Cisco Secure Firewall ASDM 7.20(x) リリースノート

最終更新：2024 年 10 月 4 日

Cisco Secure Firewall ASDM 7.20(x) リリースノート

このドキュメントには、 Cisco Secure Firewall ASA 対応の ASDM バージョン 7.20(x) のリリース情報が記載されています。

（注） ASA 9.20(1) は、Cisco Secure Firewall 4200 でのみサポートされます。以降のリリースは、他のモデルでサポートされます。

特記事項

- **ASA 9.20(2) は、現在のすべてのモデルをサポートします。**
- **プレフィックスリストと一致するルートマップを指定する OSPF redistribute コマンドは、9.20(2) で削除されます。**9.20(2) にアップグレードすると、指定された**ルートマップ**が **match ip address prefix-list** を使用する OSPF **redistribute** コマンドが設定から削除されます。プレフィックスリストはサポートされていませんが、パーサーでは引き続きこのコマンド使用できます。アップグレードする前に、**match ip address** コマンドで ACL を指定するルートマップを使用するように OSPF を再設定する必要があります。
- **ASA バージョン 9.20(1) は、Cisco Secure Firewall 4200 のみをサポートします。**ASDM 7.20(1) は、9.20(1) 上の Cisco Secure Firewall 4200 をサポートしますが、他のプラットフォーム上の以前のリリースとも下位互換性があります。
- **ASDM の自己署名証明書は、ASA との日時の不一致により無効になります。**ASDM は自己署名 SSL 証明書を検証し、ASA の日付が証明書の **[発行日（Issued On）]** と **[有効期限（Expires On）]** の日付の範囲内にない場合は起動しません。詳細については、ASDM の互換性に関する注意事項 （2 ページ）を参照してください。

システム要件

ASDM には、4 コア以上の CPU を搭載したコンピュータが必要です。コア数が少ないと、メモリ使用量が高くなる可能性があります。

ASDM Java の要件

ASDM は、Oracle JRE 8.0（**asdm-*version*.bin**）または OpenJRE 1.8.x（**asdm-openjre-*version*.bin**）を使用してインストールできます。

表 *1*: *ASDM* オペレーティングシステムとブラウザの要件

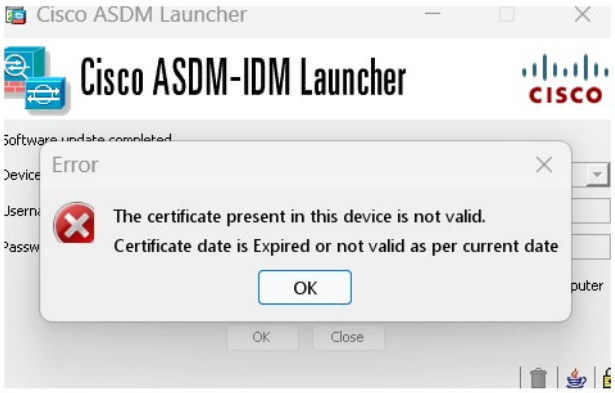
オペレーティング システム	ブラウザ			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows（英語および日本語）： • 11 • 10 （注） ASDM ショートカットに問題がある場合は、ASDM の互換性に関する注意事項 （2 ページ）の「Windows 10」を参照してください。 • 8 • 7 • Server 2016 と Server 2019 • Server 2012 R2 • Server 2012 • Server 2008	対応	サポートなし	対応	8.0 バージョン 8u261 以降	1.8 （注） Windows 7 または 10（32 ビット）のサポートなし
Apple OS X 10.4 以降	対応	対応	対応（64 ビット バージョンのみ）	8.0 バージョン 8u261 以降	1.8

