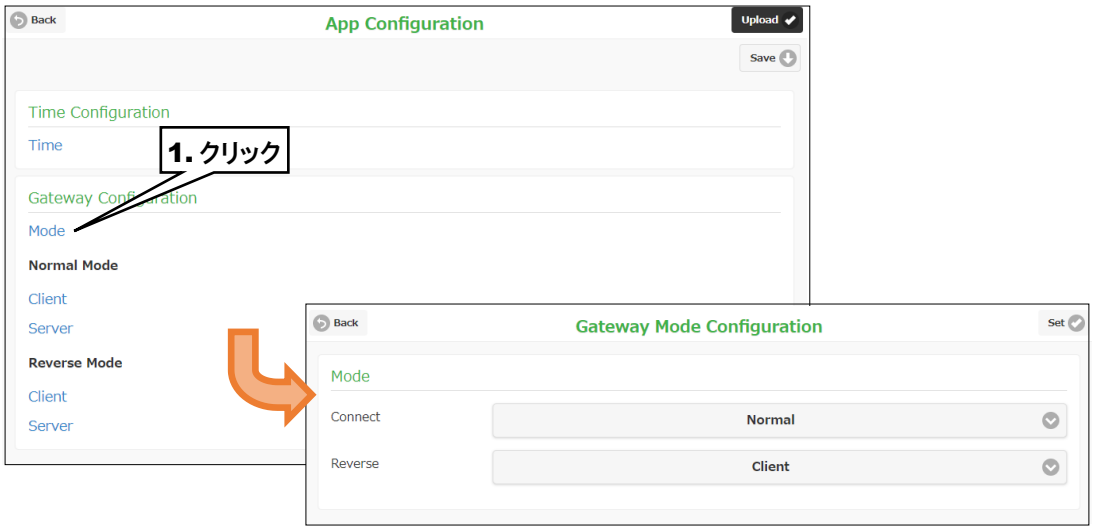
②「Set」をクリックし、設定を確定し、「App Configuration」画面に戻ります。

3.5.2 ネットワーク変換機能の設定

ネットワーク変換機能の設定を行います。接続方向を決定するモード設定を行い、モード設定に応じたクライアント、サーバの設定を行います。

1. モード設定

① 「App Configuration」画面の「Mode」をクリックすると、「Gateway Mode Configuration」画面が表示されます。

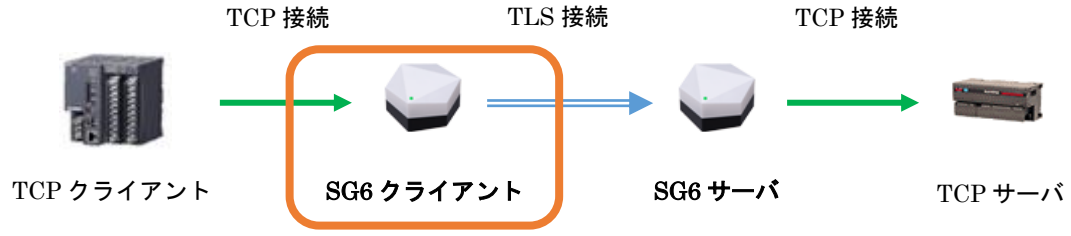


項　目	内　容
Set	設定を確定し、「App Configuration」画面に戻ります。
Back	「App Configuration」画面に戻ります。

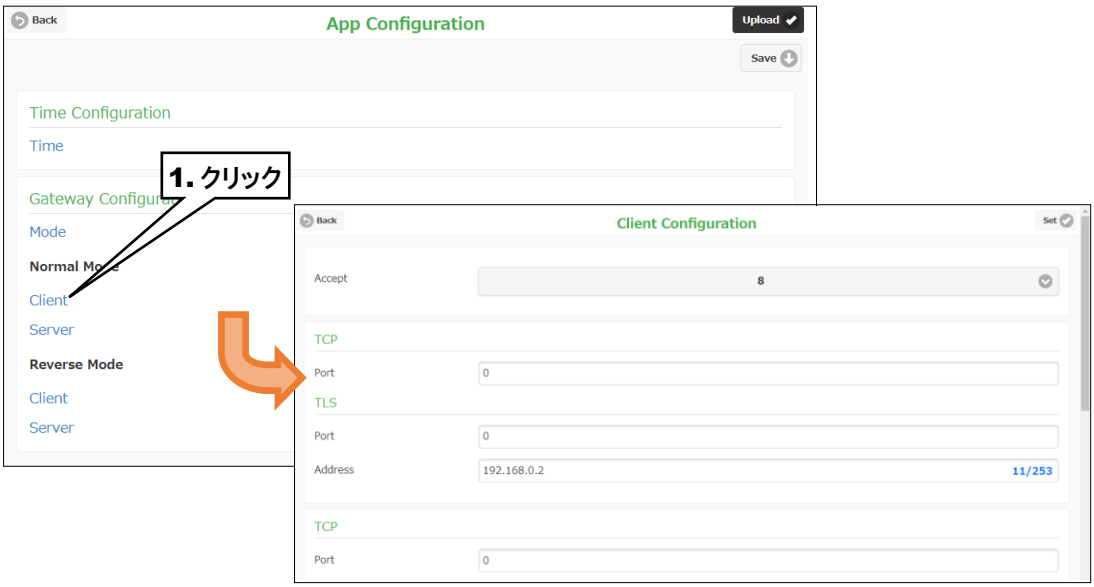
設定項目	内　容	初期値
Connect	接続モードを標準モード（Normal）、逆接続モード（Reverse）から選択します。	Normal
Reverse	逆接続モード時に有効となります。 クライアント機能（Client）、サーバ機能（Server）から選択します。	Client

2. 標準モード

クライアント設定



① 「App Configuration」画面の Normal Mode にある「Client」をクリックすると、「Client Configuration」画面が表示されます。



項　目	内　容
Set	設定を確定し、「App Configuration」画面に戻ります。
Back	「App Configuration」画面に戻ります。

設定項目	内　容	初期値
Accept	TCP 接続の待ち受けポート数を 1/2/4/8 から設定します。 待ち受けポート数と各ポートのコネクション数は下表となります。	8

