変換の例

この項には、ASA 設定の例と、移行ツールが変換先とする FirePOWER Threat Defenseのルールおよびオブジェクトの例が含まれています。

- 例，1 ページ

例

個々のネットワークを指定するアクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
access-group acp1 global
```

変換先：

表 *1*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意（Any）	同等の許可	はい（True）

ネットワーク オブジェクト グループによるアクセス ルール

ASA の設定：

```
access-list acp1 extended permit ip object-group host1 object-group host2
access-group acp1 global
```

変換先：

表 *2*：ネットワーク オブジェクト グループ

名前	ドメイン	値（ネットワーク）	タイプ（**Type**）	オーバーライド（**Override**）
host1	なし	obj1 obj2	グループ	いいえ（False）
host2	None	obj3 obj4	グループ	いいえ（False）

表 *3*：ネットワーク オブジェクト グループを使用したアクセス ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	host1	host2	任意（Any）	任意（Any）	同等の許可	はい（True）

個々のネットワークおよびポートを指定するアクセス ルール

ASA アクセス ルール

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 5.6.7.0 255.255.255.0 eq
80
access-group acp1 global
```

変換先：

表 *4*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/32	5.6.7.0/32	TCP(6)/90	TCP(6)/80	同等の許可	はい（True）

サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object service servObj1
 service tcp destination eq 78
access-list acp1 extended permit object servObj1 any any
access-group acp1 in interface outside
```

変換先：

表 *5*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
servObj1	オブジェクト	なし	TCP(6)/78	いいえ（False）

表 *6*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	servObj1	同等の許可	はい（True）

サービス オブジェクト グループによるアクセス ルール

ASA の設定：

```
object-group service legServGroup tcp
 port-object eq 78
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legServGroup
access-group acp1 global
```

変換先：

表 *7*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
legServGroup	オブジェクト	None	TCP(6)/78	いいえ（False）

表 *8*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート（**Source Port**）	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup	同等の許可	はい（True）

ネストされたサービス オブジェクト グループによるアクセス ルール

ASA の設定：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

変換先：

表 *9*：ポート オブジェクトおよびグループ

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
legServGroup1_1	オブジェクト	None	TCP(6)/78	いいえ（False）
legServGroup1_2	オブジェクト	なし	TCP(6)/79	いいえ（False）
legServGroup2_1	オブジェクト	なし	TCP(6)/80	いいえ（False）
legServGroup2_2	オブジェクト	None	TCP(6)/81	いいえ（False）
legServGroup1	グループ	なし	legServGroup1_1 legServGroup1_2	いいえ（False）
legServGroup2	グループ	なし	legServGroup2_1 legServGroup2_2	いいえ（False）

変換された設定には、ネストされたグループ legacyServiceNestedGrp に相当するものは含まれていないことに注意してください。そのグループはフラット化されていないためです。

表 *10*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	同等の許可	はい（True）

ネストされた拡張サービス オブジェクト グループによるアクセス ルール

ASA の設定：

```
object service http
 service tcp source range 9000 12000 destination eq www
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
object-group service all-http
 service-object object http
 service-object object http-proxy
object-group service all-httpz
 group-object all-http
 service-object tcp destination eq 443
access-list acp1 extended permit object-group all-httpz any any
access-group acp1 in interface inside
```

変換先：

表 *11*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
http_src	オブジェクト	None	TCP(6)/9000 ～ 12000	いいえ（False）
http_dst	オブジェクト	None	TCP(6)/80	いいえ（False）
http-proxy_src	オブジェクト	None	TCP(6)/9000 ～ 12000	いいえ（False）
http-proxy_dst	オブジェクト	None	TCP(6)/8080	いいえ（False）
all-httpz-dst	グループ	なし	TCP(6)/443	いいえ（False）

変換された設定には、ネストされたグループ all-httpz に相当するものは含まれていないことに注意してください。そのグループはフラット化されていないためです。

表 *12*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1_1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	http_src	http_dst	同等の許可	はい（True）
acp1#1_2	任意（Any）	任意（Any）	任意（Any）	任意（Any）	http-proxy_src	http-proxy_dst	同等の許可	はい（True）

名前	送信元ゾーン（Source Zone）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（Destination Port）]	操作	有効（Enabled）
acp1#1_3	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	all-httpz-dst	同等の許可	はい（True）

「gt」および「neq」演算子を使用したサービス オブジェクトによるアクセス ルール

ASA の設定：

```
object service testOperator
 service tcp source gt 100 destination neq 200
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *13*：ポート オブジェクト

名前	タイプ（Type）	ドメイン	値（プロトコル/ポート）	オーバーライド（Override）
testOperator_src	オブジェクト	なし	TCP(6)/101 ～ 65535	いいえ（False）
testOperator_dst_1	オブジェクト	なし	TCP(6)/1 ～ 199	いいえ（False）
testOperator_dst_2	オブジェクト	None	TCP(6)/201 ～ 65535	いいえ（False）
testOperator_dst	グループ	なし	testOperator_dst_1、testOperator_dst_2	いいえ（False）

表 *14*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（Source Zone）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート	操作	有効（Enabled）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	testOperator_src	testOperator_dst	同等の許可	はい（True）

