

高度なインターフェイス設定

この章では、インターフェイスのMACアドレスを設定する方法、最大伝送ユニット（MTU）を設定する方法、TCP最大セグメントサイズ（TCP MSS）を設定する方法、および同じセキュリティ レベルの通信を許可する方法について説明します。最高のネットワーク パフォーマンスを実現するには、正しい MTU と最大 TCP セグメント サイズの設定が不可欠です。

- インターフェイスの詳細設定について （1 ページ）
- MAC アドレスの自動割り当て （7 ページ）
- 手動 MAC アドレス、MTU、および TCP MSS の設定 （8 ページ）
- 同一のセキュリティ レベル通信の許可 （10 ページ）
- ARP および MAC アドレス テーブルのモニタリング （11 ページ）
- インターフェイスの詳細設定の履歴 （11 ページ）

インターフェイスの詳細設定について

ここでは、インターフェイスの詳細設定について説明します。

MAC アドレス

Media Access Control（MAC）アドレスは、ネットワークデバイスの一意の物理アドレスです。

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。。

（注） 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

デフォルトの MAC アドレス

この参考資料では、ネットワークデバイスで使用されるデフォルトの MAC アドレスとその設定に関する情報を提供します。

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- VLAN インターフェイス（Firepower 1010 および）：ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。手動 MAC アドレス、MTU、および TCP MSS の設定 （8 ページ）を参照してください。

  トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。手動 MAC アドレス、MTU、および TCP MSS の設定（8 ページ）を参照してください。
- EtherChannel：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- EtherChannel（ASA モデル）：ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポート チャネル インターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイス メンバーシップが変更された場合に備えて、一意の MAC アドレスを構成することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス：物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーに

よっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスはMACアドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成が有効になっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効な場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されるプレフィックスです。*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます（*xxyy*）。

A2**4D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンド リファレンスの **mac-address auto** コマンドを参照してください。

MTU

Maximum Transmission Unit（MTU）は、ASA が特定のイーサネット インターフェイスで送信できる最大フレームペイロードサイズを指定します。MTU 値には、イーサネットヘッダー、VLAN タグ、その他のオーバーヘッドは含まれません。たとえば MTU を 1500 に設定した場合、想定されるフレームサイズはヘッダーを含めて 1518 バイト、VLAN タギングを使用する

場合は1522バイトです。これらのヘッダーに対応するためにMTU値を高く設定しないでください。

VXLAN および Geneve カプセル化の要件

VXLAN または Geneve では、イーサネットデータグラム全体がカプセル化されるため、新しいIPパケットは大きくなり、より大きなMTUが必要になります。ASA VTEP送信元インターフェイスMTUを、ネットワークMTUに54バイト（VXLANの場合）または306バイト（Geneveの場合）を加えた値に設定します。

パスのMTU検出

パスMTUディスカバリは、2台のホスト間のネットワークパス内のすべてのデバイスでMTUを調整できます。したがってパスの最小MTUの標準化が可能です。

パス MTU ディスカバリのサポート

ASAは、パスMTUディスカバリ（RFC 1191で定義）をサポートしています。

デフォルト MTU

ASAのデフォルトMTUは、1500バイトです。この値には、イーサネットヘッダー、VLANタギングや他のオーバーヘッド分の18～22バイトは含まれません。

VTEP送信元インターフェイスのVXLANを有効にし、MTUが1554バイト未満の場合、ASAは自動的にMTUを1554バイトに増やします。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きなMTUが必要になります。一般的には、ASA送信元インターフェイスMTUをネットワークMTU＋54バイトに設定する必要があります。

MTU とフラグメンテーション

指定されたMTUより大きいIPv4パケットは、複数のフレームにフラグメント化されます。

パケット処理の詳細

IPv4では、出力IPパケットが指定されたMTUより大きい場合、2つ以上のフレームにフラグメント化されます。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6では、通常、パケットをフラグメント化することはできません。したがって、フラグメント化を避けるために、IPパケットをMTUサイズ以内に収める必要があります。

TCPパケットでは、通常、エンドポイントはMTUを使用してTCPの最大セグメントサイズを決定します（MTU - 40など）。途中で追加のTCPヘッダーが追加された場合（たとえば、サイト間VPNトンネル）、TCP MSSはトンネリングエンティティで下方調整しないといけない場合があります。TCP MSS （5 ページ）を参照してください。

UDPまたはICMPの場合、アプリケーションではフラグメント化を避けるためにMTUを考慮する必要があります。

（注） ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

検査対象のフラグメント化されたパケットの完全な再アセンブリ

ASA はデフォルトで仮想再アセンブリを実行します。ただし、DNS や音声メディア検査などの機能がアクティブになっている場合、ファイアウォールは転送前に完全な再アセンブリを実行します。これにより、パケットが検査エンジンによって正しく処理されます。

