Cisco Start Firewall

Cisco ASA 5506-X および FirePOWER クイックスタートガイド

2016 年 3 月 23 日
第 1.1 版

株式会社ネットワールド
Networld

改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016 年 3 月 11 日	ネットワールド	● 新規
1.1	2016 年 3 月 23 日	ネットワールド	誤記修正

免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワールド(以下 弊社)が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではございません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃止する場合がございます。なお、弊社が本書を更新することをお約束するものではございません。

表記規則

表記	表記の意味
「」(括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold(ボールド文字)	入力または選択する値
italic(イタリック文字)	入力または選択する値(変数)
□(囲み線)	入力または選択するオブジェクト
“”(二重引用符記号)	表示された値
(蛍光マーカー)	表示された値(強調)

表記の例)

① 「Exec」ラジオボタンを選択します。

② テキストボックスに以下のコマンドを入力します。

```
copy running-config <file name>
```

③ 「コマンドを実行」ボタンをクリックします。正常に実行されれば、画面に”[OK]”が表示されます。

目次

1. はじめに

本書は Cisco ASA 5506-X および FirePOWER 機能を使用するにあたって、機器の基本情報および初期設定について記載しています。

1.1 対象機器

本書で対象としている機器は以下になります。

表 1 本書の対象機器

ASA 5506-X (ASA5506-K9)	ASA 5506W-X (ASA5506W-Q-K9)
☑	☑

2. 機器について

2.1 パッケージの内容

この節では、製品に同梱されている内容物について説明します。ライセンスを購入、またはバンドル製品を購入した場合は関連書類が追加されますが、ここでは説明は省略します。また、この内容は変更される場合があるため、ご注意下さい。

図 1　ASA 5506-X または ASA 5506W-X の同梱物

表 1　図 1 の各同梱物について

①	ASA 5506-X または ASA 5506W-X シャーシ	②	青いコンソールケーブルおよびシリアル PC ターミナルアダプタ(DB-9 to RJ-45)
③	電源ケーブル	④	電源モジュール

2.1.1　機器の外観

図 2　ASA 5506-X または ASA 5506W-X の前面

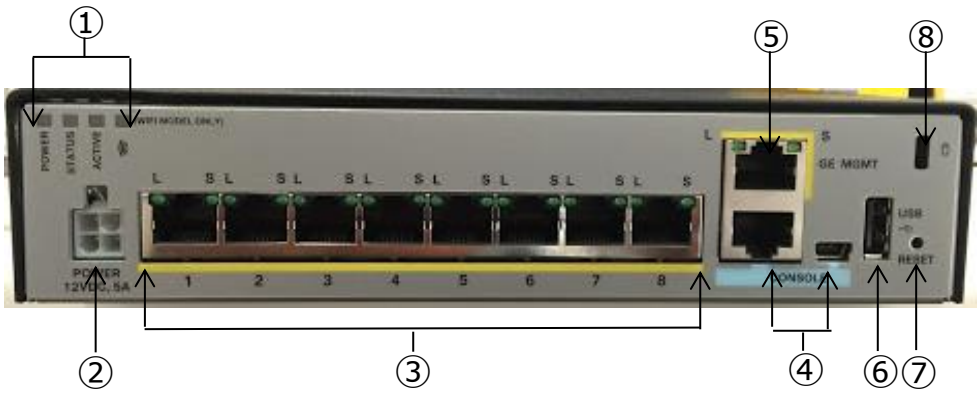

図 3　ASA 5506-X または ASA 5506W-X の背面

表 2 各 LED、ポート類等について

①	ステータス LED	各 LED で機器の状態を以下のように示します。 ・Power　消灯：電源オフ 緑に点灯：電源オン ・Status　緑：システムは正常に機能 オレンジ：次の 1 つまたは複数のクリティカルな状態を示すアラーム→ハードウェアまたはソフトウェア コンポーネントの重大な障害、過熱状態、許容範囲外の電圧 ・Active　緑に点灯：フェールオーバーペアが正常に動作中です。ASA が HA ペアでなければ、LED は常に緑です ・WLAN(ASA 5506W-X でのみ使用されます) 緑のチャーピング：正常に動作していますが、ワイヤレス クライアントはありません。 緑：正常に動作しており、少なくとも 1 つのワイヤレス クライアントが関連付けられています。 オレンジの点滅：ソフトウェア アップグレードが進行中です。 緑、赤、オレンジの順で点灯：Discovery/Join プロセスが進行中です。 赤の点滅：イーサネット リンクが使用できません。 消灯：ワイヤレスを使用できません。
②	電源コードソケット	電源ケーブルを接続する電源ソケットです。 (注) ASA は AC 電源に接続すると電源が投入されます。
③	ネットワークデータインタフェース	8個のギガビットイーサネットRJ-45インターフェイスです。ポートには(左から右に)1、2、3、4、5、6、7、8の番号が記載されており、設定上はGigabit Ethernet1/1

