CHAPTER 63

保護ツールの使用

この章では、ネットワーク保護に使用できる多くのツールの一部について説明します。次の項目を取り上げます。

IP スプーフィングの防止

この項では、インターフェイスで Unicast Reverse Path Forwarding（Unicast RPF; ユニキャスト逆経路転送）をイネーブルにします。Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、ASA は、パケットの転送先を判定するときに宛先アドレスだけを調べます。Unicast RPF は、送信元アドレスも調べるように ASA に指示します。そのため、逆経路転送（Reverse Path Forwarding）と呼ばれます。ASA の通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートを ASA のルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、ASA はデフォルト ルートを使用して Unicast RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、ASA はデフォルト ルートを使用して、外部インターフェイスを発信元インターフェイスとして正しく識別します。

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、ASA はパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、ASA はパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

Unicast RPF をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# ip verify reverse-path interface interface_name
```

フラグメント サイズの設定

デフォルトでは、ASA は 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントが ASA を通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

フラグメントの禁止を設定するには、次のコマンドを入力します。

```
hostname(config)# fragment chain 1 [interface_name]
```

特定のインターフェイスでフラグメント化を禁止する場合は、インターフェイス名を入力します。デフォルトでは、このコマンドはすべてのインターフェイスに適用されます。

不要な接続のブロック

あるホストがネットワークを攻撃しようとしていることがわかった場合（たとえば、システム ログ メッセージで攻撃が示された場合）、送信元 IP アドレスに基づいて接続をブロック（排除）できます。排除を削除するまで、すべての既存の接続および新しい接続がブロックされます。

（注） トラフィックをモニタする IPS（AIP SSM など）がある場合は、IPS で自動的に接続を排除できます。

接続を手動で排除するには、次の手順を実行します。

ステップ 1　必要に応じて、次のコマンドを入力し、接続に関する情報を表示します。

```
hostname# show conn
```

ASA は、各接続に関する情報を次のように表示します。

```
TCP out 64.101.68.161:4300 in 10.86.194.60:23 idle 0:00:00 bytes 1297 flags UIO
```

ステップ 2　この送信元 IP アドレスからの接続を排除するには、次のコマンドを入力します。

```
hostname(config)# shun src_ip [dst_ip src_port dest_port [protocol]] [vlan vlan_id]
```

送信元 IP アドレスだけを入力した場合、*以後の*すべての接続が排除されます。既存の接続はアクティブのままです。

送信元 IP アドレスからの以後の接続をブロックするだけでなく、既存の接続もドロップするには、宛先 IP アドレス、送信元と宛先のポート、およびプロトコルを入力します。デフォルトでは、プロトコルは IP を表す 0 です。追加パラメータの指定は、特定の現在の接続をドロップするための簡単な方法ですが、その送信元 IP アドレスからの今後のすべての接続には、宛先パラメータに関係なく、shun がそのまま維持されます。

マルチ コンテキスト モードでは、このコマンドは管理コンテキストで入力できます。また、他のコンテキストのインターフェイスに割り当てられている VLAN ID を指定することで、他のコンテキストの接続を排除できます。

ステップ 3　排除を無効するには、次のコマンドを入力します。

```
hostname(config)# no shun src_ip [vlan vlan_id]
```

基本 IPS をサポートする IP 監査の設定

IP 監査機能は、ASA を使用しない AIP SSM に基本 IPS サポートを提供します。署名の基本リストをサポートし、署名と一致するトラフィックに対して 1 つ以上のアクションを実行するように ASA を設定できます。

この項は、次の内容で構成されています。

IP 監査の設定

IP 監査をイネーブルにするには、次の手順を実行します。

ステップ 1　情報シグニチャに対する IP 監査ポリシーを定義するには、次のコマンドを入力します。

```
hostname(config)# ip audit name name info [action [alarm] [drop] [reset]]
```

ここで、**alarm** はパケットが署名と一致したことを示すシステム メッセージを生成し、**drop** はパケットをドロップし、**reset** はパケットをドロップして接続を閉じます。アクションを定義しない場合、デフォルト アクションはアラームの生成です。

ステップ 2　攻撃シグニチャに対する IP 監査ポリシーを定義するには、次のコマンドを入力します。

