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

ユニキャスト RPF（uRPF）をインターフェイス上でイネーブルにすることができます。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。

[Configuration] > [Firewall] > [Advanced] > [Anti-Spoofing Fields]

- [Interface]：インターフェイス名を一覧表示します。
- [Anti-Spoofing Enabled]：インターフェイスで Unicast RPF がイネーブルになっているかどうかを、Yes または No で示します。
- [Enable]：選択したインターフェイスに対する Unicast RPF をイネーブルにします。
- [Disable]：選択したインターフェイスに対する Unicast RPF をディセーブルにします。

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。

インターフェイスの IP フラグメント データベースのパラメータを変更するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [Fragment] ペインを選択し、[Fragment] テーブルで変更するインターフェイスを選択して、[Edit] をクリックします。

[Edit Fragment] ダイアログボックスが表示されます。

ステップ 2　[Size] フィールドで、リアセンブリを待機している IP リアセンブリ データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。

ステップ 3　[Chain] フィールドで、1 つの完全な IP パケットをフラグメント化できる最大パケット数を設定します。デフォルトは 24 パケットです。

ステップ 4　[Timeout] フィールドで、フラグメント化されたパケット全体が到着するのを待機する最大秒数を設定します。

タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。

ステップ 5　[OK] をクリックします。

ステップ 6　[Apply] をクリックします。

ステップ 7　フラグメント統計を表示するには、[Show Fragment] をクリックします。詳細については、「Show Fragment」（P.27-2）を参照してください。

Show Fragment

[Configuration] > [Properties] > [Fragment] > [Show Fragment] ペインに、各インターフェイスの現在の IP フラグメント データベースの統計情報が表示されます。

フィールド

- [Size]：*表示専用*。リアセンブリを待機する IP リアセンブリ データベース内のパケット数を表示します。デフォルトは 200 です。

- [Chain]：*表示専用*。1 つの完全な IP パケットにフラグメント化できる最大パケット数を表示します。デフォルトは 24 パケットです。
- [Timeout]：*表示専用*。フラグメント化されたパケットの全体の到着を待機する最大秒数を表示します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。パケットのすべてのフラグメントが表示の秒数内に到着しないと、すでに受信しているパケットのフラグメントはすべて破棄されます。デフォルトは 5 秒です。
- [Threshold]：*表示専用*。IP パケットのしきい値、つまりその値を超えるとリアセンブリ モジュールで新しいチェーンを作成できなくなる限界を表示します。
- [Queue]：*表示専用*。キュー内でリアセンブリを待機している IP パケットの数を表示します。
- [Assembled]：*表示専用*。正常にリアセンブリされた IP パケットの数を表示します。
- [Fail]：*表示専用*。リアセンブリの失敗試行回数を表示します。
- [Overflow]：*表示専用*。オーバーフロー キュー内の IP パケットの数を表示します。

TCP オプションの設定

[Configuration] > [Firewall] > [Advanced] > [TCP Options] ペインでは、TCP 接続のパラメータを設定できます。

フィールド

- [Inbound and Outbound Reset] : 着信および発信トラフィックの拒否された TCP 接続をリセットするかどうかを設定します。
  - [Interface]：インターフェイス名を表示します。
  - [Inbound Reset]：着信 TCP トラフィックのインターフェイスのリセット設定を、Yes または No で示します。この設定をイネーブルにすると、ASA は、ASA を通過しようとし、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての着信 TCP セッションに対して TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。
  - [Outbound Reset] : 発信 TCP トラフィックのインターフェイスのリセット設定を、Yes または No で示します。この設定をイネーブルにすると、ASA は、ASA を通過しようとし、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての発信 TCP セッションに対して TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。
  - [Edit]：インターフェイスの着信および発信のリセット設定値を設定します。
- [Other Options]：追加の TCP オプションを設定します。
  - [Send Reset Reply for Denied Outside TCP Packets]:セキュリティ レベルが最も低いインターフェイスで終了し、またアクセス リストまたは AAA 設定に基づいて ASA によって拒否された TCP パケットのリセットをイネーブルにします。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。セキュリティ レベルが最も低いインターフェイスの Inbound Resets をイネーブルにする場合（TCP Reset Settings を参照）は、この設定もイネーブルにする必要はありません。Inbound Resets は、ASA へのトラフィックとともに、ASA を通過するトラフィックも処理します。
  - [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。ホストとサーバが最初に接続を確立するときに、

