トラフィック復号の概要

デフォルトでは、ASA FirePOWER モジュールはセキュア ソケット レイヤ（SSL）プロトコルまたはその後継である Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。アクセス コントロールの一部として *SSL インスペクション*機能を使用すると、暗号化トラフィックのインスペクションを実行せずにブロックしたり、暗号化または復号されたトラフィックをアクセス コントロールで検査したりできます。暗号化されたセッションをモジュールが処理するときは、トラフィックの詳細がログに記録されます。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、ネットワーク内の暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

SSL インスペクションは、ポリシーベースの機能です。FirePOWER システムでは、アクセス コントロール ポリシーは、SSL ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。アクセス コントロールと SSL ポリシーを関連付ければ、システムはアクセス コントロール ルールで評価する前に、その SSL ポリシーを使用して暗号化セッションを処理します。SSL インスペクションを設定していない場合、またはデバイスがサポートしていない場合、アクセス コントロール ルールは、すべての暗号化トラフィックを処理します。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、そのトラフィックがアクセス コントロール ルールによって処理されることにも注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイル インスペクションを無効にしています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、アクセス コントロール ルールの作成および編集（6-3 ページ）および SSL プリプロセッサの使用（22-83 ページ）を参照してください。

モジュールで TCP 接続での SSL または TLS ハンドシェイクが検出されると、そのトラフィックを復号できるかどうかが判定されます。復号できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化されたトラフィックをブロックし、オプションで TCP 接続をリセットする
- 暗号化されたトラフィックを復号しない

モジュールによるトラフィックの復号が可能な場合は、それ以上のインスペクションなしでトラフィックをブロックするか、復号されていないトラフィックをアクセス コントロールによって評価するか、あるいは次のいずれかの方法を使用して復号します。

- 既知の秘密キーを使用して復号する。外部ホストがネットワーク上のサーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書とアプライアンスにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。
- サーバ証明書の再署名によって復号する。ネットワーク上のホストが外部サーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書がアップロード済みの認証局（CA）証明書で再署名されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。

復号化されたトラフィックに対しては、はじめから暗号化されていないトラフィックと同じ処理と分析が施されます。これには、ネットワーク、レピュテーション、ユーザベースのアクセス コントロール、侵入の検知と防止、および高度なマルウェア防御が該当します。復号されたトラフィックのポスト分析をブロックしない場合、トラフィックは再暗号化されて宛先ホストに渡されます。

（注）　トラフィックのブロックや発信トラフィックの復号など、いくつかの SSL インスペクション アクションはトラフィックのフローを変更します。インラインに配置された ASA FirePOWER モジュールはこれらのアクションを実行できます。パッシブに配置された ASA FirePOWER モジュールはトラフィック フローを変更できません。ただし、これらのデバイスでも着信トラフィックを復号することは可能です。詳細については、例：パッシブ展開でのトラフィック復号化（14-9 ページ）を参照してください。

詳細については、次の項を参照してください。

- SSL ハンドシェイク処理（14-2 ページ）
- SSL インスペクションの要件（14-6 ページ）
- SSL インスペクション アプライアンス展開の分析（14-8 ページ）

SSL ハンドシェイク処理

このマニュアルでは、用語 *SSL ハンドシェイク*は SSL プロトコルとその後継のプロトコル TLS の両方の暗号化セッションを開始する、2 ウェイ ハンドシェイクを表します。

パッシブ展開では、FirePOWER システムはハンドシェイクのコピーを確認しますが、実際のハンドシェイクを処理しません。インライン展開では、FirePOWER システムは SSL ハンドシェイクを処理し、ClientHello メッセージを修正する可能性があり、セッションの TCP プロキシ サーバとして機能します。

（正常に TCP 3 ウェイ ハンドシェイクが完了した後）クライアントがサーバとの TCP 接続を確立すると、管理対象デバイスは TCP セッションでの暗号化されたセッションの開始の試行をモニタします。SSL ハンドシェイクは、クライアントとサーバ間の特殊なパケットの交換によって、暗号化セッションを確立します。SSL と TLS プロトコルでは、これらの特殊なパケットは*ハンドシェイク メッセージ*と呼ばれます。ハンドシェイク メッセージは、クライアントとサーバの両方がサポートする暗号化属性を伝えます。

