他の MTA との暗号化通信

この章は、次の項で構成されています。

- 他の MTA との暗号化通信の概要 （1 ページ）
- 証明書の使用 （2 ページ）
- リスナー HAT の TLS の有効化 （8 ページ）
- 配信時の TLS および証明書検証の有効化 （11 ページ）
- 名前付きエンティティの DNS ベースの認証 （15 ページ）
- 認証局のリストの管理 （19 ページ）
- HTTPS の証明書のイネーブル化 （22 ページ）

他の MTA との暗号化通信の概要

エンタープライズゲートウェイ（またはメッセージ転送エージェント、つまり MTA）は通常、インターネット上で「素性が判別している相手」と通信します。つまり、通信は暗号化されません。場合によっては、悪意のあるエージェントが、送信者または受信者に知られることなく、この通信を傍受する可能性があります。通信は第三者によってモニタされる可能性や、変更される可能性さえあります。

Transport Layer Security（TLS）はセキュア ソケット レイヤ（SSL）テクノロジーを改良したバージョンです。これは、インターネット上での SMTP カンバセーションの暗号化に広く使用されているメカニズムです。AsyncOS では SMTP への STARTTLS 拡張（セキュアな SMTP over TLS）がサポートされます。詳細については、RFC 3207 を参照してください（これは、廃止になった RFC 2487 に代わるバージョンです）。

AsyncOS の TLS 実装では、暗号化によってプライバシーが確保されます。これによって、X.509 証明書および証明書認証サービスからの秘密キーをインポートしたり、アプライアンス上で使用する自己署名証明書を作成したりできます。AsyncOS では、パブリック リスナーおよびプライベート リスナーに対する個々の TLS 証明書、インターフェイス上の セキュア HTTP（HTTPS）管理アクセス、LDAP インターフェイス、およびすべての発信 TLS 接続がサポートされます。

関連項目

- TLS を使用した SMTP カンバセーションの暗号化方法 （2 ページ）

TLS を使用した SMTP カンバセーションの暗号化方法

TLS を使用した SMTP カンバセーションの暗号化方法

	操作内容	詳細
ステップ 1	公認の認証局からの X.509 証明書と秘密キーを取得します。	証明書の使用 （2 ページ）
ステップ 2	E メール セキュリティ アプライアンスに証明書をインストールします。	次のいずれかで証明書をインストールします。 • 自己署名証明書の作成 （5 ページ） • 証明書のインポート （7 ページ）
ステップ 3：	メッセージ受信用、またはメッセージ配信用、またはその両方の TLS をイネーブルにします。	• リスナー HAT の TLS の有効化 （8 ページ） • 配信時の TLS および証明書検証の有効化 （11 ページ）
ステップ 4：	（任意）リモート ドメインからの証明書を検証し、ドメインのクレデンシャルを確立するためにアプライアンスが使用する信頼できる認証局のリストをカスタマイズします。	認証局のリストの管理 （19 ページ）
ステップ 5：	（任意）TLS 接続が必要なドメインにメッセージを送信できない場合に警告を送信するよう E メール セキュリティ アプライアンスを設定します。	要求された TLS 接続が失敗した場合のアラートの送信 （14 ページ）

証明書の使用

TLS を使用するには、E メール セキュリティ アプライアンスに対する受信および配信のための X.509 証明書および一致する秘密キーが必要です。SMTP での受信および配信の両方には同じ証明書を使用し、インターフェイス（LDAP インターフェイス）上での HTTPS サービスや宛先ドメインへのすべての発信 TLS 接続には別の証明書を使用することも、それらのすべてに対して 1 つの証明書を使用することもできます。

certconfig を使用して証明書を設定した後で、Web インターフェイスの [ネットワーク（Network）] > [証明書（Certificates）] ページおよび CLI の print コマンドを使用して証明書の

リスト全体を表示できます。print コマンドでは中間証明書が表示されないことに注意してください。

⚠

注意 アプライアンスには TLS および HTTPS 機能がテスト済みであることを示すデモ証明書が同梱されますが、デモ証明書付きのサービスのいずれかをイネーブルにすることはセキュアではないため、通常の使用には推奨できません。デフォルトのデモ証明書が付属しているいずれかのサービスをイネーブルにすると、CLI に警告メッセージが表示されます。

関連項目

- 署名付き証明書の導入 （3 ページ）
- 自己署名証明書の導入 （3 ページ）

署名付き証明書の導入

たとえば、マシンがドメインにないために E メール セキュリティ アプライアンスと他のマシン間で自己署名証明書を交換できない場合、署名付き証明書を使用します。企業のセキュリティ部門には、他にも要件が存在する場合があります。

	操作内容	詳細
ステップ 1	クラスタに導入する場合は、次の手順に従います。	証明書と集中管理 （4 ページ）
ステップ 2	自己署名証明書および証明書署名要求（CSR）を生成します。	自己署名証明書の作成 （5 ページ）
ステップ 3：	生成された証明書を、署名のために既知の認証局に送信します。	認証局への証明書署名要求（CSR）の送信について （6 ページ）
ステップ 4：	署名付き証明書をアップロードします。	認証局によって署名された証明書のアップロード （6 ページ）
ステップ 5：	証明書に署名した認証局が、信頼できる認証局のリストにあることを確認します。	認証局のリストの管理 （19ページ）
ステップ 6：	該当する場合、中間証明書を使用します。	中間証明書 （4 ページ）