```
hostname(config)# ip audit name name attack [action [alarm] [drop] [reset]]
```

ここで、**alarm** はパケットが署名と一致したことを示すシステム メッセージを生成し、**drop** はパケットをドロップし、**reset** はパケットをドロップして接続を閉じます。アクションを定義しない場合、デフォルト アクションはアラームの生成です。

ステップ 3　ポリシーをインターフェイスに割り当てるには、次のコマンドを入力します。

```
ip audit interface interface_name policy_name
```

ステップ 4　署名をディセーブルにする方法および署名の詳細については、コマンド リファレンスの **ip audit signature** コマンドを参照してください。

IP 監査のシグニチャ リスト

表 63-1 に、サポートされているシグニチャおよびメッセージ番号の一覧を示します。

表 63-1　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP options-Bad Option List	情報	IP データグラム ヘッダーの IP オプションのリストが不完全であるか、または不正な形式になっている IP データグラムを受信するとトリガーされます。IP オプションのリストには、さまざまなネットワーク管理タスクまたはデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP options-Record Packet Route	情報	データグラムの IP オプション リスト中にオプション 7（記録パケット ルート）を含む IP データグラムを受信するとトリガーされます。
1002	400002	IP options-Timestamp	情報	データグラムの IP オプション リスト中にオプション 4（タイムスタンプ）を含む IP データグラムを受信するとトリガーされます。
1003	400003	IP options-Security	情報	データグラムの IP オプション リスト中にオプション 2（セキュリティ オプション）を含む IP データグラムを受信するとトリガーされます。
1004	400004	IP options-Loose Source Route	情報	データグラムの IP オプション リスト中にオプション 3（緩慢な送信元ルート）を含む IP データグラムを受信するとトリガーされます。
1005	400005	IP options-SATNET ID	情報	データグラムの IP オプション リスト中にオプション 8（SATNET ストリーム ID）を含む IP データグラムを受信するとトリガーされます。
1006	400006	IP options-Strict Source Route	情報	データグラムの IP オプション リスト中にオプション 2（厳密な送信元ルーティング）を含む IP データグラムを受信するとトリガーされます。
1100	400007	IP Fragment Attack	攻撃	オフセット フィールドのオフセット値が 0 より大きく 5 未満になっている IP データグラムを受信するとトリガーされます。
1102	400008	IP Impossible Packet	攻撃	送信元と宛先が同じアドレスになっている IP パケットが到着するとトリガーされます。このシグニチャは、いわゆる Land Attack を捕捉します。

表 63-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1103	400009	IP Overlapping Fragments (Teardrop)	攻撃	同じ IP データグラム内に含まれている 2 つのフラグメントのオフセット値が、そのデータグラム内の位置決めを共有していることを示す場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味します。オペレーティング システムによっては、このように重複するフラグメントが正しく処理されず、重複フラグメントを受信すると例外をスローしたり、他の不適切な動作を行ったりします。Teardrop 攻撃では、これにより DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定された IP データグラムを受信するとトリガーされます。
2001	400011	ICMP Host Unreachable	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定された IP データグラムを受信するとトリガーされます。
2002	400012	ICMP Source Quench	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（ソース クエンチ）に設定された IP データグラムを受信するとトリガーされます。
2003	400013	ICMP Redirect	情報	P ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定された IP データグラムを受信するとトリガーされます。
2004	400014	ICMP Echo Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定された IP データグラムを受信するとトリガーされます。
2005	400015	ICMP Time Exceeded for a Datagram	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムの超過時間）に設定された IP データグラムを受信するとトリガーされます。

表 63-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2006	400016	ICMP Parameter Problem on Datagram	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラムのパラメータ問題）に設定された IP データグラムを受信するとトリガーされます。
2007	400017	ICMP Timestamp Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定された IP データグラムを受信するとトリガーされます。
2008	400018	ICMP Timestamp Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定された IP データグラムを受信するとトリガーされます。
2009	400019	ICMP Information Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定された IP データグラムを受信するとトリガーされます。
2010	400020	ICMP Information Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定された IP データグラムを受信するとトリガーされます。
2011	400021	ICMP Address Mask Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定された IP データグラムを受信するとトリガーされます。