		からGigabit Ethernet1/8までの名前と番号が付けられています。
④	管理インタフェース	ネットワーク管理アクセス用のギガビットイーサネットインターフェイスです。 RJ-45 ケーブルで接続します。ASA の CLI では Management1/1、FirePOWER モジュールでは eth0 と名前と番号が付けられています。
⑤	コンソールポート	2 個のシリアルポート(ミニ USB タイプ B および標準 RJ-45)が、PC などからの管理アクセス用に提供されます。
⑥	USB ポート	標準 USB タイプ A ポートです。大容量ストレージなどの外部デバイスの接続が可能です。
⑦	リセットボタン	小さな埋め込み型のボタンです。約 3 秒以上押すと ASA がリセットされ、次のリブート後に「出荷時」のデフォルト状態に戻ります。設定変数が工場出荷時デフォルトにリセットされます。ただし、フラッシュは削除されないため、ファイルは削除されません。 (注) **service sw-reset-button** を使用して、リセットボタンを無効化できます。 デフォルトでは有効になっています。 (注) ASA 5506W-X のリセットボタンを押しても AP 設定には影響しませんが、システムが再起動されるため、保存されていない AP 設定は失われます。システムのリブート後、デフォルト AP の設定が必要な場合は **hw-module module wlan recover configuration** コマンドを使用して、AP 設定を回復してください。
⑧	ロックスロット	Kensington 標準 T バーのロックメカニズムに対応し、ASA のセキュリティを保護します

2.1.2 ASA 5506-X のデスクトップマウント

ASA 5506-X をデスク上に水平に置くことにより、デスクトップにマウントできます。ASA の上方 2.5cm (1 インチ)以内や、両側および背面の 1.3 cm(0.5 インチ)以内に、冷却の妨げになる遮蔽物や障害物がないようにしてください。 ASA に付属のゴム製の脚を取り外さないでください。それらも適切な冷却のために必要です。

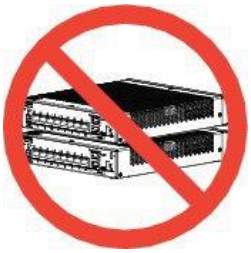

図 4 注意：ASA シャーシの上に別の ASA シャーシを積み重ねないでください。 過熱状態となり、電源が再投入される場合があります。

3. ASA 5506-X および FirePOWER の初期設定

本章では ASA 5506-X および FirePOWER の初期設定手順について説明します。

3.1 システム構成

本書での初期設定手順は以下のシステム構成に基づいて行われます。ASA 5506-X の GE1/1 は outside、GE1/2 は inside としてデフォルトで設定されており、そのまま使用します。

インターネット側に接続する GE1/1 は DHCP(デフォルトで有効)により IP アドレスとデフォルトルートの設定を取得します。

ASAの管理用にGE1/2を、FirePOWERの管理用にはManagement1/1(eth0)を使用します。

ASA 5506-X はデフォルトで any→outside の NAT 設定がされており、今回はインターネット側への通信にそのまま使用します。

図５　システム構成図

表３　本書で使用した機材およびそれらのシステム環境

機器	機器名	OS およびアプリケーション	ネットワーク設定
Firewall	ASA 5506W-X	OS Version 9.5(2) ASDM Version 7.5(2)153※ FirePOWER (Sourcefire3D) Version 5.4.1 (Build 211)	GE1/1 outside (デフォルト) IP アドレス:DHCP (デフォルト) GE1/2 inside (デフォルト) IP アドレス:172.16.1.254/24 Management1/1(eth0) IP アドレス:172.16.1.253/24 NAT any→outside への PAT (デフォルト) ルーティング DHCP によりインターネット側へのデフォルトルートを取得
L2 スイッチ	SG110D-08		
管理用 PC		OS : Windows 7 ターミナルアプリケーション (Tera Term) Web ブラウザ(Internet Explorer11)	インタフェース IP アドレス:172.16.1.1/24

※ASDM は Version 7.5(2)以降を使用して下さい

3.2 ASA 5506-X および FirePOWER の初期設定

3.2.1 コンソールからの ASA 5506-X の初期設定

管理 PC から ASA にアクセスするための初期設定をコンソール(CLI)から行います。

1) 管理用 PC から ASA のコンソールにアクセスし、以下の手順で ASA の初期設定を行います。

```
ciscoasa> enable      ①特権モードに移動します
Password:             ②何も入力せずエンターキーを押します
ciscoasa#
ciscoasa# configure terminal  ③グローバルコンフィグレーションモードに移動します
ciscoasa(config)#

****************************** NOTICE ******************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: n      ④任意でエラーレポートの送信を選択します(ここでは n を選択します)

In the future, if you would like to enable this feature,
issue the command "call-home reporting anonymous".

Please remember to save your configuration.

ciscoasa(config)#
ciscoasa(config)# interface gigabitEthernet 1/2          ⑤インタフェース GE1/2 のコンフィグレーションに移
ciscoasa(config-if)# ip address 172.16.1.254 255.255.255.0  動し、IP アドレスを設定します
Interface address is not on same subnet as DHCP pool
WARNING: DHCPD bindings cleared on interface 'inside', address pool removed
ciscoasa(config-if)# exit
ciscoasa(config)# http 172.16.1.0 255.255.255.0 inside   ⑥inside からの http(ASDM)アクセスを許可します
ciscoasa(config)# policy-map global_policy        ⑦グローバルポリシーマップを指定します
ciscoasa(config-pmap)# class inspection_default   ⑧インスペクションのクラスを指定します
ciscoasa(config-pmap-c)# inspect icmp             ⑨icmp をインスペクションの対象に指定します(Ping などによる通信を行うため
ciscoasa(config-pmap-c)# exit                      の設定です。セキュリティ上無効にすべき場合には設定しないで下さい)
ciscoasa(config-pmap)# class class-default        ⑩デフォルトのクラスを作成します
ciscoasa(config-pmap-c)# sfr fail-open            ⑪全トラフィックを FirePower モジュールに転送します(fail-open は FirePOWE
ciscoasa(config-pmap-c)# end                       R 障害時にパケットを通過させます。通過させない場合は、fail-close コマンドを
ciscoasa#                                          設定します)
ciscoasa# write memory   ⑫設定を保存します
Building configuration...
Cryptochecksum: 71c4ec3e fbc391a9 f704ac94 eed7f814

 7334 bytes copied in 0.160 secs
[OK]
```