自己署名証明書の導入

自己署名証明書は一般に、企業のファイアウォールの背後にあるアプライアンス間の通信に使用できます。企業のセキュリティ部門には、他にも要件が存在する場合があります。

	操作内容	詳細
ステップ 1	クラスタに導入する場合は、次の手順に従います。	証明書と集中管理 （4 ページ）
ステップ 2	E メール セキュリティ アプライアンスから自己署名証明書を生成します。	自己署名証明書の作成 （5 ページ）
ステップ 3：	自己署名証明書をエクスポートします。	証明書のエクスポート （7 ページ）
ステップ 4：	自己署名証明書を、E メール セキュリティ アプライアンスと通信するマシンにインポートします。	他のマシンのマニュアルを参照してください。
ステップ 5：	他のマシンから自己署名証明書を生成し、エクスポートします。	他のマシンのマニュアルを参照してください。
ステップ 6：	自己署名証明書を別のマシンから E メール セキュリティ アプライアンスにインポートします。	証明書のインポート （7 ページ） または そのマシンとの通信の設定については、このマニュアルの章を参照してください。 たとえば、Cisco AMP Threat Grid アプライアンスとのセキュアな通信を構成するには、オンプレミスのファイル分析サーバの設定の詳細設定を構成する手順を参照してください。

証明書と集中管理

証明書は通常、証明書の共通名にローカル マシンのホスト名を使用します。E メール セキュリティ アプライアンスがクラスタの一部である場合は、クラスタ レベルでインストールできるワイルド カードの証明書またはサブジェクト代替名（SAN）の証明書を除いてマシン レベルとして各クラスタ メンバの証明書をインポートする必要があります。メンバーのリスナーが別のマシンと通信するときにクラスタが参照できるように、各クラスタ メンバの証明書は、同じ証明書の名前を使用する必要があります。

中間証明書

ルート証明書の検証に加えて、AsyncOS では、中間証明書の検証の使用もサポートされます。中間証明書とは信頼できるルート認証局によって発行された証明書であり、信頼の連鎖を効率的に作成することによって、追加の証明書を作成するために使用されます。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた godaddy.com によって証明書が発行されたとします。godaddy.com によって発行された証明書では、信頼できるルート認証局の秘密キーと同様に godaddy.com の秘密キーが検証される必要があります。

自己署名証明書の作成

次のいずれかの理由により、アプライアンスで自己署名証明書を作成する可能性があります。

- 他の MTA との SMTP カンバセーションを TLS（着信と発信カンバセーションの両方）を使用して暗号化するため。
- HTTPS を使用して GUI にアクセスするためのアプライアンスの HTTPS サービスをイネーブルにするため。
- LDAP サーバがクライアント認証を要求した場合に LDAPS のクライアント証明書として使用するため。
- アプライアンスと Cisco AMP Threat Grid アプライアンスとのセキュアな通信を許可するため。

CLI を使用して自己署名証明書を作成するには、certconfig コマンドを使用します。

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] を選択します。

ステップ 2 [証明書の追加（Add Certificate）] をクリックします。

ステップ 3 [自己署名証明書の作成（Create Self-Signed Certificate）] を選択します。

ステップ 4 自己署名証明書に、次の情報を入力します。

Common Name	**完全修飾ドメイン名**
Organization	組織の正確な正式名称。
組織	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国（Country）	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
秘密キー サイズ（Private Key Size）	CSR 用に生成する秘密キーのサイズ。2048 ビットおよび 1024 ビットだけがサポートされます。

ステップ 5 [Next] をクリックします。

ステップ 6 証明書の名前を入力します。デフォルトでは、前に入力された共通名が割り当てられます。

ステップ 7 この証明書を証明書署名要求（CSR）として送信するには、[証明書署名要求のダウンロード（Download Certificate Signing Request）] をクリックして CSR を PEM 形式でローカルまたはネットワーク マシンに保存します。

ステップ 8 変更を送信し、保存します。

次のタスク

該当する次のステップを参照してください。

- 署名付き証明書の導入　（3 ページ）
- 自己署名証明書の導入　（3 ページ）

認証局への証明書署名要求（CSR）の送信について

認証局は、ID の検証および公開キーの配布に使用されるデジタル証明書を発行する第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。証明書および秘密キーは認識されている認証局から購入できます。シスコでは、サービスの重複を推奨しません。

E メール セキュリティ アプライアンスでは、自己署名証明書を作成して、公開証明書を取得するために認証局に送信する証明書署名要求（CSR）を生成できます。認証局は、秘密キーによって署名された信頼できる公開証明書を返送します。Web インターフェイスの [ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の certconfig コマンドを使用して自己署名証明書を作成し、CSR を生成して、信頼できる公開証明書をインストールします。

初めて証明書を取得または作成する場合は、インターネットで「certificate authority services SSL Server Certificates（SSL サーバ証明書を提供している認証局）」を検索して、お客様の環境のニーズに最も適したサービスを選択してください。サービスの手順に従って、証明書を取得します。