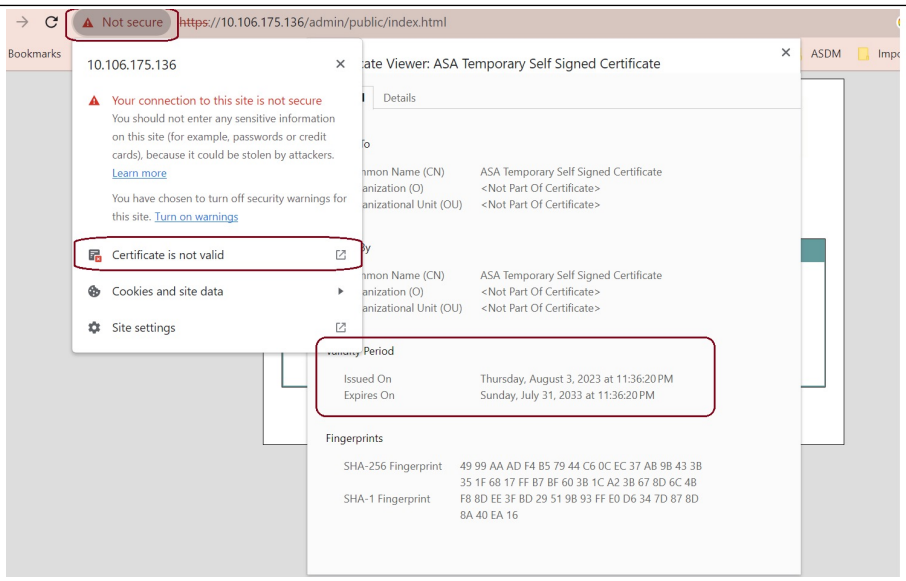
ASDM の互換性に関する注意事項

次の表に、ASDM の互換性に関する警告を示します。

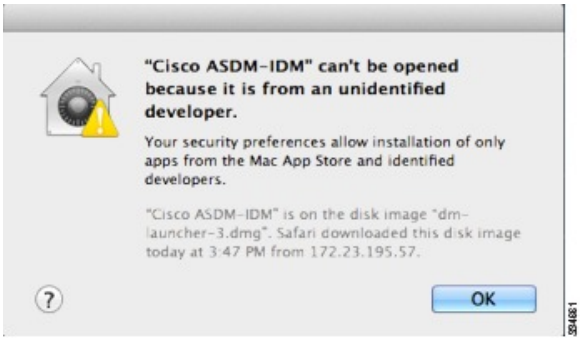
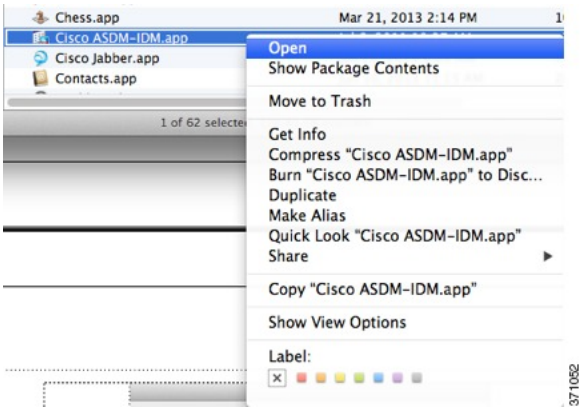
条件	注意
ASDM Launcher と ASDM バージョンの互換性	「デバイスマネージャを起動できません（Unable to Launch Device Manager）」というエラーメッセージが表示されます。 新しいASDMバージョンにアップグレードしてからこのエラーが発生した場合は、最新の Launcher を再インストールする必要があります。 1. ASA（https://<asa_ip_address>）で ASDM Web ページを開きます。 2. [ASDMランチャーのインストール（Install ASDM Launcher）] をクリックします。 **図 *1 : ASDM Launcher* のインストール**  3. ユーザー名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。 HTTPS認証が設定されていない場合は、ユーザー名および**イネーブル**パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDMにログインしたときには、この動作は適用されません。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。**注**：HTTPS 認証をイネーブルにした場合、ユーザー名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力すると、ASDMによってローカルデータベースで一致がチェックされます。

条件	注意
ASA との日時の不一致により、自己署名証明書が無効になります	

条件	注意
	ASDM は自己署名 SSL 証明書を検証し、ASA の日付が証明書の [発行日（Issued On）] と [有効期限（Expires On）] の日付の範囲内にない場合は起動しません。日時が一致しない場合は、次のエラーが表示されます。 **図 *2*：証明書が無効です**  **この問題を解決するには、**ASA で正しい時刻を設定し、リロードします。 証明書の日付を確認するには、次の手順を実行します（例は Chrome）。 **1.** https://*device_ip* に移動します。 **2.** メニューバーの [安全ではない（Not secure）] テキストをクリックします。 **3.** [証明書が無効です（Certificate is not valid）] をクリックして、証明書ビューアを開きます。 **4.** [有効期間（Validity Period）] をオンにします。 **図 *3*：証明書ビューア**

条件	注意
	
Windows Active Directory ディレクトリアクセス	場合によっては、Windows ユーザーの Active Directory 設定によって、Windows で ASDM を正常に起動するために必要なプログラムファイルの場所へのアクセスが制限されることがあります。次のディレクトリへのアクセスが必要です。 • デスクトップフォルダ • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems Active Directory がディレクトリアクセスを制限している場合は、Active Directory 管理者にアクセスを要求する必要があります。

