変換の例

このセクションでは、Cisco ASA 構成と、移行ツールが変換する Firepower Threat Defense ルールとオブジェクトの例を示します。

例

個々のネットワークを指定するアクセスルール

Cisco ASA の構成：

```
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	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	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意	同等に許可	はい（True）

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ルール

Cisco ASA の構成：

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

変換先：

変換の例

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	オーバーライド
host1	なし	obj1 obj2	グループ	False
host2	なし	obj3 obj4	グループ	False

表 *3:* 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ルール

名前	送信元ゾーン	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	アクション	有効
acp1#1	任意	任意	host1	host2	任意	任意	同等に許可	はい（True）

個々のネットワークとポートを指定するアクセスルール

Cisco 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	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	アクション	有効
acp1#1	任意	任意	3.4.5.0/32	5.6.7.0/32	TCP(6)/90	TCP(6)/80	同等に許可	はい（True）

サービスオブジェクトを使用するアクセスルール

Cisco ASA の構成：

```
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：

変換の例

表 *5:* ポートオブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
servObj1	オブジェクト	なし	TCP(6)/78	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	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	アクション	有効
acp1#1	任意	任意	任意	任意	任意	servObj1	同等に許可	はい（True）

サービス オブジェクト グループを使用するアクセスルール

Cisco ASA の構成：

```
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	ドメイン	値（プロトコル/ポート）	オーバーライド
legServGroup	オブジェクト	なし	TCP(6)/78	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	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	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup	同等に許可	はい（True）

ネストされたサービス オブジェクト グループを使用するアクセスルール

Cisco ASA の構成：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
```

変換の例

```
 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	ドメイン	値（プロトコル/ポート）	オーバーライド
legServGroup1_1	オブジェクト	なし	TCP(6)/78	False
legServGroup1_2	オブジェクト	なし	TCP(6)/79	False
legServGroup2_1	オブジェクト	なし	TCP(6)/80	False
legServGroup2_2	オブジェクト	なし	TCP(6)/81	False
legServGroup1	グループ	なし	legServGroup1_1 legServGroup1_2	False
legServGroup2	グループ	なし	legServGroup2_1 legServGroup2_2	False

ネストされたグループである LegacyServiceNestedGrp はフラット化されているため、変換された構成にはそのグループに相当するものが含まれないことに注意してください。

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	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	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	同等に許可	はい（True）

ネストされた拡張サービス オブジェクト グループを使用するアクセスルール

Cisco ASA の構成：

```
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
```

変換の例

```
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	ドメイン	値（プロトコル/ポート）	オーバーライド
http_src	オブジェクト	なし	TCP(6)/9000-12000	False
http_dst	オブジェクト	なし	TCP(6)/80	False
http-proxy_src	オブジェクト	なし	TCP(6)/9000-12000	False
http-proxy_dst	オブジェクト	なし	TCP(6)/8080	False
all-httpz-dst	グループ	なし	TCP(6)/443	False

ネストされたグループである all-httpz はフラット化されているため、変換された構成にはそのグループに相当するものが含まれないことに注意してください。

表 *12*：アクセスコントロールとプレフィルタルール

名前	送信元ゾーン	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	アクション	有効
acp1#1_1	任意	任意	任意	任意	http_src	http_dst	同等に許可	はい（True）
acp1#1_2	任意	任意	任意	任意	http-proxy_src	http-proxy_dst	同等に許可	はい（True）
acp1#1_3	任意	任意	任意	任意	任意	all-httpz-dst	同等に許可	はい（True）

「gt」および「neq」演算子を使用するサービスオブジェクトがあるアクセスルール

Cisco ASA の構成：

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

変換先：

変換の例

表 *13 :* ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
testOperator_src	オブジェクト	なし	TCP(6)/101-65535	False
testOperator_dst_1	オブジェクト	なし	TCP(6)/1-199	False
testOperator_dst_2	オブジェクト	なし	TCP(6)/201-65535	False
testOperator_dst	グループ	なし	testOperator_dst_1、testOperator_dst_2	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	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	アクション	有効
acp1#1	任意	任意	任意	任意	testOperator_src	testOperator_dst	同等に許可	はい（True）

「lt」および「neq」演算子を使用するセキュリティオブジェクトがあるアクセスルール

Cisco ASA の構成：

```
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	ドメイン	値（プロトコル/ポート）	オーバーライド
testOperator_src	オブジェクト	なし	TCP(6)/101-65535	False
testOperator_dst	オブジェクト	なし	TCP(6)/1-199	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	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	アクション	有効
acp1#1	任意	任意	任意	任意	testOperator_src	testOperator_dst	同等に許可	はい（True）

変換の例

「eq」演算子およびポートのリテラル値を使用したTCPサービスオブジェクトがあるアクセスルール

Cisco ASA の構成：

