Cisco ASA 5500 バージョン 8.3 以降への移行

リリース：2010 年 3 月 8 日
更新日：2013 年 4 月 3 日

【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。

このマニュアルでは、Cisco ASA 5500 オペレーティング システム（OS）を以前のバージョンからバージョン 8.3 以降にアップグレードする場合の設定移行プロセスについて説明します。

この文書は、次の項で構成されています。

ソフトウェアのアップグレード

CLI を使用してソフトウェアをアップグレードするには、以下の URL にある『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Managing Software and Configurations」の章を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/admin_swconfig.html

ASDM を使用してソフトウェアをアップグレードするには、以下の URL にある『*Cisco ASA 5500 Series Configuration Guide using ASDM*』の「Managing Software and Configurations」の章を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/asdm63/configuration_guide/admin_swconfig.html

移行について

ここでは、移行機能、元の設定ファイルの自動バックアップ、新しく移行した設定の保存について説明します。この項では、次のトピックについて取り上げます。

移行対象機能

バージョン 8.3 での主な変更点のうち、移行が必要なものは次のとおりです。

- アクセス リストで実際の IP アドレスが必要（サポートされている機能でアクセス リストが使用されている場合）：NAT や PAT が使用されている場合、従来はアクセス リストを使用するすべての機能について、アクセス リストでマップアドレスとポートを指定する必要がありました。現在は、サポートされている機能の一部で、実際の変換されていない IP アドレスとポートを使用する必要があります （それ以外の機能では引き続きマップ IP アドレスを使用します）。
- NAT：NAT 機能は再設計により柔軟性と機能性が向上しました。すべての NAT および NAT 関連コマンドが再設計されています。
- 名前付きネットワークおよびサービス オブジェクト：ネットワークおよびサービス オブジェクトが NAT 用に自動的に作成されます。

（注） 他の機能でも、アクセス リストやオブジェクト グループなどの名前付きネットワークおよびサービス オブジェクトを使用できますが、NAT 以外の機能に使用するオブジェクトは自動的には作成されません。

8.3 または 8.4(1) から 8.4(2) にアップグレードすると、スタティック アイデンティティ NAT の移行が実行され、既存機能が保持されます。詳細については、「8.3 および 8.4 から 8.4(2) への NAT の移行の例」（P.19）を参照してください。

以前の設定、NAT 移行ファイル、およびブートアップ エラー ログの自動バックアップ

以前のスタートアップ コンフィギュレーションは自動的にフラッシュ メモリに保存されます。すべての移行メッセージが含まれる NAT 移行ファイルおよびブートアップ エラー ログも自動的にフラッシュ メモリに保存されます。

この項では、次のトピックについて取り上げます。

コンフィギュレーション ファイルのバックアップ

従来のスタートアップ コンフィギュレーション ファイルのうち、次のファイルはフラッシュ メモリに保存されます。

- シングル モード コンフィギュレーション ファイルまたはマルチ モード システム設定：**disk0:***major_minor_maint_interim*_**startup_cfg.sav**（*major_minor_maint_interim* は従来の OS バージョン番号）

  例：8_2_1_0_startup_cfg.sav

- マルチ モード コンテキスト設定（フラッシュ メモリにある場合）：**disk0:***major_minor_maint_interim_context*_**cfg.sav**（*major_minor_maint_interim* は従来の OS バージョン番号、*context* はコンテキスト名）

  例：8_2_1_0_context1_cfg.sav

コンフィギュレーション ファイルを保存できるだけのメモリがない場合、エラー メッセージが ASA のコンソールに表示され、ブートアップ エラー ログ ファイルに保存されます。移行処理の一部として保存されたファイルは削除され、移行が中止されます。

NAT 移行ファイル

NAT 設定を移行すると、次のファイルがルート ディレクトリに追加されます。nat_ident_migrate。この空のファイルがある場合は構成が移行されたことを示し、これによってブート アップ時の再移行を防ぎます。

ブートアップ エラー ログ ファイル

ブートアップ エラー ログを表示するには、**show startup-config errors** コマンドを入力します。ログの例を以下に示します。

```
hostname# show startup-config errors
Reading from flash...
!
REAL IP MIGRATION: WARNING
In this version access-lists used in 'access-group', 'class-map',
'dynamic-filter classify-list', 'aaa match' will be migrated from
using IP address/ports as seen on interface, to their real values.
If an access-list used by these features is shared with per-user ACL
then the original access-list has to be recreated.
INFO: Note that identical IP addresses or overlapping IP ranges on
different interfaces are not detectable by automated Real IP migration.
```

```
If your deployment contains such scenarios, please verify your migrated
configuration is appropriate for those overlapping addresses/ranges.
Please also refer to the ASA 8.3 migration guide for a complete
explanation of the automated migration process.

INFO: MIGRATION - Saving the startup configuration to file

INFO: MIGRATION - Startup configuration saved to file 'flash:8_2_1_15_startup_cfg.sav'
*** Output from config line 4, "ASA Version 8.2(1)15 "
NAT migration logs:
INFO: NAT migration completed.
Real IP migration logs:
        ACL <1> has been migrated to real-ip version
```

移行した設定の保存

移行した設定は実行中のメモリに保管されているだけなので、この設定をスタートアップ コンフィギュレーションに保存する必要があります。保存しない場合、次にリロードした時点で元の設定に移行プロセスが再度実行されます。

- CLI：**write memory** コマンドを入力します。
- ASDM：ウィンドウ上部の [Save] をクリックします。

アクセス リストの移行における実際の IP アドレス

NAT または PAT を使用する場合、一部の機能ではアクセス リストにマップ アドレスおよびポートが必要なくなります。これらの機能については、必ず変換されていない実際のアドレスとポートを使用する必要があります。実際のアドレスとポートを使用すると、NAT 設定を変更してもアクセス リストを変更する必要はなくなります。この項では、次のトピックについて取り上げます。

実際の IP アドレスを使用する機能

現在、次のコマンドでアクセス リストの実際の IP アドレスを使用しています。これらの機能で使用するすべての **access-list** コマンドは、特に記載されているものを除き自動的に移行されます。ネットワーク オブジェクト グループを使用するアクセス リスト（**object-group network** コマンド）では、オブジェクト グループ内の IP アドレスは移行時に実際の IP アドレスに変換されます。

- **access-group** コマンド
- モジュラ ポリシー フレームワークの **match access-list** コマンド
- ボットネット トラフィック フィルタの **dynamic-filter enable classify-list** コマンド
- AAA の **aaa ... match** コマンド

- WCCP の **wccp redirect-list group-list** コマンド

（注） WCCP の **wccp redirect-list group-list** コマンドは自動的には移行されません。WCCP アクセス リストは起動後にダウンロードされるため、自動移行は発生しません。実際の IP アドレスが設定されたアクセス リストを使用するには、手動で **wccp redirect-list group-list** コマンドを変更する必要があります。

たとえば、従来は NAT を使用している内部ホストに外部ホストがアクセスできるようにするには、**access-group** コマンドを使用して外部インターフェイスで受信アクセス リストを適用していました。この場合、アクセス リストの内部ホストのマップ アドレスを指定する必要がありました。これは、そのアドレスが外部ネットワークで使用できるアドレスとなるためです。バージョン 8.3 以降では、アクセス リストで実際のアドレスを指定する必要があります。

ASDM

次の機能では、マップ アドレスではなく実際のアドレスを使用するようになりました。

- アクセル ルール
- AAA ルール
- サービス ポリシー規則
- ボットネット トラフィック フィルタの分類
- WCCP リダイレクション

（注） WCCP リダイレクションは自動的には移行されません。WCCP ACL は起動後にダウンロードされるため、自動移行できません。実際の IP アドレスを使用するには、手動で ACL を変更する必要があります。

引き続きマップ IP アドレスを使用する機能

次の機能はアクセス リストを使用していますが、これらのアクセス リストはインターフェイス上に表示されるマップ リストを使用します。

- IPSec アクセス リスト
- **capture** コマンド アクセス リスト
- ユーザごとのアクセス リスト
- ルーティング プロトコル アクセス リスト
- 他のすべての機能のアクセス リスト ...

実際の IP アドレスの移行の命名規則

- 多くの場合、移行後に **access-list** コマンドが元の名前で作成されます。そのため、アクセス リスト名を参照する設定は変更されません。アクセス リストが複数の機能に適用されていて、変換の結果複数の ACE が生成された場合、異なる 2 つのアクセス リストが作成され、元のアクセス リストは削除されます。新しいアクセス リストの名前は、元の名前にサフィックスを追加した「*元の名前*_migration_*X*」（*X* は 1 から始まる番号）という形式になります。

- オブジェクト グループの内容を実際の IP アドレスに変更する必要がある場合、「*元の名前_X*」（*X* は 1 から始まる番号）という新しい **object-group** コマンドが作成されます。アクセス リストでは新しい **object-group** コマンドが参照されます。

syslog メッセージの移行

次の syslog メッセージについては、宛先 IP アドレスが *mapped-id* 形式から *real-ip* 形式に変更され、syslog 内のアドレスが設定と一致するようになりました。

- **access-group** コマンドの syslog ID 106001 が変更されました。
- **access-group** コマンドの syslog ID 106100 が変更されました。
- **access-group** コマンドの syslog ID 106023 が変更されました。
- **set connection** コマンドの syslog ID 201010、201011、201012、201013 が変更されました。

実際の IP アドレスの移行の例

表 1 は、アクセス リストが実際の IP アドレスを使用するように移行する方法を示しています。参考のため、NAT 設定が従来の設定の中に示されています。NAT 移行については、「NAT 移行」（P.15）を参照してください。

表 1　実際の IP アドレスの移行の例

説明	設定の移行
入力アクセス グループがあるスタティック NAT	**従来の設定** *static (inside,outside) 172.23.57.1 10.50.50.50 netmask 255.255.255.255* access-list 1 permit ip any host **172.23.57.1** access-group 1 in interface outside **移行後の設定** access-list 1 permit ip any host **10.50.50.50** access-group 1 in interface outside
出力アクセス グループがあるスタティック NAT	**従来の設定** *static (inside,outside) 172.23.57.170 10.50.50.50* object-group network hm 　network-object host **172.23.57.170** access-list 2 extended deny tcp object-group hm any eq www access-group 2 out interface outside **移行後の設定** object-group network hm_1 　network-object host **10.50.50.50** access-list 2 extended deny tcp object-group hm_1 any eq www access-group 2 out interface outside