次の作業

署名付き証明書の導入　（3 ページ）を参照してください。

認証局によって署名された証明書のアップロード

認証局から秘密キーで署名された信頼できる公開証明書が返されたら、証明書をアプライアンスにアップロードします。

パブリック リスナーまたはプライベート リスナー、IP インターフェイスの HTTPS サービス、LDAP インターフェイス、または宛先ドメインへのすべての発信 TLS 接続に証明書を使用できます。

ステップ 1　受信した信頼できる公開証明書が PEM 形式であるか、またはアプライアンスにアップロードする前に PEM を使用するように変換できる形式であることを確認します。（変換ツールは http://www.openssl.org の無料のソフトウェア OpenSSL に含まれています）。

ステップ 2　署名付き証明書をアプライアンスにアップロードします。

（注）　証明書を認証局からアップロードすると、既存の自己署名証明書が上書きされます。

a) [ネットワーク（Network）] > [証明書（Certificates）] を選択します。
b) 署名のために認証局に送信した証明書の名前をクリックします。
c) ローカル マシンまたはネットワーク ボリューム上のファイルへのパスを入力します。

ステップ 3 自己署名証明書に関連する中間証明書をアップロードすることもできます。

次のタスク

関連項目

- 署名付き証明書の導入 （3 ページ）

証明書のインポート

AsyncOS では、アプライアンスで使用するために、PKCS #12 形式で保存された証明書を他のマシンからインポートすることもできます。

CLI を使用して証明書をインポートするには、**`certconfig`** コマンドを使用します。

（注） 署名付き証明書を導入する場合、この手順を使用して署名付き証明書をインポートしないでください。代わりに、認証局によって署名された証明書のアップロード （6 ページ）を参照してください。

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] を選択します。

ステップ 2 [証明書の追加（Add Certificate）] をクリックします。

ステップ 3 [証明書のインポート（Import Certificate）] オプションを選択します。

ステップ 4 ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。

ステップ 5 ファイルのパスフレーズを入力します。

ステップ 6 [次へ（Next）] をクリックして証明書の情報を表示します。

ステップ 7 証明書の名前を入力します。

AsyncOS のデフォルトでは、共通の名前が割り当てられます。

ステップ 8 変更を送信し、保存します。

次のタスク

- 自己署名証明書を導入する場合は、自己署名証明書の導入 （3 ページ）を参照してください。

証明書のエクスポート

AsyncOS では、証明書をエクスポートし、PKCS #12 形式で保存することも可能です。

（注） 署名付き証明書を導入する場合、この手順を使用して証明書署名要求（CSR）を生成しないでください。代わりに、署名付き証明書の導入 （3 ページ）を参照してください。

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [証明書のエクスポート（Export Certificate）] をクリックします。

ステップ 3 エクスポートする証明書を選択します。

ステップ 4 証明書のファイル名を入力します。

ステップ 5 証明書ファイルのパスフレーズを入力して確認します。

ステップ 6 [エクスポート（Export）] をクリックします。

ステップ 7 ファイルをローカル マシンまたはネットワーク マシンに保存します。

ステップ 8 さらに証明書をエクスポートするか、または [キャンセル（Cancel）] をクリックして [ネットワーク（Network）] > [証明書（Certificates）] ページに戻ります。

次のタスク

- 自己署名証明書を導入する場合は、自己署名証明書の導入 （3 ページ）を参照してください。

リスナー HAT の TLS の有効化

暗号化が必要なリスナーに対して TLS をイネーブルにする必要があります。インターネットに対するリスナー（つまり、パブリック リスナー）には TLS をイネーブルにしますが、内部システムのリスナー（つまり、プライベート リスナー）には必要ありません。また、すべてのリスナーに対して暗号化をイネーブルにすることもできます。

リスナーの TLS に次の設定を指定できます。

表 *1*: リスナーの *TLS* 設定

TLS 設定	意味
1．なし	TLS では着信接続を行えません。リスナーに対する接続では、暗号化された SMTP カンバセーションは必要ありません。これは、アプライアンス上で設定されるすべてのリスナーに対するデフォルト設定です。
2．推奨	TLS で MTA からのリスナーへの着信接続が可能です。

TLS 設定	意味
3. 必須	TLS で MTA からリスナーへの着信接続が可能です。また、STARTTLS コマンドを受信するまでアプライアンスは NOOP、EHLO、または QUIT 以外のすべてのコマンドに対してエラー メッセージで応答します。この動作は RFC 3207 によって指定されています。RFC 3207 では、Secure SMTP over Transport Layer Security の SMTP サービス拡張が規定されています。TLS が「必要」であることは、送信側で TLS の暗号化を行わない電子メールが、送信前にアプライアンスによって拒否されることを意味し、このため、暗号化されずにクリア テキストで転送されることが回避されます。

デフォルトでは、プライベート リスナーとパブリック リスナーのどちらも TLS 接続を許可しません。電子メールの着信（受信）または発信（送信）の TLS をイネーブルにするには、リスナーの HAT の TLS をイネーブルにする必要があります。また、プライベート リスナーおよびパブリック リスナーのすべてのデフォルト メール フロー ポリシー設定で tls 設定が「off」になっています。

