ClickShare Network Integration

アプリケーションノート

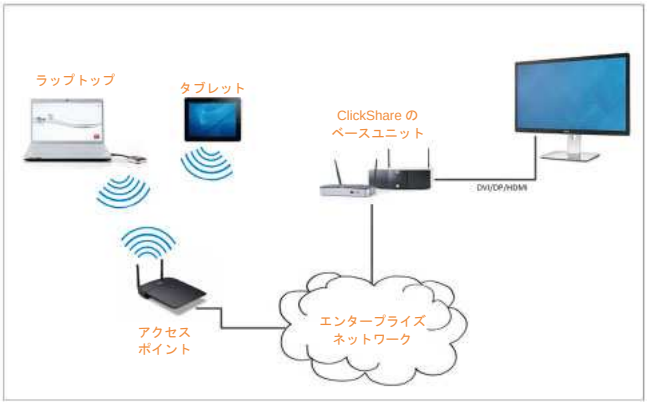
(日本語版作成：(株)内田洋行)

1　はじめに

「ClickShare Network Integration」は、既存のワイヤレスネットワークインフラと干渉することなく、より大きな組織に ClickShare を展開することを目指しています。デフォルトのスタンドアロン設定では、ClickShare ベースユニットは ClickShare ボタンが接続に使用する独自のワイヤレスアクセスポイント（AP）を作成します。これらの、いわゆる「ならず者（rogue）」AP は、より大きな設置環境では厄介者になる可能性があります。それに加えて、会議の参加者でモバイル機器からコンテンツを共有している人達は、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る必要があります。

ここが ClickShare Network Integration の出番です。いったんその構成が完了し動作を始めると、ベースユニットの内蔵 AP は無効化されます。そうすればボタンまたはモバイル機器は、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となります。この時点では､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､ベースユニットは有線イーサネットインタフェースを介して社内ネットワークに接続されていなければなりません。

本書の以下の節では、これらすべての設定方法について議論し、内部の詳細について少しばかり詳しく説明します。



2　セキュリティモード

社内ネットワークに接続するために、2 種類のセキュリティモードがボタンによってサポートされています。

- 最初のものは通常の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**です。
- より伝統的な Wi-Fi 設定を使用する可能性のあるもっと小さい組織もサポートしたいので、**WPA2 パーソナル**とも呼ばれる WPA2-PSK もサポートされます。

どちらのモードも WPA（Wi-Fi Protected Access）に基づいています。本書では、元の WPA 規格の改良版で、セキュリティ強化のため AES 暗号化を追加した WPA2 について説明します。

2.1　WWPA2 エンタープライズ、802.1X 認証

WWPA2 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（RADIUS を使用した）サーバーに依存しています。そのために、802.1x 認証（ポートベースのネットワークアクセス制御とも呼ばれています）を使用します。802.1x 認証ではローカルエリアネットワーク上で使用するため EAP（Extensible Authentication Protocol : 拡張認証プロトコル）をカプセル化します。これはまた､「EAP over LAN」や EAPoL とも呼ばれます。ネットワーク上のクライアント機器－ClickShare の場合これらはボタンとなりますが－を認証するために、これらの EAPoL メッセージは RADIUS を使用してネットワーク内を通されます。

802.11i（WPA2）規格は必要な EAP 方式の数を定義しています。しかしそれらのすべてが実際に幅広く使用されているわけではなく、（規格に収められていない）他のいくつかのものがもっと頻繁に使用されています。したがって、われわれは最も広く使用されている EAP 方式を選択しました。ClickShare システムがサポートする EAP 方式のリストは次のとおりです。

- EAP-TLS
- PEAP
- EAP-TTLS

それぞれについての詳細と設定方法は本アプリケーションノートの後の方に記されています。

3 考察

ClickShare システムを貴社の社内ネットワークに統合すると決定した場合、まず考慮すべきことがいくつかあります。最初に、貴社のベースユニットのすべて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可能であることを確認してください。また、キャプチャされたスクリーンの内容をベースユニットへストリーム配信するために各ボタンが必要とする帯域幅を考慮してください。通常は 5〜15 Mbpsの範囲のどこかです。したがって、帯域幅不足のためClickShareの使用感を低下させる貴社ネットワークのボトルネック（例：100Mbps スイッチ）を防止してください。