表 1　実際の IP アドレスの移行の例 （続き）

説明	設定の移行
マップ サブネットと一致するアクセス リストがあるスタティック ホスト NAT	**従来の設定** *static (inside,outside) 172.23.57.170 10.50.50.50* access-list 1 extended permit ip any 172.23.57.0 255.255.255.0 access-group 1 in interface outside **移行後の設定** **access-list 1 extended permit ip any host 10.50.50.50** access-list 1 extended permit ip any 172.23.57.0 255.255.255.0 access-group 1 in interface outside
スタティック PAT（アクセス規則のうち 1 つの ACE のみが PAT と一致）	**従来の設定** *static (inside,outside) tcp 172.23.57.170 5080 10.50.50.50 80* access-list 1 extended permit tcp any host 172.23.57.170 eq 5080 access-list 1 extended permit udp any host 172.23.57.170 eq 5080 access-list 1 extended permit tcp any host 172.23.57.170 eq 10000 access-list 1 extended permit tcp any host 10.2.3.4 eq 5080 access-group 1 in interface outside **移行後の設定** access-list 1 extended permit tcp any host **10.50.50.50 eq 80** access-list 1 extended permit udp any host 172.23.57.170 eq 5080 access-list 1 extended permit tcp any host 172.23.57.170 eq 10000 access-list 1 extended permit tcp any host 10.2.3.4 eq 5080 access-group 1 in interface outside
AAA があるダイナミック NAT	**従来の設定** *global (outside) 1 172.23.57.171-172.23.57.172* *nat (inside) 1 10.50.50.0 255.255.255.0* *nat (dmz) 1 192.168.4.0 255.255.255.0* *object-group network mapped_pool* *network-object host 172.23.57.171* *network-object host 172.23.57.172* access-list 1 permit udp any **object-group mapped_pool** *aaa authentication match 1 outside TEST_SERVER* **移行後の設定** access-list 1 permit udp any **10.50.50.0 255.255.255.0** access-list 1 permit udp any **192.168.4.0 255.255.255.0**

表 1　実際の IP アドレスの移行の例 （続き）

説明	設定の移行

インターフェイス固有のサービス ポリシー	**従来の設定**
	static (inside,outside) tcp 172.23.57.170 6021 10.50.50.50 21
	
	access-list 1 permit tcp any host 172.23.57.170 eq 6021
	
	class-map ftpclass
	  match access-list 1
	policy-map ftp_pol
	  class ftpclass
	  inspect ftp
	service-policy ftp_pol interface outside
	
	移行後の設定
	access-list 1 permit tcp any host **10.50.50.50 eq ftp**
	
	class-map ftpclass
	  match access-list 1
	policy-map ftp_pol
	  class ftpclass
	  inspect ftp
	service-policy ftp_pol interface outside

グローバル サービス ポリシー（インターフェイスのサブセットのみで使用する NAT）	**従来の設定**
	static (inside,outside) 172.23.57.170 10.50.50.50
	
	access-list 1 permit ip any host 172.23.57.170
	
	class-map c1
	  match access-list 1
	policy-map global_policy
	  class c1
	  ips inline fail-close
	service-policy global_policy global
	
	移行後の設定
	access-list 1 permit ip any host 10.50.50.50
	access-list 1 permit ip any host 172.23.57.170
	
	class-map c1
	  match access-list 1
	policy-map global_policy
	  class c1
	  ips inline fail-close
	service-policy global_policy global

表 1　　実際の IP アドレスの移行の例 （続き）

説明	設定の移行
アクセス グループとサービス ポリシーの間で共有するアクセス リスト（マップ サブネットと一致するアクセス リストがあるスタティック ホスト NAT）	**従来の設定** *static (inside,outside) 172.23.57.170 10.50.50.50* access-list 1 extended permit ip any 172.23.57.0 255.255.255.0 access-group 1 in interface outside class-map c1 　match access-list 1 policy-map p1 　class c1 　　inspect http service-policy global_policy global **移行後の設定** **access-list 1 extended permit ip any host 10.50.50.50** access-list 1 extended permit ip any 172.23.57.0 255.255.255.0 access-group 1 in interface outside class-map c1 　match access-list 1 policy-map p1 　class c1 　　inspect http service-policy global_policy global
移行後に複数のアクセス リストに変換された 1 件のアクセス リスト	**従来の設定** *static (outside,inside) 172.23.1.10 10.132.44.12 netmask 255.255.255.255* *static (outside,dmz) 172.23.1.10 10.132.44.135 netmask 255.255.255.255* access-list 1 extended permit ip any host 172.23.1.10 access-group 1 in interface inside access-group 1 in interface dmz **移行後の設定** access-list 1**_1** extended permit ip any host **10.132.44.12** access-group 1**_1** in interface inside access-list 1**_2** extended permit ip any host **10.132.44.135** access-group 1**_2** in interface dmz
ポリシー NAT 移行	**従来の設定** *access-list policyacl1 extended permit ip host 10.50.50.50 10.0.0.0 255.0.0.0* *global (outside) 1 172.23.57.170* *nat (inside) 1 access-list policyacl1* access-list 1 permit ip any host **172.23.57.170** access-group 1 in interface outside **移行後の設定** access-list 1 extended permit ip any host **10.50.50.50** access-group 1 in interface outside

表 1　実際の IP アドレスの移行の例 （続き）

説明	設定の移行
オブジェクト グループの拡張	**従来の設定** *object network obj-10.1.2.0* *subnet 10.1.2.0 255.255.255.0* *object-group network TEST* *network-object object obj-10.1.2.0* *network-object host 192.168.101.10* *static (inside,outside) 10.1.2.1 172.16.2.1* *static (mgmt,outside) 192.168.101.10 172.16.2.10* access-list 1 extended permit ip any **object-group TEST** access-group 1 in interface outside **移行後の設定** access-list 1 remark Migration, ACE (line 1) expanded: permit ip any object-group TEST access-list 1 extended permit ip any host **172.16.2.1** access-list 1 extended permit ip any **10.1.2.0 255.255.255.0** access-list 1 extended permit ip any host **172.16.2.10** access-list 1 remark Migration: End of expansion
拒否または許可 ACE があるアクセス グループ	**従来の設定** *global (outside) 1 10.10.10.128-10.10.10.255* *nat (inside) 1 172.16.10.0 255.255.255.0* access-list 100 extended deny ip any host **10.10.10.210** access-list 100 extended permit ip any **10.10.10.211 255.255.255.128** access-group 100 in interface outside **移行後の設定** access-list 100 extended deny ip any **172.16.10.0 255.255.255.0** access-group 100 in interface outside

実際の IP アドレスの移行のメッセージと制限

この項では、実際の IP アドレスの移行に関連するメッセージについて説明します。一部のメッセージは移行できない設定に関連しているため、ユーザの介入が必要です。また、メッセージが生成されない他の条件についても一覧にして紹介します。この項では、次のトピックについて取り上げます。

- 「実際の IP アドレスの移行のメッセージ」（P.10）
- 「ACE のインターフェイス IP アドレスでは、実際のアドレスか マップ アドレスかを判別できない」（P.14）

実際の IP アドレスの移行のメッセージ

バージョン 8.3 を最初にリロードすると、次のメッセージが表示されます。

```
REAL IP MIGRATION: WARNING
    In this version access-lists used in 'access-group', 'class-map',
    'dynamic-filter classify-list', 'aaa match' will be migrated from
    using IP address/ports as seen on interface, to their real values.
    If an access-list used by these features is shared with per-user ACL
```

```
then the original access-list has to be recreated.
Please refer to documentation for more details.
```

表 2 は、表示されるその他のメッセージの一覧です。

表 2　実際の IP アドレスの移行のメッセージ

メッセージと説明
エラー メッセージ　Couldn't migrate ACL <name> into real values, please manually migrate. Associated access-group config is removed. **説明**　**access-group** コマンドがアクセス リストを使用し、そのアクセス リストが何らかの理由で移行されなかった場合、**access-group** コマンドは削除されるため、セキュリティ ホールは発生しません。

エラー メッセージ　ACE converted to real IP/port values based on dynamic NAT or PAT. The new ACE(s) could be broader in scope than this original ACE.
 	
説明　ダイナミック NAT を使用していて、アクセス リストにグローバル プールのアドレスのサブセットがある場合、NAT コマンドがアクセス リストより幅広くなるためアクセス リストが移行されません。**nat** コマンドで実際の IP アドレスを使用してアクセス リストを移行すると、元のアクセス規則より幅広いアクセス規則が生成されます。このとき、**access-group** コマンドは削除されるため、セキュリティ ホールは発生しません。
`global (outside) 1 10.10.10.128-10.10.10.255`
`nat (inside) 1 192.168.10.0 255.255.255.0`
 	
`access-list 100 extended permit ip any host` **`10.10.10.210 <---If this were migrated, it would be 192.168.10.0, which is too broad.`**
`access-group 100 in interface outside` **`<---This is deleted`**

エラー メッセージ　ACE converted to real IP/port values based on dynamic/static Policy NAT. The new ACE(s) need to be checked for enforcing policy NAT ACL.
 	
説明　ポリシー NAT を移行する場合、新しいアクセス リストによりセキュリティ ホールが発生しないことを確認します。たとえば、次の移行前設定では、宛先アドレスが 10.0.0.0 の場合に限り 10.50.50.50 を 172.23.57.170 に変換します。
`access-list policyacl1 extended permit ip host 10.50.50.50 10.0.0.0 255.0.0.0`
 	
`static (inside,outside) 172.23.57.170 access-list policyacl1`
 	
このアクセス規則ではマップ アドレスへのすべてのトラフィックが許可されていますが、このマッピングはトラフィックが 10.0.0.0 との間で送受信される場合しか発生しないため、実質的には 10.0.0.0 に対してのみ内部ホストへのアクセスを許可していることになります。
`access-list 1 permit ip any host 172.23.57.170`
`access-group 1 in interface outside`
 	
移行後の設定は内部ホストへのすべてのトラフィックが許可されていますが、アクセス リストでは実際の IP アドレスが使用されているため、10.0.0.0 からのトラフィックだけではなくすべてのトラフィックが内部ホストにアクセスできます。
`access-list 1 extended permit ip any host 10.50.50.50`
`access-group 1 in interface outside`
 	
推奨処置　このアクセス リストは次のように修正する必要があります。
`access-list 1 extended permit ip 10.0.0.0 255.0.0.0 host 10.50.50.50`
`access-group 1 in interface outside`

表 2　実際の IP アドレスの移行のメッセージ （続き）

メッセージと説明
エラー メッセージ　ACL <inbound_auth> has been successfully migrated to real-ip version **説明**　アクセス リストが移行されて、同じ名前が使用されました。

エラー メッセージ　After migration source network is 'any', originally it wasn't 'any'.
 	