たとえば、検査対象の SIP パケットには完全な再アセンブリが必要です。SIP 検査が無効になっている場合、システムは仮想再アセンブリを維持します。問題を回避するため、大きな SIP INVITE パケットを UDP 経由で送信するのではなく、SIP メッセージサイズを小さくするか、大きなメッセージには TCP または TLS を使用することを推奨します。

ファイアウォールはメモリ内でフラグメントを結合します。出力インターフェイスの MTU が再アセンブルされたパケットよりも小さい場合、デバイスはデータが収まるように再フラグメント化します。動作を確認するには、出力インターフェイスでパケットキャプチャを使用し、必要に応じて MTU 設定を調整します。

MTU とジャンボフレームの設定

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。

- トラフィック パスの MTU の一致：すべての ASA インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボフレームへの対応：ジャンボフレームが有効な場合、MTU を 9,000 バイト以上に設定できます。最大値はモデルによって異なります。

TCP MSS

最大セグメント サイズ（TCP MSS）とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。TCP MSS 値は、接続を確立するときのスリーウェイハンドシェイク中に、クライアントとサーバーの間で交換されます。UDP パケットは影響を受けません。

TCP MSS の設定と動作

通過トラフィック用に、ASA で TCP MSS を設定できます。デフォルトで、最大 TCP MSS は 1380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化のパケットサイズを大きくする必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、ASA の最大 TCP MSS を無効化する必要があります。

最大 TCP MSS を設定している場合、接続のいずれかのエンドポイントがこの値を超える TCP MSS を要求すると、ASA は要求パケット内の TCP MSS を ASA の最大 TCP MSS で上書きしま

す。ホストやサーバーが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイト（IPv4）または 1220 バイト（IPv6）を想定しますが、パケットを変更することはありません。

また、最小 TCP MSS を設定することもできます。ホストまたはサーバーが非常に小さな TCP MSS を要求した場合、ASA は値を増やすことができます。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。ASA は MTU から TCP MSS を算出します。IPv4 の場合は MTU マイナス 40、IPv6 の場合は MTU マイナス 60 です。

TCP MSS 調整

たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。ASA の最大 TCP MSS が 1380（デフォルト）の場合は、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。ASA は最大 120 バイトのヘッダーをパケットに追加でき、追加後のパケットも 1500 バイトの MTU サイズに収まります。

デフォルト TCP MSS

デフォルトの TCP MSS は、ASA の最大 TCP MSS をデフォルトで 1380 バイトに設定するネットワーク設定であり、ヘッダーが最大 120 バイトの IPv4 IPSec VPN 接続に対応し、デフォルト MTU の 1500 バイト内に適合します。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして ASA を使用しない場合は、FlexConfig の Sysopt_Basic オブジェクトを使用して TCP MSS 設定を参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。一般に接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

インターフェイス間通信

同じセキュリティ レベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。

  各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0～100）に1つのインターフェイスしか設定できません。

- ACL がなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

インターフェイス内通信（ルーテッド ファイアウォール モード）

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブアンドスポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

MAC アドレスの自動割り当て

この項では、MAC アドレスの自動生成の設定方法について説明します。マルチ コンテキスト モードの場合、この機能によって、コンテキストに割り当てられたすべてのインターフェイス タイプに一意の MAC アドレスが割り当てられます。 シングル モードでは、この機能によって、VLAN サブインターフェイスに一意の MAC アドレスが割り当てられます。

始める前に

- インターフェイスの名前を設定すると、ただちに新規 MAC アドレスが生成されます。インターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻

ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration]** > **[Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

手順

ステップ 1 マルチ コンテキスト モードの場合：システムで次の手順を実行します。

a) **[Configuration]** > **[Context Management]** > **[Security Contexts]** の順に選択します。
b) [Mac-Address auto] をオンにします。
c) （任意） [Prefix] チェックボックスをオンにしてから、フィールドに 0 ～ 65535 の範囲内の 10 進数値を入力します。

このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。プレフィックスを入力しない場合は、ASA によって、インターフェイス MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

ステップ 2 シングル コンテキスト モードの場合：次の手順を実行します。

a) **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。
b) ページの下部で、[Enable auto-generation of MAC addresses for subinterfaces] チェックボックスをオンにします。
c) （任意） [Prefix] フィールドで、0 ～ 65535 の 10 進数値を入力します。

このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。プレフィックスを入力しない場合は、ASA によって、インターフェイス MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

ステップ 3 [Apply] をクリックします。

手動 MAC アドレス、MTU、および TCP MSS の設定

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替え

るには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイス行を選択して、[Edit] をクリックします。

[インターフェイスを編集（Edit Interface）] ダイアログボックスが、[全般（General）] タブが選択された状態で表示されます。

ステップ 3 [詳細（Advanced）] タブをクリックします。

ステップ 4 MTU を設定する、またはジャンボフレームのサポート（サポート対象モジュールのみ）をイネーブルにするには、[MTU] フィールドに値を入力します。最小値と最大値は、プラットフォームによって異なります。