リスナーの作成時に、個々のパブリック リスナーに TLS 接続の専用の証明書を割り当てることができます。詳細については、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を参照してください。

関連項目

- GUI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て （9 ページ）
- CLI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て （10 ページ）
- ログ （14 ページ）
- GUI の例：リスナーの HAT の TLS 設定の変更 （10 ページ）
- CLI の例：リスナーの HAT の TLS 設定の変更 （10 ページ）

GUI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て

ステップ 1 [ネットワーク（Network）] > [リスナー（Listeners）] ページに移動します。

ステップ 2 編集するリスナーの名前をクリックします。

ステップ 3 [証明書（Certificate）] フィールドから、証明書を選択します。

ステップ 4 変更を送信し、保存します。

CLI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て

ステップ 1 `listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。

ステップ 2 `certificate` コマンドを使用して、使用できる証明書を表示します。

ステップ 3 プロンプトが表示されたら、リスナーを割り当てる証明書を選択します。

ステップ 4 リスナーの設定が完了したら、`commit` コマンドを発行して、変更をイネーブルにします。

ログ

TLS が必要であるにもかかわらず、リスナーで使用できない場合は、E メール セキュリティ アプライアンスがメール ログ インスタンスに書き込みます。次の条件のいずれかを満たす場合、メール ログが更新されます。

- リスナーに対して TLS が「必須（required）」と設定されている。
- E メール セキュリティ アプライアンスは、「STARTTLS コマンドを最初に発行（Must issue a STARTTLS command first）」コマンドを送信した。
- 正常な受信者が受信せずに接続が終了した。

TLS 接続が失敗した理由に関する情報がメール ログに記録されます。

GUI の例：リスナーの HAT の TLS 設定の変更

ステップ 1 [メール ポリシー（Mail Policies）] > [メール フロー ポリシー（Mail Flow Policies）] ページに移動します。

ステップ 2 変更するポリシーを持つリスナーを選択し、編集するポリシーの名前へのリンクをクリックします。（デフォルト ポリシー パラメータも編集可能）。

ステップ 3 [暗号化と認証（Encryption and Authentication）] セクションの [TLS:] フィールドで、リスナーに必要な TLS のレベルを選択します。

ステップ 4 変更の送信と保存

選択した TLS 設定が反映されてリスナーのメール フロー ポリシーが更新されます

CLI の例：リスナーの HAT の TLS 設定の変更

ステップ 1 `listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。

ステップ 2 リスナーのデフォルトの HAT 設定を編集するには、`hostaccess -> default` コマンドを使用します。

ステップ 3 次の質問が表示されたら、次の選択肢のいずれかを入力して TLS 設定を変更します。

```
Do you want to allow encrypted TLS connections?

1. No

2. Preferred

3. Required

[1]> 3

You have chosen to enable TLS. Please use the 'certconfig' command to

ensure that there is a valid certificate configured.
```

ステップ 4 この例では、リスナーで使用できる有効な証明書があるかどうかを確認するために `certconfig` コマンドを使用するかどうかを質問しています。証明書を作成していない場合、リスナーではアプライアンスにあらかじめインストールされているデモ証明書を使用します。テスト目的でデモ証明書で TLS をイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。リスナーに証明書を割り当てるには、`listenerconfig -> edit -> certificate` コマンドを使用します。TLS を設定すると、CLI でリスナーの概要に設定が反映されます。

```
Name: Inboundmail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: Required
```

ステップ 5 変更をイネーブルにするには、`commit` コマンドを発行します

配信時の TLS および証明書検証の有効化

[送信先コントロール（Destination Controls）] ページまたは `destconfig` コマンドを使用すると、TLS をイネーブルにして、特定のドメインに電子メールを配信するように要求できます。

TLS だけでなく、ドメインのサーバ証明書の検証も要求できます。このドメイン証明書は、ドメインのクレデンシャルを確立するために使用されるデジタル証明書に基づいています。証明プロセスには次の 2 つの要件が含まれます。

- 信頼できる認証局（CA）によって発行された証明書で終わる SMTP セッションの証明書発行者のチェーン。
- 受信マシンの DNS 名またはメッセージの宛先ドメインのいずれかと一致する証明書に表示された Common Name（CN）。

または

メッセージの宛先ドメインが、証明書のサブジェクト代替名（subjectAltName）の拡張の DNS 名のいずれかと一致している（RFC 2459 を参照）。この一致では、RFC 2818 のセクション 3.1 で説明されているワイルドカードがサポートされます。

信頼できる CA は、ID の検証および公開キーの配布に使用されるデジタル証明書を発行する、第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。

エンベロープ暗号化の代わりに TLS 接続を介してドメインにメッセージを送信するように E メール セキュリティ アプライアンスを設定できます。詳細については、「Cisco 電子メール暗号化」の章を参照してください。

すべての発信 TLS 接続に対してアプライアンスで使用する証明書を指定できます。証明書を指定するには、[送信先コントロール（Destination Controls）] ページの [グローバル設定の編集（Edit Global Settings）] をクリックするか、または CLI で `destconfig -> setup` を使用します。証明書はドメインごとの設定ではなく、グローバル設定です。

