



System i

セキュリティー  
侵入検知

バージョン 6 リリース 1







System i

セキュリティー  
侵入検知

バージョン 6 リリース 1

#### お願い

本書および本書で紹介する製品をご使用になる前に、39 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5761-SS1) のバージョン 6、リリース 1、モディフィケーション 0 に適用されます。また、改訂版で断りが無い限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また、CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

<http://www.ibm.com/jp/manuals/>

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原 典： System i  
Security  
Intrusion detection  
Version 6 Release 1

発 行： 日本アイ・ビー・エム株式会社

担 当： ナショナル・ランゲージ・サポート

第1刷 2008.2

© Copyright International Business Machines Corporation 2006, 2008. All rights reserved.

# 目次

侵入検知	1	別のポリシーに基づく侵入検知ポリシーの作成	22
V6R1 の新機能	1	System i ナビゲーター での別のポリシーに基づくポリシーの作成	23
侵入検知の PDF ファイル	3	System i ナビゲーター での別のポリシーに基づくポリシーの作成	23
侵入検知の概念	3	侵入検知ポリシーの管理	23
侵入検知システムの初期設定	4	侵入検知ポリシーの変更	24
侵入検知システムの操作	5	侵入検知ポリシーの優先順位の変更	25
侵入検知および予防	7	侵入検知ポリシーの削除	25
リアルタイムでの侵入および侵出検知通知	8	侵入検知ポリシーの使用可能化	26
侵入および侵出のタイプ	9	「侵入検知ポリシー (Intrusion detection policies)」 ページからのポリシーの使用可能化	26
アタック・イベント	9	「IDS ポリシーのプロパティ (IDS Policy Properties)」 ページからのポリシーの使用可能化	26
侵出イベント	12	侵入検知ポリシーの使用不可化	26
スキャン・イベント	12	「侵入検知ポリシー (Intrusion detection policies)」 ページからのポリシーの使用不可化	27
トラフィック規定イベント	13	「IDS ポリシーのプロパティ (IDS Policy Properties)」 ページからのポリシーの使用不可化	27
可変で動的なスロットル	14	侵入検知ポリシー・ファイルのバックアップ	27
侵入検知システム GUI の使用	15	侵入検知プログラムの作成	27
System i Navigator での IDS GUI の使用	15	V5R4 システムでの侵入検知の使用	28
Systems Director Navigator for i5/OS での IDS GUI の使用	15	侵入検知イベントの表示	28
侵入検知システム・プロパティのセットアップ	15	侵入検知イベントのフィルター操作	29
電子メールおよびメッセージ通知のセットアップ	16	侵入モニター監査レコードの項目	30
侵入検知システムの始動	17	例: 侵入検知	32
System i Navigator での IDS の始動	17	例: トラフィック規定ポリシー	33
Systems Navigator Director for i5/OS での IDS の始動	17	例: 制限付き IP オプション・ポリシー	33
侵入検知システムの停止	17	例: 永続エコー・ポリシー	34
System i Navigator での IDS の停止	18	例: 電子メール通知	35
Systems Director Navigator for i5/OS での IDS の停止	18	例: 侵入検知スキャン・ポリシー	35
侵入検知ポリシーの作成	18	例: スキャン・イベントの可変で動的なスロットル	36
デフォルト侵入検知ポリシー・セットの作成	19	例: トラフィック規定イベントの可変で動的なスロットル	37
アタック・ポリシーの作成	19	侵入検知の関連情報	38
System i ナビゲーター でのアタック・ポリシーの作成	20	付録. 特記事項	39
Systems Director Navigator for i5/OS でのアタック・ポリシーの作成	20	プログラミング・インターフェース情報	40
スキャン・ポリシーの作成	20	商標	41
System i ナビゲーター でのスキャン・ポリシーの作成	21	使用条件	41
Systems Director Navigator for i5/OS でのスキャン・ポリシーの作成	21		
トラフィック規定ポリシーの作成	21		
System i ナビゲーター でのトラフィック規定ポリシーの作成	22		
Systems Director Navigator for i5/OS でのトラフィック規定ポリシーの作成	22		



---

## 侵入検知

侵入検知および予防システム (IDS) は、システムへのハッキング、システムの中断、またはシステムに対するサービス拒否の試行をユーザーに通知します。また、IDS は、システムがアタックの送信元として使用される可能性がある潜在的な侵入もモニターします。これらの潜在的な侵入および侵入は、セキュリティー監査ジャーナルの侵入モニター監査レコードとして記録され、侵入検知システムのグラフィカル・ユーザー・インターフェース (GUI) で侵入イベントとして表示されます。侵入および侵入の発生を防止するように、IDS を構成することができます。

**重要:** 侵入検知 という用語は、i5/OS® 資料では、2 とおりの方法で使用されます。第 1 の意味では、侵入検知は、機密漏れの予防および検出を指します。たとえば、ハッカーが無効のユーザー ID を使用してシステムに侵入しようとしている場合、または、経験が豊富でないユーザーが多くの特権を持すぎ、システム・ライブラリーの中の重要オブジェクトを変更しようとする場合などです。第 2 の意味では、侵入検知は、ポリシーを使用してシステムに対する疑わしいトラフィックをモニターする、侵入検知機能を指します。

侵入検知は、TCP/IP ネットワークを介して到着するアタックについての情報を収集することを必要とします。侵入 とは、情報を盗むことやサービス妨害攻撃などの、望ましくない多くの活動を指します。侵入の目的には、入手することを許可されていない情報を手に入れる (盗む) ということがある。また、ネットワーク、システムまたはアプリケーションを使用できないようにすることによって業務に損害を与える (サービス妨害) ことが目的である場合、あるいは、あるシステムを無許可使用し、さらに別の場所に侵入する手段にすることが目的である場合もある。ほとんどの侵入は、情報を収集する、アクセスを試みる、次に破壊アタックをかけるというパターンをとります。あるアタックは、ターゲット・システムによって検知され、制圧されます。また、ターゲット・システムが効果的に制圧できないアタックもあります。また、アタックは スプーフ (送信偽装) された パケットを使用することが多いので、アタックの発信元をトレースすることが困難です。また、アタックは、マシンまたはネットワークを、アタッカーの身元を非表示にする許可なしで使用することが多いので、アタックが行われたことが気付かれません。このような理由のために、情報の収集、およびシステム・アタックの検知と予防が侵入検知の重要な部分になります。

IDS GUI では、侵入検知ポリシーの構成と管理、および IDS の始動と停止を行うことができます。IDS ポリシー構成ファイルを直接編集する必要はなくなっています。IDS GUI を使用して、監査ジャーナルに記録されている侵入イベントを表示することができます。セキュリティー管理者は、IDS によって提供される監査レコードを分析して、これらのタイプのアタックからネットワークを保護することができます。さらに、IDS GUI を使用して、IDS を i5/OS システムで管理することもできます。

IDS は、ウィルス、トロイの木馬プログラム、または悪意による電子メール添付ファイルはモニターしません。

---

## V6R1 の新機能

侵入検知トピック・コレクションに関する新規情報または大幅に変更された情報についてお読みください。

### 侵入検知システム・サポート

ユーザーは、侵入検知ポリシーを使用して、TCP/IP ネットワークへの侵入および侵入を検知し、監査レコードを作成できます。V6R1 では、侵入検知システム (IDS) 機能が次のように拡張されています。

- l • IDS は、Quality of Service (QoS) サーバーから独立して機能します。V6R1 では、IDS を使用するの  
l に、Quality of Service (QoS) サーバーを始動する必要がなくなっています。
- l • また、侵入の監査を使用可能にするために QAUDLVL システム値で \*ATNEVT オプションを設定する  
l 必要はなくなりました。IDS の始動時に、このステップがユーザーの代わりに自動的に行われるため  
l です。17 ページの『侵入検知システムの始動』を参照してください。
- l • IDS は、いくつかの新しい侵入タイプを検出します。9 ページの『侵入および侵出のタイプ』を参照し  
l てください。
- l • リアルタイム侵入通知をメッセージとしてメッセージ待ち行列および電子メールに送信するように、IDS  
l をセットアップすることができます。16 ページの『電子メールおよびメッセージ通知のセットアップ』  
l を参照してください。
- l • IDS は、システムがアタックの送信元として使用される場合などに侵出を検出します。12 ページの『侵  
l 出イベント』を参照してください。
- l • IDS を使用して、侵入および侵出の発生を防止することができます。たとえば、システムがアタックさ  
l れた場合、侵入を制限または拒否するために可変で動的なスロットルをセットアップすることができま  
l す。7 ページの『侵入検知および予防』を参照してください。
- l • IDS は、IPv6 アドレスをサポートします。
- l • ICMP リダイレクト・メッセージを使用可能または使用不可にすることができます。15 ページの『侵入  
l 検知システム・プロパティのセットアップ』を参照してください。
- l • IDS は、IPL 時およびシステムがアクティブであるときに、侵入がないかモニターします。4 ページの  
l 『侵入検知システムの初期設定』を参照してください。

## l 侵入検知システム GUI

l 侵入検知システム GUI によって、侵入のモニターが簡単になります。IDS ポリシー構成ファイルでディレ  
l クティブを指定する必要がなく、発生した侵入のタイプを判別するために監査ジャーナルの侵入モニター監  
l 査レコードを暗号解読する必要がなくなっているためです。侵入検知システム GUI を使用して、侵入検知  
l ポリシーを構成および管理し、監査ジャーナルに記録されている侵入イベントを表示することができます。  
l 侵入検知システム GUI は、System i™ ナビゲーター と IBM® Systems Director Navigator for i5/OS の両  
l 方で使用できます。

l 侵入検知システム GUI は、i5/OS V5R4 を実行するシステムで使用して、IDS ポリシーを作成および管理  
l し、V5R4 でサポートされる侵入タイプをモニターすることができます。

l 詳しくは、以下の項目を参照してください。

- l • 15 ページの『侵入検知システム GUI の使用』
- l • 28 ページの『V5R4 システムでの侵入検知の使用』

PDF ファイルでは、新規情報および変更情報の左マージンにリビジョン・バー (l) が表示されることがあ  
ります。

このリリースでの新しい機能または変更された機能に関するその他の情報については、「iSeries プログラ  
ム資料説明書」を参照してください。

---

## 侵入検知の PDF ファイル

侵入検知情報の PDF ファイルを表示および印刷することができます。

本書の PDF 版を表示またはダウンロードするには、「侵入検知 (635KB)」を選択します。

次のような関連トピックの PDF を表示またはダウンロードすることができます。

- 「セキュリティー システム・セキュリティーの計画とセットアップ」。この資料には、他のタイプの侵入を検知する技法についての説明があります。

### PDF ファイルの保管

表示用または印刷用の PDF をワークステーションに保管するには、次のようにします。

1. ご使用のブラウザで PDF リンクを右クリックする。
2. PDF をローカルで保管するオプションをクリックする。
3. PDF を保管するディレクトリーを指定する。
4. 「保管」をクリックする。

### Adobe® Reader のダウンロード

これらの PDF を表示または印刷するには、システムに Adobe Reader がインストールされている必要があります。Adobe Web サイト ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html))  から、無償コピーをダウンロードできます。

---

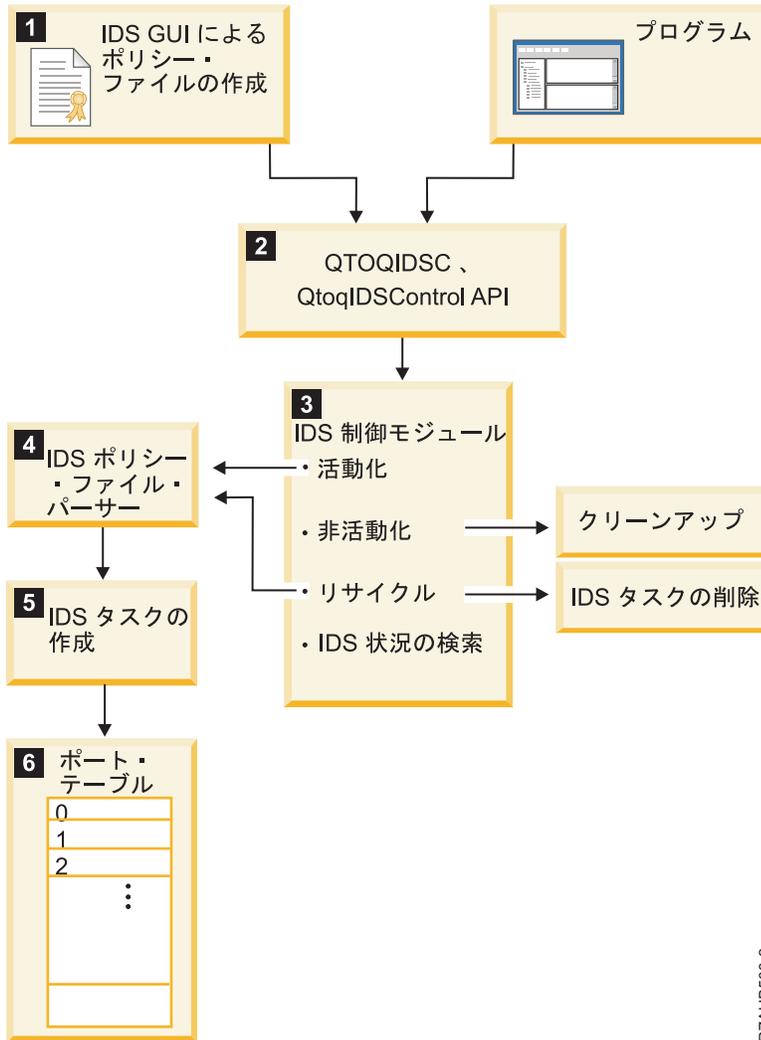
## 侵入検知の概念

- | 侵入検知ポリシー は、侵入検知システム (IDS) がシステムで潜在的な侵入および侵出がないかモニターするために使用するパラメーターを定義します。潜在的な侵入または侵出が検出された場合、侵入イベントがセキュリティー監査ジャーナルの侵入モニター・レコードに記録されます。
- | IDS が潜在的な侵入をモニターするには、その前に、侵入検知システム GUI を使用して、さまざまなタイプの侵入を対象とする侵入検知ポリシー・セットを作成する必要があります。侵入検知ポリシーが作成されて IDS が始動すると、TCP/IP スタックはこれらのポリシーに基づいて潜在的な侵入および侵出を検出します。
- | 以下を作成できます。
  - | • システム全体をモニターするデフォルト侵入検知ポリシー・セット。デフォルトのポリシーには、アタック、スキャン、およびトラフィック規定のポリシーが含まれます。
  - | • アタック・ポリシー。
  - | • スキャン・ポリシー。
  - | • トラフィック規定ポリシー。
- | 「侵入検知イベント (Intrusion detection events)」ページを使用して、システムで記録されている侵入イベントを表示したり、各イベントの詳細を表示します。