- ClientHello：クライアントは各暗号化属性に複数のサポートされる値を指定します。
- ServerHello：サーバはシステムがセキュリティで保護されたセッション中に使用する暗号化方式を決定する、各暗号化属性に 1 つのサポートされる値を指定します。

セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッション データをキャッシュに保存し、それによりフル ハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバ証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

ClientHello メッセージ処理

セキュアな接続が確立できる場合、クライアントはパケットの宛先として機能するサーバに ClientHello メッセージを送信します。クライアントは SSL ハンドシェイクを開始するメッセージを送信するか、または、宛先サーバからの Hello Request メッセージへの応答に含めます。

SSL インスペクションを設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを [復号 - 再署名（Decrypt - Resign）] アクションを含む SSL ルールと照合しようとします。照合は ClientHello メッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。考えられるデータには次のものがあります。

表 14-1　SSL ルールの条件のデータの可用性

SSL ルールの条件	データの存在場所
ゾーン	ClientHello
ネットワーク	ClientHello
VLAN タグ	ClientHello
ポート	ClientHello
ユーザ	ClientHello
アプリケーション	ClientHello（サーバ名インジケータの拡張機能）
カテゴリ	ClientHello（サーバ名インジケータの拡張機能）
証明書	サーバ証明書（キャッシュされている可能性あり）
識別名	サーバ証明書（キャッシュされている可能性あり）
証明書のステータス	サーバ証明書（キャッシュされている可能性あり）
暗号スイート	ServerHello
バージョン	ServerHello

ClientHello メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致しない場合、システムはメッセージを変更しません。次に、メッセージがアクセス コントロール評価（ディープ インスペクションを含めることができる）で合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージが [復号 - 再署名（Decrypt - Resign）] ルールに一致したら、システムは ClientHello メッセージを次のように変更します。

- 圧縮方法：クライアントがサポートする圧縮方法を指定する、compression_methods 要素を削除します。FirePOWER システムは圧縮されたセッションを復号化することはできません。この変更により、復号化できないトラフィックの圧縮されたセッション タイプが削減されます。
- 暗号スイート：FirePOWER システムがサポートしない場合、cipher_suites 要素から暗号スイートを削除します。FirePOWER システムが指定した暗号スイートのいずれもサポートしない場合、システムは、元の変更されていない要素を送信します。この変更により、復号化できないトラフィックのサポートされない暗号スイートと不明な暗号スイートが削減されます。
- セッション識別子：キャッシュされたセッション データと一致しない SessionTicket 拡張機能と Session Identifier 要素から値を削除します。ClientHello 値がキャッシュされたデータと一致した場合、一時停止したセッションは、クライアントとサーバが完全な SSL ハンドシェイクを実行せずに、中断したセッションを再開できます。この変更は、セッション再開の可能性を高め、復号化できないトラフィックのセッションが未キャッシュのタイプを削減します。
- 楕円曲線：FirePOWER システムがサポートしない場合、サポートされる楕円曲線拡張機能から楕円曲線を削除します。FirePOWER システムが指定した楕円曲線のいずれもサポートしない場合、管理対象デバイスは拡張機能を削除し、cipher_suites 要素から関連する暗号スイートを削除します。
- ALPN 拡張機能：FirePOWER システムでサポートされていないアプリケーション層プロトコル ネゴシエーション（ALPN）拡張機能から値を削除します（たとえば、SPDY と HTTP/2 プロトコル）。この変更は、メッセージがコンテンツ制限機能に関連付けられた SSL ルールに一致した場合にのみ実行されます。詳細については、コンテンツ制限を使用したアクセス コントロール（13-1 ページ）を参照してください。
- 他の拡張機能：Extended Master Secret、Next Protocol Negotiation（NPN）、および TLS チャネル ID 拡張機能を削除します。