[送信先コントロール（Destination Controls）] ページまたは `destconfig` コマンドを使用してドメインを含める場合、指定されたドメインの TLS に 5 つの異なる設定を指定できます。TLS のエンコードにドメインとの交換が必須であるか、または推奨されるかの指定に加えて、ドメインの検証が必要かどうかも指定できます。設定の説明については、次の表を参照してください。

表 *2*: 配信の *TLS* 設定

TLS 設定	意味
デフォルト	デフォルトの TLS 設定では、リスナーからドメインの MTA への発信接続に [送信先コントロール（Destination Controls）] ページまたは `destconfig -> default` サブコマンドを使用するように設定されています。 質問の "Do you wish to apply a specific TLS setting for this domain?" に対して "no" と回答すると、値の "Default" が設定されます。
1. なし	インターフェイスからドメインの MTA への発信接続には、TLS がネゴシエートされません。
2. Preferred	E メール セキュリティ アプライアンス インターフェイスからドメインの MTA に対して TLS がネゴシエートされます。ただし、（220 応答を受信する前に）TLS ネゴシエーションに失敗すると、SMTP トランザクションは「クリアな」（暗号化されない）ままです。証明書が信頼できる認証局によって発行された場合、検証は行われません。220 応答を受信した後にエラーが発生した場合、SMTP トランザクションはクリア テキストにフォールバックされません。

TLS 設定	意味
3. 必須（Required）	E メール セキュリティ アプライアンス インターフェイスからドメインの MTA に対して TLS がネゴシエートされます。ドメインの証明書の検証は行われません。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。ネゴシエーションに成功すると、暗号化されたセッションを経由して電子メールが配信されます。
4. 推奨（検証）	E メール セキュリティ アプライアンスからドメインの MTA への TLS がネゴシエートされます。アプライアンスはドメインの証明書の検証を試行します。 次の 3 つの結果が考えられます。 • TLS がネゴシエートされ、証明書が検証される。暗号化されたセッションによってメールが配信される。 • TLS がネゴシエートされるものの、証明書は検証されない。暗号化されたセッションによってメールが配信される。 • TLS 接続が確立されず、証明書は検証されない。電子メール メッセージがプレーン テキストで配信される。
5. 必須（検証）	アプライアンスからドメインの MTA への TLS がネゴシエートされます。ドメインの証明書の検証が必要です。次の結果が考えられます。 • TLS 接続がネゴシエートされ、証明書が検証される。暗号化されたセッションによって電子メール メッセージが配信される。 • TLS 接続がネゴシエートされるが、信頼できる認証局（CA）によって証明書が検証されない。メールは配信されない。 • TLS 接続がネゴシエートされない。メールは配信されない。
6. 必須 - ホステッドドメインの検証	[必要な TLS（TLS Required）]、[検証と必要な TLS（Verify and TLS Required）]、[ホステッド ドメインの検証（Verify Hosted Domain）] の各オプションは、ID 検証プロセスに相違があります。提示される ID を処理する方法および使用が許可される参照識別子の種類によって、最終的な結果に相違が生じます。 提示される ID は、最初に、`dNSName` タイプの `subjectAltName` 拡張子から派生されます。`dNSName` と承認された参照識別子（`REF-ID`）のいずれかとの間が一致しない場合、`CN` が件名フィールドに存在し、さらなる ID 検証に合格するかどうかに関係なく、検証は失敗します。件名フィールドから派生した `CN` は、証明書に `dNSName` タイプの `subjectAltName` 拡張子が含まれない場合のみ検証されます。

グッド ネイバー テーブルに指定された受信者ドメインの指定されたエントリがない場合、または指定されたエントリが存在するものの、そのエントリに対して指定された TLS 設定が存在しない場合、[送信先コントロール（Destination Controls）] ページまたは `destconfig -> default` サブコマンド（"No"、"Preferred"、"Required"、"Preferred (Verify)"、または "Required (Verify)"）を使用して動作を設定する必要があります。

関連項目

- 要求された TLS 接続が失敗した場合のアラートの送信 （14 ページ）
- ログ （14 ページ）
- 認証局のリストの管理 （19 ページ）

要求された TLS 接続が失敗した場合のアラートの送信

TLS 接続が必要なドメインにメッセージを配信する際に TLS ネゴシエーションが失敗した場合、E メール セキュリティ アプライアンスがアラートを送信するかどうかを指定できます。アラート メッセージには失敗した TLS ネゴシエーションの宛先ドメイン名が含まれます。E メール セキュリティ アプライアンスは、システム アラートのタイプの警告重大度レベル アラートを受信するよう設定されたすべての受信者にアラートメッセージを送信します。GUI の [システム管理（System Administration）]>[アラート（Alerts）] ページ（または CLI の alertconfig コマンド）を使用してアラートの受信者を管理できます。

関連項目

- TLS 接続アラートの有効化 （14 ページ）

TLS 接続アラートの有効化

ステップ 1 メール ポリシーの [送信先コントロール（Destination Controls）] ページに移動します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [必要な TLS 接続に失敗した場合にアラートを送信：（Send an alert when a required TLS connection fails:）] の [有効（Enable）] をクリックします。