## 侵入検知システムの初期設定

侵入検知システム (IDS) は、アクティブである場合、システムの IPL 時およびシステムの稼働時に侵入をモニターします。IDS GUI を使用して侵入検知ポリシーを作成すると、IDS はポリシーの情報に基づいて一連の条件およびアクションを作成します。

次の図は、IDS GUI またはプログラムを使用して侵入検知ポリシーを作成した場合に IDS が初期設定される方法を示しています。



RZAUJ600-2

1. 侵入検知ポリシーを作成すると、IDS GUI は IDS ポリシー・ファイルを作成して、侵入検知および予防の制御 (QTOQIDSC、 QtoqIDSCControl) API を使用して IDS を活動化します。

注: 新規ポリシーを作成した後、IDS は自動的に停止および再始動して、ポリシーを有効にします。  
V5R4 では、QoS サーバーが自動的に停止および再始動します。

2. QTOQIDSC API は、ポリシー情報を IDS 制御モジュールに送信します。

3. IDS 制御モジュールには、次の 4 つの機能があります。

- IDS の始動。IDS が始動またはリサイクルされると、IDS 制御はポリシー・ファイルを読み取り、IDS ポリシー・ファイル・パーサーに送信します。

- | • IDS の停止。IDS が停止すると、IDS 制御は内部クリーンアップ機能を実行します。
- | • IDS のリサイクル (停止および再始動)。IDS ポリシーが削除されると、IDS 制御はそのポリシーに関連する IDS タスクを削除します。
- | • IDS 状況の検索。この状況は、IDS が停止しているか、アクティブであるかを示します。
- | 4. IDS ポリシー・ファイル・パーサーが IDS タスクを作成します。
- | 5. IDS タスクが、ポート・テーブルを条件およびアクション・リストと一緒に作成します。
- | 6. IDS ポート・テーブルは、TCP ポート 1 から 65 535 を表します。このテーブルには、すべてのポートに適用されるポート 0 プロビジョンも入っています。IDS GUI を使用して、条件がポートに割り当てられます。IDS GUI を使用して、アクションが条件に割り当てられます。

## | 侵入検知システムの操作

| IDS は、アクティブである間、使用可能になっている IDS ポリシーによって定義された疑わしい侵入および侵入を報告します。実動スタックおよびサービス・スタックが、これらの侵入および侵入を検出します。ユーザー定義またはデフォルトのしきい値を超える侵入または侵入イベントが発生した場合、IDS は侵入モニター・レコードを監査ジャーナルに書き込み、オプションで通知をメッセージ待ち行列および電子メール・メッセージに送信します。

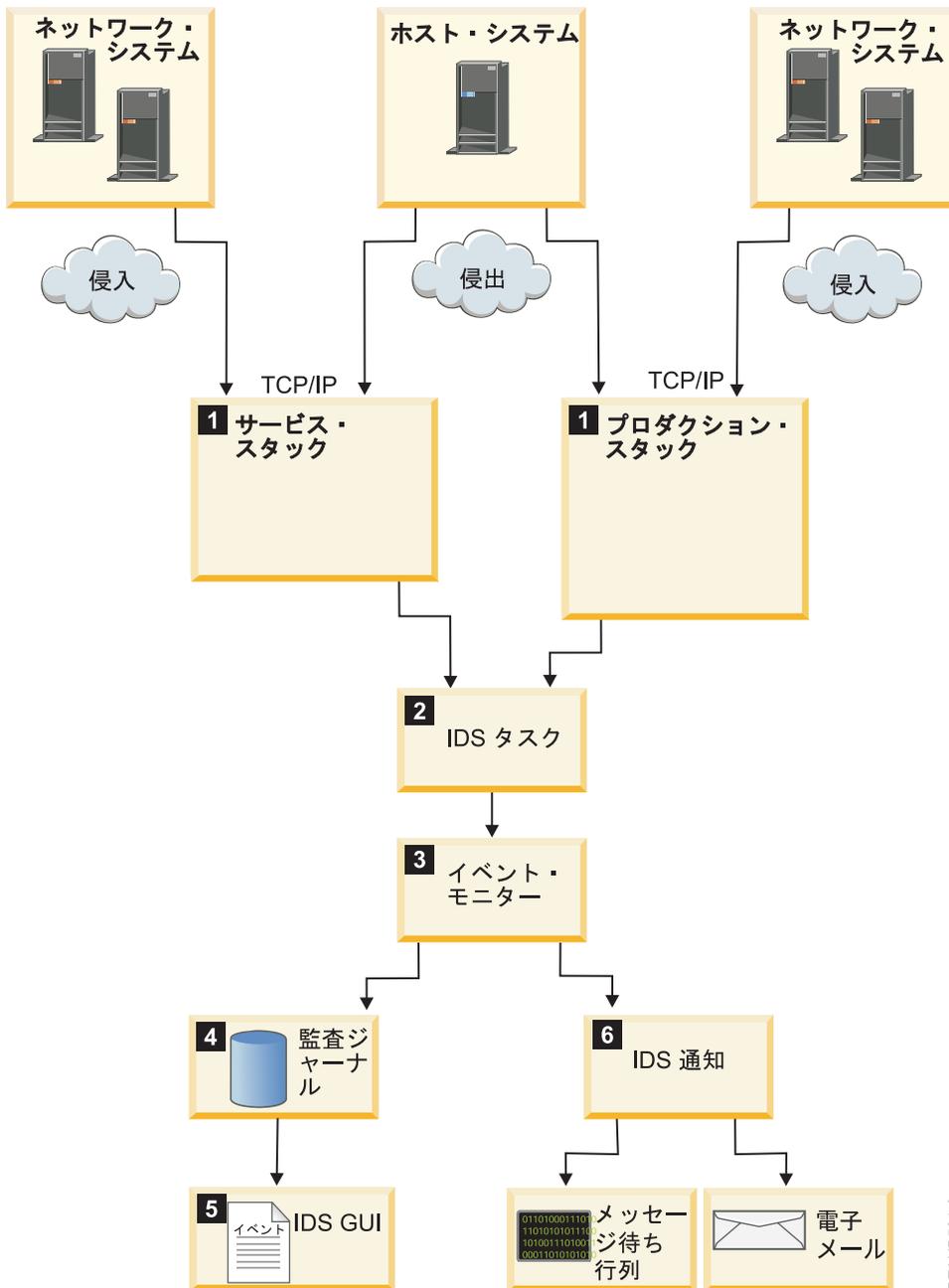
| 実動スタック は、System i プラットフォーム上の大半のネットワーク操作に関与する TCP/IP モジュールで構成されます。サービス・スタック は、System i プラットフォームのサービスおよびサポートに関与する TCP/IP モジュールで構成されます。

| サービス・スタックが最初に始動して、次の IPL まで、そのままになります。実動スタックは、サービス・スタックの後に始動して、TCP/IP が終了するまで、そのままになります。IPL の後、サービス・スタックは、IPL の前に IDS がアクティブであったかどうかを検査します。そうである場合、IDS は再び活動化されます。サービス・スタックによって検出されたすべての侵入および侵入は、VLOG または侵入モニター・レコードのいずれかによって記録されます。この段階では、IDS は、通知をメッセージ待ち行列または電子メール・アドレスに送信しません。ポリシー・ファイルが使用可能になると、両方のスタックが同じ方法で IDS と連動します。

| スタック内の TCP、UDP、および IP サポートは、潜在的に悪意のある状態を検出します。定義された侵入検知ポリシーがない場合でも、サービス・スタックは、一連のデフォルト値を使用して、特定タイプの侵入 (トラフィック規定またはスキャン・イベントなど) を検出します。一連の侵入検知ポリシーを定義すると、実動スタックは潜在的な侵入がないか検査を開始します。

| サービス・スタックは IPv4 のみの侵入および侵入を検出し、実動スタックは IPv4 と IPv6 の両方の侵入および侵入を検出します。

| 次の図は、IDS が疑わしい侵入および侵入を検出して報告する方法を示しています。



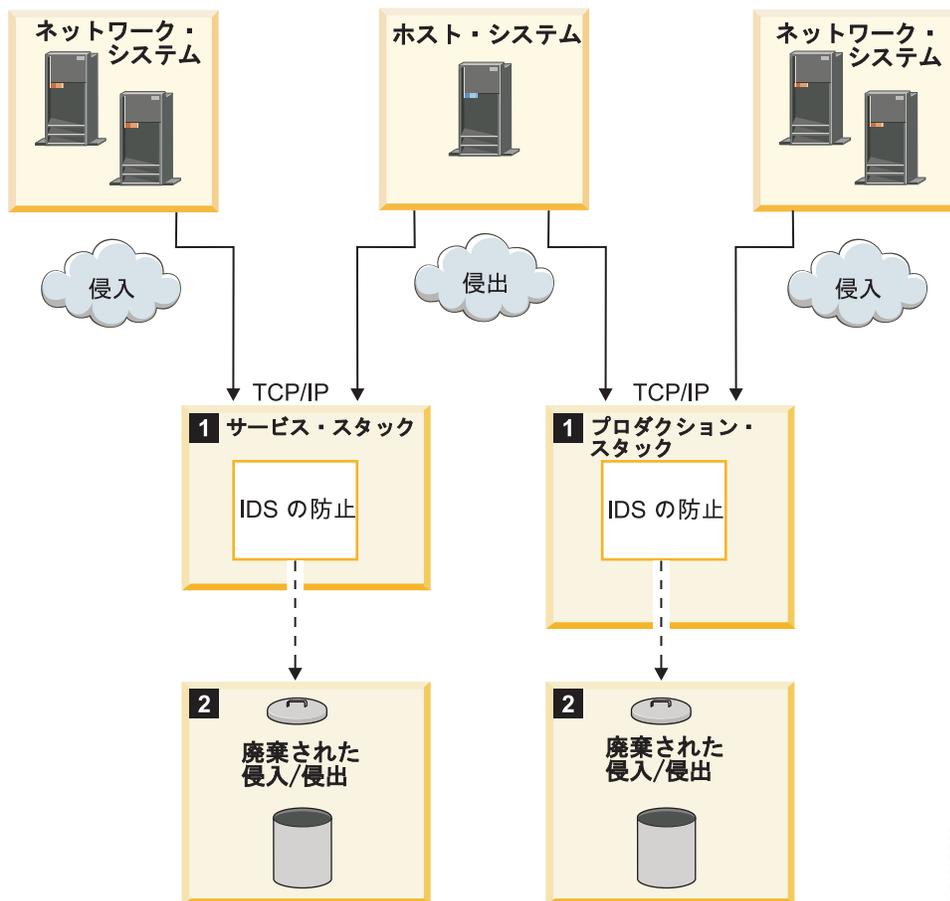
RZAUB501-0

1. 実動スタックまたはサービス・スタックが疑わしい侵入または侵入を検出すると、IDS タスクにイベントを送信します。
2. IDS タスクは、イベントを一度に 1 つずつ待ち行列から除去して、各イベントを (ポート・テーブルの) 条件と突き合わせます。また、IDS タスクは、侵入および侵入イベントに関する統計を保持します。
3. IDS は、ポリシー・ファイルで設定されたしきい値を超える侵入および侵入のイベントをシグナル通知します。
4. イベントがシグナル通知されると、侵入モニター・レコードが監査ジャーナルに作成されます。
5. IDS GUI に、侵入モニター監査レコードからの侵入イベントが表示されます。

- 6. 「IDS プロパティ (IDS Properties)」 ページで電子メールおよびメッセージ通知をセットアップしている場合、IDS 通知は、指定された電子メール・アドレスに電子メールを送信し、メッセージ待ち行列にメッセージを送信します。
- 侵入イベントを分析して、実行すべきセキュリティ・アクションを決定することができます。たとえば、侵入の発生元であるインターフェースを終了したり、可変で動的なスロットルなどの技法を用いて侵入の発生を制限または予防することができます。

## 侵入検知および予防

- 侵入検知システムを使用して、侵入および侵入の発生を予防することができます。
- 侵入防止 は、潜在的に悪意のある活動を拒否しようとするシステムです。拒否のメカニズムには、パケットのフィルター操作、可変で動的なスロットル、または接続率およびバースト限界を変更するための Quality of Service (QoS) の使用が含まれることがあります。
- 次の図は、IDS が侵入および侵入を検出してその発生を予防する方法を示しています。



1. TCP/IP サービス・サービスおよび実動スタックは、ネットワーク内のシステムからの侵入、およびホスト・システムからの侵入を検出します。
2. 可変で動的なスロットルを使用可能にしている場合、IDS は侵入または侵入を制限または廃棄します。

IDS ポリシーごとに可変で動的なスロットルを構成することができます。スロットルは、すべてのタイプの侵入および侵出を検出します。可変で動的なスロットルは、特定の侵入イベントしきい値に一致したときに自動的に始動する予防方式です。時間間隔にわたってしきい値を超えなくなるまで、スロットルはアクティブのままです。すべてまたは特定のポートおよび IP アドレスからのネットワーク・トラフィックのスロットルを選択することができます。また、低速および高速スキャンのしきい値、または最大イベント・メッセージしきい値を指定するか、IDS ポリシーでそれらのしきい値にデフォルト値を使用することもできます。そのポリシーのしきい値を超えるとスロットルは活動化され、ユーザー定義またはシステム定義のいずれかの時間間隔にわたってアクティブのままになります。時間間隔内のいずれかの時点でしきい値を超えると、スロットルは即時に増加して、時間間隔はリセットされます。スロットルは、最終的に所定のインターフェースからのすべてのパケットを拒否する可能性があります。このプロセスは、時間間隔全体にわたって、害を与えるパケット数がしきい値を超えなくなるまで続行されます。パケット数がしきい値を下回ると、スロットルは非活動状態になり、通常のパケット・フローが再開されます。

また、「IDS プロパティ (IDS Properties)」ページの「ICMP」タブで、Internet Control Message Protocol (ICMP) リダイレクト・メッセージを許可するかどうかを指定することもできます。ICMP は、エラーまたは通知メッセージの送信に使用されるプロトコルです。ICMP は、**traceroute** などの一部のユーティリティーおよび **ping** ツールによってホストに到達可能かどうかを判別するために使用されます。ICMP メッセージの例として、エコー応答、エコー要求、リダイレクト、宛先到達不能、および時間超過が挙げられます。