3.2.2 管理用 PC への ASDM のインストール

ASDM は ASA を管理するアプリケーションです。本項では ASDM を管理 PC へインストールする手順を説明します。

1) 管理用 PC で Web ブラウザを起動し、https://172.16.1.254 にアクセスします。セキュリティ証明書の警告メッセージが表示されますが閲覧を続行して下さい。

2) 以下の画面にて「Install ASDM Launcher」をクリックします。

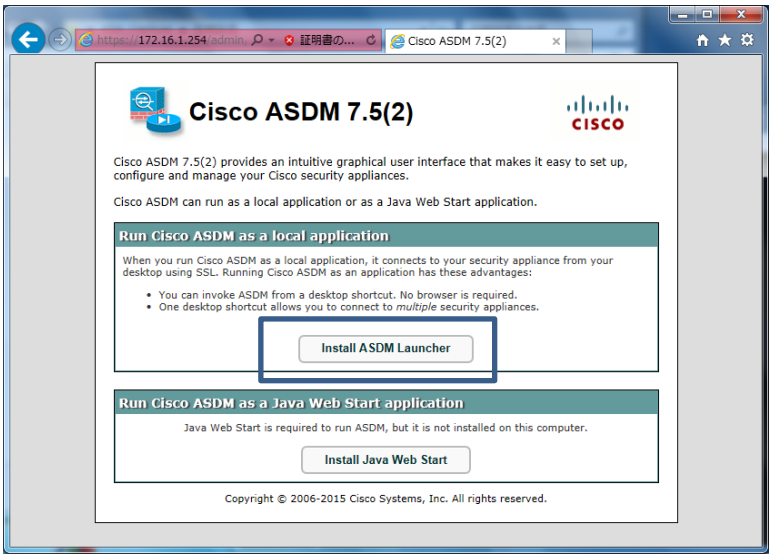

図 6　Web ブラウザからの ASDM のインストール開始

3) ユーザ名およびパスワード名を要求されますが、入力せず"OK"をクリックします。

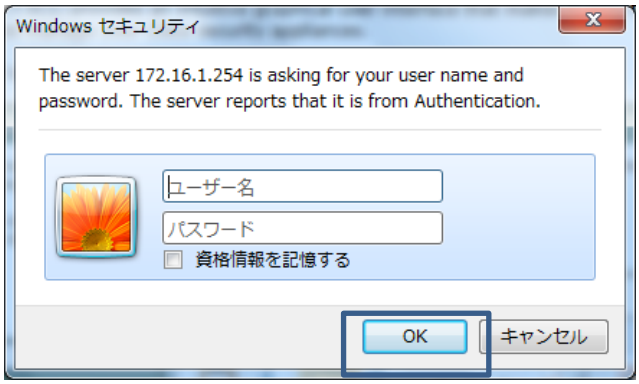

図 7　ユーザ名、パスワードの要求

4) 「dm-launcher.msi」の実行または保存を聞かれますので、「実行」をクリックします。発行元に関する警告メッセージが表示されますが、そのまま実行して下さい。

