クライアント証明書を使用したSMTPセッションの認証

この章は、次の項で構成されています。

証明書と SMTP 認証の概要

E メール セキュリティ アプライアンスは、E メール セキュリティ アプライアンスとユーザのメール クライアント間の SMTP セッションを認証するためにクライアント証明書の使用をサポートします。E メール セキュリティ アプライアンスは、アプリケーションがメッセージを送信するためにアプライアンスに接続しようとするときに、ユーザのメール クライアントからのクライアント証明書を要求することができます。アプライアンスがクライアント証明書を受け取ったとき、証明書が有効である、有効期限が切れていない、無効になっていないことを確認します。証明書が有効であれば、E メール セキュリティ アプライアンスは TLS 経由でメール アプリケーションからの SMTP 接続を許可します。

ユーザがメール クライアントに Common Access Card（CAC）を使用する必要がある組織では、CAC および ActivClient のミドルウェア アプリケーションがアプライアンスに提供する証明書を要求するために、この機能を使用して E メール セキュリティ アプライアンスを設定できます。

メールの送信時にユーザに証明書を提供することを要求するように E メール セキュリティ アプライアンスを設定できますが、ここでは特定のユーザに対する例外を許可します。これらのユーザには、ユーザの認証に SMTP 認証 LDAP クエリーを使用するようにアプライアンスを設定できます。

ユーザはセキュア接続（TLS）経由でメッセージを送信するために自分のメールクライアントを設定し、アプライアンスからサーバ証明書を受け入れる必要があります。

関連項目

- クライアント証明書でのユーザの認証方法 （2 ページ）
- SMTP 認証 LDAP クエリでのユーザの認証方法 （2 ページ）
- クライアント認証が無効な場合の LDAP SMTP 認証クエリでのユーザの認証方法 （3 ページ）

クライアント証明書でのユーザの認証方法

表 *1*: クライアント証明書でのユーザの認証方法

	操作内容	詳細
ステップ 1	LDAP サーバの認証クエリを定義します。	クライアント証明書の有効性の確認 （3 ページ）
ステップ 2	証明書ベースの SMTP 認証プロファイルを作成します。	クライアント証明書を使用した TLS 経由の SMTP 接続の認証 （5 ページ）
ステップ 3：	証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。	Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング
ステップ 4：	TLS、クライアント認証および SMTP 認証を要求するように RELAYED メール フロー ポリシーを変更します。	アプライアンスからの TLS 接続の確立 （5 ページ）

SMTP 認証 LDAP クエリでのユーザの認証方法

表 *2*: *SMTP* 認証 *LDAP* クエリでのユーザの認証方法

	操作内容	詳細
ステップ 1	許可クエリー文字列と認証方式のバインドを使用する、サーバの SMTP 認証クエリーを定義します。	LDAP ディレクトリを使用したユーザの認証 （4 ページ）
ステップ 2	LDAP ベースの SMTP 認証プロファイルを作成します。	SMTP 認証を行うための AsyncOS の設定
ステップ 3：	LDAP の SMTP 認証プロファイルを使用するようにリスナーを設定します。	ユーザが接続で LDAP ベースの SMTP 認証の使用を許可されていない場合は、アプライアンスが接続拒否するか、すべてのアクティビティを記録する間一時的に許可するかを選択します。

	操作内容	詳細
ステップ 4：	TLS および SMTP 認証を要求するように RELAYED メール フロー ポリシーを変更します。	アプライアンスからの TLS 接続の確立 （5 ページ）

クライアント認証が無効な場合の LDAP SMTP 認証クエリでのユーザの認証方法

表 *3*：クライアント認証または *LDAP SMTP* 認証クエリーでのユーザの認証方法

	操作内容	詳細
ステップ 1	許可クエリー文字列と認証方式のバインドを使用する、サーバの SMTP 認証クエリーを定義します。	LDAP ディレクトリを使用したユーザの認証 （4 ページ）
ステップ 2	LDAP サーバの認証ベースのクエリーを定義します。	クライアント証明書の有効性の確認 （3 ページ）
ステップ 3：	証明書ベースの SMTP 認証プロファイルを作成します。	クライアント証明書を使用した TLS 経由の SMTP 接続の認証 （5 ページ）
ステップ 4：	LDAP の SMTP 認証プロファイルを作成します。	SMTP 認証を行うための AsyncOS の設定
ステップ 5：	証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。	Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング
ステップ 6：	1. 次の設定を使用するように RELAYED メール フロー ポリシーを変更します。 2. TLS 推奨 3. SMTP 認証必須 4. SMTP 認証のために TLS が必要	アプライアンスからの TLS 接続の確立 （5 ページ）

