ClickShare ネットワークインテグレーション

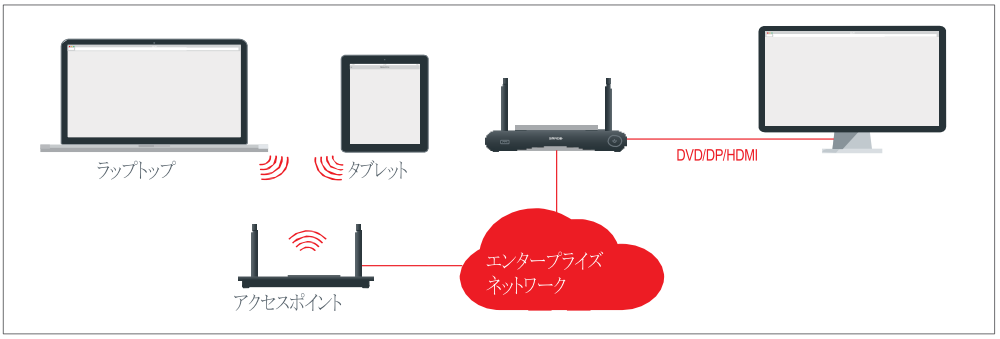
アプリケーション ノート

1 はじめに

この「ClickShare ネットワークインテグレーション」が目指すのは、大規模な組織でも既存のワイヤレスネットワークインフラストラクチャーに干渉せずに ClickShare を設置することです。デフォルトのスタンドアロン設定の場合、ClickShare ベースユニットは ClickShare ボタンによる接続に使うワイヤレスアクセスポイント(AP)を作成します。こうしたアクセスポイント、いわゆる「はぐれ(rogue)」AP は大規模な設置環境では厄介物になるおそれがあります。しかも、会議においてモバイル機器からコンテンツを共有する人たちは、ClickShare ベースユニットに接続するためにネットワークを切り替えなければなりません。

こういった状況では ClickShare ネットワークインテグレーションが役に立ちます。いったん構成が完了して動作を始めると、ベースユニットの内蔵 AP は無効化され、ボタンやモバイル機器は社内ネットワークの一部であるワイヤレスアクセスポイントに接続可能になります。この段階になると、ボタンやモバイル機器がベースユニット上のコンテンツを共有できるように、ベースユニットを有線イーサネットインタフェース経由で社内ネットワークに接続しておかなければなりません。

このアプリケーション ノートの以下の章では設定方法について詳しく説明し、システム内部について少々解説していきます。



2 セキュリティモード

ボタンを使って社内ネットワークに接続する方式としてサポートされているセキュリティモードは 2 種類あります。

- 1 つ目は一般的な社内ネットワーク設定に適用される、**WPA2 エンタープライズ、802.1X 認証**。
- 2 つ目として、従来の Wi-Fi 設定を使用する可能性のある小規模な組織にも対応できるように、**WPA2 パーソナル**とも呼ばれる WPA2-PSK もサポートしています。

どちらのモードも WPA(Wi-Fi Protected Access)に基づいています。このアプリケーション ノートでは、当初の WPA 規格の改良版としてセキュリティ強化のために AES 暗号化を追加した WPA2 についてのみ説明します。

2.1 WWPA2 エンタープライズ、802.1X 認証

WPA2 エンタープライズでは、ネットワーク上の個別クライアントの認証をサーバー(RADIUS を使用)に依存し、802.1x 認証を使います(ポートベースのネットワークアクセス制御ともいいます)。802.1x 認証はローカルエリアネットワーク上で使えるように EAP(Extensible Authentication Protocol:拡張認証プロトコル)のカプセル化が行われます。これはまた「EAP over LAN」や EAPoL とも呼ばれます。RADIUS を使いつつ、ネットワーク上のクライアント機器(ClickShare の場合はボタン)を認証するためのこのような EAPoL メッセージがネットワーク内を流れます。

802.11i(WPA2)規格ではかなりの数の必要な EAP 方式が定義されています。とはいえすべての方式が幅広く現場で使用されているわけではなく、規格外の方式が多用されているものもあります。そこで、われわれは最も広く使用されている EAP 方式を採用しました。ClickShare システムがサポートする EAP 方式は次のとおりです:

- EAP-TLS
- PEAP
- EAP-TTLS

各方式の詳細と設定方法については本アプリケーション・ノートにて後から説明します。

3 考慮すべきこと

ClickShare システムを社内ネットワークに統合すると決定した場合には考慮しなければならない点がいくつかあります。まずは、全てのベースユニットが有線イーサネットインタフェースでネットワークに接続できる状態になっていなければなりません。またキャプチャーされたスクリーンの内容を各ボタンがベースユニットへストリーム配信するのに必要な帯域幅も考慮する必要があります。これは通常 5～15Mbps の間です。ClickShare の使い心地が悪くなるような帯域幅の不足を起こすネットワークのボトルネック（例：100Mbps スイッチ）がない状態にしてください。

4 必要条件

ClickShare ネットワークインテグレーションを始める前に、インフラが以下の必要条件を満たしている必要があります。

4.1 ネットワーク

社内ネットワークを有効にすると ClickShare ベースユニットの内蔵 Wi-Fi アクセスポイントは無効になります。そのためベー スユニットを有線イーサネットインタフェース経由で社内ネットワークに接続しておく必要があります。

4.2 ファイアウォール

コンテンツが ClickShare ボタンを経由して共有されるように、あるいはモバイル機器からベースユニットときちんと共有されるように、ネットワーク上で以下のポートが開いていなければなりません：

送信元		CSE-200 ベースユニット
ClickShare ボタン	TCP UDP	6541-6545 514
ClickShare Presenter	TCP UDP	6541-6545 5353
WebUI	TCP UDP	80; 443
REST API	TCP UDP	4000; 4001
Airplay	TCP UDP	4100-4200; 7000; 7100; 47000 4100-4200; 5353
Google Cast	TCP UDP	8008; 8009; 9080 1900; 32768:61000*
MirrorOp	TCP UDP	6541-6545 5353

4.3 VLAN

社内ネットワークの多くが「基幹」社内ネットワークから BOYD（Bring Your Own Device）トラフィックを分離するためなど、複数の VLAN に分割されています。そのため社内ネットワークに ClickShare を統合する際にはこのことに気をつけてください。社内のワイヤレスインフラに接続する ClickShare ボタンがベースユニットに接続できなければなりません。さらにモバイルアプリを使うなら、それもベースユニットにアクセスできるようにする必要もあります。管理を用意にするために、すべての ClickShare ユニットを分割された VLAN に組み込むことを推奨します。

4.4 DNS

ボタンがコンテンツをベースユニットへストリーム配信するには、ベースユニットのホスト名をネットワーク内で解決できなければなりません。DNS が利用できないなら、ボタンは USB ペアリングの際にベースユニットの IP を参照するようになります。そのため、ホスト名が解決できないときに問題が発生するのを防ぐために、DHCP サーバー上でベースユニットのための IP アドレスを予約しておくことを強く推奨します。