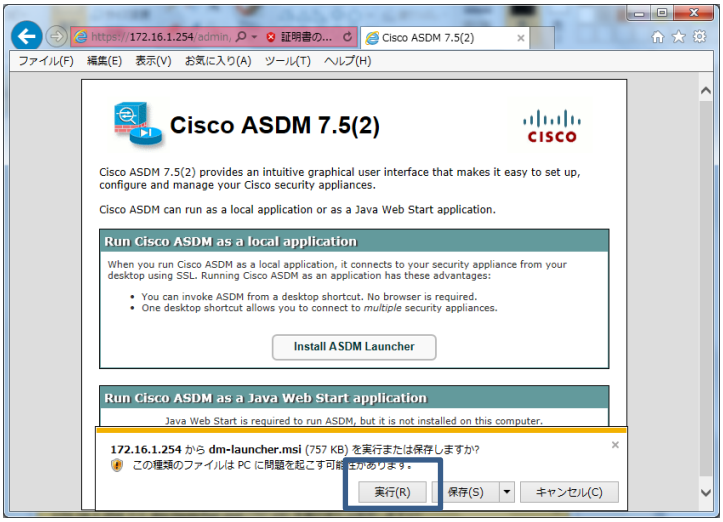

図 8　ASDM インストーラーの実行

5) ASDM のインストーラーが起動しましたら、「Next」をクリックします。

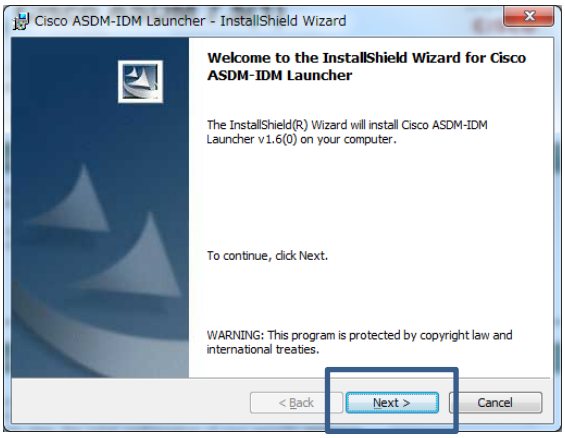

図 9　ASDM インストーラーの起動

6) ASDM のインストールフォルダを聞かれますので、そのまま「Next」をクリックします。

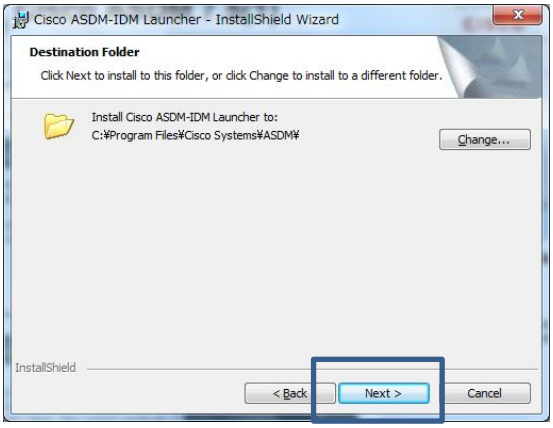

図 10　ASDM インストール先フォルダの選択

7) インストールを実行するか聞かれますので、「Install」を実行します。

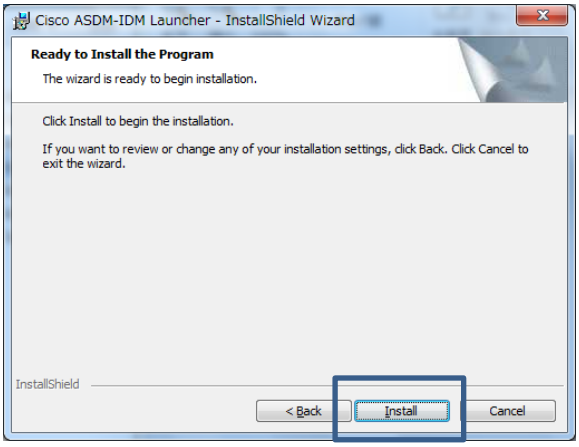

図 11 ASDM インストールの実行

8) ASDM のインストールが実行されます。

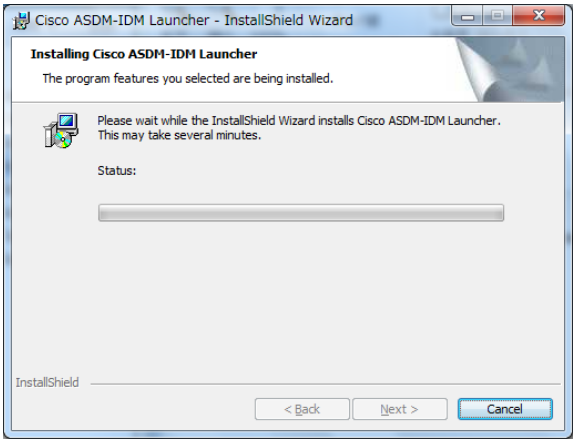

図 12 ASDM インストールの進行

9) 「Finish」をクリックしてインストールを完了します。

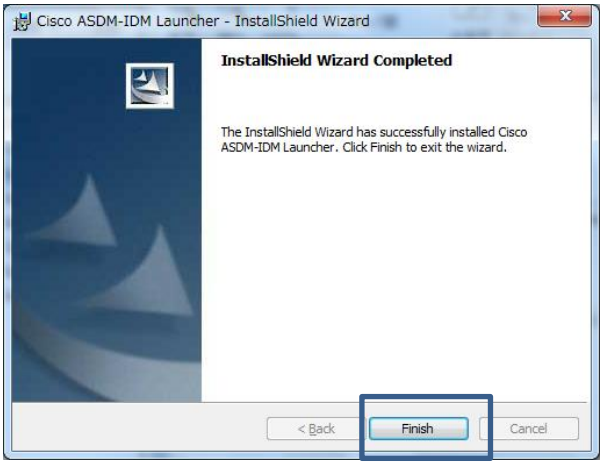

図 13 ASDM インストールの完了

3.2.3 ASDM から ASA 5506-X へのアクセス

本項では ASDM を使用して ASA 5506-X へアクセスする手順を説明します。

1) “Cisco ASDM-IDM Launcher”を起動し、”Device IP Address / Name”の欄に ASA の GE1/2 の IP アドレス(ここでは 172.16.1.254)を入力し、”Username”および”Password”は空欄のまま、“OK”をクリックします。セキュリティ警告が表示されますが続行します。