エラー メッセージ　After migration destination network is 'any', originally it wasn't 'any'.
説明　アクセス リストは移行されていません。NAT 設定に **nat (inside) 1 0 0** があるため、アクセス リストは **any any** に移行されます。**any any** アクセス リストによりセキュリティ ホールが開くため、この移行は省略されます。たとえば、すべてのアドレスはグローバル プールに変換されます。
`global (outside) 1 172.23.57.0-172.23.57.255`
`nat (inside) 1 0 0`
その後、すべてのアドレスに対してグローバル プール アドレスへのアクセスが許可されます。
`object-group network mapped_pool`
`  network-object network 172.23.57.0 255.255.255.0`
 	
`access-list 1 permit udp any object-group mapped_pool`
`access-group 1 in interface outside`
移行によりこのアクセス規則が作成されるため、この規則は次の項目には移行しません。
`access-list 1 permit udp any any`
`access-group 1 in interface outside`

エラー メッセージ　Can't convert rule to hole. **説明**　内部エラー条件です。
エラー メッセージ　Can't create new ACE with obj-grp. **説明**　内部エラー条件です。
エラー メッセージ　Can't create new hole. **説明**　内部エラー条件です。
エラー メッセージ　Conversion for interface <if_name> failed for line. **説明**　内部エラー条件です。
エラー メッセージ　Destination changed for egress ACL, can't migrate this ACL. **説明**　内部エラー条件です。

表 2　実際の IP アドレスの移行のメッセージ （続き）

メッセージと説明
エラー メッセージ　During migration of access-list <name> expanded this object-group ACE. **説明**　オブジェクト グループ内の各アドレスに対してアクセス リストを作成する必要があります。「オブジェクト グループの拡張」の移行例を参照してください。
エラー メッセージ　Failed to create acl element to track during migration. **説明**　内部エラー条件です。

エラー メッセージ　INFO: Note that identical IP addresses or overlapping IP ranges on different interfaces are not detectable by automated Real IP migration. If your deployment contains such scenarios, please verify your migrated configuration is appropriate for those overlapping addresses/ranges. Please also refer to the ASA 8.3 migration guide for a complete explanation of the automated migration process.
 	
説明　場合によっては、アドレスの重複に対応できるようアクセス規則を変更することができます（次の例を参照してください）。アクセス規則を変更できない場合、ネットワークの重複に対して新しい IP アドレス指定スキームの使用が必要になることがあります。
たとえば、次の移行前設定には 2 件のスタティック規則があり、その中で 2 つの Inside インターフェイス（group1 と group2）の IP アドレス 192.168.1.1 が、outside インターフェイスにアクセスする場合に個別にマップされます。
`static (group1,outside) 10.10.1.1 192.168.1.1`
`static (group2,outside) 10.10.2.1 192.168.1.1`
 	
次の ACE は、outside インターフェイスの送信方向に対して適用される **access-group** コマンドで使用された場合、group1 マップ アドレス（10.10.1.1）が outside インターフェイスを終了することを許可し、一方で group2 マップ アドレス（10.10.2.1）を拒否します。
`access-list out_acl extended permit ip host 10.10.1.1 any`
`access-list out_acl extended deny ip host 10.10.2.1 any`
`access-group out_acl out interface outside`
 	
しかし、ACE を実際の IP アドレスに変換すると、10.10.1.1 と 10.10.2.1 の両方のマップ アドレスが実際のアドレス 192.168.1.1 に変換されます。最初の ACE は 192.168.1.1 へのトラフィックを許可しているため、拒否 ACE が適用されることはなく、トラフィックは group1 と group2 のホストの両方に送信されます。
`object foo`
`  host 192.168.1.1`
`  nat (group1,outside) static 10.10.1.1`
`object bar`
`  host 192.168.1.1`
`  nat (group2,outside) static 10.10.2.1`
`access-list out_acl extended permit ip object foo any`
`access-list out_acl extended deny ip object bar any` **<----This ACE will never be hit**
`access-group out_acl out interface outside`
 	
推奨処置　この場合、アクセス規則は次のように変更できます。
`access-list out_acl1 extended permit ip object foo any`
`access-list out_acl2 extended deny ip object bar any`
`access-group out_acl1 in interface group1`
`access-group out_acl2 in interface group2`

表 2　実際の IP アドレスの移行のメッセージ （続き）

メッセージと説明
エラー メッセージ　No ACL was changed as part of Real-ip migration **説明**　アクセス リストの変更は必要ありません。
エラー メッセージ　Removing ACL <name>, it has been migrated to one or more ACLs with name format <name_x>, example <name_7> **説明**　アクセス リストが移行され、その結果複数のアクセス リストが新しい名前で作成されました。従来のアクセス リストは削除されました。
エラー メッセージ　Something changed in conversion but not clear what changed. **説明**　内部エラー条件です。
エラー メッセージ　Source changed for ingress ACL, can't migrate this ACL. **説明**　内部エラー条件です。

ACE のインターフェイス IP アドレスでは、実際のアドレスか マップ アドレスかを判別できない

インターフェイスに属する IP アドレスがある ACE を使用していて、対応する NAT コマンドが **interface** キーワードを使用してインターフェイス IP アドレスを識別している場合、移行スクリプトでは NAT コマンドと ACE を対応させることができず、ACE の IP アドレスが実際のアドレスかマップアドレスかを判別できません。

この場合、移行スクリプトでは IP アドレスを移行できないため、IP アドレスを手動で実際の IP アドレスに変更する必要があります。または、ACE で **interface** キーワードを使用するよう設定を変更します。

たとえば、移行前は outside インターフェイスの PAT が内部ホストに対して定義されています。

```
static (inside,outside) tcp interface 80 10.2.2.2 80
```

アクセス リストの定義には **interface** キーワードではなくインターフェイス IP アドレスを使用します。

```
access-list outside_access_in permit tcp any host 192.168.1.1 eq 80
access-group outside_access_in in interface outside
```

バージョン 8.3 に移行する場合、**static** コマンドが **access-list** コマンドと対応しないため、アクセス リストは実際の IP アドレス（10.2.2.2）には移行されません。**interface** キーワードを使用していれば、アクセス リストは **interface** キーワードではなく実際の IP アドレスを使用するよう正しく移行されています。

移行後にアクセス リストを修正するには、アクセス リストが実際の IP アドレス（10.2.2.2）を使用するよう設定を変更します。

```
access-list outside_access_in permit tcp any host 10.2.2.2 eq 80
```

NAT 移行

NAT 機能は再設計により柔軟性と機能性が向上しました。すべての NAT および NAT 関連コマンドが再設計されています。この項では、NAT 設定を新しい NAT コマンドに移行する方法について説明します。ASDM ユーザの場合は、関連する「ASDM」の項を参照してください。この項では、次のトピックについて取り上げます。

（注） ほぼすべての NAT 設定がシームレスに移行されます。まれにユーザの介入が必要になることがありますが、その場合はユーザに対して通知されます。移行後に通知なくセキュリティが低下することはありません。「NAT 移行のメッセージ」（P.36）を参照してください。

従来の NAT コマンド

次のコマンドはサポートされません。これらのコマンドは新しいコマンドに移行し、設定から削除されます。

- **alias**
- **global**
- **nat**（以前のバージョン）
- **nat-control**
- **static**
- **sysopt nodnsalias**：このコマンドは移行されません。新しい NAT コマンドで **dns** オプションを設定してください。

ASDM

ASDM ではこれまでも **alias** コマンドは使用できませんでした。

新しい NAT コマンド

表 3 に新しい NAT コマンドを示します。「NAT 用の補助コマンド」（P.17）も参照してください。

表 3　　新しい NAT コマンド

新しいコマンド	コンフィギュレーション モード	構文
ネットワーク オブジェクト NAT（通常は標準 NAT 設定に使用します）		
nat dynamic	オブジェクト ネットワーク	**object network** *name* **nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** {[*mapped_inline_host_ip*] [**interface**] | [*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**]] [**interface**]} [**dns**]
nat static	オブジェクト ネットワーク	**object network** *name* **nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface**} [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]
Twice NAT（通常はポリシー NAT 設定に使用します）		
nat source dynamic	グローバル	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source dynamic** {*real_obj* | **any**} {[*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**]] [**interface**]} [**destination static** {*mapped_obj* | **interface**} {*real_obj* | **any**}] [**service** {*mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*]
nat source static	グローバル	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** {*real_obj* | **any**} {*mapped_obj* | **interface** | **any**}} [**destination static** {*mapped_obj* | **interface**} {*real_obj* | **any**}] [**service** {*real_src_mapped_dest_svc_obj* | **any**} *mapped_src_real_dest_svc_obj*] [**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*]

（注） 8.4(2) に、**no-proxy-arp**、**route-lookup**、**pat-pool**、および **round-robin** キーワードが追加されました。

ASDM

ASDM では、既存の NAT 規則が新しい 2 種類の規則に移行されます。

- ネットワーク オブジェクト NAT：
  [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] > [Add/Edit Network Object]
- Twice NAT：
  [Configuration] > [Firewall] > [NAT Rules]