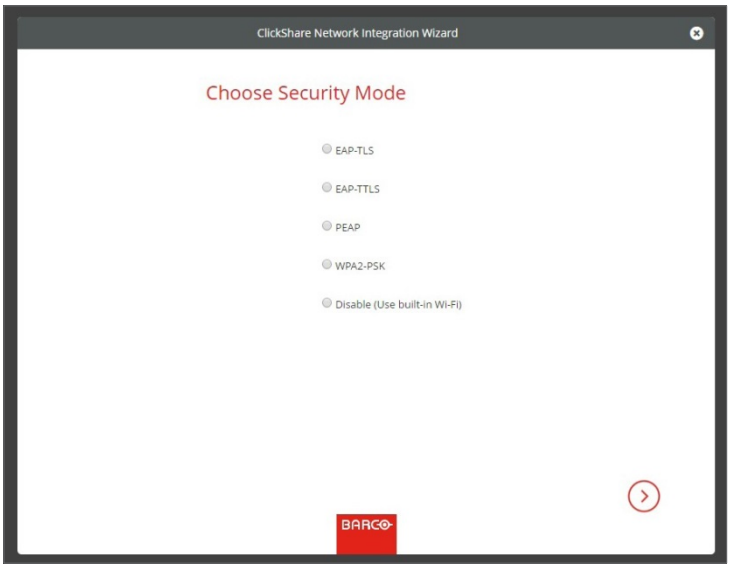
4.4 NTP

EAP-TLS を使用するなら、ベースユニット上にて NTP を設定する必要がありますが、これはベースユニットの WebUI を通じて行えます。EAP-TLS に必要な証明書を処理するためにベースユニットの時刻は正確でなければなりません。できるならローカル社内ネッ トワーク上の可用性の高い NTP サーバーを使うのが望ましいです。インターネット上の NTP サーバーを使用する場合は、ベースユニットがプロキシサーバー経由では接続できないので注意してください。

* Google Cast はビデオストリーミングを円滑に行うために 32768 以上の UDP ポートをランダムで使います。

5 設定

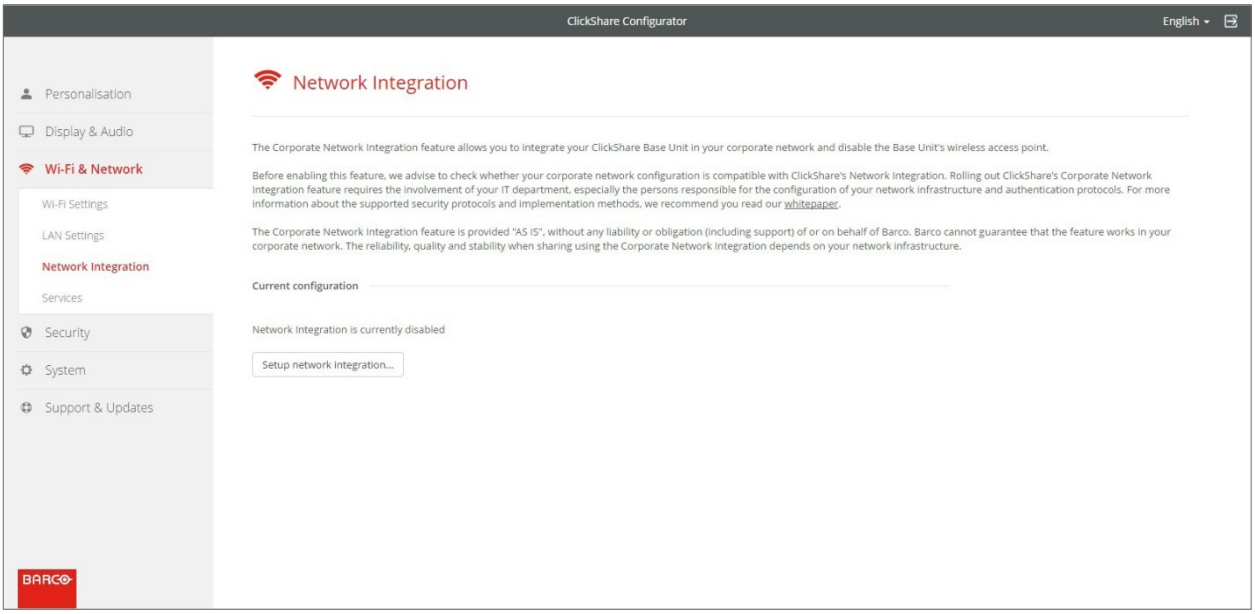
設定が容易に行えるように、ClickShare WebUI 中にウィザードを用意しました。ウィザードがお客様の選択されたセキュリティモードに沿った設定プロセスをご案内します。さらにサポートされているセキュリティモードと、すべてを統合して動作させる上で必要な入力事項についての概要と説明もご覧いただけるようになっています。



5.1 スタートする前に

この機能を有効にする前に、社内のネットワーク設定が ClickShare のネットワークインテグレーションと互換性があるか確認することを勧めます。ClickShare の社内ネットワークインテグレーション機能を有効にするには、IT 部門、ネットワークインフラストラクチャと認証プロトコルの設定の担当者の関与が特に不可欠です。