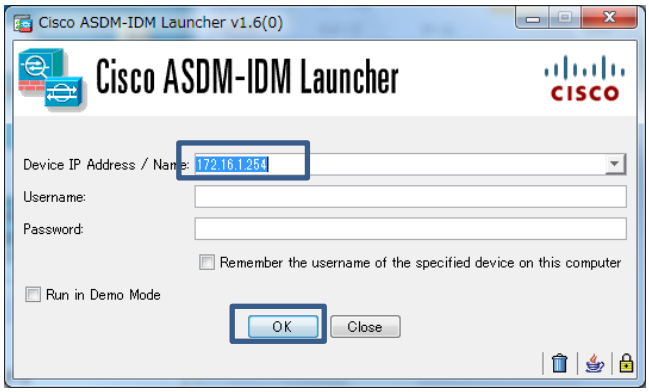

図 14 ASDM による ASA へのアクセス

2) FirePOWER モジュールにアクセスできないというメッセージも表示されますが、この時点では必要な初期設定が行われていなため、キャンセルをクリックして先に進めます。

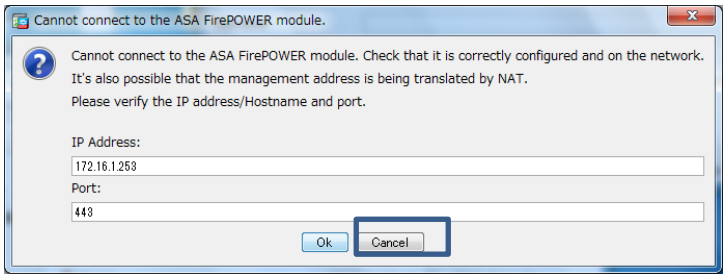

図 15 FirePOWER モジュールアクセス不可

3) ASA にアクセスできると、ASDM が起動します。

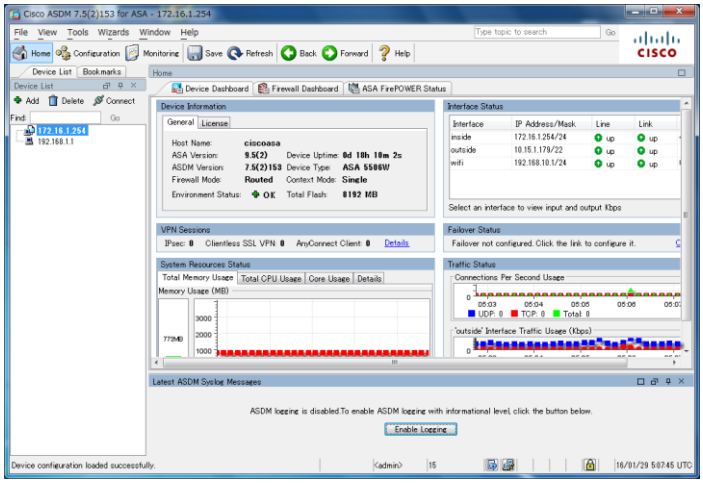

図 16 ASDM の起動

3.2.4 ASDM からの ASA 5506-X および FirePOWER の初期設定

本項では ASDM を使用して ASA 5506-X および FirePOWER の初期設定を行う手順を説明します。

1) ASDM による設定変更時に ASA に実行されるコマンドを変更前に確認できるようにするため、「Tools」>「Preference」>を開き、「Preview command before sending～」にチェックを入れ、「OK」をクリックします。