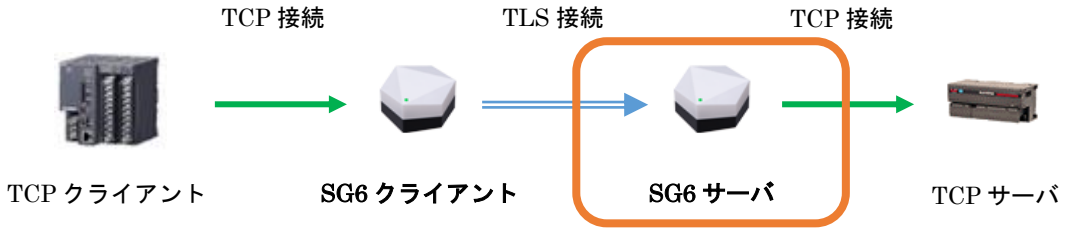
ポート数	コネクション数
1	64
2	32
4	16
8	8

②「Accept」で設定した待ち受けポート数分のクライアント設定を行います。

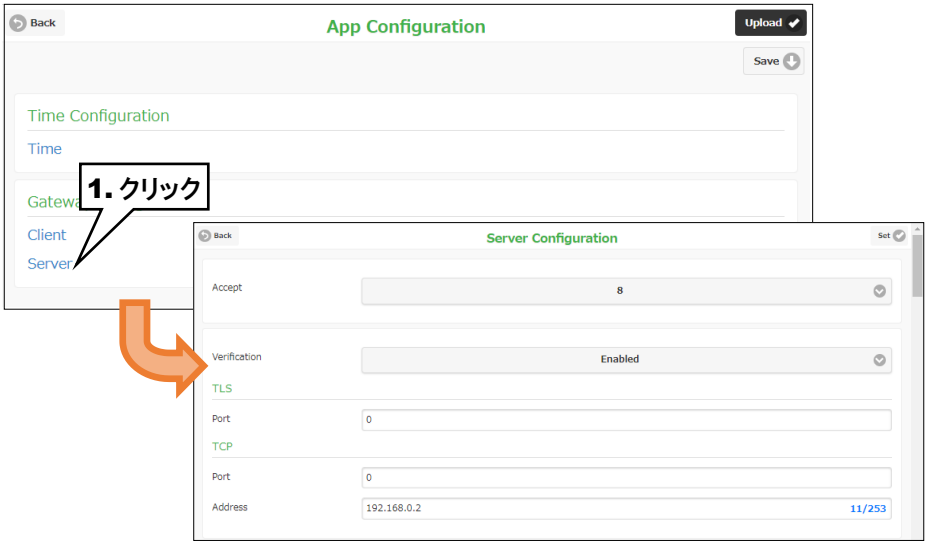
設定項目	内　容	初期値
TCP Port	TCP 接続の待ち受けポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0
TLS Port	TLS 接続先のポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0
TLS Address	TLS 接続先を IP アドレスまたはドメインネームで設定します。 入力可能ドメインネーム 1 文字目：半角英字、‘_’ 2 文字目以降：半角英数字、‘_’、‘.’、‘,’	192.168.0.2

③「Set」をクリックし、設定を確定し、「App Configuration」画面に戻ります。

サーバ設定



①「App Configuration」画面の Normal Mode にある「Server」をクリックすると、「Server Configuration」画面が表示されます。



項　目	内　容
Set	設定を確定し、「App Configuration」画面に戻ります。
Back	「App Configuration」画面に戻ります。

<table>
<tr><th>設定項目</th><th>内　容</th><th>初期値</th></tr>
<tr><td>Accept</td><td>TLS 接続の待ち受けポート数を 1/2/4/8 から設定します。
待ち受けポート数と各ポートのコネクション数は下表となります。
<table>
<tr><th>ポート数</th><th>コネクション数</th></tr>
<tr><td>1</td><td>64</td></tr>
<tr><td>2</td><td>32</td></tr>
<tr><td>4</td><td>16</td></tr>
<tr><td>8</td><td>8</td></tr>
</table></td><td>8</td></tr>
</table>

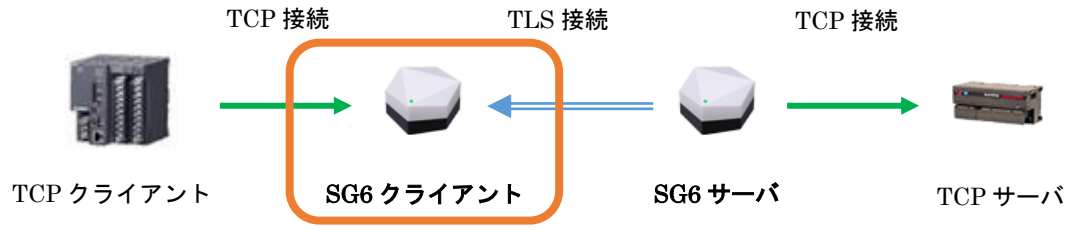
②「Accept」で設定した待ち受けポート数分のサーバ設定を行います。

設定項目	内　容	初期値
Verification	クライアント認証の有効（Enabled）、無効（Disabled）を設定します。 SG6 クライアントと通信する場合は Enabled としてください。	Enabled
TLS Port	TLS 接続の待ち受けポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0
TCP Port	TCP 接続先のポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0
TCP Address	TCP サーバを IP アドレスまたはドメインネーム 253 文字以内で設定します。 入力可能ドメインネーム 1 文字目：半角英字、‘_’ 2 文字目以降：半角英数字、‘_’、‘.’、‘,’	192.168.0.2

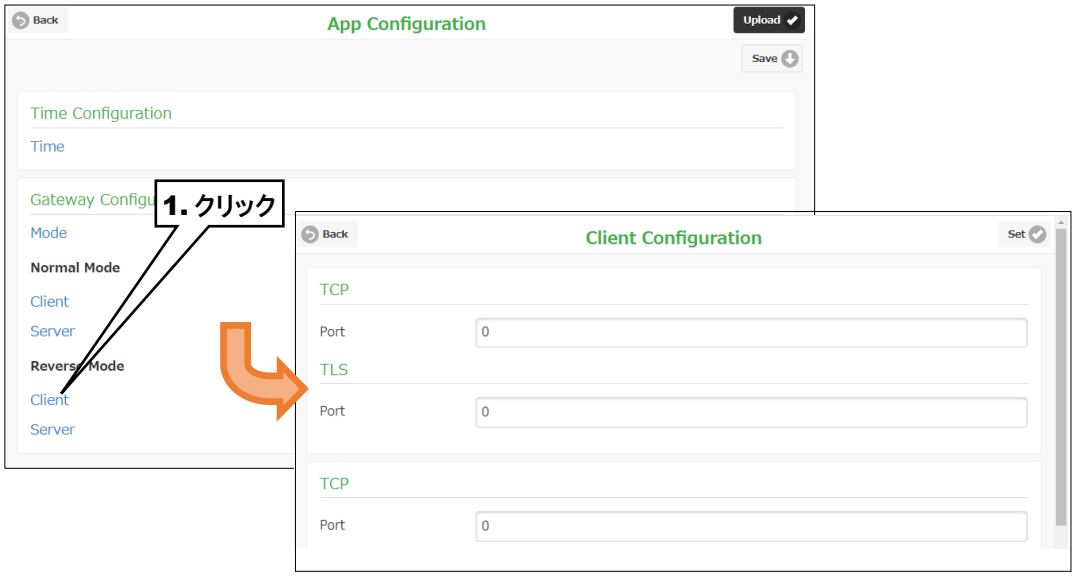
③「Set」をクリックし、設定を確定し、「App Configuration」画面に戻ります。