社内ネットワークインテグレーション機能は、バルコもしくはその代理人の責任や義務（サポートも含めて）と全く関係なく「現状のまま」提供されます。バルコは社内ネットワークでの機能の動作を保証できません。社内ネットワークインテグレーションを使って共有するときの信頼性、品質、安定度は、社内のインフラストラクチャーに左右されます。



5.2 セキュリティ方式

次の 4 つのセクションではサポートされるセキュリティ方式をひとつずつ詳しく説明します。貴社の環境に適合するものをご参照ください。

5.3 設定後

設定ウィザードを終えたら、ClickShare ボタンをすべて再ペアリングするのを忘れないでください。再ペアリング前はベースユニット上で古いスタンドアロンモードがまだ動作中なので共有が行えません。

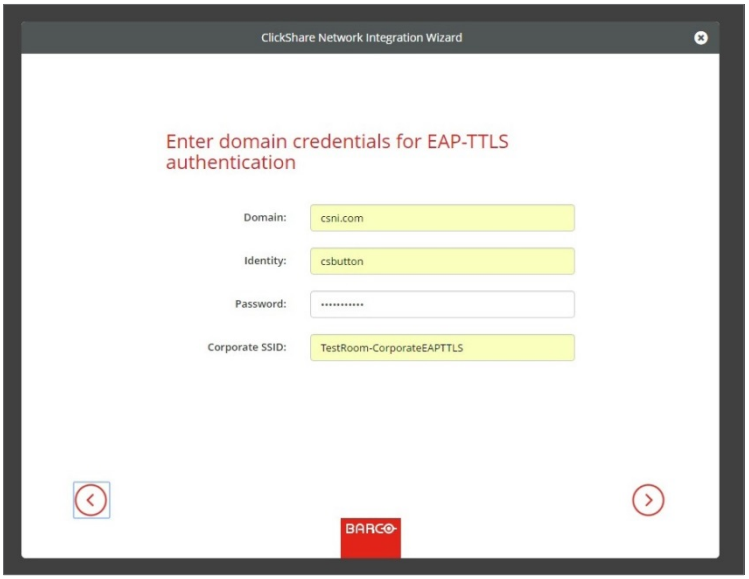
5.4 アプリ

モバイル機器はネットワークに統合されると、社内ネットワークに接続中ならネットワーク上のどのベースユニットともコンテンツを共有できるようになります。(お望みであれば、ベースユニットの WebUI を利用してモバイルデバイスからの共有を禁止することも可能です。)モバイル機器には passcode 認証を設定することをお勧めします。この認証オプションは WebUI の 'Wi-Fi & Network > Services' ページにあります。

6 EAP-TLS

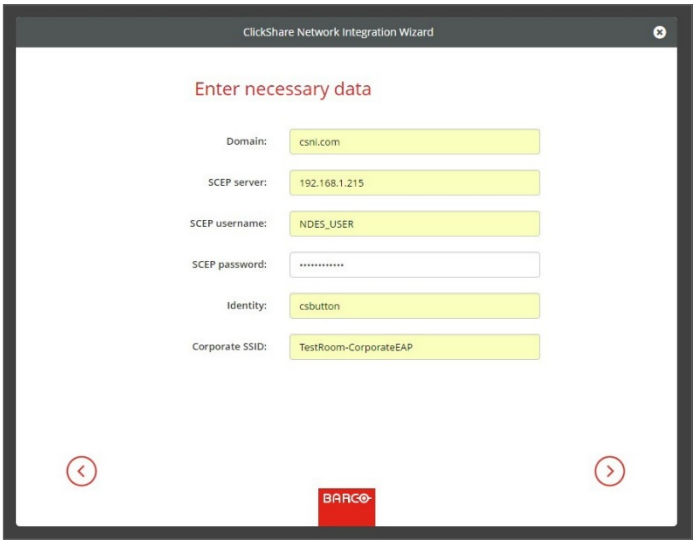
EAP-TLS(Transport Layer Security)は証明書に基づく EAP 方式で、クライアントとサーバー間の相互認証を許容します。サーバーとクライアントの証明書を配布するためには PKI(Public Key Infrasructure:公開鍵基盤)が必要です。(組織として敷居が高いという場合には EAP-TTLS や PEAP で十分代用可能です)。規格では X.509 クライアント証明書が絶対に必要だとしていませんが、当社のものをはじめとして大半の実装において必須となっています。