条件	注意
Windows 10	「**This app can't run on your PC**」エラー メッセージ。 ASDM ランチャをインストールすると、Windows 10 によって ASDM ショートカットターゲットが Windows Scripting Host パスに置き換えられて、このエラーが発生することがあります。ショートカットターゲットを修正するには、次の手順を実行します。 **1.** **[Start]** > **[Cisco ASDM-IDM Launcher]** を選択し、[Cisco ASDM-IDM Launcher] アプリケーションを右クリックします。 **2.** **[More]** > **[Open file location]** を選択します。 Windows は、ショートカットアイコンを使用してディレクトリを開きます。 **3.** ショートカット アイコンを右クリックして、[Properties] を選択します。 **4.** [Target] を次のように変更します。 **C:\Windows\System32\wscript.exe invisible.vbs run.bat** **5.** [OK] をクリックします。
OS X	OS X では、ASDM の初回実行時に、Java のインストールを要求される場合があります。必要に応じて、プロンプトに従います。インストールの完了後に ASDM が起動します。

条件	注意
OS X 10.8 以降	ASDM は Apple Developer ID で署名されていないため、実行できるようにする必要があります。セキュリティの設定を変更しないと、エラー画面が表示されます。  1. ASDM を実行できるようにするには、[Cisco ASDM-IDM Launcher] アイコンを右クリック（またはCtrl キーを押しながらクリック）して、[Open] を選択します。  2. 同様のエラー画面が表示されますが、この画面から ASDM を起動できます。[Open] をクリックします。ASDM-IDM ランチャが起動します。 

条件	注意
ASA では強力な暗号化ライセンス（3DES/AES）が必要 （注） スマートライセンスモデルを使用すると、強力な暗号化ライセンスを使用せずに ASDM での最初のアクセスが可能になります。	ASDM では、ASA に SSL 接続する必要があります。シスコが提供している 3DES ライセンスを要求できます。 1. www.cisco.com/go/license にアクセスします。 2. [Continue to Product License Registration] をクリックします。 3. ライセンシング ポータルで、テキスト フィールドの横にある [Get Other Licenses] をクリックします。 4. ドロップダウン リストから、[IPS, Crypto, Other...] を選択します。 5. [Search by Keyword] フィールドに「ASA」と入力します。 6. [Product] リストで [Cisco ASA 3DES/AES License] を選択し、[Next] をクリックします。 7. ASA のシリアル番号を入力し、プロンプトに従って ASA の 3DES/AES ライセンスを要求します。
• 自己署名証明書または信頼できない証明書 • IPv6 • Firefox および Safari	ASA が自己署名証明書または信頼できない証明書を使用する場合、Firefox と Safari では、IPv6 を介した HTTPS を使用して参照する場合にはセキュリティ例外を追加することはできません。https://bugzilla.mozilla.org/show_bug.cgi?id=633001 を参照してください。この警告は、Firefox または Safari から ASA に発信されるすべての SSL 接続に影響します（ASDM 接続を含む）。この警告を回避するには、信頼できる認証局が ASA に対して発行した適切な証明書を設定します。
• ASA で SSL 暗号化を行うには、RC4-MD5 と RC4-SHA1 を両方とも含めるか、Chrome で SSL false start を無効にする必要があります。 • Chrome	RC4-MD5 および RC4-SHA1 アルゴリズム（これらのアルゴリズムはデフォルトでイネーブル）の両方を除外するために ASA の SSL 暗号化を変更した場合、Chrome の「SSL false start」機能のために Chrome は ASDM を起動できません。これらのアルゴリズムのいずれかを再度有効にすることを推奨します（**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[詳細（Advanced）]** > **[SSL設定（SSL Settings）]** ペインを参照）。または、「Run Chromium with flags」に従って **--disable-ssl-false-start** フラグを使用して Chrome の SSL false start を無効にできます。

ASDM のアイデンティティ証明書のインストール

Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。

ASDM と一緒に使用するために ASA に自己署名アイデンティティ証明書をインストールしたり、証明書を Java に登録したりするには、『Install an Identity Certificate for ASDM』[英語] を参照してください。

ASDM コンフィギュレーションメモリの増大

ASDM でサポートされる最大設定サイズは 512 KB です。このサイズを超えると、パフォーマンスの問題が生じることがあります。たとえば、コンフィギュレーションのロード時には、完了したコンフィギュレーションの割合がステータスダイアログボックスに表示されます。このとき、サイズの大きいコンフィギュレーションでは、ASDM によってまだコンフィギュレーションの処理が行われていても、完了した割合の増分が停止し、操作が中断されているように見えます。このような状況が発生した場合は、ASDM システム ヒープ メモリの増大を検討することを推奨します。メモリが枯渇していることを確認するには、Java コンソールで「java.lang.OutOfMemoryError」メッセージをモニターします。

Windows での ASDM コンフィギュレーションメモリの増大

ASDM ヒープメモリサイズを増大するには、次の手順を実行して **run.bat** ファイルを編集します。

手順

ステップ 1 ASDM インストールディレクトリ（たとえば、C:\Program Files (x86)\Cisco Systems\ASDM）に移動します。

ステップ 2 任意のテキストエディタを使用して **run.bat** ファイルを編集します。

ステップ 3 「start javaw.exe」で始まる行で、「-Xmx」のプレフィックスが付いた引数を変更し、目的のヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