4 前提条件

ClickShare Network Integration を展開する前に、貴社のインフラが次の前提条件を満たしていることを確認してください。

4.1 ネットワーク

社内ネットワークをいったん有効にすると 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。ご使用のベースユニットが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されていることを確認してください。

4.2 ファイアウォール

ClickShare ボタン経由またはモバイル機器から、ベースユニットに確実にコンテンツ共有が可能となるように、ネットワーク上で以下のポートが開いていることを確認してください。

送信元	CSM ベースユニット	CSC ベースユニット
ClickShare ボタン	TCP：1688-1689；3268；8080； UDP：1047-1049	TCP：9876
ClickShare Presenter (iOS)	TCP/UDP：9870	TCP/UDP：9870
ClickShare Presenter (Android)	TCP/UDP：9870	TCP/UDP：9870
AirPlay	n/a	TCP：7000；7100；47000；4100-4200； UDP：4100；4200

4.3 VLAN

多数の社内ネットワークが複数の VLAN に分割されています。これはたとえば、「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にです。貴社のネットワークに ClickShare を統合する際にはこのことを考慮してください。貴社のワイヤレスインフラに接続する ClickShare ボタンは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 Apps を使用したければそれらもベースユニットにアクセスできる必要があります。

4.4 DNS

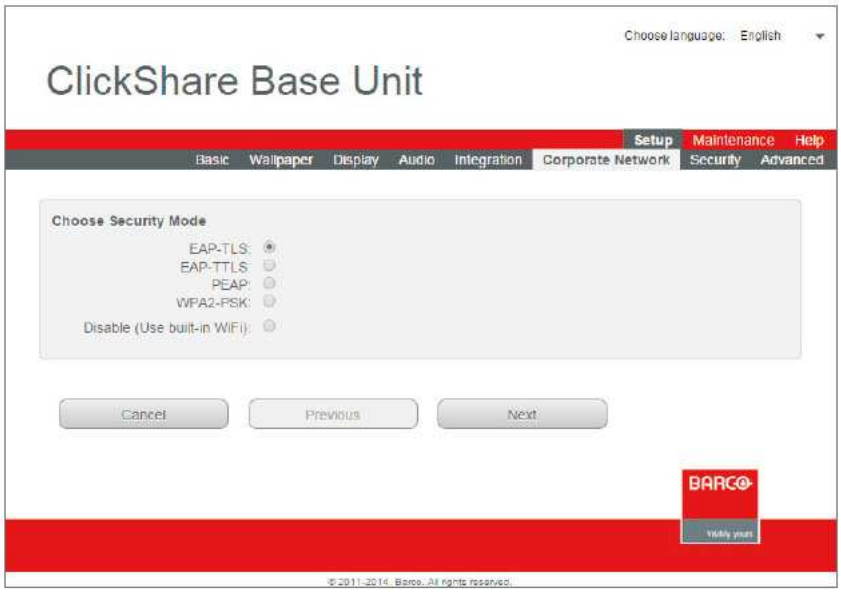
ボタンがそのコンテンツをベースユニットにストリーム配信できるためには、ボタンがベースユニットのホスト名をネットワーク内で解決できなければなりません。

4.5 NTP

EAP-TLS を使用する場合には、ベースユニット上に NTP を設定する必要があります。これはベースユニットの WebUI を使用してできます。EAP-TLS に必要な証明書を処理するためにベースユニットは正しい時刻を示すことが必要です。なるべく、ローカルな社内ネットワーク上の可用性の高い NTP サーバーを使用すべきです。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ことに注意して下さい。