NAT 用の補助コマンド

新しい NAT コマンドに移行できるようにするため、表 4 に示すように追加コマンドが作成されています。

表 4　NAT 用の補助コマンド

生成されたコマンド	説明
object network	各ネットワーク オブジェクト NAT コマンドに対して、変換する実際の IP アドレスを表す **object network** コマンドが作成されます。新しい **nat** コマンドは **object network** コマンドのサブコマンドです。同様に、インライン アドレス（コマンドに直接入力するアドレス）が使用できない場合、新しい **nat** コマンドのマップ アドレスに対して **object network** コマンドが作成されます。 Twice NAT では **object network** コマンドで IP アドレスしか識別できず、インライン アドレスや **access-list** コマンドは識別できないため、従来の設定にある IP アドレスは **object network** コマンドに変換されます。 NAT 設定で使用されていた **name** コマンドは自動的に新しい **object network** コマンドに移行されます。**name** コマンドは、**object network** コマンドをサポートしていない機能で使用するため、引き続き使用できます。
object service	Twice NAT では、すべてのインライン サービス、および従来ポリシー NAT で使用されていた **access-list** コマンドで識別されたサービスに対して **object service** コマンドが作成されます。
object-group network	ネットワーク オブジェクト NAT でマップ アドレスが複数存在する場合、複数の **object network** コマンドを含む **object-group network** コマンドが作成されます。

作成されたコマンドの命名規則などのネットワーク オブジェクトやサービス オブジェクトの詳細については、「ネットワークおよびサービス オブジェクトの移行」（P.39）を参照してください。

ASDM

これまでのリリースでは、ASDM は名前付きネットワーク オブジェクトをサポートしていました。現在、プラットフォームではコマンドによりこれらのオブジェクトを適切にサポートしています。設定のすべての名前付きネットワーク オブジェクトの表示に加えて、ASDM は、設定で使用されている IP アドレスのオブジェクトを自動的に作成します。この自動生成されるオブジェクトは IP アドレスによって識別され、プラットフォーム設定オブジェクトとしては存在しません。これらのオブジェクトの 1 つに名前を割り当てると、ASDM は、プラットフォーム設定に名前付きネットワーク オブジェクトを追加します。

（注） ASDM は、**name** コマンドから派生したオブジェクトを表示しなくなりました。以前は、ASDM において **name** コマンドから派生した名前付きオブジェクトを使用することがありました。**name** コマンドの IP アドレスが移行されなかった場合（「ネットワークおよびサービス オブジェクトの移行」（P.39）を参照）、これらのオブジェクトは、IP アドレスによって識別される自動作成オブジェクトで置換されます。

NAT 規則の順序の維持

従来の NAT 設定では、NAT コマンドの順序の評価は NAT の種類に基づいて行われ、場合によってはコマンドが設定内に登場する順序に基づいて行われていました。新しい NAT の順序は 3 つのセクションがあるテーブルに基づいています。

- セクション 1（Twice NAT 規則）：これらの規則は設定内に登場する順序に基づいて評価されます。移行のため、このセクションには移行済みのポリシー NAT 規則が含まれています。
- セクション 2（ネットワーク オブジェクト NAT（生成済み）規則）：これらの規則は内部規則に基づいて評価されます。設定内での順序は評価基準とはなりません（詳しくは『*Cisco ASA 5500 Series Configuration Guide using ASDM*』または『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください）。移行のため、このセクションには標準 NAT 規則が含まれています。
- セクション 3（ネットワーク オブジェクト NAT 規則の後に評価するよう明確に指定された Twice NAT 規則）：セクション 1 と同様に、これらの規則は設定内に登場する順序に基づいて評価されます。ただし、評価の順序はセクション 1 とセクション 2 の規則より後となります。このセクションは NAT 移行には使用しません。

ネットワークが重複する場合（たとえば、標準スタティック NAT 規則がダイナミック ポリシー NAT 規則と重複する場合）、標準スタティック NAT 規則はセクション 2 ではなくセクション 1 に移行され、設定の順序が維持されます。たとえば、従来の設定が次のようになっている場合、ネットワークが重複しています。この場合、スタティック コマンドはセクション 1 の Twice NAT 規則に移行されます。

```
static (inside,outside) 209.165.202.129 10.1.1.6 netmask 255.255.255.255
access-list NET1 permit ip 10.1.1.0 255.255.255.0 209.165.202.0 255.255.255.0
nat (inside) 100 access-list NET1
```

NAT 移行のガイドラインと制限

- ダイナミック アイデンティティ NAT（**nat 0** コマンド）は移行されません。「NAT 移行のメッセージ」（P.36）を参照してください。スタティック アイデンティティ NAT は他の **static** コマンドと同様に処理され、標準 NAT かポリシー NAT かによって変換が異なります。
- NAT 免除（**nat 0 access-list** コマンド）は、アップグレードするリリースに応じて異なる方法で移行されます。詳細については、「NAT 免除」（P.25）を参照してください。
- 8.3(1)、8.3(2)、または 8.4(1) から 8.4(2) にアップグレードすると、アイデンティティ NAT の移行が実行され、既存機能が保持されます。詳細については、「8.3 および 8.4 から 8.4(2) への NAT の移行の例」（P.19）を参照してください。
- 標準 NAT コマンドに **dns** オプションが設定されている場合、移行対象となります。スタティック PAT コマンドとポリシー NAT コマンドの **dns** オプションは無視されます。
- 従来の NAT コマンドの接続設定：**conn-max**、**emb-limit**、**norandomseq**、**nailed** などのオプションはサービス ポリシーに移動されます。

  新しいサービス ポリシーでは次の命名規則が使用されます。

  - **class-map**：class-conn-param-*protocol-n*
  - **access-list**：acl-conn-param-*protocol-n*
  - **policy-map**：policy-conn-param-*interface*

  NAT 移行に関連するこの他の命名規則については、「オブジェクト移行の命名規則」（P.41）を参照してください。

8.3 および 8.4 から 8.4(2) への NAT の移行の例

8.3(1)、8.3(2)、または 8.4(2) をすでに実行している場合、既存の機能を保持するため、すべてのアイデンティティ NAT ステートメントは次の新しいキーワードを使用するように移行されます。

- **no-proxy-arp**
- **route-lookup**（ルーテッド ファイアウォール モードのみ）

バージョン 8.4(2) 以降では、アイデンティティ NAT は、プロキシ ARP を実行し、デフォルトで、NAT 設定を使用して出力インターフェイスを決定します。8.3(1)、8.3(2)、8.4(2) にあった機能を維持するため、プロキシ ARP はディセーブルにされ、新しいキーワードを使用してルート検索が実行され、出力インターフェイスが決定されます。プロキシ ARP をイネーブルにする場合（まれな要件）、または出力インターフェイスを決定するために NAT 設定を使用する場合は、移行後に手動でキーワードを排除します。

unidirectional キーワードがある場合（8.3(2) または 8.4(1) への NAT 免除規則の最初の移行の場合など）、キーワードは除外されます。

表 5 に、スタティック アイデンティティ NAT の移行の例を示します。

表 5　アイデンティティ NAT 移行の例

説明	設定の移行

スタティック オブジェクト NAT	**従来の設定**
	`object network obj-10.1.1.6`
	`  host 10.1.1.6`
	`  nat (inside,outside) static 10.1.1.6`
	
	移行後の設定
	`object network obj-10.1.1.6`
	`  host 10.1.1.6`
	`  nat (inside,outside) static 10.1.1.6 no-proxy-arp route-lookup`

スタティック Twice NAT（unidirectional）	**従来の設定**
	`nat (inside,any) source static any any destination static obj-192.168.90.0-01 obj-192.168.90.0-01 unidirectional`
	
	移行後の設定
	`nat (inside,any) source static any any destination static obj-192.168.90.0-01 obj-192.168.90.0-01 no-proxy-arp route-lookup`

スタティック Twice NAT	**従来の設定**
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0`
	
	移行後の設定
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`

8.2 以前からの NAT の移行の例

この項では、次のトピックについて取り上げます。

スタティック NAT/PAT

表 6 に、スタティック NAT/PAT の移行の例を示します。

表 6　スタティック NAT/PAT 移行の例

説明	設定の移行	種類 / セクション

標準スタティック NAT	**従来の設定**
	`static (inside,outside) 209.165.201.15 10.1.1.6 netmask 255.255.255.255`
	
	移行後の設定
	`object network obj-10.1.1.6`
	`  host 10.1.1.6`
	`  nat (inside,outside) static 209.165.201.15`
		オブジェクト / セクション 2

表 6　スタティック NAT/PAT 移行の例 （続き）

説明	設定の移行	種類 / セクション

標準スタティック PAT	**従来の設定**
	`static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask 255.255.255.255`
	
	移行後の設定
	`object network obj-10.1.1.16`
	`  host 10.1.1.16`
	`  nat (inside,outside) static 10.1.2.45 service tcp 8080 www`
		オブジェクト / セクション 2

スタティックポリシー NAT	**従来の設定**
	`access-list NET1 permit ip host 10.1.2.27 10.76.5.0 255.255.255.224`
	
	`static (inside,outside) 209.165.202.129 access-list NET1`
	
	移行後の設定
	`object network obj-10.1.2.27`
	`  host 10.1.2.27`
	`object network obj-209.165.202.129`
	`  host 209.165.202.129`
	`object network obj-10.76.5.0`
	`  subnet 10.76.5.0 255.255.255.224`
	
	`nat (inside,outside) source static obj-10.1.2.27 obj-209.165.202.129 destination static obj-10.76.5.0 obj-10.76.5.0`
		Twice / セクション 1

ダイナミック NAT/PAT

表 7 に、ダイナミック NAT/PAT の移行の例を示します。

表 7　ダイナミック NAT/PAT の移行の例

説明	設定の移行	種類 / セクション

標準ダイナミック PAT	**従来の設定**
	`nat (inside) 1 192.168.1.0 255.255.255.0`
	`nat (dmz) 1 10.1.1.0 255.255.255.0`
	`global (outside) 1 209.165.201.3`
	
	移行後の設定
	`object network obj-192.168.1.0`
	`  subnet 192.168.1.0 255.255.255.0`
	`  nat (inside,outside) dynamic 209.165.201.3`
	`object network obj-10.1.1.0`
	`  subnet 10.1.1.0 255.255.255.0`
	`  nat (dmz,outside) dynamic 209.165.201.3`
		オブジェクト / セクション 2

標準ダイナミック PAT (2)	**従来の設定**
	`nat (inside) 1 10.1.2.0 255.255.255.0`
	`global (outside) 1 209.165.201.3`
	`global (dmz) 1 172.16.4.5`
	