ステップ 4 **run.bat** ファイルを保存します。

Mac OS での ASDM コンフィギュレーションメモリの増大

ASDM ヒープメモリサイズを増大するには、次の手順を実行して **Info.plist** ファイルを編集します。

手順

ステップ 1 [Cisco ASDM-IDM] アイコンを右クリックし、[Show Package Contents] を選択します。

ステップ 2 [Contents] フォルダで、Info.plist ファイルをダブルクリックします。開発者ツールをインストールしている場合は、**プロパティリストエディタ** で開きます。そうでない場合は、**TextEdit** で開きます。

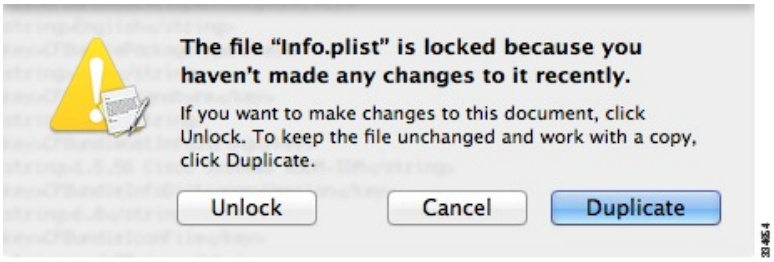
ステップ 3 **[Java]** > **[VMOptions]** で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>