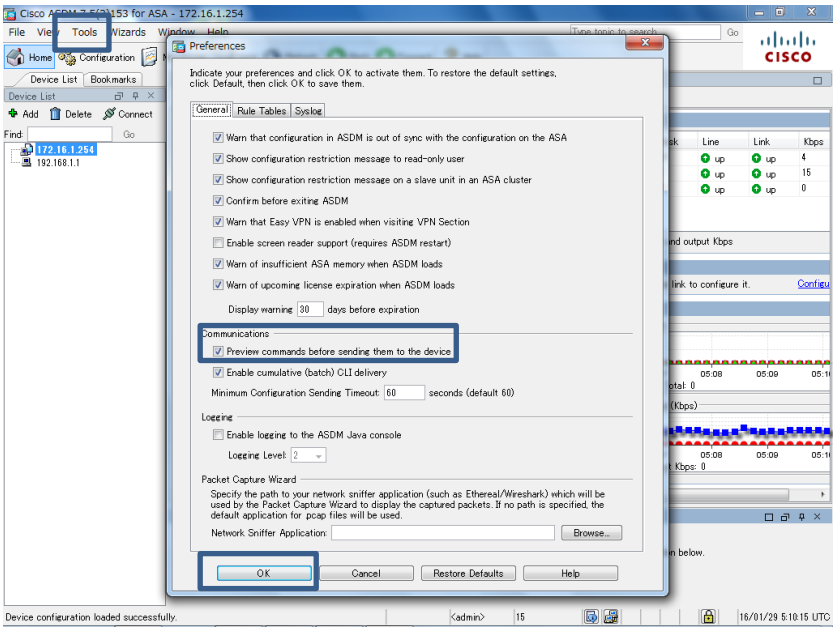

図 17 設定変更前のコマンド表示設定

2) 初期設定を開始します。「Wizards」>「Startup Wizard」を開きます。

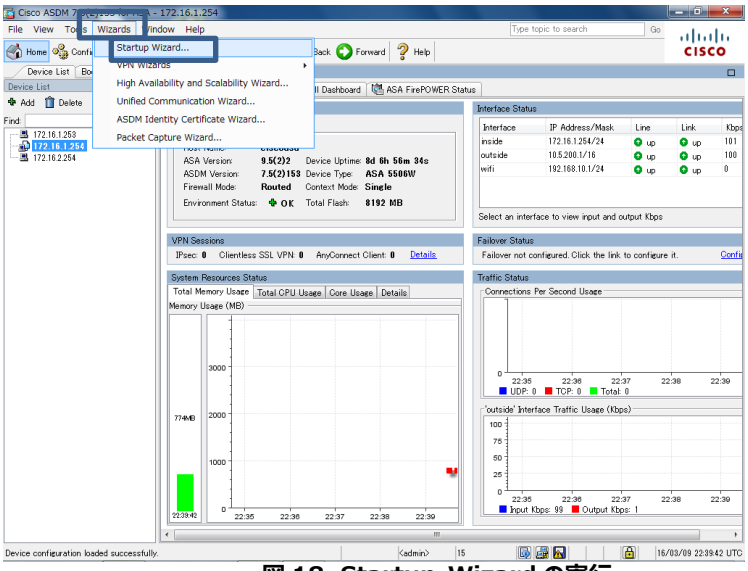

図 18 Startup Wizard の実行

3) 「Modify existing configuration」を選択し、「Next」をクリックします。

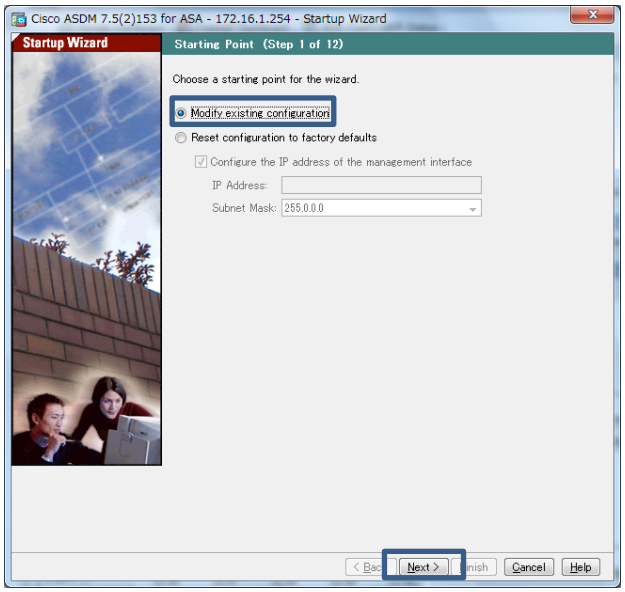

図 19 既存設定の変更

4) Step2 から Step8 までは設定の変更を行わず、「Next」をクリックします。

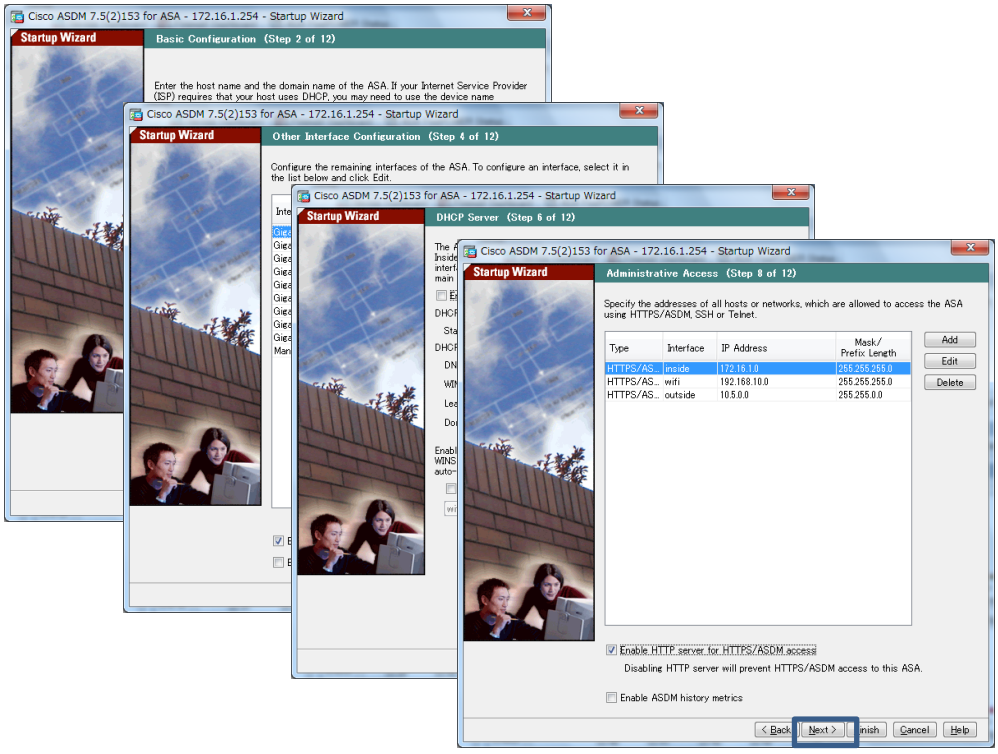

図 20 Step2 から Step8 までの省略

5) FirePOWERモジュールの管理用IPアドレスとゲートウェイアドレスを設定します。「IP Address」を「172.16.1.253」、「Subnet Mask」を「255.255.255.0」、「Gateway」を「172.16.1.254」に設定し、「Next」をクリックします。