	移行後の設定
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`  nat (inside,outside) dynamic 209.165.201.3`
	`object network obj-10.1.2.0-01`
	`  subnet 10.1.2.0 255.255.255.0`
	`  nat (inside,dmz) dynamic 172.16.4.5`
		オブジェクト / セクション 2

標準ダイナミック PAT (3)	**従来の設定**
	`nat (inside) 1 0 0`
	`global (outside) 1 interface`
	
	移行後の設定
	`object network obj_any`
	`  subnet 0.0.0.0 0.0.0.0`
	`  nat (inside,outside) dynamic interface`
		オブジェクト / セクション 2

表 7　ダイナミック NAT/PAT の移行の例 （続き）

説明	設定の移行	種類 / セクション

ダイナミックポリシー NAT	**従来の設定**
	`object-group network og-net-src`
	`  network-object 192.168.1.0 255.255.255.0`
	`  network-object 192.168.2.0 255.255.255.0`
	`object-group network og-net-dst`
	`  network-object 209.165.201.0 255.255.255.224`
	`object-group service og-ser-src`
	`  service-object tcp gt 2000`
	`  service-object tcp eq 1500`
	
	`access-list NET6 extended permit object-group og-ser-src object-group og-net-src object-group og-net-dst`
	
	`nat (inside) 10 access-list NET6`
	`global (outside) 10 209.165.200.225`
	
	移行後の設定
	`object-group network og-net-src`
	`  network-object 192.168.1.0 255.255.255.0`
	`  network-object 192.168.2.0 255.255.255.0`
	`object-group network og-net-dst`
	`  network-object 209.165.201.0 255.255.255.224`
	`object network obj-209.165.200.225`
	`  host 209.165.200.225`
	`object service obj_tcp_range_2001_65535`
	`  service tcp destination range 2001 65535`
	`object service obj_tcp_eq_1500`
	`  service tcp destination eq 1500`
	
	`nat (inside,outside) source dynamic og-net-src obj-209.165.200.225 destination static og-net-dst og-net-dst service obj_tcp_range_2001_65535 obj_tcp_range_2001_65535`
	
	`nat (inside,outside) source dynamic og-net-src obj-209.165.200.225 destination static og-net-dst og-net-dst service obj_tcp_eq_1500 obj_tcp_eq_1500`
		Twice / セクション 1

表 7　ダイナミック NAT/PAT の移行の例 （続き）

説明	設定の移行	種類 / セクション

ダイナミックポリシー NAT（複数の ACE）	**従来の設定**
	`access-list ACL_NAT permit ip 172.29.0.0 255.255.0.0 172.29.37.0 255.255.255.0`
	`access-list ACL_NAT permit ip 172.29.0.0 255.255.0.0 10.231.110.0 255.255.255.0`
	`access-list ACL_NAT permit ip 172.29.0.0 255.255.0.0 10.107.204.0 255.255.255.0`
	`access-list ACL_NAT permit ip 172.29.0.0 255.255.0.0 192.168.5.0 255.255.255.0`
	
	`nat (inside) 1 access-list ACL_NAT`
	`global (outside) 1 209.165.200.225`
	
	移行後の設定
	`object network obj-172.29.0.0`
	`  subnet 172.29.0.0 255.255.0.0`
	`object network obj-209.165.200.225`
	`  host 209.165.200.225`
	`object network obj-172.29.37.0`
	`  subnet 172.29.37.0 255.255.255.0`
	`object network obj-10.231.110.0`
	`  subnet 10.231.110.0 255.255.255.0`
	`object network obj-10.107.204.0`
	`  subnet 10.107.204.0 255.255.255.0`
	`object network obj-192.168.5.0`
	`  subnet 192.168.5.0 255.255.255.0`
	
	`nat (inside,outside) source dynamic obj-172.29.0.0 obj-209.165.200.225 destination static obj-172.29.37.0 obj-172.29.37.0`
	
	`nat (inside,outside) source dynamic obj-172.29.0.0 obj-209.165.200.225 destination static obj-10.231.110.0 obj-10.231.110.0`
	
	`nat (inside,outside) source dynamic obj-172.29.0.0 obj-209.165.200.225 destination static obj-10.107.204.0 obj-10.107.204.0`
	
	`nat (inside,outside) source dynamic obj-172.29.0.0 obj-209.165.200.225 destination static obj-192.168.5.0 obj-192.168.5.0`
		Twice / セクション 1

表 7　ダイナミック NAT/PAT の移行の例 （続き）

説明	設定の移行	種類 / セクション

外部 NAT	**従来の設定**
	`global (inside) 1 10.1.2.30-10.1.2.40`
	`nat (dmz) 1 10.1.1.0 255.255.255.0 outside`
	
	`static (inside,dmz) 10.1.1.5 10.1.2.27 netmask 255.255.255.255`
	
	移行後の設定
	`object network obj-10.1.2.30-10.1.2.40`
	`  range 10.1.2.30 10.1.2.40`
	`object network obj-10.1.2.27`
	`  host 10.1.2.27`
	`  nat (inside,dmz) static 10.1.1.5`
	`object network obj-10.1.1.0`
	`  subnet 10.1.1.0 255.255.255.0`
	`  nat (dmz,inside) dynamic obj-10.1.2.30-10.1.2.40`
		オブジェクト / セクション 2

NAT とインターフェイス PAT の併用	**従来の設定**
	`nat (inside) 1 10.1.2.0 255.255.255.0`
	`global (outside) 1 interface`
	`global (outside) 1 209.165.201.1-209.165.201.2`
	
	移行後の設定
	`object network obj-209.165.201.1_209.165.201.2`
	`  range 209.165.201.1 209.165.201.2`
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`  nat (inside,outside) dynamic obj_209.165.201.1_209.165.201.2 interface`
		オブジェクト / セクション 2

NAT 免除

NAT 免除（**nat 0 access-list** コマンド）はポリシー NAT の一形態で、スタティック Twice NAT に変換されます。免除されたインターフェイスとセキュリティ レベルが低いすべてのインターフェイスとの間で規則が作成されます。外部 NAT については、免除されたインターフェイスとセキュリティ レベルが高いすべてのインターフェイスとの間で規則が作成されます。同じセキュリティ レベルの通信をイネーブルにした場合、免除されたインターフェイスと同じセキュリティ レベルのインターフェイスとの間で規則が作成されます。

これらの規則はセクション 1 の最初に配置されます。

NAT 免除（**nat 0 access-list** コマンド）は、Twice NAT 規則に移行されます。NAT 免除がどのように移行されるかに関して、アップグレードするバージョンに固有の情報は、次の注を参照してください。

- バージョン 8.3(1)：警告 #CSCtf89372 が表示されることがあります。8.4(2) に直接移行することが推奨されます。この警告の詳細については、次の URL の Bug Toolkit を参照してください。

  http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

- バージョン 8.3(2) から 8.4(1)：**unidirectional** キーワードが追加されました。**unidirectional** キーワードは、接続を開始するために、送信元ネットワークのトラフィックのみを許可します。この移行の変更は、CSCtf89372 を解消するために、実施されました。NAT 免除が通常双方向であるため、**unidirectional** キーワードを取り除いて元の機能を復元する必要がある場合があります。具体的には、この変更により、NAT 免除ルールを含む、多くの VPN 設定に悪い影響があります（この新しい問題については CSCti36048 を参照してください）。手動による介入を避けるために、8.4(2)