（注）　システムはデフォルトで ClientHello の変更を実行します。SSL ポリシーが正しく設定されていると、このデフォルトの動作により、トラフィックの復号化がより頻繁に発生します。各ネットワークにおけるデフォルトの動作を調整するには、サポートにお問い合わせください。

システムが ClientHello メッセージを変更した後、メッセージがアクセス コントロール評価（ディープ インスペクションを含めることができる）を合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージを変更した後はクライアントおよびサーバで計算されたメッセージ認証コード（MAC）が一致しなくなるため、SSL ハンドシェイク時のクライアントとサーバの間の直接通信はできなくなります。すべての後続のハンドシェイク メッセージ（および一度設定された暗号化セッションに対し）、管理対象デバイスは、中間者（MITM）として機能します。ここでは、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間をつなぐ、2 つの SSL セッションが作成されます。その結果、暗号セッションの詳細はセッションごとに異なります。

（注）　FirePOWER システムが復号化できる暗号スイートは頻繁に更新されるので、SSL ルールの条件で使用可能な暗号スイートと直接対応しません。現在、復号化できる暗号スイートのリストについては、サポートに連絡してください。

ServerHello とサーバ証明書メッセージの処理

ServerHello メッセージは、正常な SSL ハンドシェイクの ClientHello メッセージへの応答です。

管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式が認証に証明書を使用する場合、サーバ証明書メッセージはすぐに ServerHello メッセージに続きます。

管理対象デバイスがこれらのメッセージを受信すると、SSL ルールとの一致を試みます。これらのメッセージには、ClientHello メッセージまたはセッション データ キャッシュにはなかった情報が含まれます。具体的には、システムは、識別名、証明書のステータス、暗号スイート、およびバージョン条件でのこれらのメッセージと一致する可能性があります。

メッセージが SSL ルールと一致しない場合、管理対象デバイスは、SSL ポリシーのデフォルトのアクションを実行します。詳細については、基本 SSL ポリシーの作成（15-2 ページ）を参照してください。

メッセージが SSL ルールに一致する場合、管理対象デバイスは、必要に応じて次に進みます。

アクション：[モニタ（Monitor）]

SSL ハンドシェイクは完了に進みます。管理対象デバイスは追跡およびログに記録しますが、暗号化トラックを復号化しません。

アクション：[ブロック（Block）] または [リセットしてブロック（Block with Reset）]

管理対象デバイスは、SSL セッションをブロックします。必要に応じて、TCP 接続もリセットします。

アクション：[復号しない（Do Not Decrypt）]

SSL ハンドシェイクは完了に進みます。管理対象デバイスは、SSL セッションの間で交換されるアプリケーション データを復号化しません。

まれに、システムでは ClientHello メッセージと [復号 - 再署名（Decrypt - Resign）] ルールが一致してメッセージを変更しますが、関連する ServerHello メッセージは [復号しない（Do Not Decrypt）] ルールに一致することがあります。このような場合、クライアントから更新されたハンドシェイクをトリガーするために、システムは TCP 接続をリセットします。更新された ClientHello メッセージは [復号 - 再署名（Decrypt - Resign）] ルールに一致しなくなり、SSL セッションは復号化せずに進みます。

アクション：[復号 - 既知のキー（Decrypt - Known Key）]

管理対象デバイスは、サーバ証明書データを以前にアップロードされたサーバ証明書と照合しようとします。

証明書が以前に生成された証明書と一致した場合、SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSL セッション中に交換されたアプリケーション データを復号化および再暗号化します。

まれに、システムでは、サーバ証明書メッセージが以前に生成された証明書と一致しないことがあります。たとえば、サーバはクライアントとの最初の接続と後続の接続の間に証明書を変更することがあります。この場合、システムは SSL 接続をブロックし、クライアントが再接続して、システムが新しい証明書データとのハンドシェイクを処理できるようにします。

アクション：[復号 - 再署名（Decrypt - Resign）]