#### 関連概念

14 ページの『可変で動的なスロットル』

可変で動的なスロットル は、それぞれの侵入検知 (IDS) ポリシーで指定できます。使用可能にされた IDS ポリシーにスロットルが指定されている場合、疑わしい侵入または侵出が発生し、特定のしきい値に達した後でスロットルが行われます。可変で動的なスロットルは、所定の統計間隔またはスキャン間隔の間にしきい値を超えた場合にパケットの廃棄を開始します。

## リアルタイムでの侵入および侵出検知通知

IDS は、通知システムです。リアルタイム侵入通知をメッセージとしてメッセージ待ち行列および電子メールに送信するように、IDS を構成することができます。このようにして、システム管理者に特定タイプの侵入および侵出についてアラートを出し、管理者が適切な処置を取れるようにすることができます。

「IDS プロパティ (IDS Properties)」ページの「通知 (Notification)」タブを使用して、電子メールおよびメッセージ通知をセットアップします。電子メールを最大 3 つの電子メール・アドレス、メッセージ待ち行列、または両方の場所に送信することができます。また、個々の侵入検知ポリシーで電子メール通知を使用可能または使用不可にすることもできます。

IDS 通知は、次の形式を使用して電子メールを生成します。

- 「差出人」行は、侵入が検出されたシステムの名前である `qsys@system_name` を指定します。
- 「件名」行は、そのシステム上で検出された侵入または侵出のタイプの要約を示します。
- 電子メールの本文は、侵入または侵出について詳しく説明します。

ユーザー (システム管理者) は、アタックが進行中であると判別した場合、さらなるアタックを防止するために適切な手順を実行することができます。

注: 電子メールおよびメッセージ通知は、V5R4 を実行するシステムでは使用できません。

#### 関連タスク

16 ページの『電子メールおよびメッセージ通知のセットアップ』

IDS は、通知システムです。オプションで、リアルタイム侵入通知をメッセージ待ち行列および特定の電子メール・アドレスに送信するように、IDS を構成することができます。このようにして、システム

管理者に特定タイプの侵入および侵出についてアラートを出し、管理者がさらなる侵入の発生を止めるために処置を取れるようにすることができます。ポリシーごとに IDS 電子メールおよびメッセージ通知を使用可能または使用不可にすることができます。

## 侵入および侵出のタイプ

侵入検知システムは、多くのタイプの侵入イベントおよび侵出イベントを検出します。

- アドレス・ポイズニング
- フラグル・アタック
- Internet Control Message Protocol (ICMP) リダイレクト・メッセージ
- インターネット・プロトコル (IP) のフラグメント
- 誤った形式のパケット
- アウトバウンド・ロー
- ユーザー・データグラム・プロトコル (UDP) ポートに対する永続エコー
- ping of death アタック
- 制限付き IP オプション
- 制限付き IP プロトコル (侵入のみ)
- 低速および高速スキャン
- スマーフ・アタック
- SYN フラッディング
- TCP ACK ストーム
- トラフィック規定条件

## アタック・イベント

アタック・ポリシーは、システムに対するさまざまなタイプのアタックがないかモニターします。システムはアタックされたり、アタックの送信元として使用される可能性があります。IDS はアタックを検出すると、侵入イベントを監査レコードに書き込みます。

たとえば、侵入者がシステムの破壊または停止を引き起こそうとしたり、システム・リソースを拘束してサービスを妨害したり、ファイアウォールをすり抜けたり、システムに裏口から入ろうとすることがあります。侵入検知システムは、以下のタイプのアタック・イベントを検出します。

### アドレス・ポイズニング

データを別のシステム (パケットのスヌープを目的として) または存在しないアドレスにリダイレクトするハッキング手法です。アドレス・ポイズニングは、IPv4 ではアドレス解決プロトコル (ARP) スプーフィング、IPv6 では隣接者探索スプーフィングとも呼ばれます。IDS は、ARP キャッシュまたは隣接者探索キャッシュの変更時に通知を受けます。

### フラグル・アタック

ユーザー・データグラム・プロトコル (UDP) エコー要求がブロードキャストまたはマルチキャスト・アドレスに送信され、ソース・アドレスが被害者のアドレスとしてスプーフされるサービス妨害攻撃の 1 タイプです。フラグル・アタックのターゲット・ポートはエコー・ポート 7 です。アタッカーの目的は、アタッカーが送信する各ブロードキャストまたはマルチキャスト・パケットにネットワーク上の各ホストが応答することで、大量のトラフィックが生じてシステムを過負荷の状態にすることです。ソース・アドレスの

1 | プーフィングによって、複数の応答の受信側がサービス妨害 (DoS) 攻撃の被害者となります。(サービス妨害攻撃は、ネットワーク上の 1 つ以上のホストをダウンさせてその機能を正常に実行できなくなるような、ネットワークに与えられる攻撃です。)

1 | IDS は、UDP エコー要求の受信時に通知を受けて、宛先アドレスが IP ブロードキャストまたはマルチキャスト・アドレスであるかを判別します。宛先アドレスがブロードキャストまたはマルチキャスト・アドレスである場合、IDS は攻撃をシグナル通知します。

### 1 | ICMP リダイレクト・メッセージ

1 | さらに最適な経路をネットワーク経由でホストに通知することを目的としたアウト・オブ・バンド・メッセージですが、悪意によってトラフィックを特定システムにリダイレクトする攻撃のために使用される可能性があります。このタイプの攻撃では、ルーターを装うハッカーは、Internet Control Message Protocol (ICMP) リダイレクト・メッセージをホストに送信します。このメッセージには、以降のトラフィックをすべて、さらに最適な宛先への経路として特定システムに送信する必要があることが示されています。これらの ICMP リダイレクト・メッセージが発生した場合に、ユーザーに通知するか、またはそれらを見逃すように IDS をセットアップすることができます。

### 1 | IP フラグメント

1 | より大きな IP データグラムからのユーザー・データの部分のみが入ったインターネット・プロトコル (IP) データグラムです。攻撃の場合、IP フラグメントの長さが 576 バイトより小さいか、オフセットが 256 バイトより小さい可能性があります。IP フラグメントが小さすぎる場合は、ファイアウォールをすり抜けようとする、悪意のある試行の可能性があります。パケット再送信という正常な状態の場合もあります。IDS は、疑わしい IP フラグメントを検出します。

### 1 | 誤った形式のパケット

1 | TCP ヘッダーのサイズ、宛先、またはフラグが TCP/IP 規格に準拠していないパケットです。その意図は、システムを破壊または停止させることの可能性があります。また、IDS は、誤った形式のパケット・攻撃に制限付き IP プロトコルおよびオプションがあるか検査します。TCP/IP スタックは、誤った形式のパケットについて IDS に通知し、通常はそれらを廃棄します。

### 1 | アウトバウンド・ロー・アタック

1 | 標準外プロトコルを使用するアウトバウンド・パケットです。アウトバウンド・パケットは、侵出の 1 タイプです。アウトバウンド制限付き IP プロトコルは、アウトバウンド・ロー・アタックに含まれます。標準プロトコルは、TCP、UDP、ICMP、ICMPv6、Internet Group Management Protocol (IGMP)、または Open Shortest Path First (OSPF) などです。

### 1 | 永続エコー

1 | UDP エコー・ポート 7 でのサービス妨害攻撃です。ソース・ポートおよびターゲット・ポートがポート 7 に設定されると、要求は、これらのポート間を往復してエコー出力されます。アタッカーは UDP エコー要求を IP ブロードキャストまたはマルチキャスト・アドレスに送信して、スプーフ・ソース・アドレスをすべてのターゲットに提示し、応答をエコーバックさせます。スプーフ・ソース・アドレスは、ハッカーのアドレスではなく、大容量のネットワーク・トラフィックの被害者となる可能性があります。永続エコーは、侵入または侵出です。

## | Ping of death

| 最大 IP パケット・サイズの 65 536 バイトより大きな ping パケットを送信する攻撃であり、システムが過負荷の状態になる場合があります。

## | 制限付き IP オプション

| Loose Source and Record Route (LSRR) などの IP オプションで、ネットワークのトポロジーをマップして、専用 IP アドレスを発見するために使用されます。ハッカーは、ファイアウォールを通過するために、制限付き IP オプションを使用しようとする可能性があります。ユーザーは、IDS ポリシーを使用して、インバウンド・パケットまたはアウトバウンド・パケットに入れることができる IP オプションを制限することができます。制限付き IP オプションは、侵入または侵出です。

## | 制限付き IP プロトコル

| ネットワークで攻撃を攻撃するために使用できる未認識プロトコルです。  
| ICMPv6、ICMP、IGMP、TCP、または UDP 以外の IP プロトコルは、未認識プロトコルです。ハッカーは、TCP/IP プログラミング・インターフェースを経由せずにロー・ソケットに直接的に入るようにプログラミングする可能性があります。IDS は、潜在的な侵入を制限付きプロトコル・攻撃として分類することによって、その通知を受けます。制限付きプロトコルに対応する IDS ポリシーがない場合は、通知は記録されません。メインストリームでないアウトバウンド・プロトコルは、アウトバウンド・ロー・攻撃に含まれます。

| *Open Shortest Path First (OSPF)* は、ネットワーク内の各ノードへの最短パスに関する情報をルーターに送信するために使用される、内部ゲートウェイ・プロトコルです。IDS が通知を受けないその他の既知のプロトコルとは異なり、IDS は、OSPF プロトコルと「制限付きプロトコル」攻撃が入ったインバウンド・パケットに関する通知を受けます。システム内のネットワークが OSPF を使用している場合は、制限するプロトコルの範囲から OSPF を除外することを検討してください。OSPF は、ポリシーの制限付きプロトコル範囲に組み込まれている方が、頻繁に監査ジャーナルに表示されることがあります。OSPF プロトコルに関する侵入通知を受け取った場合、情報を確認して、システムが正当な目的で OSPF を使用しているかどうかを判別してください。

## | Smurf

| エコー応答でスプーフ・ソース・アドレスのフラッドが起るサービス妨害攻撃です。この応答は、スプーフ・ソース・アドレスを使用する多数の ping (ICMP エコー) 要求が 1 つ以上のブロードキャストまたはマルチキャスト・アドレスに送信される場合に引き起こされます。

## | SYN フラッド

| サービス妨害攻撃の 1 タイプであり、アタッカーは、ターゲット・コンピューターの肯定応答要求に応答せずに、多数の TCP 接続要求をターゲット・コンピューターに送信します。ターゲット・コンピューターは過負荷の状態になり、正当なユーザーに対してサービスを拒否します。

## | TCP ACK ストーム

| ハッカーまたはクラッカーがクライアント/サーバー・セッションにデータをひそかに挿入して、セッションを中断しようとする、サーバー上のサービス妨害攻撃です。ハッカーが挿入データで正しいシーケンス番号を使用すると、サーバーは、クライアントが予期しないシーケンス番号が入った ACK パケットをクライアントに送信します。実際のクライアントは、予期するシーケンス番号が入った ACK パケットを送信することによって、サーバーと再同期しようとし、この ACK パケットには、サーバーが予期しない

シーケンス番号が入っています。その後、サーバーは、前回送信した ACK パケットを送信し、この状態が繰り返されます。結果として、肯定応答 (ACK) は往復し、ハッカーが複数のクライアント/サーバー・セッションをハイジャックした後で TCP ACK ストームが発生します。

### 関連タスク

19 ページの『アタック・ポリシーの作成』

スマーフ・アタックまたは SYN フラッディングなど、さまざまなタイプのアタックからご使用のシステムを保護するために、「すべてのポリシー (All Policies)」ビューまたは「アタック・ポリシー (Attack Policies)」ビューから 1 つ以上の検出検出アタック・ポリシーを作成することができます。

## 侵出イベント

侵出は、ローカル・ホスト・システムからリモート・システムに対して引き起こされるアタック、トラフィック規定、またはスキャン・イベントです。例えば、信頼された内部関係者が、サービス妨害攻撃の発信元として会社のマシンを使用する可能性があります。侵出は、アウトバウンド侵入とも呼ばれます。

IDS は、以下のタイプのアウトバウンド・アタックを検出します。

- アウトバウンド・アタック (フラグル、フラッディング、UDP エコー要求、またはスマーフ・アタックなど)。これらのアタックは、ホストの接続先であるサブネットに対するブロードキャストまたはマルチキャスト試行として発生することがあります。これらのアタックは、侵入モニター・レコードで XATTAC として表示されます。

- 標準外プロトコルを使用するアウトバウンド・ロー・パケット。標準プロトコルは、TCP、UDP、ICMP、ICMPv6、IGMP、および OSPF などです。

- IPv6 ルーティング・ヘッダー。

- 非 listen ポートまたはクローズしたポートに対するアウトバウンド・スキャン。これらのアタックは、侵入モニター・レコードで XSCAN として表示されます。

- UDP に対するアウトバウンド・トラフィック規定イベント。これらのアタックは、侵入モニター・レコードで XTRUDP として表示されます。

- TCP に対するアウトバウンド・トラフィック規定イベント。これらのアタックは、侵入モニター・レコードで XTRTCP として表示されます。

## スキャン・イベント

スキャンは、システムに押し入ろうとする方法を探して未使用ポートに接続しようとするアタックです。

スキャンは、スプーフ IP アドレスからの接続要求の場合もあります。オープン・ポートが発見されると、ハッカーは、ぜい弱さを発見してシステムにアクセスしようとします。

IDS は、インバウンドおよびアウトバウンドの両方のスキャン・イベントを検出します。

ポート・スキャンは、管理者によってネットワークのセキュリティーを検査するために使用され、ハッカーまたはクラッカーによってシステムのオープン・ポートとぜい弱さを見つけるために使用されます。

スキャン・ポリシーは、低速スキャンと高速スキャンの両方をモニターすることができます。高速スキャンは、情報収集の試行が速いか、サービス妨害の試行を示している可能性があります。低速スキャンは、加害者がプローブするポートまたは実行中のオペレーティング・システムに関する情報を探していることを示している可能性があります。

システムの IPL 前に IDS がアクティブである場合は、IDS ポリシーが存在しなくても、サービス・スタックが侵入および侵出を検出します。IDS スキャン・ポリシーが存在する場合、低速スキャンまたは高速スキャンのしきい値を超えると、IDS はスキャン・イベントを検出したときに監査レコードを作成します。