これは、ドメイン単位ではなく、グローバルな設定です。アプライアンスが配信を試行したメッセージの情報については、[モニタ（Monitor）]>[メッセージ トラッキング（Message Tracking）] ページまたはメール ログを使用します。

ステップ 4 変更を送信し、保存します。

次のタスク

これはコマンドライン インターフェイスでも構成できます。CLI で destconfig -> setup コマンドを使用して TLS 接続アラートを有効化します。

ログ

ドメインに TLS が必要であるにもかかわらず、使用できない場合は、E メール セキュリティ アプライアンスがメール ログ インスタンスに書き込みます。TLS 接続を使用できなかった理由も記載されています。次の条件のいずれかを満たす場合、メール ログが更新されます。

- リモート MTA で ESMTP がサポートされない（たとえば、E メール セキュリティ アプライアンスからの EHLO コマンドが理解できない）。
- リモート MTA で ESMTP がサポートされるものの、「STARTTLS」が EHLO 応答でアドバタイズされる拡張のリストにない。
- リモート MTA で「STARTTLS」拡張がアドバタイズされたものの、E メール セキュリティ アプライアンスで STARTTLS コマンドを送信した際にエラーが返される。

名前付きエンティティの DNS ベースの認証

- 名前付きエンティティの SMTP DNS ベースの認証の概要 （15 ページ）
- DANE をサポートする配信に向けた TLS の有効化 （18 ページ）
- DANE 失敗時のアラートの送信 （19 ページ）

名前付きエンティティの SMTP DNS ベースの認証の概要

証明書を使用して認証された TLS 接続は、以下のいずれかの方法でセキュリティ侵害に対して脆弱となる可能性があります。

- 信頼できる認証局（CA）は任意のドメイン名に証明書を発行できます。
- 攻撃者は、中間者（man-in-the-middle）攻撃を使用して、TLS 接続をプレーン テキスト通信にダウングレードできます。
- DNS サーバで DNSSEC が設定されていない場合、攻撃者は偽の DNS MX レコードで DNS レスポンスを偽って安全でないサーバにメッセージをリダイレクトし、DNS キャッシュ ポイズニング攻撃を仕掛けます。
- 受信側のメール転送エージェント（MTA）に信頼できる認証局（CA）のリストが設定されていない場合は、自己署名の証明書またはプライベート認証局によって発行された証明書を使用できます。

名前付きエンティティの SMTP DNS ベースの認証（DANE）プロトコルは、DNS サーバで設定したドメイン ネーム システム セキュリティ（DNSSEC）拡張と、TLSA としても知られる DNS リソース レコードを使用して、X.509 証明書と DNS 名を検証します。

TLSA レコードは *RFC 6698* で記述される DNS 名に対して使用される認証局（CA）、エンドエンティティの証明書、トラスト アンカーのいずれかの詳細が含まれる証明書に追加されます。詳細については、TLSA レコードの作成 （17ページ）を参照してください。ドメイン ネーム システム セキュリティ（DNSSEC）拡張は、DNS セキュリティの脆弱性に対応することで、DNS のセキュリティを強化します。暗号化キーおよびデジタル署名を使用する DNSSEC は、ルックアップ データが正確で、適切なサーバに接続されていることを保証します。

以下は、送信 TLS 接続に SMTP DANE を使用する利点です。

- 中間者（MITM）ダウングレード攻撃、傍受、DNS キャッシュ ポイズニング攻撃を防ぎ、メッセージを安全に配信します。

- DNSSEC によって保護することで、TLS 証明書と DNS 情報の信憑性を保証します。

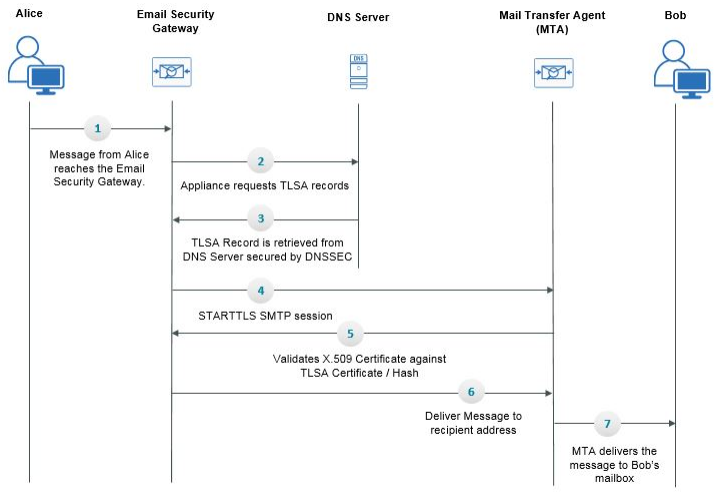
関連項目

- SMTP DANE ワークフロー （16 ページ）
- TLSA レコードの作成 （17 ページ）
- DANE をサポートする配信に向けた TLS の有効化 （18 ページ）
- DANE 失敗時のアラートの送信 （19 ページ）