3. 逆接続モード

クライアント設定



① 「App Configuration」画面の Reverse Mode にある「Client」をクリックすると、「Client Configuration」画面が表示されます。

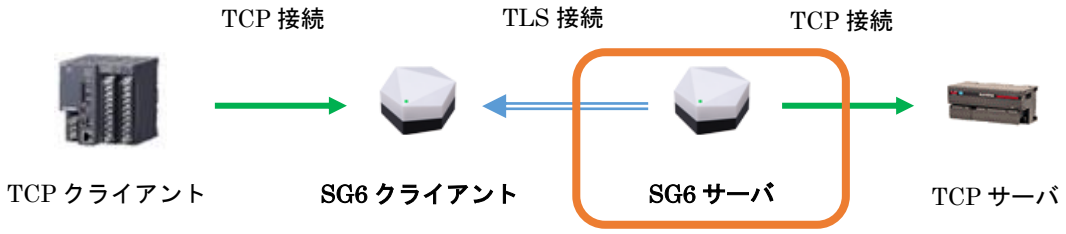


項　目	内　容
Set	設定を確定し、「App Configuration」画面に戻ります。
Back	「App Configuration」画面に戻ります。

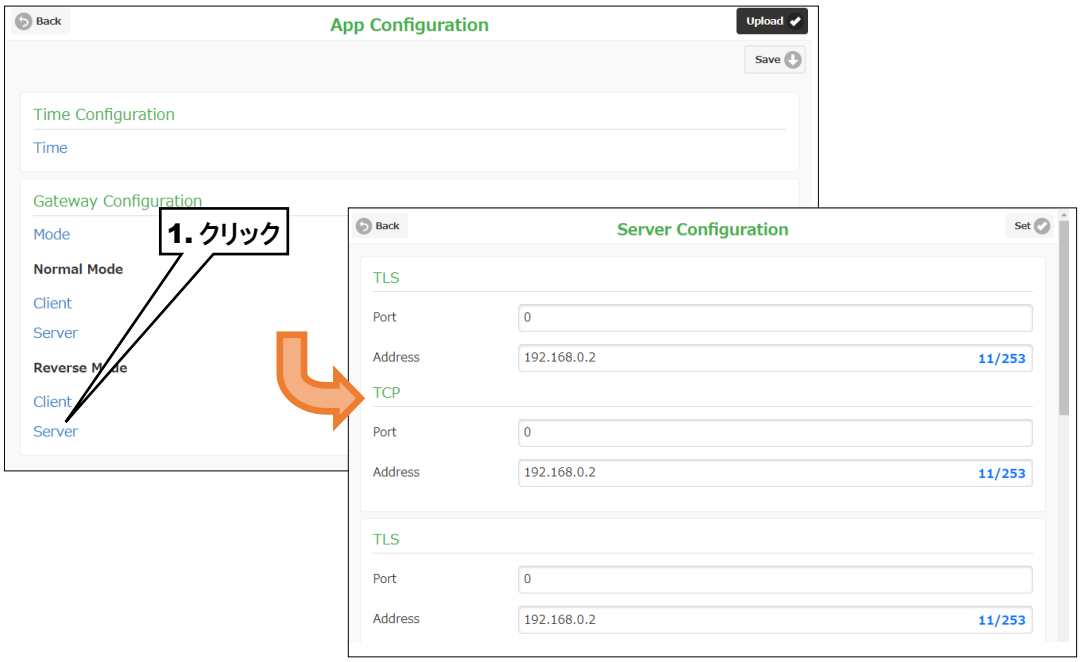
設定項目	内　容	初期値
TCP Port	TCP 接続の待ち受けポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0
TLS Port	TLS 接続の待ち受けポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0

③ 「Set」をクリックし、設定を確定し、「App Configuration」画面に戻ります。

サーバ設定



①「App Configuration」画面の「Server」をクリックすると、「Server Configuration」画面が表示されます。



項　目	内　容
Set	設定を確定し、「App Configuration」画面に戻ります。
Back	「App Configuration」画面に戻ります。

設定項目	内　容	初期値
TLS Port	TLS 接続先の待ち受けポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0
TLS Address	TLS 接続先を IP アドレスまたはドメインネーム 253 文字以内で設定します。 入力可能ドメインネーム 1 文字目：半角英字、‘_’ 2 文字目以降：半角英数字、‘_’、‘.’、‘,’	192.168.0.2
TCP Port	TCP 接続先の待ち受けポート番号を 0~65535 で設定します。 0 とするとポートは未使用となります。	0
TCP Address	TCP 接続先の IP アドレスまたはドメインネーム 253 文字以内で設定します。 入力可能ドメインネーム 1 文字目：半角英字、‘_’ 2 文字目以降：半角英数字、‘_’、‘.’、‘,’	192.168.0.2

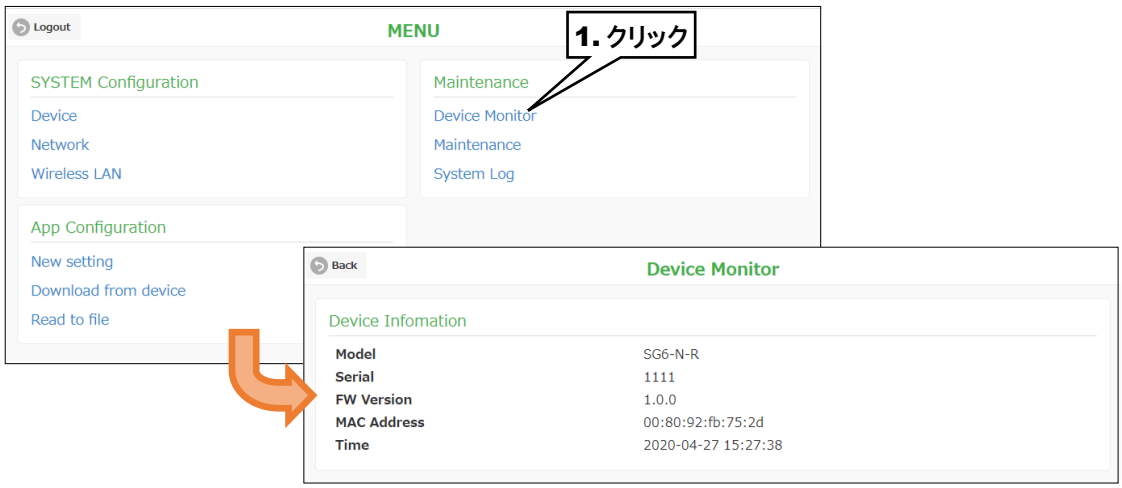
③「Set」をクリックし、設定を確定し、「App Configuration」画面に戻ります。