  <key>CFBundleDocumentTypes</key>
    <array>
```

ステップ 4 このファイルがロックされると、次のようなエラーが表示されます。



ステップ 5 [Unlock] をクリックし、ファイルを保存します。

[Unlock] ダイアログボックスが表示されない場合は、エディタを終了します。[Cisco ASDM-IDM] アイコンを右クリックし、[Copy Cisco ASDM-IDM] を選択して、書き込み権限がある場所（デスクトップなど）に貼り付けます。その後、このコピーからヒープサイズを変更します。

ASA と ASDM の互換性

ASA/ASDM ソフトウェアおよびハードウェアの要件およびモジュールの互換性を含む互換性の詳細については、『Cisco Secure Firewall ASA Compatibility』を参照してください。

VPN の互換性

VPN の互換性については、『Supported VPN Platforms, Cisco ASA 5500 Series 』を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。

（注） syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

ASA 9.20(2)/ASDM 7.20(2) の新機能

リリース日：**2023** 年 **12** 月 **13** 日

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 3100 における 100GB ネットワークモジュールのサポート	Cisco Secure Firewall 3100 で 100GB のネットワークモジュールを使用できるようになりました。このモジュールは、Cisco Secure Firewall 4200 でもサポートされています。
Cisco Secure Firewall 4200 の接続制限の引き上げ	最大接続数が引き上げられました。 • 4215：15M → **40M** • 4225：30M → **80M** • 4245：60M → **80M**
OCI 上の ASAv：追加のインスタンス	OCI 上の ASA 仮想インスタンスは、最高のパフォーマンスとスループットレベルを達成するために追加のシェイプをサポートするようになりました。
ハイ アベイラビリティとスケーラビリティの各機能	
Azure 上の ASAv：ゲートウェイロード バランシングによるクラスタリング	Azure Resource Manager（ARM）テンプレートを使用した Azure での ASA 仮想クラスタリングの展開がサポートされるようになり、ネットワークトラフィックのロードバランシングにゲートウェイロードバランサ（GWLB）を使用するように ASAv クラスタが設定されています。 新しい/変更された画面：
AWS 上の ASAv：ゲートウェイロード バランシングによるクラスタリングの復元力	AWS のターゲットグループサービスでターゲット フェールオーバー オプションを設定できます。これにより、仮想インスタンスのフェールオーバーが発生した場合に GWLB が既存のフローを正常なターゲットに転送できます。ASAv クラスタリングでは、各インスタンスがターゲットグループに関連付けられ、ターゲットフェールオーバーオプションが有効になっています。これは、GWLB が異常なターゲットを識別して、ターゲットグループ内のターゲットノードとして識別または登録されている正常なインスタンスにネットワークトラフィックをリダイレクトまたは転送するのに役立ちます。
シャーシハートビート障害後にクラスタに再参加するための設定可能な遅延（Firepower 4100/9300）	デフォルトでは、シャーシハートビート障害から回復すると、ノードはすぐにクラスタに再参加します。ただし、**health-check chassis-heartbeat-delay-rejoin** コマンドを設定すると、**health-check system auto-rejoin** コマンドの設定に従って再参加します。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [高可用性と拡張性（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [自動再参加（Auto Rejoin）]**

機能	説明
show failover statistics にクライアント統計情報を追加	フェールオーバークライアントのパケット統計情報が拡張され、デバッグ機能が向上しました。**show failover statistics** コマンドは、**np-clients**（データパスクライアント）および **cp-clients**（コントロールプレーン クライアント）の情報を表示するように拡張されています。 変更されたコマンド：**show failover statistics cp-clients**、**show failover statistics np-clients** *9.18(4)* でも同様です。
show failover statistics events に新しいイベントを追加	**show failover statistics events** コマンドが拡張され、アプリケーション エージェントによって通知されるローカル障害（フェールオーバーリンクの稼働時間、スーパーバイザハートビート障害、およびディスクフルの問題）を表示するようになりました。 変更されたコマンド： **show failover statistics events** *9.18(4)* でも同様です。

ASA 9.20(1)/ASDM 7.20(1) の新機能

リリース：**2023** 年 **9** 月 **7** 日

（注） このリリースは、Cisco Secure Firewall 4200 でのみサポートされます。

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 4200	Cisco Secure Firewall 4215、4225、および 4245 向けの ASA を導入しました。Cisco Secure Firewall 4200 は、スパンド EtherChannel クラスタリングで最大 8 ユニットをサポートします。ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Cisco Secure Firewall 4200 の 25 Gbps 以上のインターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSDは自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。管理インターフェイスが 2 つあります。
ファイアウォール機能	

機能	説明
sysopt connection tcp-max-unprocessed-seg コマンドの ASDM サポート	TCP 未処理セグメントの最大数を 6 ～ 24 に設定できます。デフォルト値は 6 です。SIP 電話機が Call Manager に接続していないことを確認したら、未処理の TCP セグメントの最大数を増やすことができます。 新規/変更された画面：**[設定（Configuration）] > [ファイアウォール（Firewall）] > [高度（Advanced）] > [TCPオプション（TCP Options）]**
データプレーンにオフロードされた ASP ルールエンジンのコンパイル。	デフォルトでは、ルールベースのポリシー（ACL、NAT、VPN など）に 100 を超えるルール更新がある場合、ASP ルールエンジンのコンパイルはコントロールプレーンではなくデータプレーンにオフロードされます。このオフロードにより、コントロールプレーンで他のタスクを実行する時間が長くなります。 次のコマンドが追加または変更されました。**asp rule-engine compile-offload**、**show asp rule-engine**。
ハイ アベイラビリティとスケーラビリティの各機能	
ASA の高可用性のための偽フェールオーバーの削減	ASA 高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳や CPU の過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。 *9.18(4)* でも同様です。
フローステータスの設定可能なクラスタキープアライブ間隔	フローオーナーは、キープアライブ（clu_keepalive メッセージ）と更新（clu_update メッセージ）をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15 ～ 55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [高可用性と拡張性（High Availability and Scalability）] > [ASAクラスタ（ASA Cluster）] > [クラスタの設定（Cluster Configuration）]**