管理対象デバイスは、サーバ証明書メッセージを処理し、以前にアップロードされた認証局（CA）証明書で交換されるサーバ証明書を再署名します。SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSL セッション中に交換されたアプリケーション データを復号化および再暗号化します。

ServerHello および証明書メッセージの処理中、管理対象デバイスは識別名と証明書データをキャッシュし、再確立されたセッションと、後続の SSL セッションの両方でハンドシェイクが高速で処理されるようにします。

SSL インスペクションの要件

ライセンス：機能に応じて異なる

構成設定やライセンスに加え、デバイスをネットワーク上にどのように展開しているかにより、暗号化トラフィックの制御や復号化に適用できるアクションが異なります。

SSL インスペクションの一部の機能では、公開キー証明書と秘密キーのペアが必要です。暗号化セッションの特性に応じてトラフィックを復号したり制御したりするためには、証明書および秘密キーのペアを ASA FirePOWER モジュールにアップロードする必要があります。

詳細については、次の項を参照してください。

- SSL インスペクションをサポートする ASA FirePOWER モジュールの導入（14-6 ページ）
- SSL インスペクションのライセンス要件（14-7 ページ）
- SSL ルールを設定するために必要な情報の収集（14-7 ページ）

SSL インスペクションをサポートする ASA FirePOWER モジュールの導入

ライセンス：任意（Any）

設定されインラインに展開された ASA FirePOWER モジュールでは、トラフィック フローを変更できます。これらのデバイスでは、着信および発信トラフィックのモニタリング、ブロック、許可、および復号を行うことができます。

設定されパッシブに展開された ASA FirePOWER モジュールでは、トラフィック フローを変更できません。これらのデバイスで行えるのは、着信トラフィックのモニタリング、許可、および復号だけです。パッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）の暗号スイートを使用した暗号化トラフィックの復号はサポートされません。

最適な展開タイプを決定するときは、マッピングされたアクション、既存のネットワーク展開、および全体的な要件のリストを確認してください。詳細については、SSL インスペクション アプライアンス展開の分析（14-8 ページ）を参照してください。

SSL インスペクションのライセンス要件

ライセンス：機能に応じて異なる

ライセンスによっては、いくつかの条件を組み合わせて暗号化トラフィックの処理方法を決定できます。ASA FirePOWER モジュールでは、ご使用の展開環境でサポートされない機能を示すために、警告アイコン（⚠）および確認ダイアログ ボックスを使用します。警告アイコンの上にポインタを置くと詳細が表示されます。

アクセス コントロール ポリシーの一部として SSL ポリシーを適用すると、SSL ポリシーで復号化されたトラフィックがこのアクセス コントロール ポリシーにより検査されます。アクセス コントロールのライセンスの詳細については、アクセス コントロールのライセンスおよびロール要件（4-2 ページ）を参照してください。

次の表に、アクセス コントロール ポリシーの一部として SSL ポリシーを適用するためのライセンス要件を示します。

表 14-2　SSL インスペクションのライセンス要件

SSL ポリシーの機能	ライセンス
ゾーン、ネットワーク、ポート、または SSL 関連の基準に基づいて、暗号化されたトラフィックを処理する	任意（Any）
位置情報のデータを使用して暗号化トラフィックを処理する	任意（Any）
アプリケーションまたはユーザの条件を使用して暗号化トラフィックを処理する	Control
URL カテゴリおよびレピュテーション データを使用して暗号化されたトラフィックをフィルタ処理する	URL Filtering

SSL ルールを設定するために必要な情報の収集

ライセンス：機能に依存

SSL インスペクションは、サポートする公開キー インフラストラクチャ（PKI）の多くの情報に依存しています。照合ルールの条件を設定するときは、その組織におけるトラフィック パターンについて検討する必要があります。次の表に示す情報を収集しておく必要があります。

表 14-3　SSL ルール条件の設定に必要な情報

一致対象	必要な情報
自己署名サーバ証明書を含む、検出されたサーバ証明書	サーバ証明書
信頼できるサーバ証明書	CA 証明書
検出されたサーバ証明書のサブジェクトまたは発行元	サーバ証明書のサブジェクト DN または発行元 DN