4. 保守

4.1 メンテナンス

4.1.1 機器情報の閲覧

「MENU」画面の「Device Monitor」をクリックすると、「Device Monitor」画面が表示されます。



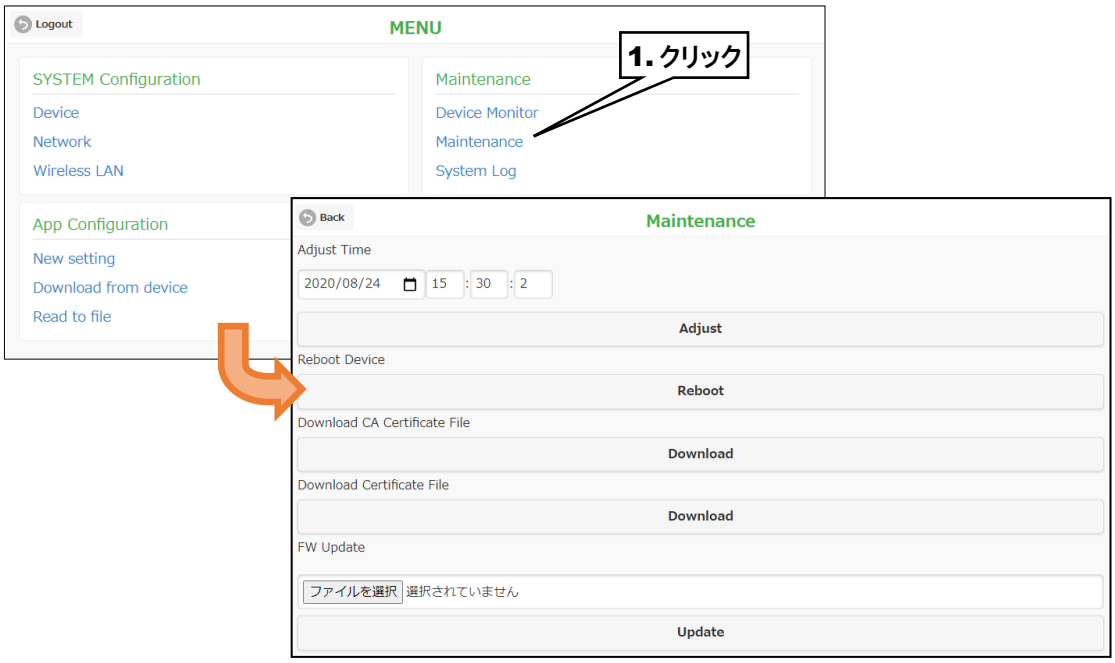
項　目	内　容
Back	「MENU」画面に戻ります。
Device Infomation	機器情報が表示されます。

「Device Monitor」画面の Device Information で閲覧できる機器情報は下表となります。

機器情報	内　容
Model	形式
Serial	機番
FW Version	ファームウェアバージョン
MAC address	MAC アドレス
Time	現在時刻

4.1.2 機器のメンテナンス

「MENU」画面の「Maintenance」をクリックすると、「Maintenance」画面が表示されます。
「Maintenance」画面では、手動時刻修正、機器の再起動、CA 証明書のダウンロード、ファームウェアアップデートがおこなえます。



項　目	内　容
Back	「MENU」画面に戻ります。

項　目	内　容
Adjust Time	SG6 に時刻を設定します。 画面表示時には PC の時刻が表示されます。
Reboot Device	SG6 を再起動します。
Download CA Certificate File	SG6 に転送された CA 証明書をファイルに保存することができます。
Download Certificate File	SG6 に転送された機器証明書をファイルに保存することができます。
FW Update	ファイルを選択ボタンでファームウェアファイルを選択し、Update ボタンでファームウェアを機器に転送します。転送後、機器を再起動するとファームウェアのアップデートがおこなわれます。

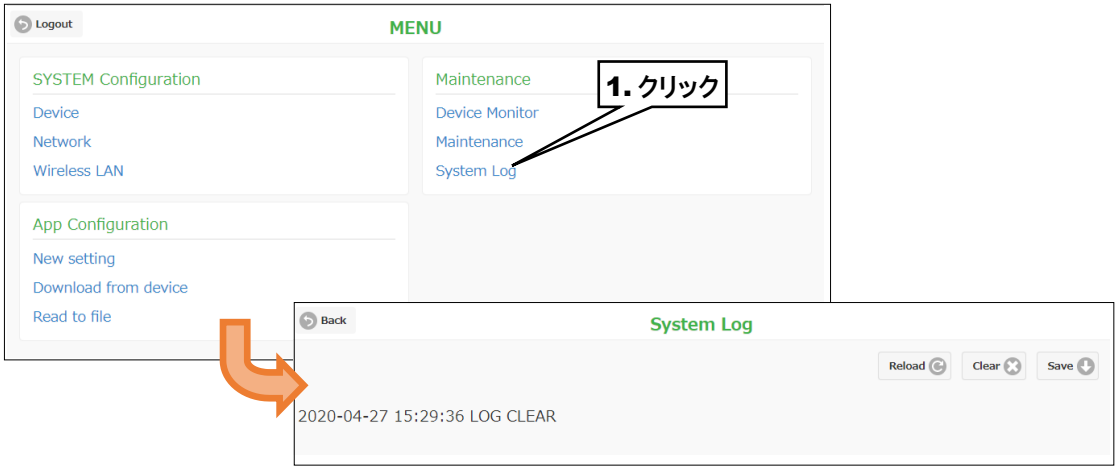
ご注意

●ファームウェアアップデート中に電源断されますと、故障の原因となりますので絶対に電源断しないでください。

4.1.3 システムログ

1. 閲覧方法と操作について

「MENU」画面の「System Log」をクリックすると、「System Log」画面が表示されます。



項　目	内　容
Back	「MENU」画面に戻ります。
Reload	システムログを再読み込みします。
Clear	システムログをクリアします。 クリア後は「Reload」にて再読み込みしてください。
Save	現在表示されているシステムログをファイルに保存します。

2. メッセージについて

システムログは、最新の 1000 件を記録することができ、停電時も保持されています。

システムログのメッセージ（抜粋）は下表を参照ください。

メッセージ	説　明
Client:Start	1 つ以上のクライアントを開始しました。
Client:Certificate error	1 つ以上のクライアントが有効で、CA 証明書がない、または 機器証明書と機器秘密鍵の組み合わせが正しくありません。
Client：TLS Connection fail dst=192.168.0.2:802	192.168.0.2:802 への TLS コネンクションに失敗しました。
Server:Start	1 つ以上のサーバを開始しました。
Server:Certficate error	1 つ以上のサーバが有効で、CA 証明書がない、または 機器照明と鍵の組み合わせが正しくありません。
Server:TLS Accept fail port=802	接続要求は受け付けられませんでした。
Server:TCP Connection fail dst=192.168.3.10:502	192.168.3.10:502 への TCP コネクションに失敗しました。
Sntp start error	起動時の時刻修正に失敗しました。
Sntp error	指定時刻の時刻自動修正に失敗しました。
Configuration change	設定変更がありました（起動後の初回のみ）。
Certificate change	新しい証明書が転送されました（起動後の初回のみ）。
TIME ADJUST	手動時刻修正をおこないました。
LOG CLEAR	システムログをクリアしました。