場合によっては、高いスキャン率は、ユーザーが本当にシステムをアタックしているのではなく、ダウンしているサービスに接続しようとして試行していることを示しています。たとえば、Telnet または TCP/IP サーバーがダウンしている場合は、スキャンのように見え、IDS はスキャンを検出します。

#### 関連タスク

20 ページの『スキャン・ポリシーの作成』

オープン・ポートに対する無許可スキャンからシステムを保護するために、「すべてのポリシー (All Policies)」ビューまたは「スキャン・ポリシー (Scan Policies)」ビューから侵入検知スキャン・ポリシーを作成することができます。

#### 関連資料

35 ページの『例: 侵入検知スキャン・ポリシー』

次の例では、すべての IP アドレスおよびポート 1 から 5000 で低速スキャンと高速スキャンの両方をモニターする侵入検知スキャン・ポリシーを示します。

36 ページの『例: スキャン・イベントの可変で動的なスロットル』

次の例は、スキャン・ポリシー用に可変で動的なスロットルを設定する方法を示しています。システムがアタックされた場合、侵入を制限または拒否するためにスロットルをセットアップすることができます。

### トラフィック規定イベント

トラフィック規定ポリシーは、すべてまたは特定の IP アドレスおよびポートで確立された TCP 接続をモニターします。

トラフィック規定ポリシーは、特定範囲のアドレス、ポート、またはアプリケーションへの過度な数の接続、あるいはシステムに対するサービス妨害攻撃を探す場合があります。トラフィック規定ポリシーは、ユーザー・データグラム・プロトコル (UDP) エラーもキャッチすることができます。

場合によっては、高いネットワーク・トラフィック率は、ハッカーがネットワークを妨害しようとしているのではなく、多数の正当なユーザーまたはアプリケーションが同時にシステムにアクセスしていることを示します。正常なネットワーク・トラフィックがトラフィック規定イベントを生成していると判断した場合、トラフィック規定ポリシーを適宜に調整することができます。

UDP は、インターネット・プロトコルの 1 つで、信頼性の低い、コネクションレス・データグラム・サービスを提供します。このプロトコルによって、あるマシンまたはプロセス上のアプリケーション・プログラムが、別のマシンまたはプロセス上のアプリケーション・プログラムにデータグラムを送信できるようになる。IDS は、以下のタイプの UDP トラフィック規定イベントを検出します。

- ソケット・エラー。
- 送信側に接続されていない。
- データグラムに十分なスペースがない (バッファオーバーフロー)。

#### 関連タスク

21 ページの『トラフィック規定ポリシーの作成』

システムを過負荷の状態にする可能性がある大量のネットワーク・トラフィックがないかモニターするために、「すべてのポリシー (All Policies)」ビューまたは「トラフィック規定ポリシー (Traffic

Regulation Policies) ビューから 1 つ以上の侵入検知トラフィック規定ポリシーを作成することができます。TCP または UDP 接続をモニターすることができます。

#### 関連資料

33 ページの『例: トラフィック規定ポリシー』

次のトラフィック規定ポリシーの例は、ネットワーク全体をとおして疑わしいトラフィック、たとえば、異常に高い速度での TCP 接続の有無をトレースします。

37 ページの『例: トラフィック規定イベントの可変で動的なスロットル』

次の例は、侵入を制限または拒否するためにトラフィック規定ポリシー用に可変で動的なスロットルを設定する方法を示しています。

### 可変で動的なスロットル

可変で動的なスロットルは、それぞれの侵入検知 (IDS) ポリシーで指定できます。使用可能にされた IDS ポリシーにスロットルが指定されている場合、疑わしい侵入または侵入が発生し、特定のしきい値に達した後でスロットルが行われます。可変で動的なスロットルは、所定の統計間隔またはスキャン間隔の間にしきい値を超えた場合にパケットの廃棄を開始します。

特定の侵入検知ポリシーが多くの侵入イベントを生成している場合、サービス妨害 (DoS) 攻撃の可能性があるものによってシステムが過負荷の状態になるのを防止するために、可変で動的なスロットルの使用を検討してください。

間隔の中で「イベント・ログの最大数 (Maximum number of events to log)」しきい値に達した場合、可変で動的なスロットルが始動します。スキャンが引き続き問題となっている場合は、スロットルは次の間隔でも続行されます。

IDS スロットルは、可変かつ動的です。スロットルは、しきい値を超えたら即時に有効になる点で動的です。連続した間隔でしきい値の超過が続くとパケットの廃棄率が増える点で、スロットルは可変です。

たとえば、スロットルをデフォルト値の 100% で行うと、しきい値を 2 回続けて超えるまで、ポリシー・ポートおよび IP アドレス範囲に準拠するすべてのパケットは通過を許可されます。いずれの場合も、スロットル間隔の中でしきい値を超えると、スロットル率は自動的に 10% 減分されます。スロットルを 100% で行うと、2 回目のスロットル間隔では、10 個のパケットのうち 9 個のみが通過を許可されます。スロットルを 50% で行うと、間隔の間にパケット 2 個ごとに 1 個が廃棄されます。スロットルを 0% で行うと、スロットル間隔の中ですべてのパケットが廃棄されます。

IDS ポリシーでスロットルを指定すると、しきい値を超えた場合にスロットルは自動的に開始され、連続する各スロットル間隔ごとに 10% ずつ減分されます。スロットルは、侵入と侵入の両方で使用することができます。

#### 関連概念

7 ページの『侵入検知および予防』

侵入検知システムを使用して、侵入および侵入の発生を予防することができます。

#### 関連資料

36 ページの『例: スキャン・イベントの可変で動的なスロットル』

次の例は、スキャン・ポリシー用に可変で動的なスロットルを設定する方法を示しています。システムがアタックされた場合、侵入を制限または拒否するためにスロットルをセットアップすることができます。

- | 37 ページの『例: トラフィック規定イベントの可変で動的なスロットル』
- | 次の例は、侵入を制限または拒否するためにトラフィック規定ポリシー用に可変で動的なスロットルを設定する方法を示しています。

---

## | 侵入検知システム GUI の使用

- | 侵入検知システム GUI を使用して、侵入検知ポリシーを構成および管理し、監査ジャーナルに記録されている侵入イベントを表示することができます。侵入検知システム GUI は、System i ナビゲーター と IBM Systems Director Navigator for i5/OS の両方で使用できます。

## | System i Navigator での IDS GUI の使用

- | System i ナビゲーター で侵入検知システム GUI を使用するには、以下のステップを実行します。
- | 1. System i ナビゲーター を開始して、IDS の構成と管理を行いたいシステムにサインオンします。このシステムは、V5R4 または V6R1 を実行しています。
- | 2. 「セキュリティ (Security)」 → 「侵入検知 (Intrusion Detection)」を選択します。
- | 3. 「侵入検知システム (Intrusion Detection System)」を右クリックして、「開始 (Start)」を選択し、IDS を始動します。

## | Systems Director Navigator for i5/OSでの IDS GUI の使用

- | Systems Director Navigator for i5/OS で侵入検知システム GUI を使用するには、以下のステップを実行します。
  - | 1. ご使用の Web ブラウザーから「System i ナビゲーター・タスク (System i Navigator Tasks)」にサインオンします。
  - | 2. 「セキュリティ (Security)」を展開してから、「侵入検知 (Intrusion detection)」を展開します。
  - | 3. 「侵入検知の管理 (Manage intrusion detection)」タスクをクリックして、「侵入検知の管理 (Intrusion detection management)」ページを表示します。
- | IDS を始動した後、以下のタスクを実行できます。
  - | • IDS の始動。
  - | • IDS の停止。
  - | • 侵入検知ポリシーの管理。
  - | • 侵入検知イベントの表示。
  - | • IDS プロパティーの表示または変更 (V6R1 でのみ使用可能)。

- | 既存のポリシーまたは侵入イベントを表示するために IDS を始動する必要はありませんが、新規ポリシーを選択したり、新しい侵入および侵入がないかシステムをモニターするには IDS を始動する必要があります。

---

## | 侵入検知システム・プロパティーのセットアップ

- | 「IDS プロパティー (IDS Properties)」で、IDS の電子メールおよびメッセージ通知をセットアップして、Internet Control Message Protocol (ICMP) リダイレクト・メッセージを許可するかどうかを決定できます。
- | **前提条件:** IDS プロパティーを表示または変更するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。
- | 以下のいずれかを実行して、「IDS プロパティー (IDS Properties)」ページを開きます。

- System i ナビゲーター で、「侵入検知システム (Intrusion Detection System)」を右クリックして、「プロパティ」を選択します。
- Systems Director Navigator for i5/OS で、「侵入検知 (Intrusion detection)」を展開して、「侵入検知システム・プロパティ (Intrusion Detection System Properties)」タスクをクリックします。

注: IDS プロパティで指定するフィールドはいずれも V5R4 では使用できないため、V5R4 を実行するシステムに接続している場合は「IDS プロパティ (IDS Properties)」ページを使用できません。

#### 関連情報

特殊権限

## 電子メールおよびメッセージ通知のセットアップ

IDS は、通知システムです。オプションで、リアルタイム侵入通知をメッセージ待ち行列および特定の電子メール・アドレスに送信するように、IDS を構成することができます。このようにして、システム管理者に特定タイプの侵入および侵出についてアラートを出し、管理者がさらなる侵入の発生を止めるために処置を取れるようにすることができます。ポリシーごとに IDS 電子メールおよびメッセージ通知を使用可能または使用不可にすることができます。

**前提条件:** IDS プロパティを表示または変更するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。

IDS の電子メールおよびメッセージ通知をセットアップするには、以下のステップを実行します。

- 以下のいずれかを実行します。
    - System i ナビゲーター で、「侵入検知システム (Intrusion detection system)」を右クリックして、「プロパティ」を選択します。
    - Systems Director Navigator for i5/OS で、「侵入検知 (Intrusion detection)」を展開して、「侵入検知システム・プロパティ (Intrusion Detection System Properties)」タスクをクリックします。
  - 「IDS プロパティ (IDS Properties)」ページで、「通知 (Notification)」タブを選択します。
  - 侵入メッセージをメッセージ待ち行列に送信するには、「メッセージ通知の送信 (Send message notifications)」チェック・ボックスを選択して、メッセージ待ち行列およびライブラリーの名前を指定します。(チェック・ボックスがクリアされたままの場合、IDS はメッセージ待ち行列に通知を送信しません。)
  - 侵入メッセージを電子メール・アドレスに送信するには、「電子メール・アドレス」チェック・ボックスを選択して、電子メール・アドレスを入力します。侵入メッセージを最大 3 つの電子メール・アドレスに送信することができます。(チェック・ボックスがクリアされたままの場合、IDS は電子メール・アドレスに通知を送信しません。)
  - Internet Control Message Protocol (ICMP) リダイレクト・メッセージを許可するには、「ICMP」タブをクリックして、チェック・ボックスを選択します。(チェック・ボックスがクリアされたままの場合、IDS は ICMP リダイレクト・メッセージについて通知しません。)
- ICMP リダイレクト・メッセージは、さらに最適な宛先への経路についてホストに通知するために使用されます。ただし、ハッカーが ICMP リダイレクト・メッセージをホストに送信して、以降のトラフィックがハッカーのシステムに送信されるようにすることがあります。

侵入検知イベントは、指定されたメッセージ待ち行列および電子メール・アドレスに送信されます。「IDS プロパティ (IDS Properties)」の設定は、すべての侵入検知ポリシーに適用されます。

注: V5R4 ではこのサポートを使用できないため、V5R4 を実行しているシステムに接続されている場合は、電子メールおよびメッセージ通知をセットアップすることはできません。

ヒント: 侵入イベントの検出時に電子メールおよびメッセージ通知を送信するように、それぞれの侵入検知ポリシーを構成することができます。これを行うには、特定ポリシーの「IDS ポリシーのプロパティ (IDS Policy Properties)」ページの「通知 (Notification)」タブを選択します。

#### 関連概念

8 ページの『リアルタイムでの侵入および侵入検知通知』  
IDS は、通知システムです。リアルタイム侵入通知をメッセージとしてメッセージ待ち行列および電子メールに送信するように、IDS を構成することができます。このようにして、システム管理者に特定タイプの侵入および侵入についてアラートを出し、管理者が適切な処置を取れるようにすることができます。

## 侵入検知システムの始動

システムで侵入および侵入を検出するには、その前に侵入検知システム (IDS) を始動する必要があります。

前提条件: IDS を始動するには、\*ALLOBJ および \*IOSYSCFG 特殊権限が必要です。

侵入の監査を使用可能にするために QAUDLVL システム値で \*ATNEVT オプションを設定する必要はなくなりました。IDS の始動時に、このステップがユーザーの代わりに自動的に行われるためです。

注: V5R4 を実行するシステムで IDS を始動する場合、Quality of Service (QoS) サーバーも始動します。IDS が潜在的な侵入をモニターするには、V5R4 システムで QoS サーバーがアクティブでなければなりません。V6R1 で、IDS は QoS から分離されるため、IDS を独立して始動および停止することができます。

## System i Navigator での IDS の始動

System i ナビゲーターで IDS を始動するには、以下のステップを実行します。

「侵入検知システム (Intrusion detection system)」を右クリックして、「開始 (Start)」を選択します。

侵入検知システムが始動して、侵入の監査が使用可能になります。

## Systems Navigator Director for i5/OSでの IDS の始動

Systems Director Navigator for i5/OS で IDS を始動するには、以下のステップを実行します。

1. ご使用の Web ブラウザーから「System i ナビゲーター・タスク (System i Navigator Tasks)」にサインオンします。
2. 「セキュリティ (Security)」を展開して、「侵入検知 (Intrusion detection)」を展開し、「侵入検知の管理 (Manage intrusion detection)」タスクをクリックします。
3. 「侵入検知の管理 (Intrusion detection management)」ページで「開始 (Start)」をクリックします。

「侵入検知通知の状況 (Intrusion detection notification status)」が最新表示されて、IDS が始動され、侵入の監査が使用可能になったことが示されます。

## 侵入検知システムの停止

侵入検知システム (IDS) を停止すると、システムで侵入および侵入のモニターは行われなくなります。

前提条件: IDS を停止するには、\*ALLOBJ および \*IOSYSCFG 特殊権限が必要です。

#### 関連情報

TCP/IP テーブル除去 (RMVTCPTBL)

| TCP/IP サーバーの終了 (ENDTCPSVR)