に移行することが推奨されます。

この問題が発生した場合、次のような syslog メッセージが表示されます。

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection
for icmp src Outside:192.168.1.5 dst inside:10.10.5.20 (type 8, code 0) denied due to
NAT reverse path failure
```

- バージョン 8.4(2) 以降：**unidirectional** キーワードは追加されなくなります。代わりに、新しい **no-proxy-arp キーワード**、および **route-lookup** キーワードが追加されます。警告 CSCtf89372 および CSCti36048 の両方が、このリリースで解決されます。

この項で紹介する例では、システムには inside（レベル 100）、outside（レベル 0）、dmz（レベル 50）の 3 つのインターフェイスがあります。

表 8 に、NAT 免除の移行の例を示します。

表 8　NAT 免除の移行の例

説明	設定の移行	種類 / セクション

標準 NAT 免除（ダイナミック NAT の重複が見られる）	**従来の設定**
	`access-list outside_nat_outbound extended permit ip 192.168.90.0 255.255.254.0 host 10.1.4.5`
	
	`nat (outside) 2 access-list outside_nat_outbound outside`
	`global (inside) 2 interface`
	
	`access-list inside_nat0_outbound_1 extended permit ip any 192.168.90.0 255.255.254.0`
	
	`nat (inside) 0 access-list inside_nat0_outbound_1`
	
	移行後の設定
	8.3(1)：
	`nat (outside,inside) source dynamic obj-192.168.90.0-01 interface destination static obj-10.1.4.5 obj-10.1.4.5`
	
	`nat (inside,any) source static any any destination static obj-192.168.90.0-01 obj-192.168.90.0-01`
	
	8.3(2) ～ 8.4(1)：
	`nat (outside,inside) source dynamic obj-192.168.90.0-01 interface destination static obj-10.1.4.5 obj-10.1.4.5`
	
	`nat (inside,any) source static any any destination static obj-192.168.90.0-01 obj-192.168.90.0-01 unidirectional`
	
	8.4(2) 以降：
	`nat (outside,inside) source dynamic obj-192.168.90.0-01 interface destination static obj-10.1.4.5 obj-10.1.4.5`
	
	`nat (inside,any) source static any any destination static obj-192.168.90.0-01 obj-192.168.90.0-01 no-proxy-arp route-lookup`
		Twice / セクション 1
		（一番上に配置）

表 8　NAT 免除の移行の例 （続き）

説明	設定の移行	種類 / セクション

標準 NAT 免除	**従来の設定**
	`access-list EXEMPT permit ip 10.1.2.0 255.255.255.0 any`
	
	`nat (inside) 0 access-list EXEMPT`
	`nat (dmz) 0 access-list EXEMPT`
	
	移行後の設定
	8.3(1) :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0`
	
	8.3(2) ～ 8.4(1) :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	
	8.4(2) 以降 :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
		Twice / セクション 1
		（一番上に配置）

表 8　NAT 免除の移行の例 （続き）

説明	設定の移行	種類 / セクション

同じセキュリティ レベルがイネーブル	**従来の設定**
	`same-security-level permit intra-interface`
	
	`access-list EXEMPT permit ip 10.1.2.0 255.255.255.0 any`
	
	`nat (dmz) 0 access-list EXEMPT`
	
	移行後の設定
	8.3(1) :
	`same-security-level permit intra-interface`
	
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0`
	
	`nat (dmz,dmz) source static obj-10.1.2.0 obj-10.1.2.0`
	
	8.3(2) ～ 8.4(1) :
	`same-security-level permit intra-interface`
	
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	
	`nat (dmz,dmz) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	
	8.4(2) 以降 :
	`same-security-level permit intra-interface`
	
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	
	`nat (dmz,outside) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
	
	`nat (dmz,dmz) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
		Twice / セクション 1
		（一番上に配置）

表 8　NAT 免除の移行の例 （続き）

説明	設定の移行	種類 / セクション

外部 NAT	**従来の設定**
	`access-list EXEMPT permit ip 10.1.2.0 255.255.255.0 any`
	`nat (dmz) 0 access-list EXEMPT outside`
	`nat (outside) 0 access-list EXEMPT outside`
	
	移行後の設定
	8.3(1) :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`nat (dmz,inside) source static obj-10.1.2.0 obj-10.1.2.0`
	`nat (outside,dmz) source static obj-10.1.2.0 obj-10.1.2.0`
	`nat (outside,inside) source static obj-10.1.2.0 obj-10.1.2.0`
	8.3(2) ～ 8.4(1) :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`nat (dmz,inside) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	`nat (outside,dmz) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	`nat (outside,inside) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	8.4(2) 以降 :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`nat (dmz,inside) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
	`nat (outside,dmz) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
	`nat (outside,inside) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
		Twice / セクション 1
		（一番上に配置）

表 8　NAT 免除の移行の例 （続き）

説明	設定の移行	種類 / セクション

複数の ACE	**従来の設定**
	`access-list EXEMPT extended permit ip 10.1.2.0 255.255.255.0 any`
	`access-list EXEMPT extended permit ip 10.1.3.0 255.255.255.0 20.2.4.0 255.255.255.0`
	`access-list EXEMPT extended permit ip any 20.2.20.0 255.255.255.0`
	`nat (inside) 0 access-list EXEMPT`
	
	移行後の設定
	8.3(1) :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`object network obj-10.1.3.0`
	`  subnet 10.1.3.0 255.255.255.0`
	`object network obj-20.2.4.0`
	`  subnet 20.2.4.0 255.255.255.0`
	`object network obj-20.2.20.0`
	`  subnet 20.2.20.0 255.255.255.0`
	
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0`
	`nat (inside,any) source static obj-10.1.3.0 obj-10.1.3.0 destination static obj-20.2.4.0 obj-20.2.4.`
	`nat (inside,any) source static any any destination static obj-20.2.20.0 obj-20.2.20.0`
	
	8.3(2) ～ 8.4(1) :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`object network obj-10.1.3.0`
	`  subnet 10.1.3.0 255.255.255.0`
	`object network obj-20.2.4.0`
	`  subnet 20.2.4.0 255.255.255.0`
	`object network obj-20.2.20.0`
	`  subnet 20.2.20.0 255.255.255.0`
	
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0 unidirectional`
	`nat (inside,any) source static obj-10.1.3.0 obj-10.1.3.0 destination static obj-20.2.4.0 obj-20.2.4.0 unidirectional`
	`nat (inside,any) source static any any destination static obj-20.2.20.0 obj-20.2.20.0 unidirectional`
	
	8.4(2) 以降 :
	`object network obj-10.1.2.0`
	`  subnet 10.1.2.0 255.255.255.0`
	`object network obj-10.1.3.0`
	`  subnet 10.1.3.0 255.255.255.0`
	`object network obj-20.2.4.0`
	`  subnet 20.2.4.0 255.255.255.0`
	`object network obj-20.2.20.0`
	`  subnet 20.2.20.0 255.255.255.0`
	
	`nat (inside,any) source static obj-10.1.2.0 obj-10.1.2.0 no-proxy-arp route-lookup`
	`nat (inside,any) source static obj-10.1.3.0 obj-10.1.3.0 destination static obj-20.2.4.0 obj-20.2.4.0 no-proxy-arp route-lookup`
	`nat (inside,any) source static any any destination static obj-20.2.20.0 obj-20.2.20.0 no-proxy-arp route-lookup`
		Twice / セクション 1
		（一番上に配置）

NAT コントロール

nat-control コマンドは非推奨となっています。セキュリティの高いインターフェイスからセキュリティの低いインターフェイスまでの、すべてのトラフィックを変換する要件を維持するため、各インターフェイスのセクション 2 の末尾に NAT 規則が挿入され、残りのトラフィックがすべて拒否されます。**nat-control** コマンドは、旧バージョンの ASA で定義された NAT コンフィギュレーションに対して使用されました。NAT ルールが存在しないことに基づくのではなく、アクセス コントロールにアクセス ルールを使用して、ASA を通過するトラフィックを阻止することがベスト プラクティスです。

表 9 に、NAT コントロールの移行の例を示します。

表 9　NAT コントロールの移行の例

説明	設定の移行	種類 / セクション

4 種類のインターフェイス（inside、outside、dmz、mgmt）	**従来の設定**
	`nat-control`
	
	移行後の設定
	`object network obj_any`
	`  subnet 0.0.0.0 0.0.0.0`
	`  nat (inside,outside) dynamic obj-0.0.0.0`
	`object network obj-0.0.0.0`
	`  host 0.0.0.0`
	`object network obj_any-01`
	`  subnet 0.0.0.0 0.0.0.0`
	`  nat (inside,mgmt) dynamic obj-0.0.0.0`
	`object network obj_any-02`
	`  subnet 0.0.0.0 0.0.0.0`
	`  nat (inside,dmz) dynamic obj-0.0.0.0`
	`object network obj_any-03`
	`  subnet 0.0.0.0 0.0.0.0`
	`  nat (mgmt,outside) dynamic obj-0.0.0.0`
	`object network obj_any-04`
	`  subnet 0.0.0.0 0.0.0.0`
	`  nat (dmz,outside) dynamic obj-0.0.0.0`
	`object network obj_any-05`
	`  subnet 0.0.0.0 0.0.0.0`
	`  nat (dmz,mgmt) dynamic obj-0.0.0.0`
		オブジェクト / セクション 2
		
		（一番下に配置）

DNS Rewrite

標準 NAT コマンドに **dns** オプションが設定されている場合、移行対象となります。スタティック PAT コマンドとポリシー NAT コマンドの **dns** オプションは無視されます。

表 10 に、DNS リライトの移行の例を示します。

表 10　DNS リライトの移行の例

説明	設定の移行	種類 / セクション

dns オプションが設定されたスタティック コマンド	**従来の設定**
	`static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns`
	
	移行後の設定
	`object network obj-192.168.100.10`
	`  host 192.168.100.10`
	`  nat (inside,outside) static 172.20.1.10 dns`
		オブジェクト / セクション 2

Connection Settings

従来の NAT コマンドの接続設定：**conn-max**、**emb-limit**、**norandomseq**、**nailed** などのオプションはサービス ポリシーに移動されます。

命名規則については、「NAT 移行のガイドラインと制限」（P.18）を参照してください。

表 11 に接続設定の移行の例を示します。

表 11　接続設定の移行の例

説明	設定の移行	種類 / セクション

TCP および UDP 最大接続数、ランダム シーケンス番号のディセーブル化、nailed オプション	**従来の設定**
	`static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 tcp 10 20 norandomseq nailed`
	
	移行後の設定
	`access-list acl-conn-param-tcp-01 extended permit tcp host 192.168.100.10 any`
	`t`
	`class-map class-conn-param-tcp-01`
	`  match access-list acl-conn-param-tcp-01`
	
	`policy-map policy-conn-param-inside`
	`  class class-conn-param-tcp-01`
	`  set connection per-client-max 10 per-client-embryonic-max 20`
	`  random-sequence-number disable`
	
	`  set connection advanced-options tcp-state-bypass`
	
	`service-policy policy-conn-param-inside interface inside`
	
	`object network obj-192.168.100.10`
	`  host 192.168.100.10`
	`  nat (inside,outside) static 172.20.1.10`
		オブジェクト / セクション 2

表 11　接続設定の移行の例 （続き）

説明	設定の移行	種類 / セクション

UDP 最大接続数	**従来の設定**
	`access-list NAT_ACL permit ip host 10.76.6.111 any`
	
	`nat (dmz) 101 access-list NAT_ACL` **`udp 6`**
	`global (outside) 101 225.22.22.1`
	
	移行後の設定
	`access-list NAT_ACL extended permit ip host 10.76.6.111 any`
	
	`class-map class-conn-param-udp-01`
	`  match access-list NAT_ACL`
	
	`policy-map policy-conn-param-dmz`
	`  class class-conn-param-udp-01`
	`  set connection per-client-max 6`
	
	`service-policy policy-conn-param-dmz interface dmz`
	
	`object network obj-10.76.6.111`
	`  host 10.76.6.111`
	`  nat (dmz,outside) dynamic 225.22.22.1`
		オブジェクト / セクション 2

送信元 NAT と宛先 NAT

バージョン 8.3 よりも前では、ポリシー NAT を使用して送信元 NAT と宛先 NAT を指定していましたが、送信元 NAT アドレス上でしか NAT は実行されませんでした。バージョン 8.3 以降では、必要があれば NAT を宛先アドレスに対しても設定できます。従来の設定では、この機能を実現するには、1 件の接続に対し、送信元 NAT と宛先 NAT の NAT 規則を別々に、あわせて 2 件設定する必要がありました。移行の過程で、別々の 2 件の NAT 規則が結合され、1 件の Twice NAT コマンドが生成されます。

表 12 にの送信元 NAT と宛先 NAT の移行の例を示します。

表 12　送信元 NAT と宛先 NAT の移行の例

説明	設定の移行	種類 / セクション

送信元 NAT と宛先 NAT のスタティック コマンド	**従来の設定**
	`access-list NET1 permit ip host 192.168.1.1 host 192.168.1.10`
	`access-list NET2 permit ip host 209.165.200.225 host 209.165.200.228`
	`static (inside,outside) 209.165.200.228 access-list NET1`
	`static (outside,inside) 192.168.1.10 access-list NET2`
	
	移行後の設定
	`object network obj-192.168.1.1`
	`  host 192.168.1.1`
	`object network obj-209.165.200.228`
	`  host 209.165.200.228`
	`object network obj-209.165.200.225`
	`  host 209.165.200.225`
	`object network obj-192.168.1.10`
	`  host 192.168.1.10`
	`nat (inside,outside) source static obj-192.168.1.1 obj-209.165.200.228 destination static obj-192.168.1.10 obj-209.165.200.225`
	(次の規則は移行スクリプトにより作成されていますが、必要であるとは限りません。まれに、トラフィックがこれらの規則のうちいずれかを使用することがあります)
	`nat (inside,outside) source static obj-192.168.1.1 obj-209.165.200.228 destination static obj-192.168.1.10 obj-192.168.1.10`
	`nat (outside,inside) source static obj-209.165.200.225 obj-192.168.1.10 destination static obj-209.165.200.228 obj-209.165.200.228`
		Twice / セクション 1

表 12　送信元 NAT と宛先 NAT の移行の例 （続き）

説明	設定の移行	種類 / セクション

送信元 NAT と宛先 NAT のスタティック コマンドとダイナミック コマンド	**従来の設定**
	`access-list NET1 permit ip host 192.168.1.1 host 192.168.1.10`
	
	`access-list NET2 permit ip host 209.165.200.225 host 209.165.200.228`
	
	`static (outside,inside) 192.168.1.10 access-list NET2`
	
	`global (outside) 100 209.165.200.228`
	`nat (inside) 100 access-list NET1`
	
	移行後の設定
	`object network obj-192.168.1.1`
	`  host 192.168.1.1`
	`object network obj-209.165.200.228`
	`  host 209.165.200.228`
	`object network obj-209.165.200.225`
	`  host 209.165.200.225`
	`object network obj-192.168.1.10`
	`  host 192.168.1.10`
	
	`nat (inside,outside) source dynamic obj-192.168.1.1 obj-209.165.200.228 destination static obj-192.168.1.10 obj-209.165.200.225`
	
	(次の規則は移行スクリプトにより作成されていますが、必要であるとは限りません。まれに、トラフィックがこの規則を使用することがあります)
	`nat (inside,outside) source dynamic obj-192.168.1.1 obj-209.165.200.228 destination static obj-192.168.1.10 obj-192.168.1.10`
	
	`nat (outside,inside) source static obj-209.165.200.225 obj-192.168.1.10 destination static obj-209.165.200.228 obj-209.165.200.228`
		Twice / セクション 1

alias コマンド

alias コマンドは任意のインターフェイスにある IP ネットワークのアドレスを、別のインターフェイス経由で接続している別の IP ネットワークのアドレスに変換します。

表 13 に alias の移行の例を示します。

表 13　alias コマンドの移行の例

説明	設定の移行	種類 / セクション

alias コマンド	**従来の設定**
	`alias (inside) 209.165.200.225 192.168.100.10`
	
	移行後の設定
	`object network obj-192.168.100.10`
	`  host 192.168.100.10`
	`  nat (any,inside) static 209.165.200.225 dns`
		オブジェクト / セクション 2

NAT 移行のメッセージ

一部の NAT 設定は自動的には移行されません。また、元の設定とやや異なる場合もあります。表 14 は表示される可能性があるエラー メッセージと、各メッセージに関する情報の一覧です。

表 14　NAT 移行のメッセージ

メッセージと説明
エラー メッセージ　`The following 'nat' command didn't have a matching 'global' rule on interface '<name>' and was not migrated.` **説明**　**global** コマンドが欠落しています。**nat** コマンドに対応する **global** コマンドがない場合、この **nat** コマンドは削除され、移行されません。 **推奨処置**　対応する **global** コマンドが存在しているはずの場合、新しい NAT コマンドで設定を再作成する必要があります。 **例：** **従来の設定** `nat (dmz) 1 10.1.1.0 255.255.255.0` **移行後の設定** 移行されません。

エラー メッセージ　`Alias command was migrated between interfaces 'any' and 'inside' as an estimate.`
 	
説明　**alias** コマンドの移行です。**alias** コマンドは、セキュリティ レベルが同じまたは低いインターフェイスの間で適用されます。移行後、規則は所定のインターフェイスと**任意**のインターフェイスの間に追加されます。新しい規則は自分自身を含むすべてのインターフェイスに適用されるため、これは意味が異なります。
 	
推奨処置　移行方法としては比較的安全で、多くの場合は特別な注意を払う必要はありません。移行の例については、「alias コマンド」（P.35）を参照してください。
 	
例：
 	
従来の設定
`alias (inside) 209.165.200.225 192.168.100.10`
 	
移行後の設定
`object network obj-192.168.100.10`
`  host 192.168.100.10`
`  nat (any,inside) static 209.165.200.225 dns`

表 14　NAT 移行のメッセージ （続き）

メッセージと説明
エラー メッセージ　Identity-NAT was not migrated. If required, an appropriate bypass NAT rule needs to be added. **説明**　アイデンティティ NAT が移行されていません。アイデンティティ NAT（**nat 0** コマンド）は移行されません。また、そのインターフェイスの **nat-control** コマンドも移行されません。 **推奨処置**　スタティック NAT コマンド（オブジェクトまたは Twice NAT）を使用して、新しいアイデンティティ NAT 規則を手動で追加します。 **例：** **従来の設定** `nat (inside) 0 192.168.1.0 255.255.255.0` **移行後の設定** 移行されません。

表 14　　NAT 移行のメッセージ （続き）

メッセージと説明
エラー メッセージ　Range a.b.c.d-p.q.r.s also includes broadcast address as mapped value. **説明**　外部スタティック ポリシー NAT の宛先とブロードキャスト アドレスが重複しています。従来は /31 サブネットを使用してグローバル プールからブロードキャスト アドレスを削除するよう **global** コマンドを設定していました。新しい NAT コマンドでこの機能を設定することはできません。ダイナミック NAT 規則と外部スタティック ポリシー NAT 規則で宛先が重複している場合、移行した設定にはマップされた送信元のブロードキャスト アドレスが含まれます。これらのアドレスを削除するには、ユーザの介入が必要です。 **推奨処置**　マップされたオブジェクトからブロードキャスト アドレスを削除します。

例：

従来の設定