3. システムログの時刻について

システムログに記録される時刻は起動時にリセットされます。
起動後に一度も、自動時刻修正に成功していないまたは手動時刻修正されていない場合は、システムログに記録される時刻の先頭に「*」が付加されます。

ご注意

●バックアップ電池を搭載していないため起動時に時刻がリセットされます。
リセット後の時刻は以下となります。
・工場出荷時設定：2020 年 1 月 1 日 0:00:00
・LCA-SG から証明書転送済み：証明書を転送したときの転送元 PC の時刻

5. 付録

5.1 トラブルシューティング

弊社ホームページのよくあるご質問も併せて参照ください。

5.1.1 ランプ表示

現 象	チェック内容	対応方法
状態表示ランプが点灯しない。	SG6 の電源は入っていますか？	電源を確認してください。
状態表示ランプが赤色で点灯している。	SNTP の時刻修正はできていますか？	ネットワーク設定を確認してください。
	証明書は転送されていますか？	LCA-SG から証明書を転送してください。

5.1.2 設定用 Web サーバ

現 象	チェック内容	対応方法
LAN 経由で設定用 Web サーバの画面を表示できない。	LAN ケーブルが HUB から抜けていませんか？	LAN ケーブルをしっかりと接続してください。
無線 LAN 経由で設定用 Web サーバの画面を表示できない。	アクセスポイントが有効になっていますか？	設定を確認してください。 「3.4.3 **無線 LAN の設定**」を参照ください
	設定が反映されていますか？	設定を反映するために再起動してください。
	アクセスポイントへのパスワードは合っていますか？	アクセスポイントのパスワードを確認してください。 「3.4.3 **無線 LAN の設定**」を参照ください
設定用 Web サーバの画面を表示できない。	端末・パソコンに IP アドレスが割り振られていますか？	DHCP サーバ機能が有効か確認してください。 「3.4.2 ネットワークの設定」を参照ください 無効の場合は、手動で IP アドレスを入力してください。
	SG6 とパソコンの IP アドレスは、同じネットワークアドレスとしていますか？	IP アドレスを見直し、パソコンから ping コマンドを打って応答があるか確認してください。 例） SG6：192.168.0.10 パソコン：192.168.0.5 サブネットマスク：255.255.255.0
	SG6 の IP アドレスを忘れていませんか？。	設定初期化ボタンを長押しして設定を初期化してください。
	ポート番号を忘れていませんか？	設定初期化ボタンを長押しして設定を初期化してください。
	パソコンにファイアウォールやプロキシサーバの設定をされていませんか？	ネットワーク管理者にファイアウォール、プロキシサーバの設定値を確認してください。
	対応端末、対応ブラウザを使用していますか？	端末・ブラウザソフトのバージョンを確認してください。
	ご使用の端末やパソコンに問題はありませんか？	別の端末・パソコンを使用してください。

5.1.3 SG6 クライアント／SG6 サーバ

現 象	チェック内容	対応方法
SG6 クライアントに接続できない	SG6 に接続できますか？	設定用 Web サーバの項目を参照ください。
	ポート番号を忘れていませんか？	設定用 Web サーバに接続し、設定を確認してください。
	設定は反映されていますか？	設定変更後は反映のために再起動してください。
	証明書は転送済みですか？	LCA-SG を用いて証明書を転送してください。
SG6 サーバに接続できない	ポート番号を忘れていませんか？	設定用 Web サーバに接続し、設定を確認してください。
	設定は反映されていますか？	設定変更後は反映のために再起動してください。
	証明書は転送済みですか？	LCA-SG を用いて証明書を転送してください。
	時刻は修正されていますか？	自動時刻修正または手動時刻修正をおこなってください。
	証明書有効期間を超えていませんか？	LCA-SG から証明書を再度、作成・転送してください。
	SG6 クライアントの設定はあっていますか？	SG6 クライアントの設定を確認してください。