## | System i Navigator での IDS の停止

| System i ナビゲーター で IDS を停止するには、以下のステップを実行します。

| 「侵入検知システム (Intrusion detection system)」を右クリックして、「停止 (Stop)」を選択します。

| IDS が停止します。

## | Systems Director Navigator for i5/OS での IDS の停止

| Systems Director Navigator for i5/OS で IDS を停止するには、以下のステップを実行します。

| 1. ご使用の Web ブラウザーから「System i ナビゲーター・タスク (System i Navigator Tasks)」にサインオンします。

| 2. 「セキュリティ (Security)」を展開して、「侵入検知 (Intrusion detection)」を展開し、「侵入検知の管理 (Manage intrusion detection)」タスクをクリックします。

| 3. 「侵入検知の管理 (Intrusion detection management)」ページで「停止 (Stop)」をクリックします。

| 「侵入検知通知の状況 (Intrusion detection notification status)」が最新表示されて、IDS が停止したことが示されます。

| **重要:** IDS GUI が使用不可の場合 (System i ナビゲーター 接続が失敗したか、ユーザーが誤って Web サーバー・ポートをシャットダウンしたことが原因として考えられます)、TCP/IP テーブル除去 (RMVTCPTBL \*IDS) CL コマンドを使用して、手動で IDS を停止します。

| **注:** V5R4 システムで IDS GUI を使用して IDS サポートを停止した場合は、Quality of Service (QoS) サーバーも停止します。V5R4 で IDS を手動で停止する必要がある場合は、ENDTCPSVR \*QOS コマンドを指定して QoS サーバーを停止します。これにより、IDS も停止します。

---

## | 侵入検知ポリシーの作成

| システム全体ですべてのタイプの侵入または侵出をモニターする、デフォルト侵入検知ポリシー・セットを作成することができます。また、特定の攻撃・ポリシー、スキャン・ポリシー、およびトラフィック規定ポリシーを作成することもできます。

| 侵入検知ポリシーは、「侵入検知ポリシー (Intrusion Detection Policies)」ページから作成することができます。「すべてのポリシー (All Policies)」ビューでは、攻撃・ポリシー、スキャン・ポリシー、またはトラフィック規定ポリシーを作成することができます。「攻撃・ポリシー (Attack Policies)」、「スキャン・ポリシー (Scan Policies)」、または「トラフィック規定ポリシー (Traffic Regulation Policies)」ビューでは、その特定タイプのポリシーを作成することができます。

### | 関連タスク

| 24 ページの『侵入検知ポリシーの変更』

| ユーザーが作成した侵入検知ポリシーのプロパティは、すべて変更することができます。ただし、デフォルト・ポリシーの多くのプロパティは変更することができません。

| 25 ページの『侵入検知ポリシーの削除』

| 使用する必要がなくなった侵入検知ポリシーを削除することができます。

| 26 ページの『侵入検知ポリシーの使用可能化』

| IDS は、使用可能にされた侵入検知ポリシーのみに関する侵入をモニターします。

26 ページの『侵入検知ポリシーの使用不可化』  
IDS は、使用可能にされた侵入検知ポリシーのみに関する侵入をモニターします。侵入検知ポリシーを一時的に使用不可にして、IDS が侵入のモニターにそのポリシーを使用することを防止することができます。

## デフォルト侵入検知ポリシー・セットの作成

システム上のすべての IP アドレスおよびポートですべての侵入および侵出をモニターするために使用できる、デフォルト侵入検知ポリシー・セットを作成します。

**前提条件:** 侵入検知ポリシーを処理するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。

デフォルトの侵入検知ポリシーには、アタック、スキャン、およびトラフィック規定のポリシーがあります。デフォルト侵入検知ポリシー・セットを作成するには、以下のステップを実行します。

- 以下のいずれかを実行します。
  - System i ナビゲーター で、「侵入検知システム (Intrusion detection system)」を右クリックして、「ポリシーの管理 (Manage Policies)」を選択します。
  - Systems Director Navigator for i5/OS で、「侵入検知 (Intrusion detection)」を展開して、「IDS ポリシーの管理 (Manage IDS Policies)」タスクをクリックします。
- 「侵入検知ポリシー (Intrusion detection policies)」ページで、「アクション」メニューから「新規」を選択します。「新規侵入検知ポリシー (New intrusion detection policy)」ウィザードが表示されます。
- 「作成するポリシーの選択 (Select Policy to Create)」ページで、「デフォルト侵入検知ポリシーのセットを作成 (Create a set of default intrusion detection policies)」を選択します。(この機能は、デフォルト・ポリシーがすでに存在する場合は使用不可になっています。)
- ウィザードの指示に従って、ポリシーを作成します。
- 「侵入検知ポリシー (Intrusion detection policies)」ページで「OK」をクリックして、変更を適用します。

これで、システムは、TCP/IP ネットワークを介して入ってくる疑わしいイベントを捕らえる準備ができました。

デフォルト IDS ポリシーの多くのプロパティ設定は読み取り専用ですが、ユーザーが作成した IDS ポリシーのプロパティ設定はすべて編集可能です。デフォルト IDS ポリシーの侵入検知は、システム全体を対象としています。特定範囲の IP アドレスまたはポートを対象とする、さらに具体的なポリシーが必要な場合は、たとえば、デフォルト・ポリシーに基づいてポリシーを作成して、それらの設定を変更することができます。その後、新しいポリシーをデフォルト・ポリシーより優先されるように構成することができます。ユーザーが作成した IDS ポリシーは侵入のサブセットをモニターし、システム提供の IDS ポリシーは残りの侵入をモニターします。

## アタック・ポリシーの作成

スマーフ・アタックまたは SYN フラッドなど、さまざまなタイプのアタックからご使用のシステムを保護するために、「すべてのポリシー (All Policies)」ビューまたは「アタック・ポリシー (Attack Policies)」ビューから 1 つ以上の検出アタック・ポリシーを作成することができます。

**前提条件:** 侵入検知ポリシーを処理するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。

関連タスク

22 ページの『別のポリシーに基づく侵入検知ポリシーの作成』

多くの同じ特性 (IP アドレス、ポート、および通知方式など) を持つ IDS ポリシーを作成する場合、別のポリシーに基づく IDS ポリシーを作成することができます。

#### 関連資料

9 ページの『アタック・イベント』

アタック・ポリシーは、システムに対するさまざまなタイプのアタックがないかモニターします。システムはアタックされたり、アタックの送信元として使用される可能性があります。IDS はアタックを検出すると、侵入イベントを監査レコードに書き込みます。

## System i ナビゲーター でのアタック・ポリシーの作成

System i ナビゲーター で 1 つ以上のアタック・ポリシーを作成するには、以下のステップを実行します。

1. 「侵入検知システム (Intrusion detection system)」を右クリックして、「ポリシーの管理 (Manage Policies)」を選択します。
2. 「侵入検知ポリシー (Intrusion detection policies)」ページで、「すべてのポリシー (All Policies)」ビューまたは「アタック・ポリシー (Attack Policies)」ビューのいずれかを表示します。
3. 「アクション」メニューから「新規」を選択します。
4. すべてのアタック・タイプまたは 1 つのアタック・タイプのどちらのポリシーを作成するかを決定します。ウィザードの指示に従って、アタック・ポリシーを作成します。
5. ポリシーの作成が終了したら、「侵入検知ポリシー (Intrusion detection policies)」ページで「OK」をクリックして、変更を適用します。

## Systems Director Navigator for i5/OS でのアタック・ポリシーの作成

Systems Director Navigator for i5/OS で 1 つ以上のアタック・ポリシーを作成するには、以下のステップを実行します。

1. 「侵入検知 (Intrusion detection)」を展開して、「IDS ポリシーの管理 (Manage IDS Policies)」タスクをクリックします。
2. 「侵入検知ポリシー (Intrusion detection policies)」ページで、「すべてのポリシー (All Policies)」ビューまたは「アタック・ポリシー (Attack Policies)」ビューのいずれかを表示します。
3. 「アクションの選択 (Select Action)」メニューから「新規」を選択します。
4. すべてのアタック・タイプまたは 1 つのアタック・タイプのどちらのポリシーを作成するかを決定します。ウィザードの指示に従って、アタック・ポリシーを作成します。
5. ポリシーの作成が終了したら、「侵入検知ポリシー (Intrusion detection policies)」ページで「OK」をクリックして、変更を適用します。

## スキャン・ポリシーの作成

オープン・ポートに対する無許可スキャンからシステムを保護するために、「すべてのポリシー (All Policies)」ビューまたは「スキャン・ポリシー (Scan Policies)」ビューから侵入検知スキャン・ポリシーを作成することができます。

**前提条件:** 侵入検知ポリシーを処理するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。

#### 関連タスク

22 ページの『別のポリシーに基づく侵入検知ポリシーの作成』

多くの同じ特性 (IP アドレス、ポート、および通知方式など) を持つ IDS ポリシーを作成する場合、別のポリシーに基づく IDS ポリシーを作成することができます。

## 関連資料

12 ページの『スキャン・イベント』

スキャンは、システムに押し入ろうとする方法を探して未使用ポートに接続しようとするアタックです。スキャンは、スプーフ IP アドレスからの接続要求の場合もあります。オープン・ポートが発見されると、ハッカーは、ぜい弱さを発見してシステムにアクセスしようとします。

## System i ナビゲーター でのスキャン・ポリシーの作成

System i ナビゲーター でスキャン・ポリシーを作成するには、以下のステップを実行します。

1. 「**侵入検知システム (Intrusion detection system)**」を右クリックして、「**ポリシーの管理 (Manage Policies)**」を選択します。
2. 「**侵入検知ポリシー (Intrusion detection policies)**」ページで、「**すべてのポリシー (All Policies)**」ビューまたは「**スキャン・ポリシー (Scan Policies)**」ビューのいずれかを表示します。
3. 「**アクション**」メニューから「**新規**」を選択します。
4. ウィザードの指示に従って、スキャン・ポリシーを作成します。
5. ポリシーの作成が終了したら、「**侵入検知ポリシー (Intrusion detection policies)**」ページで「**OK**」をクリックして、変更を適用します。

## Systems Director Navigator for i5/OS でのスキャン・ポリシーの作成

Systems Director Navigator for i5/OS でスキャン・ポリシーを作成するには、以下のステップを実行します。

1. 「**侵入検知 (Intrusion detection)**」を展開して、「**IDS ポリシーの管理 (Manage IDS Policies)**」タスクをクリックします。
2. 「**侵入検知ポリシー (Intrusion detection policies)**」ページで、「**すべてのポリシー (All Policies)**」ビューまたは「**スキャン・ポリシー (Scan Policies)**」ビューのいずれかを表示します。
3. 「**アクションの選択 (Select Action)**」メニューから「**新規**」を選択します。
4. ウィザードの指示に従って、スキャン・ポリシーを作成します。
5. ポリシーの作成が終了したら、「**侵入検知ポリシー (Intrusion detection policies)**」ページで「**OK**」をクリックして、変更を適用します。

## トラフィック規定ポリシーの作成

システムを過負荷の状態にする可能性がある大量のネットワーク・トラフィックがないかモニターするために、「**すべてのポリシー (All Policies)**」ビューまたは「**トラフィック規定ポリシー (Traffic Regulation Policies)**」ビューから 1 つ以上の侵入検知トラフィック規定ポリシーを作成することができます。TCP または UDP 接続をモニターすることができます。

**前提条件:** 侵入検知ポリシーを処理するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。

## 関連概念

13 ページの『トラフィック規定イベント』

トラフィック規定ポリシーは、すべてまたは特定の IP アドレスおよびポートで確立された TCP 接続をモニターします。

## 関連タスク

22 ページの『別のポリシーに基づく侵入検知ポリシーの作成』

多くの同じ特性 (IP アドレス、ポート、および通知方式など) を持つ IDS ポリシーを作成する場合、別のポリシーに基づく IDS ポリシーを作成することができます。

## System i ナビゲーター でのトラフィック規定ポリシーの作成

System i ナビゲーター でトラフィック規定ポリシーを作成するには、以下のステップを実行します。

1. 「侵入検知システム (Intrusion detection system)」を右クリックして、「ポリシーの管理 (Manage Policies)」を選択します。
2. 「侵入検知ポリシー (Intrusion detection policies)」ページで、「すべてのポリシー (All Policies)」ビューまたは「トラフィック規定ポリシー (Traffic Regulation Policies)」ビューのいずれかを表示します。
3. 「アクション」メニューから「新規」を選択します。
4. ウィザードの指示に従って、トラフィック規定ポリシーを作成します。
5. ポリシーの作成が終了したら、「侵入検知ポリシー (Intrusion detection policies)」ページで「OK」をクリックして、変更を適用します。

## Systems Director Navigator for i5/OS でのトラフィック規定ポリシーの作成

Systems Director Navigator for i5/OS でトラフィック規定ポリシーを作成するには、以下のステップを実行します。

1. 「侵入検知 (Intrusion detection)」を展開して、「IDS ポリシーの管理 (Manage IDS Policies)」タスクをクリックします。
2. 「侵入検知ポリシー (Intrusion detection policies)」ページで、「すべてのポリシー (All Policies)」ビューまたは「トラフィック規定ポリシー (Traffic Regulation Policies)」ビューのいずれかを表示します。
3. ウィザードの指示に従って、トラフィック規定ポリシーを作成します。
4. ポリシーの作成が終了したら、「侵入検知ポリシー (Intrusion detection policies)」ページで「OK」をクリックして、変更を適用します。

## 別のポリシーに基づく侵入検知ポリシーの作成

多くの同じ特性 (IP アドレス、ポート、および通知方式など) を持つ IDS ポリシーを作成する場合、別のポリシーに基づく IDS ポリシーを作成することができます。

**前提条件:** 侵入検知ポリシーを処理するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。

### 関連タスク

19 ページの『アタック・ポリシーの作成』

スマーフ・アタックまたは SYN フラッディングなど、さまざまなタイプのアタックからご使用のシステムを保護するために、「すべてのポリシー (All Policies)」ビューまたは「アタック・ポリシー (Attack Policies)」ビューから 1 つ以上の検出検出アタック・ポリシーを作成することができます。

20 ページの『スキャン・ポリシーの作成』

オープン・ポートに対する無許可スキャンからシステムを保護するために、「すべてのポリシー (All Policies)」ビューまたは「スキャン・ポリシー (Scan Policies)」ビューから侵入検知スキャン・ポリシーを作成することができます。

21 ページの『トラフィック規定ポリシーの作成』

システムを過負荷の状態にする可能性がある大量のネットワーク・トラフィックがないかモニターするために、「すべてのポリシー (All Policies)」ビューまたは「トラフィック規定ポリシー (Traffic Regulation Policies)」ビューから 1 つ以上の侵入検知トラフィック規定ポリシーを作成することができます。TCP または UDP 接続をモニターすることができます。