```
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	ドメイン	値（プロトコル/ポート）	オーバーライド
svcObj1_src	オブジェクト	なし	TCP(6)/21	False
svcObj1_dst	オブジェクト	なし	TCP(6)/22	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	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	アクション	有効
acp1#1	任意	任意	任意	任意	svcObj1_src	svcObj1_dst	同等に許可	はい（True）

Cisco ASA の構成：

```
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	ドメイン	値（プロトコル/ポート）	オーバーライド
icmpObj	オブジェクト	なし	ICMP(1)/Echo reply	False

変換の例

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	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	アクション	有効
acp1#1	任意	任意	任意	任意	任意	icmpObj	同等に許可	はい（True）

プロトコル サービス オブジェクトを使用するアクセスルール

Cisco ASA の構成：

```
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	ドメイン	値（プロトコル/ポート）	オーバーライド
testProtocol	オブジェクト	なし	TCP(6)	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	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	アクション	有効
acp1#1	任意	任意	任意	任意	任意	testProtocol	同等に許可	はい（True）

拡張済みサービスオブジェクトを使用するアクセスルール（送信元のみ）

Cisco ASA の構成：

```
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：

変換の例

表 *23 :* ポート オブジェクト

名前	タイプ	ドメイン	値（プロトコル/ポート）	オーバーライド
serviceObj_src_1	オブジェクト	なし	TCP(6)/300	False
serviceObj_src_2	オブジェクト	なし	TCP(6)/800	False
serviceObj	グループ	なし	serviceObj_src_1 serviceObj_src_2	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	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	アクション	有効
acp1#1	任意	任意	任意	任意	任意	serviceObj	同等に許可	はい（True）

拡張済みサービスオブジェクトを使用するアクセスルール（送信元および接続先のみ）

Cisco ASA の構成：

```
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	ドメイン	値（プロトコル/ポート）	オーバーライド
serviceObj_src	オブジェクト	なし	TCP(6)/300	False
serviceObj_dst	オブジェクト	なし	TCP(6)/400	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	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	アクション	有効
acp1#1	任意	任意	任意	任意	serviceObj_src	serviceObj_dst	同等に許可	はい（True）

変換の例

送信元ポートのポート引数演算子「neq」を使用するアクセスルール

Cisco ASA の構成：

```
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	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	アクション	有効
acp1#1	任意	任意	任意	任意	1-299、301-65535	任意	同等に許可	はい（True）

送信元ポートと宛て先ポートのポート引数演算子「neq」を使用するアクセスルール

Cisco ASA の構成：

```
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とプレフィルタルール

名前	送信元ゾーン	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	アクション	有効
acp1#1_1	任意	任意	任意	任意	1-299	1-399	同等に許可	はい（True）
acp1#1_2	任意	任意	任意	任意	301-65535	1-399	同等に許可	はい（True）
acp1#1_3	任意	任意	任意	任意	1-299	401-65535	同等に許可	はい（True）
acp1#1_4	任意	任意	任意	任意	301-65535	401-65535	同等に許可	はい（True）

非アクティブなアクセスルール

Cisco ASA の構成：

```
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：

変換の例

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	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	アクション	有効
acp1#1	任意	任意	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意	同等に許可	False

インバウンドトラフィックに適用されるアクセス制御リスト

Cisco ASA の構成：

```
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	選択したインターフェイス
acp1_inside_in_zone	• ルーテッド（Cisco ASA デバイスがルーテッドモードで実行されている場合） • スイッチ（Cisco ASA デバイスが透過モードで実行されている場合）	なし	任意

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	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	アクション	有効
acp1#1	acp1_inside_in_zone	任意	3.4.5.0/24	任意	TCP(6)/90	TCP(6)/80	同等に許可	はい（True）

アウトバウンドトラフィックに適用されるアクセス制御リスト

Cisco ASA の構成：

```
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：

変換の例

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	選択したインターフェイス
acp1_outside_out_zone	• ルーテッド（Cisco ASA デバイスがルーテッドモードで実行されている場合） • スイッチ（Cisco ASA デバイスが透過モードで実行されている場合）	なし	任意

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	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	アクション	有効
acp1#1	acp1_outside_out_zone	任意	3.4.5.0/24	任意	TCP(6)/90	TCP(6)/80	同等に許可	True

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。

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。