両方で最大セグメント サイズを設定できます。どちらかの最大値がここで設定する値を超えると、ASA はその最大値を無効化し、ユーザが設定した値を挿入します。たとえば、ユーザが最大サイズを 1200 バイトに設定した場合に、ホストが最大サイズとして 1300 バイトを要求すると、ASA は 1200 バイトを要求するようにパケットを変更します。詳細については、“Controlling Fragmentation with the Maximum Transmission Unit and TCP Maximum Segment Size” section on page 8-8 を参照してください。

- [Force Minimum Segment Size for TCP] : 48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。ホストとサーバが最初に接続を確立するときに、両方で最大セグメント サイズを設定できます。いずれかの最大値が [Force Minimum Segment Size for TCP Proxy] フィールドで設定した値未満になる場合、ASA はその最大値を無効化し、ユーザが設定した「最小」値を挿入します（最小値は、実際には許容される最大値の中での最小の値です）。たとえば、ユーザが最小サイズを 400 バイトに設定した場合に、ホストが最大値として 300 バイトを要求すると、ASA は 400 バイトを要求するようにパケットを変更します。
- [Force TCP Connection to Linger in TIME_WAIT State for at Least 15 Seconds] : 最後の標準 TCP クローズダウン シーケンスの後、最低でも 15 秒間、各 TCP 接続が短縮 TIME_WAIT 状態に保持するように強制します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。ASA のデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後で接続が解放されます。この即時解放ヒューリスティックにより、ASA では、標準クローズ シーケンスと呼ばれる最も一般的なクロージング シーケンスに基づいて、高い接続レートを維持できます。ただし、一方の端が閉じ、もう一方の端が確認応答してから独自のクロージング シーケンスを開始する標準クローズ シーケンスとは異なり、同時クローズでは、トランザクションの両端がクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、即時解放によって接続の一方の側で CLOSING 状態が保持されます。多くのソケットを CLOSING 状態にすると、エンド ホストのパフォーマンスが低下する可能性があります。たとえば、一部の WinSock メインフレーム クライアントはこの動作を示し、メインフレーム サーバのパフォーマンスを低下させることが知られています。この機能を使用すると、同時クローズダウン シーケンスを完了するためのウィンドウが作成されます。

TCP Reset Settings

[Configuration] > [Firewall] > [Advanced] > [TCP Options] > [TCP Reset Settings] ダイアログボックスでは、インターフェイスの着信および発信リセットの設定を行えます。

フィールド

- [Send Reset Reply for Denied Inbound TCP Packets] : ASA を通過しようとし、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての着信 TCP セッションに対して TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。

  アイデンティティ要求（IDENT）接続をリセットする必要がある場合は、着信トラフィックに対して明示的にリセットを送信できます。拒否されたホストに TCP RST（TCP ヘッダーのリセット フラグ）を送信すると、RST によって着信 IDENT プロセスが停止されるため、IDENT がタイムアウトするのを待機する必要がなくなります。外部ホストは IDENT がタイムアウトするまで SYN を継続的に再送信するため、IDENT がタイムアウトするのを待機するとトラフィックの速度低下の原因となる可能性があります。そのため、**service resetinbound** コマンドによってパフォーマンスが向上する可能性があります。

- [Send Reset Reply for Denied Outbound TCP Packets]：ASA を通過しようとし、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての発信 TCP セッションに対して TCP リセットを送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。

基本 IPS をサポートする IP 監査の設定

IP 監査機能は、AIP SSM を使用しない ASA 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。

この項では、次のトピックについて取り上げます。

IP Audit Policy

[Configuration] > [Firewall] > [Advanced] > [IP Audit] > [IP Audit Policy] ペインでは、監査ポリシーを追加してインターフェイスに割り当てることができます。攻撃ポリシーと情報ポリシーは、各インターフェイスに割り当てられます。攻撃ポリシーにより、パケットが攻撃シグニチャに一致するときに実行するアクションが決まります。そのパケットは、DoS 攻撃など、ネットワークでの攻撃の一部である可能性があります。情報ポリシーにより、パケットが情報シグニチャに一致するときに実行するアクションが決まります。そのパケットは、現時点ではネットワークを攻撃していなくても、ポート スイープなどの情報収集アクティビティの一部になる可能性があります。すべてのシグニチャのリストについては、IP 監査のシグニチャ リストを参照してください。