SMTP DANE ワークフロー

以下の図は、送信 TLS 接続と DANE サポートを使用したメッセージのフローを説明しています。

図 *1 : TLS* と *DANE* サポートを使用したメッセージの配信



1. 送信側（アリス）は、組織外の受信者（ボブ）にメッセージを送信します。
2. メッセージが E メール セキュリティ ゲートウェイに到達します。
3. E メール セキュリティ ゲートウェイが、DNS の TLSA レコードとしても知られる DNS リソース レコードを DNS サーバからリクエストします。
4. 証明書と TLSA レコードは DNS サーバから取得され、DNSSEC によって保護されます。
5. アプライアンスが、受信者のアドレスに対する STARTTLS SMTP セッションを確立します。
6. X.509 証明書が、受信者のアドレスの完全な TLSA レコードまたは TLSA レコードのハッシュ値に対して検証されます。検証に成功した後、メッセージは受信者のメール転送エー

ジェント（MTA）に配信されます。証明書の検証が失敗すると、メッセージが後ほど配信されるか、メッセージがバウンスされます。

7. MTA が受信者の、メールボックスにメッセージを配信します。

TLSA レコードの作成

DNSSEC で署名した DNS レコード上で、希望する認証局（CA）の TLSA レコードを作成できます。以下は、完全修飾ドメイン名（FQDN）`www.example.com:` の TLSA レコードのサンプルです。

```
_443._tcp.www.example.com。IN TLSA (0 0 1
91751cee0a1ab8414400238a761411daa29643ab4b8243e9a91649e25be53ada)
```

上記の例 TLSA レコードには、暗号化は、次のフィールドがあります。

- **証明書の使用状況**：証明書のタイプを指定します。
  - サンプルでは、最初の「0」の桁は CA の証明書を指定しており、RFC 6698 に記述される PKIX 証明書パスと一致する必要があります。
  - 「1」の場合はエンド エンティティの証明書を指定しており、TLS のサーバによって提供されるエンド エンティティの証明書と一致する必要があります。
  - 「2」の場合は、TLS のサーバによって提供されるエンド エンティティの証明書を検証する際にトラスト アンカーとして使用する必要がある証明書を指定します。
  - 「3」の場合は、TLS のサーバによって提供されるエンド エンティティの証明書と一致する必要がある証明書を指定します。
- **セレクタ フィールド**：関連データと一致する TLS 証明書の部分を指定します。
  - サンプルでは、2 つ目の「0」は、完全な証明書が一致する必要があることを指定しています。
  - 「1」の場合は、「SubjectPublicKeyInfo」フィールドのみが一致する必要があることを指定します。
- **一致タイプ**：使用されるハッシュ値のタイプを指定します。
  - サンプルでは、3 番目の「1」は選択したコンテンツの SHA-256 ハッシュを指定しています。
  - 「0」の場合は、選択したコンテンツの完全一致を指定します。
  - 「2」の場合は、選択したコンテンツの SHA-512 ハッシュを指定します。

DANE をサポートする配信に向けた TLS の有効化

始める前に

- エンベロープ送信者と TLSA リソース レコードが DNSSEC で検証されていることを確認します。
- アプライアンスで DANE を設定するために TLS を有効にしていることを確認します。詳細については、配信時の TLS および証明書検証の有効化 （11 ページ）を参照してください。

ステップ 1 [メールポリシー（Mail Policies）] > [送信先コントロール（Destination Controls）] ページに移動します。

ステップ 2 [送信先コントロールの追加（Add Destination Controls）] をクリックするか、既存のエントリを変更します。

ステップ 3 [TLSサポート（TLS Support）] フィールドから [推奨（Preferred）]、[必要（Required）]、[必須（Mandatory）] のいずれかを選択し、アプライアンスで DANE サポートを有効にします。

ステップ 4 [DANEサポート（DANE Support）] フィールドから、特定の TLS 接続に対する DANE に以下の設定を指定できます。

DANE 設定	説明
デフォルト	送信先コントロール ページを使用して設定するデフォルトの DANE 設定は、リスナーからドメインの MTA への送信 TLS 接続に使用されます。 [デフォルト（Default）] の DANE 設定は、送信先コントロールのデフォルト TLS 設定から継承されます。この設定は、カスタムの送信先コントロール エントリに上書きできます。
なし	インターフェイスからドメインの MTA への送信接続のネゴシエートに DANE を使用しない場合は、[なし（None）] を選択します。
状況対応型	[状況対応型（Opportunistic）] を選択し、リモート ホストが DANE をサポートしていない場合、SMTP カンバセーションの暗号化に状況対応型の TLS が使用されます。 [状況対応型（Opportunistic）] を選択し、リモート ホストが DANE をサポートしている場合、SMTP カンバセーションの暗号化の優先モードとなります。

DANE 設定	説明
必須	[必須（Mandatory）] を選択し、リモート ホストが DANE をサポートしていない場合、送信先ホストに対する接続が確立されません。 「[必須（Mandatory）] を選択し、リモート ホストが DANE をサポートしている場合、SMTP カンバセーションの暗号化の優先モードとなります。

ステップ 5 変更を [実行（Submit）] して [確定する（Commit）] します。

DANE 失敗時のアラートの送信

TLS 接続と DANE サポートが必要なドメインにメッセージを配信する際に、すべての MX ホストに対して DANE の検証が失敗した場合、E メール セキュリティ アプライアンスがアラートを送信するかどうかを指定できます。E メール セキュリティ アプライアンスは、システム アラートのタイプの警告重大度レベルアラートを受信するよう設定されたすべての受信者にアラートメッセージを送信します。