クライアント証明書の有効性の確認

ユーザのメール クライアントと E メール セキュリティ アプライアンス間の SMTP セッションを認証するために、証明書認証 LDAP クエリーはクライアント証明書の有効性をチェックします。このクエリを作成する際に、認証のための証明書フィールドのリストを選択して、ユーザ ID 属性（デフォルトは uid）を指定して、クエリ文字列を入力します。

たとえば、証明書の共通名とシリアル番号を検索するクエリー文字列は、**`(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})`** のようになります。クエリーを作成した後で、証明書 SMTP 認証プロファイルで使用できます。この LDAP クエリーは、OpenLDAP、Active Directory および Oracle Directory をサポートします。

LDAP サーバの設定の詳細については、LDAP クエリを参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2 新しい LDAP プロファイルを作成します。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成を参照してください。

ステップ 3 [認証クエリーを証明（Certificate Authentication Query）] チェックボックスをオンにします。

ステップ 4 クエリー名を入力します。

ステップ 5 ユーザの証明書を認証するためのクエリー文字列を入力します。たとえば、**(&(objectClass=user)(cn={cn}))** と入力します。

ステップ 6 **sAMAccountName** などのユーザ ID 属性を入力します。

ステップ 7 変更を送信し、保存します。

LDAP ディレクトリを使用したユーザの認証

SMTP 認証 LDAP クエリーには、E メール セキュリティ アプライアンスがユーザのメール クライアントが LDAP ディレクトリのユーザのレコードに基づいてアプライアンスを介してメール送信できるかを判断する、許可クエリー文字列が含まれています。これは、レコードに許可することが指定してされていれば、クライアントの証明書のないユーザがメールを送信することが可能です。

その他の属性に基づいた結果のフィルタリングもできます。たとえば、`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` というクエリー文字列は、次の条件のいずれかがユーザに当てはまるかどうかチェックします。

- CAC がユーザに発行されていない（`caccn=*`）
- CAC が免除される（`cacexempt=*`）
- CAC なしで一時的にユーザがメールを送信できる期間が将来切れる（`cacemergency>={t}`）

SMTP 認証クエリーの使用の詳細については、SMTP 認証を行うための AsyncOS の設定を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2 LDAP プロファイルを定義します。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成を参照してください。

ステップ 3 LDAP プロファイルの SMTP 認証クエリーを定義します。

ステップ 4 [SMTP 認証クエリー（SMTP Authentication Query）] チェックボックスをオンにします。

ステップ 5 クエリー名を入力します。

ステップ 6 ユーザの ID を問い合わせる文字列を入力します。たとえば、`(uid={u})`。

ステップ 7 認証方式に [LDAP BIND] を選択します。

ステップ 8 許可クエリー文字列を入力します。たとえば、
`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。

ステップ 9 変更を送信し、保存します。

クライアント証明書を使用した TLS 経由の SMTP 接続の認証

証明書ベースの SMTP 認証プロファイルでは、E メール セキュリティ アプライアンスがクライアント証明書を使用して TLS 経由の SMTP 接続を認証できます。プロファイルを作成する場合、証明書を確認するために使用する証明書認証LDAP クエリーを選択します。また、クライアント証明書が使用できなかった場合、E メール セキュリティ アプライアンスがユーザ認証するための **`SMTP AUTH`** コマンドにフォールバックするかどうかを指定できます。

LDAP を使用した SMTP 接続の認証の詳細については、SMTP 認証を行うための AsyncOS の設定を参照してください。

手順

ステップ 1 [ネットワーク（Network）] > [SMTP 認証（SMTP Authentication）] を選択します。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 SMTP 認証プロファイルの名前を入力します。

ステップ 4 [プロファイルタイプ（Profile Type）] で [証明書（Certificate）] を選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 プロファイル名を入力します。

ステップ 7 この SMTP 認証プロファイルに使用する証明書 LDAP クエリーを選択します。

（注） クライアント証明書が使用可能でない場合、SMTP AUTH コマンドを許可するオプションを選択しないでください。

ステップ 8 [終了（Finish）] をクリックします。

ステップ 9 変更を送信し、保存します。

アプライアンスからの TLS 接続の確立

RELAYED メール フロー ポリシーの [クライアント証明書の検証（Verify Client Certificate）] オプションは、クライアント証明書が有効な場合ユーザのメール アプリケーションへの TLS 接続を確立するように、E メール セキュリティ アプライアンスに指示します。TLS 推奨設定