詳細については、SSL ルールを使用したトラフィック復号の調整（17-1 ページ）を参照してください。

ルールの適用先となる暗号化トラフィックの復号、ブロック、モニタリングが不要かどうか、または復号が必要かどうかについて検討します。その結果を、SSL ルールのアクション、復号できないトラフィックのアクション、および SSL ポリシーのデフォルト アクションに反映させます。トラフィックを復号する場合は、次の表に示す情報を収集しておく必要があります。

表 14-4　SSL 復号に必要な情報

復号の対象	必要な情報
制御対象のサーバへの着信トラフィック	サーバ証明書のファイルと秘密キー ファイルのペア
外部サーバへの発信トラフィック	CA 証明書のファイルと秘密キー ファイルのペア CA 証明書と秘密キーを生成することもできます。

詳細については、ルール アクションを使用した暗号化トラフィックの処理と検査の決定（16-9 ページ）を参照してください。

これらの情報を収集したら、システムにアップロードして、再利用可能なオブジェクトを設定します。詳細については、再使用可能オブジェクトの管理（2-1 ページ）を参照してください。

SSL インスペクション アプライアンス展開の分析

ライセンス：機能に依存

ここでは Life Insurance Example, Inc.（LifeIns）という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インスペクションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- カスタマー サービス部門では、単一の ASA FirePOWERデバイスをパッシブ展開する
- 契約審査部門では、単一の ASA FirePOWER デバイスをインライン展開する

カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する見込み顧客からの暗号化された質問や要求を、Web サイトや電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクト メトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマー サービスでは、オンライン フォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。

契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC（MedRepo）という医療データ リポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング（なりすまし）応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと考えています。

LifeIns では、経験の浅い契約審査担当者に対して 6 ヵ月のトレーニング期間を設けています。最近、こうした契約審査担当者が MedRepo のカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのため MedRepo から LifeIns に複数の苦情が提出されています。LifeIns は、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者から MedRepo への要求についても監査を入れることを計画しています。

詳細については、次の項を参照してください。

- 例:パッシブ展開でのトラフィック復号化（14-9 ページ）
- 例:インライン展開でのトラフィック復号化（14-12 ページ）

例:パッシブ展開でのトラフィック復号化

ライセンス:機能に依存

LifeIns のビジネス要件では、カスタマー サービスに次の要求をしています。

- すべての要求と申請書類を 24 時間以内に処理する
- 着信するコンタクト メトリックのコレクション プロセスを改善する
- 着信した不正な申請書類を特定して廃棄する

カスタマー サービス部門では、追加の監査用レビューを必要としません。

LifeIns ではカスタマー サービス デバイスのパッシブ展開を計画しています。

外部ネットワークからのトラフィックは LifeIns のルータに送信されます。ルータはトラフィックをカスタマー サービス部門にルーティングし、検査用にトラフィックのコピーを ASA FirePOWER モジュールに送信します。

管理する ASA FirePOWER モジュールでは、[アクセス コントロール（Access Control）] および [SSL エディタ（SSL Editor）] のカスタム ロールを持つユーザにより、次の SSL インスペクションの設定を行います。

- カスタマー サービス部門に送信された暗号化トラフィックをすべてログに記録する
- オンラインの申請フォームからカスタマー サービスに送信された暗号化トラフィックを復号する
- カスタマー サービスに送信された他の暗号化トラフィックは、オンライン リクエスト フォームからのトラフィックも含め、すべて復号しない

さらに、復号された申請フォーム トラフィック中に偽の申請データが含まれていないかを検査し、検出された場合はログに記録するためのアクセス コントロールも設定します。

次のシナリオでは、ユーザからカスタマー サービスにオンライン フォームが送信されます。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。ASA FirePOWER モジュールは、このトラフィックのコピーを受信します。クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。システムは、ハンドシェイクと接続の詳細に応じて、接続のログを記録し、暗号化トラフィックのコピーを処理します。