ルーティング機能	
EIGRPv6	EIGRP for IPv6 を設定し、それらを個別に管理できるようになりました。各インターフェイスで EIGRP を設定するときは、IPv6 を明示的に有効にする必要があります。 新規/変更された画面：**[設定（Configuration）] > [デバイスの設定（Device Setup）] > [ルーティング（Routing）] > [EIGRPv6]**、[セットアップ（Setup）]、[フィルタルール（Filter Rules）]、[インターフェイス（Interface）]、[パッシブインターフェイス（Passive Interface）]、[再配布（Redistribution）]、および [スタティックネイバー (Static Neighbor）] タブ。

機能	説明
HTTPクライアントによるパスモニタリング	PBRは、特定の宛先IPのメトリックではなく、アプリケーションドメインのHTTPクライアントを介したパスモニタリングによって収集されたパフォーマンスメトリック（RTT、ジッター、パケット損失、およびMOS）を使用できるようになりました。インターフェイスのHTTPベースのアプリケーションモニタリングオプションは、デフォルトで有効になっています。HTTPベースのパスモニタリングは、ネットワーク サービス グループのオブジェクトを使用してインターフェイスで設定できます。モニタリング対象のアプリケーションが搭載され、パスを決定するためのインターフェイスの順序付けを行う一致 ACL を使用して、PBR ポリシーを設定できます。 新規/変更された画面：**[設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [パスモニタリング（Path Monitoring）]**
インターフェイス機能	
VXLAN VTEP IPv6 のサポート	VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 では、ASA 仮想 クラスタ制御リンクまたは Geneve カプセル化がサポートされていません。 新しい/変更された画面： • **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [VXLAN]** • **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [VNIインターフェイス（VNI Interface）]**
DNS、HTTP、ICMP、IPsec フローオフロードのループバックインターフェイスのサポート	ループバック インターフェイスを追加して、以下に使用できるようになりました。 • DNS • HTTP • ICMP • IPsec フローのオフロード
ライセンス機能	
スマートライセンスやSmart Call Homeといったクラウドサービスの IPv6	ASA は、スマートライセンスや Smart Call Home などのクラウドサービスの IPv6 をサポートするようになりました。
証明書の機能	

機能	説明
OCSP および CRL の IPv6 PKI	ASA で、IPv4 と IPv6 両方の OCSP および CRL URL をサポートするようになりました。URL で IPv6 を使用する場合は、角カッコで囲む必要があります。 新規/変更された画面：**[設定（Configuration）] > [サイト間VPN（Site-to-Site VPN）] > [証明書管理（Certificate Management）] > [CA証明書（CA Certificates）] > [追加（Add）]**
管理、モニタリング、およびトラブルシューティングの機能	
SNMP syslog のレート制限	システム全体のレート制限を設定しない場合、SNMP サーバーに送信される syslog に対して個別にレート制限を設定できるようになりました。 新規/変更されたコマンド： **logging history rate-limit**
スイッチのパケットキャプチャ	スイッチの出力および入力トラフィックパケットをキャプチャするように設定できるようになりました。このオプションは、Secure Firewall 4200 モデルデバイスに対してのみ使用できます。 新規/変更された画面：**[ウィザード（Wizards）] > [パケット キャプチャ ウィザード（Packet Capture Wizard）] > [入力トラフィックセレクタ（Ingress Traffic Selector）]** および **[ウィザード（Wizards）] > [パケット キャプチャ ウィザード（Packet Capture Wizard）] > [出力トラフィックセレクタ（Egress Traffic Selector）]**
VPN 機能	
暗号デバッグの機能拡張	暗号デバッグの機能拡張は次のとおりです。 • 暗号アーカイブは、テキスト形式とバイナリ形式の 2 つの形式で使用できるようになりました。 • 追加の SSL カウンタ。 • スタックした暗号化ルールは、デバイスを再起動せずに ASP テーブルから削除できます。
IKEv2 の複数のキー交換	ASA は、量子コンピュータ攻撃から IPsec 通信を保護するために、IKEv2 で複数のキー交換をサポートします。
SAML を使用した セキュアクライアント 接続認証	DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるローカルベース URL を指定できます。 新規/変更された画面： **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [安全なクライアント接続プロファイル（Secure Client Connection Profiles）] > [追加/編集（Add/Edit）] > [ベーシック（Basic）] > [SAMLアイデンティティ プロバイダー（SAML Identity Provider）] > [管理（Manage）] > [追加/編集（Add/Edit）]**
ASDM 機能	
Windows 11 のサポート	ASDM は Windows 11 で動作することが確認されています。

ソフトウェアのアップグレード

このセクションには、アップグレードを完了するためのアップグレードパス情報とリンクが記載されています。

アップグレードリンク

アップグレードを完了するには、『ASA アップグレード ガイド』を参照してください。

アップグレードパス：ASA アプライアンス

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- ASDM：**[Home]** > **[Device Dashboard]** > **[Device Information]** の順に選択します。
- CLI：**show version** コマンドを使用します。

次の表に、ASA のアップグレードパスを示します。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要な場合があります。推奨バージョンは**太字**で示されています。

開始バージョンと終了バージョンの間で、各リリースのアップグレードガイドラインを必ず確認してください。場合によっては、アップグレードする前に構成を変更する必要があります。そうしないと、停止が発生する可能性があります。

ASA のセキュリティの問題と、各問題に対する修正を含むリリースについては、ASA Security Advisories を参照してください。

（注） ASA 9.18 は Firepower 4110、4120、4140、4150、および Firepower 9300 のセキュリティモジュール SM-24、SM-36、SM-44 の最終バージョンです。

ASA 9.16 は ASA 5506-X、5508-X、および 5516-X の最終バージョンです。

ASA 9.14 は ASA 5525-X、5545-X、および 5555-X の最終バージョンです。

ASA 9.12 は ASA 5512-X、5515-X、5585-X、および ASASM 用の最終バージョン、

ASA 9.2 は ASA 5505 の最終バージョンです。

ASA 9.1 は ASA 5510、5520、5540、5550、および 5580 の最終バージョンです。

表 *2:* アップグレードパス

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.19	—	次のいずれかになります。 → **9.20**

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.18	—	次のいずれかになります。 → **9.20** → **9.19**
9.17	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18**