デフォルト値は 1500 バイトです。

（注） ポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

- ジャンボフレームをサポートする、シングルモードのモデルの場合：いずれかのインターフェイスに 1500 を超える値を入力すると、ジャンボフレームサポートがすべてのインターフェイスに対して自動的にイネーブルになります。すべてのインターフェイスの MTU の設定を 1500 未満に戻すと、ジャンボ フレーム サポートが無効になります。
- ジャンボフレームをサポートするマルチモードの場合：いずれかのインターフェイスに 1500 を超える値を入力する場合、お使いのモデルで必要があれば、システム コンフィギュレーションのジャンボフレームサポートを必ずイネーブルにしてください。ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000）を参照してください。

（注） 一部のモデルでは、ジャンボフレームサポートを有効化または無効化する場合、ASA をリロードする必要があります。

ステップ 5 MAC アドレスをこのインターフェイスに手動で割り当てるには、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 6 フェールオーバーを使用する場合、[スタンバイMACアドレス（Standby Mac Address）] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタ

ンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 7 TCP MSS を設定するには、**[設定（Configuration）] > [ファイアウォール（Firewall）] > [詳細（Advanced）] > [TCPオプション（TCP Options）]** の順に選択します。次のオプションを設定できます。

- [拒否された外部TCPパケットのリセット応答を送信します（Send reset reply for denied outside TCP packets）]：ASA の通過を試みたものの アクセスリストまたは AAA 設定に基づいて ASA によって拒否されたすべての発信 TCP セッションに関して、ASA が TCP リセットを送信できるようになります。
- [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能を無効にするには、bytes を 0 に設定します。
- [Force Minimum Segment Size for TCP]：48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメントサイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。

ステップ 8 [Secure Group Tagging] 設定については、ファイアウォール コンフィギュレーション ガイドを参照してください。

ステップ 9 （Secure Firewall 3100）[自動ネゴシエーション（Auto-negotiate）] をクリックして、1 ギガビット以上のインターフェイスのリンクステータスとフロー制御をネゴシエートします。

自動ネゴシエーションは、速度とは別に設定されます。一部のスイッチは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合は、Cisco ASA のインターフェイスを手動速度に設定し、[自動ネゴシエーション（Auto-negotiate）] も無効にして、リンクがアップ状態になるようにします。

ステップ 10 [ASA Cluster] 設定については、（推奨、マルチコンテキストモードでは必須）制御ノードでのインターフェイスの設定を参照してください。

同一のセキュリティ レベル通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

手順

ステップ 1 同じセキュリティ レベルのインターフェイス間の通信を有効にするには、**[Configuration]** > **[Interfaces]** ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。

ステップ 2 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、[Enable traffic between two or more hosts connected to the same interface] をオンにします。

ARP および MAC アドレス テーブルのモニタリング

- **[Monitoring] > [Interfaces] > [ARP Table]**

  スタティック エントリやダイナミック エントリを含む ARP テーブルを表示します。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

- **[Monitoring] > [Interfaces] > [MAC Address Table]**

  スタティックおよびダイナミック MAC アドレス エントリを表示します。

インターフェイスの詳細設定の履歴

表 *1*: インターフェイスの詳細設定の履歴

機能名	リリース	機能情報
最大 MTU が 9198 バイトになりました	9.1(6)、9.2(1)	ASA で使用できる最大の MTU は 9198 バイトです（CLI のヘルプでご使用のモデルの正確な最大値を確認してください）。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性がありました。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。 次の画面が変更されました。**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Edit Interface]** > **[Advanced]**

機能名	リリース	機能情報
Firepower 4100/9300 シャーシ の ASA のMTU サイズ増加	9.6(2)	Firepower 4100 および 9300 で、最大 MTU を 9184 バイトに設定できます。これまでは 9000 バイトが最大でした。この MTU は FXOS 2.0.1.68 以降でサポートされます。 次の画面が変更されました。**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Advanced]**
シングル コンテキスト モード用の一意の MAC アドレス生成	9.8(3), 9.8(4), 9.9(2)	シングル コンテキスト モードで VLAN サブインターフェイスの一意の MAC アドレス生成を有効にできるようになりました。通常、サブインターフェイスはメインインターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更されたコマンド：**mac-address auto** ASDM サポートはありません。
シングルコンテキストモード用の一意の MAC アドレスの生成に関する ASDM のサポート	ASDM 7.15(1)	ASDM でシングルコンテキストモードの VLAN サブインターフェイス用に一意の MAC アドレスを生成することを有効にできるようになりました。通常、サブインターフェイスはメイン インターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更された画面：**[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]**
Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。	9.17(1)	Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。他のモデルの SFP ポートの場合、**no speed nonegotiate** オプションは速度を 1000 Mbps に設定します。新しいコマンドは、自動ネゴシエーションと速度を個別に設定できることを意味します。 新規/変更された画面： **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Advanced]**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。