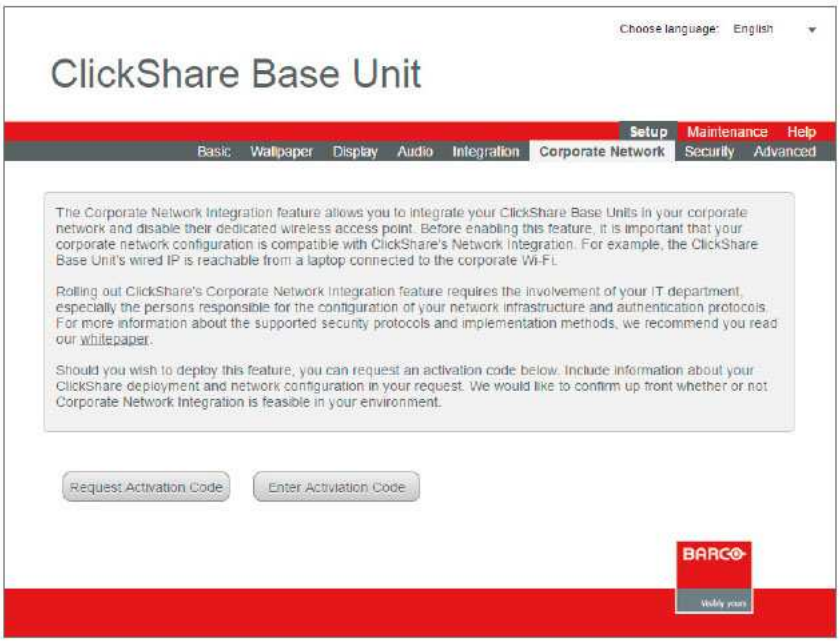
5　設定

設定を容易にするため、ClickShare　WebUI 中にウィザードを用意しました。このウィザードはお客様が選択されたセキュリティモードに従って設定プロセスでのガイドを行います。さらに、サポートされているセキュリティモード、ならびにすべてのものを統合し動作させるために必要な、入力に関する概要と説明も与えられます。



5.1　アクティベーション

ClickShare Network Integration 機能が複雑なので、まず最初にアクティベーションを行う必要があります。そのためには、ベースユニットの WebUI で［Corporate Network（社内ネットワーク）］タブを選択し、request（申請）ページに移動するボタンをクリックしてください。貴社の ClickShare の配備およびネットワーク構成に関する詳細データを入力してください。貴社からのご依頼を受領後、貴社の環境にて ClickShare Network Integration 機能の有効化が可能かどうか当社にて確認します。もし可能であれば、アクティベーションコードをお送りしますのでベースユニットの WebUI に入力してこの機能にアクセスできるようにしてください。



5.2 セキュリティ方式

次の 4 つの節ではサポートされるセキュリティ方式のそれぞれを詳細に説明します。貴社の環境に適合するものをご参照ください。

5.3 ポスト設定

設定ウィザードの完了後、ClickShare ボタンをすべて再ペアリングしなければならないことに注意して下さい。再ペアリング前では、ベースユニット上で旧スタンドアロンモードが依然として動作中で、共有が不可能となっています。

5.4 Apps

いったんネットワークに統合されると、社内ネットワークに接続された任意のモバイル機器は、ネットワーク上の任意のベースユニットとコンテンツを共有することが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 で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。）

