Cisco Secure Firewall ASDM 7.22(x) リリースノート

最終更新：2026 年 8 月 16 日

Cisco Secure Firewall ASDM 7.22(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 7.22(x) のリリース情報が記載されています。

特記事項

- **Firepower 2100 では、ASA 9.22(1) 以降はサポートされていません**。ASA 9.20(x) が最後にサポートされるバージョンです。
- **9.22 における、スマートライセンスのデフォルト転送の変更**：9.22 において、スマートライセンスのデフォルト転送が Smart Call Home から Smart Transport に変更されました。必要な場合は、**transport type callhome** コマンドを使用して Smart Call Home を使用するように ASA を設定できます。9.22 にアップグレードすると、転送が自動的に Smart Transport に変更されます。ダウングレードすると、転送は Smart Call Home に戻ります。Smart Transport を使用する場合は、**transport type smart** を指定する必要があります。また、Smart Transport のライセンスの URL は（tools.cisco.com ではなく）https://smartreceiver.cisco.com であるため、アップストリームルータでその URL を許可するようにしてください。
- **組み込みスイッチがあるモデルの場合、9.22 以降ではサブインターフェイスで VLAN 1 を使用できません**。組み込みスイッチがあるモデルの場合、VLAN 1 を使用してサブインターフェイスを作成することはできません。VLAN 1 は、スイッチポートの論理的な VLAN インターフェイス用に予約されています。1010 から 9.22(1) 以降にアップグレードし、VLAN 1 をサブインターフェイスに割り当てている場合は、まずサブインターフェイスの VLAN ID を新しい VLAN に変更する必要があります。アップグレード後、VLAN 1 がサブインターフェイスから削除されます(存在する場合)。

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。

ASDM の Oracle バージョンが ASA パッケージに含まれています。OpenJRE バージョンを使用する場合は、それを ASA にコピーし、そのバージョンの ASDM を使用するように ASA を構成する必要があります。

（注） ASDM は Linux ではサポートされていません。

表 *1*：*ASDM* オペレーティングシステムとブラウザの要件

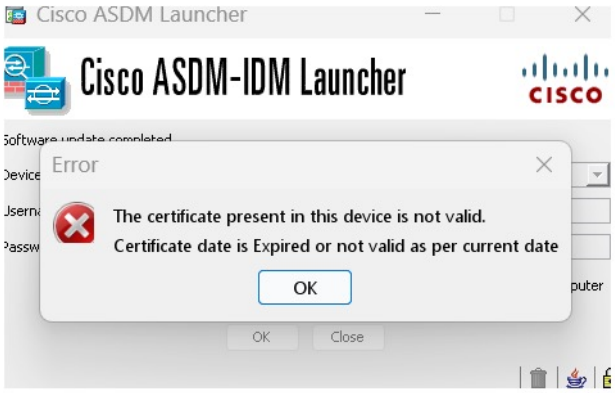
オペレーティング システム	ブラウザ			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows（英語および日本語）： • 11 • 10 （注） ASDM ショートカットに問題がある場合は、ASDM の互換性に関する注意事項 （2 ページ）の「Windows 10」を参照してください。 • 8 • 7 • Server 2016 と Server 2019 • Server 2012 R2 • Server 2012 • Server 2008	対応	サポートなし	対応	8.0 バージョン 8u261 以降	1.8 （注） Windows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