5.2 参考資料

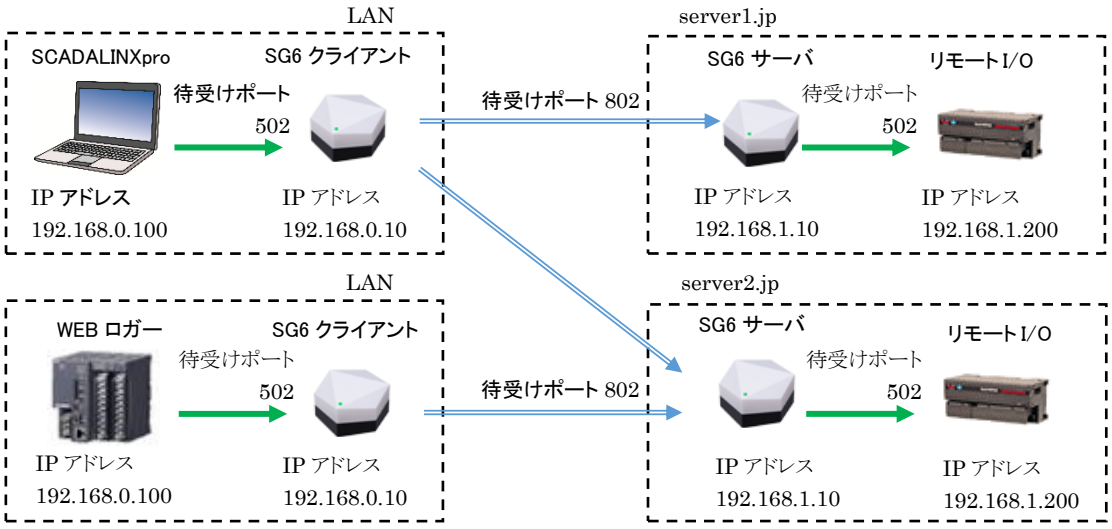
5.2.1 導入例

SG6 を利用したときのプロトコルごとの使用例は以下となります。

1. 標準モード

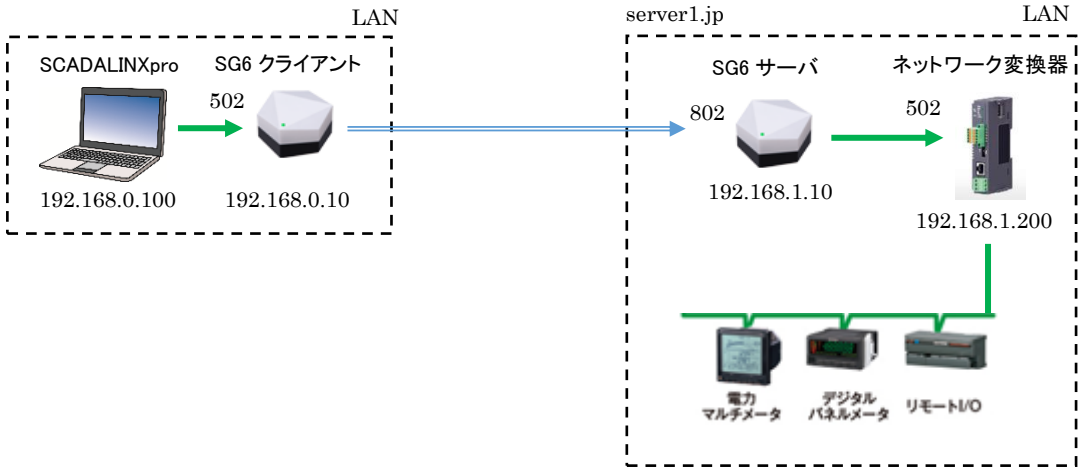
Modbus/TCP

SCADALINXpro による遠隔監視や、DL30 による I/O マッピング等に使用できます。



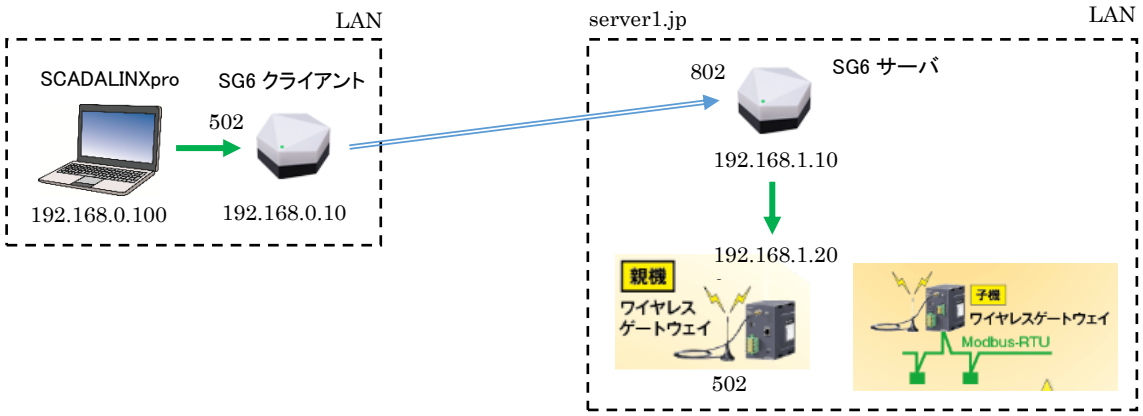
Modbus-RTU（RS485）

GR8-EM や 72EM2 を使用すれば、Modbus-RTU（RS485）対応機器のデータを Modbus/TCP に変換し、インターネットを経由しての運用ができます。



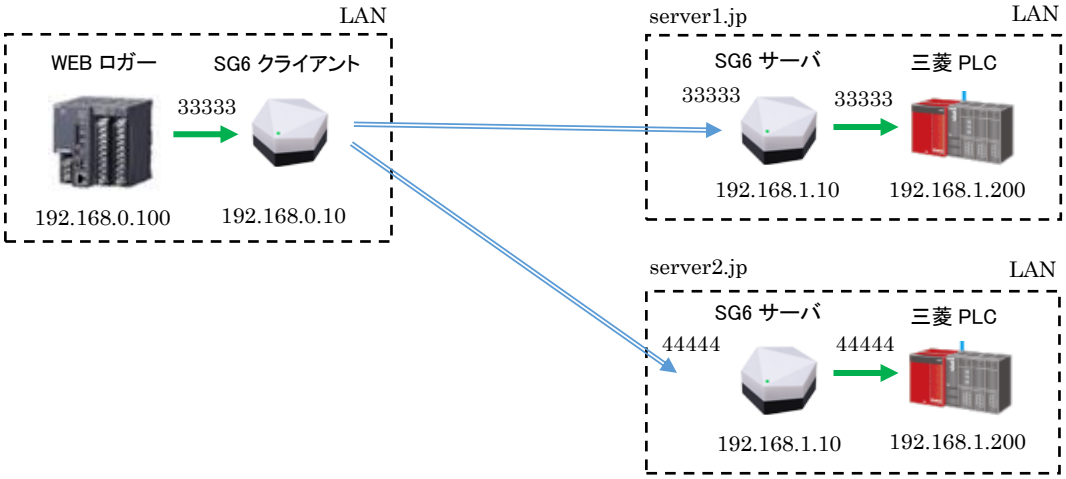
Modbus-RTU（920MHz 帯マルチホップ無線－RS485）

Modbus-RTU（RS485）対応機器のデータを、WL40 を使用した 920MHz 帯無線経由で Modbus/TCP に変換し、インターネットを経由しての運用ができます。



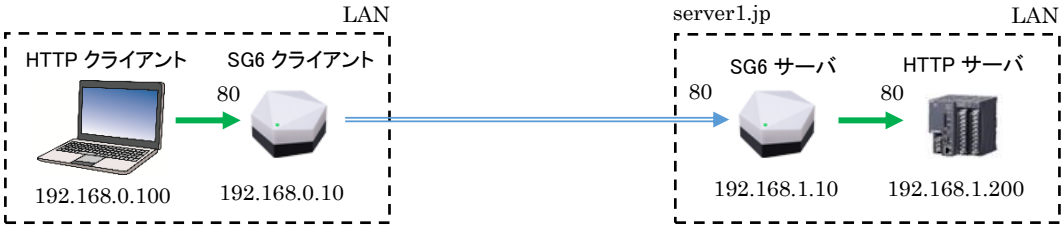
SLMP

DL30 によるデータロギング等に使用できます。



HTTP

DL30 などのブラウザを使用した遠隔監視に使用できます。通常の HTTPS とは異なり、ログイン名、パスワードによらない接続制限が行えます。



ご注意

- ブラウザの Cookie は接続先（IP アドレス、ドメインネーム）ごとに保存されます。SG6 から複数台の HTTP サーバに接続可能ですが、ブラウザの接続先は SG6 となるため、Cookie が正しく保存されない場合があります。
- HTTP サーバごとに Cookie が必要な場合は複数台の SG6 クライアントが必要となります。

HTTP サーバの HTTPS

DL30-N 等の HTTP サーバ機能しか持たない機器との通信を、HTTPS 化できます。この場合は、SG6 サーバのみの使用となります。通常の HTTPS と同様に、ログイン名／パスワードで認証します。