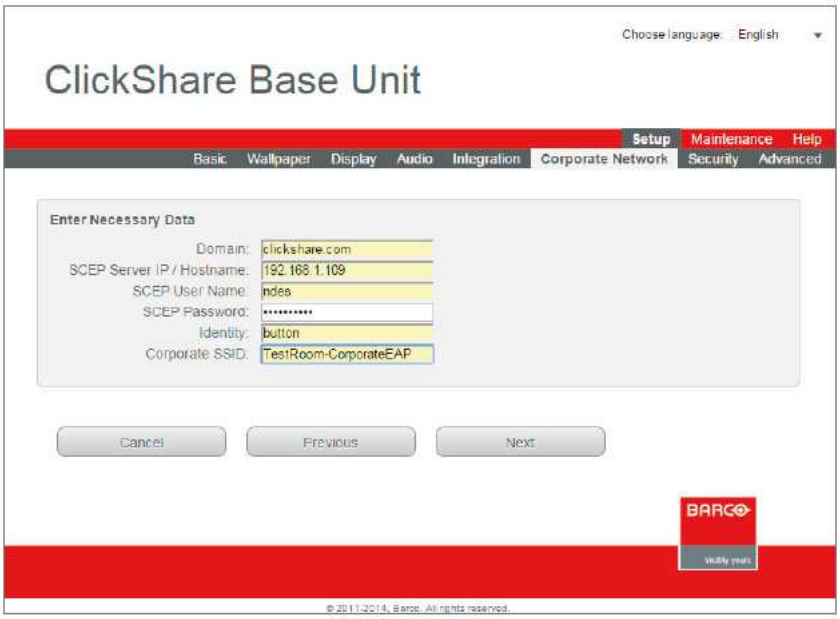
6 EAP-TLS

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 PKI（Public Key Infrasructure：公開鍵基盤）が必要です。（もしこれは貴社組織にとって障害が大きすぎるということであれば、EAP-TTLS や PEAP が代わりに使用できます）。規格では X.509 クライアント証明書は厳密には不要ですが、当社のものを含めて大部分の実装では必須とされています。

クライアントの証明書を使用して実装した場合、EAP-TLS は最も安全な EAP 方式の一つであると考えられています。PEAP や EAP-TTLS と比較した場合、EAP-TLS の唯一の些細な欠点は、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 またはマニュアル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

SCEP（Simple Certificate Enrolment Protocol）はスケーラブルな方法で証明書の発行と破棄を可能とします。当社では、ClickShare のベースユニットとボタンをより素早くかつ円滑に社内ネットワークに統合できるよう、SCEP のサポートを追加しました。ほとんど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：Active Directory）を使用してユーザーと機器の管理を行っているので、当社の SCEP 実装は特に、Windows Server 2008 R2 および 2012 に含まれている 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。現時点では、他の SCEP サーバー実装はどれも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 を使用して EAP-TLS を有効にする場合には、貴社の Windows Server 上で NDES が有効化および設定され、動作中であることを確認してください。NDES 設定に関する詳細は、マイクロソフト社のインターネットサイトをご覧ください[1]。

SCEP は登録申請を認証するために、いわゆる「challenge password」を使用します。NDES に対しては、この challenge は貴社サーバーの http(s)://[貴社サーバーのホスト名]/CertSrv/mscep_admin から取り出すことができます。必要な資格情報を設定ウィザードに入力する場合、ベースユニットはこの challenge 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。このようにして手続きを完全自動化します。

6.1.2 マニュアルで証明書を提供

貴社の現在の構成が SCEP をサポートしない、または SCEP は使いたくないけれども EAP-TLS が提供する相互認証の恩恵は受けたい場合は、必要な証明書をマニュアル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
- 社内 SSID

各設定の詳細説明は第 10 節「構成の詳細」をご覧ください。

[1] NDES 白書（英文）：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 マニュアルで証明書を提供

貴社の現在の構成が SCEP をサポートしない、または SCEP は使いたくないけれども EAP-TLS が提供する相互認証の恩恵は受けたい場合は、必要な証明書をマニュアルでアップロードすることも可能です。

6.2.1 クライアント証明書

お客様が提供するクライアント証明書は貴社ドメイン内の正式なルート CA の署名が必要であり、ID フィールドで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、お客様が提供するクライアント証明書にはプライベート鍵が含まれていることを確認してください。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。

6.2.2 CA 証明書

CA 証明書は貴社ドメインでの正式なルート CA の証明書であり、EAP-TLS 接続の設定に使用されます。ウィザードの際、ベースユニットはお客様が提供されたクライアント証明書と CA 証明書間の信頼の連鎖を確証できることを保証します。