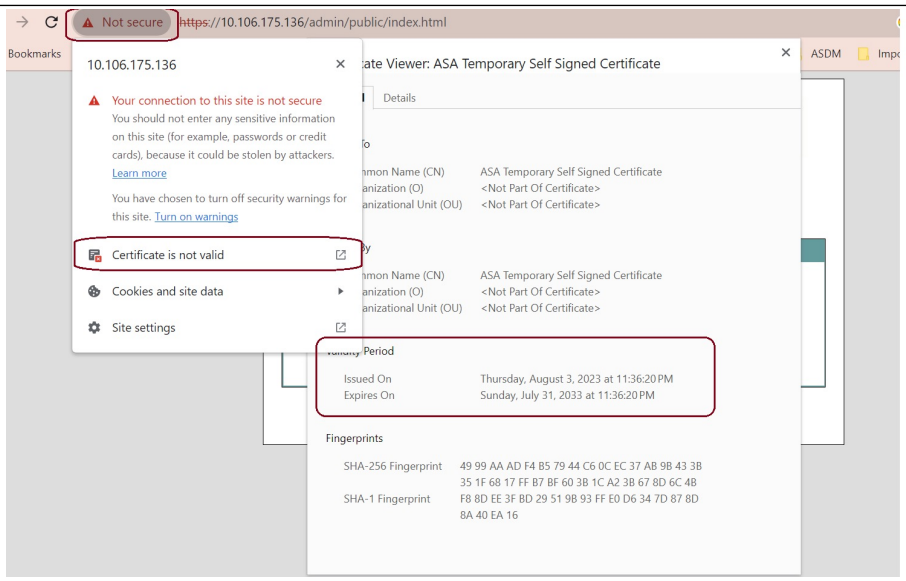
ASDM の互換性に関する注意事項

次の表に、ASDM の互換性に関する警告を示します。

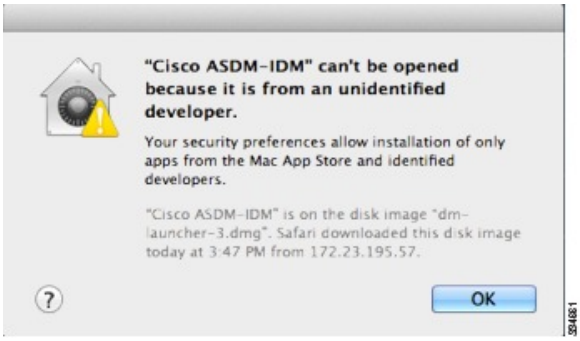
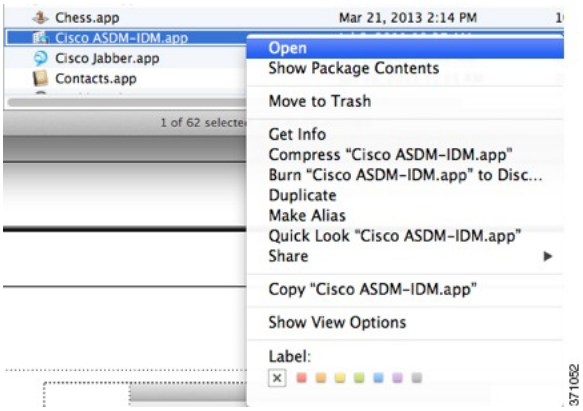
条件	注意
ASDM Launcher と ASDM バージョンの互換性	「デバイスマネージャを起動できません（Unable to Launch Device Manager）」というエラーメッセージが表示されます。 新しいASDMバージョンにアップグレードしてからこのエラーが発生した場合は、最新の Launcher を再インストールする必要があります。 **1.** ASA（https://<asa_ip_address>）で ASDM Web ページを開きます。 **2.** [ASDMランチャーのインストール（Install ASDM Launcher）] をクリックします。 **図 *1 : 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 5500 および ISA 3000）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 PAK ライセンスを要求できます。 1. https://www.cisco.com/jp/go/license にアクセスします。 2. [従来のライセンス（Traditional Licenses）] で、[LRPにアクセス（Access LRP）] をクリックします。 3. [ライセンスを取得（Get Licenses）] をクリックし、ドロップダウンリストから [IPS、Crypto、その他...（IPS, Crypto, Other...）] を選択します。 4. [Search by Keyword] フィールドに「ASA」と入力します。 5. [Product] リストで [Cisco ASA 3DES/AES License] を選択し、[Next] をクリックします。 6. 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。