詳細については、次のトピックを参照してください。

- パッシブ展開で暗号化トラフィックをモニタする（14-10 ページ）
- パッシブ展開で暗号化トラフィックを復号しない（14-10 ページ）
- パッシブ展開で暗号化トラフィックを秘密キーで検査する（14-11 ページ）

パッシブ展開で暗号化トラフィックをモニタする

ライセンス：任意（Any）

システムは、カスタマー サービスに送信されるすべての SSL 暗号化トラフィックについて、接続のログを記録します。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`info`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`info`）に復号します。
4. モジュールはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、モジュールは接続イベントを生成します。
5. ASA FirePOWER モジュールが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを復号しない

ライセンス：任意（Any）

保険契約に関する要求を含むすべての SSL 暗号化トラフィックは復号されずに許可され、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`info`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`info`）に復号します。

4. ASA FirePOWER モジュールはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、モジュールは接続イベントを生成します。

5. ASA FirePOWER モジュールが接続イベントを受信します。

パッシブ展開で暗号化トラフィックを秘密キーで検査する

ライセンス:任意（Any）

申請フォームのデータを含むすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。

（注） パッシブ展開の場合、DHE または ECDHE 暗号スイートで暗号化されたトラフィックは、既知の秘密キーを使って復号することはできません。

有効な申請フォームの情報を含むトラフィックについては、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`form`）を送信します。クライアントがこれを暗号化（`AaBb`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`form`）に復号します。
4. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（`form`）に復号します。

   アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続します。偽の申請書であることを示す情報は検出されません。セッション終了後、モジュールは接続イベントを生成します。

5. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、復号されたトラフィックに偽の申請データが含まれていた場合、接続および偽のデータについてのログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`fake`）を送信します。クライアントがこれを暗号化（`CcDd`）し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、デバイスにそのトラフィックのコピーを送信します。
3. カスタマー サービス部門のサーバが、暗号化された情報の要求（`CcDd`）を受信し、これをプレーン テキスト（`fake`）に復号します。

4. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（fake）に復号します。

   アクセス コントロール ポリシーは、復号されたトラフィックの処理を継続して、偽の申請書であることを示す情報を検出します。モジュールは侵入イベントを生成します。セッション終了後、デバイスは接続イベントを生成します。

5. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび偽の申請データの侵入イベントを受信します。

例:インライン展開でのトラフィック復号化

ライセンス:機能に依存

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepo への情報要求が適切なすべての規則に準じていることを検証する
- その契約審査によるメトリック コレクション プロセスを改善する
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する
- 契約審査部門から MedRepo のカスタマー サービス部門へのすべての不適切な規制要求を排除する
- 経験豊富な契約審査担当者は監査しない

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。

MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeIns のネットワークにトラフィックがルーティングされます。デバイスはトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送して、ASA FirePOWER モジュールにイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

ASA FirePOWER モジュールでは、次の SSL インスペクションの設定を行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号する
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号しない

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号トラフィックを検査するアクセス コントロールを設定します。

- 復号トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する
- 規制に準拠しない情報を含んでいる復号トラフィックをブロックし、不適切な情報をログに記録する
- 他の暗号化および復号されたトラフィックをすべて許可する

許可された復号トラフィックは、再暗号化されて宛先ホストに転送されます。

次のシナリオでは、ユーザが情報をオンラインでリモート サーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。モジュールはこのトラフィックを受信し、ハンドシェイクと接続の詳細に応じて、システムが接続をログに記録し、トラフィックを処理します。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

詳細については、次のトピックを参照してください。

- インライン展開で暗号化トラフィックをモニタする（14-13 ページ）
- インライン展開で特定ユーザからの暗号化トラフィックを許可する（14-13 ページ）
- インライン展開で暗号化トラフィックをブロックする（14-14 ページ）
- インライン展開で暗号化トラフィックを秘密キーで検査する（14-14 ページ）
- インライン展開で特定ユーザの暗号化トラフィックを、再署名された証明書で検査する（14-15 ページ）