DANE アラートの有効化

ステップ 1 [システム管理（System Administration）] > [アラート（Alerts）] ページに移動します。

ステップ 2 アラートを有効にするアラートの受信者を選択します。

ステップ 3 アラート タイプに対応する [メッセージ配信（Message Delivery）] チェック ボックスを選択します。

ステップ 4 変更を送信し、保存します。

認証局のリストの管理

アプライアンスは、リモート ドメインからの証明書の検証にはドメインのクレデンシャルを確立するために使用する保存された信頼できる認証局を使用します。次の信頼できる認証局を使用するようにアプライアンスを設定できます。

- **プレインストールされたリスト。**アプライアンスには信頼できる認証局のリストがあらかじめインストールされています。これは、システム リストと呼ばれます。
- **ユーザ定義のリスト。**信頼できる認証局のリストをカスタマイズし、アプライアンスにリストをインポートできます。

システム リストまたはカスタマイズされたリストのいずれか、または両方のリストを使って、リモート ドメインからの証明書を検証できます。

GUI の [ネットワーク（Network）] > [証明書（Certificates）] > [認証局の編集（Edit Certificate Authorities）] ページまたは CLI の certconfig > certauthority コマンドを使用してリストします。

[ネットワーク（Network）] > [証明書（Certificates）] > [認証局の編集（Edit Certificate Authorities）] ページで、次のタスクを実行できます。

- **認証局のシステム リスト（インストール済み）を参照します。**詳細については、プレインストールされた認証局リストの参照 （20 ページ）を参照してください。
- **システム リストを使用するかどうかを選択します。**システム リストはイネーブルまたはディセーブルにできます。詳細については、システム認証局リストの無効化 （20ページ）を参照してください。
- **カスタム認証局リストを使用するかどうかを選択します。**カスタム リストを使用して、テキスト ファイルからリストをインポートするようにアプライアンスをイネーブルにできます。詳細については、カスタム認証局リストのインポート （21 ページ）を参照してください。
- **ファイルに、認証局のリストをエクスポートします。**テキスト ファイルに、認証局のシステム リストまたはカスタム リストをエクスポートできます。詳細については、認証局リストのエクスポート （21 ページ）を参照してください。

関連項目

- プレインストールされた認証局リストの参照 （20 ページ）
- システム認証局リストの無効化 （20 ページ）
- カスタム認証局リストのインポート （21 ページ）
- 認証局リストのエクスポート （21 ページ）

プレインストールされた認証局リストの参照

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [システム認証局を表示（View System Certificate Authorities）] をクリックします。

システム認証局リストの無効化

プレインストールされたシステム認証局リストはアプライアンスから削除できませんが、イネーブルまたはディセーブルにできます。アプライアンスがリモート ホストからの証明書を確認するためにカスタム リストのみを使用することをディセーブルにすることがあります。

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [システム リスト（System List）] で [ディセーブル（Disable）] をクリックします。

ステップ 4 変更を送信し、保存します。

カスタム認証局リストのインポート

信頼できる認証局のカスタム リストを作成して、アプライアンスにインポートできます。ファイルは PEM 形式にして、アプライアンスで信頼する認証局の証明書が含まれている必要があります。

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [カスタム リスト（Custom List）] の [有効（Enable）] をクリックします。

ステップ 4 ローカル マシンまたはネットワーク マシンのカスタム リストへのフル パスを入力します。

ステップ 5 変更を送信し、保存します。

認証局リストのエクスポート

システム内の信頼できる認証局のサブセットのみを使用するか、既存のカスタム リストの編集を行う場合、リストを .txt ファイルにエクスポートして、認証局を追加または削除するように編集できます。リストの編集が完了したら、ファイルをカスタム リストとしてアプライアンスにインポートします。

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [リストのエクスポート（Export List）] をクリックします。

[認証局リストのエクスポート（Export Certificate Authority List）] ページが表示されます。

ステップ 4 自分がエクスポートするリストを選択します。

ステップ 5 リストのファイル名を入力します。

ステップ 6 [エクスポート（Export）] をクリックします。

AsyncOS では、.txt ファイルとしてリストを開くか、または保存するかを確認するダイアログボックスが表示されます。

HTTPS の証明書のイネーブル化

GUI の [ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] ページまたは CLI の **interfaceconfig** コマンドのいずれかを使用して、IP インターフェイスで HTTPS サービスの証明書をイネーブルにできます。

ステップ 1 [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページに移動します。

ステップ 2 HTTPS サービスを有効化するインターフェイスを選択します。

ステップ 3 [アプライアンス管理（Appliance Management）] で、[HTTPS] チェック ボックスをオンにし、ポート番号を入力します。

ステップ 4 変更を送信し、保存します。

次のタスク

（注） アプライアンスにあらかじめインストールされているデモ証明書。テスト目的でデモ証明書で HTTPS サービスをイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。

GUI のシステム設定ウィザードを使用して HTTPS サービスをイネーブルにできます。詳細については、セットアップおよび設置を参照してください。