さらに、可能であれば、未使用のオブジェクトを削除するなどして、構成サイズを減らすことをお勧めします。

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。

非常に大規模な構成では、最大 2 GB のヒープサイズを指定する必要がある場合があります。

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。

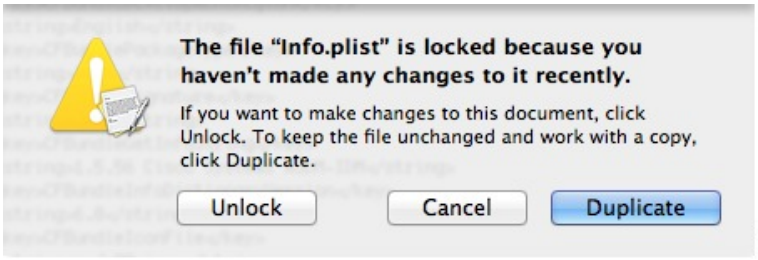
```
<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

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


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

非常に大規模な構成では、最大 2 GB のヒープサイズを指定する必要がある場合があります。

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。

Cisco ASA 9.22(3)/ASDM 7.22(3) の新機能

リリース：**2026 年 3 月 26 日**

（注） ASDM 7.22(2) リリースはありませんでした。

機能	説明
ハイ アベイラビリティとスケーラビリティの各機能	
ASAc 高可用性および SR-IOV 機能の有効化	これにより、Docker および Kubernetes 環境での Cisco ASA コンテナ（ASAc）展開の高可用性（HA）サポートが有効になります。2 つの ASAc コンテナインスタンスを個別の Docker ホストに展開し、プライマリとセカンダリのフェールオーバーのペアとして設定できます。 SR-IOV 機能は、Docker および Kubernetes 環境内の ASAc コンテナ展開で単一ルート I/O 仮想化（SR-IOV）インターフェイスをサポートします。
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	
SSH X.509 証明書認証	X.509v3 証明書を使用して SSH のユーザーを認証できるようになりました（RFC 6187）。 Firepower 4100/9300 の場合、FXOS バージョン 2.16（2.109 以降）または 2.18 以降が必要です。 新しい/変更された画面： • **[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] > [AAAアクセス（AAA Access）] > [承認（Authorization）]** • **[設定（Configuration）] > [デバイス管理（Device Management）] > [証明書管理（Certificate Management）] > [CA証明書（CA Certificates）] > [トラストポイントの追加/編集（Add/Edit Trustpoint）] > [詳細設定（Advanced）]** • **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** *9.20(4)*、*9.24(1)* でも同様です。

機能	説明
AES-256-GCM SSH 暗号	ASA は、SSH の AES-256-GCM 暗号をサポートしています。デフォルトでは、暗号化レベル [すべて（all）] と [高（high）] で有効になっています。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [詳細設定（Advanced）] > [SSH暗号（SSH Ciphers）]** *9.20(4)*、*9.24(1)* でも同様です。
Message-of-the-Day（motd）バナーに、フェールオーバー状態と最後のフェールオーバー時刻が表示されます	フェールオーバーを使用する場合、message-of-the-day (motd) バナーを設定すると、ログインしているユニットのフェールオーバー状態と最後のフェールオーバー時刻に関する情報がバナーに表示されます。この情報は、CLI で障害対応などのアクションを実行しており、CLI セッション間でフェールオーバーが発生する場合に役立ちます。 新規または変更された画面： **[Configuration] > [Device Management] > [Management Access] > [Command Line (CLI)] > [Banner]** の順に選択します。 *9.24(1)* でも同様です。
TLS デバイス証明書用の Automated Certificate Management Environment（ACME）プロトコル	Cisco ASA トラストポイントに Automated Certificate Management Environment（ACME）プロトコルを設定して、TLS デバイス証明書を管理できます。ACME は、自動更新、ドメイン検証、および証明書の簡単な登録と失効を通じて、簡素化された証明書管理を可能にします。認証に Let's Encrypt CA サーバーを使用するか、他の ACME サーバーを使用するかを選択できます。ACME は認証に http01 方式を使用します。 新規または変更された画面： [アイデンティティ証明書の追加（Add Identity Certificate）] > [新しいアイデンティティ証明書の追加（Add a new Identity Certificate）] > [詳細（Advanced）] > [CAからの要求（Request from a CA）] *9.23(1)* でも同様です。
接続ステータス出力における UDP のイニシエータおよびレスポンダ値の表示	UDP 通信フローの場合、Cisco ASA は接続の詳細ステータスにイニシエータおよびレスポンダフィールド値を表示します。これらのフィールド値は通信の方向を示すため、ネットワーク接続に関する問題のトラブルシュートに役立ちます。 *9.20(4)*、*9.24(1)* でも同様です。
フェールオーバーおよびスタンドアロンユニットでのブロック枯渇の監視	ブロックの枯渇が発生すると、ASA は障害対応ログを収集し、syslog を送信します。フェールオーバーの場合、Cisco ASA はスタンバイユニットにフェールオーバーします。ASA は、クラッシュおよびリロードを強制して枯渇から回復することもできます。 また、*9.23(1)* にも記載されています。

Cisco ASA 9.22(2) の新機能

リリース日：**2025** 年 **4** 月 **10** 日

このリリースに新機能はありません。

Cisco ASA 9.22(1.1)/ASDM 7.22(1) の新機能

リリース：**2024** 年 **9** 月 **16** 日

（注） 9.22(1) はリリースされませんでした。