9.16	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.13	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.12	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.9	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.7	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.6	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.5	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.4	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.3	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.2	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15 → 9.14 → 9.12 → 9.8
9.1(2)、9.1(3)、9.1(4)、9.1(5)、9.1(6)、または 9.1(7.4)	—	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.0(2)、9.0(3)、または 9.0(4)	—	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.6 → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.0(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.6(1)	→ 9.0(4)	次のいずれかになります。 → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4)
8.4(5+)	—	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) ～ 8.4(4)	→ 9.0(4)	→ **9.12** → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4)

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
8.2 以前	→ 9.0(4)	次のいずれかになります。 → **9.12** → 9.8 → 9.1(7.4)

アップグレードパス：Firepower 2100 の ASA（プラットフォームモード）

現在のバージョンとモデルを表示するには、次のいずれかの方法を使用します。

- ASDM：**[Home]** > **[Device Dashboard]** > **[Device Information]** の順に選択します。
- CLI：**show version** コマンドを使用します。

次の表に、Firepower 2100 上のプラットフォームモードの ASA に対応するアップグレードパスを示します。バージョンによっては、新しいバージョンにアップグレードする前に、中間アップグレードが必要になります。推奨バージョンは**太字**で示されています。

開始バージョンと終了バージョンの間で、各リリースのアップグレードガイドラインを必ず確認してください。場合によっては、アップグレードする前に構成を変更する必要があります。そうしないと、停止が発生する可能性があります。

ASA のセキュリティの問題と、各問題に対する修正を含むリリースについては、ASA Security Advisories を参照してください。

表 *3:* アップグレードパス

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.19	—	次のいずれかになります。 → **9.20**
9.18	—	次のいずれかになります。 → **9.20** → **9.19**
9.17	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18**

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.16	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	次のいずれかになります。 → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15
9.13	→ 9.18	次のいずれかになります。 → **9.20** → **9.19**
9.13	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.12	→ 9.18	次のいずれかになります。 → **9.20** → **9.19**
9.12	—	次のいずれかになります。 → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	→ 9.17	次のいずれかになります。 → **9.20** → **9.19** → **9.18**
9.10	—	次のいずれかになります。 → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.9	→ 9.17	次のいずれかになります。 → **9.20** → **9.19** → **9.18**

現在のバージョン	暫定アップグレードバージョン	ターゲットバージョン
9.9	—	次のいずれかになります。 → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	→ 9.17	次のいずれかになります。 → **9.20** → **9.19** → **9.18**
9.8	—	次のいずれかになります。 → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

アップグレードパス：Firepower 4100/9300 用の ASA 論理デバイス

アップグレードについては、次のガイドラインを参照してください。

- FXOS：2.2.2 以降では、上位バージョンに直接アップグレードできます。2.2.2 より前のバージョンからアップグレードする場合は、各中間バージョンにアップグレードする必要があります。現在の論理デバイスバージョンをサポートしていないバージョンにFXOSをアップグレードすることはできないことに注意してください。次の手順でアップグレードを行う必要があります。現在の論理デバイスをサポートする最新のバージョンにFXOSをアップグレードします。次に、論理デバイスをそのFXOSバージョンでサポートされている最新のバージョンにアップグレードします。たとえば、FXOS 2.2/ASA 9.8 から FXOS 2.13/ASA 9.19 にアップグレードする場合は、次のアップグレードを実行する必要があります。

  1. FXOS 2.2→FXOS 2.11（9.8 をサポートする最新バージョン）
  2. ASA 9.8→ASA 9.17（2.11 でサポートされている最新バージョン）
  3. FXOS 2.11→FXOS 2.13

4. ASA 9.17→ASA 9.19

• ASA：ASA では、上記の FXOS 要件に注意して、現在のバージョンから任意の上位バージョンに直接アップグレードできます。

表 *4 : ASA* または *Threat Defense* 、および *Firepower 4100/9300* の互換性

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.14(1)	Firepower 4112	**9.20**（推奨） 9.19 9.18 9.17 9.16 9.15 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.20**（推奨） 9.19 9.18 9.17 9.16 9.15 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 6.7 6.6
2.13	Firepower 4112	**9.19**（推奨） 9.18 9.17 9.16 9.15 9.14	**7.3**（推奨） 7.2 7.1 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.19**（推奨） 9.18 9.17 9.16 9.15 9.14	**7.3**（推奨） 7.2 7.1 7.0 6.7 6.6