にこのオプションを選択した場合、ユーザが証明書を持たない場合にもアプライアンスは非TLS接続を許可しますが、ユーザが無効な証明書を持つ場合は、接続を拒否します。TLS必須設定の場合、このオプションを選択すると、アプライアンスが接続を許可するために有効な証明書が必要になります。

クライアント証明書を持つユーザの SMTP セッションを認証するには、次の設定を選択します。

- TLS 必須（TLS - Required）
- クライアント証明書の検証（Verify Client Certificate）
- SMTP 認証が必要（Require SMTP Authentication）

（注） SMTP認証は必須ですが、Eメール セキュリティ アプライアンスは証明書認証を使用しているため、SMTP 認証 LDAP クエリーを使用しません。

クライアント証明書の代わりにSMTP認証クエリーを使用して、ユーザのSMTPセッションを認証するには、次の RELAYED メール フロー ポリシーの設定を選択します。

- TLS 必須（TLS - Required）
- SMTP 認証が必要（Require SMTP Authentication）

他のユーザからのLDAPベースのSMTP認証を許可する一方で、特定のユーザからのクライアントの認証を要求するようにE メール セキュリティ アプライアンスに要求するには、次の RELAYED メール フロー ポリシーの設定を選択します。

- TLS 推奨（TLS - Preferred）
- SMTP 認証が必要（Require SMTP Authentication）
- TLS に SMTP 認証を提供するよう義務付けます。

無効にされた証明書のリストの更新

E メール セキュリティ アプライアンスは、ユーザの証明書が失効していないことを確認するために、証明書検証の一環として（証明書失効リストと呼ばれる）失効した証明書のリストを確認します。サーバ上でこのリストを最新のバージョンに保ち、E メール セキュリティ アプライアンスはユーザが作成したスケジュールでこれをダウンロードします。

手順

ステップ 1 [ネットワーク（Network）] > [CRL ソース（CRL Sources）] に移動します。

ステップ 2 SMTP TLS 接続のため CRL チェックをイネーブルにします。

a) [グローバル設定（Global Settings）] で [設定を編集（Edit Settings）] をクリックします。

b) （省略可能）すべてのオプションを選択する場合、[グローバル設定（Global Settings）] チェック ボックスを選択します。

- インバウンドSMTP TLSのCRLチェック（CRL check for inbound SMTP TLS）。
- アウトバウンドSMTP TLSのCRLチェック（CRL check for outbound SMTP TLS）
- WebインターフェイスのCRLチェック（CRL Check for Web Interface）

c) [インバウンドSMTP TLSのCRLチェック（CRL check for inbound SMTP TLS）]、[アウトバウンドSMTP TLSのCRLチェック（CRL check for outbound SMTP TLS）] または [WebインターフェイスのCRLチェック（CRL Check for Web Interface）] オプションのいずれかのチェック ボックスを選択します。

d) 変更を送信します。

ステップ 3 [CRL ソースの追加（Add CRL Source）] をクリックします。

ステップ 4 CRL ソースの名前を入力します。

ステップ 5 ファイル タイプを選択します。ASN.1 または PEM を指定できます。

ステップ 6 ファイル名を含むファイルのプライマリ ソースの URL を入力します。たとえば、**`https://crl.example.com/certs.crl`**

ステップ 7 アプライアンスがプライマリ ソースに接続できない場合は、必要に応じて 2 番めのソースの URL を入力します。

ステップ 8 CRL ソースをダウンロードするスケジュールを指定します。

ステップ 9 CRL ソースをイネーブルにします。

ステップ 10 変更を送信し、保存します。

クライアント証明書を使用したユーザの SMTP セッションの認証

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] に移動して、LDAP サーバ プロファイルを設定します

ステップ 2 LDAP プロファイルの証明書クエリーを定義します。

a) クエリー名を入力します。

b) 認証する証明書フィールド（シリアル番号、共通名など）を選択します。

c) クエリー文字列を入力します。たとえば、**`(&(caccn={cn})(cacserial={sn}))`**。

d) uid などのユーザ ID フィールドを入力します。

e) 変更を送信します。

ステップ 3 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] に移動し、証明書 SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。

b) 使用する証明書 LDAP クエリーを選択します。

c) クライアント証明書が使用可能でない場合、**SMTP AUTH** コマンドを許可するオプションを選択しないでください。
d) 変更を送信します。

ステップ 4 [ネットワーク（Network）] > [リスナー（Listener）] に移動して、作成した証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。