特記事項

- 「サーバ設定」の「Verification」を Disabled に設定し、クライアント認証を無効としてください。
- LCA-SG の CA 証明書を OS またはブラウザにインストールしてください。
  CA 証明書は「4.1.2 **機器のメンテナンス**」からダウンロードしインストールするか、LCA-SG から保存しインストールしてください。

ご注意

- ブラウザの Cookie は接続先ごとに保存されます。SG6 から複数台の HTTP サーバに接続可能ですが、ブラウザの接続先は SG6 となるため、Cookie が正しく保存されない場合があります。
- HTTP サーバごとに Cookie が必要な場合は複数台の SG6 サーバが必要となる場合があります。

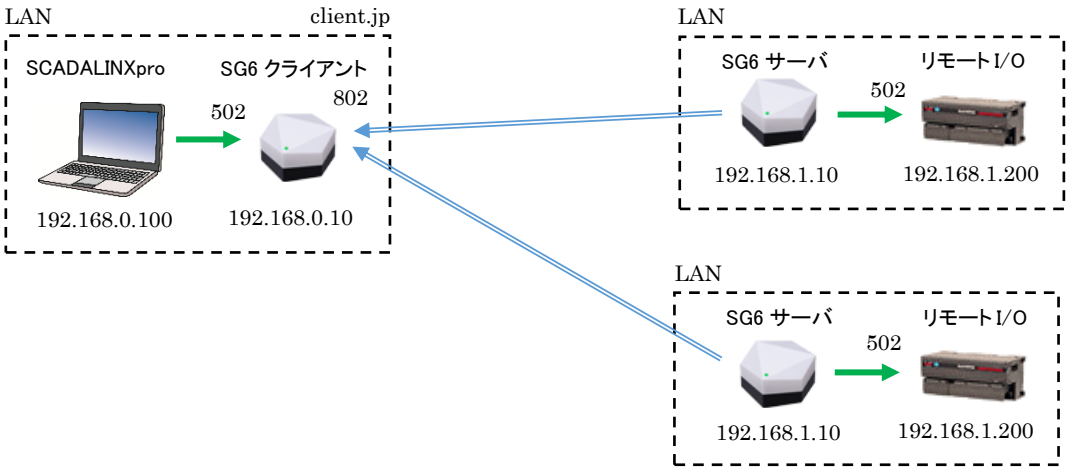
専用プロトコル

コンフィギュレータソフトウェアによる、DL30 のリモートメンテナンスがおこなえます。DL8 や TR30 についても同様におこなえます。

2. 逆接続モード

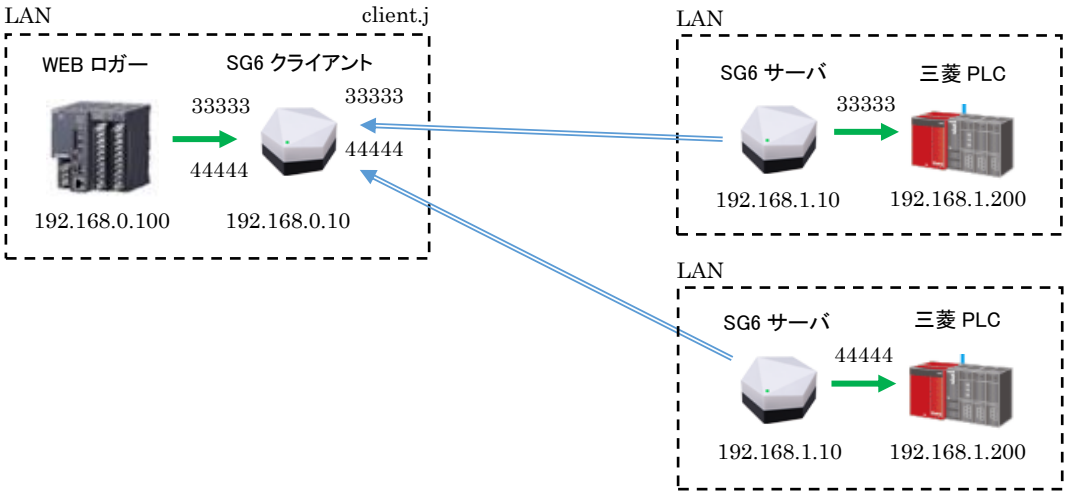
Modbus/TCP

SCADALINXpro による遠隔監視や、DL30 による I/O マッピング等に使用できます。標準モードの場合と同様、ゲートウェイを経由した Modbus-RTU 機器の混在も可能です。



SLMP

DL30 によるデータロギング等に使用できます。

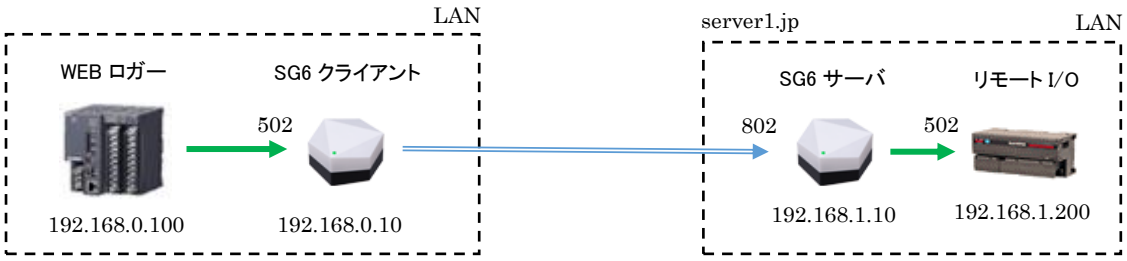


5.2.2 設定例

SG6 を利用したときの接続モードごとの代表的なプロトコルの設定例は以下となります。

1. 標準モード

Modbus/TCP



標準モードの SG6 を 1 対 1 で使用する場合の SG6 の「App Configuration」の設定例は以下となります。その他の HTTP サーバを HTTPS 以外のプロトコルの場合でも同様の設定となります。
その他の設定項目は必要に応じて設定してください。

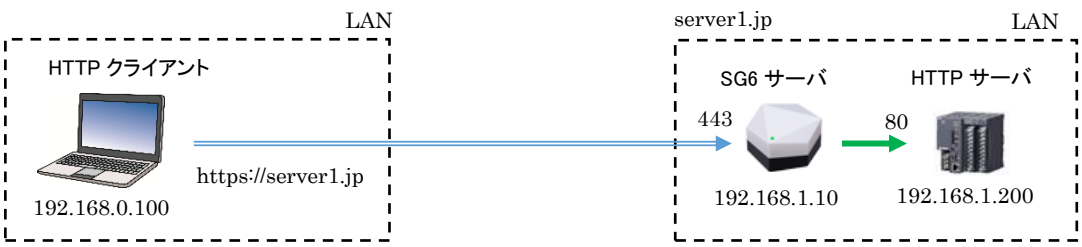
SG6 クライアント設定

設定項目			内　容
Mode		Connect	Normal
Normal Mode	Client	Accept	8
		TCP Port	502
		TLS Port	802
		TLS Address	server1.jp