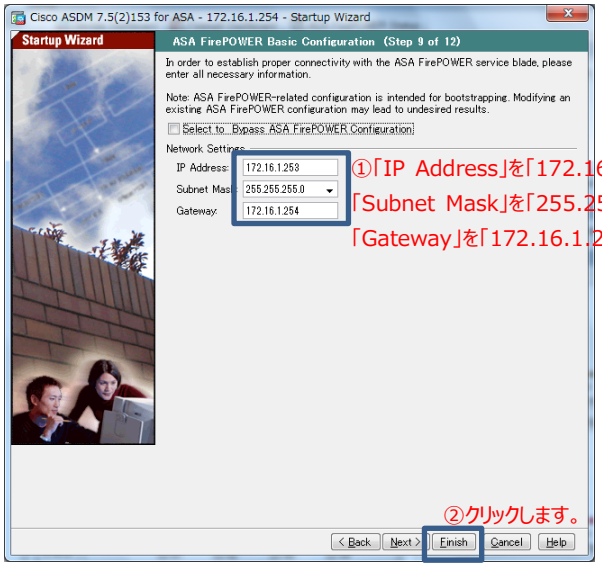

図 21　FirePOWER モジュールの管理用 IP アドレスの設定

6) Step10 では変更せず「Next」をクリックし、Step11 では「Do not enable Smart Call Home」選択して「Next」をクリックします。Step12 の「Configuration Summary」を確認して「Finish」をクリックすると、「Preview CLI Commands」に ASA と FirePOWER モジュールに対して実行されるコマンドが表示されますので、「Send」をクリックして設定変更を実行します。

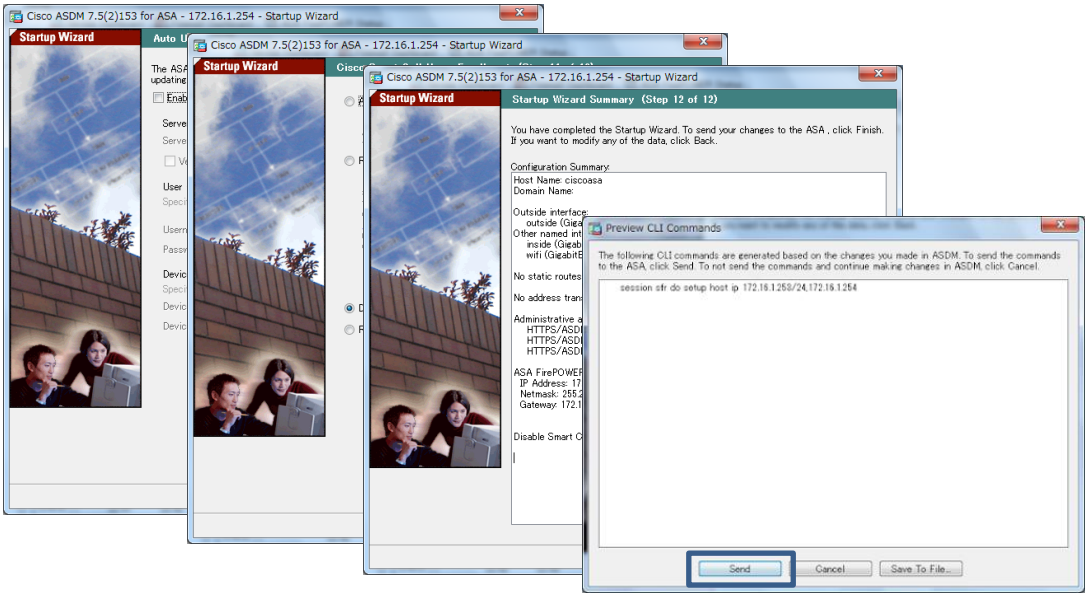

図 22　設定のコマンド確認と実行

7) 設定変更の実行後に、**ASDM を一旦クローズし、再度アクセスします。**ASDM 起動後に「ASA FirePOWER Dashboard]や[ASA FirePOWER Reporting]のダッシュボードのタブが表示されている場合、正常に接続ができています。