```
nat (inside) 10 10.0.0.0 255.0.0.0
global (outside) 10 192.168.1.3-192.168.2.3 netmask 255.255.255.254
```

（ブロードキャスト アドレス 192.168.1.255 は自動的にプールから削除されます）

```
access-list SNAT extended permit ip 10.10.10.0 255.255.255.0 192.168.2.0 255.255.255.0

static (outside,inside) 10.1.1.0 access-list SNAT
```

移行後の設定

```
object network obj-192.168.1.3-192.168.2.3
    range 192.168.1.3 192.168.2.3
```

（192.168.1.255 はこのプールから自動的には削除されません。192.168.1.255 が割り当てられないようにするには、ネットワーク グループを作成して、次の **nat** コマンドで使用します。

```
object network global_pool1
    range 192.168.1.3 192.168.1.254
object network global_pool2
    range 192.168.2.1 192.168.2.3
object-group network global_pool
    network-object object global_pool1
    network-object object global_pool2
)

object network obj-10.10.10.0
    subnet 10.10.10.0 255.255.255.0
object network obj-10.1.1.0
    subnet 10.1.1.0 255.255.255.0
object network obj-192.168.2.0
    subnet 192.168.2.0 255.255.255.0

object network obj-10.0.0.0
    subnet 10.0.0.0 255.0.0.0
    nat (inside,outside) dynamic obj-192.168.1.3-192.168.2.3

nat (inside,outside) source dynamic obj-10.0.0.0 obj-192.168.1.3-192.168.2.3 destination static obj-10.1.1.0
obj-10.10.10.0