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 1210/1220	Cisco Secure Firewall 1210/1220 は、組み込みスイッチを備えたコンパクトなデスクトップ ファイアウォールです。モデルによっては Power over Ethernet+（PoE+）が利用できます。 • Cisco Secure Firewall 1210CE：8 つの 1Gbps RJ-45 銅線データポートを搭載しています。 • Cisco Secure Firewall 1210CP：これらのポートの 4 つに PoE+ を搭載しています。 • Cisco Secure Firewall 1220CX：2 つの 10Gbps SFP+ 追加ポートを搭載しており、パフォーマンスが向上します。

機能	説明
Cisco ASA Virtual による、GWLB を使用した AWS 環境でのデュアルアーム デプロイメント モードのサポート	Cisco ASA Virtual は、GWLB を使用した AWS 環境でのデュアルアーム デプロイメント モードをサポートするようになりました。このモードにより、Cisco ASA Virtual は通信のインスペクション後、インターネットに向かうトラフィックをインターネットゲートウェイ経由でインターネットに直接転送できると同時に、ネットワークアドレス変換（NAT）も実行できます。 デュアルアームモードはシングルアームモードとは異なり、検査されたアウトバウンド通信をまずGWLBに、次にインターネットゲートウェイを介してインターネットにルーティングするのに役立ちます。 デュアルアームモードは、単一 VPC ネットワーク環境と複数 VPC ネットワーク環境の両方で、検査済み通信の Cisco ASA Virtual からインターネットへの転送をサポートします。 Cisco ASA Virtual のデュアルアームモードの利点は次のとおりです。 • 通信のホップを最小限に抑えることで通信の遅延を減らし、スループットパフォーマンスを向上させます。 • インターネットに転送する前に、複数のVPCからのアウトバウンド通信を統合して検査します。 • インフラストラクチャの要件が軽減されるため、費用対効果の高いソリューションが得られます。 詳細については、『Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.22』を参照してください。
Kubernetes または Docker 環境での Cisco Secure Firewall ASA コンテナ（ASAc）の展開	コンテナは、コンピューティング環境でアプリケーションが正常に実行されるようにするためのコードと関連する要件（システムライブラリ、システムツール、デフォルト設定など）をバンドルしたソフトウェアパッケージです。オープンソースの Kubernetes または Docker 環境に Cisco ASA コンテナ（ASAc）を展開できます。
VMware ESXi 上の Cisco ASA Virtual のサポート	VMware 上の Cisco ASA Virtual は、ESXi バージョン 8.0 をサポートするようになりました。 詳細については、『Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.22』を参照してください。
ファイアウォール機能	
オブジェクトグループ検索の最適化。	オブジェクトグループ検索機能が拡張され、アクセスコントロールルールを評価して接続を照合する際のオブジェクトルックアップ時間が短縮され、CPU オーバーヘッドが削減されました。オブジェクトグループ検索の設定に変更はありません。最適化された動作は自動的に行われます。 デバイス CLI に次のコマンドが追加されました。または、コマンド出力が拡張されました。 **clear asp table network-object**、 **debug ac logs**、 **packet-tracer**、 **show access-list**、 **show asp table network-group**、 **show object-group**。

機能	説明
ハイ アベイラビリティとスケーラビリティの各機能	
Cisco Secure Firewall 3100 および 4200 の最大クラスターノード数が 16 に増加しました。	Cisco Secure Firewall 3100 および 4200 では、最大ノード数が 8 から 16 に増加しました。
Cisco Secure Firewall 3100 および 4200 クラスターの個別インターフェイスモード	個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル *IP* アドレスを持ちます。各インターフェイスのメインクラスタ *IP* アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。 アップストリームスイッチ上でロードバランシングを別途する必要があります。 新規/変更されたコマンド： **cluster interface-mode individual** 新規/変更された画面：[**ウィザード（Wizards）> > 高可用性（HA）および拡張性ウィザード（High Availability and Scalability Wizard）**]
AWS マルチアベイラビリティゾーンでの Cisco ASA Virtual クラスタリング デプロイメントのサポート	AWS リージョン内の複数のアベイラビリティゾーンにまたがる形で Cisco ASA 仮想クラスターを展開および構成できるようになりました。このクラスターには、需要に基づいた仮想デバイスのスケールアップまたはスケールダウンに役立つダイナミックスケーリング機能（Autoscale）も備わっています。 AWS リージョンの複数のアベイラビリティゾーンにまたがる形で Cisco ASA 仮想クラスターを拡張することにより、ディザスタリカバリ中の継続的な通信インスペクションとダイナミックスケーリングが可能になります。 詳細については、『パブリッククラウドにおける Cisco ASA Virtual クラスターの展開』を参照してください。
ノード参加時の MTU ping テスト	クラスターに参加したノードは、クラスター制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。以前は、制御ノードのみが ping を送信していました。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。 追加/変更された画面：[**Monitoring** > **ASA Cluster** > **Cluster Summary**]
インターフェイス機能	
組み込みスイッチを搭載したモデルの場合、サブインターフェイスで VLAN 1 は使用不可	組み込みスイッチを搭載したモデルの場合、VLAN 1 を使用してサブインターフェイスを作成することはできません。VLAN 1 は、スイッチポートの論理的な VLAN インターフェイス用に予約されています。 1010 から 9.22(1) 以降にアップグレードし、VLAN 1 をサブインターフェイスに割り当てている場合は、まずサブインターフェイスの VLAN ID を新しい VLAN に変更する必要があります。アップグレード後、VLAN 1 がサブインターフェイスから削除されます。

機能	説明
ライセンス機能	