インライン展開で暗号化トラフィックをモニタする

ライセンス：任意（Any）

契約審査部門で送受信されるすべての SSL 暗号化トラフィックについて、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. 契約審査部門のサーバは、暗号化された情報の要求（`AaBb`）を受信し、これをプレーン テキスト（`help`）に復号します。
6. ASA FirePOWER モジュールが接続イベントを受信します。

インライン展開で特定ユーザからの暗号化トラフィックを許可する

ライセンス：Control

経験豊富な契約審査担当者から送信されるすべての SSL 暗号化トラフィックは復号されずに許可され、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（`help`）を送信します。クライアントがこれを暗号化（`AaBb`）し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。

3. ASA FirePOWER モジュールはトラフィックを復号しません。

   アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。

4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
5. リクエスト部門のサーバは、暗号化された情報の要求（AaBb）を受信し、これをプレーン テキスト（help）に復号します。
6. ASA FirePOWER モジュールが接続イベントを受信します。

インライン展開で暗号化トラフィックをブロックする

ライセンス：任意（Any）

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべての SMTPS 電子メール トラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。

次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアント ブラウザから SSL ハンドシェイクの確立要求を受信すると、SSL ハンドシェイクの次のステップとして、サーバ証明書（cert）を LifeIns の契約審査担当者に送信します。
2. MedRepo のルータが証明書を受信し、これを LifeIns の契約審査担当者にルーティングします。
3. ASA FirePOWER モジュールは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. ASA FirePOWER モジュールが接続イベントを受信します。

インライン展開で暗号化トラフィックを秘密キーで検査する

ライセンス：任意（Any）

MedRepo から LifeIns の契約審査部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、アップロードされたサーバ秘密キーを使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（stats）を送信します。クライアントがこれを暗号化（AaBbC）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（stats）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック（AaBbC）を転送し、セッション終了後に接続イベントを生成します。

4. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。

5. 契約審査部門のサーバは、暗号化された情報（AaBbC）を受信し、これをプレーン テキスト（stats）に復号します。
6. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（spoof）を送信しますが、このトラフィックは改変されており、発信元が MedRepo, LLC であるかのように偽装されています。クライアントがこれを暗号化（FfGgH）し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（spoof）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、スプーフィング行為を検出します。ASA FirePOWER モジュールはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
3. 内部ルータは、ブロックされたトラフィックを受信しません。
4. 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。
5. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

インライン展開で特定ユーザの暗号化トラフィックを、再署名された証明書で検査する

ライセンス：Control

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、再署名されたサーバ証明書を使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。

（注） インライン展開においてサーバ証明書の再署名によりトラフィックを復号する場合、ASA FirePOWER モジュールは中間者（man-in-the-middle）として機能します。ここでは 2 つの SSL セッション（クライアントと ASA FirePOWER モジュールの間に 1 つ、ASA FirePOWER モジュールとサーバの間に 1 つ）が作成されます。その結果、暗号セッションの詳細はセッションごとに異なります。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（help）を送信します。クライアントがこれを暗号化（AaBb）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（help）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続します。不適切な要求は検出されません。モジュールはトラフィックを再暗号化（CcDd）して、送信を許可します。セッション終了後、接続イベントを生成します。
4. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。

5. リクエスト部門のサーバは、暗号化された情報（ccDd）を受信し、これをプレーン テキスト（help）に復号します。
6. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントを受信します。

（注）　再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメイン ルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアに CA 証明書を追加します。

これに対し、規制要件を満たさない情報を含んでいる復号トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。

次のステップが実行されます。

1. ユーザが規制要件に準拠していない要求をプレーン テキスト（regs）で送信します。クライアントがこれを暗号化（EeFf）し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（regs）に復号します。

   アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号トラフィックの処理を継続し、不適切な要求を検出します。モジュールはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。
4. 外部ルータは、ブロックされたトラフィックを受信しません。
5. リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。
6. ASA FirePOWER モジュールは、暗号化および復号されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。