フィールド

- [Name]：定義済み IP 監査ポリシーの名前を示します。このテーブルには、名前付きポリシーのデフォルト アクションが一覧表示されていますが（「--Default Action--」）、インターフェイスに割り当てることができる名前付きポリシーではありません。デフォルト アクションは、ポリシーでアクションを設定しない場合に、名前付きポリシーによって使用されます。デフォルト アクションを変更するには、そのアクションを選択して [Edit] ボタンをクリックします。
- [Type]：ポリシー タイプ（[Attack] または [Info]）を示します。
- [Action]：ポリシーに一致するパケットに対して実行されるアクション（[Alarm]、[Drop]、または [Reset]）を示します。複数のアクションが一覧表示されることもあります。
- [Add]：新しい IP 監査ポリシーを追加します。
- [Edit]：IP 監査ポリシーまたはデフォルト アクションを編集します。
- [Delete]：IP 監査ポリシーを削除します。デフォルト アクションは削除できません。
- [Policy-to-Interface Mappings]：攻撃および情報ポリシーを各インターフェイスに割り当てます。
  - [Interface]：インターフェイス名を表示します。

- [Attack Policy]：使用できる攻撃監査ポリシー名を一覧表示します。リストにある名前をクリックして、ポリシーをインターフェイスに割り当てます。
- [Info Policy]：使用できる情報監査ポリシー名を一覧表示します。リストにある名前をクリックして、ポリシーをインターフェイスに割り当てます。

Add/Edit IP Audit Policy Configuration

[Configuration] > [Firewall] > [Advanced] > [IP Audit] > [IP Audit Policy] > [Add/Edit IP Audit Policy Configuration] ダイアログボックスでは、インターフェイスに割り当てられる名前付き IP 監査ポリシーを追加または編集し、シグニチャ タイプごとにデフォルト アクションを変更できます。

フィールド

- [Policy Name]：IP 監査ポリシー名を設定します。ポリシー名は、追加した後では変更できません。
- [Policy Type]：ポリシー タイプを設定します。ポリシー タイプは、追加した後では変更できません。
  - [Attack]：ポリシー タイプを攻撃として設定します。
  - [Information]：ポリシー タイプを情報として設定します。
- [Action]：パケットがシグニチャに一致するときに実行するアクションを 1 つ以上設定します。アクションを選択しない場合には、デフォルト ポリシーが使用されます。
  - [Alarm]：パケットがシグニチャに一致したことを示すシステム メッセージを生成します。すべてのシグニチャのリストについては、「IP 監査のシグニチャ リスト」を参照してください。
  - [Drop]：パケットをドロップします。
  - [Reset]：パケットをドロップし、接続を閉じます。

IP Audit Signatures

[Configuration] > [Firewall] > [Advanced] > [IP Audit] > [IP Audit Signatures] ペインでは、監査シグニチャをディセーブルにできます。正規のトラフィックが頻繁にシグニチャに一致する場合には、シグニチャをディセーブルにしてみてください。リスクが伴うことを承知でシグニチャをディセーブルにすると、多数のアラームを回避できます。

すべてのシグニチャのリストについては、「IP 監査のシグニチャ リスト」（P.27-7）を参照してください。

フィールド

- [Enabled]：イネーブルになっているシグニチャを一覧表示します。
- [Disabled]：ディセーブルになっているシグニチャを一覧表示します。
- [Disable]：選択したシグニチャを [Disabled] ペインに移動します。
- [Enable]：選択したシグニチャを [Enabled] ペインに移動します。

IP 監査のシグニチャ リスト

表 27-1 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 27-1　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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Attack	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	Attack	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 27-1　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）	Attack	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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 27-1　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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Attack	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	Attack	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 27-1　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	Attack	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	Attack	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	Attack	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	Attack	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	Informational	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	Informational	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	Attack	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	Attack	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	Attack	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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 27-1　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	Informational	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	Informational	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	Attack	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Informational	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	Attack	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。