## System i ナビゲーター での別のポリシーに基づくポリシーの作成

System i ナビゲーター で、別のポリシーに基づいて侵入検知ポリシーを作成するには、以下のステップを実行します。

1. 「侵入検知システム (Intrusion detection system)」を右クリックして、「ポリシーの管理 (Manage Policies)」を選択します。「侵入検知ポリシー (Intrusion detection policies)」ページが表示されます。
2. 侵入検知ポリシーを右クリックして、コンテキスト・メニューから「別のポリシーに基づいた新規作成 (New Based On)」を選択します。
3. 「一般」タブで新規ポリシー名を入力して、「プロパティ」タブでその他の任意の設定を変更します。
4. 「プロパティ」ページで「OK」をクリックして、侵入検知ポリシーを作成します。ポリシーのリストに侵入検知ポリシーが表示されます。
5. 「OK」をクリックして、変更を適用します。

## System i ナビゲーター での別のポリシーに基づくポリシーの作成

System i ナビゲーター で、別のポリシーに基づいて侵入検知ポリシーを作成するには、以下のステップを実行します。

1. 「侵入検知 (Intrusion detection)」を展開して、「IDS ポリシーの管理 (Manage IDS Policies)」タスクをクリックします。「侵入検知ポリシー (Intrusion detection policies)」ページが表示されます。
2. 侵入検知ポリシーを選択して、「アクションの選択 (Select Action)」メニューから「別のポリシーに基づいた新規作成 (New Based On)」を選択します。
3. 「一般」タブで新規ポリシー名を入力して、「プロパティ」タブでその他の任意の設定を変更します。
4. 「プロパティ」ページで「OK」をクリックして、侵入検知ポリシーを作成します。ポリシーのリストに新しい侵入検知ポリシーが表示されます。
5. 「OK」をクリックして、変更を適用します。

---

## 侵入検知ポリシーの管理

ポリシーの作成、使用可能化、使用不可化、削除、または変更、別のポリシーに基づくポリシーの作成、あるいは侵入検知ポリシーの優先順位の変更を行うことができます。

**前提条件:** 侵入検知ポリシーを処理するには、\*ALLOBJ および \*IOSYSCFG 権限が必要です。

「侵入検知ポリシー (Intrusion detection policies)」ページから、以下の任意のアクションを実行できます。

- すべてのタイプの侵入検知ポリシーを表示するには、「すべてのポリシー (All Policies)」ビューを選択します。
- 1 つのタイプの侵入検知ポリシーを表示するには、「アタック・ポリシー (Attack Policies)」ビュー、「スキャン・ポリシー (Scan Policies)」ビュー、または「トラフィック規定ポリシー (Traffic Regulation Policies)」ビューを選択します。
- 「アタック (Attack)」、「スキャン (Scan)」、または「トラフィック規定ポリシー (Traffic Regulation Policy)」ビューで、「上に移動 (Move Up)」および「下に移動 (Move Down)」アクションを使用して、侵入検知ポリシーの優先順位を変更することができます。ポリシーは優先順位の順序でリストされ、優先順位が最高のポリシーがリストの先頭に表示されます。

- | • 侵入検知ポリシーを作成するには、「**アクションの選択 (Select Action)**」メニューから「**新規**」を選択  
 | します。
  - | • 別のポリシーに基づいて侵入検知ポリシーを作成するには、ポリシーを選択してから、コンテキスト・  
 | メニューまたは「**アクション**」メニューから「**別のポリシーに基づいた新規作成 (New Based On)**」を  
 | 選択します。
  - | • 侵入検知ポリシーを使用不可にするには、ポリシーを選択してから、コンテキスト・メニューまたは  
 | 「**アクション**」メニューから「**使用不可**」を選択します。
  - | • 侵入検知ポリシーを使用可能にするには、ポリシーを選択してから、コンテキスト・メニューまたは  
 | 「**アクション**」メニューから「**使用可能**」を選択します。
  - | • 侵入検知ポリシーを削除するには、ポリシーを選択してから、コンテキスト・メニューまたは「**アクシ  
 | ョン**」メニューから「**削除**」を選択します。
  - | • 侵入検知ポリシーのプロパティを表示するには、ポリシーを選択してから、コンテキスト・メニュー  
 | または「**アクション**」メニューから「**プロパティ**」を選択します。
  - | • 「**すべてのポリシー (All Policies)**」ビューでは、表示されるポリシーのリストをさらに調整するための  
 | 追加アクションを実行することもできます。たとえば、テーブルのポリシーのソートおよびフィルター  
 | を実行できます。
- | **制約事項:** V5R4 を実行しているシステムでは、ポリシーの優先順位を変更することはできません。

## | **侵入検知ポリシーの変更**

| ユーザーが作成した侵入検知ポリシーのプロパティは、すべて変更することができます。ただし、デフォ  
 | ルト・ポリシーの多くのプロパティは変更することができません。

| **前提条件:** 侵入検知ポリシーのプロパティを変更するには、\*ALLOBJ および \*IOSYSCFG 権限が必要で  
 | す。

| 侵入検知ポリシーを変更するには、以下のステップを実行します。

- | 1. 以下のいずれかを実行します。
  - | • System i ナビゲーター で、「**侵入検知システム (Intrusion detection system)**」を右クリックして、  
 | 「**ポリシーの管理 (Manage Policies)**」を選択します。
  - | • Systems Director Navigator for i5/OS で、「**侵入検知 (Intrusion detection)**」を展開して、「**IDS ポリ  
 | シーの管理 (Manage IDS Policies)**」タスクをクリックします。
- | 2. 「**侵入検知ポリシー (Intrusion detection policies)**」ページで、リストからポリシーを選択して、コンテ  
 | キスト・メニューから「**プロパティ**」を選択します。
- | 3. 侵入検知ポリシーに対して、以下の変更を行います。
  - | • 「**一般**」タブを使用して、ポリシーの説明を変更します。
  - | • 「**ローカル IP アドレス**」タブを使用して、モニターするローカル IP アドレスを選択します。IPv4  
 | または IPv6 のいずれかのアドレスをモニターできます。
  - | • 「**ローカル・ポート (Local Ports)**」タブを使用して、モニターするローカル・ポートを選択します。
  - | • 「**リモート IP アドレス**」タブを使用して、モニターするリモート IP アドレスを選択します。IPv4  
 | または IPv6 のいずれかのアドレスをモニターできます。
  - | • 「**リモート・ポート (Remote Ports)**」 タブを使用して、モニターするリモート・ポートを選択しま  
 | す。
  - | • 「**通知 (Notification)**」タブを使用して、このポリシーが通知を処理する方法、および「**IDS プロパテ  
 | ィー (IDS Properties)**」で定義されているアドレスに電子メールを送信するかどうかを変更します。

- 「**拡張 (Advanced)**」タブを使用して、パケット・スロットルを制御します。この設定は、特定の侵入イベントに関して受信する通知が多すぎる場合に役立ちます。
- スキャン・ポリシーの場合、「**スキャンしきい値 (Scan Thresholds)**」タブを使用して、低速および高速スキャンのしきい値を変更します。
- トラフィック規定ポリシーの場合、「**TCP しきい値 (TCP Thresholds)**」タブを使用して、定義された接続しきい値に基づいて侵入通知を送信するタイミングを指定します。

注: V5R4 を実行するシステムでは、ポリシーの一部のプロパティを使用できません。

#### 関連タスク

18 ページの『侵入検知ポリシーの作成』

システム全体ですべてのタイプの侵入または侵入をモニターする、デフォルト侵入検知ポリシー・セットを作成することができます。また、特定のアタック・ポリシー、スキャン・ポリシー、およびトラフィック規定ポリシーを作成することもできます。

## 侵入検知ポリシーの優先順位の変更

「アタック (Attack)」、 「スキャン (Scan)」、または「トラフィック規定ポリシー (Traffic Regulation Policies)」ビューで、侵入検知ポリシーの優先順位を変更することができます。ただし、「すべてのポリシー (All Policies)」ビューで侵入検知ポリシーの優先順位を変更することはできません。

ポリシーの優先順位は、ポリシーがリストされている順序によって決まります。ポリシーで定義されている IP アドレスおよびポートに関する侵入イベントが発生した場合、ポリシーはこの順序で処理されます。

侵入検知ポリシーの優先順位を変更するには、以下のステップを実行します。

- 「**侵入検知ポリシー (Intrusion detection policies)**」テーブルで、「**アタック・ポリシー (Attack Policies)**」、 「**スキャン・ポリシー (Scan Policies)**」、または「**トラフィック規定ポリシー (Traffic Regulation Policies)**」ビューを選択します。
- 次のようにして、1 つ以上の侵入検知ポリシーを選択します。
  - 優先順位を上げるには、アクション・メニューで「**上に移動 (Move Up)**」をクリックします。
  - 優先順位を下げるには、アクション・メニューで「**下に移動 (Move Down)**」をクリックします。

注: 「**上に移動 (Move Up)**」および「**下に移動 (Move Down)**」アクションは V6R1 でのみ使用可能です。V5R4 では、侵入検知ポリシーは、テーブルのリスト順ではなく、アルファベット順で処理されます。V5R4 では、ポリシーの優先順位を変更することはできません。

## 侵入検知ポリシーの削除

使用する必要がなくなった侵入検知ポリシーを削除することができます。

侵入検知ポリシーを削除するには、以下のステップを実行します。

- 「**侵入検知ポリシー (Intrusion detection policies)**」ページから、削除する 1 つ以上のポリシーを選択して、コンテキスト・メニューから「**削除**」を選択します。

「**すべてのポリシー (All Policies)**」、 「**アタック・ポリシー (Attack Policies)**」、 「**スキャン・ポリシー (Scan Policies)**」、および「**トラフィック規定ポリシー (Traffic Regulation Policies)**」ビューからポリシーを削除することができます。

- 削除するポリシーを確認して、「**OK**」をクリックします。

- 「**侵入検知ポリシー (Intrusion detection policies)**」ページで「**OK**」をクリックして、変更を適用します。

## 関連タスク

18 ページの『侵入検知ポリシーの作成』

システム全体ですべてのタイプの侵入または侵出をモニターする、デフォルト侵入検知ポリシー・セットを作成することができます。また、特定の攻撃・ポリシー、スキャン・ポリシー、およびトラフィック規定ポリシーを作成することもできます。

## 侵入検知ポリシーの使用可能化

IDS は、使用可能にされた侵入検知ポリシーのみに関する侵入をモニターします。

### 関連タスク

18 ページの『侵入検知ポリシーの作成』

システム全体ですべてのタイプの侵入または侵出をモニターする、デフォルト侵入検知ポリシー・セットを作成することができます。また、特定の攻撃・ポリシー、スキャン・ポリシー、およびトラフィック規定ポリシーを作成することもできます。

## 「侵入検知ポリシー (Intrusion detection policies)」 ページからのポリシーの使用可能化

侵入検知ポリシーを使用可能にするには、2 とおりの方法があります。「侵入検知ポリシー (Intrusion detection policies)」 ページから侵入検知ポリシーを使用可能にするには、以下のステップを実行します。

1. 「侵入検知ポリシー (Intrusion detection policies)」 ページで、1 つ以上のポリシーを選択して、コンテキスト・メニューから「使用可能」を選択します。選択されたポリシーが使用可能になります。
2. 「侵入検知ポリシー (Intrusion detection policies)」 ページで「OK」をクリックして、変更を適用します。

## 「IDS ポリシーのプロパティ (IDS Policy Properties)」 ページからのポリシーの使用可能化

「IDS ポリシーのプロパティ (IDS Policy Properties)」 ページから侵入検知ポリシーを使用可能にするには、以下のステップを実行します。

1. 「侵入検知ポリシー (Intrusion detection policies)」 ページで、ポリシーを選択して、コンテキスト・メニューから「プロパティ」を選択します。
2. 「一般」タブで、「使用可能なポリシー (Policy enabled)」にチェック・マークを付けて、「OK」をクリックします。選択されたポリシーが使用可能になります。
3. 「侵入検知ポリシー (Intrusion detection policies)」 ページで「OK」をクリックして、変更を適用します。

## 侵入検知ポリシーの使用不可化

IDS は、使用可能にされた侵入検知ポリシーのみに関する侵入をモニターします。侵入検知ポリシーを一時的に使用不可にして、IDS が侵入のモニターにそのポリシーを使用することを防止することができます。

### 関連タスク

18 ページの『侵入検知ポリシーの作成』

システム全体ですべてのタイプの侵入または侵出をモニターする、デフォルト侵入検知ポリシー・セットを作成することができます。また、特定の攻撃・ポリシー、スキャン・ポリシー、およびトラフィック規定ポリシーを作成することもできます。

## 「侵入検知ポリシー (Intrusion detection policies)」ページからのポリシーの使用不可化

侵入検知ポリシーを使用不可にするには、2 とおりの方法があります。「侵入検知ポリシー (Intrusion detection policies)」ページから侵入検知ポリシーを使用不可にするには、以下のステップを実行します。

1. 「侵入検知ポリシー (Intrusion detection policies)」ページで、1 つ以上のポリシーを選択します。
2. コンテキスト・メニューから「使用不可」を選択します。選択されたポリシーが使用不可になります。
3. 「侵入検知ポリシー (Intrusion detection policies)」ページで「OK」をクリックして、変更を適用します。

## 「IDS ポリシーのプロパティ (IDS Policy Properties)」ページからのポリシーの使用不可化

「IDS ポリシーのプロパティ (IDS Policy Properties)」ページから侵入検知ポリシーを使用不可にするには、以下のステップを実行します。

1. 「侵入検知ポリシー (Intrusion detection policies)」ページで、ポリシーを選択して、コンテキスト・メニューから「プロパティ」を選択します。
2. 「一般」タブで、「使用可能なポリシー (Policy enabled)」チェック・ボックスをクリアして、「OK」をクリックします。選択されたポリシーが使用不可になります。
3. 「侵入検知ポリシー (Intrusion detection policies)」ページで「OK」をクリックして、変更を適用します。

## 侵入検知ポリシー・ファイルのバックアップ

侵入検知ポリシーをバックアップすると、システムをスクラッチ・インストールする必要が生じたり、これらのポリシー定義を別のシステムに移動する場合にポリシーを復元することができます。