ステップ 5 TLS、クライアント認証およびSMTP認証を要求するようにRELAYEDメールフローポリシーを変更します。

（注） SMTP認証は必須ですが、Eメールセキュリティアプライアンスは証明書認証を使用しているため、SMTP 認証 LDAP クエリーを使用しません。E メール セキュリティ アプライアンスは、ユーザを認証するためにメールアプリケーションからのクライアント証明書を要求します。

ステップ 6 変更を送信し、保存します。

SMTP AUTH コマンドを使用したユーザの SMTP セッションの認証

E メール セキュリティ アプライアンスでは、クライアント証明書の代わりに SMTP AUTH コマンドを使用してユーザのSMTPセッションを認証することができます。ユーザが接続でSMTP AUTH の使用を許可されていない場合は、アプライアンスが接続拒否するか、すべてのアクティビティを記録する間一時的に許可するかを選択できます。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] に移動して、LDAP サーバ プロファイルを設定します。

ステップ 2 LDAP プロファイルの SMTP 認証クエリーを定義します。

a) クエリー名を入力します。
b) クエリー文字列を入力します。たとえば、**(uid={u})**。
c) 認証方式として [LDAP BIND] を選択します。
d) 許可クエリー文字列を入力します。たとえば、**(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))**。
e) 変更を送信します。

ステップ 3 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] に移動し、LDAP SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。
b) 使用する SMTP 認証 LDAP クエリーを選択します。
c) [ユーザがSMTP AUTHコマンドを使用できるかどうかをLDAPで確認する （Check with LDAP if user is allowed to use SMTP AUTH Command）] を選択し、ユーザのアクティビティをモニタして報告することを選択します。
d) 変更を送信します。

ステップ 4 [ネットワーク（Network）] > [リスナー（Listener）] に移動して、作成した LDAP SMTP 認証プロファイルを使用するようにリスナーを設定します。

ステップ 5 TLS および SMTP 認証を要求するように RELAYED メール フロー ポリシーを変更します。

ステップ 6 変更を送信し、保存します。

クライアント証明書または SMTP AUTH を使用したユーザの SMTP セッションの認証

この設定では、E メール セキュリティ アプライアンスが、クライアント証明書を持つユーザに対してはクライアント認証を要求し、クライアント認証を持たないユーザまたは電子メールの送信にクライアント認証を使用できないユーザに対しては SMTP AUTH を許可する必要があります。

許可されていないユーザによる SMTP AUTH コマンドの使用は禁止されます。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] に移動して、LDAP サーバ プロファイルを設定します。

ステップ 2 プロファイルの SMTP 認証クエリーを定義します。

a) クエリー名を入力します。
b) クエリー文字列を入力します。たとえば、**(uid={u})**。
c) 認証方式として [LDAP BIND] を選択します。
d) 許可クエリー文字列を入力します。たとえば、**(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))**。

ステップ 3 LDAP プロファイルの証明書クエリーを定義します。

a) クエリー名を入力します。
b) 認証するクライアント証明書フィールド（シリアル番号、共通名など）を選択します。
c) クエリー文字列を入力します。たとえば、**(&(caccn={cn})(cacserial={sn}))**。
d) uid などのユーザ ID フィールドを入力します。
e) 変更を送信します。

ステップ 4 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] に移動し、LDAP SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。
b) 使用する SMTP 認証 LDAP クエリーを選択します。
c) [ユーザがSMTP AUTHコマンドを使用できるかどうかをLDAPで確認する（Check with LDAP if user is allowed to use SMTP AUTH Command）] を選択し、接続を拒否することを選択します。

d) カスタム SMTP AUTH 応答を入力します。たとえば 525, “Dear user, please use your CAC to send email.” と入力します。
e) 変更を送信します。

ステップ 5 証明書 SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。
b) 使用する証明書 LDAP クエリーを選択します。
c) クライアント証明書が使用可能でない場合、SMTP AUTH コマンドを許可するオプションを選択します。
d) ユーザにクライアント証明書がない場合にアプライアンスが使用する LDAP SMTP 認証プロファイルを選択します。
e) 変更を送信します。

ステップ 6 [ネットワーク（Network）] > [リスナー（Listener）] に移動して、作成した証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。

ステップ 7 RELAYED メール フロー ポリシーを変更して次のオプションを選択します。

- TLS 推奨
- SMTP 認証必須
- SMTP 認証のために TLS が必要

ステップ 8 変更を送信し、保存します。