nat (outside,inside) source static obj-10.10.10.0 obj-10.1.1.0 destination static obj-192.168.2.0
obj-192.168.2.0
```

表 14　NAT 移行のメッセージ （続き）

メッセージと説明
エラー メッセージ　The nodnsalias option is deprecated. Use 'dns' option in nat command to enable/disable dns rewrite. **説明**　**sysopt nodnsalias** コマンドが移行されていません。**alias** コマンドがサポートされていないため、**sysopt nodnslias** コマンドは非推奨となっています。 **推奨処置**　DNS リライトをイネーブルまたはディセーブルにするには、新しい NAT コマンドで **dns** オプションを使用します。 **例：** **従来の設定** sysopt nodnsalias **移行後の設定** 移行されません。

ネットワークおよびサービス オブジェクトの移行

ここでは、ネットワークおよびサービス オブジェクトの移行について説明します。次の項目を取り上げます。

オブジェクトでサポートされる機能

バージョン 8.3 では次の機能で名前付きのネットワークおよびサービス オブジェクトを使用しています。

- NAT：詳細については、「NAT 移行」（P.15）を参照してください。NAT では名前付き IP アドレス（name **コマンド**を使用）を使用できなくなりました。
- アクセス リスト：**access-list** コマンド。アクセス リストでは名前付き IP アドレス（name **コマンド**を使用）を使用できなくなりました。
- オブジェクト グループ：**object-group network** および **object-group service** コマンド。名前付き IP アドレスは、オブジェクト グループ、およびネットワーク オブジェクトでは引き続き許可されます。

オブジェクトの移行

新しいネットワークおよびサービス オブジェクト（**object network** および **object service** コマンド）は、次の場合、既存のコマンドに置換されます。

- 各ネットワーク オブジェクト NAT コマンドに対して、変換する実際の IP アドレスを表すために、**object network** コマンドが作成されます。
- 新しい **nat** コマンドでインライン値の代わりにオブジェクトが必要な場合、ネットワークおよびサービス オブジェクトが自動的に作成されます。
- 名前付き IP アドレス（**name** コマンドを使用）を NAT で使用し、**names** コマンドがイネーブルである場合、新しい **nat** コマンドでインライン IP アドレスが使用された場合にも、ネットワーク オブジェクトが作成されます。
- **access-list** コマンドが NAT で使用されていた IP アドレスを含み、その IP アドレスに対して NAT 移行がネットワーク オブジェクトを作成した場合、ネットワーク オブジェクトは、**access-list** コマンドの IP アドレスを置換します。
- **access-list** コマンドで名前付き IP アドレスを使用し（**name** コマンド使用）、**names** コマンドがイネーブルな場合、オブジェクトは名前を置換します。
- 複数の **global** コマンドが同じ NAT ID を共有している場合、インライン IP アドレスに対して作成されたネットワーク オブジェクトで構成されるネットワーク オブジェクト グループが作成されます。

次の場合には、オブジェクトは作成されません。

- **name** コマンドが設定に存在するが、**nat** または **access-list** コマンドで使用されていない。
- **nat** コマンドでまだ許可されているインライン値。
- **object-group** コマンドで使用される **name** コマンド。
- NAT または **name** コマンドによる名前付きに使用されていない、**access-list** コマンドで使用されている IP アドレス。

（注） **name** コマンドは引き続き設定内に存在し、ネットワーク オブジェクトをサポートしていない機能で使用できます。

ASDM

これまでのリリースでは、ASDM は名前付きネットワーク オブジェクトをサポートしていました。現在、プラットフォームではコマンドによりこれらのオブジェクトを適切にサポートしています。

ASDM も、設定で使用されている IP アドレスの非名前付きオブジェクトを自動的に作成します。これらの自動作成されるオブジェクトは *IP アドレス*によってのみ識別され、名前がなく、プラットフォーム設定に名前付きオブジェクトとしては存在しません。

これらの非名前付き ADSM オブジェクトの 1 つに名前を手動で割り当てると、ASDM は、プラットフォーム設定に名前付きネットワーク オブジェクトを追加します。名前を追加しなければ、ASDM 専用オブジェクトのままです。

移行の一部として名前付きオブジェクトを ASA が作成する場合、合致する非名前付き ASDM 専用オブジェクトは、名前付きオブジェクトに置換されます。唯一の例外は、ネットワーク オブジェクト グループの非名前付きオブジェクトです。ネットワーク オブジェクト グループ内にある IP アドレスの名前付きオブジェクトを ASA が作成する場合、ASDM は非名前付きオブジェクトを維持したまま、重複したオブジェクトを ASDM で作成します。これらのオブジェクトをマージするには、[Tools > Migrate Network Object Group Members] を選択します。

（注） ASDM は、**name** コマンドから派生したオブジェクトを表示しなくなりました。以前は、ASDM において **name** コマンドから派生した名前付きオブジェクトを使用することがありました。**name** コマンドの IP アドレスが移行されなかった場合、これらのオブジェクトは、IP アドレスによって識別される自動作成オブジェクトで置換されます。

オブジェクト移行の命名規則

この項では、次のトピックについて取り上げます。

名前または IP アドレスが移行される場合の詳細については、「オブジェクトの移行」（P.39）を参照してください。

name コマンドの命名規則

names コマンドがイネーブルである場合、移行された **name** コマンドに対して、**object network** コマンドに同じ名前が使用されます。

たとえば、次の **name** コマンドが NAT で使用されます。

```
name 10.1.1.1 test
```

次の **object network** コマンドが作成されます。

```
object network test
   host 10.1.1.1
```

names コマンドがイネーブルではなく、IP アドレスがネットワーク オブジェクトに移行された場合は、**name** コマンドと同じ IP アドレスのネットワーク オブジェクトが設定に含まれることはありますが、ネットワーク オブジェクトの名前は自動的に生成され（「インライン IP アドレスの命名規則」（P.41）を参照）、**name** コマンドと同じ名前ではありません。

インライン IP アドレスの命名規則

インラインで使用する移行された IP アドレスの場合、次の命名規則により作成されます。

- ホストとサブネット：**obj-***a.b.c.d*

（注） NAT のインスタンスのうち 1 つだけをオブジェクト上でイネーブルにできます。特定のホストまたはサブネットに複数の NAT ポリシーが割り当てられている場合は、別のネットワーク オブジェクト **obj-***a.b.c.d***-01** が作成されます。

表 15 に、ホストとサブネットのインライン オブジェクトの移行に関する名前設定の例を示します。

表 15　ホストとサブネットのインライン オブジェクトの移行に関する名前の設定の例

インライン値	ネットワーク オブジェクト名
10.76.6.111 255.255.255.255	obj-10.76.6.111
10.76.0.0 255.255.0.0	obj-10.76.0.0

- 範囲：**obj-***a.b.c.d-p.q.r.s*

表 16 に、範囲のインライン オブジェクトの移行に関する名前の設定の例を示します。

表 16　範囲のインライン オブジェクトの移行に関する名前の設定の例

インライン値	ネットワーク オブジェクト名
10.76.6.111-10.76.6.112	obj-10.76.6.111-10.76.6.112

インライン プロトコルの命名規則

インラインで使用する移行されたプロトコルの場合、サービス オブジェクトは **obj-***inline_text* という命名規則により作成されます。

表 17 に、プロトコルのインライン オブジェクトの移行に関する名前の設定の例を示します。

表 17　プロトコルのインライン オブジェクトの移行に関する名前の設定の例

インライン値	サービス オブジェクト名
tcp source range 20 50 eq 2000	obj-tcp_source_range_20_50_eq_2000
tcp gt 1500	obj-tcp_gt_1500

同じ NAT ID で複数の global コマンドを使用する場合のネットワーク オブジェクトの命名規則

複数の **global** コマンドが同じ NAT ID を共有している場合、インライン IP アドレスに対して作成されたネットワーク オブジェクトで構成されるネットワーク オブジェクト グループが作成されます。**og-global-***interface_nat-id* という命名規則が使用されます。

従来の設定

```
global (outside) 1 10.76.6.111
global (outside) 1 10.76.6.109-10.76.6.110
```

新しいネットワーク オブジェクトとグループ

```
object network obj-10.76.6.111
    host 10.76.6.111
object network obj-10.76.6.109-10.76.6.110
    range 10.76.6.109-10.76.6.110
object-group og-global-outside_1
    network-object obj-10.76.6.111
    network-object obj-10.76.6.109-10.76.6.110
```

バージョン 8.3 からのダウングレード

バージョン 8.3 にアップグレードすると、コンフィギュレーションが移行されます。既存のコンフィギュレーションは、自動的にフラッシュ メモリに保存されます。たとえば、8.2(1) から 8.3(1) にアップグレードすると、既存の 8.2(1) コンフィギュレーションはフラッシュ メモリ内の 8_2_1_0_startup_cfg.sav というファイルに保存されます。

この項では、ダウングレードする方法について説明します。次の項目を取り上げます。

- 「アクティベーション キーの互換性に関する情報」（P.43）
- 「ダウングレードの実行」（P.43）

アクティベーション キーの互換性に関する情報

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、*8.2 よりも前*に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2 以降*で導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 旧バージョンでアクティベーション キーを入力した場合は、そのキーが ASA で使用されます（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。最後の時間ベース ライセンスが 8.3 で導入された機能に対応している場合、そのライセンスは旧バージョンでの使用はできなくても、アクティブ ライセンスのままです。永続キーまたは有効な時間ベース キーを再入力してください。
  - フェールオーバー ペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。
  - 1 つの時間ベース ライセンスをインストールしているが、それが 8.3 で導入された機能に対応している場合、ダウングレードの実行後、その時間ベース ライセンスはアクティブなままです。この時間ベース ライセンスをディセーブルにするには、永続キーを再入力する必要があります。

ダウングレードの実行

8.3 からダウングレードするには、次の手順を実行します。

手順の詳細

CLI の場合

ステップ 1 次のコマンドを入力します。

```
hostname(config)# downgrade [/noconfirm] old_image_url old_config_url [activation-key old_key]
```

/noconfirm オプションを指定すると、プロンプトは表示されずにダウングレードされます。*image_url* は、disk0、disk1、tftp、ftp、または smb 上の古いイメージへのパスです。*old_config_url* は、保存されている移行前のコンフィギュレーションへのパスです（デフォルトでは、disk0 に保存されます）。8.3 よりも前のアクティベーション キーに戻る必要がある場合は、そのアクティベーション キーを入力できます。

このコマンドは、次の機能を完了するためのショートカットです。

1. ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。

2. 古いイメージへのブート イメージの設定（**boot system**）。
3. （任意）新たなアクティベーション キーの入力（**activation-key**）。
4. 実行コンフィギュレーションのスタートアップ コンフィギュレーションへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
5. 古いコンフィギュレーションのスタートアップ コンフィギュレーションへのコピー（**copy** *old_config_url* **startup-config**）。
6. リロード（**reload**）。

次に例を示します。

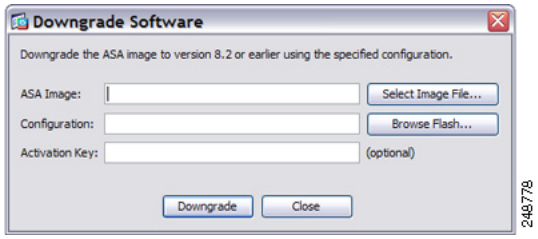
```
hostname(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

ASDM の場合

ステップ 1 [Tools] > [Downgrade Software] を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

図 1　　Downgrade Software



ステップ 2 ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ 3 次のいずれかのオプション ボタンをクリックします。

- [Remote Server]：ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージ ファイルのパスを入力します。
- [Flash File System]：[Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージ ファイルを選択します。

ステップ 4 [Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します （デフォルトでは disk0 に保存されています）。

ステップ 5 （任意）バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

ステップ 6 [Downgrade] をクリックします。

このツールは、次の機能を実行するためのショートカットです。

1. ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
2. 古いイメージへのブート イメージの設定（**boot system**）。
3. （任意）新たなアクティベーション キーの入力（**activation-key**）。

4. 実行コンフィギュレーションのスタートアップ コンフィギュレーションへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
5. 古いコンフィギュレーションのスタートアップ コンフィギュレーションへのコピー（**copy** *old_config_url* **startup-config**）。
6. リロード（**reload**）。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/