侵入検知ポリシーはローカルで保管することも、ディレクトリー・サーバーにエクスポートすることもできます。/QIBM/UserData/OS400/QOS/ETC ディレクトリーの idspolicy.conf ファイルをバックアップします。

失った IDS ポリシーを簡単に置き換えられるようにするには、以下のステップを実行します。

1. バックアップおよびリカバリーの計画が適切に実施されていることを確認してください。
2. IDS ポリシーを全システム・バックアップの一環としてバックアップするか、またはその他の統合ファイル・システム・ファイルと一緒にバックアップするかを決定します。

2 つの IDS ポリシー・セットを維持することを検討してください。1 つのセットは通常の勤務時間用で、もう 1 つのセットは夜間用です。たとえば、通常の勤務時間のトラフィック規定ポリシーでは多数の接続を許可しますが、夜間のポリシーではいくつかの接続のみを許可します。1 つのポリシー・セットを ETC ディレクトリーに保管して、もう 1 つのセットを別のディレクトリーに保管します。その後、毎日の終わりにポリシー・セットを交換する制御言語プログラムを作成して、IDS を再始動し、これらのポリシーを有効にします。

### 関連情報

統合ファイル・システムのバックアップ

## 侵入検知プログラムの作成

監査データおよび統計を分析して、侵入イベントまたは侵出イベントのパターンがあるかどうかを調べたり、ジャーナル処理 API を使用して監査証跡を作成するためのプログラムを作成することができます。

たとえば、疑わしいイベントが時間外に発生していることが統計からわかることがあります。システムにアタックが試みられていたことも統計からわかります。また、ネットワークが正しく構成されていなかったことや、正しく作動していないことも統計で示すことができます。

侵入検知プログラムは、ハードウェアの問題または構成の問題などの理由で発生するネットワーク問題はもちろん、疑わしいイベントも考慮に入れることがあります。たとえば、ルーターの構成がまだ完了していないことを Internet Control Message Protocol (ICMP) リダイレクト・メッセージが示す場合があります。ときどき、ネットワーク内のどのルーターが宛先までの最適の経路なのかの答えを出すのにルーターの時間がかかることがあります。

また、QTOQIDSC API を使用して、IDS の始動、停止、またはリサイクル、あるいは IDS 状況の検索を行うことができます。

#### 関連情報

侵入検知および予防の制御 (QTOQIDSC、QtoqIDSCControl) API  
ジャーナルおよびコミット API

## V5R4 システムでの侵入検知の使用

V5R4 を実行するシステムに接続している場合、IDS の始動、侵入検知ポリシーの作成と管理、および侵入イベントの表示など、大半の侵入検知システム GUI 機能を使用することができます。

V5R4 を実行するシステムで IDS GUI を使用する場合、以下の制約事項が適用されます。

- V5R4 では、「IDS プロパティー (IDS Properties)」ページを使用できません。そのため、侵入イベントに関する電子メールおよびメッセージ通知をセットアップしたり、ICMP リダイレクト・メッセージを許可するかどうかを指定することはできません。
- V5R4 侵入検知システムがサポートする侵入タイプに関するポリシーのみを作成できます。
- ポリシー名の最大長は、128 文字ではなく、31 文字です。
- IDS は、V5R4 を実行するシステムでは IPv6 アドレスをサポートしません。
- IDS ポリシーに関して送信される侵入通知の数を減らすことができる、可変で動的なスロットルを実行することはできません。
- IDS ポリシーは、優先順位の順序ではなく、アルファベット順で処理されます。V5R4 では、IDS ポリシーの優先順位を変更することはできません。
- V5R4 では、IDS は Quality of Service (QoS) と統合されています。IDS を始動または停止するには、QoS サーバーを始動または停止する必要があります。侵入をモニターするには、QoS サーバーがアクティブでなければなりません。

---

## 侵入検知イベントの表示

侵入検知システム GUI を使用して、潜在的な侵入イベントのリストと各イベントの詳細情報を表示します。System i ナビゲーター を使用している場合は、指定した間隔で侵入イベントを最新表示することもできます。

侵入検知イベントを表示するには、以下のステップを実行します。

1. 以下のいずれかを実行します。
  - System i ナビゲーター で、「侵入検知システム (Intrusion detection system)」を右クリックして、「侵入検知イベント (Intrusion detection events)」を選択します。

- Systems Director Navigator for i5/OS で、「**侵入検知 (Intrusion detection)**」を展開して、「**侵入検知イベント (Intrusion detection events)**」タスクをクリックします。

2. デフォルトで、「**侵入検知イベント (Intrusion detection events)**」ページには直前の 24 時間に発生したイベントがリストされます。以下のタスクのいずれかを実行します。

- 侵入検知イベントを即時に最新表示するには、「**アクション**」メニューから「**即時最新表示 (Refresh Now)**」を選択します。
- 侵入検知イベントを間隔ごとに最新表示するには、「**アクション**」メニューから「**間隔指定最新表示 (Timed Refresh)**」を選択します。「**間隔指定最新表示 (Timed Refresh)**」ページで、間隔指定最新表示をオンにするためにチェック・マークを付けて、最新表示の間の時間を分単位で入力します。
- イベント詳細を表示するには、イベントを選択して、コンテキスト・メニューまたは「**アクション**」メニューから「**詳細**」を選択します。また、これらのイベント詳細を侵入モニター監査記録で見つけることもできます。
- 侵入イベントをフィルターに掛けるには、「**アクション**」メニューから「**編集**」または「**組み込み (Include)**」をクリックします。たとえば、システム上で発生したすべての IDS イベントを表示したり、直前の 5 時間内に発生したイベントのみを組み込むことができます。

**ヒント:** IDS GUI を使用して侵入イベントを検索できない場合は、次の CL コマンドを使用して、システム上の侵入モニター (IM) 監査記録を表示します。

```
DSPJRN JRN(QSYS/QAUDJRN) RCVRNG(*CURCHAIN) ENTYP(IM)
```

また、IM レコードをファイルにコピーして、すべての IM レコードとそれらのフィールドを表示することもできます。こうすると、侵入が関連しているかどうかを IP アドレス、タイプ、到着時刻などの順で表示することができます。次の CL コマンドを使用します。

```
CPYAUDJRNE IM  
RUNQRY *NONE QAUDITIM
```

## 侵入検知イベントのフィルター操作

IDS GUI で、侵入検知イベントの組み込み基準を指定することができます。たとえば、すべてのイベント、特定の日時から始まるすべてのイベント、または日時間隔の中のすべてのイベントを組み込むことができます。

デフォルトで、「**侵入検知イベント (Intrusion detection events)**」ページには直前の 24 時間以内に記録されたイベントが表示されます。侵入検知ポリシーをフィルターに掛けるには、以下のステップを実行します。

1. 「**侵入検知イベント (Intrusion detection events)**」ページを表示します。
2. 「**アクション**」メニューから「**組み込み (Include)**」を選択します。「**IDS イベント - 組み込み (IDS Events - Include)**」ページが表示されます。
3. イベントに関する以下の組み込み基準のいずれか 1 つを指定して、「**OK**」をクリックします。
  - すべての侵入検知イベント
  - 特定の日時から始まるすべての侵入検知イベント
  - 特定の日時間隔の中のすべての侵入検知イベント

「**侵入検知イベント (Intrusion detection events)**」ページは即時に最新表示されて、組み込み基準に一致するイベントが表示されます。「**編集**」ボタンの隣にある「**組み込み (Include)**」フィールドには、使用されている組み込み基準が表示されます。

**ヒント:** 「**編集**」をクリックすることによっても、侵入イベントの組み込み基準を変更することができます。

## 侵入モニター監査レコードの項目

侵入検知システム (IDS) GUI は、侵入モニター (IM) 監査レコードから生成された検出イベントを読みやすい形式で表示します。ただし、その他の監査レコードを検討しながら IM 監査レコードを検査することもできます。

次の例には、TCP ACK ストーム・アタックの侵入イベントについての情報と一緒に、IM 監査レコードの項目が示されています。151 行目から 201 行目までの情報は 16 進数であるため、奇数文字として表示される場合があります。F11 を押して、この情報を読みやすい形式で表示します。

```

          ジャーナル項目の表示
オブジェクト . . . . .      ライブラリー . . . . .
メンバー . . . . .
未完了データ . . . . . NO      項目データの最小化 . . . . . *NONE
順序 . . . . .      1201
コード . . . . .      T -  監査証跡項目
タイプ . . . . .      IM -  侵入モニター

          項目固有のデータ
桁          *...+....1....+....2....+....3....+....4....+....5
00001      'P2007-06-08-13.38.06.8811471114 004499.5.6.170 '
00051      '          020019.10.108.13'
00101      '6          ATTACK0023ACKST'
  
```

次の例には、SCAN アタックの侵入イベントについての情報と一緒に、IM 監査レコードの項目が示されています。

```

          ジャーナル項目の表示
オブジェクト . . . . .      ライブラリー . . . . .
メンバー . . . . .
未完了データ . . . . . NO      項目データの最小化 . . . . . *NONE
順序 . . . . .      1201
コード . . . . .      T -  監査証跡項目
タイプ . . . . .      IM -  侵入モニター

          項目固有のデータ
桁          *...+....1....+....2....+....3....+....4....+....5
00001      'P2007-05-25-16.03.28.8169131107 003899.5.138.154 '
00051      '          250799.5.138.154'
00101      '          SCANE 0024'
00151      ' 6 22 100000P '
  
```

次の表には、IM 監査レコードのレイアウトが示されています。この表の情報を使用して、IM 監査レコードを分析および解釈してください。

表 1. IM 監査レコードのレイアウト

フィールド・タイプ	形式	説明
項目タイプ	Char(1)	項目のタイプ <b>P</b> 潜在的な侵入イベントが検出されました。
イベントの時刻	TIMESTAMP	イベントが検出されたタイム・スタンプ (SAA タイム・スタンプ形式)。
検出点の識別コード	Char(4)	侵入イベントを検出した場所を処理するための固有 ID。このフィールドは、サービス担当員が使用します。
ローカル・アドレス・ファミリー	Char(1)	検出されたイベントに関連したローカル IP アドレス・ファミリー。

表 1. IM 監査レコードのレイアウト (続き)

フィールド・タイプ	形式	説明
ローカル・ポート番号	Zoned(5,0)	検出されたイベントに関連したローカル・ポート番号。
ローカル IP アドレス	Char(46)	検出されたイベントに関連したローカル IP アドレス。
リモート・アドレス・ファミリー	Char(1)	検出されたイベントに関連したリモート・アドレス・ファミリー。
リモート・ポート番号	Zoned(5,0)	検出されたイベントに関連したリモート・ポート番号。
リモート IP アドレス	Char(46)	検出されたイベントに関連したリモート IP アドレス。
プローブ・タイプ識別コード	Char(6)	<p>侵入または侵入の可能性を検出するために使用される条件のタイプ。可能な値には、次のものがあります。</p> <p><b>ATTACK</b> イベントを検出したアタック処置。</p> <p><b>TR-TCP、TR-UDP</b> イベントを検出したトラフィック規定処置。</p> <p><b>SCANG</b> イベントを検出したスキャン・グローバル処置。</p> <p><b>SCANE</b> イベントを検出したスキャン・イベント処置。</p> <p><b>XATTAC</b> 侵入アタックの可能性。</p> <p><b>XTRTCP</b> イベントを検出したアウトバウンド TR。</p> <p><b>XTRUDP</b> イベントを検出したアウトバウンド TR。</p> <p><b>XSCAN</b> 検出されたアウトバウンド・スキャン・イベント。</p>
イベント相関係数	Char(4)	この特定侵入イベント用の固有 ID。この ID は、監査レコードと、その他の侵入検出情報を関連付ける場合に使用できます。

表 1. IM 監査レコードのレイアウト (続き)

フィールド・タイプ	形式	説明
イベント・タイプ	Char(8)	<p>検出された潜在的な侵入のタイプを示します。可能な値:</p> <p><b>MALFPKT</b> 誤った形式のパケット</p> <p><b>FLOOD</b> フラッディング・イベント</p> <p><b>ICMPRED</b> Internet Control Message Protocol (ICMP) リダイレクト</p> <p><b>PERPECH</b> 永続エコー</p> <p><b>IPFRAG</b> IP フラグメント</p> <p><b>RESTPROT</b> 制限付き IP プロトコル</p> <p><b>RESTOPT</b> 制限付き IP オプション</p> <p><b>SMURF</b> スマーフ・アタック</p> <p><b>FRAGGLE</b> フラグル・アタック</p> <p><b>OUTRAW</b> アウトバウンド・ロー・アタック</p> <p><b>PNGDEATH</b> ping of death アタック</p>
プロトコル	Char(3)	プロトコル番号。
条件	Char(4)	IDS ポリシー・ファイルからの条件番号。
スロットル	Char(1)	<p>可能な値には、次のものがあります。</p> <p><b>0</b>      スロットルはアクティブではありません</p> <p><b>1</b>      スロットルはアクティブです</p>
廃棄パケット	Zoned(5,0)	スロットル時の廃棄パケットの数。
予約済み	Char(7)	将来の使用のために予約済み。
疑わしいパケット	Char(1002)	<p>検出されたイベントに関連付けられている IP パケットの最初の 1000 バイトまでを含むことが可能な可変長フィールド。このフィールドにはバイナリー・データが含まれており、65535 の CCSID が含まれている場合と同様に処理する必要があります。最初の 2 バイトには、疑いがあるパケット情報の長さが含まれます。</p>

## 例: 侵入検知

このセクションに記載されている例を読んで、さまざまなタイプの侵入検知ポリシーを作成します。

## 例: トラフィック規定ポリシー

次のトラフィック規定ポリシーの例は、ネットワーク全体をとおして疑わしいトラフィック、たとえば、異常に高い速度での TCP 接続の有無をトレースします。

トラフィック規定イベントは、完了した接続ハンドシェイクと相関関係をとります。侵入検知システムは、IDS ポリシーで指定されている IP アドレスおよびポートを介して TCP トラフィックを追跡します。ユーザー指定のしきい値に一致した場合、IDS は侵入イベントを生成します。

この侵入検知ポリシーでは、1000 という TCP 接続制限、100% の TCP 接続パーセンテージ、60 分の統計間隔、および 5 つの最大イベント・メッセージ数が指定されています。IDS が、ローカル・アドレス 9.10.11.000 から 9.10.11.255 でポート 8000 への 1001 番目の TCP 接続を検出すると、侵入通知を指定された電子メール・アドレスに送信して、通知を監査ジャーナルに記録します。「**侵入検知イベント (Intrusion detection events)**」ページを使用して、記録されているイベントを表示します。IDS は、それぞれ 60 分の間隔の中で最大 5 つの侵入通知を送信することができます。