Smart Transport はスマートライセンスのデフォルトの転送です	スマートライセンスでは現在、デフォルトの転送として Smart Transport を使用しています。必要に応じて、旧タイプの Smart Call Home を任意で有効にできます。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [スマートライセンス（Smart Licensing）]**。
32 コアと 64 コアで Cisco ASA Virtual を展開するための ASAvU（無制限）ライセンス	ASAvU ライセンスでは、32 コアと 64 コアのデプロイメントで最大のスループットを実現します。このライセンスは VMware と KVM でのみサポートされます。 新規/変更された画面：**[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [スマートライセンス（Smart Licensing）]**。
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	
USB ポート（disk1）の無効化	デフォルトではタイプ A の USB ポート（disk1）が有効になっており、無効化することはできませんでした。次のモデルで、セキュリティ上の目的で USB ポートアクセスを無効化できるようになりました。 • Firepower 1000 • Cisco Secure Firewall 3100 • Cisco Secure Firewall 4200 この設定はファームウェアに保存され、リロードが必要です。さらに、USB ポートが無効化されていて、この機能をサポートしていないバージョンにダウングレードすると、ポートは無効化されたままになります。NVRAM を消去せずに再度有効にすることはできません。 （注） この機能は、タイプ B USB コンソールポート（存在する場合）には影響しません。 新規/変更された画面： • [**構成（Configuration）** > **デバイス管理（Device Management）** > **詳細（Advanced）** > **USBポートの有効化/無効化（Enable/Disable USB Port）**] • [**モニタリング（Monitoring）** > **プロパティ（Properties）** > **USB ポート（USB Port）** > **USB ポート情報（USB Port Info）**]
フェールオーバーおよびスタンドアロンユニットでのブロック枯渇の監視	ブロックの枯渇が発生すると、ASA は障害対応ログを収集し、syslog を送信します。フェールオーバーの場合、Cisco ASA はスタンバイユニットにフェールオーバーします。ASA は、クラッシュおよびリロードを強制して枯渇から回復することもできます。
VPN 機能	

機能	説明
DTLS暗号化アクセラレーション	Cisco Secure Firewall 4200 および 3100 シリーズは、DTLS 暗号化アクセラレーションをサポートします。ハードウェアは DTLS 暗号化と復号化を実行し、DTLS 暗号化トラフィックと DTLS 復号化トラフィックのスループットを向上させます。ハードウェアは、遅延を改善するために、出力暗号化パケットの最適化も実行します。 新規/変更された画面：[設定（Configuration）] > [ファイアウォール（Firewall）] > [詳細（Advanced）] > [DTLSオフロード（DTLS Offload）] > [DTLSオフロード（DTLS Offload）] および [DTLSオフロードの出力最適化（Egress Optimization for DTLS Offload）] チェックボックス。

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

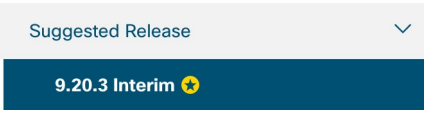
アップグレードを完了するには、『ASA アップグレード ガイド』を参照してください。

アップグレードパス：ASA アプライアンス

アップグレードするバージョン

シスコサポート & ダウンロードサイトでは、推奨リリースに金色の星が付いています。次に例を示します。

図 *4:* 推奨リリース



現在のバージョンの表示

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。

アップグレードのガイドライン

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。

アップグレードパス

次の表に、ASA のアップグレードパスを示します。

（注） ASA 9.20 は Firepower 2100 の最終バージョンです。

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
9.20	—	次のいずれかになります。 → 9.22
9.19	—	次のいずれかになります。 → 9.22 → 9.20
9.18	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19

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
9.17	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18
9.16	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17
9.15	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.14	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

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。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.12	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.10	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.9	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

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
9.8	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.7	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.6	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.5	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