6.2.3 入力

SCEP を使用して EAP-TLS 構成を正しく設定するためには以下のデータが必要です。

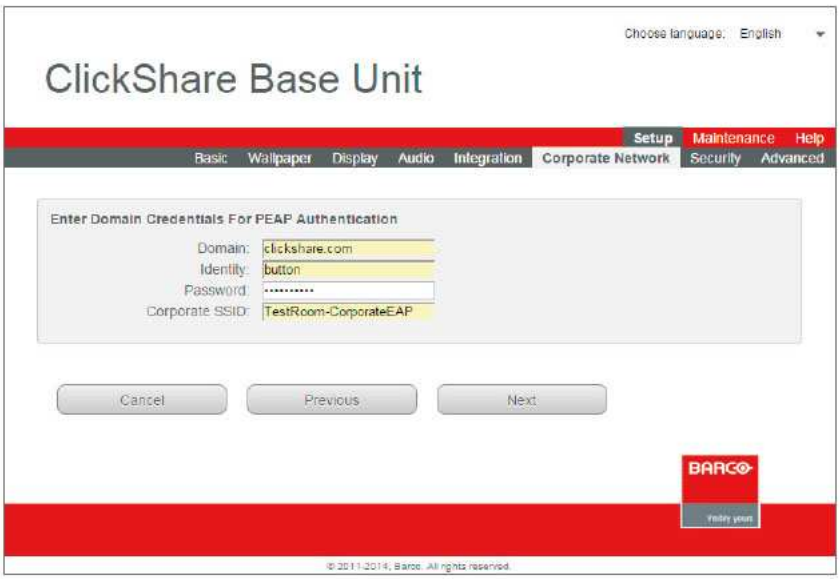
- クライアント証明書
- CA 証明書
- ドメイン
- ID
- 社内 SSID

各設定の詳細説明は第 10 節「構成の詳細」をご覧ください。

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 セキュリティ社が共同で開発した EAP の実装です。PEAP はサーバーの CA 証明書を使用して安全な TLS トンネルを設定し、その後トンネル内で実際のユーザー認証を行います。この処理法では、ユーザー認証の際に PKI が不要で、かつ TLS のセキュリティを使用することが可能となります。

この規格ではトンネル内で認証を行うためにどの方式を使用するかを規定していません。しかし本アプリケーションノートでは、PEAP に関しては内部認証方式として EAP-MSCHAPv2 付の PEAPv0 を指すこととします。これは、WPA および WPA2 規格中の 2 つの認定された PEAP 実装の内の 1 つであり、圧倒的に最も一般的で広く普及した PEAP の実装です。