クライアントの証明書を使用して実装する場合、EAP-TLS が最も安全な EAP 方式のひとつだとされています。PEAP や EAP-TTLS と比べて、EAP-TLS が些細なことながら唯一劣る点は、実際の TLS ハンドシェイクが実行される前にユーザーID が暗号化されずに送信されることです。EAP-TLS は SCEP または手動による証明書のアップロードを介してサポートされています。



6.1 SCEP

Simple Certificate Enrolment Protocol（SCEP）はスケーラブルな方法で証明書の発行および破棄を可能にするものです。ClickShare でもベースユニットおよびボタンと社内ネットワークの統合が迅速かつ円滑に行えるよう、SCEP のサポートを追加しました。大半の企業がマイクロソフトの Windows Server とそのアクティブディレクトリ（AD）を使ってユーザーと機器の管理を行っていることから、当社の SCEP 実装は特に、Windows Server 2008 R2 および Windows Server 2012 に含まれる NDES（Network Device Enrolment Service：ネットワークデバイス登録サービス）を対象としています。現時点において、これ以外の SCEP サーバー実装はサポートされていません。



6.1.1 NDES

NDES（Network Device Enrolment Service：ネットワークデバイス登録サービス）はマイクロソフト社による SCEP プロトコルのサーバー実装です。SCEP を使って EAP-TLS を有効にする場合は、Windows Server 上で NDES が有効になっていて設定が完了し、動作中になっている必要があります。NDES 設定の詳細についてはマイクロソフト社の website1 をご覧ください。[1]

SCEP では登録申請の認証にいわゆる「チャレンジパスワード」を使用します。NDES のためのチャレンジパスワードは社内サーバーの http(s)://[貴社サーバーのホスト名]/CertSrv/mscep_admin から取り出せます。必要な資格情報を設定ウィザードに入力するとき、ベースユニットはチャレンジパスワードをインターネットページから自動的に取り出し、登録申請で使用します。このようにすべてのプロセスが自動化されています。

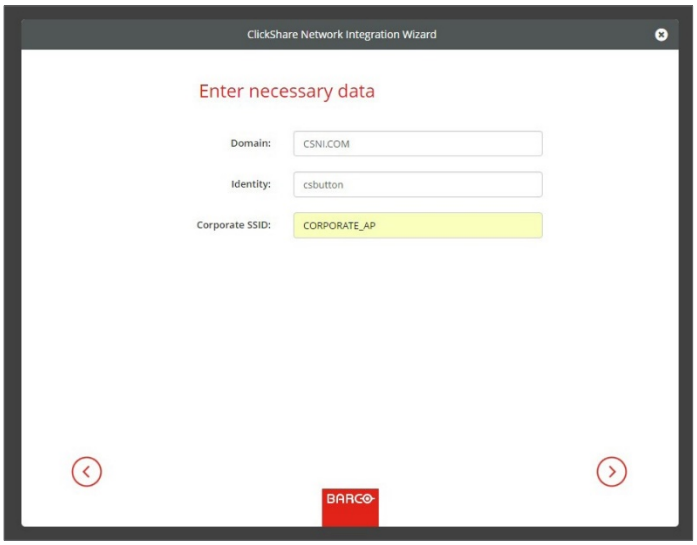
[1] NDES ホワイトペーパー：http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs-en-us.aspx

6.2　手動での証明書提供

現在の構成が SCEP をサポートしない、もしくは SCEP をあまり使いたくないけれども EAP-TLS による相互認証のメリットは捨てがたいという場合は、必要な証明書を手動でアップロードすることも可能です。