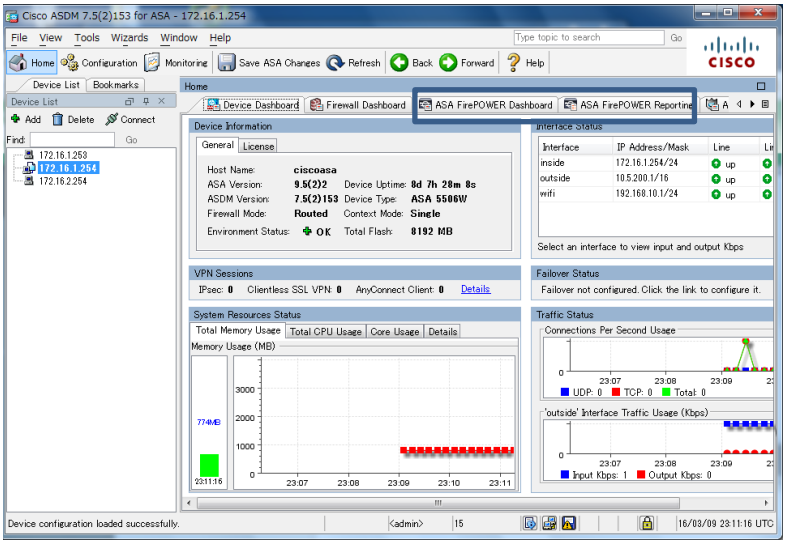

図 23 FirePOWER モジュール接続の確認

8) 「Configuration」>「Device Setup」>「System Time」>「Clock」または「NTP」で時刻設定を行います。本書では「Clock」での手動設定を行います。「Time Zone」は「(GMT+9:00)Tokyo」を選択し、「Date」に年月日、「Time」に時刻を設定し、「Apply」をクリックして設定を反映します。

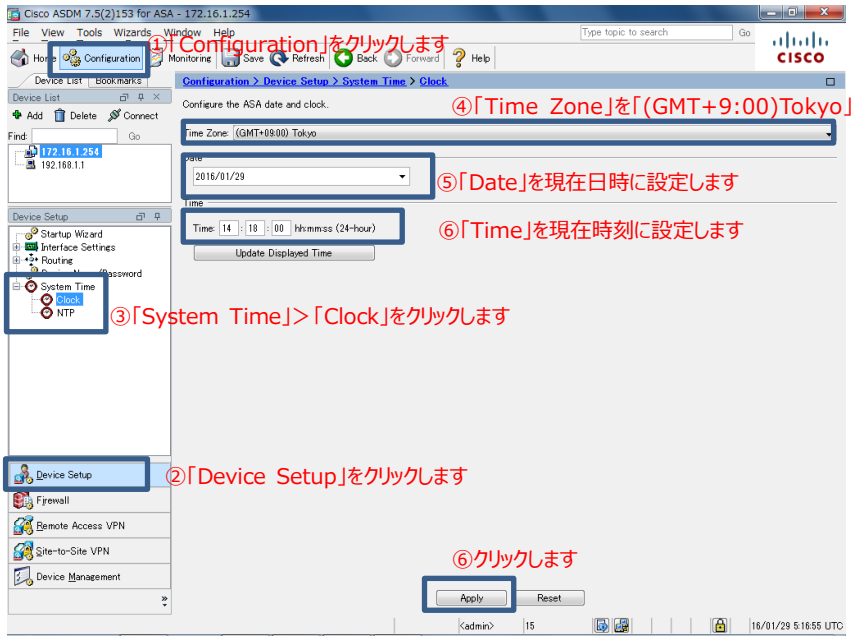

図 24 時刻設定

9) ここまでの設定の完了後、管理用 PC からインターネットに対して、Ping などにより通信が行えることを確認します。

図 25 通信確認

3.2.5 FirePOWER モジュールへのコンソールアクセスと DNS サーバ設定

本項では FirePOWER モジュールへのコンソールアクセス方法と、CLI で DNS サーバの IP アドレスを設定について説明します。※FirePOWER の URL フィルタリング機能を利用する場合は、DNS サーバの設定が必須となります。

1) ASA 5506-X の CLI で **session sfr console** コマンドを実行すると、FirePOWER モジュールのコンソールへ移動します。※ASA に戻る場合は、「Ctrl キー」+「Shit キー」+「6」を同時に押してから「x」を押します。

```
ciscoasa# session sfr console   ①ASA から FirePOWER モジュールのコンソールへ移動します
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Sourcefire3D login: admin   ②ユーザ名入力します(デフォルト:admin)
Password: Sourcefire        ③パスワード入力します(デフォルト:Sourcefire)
Last login: Thu Jan 14 03:42:29 UTC 2016 on ttyS1

Copyright 2004-2015, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Linux OS v5.4.1 (build 12)
Cisco ASA5506W v5.4.1 (build 211)

>
```

2) FirePOWER モジュールの CLI にて **configure network dns servers *<ip address>*** コマンドにより DNS サーバの IP アドレスを設定します。

```
> configure network dns servers 172.16.1.251   ①DNS サーバの IP アドレスを設定します
```

4. お問い合わせ

Q　製品のご購入に関するお問い合わせ

https://info-networld.smartseminar.jp/public/application/add/152

Q　ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q　製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

株式会社ネットワールド
Networld