7.1 入力

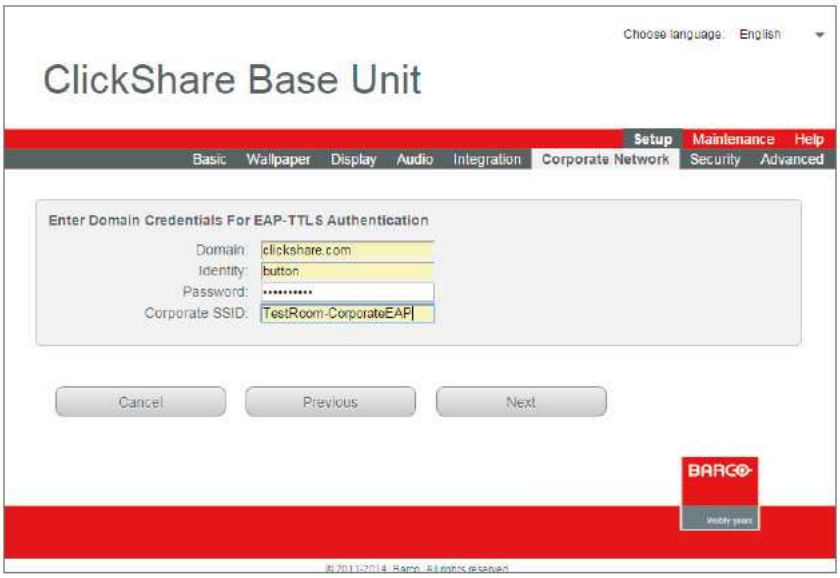
- ドメイン
- ID
- パスワード
- 社内 SSID

各設定の詳細説明は第 10 節「構成の詳細」をご覧ください。

8 EAP-TTLS

EAP-TTLS（Tunneled Transport Layer Security）は Juniper[2]ネットワークによる EAP の実装です。これは EAP-TLS と同程度の強度の認証を提供することを意図して作成されましたが、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。ユーザー認証は、社内 LAN で既に使用中のものと同一のセキュリティデータベースに対して行われます。たとえば、SQL または LDAP データベース、またはトークンシステムです。

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ので、これに対するサポートは含まれていません。ユーザーごとのクライアント証明書を使用したいのであれば、代わりに EAP-TLS を使用することを提案します。



8.1 入力

- ドメイン
- ID
- パスワード
- 社内 SSID

各設定の詳細説明は第 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-sbrc-admin/html/EAP-024.html

9 WPA-PSK

WPA2-PSKは個々のユーザーの識別は行いません。ワイヤレスインフラに接続する全ユーザーに対して1個のパスワード(PSK:Pre-Shared Key(事前共有鍵))があるのみです。これにより設定が簡単明瞭になります。接続後は、クライアントと AP 間で送信されるすべてのデータは 256 ビット鍵を使用して暗号化されます。

9.1 入力

- 社内 SSID
- 事前共有鍵（PSK）

各設定の詳細説明は第 10 節「構成の詳細」をご覧ください。

10 構成の詳細

本節は一種のクイックリファレンスガイドとして使用可能です。ここでは設定ウィザードで遭遇する可能性のあるさまざまな構成について、より詳しく説明します。

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で NDES サービスを実行している Windows サーバーの IP またはホスト名です。IIS（Internet Information Services）は HTTP と HTTPS の双方をサポートしているので 2 つの内のどちらを使用するのかを指定してください。指定がないと、デフォルトで HTTP になります。

例：http://myserver、または https://10.192.5.1、または server.mycompany.com（http を使用）

10.2 SCEP ユーザー名

これは貴社の Active Directory のユーザーで、NDES サービスへアクセスし challenge パスワードを申請するのに必要な許可を有しているユーザーです。これを確認するには、当該ユーザーは CA 管理者グループに属するか（スタンドアロン CA の場合）、または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。このパスワードは決してベースユニットには保存されません。サーバーからの Challenge パスワードを申請するのに十分な時間だけメモリに保存され、その後直ちにメモリから消去されます。

10.4 ドメイン

お客様が登録される会社ドメインは貴社の 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。When using

10.6 パスワード

社内ネットワーク上で認証するのに使用する ID 用のパスワードです。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 社内 SSID

ClickShare ボタンが接続され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のアップロード用に 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 証明書が含まれていれば、ベースユニットはそれを抽出して信頼の連鎖を検証し、あらためて CA 証明書を提供しなくても済むようにします。

10.9 CA 証明書

通常の.crt ファイル拡張子がサポートされ、Base64 でエンコードされた DER 証明書を含むことができます。

10.10 事前共有鍵（PSK）

ワイヤレスインフラに認証するための 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についての入力を有効化するために最善を尽くしますが、ボタンが依然として貴社の社内ネットワークに接続できない可能性があります。これに対しては次のものを始めとするいくつかの潜在的根本原因が存在します。つまり、間違った SSID、SSID が利用不可能、間違った EAP の ID / パスワード、ファイアウォール設定、VLAN 構成等、

ボタンが貴社の社内ネットワークに接続しようとしている際に、ボタンからのフィードバックを得るためには 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］キーを押すことにより有効化されます。「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短く記されているはずです。