- SCEP サーバーIP / ホスト名
- SCEP-ユーザー名
- SCEP パスワード
- ドメイン
- ID
- Cororate SSID

各設定の詳細については第10 節「構成の詳細」をご覧ください



6.2.1　クライアント証明書

お客様の提供するクライアント証明書にはお客様のドメイン内の正式なルート CA による署名が必要であり、ID フィールドに指定されたユーザーにリンクされていなければなりません。またお客様の提供するクライアント証明書には秘密鍵が含まれるようにしてください。プライベート鍵は TLS 接続を正しく設定するために必要です。クライアント証明書は、いわゆるデバイスもしくはマシン証明書でなければならず、ユーザー証明書であってはなりません。

6.2.2　CA 証明書

CA 証明書はドメインでの正式なルート CA の証明書であり、EAP-TL 接続の設定に使います。ウィザード中、お客様の提供するクライアント証明書と CA 証明書間の信頼の連鎖(トラストチェーン)を確証できることをベースユニットは保証します。

6.2.2　入力

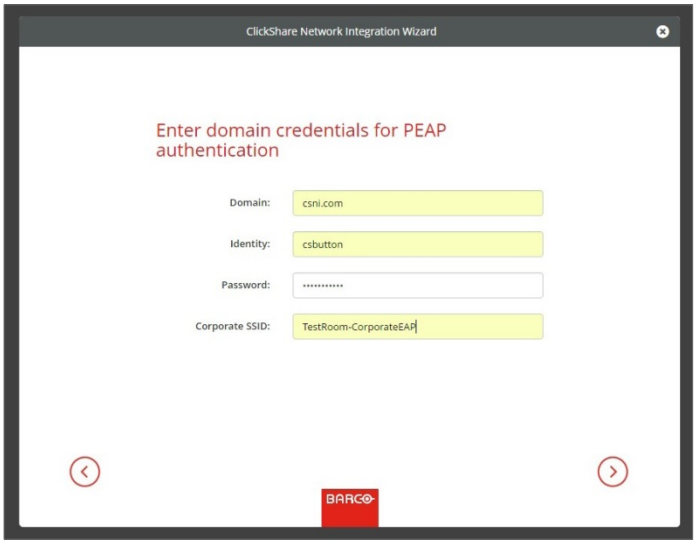
SCEP を使用して EAP-TLS 構成を正しく設定するために必要なデータは:

- クライアント証明書

7 PEAP

PEAP（Protected Extensible Authentication Protocol）はシスコシステムズ社、マイクロソフト社および RSA セキュリティ社の共同開発による EAP の実装です。PEAP はサーバーの CA 証明書を使って安全な TLS トンネルを設定したのち、そのトンネル内で実際のユーザー認証を行います。この方法だとユーザー認証の際に PKI が不要になるだけでなく、TLS のセキュリティを利用することできます。

この規格ではトンネル内の認証に使う方式が定められていませんが、本アプリケーション・ノートにおいて PEAP といえば、内部認証方式としての EAP-MSCHAPv2 付の PEAPv0 のことです。これは WPA および WPA2 規格にて認定された 2 つの PEAP 実装のうちの 1 つであり、他より群を抜いて最も一般的かつ広く普及している PEAP 実装です。