SG6 サーバの設定

設定項目			内　容
Mode		Connect	Normal
Normal Mode	Server	Accept	8
		Verification	Enabled
		TLS Port	802
		TCP Port	502
		TCP Address	192.168.1.200

HTTP サーバの HTTPS



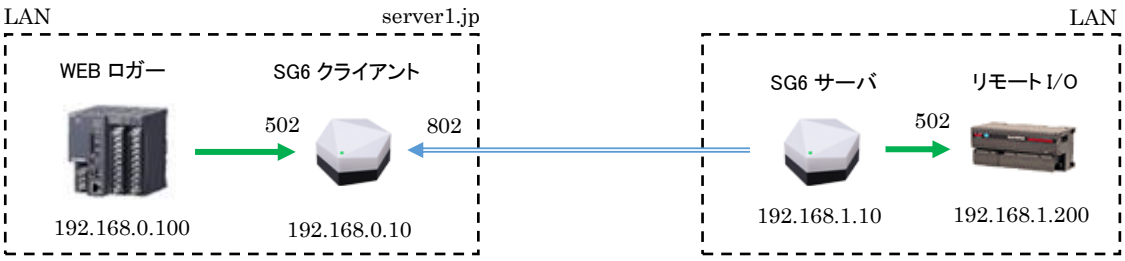
標準モードの SG6 サーバのみを使用したときの SG6 の「App Configuration」の設定例は以下となります。
その他の設定項目は必要に応じて設定してください。

SG6 サーバの設定

設定項目			内　容
Mode		Connect	Normal
Normal Mode	Server	Accept	8
		Verification	Disabled
		TLS Port	443
		TCP Port	80
		TCP Address	192.168.1.200

2. 逆接続モード

Modbus/TCP



逆接続モードの SG6 を 1 対 1 で使用したときの SG6 の「App Configuration」の設定例は以下となります。SLMP の場合でも同様の設定となります。
その他の設定項目は必要に応じて設定してください。

SG6 クライアント設定

設定項目			内　容
Mode		Connect	Reverse
		Reverse	Client
Reverse Mode	Client	TCP Port	502
		TLS Port	802

SG6 サーバの設定

設定項目			内　容
Mode		Connect	Reverse
		Reverse	Server
Reverse Mode	Server	TLS Port	802
		TLS Address	server1.jp
		TCP Port	502
		TCP Address	192.168.1.200

5.2.3 設定用 Web サーバ

以下の環境に対応しています。対応しているブラウザについては仕様書を参照ください。

項　目	内　容
ポート番号	可変（初期値：8080）
同時接続数	1 台まで
文字コード	UTF-8
ブラウザ設定条件	・Javascript を「使用」に設定 ・Cookie を「使用」に設定

5.2.4 ルータ設定

各接続モードでのルータの設定内容は、下表の通りです。設定については、お使いのルータの取扱説明書を参照してください。

モード	ルータ	内　容
標準	クライアント側	不要
	サーバ側	・SG6 サーバ機能の TLS 受付ポートに設定したポートを開放し、SG6 サーバに通す ・固定 IP アドレスもしくは DDNS にて、外部から宛先を特定可とする
逆接続	クライアント側	・受付ポートを開き、パケットを対象 SG6 クライアントのローカルアドレス・ポートに通す ・固定 IP アドレスもしくは DDNS にて、外部から宛先を特定可とする
	サーバ側	不要

ご注意

- 必ず LAN 内の端末より SG6 の設定を行ってください。TCP8080 のポートを開放しての外部からの設定は、安全ではありません。絶対に行わないようにしてください。
- 必ず LAN 内の PC にインストールした LCA-SG より、SG6 への証明書転送を行ってください。TCP48565 のポートを開放しての外部からの転送は、安全ではありません。絶対に行わないようにしてください。
- Modbus/TCP の TCP502 のポートを開放して対象機器に通してしまうと、SG6 採用の意味がなくなってしまいます。必要分以外のポートを開放しないように設定してください。

5.2.5 無線 LAN

1. アクセスポイント

複数のステーション（無線子機）を無線ネットワークに接続させる無線親機の役割を持ち、アクセスポイントと接続している全てのステーションで相互に無線通信できます。

SG6 は無線/Ethernet 間のブリッジ機能を持ち、Ethernet 側に接続している Ethernet 機器と無線接続している機器が相互に通信できます。最大 32 台までステーションを接続することができます。

ご注意

- ブリッジ機能は、IP 通信（TCP、UDP）のみ対応しています。
  IP 通信を使用しない Ethrernet 通信（EthrerCAT など）は非対応となります。

2. 使用可能チャネルと帯域幅

使用可能な無線チャネルは、2.4GHz 帯では 1～13、5GHz 帯では 36～64、100～140 です。
チャネルは単独（帯域幅 20MHz）または、2 つのチャネルを束ねて（帯域幅 40MHz）使用することができます。2 つのチャネルを束ねて使用する場合は「1 + [5]」等、“+ [拡張チャネル]” 表記の項目を選択してください。

帯　域		チャネル	拡　張	屋　外	備　考
2.4GHz		1	5	可	アクセスポイントが無線の混雑となると判定した場合は、拡張チャネルを使用する設定にしていたとしても使用せず、単独（帯域幅 20MHz）チャネルでの無線通信となります。
		2	6		
		3	7		
		4	8		
		5	1 または 9		
		6	2 または 10		
		7	3 または 11		
		8	4 または 12		
		9	5 または 13		
		10	6		
		11	7		
		12	8		
		13	9		
5GHz	W52	36	40	不可	－
		40	36		
		44	48		
		48	44		
	W53	52	56	不可	気象レーダ等が使用している電波を避けて動作するための DFS 機能により、機器起動後 1 分間は無線通信が停止します。 気象レーダ等の電波を検出した場合は、自動的に使用チャネルが変更され、1 分間無線通信が停止した後、無線通信開始します。
		56	52		
		60	64		
		64	60		
	W56	100	104	可	
		104	100		
		108	112		
		112	108		
		116	120		
		120	116		
		124	128		
		128	124		
		132	136		
		136	132		
		140	なし		

ご注意
●屋外使用の項目は、法令で定められた無線の屋外使用の可不可を示したものであり、SG6 の屋外使用を保証するものではありません。

5.3 変更履歴

5.3.1 新規作成

・ 新規作成

5.4 ライセンス

本装置には、expat（http://expat.sourceforge.net/）を組み込んでいます。
この expat は MIT License によって配布されています。
以下は、MIT/X Consortium License によって義務付けられている著作権表示およびライセンス文、免責条項です。

本製品には、以下の Camellia ライセンスの適用を受けるソフトウェアが含まれています。

camellia.c ver 1.2.0