「lt」および「gt」演算子を使用したセキュリティ オブジェクトによるアクセス ルール

ASA の設定：

```
object service testOperator
 service tcp source gt 100 destination lt 200
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *15*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
testOperator_src	オブジェクト	なし	TCP(6)/101 ～ 65535	いいえ（False）
testOperator_dst	オブジェクト	なし	TCP(6)/1 ～ 199	いいえ（False）

表 *16*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	[接続先ポート（**Destination Port**）]	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	testOperator_src	testOperator_dst	同等の許可	はい（True）

「eq」演算子とポート リテラル値を使用した TCP サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object service svcObj1
 service tcp source eq telnet destination eq ssh
access-list acp1 extended permit object testOperator any any
```

変換先：

表 *17*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
svcObj1_src	オブジェクト	なし	TCP(6)/21	いいえ（False）
svcObj1_dst	オブジェクト	なし	TCP(6)/22	いいえ（False）

表 *18*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	svcObj1_src	svcObj1_dst	同等の許可	はい（True）

ICMP サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object-group service icmpObj
 service-object icmp echo-reply 8
 access-list acp1 extended permit object icmpObj any any
```

変換先：

表 *19*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
icmpObj	オブジェクト	なし	ICMP(1)/Echo 応答	いいえ（False）

表 *20*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	icmpObj	同等の許可	はい（True）

プロトコル サービス オブジェクトによるアクセス ルール

ASA の設定：

```
object-group protocol testProtocol
 protocol-object tcp
access-list acp1 extended permit object testProtocol any any
```

変換先：

表 *21*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
testProtocol	オブジェクト	なし	TCP(6)	いいえ（False）

表 *22*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	testProtocol	同等の許可	はい（True）

拡張サービス オブジェクトによるアクセス ルール（送信元のみ）

ASA の設定：

```
object service serviceObj
 service tcp source eq 300
 service tcp source eq 800
access-list acp1 extended permit object serviceObj any any
```

変換先：

表 *23*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
serviceObj_src_1	オブジェクト	None	TCP(6)/300	いいえ（False）
serviceObj_src_2	オブジェクト	None	TCP(6)/800	いいえ（False）
serviceObj	グループ	なし	serviceObj_src_1 serviceObj_src_2	いいえ（False）

表 *24*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	任意（Any）	serviceObj	同等の許可	はい（True）

拡張サービス オブジェクトによるアクセス ルール（送信元と宛先）

ASA の設定：

```
object service serviceObj
 service tcp source eq 300 destination eq 400
access-list acp1 extended permit tcp object serviceObj any any
```

変換先：

表 *25*：ポート オブジェクト

名前	タイプ（**Type**）	ドメイン	値（プロトコル/ポート）	オーバーライド（**Override**）
serviceObj_src	オブジェクト	なし	TCP(6)/300	いいえ（False）
serviceObj_dst	オブジェクト	なし	TCP(6)/400	いいえ（False）

表 *26*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	serviceObj_src	serviceObj_dst	同等の許可	はい（True）

送信元ポートでポート引数演算子「**neq**」を使用したアクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp any neq 300
```

変換先：

表 *27*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート（**Destination Port**）	アクション（**Action**）	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299、301 ～ 65535	任意（Any）	同等の許可	はい（True）

送信元ポートおよび宛先ポートでポート引数演算子「neq」を使用したアクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp any neq 300 any neq 400
```

変換先：

表 *28*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1_1	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299	1 ～ 399	同等の許可	はい（True）
acp1#1_2	任意（Any）	任意（Any）	任意（Any）	任意（Any）	301 ～ 65535	1 ～ 399	同等の許可	はい（True）
acp1#1_3	任意（Any）	任意（Any）	任意（Any）	任意（Any）	1 ～ 299	401 ～ 65535	同等の許可	はい（True）
acp1#1_4	任意（Any）	任意（Any）	任意（Any）	任意（Any）	301 ～ 65535	401 ～ 65535	同等の許可	はい（True）

非アクティブ アクセス ルール

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0 inactive
access-group acp1 global
```

変換先：

表 *29*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン（**Destination Zone**）	送信元ネットワーク	宛先ネットワーク	送信元ポート	接続先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	任意（Any）	任意（Any）	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意（Any）	同等の許可	いいえ（False）

着信トラフィックに適用されるアクセス コントロール リスト

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 in inside
```

変換先：

表 *30*：セキュリティ ゾーン/インターフェイス グループ

名前	インターフェイス タイプ	ドメイン	選択されたインターフェイス
acp1_inside_in_zone	• ルーテッド（ASA デバイスがルーテッドモードで動作している場合） • スイッチド（ASA デバイスがトランスペアレントモードで動作している場合）	なし	任意（Any）

表 *31*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	アクション	有効（**Enabled**）
acp1#1	acp1_inside_in_zone	任意（Any）	3.4.5.0/24	任意（Any）	TCP(6)/90	TCP(6)/80	同等の許可	はい（True）

発信トラフィックに適用されるアクセス コントロール リスト

ASA の設定：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 out outside
```

変換先：

表 *32*：セキュリティ ゾーン/インターフェイス グループ

名前	インターフェイス タイプ	ドメイン	選択されたインターフェイス
acp1_outside_out_zone	• ルーテッド（ASA デバイスがルーテッドモードで動作している場合） • スイッチド（ASAデバイスがトランスペアレントモードで動作している場合）	なし	任意（Any）

表 *33*：アクセス コントロール ルールまたはプレフィルタ ルール

名前	送信元ゾーン（**Source Zone**）	宛先ゾーン	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート（**Destination Port**）	操作	有効（**Enabled**）
acp1#1	acp1_outside_out_zone	任意（Any）	3.4.5.0/24	任意（Any）	TCP(6)/90	TCP(6)/80	同等の許可	はい（True）

例