7.1 入力

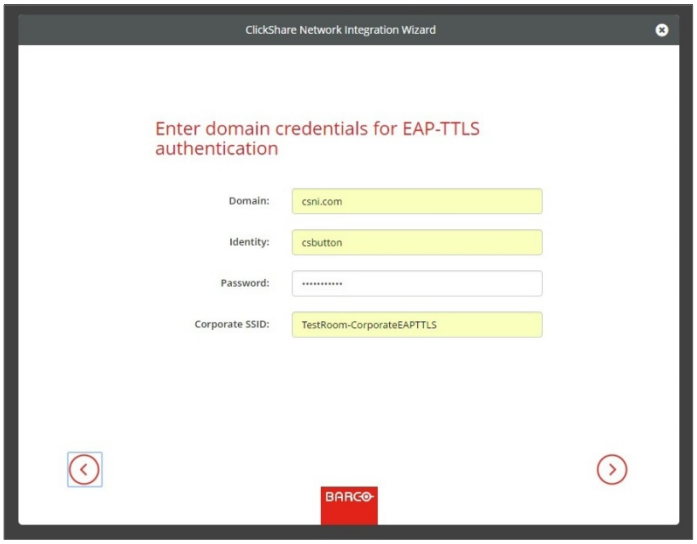
- ドメイン
- ID
- パスワード
- Corporate SSID

各設定の詳細については第 10 節「構成の詳細」をご覧ください。

8 EAP-TTLS

EAP-TTLS（Tunneled Transport Layer Security）は Juniper2 ネットワークによる EAP 実装です。EAP-TLS と同程度の強度の認証を提供すべく作成されたものですが、各ユーザーに証明書を発行する必要はありません。その代わりに認証サーバーにのみ証明書が発行されます。ユーザー認証はパスワードにより行われますが、パスワードの資格情報はサーバーの証明書に基づいて安全に暗号化されたトンネル内を転送されます。ユーザー認証が行われるのは社内 LAN ですでに使用中のものと同一のセキュリティデータベース、たとえば SQL や LDAP データベース、トークンシステムなどです。

EAP-TTLS は通常、社内環境でクライアントの証明書なしに実装されるため、当社のサポート対象にはなっていません。ユーザーごとのクライアント証明書を使いたいという場合は、EAP-TTLS の代わりに EAP-TLS を使うのがいいでしょう。



8.1 入力

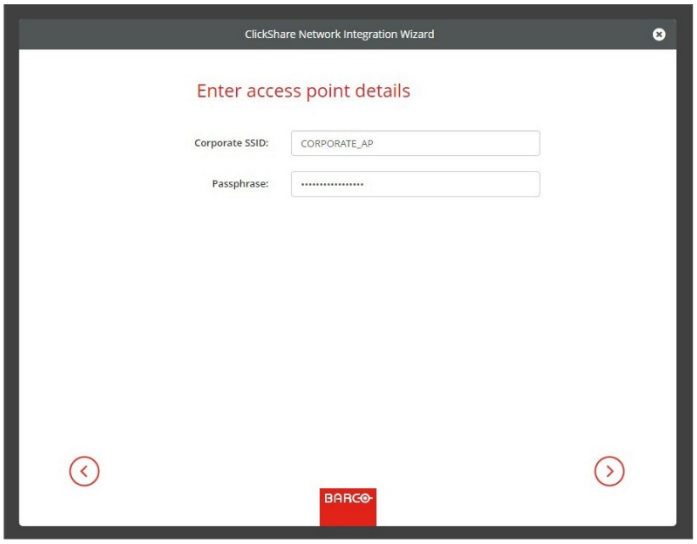
- ドメイン
- ID
- パスワード
- Corporate SSID

各設定の詳細については第 10 節「構成の詳細」をご覧ください。

[2] https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbro-admin/html/EAP-024.html

9 WPA-PSK

WPA2-PSK では個々のユーザーの識別を行いません。ワイヤレスインフラに接続する全クライアントに対して 1 個のパスワード（PSK：Pre-Shared Key（事前共有鍵））しかありません。おかげで設定が極めて簡単に行えます。接続後のクライアントと AP 間でやり取りするデータはすべて 256 ビット鍵を使用して暗号化されます。



9.1 入力

- Corporate SSID
- Pre-Shared Key（事前共有鍵）

各設定の詳細については第 10 節「構成の詳細」をご覧ください。

10 構成の詳細

ここでは設定ウィザードで遭遇するかもしれないさまざまな構成について詳しく説明していきます。本節はクイックリファレンスガイドとしてもご活用いただけます。

10.1 SCEP サーバーURL / ホスト名

これはお客様のネットワークにおいて NDES サービスを実行している Windows サーバーの IP ないしホスト名です。IIS（Internet Information Services）は HTTP と HTTPS の両方をサポートしているので、どちらを使うか指定してください。指定がない場合はデフォルトで HTTP になります。

例：http://myserver or https://10.192.5.1 or server.mycompany.com (will use http)

10.2 SCEP ユーザー名

これは社内の Active Directory のユーザーのなかで、NDES サービスへのアクセスと、チャレンジパスワードの申請に必要な許可を有している者のことです。これを確認するためには、このユーザーが CA 管理者グループに属しているか（スタンドアロン CA の場合）、あらかじめ構成された証明書テンプレート上で登録許可を有していなければなりません。