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。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.3	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.2	—	次のいずれかになります。 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

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

- FXOS：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。（FXOS 2.0.1 ～ 2.2.1 は 2.8.1 までアップグレードできます。2.0.1 より前のバージョンについては、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

- Firewall Threat Defense：上記の FXOS 要件に加えて、Firewall Threat Defense に対して中間アップグレードが必要になる場合があります。正確なアップグレードパスについては、ご使用のバージョンの アップグレードガイド を参照してください。
- Cisco ASA：Cisco 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 *3 : Firepower 4100/9300* と *ASA* および *Firewall Threat Defense* の互換性

FXOS のバージョン	モデル	ASA のバージョン	Firewall Threat Defense バージョン
2.16	Firepower 4112	**9.22**（推奨） 9.20 9.19 9.18 9.17	**7.6**（推奨） 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	**9.22**（推奨） 9.20 9.19 9.18 9.17	**7.6**（推奨） 7.4 7.3 7.2 7.1
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS のバージョン	モデル	ASA のバージョン	Firewall Threat Defense バージョン
2.14(1)	Firepower 4112	**9.20**（推奨） 9.19 9.18 9.17 9.16 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 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 9.14	**7.4**（推奨） 7.3 7.2 7.1 7.0 6.6
2.13	Firepower 4112	**9.19**（推奨） 9.18 9.17 9.16 9.14	**7.3**（推奨） 7.2 7.1 7.0 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 9.14	**7.3**（推奨） 7.2 7.1 7.0 6.6

FXOS のバージョン	モデル	ASA のバージョン	Firewall Threat Defense バージョン
2.12	Firepower 4112	**9.18**（推奨） 9.17 9.16 9.14	**7.2**（推奨） 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18**（推奨） 9.17 9.16 9.14 9.12	**7.2**（推奨） 7.1 7.0 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 9.14 9.12	**7.2**（推奨） 7.1 7.0 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	Firewall Threat Defense バージョン
2.11	Firepower 4112	**9.17**（推奨） 9.16 9.14	**7.1**（推奨） 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17**（推奨） 9.16 9.14 9.12	**7.1**（推奨） 7.0 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 9.14 9.12 9.8	**7.1**（推奨） 7.0 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	Firewall 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） 9.14	**7.0**（推奨） 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16**（推奨） 9.14 9.12	**7.0**（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	**9.16**（推奨） 9.14 9.12 9.8	**7.0**（推奨） 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	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	Firewall 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	Firewall 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**	Firewall 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 7.22(3) 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。

バージョン 7.22(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 7.22(3) 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 7.22(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
CSCwa87515	コンテキストの切り替え中に ASDM セッションが切断される
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
CSCwj14147	L2 および L3 ACL が混在していると、ASDM がアクセスグループ設定をロードできない
CSCwj14498	ASDM GUI で送信元および宛先ファイル拡張子エラーが表示される
CSCwj17213	アプリケーション クライアント タイプ属性の変更
CSCwj28481	「前方参照」行があると、ASDM で新しいルールが間違った順序で適用される
CSCwj66085	ASA が ASDM を介して NAT ルールを .csv 形式でエクスポートできない
CSCwk64399	ASDM：Secure Client プロファイルを編集できない

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。