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.12	Firepower 4112	**9.18**（推奨） 9.17 9.16 9.15 9.14	**7.2**（推奨） 7.1 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18**（推奨） 9.17 9.16 9.15 9.14 9.12	**7.2**（推奨） 7.1 7.0 6.7 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18**（推奨） 9.17 9.16 9.15 9.14 9.12	**7.2**（推奨） 7.1 7.0 6.7 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.11	Firepower 4112	**9.17**（推奨） 9.16 9.15 9.14	**7.1**（推奨） 7.0 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17**（推奨） 9.16 9.15 9.14 9.12	**7.1**（推奨） 7.0 6.7 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17**（推奨） 9.16 9.15 9.14 9.12 9.8	**7.1**（推奨） 7.0 6.7 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.10 （注） 7.0.2+ および 9.16(3.11)+ との互換性を確保するには、FXOS 2.10(1.179)+ が必要です。	Firepower 4112	**9.16**（推奨） 9.15 9.14	**7.0**（推奨） 6.7 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16**（推奨） 9.15 9.14 9.12	**7.0**（推奨） 6.7 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16**（推奨） 9.15 9.14 9.12 9.8	**7.0**（推奨） 6.7 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.9	Firepower 4112	**9.15**（推奨） 9.14	**6.7**（推奨） 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.15**（推奨） 9.14 9.12	**6.7**（推奨） 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.15**（推奨） 9.14 9.12 9.8	**6.7**（推奨） 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.8	Firepower 4112	**9.14**	**6.6** （注） 6.6.1+ では FXOS 2.8(1.125)+ が必要です。
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14**（推奨） 9.12 （注） Firepower 9300 SM-56 には ASA 9.12(2)+ が必要	**6.6**（推奨） （注） 6.6.1+ では FXOS 2.8(1.125)+ が必要です。 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14**（推奨） 9.12 9.8	**6.6**（推奨） （注） 6.6.1+ では FXOS 2.8(1.125)+ が必要です。 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.157) （注） ASA 9.12+ および FTD 6.4+ では、同じ Firepower 9300 シャーシ内の別のモジュールで実行できるようになりました。	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** （注） Firepower 9300 SM-56 には ASA 9.12.2+ が必要	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12**（推奨） 9.8	**6.4**（推奨） 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS のバージョン	モデル	ASA のバージョン	Threat Defense バージョン
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	サポート対象外
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12**（推奨） 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 （注） FXOS 2.3(1.130)+ を実行している場合、フローオフロードには 9.8(2.12)+ が必要です。	**6.2.3**（推奨） （注） 6.2.3.16+ には FXOS 2.3.1.157+ が必要
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 （注） FXOS 2.3(1.130)+ を実行している場合、フローオフロードには 9.8(2.12)+ が必要です。	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Threat Defense バージョンはサポートが終了しています
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

ダウングレードについての注記

FXOS イメージのダウングレードは公式にはサポートされていません。シスコがサポートする唯一の FXOS のイメージバージョンのダウングレード方法は、デバイスの完全な再イメージ化を実行することです。

未解決のバグおよび解決されたバグ

このリリースで未解決のバグおよび解決済みのバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベースツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。シスコサポート契約がない場合は、ID でのみバグを探すことができます。検索は実行できません。

Cisco Bug Search Tool の詳細については、Bug Search Tool Help & FAQ [英語] を参照してください。

未解決のバグ

このセクションでは、各バージョンの未解決のバグを一覧表で示します。

バージョン 7.20(2) で未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

ID	見出し
CSCwh18177	ASDM のバックアップ復元時に、カスタムの policy-map がデフォルトのクラス インスペクション オプションに置き換えられる
CSCwh50291	MAC アドレスの自動生成を有効にするチェックボックスが正しく機能しない
CSCwi11925	ASDM を介して object-group を編集するときに、「any」キーワードをオブジェクトとして使用できない

バージョン 7.20(1) で未解決のバグ

このリリースに未解決のバグはありません。

解決済みのバグ

このセクションでは、リリースごとに解決済みのバグを一覧表で示します。

バージョン 7.20(2) で解決済みのバグ

このリリースでは解決済みのバグはありません。

バージョン 7.20(1) で解決済みのバグ

次の表に、このリリースノートの発行時点で解決済みのバグを示します。

ID	見出し
CSCwc48458	/api/monitoring/authusers の GET 結果に AnyConnect 認証ユーザーが表示されない
CSCwd23375	ASDM - SSL 証明書検証の脆弱性
CSCwe00348	ASDM からホストスキャンファイルを更新できない。ホストスキャンイメージをインストールすると、DAP を編集できない
CSCwe34665	ACL オブジェクトがすでに使用されている場合は編集できず、例外が発生する。
CSCwf11170	ポスト量子キー検証を適切に処理する必要があります。
CSCwf71723	ASDM で設定済みオブジェクト/オブジェクトグループが失われる

シスコの一般規約

シスコのソフトウェア使用時には、シスコの一般規約（その他の関連規約を含む）が適用されます。以下の住所宛てに物理コピーをリクエストできます。Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387。シスコから購入したシスコ以外のソフトウェアでは、該当するベンダーのライセンス条項に従う必要があります。関連項目：https://cisco.com/go/generalterms

関連資料

ASA の詳細については、『Navigating the Cisco Secure Firewall ASA Series Documentation』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。