システムが生成する監査レコードの数は、侵入検知ポリシー・ファイルの「最大イベント・メッセージ数」の値によって決まります。

表 2. トラフィック規定ポリシーの例

設定値	値
ポリシー名	TR_policy
ポリシー・タイプ	トラフィック規定 (TCP)
合計 TCP 接続数のしきい値	1000
TCP 接続パーセンテージ	100
ローカル IP アドレス	9.10.11.000-9.10.11.255
ローカル・ポート	8000
リモート IP アドレス	すべての IP アドレス
リモート・ポート	すべてのポート
統計間隔	60 分間
最大イベント・メッセージ数	5
電子メール通知の送信 <sup>1</sup>	はい

<sup>1</sup> IDS が電子メール通知を送信するのは、「IDS プロパティ (IDS Properties)」ページでこのサポートを使用可能にしている場合のみです。このページで、電子メール・アドレスが指定されます。電子メール通知は、VSR4 を実行するシステムでは使用できません。

### 関連概念

13 ページの『トラフィック規定イベント』

トラフィック規定ポリシーは、すべてまたは特定の IP アドレスおよびポートで確立された TCP 接続をモニターします。

## 例: 制限付き IP オプション・ポリシー

下記は、単一のローカル IPv6 アドレス、リモート IPv6 アドレスの範囲、およびすべてのポートに対する制限付き IP オプションをターゲットとする IDS アタック・ポリシーの例です。

256 の IP オプションを使用できますが、現在よく使われているのは、わずかな数のみです。制限付き IP オプションの検査は、別のシステムに転送されるものでも、すべてのインバウンド・パケットおよびアウト

パウンド・パケットに対して行われています。ユーザーは IDS ポリシーを使用して、制限付き IP オプションが指定されたパケットについて通知して、パケットを廃棄することができます。

ハッカーが、ファイアウォールを通過するために、Loose Source and Record Route (LSRR) などの制限付き IP オプションを使用しようとする可能性があります。LSRR は、ネットワークのトポロジをマップして、専用 IP アドレスを発見するために使用されます。

表 3. 制限付き IP オプションの例

設定値	値
ポリシー名	Restricted_IP_option_policy
ポリシー・タイプ	アタック
アタック・タイプ	制限付き IP オプション
ローカル IP アドレス	2001:0db8:3c4d:0015:0000:0000:abcd:ef12
ローカル・ポート	すべてのポート
リモート IP アドレス	2002:9436:7a00:0000:0000:0000:0000:0000- 2002:9436:7aff:ffff:ffff:ffff:ffff:ffff
リモート・ポート	すべてのポート
統計間隔	5 分間
最大イベント・メッセージ数	5
電子メール通知の送信	はい

## 例: 永続エコー・ポリシー

この例は、ローカル・ポート 7 およびリモート・ポート 7 で永続エコーをターゲットにしている IDS アタック・タイプのポリシーの例です。

UDP ポート 7 はエコー・ポートです。アタックにおいて、ヘッダーがソース・ポートおよびターゲット・ポートをポート 7 として指定している場合、UDP データグラムは、ローカル・ポート 7 とリモート UDP ポート 7 の間を行ったり来たりエコー出力します。

永続エコーがポート 7 で発生した場合、IDS は侵入通知を「**侵入検知イベント (Intrusion detection events)**」ページおよび監査ジャーナルに送信しますが、電子メール通知は送信しません。

検出された各イベントは記録されます。IDS が多数のイベントを記録している場合は、そのためにシステムが過負荷の状態になっていないことを確認してください。IDS が記録するイベントが多すぎる場合は、以下のいずれかの方式で記録されるイベント数を減らすことができます。

- 可変で動的なスロットルを使用します。
- IDS ポリシーを変更して、より少ない数の IP アドレスをモニターするようにします。
- メッセージの最大数を制限します。

表 4. 永続エコー・ポリシーの例

設定値	値
ポリシー名	Echoes_policy
ポリシー・タイプ	アタック
アタック・タイプ	永続エコー
ローカル IP アドレス	すべての IP アドレス
ローカル・ポート	7

表 4. 永続エコー・ポリシーの例 (続き)

設定値	値
リモート IP アドレス	すべての IP アドレス
リモート・ポート	7
侵入ごとのメッセージの送信	はい
電子メール通知の送信	いいえ

## 例: 電子メール通知

次の例では、IDS がローカル・システムで侵入を検出し、電子メール通知をシステム管理者に送信しています。

以下は、制限付き IP オプション・アタックについて受信する電子メール通知の例です。

宛先: Sysadmin

件名: 潜在的な侵入である、疑わしいインバウンド・アクティビティーが sys1234 で検出されました。

このイベントについて、以下の情報が収集されました。

イベントの時刻: 日付 時刻

侵入タイプ: ATTACK

アタック・タイプ: RESTOPT

ローカル IP アドレス: 224.0.0.1

ローカル・ポート: 0

リモート IP アドレス: 9.5.211.4

リモート・ポート: 0

プロトコル: 2

スロットル・アクティブ: \*NO

廃棄パケット数: 0

条件 ID: 11

スタック: P

イベント相関係数: 0001

検出点 ID: 1001

疑わしいパケット:

X'<長い 16 進数ストリング>'

リカバリー . . . : 将来の疑わしいインバウンド・アクティビティーをブロックして妨げるために

実行できるアクションについては、i5/OS Information Center の「セキュリティ」カテゴリにある

「侵入検知」トピックを参照してください。

## 例: 侵入検知スキャン・ポリシー

次の例では、すべての IP アドレスおよびポート 1 から 5000 で低速スキャンと高速スキャンの両方をモニターする侵入検知スキャン・ポリシーを示します。

高速スキャン の数が多い場合は、情報収集の試行が速いか、サービス妨害の試行を示している可能性があります。低速スキャン の数が多い場合は、加害者がプローブするポートまたは実行中のオペレーティング・システムに関する情報を探していることを示している可能性があります。場合によっては、高いスキャン率は、ユーザーが本当にシステムをアタックしているのではなく、ダウンしているシステムに接続しようと試行していることを示しています。

この IDS スキャン・ポリシーは、ローカル・ポートとリモート・ポートの 1 から 5000 をターゲットにして、疑わしいイベントがあるかを調べます。侵入通知が記録されるのは、100 分間の間隔の中で低速スキャンの数が 64 を超えた場合、または 1 分間の間隔の中で高速スキャンの数が 20 を超えた場合です。

IDS は、各スキャン間隔の中で最大 5 つの侵入通知を送信することができます。

表 5. スキャン・ポリシーの例

設定値	値
ポリシー名	Fast_scan
ポリシー・タイプ	スキャン
低速スキャン間隔	100 分間
低速スキャンしきい値	64
高速スキャン間隔	1 分間
高速スキャンしきい値	20
ローカル IP アドレス	すべての IP アドレス
ローカル・ポート	1-5000
リモート IP アドレス	すべての IP アドレス
リモート・ポート	1-5000
最大イベント・メッセージ数	5
電子メール通知の送信	はい

### 関連資料

12 ページの『スキャン・イベント』

スキャンは、システムに押し入ろうとする方法を探して未使用ポートに接続しようとするアタックです。スキャンは、スプーフ IP アドレスからの接続要求の場合もあります。オープン・ポートが発見されると、ハッカーは、ぜい弱さを発見してシステムにアクセスしようとします。

## 例: スキャン・イベントの可変で動的なスロットル

次の例は、スキャン・ポリシー用に可変で動的なスロットルを設定する方法を示しています。システムがアタックされた場合、侵入を制限または拒否するためにスロットルをセットアップすることができます。

スロットルを使用すると、スキャン間隔の中で侵入しきい値を超えた場合にパケットを廃棄することができます。侵入しきい値を超えると、スロットルは自動的に始動します。スロットル率は、連続するスロットル間隔ごとに自動的に 10% ずつ減少します。つまり、連続する各スロットル間隔でさらに 10% 多くのパケットが廃棄されます。スロットルは、侵入と侵入の両方で使用することができます。

次の例では、以下の条件に該当する場合に、IDS スキャン・ポリシーがスキャン・イベントをシグナル通知します。

- リモート IP アドレス 9.0.0.0 から 9.255.255.255 の範囲から非 listen ポート 26 から 136 に対して接続が試行された。
- 高速スキャンが 1 分間の間隔に対して 5 回の速度で行われる、または低速スキャンが 120 分の間隔に対して 10 回の速度で行われる。

「IDS ポリシーのプロパティ (IDS Policy Properties)」の「詳細」タブでスロットルを設定します。スロットルがアクティブで、50% の比率で行われている場合、スキャン間隔で最初のパケットが廃棄され、2 番目のパケットは通過を許可されます。高速スキャンまたは低速スキャンのしきい値を超えると、スロットルは始動します。しきい値違反は、ユーザー定義の高速スキャン間隔の間に受け取るスキャン回数が高速スキャンしきい値を超える場合、またはユーザー定義の低速スキャン間隔の間に受け取る低速スキャンの回数が低速スキャンしきい値を超える場合に起こります。

スロットル間隔の中でしきい値を超えない場合、スロットルはその間隔の中でのみアクティブになります。次の例では、低速スキャンしきい値を超える場合に、スロットルが最小 120 分間にわたって有効になります。

す。スロットル間隔の中でしきい値を超えると、スロットル率は 10% ずつ減分して、最小 0% になると、その間隔ですべてのパケットが廃棄されます。スロットルが非活動化されるのは、時間間隔の中でしきい値を超えない場合のみです。

スロットル値 100% ではすべてのパケットが許可され、スロットル値 0% ではすべてのパケットの着信が停止されます。アタックの送信元を完全にシャットダウンする場合は、スロットルを 0% に設定します。

表 6. スキャン・イベントの可変で動的なスロットル

設定値	値
ポリシー名	Scan_policy2
ポリシー・タイプ	スキャン
高速スキャン間隔	1 分間
高速スキャンしきい値	5
低速スキャン間隔	120 分間
低速スキャンしきい値	10
ローカル IP アドレス	すべての IP アドレス
ローカル・ポート	すべてのポート
リモート IP アドレス	9.0.0.0 から 9.255.255.255
リモート・ポート	26 から 136
最大イベント・メッセージ数	5
スロットル	50%

### 関連概念

14 ページの『可変で動的なスロットル』

可変で動的なスロットル は、それぞれの侵入検知 (IDS) ポリシーで指定できます。使用可能にされた IDS ポリシーにスロットルが指定されている場合、疑わしい侵入または侵入が発生し、特定のしきい値に達した後でスロットルが行われます。可変で動的なスロットルは、所定の統計間隔またはスキャン間隔の間にしきい値を超えた場合にパケットの廃棄を開始します。

### 関連資料

12 ページの『スキャン・イベント』

スキャン は、システムに押し入ろうとする方法を探して未使用ポートに接続しようとするアタックです。スキャンは、スプーフ IP アドレスからの接続要求の場合もあります。オープン・ポートが発見されると、ハッカーは、ぜい弱さを発見してシステムにアクセスしようとしています。

## 例: トラフィック規定イベントの可変で動的なスロットル

次の例は、侵入を制限または拒否するためにトラフィック規定ポリシー用に可変で動的なスロットルを設定する方法を示しています。

次のトラフィック規定ポリシーを作成していて、スロットルを 50% に設定しているとします。侵入イベントが生成されるのは、確立された TCP 接続数が 1000 の接続を超える場合、または 10 分の間隔の中でシステムへの合計接続数の 10% を超える場合です。それぞれの統計間隔の間のイベント・メッセージの最大数は 1 です。この時点で、スロットルは始動します。ポート 80 で着信するすべての IP アドレスからの入力データは、10 分間 (統計間隔) にわたって正確に 50% に削減されます。この時間の間、IDS は所定プロトコル、IP アドレスの範囲、およびポートに関する統計を保持します。統計間隔が終了すると、IDS は、スロットル間隔に収集された統計に基づいて、次の 10 分の間隔でスロットルを続行するかどうかを評価します。

表 7. トラフィック規定イベントの可変で動的なスロットル

設定値	値
ポリシー名	TR_policy2
ポリシー・タイプ	トラフィック規定 (TCP)
合計 TCP 接続数のしきい値	1000
TCP 接続パーセンテージ	10
ローカル IP アドレス	すべての IP アドレス
ローカル・ポート	80
リモート IP アドレス	すべての IP アドレス
リモート・ポート	すべてのポート
統計間隔	10 分間
最大イベント・メッセージ数	1
スロットル	50%

### 関連概念

13 ページの『トラフィック規定イベント』

トラフィック規定ポリシーは、すべてまたは特定の IP アドレスおよびポートで確立された TCP 接続をモニターします。

14 ページの『可変で動的なスロットル』

可変で動的なスロットル は、それぞれの侵入検知 (IDS) ポリシーで指定できます。使用可能にされた IDS ポリシーにスロットルが指定されている場合、疑わしい侵入または侵出が発生し、特定のしきい値に達した後でスロットルが行われます。可変で動的なスロットルは、所定の統計間隔またはスキャン間隔の間にしきい値を超えた場合にパケットの廃棄を開始します。

## 侵入検知の関連情報

製品資料、IBM Redbooks™ 資料、Web サイト、およびその他の Information Center トピック・コレクションには、侵入検知トピック・コレクションに関連する情報が記載されています。PDF ファイルは、いずれも表示または印刷することができます。

### その他の情報

- 「セキュリティ システム・セキュリティの計画とセットアップ」トピック。他のタイプの侵入を検出する技法についての説明があります。
- 「機密保護解説書」トピック。侵入モニター・ジャーナル項目に関する参照情報があります。
- 「Quality of Service」トピック。V5R4 で QoS コマンドを使用して侵入検知ポリシーを活動状態にする方法の説明があります。

---

## 付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711  
東京都港区六本木 3-2-12  
日本アイ・ビー・エム株式会社  
法務・知的財産  
知的財産権ライセンス渉外

**以下の保証は、国または地域の法律に沿わない場合は、適用されません。** IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

- 1 本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム
- 1 契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項
- 1 に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. \_年を入れる\_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

---

## プログラミング・インターフェース情報

本書（「侵入検知」）には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

---

## 商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

i5/OS

IBM

IBM (ロゴ)

Redbooks

System i

- | Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国
- | における登録商標または商標です。

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

---

## 使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

**個人使用:** これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

**商業的使用:** これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。







Printed in Japan