2012	400022	ICMP Address Mask Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定された IP データグラムを受信するとトリガーされます。
2150	400023	Fragmented ICMP Traffic	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、他にも 1（ICMP）に設定されたフラグメント フラグが存在するか、またはオフセット フィールドにオフセット値が指定されている IP データグラムを受信するとトリガーされます。
2151	400024	Large ICMP Traffic	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP 長が 1024 より大きくなっている IP データグラムを受信するとトリガーされます。

表 63-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2154	400025	Ping of Death Attack	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、Last Fragment ビットが設定され、（IP オフセット * 8）+（IP データ長）> 65535 になっている（つまり、IP オフセット（元のパケットでのこのフラグメントの開始位置、8 バイト単位）と残りのパケットの合計が IP パケットの最大サイズより大きくなっている）IP データグラムを受信するとトリガーされます。
3040	400026	TCP NULL flags	攻撃	SYN、FIN、ACK、または RST のいずれのフラグも設定されていない 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3041	400027	TCP SYN+FIN flags	攻撃	SYN および FIN のフラグが設定されている 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3042	400028	TCP FIN only flags	攻撃	1 つの孤立 TCP FIN パケットが特定のホストの特権ポート（ポート番号が 1024 未満）に送信されるとトリガーされます。
3153	400029	FTP Improper Address Specified	情報	要求側ホストと異なるアドレスを指定して port コマンドが発行された場合にトリガーされます。
3154	400030	FTP Improper Port Specified	情報	1024 未満または 65535 より大きい値のデータ ポートを指定して port コマンドが発行された場合にトリガーされます。
4050	400031	UDP Bomb attack	攻撃	指定されている UDP 長が、指定されている IP 長より短い場合にトリガーされます。この不正な形式のパケット タイプは、サービス拒絶攻撃と関連付けられています。
4051	400032	UDP Snork attack	攻撃	送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 になっている UDP パケットが検出されるとトリガーされます。
4052	400033	UDP Chargen DoS attack	攻撃	このシグニチャは、送信元ポート 7 および宛先ポート 19 において UDP パケットが検出されるとトリガーされます。
6050	400034	DNS HINFO Request	情報	DNS サーバから HINFO レコードへのアクセスが試みられるとトリガーされます。
6051	400035	DNS Zone Transfer	情報	送信元ポートが 53 の通常の DNS ゾーン転送が実行されるとトリガーされます。
6052	400036	DNS Zone Transfer from High Port	情報	送信元ポートが 53 以外のときに不正な DNS ゾーン転送が発生するとトリガーされます。
6053	400037	DNS Request for All Records	情報	すべてのレコードに対する DNS 要求があるとトリガーされます。
6100	400038	RPC Port Registration	情報	ターゲット ホストで新しい RPC サービスを登録する試みがあるとトリガーされます。

表 63-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6101	400039	RPC Port Unregistration	情報	ターゲット ホストで既存の RPC サービスを登録解除する試みがあるとトリガーされます。
6102	400040	RPC Dump	情報	ターゲット ホストに対して RPC ダンプ要求が発行されるとトリガーされます。
6103	400041	Proxied RPC Request	攻撃	ターゲット ホストのポートマッパーにプロキシ RPC 要求が送信されるとトリガーされます。
6150	400042	ypserv (YP server daemon) Portmap Request	情報	YP サーバ デーモン（ypserv）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6151	400043	ypbind (YP bind daemon) Portmap Request	情報	YP バインド デーモン（ypbind）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6152	400044	yppasswdd (YP password daemon) Portmap Request	情報	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6153	400045	ypupdated (YP update daemon) Portmap Request	情報	YP 更新デーモン（ypupdated）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	情報	YP 転送デーモン（ypxfrd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6155	400047	mountd (mount daemon) Portmap Request	情報	マウント デーモン（mountd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6175	400048	rexd (remote execution daemon) Portmap Request	情報	リモート実行デーモン（rexd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6180	400049	rexd (remote execution daemon) Attempt	情報	rexd プログラムの呼び出しが行われるとトリガーされます。リモート実行デーモンは、プログラムをリモート実行する役割を担うサーバです。rexd プログラムの呼び出しは、システム リソースへの不正アクセスの試みを示唆している場合があります。
6190	400050	statd Buffer Overflow	攻撃	サイズの大きな statd 要求が送信されるとトリガーされます。これは、バッファをオーバーフローさせてシステムへアクセスしようとする試みの可能性があります。