10.3 SCEP パスワード

これは SCEP ユーザー名として使用されるユーザーアカウントのパスワードです。このパスワードがベースユニットに保存されることはありません。サーバーからのチャレンジパスワードを申請するのに十分な時間だけメモリー内に保存され、その後直ちにメモリーから消去されます。

10.4 ドメイン
お客様が登録される会社ドメインはお客様の会社の Active Directory に定義されたものと一致しなければなりません。

10.5 ID
Active Directory 中のユーザーアカウントの ID で、ClickShare ボタンが社内ネットワークに接続するために使用するものです。

10.6 パスワード
社内ネットワークでの認証を受ける際に使用する ID に対応するパスワードです。ベースユニットごとに、各ボタンが同一の ID とパスワードを使用して社内ネットワークに接続します。

10.7 Corporate SSID
ClickShare ボタンが接続する社内ワイヤレスインフラの SSID です。

10.8 クライアント証明書
クライアント証明書という場合はいわゆるデバイスやマシン証明書のことで、ユーザー証明書ではありません。
クライアント証明書のアップロード用に、以下の 2 種類のフォーマットをサポートしています。

- PKCS#12（.pfx）－複数の暗号化オブジェクトを保存するためのアーカイブファイルフォーマット
- プライバシー強化メール（.pem）－Base64 でエンコードされた DER 証明書で以下の 2 つのタグの間に保存されています。
  「-----BEGIN CERTIFICATE-----」および「-----END CERTIFICATE-----」

もし与えられた PKCS#12 ファイルにも必要な CA 証明書が入っている場合、ベースユニットがそれを抽出して信頼の連鎖（トラストチェーン）を検証するので、別途 CA 証明書を提供する必要はありません。

10.9 CA 証明書
一般的な.crt ファイル拡張子をサポートします。これには Base64 でエンコードされた DER 証明書が含まれることもあります。

10.10 Pre-Shared Key（事前共有鍵）
ワイヤレスインフラ上で認証するための WPA2-PSK で使用される鍵です。これは、64 桁の 16 進数字列または 8 から 63 文字の印刷可能な ASCII 文字のパスフレーズです。

11 トラブルシューティング
ベースユニットは与えられた構成情報の入力を確認するためにできる限りの努力はしますが、それでもボタンが社内ネットワークに接続できないこともあります。いくつかの根本原因として、SSID が間違っている、SSID が利用できない、EAP の ID/パスワードが間違っている、ファイアウォール設定、VLAN 構成などが考えられます（ただしこれだけに限りません）。

ボタンが社内ネットワークに接続しようとしているときのボタンからフィードバックが欲しいときは、ClickShare クライアントのログを参照してください。
このログはクライアント実行ファイルを起動する際に[シフト]キーを押したままにすると見ることができます。
「EDSUSBDongleConnection::mpParseDongleMessages」の行を探してください。エラーコードと問題点の概要が書かれているはずです。
たとえば下に挙げるような行です。

EDSUSBDongleConnection::mpParseDongleMessages - error message Selected interface 'wlan0';bssid=00:0e:8e:3a:a8:efssid= ClickShare-CorporateCSC-1;id=0;mode=station;pairwise_cipher=CCMP;group_cipher=CCMP;key_mgmt=WPA2-PSK;wpa_state=COMPLETED;ip_address=192.168.2.2;address=00:23:a7:3a:17:bd;#012

ボタンがベースユニットまで到達できたかどうかを確認するためには、ボタンの接続と同じ方法（同じユーザー名、pw、証明書）で PC を接続し、ベースユニットのホスト名に ping を送ってください。ホスト名はベースユニットの WebUI 上で見つかります。この ping が失敗したら、IP アドレスへの ping 送信を試して、ホストネームへ ping 送信が成功するようにネットワークを調整してください。

ホスト名が解決できない場合でも問題が起こらないように、DHCP サーバー上で各ベースユニットのためのアドレスを予約しておくことを強く勧めます。